NIST Special Publication 800-53
Revision 5

組織と情報システムのための
セキュリティおよびプライバシー管理策

ジョイントタスクフォース

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-53
Revision 5

組織と情報システムのための
セキュリティおよびプライバシー管理策

ジョイントタスクフォース

2020 年 9 月
2020 年 12 月 10 日時点の更新を含む

米国商務省
長官 Wilbur L. Ross, Jr.

米国国立標準技術研究所
所長兼標準技術担当次官 Walter Copan

発行機関

本出版物は、連邦情報セキュリティ近代化法（FISMA：Federal Information Security Modernization Act）、合衆国法典（U.S.C.）第 44 編第 3551 条以下、および公法（P.L.：Public Law）113 条-283 条に基づく法的責任を受けて米国国立標準技術研究所（NIST：National Institute of Standards and Technology）によって策定された。NIST は、連邦政府情報システムの最小限の要件を含む、情報セキュリティ規格およびガイドラインを策定する責務を負う。そうした情報セキュリティ規格およびガイドラインは、国家安全保障システムにおいては、それらのシステムに対して政策権限を行使する適切な連邦政府担当官の明示的な承認なしに適用してはならない。このガイドラインは、行政管理予算局（OMB：Office of Management and Budget）による通達（Circular）A-130 号の要件と一致している。

本出版物のいかなる内容も、法的権限の下で商務長官（Secretary of Commerce）が連邦政府機関に順守を義務付けた基準およびガイドラインを否定するものと解釈されることは望ましくない。また、これらのガイドラインは、商務長官、行政管理予算局長官（OMB Director）、またはその他の連邦政府担当官の既存の権限を変更する、または代わるものとして解釈されることは望ましくない。本出版物は、非政府組織が自由に使用してもよく、米国における著作権の対象外であるが、NIST に帰属する。

米国国立標準技術研究所　特別出版物（Special Publication）800-53　改訂第 5 版
NIST SP 800-53、Rev. 5、458 ページ（2020 年 9 月）

CODEN: NSPUE2

本出版物は、https://doi.org/10.6028/NIST.SP.800-53r5 から無料で入手可能である。

本出版物では、試行的手順や概念を適切に説明するために、特定の商業エンティティ、装置、または資料が記載されている場合がある。そうした記載は、NIST による推奨または承認を意図するものではなく、目的を達成するうえでそれらのエンティティ、装置、または資料が必ずしも最良なものであるということを意図するものでもない。

本出版物では、NIST が担う法的責任に従って現在策定している他の出版物を参照する場合がある。連邦政府機関は、本出版物に記載の情報を、概念、プラクティス、および方法論を含め、関連出版物の完成前であっても使用してもよい。したがって、現行の要件、ガイドライン、および手順が存在する場合には、各出版物が完成するまでの間、それらは引き続き有効である。計画の策定および移行のために、連邦政府機関は、NIST によるそうした新たな出版物策定の進展を綿密に追うことが望まれる。

各組織は、指定されたパブリックコメント期間中に出版物のドラフトをレビューし、NIST にフィードバックを提供することが推奨される。上記の出版物に加え、多くの NIST 出版物が https://csrc.nist.gov/publications から入手可能である。

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: sec-cert@nist.gov

寄せられたすべての意見は、情報公開法（FOIA）[FOIA96]に基づき公開対象である。

コンピュータシステム技術に関する報告

米国国立標準技術研究所（NIST）の情報技術研究所（ITL：Information Technology Laboratory）は、米国の計量と規格に関するインフラにおいて技術的リーダーシップを発揮することにより、米国経済と公共福祉を発展させている。また、ITL は、試験、試験方法、参照データ、概念実証の実施、および技術分析を開発し、情報技術（IT）の開発と生産的利用を促進している。ITL の責務には、連邦政府情報システムにおける国家安全保障関連情報以外の情報を対象とした、費用対効果の高いセキュリティのための管理、運用、技術、および物理的な規格とガイドラインを策定することが含まれる。SP 800 シリーズは、情報システムセキュリティおよびプライバシーに関する ITL の研究、ガイドライン、および普及の取り組みならびに産業界、政府、および学術機関との共同活動について報告する。

摘要

本出版物は、組織の運営や資産、個人、他の組織、および国家を、敵対的な攻撃、人的エラー、自然災害、構造的欠陥、外国諜報機関、プライバシーリスクなどの多様な脅威とリスクから保護するために、情報システムおよび組織のためのセキュリティおよびプライバシー管理策のカタログを提供する。管理策は柔軟でカスタマイズすることができ、リスクを管理するための組織全体のプロセスの一部として実装される。これらの管理策は、ミッション、事業のニーズ、法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインから導出される多様な要件に対応している。最後に、管理策の総合カタログは、機能性の観点（すなわち、管理策によって提供される機能とメカニズムの強度）および保証の観点（すなわち、管理策によって提供されるセキュリティまたはプライバシーのケイパビリティ（capability）に対する信頼度）からセキュリティとプライバシーに対応している。機能性と保証に取り組むことは、情報技術製品とそれらの製品に依存するシステムに十分な統合的信頼性があることを保証するのに役立つ。

キーワード

保証；可用性；コンピュータセキュリティ；機密性；管理策；サイバーセキュリティ；FISMA；情報セキュリティ；情報システム；完全性；個人情報；プライバシー法；プライバシー管理策；プライバシー機能；プライバシー要件；リスクマネジメントフレームワーク；セキュリティ管理策；セキュリティ機能；セキュリティ要件；システム；システムセキュリティ

謝辞

本出版物は、省庁間ワーキンググループのジョイントタスクフォース（Joint Task Force Interagency Working Group）が策定したものである。このグループには、民間、防衛、情報機関の代表が含まれる。米国国立標準技術研究所は、商務省（Department of Commerce）、国防総省（Department of Defense）、国家情報長官室（Office of the Director of National Intelligence）、および国家安全保障システム委員会（Committee on National Security Systems）の各上級幹部、ならびに関係省庁のワーキンググループのメンバーに感謝の意を表したい。彼らの献身的な尽力が本出版物に大きく貢献した。

国防総省

Dana Deasy
Chief Information Officer

John Sherman
Principal Deputy CIO

Mark Hakun
Deputy CIO for Cybersecurity and DoD SISO

Kevin Dulany
Director, Cybersecurity Policy and Partnerships

国家情報長官室

Matthew A. Kozma
Chief Information Officer

Michael E. Waschull
Deputy Chief Information Officer

Clifford M. Conner
Cybersecurity Group and IC CISO

Vacant
Director, Security Coordination Center

国立標準技術研究所

Charles H. Romine
Director, Information Technology Laboratory

Kevin Stine
Acting Cybersecurity Advisor, ITL

Matthew Scholl
Chief, Computer Security Division

Kevin Stine
Chief, Applied Cybersecurity Division

Ron Ross
FISMA Implementation Project Leader

国家安全保障システム委員会

Mark G. Hakun
Chair

Susan Dorr
Co-Chair

Kevin Dulany
Tri-Chair—Defense Community

Chris Johnson
Tri-Chair—Intelligence Community

Vicki Michetti
Tri-Chair—Civil Agencies

ジョイントタスクフォースワーキンググループ

Victoria Pillitteri
NIST, JTF Leader

Ehijele Olumese
The MITRE Corporation

Esten Porter
The MITRE Corporation

David Black
The MITRE Corporation

Eduardo Takamura
NIST

McKay Tolboe
DoD

Lydia Humphries
Booz Allen Hamilton

Julie Nethery Snyder
The MITRE Corporation

Rich Graubart
The MITRE Corporation

Ned Goren
NIST

Dorian Pappas
Intelligence Community

Daniel Faigin
Aerospace Corporation

Christina Sames
The MITRE Corporation

Peter Duspiva
Intelligence Community

Andrew Regenscheid
NIST

Kelley Dempsey
NIST

Naomi Lefkovitz
NIST

Christian Enloe
NIST

Kaitlin Boeckl
NIST

Jon Boyens
NIST

上記の謝辞に加えて、Jeff Brewer、Jim Foti、および NIST ウェブチームには、彼らの優れた管理サポートに対して特に感謝の意を表する。また、本出版物の内容の改善において継続的にご尽力いただいた Kristen Baldwin, Carol Bales、John Bazile、Jennifer Besceglie、Sean Brooks、Ruth Cannatti、Kathleen Coupe、Keesha Crosby、Charles Cutshall、Ja'Nelle DeVore、Jennifer Fabius、Jim Fenton、Hildy Ferraiolo、Ryan Galluzzo、Robin Gandhi、Mike Garcia、Paul Grassi、Marc Groman、Matthew Halstead、Kevin Herms、Scott Hill、Ralph Jones、Martin Kihiko、Raquel Leone、Jason Marsico、Kirsten Moncada、Ellen Nadeau、Elaine Newton、Michael Nieles、Michael Nussdorfer、Taylor Roberts、Jasmeet Seehra、Joe Stuntz、Jeff Williams の各氏、NIST コンピュータセキュリティ部門（Computer Security Division）および応用サイバーセキュリティ部門（Applied Cybersecurity Division）の専門スタッフ、ならびに連邦 CIO 協議会（Federal CIO Council）、連邦 CISO 協議会（Federal CISO Council）、連邦プライバシー協議会（Federal Privacy Council）、管理策ベースラインに関する省庁間ワーキンググループ（Control Baseline Interagency Working Group）、セキュリティとプライバシーのコラボレーションに関するワーキンググループ（Security and Privacy Collaboration Working Group）、および連邦プライバシー協議会のリスクマネジメント分科会（Federal Privacy Council Risk Management Subcommittee）の代表者に感謝したい。最後に、国内外の公共および民間分野の個人および組織からの貢献に心からの感謝を表明する。彼らの洞察に満ちた建設的な意見は、本出版物の全体的な品質、網羅性、および有用性を高めるものであった。

NIST SP 800-53 への過去の貢献者

2005 年当初より、SP 800-53 の過去の各版に貢献いただいた Marshall Abrams、Dennis Bailey、Lee Badger、Curt Barker、Matthew Barrett、Nadya Bartol、Frank Belz、Paul Bicknell、Deb Bodeau、Paul Brusil、Brett Burley、Bill Burr、Dawn Cappelli、Roger Caslow、Corinne Castanza、Mike Cooper、Matt Coose、Dominic Cussatt、George Dinolt、Randy Easter、Kurt Eleam、Denise Farrar、Dave Ferraiolo、Cita Furlani、Harriett Goldman、Peter Gouldmann、Tim Grance、Jennifer Guild、Gary Guissanie、Sarbari Gupta、Priscilla Guthrie、Richard Hale、Peggy Himes、Bennett Hodge、William Hunteman、Cynthia Irvine、Arnold Johnson、Roger Johnson、Donald Jones、Lisa Kaiser、Stuart Katzke、Sharon Keller、Tom Kellermann、Cass Kelly、Eustace King、Daniel Klemm、Steve LaFountain、Annabelle Lee、Robert Lentz、Steven Lipner、William MacGregor、Thomas Macklin、Thomas Madden、Robert Martin、Erika McCallister、Tim McChesney、Michael McEvilley、Rosalie McQuaid、Peter Mell、John Mildner、Pam Miller、Sandra Miravalle、Joji Montelibano、Douglas Montgomery、George Moore、Rama Moorthy、Mark Morrison、Harvey Newstrom、Sherrill Nicely、Robert Niemeyer、LouAnna Notargiacomo、Pat O'Reilly、Tim Polk、Karen Quigg、Steve Quinn、Mark Riddle、Ed Roback、Cheryl Roby、George Rogers、Scott Rose、Mike Rubin、Karen Scarfone、Roger Schell、Jackie Snouffer、Ray Snouffer、Murugiah Souppaya、Gary Stoneburner、Keith Stouffer、Marianne Swanson、Pat Toth、Glenda Turner、Patrick Viscuso、Joe Weiss、Richard Wilsher、Mark Wilson、John Woodward、および Carol Woody の各氏を含む多くの個人に対してここに感謝の意を表す。

特許開示に関する通知

通知：情報技術研究所（ITL）は、本出版物のガイダンスや要件に準拠するために使用が必要となる可能性のある特許請求項の所有者に対して、そうした特許請求項を ITL に開示するよう要請している。ただし、特許所有者は、ITL の要請に応じる義務はなく、ITL は、本出版物に適用される可能性のある特許を特定するための特許調査を実施していない。

本出版物の公開日において、および本出版物のガイダンスや要件に準拠するために使用が必要となる可能性のある特許請求項を特定するよう要請を行った時点において、ITL はそうした特許請求項を特定していない。

ITL は、本出版物の使用に際して特許侵害を回避するにはライセンス許諾が不要であることを、明示的にも暗示的にも表明していない。

リスクマネジメント

組織は、情報セキュリティとプライバシーに関するリスクの管理を行うに際して十分な調査・分析を行う必要がある。これは、部分的には、NIST 出版物に備わる柔軟性を利用して、システムの分類、ミッションおよび事業のニーズを満たすセキュリティおよびプライバシー管理策の選択と実装、管理策の有効性のアセスメント、システム運用の認可、ならびにシステムの継続的な監視を行う包括的なリスクマネジメントプログラムを確立することによって達成される。十分な調査・分析を行い、堅牢で包括的な情報セキュリティおよびプライバシーのリスクマネジメントプログラムを実装することにより、適用される法律、規則、大統領令、および政府全体のポリシーへの遵守を促進することができる。リスクマネジメントフレームワークとリスクマネジメントプロセスは、利害関係者のニーズ、ならびに組織の運営、組織の資産、個人、他の組織、および国家に対する現在の脅威に対応するために必要な保護手段を開発、実装、および維持するうえで不可欠である。効果的なリスクベースのプロセス、手順、方法、および技術を採用することで、情報システムおよび組織は、重要なミッションと事業機能、米国の重要インフラ、および政府の継続性をサポートするために必要な統合的信頼性とレジリエンスを確実に得ることができる。

セキュリティおよびプライバシーの共通基盤

NIST は、FISMA によって求められる基準およびガイドラインを行政管理予算局と共同で策定するうえで、情報セキュリティとプライバシーを向上させ、コストのかかる不要な重複作業を回避し、そして、NIST 出版物が国家安全保障システムの保護のために使用される基準およびガイドラインを補完できるようにするために、連邦政府機関、州政府、地方自治体、部族政府、および民間組織と協議を行っている。包括的かつ透明性の高いパブリックレビューおよびパブリックコメントプロセスに加えて、NIST は、行政管理予算局、国家情報長官室、国防総省、国家安全保障システム委員会、連邦 CIO 協議会、および連邦プライバシー協議会と提携し、連邦政府の情報セキュリティとプライバシーのためのリスクマネジメントフレームワーク（RMF : Risk Management Framework）を確立している。この共通基盤は、組織の運営、組織の資産、個人、他の組織、および国家に対するセキュリティとプライバシーのリスクを管理するための、費用対効果の高い、柔軟で一貫した方法を連邦政府とその契約事業者に提供する。このフレームワークは、セキュリティおよびプライバシー管理策のアセスメントのエビデンスと認可の決定を相互に受け入れるための基盤を提供し、情報共有とコラボレーションを促進するものである。NIST は、他の組織が作成した規格およびガイドラインと NIST が作成した規格およびガイドラインとのマッピング（対応付け）や関係を確立するために、公共および民間分野のエンティティと引き続き協力を進めていく。NIST は、これらのマッピングとそれらが識別する相違を用いて、管理策のカタログを改善することを期待している。

情報システム、システムコンポーネント、およびサービスの開発

統合的信頼性が高いセキュアな情報システムとサプライチェーンセキュリティを使用することに新たな重点が置かれているなかで、ミッションと事業の成功に必要なシステム、システムコンポーネント、およびサービスを取得するには、組織は、セキュリティとプライバシーの要件を明確かつ具体的に表現することが不可欠である。このため、本出版物では、開発者向けに「システムおよびサービスの取得（SA）」ファミリーおよび「サプライチェーンのリスクマネジメント（SR）」ファミリーの管理策を提供している。これらのファミリーの管理策は、開発が組織内で行われるか、委託や取得プロセスにより外部で行われるかを問わず、情報システム、システムコンポーネント、およびシステムサービスの開発、ならびに関連する開発者を対象としている。管理策カタログのうち影響を受ける管理策には、SA-8, SA-10, SA-11, SA-15, SA-16, SA-17, SA-20, SA-21, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, SR-11 が含まれる。

情報システム　幅広い視点

「エッジ・コンピューティング」が普及し、システムとデバイスが相互接続された、ますます複雑化する世界が構築されるに伴い、セキュリティとプライバシーに関する話題に国民の関心が高まっている。重要インフラのあらゆる分野で私たちが依存している根幹をなすシステム、製品、およびサービスが十分な統合的信頼性があるものであり、かつ米国経済および国家安全保障上の利益を支援するのに必要なレジリエンスが提供されるように、そうしたシステム、製品、およびサービスをさらに強化する必要性が差し迫っている。NIST SP 800-53 改訂第 5 版は、あらゆるタイプのコンピューティングプラットフォーム（汎用コンピューティングシステム、サイバーフィジカルシステム、クラウドシステム、モバイルシステム、産業用制御システム、IoT（Internet of Things）デバイスなど）のための包括的なセキュリティおよびプライバシー保全手段を開発し、公的機関や民間組織の幅広い基盤が利用することができるよう、積極的かつ体系的なアプローチを取ることで、そうした必要性に応じている。保全手段には、組織の重要かつ不可欠な活動と資産および個人のプライバシーを保護するためのセキュリティおよびプライバシー管理策の両方が含まれる。これは、私たちが依存しているシステムの攻撃に対する侵入耐性を高め、攻撃が発生した場合の被害を限定し、システムのレジリエンスと存続性を高め、そして個人のプライバシーを保護することを目的としたものである。

管理策ベースライン

これまでの NIST SP 800-53 に含まれていた管理策ベースラインは、NIST SP 800-53B に移されている。SP 800-53B には、連邦政府組織および連邦情報システムのためのセキュリティとプライバシーの管理策ベースラインが含まれている。SP 800-53B は、管理策ベースラインをテーラリングするためのガイダンスと、利害関係者とその組織のセキュリティとプライバシーの要件をサポートするオーバーレイを開発するためのガイダンスを提供している。国家安全保障システム委員会指示（CNSSI：CNSS Instruction）第 1253 号は、国家安全保障システムのセキュリティ分類化とセキュリティ管理策選択のための管理策ベースラインとガイダンスを提供している。

本出版物における事例の使用

本出版物では、各章の節、管理策、および拡張管理策において特定の項目を解説、明確化、または説明する目的で事例が使用されている。これらの事例は、本質的に例示的なものであり、組織による管理策または拡張管理策の適用を限定または制約することを意図するものではない。

連邦政府の記録管理との協力

連邦政府の記録管理プロセスは、特定の情報セキュリティとプライバシーの要件および管理策と結びついている。例えば、記録担当官は、記録がいつ削除されるかなど、記録の保持を管理している場合がある。記録管理に関連するセキュリティおよびプライバシー管理策の選択と実装の際に記録担当官と協力することで、一貫性と効率性をサポートし、ひいては組織のセキュリティとプライバシー態勢を強化することができる。

目次

エグゼクティブサマリ

「エッジ・コンピューティング」が普及し、情報システムとデバイスが接続された、ますます複雑化する世界が構築されるに伴い、セキュリティとプライバシーに関する話題に国民の関心が高まっている。国防科学評議委員会（DSB：Defense Science Board）は、2017 年の報告書「Task Force on Cyber Deterrence」[DSB 2017]で、公共および民間分野のミッションに不可欠な運営と資産をサポートする情報システムならびに米国の重要インフラにおける現在の脆弱性について慎重なアセスメントを示した。

> *「…米国の重要インフラに対するサイバー脅威は、蔓延する脆弱性を削減する取り組みを上回っており、少なくとも今後10年間米国は、非常に有能な米国への敵対者によってもたらされるサイバー脅威に対処するために抑止力に大きく依存しなければならない、とタスクフォースは指摘している。米国のサイバー抑止力には、より積極的かつ体系的なアプローチが早急に必要であることは明らかである…」*

重要インフラのあらゆる分野で国家が依存している根幹をなす情報システム、システムコンポーネント、およびサービスが十分な統合的信頼性があるものであり、かつ米国経済および国家安全保障上の利益を支えるのに必要なレジリエンスが提供されるように、そうしたシステム、システムコンポーネント、およびサービスをさらに強化する必要性が差し迫っている。NIST SP 800-53 の今回のアップデートは、あらゆるタイプのコンピューティングプラットフォーム（汎用コンピューティングシステム、サイバーフィジカルシステム、クラウドシステム、モバイルデバイス、IoT デバイス、兵器システム、宇宙システム、通信システム、環境制御システム、スーパーコンピュータ、および産業用制御システムを含む）のための包括的な保全手段を開発し、公的機関や民間組織の幅広い基盤が利用することができるよう、積極的かつ体系的なアプローチを取ることで、DSB による呼びかけに応じている。これらの保全手段には、組織の重要かつ不可欠な運営と資産および個人のプライバシーを保護するためのセキュリティおよびプライバシー管理策の実装が含まれる。これは、私たちが依存している情報システムの侵入耐性を高め、攻撃が発生した場合の被害を限定し、システムのサイバーレジリエンスと存続性を高め、個人のプライバシーを保護することを目的としている。

この基礎的な NIST 出版物の改訂第 5 版は、上記の目的を達成するために必要となる次世代のセキュリティおよびプライバシー管理策を開発する数年にわたる取り組みを象徴している。これには、様々な消費者グループ（ミッションや事業機能を遂行する企業、情報システム、IoT デバイス、システム・オブ・システムズを開発するエンジニアリング組織、およびシステムコンポーネント、製品、サービスを構築する業界パートナーなど）にとって管理策をより使いやすいものにするための変更が含まれる。本出版物の最も重要な変更点は次のとおりである。

- 管理策を満たす責任のあるエンティティ（すなわち、情報システムや組織）を管理策ステートメントから削除することにより、管理策をより成果ベースに変更した。
- 情報セキュリティおよびプライバシー管理策を統合し、情報システムおよび組織のためのシームレスな管理策の総合カタログにした。
- サプライチェーンのリスクマネジメントに関する管理策ファミリーを新たに規定した。
- 管理策の選択*プロセス*を*管理策*から分けることで、システムエンジニア、セキュリティアーキテクト、ソフトウェア開発者、エンタープライズアーキテクト、システムセキュリティおよびプライバシーエンジニア、ミッションオーナーまたは事業オーナーなど、関心のある様々なコミュニティで管理策が使用されるようにした。

- 管理策ベースラインおよびテーラリングガイダンスを本出版物から削除し、その内容をNIST SP 800-53B「*組織および情報システムのための管理策ベースライン（Control Baselines for Information Systems and Organizations）*」に移行した。
- 要件と管理策の関係およびセキュリティ管理策とプライバシー管理策の関係を明確にした。
- 最新の脅威インテリジェンスとサイバー攻撃データに基づいて、新しい実践的な管理策（サイバーレジリエンスを支援する管理策、セキュアなシステム設計を支援する管理策、セキュリティとプライバシーのガバナンスと説明責任を強化する管理策など）を組み込んだ。

管理策選択のプロセスを管理策から分離し、管理策ベースラインを削除することで、これまでの SP 800-53 に含まれていた多くのガイダンスやその他の参考となる資料が除かれた。それらの内容は、次回の更新サイクルで SP 800-37（リスクマネジメントフレームワーク）や SP 800-53B などの他の NIST 出版物に移行される。近い将来、NIST は SP 800-53、SP 800-53A、および SP 800-53B の内容をウェブベースのポータルで提供して、すべての管理策、管理策ベースライン、オーバーレイおよびアセスメント情報へのインタラクティブなオンラインアクセスを利用者に提供することも計画している。

序文

「…リスクマネジメントプロセスを通じて、リーダーは、サイバー空間を自身の利益のために利用する敵対者による米国の利益に対するリスク、および、サイバー空間のグローバルな性質を利用して軍事活動、情報収集活動、業務活動の目的を達成するための我々自身の取り組みから生ずる米国の利益に対するリスクを考慮しなければならない…」

「…運用計画の策定では、脅威、脆弱性、およびインパクトの組み合わせを検討して、重要な傾向を特定するとともに、脅威となるケイパビリティおよび脆弱性を排除、軽減し、すべてのサイバー空間運用のアセスメント、調整、および衝突回避のための取り組みをどこに適用すべきかを決定する必要がある…」

「…すべてのレベルのリーダーは、他のあらゆる分野と同等の準備態勢とセキュリティを確保する責任がある…」

サイバー空間運用に関する国家戦略（THE NATIONAL STRATEGY FOR CYBERSPACE OPERATIONS）
国防総省　統合参謀本部議長（OFFICE OF THE CHAIRMAN, JOINT CHIEFS OF STAFF, U.S. DEPARTMENT OF DEFENSE）

「ネットワークの形成と情報技術は、21 世紀の生活を一変させ、人々、企業、政府による交流の仕方に変化をもたらしてきた。コンピューティング、ストレージ、および通信の大幅な改善により、社会福祉の向上、健康や医療の改善、教育や雇用障壁の排除、そして、製造業、輸送業、農業などの多くの分野での効率の向上、といった新たな機会が創出されている。

こうした新しい応用の可能性は、多くの場合、情報を大規模に作成、収集、伝送、処理、およびアーカイブすることができる能力に起因する。しかし、収集および保持される個人情報の量が大幅に増加し、情報を分析して他の情報と組み合わせる能力が向上したことに伴い、プライバシーに関する懸念や、こうした前例のない量のデータを責任を持って管理するエンティティの能力に関する懸念が当然ながら生じている…膨大な量の情報を作成、キャプチャ、保存、および処理する能力の向上が国の本質的価値を損なうことがないように保証することが、現代の重要な課題である…」

「…システムが個人情報を収集、分析、生成、開示、保持、または使用するなど、その方法に関わらず、個人情報を取扱う際には、個人のプライバシーにインパクトを及ぼす可能性がある。システム設計者は、ソリューションの全体的な開発において、個人を利害関係者として考慮する必要がある…プライバシーの設計では、個人のプライバシーに関する要求をシステム要件および管理策と結びつけて、理想と現実的な開発との隔たりを効果的に埋めなければならない…」

国家プライバシー研究戦略（THE NATIONAL PRIVACY RESEARCH STRATEGY）
国家科学技術会議　ネットワークおよび情報技術研究開発プログラム（NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT PROGRAM）

正誤表

この表には、SP 800-53 改訂第 5 版に組み込まれた変更が含まれている。正誤表の更新には、本出版物における*編集上*または*実質的*な訂正、明確化、またはその他の軽微な変更が含まれる。正誤表の更新や改訂でまだ公開されていない、本出版物への潜在的な更新（追加の課題や潜在的な訂正を含む）は特定され次第掲載される。SP 800-53 改訂第 5 版の出版情報を参照のこと。

（訳者注：正誤表の内容については翻訳を提供していません）

日付	種類	改訂内容	頁

第 1 章

はじめに

情報、システム、組織、および個人を保護する必要性

現代の情報システム[1]には、様々なコンピューティングプラットフォーム（例えば、産業用制御システム、汎用コンピューティングシステム、サイバーフィジカルシステム、スーパーコンピュータ、兵器システム、通信システム、環境制御システム、医療デバイス、組み込み型デバイス、センサ、スマートフォンやタブレットなどのモバイルデバイス）が含まれる。これらのプラットフォームはすべて、組織の重要なミッションと事業機能を支援する能力を提供する複雑なハードウェア、ソフトウェア、およびファームウェアを備えたコンピュータ、という共通の基盤を共有している[2]。

セキュリティ管理策とは、システムおよびその情報の機密性、完全性、可用性を保護し、情報セキュリティ[3]リスクを管理するために、システムまたは組織内で採用される保全措置または対策のことである。プライバシー管理策とは、プライバシーリスクを管理し、適用されるプライバシー要件への準拠を確保するために、システムまたは組織内で採用される管理上、技術的、および物理的な保全措置である[4]。セキュリティおよびプライバシー管理策は、システムまたは組織に課されたセキュリティとプライバシーの要件を満たすように選択し実装される。セキュリティとプライバシーの要件は、処理、保存、または伝送される情報の機密性、完全性、可用性を確保し、個人のプライバシーに対するリスクを管理するために、適用される法律、大統領令、指令、規則、ポリシー、基準、およびミッションのニーズから導出される。

セキュリティおよびプライバシー管理策[5]の選択、設計、および実装は、組織の運営[6]や資産ならびに個人や国家の繁栄に重大な影響を与える重要なタスクである。組織は、情報セキュリティおよびプライバシー管理策に取り組む際、次のようないくつかの重要な質問に答えるべきである。

- セキュリティとプライバシーの要件を満たし、ミッション／事業リスクまたは個人に対するリスクを適切に管理するには、どのようなセキュリティおよびプライバシー管理策が必要なのか。
- 選択された管理策は実装されているか、または、実装する計画はあるか。
- 選択された管理策が設計通りに実装されている場合に効果的であることを示すために要求される保証レベル（すなわち、信頼性の根拠）は何か[7]。

これらの質問は、個別に回答されるのではなく、組織の情報とシステムから継続的に発生するセキュリティおよびプライバシーのリスクを特定、アセスメント、対応、および監視するリスク

[1] *情報システム*とは、情報の収集、処理、維持、使用、共有、配布、または廃棄のために組織された個別の一連の情報リソースである[OMB A-130]。
[2] *組織*という用語は、組織構造内のあらゆるサイズ、複雑さ、または位置付けのエンティティを表す（例えば、連邦政府機関、または必要に応じて、その部局）。
[3] 本出版物では、*情報セキュリティ*と*セキュリティ*という 2 つの用語を同義語として使用している。
[4] [OMB A-130]は、*セキュリティ管理策*および*プライバシー管理策*を規定している。
[5] 管理策は、システム開発ライフサイクル中のリスクを軽減するために、システムセキュリティおよびプライバシーエンジニアリングプロセスにおける保全措置および対策を提供する。
[6] 組織の運営には、ミッション、機能、イメージ、および評判が含まれる。
[7] セキュリティおよびプライバシー管理策の有効性は、管理策が適切に実装され、意図したとおりに運用され、指定されたセキュリティおよびプライバシーの要件を満たすことに関して望ましい結果を生み出す程度を扱う[SP 800-53A]。

マネジメントプロセスとの関連において回答される[8]。本出版物のセキュリティおよびプライバシー管理策は、組織が情報セキュリティとプライバシーの要件を満たすために使用することが推奨される。管理策カタログは、セキュリティとプライバシーのリスクに対応するための保全措置、対策、技法、およびプロセスを含むツールボックスと見なすことができる。管理策は、組織の情報セキュリティおよびプライバシープログラムをサポートする、明確に規定されたリスクマネジメントプロセスの一環として採用される。同様に、これらの情報セキュリティおよびプライバシープログラムは、組織のミッションと事業を成功させるための基盤となる。

組織の運営や資産、個人、他の組織、および国家に悪影響を及ぼしかねないセキュリティとプライバシーのリスクについて責任者が理解していることが重要である[9]。また、責任者は、特定されたリスクに許容される方法で対応するための、十分な情報に基づいた判断と投資を行うために、セキュリティおよびプライバシープログラムの現在の状況と、情報、情報システム、および組織を保護するために計画または導入されている管理策の現在の状況を理解していなければならない。その目的は、セキュリティおよびプライバシー管理策の選択と実装を通じてリスクを管理することである。

1.1 目的および適用性

本出版物は、組織およびシステムのための管理策を規定している。管理策は、情報を処理、保存、または伝送するあらゆる組織やシステム内で実装することができる。これらの管理策は、行政管理予算局（OMB：Office of Management and Budget）の通達（Circular）A-130 号［OMB A-130］および連邦情報セキュリティ近代化法[10]（FISMA：Federal Information Security Modernization Act）［FISMA］の規定により、連邦政府情報システム[11]での使用が義務付けられている[12]。FISMA は、連邦政府情報および連邦政府情報システムを保護するための最小限の管理策の実装を要求する法律である。本出版物は、その他の NIST の関連出版物とともに、組織がリスクを管理するために必要なセキュリティおよびプライバシー管理策を特定し、FISMA、1974 年プライバシー法（Privacy Act）［PRIVACT］、OMB のポリシー（［OMB A-130］など）、および指定された連邦情報処理規格（FIPS：Federal Information Processing Standards）などのセキュリティとプライバシーの要件を満たすべく設計されている。この目的は、変化する脅威、脆弱性、要件、および技術に基づいて、現在および今後の保護ニーズを満たすセキュリティおよびプライバシー管理策を含む包括的かつ柔軟なカタログを提供することにより達成される。また、本出版物は、セキュリティ、プライバシー、およびリスクマネジメントの概念の議論をサポートする共通の用語集を提供することにより、組織間のコミュニケーションを改善する。

最後に、管理策は、管理策を選択するために採用されるプロセスから独立している。管理策

[8] ［SP 800-37］のリスクマネジメントフレームワークは、包括的なリスクマネジメントプロセスの一例である。

[9] これには、［HSPD 7］に記載される重要インフラおよび主要リソースに対するリスクが含まれる。

[10] 合衆国法典（U.S.C.）第 44 編第 3542 条で規定されている、国家安全保障システムとして指定されている情報システムは、［FISMA］の要件の対象ではない。しかし、本出版物で定められている管理策は、別段に要求される場合（例えば、1974 年プライバシー法（Privacy Act of 1974））、または国家安全保障システムに対して政策権限を行使する適切な連邦政府担当官の承認を得て、国家安全保障システムのために選択してもよい。［CNSSP 22］および［CNSSI 1253］は、国家安全保障システムに関するガイダンスを提供している。［DODI 8510.01］は国防総省のガイダンスを提供している。

[11] *連邦政府情報システム*は、政府機関、政府機関の契約事業者、または政府機関に代わる別の組織が使用または運用する情報システムを指す。

[12] 本出版物に規定される管理策は連邦政府組織および連邦政府情報システムで必須であるが、州政府、地方自治体、部族政府などの他の組織および民間組織は、必要に応じてこれらのガイドラインの使用を検討することが推奨される。連邦政府の管理策ベースラインについては、［SP 800-53B］を参照のこと。

の選択プロセスは、組織全体のリスクマネジメントプロセス、システムエンジニアリングプロセス[SP 800-160-1][13]、リスクマネジメントフレームワーク（Risk Management Framework）[SP 800-37]、サイバーセキュリティフレームワーク（Cybersecurity Framework）[NIST CSF]、またはプライバシーフレームワーク（Privacy Framework）[NIST PF]の一部とすることができる[14]。管理策を選択する基準は、ミッションおよび事業のニーズ、利害関係者保護のニーズ、脅威、脆弱性、および連邦法、大統領令、指令、規則、ポリシー、基準、およびガイドラインに準拠する要件など、多くの要因によって導かれ、情報が提供される。セキュリティおよびプライバシー管理策のカタログとリスクベースの管理策の選択プロセスを組み合わせることにより、組織は、規定されたセキュリティとプライバシー要件に準拠し、情報システムの適切なセキュリティを確保し、個人のプライバシーを保護することができる。

1.2 対象読者

本出版物は、次のような多様な読者を対象とする。

- システム、情報セキュリティ、プライバシー、またはリスクマネジメントおよび監督に責任を有する個人（認可権限のある担当者、最高情報責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者など）
- システム開発に責任を有する個人（ミッションオーナー、プログラムマネージャー、システムエンジニア、システムセキュリティエンジニア、プライバシーエンジニア、ハードウェア開発者、ソフトウェア開発者、システムインテグレータ、購買・調達担当者など）
- ロジスティクスまたは廃棄に関連する責任を有する個人（プログラムマネージャー、調達担当者、システムインテグレータ、プロパティマネージャーなど）
- セキュリティおよびプライバシーの実装および運用に責任を有する個人（ミッションオーナー、事業オーナー、システムオーナー、情報オーナー、情報スチュワード、システム管理者、継続計画担当者、システムセキュリティ責任者、プライバシー保護責任者など）
- セキュリティおよびプライバシーのアセスメントおよび監視に責任を有する個人（監査人、監察官、システム評価者、管理策アセッサー、独立した検証および妥当性確認者、アナリストなど）
- コンポーネント製品およびシステムの製造、セキュリティおよびプライバシー技術の開発、または情報セキュリティやプライバシーをサポートするサービスや能力の提供などを行う業界パートナーを含む商業エンティティ

1.3 組織の責任

セキュリティとプライバシーのリスクマネジメントは、以下を必要とする複雑で多面的な活動で

[13] リスクマネジメントは、システムエンジニアリング、システムセキュリティエンジニアリング、およびプライバシーエンジニアリングの不可欠な要素である。

[14] [OMB A-130]は、連邦政府機関に対して連邦情報システムの管理策を選択するための NIST リスクマネジメントフレームワークを実装することを要求している。[EO 13800]は、サイバーセキュリティリスクを管理するために、連邦政府機関に対して*重要インフラのサイバーセキュリティを改善するための NIST フレームワーク*を実装することを要求している。NIST のフレームワークは、非連邦政府組織においても任意のリソースとして利用することができる。

ある。

- システムと組織に関して明確に規定されたセキュリティおよびプライバシー要件
- 実践的なハードウェア、ファームウェア、およびソフトウェアの開発と取得プロセスに基づいて、統合的信頼性の高い情報システムコンポーネントを使用すること
- 厳密なセキュリティおよびプライバシーの計画策定ならびにシステム開発ライフサイクルの管理
- システムコンポーネントをセキュアに開発し情報システムに統合するために、システムセキュリティおよびプライバシーエンジニアリングの原則および実施項目を適用すること
- 組織の制度上および運用上のプロセスに統合され支援する、適切に文書化されたセキュリティおよびプライバシー実施項目を採用すること
- 管理策の有効性の継続、情報システムと運用環境の変化、および組織全体のセキュリティとプライバシーの状態を判定するために、情報システムと組織を継続的に監視すること

組織は、組織の運営や資産、個人、他の組織、および国家に対するセキュリティとプライバシーのリスクを継続的にアセスメントする。セキュリティとプライバシーのリスクは、組織のミッションと事業の計画および実行、情報システムの導入、またはシステム運用の継続から生じる。リスクの現実的なアセスメントには、情報システムや組織における特定の脆弱性に基づく脅威の受容可能性、および、それらの脅威による脆弱性の悪用の可能性と潜在的な有害なインパクトに関する十分な理解が必要である[15]。また、リスクアセスメントには、プライバシーリスクに関する理解も必要である[16]。

リスクのアセスメントと判定に関する組織の懸念に対処するために、組織のリスクマネジメント戦略に関する知識と理解を用いることで、セキュリティおよびプライバシーの要件が満たされる[17]。リスクマネジメント戦略では、組織のシステムの設計、開発、取得、導入、運用、維持、および廃棄に関連するコスト、スケジュール、パフォーマンス、およびサプライチェーンに関わる問題を考慮する。その後、継続的にリスクを管理するためにリスクマネジメントプロセスを適用する[18]。

セキュリティおよびプライバシー管理策カタログを効果的に使用することで、様々な運用、環境、および技術シナリオにおける個人情報（PII）の取扱いから生じる従来の脅威、持続的標的型攻撃（APT 攻撃）、およびプライバシーリスクから組織、個人、情報システムを保護することができる。これらの管理策は、政府、組織、または制度の様々なセキュリティおよびプライバシー要件への準拠を実証するためにも使用することができる。組織には、適切なセキュリティおよびプライバシー管理策を選択し、それらの管理策を正しく実装し、セキュリティおよびプライバシー要求事項を満たす上で管理策の有効性を実証する責任がある[19]。セキュリティおよびプライバシー管理策は、独自のまたは特殊なミッションまたはビジネスアプリケーション、情報システム、脅威の懸念、運用環境、技術、または対象のコミュニティのための専門のベース

[15] [SP 800-30]は、リスクアセスメントプロセスに関するガイダンスを提供している。
[16] [IR 8062]は、プライバシーリスクの概念を紹介している。
[17] [SP 800-39]は、リスクマネジメントプロセスおよび戦略に関するガイダンスを提供している。
[18] [SP 800-37SP 800-37]は、包括的なリスクマネジメントプロセスを提供している。
[19] [SP 800-53A]は、管理策の有効性評価に関するガイダンスを提供している。

ラインやオーバーレイの開発にも使用できる[20]。

組織のリスクアセスメントは、セキュリティおよびプライバシー管理策の選択プロセスに情報を提供するために、部分的に使用される。選択プロセスでは、組織のリスク許容度と一致する特定のミッションまたは事業のニーズに対応する、合意された一連のセキュリティおよびプライバシー管理策が決定される[21]。また、このプロセスにより、組織は、ますます高度化する敵対的な脅威の領域、ミッションおよび事業の要件、急速に変化する技術、複雑なサプライチェーン、ならびに多くのタイプの運用環境に対処するために必要な即応性と柔軟性を可能な限り維持することができる。

1.4 他の出版物との関係

本出版物は、情報システムおよび組織に課せられた多様なセキュリティおよびプライバシー要件、ならびに、国内外で認知された他の情報セキュリティおよびプライバシー規格と整合性があり、それらを補完する多様なセキュリティおよびプライバシー要件を満たす管理策を規定している。情報システムおよび組織のための、広く適用可能で技術的に健全な一連の管理策を策定するため、本出版物の作成にあたり多くのソースが考慮された。これらのソースには、製造、防衛、金融、医療、輸送、エネルギー、インテリジェンス、産業制御、および監査のコミュニティ、ならびに国内外の規格関連機関の要件と管理策が含まれている。さらに、本出版物の管理策は、国家安全保障システムとして指定されたシステムに固有のガイダンスを提供するために、国家安全保障システム委員会（CNSS：Committee on National Security Systems）指示第 1253 号[CNSSI 1253]などの出版物において国家安全保障コミュニティによって使用されている。有用性と適用性を最大限確保するため、管理策は可能な限り、国際基準とマッピング（対応付け）されている[22]。本出版物と他のセキュリティ、プライバシー、およびリスクマネジメントに関する出版物との関係は、[FISMA IMP]で確認することができる。

1.5 改訂および拡張

本出版物に記載されているセキュリティおよびプライバシー管理策は、個人、情報システム、および組織のための実践的な保護手段である。これらの管理策は、(1)管理策の使用から得られた経験、(2)新しいまたは改正された法律、大統領令、指令、規則、ポリシー、および基準、(3)変化するセキュリティおよびプライバシーの要件、(4)新たな脅威、脆弱性、攻撃および情報処理方法、ならびに(5)新たに利用可能となった技術、を反映するために定期的にレビューされ、改訂される。

また、管理策カタログ内のセキュリティおよびプライバシー管理策も、管理策の撤回、改訂、追加に伴い、時間の経過とともに変更されることが予想される。変更の必要性に加えて、セキュリティおよびプライバシー管理策に対して提案される修正が、公共および民間分野のフィードバックを受け、変更についての合意を得るために、厳正かつ透明性の高いパブリックレビュ

[20] [SP 800-53B]は、セキュリティおよびプライバシー管理策ベースラインをテーラリングするためのガイダンス、ならびに利害関係者とその組織の特定の保護ニーズおよび要件をサポートするオーバーレイを作成するためのガイダンスを提供している。

[21]認可権限のある担当者または認可権限のある担当者が指定した代理人は、セキュリティおよびプライバシー計画を承認することにより、組織およびシステムのセキュリティとプライバシー要件を満たすために提案されたセキュリティおよびプライバシー管理策に同意する。

[22]マッピング表は、[SP 800-53 RES]で利用可能である。

ープロセスを経ることを要求することによって、安定性の必要性に対処する。このレビュープロセスにより、技術的に信頼でき、柔軟かつ安定した一連のセキュリティおよびプライバシー管理策が、管理策カタログを使用する組織に提供される。

1.6 本出版物の構成

本出版物の第 2 章以降は、次のように構成される。

- **第 2 章**では、セキュリティおよびプライバシー管理策に関連する基本的な概念を説明する。これには、管理策の構造、総合カタログにおける管理策の構成、管理策実装アプローチ、セキュリティ管理策とプライバシー管理策の関係、および統合的信頼性と保証などが含まれる。
- **第 3 章**では、セキュリティおよびプライバシー管理策の総合カタログを提供する。各管理策の目的を説明し、管理策の実装とアセスメントに関する有用な情報を提供する詳解セクション、管理策間の関係と従属を示す関連管理策のリスト、および組織に役立つ関連出版物への参照資料のリストが含まれる。
- **参照資料**、**用語集**、**略語**、および**管理策の要約**は、セキュリティおよびプライバシー管理策の使用について更なる情報を提供する[23]。

[23]特に明記しない限り、NIST 出版物が参照される場合はすべて、それら出版物の最新版を指すものとする。

第 2 章

基本的事項

セキュリティおよびプライバシー管理策の構造、タイプ、および構成

本章では、セキュリティおよびプライバシー管理策に関連する基本的な概念を説明する。これには、要件と管理策の関係、管理策の構造、管理策総合カタログにおける管理策の構成、組織と情報システムのための様々な管理策実装アプローチ、セキュリティ管理策とプライバシー管理策の関係、セキュリティおよびプライバシー管理策における統合的信頼性と保証の概念の重要性、統合的信頼性やレジリエンスが高いセキュアなシステムを実現する際の管理策の影響などが含まれる。

2.1 要件および管理策

要件と管理策の関係を理解することは重要である。連邦政府の情報セキュリティおよびプライバシーポリシーでは、要件という用語は通常、組織に課される情報セキュリティおよびプライバシーに関する義務を指すために使用される。例えば、[OMB A-130]は、連邦政府機関に対して、情報リソースを管理する際に準拠しなければならない情報セキュリティおよびプライバシー要件を課している。また、要件という用語は、特定の組織やシステムにおける利害関係者保護のニーズを表現するためにより広い意味で使用される場合もある。利害関係者保護のニーズとそれに対応するセキュリティおよびプライバシー要件は、多くのソース（法律、大統領令、指令、規則、ポリシー、基準、ミッションおよび事業のニーズ、またはリスクアセスメントなど）から導出される場合がある。本ガイドラインで使用される要件という用語には、法的要件とポリシー要件の両方に加えて、他のソースから導出される場合がある広範な利害関係者保護のニーズといった表現も含まれる。これらの要件のすべてをシステムに適用すると、セキュリティ、プライバシー、および保証を含む、システムに必要な特徴を判定するのに役に立つ[24]。

組織は、セキュリティおよびプライバシー要件がシステム開発ライフサイクル（SDLC）のどこで何の目的で採用されているのかに応じて、要件をさらに細かいカテゴリに分類することができる。組織またはシステムが利害関係者保護のニーズを満たすうえで提供しなければならないケイパビリティ（capability）を示すにはケイパビリティ要件（capability requirements）という用語を使用し、また、システムの特定のハードウェア、ソフトウェア、およびファームウェアコンポーネントに関連するシステム要件を仕様要件（specification requirements）と呼ぶことがある。仕様要件とは、管理策のすべてまたは一部を実装するケイパビリティであり、アセスメントの対象（検証、妥当性の確認、テスト、および評価プロセスの一環として）になり得るケイパビリティである。最後に、組織は作業指示（SOW）要件という用語を使用して、運用上またはシステム開発中に実施しなければならないアクションを指す場合がある。

*管理策*は、組織の特定のセキュリティおよびプライバシーに関する目的を達成し、組織の利害関係者保護のニーズを反映するのに適切な保全措置および保護ケイパビリティの記述と見なすことができる。管理策は、システム要件を満たすために組織によって選択および実装

[24]セキュリティとプライバシーにインパクトを与えるシステムの特徴はさまざまであり、（1）その主な目的に基づくシステムのタイプと機能、（2）その技術、機械的、物理的、および人的要素に基づくシステムの構成、（3）システムがその機能とサービスを提供する形態および状態、（4）システムとその構成要素である機能およびサービスの重要度または重要性、（5）処理、保存、または送信されるデータまたは情報の機微性、（6）システムが正しく実行され、システム自体の保護（すなわち、自己保護）を提供する能力と比較した損失、障害、または機能低下の影響、ならびに、（7）金銭的またはその他の価値、が含まれる[SP 800-160-1]。

される。管理策は、管理上、技術的、および物理的な側面を含むことができる。場合によっては、管理策の選択と実装のために、*派生要件*またはインスタンス化された管理策パラメータ値の形で、組織による追加の指定が必要になることがある。派生要件と管理策パラメータ値は、SDLC において特定の管理策に適切なレベルの実装詳細を提供するために必要な場合がある。

2.2 管理策の構造および構成

本出版物に記載のセキュリティおよびプライバシー管理策は、構成と構造が明確に規定されている。セキュリティおよびプライバシー管理策は、選択と指定のプロセスにおいて使用を容易にするため、20 のファミリーから構成される[25]。各ファミリーには、そのファミリーの特定のトピックに関連した管理策が含まれ、2 文字の識別子により各管理策ファミリーは一意に識別されている（例えば、「職員のセキュリティ」の場合は PS）。セキュリティおよびプライバシー管理策には、システムまたは個人のアクションによって実装される、ポリシー、監督、監理、手動プロセス、および自動化されたメカニズムの側面が含まれる場合がある。表 1 は、セキュリティおよびプライバシー管理策ファミリーと、それに対応するファミリー識別子を示す。

表 1：セキュリティおよびプライバシー管理策ファミリー

識別子	ファミリー	識別子	ファミリー
AC	アクセス制御	PE	物理的および環境的保護
AT	意識向上およびトレーニング	PL	計画
AU	監査および説明責任	PM	プログラムマネジメント
CA	アセスメント、認可、および監視	PS	職員のセキュリティ
CM	構成管理	PT	個人情報の取扱いおよび透明性
CP	緊急時対応計画	RA	リスクアセスメント
IA	識別および認証	SA	システムおよびサービスの取得
IR	インシデント対応	SC	システムおよび通信の保護
MA	メンテナンス	SI	システムおよび情報の完全性
MP	媒体保護	SR	サプライチェーンのリスクマネジメント

管理策ファミリーには、基本管理策と拡張管理策が含まれており、拡張管理策は基本管理策に直接関連している。拡張管理策は、基本管理策に機能性や特殊性を追加する、または基本管理策の強度を向上させる。拡張管理策は、基本管理策によって提供される保護よりも強力な保護を必要とするシステムおよび動作環境で使用される。組織が拡張管理策を選択して実装する必要性は、組織または個人への有害なインパクトが予測される場合、もしくは組織がリスクアセスメントに基づいて追加の保証や基本管理策への機能性の追加を要する場合

[25] NIST SP 800-53 に記載される 20 の管理策ファミリーのうち、17 の管理策ファミリーは[FIPS 200]の最低限のセキュリティ要件に適合している。「プログラムマネジメント（PM）」、「個人情報の取扱いおよび透明性（PT）」、および「サプライチェーンのリスクマネジメント（SR）」のファミリーは、[FIPS 200]以降に発令された連邦政府命令に付随する企業レベルのプログラムマネジメント、プライバシー、およびサプライチェーンリスクの考慮事項に対応するものである。

に生ずる。拡張管理策を選択し実装する場合には、*必ず*基本管理策の選択と実装が必要となる。

ファミリーはアルファベット順に記載され、各ファミリー内の管理策と拡張管理策は番号順に列挙される。ファミリー、管理策、および拡張管理策の順序は、論理的な進行、優先順位、重要度、または、管理策や拡張管理策が実装される順序を意味するものではなく、単にカタログに含まれた順序を反映している。管理策の名称は、管理策が取り消された場合、再度利用されない。

セキュリティおよびプライバシー管理策は、基本管理策セクション、詳解セクション、関連管理策セクション、拡張管理策セクション、および参照資料セクションといった構造から成る。図 1 は、一般的な管理策の構造を示している。

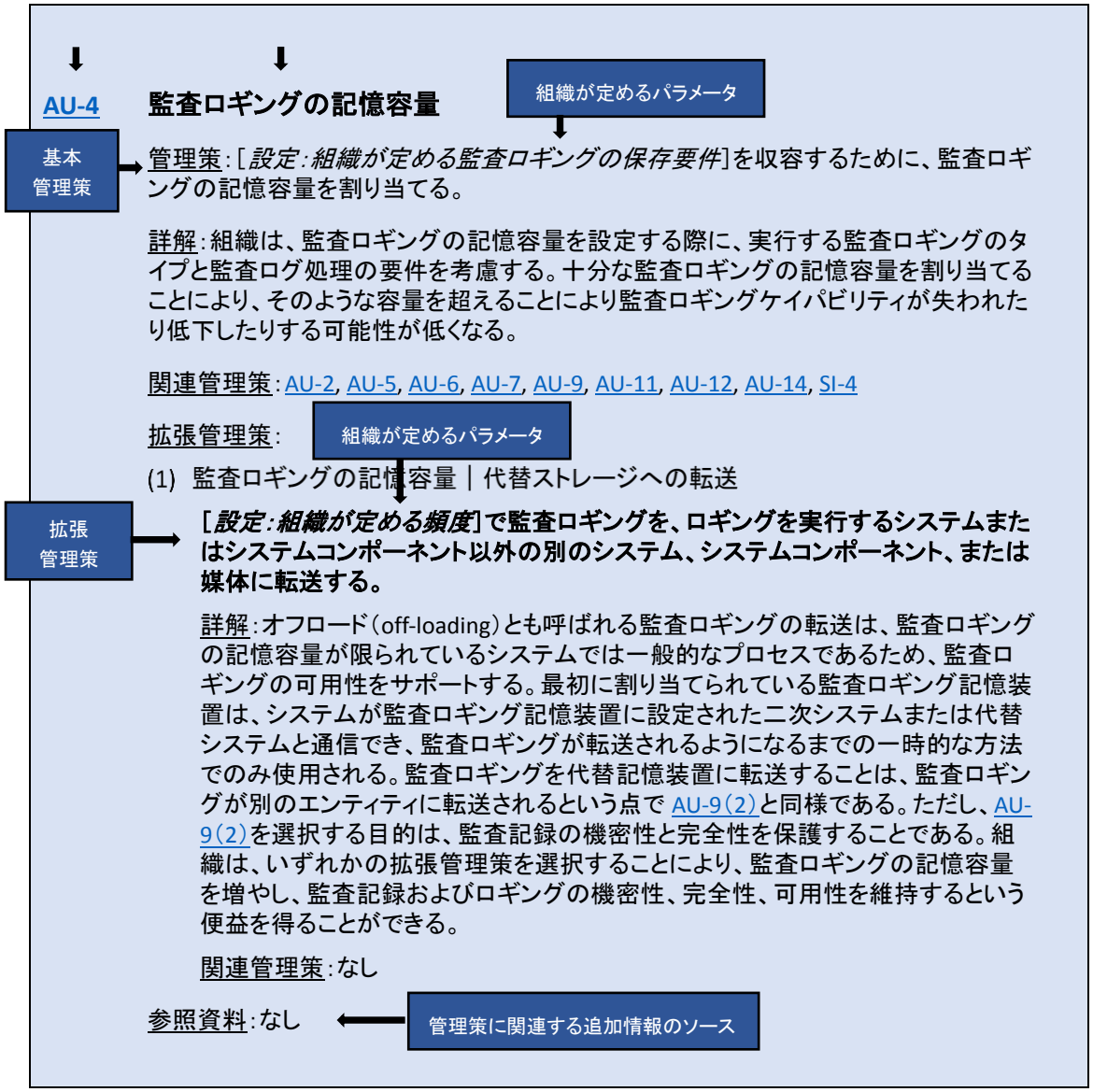

図 1：管理策の構造

*管理策*のセクションは、実装されるセキュリティまたはプライバシーのケイパビリティを定めている。セキュリティおよびプライバシーのケイパビリティは、組織や情報システムが行う自動ま

たは手動の活動やアクションによって達成される。組織は、管理策の策定、実装、アセスメント、および監視の責任を指定する。また、組織は、法律、規則、およびポリシーに適合し、組織のミッションまたは事業のニーズを満たすように選択した管理策をあらゆる形態で柔軟に実装することができる。

*詳解*のセクションは、管理策に関する追加の情報を提供する。組織は、管理策を策定、テーラリング、実装、アセスメント、または監視する際に、必要に応じてこの追加情報を使用することができる。追加情報は、ミッションや事業の要件、運用環境、またはリスクアセスメントに基づいて管理策を実装するための重要な考慮事項を提供する。また、追加情報は、管理策の目的を説明するとともに、多くの場合、事例が含まれる。詳解情報が特定の拡張管理策のみに適用される場合には、拡張管理策に個別の詳解セクションが含まれることもある。

*関連管理策*のセクションは、(1)特定の管理策または拡張管理策の実装にインパクトを与えるまたはサポートする管理策、(2)関連するセキュリティまたはプライバシーのケイパビリティに対応する管理策、または(3)詳解セクションで参照される管理策など、管理策カタログから管理策のリストを提供する。拡張管理策は、本質的に基本管理策に関連している。したがって、基本管理策で参照されている関連管理策は、拡張管理策で再度掲載されない。ただし、基本管理策で参照されていない関連管理策が拡張管理策で特定されていることがある(すなわち、関連管理策が特定の拡張管理策にのみ関連している)。管理策は、他の基本管理策の拡張管理策に関連する場合もある。管理策が関連管理策として表示されている場合、双方向の関係を示すために、カタログ内のソースの箇所でその管理策に対応する表示がされる。さらに、ファミリーの各管理策は、同じファミリー内の冒頭の管理策(「ポリシーと手順」)に本質的に関連している。したがって、同じファミリー内の冒頭の管理策と他の管理策との関係は、各管理策の*関連管理策*セクションに明記されない。

*拡張管理策*のセクションは、基本管理策を強化するセキュリティおよびプライバシーのケイパビリティについて説明する。拡張管理策は、各管理策内で順番に番号が付けられており、基本管理策を補足するために選択する際、容易に特定することができる。各拡張管理策には、拡張管理策によって提供が意図される機能またはケイパビリティを示す短い副題が付けられている。AU-4 の例では、拡張管理策が選択される場合、管理策の記号は AU-4(1)である。拡張管理策の数字記号は、管理策内で拡張管理策を識別するためにのみ使用される。この記号は、拡張管理策の強度、保護レベル、優先度、重要度、または拡張管理策の階層関係を示すものではない。拡張管理策は、個別に選択されることを意図したものではない。すなわち、拡張管理策が選択される場合、対応する基本管理策も選択され実装される。

*参照*のセクションには、特定の管理策や拡張管理策に関連する、適用される法律、ポリシー、基準、ガイドライン、ウェブサイト、およびその他の有益な参考資料のリストが含まれる[26]。参照セクションには、管理策の策定、実装、アセスメント、および監視に関する追加情報を入手できるように出版物へのリンクも含まれる。

一部の管理策では、組織は、管理策に関連付けられた指定のパラメータに対して特定の値を定義することができ、さらなる柔軟性がもたらされる。柔軟性は、管理策内に組み込まれ、括弧で囲まれた*設定*および*選択*操作を使用したテーラリングプロセスの一部として実現される。組織は、設定および選択操作により、組織のセキュリティおよびプライバシー要件に基づいて管理策をカスタマイズすることができる。パラメータ値の指定を完全に柔軟に行うことができる設定操作とは対照的に、選択操作は、組織が選択する項目の特定のリストを提供することで、パラメータ値の範囲を限定する。

[26] 参照は、組織がセキュリティおよびプライバシー管理策を理解し実装することを支援するために提供されており、包括的または完全なものであることを意図していない。

組織が定めるパラメータの決定は、法律、大統領令、指令、規則、ポリシー、基準、ガイダンス、ミッションまたは事業のニーズなど、多くのソースから発展し得る。組織のリスクアセスメントとリスク許容度も、管理策パラメータ値を決定する上で重要な要因である。設定および選択操作の値は、組織によって規定されると管理策の一部となる。基本管理策で使用される組織が定める管理策パラメータは、それらの基本管理策に関連する拡張管理策にも適用される。管理策の実装は、完成した管理策ステートメントに照らして有効性が評価される。

管理策に組み込まれた設定と選択操作に加えて、反復と詳細化アクションによってさらなる柔軟性がもたらされる。反復により、組織は、異なる設定値や選択値を使用して管理策を何度も使用することができ、異なる状況で適用したり、複数のポリシーを実施することができる。例えば、組織では、1 つの管理策が複数のシステムで実装され、システムや運用環境ごとに異なるリスクに対応するために異なるパラメータが定められている場合がある。詳細化は、管理策に追加の実装詳細を提供するプロセスである。詳細化を使用して、適用可能なすべての範囲をカバーするために、反復と組み合わせて管理策の範囲を限定することもできる（例えば、異なる認証メカニズムを異なるシステムインタフェースに適用する）。組織は設定と選択操作、反復と詳細化アクションの組み合わせを管理策に適用することで、組織、ミッションと事業プロセス、およびシステムの実装レベルで幅広いセキュリティおよびプライバシー要件を満たすために必要な柔軟性を得ることができる。

設計課題としてのセキュリティ

「コンピュータシステムに十分なセキュリティ管理策を提供することは…システム設計の課題である。包括的なセキュリティを実現するには、ハードウェア、ソフトウェア、通信、物理的、人的、および管理手順上の保全措置の組み合わせが求められ…ソフトウェアによる保全措置だけでは不十分である。」

-- ***The Ware Report***
コンピュータセキュリティに関する国防科学評議委員会タスクフォース（Defense Science Board Task Force on Computer Security）、1970 年

2.3 管理策の実装アプローチ

第 3 章の管理策を実装するには、(1) *共通*（継承可能な）管理策の実装アプローチ、(2) *システム固有*管理策の実装アプローチ、および (3) *ハイブリッド*管理策の実装アプローチ、の 3 つの方法がある。管理策の実装アプローチは、管理策の適用範囲、管理策の共有性または継承性、および管理策の策定、実装、アセスメント、認可の責任を定義する。管理策の各実装アプローチには特定の目的があり、組織が適切な管理策を選択し、効果的な方法で管理策を実装し、また、セキュリティおよびプライバシー要件を満たすのに役立つことに重点を置いている。特定の管理策の実装アプローチは、複数のシステムおよび運用環境にまたがるセキュリティおよびプライバシーのケイパビリティを活用することにより、コストメリットを達成することができる。[27]

共通管理策とは、その実装によって、複数のシステムまたはプログラムにより*継承可能*なケ

[27] [SP 800-37]は、管理策実装アプローチ（以前は管理策の指定と呼ばれていた）についてと、*リスクマネジメントフレームワーク*において異なる実装アプローチがどのように使用されるかについて、追加のガイダンスを提供する。

イパビリティがもたらされる管理策のことである。システムまたはプログラムが、実装された管理策により保護されている場合に、管理策は継承可能と見なされるが、そうした管理策は、システムまたはプログラムに対して責任を負うエンティティとは別の、内部または外部のエンティティによって策定、実装、アセスメント、認可、および監視される。共通管理策によって提供されるセキュリティおよびプライバシーのケイパビリティは、ミッションまたは事業ライン、組織、エンクレーブ、運用環境、サイト、もしくはその他のシステムやプログラムなど、多くのソースから継承することができる。ただし、管理策を共通管理策として実装する場合、単一障害点のリスクが発生する可能性がある。

組織の情報システムの保護に必要な多くの管理策（「物理的および環境的保護」管理策、「職員のセキュリティ」管理策、「インシデント対応」管理策など）は継承可能であるため、共通管理策として有力な選択肢である。共通管理策には、「識別および認証」管理策、「境界保護」管理策、「監査および説明責任」管理策、「アクセス制御」管理策などの技術ベースの管理策も含まれる。開発、実装、アセスメント、認可、および監視に伴うコストは、共通管理策の実装アプローチを使用して、複数のシステム、組織要素、およびプログラムにわたって償却することができる。

共通管理策として実装されない管理策は、*システム固有*管理策または*ハイブリッド*管理策として実装される。システム固有管理策は、所定のシステムのシステムオーナーおよび認可権限のある担当者が主要な責任を担う。システム固有管理策を実装する際、管理策の実装が共通管理策と相互運用できない場合にリスクが生じる可能性がある。管理策の一部が共通（継承可能）で、他の部分がシステム固有である場合、組織は管理策を*ハイブリッド*管理策として実装することができる。例えば、組織は、組織のすべての情報システムのための緊急時対応計画に対し、事前に規定されたテンプレートを使用して管理策 CP-2 を実装し、必要に応じて、個々のシステムオーナーがシステム固有の使用に対して緊急時対応計画をテーラリングすることができる。ハイブリッド管理策における共通（継承可能）部分とシステム固有部分への分割は、採用する情報技術のタイプ、管理策を管理するために組織が使用するアプローチ、および責任の割り当てに応じて、組織によって異なる場合がある。管理策がハイブリッド管理策として実装されている場合、共通管理策プロバイダは、ハイブリッド管理策の*共通*部分を実装、アセスメント、および監視する責任を負い、システムオーナーは、ハイブリッド管理策の*システム固有*の部分を実装、アセスメント、および監視する責任を負う。管理策の共通部分とシステム固有の部分の実装および継続的な管理に関する責任が明確でない場合、管理策をハイブリッド管理策として実装すると、リスクが生じる可能性がある。

適切な管理策の実装アプローチ（すなわち、共通、ハイブリッド、またはシステム固有）の判断は状況によって異なる。単に管理策の文言に基づいて、管理策の実装アプローチを共通、ハイブリッド、またはシステム固有のいずれかであると判定することはできない。管理策の実装アプローチを特定することにより、組織は実装およびアセスメントに係るコストを大幅に節約でき、組織全体で管理策をより一貫して適用することができるようになる。通常、管理策の実装アプローチを特定するのは容易だが、実装には多大な計画と調整を要する。

管理策の実装アプローチ（すなわち、共通、ハイブリッド、またはシステム固有）の計画は、システム開発ライフサイクルの早い段階で実行し、管理策を提供するエンティティと調整することが最善である[SP 800-37]。同様に、管理策が継承可能である場合、管理策が、継承側のエンティティのニーズを満たすように、そうしたエンティティとの調整が必要である。これは、管理策パラメータの性質上、特に重要である。継承側のエンティティは、管理策の識別子（AC-1 など）が同一であるという理由だけで、管理策が同じであると想定してシステムに対する適切なリスクを軽減することはできない。システム固有のリスクを軽減するのに共通管理策が適切であるかどうかを判断するには、管理策パラメータ（設定や選択操作など）を考慮することが不可欠である。

2.4 セキュリティおよびプライバシー管理策

セキュリティおよびプライバシー管理策の選択と実装は、情報セキュリティおよびプライバシープログラムの目的と、それらのプログラムがそれぞれのリスクをどのように管理しているかを反映する。状況により、そうした目的とリスクは、独立している場合も、重複している場合もある。連邦政府の情報セキュリティプログラムは、機密性、完全性、可用性を提供するために、情報および情報システムを認可されていないアクセス、使用、開示、中断、変更、または破壊（すなわち、認可されていない行為またはシステム動作）から保護する責任を負う。これらのプログラムは、セキュリティリスクを管理し、適用されるセキュリティ要件への準拠を確保する責任も負っている。連邦政府のプライバシープログラムは、PII の作成、収集、使用、処理、保存、維持、配布、開示、または廃棄（総称して「取扱い」と呼ぶ）に付随する個人へのリスクを管理し、適用されるプライバシー要件への準拠を確保する責任を負う[28]。システムが PII を取扱う場合、情報セキュリティおよびプライバシープログラムは、システム内の PII のセキュリティリスクを管理する責任を共有する。このように責任が重複することから、管理策ベースラインにおけるセキュリティまたはプライバシー管理策としての指定や、プログラムまたはシステム計画に関係なく、セキュリティリスクを管理するために組織が選択する管理策は概ね同じものとなる。

管理策または拡張管理策の選択および／または実装が、プログラムの目的達成およびそれぞれのリスクを管理する能力に影響を与える状況もあり得る。管理策の詳解セクションでは、組織が管理策を実装するための最も効果的な方法を決定する際に特定のセキュリティおよび／またはプライバシーの考慮事項を考慮することができるように、これらの考慮事項を強調している場合がある。ただし、これらの考慮事項は網羅的なものではない。

例えば、組織は、PII を含まない情報リソースに対する認可されていないアクセスの監視をサポートするために、AU-3（「監査記録の内容」）を選択する場合がある。情報リソースの機密性が失われる可能性はプライバシーに影響しないため、セキュリティの目的が、管理策を選択する際の主要な要因となる。ただし、認可されていないアクセスの監視に関する管理策を実装する場合には、PII の取扱いが含まれる可能性があり、プライバシーリスクをもたらし、プライバシープログラムの目的に影響を与える可能性がある。AU-3 の詳解セクションにはプライバシーリスクの考慮事項が含まれているため、組織は管理策を実装するための最良の方法を判定する際にそれらの考慮事項を検討することができる。さらに、これらのプライバシーリスクの管理をサポートするために、拡張管理策 AU-3(3)（「個人情報要素の限定」）を選択することができる。

情報セキュリティおよびプライバシープログラムの目的とリスクマネジメントとの関係には順列があるため、PII を取扱う情報システムに対して適切な管理策を選択して実装するには、プログラム間の緊密な連携が必要である。組織は、両プログラムの目的の達成と、リスクの適切な管理を確実にするために、どのようにプログラム間の連携を促進し、制度化するかを考慮する[29]。

[28]プライバシープログラムは、個人情報の取扱いが、システムが個人の行動や活動に与える影響よりも影響が少ない場合、情報システムとの相互作用から生じる可能性のある個人へのリスクを考慮することもある。そのような影響は、個人の自律性に対するリスクを構成し、組織は、情報セキュリティおよびプライバシーのリスクに加えて、それらのリスクを管理するための措置を講じなければならない場合がある。

[29] 情報セキュリティおよびプライバシープログラムの連携をサポートするためのリソースは、[SP 800-53 RES]で入手可能である。

2.5 統合的信頼性および保証

システム、システムコンポーネント、およびシステムサービスの統合的信頼性（trustworthiness）は、組織が策定するリスクマネジメント戦略の重要な要素である[30]。ここでいう統合的信頼性とは、システムコンポーネント、サブシステム、システム、ネットワーク、アプリケーション、ミッション、事業機能、企業、またはその他のエンティティに求められる可能性のある要件を満たすために、それらが信頼されるに値するということを意味している[31]。統合的信頼性に関する要件には、中断、危険、脅威、プライバシーリスクといった形の様々な潜在的な逆境下における、（故障率などの狭義の）信頼性（reliability）、（保守・運用性を含む広義の）信頼性（dependability）、パフォーマンス、レジリエンス、安全性、セキュリティ、プライバシー、および生存性などの属性を含めることができる。なお、統合的信頼性の効果的な措置は、要件が完全かつ明確に規定されており、的確にアセスメントできる範囲でのみ意味を持つ。

システムの統合的信頼性に影響を与える 2 つの基本的な概念は、機能性と保証である。機能性は、組織のシステムとプログラム、およびそれらのシステムとプログラムが動作する環境内に実装されたセキュリティとプライバシーの特徴、機能、メカニズム、サービス、手順、アーキテクチャなどの観点から定義される。保証とは、システムの機能性が正しく実装され、意図したとおりに動作し、システムのセキュリティおよびプライバシー要件を満たすことに関して望ましい結果を生み出しているということ、すなわち、規定されたセキュリティおよびプライバシーポリシーを的確に仲介し実施する能力を備えていることに関する確実性の尺度である。

一般に、システムが期待どおりのことを実行し、有意義な保証を提供するという課題については、例えば、システムアーキテクチャ、ソフトウェア設計、仕様、プログラミングスタイル、および構成管理などに適用される規則を増やすことなどにより分析を簡素化または絞り込むといった技法によって向上させることができる。セキュリティおよびプライバシー管理策は、機能性と保証に対応しており、主に機能性に焦点をあてている管理策もあれば、主に保証に焦点をあてている管理策もある。また、一部の管理策は機能性と保証の双方をサポートすることができる。

組織は、保証に関連する管理策を選択することによって、システム開発活動を定義し、システムの機能性と動作に関するエビデンスを生成し、そうした機能性を提供したり、そうした動作を示すシステム要素までエビデンスを追跡したりすることができる。エビデンスは、システムが組織のミッションと事業機能をサポートしながら、規定されたセキュリティおよびプライバシー要件を満たしているといった一定の信頼を得るために使用される。保証に関連する管理策は、付属書 C の管理策要約表に示されている。

[30] [SP 800-160-1]は、システムセキュリティエンジニアリングと、信頼できるシステムを実現するためのセキュリティ設計原則の適用に関するガイダンスを提供している。
[31] [NEUM04]を参照のこと。

管理策実装のエビデンス

管理策の選択と実装にあたり、組織は、現在および今後の管理策アセスメントを支援するために必要となるエビデンス（成果物、文書など）を考慮することが重要である。こうしたアセスメントは、管理策が正しく実装され、意図したとおりに機能し、セキュリティおよびプライバシーポリシーを満たしているかどうかを判定するのに役立ち、ひいては、上級幹部が十分な情報に基づき*リスクベース*の意思決定を行うのに必要な情報を提供する。

第 3 章

管理策

セキュリティおよびプライバシー管理策および拡張管理策

本セキュリティおよびプライバシー管理策カタログは、システム、組織、および個人を保護する手段を提供している[32]。これらの管理策は、リスクマネジメントと、適用される連邦法、大統領令、指令、規則、ポリシー、および基準への遵守を促進するように設計されている。いくつかの例外を除いて、カタログ内のセキュリティおよびプライバシー管理策は、ポリシー、技術、および適用分野に中立であるため、管理策は、情報のライフサイクル全体にわたって情報と個人のプライバシーを保護するために必要な基本的な措置に焦点を当てている。セキュリティおよびプライバシー管理策が、全体的にポリシー、技術、および適用分野に中立であるからといって、それは、管理策がポリシー、技術、および適用分野を意識していないということを意味するものではない。ポリシー、技術、適用分野を理解することは、それらが実装されるときに管理策が適切であるようにするために必要なことである。ポリシー、技術、適用分野に中立な管理策カタログを採用することには、多くのメリットがある。また、組織に対して以下を行うことを奨励している。

- 組織のシステムで採用されている技術に関係なく、ミッションと事業の成功に必要なセキュリティおよびプライバシー機能とケイパビリティ、および情報の保護と個人のプライバシー保護に重点を置く。
- 特定の技術、運用環境、ミッションおよび事業機能、および関心のあるコミュニティへの適用可能性について、各セキュリティおよびプライバシー管理策を分析する。
- 可変パラメータを持つ管理策のテーラリングプロセスの一環として、セキュリティおよびプライバシーポリシーを規定する。

特定の技術が管理策で参照されているような少数のケースでは、セキュリティおよびプライバシーのリスクを管理する必要性が、技術に関連付けられている単一の管理策の要件の範囲を超える可能性があり、組織は留意する必要がある。追加で必要な保護対策は、カタログ内の他の管理策から入手できる。連邦情報処理標準規格（FIPS）、NIST 特別出版物（SP）、および NIST 機関間／内部報告書（NISTIR）は、スマートグリッド、クラウド、医療、モバイル、産業用制御システム、IoT デバイスなど、特定の技術や適用分野固有のアプリケーションのリスクを軽減するセキュリティおよびプライバシー管理策の選択に関するガイダンスを提供している[33]。また NIST 出版物は、第 3.1 節から第 3.20 節で特定の管理策に適用可能な参照として引用されている。

カタログ内のセキュリティおよびプライバシー管理策は、管理策の撤回、改訂、追加に伴い、時間の経過とともに変更されることが予想される。セキュリティおよびプライバシー計画の安定性を維持するために、管理策が撤回されるたびに管理策の番号が付け直されることはなく、むしろ、撤回された管理策の表示は、履歴管理上の目的のために管理策カタログに維持されている。管理策は、その管理策によって規定される機能またはケイパビリティが別の管理策に組み込まれた場合や、その管理策が既存の管理策と重複している場合、またはその管理策がもはや必要ではない、または効果的ではないと見なされる場合など、様々な理由で撤回されることがある。

[32] 本出版物の管理策は様々な形式でオンラインで入手できる。[NVD 800-53]を参照のこと。

[33] 例えば、[SP 800-82SP 800-82]は、産業用制御システムにおけるリスクマネジメントおよび管理策の選択に関するガイダンスを提供している。

脅威と脆弱性の情報、および敵対者が使用する戦術、技法、手順に関する情報を用いて、新たな管理策が定期的に策定されている。さらに、システムや組織に対する情報セキュリティのリスク、および情報処理に起因する個人のプライバシーに対するリスクを軽減する方法についての理解を深めることにより、新たな管理策が策定されている。また、新たな管理策は、法律、大統領令、規則、ポリシー、基準、またはガイドラインの新しい要件または変化する要件に基づいても策定されている。提案された管理策の変更は、管理策の安定性の必要性と、技術、脅威、脆弱性、攻撃のタイプ、および処理方法の変化に対応する必要性を考慮して、各改訂周期の中で慎重に分析されている。その目的は、組織や個人のニーズに適合させるために、情報セキュリティおよびプライバシーのレベルを経時的に調整することである。

3.1 アクセス制御

アクセス制御の要約表へのクイックリンク

AC-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。

1. 以下の[*選択(1 つ以上):組織レベル;ミッション/事業プロセスレベル;システムレベル*]のアクセス制御のポリシー。

(a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、および準拠に対処する。

(b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに適合している。

2. アクセス制御のポリシーと関連するアクセス制御の管理策の実装を促進するための手順。

b. アクセス制御のポリシーと手順の策定、文書化、および配布することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行のアクセス制御をレビューし、更新する。

1. ポリシーについて[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

2. 手順について[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

詳解:アクセス制御のポリシーと手順は、システムおよび組織で実装される AC ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に寄与する。したがって、セキュリティおよびプライバシープログラムがアクセス制御のポリシーと手順の策定と連携していることが重要である。組織レベルのセキュリティおよびプライバシープログラムのポリシーと手順を確立するがは望ましく、一般的には、ミッションまたはシステム固有のポリシーと手順の必要性をなくすことができる。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映する複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムに対して規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述するもので、手順の対象である個人または役割に指示することができる。手順は、システムのセキュリティおよびプライバシー計画の中に、または 1 つ以上の別の文書に文書化することもできる。アクセス制御のポリシーと手順の更新を引き起こす可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれる。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策:IA-1, PM-9, PM-24, PS-8, SI-12

拡張管理策:なし

参照資料:[OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100], [IR 7874]

AC-2 アカウント管理

管理策:

a. システム内での使用が許可されているアカウント、および特別に禁止されているアカウントのタイプを規定し、文書化する。

b. アカウントの管理者を設定する。

c. グループと役割の資格には[*設定:組織が定める前提条件と基準*]を必要とする。

d. 以下を規定する。

   1. システムの認可されたユーザ。

   2. グループおよび役割の資格。

   3. 各アカウントのアクセス認可(すなわち、特権)および[*設定:組織が定める属性(必要に応じて)*]。

e. アカウントの作成要求には[*設定:組織が定める職員または役割*]による承認を必要とする。

f. [*設定:組織が定めるポリシー、手順、前提条件、および基準*]に従って、アカウントを作成、有効化、変更、無効化、および削除する。

g. アカウントの使用を監視する。

h. アカウント管理者および[*設定:組織が定める職員または役割*]に以下の期間内に通知する。

   1. アカウントが不要になった場合[*設定:組織が定める期間*]。

   2. ユーザが退職または異動となった場合[*設定:組織が定める期間*]。

   3. 個人のシステムの利用権限または知る必要性を変更する場合[*設定:組織が定める期間*]。

i. 以下に基づいて、システムへのアクセスを認可する。

   1. 有効なアクセス認可。

   2. 意図されたシステムの利用。

   3. [*設定:組織が定める属性(必要に応じて)*]。

j. [*設定:組織が定める頻度*]でアカウントのアカウント管理要件への準拠をレビューする。

k. 個人がグループから削除されたときに、共有またはグループアカウントオーセンティケータ(配備されている場合)を変更するプロセスを規定し実装する。

l. アカウント管理プロセスを、職員の退職および異動プロセスと連携させる。

詳解:システムアカウントのタイプの例には、個人、共有、グループ、システム、ゲスト、匿名、緊急、開発者、一時的、保守などがある。認可されたシステムユーザの識別およびアクセス権限の指定は、セキュリティ計画の他の管理策の要件を反映している。システムアカウントの管理者権限を必要とするユーザは、システムオーナー、ミッションまたは事業オーナー、政府機関の情報セキュリティ責任者、または政府機関のプライバシー保護責任者など、そのようなアカウントと特権アクセスを承認する責任を有する組織の職員による追加の精査を受ける。リスクが増大するため、可能であれば組織が禁止すべきアカウントのタイプには、共有アカウント、グループアカウント、緊急アカウント、匿名アカウント、一時アカウント、ゲストアカウントなどがある。

アクセスされる場所に個人情報が含まれる場合、セキュリティプログラムは政府機関のプライバシー保護責任者と連携して、グループおよび役割の資格に関する特定の条件を定めたり、認可されたユーザ、グループと役割の資格、および各アカウントのアクセス権限を規定したり、組織のポリシーに従って、システムアカウントを作成、調整、または削除する。ポリシーには、アカウントの有効期限や、アカウントの無効化を引き起こすその他の要因などの情報を含めることができる。組織は、アカウント、アカウントのタイプ、またはその両方の組み合わせによって、

アクセス権やその他の属性を規定することを選択してもよい。アクセスを許可するために必要なその他の属性の例には、時刻、曜日、およびアクセス要求起点の制限などが含まれる。組織は、他のシステムアカウント属性を規定する際に、システム関連の要件とミッション／事業要件を考慮する。これらの要因を考慮しないと、システムの可用性に影響を与える可能性がある。

一時アカウントと緊急アカウントは、短期間の使用を目的としている。組織は、アカウントの即時有効化を必要としない短期アカウントを必要とする場合、通常のアカウントの有効化手順の一部として一時的なアカウントを作成する。組織は、危機的状況に対応し、アカウントの迅速な有効化が必要な場合には、緊急アカウントを作成する。したがって、緊急アカウントの有効化では、通常のアカウント認可プロセスが無視される場合がある。緊急用アカウントと一時アカウントを、特別なタスクやネットワークリソースが利用できない場合などに使用されるローカルログオンアカウント（最終手段のアカウントとも呼ばれる）などの使用頻度の低いアカウントと混同してはならない。このようなアカウントは引き続き利用可能であり、自動的な無効化または削除指定日の対象にはならない。アカウントを無効化または停止する条件には、共有/グループ、緊急、または一時的なアカウントが不要になった場合や、個人が異動または退職した場合が含まれる。メンバーがグループを離れるときに共有／グループオーセンティケータを変更することは、以前のグループメンバーが共有アカウントまたはグループアカウントへのアクセスを保持しないようにすることを目的としている。なおシステムアカウントのタイプによっては、専門的なトレーニングが必要な場合がある。

関連管理策：AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-2, AU-12, CM-5, IA-2, IA-4, IA-5, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, PT-2, PT-3, SC-7, SC-12, SC-13, SC-37

拡張管理策：

(1) アカウント管理 | 自動化されたシステムアカウント管理

[*設定：組織が定める自動化されたメカニズム*]を使用したシステムアカウントの管理をサポートする。

詳解：自動化されたシステムアカウント管理には、自動化されたメカニズムを使用したアカウントの作成、有効化、変更、無効化、および削除することが含まれている。また、アカウントが作成、有効化、変更、無効化、削除されたとき、またはユーザが退職や異動したときには、アカウント管理者に通知すること、システムアカウントの使用状況を監視すること、非定形的なシステムアカウントの使用状況を報告することが含まれる。自動化されたメカニズムには、内部システム機能と、電子メール、電話、およびテキストメッセージによる通知を含めることができる。

関連管理策：なし

(2) アカウント管理 | 一時アカウントおよび緊急アカウントの自動化された管理

[*設定：アカウントのタイプごとに組織が定める期間*]後の一時アカウントおよび緊急アカウントを自動的に[*選択：削除；無効化*]する。

詳解：一時アカウントおよび緊急アカウントの管理には、システム管理者の都合によるものではなく、事前に規定された期間が経過した後のアカウントの削除または無効化が含まれる。アカウントを自動的に削除または無効化することは、より一貫した実装となる。

関連管理策：なし

(3) アカウント管理 | アカウントの無効化

アカウントが次の場合は、[*設定：組織が定める期間*]内にアカウントを無効化する。

(a) 失効している。

(b) すでにユーザまたは個人に関連付けられていない。

(c) 組織のポリシーに違反している。または

(d) [*設定：組織が定める期間*]にわたって非アクティブであった。

詳解：失効、非アクティブ、またはその他の異常なアカウントの無効化は、システムの攻撃対象領域を減らすことになる最小特権と最小機能の概念をサポートする。

関連管理策：なし

(4) アカウント管理 | 自動化された監査

アカウントの作成、変更、有効化、無効化、および削除措置を自動的に監査する。

詳解：アカウント管理の監査記録は、AU-2 に従って規定され、AU-6 に従ってレビューし、分析し、報告される。

関連管理策：AU-2, AU-6

(5) アカウント管理 | 非アクティブログアウト

[*設定：組織が定める予想された非アクティブ期間を経過または定められたログアウトするタイミング*]の場合、ユーザにログアウトを要求する。

詳解：非アクティブ時のログアウトは行動ベースまたはポリシーベースであり、定められた期間よりも長い間非アクティブであることが予想される場合、ユーザはログアウトするために物理的な行動をとる必要がある。なお非アクティブ時のログアウトの自動実施は、AC-11 で対処されている。

関連管理策：AC-11

(6) アカウント管理 | 動的権限管理

[*設定：組織が定める動的権限管理ケイパビリティ*]を実装する。

詳解：静的アカウントおよび事前に規定されたユーザ権限を使用するアクセス制御アプローチとは対照的に、動的アクセス制御アプローチは、属性ベースのアクセス制御などの動的権限管理によって行われる実行時のアクセス制御の決定に依存する。ユーザアイデンティティは時間が経過しても比較的一定のままであるが、ユーザ特権は通常、現在進行中のミッションまたは事業要件および組織の運用上のニーズに基づいてより頻繁に変更される。動的権限管理の例としては、権限の変更を反映するためにユーザにセッションを終了して再起動することを要求するのとは対照的に、ユーザから権限を即座に取り消すことが挙げられる。動的権限管理には、特定のユーザプロファイルを編集するのではなく、動的ルールに基づいてユーザ権限を変更するメカニズムを含めることもできる。例えば、ユーザが通常の勤務時間外に業務を行っている場合や、職務機能または任務が変更された場合、またはシステムが緊急または緊急事態にある場合のユーザ権限の自動調整などである。動的権限管理には、例えば、通信に使用される暗号化キーに変更があった場合など、権限の変更による影響が含まれる。

関連管理策：AC-16

(7) アカウント管理 | 特権ユーザアカウント

(a) **[*選択：役割ベースのアクセスに関する基本的なスキーム；属性ベースのアクセスに関する基本的なスキーム*]に従って、特権ユーザアカウントを作成し管理する。**

(b) **特権的役割または属性設定を監視する。**

(c) **役割または属性の変更を監視する。**

(d) **特権的役割または属性の設定が適切でなくなった場合にアクセスを無効にする。**

詳解：特権的役割は、個人に設定された組織が定める役割であり、通常のユーザには実行が許可されていない特定のセキュリティ関連機能を個人が実行できるようにする。特権的役割には、キー管理、アカウント管理、データベース管理、システムおよびネットワーク管理、およびウェブ管理が含まれる。役割ベースのアクセスに関するスキームは、許可されたシステムアクセスと特権を役割にまとめるものである。対照的に、属性ベースのアクセスに関するスキームは、属性に基づいて、許可されるシステムアクセスおよび特権を指定する。

関連管理策：なし

(8) アカウント管理 | 動的アカウント管理

[*設定：組織が定めるシステムアカウント*]を動的に作成、有効化、管理、および無効化する。

詳解：システムアカウントを動的に作成、有効化、管理、および無効化する手法は、未知のエンティティに対して、実行時にアカウントを自動的にサービス利用可能な状態にするメカニズム（プロビジョニング）に依存している。組織は、関連する認可と特権を検証するための適切な権限者との信頼関係、事業ルール、およびメカニズムを確立することにより、システムアカウントの動的な管理、作成、有効化、および無効化を計画する。

関連管理策：AC-16

(9) アカウント管理 | 共有アカウントおよびグループアカウントの使用に対する制限

[*設定：組織が定める共有アカウントおよびグループアカウントを設定するための条件*]を満たす共有アカウントおよびグループアカウントの使用のみを許可する。

詳解：組織は、共有アカウントまたはグループアカウントの使用を許可する前に、そのようなアカウントに対する説明責任の欠如によるリスクの増大を考慮する。

関連管理策：なし

(10) アカウント管理 | 共有アカウントおよびグループアカウントのクレデンシャルの変更

［撤回：AC-2k に組み込まれた］

(11) アカウント管理 | 使用条件

[*設定：組織が定めるシステムアカウント*]に[*設定：組織が定める状況および／または使用条件*]を実施する。

詳解：使用条件を規定し実施することで、最小特権の原則を適用し、ユーザの説明責任を強化し、効果的なアカウント監視を有効にすることができる。アカウントの監視には、アカウントが組織のパラメータに違反して使用された場合に生成されるアラートが含まれる。組織は、システムアカウントを特定の曜日、時刻、または特定の期間に使用を制限するなど、特定の条件または状況を記述することができる。

関連管理策：なし

(12) アカウント管理 | 非定型的な使用のアカウントの監視

(a) [*設定：組織が定める非定型的な使用*]のシステムアカウントを監視する。

(b) システムアカウントの非定型的な使用を[*設定：組織が定める職員または役割*]に報告する。

詳解：非定型的な使用には、個人の通常の使用パターンと異なる、1 日の特定の時間帯や場所からのシステムへのアクセスが含まれる。非定型的な使用状況を監視することで、個人による不正な行動や進行中の攻撃が明らかになる場合がある。非定型的な使用法を識別するために収集されたデータは、個人の行動に関するこれまで知られていなかった情報を明らかにする可能性があるため、アカウント監視は、プライバシーリスクを不注意に引き起こす可能性がある。組織は、アカウントの非定型的な使用を監視することによるプライバシーリスクを、プライバシー影響評価においてアセスメントおよび文書化し、プライバシープログラム計画に沿った判断を行う。

関連管理策：AU-6, AU-7, CA-7, IR-8, SI-4

(13) アカウント管理 | リスクの高い個人のアカウントの無効化

[*設定：組織が定める重大なリスク*]を発見した場合、[*設定：組織が定める期間*]内に個人のアカウントを無効にする。

詳解：重大なセキュリティおよび／またはプライバシーリスクをもたらすユーザには、システムへの認可されたアクセスを使用して危害を加える意図があること、または敵対者が危害を加えることを、信頼できるエビデンスが示している個人が含まれる。そのような危害には、組織の運営、組織の資産、個人、他の組織、または国家に対する有害なインパクトが含まれる。リスクの高い個人のシステムアカウントを無効にする場合には、システム管理者、法務スタッフ、人事管理者、および認可権限のある担当者の間の緊密な連携が不可欠である。

関連管理策：AU-6, SI-4

参照資料: [SP 800-162], [SP 800-178], [SP 800-192]

AC-3 アクセス実施

管理策: 適切なアクセス制御ポリシーに従って、情報およびシステムリソースへの論理アクセスに対して承認された認可を実施する。

詳解: アクセス制御ポリシーは、組織のシステム内のアクティブなエンティティまたはサブジェクト(ユーザまたはユーザに代わって動作するプロセス)とパッシブなエンティティまたはオブジェクト(デバイス、ファイル、レコード、ドメインなど)間のアクセスを制御する。システムレベルで認可されたアクセスを実施し、システムがミッションおよび事業機能をサポートする多くのアプリケーションおよびサービスをホストできることを認識することに加えて、アクセス実施のメカニズムをアプリケーションおよびサービスレベルで採用して、情報セキュリティおよびプライバシーを強化することもできる。なおシステム内に実装されている論理アクセス制御とは別に、物理アクセス制御は、物理環境保護(PE)ファミリーの管理策で対処されている。

関連管理策: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC-24, AC-25, AT-2, AT-3, AU-9, CA-9, CM-5, CM-11, IA-2, IA-5, IA-6, IA-7, IA-11, MA-3, MA-4, MA-5, MP-4, PM-2, PS-3, PT-2, PT-3, SA-17, SC-2, SC-3, SC-4, SC-12, SC-13, SC-28, SC-31, SC-34, SI-4, SI-8

拡張管理策:

(1) アクセス実施 | 特権機能への制限付きアクセス

[撤回: AC-6 に組み込まれた]

(2) アクセス実施 | 二重認可

[*設定: 組織が定める特権コマンドおよび/または他の組織が定める措置*]に二重認可を実施する。

詳解: 一業務二人担当制(ダブルアサインメント)としても知られる二重認可は、インサイダー脅威に関連するリスクを軽減することができる。二重認可のメカニズムでは、実行するために二人の認可された個人の承認が必要となる。また共謀のリスクを軽減するために、組織は二重認可の職務をローテーションすることを考慮する。なお組織は、公共および環境の安全を確保するために迅速な対応が必要な場合、二重認可のメカニズムの実装に伴うリスクを考慮する必要がある。

関連管理策: CP-9, MP-6

(3) アクセス実施 | 必須アクセス制御

ポリシーが以下の場合に、ポリシーで規定された管理対象となるサブジェクト(subject)とオブジェクト(object)の集合に対して[*設定: 組織が定める必須アクセス制御ポリシー*]を実施する。

(a) システム内の管理対象のサブジェクトとオブジェクトの全体にわたって一様に実施されている場合。

(b) 情報へのアクセスを許可されたサブジェクトが、以下のいずれかを実行できないように規定されている場合。

(1) **認可されていないサブジェクトまたはオブジェクトに情報を渡す。**

(2) **他のサブジェクトにその権限を付与する。**

(3) **サブジェクト、オブジェクト、システム、またはシステムコンポーネントの 1 つ以上のセキュリティ属性(ポリシーで規定)を変更する。**

(4) **新しく作成または変更されたオブジェクトに関連付けるセキュリティ属性と(ポリシーで規定された)属性値を選択する。**

(5) **アクセス制御を管理するルールを変更する。**

(c) 上記制約の定められた部分(またはすべて)によって限定されないように、[*設定: 組織が定めるサブジェクト*]に、[*設定: 組織が定める権限*]を明示的に付与してもよいことを規定する。

詳解：必須アクセス制御は、任意アクセス制御の一つのタイプである。必須アクセス制御ポリシーは、すでにアクセスが許可されているオブジェクトから取得した情報を使用して、サブジェクトが実行できる措置を制限する。これによって、サブジェクトが認可されていないサブジェクトやオブジェクトに情報を渡すことを防ぐ。必須アクセス制御ポリシーは、アクセス制御権限の伝播に関してサブジェクトが実行できる措置を制限する。つまり、権限を持つサブジェクトは、その権限を他のサブジェクトに渡すことはできない。このポリシーは、システムが制御するすべてのサブジェクトとオブジェクトに一様に実施される。さもなければ、アクセス制御ポリシーが回避される可能性がある。この実施については、AC-25 に記述されているリファレンスモニタの考え方に適合する実装によって行われる。このポリシーはシステムによって制約される（つまり、情報がシステムの制御外に渡されると、情報に対する制限が有効であることを保証するために追加の手段が必要になる場合がある）。

上記の信頼できるサブジェクトには、最小特権の概念と一致する権限が付与される（AC-6 を参照）。信頼できるサブジェクトには、上記のポリシーに関連して、組織のミッション／事業ニーズを満たすために必要な最小限の権限のみが付与される。この管理策は、管理対象非機密情報（CUI）または機密情報（CI）へのアクセスに関するポリシーを確立する権限があり、システムの一部のユーザが、システム内に常駐するそのようなすべての情報へのアクセスを許可されていない場合に最適である。必須アクセス制御は、AC-3(4)で説明されている任意アクセス制御と連携して動作することができる。必須アクセス制御ポリシーによって動作が制限されているサブジェクトは、AC-3(4)のそれほど厳密でない制約の下でも動作できるが、必須アクセス制御ポリシーは AC-3(4)のそれほど厳密でない制約よりも優先される。例えば、必須アクセス制御ポリシーは、サブジェクトが異なるインパクトレベルまたは機密性レベルで運用している別のサブジェクトに情報を渡すことを防止する制約を課しているが、AC-3(4)は、サブジェクトがサブジェクトと同じインパクトレベルまたは機密性レベルを持つ他のサブジェクトに情報を渡すことを許可する。必須アクセス制御ポリシーの例としては、情報の機密性を保護するための Bell-LaPadula ポリシーおよび情報の完全性を保護するための Biba ポリシーなどがある。

関連管理策：SC-7

(4) アクセス実施 | 任意アクセス制御

ポリシーで規定された管理対象となるサブジェクトとオブジェクトのセットに対して[*設定：組織が定める任意アクセス制御ポリシー*]を実施し、ポリシーは、情報へのアクセスを許可されたサブジェクトが以下のうちの 1 つ以上のことを実行できることを規定する。

(a) 情報を他のサブジェクトまたはオブジェクトに渡す。

(b) その権限を他のサブジェクトに付与する。

(c) サブジェクト、オブジェクト、システム、またはシステムのコンポーネントのセキュリティ属性を変更する。

(d) 新しく作成または改訂されたオブジェクトに関連付けるセキュリティ属性を選択する。または

(e) アクセス制御を管理するルールを変更する。

詳解：任意アクセス制御ポリシーが実装されている場合、サブジェクトは、すでにアクセスが許可されている情報に対してどのような措置を実行できるかについて制約を受けない。したがって、情報へのアクセスを許可されたサブジェクトは、情報を他のサブジェクトまたはオブジェクトに渡すことを妨げられない（すなわち、サブジェクトは情報を渡す裁量権を有する）。任意アクセス制御は、AC-3(3)および AC-3(15)で説明されている必須アクセス制御と連携して動作することができる。必須アクセス制御ポリシーによってその動作が制限されているサブジェクトは、任意アクセス制御のそれほど厳密でない制約の下でも動作することができる。したがって、AC-3(3)では、サブジェクトが異なるインパクトレベルまたは機密性レベルで動作している別のサブジェクトに情報を渡すことを防止する制約を課しているが、AC-3(4)では、同じインパクトレベルまたは機密性レベルで任意のサブジェクトに情報を渡すことを許可している。ポリシーはシステムによる制約を受ける。情報がシステムによる管理の外部に渡される場合には、制約が有効なままであることを保証するために追加の手段が必要になることがある。任意アクセス制御の従来の定義ではアイデンティティベースのアクセス制御が必要であるが、任意アクセス制御のこの特定の使用方法では、そ

の制限は必要ない。

関連管理策：なし

(5) アクセス実施 | セキュリティ関連情報

セキュアで操作不可能なシステム状態の間を除き、[*設定：組織が定めるセキュリティ関連情報*]へのアクセスを防止する。

詳解：セキュリティ関連情報とは、システムのセキュリティおよびプライバシーポリシーの実施や、コードとデータの分離の維持に失敗する可能性のある方法で、セキュリティ機能の運用またはセキュリティサービスの提供にインパクトを与える可能性のあるシステム内の情報のことである。セキュリティ関連情報には、アクセス制御リスト、ルータまたはファイアウォールのフィルタリングルール、セキュリティサービスの構成パラメータ、および暗号鍵管理情報が含まれる。セキュアで操作不可能なシステム状態には、システムがメンテナンス、起動、トラブルシューティング、またはシャットダウンのためにオフラインになっているときなど、システムがミッションまたは事業関連の処理を実行していない時間が含まれる。

関連管理策：CM-6, SC-39

(6) アクセス実施 | ユーザおよびシステム情報の保護

[撤回：MP-4 および SC-28 に組み込まれた]

(7) アクセス実施 | 役割ベースのアクセス制御

規定されたサブジェクトとオブジェクトに対して役割ベースのアクセス制御ポリシーを実施し、[*設定：組織が定める役割とそのような役割を引き受ける認可されたユーザ*]に基づいてアクセスを制御する。

詳解：役割ベースのアクセス制御（RBAC）は、サブジェクトの規定された役割（すなわち、職務機能）に基づいてオブジェクトおよびシステム機能へのアクセスを実施するアクセス制御ポリシーである。組織は、職務機能に基づいて特定の役割を作成し、組織が定める役割に関連付けられたシステムで必要な操作を実行する認可（権限）を付与できる。ユーザに特定の役割が設定されると、それらの役割に規定された認可または権限を継承する。RBAC は、権限がすべてのユーザ（多数の個人になる可能性がある）に直接設定されるのではなく、役割の設定を通じて取得されるため、組織の権限管理を簡素化する。また、RBAC は、役割が設定された個人が、組織のミッションや事業機能をサポートするために必要な範囲を超えた情報へのアクセス権を与えられた場合、プライバシーとセキュリティのリスクを高める可能性もある。RBAC は、必須または任意のアクセス制御として実装できる。必須アクセス制御を使用して RBAC を実装する組織の場合、AC-3(3)の要件で、ポリシーの対象となるサブジェクトとオブジェクトの範囲が定められる。

関連管理策：なし

(8) アクセス実施 | アクセス認可の取り消し

[*設定：組織が定めるアクセス認可の取り消しのタイミングの管理に関するルール*]に基づいて、サブジェクトおよびオブジェクトのセキュリティ属性の変更に起因するアクセス認可の取り消しを実施する。

詳解：アクセスルールにおける取り消しは、取り消されるアクセスのタイプによって異なる場合がある。例えば、サブジェクト（ユーザまたはユーザに代わって動作するプロセス）がグループから削除された場合、オブジェクトが次に開かれるまで、またはサブジェクトがオブジェクトにアクセスしようとするまで、アクセス権が取り消されない場合がある。また、セキュリティラベルの変更に基づく取り消しは、すぐに有効になる場合がある。組織は、システムがそのようなケイパビリティを提供することができず、即時の取り消しが必要な場合、どのようにしたら取り消しを即時に実施できるかについての代替アプローチを提供する。

関連管理策：なし

(9) アクセス実施 | 管理されたリリース

以下の場合に限り、情報をシステム外にリリースする。

(a) 受理する[*設定：組織が定めるシステムまたはシステムコンポーネント*]が[*設定：組織が定める管理策*]を提供している場合。

(b) [*設定：組織が定める管理策*]が、リリースに指定された情報の適切性を検証するために使用される場合。

詳解：組織が情報を直接保護できるのは、情報がシステム内に存在する場合のみである。組織の情報がシステムの外部に伝送されると、組織の情報が適切に保護されていることを保証するために、追加の管理策が必要になる場合がある。システムが外部エンティティによって規定される保護の適切性を判断できない状況では、緩和措置として、組織は外部システムが適切な管理策を提供しているかどうかを手続き的に判断する。外部システムが提供する管理策の妥当性を判断するために使用される手段には、定期的なアセスメント（検査／テスト）の実施、組織とその相手方組織との間の合意の確立、またはその他のプロセスが含まれる。受信した情報を保護するために外部エンティティが使用する手段は、組織が使用する手段と同じである必要はないが、採用された手段は、情報と個人のプライバシーを保護するためのセキュリティおよびプライバシーポリシーの一貫した裁定を提供する上で十分なものである。

管理された情報開示には、情報を外部システムに開示する前に、情報を検証するための技術的または手続き的手段をシステムに実装することが求められる。例えば、システムが他の組織によって管理されているシステムに情報を渡す場合、技術的手段を用いて、エクスポートされた情報に関連するセキュリティおよびプライバシー属性が、受け取るシステムにとって適切であることを検証する。あるいは、組織が管理する空間内のプリンタにシステムが情報を送る場合、認可された個人だけがプリンタにアクセスできるようにするための手続的な手段を採用することができる。

関連管理策：CA-3, PT-7, PT-8, SA-9, SC-16

(10) アクセス実施｜アクセス制御のメカニズムへの監査優先

[*設定：組織が定める役割*]による[*設定：組織が定める条件*]の下で、自動アクセス制御のメカニズムへの監査済みオーバーライドを採用する。

詳解：人の生命に対する脅威や、組織の重要なミッションや事業機能を実行する能力を脅かすイベントなど、特定の状況では、アクセス制御のメカニズムのオーバーライド・ケイパビリティが必要になる場合がある。オーバーライドの条件は組織によって定められ、それらの限定された状況でのみ使用される。監査イベントについては AU-2 に規定されている。また監査記録については AU-12 で規定されている。

関連管理策：AU-2, AU-6, AU-10, AU-12, AU-14

(11) アクセス実施｜特定の情報タイプへのアクセスの制限

[*設定：組織が定める情報タイプ*]を含むデータリポジトリへのアクセスを制限する。

詳解：特定の情報へのアクセスを制限することは、システム内の特定の情報タイプのアクセス制御に柔軟性を与えることを目的としている。例えば、データベース全体へのアクセスを許可するのではなく、データベース内の特定のタイプの個人情報にのみアクセスを許可するために、役割ベースのアクセスを採用することができる。その他の例としては、暗号鍵、認証情報、および選択されたシステム情報へのアクセスの制限などがある。

関連管理策：CM-8, CM-12, CM-13, PM-5

(12) アクセス実施｜アプリケーションアクセスへのアサーションおよび実施

(a) インストールプロセスの一環として、[*設定：組織が定めるシステムアプリケーションおよび機能*]に必要なアクセスをアサーションするようアプリケーションに要求する。

(b) 認可されていないアクセスを防止するメカニズムを提供する。

(c) アプリケーションの初期インストール後のアクセス変更を承認する。

詳解：アプリケーションアクセスへのアサーションおよび実施は、ユーザの連絡先、全地球測位システム（GPS）、カメラ、キーボード、マイク、ネットワーク、電話、またはその他のファイルなど、既存のシステムアプリケーションおよび機能にアクセスする必要があるアプリケーションに対処することを目的としている。

関連管理策：CM-7

(13) アクセス実施 | 属性ベースのアクセス制御

規定されたサブジェクトおよびオブジェクトに対して属性ベースのアクセス制御ポリシーを実施し、[*設定：アクセス許可を引き受けるための組織が定める属性*]に基づいてアクセスを制御する。

詳解：属性ベースのアクセス制御は、規定された組織属性（例えば、職務権限、アイデンティティ）、処理属性（例えば、読み取り、書き込み、削除）、環境属性（例えば、時刻、位置）、およびリソース属性（文書の機密性区分など）に基づいて、認可されたユーザにシステムアクセスを制御するアクセス制御ポリシーである。組織は、組織が定める属性とルールに関連付けられたシステムで必要な操作を実行するために、属性と認可（権限）に基づいてルールを作成することができる。ユーザは、属性ベースのアクセス制御ポリシーまたはルールで規定された属性に設定されると、適切な権限を持つシステムが利用できるよう設定されたり、保護されたリソースへのアクセス権を動的に付与されたりする。属性ベースのアクセス制御は、必須または任意のアクセス制御として実装できる。AC-3(3)の要件は、必須アクセス制御とともに実装される場合、ポリシーの対象となるサブジェクトとオブジェクトの範囲を規定する。

関連管理策：なし

(14) アクセス実施 | 個人アクセス

個人が自身の個人情報の[*設定：組織が定める要素*]にアクセスできるようにするために、[*設定：組織が定めるメカニズム*]を規定する。

詳解：個人アクセスにより、個人は、その形式に関わらず、組織の記録内に保持されている個人情報を確認することができる。アクセスすることは、個人情報がどのように処理されているかについて理解を深めるのに役立つ。また、個人のデータが正確であることを保証するのにも役立つ。アクセスのメカニズムには、リクエストフォームとアプリケーションインタフェースを含めることができる。連邦政府機関の場合、[PRIVACT]プロセスは、記録通知システムおよび政府機関のウェブサイトに配置することができる。特定のタイプの記録へのアクセスは、適切でない場合（例えば、連邦政府機関の場合、記録システム内の法執行機関の記録は、[PRIVACT]に基づく開示を免除される場合がある）、または特定のレベルの認証保証が必要になる場合がある。組織の職員は、適切なメカニズムとアクセス権またはアクセス制限を決定するために、政府機関のプライバシー保護責任者および法律顧問に相談する。

関連管理策：IA-8, PM-22, PM-20, PM-21, PT-6

(15) アクセス実施 | 任意および必須アクセス制御

(a) ポリシーで指定された対象サブジェクトおよびオブジェクトのセットに対して[*設定：組織が定める必須アクセス制御ポリシー*]を実施する。

(b) ポリシーで指定された対象サブジェクトとオブジェクトのセットに対して、[*設定：組織が定める任意アクセス制御ポリシー*]を実施する。

詳解：必須アクセス制御ポリシーおよび任意アクセス制御ポリシーを同時に実装することで、ユーザまたはユーザに代わって動作するプロセスによるコードの認可されていない実行に対する追加の保護を提供できる。これにより、単一の侵害されたユーザまたはプロセスがシステム全体を侵害するのを防止することができる。

関連管理策：SC-2, SC-3, AC-4

参照資料：[PRIVACTPRIVACT], [OMB A-130], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-162], [SP 800-178], [IR 7874]

AC-4 情報フローの実施

管理策：[*設定：組織が定める情報フロー制御ポリシー*]に基づいて、システム内および接続されたシステム間の情報フローを制御するための承認された認可を実施する。

詳解：情報フロー制御は、情報がシステム内およびシステム間で情報が移動できる場所を（情報へのアクセスを許可されている人とは対照的に）、その情報への後続のアクセスに関係なく

規制する。フロー制御の制限には、組織内からのものであると主張する外部トラフィックを遮断すること、エクスポートが規制された情報が平文でインターネットに伝送されないようにすること、内部のウェブプロキシサーバからではないウェブリクエストを制限すること、データ構造と内容に基づく組織間の情報転送を限定することなどが含まれる。組織間で情報を転送するには、情報フローの実施方法を規定する合意が必要な場合がある（CA-3 を参照）。異なるセキュリティまたはプライバシーポリシーを持つ、異なるセキュリティまたはプライバシードメイン内のシステム間で情報を転送すると、そのような転送が 1 つまたは複数ドメインのセキュリティまたはプライバシーポリシーに違反するリスクが生じる。このような状況では、情報オーナー／スチュワードは、接続されたシステム間における指定されたポリシー実施ポイントにおけるガイダンスを提供する。組織は、特定のセキュリティおよびプライバシーポリシーを実施するために、特定の構造的な問題解決方法を義務付けることを検討する。実施には、接続されたシステム間の情報転送を禁止（すなわち、アクセスのみを許可）すること、別のセキュリティまたはプライバシードメインまたは接続されたシステムから情報を受け入れる前に書き込み許可を確認すること、一方向の情報フローを実施するためのハードウェアによるメカニズムを採用すること、およびセキュリティまたはプライバシーの属性とラベルを再設定するための信頼性のある再評価のメカニズムを実装することなどが含まれる。

組織は通常、システム内の指定された発信元と宛先の間、および接続されたシステム間の情報フローを制御するために、情報フロー制御ポリシーおよび実施のメカニズムを採用する。フロー制御は、情報または情報パス、あるいはその両方の特性に基づいている。実施は、例えば、ルールセットを採用したり、システムサービスを制限する構成設定を確立したり、ヘッダー情報に基づいてパケットフィルタリングケイパビリティを提供する、またはメッセージの内容に基づいてメッセージフィルタリングケイパビリティを提供したりする境界保護デバイスで行われる。組織はまた、情報フローの実施に重要なフィルタリングおよび／または検査のメカニズム（すなわち、ハードウェア、ファームウェア、およびソフトウェアコンポーネント）の統合的信頼性についても考慮する必要がある。拡張管理策 3～32 は、主に、クロスドメインソリューションのニーズに対応し、高度なフィルタリング技法、詳細な分析、および複数ドメインを接続する製品に実装された強力なフローの実施のメカニズム（高保証ガードなど）に焦点を当てている。このようなケイパビリティは、一般的には市販の製品では利用できない。また情報フローの実施は、コントロールプレーンにおけるトラフィック（ルーティングや DNS など）にも適用される。

関連管理策：AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-3, CA-9, CM-7, PL-9, PM-24, SA-17, SC-4, SC-7, SC-16, SC-31

拡張管理策：

(1) 情報フローの実施 | オブジェクトのセキュリティおよびプライバシー属性

[*設定：組織が定める情報、ソース、および宛先オブジェクト*]に関連付けられた[*設定：組織が定めるセキュリティおよびプライバシー属性*]を使用して、フロー制御の決定の根拠として[*設定：組織が定める情報フロー制御ポリシー*]を実施する。

詳解：情報フローの実施のメカニズムは、情報（すなわち、データのコンテンツと構造）と発信元および宛先のオブジェクトに関連付けられたセキュリティおよびプライバシーの属性を比較し、実施のメカニズムが情報フロー制御ポリシーで明示的に許可されていない情報フローに遭遇した場合に適切に対応する。例えば、「極秘」というラベルの付いた情報オブジェクトは、「極秘」というラベルの付いた宛先オブジェクトにフローすることは許可されるが、「機密」というラベルの付いた情報オブジェクトは、「極秘」というラベルが付いた宛先オブジェクトにフローすることは許可されない。個人情報のデータセットには、他のタイプのデータセットとの結合を制限するタグが付けられている可能性があるため、その場合、制限されたデータセットへのフローは許可されない。セキュリティおよびプライバシーの属性には、トラフィックフィルタファイアウォールで使用される発信元アドレスと宛先アドレスを含めることもできる。明示的なセキュリティまたはプライバシー属性を使用したフロー制御の実施は、例えば、特定のタイプの情報の開示を制御するために使用することができる。

関連管理策：なし

(2) 情報フローの実施 | 処理ドメイン

フロー制御の決定の根拠として[*設定：組織が定める情報フロー制御ポリシー*]を実施するために保護された処理ドメインを使用する。

詳解：システム内の保護された処理ドメインは、他の処理スペースとの相互作用が制御された処理スペースであり、これらのスペース間および情報オブジェクトとの間の情報フローの制御を可能にする。保護された処理ドメインは、例えば、ドメインおよびタイプの適用を実装することによって提供できる。ドメインおよびタイプの適用の実施では、システムプロセスがドメインに割り当てられ、情報はタイプによって識別され、情報フローは、許可された情報アクセス（すなわち、ドメインおよびタイプによって決定される）、ドメイン間の許可されたシグナル送付、および他のドメインへの許可されたプロセス遷移などに基づいて制御される。

関連管理策：SC-39

(3) 情報フローの実施 | 動的情報フロー制御

[*設定：組織が定める情報フロー制御ポリシー*]を実施する。

詳解：動的な情報フロー制御に関する組織のポリシーには、変化する状況、ミッション、または運用上の考慮事項に基づく情報フローの許可または禁止が含まれる。変化する状況には、ミッションまたは事業ニーズの緊急性の変化によるリスク許容度の変化、脅威環境の変化、および潜在的に有害または不利益となるイベントの検知などが含まれる。

関連管理策：SI-4

(4) 情報フローの実施 | 暗号化された情報のフロー制御

[*設定：組織が定める手順またはメカニズム*]として、[*選択（1 つ以上）：情報を復号する；暗号化された情報のフローを阻止する；暗号化された情報を渡そうとする通信セッションを終了する*]ことにより、暗号化された情報が[*設定：組織が定める情報フロー制御メカニズム*]を迂回することを防止する。

詳解：フロー制御のメカニズムには、コンテンツチェック、セキュリティポリシーフィルタ、データタイプ識別子などがある。暗号化という用語は、フィルタリングのメカニズムによって認識されないようにエンコードされたデータを範囲に含めるべく拡張されている。

関連管理策：SI-4

(5) 情報フローの実施 | 組み込みデータタイプ

他のデータタイプ内へのデータタイプの組み込みに[*設定：組織が定める制限*]を実施する。

詳解：データタイプを他のデータタイプに組み込むと、フロー制御の有効性が低下する可能性がある。データタイプの組み込みには、他のファイル内のオブジェクトとしてファイルを挿入することや、複数の組み込みデータタイプを含む可能性のある圧縮またはアーカイブされたデータタイプを使用することが含まれる。データタイプの組み込みに関する制限は、組み込みのレベルを考慮し、検査ツールのケイパビリティを超えるデータタイプの組み込みのレベルを禁止する。

関連管理策：なし

(6) 情報フローの実施 | メタデータ

[*設定：組織が定めるメタデータ*]に基づいて情報フロー制御を実施する。

詳解：メタデータは、データの特性を記述する情報である。メタデータには、データ構造を記述する構造メタデータ、またはデータコンテンツを記述する記述メタデータを含めることができる。メタデータに基づいて許可された情報フローを実施することで、より簡単かつ効果的なフロー制御が可能となる。組織は、データの的確性（つまり、メタデータの値がデータに関して正しいという情報）、データの完全性（メタデータのタグへの認可されていない変更からの保護）、およびメタデータのデータ本体部分へのバインディング（すなわち、適切に保証された十分に強いバインディング技法を採用すること）に関するメタデータの統合的信頼性を考慮する。

関連管理策：AC-16, SI-7

(7) 情報フローの実施 | 一方向フローのメカニズム

ハードウェアベースのフロー制御のメカニズムを介して一方向の情報フローを実施す

る。

詳解：一方向フローのメカニズムは、単方向ネットワーク、単方向セキュリティゲートウェイ、またはデータダイオードと呼ばれることもある。一方向フローのメカニズムを使用すると、インパクトの小さいあるいは非機密情報を扱うドメインまたはシステムからのデータのインポートを許可すると同時に、インパクトの大きいあるいは国家機密情報を扱うドメインまたはシステムからのデータのエクスポートを防止することができる。

関連管理策：なし

(8) 情報フローの実施 | セキュリティおよびプライバシーポリシーフィルタ

(a) [*設定：組織が定める情報フロー*]のフロー制御の決定の根拠として、[*設定：組織が定めるセキュリティまたはプライバシーポリシーフィルタ*]を使用して、情報フロー制御を実施する。

(b) [*設定：組織が定めるセキュリティまたはプライバシーポリシー*]に従って、フィルタ処理に失敗した後のデータを[*選択（1 つ以上）：阻止；除去；変更；隔離*]する。

詳解：組織が定めるセキュリティまたはプライバシーポリシーフィルタは、データ構造とコンテンツに対応できる。例えば、データ構造に対するセキュリティまたはプライバシーポリシーフィルタは、最大ファイル長、最大フィールドサイズ、およびデータ／ファイルタイプ（構造化データと非構造化データの場合）をチェックできる。データコンテンツのセキュリティまたはプライバシーポリシーフィルタは、特定の単語、列挙値またはデータ値の範囲、および隠蔽されたコンテンツなどをチェックできる。構造化データは、アプリケーションによるデータコンテンツの解釈を可能にする。非構造化データとは、データ構造を持たないデジタル情報、あるいはデータまたはフロー実施の決定によって伝達される情報のインパクトまたは機密性レベルに対処するためのルールセットの策定を容易にしないデータ構造を持つデジタル情報を指す。非構造化データは、本質的に言語ベースではないビットマップオブジェクト（すなわち、画像、ビデオ、またはオーディオファイル）と、手書きまたは印刷された言語に基づくテキストオブジェクトで構成される。組織は、情報フロー制御の目的を達成するために、複数のセキュリティまたはプライバシーポリシーフィルタを実装できる。

関連管理策：なし

(9) 情報フローの実施 | 人によるレビュー

[*設定：組織が定める条件*]の下で、[*設定：組織が定める情報フロー*]に対して人によるレビューを実施する。

詳解：組織は、自動フロー制御の決定が可能なすべての状況に対して、セキュリティまたはプライバシーポリシーフィルタを規定する。完全に自動化されたフロー制御の決定が不可能な場合は、自動化されたセキュリティまたはプライバシーポリシーフィルタリングの代わりに、またはそれを補完するものとして、人によるレビューを採用することができる。組織が必要と判断した場合にも、人によるレビューが採用される場合がある。

関連管理策：なし

(10) 情報フローの実施 | セキュリティまたはプライバシーポリシーフィルタの有効化および無効化

特権管理者が、[*設定：組織が定めるセキュリティまたはプライバシーポリシーフィルタ*]を[*設定：組織が定める条件*]の下で有効化および無効化するケイパビリティを提供する。

詳解：例えば、システム認可によって許可されている場合、管理者はセキュリティまたはプライバシーポリシーフィルタを有効にして、承認されたデータタイプに対応することができる。管理者は、転送されるデータタイプ、発信元と宛先のセキュリティドメイン、およびその他のセキュリティまたはプライバシー関連機能に基づいて、特定のデータフローで実行されるフィルタを必要に応じて選択するケイパビリティも有している。

関連管理策：なし

(11) 情報フローの実施 | セキュリティまたはプライバシーポリシーフィルタの構成

特権管理者が異なるセキュリティまたはプライバシーポリシーをサポートする[*設定：組*]

***組織が定めるセキュリティまたはプライバシーポリシーフィルタ*]を構成するケイパビリティを提供する。**

詳解：文書化には、セキュリティまたはプライバシーポリシーフィルタの構成に関する詳細情報が含まれる。例えば、管理者は、セキュリティまたはプライバシーポリシーのメカニズムが組織から提供される規定に従ってチェックする不適切な単語のリストを含むように、セキュリティまたはプライバシーポリシーフィルタを構成することができる。

関連管理策：なし

(12) 情報フローの実施 | データタイプ識別子

異なるセキュリティドメイン間で情報を転送する場合、[*設定：組織が定めるデータタイプ識別子*]を使用して、情報フローの決定に不可欠なデータを検証する。

詳解：データタイプ識別子には、ファイル名、ファイルタイプ、ファイル署名またはトークン、および複数の内部ファイル署名またはトークンが含まれる。システムは、データタイプフォーマット仕様に準拠するデータの転送のみを許可する。データタイプの識別と検証は、許可された各データ形式に関連する規定された仕様に基づいている。ファイル名と番号だけでは、データタイプの識別には使用できない。コンテンツは、適切なデータタイプであることを確認するために、その仕様に対して構文的および意味的に検証される。

関連管理策：なし

(13) 情報フローの実施 | ポリシー関連サブコンポーネントへの分解

異なるセキュリティドメイン間で情報を転送する場合、ポリシー実施のメカニズムに供するために、情報を[*設定：組織が定めるポリシー関連サブコンポーネント*]に分解する。

詳解：情報を転送する前に情報をポリシー関連のサブコンポーネントに分解すると、発信元、宛先、電子証明書、機密性区分、添付ファイル、およびその他のセキュリティまたはプライバシー関連のコンポーネントの差別化要因に関するポリシー決定が容易になる。ポリシー実施のメカニズムは、情報のポリシー関連サブコンポーネントにフィルタリング、検査、および／または無害化のルールを適用して、そのような情報を異なるセキュリティドメインに転送する前にフロー制御の実施を容易にしている。

関連管理策：なし

(14) 情報フローの実施 | セキュリティまたはプライバシーポリシーフィルタの制約

異なるセキュリティドメイン間で情報を転送する場合は、データ構造とコンテンツを制限する完全に列挙された形式を必要とする[*設定：組織が定めるセキュリティまたはプライバシーポリシーフィルタ*]を実装する。

詳解：データ構造およびコンテンツの制限は、ドメイン間のトランザクションにおける潜在的に悪意のある、または容認されないコンテンツの範囲を縮小する。データ構造を制限するセキュリティまたはプライバシーポリシーフィルタには、ファイルサイズとフィールド長の制限が含まれる。データコンテンツポリシーフィルタには、文字セットのエンコード形式、文字データフィールドが英数字のみを含むように制限すること、特殊文字を禁止すること、スキーマ構造を検証することなどが含まれる。

関連管理策：なし

(15) 情報フローの実施 | 容認されない情報の検知

異なるセキュリティドメイン間で情報を転送するときは、[*設定：組織が定める容認されない情報*]が存在するかどうかを調べ、[*設定：組織が定めるセキュリティまたはプライバシーポリシー*]に従って、そのような情報の転送を禁止する。

詳解：容認されない情報には、悪意のあるコード、発信元ネットワークからの開示に不適切な情報、または宛先ネットワーク上のサービスやシステムを混乱または害する可能性のある実行可能コードが含まれる。

関連管理策：SI-3

(16) 情報フローの実施 | 相互接続されたシステムでの情報転送

[撤回：AC-4 に組み込まれた]

(17) 情報フローの実施 | ドメイン認証

情報転送のために、[*選択(1 つ以上):組織;システム;アプリケーション;サービス;個人*]によって発信元ポイントおよび宛先ポイントを一意に識別および認証する。

詳解:アトリビューションは、セキュリティおよびプライバシーの運用の概念における重要なコンポーネントである。システム内を流れる情報の発信元ポイントと宛先ポイントを識別する機能により、イベントのフォレンジックな再構築が可能になり、ポリシー違反を特定の組織または個人によるものであるとすることにより、ポリシーへの準拠が促進される。ドメイン認証を成功させるには、システムラベルが、情報の準備、送信、受信、または配布に関与するシステム、組織、および個人を区別する必要がある。また、組織は、アトリビューションによって、システム内を流れる際に個人情報の取扱いの系統をより良く維持することができ、同意の追跡、ならびに個人からの修正、削除、アクセス要求を容易にすることができる。

関連管理策:IA-2, IA-3, IA-9

(18) 情報フローの実施 | セキュリティ属性のバインディング

[撤回:AC-16 に組み込まれた]

(19) 情報フローの実施 | メタデータの検証

異なるセキュリティドメイン間で情報を転送する場合、メタデータに[*設定:組織が定めるセキュリティまたはプライバシーポリシーのフィルタ*]を実装する。

詳解:すべての情報(メタデータとそのメタデータが適用されるデータを含む)は、フィルタリングおよび検査の対象となる。組織によっては、メタデータとデータのデータ本体(つまり、メタデータがバインディングされているデータのみ)を区別する。また、他の組織ではそのような区別をせず、メタデータおよびメタデータが適用されるデータをデータ本体の一部とみなす。

関連管理策:なし

(20) 情報フローの実施 | 承認されたソリューション

[*設定:組織が定める承認された構成におけるソリューション*]を採用して、セキュリティドメイン全体の[*設定:組織が定める情報*]のフローを制御する。

詳解:組織は、機密性区分の境界を越えた情報フローのタイプに応じて、ドメイン間のポリシーおよびガイダンスで承認されたソリューションと構成を規定する。国家安全保障局(NSA:National Security Agency)の国家クロスドメイン戦略管理局(NCDSMO:National Cross Domain Strategy and Management Office)は、承認されたクロスドメインソリューションの一覧表を提供している。詳細については、ncdsmo@nsa.gov に問い合わせのこと。

関連管理策:なし

(21) 情報フローの実施 | 情報フローの物理的または論理的分離

[*設定:組織が定めるメカニズムおよび/または技法*]を使用して、論理的または物理的に分離された情報フローの[*設定:組織が定める情報のタイプごとに必要な分離*]を行う。

詳解:規定されたタイプのデータに関連付けられている情報フローの分離を実施することで、伝送中に情報が混在しないようにしたり、他の方法では実現できない伝送路によるフロー制御を可能にしたりすることで、保護を強化できる。分離可能な情報のタイプには、インバウンドおよびアウトバウンドの通信トラフィック、サービス要求と応答、セキュリティへのインパクトや機密性レベルが異なる情報が含まれる。

関連管理策:SC-32

(22) 情報フローの実施 | アクセス専用

異なるセキュリティドメイン間の情報フローを防止しつつ、単一のデバイスから複数の異なるセキュリティドメインに存在するコンピューティングプラットフォーム、アプリケーション、またはデータへのアクセスを提供する。

詳解:システムは、ユーザが異なるセキュリティドメイン間でデータまたは情報を転送する

ことを可能にするメカニズムを提供することなく、接続された各セキュリティドメインにアクセスするケイパビリティをユーザに提供する。アクセス専用ソリューションの例としては、情報を確実に分離したまま、異なるセキュリティ区分を持つ情報へのアクセスをユーザに提供する端末がある。

関連管理策：なし

(23) 情報フローの実施 | 非公開情報の更新

異なるセキュリティドメイン間で情報を転送する場合、[*設定：組織が定める更新措置*]を実装することにより、非公開情報を更新する。

詳解：非公開情報を更新することで、セキュリティドメイン間で情報が転送される際のデータの流出や攻撃を防止することができる。更新措置には、マスキング、置換、修正、削除、または改訂が含まれる。

関連管理策：なし

(24) 情報フローの実施 | 内部正規化フォーマット

異なるセキュリティドメイン間で情報を転送する場合、受信データを解析して内部正規化フォーマットにすることで、意図した仕様と一致するようにデータを再生成する。

詳解：データを正規化された形式に変換することは、悪意のある攻撃や大量のデータ抜き取りを阻止するための最も効果的なのメカニズムの 1 つである。

関連管理策：なし

(25) 情報フローの実施 | データのサニタイズ

異なるセキュリティドメイン間で情報を転送する場合は、[*設定：組織が定めるポリシー*]に従って、データをサニタイズし、[*選択（1 つ以上）：悪意のあるコンテンツの配信、悪意のあるコードによる乗っ取り操作（コマンドアンドコントロール）、悪意のあるコードの増強、およびデジタル迷彩技術（ステガノグラフィー）でエンコードされたデータ；機微情報の流出*]などを最小限に抑える。

詳解：データのサニタイズは、メモリデバイス（ハードドライブ、フラッシュメモリ／ソリッドステートドライブ、モバイルデバイス、CD、DVD など）に保存されたデータまたはハードコピー形式で保存されたデータを不可逆的に削除または破壊するプロセスである。

関連管理策：MP-6

(26) 情報フローの実施 | フィルタリング処理の監査

異なるセキュリティドメイン間で情報を転送する場合、フィルタリングされる情報のコンテンツフィルタリング処理と結果を記録し監査する。

詳解：コンテンツフィルタリングとは、クロスドメインソリューションを通過する情報を検査し、その情報が事前に規定されたポリシーを満たすかどうかを判定するプロセスである。コンテンツフィルタリング処理およびフィルタリング処理の結果は、適切なフィルタリング処理が確実に適用されるように、個々のメッセージに対して記録される。コンテンツフィルタレポートは、メッセージコンテンツが更新された理由やフィルタリングプロセスが失敗した理由を特定するなど、トラブルシューティングを支援するために使用される。監査イベントは AU-2 で規定される。監査記録は AU-12 で作成される。

関連管理策：AU-2, AU-3, AU-12

(27) 情報フローの実施 | 冗長／独立フィルタリングのメカニズム

異なるセキュリティドメイン間で情報を転送する場合、各データタイプに冗長かつ独立したフィルタリングのメカニズムを提供するコンテンツフィルタリングソリューションを実装する。

詳解：コンテンツフィルタリングは、クロスドメインソリューションを通過する情報を検査し、その情報が事前に規定されたポリシーに適合しているかどうかを判定するプロセスである。冗長かつ独立したコンテンツフィルタリングは、単一障害点（SPOF：single point of failure）フィルタリングシステムを排除する。独立性は、異なるコードベースとサポートライブラリ（異なるベンダの JPEG ライブラリを使用する 2 つの JPEG フィルタなど）および複数

の独立したシステムプロセスを使用するコンテンツフィルタの実装として規定される。

関連管理策:なし

(28) 情報フローの実施 | 線形フィルタパイプライン

異なるセキュリティドメイン間で情報を転送する場合は、任意および必須アクセス制御で実施される線形コンテンツフィルタパイプラインを実装する。

詳解:コンテンツフィルタリングは、クロスドメインソリューションを通過する情報を検査し、その情報が事前に規定されたポリシーに適合しているかどうかを判定するプロセスである。線形コンテンツフィルタパイプラインを使用することで、フィルタプロセスが迂回されず、常に呼び出されるようになる。一般に、単一のデータタイプのコンテンツフィルタリングに並列フィルタリングアーキテクチャを使用すると、迂回と非呼び出しの問題が発生する。

関連管理策:なし

(29) 情報フローの実施 | フィルタオーケストレーションエンジン

異なるセキュリティドメイン間で情報を転送する場合、コンテンツフィルタオーケストレーションエンジンを使用して、以下を確認する。

(a) コンテンツフィルタリングのメカニズムが、エラーなしで実行を正常に完了する。

(b) コンテンツフィルタリング処理が正しい順序で行われ、[*設定:組織が定めるポリシー*]に準拠している。

詳解:コンテンツフィルタリングは、クロスドメインソリューションを通過する情報を検査し、その情報が事前に規定されたセキュリティポリシーに適合しているかどうかを判定するプロセスである。オーケストレーションエンジンは、コンテンツフィルタリングプロセスでの活動(手動および自動)のシーケンスを調整する。エラーは、コンテンツフィルタリングプロセスの異常な処理または予期しない終了として規定される。これは、ポリシーに準拠していないため、フィルタリングが失敗した場合とは異なる。コンテンツフィルタレポートは、期待されるフィルタリング処理が正常に完了することを保証するために一般的に使用されるメカニズムである。

関連管理策:なし

(30) 情報フローの実施 | 複数のプロセスを使用するフィルタリングのメカニズム

異なるセキュリティドメイン間で情報を転送する場合、複数のプロセスを使用してコンテンツフィルタリングのメカニズムを実装する。

詳解:コンテンツフィルタリングのメカニズムを実装するために複数のプロセスを使用することで、単一障害点の可能性が減少する。

関連管理策:なし

(31) 情報フローの実施 | 失敗したコンテンツの転送防止

異なるセキュリティドメイン間で情報を転送する場合、失敗したコンテンツが受信ドメインへの転送されることを防止する。

詳解:フィルタリングチェックに失敗したコンテンが受信ドメインに転送された場合、システムが損傷する可能性がある。

関連管理策:なし

(32) 情報フローの実施 | 情報転送のプロセス要件

異なるセキュリティドメイン間で情報を転送する場合、フィルタパイプライン間で情報を転送するプロセスは、以下のとおりである。

(a) メッセージコンテンツをフィルタリングしない。

(b) フィルタリングメタデータを検証する。

(c) フィルタリングメタデータに関連するコンテンツがフィルタリングを正常に完了したことを保証する。

(d) コンテンツを宛先フィルタパイプラインに転送する。

詳解：フィルタパイプライン間で情報を転送するプロセスは、そのプロセスが正しく動作することを保証するために、最小限の複雑さおよび機能性を備えている。

関連管理策：なし

参照資料：[SP 800-160-1], [SP 800-162], [SP 800-178], [IR 8112]

AC-5 職務の分離

管理策：

a. [*設定：組織が定める分離を必要とする個人の職務*]を識別し、文書化する。

b. 職務の分離をサポートするためのシステムアクセス認可を規定する。

詳解：職務の分離は、認可された権限の乱用の可能性に対処し、共謀のない悪意のある活動のリスクを軽減するのに役立つ。職務の分離には、ミッションまたは事業機能とサポート機能を異なる個人または役割に分割することや、システムサポート機能を異なる個人が実施すること、およびアクセス制御機能を管理するセキュリティ職員が監査機能も管理しないようにすることなどが含まれる。職務の分離違反は、システムとアプリケーションドメインにまたがる可能性があるため、組織は職務分離に関するポリシーを策定する際に、システムとシステムコンポーネント全体を考慮する。AC-2 のアカウント管理活動、AC-3 のアクセス制御のメカニズム、および IA-2、IA-4、IA-12 のアイデンティティ管理活動を通じて、職務の分離が実施される。

関連管理策：AC-2, AC-3, AC-6, AU-9, CM-5, CM-11, CP-9, IA-2, IA-4, IA-5, IA-12, MA-3, MA-5, PS-2, SA-8, SA-17

拡張管理策：なし

参照資料：なし

AC-6 最小特権

管理策：設定された組織のタスクを実行するために必要なユーザ（またはユーザに代わって動作するプロセス）に対して認可されたアクセスのみを許可する、最小特権の原則を採用する。

詳解：組織は、特定の職務およびシステムに対して最小特権を採用する。最小特権の原則はシステムプロセスにも適用され、プロセスがシステムにアクセスし、組織のミッションまたは事業機能を達成するために必要なレベル以下の特権レベルで動作することを保証する。組織は、最小特権を達成するために、必要に応じて追加のプロセス、役割、およびアカウントの作成を考慮する。また組織は、組織のシステムの開発、実装、運用に最小特権を適用する。

関連管理策：AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-8, SA-15, SA-17, SC-38

拡張管理策：

(1) 最小特権 | セキュリティ機能へのアクセスの認可

以下に対するアクセスを[*設定：組織が定める個人または役割*]に認可する。

(a) [*設定：組織が定めるセキュリティ機能（ハードウェア、ソフトウェア、およびファームウェアに展開）*]。

(b) [*設定：組織が定めるセキュリティ関連情報*]。

詳解：セキュリティ機能には、システムアカウントの作成、アクセス認可（すなわち、許諾、特権）の構成、監査対象イベント設定の構成、および侵入検知パラメータの作成が含まれる。セキュリティ関連情報には、ルータまたはファイアウォールのフィルタリングルール、セキュリティサービスの構成パラメータ、暗号鍵管理情報、アクセス制御リストなどがある。認可された職員としては、セキュリティ管理者、システム管理者、システムセキュリティ責任者、システムプログラマ、およびその他の特権ユーザが含まれる。

関連管理策：AC-17, AC-18, AC-19, AU-9, PE-2

(2) 最小特権 | 非セキュリティ機能に関する非特権アクセス

[*設定：組織の定めるセキュリティ機能またはセキュリティ関連情報*]にアクセスできるシステムアカウント（または役割）のユーザが、非セキュリティ機能にアクセスする場合は、非特権アカウントまたは役割を使用することを要求する。

詳解：非セキュリティ機能にアクセスするときに非特権アカウントの使用を要求することで、特権アカウントまたは役割によって操作していることによる露出を制限する。役割を含めることで、組織が役割ベースのアクセス制御などのアクセス制御ポリシーを実装し、役割の変更により特権アカウントと非特権アカウントの間の変更によって提供されるのと同程度の保証がユーザとユーザに代わって動作するプロセスのアクセス認可の変更に提供される状況に対処する。

関連管理策：AC-17, AC-18, AC-19, PL-4

(3) 最小特権 | 特権コマンドへのネットワークアクセス

[*設定：組織が定める特権コマンド*]へのネットワークアクセスを[*設定：組織が定める強制的な運用ニーズ*]に対してのみ認可し、そのようなアクセスの根拠をシステムセキュリティ計画に文書化する。

詳解：ネットワークアクセスとは、ローカルアクセス（すなわち、ユーザがデバイス側に物理的に存在する）の代わりに、ネットワーク接続を介したあらゆるアクセスのことである。

関連管理策：AC-17, AC-18, AC-19

(4) 最小特権 | 個別の処理ドメイン

ユーザ特権のより細かい設定を可能にするために、個別の処理ドメインを規定する。

詳解：ユーザ特権をよりきめ細かく割り当てるために個別の処理ドメインを規定することには、仮想化技法を使用して仮想マシン内で追加のユーザ特権を許可するとともに、特権を他の仮想マシンまたは基盤となる物理マシンに制限すること、個別の物理ドメインを実装すること、およびハードウェアまたはソフトウェアドメインを分離するメカニズムなどが含まれる。

関連管理策：AC-4, SC-2, SC-3, SC-30, SC-32, SC-39

(5) 最小特権 | 特権アカウント

システム上の特権アカウントを[*設定：組織が定める職員または役割*]に制限する。

詳解：スーパーユーザアカウントを含む特権アカウントは、通常、様々なタイプの市販のオペレーティングシステムのシステム管理者として説明されている。特権アカウントを特定の職員または役割に制限することは、日常のユーザが特権情報または特権機能にアクセスすることを防止する。組織は、主要なパラメータのシステム構成を制御する機能を保持している場合や、リスクを十分に軽減するために必要な場合に限り、特権アカウントを制限するアプリケーションで、ローカルアカウントおよびドメインアカウントに許可されている特権を区別することができる。

関連管理策：IA-2, MA-3, MA-4

(6) 最小特権 | 非組織ユーザによる特権アクセス

非組織ユーザによるシステムへの特権アクセスを禁止する。

詳解：組織のユーザとは、従業員、または組織が従業員と同等の地位にあると見なした個人のことである。組織のユーザには、契約作業者、ゲスト研究者、または他の組織から派遣された個人が含まれる。非組織ユーザとは、組織ユーザではないユーザのことである。従業員と同等の地位を個人に付与するためのポリシーおよび手順には、知る必要があること、市民権、および組織との関係が含まれる。

関連管理策：AC-18, AC-19, IA-2, IA-8

(7) 最小特権 | ユーザ特権のレビュー

(a) [*設定：組織が定める役割またはユーザのクラス*]で設定された特権の必要性を検証するするために、[*設定：組織が定める頻度*]でそのような特権をレビューす

る。

(b) 組織の職務および業務要件を正しく反映するために、必要に応じて、特権を再設定または削除する。

詳解：特定の設定されたユーザ特権の必要性は、組織のミッションおよび事業機能、運用環境、技術、または脅威の変化を反映して、時間とともに変化する可能性がある。設定されたユーザ特権の定期的なレビューは、そのような特権を設定する根拠が有効であり続けるかどうかを判定するために必要である。必要性を再検証できない場合、組織は適切な是正措置を講じる。

関連管理策：CA-7

(8) 最小特権 | コード実行の特権レベル

[*設定：組織が定めるソフトウェア*]が、そのソフトウェアを実行しているユーザよりも高い特権レベルで実行されることを防止する。

詳解：場合によっては、ソフトウェアアプリケーションまたはプログラムは、必要な機能の遂行にはより高い特権で実行することが必要な場合がある。ただし、ソフトウェアの機能や構成によっては、実行に必要な特権が、そのようなアプリケーションまたはプログラムを呼び出す組織のユーザに割り当てられた特権よりも高いレベルである場合、それらのユーザには、割り当てられたものより高い特権が間接的に与えられる場合がある。

関連管理策：なし

(9) 最小特権 | 特権機能使用のロギング

特権機能の実行をロギングする。

詳解：認可されたユーザ、またはシステムアカウントを侵害した認可されていない外部エンティティによる、意図的または非意図的な特権機能の悪用は、深刻かつ継続的な懸念事項であり、組織に重大な有害なインパクトを及ぼす可能性がある。特権機能の使用をロギングして分析することは、このような誤用を検知する方法の 1 つであり、そうすることは、インサイダー脅威や持続的標的型攻撃（APT 攻撃）からのリスクを軽減するのに役立つ。

関連管理策：AU-2, AU-3, AU-12

(10) 最小特権 | 非特権ユーザによる特権機能の実行の禁止

非特権ユーザが特権機能を実行することを防止する。

詳解：特権機能には、実装されたセキュリティまたはプライバシー制御の無効化、回避、変更、システムアカウントの確立、システム完全性チェックの実行、および暗号鍵管理活動の管理などが含まれる。非特権ユーザとは、適切な認可を持たない個人のことである。非特権ユーザからの保護を必要とする特権機能には、侵入検知・防止のメカニズムや悪意のあるコード保護のメカニズムの回避が含まれる。非特権ユーザが特権機能を実行できないようにすることは、AC-3 によって実施される。

関連管理策：なし

参照資料：なし

AC-7 ログオン試行の失敗

管理策：

a. [*設定：組織が定める期間*]の間にユーザが連続して無効なログオンを試行する回数を[*設定：組織が定める数*]に制限する。

b. 試行の失敗回数の最大数を超えた場合は、自動的に[*選択（1 つ以上）：[設定：組織が定める期間]アカウントまたはノードをロックする；管理者によって解除されるまでアカウントまたはノードをロックする；[設定：組織が定める遅延アルゴリズム]に従って次のログオンプロンプトを遅らせる；システム管理者に通知する；他の[設定：組織が定める処理]を行う*]]。

詳解：ログオンがローカル接続で行われるかネットワーク接続で行われるかに関係なく、ログオ

ン試行の失敗を制限し、最大試行回数を超えた場合に後続措置を取る必要性が適用される。サービス拒否（DoS）攻撃の可能性があるため、通常、システムによって開始される自動ロックアウトは一時的なものであり、組織が定める所定の時間が過ぎると自動的に解除される。遅延アルゴリズムが選択される場合、組織は、システムの様々なコンポーネントのケイパビリティに基づいて、それらのコンポーネントに様々なアルゴリズムを採用することができる。ログオン試行の失敗に対する対応は、オペレーティングシステムレベルおよびアプリケーションレベルで実装される場合がある。無効なログオン試行の連続回数が許容回数を超えた場合に実行される可能性のある組織が定める措置には、ユーザ名とパスワードに加えて秘密の質問に答えるようにユーザに促すこと、（完全なロックアウトの代わりに）ユーザのケイパビリティが限定されたロックダウンモードを呼び出す、ユーザが特定のインターネットプロトコル（IP）アドレスからのみログオンできるようにする、自動攻撃を防ぐために CAPTCHA を要求する、または位置、時刻、IP アドレス、デバイス、メディアアクセス制御（MAC）アドレスなどのユーザプロファイルを適用することなどが含まれる。自動システムロックアウトまたは遅延アルゴリズムの実行が可用性の目的をサポートするために実装されていない場合、組織はブルートフォース攻撃を防ぐために他の措置の組み合わせを考慮する。上記に加えて、組織は、ログオン試行の失敗許容回数を超える前に、ユーザに秘密の質問に答えるよう促すことができる。指定された時間が経過した後にアカウントのロックを自動的に解除することは、通常は許可されていない。ただし、運用上のミッションまたは必要性に応じて、例外が必要となる場合がある。

関連管理策：AC-2, AC-9, AU-2, AU-6, IA-5

拡張管理策：

(1) ログオン試行の失敗 | 自動アカウントロック

［撤回：AC-7 に組み込まれた］

(2) ログオン試行の失敗 | モバイルデバイスからの除去または抹消

［*設定：組織が定める数*］連続してデバイスへのログオン試行の失敗の後に［*設定：組織が定める除去（purge）または抹消（wipe）要件および技法*］に基づいて、［*設定：組織が定めるモバイルデバイス*］から情報を除去または抹消する。

詳解：モバイルデバイスは、個人が持ち運べるような小さな形態を有し；物理的な接続なしで動作するように設計されており；ローカルで、取り外し不可、または取り外し可能なデータストレージを所有しており；自給式電源を備えているコンピューティングデバイスである。デバイスの除去または抹消は、組織が定めるログオンの失敗回数が発生したモバイルデバイスにのみ適用される。ログオン先はモバイルデバイスであり、デバイス上のいずれか 1 つのアカウントに対してではない。モバイルデバイス上のアカウントへのログオンに成功すると、ログオンの失敗回数がゼロにリセットされる。デバイス上の情報が十分に強力な暗号化のメカニズムで保護されている場合、除去や抹消は不要な場合がある。

関連管理策：AC-19, MP-5, MP-6

(3) ログオン試行の失敗 | 生体認証の試行の限定

生体認証によるログオン試行の失敗回数を［*設定：組織が定める数*］に制限する。

詳解：生体認証は本質的には確率論的なものである。認証に成功するかどうかは、マッチング性能やプレゼンテーション攻撃検知のメカニズムなど、多くの要因に影響される可能性がある。組織は、組織として定める様々な要素に基づいて、ユーザの適切な試行回数を選択する。

関連管理策：IA-3

(4) ログオン試行の失敗 | 代替認証要素の使用

(a) 組織が定める連続した無効なログオン試行回数を超えた後、最初に用いた認証要素とは異なる［*設定：組織が定める認証要素*］の使用を許可する。

(b) ［*設定：組織が定める期間*］の間に、ユーザが代替要素を使用して、［*設定：組織が定める数*］の連続する無効なログオン試行に限定する。

詳解：代替の認証要素の使用は、可用性の目的をサポートし、不注意にロックアウトされたユーザが追加の認証要素を使用してロックアウトを迂回できるようになる。

関連管理策：IA-3

参照資料：[SP 800-63-3], [SP 800-124]

AC-8 システム使用の通知

管理策：

a. 適用される法律、大統領令、指令、規則、ポリシー、基準、ガイドラインに準拠したプライバシーおよびセキュリティ通知を提供するシステムへのアクセスを許可する前に、[*設定：組織が定めるシステム使用通知メッセージまたはバナー*]をユーザに表示し、次のように述べる。
   1. ユーザは米国政府のシステムにアクセスしている。
   2. システムの使用状況が監視、記録され、監査の対象となる場合がある。
   3. システムの認可されていない使用は禁止されており、刑事罰および民事罰の対象となる場合がある。
   4. システムの使用は、監視および記録に同意することを示す。

b. ユーザが使用条件を確認し、システムへのログオンまたはさらなるアクセスのための明示的な行動をとるまで、通知メッセージまたはバナーを画面に表示する。

c. 公的にアクセス可能なシステムの場合。
   1. 公的にアクセス可能なシステムへのさらなるアクセスを許可する前に、システム使用情報の[*設定：組織が定める条件*]を表示する。
   2. 監視、記録、または監査への参照がある場合は、それらの活動を一般的に禁止しているシステムのプライバシーへの対応と整合性があるものを表示する。
   3. システムの認可された使用法の説明を含める。

詳解：システム使用通知は、個人がシステムにログインする前に表示されるメッセージまたは警告バナーを使用して実装できる。システム使用通知は、人間のユーザとのログオンインタフェースを介したアクセスにのみ使用される。ヒューマンインタフェースが存在しない場合は、通知は必要ない。組織は、リスクアセスメントに基づいて、最初のネットワークログオン後にアプリケーションやその他のシステムリソースにアクセスする際に、二次的なシステム使用通知が必要かどうかを検討する。組織は、組織のニーズとシステムユーザの人口統計に基づいて、複数の言語で表示されるシステム使用通知メッセージまたはバナーを検討。組織は、プライバシー情報交換に関する意見を得るためにプライバシー事務局に相談し、警告バナーのコンテンツの法的審査および承認について法律顧問室（OGC：Office of the General Counsel）または組織の同等の部署に相談する。

関連管理策：AC-14, PL-4, SI-4

拡張管理策：なし

参照資料：なし

AC-9 過去のログオンに関する通知

管理策：システムへのログオンが成功したときに、最後にログオンした日時をユーザに通知する。

詳解：前回のログオンに関する通知は、ヒューマンユーザインタフェースを介したシステムアクセス、および他のタイプのアーキテクチャで発生するシステムへのアクセスに適用される。最後に成功したログオンに関する情報により、ユーザは、提供された日時がユーザの最後のアクセスと一致していないかどうかを認識することができる。

関連管理策：AC-7, PL-4

拡張管理策：

(1) 過去のログオンに関する通知 | 失敗したログオン

ログオン成功時に、前回のログオン成功以降に失敗したログオン試行回数をユーザに通知する。

詳解：前回のログオン成功以降の失敗したログオン試行回数に関する情報により、ユーザは、失敗したログオン試行回数がユーザの実際のログオン試行と一致しているかどうかを認識することができる。

関連管理策：なし

(2) 過去のログオンに関する通知 | 成功したログオンおよび失敗したログオン

[*設定：組織が定める期間*]における[*選択：ログオン成功；ログオン試行の失敗；両方*]の回数をログオン成功時にユーザに通知する。

詳解：規定された期間内のログオン試行の成功および失敗の回数に関する情報により、ユーザは、ログオン試行の回数およびタイプがユーザの実際のログオン試行と一致しているかどうかを認識することができる。

関連管理策：なし

(3) 過去のログオンに関する通知 | アカウント変更の通知

ログオン成功時に、[*設定：組織が定める期間*]中に[*設定：組織が定めるユーザアカウントのセキュリティ関連の特性またはパラメータ*]が変更されたことをユーザに通知する。

詳解：規定された期間内のセキュリティ関連のアカウント特性の変更に関する情報により、ユーザは知らない間に変更が行われたかどうかを認識できる。

関連管理策：なし

(4) 過去のログオンに関する通知 | 追加のログオン情報

ログオンが成功した場合、[*設定：組織が定める追加情報*]をユーザに通知する。

詳解：組織は、ログオン時にユーザに提供する追加情報として、最後にログオンした位置などを指定できる。ユーザの位置は、ネットワークログオンが発生したインターネットプロトコル（IP）アドレス、ローカルログオンの通知、デバイス識別子など、システムによって判別できる情報として規定される。

関連管理策：なし

参照資料：なし

AC-10 同時セッション制御

管理策：[*設定：組織が定めるアカウントおよび／またはアカウントタイプ*]ごとの同時セッション数を[*設定：組織が定める数*]に制限する。

詳解：組織は、システムアカウントの最大同時セッション数を、アカウントのタイプ、アカウント、またはそれらの任意の組み合わせによって、包括的に規定できる。例えば、組織は、システム管理者や、特に機微ドメインや失敗や中断が許されない基幹業務システムにおけるアプリケーションで作業する他の個人の同時セッション数を制限する場合がある。同時セッション制御は、システムアカウントの同時セッションに対応する。ただし、複数のシステムアカウントを介した単一ユーザによる同時セッションには対応しない。

関連管理策：SC-23

拡張管理策：なし

参照資料：なし

AC-11 デバイスロック

管理策：

a. [*選択(1 つ以上):システムの[設定:組織が定める期間]の非アクティブ状態の後にデバイスロックを起動すること;システムを離れる前に、ユーザにデバイスロックを起動することを要求すること*]により、システムへのさらなるアクセスを防止する。

b. ユーザが定められた識別および認証手順を使用してアクセスを再確立するまで、デバイスロックを保持する。

詳解:デバイスロックは、ユーザが作業を停止して、組織のシステムのすぐ近くから離れたが、一時的な不在のためにログアウトしたくない場合に使用される、組織のシステムへの論理的なアクセスを防ぐために行われる一時的な措置である。デバイスロックは、オペレーティングシステムレベルまたはアプリケーションレベルで実装できる。近接ロックを使用して、デバイスロックを起動することができる(例えば、Bluetooth 対応デバイスまたはドングルを介して)。ユーザが起動するデバイスロックは動作またはポリシーベースであるため、ユーザはデバイスのロックを起動するために物理的な措置をとる必要がある。なおデバイスロックは、組織がユーザに就業日の終わりにログアウトすることを要求する場合など、システムからのログアウトの代替としては容認できない。

関連管理策:AC-2, AC-7, IA-11, PL-4

拡張管理策:

(1) デバイスロック | パターン表示による隠蔽

以前にディスプレイ上に表示されていた情報を、デバイスのロックを介して、公開されている画像で秘匿する。

詳解:パターン表示による隠蔽には、スクリーンセーバーで使用されるパターン、写真画像、単色、時計、バッテリー寿命インジケータ、または管理対象非機密情報(CUI)が表示されないという警告のある空白の画面などの静的または動的な画像を含めることができる。

関連管理策:なし

参照資料:なし

AC-12 セッションの終了

管理策:[*設定:組織が定める条件またはセッションの切断を必要とする契機となるイベント*]により、ユーザセッションを自動的に終了する。

詳解:セッションの終了は、ユーザが開始した論理セッションの終了に対処するものである(SC-10 は、通信セッションに関連するネットワーク接続の終了(つまり、ネットワークの切断)に対処している)。論理セッション(ローカル、ネットワーク、およびリモートアクセス用)は、ユーザ(またはユーザに代わって動作するプロセス)が組織のシステムにアクセスするたびに開始される。このようなユーザセッションは、ネットワークセッションを終了せずに終了できる。セッションの終了は、ユーザ(つまり、セッションオーナー)がセッションの終了後に続行するために特別に作成したプロセスを除いて、ユーザの論理セッションに関連付けられたすべてのプロセスを終了させる。セッションの自動終了を必要とする条件または契機となるイベントには、組織が定めるユーザの非アクティブな期間、特定のタイプのインシデントを対象とした対応措置、またはシステムの使用に関する時刻の制限が含まれる。

関連管理策:MA-4, SC-10, SC-23

拡張管理策:

(1) セッションの終了 | ユーザ起動ログアウト

[*設定:組織が定める情報リソース*]へのアクセスに認証が使用される場合は常に、ユーザが開始した通信セッションにログアウトケイパビリティを提供する。

詳解:ユーザが認証を介してアクセスできる情報リソースには、ローカルワークステーション、データベース、パスワードで保護されたウェブサイトまたはウェブベースのサービスなどがある。

関連管理策:なし

(2) セッションの終了 | 終了メッセージ

認証された通信セッションの終了を示す明示的なログアウトメッセージをユーザに表示する。

詳解：ウェブアクセスのログアウトメッセージは、認証されたセッションが終了した後に表示することができる。ただし、ファイル転送プロトコル（FTP）セッションを含む特定のタイプのセッションの場合、システムは通常、セッションを終了する前に、ログアウトメッセージを最終メッセージとして送信する。

関連管理策：なし

(3) セッションの終了 | タイムアウト警告メッセージ

[*設定：組織が定めるセッション終了までの時間*]にセッションが終了することを示す明示的なメッセージをユーザに表示する。

詳解：ユーザビリティを向上させるために、保留中のセッションの終了をユーザに通知し、ユーザにセッションの続行を促す。保留中のセッション終了時間は、AC-12 の基本管理策で定められたパラメータに基づいている。

関連管理策：なし

参照資料：なし

AC-13 監視およびレビュー — アクセス制御

[撤回：AC-2 および AU-6 に組み込まれた]

AC-14 識別または認証なしに許可される処理

管理策：

a. 組織のミッションおよび事業機能と整合性のある識別または認証なしでシステム上で実行できる[*設定：組織が定めるユーザ行為*]を規定する。

b. 識別や認証を必要としないユーザ行為について、システムのセキュリティ計画で文書化し、裏付けとなる根拠を提供する。

詳解：特定のユーザ行為に識別と認証が必要でないと組織が判断した場合、特定のユーザ行為は、識別または認証なしで許可される場合がある。組織は、個人が公開ウェブサイトまたは他の公的アクセス可能な連邦政府システムにアクセスするときや、個人が携帯電話を使用して電話を受信するとき、またはファクシミリを受信するときなど、識別または認証なしに限定された数のユーザ行為を許可することができる。組織は、通常は識別または認証を必要とする行為を特定するが、特定の状況下では、識別または認証のメカニズムを迂回できる処理を許可することができる。そのような迂回には、例えば、ログオン機能の迂回を命令し、偶発的または監視されていない利用から保護される、ソフトウェア読み取り可能な物理スイッチを介して発生する可能性がある。識別または認証なしに処理を許可することは、識別および認証がすでに行われており、それが繰り返されていない状況には適用されることはないが、識別および認証がまだ行われていない状況には適用される。組織は、識別と認証なしに組織のシステムで実行できるユーザ行為がないと判断することがあるので、設定操作の値は「なし（none）」になる可能性がある。

