NIST Special Publication 800-53B

組織と情報システムのための管理策ベースライン

ジョイントタスクフォース

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

この文書は以下の団体によって翻訳監修されています

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

NIST Special Publication 800-53B

組織と情報システムのための管理策ベースライン

ジョイントタスクフォース

2020 年 10 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）800-53B
NIST SP 800-53B、**83 ページ**（2020 年 10 月）

CODEN: NSPUE2

本出版物は、https://doi.org/10.6028/NIST.SP.800-53B 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、実践例、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しい。

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。

本出版物に対するご意見は下記まで：
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、および普及活動ならびに産業界、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、連邦政府のための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提供する。セキュリティ管理策には 3 つのベースライン（低・中・高のシステム影響度レベルそれぞれに対して 1 つ）がある一方、プライバシー管理策ベースラインは影響度レベルを問わずシステムに適用される。本出版物では、管理策ベースラインに加えて、テーラリングガイダンスと、管理策の選択プロセスをガイドし情報提供に役立つ一連の実用的な前提事項を提供する。最後に、本出版物では、関心のある特定のコミュニティ、技術、および運用環境において管理策ベースラインのカスタマイズを促進するオーバーレイの策定に関するガイダンスを提供する。

キーワード

保証；影響度レベル；プライバシー管理策；プライバシー管理策ベースライン；セキュリティ管理策；セキュリティ管理策ベースライン；テーラリング；管理策の選択；管理策オーバーレイ

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

McKay Tolboe
DoD

Dorian Pappas
Intelligence Community

Kelley Dempsey
NIST

Ehijele Olumese
The MITRE Corporation

Lydia Humphries
Booz Allen Hamilton

Daniel Faigin
Aerospace Corporation

Naomi Lefkovitz
NIST

Esten Porter
The MITRE Corporation

Julie Nethery Snyder
The MITRE Corporation

Christina Sames
The MITRE Corporation

Christian Enloe
NIST

David Black
The MITRE Corporation

Rich Graubart
The MITRE Corporation

Peter Duspiva
Intelligence Community

Kaitlin Boeckl
NIST

Eduardo Takamura
NIST

Ned Goren
NIST

Andrew Regenscheid
NIST

Jon Boyens
NIST

上記の謝辞に加えて、Jeff Brewer、Jim Foti、および NIST Web 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、本出版物の技術的な内容の改善においてご尽力いただいた 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 OMB の情報・規制業務室（OIRA：Office of Information and Regulatory Affairs）プライバシー部門（Privacy Branch）、連邦 CIO 協議会（Federal CIO Council）、省庁間ワーキンググループ（Interagency Working Group）の代表者からのご意見に感謝したい。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多大な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、完全性、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コンプライアンス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や資産、個人、その他の組織、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、組織の運営や資産、個人、その他の組織、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。

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制限または制約することを意図するものではない。

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（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 800-53B 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、クラウドベースのシステム、モバイルデバイス、および産業用制御システム、プロセス制御システムを含む）のための包括的な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策定し、連邦政府機関や民間組織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、国防科学評議委員会の呼びかけに応じている。管理策ベースラインは、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おける始点を組織に提供する。組織は、組織の重要かつ不可欠な運営と資産を保護するケイパビリティを確保するために、提供されるテーラリングガイダンスと前提事項を使用して、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カスタマイズすることができる。

正誤表

この表には、SP 800-53B 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 800-53B 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

セキュリティおよびプライバシー管理策ベースラインの必要性

セキュリティ管理策とは、情報システム[1]およびその情報の機密性、完全性、可用性を保護し、情報セキュリティリスクを管理するために、情報システムまたは組織内で選択および実装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、適用されるプライバシー要件へのコンプライアンスを確保し、プライバシー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管理上、技術的、および物理的な保全措置である[2]。セキュリティおよびプライバシー管理策は、情報システムおよび／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。そうした要件は、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。管理策の選択、設計、および効果的な実装は、組織の運営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。

NIST 特別出版物（SP：Special Publication）800-37 [SP 800-37]は、*ベースライン*管理策の選択アプローチと、*組織が作成する*管理策の選択アプローチといった、セキュリティおよびプライバシー管理策を選択するための 2 つのアプローチを規定している。ベースライン管理策の選択アプローチでは、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を満たす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、管理策ベースラインを使用する。管理策ベースラインは、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始点となる。本出版物は、組織が作成する管理策の選択アプローチには対応していない。

1.1 目的および適用性

本出版物は、連邦政府組織および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ベースラインを定め、それらのベースラインのためのテーラリングガイダンスを提供している。管理策ベースラインは、情報を処理、保存、または伝送するあらゆる組織（連邦政府機関、州政府、地方自治体、部族政府、および民間組織など）で実装することができる。NIST SP 800-53 改訂第 5 版[SP 800-53]から選択された一連の最小限の管理策は、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[3]（FISMA：Federal Information Security Modernization Act）[FISMA]の規定に従って、連邦政府情報システム[4]および連邦政府情報を保護するために実装することが義務付けられている。プライバシー管理策ベースラインは、法律または[OMB A-130]によって使用を義務付けられていないが、SP 800-53B は、その他の NIST の関連出版物

[1] *情報システム*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情報リソースのセットである。

[2] [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。

[3] （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（たとえば、1974 年のプライバシー法）、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職員の承認を得て、国家安全保障システムのために選択してもよい。CNSS ポリシー第 22 号[CNSSP 22]および CNSS 指示第 1253 号[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。DoD 指示第 8510.01 号[DODI 8510.01]は国防総省のガイダンスを提供している。

[4] *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。

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識別し、FISMA、1974 年プライバシー法（Privacy Act）[PRIVACT]、選択された 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およびプライバシーの要件を満たすべく設計されている。

本出版物は、第 2.3 節に記載されているように、セキュリティおよびプライバシー管理策ベースラインの策定に情報提供する前提事項を適用することにより、セキュリティおよびプライバシーの要件を満たしている。ベースラインは、組織の保護ニーズを満たす始点として機能する。ベースラインの管理策は、組織に固有のセキュリティおよびプライバシーリスクの管理をさらに促進するために、第 2.4 節に記載されるプロセスに従ってテーラリングされる。テーラリングプロセスは、組織の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、リスクアセスメントなど、多くの要因によってガイドされ、情報提供されることができる。管理策ベースラインの選択と管理策のテーラリングプロセスを組み合わせることにより、組織は、セキュリティおよびプライバシーの要件を満たすことができる。

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、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

組織は、[SP 800-37]に従って管理策の選択アプローチを選択する責任がある[5]。組織は、ベースライン管理策の選択アプローチを選択する場合、第 3 章に記載されているセキュリティ管理策ベースラインとプライバシー管理策ベースラインを選択する。管理策ベースラインを選択した後、組織は、最終的に得られる管理策がセキュリティリスク[6]とプライバシーリスク[7]を管理するのに必要かつ十分なものであることを確保するために、第 2 章で提供されるテーラリングガイダンスを適用する。

1.4 他の出版物との関係

本出版物は、[SP 800-53]の管理策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ベースラインを定めている。本出版物の管理策ベースラインは、[OMB A-130][8]、連邦情報処理規格 199[FIPS 199]、および連邦情報処理規格 200[FIPS 200]に含まれる、連邦政府情報システムや連邦政府情報に対する要件に従っている。[SP 800-37]は、管理策の選択アプローチに関するガイダンスを提供している。

1.5 改訂および拡張

ベースラインにおいて特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、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。ベースラインを構成する管理策は、(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。したがって、ベースラインにおいて特定されている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、ベースラインに対して提案される変更が、公共および民間分野のフィードバックを受け、ベースラインの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、安定性の必要性も対処する。パブリック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ベースラインが提供される。

---

[5] *ベースライン*管理策の選択アプローチおよび*組織が作成する*管理策の選択アプローチにおいて、組織は、リスクマネジメントフレームワーク(RMF:Risk Management Framework)における*システムレベルの準備(Prepare—System Level)ステップ*の Task P-15, *Requirements Definition* で説明されているように、ライフサイクルベースのシステムエンジニアリングプロセスを使用して、明確に規定された一連のセキュリティおよびプライバシーの要件を策定する。要件定義プロセスは、要件を満たすための管理策の選択をガイドし、情報提供するために使用することができる一連の要件を作成する。

[6] [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。

[7] [IR 8062]は、プライバシーリスクの概念を紹介している。

[8] [OMB A-130]は、連邦情報、職員、装置、資金、IT リソース、サポートインフラおよびサービスの計画、予算編成、ガバナンス、取得、および管理に関するポリシーを定めている。

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、管理策ベースライン、適切なベースラインの選択、ベースラインの前提事項、ベースラインのテーラリング、オーバーレイ、およびケイパビリティに関連する基本的な概念を説明する。
- 第 3 章では、低・中・高の影響度のセキュリティ管理策ベースラインと、プライバシー管理策ベースラインを構成する管理策を含む、管理策ファミリーごとに組織された一連の表を提供する。
- 第 3 章の後に参照資料[9]のリストが提供される。
- 補足の付属書には次のものが含まれる。
  - 付属書 A：用語集
  - 付属書 B：略語
  - 付属書 C：オーバーレイに関するガイダンス

セキュリティおよびプライバシー管理策ベースライン

セキュリティおよびプライバシー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始点となり、組織のミッションや事業機能、特定の信頼できる脅威情報、組織が運営する環境、個人のプライバシー権を適切に考慮して、テーラリング（すなわち、カスタマイズ）することができる。

[9] 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、それらの出版物の最新版を指すものとする。

第 2 章

基本的事項

管理策ベースライン、テーラリング、オーバーレイ、およびケイパビリティ

本章では、セキュリティおよびプライバシー管理策ベースラインに関連する基本的な概念について説明する。これには、管理策ベースラインの目的、管理策ベースラインの選択方法、管理策ベースラインに関連する前提事項、管理策およびベースラインをカスタマイズするためのテーラリングプロセスの使用方法、オーバーレイの目的、関心のあるコミュニティのセキュリティとプライバシーのニーズに対応するためのオーバーレイの使用方法、および、ケイパビリティの概念が相互に補強し合う管理策のグループ化をどのように促進することができるのか、などについて説明する。

2.1 管理策ベースライン

組織のミッションと事業機能を保護し、セキュリティとプライバシーのリスクを管理するケイパビリティを提供することができる一連のセキュリティおよびプライバシー管理策を選択することは、組織にとって重要な課題である。選択した管理策は、正しく実装され有効であると判定された場合に、適用される法律、大統領令、ポリシー、規則、および指令によって規定されるセキュリティおよびプライバシーの要件を満たす。一組の管理策だけで、あらゆる状況においてすべてのセキュリティやプライバシーの懸念に対応することはできない。特定の状況やシステムに対して最も適切な管理策を選択してリスクに適切に対応するには、組織のミッションと事業の優先順位、システムがサポートするミッションと事業機能、および、システムが動作する環境を根本的に理解する必要がある。また、組織の重要な利害関係者との緊密な連携も必要である。こうした理解により、組織は、組織のミッションと事業機能をサポートする中で、組織の情報やシステムの機密性、完全性、可用性、および個人のプライバシーを効率的かつ費用対効果高く保証する方法を実証することができる。

管理策 *ベースライン*という概念は、セキュリティとプライバシーのリスクに見合った一連の管理策をシステムのために選択する組織を支援するために導入された。管理策ベースラインとは、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構築された[SP 800-53]の管理策の集合体である[10]。これは、ベースラインに適用される後続のテーラリング活動の始点となる汎用的な一連の管理策を提供し、ベースラインが対応するエンティティ用に対象を絞ったまたはカスタマイズされたセキュリティおよびプライバシーソリューションを作成する。管理策ベースラインは、脅威情報、ミッションや事業要件、システムのタイプ、分野固有の要件、特定の技術、運用環境、組織の前提事項および制約、個人のプライバシー権、法律、大統領令、規則、ポリシー、指令、基準、業界のベストプラクティスなど、様々な要因に基づいてテーラリングされる。テーラリング活動については、第 2.4 節で詳細に説明される。

[10] 米国政府は、[FISMA]、[OMB A-130]、および連邦情報処理規格に定められた要件に従って、連邦政府に義務付けられるセキュリティ管理策ベースラインを定めている。国家安全保障システム以外のシステムのための管理策ベースラインは第 3 章に記載されている。

2.2 管理策ベースラインの選択

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、認可されていないシステム活動または動作）から保護する責任を負う。プライバシープログラムは、個人情報（PII）の作成、収集、使用、処理、配布、保存、維持、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コンプライアンスを確保する責任を負う[11]。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、セキュリティリスクから生じる個人への影響を管理し、セキュリティ管理策ベースラインからの管理策の選択およびテーラリングや、セキュリティ分類化について共同で判定する責任を共有する。

セキュリティ管理策ベースライン

組織は、組織のシステムおよびそれぞれの運用環境に対して適切なセキュリティ管理策ベースラインを選択およびテーラリングする準備として、まず、それらのシステムによって処理、保存、または伝送される情報の重要度と機微性を判定する。情報の重要度と機微性を判定するプロセスは*セキュリティ分類化*と呼ばれ、[FIPS 199]で説明されている[12]。セキュリティ分類化の結果は、システムと情報を保護するためのセキュリティ管理策ベースラインの選択をガイドし、情報提供をする。システムのために選択された管理策ベースラインは、機密性、完全性、または可用性が失われた場合に、組織運営、組織資産、個人、その他の組織、または国家に対する潜在的な悪影響に見合ったものである。[FIPS 199]では、組織に対し、機密性、完全性、可用性といった所定のセキュリティ目的について、システムを低、中、または高の影響度に分類することを求めている[13]。

機密性、完全性、可用性の潜在的影響度の値は、特定のシステムで必ずしも同じではないため、システムの影響度レベルを判定するために[FIPS 200]では最高水準の概念（[FIPS 199]で紹介される）が使用されている。システムの影響度レベルは、第 3 章で識別されている 3 つのベースラインの 1 つから適用可能なセキュリティ管理策ベースラインを選択するという明確な目的のために使用される[14]。よって、*低影響度*システムは、3 つのセキュリティ目的すべてが低のシステムと規定されている。*中影響度*システムは、セキュリティ目的の少なくとも 1 つが中であり高のセキュリティ目的がないシステムである。最後に、*高影響度*システムは、少なくとも 1 つのセキュリティ目的が高のシステムである。