関連管理策：AC-8, IA-2, PL-2

拡張管理策：なし

(1) 識別または認証なしに許可される処理 | 必要な使用法

[撤回：AC-14 に組み込まれた]

参照資料：なし

AC-15 自動マーキング

[撤回：MP-3 に組み込まれた]

AC-16 セキュリティおよびプライバシー属性

管理策：

a. 保存中、処理中、および／または伝送中の情報について、[*設定：組織が定めるセキュリティおよびプライバシーの属性タイプ*]を[*設定：組織が定めるセキュリティおよびプライバシー属性の値*]に関連付けるための手段を規定する。

b. 属性の関連付けが行われ、情報とともに保持されていることを確実にする。

c. [*設定：組織が定めるシステム*]向けに AC-16a で規定された属性から、許可された[*設定：組織が定めるセキュリティおよびプライバシー属性*]を定める。

d. 規定された各属性について、[*設定：組織が定める属性の属性値または範囲*]を決定する。

e. 属性の変更を監査する。

f. [*設定：組織が定めるセキュリティおよびプライバシー属性*]の適用可能性について[*設定：組織が定める頻度*]でレビューする。

詳解：情報は、データ構造と呼ばれる抽象概念を使用して、システム内で内部的に表現される。内部データ構造は、アクティブとパッシブの両方の異なるタイプのエンティティを表すことができる。サブジェクトとも呼ばれるアクティブなエンティティは、通常、個人、デバイス、または個人に代わって動作するプロセスに関連付けられる。また、オブジェクトとも呼ばれるパッシブなエンティティは、通常、レコード、バッファ、テーブル、ファイル、プロセス間パイプ、通信ポートなどのデータ構造に関連付けられる。メタデータの一形式であるセキュリティ属性は、情報の保全に関するアクティブおよびパッシブなエンティティの基本的な特性または特徴を表す抽象概念である。プライバシー属性は、独立して、またはセキュリティ属性と併せて使用され、個人情報の管理に関するアクティブまたはパッシブなエンティティの基本的な特性または特徴を表す。属性は、組織のシステムまたはシステムコンポーネントに含まれる情報に明示的または暗黙的に関連付けることができる。

属性は、情報を送受信したり、オブジェクト間で情報を流したり、システム状態を変更したりする可能性のあるアクティブなエンティティ（つまり、サブジェクト）に関連付けることができる。これらの属性は、情報を含む、または受け取るパッシブなエンティティ（すなわち、オブジェクト）に関連付けられることもある。システムによるサブジェクトおよびオブジェクトへの属性の関連付けはバインディングと呼ばれ、属性値および属性タイプの設定を含む。属性は、データまたは情報にバインディングされると、データ保持規制、個人情報の使用の許可、およびデータオブジェクト内の個人情報の識別など、アクセス制御および情報フロー制御のためのセキュリティおよびプライバシーポリシーを実施を可能にする。これらの適用は、組織のプロセスまたはシステムの機能あるいはメカニズムを通じて行われる。システムによって実装されるバインディング技法は、情報への属性のバインディング強度に影響を与える。バインディング強度およびバインディング技法に関連する保証は、組織が情報フローの実施プロセスにおいて持つ信頼性に重要な役割を果たす。バインディング技法は、組織が必要とする追加レビューの回数および程度に影響を与える。属性の内容または設定された値は、個人が組織の情報にアクセスする能力に直接影響を与える可能性がある。

組織は、ミッションまたは事業機能をサポートするシステムに必要な属性のタイプを規定できる。セキュリティ属性には、多くの値を設定することができる。組織は、許可された属性の範囲と値を指定することで、属性値を意味があり関連性があるものであることを保証する。ラベル付けとは、システム内の内部データ構造によって表されるサブジェクトおよびオブジェクトと属性を関連づけることである。これにより、情報セキュリティおよびプライバシーポリシーのシステムベースでの実施が容易になる。ラベルには、法的要件およびコンプライアンス要件（機密、極秘、秘、管理対象非機密など）に従った情報の機密性区分、情報へのインパクトレベル；価値の高い資産情報、アクセス認可、国籍；データのライフサイクル保護（すなわち、暗号化およびデータの有効期限）、個人情報の取扱いへの個人の同意を含む個人情報の取扱い権限、および契約作業者の所属などが含まれる。ラベル付けに関連する用語に、マーキングがある。マーキングとは、人間が読める形式でオブジェクトと属性を関連付け、システム媒体に表示することを指

す。マーキングにより、情報セキュリティおよびプライバシーポリシーを手作業、手続型、またはプロセスベースで実施することが可能になる。セキュリティラベルとプライバシーラベルは、(例えば、機密、極秘、秘)など媒体へのマーキングと同じ値を持つ場合がある。MP-3(媒体へのマーキング)参照。

関連管理策: AC-3, AC-4, AC-6, AC-21, AC-25, AU-2, AU-10, MP-3, PE-22, PT-2, PT-3, PT-4, SC-11, SC-16, SI-12, SI-18

拡張管理策:

(1) セキュリティおよびプライバシー属性 | 動的属性関連付け

情報が作成されたり結合されたりする際に、[*設定:組織が定めるセキュリティおよびプライバシーポリシー*]に従って、セキュリティおよびプライバシー属性を[*設定:組織が定めるサブジェクトおよびオブジェクト*]に動的に関連付ける。

詳解:属性の動的な関連付けは、情報のセキュリティまたはプライバシーの特性が経時的に変化する場合には適切である。属性は、情報集約の問題(すなわち、個々のデータ要素の特性がそれらが結合された要素とは異なる)、個々のアクセス認可(すなわち、権限)の変更、情報のセキュリティカテゴリーの変更、またはセキュリティやプライバシーポリシーの変更などにより変更される場合がある。属性は状況に応じて変化する可能性もある。

関連管理策:なし

(2) セキュリティおよびプライバシー属性 | 認可された個人による属性値の変更

認可された個人(または個人に代わって動作するプロセス)に、関連するセキュリティおよびプライバシー属性の値を規定または変更するケイパビリティを提供する。

詳解:属性の内容または設定された値は、個人が組織の情報にアクセスする機能に直接影響を与える可能性がある。したがって、システムが属性を作成または変更する能力」を認可された個人に限定できることが重要である。

関連管理策:なし

(3) セキュリティおよびプライバシー属性 | システムによる属性関連付けの維持

[*設定:組織が定めるセキュリティおよびプライバシー属性*]および[*設定:組織が定めるサブジェクトおよびオブジェクト*]との関連付けおよび完全性を維持する。

詳解:サブジェクトおよびオブジェクトに対するセキュリティおよびプライバシー属性の関連付けと整合性を十分に保証し維持することは、属性の関連付けを自動ポリシー処理基盤として使用できることを保証するのに役立つ。セキュリティ構成ファイルなどの特定のアイテムの整合性は、「既知の良好な」ベースラインから逸脱した異常や変更を検知する整合性監視のメカニズムを使用することで維持すつことができる。自動ポリシー処理には、保存期限、アクセス制御の決定、情報フロー制御の決定、情報開示の決定などが含まれる。

関連管理策:なし

(4) セキュリティおよびプライバシー属性 | 認可された個人による属性の関連付け

[*設定:組織が定めるセキュリティおよびプライバシー属性*]を、認可された個人(または個人に代わって動作するプロセス)が[*設定:組織が定めるサブジェクトおよびオブジェクト*]に関連付けるケイパビリティを提供する。

詳解:一般に、システムは、特権ユーザにシステムが定めるサブジェクト(ユーザなど)およびオブジェクト(ディレクトリ、ファイル、ポートなど)にセキュリティおよびプライバシー属性を設定するケイパビリティを提供している。一部のシステムは、一般ユーザがセキュリティおよびプライバシー属性を追加のオブジェクト(例えば、ファイル、電子メール)に設定するための追加のケイパビリティを提供している。認可された個人による属性の関連付けは、設計文書に記載されている。システムによって提供されるサポートには、情報オブジェクトに関連付けるセキュリティおよびプライバシー属性を選択するようユーザに促すこと、規定されたポリシーに基づいて属性で情報を分類する自動のメカニズムを採用すること、または選択したセキュリティおよびプライバシー属性の組み合わせが有効であることを確

認することなどが含まれる。組織は、監査可能なイベントの規定に際し、属性の作成、削除、または変更を検討する。

関連管理策：なし

(5) セキュリティおよびプライバシー属性 | 出力されるオブジェクトへの属性表示

システムが出力装置に伝送する各オブジェクトにセキュリティおよびプライバシー属性を[*設定：組織が定める、人間が可読の、標準的な命名規則*]を用いて人間が可読の形式で表示し、[*設定：組織が定める特別な周知、取り扱い、または配布の指示*]を識別する。

詳解：システム出力には、印刷されたページ、画面、または同等の項目が含まれる。システム出力装置には、プリンタ、ノートパソコン、ビデオディスプレイ、スマートフォン、タブレットなどがある。認可されていない情報の暴露（ショルダーサーフィンなど）のリスクを軽減するために、出力にあたっては、加入者がマスクを解除した場合にのみ完全な属性値を表示する。

関連管理策：なし

(6) セキュリティおよびプライバシー属性 | 属性の関連付けの維持

[*設定：組織が定めるセキュリティおよびプライバシーポリシー*]に従って、[*設定：組織が定めるセキュリティおよびプライバシー属性*]と[*設定：組織が定めるサブジェクトおよびオブジェクト*]との関連付けを維持することを職員に義務付ける。

詳解：属性の関連付けを維持するには、（システムではなく）個々のユーザが、規定されたセキュリティおよびプライバシー属性とサブジェクトおよびオブジェクトとの関連付けを維持する必要がある。

関連管理策：なし

(7) セキュリティおよびプライバシー属性 | 一貫した属性解釈

分散システムコンポーネント間で伝送されるセキュリティおよびプライバシー属性の一貫した解釈を規定する。

詳解：分散システム内の複数のシステムコンポーネント全体にセキュリティポリシーおよびプライバシーポリシーを実施するために、組織は、アクセスの実施とフローの実施の決定に使用されるセキュリティおよびプライバシー属性の一貫した解釈を規定する。組織は、分散システムコンポーネントが、自動化されたアクセスの実施およびフローの実施処理で、一貫した解釈を使用して属性を実装することを保証するための合意書およびプロセスを確立することができる。

関連管理策：なし

(8) セキュリティおよびプライバシー属性 | 関連付けの技法と技術

セキュリティおよびプライバシー属性を情報に関連付ける際に、[*設定：組織が定める技法と技術*]を実装する。

詳解：セキュリティ属性とプライバシー属性をシステム内の情報に関連付けることは、自動化されたアクセスの実施およびフローの実施処理を管理するために重要である。そのような属性の情報への結び付け（すなわち、バインディング）は、異なるレベルの保証を規定する技術および技法を用いて達成することができる。例えば、システムは、ハードウェア装置（ハードウェア信頼基点（roots of trust）とも呼ばれる）で保護された暗号化キーをサポートするデジタル署名を使用して、属性を暗号化して情報に結び付けることができる。

関連管理策：SC-12, SC-13

(9) セキュリティおよびプライバシー属性 | 属性の再設定 ― 付け替えのメカニズム

[*設定：組織が定める技法または手順*]を使用して検証された付け替えのメカニズムによってのみ、情報に関連するセキュリティおよびプライバシー属性を変更する。

詳解：付け替えのメカニズムとは、規定されたポリシーの例外に沿ってデータの機密性について再分類し、ラベルを付け直すことが認可された、信頼できるプロセスである。検証済みの付け替えのメカニズムは、組織が属性の再設定活動に必要なレベルの保証を提供

するために使用される。付け替えのメカニズムが単一の目的かつ機能が限定されていることを確実にすることで、検証が容易になる。セキュリティおよびプライバシー属性の変更はポリシー実施処理に直接影響する可能性があるため、信頼できる付け替えのメカニズムを実装することは、そのようなメカニズムが一貫した正しい動作モードで動作することを保証するために必要である。

関連管理策：なし

(10) セキュリティおよびプライバシー属性 | 認可された個人による属性の構成

認可された個人に、サブジェクトおよびオブジェクトとの関連付けに使用可能なセキュリティおよびプライバシー属性のタイプと値を規定または変更するケイパビリティを提供する。

詳解：セキュリティおよびプライバシー属性の内容または設定された値は、個人が組織の情報にアクセスする能力に直接影響を与える可能性がある。したがって、サブジェクトおよびオブジェクトとの関連付けに使用可能な属性のタイプおよび値を作成または変更する機能を、認可された個人のみに限定できることがシステムにとって重要である。

関連管理策：なし

参照資料：[OMB A-130], [FIPS 140-3], [FIPS 186-4], [SP 800-162], [SP 800-178]

AC-17 リモートアクセス

管理策：

a. 許可されるリモートアクセスの各タイプについて、使用制限、構成／接続要件、および実装ガイダンスを定め、文書化する。

b. そのような接続を許可する前に、システムへのリモートアクセスの各タイプを認可する。

詳解：リモートアクセスとは、インターネットなどの外部ネットワークを介して通信する、組織のシステム（またはユーザに代わって動作するプロセス）へのアクセスである。リモートアクセスのタイプには、ダイヤルアップ、ブロードバンド、ワイヤレスなどがある。組織は、リモート接続の機密性と完全性を向上させるために、暗号化された仮想プライベートネットワーク（VPN）を使用する。暗号化された VPN を使用することで、適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに従って暗号化のメカニズムが実装されている場合、そのような接続を内部ネットワークとして効果的に処理できるという十分な保証を組織に提供する。それでも、VPN 接続は外部ネットワークを通過するため、暗号化された VPN はリモート接続の可用性を向上させることはない。また、暗号化されたトンネルを備えた VPN は、悪意のあるコードのネットワーク通信トラフィックを適切に監視する機能にも影響を与える可能性がある。リモートアクセス制御は、公開ウェブサーバまたはパブリックアクセス用に設計されたシステム以外のシステムに適用される。各リモートアクセスのタイプの認可は、そのような認可の特定の形式を指定せずに、リモートアクセスの許可に先立つ認可に対処する。組織は、他のシステムへのリモートアクセス接続を管理するために、情報交換およびシステム接続セキュリティ合意書を使用することがあるが、そのような合意書は CA-3 の一部として扱われる。リモートアクセスのアクセス制限の実施は、AC-3 を介して対処される。

関連管理策：AC-2, AC-3, AC-4, AC-18, AC-19, AC-20, CA-3, CM-10, IA-2, IA-3, IA-8, MA-4, PE-17, PL-2, PL-4, SC-10, SC-12, SC-13, SI-4

拡張管理策：

(1) リモートアクセス | 監視および制御

リモートアクセス方法を監視および制御する自動化されたメカニズムを採用する。

詳解：リモートアクセス方法の監視および制御により、組織は、サーバ、ノートブックコンピュータ、ワークステーション、スマートフォン、タブレットなどの様々なシステムコンポーネント上のリモートユーザの接続活動を監査することで、攻撃を検知し、リモートアクセスポリシーへの準拠を確保できる。リモートアクセスの監査ロギングは、AU-2 によって実施される。また監査イベントは AU-2a で規定される。

関連管理策：AU-2, AU-6, AU-12, AU-14

(2) リモートアクセス｜暗号化を使用した機密性および完全性の保護

リモートアクセスセッションの機密性と完全性を保護するために暗号化のメカニズムを実装する。

詳解：仮想プライベートネットワークを使用して、リモートアクセスセッションの機密性と完全性を保護することができる。トランスポート層セキュリティ（TLS）は、ネットワーク上でエンドツーエンドの通信セキュリティを提供する暗号化プロトコルの一例であり、インターネット通信やオンライン取引に使用される。

関連管理策：SC-8, SC-12, SC-13

(3) リモートアクセス｜管理されたアクセス制御ポイント

認可され管理されたネットワークアクセス制御ポイントを介してリモートアクセスをルーティングする。

詳解：リモートアクセスのアクセス制御ポイントの数を限定することで攻撃対象領域が減少するため、組織は外部ネットワーク接続について、「信頼できるインターネット接続（TIC：Trusted Internet Connections）イニシアチブ」[DHS TIC]要件を考慮する。

関連管理策：SC-7

(4) リモートアクセス｜特権コマンドおよびアクセス

(a) [*設定：組織が定める必要性*]における評価可能なエビデンスを提供する形式でのみ、リモートアクセスを介した特権コマンドの実行とセキュリティ関連情報へのアクセスを認可する。

(b) システムのセキュリティ計画にリモートアクセスの根拠を文書化する。

詳解：システムへのリモートアクセスは、敵対者によって悪用される可能性のある重大な潜在的脆弱性を意味する。そのため、特権コマンドの実行およびリモートアクセスを介したセキュリティ関連情報へのアクセスを制限することで、組織が外部にさらされる可能性と、リモートアクセスのケイパビリティに対する敵対者の脅威にさらされる可能性を低減することができる。

関連管理策：AC-6, SC-12, SC-13

(5) リモートアクセス｜認可されていない接続の監視

［撤回：SI-4 に組み込まれた］

(6) リモートアクセス｜メカニズムに関する情報の保護

リモートアクセスのメカニズムに関する情報を、認可されていない使用および開示から保護する。

詳解：非組織エンティティによる組織情報へのリモートアクセスは、リモートアクセスのメカニズムに関する情報の認可されていない使用および開示のリスクを増大させる可能性がある。組織は、必要に応じて、他の組織との情報交換に関する協定にリモートアクセス要件を含めることを考慮する。リモートアクセス要件は、行動規則（PL-4 を参照）およびアクセス規約（PS-6 を参照）に含めることもできる。

関連管理策：AT-2, AT-3, PS-6

(7) リモートアクセス｜セキュリティ機能へのアクセスに対する追加的な保護

［撤回：AC-3(10)に組み込まれた］

(8) リモートアクセス｜非セキュアネットワークプロトコルの無効化

［撤回：CM-7 に組み込まれた］

(9) リモートアクセス｜アクセスの切断または無効化

[*設定：組織が定める時間*]内にシステムへのリモートアクセスを切断または無効化するケイパビリティを提供する。

詳解：システムの切断または無効化の迅速性は、ミッションまたは事業機能の重要性、およびシステムへの即時または将来のリモートアクセスを制限する必要性に応じて異なる。

関連管理策：なし

(10) リモートアクセス | リモートコマンドの認証

[*設定：組織が定めるリモートコマンド*]を認証するための[*設定：組織が定めるメカニズム*]を実装する。

詳解：リモートコマンドを認証することで、認可されていないコマンドや認可されたコマンドのリプレイから保護できる。リモートコマンドを認証する機能は、負傷、死亡、物的損害、高価値資産の損失、ミッションまたは事業機能の失敗、国家機密情報または管理対象非機密情報の侵害などの損失、誤動作、誤配、または悪用が即時または深刻な結果をもたらすリモートシステムにとって重要である。リモートコマンドの認証のメカニズムにより、システムが意図した順序でコマンドを受け入れて実行し、認可されたコマンドのみを実行し、認可されていないコマンドを拒否することを保証する。暗号化のメカニズムは、例えば、リモートコマンドを認証するために使用することができる。

関連管理策：SC-12, SC-13, SC-23

参照資料：[SP 800-46], [SP 800-77], [SP 800-113], [SP 800-114], [SP 800-121], [IR 7966]

AC-18 ワイヤレスアクセス

管理策：

a. ワイヤレスアクセスのタイプごとに、構成要件、接続要件、および実装ガイダンスを定める。

b. そのような接続を許可する前に、システムへの各タイプのワイヤレスアクセスを認可する。

詳解：ワイヤレス技術には、マイクロ波、パケット無線（極超短波（UHF）または超短波（VHF））、802.11x、および Bluetooth が含まれる。ワイヤレスネットワークには、オーセンティケータの保護と相互認証を提供する認証プロトコルを使用する。

関連管理策：AC-2, AC-3, AC-17, AC-19, CA-9, CM-7, IA-2, IA-3, IA-8, PL-4, SC-40, SC-43, SI-4

拡張管理策：

(1) ワイヤレスアクセス | 認証および暗号化

[*選択（1 つ以上）：ユーザ；デバイス*]認証および暗号化を使用して、ワイヤレスアクセスからシステムへのアクセスを保護する。

詳解：ワイヤレスネットワーキング・ケイパビリティは、攻撃者によって悪用される可能性のある重大な潜在的脆弱性である。ワイヤレスアクセスポイントを備えたシステムを保護するために、強度の高い暗号化とともにユーザおよびデバイスの高い保証レベルの認証を行うことで、ワイヤレス技術を利用した敵対者の脅威による影響を減らすことができる。

関連管理策：SC-8, SC-12, SC-13

(2) ワイヤレスアクセス | 認可されていない接続の監視

[撤回：SI-4 に組み込まれた]

(3) ワイヤレスアクセス | ワイヤレスネットワーキングの無効化

使用を意図していない場合は、発行および展開の前に、システムコンポーネント内に組み込まれたワイヤレスネットワーキング・ケイパビリティを無効にする。

詳解：システムコンポーネント内に組み込まれているワイヤレスネットワーキング・ケイパビリティは、敵対者によって悪用される可能性のある重大な潜在的脆弱性である。組織の重要な任務やケイパビリティに必要でない場合にワイヤレス機能を無効にすることで、ワイヤレス技術を利用した敵対者の脅威による影響を減らすことができる。

関連管理策：なし

(4) ワイヤレスアクセス｜ユーザによる構成の制限

ワイヤレスネットワーキング・ケイパビリティを個別に構成することを許可されたユーザを識別し、明示的に認可する。

詳解：選択されたユーザがワイヤレスネットワーキング・ケイパビリティを構成できるようにするための組織による認可は、部分的には、組織のシステム内で採用されているアクセス実施のメカニズムによって実施される。

関連管理策：SC-7, SC-15

(5) ワイヤレスアクセス｜アンテナおよび伝送電力レベル

無線アンテナを選択し、伝送電力レベルを調整して、ワイヤレスアクセスポイントからの信号が、組織が管理する境界の外で受信される可能性を低減する。

詳解：組織が管理する境界の外での認可されていないワイヤレス通信の使用を限定するために取ることができる措置には、組織の物理的境界の外部でキャプチャできる信号を発信する可能性が低くなるようにワイヤレス伝送の電力を低減すること、ワイヤレス放射を制御するために放射セキュリティなどの手段を採用すること、および意図しない受信者が信号を傍受できる可能性を低減する指向性アンテナまたはビーム形成アンテナを使用すること、などが含まれる。このような緩和策を講じる前に、組織は定期的なワイヤレス調査を実施することにより、組織のシステムおよびその地域で運用されている可能性のある他のシステムの無線周波数プロファイルを把握することができる。

関連管理策：PE-19

参照資料：[SP 800-94], [SP 800-97]

AC-19 モバイルデバイスのアクセス制御

管理策：

a. 組織が管理するモバイルデバイスについて、管理エリア外にある場合を含め、構成要件、接続要件、および実装ガイダンスを定める。

b. モバイルデバイスの組織のシステムへの接続を認可する。

詳解：モバイルデバイスとは、個人が一人で容易に持ち運べるような小さな形態を持ち；物理的な接続なしで動作するように設計されており；ローカルで取り外し不可または取り外し可能なデータ記憶装置を持ち；自給式電源を有したコンピューティングデバイスである。モバイルデバイスの機能には、音声通信ケイパビリティ、デバイスが情報をキャプチャできるオンボードセンサ、および／または遠隔地のローカルデータと同期させるための内蔵機能なども含まれる場合がある。例として、スマートフォンやタブレットが挙げられる。モバイルデバイスは通常、1 人の個人に関連付けられている。モバイルデバイスの処理、記憶、および伝送するケイパビリティは、デバイスの性質および意図される目的に応じて、ノートブック／デスクトップシステムに匹敵するか、または単に一部分である場合がある。モバイルデバイスの保護と制御は、動作またはポリシーに基づいており、ユーザが管理エリア外にいる場合は、そのようなデバイスを保護および管理するために物理的な措置をとる必要がある。管理エリアとは、組織が情報やシステムを保護するために定められた要件を満たすために、物理的または手続き的な管理を提供する空間のことである。

様々な特性やケイパビリティを持つモバイルデバイスは多種多様であるため、組織の制限は、そのようなデバイスのクラスやタイプによって異なる場合がある。モバイルデバイスの使用制限および具体的な実装ガイダンスには、構成管理、デバイスの識別および認証、必須の保護ソフトウェアの実装、悪意のあるコード検知のためのデバイスのスキャン、ウイルス保護ソフトウェアの更新、重要なソフトウェアの更新とパッチのスキャン、プライマリ OS（および場合によってはその他の常駐ソフトウェア）の整合性チェック、不要なハードウェアの無効化などが含まれる。

使用制限および接続の認可は、組織のシステムによって異なる場合がある。例えば、組織はモバイルデバイスのネットワークへの接続を認可した後、一連の使用制限を課すことがあるが、

システムオーナーはモバイルデバイスのシステムへの接続を許可する前に、モバイルデバイスの特定のアプリケーションへの接続の認可を保留したり、追加の使用制限を課したりする場合がある。モバイルデバイスに関する多くの保全措置は、他の管理策にも反映されている。モバイルデバイスの適切なセキュリティは、AC-19 で指定されている要件を超えている。モバイルデバイスの保全措置の多くは、他の管理策にも反映されている。AC-20 では、組織の管理下にないモバイルデバイスに対応している。

関連管理策：AC-3, AC-4, AC-7, AC-11, AC-17, AC-18, AC-20, CA-9, CM-2, CM-6, IA-2, IA-3, MP-2, MP-4, MP-5, MP-7, PL-4, SC-7, SC-34, SC-43, SI-3, SI-4

拡張管理策：

(1) モバイルデバイスのアクセス制御 | 書き込み可能なポータブルストレージデバイスの使用

［撤回：MP-7 に組み込まれた］

(2) モバイルデバイスのアクセス制御 | 個人所有のポータブルストレージデバイスの使用

［撤回：MP-7 に組み込まれた］

(3) モバイルデバイスのアクセス制御 | 識別可能なオーナーのないポータブルストレージデバイスの使用

［撤回：MP-7 に組み込まれた］

(4) モバイルデバイスのアクセス制御 | 国家機密情報の制限

(a) 認可権限のある担当者が特に許可しない限り、国家機密情報を処理、保存、または伝送するシステムを含む施設で、非機密モバイルデバイスを使用することを禁止する。

(b) 国家機密情報を処理、保存、または伝送するシステムを扱う施設で非機密モバイルデバイスを使用する認可権限のある担当者により許可された個人に対して、以下の制限を実施する。

(1) 非機密モバイルデバイスの国家機密情報を扱うシステムへの接続の禁止。

(2) 非機密モバイルデバイスを非機密情報を扱うシステムに接続するには、認可権限のある担当者の承認が必要。

(3) 非機密モバイルデバイスの内蔵または外付けのモデムまたは無線インタフェースの使用は禁止される。

(4) 非機密モバイルデバイスおよびそれらのデバイスに保存された情報は、[*設定：組織が定めるセキュリティ担当者*]による不定期なレビュー、および検査の対象となり、国家機密情報が検出された場合は、インシデント対応ポリシーに従う。

(c) [*設定：組織が定めるセキュリティポリシー*]に従って、国家機密情報を扱うモバイルデバイスの国家機密情報を扱うシステムへの接続を制限する。

詳解：なし

関連管理策：CM-8, IR-4

(5) モバイルデバイスのアクセス制御 | デバイス全体またはコンテナ単位の暗号化

[*設定：組織が定めるモバイルデバイス*]上の情報の機密性と完全性を保護するために[*選択：デバイス全体の暗号化；コンテナ単位の暗号化*]を採用する。

詳解：コンテナ単位の暗号化は、ファイル、レコード、フィールドなどの選択されたデータ構造への暗号化など、モバイルデバイス上のデータおよび情報の暗号化について、よりきめの細かいアプローチを提供できる。

関連管理策：SC-12, SC-13, SC-28

参照資料: [SP 800-114], [SP 800-124]

AC-20 外部システムの使用

管理策:

a. 外部システムを所有、運用、および／または維持する他の組織と確立された信頼関係と一致する[*選択(1 つ以上):[設定:組織が定める契約条件]を定め;[設定:組織が定める外部システムに実装するように強く求められる管理策]を識別し*]、認可された個人が以下を行えるようにする。

1. 外部システムからシステムへアクセスする。
2. 外部システムを使用して、組織が管理する情報を処理、保存、または伝送する。または、

b. [*設定:組織が定める外部システムのタイプ*]の使用を禁止する。

詳解:外部システムとは、組織のシステムによって使用されてはいるが、その一部ではないシステムであり、組織は必要な管理策の実施または管理策の有効性のアセスメントについては直接管理していない。外部システムには、個人所有のシステム、コンポーネント、またはデバイス;商業施設または公共施設における民間所有のコンピューティングおよび通信デバイス;非連邦政府組織によって所有または管理されているシステム;契約事業者によって管理されているシステム;および、連邦政府組織が所有していない、運営していない、または直接の監督または権限下にない、連邦政府情報システムなどが含まれる。外部システムには、同じ組織内の他の部署によって所有または運用されているシステムや、同組織内の認可の境界が異なるシステムも含まれる。組織には、あらゆるタイプの外部システムの使用を禁止するか、特定のタイプの外部システムの使用を禁止するかの選択肢がある(例えば、組織が所有していない外部システムの使用を禁止したり、個人所有のシステムの使用を禁止したりする)。

一部の外部システム(すなわち、他の組織によって運用されるシステム)では、それらの組織と依頼元組織との間に確立されている信頼関係には、明示的な契約条件を必要としない場合がある。これらの組織内のシステムは外部とは見なされない場合もある。このような状況は、例えば、組織またはコンポーネント間で既存の情報交換合意書(暗黙的または明示的)が確立されている場合、またはそのような合意書が適用される法律、大統領令、指令、規則、ポリシー、または基準によって規定されている場合に生ずる。認可された個人には、組織の職員、契約作業者、または組織のシステムへのアクセス権を持つその他の個人が含まれ、組織はシステムへのアクセスに関する特定の行動規則を課す権限を有する。組織が認可された個人に課す制限は、組織間の信頼関係によって制限が異なる場合があるため、一律である必要はない。したがって、組織は、契約作業者に対して州政府、地方政府、または部族政府とは異なるセキュリティ制限を課すことを選択する場合がある。

組織のシステムの公開インタフェースにアクセスするために使用される外部システムは、AC-20 の範囲外である。組織は、組織のセキュリティポリシーおよび手順に従って、外部システムの使用に関する特定の契約条件を定める。少なくとも、契約条件は、外部システムから組織のシステムにアクセスできる特定のタイプのアプリケーションと、外部システムで処理、保存、または伝送できる最も高いセキュリティ分類の情報に対処する。外部システムのオーナーとの契約条件を確立できない場合、組織はそれらの外部システムを使用する組織の職員に制限を課すことができる。

関連管理策: AC-2, AC-3, AC-17, AC-19, CA-3, PL-2, PL-4, SA-9, SC-7

拡張管理策:

(1) 外部システムの使用 | 認可された使用に限定

以下の場合のみ、認可された個人が外部システムを使用してシステムにアクセスし、組織が管理する情報を処理、保存、または伝送することを許可する。

(a) 組織のセキュリティおよびプライバシーポリシーならびにセキュリティおよびプライバシー計画で規定されている外部システムに対する管理策の実装の検証。または、

(b) 外部システムをホストしている組織のエンティティとの承認されたシステム接続または処理に関する合意書の保持。

詳解：認可された使用を制限することにより、外部システムを使用する個人が組織のシステムにアクセスする必要性のある状況を認識できる。組織は、組織のシステムを侵害したり、損傷したり、その他の形で害を与えたりしないように、外部システムに必要な管理策が含まれていることを保証する必要がある。必要な管理策が実装されていることの検証は、組織が必要とする信頼性のレベルに応じて、外部の独立したアセスメント、証明、またはその他の手段によって達成することができる。

関連管理策：CA-2

(2) 外部システムの使用 | ポータブルストレージデバイス — 使用制限

[*設定：組織が定める制限*]を適用して、認可された個人による組織が管理するポータブルストレージデバイスの外部システム上での使用を制限する。

詳解：外部システムでの組織管理のポータブルストレージデバイスの使用に関する制限には、デバイスの使用方法およびデバイスの使用条件に関する制限が含まれる。

関連管理策：MP-7, SC-41

(3) 外部システムの使用 | 組織が所有していないシステム — 使用制限

[*設定：組織が定める制限*]を使用して、組織の情報を処理、保存、または伝送するための、組織が所有していないシステムまたはシステムコンポーネントの使用を制限する。

詳解：組織が所有していないシステムまたはシステムコンポーネントには、他の組織が所有するシステムまたはシステムコンポーネントだけでなく、個人所有のデバイスも含まれる。組織が所有していないシステムまたはコンポーネントを使用することには、潜在的なリスクがある。場合によっては、そのような使用を禁止しなくてはならないほどにリスクが高いことがある（AC-20 b を参照）。他の場合では、そのようなシステムまたはシステムコンポーネントの使用は許可されるが、何らかの方法で制限される場合がある。制限には、組織が所有していないシステムおよびコンポーネントの接続を認可する前に、承認された管理策の実装を要求すること；情報、サービス、またはアプリケーションのタイプによりアクセスを制限すること；仮想化技術を使用して、処理および保存行為を、組織によって利用可能な状態にされたサーバまたはシステムコンポーネントに限定すること；使用契約に同意することなどが含まれる。組織は、インシデント後の調査中にフォレンジック分析を実施するための要件など、個人所有のデバイスの使用に関連する法的問題について、法律顧問室（OGC）に相談する。

関連管理策：なし

(4) 外部システムの使用 | ネットワークアクセス可能なストレージデバイス — 使用禁止

外部システムにおける[*設定：組織が定めるネットワークアクセス可能なストレージデバイス*]の使用を禁止する。

詳解：外部システムのネットワークアクセス可能なストレージデバイスには、パブリック、ハイブリッド、またはコミュニティのクラウドベースのシステムにおけるオンラインストレージデバイスが含まれる。

関連管理策：なし

(5) 外部システムの使用 | ポータブルストレージデバイス — 使用禁止

認可された個人が、組織が管理するポータブルストレージデバイスを外部システム上で使用することを禁止する。

詳解：組織が管理するポータブルストレージデバイスの外部システムにおける使用に関する制限には、そのようなデバイスの使用を完全に禁止することが含まれる。そのような使用の禁止は、技術的方法および／または非技術的（すなわち、プロセスベースの）方法を使用して実施される。

関連管理策：MP-7, PL-4, PS-6, SC-41

参照資料: [FIPS 199], [SP 800-171], [SP 800-172]

AC-21 情報共有

管理策:

a. 共有パートナーに設定されたアクセス認可が、[*設定:組織が定めるユーザの裁量が必要な情報共有の状況*]における情報のアクセスおよび使用制限に一致するかどうかを、認可されたユーザが判定できるようにする。

b. ユーザが情報共有およびコラボレーションの決定を行うことを支援するために、[*設定:組織が定める自動化のメカニズムまたは手動によるプロセス*]を採用する。

詳解:情報共有は、何らかの正式なあるいは管理的な意思決定に基づいて何らかの方法で制限される可能性のある情報に対して適用される。そのような情報の例には、契約上の機微情報、特別なアクセスプログラムまたはコンパートメントに関連する国家機密情報、特権情報、専有情報、および個人情報などが含まれる。セキュリティおよびプライバシーのリスクアセスメント、ならびに適用される法律、規則、およびポリシーは、これらの意思決定に有用な情報を提供することができる。状況に応じて、情報共有を行うパートナーは、個人、グループ、または組織のレベルで規定されることもある。情報は、コンテンツ、タイプ、セキュリティ分類、または特別なアクセスプログラムまたはコンパートメントによって規定される場合がある。アクセス制限には、秘密保持契約書(NDA)が含まれる場合がある。情報フロー技法およびセキュリティ属性は、情報共有およびコラボレーションの判断を行うユーザに自動化された支援を提供するために使用することができる。

関連管理策: AC-3, AC-4, AC-16, PT-2, PT-7, RA-3, SC-15

拡張管理策:

(1) 情報共有 | 自動化された意思決定支援

共有パートナーのアクセス認可と共有される情報のアクセス制限に基づいて、認可されたユーザによる情報共有を意思決定するために[*設定:組織が定める自動化のメカニズム*]を採用する。

詳解:自動化されたメカニズムは、情報共有の意思決定を行うために使用される。

関連管理策:なし

(2) 情報共有 | 情報調査および検索

[*設定:組織が定める情報共有制限*]を実施する情報調査および検索サービスを実装する。

詳解:情報調査および検索サービスは、情報ニーズに関連する情報システムリソースを識別する。

関連管理策:なし

参照資料: [OMB A-130], [SP 800-150], [IR 8062]

AC-22 公的にアクセス可能なコンテンツ

管理策:

a. 情報を公的にアクセス可能にすることを認可された個人を指定する。

b. 公的にアクセス可能な情報に非公開情報が含まれていないことを確実にするために、認可された個人をトレーニングする。

c. 非公開情報が含まれていないことを確実にするために、公的にアクセス可能なシステムに投稿する前に情報の、提案された内容をレビューする。

d. 公的にアクセス可能なシステムのコンテンツに非公開情報が含まれていないか[*設定:組織が定める頻度*]でレビューを行い、検出された場合は、そのような情報を削除する。

詳解：適用される法律、大統領令、指令、ポリシー、規則、基準、およびガイドラインに従って、[PRIVACT]で保護されている情報や機密情報を含む非公開情報に一般市民がアクセスすることは認可されていない。公的にアクセス可能なコンテンツは、組織によって管理され、一般的には識別や認証なしで公的にアクセス可能なシステムを対象としている。組織外のシステム（例えば、組織外の公開ウェブサイト、フォーラム、ソーシャルメディアなど）への情報の投稿は、組織のポリシーが適用される。組織には、公的にアクセス可能にすることができる情報に関するポリシーの策定および実装に責任を負う個人がいる場合があるが、公的にアクセス可能なコンテンツは、そのような情報を公的にアクセス可能にする個人の管理を対象としている。

関連管理策：AC-3, AT-2, AT-3, AU-13

拡張管理策：なし

参照資料：[PRIVACT]

AC-23 データマイニングの保護

管理策：認可されていないデータマイニングを検知し保護するために、[*設定：組織が定めるデータ記憶オブジェクト*]に[*設定：組織が定めるデータマイニングの防止および検知技法*]を採用する。

詳解：データマイニングとは、データまたは知識の発見を目的として、大規模なデータセット内の相関関係またはパターンを見つけようとする分析プロセスである。データストレージオブジェクトには、データベースレコードとデータベースフィールドが含まれる。機微情報は、データマイニングの操作から抽出できる。情報が個人情報である場合、個人に関する予期せぬ暴露につながり、プライバシーリスクを引き起こす可能性がある。組織は、データマイニング活動を実行する前に、そのような活動が認可されているかどうかを判定する。組織は、データマイニングの要件に対処する適用法、大統領令、指令、規則、またはポリシーの対象となる場合がある。組織の担当者は、そのような要件に関する政府機関のプライバシー保護責任者および法律顧問に相談する。

データマイニングの防止および検知技法には、データベースの内容を判定するために必要な作業要因を増やすために、データベースのクエリの数と頻度を制限すること、データベースのクエリに対して提供される応答のタイプを制限すること、差分プライバシー技法または準同型暗号化を適用すること、およびデータベースの非定形的な処理要求またはアクセスが発生した場合に職員に通知することなどが含まれる。データマイニングの保護は、情報が組織のデータストアに存在する間、データマイニングから情報を保護することに重点を置いている。対照的に、AU-13 は、データストアからマイニングまたは取得された可能性のある組織情報の監視に重点を置いており、ソーシャルネットワーキングやソーシャルメディアのウェブサイトなどの外部サイトにあるオープンソース情報として利用できる。

[EO 13587]は、機微情報を悪用、侵害、またはその他の認可されていない開示からの保全することを含む、インサイダー脅威を阻止、検知、および軽減するためのインサイダー脅威プログラムの確立を要求している。データマイニングの保護では、組織が、不要なまたは認可されていないデータマイニングを防止および検知するための適切な技法を識別する必要がある。データマイニングは、インサイダーが漏出を目的として組織情報を収集するために利用される可能性がある。

関連管理策：PM-12, PT-2

拡張管理策：なし

参照資料：[EO 13587]

AC-24 アクセス制御の決定

管理策：[*設定：組織が定めるアクセス制御の決定*]がアクセス実施前に各アクセス要求に適用されることを確実にするために、[*選択：手順を確立；メカニズムを実装*]する。

詳解：アクセス制御の決定（認可の決定とも呼ばれる）は、認可情報が特定のアクセスに適用さ

れるときに生ずる。対照的に、アクセスの実施は、システムがアクセス制御の決定を実施するときに発生する。アクセス制御の決定とアクセスの実施を同じエンティティで実装することは一般的であるが、これは必須ではなく、常に最適な実装の選択であるとは限らない。一部のアーキテクチャおよび分散システムでは、異なるエンティティがアクセス制御の決定を行い、アクセスを実施する場合がある。

関連管理策: AC-2, AC-3

拡張管理策:

(1) アクセス制御の決定 | アクセス認可情報の伝送

アクセス制御の決定を実施する[*設定:組織が定めるシステム*]に、[*設定:組織が定めるアクセス認可情報*]を、[*設定:組織が定める制御*]を使用して伝送する。

詳解: 認可プロセスおよびアクセス制御の決定は、システムの別の部分または別のシステムで行われる場合がある。そのような場合、認可情報は(例えば、暗号化のメカニズムを使用して)セキュアに伝送され、適切な場所でタイムリーなアクセス制御の決定を実施することができる。アクセス制御の決定をサポートするために、セキュリティおよびプライバシーの属性を、サポートするアクセス認可情報の一部として伝送することが必要な場合がある。これは、分散システムでは、様々なアクセス制御の決定を行う必要があり、様々なエンティティがこれらの決定を一連の方法で行うため、それぞれの決定にこれらの属性が必要になるためである。アクセス認可情報を保護することにより、そのような情報が伝送中に変更、偽装、または侵害されないようにすることができる。

関連管理策: AU-10

(2) アクセス制御の決定 | ユーザまたはプロセスのアイデンティティが無い場合

[*設定:組織が定めるセキュリティまたはプライバシー属性*]に基づいて、ユーザまたはユーザに代わって動作するプロセスのアイデンティティを含まないアクセス制御の決定を行う。

詳解: 特定の状況では、リクエストを発行するユーザのアイデンティティに関する情報なしにアクセス制御の決定を行うことが重要である。これらは一般的に、個人のプライバシーを保護することが最も重要な場合である。他の状況では、ユーザ識別情報は単にアクセス制御の決定に必要ではなく、特に分散システムの場合には、求められる保証レベルでそのような情報を伝送することは、非常に費用がかかるか、実現が困難な場合がある。例えば、MAC、RBAC、ABAC、およびラベルベースの制御ポリシーには、ユーザアイデンティティが属性として含まれていない場合がある。

関連管理策: なし

参照資料: [SP 800-162], [SP 800-178]

AC-25 リファレンスモニタ

管理策: 耐タンパー性があり、常に起動され、分析とテストの対象となるほど十分に小さく、完全性が保証される、[*設定:組織が定めるアクセス制御ポリシー*]のためのリファレンスモニタを実装する。

詳解: リファレンスモニタは、オペレーティングシステムの重要なコンポーネントとして、すべてのサブジェクトとオブジェクトに対してアクセス制御ポリシーを実施する、リファレンス検証メカニズムに関する一連の設計要件である。リファレンス検証メカニズムは常に起動され、耐タンパー性があり、分析とテストの対象となるほど十分小さいため、その完全性を保証できる(つまり、検証可能である)。情報は、データ構造と呼ばれる抽象化を使用して、システム内で内部的に表現される。内部データ構造は、アクティブおよびパッシブの両方の異なるタイプのエンティティを表すことができる。サブジェクトとも呼ばれるアクティブなエンティティは、個人、デバイス、または個人に代わって動作するプロセスに関連付けられる。オブジェクトとも呼ばれるパッシブなエンティティは、レコード、バッファ、通信ポート、テーブル、ファイル、プロセス間パイプなどのデータ構造に関連付けられる。リファレンスモニタは、サブジェクトまたはサブジェクトが属するグループのアイデンティティに基づいてオブジェクトへのアクセスを制限するアクセス制御ポリシ

ーを実施する。システムは、ポリシーによって確立されたルールセットに基づいてアクセス制御ポリシーを実施する。リファレンスモニタの耐タンパー性は、判別された敵対者がリファレンス検証メカニズムの機能を侵害することを防止する。また常に起動されるという特性は、敵対者がメカニズムを迂回してセキュリティポリシーに違反することを防止する。十分に小さいという特性は、セキュリティポリシーの実施を妨げるあらゆる弱点または欠陥（つまり、潜在的な欠陥）を検知するメカニズムの分析とテストの完全性を確保するのに役立つ。

関連管理策：AC-3, AC-16, SA-8, SA-17, SC-3, SC-11, SC-39, SI-13

拡張管理策：なし

参照資料：なし

3.2 意識向上およびトレーニング

意識向上およびトレーニングの要約表へのクイックリンク

AT-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。

1. 以下の[*選択(1 つ以上):組織レベル;ミッション／事業プロセスレベル;システムレベル*]の意識向上およびトレーニングのポリシー。

(a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、および準拠への対処。

(b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインとの整合性。

2. 意識向上およびトレーニングのポリシーと関連する意識向上およびトレーニングの管理策の実装を促進するための手順。

b. 意識向上およびトレーニングのポリシーと手順の策定、文書化、および配布することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行の意識向上およびトレーニングをレビューし、更新する。

1. ポリシーは[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]の後で。

2. 手順は[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]の後で。

詳解:意識向上およびトレーニングのポリシーと手順は、システムおよび組織内で実装される AT ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に貢献する。したがって、セキュリティおよびプライバシープログラムが連携して、意識向上およびトレーニングのポリシーと手順を策定することが重要である。一般的には、セキュリティおよびプライバシープログラムのポリシーと手順を組織レベルで確立することは望ましく、ミッションまたはシステム固有のポリシーと手順の必要性をなくすことができる場合がある。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映した複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムに対して規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述し、手順の対象である個人または役割に対して指示することができる。手順は、システムのセキュリティおよびプライバシー計画の中で文書化することもできるし、1 つ以上の個別の文書で文書化することもできる。意識向上およびトレーニングのポリシーと手順の更新を促す可能性のあるイベントには、アセスメントまたは監査の結果、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれる。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策:PM-9, PS-8, SI-12

拡張管理策:なし

参照資料:[OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-50], [SP 800-100]

AT-2 リテラシートレーニングおよび意識向上

管理策:

a. システムユーザ(管理職、役員、契約作業者を含む)に対して、セキュリティおよびプライバシーに関するリテラシートレーニングを行う。

1. 新規ユーザへの初期トレーニングの一環として、および[*設定:組織が定める頻度*]で。

2. システムの変更または[*設定:組織が定めるイベント*]の後で必要な場合。

b. システムユーザのセキュリティおよびプライバシー意識向上のために[*設定:組織が定める意識向上技法*]を採用する。

c. [*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]の後に、リテラシートレーニングおよび意識向上のためのコンテンツを更新する。

d. 内部または外部のセキュリティインシデントまたはブリーチから学んだ教訓を、リテラシートレーニングおよび意識向上技法に取り入れる。

詳解:組織は、ユーザの知識レベルをテストするための措置を含む、基本的および高度なレベルのリテラシートレーニングをシステムユーザに提供する。組織は、特定の組織の要件、職員がアクセスを認可されたシステム、および作業環境(テレワークなど)に基づいて、リテラシートレーニングおよび意識向上のためのコンテンツを定める。このコンテンツには、セキュリティおよびプライバシーの必要性の理解、およびセキュリティおよび個人のプライバシーを維持し、疑わしいインシデントに対応するためのユーザの措置が含まれている。このコンテンツは、運用上のセキュリティおよび個人情報の取り扱いの必要性に対応している。

意識向上の技法としては、ポスターの掲示、セキュリティおよびプライバシーの注意喚起が記された支給物の提供、ログオン画面へのメッセージの表示、組織の担当者からの電子メールによる通知または通知の生成、意識向上イベントの実施などがある。AT-2a.1 に記載されている最初のトレーニング後のリテラシートレーニングは、適用される法律、指令、規則、およびポリシーに合致する最低限の頻度で実施される。その後のリテラシートレーニングは、1 回以上の短い臨時のセッションで十分な場合があり、最近の攻撃スキームに関するトピック情報、組織のセキュリティおよびプライバシーポリシーの変更、セキュリティおよびプライバシーの期待の改訂、または初期トレーニングからのトピックの一部などが含まれる場合がある。リテラシートレーニングおよび意識向上のためのコンテンツを定期的に更新することで、コンテンツの関連性を維持することができる。リテラシートレーニングおよび意識向上のためのコンテンツの更新を引き起こす可能性のあるイベントとしては、アセスメントまたは監査の結果、セキュリティインシデントまたはブリーチ、または適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれるが、これらに限定されない。

関連管理策:AC-3, AC-17, AC-22, AT-3, AT-4, CP-3, IA-4, IR-2, IR-7, IR-9, PL-4, PM-13, PM-21, PS-7, PT-2, SA-8, SA-16

拡張管理策:

(1) リテラシートレーニングおよび意識向上 | 実践的な演習

イベントやインシデントをシミュレートするリテラシートレーニングの実践的な演習を提供する。

詳解:実践的な演習には、情報を収集したり、認可されていないアクセスをしたりすることや、悪意のある電子メールの添付ファイルを開いたり、スピアフィッシング攻撃や悪意のあるウェブリンクを呼び出したりすることによる有害なインパクトをシミュレートする、事前通知のないソーシャルエンジニアリングの試みなどが含まれる。

関連管理策:CA-2, CA-7, CP-4, IR-3

(2) リテラシートレーニングおよび意識向上 | インサイダー脅威

インサイダー脅威の潜在的な兆候を認識し、報告することに関するリテラシートレーニングを提供する。

詳解：インサイダー脅威の潜在的な兆候や可能性のある前兆には、過度の長期的な職務上の不満などの行動；職務遂行に必要のない情報へのアクセスを試みること；財源への説明できないアクセス；同僚従業員に対するいじめや嫌がらせ；職場での暴力；およびポリシー、手順、指令、規則、規定、または手続へのその他の重大な違反などが含まれる可能性がある。リテラシートレーニングには、組織によって確立されたチャネルを通じて、確立されたポリシーおよび手順に従って、インサイダー脅威の潜在的な兆候に関する従業員と経営陣の懸念をどのように伝えるかが含まれる。組織は、インサイダー脅威の認識に関するテーマを、役割に合わせてテーラリングすることを考慮してもよい。例えば、管理者向けのトレーニングでは、チームメンバーの行動の変化に焦点を当て、従業員向けのトレーニングでは、より一般的な観察に焦点を当てる場合がある。

関連管理策：PM-12

(3) リテラシートレーニングおよび意識向上 | ソーシャルエンジニアリングおよびマイニング

ソーシャルエンジニアリングおよびソーシャルマイニングの潜在的な事例および実際の事例を認識し報告することに関するリテラシートレーニングを提供する。

詳解：ソーシャルエンジニアリングとは、個人をだまして情報を漏えいさせたり、システムをブリーチしたり、侵害したり、あるいはシステムに悪影響を与えたりするために利用される可能性のある処理を実行しようとする試みである。ソーシャルエンジニアリングには、フィッシング、プリテキスティング、なりすまし、餌付け（baiting）、報復、スレッドハイジャック、ソーシャルメディアの不当な利用、および共連れ（tailgating）などがある。ソーシャルマイニングは、将来の攻撃をサポートするために使用される可能性のある、組織に関する情報を収集する試みである。リテラシートレーニングには、、ソーシャルエンジニアリングおよびデータマイニングの潜在的な事例および実際の事例に関する従業員と経営者の懸念を、確立されたポリシーおよび手順に基づく組織内の正しい系統を通じてどのように伝えるかに関する情報が含まれる。

関連管理策：なし

(4) リテラシートレーニングおよび意識向上 | 疑わしい通信および異常なシステム動作

[*設定：組織が定める悪意のあるコードの兆候*]を使用して、組織のシステムにおける不審な通信および異常な動作を認識することに関するリテラシートレーニングを提供する。

詳解：良く訓練された従業員は、電子メールまたはウェブアプリケーションを介して組織に侵入する悪意のあるコードから保護するための多層防御戦略の一部として採用できる、組織の別の管理策を提供する。職員は、疑わしい可能性のある電子メールの兆候を探すようにトレーニングされている（例えば、予期しない電子メールの受信、奇妙なあるいは貧弱な文法を含む電子メールの受信、既知のスポンサーまたは契約事業者からのように見える見知らぬ送信者からの電子メールの受信など）。職員は、疑わしい電子メールまたはウェブ通信への対応方法についてもトレーニングを受ける。このプロセスが効果的に機能するために、職員はトレーニングを受け、不審な通信の構成を認識する。システムの異常な振る舞いを認識する方法について職員をトレーニングすることで、悪意のあるコードの存在を早期に警告することができる。組織の職員が異常な動作を認識することにより、組織で採用されている悪意のあるコードの検知および保護ツールやシステムを補完することができる。

関連管理策：なし

(5) リテラシートレーニングおよび意識向上 | 持続的標的型攻撃（APT 攻撃）

APT 攻撃に関するリテラシートレーニングを提供する。

詳解：APT（Advanced Persistent Threat）攻撃を検知し、攻撃の成功を妨げる効果的な方法は、個人に特定のリテラシートレーニングを提供することである。脅威に対するリテラシートレーニングには、APT 攻撃が組織に侵入する様々な方法（例えば、ウェブサイト、電子メール、広告のポップアップ、記事、ソーシャルエンジニアリングなど）について個人を教育することが含まれる。効果的なトレーニングには、不審な電子メールを認識する技法、セキュアでない設定のリムーバルシステムの使用、および自宅にいる個人への潜在的な標

的化などが含まれる。

関連管理策：なし

(6) リテラシートレーニングおよび意識向上 | サイバー脅威環境

(a) サイバー脅威環境に関するリテラシートレーニングを行う。

(b) 現在のサイバー脅威情報をシステム運用に反映する。

詳解：脅威は時間とともに変化し続けるため、組織による脅威に関するリテラシートレーニングは動的である。さらに、脅威に関するリテラシートレーニングは、組織のミッションおよび事業機能を支援するシステム運用と切り離しては実施されるものではない。

関連管理策：RA-3

参照資料：[OMB A-130], [SP 800-50], [SP 800-160-2], [SP 800-181], [ODNI CTF]

AT-3 役割ベースのトレーニング

管理策：

a. [*設定：組織が定める役割と責任*]を持つ職員に役割ベースのセキュリティおよびプライバシーのトレーニングを提供する。

1. システム、情報へのアクセスを認可する前、または割り当てられた職務を実行する前、および[*設定：組織が定める頻度*]の後で。

2. システム変更によって必要な場合。

b. 役割ベースのトレーニングコンテンツを[*設定：組織が定める頻度*]および[*設定：組織が定めるイベント*]の後で更新する。

c. 内部または外部のセキュリティインシデントまたはブリーチから学んだ教訓を役割ベースのトレーニングに組み込む。

詳解：組織は、割り当てられた職務に合わせて特別にテーラリングされた技術トレーニングを含め、個人に割り当てられた役割と責任、組織のセキュリティおよびプライバシーの要件、および職員がアクセスを認可されたシステムに基づいて、トレーニングのコンテンツを決定する。役割ベースのトレーニングを必要とする可能性のある役割には、責任者または管理担当者（例えば、政府機関の責任者／最高経営責任者、最高情報責任者、リスクネジメント責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者）、システムオーナー；認可権限のある担当者；システムセキュリティ責任者；プライバシー担当者；調達および購買担当者；エンタープライズアーキテクト；システムエンジニア；ソフトウェア開発者；システムセキュリティエンジニア;プライバシーエンジニア;システム、ネットワーク、およびデータベースの管理者；監査人；構成管理措置を実施する職員；検証および妥当性確認措置を実施する職員；システムレベルのソフトウェアにアクセスできる職員；セキュリティ管理策アセッサー；緊急時対応計画およびインシデント対応の職務を有する職員；プライバシー管理責任者；個人情報にアクセスできる職員などが含まれる。

包括的な役割ベースのトレーニングは、管理、運用、および技術的な役割と、物理的、人的、および技術的な管理策に関係するする責任者を対象とする。役割ベースのトレーニングには、規定されたセキュリティおよびプライバシーの役割に関するポリシー、手順、ツール、方法、および成果物も含まれる。組織は、組織のセキュリティおよびプライバシープログラムという文脈の中で、運用とサプライチェーンのリスクネジメントに関連する責任を果たすために個人に必要なトレーニングを行う。役割ベースのトレーニングは、連邦政府機関にサービスを提供する契約事業者にも適用される。トレーニングのタイプには、ウェブベースのトレーニングおよびコンピュータベースのトレーニング、教室形式のトレーニング、実地トレーニング（マイクロトレーニングを含む）などがある。役割ベースのトレーニングのコンテンツを定期的に更新することで、コンテンツの適切性および効果を維持することができる。役割ベースのトレーニングコンテンツの更新を促す可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、または適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれるが、これらに限定されない。

関連管理策：AC-3, AC-17, AC-22, AT-2, AT-4, CP-3, IR-2, IR-4, IR-7, IR-9, PL-4, PM-13, PM-23, PS-7, PS-9, SA-3, SA-8, SA-11, SA-16, SR-5, SR-6, SR-11

拡張管理策：

(1) 役割ベースのトレーニング｜環境に関する管理策

環境に関する管理策の採用および運用に関する初期および[*設定：組織が定める頻度*]でのトレーニングを[*設定：組織が定める職員または役割*]に提供する。

詳解：環境に関する管理策には、火災検知および消火デバイスまたはシステム、スプリンクラーシステム、手持ち式消火器、固定式消火ホース、煙感知器、温度、湿度、暖房、換気、空調、および施設内の電力などが含まれる。

関連管理策：PE-1, PE-11, PE-13, PE-14, PE-15

(2) 役割ベースのトレーニング｜物理的セキュリティ管理策

物理的セキュリティ管理策の採用と運用に関する初期および[*設定：組織が定める頻度*]でのトレーニングを[*設定：組織が定める職員または役割*]に提供する。

詳解：物理的セキュリティ管理策には、物理的入退室管理デバイス、物理的侵入検知アラーム、施設警備員の運用手順、および監視または監視デバイスが含まれる。

関連管理策：PE-2, PE-3, PE-4

(3) 役割ベースのトレーニング｜実践的な演習

セキュリティとプライバシーのトレーニングにおいて、トレーニングの目的を強化する実践的な演習を提供する。

詳解：セキュリティに関する実践的な演習には、一般的なソフトウェアの脆弱性を悪用した模擬的な攻撃、または上級責任者や幹部を標的としたスピアフィッシング攻撃またはホエールフィッシング攻撃に対処するソフトウェア開発者向けのトレーニングが含まれる。プライバシーに関する実践的な演習には、様々なシナリオまたはプライバシー影響評価の実施シナリオにおける個人情報の識別と取扱いに関するクイズを含むモジュールが含まれる。

関連管理策：なし

(4) 役割ベースのトレーニング｜疑わしい通信および異常なシステム動作

[撤回：AT-2(4)に移動した]

(5) 役割ベースのトレーニング｜個人情報の取扱い

[*設定：組織が定める職員または役割*]に、個人情報の取扱いおよび透明性に関する管理策の採用および運用に関する初期および[*設定：組織が定める頻度*]でのトレーニングを提供する。

詳解：個人情報の取扱いおよび透明性に関する管理策には、個人情報を取扱う組織の権限および個人情報取扱いの目的が含まれる。連邦政府機関向けの役割ベースのトレーニングでは、個人情報を構成する可能性のある情報のタイプと、その処理に関連するリスク、考慮事項、および義務を扱う。このようなトレーニングでは、プライバシーポリシーおよび通知、記録システムの通知、コンピュータマッチング合意書（CMA）と通知、プライバシー影響評価、[PRIVACT]ステートメント、契約、情報共有合意書、覚書（MOU）および／または他のドキュメントに記載された個人情報を処理する権限も考慮する。

関連管理策：PT-2, PT-3, PT-5, PT-6

参照資料：[OMB A-130], [SP 800-50], [SP 800-181]

AT-4 トレーニングの記録

管理策：

a. セキュリティおよびプライバシー意識向上トレーニング、特定の役割ベースのセキュリティおよびプライバシートレーニングを含む、情報セキュリティおよびプライバシートレーニ

ング活動を文書化および監視する。

b. ［*設定：組織が定める期間*］個々のトレーニングの記録を保持する。

詳解：専門的なトレーニングの文書は、組織の裁量により、個々の監督者が維持管理することができる。アメリカ国立公文書記録管理局（NARA）は、連邦政府機関の記録保持に関するガイダンスを提供している。

関連管理策：AT-2, AT-3, CP-3, IR-2, PM-14, SI-12

拡張管理策：なし

参照資料：［OMB A-130］

AT-5 セキュリティグループおよび団体等との接触

［撤回：PM-15 に組み込まれた］

AT-6 トレーニングのフィードバック

管理策：組織のトレーニングの結果に関するフィードバックを［*設定：組織が定める頻度*］で［*設定：組織が定める職員*］に行う。

詳解：トレーニングのフィードバックには、意識向上トレーニングの結果と役割ベースのトレーニングの結果が含まれる。トレーニングの結果、特に重要な役割を担う要員の失敗は、深刻な問題となる可能性がある。したがって、適切な対応策を講じるためには、上級管理職がそのような状況を認識していることが重要である。トレーニングのフィードバックは、AT-2b および AT-3b で説明されている組織のトレーニングの評価およびコンテンツの更新をサポートする。

関連管理策：なし

拡張管理策：なし

参照資料：なし

3.3 監査および説明責任

監査および説明責任の要約表へのクイックリンク

AU-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。

1. 以下の[*選択(1 つ以上):組織レベル;ミッション/事業プロセスレベル;システムレベル*]の監査および説明責任のポリシー。

(a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、およびコンプライアンスに対処する。

(b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに適合している。

2. 監査および説明責任のポリシーおよび関連する監査および説明責任に関する管理策を実装するための手順。

b. 監査および説明責任のポリシーと手順の策定、文書化、および配布することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行の監査および説明責任をレビューし、更新する。

1. ポリシーは[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]の後で。

2. 手順は[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]の後で。

詳解:監査および説明責任のポリシーと手順は、システムおよび組織で実装される AU ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に寄与する。したがって、セキュリティおよびプライバシープログラムが、監査および説明責任のポリシーと手順の策定において協働することが重要である。一般的には、組織レベルでのセキュリティおよびプライバシープログラムのポリシーと手順が望ましく、ミッションまたはシステム固有のポリシーと手順の必要性をなくすことができる。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映した複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムについて規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述し、手順の対象である個人または役割向けとすることができる。手順は、システムのセキュリティおよびプライバシー計画の中で文書化することもできるし、1 つ以上の別の文書で文書化することもできる。監査および説明責任のポリシーと手順の更新を引き起こす可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれる。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策:PM-9, PS-8, SI-12

拡張管理策:なし

参照資料:[SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100]

AU-2 イベントロギング

管理策:

a. システムが監査機能をサポートしてロギングが可能となる[*設定:組織が定めるシステムがロギングできるイベントタイプ*]を識別する。

b. イベントロギング機能を、監査関連情報を必要とする他の組織エンティティと調整して、ロギングするイベントの選択基準を案内および通知する。

c. システム内のロギングについて、[*設定:組織が定めるイベントタイプ(AU-2a で規定されたイベントタイプのサブセット)と、識別された各イベントタイプのロギングの頻度(または必要な状況)*]を規定する。

d. ロギングのために選択されたイベントタイプがインシデントの事後調査をサポートするのに十分であるとみなされる理由の根拠を提供する。

e. ロギング用に選択されたイベントタイプを[*設定:組織が定める頻度*]でレビューし、更新する。

詳解:イベントは、システム内で観察可能な発生事象である。ロギングを必要とするイベントのタイプは、重要なイベントであり、かつシステムのセキュリティと個人のプライバシーに関連するイベントである。また、イベントロギングは、特定の監視および監査のニーズもサポートする。イベントのタイプには、パスワードの変更、システムに関連するログオンまたはアクセスの失敗、セキュリティまたはプライバシー属性の変更、管理者特権の使用、PIV クレデンシャルの使用、データアクションの変更、問い合わせ(クエリー)のパラメータ、または外部クレデンシャルの使用が含まれる。組織は、ロギングを必要とする一連のイベントタイプを決定する際には、実装する各管理策に適した監視と監査を考慮する。正確性を期すために、イベントロギングには、システムで動作しサポートされているすべてのプロトコルを含める。

監視および監査の要件と他のシステムのニーズのバランスを取るために、イベントロギングでは、特定の時点でロギングされるイベントタイプのサブセットを識別する必要がある。例えば、組織は、すべてのファイルアクセスの成功および失敗をロギングするケイパビリティがシステムに必要であるが、システムパフォーマンスへの潜在的な負担がある特定の状況を除いて、そのケイパビリティを有効にしないと判断する場合がある。組織がロギングすることを望むイベントタイプは変更される可能性がある。ロギングされた一連のイベントをレビューし、更新することは、イベントが関連性を保ち、組織のニーズをサポートし続けるために必要である。組織は、プライバシーリスクを引き起こす可能性のある個人に関する情報をロギングするイベントタイプがどのように明らかにすることができるか、およびそのようなリスクをどのように軽減するのが最善であるかを考慮する。例えば、ロギングイベントがパターンまたは使用時間に基づいている場合は特に、個人情報が監査証跡で明らかにされる可能性がある。

特定のタイプのイベントをロギングする必要性を含むイベントロギング要件は、他の管理策や管理策の拡張機能で参照される場合がある。これらには、AC-2(4)、AC-3(10)、AC-6(9)、AC-17(1)、CM-3f、CM-5(1)、IA-3(3.b)、MA-4(1)、MP-4(2)、PE-3、PM-21、PT-7、RA-8、SC-7(9)、SC-7(15)、SI-3(8)、SI-4(22)、SI-7(8)、SI-10(1)が含まれる。組織は、適用される法律、大統領令、指令、ポリシー、規則、基準、およびガイドラインで要求されるイベントのタイプを含める。監査記録は、情報がネットワークを通過する際のパケットレベルなど、様々なレベルで生成可能である。イベントロギングの適切なレベルを選択することは、監視および監査ケイパビリティの重要な部分であり、問題の根本原因を特定することができる。組織は、イベントタイプを定義する際に、分散型トランザクションベースのプロセスのステップや、サービス指向アーキテクチャで発生する処理など、関連するイベントタイプを網羅するために必要なロギングを考慮する。

関連管理策:AC-2, AC-3, AC-6, AC-7, AC-8, AC-16, AC-17, AU-3, AU-4, AU-5, AU-6, AU-7, AU-11, AU-12, CM-3, CM-5, CM-6, CM-13, IA-3, MA-4, MP-4, PE-3, PM-21, PT-2, PT-7, RA-8, SA-8, SC-7, SC-18, SI-3, SI-4, SI-7, SI-10, SI-11

拡張管理策:

(1) イベントロギング | 複数のソースからの監査記録の編集

[撤回:AU-12 に組み込まれた]

(2) イベントロギング｜コンポーネントによる監査イベントの選択

［撤回：AU-12 に組み込まれた］

(3) イベントロギング｜レビューおよび更新

［撤回：AU-2 に組み込まれた］

(4) イベントロギング｜特権機能

［撤回：AC-6(9)に組み込まれた］

参照資料：[OMB A-130], [SP 800-92]

AU-3 監査記録の内容

管理策：監査記録に、以下に規定する情報が含まれていることを確認する。

a. 発生したイベントのタイプ。

b. イベントが発生した日時。

c. イベントが発生した場所。

d. イベントの発生源。

e. イベントの結果。

f. イベントに関連する個人、サブジェクト、またはオブジェクト／エンティティのアイデンティティ。

詳解：監査機能をサポートするために必要となる可能性のある監査記録の内容には、イベントに関する事柄（項目 a）、タイムスタンプ（項目 b）、発信元と宛先のアドレス（項目 c）、ユーザまたはプロセスの識別子（項目 d と f）、成功または失敗の表示（項目 e）、および関連するファイル名（項目 a、c、e、および f）が含まれる。イベントの結果には、イベントの成功または失敗の表示、およびイベント発生後のシステムのセキュリティやプライバシーの状態など、イベント固有の結果が含まれる。組織は、プライバシーリスクを引き起こす可能性のある個人に関する情報が監査記録がどのようにして明らかにすることができるか、およびそのようなリスクをどのように軽減するのが最善かを考慮する。例えば、特に監査証跡が入力情報を記録している場合や、パターンや使用時間に基づいている場合は、監査証跡で個人情報が明らかになる可能性がある。

関連管理策：AU-2, AU-8, AU-12, AU-14, MA-4, PL-9, SA-8, SI-7, SI-11

拡張管理策：

(1) 監査記録の内容｜追加の監査情報

［*設定：組織が定める追加情報*］を含む監査記録を生成する。

詳解：監査記録で生成された情報を追加する機能は、監査記録の内容を構成するシステムの機能に依存する。組織は、アクセス制御やフロー制御ルールの呼び出し、グループアカウントユーザの個人のアイデンティティなど、監査記録の追加情報を考慮する場合があるが、これに限定されるものではない。組織はまた、追加の監査記録情報を、監査要件のために明示的に必要とされる情報のみに制限することを考慮する場合がある。これにより、誤解を招く可能性があったり、関心のある情報の特定がより困難になったり、または個人のプライバシーに対するリスクが高まったりするような情報を監査記録に含めないことで、監査証跡および監査ログの使用が容易になる。

関連管理策：なし

(2) 監査記録の内容｜計画された監査記録内容の集中管理

［撤回：PL-9 に組み込まれた］

(3) 監査記録の内容｜個人情報の要素の限定

**監査記録に含まれる個人情報を、プライバシーリスクアセスメントで特定された［*設定：*

組織が定める要素]**に限定する。**

詳解：監査記録に含まれる個人情報が運用目的上必要とされない場合は、その情報を限定することで、システムによって生じるプライバシーリスクのレベルを低減することができる。

関連管理策：RA-3

参照資料：[OMB A-130], [IR 8062]

AU-4 監査ロギングのストレージ容量

管理策：[*設定：組織が定める監査ロギングの保存要件*]に対応するために、監査ロギングのストレージ容量を割り当てる。

詳解：組織は、監査ロギングの記憶容量を設定する際に、実行する監査ロギングのタイプと監査ログ処理の要件を考慮する。十分な監査ロギングのストレージ容量を割り当てることで、その容量を超えてしまい、監査ロギングのケイパビリティが失われたり低下したりする可能性が低くなる。

関連管理策：AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4

拡張管理策：

(1) 監査ロギングのストレージ容量 | 代替ストレージへの転送

[*設定：組織が定める頻度*]で監査ロギングを、ロギングを実行するシステムまたはシステムコンポーネント以外の別のシステム、システムコンポーネント、または媒体に転送する。

詳解：オフロード（off-loading）とも呼ばれる監査ロギングの転送は、監査ロギングのストレージ容量が限られているシステムでは一般的なプロセスであり、監査ロギングの可用性をサポートする。最初の監査ロギングのストレージは、システムが監査ロギングのストレージに設定されたセカンダリまたは代替システムと通信できるようになるまで、一時的な方法でのみ使用され、その時点で監査ログが転送される。監査ロギングを代替ストレージに転送することは、監査ロギングが別のエンティティに転送されるという点で AU-9（2）と同様である。ただし、AU-9（2）を選択する目的は、監査記録の機密性と完全性を保護することである。組織は、いずれかの拡張管理策を選択することにより、監査ロギングのストレージ容量を増やし、監査記録およびロギングの機密性、完全性、可用性を維持するというメリットを得ることができる。

関連管理策：なし

参照資料：なし

AU-5 監査ロギングプロセス障害時の対応

管理策：

a. 監査ロギングプロセスに障害が発生した場合は、[*設定：組織が定める期間*]内に[*設定：組織が定める職員または役割*]に警告する。

b. [*設定：組織が定める追加措置*]を実行する。

詳解：監査ロギングプロセスの障害には、ソフトウェアおよびハードウェアのエラー、監査ロギングの取得メカニズムの障害、監査ロギングのストレージ容量限度への到達または超過が含まれる。組織が定める措置には、最も古い監査記録への上書き、システムのシャットダウン、監査記録の生成の停止を含める。組織は、障害のタイプ、障害の部位、障害の重大性、またはそのような要因の組み合わせに基づいて、監査ロギングプロセスの障害に対する追加の措置を規定することを選択できる。監査ロギングプロセスの障害がストレージ容量に関連している場合、その対応は、監査ロギングのストレージのリポジトリ（すなわち、監査ロギングが格納されている別個のシステムコンポーネント）、監査ロギングが存在するシステム、組織の監査ロギングストレージ容量の合計（つまり、すべての監査ロギングのストレージのリポジトリを合わせたも

の）、またはこれら 3 つすべてに対して実行される。組織は、指定された役割または職員に警告した後、追加措置を講じないことを決定してもよい。

関連管理策：AU-2, AU-4, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4, SI-12

拡張管理策：

(1) 監査ロギングプロセス障害時の対応 | ストレージ容量の警告

蓄積された監査ロギング量が、リポジトリの最大監査ロギングストレージ容量の[*設定：組織が定める割合*]に達したときに、[*設定：組織が定める期間*]内に[*設定：組織が定める職員、役割、または場所*]に警告を行う。

詳解：組織には、複数のシステムコンポーネントに分散された、複数の監査ロギングストレージのリポジトリがあり、各リポジトリのストレージ容量が異なる場合がある。

関連管理策：なし

(2) 監査ロギングプロセス障害時の対応 | リアルタイムアラート

[*設定：組織が定めるリアルタイムアラートを必要とする監査ロギング障害イベント*]が発生した場合、[*設定：組織が定める即時の期間*]内に[*設定：組織が定める職員、役割、および／または場所*]にアラートを発する。

詳解：アラートは、組織に緊急のメッセージを提供する。リアルタイムアラートは、これらのメッセージを情報技術の速度（すなわち、イベント検知からアラート発生までの時間が数秒以下）で行われる。

関連管理策：なし

(3) 監査ロギングプロセス障害時の対応 | 設定可能なトラフィック量のしきい値

監査ロギングのストレージ容量の制限を反映した設定可能なネットワーク通信トラフィック量のしきい値を設定し、これらのしきい値を超えるネットワークトラフィックを[選択：拒否；遅延]する。

詳解：組織は、ネットワーク通信トラフィックの監査ロギング情報がシステム監査ロギング機能のストレージ容量を超えていると判断された場合、そのネットワーク通信トラフィックの処理を拒否または遅延させるケイパビリティを備える。拒否または遅延応答は、監査ロギングのストレージ容量の変更に基づいて調整することができる、規定された組織のトラフィック量のしきい値によって発生する。

関連管理策：なし

(4) 監査ロギングプロセス障害時の対応 | 障害時のシャットダウン

代替監査ロギングのケイパビリティが存在する場合を除き、[*設定：組織が定める監査ロギング障害*]イベントが発生した場合は、[*選択：システム全体のシャットダウン；システムの部分的なシャットダウン；ミッションや事業機能の稼働を限定する縮退運用モード*]を起動する。

詳解：組織は、システムの自動シャットダウンや運用の低下を引き起こす可能性のある監査ロギング障害のタイプを定める。ミッションおよび事業継続性を確保することの重要性のため、組織は、監査ロギング障害の性質が、組織の中核となるミッションおよび事業機能をサポートするシステムの完全なシャットダウンを必要とするほど深刻ではないと判断する場合がある。そのような場合には、部分的なシステムのシャットダウン、またはケイパビリティが低下した縮退モードでの運用が、実行可能な代替策となり得る。

関連管理策：AU-15

(5) 監査ロギングプロセス障害時の対応 | 代替監査ロギングケイパビリティ

[*設定：組織が定める代替監査ロギング機能*]を実装するプライマリ監査ロギングケイパビリティに障害が発生した場合に、代替監査ロギングケイパビリティを提供する。

詳解：代替監査ロギングケイパビリティは、プライマリ監査ロギングケイパビリティの障害が修正されるまで採用される短期的な保護ソリューションである可能性があるため、組織は、代替監査ロギングケイパビリティが、障害の影響を受けるプライマリ監査ロギング機

能のサブセットのみを提供すればよいと判断する場合がある。

関連管理策：AU-9

参照資料：なし

AU-6 監査記録のレビュー、分析、および報告

管理策：

a. [*設定：組織が定める不適切または異常な活動*]の兆候、および不適切または異常な活動の潜在的な影響について[*設定：組織が定める頻度*]で、システム監査記録をレビューし、分析する。

b. 結果を[*設定：組織で定められた職員または役割*]に報告する。

c. 法執行機関の情報、情報機関の情報、またはその他の信頼できるソースに基づいてリスクに変化があった場合、システム内の監査記録のレビュー、分析、および報告のレベルを調整する。

詳解：監査記録のレビュー、分析、および報告には、組織によって実行される情報セキュリティおよびプライバシー関連のロギングを対象とする。これには、アカウントの使用状況、リモートアクセス、ワイヤレス接続、モバイルデバイスの接続、構成設定、システムコンポーネントの資産台帳（インベントリー）、メンテナンスツールと非ローカルメンテナンスの使用、物理的アクセス、温度と湿度、デバイスの配送と取り外し、システムインタフェースでの通信、モバイルコードまたはボイスオーバーインターネットプロトコル（VoIP）などの使用状況の監視から生じるロギングが含まれる。結果は、インシデント対応チーム、ヘルプデスク、セキュリティまたはプライバシーオフィスなどの組織のエンティティに報告することができる。組織が監査記録のレビューおよび分析を禁じられているか、そのような活動を行うことができない場合は、そのような権限を付与された他の組織によってレビューまたは分析が行われることがある。監査記録のレビュー、分析、報告の頻度、範囲、および／または複雑さは、入手した新しい情報に基づいて組織のニーズを満たすように調整することができる。

関連管理策：AC-2, AC-3, AC-5, AC-6, AC-7, AC-17, AU-7, AU-16, CA-2, CA-7, CM-2, CM-5, CM-6, CM-10, CM-11, IA-2, IA-3, IA-5, IA-8, IR-5, MA-4, MP-4, PE-3, PE-6, RA-5, SA-8, SC-7, SI-3, SI-4, SI-7

拡張管理策：

(1) 監査記録のレビュー、分析、および報告 | 自動化されたプロセス統合

[*設定：組織が定める自動化されたメカニズム*]を使用して、監査記録のレビュー、分析、報告プロセスを統合する。

詳解：統合された監査記録のレビュー、分析、報告から恩恵を受ける組織プロセスには、インシデント対応、継続的な監視、危機管理計画、疑わしい活動の調査と対応、および査察総監（Inspector General）による監査が含まれる。

関連管理策：PM-7

(2) 監査記録のレビュー、分析、および報告 | 自動化されたセキュリティアラート

[撤回：SI-4 に組み込まれた]

(3) 監査記録のレビュー、分析、および報告 | 監査記録リポジトリの関連付け

組織全体の状況を認識するために、異なるリポジトリに渡って監査記録を分析し、相互に関連付ける。

詳解：組織全体の状況認識には、リスクマネジメントの 3 つのレベル（すなわち、組織レベル、ミッション／事業プロセスレベル、情報システムレベル）すべてにわたる認識が含まれ、組織横断的な認識をサポートする。

関連管理策：AU-12, IR-4

(4) 監査記録のレビュー、分析、および報告 | 一元的なレビューおよび分析

システム内の複数のコンポーネントからの監査記録を一元的にレビューおよび分析す

るケイパビリティを規定し実装する。

詳解：一元的なレビューおよび分析のための自動化されたメカニズムには、セキュリティ情報およびイベント管理製品が含まれる。

関連管理策：AU-2, AU-12

(5) 監査記録のレビュー、分析、および報告 | 監査記録の統合分析

不適切または異常な活動を識別する能力をさらに強化するために、監査記録の分析を、[*選択(1 つ以上)：脆弱性スキャン情報；パフォーマンスデータ；システム監視情報；[設定：組織が定める他のソースから収集されたデータ／情報*]]の分析と統合する。。

詳解：監査記録の統合分析では、脆弱性スキャン、パフォーマンスデータの生成、またはシステム監視は必要ない。むしろ、統合分析では、スキャン、監視、またはその他のデータ収集活動によって生成された情報の分析を、監査記録情報の分析と統合することが必要である。セキュリティ情報およびイベント管理ツールは、複数のシステムコンポーネントからの監査記録の集約または統合、および監査記録の相関および分析を容易にすることができる。組織が開発した標準化された監査記録分析スクリプト（必要に応じてローカライズされたスクリプト調整を伴う）を使用すると、収集された監査記録情報を分析するためのより費用対効果の高いアプローチが提供される。監査記録情報と脆弱性スキャン情報との相関関係は、システムの脆弱性スキャンの信憑性を判断したり、攻撃検知イベントとスキャン結果を関連付けたりする際に重要である。パフォーマンスデータとの相関関係により、DoS（サービス拒否）攻撃や、認可されていないリソース使用となるその他のタイプの攻撃を発見することができる。システム監視情報との相関関係は、攻撃を発見したり、監査情報を運用状況に適切に関連付けたりするのに役立てることができる。

関連管理策：AU-12, IR-4

(6) 監査記録のレビュー、分析、および報告 | 物理的監視との相関

疑わしい、不適切な、異常な、または悪意のある活動を識別する能力をさらに強化するために、監査記録情報と物理的アクセス監視から得られた情報を相互に関連付ける。

詳解：物理的監査記録情報およびシステムの監査記録との相関関係は、組織が疑わしい行動を識別したり、そのような行動の証拠を裏付けたりするのに役立つ場合がある。例えば、特定のシステムへの論理アクセスに関する個人のアイデンティティと、論理アクセスが発生したときに個人が施設にいたという追加の物理的セキュリティ情報との相関関係は、調査に役立つ可能性がある。

関連管理策：なし

(7) 監査記録のレビュー、分析、および報告 | 許可される措置

監査記録情報のレビュー、分析、および報告に関連する、[*選択(1 つ以上)：システムプロセス；役割；ユーザ*]ごとに許可される措置を規定する。

詳解：組織は、システムアカウント管理活動を通じて、監査記録のレビュー、分析、および報告に関連するシステムプロセス、役割、ユーザに許可される措置を規定する。監査記録情報に許可される措置を規定することは、最小特権の原則を実施する方法の 1 つである。許可される措置には、システムによって実施され、読み取り、書き込み、実行、追加、および削除が含まれる。

関連管理策：なし

(8) 監査記録のレビュー、分析、および報告 | 特権コマンドの全文分析

システムの物理的に異なるコンポーネントまたはサブシステム、またはその分析専用の他のシステムで、ロギングされた特権コマンドの全文分析を実行する。

詳解：特権コマンドの全文分析には、特権コマンドを実行するケイパビリティなど、ユーザが昇格された特権を持っているシステム上の情報を危険にさらすことなく、特権ユーザに関する監査記録情報を分析するための別個の環境が必要である。全文分析は、コマンドの名前のみを考慮する分析とは対照的に、特権コマンド（すなわち、コマンドおよびパラメータ）の全文を考慮する分析である。全文分析には、パターンマッチングとヒューリスティックス（発見的手法）な使用が含まれる。

関連管理策：AU-3, AU-9, AU-11, AU-12

(9) 監査記録のレビュー、分析、および報告 | 非技術的ソースからの情報との相関

組織全体の状況認識を強化するために、非技術的ソースからの情報を監査記録情報と関連付ける。

詳解：非技術的なソースには、ハラスメント（迷惑行為）のインシデントおよび情報資産の不適切な使用に関連する組織のポリシー違反を文書化した記録が含まれる。そのような情報は、潜在的な悪意のあるインサイダー行為を検知するための、指向的な分析の取り組みにつながる可能性がある。組織は、非技術的なソースから入手できる情報は、その機微性のため、アクセスを制限する。アクセスを制限することで、知る必要のない個人にプライバシー関連情報が不注意に開示される可能性を最小限に抑えることができる。非技術的なソースからの情報と監査記録情報との相関は、通常、個人がインシデントに関与している疑いがある場合にのみ発生する。組織は、そのような措置に先立って法的助言を得る。

関連管理策：PM-12

(10) 監査記録のレビュー、分析、および報告 | 監査レベルの調整

［撤回：AU-6 に組み込まれた］

参照資料：[SP 800-86], [SP 800-101]

AU-7 監査記録の整理および報告書の作成

管理策：以下の監査記録の整理および報告書作成ケイパビリティを規定し実装する。

a. オンデマンドの監査記録のレビュー、分析、報告の要件、およびインシデントの事後調査をサポートする。

b. 監査記録の元の内容または時間順序を変更しない。

詳解：監査記録の整理は、収集された監査ロギング情報を操作し、アナリストにとってより意味のある要約形式に編成するプロセスである。監査記録の整理およびレポート生成のケイパビリティは、監査ロギング活動を実施する同じシステムまたは同じ組織のエンティティから常に発生するとは限らない。監査記録の整理ケイパビリティには、監査記録の異常な振る舞いを識別するための高度なデータフィルタを備えた最新のデータマイニング技法が含まれる。システムが提供するレポート生成のケイパビリティにより、カスタマイズ可能なレポートを生成できる。監査記録のタイムスタンプの精度が不十分な場合、監査記録の時間順序が問題になる可能性がある。

関連管理策：AC-2, AU-2, AU-3, AU-4, AU-5, AU-6, AU-12, AU-16, CM-5, IA-5, IR-4, PM-12, SI-4

拡張管理策：

(1) 監査記録の整理および報告の生成 | 自動処理

[*設定：組織が定める監査記録内の領域*]の内容に基づいて、関心のあるイベントの監査記録を処理、ソート、および検索するケイパビリティを規定し実装する。

詳解：関連するシステムリソース、アクセスされる情報オブジェクト、個人のアイデンティティ、イベントのタイプ、イベントの場所、イベントの日時、関連する IP アドレス、イベントの成功または失敗など、監査記録の内容によって対象となるイベントを識別できる。組織は、一般的なネットワークの場所や特定のシステムコンポーネントによって選択可能な場所など、必要に応じてどの程度の粒度でもイベントの基準を規定できる。

関連管理策：なし

(2) 監査記録の整理および報告の生成 | 自動ソートおよび検索

［撤回：AU-7(1)に組み込まれた］

参照資料：なし

AU-8 タイムスタンプ

管理策:

a. 内部システムクロックを使用して、監査記録のタイムスタンプを生成する。

b. [*設定:組織が定める時間測定の粒度*]を満たす、協定世界時(UTC)、協定世界時からの固定現地時間オフセット、またはタイムスタンプの一部として現地時間オフセットを使用する監査記録のタイムスタンプを記録する。

詳解:システムによって生成されるタイムスタンプには、日付と時刻が含まれる。時刻は通常、協定世界時(UTC)、現行のグリニッジ標準時(GMT)、または UTC からのオフセットを持つ現地時間で表される。時間測定の粒度とは、システムクロックと基準クロックとの間の同期の度合いを指す(例えば、数百ミリ秒または数十ミリ秒以内に同期するクロック)。組織は、システムコンポーネントごとに異なる時間の粒度を定めることができる。タイムサービスは、アクセス制御、識別、認証など、他のセキュリティケイパビリティをサポートするために使用されるメカニズムの性質に応じて、非常に重要となる場合がある。

関連管理策:AU-3, AU-12, AU-14, SC-45

拡張管理策:

(1) タイムスタンプ | 信頼できる時刻ソースとの同期

[撤回:SC-45(1)に移動した]

(2) タイムスタンプ | 二次的な信頼できる時刻ソース

[撤回:SC-45(2)に移動した]

参照資料:なし

AU-9 監査情報の保護

管理策:

a. 監査情報と監査ロギングツールを認可されていないアクセス、変更、削除から保護する。

b. 監査情報の認可されていないアクセス、変更、または削除が検知された場合は、[*設定:組織が定める職員または役割*]にアラートする。

詳解:監査情報には、監査記録、監査ロギング設定、監査報告書、個人情報など、システムの活動を正しく監査するために必要なすべての情報が含まれる。監査ロギングツールとは、システム監査およびロギング活動を実施するために使用されるプログラムおよびデバイスである。監査情報の保護は、技術的保護に焦点を当てるとともに、監査ロギングツールにアクセスする機能の実施を認可された個人に限定する。監査情報の物理的保護は、媒体保護の管理策と物理的および環境的保護の管理策の双方によって対処される。

関連管理策:AC-3, AC-6, AU-6, AU-11, AU-14, AU-15, MP-2, MP-4, PE-2, PE-3, PE-6, SA-8, SC-8, SI-4

拡張管理策:

(1) 監査情報の保護 | ハードウェア強制型ライトワンスメディア

監査証跡をハードウェア強制型ライトワンスメディアに書き込む。

詳解:監査証跡をハードウェア強制型ライトワンスメディアに書き込むことは、監査証跡の初期生成(すなわち、検知、分析、および報告の目的に使用される情報を表す監査記録の収集)およびそれらの監査証跡のバックアップに適用される。監査証跡をハードウェア強制型ライトワンスメディアに書き込むことは、監査証跡に書き込まれる前の監査記録の初期生成には適用されない。ライトワンスメディア(WORM)には、CD-R、BD-R、および DVD-R などがある。対照的に、テープカートリッジ、USB ドライブ、CD-RW、DVD-RW などの切り替え可能な書き込み保護メディアの使用は、書き込み保護されたメディアになるが、ラ

イトワンスメディアにはならない。

関連管理策：AU-4, AU-5

(2) 監査情報の保護｜異なる物理的システムまたはコンポーネントへの保存

監査対象のシステムまたはコンポーネントとは物理的に異なるシステムまたはシステムコンポーネントの一部であるリポジトリに、監査記録を[*設定：組織が定める頻度*]で保存する。

詳解：監査記録を、監査対象のシステムまたはシステムコンポーネントとは別のリポジトリに保存することで、監査対象のシステムが侵害されたとしても監査記録の侵害につながらないようにすることができる。監査記録を物理的に別のシステムまたはコンポーネントに保存することで、監査記録の機密性と完全性が維持され、組織全体の活動としての監査記録の管理が容易になる。監査記録を別のシステムまたはコンポーネントに保存することは、監査記録の初期生成だけでなく、バックアップまたは長期保存にも適用される。

関連管理策：AU-4, AU-5

(3) 監査情報の保護｜暗号化による保護

監査情報と監査ツールの完全性を保護するために、暗号化のメカニズムを実装する。

詳解：監査情報の完全性を保護するために使用される暗号化のメカニズムには、非対称暗号を使用した署名付きハッシュ関数が含まれる。これにより、ハッシュの生成するための秘密鍵の機密性を維持したまま、ハッシュ情報を検証するための公開鍵の配布が可能になる。

関連管理策：AU-10, SC-12, SC-13

(4) 監査情報の保護｜一部の特権ユーザによるアクセス

監査ロギング機能の管理へのアクセスを[*設定：組織が定める特権ユーザまたは役割の一部*]にのみ認可する。

詳解：システムへの特権アクセスを持ち、そのシステムによる監査の対象でもある個人または役割は、監査活動を阻害したり、監査記録を変更したりすることにより、監査情報の信頼性に影響を与える可能性がある。監査関連の特権とその他の特権との間にさらに特権アクセスを規定することを要求することで、監査関連の特権を持つユーザまたは役割の数を制限する。

関連管理策：AC-5

(5) 監査情報の保護｜二重認可

[*設定：組織が定める監査情報*]の[*選択（1 つ以上）：移動；削除*]に二重認可を実施する。

詳解：組織は、監査情報のタイプごとに異なる選択オプションを選択することができる。二重認可のメカニズム（二人担当制とも呼ばれる）では、監査機能を実行するためには 2 人の認可された個人の承認が必要となる。共謀のリスクを低減するために、組織は二重認可の職務を他の個人に交代させることを考慮する。組織は、公共および環境の安全を確保するために即時の対応が必要な場合には、二重認可のメカニズムを必要としない。

関連管理策：AC-3

(6) 監査情報の保護｜読み取り専用アクセス

監査情報への読み取り専用アクセスを[*設定：組織が定める特権ユーザまたは役割の一部*]に認可する。

詳解：特権ユーザまたは役割への認可を読み取り専用に制限することで、悪意のある行為を隠蔽するために監査記録を削除するなど、そのようなユーザまたは役割によって開始される可能性のある組織への潜在的な損害を限定することができる。

関連管理策：なし

(7) 監査情報の保護｜異なるオペレーティングシステムのコンポーネントへの保存

監査対象のシステムまたはコンポーネントとは異なるオペレーティングシステムを実行しているコンポーネントに監査情報を保存する。

詳解：異なるオペレーティングシステムを実行しているシステムコンポーネントに監査情報を保存することにより、監査記録が侵害される原因となるそのシステムに固有の脆弱性のリスクが軽減される。

関連管理策：AU-4, AU-5, AU-11, SC-29

参照資料：[FIPS 140-3], [FIPS 180-4], [FIPS 202]

AU-10 否認防止

管理策：個人（または個人に代わって行動するプロセス）が[*設定：組織が定める否認防止の対象となる措置*]を実行したという反論の余地のないエビデンスを提供する。

詳解：否認防止の対象となる個人の行為のタイプには、情報の作成、メッセージの送受信、情報の承認などがある。否認防止は、特定の文書を作成してないという執筆者、メッセージを伝送していないという送信者、メッセージを受信していないという受信者、および文書に署名してないという署名者による主張から保護する。否認防止サービスは、情報が個人から発信されたものか、個人が特定の措置（電子メールの送信、契約書への署名、調達要求の承認、特定の情報の受信など）を行ったかどうかを判断するために使用できる。組織は、デジタル署名やデジタルメッセージの受信など、様々な技法やメカニズムを採用することにより、否認防止サービスを利用できる。

関連管理策：AU-9, PM-12, SA-8, SC-8, SC-12, SC-13, SC-16, SC-17, SC-23

拡張管理策：

(1) 否認防止 | アイデンティティとの関連性

(a) 情報作成者のアイデンティティと情報を[*設定：組織が定めるバインディングの強さ*]でバインディングする。

(b) 認可された個人が情報作成者のアイデンティティを確定する手段を提供する。

詳解：情報へのアイデンティティのバインディングは、情報転送の際に特定の情報を作成した人物を識別する手段を組織の職員に提供する監査要件をサポートする。組織は、情報のセキュリティ分類およびその他の関連するリスク要因に基づいて、情報作成者と情報の間の属性のバインディングの強さを定め、承認する。

関連管理策：AC-4, AC-16

(2) 否認防止 | 情報作成者のアイデンティティのバインディングの妥当性確認

(a) [*設定：組織が定める頻度*]で、情報作成者のアイデンティティと情報とのバインディングの妥当性を確認する。

(b) 妥当性確認エラーが発生した場合は、[*設定：組織が定める措置*]を実行する。

詳解：情報作成者のアイデンティティと情報とのバインディングの妥当性を確認することで、作成時とレビューの間の情報の変更を防止することができる。バインディングの妥当性確認は、例えば、暗号チェックサムを使用することによって実現できる。組織は、妥当性確認がユーザの要求に対応するものか、自動的に生成されるものかを規定する。

関連管理策：AC-3, AC-4, AC-16

(3) 否認防止 | 過程管理

レビューまたは開示された情報について、確立された過程管理内で、レビュー実施者または情報開示者の認証情報を維持する。

詳解：過程管理とは、エビデンスを取り扱った各個人、エビデンスが収集または転送された日時、および転送の目的を文書化することにより、その収集、保全、および分析のライフサイクルを通じてエビデンスの動きを追跡するプロセスである。レビュー実施者が人間である場合、またはレビュー機能が自動化されているが開示または転送機能とは別個であ

る場合、システムは、開示される情報のレビュー実施者のアイデンティティを情報および情報ラベルに関連付ける。人間によるレビューの場合、レビュー実施者または情報開示者の認証情報を維持することで、誰が情報をレビューして開示したかを識別する手段が組織に提供される。自動化されたレビューの場合には、承認されたレビュー機能のみが使用されることを確実にする。

関連管理策：AC-4, AC-16

(4) 否認防止 | 情報レビュー実施者のアイデンティティのバインディングの妥当性確認

(a) [*設定：組織が定めるセキュリティドメイン*]間で開示または転送を行う前に、開示ポイントまたは転送ポイントで情報レビュー実施者のアイデンティティと情報とのバインディングの妥当性を確認する。

(b) 妥当性確認エラーが発生した場合は、[*設定：組織が定める措置*]を行う。

詳解：転送ポイントまたは開示ポイントにおいて情報レビュー実施者のアイデンティティと情報とのバインディングの妥当性を確認することで、レビューと転送または開示との間で情報の認可されていない変更を防ぐことができる。バインディングの妥当性確認は、暗号化されたチェックサムを使用して行うことができる。組織は、妥当性確認がユーザの要求に対応するものか、自動的に生成されるものかを規定する。

関連管理策：AC-4, AC-16

(5) 否認防止 | デジタル署名

[撤回：SI-7 に組み込まれた]

参照資料：[FIPS 140-3], [FIPS 180-4], [FIPS 186-4], [FIPS 202], [SP 800-177]

AU-11 監査記録の保持

管理策：インシデントの事後調査のサポートを提供し、規則および組織の情報保持要件を満たすために、[*設定：組織が定める記録保持ポリシーと一致する期間*]、監査記録を保持する。

詳解：組織は、管理、法務、監査、またはその他の運用目的で記録が不要になったと判断されるまで、監査記録を保持する。これには、情報公開法（FOIA）の要求、召喚状、および法執行措置に関連する監査記録の保持および可用性が含まれる。組織は、そのようなタイプの措置に関連する監査記録の標準的なカテゴリと、各タイプの措置に対する標準的な対応プロセスを策定する。公文書記録管理局（NARA）の GRS（General Records Schedules）では、記録保持に関する連邦政府のポリシーを規定している。

関連管理策：AU-2, AU-4, AU-5, AU-6, AU-9, AU-14, MP-6, RA-5, SI-12

拡張管理策：

(1) 監査記録の保持 | 長期的な検索ケイパビリティ

システムによって生成された長期監査記録を確実に検索できるように、[*設定：組織が定める手段*]を採用する。

詳解：組織は、長期間の保存（数年程度）を必要とする監査記録にアクセスして読み取る必要がある。監査記録の検索を容易にするために採用される手段には、記録をより新しいフォーマットに変換すること、記録を読み取ることができるデバイスを保持すること、職員が記録を解釈する方法を理解するのに役立つ必要な文書を保持することなどが含まれる。

関連管理策：なし

参照資料：[OMB A-130]

AU-12 監査記録の生成

管理策：

a. [*設定：組織が定めるシステムコンポーネント*]に、AU-2a で規定されているシステムが

監査可能なイベントタイプに監査記録生成ケイパビリティを提供する。

b. [*設定：組織が定める職員または役割*]が、システムの特定のコンポーネントによってロギングされるイベントタイプを選択できるようにする。

c. AU-3 で規定された監査記録の内容を含む、AU-2c で規定されたイベントタイプの監査記録を生成する。

詳解：監査記録は、様々なシステムコンポーネントから生成できる。AU-2d で規定されたイベントタイプは、監査ロギングが生成されるイベントタイプであり、システムが監査記録を生成することができるすべてのイベントタイプのサブセットである。

関連管理策：AC-6, AC-17, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-14, CM-5, MA-4, MP-4, PM-12, SA-8, SC-18, SI-3, SI-4, SI-7, SI-10

拡張管理策：

(1) 監査記録の生成 | システム全体の時間相関のある監査証跡

[*設定：組織が定めるシステムコンポーネント*]からの監査記録を、[*設定：監査証跡内の個々の記録のタイムスタンプ間の関係に関する組織が定める許容レベル*]内で時間相関のあるシステム全体の（論理的または物理的）監査証跡にまとめる。

詳解：個々の監査記録のタイムスタンプを他の監査記録のタイムスタンプと確実に関連付けて、組織の許容範囲内で記録の時間順序を実現できる場合、監査証跡は時間相関がある。

関連管理策：AU-8, SC-45

(2) 監査記録の生成 | 標準化されたフォーマット

標準化されたフォーマットの監査記録で構成されるシステム全体の（論理的または物理的）監査証跡を作成する。

詳解：共通の標準に準拠する監査記録は、デバイスとシステム間の相互運用性および情報交換を促進する。相互運用性および情報交換を促進することで、分析および相関できるイベント情報の作成が容易になる。ロギングのメカニズムが標準化されたフォーマットに準拠していない場合、システムは、システム全体の監査証跡をまとめる際に、個々の監査記録を標準化されたフォーマットに変換することがある。

関連管理策：なし

(3) 監査記録の生成 | 認可された個人による変更

[*設定：組織が定める個人または役割*]が、[*設定：組織が定める時間しきい値*]内の[*設定：組織が定める選択可能なイベントの判断基準*]に基づいて[*設定：組織が定めるシステムコンポーネント*]で実行されるロギングを変更するケイパビリティを提供し実装する。

詳解：認可された個人がシステムのロギングに変更できるよう許可すると、組織は、組織の要件を満たすために必要に応じてロギングを拡張または制限できる。システムリソースを節約するために制限されたロギングは、特定の脅威状況に対処するために（一時的または永続的に）拡張される場合がある。さらに、監査の削減、分析、報告を容易にするために、ロギングを特定のイベントタイプのセットに制限することもできる。組織は、ロギング措置が変更される時間のしきい値を設定できる（例えば、ほぼリアルタイム、数分以内、または数時間以内など）。

関連管理策：AC-3

(4) 監査記録の生成 | 個人情報のクエリパラメータの監査

個人情報を含むデータセットに対するユーザのクエリイベントのパラメータを監査するケイパビリティを提供し実装する。

詳解：クエリパラメータは、個々のシステムまたは自動化されたシステムがデータを取得するためにシステムに送信する明示的な判断基準である。個人情報を含むデータセットのクエリパラメータを監査することにより、組織は、認可された職員による個人情報へのアクセ

ス、使用、または共有を追跡し、理解するケイパビリティを強化される。

関連管理策:なし

参照資料:なし

AU-13 情報開示の監視

管理策:

a. [*設定:組織が定める頻度*]で[*設定:組織が定めるオープンソース情報および/または情報サイト*]を監視し、組織情報の認可されていない開示のエビデンスがないか監視する。

b. 情報開示が発見された場合:

1. [*設定:組織が定める職員または役割*]に通知する。

2. [*設定:組織が定める追加措置*]を講ずる。

詳解:認可されていない情報の開示は、データ流出の一形態である。オープンソース情報には、ソーシャルネットワーキングサイト、コード共有プラットフォームおよびリポジトリなどがある。組織情報の例としては、組織が保持する個人情報、または組織が生成する専有情報などがある。

関連管理策:AC-22, PE-3, PM-12, RA-5, SC-7, SI-20

拡張管理策:

(1) 情報開示の監視 | 自動化されたツールの使用

[*設定:組織が定める自動化されたメカニズム*]を使用して、オープンソース情報および情報サイトを監視する。

詳解:自動化されたメカニズムには、組織に通知やアラートを提供する商用サービスや、ウェブサイト上の新しい投稿を監視するための自動化されたスクリプトが含まれる。

関連管理策:なし

(2) 情報開示の監視 | 監視対象サイトのレビュー

監視対象のオープンソース情報サイトのリストを[*設定:組織が定める頻度*]でレビューを実施する。

詳解:定期的に監視されているオープンソース情報サイトの現在のリストをレビューすることは、選択されたサイトが関連性を維持することを保証するのに役立つ。このレビューはまた、組織情報の認可されていない開示のエビデンスを提供する可能性のある新しいオープンソース情報サイトを追加する機会も提供する。監視されているサイトのリストは、他の信頼できるソースの脅威インテリジェンスから案内ならびに通知を受けることができる。

関連管理策:なし

(3) 情報開示の監視 | 認可されていない情報の複製

外部エンティティが組織の情報を認可を受けずに複製していないかどうかを判断するために、検出技法、プロセス、およびツールを採用する。

詳解:外部エンティティによる認可されていない組織情報の使用または複製は、評判の低下など、組織の運営および資産に悪影響を与える可能性がある。このような行為には、ウェブホスティング組織になりすまそうとする敵対者または敵対的な脅威行為者による組織のウェブサイトの複製が含まれる場合がある。外部エンティティが組織情報を認可されずに複製しているかどうかを判断するために使用される検出ツール、技法、およびプロセスには、外部のウェブサイトのスキャン、ソーシャルメディアの監視、認可を受けていない組織情報の使用を認識するためのスタッフのトレーニングが含まれる。

関連管理策:なし

参照資料:なし

AU-14 セッション監査

管理策:

a. [*設定:組織が定めるユーザまたは役割*]の[*設定:組織が定める状況下*]におけるユーザセッションの内容を[*選択(1 つ以上):記録する;見る;聞き取る;ロギングする*]ケイパビリティを提供し実装する。

b. 法律顧問と協議し、適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに従って、セッション監査活動を策定、統合、および使用する。

詳解:セッション監査には、キーストロークの打鍵監視、アクセスしたウェブサイトの追跡、情報やファイル転送を記録することなどが含まれる。セッション監査ケイパビリティは、イベントのロギングに追加して実装され、特殊なセッションキャプチャ技術の実装を伴う場合がある。組織は、セッション監査がプライバシーリスクを引き起こす可能性のある個人に関する情報をどのように明らかにできるか、およびそれらのリスクをどのように軽減するかを考慮する。セッション監査はシステムおよびネットワークのパフォーマンスにインパクトを与える可能性があるため、組織は明確に規定された状況下でケイパビリティを有効化する(例えば、組織が特定の個人を疑っている場合など)。組織は、個人情報の使用を含む、法律、プライバシー、市民権、または人権に関するあらゆる問題を適切に対処するために、法律顧問、市民自由権担当者、プライバシー担当者と相談する。

関連管理策:AC-3, AC-8, AU-2, AU-3, AU-4, AU-5, AU-8, AU-9, AU-11, AU-12

拡張管理策:

(1) セッション監査 | システムの起動

システムの起動時にセッション監査を自動的に開始する。

詳解:起動時にセッション監査を自動的に開始することで、選択した個人についてキャプチャされている情報が完全であり、悪意のある脅威行為者によるタンパリングによって侵害されないようにすることができる。

関連管理策:なし

(2) セッション監査 | キャプチャおよび記録内容

[撤回:AU-14 に組み込まれた]

(3) セッション監査 | リモートでの視聴

認可されたユーザが、確立されたユーザセッションに関連するコンテンツをリモートでリアルタイム視聴できるケイパビリティを提供し実装する。

詳解:なし

関連管理策:AC-17

参照資料:なし

AU-15 代替監査ロギングケイパビリティ

[撤回:AU-5(5)に移動した]

AU-16 組織横断的監査ロギング

管理策:組織の境界を越えて監査情報が伝送される場合、外部組織間で[*設定:組織が定める監査情報*]を調整するために[*設定:組織が定める方法*]を採用する。

詳解:組織が外部組織のシステムまたはサービスを使用する場合、監査ロギングケイパビリティには、組織間で協調的なアプローチが必要である。例えば、組織の境界を越えて特定のサービスを要求する個人のアイデンティティを維持することは、しばしば困難な場合があり、そうすることで、パフォーマンスおよびプライバシーに重大な影響を及ぼすことが判明する場合がある。したがって、多くの場合、組織横断的な監査ロギングでは、最初のシステムで要求を発行した

個人のアイデンティティを単にキャプチャし、後続のシステムでは、要求が認可された個人から発信されたものであることを記録する。組織は、監査情報の要件と監査情報の保護を調整するプロセスを情報交換合意書に含めることを考慮する。

関連管理策：AU-3, AU-6, AU-7, CA-3, PT-7

拡張管理策：

(1) 組織横断的監査ロギング｜アイデンティティの保持

組織横断的な監査証跡において個人のアイデンティティを保持する。

詳解：アイデンティティの保持は、組織の境界を越えて実行される措置を特定の個人まで追跡できる必要がある場合に適用される。

関連管理策：IA-2, IA-4, IA-5, IA-8

(2) 組織横断的監査ロギング｜監査情報の共有

[*設定：組織が定める組織間共有合意*]に基づいて、組織横断的な監査情報を[*設定：組織が定める組織*]に提供する。

詳解：監査情報は分散しているため、実施されている監査を効果的に分析するためには、組織横断的な監査情報の共有が不可欠な場合がある。例えば、ある組織の監査記録は、他の組織の個人による組織情報リソースの適切または不適切な使用を判断するのに十分な情報を提供できない可能性がある。場合によっては、そのような判断をするための適切な知識を持っているのは、個人の所属組織だけであるため、組織間で監査情報を共有する必要がある。

関連管理策：IR-4, SI-4

(3) 組織横断的な監査｜分離可能性

組織の境界を越えて伝送される監査情報から個人の関連付けを切り離すために、[*設定：組織が定める手段*]を実装する。

詳解：監査証跡でアイデンティティを保持すると、個人の追跡やプロファイリングが可能になるなど、プライバシーに影響を及ぼす可能性があるが、運用上必要ではない場合がある。これらのリスクは、組織の境界を越えて情報を伝送する際にさらに増幅される可能性がある。プライバシーを強化する暗号技法を実装することで、監査情報から個人の関連付けを切り離し、説明責任を維持しながらプライバシーリスクを軽減することができる。

関連管理策：なし

参照資料：なし

3.4 アセスメント、認可、および監視

アセスメント、認可、および監視の要約表へのクイックリンク

CA-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。

1. 以下の[*選択(1 つ以上):組織レベル;ミッション／事業プロセスレベル;システムレベル*]のアセスメント、認可、および監視のポリシー。

(a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、および準拠に対処する。

(b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに適合している。

2. アセスメント、認可、および監視のポリシーと関連するアセスメント、認可、および監視の管理策の実装を促進するための手順。

b. アセスメント、認可、および監視のポリシーと手順の策定、文書化、および配布することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行のアセスメント、認可、および監視をレビューし、更新する。

1. ポリシーについて[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

2. 手順について[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

詳解:アセスメント、認可、および監視のポリシーと手順は、システムおよび組織で実装されるCA ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に寄与する。したがって、セキュリティおよびプライバシープログラムがアセスメント、認可、および監視のポリシーと手順の策定と連携していることが重要である。セキュリティおよびプライバシープログラムのポリシーと手順を組織レベルで確立することは望ましく、一般的には、ミッションまたはシステム固有のポリシーと手順を不要にすることができる。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映する複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムに対して規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述し、手順の対象である個人または役割向けとすることができる。手順は、システムのセキュリティおよびプライバシー計画の中に、または 1 つ以上の別の文書に文書化することもできる。アセスメント、認可、および監視のポリシーと手順の更新を引き起こす可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれる。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策:PM-9, PS-8, SI-12

拡張管理策:なし

参照資料:[OMB A-130], [SP 800-12], [SP 800-30], [SP 800-37], [SP 800-39], [SP 800-53A], [SP 800-100], [SP 800-137], [SP 800-137A], [IR 8062]

CA-2 管理策アセスメント

管理策:

a. 実施するアセスメントのタイプに応じて、適切なアセッサーまたはアセスメントチームを選択する。

b. 以下を含む、アセスメントの範囲を説明する管理策アセスメント計画を策定する。

1. アセスメント対象となる管理策および拡張管理策。

2. 管理策の有効性を判断するために使用されるアセスメント手順。

3. アセスメント環境、アセスメントチーム、およびアセスメントの役割と責任。

c. アセスメントを実施する前に、管理策アセスメント計画が認可権限のある担当者または指定された代表者によってレビューがなされ、承認されていることを確認する。

d. [*設定:組織が定める頻度*]でシステムおよびその運用環境における管理策のアセスメントを実施し、管理策が正しく実装され、意図されたとおりに運用され、規定されたセキュリティおよびプライバシー要件を満たすことに関して望ましい結果を生み出す範囲を定める。

e. アセスメントの結果を文書化した管理策アセスメント報告書を作成する。

f. 管理策アセスメントの結果を[*設定:組織が定める個人または役割*]に提示する。

詳解:組織は、管理策アセッサーが、効果的なアセスメント計画を策定し、必要に応じて、共通管理策、システム固有管理策、その両方の混ざったハイブリッド管理策、およびプログラムマネジメント(PM)の管理策のアセスメントを実施するために必要なスキルと技術的専門知識を持っていることを確認する。必要なスキルには、リスクマネジメントの概念とアプローチに関する一般的な知識、および実装されたハードウェア、ソフトウェア、ファームウェアのシステムコンポーネントに関する包括的な知識と経験が含まれる。

組織は、初期および現在実施している認可、継続的監視、FISMA の年次アセスメント、システム設計および開発、システムセキュリティエンジニアリング、プライバシーエンジニアリング、およびシステム開発ライフサイクルなどの一部として、システムおよびそれらのシステムが動作する環境における管理策をアセスメントする。アセスメントは、組織が情報セキュリティおよびプライバシー要件を満たし、システム設計および開発プロセスの弱点と欠陥を識別し、認可プロセスの一環としてリスクベースの意思決定を行うために必要な重要な情報を提供し、脆弱性軽減手順に準拠することを保証するのに役立つ。組織は、セキュリティおよびプライバシー計画に文書化されているとおりに、実装された管理策のアセスメントを実施する。アセスメントは、システム開発およびシステムセキュリティエンジニアリング手順の一環として、システム開発ライフサイクル全体にわたって実施することもできる。管理策の設計は、RFP が作成された際、それへの対応がアセスメントされる際、および設計レビューが実施される際にアセスメントできる。管理策を実装するための設計およびその設計に従ってその後の実装が開発中にアセスメントされる場合、最終的な管理策のテストでは、以前に完了した管理策アセスメントを活用して結果を集約する簡単な確認にすることができる。

組織は、システムにおける一つの統合セキュリティおよびプライバシーアセスメント計画を策定、あるいは個別の計画を整備してもよい。統合されたアセスメント計画は、管理策アセスメントにおける役割と責任を明確に描いている。複数の組織がシステムのアセスメントに参加する場合、取り組み方を調整することにより、冗長性と関連コストを削減することができる。

組織は、脆弱性スキャンやシステム監視などの他のタイプのアセスメント活動を適用して、システムのライフサイクル中にシステムのセキュリティとプライバシーの状態を整備することができる。アセスメントの報告に際しては、レポートの的確性および正確性、および管理策が正しく実装され、意図したとおりに機能しているか、要件を満たすことに関して望ましい結果が得られているかどうかを判断するために、組織が必要と考える十分に詳細なアセスメント結果を文書化する。アセスメントの結果は、実施されているアセスメントのタイプとして適切な個人または役割に提供される。例えば、認可の意思決定に関して実施されたアセスメントは、認可権限のある担当者、政府機関のプライバシー保護責任者、政府機関の情報セキュリティ責任者、および指定された認可権限責任者に提供される。

毎年のアセスメント実施要件を満たすために、組織は、初期のまたは現在実施中のシステムにおける様々な認可、継続的監視、システムエンジニアリング手順、またはシステム開発のライフサイクルを通じた活動に関するソースからのアセスメント結果を利用できる。組織は、アセスメント結果が最新であり、管理策の有効性の決定に関連しており、適切なレベルのアセッサーの独立性を得ていることを保証する必要がある。既存の管理策アセスメントの結果は、その結果がまだ有効である限り再利用でき、必要に応じて追加のアセスメントで補足することもできる。初回の認可後は、組織は継続的監視を通じて管理策のアセスメントを実施する。組織はまた、組織の継続的監視戦略に従って、継続的なアセスメントの頻度を設定する。規制当局などの外部組織による監査を含む外部監査は、CA-2 の範囲外である。

関連管理策：AC-20, CA-5, CA-6, CA-7, PM-9, RA-5, RA-10, SA-11, SC-38, SI-3, SI-12, SR-2, SR- 3

拡張管理策：

(1) 管理策アセスメント｜独立したアセッサー

独立したアセッサーまたはアセスメントチームを使用して、管理策アセスメントを実施する。

詳解：独立したアセッサーまたはアセスメントチームは、システムの公平なアセスメントを行う個人またはグループである。公平性とは、アセスメント対象のシステムの開発、運用、維持、または管理、または管理策の有効性の決定に関して、アセッサーが認識された、または実際の利益相反から自由であることを意味する。公平性を達成するために、アセッサーは、アセスメントが行われている組織と相互利益や利益相反を生み出したり、自分の仕事をアセスメントしたり、サービスを提供している組織の管理者や従業員として行動したり、サービスを取得している組織を擁護する立場に置かれたりしない。

独立したアセスメントは、組織内の部署から取得することも、組織外の公共または民間分野のエンティティに委託することもできる。認可権限のある担当者は、システムのセキュリティ分類および／または組織の運営、組織の資産、または個人に対するリスクに基づいて、必要な独立性のレベルを決定する。また、認可権限のある担当者はアセッサーの独立性のレベルが、結果が健全であり、信頼できるリスクベースの判断を行うために使用できるという十分な保証を提供できるかどうかを判断する。アセッサーの独立性の判断には、システムオーナーが契約プロセスに直接関与していないことや、アセスメントを実施するアセッサーの公平性に影響を与えないことなど、契約したアセスメントサービスに十分な独立性があるかどうかが含まれる。システムの設計および開発段階において、独立したアセッサーがいるということは、独立したサブジェクトエキスパート（SME）が設計レビューに関与していることに類似している。

システムを所有する組織が小規模である場合、または組織の構造上、システムオーナーの開発、運用、または管理の連鎖の中にいる個人がアセスメントを実施する必要がある場合、アセスメントプロセスの独立性は、アセスメント結果の、正確性、的確性、完全性、および信頼性を妥当性確認するために、アセスメント結果が専門家による独立したチームによって注意深くレビューおよび分析されることを保証することによって達成できる。認可の判断を支援する以外の目的で実行されるアセスメントは、十分な独立性を持つアセッサーによって実施される場合、そのような判断に使用できる可能性が高く、それによりアセスメントを繰り返す必要性が減少する。

関連管理策：なし

(2) 管理策アセスメント｜特化したアセスメント

[*設定：組織が定める頻度*]で、[*選択：予告済み；抜き打ち*]で行う、[*選択（1 つ以上）：詳細な監視；セキュリティデバイス；自動セキュリティテストケース；脆弱性スキャン；悪意のあるユーザのテスト；インサイダー脅威アセスメント；パフォーマンスおよび負荷テスト；データ漏えいまたはデータ損失のアセスメント；*[*設定：組織が定める他の形式のアセスメント*]]を管理策アセスメントの一部として含める。

詳解：組織は、検証および妥当性確認、システム監視、インサイダー脅威アセスメント、悪意のあるユーザのテスト、その他の形式のテストなど、特化したアセスメントを実施できる。これらのアセスメントは、組織のケイパビリティの演習を通じて、セキュリティとプライバシーを向上させるための措置に焦点を合わせる手段として現在の遂行能力のレベルを示

すことにより、準備態勢を改善することができる。組織は、適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに従って特化したアセスメントを実施する。認可権限のある担当者は、組織のリスク管理部署と連携してアセスメント方法を承認する。組織は、アセスメント中に発見された脆弱性を脆弱性改善プロセスに含めることができる。特化したアセスメントは、システム開発ライフサイクルの初期（例えば、初期設計、開発、ユニットテスト中）に実施することもできる。

関連管理策：PE-3, SI-2

(3) 管理策アセスメント｜外部組織からの結果の活用

アセスメントが［*設定：組織が定める要件*］を満たしている場合、［*設定：組織が定める外部組織*］が［*設定：組織が定めるシステム*］に対して実施した管理策アセスメントの結果を活用する。

詳解：組織は、他の（外部）組織に組織のシステムの管理策アセスメントを依頼できる。そのようなアセスメントを利用し、既存のアセスメントのエビデンスを再利用すると、組織が実行する必要のある独立したアセスメント活動を限定することにより、アセスメントに必要な時間とリソースを減らすことができる。外部組織によるアセスメント結果を受け入れるかどうかを判断する際に組織が考慮する要因は様々である。そのような要因としては、アセスメントを実施した組織との過去の経験、アセスメント組織の評判、提供されたアセスメントのエビデンスの詳細レベル、および適用される法律、大統領令、指令、規則、ポリシー、基準およびガイドラインによって課せられた義務などが含まれる。コモンクライテリア［ISO 15408-1］、NIST 暗号モジュール認証制度（CMVP）、または NIST 暗号アルゴリズム認証制度（CAVP）をサポートする認定試験所は、組織が活用できる独立したアセスメント結果を提供することができる。

関連管理策：SA-4

参照資料：［OMB A-130］, ［FIPS 199］, ［SP 800-18］, ［SP 800-37］, ［SP 800-39］, ［SP 800-53A］, ［SP 800-115］, ［SP 800-137］, ［IR 8011-1］, ［IR 8062］

CA-3 情報交換

管理策：

a. ［*選択（1 つ以上）：相互接続に関するセキュリティ合意書；情報交換に関するセキュリティ合意書;MOU または覚書; サービスレベル合意書（SLA）;ユーザ合意書；秘密保持契約書;［設定：組織が定める合意のタイプ*］］などを使用してシステムと他のシステムとの間の情報交換を承認および管理する。

b. 各情報交換に関する合意の一環として、各システムのインタフェース特性、セキュリティおよびプライバシー要件、管理策、責任、および通信される情報のインパクトレベルなどを文書化する。

c. ［*設定：組織が定める頻度*］で合意書の内容をレビューし、更新する。

詳解：システム情報交換要件は、2 つ以上のシステム間の情報交換に適用される。システム情報交換には、専用線または仮想プライベートネットワークを介した接続、インターネットサービスプロバイダへの接続、データベーストランザクション情報のデータベースの共有または交換、クラウドサービスとの接続および情報交換、ウェブベースのサービスを介した情報交換、またはファイル転送プロトコルを介したファイルの交換、ネットワークプロトコル（IPv4、IPv6 など）、電子メール、またはその他の組織間通信などがある。組織は、セキュリティおよびプライバシーに関する要件や管理策が異なる可能性のある他のシステムと情報交換する際に生ずる可能性のある新たな脅威や増大する脅威に関するリスクを考慮する。これには、同じ組織内のシステムと、組織の外部にあるシステムが含まれる。CA-6(1)または CA-6(2)に記述されているように、システムの情報交換に関する共同認可は、リスクを明らかにするとともにその軽減に役立つ可能性がある。

認可権限のある担当者は、システムの情報交換に関連するリスクおよび、適切なリスク軽減に必要な管理策を規定する。選択される合意のタイプは、交換される情報のインパクトレベル、情報を交換する組織間の関係（例えば、政府から政府、政府から企業、企業から企業、政府また

は企業からサービスプロバイダ、政府または企業から個人へ)、または他のシステムのユーザによる組織システムへのアクセスレベルなどの要因に基づいている。情報交換するシステムが同じ認可権限のある担当者の場合、組織は合意書を結ぶ必要はない。代わりに、システム間のインタフェース特性(例えば、情報がどのように交換されているか、情報がどのように保護されているか)が、それぞれのセキュリティおよびプライバシー計画に記述される。情報交換するシステムは同じ組織内だが認可権限のある担当者が異なる場合、組織は合意書を作成するか、システムのそれぞれのセキュリティおよびプライバシー計画の中で CA-3a から適切な合意のタイプとして規定されるものを提供することができる。組織は、特に連邦政府機関と非連邦政府組織(サービスプロバイダ、契約事業者、システム開発者、システムインテグレータを含む)の間で確立された情報交換のために、正式な契約に合意情報を組み込むことができる。リスクに関する考慮事項には、同じネットワークを共有するシステムが含まれる。

関連管理策: AC-4, AC-20, AU-16, CA-6, IA-3, IR-4, PL-2, PT-7, RA-3, SA-9, SC-7, SI-12

拡張管理策:

(1) システム接続 | 非機密国家安全保障システムの接続

[撤回: SC-7(25)に移動した]

(2) システム接続 | 国家機密安全保障システムの接続

[撤回: SC-7(26)に移動した]

(3) システム接続 | 非機密非国家安全保障システムの接続

[撤回: SC-7(27)に移動した]

(4) システム接続 | パブリックネットワークへの接続

[撤回: SC-7(28)に移動した]

(5) システム接続 | 外部システム接続の制限

[撤回: SC-7(5)に移動した]

(6) 情報交換 | 転送の認可

相互接続するシステム間でデータを転送する個人またはシステムが、そのようなデータを受け入れる前に、必要な認可(つまり、書き込み許可または特権)を受けていることを確認する。

詳解: 認可されていない個人およびシステムが保護されたシステムに情報を転送することを防止するために、保護されたシステムは、独立した手段によって、情報を転送しようとする個人またはシステムがそうすることが認可されているかどうかを検証する。情報を転送することの認可の検証は、コントロールプレーンにおけるトラフィック(ルーティングや DNS など)およびサービス(認証済み SMTP リレーなど)にも適用される。

関連管理策: AC-2, AC-3, AC-4

(7) 情報交換 | 推移的(transitive)情報交換

(a) CA-3a で識別されたシステムを通じて他のシステムとの推移的(下流の)情報交換を識別する。

(b) 識別された推移的(下流の)システムの管理策を検証または妥当性確認できない場合、推移的(下流の)情報交換が停止することを確実にするための措置を講ずる。

詳解: 推移的または「下流へ」の情報交換は、組織のシステムが情報交換するシステムおよび他のシステムとの間の情報交換である。高価値の資産を含む、ミッションクリティカルなシステム、サービス、およびアプリケーションの場合、そのような情報交換を識別する必要がある。組織のシステムに直接または間接的に接続されたそのような下流のシステムで導入されている管理策または保護措置の透明性は、それらの情報交換から生じるセキュリティおよびプライバシーリスクを理解するために不可欠である。組織のシステムは、推移的な接続や情報交換を通じて下流のシステムからリスクを引き継ぐことがあるため、組織のシステムは、脅威、危険、および有害なインパクトなどを受けやすくなる可能性があ

る。

関連管理策：SC-7

参照資料：[OMB A-130], [FIPS 199], [SP 800-47]

CA-4 セキュリティ証明書

［撤回：CA-2 に組み込まれた］

CA-5 実施計画およびマイルストーン

管理策：

a. 管理策のアセスメントの中で指摘された弱点または欠陥を修正し、システムの既知の脆弱性を軽減または排除するために、組織の計画された是正措置を文書化するためのシステムの実施計画およびマイルストーンを作成する。

b. 管理策アセスメント、個々の監査またはレビュー、および継続的監視活動からの知見に基づいて、［*設定：組織が定める頻度*］で既存の実施計画およびマイルストーンを更新する。

詳解：実施計画およびマイルストーンは、どのようなタイプの組織においても、計画された是正措置を追跡するのに役立つ。実施計画およびマイルストーンは、認可対策に必要であり、行政予算管理局（OMB）によって制定された連邦政府の報告要件に従う。

関連管理策：CA-2, CA-7, PM-4, PM-9, RA-7, SI-2, SI-12

拡張管理策：

(1) 実施計画およびマイルストーン｜的確性および最新性サポートの自動化

［*設定：組織が定める自動化のメカニズム*］を使用して、システムの実施計画およびマイルストーンの的確性、最新性、可用性を確保する。

詳解：自動化されたツールを使用すると、実施計画およびマイルストーンの的確性、最新性、可用性を維持し、組織全体のセキュリティ情報とプライバシー情報の調整と共有が容易になる。このような調整と情報共有は、組織のシステムにおけるシステムの弱点または欠陥を識別し、適切なリソースがシステムの脆弱性の最も重大な箇所にタイムリーに配分されることに役立つ。

関連管理策：なし

参照資料：[OMB A-130], [SP 800-37]

CA-6 認可

管理策：

a. システムの認可責任者を任命する。

b. 組織のシステムによる継承に利用可能な共通管理策の認可責任者を任命する。

c. 運用を開始する前に、システムの認可権限のある担当者が以下を行うことを確認する。

1. システムが継承した共通管理策の使用を受け入れる。

2. システムが運用することを認可する。

d. 共通管理策の認可権限のある担当者が、組織のシステムによる継承のためのそれらの管理策の使用を認可することを確認する。

e. ［*設定：組織が定める頻度*］で認可を更新する。

詳解：ここでいう認可とは、システムの運用を認可し、組織のシステムによる継承のための共通管理策の使用を認可し、合意された管理策の実施に基づいて組織の運営と資産、個人、他の組織、および国家に対するリスクを明示的に受け入れるための、責任者による公式の管理上

の意思決定のことである。認可権限のある担当者は、組織のシステムと共通管理策の予算管理を行う、あるいはそれらのシステムまたは共通管理策によってサポートされるミッションおよび事業機能に対して責任を負う。認可のプロセスは連邦政府の責任であるため、認可権限のある担当者は連邦政府職員でなければならない。認可権限のある担当者は、組織のシステムの運用と使用に関連するセキュリティおよびプライバシーのリスクに対する責任と説明責任を負う。非連邦政府組織は、認可の役割と関連する責任を負うシステムおよび責任者を認可するための同様のプロセスを有することがある。

認可権限のある担当者は、実施された継続的監視プログラムから作成されたエビデンスに基づいて、システムの現在実施中の認可を発行する。堅牢な継続的監視プログラムは、個別の再認可プロセスの必要性を減少する。包括的な継続的監視プロセスを採用することにより、認可対策に含まれる情報（すなわち、セキュリティおよびプライバシー計画、アセスメントレポート、ならびに実施計画およびマイルストーン）が継続的に更新される。これにより、認可権限のある担当者、共通管理策の提供者、およびシステムオーナーは、システム、管理策、および運用環境のセキュリティとプライバシーの最新状況を知ることができる。再認可のコストを削減するために、認可権限のある担当者は、継続的監視プロセスの結果を、再認可の意思決定を下すための基礎として可能な限り活用することができる。

関連管理策：CA-2, CA-3, CA-7, PM-9, PM-10, RA-3, SA-10, SI-12

拡張管理策：

(1) 認可 | 共同認可 — 組織内

認可を実施する同じ組織からの複数の認可権限のある担当者を含むシステムの共同認可プロセスを採用する。

詳解：同じ組織の複数の認可権限のある担当者をシステムの共同認可権限のある担当者として任命すると、リスクベースの意思決定プロセスの独立性が高まる。これは、システムの認可プロセスに適用される職務分掌および二重認可の概念も実装することにもなる。組織内の共同認可プロセスは、接続されたシステム、共有システム、および複数の情報オーナーがいるシステムに最も適切である。

関連管理策：AC-6

(2) 認可 | 共同認可 — 組織間

複数の認可権限のある担当者と、認可を実施する組織外の組織の少なくとも 1 人の認可権限のある担当者を含む、システムの共同認可プロセスを採用する。

詳解：複数の認可権限のある担当者を、少なくとも 1 人は外部組織の出身者として、システムの共同認可権限のある担当者として任命することで、リスクベースの意思決定プロセスの独立性が高まる。また、システム認可プロセスに適用される職務分掌および二重認可の概念を実装する。外部組織が認可に関する意思決定の結果に既得権または株式を有する場合、システムを所有またはホストする組織の認可権限のある担当者を補うために外部組織の認可権限のある担当者を任命することが必要となる場合がある。組織間の共同認可プロセスは、接続されたシステム、共有システムまたはサービス、および複数の情報オーナーを有するシステムには適切である。外部組織からの認可権限のある担当者は、認可を受けるシステムの主要な経営行動等における利害関係者である。

関連管理策：AC-6

参照資料：[OMB A-130], [SP 800-37], [SP 800-137]

CA-7 継続的監視

管理策：下記を含む、システムレベルの継続的監視戦略を策定し、組織レベルの継続的監視戦略に従って継続的監視を実装する。

a. 監視対象となる[*設定：組織が定めるシステムレベルの指標*]の確立。

b. 監視の[*設定：組織が定める頻度*]および管理策の有効性アセスメントの[*設定：組織が定める頻度*]の確立。

c. 現在実施中の監視戦略に基づく継続的な管理策アセスメント。

d. 現在実施中の監視戦略に従った、システムおよび組織が定める指標の継続的な監視。

e. 管理策アセスメントと監視によって生成された情報の相関と分析。

f. 管理策アセスメントおよび監視情報の分析結果に対処するための対応措置。

g. システムのセキュリティおよびプライバシーの状態を[*設定:組織が定める頻度*]で[*設定:組織が定める職員または役割*]に報告すること。

詳解:システムレベルでの継続的監視により、現在実施中のシステムのセキュリティおよびプライバシーの態勢を認識し、組織のリスクマネジメントの意思決定をサポートできる。「継続的」および「現在実施中の」という用語は、組織がリスクベースの意思決定を支援するのに十分な頻度でその管理策およびリスクをアセスメントおよび監視することを意味する。異なるタイプの管理策は、異なる監視頻度を必要とする場合がある。継続的監視の結果は、組織によるリスク対応措置を生み出す。ケイパビリティにグループ化された複数の管理策の有効性を監視する場合、失敗した管理策を特定するために根本原因の分析が必要になる場合がある。継続的監視プログラムにより、組織は、ミッションおよび事業のニーズ、脅威、脆弱性、および技術が変化する非常に動的な運用環境において、システムと共通管理策の認可を維持することができる。レポートおよびダッシュボードを介してセキュリティおよびプライバシー情報に継続的にアクセスできるため、組織の担当者は、現在実施中の認可に関する判断を含め、効果的かつタイムリーなリスクマネジメントの意思決定を行うことができる。

自動化は、ハードウェア、ソフトウェア、およびファームウェアのインベントリ、認可対策、およびその他のシステム情報のより頻繁な更新をサポートする。継続的監視機能の出力が特定の測定可能な実用的な関連性のあるタイムリーな情報を提供するようにフォーマットされている場合、効果はさらに高まる。継続的監視活動は、システムのセキュリティ分類に従って増減される。特定の監視の必要性を含む監視要件は、AC-2g, AC-2(7), AC-2(12)(a), AC-2(7)(b), AC-2(7)(c), AC-17(1), AT-4a, AU-13, AU-13(1), AU-13(2), CM-3f, CM-6d, CM-11c, IR-5, MA-2b, MA-3a, MA-4a, PE-3d, PE-6, PE-14b, PE-16, PE-20, PM-6, PM-23, PM-31, PS-7e, SA-9c, SR-4, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b および SI-4 などの他の管理策および拡張管理策で参照される場合がある。

関連管理策:AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PM-31, PS-7, PT-7, RA-3, RA-5, RA-7, RA-10, SA-8, SA-9, SA-11, SC-5, SC-7, SC-18, SC-38, SC-43, SI-3, SI-4, SI-12, SR-6

拡張管理策:

(1) 継続的監視 | 独立したアセスメント

独立したアセッサーまたはアセスメントチームを採用して、システムの管理を継続的に監視する。

詳解:組織は、適切なレベルの独立性を持つアセッサーがアセスメントを実施することを要求することにより、管理策アセスメントの価値を最大化できる。必要な独立性のレベルは、組織の継続的監視戦略に基づいている。アセッサーの独立性は、監視プロセスにある程度の公平性を提供する。そのような公平性を達成するために、アセッサーは、アセスメントが行われている組織との相互利益または相反する利益を生み出したり、自身の担当した仕事をアセスメントしたり、彼らがサービスを提供している組織の経営者または従業員として行動したり、サービスを取得する組織を擁護する立場に身を置いたりしない。

関連管理策:なし

(2) 継続的監視 | アセスメントのタイプ

[撤回:CA-2 に組み込まれた]

(3) 継続的監視 | トレンド分析

トレンド分析を採用して、管理策の実施、継続的監視活動の頻度、および継続的監視プロセスで使用される活動のタイプを、経験的データに基づいて修正する必要がある

かどうかを判断する。

詳解:トレンド分析には、組織または連邦政府内で発生した脅威に関するイベントのタイプ、特定のタイプの攻撃の成功率、技術分野における新たな脆弱性、進化するソーシャルエンジニアリング技法、構成設定の効果、複数の管理策アセスメント結果、および監察官または監査人の所見などに対処する最近の脅威情報の調査が含まれる。

関連管理策:なし

(4) 継続的監視 | リスク監視

リスク監視が、以下を含む継続的監視戦略の不可欠な部分であることを確認する。

(a) 有効性の監視。

(b) 準拠の監視。

(c) 変更の監視。

詳解:リスク監視は規定された組織のリスク許容度によって通知される。有効性の監視は、実装された現在実施中のリスク対応措置の有効性を決定する。準拠の監視は、必要なリスク対応措置が実施されていることを検証する。また、セキュリティおよびプライバシーの要件が満たされていることも確認する。変更を監視することで、セキュリティおよびプライバシーのリスクに影響を与える可能性のある組織のシステムおよび運用環境の変更を識別できる。

関連管理策:なし

(5) 継続的監視 | 一貫性の分析

[*設定:組織が定める措置*]を適用して、ポリシーが確立され、実装されている管理策が一貫した方法で運用されていることを妥当性確認する。

詳解:セキュリティおよびプライバシーの管理策は、システムに段階的に追加されることがよくある。その結果、管理策の選択および実装のポリシーに一貫性がなくなり、管理策が一貫した方法または調整された方法で連携できない場合が生ずる。少なくとも、一貫性と調整の欠如は、システムに許容できないセキュリティおよびプライバシーのギャップがあることを意味している。最悪の場合、ある部位またはコンポーネントによって実装された管理策の一部が、他の管理策の機能を実は妨げているということを意味する可能性がある(例えば、内部ネットワークトラフィックの暗号化が監視を妨げる可能性がある)。もしくは、実装されているすべてのネットワークプロトコル(IPv4 と IPv6 のデュアルスタックなど)を一貫して監視できないと、システムに意図しない脆弱性が発生し、敵対者に悪用される可能性がある。テスト、監視、および分析を通じて、実装された管理策が一貫性のある、調整された、干渉しない方法で動作していることを妥当性確認することが重要である。

関連管理策:なし

(6) 継続的監視 | 監視サポートの自動化

[*設定:組織が定める自動化のメカニズム*]を使用して、システムの監視結果の的確性、最新性、可用性を確保する。

詳解:自動化された監視ツールを使用すると、監視情報の的確性、最新性、可用性を維持するのに役立ち、組織のリスクマネジメントの意思決定を支援するために、システムのセキュリティおよびプライバシーに対する意識の継続的な認識レベルを高めるのに役立つ。

関連管理策:なし

参照資料:[OMB A-130], [SP 800-37], [SP 800-39], [SP 800-53A], [SP 800-115],[SP 800-137], [IR 8011-1], [IR 8062]

CA-8 侵入テスト

管理策:[*設定:組織が定める頻度*]で[*設定:組織が定めるシステムまたはシステムコンポーネント*]に対して侵入テストを実施する。

詳解：侵入テストは、敵対者が悪用する可能性のある脆弱性を識別するために、システムまたは個々のシステムコンポーネントに対して実施される特別なタイプのアセスメントである。侵入テストは、自動化された脆弱性スキャンにとどまらず、ネットワーク、オペレーティングシステム、アプリケーションレベルのセキュリティなどの技術的専門知識を含む実証可能なスキルと経験を持つエージェントとチームによって実施される。侵入テストを使用して、脆弱性を検証したり、指定された制約内でのシステムに対する敵対者の侵入抵抗の程度を判断することができる。そのような制約には、時間、リソース、およびスキルが含まれる。侵入テストは、敵対者の行動を再現することを試み、セキュリティおよびプライバシー関連の弱点または欠陥のより詳細な分析を行う。侵入テストは、組織が古い技術から新しい技術に移行する場合（例えば、IPv4 から IPv6 ネットワークプロトコルに移行する場合）に特に重要である。

組織は、脆弱性分析の結果を使用して、侵入テスト活動をサポートできる。侵入テストは、システムのハードウェア、ソフトウェア、またはファームウェアのコンポーネントに対して内部または外部から実施でき、物理的および技術的な管理策の両方に対して適用することができる。侵入テストの標準的な方法には、システムの完全な知識に基づく事前テスト分析、事前テスト分析に基づく潜在的な脆弱性の事前テスト識別、および脆弱性を悪用する可能性を判断するために設計されたテストなどが含まれる。すべての当事者は、侵入テストのシナリオを開始する前に、交戦規定（ROE：Rules of engagement）に同意する。組織は、侵入テストの交戦規定を、敵対者によって採用されることが予想されるツール、技法、および手順と相互に関連付ける。侵入テストでは、テストを実施する個人に対して、法律または規則によって保護されている情報が漏えいする可能性がある。交戦規定、契約、またはその他の適切なメカニズムを仕様して、この情報を保護する方法に対する期待を伝えることができる。リスクアセスメントは、侵入テストを実施する職員に必要な独立性のレベルに関する判断の手引きとなる。

関連管理策：RA-5, RA-10, SA-11, SR-5, SR-6

拡張管理策：

(1) 侵入テスト | 独立した侵入テストエージェントまたはチーム

独立した侵入テストエージェントまたはチームを利用して、システムまたはシステムコンポーネントの侵入テストを実行する。

詳解：独立した侵入テストエージェントまたはチームは、組織のシステムの公平な侵入テストを実施する個人またはグループである。公平性とは、侵入テストのエージェントまたはチームが、侵入テストの標的となるシステムの開発、運用、または管理に関する知見がない、または実際の利益相反がないことを意味する。CA-2(1)は、侵入テストに適用できる独立したアセスメントに関する追加情報を提供する。

関連管理策：CA-2

(2) 侵入テスト | レッドチーム演習

適用可能な交戦規定に従って組織のシステムを危険にさらすための敵対者による試みを模擬するために、[*設定：組織が定めるレッドチーム演習*]を採用する。

詳解：レッドチーム演習は、組織のセキュリティとプライバシーに関する態勢、および効果的なサイバー防御を実装するケイパビリティを調べることで、侵入テストの目的を拡張できる。レッドチーム演習は、ミッションおよび事業機能を危険にさらすための敵対者による試みを模擬し、システムおよび組織のセキュリティおよびプライバシー態勢の包括的なアセスメントを提供する。そのような試みには、テクノロジーベースの攻撃やソーシャルエンジニアリングベースの攻撃を含めることがある。テクノロジーベースの攻撃には、ハードウェア、ソフトウェア、またはファームウェアのコンポーネントおよび／またはミッションおよび事業プロセスとの相互作用などが含まれる。ソーシャルエンジニアリングベースの攻撃には、電子メール、電話、ショルダーサーフィン、または個人的な会話を介した相互作用が含まれる。レッドチーム演習は、侵入テストのエージェントと、現在の敵対的な戦術、技法、手順、およびツールに関する知識と経験を持つチームが実施する場合に最も効果的である。侵入テストは主として実験室ベースのテストであるが、組織は、実際の状況を反映したより包括的なアセスメントを行うために、レッドチーム演習を導入することができる。レッドチーム演習の結果は、組織がセキュリティおよびプライバシーの意識向上およびトレーニングを改善し、管理策の有効性をアセスメントするために使用できる。

関連管理策：なし

(3) 侵入テスト｜施設への侵入テスト

[*設定：組織が定める頻度*]で[*選択：予告済み；予告なし*]での施設への物理的なアクセスポイントに関連する管理策を迂回または回避する試みを含む侵入テストプロセスを採用する。

詳解：物理的アクセスポイントの侵入テストは、組織のシステムの運用環境における重大な脆弱性に関する情報を提供することができる。このような情報は、組織のシステムを保護するために必要な物理的管理策の弱点や欠陥を修正するために使用できる。

関連管理策：CA-2, PE-3

参照資料：なし

CA-9 内部システム接続

管理策：

a. システムへの[*設定：組織が定めるシステムコンポーネントまたはコンポーネントのクラス*]の内部接続を認可する。

b. 内部接続ごとに、インタフェースの特性、セキュリティおよびプライバシーの要件、および通信される情報の性質を文書化する。

c. [*設定：組織が定める条件*]後に内部システム接続を終了させる。

d. 各内部接続の継続的な必要性については、[*設定：組織が定める頻度*]でレビューする。

詳解：内部システム接続とは、システム開発に使用されるコンポーネントを含む、組織のシステムと個別の構成システムコンポーネント間の接続（つまり、同じシステムの一部であるコンポーネント間の接続）のことである。システム内接続には、モバイルデバイス、ノートブックおよびデスクトップコンピュータ、タブレット、プリンタ、コピー機、ファクシミリ装置、スキャナ、センサ、およびサーバとの接続などが含まれる。組織は、各内部システム接続を個別に認可する代わりに、特定の処理、伝送、保存ケイパビリティを備えたプリンタ、スキャナ、コピー機、または特定のベースライン構成を備えたスマートフォンやタブレットなど、共通の特性および／または構成を持つシステムコンポーネントのクラスの内部接続を認可することができる。内部システム接続の継続的な必要性については、組織のミッションまたは事業機能をサポートするかどうかの観点からレビューされる。

関連管理策：AC-3, AC-4, AC-18, AC-19, CM-2, IA-3, SC-7, SI-12

拡張管理策：

(1) 内部システム接続｜準拠の確認

内部接続を確立する前に、構成するシステムコンポーネントのセキュリティおよびプライバシーに関する準拠を確認する。

詳解：準拠の確認には、関連するベースライン構成の検証が含まれる。

関連管理策：CM-6

参照資料：[SP 800-124], [IR 8023]

3.5 構成管理

構成管理の要約表へのクイックリンク

CM-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。
   1. 以下の[*選択(1 つ以上):組織レベル;ミッション/事業プロセスレベル;システムレベル*]の構成管理のポリシー。
      (a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、および準拠に対処する。
      (b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに適合している。
   2. 構成管理のポリシーと関連する構成管理の管理策の実装を促進するための手順。

b. 構成管理のポリシーと手順の策定、文書化、および配布することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行の構成管理をレビューし、更新する。
   1. ポリシーについて[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。
   2. 手順について[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

詳解:構成管理のポリシーと手順は、システムおよび組織で実装される CM ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に寄与する。したがって、セキュリティおよびプライバシープログラムが構成管理のポリシーと手順の策定と連携していることが重要である。セキュリティおよびプライバシープログラムのポリシーと手順を組織レベルで確立することは望ましく、一般的には、ミッションまたはシステム固有のポリシーと手順を不要にすることができる。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映する複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムに対して規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述し、手順の対象である個人または役割向けとすることができる。手順は、システムのセキュリティおよびプライバシー計画の中に、または 1 つ以上の別の文書に文書化することもできる。構成管理のポリシーと手順の更新を引き起こす可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれるが、これらに限定されない。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策:PM-9, PS-8, SA-8, SI-12

拡張管理策:なし

参照資料:[OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100]

CM-2 ベースライン構成

管理策:

a. システムの現在のベースライン構成を構成変更管理下で作成、文書化し、維持する。

b. システムのベースライン構成をレビューし、更新する。

1. [*設定:組織が定める頻度*]で。

2. [*設定:組織が定める状況*]により必要な場合。

3. システムコンポーネントがインストールまたはアップグレードされたとき。

詳解:システムおよびシステムコンポーネントのベースライン構成には、システムの接続性、運用上の、および通信の側面がある。ベースライン構成は文書化され、公式なレビューがなされ、システムまたはそれらのシステム内の構成アイテムの仕様が合意される。ベースライン構成には、セキュリティおよびプライバシーの管理策の実装、運用手順、システムコンポーネントに関する情報、ネットワーク構成、およびシステムアーキテクチャ内のコンポーネントの論理的な配置などを含んでおり、システムの将来の構築、リリース、または変更の基礎として機能する。ベースライン構成を維持するには、組織のシステムが時間とともに変化するにつれて、新しいベースラインを作成する必要がある。システムのベースライン構成は、現在のエンタープライズアーキテクチャを反映している。

関連管理策:AC-19, AU-6, CA-9, CM-1, CM-3, CM-5, CM-6, CM-8, CM-9, CP-9, CP-10, CP-12, MA-2, PL-8, PM-5, SA-8, SA-10, SA-15, SC-18

拡張管理策:

(1) ベースライン構成 | レビューおよび更新

[撤回:CM-2 に組み込まれた]

(2) ベースライン構成 | 的確性および最新性サポートの自動化

[*設定:組織が定める自動化のメカニズム*]を使用して、システムのベースライン構成の最新性、正確性、的確性、可用性を維持する。

詳解:組織がシステムの一貫したベースライン構成を維持するのに役立つ自動化のメカニズムには、構成管理ツール、ハードウェア、ソフトウェア、ファームウェアインベントリツール、ネットワーク管理ツールなどがある。自動化ツールは、ワークステーション、サーバ、ノートブックコンピュータ、ネットワークコンポーネント、またはモバイルデバイスの組織レベル、ミッションおよび事業プロセスレベル、またはシステムレベルで使用することができる。ツールを使用して、オペレーティングシステム、アプリケーション、インストールされているソフトウェアのタイプ、および現在のパッチレベルのバージョン番号を追跡できる。的確性と最新性サポートの自動化は、システムコンポーネントインベントリおよびベースライン構成に関する活動を組み合わせる組織向けの CM-8(2)の実装によって満たすことができる。

関連管理策:CM-7, IA-3, RA-5

(3) ベースライン構成 | 過去の構成の保持

ロールバックをサポートするために、システムのベースライン構成に関する[*設定:組織が定める回数*]分の過去のバージョンを保持する。

詳解:ロールバックをサポートするために過去のバージョンのベースライン構成を保持するものとしては、ハードウェア、ソフトウェア、ファームウェア、構成ファイル、構成記録、および関連文書が含まれる。

関連管理策:なし

(4) ベースライン構成 | 認可されていないソフトウェア

[撤回:CM-7(4)に組み込まれた]

(5) ベースライン構成 | 認可されたソフトウェア

[撤回:CM-7(5)に組み込まれた]

(6) ベースライン構成 | 開発およびテスト環境

運用中のベースライン構成とは別に管理されている、システム開発およびテスト環境用のベースライン構成を維持する。

詳解：開発、テスト、および運用環境用に個別のベースライン構成を確立することで、開発およびテスト活動に関連する計画外または予期しないイベントからシステムを保護することができる。個別のベースライン構成により、組織は構成のタイプごとに最適な構成管理を適用できる。例えば、運用環境の構成管理では通常、安定性の必要性が強調されるが、開発やテスト環境の構成管理にはより高い柔軟性が必要となる。テスト環境の構成は、実行可能な範囲で運用環境の構成を反映しているため、テストの結果は、運用システムに対して提案された変更を代表している。個別のベースライン構成は、必ずしも個別の物理環境を必要としていない。

関連管理策：CM-4, SC-3, SC-7

(7) ベースライン構成 | 高リスク領域のシステムおよびコンポーネントの構成

(a) 組織が大きなリスクがあると見なす場所に移動する個人に[*設定：組織が定める構成*]を持つ[*設定：組織が定めるシステムまたはシステムコンポーネント*]を用意する。

(b) 個人が移動先から戻ったときに、システムまたはコンポーネントに[*設定：組織が定める管理策*]を適用する。

詳解：システムまたはシステムコンポーネントが組織の外部のリスクの高い場所にあることがわかっている場合、そのような場所で増大する脅威に対抗するために追加の管理策を実装することができる。例えば、組織は、そうした場所に出入りする個人が使用するノートパソコンに対して様々な措置を取ることができる。措置には、懸念のある場所の特定、コンポーネントに必要な構成の規定、移動前にコンポーネントが意図したとおりに構成されていることの確認や移動完了後のコンポーネントへの管理策の適用などがある。特別に構成されたノートブックコンピュータとしては、サニタイズされたハードドライブ、限定されたアプリケーション、およびより厳密な構成設定をしたコンピュータなどが含まれる。移動先から戻ったときにモバイルデバイスに適用される管理策としては、物理的な改ざんの兆候がないかどうかモバイルデバイスを検査し、ディスクドライブの情報を消去して再書き込みすることなどが含まれる。モバイルデバイスに存在する情報の保護は、MP（媒体保護）ファミリーで対処される。

関連管理策：MP-4, MP-5

参照資料：[SP 800-124], [SP 800-128]

CM-3 構成変更管理

管理策：

a. 構成変更管理されているシステムの変更のタイプを特定し、文書化する。

b. システムに対して提案されている構成変更管理された変更をレビューし、セキュリティとプライバシーへの系統立てられたインパクト分析を行った上で、そのような変更を承認または不承認にする。

c. システムに関連する構成変更の判断を文書化する。

d. 承認された構成変更管理された変更をシステムに実装する。

e. システムへの構成変更管理に関する変更の記録を[*設定：組織が定める期間*]保持する。

f. システムに対する構成変更管理に関する変更に伴う活動を監視し、レビューする。

g. [*選択：（1 つ以上）：[設定：組織が定める頻度]；[設定：組織が定める構成変更の条件]が生じた場合*]に招集する[*設定：組織が定める構成変更管理部署*]を通じて、構成変更管理活動を調整し、監視する。

詳解：組織のシステムの構成変更管理には、システムのアップグレードや変更を含むシステム

変更に関する手続に沿った企画、正当性の確認、実装、テスト、レビュー、および廃棄などが含まれる。構成変更管理には、ベースライン構成の変更、システムの構成アイテム、運用手順、システムコンポーネントの構成設定、脆弱性の修正、および予定外の変更や認可されていない変更などが含まれる。システムの構成変更管理には、構成変更管理委員会または変更諮問委員会などによる提案された変更のレビューおよび承認を行うプロセスが含まれる。プライバシーリスクにインパクトを与える変更については、政府機関のプライバシー保護責任者がプライバシー影響評価と記録システム通知を更新する。新しいシステムまたは主要なアップグレードの場合、組織は、構成変更管理委員会または変更諮問委員会に開発組織の代表者を含めることを考慮する。変更の監査には、システムに変更が加えられる前後の活動と、そのような変更を実装するために必要な監査活動が含まれる。SA-10 も参照。

関連管理策：CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, CM-11, IA-3, MA-2, PE-16, PT-6, RA-8, SA-8, SA-10, SC-28, SC-34, SC-37, SI-2, SI-3, SI-4, SI-7, SI-10, SR-11

拡張管理策：

(1) 構成変更管理 | 自動化された文書化、通知、および変更禁止

[*設定：組織が定める自動化のメカニズム*]を使用して、次のことを行う。

(a) システムに提案された変更を文書化する。

(b) [*設定：組織が定める承認機関*]にシステムに提案された変更を通知し、変更の承認を要求する。

(c) [*設定：組織が定める期間*]内に承認または不承認とされていない、システムに対して提案された変更について目立つように表示する。

(d) 指定された承認が受けられるまで、システムへの変更を禁止する。

(e) システムに対するすべての変更を文書化する。

(f) システムへの承認された変更が完了した場合、[*設定：組織が定める職員*]に通知する。

詳解：なし

関連管理策：なし

(2) 構成変更管理 | 変更のテスト、妥当性確認、および文書化

変更の実装を完了する前に、システムへの変更をテスト、妥当性確認、および文書化する。

詳解：システムの変更には、CM-6 で規定されたハードウェア、ソフトウェア、またはファームウェアのコンポーネントおよび構成設定の変更が含まれる。組織は、テストが組織のミッションおよび事業機能をサポートするシステム運用に干渉しないようにする。テストを実施する個人またはグループは、セキュリティとプライバシーのポリシーと手順、システムのセキュリティおよびプライバシーのポリシーと手順、特定の施設またはプロセスに関連する健全性、安全性、および環境におけるリスクを理解する。運用システムは、テストを実施する前に、オフラインにするか、可能な範囲で複製する必要がある場合がある。テストのためにシステムをオフラインにする必要がある場合、テストは、可能な限り、計画されたシステム停止期間中に実行されるようにスケジュールする。運用システムでテストを実施できない場合、組織は代替管理策を採用する。

関連管理策：なし

(3) 構成変更管理 | 自動化された変更措置の反映

[*設定：組織が定める自動化のメカニズム*]を使用して、現在のシステムベースラインに変更措置を反映し、更新されたベースラインを導入されている拠点全体に展開する。

詳解：自動化ツールは、構成ベースライン情報の的確性、一貫性、可用性を向上させることができる。自動化は、データの集約およびデータ相関ケイパビリティ、アラートのメカニズム、およびダッシュボードを提供して、組織内のリスクベースの意思決定をサポートすることもできる。

関連管理策：なし

(4) 構成変更管理 | セキュリティおよびプライバシーに関する代表者

[*設定：組織が定めるセキュリティおよびプライバシーに関する代表者*]は[*設定：組織が定める構成変更管理部署*]のメンバーであることが求められる。

詳解：情報セキュリティおよびプライバシーに関する代表者には、システムセキュリティ責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、またはシステムプライバシー責任者などが含まれる。システム構成への変更は、その一部はセキュリティまたはプライバシーに関連する可能性があり、意図しない制限をもたらす可能性があるため、情報セキュリティおよびプライバシーの専門知識を持つ職員による代表者の参加が重要である。プロセスの早い段階でそのような変更を検知することは、システムのセキュリティおよびプライバシーの態勢に最終的に影響する可能性のある、意図しない悪影響を回避するのに役立つ。組織が定めるパラメータの2番目で参照されている構成変更管理部署については、CM-3g で組織によって定められた変更管理部署を反映している。

関連管理策：なし

(5) 構成変更管理 | 自動化されたセキュリティ対応

ベースライン構成が認可を受けずに変更された場合、自動的な[*設定：組織が定めるセキュリティ対応*]を行う機能を実装する。

詳解：構成アイテムの認可されていない変更があった場合の自動化されたセキュリティ対応には、選択されたシステム機能の停止、システム処理の停止、組織の職員へのアラートまたは通知の発行などがある。

関連管理策：なし

(6) 構成変更管理 | 暗号技術による管理

[*設定：組織が定める管理策*]に使用される暗号化のメカニズムが構成管理下にあることを確実にする。

詳解：拡張管理策で参照される管理策は、管理策カタログのセキュリティおよびプライバシー管理策を参照している。採用された暗号化のメカニズムに関係なく、それらのメカニズムを管理するためのプロセスと手順は導入される。例えば、システムコンポーネントが識別と認証に証明書を使用する場合には、それらの証明書の有効期限に対処するためのプロセスが実装されている。

関連管理策：SC-12

(7) 構成変更管理 | システム変更のレビュー

[*設定：組織が定める頻度*]または[*設定：組織が定める状況*]となった場合、システムへの変更をレビューし、認可されていない変更が発生したかどうかを判断する。

詳解：システムへの変更のレビューを正当化する指摘、およびそのようなレビューを正当化する特定の状況は、構成変更プロセスまたは継続的監視プロセスの間に組織が実施する活動から得ることができる。

関連管理策：AU-6, AU-7, CM-3

(8) 構成変更管理 | 構成変更の防止または制限

[*設定：組織が定める状況*]の場合には、システムの構成への変更を防止または制限する。

詳解：システム構成の変更は、重要なシステムセキュリティとプライバシー機能に悪影響を及ぼす可能性がある。変更の制限は、自動化されたメカニズムによって実施できる。

関連管理策：なし

参照資料：[SP 800-124], [SP 800-128], [IR 8062]

CM-4 インパクト分析

管理策：システムの変更を分析し、変更を実施する前に、潜在的なセキュリティとプライバシーへのインパクトを判断する。

詳解：セキュリティまたはプライバシーの責任者である組織の職員がインパクト分析を実施する。インパクト分析を実施する個人にはシステムへの変更とセキュリティまたはプライバシーへのインパクトを分析するために必要なスキルと技術的専門知識が求められる。インパクト分析には、管理策要件を理解するためのセキュリティおよびプライバシー計画、ポリシー、手順をレビューすること、システム設計文書および運用手順をレビューし、管理策の実装および特定のシステムの構成変更が管理策にどのようにインパクトを与えるかを理解すること、経営行動等における利害関係者と組織のサプライチェーンパートナーに対する変更のインパクトをレビューすること、ならびに、システムへの潜在的な変更が個人のプライバシーおよびそれらのリスクを軽減するために実装された管理策の能力に新たなリスクをどのように生み出すかを判断することなどが含まれる。インパクト分析には、変更のインパクトを理解し、追加の管理策が必要かどうかを判断するためのリスクアセスメントも含まれる。

関連管理策：CA-7, CM-3, CM-8, CM-9, MA-2, RA-3, RA-5, RA-8, SA-5, SA-8, SA-10, SI-2

拡張管理策：

(1) インパクト分析 | 独立したテスト環境

運用環境に実装する前に、独立したテスト環境でシステムへの変更を分析し、欠陥、弱点、非互換性、または意図的な悪意によるセキュリティおよびプライバシーへのインパクトを探す。

詳解：独立したテスト環境には、物理的または論理的に運用環境とは分離された異なる環境が必要である。分離には、テスト環境における様々な活動が運用環境における活動にインパクトを与えないこと、および運用環境での情報がテスト環境に誤って伝送されないことを十分に保証することが求められる。物理的または論理的手段により、独立した環境を実現することができる。物理的に独立したテスト環境が実装されていない場合には、組織はテスト環境を論理的な分離により実装する際の必要な強度を定めることが求められる。

関連管理策：SA-11, SC-7

(2) インパクト分析 | 管理策の検証

システムの変更後、インパクトを受ける管理策が正しく実装され、意図したとおりに動作し、システムのセキュリティ要件およびプライバシー要件を満たすために望ましい結果が得られることを検証する。

詳解：ここでいう実装とは、セキュリティまたはプライバシー管理策にインパクトを与える可能性がある変更されたコードを運用システムにインストールすることを指す。

関連管理策：SA-11, SC-3, SI-6

参照資料：[SP 800-128]

CM-5 変更に対するアクセス制限

管理策：システムへの変更に関連する物理的および論理的アクセス制限を規定、文書化、承認、および実施する。

詳解：システムのハードウェア、ソフトウェア、またはファームウェアコンポーネントの変更、またはシステムに関連する運用手順は、システムのセキュリティまたは個人のプライバシーに重大な影響を及ぼす可能性がある。したがって、組織は変更を開始するために、適格な認可された個人にのみシステムへのアクセスを許可する。アクセス制限には、物理的および論理的アクセス制御（AC-3 および PE-3 を参照）、ソフトウェアライブラリ、自動化されたワークフロー、メディアライブラリ、抽象レイヤー（すなわち、システムに直接ではなく外部インタフェースに実装された変更）、および変更ウィンドウ（すなわち、変更は特定の時間にのみ発生する）などが含まれる。

関連管理策：AC-3, AC-5, AC-6, CM-9, PE-3, SC-28, SC-34, SC-37, SI-2, SI-10

拡張管理策:

(1) 変更に対するアクセス制限 | 自動化されたアクセス実施および監査記録

(a) [*設定:組織が定める自動化のメカニズム*]を使用してアクセス制限を実施する。

(b) 実施措置の監査記録を自動的に生成する。

詳解:組織は、構成変更の適用に関連するシステムアクセスをロギングして、構成変更管理が実装されていることを確実にし、組織が認可されていない変更を発見した場合の事後措置をサポートする。

関連管理策:AU-2, AU-6, AU-7, AU-12, CM-6, CM-11, SI-12

(2) 変更に対するアクセス制限 | システム変更のレビュー

[撤回:CM-3(7)に組み込まれた]

(3) 変更に対するアクセス制限 | 署名されたコンポーネント

[撤回:CM-14 に移動した]

(4) 変更に対するアクセス制限 | 二重認可

[*設定:組織が定めるシステムコンポーネントとシステムレベルの情報*]への変更を実装するために二重認可を実施する。

詳解:組織は、2 人の認可された個人がそのような変更を承認および実装しない限り、選択されたシステムコンポーネントおよび情報への変更が発生しないようにするために、二重認可を採用する。その 2 人は、提案された変更が承認された変更の正しい実装となっているかどうかを判断するスキルと専門知識を保有している。個人はまた、変更に対して説明責任を負う。二重認可は、2 人による管理としても知られている。共謀のリスクを軽減するために、組織は他の個人に二重認可職務をローテーションすることを考慮する。システムレベルの情報には、運用手順が含まれる。

関連管理策:AC-2, AC-5, CM-3

(5) 変更に対するアクセス制限 | 開発および運用に関する特権の限定

(a) 運用環境または運用環境内のシステムコンポーネントおよびシステム関連情報を変更する特権を限定する。

(b) [*設定:組織が定める頻度*]で特権をレビューし、再評価する。

詳解:多くの組織では、システムは複数のミッションおよび事業機能をサポートしている。運用システムに関してシステムコンポーネントを変更する特権を限定することが必要である。なぜなら、システムコンポーネントへの変更は、システムがサポートするミッションおよび事業プロセスに広範囲にわたる影響を与える可能性があるからである。システムおよびミッション／事業プロセスの関係は開発者に知らされていない場合もある。システム関連の情報には、運用手順が含まれる。

関連管理策:AC-2

(6) 変更に対するアクセス制限 | ライブラリに関する特権の限定

ソフトウェアライブラリ内に常駐するソフトウェアを変更する特権を限定する。

詳解:ソフトウェアライブラリには特権プログラムが含まれる。

関連管理策:AC-2

(7) 変更に対するアクセス制限 | セキュリティ保全措置の自動実装

[撤回:SI-7 に組み込まれた]

参照資料:[FIPS 140-3], [FIPS 186-4]

CM-6 構成設定

管理策:

a. [*設定：組織が定める共通セキュア構成*]を使用して、最も制限のきびしい運用要件と一致する状態を反映する、システム内で採用されているコンポーネントの構成設定を定め、文書化する。

b. その構成設定を実装する。

c. [*設定：組織が定める運用要件*]に基づく[*設定：組織が定めるシステムコンポーネント*]に対し、定められた構成設定からの逸脱を識別し、文書化し、承認する。

d. 組織のポリシーおよび手順に従って、構成設定の変更を監視および管理する。

詳解：構成設定は、システムのセキュリティおよびプライバシーの状態または機能に影響を及ぼす、システムのハードウェア、ソフトウェア、またはファームウェアのコンポーネントで変更可能なパラメータである。構成設定を規定できる情報技術製品には、メインフレームコンピュータ、サーバ、ワークステーション、オペレーティングシステム、モバイルデバイス、入出力デバイス、プロトコル、アプリケーションなどが含まれる。システムのセキュリティ態勢にインパクトを与えるパラメータには、レジストリの設定、アカウント、ファイル、またはディレクトリのアクセス許可の設定、および機能、プロトコル、ポート、サービス、リモート接続の設定などが含まれる。プライバシーパラメータは、他のプライバシー管理策を満たすために必要なパラメータを含む、システムのプライバシー態勢にインパクトを与えるパラメータである。プライバシーパラメータには、アクセス制御、データ処理の優先権、処理および保持の許可などの設定が含まれる。組織は、組織全体の構成設定を定め、その後、システムに固有の構成設定を導出する。定められたこれらの設定は、システムの構成ベースラインの一部になる。

共通セキュア構成（セキュリティ構成チェックリスト、ロックダウンおよび強化ガイド、およびセキュリティ参照ガイドとも呼ばれる）は、情報技術製品およびプラットフォームのセキュアな構成設定と、運用要件を満たすように、これらの製品またはプラットフォームの構成手順を規定する、認識され、標準化され、確立されたベンチマークを提供する。共通セキュア構成は、情報技術製品の開発者、製造業者、ベンダ、連邦政府機関、コンソーシアム、学界、産業界、および公共および民間分野の他の組織など、様々な組織によって開発される。

共通セキュア構成の実装は、組織レベル、ミッションおよび事業プロセスレベル、システムレベル、または規制当局を含むより高いレベルで義務付けられる場合がある。共通セキュア構成には、米国政府共通設定基準[USGCB]およびセキュリティ技術実装ガイド（STIG）が含まれ、これらは CM-6 および AC-19 や CM-7 などの他の管理策の実装に影響を与える。セキュリティ設定共通化手順（SCAP）およびその中で規定規格は、構成設定を一意に識別、追跡、および管理するための効果的な方法を提供する。

関連管理策：AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, PL-9, RA-5, SA-4, SA-5, SA-8, SA-9, SC-18, SC-28, SC-43, SI-2, SI-4, SI-6

拡張管理策：

(1) 構成設定 | 自動化された管理、適用、および検証

[*設定：組織が定める自動化されたメカニズム*]を使用して、[*設定：組織が定めるシステムコンポーネント*]の構成設定を管理、適用、および検証する。

詳解：自動化されたツール（強化ツール、ベースライン構成ツールなど）は、構成設定情報の的確性、一貫性、および可用性を向上させることができる。自動化は、データ集約およびデータ相関ケイパビリティ、アラートのメカニズム、およびダッシュボードを提供して、組織内のリスクベースの意思決定をサポートすることもできる。

関連管理策：CA-7

(2) 構成設定 | 認可されていない変更への対応

[*設定：組織が定める構成設定*]への認可されていない変更に対応して、[*設定：組織が定める措置*]を実行する。

詳解：構成設定への認可されていない変更への対応には、指定された組織の職員への警告発出、確立された構成設定の復元、または、極端な場合には、影響を受けるシステム処理の停止などがある。

関連管理策：IR-4, IR-6, SI-7

(3) 構成設定 | 認可されていない変更の検知

［撤回：SI-7 に組み込まれた］

(4) 構成設定 | 適合性の立証

［撤回：CM-4 に組み込まれた］

参照資料：[SP 800-70], [SP 800-126], [SP 800-128], [USGCB], [NCPR], [DOD STIG]

CM-7 最小機能性

管理策：

a. ［*設定：組織が定めるミッションに必須なケイパビリティ*］のみを提供するようにシステムを構成する。

b. ［*設定：組織が定める禁止または制限された機能、システムポート、プロトコル、ソフトウェア、および／またはサービス*］の使用を禁止または制限する。

詳解：システムは、様々な機能とサービスを提供する。デフォルトで日常的に提供されている機能やサービスの中には、組織の必須なミッション、機能、または運用をサポートするために必要でないものもある。さらに、単一のシステムコンポーネントから複数のサービスを提供すると便利な場合があるが、そうすることによって、その単一のコンポーネントによって提供されるサービスに限定されてしまうリスクが高まる。可能であれば、組織はコンポーネントの機能をコンポーネントごとに 1 つの機能に限定する。組織は、コンポーネントへの認可されていない接続、情報の転送、およびトンネリングを防止するために、未使用または不要なソフトウェアを削除し、未使用または不要な物理および論理ポートおよびプロトコルを無効にすることを考慮する。組織は、ファイアウォールやホストベースの侵入検知システムなどのネットワークスキャンツール、侵入検知および防止システム、エンドポイント保護技術などを使用して、禁止されている機能、プロトコル、ポート、およびサービスの使用を識別および防止する。最小機能性は、システムの基本的な設計および開発の一部として達成することもできる（SA-8、SC-2、および SC-3 を参照）。

関連管理策：AC-3, AC-4, CM-2, CM-5, CM-6, CM-11, RA-5, SA-4, SA-5, SA-8, SA-9, SA-15, SC-2, SC-3, SC-7, SC-37, SI-4

拡張管理策：

(1) 最小機能性 | 定期的なレビュー

(a) ［*設定：組織が定める頻度*］でシステムをレビューし、不必要および／またはセキュアでない機能、ポート、プロトコル、ソフトウェア、サービスを識別する。

(b) ［*設定：組織が定めるシステム内の不要またはセキュアでないとみなされる機能、ポート、プロトコル、ソフトウェア、およびサービス*］を無効化または削除する。

詳解：組織は、システムまたはシステムコンポーネントによって提供される機能、ポート、プロトコル、およびサービスをレビューして、削除の候補となる機能とサービスを決定する。そのようなレビューは、古い技術から新しい技術への移行期間中（例えば、IPv4 から IPv6 への移行）には特に重要である。これらの技術の移行に際しては、移行期間中に新旧の技術を同時に実装し、最小限の必須機能、ポート、プロトコル、およびサービスにできるだけ早く戻す必要がある場合がある。組織は、機能、ポート、プロトコル、サービスの相対的なセキュリティを決定するか、他のエンティティのアセスメントに基づいてセキュリティを決定することができる。セキュアでないプロトコルには、Bluetooth、FTP、ピアツーピアネットワークなどがある。

関連管理策：AC-18

(2) 最小機能性 | プログラムの実行の防止

［選択（1 つ以上）：［設定：ソフトウェアプログラムの使用および制限に関する組織が定めるポリシー、行動規則、および／またはアクセス規約］；ソフトウェアプログラムの使

用条件を承認する規則]**に従って、プログラムの実行を防止する。**

詳解:プログラム実行の防止は、組織のポリシー、行動規則、および／またはソフトウェアの使用を制限するアクセス規約、およびソフトウェアのライセンスと著作権を含む、開発者または製造者が課す契約条件に対応している。制限には、自動実行機能の禁止、プログラム実行の承認を許可する役割の制限、特定のソフトウェアプログラムの許可または禁止、または同時に実行されるプログラムインスタンス数の制限などが含まれる。

関連管理策:CM-8, PL-4, PL-9, PM-5, PS-6

(3) 最小機能性｜登録に関する準拠

[*設定:組織が定める機能、ポート、プロトコル、およびサービスの登録要件*]への準拠を確保する。

詳解:組織は、登録プロセスを使用して、システム、実装されている機能、ポート、プロトコル、およびサービスを管理、追跡、および監視する。

関連管理策:なし

(4) 最小機能性｜認可されていないソフトウェア － 例外による拒否

(a) [*設定:組織が定めるシステム上での実行が認可されていないソフトウェアプログラム*]を識別する。

(b) システム上で認可されていないソフトウェアプログラムの実行を禁止するために、すべて許可、例外による拒否のポリシーを採用する。

(c) [*設定:組織が定める頻度*]で認可されていないソフトウェアプログラムのリストをレビューし、更新する。

詳解:認可されていないソフトウェアプログラムは、特定のバージョンまたは特定のソースからのもののみに限定することができる。認可されていないソフトウェアの実行を禁止するという概念は、ユーザ行為、システムのポートとプロトコル、IP アドレス／範囲、ウェブサイト、および MAC アドレスにも適用できる。

関連管理策:CM-6, CM-8, CM-10, PL-9, PM-5

(5) 最小機能性｜認可されたソフトウェア － 例外による許可

(a) [*設定:組織が定めるシステム上で実行することを認可されたソフトウェアプログラム*]を識別する。

(b) システム上で許可されたソフトウェアプログラムの実行を許可するために、すべて拒否、例外による認可のポリシーを採用する。

(c) [*設定:組織が定める頻度*]で認可されたソフトウェアプログラムのリストをレビューし、更新する。

詳解:認可されたソフトウェアプログラムは、特定のバージョンまたは特定のソースからのもののみに限定することができる。包括的な認可済みソフトウェアプロセスを促進し、アプリケーションレベルの認可済みソフトウェアを迂回する攻撃に対する保護の強度を高めるために、ソフトウェアプログラムを様々な詳細レベルに分解して監視することができる。これらのレベルには、アプリケーション、アプリケーションプログラミングインタフェース、アプリケーションモジュール、スクリプト、システムプロセス、システムサービス、カーネル関数、レジストリ、ドライバー、ダイナミックリンクライブラリなどがある。認可されたソフトウェアの実行を許可するという概念は、ユーザ行為、システムのポートとプロトコル、IP アドレス／範囲、ウェブサイト、および MAC アドレスにも適用できる。組織は、デジタル署名、暗号チェックサム、またはハッシュ関数を使用して、認可されたソフトウェアプログラムの完全性を検証することを考慮する。認可されたソフトウェアの検証は、実行前またはシステム起動時に行うことができる。ウェブサイトの認可済み URL の識別は、CA-3(5)および SC-7 で扱われている。

関連管理策:CM-2, CM-6, CM-8, CM-10, PL-9, PM-5, SA-10, SC-34, SI-7

(6) 最小機能性｜限定された特権を備えた制限環境

***[設定:組織が定めるユーザがインストールしたソフトウェア]*が、限定された特権を持**

つ一定の制限された物理または仮想マシン環境で実行されることを要求する。

詳解：組織は、その出所または悪意のあるコードを含む可能性に関して懸念されるソフトウェアを識別する。このタイプのソフトウェアの場合、ユーザのインストールは、実行される可能性のある悪意のあるコードによる被害を限定または抑制するために、制限された動作環境で行われる。

関連管理策：CM-11, SC-44

(7) 最小機能性｜保護された環境内でのコードの実行

バイナリまたはマシン実行可能コードの実行については、それらのコードが以下の場合には、制限された物理マシンまたは仮想マシン環境で、[*設定：組織が定める職員または役割*]の明確な承認があるときにのみ、許可する。

(a) 限定的な保証または無保証のソースから取得した場合。および／または

(b) ソースコードの提供がない場合。

詳解：保護された環境内でコードを実行することは、商用ソフトウェアおよびファームウェア、オープンソースソフトウェアを含む、すべてのソースからのバイナリまたはマシン実行可能コードに適用される。

関連管理策：CM-10, SC-44

(8) 最小機能性｜バイナリまたはマシン実行可能コード

(a) 限定的な保証の、または無保証の、あるいはソースコードの提供を伴わない、ソースからのバイナリまたはマシン実行可能コードの使用を禁止する。

(b) 例外を認めるのは、従わざるを得ないミッションまたは運用上の要件に対してのみ、かつ認可権限のある担当者の承認を得た場合のみである。

詳解：バイナリまたはマシン実行可能コードは、商用ソフトウェアおよびファームウェア、オープンソースソフトウェアのすべてのソースに適用される。組織は、ソースコードを伴わない、あるいはセキュリティへのインパクトの可能性について限定的またはまったく保証されていないソースからのソフトウェア製品に対してはアセスメントを実施する必要がある。このアセスメントは、ソースコードが提供されていないソフトウェア製品は、レビュー、修復、または機能拡張が難しい場合があるという事実に対応している。加えて、組織に代わってそのような修理を行うオーナーがいない可能性もある。オープンソースソフトウェアが使用されている場合には、アセスメントは、無保証で、オープンソースソフトウェアにバックドアやマルウェアが含まれている可能性があり、利用可能なサポートがない可能性があるなどの事実に対処するために実施される。

関連管理策：SA-5, SA-22

(9) 最小機能性｜認可されていないハードウェアの使用の禁止

(a) [*設定：組織が定めるシステムでの使用が認可されたハードウェアコンポーネント*]を識別する。

(b) 認可されていないハードウェアコンポーネントの使用または接続を禁止する。

(c) [*設定：組織が定める頻度*]で認可されたハードウェアコンポーネントの一覧表をレビューし、更新する。

詳解：ハードウェアコンポーネントは、組織のシステムと、認可されたソフトウェアプログラムを実行するためのプラットフォームの基盤を提供する。適切なセキュリティを提供するためには、ハードウェアコンポーネントのインベントリを管理することによって、組織のシステムへのインストールまたは接続を許可するハードウェアコンポーネントを管理することが不可欠である。

関連管理策：なし

参照資料：[FIPS 140-3], [FIPS 180-4], [FIPS 186-4], [FIPS 202], [SP 800-167]

CM-8 システムコンポーネントのインベントリ

管理策:

a. 以下のシステムコンポーネントのインベントリを作成し、文書化する。

1. システムを的確に反映している。
2. システム内のすべてのコンポーネントを含む。
3. コンポーネントまたは他のシステムに設定されたコンポーネントとの重複算出を含まない。
4. 追跡および報告に必要と思われる細分性のレベルにある。
5. システムコンポーネントの説明責任を果たすために[*設定:組織が定める効果的なシステムコンポーネントの説明責任を達成するために必要とみなされる情報*]を含む。

b. [*設定:組織が定める頻度*]でシステムコンポーネントのインベントリをレビューし、更新する。

詳解:システムコンポーネントは、ハードウェア、ソフトウェア、およびファームウェアを含む、識別可能な個別の情報技術(IT)資産である。組織は、すべての組織のシステムコンポーネントを含む、集中化されたシステムコンポーネントのインベントリを実装することを選択できる。このような状況では、組織は、コンポーネントの説明責任に必要なシステム固有の情報がインベントリに含まれるようにする。システムコンポーネントの効果的な説明責任に必要な情報には、システム名、ソフトウェアオーナー、ソフトウェアバージョン番号、ハードウェアインベントリの仕様、ソフトウェアライセンス情報などが含まれ、ネットワークコンポーネントの場合、実装されているすべてのプロトコル(IPv4、IPv6 など)にわたるマシン名とネットワークアドレスなどが含まれる。インベントリの仕様には、受領日、コスト、モデル、シリアル番号、製造元、サプライヤ情報、コンポーネントのタイプ、および物理的な位置などが含まれる。

システムコンポーネントの重複算出を防止することで、特に大規模または複雑な接続システムにおいて、コンポーネントのオーナーとシステムの関連付けが不明な場合に発生する説明責任の欠如に対処する。システムコンポーネントの重複算出を効果的に防止するには、各コンポーネントに一意の識別子を使用する必要がある。ソフトウェアのインベントリの場合、他のシステムを介してアクセスされる集中管理されたソフトウェアは、それがインストールおよび管理されているシステムのコンポーネントとして扱われる。複数の組織のシステムにインストールされ、システムレベルで管理されるソフトウェアは、個々のシステムごとに扱われ、集中型コンポーネントインベントリに複数回現れる可能性があるため、コンポーネントの重複した算出処理を回避するために、集中型インベントリ内の各ソフトウェアにシステムを関連付ける必要がある。複数のネットワークプロトコル(IPv4 や IPv6 など)を実装したスキャンシステムは、異なるアドレス空間における重複したコンポーネントとして識別される可能性がある。CM-8(7)の実装は、コンポーネントの重複算出を排除するのに役立つ。

関連管理策:CM-2, CM-7, CM-9, CM-10, CM-11, CM-13, CP-2, CP-9, MA-2, MA-6, PE-20, PL-9, PM-5, SA-4, SA-5, SI-2, SR-4

拡張管理策:

(1) システムコンポーネントのインベントリ | インストール中および削除中の更新

コンポーネントのインストール、削除、およびシステム更新の一環として、システムコンポーネントのインベントリを更新する。

詳解:組織は、コンポーネントのインストールまたは削除の一部として、または一般的なシステムの更新中にインベントリが更新される場合、システムコンポーネントのインベントリの的確性、正確性、および一貫性を向上させることができる。これらの主要なタイミングでインベントリが更新されない場合、情報が適切にキャプチャ、文書化されない可能性が高くなる。システムの更新には、ハードウェア、ソフトウェア、ファームウェアのコンポーネントなどの変更が含まれる。

関連管理策:PM-16

(2) システムコンポーネントのインベントリ | 自動化されたメンテナンス

[*設定：組織が定める自動化されたメカニズム*]を使用して、システムコンポーネントのインベントリの最新性、正確性、的確性、可用性を維持する。

詳解：組織は、可能な範囲でシステムのインベントリを維持する。例えば、仮想マシンは、使用されていないときはネットワークから見えないため、監視が難しい場合がある。このような場合、組織は、合理的であると見なされる限り、最新の正確かつ的確なインベントリを維持する。自動化されたメンテナンスは、組織にシステムコンポーネントのインベントリとベースライン構成の活動を組み合わせた CM-2(2)を実装することで実現できる。

関連管理策：なし

(3) システムコンポーネントのインベントリ｜認可されていないコンポーネントの自動化された検知

(a) [*設定：組織が定める頻度*]で[*設定：組織が定める自動化されたメカニズム*]を使用して、システム内の認可されていないハードウェア、ソフトウェア、およびファームウェアコンポーネントの存在を検知する。

(b) 認可されていないコンポーネントが検知された場合は、[*選択（1 つ以上）：そのようなコンポーネントによるネットワークアクセスの無効化；コンポーネントを分離する；[設定：組織が定める職員または役割] への通知*]を行う。

詳解：認可されていないリモート接続およびモバイルデバイスの監視に加えて、認可されていないコンポーネントの自動検知が適用される。認可されていないシステムコンポーネントの監視は、継続的に、またはその目的のためにシステムを定期的にスキャンすることによって達成することができる。認可されていないコンポーネントの接続を防止するために、自動化されたメカニズムを使用することもできる（CM-7(9)を参照）。自動化のメカニズムは、システムまたは個別のシステムコンポーネントに実装することができる。一部のタイプのコンポーネント（IoT デバイス、センサなど）にはエージェントを持たないかサポートできないため、自動化されたメカニズムを取得して実装する場合、組織は、そうしたメカニズムの検知が、エージェントまたはサプリカントをサポートするシステムコンポーネントの能力に左右されるかどうかを考慮する。分離は、例えば、認可されていないシステムコンポーネントを別のドメインまたはサブネットに配置するか、そのようなコンポーネントを隔離することによって実現できる。このタイプのコンポーネントの分離は、一般に「サンドボックス化」と呼ばれる。

関連管理策：AC-19, CA-7, RA-5, SC-3, SC-39, SC-44, SI-3, SI-4, SI-7

(4) システムコンポーネントのインベントリ｜説明責任情報

システムコンポーネントのインベントリ情報に、[*選択（1 つ以上）：名前；職位；役割*]など、それらのコンポーネントの管理に責任および説明責任を負う個人を識別する手段を含める。

詳解：システムコンポーネントの管理に責任と説明責任を負う個人を識別することで、設定されたコンポーネントが適切に管理され、何らかの措置が必要な場合（例えば、そのコンポーネントがブリーチの発生源であると判断された場合や、リコールまたは交換、または移設される必要がある場合など）に、組織がその個人に連絡できるようにする。

関連管理策：AC-3

(5) システムコンポーネントのインベントリ｜コンポーネントの非重複算出

[撤回：CM-8 に組み込まれた]

(6) システムコンポーネントのインベントリ｜アセスメント済みの構成および承認された偏差

アセスメント済みのコンポーネントの構成と、システムコンポーネントのインベントリに現在展開されている構成に対する承認された偏差を含める。

詳解：アセスメント済みの構成および承認された偏差は、システムコンポーネントに対して組織によって確立された構成設定、必要な構成設定への準拠を判断するためにアセスメントされた特定のコンポーネント、および確立された構成設定からの承認された偏差に焦点を当てている。

関連管理策：なし

(7) システムコンポーネントのインベントリ｜集中化されたリポジトリ

システムコンポーネントのインベントリのための集中化されたリポジトリを提供する。

詳解：組織は、すべての組織システムからのコンポーネントを含む、集中化されたシステムコンポーネントインベントリを実装することができる。コンポーネントインベントリの一元化されたリポジトリは、組織のハードウェア、ソフトウェア、およびファームウェア資産の算定を効率化する機会を提供する。このようなリポジトリは、侵害や、ブリーチ、またはその他軽減措置が必要なコンポーネントの位置や責任者を、組織が迅速に識別するのにも役立つ。組織は、作成された集中型インベントリに、適切なコンポーネントの説明責任に必要なシステム固有の情報が含まれていることを確認する。

関連管理策：なし

(8) システムコンポーネントのインベントリ｜自動化された位置追跡機能

[*設定：組織が定める自動化されたメカニズム*]を使用して、システムコンポーネントの地理的位置による追跡機能をサポートする。

詳解：自動化されたメカニズムを使用してシステムコンポーネントの位置を追跡することにより、コンポーネントのインベントリの的確性を向上させることができる。そのようなケイパビリティは、侵害された、ブリーチされた、またはその他軽減措置が必要なシステムコンポーネントの位置と責任者を組織が迅速に識別するのに役立つ可能性がある。個人のプライバシーに影響する可能性がある場合、追跡のメカニズムの使用は、政府機関のプライバシー保護責任者と調整することができる。

関連管理策：なし

(9) システムコンポーネントのインベントリ｜システムへのコンポーネントの設定

(a) システムコンポーネントをシステムに設定する。

(b) この設定について、[*設定：組織が定める職員または役割*]から承認を受ける。

詳解：システムに設定されていないシステムコンポーネントは、管理対象外となり、必要な保護が欠如しており、組織の脆弱性となる可能性がある。

関連管理策：なし

参照資料：[OMB A-130], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-128], [IR 8011-2], [IR 8011-3]

CM-9 構成管理計画

管理策：以下のシステム構成管理計画を策定、文書化、実装する。

a. 役割、責任、および構成管理のプロセスと手順を取り扱う。

b. システム開発ライフサイクル全体を通じて構成管理の管理対象となる構成アイテムを識別し、構成アイテムの構成を管理するプロセスを定める。

c. システムの構成アイテムを規定し、構成アイテムを構成管理下に置く。

d. [*設定：組織が定める職員または役割*]によってレビューされ、承認されている。

e. 構成管理計画を認可されていない開示や変更から保護する。

詳解：構成管理活動は、システム開発ライフサイクル全体を通じて発生する。したがって、開発に関する構成管理活動（コードおよびソフトウェアライブラリの管理など）と運用に関する構成管理活動（インストールされているコンポーネントの管理およびコンポーネントの構成方法など）が存在する。構成管理計画は、個々のシステムに合わせてテーラリングされ、構成管理ポリシーの要件を満たすことが求められる。構成管理計画には、構成管理を使用してシステム開発ライフサイクル活動をサポートするためのプロセスと手順が規定される。

構成管理計画は、システム開発ライフサイクルの開発および取得段階で生成される。この計画には、変更管理プロセスを通じて変更を進める方法；構成設定とベースラインの更新；コンポー

ネントのインベントリの維持；開発、テスト、運用環境の管理；主要なドキュメントの作成、リリース、更新などが記述されている。

組織は、テンプレートを使用して、構成管理計画の一貫したタイムリーな策定と実装を実施することができる。テンプレートは、システムごとに実装された計画のサブセットを使用して、組織の構成管理計画を表すことができる。構成管理の承認プロセスには、システムへの提案された変更のレビューおよび承認を担当する主要な経営行動等における利害関係者の指名、およびシステムへの変更の実装前にセキュリティおよびプライバシー影響評価を実施する職員の指定が含まれる。構成アイテムには、構成管理対象のハードウェア、ソフトウェア、ファームウェア、ドキュメントなどのシステムコンポーネントなどがある。システムがシステム開発ライフサイクルを継続するにつれて、新しい構成アイテムが識別され、一部の既存の構成アイテムが構成管理下にある必要がなくなる場合がある。

関連管理策：CM-2, CM-3, CM-4, CM-5, CM-8, PL-2, RA-8, SA-10, SI-12

拡張管理策：

(1) 構成管理計画｜責任の設定

システム開発に直接関与しない組織の職員に、構成管理プロセスを策定する責任を設定する。

詳解：組織内に専任の構成管理チームが設定されていない場合、システム開発者は、システム開発またはシステム構築に直接関与しない職員を用いて構成管理プロセスを策定する必要がある。この職務の分離により、組織は、システム開発および構築プロセスと構成管理プロセスとの間に十分な独立性を保証および維持して、品質管理とより効果的な監視を容易にすることができる。

関連管理策：なし

参照資料：[SP 800-128]

CM-10 ソフトウェアの使用制限

管理策：

a. 請負契約書および著作権法に従ってソフトウェアおよび関連文書を使用する。

b. コピーと配布を管理するために、数量ライセンスで保護されたソフトウェアと関連文書の使用を追跡する。

c. ピアツーピアのファイル共有技術の使用を管理および文書化し、このケイパビリティが、著作権で保護された製品の認可されていない配布、表示、実行、または複製に使用されないようにする。

詳解：ソフトウェアライセンスの追跡は、組織のニーズに応じて、手動または自動で遂行できる。請負契約書の例には、ソフトウェアライセンス契約書および秘密保持契約書が含まれる。

関連管理策：AC-17, AU-6, CM-7, CM-8, PM-30, SC-7

拡張管理策：

(1) ソフトウェアの使用制限｜オープンソースソフトウェア

オープンソースソフトウェアの使用に関する[*設定：組織が定める制限*]を定める。

詳解：オープンソースソフトウェアとは、ソースコード形式で入手可能なソフトウェアを指す。通常、著作権者に確保されている特定のソフトウェアの権利は、個人がソフトウェアを研究、変更、および改善することを許可するソフトウェア使用許諾契約書に基づいて日常的に提供されている。セキュリティの観点から見ると、オープンソースソフトウェアの主な利点は、組織がソースコードを検査できることである。場合によっては、ソフトウェアで発見された問題を継続的に検査、テスト、更新、報告するソフトウェアに関連付けられたオンラインコミュニティがある。ただし、オープンソースソフトウェアの脆弱性を修正することは問題となる可能性がある。また、オープンソースソフトウェアに関連するライセンスの問題が存

在する場合がある。バイナリ形式でのみ入手可能なオープンソースソフトウェアは、そのようなソフトウェアを使用する際のリスクレベルを高める可能性がある。

関連管理策：SI-7

参照資料：なし

CM-11 ユーザがインストールしたソフトウェア

管理策：

a. ユーザによるソフトウェアのインストールを管理する［*設定：組織が定めるポリシー*］を定める。

b. ［*設定：組織が定める方法*］でソフトウェアのインストールポリシーを実施する。

c. ［*設定：組織が定める頻度*］でポリシーへの準拠を監視する。

詳解：必要な特権が付与されている場合、ユーザは組織のシステムにソフトウェアをインストールできる。インストールされたソフトウェアに対する管理を維持するために、組織はソフトウェアのインストールに関して許可された措置と禁止された措置を識別することが求められる。許可されたソフトウェアのインストールには、既存のソフトウェアへのアップデートとセキュリティパッチ、および組織が承認したソフトウェアの「アプストア」からの新しいアプリケーションのダウンロードが含まれる。禁止されているソフトウェアのインストールには、由来が不明または疑わしいソフトウェア、または組織が潜在的に悪意があると考えるソフトウェアが含まれる。ユーザがインストールしたソフトウェアを管理するために選択されたポリシーは、組織によって策定されたものであるか、外部エンティティによって提供されたものである。ポリシー実施方法には、手続き的方法および自動化された方法を含めることができる。

関連管理策：AC-3, AU-6, CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, PL-4, SI-4, SI-7

拡張管理策：

(1) ユーザがインストールしたソフトウェア｜認可されていないインストールに対するアラート

［撤回：CM-8(3)に組み込まれた］

(2) ユーザがインストールしたソフトウェア｜特権状態でのソフトウェアのインストール

ユーザによるソフトウェアのインストールは、明確な特権ステータスを有する場合にのみ許可する。

詳解：特権ステータスは、例えば、システム管理者の役割を務めることによって取得できる。

関連管理策：AC-5, AC-6

(3) ユーザがインストールしたソフトウェア｜自動化された実施および監視

［*設定：組織が定める自動化されたメカニズム*］を使用して、ソフトウェアインストールポリシーを実施し、準拠を監視する。

詳解：組織は、内部または外部の敵対的な攻撃の兆候である可能性のある、認可されていないソフトウェアのインストールをより迅速に検知し対処するために、自動化されたメカニズムを用いて、ソフトウェアインストールポリシーを実施し、準拠を監視する。

関連管理策：なし

参照資料：なし

CM-12 情報の位置

管理策：

a. ［*設定：組織の定める情報*］の位置と、その情報が処理および保存される特定のシステムコンポーネントを識別し、文書化する。

b. 情報が処理および保存されるシステムおよびシステムコンポーネントにアクセスできるユーザを識別し、文書化する。

c. 情報が処理および保管される位置（すなわち、システムまたはシステムコンポーネント）の変更を文書化する。

詳解：情報の位置は、情報が処理および保存されている場所を理解把握する必要性に対応している。情報の位置には、情報の流れを把握し、そのような情報とシステムコンポーネントに適切な保護とポリシーの管理を提供することができるように、特定の情報タイプと情報がシステムコンポーネントのどこに存在し、情報がどのように処理されているかを識別することが含まれる。情報のセキュリティ分類も、情報とその情報が存在するシステムコンポーネントを保護するために必要な管理策を決定する際の要因となる（FIPS 199 を参照）。情報コンポーネントとシステムコンポーネントの位置も、システムのアーキテクチャと設計の要因である（SA-4, SA-8, SA-17 を参照）。

関連管理策：AC-2, AC-3, AC-4, AC-6, AC-23, CM-8, PM-5, RA-2, SA-4, SA-8, SA-17, SC-4, SC-16, SC-28, SI-4, SI-7

拡張管理策：

(1) 情報の位置 | 情報の位置をサポートする自動化されたツール

自動化されたツールを使用して、[*設定：組織が定めるシステムコンポーネント*]で[*設定：組織が定める情報タイプごとの情報*]を識別し、組織情報と個人のプライバシーを保護するための管理策が導入されていることを確実にする。

詳解：自動化されたツールの使用は、システム内に実装された情報位置特定ケイパビリティの有効性および効率を高めるのに役立つ。自動化は、組織が情報位置特定活動中に生成されたデータを管理し、組織全体でそのような情報を共有するのにも役立つ。自動化された情報位置特定ツールの出力は、システムのアーキテクチャおよび設計の意思決定におけるガイドや情報提供に役立つ。

関連管理策：なし

参照資料：[FIPS 199], [SP 800-60-1], [SP 800-60-2]

CM-13 データアクションのマッピング

管理策：システムによるデータアクションの対応付け表（マップ）を作成し、文書化する。

詳解：データアクションは、個人情報を取扱うシステム操作である。そのような情報の処理には、収集、生成、変換、使用、開示、保持、および廃棄を含む情報ライフサイクル全体が含まれる。システムによるデータアクションのマップには、個別のデータアクション、データアクションで処理される個人情報の要素、データアクションに関与するシステムコンポーネント、およびシステムコンポーネントのオーナーまたは操作者が含まれる。どの個人情報が（例えば、個人情報の機微性など）処理されているか、個人情報がどのように処理されているか（データアクションが当該個人に可視化されているか、システムの別の部分で処理されているかなど）、そして誰が（例えば、個人は個人情報を取り扱っているエンティティに基づいて、異なるプライバシー認識を持っている可能性がある）システムによって生み出されたプライバシーリスクの程度をアセスメントするために重要な多くのコンテキスト要因を提供するかなどを把握する。データマップは様々な方法で示すことができ、詳細さのレベルは組織のミッションおよび事業ニーズに基づいて異なる場合がある。データマップは、組織が使用しているシステム設計成果物の組織特有のオーバーレイ管理策である場合がある。このマップの作成では、対象となるデータアクションとシステムの一部として識別されるコンポーネントに関するプライバシープログラムおよびセキュリティプログラム間の調整が必要になる場合がある。

関連管理策：AC-3, CM-4, CM-12, PM-5, PM-27, PT-2, PT-3, RA-3, RA-8

CM-14 署名されたコンポーネント

管理策：組織によって受け入れられ承認された証明書を用いてデジタル署名されていることが検証されていない[*設定：組織が定めるソフトウェアおよびファームウェアコンポーネント*]のイン

ストールを防止する。

詳解：ソフトウェアおよびファームウェアのコンポーネントは、ソフトウェアおよびファームウェアのバージョンの更新、パッチ、サービスパック、デバイスドライバ、および基本的な入出力システムの更新を含め、受け入れられ承認された証明書で署名されていない限り、インストールが防止される。組織は、タイプ、特定のアイテム、または両方の組み合わせによって、該当するソフトウェアおよびファームウェアのコンポーネントを識別できる。デジタル署名およびそのような署名の組織による検証は、コード認証の一つの方法である。

関連管理策：CM-7, SC-12, SC-13, SI-7

参照資料：[IR 8062]

3.6 緊急時対応計画

緊急時対応計画の要約表へのクイックリンク

CP-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。

1. 以下の[*選択(1 つ以上):組織レベル;ミッション/事業プロセスレベル;システムレベル*]の緊急時対応計画のポリシー。

(a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、および準拠に対処する。

(b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに適合している。

2. 緊急時対応計画のポリシーと関連する緊急時対応計画の管理策の実装を促進するための手順。

b. 緊急時対応計画のポリシーと手順の策定、文書化、および配布することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行の緊急時対応計画をレビューし、更新する。

1. ポリシーについて[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

2. 手順について[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

詳解:緊急時対応計画のポリシーと手順は、システムおよび組織で実装される CP ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に寄与する。したがって、セキュリティおよびプライバシープログラムが緊急時対応計画のポリシーと手順の策定と連携していることが重要である。セキュリティおよびプライバシープログラムのポリシーと手順を組織レベルで確立することは望ましく、一般的には、ミッションまたはシステム固有のポリシーと手順を不要にすることができる。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映する複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムに対して規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述し、手順の対象である個人または役割向けとすることができる。手順は、システムのセキュリティおよびプライバシー計画の中に、または 1 つ以上の別の文書に文書化することもできる。緊急時対応計画のポリシーと手順の更新を引き起こす可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれる。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策:PM-9, PS-8, SI-12

拡張管理策:なし

参照資料:[SP 800-12], [SP 800-30], [SP 800-34], [SP 800-39], [SP 800-50], [SP 800-100]

CP-2 緊急時対応計画

管理策:

a. 以下を含む、システムの緊急時対応計画を策定する。

1. 重要なミッションおよび事業機能ならびに関連する緊急時対応要件を特定する。
2. 復旧目標、優先順位、および指標を提供する。
3. 緊急時対応の役割、責任、連絡先情報を持つ割り当てられた個人に対処する。
4. システムの中断、侵害、または障害が発生した場合でも、重要なミッションおよび事業機能を維持できるよう対処する。
5. 当初計画され実装された管理策を低下させることなく、最終的にシステムを完全復元できるよう対処する。
6. 緊急時対応情報を共有できるよう対処する。
7. [*設定:組織が定める職員または役割*]により、レビューならびに承認されている。

b. 緊急時対応計画のコピーを[*設定:組織が定める主要緊急時対応職員(氏名および/または役割によって特定される)および部署*]に配布する。

c. 緊急時対応計画措置とインシデント対応措置を調整する。

d. システムの緊急時対応計画を[*設定:組織が定める頻度*]でレビューする。

e. 組織、システム、運用環境の変更に対処するために、または緊急時対応計画の実装、実行、テスト中に発生した問題に対処するために、緊急時対応計画を更新する。

f. 緊急時対応計画の変更を[*設定:組織が定める主要緊急時対応職員(氏名および/または役割によって特定される)および部署*]に伝達する。

g. 緊急時対応計画のテスト、トレーニング、または実際の緊急時対応措置から学んだ教訓を、緊急時対応テストおよびトレーニングに組み込む。

h. 認可されていない開示や変更から緊急時対応計画を保護する。

詳解:システムの緊急時対応計画は、組織のミッションおよび事業機能の運用の継続性を達成するための全体的な計画の一部である。緊急時対応計画は、システムが侵害またはブリーチされた場合に、システムの復元と代替のミッションまたは事業プロセスの実装に対処する。緊急時対応計画は、システム開発ライフサイクル全体で考慮され、システム設計の基本的な部分である。システムは、冗長性、バックアップケイパビリティ、およびレジリエンスを持つように設計する。すべてのシステムが、必要な運用の継続性のレベルを達成するために完全に復旧する必要があるわけではないため、緊急時対応計画は、組織のシステムに必要な復旧の程度を反映する。システム復旧の目標は、適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドライン、組織のリスク許容度、およびシステムインパクトレベルを反映する。

緊急時対応計画で対処される措置には、規則に従ったシステムの縮退運用、システムのシャットダウン、手動モードへのフォールバック、情報フローの変更、およびシステムが攻撃を受けている際に用意したモードでの運用が含まれる。緊急時対応計画とインシデント対応措置を調整することにより、組織は、必要な計画活動が導入され、インシデント発生時に有効化されることを確実にする。組織は、インシデント発生時の運用の継続性について、IR-4(5)で規定されているシステムを自動的に無効化するケイパビリティと矛盾するかどうかを考慮する。インシデント対応計画は、組織の緊急時対応計画の一部であり、IR(インシデント対応)管理策ファミリーで対処される。

関連管理策:CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13, IR-4, IR-6, IR-8, IR-9, MA-6, MP-2, MP-4, MP-5, PL-2, PM-8, PM-11, SA-15, SA-20, SC-7, SC-23, SI-12

拡張管理策:

(1) 緊急時対応計画 | 関連計画との調整

緊急時対応計画の策定を、関連計画を担当する組織の部署と調整する。

詳解：緊急時対応計画に関連する計画には、事業継続計画、災害時復旧計画、重要インフラ計画、運用継続計画、危機コミュニケーション計画、インサイダー脅威対策実装計画、データ侵害対応計画、サイバーインシデント対応計画、侵害対応計画、および居住者非常時対応計画が含まれる。

関連管理策：なし

(2) 緊急時対応計画 | 処理能力計画

緊急時対応の運用において、情報処理、通信、環境サポートに必要な処理能力を有するように処理能力計画を立てる。

詳解：様々な脅威が、重要なミッションおよび事業機能をサポートするための利用可能な処理、通信、およびサポートサービスの低下につながる可能性があるため、処理能力計画が必要である。組織は、緊急時の運用における縮退に備え、縮退運用方式を処理能力計画に織り込む。処理能力計画において、環境サポートとは、組織が機能低下状態であっても、緊急時対応にサポートを提供する必要があると組織が決定する環境要因のことである。そのような決定は、組織のリスクアセスメント、システム分類（インパクトレベル）、および組織のリスク許容度に基づいている。

関連管理策：PE-11, PE-12, PE-13, PE-14, PE-18, SC-5

(3) 緊急時対応計画 | ミッションおよび事業機能の再開

[*選択：すべての；必須の*]緊急時対応計画を発動してから[*設定：組織が定める期間*]内で、ミッションおよび事業機能の再開を計画する。

詳解：組織は、事業継続計画の一環として、または事業インパクト分析の一環として、ミッションおよび事業機能を再開するための緊急時対応計画措置を実施することを選択することができる。組織は、ミッションおよび事業機能の再開に優先順位をつける。ミッションおよび事業機能を再開するための期間は、システムおよびそのサポートインフラの中断の深刻度および程度に依存する場合がある。

関連管理策：なし

(4) 緊急時対応計画 | すべてのミッションおよび事業機能の再開

[撤回：CP-2(3)に組み込まれた]

(5) 緊急時対応計画 | ミッションおよび事業機能の継続

[*選択：すべての；必須の*]ミッションおよび事業機能の継続性について、運用継続性の喪失を最小限とするか、喪失を伴わないよう、一次処理サイトおよび／または一次保管サイトで、システムが完全に復元するまで継続性を維持するよう、計画する。

詳解：組織は、事業継続計画または事業インパクト分析の一環として、ミッションおよび事業機能を継続するために緊急時対応計画措置を実施することを選択できる。緊急時対応計画の一環として組織によって定められた一次処理サイトおよび／または一次保管サイトは、緊急時対応に関連する状況に応じて変更してもよい。

関連管理策：なし

(6) 緊急時対応計画 | 代替処理サイトおよび代替保管サイト

[*選択：すべての；必須の*]ミッションおよび事業機能の代替処理サイトおよび／または代替保管サイトへの移転について、運用継続性の喪失を最小限とするか、喪失を伴わないよう、一次処理サイトおよび／または一次保管サイトのシステムが完全に復元するまで継続性を維持するよう、計画する。

詳解：組織は、事業継続計画または事業インパクト分析の一環として、代替処理サイトおよび代替保管サイトのために、緊急時対応計画措置を実施することを選択できる。緊急時対応計画の一環として組織によって定義された一次処理サイトおよび／または一次保管サイトは、緊急時対応に関連する状況に応じて変更してもよい。

関連管理策：なし

(7) 緊急時対応計画 | 外部サービスプロバイダとの調整

緊急時対応計画を外部サービスプロバイダの緊急時対応計画と調整して、緊急時対応の要件が確実に満たされるようにする。

詳解：組織のミッションおよび事業機能を実行するケイパビリティが外部サービスプロバイダに依存している場合、包括的かつタイムリーな緊急時対応計画の策定が、より困難になる可能性がある。ミッションおよび事業機能が外部サービスプロバイダに依存している場合、組織は、外部のエンティティと緊急時対応計画措置を調整して、個々の計画が組織の全体的な緊急時対応ニーズを確実に反映するようにする。

関連管理策：SA-9

(8) 緊急時対応計画 | 重要な資産の特定

[*選択：すべての；必須の*]ミッションおよび事業機能をサポートする重要なシステム資産を特定する。

詳解：組織は、重要性分析、事業継続計画、または事業インパクト分析の一環として、重要な資産を特定することを選択する場合がある。組織は、重要なシステム資産を特定し、追加の管理策を（通常の管理策を超えて）採用し、組織のミッションおよび事業機能を緊急時対応の運用中に継続し実施できるようにする。重要な情報資産を特定することで、組織の資産の優先順位付けも容易になる。重要なシステム資産には、技術的側面および運用的側面が含まれる。技術的側面には、システムコンポーネント、情報技術サービス、情報技術製品、メカニズムが含まれる。運用的側面には、手順（すなわち、手動で実行する操作）および職員（すなわち、技術的制御を操作する個人および／または手動手順を実行する個人）が含まれる。組織のプログラム保護計画は、重要な資産の特定に役立つ。重要な資産が外部サービスプロバイダ内にあるか、外部サービスプロバイダによってサポートされている場合、組織は CP-2(7)の実装を拡張管理策として考慮する。

関連管理策：CM-8, RA-9

参照資料：[SP 800-34], [IR 8179]

CP-3 緊急時対応トレーニング

管理策：

a. システムユーザに対し、割り当てられた役割および責任に応じ、緊急時対応トレーニングを実施する。

   1. 緊急時対応の役割または責任を担ってから[*設定：組織が定める期間*]内に。
   2. システム変更により、必要になった場合に。
   3. その後、[*設定：組織が定める頻度*]で。

b. 緊急時対応トレーニングの内容を、[*設定：組織が定める頻度*]および[*設定：組織が定めるイベント*]に応じて、レビューし、更新する。

詳解：組織が提供する緊急時対応トレーニングは、組織の職員の割り当てられた役割と責任に応じ、適切な内容と詳細レベルを含んだものとする。例えば、一部の個人は、緊急時対応の運用中に、通常のミッションが影響を受けた場合、いつ、どこで報告する義務があるかを知るだけでよい場合がある。システム管理者は、代替処理サイトおよび代替保管サイトにシステムを構築する方法に関する追加のトレーニングを必要とする場合がある。組織の担当者は、指定されたオフサイトでミッション遂行に必要な機能を実施する方法、緊急時対応措置の調整を目的として他の政府のエンティティとの連絡を確立する方法について、より具体的なトレーニングを受ける場合がある。緊急時対応の役割または責任に応じたトレーニングは、緊急時対応計画の特定の継続性要件を反映する。緊急時対応のトレーニング内容の更新を引き起こす可能性のあるイベントには、緊急時対応計画のテストや実際の緊急時対応（教訓）、アセスメントや監査の所見、セキュリティインシデントやブリーチ、法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれるが、これらに限定したものではない。組織の裁量で、緊急時対応計画のテストや演習への参加は、テストや演習に続く教訓セッションを含め、緊急時対応計画のトレーニング要件を満たすことができる。

関連管理策：AT-2, AT-3, AT-4, CP-2, CP-4, CP-8, IR-2, IR-4, IR-9

拡張管理策:

(1) 緊急時対応トレーニング | シミュレーションイベント

危機的状況において職員が効果的に対応できるよう、シミュレーションイベントを緊急時対応トレーニングに組み込む。

詳解:シミュレーションイベントを使用することで、ウェブサイトを無効にするサイバー攻撃、サーバ上の組織のデータを暗号化するランサムウェア攻撃、組織の施設を損傷または破壊するハリケーン(強い熱帯低気圧)、ハードウェアまたはソフトウェアの障害など、実際の脅威イベントを職員が経験するための環境を作り出せる。

関連管理策:なし

(2) 緊急時対応トレーニング | トレーニング環境で使用されるメカニズム

より徹底した現実的な緊急時対応トレーニング環境を提供するために、運用で使用されているメカニズムを採用する。

詳解:運用のメカニズムとは、組織の目標を達成するために確立されたプロセス、または特定の組織のミッションまたは事業目的をサポートするシステムを指す。実際のミッションおよび事業プロセス、システム、および/または施設が、シミュレーションイベントを作り、緊急時対応トレーニング中にシミュレーションイベントの現実性を高めるために、使用される場合がある。

関連管理策:なし

参照資料:[SP 800-50]

CP-4 緊急時対応計画テスト

管理策:

a. 計画の有効性と計画実行の準備ができているかどうかを判断するために、[*設定:組織が定める頻度*]で[*設定:組織が定めるテスト*]を使用し、システムの緊急時対応計画をテストする。

b. 緊急時対応計画のテスト結果をレビューする。

c. 必要に応じて、是正措置を始める。

詳解:計画の有効性を判断し、潜在的な弱点を特定するための緊急時対応計画のテスト方法には、チェックリスト、ウォークスルーと机上演習、シミュレーション(平行または完全割り込み型)、包括的な演習がある。組織は、緊急時対応計画の要件に基づいてテストを実施する。テストには、緊急時対応運用にともなう、組織の運営、資産、個人への影響の判断を含む。組織は、是正措置の幅、深さ、適時性について、柔軟性と裁量を持っている。

関連管理策:AT-3, CP-2, CP-3, CP-8, CP-9, IR-3, IR-4, PL-2, PM-14, SR-2

拡張管理策:

(1) 緊急時対応計画テスト | 関連計画との調整

緊急時対応計画のテストを、関連計画を担当する部署と調整する。

詳解:組織のシステムの緊急時対応計画に関連する計画には、事業継続計画、災害時復旧計画、運用継続計画、危機コミュニケーション計画、重要インフラ計画、サイバーインシデント対応計画、居住者非常時計画が含まれる。緊急時対応計画テストの調整では、組織が関連する計画を取扱う部署を作ったり、そのような部署に特定の計画に協調させることは、求めていない。ただし、そのような部署が関連する計画を担当している場合、組織はそれらの部署と調整する必要がある。

関連管理策:IR-8, PM-8

(2) 緊急時対応計画テスト | 代替処理サイト

代替処理サイトで緊急時対応計画をテストする。

(a) 緊急時対応職員に施設と利用可能なリソースを習熟させる。

(b) 緊急時対応業務をサポートする代替処理サイトのケイパビリティを評価する。

詳解：代替処理サイトの状態は、一次サイトの状態とは大幅に異なる場合がある。代替サイトを訪問し、そのサイトで利用可能な実際のケイパビリティを体験する機会を持つことは、必須の組織のミッションおよび事業機能に影響を与える可能性のある潜在的な脆弱性に関する貴重な情報を提供することができる。オンサイト訪問は、テスト中に発見された脆弱性に対処するための緊急時対応計画を改善する機会を提供することもできる。

関連管理策：CP-7

(3) 緊急時対応計画テスト | 自動化されたテスト

[*設定：組織が定める自動化されたメカニズム*]を使用して、緊急時対応計画をテストする。

詳解：自動化されたメカニズムは、緊急時対応の問題をより完全にカバーし、より現実的なテストシナリオと環境を選択し、システムとサポートされているミッションおよび事業機能に効果的にストレスをかけることで、緊急時対応計画の徹底的かつ効果的なテストを促す。

関連管理策：なし

(4) 緊急時対応計画テスト | 完全な復旧および再構成

緊急時対応計画テストに、システムの完全な復旧および既知の状態への再構成を含める。

詳解：復旧は、組織のミッションと事業機能を復元するための緊急時対応計画措置を実施することである。再構成は復旧後に行われ、システムを完全に稼働状態に戻すための活動が含まれる。組織は、ハードウェア、ソフトウェアプログラム、データに関するシステム状態情報を含むシステムの既知の状態を確立する。システム状態情報を保持することで、システムの再起動が容易になり、ミッションおよび事業プロセスの中断が少なく、運用モードに戻すことができる。

関連管理策：CP-10, SC-24

(5) 緊急時対応計画テスト | 自己チャレンジ

システムまたはシステムコンポーネントを中断させ、悪影響を与えるよう、[*設定：組織が定めるシステムまたはシステムコンポーネント*]に対し、[*設定：組織が定めるメカニズム*]を採用する。

詳解：多くの場合、システムのレジリエンスを評価する最良の方法は、何らかの方法でシステムを中断させることである。組織が使用するメカニズムは、重要なシステムコンポーネントの停止または無効化、システムコンポーネントの構成の変更、重要な機能の低下（ネットワーク帯域幅の制限など）、特権の変更など、様々な方法で、システム機能またはシステムサービスを中断させることができる。自動化された、進行中の、シミュレーションされたサイバー攻撃とサービスの中断により、予期しない機能の依存関係が明らかになり、組織が実際のサイバー攻撃に直面した際のレジリエンスを確実にする能力を判断するのに役立つ。

関連管理策：なし

参照資料：[FIPS 199], [SP 800-34], [SP 800-84], [SP 800-160-2]

CP-5 緊急時対応計画の更新

[撤回：CP-2 に組み込まれた]

CP-6 代替保管サイト

管理策：

a. 代替保管サイトを確立する。これには、システムのバックアップ情報の保管と取り出しを

可能にするために必要な合意書を含む。

b. 代替保管サイトが一次サイトと同等の管理策を実施していることを確実にする。

詳解：代替保管サイトは地理的に一次保管サイトから離れており、一次保管サイトが利用できない場合に、情報とデータの複製コピーを保持する。同様に、一次処理サイトが利用できない場合に、代替処理サイトが処理ケイパビリティを提供する。緊急時対応要件をサポートする地理的に分散した建築物は、代替保管サイトと見なされる場合がある。代替保管サイトの合意書の対象となる項目には、代替サイトの環境条件、システムと施設のアクセス規則、物理的および環境的保護要件、バックアップ媒体の配備と取り出しの調整が含まれる。代替保管サイトは、組織のシステムの侵害、障害、中断が発生しても、組織が必須のミッションおよび事業機能を維持することができるように、緊急時対応計画の要件を反映する。

関連管理策：CP-2, CP-7, CP-8, CP-9, CP-10, MP-4, MP-5, PE-3, SC-36, SI-13

拡張管理策：

(1) 代替保管サイト | 一次サイトからの分離

同じ脅威に対する影響を低減するために、代替保管サイトが、一次保管サイトから十分に離れていることを確認する。

詳解：代替保管サイトに影響を与える脅威には、組織のリスクアセスメントで規定されており、自然災害、構造上の欠陥、敵対的攻撃、作為や不作為の誤りなどがある。組織は、懸念される脅威のタイプに基づいて、一次保管サイトと代替保管サイトの間の十分な分離の程度を決定する。敵対的攻撃などの脅威の場合、サイト間の分離の程度はそれほど重要ではない。

関連管理策：RA-3

(2) 代替保管サイト | 復旧時間および復旧ポイントの目標

復旧時間および復旧ポイントの目標に従って、復旧作業を容易にするよう、代替保管サイトを構成する。

詳解：組織は、緊急時対応計画の一環として、復旧時間と復旧ポイントの目標を設定する。代替保管サイトの構成には、物理的施設と、アクセシビリティと正確な実行を確実にする復旧操作をサポートするシステムが含まれる。

関連管理策：なし

(3) 代替保管サイト | アクセシビリティ

エリア全体に中断や災害が発生したイベントでの、代替保管サイトへの潜在的なアクセシビリティの問題を確認し、明確な軽減措置の要点を概説する。

詳解：エリア全体の中断とは、組織によるリスクアセスメントに基づき組織が決定した地理的範囲が広い中断のタイプを指す。明確な軽減措置には、最初に指定された代替サイトでアクセス問題が発生した場合に他の代替保管サイトでバックアップ情報を複製することや、代替サイトへの電子的アクセシビリティが中断された場合にバックアップ情報を取り出すための物理的アクセスの計画策定が含まれる。

関連管理策：RA-3

参照資料：[SP 800-34]

CP-7 代替処理サイト

管理策：

a. 代替処理サイトを確立する。これには、一次処理ケイパビリティが利用できない場合、[*設定：組織が定める、復旧時間と復旧ポイントの目標と一致する期間*]内に、必須のミッションや事業機能に関する[*設定：組織が定めるシステム運用*]の移転と再開を可能にするために必要な合意書を含む。

b. 代替処理サイトで、組織が定める移転と再開の期間内にサイトへの配備をサポートす

るために、移転と運用再開に必要な装置と備品を利用できるようにするか、サイトへの配備を支援するための契約を締結する。

c. 代替サイトには、一次サイトと同等の管理策を備える。

詳解：代替処理サイトは、地理的に一次処理サイトから離れており、一次処理サイトが利用できない場合に処理ケイパビリティを提供する。代替処理ケイパビリティは、物理的な処理サイト、またはクラウドベースのサービスプロバイダまたは他の内部的あるいは対外的に提供される処理サービスへのフェイルオーバーなど、他の代替手段を使用して対処することができる。緊急時対応要件をサポートする地理的に分散した建築物は、代替保管サイトと見なされる場合がある。代替処理サイトの合意書の対象となる管理策には、代替サイトの環境条件、アクセス規則、物理的および環境的保護要件、職員の移動と配置の調整が含まれる。要件は、組織のシステムの中断、侵害、機能停止があっても、必須のミッションおよび事業機能を維持するための緊急時対応計画の要件を反映するように、代替処理サイトに割り当てられる。

関連管理策：CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17, SC-36, SI-13

拡張管理策：

(1) 代替処理サイト | 一次サイトからの分離

同じ脅威に対する影響を低減するために、代替処理サイトが一次処理サイトから十分に離れていることを確認する。

詳解：代替処理サイトに影響を与える脅威は、組織のリスクアセスメントで定義されており、自然災害、構造上の欠陥、敵対的攻撃、作為や不作為の誤りなどがある。組織は、懸念される脅威のタイプに基づいて、一次処理サイトと代替処理サイトの間の十分な分離の程度を決定する。敵対的攻撃などの脅威の場合、サイト間の分離の程度はそれほど重要ではない。

関連管理策：RA-3

(2) 代替処理サイト | アクセシビリティ

広域にわたる中断や災害が発生した場合の、代替処理サイトへの潜在的なアクセシビリティの問題を特定し、明確な軽減措置の要点を概説する。

詳解：広域にわたる中断とは、組織によるリスクアセスメントに基づき組織が決定した地理的範囲が広い中断のタイプを指す。

関連管理策：RA-3

(3) 代替処理サイト | サービスの優先順位

可用性要件（復旧時間の目標を含む）に従って、サービスの優先順位の条項を含む代替処理サイトの合意書を策定する。

詳解：サービス合意書の優先順位は、サービスプロバイダとの交渉による合意書が関係する。この合意書では、組織が可用性要件と論理的代替処理サイトおよび／または物理的代替処理サイトの情報リソースの可用性と一致した優先度の扱いを受けることを確実にする。組織は、緊急時対応計画の一部として、復旧時間の目標を設定する。

関連管理策：なし

(4) 代替処理サイト | 使用準備

必須のミッションおよび事業機能をサポートする運用サイトとして機能できる代替処理サイトを準備する。

詳解：サイトの準備には、代替処理サイトでのシステム構成設定を、一次サイトでの設定要件と一致させること、および必要な物資と運搬上の考慮事項を確実に導入することが含まれる。

関連管理策：CM-2, CM-6, CP-4

(5) 代替処理サイト | 同等の情報セキュリティ保全措置

［撤回：CP-7 に組み込まれた］

(6) 代替処理サイト | 一次サイトに復帰できない状況

一次処理サイトへの復帰を妨げる状況に対して、計画し準備する。

詳解：自然災害（洪水やハリケーンなど）が施設を損傷または破壊し、同じ場所での再建が賢明でないと判断された場合など、組織が一次処理サイトに戻ることができない状況がありうる。

関連管理策：なし

参照資料：[SP 800-34]

CP-8 通信サービス

管理策：代替通信サービスを確立する。これには、一次通信ケイパビリティが、一次処理サイト、一次保管サイト、代替処理サイト、代替保管サイトで利用できない場合、[*設定：組織が定める期間*]内に、必須のミッションおよび事業機能の[*設定：組織が定めるシステム運用*]の再開を可能にするために必要な合意書を含む。

詳解：一次処理サイト、一次保管サイト、代替処理サイト、代替保管サイト向けの通信サービス（データと音声用）が、この管理策 CP-8 の対象である。代替通信サービスは、一次通信サービスが喪失しても、必須のミッションおよび事業機能を維持するための緊急時対応計画における継続性要件を反映したものである。組織では、一次サイト、代替サイトに異なる期間を指定できる。代替通信サービスには、追加の、組織が準備した、または商用の地上ベースの通信回路または通信回線、ネットワークベースの通信への取り組み、衛星の利用などがある。組織は、代替通信の合意書を締結する際に、可用性、サービス品質、アクセスなどの要素を考慮する。

関連管理策：CP-2, CP-6, CP-7, CP-11, SC-7

拡張管理策：

(1) 通信サービス | サービス提供の優先順位

(a) 可用性要件（復旧時間の目標を含む）に従って、サービスの優先順位の条項を含む一次通信サービスおよび代替通信サービスの合意書を策定する。

(b) 一次通信サービスおよび／または代替通信サービスが、通信事業者から提供されている場合、国家安全保障非常時準備（national security emergency preparedness）で使用されるすべての通信サービスについて、優先的通信サービスを要求する。

詳解：組織は、通信サービスプロバイダが、他の組織に対し、同様のサービス優先条項で、通信サービスを提供している場合、潜在的なミッションまたは事業へのインパクトを考慮する。優先的通信サービス（TSP：Telecommunications Service Priority）は、連邦通信委員会（FCC： Federal Communications Commission）のプログラムであり、通信サービスプロバイダ（固定電話会社や携帯電話会社など）に、理由を問わず、サービス中断に際し新しい回線を追加したり回線を復旧する必要がある場合に、プログラムに登録したユーザを優遇するように指示を行う。FCC が TSP プログラムの規則とポリシーを定め、国土安全保障省が TSP プログラムを管理している。TSP プログラムは常に有効であり、大規模な災害や攻撃の発生を前提にしていない。TSP プログラムに登録するには、連邦政府の公的支援が必要である。

関連管理策：なし

(2) 通信サービス | 単一障害点

一次通信サービスと単一障害点（SPOF）を共有する可能性を減らすよう、代替通信サービスを取得する。

詳解：特定の状況では、通信サービスプロバイダやサービスが同じ物理回線を共有する場合があり、単一障害点の脆弱性が増大する。通信サービスの実際の物理的伝送ケイパビリティについてプロバイダに透明性を持たせることが重要である。

関連管理策：なし

(3) 通信サービス | 一次プロバイダおよび代替プロバイダの分離

同じ脅威に対する影響を減らすために、一次サービスプロバイダとは別のプロバイダから代替通信サービスを取得する。

詳解：通信サービスに影響を与える脅威は、組織のリスクアセスメントで規定されており、自然災害、構造上の欠陥、サイバー攻撃または物理的攻撃、作為または不作為の誤りなどが含まれる。組織は、通信サービスプロバイダ間の共有インフラを最小限に抑え、サービス間の地理的距離を十分に確保することで、共通の影響を受けにくくすることができる。組織は、リスクアセスメントで取り上げられている分離ニーズを満たす代替通信サービスをそのサービスプロバイダが提供できる状況では、単一のサービスプロバイダの利用を考慮する場合がある。

関連管理策：なし

(4) 通信サービス | プロバイダの緊急時対応計画

(a) 一次通信および代替通信サービスプロバイダに緊急時対応計画を要求する。

(b) プロバイダの緊急時対応計画をレビューし、その計画が組織の緊急時対応要件を満たしていることを確実にする。

(c) [*設定：組織が定める頻度*]でプロバイダによる緊急時対応テストおよびトレーニングのエビデンスを取得する。

詳解：プロバイダの緊急時対応計画のレビューでは、そうした計画の非公開性を考慮する。状況によっては、プロバイダの緊急時対応計画の要約が、組織がレビュー要件を満たすための十分なエビデンスとしてもよい。通信サービスプロバイダは、国土安全保障省、州政府、地方自治体と連携して開催されている災害時復旧訓練に参加することもできる。組織は、サービスプロバイダの緊急時対応計画のレビュー、テスト、およびトレーニングに関するエビデンス要件を満たすために、これらのタイプの活動を利用できる。

関連管理策：CP-3, CP-4

(5) 通信サービス | 代替通信サービスのテスト

[*設定：組織が定める頻度*]で代替通信サービスをテストする。

詳解：代替通信サービスのテストは、サービスプロバイダとの契約上の合意書を通じて調整される。テストは、組織のミッションや機能の低下がないことを確実にするために、通常の運用と並行して行われる場合がある。

関連管理策：CP-3

参照資料：[SP 800-34]

CP-9 システムバックアップ

管理策：

a. [*設定：組織が定める復旧時間と復旧ポイントの目標と整合した頻度*]で[*設定：組織が定めるシステムコンポーネント*]のユーザレベルの情報をバックアップする。

b. [*設定：組織が定める復旧時間と復旧ポイントの目標と整合した頻度*]でシステムのシステムレベルの情報をバックアップする。

c. [*設定：組織が定める復旧時間と復旧ポイントの目標と整合した頻度*]でセキュリティおよびプライバシーの関連の文書を含む、システム文書のバックアップを実施する。

d. バックアップ情報の機密性、完全性、可用性を保護する。

詳解：システムレベルの情報には、システム状態情報、オペレーティングシステムソフトウェア、ミドルウェア、アプリケーションソフトウェア、およびライセンスが含まれる。ユーザレベルの情報には、システムレベルの情報以外の情報が含まれる。システムバックアップの完全性を保護するために採用されるメカニズムには、デジタル署名や暗号ハッシュ化などがある。輸送中のシステムバックアップ情報の保護は、管理策 MP-5 および SC-8 により対処する。システムのバックアップには、緊急時対応計画の要件と、情報をバックアップするための他の組織要件を反映

する。組織は、特定の分類の情報（個人の健康情報など）に関する要件を伴う法律、大統領令、指令、規則、ポリシーに従う必要がある。組織の職員は、そのような要件について政府機関のプライバシー保護責任者や法律顧問と協議する。

関連管理策：CP-2, CP-6, CP-10, MP-4, MP-5, SC-8, SC-12, SC-13, SI-4, SI-13

拡張管理策：

(1) システムバックアップ | 信頼性および完全性のテスト

媒体の信頼性および情報の完全性を検証するために、[*設定：組織が定める頻度*]でバックアップ情報をテストする。

詳解：組織は、バックアップ情報を確実に取り出せることを保証する必要がある。確実性は、バックアップ情報が保管されているシステムとシステムコンポーネント、情報を取り出すために使われる操作、および取り出される情報の完全性に関係する。確実性の各側面について、独立し特化したテストを利用することができる。例えば、代替保管サイトまたはバックアップサイトから、ランダムにサンプリングしたバックアップファイルを復号し移送（または伝送）し、その情報を一次処理サイトで同じ情報と比較することにより、そのような保証を与えることができる。

関連管理策：CP-4

(2) システムバックアップ | サンプリングを使用した復元テスト

緊急時対応計画テストの一部として、選択したシステム機能の復元にバックアップ情報のサンプルを使用する。

詳解：組織は、システム機能が正しく復元され、規定された組織のミッションをサポートできることを保証する必要がある。選択したシステム機能が緊急時対応計画のテスト中に完全に実行されることを確実にするため、バックアップ情報のサンプルを取り出して、機能が意図したとおりに動作しているかどうかを判断する。組織は、必要な保証レベルに基づいて、機能とバックアップ情報のサンプルサイズを決定することができる。

関連管理策：CP-4

(3) システムバックアップ | 重要な情報の分離保管

[*設定：組織が定める重要なシステムソフトウェアおよびその他のセキュリティ関連情報*]のバックアップのコピーを、別の施設または運用システムと併設されていない耐火コンテナに保管する。

詳解：重要な情報の分離保管は、バックアップ保管媒体のタイプに関係なく、すべての重要な情報に適用される。重要なシステムソフトウェアには、オペレーティングシステム、ミドルウェア、暗号鍵管理システム、侵入検知システムなどがある。セキュリティ関連の情報には、システムハードウェア、ソフトウェア、およびファームウェアコンポーネントのインベントリが含まれる。地理的に分散された建築物などを含む代替保管サイトは、組織の分離保管施設として機能する。組織は、代替保管サイト（データセンターなど）で自動バックアッププロセスを実装することにより、分離保管を実施できる。一般調達局（GSA：General Services Administration）は、セキュリティおよび耐火コンテナの基準と仕様を規定している。

関連管理策：CM-2, CM-6, CM-8

(4) システムバックアップ | 認可されていない変更からの保護

[撤回：CP-9 に組み込まれた]

(5) システムバックアップ | 代替保管サイトへの転送

[*設定：組織が定める復旧時間と復旧ポイントの目標と整合した期間と転送速度*]でシステムのバックアップ情報を代替保管サイトに転送する。

詳解：システムのバックアップ情報は、電子的に、または保管媒体の物理的輸送により、代替保管サイトに転送することができる。

関連管理策：CP-7, MP-3, MP-4, MP-5

(6) システムバックアップ | 冗長二次システム

一次システムと併設されておらず、情報の喪失や運用の中断なしに活性化できる冗長二次システムを維持することにより、システムのバックアップを実施する。

詳解：システムバックアップの効果は、情報の複製を含め、一次システムをミラーリングする冗長二次システムを維持することで達成できる。このタイプの冗長システムが導入されており、2 つのシステム間に十分な地理的距離がある場合、二次システムは代替処理サイトとしても機能する。

関連管理策：CP-7

(7) システムバックアップ | 削除や破壊に対する二重認可

[*設定：組織が定めるバックアップ情報*]の削除または破壊について、二重認可を実施する。

詳解：二重認可は、資格のある 2 人の個人がその作業を実施しない限り、バックアップ情報の削除または破壊が行われないことを確実にする。バックアップ情報を削除または破壊する個人は、提案された情報の削除または破壊が組織のポリシーおよび手順を反映しているかどうかを判断するスキルまたは専門知識を有する。二重認可は、二人担当制としても知られている。共謀のリスクを軽減するために、組織は他の個人に二重認可の職務をローテーションすることを考慮する。

関連管理策：AC-3, AC-5, MP-2

(8) システムバックアップ | 暗号化による保護

[*設定：組織が定めるバックアップ情報*]の認可されていない開示や変更を防止するために、暗号化のメカニズムを実装する。

詳解：暗号化のメカニズムの選択は、バックアップ情報の機密性と完全性を保護するニーズに基づいている。選択されるメカニズムの強度は、その情報のセキュリティ分類または機密性区分に見合ったものである。暗号化による保護は、一次と代替の両方の場所にある記憶装置内のシステムバックアップ情報に適用される。保管中の情報を保護するために暗号化のメカニズムを実装する組織は、暗号鍵管理ソリューションも考慮する。

関連管理策：SC-12, SC-13, SC-28

参照資料：[FIPS 140-3], [FIPS 186-4], [SP 800-34], [SP 800-130], [SP 800-152]

CP-10 システムの復旧および再構成

管理策：システムの中断、侵害、または障害の発生後、[*設定：組織が定める復旧時間と復旧ポイントの目標と整合した期間*]内で、システムを既知の状態に復旧し再構成する。

詳解：復旧は、組織のミッションおよび事業機能を回復するための緊急時対応計画措置を実施することである。再構成は、復旧後に行われ、システムを完全に稼働状態に戻すための措置が含まれる。復旧と再構成作業は、緊急時対応計画の要件と整合し、ミッションおよび事業の優先順位、復旧時間と復旧ポイントの目標、組織の指標を反映する。再構成には、復旧作業中に必要であった暫定システムケイパビリティの非活性化を含む。再構成には、完全に復元されたシステムケイパビリティのアセスメント、継続的監視措置の再設定、システムの再認可（必要に応じ）、将来のシステム中断、ブリーチ、侵害、障害に備えるためのシステムと組織の整備に関する措置も含まれる。復旧と再構成ケイパビリティには、自動化したメカニズムと手動による手順を含めることができる。組織は、緊急時対応計画の一環として、復旧時間と復旧ポイントの目標を設定する。

関連管理策：CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8, SC-24, SI-13

拡張管理策：

(1) システムの復旧および再構成 | 緊急時対応計画のテスト

[撤回：CP-4 に組み込まれた]

(2) システムの復旧および再構成 | トランザクションの復旧

トランザクションベースのシステムについて、トランザクションの復旧を実装する。

詳解:トランザクションベースのシステムには、データベース管理システムとトランザクション処理システムがある。トランザクションの復旧をサポートするメカニズムには、トランザクションのロールバックとトランザクションのジャーナル処理がある。

関連管理策:なし

(3) システムの復旧および再構成 | 代替セキュリティ管理策

[撤回:テーラリングにより対処される]

(4) システムの復旧および再構成 | 期間内の復元

システムコンポーネントの既知の稼働状態を示す、構成変更管理下にあって完全性が保護された情報から、[*設定:組織が定める復元期間*]内に、システムコンポーネントを復元するケイパビリティを提供する。

詳解:システムコンポーネントの復元には、システムコンポーネントを既知の稼働状態に復元するバックアップされたシステムイメージからの復元が含まれる。

関連管理策:CM-2, CM-6

(5) システムの復旧および再構成 | フェイルオーバーケイパビリティ

[撤回:SI-13 に組み込まれた]

(6) システムの復旧および再構成 | コンポーネントの保護

復旧と再構成に使用されるシステムコンポーネントを保護する。

詳解:システムの復旧および再構成のコンポーネント(例えば、ハードウェア、ファームウェア、ソフトウェア)の保護には、物理的管理策と技術的管理策がある。復旧と再構成に使用されるバックアップおよび復元のコンポーネントには、ルータ制御表、コンパイラ、その他のシステムソフトウェアが含まれる。

関連管理策:AC-3, AC-6, MP-2, MP-4, PE-3, PE-6

参照資料:[SP 800-34]

CP-11 代替通信プロトコル

管理策:運用の継続性を維持するために、[*設定:組織が定める代替通信プロトコル*]を採用しているケイパビリティを提供する。

詳解:緊急時対応計画とそれらの計画に関連する緊急時対応トレーニングやテストには、組織のシステムのレジリエンスを確立する一環として、代替通信プロトコルケイパビリティを取り入れる。通信プロトコルの切り替えは、ソフトウェアアプリケーションやシステムの運用面に影響を与える可能性がある。組織は、実装の前に代替通信プロトコル導入による潜在的な副作用をアセスメントする。

関連管理策:CP-2, CP-8, CP-13

拡張管理策:なし

参照資料:なし

CP-12 セーフモード

管理策:[*設定:組織が定める条件*]が検知された場合、[*設定:組織が定めるセーフモード運用の制約*]のもと、セーフモード運用に入る。

詳解:軍事作戦システム、民間宇宙運用システム、原子力発電所運用システム、航空管制運用システム(特にリアルタイム運用環境)などの重要なミッションと事業機能をサポートするシステムについて、組織は、これらのシステムを事前に規定されたセーフモード運用に切換える条件を特定できる。自動または手動のいずれかで活性化できるセーフモード運用は、これらの条件が発生した場合、システムが実行できるオペレーションを制限する。制限には、限定された電力

下で、または通信帯域幅の低減下で、選択された機能のみを実行できるようにすることが含まれる。

関連管理策：CM-2, SA-8, SC-24, SI-13, SI-17

拡張管理策：なし

参照資料：なし

CP-13 代替セキュリティのメカニズム

管理策：[*設定：組織が定めるセキュリティ機能*]を実装する主要な手段が利用できないか、侵害している場合、そのセキュリティ機能を充足するために、[*設定：組織が定める代替または補完のセキュリティのメカニズム*]を採用する。

詳解：代替のセキュリティのメカニズムの利用は、システムの復元力、緊急時対応計画、運用の継続性をサポートする。ミッションと事業の継続性を確保するために、組織は代替または補完のセキュリティのメカニズムを実装できる。これらのメカニズムは、一次的なメカニズムよりも効果が低い可能性がある。ただし、代替のメカニズムや補足のメカニズムをすぐに採用できるケイパビリティを持つことは、機能を実装する一次的な手段が復元するまで運用を縮小しなければならない場合、有害なインパクトを受ける可能性のあるミッションと事業の継続性を高める。そのような代替ケイパビリティを提供するために必要なコストと労力のレベルを考えると、代替のメカニズムや補足のメカニズムは、システム、システムコンポーネント、またはシステムサービスによって提供される重要なセキュリティケイパビリティにのみ適用される。例えば、組織は、多要素トークン（セキュアな認証を行うための標準的な手段）が侵害されている場合、役員、担当者、システム管理者にワンタイムパッドを発行することがある。

関連管理策：CP-2, CP-11, SI-13

拡張管理策：なし

参照資料：なし

3.7 識別および認証

識別および認証の要約表へのクイックリンク

IA-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。

   1. 以下の[*選択(1 つ以上):組織レベル;ミッション/事業プロセスレベル;システムレベル*]の識別および認証のポリシー。

      (a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、および準拠に対処する。

      (b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに適合している。

   2. 識別および認証のポリシーと関連する識別および認証の管理策の実装を促進するための手順。

b. 識別および認証のポリシーと手順の策定、文書化、および配布することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行の識別と認証をレビューし、更新する。

   1. ポリシーについて[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

   2. 手順について[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

詳解:識別および認証のポリシーと手順は、システムおよび組織で実装される IA ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に寄与する。したがって、セキュリティおよびプライバシープログラムが識別および認証のポリシーと手順の策定と連携していることが重要である。セキュリティおよびプライバシープログラムのポリシーと手順を組織レベルで確立することは望ましく、一般的には、ミッションまたはシステム固有のポリシーと手順を不要にすることができる。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映する複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムに対して規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述し、手順の対象である個人または役割向けとすることができる。手順は、システムのセキュリティおよびプライバシー計画の中に、または 1 つ以上の別の文書に文書化することもできる。識別および認証のポリシーと手順の更新を引き起こす可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれる。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策:AC-1, PM-9, PS-8, SI-12

拡張管理策:なし

参照資料:[OMB A-130], [FIPS 201-2], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-63-3], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4], [SP 800-100], [IR 7874]

IA-2 識別および認証（組織のユーザ）

管理策：組織のユーザを一意に識別および認証し、その一意の識別情報をそれらのユーザに代わって動作するプロセスに関連付ける。

詳解：組織は、[HSPD 12]の要件に準拠することにより、識別および認証の要件を満たすことができる。組織のユーザには、従業者、または組織が従業者と同等の地位にあると考えている個人（契約作業者、客員研究者など）が含まれる。ユーザの一意の識別と認証は、AC-14 で明示的に識別されたアクセスや、個人認証なしの認可されたグループオーセンティケータを利用したアクセスを除く、すべてのアクセスに適用される。プロセスはグループと役割の代理として実行されるので、組織はグループアカウント内の個人の一意の識別、または個人の活動の詳細な説明責任を求められる場合がある。

組織は、ユーザのアイデンティティを認証するために、パスワード、物理オーセンティケータ、生体認証を採用し、多要素認証の場合は、それらの組み合わせを採用する。組織のシステムへのアクセスは、ローカルアクセスまたはネットワークアクセスとして定義される。ローカルアクセスとは、ユーザまたはユーザに代わって動作するプロセスによる組織のシステムへのアクセスで、ネットワークを使用せず直接接続によりアクセスが行われる。ネットワークアクセスは、ネットワーク接続を介した、ユーザ（またはユーザに代わって動作するプロセス）による組織のシステムへのアクセスである（すなわち、非ローカルアクセス）。リモートアクセスは、外部ネットワークを介した通信を伴うネットワークアクセスの一種である。内部ネットワークには、ローカルエリアネットワークとワイドエリアネットワークがある。

組織が管理するエンドポイントと組織が管理しないエンドポイントとの間のネットワーク接続に、暗号化された仮想プライベートネットワークを使用することは、ネットワークを通過する情報の機密性と完全性を保護する観点から、内部ネットワークとして扱うことができる。非組織ユーザの識別および認証の要件は、IA-8 に記載されている。

関連管理策：AC-2, AC-3, AC-4, AC-14, AC-17, AC-18, AU-1, AU-6, IA-4, IA-5, IA-8, MA-4, MA-5, PE-2, PL-4, SA-4, SA-8

拡張管理策：

(1) 識別および認証（組織のユーザ）｜特権アカウントへの多要素認証

特権アカウントにアクセスするための多要素認証を実装する。

詳解：多要素認証では、認証を実現するために 2 つ以上の異なる要素を使用する必要がある。認証要素は、次のように定義される。ユーザが知っているもの（個人識別番号［PIN］など）、ユーザが持っているもの（暗号化プライベート鍵などの物理オーセンティケータなど）、ユーザ自身の特徴（生体認証など）。物理オーセンティケータを特徴とする多要素認証ソリューションには、時間ベースまたはチャレンジレスポンス方式のハードウェアオーセンティケータ、個人アイデンティティ検証（PIV：Personal Identity Verification）カードや国防総省（DoD：Department of Defense）の共通アクセスカード（CAC：Common Access Card）などのスマートカードがある。組織は、システムレベルで（ログオン時）、ユーザを認証することに加えて、アプリケーションレベルで、独自の裁量で認証メカニズムを採用し、セキュリティを強化することができる。アクセスのタイプ（ローカル、ネットワーク、リモート）に関係なく、特権アカウントは、リスクレベルに適した多要素オプションを使用して認証する。組織は、特定のタイプのアクセスに対して、追加のメカニズムや、より厳密な認証のメカニズムなどの追加のセキュリティ手段を追加できる。

関連管理策：AC-5, AC-6

(2) 識別および認証（組織のユーザ）｜非特権アカウントへの多要素認証

非特権アカウントにアクセスするための多要素認証を実装する。

詳解：多要素認証では、認証を実現するために 2 つ以上の異なる要素を使用する必要がある。認証要素は、次のように定義される。ユーザが知っているもの（個人識別番号［PIN］など）、ユーザが持っているもの（暗号化プライベート鍵などの物理的オーセンティケータなど）、ユーザ自身の特徴（生体認証など）。物理オーセンティケータを特徴とする多要素認証ソリューションには、時間ベースまたはチャレンジレスポンス方式のハードウェアオー

センティケータ、および個人アイデンティティ検証（PIV）カードや国防総省（DoD）の共通アクセスカード（CAC）などのスマートカードがある。組織は、システムレベルで（ログオン時）、ユーザを認証することに加えて、アプリケーションレベルで、独自の裁量で認証メカニズムを採用し、セキュリティを強化することができる。アクセスのタイプ（ローカル、ネットワーク、リモート）に関係なく、非特権アカウントは、リスクレベルに適した多要素オプションを使用して認証する。組織は、特定のタイプのアクセスに対して、追加のメカニズムや、より厳密な認証のメカニズムなどの追加のセキュリティ手段を追加できる。

関連管理策：AC-5

(3) 識別および認証（組織のユーザ）｜特権アカウントへのローカルアクセス

［撤回：IA-2(1)に組み込まれた］

(4) 識別および認証（組織のユーザ）｜非特権アカウントへのローカルアクセス

［撤回：IA-2(2)に組み込まれた］

(5) 識別および認証（組織のユーザ）｜グループ認証時の個人認証

共有アカウントまたは共有オーセンティケータが採用されている場合、共有アカウントまたは共有リソースへのアクセスを許可する前に、ユーザが個人認証されることを要求する。

詳解：共有グループ認証の前に、個人認証を行うことで、グループアカウントまたはグループオーセンティケータを使用するリスクを軽減できる。

関連管理策：なし

(6) 識別および認証（組織のユーザ）｜アカウントへのアクセス ― 別のデバイス

［*選択（1 つ以上）：特権アカウント；非特権アカウント*］への［*選択（1つ以上）：ローカルアクセス；ネットワークアクセス；リモートアクセス*］のための多要素認証を実装する。

(a) 要素の 1 つは、アクセスを取得するシステムとは別のデバイスで提供される。

(b) デバイスは、［*設定：組織が定めるメカニズムの強度に関する要件*］を満たす。

詳解：多要素認証において、要素の 1 つにアクセスしようとしているシステムとは別のデバイスを要求する目的は、システムに記憶されているオーセンティケータまたはクレデンシャルが侵害する可能性を減らすことである。敵対者は、このようなオーセンティケータまたはクレデンシャルを侵害し、その後、認可されたユーザになりすますことができる。要素の 1 つを別のデバイス（ハードウェアトークンなど）に実装すると、メカニズムの強度が高まり、認証プロセスの保証レベルが向上する。

関連管理策：AC-6

(7) 識別および認証（組織のユーザ）｜非特権アカウントへのネットワークアクセス ― 別のデバイス

［撤回：IA-2(6)に組み込まれた］

(8) 識別および認証（組織のユーザ）｜アカウントへのアクセス ― リプレイ攻撃耐性

［*選択（1 つ以上）：特権アカウント；非特権アカウント*］のアクセスについてリプレイ攻撃耐性のある認証のメカニズムを実装する。

詳解：以前の認証メッセージをリプレイして認証を成功させることが現実的でない場合は、認証プロセスはリプレイ攻撃に耐性を持つ。リプレイ攻撃耐性の技法には、時刻同期オーセンティケータや暗号化オーセンティケータなどのノンスやチャレンジ乱数を使用するプロトコルがある。

関連管理策：なし

(9) 識別および認証（組織のユーザ）｜非特権アカウントへのネットワークアクセス ― リプレイ攻撃耐性

［撤回：IA-2(8)に組み込まれた］

(10) 識別および認証（組織のユーザ）｜シングルサインオン

[*設定：組織が定めるシステムアカウントおよびサービス*]に対し、シングルサインオンケイパビリティを提供する。

詳解：シシングルサインオンを使用すると、ユーザは一度ログインすると、複数のシステムリソースにアクセスできる。組織は、シングルサインオンケイパビリティによって提供される運用効率と、単一の認証イベントを介して複数のシステムへのアクセスを許可することによってもたらされるリスクについて考慮する。シングルサインオンは、例えば、本来は多要素認証をサポートできない可能性のあるアプリケーションおよびシステム（既存および新規）に、多要素認証を追加できることにより、システムのセキュリティを向上させる機会を提供することができる。

関連管理策：なし

(11) 識別および認証（組織のユーザ）｜リモートアクセス ― 別のデバイス

［撤回：IA-2(6)に組み込まれた］

(12) 識別および認証（組織のユーザ）｜PIV クレデンシャルの受け入れ

PIV クレデンシャルを受け入れ、電子的に検証する。

詳解：個人アイデンティティ検証（PIV）に準拠したクレデンシャルの受け入れは、論理アクセス制御システムと物理アクセス制御システムを実装する組織に適用される。PIV 準拠のクレデンシャルは、FIPS 201 とその補足ガイダンス文書に従って、政府機関により発行されたクレデンシャルである。PIV カード発行者の妥当性と信頼性は、[SP 800-79-2]を用いて認可される。PIV 準拠のクレデンシャルの受け入れには、派生した PIV クレデンシャルが含まれ、その使用については[SP 800-166]で扱っている。DOD の共通アクセスカード（CAC）は、PIV クレデンシャルの一例である。

関連管理策：なし

(13) 識別および認証（組織のユーザ）｜経路外通信認証

[*設定：組織が定める条件*]の下で、[*設定：組織が定める経路外通信認証*]のメカニズムを実装する。

詳解：経路外通信認証とは、2 つの別個の通信経路を使用して、情報システムにアクセスするユーザまたはデバイスを識別し、認証することを指す。第 1 の経路（つまり、経路内通信経路）は、ユーザまたはデバイスを識別し、認証するために使用され、通常は、情報が流れる経路である。第 2 の経路（すなわち、経路外通信経路）は、認証および／または要求されたアクションを独立して検証するために使用される。例えば、ユーザは、アクセスしたいリモートサーバーに対してノートブックコンピュータを介して認証し、その通信経路を介してサーバの何らかのアクションを要求する。続いて、要求されたアクションがユーザからのものであることを確認するために、サーバは、ユーザの携帯電話に連絡する。ユーザは、個人に対する意図されたアクションであることを電話で確認するか、電話を介して認証コードを提供することができる。経路外通信認証は、実際の、または疑わしい「中間者」攻撃を軽減するために使用できる。アクティベーションの条件または評価基準には、疑わしい行為、新たな脅威の兆候、脅威レベルの上昇、または要求されたトランザクションにおける情報のインパクトレベルまたは機密性レベルが含まれる。

関連管理策：IA-10, IA-11, SC-37

参照資料：[FIPS 140-3], [FIPS 201-2], [FIPS 202], [SP 800-63-3], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4], [SP 800-79-2], [SP 800-156], [SP 800-166], [IR 7539], [IR 7676], [IR 7817], [IR 7849], [IR 7870], [IR 7874], [IR 7966]

IA-3 デバイスの識別および認証

管理策：[*選択（1つ以上）：ローカル、リモート、ネットワーク*]接続を確立する前に、[*設定：組織が定めるデバイスおよび／またはデバイスのタイプ*]を一意に識別し認証する。

詳解：一意のデバイス間の識別および認証を必要とするデバイスは、デバイスのタイプ、デバイス、またはデバイスのタイプとデバイスの組み合わせによって規定される。組織が定めるデバイス・タイプには、組織が所有していないデバイスを含む。システムは、ローカルおよびワイドエ

リアネットワーク上のデバイスを識別し認証するために、デバイス識別または組織の認証ソリューション（IEEE802.1x と拡張認証プロトコル［EAP：Extensible Authentication Protocol］、EAP-トランスポート層セキュリティ［TLS：Transport Layer Security］認証を備えた RADIUS サーバ、ケルベロス認証など）で、共有された既知情報（メディアアクセス制御［MAC：Media Access Control］、伝送制御プロトコル/インターネット プロトコル［TCP/IP：Transmission Control Protocol/Internet Protocol］など）を利用する。組織は、システムのセキュリティ分類とミッションや事業要件に基づいて、認証のメカニズムに求められる強度を決定する。デバイス認証を大規模に実装するには課題があるため、組織は、この管理策の適用を、ミッションや事業ニーズに基づいて、限られた数／タイプのデバイスに限定することができる。

関連管理策：AC-17, AC-18, AC-19, AU-6, CA-3, CA-9, IA-4, IA-5, IA-9, IA-11, SI-4

拡張管理策：

(1) デバイスの識別および認証 | 暗号双方向認証

暗号技術による双方向認証を使用し、［*選択（1 つ以上）：ローカル；リモート；ネットワーク*］接続を確立する前に、［*設定：組織が定めるデバイスおよび／またはデバイス・タイプ*］を認証する。

詳解：ローカル接続とは、ネットワークを使用せずに通信するデバイスとの接続である。ネットワーク接続とは、ネットワークを介して通信するデバイスとの接続である。リモート接続とは、外部ネットワークを介して通信するデバイスとの接続である。双方向認証は、よりリスクの高い接続について他のデバイスのアイデンティティを確認するための、より強力な保護措置を提供する。

関連管理策：SC-8, SC-12, SC-13

(2) デバイスの識別および認証 | 暗号双方向ネットワーク認証

［撤回：IA-3(1)に組み込まれた］

(3) デバイスの識別および認証 | 動的アドレス割り当て

(a) アドレスが動的に割り当てられる場合、［*設定：組織が定めるリース情報とリース期間*］に従って、デバイスに割り当てられる動的アドレス割り当てのリース情報とリース期間を規格化する。

(b) リース情報がデバイスに割り当てられた際、リース情報を監査する。

詳解：DHCP（Dynamic Host Configuration Protocol）は、クライアントがネットワークアドレス割り当てを動的に受けとる方法の一例である。

関連管理策：AU-2

(4) デバイスの識別および認証 | デバイス証明

［*設定：組織が定める構成管理プロセス*］によるデバイス証明に基づいて、デバイスの識別および認証を処理する。

詳解：デバイス証明とは、デバイスの構成と既知の動作状態に基づいたデバイスの識別および認証を指す。デバイス証明は、デバイスの暗号学的ハッシュにより決定できる。デバイス認証が識別および認証の手段である場合、デバイスへのパッチ適用と更新がセキュアに行われ、他のデバイスの識別および認証を中断しないよう、デバイスへのパッチ適用と更新が構成管理プロセスを介して処理されることが重要である。

関連管理策：CM-2, CM-3, CM-6

参照資料：なし

IA-4 識別子管理

管理策：次のように識別子を管理する。

a. 個人、グループ、役割、サービス、デバイスに識別子を割り当てるために、［*設定：組織が定める職員または役割*］から認可を得る。

b. 個人、グループ、役割、サービス、デバイスを識別する識別子を選択する。

c. 対象の個人、グループ、役割、サービス、デバイスに識別子を割り当てる。

d. [*設定：組織が定める期間*]の間、識別子の再利用を防止する。

詳解：一般的なデバイス識別子には、メディアアクセス制御（MAC）アドレス、インターネットプロトコル（IP）アドレス、またはデバイス固有のトークン識別子がある。個別識別子の管理は、共有システムアカウントには適用されない。通常、個別識別子は、それらの個人に割り当てられたシステムアカウントのユーザ名である。その場合、AC-2 のアカウント管理措置では、IA-4 により提供されるアカウント名を使用する。識別子管理は、必ずしもシステムアカウントに関連付けられていない個別識別子も扱う。識別子の再利用を防止することは、以前に使用された個人、グループ、役割、サービス、デバイスの識別子が、異なる個人、グループ、役割、サービス、デバイスに割り当てられないようにすることを意味する。

関連管理策：AC-5, IA-2, IA-3, IA-5, IA-8, IA-9, IA-12, MA-4, PE-2, PE-3, PE-4, PL-4, PM-12, PS-3, PS-4, PS-5, SC-37

拡張管理策：

(1) 識別子管理 | 公開識別子のアカウント識別子使用禁止

個人のアカウントとして公開識別子と同じシステムアカウント識別子の使用を禁止する。

詳解：公開識別子のアカウント識別子としての使用禁止は、電子メールやインスタントメッセージなどの通信に使用される公開されたアカウント識別子に適用される。電子メールアドレスの個別識別子セクションなど、一部の公開識別子と同じシステムアカウント識別子の使用を禁止することで、敵対者がユーザ識別子を推測することがより困難になる。アカウント識別子について、他の補助管理策を実装せずに公開識別子として禁止することは、識別子の推測を複雑にするだけである。オーセンティケータとアカウントを保護するためのクレデンシャルには、追加の保護が必要である。

関連管理策：AT-2, PT-7

(2) 識別子管理 | 監督者による認可

[撤回：IA-12(1)に組み込まれた]

(3) 識別子管理 | 複数の認証形態

[撤回：IA-12(2)に組み込まれた]

(4) 識別情報管理 | ユーザステータスの識別

[*設定：組織が定める個人のステータスを識別する特性*]で各個人を一意に識別することにより、個別識別子を管理する。

詳解：個人のステータスを識別する特性には、契約作業者、外国人、非組織のユーザがある。これらの特性によって個人のステータスを識別することで、組織の職員がコミュニケーションしている人々に関する追加情報が提供される。例えば、政府職員が電子メールメッセージの個人の送信先の 1 人が契約作業者であることを知っていると役立つ場合がある。

関連管理策：なし

(5) 識別子管理 | 動的管理

[*設定：組織が定める動的識別子ポリシー*]に従って、個別識別子を動的に管理する。

詳解：事前登録されたユーザの静的アカウントを割り当てる従来の識別アプローチとは対照的に、多くの分散システムは、事前に知られていないエンティティに対し実行時に識別子を割り当てる。事前に知られていないエンティティの識別子が実行時に割り当てられる場合、組織は識別子の動的な割り当てを予測して準備することができる。クレデンシャルと関連する識別子の有効性確認のために、適切な機関との間の事前に確立された信頼関係とメカニズムが不可欠である。

関連管理策：AC-16

(6) 識別子管理｜組織横断的な管理

識別子の組織横断的な管理のために、[*設定：組織が定める外部組織*]と調整する。

詳解：組織横断的な識別子管理は、情報の処理、保存、伝送を含む組織横断的な活動を実施する際に、個人、グループ、役割、デバイスを識別するケイパビリティを提供する。

関連管理策：AU-16, IA-2, IA-5

(7) 識別子管理｜対面による登録

［撤回：IA-12(4)に組み込また］

(8) 識別子管理｜ペアワイズ仮名識別子

ペアワイズ仮名識別子を生成する。

詳解：ペアワイズ仮名識別子は、特定の独立したリライングパーティで使用するためにアイデンティティプロバイダによって生成された不透明で推測不可能な加入者識別子である。利用者に関する識別情報を持たない別個のペアワイズ仮名識別子を生成することで、組織によって確立された運用要件を超えた利用者の活動追跡とプロファイリングを妨げる。ペアワイズ仮名識別子は、リライングパーティが相互関係の運用ニーズを正当化する実証可能な関係を示すことができる場合、またはすべての当事者がそのような方法での相互関係に同意する場合を除いて、各リライングパーティに固有である。

関連管理策：IA-5

(9) 識別子管理｜属性の維持および保護

[*設定：組織が定める保護された中央の記憶装置*]で、一意に識別された個人、デバイス、サービスの属性を維持する。

詳解：管理策 IA-2、IA-3、IA-8、IA-9 の対象となる各エンティティについて、中央の（保護された）記憶装置で、継続的に認証された各エンティティの属性を維持することが重要である。

関連管理策：なし

参照資料：[FIPS 201-2], [SP 800-63-3], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4]

IA-5 オーセンティケータ管理

管理策：以下によりシステムオーセンティケータを管理する。

a. 初回のオーセンティケータ配付の一環として、オーセンティケータを受け取る個人、グループ、役割、サービス、デバイスのアイデンティティを検証する。

b. 組織が発行したオーセンティケータの初期オーセンティケータ内容を定める。

c. オーセンティケータが、意図された使用のためのメカニズムについて十分な強度を備えていることを保証する。

d. オーセンティケータの初回配付管理手順、紛失、侵害、破損したオーセンティケータ管理手順、オーセンティケータの失効管理手順を規定し実装する。

e. オーセンティケータを初めて使用する前に、デフォルトのオーセンティケータを変更する。

f. [*設定：組織が定めるオーセンティケータのタイプごとの期間*]で、または[*設定：組織が定めるイベントを契機*]に、オーセンティケータの変更または更新を行う。

g. オーセンティケータの内容を認可されていない開示や変更から保護する。

h. オーセンティケータを保護するための特定の管理策を、個人に実施することを要求し、デバイスに実装する。

i. グループアカウントや役割アカウントの資格が変更された場合、それらのアカウントのオーセンティケータを変更する。

詳解：オーセンティケータには、パスワード、暗号デバイス、生体認証、証明書、ワンタイムパスワードデバイス、ID バッジなどがある。デバイスオーセンティケータには、証明書とパスワードが含まれる。初期のオーセンティケータの内容は、オーセンティケータの現在の内容（初期パスワードなど）である。対照的に、オーセンティケータの内容の要件には、特定の基準や特性（最小パスワード長など）が含まれている。開発者は、初期インストールおよび設定を可能にするために、工場出荷時の認証クレデンシャル（すなわち、パスワード）を備えたシステムコンポーネントを提供することができる。多くの場合、デフォルトの認証クレデンシャルはよく知られており、簡単に発見でき、重大なリスクをもたらす。個人のオーセンティケータを保護する要件は、個人が所有するオーセンティケータについては管理策 PL-4、PS-6 により実装できる。ハッシュ化または暗号化形式で記憶されたパスワード、管理者権限でアクセス可能な暗号化またはハッシュ化されたパスワードが入ったファイルを含む、組織のシステムに記憶されているオーセンティケータについては、管理策 AC-3、AC-6、SC-28 により実装できる。

システムは、様々なオーセンティケータの特性に対して、組織が定める設定および制限（最小パスワード長、時刻同期ワンタイムトークンの妥当性確認時間枠、生体認証の検証段階で許容される拒否回数など）により、オーセンティケータ管理をサポートする。オーセンティケータの所有を維持すること、オーセンティケータを他と共有しないこと、紛失、盗難、侵害されたオーセンティケータを直ちに報告することを含む、個人のオーセンティケータを保護するための措置をとることができる。オーセンティケータ管理には、一時的なアクセスのためだけで不要になるオーセンティケータの発行と取消しが含まれる。

関連管理策：AC-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, IA-9, MA-4, PE-2, PL-4, SC-12, SC-13

拡張管理策：

(1) オーセンティケータ管理 | パスワードによる認証

パスワードによる認証の場合、

(a) 一般的に使用される、予想される、または侵害されたパスワードのリストを維持し、[*設定：組織が定める頻度*]で、および組織のパスワードが直接的または間接的に侵害された疑いがある場合、リストを更新する。

(b) ユーザがパスワードを作成または更新する時に、そのパスワードが管理策 IA-5(1)(a)の一般的に使用される、予想される、または侵害されたパスワードのリストにないことを検証する。

(c) 暗号で保護されたチャネルを介してのみパスワードを送信する。

(d) 承認されたソルトキー導出関数を使用して、なるべくキー付きハッシュを使用してパスワードを記憶する。

(e) アカウント復旧時に新しいパスワードを即座に選択することを要求する。

(f) スペースやすべての印刷可能な文字を含む長いパスワードとパスフレーズをユーザが選択できるようにする。

(g) ユーザが強力なパスワードオーセンティケータを選択するのを支援する自動化ツールを採用する。

(h) [*設定：組織が定める構成および複雑さのルール*]を実施する。

詳解：パスワードによる認証は、単一要素認証で使用されるか、多要素認証で使用されるかに関係なく、パスワードが適用される。長いパスワードまたはパスフレーズは、短いパスワードよりも望ましい。実施された構成ルールは、使いやすさを低下させるが、わずかなセキュリティ上の利点を提供する。ただし、組織は、特定の状況下でパスワード生成に関する特定のルール（長いパスワードの最小文字長など）を規定することを選択することがあり、管理策 IA-5(1)(h)でこの要件を実施することができる。アカウントの復旧は、例えば、パスワードを忘れた場合などに起こることができる。暗号で保護されたパスワードには、パスワードのソルト化された一方向暗号ハッシュが含まれる。一般的に使用される、侵害された、または予想されるパスワードのリストには、以前のブリーチのデータベースから得たパスワード、辞書の単語、反復または連続した文字列が含まれる。リストには、サービス名、ユーザ名、およびそれらの派生語など、コンテキスト固有の単語が含まれる。

関連管理策：IA-6

(2) オーセンティケータ管理 | 公開鍵ベースの認証

(a) 公開鍵ベースの認証の場合、

(1) 対応する秘密鍵への認可されたアクセスを実施する。

(2) 認証されたアイデンティティを個人またはグループのアカウントにマッピングする。

(b) 公開鍵基盤（PKI：Public Key Infrastructure）が使用される場合、

(1) 証明書のステータス情報の確認を含め、受け入れられたトラストアンカーへの証明書パスを組み立て検証することにより、証明書を検証する。

(2) パスの発見と妥当性確認をサポートするために、失効データのローカルキャッシュを実装する。

詳解：公開鍵暗号技術は、個人、機械、デバイスにとって有効な認証のメカニズムである。PKI ソリューションの場合、証明書パスのステータス情報には、証明書失効リストまたは証明書ステータスプロトコル対応が含まれる。PIV カードの場合、証明書の妥当性確認には、証明書ポリシーの処理を含む、共通ポリシールートのトラストアンカーへの証明書パスの組み立てと検証が含まれる。パスの検出と妥当性確認をサポートするために失効データのローカルキャッシュを実装することで、組織がネットワークを介して失効情報にアクセスできない場合のシステムの可用性をサポートする。

関連管理策：IA-3, SC-17

(3) オーセンティケータ管理 | 対面または信頼できる外部関係者による登録

［撤回：IA-12(4)に組み込まれた］

(4) オーセンティケータ管理 | パスワード強度決定の自動化されたサポート

［撤回：IA-5(1)に組み込まれた］

(5) オーセンティケータ管理 | 出荷前のオーセンティケータ変更

システムコンポーネントの開発者とインストールを行う者に、出荷およびインストールの前に、一意のオーセンティケータを提供するか、デフォルトのオーセンティケータを変更するように要求する。

詳解：システムコンポーネントの出荷およびインストール前のオーセンティケータ変更は、開発者および／またはインストールを行う者に、出荷および／またはインストールに先立ってシステムコンポーネントの一意のオーセンティケータを提供および／またはデフォルトのオーセンティケータを変更することを要求することにより、システムインスール時にデフォルトのオーセンティケータを変更する組織の要件を拡張する。ただし、通常、市販の情報技術製品の開発者には適用されない。一意のオーセンティケータの要件は、システムまたはシステムコンポーネントを調達する際に組織が作成する取得文書に含めることができる。

関連管理策：なし

(6) オーセンティケータ管理 | オーセンティケータの保護

オーセンティケータの使用によりアクセスを許可する情報のセキュリティ分類に応じて、オーセンティケータを保護する。

詳解：複数のセキュリティ分類の情報を含むシステムの場合で、複数のセキュリティ分類間で信頼できる物理的または論理的な分離がされていない場合には、システムへのアクセスを許可するために使用されるオーセンティケータは、システムの情報の最も高いセキュリティ分類に対応して保護する。情報のセキュリティ分類は、セキュリティ分類化プロセスの一環として決定される。

関連管理策：RA-2

(7) オーセンティケータ管理 | 暗号化されていない静的オーセンティケータの組み込み禁止

暗号化されていない静的オーセンティケータが、アプリケーションや他の形式の静的ストレージに組み込まれていないことを確実にする。

詳解：アプリケーションに加えて、他の形式の静的ストレージには、アクセススクリプトとファンクションキーが含まれる。組織は、組み込まれた、または記憶されたオーセンティケータが、暗号化されているか暗号化されていないかを判断する際に、注意が必要である。オーセンティケータが記憶される方法で使用される場合、それらは暗号化されていないオーセンティケータと見なされる。

関連管理策：なし

(8) オーセンティケータ管理 | 複数のシステムアカウント

個人が複数のシステムにアカウントを持っていることによる侵害のリスクを管理するために、[*設定：組織が定めるセキュリティ管理策*]を実装する。

詳解：個人が複数のシステムにアカウントを持ち、パスワードなど同じオーセンティケータを使用する場合、1 つのアカウントの侵害が他のアカウントの侵害につながるリスクがある。代替アプローチとして、すべてのシステムで異なるオーセンティケータ（パスワード）を使用すること、シングルサインオンまたはフェデレーションのメカニズムを採用すること、またはすべてのシステムで何らかのワンタイムパスワードを使用することなどがある。組織は、複数のシステムアカウントのリスクを軽減するために、行動規則（ROB：Rules of Behavior：PL-4 を参照）およびアクセス合意書（PS-6 を参照）を使用することもできる。

関連管理策：PS-6

(9) オーセンティケータ管理 | フェデレーションによるクレデンシャル管理

[*設定：組織が定める外部組織*]とクレデンシャルをフェデレーションし利用する。

詳解：フェデレーションは、情報の処理、保存、伝送を含む組織間活動を実施する際に、個人とデバイスを認証するケイパビリティを組織に提供する。承認された外部組織の特定のリストを認証に使用することで、それらの組織が調査され信用されたことを保証するのに役立つ。

関連管理策：AU-7, AU-16

(10) オーセンティケータ管理 | 動的クレデンシャルのバインディング

[*設定：組織が定める結び付けルール*]を使用して、アイデンティティとオーセンティケータを動的にバインディングする。

詳解：認証には、アイデンティティと、アイデンティティの確認に使用されるオーセンティケータとの間をバインディングする何らかの方式が必要である。従来のアプローチでは、バインディングは、アイデンティティとオーセンティケータの両方をシステムに事前に提供することによって確立される。例えば、ユーザ名（すなわち、アイデンティティ）とパスワード（すなわち、オーセンティケータ）との間のバインディングは、システムで一対としてアイデンティティとオーセンティケータを提供することによって達成される。新しい認証技法により、アイデンティティとオーセンティケータの間のバインディングをシステムの外部で実装することができる。例えば、スマートカードのクレデンシャルでは、アイデンティティとオーセンティケータがスマートカード上でバインディングされる。これらのクレデンシャルを使用して、システムは事前提供されていないアイデンティティを認証し、認証後にアイデンティティを動的に提供できる。これらの状況では、組織はアイデンティティの動的提供を予想し対処できる。アイデンティティと関連するクレデンシャルを検証するためには、適切な権限を持つ事前に確立された信用できる関係とメカニズムが、不可欠である。

関連管理策：AU-16, IA-5

(11) オーセンティケータ管理 | ハードウェアトークンによる認証

[撤回：IA-2(1)および IA-2(2)に組み込まれた]

(12) オーセンティケータ管理 | 生体認証のパフォーマンス

生体情報に基づく認証については、[*設定：組織が定める生体情報の品質要件*]を満たすメカニズムを採用する。

詳解：ユーザ入力パスワードと保存されているパスワードの完全一致を提供するパスワードによる認証とは異なり、生体認証は完全一致を提供しない。生体情報のタイプと収集のメカニズムのタイプにより、提示された生体情報と、比較の基準となる保存されている生体情報とが多少異なる可能性がある。マッチングのパフォーマンスは、生体情報アルゴリズムが正規のユーザに対して正しくマッチングされ、他のユーザを拒否する割合である。生体情報のパフォーマンス要件には、システムで使用される生体情報マッチングアルゴリズムの精度を反映する一致率が含まれる。

関連管理策：AC-7

(13) オーセンティケータ管理 | キャッシュされたオーセンティケータの期限

[*設定：組織が定める期間*]以降は、キャッシュされたオーセンティケータの使用を禁止する。

詳解：ネットワークが利用できない場合、キャッシュされたオーセンティケータはローカルマシンへの認証に使用される。キャッシュされた認証情報が古い場合、認証情報の有効性が疑わしい場合がある。

関連管理策：なし

(14) オーセンティケータ管理 | PKI トラストストアの内容管理

PKI による認証の場合、ネットワーク、オペレーティングシステム、ブラウザ、アプリケーションなど、すべてのプラットフォームにインストールされた PKI トラストストアの内容を管理するための、組織全体の手法を採用する。

詳解：PKI トラストストアの内容を管理するための組織全体の手法は、組織全体の PKI による認証クレデンシャルの的確性と最新性を向上させるのに役立つ。

関連管理策：なし

(15) オーセンティケータ管理 | GSA 承認の製品およびサービス

アイデンティティ、クレデンシャル、アクセス管理には、一般調達局（GSA：General Services Administration）が承認した製品およびサービスのみを使用する。

詳解：一般調達局（GSA）承認の製品およびサービスは、GSA 適合プログラムを通じて承認され、該当する場合は GSA 承認製品リストに掲載された製品およびサービスである。GSA は、連邦政府トラストフレームワーク（FICAM：Federal Identity, Credential, and Access Management）のポリシー、技術、実装パターンに準拠する機能的でセキュアなシステムを設計および構築するためのチーム向けガイダンスを提供している。

関連管理策：なし

(16) オーセンティケータ管理 | 対面または信頼できる外部関係者によるオーセンティケータの発行

[*設定：組織が定める職員または役割*]による認可を得て、[*設定：組織が定める登録局*]により、[*選択：対面；信頼できる外部関係者*]が管理する[*設定：組織が定めるタイプおよび／または特定のオーセンティケータ*]の発行が行われることを要求する。

詳解：対面または信頼できる外部関係者によるオーセンティケータの発行は、アイデンティティ証明プロセスの統合的信頼性を高め、強化する。

関連管理策：IA-12

(17) オーセンティケータ管理 | 生体情報の提示型攻撃検知

生体認証のために提示型攻撃検知のメカニズムを採用する。

詳解：生体情報の特性は秘密の構成要素とならない。このような特性は、オンラインウェブアクセス、知識の有無にかかわらず顔画像を取得するカメラ付き電話での誰かの写真撮影、誰かが触れた物体の持ち上げ（見えない指紋など）、高解像度画像のキャプチャ（虹彩パターンなど）により、取得できる。生きていることの検知を含む提示型攻撃検知技術は、生体情報センサを破るものを作りにくくすることで、これらのタイプの攻撃リスクを軽減することができる。

関連管理策：AC-7

(18) オーセンティケータ管理｜パスワードマネージャー

(a) パスワードを生成および管理するために、[*設定：組織が定めるパスワードマネージャー*]を採用する。

(b) [*設定：組織が定める管理策*]を使用してパスワードを保護する。

詳解：静的パスワードが採用されているシステムでは、パスワードが適切に複雑であること、および同じパスワードが複数のシステムで採用されていないことを確実にすることが難しい場合が多い。パスワードマネージャーは、様々なアカウントに対して強力で異なるパスワードを自動的に生成して保存するため、この問題の解決策である。パスワードマネージャーを使用する潜在的なリスクは、敵対者がパスワードマネージャーによって生成されたパスワードのコレクションを標的にすることができることである。従って、パスワードのコレクションには、パスワードの暗号化（IA-5(1)(d)を参照）やパスワードのコレクションをオフラインでトークンに格納するなどの保護が必要である。

関連管理策：なし

参照資料：[FIPS 140-3], [FIPS 180-4], [FIPS 201-2], [FIPS 202], [SP 800-63-3], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4], [IR 7539], [IR 7817], [IR 7849], [IR 7870], [IR 8040]

IA-6 認証フィードバック

管理策：認証情報について、認可されていない個人による認証情報の悪用や使用から保護するために、認証プロセス中の認証情報のフィードバックを覆い隠す。

詳解：システムからの認証フィードバックは、認可されていない個人が認証のメカニズムを侵害することを可能にする情報を提供しない。比較的大型のモニタを備えたデスクトップやノートブックなど、一部のタイプのシステムでは、脅威（ショルダーサーフィンと呼ばれる）が重要になる場合がある。小さなディスプレイを備えたモバイルデバイスなど、他のタイプのシステムでは、その脅威はそれほど重要ではなく、小さなキーボードが原因の入力ミスの可能性の増加とバランスしている。従って、認証フィードバックを不明瞭にする手段は、その形態に応じて選択される。認証フィードバックを不明瞭にすることには、ユーザが入力デバイスにパスワードを入力するときにアスタリスクを表示すること、または非常に限定された時間内にフィードバックを覆い隠す前に表示することが含まれる。

関連管理策：AC-3

拡張管理策：なし

参照資料：なし

IA-7 暗号モジュール認証

管理策：認証に関し、適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインなどの要件を満たす暗号化モジュールの認証のメカニズムを実装する。

詳解：暗号モジュールにアクセスするオペレータを認証し、オペレータが要求された役割を引き受け、その役割内でサービスを実行する権限が与えられていることを検証するために、暗号モジュール内で、認証のメカニズムが必要になる場合がある。

関連管理策：AC-3, IA-5, SA-4, SC-12, SC-13

拡張管理策：なし

参照資料：[FIPS 140-3]

IA-8 識別および認証（非組織のユーザ）

管理策：非組織のユーザまたは非組織のユーザに代わって動作するプロセスを一意に識別および認証する。

詳解：非組織のユーザには、IA-2 で明示的にカバーされている組織のユーザ以外のシステムユーザが含まれる。非組織のユーザは、AC-14 で明示的に特定および文書化されている以外のアクセスについて、一意に識別および認証される。連邦政府のシステムにアクセスする非組織のユーザの識別および認証は、連邦政府情報、占有情報、またはプライバシー関連情報を保護するために必要となる場合がある（国家安全保障システムについては除く）。組織は、連邦政府の情報およびシステムへのアクセスの使いやすさを確保するニーズと、情報を保護しリスクを適切に軽減するニーズとのバランスをとる際に、セキュリティ、プライバシー、スケーラビリティ、実用性などの多くの要素を考慮する。

関連管理策：AC-2, AC-6, AC-14, AC-17, AC-18, AU-6, IA-2, IA-4, IA-5, IA-10, IA-11, MA-4, RA-3, SA-4, SC-8

拡張管理策：

(1) 識別および認証（非組織のユーザ）｜他の機関からの PIV クレデンシャルの受け入れ

他の連邦政府機関からの個人アイデンティティ検証（PIV：Personal Identity Verification）準拠のクレデンシャルを受け入れ、電子的に検証する。

詳解：他の連邦政府機関からの個人アイデンティティ検証（PIV）の受け入れは、論理的アクセス制御システムおよび物理的アクセス制御システムの両方に適用される。PIV のクレデンシャルは、FIPS 201 とその補足ガイダンス文書に従って、政府機関により発行されたクレデンシャルである。PIV カード発行者の妥当性と信頼性は、[SP 800-79-2]を用いて対処し承認される。

関連管理策：PE-3

(2) 識別および認証（非組織のユーザ）｜外部オーセンティケータの受け入れ

(a) NIST 準拠の外部オーセンティケータのみを受け入れる。

(b) 受け入れた外部オーセンティケータのリストを文書化し、維持する。

詳解：NIST 準拠の外部オーセンティケータのみを受け入れることは、一般にアクセス可能な組織のシステム（一般に公開されているウェブサイトなど）に適用される。外部オーセンティケータは非連邦政府機関によって発行され、[SP 800-63B]に準拠している。承認された外部オーセンティケータは、連邦政府全体の、技術、セキュリティ、プライバシー、組織成熟度の最小限の要件を満たしているか、上回ることにより、連邦政府のリライングパーティは、指定されたオーセンティケータ保証レベルでの認証トランザクションによる接続で、外部オーセンティケータを信頼することができる。

関連管理策：なし

(3) 識別および認証（非組織のユーザ）｜FICAM 承認製品の使用

［撤回：IA-8(2)に組み込まれた］

(4) 識別および認証（非組織のユーザ）｜定義したプロファイルの使用

アイデンティティ管理のための［*設定：組織が定めるアイデンティティ管理プロファイル*］に準拠する。

詳解：組織は、オープンなアイデンティティ管理規格に基づいて、アイデンティティ管理のプロファイルを定義する。オープンなアイデンティティ管理規格が実行可能で、堅牢で、信頼性が高く、持続可能で、文書化されたとおり相互運用可能であることを保証するために、連邦政府は、適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに照らして、規格および技術の実装をアセスメントし、適用範囲を定める。

関連管理策：なし

(5) 識別および認証（非組織のユーザ）｜PIV-I クレデンシャルの受け入れ

［*設定：組織が定めるポリシー*］を満たすフェデレーションしたクレデンシャルまたは PKI クレデンシャルを受け入れ、検証する。

詳解：PIV-I クレデンシャルの受け入れは、PIV、PIV-I、およびその他の商用または外部の

アイデンティティプロバイダによって実装できる。PIV-I 準拠のクレデンシャルの受け入れと検証は、論理的アクセス制御システムおよび物理的アクセス制御システムの両方に適用される。PIV-I クレデンシャルの受け入れと検証は、合衆国政府の PIV システムとの相互運用を望んでいて、連邦政府のリライングパーティにより信頼されている ID カードの非連邦政府発行者に対応している。連邦ブリッジ認証局（FBCA：Federal Bridge Certification Authority）の X.509 証明書ポリシーは、PIV-I 要件に対応している。PIV-I カードは、引用参照資料で定義されている PIV クレデンシャルと同一基準である。PIV-I クレデンシャルは、PIV-I プロバイダによって発行されたクレデンシャルであり、その PIV-I 証明書ポリシーは、連邦ブリッジ PIV-I 証明書ポリシーにマッピングされる。PIV-I プロバイダは、FBCA 証明書ポリシーで定義された PIV-I ポリシーの要件を満たすものとしてマップされ、承認されたポリシーを使用して、FBCA と（直接または別の PKI ブリッジを介して）相互認証される。

関連管理策：なし

(6) 識別および認証（非組織のユーザ）｜分離可能性

個人、クレデンシャルサービスプロバイダ、リライングパーティ間のユーザ属性または識別子のアサーション関係を分離するために、[*設定：組織が定める手段*]を実装する。

詳解：フェデレーションによるアイデンティティソリューションは、個人の追跡とプロファイリングにより、プライバシーリスクを増大させる可能性がある。識別子マッピングテーブルまたは暗号技法を使用して、クレデンシャルサービスプロバイダとリライングパーティを相互に見えなくしたり、アイデンティティ属性を送信者から見えにくくしたりすることで、これらのプライバシーリスクを軽減できる。

関連管理策：なし

参照資料：[OMB A-130], [FED PKI], [FIPS 201-2], [SP 800-63-3], [SP 800-79-2], [SP 800-116], [IR 8062]

IA-9 サービスの識別および認証

管理策：デバイス、ユーザ、その他のサービス、アプリケーションとの通信を確立する前に、[*設定：組織が定めるシステム サービスおよびアプリケーション*]を一意に識別および認証する。

詳解：識別および認証を必要とするサービスには、デジタル証明書を使用するウェブアプリケーションや、データベースに問い合わせるサービスやアプリケーションが含まれる。システムサービスやアプリケーションの識別および認証方法には、情報またはコード署名、履歴グラフ、サービスのソースを示す電子署名が含まれる。識別および認証請求の有効性に関する判断は、それらの判断のもとに動作するサービスとは別のサービスによって行うことができる。これは、分散システムアーキテクチャで行われることがある。そのような状況では、（実際の識別子と認証データの代わりに）識別および認証の判断が、それらの判断のもとで動作する必要があるサービスに提供される。

関連管理策：IA-3, IA-4, IA-5, SC-8

拡張管理策：

(1) サービスの識別および認証｜情報交換

［撤回：IA-9 に組み込まれた］

(2) サービスの識別および認証｜判断の伝達

［撤回：IA-9 に組み込まれた］

参照資料：なし

IA-10 リスクベース認証

管理策：システムにアクセスする個人に対し、特定の[*設定：組織が定める環境や状況*]のもとで[*設定：組織が定める追加の認証技法またはメカニズム*]を採用することを要求する。

詳解：敵対者は、組織が採用している個々の認証のメカニズムを侵害し、その後、正当なユーザになりすまそうとする可能性がある。この脅威に対処するために、組織は特定の技法やメカニズムを採用し、不審なふるまいをアセスメントするためのプロトコルを確立してもよい。不審なふるまいには、個人がそのミッション、役割、責任の一部として通常アクセスしない情報にアクセスすること、個人が定常的にアクセスするよりも多くの情報にアクセスすること、不審なネットワークアドレスから情報にアクセスしようとすることが、含まれる。事前に確立された条件やトリガーが発生した場合、組織は個人に追加の認証情報を提供するように要求できる。リスクベース認証の別の潜在的な用途は、アクセスされたレコードの数やタイプに基づいてメカニズムの強度を高めることである。リスクベース認証は、多要素認証のメカニズムの使用を回避するために置き換えられたり、多要素認証を使用しないものではなく、多要素認証の実装を強化することができるものである。

関連管理策：IA-2, IA-8

拡張管理策：なし

参照資料：[SP 800-63-3]

IA-11 再認証

管理策：[*設定：組織が定める環境や状況*]の場合、ユーザに再認証を要求する。

詳解：組織は、デバイスのロックに関連する再認証要件に加えて、役割、オーセンティケータやクレデンシャルが変更された場合、システムのセキュリティ分類が変更された場合、特権機能を実行する場合、一定期間経過後や定期的など、一定の状況下で、個人の再認証を要求する。

関連管理策：AC-3, AC-11, IA-2, IA-3, IA-4, IA-8

拡張管理策：なし

参照資料：なし

IA-12 アイデンティティ証明

管理策：

a. 適用される基準やガイドラインで規定されている適切なアイデンティティ保証レベル要件に基づき、システムへの論理アクセスのためのアカウントを必要とするユーザのアイデンティティを証明する。

b. ユーザアイデンティティを一意の個人に分解する。

c. アイデンティティのエビデンスを収集し、妥当性確認し、検証する。

詳解：アイデンティティ証明は、システムにアクセスするためのクレデンシャルを確立する目的で、ユーザのアイデンティティ情報を収集し、妥当性を確認し、検証するプロセスである。アイデンティティ証明は、ユーザの登録とそのアカウントの確立に対する脅威を軽減することを目的としている。アイデンティティ証明のためのアイデンティティ保証レベルを規定する基準およびガイドラインには、[SP 800-63-3]および[SP 800-63A]が含まれる。組織は、アイデンティティのエビデンスの収集を取り扱う法律、大統領令、指令、規則、ポリシーに従う必要がある。組織の職員は、そのような要件について政府機関のプライバシー保護責任者や法律顧問と協議する。

関連管理策：AC-5, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-8

拡張管理策：

(1) アイデンティティ証明 | 監督者認可

論理アクセス用のアカウントを取得するための登録プロセスに、監督者または主催者の認可を含むことを要求する。

詳解：登録プロセスの一部として監督者または主催者の認可を含めることにより、ユーザ

管理における繋がりにおいてそのアカウントを認識すること、アカウントが組織のミッションおよび機能を実行するために必須であること、ユーザの特権が組織で想定される責任と権限に対して適切であることを確実にするための、追加レベルの精査を行う。

関連管理策：なし

(2) アイデンティティ証明 | アイデンティティのエビデンス

個人識別のエビデンスを登録局に提示することを要求する。

詳解：文書によるエビデンス、または文書と生体情報の組み合わせなどのアイデンティティのエビデンスは、個人が不正な身分証明書を使用してアイデンティティを確立する可能性を減らすか、少なくとも潜在的な敵対者の作業要因を増加させる。許容できるエビデンスの形態は、ユーザアカウントに関連するシステム、役割、特権に対するリスクと一致している。

関連管理策：なし

(3) アイデンティティ証明 | アイデンティティのエビデンスの妥当性確認および検証

提示されたアイデンティティのエビデンスを、[*設定：組織が定める妥当性確認と検証の方法*]を通じて妥当性確認し、検証することを要求する。

詳解：アイデンティティのエビデンスの妥当性確認と検証により、正しいユーザのアカウントと識別子が確立され、オーセンティケータがそのユーザに結び付けられているという保証を高める。妥当性確認とは、エビデンスが真正であり、エビデンスに含まれるデータが正しく、最新であり、個人に関連していることを確認するプロセスを指す。検証は、要求されたアイデンティティとエビデンスを提示するユーザの実際の存在との間のつながりを確認および確立する。アイデンティティのエビデンスを妥当性確認および検証するための許容可能な方法は、ユーザアカウントに関連するシステム、役割、特権に対するリスクと一致している。

関連管理策：なし

(4) アイデンティティ証明 | 対面による妥当性確認および検証

アイデンティティ証明の妥当性確認と検証が、指定された登録局で対面で行われることを要求する。

詳解：対面証明は、個人の実在、身分証明書の提示、および指定された登録機関との実際の対面でのやり取りを必要とするため、不正なクレデンシャルが発行される可能性を低減する。

関連管理策：なし

(5) アイデンティティ証明 | アドレス確認

[*選択：登録コード；証明通知*]は、記録のユーザアドレス（物理アドレスまたはデジタルアドレス）を検証するために、経路外通信チャネルを介して配信することを要求する。

詳解：アイデンティティ証明プロセス中に、敵対者が正当なユーザになりすますことをより困難にするために、組織は、記録のアドレスに関連付けられた個人が、登録に参加した個人と同一であることを確実にする経路外通信方式を利用できる。確認は、仮登録コードまたは証明通知の形式をとることができる。これらの送付先アドレスは、ユーザが自己表明するのではなく、記録から取得される。アドレスは、物理アドレスまたはデジタルアドレスを含むことができる。自宅住所は、物理アドレスの例である。電子メールアドレスと電話番号は、デジタルアドレスの例である。

関連管理策：IA-12

(6) アイデンティティ証明 | 外部で証明されたアイデンティティの受け入れ

[*設定：組織が定めるアイデンティティ保証レベル*]で、外部で証明されたアイデンティティを受け入れる。

詳解：特に非 PIV ユーザのアイデンティティの不必要な再証明を限定するために、組織は、他の機関または組織による相応の保証レベルで実施された証明を受け入れる。証明は、組織のセキュリティポリシー、およびアクセスされるシステム、アプリケーション、情報

に適したアイデンティティ保証レベルと整合する。外部で証明されたアイデンティティを受け入れることは、機関や組織全体でフェデレーションしたアイデンティティを管理するための基本的なコンポーネントである。

関連管理策：IA-3, IA-4, IA-5, IA-8

参照資料：[FIPS 201-2], [SP 800-63-3], [SP 800-63A], [SP 800-79-2]

3.8 インシデント対応

インシデント対応の要約表へのクイックリンク

IR-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。

1. 以下の[*選択(1 つ以上):組織レベル;ミッション／事業プロセスレベル;システムレベル*]のインシデント対応のポリシー。

(a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、および準拠に対処する。

(b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに適合している。

2. インシデント対応のポリシーと関連するインシデント対応の管理策の実装を促進するための手順。

b. インシデント対応のポリシーと手順の策定、文書化、および配布することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行の識別および認証をレビューし、更新する。

1. ポリシーについて[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

2. 手順について[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

詳解:インシデント対応のポリシーと手順は、システムおよび組織で実装される IR ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に寄与する。したがって、セキュリティおよびプライバシープログラムがインシデント対応のポリシーと手順の策定と連携していることが重要である。セキュリティおよびプライバシープログラムのポリシーと手順を組織レベルで確立することは望ましく、一般的には、ミッションまたはシステム固有のポリシーと手順を不要にすることができる。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映する複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムに対して規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述し、手順の対象である個人または役割向けとすることができる。手順は、システムのセキュリティおよびプライバシー計画の中に、または 1 つ以上の別の文書に文書化することもできる。インシデント対応のポリシーと手順の更新を引き起こす可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれる。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策:PM-9, PS-8, SI-12

拡張管理策:なし

参照資料:[OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-50], [SP 800-61], [SP 800-83], [SP 800-100]

IR-2 インシデント対応トレーニング

管理策:

a. 設定した役割と責任に一致するシステムユーザに、以下のようにインシデント対応トレーニングを実施する。

1. インシデント対応の役割または責任を引き受けるか、システムへのアクセス権を取得してから[*設定:組織が定める期間*]内に。
2. システム変更により、必要になった場合に。
3. その後、[*設定:組織が定める頻度*]で。

b. [*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機に、インシデント対応トレーニングの内容をレビューし、更新する。

詳解:インシデント対応トレーニングは、組織の職員に設定された役割と責任に関連付けられ、適切な内容と詳細のレベルがそのようなトレーニングに含まれることを確実にする。例えば、ユーザは、誰に電話をかけるか、どのようにインシデントを認識するかを知るだけでよい場合がある。システム管理者は、インシデントの処理方法に関する追加のトレーニングを必要とする場合がある。インシデント対応者は、フォレンジック、データ収集技法、報告、システム復旧、システム復元に関するより具体的なトレーニングを受ける場合がある。インシデント対応トレーニングには、外部および内部のソースから不審な行為を特定して報告するユーザトレーニングが含まれる。ユーザ向けのインシデント対応トレーニングは、AT-2 または AT-3 の一部として提供される場合がある。インシデント対応トレーニング内容の更新を促す可能性のあるイベントには、インシデント対応計画のテストまたは実際のインシデントへの対応(教訓)、アセスメントまたは監査結果、適用される法律、大統領令、指令、規則、ポリシー、基準、ガイドラインの変更などがあるが、これらに限定されない。

関連管理策:AT-2, AT-3, AT-4, CP-3, IR-3, IR-4, IR-8, IR-9

拡張管理策:

(1) インシデント対応トレーニング | シミュレーションイベント

危機的状況下で職員が必要とする対応を容易にできるように、シミュレーションイベントをインシデント対応トレーニングに組み込む。

詳解:組織は、インシデント対応計画でインシデントに対応するための要件を規定する。シミュレーションイベントをインシデント対応トレーニングに組み込むことで、職員が個人の責任を理解し、危機的状況でどのような行動を取るべきかを確実に理解することができる。

関連管理策:なし

(2) インシデント対応トレーニング | 自動化されたトレーニング環境

[*設定:組織が定める自動化されたメカニズム*]を使用して、インシデント対応トレーニング環境を提供する。

詳解:自動化されたメカニズムは、より完全で現実的なインシデント対応教育環境を提供することができる。これは、例えば、インシデント対応の重要な点をより完全にカバーし、より現実的なトレーニングのシナリオと環境を選択し、インシデント対応ケイパビリティに重点を置くことで達成できる。

関連管理策:なし

(3) インシデント対応トレーニング | ブリーチ

組織がブリーチを報告するプロセスを含め、ブリーチを特定して対応する方法に関するインシデント対応トレーニングを提供する。

詳解:連邦政府機関の場合、個人情報に関係するインシデントは、ブリーチと見なされる。ブリーチは、認可されていないユーザが個人情報にアクセスするまたはアクセスすることが予想される場合や、認可されたユーザが認可された目的以外で個人情報にアクセスするまたはアクセスすることが予想される場合、制御の喪失、侵害、認可されていない開

示、認可されていない情報取得、同様の事態の発生をもたらす。インシデント対応トレーニングでは、紙媒体、口頭、電子媒体などのあらゆる媒体または形式の情報を伴う確認されたブリーチと疑わしいブリーチの両方を報告する個人の義務に重点をおく。インシデント対応トレーニングには、ブリーチをシミュレーションする机上演習が含まれる。IR-2(1)を参照。

関連管理策：なし

参照資料：[OMB M-17-12], [SP 800-50]

IR-3 インシデント対応テスト

管理策：[*設定：組織が定める頻度*]で、[*設定：組織が定めるテスト*]を使用して、システムのインシデント対応ケイパビリティの有効性をテストする。

詳解：組織は、インシデント対応ケイパビリティの有効性を判断し、潜在的な弱点または欠陥を特定するために、インシデント対応ケイパビリティをテストする。インシデント対応テストには、チェックリスト、ウォークスルーや机上演習、シミュレーション（平行型または完全割り込み型）の利用が含まれる。インシデント対応テストには、インシデント対応のための組織の運営および資産、個人に対する効果の判断を含めることができる。定性的および定量的データの利用は、インシデント対応プロセスの有効性を判断するのに役立つ。

関連管理策：CP-3, CP-4, IR-2, IR-4, IR-8, PM-14

拡張管理策：

(1) インシデント対応テスト | 自動化されたテスト

[*設定：組織が定める自動化されたメカニズム*]を使用してインシデント対応ケイパビリティをテストする。

詳解：組織は、自動化されたメカニズムを使用して、インシデント対応ケイパビリティをより完全に効果的にテストする。これは、インシデント対応の重要な点をより完全にカバーし、より現実的なテストシナリオと環境を選択し、インシデント対応ケイパビリティに重点を置くことで達成できる。

関連管理策：なし

(2) インシデント対応テスト | 関連計画との調整

インシデント対応テストを、関連計画を担当する組織の部署と調整する。

詳解：インシデント対応テストに関連する組織の計画には、事業継続計画、災害復旧計画、運用継続計画、緊急時対応計画、危機コミュニケーション計画、重要インフラ計画、居住者緊急対応計画が含まれる。

関連管理策：なし

(3) インシデント対応テスト | 継続的改善

テストからの定性的および定量的データを使用して、以下を行う。

(a) インシデント対応プロセスの有効性を判断する。

(b) インシデント対応プロセスを継続的に改善する。

(c) 適格で一貫性があり再現可能な形式のインシデント対応手段と指標を提供する。

詳解：インシデント対応措置が意図したとおりに機能するように、組織は、インシデント対応パフォーマンスを継続的に改善する取り組みの一環として、インシデント対応プログラムをアセスメントするために、指標と評価基準を利用することがある。これらの取り組みにより、インシデント対応の有効性が向上し、インシデントのインパクトが軽減される。

関連管理策：なし

参照資料：[OMB A-130], [SP 800-84], [SP 800-115]

IR-4 インシデント対応

管理策:

a. インシデント対応計画と整合し、準備、検知と分析、封じ込め、根絶、復旧を含むインシデント処理ケイパビリティを実装する。

b. インシデント対応措置と緊急時対応計画措置を調整する。

c. 進行中のインシデント対応措置から学んだ教訓をインシデント対応手順、トレーニング、テストに組み込み、それに対応した結果として生じる変更を実装する。

d. インシデント対応措置の厳密さ、強度、範囲、結果が、組織全体で比較可能で、予測可能であることを確実にする。

詳解:組織は、インシデント対応ケイパビリティが、組織のシステムのケイパビリティと、それらのシステムによってサポートされているミッションおよび事業プロセスに依存していることを認識する。組織は、インシデント対応を、ミッションおよび事業プロセスとシステムの定義、設計、開発の一部と見なしている。インシデント関連情報は、監査監視、物理的アクセス監視、ネットワーク監視、ユーザまたは管理者報告、報告されたサプライチェーンのイベントなど、様々なソースから取得できる。効果的なインシデント対応ケイパビリティには、多くの組織のエンティティ(例えば、ミッションまたは事業オーナー、システムオーナー、認可権限のある担当者、人事部門、物理セキュリティ部門、人事セキュリティ部門、法務部門、リスク管理者[部署]、運用職員、調達部門)間の調整が含まれる。疑いのあるセキュリティインシデントには、悪意のあるコードを含む可能性のある不審な電子メールの受信が含まれる。疑いのあるサプライチェーンインシデントには、組織のシステムまたはシステムコンポーネントへの偽造ハードウェアまたは悪意のあるコードの差し込みが含まれる。連邦政府機関の場合、個人情報を含むインシデントは、ブリーチと見なされる。ブリーチは、認可されていないユーザが個人情報にアクセスするまたはアクセスすることが予想される場合、認可されたユーザが認可された目的以外で個人情報にアクセスするまたはアクセスすることが予想される場合、認可されていない開示、制御の喪失、認可されていない情報取得、侵害、同様の事態の発生をもたらす。

関連管理策:AC-19, AU-6, AU-7, CM-6, CP-2, CP-3, CP-4, IR-2, IR-3, IR-5, IR-6, IR-8, PE-6, PL-2, PM-12, SA-8, SC-5, SC-7, SI-3, SI-4, SI-7

拡張管理策:

(1) インシデント対応 | 自動化されたインシデント対応プロセス

[*設定:組織が定める自動化されたメカニズム*]を使用して、インシデント処理プロセスをサポートする。

詳解:インシデント対応プロセスをサポートする自動化されたメカニズムには、実際の対応データの収集、完全なネットワークパケットキャプチャ、フォレンジック分析を支援するオンラインのインシデント管理システムやツールが含まれる。

関連管理策:なし

(2) インシデント対応 | 動的再構成

インシデント対応ケイパビリティの一部として、[*設定:組織が定めるシステムコンポーネント*]の[*設定:組織が定める動的再構成のタイプ*]を含める。

詳解:動的再構成には、ルータルール、アクセス制御リスト、侵入検知システムや侵入防止システムのパラメータ、ガード装置やファイアウォールのフィルタルールの変更が含まる。組織は、システムの動的再構成を実施して、攻撃を阻止し、攻撃者を誤った方向に向け、システムコンポーネントを分離することにより、ブリーチや侵害による被害の広がりを限定することができる。組織は、サイバー脅威に効果的に対処するための迅速な対応の潜在的なニーズを考慮して、再構成ケイパビリティの規定に、システムの再構成を達成するための明確な時間枠を含める。

関連管理策:AC-2, AC-4, CM-2

(3) インシデント対応 | 運用の継続性

[*設定:組織が定めるインシデントの種類*]を特定し、組織のミッションと事業機能の継続を確保するために、それらのインシデントに対応して[*設定:インシデントの種類に対*]

応して実施する組織が定める措置]をとる。

詳解:インシデントの種類には、設計や実装の誤りや手抜かりによる誤動作、標的型の悪意のある攻撃、非標的型の悪意のある攻撃が含まれる。インシデント対応措置には、秩序だったシステムの縮退運用、システムのシャットダウン、手動モードやシステムが異なる方法で動作する代替技術の起動へのフォールバック、代替手段の採用、代替の情報フロー、システムが攻撃を受けた場合に備えて用意してあるモードでの運用などが含まれる。組織は、インシデント発生時の運用継続要件が、IR-4(5)の一部として指定されているシステムを自動的に無効にするケイパビリティと矛盾するかどうかを考慮する。

関連管理策:なし

(4) インシデント対応 | 情報の相互関連付け

インシデント意識向上と対応に関する組織全体の見方ができるよう、インシデント情報と個々のインシデント対応を相互に関連付ける。

詳解:場合によっては、敵対的なサイバー攻撃などの脅威イベントは、組織によって確立された様々な報告や報告手順など、様々なソースからの情報をまとめることによってのみ気づくことができる。

関連管理策:なし

(5) インシデント対応 | システムの自動無効化

[*設定:組織が定めるセキュリティ侵害*]が検知された場合、システムを自動的に無効にする設定可能なケイパビリティを実装する。

詳解:組織は、システムを自動的に無効にするケイパビリティが、CP-2 または IR-4(3)の一部として規定された運用継続要件と矛盾するかどうかを考慮する。セキュリティ侵害には、システムの完全性を侵害したり組織の情報を漏出させるサイバー攻撃や、組織のミッションや機能に有害なインパクトを及ぼしたり個人の安全を脅かしたりする可能性のあるソフトウェアプログラムの重大な欠陥などがある。

関連管理策:なし

(6) インシデント対応 | インサイダー脅威

インサイダー脅威を含むインシデントに対するインシデント対応ケイパビリティを実装する。

詳解:インサイダー脅威を含むインシデント処理に明確に焦点を当てることで、このタイプの脅威と、適切でタイムリーな対応を行うための明確なインシデント対応ケイパビリティのニーズをさらに重要視する。

関連管理策:なし

(7) インシデント対応 | インサイダー脅威 — 組織内連携

[*設定:組織が定めるエンティティ*]とインサイダー脅威のインシデント対応ケイパビリティを連携させる。

詳解:インサイダー脅威インシデントのインシデント対応(準備、検知と分析、封じ込め、根絶、復旧など)には、ミッションまたは事業オーナー、システムオーナー、人材部門、調達部門、人事部門、物理セキュリティ部門、政府機関の情報セキュリティ責任者、運用職員、リスク管理者(部署)、政府機関のプライバシー保護責任者、法律顧問などの多くの組織のエンティティ間の連携が必要である。さらに、組織は、連邦政府、州、地方の法執行機関からの外部サポートを必要とする場合がある。

関連管理策:なし

(8) インシデント対応 | 外部組織との相互関連付け

インシデント意識向上とより効果的なインシデント対応に関する組織横断の見方ができるよう、[*設定:組織が定める外部組織*]と[*設定:組織が定めるインシデント情報*]を関連付け、共有するよう調整する。

詳解:ミッションや事業パートナー、軍事や連合パートナー、顧客、開発者などの外部組織

とのインシデント情報の連携は、大きなメリットをもたらす。組織を横断した調整は、重要なリスクマネジメントケイパビリティとして役立てることができる。このケイパビリティは、組織が、様々なソースからの情報を活用して、組織の運用、資産、個人に影響を与える可能性のあるインシデントやブリーチに効果的に対応できるようにする。

関連管理策：AU-16, PM-16

(9) インシデント対応 | 動的対応ケイパビリティ

インシデントに対応するために、[*設定：組織が定める動的対応ケイパビリティ*]を採用する。

詳解：動的対応ケイパビリティは、インシデント対応に関する新規または代替の組織ケイパビリティをタイムリーに展開することを目的としている。これには、ミッションおよび事業プロセスレベルと、システムレベルで実装されるケイパビリティが含まれる。

関連管理策：なし

(10) インシデント対応 | サプライチェーンとの連携

サプライチェーンに関与する他の組織とサプライチェーンのイベントに関連するインシデント対応措置を連携する。

詳解：サプライチェーン活動に関与する組織には、製品開発者、システムインテグレータ、製造事業者、包装事業者、組立事業者、販売代理事業者、ベンダ、再販事業者が含まれる。サプライチェーンのインシデントは、サプライチェーンを通して、またサプライチェーンに至るあらゆる場所で発生する可能性があり、一次または二次プロバイダ、情報技術製品、システムコンポーネント、開発プロセスや開発職員、流通過程や倉庫施設が関係する、侵害やブリーチが含まれる。組織は、情報交換協定でインシデント情報を保護および共有するためのプロセス、インシデントを政府監視機関（連邦調達安全保障会議など）に報告する義務について考慮する。

関連管理策：CA-3, MA-2, SA-9, SR-8

(11) インシデント対応 | 統合インシデント対応チーム

[*設定：組織が定める期間*]内に、組織が特定した任意の場所に展開できる統合インシデント対応チームを立ち上げ、維持する。

詳解：統合インシデント対応チームは、インシデントをアセスメントし、文書化し、対応する専門家のチームであり、組織のシステムとネットワークを迅速に復旧し、将来のインシデントを回避するために必要な管理策を実装できるようにする。インシデント対応チームの職員には、フォレンジック分析者や悪意のあるコードのアナリスト、ツール開発者、システムセキュリティやプライバシー技術者、リアルタイム運用職員が含まれる。インシデント処理ケイパビリティには、エビデンスの迅速なフォレンジック保存、侵入の分析と侵入への対応が含まれる。一部の組織では、インシデント対応チームは組織横断的なエンティティとすることができる。

統合インシデント対応チームは、情報共有を促進し、組織の職員（開発者、実装者、運用者など）が、脅威に関するチームの知識を活用して、組織が侵入をより効果的に阻止できるようにする防御策を実装できるようにする。さらに、統合チームは、侵入の迅速な検知、適切な軽減策の策定、効果的な防御策の展開に努める。例えば、侵入が検知された場合、統合チームは、オペレータの適切な対応を迅速に策定し、新しいインシデントを過去の侵入に関する情報と関連付け、進行中のサイバーインテリジェンスの開発を強化することができる。統合インシデント対応チームは、運用のテンポや特定のミッションや事業機能に関連する敵対者の戦術、技法、手順をより適切に特定し、それらのミッションや事業機能を中断しない方法で対応措置を定める。インシデント対応ケイパビリティをレジリエンスのあるものにするために、インシデント対応チームを組織内に分散させることができる。

関連管理策：AT-3

(12) インシデント対応 | 悪意のあるコードおよびフォレンジック分析

インシデント後に、システムに残っている悪意のあるコードおよび／またはその他の残留物を分析する。

詳解：隔離された環境で注意深く処理する場合、悪意のあるコードを分析し、セキュリティインシデントやブリーチのその他の残留物を分析することで、組織は敵対者の戦術、技法、手順を理解することができる。それはまた、敵対者のアイデンティティや、いくつかの明確な特徴を示すことができる。さらに、悪意のあるコードの分析は、組織が将来のインシデントに対する対応策を策定するのに役立つ。

関連管理策：なし

(13) インシデント対応 | ふるまい分析

[*設定：組織が定める環境またはリソース*]に対する、または関連する、異常なふるまいや不審な敵対的ふるまいを分析する。

詳解：組織が欺くための環境を維持している場合、その環境でのふるまいを分析することで、敵対者が標的とするリソースや、インシデントやイベントのタイミングを分析することで、敵対的な戦術、技法、手順を理解することができる。欺くための環境の外部で、異常な敵対的なふるまい（例えば、システムのパフォーマンスや使用パターンの変化）や不審なふるまい（例えば、特定のリソースの場所についての検索の変化）を分析することで、組織にそのようなふるまいについての見識を与えることができる。

関連管理策：なし

(14) インシデント対応 | セキュリティオペレーションセンター

セキュリティオペレーションセンターを設立し、維持する。

詳解：セキュリティオペレーションセンター（SOC：Security Operations Center）は、組織のセキュリティオペレーションおよびコンピュータネットワーク防御の中心である。SOC の目的は、組織のシステムやネットワーク（すなわち、サイバーインフラ）を継続的に防御および監視することである。SOC は、サイバーセキュリティインシデントをタイムリーに、検知、分析、対応する責任を負う。組織は、SOC にスキルのある技術職員および運用職員（セキュリティアナリスト、インシデント対応職員、システムセキュリティエンジニアなど）を配置し、複数のソースからの脅威およびセキュリティ関連イベントのデータを監視、融合、関連付け、分析、対応するために、技術的管理策、マネジメント管理策、運用管理策（監視、スキャン、フォレンジックツールなど）の組み合わせを実装する。これらのソースには、境界防御、ネットワークデバイス（ルータ、スイッチなど）、エンドポイントエージェントのデータフィードが含まれる。SOC は、組織がシステムと組織のセキュリティ態勢を決定するのに役立つ包括的な状況認識ケイパビリティを提供する。SOC のケイパビリティは、様々な方法で取得できる。大規模な組織では専用の SOC を実装してもよく、小規模な組織では SOC のケイパビリティを提供するためにサードパーティ組織を利用してもよい。

関連管理策：なし

(15) インシデント対応 | 広報活動および評判の修復

(a) インシデントに関連する広報活動を管理する。

(b) 組織の評判を回復するための手段を採用する。

詳解：一般の人々の注意を引いた、組織に否定的な影響を与えた、組織の構成員（パートナー、顧客など）に影響を与えたインシデントに対処するための戦略を導入することが組織にとって重要である。そのような世間の注目は、組織にとって非常に有害であり、そのミッションや事業機能を遂行する能力に影響を与える可能性がある。組織の評判を回復するために事前対策を講じることは、組織の構成員の信頼と信用を再確立するための重要な側面である。

関連管理策：なし

参照資料：[FASC18], [41 CFR 201], [OMB M-17-12], [SP 800-61], [SP 800-86], [SP 800-101], [SP 800-150], [SP 800-160-2], [SP 800-184], [IR 7559]

IR-5 インシデント監視

管理策：インシデントを追跡して文書化する。

詳解：インシデントの文書化には、インシデントの詳細、傾向、処理の評価はもちろん、各インシデントの記録、インシデントのステータス、フォレンジックに必要なその他の関連情報の維持が含まれる。インシデント情報は、ネットワーク監視、インシデント報告、インシデント対応チーム、ユーザの苦情、サプライチェーンパートナー、監査監視、物理アクセス監視、ユーザと管理者の報告など、様々なソースから取得できる。IR-4 は、監視に適したインシデントのタイプに関する情報を提供する。

関連管理策：AU-6, AU-7, IR-4, IR-6, IR-8, PE-6, PM-5, SC-5, SC-7, SI-3, SI-4, SI-7

拡張管理策：

(1) インシデント監視 | 自動化された追跡、データ収集、および分析

[*設定：組織が定める自動化されたメカニズム*]を使用して、インシデントを追跡し、インシデント情報を収集および分析する。

詳解：インシデントを追跡し、インシデント情報を収集、分析するための自動化されたメカニズムには、コンピュータインシデント対応センターやインシデントの他の電子データベース、ネットワーク監視デバイスが含まれる。

関連管理策：なし

参照資料：[SP 800-61]

IR-6 インシデント報告

管理策：

a. [*設定：組織が定める期間*]内に、不審なインシデントを組織のインシデント対応ケイパビリティに報告することを職員に要求する。

b. インシデント情報を[*設定：組織が定める機関*]に報告する。

詳解：報告するインシデントのタイプ、報告の内容とタイムライン、指定された報告先機関については、適用される法律、大統領令、指令、規則、ポリシー、基準、ガイドラインを反映する。インシデント情報は、リスクアセスメント、管理策の有効性アセスメント、資産の取得に関するセキュリティ要件、技術製品の選択基準に対し情報を提供することができる。

関連管理策：CM-6, CP-2, IR-4, IR-5, IR-8, IR-9

拡張管理策：

(1) インシデント報告 | 自動化された報告

[*設定：組織が定める自動化されたメカニズム*]を使用してインシデントを報告する。

詳解：インシデント報告の報告先は、IR-6b で指定される。自動化された報告のメカニズムには、電子メール、（自動更新のある）ウェブサイトへの投稿、自動化されたインシデント対応ツールとプログラムが含まれる。

関連管理策：IR-7

(2) インシデント報告 | インシデントに関連する脆弱性

[*設定：組織が定める職員または役割*]に、報告されたインシデントに関連するシステムの脆弱性を報告する。

詳解：システムの脆弱性が明らかになった報告されたインシデントは、システムオーナー、ミッションまたは事業オーナー、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、認可権限のある担当者、およびリスク管理者（部署）などの組織の職員によって分析される。分析は、発見されたシステムの脆弱性に対処するための軽減措置に優先順位を付け、着手するのに役立つ。