システムの影響度レベルを判定した後、組織は適切なセキュリティ管理策ベースラインを選

---

[11] プライバシープログラムは、PII 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場合が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。

[12] [CNSSI 1253]は、国家安全保障システムのセキュリティ分類化と管理策選択に関するガイダンスを提供する。

[13] NIST SP 800-60（第 1 巻および第 2 巻）[SP 800-60-1] [SP 800-60-2]では、情報システムにセキュリティ分類を設定するためのガイダンスを提供している。[SP 800-37]では、リスクマネジメントフレームワーク（RMF）の分類（Categorize）ステップにおける特定のタスクに関するガイダンスを提供している。

[14] 最高水準の概念は、機密性、完全性、可用性というセキュリティ目的の間に大きな依存関係があるために採用されている。多くの場合、1 つのセキュリティ目的が脅かされると、最終的には他のセキュリティ目的にも影響する。したがって、セキュリティ管理策はセキュリティ目的によって分類されない。セキュリティ管理策は、影響度レベルに基づいたシステムクラスに対して汎用的な保護ケイパビリティを提供するよう、ベースラインにグループ化される。

択する[15]。セキュリティ管理策ベースラインは、上記のセキュリティ分類化プロセスによって判定されたシステムの影響度レベル[FIPS 200]に基づいて選択される。組織は、システムの低・中・高の影響度の分類化に対応する、第 3 章の 3 つのセキュリティ管理策ベースラインのいずれかを選択する。第 3 章の表に示すように、[SP 800-53]で識別されているすべての管理策または拡張管理策が管理策ベースラインに設定されているわけではない。ベースラインに設定されている管理策と拡張管理策は、表 3-1 から表 3-20 で低・中・高の列に「x」で示されている。管理策 *ベースライン*という用語の使用は意図的なものである。ベースラインの管理策と拡張管理策は、第 2.4 節のテーラリングガイダンスに基づいて、管理策または拡張管理策を削除、追加、または特化してもよい始点である[16]。

プライバシー管理策ベースライン

3 つのセキュリティ管理策ベースラインに加えて、第 3 章は、[OMB A-130]によるプライバシープログラムの責任に基づいて、連邦政府機関が PII の *取扱い* から生じるプライバシーリスクを管理しプライバシー要件に対応するための、初期のプライバシー管理策ベースラインを提供する[17]。プライバシー管理策ベースラインに設定されている管理策と拡張管理策は「x」で示されている[18]。プライバシーリスクに対応するすべての管理策または拡張管理策が、プライバシー管理策ベースラインに設定されているわけではない。このアプローチは、第 2.4 節のテーラリングガイダンスに基づいて、管理策または拡張管理策を削除、追加、または特化してもよい始点を提供している[19]。

組織は、組織のプログラムおよびシステムのためのプライバシー管理策ベースラインのテーラリングをガイドするために、PII の取扱いの性質と個人への影響を考慮したプライバシーリスクアセスメントを実施する。プライバシーリスクアセスメントには、プログラムへの法的要件とポリシー要件の適用性を評価することが含まれる。たとえば、組織は、プライバシーリスクアセスメントに基づいて、識別されたプライバシーリスクを緩和するのに管理策または拡張管理策が有用であると判定した場合を除いて、組織に適用されない法的要件またはポリシー要件に関連する管理策や拡張管理策を削除してもよい。さらに、組織は、プライバシーリスクアセスメントによって判定された情報システムに固有のプライバシーリスクを軽減するために、設定されていない管理策や拡張管理策を追加してもよい。

2.3 管理策ベースラインの前提事項

第 3 章の管理策ベースラインは、個々の利用者や組織を含む多様な読者層の保護ニーズに

---

15 一般的な管理策ベースラインの選択プロセスは、付属書 C 「*オーバーレイ*」で説明されているように、共通のリスク管理目標を持つコミュニティや産業下位分野など、分野固有の追加ガイダンスによって補足または詳細化される場合がある。

16 特化とは、管理策または拡張管理策（組織が定めるパラメータを含む）の変更、または、組織が特定の要件、技術、ミッションや事業機能、または運用環境に対応するために管理策ベースラインをさらに改良できるようにする補足的なガイダンスを指す。関心のあるコミュニティ、システム、および組織のための特別な一連の管理策の必要性に対応するために*オーバーレイ*という概念は導入された。オーバーレイの詳細については、付属書 C を参照のこと。

17 プライバシー管理策ベースラインを実装していることが、[OMB A-130]のすべての義務を履行していることを意味していると連邦政府機関が想定することは望ましくない。連邦政府機関は、OMB のプライバシー要件に完全に準拠するために、別途追加の措置を講じなければならない場合がある。

18 第 3 章の表 3-1 から表 3-20 のプライバシー拡張管理策は、関連する基本管理策を選択および実装せずに、選択および実装することはできない。このようなアクションは、基本管理策の責任がセキュリティプログラムにある場合にセキュリティプログラムとの連携を必要とする。組織は、情報セキュリティとプライバシープログラムとの間で、管理策の選択と実装に関する責任を明確に規定する。

19 注釈 16 を参照のこと。

対応している。したがって、一定の実用的な*前提事項*が一般に第 3 章の管理策ベースラインの土台となっている。第 3 章のベースラインを決定する際になされたこれらの前提事項は、(1)法律、規則、またはポリシーに係る義務を含む、組織の情報システムが動作する環境、(2)組織運営の性質、(3)システム内で採用されている特定の機能性、(4)組織が直面する脅威のタイプ、(5)ミッションと事業プロセスおよびシステム、(6)個人のプライバシー権、(7)システムによって処理、保存、または伝送される情報のタイプ、などを考慮する[20]。土台となる前提事項を明確にすることは、[SP 800-39]で説明されているリスクマネジメントプロセスにおけるリスクの枠決め(Risk Framing)ステップにおいて重要な要素であり、[SP 800-37]の準備(Prepare)ステップで補足されている。第 3 章の管理策ベースラインの土台となる特定の前提事項は次のとおりである。

- 組織システム内の情報は比較的永続的なものである[21]。
- 組織システムはマルチユーザーで(逐次または同時に)動作する。
- 組織システム内の一部の情報は、同じシステムへのアクセス権限を持つ他のユーザーと共有できない。
- 組織システムはネットワーク環境に存在し、本質的に汎用的である。
- 組織は、管理策を実装するのに必要な構造、リソース、およびインフラを有している[22]。

上記の前提事項のいずれかが有効でない場合、第 3 章で管理策ベースラインに割り当てられているセキュリティ管理策の一部を適用できない可能性がある。この状況は、第 2.4 節のテーラリングガイダンスと、組織レベルおよびシステムレベルのリスクアセスメントの結果を適用することによって対処することができる。ベースラインで対応されて**いない**他の前提事項は次のとおりである。

- 組織内にインサイダー脅威が存在する。
- 国家機密情報が組織システムによって処理、保存、または伝送される[23]。
- 組織内に持続的標的型攻撃(APT 攻撃)が存在する。
- 情報が、法律、指令、規則、またはポリシーに基づき特別な保護を必要とする。
- 組織システムが異なるセキュリティドメインにわたり他のシステムと通信する。

これらの前提事項のいずれかが当てはまる場合、適切な保護を確保するには[SP 800-53]から追加の管理策が必要になる可能性がある。この状況も、第 2.4 節のテーラリングガイダンス(特に、セキュリティ管理策の補足)と、組織レベルおよびシステムレベルのリスクアセスメントの結果を適用することによって効果的に対処することができる。

[20] 管理策ベースラインは、脅威の動的な性質を前提として、可能な範囲で脅威の性質を考慮する。
[21] 永続的データ/情報は、比較的長い期間(例えば、数日、数週)、有用なデータ/情報を指す。
[22] 一般的に、連邦政府の部門および機関はこの前提事項を満たしている。しかし、この前提事項は、自治体、初期対応者、中小企業などの非連邦政府エンティティにとって問題になる可能性がある。そのようなエンティティは、ベースラインによって想定されるセキュリティまたはプライバシーケイパビリティを提供するための専用の要素を保持するほど規模が大きくない、または十分なリソースがない可能性がある。組織は、リスクベースの意思決定においてこのような要因を考慮する。
[23] NIST SP 800-59 [SP 800-59]および CNSS 指示第 1253 号[CNSSI 1253]を参照のこと。

2.4 管理策ベースラインのテーラリング

適切な管理策ベースラインを選択した後、組織は、組織が識別している特定のセキュリティおよびプライバシーの要件に管理策をより密接に適合させるためにテーラリングプロセスを実施する。テーラリングプロセスは、組織全体のリスクマネジメントプロセスの一部であり、情報セキュリティおよびプライバシーリスクの枠決め、アセスメント、対応、および監視が含まれる。テーラリングの決定は、組織またはシステム固有の要因によって異なる。テーラリングの決定はセキュリティおよびプライバシーに関する考慮事項に重点を置く一方、通常、組織が定常的に対応しなければならない他のリスク関連の問題にも適合される。どの管理策を採用するかを判定する際や、組織のシステムおよび運用環境でどのように管理策を実装するかを判定する際には、コスト、スケジュール、パフォーマンスなどのリスク関連の問題が考慮される[24]。テーラリングプロセスには以下の活動を含むことができるが、これらに限定されない[25]。

- 共通管理策の識別と指定
- スコーピングの考慮事項の適用
- 代替管理策の選択
- 明示的な設定および選択操作による、組織が定める管理策パラメータへの値の設定
- 追加の管理策と拡張管理策によるベースラインの補完
- 管理策実装のための仕様情報の提供

組織は、ベースラインの管理策の適用性についてリスクベースの意思決定を促進するために、リスクマネジメントのガイダンスを使用する。最終的に、組織は、テーラリングプロセスを採用することで、組織のミッションと事業ニーズをサポートし、リスクに見合ったセキュリティおよびプライバシー保護を提供する費用対効果の高いソリューションを実現する[26]。組織は、基幹業務、ミッションまたは事業プロセスをサポートするシステムに合わせて、組織レベルで、個々のシステムレベルで、または 2 つの組み合わせを使用して、テーラリングを行う柔軟性を備えている。ただし、組織はベースラインからセキュリティおよびプライバシー管理策を任意に削除してはならない。テーラリングの決定は、ミッションと事業のニーズ、健全な根拠、および明示的なリスクベースの判定に基づいた正当なものであることが期待される[27]。

テーラリングの決定は、その決定に関するリスクベースの正当性を含め、組織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に文書化される[28]。組織は、選択した管理策ベー

[24] 適用される連邦法、規則、またはポリシーに係る要件に関連するセキュリティまたはプライバシー管理策を組織がテーラリングすることは不適切である。

[25] プライバシー管理策のテーラリングに関する追加のガイダンスについては、第 2.2 節に記載されるプライバシー管理策ベースラインを参照のこと。

[26] 組織全体で使用される管理策ベースラインのテーラリングに関する追加のガイダンスについては、[SP 800-37]に記載の Task P-4, Organizationally-Tailored Control Baselines and Cybersecurity Framework Profiles (Optional)を参照のこと。システムおよび運用環境のための管理策ベースラインのテーラリングに関する追加のガイダンスについては、[SP 800-37]に記載の Task S-2, Control Tailoring を参照のこと。

[27] テーラリングは、選択した管理策のタイミングと適用性に基づいて一定の条件の下で決定することができる。すなわち、セキュリティおよびプライバシー管理策はすべての状況で適用されない、または、一定の状況下で設定操作のパラメータ値が変更される場合がある。連邦政府機関は、OMB ポリシーに従ってベースラインのテーラリング活動を実施する。一定の状況において、OMB は、連邦政府機関に対して特定のセキュリティまたはプライバシー管理策のテーラリングを禁止してもよい。

[28] [SP 800-18]は、システムセキュリティ計画の策定に関するガイダンスを提供している。プライバシー計画およびサプライチェーンリスクマネジメント計画の策定に関するガイダンスは近く公開予定である。

スラインのすべての管理策を明らかにする。特定の管理策がテーラリングされる場合、その根拠はシステムセキュリティおよびプライバシー計画に記録され、その後、計画の承認プロセスの一部として組織内の責任者によって承認される。ベースラインのテーラリングプロセス中にリスクマネジメントの決定を文書化することは、組織の担当者が、セキュリティとプライバシーに関する信頼できるリスクベースの意思決定を行い、透明性、追跡可能性、および説明責任を完全にサポートするような形で必要な情報を得るために不可欠である。

共通管理策の識別と指定

共通管理策とは、1 つ以上の組織システムによって継承される管理策である。システムが別のエンティティ（内部または外部）によって提供される共通管理策を継承する場合、そのシステムに管理策を実装する必要はない。どの管理策を共通管理策として指定するかについての組織による決定は、ベースラインの管理策の実装において、個々のシステムオーナーの責任に影響を与える場合がある[29]。共通管理策の提供者は、最新の実装情報とアセスメント結果を利用可能にすることで、システムオーナーおよび認可権限のある担当者による意思決定を促進する。システムオーナーおよび認可権限のある担当者は、継承して利用できる共通管理策が、継承するシステムのリスクに見合った保護を実際に提供するかどうかを判定する[30]。

共通管理策の指定と管理策の実装は、組織のリソース支出に影響を与える可能性がある。つまり、一般に、実装する共通管理策の数が多いほど、保護手段が多くのシステムにわたって経費化されるため、潜在的なコスト削減が大きくなる。さらに、管理策を共通管理策として展開した場合、同じ管理策を複数のシステムに個別に実装する場合と比べて、多くの場合、より標準的且つ安定したスケーラブルでセキュアな実装が組織全体で提供される。

スコーピングの考慮事項の適用

スコーピングの考慮事項はリスクマネジメントのガイダンスと組み合わせて適用されると、リスクベースの意思決定を行うためのより詳細な基盤が組織に提供される[31]。スコーピングの考慮事項を適用することにより、初期の管理策ベースラインから不要な管理策を取り除くことができ、組織は、リスクに見合った保護レベルを提供するのに必要な管理策*のみ*を確実に選択することができる。組織は、管理策の選択と仕様化に関するリスクベースの意思決定を支援するために、必要に応じて以下に説明するスコーピングの考慮事項を適用してもよい。