関連管理策：なし

(3) インシデント報告 | サプライチェーンとの連携

インシデントに関連するシステムやシステムコンポーネントのサプライチェーンやサプライチェーンガバナンスに関与する製品やサービスのプロバイダおよびその他の組織にインシデント情報を提供する。

詳解：サプライチェーン活動に関与する組織には、製品開発者、システムインテグレータ、製造事業者、包装事業者、組立事業者、販売代理事業者、ベンダ、再販事業者が含まれる。サプライチェーンガバナンスを提供する部署には、連邦調達安全保障会議（FASC：Federal Acquisition Security Council）がある。サプライチェーンのインシデントには、IT 製品、システムコンポーネント、開発プロセスや開発職員、流通過程や倉庫施設が関係する侵害やブリーチが含まれる。組織は、プロセスを改善したり、インシデントの根本原因を特定したりする力量など、サプライチェーンのインシデントについて外部組織に知らせることで得られる価値を共有し考慮するための、適切な情報を決定する。

関連管理策：SR-8

参照資料：[FASC18], [41 CFR 201], [USCERT IR], [SP 800-61]

IR-7 インシデント対応支援

管理策：インシデント処理と報告のためのシステムのユーザに助言とサポートを提供する、組織のインシデント対応ケイパビリティに不可欠な、インシデント対応サポートリソースを提供する。

詳解：組織が提供するインシデント対応サポートリソースには、必要に応じて、ヘルプデスク、サポートグループ、インシデント対応チケットを発行し追跡するための自動化されたチケット管理システム、フォレンジックサービスや消費者救済サービスへのアクセスなどがある。

関連管理策：AT-2, AT-3, IR-4, IR-6, IR-8, PM-22, PM-26, SA-9, SI-18

拡張管理策：

(1) インシデント対応支援｜情報およびサポートの可用性のための自動化されたサポート

[*設定：組織が定める自動化されたメカニズム*]を使用して、インシデント対応情報とサポートの可用性を向上させる。

詳解：自動化されたメカニズムは、ユーザがインシデント対応支援を得るためのプッシュ型またはプル型のケイパビリティを提供できる。例えば、個人が支援ケイパビリティに照会するためにウェブサイトにアクセスしたり、現在の対応ケイパビリティやサポートの理解を深める一環として、支援ケイパビリティがインシデント対応情報をユーザに積極的に送信（一般配布または対象宛に送信）したりする場合がある。

関連管理策：なし

(2) インシデント対応支援｜外部プロバイダとの連携

(a) 自組織のインシデント対応ケイパビリティと、システム保護ケイパビリティを提供する外部プロバイダとの間で、直接的な協力関係を確立する。

(b) 外部プロバイダに対する組織のインシデント対応チームメンバーを特定する。

詳解：システム保護ケイパビリティの外部プロバイダには、米国国防総省内のコンピュータネットワーク防衛プログラムが含まれる。外部プロバイダは、組織の情報システムおよびネットワーク内の認可されていない行為に対する保護、監視、分析、検知、対応を支援する。インシデントが発生する前に、外部プロバイダとの役割と責任を明確にするために、外部プロバイダと適切な協定を結ぶことが有益な場合がある。

関連管理策：なし

参照資料：[OMB A-130], [IR 7559]

IR-8 インシデント対応計画

管理策：

a. 以下のインシデント対応計画を策定する。

1. インシデント対応ケイパビリティを実装するためのロードマップを組織に提供する。
2. インシデント対応ケイパビリティの構造と組織を説明する。
3. インシデント対応ケイパビリティが組織全体にどのように適合するかについての高レベルのアプローチを提供する。
4. ミッション、規模、構造、機能に関連する組織固有の要件を満たす。
5. 報告する必要のあるインシデントを定める。
6. 組織内のインシデント対応ケイパビリティを測定するための指標を提供する。
7. インシデント対応ケイパビリティを効果的に維持し成熟させるために必要なリソースと管理サポートを定める。
8. インシデント情報の共有に対処する。
9. [*設定：組織が定める頻度*]で[*設定：組織が定める職員または役割*]により、レビューし、承認される。
10. [*設定：組織が定めるエンティティ、職員または役割*]に対するインシデント対応の責任を明示的に指定する。

b. インシデント対応計画のコピーを[*設定：組織が定めるインシデント対応職員（名前および／または役割で識別される）および組織の部署*]に配布する。

c. インシデント対応計画の実装、実行、テスト中に発生したシステムおよび組織の変更や問題に対処するために、インシデント対応計画を更新する。

d. インシデント対応計画の変更を、[*設定：組織が定めるインシデント対応職員（名前および／または役割で識別される）および組織の部署*]に伝達する。

e. インシデント対応計画を認可されていない開示や変更から保護する。

詳解：インシデント対応への調整されたアプローチを組織が策定し、実装することが重要である。組織のミッションと事業機能が、インシデント対応ケイパビリティの構造を決定する。インシデント対応ケイパビリティの一部として、組織は、外部サービスプロバイダやサプライチェーンに関与する他の組織を含む外部組織との情報の連携と共有を考慮する。個人情報が含まれるインシデント（すなわちブリーチ）の場合、監督組織または影響を受ける個人への通知が適切かどうかを判断し、その判断に応じて通知を提供するプロセスを含める。

関連管理策：AC-2, CP-2, CP-4, IR-4, IR-7, IR-9, PE-6, PL-2, SA-15, SI-12, SR-8

拡張管理策：

(1) インシデント対応計画 | ブリーチ

個人情報を含むブリーチについてインシデント対応計画に以下を含める。

(a) 個人または監督組織を含む他の組織への通知が必要かどうかを判断するプロセス。

(b) 影響を受ける個人に対する危害、困惑、不便さ、不公平の程度を判断するためのアセスメントプロセス、およびそのような危害を軽減するためのメカニズム。

(c) 適用されるプライバシー要件の特定。

詳解：組織は、法律、規則、ポリシーにより、ブリーチに関連する、個人や影響を受ける組織や監督機関への通知、危害の基準、軽減やその他の特定の要件などを含む特定の手順に従うよう要求される場合がある。

関連管理策：PT-1, PT-2, PT-3, PT-4, PT-5, PT-7

参照資料：[OMB A-130], [SP 800-61], [OMB M-17-12]

IR-9 情報流出対応

管理策：情報流出には以下の方法で対応する。

a. 情報流出に対応する責任を[*設定：組織が定める職員または役割*]に設定する。

b. システムの汚染に関連する情報を特定する。

c. 情報流出に関連しない通信方法を使用して、[*設定：組織が定める職員または役割*]に情報流出を警告する。

d. 汚染されたシステムまたはシステムコンポーネントを分離する。

e. 汚染されたシステムまたはシステムコンポーネントから当該情報を根絶する。

f. その後、汚染された可能性のある他のシステムまたはシステム構成要素を特定する。

g. [*設定：組織が定める措置*]を追加措置する。

詳解：情報流出とは、情報が、その情報の処理を認可されていないシステムに置かれる場合を指す。情報流出は、特定の機密性レベルまたはインパクトレベルであると考えられる情報がシステムに送信され、その後、より高い機密性レベルまたはインパクトレベルであると判断された場合に発生する。その時点で是正措置が必要となる。対応は、流出した情報の機密性レベルまたはインパクトレベル、システムのセキュリティケイパビリティ、汚染された記憶媒体の特性、および汚染されたシステムへのアクセスを認可された個人のアクセス認可に基づいて行う。情報流出後の流出に関する情報の伝達に使用する方法には、汚染が分離されて根絶される前に汚染をさらに拡大させるリスクを最小限にするために、実際の流出に直接関連した方法を関係させない。

関連管理策：CP-2, IR-6, PM-26, PM-27, PT-2, PT-3, PT-7, RA-7

拡張管理策：

(1) 情報流出対応 | 責任者

[撤回：IR-9 に組み込まれた]

(2) 情報流出対応 | トレーニング

[*設定：組織が定める頻度*]で情報流出対応トレーニングを提供する。

詳解：組織は、インシデント対応計画で情報流出インシデントに対応するための要件を規定する。定期的にインシデント対応トレーニングを実施することは、組織の職員が個人の責任を理解し、流出インシデントが発生した場合に取るべき具体的な措置を確実に理解することに役立つ。

関連管理策：AT-2, AT-3, CP-3, IR-2

(3) 情報流出対応 | 流出後の運用

汚染されたシステムが是正措置を講じられている間、情報流出のインパクトを受けた組織の職員が割り当てられたタスクを引き続き実施できるように、[*設定：組織が定める手順*]を実装する。

詳解：情報の流出により汚染されたシステムの是正措置には時間がかかる場合がある。職員は、是正措置が講じられている間、汚染されたシステムにアクセスできず、組織の事業遂行能力に影響を与える可能性がある。

関連管理策：なし

(4) 情報流出対応 | 認可されていない職員への露出

割り当てられたアクセス認可の範囲外の情報が露出された職員に対し、[*設定：組織が定める管理策*]を採用する。

詳解：管理策には、流出した情報が露出された職員が、その情報およびその情報の露出に基づいて課せられる規制に関する、法律、大統領令、指令、規則、ポリシー、基準、ガイドラインを確実に認識できるようにすることが含まれる。

関連管理策：なし

参照資料：なし

IR-10 統合情報セキュリティ分析チーム

［撤回：IR-4(11)に移動された］

3.9 メンテナンス

メンテナンスの要約表へのクイックリンク

MA-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。

1. 以下の[*選択(1 つ以上):組織レベル;ミッション／事業プロセスレベル;システムレベル*]のメンテナンスのポリシー。

(a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、および準拠に対処する。

(b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに適合している。

2. メンテナンスのポリシーと関連するメンテナンスの管理策の実装を促進するための手順。

b. メンテナンスのポリシーと手順の策定、文書化、および配布することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行のメンテナンスをレビューし、更新する。

1. ポリシーについて[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

2. 手順について[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

詳解:メンテナンスのポリシーと手順は、システムおよび組織で実装される MA ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に寄与する。したがって、セキュリティおよびプライバシープログラムがメンテナンスのポリシーと手順の策定と連携していることが重要である。セキュリティおよびプライバシープログラムのポリシーと手順を組織レベルで確立することは望ましく、一般的には、ミッションまたはシステム固有のポリシーと手順を不要にすることができる。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映する複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムに対して規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述し、手順の対象である個人または役割向けとすることができる。手順は、システムのセキュリティおよびプライバシー計画の中に、または 1 つ以上の別の文書に文書化することもできる。メンテナンスのポリシーと手順の更新を引き起こす可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれる。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策:PM-9, PS-8, SI-12

拡張管理策:なし

参照資料:[OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100]

MA-2 管理されたメンテナンス

管理策:

a. 製造事業者やベンダの仕様および／または組織の要件に従って、システムコンポーネントのメンテナンス、修理、交換について、スケジュールし、文書化し、記録をレビューする。

b. メンテナンス措置がオンサイトで実施されるかリモートで実施されるか、システムまたはシステムコンポーネントがオンサイトでメンテナンスサービスを受けるか別の場所に移動されてメンテナンスサービスを受けるかを問わず、すべてのメンテナンス措置を承認し、監視する。

c. [*設定:組織が定める職員または役割*]が、オフサイトでのメンテナンス、修理、交換のために、組織の施設からのシステムやシステムコンポーネントの移動を明示的に承認することを要求する。

d. オフサイトでのメンテナンス、修理、交換のために組織の施設から移動する前に、関連する媒体から[*設定:組織が定める情報*]を取り除くために、装置をサニタイズする。

e. メンテナンス、修理、交換措置の後も、管理策が依然として適切に機能していることを検証するために、インパクトを受ける可能性のある、すべての管理策をチェックする。

f. 組織のメンテナンス記録に[*設定:組織が定める情報*]を含める。

詳解:システムメンテナンスの管理は、システムメンテナンス計画の情報セキュリティの側面に対応し、ローカルエンティティや非ローカルエンティティによって行われるシステムコンポーネントのすべてのタイプのメンテナンスに適用される。メンテナンスには、スキャナ、コピー機、プリンタなどの周辺装置が含まれる。効果的なメンテナンス記録を作成するために必要な情報には、メンテナンスの日時、実施されたメンテナンスの説明、メンテナンスを実施した個人またはグループの名前、エスコートした人の名前、除去または交換されたシステムコンポーネントや装置が含まれる。組織は、システムの交換部品に関連するサプライチェーン関連のリスクを考慮する。

関連管理策:CM-2, CM-3, CM-4, CM-5, CM-8, MA-4, MP-6, PE-16, SI-2, SR-3, SR-4, SR-11

拡張管理策:

(1) 管理されたメンテナンス | 記録内容

[撤回:MA-2 に組み込まれた]

(2) 管理されたメンテナンス | 自動化されたメンテナンス措置

(a) [*設定:組織が定める自動化されたメカニズム*]を使用して、システムのメンテナンス、修理、交換の措置を、スケジュールし、実施し、文書化する。

(b) 要求、スケジュール、処理中、および完了したすべてのメンテナンス、修理、交換措置の最新かつ正確で完全な記録を作成する。

詳解:システムメンテナンスの計画と措置を処理、管理するための自動化されたメカニズムの利用は、タイムリーで、正確で、完全で、一貫性のあるメンテナンス記録の生成を確実にするのに役立つ。

関連管理策:MA-3

参照資料:[OMB A-130], [IR 8023]

MA-3 メンテナンスツール

管理策:

a. システムメンテナンスツールの使用を承認し、管理し、監視する。

b. [*設定:組織が定める頻度*]で以前に承認されたシステムメンテナンスツールをレビューする。

詳解:メンテナンスツールの承認、管理、監視、レビューは、システムの認可境界内になく、特に

組織のシステムの診断と修理措置に使用されるメンテナンスツールに関連するセキュリティ関係の問題に対応する。組織は、メンテナンスツールの承認の役割とその承認を文書化する方法を、柔軟に決定できる。メンテナンスツールを定期的にレビューすることで、古いツール、サポートされていないツール、無関係なツール、使用されなくなったツールについて承認の撤回を促す。メンテナンスツールは、ハードウェア、ソフトウェア、ファームウェアのアイテムがあり、プリインストールされている場合、メンテナンス作業員が媒体で持ち込む場合、クラウドベースの場合、ウェブサイトからダウンロードされる場合がある。このようなツールは、悪意のあるコードを意図的または非意図的に、施設内に移送し、システム内に移送する媒介物となり得る。メンテナンスツールには、ハードウェアとソフトウェアの診断テスト装置とパケットスニファを含めることができる。メンテナンスをサポートし、システムの一部であるハードウェアとソフトウェアコンポーネント(「ping」「ls」「ipconfig」などのソフトウェアで実装しているユーティリティ、またはイーサネットスイッチのポート監視を実装しているハードウェアとソフトウェアを含む)は、メンテナンスツールとして扱わない。

関連管理策: MA-2, PE-16

拡張管理策:

(1) メンテナンスツール | ツールの検査

メンテナンス作業員が使用するメンテナンスツールに、不適切または認可されていない変更がないかを検査する。

詳解: メンテナンスツールは、メンテナンス作業員が施設に直接持ち込むか、ベンダのウェブサイトからダウンロードされることができる。メンテナンスツールを検査した結果、ツールが不適切に変更されている、またはツールに悪意のあるコードが含まれていると組織が判断した場合、インシデント対応に関する組織のポリシーおよび手順に従って、インシデントを処理する。

関連管理策: SI-7

(2) メンテナンスツール | 媒体の検査

診断およびテストプログラムを含む媒体がシステムで使用される前に、悪意のあるコードについて媒体をチェックする。

詳解: メンテナンス、診断、およびテストプログラムを含む媒体を検査した結果、組織がその媒体に悪意のあるコードが含まれていると判断した場合、インシデントは、組織のインシデント対応ポリシーおよび手順に従って処理する。

関連管理策: SI-3

(3) メンテナンスツール | 認可されていない移動の防止

以下により、組織の情報を含むメンテナンス装置の移動を防止する。

(a) 装置に組織の情報が含まれていないことを検証する。

(b) 装置をサニタイズまたは破壊する。

(c) 装置を施設内に留める。

(d) 施設からの装置の移動を明示的に認可する[*設定: 組織が定める職員または役割*]から、移動禁止の除外を受ける。

詳解: 組織の情報には、組織が所有するすべての情報、情報スチュワードとしての役割を果たす組織に提供される情報が含まれる。

関連管理策: MP-6

(4) メンテナンスツール | ツールの使用制限

メンテナンスツールの使用を、認可された職員のみに制限する。

詳解: メンテナンスツールの使用を認可された職員のみに制限することを、メンテナンス機能を実行するために使用するシステムに適用する。

関連管理策: AC-3, AC-5, AC-6

(5) メンテナンスツール | 特権での実行

増強された特権で実行するメンテナンスツールの使用を監視する。

詳解：増強されたシステム特権で実行するメンテナンスツールは、システム特権がなければアクセスできない組織の情報や資産への、認可されていないアクセスをもたらす可能性がある。

関連管理策：AC-3, AC-6

(6) メンテナンスツール | ソフトウェアの更新およびパッチ

最新のソフトウェア更新とパッチがインストールされていることを確実にするために、メンテナンスツールを検査する。

詳解：古くなった、および／またはパッチが適用されていないソフトウェアを使用するメンテナンスツールは、敵対者に脅威ベクトルを与え、組織に重大な脆弱性をもたらす可能性がある。

関連管理策：AC-3, AC-6

参照資料：[SP 800-88]

MA-4 非ローカルメンテナンス

管理策：

a. 非ローカルメンテナンス措置とリモート診断措置を承認し、監視する。

b. 組織のポリシーと整合性があり、システムのセキュリティ計画に文書化されている場合に限り、非ローカルメンテナンスツールとリモート診断ツールの使用を許可する。

c. 非ローカルメンテナンスセッションとリモート診断セッションの確立に強力な認証を採用する。

d. 非ローカルメンテナンス措置とリモート診断措置の記録を維持する。

e. 非ローカルメンテナンスが完了した際、セッションとネットワーク接続を切断する。

詳解：非ローカルメンテナンス措置とリモート診断措置は、外部ネットワークまたは内部ネットワークのいずれかを介して通信する個人によって実施される。ローカルでのメンテナンス措置と診断措置は、システムのある場所に物理的に居て、ネットワーク接続を介して通信しない個人によって実施される。非ローカルメンテナンスセッションとリモート診断セッションを確立するために使用される認証技法は、IA-2 のネットワークアクセス要件を反映する。強力な認証には、リプレイ攻撃に耐性があり、多要素認証を採用しているオーセンティケータが求められる。強力なオーセンティケータには、パスワード、パスフレーズ、生体情報によって保護されたトークンに証明書が記憶される PKI が含まれる。MA-4 の要件の実施は、一部、他の管理策によって達成される。[SP 800-63B]は、強力な認証とオーセンティケータに関する追加のガイダンスを提供している。

関連管理策：AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, PL-2, SC-7, SC-10

拡張管理策：

(1) 非ローカルメンテナンス | ロギングおよびレビュー

(a) 非ローカルメンテナンスセッションとリモート診断セッションについて[*設定：組織が定める監査イベント*]をロギングする。

(b) 異常なふるまいを検知するために、メンテナンスセッションと診断セッションの監査記録をレビューする。

詳解：非ローカルメンテナンスのための監査ロギングは、AU-2 によって実施される。監査イベントは AU-2a で規定される。

関連管理策：AU-6, AU-12

(2) 非ローカルメンテナンス | 非ローカルメンテナンスの文書化

［撤回：MA-1 および MA-4 に組み込まれた］

(3) 非ローカルメンテナンス | 同等のセキュリティおよびサニタイズ

(a) サービス対象のシステムに実装されているセキュリティケイパビリティと同等のセキュリティケイパビリティを実装しているシステムから、非ローカルメンテナンスサービスやリモート診断サービスを実行することを要求する。

(b) 非ローカルメンテナンスサービスやリモート診断サービスの前に、サービス対象のコンポーネントをシステムから切り離す。コンポーネントを（組織の情報について）サニタイズする。サービスが実施された後、コンポーネントをシステムに再接続する前に、コンポーネントを検査して（潜在的な悪意のあるソフトウェアを）サニタイズする。

詳解：メンテナンスサービスを提供するシステム、診断ツール、装置の同等のセキュリティケイパビリティとは、それらのシステム、ツール、装置に実装された管理策が、サービス対象のシステムの管理策と少なくとも同程度に包括的であることを意味する。

関連管理策：MP-6, SI-3, SI-7

(4) 非ローカルメンテナンス | メンテナンスセッションの認証および分離

非ローカルメンテナンスセッションを以下のように保護する。

(a) ［*設定：リプレイ耐性のある組織が定めるオーセンティケータ*］を採用する。

(b) 以下のいずれかによって、メンテナンスセッションをシステムの他のネットワークセッションから分離する。

(1) 物理的に分離された通信経路。

(2) 論理的に分離された通信経路。

詳解：通信経路は、暗号を使用して論理的に分離することができる。

関連管理策：なし

(5) 非ローカルメンテナンス | 承認および通知

(a) 各非ローカルメンテナンスセッションについて［*設定：組織が定める職員または役割*］による承認を要求する。

(b) ［*設定：組織が定める職員または役割*］に、計画された非ローカルメンテナンスの日時を通知する。

詳解：通知は、メンテナンス作業員が行うことができる。非ローカルメンテナンスの承認は、提案されたメンテナンスの適切性を判断するための十分な情報セキュリティとシステム知識を有する職員によって果たされる。

関連管理策：なし

(6) 非ローカルメンテナンス | 暗号による保護

非ローカルメンテナンス通信とリモート診断通信の完全性と機密性を保護するために、［*設定：組織が定める暗号のメカニズム*］を実装する。

詳解：非ローカルメンテナンス通信とリモート診断通信を保護しないと、認可されていない個人が組織の情報にアクセスする可能性がある。非ローカルメンテナンスセッション中の認可されていないアクセスは、悪意のあるコードの挿入、システムパラメータの認可されていない変更、組織の情報漏出など、様々な敵対行為をもたらす可能性がある。そのような行為は、ミッションまたは事業ケイパビリティの喪失または低下をもたらす可能性がある。

関連管理策：SC-8, SC-12, SC-13

(7) 非ローカルメンテナンス | 切断の検証

非ローカルメンテナンスセッションとリモート診断セッションの完了後、セッションとネットワーク接続の切断を検証する。

詳解：メンテナンスの完了後に接続の切断を検証することで、非ローカルメンテナンスセッションとリモート診断セッション中に確立された接続が切断され、使用できなくなることが保証される。

関連管理策：AC-12

参照資料：[FIPS 140-3], [FIPS 197], [FIPS 201-2], [SP 800-63-3], [SP 800-88]

MA-5 メンテナンス作業員

管理策：

a. メンテナンス作業員の認可プロセスを確立し、認可されたメンテナンス組織または作業員のリストを維持する。

b. システムのメンテナンスを行うエスコートされていない作業員が、必要なアクセス認可を持っていることを確認する。

c. 必要なアクセス認可を持たないメンテナンス作業員の活動を監督するために、必要なアクセス認可と技術的力量を持つ組織の職員を指名する。

詳解：メンテナンス作業員は、組織のシステムでハードウェアまたはソフトウェアのメンテナンスを行う個人を意味し、PE-2 では、システムの物理的保護境界内でメンテナス作業を行う個人の物理的アクセスに対処している。個人を監督する技術的力量はシステム上で実施されるメンテナンスに関係し、一方、必要なアクセス認可を有することはシステム上およびシステム近くでのメンテナンスに関連する。IT 製造事業者、ベンダ、システムインテグレータ、コンサルタントなど、前もって認可されたメンテナンス作業員として識別されていない個人が、通知をほとんどまたはまったく行わずにメンテナンス措置を行う必要がある場合など、組織のシステムへの特権アクセスが必要になることがある。組織はリスクに関する組織のアセスメントに基づいて、これらの個人に一時的なクレデンシャルを発行してもよい。一時的なクレデンシャルは、1 回限りの使用、または非常に限定された期間の使用とする。

関連管理策：AC-2, AC-3, AC-5, AC-6, IA-2, IA-8, MA-4, MP-2, PE-2, PE-3, PS-7, RA-3

拡張管理策：

(1) メンテナンス作業員 | 適切なアクセス権限のない個人

(a) 適切なセキュリティクリアランスがない、または米国市民ではないメンテナンス作業員の使用に関する、次の要件を含む手順を実装する。

(1) 必要なアクセス認可、クリアランス、正式なアクセス承認のないメンテナンス作業員は、システム上でのメンテナンス措置および診断措置を実施している間、完全にクリアランスされ、適切なアクセス認可を有し、技術的資格のある承認された組織の職員によって、エスコートされ、監督される。

(2) 必要なアクセス認可、クリアランス、正式なアクセス承認のないメンテナンス作業員がメンテナンス行為および診断行為を開始する前に、システム内のすべての揮発性情報記憶コンポーネントはサニタイズされ、すべての不揮発性記憶媒体はシステムから取り出されるか物理的に切り離され、セキュアに保管される。

(b) システムコンポーネントをサニタイズできない場合、システムから取り出せない場合、システムから切り離せない場合に備えて、[*設定：組織が定める代替管理策*]を策定し、実装する。

詳解：適切なセキュリティクリアランスがない、または米国市民でない個人のための手順は、組織のシステムに含まれる国家機密情報または管理対象非機密情報（CUI）への視覚的アクセスおよび電子的アクセスを拒否することが意図されている。メンテナンス作業員の使用に関する手順は、システムのセキュリティ計画の中に文書化することができる。

関連管理策：MP-6, PL-2

(2) メンテナンス作業員 | 国家機密情報を扱うシステムのセキュリティクリアランス

国家機密情報を処理、保存、伝送するシステムでメンテナンス措置と診断措置を行う作業員が、少なくとも最も高い機密性レベルとそのシステムの情報区画について、セキュリティクリアランスおよび正式なアクセス承認を有していることを検証する。

詳解：組織のシステムのメンテナンスを行う作業員は、メンテナンス措置の過程で国家機密情報が露出される可能性がある。そのような露出の固有のリスクを軽減するために、組織は、システムに保管されている情報の機密性レベルまでのアクセスが許可されている（すなわち、セキュリティクリアランスを有している）メンテナンス作業員を使用する。

関連管理策：PS-3

(3) メンテナンス作業員 | 国家機密情報を扱うシステムの米国市民権要件

国家機密情報を処理、保存、伝送するシステムでメンテナンス措置と診断措置を行う作業員が、米国市民であることを検証する。

詳解：組織のシステムのメンテナンスを行う作業員は、メンテナンス措置の過程で国家機密情報が露出される可能性がある。組織のシステム上の国家機密情報へのアクセスが米国市民に制限されている場合、同じ制限がそれらのシステムのメンテナンスを行う作業員に適用される。

関連管理策：PS-3

(4) メンテナンス作業員 | 外国人

以下を確実にする。

(a) システムが米国と外国の同盟政府によって共同所有および運営されている場合、または外国の同盟政府によってのみ所有および運営されている場合に限り、適切なセキュリティクリアランスを有する外国人を、国家機密情報を扱うシステムのメンテナンス措置と診断措置を実施するために使用する。

(b) 国家機密情報を扱うシステムのメンテナンス措置と診断措置を実施するための外国人の使用に関する承認、同意、詳細な運用条件は、覚書に完全に文書化する。

詳解：組織のシステムのメンテナンスを行う作業員は、メンテナンス措置の過程で国家機密情報が露出される可能性がある。非米国市民が国家機密情報を扱うシステムのメンテナンス措置と診断措置実施することを許可されている場合、合意事項と制限事項に違反していないことを保証するために追加の審査が要求される。

関連管理策：PS-3

(5) メンテナンス作業員 | システム以外のメンテナンス

システムに直接関連するメンテナンスではなく、システムに物理的に近接した場所でメンテナンス措置を行うエスコートされていない作業員が、必要なアクセス認可を有していることを確実にする。

詳解：システムに直接関係のない他の立場でメンテナンス措置を行う作業員には、物理設備担当職員と警備担当職員が含まれる。

関連管理策：なし

参照資料：なし

MA-6 タイムリーなメンテナンス

管理策：障害が発生した場合、[*設定：組織が定める期間*] 内に、[*設定：組織が定めるシステムコンポーネント*] のメンテナンスサポートおよび／またはスペアパーツを取得する。

詳解：組織は、システムコンポーネントによって提供される機能が動作しない場合、組織の運営および資産、個人、他の組織、国家へのリスクを増大させるシステムコンポーネントを特定する。メンテナンスサポートを受けるための組織の措置には、適切な契約を締結することが含まれる。

関連管理策：CM-8, CP-2, CP-7, RA-7, SA-15, SI-13, SR-2, SR-3, SR-4

拡張管理策:

(1) タイムリーなメンテナンス | 予防メンテナンス

[*設定:組織が定めるシステムコンポーネント*]の予防メンテナンスを[*設定:組織が定める時間間隔*]で実施する。

詳解:予防メンテナンスには、組織の装置と施設を満足のいく稼働状態に維持するための予防的ケアとシステムコンポーネントのメンテナンスが含まれる。このようなメンテナンスには、初期障害が発生する前に、または重大な欠陥に発展する前に、初期障害の系統的な検査、テスト、測定、調整、部品交換、検知、修正を実施することが含まれる。予防メンテナンスの主な目的は、装置の障害による結果を回避または軽減することである。予防メンテナンスは、使い古したコンポーネントが障害を起こす前に交換することにより、装置の信頼性を維持し復元するように設計される。適用する予防的(またはその他の)障害管理ポリシーを決定する方法には、相手先商標製造会社(OEM)の推奨事項、統計的障害記録、専門家の意見、同様の装置で既に実施されているメンテナンス、管轄区域内の規範、法律、規則の要件、測定値と性能指標が含まれる。

関連管理策:なし

(2) タイムリーなメンテナンス | 予測メンテナンス

[*設定:組織が定めるシステムコンポーネント*]に対して、[*設定:組織が定める時間間隔*]で、予測メンテナンスを実施する。

詳解:予測メンテナンスは、定期的または継続的な(オンライン)装置状態監視を実施することにより、装置の状態を評価する。予測メンテナンスの目標は、メンテナンス措置が、最も費用対効果が高く、装置の性能が閾値以下に低下する前に、スケジュールされた時期にメンテナンスを実施することである。予測メンテナンスの予測構成要素は、装置の状態の将来の傾向を予測するという目的に起因している。予測メンテナンスアプローチでは、将来どの時点でメンテナンス措置を行うのが適切かを判断するために、統計的プロセス管理の原則を採用する。ほとんどの予測メンテナンス点検は、装置の稼働中に行われるため、通常のシステム運用の中断が最小限に抑えられる。予測メンテナンスにより、大幅なコスト削減とシステム信頼性の向上を実現できる。

関連管理策:なし

(3) タイムリーなメンテナンス | 予測メンテナンスのための自動化されたサポート

[*設定:組織が定める自動化されたメカニズム*]を使用して、予測メンテナンスデータをメンテナンス管理システムに転送する。

詳解:コンピュータ化されたメンテナンス管理システムは、組織のメンテナンス運用に関する情報のデータベースを維持し、装置の状態データの処理を自動化し、メンテナンスの計画、実行、報告をトリガーする。

関連管理策:なし

参照資料:なし

MA-7 フィールドメンテナンス

管理策:[*設定:組織が定めるシステムまたはシステムコンポーネント*]のフィールドメンテナンスを[*設定:組織が定める信頼されたメンテナンス施設*]に制限するか禁止する。

詳解:フィールドメンテナンスは、システムまたはシステムコンポーネントが特定のサイト(すなわち、運用環境)に配備された後に、システムまたはシステムコンポーネントに対して行われるメンテナンスのタイプである。場合によっては、フィールドメンテナンス(すなわち、サイトでのローカルメンテナンス)は、軍事補給所メンテナンスと同じ程度の厳密さや同じ品質管理チェックでは、実行されなくてもよい。組織によって指定された重要システムの場合、ローカルサイトでのフィールドメンテナンスを制限または禁止する必要があり、そのようなメンテナンスは、追加の管理策を備えた信頼できる施設で実施する必要がある。

関連管理策:MA-2, MA-4, MA-5

拡張管理策:なし

参照資料:なし

3.10 媒体保護

媒体保護の要約表へのクイックリンク

MP-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。

1. 以下の[*選択(1 つ以上):組織レベル;ミッション／事業プロセスレベル;システムレベル*]の媒体保護のポリシー。

(a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、および準拠に対処する。

(b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに適合している。

2. 媒体保護のポリシーと関連する媒体保護の管理策の実装を促進するための手順。

b. 媒体保護のポリシーと手順の策定、文書化、および配布することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行の媒体保護をレビューし、更新する。

1. ポリシーについて[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

2. 手順について[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

詳解:媒体保護のポリシーと手順は、システムおよび組織で実装される MP ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に寄与する。したがって、セキュリティおよびプライバシープログラムが媒体保護のポリシーと手順の策定と連携していることが重要である。セキュリティおよびプライバシープログラムのポリシーと手順を組織レベルで確立することは望ましく、一般的には、ミッションまたはシステム固有のポリシーと手順を不要にすることができる。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映する複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムに対して規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述し、手順の対象である個人または役割向けとすることができる。手順は、システムのセキュリティおよびプライバシー計画の中に、または 1 つ以上の別の文書に文書化することもできる。媒体保護のポリシーと手順の更新を引き起こす可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれる。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策: PM-9, PS-8, SI-12

拡張管理策:なし

参照資料: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100]

MP-2 媒体へのアクセス

管理策：[*設定：組織が定めるデジタルおよび／または非デジタル媒体のタイプ*]へのアクセスを[*設定：組織が定める職員または役割*]に制限する。

詳解：システム媒体には、デジタル媒体と非デジタル媒体がある。デジタル媒体には、フラッシュドライブ、ディスケット、磁気テープ、外付けまたは取り外し可能なハードディスクドライブ（ソリッドステートディスクドライブ、磁気ディスクドライブなど）、CD、DVD がある。非デジタル媒体には、紙とマイクロフィルムがある。地域病院で患者の医療記録へのアクセスを求める個人が認可された医療提供者でない限り、アクセスを拒否することは、非デジタル媒体へのアクセス制限の例である。メディアライブラリの CD に保管されている設計仕様へのアクセスを、システム開発チームの個人に限定することは、デジタル媒体へのアクセス制限の例である。

関連管理策：AC-19, AU-9, CP-2, CP-9, CP-10, MA-5, MP-4, MP-6, PE-2, PE-3, SC-12, SC-13, SC-34, SI-12

拡張管理策：

(1) 媒体へのアクセス｜自動化されたアクセス制限

［撤回：MP-4(2)に組み込まれた］

(2) 媒体へのアクセス｜暗号による保護

［撤回：SC-28(1)に組み込まれた］

参照資料：[OMB A-130], [FIPS 199], [SP 800-111]

MP-3 媒体へのマーキング

管理策：

a. 情報の配布限定、取り扱いに関する警告、該当するセキュリティマーキング（在る場合）を示すために、システム媒体にマークを付ける。

b. 媒体が[*設定：組織が定める管理エリア*]内にある場合は、[*設定：組織が定めるシステム媒体のタイプ*]について、マーキングから除外する。

詳解：セキュリティマーキングとは、可読形式のセキュリティ属性の適用または使用を指す。デジタル媒体には、フラッシュドライブ、ディスケット、磁気テープ、外付けまたは取り外し可能なハードディスクドライブ（ソリッドステートディスクドライブ、磁気ディスクドライブなど）、CD、DVD がある。非デジタル媒体には、紙とマイクロフィルムがある。管理対象非機密情報（CUI）は、国立公文書記録管理局により、管理対象非機密情報の適切な保全および配布の要件とともに定義されており、[32 CFR 2002]で体系化されている。一般に、組織がパブリックドメインである、または公開リリース可能であると判断した情報からなる媒体には、セキュリティマーキングは必要ない。組織によっては、公開リリース情報であることを示すために、公開情報にマーキングを要求する場合がある。システム媒体のマーキングは、適用される法律、大統領令、指令、ポリシー、規則、基準、ガイドラインを反映する。

関連管理策：AC-16, CP-9, MP-5, PE-22, SI-12

拡張管理策：なし

参照資料：[EO 13556], [32 CFR 2002], [FIPS 199]

MP-4 媒体保管

管理策：

a. [*設定：組織が定める管理エリア*]内で、[*設定：組織が定めるタイプのデジタル媒体および／または非デジタル媒体*]を物理的に管理し、セキュアに保管する。

b. MP-4a で定義したタイプのシステム媒体を、承認された装置、技法、手順を使用して破壊またはサニタイズされるまで保護する。

詳解：システム媒体には、デジタル媒体と非デジタル媒体がある。デジタル媒体には、フラッシュドライブ、ディスケット、磁気テープ、外付けまたは取り外し可能なハードディスクドライブ（ソリッドステートディスクドライブ、磁気ディスクドライブなど）、CD、DVD がある。非デジタル媒体には、紙とマイクロフィルムがある。保管された媒体を物理的に管理することには、媒体のインベントリを管理すること、個人が媒体を貸し出しライブラリに返却を可能にする手順を導入すること、保管された媒体に対する説明責任を維持することが含まれる。セキュアな保管場所には、施錠された引出、施錠された机、施錠されたキャビネット、管理されたメディアライブラリが含まれる。媒体保管のタイプは、媒体上の情報のセキュリティ分類または機密性区分に対応している。管理エリアとは、情報とシステムを保護するために規定された要件を満たすために、物理的および手続き的管理策を適用する場所である。パブリックドメインであるか、公開リリース可能であるか、または認可された担当者以外がアクセスした場合に組織、業務、個人への有害なインパクトが限定的であると判断された情報を含む媒体については、必要となる管理策は少ない。これらの状況では、物理的なアクセス制御が適切な保護を提供する。

関連管理策：AC-19, CP-2, CP-6, CP-9, CP-10, MP-2, MP-7, PE-3, PL-2, SC-12, SC-13, SC-28, SC-34, SI-12

拡張管理策：

(1) 媒体保管 | 暗号による保護

[撤回：SC-28(1)に組み込まれた]

(2) 媒体保管 | 自動化されたアクセス制限

媒体保管エリアへのアクセスを制限し、[*設定：組織が定める自動化されたメカニズム*]を使用して、アクセスの試みとアクセスの許可をロギングする。

詳解：自動化されたメカニズムには、媒体保管エリアに外部から入室する際の、キーパッド、生体認証リーダー、カードリーダーが含まれる。

関連管理策：AC-3, AU-2, AU-6, AU-9, AU-12, PE-3

参照資料：[FIPS 199], [SP 800-56A], [SP 800-56B], [SP 800-56C], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-111]

MP-5 媒体移送

管理策：

a. [*設定：組織が定める管理策*]を使用して、管理エリア外への移送中に、[*設定：組織が定めるタイプのシステム媒体*]を保護し、管理する。

b. 管理エリア外への移送中、システム媒体の説明責任を維持する。

c. システム媒体の移送に関連する活動を文書化する。

d. システム媒体の移送に関連する活動を認可された職員に制限する。

詳解：システム媒体には、デジタル媒体と非デジタル媒体がある。デジタル媒体には、フラッシュドライブ、ディスケット、磁気テープ、外付けまたは取り外し可能なハードディスクドライブ（ソリッドステートディスクドライブ、磁気ディスクドライブなど）、CD、DVD がある。非デジタル媒体には、紙とマイクロフィルムがある。管理エリアとは、情報やシステムを保護するために規定された要件を満たすために、組織が物理的および手続き的管理策を適用する場所である。移送中に媒体を保護するための管理策には、暗号技術と施錠されたコンテナが含まれる。暗号化のメカニズムは、実装されたメカニズムに応じて、機密性と完全性を保護することができる。媒体移送に関連する活動には、移送のための媒体の持ち出し、媒体が適切な移送プロセスをとること、実際の移送が含まれる。認可された移送および配送担当職員には、組織外の個人が含まれる場合がある。移送中の媒体の説明責任の維持には、移送活動を認可された職員に制限すること、媒体の紛失、破壊、改ざんを防止および検知するために媒体が移送システムを移動する際に移送活動の記録を追跡および／または取得することが含まれる。組織は、組織のリスクアセスメントに従い、システム媒体の移送に関連する活動の文書化要件を規定する。組織は、移送関連の記録のシステムの一部として、様々なタイプの媒体移送の記録保持方法を定

める柔軟性を維持する。

関連管理策: AC-7, AC-19, CP-2, CP-9, MP-3, MP-4, PE-16, PL-2, SC-12, SC-13, SC-28, SC-34

拡張管理策:

(1) 媒体移送 | 管理エリア外での保護

[撤回: MP-5 に組み込まれた]

(2) 媒体移送 | 活動の文書化

[撤回: MP-5 に組み込まれた]

(3) 媒体移送 | 管理人

管理エリア外へのシステム媒体の移送中、身元が明らかな管理人を採用する。

詳解: 身元が明らかな管理人は、媒体移送過程における特定の連絡窓口を組織に提供し、個人の説明責任を容易にする。明確な管理人の身元が明らかな場合、管理人の責任は、ある個人から別の個人に移転することができる。

関連管理策: なし

(4) 媒体移送 | 暗号による保護

[撤回: SC-28(1)に組み込まれた]

参照資料: [FIPS 199], [SP 800-60-1], [SP 800-60-2]

MP-6 媒体のサニタイズ

管理策:

a. [*設定: 組織が定めるシステム媒体*]を廃棄する前、組織の管理外に持ち出す前、再利用のために持ち出す前に、[*設定: 組織が定めるサニタイズ技法および手順*]を使用して、サニタイズする。

b. セキュリティ分類または情報の機密性区分に見合った強度と完全性を備えたサニタイズのメカニズムを採用する。

詳解: 媒体のサニタイズは、媒体が取り外し可能と見なされるかどうかに関係なく、廃棄または再利用の対象となるすべてのデジタルシステム媒体および非デジタルシステム媒体に適用する。デジタル媒体の例として、スキャナ、コピー機、プリンタ、ノートブックコンピュータ、ワークステーション、ネットワークコンポーネント、モバイルデバイスがあり、非デジタル媒体の例として、紙とマイクロフィルムがある。サニタイズのプロセスでは、情報をシステム媒体から取り除き、情報を取得または再構成できないようにする。上書き消去、消去、暗号消去、個人情報の匿名化、破壊などのサニタイズ技法により、そのような媒体が再利用または廃棄のために持ち出された際、認可されていない個人が情報を開示することを防止する。組織は、サニタイズを必要とする媒体に他の方法を適用できない場合は、破壊が必要となる場合があることを認識し、適切なサニタイズ方法を決定する。組織は、パブリックドメインにあるとみなされる情報、公開リリース可能であるとみなされる情報、再利用または廃棄のために持ち出された場合に組織または個人に有害なインパクトを及ぼさないとみなされる情報を含む媒体に対して、承認されたサニタイズ技法および手順の採用に関して裁量権を持つ。非デジタル媒体のサニタイズには、破壊、国家機密文書から国家機密付属書部分を取り除くこと、黒塗りされたセクションまたは単語を文書から取り除くのと同等の方法で隠蔽して文書から選択されたセクションまたは単語を改訂することが含まれる。NSA の基準とポリシーは、国家機密情報を含む媒体のサニタイズプロセスを統制している。NARA のポリシーは、管理対象非機密情報（CUI）のサニタイズプロセスを統制している。

関連管理策: AC-3, AC-7, AU-11, MA-2, MA-3, MA-4, MA-5, PM-22, SI-12, SI-18, SI-19, SR-11

拡張管理策:

(1) 媒体のサニタイズ | レビュー、承認、追跡、文書化、検証

媒体のサニタイズと廃棄の措置をレビュー、承認、追跡、文書化、検証する。

詳解：組織は、記録保持ポリシーの準拠を確実にするために、サニタイズされる媒体をレビューし、承認する。措置の追跡および文書化には、サニタイズおよび廃棄措置をレビューし承認した職員のリスト、サニタイズした媒体のタイプ、媒体に保管されていたファイル、使用されたサニタイズ方法、サニタイズ措置の日時、サニタイズを実施した職員、実施した検証措置と検証した職員、実施した廃棄措置が含まれる。組織は、媒体のサニタイズが有効であったことを廃棄前に検証する。

関連管理策：なし

(2) 媒体のサニタイズ | 装置のテスト

[*設定：組織が定める頻度*]でサニタイズの装置と手順をテストし、意図したサニタイズが達成されていることを確実にする。

詳解：サニタイズの装置と手順のテストは、連邦政府機関または外部サービスプロバイダを含む、資格のある認可された外部エンティティによって実施される場合がある。

関連管理策：なし

(3) 媒体のサニタイズ | 非破壊的技法

[*設定：組織が定めるポータブルストレージデバイスのサニタイズを必要とする状況*]下で、ポータブルストレージデバイスをシステムに接続する前に、非破壊的サニタイズ技法を適用する。

詳解：ポータブルストレージデバイスには、外付けまたは取り外し可能なハードディスクドライブ（例えば、ソリッドステート、磁気）、光ディスク、磁気または光学テープ、フラッシュメモリデバイス、フラッシュメモリカード、および他の外付けまたは取り外し可能なディスクが含まれる。ポータブルストレージデバイスは信頼できないソースから入手でき、USB ポートまたはその他のエントリポータルを介して組織のシステムに差し込みまたは転送できる悪意のあるコードを含んでいる可能性がある。ストレージデバイスをスキャンすることを推奨し、サニタイズは、ストレージデバイスに悪意のあるコードがないことの追加の保証を提供する。組織は、製造元やベンダから購入したポータブルストレージデバイスを最初に使用する場合、または組織がポータブルストレージデバイスの確実なエビデンスの連続性を維持できない場合、ポータブルストレージデバイスの非破壊的サニタイズを考慮する。

関連管理策：なし

(4) 媒体のサニタイズ | 管理対象非機密情報

[撤回：MP-6 に組み込まれた]

(5) 媒体のサニタイズ | 国家機密情報

[撤回：MP-6 に組み込まれた]

(6) 媒体のサニタイズ | 媒体の破壊

[撤回：MP-6 に組み込まれた]

(7) 媒体のサニタイズ | 二重認可

[*設定：組織が定めるシステム媒体*]について、サニタイズの二重認可を実施する。

詳解：組織は、システム媒体のサニタイズについて、技術的に資格のある 2 人の個人が指定したタスクを実行しない限り、サニタイズを行えないようにするために、二重認可を採用する。システムメディアをサニタイズする個人は、提案されたサニタイズが、適用される連邦政府および組織の基準、ポリシー、手順を反映しているかどうかを判断するための十分なスキルと専門知識を有する。二重認可は、サニタイズ措置の実施に関する誤りや不正請求から保護し、サニタイズが意図したとおりに行われることを確実にするのにも役立つ。二重認可は、二人担当制としても知られている。共謀のリスクを軽減するために、組織は他の個人に二重認可の職務をローテーションすることを考慮する。

関連管理策：AC-3, MP-2

(8) 媒体のサニタイズ | 情報のリモート除去またはリモート抹消

[*設定：組織が定めるシステムまたはシステムコンポーネント*]から、[*選択：リモートで；[設定：組織が定める条件]の下で*]、情報を除去または抹消するケイパビリティを提供する。

詳解：システムまたはシステムコンポーネントが認可されていない個人によって取得された場合、情報のリモート除去またはリモート抹消により、組織のシステムおよびシステムコンポーネント上の情報を保護する。リモート除去またはリモート抹消のコマンドでは、認可されていない個人が、システム、システムコンポーネント、デバイスを除去または抹消するリスクを軽減するために、強力な認証が求められる。除去または抹消機能は、データまたは情報を複数回上書きすることによって、または暗号化されたデータを複合するために必要な鍵を破壊することによってなど、様々な方法で実装することができる。

関連管理策：なし

参照資料：[32 CFR 2002], [OMB A-130], [NARA CUI], [FIPS 199], [SP 800-60-1], [SP 800-60-2], [SP 800-88], [SP 800-124], [IR 8023], [NSA MEDIA]

MP-7 媒体の使用

管理策：

a. [*設定：組織が定める管理策*]を用いて、[*設定：組織が定めるシステムまたはシステムコンポーネント*]で[*設定：組織が定めるシステム媒体*]の使用を[*選択：制限する；禁止する*]。

b. ポータブルストレージデバイスに識別可能なオーナーがいない場合、組織のシステムでのポータブルストレージデバイスの使用を禁止する。

詳解：システム媒体には、デジタル媒体と非デジタル媒体がある。デジタル媒体には、ディスケット、磁気テープ、フラッシュドライブ、CD、DVD、取り外し可能なハードディスクドライブがある。非デジタル媒体には、紙とマイクロフィルムがある。媒体使用の保護は、情報ストレージケイパビリティを備えたモバイルデバイスにも適用される。媒体へのユーザアクセスを制限する MP-2 とは対照的に、MP-7 は、例えば、フラッシュドライブや外付けハードディスクドライブの使用制限や禁止など、システムで特定のタイプの媒体の使用を制限する。組織は、システム媒体の使用を制限するために、技術的および非技術的な管理策を用いる。組織は、例えば、ワークステーションに物理ケージを使用して特定の外部ポートへのアクセスを禁止したり、ポータブルストレージデバイスの差し込み、読み取り、書き込み機能を無効化または削除したりすることにより、ポータブルストレージデバイスの使用を制限してもよい。組織はまた、ポータブルストレージデバイスの使用を、組織が提供するデバイス、他の承認された組織が提供するデバイス、個人所有でないデバイスなど、承認されたデバイスのみに限定してもよい。最後に、組織は、書き込み可能なポータブルストレージデバイスの使用を禁止し、そのようなデバイスへの書き込みケイパビリティを無効化または削除することにより、この制限を実装するなど、デバイスのタイプに基づいてポータブルストレージデバイスの使用を制限してもよい。記憶装置に識別可能なオーナーを要求することで、組織がストレージデバイスの既知の脆弱性に対処する責任を割り当てることができるようになり、ストレージデバイスを使用するリスクが軽減される。

関連管理策：AC-19, AC-20, PL-4, PM-12, SC-34, SC-41

拡張管理策：

(1) 媒体の使用 | オーナーなしでの使用禁止

[撤回：MP-7 に組み込まれた]

(2) 媒体の使用 | サニタイズ耐性のある媒体の使用禁止

組織のシステムにサニタイズ耐性のある媒体の使用を禁止する。

詳解：サニタイズ耐性とは、媒体から情報を除去するケイパビリティに関して、媒体が非破壊的なサニタイズ技法に対してどの程度耐性があるかを指す。あるタイプの媒体は、サニタイズコマンドをサポートしていないか、サポートしている場合でも、これらのデバイス間でインタフェースが標準化された方法でサポートされていない。サニタイズ耐性のある媒体には、コンパクトフラッシュ、基板やデバイスに組み込まれたフラッシュ、ソリッドステートド

ライブ、USB リムーバブルメディアなどがある。

関連管理策: MP-6

参照資料: [FIPS 199], [SP 800-111]

MP-8 媒体のダウングレード

管理策:

a. 情報のセキュリティ分類または情報の機密性区分に見合った強度と完全性を備えたダウングレードのメカニズムを採用することを含む[*設定:組織が定めるシステム媒体のダウングレードプロセス*]を規定する。

b. システム媒体のダウングレードプロセスが、取り除く情報のセキュリティ分類および／または情報の機密性区分に見合ったものであり、ダウングレードした情報を潜在的に受け取る者のアクセス認可に見合ったものであることを検証する。

c. [*設定:組織が定めるダウングレードが要求されるシステム媒体*]を特定する。

d. 規定されたプロセスを用いて、特定されたシステム媒体をダウングレードする。

詳解:媒体のダウングレードは、媒体が取り外し可能と見なされるかどうかに関係なく、組織外にリリースされるデジタル媒体と非デジタル媒体に適用される。ダウングレードプロセスは、システム媒体に適用される場合、通常はセキュリティ分類または機密性区分レベルにより、情報を取得したり再構成したりすることができないよう、媒体から情報を取り除く。媒体のダウングレードは、より広範な公開と配布を可能にするための情報の黒塗り編集を含む。ダウングレードは、媒体の空きスペースに情報が無いことを確実にする。

関連管理策:なし

拡張管理策:

(1) 媒体のダウングレード | プロセスの文書化

システム媒体のダウングレード措置を文書化する。

詳解:組織は、採用したダウングレード技法、ダウングレードされた媒体の識別番号、ダウングレード措置を認可および／または実施した個人のアイデンティティなどの情報を提供することにより、媒体のダウングレードプロセスを文書化することができる。

関連管理策:なし

(2) 媒体のダウングレード | 装置のテスト

ダウングレード措置が達成されていることを確実にするために、[*設定:組織が定める頻度*]でダウングレードの装置と手順をテストする。

詳解:なし

関連管理策:なし

(3) 媒体のダウングレード | 管理対象非機密情報

一般公開前に、管理対象非機密情報を含むシステム媒体をダウングレードする。

詳解:管理対象非機密情報のダウングレードには、承認されたサニタイズツール、サニタイズ技法、サニタイズ手順を使用する。

関連管理策:なし

(4) 媒体のダウングレード | 国家機密情報

必要なアクセス認可のない個人に公開する前に、国家機密情報を含むシステム媒体をダウングレードする。

詳解:国家機密情報のダウングレードでは、国家機密でないことが確認された情報を国家機密情報を扱うシステムから非機密媒体に転送するために、承認されたサニタイズツール、サニタイズ技法、サニタイズ手順を利用する。

関連管理策：なし

参照資料：[32 CFR 2002], [NSA MEDIA]

3.11 物理的および環境的保護

物理的および環境的保護の要約表へのクイックリンク

PE-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。

1. 以下の[*選択(1 つ以上):組織レベル;ミッション/事業プロセスレベル;システムレベル*]の物理的および環境的保護のポリシー。

(a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、および準拠に対処する。

(b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに適合している。

2. 物理的および環境的保護のポリシーと関連する物理的および環境的保護の管理策の実装を促進するための手順。

b. 物理的および環境的保護のポリシーと手順の策定、文書化、および*配布*することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行の物理的および環境的保護をレビューし、更新する。

1. ポリシーについて[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

2. 手順について[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

詳解:物理的および環境的保護のポリシーと手順は、システムおよび組織で実装される PE ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に寄与する。したがって、セキュリティおよびプライバシープログラムが物理的および環境的保護のポリシーと手順の策定と連携していることが重要である。セキュリティおよびプライバシープログラムのポリシーと手順を組織レベルで確立することは望ましく、一般的には、ミッションまたはシステム固有のポリシーと手順を不要にすることができる。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映する複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムに対して規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述し、手順の対象である個人または役割向けとすることができる。手順は、システムのセキュリティおよびプライバシー計画の中に、または 1 つ以上の別の文書に文書化することもできる。物理的および環境的保護のポリシーと手順の更新を引き起こす可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれる。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策:AT-3, PM-9, PS-8, SI-12

拡張管理策:なし

参照資料:[SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100]

PE-2 物理的アクセス認可

管理策:

a. システムが在る施設へのアクセスについて認可された個人のリストを作成し、承認し、維持する。

b. 施設へのアクセスのための認可クレデンシャルを発行する。

c. [*設定:組織が定める頻度*]で個人の認可された施設へのアクセスを詳述するアクセスリストをレビューする。

d. アクセスする必要がなくなった個人を施設のアクセスリストから除く。

詳解:物理的アクセス認可は、従業員と来訪者に適用される。永続的な物理的アクセスの認可クレデンシャルを有する個人は、来訪者とは見なさない。認可クレデンシャルには、ID バッジ、ID カード、スマートカードが含まれる。組織は、適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに準拠して、必要な認可クレデンシャルの強度を決定する。一般アクセス可能として指定された施設内の特定のエリアへのアクセスには、物理的なアクセス認可が必要ない場合がある。

関連管理策:AT-3, AU-9, IA-4, MA-5, MP-2, PE-3, PE-4, PE-5, PE-8, PM-12, PS-3, PS-4, PS-5, PS-6

拡張管理策:

(1) 物理的アクセス認可 | 職位または役割によるアクセス

システムが在る施設への物理的アクセスを、職位または役割に基づいて認可する。

詳解:役割ベースの施設へのアクセスには、認可された永続的および定例的／定常的なメンテナンス作業員、当直担当者、緊急医療スタッフによるアクセスが含まれる。

関連管理策:AC-2, AC-3, AC-6

(2) 物理的アクセス認可 | 2 つの身分証明書

システムが在る施設への来訪者のアクセスに対し、[*設定:組織が定める許容可能な身分証明書リスト*]の内、2 つの身分証明書を要求する。

詳解:許容可能な身分証明書には、パスポート、REAL ID 準拠の運転免許証、個人アイデンティティ検証(PIV:Personal Identity Verification)カードが含まれる。自動化されたメカニズムを使用して施設にアクセスするために、組織は PIV カード、キーカード、PIN、生体認証を使用してもよい。

関連管理策:IA-2, IA-4, IA-5

(3) 物理的アクセス認可 | エスコートされていないアクセスの制限

システムが存する施設へのエスコートされていないアクセスについて、[*選択(1 つ以上):システム内に含まれるすべての情報に対するセキュリティクリアランス;システム内に含まれるすべての情報に対する正式なアクセス認可;システム内に含まれるすべての情報へのアクセスの必要性;[設定:組織が定める物理的アクセス認可*]]を有する職員に制限する。

詳解:必要なセキュリティクリアランス、アクセス承認、知る必要性を有さない個人は、適切な物理的アクセス認可を有する個人がエスコートし、情報が露出されたり、侵害されたりしないようにする。

関連管理策:PS-2, PS-6

参照資料:[FIPS 201-2], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4]

PE-3 物理的アクセス制御

管理策:

a. [*設定:組織が定めるシステムが在る施設への入口と出口*]で、物理的アクセス認可を

実施する。

1. 施設へのアクセスを許可する前に、個人のアクセス認可を検証する。
2. [*選択(1つ以上):[設定:組織が定める物理的アクセス制御システムまたはデバイス];警備員*]]により、施設への入退を制御する。

b. [*設定:組織が定める入口または出口*]の物理的アクセス監査ロギングを維持する。

c. [*設定:組織が定める物理的アクセス制御*]を実施することにより、公衆アクセス可能として指定された施設内のエリアへのアクセスを制御する。

d. [*設定:組織が定める、来訪者のエスコートと来訪者の活動の管理を要求する状況*]において、来訪者をエスコートし、来訪者の活動を管理する。

e. 鍵、文字合せ錠、その他の物理的アクセスデバイスをセキュアに管理する。

f. [*設定:組織が定める頻度*]ごとに、[*設定:組織が定める物理的アクセスデバイス*]を棚卸しする。

g. [*設定:組織が定める頻度*]で、および／または鍵を紛失した場合、文字合せ錠が侵害した場合、鍵または文字合せ錠を有する個人が異動または雇用が終了した場合、文字合せ錠と鍵を変更する。

詳解:物理的アクセス制御は、従業員と来訪者に適用される。永続的な物理的アクセス認可を持つ個人は、来訪者とは見なさない。一般アクセス可能なエリアの物理的アクセス制御には、一般アクセス可能なエリアから非一般エリアへの移動を防止するための、物理的アクセス制御ロギング／記録、警備員、物理的アクセスデバイスおよび障壁がある。組織は、専門のセキュリティスタッフ、システムユーザ、管理スタッフなど、必要な警備員のタイプを決定する。物理的アクセスデバイスには、鍵、錠、文字合せ錠、生体認証読取装置、カード読取装置が含まれる。物理的アクセス制御システムは、適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに準拠する。組織は、採用する監査ロギングのタイプに柔軟性を持つ。監査ロギングは、手続き型、自動化型、またはそれらのいくつかの組み合わせにすることができる。物理的なアクセスポイントには、施設のアクセスポイント、補足的なアクセス制御を必要とするシステムへの施設内部のアクセスポイント、またはその両方を含めることができる。システムのコンポーネントは、コンポーネントへのアクセスを制御する組織と共に、公衆アクセス可能として指定されたエリアにある場合がある。

関連管理策:AT-3, AU-2, AU-6, AU-9, AU-13, CP-10, IA-3, IA-8, MA-5, MP-2, MP-4, PE-2, PE-4, PE-5, PE-8, PS-2, PS-3, PS-6, PS-7, RA-3, SC-28, SI-4, SR-3

拡張管理策:

(1) 物理的アクセス制御 | システムアクセス

[*設定:システムの1つ以上のコンポーネントを含む組織が定める物理的スペース*]で、施設への物理的アクセス制御に加えて、システムへの物理的アクセス認可を実施する。

詳解:システムへの物理的アクセスを制御することで、システムコンポーネントが集中している施設内のエリアに、追加の物理的セキュリティを提供する。

関連管理策:なし

(2) 物理的アクセス制御 | 施設およびシステム

情報の漏出またはシステムコンポーネントの取り外しに対し、施設またはシステムの物理的境界で、[*設定:組織が定める頻度*]でセキュリティチェックを実施する。

詳解:組織は、漏出に関連するリスクを適切に軽減するために、セキュリティチェックの範囲、頻度、および／またはランダム性を決定する。

関連管理策:AC-4, SC-7

(3) 物理的アクセス制御 | 継続的な警備

システムが在る施設への[設*定:組織が定める物理的アクセスポイント*]を 1 日 24 時

間、週 7 日間制御するために、警備員を配置する。

詳解：施設への選定した物理的アクセスポイントに警備員を配置することは、組織のより迅速な対応ケイパビリティを提供する。警備員はまた、ビデオ監視の対象外となる施設のエリアで、人間による監視の機会を提供する。

関連管理策：CP-6, CP-7, PE-6

(4) 物理的アクセス制御 | 施錠可能なケース

[*設定：組織が定めるシステムコンポーネント*]を認可されていないアクセスから保護するために、施錠可能な物理的なケースを使用する。

詳解：スマートフォン、タブレット、ノートパソコンなどのポータブルデバイスの使用による最大のリスクは盗難である。組織は、機器の盗難リスクを軽減または排除するために、施錠可能な物理的なケースを採用することができる。このようなケースには、1 台のノートパソコンを保護するユニットから、複数のサーバ、コンピュータ、周辺装置を保護できるキャビネットまで、様々なサイズがある。コンピュータ機器を含む施錠されたケースの盗難を防止するために、施錠可能な物理的なケースをケーブルロックや固定プレートと組み合わせて使用することができる。

関連管理策：なし

(5) 物理的アクセス制御 | タンパー保護

システム内の[*設定：組織が定めるハードウェアコンポーネント*]の物理的改ざんや改変を[*選択（1 つ以上）：検知する；防止する*]ために、[*設定：組織が定める耐タンパー技術*]を採用する。

詳解：組織は、選択したハードウェアコンポーネントにタンパー検知とタンパー防止を実装するか、一部のコンポーネントにタンパー検知を実装し、他のコンポーネントにタンパー防止を実装することができる。検知および防止措置には、タンパー検知シールおよびタンパー防止コーティングを含む、多くのタイプの耐タンパー技術を採用することができる。耐改ざんプログラムは、偽造品やその他のサプライチェーン関連のリスクを通じてハードウェアの改変を検知するのに役立つ。

関連管理策：SA-16, SR-9, SR-11

(6) 物理的アクセス制御 | 施設の侵入テスト

[撤回：CA-8 に組み込まれた]

(7) 物理的アクセス制御 | 物理的障壁

物理的障壁を使用してアクセスを限定する。

詳解：物理的な障壁には、保護柱、コンクリート板、コンクリート防護柵、油圧車両による障壁などがある。

関連管理策：なし

(8) 物理的アクセス制御 | 前室のアクセス制御

[*設定：施設内の組織が定めた場所*]に、前室のアクセス制御を採用する。

詳解：前室のアクセス制御は、通常、2 組の連動ドアの間にスペースを提供する物理的アクセス制御システムの一部である。前室は、アクセスが制御された施設に、認可されていない個人が、認可された個人に連なって入ることを防止するように設計されている。この行為は、ピギーバックまたはテールゲートとしても知られ、施設への認可されていないアクセスを引き起こす。連動ドア制御装置を使用して、制御されたアクセスポイントに入る個人の数を限定したり、物理的アクセスの認可を検証する封じ込めエリアを提供したりすることができる。連動ドア制御装置は、完全に自動化する（すなわち、ドアの開閉を制御する）ことも、部分的に自動化する（すなわち、警備員を使って封じ込めエリアに入る個人の数を制御する）こともできる。

関連管理策：なし

参照資料：[FIPS 201-2], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4], [SP 800-116]

PE-4 伝送設備のアクセス制御

[*設定:組織が定めるセキュリティ管理策*]を使用して、組織施設内の[*設定:組織が定めるシステムの配電線および伝送回線*]への物理的アクセスを制御する。

詳解:システムの配電線および伝送回線に適用されるセキュリティ管理策は、偶発的な損傷、中断、物理的改ざんを防止する。このような管理策は、暗号化されていない伝送の盗聴や変更を防止するためにも必要な場合がある。システムの配電線および伝送回線への物理的アクセスを制御するために使用されるセキュリティ管理策には、切断または施錠された予備ジャック、施錠された配線盤、電線管またはケーブルトレイによるケーブル配線の保護、盗聴センサが含まれる。

関連管理策:AT-3, IA-4, MP-2, MP-4, PE-2, PE-3, PE-5, PE-9, SC-7, SC-8

拡張管理策:なし

参照資料:なし

PE-5 出力デバイスのアクセス制御

管理策:認可されていない個人が出力情報を取得することを防止するために、[*設定:組織が定める出力デバイス*]からの出力情報への物理的アクセスを制御する。

詳解:出力デバイスへの物理的アクセスの制御には、キーパッドまたはカードリーダーのアクセス制御を使用して施錠した部屋またはその他のセキュアなエリアに出力デバイスを設置して認可された個人にのみアクセスを許可すること、職員が監視できる場所に出力デバイスを設置すること、モニタフィルタまたは画面フィルタを取り付けること、ヘッドフォンを使用することが含まれる。出力デバイスの例として、モニタ、プリンタ、スキャナ、オーディオデバイス、ファクシミリ装置、コピー機がある。

関連管理策:PE-2, PE-3, PE-4, PE-18

拡張管理策:

(1) 出力デバイスのアクセス制御 | 認可された個人による出力情報へのアクセス

[撤回:PE-5 に組み込まれた]

(2) 出力デバイスのアクセス制御 | 個人のアイデンティティへのリンク

個人のアイデンティティを出力デバイスからの出力情報の受け取りに結び付ける。

詳解:個人のアイデンティティを出力デバイスからの出力情報の受け取りに結び付ける方法には、ファクシミリ機、コピー機、プリンタにセキュリティ機能をインストールすることが含まれる。このような機能により、組織は、出力情報を個人にリリースする前の出力デバイス認証を実装できる。

関連管理策:なし

(3) 出力デバイスのアクセス制御 | 出力デバイスのマーキング

[撤回:PE-22 に組み込まれた]

参照資料:[IR 8023]

PE-6 物理的アクセスの監視

管理策:

a. システムが在る施設への物理的アクセスを監視し、物理的セキュリティインシデントを検知し対応する。

b. [*設定:組織が定める頻度*]および[*設定:組織が定めるイベントまたはイベントの潜在的兆候*]の発生時、物理的アクセスログをレビューする。

c. レビューおよび調査の結果を組織のインシデント対応ケイパビリティと調整する。

詳解：物理的アクセス監視には、組織の施設内の公衆アクセス可能なエリアが含まれる。物理的アクセス監視の例には、警備員、ビデオ監視装置（すなわち、カメラ）、およびセンサデバイスの採用が含まれる。物理的なアクセスロギングをレビューすることで、不審な行為、異常なイベント、潜在的な脅威を特定することができる。アクセスロギングが自動化されたシステムの一部である場合、レビューは AU-2 などの監査ロギングの管理策によってサポートされ得る。組織のインシデント対応ケイパビリティには、物理的なセキュリティインシデントの調査とインシデントへの対応が含まれる。インシデントには、セキュリティ侵害や不審な物理的アクセス行為が含まれる。不審な物理的アクセス行為には、通常の勤務時間外のアクセス、通常はアクセスされないエリアへの繰り返しアクセス、異常に長い時間のアクセス、順番が違うアクセスなどがある。

関連管理策：AU-2, AU-6, AU-9, AU-12, CA-7, CP-10, IR-4, IR-8

拡張管理策：

(1) 物理的アクセスの監視 | 侵入警報装置および侵入監視装置

物理的侵入警報装置および物理的侵入監視装置を使用して、システムが在る施設への物理的アクセスを監視する。

詳解：物理的侵入警報装置を使用して、施設への認可されていないアクセスが試みられた際、セキュリティ職員に警告することができる。警報システムは、物理的障壁、物理的アクセス制御システム、セキュリティ警備員と連携して、これらの他の形態のセキュリティが侵害またはブリーチされた際に、対応をとる。物理的侵入警報装置には、モーションセンサ、接触センサ、ガラス破壊センサなど、様々なタイプのセンサデバイスが含まれる。物理的侵入監視装置には、施設全体の戦略的な場所に設置されたビデオカメラが含まれる。

関連管理策：なし

(2) 物理的アクセスの監視 | 自動化された侵入検知および侵入対応

[*設定：組織が定める侵入の部類またはタイプ*]を検知し、[*設定：組織が定める自動化されたメカニズム*]を使用して[*設定：組織が定める対応措置*]を開始する。

詳解：対応措置には、選定された組織の職員または法執行機関職員への通知を含めることができる。対応措置を開始するために実装された自動化されたメカニズムには、システム警報通知、電子メールおよびテキストメッセージ、ドア施錠のメカニズムの起動が含まれる。物理的アクセス監視は、統合された脅威保障範囲を組織に提供するために侵入検知システムおよびシステム監視ケイパビリティと連携することができる。

関連管理策：SI-4

(3) 物理的アクセスの監視 | ビデオ監視

(a) [*設定：組織が定める運用エリア*]へのビデオ監視を採用する。

(b) [*設定：組織が定める頻度*]でビデオ録画記録をレビューする。

(c) [*設定：組織が定める期間*]の間、ビデオ録画記録を保持する。

詳解：ビデオ監視は、状況により必要な場合、後のレビューを目的として、特定されたエリアでの録画措置に重点を置いている。ビデオ録画は通常、異常なイベントやインシデントを検知するためにレビューする。組織が監視ビデオを実施することを選択しても、監視ビデオを絶えず監視する必要はない。特にそのような監視が公共の場所にある場合は、ビデオ監視を実施および保持する際に法的考慮事項がある場合がある。

関連管理策：なし

(4) 物理的アクセスの監視 | システムへの物理的アクセスの監視

[*設定：組織が定めるシステムの1つ以上のコンポーネントを含む物理的スペース*]で、施設への物理的アクセスの監視に加えて、システムへの物理的アクセスを監視する。

詳解：システムへの物理的アクセスを監視することで、サーバールーム、媒体保管エリア、通信センターなど、システムコンポーネントが集中している施設内のエリアに対し、追加の監視を行える。物理的アクセスの監視は、統合された脅威保障範囲を組織に提供するた

めに侵入検知システムおよびシステム監視ケイパビリティと連携することができる。

関連管理策：なし

参照資料：なし

PE-7 来訪者制御

［撤回：PE-2 および PE-3 に組み込まれた］

PE-8 来訪者アクセス記録

管理策：

a. ［*設定：組織が定める期間*］システムが在る施設への来訪者アクセス記録を維持する。

b. ［*設定：組織が定める頻度*］で来訪者アクセス記録をレビューする。

c. 来訪者アクセス記録の中の異常を［*設定：組織が定める職員*］に報告する。

詳解：来訪者アクセス記録には、来訪した個人の名前と組織、来訪者の署名、身分証明書の形式、アクセスの日付、入退室時刻、来訪の目的、来訪先の個人の名前と組織が含まれる。アクセス記録のレビューは、アクセス認可が最新であり、組織のミッションおよび事業機能をサポートするために依然として必要かどうかを判断する。公衆アクセス可能なエリアでは、アクセス記録は必要ない。

関連管理策：PE-2, PE-3, PE-6

拡張管理策：

(1) 訪問者アクセス記録 | 自動化された記録の維持およびレビュー

［*設定：組織が定める自動化されたメカニズム*］を使用して、来訪者のアクセス記録を維持し、レビューする。

詳解：来訪者のアクセス記録は、組織の担当者がアクセスできるデータベース管理システムに保管および維持される場合がある。このような記録への自動化されたアクセスにより、定期的な記録のレビューが容易になり、アクセス認可が最新であり、組織のミッションおよび事業機能をサポートするために依然として必要かどうかを判断できる。

関連管理策：なし

(2) 訪問者アクセス記録 | 物理的アクセス記録

［撤回：PE-2 に組み込まれた］

(3) 訪問者アクセス記録 | 個人情報要素の限定

来訪者のアクセス記録に含む個人情報を、プライバシーリスクアセスメントで特定した［*設定：組織が定める要素*］に限定する。

詳解：組織には、来訪者のアクセス記録の内容を指定する要件がある場合がある。運用上の目的で必要としない場合、来訪者のアクセス記録に含まれる個人情報を限定することは、システムによって生じるプライバシーリスクのレベル低減に役立つ。

関連管理策：RA-3, SA-8

参照資料：なし

PE-9 電源装置およびケーブル

管理策：システムの電源装置およびケーブルを損傷や破壊から保護する。

詳解：組織は、組織の施設および運用環境の内部および外部の異なる場所で使用される電源装置およびケーブルに必要な保護のタイプを決定する。電源装置およびケーブルのタイプには、オフィスやデータセンターの内部ケーブルと無停電電源、建物の外の発電機と電源ケーブル、サテライトや車両やその他の展開可能なシステムなどの内蔵型コンポーネントの電源など

がある。

関連管理策：PE-4

拡張管理策：

(1) 電源装置およびケーブル｜冗長ケーブル

[*設定：組織が定める距離間隔*]で物理的に分離された冗長電源ケーブル経路を採用する。

詳解：物理的に分離された冗長電源ケーブルにより、ケーブルの 1 本が切断されたり損傷したりした場合でも、電力が流れ続けることを確実にする。

関連管理策：なし

(2) 電源装置およびケーブル｜自動電圧制御

[*設定：組織が定める重要なシステムコンポーネント*]に自動電圧制御を採用する。

詳解：自動電圧制御は、電圧を監視および制御することができる。そのような制御には、電圧レギュレータ、電圧調整器、および電圧安定器が含まれる。

関連管理策：なし

参照資料：なし

PE-10 緊急遮断

管理策：

a. 緊急事態において、[*課題：組織が定めるシステムまたは個々のシステムコンポーネント*]の電源を遮断するケイパビリティを提供する。

b. 認可された担当者が簡単にアクセスできるように、[*設定：組織が定めるシステムまたはシステムコンポーネントの場所*]に緊急遮断スイッチまたはデバイスを設置する。

c. 認可されていない緊急電源遮断ケイパビリティの起動が行われないよう、緊急電源遮断ケイパビリティを保護する。

詳解：緊急電源遮断は、主に、データセンター、メインフレームコンピュータルーム、サーバールーム、およびコンピュータ制御の機械が設置されているエリアなど、システムリソースが集中している組織の施設に適用する。

関連管理策：PE-15

拡張管理策：

(1) 緊急遮断｜偶発的および認可されていない起動

[撤回：PE-10 に組み込まれた]

参照資料：なし

PE-11 非常用電源

管理策：一次電源が喪失した場合、[*選択（1 つ以上）：システムの正常なシャットダウン；システムの長期代替電源への移行*]を容易にするために、無停電電源装置を提供する。

詳解：無停電電源装置（UPS：Uninterruptible Power Supply）は、主電源に障害が発生した場合に緊急電源を供給する電気的なシステムまたはメカニズムである。UPS は通常、予期しない停電により、傷害、死亡、重大なミッションまたは事業の中断、またはデータや情報の消失が発生する可能性がある場合に、コンピュータ、データセンター、通信装置、またはその他の電子装置を保護するために使用さる。UPS は、バッテリー、スーパーコンデンサー、またはフライホイールに蓄えられたエネルギーを供給することにより、主電源の予期しない停電からほぼ瞬時の保護を提供するという点で、非常用電源システムまたはバックアップ発電機とは異なる。UPS のバッ

テリー持続時間は比較的短いが、バックアップ発電機などの予備電源を起動したり、システムを適切にシャットダウンするのに十分な時間を提供する。

関連管理策：AT-3, CP-2, CP-7

拡張管理策：

(1) 非常用電源 | 代替電源 — 最小運用ケイパビリティ

一次電源の長期にわたる消失の場合に、代替電源装置を[*選択：手動で；自動で*]起動し、最小限必要な運用ケイパビリティを維持することができるように、運用中のシステムに代替電源を提供する。

詳解：二次商用電源またはその他の外部電源にアクセスすることで、最小運用ケイパビリティの代替電源を供給することができる。

関連管理策：なし

(2) 非常用電源 | 代替電源 — 自給型

以下のような代替電源装置を[*選択：手動で；自動で*]起動し、システムに代替電源を提供する。

(a) 自給型である。

(b) 外部発電に依存しない。

(c) 一次電源が長時間失われた場合、[*選択：最小限必要な運用ケイパビリティ；完全な運用ケイパビリティ*]を維持できる。

詳解：組織のニーズを満たすのに十分な容量の 1 つ以上の発電機を使用することにより、長期の自給型電源の供給を満たすことができる。

関連管理策：なし

参照資料：なし

PE-12 非常用照明

管理策：停電や電源中断時に起動し、施設内の非常口や避難経路をカバーする、システムの自動非常用照明を採用して維持する。

詳解：非常用照明の提供は、主に、データセンター、サーバールーム、メインフレームのコンピュータルームなど、システムリソースが集中している組織の施設に主に適用される。システムの非常用照明設備は、組織の緊急時対応計画に記載する。システムの非常用照明が故障しているか提供できない場合、組織は電力関連の緊急時対応に備えて代替処理サイトを考慮する。

関連管理策：CP-2, CP-7

拡張管理策：

(1) 非常用照明 | 必須のミッションおよび事業機能

必須のミッションおよび事業機能をサポートする施設内のすべてのエリアに非常用照明を提供する。

詳解：組織は、必須のミッションおよび事業機能を定める。

関連管理策：なし

参照資料：なし

PE-13 防火

管理策：独立したエネルギー源によってサポートされている火災検知および消火システムを採用し、維持する。

詳解：火災検知および消火システムの提供は、主に、データセンター、サーバールーム、メインフレームのコンピュータルームなど、システムリソースが集中している組織の施設に適用される。独立したエネルギー源を必要とする場合がある火災検知および消火システムには、スプリンクラーシステムおよび煙探知器が含まれる。独立したエネルギー源は、施設の他の部分に電力を供給するエネルギー源から分離されているか分離することができる、マイクログリッドなどのエネルギー源である。

関連管理策：AT-3

拡張管理策：

(1) 防火 | 検知システム — 自動起動および通知

火災が発生した場合、自動的に起動し、[*設定：組織が定める職員または役割*]および[*設定：組織が定める緊急対応者*]に通知する火災検知システムを採用する。

詳解：組織は、通知リストに記載された個人がアクセス認可またはクリアランスを必要とする場合（例えば、施設内の情報の機密性区分またはインパクトレベルのためにアクセスが制限されている施設に入場する場合）、職員、役割、緊急対応者を特定することができる。通知のメカニズムは、通知ケイパビリティが火災によって悪影響を受けないようにするために、独立したエネルギー源を必要とする場合がある。

関連管理策：なし

(2) 防火 | 消火システム — 自動起動および通知

(a) 自動的に起動し、[*設定：組織が定める職員または役割*]および[*設定：組織が定める緊急対応者*]に通知する消火システムを採用する。

(b) 施設に継続的に人員が配置されていない場合、自動消火ケイパビリティを採用する。

詳解：組織は、通知リストに記載された個人がアクセス認可および／またはクリアランスを必要とする場合（例えば、施設内の情報の機密性区分またはインパクトレベルのためにアクセスが制限されている施設に入場する場合）、職員、役割、緊急対応者を特定することができる。通知のメカニズムは、通知ケイパビリティが火災によって悪影響を受けないようにするために、独立したエネルギー源を必要とする場合がある。

関連管理策：なし

(3) 防火 | 自動消火

[撤回：PE-13(2)に組み込まれた]

(4) 防火 | 点検

[*設定：組織が定める頻度*]で施設が、認可され資格のある点検者による防火点検を受け、特定された欠陥が[*設定：組織が定める期間*]内に解決されていることを確実にする。

詳解：組織の管轄区域内の認可された資格のある担当者には、州、郡、市の消防検査官および消防部長が含まれる。組織は、施設内にあるシステムに機微情報が含まれている状況下では、点検中、エスコートする。

関連管理策：なし

参照資料：なし

PE-14 環境制御

管理策：

a. システムが在る施設内の[*選択（1つ以上）：温度；湿度；気圧；放射線；* [*設定：組織が定める環境制御*]]レベルを、[*設定：組織が定める許容レベル*]に、維持する。

b. [*設定：組織が定める頻度*]で環境制御レベルを監視する。

詳解：環境制御は、主にシステムリソースが集中している組織の施設（例えば、データセンター、メインフレームコンピュータルーム、サーバールーム）に適用する。特に非常に苛酷な環境において、不十分な環境制御は、組織のミッションおよび事業機能をサポートするために必要なシステムおよびシステムコンポーネントの可用性に重大な有害なインパクトを及ぼす可能性がある。

関連管理策：AT-3, CP-2

拡張管理策：

(1) 環境制御 | 自動制御

システムに有害な可能性のある変動を防止するために、施設に[*設定：組織が定める自動環境制御*]を採用する。

詳解：自動環境制御の実装により、組織のシステムまたはシステムコンポーネントを損傷、劣化、または破壊する可能性のある環境条件に対し即座に対応する。

関連管理策：なし

(2) 環境制御 | 警報および通知による監視

職員または装置に有害な可能性のある変更を[*設定：組織が定める職員または役割*]に警報または通知する環境制御監視を採用する。

詳解：警報または通知は、組織が定める職員または役割に対するリアルタイムの音声警報または視覚的メッセージがあり得る。このような警報や通知は、タイムリーなインシデント対応を促すことで、個人への危害や組織の資産への損害を最小限に抑えるのに役立つ。

関連管理策：なし

参照資料：なし

PE-15 漏水損傷保護

管理策：アクセス可能で、適切に機能し、主要職員に知られている主遮断弁または遮断弁を提供することにより、水漏れによる損傷からシステムを保護する。

詳解：漏水損傷保護は、主に、データセンター、サーバールーム、メインフレームコンピュータルームなど、システムリソースが集中している組織の施設に適用する。組織全体に影響を与えることなく、懸念のある特定のエリアで水供給を遮断するために、主遮断弁に加えて、またはその代わりに、遮断弁を採用することができる。

関連管理策：AT-3, PE-10

拡張管理策：

(1) 漏水損傷保護 | 自動サポート

[*設定：組織が定める自動化されたメカニズム*]を使用して、システムの周辺の水の存在を検知し、[*設定：組織が定める職員または役割*]に警告する。

詳解：自動化されたメカニズムには、通知システム、水検知センサ、および水検知警報装置が含まれる。

関連管理策：なし

参照資料：なし

PE-16 搬入および搬出

管理策：

a. [*設定：組織が定めるシステムコンポーネントのタイプ*]について、施設への搬入および搬出を認可し、制御する。

b. システムコンポーネントの記録を維持する。

詳解：システムコンポーネントの搬入と搬出の認可を適用するには、搬出エリアへのアクセスを制限し、システムおよびメディアライブラリからエリアを分離する必要がある場合がある。

関連管理策：CM-3, CM-8, MA-2, MA-3, MP-5, PE-20, SR-2, SR-3, SR-4, SR-6

拡張管理策：なし

参照資料：なし

PE-17 代替作業サイト

管理策：

a. 従業員が使用を許可されている[*設定：組織が定める代替作業サイト*]を決定し、文書化する。

b. 代替作業サイトで[*設定：組織が定める管理策*]を採用する。

c. 代替作業サイトでの管理策の有効性をアセスメントする。

d. インシデントが発生した場合に従業者が情報セキュリティおよびプライバシー職員と連絡する手段を提供する。

詳解：代替作業サイトには、政府施設または従業者の自宅が含まれる。代替作業サイトは、代替処理サイトとは異なるが、緊急時対応の作業中にすぐに利用できる代替場所を提供できる。組織は、サイトで実施されている業務関連の活動に応じて、特定の代替作業サイトまたはサイトのタイプに応じて、様々な管理策セットを定めることができる。組織が定める管理策を実装しその有効性をアセスメントし、代替作業サイトでインシデントを連絡する手段を提供することは、組織の緊急時対応計画措置をサポートする。

関連管理策：AC-17, AC-18, CP-7

拡張管理策：なし

参照資料：[SP 800-46]

PE-18 システムコンポーネントの設置場所

管理策：[*設定：組織が定める物理的および環境的ハザード*]による潜在的な損傷を最小限に抑え、認可されていないアクセスの機会を最小限に抑えるように、システムコンポーネントを施設内に設置する。

詳解：物理的および環境的ハザードには、洪水、火災、竜巻、地震、ハリケーン、テロ行為、破壊行為、電磁パルス、電気干渉、およびその他の形態の入射する電磁放射線が含まれる。組織は、認可されていない個人がアクセスを許可されていないにもかかわらず、システムの近くにいる可能性があるエントリポイントの場所を考慮する。そのような近接性は、ワイヤレスパケットスニファまたはマイクロフォンを使用した、組織の通信への認可されていないアクセスまたは情報の認可されていない開示のリスクを増大させる可能性がある。

関連管理策：CP-2, PE-5, PE-19, PE-20, RA-3

拡張管理策：

(1) システムコンポーネントの設置場所 | 施設サイト

[撤回：PE-23 に移動した]

参照資料：なし

PE-19 情報漏えい

管理策：電磁信号の放射による情報漏えいからシステムを保護する。

詳解：情報漏えいは、電磁信号の放射から信頼できない環境への、データまたは情報の意図的または意図的でないリリースである。システムのセキュリティ分類または機密性区分（機密性に関して）、組織のセキュリティポリシー、およびリスク許容度が、電磁信号の放射による情報漏えいからシステムを保護するために採用する管理策の選択をガイドする。

関連管理策：AC-18, PE-18, PE-20

拡張管理策：

(1) 情報漏えい | 国家エミッションポリシーおよび手順

情報のセキュリティ分類または機密性区分に基づき、国家エミッションセキュリティポリシーおよび手順に従って、システムコンポーネント、関連するデータ通信、およびネットワークを保護する。

詳解：エミッション・セキュリティ（EMSEC）ポリシーには、以前の TEMPEST ポリシーが含まれる。

関連管理策：なし

参照資料：[FIPS 199]

PE-20 資産の監視および追跡

管理策：[*設定：組織が定める制御エリア*]内の[*設定：組織が定める資産*]の位置および移動について、追跡および監視するために、[*設定：組織が定める資産位置情報技術*]を採用する。

詳解：資産位置情報技術は、重要な資産（車両、装置、システムコンポーネントなど）が認可された場所に確実に存続するようにするのに役立つ。組織は、潜在的なプライバシーの懸念に対処するために、資産位置情報技術の導入と使用に関して、法律顧問および政府機関のプライバシー保護責任者と相談する。

関連管理策：CM-8, PE-16, PM-8

拡張管理策：なし

参照資料：なし

PE-21 電磁パルス保護

管理策：[*設定：組織が定めるシステムおよびシステムコンポーネント*]の電磁パルス損傷に対する[*設定：組織が定める保護手段*]を採用する。

詳解：電磁パルス（EMP：Electromagnetic Pulse）は、ある範囲の周波数に広がる電磁エネルギーの短いバーストである。そのようなエネルギーバーストは、自然のものや人工のものがある。EMP 干渉は、電子装置を破壊または損傷する可能性がある。EMP リスクを軽減するために使用される保護手段には、シールド、サージ抑制装置、トランス、およびアース接地が含まれる。EMP 保護は、米国の重要インフラの一部であるシステムおよびアプリケーションにとって特に重要な場合がある。

関連管理策： PE-18, PE-19

拡張管理策：なし

参照資料：なし

PE-22 コンポーネントマーキング

管理策：[*設定：組織が定めるシステムハードウェアコンポーネント*]について、ハードウェアコンポーネントによる処理、保存、または伝送が許可された情報のインパクトレベルまたは機密性レベルを示すマーキングを行う。

詳解：マーキングを必要とする可能性のあるハードウェアコンポーネントには、入出力デバイス

が含まれる。入力デバイスには、デスクトップおよびノートブックコンピュータ、キーボード、タブレット、およびスマートフォンが含まれる。出力デバイスには、プリンタ、モニタ／ビデオディスプレイ、ファクシミリ、スキャナ、コピー機、オーディオデバイスが含まれる。出力デバイスへの出力を制御する権限は、AC-3 または AC-4 で扱われている。コンポーネントは、デバイスが接続されているシステムのインパクトレベルまたは機密性レベル、または出力が許可されている情報のインパクトレベルまたは機密性レベルを示すためにマーキングする。セキュリティマーキングとは、可読形式のセキュリティ属性の使用を指す。セキュリティラベル付けは、内部システムデータ構造のセキュリティ属性の使用を指す。セキュリティマーキングは、一般に、組織によってパブリックドメインである、または公衆リリース可能であると判断された情報を処理、保存、または伝送するハードウェアコンポーネントには必要ない。ただし、組織は、そのような情報が公開されていることを示すために、公開情報を処理、保存、または伝送するハードウェアコンポーネントにマーキングを要求する場合がある。システムハードウェアコンポーネントのマーキングは、適用される法律、大統領令、指令、ポリシー、規則、および基準を反映する。

関連管理策：AC-3, AC-4, AC-16, MP-3

拡張管理策：なし

参照資料：[IR 8023]

PE-23 施設の場所

管理策：

a. 物理的および環境的ハザードを考慮して、システムが在る施設の場所またはサイトを計画する。

b. 既存の施設については、組織のリスクマネジメント戦略において物理的および環境的ハザードを考慮する。

詳解：物理的および環境的ハザードには、洪水、火災、竜巻、地震、ハリケーン、テロ行為、破壊行為、電磁パルス、電気干渉、およびその他の形態の入射する電磁放射線が含まれる。施設内のシステムコンポーネントの設置場所については、PE-18 で取り扱っている。

関連管理策：CP-2, PE-18, PE-19, PM-8, PM-9, RA-3

参照資料：なし

3.12 計画

計画の要約表へのクイックリンク

PL-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。

1. 以下の[*選択(1 つ以上):組織レベル;ミッション／事業プロセスレベル;システムレベル*]の計画のポリシー。

(a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、および準拠に対処する。

(b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに適合している。

2. 計画のポリシーと関連する計画の管理策の実装を促進するための手順。

b. 計画のポリシーと手順の策定、文書化、および配布することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行の計画をレビューし、更新する。

1. ポリシーについて[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

2. 手順について[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

詳解:計画のポリシーと手順は、システムおよび組織で実装される PL ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に寄与する。したがって、セキュリティおよびプライバシープログラムが計画のポリシーと手順の策定と連携していることが重要である。セキュリティおよびプライバシープログラムのポリシーと手順を組織レベルで確立することは望ましく、一般的には、ミッションまたはシステム固有のポリシーと手順を不要にすることができる。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映する複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムに対して規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述し、手順の対象である個人または役割向けとすることができる。手順は、システムのセキュリティおよびプライバシー計画の中に、または 1 つ以上の別の文書に文書化することもできる。計画のポリシーと手順の更新を引き起こす可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれる。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策:PM-9, PS-8, SI-12

拡張管理策:なし

参照資料:[OMB A-130], [SP 800-12], [SP 800-18], [SP 800-30], [SP 800-39], [SP 800-100]

PL-2 システムセキュリティおよびプライバシー計画

管理策:

a. 以下のようなシステムセキュリティおよびプライバシー計画を策定する。
   1. 組織のエンタープライズアーキテクチャと整合している。
   2. 構成するシステムコンポーネントを明示的に定める。
   3. システムの運用状況を、ミッションおよび事業プロセスの観点から記述する。
   4. システムの役割と責任を果たす個人を特定する。
   5. システムによって処理、保存、および伝送される情報タイプを特定する。
   6. システムのセキュリティ分類化を、根拠を含めて、提供する。
   7. 組織が懸念するシステムに対する特定の脅威を記述する。
   8. 個人情報を取扱うシステムのプライバシーリスクアセスメントの所見を提供する。
   9. システム、および他のシステムまたはシステムコンポーネントへの依存関係または接続に関するシステムの運用環境について記述する。
   10. システムのセキュリティおよびプライバシー要件の概要を提供する。
   11. 該当する場合、関連する管理策ベースラインまたはオーバーレイを特定する。
   12. セキュリティおよびプライバシーの要件を満たすために導入または計画されている管理策を、テーラリング判断の根拠を含め、記述する。
   13. セキュリティおよびプライバシーのアーキテクチャおよび設計上の判断に関するリスクの決定を含める。
   14. [*設定:組織が定める個人またはグループ*]との計画策定および調整を必要とする、システムに影響を与えるセキュリティおよびプライバシー関連の措置を含める。
   15. 計画の実装前に、認可権限のある担当者または指定された代理人によってレビューされ、承認されている。
b. 計画のコピーを配布し、計画に対するその後の変更を[*設定:組織が定める職員または役割*]に通知する。
c. [*設定:組織が定める頻度*]で計画をレビューする。
d. システムおよび運用環境の変更、または計画の実装または管理策アセスメント中に特定された問題に対応するために計画を更新する。
e. 計画を認可されていない開示や変更から保護する。

詳解:システムのセキュリティおよびプライバシー計画は、定義された認可境界内のシステムとシステムコンポーネントを適用範囲とし、システムのセキュリティおよびプライバシーの要件の概要、およびその要件を満たすために選択した管理策を含む。計画は、システムの分野で選択した各管理策の意図した適用について、管理策を正しく実装し、その後管理策の有効性をアセスメントするために十分な詳細レベルで記述する。管理策文書には、システム固有管理策とハイブリッド管理策の実装方法、およびシステムの機能に関する計画と期待事項を記述する。システムセキュリティおよびプライバシー計画は、ライフサイクルベースのセキュリティおよびプライバシーエンジニアリングプロセスをサポートするシステムの設計および開発にも利用できる。システムセキュリティおよびプライバシー計画は、システムの開発ライフサイクル(例えば、ケイパビリティ決定中、代替案の分析中、提案依頼中、設計レビュー中)全体を通して更新され、適応される、生きている文書である。第 2.1 節では、システム開発ライフサイクル中に組織に関連する様々なタイプの要件、および要件と管理策の関係について記述している。

組織は、単一の統合されたセキュリティおよびプライバシー計画を策定することも、別々の計画を維持することもできる。セキュリティおよびプライバシー計画は、セキュリティおよびプライバシーの要件を一連の管理策と拡張管理策に関連付ける。この計画は、管理策と拡張管理策がセ

キュリティおよびプライバシーの要件をどのように満たすかを記述するが、管理策と拡張管理策の設計または実装に関する詳細な技術的記述は提供しない。セキュリティおよびプライバシー計画には、計画の意図、および計画が実装された場合の組織の運営および資産、個人、他の組織、国家に対するリスクのその後の決定に、明確に準拠した設計および実装を可能にする十分な情報（明示的または参照による選択および設定操作に関する管理策パラメータ値の詳述を含む）を含む。

セキュリティおよびプライバシー計画は単一の文書である必要はない。計画は、すでに存在する文書を含む、様々な文書の集合であり得る。効果的なセキュリティおよびプライバシー計画では、ポリシー、手順、および詳細な情報を入手できる設計および実装の仕様を含む追加の文書を広く参照する。参照の利用は、セキュリティおよびプライバシープログラムに関連する文書を削減し、エンタープライズアーキテクチャ、システム開発ライフサイクル、システムエンジニアリング、および資産の取得を含む、他の確立されたマネジメントおよび運用領域におけるセキュリティおよびプライバシー関連情報を維持するのに役立つ。セキュリティおよびプライバシー計画には、詳細な緊急時対応計画やインシデント対応計画の情報を含める必要はないが、代わりに、これらの計画で達成する必要があることを規定するための明示的または参照による十分な情報を提供できる。

組織内の他の個人またはグループとの調整および計画策定を必要とする可能性があるセキュリティおよびプライバシー関連の措置には、アセスメント、監査、点検、ハードウェアおよびソフトウェアのメンテナンス、資産の取得およびサプライチェーンのリスクマネジメント、パッチ管理、および緊急時対応計画のテストが含まれる。計画策定および調整には、緊急事態および非緊急事態（すなわち、計画されたまたは非緊急の計画されていない）状況が含まれる。セキュリティおよびプライバシー関連の措置を計画および調整するために組織によって規定されたプロセスは、必要に応じて他の文書に含めることもできる。

関連管理策：AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CM-13, CP-2, CP-4, IR-4, IR-8, MA-4, MA-5, MP-4, MP-5, PL-7, PL-8, PL-10, PL-11, PM-1, PM-7, PM-8, PM-9, PM-10, PM-11, RA-3, RA-8, RA-9, SA-5, SA-17, SA-22, SI-12, SR-2, SR-4

拡張管理策：

(1) システムセキュリティおよびプライバシー計画 | 業務構想文書

［撤回：PL-7 に組み込まれた］

(2) システムセキュリティおよびプライバシー計画 | 機能アーキテクチャ

［撤回：PL-8 に組み込まれた］

(3) システムセキュリティおよびプライバシー計画 | 他の組織のエンティティとの計画策定および調整

［撤回：PL-2 に組み込まれた］

参照資料：[OMB A-130], [SP 800-18], [SP 800-37], [SP 800-160-1], [SP 800-160-2]

PL-3 システムセキュリティ計画の更新

［撤回：PL-2 に組み込まれた］

PL-4 行動規則

管理策：

a. システムへのアクセスを必要とする個人に、情報とシステムの利用、セキュリティおよびプライバシーに関する責任と期待される振る舞いについて説明した規則を規定し、提供する。

b. 対象の個人から、情報およびシステムへのアクセスを認可する前に、行動規則を読み、理解し、遵守することに同意したことを示す文書化された承諾書を受け取る。

c. ［*設定：組織が定める頻度*］で行動規則を見直し、更新する。

d. [*選択（1つ以上）：[設定：組織が定める頻度]；規則が改訂または更新された場合*]、以前の版の行動規則を承諾した個人に、読んで再度承諾するよう要求する。

詳解：行動規則は、組織のユーザに対するアクセス合意書の一つのタイプである。その他のタイプのアクセス合意書には、秘密保持契約、利益相反契約、および受容可能な利用合意書が含まれる（PS-6 を参照）。組織は、個々のユーザの役割と責任に基づいて行動規則を考慮し、特権ユーザに適用される規則と一般ユーザに適用される規則を区別する。連邦政府のシステムから情報を受け取る個人を含む、あるタイプの非組織のユーザの行動規則を規定することは、そのようなユーザの数が多く、システムとのインタラクションの種類が限定されていることを考えると、実現できないことが多い。組織のユーザと非組織のユーザの行動規則を AC-8 でも規定することができる。関連管理策セクションでは、組織の行動規則に関連する管理策のリストを提供する。組織が実施するリテラシートレーニングと意識向上活動および役割ベースのトレーニングプログラムに行動規則が含まれている場合、管理策の文書化された承諾の部分である PL-4b は、これらのトレーニングによって満たしてもよい。行動規則の文書化された承諾には、電子的または物理的な署名、および電子的な同意のチェックボックスまたはラジオボタンが含まれる。

関連管理策：AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5, SI-12

拡張管理策：

(1) 行動規則 | ソーシャルメディアおよび外部サイト／アプリケーションの使用制限

行動規則に以下に対する制限を含める。

(a) ソーシャルメディア、SNS、および外部サイト／アプリケーションの使用。

(b) 公開ウェブサイトへの組織の情報の掲載。

(c) 外部サイト／アプリケーション上にアカウントを作成するための、組織が提供する識別子（例えば、電子メールアドレス）および認証秘密情報（例えば、パスワード）の使用。

詳解：ソーシャルメディア、SNS、および外部サイト／アプリケーションの使用制限は、組織の職員がそのようなサイトを業務または公用に使用している場合について、組織の情報がソーシャルメディアおよびソーシャルネットワーキングトランザクションに関係している場合について、および職員が組織のシステムからソーシャルメディアおよび SNS にアクセスする場合について、ソーシャルメディア、SNS、および外部サイトの使用に関連する行動規則で対処する。組織はまた、認可されていないエンティティが非公開の組織の情報をソーシャルメディアおよび SNS から直接または推論を通じて取得することを防止する具体的な規則でも対処する。非公開情報には、個人情報やシステムアカウント情報が含まれる。

関連管理策：AC-22, AU-13

参照資料：[OMB A-130], [SP 800-18]

PL-5 プライバシー影響評価

[撤回：RA-8 に組み込まれた]

PL-6 セキュリティ関連措置計画

[撤回：PL-2 に組み込まれた]

PL-7 業務構想文書

管理策：

a. 組織が情報セキュリティおよびプライバシーの観点からシステムをどのように運用しようとしているのかを記述する業務構想文書（CONOPS：Concept of Operations）を作成する。

b. [*設定：組織が定める頻度*]で CONOPS をレビューし、更新する。

詳解：CONOPS は、システムのセキュリティまたはプライバシー計画、または他のシステム開発ライフサイクル文書に含まれる場合がある。CONOPS は、システム開発ライフサイクル全体を通じて更新する必要のある生きている文書である。例えば、システム設計レビューでは、管理策の設計、システムアーキテクチャ、および運用手順と一貫性が保たれていることを確実にするために、業務構想文書がチェックされる。CONOPS への変更は、調達仕様書、システム開発ライフサイクル文書、システムエンジニアリング文書などの、セキュリティおよびプライバシー計画、セキュリティおよびプライバシーアーキテクチャ、その他の組織文書に対する進行中の更新を反映する。

関連管理策：PL-2, SA-2, SI-12

拡張管理策：なし

参照資料：[OMB A-130]

PL-8 セキュリティおよびプライバシーアーキテクチャ

管理策：

a. 以下のようなシステムセキュリティおよびプライバシーアーキテクチャを策定する。
   1. 組織の情報の機密性、完全性、および可用性を保護するために取るべき要件とアプローチを記述する。
   2. 個人のプライバシーリスクを最小限に抑えるよう個人情報を取扱うために取るべき要件とアプローチを記述する。
   3. このアーキテクチャがエンタープライズアーキテクチャにどのように統合されサポートされているかを記述する。
   4. 外部システムおよびサービスに関する前提条件および依存関係を記述する。

b. [*設定：組織が定める頻度*]でエンタープライズアーキテクチャの変更を反映するために、このアーキテクチャをレビューし、更新する。

c. セキュリティおよびプライバシー計画、業務構想文書（CONOPS：Concept of Operations）、重要度分析、組織の手順、調達および取得における、計画されたアーキテクチャの変更を反映する。

詳解：システムレベルのセキュリティおよびプライバシーアーキテクチャは、エンタープライズアーキテクチャに統合され、その一部として策定された PM-7 で記述されている組織全体のセキュリティおよびプライバシーアーキテクチャと一致している。アーキテクチャには、アーキテクチャの説明、セキュリティおよびプライバシーの機能（管理策を含む）の割り当て、外部インタフェースでのセキュリティおよびプライバシー関連情報、インタフェース間で交換される情報、および各インタフェースに関連する保護のメカニズムが含まれる。アーキテクチャには、ユーザの役割や各役割に割り当てられたアクセス特権；セキュリティおよびプライバシーの要件；システムによって処理、保存、伝送される情報タイプ；サプライチェーンのリスクマネジメント要件；情報およびシステムサービスの復元優先順位；およびその他の保護ニーズなどの、他の情報も含めることもできる。

[SP 800-160-1]は、システム開発ライフサイクルプロセスの一部としてのセキュリティアーキテクチャの利用に関するガイダンスを提供している。[OMB M-19-03]は、高価値資産に対して[SP 800-160-1]で記述されているシステムセキュリティエンジニアリングの概念を利用することを要求している。セキュリティおよびプライバシーのアーキテクチャは、RFP 対応として提案されたアーキテクチャのレビューを通した代替案の分析から、実装前および実装中の設計レビュー（例えば、予備的な設計レビューおよび重要な設計レビュー中）まで、システム開発ライフサイクル全体にわたってレビューおよび更新する。

今日の現代のコンピューティングアーキテクチャでは、組織がすべての情報リソースを管理することは一般的でなくなってきている。外部の情報サービスやサービスプロバイダと主要な依存関係がある場合がある。セキュリティおよびプライバシーのアーキテクチャにおけるそのような依存関係を記述することは、包括的なミッションと事業保護戦略を策定するために必要である。

構成変更管理の下で、組織のシステムのベースライン構成を規定し、策定し、文書化し、維持することは、効果的なアーキテクチャを実装および維持するために重要である。アーキテクチャの策定は、セキュリティおよびプライバシー要件をサポートするために必要な管理策が確実に特定され、効果的に実装されるように、政府機関の情報セキュリティ責任者および政府機関のプライバシー保護責任者と調整する。多くの状況では、システムのセキュリティおよびプライバシーアーキテクチャに違いがない場合がある。他の状況では、セキュリティ目的は適切に満たされるが、プライバシー目的は、セキュリティ要件によって部分的にのみ満たされる場合がある。これらのケースでは、要件を満足するために必要なプライバシー要件を考慮することで、別個のプライバシーアーキテクチャをもたらす。ただし、文書は、組み合わせたアーキテクチャを単に反映してもよい。

PL-8 は主に、アーキテクチャをシステム用に策定すること、さらに、アーキテクチャをエンタープライズアーキテクチャに統合または密接に結合することを確実にするために、組織に向けられたものとなっている。対照的に、SA-17 は、主に外部の IT 製品およびシステムの開発者とインテグレーターに向けられたものとなっている。PL-8 を補完する SA-17 は、組織がシステムまたはコンポーネントの開発を外部エンティティに外部委託する場合、および組織のエンタープライズアーキテクチャとセキュリティおよびプライバシーアーキテクチャとの一貫性を実証する必要がある場合に選択される。

関連管理策：CM-2, CM-6, PL-2, PL-7, PL-9, PM-5, PM-7, RA-9, SA-3, SA-5, SA-8, SA-17, SC-7

拡張管理策：

(1) セキュリティおよびプライバシーアーキテクチャ | 多層防御

次のような多層防御アプローチを利用して、システムセキュリティおよびプライバシーアーキテクチャを設計する。

(a) [*設定：組織が定める管理策*]を[*設定：組織が定める場所とアーキテクチャ層*]に割り当てる。

(b) 割り当てられた管理策が協調し、相互に補強し合う形で機能することを確実にする。

詳解：組織は、セキュリティおよびプライバシーアーキテクチャにおいて戦略的にセキュリティおよびプライバシー管理策を割り当て、敵対者が目的を達成するために複数の管理策を克服しなければならないようにする。複数の管理策を破ることを敵対者に要求することで、敵対者の作業要因を増加させることにより、情報リソースを攻撃することをより困難にする。また、攻撃を検知する可能性が高くなる。割り当てられた管理策の調整は、1 つの管理策に関与する攻撃が、他の管理策を妨害して悪影響を与え、意図しない結果をもたらさないことを確実にするために不可欠である。意図しない結果には、システムのロックアウトや警報の連鎖反応などがある。システムおよび組織における管理策の選定は、慎重な分析を必要とする重要な活動である。組織の資産の価値は、追加の階層化を提供する上で重要な考慮事項である。多層防御アーキテクチャのアプローチには、モジュール化と階層化（SA-8(3)を参照）、システムとユーザ機能の分離（SC-2 を参照）、およびセキュリティ機能の分離（SC-3 を参照）が含まれる。

関連管理策：SC-2, SC-3, SC-29, SC-36

(2) セキュリティおよびプライバシーアーキテクチャ | サプライヤの多様性

[*設定：組織が定める場所およびアーキテクチャ層*]に割り当てた[*設定：組織が定める管理策*]を、異なるサプライヤから取得することを要求する。

詳解：IT 製品には、様々な長所と短所がある。幅広い製品を提供することで、個々の製品が補完される。例えば、悪意のあるコードからの保護を提供するベンダは通常、製品を様々なタイミングで更新し、多くの場合、優先順位と開発スケジュールに基づいて、既知のウイルス、トロイの木馬、またはワームに対するソリューションを開発する。異なる製品を異なる場所に展開することにより、製品の少なくとも 1 つが悪意のあるコードを検知する可能性が高まる。プライバシーに関しては、ベンダはシステム内の個人情報を追跡する製品を提供してもよい。製品は異なる追跡方法を使用してもよい。複数の製品を使用し、より確実な個人情報のインベントリの作成につなげてもよい。

関連管理策：SC-29, SR-3

参照資料：[OMB A-130], [SP 800-160-1], [SP 800-160-2]

PL-9 一元管理

管理策：[*設定：組織が定める管理策および関連プロセス*]を一元管理する。

詳解：一元管理では、選択された管理策とプロセスの組織全体の管理と実装を参照する。これには、組織が定める一元管理された管理策とプロセスの計画、実装、アセスメント、認可、監視が含まれる。管理策の一元管理は、一般に（受け継がれた）共通管理策の概念に関連しているため、集中管理は、管理策の実装と管理の基準化、および組織のリソースの賢明な利用を奨励し促進する。集中管理された管理策とプロセスは、運用の初期および進行中の認可をサポートし、組織の継続的監視の一環として、アセスメントの独立性要件を満たしてもよい。

自動化されたツール（例えば、セキュリティ情報およびイベント管理ツール、またはエンタープライズセキュリティ監視および管理ツール）は、集中管理された管理策およびプロセスに関連する情報の正確性、一貫性および可用性を改善することができる。自動化ツールは、データ集約およびデータ相関ケイパビリティ、警告のメカニズム、組織内のリスクベースの意思決定をサポートするダッシュボードも提供できる。

組織は、管理策選択プロセスの一環として、リソースとケイパビリティに基づいて、一元管理に適した管理策を決定する。管理策のあらゆる側面を一元管理することが常に可能であるとは限らない。そのような場合、管理策は、管理策が集中的にまたはシステムレベルで管理および実装されるハイブリッド管理策として扱うことができる。完全または部分的一元管理の候補となる管理策および拡張管理策には、AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-4（すべて）, AC-17(1), AC-17(2), AC-17(3), AC-17(9), AC-18(1), AC-18(3), AC-18(4), AC-18(5), AC-19(4), AC-22, AC-23, AT-2(1), AT-2(2), AT-3(1), AT-3(2), AT-3(3), AT-4, AU-3, AU-6(1), AU-6(3), AU-6(5), AU-6(6), AU-6(9), AU-7(1), AU-7(2), AU-11, AU-13, AU-16, CA-2(1), CA-2(2), CA-2(3), CA-3(1), CA-3(2), CA-3(3), CA-7(1), CA-9, CM-2(2), CM-3(1), CM-3(4), CM-4, CM-6, CM-6(1), CM-7(2), CM-7(4), CM-7(5), CM-8（すべて）, CM-9(1), CM-10, CM-11, CP-7（すべて）, CP-8（すべて）, SC-43, SI-2, SI-3, SI-4（すべて）, SI-7, SI-8 を含むが、これらに限定しない。

関連管理策：PL-8, PM-9

拡張管理策：なし

参照資料：[OMB A-130], [SP 800-37]

PL-10 ベースラインの選択

管理策：システムの管理策ベースラインを選択する。

詳解：管理策ベースラインは、関心のあるグループ、組織、またはコミュニティの保護ニーズに対応するために特別に構築され、事前に規定された一連の管理策である。管理策は、法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインによって課せられた命令を満たすか、またはベースラインに固有の仮定の下でベースラインのすべてのユーザに共通する脅威に対応するために、ベースラインに対して選択する。ベースラインは、個人のプライバシー、情報、および情報システムを保護するための出発点であり、ミッション、事業、またはその他の制約に従ってリスクをマネジメントするための後続のテーラリング措置を伴う（PL-11 を参照）。連邦政府の管理策ベースラインは[SP 800-53B]で提供されている。管理策ベースラインの選択は、利害関係者のニーズによって決定される。利害関係者のニーズは、適用される法律、大統領令、指令、規則、ポリシー、標準、およびガイドラインによって課せられる命令と同様に、ミッションおよび事業要件を考慮する。例えば、[SP 800-53B]の管理策ベースラインは、[FISMA]および[PRIVACT]の要件に基づいている。要件は、法律を実装する NIST 基準およびガイドラインとともに、システムで処理、保存、および伝送される情報タイプと情報をレビューした後、組織の運用および資産、個人、他の組織、または国家に対する情報またはシステムの喪失または侵害の潜在的な有害なインパクトを分析した後、システムと組織のリスクアセスメント所見を考慮した後、管理策ベースラインの 1 つを選択するよう組織に指示する。[CNSSI 1253]は、国家安全保

障システムの管理策ベースラインに関するガイダンスを提供している。

関連管理策：PL-2, PL-11, RA-2, RA-3, SA-8

拡張管理策：なし

参照資料：[FIPS 199], [FIPS 200], [SP 800-30], [SP 800-37], [SP 800-39], [SP 800-53B], [SP 800-60-1], [SP 800-60-2], [SP 800-160-1], [CNSSI 1253]

PL-11 ベースラインのテーラリング

管理策：指定されたテーラリング措置を適用し、選択された管理策ベースラインを適合させる。

詳解：テーラリングの概念により、組織は、規定された一連のテーラリング措置を適用することにより、一連のベースライン管理策を固有化またはカスタマイズすることができる。テーラリング措置は、特定のミッションと事業機能、システムが動作する環境、システムに影響を与える可能性のある脅威と脆弱性、ミッションと事業の成功にインパクトを与えるその他の状況や状態を反映するセキュリティおよびプライバシー計画を組織が策定できるようにすることで、そのような固有化とカスタマイズを促進する。テーラリングガイダンスは[SP 800-53B]で提供されている。管理策ベースラインのテーラリングは、共通管理策の特定と指定、スコーピングの考慮事項の適用、代替管理策の選択、管理策パラメータへの値の設定、必要に応じて管理策ベースラインへの追加の管理策の補足、および管理策の実装に関する情報の提供によって行われる。[SP 800-53B]の一般的なテーラリング措置は、組織のニーズに基づいて追加の措置で補足することができる。[FISMA]、[PRIVACT]、および[OMB A-130]のセキュリティおよびプライバシー要件に従って、[SP 800-53B]のベースラインに、テーラリング措置を適用できる。あるいは、異なる管理策ベースラインを採用している他の関心のあるコミュニティは、[SP 800-53B]のテーラリング措置を適用して、それらのエンティティの特定のニーズや懸念を表す管理策を固有化またはカスタマイズすることができる。

関連管理策：PL-10, RA-2, RA-3, RA-9, SA-8

拡張管理策：なし

参照資料：[FIPS 199], [FIPS 200], [SP 800-30], [SP 800-37], [SP 800-39], [SP 800-53B], [SP 800-60-1], [SP 800-60-2], [SP 800-160-1], [CNSSI 1253]

3.13 プログラムマネジメント

プログラムマネジメント管理策

[FISMA]、[PRIVACT]、および[OMB A-130]は、連邦政府情報システムにより処理、保存、伝送される連邦政府情報の機密性、完全性、可用性を確保するために、および個人のプライバシーを保護するために、組織全体の情報セキュリティおよびプライバシープログラムを策定、実装、および監視することを連邦政府機関に要求する。このセクションで記述されたプログラムマネジメント(PM)管理策は、組織レベルで実装されるもので、個々の情報システムに向けられたものではない。PM 管理策は、適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインへの組織の遵守を促進するように設計されている。この管理策は、[FIPS 200]のインパクトレベルとは無関係であるため、[SP 800-53B]で記述されている管理策ベースラインとは関連付けられていない。

組織は、情報セキュリティおよびプライバシープログラム計画におけるプログラムマネジメント管理策を文書化する。組織全体の情報セキュリティプログラム計画(PM-1 を参照)およびプライバシープログラム計画(PM-18 を参照)は、組織の情報システムのために策定されたシステムセキュリティおよびプライバシー計画(PL-2 を参照)を補足する。個々の情報システムのシステムセキュリティおよびプライバシー計画と、情報セキュリティおよびプライバシープログラム計画は、組織が採用するセキュリティおよびプライバシー管理策の全体をカバーする。

プログラムマネジメントの要約表へのクイックリンク

PM-1 情報セキュリティプログラム計画

管理策:

a. 以下のような組織全体の情報セキュリティプログラム計画を策定し、配布する。
   1. セキュリティプログラムの要件の概要、およびセキュリティプログラムマネジメント管理策と、それらの要件を満たすために導入または計画されている共通管理策の記述を提供する。
   2. 役割、責任、管理責任、組織のエンティティ間の調整、準拠の特定と割り当てを含む。
   3. 情報セキュリティに責任を負う組織エンティティ間の調整を反映する。
   4. 組織の運営(ミッション、事業、イメージ、評判を含む)、組織の資産、個人、他の組織、および国家が被るリスクについて責任と説明責任を有する責任者が承認する。

b. [*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機に、組織全体の情報セキュリティプログラム計画をレビューし、更新する。

c. 情報セキュリティプログラム計画を認可されていない開示および変更から保護する。

詳解:情報セキュリティプログラム計画は、組織全体の情報セキュリティプログラムについてのセキュリティ要件の概要を提供する正式な文書であり、それらの要件を満たすために導入または計画されているプログラムマネジメント管理策および共通管理策を記述する。情報セキュリティプログラム計画は、単一の文書または複数の文書の編集物で表すことができる。プライバシープログラム計画とサプライチェーンのリスクマネジメント計画は、それぞれ PM-18 と SR-2 で

別々に扱われている。

情報セキュリティプログラム計画は、プログラムマネジメント管理策と共通管理策に関する実装の詳細を文書化する。計画は、計画の意図に明確に準拠している実装を可能にするための管理策（明示または参照による、設定および選択操作のパラメータの指定を含む）、および計画が意図通りに実装された場合に発生するリスクの決定に関する十分な情報を提供する。情報セキュリティプログラム計画の更新には、計画の実装中または管理策のアセスメント中に特定された組織の変更や問題を含める。

プログラムマネジメント管理策は、組織レベルまたはミッションまたは事業プロセスレベルで実装することができ、組織の情報セキュリティプログラムをマネジメントするために不可欠である。プログラムマネジメント管理策は、特定のシステムから独立しているため、プログラムマネジメント管理策は、共通管理策、システム固有管理策、ハイブリッド管理策とは異なる。個別のシステムセキュリティ計画と組織全体の情報セキュリティプログラム計画を合わせて、組織内で採用されているセキュリティ管理策を完全にカバーする。

組織のシステムにより受け継がれ利用可能な共通管理策は、管理策がシステムの個別のセキュリティ計画に含まれていない限り、組織の情報セキュリティプログラム計画の付属書に記載する。組織全体の情報セキュリティプログラム計画は、共通の管理策の記述を含む別個のセキュリティ計画を示している。

情報セキュリティプログラム計画の更新を促す可能性のあるイベントには、組織全体のアセスメントまたは監査所見、セキュリティインシデントまたはブリーチ、または法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更などが含まれるが、これらに限定されない。

関連管理策：PL-2, PM-18, PM-30, RA-9, SI-12, SR-2

拡張管理策：なし

参照資料：[FISMA], [OMB A-130], [SP 800-37], [SP 800-39]

PM-2 情報セキュリティプログラムの責任者の役割

管理策：組織全体の情報セキュリティプログラムを調整、策定、実装、維持するためのミッションとリソースを有する政府機関の情報セキュリティ責任者を任命する。

詳解：政府機関の情報セキュリティ責任者は、組織の担当者である。（適用される法律、大統領令、指令、規則、ポリシー、および基準によって定められた）連邦政府機関の場合、この担当者は政府機関の情報セキュリティ責任者である。組織では、この担当者を情報セキュリティ責任者または最高情報セキュリティ責任者と呼ぶこともある。

関連管理策：なし

拡張管理策：なし

参照資料：[OMB M-17-25], [SP 800-37], [SP 800-39], [SP 800-181]

PM-3 情報セキュリティおよびプライバシーリソース

管理策：

a. 資金計画および投資要件において、情報セキュリティおよびプライバシープログラムを実装するために必要なリソースを含め、この要件に対するすべての例外事項を文書化する。

b. 適用される法律、大統領令、指令、規則、ポリシー、および基準に従って、資金計画および投資要件における情報セキュリティおよびプライバシープログラムに対処するために必要な文書を準備する。

c. 計画された情報セキュリティおよびプライバシーリソースに、経費を利用できるようにする。

詳解：組織は、情報セキュリティおよびプライバシーの推進者を規定することを考慮し、必要なリソースを含める一環として、必要に応じて専門技術とリソースを割り当てる。組織は、資金計画および投資管理プロセスの情報セキュリティおよびプライバシーの側面を管理および監督するために、投資計画委員会または同様のグループを指定し、権限を与える。

関連管理策：PM-4, SA-2

拡張管理策：なし

参照資料：[OMB A-130]

PM-4 実施計画およびマイルストーンプロセス

管理策：

a. 情報セキュリティ、プライバシー、サプライチェーンのリスクマネジメントプログラムおよび関連する組織のシステムの実施計画およびマイルストーンを確実にするためのプロセスを、以下のように実装する。

   1. 策定し、維持する。
   2. 組織の運営および資産、個人、他の組織、および国家に対するリスクに適切に対応するために、情報セキュリティ、プライバシー、およびサプライチェーンのリスクマネジメントに関する是正措置を文書化する。
   3. 規定された報告要件に従って報告する。

b. 組織のリスクマネジメント戦略およびリスク対応措置に関する組織全体の優先事項との整合性のために、実施計画およびマイルストーンをレビューする。

詳解：実施計画およびマイルストーンは重要な組織の文書であり、行政管理予算局によって規定された報告要件の対象となる。組織は、リスク対応措置に優先順位を付け、組織の目標と目的との一貫性を確保し、組織全体の視点で実施計画およびマイルストーンを策定する。実施計画およびマイルストーンの更新は、管理策アセスメントと継続的監視措置からの所見に基づいている。情報システムレベル、ミッション／事業プロセスレベル、組織／ガバナンスレベルに対応する複数の実施計画およびマイルストーンが存在し得る。連邦政府の組織では、実施計画およびマイルストーンを要求されるが、他のタイプの組織では、計画された是正措置を文書化し追跡することで、リスクを軽減することができる。システムレベルでの実施計画およびマイルストーンに関する具体的なガイダンスは、CA-5 に記載されている。

関連管理策：CA-5, CA-7, PM-3, RA-7, SI-12

拡張管理策：なし

参照資料：[PRIVACT], [OMB A-130], [SP 800-37]

PM-5 システムインベントリ

管理策：[*設定：組織が定める頻度*]で組織のシステムインベントリを作成および更新する。

詳解：[OMB A-130]は、システムインベントリの作成および関連する報告要件に関するガイダンスを提供する。システムインベントリとは、CM-8 で記述されているシステムコンポーネントではなく、組織全体のシステムのインベントリを指す。

関連管理策：なし

拡張管理策：

(1) システムインベントリ｜個人情報のインベントリ

[*設定：組織が定める頻度*]で個人情報を取扱うすべてのシステム、アプリケーション、およびプロジェクトのインベントリを作成し、維持し、更新する。

詳解：個人情報を取扱うシステム、アプリケーション、およびプロジェクトのインベントリは、

データアクションのマッピングをサポートし、個人にプライバシー通知を提供し、的確な個人情報を維持し、個人情報を運用目的として必要としない場合に個人情報の取扱いを限定する。組織は、システムが個人情報を認可された目的でのみ取扱うこと、およびこの取扱いが、そこに明示された目的に関連し、かつ必要であることを保証することを確実にするために、このインベントリを使用する場合がある。

関連管理策：AC-3, CM-8, CM-12, CM-13, PL-8, PM-22, PT-3, PT-5, SI-12, SI-18

参照資料：[OMB A-130], [IR 8062]

PM-6 パフォーマンス尺度

管理策：情報セキュリティおよびプライバシーのパフォーマンス尺度を策定し、監視し、報告する。

詳解：パフォーマンス尺度は、情報セキュリティおよびプライバシープログラムと、そのプログラムをサポートするために採用された管理策の有効性または効率を測定するために組織が使用する結果ベースの指標である。セキュリティおよびプライバシーのリスクマネジメントを促進するために、組織は、パフォーマンス尺度を、リスクマネジメント戦略で定義されている組織のリスク許容度と一致させることを考慮する。

関連管理策：CA-7, PM-9

拡張管理策：なし

参照資料：[OMB A-130], [SP 800-37], [SP 800-39], [SP 800-55], [SP 800-137]

PM-7 エンタープライズアーキテクチャ

管理策：情報セキュリティ、プライバシー、および組織の運営と資産、個人、他の組織、国家に対するリスクの結果を考慮して、エンタープライズアーキテクチャを策定し、維持する。

詳解：セキュリティおよびプライバシーの要件と管理策をエンタープライズアーキテクチャに統合することで、セキュリティおよびプライバシーの考慮事項がシステム開発ライフサイクル全体にわたって確実に対処され、組織のミッションと事業プロセスに明確に関連するようになる。セキュリティおよびプライバシー要件を統合するプロセスは、組織のリスクマネジメント戦略と整合性のあるエンタープライズアーキテクチャと組織のセキュリティおよびプライバシーアーキテクチャにも組み込む。PM-7 では、セキュリティおよびプライバシーのアーキテクチャは、複数システムを代表する1つのシステムレベルで策定し、すべての組織のシステムを表す。PL-8 では、セキュリティおよびプライバシーのアーキテクチャは、個々のシステムを表すレベルで策定する。システムレベルのアーキテクチャは、組織が定めたセキュリティおよびプライバシーのアーキテクチャと一致している。セキュリティおよびプライバシーの要件および管理策の統合は、リスクマネジメントフレームワーク[SP 800-37]の厳格な適用と、セキュリティ基準およびガイドラインのサポートを通じて最も効果的に達成される。

関連管理策：AU-6, PL-2, PL-8, PM-11, RA-2, SA-3, SA-8, SA-17

拡張管理策：

(1) エンタープライズアーキテクチャ | オフロード

[*設定：組織が定める非必須機能またはサービス*]を他のシステム、システムコンポーネント、または外部プロバイダにオフロードする。

詳解：システムが提供するすべての機能またはサービスが、組織のミッションまたは事業機能に必須であるとは限らない。印刷またはコピーは、組織にとって必須ではないがサポートするサービスの一例である。そのようなサポート的であるが必須ではない機能またはサービスは、可能な場合はいつでも、必須のミッションまたは事業機能をサポートする機能またはサービスと同じ場所に配置しない。同じシステムまたはシステムコンポーネントでそのような機能を維持することは、組織の必須ミッションの機能またはサービスへの攻撃対象領域を増大させる。サポート的であるが必須ではない機能を重要ではないシステム、システムコンポーネント、または外部プロバイダに移動することは、それらの機能またはサー

ビスを、その機能またはサービスの専門家である個人またはプロバイダの管理下に置くことにより、効率を高めることもできる。

関連管理策：SA-8

参照資料：[OMB A-130], [SP 800-37], [SP 800-39], [SP 800-160-1], [SP 800-160-2]

PM-8 重要インフラ計画

管理策：重要インフラおよび主要リソース保護計画の策定、文書化、更新における情報セキュリティおよびプライバシーの課題に対処する。

詳解：保護戦略は重要な資産とリソースの優先順位付けに基づいている。重要インフラと主要リソースを定義し、関連する重要インフラ保護計画を準備するための要件とガイダンスは、適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに記載されている。

関連管理策：CP-2, CP-4, PE-18, PL-2, PM-9, PM-11, PM-18, RA-3, SI-12

拡張管理策：なし

参照資料：[EO 13636], [OMB A-130], [HSPD 7], [DHS NIPP]

PM-9 リスクマネジメント戦略

管理策：

a. 以下を管理するための包括的な戦略を策定する。
   1. 組織のシステムの運用と利用に関連する、組織の運営および資産、個人、他の組織、および国家に対するセキュリティリスク。
   2. 個人情報の認可された取扱いに起因する個人のプライバシーリスク。
b. 組織全体で一貫したリスクマネジメント戦略を実装する。
c. 組織の変更に対処するために、[*設定：組織が定める頻度*]、または必要に応じて、リスクマネジメント戦略をレビューし、更新する。

詳解：組織全体のリスクマネジメント戦略には、組織のセキュリティおよびプライバシーのリスク許容度、セキュリティおよびプライバシーのリスク軽減戦略、許容可能なリスクアセスメント方法、組織のリスク許容度に関して組織全体のセキュリティおよびプライバシーのリスクを評価するプロセス、リスクを長期にわたって監視するためのアプローチを含む。リスクマネジメントの責任者（機関の長または指名された担当者）は、情報セキュリティ管理プロセスを、戦略プロセス、運用プロセス、および予算計画プロセスと連携させる。リスクマネジメントの責任者が率いるリスク管理部署は、組織全体のリスクマネジメント戦略の一貫した適用を促進することができる。リスクマネジメント戦略は、戦略が広範かつ包括的であることを確実にするために、組織の内部および外部両方の他のソースからのセキュリティおよびプライバシーリスク関連のインプット情報により、情報を得ることができる。PM-30 に記述されているサプライチェーンのリスクマネジメント戦略は、組織全体のリスクマネジメント戦略に有用なインプット情報を提供することもできる。

関連管理策：AC-1, AU-1, AT-1, CA-1, CA-2, CA-5, CA-6, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PM-2, PM-8, PM-18, PM-28, PM-30, PS-1, PT-1, PT-2, PT-3, RA-1, RA-3, RA-9, SA-1, SA-4, SC-1, SC-38, SI-1, SI-12, SR-1, SR-2

拡張管理策：なし

参照資料：[OMB A-130], [SP 800-30], [SP 800-37], [SP 800-39], [SP 800-161], [IR 8023]

PM-10 認可プロセス

管理策：

a. 組織のシステムのセキュリティおよびプライバシーの状態、およびそれらのシステムが

認可プロセスを通して運用する環境を管理する。

b. 組織のリスクマネジメントプロセスにおいて特定の役割および責任を果たす個人を指定する。

c. 認可プロセスを組織全体のリスクマネジメントプログラムに統合する。

詳解：組織のシステムと運用環境の認可プロセスでは、組織全体のリスクマネジメントプロセス、および関連するセキュリティおよびプライバシーの基準とガイドラインの実装が求められる。リスクマネジメントプロセスの特定の役割には、リスク管理者（部署）および各組織のシステムおよび共通管理策の提供者に対する指定された認可権限のある担当者が含まれる。組織の認可プロセスは、組織の運営、組織の資産、個人、他の組織、国家に対するセキュリティおよびプライバシーリスクの現時点での理解と受容を促すために、継続的監視プロセスと統合する。

関連管理策：CA-6, CA-7, PL-2

拡張管理策：なし

参照資料：[SP 800-37], [SP 800-39], [SP 800-181]

PM-11 ミッションおよび事業プロセスの規定

管理策：

a. 情報セキュリティおよびプライバシー、および組織の運営、組織の資産、個人、他の組織、国家にもたらされるリスクを考慮して、組織のミッションおよび事業プロセスを規定する。

b. 規定したミッションおよび事業プロセスから生じる情報保護および個人情報の取扱いのニーズを決定する。

c. [*設定：組織が定める頻度*]でミッションおよび事業プロセスをレビューし、改訂する。

詳解：情報保護のニーズは、技術に依存しないケイパビリティであり、情報の侵害（すなわち、機密性、完全性、可用性、またはプライバシーの喪失）による、組織、個人、システム、国家に対する脅威に対抗するために求められるものである。情報保護と個人情報の取扱いのニーズは、組織の利害関係者により規定されたミッションと事業ニーズ、それらのニーズを満たすように設計されたミッションと事業プロセス、および組織のリスクマネジメント戦略から導出される。情報保護と個人情報の取扱いのニーズは、組織とシステムに求められる管理策を決定する。情報保護と個人情報取扱いのニーズを規定するために本質的なことは、情報の侵害やブリーチが発生した場合に生ずる可能性のある有害なインパクトを理解することである。分類プロセスは、このような潜在的インパクトを判定するために使用される。個人のプライバシーリスクは、個人情報の侵害から生ずる可能性があるだけでなく、情報ライフサイクルのいずれかの段階における個人情報の取扱いの意図しない結果または副産物として生ずる可能性がある。プライバシーリスクアセスメントは、個人情報のシステムでの取扱いから個人に生ずるリスクに優先順位を付けるために使用される。これらのリスクアセスメントにより、組織およびシステムに求められるプライバシー管理策の選択が可能になる。ミッションおよび事業プロセスの規定、および関連する保護要件は、組織のポリシーおよび手順に従って文書化される。

関連管理策：CP-2, PL-2, PM-7, PM-8, RA-2, RA-3, RA-9, SA-2

拡張管理策：なし

参照資料：[OMB A-130], [FIPS 199], [SP 800-39], [SP 800-60-1], [SP 800-60-2], [SP 800-160-1]

PM-12 インサイダー脅威対策プログラム

管理策：分野横断的なインサイダー脅威対策インシデント対応チームを含むインサイダー脅威対策プログラムを実装する。

詳解：国家機密情報を取り扱う組織は、大統領令 13587 [EO 13587]および国家インサイダー脅

威ポリシー[ODNI NITP]に基づき、インサイダー脅威対策プログラムを規定することが求められる。国家機密情報を扱う環境のインサイダー脅威対策プログラムに適用されるものと同じ基準およびガイドラインを効果的に採用して、非国家安全保障システムにおける管理対象非機密情報およびその他の情報のセキュリティを向上させることもできる。インサイダー脅威対策プログラムは、潜在的なインサイダー脅威の懸念を特定するために、技術情報と非技術情報の両方を一元的に統合し分析することにより、悪意のあるインサイダー行為を検知し防止するための管理策を含む。責任者は、プログラムの実装と監督を担当する責任ある個人として、政府部局や政府機関の長によって指名される。集中化された統合および分析ケイパビリティに加えて、インサイダー脅威対策プログラムは、政府部局や政府機関のインサイダー脅威ポリシーおよび実装計画を準備し、国家機密情報を取扱う政府所有のコンピュータを利用する個々の従業員の活動をコンピュータ上で監視し、従業員にインサイダー脅威対策啓発トレーニングを行い、インサイダー脅威分析のために政府部局や政府機関の部署からの情報にアクセスできるようにし、政府部局や政府機関のインサイダー脅威対策態勢についてセルフアセスメントすることを、組織に求めている。

インサイダー脅威対策プログラムは、コンピュータセキュリティインシデント対応チームなど、組織が既に導入しているインシデント対応チームを活用することもできる。ある種の内部関係者による犯罪の前に、不満を持った行動の継続的なパターンや職場仲間や他の同僚との対立を含む、職場での非技術的な行動がしばしば見られるという有力なエビデンスがあり、人事記録はこの取り組みにおいて特に重要である。これらの前兆は、より焦点を絞り、対象を絞った監視措置を行うべく、組織の担当者を導くことができる。ただし、人事記録の使用にはプライバシーに関する重大な懸念を引き起こす可能性がある。なお、政府機関のプライバシー保護責任者との協議を含め、法務チームを参画させることは、監視措置が、適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに従って実施されることを確実にすることができる。

関連管理策：AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PM-16, PS-3, PS-4, PS-5, PS-7, PS-8, SC-7, SC-38, SI-4, PM-14

拡張管理策：なし

参照資料：[EO 13587], [NITP12], [ODNI NITP]

PM-13 セキュリティおよびプライバシー要員

管理策：セキュリティおよびプライバシー要員の育成および向上プログラムを確立する。

詳解：セキュリティおよびプライバシーに関する要員の育成および向上プログラムには、セキュリティおよびプライバシーに関する職務およびタスクを実行するために必要な知識、スキル、力量を規定すること、セキュリティおよびプライバシーの役割と責任を割り当てられた個人を対象とした役割ベースのトレーニングプログラムを開発すること、セキュリティおよびプライバシー関連の職位の在職者および応募者の個人の資格を測定および構築するための基準およびガイドラインを提供することが含まれる。そのような要員の育成および向上プログラムは、セキュリティおよびプライバシーの専門家が現場で昇進し、より大きな責任を負う職位に就くことができるように、セキュリティおよびプライバシーのキャリアパスを含めることもできる。このプログラムは、組織がセキュリティおよびプライバシー関連の職位を資格のある要員で占めることを奨励している。セキュリティおよびプライバシー要員の育成および向上プログラムは、組織のセキュリティ意識向上およびトレーニングプログラムを補完するものであり、組織の運営、資産、個人を保護するために必要な職員の核となるセキュリティおよびプライバシーケイパビリティの開発と制度化に焦点を当てている。

関連管理策：AT-2, AT-3

拡張管理策：なし

参照資料：[OMB A-130], [SP 800-181]

PM-14 テスト、トレーニング、および監視

管理策:

a. 組織のシステムに関連するセキュリティおよびプライバシーのテスト、トレーニング、監視措置を実施する組織の計画を確実にするためのプロセスを以下のように実装する。

   1. 策定し、維持する。

   2. 実施を継続する。

b. 組織のリスクマネジメント戦略およびリスク対応措置に関する組織全体の優先順位との整合性について、テスト、トレーニング、および監視計画をレビューする。

詳解:組織全体のセキュリティおよびプライバシーのテスト、トレーニング、監視のプロセスは、組織がテスト、トレーニング、監視の措置を監督し、それらの措置が調整されていることを確実にするのに役立つ。継続的監視プログラムの重要性の高まり、リスクマネジメント階層の 3 つのレベルにわたる情報セキュリティおよびプライバシーの実装、および共通管理策の広範な使用により、組織は、様々な管理策をサポートする進行中のアセスメントの一部として、定常的に実施するテストおよび監視措置を調整し、統合する。セキュリティおよびプライバシーのトレーニング措置は、個々のシステムと特定の役割に焦点を当てているが、すべての組織部署にわたる調整が必要である。テスト、トレーニング、および監視の計画と措置に、現在の脅威と脆弱性のアセスメント情報を反映する。

関連管理策:AT-2, AT-3, CA-7, CP-4, IR-3, PM-12, SI-4

拡張管理策:なし

参照資料:[OMB A-130], [SP 800-37], [SP 800-39], [SP 800-53A], [SP 800-115], [SP 800-137]

PM-15 セキュリティおよびプライバシーのグループおよび団体

管理策:セキュリティおよびプライバシーのコミュニティ内の選定したグループおよび団体との接点を確立し、制度化する。

a. 組織の職員に対する継続的なセキュリティおよびプライバシー教育およびトレーニングを促進するため。

b. 推奨されるセキュリティおよびプライバシーの実施項目、技法、および技術を最新に維持するため。

c. 脅威、脆弱性、インシデントなど、現在のセキュリティおよびプライバシー情報を共有するため。

詳解:セキュリティおよびプライバシーのグループおよび団体との継続的な接点は、急速に変化する技術と脅威の環境において重要である。グループおよび団体には、SIG(Special Interest Groups)、専門家団体、フォーラム、ニュースグループ、ユーザグループ、および類似組織のセキュリティおよびプライバシー専門家の同業者グループが含まれる。組織は、ミッションおよび事業機能に基づいて、セキュリティおよびプライバシーのグループおよび団体を選定する。組織は、適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインと整合性のある、文脈的洞察、準拠技法、プライバシーの問題など、脅威、脆弱性、インシデント情報を共有する。

関連管理策:SA-11, SI-5

拡張管理策:なし

参照資料:[OMB A-130]

PM-16 脅威認識プログラム

管理策:脅威インテリジェンスのための組織間の情報共有ケイパビリティを含む脅威認識プログラムを実装する。

詳解:絶え間なく変化する敵対者、特に持続的標的型攻撃(APT 攻撃)の巧妙化により、敵対者

が組織のシステムを侵害またはブリーチする可能性が高くなることがある。この懸念に対応するための最良の技法の 1 つは、組織が経験した脅威イベント（すなわち、戦術、技法、および手順）、特定のタイプの脅威に対して効果的であることが判明した軽減策、脅威インテリジェンス（つまり、脅威に関する兆候と警告）を含む、脅威情報を組織が共有することである。脅威情報の共有は、二者間または多者間である。二者間の脅威の共有には、政府機関、営利団体間および政府機関間がある。多者間脅威共有には、脅威共有コンソーシアムに参加する組織が含まれる。脅威情報には、特別な合意と保護が必要な場合や、自由に共有できる場合がある。

関連管理策：IR-4, PM-12

拡張管理策：

(1) 脅威認識プログラム｜脅威インテリジェンスを共有するための自動化された手段

脅威インテリジェンス情報を共有する効果を最大化するために、自動化されたメカニズムを採用する。

詳解：監視の有効性を最大限に高めるには、センサが検索する必要のある観測可能な脅威と兆候を知ることが重要である。組織は、定着したフレームワーク、サービス、および自動化ツールを使用することにより、関連する脅威検知シグネチャを迅速に共有し監視ツールに供給する能力を向上させる。

関連管理策：なし

参照資料：なし

PM-17 外部システム上の管理対象非機密情報の保護

管理策：

a. 外部システムで処理、保存、伝送される管理対象非機密情報の保護に関する要件が、適用される法律、大統領令、指令、規則、ポリシー、および基準に従って、確実に実装されるようにするためのポリシーおよび手順を規定する。

b. [*設定：組織が定める頻度*]でポリシーおよび手順をレビューし、更新する。

詳解：管理対象非機密情報は、管理対象非機密情報の保全と配布の要件にそって、国立公文書記録管理局によって定義され、[32 CFR 2002]で成文化され、特に非連邦政府組織のシステムについては、32 CFR 2002.14h で成文化されている。このポリシーは、その契約プロセスを含め、組織の手順に従って実装される特定の使用法と条件を規定する。

関連管理策：CA-6, PM-10

拡張管理策：なし

参照資料：[32 CFR 2002], [SP 800-171], [SP 800-172], [NARA CUI]

PM-18 プライバシープログラム計画

管理策：

a. 政府機関のプライバシープログラムの概要を提供する組織全体のプライバシープログラム計画を策定し、配布する。

1. プライバシープログラムの構造とプライバシープログラム専用のリソースの記述を含む。
2. プライバシープログラムの要件の概要、およびプライバシープログラムマネジメント管理策と、それらの要件を満たすために導入または計画されている共通管理策の記述を提供する。
3. 政府機関のプライバシー保護責任者の役割、および他のプライバシー担当者とスタッフの役割の特定と割り当て、およびそれらの責任を含む。
4. マネジメントコミットメント、準拠、プライバシープログラムの戦略的目標と目的を記

述する。

5. プライバシーの様々な側面を担当する組織エンティティ間の調整を反映する。
6. 組織の運営（ミッション、事業、イメージ、評判を含む）、組織の資産、個人、他の組織、国家に対して生じるプライバシーリスクに対する責任と説明責任を有する上級職員によって承認されている。

b. ［*設定：組織が定める頻度*］で計画を更新して、連邦政府のプライバシーの法律およびポリシーの変更、ならびに計画の実装中またはプライバシー管理策のアセスメント中に特定された組織の変更および問題に対応する。

詳解：プライバシープログラム計画は、組織のプライバシープログラムの概要を提供する正式な文書であり、プライバシープログラムの構造、プライバシープログラム専用のリソース、政府機関のプライバシー保護責任者および他のプライバシー担当者とスタッフの役割、プライバシープログラムの戦略的目標と目的、および適用されるプライバシー要件を満たし、プライバシーリスクを管理するために導入または計画されているプログラムマネジメント管理策や共通管理策の記述を含む。プライバシープログラム計画は、単一の文書または複数の文書の編集物で表すことができる。

政府機関のプライバシー保護責任者は、組織がプログラムマネジメント管理策、共通管理策、システム固有管理策、ハイブリッド管理策として扱うプライバシー管理策を指定する責任がある。プライバシープログラム計画は、プライバシープログラムマネジメント管理策と共通管理策（パラメータの指定、明示的な設定および選択操作、参照を含む）に関する十分な情報を提供し、計画の意図と計画が意図したとおりに実装された場合に発生するリスクの決定に明確に準拠する管理策の実装を可能にする。

プログラムマネジメント管理策は、通常、組織レベルで実装され、組織のプライバシープログラムをマネジメントするために不可欠である。プログラムマネジメント管理策は、特定の情報システムから独立しているため、プログラムマネジメント管理策は、共通管理策、システム固有管理策、ハイブリッド管理策とは異なる。個々のシステムのプライバシー計画と組織全体のプライバシープログラム計画を組み合わせると、組織内で採用されているプライバシー管理策を完全にカバーできる。

共通管理策は、管理策がシステムの個別のプライバシー計画に含まれていない限り、組織のプライバシープログラム計画の付属書に文書化する。組織全体のプライバシープログラム計画は、プライバシー管理策の記述を含む個別のプライバシー計画を示す。

関連管理策：PM-8, PM-9, PM-19

拡張管理策：なし

参照資料：[PRIVACT], [OMB A-130]

PM-19 プライバシープログラムの責任者の役割

管理策：組織全体のプライバシープログラムを通して、適用可能なプライバシー要件を調整、策定、実装し、プライバシーリスクを管理する権限、ミッション、説明責任、およびリソースを有する政府機関のプライバシー保護責任者を任命する。

詳解：プライバシー責任者は組織の担当者である。連邦政府機関の場合（適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインで定義されているように）、この担当者は政府機関のプライバシー保護責任者に指定されている。組織では、この担当者をプライバシー保護最高責任者と呼ぶこともある。政府機関のプライバシー保護責任者は、データマネジメント委員会（PM-23 を参照）およびデータインテグリティ委員会（PM-24 を参照）の役割も担っている。

関連管理策：PM-18, PM-20, PM-23, PM-24, PM-27

拡張管理策：なし

参照資料: [OMB A-130]

PM-20 プライバシープログラム情報の配布

管理策: 組織のプライバシープログラムに関する情報の中心的な情報ソースとして機能する、組織の主要な公開ウェブサイト上の中心的なウェブページを維持する。

a. 一般の人々が組織のプライバシー措置に関する情報にアクセスでき、政府機関のプライバシー保護責任者と連絡できることを確実にする。

b. 組織のプライバシー実施項目および報告が一般に利用可能であることを確実にする。

c. 一般に公開されている電子メールアドレスや電話回線を利用して、プライバシー実施項目に関してフィードバックを提供したり、プライバシー事務局に直接質問したりできるようにする。

詳解: 連邦政府機関の場合、このウェブページは www.[agency].gov/privacy に配置する。連邦政府機関は、公共プライバシー影響評価、記録システム通知、コンピュータマッチング通知および同意、[PRIVACT]免責および実装規則、プライバシーレポート、プライバシーポリシー、アクセスまたは訂正要求を行う個人向けの指示、質問／苦情受付の電子メールアドレス、ブログ、定期刊行物を含む。

関連管理策: AC-3, PM-19, PT-5, PT-6, PT-7, RA-8

拡張管理策:

(1) プライバシープログラム情報の配布 | ウェブサイト、アプリケーション、およびデジタルサービスのプライバシーポリシー

すべての外部向けウェブサイト、モバイルアプリケーション、およびその他のデジタルサービスのプライバシーポリシーを以下のように作成し、掲載する。

(a) わかりやすい言葉で記載し、理解しやすくナビゲートする方法で編成されている。

(b) 一般の人々が、組織と情報交換するかどうか、どのように情報交換するかについて情報に基づいた決定を下すために、必要とする情報を提供する。

(c) 組織が記述する実施項目に実質的な変更を加えるたびに更新し、最新の改訂日付を一般の人々に知らせるための日時を含める。

詳解: 組織は、すべての外部向けウェブサイト、モバイルアプリケーション、およびその他のデジタルサービスにプライバシーポリシーを掲載する。組織は、ウェブサイト、アプリケーション、またはデジタルサービスへの既知の主要なエントリポイントに、関連するプライバシーポリシーへのリンクを掲載する。さらに、組織は個人情報を取得するウェブページにプライバシーポリシーへのリンクを提供する。組織は、特定の情報を一般の人々に提供することを要求する適用される法律、大統領令、指令、規則、またはポリシーの対象となる場合がある。組織の担当者は、そのような要件について、政府機関のプライバシー保護責任者および法律顧問に相談する。

関連管理策: なし

参照資料: [PRIVACT], [OMB A-130], [OMB M-17-06]

PM-21 開示事項のアカウンティング

管理策:

a. 個人情報の開示について、以下を含む正確なアカウンティングを作成および維持する。

1. 各開示の日付、性質、目的。

2. 開示先の個人または組織の名称および住所、またはその他の連絡先情報。

b. 個人情報が維持される期間または開示してから 5 年のいずれか長い方の期間、開示事項のアカウンティングを保持する。

c. 個人情報が関連する個人の要求に応じ、開示事項のアカウンティングを利用できるよう

にする。

詳解：開示事項のアカウンティングの目的は、個人が本人の個人情報が誰に開示されたかを知ることを可能にすること、訂正されたまたは異議のあった個人情報について開示先に後で通知するための基礎を提供すること、開示の条件に関する組織の準拠についてその後のレビューのための監査証跡を提供することである。連邦政府機関の場合、[PRIVACT]により開示事項のアカウンティング維持を要求されている。政府機関は、この要件に関して政府機関のプライバシー保護責任者および法律顧問に相談し、規定に関する法的例外および OMB ガイダンスに注意することが望ましい。

組織は、開示の記録を維持するために、システムで要求された情報をもとにすべての開示事項の文書リストを作成できる場合は、そのようなシステムを使用できる。組織は、自動化されたメカニズムを使用して、通知や警告を提供する商用サービスなど、個人情報がいつ開示されたかを判断することができる。開示事項のアカウンティングは、組織が情報の開示または配布および配布制限を統制する適用されるプライバシー法およびポリシーへの遵守を検証するのを助けるために使用することもできる。

関連管理策：AC-3, AU-2, PT-2

拡張管理策：なし

参照資料：[PRIVACT], [OMB A-130]

PM-22 個人情報の品質管理

管理策：以下について組織全体のポリシーおよび手順を策定し、文書化する。

a. 情報ライフサイクル全体にわたって、個人情報の的確性、関連性、適時性、正確性についてレビューする。

b. 不正確または古い個人情報を訂正または削除する。

c. 訂正または削除された個人情報の通知を、個人または他の適切な組織に配布する。

d. 訂正または削除要求に対する不利な決定の申し立て。

詳解：個人情報の品質管理には、組織が情報ライフサイクル全体にわたって個人情報の正確性と関連性を確認するために取る手順が含まれる。情報ライフサイクルには、個人情報の作成、収集、利用、処理、保存、維持、配布、開示、および廃棄が含まれる。個人情報の品質管理のための組織のポリシーおよび手順は、組織が維持する不正確または古い個人情報が個人に問題を引き起こす可能性があるため、重要である。組織は、不正確な情報が不利な決定や利益やサービスの拒否につながる可能性がある、または情報の開示により非難をあびせられる可能性がある事業機能に関与する個人情報の品質を考慮する。正しい情報が、ある状況において、情報を維持する組織の便益を上回り個人に問題を引き起こす可能性がある。組織は、そのような情報を削除するためのポリシーおよび手順を作成することを考慮する。

政府機関のプライバシー保護責任者は、実用的な手段とメカニズムが存在し、個人またはその認可された代理人が個人情報の訂正または削除を求めてアクセスできることを確実にする。データを訂正または削除するプロセスを明確に規定し、公開する。組織は、要求の範囲、求められる変更、変更のインパクトに基づいて、データを削除するか訂正するかを決定する裁量を有する。さらに、プロセスには、訂正または削除の要求を拒否する決定についての個人への対応が含まれる。対応には、決定の理由、決定に対する個々の異議を記録する手段、および最初の決定のレビューを要求する手段が含まれる。

組織は、個人情報が訂正または削除された場合、透明性を確保し完了した措置を確認するために、個人または指定された代理人に通知する。データフローと保管が複雑なため、他のエンティティに訂正または削除を通知する必要がある場合がある。通知は、データのエコシステム全体で個人情報の一貫した訂正と削除をサポートする。

関連管理策：PM-23, SI-18

拡張管理策：なし

参照資料: [OMB A-130], [OMB M-19-15], [SP 800-188]

PM-23 データガバナンス会議体

管理策: [*設定:組織が定める責任*]を有する[*設定:組織が定める役割*]で構成されるデータガバナンス会議体を設置する。

詳解: データガバナンス会議体は、組織が一貫したポリシーを持ち、データの有用性とセキュリティおよびプライバシー要件のバランスを取る機能を持っていることを確実にするのに役立つ。データガバナンス会議体は、個人情報を含むデータが、適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイダンスに従って効果的に管理および維持されるように、データガバナンスを促進するポリシー、手順、および基準を規定する。責任には、組織外にデータをリリースするためのアプリケーションのレビューと承認はもちろん、データのモデリング、品質、完全性、および情報ライフサイクル全体にわたる個人情報の匿名化のニーズをサポートするガイドラインの策定と実装、アプリケーションとリリースされたデータのアーカイブ、データリリースの一部として行った仮定が引き続き有効であることを確認するためのリリース後の監視実施を含むことができる。メンバーには、最高情報責任者、政府機関の情報セキュリティ責任者、および政府機関のプライバシー保護責任者が含まれる。連邦政府機関は、[EVIDACT]および[OMB M-19-23]に規定されたポリシーに従って、特定の役割および責任を有するデータガバナンス会議体を設置する必要がある。

関連管理策: AT-2, AT-3, PM-19, PM-22, PM-24, PT-7, SI-4, SI-19

拡張管理策: なし

参照資料: [EVIDACT], [OMB A-130], [OMB M-19-23], [SP 800-188]

PM-24 データインテグリティ委員会

管理策: 以下を行うデータインテグリティ委員会を設置する。

a. マッチングプログラムを実施または参加するための提案をレビューする。

b. 政府機関が参加したすべてのマッチングプログラムの年次レビューを実施する。

詳解: データインテグリティ委員会は、連邦政府機関の長によって指定された責任者の委員会であり、とりわけ、マッチングプログラムを実施または参加するための政府機関の提案をレビューし、機関が参加したすべてのマッチングプログラムの年次レビューを実施する責任を負う。一般的な事実として、マッチングプログラムは、2 つ以上の自動化された[PRIVACT]記録システムまたは自動化された記録システムと、非連邦政府機関(またはその代理人)によって維持される自動化された記録との、コンピュータによる記録の比較である。マッチングプログラムは、連邦政府の福利厚生プログラム、連邦政府職員記録、給与計算記録のいずれかに関係する。少なくとも、データインテグリティ委員会には、機関の監察官、もしあれば政府機関のプライバシー保護責任者を含む。

関連管理策: AC-4, PM-19, PM-23, PT-2, PT-8

拡張管理策: なし

参照資料: [PRIVACT], [OMB A-130], [OMB A-108]

PM-25 テスト、トレーニング、および研究で使用される個人情報の最小化

管理策:

a. 内部テスト、トレーニング、および研究のための個人情報の利用に対処するポリシーおよび手順を策定、文書化、および実装する。

b. 内部テスト、トレーニング、および研究の目的で利用する個人情報の量を限定または最小化する。

c. 個人情報が内部テスト、トレーニング、および研究に必要な場合は、その個人情報の利

用を認可する。

d. [*設定：組織が定める頻度*]で、ポリシーおよび手順をレビューし、更新する。

詳解：個人情報をテスト、研究、トレーニングで使用すると、個人情報の認可されていない開示や悪用のリスクが高まる。組織は、個人情報をテスト、トレーニング、および研究で利用することが、取得した当初の目的と適合していることを確実にするために、政府機関のプライバシー保護責任者および／または法律顧問と相談する。組織は、可能な場合、プレースホルダーデータを使用して、テスト、トレーニング、および研究を実施する際に個人情報が露出するのを防ぐ。

関連管理策：PM-23, PT-3, SA-3, SA-8, SI-12

拡張管理策：なし

参照資料：[OMB A-130]

PM-26 苦情管理

管理策：組織のセキュリティおよびプライバシー実施項目に関する個人からの苦情、懸念事項、または質問を受け付け、対応するための以下のようなプロセスを実装する。

a. 利用しやすく、一般の人々が容易にアクセスできるメカニズム。

b. 苦情を適切に提出するために必要なすべての情報。

c. 受け付けたすべての苦情を[*設定：組織が定める期間*]内にレビューし対処することを確実にするための追跡のメカニズム。

d. [*設定：組織が定める期間*]内に、個人から苦情、懸念事項、または質問を受け付けたことの通知。

e. [*設定：組織が定める期間*]内に、個人からの苦情、懸念事項、または質問への対応。

詳解：個人からの苦情、懸念事項、および質問は、組織への貴重なソースとして役立ち、最終的には運用モデル、技術の利用、データ収集実施項目、および管理策を改善することができる。一般の人々が使用できるメカニズムには、電話ホットライン、電子メール、またはウェブベースのフォームが含まれる。苦情を適切に提出するために必要な情報には、政府機関のプライバシー保護責任者または苦情を受け付けるように指定された他の担当者の連絡先情報が含まれる。プライバシーの苦情には、関連するポリシーやプロセスに従って取り扱われる個人情報が含まれてもよい。

関連管理策：IR-7, IR-9, PM-22, SI-18

拡張管理策：なし

参照資料：[OMB A-130]

PM-27 プライバシー報告

管理策：

a. [*設定：組織が定めるプライバシー報告*]を作成し、以下に配布する。

1. 法令、規則、およびポリシーのプライバシー権限に対する説明責任を実証する[*設定：組織が定める監視機関*]。

2. [*設定：組織が定める担当者*]およびプライバシープログラムの準拠を監視する責任を有するその他の職員。

b. [*設定：組織が定める頻度*]で、プライバシー報告をレビューし、更新する。

詳解：組織は、内部および外部の報告を通じて、組織のプライバシー運用における説明責任と透明性を促進する。報告はまた、組織がプライバシーの準拠要件とプライバシー管理策への対応の進捗状況を判断し、連邦政府全体のパフォーマンスを比較し、脆弱性を発見し、ポリシー