- *管理策の実装、適用性、および導入の考慮事項*

システムの複雑さが増す中、セキュリティおよびプライバシー管理策の実装には慎重な分析が必要である。初期のベースラインの管理策は、システム内のすべてのコンポーネントに適用可能ではない場合がある。管理策は、管理策が対応するセキュリティまたはプライバシー機能やケイパビリティを提供する、またはサポートするシステムコンポーネントにのみ適用される[32]。組織は、必要なセキュリティまたはプライバシー機能やケイパビリティを実現するために、また、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、特定の管理策を組織システム内のどこに適用または割り当てるかについて、リスクベースの明確な決定を下す。

---

[29] 共通管理策の指定に関する組織による決定の詳細については、[SP 800-37]に記載される *Organizational Prepare* Step の Task P-5, *Common Control Identification* を参照のこと。管理策実装アプローチとしての共通管理策の詳細については、[SP 800-53]の第 2.3 節を参照のこと。

[30] 組織は、ハイブリッド管理策を活用してもよい。ハイブリッド管理策は、1 人以上の共通管理策の提供者によって一部が実装され、システムによって一部が実装される。

[31] この節に記載されているスコーピングの考慮事項は例示的なものであり、組織が定めるその他の考慮事項に基づいて、適切な正当性または根拠をもって組織が行うリスクベースの意思決定を制限するものでは*ない*。

[32] 例えば、監査の管理策は通常、監査能力を提供するシステムのコンポーネントに適用され、必ずしも組織内のすべてのユーザーレベルのコンポーネントに適用されるわけではない。

- *運用と環境の考慮事項*

管理策ベースラインの一定の管理策は、運用上または環境的な要素が存在することを前提としている。運用上または環境的な要素が存在しない場合、もしくは第 2.3 節で説明されるベースラインの前提事項から大きく逸脱している場合には、ベースラインをテーラリングすることは正当と認められる。一般的な運用上および環境的な要素には、(1)モバイルデバイスおよびその運用、(2)シングルユーザーシステムおよびその運用、(3)データ接続と帯域幅、(4)エアギャップシステム、(5)戦闘機や法執行機関のミッションをサポートする戦術的なシステムなど非常に限られた、または散発的な帯域幅を持つシステム、(6)サイバーフィジカルシステム、センサー、IoT デバイス、(7)ファクシミリ装置、プリンタ、デジタルカメラなどの機能が限定的なシステム、(8)非永続情報を処理、保存、または伝送する、または仮想化技術を使用してオペレーティングシステムおよびアプリケーションの非永続的なインスタンス化を確立するシステム、(9)パブリックアクセスを必要とするシステム、などが含まれる。

- *技術の考慮事項*

ワイヤレス、暗号技術、公開鍵基盤などの特定の技術に関係する管理策は、それらの技術が組織システム内で実装されている場合や、組織システムでの使用が必要な場合にのみ適用される。自動化されたメカニズムによって効果的にサポートされることができる管理策では、自動化されたメカニズムがまだ存在しない場合や、市販製品または政府製品で容易に入手できない場合は、そうしたメカニズムの開発を要求していない。自動化されたメカニズムが利用できない場合には、自動化されていないメカニズムまたは手順を介して実装される、費用対効果が高く、技術的に実現可能な代替管理策を、特定の管理策や拡張管理策を満たすために実装することができる。

- *ミッションと事業の考慮事項*

特定の管理策を実装することで、個人を危険にさらす、または危害を加えることを含め、組織のミッションや事業機能を低下、衰弱、または妨害する可能性がある場合には、そうした管理策は適切でない場合がある。ただし、管理策実装の適切性に関する決定は、常に、法律、規則、またはポリシーに係る要件を考慮する。

- *セキュリティ目的の考慮事項*

セキュリティ目的(すなわち、機密性、完全性、または可用性)の 1 つまたは 2 つのみをサポートする管理策は、より低いベースラインの、対応する管理策にダウングレード(または、より低いベースラインで規定されていない場合は変更または削除)してもよい。ただし、これは、ダウングレードアクションが、(1)[FIPS 200]の影響度レベルを考慮する前に、サポートされているセキュリティ目的の[FIPS 199]セキュリティ分類を反映している場合(すなわち、最高水準)、(2)組織のリスクアセスメントによってサポートされている場合、(3)システム内のセキュリティ関連情報の保護レベルに悪影響を及ぼさない場合のみに限られる。例えば、機密性および／または完全性が「中」で、可用性が「低」であることから、最高水準の概念によりシステムが中影響度に分類化される場合、可用性のセキュリティ目的のみをサポートするいくつかの管理策は、「低」ベースラインの管理策にダウングレードできる可能性がある。こうした状況では、拡張管理策は可用性のみをサポートすることになり、「中」ベースラインでは選択されるが「低」ベースラインでは選択されないため、CP-2(1)の実装を控えるのが適切な場合がある。次のセキュリティ管理策と拡張管理策は、各セキュリティ分類におけるダウングレードの候補である。

- 機密性のみをサポート: AC-21, MA-3(3), MP-3, MP-4, MP-5, MP-6(1), MP-6(2), PE-4, PE-5, SC-4

- 完全性のみをサポート：CM-5, CM-5(1), CM-5(3), SI-7, SI-7(1), SI-7(5), SI-10
- 可用性のみをサポート：CP-2(1), CP-2(2), CP-2(3), CP-2(5), CP-2(8), CP-3(1), CP-4(1), CP-4(2), CP-6, CP-6(1), CP-6(2), CP-6(3), CP-7, CP-7(1), CP-7(2), CP-7(3), CP-7(4), CP-7(6), CP-8,CP-8(1), CP-8(2), CP-8(3), CP-8(4), CP-8(5), CP-9(2), CP-9(3), CP-9(5), CP-9(6), CP-10(2), CP- 10(4), CP-11, MA-6, PE-9, PE-10, PE-11, PE-11(1), PE-13(1), PE-13(2), PE-15(1)

- *法律およびポリシーの考慮事項*

法律、規則、またはポリシーに係る要件を満たすために使用される管理策は、管理策ベースラインからテーラリングしてはならないが、一部の法律、規則、またはポリシーに係る要件は、特定の状況においてのみ適用される。こうした特定の状況が組織や特定のシステムに適用されない場合は、ベースラインをテーラリングすることは正当と認められる。

代替管理策の選択

代替管理策は、管理策ベースラインの特定の管理策の代わりに組織によって使用される。代替管理策を使用することは、必要に迫られて管理策を管理策ベースラインからテーラリングする場合には適切であるが、管理策によって提供される保護は、リスクを許容可能なレベルまで低減させる必要がある。ベースライン管理策の実装が技術的に不可能で費用対効果が低い場合や、ベースライン管理策の実装が組織のミッションや事業機能に悪影響を及ぼす場合に、多くの場合、代替管理策が選択される[33]。技術ベースのスコーピングの考慮事項については、代替管理策は一時的なものであり、システムが更新されるまでの間のみ使用される。代替管理策は、システム、組織、個人に対して同等または同様の保護[34]を提供することを目的としている[35]。代替管理策は、テーラリングプロセスでスコーピングの考慮事項を適用した後に選択される。代替管理策を使用するには、組織は、次のことを行う。

- [SP 800-53]の管理策カタログから代替管理策を選択する。
- 代替管理策がセキュリティまたはプライバシーの要件をどのように満たすのかについての根拠と、ベースライン管理策を実装できない理由の根拠を提供する。
- 適切な代替管理策が[SP 800-53]において利用可能でない場合は、他のソースから適切な代替管理策を採用する[36]。
- 代替管理策の実装に伴うセキュリティリスクとプライバシーリスクをアセスメントし、リスクを許容する。

管理策パラメータ値の設定

組み込み型パラメータ（すなわち、*設定*および*選択*操作）を含む管理策と拡張管理策により、組織は、組織の特定の要件をサポートする管理策や拡張管理策の特定の部分に値を柔軟に

[33] 例えば、特定のリアルタイムのミッションやビジネスアプリケーションにおいて、デバイスロックの代わりに追加の物理的なセキュリティ管理策が実装されることがある。小規模な組織では、職務の分離の代わりに、より頻繁な監査、対象を絞った役割ベースのトレーニング、またはより厳しい職員のスクリーニングを実装することができる。明確に規定された手順、対象を絞った役割ベースのトレーニング、および、より頻繁な監査は、自動化されたメカニズムの代わりに実装されることがある。

[34] 代替管理策は、要件に準拠する必要性を回避する目的では使用されない。代替管理策を使用することで、リスクマネジメントを促進する代わりの適切なセキュリティおよびプライバシー保護が提供される。

[35] 管理策ベースラインからテーラリングされた管理策に対して同等の保護を提供するには、複数の代替管理策が必要な場合がある。

[36] 組織は[SP 800-53]の統合管理策カタログから代替管理策を選択するよう最大限努める。組織が定める代替管理策は、組織が管理策カタログには適切な代替管理策が含まれていないと判定した場合に*のみ*採用される。

指定する。スコーピングの考慮事項の適用と代替管理策の選択後、組織は、設定や選択操作のために管理策や拡張管理策をレビューし、識別されたパラメータに対して適切な、組織が定める値を判定する。パラメータ値は、ミッションまたは事業要件によって決定される場合や、法律、大統領令、指令、規則、ポリシー、基準、ガイドライン、または業界のベストプラクティスによって定められている場合がある。

組織が管理策や拡張管理策のパラメータ値を指定すると、指定された設定値と選択値は管理策や拡張管理策の永続的な一部になる。そのため、それらは、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計画、またはシステムセキュリティおよびプライバシー計画に文書化される。パラメータの仕様化は管理策の規定を完成させ、代替管理策の必要性に影響を与える場合があるため、組織は、代替管理策を選択する前にパラメータ値を指定することができる。管理策のパラメータ値を策定する際に、コラボレーションをすることには大きな利点がある可能性がある。頻繁に協力したり、定期的に情報交換を行ったりする組織の場合には、互いに同意できる一連の管理策パラメータ値を策定すると便利である。

管理策ベースラインの補足

特定の状況では、(1)組織、ミッションと事業プロセス、およびシステムに対する特定の脅威に対応するために、(2)特定のタイプの PII の取扱いおよび関連するプライバシーリスクに対応するために、(3)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の要件を満たすために、第 3 章の管理策ベースラインに含まれる管理策および拡張管理策以外の追加の管理策や拡張管理策が必要になる場合がある。組織のリスクアセスメントは、管理策ベースラインにおける管理策および拡張管理策の必要性と充足性を判定するための情報を提供する。組織は、管理策ベースラインを追加の管理策や拡張管理策で補足するには、[SP 800-53]の管理策カタログを最大限に活用することが推奨される。

管理策実装のための追加の仕様情報の提供

管理策と拡張管理策は、より大まかに抽象的に表されるセキュリティやプライバシー機能またはケイパビリティのステートメントであるため、管理策には、実装に必要な情報が不足している場合がある。したがって、実装のために、所与の管理策の意図を完全に規定し、その管理策に関連するセキュリティおよびプライバシーの要件を確実に満たすためには、追加の詳細が必要な場合がある。たとえば、管理策を仕様要件(specification requirements)に移行させるプロセスの一部として追加情報が提供され、同じ管理策を異なる範囲に別様に適用するために実装詳細の*詳細化*、範囲の*詳細化*、または*反復*を伴う場合がある。管理策の仕様情報を提供する必要性は、要求エンジニアリング(requirements engineering)の一部としてシステムエンジニアリングプロセスで管理策が採用されている場合に、定常的に発生する。既存の管理策情報が、その管理策で意図される実装詳細を規定するのに不十分である場合、組織は、そうした情報がシステムオーナーおよび共通管理策の提供者に確実に提供されるようにする。組織は、管理策の仕様情報を管理策ステートメントの一部として含めるか、管理策の補遺セクションに別途含めるかを柔軟に決定する。詳細を追加する場合、組織は、基本管理策の意図を変更したり、管理策の元の文言を変更したりしないように注意しなければならない。実装情報は、システムセキュリティおよびプライバシー計画に文書化される。

2.5 ケイパビリティ

組織は、管理策の選択プロセスに先行して一連のケイパビリティ(capability)を規定することを考慮する。*ケイパビリティ*の概念では、セキュリティやプライバシーの要件は、単一の管理策で満たされることはほとんどないが、相互に補強し合う一連の管理策から生じるということ

を認識している。たとえば、組織は、セキュアなリモート認証のためのケイパビリティを規定することを望む場合がある。このケイパビリティは、[SP 800-53]の IA-2(1)、IA-2(2)、IA-2(8)、IA-2(9)、SC-8(1)などの一連の管理策を選択し実装することによって実現することができる。さらに、ケイパビリティは、技術的手段、物理的手段、手続き的手段、またはそれらの任意の組み合わせを含むことができる様々な領域に対応することができる。組織は、セキュアなリモートアクセスのための上記のケイパビリティに加えて、暗号モジュールの改ざん検知や軌道上の宇宙船での異常検知／分析など、物理的手段に対応するセキュリティのケイパビリティを必要とする場合もある。

ますます高度化する脅威空間に応じて[SP 800-53]の管理策の数が増えるにつれて、組織のミッションと事業機能を保護するために必要な、主要なケイパビリティの説明が可能であること、また、適切に設計、策定、実装された場合に、そうしたケイパビリティをもたらす管理策を選択することが組織にとって重要である。ケイパビリティを用いることで、保護に関する課題の概念的な見方が簡素化される。ケイパビリティの構成体により、共通の目的または共通の目標を達成するために採用される管理策をグループ化する方法が提供される。たとえば、管理策のグループ化は、管理策の有効性をアセスメントする際の重要な考慮事項である[37]。