と実装のギャップを特定し、成功のためのモデルを特定するのにも役立つ。連邦政府機関の場合、プライバシー報告には、OMB への政府機関のプライバシー保護責任者の年次報告、9/11 委員会法の実施規則が要求する議会への報告、および組織の内部ポリシーを含む、法律、規則、またはポリシーが要求するその他の公開報告が含まれる。政府機関のプライバシー保護責任者は、組織がすべての該当するプライバシー報告要件を満たしていることを確認するために、必要に応じて法律顧問に相談する。

関連管理策：IR-9, PM-19

拡張管理策：なし

参照資料：[FISMA], [OMB A-130], [OMB A-108]

PM-28 リスクの枠組み

管理策：

a. 以下を特定および文書化する。
   1. リスクアセスメント、リスク対応、およびリスク監視に影響を与える仮定。
   2. リスクアセスメント、リスク対応、およびリスク監視に影響を与える制約。
   3. リスクマネジメントのために組織が考慮する優先順位とトレードオフ。
   4. 組織のリスク許容度。
b. リスクの枠組み措置の所見を[*設定：組織が定める職員*]に配布する。
c. [*設定：組織が定める頻度*]で、リスクの枠組みの考慮事項をレビューし、更新する。

詳解：リスクの枠組みは、組織レベルで実施され、ミッションオーナー、事業オーナー、およびシステムオーナーを含む組織全体の利害関係者と協議して実施される場合に最も効果的である。リスクの枠組みの一部として特定された仮定、制約、リスク許容度、優先順位、およびトレードオフは、リスクマネジメント戦略に影響を与え、同様に、リスクアセスメント、リスク対応、およびリスク監視措置の実施に影響を与える。リスクの枠組みによる結果は、ミッションオーナーと事業オーナー、情報オーナーまたはスチュワード、システムオーナー、認可権限のある担当者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、およびリスクマネジメント担当責任者などの組織の職員と共有する。

関連管理策：CA-7, PM-9, RA-3, RA-7

拡張管理策：なし

参照資料：[OMB A-130], [SP 800-39]

PM-29 リスクマネジメントプログラムの責任者の役割

管理策：

a. 組織の情報セキュリティおよびプライバシーマネジメントプロセスを戦略プロセス、運用プロセス、予算計画プロセスと整合させるために、リスクマネジメント担当責任者を任命する。
b. 組織全体の視点からリスクを可視化および分析し、リスクマネジメントが組織全体で一貫していることを確実にするために、リスク管理者（部署）を設置する。

詳解：リスクマネジメント担当責任者が、組織全体のリスクマネジメント措置においてリスク管理者（部署）を指揮する。

関連管理策：PM-2, PM-19

拡張管理策：なし

参照資料：[SP 800-37], [SP 800-181]

PM-30 サプライチェーンのリスクマネジメント戦略

管理策:

a. システム、システムコンポーネント、およびシステムサービスの開発、取得、保守、および廃棄に関連するサプライチェーンのリスクを管理するための組織全体の戦略を策定する。

b. 組織全体で一貫してサプライチェーンのリスクマネジメント戦略を実装する。

c. [*設定:組織が定める頻度*]または必要に応じて、組織の変更に対処するために、サプライチェーンのリスクマネジメント戦略をレビューし、更新する。

詳解:組織全体のサプライチェーンのリスクマネジメント戦略には、サプライチェーンのリスク選好度と許容度の明確な表現、適用可能なサプライチェーンのリスク軽減戦略または管理策、サプライチェーンのリスクを一貫して評価および監視するプロセス、サプライチェーンのリスクマネジメント戦略を実装し伝達するためのアプローチ、および関連する役割と責任を含む。サプライチェーンのリスクマネジメントには、システム、システムコンポーネント、およびシステムサービスの開発、取得、保守、および廃棄に関連するセキュリティおよびプライバシーリスクの考慮が含まれる。サプライチェーンのリスクマネジメント戦略は、組織の包括的なリスクマネジメント戦略に組み込むことができ、サプライチェーンのポリシー—とシステムレベルのサプライチェーンのリスクマネジメント計画を導き、情報を与えることができる。さらに、リスク管理部署を利用することで、サプライチェーンのリスクマネジメント戦略を組織全体に一貫して適用することを促進することができる。サプライチェーンのリスクマネジメント戦略は、組織レベルおよびミッション／事業レベルで実装され、サプライチェーンのリスクマネジメント計画(SR-2 を参照)はシステムレベルで実装される。

関連管理策:CM-10, PM-9, SR-1, SR-2, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, SR-11

拡張管理策:

(1) サプライチェーンのリスクマネジメント戦略 | 重要なまたはミッションに必須のアイテムのサプライヤ

重要なまたはミッションに必須の技術、製品、およびサービスのサプライヤを特定し、優先順位を付け、アセスメントする。

詳解:重要なまたはミッションに必須の技術、製品、およびサービスのサプライヤの特定と優先順位付けは、組織のミッション／事業の成功にとって最重要である。サプライヤのアセスメントは、サプライヤのレビュー(SR-6 を参照)およびサプライチェーンのリスクアセスメントプロセス(RA-3(1)を参照)を使用して実施する。サプライチェーンのリスク分析は、組織が追加のサプライチェーンのリスク軽減策が必要なシステムまたはコンポーネントを特定するのに役立つ。

関連管理策:RA-3, SR-6

参照資料:[PRIVACT], [FASC18], [EO 13873], [41 CFR 201], [OMB A-130], [OMB M-17-06] [CNSSD 505], [ISO 27036], [ISO 20243], [SP 800-161], [IR 8272]

PM-31 継続的監視戦略

管理策:組織全体の継続的監視戦略を策定し、以下を含む継続的監視プログラムを実装する。

a. 監視対象の組織全体の[*設定:組織が定める指標*]を規定すること。

b. 監視のための[*設定:組織が定める頻度*]、および管理策の有効性アセスメントのための[*設定:組織が定める頻度*]を規定すること。

c. 継続的監視戦略に従って、組織が定める指標について継続進行中の監視を行うこと。

d. 管理策のアセスメントと監視によって生成される情報の相関および分析。

e. 管理策のアセスメントと監視情報の分析結果に対応するための対応措置。

f. [*設定：組織が定める頻度*]で、組織のシステムのセキュリティおよびプライバシー状態を[*設定：組織が定める職員または役割*]に報告すること。

詳解：組織レベルでの継続的監視は、組織全体のセキュリティおよびプライバシー態勢の継続進行中の認識を促進し、組織のリスクマネジメントに関する意思決定をサポートする。「継続的」および「継続進行中」という用語は、リスクベースの意思決定をサポートするために、組織が十分な頻度でその管理策とリスクをアセスメントすることおよび監視することを意味する。異なるタイプの管理策は、異なる監視頻度を求められる場合がある。継続的監視の結果は、組織によるリスク対応措置を導き、情報を与える。継続的監視プログラムにより、組織は、ミッションと事業ニーズ、脅威、脆弱性、および技術が変化する中で非常に動的な運用環境において、システム管理策と共通管理策の認可を維持することができる。報告書およびダッシュボードを介してセキュリティおよびプライバシー関連の情報に継続的にアクセスできることにより、組織の担当者は、継続進行中の認可決定を含む、効果的でタイムリーな情報に基づいたリスクマネジメントの決定を行うケイパビリティを得られる。セキュリティおよびプライバシーのリスクマネジメントをさらに促進するために、組織は、組織が定める監視指標を、リスクマネジメント戦略で定める組織のリスク許容度と整合させることを考慮する。監視のニーズを含む監視要件は、以下のような他の管理策および拡張管理策を参照してもよい。AC-2g, AC-2(7), AC-2(12)(a), AC-2(7)(b), AC-2(7)(c), AC-17(1), AT-4a, AU-13, AU-13(1), AU-13(2), CA-7, CM-3f, CM-6d, CM-11c, IR-5, MA-2b, MA-3a, MA-4a, PE-3d, PE-6, PE-14b, PE-16, PE-20, PM-6, PM-23, PS-7e, SA-9c, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b, SI-4。

関連管理策：AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CA-7, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PS-7, PT-7, RA-3, RA-5, RA-7, SA-9, SA-11, SC-5, SC-7, SC-18, SC-38, SC-43, SI-3, SI-4, SI-12, SR-2, SR-4

参照資料：[SP 800-37], [SP 800-39], [SP 800-137], [SP 800-137A]

PM-32 目的

管理策：情報リソースが意図された目的と一致して使用されていることを確実にするために、ミッションに必須のサービスまたは機能をサポートする[*設定：組織が定めるシステムまたはシステムコンポーネント*]を分析する。

詳解：システムは、特定のミッションまたは事業機能をサポートするように設計されている。しかしながら、時間の経過とともに、システムおよびシステムコンポーネントは、意図されたミッションまたは事業機能の範囲外のサービスおよび機能をサポートするために使用される可能性がある。その結果、情報リソースが意図しない環境や用途にさらされ、脅威にさらされる可能性が大幅に高まる。そうすることで、システムは侵害に対してより脆弱になり、最終的にはシステムが意図したサービスや機能にインパクトを与える可能性がある。これは、ミッションに必須のサービスと機能に特にインパクトを与える。リソースの使用状況を分析することで、組織はそのような潜在的な露出を特定できる。

関連管理策：CA-7, PL-2, RA-3, RA-9

拡張管理策：なし

参照資料：[SP 800-160-1], [SP 800-160-2]

3.14 職員のセキュリティ

職員のセキュリティの要約表へのクイックリンク

PS-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。

1. 以下の[*選択(1 つ以上):組織レベル;ミッション/事業プロセスレベル;システムレベル*]の職員のセキュリティのポリシー。

(a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、および準拠に対処する。

(b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに適合している。

2. 職員のセキュリティのポリシーと関連する職員のセキュリティの管理策の実装を促進するための手順。

b. 職員のセキュリティのポリシーと手順の策定、文書化、および配布することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行の職員のセキュリティをレビューし、更新する。

1. ポリシーについて[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

2. 手順について[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

詳解:職員のセキュリティのポリシーと手順は、システムおよび組織で実装される PS ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に寄与する。したがって、セキュリティおよびプライバシープログラムが職員のセキュリティのポリシーと手順の策定と連携していることが重要である。セキュリティおよびプライバシープログラムのポリシーと手順を組織レベルで確立することは望ましく、一般的には、ミッションまたはシステム固有のポリシーと手順を不要にすることができる。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映する複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムに対して規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述し、手順の対象である個人または役割向けとすることができる。手順は、システムのセキュリティおよびプライバシー計画の中に、または 1 つ以上の別の文書に文書化することもできる。職員のセキュリティのポリシーと手順の更新を引き起こす可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれる。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策:PM-9, PS-8, SI-12

拡張管理策:なし

参照資料:[SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100]

PS-2 職位のリスク指定

管理策:

a. すべての組織の職位にリスク指定を割り当てる。

b. それらの職位を担当する個人のスクリーニング基準を規定する。

c. [*設定:組織が定める頻度*]で職位のリスク指定をレビューし、更新する。

詳解:職位のリスク指定は、人事管理局(OPM:Office of Personnel Management)のポリシーとガイダンスを反映する。適切な職位の指定は、効果的で一貫した適合性および職員のセキュリティプログラムの基礎となる。連邦政府規則による職位指定システム(PDS:Position Designation System)は、職位在職者の不正行為によるサービスの有効性や完全性への潜在的な損害の程度を判断するために、その職位の職務や責任をアセスメントし、その職位のリスクレベルを規定する。PDS のアセスメントでは、その職位の職務と責任が、その職位の在職者が国家安全保障に重大な悪影響をもたらす可能性があるかどうか、およびその潜在的影響の程度を決定し、職位の機微性レベルを規定する。アセスメントの結果により、職位に対してどのレベルの調査が実施されるかが決まる。リスク指定は、個人が組織の情報および情報システムにアクセスする場合に受ける認可のタイプをガイドし、情報を提供することができる。職位のスクリーニング基準には、明示的な情報セキュリティの役割任命要件が含まれる。連邦規則集 Title 5 の Parts 1400 および 731 は、組織がそれらの職位の職務と責任に見合った職位の機微性と職位のリスク指定について、関連する対象職位を評価するための要件を定めている。

関連管理策:AC-5, AT-3, PE-2, PE-3, PL-2, PS-3, PS-6, SA-5, SA-21, SI-12

拡張管理策:なし

参照資料:[5 CFR 731], [SP 800-181]

PS-3 職員のスクリーニング

管理策:

a. システムへのアクセスを認可する前に個人をスクリーニングする。

b. [*設定:組織が定める再スクリーニングを要求する条件、および再スクリーニングの頻度が示されている場合は、その頻度*]で、個人を再スクリーニングする。

詳解:職員のスクリーニングおよび再スクリーニング措置は、適用される法律、大統領令、指令、規則、ポリシー、基準、ガイドライン、および割り当てられた職位のリスク指定のために規定された特定の基準を反映する。職員のスクリーニングの例としては、経歴調査や政府機関チェックがある。組織は、システムにより処理、保存、または伝送される情報タイプに基づいて、システムにアクセスする職員に対して、異なる再スクリーニング条件および頻度を定めてもよい。

関連管理策:AC-2, IA-4, MA-5, PE-2, PM-12, PS-2, PS-6, PS-7, SA-21

拡張管理策:

(1) 職員のスクリーニング | 国家機密情報

国家機密情報を処理、保存、または伝送するシステムにアクセスする個人が、クリアになり、システム上でアクセスできる情報の最高の機密性区分機密レベルについて教え込まれていることを検証する。

詳解:国家機密情報は、連邦政府が処理、保存、または伝送する最高の機微情報である。そのような情報にアクセスする前に、個人が必要なセキュリティクリアランスとシステムアクセス認可を有していることが不可欠である。アクセス認可は、システムのアクセス制御(AC-3 を参照)およびフロー制御(AC-4 を参照)により実施される。

関連管理策:AC-3, AC-4

(2) 職員のスクリーニング | 正式な教化

正式な教化を必要とする国家機密情報を処理、保存、または伝送するシステムにアク

セスする個人が、システム上でアクセスできるすべての関連情報について正式に教化されていることを検証する。

詳解：正式な教化を必要とする国家機密情報のタイプには、連邦政府高度機密情報アクセスプログラム（SAP）、秘密データ（RD）、機微区分情報（SCI）などがある。

関連管理策：AC-3, AC-4

(3) 職員のスクリーニング｜特別な保護手段を必要とする情報

特別な保護を必要とする情報を処理、保存、または伝送するシステムにアクセスする個人が、以下であることを検証する。

(a) 割り当てられた政府の公務を実施するのに妥当なアクセス認可を有する。

(b) [*設定：組織が定める追加の職員スクリーニング基準*]を満たす。

詳解：特別な保護を必要とする組織の情報には、管理対象非機密情報が含まれる。職員のセキュリティ基準には、職位の機微性経歴スクリーニング要件が含まれる。

関連管理策：なし

(4) 職員のスクリーニング｜市民権要件

[*設定：組織が定める情報タイプ*]を処理、保存、または伝送するシステムにアクセスする個人が、[*設定：組織が定める市民権要件*]を満たしていることを検証する。

詳解：なし

関連管理策：なし

参照資料：[EO 13526], [EO 13587], [FIPS 199], [FIPS 201-2], [SP 800-60-1], [SP 800-60-2], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4]

PS-4 職員の雇用終了

管理策：個人の雇用終了時に、以下を行う。

a. [*設定：組織が定める期間*]内にシステムへのアクセスを無効にする。

b. その個人に関連するオーセンティケータおよびクレデンシャルをすべて終結または取り消す。

c. [*設定：組織が定める情報セキュリティトピック*]に関するディスカッションを含む、退職者面接を実施する。

d. セキュリティ関連の組織のシステム関連の所有物をすべて回収する。

e. 雇用が終了した個人が以前管理していた組織の情報やシステムへのアクセスを保持する。

詳解：システム所有物には、ハードウェア認証トークン、システム管理技術マニュアル、鍵、身分証明書、および建物の入館証が含まれる。退職者面接では、雇用が終了した個人が元従業者であることによって課されるセキュリティ上の制約を理解し、システム関連の所有物の適切な説明責任が果たせることを確実にする。退職者面接でのセキュリティトピックには、秘密保持契約および将来の雇用に関する潜在的な制約を個人に想起させることが含まれる。監督者の不在、病気、または就業放棄に関連する場合を含め、一部の個人にとって、退職者面接は必ずしも可能とは限らない。退職者面接は、セキュリティクリアランスを有する個人にとって重要である。正当な理由により雇用が終了した個人に対して、雇用終了措置のタイムリーな実施は不可欠である。ある状況では、組織は、雇用終了を個人に通知する前に、雇用終了される個人のシステムアカウントを無効にすることを考慮する。

関連管理策：AC-2, IA-4, PE-2, PM-12, PS-6, PS-7

拡張管理策：

(1) 職員の雇用終了｜雇用終了後要件

(a) 組織の情報の保護に関して適用される法的拘束力のある雇用終了後要件を雇用が終了した個人に通知する。

(b) 雇用が終了した個人に、組織の雇用終了プロセスの一環として、雇用終了後要件の承諾書に署名することを要求する。

詳解:組織は、雇用が終了した個人の雇用終了後要件に関する事項について、法律顧問に相談する。

関連管理策:なし

(2) 職員の雇用終了 | 自動化された措置

[選択(1つ以上)]:個人の雇用終了措置を[設定:組織が定める職員または役割]に通知する;システムリソースへのアクセスを無効にする]ために、[設定:組織が定める自動化されたメカニズム]を利用する。

詳解:多くの従業員を抱える組織では、雇用終了措置について知る必要のあるすべての職員が適切な通知を受け取るわけではなく、そのような通知を受け取る場合でも、タイムリーに行われない場合がある。自動化されたメカニズムを使用して、個人が雇用終了した場合、組織の職員または役割に自動警告または通知を送信できる。そのような自動警告または通知は、電話、電子メール、テキストメッセージ、またはウェブサイトを含む様々な方法で伝達することができる。自動化されたメカニズムを採用して、従業員の雇用終了後にシステムリソースへのアクセスを迅速かつ完全に無効にすることもできる。

関連管理策:なし

参照資料:なし

PS-5 職員の異動

管理策:

a. 個人が組織内の他の職位に再配置または異動する場合、システムおよび施設への現在の論理的および物理的アクセス認可に関する継続的な運用上の必要性をレビューし、確認する。

b. [*設定:組織が定める正式な異動措置後の期間*]内に[*設定:組織が定める異動または再配置措置*]を開始する。

c. 再配置または異動による運用上の必要性の変化に対応するために、必要に応じてアクセス認可を変更する。

d. [*設定:組織が定める期間*]内に[*設定:組織が定める職員または役割*]に通知する。

詳解:職員の異動の管理策は、個人の再配置または異動が恒久的である場合、またはその措置が保証されるほど長期である場合に適用する。組織は、恒久的であるか延長されたものであるかにかかわらず、再配置または異動のタイプに適した措置を定める。組織内の他の職位への職員の異動または再配置で必要となる可能性のある措置には、以下が含まれる。鍵、身分証明書、建物の入館証について、古いものを返却し、新しいものを発行する。システムアカウントを閉鎖し、新しいアカウントを確立する。システムアクセス認可(すなわち、特権)を変更する。個人が以前の作業場所および以前のシステムアカウントでアクセスした職務上の記録へのアクセスを提供する。

関連管理策:AC-2, IA-4, PE-2, PM-12, PS-4, PS-7

拡張管理策:なし

参照資料:なし

PS-6 アクセス合意書

管理策:

a. 組織のシステムについてのアクセス合意書を作成し、文書化する。

b. [*設定:組織が定める頻度*]でアクセス合意書をレビューし、更新する。

c. 組織の情報およびシステムへのアクセスを必要とする個人が、以下を実施することを検証する。

1. アクセスを許可される前に、適切なアクセス合意書に署名する。

2. アクセス合意書が更新された場合、または[*設定:組織が定める頻度*]で、組織のシステムへのアクセスを維持するために、アクセス合意書に再署名する。

詳解:アクセス合意書には、秘密保持合意書、使用許諾合意書、行動規則、および利益相反合意書が含まれる。署名されたアクセス合意書には、アクセスが認可された組織のシステムに関連する制約事項を読み、理解し、遵守することに個人が同意したことの承諾が含まれる。組織のポリシーで特に禁止されていない限り、組織は電子署名をアクセス合意書の承諾に使用できる。

関連管理策:AC-17, PE-2, PL-4, PS-2, PS-3, PS-6, PS-7, PS-8, SA-21, SI-12

拡張管理策:

(1) アクセス合意書 | 特別な保護が必要な情報

[撤回:PS-3 に組み込まれた]

(2) アクセス合意書 | 特別な保護を必要とする国家機密情報

特別な保護を必要とする国家機密情報へのアクセスが、以下の個人にのみ許可されていることを検証する。

(a) 割り当てられた政府の公務を実施するのに妥当なアクセス認可を有する。

(b) 関連する職員のセキュリティ基準を満たす。

(c) 秘密保持合意書を読み、理解し、署名している。

詳解:特別な保護を必要とする国家機密情報には、付帯情報、連邦政府高度機密情報アクセスプログラム(SAP)、機微区分情報(SCI)が含まれる。職員のセキュリティ基準は、適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインを反映する。

関連管理策:なし

(3) アクセス合意書 | 雇用終了後要件

(a) 組織の情報の保護に関する適用可能な法的拘束力のある雇用終了後要件を個人に通知する。

(b) 対象となる情報への最初のアクセスを認可する一環として、該当する場合、個人にこれらの要件の承諾書に署名することを要求する。

詳解:組織は、雇用が終了した個人の雇用終了後要件に関する事項について、法律顧問に相談する。

関連管理策:PS-4

参照資料:なし

PS-7 外部職員のセキュリティ

管理策:

a. 外部プロバイダに対する、セキュリティの役割と責任を含む、職員のセキュリティ要件を規定する。

b. 外部プロバイダに、組織によって規定された職員のセキュリティポリシーおよび手順に準拠することを要求する。

c. 職員のセキュリティ要件を文書化する。

d. 組織のクレデンシャルおよび/またはバッジを所持している外部職員、または[*設定:組織が定める期間*]内にシステム特権を有する外部職員の異動または雇用の終了につ

いて、[*設定：組織が定める職員または役割*]に通知することを、外部プロバイダに要求する。

e. 職員のセキュリティ要件に対するプロバイダの準拠を監視する。

詳解：外部プロバイダとは、システムを運用または取得している組織以外の組織を指す。外部プロバイダには、システム開発、IT サービス、テストまたはアセスメントサービス、外部委託アプリケーション、およびネットワーク／セキュリティ管理を提供するサービス機関、請負事業者、および他の組織が含まれる。組織は、取得関連文書に職員のセキュリティ要件を明示的に含める。外部プロバイダは、組織が発行したクレデンシャル、バッジ、またはシステム特権を使用して、組織の施設で働く職員を有している場合がある。外部職員の変更の通知により、特権とクレデンシャルの適切な終結を確実にする。組織は、異動または雇用終了した個人に関連する機能、役割、およびクレデンシャルまたは特権の性質を含むセキュリティ関連の特性により、報告価値があるとみなされる異動者および雇用終了者を定める。

関連管理策：AT-2, AT-3, MA-5, PE-3, PS-2, PS-3, PS-4, PS-5, PS-6, SA-5, SA-9, SA-21

拡張管理策：なし

参照資料：[SP 800-35]、[SP 800-63-3]

PS-8 職員の制裁

管理策：

a. 規定された情報セキュリティおよびプライバシーのポリシーおよび手順を遵守しない個人に対して、正式な制裁プロセスを採用する。

b. 正式な従業者制裁プロセスが開始された場合、[*設定：組織が定める期間*]内に、制裁対象の個人および制裁の理由を特定し、[*設定：組織が定める職員または役割*]に通知する。

詳解：組織の制裁には、適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインを反映する。制裁プロセスは、アクセス合意書に記述されており、組織の一般的な人事ポリシーの一部として含めることも、および／またはセキュリティやプライバシーポリシーで指定することもできる。組織は、従業者の制裁の問題について法律顧問に相談する。

関連管理策：すべての XX-1 管理策, PL-4, PM-12, PS-6, PT-1

拡張管理策：なし

参照資料：なし

PS-9 職位記述

管理策：セキュリティおよびプライバシーの役割および責任を組織の職位記述に組み入れる。

詳解：個人の組織の職位記述に、セキュリティおよびプライバシーの役割を明記することで、役割に関連するセキュリティまたはプライバシーの責任と、役割に基づくセキュリティおよびプライバシーのトレーニング要件を明解に理解しやすくする。

関連管理策：なし

拡張管理策：なし

参照資料：[SP 800-181]

3.15 個人情報の取扱いおよび透明性

個人情報の取扱いおよび透明性の要約表へのクイックリンク

PT-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。

1. 以下の[*選択(1 つ以上):組織レベル;ミッション/事業プロセスレベル;システムレベル*]の個人情報の取扱いおよび透明性のポリシー。

(a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、および準拠に対処する。

(b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに適合している。

2. 個人情報の取扱いおよび透明性のポリシーと関連する個人情報の取扱いおよび透明性の管理策の実装を促進するための手順。

b. 個人情報の取扱いおよび透明性のポリシーと手順の策定、文書化、および配布することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行の個人情報の取扱いおよび透明性を、レビューし、更新する。

1. ポリシーについて[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

2. 手順について[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

詳解:個人情報の取扱いおよび透明性のポリシーと手順は、システムおよび組織で実装されるPT ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に寄与する。したがって、セキュリティおよびプライバシープログラムが個人情報の取扱いおよび透明性のポリシーと手順の策定と連携していることが重要である。セキュリティおよびプライバシープログラムのポリシーと手順を組織レベルで確立することは望ましく、一般的には、ミッションまたはシステム固有のポリシーと手順を不要にすることができる。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映する複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムに対して規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述し、手順の対象である個人または役割向けとすることができる。手順は、システムのセキュリティおよびプライバシー計画の中に、または 1 つ以上の別の文書に文書化することもできる。個人情報の取扱いおよび透明性のポリシーと手順の更新を引き起こす可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれる。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策:なし

拡張管理策:なし

参照資料:[OMB A-130]

PT-2 個人情報を取扱う職権

管理策:

a. 個人情報の[*設定:組織が定める取扱い*]の許可を与える[*設定:組織が定める職権*]を決定し、文書化する。

b. 個人情報の[*設定:組織が定める取扱い*]を、認可されたもののみに制限する。

詳解:個人情報の取扱いとは、情報のライフサイクル全体にわたり、個人情報に関して情報システムまたは組織が実施する一つのオペレーションまたは一連のオペレーションである。取扱いには、作成、収集、利用、処理、保存、維持、配布、開示、および廃棄が含まれるが、これらに限定されない。取扱いのオペレーションには、ロギング、生成、変換のほか、データマイニングなどの分析技法も含まれる。

組織は、組織の職権を規定し、それにより個人情報のあるタイプの取扱いを限定する、または取扱いに関連するその他の要件を規定する法律、大統領令、指令、規則、ポリシーの対象となる場合がある。組織の職員は、特に組織が複数の管轄または職権の対象である場合は、そのような職権について政府機関のプライバシー保護責任者および法律顧問に相談する。法務当局により取扱いが決定されていない組織の場合、組織のポリシーと決定が、個人情報の取扱い方法を決定する。個人情報の取扱いが法的に許容される場合があるが、それでもプライバシーリスクが生じる可能性がある。プライバシーリスクアセスメントは、個人情報の認可された取扱いに関連するプライバシーリスクを特定し、そのようなリスクを管理するソリューションをサポートすることができる。

組織は、この職権を文書化する方法を決定するために、適用される要件と組織のポリシーを考慮する。連邦政府機関の場合、個人情報を取扱う職権は、プライバシーポリシーと通知、記録システムの通知、プライバシー影響評価、[PRIVACT]ステートメント、コンピュータマッチング合意と通知、契約、情報共有の合意、覚書、およびその他の文書で、文書化される。

組織は、個人情報の認可された取扱いにおける組織の職員のトレーニング、および個人情報の組織の利用に関する監視と監査を含め、個人情報を認可された目的でのみ取扱うことを確実にするための措置を講じる。

関連管理策:AC-2, AC-3, CM-13, IR-9, PM-9, PM-24, PT-1, PT-3, PT-5, PT-6, RA-3, RA-8, SI-12, SI-18

拡張管理策:

(1) 個人情報を取扱う職権 | データタグ付け

[*設定:組織が定める認可された取扱い*]を含むデータタグを、[*設定:組織が定める個人情報の要素*]に付加する。

詳解:データタグは、システム全体で個人情報の関連要素とともに認可された取扱いのタイプを伝えることにより、認可された取扱いの追跡と実施をサポートする。データタグは、自動化されたツールの使用をサポートしてもよい。

関連管理策:AC-16, CA-6, CM-12, PM-5, PM-22, PT-4, SC-16, SC-43, SI-10, SI-15, SI-19

(2) 個人情報を取扱う職権 | 自動化

[*設定:組織が定める自動化されたメカニズム*]を使用して、個人情報の認可された取扱いの実施を管理する。

詳解:自動化されたメカニズムは、認可された取扱いのみが行われているという検証を強化する。

関連管理策:CA-6, CM-12, PM-5, PM-22, PT-4, SC-16, SC-43, SI-10, SI-15, SI-19

参照資料:[PRIVACT], [OMB A-130], [IR 8112]

PT-3 個人情報の取扱い目的

管理策:

a. 個人情報を取扱うための[*設定:組織が定める目的*]を特定し、文書化する。

b. 組織の公開プライバシー通知およびポリシーに目的を記述する。

c. 個人情報の[*設定:組織が定める取扱い*]を、特定された目的と矛盾していない情報のみに制限する。

d. 個人情報の取扱いにおける変更を監視し、変更が[*設定:組織が定める要件*]に従って行われることを確実にするために[*設定:組織が定めるメカニズム*]を実装する。

詳解:取扱いの目的を特定して文書化することで、組織が、個人情報が取扱われる理由を理解するための基礎が得られる。「取扱い」という用語には、作成、収集、利用、処理、保存、維持、配布、開示、および廃棄を含む、情報ライフサイクルのすべての段階が含まれる。取扱いの目的を特定して文書化することは、システムのオーナーと運用者、およびシステムによって情報が取扱われる個人が、情報がどのように取り扱われるかを理解できるようにするための必要条件である。これにより、個人は、情報システムや組織との関わりについて情報に基づいた意思決定を行い、プライバシーの権利を管理することができる。いったん具体的な取扱い目的を特定すると、その目的を、組織のプライバシーに関する通知、ポリシー、および、プライバシー影響評価、記録システムに関する通知、[PRIVACT]ステートメント、コンピュータマッチングに関する通知、およびその他適用される官報通知などの該当するプライバシーに関する準拠文書に記載する。

組織は、個人情報の認可された取扱いにおける組織の職員のトレーニング、および個人情報の組織の利用に関する監視と監査を含め、個人情報を認可された目的でのみ取扱うことを確実にするための措置を講じる。

組織は、個人情報の取扱いの変更を監視する。該当する場合、組織の職員は、個人情報の取扱いの変更にともなう新たな目的が、情報を取得した際の目的と矛盾がないことを確実にするために、または、新たな目的が矛盾する場合、新たな取扱いを可能とするために定めた要件に従ってメカニズムを実装することを確実にするために、政府機関のプライバシー保護責任者および法律顧問に相談する。メカニズムには、個人からの同意の取得、プライバシーポリシーの改訂、または個人情報の取扱い目的の変更から生じるプライバシーリスクをマネジメントするための他の措置を含めてもよい。

関連管理策:AC-2, AC-3, AT-3, CM-13, IR-9, PM-9, PM-25, PT-2, PT-5, PT-6, PT-7, RA-8, SC-43, SI-12, SI-18

拡張管理策:

(1) 個人情報の取扱い目的 | データタグ付け

[*設定:組織が定める取扱い目的*]を含むデータタグを[*設定:組織が定める個人情報の要素*]に付加する。

詳解:データタグは、システム全体で個人情報の関連要素とともにその取扱い目的を伝えることにより、取扱い目的の追跡をサポートする。個人情報がシステムを通過する際、個人情報とともにデータタグで取扱い目的を伝えることにより、システムオーナーまたはオペレータは、取扱いの変更が特定され文書化された目的と矛盾がないかどうかを特定することができる。データタグは、自動化されたツールの使用もサポートする場合がある。

関連管理策:CA-6, CM-12, PM-5, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19

(2) 個人情報の取扱い目的 | 自動化

[*設定:組織が定める自動化されたメカニズム*]を使用して、個人情報の取扱い目的を追跡する。

詳解:自動化されたメカニズムは、取扱い目的の追跡を強化する。

関連管理策:CA-6, CM-12, PM-5, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19

参照資料:[PRIVACT], [OMB A-130], [IR 8112]

PT-4 同意

管理策：個人が情報に基づいた意思決定を容易にするように、個人情報の取得前に、個人情報の取扱いに個人が同意するための[*設定：組織が定めるツールまたはメカニズム*]を実装する。

詳解：同意により、個人は自分の情報の取扱いに関する意思決定に参加し、個人情報の取扱いから生じるリスクの一部を組織から個人に移すことができる。適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインにより、同意が要求される場合がある。それ以外の場合、同意を管理策として選択する場合、組織は、個人がその認可から生じるプライバシーリスクを理解して受け入れることが合理的に期待できるかどうかを考慮する。組織は、他の管理策が、単独または同意と組み合わせて、プライバシーリスクをより効果的に軽減できるかどうかを考慮する。組織はまた、システムまたは組織によって実行される取扱いに関して、個人の理解または行動に影響を与える可能性のある人口統計学的属性要素または文脈上の要素を考慮する。組織は、個人から同意を求める場合、同意のタイプ（オプトイン、オプトアウトなど）、個人を適切に認証して身元を証明する方法、電子的手段を通じて同意を得る方法など、同意を取得するための適切なメカニズムを考慮する。さらに、組織は、必要に応じて、個人が同意を取消すメカニズムを提供することを考慮する。最後に、組織は、わかりやすい言葉の使用や専門用語の回避など、同意を提供する際に受け入れるリスクを個人が理解できるように、ユーザビリティの要因を考慮する。

関連管理策：AC-16, PT-2, PT-5

拡張管理策：

(1) 同意 | テーラリングされた同意

個人情報の選択された要素に対する取扱い権限を個人がテーラリングできるように、[*設定：組織が定めるメカニズム*]を提供する。

詳解：製品またはサービスの基本的な機能のために一部の取扱いが必要になる場合があるが、他の取扱いは必要ない場合がある。これらの状況では、組織は、個人情報の要素をどのように取り扱うかを個人が選択できるようにする。よりテーラリングされた同意は、プライバシーのリスクを軽減し、個人の満足度を高め、製品やサービスの放棄などの有害な行動を回避するのに役立つ。

関連管理策：PT-2

(2) 同意 | ジャストインタイムの同意

[*設定：組織が定める個人情報の取扱い*]と組み合わせて、[*設定：組織が定める同意のメカニズム*]を[*設定：組織が定める頻度*]で個人に提示する。

詳解：ジャストインタイムの同意により、個人は、個人情報が、その時点で、または特定のタイプのデータ取扱いとともに、取り扱われる方法での参画が個人にとって最も有用である場合、参画を可能とする。個人情報がどのように取り扱われるかについての個人の想定は、個人が最後に同意してから時間が経過した場合、または取扱いのタイプによってプライバシー上の重大なリスクが生じる場合、的確でないか信頼できない可能性がある。組織は裁量により、ジャストインタイムの同意をいつ使用するかを決定し、個人のプライバシーへの関心や懸念についてさらに学ぶために、人口統計学的属性、フォーカスグループ、または調査に関する補足情報を利用してもよい。

関連管理策：PT-2

(3) 同意 | 取消し

個人が自分の個人情報の取扱いへの同意を取消すための[*設定：組織が定めるツールまたはメカニズム*]を実装する。

詳解：同意の取消しにより、個人は、状況が変化したときに最初の同意の決定を管理することができる。組織は、使いやすい取消しケイパビリティを有効にする際に、ユーザビリティの要因を考慮する。

関連管理策：PT-2

参照資料: [PRIVACT], [OMB A-130], [SP 800-63-3]

PT-5 プライバシー通知

管理策: 個人情報の取扱いについて、以下のように個人に通知を提供する。

a. 個人が最初に組織とやり取りする際に入手可能であり、その後[*設定: 組織が定める頻度*]で入手可能である。

b. 明確かつ理解しやすく、個人情報の取扱いに関する情報をわかりやすい言葉で表現している。

c. 個人情報の取扱いを認可する職権を特定する。

d. 個人情報を取扱う目的を特定する。

e. [*設定: 組織が定める情報*]を含める。

詳解: プライバシー通知は、個人情報がシステムまたは組織によってどのように取扱われているかを個人に知らせるのに役立つ。組織はプライバシー通知を使用して、個人情報がどのように、どのような職権の下で、どのような目的で取扱われるか、およびその取扱いに関して個人が持つ可能性のある選択肢や、情報を共有する他の当事者についての他の情報を個人に情報提供する。法律、大統領令、指令、規則、またはポリシーでは、プライバシーに関する通知に特定の要素を含めるか、特定の形式で提供する必要がある場合がある。連邦政府機関の職員は、プライバシー通知を提供する時期と場所、およびプライバシー通知に含める要素と必要な形式について、政府機関のプライバシー保護責任者および法律顧問に相談する。法律または政府全体のポリシーがプライバシー通知を必要としない状況で、組織のポリシーおよび決定が、プライバシー通知を要求する場合があり、プライバシー通知に含める要素のソースとして役立つ場合がある。

プライバシーリスクアセスメントは、個人情報の取扱いに関連するプライバシーリスクを特定し、組織がそのようなリスクをマネジメントするためにプライバシー通知に含める適切な要素を決定するのに役立つ場合がある。個人が自分の情報がどのように取扱われているかを理解できるように、組織は簡単な言葉で資料を書き、専門用語を避ける。

関連管理策: PM-20, PM-22, PT-2, PT-3, PT-4, PT-7, RA-3, SC-42, SI-18

拡張管理策:

(1) プライバシー通知 | ジャストインタイムの通知

個人が個人情報を提供する時間と場所で、またはデータアクションと関連して、または[*設定: 組織が定める頻度*]で、個人情報の取扱いの通知を提示する。

詳解: ジャストインタイムの通知は、そのような通知が個人にとって最も役立つ可能性がある時に、組織が個人情報をどのように取扱うかを個人に通知する。個人情報がどのように取扱われるかについての個人の想定は、組織が最後に通知を提示してから時間が経過した場合、または個人が最後に通知を提供された状況が変化した場合、的確でないか信頼できない可能性がある。ジャストインタイムの通知は、組織が個人のプライバシーリスクを増大させる可能性があると特定したデータアクションを説明することができる。組織は、特定のデータアクションが発生した際や、前回の通知以降に発生した特定の変更を強調する際に、特定のデータアクションについて更新したり、個人に思い出させるために、ジャストインタイムの通知を使用することができる。ジャストインタイムの通知は、同意が拒否された場合にどうなるかを説明するために、ジャストインタイムの同意とともに使用することができる。組織は裁量により、ジャストインタイムの通知をいつ使用するかを決定し、個人のプライバシーへの関心や懸念についてさらに学ぶために、人口統計学的属性、フォーカスグループ、または調査に関する補足情報を利用してもよい。

関連管理策: PM-21

(2) プライバシー通知 | プライバシー保護法のステートメント

プライバシー保護法の記録システムで維持される情報を取得するフォームにプライバシー保護法のステートメントを含めるか、個人が保持できる別のフォームにプライバシ

一保護法のステートメントを提供する。

詳解：連邦政府機関が個人に記録システムの一部となる情報の提供を求める場合、その機関は、情報を取得するために使用するフォームまたは個人が保持可能な別のフォームに[PRIVACT]ステートメントを提供する必要がある。政府機関は、情報を紙または電子フォーム、ウェブサイト、モバイルアプリケーション、電話、または他の何らかの媒体を通して取得するかどうかに関係なく、そのような状況において[PRIVACT]ステートメントを提供する。この要件により、情報に基づいて対応するかどうかを決定するための情報の要求に関する十分な情報が個人に提供されることを確実にする。

[PRIVACT]ステートメントは、情報の提供依頼を認可する職権の個人に、情報の提供が必須か任意か、情報が使用される主要な目的、情報の対象となる公開された定常的な利用、要求された情報の全部または一部を提供しないことによる個人への影響、適切な引用と関連する記録システムへのリンクについて、公式の通知文を提供する。連邦政府機関の職員は、[PRIVACT]の通知規定に関して政府機関のプライバシー保護責任者および法律顧問に相談する。

関連管理策：PT-6

拡張管理策：なし

参照資料：[PRIVACT], [OMB A-130], [OMB A-108]

PT-6 記録システムの通知

管理策：プライバシー保護法の記録システムで維持される情報を取扱うシステムの場合：

a. OMB のガイダンスに従って記録システムの通知の草案を作成し、事前レビューのために、OMB および該当する議会の委員会に新しく大幅に変更された記録システムの通知を提出する。

b. 官報に記録システムの通知を公表する。

c. 記録システムの通知を、的確に、最新のものを、ポリシーに従った範囲で保管する。

詳解：[PRIVACT]は、[PRIVACT]の記録システムの確立および／または変更時に、連邦政府機関が官報に記録システムの通知を発行することを要求する。一般的な問題として、個人の名前または識別番号、記号、またはその他の識別子によって情報を検索する機関の管理下にある記録のグループを機関が維持する場合、記録システムの通知が必要となる。通知は、システムの存在と特徴を記述し、記録システム、システムの目的、記録の維持管理の職権、システムで維持される記録の分類、記録を維持する個人の分類、記録の対象となる公開された定常的な利用、[OMB A-108]で記述されているシステムに関する追加の詳細を特定する。

関連管理策：AC-3, PM-20, PT-2, PT-3, PT-5

拡張管理策：

(1) 記録システムの通知 | 定常的な利用

[*設定：組織が定める頻度*]で、記録システムの通知に掲載されているすべての定常的な利用をレビューし、継続的に的確性を確保し、定常的な利用が情報取得時の目的と矛盾がないことを確実にする。

詳解：[PRIVACT]の定常的な利用は、記録システムを維持する連邦政府機関の外部での特定の種類の記録の開示である。定常的な利用は、記録が関係する個人の事前の書面による同意なしに、記録システムにおける記録開示の[PRIVACT]禁止に関する例外である。定常的な利用としての資格を得るには、開示は、情報を最初に取得した際の目的と矛盾のない目的としたものでなければならない。[PRIVACT]は、記録の利用者の分類や利用目的など、記録システムで維持されている記録の定常的な利用について記述することを機関に要求している。機関は、関連する記録システムの通知で明示的に定常的な利用を公表することによってのみ、定常的な利用を確立してもよい。

関連管理策：なし

(2) 記録システムの通知 | 適用除外規定

[*設定：組織が定める頻度*]で、記録システムに対して要求されたすべてのプライバシー保護法の適用除外をレビューし、それらが法律に従って適切かつ必要なままであり、それらが規則として公布されており、それらが記録システムの通知に的確に記述されていることを確実にする。

詳解：[PRIVACT]には、連邦政府機関が法令の特定の要件の適用除外を要求できるようにする 2 組の条項が含まれている。ある状況では、これらの規定により、機関は、[PRIVACT]の選択された規定から記録システムを除外する規則を公布することができる。組織の[PRIVACT]適用除外規則には、少なくとも、適用除外される記録システムの具体的な名称、記録システムが除外される[PRIVACT]の具体的な条項、適用除外の理由、適用除外が必要かつ適切である理由の説明を含む。

関連管理策：なし

参照資料：[PRIVACT], [OMB A-108]

PT-7 個人情報の特定の分類

管理策：個人情報の特定の分類に対して[*設定：組織が定める取扱い条件*]を適用する。

詳解：組織は、個人情報の特定の分類に、必要となる可能性のある条件または保護を適用する。これらの条件は、法律、大統領令、指令、規則、ポリシー、基準、またはガイドラインによって要求される場合がある。この要件は、個人情報の特定の分類が特に機微である、または特定のプライバシーリスクを引き起こすという組織の決定につながる前後関係の変化を考慮に入れたプライバシーリスクアセスメントの所見からも生じる場合がある。組織は、必要となる可能性のあるあらゆる保護について、政府機関のプライバシー保護責任者および法律顧問に相談する。

関連管理策：IR-9, PT-2, PT-3, RA-3

拡張管理策：

(1) 個人情報の特定の分類 | 社会保障番号

システムが社会保障番号を取扱う場合。

(a) 社会保障番号の不必要な収集、維持、利用を排除し、個人識別子としてのそれらの利用の代替手段を探求する。

(b) 個人が社会保障番号を開示することを拒否したことを理由に、個人が法律によって与えられた権利、利益、または特権を否定しない。

(c) 社会保障番号の開示を義務付けられているか任意かを問わず、その開示が義務付けられているか任意であるかを個人に知らせる。

詳解：連邦法およびポリシーは、組織の社会保障番号の取扱いに関する特定の要件を定めている。組織は、社会保障番号やその他の機微情報の不必要な利用を排除するための措置を講じ、適用される特定の要件を遵守する。

関連管理策：IA-4

(2) 個人情報の特定の分類 | 第一修正条項情報

法令または個人により明示的に認可されている場合を除き、または認可された法執行活動の範囲内にある場合を除き、個人が第一修正条項により保証された権利を行使する方法を説明する情報の取扱いを禁止する。

詳解：[PRIVACT]は、第一修正条項によって保証された権利を個人がどのように行使するかを説明する情報を取扱う機関の能力を限定する。組織は、これらの要件に関して政府機関のプライバシー保護責任者および法律顧問に相談する。

関連管理策：なし

参照資料：[PRIVACT], [OMB A-130], [OMB A-108], [NARA CUI]

PT-8 コンピュータマッチング要件

管理策：システムまたは組織がマッチングプログラムを実施する目的で情報を取扱う場合。

a. マッチングプログラムを実施するためにデータインテグリティ委員会から承認を得る。

b. コンピュータマッチングの合意書を作成し、締結する。

c. マッチングの通知を官報に公表する。

d. 必要に応じて、個人に対して不利な措置をとる前に、マッチングプログラムによって生成された情報を独立して検証する。

e. 個人に通知し、個人に対して不利な措置をとる前に、調査結果に異議を唱える機会を提供する。

詳解：[PRIVACT]は、連邦政府機関および非連邦政府機関がマッチングプログラムに携わる場合の要件を規定している。一般に、マッチングプログラムは、2 つ以上の自動化された[PRIVACT]記録システム、または自動化された記録システムおよび非連邦政府機関（またはその代理機関）によって維持される自動化された記録との、記録のコンピュータによる比較である。マッチングプログラムは、連邦政府の給付制度、連邦政府の職員または給与記録のいずれかに関係する。連邦給付制度のもとでの支払いの適格性を判断または検証するため、または連邦給付制度のもとでの支払いまたは滞納債務を埋め合わすために、連邦給付マッチングが行われる。マッチングプログラムには、マッチング活動自体だけでなく、調査フォローアップや最終的な措置も含まれる場合もある。

関連管理策：PM-24

拡張管理策：なし

参照資料：[PRIVACT], [CMPPA], [OMB A-130], [OMB A-108]

3.16 リスクアセスメント

リスクアセスメントの要約表へのクイックリンク

RA-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。

1. 以下の[*選択(1 つ以上):組織レベル;ミッション／事業プロセスレベル;システムレベル*]のリスクアセスメントのポリシー。

(a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、および準拠に対処する。

(b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに適合している。

2. リスクアセスメントのポリシーと関連するリスクアセスメントの管理策の実装を促進するための手順。

b. リスクアセスメントのポリシーと手順の策定、文書化、および配布することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行のリスクアセスメントをレビューし、更新する。

1. ポリシーについて[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

2. 手順について[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

詳解:リスクアセスメントのポリシーと手順は、システムおよび組織で実装される RA ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に寄与する。したがって、セキュリティおよびプライバシープログラムがリスクアセスメントのポリシーと手順の策定と連携していることが重要である。セキュリティおよびプライバシープログラムのポリシーと手順を組織レベルで確立することは望ましく、一般的には、ミッションまたはシステム固有のポリシーと手順を不要にすることができる。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映する複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムに対して規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述し、手順の対象である個人または役割向けとすることができる。手順は、システムのセキュリティおよびプライバシー計画の中に、または 1 つ以上の別の文書に文書化することもできる。リスクアセスメントのポリシーと手順の更新を引き起こす可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれる。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策:PM-9, PS-8, SI-12

拡張管理策:なし

参照資料:[OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100]

RA-2 セキュリティ分類化

管理策:

a. システムと、システムが処理、保存、伝送する情報を分類する。

b. システムのセキュリティ計画に、裏付けとなる根拠を含むセキュリティ分類化の結果を文書化する。

c. 認可権限のある担当者または認可権限のある担当者が指定した代表者がセキュリティ分類化の決定をレビューおよび承認することを検証する。

詳解:セキュリティの分類化は、機密性、完全性、または可用性の喪失により組織の情報およびシステムが侵害された場合の、組織の運営、組織の資産、および個人に対する潜在的な有害なインパクトまたは悪影響を表す。セキュリティ分類化は、システム開発ライフサイクル全体にわたって実行されるシステムセキュリティエンジニアリングプロセスにおける資産損失の特性評価の一種でもある。組織は、プライバシーリスクアセスメントまたはプライバシー影響評価を使用して、個人への潜在的な悪影響をよりよく理解することができる。[CNSSI 1253]は、国家安全保障システムの分類に関する追加のガイダンスを提供する。

組織は、セキュリティ分類化プロセスを組織全体の活動として実施し、最高情報責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、事業オーナー、ミッションおよびシステムオーナー、ならびに情報オーナーまたはスチュワードが直接関与する。組織は、他の組織への潜在的な有害なインパクトを考慮し、[USA PATRIOT]および国土安全保障省への大統領指令に従って、国家レベルの潜在的な有害なインパクトを考慮する。

セキュリティ分類化プロセスは、情報資産のインベントリの開発を促進し、CM-8 とともに、情報が処理、保存、または伝送される特定のシステムコンポーネントへのマッピングを容易にする。セキュリティ分類化プロセスは、システム開発ライフサイクル全体を通して再検討され、セキュリティの分類化が的確かつ適切な状態を保つようにする。

関連管理策:CM-8, MP-4, PL-2, PL-10, PL-11, PM-7, RA-3, RA-5, RA-7, RA-8, SA-8, SC-7, SC-38, SI-12

拡張管理策:

(1) セキュリティ分類化 | インパクトレベルの優先順位付け

組織のシステムにインパクトレベルの優先順位付けを行い、システムの影響度レベルに対する詳細を把握する。

詳解:組織は、[FIPS 199]に従って分類された各システムに「最高水準点」の概念を適用し、その結果、システムは低インパクト、中インパクト、または高インパクトに指定される。リスクベースの意思決定のためにシステムのインパクトの指定をさらに細かくしたい組織は、最初のシステムの分類をさらにサブカテゴリーに分割できる。例えば、中インパクトを受けたシステムに対するインパクトレベルの優先順位付けは、低-中システム、中-中システム、および高-中システムの 3 つの新しいサブカテゴリーを生成できる。インパクトレベルの優先順位付けおよび結果として生じるシステムのサブカテゴリーにより、組織は、特定されたリスクへの対応において、セキュリティ管理策の選択および管理策のベースラインのテーラリングに関連する投資に集中する機会が与えられる。インパクトレベルの優先順位付けを使用して、敵対者への関心や価値が高まる可能性のあるシステム、または連邦政府事業にとって重要な損失を表す可能性のあるシステムを決定することもできる。そのような価値の高い資産の場合、組織は、複雑さ、集約、および情報交換により重点を置くことができる。価値の高い資産を持つシステムは、インパクトの大きいシステムを低-高システム、中-高システム、高-高システムに分割することによって優先順位を付けることができる。あるいは、組織は、セキュリティ目的関連の分類について、[CNSSI 1253]のガイダンスを適用することができる。

関連管理策:なし

参照資料:[FIPS 199], [FIPS 200], [SP 800-30], [SP 800-37], [SP 800-39], [SP 800-60-1], [SP 800-60-2], [SP 800-160-1], [CNSSI 1253], [NARA CUI]

RA-3 リスクアセスメント

管理策:

a. 以下を含むリスクアセスメントを実施する。

1. システムに対する脅威および脆弱性を特定する。
2. システム、システムが処理、保存、または伝送する情報、および関連情報への認可されていないアクセス、使用、開示、中断、改変、または破壊による危害の可能性と程度を判断する。
3. 個人情報の取扱いから生じる個人への悪影響の可能性とインパクトを判断する。

b. 組織およびミッションまたは事業プロセスの観点からリスクアセスメント結果とリスクマネジメント決定をシステムレベルのリスクアセスメントと統合する。

c. リスクアセスメント結果を[*選択:セキュリティおよびプライバシー計画;リスクアセスメント報告書*]を[*設定:組織が定める文書*]として文書化する。

d. アセスメント結果を[*設定:組織が定める頻度*]でレビューする。

e. リスクアセスメント結果を[*設定:組織が定める職員または役割*]に配布する。

f. リスクアセスメントを[*設定:組織が定める頻度*]で、またはシステム、システムの運用環境、またはシステムのセキュリティまたはプライバシーの状態にインパクトを与える可能性があるその他の条件に重大な変更がある場合に更新する。

詳解:リスクアセスメントでは、脅威、脆弱性、可能性、および組織の運営と資産、個人、他の組織、および国家へのインパクトが考慮される。リスクアセスメントでは、組織に代わってシステムを運用する契約事業者、組織のシステムにアクセスする個人、サービスプロバイダ、およびアウトソーシングエンティティなどの外部関係者からのリスクも考慮する。

組織は、リスクマネジメント階層の 3 つすべてのレベル(すなわち、組織レベル、ミッション/事業プロセスレベル、または情報システムレベル)およびシステム開発ライフサイクルの任意の段階でリスクアセスメントを実施することができる。リスクアセスメントは、準備、分類、管理策の選択、管理策の実施、管理策アセスメント、認可、管理策監視など、リスクマネジメントフレームワークの様々なステップで実施することもできる。リスクアセスメントは、システム開発ライフサイクル全体を通じて実行される継続的な活動である。

リスクアセスメントでは、システム設計、システムの使用目的、テスト結果、サプライチェーン関連の情報やアーティファクトなど、システムに関連する情報を扱うこともできる。リスクアセスメントは、管理策選択プロセスにおいて、特にテーラリングガイダンスの適用中および能力決定の初期段階において重要な役割を果たすことができる。

関連管理策:CA-3, CA-6, CM-4, CM-13, CP-6, CP-7, IA-8, MA-5, PE-3, PE-8, PE-18, PL-2, PL-10, PL-11, PM-8, PM-9, PM-28, PT-2, PT-7, RA-2, RA-5, RA-7, SA-8, SA-9, SC-38, SI-12

拡張管理策:

(1) リスクアセスメント | サプライチェーンのリスクアセスメント

(a) [*設定:組織が定めるシステム、システムコンポーネント、およびシステムサービス*]に関連するサプライチェーンリスクをアセスメントする。

(b) 関連するサプライチェーンに大幅な変更がある場合、またはシステム、運用環境、またはその他の条件の変更によりサプライチェーンの変更が必要になる場合、サプライチェーンのリスクアセスメントを[*設定:組織が定める頻度*]で更新する。

詳解:サプライチェーン関連のイベントには、中断、欠陥のあるコンポーネントの使用、偽造品の挿入、盗難、悪意のある開発行為、不適切な配信行為、悪意のあるコードの挿入などがある。これらのイベントは、システムとその情報の機密性、完全性、または可用性に重大なインパクトを与える可能性があるため、組織の運営(ミッション、機能、イメージ、または評判を含む)、組織の資産、個人、他の組織、そして国家にも有害なインパクトを与える可能性がある。サプライチェーン関連のイベントは、意図的ではないことも、または悪意

のある場合もあり、システムのライフサイクルの任意の時点で発生する可能性がある。サプライチェーンリスクの分析は、組織が追加のサプライチェーンリスク軽減が必要なシステムまたはコンポーネントを特定するのに役立つ。

関連管理策：RA-2, RA-9, PM-17, PM-30, SR-2

(2) リスクアセスメント｜オールソースインテリジェンスの活用

オールソースインテリジェンスを活用して、リスク分析を支援する。

詳解：組織は、エンジニアリング、取得、およびリスクマネジメントの決定を通知するために、オールソースインテリジェンスを活用する。オールソースインテリジェンスは、公開またはオープンソースの情報、対象の特徴を決定づける情報、人を介した情報収集と分析技術、電気信号による情報収集と分析技術、画像による情報収集と分析技術など、利用可能なすべてのソースから得られた情報で構成されている。オールソースインテリジェンスは、開発、製造、および引き渡しプロセス、人、および環境からの（意図的および非意図的の両方の）脆弱性のリスクを分析するために使用される。リスク分析は、リスクを管理するのに十分なサプライチェーン内の複数の階層のサプライヤに対して実施することができる。組織は、必要に応じて、オールソースインテリジェンスの情報またはその結果による判断を他の組織と共有するための合意を策定することができる。

関連管理策：なし

(3) リスクアセスメント｜動的脅威認識

[*設定：組織が定める手段*]を使用して、継続的に現在のサイバー脅威環境を見極める。

詳解：収集された脅威認識情報は、組織の情報セキュリティ運用に組み込まれ、脅威環境の変化に対応して手順が更新されるようにする。例えば、脅威レベルが高くなると、組織は特定の操作を実行するために必要な特権または認証のしきい値を変更する場合がある。

関連管理策：AT-2

(4) リスクアセスメント｜予測的サイバー分析

[*設定：組織が定める高度な自動化および分析機能*]を使用して、[*設定：組織が定めるシステムまたはシステムコンポーネント*]に対するリスクを予測および特定する。

詳解：適切なリソースを備えたセキュリティオペレーションセンター（SOC: Security Operations Center）またはコンピュータインシデント対応チーム（CIRT: Computer Incident Response Team）は、高度な自動化と分析機能を使用してデータを分析しない限り、セキュリティツールと装置の急増によって生成される情報量に圧倒される可能性がある。高度な自動化および分析機能は、通常、機械学習を含む人工知能の概念によってサポートされている。例としては、自動脅威発見および対応（広範囲にわたる収集、文脈ベースの分析、および適応型対応機能を含む）、自動化されたワークフロー操作、およびマシン支援決定ツールが含まれる。ただし、高度な敵対者は分析パラメータに関連する情報を抽出し、悪意のある行為を良性と分類すべく機械学習を再トレーニングする可能性があることに注意する。したがって、機械学習は、高度な敵対者が彼らの活動を秘匿することができないことを確実にするために、人間の監視によって増強される。

関連管理策：なし

参照資料：[OMB A-130], [SP 800-30], [SP 800-39], [SP 800-161], [IR 8023], [IR 8062], [IR 8272]

RA-4 リスクアセスメントの更新

［撤回：RA-3 に組み込まれた］

RA-5 脆弱性の監視およびスキャン

管理策：

a. [*設定：組織が定める頻度、および／または組織が規定したプロセスに従ってランダム*]

に、およびシステムに影響を与える可能性のある新しい脆弱性が特定および報告された場合、システムおよびホストされているアプリケーションの脆弱性を監視およびスキャンする。

b. ツール間の相互運用性を促進し、以下の規格を使用して脆弱性管理プロセスの一部を自動化する脆弱性監視ツールおよび技法を採用する。

1. プラットフォーム、ソフトウェアの欠陥、および不適切な構成を列挙する。
2. チェックリストとテスト手順をフォーマットする。
3. 脆弱性のインパクトを測定する。

c. 脆弱性スキャンレポートと脆弱性監視の結果を分析する。

d. リスクの組織によるアセスメントに従って、妥当な脆弱性へ[*設定:組織が定める対応時間*]で修正する。

e. 脆弱性監視プロセスおよび管理策アセスメントから得られた情報を[*設定:組織が定める職員または役割*]と共有し、他のシステムにおける同様の脆弱性を排除する。

f. スキャンされる脆弱性を直ちに更新する機能を含む脆弱性監視ツールを採用する。

詳解:情報とシステムのセキュリティ分類化は、脆弱性監視(スキャンを含む)の頻度と包括性の目安となる。組織は、インフラストラクチャコンポーネント(スイッチ、ルータ、ガード、センサなど)、ネットワークに接続されたプリンタ、スキャナ、コピー機などの潜在的な脆弱性のソースを見落とさないように、システムコンポーネントに必要な脆弱性監視を決定する。脆弱性監視ツールを即座に更新する機能は、新しい脆弱性が発見および発表されたとき、および新しいスキャン方法が開発されたときに、採用されている脆弱性監視ツールが新しい脆弱性を見逃さないようにするのに役立つ。脆弱性監視ツールの更新プロセスは、システム内の潜在的な脆弱性が可能な限り迅速に特定され、対処されることを保証するのに役立つ。カスタムソフトウェアの脆弱性の監視と分析には、静的分析、動的分析、バイナリ分析、または 3 つのアプローチのハイブリッドなど、追加のアプローチが必要になる場合がある。組織は、これらの分析技法を、ソースコードのレビューや、ウェブベースのアプリケーションスキャナ、静的分析ツール、バイナリアナライザーなどの様々なツールで使用できる。

脆弱性の監視には、パッチレベルのスキャン;ユーザまたはデバイスがアクセスすることが望ましくない機能、ポート、プロトコル、およびサービスのスキャン;および不適切に構成されているか正しく動作していないフロー制御メカニズムのスキャンが含まれる。脆弱性監視には、コンポーネントを継続的に分析するために計装を使用する継続的な脆弱性監視ツールが含まれても良い。計装型のツールは的確性を向上させ、スキャンすることなく組織全体で実行できる。相互運用性を促進する脆弱性監視ツールには、セキュリティコンテンツ自動化プロトコル(SCAP:Security Content Automated Protocol)で検証されたツールが含まれる。したがって、組織は共通脆弱性識別子(CVE: Common Vulnerabilities and Exposures)命名規則で脆弱性を表現し、セキュリティ検査言語(OVAL: Open Vulnerability Assessment Language)を使用して脆弱性の存在を判断するスキャンツールの使用を考慮する。脆弱性情報のソースには、共通脆弱性タイプ一覧(CWE: Common Weakness Enumeration)および国有脆弱性情報データベース(NVD: National Vulnerability Database)が含まれる。レッドチーム演習などの管理策アセスメントは、スキャンする潜在的な脆弱性の追加のソースを提供する。また、組織は共通脆弱性評価システム(CVSS: Common Vulnerability Scoring System)による脆弱性のインパクトを表すスキャンツールの使用を考慮する。

脆弱性の監視には、一般の人々からセキュリティの脆弱性の報告を受けるためのチャネルとプロセスが含まれる。脆弱性開示プログラムは、誠実な調査を認可する通知やセキュリティの脆弱性の開示など、レポートを受信できる監視対象の電子メールアドレスや ウェブ フォームを公開するのと同じくらい簡単である。組織は通常、そのような調査が許可の有無にかかわらず行われることを期待しており、公開された脆弱性開示チャネルを使用して、発見された脆弱性が改善のために組織に直接報告される可能性を高めることができる。

組織は、外部のセキュリティ研究者が発見された脆弱性を報告することをさらに奨励するために、金銭的インセンティブ(「バグ報奨金」としても知られる)の使用を採用することもできる。バグ報奨金プログラムは、組織のニーズに合わせて調整できる。報奨金は無期限に、または規

定された期間にわたって運用することができ、一般の人々または精選されたグループに提供することができる。組織は、パブリック報奨金とプライベート報奨金を同時に実行でき、特権的な観点からセキュリティの脆弱性を評価するために、一部の参加者に部分的に資格情報が必要なアクセスを提供することを選択できる。

関連管理策：CA-2, CA-7, CA-8, CM-2, CM-4, CM-6, CM-8, RA-2, RA-3, SA-11, SA-15, SC-38, SI-2, SI-3, SI-4, SI-7, SR-11

拡張管理策：

(1) 脆弱性の監視およびスキャン｜ツール機能の更新

［撤回：RA-5 に組み込まれた］

(2) 脆弱性の監視およびスキャン｜スキャンする脆弱性の更新

スキャンするシステムの脆弱性を[*選択（1 つまたは複数）：[設定：組織が定める頻度]；新しいスキャンの前；新しい脆弱性が特定され、報告された場合*]に更新する。

詳解：最新のソフトウェア、システム、およびその他の要因の複雑さにより、新しい脆弱性が日常的に発見されている。新しく発見された脆弱性をスキャン対象の脆弱性のリストに追加し、組織がそれらの脆弱性を適時に緩和するための措置を講じることができるようにすることが重要である。

関連管理策：SI-5

(3) 脆弱性の監視およびスキャン｜カバレッジの幅および深さ

脆弱性スキャンのカバレッジの幅および深さを規定する。

詳解：脆弱性スキャンのカバレッジの広さは、システム内のコンポーネントの割合、特定のタイプのシステム、システムの重要度、またはチェックされる脆弱性の数として表すことができる。逆に、脆弱性スキャンのカバレッジの深さは、組織が監視する予定のシステム設計のレベル（コンポーネント、モジュール、サブシステム、要素など）として表すことができる。組織は、そのリスク許容度およびその他の要因に関して、脆弱性スキャンのカバレッジの十分性を判断できる。スキャンツールとツールの構成方法は、深さとカバレッジに影響する場合がある。必要な深さとカバレッジを実現するには、複数のスキャンツールが必要になる場合がある。[SP 800-53A]は、カバレッジの幅と深さに関する追加情報を提供する。

関連管理策：なし

(4) 脆弱性の監視およびスキャン｜検出可能な情報

検出可能なシステムに関する情報を決定し、[*設定：組織が定める是正措置*]を講じる。

詳解：検出可能な情報には、システムを侵害したり、システムをブリーチしたりせずに、システムが公開している情報を収集したり、大規模なウェブ検索を行ったりすることによって、敵対者が入手できる情報が含まれる。是正措置には、適切な組織職員への通知、指定された情報の削除、または指定された情報の敵対者にとって関連性が低く、また目立たなくなるようにシステムを変更することが含まれる。この拡張機能は、組織が展開するデコイ機能（ハニーポット、ハニーネット、擬装ネットなど）の一部である可能性のある意図的な検出可能情報を除外する。

関連管理策：AU-13, SC-26

(5) 脆弱性の監視およびスキャン｜特権アクセス

[*設定：組織が定める脆弱性スキャン措置*]の[*設定：組織が定めるシステムコンポーネント*]に特権アクセス認可を実装する。

詳解：特定の状況では、脆弱性スキャンの性質がより煩わしい場合や、スキャンの対象となるシステムコンポーネントに、個人情報などの機密情報または管理対象非機密情報が含まれている場合がある。選択されたシステムコンポーネントへの特権アクセス認可により、脆弱性スキャンの徹底が容易になり、そのようなスキャンの機微性が保護される。

関連管理策：なし

(6) 脆弱性の監視およびスキャン｜自動化された傾向分析

[*設定：組織が定める自動化されたメカニズム*]を使用して、複数の脆弱性スキャンの結果を比較する。

詳解：自動化されたメカニズムを使用して、複数の脆弱性スキャンを長期間にわたって分析すると、システムの脆弱性の傾向を明らかにし、攻撃のパターンを特定するのに役立つ。

関連管理策：なし

(7) 脆弱性の監視およびスキャン｜認可されていないコンポーネントの自動化された検知および通知

[撤回：CM-8 に組み込まれた]

(8) 脆弱性の監視およびスキャン｜過去の監査ログのレビュー

過去の監査ログをレビューすることで、[*設定：組織が定めるシステム*]で特定された脆弱性が[*設定：組織が定める期間*]内に以前に悪用されたかどうかを判断する。

詳解：システムで最近検知された脆弱性が敵対者によって以前に悪用されたかどうかを判断するために過去の監査ログをレビューすることは、フォレンジック分析に重要な情報を提供することができる。このような分析は、例えば、以前の侵入の程度、攻撃中に採用された窃取技術、漏出または変更された組織情報、影響を受けたミッションまたは事業能力、および攻撃の期間を特定するのに役立つ。

関連管理策：AU-6, AU-11

(9) 脆弱性の監視およびスキャン｜侵入テストおよび分析

[撤回：CA-8 に組み込まれた]

(10) 脆弱性の監視およびスキャン｜スキャン情報の相関

脆弱性スキャンツールからの出力の相関をとり、複数の脆弱性およびマルチホップ攻撃ベクトルの存在を判断する。

詳解：攻撃ベクトルとは、敵対者が悪意のあるコードを配信したり、情報を漏出したりするために、システムにアクセスするための経路または手段である。組織は、アタックツリー（セキュリティ脅威分析技法）を使用して、敵対者による敵対的行為がどのように相互作用し、組み合わされて、システムおよび組織に有害なインパクトまたはネガティブな結果をもたらすかを示すことができる。このような情報は、脆弱性スキャンツールからの相関データとともに、複数の脆弱性とマルチホップの攻撃ベクトルをより明確に提供することができる。脆弱性スキャン情報の相関関係は、組織が古い技術から新しい技術に移行する場合（例えば、IPv4 から IPv6 ネットワークプロトコルに移行する場合）に特に重要である。このような移行中、一部のシステムコンポーネントが誤って管理されなくなり、敵対者が悪用する機会が生じる可能性がある。

関連管理策：なし

(11) 脆弱性の監視およびスキャン｜公開開示プログラム

組織のシステムおよびシステムコンポーネントの脆弱性の報告を受け取るための公開報告チャネルを確立する。

詳解：報告チャネルは一般に公開されており、誠実な調査と組織への脆弱性の開示を認可する明確な言葉が含まれている。組織は、報告エンティティによる公衆への無制限の非開示の期待に基づいてその認可を条件付けないが、脆弱性を適切に修正するために特定の期間を要求することがある。

関連管理策：なし

参照資料：[ISO 29147], [SP 800-40], [SP 800-53A], [SP 800-70], [SP 800-115], [SP 800-126], [IR 7788], [IR 8011-4], [IR 8023]

RA-6 技術監視対策調査

管理策:[*設定:組織が定める場所*]で[*選択(1 つ以上):[設定:組織が定める頻度];[設定:組織が定めるイベントまたは兆候*]]が発生した場合に技術監視対策調査を採用する。

詳解:技術監視対策調査は、資格のある職員が提供するサービスで、技術監視デバイスの存在と危険性を検知し、調査対象の施設への技術侵入に使用される可能性のある技術セキュリティの弱点を特定する。技術監視対策調査は、組織および施設の技術的セキュリティ態勢の評価も提供し、調査対象施設の内部、外部の目視検査、電子的検査、および物理的検査を含む。調査はまた、潜在的な敵対者に対する組織の露出に関するリスクアセスメントおよび情報のための有用な情報を提供する。

関連管理策:なし

拡張管理策:なし

参照資料:なし

RA-7 リスク対応

管理策:組織のリスク許容度に応じて、セキュリティおよびプライバシーのアセスメント、監視、監査の結果に対応する。

詳解:組織には、新しい管理策の導入や既存の管理策の強化によるリスクの軽減、適切な正当化または根拠のあるリスクの受け入れ、リスクの共有または転送、リスクの回避など、リスクに対応するための多くのオプションがある。組織のリスク許容度は、リスク対応の決定と行動に影響を与える。リスク対応は、実施計画およびマイルストーンの記載事項を作成する前に、リスクに対する適切な対応を決定する必要性に対処する。例えば、対応として、リスクを受け入れる、またはリスクを拒否する、またはすぐにリスクを軽減して、実施計画およびマイルストーンの記載事項が不要になるようにすることができる。ただし、リスク対応がリスクを軽減することであり、軽減策をすぐに完了できない場合は、実施計画およびマイルストーンの記載事項が作成される。

関連管理策:CA-5, IR-9, PM-4, PM-28, RA-2, RA-3, SR-2

拡張管理策:なし

参照資料:[FIPS 199], [FIPS 200], [SP 800-30], [SP 800-37], [SP 800-39], [SP 800-160-1]

RA-8 プライバシー影響評価

管理策:システム、プログラム、またはその他の活動に対するプライバシー影響評価を以下の前に実施する。

a. 個人情報を処理する情報技術を開発または調達する。

b. 次のような個人情報の新たな収集を開始する。

   1. 情報技術を使用して処理される。

   2. 連邦政府の機関、補助機関、職員以外の 10 人以上の個人に同一の質問または同一の報告要件が課せられている場合、特定の個人の物理的またはネットワークによる(オンライン)連絡を許可する個人情報を含む。

詳解:プライバシー影響評価は、個人情報がどのように処理されるかを分析して、その処理が適用されるプライバシー要件に適合し、情報システムまたは活動に関連するプライバシーリスクを特定し、プライバシーリスクを軽減する方法を評価するものである。プライバシー影響評価の評価は、分析と、分析のプロセスと結果を詳述する正式な文書の両方である。

組織は、組織がプライバシーを十分に考慮し、組織の活動の初期段階から情報ライフサイクル全体にわたって適切なプライバシー保護を組み込んだことを示すために、十分な明確性と具体性を備えたプライバシー影響評価を開発し実施する。有意義なプライバシー影響評価を実施す

るために、組織の政府機関のプライバシー保護責任者は、プログラム管理者、システムオーナー、情報技術専門家、セキュリティ担当者、弁護士、およびその他の関連組織職員と緊密に協力する。さらに、プライバシー影響評価は、情報システムの特定のマイルストーンや段階、または個人情報のライフサイクルに限定される時間制限のある活動ではない。むしろ、プライバシー分析は、システムおよび個人情報のライフサイクル全体を通じて継続される。したがって、プライバシー影響評価は、情報技術の変更、組織慣行の変更、またはその他の要因がそのような情報技術の使用に関連するプライバシーリスクを変更するたびに組織が更新する随時更新文書である。

プライバシー影響評価を実施するために、組織はセキュリティリスクアセスメントおよびプライバシーリスクアセスメントを使用することができる。組織は、プライバシーしきい値分析など、名前が異なる他の関連プロセスを使用する場合もある。プライバシー影響評価は、プライバシーに関する組織の慣行に関する公衆への通知としての役割を果たすこともできる。プライバシー影響評価の実施および公表は法律で義務付けられている場合があるが、適用される法律がない場合、組織はそのようなポリシーを策定することがある。連邦政府機関の場合、プライバシー影響評価が[EGOV]によって要求されることがある。政府機関は、この要件とこの規定に関する法的例外および OMB ガイダンスに注意して、政府機関のプライバシー保護責任者および法務官に相談する事が望ましい。

関連管理策: CM-4, CM-9, CM-13, PT-2, PT-3, PT-5, RA-1, RA-2, RA-3, RA-7

拡張管理策: なし

参照資料: [EGOV], [OMB A-130], [OMB M-03-22]

RA-9 重要度分析

管理策: [*設定: 組織が定めるシステム開発ライフサイクルにおける意思決定ポイント*]で、[*設定: 組織が定めるシステム、システムコンポーネント、またはシステム サービス*]の重要度分析を実行して、重要なシステムコンポーネントおよび機能を特定する。

詳解: すべてのシステムコンポーネント、機能、またはサービスが必ずしも重要な保護を必要とするわけではない。例えば、重要度分析はサプライチェーンのリスクマネジメントの重要な要素であり、保護措置の優先順位を与える。重要なシステムコンポーネントと機能の特定では、適用される法律、大統領令、規則、指令、ポリシー、基準、システム機能要件、システムとコンポーネントのインタフェース、およびシステムとコンポーネントの依存関係が考慮される。システムエンジニアは、ミッションクリティカルな機能やコンポーネントを特定するために、システムの機能分解を行う。機能分解には、システムがサポートする組織のミッションの特定、それらのミッションを実行するための特定の機能への分解、およびそれらの機能を実装するハードウェア、ソフトウェア、およびファームウェアコンポーネントのトレーサビリティが含まれ、システム内外の多くのコンポーネントで機能が共有されている場合を含め、これらの機能を実装する。

システムまたはシステムコンポーネントの運用環境は、サイバーフィジカルシステム、デバイス、システム・オブ・システムズ、およびアウトソーシングされた IT サービスへの接続および依存性を含め、重要性にインパクトを与える可能性がある。重要なシステムコンポーネントまたは機能へ直接アクセス可能なシステムコンポーネントは、そのようなコンポーネントが作り出す固有の脆弱性のために、重要であると考えられる。コンポーネントおよび機能の重要性は、コンポーネントまたは機能を含むシステムによってサポートされる組織のミッションに対するコンポーネントまたは機能の障害のインパクトの観点からアセスメントされる。

重要度分析は、構成または設計が開発、変更、またはアップグレードされるときに実行される。このような分析がシステム開発ライフサイクルの早い段階で実行される場合、組織は、システム設計に冗長性や代替パスを追加するなどして、システム設計を変更して、これらのコンポーネントや機能の重要な性質を軽減できる可能性がある。重要度分析は、開発契約事業者が必要とする保護対策にも影響を及ぼす可能性がある。システム、システムコンポーネント、およびシステムサービスの重要度分析に加えて、情報の重要度分析は重要な考慮事項である。このような分析は、RA-2 のセキュリティ分類化の一部として行われる。

関連管理策: CP-2, PL-2, PL-8, PL-11, PM-1, PM-11, RA-2, SA-8, SA-15, SA-20, SR-5

拡張管理策：なし

参照資料：[IR 8179]

RA-10 脅威ハンティング

管理策：

a. 以下のサイバー脅威ハンティング能力を確立して維持する。

1. 組織のシステムにおける侵害の兆候を探す。
2. 既存の管理策をくぐりぬける脅威を検知、追跡、および行為を中断させる。

b. 脅威ハンティング機能を[*設定：組織が定める頻度*]で行使する。

詳解：脅威ハンティングは、ファイアウォール、侵入検知および防止システム、サンドボックス内の悪意のあるコードの隔離、セキュリティ情報およびイベント管理技術やシステムなどの従来の保護手段とは対照的に、サイバー防御の積極的な手段である。サイバー脅威ハンティングでは、組織のシステム、ネットワーク、インフラストラクチャを積極的に検索し、高度な脅威を探す。目的は、攻撃シーケンスのできるだけ早い段階でサイバー敵対者を追跡して行為を中断させること、および組織の対応の速度と精度を測定可能なまでに改善することである。侵害の兆候には、異常なネットワークトラフィック、異常なファイル変更、悪意のあるコードの存在などがある。脅威ハンティングチームは、既存の脅威に関する情報収集と分析技術を活用し、新しい脅威に関する情報収集と分析技術を作成する場合がある。この脅威に関する情報収集と分析技術は、同業者、情報共有分析機関（ISAO: Information Sharing and Analysis Organizations）、情報共有分析センター（ISAC: Information Sharing and Analysis Centers）、および関係省庁と共有される。

関連管理策：CA-2, CA-7, CA-8, RA-3, RA-5, RA-6, SI-4

拡張管理策：なし

参照資料：[SP 800-30]

3.17 システムおよびサービスの取得

システムおよびサービスの取得の要約表へのクイックリンク

SA-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。

1. 以下の[*選択(1 つ以上):組織レベル;ミッション/事業プロセスレベル;システムレベル*]のシステムおよびサービスの取得のポリシー。

(a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、および準拠に対処する。

(b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに適合している。

2. システムおよびサービスの取得のポリシーと関連するシステムおよびサービスの取得の管理策の実装を促進するための手順。

b. システムおよびサービスの取得のポリシーと手順の策定、文書化、および配布することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行のシステムおよびサービスの取得をレビューし、更新する。

1. ポリシーについて[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

2. 手順について[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

詳解:システムおよびサービスの取得のポリシーと手順は、システムおよび組織で実装されるSA ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に寄与する。したがって、セキュリティおよびプライバシープログラムがシステムおよびサービスの取得のポリシーと手順の策定と連携していることが重要である。セキュリティおよびプライバシープログラムのポリシーと手順を組織レベルで確立することは望ましく、一般的には、ミッションまたはシステム固有のポリシーと手順を不要にすることができる。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映する複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムに対して規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述し、手順の対象である個人または役割向けとすることができる。手順は、システムのセキュリティおよびプライバシー計画の中に、または 1 つ以上の別の文書に文書化することもできる。システムおよびサービスの取得のポリシーと手順の更新を引き起こす可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれる。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策:PM-9, PS-8, SA-8, SI-12

拡張管理策:なし

参照資料:[OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100], [SP 800-160-1]

SA-2 リソースの割り当て

管理策:

d. ミッションと事業プロセス計画におけるシステムまたはシステムサービスの高度な情報セキュリティおよびプライバシー要件を決定する。

e. 組織の資本計画および投資管理プロセスの一環として、システムまたはシステムサービスを保護するために必要なリソースを決定し、文書化し、割り当てる。

f. 組織の計画策定および予算編成の文書に、情報セキュリティとプライバシーに関する個別の項目を設定する。

詳解:情報セキュリティとプライバシーのためのリソース配分には、システム開発ライフサイクル全体にわたるシステムとサービスの取得、維持、サプライチェーン関連のリスクへの資金提供が含まれる。

関連管理策:PL-7, PM-3, PM-11, SA-9, SR-3, SR-5

拡張管理策:なし

参照資料:[OMB A-130], [SP 800-37], [SP 800-160-1]

SA-3 システム開発ライフサイクル

管理策:

a. 情報セキュリティとプライバシーに関する考慮事項を組み込んだ[*設定:組織が定めるシステム開発ライフサイクル*]を使用して、システムを取得、開発、管理する。

b. システム開発ライフサイクル全体を通じて、情報セキュリティとプライバシーの役割と責任を規定し、文書化する。

c. 情報セキュリティおよびプライバシーの役割と責任を有する個人を特定する。

d. 組織の情報セキュリティおよびプライバシーリスクマネジメントプロセスをシステム開発ライフサイクル活動に統合する。

詳解:システム開発ライフサイクルプロセスは、組織システムの開発、実装、運用を成功させるための基盤を提供する。システム開発ライフサイクルの初期にセキュリティとプライバシーの考慮事項を統合することは、システムセキュリティエンジニアリングとプライバシーエンジニアリングの基本原則である。システム開発ライフサイクルで必要な管理策を適用するには、情報セキュリティとプライバシー、脅威、脆弱性、有害なインパクト、および重要なミッションと事業の機能に対するリスクの基本的な理解が必要である。SA-8 のセキュリティエンジニアリングの原則は、個人がシステムおよびシステムコンポーネントを適切に設計、コーディング、およびテストするのに役立つ。組織は、確立されたセキュリティ要件とプライバシー要件が組織のシステムに確実に組み込まれるように、システム開発ライフサイクルプロセスに資格のある職員(例えば、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、セキュリティおよびプライバシーアーキテクトの上級機関職員、セキュリティおよびプライバシーエンジニアなど)を含める。役割ベースのセキュリティおよびプライバシートレーニングプログラムは、重要なセキュリティおよびプライバシーの役割と責任を持つ個人が、割り当てられたシステム開発ライフサイクル活動を実施するための経験、スキル、専門知識を確実に持つことができる。

また、セキュリティとプライバシーの要件をエンタープライズアーキテクチャに効果的に統合することで、セキュリティとプライバシーに関する重要な考慮事項がシステムライフサイクル全体にわたって確実に対処され、それらの考慮事項が組織のミッションと事業プロセスに直接関連するようになる。このプロセスにより、組織のリスクマネジメント戦略と一致した、情報セキュリティおよびプライバシーアーキテクチャのエンタープライズアーキテクチャへの統合も容易になる。システム開発ライフサイクルには複数の組織(外部サプライヤ、開発者、インテグレーター、サービスプロバイダなど)が関与するため、取得およびサプライチェーンのリスクマネジメント機能と管理策は、ライフサイクルにおけるシステムの効果的な管理に重要な役割を果たす。

関連管理策: AT-3, PL-8, PM-7, SA-4, SA-5, SA-8, SA-11, SA-15, SA-17, SA-22, SR-3, SR-4, SR- 5, SR-9

拡張管理策:

(1) システム開発ライフサイクル | 運用前環境の管理

システム、システムコンポーネント、またはシステムサービスのシステム開発ライフサイクル全体を通じて、リスクに見合ったシステム運用前環境を保護する。

詳解: 運用前環境には、開発、テスト、および統合環境が含まれる。国防総省によって確立されたプログラム保護計画プロセスは、防衛関連事業者の運用前環境を管理する例である。重要度分析と開発者に対する管理策の適用も、よりセキュアなシステム開発環境に貢献する。

関連管理策: CM-2, CM-4, RA-3, RA-9, SA-4

(2) システム開発ライフサイクル | ライブデータまたは運用データの使用

(a) システム、システムコンポーネント、またはシステムサービスの運用前環境でのライブデータの使用を承認、文書化、および管理する。

(b) システム、システムコンポーネント、またはシステムサービスの運用前環境を、運用前環境で使用されているライブデータと同じインパクトまたは分類レベルで保護する。

詳解: ライブデータは運用データとも呼ばれる。運用前(つまり、開発、テスト、統合)環境でライブデータまたは運用データを使用すると、組織に重大なリスクが生じる可能性がある。さらに、テスト、調査、およびトレーニングにおける個人情報の使用は、そのような情報の認可されていない開示や誤用のリスクが高まる。したがって、組織は、ライブデータまたは運用データの使用から生じる可能性のある追加のリスクを管理することが重要である。組織は、システム、システムコンポーネント、およびシステムサービスの設計、開発、およびテスト中にテストデータまたはダミーデータを使用することにより、このようなリスクを最小限に抑えることができる。リスクアセスメント技法を使用して、ライブデータまたは運用データを使用するリスクが許容できるかどうかを判断することができる。

関連管理策: PM-25, RA-3

(3) システム開発ライフサイクル | 技術の更新

システム開発ライフサイクル全体を通じて、システムの技術更新スケジュールを計画し、実施する。

詳解: 技術更新計画には、ハードウェア、ソフトウェア、ファームウェア、プロセス、職員のスキルセット、サプライヤ、サービスプロバイダ、および施設が含まれる場合がある。廃止された、または廃止されつつある技術を使用すると、サポートされていないコンポーネント、偽造品または転用されたコンポーネント、セキュリティ要件またはプライバシー要件を実装できないコンポーネント、動作が遅いまたは動作しないコンポーネント、信頼できないソースからのコンポーネント、職員の不注意によるエラー、または複雑さの増加に関連したセキュリティやプライバシーのリスクが高まる場合がある。通常、技術の更新は、システム開発ライフサイクルの運用および保守段階で行われる。

関連管理策: MA-6

参照資料: [OMB A-130], [SP 800-30], [SP 800-37], [SP 800-160-1], [SP 800-171], [SP 800-172]

SA-4 取得プロセス

管理策: システム、システムコンポーネント、またはシステムサービスの取得契約では[*選択(1つ以上): 標準化された契約言語; [設定: 組織が定める契約言語]*]を使用して、明示的または参照により、次の要件、説明、および基準を含める。

a. セキュリティとプライバシーの機能要件。

b. メカニズム要件の強度。

c. セキュリティとプライバシーの保証要件。

d. セキュリティとプライバシーの要件を満たすために必要な管理策。

e. セキュリティとプライバシーに関するドキュメントの要件。

f. セキュリティおよびプライバシードキュメントに関する保護の要件。

g. システム開発環境およびシステムが動作することが意図されている環境の説明。

h. 情報セキュリティ、プライバシー、およびサプライチェーンのリスクマネジメントに責任を負う当事者の割り当てまたは識別。

i. 受領基準。

詳解:セキュリティとプライバシーの機能要件は、通常、SA-2 に記述されている高レベルのセキュリティとプライバシー要件から派生する。派生要件には、セキュリティとプライバシーの能力、機能、およびメカニズムが含まれる。そのような能力、機能、およびメカニズムに関連する強度要件には、仕様への適合性、正確性、改ざんまたはバイパスに対する耐性、および直接攻撃に対する耐性が含まれる。保証要件には、開発プロセス、手順、および方法論、ならびに必要な機能が実装され、メカニズムの必要な強度を有しているという信頼の根拠を提供する開発およびアセスメント活動からのエビデンスが含まれる。[SP 800-160-1]は、システム開発ライフサイクルの一部としての要件エンジニアリングのプロセスについて説明している。

管理策は、組織の特定のセキュリティおよびプライバシーの目的を達成するため、および利害関係者のセキュリティおよびプライバシー要件を反映するために適切な保護手段および保護機能の記述と見なすことができる。システム要件を満たし、開発者および組織の責任を含むために、管理策が選択され、実装されている。管理策には、技術的、管理的、および物理的な側面を含めることができる。場合によっては、管理策の選択と実装のために、派生要件または生成された管理策パラメータ値の形で、組織による追加の仕様が必要になることがある。システム開発ライフサイクル内の管理策に適切なレベルの実装の詳細を提供するために派生要件および管理策パラメータ値が必要となる場合がある。

セキュリティとプライバシーに関するドキュメントの要件は、システム開発ライフサイクルのすべての段階に対応している。ドキュメントは、管理策の実装および操作に関するユーザおよび管理者向けガイダンスを提供する。このようなドキュメントで必要とされる詳細レベルは、システムのセキュリティ分類化または分類レベル、および組織がリスク対応の期待に応えるために能力、機能、またはメカニズムに依存する度合いに基づいている。要件には、許可される機能、ポート、プロトコル、およびサービスを指定する必須の構成設定を含めることができる。システム、システムコンポーネント、およびシステムサービスの受領基準は、組織の取得または調達の基準と同じ方法で規定される。

関連管理策:CM-6, CM-8, PS-7, SA-3, SA-5, SA-8, SA-11, SA-15, SA-16, SA-17, SA-21, SR-3, SR-5

拡張管理策:

(1) 取得プロセス | 管理策の機能特性

システム、システムコンポーネント、またはシステムサービスの開発者に、実装する管理策の機能特性の説明書を提供するよう要求する。

詳解:セキュリティおよびプライバシー管理策の機能特性は、管理策のインタフェースで見える機能(すなわち、セキュリティまたはプライバシー能力、機能、またはメカニズム)を記述し、特に、管理策の操作の内部の機能およびデータ構造を除外する。

関連管理策:なし

(2) 取得プロセス | 管理策のための設計および実装情報

システム、システムコンポーネント、またはシステムサービスの開発者に、以下を含む管理策の設計および実装情報[*選択(1 つ以上):セキュリティ関連の外部システムインタフェース;高レベルの設計;低レベルの設計;ソースコードまたはハードウェアの回路図;*[*設定:組織が定める設計および実装情報*]]を[*設定:組織が定める詳細レベル*]で提供するよう要求する。

詳解：組織は、ミッションおよび事業の要件、復元力と統合的信頼性の要件、および分析とテストの要件に基づいて、組織のシステム、システムコンポーネント、またはシステムサービスにおける管理策の設計と実装のために、文書に様々な詳細レベルを要求することがある。システムは複数のサブシステムに分割できる。システム内の各サブシステムには、1 つ以上のモジュールを含めることができる。システムの高レベルの設計は、サブシステムと、セキュリティ関連の機能を提供するサブシステム間のインタフェースの観点から表現されている。システムの低レベルの設計は、セキュリティ関連の機能を提供するモジュールとモジュール間のインタフェースの観点から表現されている。設計および実装の参照文書には、製造元、バージョン、シリアル番号、検証ハッシュ署名、使用されたソフトウェアライブラリ、購入またはダウンロードの日付、およびベンダまたはダウンロードソースを含めることができる。ソースコードとハードウェアの回路図は、システムの実装表現と呼ばれる。

関連管理策：なし

(3) 取得プロセス | 開発方法、技法、および実践

システム、システムコンポーネント、またはシステムサービスの開発者に、以下を含むシステム開発ライフサイクルプロセスの使用を実証することを要求する。

(a) **[*設定：組織が定めるシステムエンジニアリング方法*]。**

(b) **[*設定：組織が定める[選択（1 つ以上）：システムセキュリティ；プライバシー]エンジニアリング方法*]。**

(c) **[*設定：組織が定めるソフトウェア開発方法；テスト、評価、アセスメント、検証、および妥当性確認方法；および品質管理プロセス*]。**

詳解：最先端のソフトウェア開発方法、システムエンジニアリング方法、システムセキュリティとプライバシーエンジニアリング方法、および品質管理プロセスを含むシステム開発ライフサイクルに従うことで、システム、システムコンポーネント、およびシステムサービス内の潜在的なエラーの数と重大度を減らすことができる。このようなエラーの数と重大度を減らすことで、それらのシステム、コンポーネント、およびサービスの脆弱性の数を減らすことができる。開発者がシステムエンジニアリング、システムセキュリティとプライバシーエンジニアリング、ソフトウェア開発、コンポーネントとシステムのアセスメント、品質管理プロセスのために選択および実装する方法と技法の透明性は、取得されるシステム、システムコンポーネント、またはシステムサービスの統合的信頼性に対する保証のレベルを高める。

関連管理策：なし

(4) 取得プロセス | システムへのコンポーネントの割り当て

[撤回：CM-8(9)に組み込まれた]

(5) 取得プロセス | システム、コンポーネント、およびサービスの構成

システム、システムコンポーネント、またはシステムサービスの開発者には、以下を要求する。

(a) **[*設定：組織が定めるセキュリティ構成*]を実装して、システム、コンポーネント、またはサービスを提供する。**

(b) **構成を、以降のシステム、コンポーネント、またはサービスの再インストールまたはアップグレードのデフォルトとして使用する。**

詳解：セキュリティ構成の例には、米国政府共通設定基準（USGCB: the U.S. Government Configuration Baseline）、セキュリティ技術実装ガイド（STIG: Security Technical Implementation Guides）、および機能、ポート、プロトコル、サービスの制限などがある。セキュリティ特性には、デフォルトのパスワードの変更を要求することが含まれる。

関連管理策：なし

(6) 取得プロセス | 情報保証製品の使用

(a) **情報の伝送に使用されるネットワークが伝送される情報よりも低い分類レベルにある場合に国家機密情報を保護するために NSA 承認済みソリューションを構成**

する、政府調達向け既製品（GOTS）または商用既製品（COTS）の情報保証および情報保証対応情報技術製品のみを採用する。

(b) これらの製品が NSA によって、または NSA 承認済みの手順に従って評価および／または検証されていることを確認する。

詳解：暗号化手段で国家機密情報を保護するために使用される市販の IA または IA 対応の情報技術製品は、NSA 承認済み鍵管理を使用するために必要とされる場合がある。[NSA CSFC]を参照。

関連管理策：SC-8, SC-12, SC-13

(7) 取得プロセス | NIAP 承認済みプロテクションプロファイル

(a) 商業的に提供される情報保証および情報保証対応の情報技術製品の使用を、特定の技術タイプに対して、該当するプロファイルが存在する場合、国家情報保証パートナーシップ（NIAP：National Information Assurance Partnership）承認済みプロテクションプロファイルに対して正常に評価された製品に限定する。

(b) 特定の技術タイプに対して NIAP 承認済みのプロテクションプロファイルが存在しないが、商業的に提供されている情報技術製品がそのセキュリティポリシーを実施するために暗号機能に依存している場合、暗号モジュールが FIPS 検証済みまたは NSA 承認済みであることを要求する。

詳解：NIAP の詳細については、[NIAP CCEVS]を参照。FIPS 検証済み暗号モジュールの詳細については、[NIST CMVP]を参照。

関連管理策：IA-7, SC-12, SC-13

(8) 取得プロセス | 管理策の継続的監視計画

システム、システムコンポーネント、またはシステムサービスの開発者には、組織の継続的監視プログラムと一致している管理策の効果の継続的監視計画を作成する必要がある。

詳解：継続的な監視計画の目的は、システム、システムコンポーネント、またはシステムサービス内の計画され、要求され、展開された管理策が、発生する避けられない変化に基づいて、長期にわたって有効であり続けるかどうかを判断することである。開発者の継続的監視計画には、組織が実施する継続的監視プログラムに情報を組み込むことができるように、十分な詳細レベルが含まれている。継続的監視計画には、計画された管理策のアセスメントおよび監視活動のタイプ、管理監視の頻度、管理策が失敗または無効になった場合に取るべき措置を含めることができる。

関連管理策：CA-7

(9) 取得プロセス | 使用中の機能、ポート、プロトコル、およびサービス

システム、システムコンポーネント、またはシステムサービスの開発者に、組織での使用を目的とした機能、ポート、プロトコル、およびサービスを特定することを要求する。

詳解：システム開発ライフサイクルの早い段階（例えば、初期要件定義および設計段階）で機能、ポート、プロトコル、およびサービスの特性を見分けることにより、組織はシステム、システムコンポーネント、またはシステムサービスの設計に影響を与えることができる。システム開発のライフ サイクルに早期に関与することにより、組織は、不必要に高いリスクをもたらす機能、ポート、プロトコル、またはサービスの使用を回避または最小化すると共に、特定のポート、プロトコル、サービスを取りやめること、システムサービスプロバイダに要求することに伴うトレードオフを理解するのに役立つ。機能、ポート、プロトコル、およびサービスを早期に特定することで、システム、コンポーネント、またはシステムのサービスが実装された後の、コストのかかる管理策の改造を回避できる。SA-9 は、外部システムサービスの要件について説明している。組織は、外部ソースから提供される機能、ポート、プロトコル、およびサービスを特定する。

関連管理策：CM-7, SA-9

(10) 取得プロセス | 承認された PIV 製品の使用

組織のシステム内に実装された個人アイデンティティの検証（PIV：Personal Identity

Verification）機能には、FIPS 201 承認済み製品リストにある情報技術製品のみを採用する。

詳解：FIPS 201 承認済み製品リストの製品は、連邦政府職員および契約事業者の連邦政府職員用個人識別身分証に関する NIST 要件を満たしている。PIV カードは、システムや組織の多要素認証に使用される。

関連管理策：IA-2, IA-8, PM-9

(11) 取得プロセス｜記録システム

組織のミッションまたは機能を達成するために組織に代わって記録システムを運用するための取得契約に[*設定：組織が定めるプライバシー法の要件*]を含める。

詳解：契約により、組織が組織のミッションまたは機能を達成するために記録システムの運用を提供する場合、組織は、その権限と一致した[PRIVACT]の要件を記録システムに適用する。

関連管理策：PT-6

(12) 取得プロセス｜データオーナー

(a) 組織のデータオーナーに関する要件を取得契約に含める。

(b) すべてのデータを契約事業者のシステムから削除し、[*設定：組織が定める時間枠*]内に組織に戻すことを要求する。

詳解：契約を締結する組織が所有するデータを含むシステムを運用する契約事業者は、システムからデータを削除したり、契約で規定された期間内にデータを返却したりするためのポリシーと手順を導入する。

関連管理策：なし

参照資料：[PRIVACT], [OMB A-130], [ISO 15408-1], [ISO 15408-2], [ISO 15408-3], [ISO 29148], [FIPS 140-3], [FIPS 201-2], [SP 800-35], [SP 800-37], [SP 800-70], [SP 800-73-4], [SP 800-137], [SP 800-160-1], [SP 800-161], [IR 7539], [IR 7622], [IR 7676], [IR 7870], [IR 8062], [NIAP CCEVS], [NSA CSFC]

SA-5 システムドキュメント

管理策：

a. 以下を説明するシステム、システムコンポーネント、またはシステムサービスの管理者用ドキュメントを入手または作成する。

1. システム、コンポーネント、またはサービスのセキュアな構成、インストール、および操作。
2. セキュリティおよびプライバシー機能とメカニズムの効果的な使用と維持管理。
3. 管理機能または特権機能の構成および使用に関する既知の脆弱性。

b. 以下を説明するシステム、システムコンポーネント、またはシステムサービスのユーザドキュメントを入手または開発する。

1. ユーザがアクセス可能なセキュリティおよびプライバシー機能とメカニズム、およびそれらの機能とメカニズムを効果的に使用する方法。
2. 個人がシステム、コンポーネント、またはサービスをよりセキュアな方法で使用し、個人のプライバシーを保護することを可能にするユーザインタラクションの方法。
3. システム、コンポーネント、またはサービスのセキュリティと個人のプライバシーを維持するためのユーザの責任。

c. システム、システムコンポーネント、またはシステムサービスのドキュメントが入手できないか存在しない場合に、それらのドキュメントを入手するために[*設定：組織が定める措置*]を実行する。

d. [*設定：組織が定める職員または役割*]に文書を配布する。

詳解：システムドキュメントは、職員が管理策の実施と運用を理解するのに役立つ。組織は、提供されるコンテンツの品質と正確性を判断するための具体的な手段を確立することを考慮する。システムドキュメントは、サプライチェーンリスク、インシデント対応、およびその他の機能の管理を支援するために使用される場合がある。ドキュメントを必要とする職員または役割には、システムオーナー、システムセキュリティ担当者、およびシステム管理者が含まれる。ドキュメントを入手する試みには、製造業者または供給業者への連絡、ウェブベースの検索の実施が含まれる。システムまたはコンポーネントの古さ、または開発者や契約事業者からのサポートの欠如が原因で、ドキュメントを入手できない場合がある。ドキュメントを入手できない場合、組織は、それが管理策の実施または運用に不可欠である場合、ドキュメントを再作成する必要がある場合がある。ドキュメントに対して提供される保護は、システムのセキュリティの分類または機密性区分に見合ったものである。システムの脆弱性に対処するドキュメントでは、より高いレベルの保護が必要になる場合がある。システムのセキュアな運用には、システムを最初に起動すること、およびシステムの運用が停止した後にセキュアなシステム運用を再開することが含まれる。

関連管理策：CM-4, CM-6, CM-7, CM-8, PL-2, PL-4, PL-8, PS-2, SA-3, SA-4, SA-8, SA-9, SA-10, SA-11, SA-15, SA-16, SA-17, SI-12, SR-3

拡張管理策：

(1) システムドキュメント | セキュリティ管理策の機能的特性

［撤回：SA-4(1)に組み込まれた］

(2) システムドキュメント | セキュリティ関連の外部システムインタフェース

［撤回：SA-4(2)に組み込まれた］

(3) システムドキュメント | 高レベル設計

［撤回：SA-4(2)に組み込まれた］

(4) システムドキュメント | 低レベル設計

［撤回：SA-4(2)に組み込まれた］

(5) システムドキュメント | ソースコード

［撤回：SA-4(2)に組み込まれた］

参照資料：[SP 800-160-1]

SA-6 ソフトウェアの使用制限

［撤回：CM-10 および SI-7 に組み込まれた］

SA-7 ユーザがインストールしたソフトウェア

［撤回：CM-11 および SI-7 に組み込まれた］

SA-8 セキュリティおよびプライバシーエンジニアリングの原則

管理策：システムおよびシステムコンポーネントの仕様、設計、開発、実装、および変更において、［*設定：組織が定めるシステムセキュリティとプライバシーエンジニアリングの原則*］を適用する。

詳解：システムのセキュリティおよびプライバシーエンジニアリングの原則は、システム開発ライフサイクル全体に密接に関連し、実装されている（SA-3 を参照）。組織は、システムセキュリティとプライバシーエンジニアリングの原則を、開発中の新しいシステムまたはアップグレード中のシステムに適用できる。既存のシステムの場合、組織は、システムのセキュリティおよびプライバシーエンジニアリングの原則を、システム内のハードウェア、ソフトウェア、およびファームウェアコンポーネントの現在の状態を考慮して、可能な範囲でシステムのアップグレードおよび変更に適用する。

システムのセキュリティおよびプライバシーエンジニアリングの原則を適用することで、組織は統合的信頼性のある、セキュアで、回復力のあるシステムを開発し、中断、危険、脅威、および個人のプライバシー問題の発生に対する感受性を低減することができる。システムセキュリティエンジニアリングの原則の例には以下が含まれる：階層化された保護の開発；設計および開発の基盤としてのセキュリティおよびプライバシーポリシー、アーキテクチャ、および管理策の確立；システム開発ライフサイクルへのセキュリティおよびプライバシー要件の組み込み；物理的および論理的なセキュリティ境界の明確化；セキュアなソフトウェアを構築する方法について開発者が訓練されていることを保証すること；組織のニーズに合わせて管理策をテーラリングすること；脅威のモデル化を実行して、ユースケース、脅威エージェント、攻撃ベクトルとパターン、設計パターン、リスクを軽減するために必要な代替管理策を特定することなど。

システムのセキュリティおよびプライバシーエンジニアリングの概念と原則を適用する組織は、統合的信頼のあるセキュアなシステム、システムコンポーネント、およびシステムサービスの開発を促進し；リスクを許容レベルまで低減し；情報に基づいたリスクマネジメントの決定を行うことができる。システムセキュリティエンジニアリングの原則は、耐タンパー性のハードウェアを設計に組み込むなど、特定のサプライチェーンリスクから保護するためにも使用できる。

関連管理策：PL-8, PM-7, RA-2, RA-3, RA-9, SA-3, SA-4, SA-15, SA-17, SA-20, SC-2, SC-3, SC-32, SC-39, SR-2, SR-3, SR-4, SR-5

拡張管理策：

(1) セキュリティおよびプライバシーエンジニアリングの原則 | 明確な抽象化

明確な抽象化のセキュリティ設計原則を実装する。

詳解：明確な抽象化の原則は、システムには、データとデータの管理方法について一貫性のある直感的なビューを提供する、シンプルで明確に規定されたインタフェースと機能があることを示している。システムインタフェースの明確さ、単純さ、必要性、および十分性は、それらの機能動作の精密な規定と相まって、分析、検査、およびテストの容易さ、ならびにシステムの正確でセキュアな使用を促進する。抽象化の明確さは主観的である。この原則の適用を反映する例としては、冗長な未使用のインタフェースの回避；情報隠蔽；および、インタフェースまたはそれらのパラメータの多重定義の回避等が含まれる。情報隠蔽（すなわち、表現に依存しないプログラミング）は、公開された抽象化が影響を受けないように、データが内部でどのように管理されるかによって、あるシステムコンポーネントの情報の内部表現が、そのコンポーネントを起動したり呼び出したりする別のシステムコンポーネントから見えないようにするために使用される設計技法である。

関連管理策：なし

(2) セキュリティおよびプライバシーエンジニアリングの原則 | 最小共通メカニズム

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に最小共通メカニズムのセキュリティ設計原則を実装する。

詳解：最小共通メカニズムの原則は、複数のユーザに共通であり、すべてのユーザに依存するメカニズムの量が最小限に抑えられることを示している[POPEK74]。メカニズムの最小化とは、システムの異なるコンポーネントが同じメカニズムを使用してシステムリソースにアクセスすることを控えることを意味する。すべての共有メカニズム（特に共有変数を含むメカニズム）は、ユーザ間の潜在的な情報パスを表し、意図せずにセキュリティを侵害しないように注意深く設計されている[SALTZER75]。最小共通メカニズムの原則を実装することで、異なるプログラム間でシステム状態を共有することによる悪影響を減らすことができる。共有状態（共有変数を含む）を乱す、ある一つのプログラムは、その状態に依存する他のプログラムを乱す可能性がある。最小共通メカニズムの原則は、設計の簡素化の原則もサポートし、カバーストレージチャネルの問題に対処している[LAMPSON73]。

関連管理策：なし

(3) セキュリティおよびプライバシーエンジニアリングの原則 | モジュール性および階層化

[*設定：組織が定めるシステムまたはシステムコンポーネント*]にモジュール性と階層化のセキュリティ設計原則を実装する。

詳解：モジュール性および階層化の原則は、システムエンジニアリング分野全体の基本である。機能分解から導出されたモジュール性と階層化は、システムの構造を理解することを可能にすることにより、システムの複雑さを管理するのに効果的である。モジュールの分解やシステム設計の精細化は挑戦的であり、原則の総論に反している。モジュール性は、機能および関連するデータ構造を明確に規定された論理ユニットに分離する役割を果たしている。階層化を行うことにより、これらのユニットの関係をよりよく理解できるため、依存関係が明確になり、望ましくない複雑さを回避できる。モジュール性のセキュリティ設計原則は、機能モジュール性を拡張して、信用、統合的信頼性、権限、およびセキュリティポリシーに基づく考慮事項を含める。セキュリティ情報に基づくモジュール分解には、ネットワーク内のシステムへのポリシーの割り当て、システムアプリケーションの個別のアドレス空間を持つプロセスへの分離、システムポリシーのレイヤーへの割り当て、およびハードウェアでサポートされる特権ドメインに基づく個別の特権を持つサブジェクトへのプロセスの分離が含まれる。

関連管理策：SC-2, SC-3

(4) セキュリティおよびプライバシーエンジニアリングの原則 | 半順序の依存関係

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に半順序の依存関係のセキュリティ設計原則を実装する。

詳解：半順序の依存関係の原則は、システム内の同期、呼び出し、およびその他の依存関係が半順序であることを示している。システム設計における基本的な概念は階層化であり、これにより、システムは明確に規定された、機能的に関連するモジュールまたはコンポーネントに編成される。レイヤーは、上位レイヤーが下位レイヤーに依存するように、レイヤー間依存性に関して線形に配列されている。上位レイヤーに機能を提供する一方で、一部のレイヤーは自己完結型であり、下位レイヤーに依存しない場合がある。特定のシステム内のすべての機能を半順序とすることはできない場合があるが、循環依存関係がレイヤー内で発生するように制限されている場合、循環性の固有の問題をより簡単に管理できる。半順序の依存関係とシステムの階層化は、システム設計のシンプルさと一貫性に大きく貢献する。半順序の依存関係は、システムのテストと分析も容易にする。

関連管理策：なし

(5) セキュリティおよびプライバシーエンジニアリングの原則 | 効率的に仲介されたアクセス

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に効率的に仲介されたアクセスのセキュリティ設計原則を実装する。

詳解：効率的に仲介されたアクセスの原則は、ポリシー実施カニズムにおいては、表現された制約内で利害関係者の要件を満たしながら、利用可能な最も一般的でないメカニズムを利用することを示している。システムリソース（すなわち、CPU、メモリ、デバイス、通信ポート、サービス、インフラストラクチャ、データ、および情報）へのアクセスの仲介は、多くの場合、セキュアなシステムの主要なセキュリティ機能である。また、システムによって利害関係者に提供される機能の保護の実現も可能にする。システムが正しく設計されていない場合、リソースアクセスの仲介は、パフォーマンスのボトルネックになる可能性がある。例えば、ハードウェアメカニズムを使用することにより、効率的な仲介アクセスを実現できる。メモリなどの低レベルのリソースへのアクセスが行なわれると、ハードウェア保護メカニズムにより、境界外のアクセスが発生しないようにすることができる。

関連管理策：AC-25

(6) セキュリティおよびプライバシーエンジニアリングの原則 | 共有の最小化

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に、共有の最小化のセキュリティ設計原則を実装する。

詳解：共有の最小化の原則は、絶対にそうする必要がない限り、システムコンポーネント（例えば、サブジェクト、プロセス、機能）間でコンピュータリソースが共有されないことを示している。共有の最小化は、システムの設計と実装を簡素化するのに役立つ。ユーザドメインのリソースを任意のアクティブなエンティティから保護するために、その共有が明示的に要求および許可されていない限り、リソースは共有されない。リソース共有の必要性

は、内部エンティティの場合の共通メカニズムの最小化の設計原則によって動機付けられるか、または利害関係者の要件によって動機付けされる。ただし、内部共有は、パフォーマンス、隠しストレージ、およびタイミングチャネルの問題を回避するために慎重に設計されている。共通のメカニズムを介して共有すると、データおよび情報の認可されていないアクセス、開示、使用、または変更に対する感受性が高まり、システムが提供する固有の機能に悪影響を及ぼす可能性がある。共通のメカニズムによって引き起こされる共有を最小限にするために、そのようなメカニズムは、分離を維持するために再入可能とするかまたは仮想化されるように設計することができる。さらに、情報を共有するためのグローバルデータの使用は注意深く精査されている。カプセル化の欠如は、共有エンティティ間の関係を曖昧にする可能性がある。

関連管理策：SC-31

(7) セキュリティおよびプライバシーエンジニアリングの原則｜複雑さの軽減

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に複雑さの軽減セキュリティ設計原則を実装する。

詳解：複雑さの軽減の原則では、システム設計は可能な限り小ささくてシンプルな事を示している。小さくシンプルな設計は、理解しやすく、分析しやすく、エラーが発生しにくくなる。複雑さの軽減の原則は、システムのあらゆる側面に適用されるが、システムの緊急のセキュリティ特性に関するエビデンスを得るために実行される様々な分析のため、セキュリティにとって特に重要である。このような分析を成功させるには、小さくてシンプルな設計が不可欠である。複雑さの軽減の原則は、システムのあらゆる側面に適用されるが、システムの緊急のセキュリティ特性に関するエビデンスを取得するために実行される様々な分析のため、セキュリティにとって特に重要である。複雑さを軽減するという原則の適用は、システム開発者がシステムセキュリティ機能の適合性と正確性を理解するのに役立つ。また、潜在的な脆弱性の特定を容易にする。複雑さが軽減された当然の結果として、システムの単純性は、システムに含まれる脆弱性の数に直接関係しているとされている。つまり、単純なシステムほど脆弱性が少なくなる。複雑さが軽減されることの利点は、意図されたセキュリティポリシーがシステム設計にキャプチャされているかどうかを理解しやすくなること、およびエンジニアリング開発中に導入される脆弱性が少なくなる可能性があることである。追加の利点は、システム設計が本質的に複雑な状況で到達する結論とは対照的に、仕様への適合性、正確性、および脆弱性の存在についてのそのような結論に、より高い保証度で到達できることである。古い技術から新しい技術への移行（例えば、IPv4 から IPv6 への移行）では、移行期間中に古い技術と新しい技術を同時に実装する必要がある場合がある。これにより、移行中にシステムが一時的に複雑になる可能性がある。

関連管理策：なし

(8) セキュリティおよびプライバシーエンジニアリングの原則｜セキュアな保守拡張性

[*設定：組織が定めるシステムまたはシステムコンポーネント*]にセキュアな保守拡張性のセキュリティ設計原則を実装する。

詳解：セキュアな保守拡張性の原則は、システムの構造、インタフェース、相互接続（つまり、システムアーキテクチャ）、機能、または構成（つまり、セキュリティポリシー実施）に変更があった場合に、セキュリティ特性の維持を容易にするようにシステムが開発されることを示している。変更には、新規、拡張、またはアップグレードされたシステム機能；メンテナンスと維持活動；および再構成などが含まれる。システムの保守拡張のすべての側面を計画することは不可能であるが、システムのアップグレードと変更は、ミッションや事業の戦略的方向性、脅威環境の予想される変化、予想されるメンテナンスと維持のニーズを分析することによって予想できる。複雑なシステムが、そのような状況でセキュアなままであり続けることを期待するのは非現実的である。そのような状況が運用環境に関連しているか、使用に関連しているかどうかにかかわらず、開発中には想定されていない状況でセキュアなままであり続けるシステムである。システムはいくつかの新しい状況でセキュアである可能性はあるが、その緊急動作が常にセキュアであるという保証はない。統合的信頼性を最初からシステムに組み込む方が簡単であり、システムの統合的信頼性を維持するには、アドホックまたは非体系的な方法ではなく、変更を計画する必要がある。この原則の利点には、ベンダのライフサイクルコストの削減、所有コストの削減、システムセキュリティの向上、セキュリティリスクのより効果的な管理、およびリスクの不確実性の低減など

がある。

関連管理策：CM-3

(9) セキュリティおよびプライバシーエンジニアリングの原則｜信頼できるコンポーネント

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に信頼できるコンポーネントのセキュリティ設計原則を実装する。

詳解：信頼できるコンポーネントの原則は、コンポーネントが、サポートするセキュリティの依存関係に見合ったレベル（すなわち、他のコンポーネントがそのセキュリティ機能を実行するためにどれだけ信頼できるか）まで統合的信頼性があることを示している。この原則は、統合的信頼性が不注意に低下したり、結果として信頼が失われることがないように、コンポーネントの構成を可能にする。結局のところ、この原則は、コンポーネントへの信頼とコンポーネントの統合的信頼性を同じ抽象スケールで測定できるいくつかの測定基準を要求する。信頼できるコンポーネントの原則は、信頼関係の複雑な連鎖があるシステムおよびコンポーネントを考慮する場合に特に関連する。信頼の依存状態は、信頼関係とも呼ばれ、信頼関係の連鎖が存在する場合がある。

信頼できるコンポーネントの原則は、様々なレベルの統合的信頼性を有する可能性のあるサブコンポーネント（例えば、サブシステム）からなる複合コンポーネントにも適用される。控えめな仮定では、複合コンポーネントの統合的信頼性は、その中の最も信頼性の低いサブコンポーネントの統合的信頼性である。特定の複合コンポーネントの信頼性が控えめな仮定よりも大きいというセキュリティエンジニアリングの根拠を提供することが可能な場合がある。ただし、そのような論理的根拠は、統合的信頼性の目的の明確な記述と、関連する信頼できるエビデンスに基づく論理的推論を反映している。複合コンポーネントの統合的信頼性は、コンポーネント内の多層防御またはコンポーネントの複製の適用の増加と一致しない。多層防御技法は、全体の統合的信頼性を、最も信頼性の低いコンポーネントの統合的信頼性よりも高くするものではない。

関連管理策：なし

(10) セキュリティおよびプライバシーエンジニアリングの原則｜階層的信頼

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に階層的信頼のセキュリティ設計原則を実装する。

詳解：コンポーネントの階層的信頼の原則は、信頼できるコンポーネントの原則に基づいており、システムのセキュリティ依存関係が、信頼できるコンポーネントの原則を維持する場合、半順序を形成すると述べている。半順序は、異種の信頼できるコンポーネントからセキュアなシステムを構成する際の、統合的信頼性の推論または保証ケース（保証論）の基礎を提供する。異種の信頼性のあるコンポーネントで構成されるシステムの統合的信頼性を分析するには、統合的信頼性に関する循環依存関係を排除することが不可欠である。システムの下位層にあるより信頼性の高いコンポーネントが上位層のより信頼性の低いコンポーネントの影響を受ける場合、事実上、信頼できるコンポーネントの原則に従って、これらのコンポーネントを上位層のコンポーネントと同じ「信頼性の低い」クラスに置くことになる。信頼関係、または信頼の連鎖は、様々な形で現れる。例えば、証明書階層のルート証明書は、階層内で最も信頼できるノードであるのに対し、階層内の葉ノードは最も統合的信頼性の低いノードである可能性がある。別の例は、システムの最下層にあるセキュリティカーネル（ハードウェアベースを含む）が最も信頼できるコンポーネントである階層化された高保証システムとして見られる。ただし、階層的信頼の原則は、過度に信頼できるコンポーネントの使用を禁止するものではない。信頼性の低いシステムでは、信頼性の低いコンポーネントではなく（例えば、可用性や他の費用対効果の要因により信頼性の高いコンポーネントを採用することが合理的である場合がある。このような場合、信頼性の高いコンポーネントが信頼性の低いコンポーネントに依存しても、結果として生じる低信頼性システムの統合的信頼性は低下しない。

関連管理策：なし

(11) セキュリティおよびプライバシーエンジニアリングの原則｜逆変更しきい値

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に逆変更しきい値のセキュリティ設計原則を実装する。

詳解：逆変更しきい値の原則は、信頼できるコンポーネントの原則と階層的信頼の原則に基づいており、コンポーネントに提供される保護の程度はその統合的信頼性に見合っていると述べている。コンポーネントへの信頼が高まるにつれて、コンポーネントの認可されていない変更に対する保護も同様に高まる。認可されていない変更からの保護は、コンポーネント自体の自己保護および生来の統合的信頼性の形でもたらされるか、またはセキュリティアーキテクチャの他の要素または属性からコンポーネントに与えられた保護から行なうことも出来る（動作環境における保護を含むため）。

関連管理策：なし

(12) セキュリティおよびプライバシーエンジニアリングの原則 | 階層的保護

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に階層的保護のセキュリティ設計原則を実装する。

詳解：階層的保護の原則では、コンポーネントをより信頼できるコンポーネントから保護する必要はないことを示している。最も信頼できるコンポーネントが低下したものに接するケースでは、他のすべてのコンポーネントから自分自身を保護する。例えば、オペレーティングシステムのカーネルがシステムで最も信頼できるコンポーネントであると見なされた場合、オペレーティングシステムのカーネルは、サポートするすべての信頼できないアプリケーションから自身を保護するが、逆に、アプリケーションをカーネルから保護する必要はない。ユーザの統合的信頼性は、階層的保護の原則を適用する際の考慮事項である。信頼できるシステムは、ユーザが非常に信頼できる「システムハイ」環境での信頼できないシステムの使用を反映し、「システムハイ」実行環境をバインドして保護する他の保護が導入されている場合、同様に信頼できるユーザから自身を保護する必要はない。

関連管理策：なし

(13) セキュリティおよびプライバシーエンジニアリングの原則 | 最小化されたセキュリティ要素

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に最小化されたセキュリティ要素のセキュリティ設計原則を実装する。

詳解：最小化されたセキュリティ要素の原則は、システムに無関係な信頼できるコンポーネントがないことを示している。セキュリティ要素の最小化の原則には、セキュリティ分析の全体的なコストとセキュリティ分析の複雑さという 2 つの側面がある。信頼できるコンポーネントは、開発プロセスの厳格さが増しているため、一般に構築と実装にコストがかかる。信頼されたコンポーネントは、それらの統合的信頼性を評価するために、より高度なセキュリティ分析を必要とする。したがって、セキュリティ分析のコストを削減し、複雑さを軽減するために、システムは、可能な限り少ない信頼できるコンポーネントで構成される。信頼できるコンポーネントとシステムの他のコンポーネントとの相互作用の分析は、システムセキュリティ検証の最も重要な側面の 1 つである。コンポーネント間の相互作用が不必要に複雑である場合、システムのセキュリティは、内部の信頼関係が単純かつ洗練されて構築されたものよりも確認することが困難になる。一般に、信頼できるコンポーネントが少ないほど、内部の信頼関係が少なくなり、システムがシンプルになる。

関連管理策：なし

(14) セキュリティおよびプライバシーエンジニアリングの原則 | 最小特権

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に最小特権のセキュリティ設計原則を実装する。

詳解：最小特権の原則では、各システムコンポーネントには、指定された機能を実行するのに十分な特権が割り当てられているが、それ以上の特権は割り当てられていない。最小特権の原則を適用すると、コンポーネントのアクションの範囲が限定され、これには、2 つの望ましい影響がある。コンポーネントの障害、破損、または誤用によるセキュリティへのインパクトは最小限に抑えられ、コンポーネントのセキュリティ分析は、簡略化される。最小特権は、セキュアなシステム設計のすべての側面に反映されている一般的な原則である。コンポーネント機能を呼び出すために使用されるインタフェースは、ユーザ集団の特定のサブセットのみが使用でき、コンポーネント設計は、特権分解の十分に細かい粒度をサポートしている。例えば、監査メカニズムの場合、監査設定を構成する監査マネージャ

一用のインタフェース；監査データが安全に収集および保管されることを保証する監査オペレータのためのインタフェース；および、収集された監査データを表示するだけで、そのデータに対して操作を実行する必要がない監査レビューアのためのさらに別のインタフェースなどが存在する場合がある。

システムインタフェースでの明示に加えて、最小特権は、システム自体の内部構造の指針として使用することができる。内部最小特権の 1 つの側面は、モジュールによってカプセル化された要素のみがモジュール内の関数によって直接操作されるようにモジュールを構築することである。モジュールの操作によって影響を受ける可能性のあるモジュールの外部の要素は、それらの要素を含むモジュールとの相互作用（例えば、関数呼び出しを介して）を通じて間接的にアクセスされる。内部最小特権の別の側面は、所定のモジュールまたはコンポーネントのスコープに、その機能に必要なシステム要素のみが含まれ、要素のアクセスモード（例えば、読み取り、書き込み）が最小限であることである。

関連管理策：AC-6, CM-7

(15) セキュリティおよびプライバシーエンジニアリングの原則｜根拠のある許可

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に根拠のある許可のセキュリティ設計原則を実装する。

詳解：根拠のある許可の原則では、システム設計者は、非常に重要な操作や機微性の高いデータ、情報、またはリソースへのアクセスを続行する前に、複数の権限のあるエンティティに同意を求めることを考慮することを定めている。[SALTZER75]では根拠のある許可を特権の分離と独自に名付けている。職務分離と同等である。複数の当事者間で権限を分割することにより、悪用の可能性が減少し、事故、ごまかし行為、あるいは信頼のブリーチなど、重大な影響をもたらす可能性のある復旧不可能な行為を可能にすることがおこらないような保全措置が提供される。そのようなメカニズムの設計オプションには、同時行動（例えば、核兵器の発射が、2 人の異なる権限のある個人が短い時間枠内に正しい命令を与えることを必要とする）または後続する各操作は先行する操作によって有効化されるが、一人では一つの操作しか有効にできないという一連の操作などがある。

関連管理策：AC-5

(16) セキュリティおよびプライバシーエンジニアリングの原則｜自立した統合的信頼性

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に自立した統合的信頼性のセキュリティ設計原則を実装する。

詳解：自立した統合的信頼性の原則は、システムが他のシステムへの統合的信頼性を最小化することを述べている。システムはデフォルトで信頼でき、外部エンティティへの接続はその機能を補足するために使用される。システムがその統合的信頼性を維持するために別の外部エンティティとの接続を維持する必要がある場合、そのシステムは、その接続の喪失または劣化を引き起こす可能性のある悪意のある脅威および悪意のない脅威に対して脆弱である。自立した統合的信頼性の原則の利点は、システムを分離することにより、システムの脆弱性が低くなることである。この原則の当然の帰結は、システム（またはシステムコンポーネント）が分離して動作し、他のコンポーネントと再結合したときに、それらのコンポーネントと再同期する能力に関係する。

関連管理策：なし

(17) セキュリティおよびプライバシーエンジニアリングの原則｜セキュアな分散構成

[*設定：組織が定めるシステムまたはシステムコンポーネント*]にセキュアな分散構成のセキュリティ設計原則を実装する。

詳解：セキュアな分散構成の原則は、同じシステムセキュリティポリシーを実施する分散コンポーネントの構成では、個々のコンポーネントと同様に少なくともそのポリシーを適用するシステムをもたらすことを述べている。セキュアなシステムの設計原則の多くは、コンポーネントがどのように相互作用できるか、または相互作用する事が望ましいかを扱う。分散コンポーネントの構成から機能を作成または有効化する必要があるため、これらの原則の関連性が高まる可能性がある。特に、セキュリティポリシーをスタンドアロンから分散システムまたはシステムオブシステムに変換すると、予期しない結果またはこれまでになかったような結果が生じる可能性がある。通信プロトコルと分散データ整合性メカニズム

は、分散システム全体で一貫してポリシーを実施するのに役立つ。正しいポリシー実施をシステム全体で保証するためには、分散複合システムのセキュリティアーキテクチャは十分に分析される必要がある。

関連管理策：なし

(18) セキュリティおよびプライバシーエンジニアリングの原則｜信頼できる通信チャネル

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に信頼できる通信チャネルのセキュリティ設計原則を実装する。

詳解：信頼できる通信チャネルの原則は、コンポーネント間の通信（つまり、コンポーネント間の相互接続）に潜在的な脅威があるシステムを構成する場合、各通信チャネルは、サポートするセキュリティの依存関係（つまり、セキュリティ機能を実行するために他のコンポーネントからどれだけ信頼されているか）に見合ったレベルで信頼できると述べている。信頼できる通信チャネルは、通信チャネルへのアクセスを制限すること（通信に関与するエンドポイントの統合的信頼性を確実に一致させるため）と、通信チャネルを介して伝送されるデータにエンドツーエンドの保護（傍受や改ざんから保護し、適切なエンドツーエンド通信の保証をさらに強化するため）を適用することの組み合わせで実現される。

関連管理策：SC-8, SC-12, SC-13

(19) セキュリティおよびプライバシーエンジニアリングの原則｜継続的な保護

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に継続的な保護のセキュリティ設計原則を実装する。

詳解：継続的な保護の原則では、セキュリティポリシーを実施するために使用されるコンポーネントとデータには、セキュリティポリシーとセキュリティアーキテクチャの前提条件に一致する中断のない保護機能があることを示している。保護にギャップがある場合、システムがその設計能力に対して機密性、完全性、可用性、およびプライバシー保護を提供できるという保証はない。提供された機能をセキュアにする機能に関するいかなる保証も、データと情報が継続的に保護されることを必要としている。つまり、システムの制御下にある間は、データおよび情報が保護されないままになっている期間はない（すなわち、データおよび情報の作成、保管、処理、または通信中、ならびにシステムの初期化、実行、障害、中断、シャットダウンしている間も同様である）。継続的な保護には、リファレンスモニタの概念の指針（すなわち、すべての要求はリファレンスモニタによって検証されること；リファレンスモニタは、改ざんから保護することができること；メカニズムの適合性と正確性の十分な保証は、分析とテストから確認できること）およびセキュアな障害と復旧の原則（すなわち、エラー、欠陥、障害、および成功した攻撃などの間におけるセキュアな状態の保持；通常、縮退、または代替の動作モードへの復旧時のセキュアな状態の保持）を遵守する必要がある。

継続的な保護は、すべての運用機能を提供するシステムや部分的な運用機能を提供する縮退モード構成など、様々な構成で動作するように設計されたシステムにも適用される。継続的な保護の原則では、システムのセキュリティポリシーの変更が、構成を推進する運用上の必要性にトレーサビリティがあり、検証可能である必要がある（つまり、提案された変更によってシステムがセキュアでない状態になることがないことを検証できる）。トレーサビリティと検証が不十分であると、問題の複雑なまたは決定不可能な性質のために、一貫性のない状態または保護の不連続が生じる可能性がある。新しいセキュリティポリシーを反映する事前検証済みの構成定義を使用することで、古いポリシーから新しいポリシーへの移行が本質的に不可分であり、古いポリシーからの残りの影響が新しいポリシーと矛盾しないことが保証されることを分析による判断が可能になる。継続的な保護を実証する能力は、利害関係者のセキュリティ要件としてのライフサイクル保護のニーズの明確な表現に基づいている。

関連管理策：AC-25

(20) セキュリティおよびプライバシーエンジニアリングの原則｜セキュアなメタデータ管理

[*設定：組織が定めるシステムまたはシステムコンポーネント*]にセキュアなメタデータ管理のセキュリティ設計原則を実装する。

詳解：セキュアなメタデータ管理の原則では、ポリシーが情報の正確な保護を必要とする

場合、またはセキュリティサブシステムが自己保護的である場合、メタデータはセキュリティポリシーに関する「ファーストクラス」オブジェクトであると規定されている。セキュアなメタデータ管理の原則は、システム、サブシステム、またはコンポーネントが、適切な実行のために依存するデータを保護しない限り、自己保護を実現できないという認識によって推進される。通常、データはそれを格納するシステムによって解釈されない。それは、データを処理するユーザおよびプログラムにとって意味的価値を有する可能性がある（すなわち、情報を含む）。対照的に、メタデータは、ファイル名やファイルが作成された日付など、データに関する情報である。メタデータは、システムが解釈できる方法で記述されている標的データにバインドされているが、その標的データ内またはその近傍に格納する必要はない。自己参照メタデータを含む、それ自体がメタデータ（例えば、ファイル名の機密性区分レベルまたはインパクトレベル）を標的とするメタデータが存在する場合がある。

メタデータの明らかな二次的な性質は、保護の正当な必要性を無視することにつながり、情報の漏出を含むセキュリティポリシーに違反する可能性がある。メタデータの不十分な保護に関連する特定の懸念は、マルチレベルセキュア（MLS: multilevel secure）システムに関連している。MLS システムは、相対的な機微性レベルに基づいて、対象者によるオブジェクトへのアクセスを仲介する。したがって、MLS システムの管理範囲内にあるすべてのサブジェクトとオブジェクトは、直接的に、または間接的に機微性レベルに起因してラベル付けされる。MLS システムのラベル付けされたメタデータの当然の結果は、メタデータを含むオブジェクトがラベル付けされていることを示している。データの保護ニーズのアセスメントと同様に、機密性および完全性の保護が、ミッション、ビジネス、およびシステムデータに対して行われるように、個別に評価、指定、およびメタデータに割り当てられるように注意が払われる。

関連管理策：なし

(21) セキュリティおよびプライバシーエンジニアリングの原則 | 自己分析

***[設定：組織が定めるシステムまたはシステムコンポーネント]*に自己分析のセキュリティ設計原則を実装する。**

詳解：自己分析の原則は、システムコンポーネントでは、実行の様々な段階でシステムの内部状態と機能性を限定的にアセスメントできること、およびこの自己分析機能は、システムに投入された統合的信頼性のレベルに見合ったものであると規定されている。システムレベルでは、ボトムアップ方式で確立された統合的信頼性の階層的アセスメントを通じて自己分析を達成することができる。このアプローチでは、下位レベルのコンポーネントは、上位レベルのコンポーネントのデータの完全性と適正な機能性を（限定された範囲で）チェックする。例えば、信頼できるブートシーケンスには、次に高いレベルのコンポーネントの統合的信頼性を証明する信頼できる下位レベルのコンポーネントが含まれるため、推移的な信頼チェーンを確立できる。基本的には、コンポーネントは通常、その完全性に関する公理的または環境的に強制された仮定を含め、それ自体を証明する。自己分析の結果は、外部から引き起こされたエラー、内部の誤動作、または一時的なエラーから保護するために使用できる。この原理に従うことにより、エラーまたは誤動作の影響をコンポーネントの外部に伝播させることなく、いくつかの単純な誤動作またはエラーを検知することができる。さらに、セルフテストを使用して、コンポーネントの構成を証明し、予想される構成に関する矛盾の可能性を検知することができる。

関連管理策：CA-7

(22) セキュリティおよびプライバシーエンジニアリングの原則 | 説明責任およびトレーサビリティ

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に説明責任およびトレーサビリティのセキュリティ設計原則を実装する。

詳解：説明責任およびトレーサビリティの原則は、セキュリティに関連するアクション（つまり、サブジェクトとオブジェクトの相互作用）を、その代理としてアクションが実行されるエンティティまで追跡することが可能であると述べている。説明責任とトレーサビリティの原則は、システムのセキュリティに影響を与えるアクションに関する詳細を記録できる信頼できるインフラストラクチャ（監査サブシステムなど）を必要とする。アクションに関する詳細を記録するために、システムは、アクションが実行されているエンティティを一意に識別し、実行されたアクションの関連シーケンスを記録することもできる。また、説明責任ポリシーで

は、監査証跡を認可されていないアクセスや変更から保護される必要がある。最小特権の原則は、説明責任の粒度を高めるため、特定のエンティティへのアクションの追跡を支援する。特定のアクションをシステムエンティティ、最終的にはユーザに関連付け、監査証跡を不正なアクセスや変更から保護することで、アクションが記録されると監査証跡を変更することができないため、否認防止性が提供される。説明責任とトレーサビリティが果たすもう 1 つの重要な機能は、セキュリティポリシーの違反に関連するイベントの日常分析やフォレンジック分析にある。監査ロギングの分析は、セキュリティポリシーの違反を許した経路またはコンポーネントおよびセキュリティポリシーの違反に関連する個人の行動を特定するのに役立つかもしれない追加情報を提供しても良い。

関連管理策：AC-6, AU-2, AU-3, AU-6, AU-9, AU-10, AU-12, IA-2, IR-4

(23) セキュリティおよびプライバシーエンジニアリングの原則｜セキュアデフォルト

[*設定：組織が定めるシステムまたはシステムコンポーネント*]にセキュアデフォルトのセキュリティ設計原則を実装する。

詳解：セキュアデフォルトの原則は、システムのデフォルト構成（その構成サブシステム、コンポーネント、およびメカニズムを含む）が、セキュリティポリシーの限定的かつ保守的な実施を反映していることを述べている。セキュアデフォルトの原則は、システムの初期（すなわちデフォルト）構成に加えて、「明示的に認可されない限り拒否」戦略に従うアクセス制御およびその他のセキュリティ機能のセキュリティエンジニアリングおよび設計に適用される。。この原則の初期設定の側面では、システム、サブシステム、またはシステムコンポーネントの「出荷時」の設定が、セキュリティポリシーの違反を助長しないことが要求され、また、セキュリティポリシー自体が運用ユーザによる設定を必要とする場合には、システムがデフォルト設定で動作するのを防ぐことができる。

デフォルトの制限とは、システムが適切な自己保護機能を備えた「出荷時の状態」で動作し、意図したセキュリティポリシーとシステム構成が確立される前にセキュリティブリーチを防止できることを意味する。「出荷時」の製品によって提供される保護が不十分な場合、利害関係者は、セキュアな初期状態を確立する前にそれを使用するリスクを評価する。セキュアなデフォルトの原則を順守することにより、初期化が正常に完了したときにシステムがセキュアな状態で確立されることが保証される。システムが初期化に失敗した状況では、セキュアデフォルトを使用して要求された操作を実行するか、動作しないかのどちらかである。障害を検知して復旧する機能を提供するためには、この原則に対応する継続的な保護とセキュアな障害および復旧の原則を参照。

この原則に対するセキュリティエンジニアリングアプローチでは、リクエストが適切な形式であり、セキュリティポリシーと一致していることが判明しない限り、セキュリティメカニズムはリクエストを拒否すると述べている。セキュアでない代替策は、ポリシーと矛盾していることが示されていない限り、リクエストを許可することである。大規模なシステムでは、デフォルトで拒否された要求を許可するために満たされる条件は、デフォルトで許可された要求を拒否するためにチェックする必要がある条件よりもはるかにコンパクトで正確な場合が多い。

関連管理策：CM-2, CM-6, SA-4

(24) セキュリティおよびプライバシーエンジニアリングの原則｜セキュアな障害および復旧

[*設定：組織が定めるシステムまたはシステムコンポーネント*]にセキュアな障害および復旧のセキュリティ設計原則を実装する。

詳解：セキュアな障害および復旧の原則では、システムの機能またはメカニズムの障害も、障害への応答としての復旧アクションも、セキュリティポリシーの違反につながることはない。セキュアな障害と復旧の原則は、システムが(制限内で)実際の障害と差し迫った障害を、その操作の任意の段階（すなわち、初期化、通常の操作、シャットダウン、および保守）で検知できることを保証するもので、セキュリティポリシーに違反しないように適切な措置を講じるための継続的な保護の原則と同様な関係にある。さらに、指定された場合、システムは、セキュリティポリシーに違反しないようにセキュアな状態が維持されることを保証しながら、差し迫った障害または実際の障害から復旧して、通常の、縮退した、あるいは代替のセキュアな動作を再開することができる。

障害とは、コンポーネントの動作が、明示的に文書化された入力の指定された動作または期待される動作から逸脱する状態のことである。障害のあるセキュリティ機能が検知されると、システムはセキュリティを維持しながら、それ自体を再構成して、障害を起こしたコンポーネントを迂回し、元のシステムの機能のすべてまたは一部を提供するか、完全にシャットダウンすることで、セキュリティポリシーへの違反を防止する。これを実現するために、システムの再構成機能は、再構成の様々な段階でセキュリティポリシーが継続的に実施されるように設計されている。

障害から復旧するために使用できるもう 1 つの手法は、セキュアな状態（初期状態である可能性がある）にロールバックを実行し、セキュアな操作を再開できるように、障害が発生したサービスまたはコンポーネントをシャットダウンまたは置き換えることである。コンポーネントの障害は、それを使用しているコンポーネントが検知できる場合とできない場合がある。セキュアな障害の原則は、コンポーネントはアクセスを許可した後ではなく、拒否した状態で障害を起こすことを示している。例えば、完了前に中断された名目上「アトミック」な操作はセキュリティポリシーに違反せず、高レベルの最小単位およびロールバックメカニズム（トランザクションなど）を使用して中断イベントを処理するように設計されている。サービスが使用されている場合、その最小単位の特性は十分に文書化され、特徴付けされているため、そのサービスを利用するコンポーネントは、中断イベントを適切に検知して処理できる。例えば、システムは切断に適切に対応し、切断後の再同期とデータの整合性をサポートするように設計されている。

ポリシー実施メカニズムの複製を採用する障害防御戦略は、「多層防御」と呼ばれることもあり、1 つのメカニズムがシステムの保護に失敗した場合でも、システムをセキュアな状態で継続させることができる。ただし、メカニズムが類似している場合、敵対者は単純に連続して攻撃できるため、追加の保護は非現実的である可能性がある。同様に、ネットワーク化されたシステムでは、1 つのシステムまたはサービスのセキュリティを破ると、攻撃者が他の同様の複製されたシステムおよびサービスで同じことを行う可能性がある。機能が大幅に異なる複数の保護メカニズムを採用することにより、攻撃の複製や繰り返しの可能性を減らすことができる。分析は、リソース使用量の増加やシステム全体のパフォーマンスへの悪影響に対して、このような冗長性技術のコストと利点を比較検討するために行われる。動的動作の場合と同様に、これらのメカニズムの複雑さが増すにつれて、追加の分析が行われる。複雑さが増すと、一般に統合的信頼性が低下する。リソースを継続的に保護できない場合は、リソースが再びセキュアな状況で使用される前に、セキュリティのブリーチを検知して修復することが重要である

関連管理策：CP-10, CP-12, SC-7, SC-8, SC-24, SI-13

(25) セキュリティおよびプライバシーエンジニアリングの原則 | 経済的セキュリティ

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に経済的セキュリティのセキュリティ設計原則を実装する。

詳解：経済的セキュリティの原則は、セキュリティメカニズムは、セキュリティのブリーチによって発生する可能性のある損害よりもコストがかかるものではないと述べている。これは、リスク管理で使用される費用便益分析のセキュリティ関連形式である。費用便益分析の費用仮定は、システム設計者が必要以上の強さのセキュリティメカニズムを組み込むことを妨げ、メカニズムの強さは費用に比例する。経済的セキュリティの原則は、関連性のある信頼できるエビデンスを取得するために費やされた努力の観点から、その保証の費用に対する保証の便益の分析、ならびにエビデンスから統合的信頼性とリスクの結論を評価し引き出すために必要な分析も必要とする。

関連管理策：RA-3

(26) セキュリティおよびプライバシーエンジニアリングの原則 | パフォーマンスセキュリティ

[*設定：組織が定めるシステムまたはシステムコンポーネント*]にパフォーマンスセキュリティのセキュリティ設計原則を実装する。

詳解：パフォーマンスセキュリティの原則では、セキュリティメカニズムはシステムのパフォーマンスを不必要に低下させないように構築されているとされている。パフォーマンスとセキュリティに関する利害関係者とシステム設計の要件は、明確に規定され、優先順位が

付けられている必要がある。システムの実装がその設計要件を満たし、利害関係者に受け入れられることがわかった場合（すなわち、利害関係者の要件に対する妥当性確認）、設計者は、機能のパフォーマンスのニーズが保護のニーズに課す特定の制約を遵守する。計算集約型のセキュリティサービス（暗号技術など）は、優先順位の高いパフォーマンスの考慮事項に大きなインパクトを与えないか、または、信頼できる保護のために、性能とのトレードオフが許容できるかである。トレードオフの考慮事項には、利用できないか不十分でない限り、計算量の少ないセキュリティサービスが含まれる。セキュリティサービスが不十分かどうかは、機能的能力とメカニズムの強さによって決定される。メカニズムの強度は、セキュリティ要件、パフォーマンスが重要なオーバーヘッドの問題（暗号鍵管理など）、および脅威に対する能力のアセスメントに関して選択される。

パフォーマンスセキュリティの原則は、セキュリティポリシーの実施に役立つ、高レベルのサービスを構築できる低レベルのハードウェアメカニズムなど、最小限のオーバーヘッドしか発生しない機能の組み込みにつながる。このような低レベルのメカニズムは通常、かなり特殊なもので、機能が非常に限定されており、パフォーマンスが最適化されている。例えば、メモリの一部へのアクセス権が付与されると、多くのシステムはハードウェアメカニズムを使用して、以降のすべてのアクセスで正しいメモリアドレスとアクセスモードが使用されるようにする。この原則を適用すると、システムにセキュリティを一から設計する必要性が高くなり、上位レベルのメカニズムの構成要素として使用できる単純なメカニズムを下位層に組み込む必要性が高まる。

関連管理策：SC-12, SC-13, SI-2, SI-7

(27) セキュリティおよびプライバシーエンジニアリングの原則｜人的要因によるセキュリティ

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に人的要因によるセキュリティのセキュリティ設計原則を実装する。

詳解：人的要因によるセキュリティの原則では、セキュリティ機能とサポートサービスのユーザインタフェースは直感的でユーザフレンドリーであり、そのようなポリシーとその実施に影響を与えるユーザアクションについてフィードバックを提供する。セキュリティポリシーを実施するメカニズムは、ユーザの邪魔にならず、ユーザの効率を低下させないように設計されている。セキュリティポリシー実施メカニズムは、セキュアでない選択がなされた場合に、意味のある明確で関連性のあるフィードバックと警告をユーザに提供する。システム管理および運用を担当する職員がセキュリティポリシーを構成および実施するためのインタフェースに特に注意が払われる。理想的には、これらの職員は自分の選択のインパクトを理解することができることが求められる。システム管理責任および運用責任を負う職員は、システムの起動前にシステムを構成し、システムのメカニズムに意図が正しくマッピングされていることを確信して、実行時にシステムを管理することができる。セキュリティサービス、機能、およびメカニズムは、システムの意図された使用を妨げたり、不必要に複雑にすることはない。システムの使いやすさとセキュリティポリシーの実施に必要な厳格さの間にはトレードオフがある。セキュリティメカニズムがもどかしいか、または使用するのが難しい場合、ユーザはそれらを無効にするか、回避するか、またはメカニズムが満たすように設計されたセキュリティ要件および保護ニーズと矛盾する方法で使用しても良い。

関連管理策：なし

(28) セキュリティおよびプライバシーエンジニアリングの原則｜許容可能なセキュリティ

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に許容可能なセキュリティのセキュリティ設計原則を実装する。

詳解：許容可能なセキュリティの原則では、システムが提供するプライバシーとパフォーマンスのレベルがユーザの期待と一致している必要がある。個人のプライバシーの認識は、ユーザの行動、士気、および有効性に影響を与える可能性がある。組織のプライバシーポリシーとシステム設計に基づいて、ユーザは自分のプライバシーを保護するためにアクションを制限できることが望ましい。システムが直感的なインタフェースを提供できない、またはプライバシーとパフォーマンスの期待に応えられない場合、ユーザはシステムを完全に回避するか、非効率的またはセキュアでない方法で使用するかを選択できる。

関連管理策：なし

(29) セキュリティおよびプライバシーエンジニアリングの原則 | 再現性のある文書化された手順

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に再現性のある文書化された手順のセキュリティ設計原則を実装する。

詳解：再現性のある文書化された手順の原則は、システムコンポーネントを構築するために採用された技術および方法により、同じコンポーネントを後で正確かつ適切に再構築できることを示している。再現性のある文書化された手順は、以前に作成されたコンポーネントと同一のコンポーネントの開発をサポートしており、広く使用されている可能性がある。他のシステム成果物（例えば、ドキュメントやテスト結果）の場合、再現性は一貫性と成果物を検査する能力をサポートする。再現性のある文書化された手順は、システム開発ライフサイクルの様々な段階で導入でき、システムに求められる保証レベルを評価する能力に貢献できる。例としては、コードの開発とレビューの体系的な手順、開発ツールとシステム成果物の構成管理の手順、およびシステム配信の手順などがある。

関連管理策：CM-1, SA-1, SA-10, SA-11, SA-15, SA-17, SC-1, SI-1

(30) セキュリティおよびプライバシーエンジニアリングの原則 | 手順の厳格さ

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に手順の厳密さのセキュリティ設計原則を実装する。

詳解：手順の厳密さの原則は、システムのライフサイクルプロセスの厳密さは、その意図された統合的信頼性に見合っていると述べている。手順の厳密さは、システムのライフサイクル手順の範囲、深さ、および詳細を定義する。厳密なシステムのライフサイクル手順は、システムが適切であって、別々の意図しない機能がないことの保証に役立つ。第一に、手順はライフサイクルプロセスにチェックとバランスを課し、不特定の機能の導入を防止する。

第二に、仕様書やその他のシステム設計文書を作成するシステムセキュリティエンジニアリング活動に適用される厳密な手順は、実装されたコンポーネントが信頼できる（そして誤解を招く可能性のある）仕様であると信用するというものではなく、構築されたシステムを理解する能力に貢献する。

最後に、既存のシステムコンポーネントへの変更は、ソースコードや回路図を調べてどのように機能するかを理解するのではなく、現在の設計を説明する詳細な仕様がある場合には容易なものとなる。手続き上の厳密性は、セキュリティ機能要件と保証要件が満たされていることを保証するのに役立ち、統合的信頼性とリスク態勢を判断するための十分な情報に基づく基礎に貢献する。手順の厳密さは、システムに望まれる保証の程度に見合っていることが求められる。システムに必要な統合的信頼性が低い場合、手順の厳密さが高ければ不必要なコストが追加される可能性もあるが、高い統合的信頼性が重要である場合は、高い手順の厳密さのコストはメリットがある。

関連管理策：なし

(31) セキュリティおよびプライバシーエンジニアリングの原則 | セキュアなシステム変更

[*設定：組織が定めるシステムまたはシステムコンポーネント*]にセキュアなシステム変更のセキュリティ設計原則を実装する。

詳解：セキュアなシステム変更の原則は、システム変更がセキュリティ要件と利害関係者のリスク許容度に関してシステムのセキュリティを維持することを規定している。システムのアップグレードまたは変更は、セキュアなシステムをセキュアでないシステムに変える可能性がある。本システム変更の手順により、システムがその統合的信頼性を維持する場合、最初の開発に適用されたのと同じ厳密さがすべてのシステム変更に適用されることを保証できる。変更は、システムのセキュアな状態を維持する能力に影響を与える可能性があるため、変更を実装および展開する前に、変更の慎重なセキュリティ分析が必要である。この原則は、セキュアな保守拡張性の原則に対応している。

関連管理策：CM-3, CM-4

(32) セキュリティおよびプライバシーエンジニアリングの原則 | 十分なドキュメント

[*設定：組織が定めるシステムまたはシステムコンポーネント*]に十分なドキュメントのセ

キュリティ設計原則を実装する。

詳解：十分なドキュメントの原則は、システムと対話する責任のある組織の職員には、職員がシステムのセキュリティを損なうのではなく貢献することができるように適切なドキュメントおよびその他の情報が提供されることを示している。人的要因によるセキュリティや許容可能なセキュリティなどの原則に準拠しようとする試みにもかかわらず、システムは本質的に複雑であり、セキュリティメカニズムの使用に関する設計意図と、セキュリティメカニズムの誤用または誤設定の影響は、必ずしも直感的に明らかではない。知識のない、十分に訓練されていないユーザは、省略および依頼の間違いにより脆弱性をもたらす可能性がある。ドキュメントやトレーニングを利用できることで、継続的な保護などの原則を達成する上で重要な役割を果たす、知識豊富な職員を確保することができる。ドキュメントが明確に記述され、トレーニングによってサポートされることにより、セキュリティに関する意識向上とセキュリティに関する責任の理解が提供される。

関連管理策：AT-2, AT-3, SA-5

(33) セキュリティおよびプライバシーエンジニアリングの原則｜最小化

[*設定：組織が定めるプロセス*]を使用して最小化のプライバシー原則を実装する。

詳解：最小化の原則では、組織は認可された目的を達成するために直接関連し必要な個人情報のみを処理し、目的を達成するために必要な間だけ個人情報を維持することが望ましいと述べている。組織は、最小化の原則を実装するために、適用される法律およびポリシーに準拠したプロセスを導入する。

関連管理策：PE-8, PM-25, SC-42, SI-12

参照資料：[PRIVACT], [OMB A-130], [FIPS 199], [FIPS 200], [SP 800-37], [SP 800-53A], [SP 800-60-1], [SP 800-60-2], [SP 800-160-1], [IR 8062]

SA-9 外部システムサービス

管理策：

a. 外部システムサービスのプロバイダが組織のセキュリティおよびプライバシー要件を遵守し、[*設定：組織が定める管理策*]を採用することを要求する。

b. 外部システムサービスに関する組織の監視とユーザの役割と責任を規定し文書化する。

c. [*設定：組織が定めるプロセス、方法、および技法*]を採用して、外部のサービスプロバイダによる管理策への準拠を継続的に監視する。

詳解：外部システムサービスは外部のプロバイダによって提供されるので、組織は必要な管理策の実施や管理策の有効性のアセスメントを直接管理することはできない。組織は、業務提携、契約、省庁間協定、基幹業務協定、ライセンス契約、合弁事業、サプライチェーンとの取引など、様々な方法で外部のサービスプロバイダとの関係を確立している。外部システムサービスの使用によるリスクを管理する責任は、使用を認可する担当者にある。組織外部のサービスの場合、信頼の連鎖では、消費者とプロバイダの関係にある各プロバイダから提供されるサービスに対して適切な保護を提供するという一定レベルの信頼を組織が確立して保持する必要がある。この信頼の連鎖の範囲と性質は、組織と外部プロバイダとの関係によって異なっている。組織は、信頼関係を監視できるように、信頼関係の基礎を文書化する必要がある。外部システムサービスのドキュメントには、政府、サービスプロバイダ、エンドユーザのセキュリティの役割と責任、およびサービスレベル契約などが含まれる。サービスレベル契約では、実装された管理策の実績への期待値を規定し、測定可能な結果を記載すると共に、特定された準拠違反の事例に対する救済策と対応要件を明らかにする必要がある。

関連管理策：AC-20, CA-3, CP-2, IR-4, IR-7, PL-10, PL-11, PS-7, SA-2, SA-4, SR-3, SR-5

拡張管理策：

(1) 外部システムサービス｜リスクアセスメントおよび組織承認

(a) 情報セキュリティサービスの取得またはアウトソーシングの前に、組織のリスクア

セスメントを実施する。

(b) 専用の情報セキュリティサービスの取得またはアウトソーシングが、[*設定：組織が定める職員または役割*]によって承認済みであることを確認する。

詳解：情報セキュリティサービスには、ファイアウォールや鍵管理サービスなどのセキュリティデバイスの運用だけでなく、インシデントの監視、分析、対応などが含まれる。評価されるリスクには、システム、ミッションまたは事業、セキュリティ、プライバシー、またはサプライチェーンのリスクが含まれる。

関連管理策：CA-6, RA-3, RA-8

(2) 外部システムサービス | 機能、ポート、プロトコル、およびサービスの特定

[*設定：組織が定める外部システムサービス*]のプロバイダに、そのようなサービスの使用に必要な機能、ポート、プロトコル、およびその他のサービスを特定するように要求する。

詳解：そのようなサービスの提供に使用される特定の機能、ポート、プロトコル、およびサービスに関する外部サービスプロバイダからの情報は、特定の機能およびサービスの制限、または特定のポートおよびプロトコルのブロックに関連するトレードオフを理解する必要が生じた場合に役立つ。

関連管理策：CM-6, CM-7

(3) 外部システムサービス | プロバイダとの信頼関係の確立および維持

[*設定：組織が定める許容される信頼関係を規定するセキュリティおよびプライバシー要件、特性、要因、または条件*]に基づいて、外部サービスプロバイダとの信頼関係を確立、文書化、および維持する。

詳解：組織と外部サービスプロバイダ間の信頼関係は、外部サービスの使用によるリスクが許容可能なレベルにあるという信頼度を反映している。信頼関係は、サービスプロバイダが提供するサービスに対して適切な保護機能を提供していることへの組織の信頼レベルを高めるのに役立ち、インシデント対応を実施するとき、またはアップグレードや廃止を計画するときにも役立つ。信頼関係は消費者とプロバイダの相互作用に参加している潜在的に多数のエンティティ、従属関係と信頼のレベル、および当事者間の相互作用のタイプのために複雑になる可能性がある。場合によっては、信頼度は、サービス、情報、または個人のプライバシーの保護に必要な管理策と、実装された管理策の有効性に関してもたらされたエビデンスに関して、組織が外部サービスプロバイダに及ぼすことができる管理のレベルに基づいている。管理のレベルは、契約またはサービスレベル契約の契約条件によって確立される。

関連管理策：SR-2

(4) 外部システムサービス | 消費者およびプロバイダの一貫した利益

[*設定：組織が定めるアクション*]を実行して、[*設定：組織が定める外部サービスプロバイダ*]の利益が組織の利益と一致し、反映していることを確認する。

詳解：組織がますます外部のサービスプロバイダを使用するようになるにつれて、サービスプロバイダの利益が組織の利益から逸脱する可能性がある。必要な技術、管理、または運用の管理を定められたとおりに実施しているだけで、それらの管理を実装および管理するプロバイダが消費者側の組織の利益と一致する方法で運用されていないような状況では、管理が十分ではない場合がある。そのような懸念に対処するために組織が取る措置としては、選択されたサービスプロバイダの職員の身元調査の要求；所有権記録の調査；組織が信頼関係を築いてきたプロバイダなど、信頼できるサービスプロバイダのみの採用；および、サービスプロバイダ施設への日常的、定期的、計画外の訪問を実施することなどがある。

関連管理策：なし

(5) 外部システムサービス | 処理、保管、およびサービスの場所

[*設定：組織が定める要件または条件*]に基づいて、[*選択（1 つ以上）：情報処理；情報またはデータ；システムサービス*]の場所を[*設定：組織が定める場所*]に制限する。

詳解：情報処理、情報とデータの保管、またはシステムサービスの場所は、組織のミッションおよび事業の機能を正常に実行する能力に直接インパクトを与える可能性がある。このインパクトは、外部プロバイダが処理、保存、またはサービスの場所を管理するときに発生する。外部プロバイダが処理、保管、またはサービス場所の選択に使用する基準は、組織が使用する基準とは異なる場合がある。例えば、組織は、データまたは情報の格納場所を特定の場所に限定して、情報セキュリティインシデントまたはブリーチが発生した場合のインシデント対応措置を容易にすることを望む場合がある。フォレンジック分析および事後調査を含むインシデント対応措置は、処理および保管が行われる場所、および／またはシステムサービスが発信される場所における準拠法、ポリシー、またはプロトコルによって悪影響を受ける可能性がある

関連管理策：SA-5, SR-4

(6) 外部システムサービス | 組織が管理する暗号鍵

外部システムを介して保存または伝送される暗号化された資料の暗号鍵の排他的管理を維持する。

詳解：外部システムで暗号鍵の排他的管理を維持することで、外部システムスタッフによる組織データの解読を防ぐ。暗号鍵の組織による管理は、外部システムとの間でデータを送受信する際に組織内のデータを暗号化および復号することによって、または暗号化および復号化機能を外部システムに対してローカルにすることを許可するが、暗号化キーに組織の排他的アクセスを可能にするコンポーネントを採用することで実装できる。

関連管理策：SC-12, SC-13, SI-4

(7) 外部システムサービス | 組織管理の完全性チェック

情報が外部システムにあるときに、情報の完全性をチェックする機能を提供する。

詳解：外部システムに組織情報を保存すると、そのデータのセキュリティ状況の可視性が限定される可能性がある。保存されたデータの完全性を外部システムから転送せずに検証および妥当性確認する組織の能力は、そのような可視性を提供する。

関連管理策：SI-7

(8) 外部システムサービス | 処理および保管場所 ― 米国の司法管轄

情報処理およびデータ保管の地理的場所を、米国の法的管轄区域内にある施設に制限する。

詳解：情報処理とデータ保管の地理的位置は、組織のミッションおよび事業の機能を正常に実行する能力に直接インパクトを与える可能性がある。インパクトの大きい情報やシステムへの侵害やブリーチは、組織の資産や運用、個人、他の組織、そして国家に深刻な、あるいは壊滅的な悪影響を及ぼす可能性がある。影響力の大きい情報の処理と保管を米国の法的管轄区域内の施設に制限することで、そのような処理と保管をより適切に管理することができる。

関連管理策：SA-5, SR-4

参照資料：[OMB A-130], [SP 800-35], [SP 800-160-1], [SP 800-161], [SP 800-171]

SA-10 開発者構成管理

管理策：システム、システムコンポーネント、またはシステムサービスの開発者に以下を要求する。

a. システム、コンポーネント、またはサービスの[*選択（1 つ以上）：設計；開発；実装；操作；処分*]中に構成管理を実行する。

b. [*設定：組織が定める構成管理下の構成項目*]の変更の完全性を文書化、管理、および統制する。

c. システム、コンポーネント、またはサービスに対して、組織が承認済みの変更のみを実装する。

d. システム、コンポーネント、またはサービスに対する承認済みの変更と、そのような変更

がセキュリティおよびプライバシーに及ぼす潜在的なインパクトを文書化する。

e. システム、コンポーネント、またはサービス内のセキュリティの欠陥と欠陥の解決を追跡し、結果を[*設定：組織が定める職員*]に報告する。

詳解：組織は、開発者が実施した構成管理活動の質と正確性を、効果的なセキュリティ管理策を適用した直接的な証拠と見なしている。管理策には、システムのハードウェア、ソフトウェア、およびファームウェアのセキュリティ関連部分を生成するために使用される素材のマスターコピーを、認可されていない変更または破壊から保護することが含まれる。システム、システムコンポーネント、またはシステムサービスに対する変更の完全性を維持するには、システム開発ライフサイクル全体を通じて、構成の厳密な管理を行い、認可された変更を追跡し、認可されていない変更を防止する必要がある。

構成管理下に置かれる構成アイテムには、正式なモデル；機能；高レベル、および低レベルの設計仕様；その他の設計データ；実装ドキュメント；ソースコードとハードウェアの回路図；オブジェクトコードの現在実行中のバージョン；セキュリティ関連のハードウェア記述およびソースコードの新しいバージョンを以前のバージョンと比較するためのツール；試験装置とドキュメントなどが含まれる。組織のミッションと事業ニーズ、および実施されている契約関係の性質に応じて、開発者は、システム開発ライフサイクルの運用および保守段階で構成管理サポートを提供することがある。

関連管理策：CM-2, CM-3, CM-4, CM-7, CM-9, SA-4, SA-5, SA-8, SA-15, SI-2, SR-3, SR-4, SR-5, SR-6

拡張管理策：

(1) 開発者構成管理 | ソフトウェアおよびファームウェアの完全性の検証

システム、システムコンポーネント、またはシステムサービスの開発者にソフトウェアおよびファームウェアコンポーネントの完全性の検証を可能にすることを要求する。

詳解：ソフトウェアおよびファームウェアの完全性検証により、組織は、開発者が提供するツール、技法、およびメカニズムを使用して、ソフトウェアおよびファームウェアコンポーネントへの認可されていない変更を検知できる。完全性のチェックメカニズムは、ソフトウェアおよびファームウェアコンポーネントの偽造にも対処できる。組織は、例えば、開発者が提供するセキュアな一方向ハッシュを通じて、ソフトウェアおよびファームウェアコンポーネントの完全性を検証する。提供されるソフトウェアおよびファームウェアコンポーネントには、そのようなコンポーネントのアップデートも含まれる。

関連管理策：SI-7, SR-11

(2) 開発者構成管理 | 代替構成管理プロセス

専任の開発者の構成管理チームが不在の場合、組織の職員を使用して代替構成管理プロセスを提供する。

詳解：組織が市販の情報技術製品を使用する場合、代替の構成管理プロセスが必要になる場合がある。代替構成管理プロセスには、システム、システムコンポーネント、およびシステムサービスへの提案された変更をレビューおよび承認し、システム、コンポーネント、またはサービスへの変更の実装前にセキュリティおよびプライバシー影響評価を実施する組織の職員が含まれる。

関連管理策：なし

(3) 開発者構成管理 | ハードウェアの完全性の検証

システム、システムコンポーネント、またはシステムサービスの開発者に、ハードウェアコンポーネントの完全性の検証を可能にするよう要求する。

詳解：ハードウェアの完全性の検証により、組織は、開発者が提供するツール、技法、方法、およびメカニズムを使用して、ハードウェアコンポーネントへの認可されていない変更を検知することができる。組織は、ハードウェアコンポーネントの完全性を、コピーが困難なラベル、開発者が提供する検証可能なシリアル番号、および改ざん防止技術の使用を要求することによって検証できる。提供されるハードウェアコンポーネントには、そのようなコンポーネントに対するハードウェアおよびファームウェアのアップデートも含まれる。

関連管理策：SI-7

(4) 開発者構成管理 | 信頼できる世代

システム、システムコンポーネント、またはシステムサービスの開発者に、セキュリティ関連のハードウェア記述、ソースコード、およびオブジェクトコードの新しく生成されたバージョンを以前のバージョンと比較するためのツールを採用するよう要求する。

詳解：記述、ソースコード、およびオブジェクトコードの信頼できる世代は、開発中のバージョン間のハードウェア、ソフトウェア、およびファームウェアコンポーネントへの認可された変更に対応している。焦点は、セキュリティ関連のハードウェア記述、ソースコード、およびオブジェクトコードの新しく生成されたバージョンが、システム、システムコンポーネント、またはシステムサービスのセキュリティポリシーを引き続き実施することを保証する、開発者による構成管理プロセスの有効性にある。対照的に、SA-10(1)および SA-10(3)を使用すると、組織は、開発者が提供するツール、手法、またはメカニズムを使用して、ハードウェア、ソフトウェア、およびファームウェアのコンポーネントに対する認可されていない変更を検知できる。

関連管理策：なし

(5) 開発者構成管理 | バージョン管理のための完全性のマッピング

システム、システムコンポーネント、またはシステムサービスの開発者に、セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアの現在のバージョンを記述するマスタービルドデータとオンサイトの現在のバージョンのデータのマスターコピーとの間のマッピングの完全性を維持することを要求する。

詳解：バージョン管理のマッピングの完全性は、初期開発とシステム開発の両方のライフサイクル更新中のハードウェア、ソフトウェア、およびファームウェアコンポーネントの変更に対処している。重要なミッションおよび事業の機能をサポートする組織のシステムの可用性を確保するには、セキュリティ関連のハードウェア、ソフトウェア、およびファームウェア（設計、ハードウェア図面、ソースコードを含む）のマスターコピーと運用環境のマスターコピー内の同等のデータとの間の完全性を維持することが不可欠である。

関連管理策：なし

(6) 開発者構成管理 | 信頼できる配布

システム、システムコンポーネント、またはシステムサービスの開発者に、組織に配布されるセキュリティ関連のハードウェア、ソフトウェア、およびファームウェアのアップデートがマスターコピーによって指定されたものと正確に一致することを保証するための手順を実行するよう要求する。

詳解：セキュリティ関連のハードウェア、ソフトウェア、およびファームウェア更新の信頼できる配布は、更新が開発者によって維持されているマスターコピーの正しい表現であり、配布中に改ざんされていないことを保証するのに役立つ。

関連管理策：なし

(7) 開発者構成管理 | セキュリティおよびプライバシーの代表者

[*設定：組織が定めるセキュリティおよびプライバシーの代表者*]が[*設定：組織が定める構成変更管理および管理プロセス*]に含まれることを要求する。

詳解：情報セキュリティおよびプライバシーの代表者には、システムセキュリティ担当者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、およびシステムプライバシー担当者を含めることができる。システム構成の変更は意図しない影響をもたらす可能性があり、その一部はセキュリティまたはプライバシーに関連する可能性があるため、情報セキュリティとプライバシーの専門知識を持つ職員による説明が重要である。プロセスの早い段階でそのような変更を検知することは、システムのセキュリティとプライバシーへの姿勢に最終的に影響する可能性のある、意図しない悪影響を回避するのに役立つ。この拡張管理策における構成変更管理および統制プロセスは、SA-10b の組織によって規定された変更管理および統制プロセスを指す。

関連管理策：なし

参照資料: [FIPS 140-3], [FIPS 180-4], [FIPS 202], [SP 800-128], [SP 800-160-1]

SA-11 開発者のテストおよび評価

管理策: システム開発ライフサイクルの設計後のすべての段階で、システム、システムコンポーネント、またはシステムサービスの開発者に以下を要求する。

a. 継続的なセキュリティおよびプライバシー管理策アセスメントのための計画を策定し、実施する。

b. [*設定: 組織が定める頻度*] と [*設定: 組織が定める深さと適用範囲*] で [*選択 (1 つ以上): ユニット; 統合; システム; 回帰*] のテスト／評価を行なう。

c. アセスメント計画を実施したエビデンスと、試験および評価の結果を作成する。

d. 検証可能な欠陥修正プロセスを実装する。

e. テストおよび評価中に特定された欠陥を修正する。

詳解: 開発テストおよび評価により、必要な管理策が正しく実装され、意図したとおりに動作し、必要なセキュリティポリシーおよびプライバシーポリシーが適用され、確立されたセキュリティおよびプライバシー要件を満たしていることが確認される。システムのセキュリティ特性および個人のプライバシーは、システムコンポーネントの相互接続またはそれらのコンポーネントへの変更によって影響を受ける可能性がある。アプリケーション、オペレーティングシステム、およびファームウェアのアップグレードまたは交換を含む相互接続または変更は、以前に実装された管理策に悪影響を及ぼす可能性がある。開発期間中における継続的なアセスメントにより、潜在的な欠陥を軽減または排除するために開発者が実施できる追加のタイプのテストおよび評価が可能になる。個別要求に沿って開発されたソフトウェアアプリケーションをテストするには、手動のコードのレビュー、セキュリティアーキテクチャレビュー、侵入テスト、および静的分析、動的分析、バイナリ分析、または 3 つの分析アプローチのハイブリッドなどのアプローチが必要になる場合がある。

開発者は、様々なツールやソースコードのレビューで、セキュリティ手法やファジングとともに分析アプローチを使用できる。セキュリティとプライバシーのアセスメント計画には、ソフトウェアとファームウェアのコンポーネントの分析、テスト、評価、レビューのタイプ; 適用される厳密さの程度; 進行中のテストと評価の頻度; および、それらのプロセスの間に生成された成果物のタイプなど、開発者が実施する予定の具体的な活動が含まれる。テストと評価の深さは、アセスメントプロセスに関連する厳密さと詳細レベルを指す。テストと評価の対象範囲は、アセスメントプロセスに含まれる成果物の範囲 (すなわち、数とタイプ) を指す。契約では、セキュリティとプライバシーのアセスメント計画の受領基準、欠陥の修正プロセス、および計画とプロセスが詳細に適用されたエビデンスを指定する。アセスメント計画、エビデンス、およびドキュメントをレビューおよび保護する方法は、システムのセキュリティ分類または機密性区分レベルに対応する。契約では、ドキュメントの保護要件を指定することができる。

関連管理策: CA-2, CA-7, CM-4, SA-3, SA-4, SA-5, SA-8, SA-15, SA-17, SI-2, SR-5, SR-6, SR-7

拡張管理策:

(1) 開発者のテストおよび評価 | 静的コード分析

システム、システムコンポーネント、またはシステムサービスの開発者は、静的コード分析ツールを使用して、一般的な欠陥を特定し、分析結果を文書化する必要がある。

詳解: 静的コード分析は、セキュリティレビューのための技術と方法論を提供し、コードの弱点、および既知の脆弱性を持つライブラリやその他のコード、または古くてサポートされていないコードの組み込みのチェックなどを含む。静的コード分析を使用して、脆弱性を特定し、セキュアなコーディングを実施することができる。これは、開発プロセスの早い段階で使用する場合、コードの変更ごとに潜在的な弱点を自動的にスキャンする場合に最も効果的である。静的コード分析は、明確な修正ガイダンスを提供し、開発者が修正する欠陥を特定することができる。静的分析が正しく実施されていることを示すエビデンスには、重大な欠陥タイプの総欠陥密度、開発者またはセキュリティ専門家が欠陥を検査したエビデンス、および欠陥が修正されたエビデンスなどを含めることができる。調査結果が生かさ

れなかった比率が高い場合は、一般に誤検知と呼ばれ、分析プロセスまたは分析ツールに潜在的な問題があることを示している。そのような場合、組織は他のソースからのエビデンスに対してエビデンスの有効性を比較検討する。

関連管理策：なし

(2) 開発者のテストおよび評価 | 脅威のモデル化および脆弱性の分析

システム、システムコンポーネント、またはシステムサービスの開発者に、開発中およびそれに続くシステム、コンポーネント、またはサービスのテストと評価中に、脅威のモデル化と脆弱性分析を行う必要がある。

(a) **[*設定：インパクト、運用環境、既知または想定される、および許容可能なリスクレベルに関する組織が定める情報*]を使用する。**

(b) **[*設定：組織が定めるツールと方法*]を採用する。**

(c) **[*設定：組織が定めるモデル化と分析の幅と深さ*]による厳密さのレベルでモデル化と分析を実施する。**

(d) **[*設定：組織が定める受領基準*]を満たすエビデンスを作成する。**

詳解：システム、システムコンポーネント、およびシステムサービスは、システム開発ライフサイクルの要件および設計段階で作成された機能仕様および設計仕様から大幅に逸脱する場合がある。したがって、これらのシステム、コンポーネント、およびサービスを効果的に運用するには、開発中および引き渡し前のそれらのシステム、システムコンポーネント、およびシステムサービスにおける脅威のモデル化および脆弱性分析の更新が重要である。システム開発ライフサイクルのこの段階での脅威のモデル化と脆弱性分析により、設計と実装の変更が確実に説明され、それらの変更のために作成された脆弱性がレビューされ軽減されていることを確保できる。

関連管理策：PM-15, RA-3, RA-5

(3) 開発者のテストおよび評価 | アセスメント計画およびエビデンスの独立した検証

(a) **[*設定：組織が定める独立に関する判断基準*]を満たす独立したエージェントに、開発者のセキュリティおよびプライバシーアセスメント計画の適切な実施、ならびにテストおよび評価中に作成されたエビデンスを検証することを要求する。**

(b) **独立したエージェントに、検証プロセスを完了するために十分な情報が提供されていること、またはそのような情報を取得する権限が付与されていることを検証する。**

詳解：独立したエージェントは、開発者のセキュリティおよびプライバシーアセスメント計画が正しく実装されていることを確認するための専門知識、スキル、トレーニング、認定、および経験を含む資格を持っている。

関連管理策：AT-3, RA-5

(4) 開発者のテストおよび評価 | 手動のコードレビュー

システム、システムコンポーネント、またはシステムサービスの開発者に、[*設定：組織が定めるプロセス、手順、および／または技法*]を使用して[*設定：組織が定める特定のコード*]への手動のレビューを要求する。

詳解：通常、手動のコードのレビューは、システムの重要なソフトウェアおよびファームウェアコンポーネント用に用意されている。手動のコードのレビューは、ほとんどの場合、静的分析や動的分析などの自動分析ツールや技法が利用できない、アプリケーションの要件や状況の知識を必要とする弱点を特定するのに効果的である。手動のコードのレビューの利点には、管理策の適用に対してアクセス制御マトリックスを検証し、暗号の実装と管理策の詳細な側面をレビューする能力が含まれる。

関連管理策：なし

(5) 開発者のテストおよび評価 | 侵入テスト

システム、システムコンポーネント、またはシステムサービスの開発者に侵入テストを実施することを要求する。

(a) **[*設定：組織が定める幅と深さのテスト*]の厳格さのレベルで。**

(b) **[*設定：組織が定める制約*]の下で。**

詳解：侵入テストは、利用可能なすべての情報技術製品またはシステムのドキュメントを使用し、特定の制約の下で作業するアセッサーが、情報技術製品およびシステムの実装されたセキュリティおよびプライバシー機能を回避しようとするアセスメント方法である。侵入テストを実施するアセッサーにとって有用な情報には、製品とシステムの設計仕様、ソースコード、および管理者とオペレータのマニュアルが含まれる。侵入テストには、敵対者の行動をシミュレートする熟練した専門家によって実行される分析を使用したホワイトボックス、グレーボックス、またはブラックボックステストが含まれる。侵入テストの目的は、実装エラー、構成の誤り、またはその他の運用上の弱点や欠陥に起因するシステム、システムコンポーネント、およびサービスの脆弱性を検出することである。侵入テストは、自動および手動のコードレビューと組み合わせて実行でき、通常可能なレベルよりも高いレベルの分析を提供できる。侵入テスト中にユーザセッション情報やその他の個人情報がキャプチャまたは記録される場合、そのような情報はプライバシーを保護するために適切に処理される。

関連管理策：CA-8, PM-14, PM-25, PT-2, SA-3, SI-2, SI-6

(6) 開発者のテストおよび評価｜攻撃対象領域のレビュー

システム、システムコンポーネント、またはシステムサービスの開発者が攻撃対象領域のレビューを実行することを要求する。

詳解：システムおよびシステムコンポーネントの攻撃対象領域は、それらのシステムを攻撃され易くする露出された領域である。攻撃対象領域には、ハードウェア、ソフトウェア、およびファームウェアのコンポーネントの弱点または欠陥が敵対者に脆弱性を悪用する機会を提供するアクセス可能な領域が含まれる。攻撃対象領域のレビューにより、開発者はシステムの設計と実装の変更を分析し、変更の結果として生成される攻撃ベクトルを緩和することができる。特定された欠陥の修正には、セキュアでない機能の廃止が含まれる。

関連管理策：SA-15

(7) 開発者のテストおよび評価｜テストおよび評価の範囲の検証

システム、システムコンポーネント、またはシステムサービスの開発者に、テストおよび評価の範囲が、[*設定：組織が定めるテストおよび評価の幅と深さ*]の厳格さのレベルで必要な管理策を完全にカバーしていることを検証することを要求する。

詳解：テストと評価が必要な管理策を完全にカバーしていることを確認することは、非公式から公式までの様々な分析技法によって達成できる。これらの技法はそれぞれ、分析の形式的度合いに対応する保証レベルを高める。最高レベルの保証で厳密に管理策の網羅性を実証することは、管理策の実装と対応するテストケースとの相関を含む、正式なモデル化および分析技法を使用して達成することができる。

関連管理策：SA-15

(8) 開発者テストおよび評価｜動的コード分析

システム、システムコンポーネント、またはシステムサービスの開発者に、動的コード分析ツールを使用して、一般的な欠陥を特定し、分析結果を文書化することを要求する。

詳解：動的コード分析は、メモリ破損、ユーザ権限の問題、およびその他の潜在的なセキュリティ問題を監視できるツールを使用して、ソフトウェアプログラムの実行時検証を提供する。動的コード分析では、ランタイムツールを使用して、セキュリティ機能が設計どおりに機能することを確認する。ファズテストと呼ばれる動的分析の一種は、認可されていないデータやランダムなデータをソフトウェアプログラムに故意に入力することにより、プログラムの障害を引き起こす。ファズテスト戦略は、アプリケーションの使用目的と、アプリケーションの機能および設計仕様から導き出される。動的コード分析の範囲と提供される保証を理解するために、組織はコードカバレッジ分析（すなわち、テストされたサブルーチンの割合やテストスイートの実行中に呼び出されたプログラムステートメントの割合などの指標を使用してコードがテストされている度合いをチェックすること）および／またはコンコーダンス分析（すなわち、非英語の単語または軽蔑的な用語など、ソフトウェアコード内で不適

切な単語をチェックする）の実施を考慮しても良い。

関連管理策：なし

(9) 開発者のテストおよび評価 | 対話型のアプリケーションのセキュリティテスト

システム、システムコンポーネント、またはシステムサービスの開発者に、対話型のアプリケーションセキュリティテストツールを使用して欠陥を特定し、結果を文書化することを要求する。

詳解：対話型の（計装型としても知られている）アプリケーションセキュリティテストは、テスト中に実行されるアプリケーションを観察することによって脆弱性を検知する方法である。計装の使用は、実際に実行中のアプリケーションの直接測定に依存し、コードへのアクセス、ユーザとの対話処理、ライブラリ、フレームワーク、バックエンド接続、および構成を使用して、管理策の有効性を直接測定する。対話型のアプリケーションセキュリティテストは、分析技術と相まって、潜在的な脆弱性を幅広く特定し、管理策の有効性を確認することができる。計装型のテストはリアルタイムで機能し、システム開発ライフサイクル全体を通じて継続的に使用できる。

関連管理策：なし

参照資料：[ISO 15408-3], [SP 800-30], [SP 800-53A], [SP 800-154], [SP 800-160-1]

SA-12 サプライチェーンの保護

［撤回：SR ファミリーに組み込まれた］

拡張管理策：

(1) サプライチェーンの保護 | 取得戦略／ツール／方法

［撤回：SR-5 に移動した］

(2) サプライチェーンの保護 | サプライヤのレビュー

［撤回：SR-6 に移動した］

(3) サプライチェーンの保護 | 信頼できる配送および倉庫管理

［撤回：SR-3 に組み込まれた］

(4) サプライチェーンの保護 | サプライヤの多様性

［撤回：SR-3(1)に移動した］

(5) サプライチェーンの保護 | 損害の限定

［撤回：SR-3(2)に移動した］

(6) サプライチェーンの保護 | 調達時間の最小化

［撤回：SR-5(1)に組み込まれた］

(7) サプライチェーンの保護 | 選択／受領／更新前のアセスメント

［撤回：SR-5(2)に移動した］

(8) サプライチェーンの保護 | オールソースインテリジェンスの活用

［撤回：RA-3(2)に組み込まれた］

(9) サプライチェーンの保護 | 運用セキュリティ

［撤回：SR-7 に移動した］

(10) サプライチェーンの保護 | 本物であり、改変されていないことの確認

［撤回：SR-4(3)に移動した］

(11) サプライチェーンの保護 | 侵入テスト／要素、プロセス、および行為者の分析

［撤回：SR-6(1)に移動した］

(12) サプライチェーンの保護 | 組織間の合意

［撤回：SR-8 に移動した］

(13) サプライチェーンの保護 | 重要な情報システムのコンポーネント

［撤回：MA-6 および RA-9 に組み込まれた］

(14) サプライチェーンの保護 | アイデンティティおよびトレーサビリティ

［撤回：SR-4(1)および SR-4(2)に移動した］

(15) サプライチェーンの保護 | 弱点または欠陥に対処するためのプロセス

［撤回：SR-3 に組み込まれた］

SA-13 統合的信頼性

［撤回：SA-8 に組み込まれた］

SA-14 重要度分析

［撤回：RA-9 に組み込まれた］

拡張管理策：

(1) 重要度分析 | 代替調達が不可能な重要なコンポーネント

［撤回：SA-20 に組み込まれた］

SA-15 開発プロセス、規格、およびツール

管理策：

a. システム、システムコンポーネント、またはシステムサービスの開発者に、以下の文書化された開発プロセスに従うことを要求する。

1. セキュリティおよびプライバシー要件に明示的に対処する。
2. 開発プロセスで使用される規格とツールを特定する。
3. 開発プロセスで使用される特定のツールオプションおよびツール構成を文書化する。
4. 開発で使用されるプロセスおよび／またはツールに対する変更の完全性を文書化し、管理し、保証する。

b. 開発プロセス、規格、ツール、ツールオプション、およびツール構成を［*設定：組織が定める頻度*］でレビューし、選択および採用されたプロセス、規格、ツール、ツールオプション、およびツール構成が、［*設定：組織が定めるセキュリティおよびプライバシー要件*］を満たすことができるかどうかを判断する。

詳解：開発ツールには、プログラミング言語やコンピュータ支援設計システムが含まれる。開発プロセスのレビューには、成熟度モデルを使用して、そのようなプロセスの潜在的な有効性を判断することが含まれる。ツールとプロセスへの変更の完全性を維持することで、効果的なサプライチェーンのリスクアセスメントと軽減が容易になる。このような完全性には、認可された変更を追跡し、認可されていない変更を防ぐために、システム開発ライフサイクル全体を通じて構成管理が必要である。

関連管理策：MA-6, SA-3, SA-4, SA-8, SA-10, SA-11, SR-3, SR-4, SR-5, SR-6, SR-9

拡張管理策：

(1) 開発プロセス、規格、およびツール | 品質指標

システム、システムコンポーネント、またはシステムサービスの開発者に以下を要求する。

(a) 開発プロセスの最初に品質指標を規定する。

(b) 品質基準を満たしていることのエビデンスを[*選択(1 つ以上):[設定:組織が定める頻度*];[*設定:組織が定めるプログラムレビューマイルストーン*];*引き渡し時*]に提供する。

詳解:組織は、品質指標を使用して、システム品質の許容レベルを確立する。指標には、システム開発プロジェクトの特定のフェーズの満足のいく実行を表す完了基準または充足基準の集合である品質ゲートを含めることができる。例えば、品質ゲートでは、すべてのコンパイラ警告が無くなること、あるいはそのような警告が、必要なセキュリティまたはプライバシーのケイパビリティの有効性にインパクトを及ぼさないという判断を要求することなどがある。開発プロジェクトの実施段階では、品質ゲートによって進捗状況が明確かつ一義的に示される。その他、開発プロジェクト全体に適用される指標がある。指標には、例えば、共通脆弱性評価システム(CVSS: Common Vulnerability Scoring System)の重大度が中または高で、提供されたシステムに既知の脆弱性が存在しないことを要求するなど、組織のリスク許容度に従って脆弱性の重大度のしきい値を定義することを含めることができる。

関連管理策:なし

(2) 開発プロセス、規格、およびツール | セキュリティおよびプライバシーの追跡ツール

システム、システムコンポーネント、またはシステムサービスの開発者に、開発プロセス中に使用するセキュリティおよびプライバシーの追跡ツールを選択して採用するよう要求する。

詳解:システム開発チームは、開発プロセスに関連する完了した作業項目またはタスクの割り当て、分類、フィルタリング、および追跡を容易にする脆弱性または作業項目追跡システムを含む、セキュリティおよびプライバシーの追跡ツールを選択して展開する。

関連管理策:SA-11

(3) 開発プロセス、規格、およびツール | 重要度分析

システム、システムコンポーネント、またはシステムサービスの開発者に重要度分析を実行するよう要求する。

(a) [*設定:組織が定めるシステム開発ライフサイクルにおける決定ポイント*]で。

(b) [*設定:組織が定める重要度分析の幅と深さ*]の厳密さのレベルで。

詳解:開発者が実行する重要度分析は、組織が実行する重要度分析へのインプットを提供する。組織は、市販の製品として開発されたシステムコンポーネントの詳細な設計ドキュメントにアクセスできない場合があるため、組織の重要度分析には開発者のインプットが不可欠である。そのような設計文書には、機能仕様、高レベル設計、低レベル設計、ソースコード、およびハードウェアの回路図が含まれる。重要度分析は、高価値資産として指定されている組織システムにとって重要である。高価値資産は、敵対的関心の高まりや連邦政府事業への潜在的な悪影響のため、中インパクトまたは高インパクトシステムとなる可能性がある。組織がサプライチェーンの重要性分析を実施する場合、開発者のインプットは特に重要である。

関連管理策:RA-9

(4) 開発プロセス、規格、およびツール | 脅威のモデル化および脆弱性の分析

[撤回:SA-11(2)に組み込まれた]

(5) 開発プロセス、規格、およびツール | 攻撃対象領域の削減

システム、システムコンポーネント、またはシステムサービスの開発者に、攻撃対象領域を[*設定:組織が定めるしきい値*]に減らすよう要求する。

詳解:攻撃対象領域の縮小は、脅威と脆弱性の分析、システムのアーキテクチャと設計と密接に連携している。攻撃対象領域の削減は、攻撃者にシステム、システムコンポーネント、およびシステムサービス内の弱点または欠陥(すなわち、潜在的な脆弱性)を悪用する機会を減らすことにより、組織へのリスクを低減する手段である。攻撃対象領域の削減には、多層防御の概念の実装、最小特権と最小機能の原則の適用、セキュアなソフトウェア開発技法の適用、安全でない機能の廃止、認可されていないユーザが利用できるエントリ

ポイントの削減、実行するコードの量の削減、アプリケーションの排除、攻撃に対して脆弱なプログラミングインタフェース（API：Application Programming Interfaces）の排除が含まれる。

関連管理策：AC-6, CM-7, RA-3, SA-11

(6) 開発プロセス、規格、およびツール｜継続的な改善

システム、システムコンポーネント、またはシステムサービスの開発者に、開発プロセスを継続的に改善するための明示的なプロセスを実装するよう要求する。

詳解：システム、システムコンポーネント、およびシステムサービスの開発者は、品質目的を達成し、現在の脅威環境におけるセキュリティ機能およびプライバシー機能に対処するための開発プロセスの有効性と効率を考慮する。

関連管理策：なし

(7) 開発プロセス、規格、およびツール｜自動化された脆弱性分析

システム、システムコンポーネント、またはシステムサービスの開発者に、[*設定：組織が定める頻度*]で次のことを要求する。

(a) [*設定：組織が定めるツール*]を使用して、自動化された脆弱性分析を実施する。

(b) 検出された脆弱性の悪用の可能性を決定する。

(c) 提供された脆弱性に対する潜在的なリスク軽減策を決定する。

(d) ツールの出力と分析の結果を[*設定：組織が定める職員または役割*]に提出する。

詳解：自動化されたツールは、大規模で複雑なシステムにおける悪用可能な弱点や欠陥の分析、脆弱性の重大度による優先順位付け、リスク軽減のための推奨事項の提供に、より効果的である。

関連管理策：RA-5, SA-11

(8) 開発プロセス、規格、およびツール｜脅威および脆弱性情報の再利用

システム、システムコンポーネント、またはシステムサービスの開発者に、類似のシステム、コンポーネント、またはサービスからの脅威のモデル化および脆弱性分析を使用して、現在の開発プロセスに通知するよう要求する。

詳解：同様のソフトウェアアプリケーションに見られる脆弱性の分析は、開発中のシステムの潜在的な設計および実装の問題を通知することができる。同様のシステムまたはシステムコンポーネントが開発者組織内に存在する場合がある。脆弱性の情報は、NIST 国有脆弱性データベース（NVD）を含む、公共および民間の様々なソースから入手できる。

関連管理策：なし

(9) 開発プロセス、規格、およびツール｜ライブデータの使用

［撤回：SA-3(2)に組み込まれた］

(10) 開発プロセス、規格、およびツール｜インシデント対応計画

システム、システムコンポーネント、またはシステムサービスの開発者に、インシデント対応計画を提供、実装、およびテストするよう要求する。

詳解：開発者が提供するインシデント対応計画は、組織が直ちに利用できない情報を提供し、組織のインシデント対応計画に組み込まれる場合がある。組織が市販の製品の脆弱性に対応する場合など、開発者情報も非常に役立つ場合がある。

関連管理策：IR-8

(11) 開発プロセス、規格、およびツール｜システムまたはコンポーネントのアーカイブ

システムまたはコンポーネントの開発者に、リリースまたは配信されるシステムまたはコンポーネントを、最終的なセキュリティおよびプライバシーのレビューをサポートする対応するエビデンスとともにアーカイブすることを要求する。

詳解：システムまたはシステムコンポーネントをアーカイブするには、ハードウェア仕様、ソースコード、オブジェクトコード、およびシステムやコンポーネントのアップグレードや変更に直ちに利用できる構成基準を提供できる開発プロセスからの関連ドキュメントなど、主要な開発成果物を保持する必要がある。

関連管理策：CM-2

(12) 開発プロセス、規格、およびツール | 個人情報の最小化

システムまたはシステムコンポーネントの開発者に、開発およびテスト環境での個人情報の使用を最小限に抑えるよう要求する。

詳解：組織は、匿名化や合成データなどの技法を使用することで、個人のプライバシーに対するリスクを最小限に抑えることができる。開発およびテスト環境での個人情報の使用を限定することで、システムによって生じるプライバシーリスクのレベルを下げることができる。

関連管理策：PM-25, SA-3, SA-8

参照資料：[SP 800-160-1], [IR 8179]

SA-16 開発者が提供するトレーニング

管理策：システム、システムコンポーネント、またはシステムサービスの開発者に、実装されたセキュリティおよびプライバシー機能、管理策、メカニズムの正しい使用と運用に関する[*設定：組織が定めるトレーニング*]を提供するように要求する。

詳解：開発者が提供するトレーニングは、外部および内部（社内）開発者に適用される。組織のシステム内に実装された管理策の有効性を確保するには、職員の訓練が不可欠である。トレーニングのタイプには、ウェブベースのトレーニングとコンピュータベースのトレーニング、教室形式のトレーニング、実地トレーニング（マイクロトレーニングを含む）などがある。組織は、社内トレーニングを実施したり、組織の職員にセルフトレーニングを提供したりするために、開発者にトレーニング資料を要求することもできる。組織は、必要なトレーニングのタイプを決定し、異なるセキュリティおよびプライバシー機能、管理策、およびメカニズムのために異なるタイプのトレーニングを必要とする場合がある。

関連管理策：AT-2, AT-3, PE-3, SA-4, SA-5

拡張管理策：なし

参照資料：なし

SA-17 開発者のセキュリティおよびプライバシーのアーキテクチャおよび設計

管理策：システム、システムコンポーネント、またはシステムサービスの開発者に、以下の設計仕様とセキュリティおよびプライバシーのアーキテクチャを作成することを要求する。

a. 組織のエンタープライズアーキテクチャに不可欠な部分である、組織のセキュリティおよびプライバシーアーキテクチャと一貫性がある。

b. 必要なセキュリティ機能とプライバシー機能、および物理コンポーネントと論理コンポーネント間の管理策の割り当てを的確かつ正確に説明する。

c. 個々のセキュリティ機能とプライバシー機能、メカニズム、およびサービスがどのように連携して、必要なセキュリティ機能とプライバシー機能、および保護のための統一されたアプローチを提供するかを表わす。

詳解：開発者のセキュリティとプライバシーのアーキテクチャと設計は、外部の開発者を対象としているが、内部（社内）開発にも適用できる。対照的に、PL-8 は、組織がエンタープライズアーキテクチャと統合されたセキュリティとプライバシーのアーキテクチャを確実に開発するように、内部開発者を対象としている。SA-17 と PL-8 の違いは、組織がシステム、システムコンポーネント、またはシステムサービスの開発を外部委託する場合、および組織のエンタープライズアーキテクチャとセキュリティとプライバシーのアーキテクチャとの一貫性を示す必要がある場合に

特に重要である。[ISO 15408-2]、[ISO 15408-3]、および[SP 800-160-1]は、正式なポリシーモデル、セキュリティ関連コンポーネント、正式および非公式な対応、概念的に単純な設計、最小特権とテストのための構造化など、セキュリティのアーキテクチャおよび設計に関する情報を提供する。

関連管理策：PL-2, PL-8, PM-7, SA-3, SA-4, SA-8, SC-7

拡張管理策：

(1) 開発者のセキュリティおよびプライバシーのアーキテクチャおよび設計 | 正式なポリシーモデル

システム、システムコンポーネント、またはシステムサービスの開発者に次のことを要求する。

(a) [*設定：組織が定める組織のセキュリティとプライバシーのポリシーの要素*]を記述する正式なポリシーモデルを、開発プロセスの不可欠な部分として作成する。

(b) 正式なポリシーモデルが内部的に一貫しており、実装時に組織のセキュリティとプライバシーのポリシーの規定された要素を実施するのに十分であることを証明する。

詳解：正式なモデルは、正式な言語を使用して特定の動作またはセキュリティとプライバシーのポリシーを記述し、これらの動作とポリシーの適合性を正式に証明できるようにする。システムのすべてのコンポーネントをモデル化できるわけではない。一般に、正式な仕様は、任意アクセス制御ポリシーなど、対象となる動作またはポリシーに限定される。組織は、記述される行動やポリシーの性質、および利用可能なツールに基づいて、正式なモデル化言語とアプローチを選択する。

関連管理策：AC-3, AC-4, AC-25

(2) 開発者のセキュリティおよびプライバシーのアーキテクチャおよび設計 | セキュリティ関連のコンポーネント

システム、システムコンポーネント、またはシステムサービスの開発者に以下を要求する。

(a) セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアを定義する。

(b) セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアの定義が正確であるという根拠を提供する。

詳解：セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアは、必要なセキュリティ特性を維持するために正しく実行されると信頼されているシステム、コンポーネント、またはサービスの一部を表す。

関連管理策：AC-25, SA-5

(3) 開発者のセキュリティおよびプライバシーのアーキテクチャおよび設計 | 正式な対応

システム、システムコンポーネント、またはシステムサービスの開発者に以下を要求する。

(a) 開発プロセスの不可欠な部分として、例外、エラーメッセージ、および影響に関してセキュリティ関連のハードウェア、ソフトウェア、およびファームウェアへのインタフェースを指定する正式なトップレベルの仕様を作成する。

(b) 必要に応じて追加の非公式なデモンストレーションで、正式なトップレベルの仕様が正式なポリシーモデルと一貫していることを、実現可能な範囲で証明することにより示す。

(c) 非公式のデモンストレーションにより、正式なトップレベルの仕様がセキュリティ関連のハードウェア、ソフトウェア、およびファームウェアへのインタフェースを完全にカバーしていることを示す。

(d) 正式なトップレベルの仕様が、実装されたセキュリティ関連のハードウェア、ソフトウェア、およびファームウェアの正確な記述であることを示す。

(e) 正式なトップレベルの仕様では扱われていないが、厳密に言えば内部で対応されているセキュリティ関連のハードウェア、ソフトウェア、およびファームウェアのメカニズムを説明する。

詳解：対応は、モデル化を通じて得られる保証の重要な部分である。これは、実装がモデルの的確な変換であること、および存在する追加のコードや実装の詳細が、モデル化される動作やポリシーにインパクトを与えないことを示している。正式な方法を使用して、高レベルのセキュリティ特性が正式なシステム記述によって満たされていること、および正式なシステム記述がハードウェア記述を含む何らかの下位レベルの記述によって正しく実装されていることを示すことができる。正式なトップレベルの仕様と正式なポリシーモデルとの一貫性は、一般に、十分に実証されていない。したがって、そのような一貫性を実証するために、正式な方法と非公式な方法の組み合わせが必要になる場合がある。正式なトップレベル仕様と実際の実装との整合性を保つには、仕様が実装を的確に反映していることを証明するための正式な方法の適用性に限定があるため、非公式な実物に沿ったデモンストレーションを使用しても良い。セキュリティ関連コンポーネントの内部にあるハードウェア、ソフトウェア、およびファームウェアのメカニズムには、マッピングレジスタやダイレクトメモリの入出力などがある。

関連管理策：AC-3, AC-4, AC-25, SA-4, SA-5

(4) 開発者のセキュリティおよびプライバシーのアーキテクチャおよび設計 | 非公式な対応

システム、システムコンポーネント、またはシステムサービスの開発者に以下を要求する。

(a) 開発プロセスの不可欠な部分として、例外、エラーメッセージ、および影響に関して、セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアへのインタフェースを指定する、非公式の記述的トップレベル仕様を作成する。

(b) [*選択：非公式なデモンストレーション；可能な限り正式な方法で説得力のある議論*]を介して、記述的なトップレベルの仕様が正式なポリシーモデルと一致していることを示す。

(c) 非公式なデモンストレーションにより、トップレベルの記述仕様がセキュリティ関連のハードウェア、ソフトウェア、ファームウェアへのインタフェースを正確にカバーしていることを示す。

(d) 記述的なトップレベルの仕様が、セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアへのインタフェースの的確な記述であることを示す。

(e) 最上位の記述仕様で扱われていないが、セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアの内部に厳密に組み込まれている、セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアのメカニズムを説明する。

詳解：対応は、モデル化を通じて得られる保証の重要な部分である。これは、実装がモデルの的確な変換であること、および追加のコードまたは実装の詳細がモデル化される動作またはポリシーにインパクトを与えないことを示している。記述的なトップレベルの仕様（すなわち、ハイレベル／ローレベルの設計）と正式なポリシーモデルとの整合性は、一般に、十分に立証されていない。したがって、そのような一貫性を示すために、正式な方法と非公式な方法の組み合わせが必要になる場合がある。セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアに厳密に内在するハードウェア、ソフトウェア、およびファームウェアのメカニズムには、マッピングレジスタおよび直接メモリ入出力が含まれる。

関連管理策：AC-3, AC-4, AC-25, SA-4, SA-5

(5) 開発者のセキュリティおよびプライバシーのアーキテクチャおよび設計 | 概念的にシンプルな設計

システム、システムコンポーネント、またはシステムサービスの開発者に以下を要求する。

(a) セキュリティに関連するハードウェア、ソフトウェア、およびファームウェアを設計および構造化して、厳密に規定された意味を備えた、正確で概念的に単純な保護メ

カニズムを使用する。

(b) このメカニズムに特に注意して、セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアを内部的に構築する。

詳解：複雑さを軽減するという原則は、システム設計は可能な限りシンプルで小さいと述べている（SA-8(7)を参照）。小さくシンプルな設計は、理解と分析が容易であり、エラーが発生しにくい（AC-25、SA-8(13)を参照）。複雑さを軽減するという原則は、システムのあらゆる側面に適用されるが、システムの緊急時のセキュリティ特性に関するエビデンスを得るために実行される様々な分析のため、セキュリティにとって特に重要である。このような分析を成功させるには、小さくてシンプルな設計が不可欠である。複雑さを軽減するという原則の適用は、システム開発者がシステムセキュリティ機能の適合性と正確性を理解し、潜在的な脆弱性の特定を容易にすることに貢献する。複雑さが軽減された当然の結果として、システムの単純性は、システムに含まれる脆弱性の数に直接関係していることが分かる。つまり、シンプルなシステムほど脆弱性が少なくなる。複雑さを軽減することの重要な利点は、セキュリティポリシーがシステム設計にキャプチャされているかどうかを理解しやすくなること、およびエンジニアリング開発中に導入される脆弱性が少なくなる可能性があることである。追加の利点は、システム設計が本質的に複雑な状況で到達する結論とは対照的に、適合性、正確性、および脆弱性の存在に関するそのような結論に、より高い保証度で到達できることである。

関連管理策：AC-25, SA-8, SC-3

(6) 開発者のセキュリティおよびプライバシーのアーキテクチャおよび設計｜テストのための構造

テストを容易にするために、システム、システムコンポーネント、またはシステムサービスの開発者に、セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアを構築することを要求する。

詳解：[SP 800-160-1]のセキュリティ設計原則を適用すると、システム、システムコンポーネント、およびサービスの正確かつ一貫性のある包括的なテストと評価が促進される。そのようなテストの徹底は、システム、システムコンポーネント、またはサービスの統合的信頼性に関する効果的な保証ケースまたは議論を生成するために作成されたエビデンスに貢献する。

関連管理策：SA-5, SA-11

(7) 開発者のセキュリティおよびプライバシーのアーキテクチャおよび設計｜最小特権の構造

システム、システムコンポーネント、またはシステムサービスの開発者に、セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアを構築して、最小特権でアクセスを制御できるようにすることを要求する。

詳解：最小特権の原則では、各コンポーネントには指定された機能を実行するのに十分な特権が割り当てられているが、それ以上は割り当てられていない（SA-8(14)を参照）。最小特権の原則を適用すると、コンポーネントのアクションの範囲が限定され、2 つの望ましい影響がある。まず、システムコンポーネントの障害、破損、または誤用によるセキュリティへのインパクトは、セキュリティへのインパクトを最小限に抑える。次に、コンポーネントのセキュリティ分析が簡素化される。最小限の特権は、セキュアなシステム設計のすべての側面に反映される一般的な原則である。コンポーネント機能を呼び出すために使用されるインタフェースは、ユーザ集団の特定のサブセットのみが使用でき、コンポーネント設計は、特権分解の十分に細かい粒度をサポートしている。例えば、監査メカニズムの場合、監査設定を構成する監査マネージャー用のインタフェース；監査データが安全に収集および保管されることを保証する監査オペレータのためのインタフェース；および、収集された監査データを表示するだけで、そのデータに対して操作を実行する必要がない監査レビューアのためのさらに別のインタフェースなどが存在する場合がある。

システムインタフェースでの明示に加えて、最小特権は、システム自体の内部構造の指針として使用できる。内部最小特権の 1 つの側面は、モジュールをカプセル化した要素のみがモジュール内の関数によって直接操作されるようにモジュールを構築することである。モジュールの操作によって影響を受ける可能性のあるモジュールの外部の要素は、それ

らの要素を含むモジュールとの相互作用（例えば、関数呼び出しを介して）を通じて間接的にアクセスされる。内部最小特権の別の側面は、所定のモジュールまたはコンポーネントのスコープには、その機能に必要なシステム要素のみが含まれ、要素へのアクセスモード（例えば、読み取り、書き込み）が最小限であることである。

関連管理策：AC-5, AC-6, SA-8

(8) 開発者のセキュリティおよびプライバシーのアーキテクチャおよび設計 | オーケストレーション

[*設定：組織が定めるシステムまたはコンポーネントによる機能*]を[*設定：組織が定める重要なシステムまたはシステムコンポーネント*]に実装するために調整された振る舞いを備えた設計にする。

詳解：分散されているか、異なる層または異なるシステム要素に配置されているか、統合的信頼性の異なる側面をサポートするために実装されているセキュリティリソースは、予期しないまたは不正確な方法で相互作用する可能性がある。悪影響には、連鎖的な障害、干渉、カバレッジギャップなどがある。セキュリティリソースの動作を調整することで（例えば、1 つのパッチがすべてのリソースにインストールされていることを確認してから、パッチが伝播されていると想定して構成を変更することにより）、このような否定的な相互作用を回避することができる。

関連管理策：なし

(9) 開発者のセキュリティおよびプライバシーのアーキテクチャおよび設計 | 設計の多様性

[*設定：組織が定める重要なシステムまたはシステムコンポーネント*]に異なる設計を使用して、共通の要件を満たすか、同等の機能を提供する。

詳解：設計の多様性は、同じ要件仕様を複数の開発者に提供することによって達成され、各開発者は、要件を満たすシステムまたはシステムコンポーネントの変化型を開発する責任を負う。変化型は、ソフトウェア設計、ハードウェア設計、またはハードウェアとソフトウェアの両方の設計に存在することができる。設計の変化型の違いは、開発者の経験（例えば、設計パターンの以前の使用）、設計スタイル（例えば、必要な機能をより小さなタスクに分解するとき、個別のタスクを構成するもの、およびタスクをサブタスクに分解する距離を決定することに起因する可能性がある。）、変化型に組み込むライブラリの選択、および開発環境（例えば、異なる設計ツールを使用すると、いくつかの設計パターンを視覚化しやすくなる）。ハードウェア設計の多様性には、どの形式の情報をアナログ形式で保持し、どの形式の情報をデジタル形式に変換するかを決定すること、同じ情報を異なるタイミングで伝送すること、サンプリングに遅延を導入すること（時間的多様性）などがある。設計の多様性は、一般的に耐障害性をサポートするために使用される。

関連管理策：なし

参照資料：[ISO 15408-2], [ISO 15408-3], [SP 800-160-1]

SA-18 耐タンパー性および検知

［撤回：SR-9 に移動した］

拡張管理策：

(1) 耐タンパー性および検知 | システム開発ライフサイクルの複数のフェーズ

［撤回：SR-9(1)に移動した］

(2) 耐タンパー性および検知 | システムまたはコンポーネントの検査

［撤回：SR-10 に移動した］

SA-19 コンポーネントの真正性

［撤回：SR-11 に移動した］

拡張管理策:

(1) コンポーネントの真正性 | 偽造防止トレーニング

[撤回:SR-11(1)に移動した]

(2) コンポーネントの真正性 | コンポーネントのサービスおよび修理のための構成管理

[撤回:SR-11(2)に移動した]

(3) コンポーネントの真正性 | コンポーネントの廃棄

[撤回:SR-12 に移動した]

(4) コンポーネントの真正性 | 偽造防止の精査

[撤回:SR-11(3)に移動した]

SA-20 重要コンポーネントのカスタム開発

管理策:[*設定:組織が定める重要なシステムコンポーネント*]を再実装またはカスタム開発する。

詳解:組織は、リスクを適切に軽減するための実行可能なセキュリティ管理策がないコンポーネントに対する特定の脅威と内在する脆弱性により、特定のシステムコンポーネントが信頼できない可能性が高いと判断する。そのようなコンポーネントの再実装またはカスタム開発は、より高い保証の要件を満たしても良く、敵対者による標準的な攻撃が成功する可能性が低くなるように、システムコンポーネント(ハードウェア、ソフトウェア、およびファームウェアを含む)への変更を開始することによって成し遂げられる。代替の調達手段がなく、組織が重要なシステムコンポーネントを再実装またはカスタム開発しないことを選択する状況では、追加の管理策を採用することができる。管理策には、強化された監査、ソースコードおよびシステムユーティリティへのアクセスの制限、システムファイルおよびアプリケーションファイルの削除からの保護が含まれる。

関連管理策:CP-2, RA-9, SA-8

拡張管理策:なし

参照資料:[SP 800-160-1]

SA-21 開発者のスクリーニング

管理策:[*設定:組織が定めるシステム、システムコンポーネント、またはシステム サービス*]の開発者に以下を要求する。

a. 設定された[*設定:組織が定める公務*]によって決定される適切なアクセス認可を持っていること。

b. [*設定:組織が定める追加職員スクリーニング基準*]を満たすこと。

詳解:開発者のスクリーニングは外部の開発者を対象としている。内部開発者のスクリーニングは、PS-3 で対処される。システム、システムコンポーネント、またはシステムサービスは、米国の国家的または経済的安全保障上の利益に不可欠な重要な活動に使用される可能性があるため、組織は開発者の信頼性を確保することに強い関心を持っている。開発者に要求される信頼の程度は、展開されたシステム、システムコンポーネント、またはシステムサービスにアクセスする個人の信頼の程度と一致している必要がある場合がある。認可および職員のスクリーニング基準には、クリアランス、身元調査、市民権、および国籍が含まれる。開発者の統合的信頼性には、会社の所有権ならびに開発中のシステム、コンポーネント、またはサービスの品質と信頼性に影響を与える可能性のあるエンティティとの関係のレビューと分析も含まれる場合がある。必要なアクセス認可と職員スクリーニング基準を満たすには、開発者が権限とスクリーニング要件を満たしていることを組織が検証できるように、選択したシステム、システムコンポーネント、またはシステムサービスで開発活動を実行する権限があるべての個人のリストを提供することが含まれる。

関連管理策：PS-2, PS-3, PS-6, PS-7, SA-4, SR-6

拡張管理策：

(1) 開発者スクリーニング｜スクリーニングの妥当性確認

［撤回：SA-21 に組み込まれた］

参照資料：なし

SA-22 サポートされていないシステムコンポーネント

管理策：

a. 開発者、ベンダ、または製造元からのコンポーネントのサポートが利用できなくなった場合は、システムコンポーネントを交換する。または

b. サポートされていないコンポーネントを継続的にサポートするための代替ソースとして［*選択（1 つ以上）：社内サポート；［設定：組織が定める外部プロバイダからのサポート］*］のオプションを提供する。

詳解：システムコンポーネントのサポートには、ソフトウェアパッチ、ファームウェアアップデート、交換部品、およびメンテナンス契約が含まれる。サポートされていないコンポーネントの例としては、ベンダが重要なソフトウェアパッチまたは製品アップデートを提供しなくなった場合が含まれ、結果として敵対者がインストールされたコンポーネントの弱点を悪用する可能性をもたらす。サポートされていないシステムコンポーネントを交換する場合の例外には、新しい技術が利用できない、またはシステムが分離されているため交換用コンポーネントをインストールできない場合に、重要なミッションまたは事業の機能を提供するシステムが含まれる。

サポートの代替ソースは、元の製造者、開発者、またはベンダによってサポートされなくなったシステムコンポーネントが、組織のミッションおよび事業の機能に不可欠である場合に、そのサポートを継続的に提供する必要性に対処する。組織は、必要に応じて、重要なソフトウェアコンポーネント用にカスタマイズされたパッチを開発することで社内サポートを確立したり、契約関係を通じて指定されたサポートされていないコンポーネントに継続的なサポートを提供する外部プロバイダのサービスを利用できる。このような契約関係には、オープンソースソフトウェアの付加価値ベンダを含めることができる。サポートされていないシステムコンポーネントを使用するリスクの増加は、例えば、そのようなコンポーネントのパブリックネットワークまたは管理されていないネットワークへの接続を禁止したり、他の形式の分離を実装したりすることによって軽減できる。

関連管理策：PL-2, SA-3

拡張管理策：

(1) サポートされていないシステムコンポーネント｜継続的サポートの代替ソース

［撤回：SA-22 に組み込まれた］

参照資料：なし

SA-23 特殊化

管理策：［*設定：組織が定めるシステムまたはシステムコンポーネント*］に［*選択（1 つ以上）：設計；変更；拡張；再構成*］を採用し、ミッションに不可欠なサービスまたは機能をサポートし、それらのシステムまたはコンポーネントの統合的信頼性を高める。

詳解：リソースの統合的信頼性を最大化するために、ミッションに不可欠なサービスまたは機能をサポートするシステムまたはシステムコンポーネントを強化する必要がある場合がよくある。この拡張機能は、設計レベルで行われる場合がある。 他の例では、問題のシステムを変更するか、システムに追加のコンポーネントを追加することにより、設計後に行われる。例えば、補足的な認証または否認防止機能をシステムに追加して、組織の定めるリソースに依存する他のリソースに対する重要なリソースのアイデンティティを強化しても良い。

関連管理策：RA-9, SA-8

拡張管理策：なし

参照資料：[SP 800-160-1], [SP 800-160-2]

3.18 システムおよび通信の保護

システムおよび通信の保護の要約表へのクイックリンク

SC-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。

1. 以下の[*選択(1 つ以上):組織レベル;ミッション/事業プロセスレベル;システムレベル*]のシステムおよび通信の保護ポリシー。

(a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、および準拠に対処する。

(b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに適合している。

2. システムおよび通信の保護のポリシーと関連するシステムおよび通信の保護の管理策の実装を促進するための手順。

b. システムおよび通信の保護のポリシーと手順の策定、文書化、および配布することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行のシステムおよび通信の保護をレビューし、更新する。

1. ポリシーについて[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

2. 手順について[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

詳解:システムおよび通信の保護のポリシーと手順は、システムおよび組織で実装される SC ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に寄与する。したがって、セキュリティおよびプライバシープログラムがシステムおよび通信の保護のポリシーと手順の策定と連携していることが重要である。セキュリティおよびプライバシープログラムのポリシーと手順を組織レベルで確立することは望ましく、一般的には、ミッションまたはシステム固有のポリシーと手順を不要にすることができる。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映する複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムに対して規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述し、手順の対象である個人または役割向けとすることができる。手順は、システムのセキュリティおよびプライバシー計画の中に、または 1 つ以上の別の文書に文書化することもできる。システムおよび通信の保護のポリシーと手順の更新を引き起こす可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれる。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策:PM-9, PS-8, SA-8, SI-12

拡張管理策:なし

参照資料:[OMB A-130], [SP 800-12], [SP 800-100]

SC-2 システムおよびユーザ機能の分離

管理策：ユーザインタフェースサービスを含むユーザ機能をシステム管理機能から分離する。

詳解：システム管理機能には、データベース、ネットワークコンポーネント、ワークステーション、またはサーバを管理するために必要な機能が含まれる。これらの機能には通常、特権ユーザアクセスが必要である。ユーザ機能とシステム管理機能の分離は、物理的または論理的である。組織は、様々なコンピュータ、オペレーティングシステムのインスタンス、中央処理装置、またはネットワークアドレスを使用することにより、システム管理機能をユーザ機能から分離することができる。仮想化技法を採用する。またはこれらまたは他の方法のいくつかの組み合わせ。システム管理機能とユーザ機能の分離には、他のシステムリソースのユーザに対して個別の認証方法を採用するウェブ管理インタフェースが含まれる。システム機能とユーザ機能の分離には、異なるドメイン上の管理インタフェースを分離し、追加のアクセス制御を含めることが含まれる場合がある。システムとユーザの機能性の分離は、SA-8(1)、SA-8(3)、SA-8(4)、SA-8(10)、SA-8(12)、SA-8(13)、SA-8(14)、SA-8(18)を含む SA-8 のシステムセキュリティエンジニアリング設計原則を適用することにより達成できる。

関連管理策：AC-6, SA-4, SA-8, SC-3, SC-7, SC-22, SC-32, SC-39

拡張管理策：

(1) システムおよびユーザ機能の分離 | 非特権ユーザのためのインタフェース

非特権ユーザへのインタフェースでのシステム管理機能の提示を防止する。

詳解：非特権ユーザへのインタフェースでシステム管理機能が表示されないようにすることで、管理者特権を含むシステム管理オプションを一般ユーザが利用できないようにすることができる。ユーザのアクセスを制限すると、そのような情報へのアクセシビリティを排除するために一般的に使用されるグレーアウトオプションの使用も禁止される。考えられる解決策の 1 つは、ユーザが管理者特権でセッションを確立するまで、システム管理オプションを保留することである。

関連管理策：AC-3

(2) システムおよびユーザ機能の分離 | 分離可能性

アプリケーションとソフトウェアの状態情報を別々に保存する。

詳解：システムが侵害された場合、アプリケーションとソフトウェアをユーザとアプリケーションとのやりとりに関する状態情報とは別に保存することで、個人のプライバシーを保護することができる。

関連管理策：なし

参照資料：なし

SC-3 セキュリティ機能の分離

管理策：セキュリティ機能を非セキュリティ機能から分離する。

詳解：セキュリティ機能は、パーティションとドメインを介してシステム内に実装された分離境界によって非セキュリティ機能から分離される。分離境界は、システムセキュリティ機能を実行するハードウェア、ソフトウェア、およびファームウェアへのアクセスを制御し、その完全性を保護する。システムは、プロセッサリングやプロセッサモードを介したセキュリティカーネルの提供など、様々な方法でコード分離を実装する。非カーネルコードの場合、セキュリティ機能の分離は、多くの場合、ディスク上のコードを保護するファイルシステム保護と、実行中のコードを保護するアドレス空間保護によって対処される。システムは、アクセス制御メカニズムを使用し、最小特権機能を実装することにより、セキュリティ機能へのアクセスを制限できる。理想は、規定されたセキュリティ機能分離境界内のすべてのコードがセキュリティ関連コードのみを含むことであるが、非セキュリティ機能を例外として含めることが必要な場合がある。非セキュリティ機能からセキュリティ機能を分離するには、SA-8(1)、SA-8(3)、SA-8(4)、SA-8(10)、SA-8(12)、SA-8(13)、SA-8(14)、SA-8(18)を含む SA-8 のシステムセキュリティエンジニアリング設計原則を適用する。

関連管理策：AC-3, AC-6, AC-25, CM-2, CM-4, SA-4, SA-5, SA-8, SA-15, SA-17, SC-2, SC-7, SC-32, SC-39, SI-16

拡張管理策：

(1) セキュリティ機能の分離 | ハードウェアの分離

ハードウェアの分離メカニズムを採用して、セキュリティ機能の分離を実装する。

詳解：ハードウェアの分離メカニズムには、マイクロプロセッサ内に実装されるハードウェアリングアーキテクチャと、個別の属性（読み取り可能、書き込み可能）を持つ論理的に異なる保存媒体をサポートするために使用されるハードウェア強制アドレスセグメンテーションが含まれる。

関連管理策：なし

(2) セキュリティ機能の分離 | アクセスおよびフロー制御機能

アクセスおよび情報フロー制御を実施するセキュリティ機能を、非セキュリティ機能および他のセキュリティ機能から分離する。

詳解：セキュリティ機能の分離は、実装により生じる。機能は引き続きスキャンおよび監視できる。アクセスおよびフロー制御の実施機能から潜在的に隔離されているセキュリティ機能には、監査、侵入検知、および悪意のあるコードからの保護機能が含まれる。

関連管理策：なし

(3) セキュリティ機能の分離 | 非セキュリティ機能の最小化

セキュリティ機能を含む分離境界内に含まれる非セキュリティ機能の数を最小化する。

詳解：セキュリティ機能から非セキュリティ機能を厳密に分離することが可能でない場合、セキュリティ機能境界内の非セキュリティ関連機能を最小化するための措置を講じる必要がある。分離境界内に含まれる非セキュリティ機能は、ソフトウェアのエラーまたは悪意のあるコードがシステムのセキュリティ機能に直接影響を与える可能性があるため、セキュリティ関連と見なされる。基本的な設計目標は、情報セキュリティを提供するシステムの特定の部分のサイズと複雑さが最小限であることである。セキュリティ関連のシステムコンポーネントの非セキュリティ機能の数を最小限に抑えることで、設計者と実装者は、目的のセキュリティ機能（通常はアクセスの実施）を提供するために必要な機能のみに集中することができる。分離境界内の非セキュリティ機能を最小限に抑えることで、セキュリティポリシーを適用するために信頼されるコードの量が大幅に削減され、理解のしやすさが向上する。

関連管理策：なし

(4) セキュリティ機能の分離 | モジュールの結合度および凝集度

セキュリティ機能を、モジュール内の内部結合度を最大化し、モジュール間の凝集度を最小化する独立したモジュールとして実装する。

詳解：モジュール間の相互作用を減らすことで、セキュリティ機能を抑制し、複雑さを管理することができる。結合と凝集度の概念は、ソフトウェア設計におけるモジュール性に関して重要である。結合とは、あるモジュールが他のモジュールに依存していることを意味する。凝集度とは、モジュール内の機能間の関係を指す。ソフトウェアエンジニアリングおよびシステムセキュリティエンジニアリングの最善の措置は、複雑化を軽減および管理するために、階層化、最小化、およびモジュール分解に依存している。これにより、非常にまとまりがある、疎結合のソフトウェアモジュールが生成される。

関連管理策：なし

(5) セキュリティ機能の分離 | 階層構造

セキュリティ機能を階層構造として実装し、設計の階層間の相互作用を最小化し、下位階層による機能性や上位階層の適合性への依存を回避する。

詳解：セキュリティ機能と非ループ層の間の相互作用を最小化した階層構造の実装（すなわち、下位層の機能は上位層の機能に依存しない）により、セキュリティ機能の分離と複

雑性の管理が可能になる。

関連管理策：なし

参照資料：なし

SC-4 共有システムリソース内の情報

管理策：共有システムリソースを介した認可されていない意図しない情報転送を防止する。

詳解：共有システムリソースを介した認可されていない意図しない情報転送を防止することで、以前のユーザまたはロールのアクション（または以前のユーザまたはロールに代わって動作するプロセスのアクション）によって生成された情報を、リソースがリリースされた後に共有システムリソースへのアクセスを取得する現在のユーザまたはロール（または現在のユーザまたはロールに代わって動作する現在のプロセス）に対して利用できないようにする。共有システムリソース内の情報は、情報の暗号化表現にも適用される。他の状況では、共有システムリソース内の情報の制御は、オブジェクトの再利用および残存情報保護と呼ばれる。共有システムリソース内の情報は、名目上削除されたデータの残余表現を指す、情報の残留性には対応していない；情報フローの制限に違反するように共有システムリソースが操作される隠れチャネル（ストレージチャネルおよびタイミングチャネルを含む）；または、単一のユーザまたはロールしかないシステム内のコンポーネント。

関連管理策：AC-3, AC-4, SA-8

拡張管理策：

(1) 共有システムリソース内の情報 | セキュリティレベル

［撤回：SC-4 に組み込まれた］

(2) 共有システムリソース内の情報 | マルチレベルまたは期間処理

システム処理が異なる情報の分類レベルまたはセキュリティの分類を明示的に切り替える場合、［*設定：組織が定める手順*］に従って、共有リソースを介した認可されていない情報転送を防止する。

詳解：処理レベルの変更は、様々な分類レベルまたはセキュリティの分類の情報を使用して、マルチレベルまたは期間処理中に発生する可能性がある。また、異なる分類レベルでのハードウェアコンポーネントの連続的な再利用中にも発生する可能性がある。組織が定める手順には、電子的に保存された情報の承認済みの削除プロセスを含めることができる。

関連管理策：なし

参照資料：なし

SC-5 サービス拒否からの保護

管理策：

a. ［*設定：組織が定めるサービス拒否イベントのタイプ*］の影響を［*選択：保護する；限定する*］。

b. サービス拒否の目的を達成するために、［*設定：サービス拒否イベントのタイプによる組織が定める管理策*］を採用する。

詳解：サービス拒否イベントは、敵対者による攻撃や、容量と帯域幅に関する組織のニーズをサポートする計画の欠如など、内部および外部の様々な原因によって発生する可能性がある。このような攻撃は、様々なネットワークプロトコル（IPv4、IPv6 など）で発生する可能性がある。サービス拒否イベントの発生と影響を限定または排除するために、様々な技術が利用可能である。例えば、境界保護デバイスは、特定のタイプのパケットをフィルタリングして、内部ネットワーク上のシステムコンポーネントをサービス拒否攻撃の直接の影響を受けたり、サービス拒否攻撃のソースから保護したりすることができる。ネットワーク容量と帯域幅の増加とサービスの冗長性と相まって、サービス拒否イベントの影響を受けにくくなる。

関連管理策：CP-2, IR-4, SC-6, SC-7, SC-40

拡張管理策：

(1) サービス拒否からの保護 | 他のシステムへの攻撃能力の制限

個人が他のシステムに対して[*設定：組織が定めるサービス拒否攻撃*]を仕掛ける能力を制限する。

詳解：サービス拒否攻撃を仕掛ける個人の能力を制限するには、そのような攻撃に一般的に使用されるメカニズムを利用できないようにする必要がある。懸念のある個人には、システムを侵害またはブリーチし、それを使用してサービス拒否攻撃を仕掛ける敵対的なインサイダーまたは外部の敵対者が含まれる。組織は、個人が輸送媒体（すなわち、有線ネットワーク、無線ネットワーク、なりすましインターネットプロトコルパケット）上で任意の情報を接続および伝送する能力を限定することができる。サービス拒否攻撃を仕掛ける能力を持つ個人に対する保護は、標的となる可能性のあるシステムへの送信を禁止する特定のシステムまたは境界デバイスに実装される場合がある。

関連管理策：なし

(2) サービス拒否からの保護 | 容量、帯域幅、および冗長性

容量、帯域幅、またはその他の冗長性を管理して、情報フラッディングサービス拒否攻撃の影響を限定する。

詳解：容量を管理することで、フラッディング攻撃に対抗するために十分な容量を確保できる。容量の管理には、選択した使用優先順位、割り当て、パーティション分割、または負荷分散の確立が含まれる。

関連管理策：なし

(3) サービス拒否からの保護 | 検知および監視

(a) [*設定：組織が定める監視ツール*]を使用して、システムに対する、またはシステムから起動されたサービス拒否攻撃の兆候を検知する。

(b) [*設定：組織が定めるシステムリソース*]を監視して、効果的なサービス拒否攻撃を防止するのに十分なリソースが存在するかどうかを判断する。

詳解：組織は、悪意のある攻撃によるサービス拒否に関連するリスクを管理する際に、システムリソースの使用率と容量を考慮する。サービス拒否攻撃は、外部または内部のソースから発生する可能性がある。サービス拒否の影響を受けやすいシステムリソースには、物理ディスクストレージ、メモリ、CPU サイクルなどがある。ストレージの使用率と容量に関連するサービス拒否攻撃を防止するために使用される技法には、ディスククォータの設定、特定の記憶容量のしきい値に達したときに管理者に自動的に警告するシステムの設定、ファイル圧縮技術を使用した利用可能なストレージ容量の最大化、およびシステムおよびユーザデータに別々のパーティションを強制する。

関連管理策：CA-7, SI-4

参照資料：[SP 800-189]

SC-6 リソースの可用性

管理策：[*設定：組織が定めるリソース*]を[*選択（1 つ以上）：優先度；割当量；*[*設定：組織が定める管理策*]]で設定することにより、リソースの可用性を保護する。

詳解：優先度保護は、優先度の低いプロセスが、優先度の高いプロセスを処理するシステムを遅延または妨害することを防止する。割当量は、ユーザまたはプロセスが所定の量を超えるリソースを取得することを防ぐ。

関連管理策：SC-5

拡張管理策：なし

参照資料：[OMB M-08-05], [DHS TIC]

SC-7 境界保護

管理策:

a. システムへの外部管理インタフェースおよびシステム内の主要な内部管理インタフェースにおける通信を監視および制御する。

b. 内部組織ネットワークから[*選択:物理的;論理的*]に分離されている、公的にアクセス可能なシステムコンポーネントのサブネットワークを実装する。

c. 組織のセキュリティとプライバシーのアーキテクチャに従って配置された境界保護デバイスで構成される管理対象インタフェースのみを介して、外部ネットワークまたはシステムに接続する。

詳解:管理対象インタフェースには、ゲートウェイ、ルータ、ファイアウォール、ガード、ネットワークベースの悪意のあるコード分析、仮想化システム、またはセキュリティアーキテクチャ内に実装された暗号化トンネルなどがある。内部ネットワークから物理的または論理的に分離されたサブネットワークは、非武装地帯または DMZ と呼ばれる。組織のシステム内のインタフェースを制限または禁止することには、管理対象インタフェース内の指定されたウェブサーバへの外部ウェブトラフィックを制限すること、内部アドレスになりすましているように見える外部トラフィックを禁止すること、外部アドレスになりすましているように見える内部トラフィックを禁止することが含まれる。[SP 800-189]は、偽装アドレスによるトラフィックの出入りを防止するためのソースアドレス妥当性確認技法に関する追加情報を提供する。商用通信サービスは、顧客が共有するネットワークコンポーネントと統合管理システムによって提供される。これらのサービスには、サードパーティが提供するアクセス回線やその他のサービス要素も含まれる場合がある。そのようなサービスは、契約のセキュリティ規定にもかかわらず、リスクの増大の原因となる可能性がある。境界保護は、保護対象の境界がシステム固有の境界(すなわち、認可境界)よりも大きくなるように、組織ネットワークのすべてまたは一部の共通制御として実装することができる。

関連管理策:AC-4, AC-17, AC-18, AC-19, AC-20, AU-13, CA-3, CM-2, CM-4, CM-7, CM-10, CP-8, CP-10, IR-4, MA-4, PE-3, PL-8, PM-12, SA-8, SA-17, SC-5, SC-26, SC-32, SC-35, SC-43

拡張管理策:

(1) 境界保護 | 物理的に分離されたサブネットワーク

[撤回:SC-7 に組み込まれた]

(2) 境界保護 | パブリックアクセス

[撤回:SC-7 に組み込まれた]

(3) 境界保護 | アクセスポイント

システムへの外部ネットワーク接続の数を限定する。

詳解:外部ネットワーク接続の数を限定すると、インバウンドおよびアウトバウンドの通信トラフィックの監視が容易になる。 信頼できるインターネット接続[DHS TIC]イニシアチブは、外部ネットワーク接続の数に限定を必要とする米国政府のガイドラインの一例である。システムへの外部ネットワーク接続の数を限定することは、古い技術から新しい技術への移行期間中(例えば、IPv4 から IPv6 ネットワークプロトコルへの移行中)に重要である。このような移行では、移行期間中に古い技術と新しい技術を同時に実装する必要があり、システムへのアクセスポイントの数が増える場合がある。

関連管理策:なし

(4) 境界保護 | 外部通信サービス

(a) 各外部通信サービスに管理インタフェースを実装する。

(b) 管理対象インタフェースごとにトラフィックフローポリシーを確立する。

(c) 各インタフェースを介して伝送される情報の機密性と完全性を保護する。

(d) トラフィックフローポリシーが適用されない個々の例外を、それらを裏付けるミッションや事業の必要性と、その必要がある期間と共に、文書化する。

(e) トラフィックフローポリシーの例外を[*設定：組織が定める頻度*]でレビューし、明確なミッションまたは事業上のニーズによって維持する必要のなくなった例外を削除する。

(f) 外部ネットワークとのコントロールプレーントラフィックの認可されていない交換を防止する。

(g) リモートネットワークが内部ネットワークからの認可されていないコントロールプレーントラフィックを検知できるようにするための情報を公開する。

(h) 外部ネットワークからの認可されていないコントロールプレーントラフィックをフィルタリングする。

詳解：外部通信サービスは、データおよび／または音声通信サービスを提供することができる。コントロールプレーントラフィックの例には、ボーダーゲートウェイプロトコル（BGP：Border Gateway Protocol）ルーティング、ドメインネームシステム（DNS：Domain Name System）、管理プロトコルなどがある。BGP ルートを保護し、認可されていない BGP アナウンスを検知するためのリソース公開鍵基盤（RPKI：resource public key infrastructure）の使用に関する追加情報については、[SP 800-189]を参照。

関連管理策：AC-3, SC-8, SC-20, SC-21, SC-22

(5) 境界保護 | デフォルトで拒否 ― 例外で許可

[*選択（1 つ以上）：管理対象インタフェース；*[*設定：組織が定めるシステム*]]において、デフォルトでネットワーク通信トラフィックを拒否し、例外によりネットワーク通信トラフィックを許可する。

詳解：デフォルトで拒否し、例外で許可することは、インバウンドおよびアウトバウンドのネットワーク通信トラフィックに適用される。すべて拒否、例外による許可のネットワーク通信トラフィックポリシーでは、必須かつ承認済みのシステム接続のみが許可されるようにする。デフォルトで拒否、例外として許可は、外部システムに接続されているシステムにも適用される。

関連管理策：なし

(6) 境界保護 | 認識された障害への対応

［撤回：SC-7(18)に組み込まれた］

(7) 境界保護 | リモートデバイスのスプリットトンネリング

[*設定：組織が定める保全措置*]を使用してスプリットトンネリングがセキュアに提供されていない限り、組織のシステムに接続するリモートデバイスのスプリットトンネリングを防止する。

詳解：スプリットトンネリングは、リモートユーザまたはデバイスがシステムとの非リモート接続を確立し、同時に外部ネットワーク内のリソースへの他の接続を介して通信できるようにするプロセスである。このネットワークアクセス方法により、ユーザはリモートデバイスにアクセスすると同時に、制御されていないネットワークにアクセスすることができる。リモートユーザは、プリンタやファイルサーバなどのローカルシステムリソースと通信するために、スプリットトンネリングが望ましい場合がある。ただし、スプリットトンネリングは、認可されていない外部接続を容易にし、システムを攻撃や組織情報の漏出に対して脆弱にする可能性がある。スプリットトンネリングは、リモートデバイスでこのような機能を許可する構成設定を無効にし、それらの構成設定をユーザが構成できないようにすることで防止できる。また、リモートデバイスでスプリットトンネリング（またはスプリットトンネリングを許可する構成設定）を検知し、リモートデバイスがスプリットトンネリングを使用している場合は接続を禁止することによっても防止できる。仮想プライベートネットワーク（VPN：virtual private network）を使用して、スプリットトンネリングをセキュアに提供できる。セキュアに提供された VPN には、ユーザの制御なしに、排他的、管理、名前付きの環境、または事前に承認済みの特定のアドレスセットへの接続をロックすることが含まれる。

関連管理策：なし

(8) 境界保護 | 認証済みプロキシサーバへのルートトラフィック

[*設定：組織が定める内部通信トラフィック*]を[*設定：組織が定める外部ネットワーク*]へ、管理対象インタフェースの認証済みプロキシサーバを経由してルーティングする。

詳解：外部ネットワークは、組織の管理外にあるネットワークである。プロキシサーバは、非組織サーバまたは他の組織サーバからシステムリソースを要求するクライアントの仲介者として機能するサーバ（すなわち、システムまたはアプリケーション）である。要求されるシステムリソースには、ファイル、接続、ウェブページ、またはサービスが含まれる。プロキシサーバへの接続を介して確立されたクライアント要求は、複雑さを管理し、直接接続を限定することによって追加の保護を提供するために評価される。ウェブコンテンツフィルタリングデバイスは、インターネットへのアクセスを提供する最も一般的なプロキシサーバの 1 つである。プロキシサーバは、伝送制御プロトコルセッションのロギングと、特定の URL（Uniform Resource Locator）、インターネットプロトコルアドレス、およびドメイン名のブロックをサポートできる。ウェブプロキシは、組織が定める、認可済みおよび認可されていないウェブサイトのリストで構成できる。プロキシサーバは、VPN の使用を禁止し、（実装によっては）「中間者」攻撃を引き起こす可能性があることに注意が必要である。

関連管理策：AC-3

(9) 境界保護 | 脅威となる外向け通信トラフィックの制限

(a) 外部システムへの脅威となる外向け通信トラフィックを検知して拒否する。

(b) 拒否された通信に関連する内部ユーザのアイデンティティを監査する。

詳解：外部システムに脅威をもたらす可能性のある内部アクションからの外向け通信トラフィックを検知することは、エクストルージョン検知と呼ばれる。エクストルージョン検知は、管理されたインタフェースでシステム内で実行される。侵入検知には、外部システムのセキュリティに対するインサイダー脅威の兆候を検索しながら、着信および発信の通信トラフィックを分析することが含まれる。外部システムに対する内部の脅威には、サービス拒否攻撃を示すトラフィック、スプーフィング送信元アドレスを含む偽装されたトラフィック、悪意のあるコードを含むトラフィックなどがある。組織には、エクストルージョン検知に関連して特定された脅威を特定、更新、管理するための基準がある。

関連管理策：AU-2, AU-6, SC-5, SC-38, SC-44, SI-3, SI-4

(10) 境界保護 | 漏出の防止

(a) 情報の漏出を防止する。

(b) [*設定：組織が定める頻度*]で漏出テストを実施する。

詳解：漏出の防止は、意図的な情報の漏出と意図しない情報の漏出の両方に適用される。システムからの情報の漏出を防止するために使用される技法は、内部エンドポイント、外部境界、および管理対象インタフェース全体に実装でき、プロトコル形式の遵守、システムからのビーコン活動の監視、明示的に必要な場合を除いて外部ネットワークインタフェースの切断、トラフィックプロファイルの採用分析を使用して予想される伝送量とタイプからの逸脱を検知し、コマンドおよびコントロールセンターへのコールバックを含むことも良い。侵入テストの実施、ステガノグラフィーの監視、パケット ヘッダーの分解と再構成、データ損失およびデータ漏出防止ツールの使用などが含まれる。プロトコル形式を厳密に遵守するデバイスには、ディープパケットインスペクションファイアウォールやエクステンシブル・マークアップ・ランゲージ（XML：Extensible Markup Language）ゲートウェイなどがある。デバイスは、アプリケーション層のプロトコル形式と仕様への準拠を検証し、ネットワーク層またはトランスポート層で動作するデバイスでは検知できない脆弱性を特定する。漏出の防止は、データ損失防止やデータ漏えい防止に似ており、情報フロー要件を実施するクロスドメインソリューションやシステムガードと密接に関連している。

関連管理策：AC-2, CA-8, SI-3

(11) 境界保護 | 着信通信トラフィックの制限

[*設定：組織が定める認可された送信元*]からの着信通信のみを[*設定：組織が定める宛先*]にルーティングすることを許可する。

詳解：一般的な送信元アドレス妥当性確認技法を適用して、システム内でのみ使用される送信元アドレスだけでなく、認可されていない未設定の送信元アドレスの使用を制限す

る。着信通信トラフィックの制限により、送信元アドレスと宛先アドレスのペアが認可された通信または認可された通信を表すという決定が提供される。決定は、認可または許可された通信のリストにそのようなアドレスのペアが存在する、認可されていないまたは許可されていないペアのリストにそのようなアドレスのペアが存在しない、または認可または許可された送信元と宛先のより一般的な規定を満たすなど、いくつかの要因に基づくことができる。ネットワークアドレスの強力な認証は、明示的なセキュリティプロトコルを使用しないと不可能であり、そのため、アドレスがスプーフィングされることがよくある。さらに、アイデンティティベースの着信トラフィック制限方法を採用することができ、ルータアクセス制御リストおよびファイアウォール規定を含む。

関連管理策：AC-3

(12) 境界保護 | ホストベースの保護

[*設定：組織が定めるシステムコンポーネント*]に[*設定：組織が定めるホストベースの境界保護メカニズム*]を実装する。

詳解：ホストベースの境界保護メカニズムには、ホストベースのファイアウォールが含まれる。ホストベースの境界保護メカニズムを採用するシステムコンポーネントには、サーバ、ワークステーション、ノートブックコンピュータ、モバイルデバイスなどがある。

関連管理策：なし

(13) 境界保護 | セキュリティツール、メカニズム、およびサポートコンポーネントの分離

[*設定：組織が定める情報セキュリティツール、メカニズム、およびサポートコンポーネント*]を、システムの他のコンポーネントへの管理されたインタフェースを備えた物理的に別個のサブネットワークを実装することにより、他の内部システムコンポーネントから分離する。

詳解：管理されたインタフェースを持つ物理的に分離したサブネットワークは、重要な運用処理ネットワークからコンピュータネットワークの防御を分離し、敵対者が組織で採用されている分析およびフォレンジック技法を検出できないようにするのに役立つ。

関連管理策：SC-2, SC-3

(14) 境界保護 | 認可されていない物理的接続からの保護

[*設定：組織が定める管理対象インタフェース*]で、認可されていない物理的接続から保護する。

詳解：システムが同じ施設内のスペースを共有する場合があるため、異なるセキュリティの分類または分類レベルで動作するシステムは、共通の物理的および環境的制御を共有する場合がある。実際には、これらの別々のシステムが、共通の機器室、配線室、ケーブル配線経路を共有する可能性がある。認可されていない物理接続に対する保護は、管理対象インタフェースの両側に、これらの項目への限定された認可アクセスを強制する物理的なアクセス制御を備えた、明確に識別され、物理的に分離されたケーブル トレイ、接続フレーム、パッチ パネルを使用することで実現できる。

関連管理策：PE-4, PE-19

(15) 境界保護 | ネットワーク化された特権アクセス

アクセス制御と監査のために、専用の管理されたインタフェースを介してネットワーク化された特権アクセスをルーティングする。

詳解：特権アクセスにより、セキュリティ機能を含むシステム機能へのアクセシビリティが向上する。敵対者は、リモートアクセスを通じてシステムへの特権アクセスを獲得し、情報の漏出や重要なシステム機能の停止などにより、ミッションや事業に有害なインパクトを与える。専用の管理されたインタフェースを介してネットワーク化された特権アクセス要求をルーティングすると、アクセス制御と監査を強化するために特権アクセスがさらに制限される。

関連管理策：AC-2, AC-3, AU-2, SI-4

(16) 境界保護 | システムコンポーネント検出の防止

管理されたインタフェースを表す特定のシステムコンポーネントの検出を防ぐ。

詳解：管理されたインタフェースを表すシステムコンポーネントの検出を防ぐことは、ネットワーク上のデバイスを識別するために使用される一般的なツールと技法を通じた、それらのコンポーネントのネットワークアドレスの検出から保護するのに役立つ。ネットワークアドレスは検出に使用できず、アクセスするには事前の知識が必要である。コンポーネントおよびデバイスの検出を防ぐには、ネットワークアドレスを公開しないか、ネットワークアドレス変換を使用するか、またはドメインネームシステムにアドレスを入力しないことで実現できる。別の防止技法は、ネットワークアドレスを定期的に変更することである。

関連管理策：なし

(17) 境界保護 | プロトコル形式の自動化された実施

プロトコル形式の順守を強制する。

詳解：プロトコル形式を適用するシステムコンポーネントには、ディープパケットインスペクションファイアウォールや XML ゲートウェイなどがある。コンポーネントは、アプリケーション層でのプロトコル形式と仕様への準拠を検証し、ネットワーク層またはトランスポート層で動作しているデバイスでは検知できない脆弱性を特定する。

関連管理策：SC-4

(18) 境界保護 | フェールセキュア

境界保護デバイスの動作に障害が発生した場合に、システムが非セキュア状態になるのを防ぐ。

詳解：フェールセキュアは、管理対象インタフェースで境界保護デバイスの動作障害が発生した場合に、意図したセキュリティ特性が保持されていない非セキュア状態にならないようにするメカニズムを採用することによって達成される状態である。管理対象インタフェースには、保護されたサブネットワーク（一般に非武装地帯と呼ばれる）に常駐するルータ、ファイアウォール、アプリケーションゲートウェイなどがある。境界保護デバイスの故障は、デバイス外部の情報がデバイスに侵入する原因となることはなく、また、故障が認可されていない情報のリリースを許容することもない。

関連管理策：CP-2, CP-12, SC-24

(19) 境界保護 | 組織外で構成されたホストからの通信のブロック

エンドユーザと外部サービスプロバイダによって個別に構成された[*設定：組織が定める通信クライアント*]間のインバウンドおよびアウトバウンド通信トラフィックをブロックする。

詳解：エンドユーザと外部サービスプロバイダによって個別に構成された通信クライアントには、インスタントメッセージングクライアント、ビデオ会議ソフトウェアおよびアプリケーションが含まれる。トラフィックのブロックは、認可された機能を実行するように組織によって構成された通信クライアントには適用されない。

関連管理策：なし

(20) 境界保護 | 動的な分離および隔離

[*設定：組織が定めるシステムコンポーネント*]を他のシステムコンポーネントから動的に分離する機能を提供する。

詳解：特定の内部システムコンポーネントを動的に分離する機能は、統合的信頼性の高いコンポーネントから問題のある起源のシステムコンポーネントを分割または分離する必要がある場合に有用である。コンポーネントの分離により、組織のシステムの攻撃対象領域が減少する。選択されたシステムコンポーネントを分離することにより、攻撃が発生した場合の攻撃の成功による被害を限定することもできる。

関連管理策：なし

(21) 境界保護 | システムコンポーネントの分離

[*設定：組織が定めるミッションおよび／または事業の機能*]をサポートする[*設定：組織が定めるシステムコンポーネント*]を分離するために、境界保護メカニズムを採用する。

詳解：組織は、異なるミッションや事業の機能を実行するシステムコンポーネントを分離することができる。このような分離により、システムコンポーネント間の認可されていない情報の流れが限定され、選択したシステムコンポーネントに対してより高いレベルの保護を展開する機会が提供される。境界保護メカニズムを備えたシステムコンポーネントを分離することにより、個々のシステムコンポーネントの保護を強化し、それらのコンポーネント間の情報フローをより効果的に制御できる。システムコンポーネントを分離することで、攻撃者対的なサイバー攻撃やエラーによる潜在的な損害を限定する強化された保護が提供される。分離の程度は、選択したメカニズムによって異なる。境界保護メカニズムには、システムコンポーネントを物理的に分離したネットワークまたはサブネットワークに分離するルータ、ゲートウェイ、ファイアウォール；サブネットワークを分離するクロスドメインデバイス；仮想化技法；別個の暗号鍵を使用した、システムコンポーネント間の情報フローの暗号化などがある。

関連管理策：CA-9

(22) 境界保護 | 異なるセキュリティドメインに接続するための個別のサブネット

異なるセキュリティドメイン内のシステムに接続するために、個別のネットワークアドレスを実装する。

詳解：システムをサブネットワーク（すなわち、サブネット）に分解することは、異なるセキュリティ分類または分類レベルの情報を含む異なるセキュリティドメインへのネットワーク接続に適切なレベルの保護を提供できる。

関連管理策：なし

(23) 境界保護 | プロトコル妥当性確認失敗時の送信者へのフィードバックの無効化

プロトコル形式の妥当性確認失敗時の送信者へのフィードバックを無効にする。

詳解：プロトコル妥当性確認フォーマットに失敗した場合に送信者へのフィードバックを無効にすることで、敵対者が他の方法では入手できない情報を取得するのを防ぐことができる。

関連管理策：なし

(24) 境界保護 | 個人情報

個人情報を取扱うシステムの場合：

(a) [*設定：組織が定める取扱い規定*]を個人情報のデータ要素に適用する。

(b) システムへの外部インタフェースおよびシステム内の主要な内部境界で許可された取扱いを監視する。

(c) 各例外取扱いを文書化する。

(d) サポートされなくなった例外をレビューして削除する。

詳解：個人情報の取扱い管理することは、個人のプライバシーを保護するための重要な側面である。例外を処理規定に適用、監視、および文書化することにより、個人情報が、確立されたプライバシー要件に従ってのみ取扱われることが保証される。

関連管理策：PT-2, SI-15

(25) 境境界保護 | 非機密国家安全保障システムの接続

[*設定：組織が定める境界保護デバイス*]を使用せずに、[*設定：組織が定める非機密国家安全保障システム*]を外部ネットワークに直接接続することを禁止する。

詳解：直接接続とは、2 つ以上のシステム間の専用の物理的または仮想的な接続のことである。組織は通常、インターネットなどの外部ネットワークを完全に制御することはできない。境界保護デバイス（ファイアウォール、ゲートウェイ、ルータなど）は、非機密国家安全保障システムと外部ネットワーク間の通信と情報の流れを仲介する。

関連管理策：なし

(26) 境界保護 | 機密国家安全保障システムの接続

[*設定：組織が定める境界保護デバイス*]を使用せずに、機密国家安全保障システムを外部ネットワークに直接接続することを禁止する。

詳解：直接接続とは、2 つ以上のシステム間の専用の物理的または仮想的な接続のことである。組織は通常、インターネットなどの外部ネットワークを完全に制御することはできない。境界保護デバイス（例えば、ファイアウォール、ゲートウェイ、ルータ）は、機密の国家安全保障システムと外部ネットワークとの間の通信と情報の流れを仲介する。さらに、承認済みの境界保護デバイス（通常は管理対象インタフェースまたはクロスドメインシステム）は、システムから外部ネットワークへの情報フロー実施を提供する 。

関連管理策：なし

(27) 境界保護 | 非機密非国家安全保障システムの接続

[*設定：組織が定める境界保護デバイス*]を使用せずに、[*設定：組織が定める非機密非国家安全保障システム*]を外部ネットワークに直接接続することを禁止する。

詳解：直接接続とは、2 つ以上のシステム間の専用の物理的または仮想的な接続のことである。組織は通常、インターネットなどの外部ネットワークを完全に制御することはできない。境界保護デバイス（例えば、ファイアウォール、ゲートウェイ、ルータ）は、非機密非国家安全保障システムと外部ネットワークとの間の通信と情報の流れを仲介する。

関連管理策：なし

(28) 境界保護 | パブリックネットワークへの接続

[*設定：組織が定めるシステム*]からパブリックネットワークへの直接接続を禁止する。

詳解：直接接続とは、2 つ以上のシステム間の専用の物理的または仮想的な接続のことである。パブリックネットワークとは、インターネットやパブリックアクセスが可能な組織のエクストラネットなど、一般にアクセス可能なネットワークである。

関連管理策：なし

(29) 境界保護 | 機能を分離するための別のサブネット

[*設定：組織が定める重要なシステムコンポーネントと機能*]を分離するために、[*選択：物理的；論理的*]に別のサブネットワークを実装する。

詳解：システム障害の原因となる壊滅的または衰弱的なブリーチや侵害の影響を軽減するために、重要なシステムコンポーネントおよび機能を、他の重要でないシステムコンポーネントおよび機能から別のサブネットワークを通じて分離することが必要になる場合がある。例えば、民間航空機では別のサブネットワークを通じて機内エンターテインメント機能からコマンドおよびコントロール機能を物理的に分離することにより、重要なシステム機能の統合的信頼性のレベルが向上する。

関連管理策：なし

参照資料：[OMB A-130], [FIPS 199], [SP 800-37], [SP 800-41], [SP 800-77], [SP 800-189]

SC-8 伝送の機密性および完全性

管理策：伝送される情報の[*選択（1 つ以上）機密性；完全性*]を保護する。

詳解：伝送された情報の機密性および完全性の保護は、内部および外部ネットワーク、ならびにサーバ、ノートブックコンピュータ、デスクトップコンピュータ、モバイルデバイス、プリンタ、コピー機、スキャナ、ファクシミリ機、無線機など、情報を伝送できるあらゆるシステムコンポーネントに適用される。保護されていない通信経路は、傍受や改ざんの可能性にさらされている。情報の機密性と完全性を保護することは、物理的または論理的手段によって達成することができる。物理的な保護は、保護された配信システムを使用することで実現できる。保護された配信システムは、国家機密情報の暗号化されていない伝送に使用できるようにするための端末と適切な電磁的、音響的、電気的および物理的制御を含む有線または光ファイバー通信システムである。論理的保護は、暗号化技法を採用することによって達成できる。

完全に専用のサービスとしてではなく、商品サービスとして伝送サービスを提供する商用プロ

バイダに依存している組織は、伝送の機密性と完全性に必要な管理策の実装に関して必要な保証を得ることが難しい場合がある。そのような状況では、組織は、規格の商用通信サービスパッケージで利用できる機密性または完全性サービスのタイプを決定する。適切な契約手段を通じて必要な管理策と管理策の有効性の保証を得ることが実現可能でない場合、組織は適切な代替管理策を実施することができる。

関連管理策：AC-17, AC-18, AU-10, IA-3, IA-8, IA-9, MA-4, PE-4, SA-4, SA-8, SC-7, SC-16, SC-20, SC-23, SC-28

拡張管理策：

(1) 伝送の機密性および完全性 | 暗号保護

伝送中に[*選択(1 つ以上)：情報の認可されていない開示を防止する；情報の変更を検知する*]暗号化メカニズムを実装する。

詳解：暗号化は、伝送中の認可されていない開示や変更から情報を保護する。伝送中に情報の機密性と完全性を保護する暗号メカニズムには、TLS と IPSec が含まれる。情報の完全性を保護するために使用される暗号メカニズムには、デジタル署名、チェックサム、およびメッセージ認証コードに適用される暗号ハッシュ関数が含まれる。

関連管理策：SC-12, SC-13

(2) 伝送の機密性および完全性 | 送信前および送信後の処理

伝送準備中および受信中の情報の[*選択(1 つ以上)：機密性；完全性*]を維持する。

詳解：情報は、集約中、プロトコル変換ポイントで、圧縮中、および展開中など、伝送の準備中または受信中に、意図せずに、または悪意を持って開示または変更される可能性がある。このような認可されていない開示または変更は、情報の機密性または完全性を侵害する。

関連管理策：なし

(3) 伝送の機密性および完全性 | メッセージの外側の暗号化保護

[*設定：組織が定める代替の物理的管理策*]によって保護されていない限り、メッセージの外部を保護するための暗号メカニズムを実装する。

詳解：メッセージ外部の暗号化保護は、情報の認可されていない開示からの保護に対処する。メッセージの外部には、メッセージヘッダーとルーティング情報が含まれる。暗号化による保護は、外部のメッセージの悪用を防ぎ、権限のないユーザが閲覧できる内部および外部のネットワークやリンクに適用される。ヘッダーとルーティング情報は、組織によって重要な価値があると識別されていないため、または情報を暗号化するとネットワークのパフォーマンスが低下したり、コストが高くなる可能性があるため、平文（暗号化されていない）で伝送されることがある。代替の物理的管理策には、保護された配信システムが含まれる。

関連管理策：SC-12, SC-13

(4) 伝送の機密性および完全性 | 通信の秘匿化またはランダム化

暗号メカニズムを実装して、[*設定：組織が定める代替の物理的管理策*]によって保護されていない限り、通信パターンを秘匿化またはランダム化する。

詳解：通信パターンの秘匿化またはランダム化は、情報の認可されていない開示からの保護に対処する。通信パターンには、頻度、期間、予測可能性、量などがある。通信パターンの変更により、特に組織のミッションと事業の機能に関連する他の入手可能な情報と相まって、情報価値のある情報が明らかになる可能性がある。通信を秘匿化またはランダム化すると、通信パターンに基づく情報の導出が防止され、内部および外部ネットワークまたは認可されたユーザではない個人に見える可能性のあるリンクの両方に適用される。リンクを暗号化し、連続的、固定的、またはランダムなパターンで伝送することにより、システムの通信パターンから情報を引き出すことができなくなる。代替の物理的管理策には、保護された配信システムが含まれる。

関連管理策：SC-12, SC-13

(5) 伝送の機密性および完全性 | 保護された配信システム

伝送中に[*選択(1 つ以上):情報の認可されていない開示を防止する;情報の変更を検知する*]ために[*設定:組織が定める保護された配信システム*]を実装する。

詳解:保護された配信システムの目的は、国家安全保障情報を運ぶ通信回線への物理的アクセスを抑止、検知、および／または困難にすることである。

関連管理策:なし

参照資料:[FIPS 140-3], [FIPS 197], [SP 800-52], [SP 800-77], [SP 800-81-2], [SP 800-113], [SP 800-177], [IR 8023]

SC-9 伝送の機密性

[撤回:SC-8 に組み込まれた]

SC-10 ネットワーク切断

管理策:通信セッションに関連するネットワーク接続を、セッションの終了時または[*設定:組織が定める期間*]の非アクティブ状態の後に終了する。

詳解:ネットワーク切断は、内部ネットワークと外部ネットワークに適用される。特定の通信セッションに関連するネットワーク接続の切断には、オペレーティングシステムレベルでの TCP/IP アドレスまたはポートのペアの割り当て解除、および複数のアプリケーションセッションが単一のオペレーティングシステムレベルのネットワーク接続を使用している場合のアプリケーションレベルでのネットワーク割り当ての解除が含まれる。非アクティブな期間は、組織によって確立される場合があり、ネットワークアクセスのタイプ別または特定のネットワークアクセスの期間が含まれる場合がある。

関連管理策:AC-17, SC-23

拡張管理策:なし

参照資料:なし

SC-11 信頼できる経路

管理策:

a. ユーザとシステムの信頼できるコンポーネントとの間の通信のための[*選択:物理的;論理的*]に隔離された信頼できる通信経路を提供する。

b. 少なくとも、認証と再認証を含む、ユーザとシステムの[*設定:組織が定めるセキュリティ機能*]との間の通信のために、信頼できる通信経路を呼び出すことをユーザに許可する。

詳解:信頼できる経路は、ユーザがセキュリティポリシーをサポートするために必要な保証を備えたシステムのセキュリティ機能と直接(キーボードなどの入力デバイスを使用して)通信できるメカニズムである。信頼できる経路のメカニズムは、ユーザまたは組織のシステムのセキュリティ機能によってのみ活性化できる。信頼できる経路を介して発生するユーザの応答は、信頼できないアプリケーションによる変更や開示から保護されている。組織は、システムのログオン時を含め、システムとユーザのセキュリティ機能間の信頼できる高保証の接続のために、信頼できる経路を採用している。信頼できる経路の初期の実装では、なりすまし可能な文字を伝送しない<BREAK>キーの使用など、帯域外信号を使用して経路を開始する。後の実装では、ハイジャックできないキーの組み合わせが使用された(例えば、<CTRL> +<ALT> +<DEL>キー)。ただし、このようなキーの組み合わせはプラットフォーム固有であり、すべてのケースで信頼できるパス実装を提供するわけではない。信頼できる通信経路の実施は、参照モニタの概念を満たす特定の実装によって提供される。

関連管理策:AC-16, AC-25, SC-12, SC-23

拡張管理策:

(1) 信頼できる経路 | 非常に明確に区別できるコミュニケーション経路

(a) 他の通信経路と非常に明確に区別できる信頼できる通信経路を提供する。

(b) システムの[*設定:組織が定めるセキュリティ機能*]とユーザとの間の通信のための信頼できる通信経路を開設する。

詳解:常に明確に区別できる通信経路は、システムが信頼できる経路を開設することを可能にする、そのため、ユーザが通信の送信元を信頼できるシステムコンポーネントとして間違いなく認識できる。例えば、信頼できる経路は、他のアプリケーションがアクセスできない、またはなりすましができない識別子の存在に基づくディスプレイの領域に表示される場合がある。

関連管理策:なし

参照資料:[OMB A-130]

SC-12 暗号鍵の確立および管理

管理策:システム内で暗号化が採用されている場合は、[*設定:鍵の生成、配布、保管、アクセス、および破棄に関する組織が定める要件*]に従って、暗号鍵を確立および管理する。

詳解:暗号鍵の管理および確立は、手動手順または手動手順をサポートする自動化されたメカニズムを使用して実行できる。組織は、適用される法律、大統領令、指令、基準、ポリシー、規格、およびガイドラインに従って主要な管理要件を規定し、適切なオプション、パラメータ、およびレベルを指定する。組織は、トラストストアを管理して、承認済みのトラストアンカーのみがそのようなトラストストアの一部であることを保証する。これには、組織のシステムの外部に対して可視性のある証明書やシステムの内部運用に関連する証明書が含まれる。[NIST CMVP]と[NIST CAVP]は、暗号鍵の管理と確立に使用できる妥当性確認済みの暗号モジュールとアルゴリズムに関する追加情報を提供する。

関連管理策:AC-17, AU-9, AU-10, CM-3, IA-3, IA-7, SA-4, SA-8, SA-9, SC-8, SC-11, SC-12, SC-13, SC-17, SC-20, SC-37, SC-40, SI-3, SI-7

拡張管理策:

(1) 暗号鍵の確立および管理 | 可用性

ユーザが暗号鍵を紛失した場合でも、情報の可用性を維持する。

詳解:暗号鍵の第三者預託は、鍵を紛失した場合の可用性を確保するための一般的な方法である。パスフレーズの忘れは、暗号鍵紛失の一例である。

関連管理策:なし

(2) 暗号鍵の確立および管理 | 対称鍵

[*選択:NIST FIPS-検証済み;NSA 承認済み*]の鍵管理技術とプロセスを使用して、対称暗号鍵を生成、制御、および配布する。

詳解:[SP 800-56A]、[SP 800-56B]、および[SP 800-56C]は、暗号鍵の確立方式および鍵導出方法に関するガイダンスを提供する。[SP 800-57-1]、[SP 800-57-2]、および[SP 800-57-3]は、暗号鍵管理に関するガイダンスを提供する。

関連管理策:なし

(3) 暗号鍵の確立および管理 | 非対称鍵

[*選択:NSA-承認済みの鍵管理技術とプロセス;事前配置されたキーイングマテリアル;DoD 承認または DoD 発行の中保証(Medium Assurance)PKI 証明書;DoD 承認または DoD 発行のハードウェア中保証(Medium Hardware Assurance)PKI 証明書と、ユーザの秘密鍵を保護するハードウェアセキュリティトークン;組織が定める要件に従って発行される証明書*]を使用して非対称暗号鍵の作成、管理、および配布を行なう。

詳解:[SP 800-56A]、[SP 800-56B]、および[SP 800-56C]は、暗号鍵の確立方式および鍵導

出方法に関するガイダンスを提供する。[SP 800-57-1]、[SP 800-57-2]、および[SP 800-57-3]は、暗号鍵管理に関するガイダンスを提供する。

関連管理策：なし

(4) 暗号鍵の確立および管理 | PKI 証明書

[撤回：SC-12(3)に組み込まれた]

(5) 暗号鍵の確立および管理 | PKI 証明書／ハードウェアトークン

[撤回：SC-12(3)に組み込まれた]

(6) 暗号鍵の確立および管理 | 鍵の物理的管理

格納された情報が外部サービスプロバイダによって暗号化されている場合、暗号鍵の物理的管理を維持する。

詳解：外部サービスプロバイダ（例えば、クラウドサービスまたはデータセンタープロバイダ）を使用する組織にとって、暗号鍵の物理的管理は、そのような外部プロバイダによって格納された情報が認可されていない開示または変更の対象とならないことがさらに保証される。

関連管理策：なし

参照資料：[FIPS 140-3], [SP 800-56A], [SP 800-56B], [SP 800-56C], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-63-3], [IR 7956], [IR 7966]

SC-13 暗号保護

管理策：

a. [*設定：組織が定める暗号の用途*]を決定する。

b. 指定された[*設定：組織が定める指定された各暗号用途に対して暗号のタイプ*]を実装する。

詳解：暗号は、国家機密情報および管理対象非機密情報の保護、デジタル署名の提供と実装、認可された個人が必要なクリアランスを持っているが必要な情報を持たない場合の情報分離の実施など、様々なセキュリティソリューションをサポートするために使用できる。正式なアクセス承認。暗号化は、乱数とハッシュ生成をサポートするために使用することもできる。一般的に適用される暗号規格には、FIPS 検証済み暗号技術および NSA 承認済み暗号技術が含まれる。例えば、国家機密情報を保護する必要がある組織は、NSA 承認済み暗号技術の使用を指定することができる。デジタル署名をプロビジョニングおよび実装する必要がある組織は、FIPS 検証済み暗号技術の使用を指定することができる。暗号技術は、適用される法律、大統領令、指令、規制、ポリシー、基準、およびガイドラインに従って実装される。

関連管理策：AC-2, AC-3, AC-7, AC-17, AC-18, AC-19, AU-9, AU-10, CM-11, CP-9, IA-3, IA-5, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SA-8, SA-9, SC-8, SC-12, SC-20, SC-23, SC-28, SC-40, SI-3, SI-7

拡張管理策：なし

(1) 暗号保護 | FIPS 検証済み暗号技術

[撤回：SC-13 に組み込まれた]

(2) 暗号保護 | NSA 承認済み暗号技術

[撤回：SC-13 に組み込まれた]

(3) 暗号保護 | 正式なアクセス承認を受けていない個人

[撤回：SC-13 に組み込まれた]

(4) 暗号保護 | デジタル署名

[撤回：SC-13 に組み込まれた]

参照資料：[FIPS 140-3]

SC-14 パブリックアクセス保護

[撤回：AC-2、AC-3、AC-5、AC-6、SI-3、SI-4、SI-5、SI-7 および SI-10 に組み込まれた]

SC-15 共同コンピューティングデバイスおよびアプリケーション

管理策：

a. [*設定：組織が定めるリモートアクティベーションが許可される例外*]を除き、コラボレーティブコンピューティングデバイスおよびアプリケーションのリモートアクティベーションを禁止する。

b. デバイスに物理的に存在するユーザに使用の明示的な指示を提供する。

詳解：共同コンピューティングデバイスおよびアプリケーションには、リモート会議デバイスおよびアプリケーション、ネットワーク化されたホワイトボード、カメラ、マイクなどがある。使用の明示的な表示には、共同コンピューティングデバイスおよびアプリケーションが活性化されたときのユーザへの信号が含まれる。

関連管理策：AC-21, SC-42

拡張管理策：

(1) 共同コンピューティングデバイス | 物理的または論理的な切断

使いやすさをサポートする方法で、共同コンピューティングデバイスの[*選択（1 つ以上）：物理的；論理的*]な切断を提供する。

詳解：共同コンピューティンデバイスからの切断に失敗すると、組織の情報が侵害される可能性がある。共同コンピューティングセッション後にこのようなデバイスから切断する簡単な方法を提供することで、参加者は複雑で面倒な手順を踏む必要なく切断作業を実行できる。共同コンピューティングデバイスからの切断は、手動または自動で行うことができる。

関連管理策：なし

(2) 共同コンピューティングデバイス | インバウンドおよびアウトバウンド通信トラフィックの遮断

[撤回：SC-7 に組み込まれた]

(3) 共同コンピューティングデバイス | セキュアな作業領域での無効化および削除

[*設定：組織が定めるシステムまたはシステムコンポーネント*]から[*設定：組織が定めるセキュアな作業領域*]の、共同コンピューティングデバイスおよびアプリケーションを無効化または削除する。

詳解：共同コンピューティングッデバイスおよびアプリケーションをシステムまたはシステムコンポーネントから無効化または削除しないと、会話の傍受など、情報が侵害される可能性がある。機微区分情報隔離施設（SCIF）は、セキュアな作業領域の例である。

関連管理策：なし

(4) 共同コンピューティングデバイス | 現在の参加者の明示

[*設定：組織が定めるオンライン会議および電話会議*]で、現在の参加者を明示的に示す。

詳解：現在の参加者を明示的に示すことで、認可されていない個人が他の参加者の明確な認証なしに共同コンピューティングセッションに参加することを防ぐ。

関連管理策：なし

参照資料：なし

SC-16 セキュリティおよびプライバシーの属性の伝送

管理策：システム間およびシステムコンポーネント間で交換される情報に[*設定：組織が定めるセキュリティとプライバシーの属性*]を関連付ける。

詳解：セキュリティとプライバシーの属性は、組織のシステムまたはシステムコンポーネントに含まれる情報に明示的または暗黙的に関連付けることができる。属性は、情報の保護または個人情報の管理に関するエンティティの基本的な特性または特徴を表す抽象概念である。属性は通常、システム内のレコード、バッファ、ファイルなどの内部データ構造に関連付けられている。セキュリティおよびプライバシー属性は、アクセス制御および情報フロー制御ポリシーを実装するために使用される。個人情報の許可された使用を含む、特別な配布、管理、または配布の指示を反映する。または、情報セキュリティおよびプライバシーポリシーの他の側面をサポートする。プライバシー属性は、独立して、またはセキュリティ属性と組み合わせて使用することができる。

関連管理策：AC-3, AC-4, AC-16

拡張管理策：

(1) セキュリティおよびプライバシーの属性の伝達 | 完全性の検証

伝送されたセキュリティとプライバシーの属性の完全性を検証する。

詳解：伝送された情報の完全性を検証することの一部は、そのような情報に関連するセキュリティとプライバシーの属性が認可されていない変更をされていないことを保証することである。セキュリティまたはプライバシー属性を認可されていない変更がされると、伝送された情報の完全性が失われる可能性がある。

関連管理策：AU-10, SC-8

(2) セキュリティおよびプライバシーの属性の伝達 | なりすまし防止メカニズム

敵対者が、セキュリティプロセスの適用が成功したことを示す、セキュリティ属性の改ざんを防ぐために、なりすまし防止メカニズムを実装する。

詳解：一部の攻撃ベクトルは、情報システムのセキュリティ属性を変更して、システム内に不十分なレベルのセキュリティを意図的かつ悪意を持って実装することによって機能する。属性の変更により、組織は、実際に実装されているよりも多くのセキュリティ機能が導入され、運用されていると考えがちである。

関連管理策：SI-3, SI-4, SI-7

(3) セキュリティおよびプライバシーの属性の伝達 | 暗号化バインディング

[*設定：組織が定めるメカニズムまたは技法*]を実装して、セキュリティおよびプライバシー属性を伝送される情報にバインディングする。

詳解：暗号メカニズムと技法は、伝送される情報に強力なセキュリティとプライバシーの属性のバインディングを提供し、そのような情報の完全性を保証するのに役立つ。

関連管理策：AC-16, SC-12, SC-13

参照資料：[OMB A-130]

SC-17 公開鍵基盤の証明書

管理策：

a. [*設定：組織が定める証明書ポリシー*]の下で公開鍵証明書を発行するか、承認済みのサービスプロバイダから公開鍵証明書を取得する。

b. 組織が管理するトラストストアまたは証明書ストアには、承認済みのトラストアンカーのみを含める。

詳解：公開鍵基盤（PKI：Public key infrastructure）証明書は、組織のシステムの外部に可視性を持つ証明書と、アプリケーション固有のタイムサービスなど、システムの内部運用に関連する証明書である。階層構造の暗号化システムでは、トラストアンカーは、信頼が想定され、導出されない信頼できるソース（つまり、認証局）である。PKI システムのルート証明書は、トラストアンカ

一の一例である。トラストストアまたは証明書ストアは、信頼できるルート証明書のリストを保持する。

関連管理策：AU-10, IA-5, SC-12

拡張管理策：なし

参照資料：[SP 800-32], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-63-3]

SC-18 モバイルコード

管理策：

a. 許容できるモバイルコードと許容できないモバイルコードとモバイルコード技術を規定する。

b. システム内でのモバイルコードの使用を承認、監視、管理する。

詳解：モバイルコードには、ネットワークを介して伝送でき（例えば、電子メール、ドキュメント、またはウェブサイトに組み込まれている）、リモートシステムで実行できるプログラム、アプリケーション、またはコンテンツが含まれる。組織のシステム内でのモバイルコードの使用に関する決定は、コードが悪意を持って使用された場合にシステムに損傷を与える可能性に基づいている。モバイルコードテクノロジには、Java アプレット、JavaScript、HTML5、WebGL、VBScript などがある。使用制限と実装ガイドラインは、サーバにインストールされたモバイルコードの選択と使用、および個々のワークステーションとデバイス（ノートブックコンピュータやスマートフォンを含む）にダウンロードされ実行されたモバイルコードの両方に適用される。モバイルコードのポリシーと手順は、信頼できるソースによるモバイルコードへのデジタル署名を要求することを含め、組織のシステム内での容認できないモバイルコードの開発、取得、導入を防止するために講じられる特定の措置に対応する。

関連管理策：AU-2, AU-12, CM-2, CM-6, SI-3

拡張管理策：

(1) モバイルコード | 許可されないコードの特定および是正措置

[*設定：組織が定める許可されないモバイルコード*]を特定し、[*設定：組織が定める是正措置*]を講じる。

詳解：許可されないモバイルコードが検知された場合の是正措置には、ブロック、隔離、または管理者へのアラートが含まれる。ブロックには、組み込みマクロが許容できないモバイルコードであると判断された場合に、組み込みマクロを含むプロファイルの伝送を防止することが含まれる。

関連管理策：なし

(2) モバイルコード | 取得、開発、および使用

システムに導入されるモバイルコードの取得、開発、使用が、[*設定：組織が定めるモバイルコード要件*]を満たしていることを確認する。

詳解：なし

関連管理策：なし

(3) モバイルコード | ダウンロードおよび実行の防止

[*設定：組織が定める許可されないモバイルコード*]のダウンロードおよび実行を防止する。

詳解：なし

関連管理策：なし

(4) モバイルコード | 自動実行の防止

[*設定：組織が定めるソフトウェアアプリケーション*]でコードを実行する前に、モバイル

コードの自動実行を防止し、[*設定：組織が定めるアクション*]を強制する。

詳解：モバイルコードを実行する前に適用されるアクションには、電子メールの添付ファイルを開く前、またはウェブリンクをクリックする前にユーザにプロンプトを表示することが含まれる。モバイルコードの自動実行の防止には、コンパクトディスク、デジタル多用途ディスク、ユニバーサルシリアルバスデバイスなどのポータブルストレージデバイスを使用するシステムコンポーネントの自動実行機能を無効にすることが含まれる。

関連管理策：なし

(5) モバイルコード｜制限された環境に限った実行の許可

制限された仮想マシン環境でのみ、許可されたモバイルコードの実行を許可する。

詳解：限定された仮想マシン環境でのみモバイルコードの実行を許可することで、悪意のあるコードが他のシステムやシステムコンポーネントに持ち込まれるのを防ぐことができる。

関連管理策：SC-44, SI-7

参照資料：[SP 800-28]

SC-19 ボイス・オーバー・インターネット・プロトコル（VOIP）

［撤回：技術固有。他の技術またはプロトコルと同様に対処される］

SC-20 セキュアな名前／アドレス解決サービス（信頼できるソース）

管理策：

a. 外部の名前／アドレス解決クエリに対応してシステムが返す信頼できる名前解決データとともに、追加のデータ発信元認証および完全性検証アーティファクトを提供する。

b. 子ゾーンのセキュリティ状態を示す手段を提供し、（子ゾーンがセキュアな解決サービスをサポートしている場合）分散型階層名前空間の一部として動作するときに、親ドメインと子ドメイン間の信頼の連鎖を検証できるようにする。

詳解：信頼できるソース情報を提供することで、リモートインターネットクライアントを含む外部クライアントが、サービスを通じて取得したホスト名とサービス名からネットワークアドレスへの解決情報について、発信元認証と完全性検証の保証を得ることができる。名前およびアドレス解決サービスを提供するシステムには、ドメインネームシステム（DNS：domain name system）サーバが含まれる。追加の成果物には、DNSSEC（DNS Security Extensions）デジタル署名および暗号鍵が含まれる。信頼できるデータには、DNS リソースレコードが含まれる。子ゾーンのセキュリティステータスを示す手段には、DNS での委任署名者リソースレコードの使用が含まれる。DNS 以外の技術を使用してホスト名とサービス名およびネットワークアドレスをマッピングするシステムは、対応データの真正性と完全性を保証するための他の手段を提供する。

関連管理策：AU-10, SC-8, SC-12, SC-13, SC-21, SC-22

拡張管理策：

(1) セキュアな名前／アドレス解決サービス（信頼できるソース）｜子サブスペース

［撤回：SC-20 に組み込まれた］

(2) セキュアな名前／アドレス解決サービス（信頼できるソース）｜データの起源および完全性

内部の名前／アドレス解決クエリに、データの起源と完全性保護の成果物を提供する。

詳解：なし

関連管理策：なし

参照資料：[FIPS 140-3], [FIPS 186-4], [SP 800-81-2]

SC-21 セキュアな名前／アドレス解決サービス（再帰的またはリゾルバキャッシング）

管理策：システムが信頼できるソースから受け取る名前／アドレス解決対応に対して、データ発信元認証およびデータ完全性検証を要求し、実行する。

詳解：名前解決サービスの各クライアントは、この妥当性確認を独自に実行するか、信頼できる妥当性確認プロバイダへの認証済みチャネルを持っている。ローカルクライアントに名前とアドレスの解決サービスを提供するシステムには、ドメインネームシステム（DNS）サーバの再帰的な解決またはキャッシュが含まれる。DNS クライアントリゾルバは、DNSSEC 署名の妥当性確認を実行するか、クライアントが認証済みチャネルを使用して、そのような妥当性確認を実行する再帰リゾルバを実行する。DNS 以外の技術を使用してホスト名とサービス名およびネットワークアドレスをマッピングするシステムは、クライアントが対応データの真正性と完全性を検証できるようにするための手段を提供する。

関連管理策：SC-20, SC-22

拡張管理策：なし

(1) セキュアな名前／アドレス解決サービス（再帰的またはリゾルバキャッシング）｜データの起源および完全性

［撤回：SC-21 に組み込まれた］

参照資料：[SP 800-81-2]

SC-22 名前／アドレス解決サービスのアーキテクチャとプロビジョニング

管理策：組織に名前／アドレス解決サービスをまとめて提供するシステムが耐障害性であり、内部と外部の役割の分離を実装していることを確認する。

詳解：名前およびアドレス解決サービスを提供するシステムには、ドメインネームシステム（DNS：domain name system）サーバが含まれる。システムの単一障害点を排除し、冗長性を高めるために、組織は少なくとも 2 つの権限のあるドメインネームシステムサーバを使用する。1 つはプライマリサーバとして構成され、もう 1 つはセカンダリサーバとして構成される。さらに、組織は通常、地理的に離れた 2 つのネットワークサブネットワークにサーバを展開する（つまり、同じ物理施設に配置されていない）。役割を分離するために、内部の役割を持つ DNS サーバは、組織内からの（つまり、内部クライアントからの）名前とアドレスの解決要求のみを処理する。外部の役割を持つ DNS サーバは、組織の外部のクライアント（つまり、インターネットを含む外部ネットワーク上）からの名前およびアドレス解決情報要求のみを処理する。組織は、特定の役割の権限のある DNS サーバにアクセスできるクライアントを指定する（例えば、アドレス範囲や明示的なリストなど）。

関連管理策：SC-2, SC-20, SC-21, SC-24

拡張管理策：なし

参照資料：[SP 800-81-2]

SC-23 セッションの真正性

管理策：通信セッションの真正性を保護する。

詳解：セッションの真正性の保護は、パケットレベルではなく、セッションレベルでの通信保護に対応する。そのような保護は、通信セッションの両端で、他の当事者の現在進行中の身元および伝送された情報の有効性に対する信頼の根拠を確立する。真正性の保護には、「中間者」攻撃、セッション乗っ取り、およびセッションへの誤った情報の挿入に対する保護が含まれる。

関連管理策：AU-10, SC-8, SC-10, SC-11

拡張管理策：

(1) セッションの真正性｜ログアウト時のセッション識別子の無効化

ユーザのログアウト時またはその他のセッション終了時にセッション識別子を無効化する。

詳解：ログアウト時にセッション識別子を無効化すると、敵対者が以前に有効だったセッション ID をキャプチャして引き続き使用する能力が低下する。

関連管理策：なし

(2) セッション真正性 | ユーザが開始したログアウトおよびメッセージの表示

［撤回：AC-12(1)に組み込まれた］

(3) セッションの真正性 | 一意のシステム生成セッション識別子

［*設定：組織が定めるランダム性要件*］を使用して、各セッションに一意のセッション識別子を生成し、システム生成のセッション識別子のみを認識する。

詳解：一意のセッション識別子を生成すると、以前の有効なセッション識別子を再利用する敵対者の能力が削減される。一意のセッション識別子の生成にランダム性の概念を採用することで、ブルートフォース攻撃から保護し、将来のセッション識別子を特定する。

関連管理策：AC-10, SC-12, SC-13

(4) セッションの真正性 | ランダム化された一意のセッション識別子

［撤回：SC-23(3)に組み込まれた］

(5) セッションの真正性 | 許可された認証局

保護されたセッションの確立の検証には［*設定：組織が定める認証局*］の使用のみ許可をする。

詳解：セキュアなセッションの確立のための認証局への依存には、トランスポート層セキュリティ（TLS）証明書の使用が含まれる。これらの証明書は、それぞれの認証局による検証後、ウェブクライアントとウェブサーバ間の保護されたセッションの確立を容易にする。

関連管理策：SC-12, SC-13

参照資料：[SP 800-52], [SP 800-77], [SP 800-95], [SP 800-113]

SC-24 既知の安全な状態での障害

管理策：［*設定：組織が定めるシステムコンポーネントにおける組織が定めるタイプのシステム障害のリスト*］にある障害が発生した場合、［*設定：組織が定めるシステム状態情報*］を保持しながら、［*設定：組織が定める、既知のシステム状態*］に導く。

詳解：既知の状態での障害は、組織のミッションと事業ニーズに従ってセキュリティ上の懸念に対処する。既知の状態で障害が発生すると、組織のシステムまたはシステムコンポーネントに障害が発生した場合に、情報の機密性、完全性、または可用性が失われることが防止される。既知のセキュアな状態での障害は、システムが個人の負傷または資産の破壊を引き起こす可能性のある状態の障害を防ぐのに役立つ。システム状態情報を保持することで、システムの再起動と運用モードへの復帰が容易になり、ミッションと事業プロセスの中断が少なくなる。

関連管理策：CP-2, CP-4, CP-10, CP-12, SA-8, SC-7, SC-22, SI-13

拡張管理策：なし

参照資料：なし

SC-25 シンノード

管理策：［*設定：組織が定めるシステムコンポーネント*］に最小限の機能と情報ストレージを採用する。

詳解：最小限の機能を備えたシステムコンポーネントを配備することで、すべてのエンドポイントをセキュアにする必要性が減り、情報、システム、およびサービスが攻撃にさらされる可能性を減らすことができる。機能が制限されている、または最小限の機能には、ディスクレスノードとシ

ンクライアント技術が含まれる。

関連管理策：SC-30, SC-44

拡張管理策：なし

参照資料：なし

SC-26 デコイ

管理策：悪意のある攻撃の標的となるように特別に設計されたコンポーネントを組織のシステムに含め、そのような攻撃を検知、防御、分析する。

詳解：デコイ（すなわち、ハニーポット、ハニーネット、または詐欺ネット）は、敵対者を引き付け、組織のミッションと事業の機能をサポートする運用システムから攻撃をそらすために設置される。デコイの使用には、偏向した悪意のあるコードが組織のシステムに感染しないことを確実にするために、いくつかのサポートする分離手段が必要である。おとりの具体的な使用方法によっては、展開前に法務部に相談する必要があるかもしれない。

関連管理策：RA-5, SC-7, SC-30, SC-35, SC-44, SI-3, SI-4

拡張管理策：なし

(1) デコイ | 悪意のあるコードの検知

［撤回：SC-35 に組み込まれた］

参照資料：なし

SC-27 プラットフォームに依存しないアプリケーション

管理策：組織のシステム内に、［*設定：組織が定めるプラットフォームに依存しないアプリケーション*］を含める。

詳解：プラットフォームとは、ソフトウェアアプリケーションの実行に使用されるハードウェア、ファームウェア、およびソフトウェアコンポーネントの組み合わせである。プラットフォームには、オペレーティングシステム、基盤となるコンピュータアーキテクチャ、またはその両方が含まれる。プラットフォームに依存しないアプリケーションとは、複数のプラットフォームで実行する機能を備えたアプリケーションのことである。このようなアプリケーションは、異なるプラットフォームでの移植性と再構成を促進する。アプリケーションの移植性と、異なるプラットフォームで再構成できることにより、特定のオペレーティングシステムを搭載したシステムが攻撃を受けている状況で、組織内のミッションに不可欠な機能の可用性が向上する。

関連管理策：SC-29

拡張管理策：なし

参照資料：なし

SC-28 保管中の情報の保護

管理策：［*設定：組織が定める保管中の情報*］の［*選択（1 つ以上）：機密性；完全性*］を保護する。

詳解：保管中の情報とは、情報が処理中または転送中ではなく、システムコンポーネント上にあるときの情報の状態を指す。このようなコンポーネントには、内蔵または外付けハードディスクドライブ、ストレージエリアネットワークデバイス、またはデータベースが含まれる。ただし、保管されている情報を保護する目的は、記憶デバイスのタイプやアクセス頻度ではなく、情報の状態にある。保管情報は、情報の機密性と完全性を扱い、ユーザ情報とシステム情報を対象としている。保護を必要とするシステム関連情報には、ファイアウォール、侵入検知および防止システム、フィルタリングルータ、認証情報の構成または規則が含まれる。組織は、暗号化メカニズムやファイル共有スキャンの使用など、機密性と完全性の保護を実現するために様々なメカニズ

ムを採用している場合がある。完全性保護は、例えば、追記型（WORM）技術を実装することによって達成することができる。保管中の情報を適切に保護することができない場合、組織は、頻繁にスキャンして保管中の悪意のあるコードを特定し、オンラインストレージの代わりにオフラインストレージをセキュアにするなど、他の管理策を採用する場合がある。

関連管理策：AC-3, AC-4, AC-6, AC-19, CA-7, CM-3, CM-5, CM-6, CP-9, MP-4, MP-5, PE-3, SC-8, SC-12, SC-13, SC-34, SI-3, SI-7, SI-16

拡張管理策：

(1) 保管中の情報の保護 | 暗号保護

[*設定：組織が定めるシステムコンポーネントまたは媒体*]に保存されている[*設定：組織が定める情報*]の認可されていない開示および変更を防止するために、暗号メカニズムを実装する。

詳解：暗号メカニズムの選択は、組織情報の機密性と完全性を保護する必要性に基づいている。メカニズムの強度は、情報のセキュリティの分類または情報の機密性区分に対応している。組織は、システムコンポーネントや媒体に関する情報を暗号化したり、ファイル、レコード、フィールドなどのデータ構造を暗号化したりできる柔軟性を備えている。

関連管理策：AC-19, SC-12, SC-13

(2) 保管中の情報の保護 | オフラインストレージ

オンラインストレージから[*設定：組織が定める情報*]を削除し、オフラインでセキュアな場所に保管する。

詳解：オンラインストレージからオフラインストレージに組織情報を移動すると、個人がネットワークを介して情報に認可されていないアクセスをする可能性がなくなる。したがって、組織は、オンラインストレージの情報を保護する代わりに、オフラインストレージに情報を移動することを選択する場合がある。

関連管理策：なし

(3) 保管中の情報の保護 | 暗号鍵

暗号鍵のための保護されたストレージ[*選択：[設定：組織が定める保全措置]；ハードウェアで保護されたキーストア*]を提供する。

詳解：トラステッドプラットフォームモジュール（TPM：Trusted Platform Module）は、暗号鍵を保護するために使用できるハードウェアで保護されたデータストアの例である。

関連管理策：SC-12, SC-13

参照資料：[OMB A-130], [SP 800-56A], [SP 800-56B], [SP 800-56C], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-111], [SP 800-124]

SC-29 異質性

管理策：システムの実装において、[*設定：組織が定めるシステムコンポーネント*]に多様な一連の情報技術を採用する。

詳解：組織のシステム内の情報技術の多様性を高めることにより、特定の技術の潜在的な悪用または侵害のインパクトを軽減する。このような多様性は、サプライチェーン攻撃によって引き起こされる障害を含む、コモンモード障害からシステムを保護する。情報技術の多様性は、敵対者が 1 つのシステムコンポーネントの侵害のために使用する手段が他のシステムコンポーネントに対して有効である可能性も低減し、計画的な攻撃を成功させるための敵対者の作業要因をさらに増加させる。多様性が高まると、複雑さと管理オーバーヘッドが追加され、最終的にミスや認可されていない構成につながる可能性がある。

関連管理策：AU-9, PL-8, SC-27, SC-30, SR-3

拡張管理策：

(1) 異質性 | 仮想化技法

[*設定：組織が定める頻度*]で変更される、多様なオペレーティングシステムとアプリケーションの導入を支援するために仮想化技法を採用する。

詳解：オペレーティングシステムとアプリケーションに頻繁な変更を加えると、構成管理に大きな課題が生じる可能性があるが、その変更により、敵対者が攻撃を成功させるための作業要因が増加する可能性がある。実際のオペレーティングシステムまたはアプリケーションを変更するのではなく、仮想オペレーティングシステムまたはアプリケーションを変更すると、構成管理の労力を軽減しながら、攻撃者の成功を妨げる仮想的な変更が提供される。仮想化技法は、信頼できないソフトウェアまたは来歴が疑わしいソフトウェアを、限定された実行環境に分離するのに役立つ。

関連管理策：なし

参照資料：なし

SC-30 秘匿化および誤認誘導

管理策：[*設定：組織が定める期間*]で、[*設定：組織が定めるシステム*]に対して、[*設定：組織が定める秘匿化および誤認誘導技法*]を採用して、敵対者を混乱させ、誤解させる。

詳解：秘匿化および誤認誘導の技法は、攻撃を開始および完了させるための敵対者の標的化ケイパビリティ（すなわち、絶好の機会および利用可能な攻撃対象領域）を大幅に減らす可能性がある。例えば、仮想化技法は、組織にシステムを偽装する機能を提供し、複数のプラットフォームを持つことなく、攻撃が成功する可能性を減らすことができる。ランダム性、不確実性、および仮想化を含む、秘匿化および誤認誘導技法および方法の使用の増加は、敵対者を十分に混乱させ、誤解させ、結果として、窃取技術を検出および／または公開のリスクを増大させる。秘匿化技術と誤認誘導技法は、コアミッションと事業の機能を実行するための追加の時間を提供する可能性がある。秘匿化技術および誤認誘導技法の実装は、システムに必要な複雑さおよび管理オーバーヘッドを追加する可能性がある。

関連管理策：AC-6, SC-25, SC-26, SC-29, SC-44, SI-14

拡張管理策：

(1) 秘匿化および誤認誘導 | 仮想化技法

［撤回：SC-29(1)に組み込まれた］

(2) 秘匿化および誤認誘導 | ランダム性

組織の運営と資産にランダム性を導入するために[*設定：組織が定める技法*]を採用する。

詳解：ランダム性は、攻撃からシステムを防御するために組織が取る行動に関して、敵対者の不確実性のレベルを増大させる。そのような行動は、敵対者の重要なミッションまたは事業の機能をサポートする組織の情報資源を正確に標的とする能力を妨げる可能性がある。不確実性はまた、攻撃を開始または継続する前に敵対者をためらわせる可能性がある。ランダム性を伴う誤認誘導技法には、特定の日常的な行動を異なる時間に実行すること、異なる情報技術を採用すること、異なるサプライヤを使用すること、組織の職員の役割と責任をローテーションすることが含まれる。

関連管理策：なし

(3) 秘匿化および誤認誘導 | 処理場所および保管場所の変更

[*選択：[設定：組織が定める時間頻度]；ランダムな時間間隔*]で[*設定：組織が定める処理または保管、あるいはその両方*]の場所を変更する。

詳解：敵対者は、重要なミッションと事業の機能、ならびにそれらの機能をサポートするシステムを標的とし、その存在と窃取技術の露出を最小限に抑えようと試みる。敵対者が標的とする組織システムの静的、同種、および決定論的な性質により、そのようなシステムは、攻撃を受ける可能性が低くなり、敵対者のコストと労力が軽減されて成功する。処理および保管場所の変更（移動標的防御とも呼ばれる）は、仮想化、分散処理、複製などの技術を使用して、持続的標的型攻撃に対処する。これにより、組織は重要なミッションおよ

び事業の機能をサポートするシステムコンポーネント（すなわち、処理、ストレージ）を再配置することができる。処理活動や保管場所の場所を変更すると、敵対者の標的化行為にある程度の不確実性が生じる。標的の不確実性は、敵対者の作業要因を増加させ、組織のシステムの侵害やブリーチをより困難で時間のかかるものにする。また、重要な組織リソースを見つけようとする際に、敵対者が窃取技術の特定の側面を誤って開示する可能性も高まる。

関連管理策：なし

(4) 秘匿化および誤認誘導 | 誤解を招く情報

[*設定：組織が定めるシステムコンポーネント*]に、セキュリティ状態または方針に関する現実的ではあるが誤解を招く情報を採用する。

詳解：誤解を招く情報を採用することは、組織が展開する管理策の性質と範囲に関して潜在的な敵対者を混乱させることを意図する。したがって、敵対者は不正確で効果のない攻撃技法を採用する可能性がある。敵対者を誤解させる 1 つの技法は、組織が、敵対者の標的となることがわかっている外部システムに展開された特定の管理策に関する誤解を招くような情報を配置することである。別の技法は、組織のシステムの実際の側面を模倣するが、例えば、古いソフトウェア構成を使用する詐欺ネットの使用である。

関連管理策：なし

(5) 秘匿化および誤認誘導 | システムコンポーネントの秘匿化

[*設定：組織が定めるシステムコンポーネント*]を隠蔽または秘匿するために、[*設定：組織が定める技法*]を採用する。

詳解：重要なシステムコンポーネントを隠蔽、偽装、または秘匿することにより、組織は、敵対者がこれらの資産を標的とし、セキュリティ侵害を成功させる可能性を低減できる可能性がある。システムコンポーネントを隠蔽、偽装、または秘匿する潜在的な手段には、ルータの構成、または暗号化または仮想化技法の使用が含まれる。

関連管理策：なし

参照資料：なし

SC-31 カバートチャネル分析

管理策：

a. カバートチャネル分析を実行して、システム内の通信のカバートチャネル[*選択（1 つ以上）：ストレージ；タイミング*]の潜在的手段であるこれらの側面を特定する。

b. それらのチャネルの最大帯域幅を推定する。

詳解：開発者は、カバートチャネルにつながる可能性のあるシステム内の潜在的な領域を特定するのに最適な立場にある。カバートチャネル分析は、輸出管理された情報を含み、外部ネットワーク（すなわち、組織によって管理されていないネットワーク）に接続しているシステムの場合のように、セキュリティドメインを越えて認可されていない情報フローの可能性がある場合に意味のある活動である。カバートチャネル分析は、マルチレベルのセキュアなシステム、複数のセキュリティレベルのシステム、およびクロスドメインシステムにも役立つ。

関連管理策：AC-3, AC-4, SA-8, SI-11

拡張管理策：

(1) カバートチャネル分析 | 探知可能性のためのカバートチャネルのテスト

特定されたカバートチャネルの一部のサブセットをテストして、悪用可能なチャネルを特定する。

詳解：なし

関連管理策：なし

(2) カバートチャネル分析 | 最大帯域幅

特定されたカバートチャネル[*選択(1 つ以上):ストレージ;タイミング*]の最大帯域幅を[*設定:組織が定める値*]に削減する。

詳解:カバートチャネル、特にカバートタイミングチャネルを完全に排除することは、通常、パフォーマンスに大きなインパクトを与えなければ不可能である。

関連管理策:なし

(3) カバートチャネル分析 | 運用環境での帯域幅の測定

システムの運用環境で、[*設定:組織が定めるサブセットの識別されたカバートチャネル*]の帯域幅を測定する。

詳解:特定の運用環境でカバートチャネルの帯域幅を測定することで、組織が、ミッションや事業の機能に悪影響を与える前に、どの程度の情報が密かに漏えいする可能性があるかを判断することができる。研究室やシステム開発環境など、特定の運用環境に依存しない設定で測定した場合、カバートチャネル帯域幅は大幅に異なる場合がある。

関連管理策:なし

参照資料:なし

SC-32 システム分割

管理策:[*設定:組織が定めるコンポーネントの物理的または論理的分離に関する状況*]に基づきシステムを、別のドメイン:[*選択:物理的;論理的*]または環境:[*設定:組織が定めるシステムコンポーネント*]に分割する。

詳解:システム分割は、多層防御の保護戦略の一部である。組織は、システムコンポーネントの物理的な分離の程度を決定する。物理的な分離オプションには、同じ部屋の別々のラックにある物理的に異なるコンポーネント、別々の部屋の重要なコンポーネント、重要なコンポーネントの地理的な分離などがある。セキュリティ分類化は、ドメイン分割の候補の選択を導くことができる。管理されたインタフェースは、パーティション化されたシステムコンポーネント間のネットワークアクセスおよび情報フローを制限または禁止する。

関連管理策:AC-4, AC-6, SA-8, SC-2, SC-3, SC-7, SC-36

拡張管理策:

(1) システム分割 | 特権機能のための物理ドメインの分離

特権機能を個別の物理ドメインに分割する。

詳解:単一の物理ドメインで動作する特権機能は、そのドメインが侵害にさらされたりサービス拒否が発生したりした場合、単一障害点となる可能性がある。

関連管理策:なし

参照資料:[FIPS 199], [IR 8179]

SC-33 伝送準備の完全性

[撤回:SC-8 に組み込まれた]

SC-34 変更不可能な実行可能プログラム

管理策:[*設定:組織が定めるシステムコンポーネント*]の場合、以下をロードして実行する。

a. ハードウェアによる読み取り専用媒体からの動作環境。

b. ハードウェアによる読み取り専用媒体からの[*設定:組織が定めるアプリケーション*]をロードして実行する。

詳解:システムのオペレーティング環境には、オペレーティングシステム、エグゼクティブ、仮想マシンモニタ(ハイパーバイザなど)を含むアプリケーションをホストするコードが含まれている。また、ハードウェアプラットフォームで直接実行される特定のアプリケーションを含めることもで

きる。ハードウェアによる読み取り専用媒体には、CD-R（Compact Disc-Recordable）および DVD-R（Digital Versatile Disc-Recordable）ディスクドライブや、プログラム可能な読み取り専用のワンタイムメモリなどがある。変更不可能なストレージを使用することで、読み取り専用イメージの作成時点からソフトウェアの完全性が保証される。初期書き込みの時点からシステムへのメモリの挿入まで完全性が十分に保護でき、かつ組織のシステムにインストールされている間、メモリの再プログラミングに対して信頼性の高いハードウェア保護がある場合は、再プログラム可能な読み取り専用メモリの使用を読み取り専用媒体として受け入れることができる。

関連管理策：AC-3, SI-7, SI-14

拡張管理策：

(1) 変更不可能な実行可能プログラム｜書き込み可能なストレージ

[*設定：組織が定めるシステムコンポーネント*]において再起動または電源のオン／オフ後も永続的な書き込み可能なストレージを持たないものを採用する。

詳解：書き込み可能なストレージを禁止することで、指定されたシステムコンポーネント内の永続的な書き込みが可能なストレージを介して悪意のあるコードが挿入される可能性を排除できる。この制限は固定ストレージとリムーバブルストレージに適用され、後者は直接、またはモバイルデバイスのアクセス管理策を通じて課される特定の制限として対処される。

関連管理策：AC-19, MP-7

(2) 変更不可能な実行可能プログラム｜読み取り専用媒体の完全性保護

読み取り専用媒体に保存する前に情報の完全性を保護し、そのような情報が媒体に記録された後に媒体を管理する。

詳解：管理策は、システムへの媒体の置き換えや、システムへのインストール前のプログラム可能な読み取り専用媒体の再プログラミングを防止する。完全性保護の管理策には、予防、検知、対応の組み合わせが含まれる。

関連管理策：CM-3, CM-5, CM-9, MP-2, MP-4, MP-5, SC-28, SI-3

(3) 変更不可能な実行可能プログラム｜ハードウェアベースの保護

［撤回：SC-51 に移動した］

SC-35 外部の悪意のあるコードの識別

管理策：ネットワークベースの悪意のあるコードまたは悪意のあるウェブサイトを積極的に特定するシステムコンポーネントを含める。

詳解：外部の悪意のあるコードの識別は、コンポーネントが外部のウェブサイトに含まれる悪意のあるコードを探すためにインターネットなどのネットワークを積極的に調査するという点で、SC-26 のデコイとは異なる。デコイと同様に、外部の悪意のあるコードの識別技法を使用するには、検索中に検出され、その後実行された悪意のあるコードが組織のシステムに感染しないようにするために、いくつかのサポートする分離手段が必要である。仮想化は、このような分離を実現するための一般的な技法である。

関連管理策：SC-7, SC-26, SC-44, SI-3, SI-4

拡張管理策：なし

参照資料：なし

SC-36 分散処理およびストレージ

管理策：[*設定：組織が定める処理およびストレージコンポーネント*]を複数の[*選択：物理的な場所；論理ドメイン*]に分散する。

詳解：複数の物理的な場所または論理ドメインに処理とストレージを分散させると、組織にある程度の冗長性または重複が提供される。冗長性と重複は、敵対者の作業要因を増加させ、組

織の運営、資産、および個人に有害なインパクトを与える。分散処理およびストレージの使用は、単一の主要な処理またはストレージの場所を想定していない。したがって、並列処理とストレージが可能になる。

関連管理策：CP-6, CP-7, PL-8, SC-32

拡張管理策：

(1) 分散処理およびストレージ｜ポーリング技法

(a) ポーリング技法を使用して、[*設定：組織が定める分散処理およびストレージコンポーネント*]に対する潜在的な障害、エラー、または侵害を特定する。

(b) 特定された障害、エラー、または侵害に対応して、[*設定：組織が定めるアクション*]を実行する。

詳解：分散処理および／またはストレージは、敵対者が組織の情報およびシステムの機密性、完全性、または可用性を侵害する機会を減らすために使用される可能性がある。ただし、処理コンポーネントとストレージコンポーネントを分散しても、敵対者が 1 つまたは複数のコンポーネントを危険にさらすこと防ぐことはできない。ポーリングでは、分散コンポーネントからの処理結果やストレージコンテンツを比較し、結果を決める。ポーリングは、分散処理およびストレージコンポーネントの潜在的な障害、毀損、またはエラーを特定する。

関連管理策：SI-4

(2) 分散処理およびストレージ｜同期

[*設定：組織が定める重複するシステムまたはシステムコンポーネント*]を同期する。

詳解：SC-36 および CP-9(6)は、分散した場所にシステムまたはシステムコンポーネントを複製する必要がある。重複した冗長なサービスとデータの同期は、分散した場所に含まれる情報を、必要に応じて組織のミッションや事業の機能で使用できるようにするのに役立つ。

関連管理策：CP-9

参照資料：[SP 800-160-2]

SC-37 帯域外チャネル

管理策：[*設定：組織が定める情報、システムコンポーネント、またはデバイス*]の[*設定：組織が定める個人またはシステム*]への物理的送達または電子的伝送には、[*設定：組織が定める帯域外チャネル*]を採用する。

詳解：帯域外チャネルには、システムへのローカルな非ネットワークアクセスが含まれる；運用トラフィックに使用されるネットワークパスから物理的に分離されたネットワークパス；または米国郵政公社などの非電子経路。帯域外チャネルの使用は、通常の運用トラフィックを伝送する帯域内チャネル（つまり、同じチャネル）の使用と対照的である。帯域外チャネルには、帯域内チャネルと同じ脆弱性や危険性はない。したがって、インバンドチャネルの機密性、完全性、または可用性の侵害は、アウトオブバンドチャネルを侵害毀損したり悪影響を与えることはない。組織は、オーセンティケータやクレデンシャル；暗号鍵管理情報；システムおよびデータのバックアップ；ハードウェア、ファームウェア、またはソフトウェアの構成管理の変更；セキュリティアップデート；メンテナンス情報；および悪意のあるコード保護の更新を含む組織アイテムの配信または伝送に帯域外チャネルを採用することがある。

関連管理策：AC-2, CM-3, CM-5, CM-7, IA-2, IA-4, IA-5, MA-4, SC-12, SI-3, SI-4, SI-7

拡張管理策：

(1) 帯域外チャネル｜確実な配信および送信

[*設定：組織が定める管理策*]を採用して、[*設定：組織が定める個人またはシステム*]のみが[*設定：組織が定める情報、システムコンポーネント、またはデバイス*]を受け取ることを保証する。

詳解：指定されたシステムまたは個人のみが特定の情報、システムコンポーネント、またはデバイスを受け取ることを保証するために組織が採用する技法には、承認された宅配サービスを介して認証子を送達することを含むが、受信者は領収の条件として政府発行の写真付き身分証明書を提示する必要がある。

関連管理策：なし

参照資料：[SP 800-57-1], [SP 800-57-2], [SP 800-57-3]

SC-38 運用セキュリティ

管理策：システム開発ライフサイクル全体を通じて主要な組織情報を保護するために、[*設定：組織が定める運用セキュリティ管理策*]を採用する。

詳解：運用セキュリティ（OPSEC：Operations security）は体系的なプロセスであり、特に機微な組織活動の計画と実行に関連する一般的に機密扱いされていない情報を特定、制御、保護することで、潜在的な敵対者から組織の能力や意図に関する情報を守ることができる。OPSEC プロセスには、重要な情報の特定、脅威の分析、脆弱性の分析、リスクアセスメント、および適切な対策の適用という 5 つのステップが含まれる。OPSEC の管理策は、組織のシステムとそれらのシステムが動作する環境に適用される。OPSEC の管理策は、サプライヤ、潜在的なサプライヤ、およびその他の非組織的要素や個人との情報共有を限定することを含め、情報の機密性を保護する。組織の、要素の用途、サプライヤ、サプライチェーンプロセス、機能要件、セキュリティ要件、システム設計仕様、テストおよび評価プロトコル、およびセキュリティ管理実装の詳細が含まれる。

関連管理策：CA-2, CA-7, PL-1, PM-9, PM-12, RA-2, RA-3, RA-5, SC-7, SR-3, SR-7

拡張管理策：なし

参照資料：なし

SC-39 プロセス分離

管理策：実行中のシステムプロセスごとに別個の実行ドメインを維持する。

詳解：システムは、各プロセスに個別のアドレス空間を設定することにより、各実行プロセスに対して個別の実行ドメインを維持することができる。各システムプロセスには個別のアドレス空間があるため、プロセス間の通信はセキュリティ機能によって制御された方法で実行され、あるプロセスが別のプロセスの実行コードを変更することはできない。プロセスを実行するための個別の実行ドメインを維持することは、例えば、個別のアドレス空間を実装することによって達成できる。サンドボックス化または仮想化を含むプロセス分離技術は、ソフトウェアおよびファームウェアを他のソフトウェア、ファームウェア、およびデータから論理的に分離する。プロセスの分離は、信頼できない可能性のあるソフトウェアから他のシステム資源へのアクセスを限定するのに役立つ。個別の実行ドメインを維持する機能は、マルチステートプロセッサ技術を採用した商用オペレーティングシステムで利用できる。

関連管理策：AC-3, AC-4, AC-6, AC-25, SA-8, SC-2, SC-3, SI-16

拡張管理策：

(1) プロセス分離 | ハードウェア分離

ハードウェア分離メカニズムを実装して、プロセスの分離を促進する。

詳解：システムプロセスのハードウェアベースの分離は、ソフトウェアベースの分離よりも一般に侵害の影響を受けにくいため、分離が強制されることをより確実にする。ハードウェア分離メカニズムには、ハードウェアメモリ管理が含まれる。

関連管理策：なし

(2) プロセス分離 | スレッドごとの個別の実行ドメイン

[*設定：組織が定めるマルチスレッド処理*]で、スレッドごとに個別の実行ドメインを維持

する。

詳解：なし

関連管理策：なし

参照資料：[SP 800-160-1]

SC-40 ワイヤレスリンクの保護

管理策：信号パラメータ攻撃：[*設定：組織が定めるタイプの信号パラメータ攻撃またはそのような攻撃のソースへの参照*]から外部および内部の[*設定：組織が定める無線リンク*]を保護する。

詳解：ワイヤレスリンクの保護は、認可されたシステムユーザではない個人が見ることができる内部および外部ワイヤレス通信リンクに適用される。ワイヤレスリンクが適切に保護されていない場合、敵対者はワイヤレスリンクの信号パラメータを悪用する可能性がある。ワイヤレスリンクの信号パラメータを悪用して、インテリジェンスを取得したり、サービスを拒否したり、システムユーザを偽装したりする方法は数多くある。ワイヤレスリンクの保護は、ワイヤレスシステムに特有の攻撃のインパクトを軽減する。組織が完全な専用サービスとしてではなく、商品としての伝送サービスを商用サービスプロバイダに依存している場合、組織のセキュリティ要件を満たすために必要な範囲でワイヤレスリンク保護を実装することは不可能な場合がある。

関連管理策：AC-18, SC-5

拡張管理策：

(1) ワイヤレスリンクの保護 | 電磁干渉

意図的な電磁干渉の影響に対して[*設定：組織が定める保護レベル*]を達成する暗号メカニズムを実装する。

詳解：電磁干渉に対するための暗号メカニズムの実装は、電磁妨害対策を提供するために使用されるワイヤレススペクトラム拡散波形が認可されていない個人によって予測不可能であることを保証することにより、通信を拒否または損なう意図的な妨害からシステムを保護する。暗号メカニズムの実装は、同じスペクトルを共有する正当な送信機からの干渉による意図しない妨害の影響を同時に発生させて軽減しても良い。ミッション要件、予測される脅威、運用の概念、法律、大統領令、指令、規則、ポリシー、および基準によって、ワイヤレスリンクの可用性、必要な暗号、およびパフォーマンスレベルが決まる。

関連管理策：PE-21, SC-12, SC-13

(2) ワイヤレスリンクの保護 | 検知の可能性の低減

暗号メカニズムを実装して、ワイヤレスリンクの検知の可能性を[*設定：組織が定める低減レベル*]に低減する。

詳解：潜在的な検知能力を低減するための暗号メカニズムの実装は、秘密通信に使用され無線送信機を地理位置の検知から保護するために使用される。また、低い検知確率を達成するために使用されるスペクトラム拡散波形が、認可されていない個人によって予測可能でないことも保証する。ミッション要件、予想される脅威、運用の概念、適用される法律、大統領令、指令、規則、ポリシー、および基準によって、ワイヤレスリンクが検知されないレベルが決まる。

関連管理策：SC-12, SC-13

(3) ワイヤレスリンクの保護 | 模倣的または操作的な通信の偽装

暗号メカニズムを実装して、信号パラメータに基づいて模倣的または操作的な通信の偽装を達成しようとする意図的な試みである無線伝送を識別および拒否する。

詳解：模倣通信または操作通信を識別および拒否するための暗号メカニズムを実装することにより、認可されていない個人が無線通信の信号パラメータを予測できないようにする。このような予測不能性は、信号パラメータのみに基づいて、模倣または操作による通信の偽装の可能性を低減する。

関連管理策：SC-12, SC-13, SI-4

(4) ワイヤレスリンクの保護 | 信号パラメータの識別

送信機の信号パラメータを使用して、[*設定：組織が定める無線送信機*]の識別を防止するために、暗号メカニズムを実装する。

詳解：無線送信機の識別を防止するための暗号メカニズムの実装は、信号パラメータに対するフィンガープリント防止の変更が認可されていない個人によって予測可能でないことを保証することにより、諜報活動の目的で無線送信機の一意の識別から保護する。また、必要に応じて匿名性を提供する。無線フィンガープリント技法では、追跡およびミッションまたはユーザ識別の目的で、無線送信機をフィンガープリントするために、無線送信機の固有の信号パラメータを識別する。

関連管理策：SC-12, SC-13

参照資料：なし

SC-41 ポートおよび I/O デバイスへのアクセス

管理策：[*設定：組織が定めるシステムまたはシステムコンポーネント*]の[*設定：組織が定める接続ポートまたは入出力デバイス*]を[*選択：物理的；論理的*]に無効化または削除する。

詳解：接続ポートには、ユニバーサルシリアルバス（USB：Universal Serial Bus）、サンダーボルト、ファイヤーワイヤー（IEEE 1394）などがある。入出力（I/O）デバイスには、コンパクトディスクやデジタル多用途ディスクドライブが含まれる。このような接続ポートと I/O デバイスを無効化または削除することで、システムからの情報の漏出や、それらのポートやデバイスからの悪意のあるコードの侵入を防ぐことができる。ポートやデバイスを物理的に無効化または削除することはより強力な対応である。

関連管理策：AC-20, MP-7

拡張管理策：なし

参照資料：なし

SC-42 センサの能力およびデータ

管理策：

a. [*選択（1 つ以上）：[設定：組織が定める施設、エリア、またはシステム]の[設定：組織が定める環境センシング機能]を有するデバイスの使用；組織のシステムまたはシステムコンポーネント上の環境感知機能のリモートアクティベーション、ただし、[設定：組織が定めるセンサのリモートアクティベーションが許可される例外]*]を禁止する。

b. [*設定：組織が定めるユーザのグループ*]に、センサの使用の明示的な表示を提供する。

詳解：センサ機能とデータは、携帯電話、スマートフォン、タブレットなどのモバイル機器として特徴付けられるシステムまたはシステムコンポーネントのタイプに適用される。多くの場合、モバイルデバイスには、システムが使用されている環境に関するデータを収集および記録できるセンサが含まれる。モバイルデバイスに組み込まれているセンサには、マイク、カメラ、全地球測位システム（GPS）メカニズム、加速度計などがある。モバイルデバイスのセンサは重要な機能を提供するが、密かに活性化された場合、そのようなデバイスは潜在的に敵対者が個人や組織に関する貴重な情報を学習する手段を提供する可能性がある。例えば、モバイルデバイスの GPS 機能をリモートで活性化すると、敵対者に個人の動きを追跡する機能を提供できる。組織は、個人が携帯電話やデジタルカメラを、国家機密情報が保存されている施設や機微な会話が行われている施設内の指定された施設や管理区域に持ち込むことを禁止する場合がある。

関連管理策：SC-15

拡張管理策：

(1) センサの能力およびデータ｜認可された個人または役割への報告

[*設定：組織が定めるセンサ*]によって収集されたデータまたは情報が、認可された個人または役割にのみ報告されるようにシステムが構成されていることを確認する。

詳解：許可された個人がセンサを作動させる場合でも、センサが収集したデータや情報が認可されていないエンティティに送信される可能性がある。

関連管理策：なし

(2) センサの能力およびデータ｜認可された使用

[*設定：組織が定めるセンサ*]によって収集されたデータまたは情報が、認可された目的にのみ使用されるように、[*設定：組織が定める措置*]を採用する。

詳解：特定の認可された目的のためにセンサによって収集された情報は、いくつかの認可されていない目的に悪用される可能性がある。例えば、交通ナビゲーションをサポートするために使用される GPS センサは、個人の動きを追跡するために悪用される可能性がある。そのような行為を軽減するための措置には、認可された個人がその権限を悪用しないようにするための追加の訓練や、センサデータが外部の関係者によって維持されている場合、そのようなデータの使用に関する契約上の制限が含まれる。

関連管理策：PT-2

(3) センサの能力およびデータ｜デバイスの使用禁止

[撤回：SC-42 に組み込まれた]

(4) センサの機能およびデータ｜収集に関する通知

個人情報が[*設定：組織が定めるセンサ*]によって収集されているという個人の認識を促進するために、[*設定：組織が定める措置*]を採用する。

詳解：組織のセンサがデータを収集していることを意識することで、個人はより効果的にプライバシーの管理に取り組むことができる。対策には、従来の書面による通知およびセンサが情報を収集していることを他のデバイスを介して直接的または間接的に個人に知らせるセンサ構成を含めることができる。通知の使いやすさと有効性は重要な考慮事項である。

関連管理策：PT-1, PT-4, PT-5

(5) センサの能力およびデータ｜収集の最小化

必要のない個人に関する情報の収集を最小限に抑えるように構成された[*設定：組織が定めるセンサ*]を採用する。

詳解：認可された使用を制御するポリシーは、収集された情報に適用できるが、不要な情報の収集を最小限に抑えることで、システムの入口でのプライバシーリスクが軽減され、ポリシー制御が失敗するリスクが軽減される。センサの構成には、肌の色調をぼかしたり、ピクセル化したりするなど、人間の特徴を不明瞭にすることが含まれる。