従来、アセスメントは管理策ごとに行われ、合格（すなわち、管理策が満たされる）または不合格（すなわち、管理策が満たされていない）という結果をもたらしてきた。ただし、単一の管理策が不合格、または場合によっては複数の管理策が不合格であっても、組織で必要とされる全体的なケイパビリティには影響がない場合がある。さらに、より広範なケイパビリティの構成体を採用することで、組織は、システムの脆弱性の深刻度をアセスメントすることが可能になり、また、特定の管理策が不合格である場合や管理策を展開しないという決定を下した場合に、ミッションおよび事業の保護に必要なケイパビリティに影響するかどうかの判定が可能になる。また、定められた管理策の関係に基づいて、ある管理策の不合格がその他の管理策の不合格まで追跡することができるかどうかを判定するための、*根本原因*分析の実施も促進される。最終的には、認可の決定（すなわち、リスク許容の決定）は、必要なケイパビリティがどの程度効果的に達成され、組織が規定したセキュリティおよびプライバシーの要件を満たしているかに基づいて行われる。リスクベースの決定は、組織のリスク管理戦略の一部として規定される組織のリスク許容度に直接関連している。

[37] NIST 機関間報告書（NIST Interagency Report）8011、第 1 巻[IR 8011 v1]は、自動化された管理策アセスメントを促進する、目的別の管理策のグループ化について説明している。

第 3 章

管理策ベースライン

セキュリティおよびプライバシー管理策ベースライン

表 3-1 から表 3-20 は、[SP 800-53]の管理策ファミリーに設定されている管理策と拡張管理策のリストと、プライバシー管理策ベースライン、および低・中・高の影響度のセキュリティ管理策ベースラインに対するそれぞれの管理策の割り当てを示している。第 2.2 節（プライバシー管理策ベースライン）は、プライバシー管理策の選択基準に関する追加情報を提供している。

セキュリティおよびプライバシー管理策ベースラインの関係

- セキュリティ管理策ベースラインに設定されている管理策と拡張管理策は、機密性、完全性、可用性の喪失から生じるリスクを管理するために使用される。政府機関のプライバシー保護責任者（SAOP：Senior Agency Official for Privacy）は[OMB A-130]に従ってプライバシーリスクを管理する責任を負っており、PII の取扱いと PII の機密性、完全性、可用性の喪失の両方からプライバシーリスクが生じるため、組織は、プライバシーおよびセキュリティプログラムが、分類、テーラリング、実装、およびアセスメントなど、これらの管理策に関連する活動でどのように連携するかを考慮することが重要である。
- プライバシー管理策ベースラインにのみ設定され、セキュリティ管理策ベースラインに設定されていない管理策と拡張管理策は、[OMB A-130]に基づくプライバシープログラムの責任を管理するために重要であるが、一般的には、機密性、完全性、可用性の喪失から生じるリスクの管理をサポートしていない。
- プライバシーおよびセキュリティ管理策ベースラインの両方に設定されている管理策と拡張管理策は、[OMB A-130]に基づくプライバシープログラムの責任と、機密性、完全性、可用性（PII を含む）の喪失から生じるリスクを管理するために使用される。
- 一部の管理策と拡張管理策は、いずれの管理策ベースラインにも設定されていない。テーラリングを通じて、組織は、それらの管理策および拡張管理策が、適用される要件を満たすために必要であるかについて、また、機密性、完全性、可用性、または PII の取扱いから生じるリスクを管理するのに役立つかについて、独自の判定を行う。

3.1 「アクセス制御」ファミリー

表 3-1 は、「アクセス制御」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は、低・中・高の影響度のセキュリティ管理策ベースラインおよびプライバシー管理策ベースラインに適宜割り当てられている。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。

表 3-1:「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	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
AC-1	**ポリシーおよび手順**	x	x	x	x
AC-2	**アカウント管理**		x	x	x
AC-2(1)	自動化されたシステムアカウント管理			x	x
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			x	x
AC-2(3)	アカウントの無効化			x	x
AC-2(4)	自動化された監査			x	x
AC-2(5)	非アクティブログアウト			x	x
AC-2(6)	動的権限管理				
AC-2(7)	特権ユーザーアカウント				
AC-2(8)	動的アカウント管理				
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				
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				x
AC-2(12)	非定型的な使用のアカウントの監視				x
AC-2(13)	リスクの高い個人のアカウントの無効化			x	x
AC-3	**アクセス実施**		x	x	x
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				
AC-3(3)	必須アクセス制御				
AC-3(4)	非裁量的アクセス制御制御				
AC-3(5)	セキュリティ関連情報				
AC-3(6)	ユーザー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				
AC-3(8)	アクセス認可の取り消し				
AC-3(9)	管理されたリリース				
AC-3(10)	アクセス制御のメカニズムへの監査優先				
AC-3(11)	特定の情報タイプへのアクセスの制限				
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				
AC-3(13)	属性ベースのアクセス制御				
AC-3(14)	個人アクセス	x			
AC-3(15)	任意および必須アクセス制御				
AC-4	**情報フローの実施**			x	x

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
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				
AC-4(2)	処理ドメイン				
AC-4(3)	動的情報フロー制御				
AC-4(4)	暗号化された情報のフロー制御				X
AC-4(5)	組み込みデータタイプ				
AC-4(6)	メタデータ				
AC-4(7)	一方向フローのメカニズム				
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ー				
AC-4(9)	人によるレビュー				
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ーの有効化および無効化				
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ーの構成				
AC-4(12)	データタイプ識別子				
AC-4(13)	ポリシー関連サブコンポーネントへの分解				
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ーの制約				
AC-4(15)	容認されない情報の検出				
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				
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				
AC-4(20)	承認されたソリューション				
AC-4(21)	情報フローの物理的または論理的分離				
AC-4(22)	アクセス専用				
AC-4(23)	非公開情報の更新				
AC-4(24)	内部正規化フォーマット				
AC-4(25)	データのサニタイズ				
AC-4(26)	フィルタリング処理の監査				
AC-4(27)	冗長／独立フィルタリングのメカニズム				
AC-4(28)	線形フィルターパイプライン				
AC-4(29)	フィルターオーケストレーションエンジン				
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				
AC-4(31)	失敗したコンテンツの転送防止				
AC-4(32)	情報転送のプロセス要件				
AC-5	**職務の分離**			x	x
AC-6	**最小特権**			x	x
AC-6(1)	セキュリティ機能へのアクセスの認可			x	x
AC-6(2)	非セキュリティ機能に関する非特権アクセス			x	x
AC-6(3)	特権コマンドへのネットワークアクセス				x
AC-6(4)	個別の処理ドメイン				
AC-6(5)	特権アカウント			x	x
AC-6(6)	非組織ユーザーによる特権アクセス				
AC-6(7)	ユーザー特権のレビュー			x	x
AC-6(8)	コード実行の特権レベル				

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
AC-6(9)	特権機能の使用のログ取得			x	x
AC-6(10)	非特権ユーザーによる特権機能の実行の禁止			x	x
AC-7	**ログオン試行の失敗**		x	x	x
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				
AC-7(3)	生体認証の試行の限定				
AC-7(4)	代替認証要素の使用				
AC-8	**システム使用の通知**		x	x	x
AC-9	**過去のログオンに関する通知**				
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				
AC-9(3)	アカウント変更の通知				
AC-9(4)	追加のログオン情報				
AC-10	**同時セッション制御**				x
AC-11	**デバイスロック**			x	x
AC-11(1)	パターン表示による隠蔽			x	x
AC-12	**セッションの終了**			x	x
AC-12(1)	ユーザー起動ログアウト				
AC-12(2)	終了メッセージ				
AC-12(3)	タイムアウト警告メッセージ				
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**		x	x	x
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**				
AC-16(1)	動的属性関連付け				
AC-16(2)	認可された個人による属性値の変更				
AC-16(3)	システムによる属性関連付けの維持				
AC-16(4)	認可された個人による属性の関連付け				
AC-16(5)	出力されるオブジェクトの属性表示				
AC-16(6)	属性の関連付けの維持				
AC-16(7)	一貫した属性解釈				
AC-16(8)	関連付けの技法と技術				
AC-16(9)	属性の再設定 － 付け替えのメカニズム				
AC-16(10)	認可された個人による属性の構成				
AC-17	**リモートアクセス**		x	x	x
AC-17(1)	監視および制御			x	x
AC-17(2)	暗号化を使用した機密性および完全性の保護			x	x
AC-17(3)	管理されたアクセス制御ポイント			x	x
AC-17(4)	特権コマンドおよびアクセス			x	x
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				
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			

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
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				
AC-17(10)	リモートコマンドの認証				
AC-18	**ワイヤレスアクセス**		x	x	x
AC-18(1)	認証および暗号化			x	x
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ク形成の無効化			x	x
AC-18(4)	ユーザーによる構成設定の制限				x
AC-18(5)	アンテナおよび伝送電力レベル				x
AC-19	**モバイルデバイスのアクセス制御**		x	x	x
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				
AC-19(5)	デバイス全体またはコンテナ単位の暗号化			x	x
AC-20	**外部システムの使用**		x	x	x
AC-20(1)	認可された使用に限定			x	x
AC-20(2)	ポータブルストレージデバイス － 使用制限			x	x
AC-20(3)	組織が所有していないシステム － 使用制限				
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				
AC-20(5)	ポータブルストレージデバイス － 使用禁止				
AC-21	**情報共有**			x	x
AC-21(1)	自動化された意思決定支援				
AC-21(2)	情報調査および検索				
AC-22	**公開アクセス可能なコンテンツ**		x	x	x
AC-23	**データマイニングの保護**				
AC-24	**アクセス制御の決定**				
AC-24(1)	アクセス認可情報の伝送				
AC-24(2)	ユーザーまたはプロセスのアイデンティティが無い場合				
AC-25	**リファレンスモニター**				

3.2 「意識向上およびトレーニング」ファミリー

表 3-2 は、「意識向上およびトレーニング」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は、低・中・高の影響度のセキュリティ管理策ベースラインおよびプライバシー管理策ベースラインに適宜割り当てられている。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。

表 3-2:「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	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
AT-1	**ポリシーおよび手順**	x	x	x	x
AT-2	**リテラシートレーニングおよび意識向上**	x	x	x	x
AT-2(1)	実践的な演習				
AT-2(2)	インサイダー脅威		x	x	x
AT-2(3)	ソーシャルエンジニアリングおよびマイニング			x	x
AT-2(4)	疑わしい通信および異常なシステム動作				
AT-2(5)	持続的標的型攻撃（APT攻撃）				
AT-2(6)	サイバー脅威環境				
AT-3	**役割ベースのトレーニング**	x	x	x	x
AT-3(1)	環境に関する管理策				
AT-3(2)	物理的セキュリティ管理策				
AT-3(3)	実践的な演習				
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	x			
AT-4	**トレーニングの記録**	x	x	x	x
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**				

3.3 「監査および説明責任」ファミリー

表 3-3 は、「監査および説明責任」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は、低・中・高の影響度のセキュリティ管理策ベースラインおよびプライバシー管理策ベースラインに適宜割り当てられている。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。

表 3-3:「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	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
AU-1	**ポリシーおよび手順**	x	x	x	x
AU-2	**イベントログ取得**	x	x	x	x
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**		x	x	x
AU-3(1)	追加の監査情報				x
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	x			
AU-4	**監査ログの記憶容量**		x	x	x
AU-4(1)	代替ストレージへの転送				
AU-5	**監査ログ取得プロセス障害時の対応**		x	x	x
AU-5(1)	記憶容量の警告				x
AU-5(2)	リアルタイムアラート				x
AU-5(3)	構成可能なトラフィック量のしきい値				
AU-5(4)	障害時のシャットダウン				
AU-5(5)	代替監査ログ取得ケイパビリティ				
AU-6	**監査記録のレビュー、分析、および報告**		x	x	x
AU-6(1)	自動化されたプロセス統合			x	x
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			x	x
AU-6(4)	一元的なレビューおよび分析				
AU-6(5)	監査記録の統合分析				x
AU-6(6)	物理的監視との相関				x
AU-6(7)	許可される措置				
AU-6(8)	特権コマンドの全文分析				
AU-6(9)	非技術的ソースからの情報との相関				
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**			x	x
AU-7(1)	自動処理			x	x
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**		x	x	x

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
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**		x	x	x
AU-9(1)	ハードウェアによる追記型記録媒体				
AU-9(2)	別の物理的システムまたはコンポーネントへの保存				x
AU-9(3)	暗号化による保護				x
AU-9(4)	特権ユーザーの一部によるアクセス			x	x
AU-9(5)	二重認可				
AU-9(6)	読み取り専用アクセス				
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				
AU-10	**否認防止**				x
AU-10(1)	アイデンティティとの関連性				
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				
AU-10(3)	証拠保全				
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				
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**	x	x	x	x
AU-11(1)	長期的な検索ケイパビリティ				
AU-12	**監査記録の生成**		x	x	x
AU-12(1)	システム全体の時間に関連する監査証跡				x
AU-12(2)	標準化されたフォーマット				
AU-12(3)	認可された個人による変更				x
AU-12(4)	個人情報の照会パラメータの監査				
AU-13	**情報開示の監視**				
AU-13(1)	自動化されたツールの使用				
AU-13(2)	監視対象サイトのレビュー				
AU-13(3)	認可されていない情報の複製				
AU-14	**セッション監査**				
AU-14(1)	システムの起動				
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				
AU-15	**代替監査ログ取得ケイパビリティ**	W:AU-5(5)に移動			
AU-16	**組織横断的監査ログ取得**				
AU-16(1)	アイデンティティの保持				
AU-16(2)	監査情報の共有				
AU-16(3)	分離可能性				

3.4 「アセスメント、認可、および監視」ファミリー

表 3-4 は、「アセスメント、認可、および監視」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は、低・中・高の影響度のセキュリティ管理策ベースラインおよびプライバシー管理策ベースラインに適宜割り当てられている。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。

表 3-4:「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	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
CA-1	**ポリシーおよび手順**	x	x	x	x
CA-2	**管理策アセスメント**	x	x	x	x
CA-2(1)	独立したアセッサー			x	x
CA-2(2)	特化したアセスメント				x
CA-2(3)	外部組織からの結果の活用				
CA-3	**情報交換**		x	x	x
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				x
CA-3(7)	推移的(transitive)情報交換				
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**	x	x	x	x
CA-5(1)	的確性および最新性サポートの自動化				
CA-6	**認可**	x	x	x	x
CA-6(1)	共同認可 － 組織内				
CA-6(2)	共同認可 － 組織間				
CA-7	**継続的監視**	x	x	x	x
CA-7(1)	独立したアセスメント			x	x
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				
CA-7(4)	リスク監視	x	x	x	x
CA-7(5)	一貫性の分析				
CA-7(6)	監視サポートの自動化				
CA-8	**侵入テスト**				x
CA-8(1)	独立した侵入テストエージェントまたはチーム				x
CA-8(2)	レッドチーム演習				
CA-8(3)	施設への侵入テスト				
CA-9	**内部システム接続**		x	x	x
CA-9(1)	コンプライアンスの確認				