関連管理策：SA-8, SI-12

参照資料：[OMB A-130], [SP 800-124]

SC-43 使用制限

管理策：

a. [*設定：組織が定めるシステムコンポーネント*]の使用制限と実装ガイドラインを確立する。

b. システム内でのこのようなコンポーネントの使用を承認、監視、制御する。

詳解：使用制限は、モバイルコード、モバイルデバイス、ワイヤレスアクセス、有線およびワイヤレス周辺機器コンポーネント（例えば、コピー機、プリンタ、スキャナ、光学デバイス、およびその他の同様の技術）を含むすべてのシステムコンポーネントに適用される。使用規制および実装ガイドラインは、システムコンポーネントがシステムに損傷を与える可能性に基づいて、認可さ

れたシステムのみの運用が行われることを保証するのに役立つ。

関連管理策：AC-18, AC-19, CM-6, SC-7, SC-18

拡張管理策：なし

参照資料：[OMB A-130], [SP 800-124]

SC-44 デトネーションチャンバー

管理策：[*設定：組織が定めるシステム、システムコンポーネント、または場所*]内でデトネーションチャンバー機能を採用する。

詳解：動的実行環境としても知られているデトネーションチャンバーは、組織が電子メールの添付ファイルを開き、信頼できないまたは疑わしいアプリケーションを実行し、隔離された環境または仮想化されたサンドボックスのセキュアな環境でユニバーサルレコードロケータ（URL）リクエストを実行できるようにする。保護され隔離された実行環境は、関連する添付ファイルまたはアプリケーションに悪意のあるコードが含まれているかどうかを判断する手段を提供する。デトネーションネットの概念に関連しているが、デトネーションチャンバーの使用は、敵対者が操作し、その行動を観察できる長期的な環境を維持することを意図したものではない。むしろ、デトネーションチャンバーは、悪意のあるコードを迅速に特定し、コードがユーザの操作環境に伝播する可能性を減らすか、そのような伝播を完全に防ぐことを目的としている。

関連管理策：SC-7, SC-18, SC-25, SC-26, SC-30, SC-35, SC-39, SI-3, SI-7

拡張管理策：なし

参照資料：[SP 800-177]

SC-45 システム時刻同期

管理策：システム内およびシステムとシステムコンポーネント間でシステムクロックを同期する。

詳解：システムクロックの時刻同期は、アクセス制御の一部として証明書および時刻制限を伴う識別および認証プロセスを含む、多くのシステムサービスを正しく実行するために不可欠である。システムおよびシステムコンポーネント内およびシステム間でクロックが適切に同期されていないと、サービス拒否または有効期限切れの資格情報の拒否に失敗する可能性がある。時刻は通常、協定世界時（UTC：Coordinated Universal Time）、グリニッジ標準時（GMT：Greenwich Mean Time）の最新の継続時間、または UTC からのオフセットを持つ現地時刻で表される。時刻測定の粒度は、数百ミリ秒または数十ミリ秒以内で同期するクロックなど、システムクロックと基準クロックとの間の同期の程度を指す。組織は、システムコンポーネントに異なる時刻の粒度を規定する場合がある。アクセス制御や識別、認証など、他のセキュリティ機能にとって、タイムサービスは、機能をサポートするために使用されるメカニズムの性質によっては、非常に重要になる場合がある。

関連管理策：AC-3, AU-8, IA-2, IA-8

拡張管理策：

(1) システム時刻同期 | 信頼できるタイムソースとの同期

(a) [*設定：組織が定める周期*]で内部システムクロックと[*設定：組織が定める信頼できるタイムソース*]を比較する。

(b) 時間差が[*設定：組織が定める時間*]よりも大きい場合、内部システムクロックを信頼できるタイムソースに同期させる。

詳解：内部システムクロックと信頼できるソースとの同期は、複数のシステムクロックを備えたシステムおよびネットワークを介して接続されたシステムにタイムスタンプの均一性を提供する。

関連管理策：なし

(2) システム時刻同期 | 二次的な信頼できるタイムソース

(a) 一次的な信頼できるタイムソースとは異なる地理的地域にある二次的な信頼できるタイムソースを特定する。

(b) 一次的な信頼できるタイムソースが使用できない場合は、内部システムクロックを二次的な信頼できるタイムソースに同期させる。

詳解：二次的な信頼できるタイムソースが別の地理的地域にあることを決定するために、地理位置情報を使用する必要がある場合がある。

関連管理策：なし

参照資料：[IETF 5905]

SC-46 クロスドメインポリシーの実施

管理策：接続するセキュリティドメインのための物理的および／またはネットワークインタフェース間にポリシー実施メカニズム[*選択：物理的；論理的*]を実装する。

詳解：論理的ポリシー実施メカニズムの場合、組織は、ポリシー実施メカニズムをバイパスする機能を防ぐために、インタフェース間に論理パスを作成することを避ける。物理的なポリシー実施メカニズムについては、セキュリティドメインに侵入する論理的な隠れチャネルの存在を排除するために、ポリシー実施の物理的実装によって提供される物理的分離の堅牢性が必要となる場合がある。詳細については、ncdsmo@nsa.gov に問い合わせのこと。

関連管理策：AC-4, SC-7

拡張管理策：なし

参照資料：[SP 800-160-1]

SC-47 代替通信経路

管理策：システム運用組織のコマンドおよび制御のための[*設定：組織が定める代替通信経路*]を確立する。

詳解：インシデントは、敵対的か非敵対的かにかかわらず、システムの運用や組織の指揮統制に使用される確立された通信経路を中断させる可能性がある。代替通信経路は、すべての通信経路が同じインシデントの影響を受けるリスクを軽減する。問題をさらに複雑にするのは、通信経路のインシデントが発生した後、組織の担当者が中断に関するタイムリーな情報を入手したり、運用要素にタイムリーな指示を提供できないことで、組織がそのようなインシデントにタイムリーに対応する能力にインパクトを与える可能性があることである。主要な意思決定者が利用できない場合に代替の意思決定者を指定し、その行動の範囲と規制を確立することを含み、指揮統制のために代替の通信経路を確立することは、インシデント中も継続して適切な行動を取る組織の能力を大いに促進することができる。

関連管理策：CP-2, CP-8

拡張管理策：なし

参照資料：[SP 800-34], [SP 800-61], [SP 800-160-2]

SC-48 センサの再配置

管理策：[*設定：組織が定めるセンサおよび監視機能*]を[*設定：組織が定める場所*]に、[*設定：組織が定める条件または環境*]で再配置する。

詳解：敵対者は、組織（システムを含む）を横切って標的に到達するとき、または組織から情報を漏出しようとするとき、様々な経路をとり、異なるアプローチを使用することがある。多くの場合、組織は監視機能と検知機能のセットが限定されているため、重要な、または侵入または漏出の可能性の高い経路に焦点を当てている場合がある。組織が通常監視しない通信経路を使

用することにより、敵対者は、所望の目標を達成する可能性を高めることができる。センサや監視機能を新しい場所に再配置することで、組織は敵対者の目標を達成する能力を妨げることができる。センサまたは監視機能の再配置は、組織が取得した脅威情報に基づいて、またはランダムに敵対者を混乱させ、システムまたは組織を横切る移行をより困難にする可能性がある。

関連管理策: AU-2, SC-7, SI-4

拡張管理策:

(1) センサの再配置 | センサまたは監視機能の動的な再配置

[*設定:組織が定める条件または状況*]で、[*設定:組織が定めるセンサおよび監視機能*]を[*設定:組織が定める場所*]に動的に再配置する。

詳解:なし

関連管理策:なし

参照資料: [SP 800-160-2]

SC-49 ハードウェアによる分離およびポリシーの実施

管理策: [*設定:組織が定めるセキュリティドメイン*]間のハードウェアによる分離とポリシー実施メカニズムを実装する。

詳解:システムオーナーは、特定のタイプの脅威と運用環境に対するドメインの分離とポリシーの適用を確実にするために、追加のメカニズム強度と堅牢性を必要としても良い。ハードウェアによる分離とポリシーの実施は、ソフトウェアによる分離とポリシーの実施よりも優れたメカニズムを提供する。

関連管理策: AC-4, SA-8, SC-50

拡張管理策:なし

参照資料: [SP 800-160-1]

SC-50 ソフトウェアによる分離およびポリシーの実施

管理策: [*設定:組織が定めるセキュリティドメイン*]間のソフトウェアによる分離およびポリシーの実施メカニズムを実装する。

詳解:システムオーナーは、特定のタイプの脅威と運用環境に対するドメインの分離とポリシーの実施を確実にするために、追加の強力なメカニズムを必要としても良い。

関連管理策: AC-3, AC-4, SA-8, SC-2, SC-3, SC-49

拡張管理策:なし

参照資料: [SP 800-160-1]

SC-51 ハードウェアベースの保護

管理策:

a. [*設定:組織が定めるシステムファームウェアコンポーネント*]に、ハードウェアベースの書き込み保護を採用する。

b. [*設定:組織が定める認可された個人*]がファームウェアの変更に対してハードウェアの書き込み保護を手動で無効にし、操作モードに戻る前に書き込み保護を再度有効にする、特定の手順を実装する。

詳解:なし

関連管理策:なし

拡張管理策:なし

参照資料:なし

3.19 システムおよび情報の完全性

システムおよび情報の完全性の要約表へのクイックリンク

SI-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。

1. 以下の[*選択(1 つ以上):組織レベル;ミッション/事業プロセスレベル;システムレベル*]のシステムおよび情報の完全性のポリシー。

(a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、および準拠に対処する。

(b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに適合している。

2. システムおよび情報の完全性のポリシーと関連するシステムおよび情報の完全性の管理策の実装を促進するための手順。

b. システムおよび情報の完全性のポリシーと手順の策定、文書化、および配布することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行のシステムおよび情報の完全性をレビューし、更新する。

1. ポリシーについて[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

2. 手順について[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

詳解:システムおよび情報の完全性のポリシーと手順は、システムおよび組織で実装される SI ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に寄与する。したがって、セキュリティおよびプライバシープログラムがシステムおよび情報の完全性のポリシーと手順の策定と連携していることが重要である。セキュリティおよびプライバシープログラムのポリシーと手順を組織レベルで確立することは望ましく、一般的には、ミッションまたはシステム固有のポリシーと手順を不要にすることができる。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映する複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムに対して規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述し、手順の対象である個人または役割向けとすることができる。手順は、システムのセキュリティおよびプライバシー計画の中に、または 1 つ以上の別の文書に文書化することもできる。システムおよび情報の完全性のポリシーと手順の更新を引き起こす可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれる。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策:PM-9, PS-8, SA-8, SI-12

拡張管理策:なし

参照資料:[OMB A-130], [SP 800-12], [SP 800-100]

SI-2 欠陥の修正

管理策:

a. システムの欠陥を特定、報告、修正する。

b. 欠陥修正に関連するソフトウェアとファームウェアのアップデートを、インストール前に有効性と潜在的な影響についてテストする。

c. セキュリティ関連のソフトウェアおよびファームウェアのアップデートを、アップデートのリリースから[*設定:組織が定める期間*]以内にインストールする。

d. 欠陥の修正を組織の構成管理プロセスに組み込む。

詳解:システムの欠陥を修正する必要性は、すべてのタイプのソフトウェアとファームウェアに当てはまる。組織は、ソフトウェアの欠陥の影響を受けるシステムを特定し、それらの欠陥に起因する潜在的な脆弱性を特定し、この情報を、情報セキュリティとプライバシーの責任を有する指定された組織職員に報告する。セキュリティ関連の更新プログラムには、パッチ、サービスパック、悪意のあるコードの署名などがある。組織は、アセスメント、継続的な監視、インシデント対応活動、およびシステムエラー処理中に検出された欠陥にも対処する。欠陥の修正を構成管理プロセスに組み込むことにより、必要な修正アクションを追跡および検証できる。

セキュリティ関連のソフトウェアおよびファームウェアを更新するために組織が定める期間は、システムのセキュリティの分類、更新の重要度(すなわち検出された欠陥に関連する脆弱性の重大度など)、組織のリスク許容度、システムがサポートするミッション、または脅威環境など、様々なリスク要因に応じて異なっても良い。欠陥修正のタイプによっては、他のタイプよりも多くのテストが必要になっても良い。組織は、考慮中の特定のタイプの欠陥修正活動に必要なテストのタイプと、構成管理される変更のタイプを決定する。組織は、単純な悪意のあるコード署名の更新を実装する場合など、ソフトウェアまたはファームウェアの更新のテストが不要または実用的でないと判断しても良い。テストの判断において、組織は、セキュリティ関連のソフトウェアまたはファームウェアの更新が、適切なデジタル署名付きの認可されたソースから取得されているかどうかを検討する。

関連管理策:CA-5, CM-3, CM-4, CM-5, CM-6, CM-8, MA-2, RA-5, SA-8, SA-10, SA-11, SI-3, SI- 5, SI-7, SI-11

拡張管理策:

(1) 欠陥の修正 | 一元管理

[撤回:PL-9 に組み込まれた]

(2) 欠陥の修正 | 自動化された欠陥の修正ステータス

システムコンポーネントに、[*設定:組織が定める自動化されたメカニズム*]を使用して[*設定:組織が定める頻度*]で、適用されるセキュリティ関連のソフトウェアおよびファームウェアのアップデートがインストールされているかどうかを判断する。

詳解:自動化されたメカニズムは、システムコンポーネントの既知の欠陥の状態を追跡し、決定することができる。

関連管理策:CA-7, SI-4

(3) 欠陥の修正 | 欠陥を修正する時間および是正処置のベンチマーク

(a) 欠陥の特定から欠陥の修正までの時間を測定する。

(b) 是正措置を取るための[*設定:組織が定めるベンチマーク*]を確立する。

詳解:組織は、システムの欠陥が特定された後、平均してシステムの欠陥を修正するのにかかる時間を決定し、その後、修正措置を講じるための組織のベンチマーク(つまり、時間枠)を確立する。ベンチマークは、欠陥のタイプ、または欠陥が悪用される可能性がある場合に潜在的な脆弱性の重大度によって確立することができる。

関連管理策:なし

(4) 欠陥の修正 | 自動化されたパッチ管理ツール

自動化されたパッチ管理ツールを採用して、[*設定:組織が定めるシステムコンポーネント*]への欠陥修正を容易にする。

詳解:自動化ツールを使用してパッチ管理をサポートすることで、システムのパッチ適用操作の適時性と正確性を確保できる。

関連管理策:なし

(5) 欠陥の修正 | ソフトウェアおよびファームウェアの自動更新

[*設定:組織が定めるシステムコンポーネント*]に[*設定:組織が定めるセキュリティ関連のソフトウェアおよびファームウェアの更新*]を自動的にインストールする。

詳解:システムの完全性と可用性の問題から、組織は自動更新の実行に使用される方法を考慮する。組織は、更新をできるだけ早くインストールすることの必要性と、自動更新がもたらす可能性のあるミッションまたは運用へのインパクトを伴う構成管理および管理策を維持する必要性とのバランスをとる。

関連管理策:なし

(6) 欠陥の修正 | ソフトウェアおよびファームウェアの以前のバージョンの削除

更新されたバージョンがインストールされた後、以前のバージョンの[*設定:組織が定めるソフトウェアおよびファームウェアコンポーネント*]を削除する。

詳解:アップデートのインストール後にシステムから削除されない以前のバージョンのソフトウェアまたはファームウェアコンポーネントが、敵対者に悪用される可能性がある。一部の製品では、以前のバージョンのソフトウェアとファームウェアがシステムから自動的に削除されても良い。

関連管理策:なし

参照資料:[OMB A-130], [FIPS 140-3], [FIPS 186-4], [SP 800-39], [SP 800-40], [SP 800-128], [IR 7788]

SI-3 悪意のあるコードからの保護

管理策:

a. 悪意のあるコードを検知して根絶するために[*選択(1 つ以上):署名ベース;非署名ベース*]の悪意のあるコードからの保護メカニズムを、システムの入口および出口に実装する。

b. 組織の構成管理ポリシーおよび手順に従って新しいリリースが利用可能になると、悪意のあるコードからの保護メカニズムが自動的に更新される。

c. 悪意のあるコードからの保護メカニズムを以下のように構成する。

1. [*設定:組織が定める頻度*]でシステムの定期スキャン、および[*選択(1 つ以上):エンドポイント;ネットワークの入口および出口*]で、ファイルが組織のポリシーに従ってダウンロード、オープン、または実行されるときに外部ソースからのファイルのリアルタイムスキャンを実行する。

2. 悪意のあるコードの検知に対応して[*選択(1 つ以上):悪意のあるコードをブロックする;悪意のあるコードを隔離する;[設定:組織が定めるアクション]*]を行い、[*設定:組織が定める職員または役割*]にアラートを送信する。

d. 悪意のあるコードの検知と根絶の際の誤検知の受信、およびシステムの可用性への潜在的なインパクトに対処する。

詳解:システムの入口と出口には、ファイアウォール、リモートアクセスサーバ、ワークステーション、電子メールサーバ、ウェブサーバ、プロキシサーバ、ノートブックコンピュータ、モバイルデバイスなどがある。悪意のあるコードには、ウイルス、ワーム、トロイの木馬、スパイウェアが含まれる。悪意のあるコードは、ステガノグラフィーなどの技法を使用して、圧縮ファイルや隠しファイルに含まれる、またはファイルに隠された様々な形式でエンコードすることもできる。悪意のあるコードは、電子メール、ワールドワイドウェブ、ポータブルストレージデバイスなど、様々な

方法でシステムに挿入することが出来る。悪意のあるコードの挿入は、システムの脆弱性の悪用を通じて発生する。悪意のあるコードの影響を限定または排除するために、様々な技術と方法が存在する。

悪意のあるコードからの保護メカニズムには、署名ベースの技術と署名ベースでない技術の両方が含まれる。非署名ベースの検知メカニズムには、悪意のあるコードの特性または動作を検知、分析、記述し、署名がまだ存在しないか、既存の署名が有効でない可能性のあるコードを制御する人工知能技法の提供が含まれる。アクティブな署名がまだ存在しないか、効果がない可能性がある悪意のあるコードには、ポリモーフィックな悪意のあるコード（つまり、複製時に署名を変更するコード）が含まれる。非署名ベースのメカニズムには、レピュテーションベース の技術も含まれる。上記の技術に加えて、広範囲にわたる構成管理、包括的なソフトウェア完全性管理策、および悪用防止ソフトウェアが、認可されていないコードの実行を防止するのに効果的である可能性がある。悪意のあるコードは、市販のソフトウェアや注文製作のカスタムビルドされたソフトウェアに存在する可能性があり、論理爆弾、バックドア、および組織のミッションや事業の機能に影響を与える可能性のあるその他のタイプの攻撃を含む可能性がある。

悪意のあるコードが検知方法または技術で検知できない状況では、組織は、セキュアなコーディング慣行、構成管理と管理、信頼できる調達プロセス、監視慣行など、他のタイプの管理策によって、ソフトウェアが意図した機能以外の機能を実行しないようにする。組織は、悪意のあるコードの検知に対応して、様々なアクションが保証されると判断しても良い。例えば、組織は、定期的なスキャン中の悪意のあるコードの検知、悪意のあるダウンロードの検知、またはファイルを開いたり実行したりする際の悪意の検知に対応して、アクションを規定できる。

関連管理策：AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, MA-4, PL-9, RA-5, SC-7, SC-23, SC-26, SC-28, SC-44, SI-2, SI-4, SI-7, SI-8, SI-15

拡張管理策：

(1) 悪意のあるコードからの保護 | 一元管理

［撤回：PL-9 に組み込まれた］

(2) 悪意のあるコードからの保護 | 自動更新

［撤回：SI-3 に組み込まれた］

(3) 悪意のあるコードからの保護 | 非特権ユーザ

［撤回：AC-6(10)に組み込まれた］

(4) 悪意のあるコードからの保護 | 特権ユーザに限定した更新

特権ユーザからの指示があった場合にのみ、悪意のあるコードからの保護メカニズムを更新する。

詳解：悪意のあるコードからの保護メカニズムは、通常、セキュリティ関連のソフトウェアとして分類され、適切なアクセス権限を持つ組織の職員によってのみ更新される。

関連管理策：CM-5

(5) 悪意のあるコードからの保護 | ポータブルストレージデバイス

［撤回：MP-7 に組み込まれた］

(6) 悪意のあるコードからの保護 | テストおよび検証

(a) 既知の良性コードをシステムに導入することにより、[*設定：組織が定める頻度*]で悪意のあるコードの保護メカニズムをテストする。

(b) コードの検知および関連するインシデント報告が発生することを検証する。

詳解：なし

関連管理策：CA-2, CA-7, RA-5

(7) 悪意のあるコードからの保護 | 非署名ベースの検知

［撤回：SI-3 に組み込まれた］

(8) 悪意のあるコードからの保護 | 認可されていないコマンドの検知

(a) カーネルアプリケーションプログラミングインタフェースを介して、[*設定:組織が定めるシステムハードウェアコンポーネント*]の[*設定:組織が定める認可されていないオペレーティングシステムコマンド*]を検知する。

(b) [*選択(1 つ以上):警告を発行する;コマンドの実行を監査する;コマンドの実行を防止する*]。

詳解:認可されていないコマンドの検知は、仮想マシンや特権アプリケーションとのインタフェースなど、カーネルベースのインタフェース以外の重要なインタフェースに適用できる。認可されていないオペレーティングシステムコマンドには、そのようなコマンドを開始するために信頼されていないシステムプロセスからのカーネル機能のコマンドや、そのタイプのコマンドがプロセスを開始するのに妥当であるとしても疑わしいカーネル機能のコマンドが含まれる。組織は、コマンドタイプ、コマンドクラス、またはコマンドの特定のインスタンスの組み合わせによって検知される悪意のあるコマンドを規定できる。組織は、ハードウェアコンポーネントを、コンポーネントタイプ、コンポーネント、ネットワーク内のコンポーネントの場所、またはそれらの組み合わせによって規定することもできる。組織は、悪意のあるコマンドのタイプ、クラス、またはインスタンスごとに異なるアクションを選択しても良い。

関連管理策:AU-2, AU-6, AU-12

(9) 悪意のあるコードからの保護 | リモートコマンドの認証

[撤回:AC-17(10)に移動した]

(10) 悪意のあるコードからの保護 | 悪意のあるコードの分析

(a) [*設定:組織が定めるツールと技法*]を採用して、悪意のあるコードの特性と動作を分析する。

(b) 悪意のあるコードの分析の結果を組織のインシデント対応および欠陥修正プロセスに組み込む。

詳解:悪意のあるコードの分析ツールを使用することで、組織に、敵対者の窃取技術(すなわち、戦術、技法、および手順)と、悪意のあるコードの特定の事例の機能および目的のより深い理解を提供できる。悪意のあるコードの特性を理解することで、現在および将来の脅威に対する組織の効果的な対応が容易になる。組織は、リバースエンジニアリング技法を採用するか、実行中のコードの動作を監視することにより、悪意のあるコードの分析を行うことができる。

関連管理策:なし

参照資料:[SP 800-83], [SP 800-125B], [SP 800-177]

SI-4 システム監視

管理策:

a. システムを監視して以下を検知する。
   1. [*設定:組織が定める監視目的*]に一致した攻撃と潜在的な攻撃の兆候。
   2. 認可されていないローカル接続、ネットワーク接続、およびリモート接続。
b. [*設定:組織が定める技法と方法*]により、システムの認可されていない使用を特定する。
c. 内部監視機能を呼び出すか、監視デバイスを展開する。
   1. 組織が決定した重要な情報を収集するために、システム内で戦略的に実施する。
   2. システム内のアドホックな場所で、組織にとって関心のある特定のタイプの処理を追跡する。
d. 検知されたイベントと異常を分析する。
e. 組織の運営および資産、個人、他の組織、または国家に対するリスクに変化があった

場合、システム監視活動のレベルを調整する。

f. システム監視活動に関する法的意見を入手する。

g. [*設定:組織が定めるシステム監視情報*]を[*選択(1 つ以上):必要に応じて;*[*組織が定める頻度*]]で[*設定:組織が定める職員または役割*]に提供する。

詳解:システム監視には、外部および内部監視が含まれる。外部監視には、システムへの外部インタフェースで発生するイベントの監視が含まれる。内部監視には、システム内で発生するイベントの監視が含まれる。組織は、監査活動をリアルタイムで観察することにより、またはアクセスパターン、アクセスの特性、その他の行動など、システムの他の側面を観察することにより、システムを監視する。監視目的は、イベントの決定を導き、通知する。システム監視機能は、侵入検知・防止システム、悪意のあるコード保護ソフトウェア、スキャンツール、監査記録監視ソフトウェア、ネットワーク監視ソフトウェアなど、様々なツールや技法を通じて実現される。

セキュリティアーキテクチャによっては、監視デバイスの分散と構成が、ネットワークスループットの遅延の導入により、主要な内部境界と外部境界、およびネットワーク全体の他の場所のスループットにインパクトを与える可能性がある。スループット管理が必要な場合、このようなデバイスは戦略的に配置され、確立された組織全体のセキュリティアーキテクチャの一部として展開される。デバイスを監視するための戦略的な場所には、重要なアプリケーションをサポートする、選択された境界の場所や、主要サーバやサーバ群の周辺が含まれる。監視装置は、通常、管理策 SC-7 および AC-17 に関連する管理対象インタフェースで採用されている。収集される情報は、組織の監視目的と、そのような目的をサポートするシステムの機能の関数である。対象となる特定のタイプのトランザクションには、HTTP プロキシをバイパスするハイパーテキスト転送プロトコル(HTTP:Hypertext Transfer Protocol)トラフィックが含まれる。システム監視は、組織の継続的監視およびインシデント対応プログラムの不可欠な部分であり、システム監視からの出力は、これらのプログラムへの入力として機能する。特定タイプのシステム監視の必要性を含むシステム監視要件は、他の管理策(例えば、AC-2g, AC-2(7), AC-2(12)(a), AC-17(1), AU-13, AU-13(1), AU-13(2), CM-3f, CM-6d, MA-3a, MA-4a, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b)で参照される場合がある。システム監視のレベルの調整は、法執行機関の情報、インテリジェンス情報、またはその他のソースに基づいている。システム監視活動の合法性は、適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに基づく。

関連管理策:AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, AU-13, AU-14, CA-7, CM-3, CM-6, CM-8, CM-11, IA-10, IR-4, MA-3, MA-4, PL-9, PM-12, RA-5, RA-10, SC-5, SC-7, SC-18, SC-26, SC-31, SC-35, SC-36, SC-37, SC-43, SI-3, SI-6, SI-7, SR-9, SR-10

拡張管理策:

(1) システム監視 | システム全体の侵入検知システム

個々の侵入検知ツールをシステム全体の侵入検知システムに接続および構成する。

詳解:個々の侵入検知ツールをシステム全体の侵入検知システムにリンクすると、追加のカバレッジと効果的な検知機能が提供される。1 つの侵入検知ツールに含まれる情報を組織全体で広く共有できるため、システム全体の検知機能をより強力かつ強力にすることができる。

関連管理策:なし

(2) システム監視 | リアルタイム分析のための自動化されたツールおよびメカニズム

自動化されたツールおよびメカニズムを採用して、イベントのほぼリアルタイムの分析をサポートする。

詳解:自動化されたツールとメカニズムには、ホストベース、ネットワークベース、移送ベース、またはストレージベースのイベント監視ツールとメカニズム、または組織システムによって生成されたセキュリティ情報とアラートと通知のリアルタイム分析を提供するイベント管理(SIEM:security information and event management)技術が含まれる。自動化された監視技法は、自動化された管理策が外部のシステムまたはその他の無関係なシステムに接続しても良いため、意図しないプライバシーリスクを引き起こすことができる。これらのシステム間のレコードを一致させることで、意図しない結果を伴うリンケージを作成しても良い。組織は、プライバシー影響評価をする際にこれらのリスクを評価して文書化し、プライ

バシープログラム計画に沿った判断を下す。

関連管理策：PM-23, PM-25

(3) システム監視｜自動化されたツールおよびメカニズムの統合

自動化されたツールおよびメカニズムを採用して、侵入検知ツールとメカニズムをアクセス制御メカニズムとフロー制御メカニズムに統合する。

詳解：自動化されたツールおよびメカニズムを使用して、侵入検知ツールおよびメカニズムをアクセス制御メカニズムおよびフロー制御メカニズムに統合すると、攻撃の分離および排除をサポートするメカニズムの再構成を可能にすることで、攻撃への迅速な対応が容易になる。

関連管理策：PM-23, PM-25

(4) システム監視｜インバウンドおよびアウトバウンド通信のトラフィック

(a) インバウンドおよびアウトバウンド通信トラフィックの異常または認可されていない行為または条件の基準を決定する。

(b) [*設定：組織が定める頻度*]で[*設定：組織が定める異常または認可されていない行為または状態*]について、インバウンドおよびアウトバウンド通信トラフィックを監視する。

詳解：システムのインバウンドおよびアウトバウンド通信トラフィックに関連する異常なまたは認可されていない行為または条件には、組織のシステム内での、悪意のあるコードの存在、または正当なコードまたは資格情報の認可されていない使用、またはシステムコンポーネント間での伝播、外部システムへの合図、および情報の認可されていないエクスポートが含まれる。悪意のあるコード、または正当なコードまたは資格情報の認可されていない使用のエビデンスは、侵害された可能性のあるシステムまたはシステムコンポーネントを識別するために使用される。

関連管理策：なし

(5) システム監視｜システムによって生成されたアラート

システムによって生成された侵害または潜在的な侵害の兆候：[*設定：組織が定める侵害*]が発生した場合にアラートを[*設定：組織が定める職員または役割*]に警告する。

詳解：アラートは、監査記録や悪意のあるコード保護メカニズム、侵入検知または防止メカニズム、ファイアウォール、ゲートウェイ、ルータなどの境界保護デバイスからの入力など、様々なソースから生成される可能性がある。警告は自動化することができ、電話、電子メールメッセージ、またはテキストメッセージングによって伝送することができる。警告通知リストの組織職員には、システム管理者、ミッションまたは事業オーナー、情報オーナー／スチュワード、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、システムセキュリティ担当者、またはプライバシー担当者を含めることができる。システムによって生成された警告とは対照的に、SI-4(12)の組織によって生成されたアラートは、疑わしい行為のレポートや潜在的なインサイダー脅威に関するレポートなど、システム外部のソースに焦点を当てている。

関連管理策：AU-4, AU-5, PE-6

(6) システム監視｜非特権ユーザの制限

[撤回：AC-6(10)に組み込まれた]

(7) システム監視｜疑わしいイベントへの自動応答

(a) [*設定：組織が定めるインシデント対応担当者（名前または役割で識別）*]に検知された疑わしいイベントを通知する。

(b) 検知時に[*設定：組織が定める、疑わしいイベントを終了させる為の中断の最も少ないアクション*]を実行する。

詳解：中断の最も少ないアクションには、人間の対応を求める要求の実行が含まれる。

関連管理策：なし

(8) システム監視 | 監視情報の保護

[撤回：SI-4 に組み込まれた]

(9) システム監視 | 監視ツールおよびメカニズムのテスト

[*設定：組織が定める頻度*]で侵入監視ツールおよびメカニズムをテストする。

詳解：侵入監視ツールとメカニズムをテストすることは、ツールとメカニズムが正しく動作していることを確認し、組織の監視目的を継続して満たすために必要である。テストの頻度と深さは、組織が使用するツールとメカニズムのタイプ、および展開方法によって異なる。

関連管理策：なし

(10) システム監視 | 暗号化通信の可視性

[*設定：組織が定める暗号化通信トラフィック*]が[*設定：組織が定めるシステム監視ツールおよびメカニズム*]で見えるように準備する。

詳解：組織は、データの機密性を保護するために通信トラフィックを暗号化する必要性と、監視の観点からそのようなトラフィックの可視性を維持する必要性のバランスをとる。組織は、可視性要件が、内部暗号化トラフィック、外部宛先向けの暗号化トラフィック、またはトラフィックタイプのサブセットのどちらに適用されるかを決定する。

関連管理策：なし

(11) システム監視 | 通信トラフィック異常の分析

[*設定：組織が定めるシステム内の内部ポイント*]を選択してシステムへの外部インタフェースでの外部向けの通信トラフィックを分析し、異常を検出する。

詳解：組織が定める内部ポイントには、サブネットワークとサブシステムが含まれる。組織のシステム内の異常には、大きなファイル転送、長時間の永続的な接続、予期しない場所からの情報へのアクセス試行、異常なプロトコルとポートの使用、監視されていないネットワークプロトコルの使用（IPv4 移行中の IPv6 の使用など）、および悪意のある外部アドレスとの通信試行などが含まれる。

関連管理策：なし

(12) システム監視 | 自動化された組織生成アラート

[*設定：組織が定める自動化されたメカニズム*]を使用して、セキュリティまたはプライバシーに関連する不適切または異常な行為の[*設定：組織が定めるアラートをトリガーする行為*]が発生した場合に[*設定：組織が定める職員または役割*]にアラートする。

詳解：システムアラート通知リストの組織職員には、システム管理者、ミッションまたは事業オーナー、システムオーナー、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、システムセキュリティ担当者、またはプライバシー担当者が含まれる。自動化された組織生成アラートは、組織によって生成され、自動化された手段を使用して伝送されるセキュリティアラートである。組織が生成するアラートのソースは、疑わしい行為のレポートやインサイダーの潜在的な脅威に関するレポートなど、他のエンティティに焦点を当てている。組織が生成するアラートとは対照的に、SI-4(5)のシステムが生成するアラートは、監査記録など、システム内部のソースに焦点を当てている。

関連管理策：なし

(13) システム監視 | トラフィックおよびイベントのパターンの分析

(a) システムの通信トラフィックとイベントのパターンを分析する。

(b) 一般的なトラフィックとイベントのパターンを表すプロファイルを作成する。

(c) システム監視デバイスの調整にトラフィックとイベントのプロファイルを使用する。

詳解：一般的な通信トラフィックとイベントパターンを特定して理解することで、組織がシステム監視デバイスに有用な情報を提供し、疑わしいトラフィックや異常なトラフィックやイベントが発生したときに、それらをより効果的に特定できる。このような情報は、システム監視中の偽陽性や偽陰性の数を減らすのに役立つ。

関連管理策：なし

(14) システム監視 | ワイヤレス侵入検知

ワイヤレス侵入検知システムを使用して、認可されていないワイヤレスデバイスを特定し、システムへのブリーチの試みや潜在的な侵害や違反を検知する。

詳解：ワイヤレス信号は、組織の施設を超えて放射する可能性がある。組織は、認可されていないワイヤレスアクセスポイントを徹底的にスキャンするなど、認可されていないワイヤレス接続を積極的に検索する。ワイヤレススキャンは、システムを含む施設内の領域に限定されず、認可されていないワイヤレスアクセスポイントが組織のシステムに接続されていないことを確認するために施設外の領域も含む。

関連管理策：AC-18, IA-3

(15) システム監視 | ワイヤレスから有線への通信

侵入検知システムを採用して、通信トラフィックがワイヤレスネットワークから有線ネットワークに通過する場合に、ワイヤレス通信トラフィックを監視する。

詳解：ワイヤレスネットワークは本質的に有線ネットワークよりもセキュアではない。例えば、無線ネットワークは、有線ネットワークよりも盗聴者やトラフィック分析の影響を受けやすい。無線から有線への通信が存在する場合、ワイヤレスネットワークは有線ネットワークへの入り口となる可能性がある。システムの物理的境界内からの認可されていない有線ネットワークアクセスと比較して、ワイヤレスアクセスポイントを介した認可されていないネットワークアクセスの容易度が高いため、悪意のある行為を検知するには、ワイヤレスネットワークと有線ネットワーク間の遷移トラフィックの追加監視が必要になる場合がある。侵入検知システムを採用してワイヤレス通信トラフィックを監視すると、有線ネットワークに遷移する前に、トラフィックに悪意のあるコードが含まれていないことを確認できる。

関連管理策：AC-18

(16) システム監視 | 監視情報の関連付け

システム全体で使用される監視ツールおよびメカニズムからの情報を関連付ける。

詳解：異なるシステム監視ツールおよびメカニズムからの情報を関連付けることにより、システム活動のより包括的なビューを提供できる。悪意のあるコード保護ソフトウェア、ホストの監視、ネットワークの監視など、通常は分離して機能するシステム監視ツールとメカニズムを関連付けることで、組織全体の監視ビューが提供でき、他の方法では見られない攻撃パターンを明らかにしても良い。様々な監視ツールとメカニズムの機能と規制、およびそれらのツールとメカニズムによって生成される情報を最大限に活用する方法を理解することは、組織が効果的な監視プログラムを開発、運用、維持するのに役立つ。監視情報の相関関係は、古い技術から新しい技術への移行中（例えば、IPv4 から IPv6 ネットワークプロトコルへの移行中）に特に重要である。

関連管理策：AU-6

(17) システム監視 | 統合された状況認識

統合された組織全体の状況認識を達成するために、物理的活動、サイバー活動、およびサプライチェーン活動の監視からの情報を相互に関連付ける。

詳解：より多様なソースからの監視情報を相互に関連付けることは、統合された状況認識の達成に役立つ。物理的、サイバー、およびサプライチェーン監視活動の組み合わせによる統合された状況認識は、組織が高度な攻撃をより迅速に検知し、そのような攻撃を実行するために採用された方法と技法を調査する能力を強化する。様々なサイバー監視情報を相互に関連付ける SI-4(16)とは対照的に、統合された状況認識は、サイバードメインを超えて監視を関連付けることを目的としている。複数の活動からの監視情報の相関関係は、複数の攻撃ベクトルにわたって運用されている組織への攻撃を明らかにするのに役立てても良い。

関連管理策：AU-16, PE-6, SR-2, SR-4, SR-6

(18) システム監視 | トラフィックおよび秘密の漏出の分析

**システムへの外部インタフェースおよび[*設定：組織が定めるシステム内の内部ポイン*

ト]で、外部との通信トラフィックを分析して、情報の秘密の漏出を検知する。

詳解：組織が定める内部ポイントには、サブネットワークとサブシステムが含まれる。秘密とは、ステガノグラフィーを含む情報の漏出に使用できることを意味する。

関連管理策：なし

(19) システム監視｜個人のリスク

[*設定：組織が定めるソース*]によってリスクレベルが高いと特定された個人の[*設定：組織定めた追加監視*]を実施する。

詳解：個人からのリスク増加の兆候は、人事記録、諜報機関、法執行機関、およびその他のソースを含む様々なソースから得ることができる。個人の監視は、そのような監視を行う管理、法務、セキュリティ、プライバシー、および人事担当者と調整される。監視は、適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに従って実施される。

関連管理策：なし

(20) システム監視｜特権ユーザ

特権ユーザの[*設定：組織定めた追加監視*]を実施する。

詳解：特権ユーザは、一般ユーザよりも、セキュリティ関連情報などのより機微情報にアクセスできる。そのような情報へのアクセスは、特権ユーザが非特権ユーザよりもシステムや組織に大きな損害を与える可能性があることを意味する。したがって、特権ユーザに追加の監視を実施すると、組織が悪意のある行為を出来るだけ早期に特定し、適切な措置を講じることができるようになる。

関連管理策：AC-18

(21) システム監視｜試用期間

[*設定：組織定めた試用期間*]中に、個人の[*設定：組織定めた追加監視*]を実施する。

詳解：試用期間中、従業員は組織内で正社員としての地位を持っていない。このようなステータスや、システムに常駐する情報へのアクセス権がない場合、追加の監視により、悪意のある可能性のある行為や不適切な動作を特定することができる。

関連管理策：AC-18

(22) システム監視｜認可されていないネットワークサービス

(a) **[*設定：組織が定める認可または承認プロセス*]によって認可または承認されていないネットワークサービスを検知する。**

(b) **検知された場合に[*設定：組織が定める職員または役割*]に[*選択(1 つ以上)：監査；アラート*]を行なう。**

詳解：認可されていない、または承認されていないネットワークサービスには、組織の検証や妥当性確認が行われていないサービス指向アーキテクチャのサービスが含まれるため、信頼性がないか、または有効なサービスの悪意のある認可されていない役割として機能する可能性がある。

関連管理策：CM-7

(23) システム監視｜ホストベースのデバイス

[*設定：組織が定めるシステムコンポーネント*]で、[*設定：組織が定めるホストベースの監視メカニズム*]を実装する。

詳解：ホストベースの監視は、ホスト（またはホストが存在するシステム）に関する情報を収集する。ホストベースの監視を実装できるシステムコンポーネントには、サーバ、ノートブックコンピュータ、モバイルデバイスなどがある。組織は、複数の製品開発者またはベンダからのホストベースの監視メカニズムの採用を考慮してもよい。

関連管理策：AC-18, AC-19

(24) システム監視｜侵害の兆候

[*設定：組織が定めるソース*]によって提供される侵害の兆候を検出、収集して[*設定：組織が定める職員または役割*]に配布する。

詳解：侵害の兆候（IOC：Indicators of compromise）は、ホストまたはネットワークレベルで組織のシステムに特定された侵入からのフォレンジックアーティファクトである。IOC は、侵害されたシステムに関する貴重な情報を提供する。IOC には、レジストリキー値の作成を含めることができる。ネットワークトラフィックの IOC には、ユニバーサルリソースロケータ（URL）またはプロトコル要素が含まれ、悪意のあるコードのコマンドおよび制御サーバを示す。IOC の迅速な配布と採用により、システムや組織が同じ悪用や攻撃に対して脆弱である時間を短縮することで、情報セキュリティを向上させることができる。脅威の兆候、署名、戦術、技法、手順、およびその他の侵害の兆候は、インシデント対応およびセキュリティチームのフォーラム、米国コンピュータ緊急対応チーム、防衛産業基盤サイバーセキュリティ情報共有プログラム、CERT 調整センターを含む政府および非政府の協同組合を通じて利用可能である。

関連管理策：AC-18

(25) システム監視｜ネットワークトラフィック分析の最適化

外部および主要な内部システムインタフェースでネットワークトラフィックを可視化して、監視デバイスの効果を最適化する。

詳解：暗号化されたトラフィック、非対称ルーティングアーキテクチャ、容量と遅延の規制、および古い技術から新しい技術への移行（IPv4 から IPv6 へのネットワークプロトコルの移行など）により、ネットワークトラフィックを分析するときに、組織の盲点になる可能性がある。関連するトラフィックのみを収集、復号、前処理、および監視デバイスに配信することで、デバイスの効率と使用を合理化し、トラフィック分析を最適化できる。

関連管理策：なし

参照資料：[OMB A-130], [FIPS 140-3], [SP 800-61], [SP 800-83], [SP 800-92], [SP 800-94], [SP 800-137]

SI-5 セキュリティのアラート、勧告、および指令

管理策：

a. [*設定：組織が定める外部組織*]から継続的にシステムセキュリティのアラート、勧告、および指令を受け取る。

b. 必要に応じて、内部のセキュリティアラート、勧告、および指令を生成する。

c. セキュリティアラート、勧告、および指令を[*選択（1 つ以上）：*[*設定：組織が定める職員または役割*]；[*設定：組織が定める組織内の要素*]；[*設定：組織が定める外部組織*]]に配布する。

d. 確立された時間枠に従ってセキュリティ指令を実装するか、違反の程度を発行機関に通知する。

詳解：サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA: The Cybersecurity and Infrastructure Security Agency）は、連邦政府全体の状況認識を維持するためのセキュリティアラートおよび勧告を生成する。セキュリティ指令は、OMB またはそのような指令を発行する責任と権限を有する他の指定された組織によって発行される。これらの指令の多くは重大な性質を有しており、組織の運営、資産、個人、他の組織、および国家が指令を適時に実施しない場合、国家に潜在的な（即時の）悪影響を与える可能性があるため、セキュリティ指令への遵守は不可欠である。外部組織には、サプライチェーンパートナー、外部のミッションまたは事業のパートナー、外部サービスプロバイダ、および他の同業者または支援組織が含まれる。

関連管理策：PM-15, RA-5, SI-2

拡張管理策：

(1) セキュリティ警告、勧告、および指令｜自動化されたアラートおよび勧告

[*設定：組織が定める自動化されたメカニズム*]を使用して、セキュリティアラートと勧告

情報を組織全体に広める。

詳解：組織のシステムおよび運用環境に多数の変更を加えるには、組織のミッションと事業の機能の成功に直接関心を持つ様々な組織エンティティにセキュリティ関連情報を配布する必要がある。セキュリティアラートとセキュリティ勧告によって提供される情報に基づいて、管理レベル、ミッションと事業プロセスレベル、情報システムレベルなど、リスクマネジメントに関連する 3 つのレベルの 1 つ以上で変更が必要になる場合がある。

関連管理策：なし

参照資料：[SP 800-40]

SI-6 セキュリティおよびプライバシー機能の検証

管理策：

a. [*設定：組織が定めるセキュリティとプライバシーの機能*]の正しい運用を検証する。

b. SI-6a で指定された機能[*選択（1 つ以上）：*[*設定：組織が定めるシステム移行状態*]；*適切な権限を持つユーザの命令により、*[*設定：組織が定める頻度*]]で検証を実行する。

c. セキュリティとプライバシーの検証テストが失敗した場合は、[*設定：組織が定める職員または役割*]にアラートする。

d. 異常が検出された場合、[*選択（1 つ以上）：システムをシャットダウン；システムを再起動；*[*設定：組織が定める代替措置*]]を実施する。

詳解：システムの移行状態には、システムの起動、再起動、シャットダウン、中止を含む。システム通知には、ハードウェア表示ライト、システム管理者への電子的アラート、およびローカルコンピュータコンソールへのメッセージが含まれる。セキュリティ機能の検証とは対照的に、プライバシー機能の検証は、プライバシー機能が期待通りに動作し、政府機関のプライバシー保護責任者により承認済みとなっていること、またはプライバシー属性が期待通りに適用または使用されることを保証する。

関連管理策：CA-7, CM-4, CM-6, SI-7

拡張管理策：

(1) セキュリティおよびプライバシー機能の検証 | 失敗したセキュリティテストの通知

[撤回：SI-6 に組み込まれた]

(2) セキュリティおよびプライバシー機能の検証 | 分散テストの自動サポート

自動化されたメカニズムを実装して、分散セキュリティ機能およびプライバシー機能テストの管理をサポートする。

詳解：分散機能テストの管理をサポートするための自動化されたメカニズムの使用は、そのようなテストの完全性、適時性、正確性、および有効性を保証するのに役立つ。

関連管理策：SI-2

(3) セキュリティおよびプライバシー機能の検証 | 検証結果の報告

セキュリティ機能およびプライバシー機能の検証結果を[*設定：組織が定める職員または役割*]に報告する。

詳解：セキュリティ機能およびプライバシー機能の検証結果に潜在的に関心を持つ組織の職員には、システムセキュリティ担当者、政府機関の情報セキュリティ責任者、および政府機関のプライバシー保護責任者が含まれる。

関連管理策：SI-4, SR-4, SR-5

参照資料：[OMB A-130]

SI-7 ソフトウェア、ファームウェア、および情報の完全性

管理策:

a. 完全性検証ツールを使用して、[*設定:組織が定めるソフトウェア、ファームウェア、および情報*]への認可されていない変更を検知する。

b. ソフトウェア、ファームウェア、および情報への認可されていない変更が検知された場合は、[*設定:組織が定めるアクション*]を実行する。

詳解:ソフトウェア、ファームウェア、および情報への認可されていない変更は、エラーまたは悪意のある行為により発生することが出来る。ソフトウェアには、オペレーティングシステム(カーネルやドライバーなどの主要な内部コンポーネントを含む)、ミドルウェア、およびアプリケーションが含まれる。ファームウェアインタフェースには、UEFI(Unified Extensible Firmware Interface)および BIOS(Basic Input/Output System)が含まれる。情報には、個人情報と、情報に関連するセキュリティおよびプライバシー属性を含むメタデータが含まれる。完全性チェックメカニズム(パリティチェック、巡回冗長検査、暗号ハッシュ、および関連ツールなど)は、システムおよびホストされているアプリケーションの完全性を自動的に監視できる。

関連管理策:AC-4, CM-3, CM-7, CM-8, MA-3, MA-4, RA-5, SA-8, SA-9, SA-10, SC-8, SC-12, SC-13, SC-28, SC-37, SI-3, SR-3, SR-4, SR-5, SR-6, SR-9, SR-10, SR-11

拡張管理策:

(1) ソフトウェア、ファームウェア、および情報の完全性 | 完全性チェック

[*設定:組織が定めるソフトウェア、ファームウェア、および情報*]の完全性チェックを[*選択(1 つ以上):起動時;[設定:組織が定める遷移状態またはセキュリティ関連イベント*];[*設定:組織が定める頻度*]]で実行する。

詳解:セキュリティ関連のイベントには、組織のシステムが影響を受けやすい新しい脅威の特定、および新しいハードウェア、ソフトウェア、またはファームウェアのインストールが含まれる。遷移状態には、システムの起動、再起動、シャットダウン、および中止が含まれる。

関連管理策:なし

(2) ソフトウェア、ファームウェア、および情報の完全性 | 完全性違反の自動通知

完全性検証中に不一致を検出したときに、[*設定:組織が定める職員または役割*]に通知を提供する自動ツールを採用する。

詳解:システムと情報の完全性違反を報告し、タイムリーに組織の職員に通知する自動ツールの採用は、効果的なリスク対応に不可欠である。システムおよび情報の整合性違反に関心のある職員には、ミッションおよび事業オーナー、システムオーナー、政府機関の情報セキュリティ担当者、政府機関のプライバシー保護責任者、システム管理者、ソフトウェア開発者、システムインテグレータ、情報セキュリティ担当者、およびプライバシー担当者が含まれる。

関連管理策:なし

(3) ソフトウェア、ファームウェア、および情報の完全性 | 一元管理された完全性ツール

一元管理された完全性検証ツールを採用する。

詳解:一元管理された完全性検証ツールは、そのようなツールの適用においてより高い一貫性を提供し、完全性検証アクションのより包括的な適用範囲を容易にすることができる。

関連管理策:AU-3, SI-2, SI-8

(4) ソフトウェア、ファームウェア、および情報の完全性 | タンパーエビデントパッケージ

[撤回:SR-9 に組み込まれた]

(5) ソフトウェア、ファームウェア、および情報の完全性 | 完全性違反への自動対応

完全性違反が検出された場合、自動的に[*選択(1 つ以上):システムをシャットダウンする;システムを再起動する;[設定:組織が定める管理策]を実施する*]。

詳解：組織は、情報のタイプ、特定の情報、またはその両方の組み合わせによって、様々な完全性チェック応答を規定することができる。情報のタイプには、ファームウェア、ソフトウェア、およびユーザデータが含まれる。特定の情報には、特定のタイプのマシンのブートファームウェアが含まれる。組織のシステム内の管理策の自動実装には、重要なセキュリティファイルに認可されていない変更が行われた場合に、変更を元に戻す、システムを停止する、または監査アラートのトリガーが含まれる。

関連管理策：なし

(6) ソフトウェア、ファームウェア、および情報の完全性 | 暗号保護

ソフトウェア、ファームウェア、および情報に対する認可されていない変更を検知するための暗号メカニズムを実装する。

詳解：完全性を保護するために使用される暗号化メカニズムには、デジタル署名、非対称暗号を使用した署名付きハッシュの計算と適用、ハッシュの生成に使用される鍵の機密性の保護、および公開鍵を使用したハッシュ情報の検証などがある。暗号メカニズムを採用する組織は、暗号鍵管理ソリューションも考慮する。

関連管理策：SC-12, SC-13

(7) ソフトウェア、ファームウェア、および情報の完全性 | 検知および対応の統合

[*設定：組織が定めるシステムへのセキュリティ関連の変更*]の検知を組織のインシデント対応機能に組み込む。

詳解：検知と対応を統合することで、検知されたイベントを追跡、監視、修正し、履歴目的で利用できるようにすることができる。履歴記録を維持することは、長期間にわたって敵対者の行為を特定および識別できるようにし、および可能な法的措置のために重要である。セキュリティ関連の変更には、確立された構成設定に対する認可されていない変更や、システム権限の認可されていない昇格が含まれる。

関連管理策：AU-2, AU-6, IR-4, IR-5, SI-4

(8) ソフトウェア、ファームウェア、および情報の完全性 | 重要なイベントに対する監査ケイパビリティ

潜在的な完全性違反を検知したら、イベントを監査し、[*選択（1 つ以上）：監査記録を生成する；現在のユーザにアラートする；*[*設定：組織が定める職員または役割*]*にアラートする；*[*設定：組織が定めるその他のアクション*]]を開始するケイパビリティを提供する。

詳解：組織は、ソフトウェアのタイプ、特定のソフトウェア、または完全性違反の可能性がある情報に基づいて、対応措置を選択する。

関連管理策：AU-2, AU-6, AU-12

(9) ソフトウェア、ファームウェア、および情報の完全性 | ブートプロセスの確認

[*設定：組織が定めるシステムコンポーネント*]のブートプロセスの完全性を確認する。

詳解：ブートプロセスの完全性を保証することは、既知の信頼できる状態でシステムコンポーネントを起動するために重要である。完全性検証メカニズムは、ブートプロセス中に信頼できるコードのみが実行されることを保証するレベルを提供する。

関連管理策：SI-6

(10) ソフトウェア、ファームウェア、および情報の完全性 | ブートファームウェアの保護

[*設定：組織が定めるシステムコンポーネント*]のブートファームウェアの完全性を保護するために[*設定：組織が定めるメカニズム*]を実装する。

詳解：ブートファームウェアへの認可されていない変更は、巧妙な標的型攻撃を示している可能性がある。これらのタイプの標的型攻撃は、永続的なサービス拒否または永続的な悪意のあるコードの存在を引き起こす可能性がある。これらの状況は、ファームウェアが破損している場合、または悪意のあるコードがファームウェアに埋め込まれている場合に発生する可能性がある。システムコンポーネントは、システムコンポーネントに変更を適用する前にファームウェアへのすべての更新の完全性と真正性を検証し、認可されてい

ないプロセスがブートファームウェアを変更するのを防ぐことで、組織のシステムのブートファームウェアの完全性を保護できる。

関連管理策：SI-6

(11) ソフトウェア、ファームウェア、および情報の完全性 | 限定された権限を持つ限定環境

［撤回：CM-7(6)に移動した］

(12) ソフトウェア、ファームウェア、および情報の完全性 | 完全性の検証

［*設定：組織が定めるユーザインストールソフトウェア*］の完全性を実行前に検証することを要求する。

詳解：組織は、実行前にユーザがインストールしたソフトウェアの完全性を検証して、認可されていない変更によるエラーを含む悪意のあるコードやプログラムが実行される可能性を減らす。組織は、ソフトウェア開発者およびベンダからの信頼できるチェックサムの可用性を含め、ソフトウェアの完全性を検証するアプローチの実用性を考慮する。

関連管理策：CM-11

(13) ソフトウェア、ファームウェア、および情報の完全性 | 保護された環境でのコード実行

［撤回：CM-7(7)に移動した］

(14) ソフトウェア、ファームウェア、および情報の完全性 | バイナリまたはマシン実行可能コード

［撤回：CM-7(8)に移動した］

(15) ソフトウェア、ファームウェア、および情報の完全性 | コード認証

暗号メカニズムを実装して、インストール前に［*設定：組織が定めるソフトウェアまたはファームウェアコンポーネント*］を認証する。

詳解：暗号認証には、ソフトウェアまたはファームウェアのコンポーネントが、組織によって認識および承認済みの証明書を使用してデジタル署名されていることの検証が含まれる。コード署名は、悪意のあるコードから保護する効果的な方法である。暗号メカニズムを採用する組織は、暗号鍵管理ソリューションも考慮する。

関連管理策：CM-5, SC-12, SC-13

(16) ソフトウェア、ファームウェア、および情報の完全性 | 監視なしのプロセス実行の時間制限

［*設定：組織が定める期間*］を超えてプロセスが監視なしで実行されることを禁止する。

詳解：監視なしでプロセスの実行に時間制限を設けることは、通常または通常の実行期間を決定できるプロセス、および組織がそのような期間を超える状況に適用することを目的としている。監視には、オペレーティングシステムのタイマー、自動対応、およびシステムプロセスの異常が発生した場合の手動による監視と対応が含まれる。

関連管理策：なし

(17) ソフトウェア、ファームウェア、および情報の完全性 | 実行時のアプリケーションの自己保護

実行時のアプリケーションの自己保護のため［*設定：組織が定める管理策*］を実装する。

詳解：ランタイムアプリケーションの自己保護では、ランタイム計装を使用して、実行中のソフトウェアからの情報を利用することにより、ソフトウェアの脆弱性の悪用を検知してブロックする。実行時のエクスプロイト防止は、状況認識なしにネットワーク情報を使用することによってのみ攻撃を検知してブロックできるガードやファイアウォールなどの従来の境界ベースの保護とは異なる。ランタイムアプリケーションの自己保護技術は、ソフトウェアの入力を監視し、攻撃を可能にする可能性のある入力をブロックすることで、ソフトウェアの攻撃に対する脆弱性を軽減することができる。また、不要な変更や改ざんからランタイム環境を保護するのにも役立つ。脅威が検知された場合、ランタイムアプリケーションの自

己保護技術により、悪用を防止し、他のアクション（ユーザへの警告メッセージの送信、ユーザのセッションの終了、アプリケーションの終了、組織の職員へのアラートの送信など）を実行できる。ランタイムアプリケーション自己保護ソリューションは、監視モードまたは保護モードのいずれかで展開できる。

関連管理策：SI-16

参照資料：[OMB A-130], [FIPS 140-3], [FIPS 180-4], [FIPS 186-4], [FIPS 202], [SP 800-70], [SP 800-147]

SI-8 スパム保護

管理策：

a. 迷惑メッセージを検知して対処するために、システムの入口と出口にスパム保護メカニズムを採用する。

b. 組織の構成管理ポリシーおよび手順に従って新しいリリースが利用可能になったときに、スパム保護メカニズムを更新する。

詳解：システムの入口と出口には、ファイアウォール、リモートアクセスサーバ、電子メールサーバ、ウェブサーバ、プロキシサーバ、ワークステーション、ノートブックコンピュータ、モバイルデバイスなどがある。スパムは、電子メール、電子メールの添付ファイル、ウェブアクセスなど、様々な手段で移送される可能性がある。スパム保護メカニズムには、署名の規定が含まれる。

関連管理策：PL-9, SC-5, SC-7, SC-38, SI-3, SI-4

拡張管理策：

(1) スパム保護 | 一元管理

［撤回：PL-9 に組み込まれた］

(2) スパム保護 | 自動更新

スパム保護メカニズムを自動的に［*設定：組織が定める頻度*］で更新する。

詳解：自動化されたメカニズムを使用してスパム保護メカニズムを更新すると、更新が定期的に行われ、最新のコンテンツと保護機能が提供されるようになる。

関連管理策：なし

(3) スパム保護 | 継続的な学習能力

正当な通信トラフィックをより効果的に特定するための学習能力を備えるスパム保護メカニズムを実装する。

詳解：学習メカニズムには、アルゴリズムパラメータを更新することにより特定のトラフィックをスパムまたは正当なものとして識別するユーザ入力に応答するベイジアンフィルタが含まれ、それによりトラフィックのタイプをより的確に分離する。

関連管理策：なし

参照資料：[SP 800-45], [SP 800-177]

SI-9 情報入力の制限

［撤回：AC-2, AC-3, AC-5 および AC-6 に組み込まれた］

SI-10 情報入力の妥当性確認

管理策：［*設定：組織が定める情報システムへの入力*］の有効性を確認する。

詳解：文字セット、長さ、数値範囲、および許容値を含む、システム入力の有効な構文およびセマンティクスをチェックすることで、入力がフォーマットおよびコンテンツの指定された規定と一致することを検証する。例えば、組織が、1～100 の数値が特定のアプリケーションでフィールドに

受け入れられる唯一の入力であると指定している場合、「387」、「abc」、または「%K%」の入力は無効な入力であり、システムへの入力として、受け入れられない 。有効な入力は、ソフトウェアアプリケーション内でフィールドごとに異なる可能性がある。アプリケーションは通常、ソフトウェアモジュールまたはシステムコンポーネント間で通信するために構造化メッセージ（すなわち、コマンドまたはクエリ）を使用する明確に規定されたプロトコルに従う。構造化メッセージには、メタデータまたは制御情報が散在する生データまたは非構造化データを含めることができる。ソフトウェアアプリケーションが攻撃者から提供された入力を使用して、そのようなメッセージを適切にエンコードせずに構造化メッセージを構築する場合、攻撃者は悪意のあるコマンドや特殊文字データを挿入して、データを制御情報またはメタデータとして解釈させる可能性がある。その結果、破損した出力を受信するモジュールまたはコンポーネントは、誤った操作を実行するか、データを誤って解釈する。入力をインタープリターに渡す前に事前スクリーニングすることで、コンテンツが意図せずにコマンドとして解釈されるのを防ぐ。入力の妥当性確認により、的確で正しい入力が保証され、クロスサイトスクリプティングや様々なインジェクション攻撃などの攻撃が防止される。

関連管理策：なし

拡張管理策：

(1) 情報入力の妥当性確認 | 手動オーバーライド機能

(a) [*設定：基本管理策（SI-10）で規定された組織が定める入力*]の入力検証のための手動オーバーライド機能を提供する。

(b) 手動オーバーライド機能の使用を[*設定：組織が定める認可された個人*]のみに制限する。

(c) 手動オーバーライド機能の使用を監査する。

詳解：緊急時対応計画で規定されているイベント中などの特定の状況では、入力検証のための手動オーバーライド機能が必要としても良い。手動オーバーライドは、限定された状況で、組織によって規定された入力でのみ使用される。

関連管理策：AC-3, AU-2, AU-12

(2) 情報入力の妥当性確認 | エラーのレビューおよび解決

[*設定：組織が定める期間*]内の入力妥当性確認エラーをレビューして解決する。

詳解：入力妥当性確認エラーの解決には、エラーの体系的な原因の修正と、修正された入力によるトランザクションの再送信が含まれる。入力妥当性確認エラーは、組織が基本管理策（SI-10）で規定した情報入力に関連するものである。

関連管理策：なし

(3) 情報入力の妥当性確認 | 予測可能な動作

無効な入力が受信されたときに、システムが予測可能かつ文書化された方法で動作することを確認する。

詳解：組織のシステムにおける一般的な脆弱性は、無効な入力を受け取ったときの予測できない動作である。システムの予測可能性の検証は、無効な入力が受信されたときにシステムが期待どおりに動作することを保証するのに役立つ。これは、意図しない影響なくシステムを既知の状態に遷移させるシステム対応を指定することで発生する。無効な入力は、組織が基本管理策（SI-10）で規定した情報入力に関連する入力である。

関連管理策：なし

(4) 情報入力の妥当性確認 | タイミングの相互作用

無効な入力に対する適切な対応を決定する際に、システムコンポーネント間のタイミングの相互作用を明らかにする。

詳解：プロトコルインタフェースを介して受信した無効なシステム入力に対処する際、タイミングの相互作用が重要になり、プロトコルスタック内の他のプロトコルに対するエラー対応のインパクトを考慮する必要がある。例えば、802.11 規格のワイヤレスネットワークプロトコルは、パケットがドロップされたときに TCP（Transmission Control Protocol）と適切に相互

作用しません（無効なパケット入力が原因である可能性がある）。TCP は、パケットの損失は輻輳が原因であると想定していますが、802.11 リンクで失われたパケットは、通常、リンク上のノイズや衝突が原因でドロップされる。TCP が輻輳対応を行うと、衝突イベントに対して TCP が誤ったアクションを実行する。敵対者は、無効な入力の適切な構成を通じて悪影響を達成するために、プロトコルの許容可能な個々の動作と思われるものを協調して使用することができる。無効な入力は、組織が基本管理策（SI-10）で規定した情報入力に関連する入力である。

関連管理策：なし

(5) 情報入力の妥当性確認 | 信頼できるソースおよび承認済みの形式への入力の制限

情報入力の使用を、[*設定：組織が定める信頼できるソース*]および／または[*設定：組織が定める形式*]に制限する。

詳解：入力の使用を信頼できるソースと形式で制限することは、認可されたまたは許可されたソフトウェアの概念が情報入力に適用される。情報入力のための既知の信頼できるソースと、そのような入力に受け入れ可能なフォーマットを指定することで、悪意のある行為の可能性を減らすことができる。情報入力は、組織が基本管理策（SI-10）で規定したものである。

関連管理策：AC-3, AC-6

(6) 情報入力の妥当性確認 | 注入防止

信頼できないデータ注入を防止する。

詳解：信頼できないデータ注入は、パラメータ化されたインタフェースまたは出力エスケープ（出力エンコーディング）を使用することで防止できる。パラメータ化されたインタフェースは、コードからデータを分離するため、悪意のあるデータや意図しないデータの挿入によって、送信されるコマンドのセマンティクスを変更することはできない。出力エスケープでは、指定された文字を使用して、データが信頼できるかどうかをインタープリターのパーサーに通知する。信頼できないデータ注入の防止は、組織が基本管理策（SI-10）で規定した情報入力に関するものである。

関連管理策：AC-3, AC-6

参照資料：[OMB A-130]

SI-11 エラー処理

管理策：

a. 悪用される可能性のある情報を明らかにすることなく、是正措置に必要な情報を提供するエラーメッセージを生成する。

b. エラーメッセージは、[*設定：組織で定める職員または役割*]にのみ開示する。

詳解：組織は、エラーメッセージの構造と内容を考慮する。システムがエラー状態を処理できる範囲は、組織のポリシーおよび運用要件によって導かれ、通知される。悪用可能な情報には、スタックトレースと実装の詳細が含まれる；ユーザ名として誤って入力されたパスワードを使用した誤ったログオン試行；明確に述べられていない場合は、記録された情報から導き出せるミッションや事業の情報；口座番号、社会保障番号、クレジットカード番号などの個人情報。エラーメッセージは、情報を伝送するための隠れチャネルを提供することもある。

関連管理策：AU-2, AU-3, SC-31, SI-2, SI-15

拡張管理策：なし

参照資料：なし

SI-12 情報管理および保持

管理策：適用される法律、大統領令、指令、規則、ポリシー、基準、ガイドラインおよび運用要件に従って、システム内の情報およびシステムから出力された情報を管理および保持する。

詳解：情報の管理と保持の要件は、情報のライフサイクル全体をカバーし、場合によってはシステムの廃棄後も保持する場合がある。保持される情報には、ポリシー、手順、計画、レポート、実装された管理策からのデータ出力、およびその他のタイプの管理情報も含まれる。国立公文書記録管理局（NARA：the National Archives and Records Administration）は、連邦政府のポリシーと記録の保持とスケジュールに関するガイダンスを提供している。組織に記録管理事務所がある場合は、記録管理担当者との調整を考慮する。管理および保持を必要とする可能性のある実装された管理策の出力から作成された記録には、以下が含まれるが、これらに限定されない：すべての XX-1 管理策, AC-6(9), AT-4, AU-12, CA-2, CA-3, CA-5, CA-6, CA-7, CA-8, CA-9, CM-2, CM-3, CM-4, CM-6, CM-8, CM-9, CM-12, CM-13, CP-2, IR-6, IR-8, MA-2, MA-4, PE-2, PE-8, PE-16, PE-17, PL-2, PL-4, PL-7, PL-8, PM-5, PM-8, PM-9, PM-18, PM-21, PM-27, PM-28, PM-30, PM-31, PS-2, PS-6, PS-7, PT-2, PT-3, PT-7, RA-2, RA-3, RA-5, RA-8, SA-4, SA-5, SA-8, SA-10, SI-4, SR-2, SR-4, SR-8。

関連管理策：すべての XX-1 管理策, AC-16, AU-5, AU-11, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9, CM-5, CM-9, CP-2, IR-8, MP-2, MP-3, MP-4, MP-6, PL-2, PL-4, PM-4, PM-8, PM-9, PS-2, PS-6, PT-2, PT-3, RA-2, RA-3, SA-5, SA-8, SR-2

拡張管理策：

(1) 情報管理および保持 | 個人情報要素の限定

情報ライフサイクルで処理される個人情報を、個人情報の［*設定：組織が定める個人情報の要素*］に限定する。

詳解：運用目的で情報が不要な場合、情報ライフサイクル全体を通じて個人情報の使用を限定することで、システムによって作成されるプライバシーリスクのレベルを下げることができる。情報ライフサイクルには、情報の作成、収集、使用、取扱い、保管、保守、配布、開示、および廃棄が含まれる。リスクアセスメントならびに適用される法律、規則、およびポリシーは、個人情報のどの要素がリスクを作成する可能性があるかを判断するための有用な情報を提供することができる。

関連管理策：PM-25

(2) 情報の管理および保持 | テスト、トレーニング、および調査における個人情報の最小化

調査、テスト、またはトレーニングにおける個人情報の使用を最小化するために、［*設定：組織が定める技法*］を使用する。

詳解：組織は、匿名化や合成データなどの技法を採用することで、個人のプライバシーに対するリスクを最小化することができる。情報が調査、テスト、またはトレーニングに必要でない場合に、情報ライフサイクル全体を通じて個人情報の使用を限定することで、システムによって作成されるプライバシーリスクのレベルを下げることができる。リスクアセスメントならびに適用される法律、規則、およびポリシーは、使用する技法とそれらをいつ使用するかを決定するための有用な情報を提供することができる。

関連管理策：PM-22, PM-25, SI-19

(3) 情報の管理および保持 | 情報の廃棄

保持期間後の情報の処分、破壊、または消去には、［*設定：組織が定める技法*］を使用する。

詳解：組織は、不要になった情報を破棄することで、セキュリティとプライバシーの両方のリスクを最小限に抑えることができる。情報の廃棄または破棄は、個人情報を含む可能性のあるシステムロギングを含む、オリジナルおよびコピーとアーカイブされた記録に適用される。

関連管理策：なし

参照資料：[USC 2901], [OMB A-130]

SI-13 予測可能な障害の防止

管理策:

a. 特定の運用環境における[*設定:組織が定めるシステムコンポーネント*]の平均故障時間(MTTF:mean time to failure)を決定する。

b. 代替システムコンポーネントと、[*設定:組織が定めるMTTF代替基準*]に従ってアクティブコンポーネントとスタンバイコンポーネントを交換する手段を提供する。

詳解:MTTF は主に信頼性の問題であるが、予測可能な障害防止は、セキュリティ機能を提供するシステムコンポーネントの潜在的な障害に対処することを目的としている。故障率は、業界平均ではなく、設備固有の考慮事項を反映している。組織は、コンポーネントの障害による潜在的な損害を考慮して、MTTF 値に基づいて、システムコンポーネントの交換の基準を規定する。アクティブコンポーネントとスタンバイコンポーネント間の責任の移行によって、安全性、運用準備、またはセキュリティ機能が侵害することはない。システム状態変数の保存は、転送プロセスを確実に成功させるためにも重要である。スタンバイコンポーネントは、メンテナンスの問題や進行中の復旧の失敗を除いて、いつでも使用できる。

関連管理策:CP-2, CP-10, CP-13, MA-2, MA-6, SA-8, SC-6

拡張管理策:

(1) 予測可能な障害の防止 | コンポーネントの責任の移管

平均故障時間[*設定:組織が定める割合またはパーセンテージ*]までにコンポーネントの責任を、代替コンポーネントに移管することにより、システムコンポーネントのサービスを停止する。

詳解:プライマリシステムコンポーネントの障害が発生する前に、プライマリシステムコンポーネントの責任を他の代替コンポーネントに移管することは、ミッションや事業の機能の機能低下や機能低下のリスクを軽減するために重要である。平均故障時間のパーセンテージに基づいてこのような移管を行うことで、組織はリスク許容度に基づいて事前対応することができる。しかしながら、システムコンポーネントの時期尚早な交換は、システム運用のコストの増加をもたらすことができる。

関連管理策:なし

(2) 予測可能な障害の防止 | 監視なしのプロセス実行の時間制限

[撤回:SI-7(16)に組み込まれた]

(3) 予測可能な障害の防止 | コンポーネント間の手動転送

アクティブコンポーネントの使用が平均故障時間[*設定:組織が定めるパーセンテージ*]に達したら、アクティブおよびスタンバイシステムコンポーネント間の転送を手動で開始する。

詳解:例えば、システムコンポーネントの MTTF が 100 日で、組織によって規定された MTTF パーセンテージが 90%である場合、手動転送は 90 日後に発生する。

関連管理策:なし

(4) 予測可能な障害の防止 | スタンバイコンポーネントのインストールおよび通知

システムコンポーネントの障害が検知された場合:

(a) スタンバイコンポーネントが、[*設定:組織が定める期間*]内に正常かつ透過的にインストールされていることを確認する。

(b) [*選択(1 つ以上):[設定:組織が定めるアラーム]を活性化する;システムを自動的にシャットダウンする;[設定:組織が定めるアクション]*]を実装する。

詳解:コンポーネントの障害が検知されると、コンポーネントがスタンバイモードからアクティブモードに自動または手動で移行する場合がある。

関連管理策:なし

(5) 予測可能な障害の防止 | フェイルオーバー機能

システムに[*選択:リアルタイム;ほぼリアルタイム*]で[*設定:組織が定めるフェイルオーバー機能*]を実装する。

詳解:フェイルオーバーとは、プライマリシステムに障害が発生したときに、代替システムに自動的に切り替えることを意味する。フェイルオーバー機能には、代替処理サイトでのミラーリングされたシステム操作の組み込みや、組織の復旧期間で規定された定期的な間隔での定期的なデータミラーリングが含まれる。

関連管理策:CP-6, CP-7, CP-9

参照資料:なし

SI-14 非永続性

管理策:既知の状態で開始され、[*選択(1 つ以上):使用セッションの終了時;定期的に*[*設定:組織が定める頻度*]]で終了する、非永続の[*設定:組織が定めるシステムコンポーネントとサービス*]を実装する。

詳解:非永続的なコンポーネントおよびサービスの実装は、攻撃を開始および完了するための敵対者の標的化能力(すなわち、機会と利用可能な攻撃面)を減らすことにより、持続的標的型攻撃(APT 攻撃)からのリスクを軽減する。組織は、選択したシステムコンポーネントに非永続性の概念を実装することで、信頼できる既知の状態のコンピューティングリソースを、組織のシステムまたは運用環境の脆弱性を悪用するに十分な時間を敵対者に与えない特定の期間提供することができる。APT 攻撃は機能、意図、および標的化に関してハイエンドの高度な脅威であるため、組織は長期間にわたって攻撃の一部が成功すると想定している。非永続的なシステムコンポーネントおよびサービスは、保護された情報を使用して必要に応じて活性化され、定期的またはセッションの終了時に終了する。非永続性は、組織のシステムを侵害したりブリーチしたりしようとする敵対者の作業要因を増大させる。

非永続性は、システムコンポーネントを更新するか、コンポーネントを定期的に再イメージングするか、または様々な一般的な仮想化技法を使用することで実現できる。非永続的なサービスは、仮想マシンの一部として、または物理マシン上のプロセスの新しい事例(永続的または非永続的)として仮想化技法を使用することで実装できる。システムのコンポーネントとサービスを定期的に更新することの利点は、コンポーネントまたはサービスの侵害が発生しているかどうかを組織が最初に判断する必要がないことである(多くの場合、判断が困難な場合がある)。選択されたシステムコンポーネントおよびサービスの更新は、攻撃の拡散または意図されたインパクトを防ぐのに十分な頻度で行われるが、システムを不安定にするような頻度では行われない。重要なコンポーネントとサービスの更新は、敵対者が脆弱性の最適なウィンドウを悪用する能力を妨げるために、定期的に行われても良い。

関連管理策:SC-30, SC-34, SI-21

拡張管理策:

(1) 非永続性 | 信頼できるソースからのリフレッシュ

システムコンポーネントおよびサービスのリフレッシュ時に使用されるソフトウェアとデータを、[*設定:組織が定める信頼できるソース*]から取得する。

詳解:信頼できるソースには、追記型、読み取り専用媒体、または選択したオフラインのセキュアなストレージ設備からのソフトウェアとデータが含まれる。

関連管理策:なし

(2) 非永続性 | 非永続的情報

(a) [*選択:[設定:組織が定める情報]を[設定:組織が定める頻度]で更新する;[設定:組織が定める情報]をオンデマンドで生成する*]。

(b) **不要になった情報を削除する。**

詳解:情報を必要以上に長く保持することは、認可されていない開示、認可されていない変更、または漏出によって侵害するために、価値の高い資産を探す高度な敵対者の潜在的な標的となる。システム関連情報の場合、不必要な保持は、システムを介した偵察およ

び横移動を支援することができる高度な敵対者情報を提供する。

関連管理策：なし

(3) 非永続性 | 非永続的接続性

オンデマンドでシステムへの接続を確立し、[*選択：要求の完了後；不使用期間*]の後、接続を終了する。

詳解：システムへの永続的な接続は、高度な敵対者にシステム内を横方向に移動する経路を提供し、潜在的に高価値の資産の近くに位置することができる。このような接続の可用性を限定すると、組織のシステムを自由に移動する敵対者の能力が妨げられる。

関連管理策：SC-10

参照資料：なし

SI-15 情報出力フィルタリング

管理策：[*設定：組織が定めるソフトウェアプログラムおよび／またはアプリケーション*]から出力された情報を検証し、情報が期待される内容と一致していることを確認する。

詳解：SQL インジェクションを含む特定のタイプの攻撃は、予期しない出力結果を生成するか、ソフトウェアプログラムまたはアプリケーションから予期される出力結果と一致しない出力結果を生成する。情報出力フィルタリングは、無関係なコンテンツを検知し、そのような無関係なコンテンツが表示されないようにし、異常な動作が検出されたことを監視ツールにアラートすることに焦点を当てている。

関連管理策：SI-3, SI-4, SI-11

拡張管理策：なし

参照資料：なし

SI-16 メモリ保護

管理策：システムメモリを認可されていないコードの実行から保護するために、[*設定：組織が定める管理策*]を実施する。

詳解：一部の敵対者は、メモリの非実行可能領域または禁止されているメモリ領域でコードを実行する目的で攻撃を仕掛ける。メモリを保護するために使用される管理策には、データ実行防止およびアドレス空間配置のランダム化が含まれる。データ実行防止管理策は、ハードウェアによるものでも、ハードウェアによるメカニズムでより強化されたソフトウェアによるものでもかまわない。

関連管理策：AC-25, SC-3, SI-7

拡張管理策：なし

参照資料：なし

SI-17 フェイルセーフ手順

管理策：指示された障害が発生したときに、[*設定：組織が定める障害条件と関連するフェイルセーフ手順のリスト*]を実施する。

詳解：障害状態には、重要なシステムコンポーネント間、またはシステムコンポーネントと運用施設間の通信の喪失が含まれる。フェイルセーフ手順には、オペレータの職員へのアラート、および実行する後続の手順に関する具体的な指示の提供が含まれる。後続の手順には、何もしない、システム設定を再確立する、プロセスをシャットダウンする、システムを再起動する、または指定された組織の担当者に連絡することが含まれても良い。

関連管理策：CP-12, CP-13, SC-24, SI-13

拡張管理策：なし

参照資料：なし

SI-18 個人情報の品質運用

管理策：

a. [*設定：組織が定める頻度*]で情報ライフサイクル全体にわたって、個人情報の正確性、関連性、適時性、完全性を確認する。

b. 不正確または古い個人情報を修正または削除する。

詳解：個人情報品質運用には、情報ライフサイクル全体にわたって、組織が個人情報の正確性と関連性を確認するために行う手順が含まれる。情報ライフサイクルには、個人情報の作成、収集、使用、取扱い、保管、保守、配布、開示、および廃棄が含まれる。個人情報品質運用には、自動住所検証検索アプリケーションインタフェースを使用してシステムに収集または入力された住所の編集および検証が含まれる。個人情報の品質をチェックすることには、データの更新または変更を長期にわたって追跡することが含まれる。これにより、組織は、誤った情報を特定する必要がある場合にどのようにして、どのような個人情報が変更されたかを知ることができる。個人情報の品質を保護するために講じられる措置は、個人情報の性質と状況、その使用方法、取得方法、採用されている可能性のある匿名化方法に基づいている。連邦政府のプログラムの対象となる個人の権利、利益、または権限について判断するために使用される個人情報の正確性を検証するために講じられる措置は、機微性の低い目的で使用される個人情報を検証するために使用される措置よりも包括的である場合がある。

関連管理策：PM-22, PM-24, PT-2, SI-4

拡張管理策：

(1) 個人情報の品質運用 | 自動サポート

不正確または古い、インパクトに関して誤って決定された、または誤って匿名化された個人情報を[*設定：組織が定める自動化されたメカニズム*]を使用して修正または削除する。

詳解：データの品質を向上させるために自動化されたメカニズムを使用すると、プライバシーリスクが作成される可能性がある。自動化ツールは、外部のシステムまたは関連のないシステムに接続する場合があり、これらのシステム間の記録の一致により、意図しない結果を伴うリンクが作成される場合がある。組織は、プライバシー影響評価する際にこれらのリスクを評価して文書化し、プライバシープログラム計画に沿った判断を下す。

データが取得され、情報ライフサイクル全体で使用されるため、個人情報の正確性と関連性を確認することが重要である。自動化されたメカニズムは、既存のデータ品質プロセスおよび手順を補強し、組織が大規模システム内の個人情報をより適切に識別および管理できるようにする。例えば、自動化ツールは、データを常に正規化したり、認可されていない形式のデータを特定したりする作業を大幅に改善することができる。自動化ツールを使用して、データの監査を改善し、個人情報を誤って変更したり、そのような情報を間違った個人に誤って関連付けたりする可能性のあるエラーを検知することもできる。自動化された機能は、プロセスと手順を大規模に補強し、データ品質エラーのより細かい検知と修正を可能にする。

関連管理策：PM-18, RA-8

(2) 個人情報の品質運用 | データタグ

データタグを使用して、組織のシステム内の情報ライフサイクル全体にわたって、個人情報の修正または削除を自動化する。

詳解：個人情報へのデータのタグ付けには、取扱いの許可、取扱う権限、匿名化、インパクトレベル、情報ライフサイクルの段階、保持または最終更新日を記載したタグが含まれる。個人情報にデータタグを使用すると、自動化ツールを使用して、関連する個人情報を修正または削除できる。

関連管理策：AC-3, AC-16, SC-16

(3) 個人情報の品質運用｜収集

個人情報を個人から直接収集する。

詳解：個人または指定された代表者は、正確な個人情報のソースとなり得る。組織は、個人が、正しいデータと誤ったデータを提供することを促す状況要因を考慮する。収集された情報を、個人情報の性質と状況、その使用方法、および入手方法に基づいて検証するには、追加の手順が必要になる場合がある。連邦政府プログラムの下で個人の権利、利益、または権限について判断するために使用される個人情報の正確性を検証するために講じられる措置は、機微性の低い個人情報を検証するために講じられる措置よりも包括的であっても良い。

関連管理策：なし

(4) 個人情報の品質運用｜個人の要求

個人または指定された代理人の要求に応じて、個人情報を修正または削除する。

詳解：組織が保持する不正確な個人情報は、特に不正確な情報が不適切な決定や個人への利益提供やサービスの拒否 につながる可能性がある事業の機能において、個人に問題を引き起こす可能性がある。正しい情報でさえ、特定の状況では、情報を維持する組織の利益を上回る問題を個人に引き起こす可能性がある。組織は、要求の範囲、求められる変更、変更のインパクト、ならびに法律、規則、およびポリシーに基づいて、個人情報を修正または削除するかどうかを決定する際に適切な処置を取る。組織の職員は、訂正または削除の適切な事例に関して政府機関のプライバシー保護責任者および法務顧問に相談する。

関連管理策：なし

(5) 個人情報の品質操作｜修正または削除の通知

[*設定：組織が定める個人情報の受信者*]および個人に、個人情報が修正または削除されたことを通知する。

詳解：個人情報が修正または削除された場合、組織は、そのような情報の認可されたすべての受信者、および情報が関連付けられている個人または指定された代表者に、修正または削除された情報が確実に通知されるようにするための措置を講じる。

関連管理策：なし

参照資料：[OMB M-19-15], [SP 800-188], [IR 8112]

SI-19 匿名化

管理策：

a. データセットから個人情報の[*設定：組織が定める個人情報の要素*]を削除する。

b. 匿名化の有効性について、[*設定：組織が定める頻度*]で評価する。

詳解：匿名化は、一連の識別データとデータ主体との関連を削除するプロセスの総称である。多くのデータセットには、名前、社会保障番号、生年月日と出生地、母親の旧姓、生体認証記録など、個人のアイデンティティを区別または追跡するために使用できる個人に関する情報が含まれている。データセットには、医療情報、教育情報、財務情報、雇用情報など、個人にリンクされた、またはリンク可能な他の情報も含まれる場合がある。個人情報は、そのような情報がデータに想定された要件を満たすために必要ない（または、もはや必要ない）場合、訓練された個人によってデータセットから削除される。例えば、データセットが集計統計の生成にのみ使用される場合、それらの統計の生成に必要のない識別子は削除される。識別子を削除すると、削除された情報が誤って開示されたり、不適切に使用されたりすることがないため、プライバシー保護が向上する。組織は、適用される法律、規則、またはポリシーに基づく特定の匿名化の規定または方法の対象となる場合がある。再識別は、匿名化されたデータの残存リスクである。再識別攻撃は、新しいデータセットの結合やデータ分析におけるその他の改善など、様々な場合がある。潜在的な攻撃の認識を維持し、長期間にわたって匿名化の有効性を評価する

ことで、この残存リスクの管理をサポートする。

関連管理策：MP-6, PM-22, PM-23, PM-24, RA-2, SI-12

拡張管理策：

(1) 匿名化 | 収集

個人情報を収集しないことにより、収集時にデータセットを匿名化する。

詳解：データソースに個人情報が含まれているが、その情報が使用されない場合、データを作成するときに、個人情報を含むデータ要素を収集しないことにより、データを匿名化することができる。例えば、組織が申請者の社会保障番号を使用する予定がない場合、申請書は社会保障番号を要求しない。

関連管理策：なし

(2) 匿名化 | アーカイブ

データセットのアーカイブ後にデータセット内のそれらの要素が不要になる場合は、個人情報要素のアーカイブを禁止する。

詳解：データセットは、様々な理由でアーカイブされる。アーカイブされたデータセットの想定される目的が指定されており、個人情報要素が必要でない場合、その要素はアーカイブされない。例えば、社会保障番号はレコードのリンクのために収集されている場合があるが、アーカイブされたデータセットには、リンクされたレコードの必要な要素が含まれている場合がある。この場合、社会保障番号をアーカイブする必要はない。

関連管理策：なし

(3) 匿名化 | リリース

リリースデータセット内のそれらの要素がデータリリースの一部である必要がない場合は、リリース前にデータセットから個人情報要素を削除する。

詳解：データ管理者は、データセットを公開する前に、データセットの使用目的を考慮し、個人情報を公開する必要があるかどうかを判断する。個人情報が必要ない場合は、匿名化技法を使用して情報を削除できる。

関連管理策：なし

(4) 匿名化 | 直接識別子の削除、マスク、暗号化、ハッシュ化、または置換

データセット内の直接識別子を削除、マスク、暗号化、ハッシュ化、または置換する。

詳解：データセットから直接識別子を削除するには、多くの可能なプロセスがある。直接識別子を含むデータセットの列は削除できる。マスキングでは、直接の識別子が XXXXXX や 999999 などの繰り返し文字に変換される。識別子は、リンクされたレコードがリンクされたままになるように暗号化またはハッシュ化できる。暗号化またはハッシュ化の場合、高度暗号化規格またはハッシュベースのメッセージ認証コードを含む、鍵の使用を必要とするアルゴリズムが採用される。実装では、すべての識別子に同じキーを使用することも、各識別子に異なるキーを使用することもできる。各識別子に異なるキーを使用することで、より高度なセキュリティとプライバシーが提供される。あるいは、「GeorgeWashington」を「PATIENT」に変換することや、「GeorgeWashington」を「AbrahamPolk」に変換することなど、代理値に置き換えることなど、識別子をキーワードに置き換えることもできる。

関連管理策：SC-12, SC-13

(5) 匿名化 | 統計的開示管理

分析結果で個人や組織を特定できないように、数値データ、分割表、統計的所見を操作する。

詳解：多くのタイプの統計分析では、要約情報しか提供されていない場合でも、個人に関する情報が開示される可能性がある。例えば、少数派の学生の数が登録された月次テーブルを公開している学校が、1 月にそのような学生が 10～19 人いると報告し、続いて 3 月にそのような学生が 20～29 人いると報告した場合、2 月に入学した学生は少数派だったと推論することができる。

関連管理策：なし

(6) 匿名化 | ディファレンシャルプライバシー

結果が報告される前に、数学的演算の結果に非決定論的ノイズを追加することにより、個人情報の開示を防止する。

詳解：ディファレンシャルプライバシーに関する数学的定義では、データセット分析の結果は、単一のデータレコード（単一の個人からのデータであると想定される）の追加または削除の前後でほぼ同じであることが望ましい。最も基本的な形式では、ディファレンシャルプライバシーはオンラインクエリシステムにのみ適用される。ただし、機械学習の統計的分類子や合成データの生成にも使用できる。ディファレンシャルプライバシーは、結果の精度が低下し、組織はプライバシー保護と、匿名化されたデータセットの全体的な正確さ、有用性、および有用性との間のトレードオフを定量化することを余儀なくされる。非決定論的ノイズには、データセット分析の数学演算の結果に小さなランダムな値を追加することが含まれる。

関連管理策：SC-12, SC-13

(7) 匿名化 | 妥当性確認済みのアルゴリズムおよびソフトウェア

妥当性確認済みのアルゴリズムと、アルゴリズムを実装するために妥当性確認済みのソフトウェアを使用して、匿名化を実行する。

詳解：個人情報をデータセットから削除するように見えるアルゴリズムは、実際には個人情報または再特定可能なデータを残す可能性がある。妥当性確認済みのアルゴリズムを実装すると言われているソフトウェアには、バグが含まれている場合や、別のアルゴリズムが実装されている場合がある。ソフトウェアは、整数などのあるタイプのデータを匿名化することができるが、浮動小数点数などの別のタイプのデータを匿名化することはできない。これらの理由により、匿名化は、妥当性確認済みのアルゴリズムとソフトウェアを使用して実行される。

関連管理策：なし

(8) 匿名化 | 動機付けされた侵入者

匿名化されたデータセットに対して動機付けされた侵入者テストを実行して、識別されたデータが残っているかどうか、または匿名化されたデータを再識別できるかどうかを判断する。

詳解：動機付けされた侵入者テストは、個人またはグループがデータリリースと指定されたリソースを取得し、匿名化されたデータセット内の 1 人以上の個人を再識別しようとするテストである。このようなテストでは、侵入者がテストを実施するために保有する内部知識、計算リソース、財務リソース、データ、およびスキルの量を指定する。動機付けされた侵入者テストでは、匿名化が不十分かどうかを判断できる。また、匿名化が十分かどうかを評価するための有用な診断ツールにもなる。ただし、テストだけでは、匿名化が十分であることを証明することはできない。

関連管理策：なし

参照資料：[OMB A-130], [SP 800-188]

SI-20 汚染

管理策：[*設定：組織が定めるシステムまたはシステムコンポーネント*]にデータまたは機能を埋め込んで、組織のデータが漏出したか、または組織から不適切に削除されたかどうかを判断する。

詳解：多くのサイバー攻撃は、組織の情報、または組織が他のエンティティに代わって保持している情報（個人情報など）を標的として、そのデータを漏出する。さらに、インサイダー攻撃や誤ったユーザ手順により、組織のポリシーに違反する情報がシステムから削除される可能性がある。汚染アプローチは、受動的から能動的までさまざまである。受動的な汚染方法は、内部のデータベースに偽の電子メール名とアドレスを追加するだけの簡単なものである。組織が偽のメールアドレスのいずれかでメールを受信した場合、データベースが侵害されていることがわか

る。さらに、組織は、電子メールが認可されていないエンティティによって送信されたため、悪意のあるコードが含まれている可能性のあるパケットや、認可されていないエンティティがデータベースのコピーを取得した可能性があることを知っている。別の汚染アプローチには、オープンソース分析を介してデータを見つけることができるように、偽データまたはステガノグラフィックデータをファイルに埋め込むことが含まれる。最後に、アクティブな汚染アプローチには、「コールホーム」を実行できるソフトウェアをデータに埋め込むことを含めることができ、それによって、組織にその「キャプチャ」と、場合によってはその場所、および漏出または削除された経路をアラートする。

関連管理策：AU-13

拡張管理策：なし

参照資料：[OMB A-130], [SP 800-160-2]

SI-21 情報の更新

管理策：[*設定：組織が定める頻度*]で[*設定：組織が定める情報*]を更新するか、必要に応じて情報を生成し、不要になった情報を削除する。

詳解：必要以上に情報を保持することは、敵対者にとってますます価値のある魅力的な標的になる。組織のミッションや事業の機能をサポートするために必要な最小限の期間にわたって情報を利用できるようにしておくことで、敵対者がその情報を侵害したり、キャプチャしたり、データを漏出したりする機会を減らすことができる。

関連管理策：SI-14

拡張管理策：なし

参照資料：[OMB A-130], [SP 800-160-2]

SI-22 情報の多様性

管理策：

a. [*設定：組織が定める必須機能およびサービス*]に関する[*設定：組織が定める代替ソース*]を特定する。

b. 主要なソースが破損しているか利用できない場合、[*設定：組織が定めるシステムまたはシステムコンポーネント*]で重要な機能またはサービスを実行するために、代替ソースを使用する。

詳解：システムサービスまたは機能によって実行される活動は、多くの場合、受信する情報によって駆動される。その情報の破損、改ざん、変更、または削除は、サービス機能が意図された活動を適切に実行する能力にインパクトを与える可能性がある。複数の入力ソースを持つことにより、サービスまたは機能は、1 つのソースが破損しているか、使用できなくなった場合でも動作を継続できる。代替ソースは、主要なソースよりも的確性が低いかまたは的確性が低い可能性がある。しかし、そのような次善のソースを有することは、劣化または衰弱した方法でさえ、本質的なサービスまたは機能を実行することができる十分なレベルの品質を依然として提供できる可能性がある。

関連管理策：なし

拡張管理策：なし

参照資料：[SP 800-160-2]

SI-23 情報の断片化

管理策：[*設定：組織が定める状況*]に基づき、

a. [*設定：組織が定める情報*]を断片化する。

b. 断片化された情報を、[*設定：組織が定めるシステムまたはシステムコンポーネント*]に配布する。

詳解：持続的標的型攻撃目的の 1 つは、貴重な情報を漏出することである。いったん漏出されると、組織が失われた情報を復旧する方法は一般にない。したがって、組織は、情報を異なる要素に分割し、それらの要素を複数のシステムまたはシステムのコンポーネントと場所に分散させることを考慮してもよい。そのような行動は、所望の情報をキャプチャし、漏出させるための敵対者の作業要因を増加させ、そうすることで、検知の確率を増加させる。情報の断片化は、組織がタイムリーに情報にアクセスする能力にインパクトを与える。断片化の程度は、情報のインパクトまたは分類レベル（および値）、受信した脅威に関する情報収集と分析技術の情報、およびデータ汚染が使用されているかどうかによって決まる（つまり、データの汚染 － 一部の情報の漏出に関する派生情報は、残りの情報の断片化につながる可能性がある）。

関連管理策：なし

拡張管理策：なし

参照資料：[SP 800-160-2]

3.20 サプライチェーンのリスクマネジメント

サプライチェーンのリスクマネジメントの要約表へのクイックリンク

SR-1 ポリシーおよび手順

管理策:

a. 策定、文書化し、[*設定:組織が定める職員または役割*]に配布する。

1. 以下の[*選択(1 つ以上):組織レベル;ミッション/事業プロセスレベル;システムレベル*]のサプライチェーンのリスクマネジメントのポリシー。

(a) 目的、範囲、役割、責任、管理責任、組織のエンティティ間の調整、および準拠に対処する。

(b) 適用される法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインに適合している。

2. サプライチェーンのリスクマネジメントのポリシーと関連するサプライチェーンのリスクマネジメントの管理策の実装を促進するための手順。

b. サプライチェーンのリスクマネジメントのポリシーと手順の策定、文書化、および配布することを管理するために、[*設定:組織が定める担当者*]を指定する。

c. 現行のサプライチェーンのリスクマネジメントをレビューし、更新する。

1. ポリシーについて[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

2. 手順について[*設定:組織が定める頻度*]および[*設定:組織が定めるイベント*]を契機として。

詳解:サプライチェーンのリスクマネジメントのポリシーと手順は、システムおよび組織で実装される SR ファミリーの管理策に対応する。リスクマネジメント戦略は、そのようなポリシーと手順を確立する上で重要な要素である。ポリシーと手順は、セキュリティおよびプライバシーの保証に寄与する。したがって、セキュリティおよびプライバシープログラムがサプライチェーンのリスクマネジメントのポリシーと手順の策定と連携していることが重要である。セキュリティおよびプライバシープログラムのポリシーと手順を組織レベルで確立することは望ましく、一般的には、ミッションまたはシステム固有のポリシーと手順を不要にすることができる。ポリシーは、一般的なセキュリティおよびプライバシーポリシーの一部に含めることも、組織の複雑な性質を反映する複数のポリシーとして表すこともできる。手順は、必要に応じて、セキュリティおよびプライバシープログラム、ミッションまたは事業プロセス、およびシステムに対して規定することができる。手順は、ポリシーまたは管理策がどのように実装されるかを記述し、手順の対象である個人または役割向けとすることができる。手順は、システムのセキュリティおよびプライバシー計画の中に、または 1 つ以上の別の文書に文書化することもできる。サプライチェーンのリスクマネジメントのポリシーと手順の更新を引き起こす可能性のあるイベントには、アセスメントまたは監査の所見、セキュリティインシデントまたはブリーチ、もしくは法律、大統領令、指令、規則、ポリシー、基準、およびガイドラインの変更が含まれる。単に管理策を言い換えるだけでは、組織のポリシーや手順を制定することにはならない。

関連管理策:PM-9, PM-30, PS-8, SI-12

拡張管理策:なし

参照資料:[FASC18], [41 CFR 201], [EO 13873], [CNSSD 505], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100], [SP 800-161]

SR-2 サプライチェーンのリスクマネジメント計画

管理策:

a. [*設定:組織が定めるシステム、システムコンポーネント、またはシステムサービス*]の調査、設計、製造、取得、納入、統合、運用および保守、ならびに廃棄に関連するサプライチェーンリスクを管理するための計画を策定する。

b. 脅威、組織または環境の変化に対処するために、サプライチェーンのリスクマネジメント計画を[*設定:組織が定める頻度*]で、または必要に応じてレビューし、更新する。

c. サプライチェーンのリスクマネジメント計画を認可されていない開示や変更から保護する。

詳解:外部プロバイダからの製品、システム、およびサービスへの依存、ならびにそれらのプロバイダとの関係性は、組織にとってリスクのレベルを高める。セキュリティまたはプライバシーのリスクを高める可能性のある脅威には、認可されていない製造、偽造品の挿入または使用、改ざん、盗難、悪意のあるソフトウェアおよびハードウェアの挿入、サプライチェーンでの製造および開発の不十分な経験が含まれる。 サプライチェーンのリスクは、システムの要素またはコンポーネント、システム、組織、適用領域、または国家内で固有または体系的である場合がある。サプライチェーンのリスクマネジメントは、複雑で多面的な取り組みであり信頼関係を構築し、内部および外部の利害関係者とコミュニケーションをとるために組織全体で調整された取り組みを必要とする。サプライチェーンのリスクマネジメント(SCRM:Supply chain risk management)活動には、リスクの特定と評価、適切なリスク対応措置の決定、対応措置を文書化する SCRM 計画の策定、および計画に対するパフォーマンスの監視が含まれる。 SCRM 計画(システムレベル)は個別の実装であり、ポリシーの実装、要件、制約、および影響を提供する。計画はスタンドアロンにすることも、システムのセキュリティとプライバシーの計画に組み込むこともできる。SCRM 計画は、ミッションと事業の機能をサポートするために、SDLC 全体にわたる SCRM 管理策およびシステムの開発／維持の管理、実装、および監視を扱う。

サプライチェーンは組織間および組織内で大幅に異なる可能性があるため、SCRM 計画は、個々のプログラム、組織、および運用状況に合わせて調整される。カスタマイズされた SCRM 計画は、技術、サービス、システムコンポーネント、またはシステムが目的に合っているかどうかを判断するための基礎を提供するため、それに応じて管理策を調整する必要がある。カスタマイズされた SCRM 計画は、組織が、ミッションと事業要件とリスク環境に基づいて、最も重要なミッションと事業の機能にリソースを集中させるのに役立つ。サプライチェーンのリスクマネジメント計画には、組織のサプライチェーンのリスク許容度の表現、許容可能なサプライチェーンリスク軽減戦略または管理策、サプライチェーンのリスクを一貫して評価および監視するためのプロセス、計画の実施と伝達のためのアプローチ、および実施されたサプライチェーンのリスク軽減策の説明と正当性、および関連する役割と責任が含まれる。最後に、サプライチェーンのリスクマネジメント計画は、ライフサイクルベースのシステムセキュリティエンジニアリングプロセスの一部として実装されたセキュリティ設計原則の適用を含め、信頼性が高く、セキュアでプライバシー保護された、レジリエンスのあるシステムコンポーネントおよびシステムを開発するための要件に対応する(SA-8 参照)。

関連管理策:CA-2, CP-4, IR-4, MA-2, MA-6, PE-16, PL-2, PM-9, PM-30, RA-3, RA-7, SA-8, SI-4

拡張管理策:

(1) サプライチェーンのリスクマネジメント計画 | SCRM チームの確立

[*設定:組織が定める職員、役割、および責任*]から構成されるサプライチェーンのリスクマネジメントチームを設置し、[*設定:組織が定めるサプライチェーンのリスクマネジメント活動*]を主導およびサポートする。

詳解:サプライチェーンのリスクマネジメント計画を実施するために、組織は、サプライチェーンのリスクを特定および評価し、プログラム的および技術的な緩和技法を使用してこれらのリスクを管理するためのチームベースの調整されたアプローチを確立する。チームアプローチにより、組織はサプライチェーンの分析を実施し、内部および外部のパートナーや利害関係者とコミュニケーションをとり、SCRM の適切なリソースに関して幅広いコンセンサスを得ることができる。SCRM チームは、リスクエグゼクティブ、情報技術、契約、情報セ

キュリティ、プライバシー、ミッションや事業、法務、サプライチェーンおよびロジスティクス、取得、事業継続性など、SCRM 活動を主導およびサポートするための多様な役割と責任を持つ組織職員で構成される。その他の関連機能。SCRM チームのメンバーは、SDLC の様々な側面に関与しており、全体的として、取得プロセス、法的慣行、脆弱性、脅威、攻撃ベクトルに関する認識と専門知識を提供し、システムの技術的側面と依存関係を理解している。SCRM チームは、セキュリティおよびプライバシーのリスクマネジメントプロセスを拡張したり、組織のリスクマネジメントチームの一部として含めることができる。

関連管理策：なし

参照資料：[FASC18], [41 CFR 201], [EO 13873], [CNSSD 505], [SP 800-30], [SP 800-39], [SP-800-160-1], [SP 800-161], [SP 800-181], [IR 7622], [IR 8272]

SR-3 サプライチェーンの管理策およびプロセス

管理策：

a. [*設定：組織が定めるサプライチェーン職員*]と連携して、[*設定：組織が定めるシステムまたはシステムコンポーネント*]のサプライチェーン要素およびプロセスの弱点または欠陥を特定して対処するための 1 つまたは複数のプロセスを確立する。

b. システム、システムコンポーネント、またはシステムサービスに対するサプライチェーンのリスクから保護し、サプライチェーン関連の事象による損害または結果を限定するために、[*設定：組織が定めるサプライチェーン管理策*]を採用する。

c. 選択および実装されたサプライチェーンのプロセスと管理を[*選択：セキュリティ計画およびプライバシー計画；サプライチェーンのリスクマネジメント計画；*[*設定：組織が定める文書*]]を文書化する。

詳解：サプライチェーン要素には、システムおよびシステムコンポーネントの調査、設計、製造、取得、納入、統合、運用および保守、廃棄に使用される組織、エンティティ、またはツールが含まれる。サプライチェーンプロセスには、ハードウェア、ソフトウェア、ファームウェアの開発プロセスが含まれる；発送および取扱手順；人的セキュリティおよび物理的セキュリティプログラム；履歴を維持するための構成管理ツール、技法、および手段。または、システムおよびシステムコンポーネントの開発、取得、保守、および廃棄に関連する他のプログラム、プロセス、または手順。サプライチェーンの要素とプロセスは、組織、システムインテグレータ、または外部プロバイダによって提供される場合がある。サプライチェーンの要素またはプロセスの弱点または欠陥は、敵対者が悪用して組織に損害を及ぼし、その中核的なミッションまたは事業の機能を遂行する能力に影響を及ぼす可能性のある潜在的な脆弱性を表す。サプライチェーン職員は、サプライチェーンにおける役割と責任を有する個人である。

関連管理策：CA-2, MA-2, MA-6, PE-3, PE-16, PL-8, PM-30, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SC-7, SC-29, SC-30, SC-38, SI-7, SR-6, SR-9, SR-11

拡張管理策：

(1) サプライチェーンの管理策およびプロセス | 多様な供給ベース

[*設定：組織が定めるシステムコンポーネントおよびサービス*]のために多様なソースのセットを採用する。

詳解：システム、システムコンポーネント、およびサービスの供給を多様化することで、敵対者がサプライチェーンを特定して標的とする可能性を減らし、サプライチェーンのイベントや侵害のインパクトを減らすことができる。交換用コンポーネントの複数のサプライヤを認定することで、交換用コンポーネントが使用できなくなる可能性を減らすことができる。多様な開発者や物流サービスプロバイダを採用することで、自然災害やその他のサプライチェーンイベントのインパクトを軽減することができる。組織は、様々な材料やコンポーネントを含むようにシステムを設計することを考慮する。

関連管理策：なし

(2) サプライチェーン保護の管理策およびプロセス | 損害の限定

組織のサプライチェーンを特定し、標的化する潜在的な敵対者からの損害を限定するために、[*設定：組織が定める管理策*]を採用する。

詳解：敵対者がサプライチェーンを首尾よく特定して標的化する可能性を減らすために実装できる管理策には、カスタムまたは非規格化構成の購入の回避、業界で定評のある承認済みベンダリストの採用、事前に合意されたメンテナンススケジュールとアップデートまた、パッチ配信メカニズム、サプライチェーンイベントの場合の緊急時対応計画の維持、コミットメントまたは義務の除外を提供する調達カーブアウトの使用、多様な配送ルートの使用、および購入の決定と配送の間の時間の最小化がある。

関連管理策：なし

(3) サプライチェーン保護の管理策およびプロセス | 下層フローダウン

主契約事業者の契約に含まれる管理策が下請事業者の契約にも含まれるようにする。

詳解：サプライチェーンのリスクを効果的かつ全体的に管理するには、サプライチェーンのすべての層にサプライチェーンのリスクマネジメント管理策が確実に含まれるようにすることが重要である。これには、Tier 1（プライム）の契約事業者が、サブチェーンの契約事業者へのサプライチェーンのリスクマネジメント管理策の「フローダウン」を促進するためのプロセスを確実に実装することが含まれる。フローダウンの対象となる管理策は、SR-3b で特定されている。

関連管理策：SR-5, SR-8

参照資料：[FASC18], [41 CFR 201], [EO 13873], [ISO 20243], [SP 800-30], [SP 800-161], [IR 7622]

SR-4 来歴

管理策：[*設定：組織が定めるシステム、システムコンポーネント、および関連データ*]の有効な来歴を文書化、監視、および維持する。

詳解：すべてのシステムおよびシステムコンポーネントには起点があり、存在する間は変更される可能性がある。来歴とは、システムまたはシステムコンポーネントおよび関連データの起源、開発、所有権、場所、および変更の年代記である。また、システム、コンポーネント、または関連データと対話したり、システム、コンポーネント、またはデータを変更したりするための職員やプロセスも含まれる場合がある。組織は、システムおよびシステムコンポーネントの履歴の作成、保守、および監視の責任を割り当てるための手順の開発（SR-1 参照）を考慮する。組織間で来歴簿と責任を移行する。来歴簿への認可されていない変更を防止および監視する。組織には、システム、システムコンポーネント、および関連データの有効な来歴ベースラインを文書化、監視、および維持する方法がある。これらのアクションは、サプライチェーンの要素や構成の変更など、来歴の変更を追跡、評価、文書化し、来歴情報と来歴変更記録の否認防止を確実にするのに役立つ。履歴の考慮事項は、システム開発ライフサイクル全体を通じて対処され、必要に応じて契約やその他の取り決めに組み込まれる。

関連管理策：CM-8, MA-2, MA-6, RA-9, SA-3, SA-8, SI-4

拡張管理策：

(1) 来歴 | 同一性

識別された[*設定：組織が定めるシステムおよび重要システムに関連するサプライチェーン要素、プロセス、および職員*]の一意の識別を確立および維持する。

詳解：組織のサプライチェーンに誰が、何が含まれているかを知ることは、サプライチェーン活動を可視化するために重要である。サプライチェーン活動の可視性は、リスクの高いイベントや行為を監視および特定するためにも重要である。サプライチェーンの要素、プロセス、および職員に対する合理的な可視性がなければ、組織がリスクを理解および管理し、有害事象に対する感受性を低減することは非常に困難である。サプライチェーン要素には、システムおよびシステムコンポーネントの調査、設計、製造、調達、納入、統合、運用、保守、および廃棄に使用される組織、エンティティ、またはツールが含まれる。サプライチェーンプロセスには、ハードウェア、ソフトウェア、ファームウェアの開発プロセスが含

まれる。発送および取扱手順。来歴を維持するための構成管理ツール、技法、および手段。職員および物理的セキュリティプログラム。または、サプライチェーン要素の生産と流通に関連する他のプログラム、プロセス、または手順。サプライチェーン職員とは、システムまたはシステムコンポーネントのセキュアな調査、設計、製造、取得、納入、統合、運用および保守、廃棄の保護に関する特定の役割と責任を有する個人のことである。識別方法は、サプライチェーンの変更（例えば、サプライヤが購入された場合）、侵害、または事象が発生した場合の調査をサポートするのに十分である。

関連管理策：IA-2, IA-8, PE-16

(2) 来歴 | 追跡および痕跡

サプライチェーン全体で追跡するために、[*設定：組織が定めるシステムおよび重要なシステムコンポーネント*]の一意の識別を確立および維持する。

詳解：開発および移送活動中にシステムおよびシステムコンポーネントの一意の識別を追跡することは、来歴の確立および維持のための基本的なアイデンティティ構造を提供する。例えば、システムコンポーネントは、シリアル番号を使用してラベル付けされるか、RFID タグを使用してタグ付けされてもよい。ラベルとタグは、システムまたはシステムコンポーネントの来歴をよりよく可視化するのに役立つ。システムまたはシステムコンポーネントは、複数の一意の識別子を持つことができる。識別方法は、サプライチェーンの侵害または事件後のフォレンジック捜査をサポートするのに十分である。

関連管理策：IA-2, IA-8, PE-16, PL-2

(3) 来歴 | 本物であり、改変されていないことの確認

受け取ったシステムまたはシステムコンポーネントが本物であり、改変されていないことを確認するために、[*設定：組織が定める管理策*]を採用する。

詳解：多くのシステムおよびシステムコンポーネント、特にハードウェアには、光学的およびナノ技術のタグ付け、物理的に複製できない機能、サイドチャネル分析、暗号ハッシュ検証またはデジタル署名、目に見える改ざん防止ラベルまたはステッカーなど、アイテムが本物であるか変更されているかを判断する技術的手段がある。管理策には、改ざんや偽造の兆候となり得る、規格外の性能の監視も含めることができる。組織は、システムまたはコンポーネントが本物であり、変更されていないことを検証し、疑わしいシステムまたはコンポーネントを交換するために、サプライヤおよび契約事業者のプロセスを活用することができる。一貫性のないパッケージング、破損したシール、誤ったラベルなど、改ざんの兆候は、配達を受け入れる前に目に見えて対処できる場合がある。システムまたはシステムコンポーネントが改ざんまたは偽造された疑いがある場合、サプライヤ、契約事業者、または相手先ブランド供給業者は、アイテムを交換するか、または偽造品または改ざんされたアイテムの出所を特定するためのフォレンジック機能を提供することができる。組織は、疑わしいシステムまたはコンポーネントの配信を特定する方法について、職員にトレーニングを提供できる。

関連管理策：AT-3, SR-9, SR-10, SR-11

(4) 来歴 | サプライチェーンの完全性 — 系譜

[*設定：組織が定める管理策*]を採用し、[*設定：組織が定める分析*]を実施して、重要なまたはミッションクリティカルな技術、製品およびサービスの内部構成と来歴を検証することにより、システムとシステムコンポーネントの完全性を確保する。

詳解：システムコンポーネントの内部構成と、技術、製品、およびサービスの来歴に関する信頼できる情報は、信頼の強力な基盤を提供する。技術、製品、およびサービスの内部構成と来歴の妥当性確認は、系譜と呼ばれる。マイクロエレクトロニクスの場合、これにはコンポーネントの材料組成が含まれる。ソフトウェアの場合、これには、ある時点でのコンポーネントのバージョンを含む、オープンソースおよび独自仕様のコードの構成が含まれる。系譜は、彼らが提供する製品、サービス、技術の内部構成と来歴についてサプライヤが主張する保証を強化する。内部構成と来歴の妥当性確認は、技術と製品の調査、設計、製造、取得、納入、統合、運用と保守、技術、製品、サービスの廃棄の際に製造業者と サプライヤが作成する様々なエビデンス成果物または記録によって達成できる。エビデンス成果物には、ソフトウェア識別（SWID：software identification）タグ、ソフトウェアコン

ポーネントインベントリ、製造元によるプラットフォーム属性の宣言（シリアル番号、ハードウェアコンポーネントインベントリなど）、測定値（ファームウェアハッシュなど）などが含まれるが、これらに限定されない。ハードウェア自体にバインドされている。

関連管理策：RA-3

参照資料：[FASC18], [41 CFR 201], [EO 13873], [ISO 27036], [ISO 20243], [SP 800-160-1], [SP 800-161], [IR 7622], [IR 8112], [IR 8272]

SR-5 取得戦略、ツール、および方法

管理策：サプライチェーンのリスクから保護、特定、および軽減するために、[*設定：組織が定める取得戦略、契約ツール、および取得方法*]を採用する。

詳解：取得プロセスの使用は、サプライチェーンを保護するための重要な手段を提供する。システムまたはシステムコンポーネントの最終用途を曖昧にする、ブラインド購入またはフィルタ付き購入を使用する、改ざん防止パッケージが必要である、信頼できる配布または管理された配布を使用するなど、多くの有用なツールと技法が利用可能である。サプライチェーンのリスクアセスメント結果は、状況に最も適した戦略、ツール、および方法を導出し、通知することができる。ツールおよび技法は、システム開発ライフサイクル全体を通じて、認可されていない製造、盗難、改ざん、偽造品の挿入、悪意のあるソフトウェアまたはバックドアの挿入、および不十分な開発慣行に対する保護を提供しても良い。組織はまた、管理策を実装し、プロセスとセキュリティおよびプライバシー慣行の透明性を促進し、汚染または偽造コンポーネントの禁止に対処する契約文言を提供し、信頼できないサプライヤからの購入を制限するサプライヤにインセンティブを提供することを考慮する。組織は、サプライチェーンリスク、利用可能な緩和戦略、およびプログラムをいつ採用することが望ましいかについて、職員に訓練、教育、および意識向上プログラムを提供することを考慮する。開発計画、文書、エビデンスをレビューおよび保護する方法は、組織のセキュリティ要件およびプライバシー要件に見合ったものである。契約では、文書保護要件を指定できる。

関連管理策：AT-3, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SR-6, SR-9, SR-10, SR-11

拡張管理策：

(1) 取得戦略、ツール、および方法 | 適切な供給

[*設定：組織が定める重要なシステムコンポーネント*]の適切な供給を確保するために、[*設定：組織が定める管理策*]を採用する。

詳解：敵対者は、重要なシステムコンポーネントの供給を妨害したり、サプライヤの業務を破壊したりすることにより、組織の運営を妨害しようとすることが出来る。組織は、一時的なシステム機能または永続的なシステム機能の損失を軽減するために、システムとコンポーネントの平均故障時間を追跡する場合がある。重要なシステムコンポーネントの適切な供給を確保するための管理策には、特定された重要なコンポーネントのサプライチェーン全体にわたる複数のサプライヤの使用、ミッションクリティカルな時期に動作を確保するための予備コンポーネントの備蓄、および必要に応じて使用できる機能的に同一または類似のコンポーネントの特定が含まれる。

関連管理策：RA-9

(2) 取得戦略、ツール、および方法 | 選択、受領、変更、または更新前のアセスメント

選択、受領、変更、または更新の前に、システム、システムコンポーネント、またはシステムサービスのアセスメントを実施する。

詳解：組織の職員または独立した外部のエンティティが、システム、コンポーネント、製品、ツール、およびサービスのアセスメントを実施し、改ざん、意図的でないおよび意図的な脆弱性のエビデンス、またはサプライチェーン管理策が遵守されていないエビデンスを明らかにする。これらには、悪意のあるコード、悪意のあるプロセス、欠陥のあるソフトウェア、バックドア、および偽造品が含まれる。アセスメントには査定を含めることができる；設計提案レビュー；目視または物理的検査；静的および動的分析；目視検査、X 線検査、または磁性粒子検査；シミュレーション；ホワイト、グレー、またはブラックボックステスト；ファズテ

スト；ストレステスト；および侵入テスト（SR-6(1)参照）。評価中に生成されたエビデンスは、組織によるその後のアクションのために文書化される。サプライチェーン要素の組織的または独立したアセスメント中に生成されたエビデンスを使用して、サプライチェーンプロセスを改善し、サプライチェーンのリスクマネジメントプロセスに通知することができる。エビデンスは、後の評価に活用できる。エビデンスおよびその他の文書は、組織の合意に従って共有されても良い。

関連管理策：CA-8, RA-5, SA-11, SI-7

参照資料：[FASC18], [41 CFR 201], [EO 13873], [ISO 27036], [ISO 20243], [SP 800-30], [SP 800-161], [IR 7622], [IR 8272]

SR-6 サプライヤのアセスメントおよびレビュー

管理策：サプライヤまたは契約事業者、およびそれらが提供するシステム、システムコンポーネント、またはシステムサービスに関連するサプライチェーン関連リスクを[*設定：組織が定める頻度*]で評価およびレビューする。

詳解：サプライヤのリスクのアセスメントとレビューには、セキュリティおよびサプライチェーンのリスクマネジメントプロセス、外国の所有権、管理または影響力（FOCI）、およびサプライヤが第 2 層および第 3 層のサプライヤと契約事業者を効果的に評価する能力が含まれる。レビューは、組織または独立したサードパーティによって実施される場合がある。レビューでは、文書化されたプロセス、文書化された管理策、およびサプライヤまたは契約事業者に関連するオールソースインテリジェンス、公開情報が考慮される。組織は、オープンソース情報を使用して、盗まれた情報、不十分な開発と品質管理の慣行、情報漏えい、または偽造品の兆候を監視することができる。場合によっては、適用される規定、ポリシー、または組織間の合意または契約に従って、他の組織とアセスメントおよびレビューを共有することが適切または必要となる場合がある。

関連管理策：SR-3, SR-5

拡張管理策：

(1) サプライヤのアセスメントおよびレビュー | テストおよび分析

[*選択（1 つ以上）：組織による分析；独立したサードパーティによる分析；組織によるテスト；独立したサードパーティによるテスト*]をシステム、システムコンポーネント、またはシステムサービスに関連する[*設定：組織が定めるサプライチェーン要素、プロセス、および行為者*]に適用する。

詳解：開発とデリバリーを含む、サプライチェーン内のエンティティと手順の間の関係が考慮される。サプライチェーン要素には、システム、システムコンポーネント、またはシステムサービスの調査、設計、製造、取得、納入、統合、運用、保守、廃棄に使用される組織、エンティティ、またはツールが含まれる。サプライチェーンプロセスには、サプライチェーンのリスクマネジメントプログラムが含まれる；SCRM の戦略と実装計画。職員および物理的セキュリティプログラム。ハードウェア、ソフトウェア、およびファームウェア開発プロセス；履歴を維持するための構成管理ツール、技法、および手段；発送および取扱手順；サプライチェーン要素の生産と流通に関連するプログラム、プロセス、または手順。サプライチェーンにおける行為者は、サプライチェーンにおいて特定の役割と責任を有する個人である。サプライチェーンの要素、プロセス、および行為者の分析およびテスト中に生成および収集されたエビデンスは、文書化され、組織のリスクマネジメント活動および決定を通知するために使用される。

関連管理策：CA-8、SI-4

参照資料：[FASC18], [41 CFR 201], [EO 13873], [ISO 27036], [ISO 20243], [FIPS 140-3], [FIPS 180-4], [FIPS 186-4], [FIPS 202], [SP 800-30], [SP 800-161], [IR 7622], [IR 8272]

SR-7 サプライチェーン運用セキュリティ

管理策：システム、システムコンポーネント、またはシステムサービスのサプライチェーン関連情

報を保護するために、[*設定：組織が定める運用セキュリティ（OPSEC：Operations Security）管理策*]を採用する。

詳解：サプライチェーンの OPSEC は OPSEC の範囲を拡大し、サプライヤおよび潜在的なサプライヤを含む。OPSEC は、重要な情報を特定し、運用およびその他の活動に関連する友好的な行動を分析して、潜在的な敵対者が観察できる行動を特定し、潜在的な敵対者が取得または解釈し、十分な時間内に情報を導き出すことができる兆候を決定するプロセスを含む。組織に損害を及ぼすこと、利用可能な脆弱性およびリスクを許容可能なレベルまで排除または低減するための保全措置または対策を実施すること、および集約された情報がユーザまたはサプライチェーンの特定の用途をどのように公開するかを考慮すること。サプライチェーン情報には、ユーザのアイデンティティが含まれる；システム、システムコンポーネント、およびシステムサービスの使用；サプライヤのアイデンティティ；セキュリティとプライバシーの要件；システムおよびコンポーネントの構成；サプライヤプロセス；設計仕様；およびテストおよび評価結果。サプライチェーンの OPSEC は、組織がサプライヤからのミッションや事業の情報を差し控えることを要求する場合があり、システム、システムコンポーネント、またはシステムサービスの最終用途またはユーザを隠すための仲介者の使用を含む場合がある。

関連管理策：SC-38

拡張管理策：なし

参照資料：[EO 13873], [SP 800-30], [ISO 27036], [SP 800-161], [IR 7622]

SR-8 通知協定

管理策：システムコンポーネント、システムサービスのサプライチェーンに関与するエンティティとの合意と手順[*選択（1 つ以上）：システムのサプライチェーンの侵害の通知；アセスメントまたは監査の結果；*[*設定：組織が定める情報*]]を確立する。

詳解：合意と手順の確立は、サプライチェーンエンティティ間のコミュニケーションを促進する。組織がそのようなインシデントに効果的に対応するために、組織のシステムまたはシステムコンポーネントに悪影響を及ぼしたり悪影響を及ぼしたりする可能性のある、サプライチェーンにおける侵害および潜在的な侵害を早期に通知することが不可欠である。アセスメントまたは監査の結果には、意志決定または結果に貢献したオープンソース情報が含まれる場合があり、サプライチェーンエンティティが懸念を解決したり、プロセスを改善するのに役立つ可能性がある。

関連管理策：IR-4, IR-6, IR-8

拡張管理策：なし

参照資料：[FASC18], [41 CFR 201], [EO 13873] [ISO 27036], [SP 800-30], [SP 800-161], [IR 7622]

SR-9 耐タンパー性および検知

管理策：システム、システムコンポーネント、またはシステムサービスにタンパープロテクションプログラムを実装する。

詳解：改ざん防止技術、ツール、および技法は、リバースエンジニアリング、変更、置換を含む多くの脅威に対して、システム、システムコンポーネント、およびサービスに一定レベルの保護を提供する。耐タンパー性および／または改ざん検知と相まって強力な識別は、配布中および使用中のシステムおよびコンポーネントを保護するために不可欠である。

関連管理策：PE-3, PM-30, SA-15, SI-4, SI-7, SR-3, SR-4, SR-5, SR-10, SR-11

拡張管理策：

(1) 耐タンパー性および検知 | システム開発ライフサイクルの複数の段階

システム開発のライフサイクル全体を通じて、改ざん防止技術、ツール、および技法を採用する。

詳解：システム開発のライフサイクルには、調査、設計、製造、取得、納入、統合、運用および保守、廃棄が含まれる。組織は、耐タンパー性と検知のためにハードウェアとソフトウェアの技法を組み合わせて使用している。組織は、難読化とセルフチェックを使用して、リバースエンジニアリングや変更を敵対者にとってより困難で、時間と費用がかかるものにしている。システムおよびシステムコンポーネントのカスタマイズにより、代替品の検知が容易になり、損傷を限定することができる。

関連管理策：SA-3

参照資料：[ISO 20243]

SR-10 システムまたはコンポーネントの検査

管理策：[*設定：組織が定めるシステムまたはシステムコンポーネント*]を[*選択（1つ以上）：ランダム；*[*設定：組織が定める頻度*]；[*設定：組織が定める検査の必要性の兆候*]]で検査し、改ざんを検知する。

詳解：システムまたはシステムコンポーネントの耐タンパー性および検知のための検査は、物理的および論理的な改ざんに対処し、組織が管理する領域から削除されたシステムおよびシステムコンポーネントに適用される。検査の必要性の兆候には、パッケージ、仕様、工場の場所、または部品が購入されたエンティティの変更、および個人が旅行からリスクの高い場所に戻ったときなどが含まれる。

関連管理策：AT-3, PM-30, SI-4, SI-7, SR-3, SR-4, SR-5, SR-9, SR-11

参照資料：[ISO 20243]

SR-11 コンポーネントの真正性

管理策：

a. 偽造コンポーネントがシステムに侵入するのを検知および防止する手段を含む、偽造防止ポリシーおよび手順を作成し、実装する。

b. 偽造システムコンポーネントについて[*選択（1つ以上）：偽造コンポーネントのソース；*[*設定：組織が定める外部報告組織*]；[*設定：組織が定める職員または役割*]]に報告する。

詳解：偽造コンポーネントのソースには、製造業者、開発者、ベンダ、および契約事業者が含まれる。偽造防止のポリシーと手順は、耐タンパー性をサポートし、悪意のあるコードの導入に対する一定レベルの保護を提供する。外部の報告組織には CISA が含まれる。

関連管理策：PE-3, SA-4, SI-7, SR-9, SR-10

拡張管理策：

(1) コンポーネントの真正性 | 偽造防止トレーニング

偽造システムコンポーネント（ハードウェア、ソフトウェア、ファームウェアを含む）を検知するためのトレーニングを[*設定：組織が定める職員または役割*]に行なう。

詳解：なし

関連管理策：AT-3

(2) コンポーネントの真正性 | コンポーネントのサービスおよび修理のための構成管理

サービスまたは修理を待っている[*設定：組織が定めるシステムコンポーネント*]、およびサービスへの復帰を待っているサービスまたは修理されたコンポーネントの構成管理を維持する。

詳解：なし

関連管理策：CM-3, MA-2, MA-4, SA-10

(3) コンポーネントの真正性 | 偽造防止の精査

偽造システムコンポーネントを[*設定：組織が定める頻度*]で精査する。

詳解：コンポーネントのタイプにより、実施される精査のタイプを決定する（例えば、コンポーネントがウェブアプリケーションである場合、ウェブアプリケーションの精査）。

関連管理策：RA-5

参照資料：[ISO 20243]

SR-12 コンポーネントの廃棄

管理策：[*設定：組織が定める技法と方法*]を使用して、[*設定：組織が定めるデータ、文書、ツール、またはシステムコンポーネント*]を廃棄する。

詳解：データ、ドキュメント、ツール、またはシステムコンポーネントは、システム開発ライフサイクル中いつでも（ライフサイクルの廃棄フェーズまたは廃棄フェーズだけでなく）廃棄できる。例えば、廃棄は、調査、設計、プロトタイピング、または運用／保守中に発生する可能性があり、ディスクのクリーニング、暗号鍵の削除、コンポーネントの部分的な再利用などの方法が含まれる。廃棄時の侵害の機会は、紙ベースまたはデジタルファイルのシステムドキュメントを含む、物理的および論理的データに影響を与える。発送および配達の文書。ソフトウェアコード付きのメモリースティック。または、機微情報または専有情報を含む固定媒体を含む完全なルータまたはサーバ。さらに、システムコンポーネントの適切な処分は、そのようなコンポーネントがグレーマーケットに出品されるのを防ぐのに役立つ。

関連管理策：MP-6

参照資料：なし

参照資料

法律、ポリシー、指令、規則、基準、およびガイドライン[34]

法律および大統領令	
[ATOM54]	Atomic Energy Act (P.L. 83-703), August 1954. https://www.govinfo.gov/content/pkg/STATUTE-68/pdf/STATUTE-68-pg919.pdf
[CMPPA]	Computer Matching and Privacy Protection Act of 1988 (P.L. 100-503), October 1988. https://www.govinfo.gov/content/pkg/STATUTE-102/pdf/STATUTE-102-Pg2507.pdf
[EGOV]	E-Government Act [includes FISMA] (P.L. 107-347), December 2002. https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf
[EVIDACT]	Foundations for Evidence-Based Policymaking Act of 2018 (P.L. 115-435), January 2019. https://www.congress.gov/115/plaws/publ435/PLAW-115publ435.pdf
[FASC18]	Secure Technology Act [includes Federal Acquisition Supply Chain Security Act] (P.L. 115-390), December 2018. https://www.congress.gov/bill/115th-congress/senate-bill/3085
[FISMA]	Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[FOIA96]	Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996. https://www.govinfo.gov/content/pkg/PLAW-104publ231/pdf/PLAW-104publ231.pdf
[PRIVACT]	Privacy Act (P.L. 93-579), December 1974. https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf
[USA PATRIOT]	USA Patriot Act (P.L. 107-56), October 2001. https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf
[USC 552]	United States Code, 2006 Edition, Supplement 4, Title 5 - *Government Organization and Employees*, January 2011. https://www.govinfo.gov/content/pkg/USCODE-2010-title5/pdf/USCODE-2010-title5-partI-chap5-subchapII-sec552a.pdf
[USC 2901]	United States Code, 2008 Edition, Title 44 - *Public Printing and Documents*, Chapters 29, 31, and 33, January 2012. https://www.govinfo.gov/content/pkg/USCODE-2011-title44/pdf/USCODE-

[34]この付属書で引用されている参照資料は、NIST の FISMA およびプライバシープロジェクトを直接サポートする外部の出版物である。追加の NIST 基準、ガイドライン、および機関間の報告も、第 3 章の該当する管理策の参照資料セクションを含め、本出版物全体で引用されている。これらの出版物にアクセスするために、NIST Web サイトへの直接リンクが提供されています。

2011-title44-chap29-sec2901.pdf

[USC 3502] "Definitions," Title 44 U.S. Code, Sec. 3502. 2011 ed. https://www.govinfo.gov/app/details/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapI-sec3502

[USC 11101] "Definitions," Title 40 U.S. Code, Sec. 11101. 2018 ed. https://www.govinfo.gov/app/details/USCODE-2018-title40/USCODE-2018-title40-subtitleIII-chap111-sec11101

[EO 13526] Executive Order 13526, *Classified National Security Information*, December 2009. https://www.archives.gov/isoo/policy-documents/cnsi-eo.html

[EO 13556] Executive Order 13556, *Controlled Unclassified Information*, November 2010. https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information

[EO 13587] Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, October 2011. https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net

[EO 13636] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[EO 13800] Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure

[EO 13873] Executive Order 13873, *Executive Order on Securing the Information and Communications Technology and Services Supply Chain*, May 2019. https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain

規則、指令、計画、およびポリシー

[HSPD 7] Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 2003. https://www.dhs.gov/homeland-security-presidential-directive-7

[HSPD 12] Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2004. https://www.dhs.gov/homeland-security-presidential-directive-12

[NITP12] Presidential Memorandum for the Heads of Executive Departments and Agencies, *National Insider Threat Policy and Minimum Standards for*

Executive Branch Insider Threat Programs, November 2012. https://obamawhitehouse.archives.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand

[5 CFR 731] Code of Federal Regulations, Title 5, *Administrative Personnel, Section 731.106, Designation of Public Trust Positions and Investigative Requirements* (5 C.F.R. 731.106). https://www.govinfo.gov/content/pkg/CFR-2012-title5-vol2/pdf/CFR-2012-title5-vol2-sec731-106.pdf

[32 CFR 2002] Code of Federal Regulations, Title 32, *Controlled Unclassified Information* (32 C.F.R. 2002). https://www.federalregister.gov/documents/2016/09/14/2016-21665/controlled-unclassified-information

[41 CFR 201] "Federal Acquisition Supply Chain Security Act; Rule," 85 Federal Register 54263 (September 1, 2020), pp 54263-54271. https://www.federalregister.gov/d/2020-18939 [or as published in Title 41 Code of Federal Regulations, Sec. 201 (forthcoming)]

[ODNI NITP] Office of the Director National Intelligence, *National Insider Threat Policy* https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy.pdf

[OMB A-108] Office of Management and Budget Memorandum Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, December 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A108/omb_

[OMB A-130] Office of Management and Budget Memorandum Circular A-130, *Managing Information as a Strategic Resource*, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a13 0revised.pdf

[OMB M-03-22] Office of Management and Budget Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 2003. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2003/ m03_22.pdf

[OMB M-08-05] Office of Management and Budget Memorandum M-08-05, *Implementation of Trusted Internet Connections (TIC)*, November 2007. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memo randa/fy2008/m08-05.pdf

[OMB M-17-06] Office of Management and Budget Memorandum M-17-06, *Policies for Federal Agency Public Websites and Digital Services*, November 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/ m-17-06.pdf

[OMB M-17-12] Office of Management and Budget Memorandum M-17-12, *Preparing for*

and Responding to a Breach of Personally Identifiable Information, January 2017. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf

[OMB M-17-25] Office of Management and Budget Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/ M-17-25.pdf

[OMB M-19-03] Office of Management and Budget Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, December 2018. https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf

[OMB M-19-15] Office of Management and Budget Memorandum M-19-15, *Improving Implementation of the Information Quality Act*, April 2019. https://www.whitehouse.gov/wp-content/uploads/2019/04/M-19-15.pdf

[OMB M-19-23] Office of Management and Budget Memorandum M-19-23, *Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance*, July 2019. https://www.whitehouse.gov/wp-content/uploads/2019/07/M-19-23.pdf

[CNSSD 505] Committee on National Security Systems Directive No. 505, *Supply Chain Risk Management (SCRM)*, August 2017. https://www.cnss.gov/CNSS/issuances/Directives.cfm

[CNSSP 22] Committee on National Security Systems Policy No. 22, *Cybersecurity Risk Management Policy*, August 2016. https://www.cnss.gov/CNSS/issuances/Policies.cfm

[CNSSI 1253] Committee on National Security Systems Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, March 2014. https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[CNSSI 4009] Committee on National Security Systems Instruction No. 4009, *Committee on National Security Systems (CNSS) Glossary*, April 2015. https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[DODI 8510.01] Department of Defense Instruction 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, March 2014. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf

[DHS NIPP] Department of Homeland Security, *National Infrastructure Protection Plan (NIPP)*, 2009. https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

基準、ガイドライン、および報告書

[ISO 15026-1] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics

Engineers (ISO/IEC/IEEE) 15026-1:2019, *Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*, March 2019. https://www.iso.org/standard/73567.html

[ISO 15408-1] International Organization for Standardization/International Electrotechnical Commission 15408-1:2009, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*, April 2017. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

[ISO 15408-2] International Organization for Standardization/International Electrotechnical Commission 15408-2:2008, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*, April 2017. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

[ISO 15408-3] International Organization for Standardization/International Electrotechnical Commission 15408-3:2008, *Information technology— Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*, April 2017. https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

[ISO 15288] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15288:2015, *Systems and software engineering — Systems life cycle processes*, May 2015. https://www.iso.org/standard/63711.h1ml

[ISO 20243] International Organization for Standardization/International Electrotechnical Commission 20243-1:2018, *Information technology — Open Trusted Technology ProviderTM Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products — Part 1: Requirements and recommendations*, February 2018. https://www.iso.org/standard/74399.html

[ISO 25237] International Organization for Standardization/International Electrotechnical Commission 25237:2017, *Health informatics — Pseudonymization*, January 2017. https://www.iso.org/standard/63553.html

[ISO 27036] International Organization for Standardization/International Electrotechnical Commission 27036-1:2014, *Information technology— Security techniques—Information security for supplier relationships, Part 1: Overview and concepts*, April 2014. https://www.iso.org/standard/59648.html

[ISO 29100] International Organization for Standardization/International Electrotechnical Commission 29100:2011, *Information technology— Security techniques—Privacy framework*, December 2011. https://www.iso.org/standard/45123.html

[ISO 29147] International Organization for Standardization/International

Electrotechnical Commission 29147:2018, *Information technology—Security techniques—Vulnerability disclosure*, October 2018. https://www.iso.org/standard/72311.html

[ISO 29148] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 29148:2018, *Systems and software engineering—Life cycle processes—Requirements engineering*, November 2018. https://www.iso.org/standard/72089.html

[FIPS 140-3] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

[FIPS 180-4] National Institute of Standards and Technology (2015) Secure Hash Standard (SHS). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 180-4. https://doi.org/10.6028/NIST.FIPS.180-4

[FIPS 186-4] National Institute of Standards and Technology (2013) Digital Signature Standard (DSS). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 186-4. https://doi.org/10.6028/NIST.FIPS.186-4

[FIPS 197] National Institute of Standards and Technology (2001) Advanced Encryption Standard (AES). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 197. https://doi.org/10.6028/NIST.FIPS.197

[FIPS 199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[FIPS 200] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200

[FIPS 201-2] National Institute of Standards and Technology (2013) Personal Identity Verification (PIV) of Federal Employees and Contractors. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 201-2. https://doi.org/10.6028/NIST.FIPS.201-2

[FIPS 202] National Institute of Standards and Technology (2015) SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 202.

https://doi.org/10.6028/NIST.FIPS.202

[SP 800-12] Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-12, Rev. 1. https://doi.org/10.6028/NIST.SP.800-12r1

[SP 800-18] Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1. https://doi.org/10.6028/NIST.SP.800-18r1

[SP 800-28] Jansen W, Winograd T, Scarfone KA (2008) Guidelines on Active Content and Mobile Code. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-28, Version 2. https://doi.org/10.6028/NIST.SP.800-28ver2

[SP 800-30] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[SP 800-32] Kuhn R, Hu VC, Polk T, Chang S-J (2001) Introduction to Public Key Technology and the Federal PKI Infrastructure. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-32. https://doi.org/10.6028/NIST.SP.800-32

[SP 800-34] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of November 11, 2010. https://doi.org/10.6028/NIST.SP.800-34r1

[SP 800-35] Grance T, Hash J, Stevens M, O'Neal K, Bartol N (2003) Guide to Information Technology Security Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-35. https://doi.org/10.6028/NIST.SP.800-35

[SP 800-37] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[SP 800-39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[SP 800-40] Souppaya MP, Scarfone KA (2013) Guide to Enterprise Patch Management Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 3.

https://doi.org/10.6028/NIST.SP.800-40r3

[SP 800-41] Scarfone KA, Hoffman P (2009) Guidelines on Firewalls and Firewall Policy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-41, Rev. 1. https://doi.org/10.6028/NIST.SP.800-41r1

[SP 800-45] Tracy MC, Jansen W, Scarfone KA, Butterfield J (2007) Guidelines on Electronic Mail Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-45, Version 2. https://doi.org/10.6028/NIST.SP.800-45ver2

[SP 800-46] Souppaya MP, Scarfone KA (2016) Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-46, Rev. 2. https://doi.org/10.6028/NIST.SP.800-46r2

[SP 800-47] Grance T, Hash J, Peck S, Smith J, Korow-Diks K (2002) Security Guide for Interconnecting Information Technology Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-47. https://doi.org/10.6028/NIST.SP.800-47

[SP 800-50] Wilson M, Hash J (2003) Building an Information Technology Security Awareness and Training Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-50. https://doi.org/10.6028/NIST.SP.800-50

[SP 800-52] McKay KA, Cooper DA (2019) Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-52, Rev. 2. https://doi.org/10.6028/NIST.SP.800-52r2

[SP 800-53A] Joint Task Force Transformation Initiative (2014) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 4, Includes updates as of December 18, 2014. https://doi.org/10.6028/NIST.SP.800-53Ar4

[SP 800-53B] Joint Task Force (2020) Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B. https://doi.org/10.6028/NIST.SP.800-53B

[SP 800-55] Chew E, Swanson MA, Stine KM, Bartol N, Brown A, Robinson W (2008) Performance Measurement Guide for Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-55, Rev. 1. https://doi.org/10.6028/NIST.SP.800-55r1

[SP 800-56A] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R (2018) Recommendation

for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56A, Rev. 3. https://doi.org/10.6028/NIST.SP.800-56Ar3

[SP 800-56B] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R, Simon S (2019) Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56B, Rev. 2. https://doi.org/10.6028/NIST.SP.800-56Br2

[SP 800-56C] Barker EB, Chen L, Davis R (2020) Recommendation for Key-Derivation Methods in Key-Establishment Schemes. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56C, Rev. 2. https://doi.org/10.6028/NIST.SP.800-56Cr2

[SP 800-57-1] Barker EB (2020) Recommendation for Key Management: Part 1 – General. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 1, Rev. 5. https://doi.org/10.6028/NIST.SP.800-57pt1r5

[SP 800-57-2] Barker EB, Barker WC (2019) Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-57pt2r1

[SP 800-57-3] Barker EB, Dang QH (2015) Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 3, Rev. 1. https://doi.org/10.6028/NIST.SP.800-57pt3r1

[SP 800-60-1] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v1r1

[SP 800-60-2] Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v2r1

[SP 800-61] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61, Rev. 2. https://doi.org/10.6028/NIST.SP.800-61r2

[SP 800-63-3] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National

Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

[SP 800-63A] Grassi PA, Fenton JL, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines: Enrollment and Identity Proofing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63A, Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63a

[SP 800-63B] Grassi PA, Fenton JL, Newton EM, Perlner RA, Regenscheid AR, Burr WE, Richer, JP, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines: Authentication and Lifecycle Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63B, Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63b

[SP 800-70] Quinn SD, Souppaya MP, Cook MR, Scarfone KA (2018) National Checklist Program for IT Products: Guidelines for Checklist Users and Developers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-70, Rev. 4. https://doi.org/10.6028/NIST.SP.800-70r4

[SP 800-73-4] Cooper DA, Ferraiolo H, Mehta KL, Francomacaro S, Chandramouli R, Mohler J (2015) Interfaces for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-73-4, Includes updates as of February 8, 2016. https://doi.org/10.6028/NIST.SP.800-73-4

[SP 800-76-2] Grother PJ, Salamon WJ, Chandramouli R (2013) Biometric Specifications for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-76-2. https://doi.org/10.6028/NIST.SP.800-76-2

[SP 800-77] Barker EB, Dang QH, Frankel SE, Scarfone KA, Wouters P (2020) Guide to IPsec VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-77, Rev. 1. https://doi.org/10.6028/NIST.SP.800-77r1

[SP 800-78-4] Polk T, Dodson DF, Burr WE, Ferraiolo H, Cooper DA (2015) Cryptographic Algorithms and Key Sizes for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-78-4. https://doi.org/10.6028/NIST.SP.800-78-4

[SP 800-79-2] Ferraiolo H, Chandramouli R, Ghadiali N, Mohler J, Shorter S (2015) Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-79-2. https://doi.org/10.6028/NIST.SP.800-79-2

[SP 800-81-2] Chandramouli R, Rose SW (2013) Secure Domain Name System (DNS) Deployment Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-81-2. https://doi.org/10.6028/NIST.SP.800-81-2

[SP 800-82] Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 2. https://doi.org/10.6028/NIST.SP.800-82r2

[SP 800-83] Souppaya MP, Scarfone KA (2013) Guide to Malware Incident Prevention and Handling for Desktops and Laptops. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-83, Rev. 1. https://doi.org/10.6028/NIST.SP.800-83r1

[SP 800-84] Grance T, Nolan T, Burke K, Dudley R, White G, Good T (2006) Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-84. https://doi.org/10.6028/NIST.SP.800-84

[SP 800-86] Kent K, Chevalier S, Grance T, Dang H (2006) Guide to Integrating Forensic Techniques into Incident Response. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-86. https://doi.org/10.6028/NIST.SP.800-86

[SP 800-88] Kissel RL, Regenscheid AR, Scholl MA, Stine KM (2014) Guidelines for Media Sanitization. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-88, Rev. 1. https://doi.org/10.6028/NIST.SP.800-88r1

[SP 800-92] Kent K, Souppaya MP (2006) Guide to Computer Security Log Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-92. https://doi.org/10.6028/NIST.SP.800-92

[SP 800-94] Scarfone KA, Mell PM (2007) Guide to Intrusion Detection and Prevention Systems (IDPS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-94. https://doi.org/10.6028/NIST.SP.800-94

[SP 800-95] Singhal A, Winograd T, Scarfone KA (2007) Guide to Secure Web Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-95. https://doi.org/10.6028/NIST.SP.800-95

[SP 800-97] Frankel SE, Eydt B, Owens L, Scarfone KA (2007) Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-97. https://doi.org/10.6028/NIST.SP.800-97

[SP 800-100] Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007. https://doi.org/10.6028/NIST.SP.800-100

[SP 800-101] Ayers RP, Brothers S, Jansen W (2014) Guidelines on Mobile Device Forensics. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-101, Rev. 1. https://doi.org/10.6028/NIST.SP.800-101r1

[SP 800-111] Scarfone KA, Souppaya MP, Sexton M (2007) Guide to Storage Encryption Technologies for End User Devices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-111. https://doi.org/10.6028/NIST.SP.800-111

[SP 800-113] Frankel SE, Hoffman P, Orebaugh AD, Park R (2008) Guide to SSL VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-113. https://doi.org/10.6028/NIST.SP.800-113

[SP 800-114] Souppaya MP, Scarfone KA (2016) User's Guide to Telework and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-114, Rev. 1. https://doi.org/10.6028/NIST.SP.800-114r1

[SP 800-115] Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical Guide to Information Security Testing and Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-115. https://doi.org/10.6028/NIST.SP.800-115

[SP 800-116] Ferraiolo H, Mehta KL, Ghadiali N, Mohler J, Johnson V, Brady S (2018) A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-116, Rev. 1. https://doi.org/10.6028/NIST.SP.800-116r1

[SP 800-121] Padgette J, Bahr J, Holtmann M, Batra M, Chen L, Smithbey R, Scarfone KA (2017) Guide to Bluetooth Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-121, Rev. 2. https://doi.org/10.6028/NIST.SP.800-121r2

[SP 800-124] Souppaya MP, Scarfone KA (2013) Guidelines for Managing the Security of Mobile Devices in the Enterprise. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-124, Rev. 1. https://doi.org/10.6028/NIST.SP.800-124r1

[SP 800-125B] Chandramouli R (2016) Secure Virtual Network Configuration for Virtual Machine (VM) Protection. (National Institute of Standards and Technology,

Gaithersburg, MD), NIST Special Publication (SP) 800-125B. https://doi.org/10.6028/NIST.SP.800-125B

[SP 800-126] Waltermire DA, Quinn SD, Booth H, III, Scarfone KA, Prisaca D (2018) The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-126, Rev. 3. https://doi.org/10.6028/NIST.SP.800-126r3

[SP 800-128] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128, Includes updates as of October 10, 2019. https://doi.org/10.6028/NIST.SP.800-128

[SP 800-130] Barker EB, Smid ME, Branstad DK, Chokhani S (2013) A Framework for Designing Cryptographic Key Management Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-130. https://doi.org/10.6028/NIST.SP.800-130

[SP 800-137] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137. https://doi.org/10.6028/NIST.SP.800-137

[SP 800-137A] Dempsey KL, Pillitteri VY, Baer C, Niemeyer R, Rudman R, Urban S (2020) Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137A. https://doi.org/10.6028/NIST.SP.800-137A

[SP 800-147] Cooper DA, Polk T, Regenscheid AR, Souppaya MP (2011) BIOS Protection Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-147. https://doi.org/10.6028/NIST.SP.800-147

[SP 800-150] Johnson CS, Waltermire DA, Badger ML, Skorupka C, Snyder J (2016) Guide to Cyber Threat Information Sharing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-150. https://doi.org/10.6028/NIST.SP.800-150

[SP 800-152] Barker EB, Branstad DK, Smid ME (2015) A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-152. https://doi.org/10.6028/NIST.SP.800-152

[SP 800-154] Souppaya MP, Scarfone KA (2016) Guide to Data-Centric System Threat Modeling. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-154.

https://csrc.nist.gov/publications/detail/sp/800-154/draft

[SP 800-156] Ferraiolo H, Chandramouli R, Mehta KL, Mohler J, Skordinski S, Brady S (2016) Representation of PIV Chain-of-Trust for Import and Export. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-156. https://doi.org/10.6028/NIST.SP.800-156

[SP 800-160-1] Ross RS, Oren JC, McEvilley M (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. https://doi.org/10.6028/NIST.SP.800-160v1

[SP 800-160-2] Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2019) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 2. https://doi.org/10.6028/NIST.SP.800-160v2

[SP 800-161] Boyens JM, Paulsen C, Moorthy R, Bartol N (2015) Supply Chain Risk Management Practices for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161. https://doi.org/10.6028/NIST.SP.800-161

[SP 800-162] Hu VC, Ferraiolo DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone KA (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-162, Includes updates as of August 2, 2019. https://doi.org/10.6028/NIST.SP.800-162

[SP 800-166] Cooper DA, Ferraiolo H, Chandramouli R, Ghadiali N, Mohler J, Brady S (2016) Derived PIV Application and Data Model Test Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-166. https://doi.org/10.6028/NIST.SP.800-166

[SP 800-167] Sedgewick A, Souppaya MP, Scarfone KA (2015) Guide to Application Whitelisting. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-167. https://doi.org/10.6028/NIST.SP.800-167

[SP 800-171] Ross RS, Pillitteri VY, Dempsey KL, Riddle M, Guissanie G (2020) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171, Rev. 2. https://doi.org/10.6028/NIST.SP.800-171r2

[SP 800-172] Ross RS, Pillitteri VY, Graubart RD, Guissanie G, Wagner R, Bodeau D (2020) Enhanced Security Requirements for Protecting Controlled Unclassified

Information: A Supplement to NIST Special Publication 800-171 (Final Public Draft). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-172. https://doi.org/10.6028/NIST.SP.800-172-draft

[SP 800-177] Rose SW, Nightingale S, Garfinkel SL, Chandramouli R (2019) Trustworthy Email. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-177, Rev. 1. https://doi.org/10.6028/NIST.SP.800-177r1

[SP 800-178] Ferraiolo DF, Hu VC, Kuhn R, Chandramouli R (2016) A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications: Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-178. https://doi.org/10.6028/NIST.SP.800-178

[SP 800-181] Petersen R, Santos D, Smith MC, Wetzel KA, Witte G (2020) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1

[SP 800-184] Bartock M, Scarfone KA, Smith MC, Witte GA, Cichonski JA, Souppaya MP (2016) Guide for Cybersecurity Event Recovery. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-184. https://doi.org/10.6028/NIST.SP.800-184

[SP 800-188] Garfinkel S (2016) De-Identifying Government Datasets. (National Institute of Standards and Technology, Gaithersburg, MD), Second Draft NIST Special Publication (SP) 800-188. https://csrc.nist.gov/publications/detail/sp/800-188/draft

[SP 800-189] Sriram K, Montgomery D (2019) Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-189. https://doi.org/10.6028/NIST.SP.800-189

[SP 800-192] Yaga DJ, Kuhn R, Hu VC (2017) Verification and Test Methods for Access Control Policies/Models. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-192. https://doi.org/10.6028/NIST.SP.800-192

[IR 7539] Cooper DA, MacGregor WI (2008) Symmetric Key Injection onto Smart Cards. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7539. https://doi.org/10.6028/NIST.IR.7539

[IR 7559] Singhal A, Gunestas M, Wijesekera D (2010) Forensics Web Services (FWS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7559. https://doi.org/10.6028/NIST.IR.7559

[IR 7622] Boyens JM, Paulsen C, Bartol N, Shankles S, Moorthy R (2012) Notional Supply Chain Risk Management Practices for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7622. https://doi.org/10.6028/NIST.IR.7622

[IR 7676] Cooper DA (2010) Maintaining and Using Key History on Personal Identity Verification (PIV) Cards. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7676. https://doi.org/10.6028/NIST.IR.7676

[IR 7788] Singhal A, Ou X (2011) Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7788. https://doi.org/10.6028/NIST.IR.7788

[IR 7817] Ferraiolo H (2012) A Credential Reliability and Revocation Model for Federated Identities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7817. https://doi.org/10.6028/NIST.IR.7817

[IR 7849] Chandramouli R (2014) A Methodology for Developing Authentication Assurance Level Taxonomy for Smart Card-based Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7849. https://doi.org/10.6028/NIST.IR.7849

[IR 7870] Cooper DA (2012) NIST Test Personal Identity Verification (PIV) Cards. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7870. https://doi.org/10.6028/NIST.IR.7870

[IR 7874] Hu VC, Scarfone KA (2012) Guidelines for Access Control System Evaluation Metrics. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7874. https://doi.org/10.6028/NIST.IR.7874

[IR 7956] Chandramouli R, Iorga M, Chokhani S (2013) Cryptographic Key Management Issues & Challenges in Cloud Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7956. https://doi.org/10.6028/NIST.IR.7956

[IR 7966] Ylonen T, Turner P, Scarfone KA, Souppaya MP (2015) Security of Interactive and Automated Access Management Using Secure Shell (SSH). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7966. https://doi.org/10.6028/NIST.IR.7966

[IR 8011-1] Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 1: Overview. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report

(IR) 8011, Volume 1.
https://doi.org/10.6028/NIST.IR.8011-1

[IR 8011-2] Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 2: Hardware Asset Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 2.
https://doi.org/10.6028/NIST.IR.8011-2

[IR 8011-3] Dempsey KL, Eavy P, Goren N, Moore G (2018) Automation Support for Security Control Assessments: Volume 3: Software Asset Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 3.
https://doi.org/10.6028/NIST.IR.8011-3

[IR 8011-4] Dempsey KL, Takamura E, Eavy P, Moore G (2020) Automation Support for Security Control Assessments: Volume 4: Software Vulnerability Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 4.
https://doi.org/10.6028/NIST.IR.8011-4

[IR 8023] Dempsey KL, Paulsen C (2015) Risk Management for Replication Devices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8023.
https://doi.org/10.6028/NIST.IR.8023

[IR 8040] Greene KK, Kelsey JM, Franklin JM (2016) Measuring the Usability and Security of Permuted Passwords on Mobile Platforms. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8040.
https://doi.org/10.6028/NIST.IR.8040

[IR 8062] Brooks S, Garcia M, Lefkovitz N, Lightman S, Nadeau E (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8062.
https://doi.org/10.6028/NIST.IR.8062

[IR 8112] Grassi P, Lefkovitz N, Nadeau E, Galluzzo R, Dinh, A (2018) Attribute Metadata: A Proposed Schema for Evaluating Federated Attributes. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8112.
https://doi.org/10.6028/NIST.IR.8112

[IR 8179] Paulsen C, Boyens JM, Bartol N, Winkler K (2018) Criticality Analysis Process Model: Prioritizing Systems and Components. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8179.
https://doi.org/10.6028/NIST.IR.8179

[IR 8272] Paulsen C, Winkler K, Boyens JM, Ng J, Gimbi J (2020) Impact Analysis Tool for Interdependent Cyber Supply Chain Risks. (National Institute of

Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8272.
https://doi.org/10.6028/NIST.IR.8272

その他の出版物およびウェブサイト

[USCERT IR] Department of Homeland Security, *US-CERT Federal Incident Notification Guidelines*, April 2017.
https://us-cert.cisa.gov/incident-notification-guidelines

[DHS TIC] Department of Homeland Security, *Trusted Internet Connections (TIC)*.
https://www.dhs.gov/trusted-internet-connections

[DSB 2017] Department of Defense, Defense Science Board, *Task Force on Cyber Deterrence*, February 2017.
https://dsb.cto.mil/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf

[DOD STIG] Defense Information Systems Agency, *Security Technical Implementation Guides (STIG)*.
https://public.cyber.mil/stigs

[DODTERMS] Department of Defense, *Dictionary of Military and Associated Terms*.
https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

[FED PKI] General Services Administration, *Federal Public Key Infrastructure*.
https://www.idmanagement.gov/topics/fpki

[FISMA IMP] Federal Information Security Modernization Act (FISMA) Implementation Project.
https://nist.gov/RMF

[IETF 4949] Internet Engineering Task Force (IETF), Request for Comments: 4949, *Internet Security Glossary*, Version 2, August 2007.
https://tools.ietf.org/html/rfc4949

[IETF 5905] Internet Engineering Task Force (IETF), Request for Comments: 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*, June 2010.
https://tools.ietf.org/pdf/rfc5905.pdf

[LAMPSON73] B. W. Lampson, *A Note on the Confinement Problem*, Communications of the ACM 16, 10, pp. 613-615, October 1973.