3.5 「構成管理」ファミリー

表 3-5 は、「構成管理」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は、低・中・高の影響度のセキュリティ管理策ベースラインおよびプライバシー管理策ベースラインに適宜割り当てられている。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。

表 3-5:「構成管理」ファミリー

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
CM-1	**ポリシーおよび手順**	x	x	x	x
CM-2	**ベースライン構成**		x	x	x
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			x	x
CM-2(3)	過去の構成の保持			x	x
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				
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			x	x
CM-3	**構成変更管理**			x	x
CM-3(1)	自動化された文書化、通知、および変更禁止				x
CM-3(2)	変更のテスト、妥当性確認、および文書化			x	x
CM-3(3)	自動化された変更措置の反映				
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			x	x
CM-3(5)	自動化されたセキュリティ対応				
CM-3(6)	暗号技術による管理				X
CM-3(7)	システム変更のレビュー				
CM-3(8)	構成の変更の防止または制限				
CM-4	**影響度分析**	x	x	x	x
CM-4(1)	独立したテスト環境				x
CM-4(2)	管理策の検証			x	x
CM-5	**変更に対するアクセス制限**		x	x	x
CM-5(1)	自動化されたアクセス実施および監査記録				x
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				
CM-5(5)	開発および運用に関する特権の規制				
CM-5(6)	ライブラリに関する特権の規制				
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**		x	x	x
CM-6(1)	自動化された管理、適用、および検証				x
CM-6(2)	認可されていない変更への対応				x
CM-6(3)	認可されていない変更の検出	W:SI-7に組み込み			

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
CM-6(4)	適合性の立証	W:CM-4に組み込み			
CM-7	**最小機能性**		x	x	x
CM-7(1)	定期的なレビュー			x	x
CM-7(2)	プログラムの実行の防止			x	x
CM-7(3)	登録に関するコンプライアンス				
CM-7(4)	認可されていないソフトウェア – 例外による拒否				
CM-7(5)	認可されたソフトウェア – 例外による許可			x	x
CM-7(6)	限定された特権を備えた制限環境				
CM-7(7)	保護された環境内でのコードの実行				
CM-7(8)	バイナリまたはマシン実行可能コード				
CM-7(9)	認可されていないハードウェアの使用の禁止				
CM-8	**システムコンポーネントのインベントリ**		x	x	x
CM-8(1)	インストール中および削除中の更新			x	x
CM-8(2)	自動化されたメンテナンス				x
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出			x	x
CM-8(4)	説明責任情報				x
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				
CM-8(7)	集中化されたリポジトリ				
CM-8(8)	自動化された位置追跡機能				
CM-8(9)	システムへのコンポーネントの設定				
CM-9	**構成管理計画**			x	x
CM-9(1)	責任の設定				
CM-10	**ソフトウェアの使用制限**		x	x	x
CM-10(1)	オープンソースソフトウェア				
CM-11	**ユーザーがインストールしたソフトウェア**		x	x	x
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				
CM-11(3)	自動化された実施および監視				
CM-12	**情報の位置**			x	x
CM-12(1)	情報の位置をサポートする自動化されたツール			x	x
CM-13	**データアクションのマッピング**				
CM-14	**署名されたコンポーネント**				

3.6 「緊急時対応計画」ファミリー

表 3-6 は、「緊急時対応計画」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は、低・中・高の影響度のセキュリティ管理策ベースラインおよびプライバシー管理策ベースラインに適宜割り当てられている。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。

表 3-6:「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	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
CP-1	**ポリシーおよび手順**		x	x	x
CP-2	**緊急時対応計画**		x	x	x
CP-2(1)	関連計画との調整			x	x
CP-2(2)	処理能力計画				x
CP-2(3)	ミッションおよび事業機能の再開			x	x
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				x
CP-2(6)	代替処理サイトおよび代替保管サイト				
CP-2(7)	外部サービスプロバイダとの調整				
CP-2(8)	重要な資産の特定			x	x
CP-3	**緊急時対応トレーニング**		x	x	x
CP-3(1)	シミュレーションイベント				x
CP-3(2)	トレーニング環境で使用されるメカニズム				
CP-4	**緊急時対応計画テスト**		x	x	x
CP-4(1)	関連計画との調整			x	x
CP-4(2)	代替処理サイト				x
CP-4(3)	自動化されたテスト				
CP-4(4)	完全な復旧および再構成				
CP-4(5)	自己チャレンジ				
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**			x	x
CP-6(1)	一次サイトからの分離			x	x
CP-6(2)	復旧時間および復旧ポイントの目標				x
CP-6(3)	アクセシビリティ			x	x
CP-7	**代替処理サイト**			x	x
CP-7(1)	一次サイトからの分離			x	x
CP-7(2)	アクセシビリティ			x	x
CP-7(3)	サービスの優先順位			x	x
CP-7(4)	使用準備				x
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				
CP-8	**通信サービス**			x	x
CP-8(1)	サービス提供の優先順位			x	x

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
CP-8(2)	単一障害点			x	x
CP-8(3)	一次プロバイダおよび代替プロバイダの分離				x
CP-8(4)	プロバイダの緊急時対応計画				x
CP-8(5)	代替通信サービスのテスト				
CP-9	**システムバックアップ**		x	x	x
CP-9(1)	信頼性および完全性のテスト			x	x
CP-9(2)	サンプリングを使用した復元テスト				x
CP-9(3)	重要な情報の分離保管				x
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				x
CP-9(6)	冗長二次システム				
CP-9(7)	削除や破壊に対する二重認可				
CP-9(8)	暗号化による保護			x	x
CP-10	**システムの復旧および再構成**		x	x	x
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			x	x
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				x
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				
CP-11	**代替通信プロトコル**				
CP-12	**セーフモード**				
CP-13	**代替セキュリティのメカニズム**				

3.7 「識別および認証」ファミリー

表 3-7 は、「識別および認証」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は、低・中・高の影響度のセキュリティ管理策ベースラインおよびプライバシー管理策ベースラインに適宜割り当てられている。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。

表 3-7:「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	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
IA-1	**ポリシーおよび手順**		x	x	x
IA-2	**識別および認証（組織のユーザー）**		x	x	x
IA-2(1)	特権アカウントへの多要素認証		x	x	x
IA-2(2)	非特権アカウントへの多要素認証		x	x	x
IA-2(3)	特権アカウントへのローカルアクセス	W：IA-2(1)(2)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(1)(2)に組み込み			
IA-2(5)	グループ認証時の個人認証				x
IA-2(6)	アカウントへのアクセス ― 別のデバイス				
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		x	x	x
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				
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		x	x	x
IA-2(13)	経路外通信認証				
IA-3	**デバイスの識別および認証**			x	x
IA-3(1)	暗号双方向認証				
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				
IA-3(4)	デバイス証明				
IA-4	**識別子管理**		x	x	x
IA-4(1)	公開識別子のアカウント識別子使用禁止				
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)	ユーザーステータスの識別			x	x
IA-4(5)	動的管理				
IA-4(6)	組織横断的な管理				
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				
IA-4(9)	属性の維持および保護				
IA-5	**オーセンティケータ管理**		x	x	x
IA-5(1)	パスワードによる認証		x	x	x

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
IA-5(2)	公開鍵ベースの認証			x	x
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				
IA-5(6)	オーセンティケータの保護			x	x
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				
IA-5(8)	複数のシステムアカウント				
IA-5(9)	フェデレーションによるクレデンシャル管理				
IA-5(10)	動的クレデンシャルのバインディング				
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				
IA-5(13)	キャッシュされたオーセンティケータの期限				
IA-5(14)	PKIトラストストアの内容管理				
IA-5(15)	GSA承認の製品およびサービス				
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				
IA-5(17)	生体情報の提示型攻撃検出				
IA-5(18)	パスワードマネージャー				
IA-6	**認証フィードバック**		x	x	x
IA-7	**暗号モジュール認証**		x	x	x
IA-8	**識別および認証（非組織のユーザー）**		x	x	x
IA-8(1)	他の機関からのPIVクレデンシャルの受け入れ		x	x	x
IA-8(2)	外部オーセンティケータの受け入れ		x	x	x
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		x	x	x
IA-8(5)	PIV-Iクレデンシャルの受け入れ				
IA-8(6)	分離可能性				
IA-9	**サービスの識別および認証**				
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**				
IA-11	**再認証**		x	x	x
IA-12	**アイデンティティ証明**			x	x
IA-12(1)	監督者認可				
IA-12(2)	アイデンティティのエビデンス			x	x
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			x	x
IA-12(4)	対面による妥当性確認および検証				x
IA-12(5)	アドレス確認			x	x
IA-12(6)	外部で証明されたアイデンティティの受け入れ				

3.8 「インシデント対応」ファミリー

表 3-8 は、「インシデント対応」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は、低・中・高の影響度のセキュリティ管理策ベースラインおよびプライバシー管理策ベースラインに適宜割り当てられている。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。

表 3-8:「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	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
IR-1	**ポリシーおよび手順**	x	x	x	x
IR-2	**インシデント対応トレーニング**	x	x	x	x
IR-2(1)	シミュレーションイベント				x
IR-2(2)	自動化されたトレーニング環境				x
IR-2(3)	ブリーチ	x			
IR-3	**インシデント対応テスト**	x		x	x
IR-3(1)	自動化されたテスト				
IR-3(2)	関連計画との調整			x	x
IR-3(3)	継続的改善				
IR-4	**インシデント処理**	x	x	x	x
IR-4(1)	自動化されたインシデント処理プロセス			x	x
IR-4(2)	動的再構成				
IR-4(3)	運用の継続性				
IR-4(4)	情報の相互関連付け				x
IR-4(5)	システムの自動無効化				
IR-4(6)	インサイダー脅威				
IR-4(7)	インサイダー脅威 — 組織内連携				
IR-4(8)	外部組織との相互関連付け				
IR-4(9)	動的対応ケイパビリティ				
IR-4(10)	サプライチェーンとの連携				
IR-4(11)	統合インシデント対応チーム				x
IR-4(12)	悪意のあるコードおよびフォレンジック分析				
IR-4(13)	ふるまい分析				
IR-4(14)	セキュリティオペレーションセンター				
IR-4(15)	広報活動および評判の修復				
IR-5	**インシデント監視**	x	x	x	x
IR-5(1)	自動化された追跡、データ収集、および分析				x
IR-6	**インシデント報告**	x	x	x	x
IR-6(1)	自動化された報告			x	x
IR-6(2)	インシデントに関連する脆弱性				
IR-6(3)	サプライチェーンとの連携			x	x
IR-7	**インシデント対応支援**	x	x	x	x
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			x	x

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
IR-7(2)	外部プロバイダとの連携				
IR-8	**インシデント対応計画**	x	x	x	x
IR-8(1)	ブリーチ	x			
IR-9	**情報流出対応**				
IR-9(1)	責任者	W：IR-9に組み込み			
IR-9(2)	トレーニング				
IR-9(3)	流出後の運用				
IR-9(4)	認可されていない職員への露出				
IR-10	**統合情報セキュリティ分析チーム**	W：IR-4(11)に移動			

3.9 「メンテナンス」ファミリー

表 3-9 は、「メンテナンス」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は、低・中・高の影響度のセキュリティ管理策ベースラインおよびプライバシー管理策ベースラインに適宜割り当てられている。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。

表 3-9:「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	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
MA-1	**ポリシーおよび手順**		x	x	x
MA-2	**管理されたメンテナンス**		x	x	x
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				x
MA-3	**メンテナンスツール**			x	x
MA-3(1)	ツールの検査			x	x
MA-3(2)	媒体の検査			x	x
MA-3(3)	認可されていない移動の防止			x	x
MA-3(4)	ツールの使用制限				
MA-3(5)	特権での実行				
MA-3(6)	ソフトウェアの更新およびパッチ				
MA-4	**非ローカルメンテナンス**		x	x	x
MA-4(1)	ログ取得およびレビュー				
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				x
MA-4(4)	メンテナンスセッションの認証および分離				
MA-4(5)	承認および通知				
MA-4(6)	暗号による保護				
MA-4(7)	切断の検証				
MA-5	**メンテナンス作業員**		x	x	x
MA-5(1)	適切なアクセス権限のない個人				x
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				
MA-5(3)	国家機密情報を扱うシステムの米国市民権要件				
MA-5(4)	外国人				
MA-5(5)	システム以外のメンテナンス				
MA-6	**タイムリーなメンテナンス**			x	x
MA-6(1)	予防メンテナンス				
MA-6(2)	予測メンテナンス				
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				
MA-7	**フィールドメンテナンス**				

3.10 「媒体保護」ファミリー

表 3-10 は、「媒体保護」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は、低・中・高の影響度のセキュリティ管理策ベースラインおよびプライバシー管理策ベースラインに適宜割り当てられている。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。

表 3-10:「媒体保護」ファミリー

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
MP-1	**ポリシーおよび手順**	x	x	x	x
MP-2	**媒体へのアクセス**		x	x	x
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**			x	x
MP-4	**媒体保管**			x	x
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				
MP-5	**媒体移送**			x	x
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				
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**	x	x	x	x
MP-6(1)	レビュー、承認、追跡、文書化、検証				x
MP-6(2)	装置のテスト				x
MP-6(3)	非破壊的技法				x
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				
MP-6(8)	情報のリモート除去またはリモート抹消				
MP-7	**媒体の使用**		x	x	x
MP-7(1)	所有者なしでの使用禁止	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				
MP-8	**媒体のダウングレード**				
MP-8(1)	プロセスの文書化				
MP-8(2)	装置のテスト				
MP-8(3)	管理対象非機密情報				
MP-8(4)	国家機密情報				

3.11 「物理的および環境的保護」ファミリー

表 3-11 は、「物理的および環境的保護」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は、低・中・高の影響度のセキュリティ管理策ベースラインおよびプライバシー管理策ベースラインに適宜割り当てられている。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。

表 3-11：「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	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
PE-1	**ポリシーおよび手順**		x	x	x
PE-2	**物理的アクセス認可**		x	x	x
PE-2(1)	職位または役割によるアクセス				
PE-2(2)	2つの身分証明書				
PE-2(3)	エスコートされていないアクセスの制限				
PE-3	**物理的アクセス制御**		x	x	x
PE-3(1)	システムアクセス				x
PE-3(2)	施設およびシステム				
PE-3(3)	継続的な警備				
PE-3(4)	施錠可能なケース				
PE-3(5)	タンパー保護				
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				
PE-3(8)	前室のアクセス制御				
PE-4	**伝送設備のアクセス制御**			x	x
PE-5	**出力デバイスのアクセス制御**			x	x
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				
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**		x	x	x
PE-6(1)	侵入警報装置および侵入監視装置			x	x
PE-6(2)	自動化された侵入検知および侵入対応				
PE-6(3)	ビデオ監視				
PE-6(4)	システムへの物理的アクセスの監視				x
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**		x	x	x
PE-8(1)	自動化された記録の維持およびレビュー				x
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	x			
PE-9	**電源装置およびケーブル**			x	x
PE-9(1)	冗長ケーブル				
PE-9(2)	自動電圧制御				
PE-10	**緊急遮断**			x	x

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
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**			x	x
PE-11(1)	代替電源 － 最小運用ケイパビリティ				x
PE-11(2)	代替電源 － 自給型				
PE-12	**非常用照明**		x	x	x
PE-12(1)	必須のミッションおよび事業機能				
PE-13	**防火**		x	x	x
PE-13(1)	検知システム － 自動起動および通知			x	x
PE-13(2)	消火システム － 自動起動および通知				x
PE-13(3)	自動消火	W：PE-13(2)に組み込み			
PE-13(4)	点検				
PE-14	**環境制御**		x	x	x
PE-14(1)	自動制御				
PE-14(2)	警報および通知による監視				
PE-15	**漏水損傷保護**		x	x	x
PE-15(1)	自動サポート				x
PE-16	**搬入および搬出**		x	x	x
PE-17	**代替作業サイト**			x	x
PE-18	**システムコンポーネントの設置場所**				x
PE-18(1)	施設サイト	W：PE-23に移動			
PE-19	**情報漏えい**				
PE-19(1)	国家エミッションポリシーおよび手順				
PE-20	**資産の監視および追跡**				
PE-21	**電磁パルス保護**				
PE-22	**コンポーネントマーキング**				
PE-23	**施設の場所**				

3.12 「計画」ファミリー

表 3-12 は、「計画」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は、低・中・高の影響度のセキュリティ管理策ベースラインおよびプライバシー管理策ベースラインに適宜割り当てられている。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。

表 3-12:「計画」ファミリー

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
PL-1	**ポリシーおよび手順**	x	x	x	x
PL-2	**システムセキュリティおよびプライバシー計画**	x	x	x	x
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**	x	x	x	x
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	x	x	x	x
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**				
PL-8	**セキュリティおよびプライバシーアーキテクチャ**	x		x	x
PL-8(1)	多層防御				
PL-8(2)	サプライヤーの多様性				
PL-9	**一元管理**	x			
PL-10	**ベースラインの選択**		x	x	x
PL-11	**ベースラインのテーラリング**		x	x	x

3.13 「プログラムマネジメント」ファミリー

表 3-13 は、「プログラムマネジメント」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は個々の情報システムに対してではなく組織レベルで実装される。「プログラムマネジメント」管理策は、適用される連邦法、大統領令、指令、規則、ポリシー、および基準へのコンプライアンスを促進するように設計されている。

表 3-13:「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	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
PM-1	**情報セキュリティプログラム計画**		**組織全体で導入される。 情報セキュリティプログラムをサポートする。 セキュリティ管理策ベースラインと関連しない。 システム影響度レベルから独立している。**		
PM-2	**情報セキュリティプログラムの責任者の役割**				
PM-3	**情報セキュリティおよびプライバシーリソース**	x			
PM-4	**実施計画およびマイルストーンプロセス**	x			
PM-5	**システムインベントリ**				
PM-5(1)	個人情報のインベントリ	x			
PM-6	**パフォーマンス尺度**	x			
PM-7	**エンタープライズアーキテクチャ**	x			
PM-7(1)	オフロード				
PM-8	**重要インフラ計画**	x			
PM-9	**リスクマネジメント戦略**	x			
PM-10	**認可プロセス**	x			
PM-11	**ミッションおよび事業プロセスの規定**	x			
PM-12	**インサイダー脅威対策プログラム**				
PM-13	**セキュリティおよびプライバシー要員**	x			
PM-14	**テスト、トレーニング、および監視**	x			
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**				
PM-16	**脅威認識プログラム**				
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				
PM-17	**外部システム上の管理対象非機密情報の保護**	x			
PM-18	**プライバシープログラム計画**	x			
PM-19	**プライバシープログラムの責任者の役割**	x			
PM-20	**プライバシープログラム情報の周知**	x			
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	x			
PM-21	**開示事項のアカウンティング**	x			
PM-22	**個人情報の品質管理**	x			
PM-23	**データガバナンス会議体**				
PM-24	**データインテグリティ委員会**	x			
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**	x			
PM-26	**苦情管理**	x			
PM-27	**プライバシー報告**	x			
PM-28	**リスクの枠組み**	x			

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
PM-29	**リスクマネジメントプログラムの責任者の役割**				
PM-30	**サプライチェーンリスクマネジメント戦略**				
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ー				
PM-31	**継続的監視戦略**	x			
PM-32	**目的**				

3.14 「職員のセキュリティ」ファミリー

表 3-14 は、「職員のセキュリティ」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は、低・中・高の影響度のセキュリティ管理策ベースラインおよびプライバシー管理策ベースラインに適宜割り当てられている。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。

表 3-14:「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	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
PS-1	**ポリシーおよび手順**		x	x	x
PS-2	**職位のリスク指定**		x	x	x
PS-3	**職員のスクリーニング**		x	x	x
PS-3(1)	国家機密情報				
PS-3(2)	正式な教化				
PS-3(3)	特別な保護手段を必要とする情報				
PS-3(4)	市民権要件				
PS-4	**職員の雇用終了**		x	x	x
PS-4(1)	雇用終了後要件				
PS-4(2)	自動化された措置				x
PS-5	**職員の異動**		x	x	x
PS-6	**アクセス合意書**	x	x	x	x
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				
PS-6(3)	雇用終了後要件				
PS-7	**外部職員のセキュリティ**		x	x	x
PS-8	**職員の制裁**		x	x	x
PS-9	**職位記述**		x	x	x

3.15 「個人情報の取扱いおよび透明性」ファミリー

表 3-15 は、「個人情報の取扱いおよび透明性」ファミリーに設定されている管理策と拡張管理策の概要を示している。管理策は、第 2.2 節に規定されている選択基準に従ってプライバシー管理策ベースラインに割り当てられる。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。

表 3-15:「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	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
PT-1	**ポリシーおよび手順**	x	**「個人情報の取扱いおよび透明性」管理策はセキュリティ管理策ベースラインに割り当てられていない。** **プライバシーベースライン管理策は、第2.2節で規定されている選択基準に基づいて選択される。**		
PT-2	**個人情報を取扱う職権**	x			
PT-2(1)	データタグ付け				
PT-2(2)	自動化				
PT-3	**個人情報の取扱い目的**	x			
PT-3(1)	データタグ付け				
PT-3(2)	自動化				
PT-4	**同意**	x			
PT-4(1)	テーラリングされた同意				
PT-4(2)	ジャストインタイムの同意				
PT-4(3)	取消し				
PT-5	**プライバシー通知**	x			
PT-5(1)	ジャストインタイムの通知				
PT-5(2)	プライバシー保護法のステートメン	x			
PT-6	**記録システムの通知**	x			
PT-6(1)	定常的な利用	x			
PT-6(2)	適用除外規定	x			
PT-7	**個人情報の特定の分類**	x			
PT-7(1)	社会保障番号	x			
PT-7(2)	第一修正条項情報	x			
PT-8	**コンピュータマッチング要件**	x			

3.16 「リスクアセスメント」ファミリー

表 3-16 は、「リスクアセスメント」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は、低・中・高の影響度のセキュリティ管理策ベースラインおよびプライバシー管理策ベースラインに適宜割り当てられている。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。

表 3-16：「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	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
RA-1	**ポリシーおよび手順**	x	x	x	x
RA-2	**セキュリティ分類化**		x	x	x
RA-2(1)	影響度レベルの優先順位付け				
RA-3	**リスクアセスメント**	x	x	x	x
RA-3(1)	サプライチェーンのリスクアセスメント		x	x	x
RA-3(2)	オールソースインテリジェンスの活用				
RA-3(3)	動的脅威認識				
RA-3(4)	予測的サイバー分析				
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**		x	x	x
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		x	x	x
RA-5(3)	カバレッジの幅および深さ				
RA-5(4)	検出可能な情報				x
RA-5(5)	特権アクセス			x	x
RA-5(6)	自動化された傾向分析				
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出および通知	W：CM-8に組み込み			
RA-5(8)	過去の監査ログのレビュー				
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				
RA-5(11)	公開開示プログラム		x	x	x
RA-6	**技術監視対策調査**				
RA-7	**リスク対応**	x	x	x	x
RA-8	**プライバシー影響評価**	x			
RA-9	**重要度分析**			x	x
RA-10	**脅威ハンティング**				

3.17 「システムおよびサービスの取得」ファミリー

表 3-17 は、「システムおよびサービスの取得」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は、低・中・高の影響度のセキュリティ管理策ベースラインおよびプライバシー管理策ベースラインに適宜割り当てられている。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。

表 3-17:「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	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
SA-1	**ポリシーおよび手順**	x	x	x	x
SA-2	**リソースの割り当て**	x	x	x	x
SA-3	**システム開発ライフサイクル**	x	x	x	x
SA-3(1)	運用前環境の管理				
SA-3(2)	ライブデータまたは運用データの使用				
SA-3(3)	技術の更新				
SA-4	**取得プロセス**	x	x	x	x
SA-4(1)	管理策の機能特性			x	x
SA-4(2)	管理策のための設計および実装情報			x	x
SA-4(3)	開発方法、技法、および実践				
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				x
SA-4(6)	情報保証製品の使用				
SA-4(7)	NIAP承認済みプロテクションプロファイル				
SA-4(8)	管理策の継続的監視計画				
SA-4(9)	使用中の機能、ポート、プロトコル、およびサービス			x	x
SA-4(10)	承認されたPIV製品の使用		x	x	x
SA-4(11)	記録システム				
SA-4(12)	データ所有権				
SA-5	**システムドキュメント**		x	x	x
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	**ユーザー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**		x	x	x
SA-8(1)	明確な抽象化				
SA-8(2)	最小共通メカニズム				
SA-8(3)	モジュール性および階層化				
SA-8(4)	半順序の依存関係				
SA-8(5)	効率的に仲介されたアクセス				

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
SA-8(6)	共有の最小化				
SA-8(7)	複雑さの軽減				
SA-8(8)	セキュアな保守拡張性				
SA-8(9)	信頼できるコンポーネント				
SA-8(10)	階層的信頼				
SA-8(11)	逆変更しきい値				
SA-8(12)	階層的保護				
SA-8(13)	最小化されたセキュリティ要素				
SA-8(14)	最小特権				
SA-8(15)	根拠のある許可				
SA-8(16)	自立した統合的信頼性				
SA-8(17)	セキュアな分散構成				
SA-8(18)	信頼できる通信チャネル				
SA-8(19)	継続的な保護				
SA-8(20)	セキュアなメタデータ管理				
SA-8(21)	自己分析				
SA-8(22)	説明責任およびトレーサビリティ				
SA-8(23)	セキュアデフォルト				
SA-8(24)	セキュアな障害および回復				
SA-8(25)	経済的セキュリティ				
SA-8(26)	パフォーマンスセキュリティ				
SA-8(27)	人的要因によるセキュリティ				
SA-8(28)	許容可能なセキュリティ				
SA-8(29)	再現性のある文書化された手順				
SA-8(30)	手順の厳格さ				
SA-8(31)	セキュアなシステム変更				
SA-8(32)	十分なドキュメント				
SA-8(33)	最小化	x			
SA-9	**外部システムサービス**	x	x	x	x
SA-9(1)	リスクアセスメントおよび組織承認				
SA-9(2)	機能、ポート、プロトコル、およびサービスの特定			x	x
SA-9(3)	プロバイダとの信頼関係の確立および維持				
SA-9(4)	消費者およびプロバイダの一貫した利益				
SA-9(5)	処理、保管、およびサービスの場所				
SA-9(6)	組織が管理する暗号鍵				
SA-9(7)	組織管理の完全性チェック				
SA-9(8)	処理および保管場所 ― 米国の司法管轄				
SA-10	**開発者構成管理**			x	x
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				
SA-10(2)	代替構成管理プロセス				
SA-10(3)	ハードウェアの完全性の検証				
SA-10(4)	信頼できる世代				
SA-10(5)	バージョン管理のための完全性のマッピング				

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
SA-10(6)	信頼できる配布				
SA-10(7)	セキュリティおよびプライバシーの代表者				
SA-11	**開発者のテストおよび評価**	x		x	x
SA-11(1)	静的コード分析				
SA-11(2)	脅威のモデル化および脆弱性の分析				
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				
SA-11(4)	手動のコードレビュー				
SA-11(5)	侵入テスト				
SA-11(6)	攻撃対象領域のレビュー				
SA-11(7)	テストおよび評価の範囲の検証				
SA-11(8)	動的コード分析				
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				
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)	サプライヤーレビュー	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)	サプライヤーの多様性	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**			x	x
SA-15(1)	品質指標				
SA-15(2)	セキュリティおよびプライバシーの追跡ツール				
SA-15(3)	重要度分析			x	x
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				
SA-15(6)	継続的な改善				
SA-15(7)	自動化された脆弱性分析				
SA-15(8)	脅威および脆弱性情報の再利用				
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				
SA-15(11)	システムまたはコンポーネントのアーカイブ				