[NARA CUI] National Archives and Records Administration, Controlled Unclassified Information (CUI) Registry.
https://www.archives.gov/cui

[NIAP CCEVS] National Information Assurance Partnership, *Common Criteria Evaluation and Validation Scheme*.
https://www.niap-ccevs.org

[NIST CAVP] National Institute of Standards and Technology (2020) *Cryptographic Algorithm Validation Program*. Available at
https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

[NIST CMVP] National Institute of Standards and Technology (2020) *Cryptographic*

Module Validation Program. Available at https://csrc.nist.gov/projects/cryptographic-module-validation-program

[NIST CSF] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[NIST PF] National Institute of Standards and Technology (2020) Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.01162020

[NCPR] National Institute of Standards and Technology (2020) *National Checklist Program Repository*. Available at https://nvd.nist.gov/ncp/repository

[NVD 800-53] National Institute of Standards and Technology (2020) *National Vulnerability Database: NIST Special Publication 800-53 [database of controls]*. Available at https://nvd.nist.gov/800-53

[NEUM04] *Principled Assuredly Trustworthy Composable Architectures*, P. Neumann, CDRL A001 Final Report, SRI International, December 2004. http://www.csl.sri.com/users/neumann/chats4.pdf

[NSA CSFC] National Security Agency, *Commercial Solutions for Classified Program (CSfC)*. https://www.nsa.gov/resources/everyone/csfc

[NSA MEDIA] National Security Agency, *Media Destruction Guidance*. https://www.nsa.gov/resources/everyone/media-destruction

[ODNI CTF] Office of the Director of National Intelligence (ODNI) Cyber Threat Framework. https://www.dni.gov/index.php/cyber-threat-framework

[POPEK74] G. Popek, *The Principle of Kernel Design*, in 1974 NCC, AFIPS Cong. Proc., Vol. 43, pp. 977-978.

[SALTZER75] J. Saltzer and M. Schroeder, *The Protection of Information in Computer Systems*, in Proceedings of the IEEE 63(9), September 1975, pp. 1278-1308.

[SP 800-53 RES] NIST Special Publication 800-53, Revision 5 Resource Center. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[USGCB] National Institute of Standards and Technology (2020) *United States Government Configuration Baseline*. Available at https://csrc.nist.gov/projects/united-states-government-configuration-baseline

付属書 A

用語集

一般的な用語と定義

付属書 A は、NIST SP 800-53 で使用されている用語の定義を提供する。本出版物で使用されている用語のソースは、適宜引用されている。引用が記載されていない場合、定義のソースは SP 800-53 である。

アクセス制御 (access control) [FIPS 201-2]	情報および関連する情報処理サービスを取得および使用するための特定の要求、ならびに特定の物理的施設（例えば、連邦政府の建物、軍事施設、および国境検問所）に入るための特定の要求を許可または拒否するプロセス。
適切なセキュリティ (adequate security) [OMB A-130]	情報の認可されていない使用、開示、中断、変更、または破壊から生じるリスクに見合ったセキュリティ保護。これには、政府機関に代わってホストされる情報、および政府機関が使用する情報システムとアプリケーションなどが効果的に運用され、費用効果の高いセキュリティ管理策を適用することにより、適切な機密性、完全性、可用性の保護を提供することが含まれる。
持続的標的型攻撃（APT 攻撃） (advanced persistent threat) [SP 800-39]	高度なレベルの専門知識と莫大なリソースを保有し、例えば、サイバー攻撃、物理攻撃、詐欺などの複数の攻撃ベクトルを使用して目的を達成する機会を生み出す敵対者。APT 攻撃の目的には、通常、情報を漏出させること、ミッション、プログラム、組織の重要な側面を弱体化または妨害すること、もしくは、将来的にこれらの目的を実行するために自らを配置することを目的として、標的組織の IT インフラ内に足場を確立し拡張することなどが含まれる。持続的標的型攻撃は、長期間にわたって繰り返しその目的を追求し、攻撃に抵抗する防御側の取り組みに適応し、その目的を実行するために必要な相互作用のレベルを確固として維持する。
政府機関 (agency) [OMB A-130]	執行機関または省、軍事部門、連邦政府法人、連邦政府管理法人、または連邦政府の行政府におけるその他の機関、または独立した規制機関。 *執行機関*（*executive agency*）を参照。
オールソースインテリジェンス (all-source intelligence) [DODTERMS]	すべての情報ソースを組み込んだインテリジェンス（情報収集および分析活動）の成果物および／または組織と活動で、人的リソースからのインテリジェンス、データの量的および質的分析によって行う科学的かつ技術的なインテリジェンス、画像によるインテリジェンス、電気信号によるインテリジェンス、および終了したインテリジェンス成果物の中のオープンソースとなっているデータの活用などが多い。
アプリケーション (Application) [SP 800-37]	情報システムによって受入れ運用（ホスト）されるソフトウェアプログラム。
アセスメント (assessment)	*管理策アセスメント*（*control assessment*）または*リスクアセスメント*（*risk assessment*）を参照。

アセスメント計画
(assessment plan)
セキュリティおよびプライバシー管理策アセスメントの目的と、そのようなアセスメントを実施する方法の詳細なロードマップ。

アセッサー
(assessor)
セキュリティまたはプライバシー管理策のアセスメントを実施する責任がある個人、グループ、または組織。

設定操作
(assignment operation)
組織が、管理策または拡張管理策に対して組織が定める特定の値を設定することができる管理策パラメータ(例えば、通知される役割のリストやテスト頻度の値を設定する)。
組織が定める管理策パラメータ(*organization-defined control parameters*)と*選択操作*(*selection operation*)を参照。

保証
(assurance)
[ISO/IEC 15026, Adapted]
[セキュリティまたはプライバシー]に関するクレームが達成されたか、または達成されるであろうという正当な確信の根拠。
注 1: 保証は、通常、一連の特定のクレームに対して得られる。そのようなクレームの範囲と焦点は異なっていてもよく(例えば、セキュリティに関するクレーム、安全に関するクレーム)、クレーム自体が相互に関連していてもよい。
注 2: 保証は、クレームを立証するための信頼できるエビデンスを生成する技法および方法を通じて得られる。

攻撃対象領域
(attack surface)
攻撃者がシステム、システムコンポーネント、または環境に侵入したり、影響を与えたり、データを抽出したりすることを試みることができる、システム、コンポーネント、または環境の境界上の一連のポイント。

監査
(audit)
[CNSSI 4009]
確立されたポリシーと運用手順への準拠を確実にするために、システム制御の妥当性を評価するための記録と活動に関する独立したレビューと検査。

監査ログ
(audit log)
[CNSSI 4009]
特定の期間に実行されたシステムアクセスおよび操作の記録を含む、システム活動の時系列の記録。

監査記録
(audit record)
監査されたイベントに関連する監査ログの個々のエントリ。

監査記録の整理
(audit record reduction)
収集された監査情報を操作し、アナリストにとってより意味のある要約形式に編成するプロセス。

監査証跡
(audit trail)
セキュリティ関連のトランザクションにおける特定の操作、手順、またはイベントを取り巻く、または導く一連の活動を、開始から結果まで再構築および調査する時系列の記録。

認証
(authentication)
[FIPS 200]
多くの場合、システム内のリソースへのアクセスを許可するための前提条件として、ユーザ、プロセス、またはデバイスのアイデンティティを検証すること。

オーセンティケータ
(authenticator)
要求者のアイデンティティを認証するために使用される要求者が所有し管理するもの(通常は暗号モジュールまたはパスワード)で、以前はトークンと呼ばれていた。

真正性
(authenticity)
本物であり、検証および信頼できる特性。伝送、メッセージ、またはメッセージ発信者の有効性に対する信頼。
認証(*authentication*)を参照。

認可 (authorization) [CNSSI 4009]	ユーザ、プログラム、プロセスに付与されたアクセス権、またはそれらの権限を付与する行為。
認可境界 (authorization boundary) [OMB A-130]	認可権限のある担当者によって操作が認可される、情報システムのすべてのコンポーネント。これには、情報システムが接続されている個別に認可されたシステムは含まれない。
運用認可 (authorization to operate) [OMB A-130]	連邦政府の責任者または、機関の運用(ミッション、機能、イメージ、または評判を含む)、セキュリティおよびプライバシー管理策の実装に基づく資産、個人、他の組織、および国家に対するリスクを明示的に受け入れる情報システムの運用認可担当官による正式な決定。認可は、政府機関の情報システムが継承する共通管理策にも適用される。
認可権限のある担当者 (authorizing official) [OMB A-130]	情報システムの運用、または政府機関の運営(ミッション、機能、イメージ、または評判を含む)、政府機関の資産、個人、他の組織、および国家に対する許容可能なレベルのリスクで、指定された一連の共通管理策の使用を認可する(すなわち、責任を負う)権限を有する連邦政府責任者または幹部。
可用性 (availability) [FISMA]	情報へのタイムリーで信頼性の高いアクセスと使用を確保すること。
ベースライン (baseline)	*管理策ベースライン*(*control baseline*)を参照。
ベースライン構成 (baseline configuration) [SP 800-128, Adapted]	特定の時点で正式にレビューおよび合意された、変更管理手順によってのみ変更できる、システムまたはシステム内の構成アイテムに関する文書化された仕様のセット。
境界 (boundary) [CNSSI 4009]	システムの物理的または論理的境界。 *認可境界*(*authorization boundary*)と*インタフェース*(*interface*)も参照。
境界保護 (boundary protection)	境界保護デバイスを使用して悪意のある通信やその他の認可されていない通信を防止および検知するための、システムの外部インタフェースにおける通信の監視および制御。
境界保護デバイス (boundary protection device)	接続されたシステムの様々なシステムセキュリティポリシーの裁定を容易にする、または境界保護機能を提供するデバイス(例えば、ゲートウェイ、ルータ、ファイアウォール、ガード、または暗号化トンネル)。境界には、システムの認可境界、組織のネットワーク境界、または組織が定める論理境界などがある。
ブリーチ (breach) [OMB M-17-12]	認可されたユーザ以外の人が個人情報にアクセスする、またはアクセスする可能性がある;もしくは、認可されたユーザが認可されている目的以外の目的で個人情報にアクセスする場合に生じる、管理機能の損失、危殆化、認可されていない開示、認可されていない取得、または類似の出来事。
幅 (breadth)	アセスメントに含まれるアセスメント対象の範囲または適用範囲に対処するアセスメント方法に関連する属性。

[SP 800-53A]

ケイパビリティ（能力） (capability)	技術的、物理的、および手順上の手段によって実装される、相互に強化するセキュリティおよび／またはプライバシー管理策の組み合わせ。このような管理策は、一般に、情報セキュリティまたはプライバシー関連の一般的な目的を達成するために選択される。
一元管理 (central management)	選択されたセキュリティおよびプライバシー管理策と関連プロセスの組織全体の管理と実装。一元管理には、組織が定めた一元的に管理されたセキュリティとプライバシー管理策およびプロセスの計画、実装、評価、認可、および監視が含まれる。
チェックサム (checksum) [IETF 4949]	データの変更を検知するために（a）データオブジェクトの内容に依存する関数によって計算される、（b）オブジェクトとともに格納または伝送される値。
最高情報責任者 (chief information officer) [OMB A-130]	組織の長および他の幹部職員に助言およびその他の支援を行う責任者であり、情報資源が組織の戦略目標と情報資源管理目標を達成すべくIT資産が確実に取得されること；および、公的機関による情報収集の負担の軽減を含め、組織が、情報ポリシーへの準拠および情報リソース管理の責任を、迅速かつ効率的かつ効果的に履行することを保証する責任を負う。
最高情報セキュリティ責任者 (chief information security officer)	*政府機関の情報セキュリティ責任者*（*senior agency information security officer*）を参照。
国家機密情報 (classified information)	*国家機密安全保障情報*（*classified national security information*）を参照。
国家機密安全保障情報 (classified national security information) [EO 13526]	認可されていない開示からの保護を要求するために大統領令（EO：Executive Order）13526号またはその前身の命令に従って決定された情報であり、文書形式の場合には機密扱いであることを示すマークが付けられている。
コモディティサービス (commodity service)	商業サービスプロバイダが大規模で多様な消費者に提供するシステムサービス。コモディティサービスを取得または利用する組織は、プロバイダの管理構造および運用に対する可視性が限定されており、組織はサービスレベル契約を交渉することができる場合があるが、通常、組織は、プロバイダに特定のセキュリティまたはプライバシー管理策の実装を要求することは出来ない。
通信事業者 (common carrier)	一般に公開されている有料の通信伝送サービスを提供する電気通信事業者。
共通管理策 (common control) [OMB A-130]	複数の情報システムまたはプログラムによって継承されるセキュリティまたはプライバシー管理策。

共通管理策の提供者 (common control provider) [SP 800-37]	共通管理策（すなわち、システムによって継承可能なセキュリティまたはプライバシー管理策）の策定、実装、アセスメント、監視の責任を負う組織の担当者。
コモンクライテリア (common criteria) [CNSSI 4009]	製品およびシステムのセキュリティ機能および保証要件を指定するための包括的かつ厳密な方法を提供する管理文書。
共通セキュア構成 (common secure configuration) [SP 800-128]	所定の情報技術プラットフォームのための特定のセキュアな構成設定を規定する、認められた規格化され確立されたベンチマーク。
代替管理策 (compensating controls)	NIST SP 800-53B に記載されているベースラインの管理策の代わりに採用されるセキュリティおよびプライバシー管理策であり、システムまたは組織に同等または同様の保護を提供する。
コンポーネント (component)	*システムコンポーネント*（*system component*）を参照。
機密性 (confidentiality) [FISMA]	個人のプライバシーおよび専有情報を保護するための手段を含め、情報へのアクセスおよび開示に関する認可された制限を維持すること。
構成変更管理 (configuration control) [SP 800-128]	システムの実装前、実装中、および実装後の不適切な変更からシステムを保護するために、ハードウェア、ファームウェア、ソフトウェア、およびドキュメントへの変更を管理するプロセス。
構成アイテム (configuration item) [SP 800-128]	構成管理のために指定され、構成管理プロセスにおいて単一のエンティティとして扱われるシステムコンポーネントの集合体。
構成管理 (configuration management) [SP 800-128]	システム開発ライフサイクル全体を通して、情報技術製品およびシステムの構成を初期化、変更、監視するためのプロセスを管理することによって、情報技術製品およびシステムの完全性を確立し維持することに焦点を当てた活動の集合。
構成設定 (configuration settings) [SP 800-128]	ハードウェア、ソフトウェア、またはファームウェアで変更することができる、システムのセキュリティ態勢および／または機能性に影響を与える一連のパラメータ。
継続的監視 (continuous monitoring) [SP 800-137]	組織のリスクに関する判断をサポートするための継続的な意識の維持すること。
管理策 (control)	*セキュリティ管理策*（*security control*）または*プライバシー管理策*（*privacy control*）を参照。
管理策アセスメント (control assessment) [SP 800-37]	管理策が適切に実装され、意図したとおりに運用され、システムまたは組織のセキュリティ要件またはプライバシー要件に関して目的の結果を生成するために、情報システムまたは組織における管理策のテストまたは評価すること。

管理策アセッサー (control assessor)	*アセッサー*(*assessor*)を参照。
管理策ベースライン (control baseline) [SP 800-53B]	関心のあるグループ、組織、またはコミュニティの保護ニーズに対応するために特別に構築され、事前に規定された管理策のセット。 *プライバシー管理策ベースライン*(*privacy control baseline*)または*セキュリティ管理策ベースライン*(*security control baseline*)を参照。
管理策の有効性 (control effectiveness)	セキュリティまたはプライバシー管理策が情報セキュリティまたはプライバシーリスクの低減に寄与するかどうかの尺度。
拡張管理策 (control enhancement)	管理策に追加の関連する機能性を組み込み、管理策の強度を高め、または管理策への保証の追加を行なうための、セキュリティまたはプライバシー管理策の拡張。
管理策の継承 (control inheritance)	システムまたはアプリケーションが、システムまたはアプリケーションに対して責任を負うエンティティ以外のエンティティ;あるいはシステムまたはアプリケーションが存在する組織の内部または外部のエンティティによって策定、実装、アセスメント、認可、および監視されるセキュリティまたはプライバシー管理策(または管理策の一部)から保護を受ける状況。 *共通管理策*(*common control*)を参照。
管理策パラメータ (control parameter)	*組織が定める管理策パラメータ*(*organization-defined control parameter*)を参照。
管理エリア (controlled area)	提供される物理的および手順上の保護が、情報および/または情報システムを保護するために要求された要件を満たすのに十分であると組織が確信しているエリアまたは空間。
制御されたインタフェース (controlled interface)	セキュリティポリシーを適用し、接続されたシステム間の情報の流れを制御する一連のメカニズムを備えたシステムへのインタフェース。
管理対象非機密情報 (controlled unclassified information) [32 CFR 2002]	法律、規則、または政府全体のポリシーにより、政府機関が保全措置または配付管理の適用を要求または許可する、政府が作成または所有、または企業が政府のために、または政府に代わって作成または所有する情報。ただし、CUI には、国家機密情報または非行政機関が独自のシステムで保持および維持している、行政機関または行政機関の代理人からのものではない、またはそれらのために作成または所有されていない情報は含まない。
偽造品 (counterfeit) [SP 800-161]	アイテムの法的に認可された出所以外の出所によって識別、マーク、および/または変更されており、法的に認可された出所の認可されたアイテムであると偽って伝えられている認可されていないコピーまたは代替品。
対策 (countermeasures) [FIPS 200]	システムの脆弱性を低減するアクション、デバイス、手順、技法、またはその他の手段。セキュリティ管理策および保全措置と同義。

カバートチャネル (covert channel) [CNSSI 4009]	2 つの協力エンティティが、システムのセキュリティポリシーには違反するが、エンティティの認可されたアクセス権限を超えない方法で情報を転送できるようにする、意図しない、または認可されていないシステム内チャネル。
カバートチャネル分析 (covert channel analysis) [CNSSI 4009]	セキュリティポリシーモデルとそれに続く下位レベルのプログラム記述が情報への認可されていないアクセスを許可する可能性がある範囲の決定。
カバートストレージチャネル (covert storage channel) [CNSSI 4009]	あるシステムエンティティが、後に直接または間接的に 2 番目のエンティティによって読み取られるストレージ位置に直接または間接的に書き込むことによって、別のエンティティに情報を送信できるようにするシステム機能。
カバートタイミングチャネル (covert timing channel) [CNSSI 4009, Adapted]	1 つのシステムエンティティが、2 番目のエンティティによって監視されるシステム応答時間に影響を与えるような方法で、システム資源の使用を調整することによって、別のシステムエンティティに情報を通知できるようにするシステム機能。
クレデンシャル (credential) [SP 800-63-3]	1 つまたは複数の識別子、および（オプションで）追加の属性を介して、加入者が所有および管理する少なくとも 1 つの認証子に、アイデンティティを正式に関連付けするオブジェクトまたはデータ構造。
重要インフラ (critical infrastructure) [USA PATRIOT]	システムと資産は、物理的であれ仮想であれ、米国にとって非常に重要であるため、そのようなシステムと資産の機能不全または破壊は、安全保障、国家経済安全保障、国家公衆衛生または安全、またはそれらの問題のあらゆる組み合わせを弱体化させるインパクトを与える。
クロスドメインソリューション (cross domain solution) [CNSSI 1253]	異なるセキュリティドメイン間で情報に手動および／または自動でアクセスおよび／または情報を転送する機能を提供する、制御されたインタフェースの形式。
暗号モジュール (cryptographic module) [FIPS 140-3]	承認済みのセキュリティ機能（暗号アルゴリズムおよび鍵生成を含む）を実装し、暗号境界内に含まれるハードウェア、ソフトウェア、またはファームウェアのセット。
サイバーセキュリティ (cybersecurity) [OMB A-130]	可用性、完全性、認証、機密性、否認防止を保証するための、コンピュータ、電子通信システム、電子通信サービス、有線通信、およびそれらに含まれる情報の損傷の防止、保護、および復元。
サイバースペース (cyberspace) [CNSSI 4009]	インターネット、通信ネットワーク、コンピュータシステム、および重要産業における組み込みプロセッサとコントローラを含む、情報技術インフラの相互依存ネットワーク。
データアクション (data action) [IR 8062]	個人情報を取扱うシステム操作。
データマイニング (data mining)	データまたは知識の検出を目的として、大規模なデータセット内の相関またはパターンを見つけようとする分析プロセス。

匿名化 (de-identification) [ISO 25237]	識別データのセットとデータ主体との間の関連を削除するプロセスの総称。
広範囲な防御 (defense in breadth) [CNSSI 4009]	システム、ネットワーク、または製品の設計および開発；製造；包装；アセンブリ；システム統合；配布；オペレーション；メンテナンスおよび終息を含む、システム、ネットワーク、またはサブコンポーネントのライフサイクルのあらゆる段階で、悪用可能な脆弱性のリスクを特定、管理、および軽減することを目的とした、計画的かつ体系的な一連の多くの専門分野にわたる措置。
多層防御 (defense in depth)	人、技術、運用のケイパビリティを統合して、組織の複数のレイヤーとミッションにわたって可変の障壁を確立する情報セキュリティ戦略。
深さ (depth) [SP 800-53A]	その方法の適用に関連する厳密さと詳細レベルに対処するアセスメント方法に関連する属性。
開発者 (developer)	システム、システムコンポーネント、またはシステムサービスの開発者または製造者；システムインテグレータ；ベンダおよび製品の再販業者を含む一般用語。システム、コンポーネント、またはサービスの開発は、組織内で、または外部エンティティを通じて行うことができる。
デジタル媒体 (digital media)	データが（アナログではなく）デジタル形式で格納される電子媒体の形態。
任意アクセス制御 (discretionary access control)	システム内のすべてのサブジェクトおよびオブジェクトに適用されるアクセス制御ポリシー。ポリシーは、情報へのアクセスを許可されたサブジェクトが次の 1 つ以上を実行できることを指定する。他のサブジェクトまたはオブジェクトに情報を渡す。他の主体にその権限を与える。サブジェクト、オブジェクト、システム、またはシステムコンポーネントのセキュリティ属性を変更する。新しく作成または改訂されたオブジェクトに関連付けるセキュリティ属性を選択する；または、アクセス制御を管理する規定を変更する。必須アクセス制御はこのケイパビリティを制限するもの。
分離可能性 (disassociability) [IR 8062]	システムの運用要件を超えて、個人またはデバイスとの関連なしに、個人情報またはイベントの処理を可能にすること。
ドメイン (domain)	一般的なセキュリティポリシー、セキュリティモデル、またはセキュリティアーキテクチャで規定されているように、リソースにアクセスする権限を持つシステム資源のセットとシステムエンティティのセットを含む環境または状況。 *セキュリティドメイン*（*security domain*）を参照。
企業 (enterprise) [CNSSI 4009]	ミッション／目標が規定され、規定された境界を持ち、システムを使用しそのミッションを実行し、独自のリスクとパフォーマンスを管理する責任を負う組織。企業は、取得、プログラムマネジメ

	ント、人事、財務管理、セキュリティ、ミッションマネジメントのビジネス面のすべてまたは一部で構成される。 *組織*(*organization*)を参照。
エンタープライズアーキテクチャ (enterprise architecture) [OMB A-130]	以下に規定される戦略的情報資産基盤:ミッション;ミッションを遂行するために必要な情報;ミッションを遂行するために必要な技術;変化するミッションニーズに対応して新しい技術を実装するための移行プロセス;および、ベースラインアーキテクチャ;ターゲットアーキテクチャ;年次計画などを含む。
運用環境 (environment of operation) [OMB A-130]	情報システムが情報を処理、保存、伝送する物理的環境。
イベント (event) [SP 800-61, Adapted]	システム内で観察可能な事象。
執行機関 (executive agency) [OMB A-130]	合衆国法典第 5 編第 101 条(5 U.S.C. Sec. 101)で指定された執行部門、合衆国法典第 5 編第 102 条(5 U.S.C. Sec. 102)で指定された軍事部門、合衆国法典第 5 編第 104 条 1 項(5 U.S.C. Sec. 104(1))で規定された独立組織、合衆国法典第 31 編第 91 章(31 U.S.C. Chapter 91)の規定の対象である政府完全所有法人。
漏出 (exfiltration)	システムからの情報の認可されていない転送。
外部システム(またはコンポーネント) (external system (or component))	組織のシステムによって使用されているが、その一部ではなく、必要なセキュリティ管理策およびプライバシー管理策の実装または管理策の有効性のアセスメントを組織が直接管理していないシステムまたはシステムのコンポーネント。
外部システムサービス (external system service)	外部サービスプロバイダによって提供され、組織が必要なセキュリティおよびプライバシー管理策の実施や管理策の効果に関するアセスメントを直接管理できないシステムサービス。
外部システムサービスプロバイダ (external system service provider)	ジョイントベンチャー、事業パートナーシップ、アウトソーシング契約(契約、組織間契約、基幹業務契約など)、ライセンス契約/またはサプライチェーンの交換など、様々なコンシューマーとプロデューサーの関係を通じて組織に外部システムサービスを提供するプロバイダ。
外部ネットワーク (external network)	当該組織によって管理されていないネットワーク。
フェイルオーバー (failover)	以前にアクティブだったシステムの障害または異常終了時に、自動的に(通常は人の介入や警告なしに)冗長システムまたはスタンバイシステムに切り替えるケイパビリティ。
連邦政府情報システム (federal information system)	執行機関、執行機関の契約事業者、または執行機関に代わって他の組織が使用または運用する情報システム。

[OMB A-130]

FIPS 検証済み暗号技術
(FIPS-validated cryptography)
暗号モジュール認証制度(CMVP)によって妥当性確認された、FIPS 140-3(改正)に定められた要件を満たす暗号モジュール。CMVP 認証の前提条件として、暗号モジュールは、暗号アルゴリズム認証制度(CAVP)による検証テストに合格した暗号アルゴリズムの実装を採用する必要がある。
NSA 承認済み暗号技術(*NSA-approved cryptography*)を参照。

ファームウェア
(firmware)
[CNSSI 4009]
ハードドウェアに保存されたコンピュータプログラムとデータ。通常、読み取り専用メモリ(ROM)やプログラム可能な読み取り専用メモリ(PROM)に保存され、プログラムの実行中にプログラムとデータを動的に書き込んだり変更したりすることができない。
ハードウェア(*hardware*)と*ソフトウェア*(*software*)を参照。

ハードウェア
(hardware)
[CNSSI 4009]
システムの有形な物理コンポーネント。
ソフトウェア(*software*)と*ファームウェア*(*firmware*)を参照。

高インパクトシステム
(high-impact system)
[FIPS 200]
少なくとも 1 つのセキュリティ目的(すなわち、機密性、完全性、または可用性)に対して FIPS 199 の潜在的インパクト値「高」が設定されているシステム。

ハイブリッド管理策
(hybrid control)
[OMB A-130]
一部は共通管理策として、また一部はシステム固有管理策として情報システムのために実装されるセキュリティまたはプライバシー管理策。

識別子
(identifier)
[FIPS 201-2]
個人アイデンティティおよび関連する属性を表すために使用される一意のデータ。名前またはカード番号は、識別子の例である。特定のエンティティ、オブジェクト、またはグループを示すためにシステムによって使用される一意のラベル。

インパクト
(impact)
情報またはシステムの機密性、完全性、または可用性の喪失が、組織の運営、組織の資産、個人、他の組織、または国家(米国の国家安全保障上の利益を含む)に及ぼす影響。

インパクト値
(impact value)
[FIPS 199]
情報の機密性、完全性、または可用性の侵害から生じる可能性のある最悪のケースをアセスメントした潜在的インパクトを「低」、「中」、「高」の値で表したもの。

インシデント
(incident)
[FISMA]
法的権限なしに、情報または情報システムの機密性、完全性、または可用性を実際にまたは差し迫って危険にさらす出来事;あるいは、法律、セキュリティポリシー、セキュリティ手順、または利用ポリシーの違反または違反の差し迫った脅威を構成する出来事。

産業用制御システム
(industrial control system)
[SP 800-82]
監視制御およびデータ取得(SCADA)システム、分散制御システム(DCS)、および産業分野や重要なインフラストラクチャに存在するプログラマブル・ロジック・コントローラー(PLC)などの制御システム構成など、いくつかのタイプの制御システムを包含する一般用語。産業用制御システムは、一緒に作用して産業上の目的(例えば、製造物、エネルギーの輸送)を達成するために作用する制御コンポーネント(例えば、電気、機械、油圧、空気圧)の組み合わせからなる。、

情報 (information) [OMB A-130]	テキスト、数値、グラフィック、地図、叙述、電子、または視聴覚形式を含む、あらゆる媒体または形態の事実、データ、意見などの知識の伝達または表現。
情報フロー制御 (information flow control)	システムまたは組織内の情報転送がセキュリティポリシーに違反して行われないようにするための制御。
情報漏えい (information leakage)	信頼できない環境への意図的または意図的でない情報の公表。
情報オーナー (information owner) [SP 800-37]	特定の情報に対する法的または運用上の権限を有し、その生成、収集、処理、配布、および廃棄の管理を確立する責任を有する職員。
情報リソース (information resources) [OMB A-130]	人事、装置、資金、情報技術などの情報および関連リソース。
情報セキュリティ (information security) [OMB A-130]	機密性、完全性、可用性を提供するために、情報およびシステムを認可されていないアクセス、使用、開示、中断、変更、または破壊から保護すること。
情報セキュリティアーキテクチャ (information security architecture) [OMB A-130]	企業のセキュリティプロセス、セキュリティシステム、職員および組織のサブユニットの構造と動作を説明し、企業のミッションおよび戦略計画との整合性を示す、エンタープライズアーキテクチャに組み込まれた不可欠な部分。
情報セキュリティポリシー (information security policy) [CNSSI 4009]	組織が情報を管理、保護、および配布する方法を定める指令、規則、ルールおよびプラクティスの集合。
情報セキュリティプログラム計画 (information security program plan) [OMB A-130]	組織全体の情報セキュリティプログラムのセキュリティ要件の概要を提供し、それらの要件を満たすために導入または計画されているプログラムマネジメント管理策や共通管理策について説明する正式な文書。
情報セキュリティリスク (information security risk) [SP 800-30]	情報および／またはシステムの認可されていない、使用、開示、中断、変更、または破壊の可能性による、組織の運営（ミッション、機能、イメージ、評判を含む）、組織資産、個人、他の組織、および国家に対するリスク。
情報スチュワード (information steward) [SP 800-37]	特定の情報について法的または運用上の権限を有し、その生成、収集、処理、配布、および廃棄の管理を確立する責任を有する政府機関の職員。
情報システム (information system) [USC 3502]	情報の収集、処理、維持、使用、共有、配布、または廃棄のために組織された個別の一連の情報リソース。

情報技術 (information technology) [USC 11101]	政府機関によるデータまたは情報の自動取得、保存、分析、評価、操作、管理、移動、制御、表示、切り替え、交換、送信、または受信で使用される、あらゆるサービス、装置、または相互接続された装置のシステムやサブシステム。本定義の目的においては、政府機関が直接使用するサービスや装置、もしくは、その使用（またはサービスの実施や製品の提供においてかなりの程度その使用）を必要とする政府機関との契約に基づいて契約事業者が使用するサービスや装置が含まれる。情報技術には、コンピュータ、補助装置（セキュリティと監視に必要な映像周辺機器、入力、出力、および記憶デバイスを含む）、コンピュータの中央処理装置によって制御されるように設計された周辺装置、ソフトウェア、ファームウェアおよび類似の手順、サービス（クラウドコンピューティングおよびヘルプデスクサービス、または装置やサービスのライフサイクルの任意のポイントをサポートするその他の専門サービスを含む）、および関連リソースが含まれる。情報技術には、その使用を必要としない契約に付随して、契約事業者が取得した装置は含まれない。
情報技術製品 (information technology product)	*システムコンポーネント*（*system component*）を参照。
情報タイプ (information type) [FIPS 199]	組織によって、または場合によっては特定の法律、大統領令、指令、ポリシー、または規則によって定義された特定の分類の情報（プライバシー、医療、所有、財務、調査、契約事業者に依存する、セキュリティ管理など）。
インサイダー (insider) [CNSSI 4009, Adapted]	職員、施設、情報、装置、ネットワーク、またはシステムを含む組織のソースへのアクセスが認可された人物。
インサイダー脅威 (insider threat) [CNSSI 4009, Adapted]	インサイダーが、組織の運営、組織の資産、個人、他の組織、および国家のセキュリティに損害を与えるために、故意または無意識に、認可されたアクセスを使用する脅威。この脅威には、スパイ活動、テロ、国家安全保障情報の認可されていない開示、組織のリソースやケイパビリティの喪失または劣化による損害が含まれまる。
インサイダー脅威対策プログラム (insider threat program) [CNSSI 4009, Adapted]	組織によって認可され、情報の認可されていない開示を阻止、検知、および軽減するために使用されるケイパビリティの調整された集合。
インタフェース (interface) [CNSSI 4009]	相互作用が発生する独立したシステムまたはモジュール間の共通境界。
完全性 (integrity) [FISMA]	不適切な情報の変更または破壊から保護すること。情報の否認防止および真正性の確保を含む。
内部ネットワーク (internal network)	セキュリティ管理策の確立、維持、およびプロビジョニングが、組織の従業員または契約事業者の直接の管理下にあるネットワーク。組織が管理するエンドポイント間に実装された暗号カプ

	セル化または類似のセキュリティ技術は、(少なくとも機密性と完全性に関して)同じ影響をもたらす。内部ネットワークは通常、組織が所有しているが、組織が所有していない場合でも、組織が管理している場合がある。
ラベル (label)	*セキュリティラベル*(*security label*)を参照。
最小特権 (least privilege) [CNSSI 4009]	各エンティティに、そのエンティティの機能を実行するために必要な最小限のシステム資源と認可が付与されるようにセキュリティアーキテクチャが設計されるという原則。
ローカルアクセス (local access)	ネットワークを使用せずに直接接続を介して通信するユーザ(またはユーザに代わって動作するするプロセス)が組織のシステムにアクセスすること。
論理アクセス制御システム (logical access control system)	ワークステーション、ネットワーク、アプリケーション、データベースなど、1 つ以上のコンピュータシステム資源にアクセスする個人の能力を制御する自動システム。論理アクセス制御システムでは、PIN、カード、生体認証、またはその他のトークンなどのメカニズムを使用して、個人のアイデンティティを検証する必要がある。組織内での役割と責任に応じて、異なる個人に異なるアクセス権限を割り当てることができる。
低インパクトシステム (low-impact system) [FIPS 200]	3 つのセキュリティ目的(すなわち、機密性、完全性、可用性)すべてに対して FIPS 199 の潜在的インパクト値「低」が設定されているシステム。
悪意のあるコード (malicious code)	システムの機密性、完全性、または可用性に有害なインパクトを及ぼす認可されていないプロセスを実行することを目的としたソフトウェアまたはファームウェア。ホストに感染するウイルス、ワーム、トロイの木馬、またはその他のコードベースのエンティティ。スパイウェアや一部のアドウェアも悪意のあるコードの例である。
管理されたインタフェース (managed interface)	自動メカニズムまたはデバイスを使用して境界保護機能を提供するシステム内のインタフェース。
必須アクセス制御 (mandatory access control)	システム内のすべてのサブジェクトおよびオブジェクト全体に均一に適用されるアクセス制御ポリシー。情報へのアクセスが許可されたサブジェクトは、次の制約を受ける;認可されていないサブジェクトまたはオブジェクトに情報を渡す;他のサブジェクトにその特権を付与する;サブジェクト、オブジェクト、システム、またはシステムコンポーネントの 1 つ以上のセキュリティ属性を変更する;新しく作成または変更されたオブジェクトに関連付けるセキュリティ属性を選択する;または、アクセス制御を管理するための規定を変更する。組織が定めるサブジェクトには、上記の制約の一部またはすべてによって制約されない組織が定める特権を、明示的に付与することができる(すなわち、信頼できるサブジェクトである)。必須アクセス制御は、任意アクセス制御の一種と見なされる。
マーキング	*セキュリティマーキング*(*security marking*)を参照。

(marking)

マッチング合意書
(matching agreement)
[OMB A-108]

マッチングプログラムに従事する当事者のためにプライバシー保護法により要求される、受領機関とソース機関（または非連邦政府機関）との間の書面による合意。

媒体
(media)
[FIPS 200]

システム内で情報が記録、保存、または印刷される磁気テープ、光ディスク、磁気ディスク、大規模集積回路メモリチップ、および印刷物（ただし、ディスプレイ媒体は除く）を含む物理デバイスまたは書き込み面。

メタデータ
(metadata)

データ構造（すなわち、データ形式、構文、セマンティクス）を説明する構造メタデータと、データの内容を説明する説明メタデータ（すなわち、セキュリティラベル）を含む、データの特性を説明する情報。

モバイルコード
(mobile code)

リモートシステムから取得され、ネットワークを介して伝送され、受信者による明示的なインストールまたは実行なしにローカルシステム上で実行されるソフトウェアプログラムまたはプログラムの一部。

モバイルコード技術
(mobile code technologies)

モバイルコードの作成と使用のためのメカニズムを提供するソフトウェア技術。

モバイルデバイス
(mobile device)

個人が一人で簡単に持ち運べるような小さなフォームファクタを有し、物理的な接続なしで動作するように設計され（例えば、無線で情報を送受信する）、取り外し不可能なローカルのデータストレージを持ち、内臓電源で長時間電源が供給される、ポータブルコンピューティングデバイス。モバイルデバイスはまた、音声通信ケイパビリティ、デバイスが情報をキャプチャすることを可能にする搭載センサ（例えば、写真、ビデオ、記録、または位置標定）、および／またはローカルデータを遠隔地と同期させるための組み込み機能などを含む。例えば、スマートフォン、タブレット、電子書籍リーダーなどが含まれる。

中インパクトシステム
(moderate-impact system)
[FIPS 200]

少なくとも 1 つのセキュリティ目的（すなわち、機密性、完全性、または可用性）に対して FIPS 199 の潜在的インパクト値「中」が設定され、潜在的インパクト値「高」が設定されているセキュリティ目的がないシステム。

多要素認証
(multi-factor authentication)
[SP 800-63-3]

認証を成功させるために複数の認証要素を必要とする認証システムまたは認証子。多要素認証は、複数の要素を提供する単一の認証子を使用して、または異なる要素を提供する認証子の組み合わせによって実行できる。
3 つの認証要素は、あなたが知っているもの、あなたが持っているもの、そしてあなた自身の特徴が何かである。
オーセンティケータ(*authenticator*)を参照。

マルチレベルセキュリティ
(multilevel security)
[CNSSI 4009]

異なるセキュリティクリアランスを持つユーザによるアクセスを同時に許可し、認可のないユーザへのアクセスを拒否する、異なる機密性区分およびカテゴリで情報を処理する概念。

複数のセキュリティレベル (multiple security levels) [CNSSI 4009]	異なるセキュリティドメインのリソース（特に保存されたデータ）を含み、それらの間の分離を維持することが信頼されているシステムのケイパビリティ。
国家安全保障システム (national security system) [OMB A-130]	政府機関、または政府機関の契約事業者、または政府機関に代わって他の組織が使用または運用するあらゆるシステム（通信システムを含む） － (i)システムの機能、運用、または使用が、情報収集活動を伴う；国家安全保障に関連する暗号活動を伴う；軍隊の指揮統制を伴う；兵器または兵器システムの不可欠な部分である装備を伴う；または、軍事や情報収集のミッションの直接的な履行に不可欠である、システム（例えば、給与計算、財務、物流、および人事管理アプリケーションなどの日常的な管理および事業アプリケーションに使用されるシステムを除く）；または、(ii)国防または外交上の利益のために機密が維持されるように、大統領令または議会制定法によって確立された基準の下で具体的に認可された情報のために確立された手順によって常に保護されるシステム。
ネットワーク (network)	接続されたコンポーネントの集合で実装されたシステム。そのようなコンポーネントには、ルータ、ハブ、ケーブル、通信制御装置、主要な配布センター、および技術的制御デバイスが含まれる。
ネットワークアクセス (network access)	ローカルエリアネットワーク、ワイドエリアネットワーク、インターネットなどのネットワークを介して通信するユーザ（またはユーザに代わって動作するプロセス）によるシステムへのアクセス。
ノンス (nonce) [SP 800-63-3]	同じ鍵で繰り返されないセキュリティプロトコルで使用される値。例えば、チャレンジアンドレスポンス認証プロトコルでチャレンジとして使用されるノンスは、認証キーが変更されるまで繰り返されません。さもなければ、リプレイ攻撃の可能性がある。
任意アクセス制御 (nondiscretionary access control)	*必須アクセス制御*（*mandatory access control*）を参照。
非ローカルメンテナンス (nonlocal maintenance)	内部または外部ネットワークのいずれかを介して通信する個人が実施するメンテナンス活動。
非組織のユーザ (non-organizational user)	組織のユーザではないユーザ（パブリックユーザを含む）。
否認防止 (non-repudiation)	特定のアクションの実行を偽って否定する個人に対する防御であり、個人が情報の作成、メッセージの送信、情報の承認、メッセージの受信など、特定のアクションを実行したかどうかを判定するケイパビリティを提供する。
NSA 承認済み暗号技術 (NSA-approved cryptography)	承認済みのアルゴリズム、特定の環境における国家機密情報および／または管理対象非機密情報の保護のために承認された実装、およびサポートする鍵管理インフラで構成される暗号化。

オブジェクト (object)	情報を含む、または受け取るデバイス、ファイル、レコード、テーブル、プロセス、プログラム、およびドメインを含む、受動的なシステム関連エンティティ。(サブジェクトによる)オブジェクトへのアクセスは、そのオブジェクトに含まれる情報へのアクセスを意味する。 *サブジェクト*(*subject*)を参照。
運用セキュリティ (operations security) [CNSSI 4009]	機微な活動の計画と実行に関する一般的に機密扱いされていないエビデンスを特定、管理、保護することにより、潜在的な攻撃者が能力と意図に関する情報を拒否できる体系的かつ実証済みのプロセス。このプロセスには、重要な情報の特定、脅威の分析、脆弱性の分析、リスクアセスメント、適切な対策の適用の 5 つのステップが含まる。
組織 (organization) [FIPS 200, Adapted]	連邦政府機関、民間企業、学術機関、州政府、地方自治体、部族政府、または必要に応じて、それらの運用要素を含む、組織構造内の任意のサイズ、複雑さ、または位置付けのエンティティ。
組織が定める管理策パラメータ (organization-defined control parameter)	組織が定める値を設定するか、管理策または拡張管理策の一部として提供される事前に規定されたリストから値を選択することにより、テーラリングプロセス中に組織によって生成される管理策または拡張管理策の可変部分。 *設定操作*(*assignment operation*)と*選択操作*(*selection operation*)を参照。
組織のユーザ (organizational user)	契約社員、ゲスト研究者、または別の組織の詳細に説明された個人を含む、組織の従業員、または組織が従業員と同等の地位にあるとみなす個人。従業員と同等の地位を個人に付与するためのポリシーおよび手順には、知る必要があること(need-to-know)、組織との関係、および市民権が含まれる場合がある。
オーバーレイ (overlay) [OMB A-130]	テーラリングプロセス中に採用される、セキュリティまたはプライバシー管理策、拡張管理策、補足ガイダンス、およびその他のサポート情報の仕様であって、セキュリティ管理策ベースラインを補完(および、さらに改良)することを目的とする。オーバーレイ仕様は、元のセキュリティ管理策ベースラインの仕様より厳しくても厳しくなくてもよく、複数の情報システムに適用することができる。 *テーラリング*(*tailoring*)を参照。
パラメータ (parameter)	*組織が定める管理策パラメータ*(*organization-defined control parameter*)を参照。
侵入テスト (penetration testing)	通常、特定の制約の下で作業するアセッサーが、システムのセキュリティ機能を回避または無効にしようとするテスト方法。
期間処理 (periods processing)	異なる機微性の情報が同じシステムによって明らかに異なる時間に処理され、その間にシステムで情報が適切に除去またはサニタイズされるシステム動作のモード。

個人情報 (personally identifiable information) [OMB A-130]	個人のアイデンティティを、単独で、または特定の個人にリンクまたはリンク可能な他の情報と組み合わせて区別または追跡するために使用できる情報。
個人情報の取扱い (personally identifiable information processing) [ISO/IEC 29100, Adapted]	個人情報に対して実行される操作または一連の操作で、個人情報の収集、保持、ログ取得、生成、変換、使用、開示、転送、および廃棄を含むことができるがこれらに限定されない。
個人情報の取扱い許可 (personally identifiable information processing permissions)	個人情報を取扱うための要件、または個人情報を取扱うことができる条件。
職員のセキュリティ (personnel security)	統合的信頼性を必要とする職務および責任について、個人の行い、誠実さ、判断力、忠誠心、信頼性、および安定性をアセスメントする規律。
物理的アクセス制御システム (physical access control system) [SP 800-116]	アクセス制御ポイントでの認証および認可によって、保護区域に人や車両が入る能力を制御する電子システム。
実施計画およびマイルストーン (plan of action and milestones)	達成する必要のある業務を特定する文書。計画の要素を達成するために必要なリソース、業務を満たすためのマイルストーン、および節目となる完了予定日について詳しく説明する。
ポータブルストレージデバイス (portable storage device)	システムまたはネットワークと通信し、システムまたはネットワークから追加または削除でき、その主要機能として、テキスト、ビデオ、オーディオ、または画像データを含むデータストレージに限定されるシステムコンポーネント（例えば、光ディスク、外付けまたは可搬型ハードディスク）ドライブ、外付けまたは可搬型SSDドライブ、磁気または光学テープ、フラッシュメモリデバイス、フラッシュメモリカード、およびその他の外付けまたは可搬型ディスク）。
潜在的インパクト (potential impact) [FIPS 199]	機密性、完全性、または可用性の損失は、組織の運営、組織の資産、または個人に対して、限定的な悪影響（FIPS 199「低」）；深刻な悪影響（FIPS 199「中」）；あるいは、重大または壊滅的な悪影響（FIPS 199「高」）を及ぼすと予想される。
プライバシーアーキテクチャ (privacy architecture) [SP 800-37]	企業のプライバシー保護プロセス、技術的手段、人事および組織のサブユニットの構造と業務を記述し、企業のミッションおよび戦略計画との整合性を示す、エンタープライズアーキテクチャに組み込まれた不可欠な部分。
プライバシー管理策 (privacy control) [OMB A-130]	適用されるプライバシー要件への準拠を確保し、プライバシーリスクを管理するために組織内で採用される管理上、技術上、および物理的な保全措置。

プライバシー管理策ベースライン (privacy control baseline)	テーラリングプロセスの始点を提供する、プライバシー管理策の選択基準に基づいて選択された一連のプライバシー管理策。
プライバシードメイン (privacy domain)	プライバシーポリシーを実施するドメイン。
プライバシー影響評価 (privacy impact assessment) [OMB A-130]	情報がどのように取扱われるかについての分析であって、取扱いが、プライバシーに関して適用される法的、規制、およびポリシーの要件に準拠していることを確実にする;電子情報システムにおいて、識別可能な形式で情報を作成、収集、使用、処理、保存、維持、配布、開示、および廃棄することのリスクおよび影響を判定する;ならびに、潜在的なプライバシーに対する懸念を軽減するために、情報の取扱いに対する保護および代替プロセスを調査および評価する。プライバシー影響評価は、分析のプロセスと結果を詳述する分析と正式な文書の両方を含む。
プライバシー計画 (privacy plan) [OMB A-130]	適用されるプライバシー要件を満たし、プライバシーリスクを管理するために導入または計画されている情報システムまたは運用環境のために選択されたプライバシー管理策を詳述し、管理策の実装方法を詳述し、また、管理策アセスメントに使用される方法や指標を説明する正式な文書。
プライバシープログラム計画 (privacy program plan) [OMB A-130]	プライバシープログラムの構造、プライバシープログラム専用のリソース、政府機関のプライバシー保護責任者およびその他のプライバシー担当者とスタッフの役割、プライバシープログラムの戦略的目標と目的、および適用されるプライバシー要件を満たし、プライバシーリスクを管理するために導入または計画されているプログラムマネジメント管理策や共通管理策を含む、政府機関のプライバシープログラムの概要を提供する正式な文書。
特権アカウント (privileged account)	特権ユーザの権限を持つシステムアカウント。
特権コマンド (privileged command)	セキュリティ機能および関連するセキュリティ関連情報を含む、システムの制御、監視、または管理を含む、システム上で実行される人間が開始するコマンド。
特権ユーザ (privileged user) [CNSSI 4009]	一般ユーザが実行することを認可されていないセキュリティ関連機能を実行することを認可されている(したがって信頼されている)ユーザ。
保護された配信システム (protected distribution system) [CNSSI 4009]	適切な保全措置および/または対策(音響、電気、電磁気、および物理的手段などの)を実施された有線または光ファイバーシステムにより、機密性区分が低いまたは制御が不十分な領域を介した暗号化されていない情報の伝送に使用できる。
来歴 (provenance)	システムまたはシステムコンポーネントおよび関連データの起源、開発、所有権、場所、および変更の年表。また、システム、コンポーネント、または関連データを操作または変更するために使用される職員およびプロセスも含まれる場合がある。

公開鍵基盤 (public key infrastructure) [CNSSI 4009]	証明書ベースの公開鍵暗号システムの実装と運用を集合的にサポートするアーキテクチャ、組織、技法、実践、および手順。公開鍵証明書を発行、維持、および取り消すために確立されたフレームワーク。
除去 (purge) [SP 800-88]	最先端の実験室技法を使用してターゲットデータの復旧を実行不可能にする物理的または論理的技法を適用するサニタイズ方法。
互恵契約 (reciprocity) [SP 800-37]	システムリソースを再利用するために互いのセキュリティアセスメントを受け入れること、および／または情報を共有するために互いのアセスメントされたセキュリティ態勢を受け入れることについての参加組織間の合意。
記録 (records) [OMB A-130]	連邦法に基づいて、または公共事業の取引に関連して連邦政府機関によって作成または受領され、その政府機関またはその合法的な後継者によって保存、または適切に保存されるのに適した形式または特性に関係なく、すべての記録された情報、米国政府の組織、機能、ポリシー、決定、手順、運用、またはその他の活動のエビデンス、またはそれらのデータの情報価値によるもの。
レッドチーム演習 (red team exercise)	組織のミッションや事業プロセスを危殆化したり、組織とそのシステムのセキュリティ機能を包括的にアセスメントしたりするための模擬的な敵対的な試みとして行われる実際の状況を反映した演習。
リファレンスモニタ (reference monitor)	オペレーティングシステムの主要コンポーネントとして、すべてのサブジェクトおよびオブジェクトに対してアクセス制御ポリシーを適用する、参照検証メカニズムに関する一連の設計要件。参照検証メカニズムは常に呼び出され（つまり、完全な調停）、改ざん防止機能があり、分析とテストの対象となるのに十分なほど小さく、その完全性が保証されている（つまり、検証可能）。
リグレーダ (regrader) [CNSSI 4009]	定義されたポリシー例外に従って、データの再分類と再ラベル付けを明示的に認可された信頼できるプロセス。信頼できないプロセスや認可されていないプロセスは、セキュリティポリシーによりそのようなアクションを行なう。
リモートアクセス (remote access)	外部ネットワークを介して通信するユーザ（またはユーザに代わって動作するプロセス）による組織システムへのアクセス。
リモートメンテナンス (remote maintenance)	外部ネットワークを介して通信する個人によって実施されるメンテナンス活動。
リプレイ攻撃 (replay attack) [SP 800-63-3]	攻撃者が以前にキャプチャした（正当な要求者と検証者間の）メッセージを再生して、その要求者を検証者に見せかける攻撃、またはその逆の攻撃。
リプレイ耐性 (replay resistance)	認可されていない影響を及ぼすことや、認可されていないアクセスを行うことを目的として、伝送された認証またはアクセス制御情報がキャプチャされ、その後に再送信されることに対する保護。

レジリエンス (resilience) [OMB A-130]	情報システムが、劣化または衰弱した状態であっても、不可欠な運用能力を維持しながら、悪条件下またはストレス下で運用でき、運用要求と一致する時間枠で効果的な運用態勢に回復する能力。
秘密データ (restricted data) [ATOM54]	(i)核兵器の設計、製造、または利用に関するすべてのデータ;(ii)特別な核物質の製造;または(iii)エネルギーの生産における特別な核物質の使用、ただし、[1954 年原子力法]第 142 条に従って秘密データ分類から除外または削除されたデータは含まない。
リスク (risk) [OMB A-130]	エンティティが潜在的な状況またはイベントによって脅かされる程度の尺度であり、通常、以下の関数である。(i)状況またはイベントが発生した場合に生じる有害なインパクトまたは損害の規模;および(ii)発生の可能性。
リスクアセスメント (risk assessment) [SP 800-39] [IR 8062, Adapted]	システムの運用から生じる、組織の運営(ミッション、機能、イメージ、評判を含む)、組織の資産、個人、他の組織、および国家に対するリスクを識別するプロセス。 リスクマネジメントには、脅威および脆弱性の分析、ならびに情報処理から生じる個人への悪影響の分析が含まれ、計画または導入されているセキュリティおよびプライバシー管理策によって提供される緩和策を考慮する。*リスク分析*と同義。
リスク管理者(部署) (risk executive (function)) [SP 800-37]	個々のシステムのセキュリティリスク関連の考慮事項を、それらのシステムの認可決定を含めるために、組織全体の観点から、組織のミッションおよび事業の機能を遂行する上での組織の全体的な戦略的目標および目的に関する;個々のシステムからのリスクマネジメントは、組織全体で一貫しており、組織のリスク許容度を反映し、ミッションまたは事業の成功に影響を与える他の組織のリスクとともに考慮される。
リスクマネジメント (risk management) [OMB A-130]	政府機関の運営(ミッション、機能、イメージ、評判を含む)、政府機関の資産、個人、他の組織、および国家に対するリスクを管理するためのプログラムおよびサポートプロセス。リスク関連活動の状況の確立;リスクアセスメント;判定されたリスクへの対応;およびリスクの長期にわたる監視が含まれる。
リスク軽減 (risk mitigation) [CNSSI 4009]	リスクマネジメントプロセスから推奨された適切なリスク低減管理策/対策の優先順位付け、評価、および実施。
リスク対応 (risk response) [OMB A-130]	政府機関の活動、政府機関の資産、個人、他の組織、または国家に対するリスクの受け入れ、回避、軽減、共有、または移転。
リスク許容度 (risk tolerance) [SP 800-39]	組織が許容できるリスクのレベルまたは不確実性の程度。
役割ベースのアクセス制御 (role-based access control)	ユーザの役割に基づくアクセス制御(つまり、ユーザが特定の役割の明示的または暗黙的な仮定に基づいて受け取るアクセス認可の集合)。役割権限は、役割階層を介して継承され、通常、組織内で定める機能を実行するために必要な権限を反映

	する。特定の役割は、単一の個人または複数の個人に適用できる。
ランタイム (runtime)	コンピュータプログラムが実行されている期間。
サニタイズ (sanitization) [SP 800-88]	媒体上の対象データへのアクセスを、一定レベルの作業に対して実行不可能にするプロセス。消去、除去、破棄は、媒体をサニタイズするために実行できるアクションである。
スコーピングの考慮事項 (scoping considerations)	管理策ベースラインのセキュリティおよびプライバシー管理策の適用性と実装に関する特定の考慮事項を組織に提供する、テーラリングガイダンスの一部。考慮事項には、ポリシー、規則、技術、物理インフラ、システムコンポーネントの割り当て、パブリックアクセス、拡張性、共通管理策、運用、環境、およびセキュリティ目的が含まれる。
セキュリティ (security) [CNSSI 4009]	システムの使用に対する脅威によってもたらされるリスクにもかかわらず、組織がそのミッションや重要機能を実行できるようにする保護手段を確立し、維持することによって生じる状態。保護手段には、組織のリスクマネジメントアプローチの一部を形成することが望ましい抑止、回避、防止、検知、復旧、修正の組み合わせが含まれる場合がある。
セキュリティ属性 (security attribute)	情報の保全措置に関するエンティティの基本的な特性または特徴を表す抽象概念。通常、システム内のレコード、バッファ、ファイルなどの内部データ構造に関連付けられ、アクセス制御およびフロー制御ポリシーの実装を可能にするために使用される；特別な配布、処理、または配布の指示を反映する；または、情報セキュリティポリシーの他の側面をサポートする。
セキュリティ分類化 (security categorization)	情報またはシステムのセキュリティ分類を決定するプロセス。セキュリティ分類化の方法は、国家安全保障システムについてはCNSSI 第 1253 号に、国家安全保障システム以外についてはFIPS 199 に記載されている。 *セキュリティ分類*(*security category*)を参照。
セキュリティ分類 (security category) [OMB A-130]	情報または情報システムの機密性、完全性、または可用性の喪失が政府機関の運営、政府機関の資産、個人、他の組織、および国家に及ぼす潜在的インパクトのアセスメントに基づいた、情報または情報システムの特徴付け。
セキュリティ管理策 (security control) [OMB A-130]	情報システムとその情報の機密性、完全性、可用性を保護するために情報システムまたは組織のために定められた保全措置または対策。
セキュリティ管理策ベースライン (security control baseline) [OMB A-130]	低インパクト、中インパクト、または高インパクトの情報システムに対して規定された一連の最小限のセキュリティ管理策。
セキュリティドメイン (security domain) [CNSSI 4009]	セキュリティポリシーを実装し、単一の権限によって管理されるドメイン。

セキュリティ機能性 (security functionality)	組織の情報システムまたはそれらのシステムが動作する環境内に実装されるセキュリティ関連の特徴、機能、メカニズム、サービス、手順、およびアーキテクチャ。
セキュリティ機能 (security functions)	システムのセキュリティポリシーを実施し、保護の基礎となるコードとデータの分離をサポートする責任を負うシステムのハードウェア、ソフトウェア、またはファームウェア。
セキュリティインパクト分析 (security impact analysis) [SP 800-128]	システムへの変更がシステムのセキュリティ態勢にどの程度影響を与えるかを判定するために組織内の有資格職員が実施する分析。
セキュリティカーネル (security kernel) [CNSSI 4009]	リファレンスモニタの概念を実装する信頼できるコンピューティングベースのハードウェア、ファームウェア、およびソフトウェア要素。セキュリティカーネルは、すべてのアクセスを仲介し、変更から保護され、正しいことを検証できる必要がある。
セキュリティラベル (security label)	セキュリティ属性のセットを、そのオブジェクトのデータ構造の一部として特定の情報オブジェクトに関連付けるために使用される手段。
セキュリティマーキング (security marking)	情報セキュリティポリシーの組織的なプロセスベースの実施を可能にするために、一連のセキュリティ属性を人間が読める形式の標示物に関連付けるために使用される手段。
セキュリティ目的 (security objective) [FIPS 199]	機密性、完全性、または可用性。
セキュリティ計画 (security plan)	情報システムのセキュリティ要件または情報セキュリティプログラムの概要を提供し、それらの要件を満たすために導入または計画されているセキュリティ管理策を説明する正式な文書。システムセキュリティ計画は、システムに含まれるシステムコンポーネント、システムが動作する環境、セキュリティ要件の実装方法、および他のシステムとの関係または接続について説明する。 *システムセキュリティ計画*(*system security plan*)を参照。
セキュリティポリシー (security policy) [SP 800-160-1, Adapted]	セキュリティサービスの提供に関する一連の基準。セキュリティ関連のシステムおよびシステムコンポーネントの動作のすべての側面を管理する一連の規定。
セキュリティポリシーフィルタ (security policy filter)	次の機能の 1 つまたは複数を実行するハードウェアあるいは／またはソフトウェアコンポーネント。提出されたコンテンツを分析し、定義されたポリシーに準拠していることを確認するためのコンテンツ検査。送信されたコンテンツのデータタイプを確認するためのコンテンツ検証。悪意のあるコードのコンテンツを評価する悪意のあるコンテンツチェッカー。サンドボックスやデトネーションチャンバーなどのセキュアな方法でコンテンツを評価または実行し、不審なアクティビティを監視する不審なアクティビティチェッカー。または、規定されたポリシーに準拠するように送信されたコンテンツを変更する、コンテンツのサニタイズ、クレンジング、および変換。

セキュリティ要件
(security requirement)
[FIPS 200, Adapted]

処理、保存、または伝送される情報の機密性、完全性、および可用性を確保するために、適用される法律、大統領令、指令、規則、ポリシー、基準、手順、またはミッション／事業ニーズから導出され、情報システムまたは組織に課せられる要件。
*注:*セキュリティ要件は、システム開発およびエンジニアリング分野において高レベルのポリシー関連の活動から低レベルの実装関連の活動まで、様々な状況で使用することができる。

セキュリティサービス
(security service)
[SP 800-160-1]

1 つ以上のセキュリティ目的をサポートするエンティティによって提供されるセキュリティケイパビリティまたは機能。

セキュリティ関連情報
(security-relevant information)

システムのセキュリティポリシーの施行またはコードとデータの分離の維持に失敗する可能性のある方法で、セキュリティ機能の運用またはセキュリティサービスの提供にインパクトを与える可能性のあるシステム内の情報。

選択操作
(selection operation)

管理策または拡張管理策の一部として提供される事前に規定された値のリストから、組織が値を選択することができる管理策パラメータ(例えば、アクションの制限またはアクションの禁止を選択する)。
*設定操作(assignment operation)*と*組織が定める管理策パラメータ(organization-defined control parameter)*を参照。

政府機関の情報セキュリティ責任者
(senior agency information security officer)

FISMA の下で最高情報責任者の責任を遂行し、政府機関の認可権限のある担当者、情報事業オーナー、および情報システムセキュリティ担当者に対する最高情報責任者の主たる連絡窓口となる職員。
*注:*連邦政府機関の下位組織は、情報セキュリティ責任者または最高情報セキュリティ責任者という用語を使用して、政府機関の情報セキュリティ責任者と同様の職務を担当する個人を表すことができる。

政府機関のプライバシー保護責任者
(senior agency official for privacy)
[OMB A-130]

プライバシー保護の実施;プライバシーに関する連邦法、規則、およびポリシーへの遵守;政府機関におけるプライバシーリスクの管理;法律、規則、および他のポリシーに関する提案の策定と評価における政府機関の中心的なポリシー決定の役割を含む政府機関全体のプライバシー責任を負う、各政府機関の長によって指名された責任者。

情報セキュリティ責任者
(senior information security officer)

*政府機関の情報セキュリティ責任者(senior agency information security officer)*を参照。

機微区分情報
(sensitive compartmented information)
[CNSSI 4009]

国家情報長官によって確立された正式なアクセス制御システム内で処理する必要がある、情報ソース、方法、または分析プロセスに関する、またはそれらから派生した国家機密情報。

サービス指向アーキテクチャ
(service-oriented architecture)

相互運用可能なサービスの形でソフトウェアを設計および開発するための一連の原則および方法論。これらのサービスは、明確に規定された事業の機能であり、様々な目的に再利用できるソフトウェアコンポーネント(つまり、個別のコードやデータ構造)として構築される。

共有管理策 (shared control)	情報システムに、一部は共通管理策として、一部はシステム固有管理策として実装されるセキュリティまたはプライバシー管理策。 *ハイブリッド管理策*(*hybrid control*)を参照。
ソフトウェア (software) [CNSSI 4009]	実行中に動的に書き込まれたり変更されたりする可能性のあるコンピュータプログラムおよび関連データ。
スパム (spam)	電子メッセージングシステムの悪用による迷惑な大量メッセージの無差別な送信。
連邦政府高度機密情報アクセスプログラム (special access program) [CNSSI 4009]	同じ分類レベルの情報に通常必要な要件を超える保全措置要件とアクセス要件を課す、特定のクラスの国家機密情報のために確立されたプログラム。
スプリットトンネリング (split tunneling)	リモートユーザまたはデバイスがシステムとの非リモート接続を確立し、同時に他の何らかの接続を介して外部ネットワークのリソースに通信できるようにするプロセス。このネットワークアクセス方法により、ユーザはリモートデバイスにアクセスすると同時に、制御されていないネットワークにアクセスすることができる。
スパイウェア (spyware)	秘密裏に個人または組織の情報を収集するために、情報システムに密かにインストールされるソフトウェア。悪意のあるコードの一種。
サブジェクト (subject)	オブジェクト間で情報を流したり、システム状態を変化させたりする個人、プロセス、またはデバイス。 *オブジェクト*(*object*)を参照。
サブシステム (subsystem)	情報、情報技術、および 1 つ以上の特定の機能を実行する職員で構成される情報システムの主要な下位区分またはコンポーネント。
サプライヤ (supplier)	製品またはサービスの供給に関して、取得者または統合者と契約を結ぶ組織または個人。これには、サプライチェーンのすべてのサプライヤ;システム、システムコンポーネント、またはシステムサービスの開発者または製造業者;システムインテグレータ;ベンダ;製品の再販業者;サードパーティのパートナーが含まれる。
サプライチェーン (supply chain)	製品とサービスの調達から始まり、ライフサイクル全体に及ぶ、組織の複数の階層間でのリソースとプロセスのリンクされたセット。
サプライチェーン要素 (supply chain element)	システムおよびシステムコンポーネントの調査、設計、製造、取得、納入、統合、運用および保守、廃棄に使用される組織、エンティティ、またはツール。
サプライチェーンリスク (supply chain risk)	サプライヤ、サプライチェーン、およびそれらの製品またはサービスからのセキュリティリスクの結果として発生する損害または侵害の可能性。サプライチェーンリスクには、サプライチェーン

	を横断する製品およびサービスに関連する暴露、脅威、および脆弱性、ならびにサプライチェーンへの暴露、脅威、および脆弱性が含まれる。
サプライチェーンのリスクアセスメント (supply chain risk assessment)	サプライチェーンリスク、その発生の可能性、および潜在的インパクトの体系的な調査。
サプライチェーンのリスクマネジメント (supply chain risk management)	サプライチェーン全体のサイバーサプライチェーンのリスク暴露、脅威、脆弱性を管理し、サプライヤ、提供された製品とサービス、またはサプライチェーンによって提示されたリスクに対するリスク対応戦略を策定するための体系的なプロセス。
システム (system) [CNSSI 4009] [ISO 15288]	一連の特定の機能を実現するために、相互作用または相互依存によって統合および統制される、リソースと手順の組織化されたアセンブリ。 *注:*システムには、産業用制御システム、電話交換機や構内交換機(PBX)システム、環境制御システムなどの特殊なシステムも含まれる。 1 つ以上の規定された目的を達成するために組織化された相互作用要素の組み合わせ。 *注 1:*システムには多くのタイプがある。例には以下が含まれる。一般的および特殊な目的の情報システム;コマンド、制御、および通信システム;暗号モジュール;中央処理装置およびグラフィックスプロセッサボード;産業用制御システム;飛行制御システム;武器、標的、および射撃管制システム;医療デバイスおよび治療システム;金融、銀行、および商品取引システム。ソーシャルネットワーキングシステム。 *注 2:*システムの定義における相互作用要素には、ハードウェア、ソフトウェア、データ、人間、プロセス、設備、材料、および自然に存在する物理的エンティティが含まれる。 *注 3:*システムの定義には、システム・オブ・システムズが含まれる。
システムコンポーネント (system component) [SP 800-128]	システムの構成要素を表す個別の識別可能な情報技術資産。ハードウェア、ソフトウェア、およびファームウェアを含む。
記録システム (system of records) [USC 552]	個人の名前、または個人に設定された特定の識別番号、記号、またはその他の識別情報によって情報が取得される、任意の機関の管理下にある任意の記録のグループ。
記録システム通知 (system of records notice) [OMB A-108]	システムの存在と特性を説明する記録システムの確立および/または変更時に、連邦登録簿にある官庁により発行される通知。
システムオーナー(またはプログラムマネージャー) (system owner (or program manager))	システムの調達、開発、統合、変更、運用、メンテナンス全般に責任を持つ担当者。
システムセキュリティ担当者 (system security officer)	システムまたはプログラムの適切な運用セキュリティ態勢を維持する責任が割り当てられた個人。

[SP 800-37]

システムセキュリティ計画
(system security plan)
セキュリティ計画(*security plan*)を参照。

システムサービス
(system service)
情報の処理、保存、伝送を促進するシステムによって提供されるケイパビリティ。

システム関連のセキュリティリスク
(system-related security risk)
[SP 800-30]
情報またはシステムの機密性、完全性、または可用性の喪失により発生するリスク、組織(資産、ミッション、機能、イメージ、または評判を含む)、個人、他の組織、そして国家へのインパクトを考慮。
リスク(*risk*)を参照。

システム固有管理策
(system-specific control)
[OMB A-130]
システムレベルで実装され、他の情報システムによって継承されない、情報システムのためのセキュリティまたはプライバシー管理策。

システムエンジニアリング
(systems engineering)
[SP 800-160-1]
システムのライフサイクル全体を通じて、顧客と他のすべての利害関係者のニーズが高品質で信頼性が高く、費用対効果が高く、スケジュールに準拠した方法で満足されるようにするための学際的なプロセスを作成および実行する責任を持つエンジニアリング分野。

システムセキュリティエンジニアリング
(systems security engineering)
[SP 800-160-1]
システム工学に強く関連する専門工学分野。それは、科学的、工学的、および情報保証の原則を適用して確立された、リスク許容度内で利害関係者の要件を満たす信頼できるシステムを提供する。

テーラリングされた管理策ベースライン
(tailored control baseline)
管理策ベースラインにテーラリングガイダンスを適用することで得られる一連の管理策。
テーラリング(*tailoring*)を参照。

テーラリング
(tailoring)
セキュリティ管理策ベースラインが変更されるプロセスであり、共通管理策の識別と指定、ベースライン管理策の適用性と実装に関するスコーピングの考慮事項の適用、代替セキュリティ管理策の選択、組織が定めるセキュリティ管理策パラメータへの特定の値の設定、追加のセキュリティ管理策や拡張管理策によるベースラインの補足、および、管理策実装のための追加の仕様情報の提供などが行なわれる。

改ざん
(tampering)
[CNSSI 4009]
システム、システムのコンポーネント、その意図された動作、またはデータの変更をもたらす意図的ではあるが認可されていない行為。

脅威
(threat)
[SP 800-30]
情報の認可されていないアクセス、破壊、開示、変更、および/またはサービス妨害により、システムを通じて、組織の運営、組織の資産、個人、他の組織、または国家に有害なインパクトを与える可能性のある状況または事象。

脅威アセスメント
(threat assessment)
情報システムに対する脅威の正式な記述と評価。

[CNSSI 4009]

脅威のモデル化
(threat modeling)
[SP 800-154]

データ、アプリケーション、ホスト、システム、環境など、論理エンティティの攻撃側と防御側の側面をモデル化したリスクアセスメントの形式。

脅威ソース
(threat source)
[FIPS 200]

意図的に脆弱性を悪用することを目的とした意図および方法、または偶発的に脆弱性を誘発する可能性がある状況および方法。
脅威エージェント(*threat agent*)を参照。

伝送
(transmission)
[CNSSI 4009]

情報が 1 つの場所から 1 つ以上の他の場所に電子的に送信されているときに存在する状態。

信頼できる経路
(trusted path)

ユーザが(入力デバイスを介して)システムのセキュリティポリシーをサポートするために必要な信頼性を持って、システムのセキュリティ機能と直接通信できるメカニズム。このメカニズムは、ユーザまたはシステムのセキュリティ機能によってのみアクティブにすることができ、信頼できないソフトウェアによって模倣することはできない。

統合的信頼性
(trustworthiness)
[CNSSI 4009]

特定のタスクを実行し、割り当てられた責任を果たすために、そのエンティティの資格、ケイパビリティ、信頼性について他の人に信頼を提供する個人または企業の属性。

統合的信頼性(システム)
(trustworthiness (system))

情報システム(システムを構築するために使用される情報技術コンポーネントを含む)が、システムによって処理、保存、または伝送される情報の機密性、完全性、および可用性を脅威の全範囲にわたって維持することが期待できる度合い。信頼できる情報システムは、その運用環境で発生すると予想される環境破壊、人為的ミス、構造的障害、および意図的な攻撃にもかかわらず、規定されたレベルのリスク内で動作すると考えられる。

ユーザ
(user)

システムへのアクセスを認可された個人、または個人に代わって動作する(システム)プロセス。
組織のユーザ(*organizational user*)と*非組織のユーザ*(*non-organizational user*)を参照。

仮想プライベートネットワーク
(virtual private network)
[CNSSI 4009]

トンネリング、セキュリティ管理策、およびエンドポイントアドレス変換を利用して、専用回線の印象を与える保護された情報システムリンク。

脆弱性
(vulnerability)
[SP 800-30]

脅威ソースによって悪用または誘発される可能性がある、情報システム、システムセキュリティ手順、内部管理策、または実装における弱点。

脆弱性分析
(vulnerability analysis)

脆弱性アセスメント(*vulnerability assessment*)を参照。

脆弱性アセスメント
(vulnerability assessment)
[CNSSI 4009]

情報システムまたは製品の体系的な検査を行い、セキュリティ対策の妥当性を判定し、セキュリティの欠陥を特定し、提案され

たセキュリティ対策の有効性を予測するためのデータを提供し、実装後にそのような対策の妥当性を確認する。

付属書 B

略語

一般的な略語

ABAC	Attribute-Based Access Control （属性ベースのアクセス制御）
API	Application Programming Interface （アプリケーション・プログラミング・インタフェース）
APT	Advanced Persistent Threat （持続的標的型攻撃）
BGP	Border Gateway Protocol （ボーダーゲートウェイプロトコル）
BIOS	Basic Input/Output System （基本入出力システム）
CA	Certificate Authority/Certificate Authorities （認証局）
CAC	Common Access Card （共通アクセスカード）
CAVP	Cryptographic Algorithm Validation Program （暗号アルゴリズム認証制度）
CD	Compact Disc （コンパクトディスク）
CD-R	Compact Disc-Recordable （追記型 CD）
CIPSEA	Confidential Information Protection and Statistical Efficiency Act （秘密情報保護および統計の効率性に関する法律）
CIRT	Computer Incident Response Team （コンピュータインシデント対応チーム）
CISA	Cybersecurity and Infrastructure Security Agency （サイバーセキュリティ・インフラストラクチャセキュリティ庁）
CMVP	Cryptographic Module Validation Program （暗号モジュール認証制度）
CNSSD	Committee on National Security Systems Directive （国家安全保障システム委員会指令）
CNSSI	Committee on National Security Systems Instruction （国家安全保障システム委員会指示）
CNSSP	Committee on National Security Systems Policy （国家安全保障システム委員会ポリシー）
CONOPS	Concept of Operations （業務構想文書）

CUI Controlled Unclassified Information
（管理対象非機密情報）

CVE Common Vulnerabilities and Exposures
（共通脆弱性識別子）

CVSS Common Vulnerability Scoring System
（共通脆弱性評価システム）

CWE Common Weakness Enumeration
（共通脆弱性タイプ一覧）

DHCP Dynamic Host Configuration Protocol
（ダイナミック・ホスト・コンフィギュレーション・プロトコル）

DMZ Demilitarized Zone
（非武装地帯）

DNS Domain Name System
（ドメインネームシステム）

DNSSEC Domain Name System Security Extensions
（DNS セキュリティ拡張）

DoD Department of Defense
（国防総省）

DSB Defense Science Board
（国防科学評議委員会）

DVD Digital Versatile Disc
（デジタル多用途ディスク）

DVD-R Digital Versatile Disc-Recordable
（追記型 DVD）

EAP Extensible Authentication Protocol
（拡張認証プロトコル）

EMP Electromagnetic Pulse
（電磁パルス）

EMSEC Emissions Security
（電磁放射に対するセキュリティ）

FASC Federal Acquisition Security Council
（連邦調達安全保障会議）

FBCA Federal Bridge Certification Authority
（連邦ブリッジ認証局）

FCC Federal Communications Commission
（連邦通信委員会）

FICAM Federal Indentity, Credential, and Access Management
（連邦政府のトラストフレームワーク）

FIPPs Fair Information Practice Principles
（公正情報行動原則）

FIPS Federal Information Processing Standards
（連邦情報処理規格）

FISMA Federal Information Security Modernization Act
（連邦情報セキュリティ近代化法）

FOCI Foreign Ownership, Control, or Influence
（外国の所有権、支配または影響力）

FOIA Freedom of Information Act
（情報公開法）

FTP File Transfer Protocol
（ファイル転送プロトコル）

GMT Greenwich Mean Time
（グリニッジ標準時）

GPS Global Positioning System
（グローバル・ポジショニング・システム）

GSA General Services Administration
（共通役務庁）

HSPD Homeland Security Presidential Directive
（国土安全保障大統領指令）

HTTP Hypertext Transfer Protocol
（ハイパーテキスト・トランスファー・プロトコル）

ICS Industrial Control System
（産業用制御システム）

IEEE Institute of Electrical and Electronics Engineers
（電気電子学会）

I/O Input/Output
（入出力）

IOC Indicators of Compromise
（侵害の兆候）

IoT Internet of Things
（モノのインターネット）

IP Internet Protocol
（インターネットプロトコル）

IR Interagency Report or Internal Report
（省庁間報告書または内部報告書）

ISAC Information Sharing and Analysis Centers
（情報共有分析センター）

ISAO Information Sharing and Analysis Organizations
（情報共有分析機関）

IT Information Technology
（情報技術）

ITL Information Technology Laboratory
（情報技術研究所）

MAC Media Access Control
（メディアアクセス制御）

MLS Multilevel Secure
（マルチレベルセキュア）

MTTF Mean Time To Failure
（平均故障時間）

NARA National Archives and Records Administration
（国立公文書記録管理局）

NATO North Atlantic Treaty Organization
（北大西洋条約機構）

NDA Non-Disclosure Agreement
（秘密保持契約）

NIAP National Information Assurance Partnership
（国家情報保証パートナーシップ）

NICE National Initiative for Cybersecurity Education
（サイバーセキュリティ教育に関する国家戦略）

NIST National Institute of Standards and Technology
（国立標準技術研究所）

NOFORN Not Releasable to Foreign Nationals
（国外秘：米国民以外への配付禁止）

NSA National Security Agency
（国家安全保障局）

NVD National Vulnerability Database
（国有脆弱性情報データベース）

ODNI Office of the Director of National Intelligence
（国家情報長官室）

OMB Office of Management and Budget
（行政管理予算局）

OPM Office of Personnel Management
（人事管理局）

OPSEC Operation Security
（運用セキュリティ）

OVAL Open Vulnerability and Assessment Language
（セキュリティ検査言語）

PDF Portable Document Format
（ポータブル・ドキュメント・フォーマット）

PDS Position Designation System
（連邦政府規則による職位指定システム）

PII Personally Identifiable Information
（個人情報）

PIN Personal Identification Number
（暗証番号）

PIV Personal Identity Verification
（個人アイデンティ検証）

PIV-I Personal Identity Verification-Interoperable
（PIV 相当個人アイデンティティ検証）

PKI Public Key Infrastructure
（公開鍵基盤）

RBAC Role-Based Access Control
（役割ベースのアクセス制御）

RD Restricted Data
（秘密データ）

RFID Radio-Frequency Identification
（近距離無線通信で RF タグを識別・管理するシステム）

RFP Request For Proposal
（提案依頼書）

RPKI Resource Public Key Infrastructure
（リソース PKI）

SAP Special Access Program
（連邦政府高度機密情報アクセスプログラム）

SCAP Security Content Automation Protocol
（セキュリティ設定共通化手順）

SCI Sensitive Compartmented Information
（機微区分情報）

SCIF Sensitive Compartmented Information Facility
（機微区分情報隔離施設）

SCRM Supply Chain Risk Management
（サプライチェーンのリスクマネジメント）

SDLC System Development Life Cycle
（システム開発ライフサイクル）

SIEM Security Information and Event Management
（セキュリティ情報イベント管理：サイバー攻撃対策ツール）

SME Subject Matter Expert
（特定分野専門家）

SMTP Simple Mail Transfer Protocol
（電子メール通信プロトコル）

SOC Security Operations Center
（セキュリティオペレーションセンター）

SP Special Publication
（特別出版物）

STIG Security Technical Implementation Guide
（セキュリティ技術導入ガイド）

SWID Software Identification
（ソフトウェア識別）

TCP Transmission Control Protocol
（トランスミッションコントロールプロトコル）

TCP/IP Transmission Control Protocol/Internet Protocol
（インターネットプロトコルスイート）

TIC Trusted Internet Connections
（信頼できるインターネット接続）

TLS Transport Layer Security
（トランスポート層セキュリティ）

TPM Trusted Platform Module
（トラステッドプラットフォームモジュール）

TSP Telecommunications Service Priority
（優先的通信サービス）

UEFI Unified Extensible Firmware Interface
（ユニファイド・エクステンシブル・ファームウェア・インタフェース）

UPS Uninterruptible Power Supply
（無停電電源装置）

USGCB United States Government Configuration Baseline
（米国政府共通設定基準）

USB Universal Serial Bus
（ユニバーサルシリアルバス）

UTC Coordinated Universal Time
（協定世界時）

VoIP Voice over Internet Protocol
（ボイスオーバーインターネットプロトコル）

VPN Virtual Private Network
（仮想プライベートネットワーク）

WORM Write-Once, Read-Many
（ライトワンス型）

XML Extensible Markup Language
（エクステンシブル・マークアップ・ランゲージ）

付属書 C

管理策の要約

実装の撤回および保証の指定

表 C-1 から表 C-20 は、第 3 章のセキュリティおよびプライバシー管理策と拡張管理策の要約を提供している。各表は、異なる管理策ファミリーに焦点を当てている。

- 管理策カタログから撤回された管理策または拡張管理策は「W」で示され、管理策または拡張管理策の配置についての説明は薄いグレーの文字で示されている。
- 通常、技術的手段を介して情報システムによって実装される管理策または拡張管理策は、実装者の欄に「S」で示されている。
- 通常、組織によって（すなわち、非技術的手段を介して個人によって）実装される管理策または拡張管理策は、実施者の欄に「O」で示されている[35]。
- 組織、システム、またはその 2 つの組み合わせによって実装することができる管理策または拡張管理策は、「O/S」で示されている。
- 保証の欄に「✓」が付いている管理策または拡張管理策は、その管理策または拡張管理策によって、セキュリティまたはプライバシーに関するクレームが達成されたか、または達成されるであろうという確信の根拠がもたらされることを示している[36]。

表 C-1 から表 C-20 の管理策および拡張管理策は各々、第 3 章の管理策および拡張管理策のテキストにリンクされている。

管理策ファミリーには、基本管理策と拡張管理策が含まれており、拡張管理策は基本管理策に直接関連している。拡張管理策は、基本管理策に機能性や特殊性を追加する、または基本管理策の強度を向上させる。いずれの場合も、拡張管理策は、基本管理策によって提供される保護よりも強力な保護を必要とするシステムおよび動作環境で使用される。こうした強化された保護は、組織または個人への有害なインパクトが予測される場合、もしくは組織がリスクアセスメントに基づいて追加の保証や基本管理策への機能性の追加を要する場合に必要となる。拡張管理策を使用するには、**必ず**基本管理策も使用しなければならない。

ファミリーはアルファベット順に記載され、各ファミリー内の管理策と拡張管理策は番号順に列挙される。ファミリー、管理策、および拡張管理策のアルファベットまたは番号の順序は、優先順位、重要性レベル、または管理策や拡張管理策が実装される順序を意味するものではない。

[35]表 C-1 から表 C-20 における、特定の管理策または拡張管理策が組織またはシステムによって実装されていることの表示は、概念的なものである。組織は、選択した管理策と拡張管理策を、管理策または拡張管理策の意図に準拠しながら、最も費用対効果が高く効率的な方法で柔軟に実装する。特定の状況において、管理策または拡張管理策は、システム、組織、または 2 つのエンティティの組み合わせによって実施されてもよい。

[36] 保証は、システムの統合的信頼性を判定する上で重要な要素である。保証とは、組織のシステムのセキュリティとプライバシーの機能、特徴、実施項目、ポリシー、手順、メカニズム、およびアーキテクチャが、確立されたセキュリティおよびプライバシーポリシーを的確に仲介および実施する信頼性の尺度である。

表 C-1：「アクセス制御」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
AC-1	**ポリシーおよび手順**	O	✓
AC-2	**アカウント管理**	O	
AC-2(1)	自動化されたシステムアカウント管理	O	
AC-2(2)	一時アカウントおよび緊急アカウントの自動化された管理	S	
AC-2(3)	アカウントの無効化	S	
AC-2(4)	自動化された監査	S	
AC-2(5)	非アクティブログアウト	O/S	
AC-2(6)	動的権限管理	S	
AC-2(7)	特権ユーザアカウント	O	
AC-2(8)	動的アカウント管理	S	
AC-2(9)	共有アカウントおよびグループアカウントの使用に対する制限	O	
AC-2(10)	共有アカウントおよびグループアカウントのクレデンシャルの変更	W：AC-2k に組み込み	
AC-2(11)	使用条件	S	
AC-2(12)	非定型的な使用のアカウントの監視	O/S	
AC-2(13)	リスクの高い個人のアカウントの無効化	O	
AC-3	**アクセス実施**	S	
AC-3(1)	特権機能への制限付きアクセス	W：AC-6 に組み込み	
AC-3(2)	二重認可	S	
AC-3(3)	必須アクセス制御	S	
AC-3(4)	任意アクセス制御	S	
AC-3(5)	セキュリティ関連情報	S	
AC-3(6)	ユーザおよびシステム情報の保護	W：MP-4、SC-28 に組み込み	
AC-3(7)	役割ベースのアクセス制御	O/S	
AC-3(8)	アクセス認可の取り消し	O/S	
AC-3(9)	管理されたリリース	O/S	
AC-3(10)	アクセス制御のメカニズムへの監査優先	O	
AC-3(11)	特定の情報タイプへのアクセスの制限	S	
AC-3(12)	アプリケーションアクセスへのアサーションおよび実施	S	
AC-3(13)	属性ベースのアクセス制御	S	
AC-3(14)	個人アクセス	S	
AC-3(15)	任意および必須アクセス制御	S	
AC-4	**情報フローの実施**	S	
AC-4(1)	オブジェクトのセキュリティおよびプライバシー属性	S	
AC-4(2)	処理ドメイン	S	
AC-4(3)	動的情報フロー制御	S	
AC-4(4)	暗号化された情報のフロー制御	S	
AC-4(5)	組み込みデータタイプ	S	

管理策番号	管理策名 拡張管理策名	実装者	保証
AC-4(6)	メタデータ	S	
AC-4(7)	一方向フローのメカニズム	S	
AC-4(8)	セキュリティおよびプライバシーポリシーフィルタ	S	
AC-4(9)	人によるレビュー	O/S	
AC-4(10)	セキュリティまたはプライバシーポリシーフィルタの有効化および無効化	S	
AC-4(11)	セキュリティまたはプライバシーポリシーフィルタの構成	S	
AC-4(12)	データタイプ識別子	S	
AC-4(13)	ポリシー関連サブコンポーネントへの分解	S	
AC-4(14)	セキュリティまたはプライバシーポリシーフィルタの制約	S	
AC-4(15)	容認されない情報の検知	S	
AC-4(16)	相互接続されたシステムでの情報転送	W：AC-4 に組み込み	
AC-4(17)	ドメイン認証	S	
AC-4(18)	セキュリティ属性のバインディング	W：AC-16 に組み込み	
AC-4(19)	メタデータの検証	S	
AC-4(20)	承認されたソリューション	O	
AC-4(21)	情報フローの物理的または論理的分離	O/S	
AC-4(22)	アクセス専用	S	
AC-4(23)	非公開情報の更新	O/S	
AC-4(24)	内部正規化フォーマット	S	
AC-4(25)	データのサニタイズ	S	
AC-4(26)	フィルタリング処理の監査	O/S	
AC-4(27)	冗長／独立フィルタリングのメカニズム	S	
AC-4(28)	線形フィルタパイプライン	S	
AC-4(29)	フィルタオーケストレーションエンジン	O/S	
AC-4(30)	複数のプロセスを使用するフィルタリングのメカニズム	S	
AC-4(31)	失敗したコンテンツの転送防止	S	
AC-4(32)	情報転送のプロセス要件	S	
AC-5	**職務の分離**	O	
AC-6	**最小特権**	O	
AC-6(1)	セキュリティ機能へのアクセスの認可	O	
AC-6(2)	非セキュリティ機能に関する非特権アクセス	O	
AC-6(3)	特権コマンドへのネットワークアクセス	O	
AC-6(4)	個別の処理ドメイン	O/S	
AC-6(5)	特権アカウント	O	
AC-6(6)	非組織ユーザによる特権アクセス	O	
AC-6(7)	ユーザ特権のレビュー	O	
AC-6(8)	コード実行の特権レベル	S	
AC-6(9)	特権機能使用のロギング	S	
AC-6(10)	非特権ユーザによる特権機能の実行の禁止	S	

管理策番号	管理策名 拡張管理策名	実装者	保証
AC-7	**ログオン試行の失敗**	S	
AC-7(1)	自動アカウントロック	W：AC-7 に組み込み	
AC-7(2)	モバイルデバイスからの除去または抹消	S	
AC-7(3)	生体認証の試行の限定	O	
AC-7(4)	代替認証要素の使用	O/S	
AC-8	**システム使用の通知**	O/S	
AC-9	**過去のログオンに関する通知**	S	
AC-9(1)	失敗したログオン		
AC-9(2)	成功したログオンおよび失敗したログオン	S	
AC-9(3)	アカウント変更の通知	S	
AC-9(4)	追加のログオン情報	S	
AC-10	**同時セッション制御**	S	
AC-11	**デバイスロック**	S	
AC-11(1)	パターン表示による隠蔽	S	
AC-12	**セッションの終了**	S	
AC-12(1)	ユーザ起動ログアウト	O/S	
AC-12(2)	終了メッセージ	S	
AC-12(3)	タイムアウト警告メッセージ	S	
AC-13	**監視およびレビュー — アクセス制御**	W：AC-2、AU-6 に組み込み	
AC-14	**識別または認証なしに許可される処理**	O	
AC-14(1)	必要な使用法	W：AC-14 に組み込み	
AC-15	**自動マーキング**	W：MP-3 に組み込み	
AC-16	**セキュリティおよびプライバシー属性**	O	
AC-16(1)	動的属性関連付け	S	
AC-16(2)	認可された個人による属性値の変更	S	
AC-16(3)	システムによる属性関連付けの維持	S	
AC-16(4)	認可された個人による属性の関連付け	S	
AC-16(5)	出力されるオブジェクトへの属性表示	S	
AC-16(6)	属性の関連付けの維持	O	
AC-16(7)	一貫した属性解釈	O	
AC-16(8)	関連付けの技法と技術	S	
AC-16(9)	属性の再設定 — 付け替えのメカニズム	O	
AC-16(10)	認可された個人による属性の構成	O	
AC-17	**リモートアクセス**	O	
AC-17(1)	監視および制御	O/S	
AC-17(2)	暗号化を使用した機密性および完全性の保護	S	
AC-17(3)	管理されたアクセス制御ポイント	S	
AC-17(4)	特権コマンドおよびアクセス	O	
AC-17(5)	認可されていない接続の監視	W：SI-4 に組み込み	
AC-17(6)	メカニズムに関する情報の保護	O	

管理策番号	管理策名 拡張管理策名	実装者	保証
AC-17(7)	セキュリティ機能へのアクセスに対する追加的な保護	W：AC-3(10)に組み込み	
AC-17(8)	非セキュアネットワークプロトコルの無効化	W：CM-7 に組み込み	
AC-17(9)	アクセスの切断または無効化	O	
AC-17(10)	リモートコマンドの認証	S	
AC-18	**ワイヤレスアクセス**	O	
AC-18(1)	認証および暗号化	S	
AC-18(2)	認可されていない接続の監視	W：SI-4 に組み込み	
AC-18(3)	ワイヤレスネットワーキングの無効化	O/S	
AC-18(4)	ユーザによる構成設定の制限	O	
AC-18(5)	アンテナおよび伝送電力レベル	O	
AC-19	**モバイルデバイスのアクセス制御**	O	
AC-19(1)	書き込み可能なポータブルストレージデバイスの使用	W：MP-7 に組み込み	
AC-19(2)	個人所有のポータブルストレージデバイスの使用	W：MP-7 に組み込み	
AC-19(3)	識別可能なオーナーのないポータブルストレージデバイスの使用	W：MP-7 に組み込み	
AC-19(4)	国家機密情報の制限	O	
AC-19(5)	デバイス全体またはコンテナ単位の暗号化	O	
AC-20	**外部システムの使用**	O	
AC-20(1)	認可された使用に限定	O	
AC-20(2)	ポータブルストレージデバイス － 使用制限	O	
AC-20(3)	組織が所有していないシステム － 使用制限	O	
AC-20(4)	ネットワークアクセス可能なストレージデバイス － 使用禁止	O	
AC-20(5)	ポータブルストレージデバイス － 使用禁止	O	
AC-21	**情報共有**	O	
AC-21(1)	自動化された意思決定支援	S	
AC-21(2)	情報調査および検索	S	
AC-22	**公的にアクセス可能なコンテンツ**	O	
AC-23	**データマイニングの保護**	O	
AC-24	**アクセス制御の決定**	O	
AC-24(1)	アクセス認可情報の伝送	S	
AC-24(2)	ユーザまたはプロセスのアイデンティティが無い場合	S	
AC-25	**リファレンスモニタ**	S	✓

表 C-2:「意識向上およびトレーニング」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
AT-1	**ポリシーおよび手順**	O	✓
AT-2	**リテラシートレーニングおよび意識向上**	O	✓
AT-2(1)	実践的な演習	O	✓
AT-2(2)	インサイダー脅威	O	✓
AT-2(3)	ソーシャルエンジニアリングおよびマイニング	O	✓
AT-2(4)	疑わしい通信および異常なシステム動作	O	✓
AT-2(5)	持続的標的型攻撃（APT 攻撃）	O	✓
AT-2(6)	サイバー脅威環境	O	✓
AT-3	**役割ベースのトレーニング**	O	✓
AT-3(1)	環境に関する管理策	O	✓
AT-3(2)	物理的セキュリティ管理策	O	✓
AT-3(3)	実践的な演習	O	✓
AT-3(4)	疑わしい通信および異常なシステム動作	W：AT-2(4)に組み込み	
AT-3(5)	個人情報の取扱い	O	✓
AT-4	**トレーニングの記録**	O	✓
AT-5	セキュリティグループおよび団体等との接触	W：PM-15 に組み込み	
AT-6	**トレーニングのフィードバック**	O	✓

表 C-3:「監査および説明責任」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
AU-1	**ポリシーおよび手順**	O	✓
AU-2	**イベントロギング**	O	
AU-2(1)	複数のソースからの監査記録の編集	W:AU-12 に組み込み	
AU-2(2)	コンポーネントによる監査イベントの選択	W:AU-12 に組み込み	
AU-2(3)	レビューおよび更新	W:AU-2 に組み込み	
AU-2(4)	特権機能	W:AC-6(9)に組み込み	
AU-3	**監査記録の内容**	S	
AU-3(1)	追加の監査情報	S	
AU-3(2)	計画的監査記録内容の一元管理	W:PL-9 に組み込み	
AU-3(3)	個人情報要素の限定	O	
AU-4	**監査ロギングのストレージ容量**	O/S	
AU-4(1)	代替ストレージへの転送	O/S	
AU-5	**監査ロギングプロセス障害時の対応**	S	
AU-5(1)	ストレージ容量の警告	S	
AU-5(2)	リアルタイムアラート	S	
AU-5(3)	設定可能なトラフィック量のしきい値	S	
AU-5(4)	障害時のシャットダウン	S	
AU-5(5)	代替監査ロギングケイパビリティ	O	
AU-6	**監査記録のレビュー、分析、および報告**	O	√
AU-6(1)	自動化されたプロセス統合	O	√
AU-6(2)	自動化されたセキュリティアラート	W:SI-4 に組み込み	
AU-6(3)	監査記録リポジトリの関連付け	O	√
AU-6(4)	一元的なレビューおよび分析	S	√
AU-6(5)	監査記録の統合分析	O	√
AU-6(6)	物理的監視との相関	O	√
AU-6(7)	許可される措置	O	√
AU-6(8)	特権コマンドの全文分析	O	√
AU-6(9)	非技術的ソースからの情報との相関	O	√
AU-6(10)	監査レベルの調整	W:AU-6 に組み込み	
AU-7	**監査記録の整理および報告書の作成**	S	√
AU-7(1)	自動処理	S	√
AU-7(2)	自動的な仕分けおよび検索	W:AU-7(1)に組み込み	
AU-8	**タイムスタンプ**	S	
AU-8(1)	信頼できる時刻ソースとの同期	W:SC-45(1)に移動	
AU-8(2)	二次的な信頼できる時刻ソース	W:SC-45(2)に移動	
AU-9	**監査情報の保護**	S	
AU-9(1)	ハードウェア強制型ライトワンスメディア	S	
AU-9(2)	異なる物理的システムまたはコンポーネントへの保存	S	

管理策番号	管理策名 拡張管理策名	実装者	保証
AU-9(3)	暗号化による保護	S	
AU-9(4)	一部の特権ユーザによるアクセス	O	
AU-9(5)	二重認可	O/S	
AU-9(6)	読み取り専用アクセス	O/S	
AU-9(7)	異なるオペレーティングシステムのコンポーネントへの保存	O	
AU-10	**否認防止**	S	√
AU-10(1)	アイデンティティとの関連性	S	√
AU-10(2)	情報作成者のアイデンティティのバインディングの妥当性確認	S	√
AU-10(3)	過程管理	O/S	√
AU-10(4)	情報レビュー実施者のアイデンティティのバインディングの妥当性確認	S	√
AU-10(5)	デジタル署名	W：SI-7 に組み込み	
AU-11	**監査記録の保持**	O	
AU-11(1)	長期的な検索ケイパビリティ	O	√
AU-12	**監査記録の生成**	S	
AU-12(1)	システム全体の時間相関のある監査証跡	S	
AU-12(2)	標準化されたフォーマット	S	
AU-12(3)	認可された個人による変更	S	
AU-12(4)	個人情報のクエリパラメータの監査	S	
AU-13	**情報開示の監視**	O	√
AU-13(1)	自動化されたツールの使用	O/S	√
AU-13(2)	監視対象サイトのレビュー	O	√
AU-13(3)	認可されていない情報の複製	O/S	√
AU-14	**セッション監査**	S	√
AU-14(1)	システムの起動	S	√
AU-14(2)	キャプチャおよび記録内容	W：AU-14 に組み込み	
AU-14(3)	リモートでの視聴	S	√
AU-15	**代替監査ロギングケイパビリティ**	W：AU-5(5)に移動	
AU-16	**組織横断的監査ロギング**	O	
AU-16(1)	アイデンティティの保持	O	
AU-16(2)	監査情報の共有	O	
AU-16(3)	分離可能性	O	

表 C-4:「アセスメント、認可、および監視」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
CA-1	**ポリシーおよび手順**	O	√
CA-2	**管理策アセスメント**	O	√
CA-2(1)	独立したアセッサー	O	√
CA-2(2)	特化したアセスメント	O	√
CA-2(3)	外部組織からの結果の活用	O	√
CA-3	**情報交換**	O	√
CA-3(1)	非機密国家安全保障システムの接続	W:SC-7(25)に移動	
CA-3(2)	国家機密安全保障システムの接続	W:SC-7(26)に移動	
CA-3(3)	非機密非国家安全保障システムの接続	W:SC-7(27)に移動	
CA-3(4)	パブリックネットワークへの接続	W:SC-7(28)に移動	
CA-3(5)	外部システム接続の制限	W:SC-7(5)に組み込み	
CA-3(6)	転送の認可	O/S	√
CA-3(7)	推移的(transitive)情報交換	O/S	√
CA-4	**セキュリティ証明書**	W:CA-2 に組み込み	
CA-5	**実施計画およびマイルストーン**	O	√
CA-5(1)	的確性および最新性サポートの自動化	O	√
CA-6	**認可**	O	√
CA-6(1)	共同認可 – 組織内	O	√
CA-6(2)	共同認可 – 組織間	O	√
CA-7	**継続的監視**	O	√
CA-7(1)	独立したアセスメント	O	√
CA-7(2)	アセスメントのタイプ	W:CA-2 に組み込み	
CA-7(3)	トレンド分析	O	√
CA-7(4)	リスク監視	O/S	√
CA-7(5)	一貫性の分析	O	√
CA-7(6)	監視サポートの自動化	O/S	√
CA-8	**侵入テスト**	O	√
CA-8(1)	独立した侵入テストエージェントまたはチーム	O	√
CA-8(2)	レッドチーム演習	O	√
CA-8(3)	施設への侵入テスト	O	√
CA-9	**内部システム接続**	O	√
CA-9(1)	準拠の確認	O/S	√

表 C-5:「構成管理」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
CM-1	**ポリシーおよび手順**	O	√
CM-2	**ベースライン構成**	O	√
CM-2(1)	レビューおよび更新	W:CM-2 に組み込み	
CM-2(2)	的確性および最新性サポートの自動化	O	√
CM-2(3)	過去の構成の保持	O	√
CM-2(4)	認可されていないソフトウェア	W:CM-7 に組み込み	
CM-2(5)	認可されたソフトウェア	W:CM-7 に組み込み	
CM-2(6)	開発およびテスト環境	O	√
CM-2(7)	高リスク領域のシステムおよびコンポーネントの構成	O	√
CM-3	**構成変更管理**	O	√
CM-3(1)	自動化された文書化、通知、および変更禁止	O	√
CM-3(2)	変更のテスト、妥当性確認、および文書化	O	√
CM-3(3)	自動化された変更措置の反映	O	
CM-3(4)	セキュリティおよびプライバシーに関する代表者	O	
CM-3(5)	自動化されたセキュリティ対応	S	
CM-3(6)	暗号技術による管理	O	
CM-3(7)	システム変更のレビュー	O	
CM-3(8)	構成の変更の防止または制限	S	
CM-4	**インパクト分析**	O	√
CM-4(1)	独立したテスト環境	O	√
CM-4(2)	管理策の検証	O	√
CM-5	**変更に対するアクセス制限**	O	
CM-5(1)	自動化されたアクセス実施および監査記録	S	
CM-5(2)	システム変更のレビュー	W:CM-3(7)に組み込み	
CM-5(3)	署名されたコンポーネント	W:CM-14 に移動	
CM-5(4)	二重認可	O/S	
CM-5(5)	開発および運用に関する特権の限定	O	
CM-5(6)	ライブラリに関する特権の限定	O/S	
CM-5(7)	セキュリティ保全措置の自動実装	W:SI-7 に組み込み	
CM-6	**構成設定**	O/S	
CM-6(1)	自動化された管理、適用、および検証	O	
CM-6(2)	認可されていない変更への対応	O	
CM-6(3)	認可されていない変更の検知	W:SI-7 に組み込み	
CM-6(4)	適合性の立証	W:CM-4 に組み込み	
CM-7	**最小機能性**	O/S	
CM-7(1)	定期的なレビュー	O/S	
CM-7(2)	プログラムの実行の防止	S	
CM-7(3)	登録に関する準拠	O	

管理策番号	管理策名 拡張管理策名	実装者	保証
CM-7(4)	認可されていないソフトウェア – 例外による拒否	O/S	
CM-7(5)	認可されたソフトウェア – 例外による許可	O/S	
CM-7(6)	限定された特権を備えた制限環境	O	√
CM-7(7)	保護された環境内でのコードの実行	O/S	√
CM-7(8)	バイナリまたはマシン実行可能コード	O/S	√
CM-7(9)	認可されていないハードウェアの使用の禁止	O/S	√
CM-8	**システムコンポーネントのインベントリ**	O	√
CM-8(1)	インストール中および削除中の更新	O	√
CM-8(2)	自動化されたメンテナンス	O	√
CM-8(3)	認可されていないコンポーネントの自動化された検知	O	√
CM-8(4)	説明責任情報	O	√
CM-8(5)	コンポーネントの非重複算出	W：CM-8 に組み込み	
CM-8(6)	アセスメント済みの構成および承認された偏差	O	√
CM-8(7)	集中化されたリポジトリ	O	√
CM-8(8)	自動化された位置追跡機能	O	√
CM-8(9)	システムへのコンポーネントの設定	O	√
CM-9	**構成管理計画**	O	
CM-9(1)	責任の設定	O	
CM-10	**ソフトウェアの使用制限**	O	
CM-10(1)	オープンソースソフトウェア	O	
CM-11	**ユーザがインストールしたソフトウェア**	O	
CM-11(1)	認可されていないインストールに対するアラート	W：CM-8(3)に組み込み	
CM-11(2)	特権状態でのソフトウェアのインストール	S	
CM-11(3)	自動化された実施および監視	S	√
CM-12	**情報の位置**	O	√
CM-12(1)	情報の位置をサポートする自動化されたツール	O	√
CM-13	**データアクションのマッピング**	O	
CM-14	**署名されたコンポーネント**	O/S	√

表 C-6:「緊急時対応計画」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
CP-1	**ポリシーおよび手順**	O	√
CP-2	**緊急時対応計画**	O	
CP-2(1)	関連計画との調整	O	
CP-2(2)	処理能力計画	O	
CP-2(3)	ミッションおよび事業機能の再開	O	
CP-2(4)	すべてのミッションおよび事業機能の再開	W:CP-2(3)に組み込み	
CP-2(5)	ミッションおよび事業機能の継続	O	
CP-2(6)	代替処理サイトおよび代替保管サイト	O	
CP-2(7)	外部サービスプロバイダとの調整	O	
CP-2(8)	重要な資産の特定	O	
CP-3	**緊急時対応トレーニング**	O	√
CP-3(1)	シミュレーションイベント	O	√
CP-3(2)	トレーニング環境で使用されるメカニズム	O	√
CP-4	**緊急時対応計画テスト**	O	√
CP-4(1)	関連計画との調整	O	√
CP-4(2)	代替処理サイト	O	√
CP-4(3)	自動化されたテスト	O	√
CP-4(4)	完全な復旧および再構成	O	√
CP-4(5)	自己チャレンジ	O/S	√
CP-5	緊急時対応計画の更新	W:CP-2 に組み込み	
CP-6	**代替保管サイト**	O	
CP-6(1)	一次サイトからの分離	O	
CP-6(2)	復旧時間および復旧ポイントの目標	O	
CP-6(3)	アクセシビリティ	O	
CP-7	**代替処理サイト**	O	
CP-7(1)	一次サイトからの分離	O	
CP-7(2)	アクセシビリティ	O	
CP-7(3)	サービスの優先順位	O	
CP-7(4)	使用準備	O	
CP-7(5)	同等の情報セキュリティ保全措置	W:CP-7 に組み込み	
CP-7(6)	一次サイトに復帰できない状況	O	
CP-8	**通信サービス**	O	
CP-8(1)	サービス提供の優先順位	O	
CP-8(2)	単一障害点	O	
CP-8(3)	一次プロバイダおよび代替プロバイダの分離	O	
CP-8(4)	プロバイダの緊急時対応計画	O	
CP-8(5)	代替通信サービスのテスト	O	
CP-9	**システムバックアップ**	O	

管理策番号	管理策名 拡張管理策名	実装者	保証
CP-9(1)	信頼性および完全性のテスト	O	
CP-9(2)	サンプリングを使用した復元テスト	O	
CP-9(3)	重要な情報の分離保管	O	
CP-9(4)	認可されていない変更からの保護	W：CP-9 に組み込み	
CP-9(5)	代替保管サイトへの転送	O	
CP-9(6)	冗長二次システム	O	
CP-9(7)	削除や破壊に対する二重認可	O	
CP-9(8)	暗号化による保護	O	
CP-10	**システムの復旧および再構成**	O	
CP-10(1)	緊急時対応計画のテスト	W：CP-4 に組み込み	
CP-10(2)	トランザクションの復旧	O	
CP-10(3)	代替セキュリティ管理策	W：テーラリングにより対処	
CP-10(4)	期間内の復元	O	
CP-10(5)	フェイルオーバーケイパビリティ	W：SI-13 に組み込み	
CP-10(6)	コンポーネントの保護	O	
CP-11	**代替通信プロトコル**	O	
CP-12	**セーフモード**	S	√
CP-13	**代替セキュリティのメカニズム**	O/S	

表 C-7:「識別および認証」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
IA-1	**ポリシーおよび手順**	O	√
IA-2	**識別および認証（組織のユーザ）**	O/S	
IA-2(1)	特権アカウントへの多要素認証	S	
IA-2(2)	非特権アカウントへの多要素認証	S	
IA-2(3)	特権アカウントへのローカルアクセス	W：IA-2(1)に組み込み	
IA-2(4)	非特権アカウントへのローカルアクセス	W：IA-2(2)に組み込み	
IA-2(5)	グループ認証時の個人認証	O/S	
IA-2(6)	アカウントへのアクセス — 別のデバイス	S	
IA-2(7)	非特権アカウントへのネットワークアクセス — 別のデバイス	W：IA-2(6)に組み込み	
IA-2(8)	アカウントへのアクセス — リプレイ攻撃耐性	S	
IA-2(9)	非特権アカウントへのネットワークアクセス — リプレイ攻撃耐性	W：IA-2(8)に組み込み	
IA-2(10)	シングルサインオン	S	
IA-2(11)	リモートアクセス — 別のデバイス	W：IA-2(6)に組み込み	
IA-2(12)	PIV クレデンシャルの受け入れ	S	
IA-2(13)	経路外通信認証	S	
IA-3	**デバイスの識別および認証**	S	
IA-3(1)	暗号双方向認証	S	
IA-3(2)	暗号双方向ネットワーク認証	W：IA-3(1)に組み込み	
IA-3(3)	動的アドレス割り当て	O	
IA-3(4)	デバイス証明	O	
IA-4	**識別子管理**	O	
IA-4(1)	公開識別子のアカウント識別子使用禁止	O	
IA-4(2)	監督者による認可	W：IA-12(1)に組み込み	
IA-4(3)	複数の認証形態	W：IA-12(2)に組み込み	
IA-4(4)	ユーザステータスの識別	O	
IA-4(5)	動的管理	S	
IA-4(6)	組織横断的な管理	O	
IA-4(7)	対面による登録	W：IA-12(4)に組み込み	
IA-4(8)	ペアワイズ仮名識別子	O	
IA-4(9)	属性の維持および保護	O/S	
IA-5	**オーセンティケータ管理**	O/S	
IA-5(1)	パスワードによる認証	O/S	
IA-5(2)	公開鍵ベースの認証	S	
IA-5(3)	対面または信頼できる外部関係者による登録	W：IA-12(4)に組み込み	
IA-5(4)	パスワード強度決定の自動化されたサポート	W：IA-5(1)に組み込み	
IA-5(5)	出荷前のオーセンティケータ変更	O	
IA-5(6)	オーセンティケータの保護	O	
IA-5(7)	暗号化されていない静的オーセンティケータの組み込み禁止	O	

管理策番号	管理策名 拡張管理策名	実装者	保証
IA-5(8)	複数のシステムアカウント	O	
IA-5(9)	フェデレーションによるクレデンシャル管理	O	
IA-5(10)	動的クレデンシャルのバインディング	S	
IA-5(11)	ハードウェアトークンによる認証	W：IA-2(1), IA-2(2)に組み込み	
IA-5(12)	ハードウェアトークンによる認証	S	
IA-5(13)	キャッシュされたオーセンティケータの期限	S	
IA-5(14)	PKI トラストストアの内容管理	O	
IA-5(15)	GSA 承認の製品およびサービス	O	
IA-5(16)	対面または信頼できる外部関係者によるオーセンティケータの発行	O	
IA-5(17)	生体情報の提示型攻撃検知	S	
IA-5(18)	パスワードマネージャー	S	
IA-6	**認証フィードバック**	S	
IA-7	**暗号モジュール認証**	S	
IA-8	**識別および認証（非組織のユーザ）**	S	
IA-8(1)	他の機関からの PIV クレデンシャルの受け入れ	S	
IA-8(2)	外部オーセンティケータの受け入れ	S	
IA-8(3)	FICAM 承認製品の使用	W：IA-8(2)に組み込み	
IA-8(4)	定義したプロファイルの使用	S	
IA-8(5)	PIV-I クレデンシャルの受け入れ	S	
IA-8(6)	分離可能性	O	
IA-9	**サービスの識別および認証**	O/S	
IA-9(1)	情報交換	W：IA-9 に組み込み	
IA-9(2)	判断の伝達	W：IA-9 に組み込み	
IA-10	**リスクベース認証**	O	
IA-11	**再認証**	O/S	
IA-12	**アイデンティティ証明**	O	
IA-12(1)	監督者認可	O	
IA-12(2)	アイデンティティのエビデンス	O	
IA-12(3)	アイデンティティのエビデンスの妥当性確認および検証	O	
IA-12(4)	対面による妥当性確認および検証	O	
IA-12(5)	アドレス確認	O	
IA-12(6)	外部で証明されたアイデンティティの受け入れ	O	

表 C-8：「インシデント対応」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
IR-1	**ポリシーおよび手順**	O	√
IR-2	**インシデント対応トレーニング**	O	√
IR-2(1)	シミュレーションイベント	O	√
IR-2(2)	自動化されたトレーニング環境	O	√
IR-2(3)	ブリーチ	O	√
IR-3	**インシデント対応テスト**	O	√
IR-3(1)	自動化されたテスト	O	√
IR-3(2)	関連計画との調整	O	√
IR-3(3)	継続的改善	O	√
IR-4	**インシデント対応**	O	
IR-4(1)	自動化されたインシデント対応プロセス	O	
IR-4(2)	動的再構成	O	
IR-4(3)	運用の継続性	O	
IR-4(4)	情報の相互関連付け	O	
IR-4(5)	システムの自動無効化	O/S	
IR-4(6)	インサイダー脅威	O	
IR-4(7)	インサイダー脅威 — 組織内連携	O	
IR-4(8)	外部組織との相互関連付け	O	
IR-4(9)	動的対応ケイパビリティ	O	
IR-4(10)	サプライチェーンとの連携	O	
IR-4(11)	統合インシデント対応チーム	O	
IR-4(12)	悪意のあるコードおよびフォレンジック分析	O	
IR-4(13)	ふるまい分析	O	
IR-4(14)	セキュリティオペレーションセンター	O/S	
IR-4(15)	広報活動および評判の修復	O	
IR-5	**インシデント監視**	O	√
IR-5(1)	自動化された追跡、データ収集、および分析	O	√
IR-6	**インシデント報告**	O	
IR-6(1)	自動化された報告	O	
IR-6(2)	インシデントに関連する脆弱性	O	
IR-6(3)	サプライチェーンとの連携	O	
IR-7	**インシデント対応支援**	O	
IR-7(1)	情報およびサポートの可用性のための自動化されたサポート	O	
IR-7(2)	外部プロバイダとの連携	O	
IR-8	**インシデント対応計画**	O	
IR-8(1)	ブリーチ	O	
IR-9	**情報流出対応**	O	
IR-9(1)	責任者	W：IR-9 に組み込み	

管理策番号	管理策名 拡張管理策名	実装者	保証
IR-9(2)	トレーニング	O	
IR-9(3)	流出後の運用	O	
IR-9(4)	認可されていない職員への露出	O	
IR-10	統合情報セキュリティ分析チーム	W：IR-4(11)に移動	

表 C-9:「メンテナンス」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
MA-1	**ポリシーおよび手順**	O	√
MA-2	**管理されたメンテナンス**	O	
MA-2(1)	記録内容	W:MA-2 に組み込み	
MA-2(2)	自動化されたメンテナンス措置	O	
MA-3	**メンテナンスツール**	O	
MA-3(1)	ツールの検査	O	
MA-3(2)	媒体の検査	O	
MA-3(3)	認可されていない移動の防止	O	
MA-3(4)	ツールの使用制限	O/S	
MA-3(5)	特権での実行	O/S	
MA-3(6)	ソフトウェアの更新およびパッチ	O/S	
MA-4	**非ローカルメンテナンス**	O	
MA-4(1)	ロギングおよびレビュー	O	
MA-4(2)	非ローカルメンテナンスの文書化	W:MA-1, MA-4 に組み込み	
MA-4(3)	同等のセキュリティおよびサニタイズ	O	
MA-4(4)	メンテナンスセッションの認証および分離	O	
MA-4(5)	承認および通知	O	
MA-4(6)	暗号による保護	O/S	
MA-4(7)	切断の検証	S	
MA-5	**メンテナンス作業員**	O	
MA-5(1)	適切なアクセス権限のない個人	O	
MA-5(2)	国家機密情報を扱うシステムのセキュリティクリアランス	O	
MA-5(3)	国家機密情報を扱うシステムの米国市民権要件	O	
MA-5(4)	外国人	O	
MA-5(5)	システム以外のメンテナンス	O	
MA-6	**タイムリーなメンテナンス**	O	
MA-6(1)	予防メンテナンス	O	
MA-6(2)	予測メンテナンス	O	
MA-6(3)	予測メンテナンスのための自動化されたサポート	O	
MA-7	**フィールドメンテナンス**	O	

表 C-10:「媒体保護」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
MP-1	**ポリシーおよび手順**	O	√
MP-2	**媒体へのアクセス**	O	
MP-2(1)	自動化されたアクセス制限	W:MP-4(2)に組み込み	
MP-2(2)	暗号による保護	W:SC-28(1)に組み込み	
MP-3	**媒体へのマーキング**	O	
MP-4	**媒体保管**	O	
MP-4(1)	暗号による保護	W:SC-28(1)に組み込み	
MP-4(2)	自動化されたアクセス制限	O	
MP-5	**媒体移送**	O	
MP-5(1)	管理エリア外での保護	W:MP-5 に組み込み	
MP-5(2)	活動の文書化	W:MP-5 に組み込み	
MP-5(3)	管理人	O	
MP-5(4)	暗号による保護	W:SC-28(1)に組み込み	
MP-6	**媒体のサニタイズ**	O	
MP-6(1)	レビュー、承認、追跡、文書化、検証	O	
MP-6(2)	装置のテスト	O	
MP-6(3)	非破壊的技法	O	
MP-6(4)	管理対象非機密情報	W:MP-6 に組み込み	
MP-6(5)	国家機密情報	W:MP-6 に組み込み	
MP-6(6)	媒体の破壊	W:MP-6 に組み込み	
MP-6(7)	二重認可	O	
MP-6(8)	情報のリモート除去またはリモート抹消	O	
MP-7	**媒体の使用**	O	
MP-7(1)	オーナーなしでの使用禁止	W:MP-7 に組み込み	
MP-7(2)	サニタイズ耐性のある媒体の使用禁止	O	
MP-8	**媒体のダウングレード**	O	
MP-8(1)	プロセスの文書化	O	
MP-8(2)	装置のテスト	O	
MP-8(3)	管理対象非機密情報	O	
MP-8(4)	国家機密情報	O	

表 C-11:「物理的および環境的保護」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
PE-1	**ポリシーおよび手順**	O	√
PE-2	**物理的アクセス認可**	O	
PE-2(1)	職位または役割によるアクセス	O	
PE-2(2)	2 つの身分証明書	O	
PE-2(3)	エスコートされていないアクセスの制限	O	
PE-3	**物理的アクセス制御**	O	
PE-3(1)	システムアクセス	O	
PE-3(2)	施設およびシステム	O	
PE-3(3)	継続的な警備	O	
PE-3(4)	施錠可能なケース	O	
PE-3(5)	タンパー保護	O	
PE-3(6)	施設の侵入テスト	W:CA-8 に組み込み	
PE-3(7)	物理的障壁	O	
PE-3(8)	前室のアクセス制御	O	
PE-4	**伝送設備のアクセス制御**	O	
PE-5	**出力デバイスのアクセス制御**	O	
PE-5(1)	認可された個人による出力情報へのアクセス	W:PE-5 に組み込み	
PE-5(2)	個人のアイデンティティへのリンク	S	
PE-5(3)	出力デバイスのマーキング	W:PE-22 に組み込み	
PE-6	**物理的アクセスの監視**	O	√
PE-6(1)	侵入警報装置および侵入監視装置	O	√
PE-6(2)	自動化された侵入検知および侵入対応	O	√
PE-6(3)	ビデオ監視	O	√
PE-6(4)	システムへの物理的アクセスの監視	O	√
PE-7	**来訪者制御**	W:PE-2, PE-3 に組み込み	
PE-8	**来訪者アクセス記録**	O	√
PE-8(1)	自動化された記録の維持およびレビュー	O	
PE-8(2)	物理的アクセス記録	W:PE-2 に組み込み	
PE-8(3)	個人情報要素の限定	O	
PE-9	**電源装置およびケーブル**	O	
PE-9(1)	冗長ケーブル	O	
PE-9(2)	自動電圧制御	O	
PE-10	**緊急遮断**	O	
PE-10(1)	偶発的および認可されていない起動	W:PE-10 に組み込み	
PE-11	**非常用電源**	O	
PE-11(1)	代替電源 － 最小運用ケイパビリティ	O	
PE-11(2)	代替電源 － 自給型	O	
PE-12	**非常用照明**	O	

管理策番号	管理策名 拡張管理策名	実装者	保証
PE-12(1)	必須のミッションおよび事業機能	O	
PE-13	**防火**	O	
PE-13(1)	検知システム ― 自動起動および通知	O	
PE-13(2)	消火システム ― 自動起動および通知	O	
PE-13(3)	自動消火	W：PE-13(2)に組み込み	
PE-13(4)	点検	O	
PE-14	**環境制御**	O	
PE-14(1)	自動制御	O	
PE-14(2)	警報および通知による監視	O	
PE-15	**漏水損傷保護**	O	
PE-15(1)	自動サポート	O	
PE-16	**搬入および搬出**	O	
PE-17	**代替作業サイト**	O	
PE-18	**システムコンポーネントの設置場所**	O	
PE-18(1)	施設サイト	W：PE-23 に移動	
PE-19	**情報漏えい**	O	
PE-19(1)	国家エミッションポリシーおよび手順	O	
PE-20	**資産の監視および追跡**	O	
PE-21	**電磁パルス保護**	O	
PE-22	**コンポーネントマーキング**	O	
PE-23	**施設の場所**	O	

表 C-12：「計画」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
PL-1	**ポリシーおよび手順**	O	√
PL-2	**システムセキュリティおよびプライバシー計画**	O	√
PL-2(1)	業務構想文書	W:PL-7 に組み込み	
PL-2(2)	機能アーキテクチャ	W：PL-8 に組み込み	
PL-2(3)	他の組織のエンティティとの計画策定および調整	W：PL-2 に組み込み	
PL-3	システムセキュリティ計画の更新	W：PL-2 に組み込み	
PL-4	**行動規則**	O	√
PL-4(1)	ソーシャルメディアおよび外部サイト／アプリケーションの使用制限	O	√
PL-5	プライバシー影響評価	W：RA-8 に組み込み	
PL-6	セキュリティ関連措置計画	W：PL-2 に組み込み	
PL-7	**業務構想文書**	O	
PL-8	**セキュリティおよびプライバシーアーキテクチャ**	O	√
PL-8(1)	多層防御	O	√
PL-8(2)	サプライヤの多様性	O	√
PL-9	**一元管理**	O	√
PL-10	**ベースラインの選択**	O	
PL-11	**ベースラインのテーラリング**	O	

表 C-13:「プログラムマネジメント」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
PM-1	**情報セキュリティプログラム計画**	O	
PM-2	**情報セキュリティプログラムの責任者の役割**	O	
PM-3	**情報セキュリティおよびプライバシーリソース**	O	
PM-4	**実施計画およびマイルストーンプロセス**	O	
PM-5	**システムインベントリ**	O	
PM-5(1)	個人情報のインベントリ	O	
PM-6	**パフォーマンス尺度**	O	√
PM-7	**エンタープライズアーキテクチャ**	O	
PM-7(1)	オフロード	O	
PM-8	**重要インフラ計画**	O	
PM-9	**リスクマネジメント戦略**	O	√
PM-10	**認可プロセス**	O	√
PM-11	**ミッションおよび事業プロセスの規定**	O	
PM-12	**インサイダー脅威対策プログラム**	O	√
PM-13	**セキュリティおよびプライバシー要員**	O	
PM-14	**テスト、トレーニング、および監視**	O	√
PM-15	**セキュリティおよびプライバシーのグループおよび団体**	O	
PM-16	**脅威認識プログラム**	O	√
PM-16(1)	脅威インテリジェンスを共有するための自動化された手段	O	√
PM-17	**外部システム上の管理対象非機密情報の保護**	O	√
PM-18	**プライバシープログラム計画**	O	
PM-19	**プライバシープログラムの責任者の役割**	O	
PM-20	**プライバシープログラム情報の配布**	O	
PM-20(1)	ウェブサイト、アプリケーション、およびデジタルサービスのプライバシーポリシー	O	√
PM-21	**開示事項のアカウンティング**	O	
PM-22	**個人情報の品質管理**	O	√
PM-23	**データガバナンス会議体**	O	√
PM-24	**データインテグリティ委員会**	O	√
PM-25	**テスト、トレーニング、および研究で使用される個人情報の最小化**	O	
PM-26	**苦情管理**	O	
PM-27	**プライバシー報告**	O	
PM-28	**リスクの枠組み**	O	√
PM-29	**リスクマネジメントプログラムの責任者の役割**	O	
PM-30	**サプライチェーンのリスクマネジメント戦略**	O	√
PM-30(1)	重要なまたはミッションに必須のアイテムのサプライヤ	O	√
PM-31	**継続的監視戦略**	O	

管理策番号	管理策名 拡張管理策名	実装者	保証
PM-32	**目的**	O	√

表 C-14：「職員のセキュリティ」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
PS-1	**ポリシーおよび手順**	O	√
PS-2	**職位のリスク指定**	O	
PS-3	**職員のスクリーニング**	O	
PS-3(1)	国家機密情報	O	
PS-3(2)	正式な教化	O	
PS-3(3)	特別な保護手段を必要とする情報	O	
PS-3(4)	市民権要件	O	
PS-4	**職員の雇用終了**	O	
PS-4(1)	雇用終了後要件	O	
PS-4(2)	自動化された措置	O	
PS-5	**職員の異動**	O	
PS-6	**アクセス合意書**	O	√
PS-6(1)	特別な保護が必要な情報	W：PS-3 に組み込み	
PS-6(2)	特別な保護を必要とする国家機密情報	O	√
PS-6(3)	雇用終了後要件	O	√
PS-7	**外部職員のセキュリティ**	O	√
PS-8	**職員の制裁**	O	
PS-9	**職位記述**	O	

表 C-15：「個人情報の取扱いおよび透明性」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
PT-1	**ポリシーおよび手順**	O	√
PT-2	**個人情報を取扱う職権**	O	√
PT-2(1)	データタグ付け	S	√
PT-2(2)	自動化	O	√
PT-3	**個人情報の取扱い目的**	O	
PT-3(1)	データタグ付け	S	√
PT-3(2)	自動化	O	√
PT-4	**同意**	O	
PT-4(1)	テーラリングされた同意	O	
PT-4(2)	ジャストインタイムの同意	O	
PT-4(3)	取消し	O	
PT-5	**プライバシー通知**	O	
PT-5(1)	ジャストインタイムの通知	O	
PT-5(2)	プライバシー保護法のステートメン	O	
PT-6	**記録システムの通知**	O	
PT-6(1)	定常的な利用	O	
PT-6(2)	適用除外規定	O	
PT-7	**個人情報の特定の分類**	O	
PT-7(1)	社会保障番号	O	
PT-7(2)	第一修正条項情報	O	
PT-8	**コンピュータマッチング要件**	O	

表 C-16:「リスクアセスメント」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
RA-1	**ポリシーおよび手順**	O	√
RA-2	**セキュリティ分類化**	O	
RA-2(1)	インパクトレベルの優先順位付け	O	
RA-3	**リスクアセスメント**	O	√
RA-3(1)	サプライチェーンのリスクアセスメント	O	√
RA-3(2)	オールソースインテリジェンスの活用	O	√
RA-3(3)	動的脅威認識	O	√
RA-3(4)	予測的サイバー分析	O	√
RA-4	リスクアセスメントの更新	W:RA-3 に組み込み	
RA-5	**脆弱性の監視およびスキャン**	O	√
RA-5(1)	ツール機能の更新	W:RA-5 に組み込み	
RA-5(2)	スキャンする脆弱性の更新	O	√
RA-5(3)	カバレッジの幅および深さ	O	√
RA-5(4)	検出可能な情報	O	√
RA-5(5)	特権アクセス	O	√
RA-5(6)	自動化された傾向分析	O	√
RA-5(7)	認可されていないコンポーネントの自動化された検知および通知	W:CM-8 に組み込み	
RA-5(8)	過去の監査ログのレビュー	O	√
RA-5(9)	侵入テストおよび分析	W:CA-8 に組み込み	
RA-5(10)	スキャン情報の相関	O	√
RA-5(11)	公開開示プログラム	O	√
RA-6	**技術監視対策調査**	O	√
RA-7	**リスク対応**	O	√
RA-8	**プライバシー影響評価**	O	√
RA-9	**重要度分析**	O	
RA-10	**脅威ハンティング**	O/S	√

表 C-17:「システムおよびサービスの取得」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
SA-1	**ポリシーおよび手順**	O	√
SA-2	**リソースの割り当て**	O	√
SA-3	**システム開発ライフサイクル**	O	√
SA-3(1)	運用前環境の管理	O	√
SA-3(2)	ライブデータまたは運用データの使用	O	√
SA-3(3)	技術の更新	O	√
SA-4	**取得プロセス**	O	√
SA-4(1)	管理策の機能特性	O	√
SA-4(2)	管理策のための設計および実装情報	O	√
SA-4(3)	開発方法、技法、および実践	O	√
SA-4(4)	システムへのコンポーネントの割り当て	W:CM-8(9)に組み込み	
SA-4(5)	システム、コンポーネント、およびサービスの構成	O	√
SA-4(6)	情報保証製品の使用	O	√
SA-4(7)	NIAP 承認済みプロテクションプロファイル	O	√
SA-4(8)	管理策の継続的監視計画	O	√
SA-4(9)	使用中の機能、ポート、プロトコル、およびサービス	O	√
SA-4(10)	承認された PIV 製品の使用	O	√
SA-4(11)	記録システム	O	√
SA-4(12)	データオーナー	O	√
SA-5	**システムドキュメント**	O	√
SA-5(1)	セキュリティ管理策の機能的特性	W:SA-4(1)に組み込み	
SA-5(2)	セキュリティ関連の外部システムインタフェース	W:SA-4(2)に組み込み	
SA-5(3)	高レベル設計	W:SA-4(2)に組み込み	
SA-5(4)	低レベル設計	W:SA-4(2)に組み込み	
SA-5(5)	ソースコード	W:SA-4(2)に組み込み	
SA-6	**ソフトウェアの使用制限**	W:CM-10, SI-7 に組み込み	
SA-7	**ユーザがインストールしたソフトウェア**	W:CM-11, SI-7 に組み込み	
SA-8	**セキュリティおよびプライバシーエンジニアリングの原則**	O	√
SA-8(1)	明確な抽象化	O/S	√
SA-8(2)	最小共通メカニズム	O/S	√
SA-8(3)	モジュール性および階層化	O/S	√
SA-8(4)	半順序の依存関係	O/S	√
SA-8(5)	効率的に仲介されたアクセス	O/S	√
SA-8(6)	共有の最小化	O/S	√
SA-8(7)	複雑さの軽減	O/S	√
SA-8(8)	セキュアな保守拡張性	O/S	√
SA-8(9)	信頼できるコンポーネント	O/S	√
SA-8(10)	階層的信頼	O/S	√

管理策番号	管理策名 拡張管理策名	実装者	保証
SA-8(11)	逆変更しきい値	O/S	√
SA-8(12)	階層的保護	O/S	√
SA-8(13)	最小化されたセキュリティ要素	O/S	√
SA-8(14)	最小特権	O/S	√
SA-8(15)	根拠のある許可	O/S	√
SA-8(16)	自立した統合的信頼性	O/S	√
SA-8(17)	セキュアな分散構成	O/S	√
SA-8(18)	信頼できる通信チャネル	O/S	√
SA-8(19)	継続的な保護	O/S	√
SA-8(20)	セキュアなメタデータ管理	O/S	√
SA-8(21)	自己分析	O/S	√
SA-8(22)	説明責任およびトレーサビリティ	O/S	√
SA-8(23)	セキュアデフォルト	O/S	√
SA-8(24)	セキュアな障害および復旧	O/S	√
SA-8(25)	経済的セキュリティ	O/S	√
SA-8(26)	パフォーマンスセキュリティ	O/S	√
SA-8(27)	人的要因によるセキュリティ	O/S	√
SA-8(28)	許容可能なセキュリティ	O/S	√
SA-8(29)	再現性のある文書化された手順	O/S	√
SA-8(30)	手順の厳格さ	O/S	√
SA-8(31)	セキュアなシステム変更	O/S	√
SA-8(32)	十分なドキュメント	O/S	√
SA-8(33)	最小化	O/S	√
SA-9	**外部システムサービス**	O	√
SA-9(1)	リスクアセスメントおよび組織承認	O	√
SA-9(2)	機能、ポート、プロトコル、およびサービスの特定	O	√
SA-9(3)	プロバイダとの信頼関係の確立および維持	O	√
SA-9(4)	消費者およびプロバイダの一貫した利益	O	√
SA-9(5)	処理、保管、およびサービスの場所	O	√
SA-9(6)	組織が管理する暗号鍵	O	√
SA-9(7)	組織管理の完全性チェック	O	√
SA-9(8)	処理および保管場所 － 米国の司法管轄	O	√
SA-10	**開発者構成管理**	O	√
SA-10(1)	ソフトウェアおよびファームウェアの完全性の検証	O	√
SA-10(2)	代替構成管理プロセス	O	√
SA-10(3)	ハードウェアの完全性の検証	O	√
SA-10(4)	信頼できる世代	O	√
SA-10(5)	バージョン管理のための完全性のマッピング	O	√
SA-10(6)	信頼できる配布	O	√
SA-10(7)	セキュリティおよびプライバシーの代表者	O	√

管理策番号	管理策名 拡張管理策名	実装者	保証
SA-11	**開発者のテストおよび評価**	O	√
SA-11(1)	静的コード分析	O	√
SA-11(2)	脅威のモデル化および脆弱性の分析	O	√
SA-11(3)	アセスメント計画およびエビデンスの独立した検証	O	√
SA-11(4)	手動のコードレビュー	O	√
SA-11(5)	侵入テスト	O	√
SA-11(6)	攻撃対象領域のレビュー	O	√
SA-11(7)	テストおよび評価の範囲の検証	O	√
SA-11(8)	動的コード分析	O	√
SA-11(9)	対話型のアプリケーションのセキュリティテスト	O	√
SA-12	**サプライチェーンの保護**	W：SR ファミリーに移動	
SA-12(1)	取得戦略／ツール／方法	W：SR-5 に移動	
SA-12(2)	サプライヤのレビュー	W：SR-6 に移動	
SA-12(3)	信頼できる配送および倉庫管理	W：SR-3 に組み込み	
SA-12(4)	サプライヤの多様性	W：SR-3(1)に移動	
SA-12(5)	損害の限定	W：SR-3(2)に移動	
SA-12(6)	調達時間の最小化	W：SR-5(1)に組み込み	
SA-12(7)	選択／受領／更新前のアセスメント	W：SR-5(2)に移動	
SA-12(8)	オールソースインテリジェンスの活用	W：RA-3(2)に組み込み	
SA-12(9)	運用セキュリティ	W：SR-7 に移動	
SA-12(10)	本物であり、改変されていないことの確認	W：SR-4(3)に移動	
SA-12(11)	侵入テスト／要素、プロセス、および行為者の分析	W：SR-6(1)に移動	
SA-12(12)	組織間の合意	W：SR-8 に移動	
SA-12(13)	重要な情報システムのコンポーネント	W：MA-6, RA-9 に組み込み	
SA-12(14)	アイデンティティおよびトレーサビリティ	W：SR-4(1), SR-4(2)に移動	
SA-12(15)	弱点または欠陥に対処するためのプロセス	W：SR-3 に組み込み	
SA-13	**統合的信頼性**	W：SA-8 に組み込み	
SA-14	**重要度分析**	W：RA-9 に組み込み	
SA-14(1)	代替調達が不可能な重要なコンポーネント	W：SA-20 に組み込み	
SA-15	**開発プロセス、規格、およびツール**	O	√
SA-15(1)	品質指標	O	√
SA-15(2)	セキュリティおよびプライバシーの追跡ツール	O	√
SA-15(3)	重要度分析	O	√
SA-15(4)	脅威のモデル化および脆弱性の分析	W：SA-11(2)に組み込み	
SA-15(5)	攻撃対象領域の削減	O	√
SA-15(6)	継続的な改善	O	√
SA-15(7)	自動化された脆弱性分析	O	√
SA-15(8)	脅威および脆弱性情報の再利用	O	√
SA-15(9)	ライブデータの使用	W：SA-3(2)に組み込み	
SA-15(10)	インシデント対応計画	O	√

管理策番号	管理策名 拡張管理策名	実装者	保証
SA-15(11)	システムまたはコンポーネントのアーカイブ	O	√
SA-15(12)	個人情報の最小化	O	√
SA-16	**開発者が提供するトレーニング**	O	√
SA-17	**開発者のセキュリティおよびプライバシーのアーキテクチャおよび設計**	O	√
SA-17(1)	正式なポリシーモデル	O	√
SA-17(2)	セキュリティ関連のコンポーネント	O	√
SA-17(3)	正式な対応	O	√
SA-17(4)	非公式な対応	O	√
SA-17(5)	概念的にシンプルな設計	O	√
SA-17(6)	テストのための構造	O	√
SA-17(7)	最小特権の構造	O	√
SA-17(8)	オーケストレーション	O	√
SA-17(9)	設計の多様性	O	√
SA-18	**耐タンパー性および検知**	W：SR-9 に移動	
SA-18(1)	システム開発ライフサイクルの複数のフェーズ	W：SR-9(1)に移動	
SA-18(2)	システムまたはコンポーネントの検査	W：SR-10 に移動	
SA-19	**コンポーネントの真正性**	W：SR-11 に移動	
SA-19(1)	偽造防止トレーニング	W：SR-11(1)に移動	
SA-19(2)	コンポーネントのサービスおよび修理のための構成管理	W：SR-11(2)に移動	
SA-19(3)	コンポーネントの廃棄	W：SR-12 に移動	
SA-19(4)	偽造防止の精査	W：SR-11(3)に移動	
SA-20	**重要コンポーネントのカスタム開発**	O	√
SA-21	**開発者のスクリーニング**	O	√
SA-21(1)	スクリーニングの妥当性確認	W：SA-21 に組み込み	
SA-22	**サポートされていないシステムコンポーネント**	O	√
SA-22(1)	継続的サポートの代替ソース	W：SA-22 に組み込み	
SA-23	**特殊化**	O	√

表 C-18:「システムおよび通信の保護」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
SC-1	**ポリシーおよび手順**	O	√
SC-2	**システムおよびユーザ機能の分離**	S	√
SC-2(1)	非特権ユーザのためのインタフェース	S	√
SC-2(2)	分離可能性	S	√
SC-3	**セキュリティ機能の分離**	S	√
SC-3(1)	ハードウェアの分離	S	√
SC-3(2)	アクセスおよびフロー制御機能	S	√
SC-3(3)	非セキュリティ機能の最小化	O/S	√
SC-3(4)	モジュールの結合度および凝集度	O/S	√
SC-3(5)	階層構造	O/S	√
SC-4	**共有システムリソース内の情報**	S	
SC-4(1)	セキュリティレベル	W:SC-4 に組み込み	
SC-4(2)	マルチレベルまたは期間処理	S	
SC-5	**サービス拒否からの保護**	S	
SC-5(1)	他のシステムへの攻撃能力の制限	S	
SC-5(2)	容量、帯域幅、および冗長性	S	
SC-5(3)	検知および監視	S	
SC-6	**リソースの可用性**	S	√
SC-7	**境界保護**	S	
SC-7(1)	物理的に分離されたサブネットワーク	W:SC-7 に組み込み	
SC-7(2)	パブリックアクセス	W:SC-7 に組み込み	
SC-7(3)	アクセスポイント	S	
SC-7(4)	外部通信サービス	O	
SC-7(5)	デフォルトで拒否 － 例外で許可	S	
SC-7(6)	認識された障害への対応	W:SC-7(18)に組み込み	
SC-7(7)	リモートデバイスのスプリットトンネリング	S	
SC-7(8)	認証済みプロキシサーバへのルートトラフィック	S	
SC-7(9)	脅威となる外向け通信トラフィックの制限	S	
SC-7(10)	漏出の防止	S	
SC-7(11)	着信通信トラフィックの制限	S	
SC-7(12)	ホストベースの保護	S	
SC-7(13)	セキュリティツール、メカニズム、およびサポートコンポーネントの分離	S	
SC-7(14)	認可されていない物理的接続からの保護	S	
SC-7(15)	ネットワーク化された特権アクセス	S	
SC-7(16)	システムコンポーネント検出の防止	S	
SC-7(17)	プロトコル形式の自動化された実施	S	
SC-7(18)	フェールセキュア	S	√

管理策番号	管理策名 拡張管理策名	実装者	保証
SC-7(19)	組織外で構成されたホストからの通信のブロック	S	
SC-7(20)	動的な分離および隔離	S	
SC-7(21)	システムコンポーネントの分離	O/S	√
SC-7(22)	異なるセキュリティドメインに接続するための個別のサブネット	S	√
SC-7(23)	プロトコル妥当性確認失敗時の送信者へのフィードバックの無効化	S	
SC-7(24)	個人情報	O/S	
SC-7(25)	非機密国家安全保障システムの接続	O	
SC-7(26)	機密国家安全保障システムの接続	O	
SC-7(27)	非機密非国家安全保障システムの接続	O	
SC-7(28)	パブリックネットワークへの接続	O	
SC-7(29)	機能を分離するための別のサブネット	S	
SC-8	**伝送の機密性および完全性**	S	
SC-8(1)	暗号保護	S	
SC-8(2)	送信前および送信後の処理	S	
SC-8(3)	メッセージの外側の暗号化保護	S	
SC-8(4)	通信の秘匿化またはランダム化	S	
SC-8(5)	保護された配信システム	S	
SC-9	伝送の機密性	W：SC-8 に組み込み	
SC-10	**ネットワーク切断**	S	
SC-11	**信頼できる経路**	S	√
SC-11(1)	非常に明確に区別できるコミュニケーション経路	S	√
SC-12	**暗号鍵の確立および管理**	O/S	
SC-12(1)	可用性	O/S	
SC-12(2)	対称鍵	O/S	
SC-12(3)	非対称鍵	O/S	
SC-12(4)	PKI 証明書	W：SC-12(3)に組み込み	
SC-12(5)	PKI 証明書／ハードウェアトークン	W：SC-12(3)に組み込み	
SC-12(6)	鍵の物理的管理	O/S	
SC-13	**暗号保護**	S	
SC-13(1)	FIPS 検証済み暗号技術	W：SC-13 に組み込み	
SC-13(2)	NSA 承認済み暗号技術	W：SC-13 に組み込み	
SC-13(3)	正式なアクセス承認を受けていない個人	W：SC-13 に組み込み	
SC-13(4)	デジタル署名	W：SC-13 に組み込み	
SC-14	パブリックアクセス保護	W：AC-2, AC-3, AC-5, SI-3, SI-4, SI-5, SI-7, SI-10 に組み込み	
SC-15	**共同コンピューティングデバイスおよびアプリケーション**	S	
SC-15(1)	物理的または論理的な切断	S	
SC-15(2)	インバウンドおよびアウトバウンド通信トラフィックの遮断	W：SC-7 に組み込み	

管理策番号	管理策名 拡張管理策名	実装者	保証
SC-15(3)	セキュアな作業領域での無効化および削除	O	
SC-15(4)	現在の参加者の明示	S	
SC-16	**セキュリティおよびプライバシーの属性の伝送**	S	
SC-16(1)	完全性の検証	S	
SC-16(2)	なりすまし防止メカニズム	S	
SC-16(3)	暗号化バインディング	S	
SC-17	**公開鍵基盤の証明書**	O/S	
SC-18	**モバイルコード**	O	
SC-18(1)	許可されないコードの特定および是正措置	S	
SC-18(2)	取得、開発、および使用	O	
SC-18(3)	ダウンロードおよび実行の防止	S	
SC-18(4)	自動実行の防止	S	
SC-18(5)	制限された環境に限った実行の許可	S	
SC-19	ボイス・オーバー・インターネット・プロトコル	W: 技術固有；他の技術またはプロトコルと同様に対処	
SC-20	**セキュアな名前／アドレス解決サービス（信頼できるソース）**	S	
SC-20(1)	子サブスペース	W：SC-20 に組み込み	
SC-20(2)	データの起源および完全性	S	
SC-21	**セキュアな名前／アドレス解決サービス（再帰的またはリゾルバキャッシング）**	S	
SC-21(1)	データの起源および完全性	W：SC-21 に組み込み	
SC-22	**名前／アドレス解決サービスのアーキテクチャとプロビジョニング**	S	
SC-23	**セッションの真正性**	S	
SC-23(1)	ログアウト時のセッション識別子の無効化	S	
SC-23(2)	ユーザが開始したログアウトおよびメッセージの表示	W：AC-12(1)に組み込み	
SC-23(3)	一意のシステム生成セッション識別子	S	
SC-23(4)	ランダム化された一意のセッション識別子	W：SC-23(3)に組み込み	
SC-23(5)	許可された認証局	S	
SC-24	**既知の安全な状態での障害**	S	√
SC-25	**シンノード**	S	
SC-26	**デコイ**	S	
SC-26(1)	悪意のあるコードの検知	W：SC-35 に組み込み	
SC-27	**プラットフォームに依存しないアプリケーション**	S	
SC-28	**保管中の情報の保護**	S	
SC-28(1)	暗号保護	S	
SC-28(2)	オフラインストレージ	O	
SC-28(3)	暗号鍵	O/S	

管理策番号	管理策名 拡張管理策名	実装者	保証
SC-29	**異質性**	O	√
SC-29(1)	仮想化技法	O	√
SC-30	**秘匿化および誤認誘導**	O	√
SC-30(1)	仮想化技法	W：SC-29(1)に組み込み	
SC-30(2)	ランダム性	O	√
SC-30(3)	処理場所および保管場所の変更	O	√
SC-30(4)	誤解を招く情報	O	√
SC-30(5)	システムコンポーネントの秘匿化	O	√
SC-31	**カバートチャネル分析**	O	√
SC-31(1)	探知可能性のためのカバートチャネルのテスト	O	√
SC-31(2)	最大帯域幅	O	√
SC-31(3)	運用環境での帯域幅の測定	O	√
SC-32	**システム分割**	O/S	√
SC-32(1)	特権機能のための物理ドメインの分離	O/S	√
SC-33	伝送準備の完全性	W：SC-8 に組み込み	
SC-34	**変更不可能な実行可能プログラム**	S	√
SC-34(1)	書き込み可能なストレージ	O	√
SC-34(2)	読み取り専用媒体の完全性保護	O	√
SC-34(3)	ハードウェアベースの保護	W：SC-51 に移動	
SC-35	**外部の悪意のあるコードの識別**	S	
SC-36	**分散処理およびストレージ**	O	√
SC-36(1)	ポーリング技法	O	√
SC-36(2)	同期	O	√
SC-37	**帯域外チャネル**	O	√
SC-37(1)	確実な配信および送信	O	√
SC-38	**運用セキュリティ**	O	√
SC-39	**プロセス分離**	S	√
SC-39(1)	ハードウェア分離	S	√
SC-39(2)	スレッドごとの個別の実行ドメイン	S	√
SC-40	**ワイヤレスリンクの保護**	S	
SC-40(1)	電磁干渉	S	
SC-40(2)	検知の可能性の低減	S	
SC-40(3)	模倣的または操作的な通信の偽装	S	
SC-40(4)	信号パラメータの識別	S	
SC-41	**ポートおよび I/O デバイスへのアクセス**	O/S	
SC-42	**センサの能力およびデータ**	S	
SC-42(1)	認可された個人または役割への報告	O	
SC-42(2)	認可された使用	O	
SC-42(3)	デバイスの使用禁止	W：SC-42 に組み込み	
SC-42(4)	収集に関する通知	O	

管理策番号	管理策名 拡張管理策名	実装者	保証
SC-42(5)	収集の最小化	O	
SC-43	**使用制限**	O/S	
SC-44	**デトネーションチャンバー**	S	
SC-45	**システム時刻同期**	S	
SC-45(1)	信頼できるタイムソースとの同期	S	
SC-45(2)	二次的な信頼できるタイムソース	S	
SC-46	**クロスドメインポリシーの実施**	S	
SC-47	**代替通信経路**	O/S	
SC-48	**センサの再配置**	O/S	
SC-48(1)	センサまたは監視機能の動的な再配置	O/S	
SC-49	**ハードウェアによる分離およびポリシーの適用**	O/S	√
SC-50	**ソフトウェアによる分離およびポリシーの適用**	O/S	√
SC-51	**ハードウェアベースの保護**	O/S	√

表 C-19:「システムおよび情報の完全性」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
SI-1	**ポリシーおよび手順**	O	√
SI-2	**欠陥の修正**	O	
SI-2(1)	一元管理	W:PL-9 に組み込み	
SI-2(2)	自動化された欠陥の修正ステータス	O	
SI-2(3)	欠陥を修正する時間および是正処置のベンチマーク	O	
SI-2(4)	自動化されたパッチ管理ツール	O/S	
SI-2(5)	ソフトウェアおよびファームウェアの自動更新	O/S	
SI-2(6)	ソフトウェアおよびファームウェアの以前のバージョンの削除	O/S	
SI-3	**悪意のあるコードからの保護**	O/S	
SI-3(1)	一元管理	W:PL-9 に組み込み	
SI-3(2)	自動更新	W:SI-3 に組み込み	
SI-3(3)	非特権ユーザ	W:AC-6(10)に組み込み	
SI-3(4)	特権ユーザに限定した更新	O/S	
SI-3(5)	ポータブルストレージデバイス	W:MP-7 に組み込み	
SI-3(6)	テストおよび検証	O	
SI-3(7)	非署名ベースの検知	W:SI-3 に組み込み	
SI-3(8)	認可されていないコマンドの検知	S	
SI-3(9)	リモートコマンドの認証	W:AC-17(10)に移動	
SI-3(10)	悪意のあるコードの分析	O	
SI-4	**システム監視**	O/S	√
SI-4(1)	システム全体の侵入検知システム	O/S	√
SI-4(2)	リアルタイム分析のための自動化されたツールおよびメカニズム	S	√
SI-4(3)	自動化されたツールおよびメカニズムの統合	S	√
SI-4(4)	インバウンドおよびアウトバウンド通信のトラフィック	S	√
SI-4(5)	システムによって生成されたアラート	S	√
SI-4(6)	非特権ユーザの制限	W:AC-6(10)に組み込み	
SI-4(7)	疑わしいイベントへの自動応答	S	√
SI-4(8)	監視情報の保護	W:SI-4 に組み込み	
SI-4(9)	監視ツールおよびメカニズムのテスト	O	√
SI-4(10)	暗号化通信の可視性	O	√
SI-4(11)	通信トラフィック異常の分析	O/S	√
SI-4(12)	自動化された組織生成アラート	O/S	√
SI-4(13)	トラフィックおよびイベントのパターンの分析	O/S	√
SI-4(14)	ワイヤレス侵入検知	S	√
SI-4(15)	ワイヤレスから有線への通信	S	√
SI-4(16)	監視情報の関連付け	O/S	√
SI-4(17)	統合された状況認識	O	√
SI-4(18)	トラフィックおよび秘密の漏出の分析	O/S	√

管理策番号	管理策名 拡張管理策名	実装者	保証
SI-4(19)	個人のリスク	O	√
SI-4(20)	特権ユーザ	S	√
SI-4(21)	試用期間	O	√
SI-4(22)	認可されていないネットワークサービス	S	√
SI-4(23)	ホストベースのデバイス	O	√
SI-4(24)	侵害の兆候	S	√
SI-4(25)	ネットワークトラフィック分析の最適化	S	√
SI-5	**セキュリティのアラート、勧告、および指令**	O	√
SI-5(1)	自動化されたアラートおよび勧告	O	√
SI-6	**セキュリティおよびプライバシー機能の検証**	S	√
SI-6(1)	失敗したセキュリティテストの通知	W：SI-6 に組み込み	
SI-6(2)	分散テストの自動サポート	S	
SI-6(3)	検証結果の報告	O	
SI-7	**ソフトウェア、ファームウェア、および情報の完全性**	O/S	√
SI-7(1)	完全性チェック	S	√
SI-7(2)	完全性違反の自動通知	S	√
SI-7(3)	一元管理された完全性ツール	O	√
SI-7(4)	タンパーエビデントパッケージ	W：SR-9 に組み込み	
SI-7(5)	完全性違反への自動対応	S	√
SI-7(6)	暗号保護	S	√
SI-7(7)	検知および対応の統合	O	√
SI-7(8)	重要なイベントに対する監査ケイパビリティ	S	√
SI-7(9)	ブートプロセスの確認	S	√
SI-7(10)	ブートファームウェアの保護	S	√
SI-7(11)	限定された権限を持つ限定環境	W：CM-7(6)に移動	
SI-7(12)	完全性の検証	O/S	√
SI-7(13)	保護された環境でのコード実行	W：CM-7(7)に移動	
SI-7(14)	バイナリまたはマシン実行可能コード	W：CM-7(8)に移動	
SI-7(15)	コード認証	S	√
SI-7(16)	監視なしのプロセス実行の時間制限	O	√
SI-7(17)	実行時のアプリケーションの自己保護	O/S	√
SI-8	**スパム保護**	O	
SI-8(1)	一元管理	W：PL-9 に組み込み	
SI-8(2)	自動更新	S	
SI-8(3)	継続的な学習能力	S	
SI-9	**情報入力の制限**	W：AC-2, AC-3, AC-5, AC-6 に組み込み	
SI-10	**情報入力の妥当性確認**	S	√
SI-10(1)	手動オーバーライド機能	O/S	√
SI-10(2)	エラーのレビューおよび解決	O	√

管理策番号	管理策名 拡張管理策名	実装者	保証
SI-10(3)	予測可能な動作	O/S	√
SI-10(4)	タイミングの相互作用	S	√
SI-10(5)	信頼できるソースおよび承認済みの形式への入力の制限	S	√
SI-10(6)	注入防止	S	√
SI-11	**エラー処理**	S	
SI-12	**情報管理および保持**	O	
SI-12(1)	個人情報要素の限定	O	
SI-12(2)	テスト、トレーニング、および調査における個人情報の最小化	O	
SI-12(3)	情報の廃棄	O	
SI-13	**予測可能な障害の防止**	O	√
SI-13(1)	コンポーネントの責任の移管	O	√
SI-13(2)	監視なしのプロセス実行の時間制限	W：SI-7(16)に組み込み	
SI-13(3)	コンポーネント間の手動転送	O	√
SI-13(4)	スタンバイコンポーネントのインストールおよび通知	O/S	√
SI-13(5)	フェイルオーバー機能	O	√
SI-14	**非永続性**	O	√
SI-14(1)	信頼できるソースからのリフレッシュ	O	√
SI-14(2)	非永続的情報	O	√
SI-14(3)	非永続的接続性	O	√
SI-15	**情報出力フィルタリング**	S	√
SI-16	**メモリ保護**	S	√
SI-17	**フェイルセーフ手順**	S	√
SI-18	**個人情報の品質運用**	O/S	
SI-18(1)	自動サポート	O/S	
SI-18(2)	データタグ	O/S	
SI-18(3)	収集	O/S	
SI-18(4)	個人の要求	O/S	
SI-18(5)	修正または削除の通知	O/S	
SI-19	**匿名化**	O/S	
SI-19(1)	収集	O/S	
SI-19(2)	アーカイブ	O/S	
SI-19(3)	リリース	O/S	
SI-19(4)	直接識別子の削除、マスク、暗号化、ハッシュ化、または置換	S	
SI-19(5)	統計的開示管理	O/S	
SI-19(6)	ディファレンシャルプライバシー	O/S	
SI-19(7)	妥当性確認済みのアルゴリズムおよびソフトウェア	O	
SI-19(8)	動機付けされた侵入者	O/S	
SI-20	**汚染**	O/S	√
SI-21	**情報の更新**	O/S	√
SI-22	**情報の多様性**	O/S	√

管理策番号	管理策名 拡張管理策名	実装者	保証
SI-23	**情報の断片化**	O/S	√

表 C-20:「サプライチェーンのリスクマネジメント」ファミリー

管理策番号	管理策名 拡張管理策名	実装者	保証
SR-1	**ポリシーおよび手順**	O	√
SR-2	**サプライチェーンのリスクマネジメント計画**	O	√
SR-2(1)	SCRM チームの確立	O	√
SR-3	**サプライチェーンの管理策およびプロセス**	O/S	√
SR-3(1)	多様な供給ベース	O	√
SR-3(2)	損害の限定	O	√
SR-3(3)	下層フローダウン	O	√
SR-4	**来歴**	O	√
SR-4(1)	同一性	O	√
SR-4(2)	追跡および痕跡	O	√
SR-4(3)	本物であり、改変されていないことの確認	O	√
SR-4(4)	サプライチェーンの完全性 – 系譜	O	√
SR-5	**取得戦略、ツール、および方法**	O	√
SR-5(1)	適切な供給	O	√
SR-5(2)	選択、受領、変更、または更新前のアセスメント	O	√
SR-6	**サプライヤのアセスメントおよびレビュー**	O	√
SR-6(1)	テストおよび分析	O	√
SR-7	**サプライチェーン運用セキュリティ**	O	√
SR-8	**通知協定**	O	√
SR-9	**耐タンパー性および検知**	O	√
SR-9(1)	システム開発ライフサイクルの複数の段階	O	√
SR-10	**システムまたはコンポーネントの検査**	O	√
SR-11	**コンポーネントの真正性**	O	√
SR-11(1)	偽造防止トレーニング	O	√
SR-11(2)	コンポーネントのサービスおよび修理のための構成管理	O	√
SR-11(3)	偽造防止の精査	O	√
SR-12	**コンポーネントの廃棄**	O	√