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
SA-15(12)	個人情報の最小化				
SA-16	**開発者が提供するトレーニング**				x
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**				x
SA-17(1)	正式なポリシーモデル				
SA-17(2)	セキュリティ関連のコンポーネント				
SA-17(3)	正式な対応				
SA-17(4)	非公式な対応				
SA-17(5)	概念的にシンプルな設計				
SA-17(6)	テストのための構造				
SA-17(7)	最小特権の構造				
SA-17(8)	オーケストレーション				
SA-17(9)	設計の多様性				
SA-18	**耐タンパー性および検出**	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**				
SA-21	**開発者スクリーニング**				x
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**		x	x	x
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**				

3.18 「システムおよび通信の保護」ファミリー

表 3-18 は、「システムおよび通信の保護」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は、低・中・高の影響度のセキュリティ管理策ベースラインおよびプライバシー管理策ベースラインに適宜割り当てられている。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。

表 3-18:「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	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
SC-1	**ポリシーおよび手順**		x	x	x
SC-2	**システムおよびユーザー機能の分離**			x	x
SC-2(1)	非特権ユーザーのためのインタフェース				
SC-2(2)	分離可能性				
SC-3	**セキュリティ機能の分離**				x
SC-3(1)	ハードウェアの分離				
SC-3(2)	アクセスおよびフロー制御機能				
SC-3(3)	非セキュリティ機能の最小化				
SC-3(4)	モジュールの結合度および凝集度				
SC-3(5)	階層構造				
SC-4	**共有システムリソース内の情報**			x	x
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				
SC-5	**サービス拒否からの保護**		x	x	x
SC-5(1)	他のシステムへの攻撃能力の制限				
SC-5(2)	容量、帯域幅、および冗長性				
SC-5(3)	検出および監視				
SC-6	**リソースの可用性**				
SC-7	**境界保護**		x	x	x
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			x	x
SC-7(4)	外部通信サービス			x	x
SC-7(5)	デフォルトで拒否 – 例外で許可			x	x
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			x	x
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			x	x
SC-7(9)	脅威となる外向け通信トラフィックの制限				
SC-7(10)	漏出の防止				
SC-7(11)	着信通信トラフィックの制限				
SC-7(12)	ホストベースの保護				
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				

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
SC-7(14)	認可されていない物理的接続からの保護				
SC-7(15)	ネットワーク化された特権アクセス				
SC-7(16)	システムコンポーネント検出の防止				
SC-7(17)	プロトコル形式の自動化された実施				
SC-7(18)	フェールセキュア				x
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				
SC-7(20)	動的な分離および隔離				
SC-7(21)	システムコンポーネントの分離				x
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				
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				
SC-7(24)	個人情報	x			
SC-7(25)	非機密国家安全保障システムの接続				
SC-7(26)	機密国家安全保障システムの接続				
SC-7(27)	非機密非国家安全保障システムの接続				
SC-7(28)	パブリックネットワークへの接続				
SC-7(29)	機能を分離するための別のサブネット				
SC-8	**伝送の機密性および完全性**			x	x
SC-8(1)	暗号保護			x	x
SC-8(2)	送信前および送信後の処理				
SC-8(3)	メッセージの外側の暗号化保護				
SC-8(4)	通信の秘匿化またはランダム化				
SC-8(5)	保護された配信システム				
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**			x	x
SC-11	**信頼できる経路**				
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				
SC-12	**暗号鍵の確立および管理**		x	x	x
SC-12(1)	可用性				x
SC-12(2)	対称鍵				
SC-12(3)	非対称鍵				
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				
SC-13	**暗号保護**		x	x	x
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**		x	x	x
SC-15(1)	物理的または論理的な切断				

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
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			
SC-15(3)	セキュアな作業領域での無効化および削除				
SC-15(4)	現在の参加者の明示				
SC-16	**セキュリティおよびプライバシーの属性の伝送**				
SC-16(1)	完全性の検証				
SC-16(2)	なりすまし防止メカニズム				
SC-16(3)	暗号化バインディング				
SC-17	**公開鍵基盤の証明書**			x	x
SC-18	**モバイルコード**			x	x
SC-18(1)	許可されないコードの特定および是正措置				
SC-18(2)	取得、開発、および使用				
SC-18(3)	ダウンロードおよび実行の防止				
SC-18(4)	自動実行の防止				
SC-18(5)	制限された環境に限った実行の許可				
SC-19	ボイス・オーバー・インターネット・プロトコル（VOIP）	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）**		x	x	x
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				
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）**		x	x	x
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**		x	x	x
SC-23	**セッションの真正性**			x	x
SC-23(1)	ログアウト時のセッション識別子の無効化				
SC-23(2)	ユーザー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				
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				
SC-24	**既知の安全な状態での障害**				x
SC-25	**シンノード**				
SC-26	**デコイ**				
SC-26(1)	悪意のあるコードの検出	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**				
SC-28	**保管中の情報の保護**			x	x
SC-28(1)	暗号保護			x	x
SC-28(2)	オフラインストレージ				
SC-28(3)	暗号鍵				
SC-29	**異質性**				
SC-29(1)	仮想化技法				
SC-30	**秘匿化および誤認誘導**				

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
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				
SC-30(3)	処理場所および保管場所の変更				
SC-30(4)	誤解を招く情報				
SC-30(5)	システムコンポーネントの秘匿化				
SC-31	**カバートチャネル分析**				
SC-31(1)	探知可能性のためのカバートチャネルのテスト				
SC-31(2)	最大帯域幅				
SC-31(3)	運用環境での帯域幅の測定				
SC-32	**システム分割**				
SC-32(1)	特権機能のための物理ドメインの分離				
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**				
SC-34(1)	書き込み可能なストレージ				
SC-34(2)	読み取り専用媒体の完全性保護				
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**				
SC-36	**分散処理およびストレージ**				
SC-36(1)	ポーリング技法				
SC-36(2)	同期				
SC-37	**帯域外チャネル**				
SC-37(1)	確実な配信および送信				
SC-38	**運用セキュリティ**				
SC-39	**プロセス分離**		x	x	x
SC-39(1)	ハードウェア分離				
SC-39(2)	スレッドごとの個別の実行ドメイン				
SC-40	**ワイヤレスリンクの保護**				
SC-40(1)	電磁干渉				
SC-40(2)	検出の可能性の低減				
SC-40(3)	模倣的または操作的な通信の偽装				
SC-40(4)	信号パラメータの識別				
SC-41	**ポートおよびI/Oデバイスへのアクセス**				
SC-42	**センサーの能力およびデータ**				
SC-42(1)	認可された個人または役割への報告				
SC-42(2)	認可された使用				
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				
SC-42(5)	収集の最小化				
SC-43	**使用制限**				
SC-44	**デトネーションチャンバー**				
SC-45	**システム時刻同期**				
SC-45(1)	信頼できるタイムソースとの同期				
SC-45(2)	二次的な信頼できるタイムソース				

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
SC-46	**クロスドメインポリシーの実施**				
SC-47	**代替通信経路**				
SC-48	**センサーの再配置**				
SC-48(1)	センサーまたは監視機能の動的な再配置				
SC-49	**ハードウェアによる分離およびポリシーの適用**				
SC-50	**ソフトウェアによる分離およびポリシーの適用**				
SC-51	**ハードウェアベースの保護**				

3.19 「システムおよび情報の完全性」ファミリー

表 3-19 は、「システムおよび情報の完全性」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は、低・中・高の影響度のセキュリティ管理策ベースラインおよびプライバシー管理策ベースラインに適宜割り当てられている。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。

表 3-19:「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	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
SI-1	**ポリシーおよび手順**	x	x	x	x
SI-2	**欠陥の修正**		x	x	x
SI-2(1)	集中管理	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			x	x
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				
SI-2(4)	自動化されたパッチ管理ツール				
SI-2(5)	ソフトウェアおよびファームウェアの自動更新				
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				
SI-3	**悪意のあるコードからの保護**		x	x	x
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)	非特権ユーザー	W:AC-6(10)に組み込み			
SI-3(4)	特権ユーザーに限定した更新				
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				
SI-3(7)	非署名ベースの検出	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出				
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				
SI-4	**システム監視**		x	x	x
SI-4(1)	システム全体の侵入検知システム				
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			x	x
SI-4(3)	自動化されたツールおよびメカニズムの統合				
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			x	x
SI-4(5)	システムによって生成されたアラート			x	x
SI-4(6)	非特権ユーザーの制限	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				
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				
SI-4(10)	暗号化通信の可視性				x
SI-4(11)	通信トラフィック異常の分析				
SI-4(12)	自動化された組織生成アラート				x

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
SI-4(13)	トラフィックおよびイベントのパターンの分析				
SI-4(14)	ワイヤレス侵入検知				x
SI-4(15)	ワイヤレスから有線への通信				
SI-4(16)	監視情報の関連付け				
SI-4(17)	統合された状況認識				
SI-4(18)	トラフィックおよび秘密の漏出の分析				
SI-4(19)	個人のリスク				
SI-4(20)	特権ユーザー				x
SI-4(21)	試用期間				
SI-4(22)	認可されていないネットワークサービス				x
SI-4(23)	ホストベースのデバイス				
SI-4(24)	危殆化の徴候				
SI-4(25)	ネットワークトラフィック分析の最適化				
SI-5	**セキュリティのアラート、勧告、および指令**		x	x	x
SI-5(1)	自動化されたアラートおよび勧告				x
SI-6	**セキュリティおよびプライバシー機能の検証**				x
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				
SI-6(3)	検証結果の報告				
SI-7	**ソフトウェア、ファームウェア、および情報の完全性**			x	x
SI-7(1)	完全性チェック			x	x
SI-7(2)	完全性違反の自動通知				x
SI-7(3)	集中管理された完全性ツール				
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応答				x
SI-7(6)	暗号保護				
SI-7(7)	検出および対応の統合			x	x
SI-7(8)	重要なイベントの能力の監査				
SI-7(9)	ブートプロセスの確認				
SI-7(10)	ブートファームウェアの保護				
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				
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				x
SI-7(16)	監視なしのプロセス実行の時間制限				
SI-7(17)	実行時のアプリケーションの自己保護				
SI-8	**スパム保護**			x	x
SI-8(1)	一元管理	W：PL-9に組み込み			
SI-8(2)	自動更新			x	x
SI-8(3)	継続的な学習能力				
SI-9	**情報入力の制限**	W：AC-2, AC-3, AC-5, AC-6に組み込み			

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
SI-10	**情報入力の妥当性確認**			x	x
SI-10(1)	手動オーバーライド機能				
SI-10(2)	エラーのレビューおよび解決				
SI-10(3)	予測可能な動作				
SI-10(4)	タイミングの相互作用				
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				
SI-10(6)	注入防止				
SI-11	**エラー処理**			x	x
SI-12	**情報管理および保持**	x	x	x	x
SI-12(1)	個人情報要素の制限	x			
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	x			
SI-12(3)	情報の廃棄	x			
SI-13	**予測可能な障害の防止**				
SI-13(1)	コンポーネントの責任の移管				
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				
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				
SI-13(5)	フェイルオーバー機能				
SI-14	**非永続性**				
SI-14(1)	信頼できるソースからの更新				
SI-14(2)	非永続的情報				
SI-14(3)	非永続的接続性				
SI-15	**情報出力フィルタリング**				
SI-16	**メモリ保護**			x	x
SI-17	**フェイルセーフ手順**				
SI-18	**個人情報の品質運用**	x			
SI-18(1)	自動サポート				
SI-18(2)	データタグ				
SI-18(3)	収集				
SI-18(4)	個人の要求	x			
SI-18(5)	修正または削除の通知				
SI-19	**匿名化**	x			
SI-19(1)	収集				
SI-19(2)	アーカイブ				
SI-19(3)	リリース				
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				
SI-19(5)	統計的開示管理				
SI-19(6)	ディファレンシャルプライバシー				
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				
SI-19(8)	動機付けされた侵入者				
SI-20	**汚染**				
SI-21	**情報の更新**				
SI-22	**情報の多様性**				

管理策番号	管理策名 拡張管理策名	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
SI-23	情報の断片化				

3.20 「サプライチェーンのリスクマネジメント」ファミリー

表 3-20 は、「サプライチェーンのリスクマネジメント」ファミリーに設定されている管理策と拡張管理策の概要を示している。これらの管理策は、低・中・高の影響度のセキュリティ管理策ベースラインおよびプライバシー管理策ベースラインに適宜割り当てられている。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。

表 3-20:「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	プライバシー管理策ベースライン	セキュリティ管理策ベースライン		
			低	中	高
SR-1	**ポリシーおよび手順**		x	x	x
SR-2	**サプライチェーンのリスクマネジメント計画**		x	x	x
SR-2(1)	SCRMチームの確立		x	x	x
SR-3	**サプライチェーンの管理策およびプロセス**		x	x	x
SR-3(1)	多様な供給ベース				
SR-3(2)	損害の限定				
SR-3(3)	下層フローダウン				
SR-4	**来歴**				
SR-4(1)	同一性				
SR-4(2)	追跡および痕跡				
SR-4(3)	本物であり、改変されていないことの確認				
SR-4(4)	サプライチェーンの完全性 － 系譜				
SR-5	**取得戦略、ツール、および方法**		x	x	x
SR-5(1)	適切な供給				
SR-5(2)	選択、受領、変更、または更新前のアセスメント				
SR-6	**サプライヤーのアセスメントおよびレビュー**			x	x
SR-6(1)	テストおよび分析				
SR-7	**サプライチェーン運用セキュリティ**				
SR-8	**通知協定**		x	x	x
SR-9	**耐タンパー性および検出**				x
SR-9(1)	システム開発ライフサイクルの複数の段階				x
SR-10	**システムまたはコンポーネントの検査**		x	x	x
SR-11	**コンポーネントの真正性**		x	x	x
SR-11(1)	偽造防止トレーニング		x	x	x
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		x	x	x
SR-11(3)	偽造防止の精査				
SR-12	**コンポーネントの廃棄**		x	x	x

参照資料

法律、ポリシー、指示、基準、ガイドライン、および内部報告書

法律	
[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
[44 USC 3552]	Title 44 U.S. Code, Sec. 3552, Definitions. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapII-sec3552
ポリシーおよび指示	
[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
[CNSSP 22]	Committee on National Security Systems Policy No. 22, *Cybersecurity Risk Management Policy*, August 2016. https://www.cnss.gov/CNSS/issuances/Policies.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
[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/a130revised.pdf
基準、ガイドライン、および内部報告書	
[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

[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 800-30] 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 800-37] 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 800-53] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53r5

[SP 800-59] Barker W (2003) Guideline for Identifying an Information System as a National Security System. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-59. https://doi.org/10.6028/NIST.SP.800-59

[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 800-82] 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

[IR 8011v1] 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 (NISTIR) 8011, Volume 1. https://doi.org/10.6028/NIST.IR.8011-1

[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

その他の出版物およびウェブサイト

[DSB 2017] Department of Defense, Defense Science Board (2017) *Task Force on Cyber Deterrence* (Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington, DC). https://dsb.cto.mil/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf

[NIST CSRC] National Institute of Standards and Technology (2020) *Computer Security Resource Center (CSRC).* https://csrc.nist.gov

[SCOR] National Institute of Standards and Technology (2020) *Security Control Overlay Repository (SCOR)*. https://csrc.nist.gov/projects/risk-management/scor

付属書 A

用語集

一般的な用語と定義

付属書 A は、NIST 特別出版物（SP）800-53B 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 SP800-53B である。

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。
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)	[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。
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、その他の組織、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。
ケイパビリティ (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。
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。

代替管理策 (compensating controls)	NIST 特別出版物（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。
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。
管理策ベースライン (control baseline) [FIPS 200, Adapted]	低影響度、中影響度、または高影響度システムのために規定された、または、プライバシー選択基準に基づいて選択された、テーラリングプロセスの始点を提供する一連のセキュリティおよびプライバシー管理策。
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。
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。
高影響度システム (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 の潜在的な影響度「高」の値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。
影響度 (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。
影響値 (impact value) [FIPS 199]	情報の機密性、完全性、または可用性の危殆化から生じる可能性のある、最悪の場合をアセスメントした潜在的影響度。「低」、「中」、「高」の値として表される。
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。

情報システム (information system) [OMB A-130]	情報の収集、処理、維持、使用、共有、配布、または廃棄のために編成された情報リソースの個別のセット。
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。
低影響度システム (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 の潜在的な影響度「低」の値が設定されているシステム。
中影響度システム (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 の潜在的影響度「中」の値が設定され、潜在的な影響度「高」の値が設定されているセキュリティ目的がないシステム。
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。
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。
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。
個人情報 (personally identifiable	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

information) [OMB A-130]	するために使用できる情報。
潜在的影響度 (potential impact) [FIPS 199]	機密性、完全性、または可用性が失われることにより、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。
プライバシー管理策 (privacy control) [OMB A-130]	適用されるプライバシー要件へのコンプライアンスを確保し、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。
取扱い (processing) [IR 8062]	PII に対して実行される操作または一連の操作。PII 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。
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悪影響または損害の大きさ；および (ii) 発生の可能性。
リスクアセスメント (risk assessment) [SP 800-39]	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の一部には、脅威および脆弱性の分析、ならびに情報処理から生じるプライバシーの問題の分析が組み込まれ、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。
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な影響度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]	低影響度、中影響度、または高影響度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。
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コンプライアンス；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。
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、メンテナンスに責任を持つ担当者。
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。
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)	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、代替管理策の選択、組織が定める管理策パラメータへの特定の値の設定、追加の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によって、セキュリティおよびプライバシー管理策ベースラインが変更されるプロセス。

付属書 B

略語

一般的な略語

CIO	Chief Information Officer （最高情報責任者）
CISO	Chief Information Security Officer （最高情報セキュリティ責任者）
CNSS	Committee on National Security Systems （国家安全保障システム委員会）
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）
CSRC	Computer Security Resource Center （コンピュータ・セキュリティ・リソース・センター）
DoD	Department of Defense （国防総省）
DoDI	Department of Defense Instruction （国防総省指示）
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）
FOIA	Freedom of Information Act （情報公開法）
IT	Information Technology （情報技術）
ITL	Information Technology Laboratory （情報技術研究所）
JTF	Joint Task Force （ジョイントタスクフォース）
MOD	Moderate （中）
NIST	National Institute of Standards and Technology （国立標準技術研究所）
OIRA	Office of Information and Regulatory Affairs （情報・規制業務室）
O/S	Organization or Information System （組織または情報システム）

OMB Office of Management and Budget
（行政管理予算局）

PII Personally Identifiable Information
（個人情報）

RMF Risk Management Framework
（リスクマネジメントフレームワーク）

SAOP Senior Agency Official for Privacy
（政府機関のプライバシー保護責任者）

SCOR Security Control Overlay Repository
（セキュリティ管理策オーバーレイリポジトリ）

SP Special Publication
（特別出版物）

付属書 C

オーバーレイ

管理策ベースラインをさらにカスタマイズするオプション

特定の状況では、組織がテーラリングガイダンスを適用して、関心のある特定のコミュニティのために一連の管理策を策定することや、特別な要件、実装技術、または固有のミッションや運用環境に対応することが有益な場合がある。組織は、(1)クラウドベースのサービスを調達または実装する組織に適用できるクラウドベースのサービス、(2)発電や送電、または施設内の環境システムの制御を行う産業用制御システム、(3)国家機密情報を処理、保存、または伝送するシステム、もしくは、(4)輸送システムの安全性を制御するシステムなどの、特定のアプリケーションまたはユースケースのために一連の管理策を定めることを決定してもよい。こうした事例では、特定の分野、技術領域、固有の状況、または環境ごとにオーバーレイを策定し、関心のある大規模なコミュニティに普及させることができるため、標準化されたセキュリティおよびプライバシーのケイパビリティ、一貫した管理策の実装、費用対効果の高いセキュリティおよびプライバシーソリューションが実現される。

*オーバーレイ*という概念は、関心のあるコミュニティ、システム、および組織向けの特別な一連の管理策の必要性に対応するために導入された。オーバーレイは、管理策ベースライン[38][39]にテーラリングガイダンスを適用して導出される完全に指定された一連の管理策、拡張管理策、およびその他の補足情報(パラメータ値など)であってもよく、管理策ベースラインから独立して導出されてもよい[40]。オーバーレイは、以下により、関心のあるコミュニティ内の複数のシステムに適用され管理策ベースラインを補完してさらに改良するために策定される。

- 関心のあるコミュニティが管理策を追加、変更、または削除する機会を提供する。
- 特定の技術、コンピューティングパラダイム、運用環境、システムのタイプ、ミッション／運用のタイプ、運用モード、産業分野、および法的／規則要件に対して管理策の適用性と解釈を提供する。
- 管理策および拡張管理策の設定および選択操作において、関心のあるコミュニティが同意できるパラメータ値を定める。

組織は、初期の管理策ベースラインの作成に使用される基本的な前提事項から相違がある場合や、特定の技術の保護や特定の脅威への対応に特定の管理策が必要な場合に、オーバーレイの概念を使用する。管理策の実装が、オーバーレイが適用される各システム、システムコンポーネント、および運用環境のセキュリティおよびプライバシーの要件を的確に反映できるようにするには、第 3 章で説明されているテーラリングがオーバーレイに必要な場合がある。オーバーレイの概念は、類似した技術、システム、または関心のあるコミュニティのグループに適用できる(すなわち、テーラリングプロセスは個々のシステムに対して管理策ベースラインを適合させるために使用されるが、オーバーレイの概念は個々のシステムには適していない)。

---

[38] [SP 800-82]は、産業用制御システム向けの完全に指定された一連の管理策を含むオーバーレイの例を示している。また、オーバーレイには、特定のコミュニティのニーズに対応し、管理策ベースラインを補完する、関連する一連の管理策を含めることができる。

[39] 管理策ベースラインには、第 3 章の連邦政府ベースライン;州政府、地方自治体、部族政府によって策定されたベースライン;または民間組織(例えば、製造業者、コンソーシアム、業界団体、産業界、および重要インフラ分野)によって策定されたベースラインを含むことができる。

[40] ベースラインに依存しないオーバーレイは、多くの場合、非常に特定の事情(国家機密情報の保護など)、状況および／または条件に対応する。

上記の領域をサポートするオーバーレイを策定するための体系的なアプローチを提供するために、組織は、幅広いテーラリング活動を採用することができる。オーバーレイは、特定の事情、状況、または条件に対して幅広いサポートを持つシステムおよび組織のために、関心のあるコミュニティ全体で合意が築かれ、セキュリティおよびプライバシー計画を策定する機会を提供する。オーバーレイが有用なカテゴリには以下が含まれる。

- 医療、法執行機関、インテリジェンス、金融、製造、輸送、エネルギー、および同業種の連携または共有などの、関心のあるコミュニティ、産業分野、連合体、またはパートナーシップ
- 仮想システム、クラウド、モバイル、スマートグリッド、およびクロスドメインソリューションなどの、情報技術とコンピューティングパラダイム
- 宇宙、戦術、または海洋などの運用環境
- 産業用制御システム、プロセス制御システム、武器システム、シングルユーザーシステム、スタンドアロンシステム、IoT デバイス、センサーなどの、システムおよび動作モードのタイプ
- テロ対策、初期対応者（first responders）、研究、開発、テスト、評価などのミッションまたは運用のタイプ
- 持続的標的型攻撃やインサイダー脅威などの、脅威のタイプ
- 外国情報監視法（Foreign Intelligence Surveillance Act）、医療保険の相互運用性と説明責任に関する法律（Health Insurance Portability and Accountability Act）、FISMA、プライバシー法（Privacy Act）などの、法的または規則要件

オーバーレイは、セキュリティおよびプライバシーの専門家や他の特定分野の専門家によって策定されたテーラリングのオプションを、システムの実装とメンテナンスを担当するシステムオーナーに提示することで、管理策の選択において統一性と効率性をもたらす。オーバーレイの策定者が求める特殊性に応じて、オーバーレイを構築する際には多くのオプションを使用することができる。一部のオーバーレイは、対象となるシステムタイプの主要コンポーネントを形成するハードウェア、ファームウェア、およびソフトウェア、ならびにシステムが動作する環境に関して非常に特定的であってもよい。その他のオーバーレイは、異なる運用環境に展開されてもよい、より広いシステムクラスに適用できるように、より抽象的であってもよい。

オーバーレイの公開

オーバーレイは、OMB ポリシー、CNSS 指示、NIST 出版物、業界基準、および分野固有のガイダンスを含む様々な立場や出版物で独立して公開することができる。セキュリティ管理策オーバーレイリポジトリ（SCOR：Security Control Overlay Repository）は、セキュリティ管理策のオーバーレイを自主的に共有するためのプラットフォームを利害関係者に提供している。オーバーレイの提出方法など、リポジトリの詳細を知るには、また、公開されたオーバーレイのリストを入手するには、[SCOR]を参照のこと。

組織はオーバーレイを策定する際に以下のアウトラインを使用してもよい[41]。アウトラインは例としてのみ提供されている。組織は、特定の組織のニーズと策定中のオーバーレイのタイプに基づいて、任意の形式を使用してもよい。オーバーレイに含まれる詳細さの度合いは、オーバーレイを策定する関心のある組織またはコミュニティの裁量によるが、オーバーレイ策定プロセス中になされたリスクベースの決定を含め、オーバーレイに対する適切な正当性と根拠を提供するよう十分な幅と深度であることが望ましい。オーバーレイの例示的なアウトラインには、以下のセクションが含まれる。

- 識別
- オーバーレイの特徴
- 適用性
- オーバーレイの概要
- オーバーレイによる管理策仕様
- テーラリングの考慮事項
- 用語と定義
- 追加情報または指示

識別

組織は、オーバーレイの一意の名称、版数と日付、オーバーレイの作成に使用された[SP 800-53]の版数、オーバーレイの作成に使用されたその他のドキュメント、作成者または作成グループと連絡先、および、組織による承認のタイプを提供することで、オーバーレイを識別する。組織は、オーバーレイが有効である期間と、[SP 800-53]や組織固有のガイダンスへの変更以外でオーバーレイの更新を引き起こすイベントを規定する。オーバーレイの更新を引き起こすことができる固有のイベントがない場合は、識別セクションにその旨を記載する。

オーバーレイの特徴

組織は、潜在的な利用者が各自のミッションまたは事業機能に最適なオーバーレイを選択できるように、以下のようなオーバーレイの使用目的を規定する特徴を記載する。

- システム、システムコンポーネント、または技術が使用または運用される、オーバーレイの対象となる物理的環境の説明（例えば、米国本土内の警備された建物の中、無人宇宙船の中、機微情報や国家機密情報へのアクセスを試みることで知られる外国への出張中、または敵対的なエンティティ付近の移動車両内）
- システム、システムコンポーネント、または技術によって処理、保存、または伝送される、オーバーレイの対象となる情報のタイプ（例えば、個人のアイデンティティ情報と認証情報；財務管理情報；施設、艦隊、装置の管理情報；防衛および国家安全保障情報;システム開発情報）
- 対象となるシステム、システムコンポーネント、または技術の機能性、もしくはシステムのタイプ（例えば、スタンドアロンシステム、産業用制御システム、プロセス制御システム、

[41] 組織はオーバーレイの概念を使用することが奨励されているが、同じトピックに対して著しくかけ離れたオーバーレイの策定は逆効果であることが判明する場合がある。オーバーレイの概念は、関心のあるコミュニティが連携して、合意に基づいた重複していないオーバーレイを作成する場合に最も効果的である。

クロスドメインシステム）

- 第 2.3 節に記載される前提事項では対応できない特定の脅威から組織のミッションや事業機能、システム、情報、または個人を保護することを目的とするオーバーレイに関連するその他の特徴

適用性

組織は、オーバーレイの利用者が、オーバーレイが特定のシステム、システムコンポーネント、技術、または運用環境に適用されるかどうかを判定する際に役立つ基準を提供する。典型的なフォーマットには、オーバーレイの対象（関連するアプリケーションを含む）と、その運用環境の特徴の記述に基づいた、オーバーレイに適した詳細レベルの質問一覧またはデシジョンツリーを含んでもよい。

オーバーレイの概要

組織は、オーバーレイの特徴について簡単な概要を提供する。概要には、(1)オーバーレイの影響を受ける管理策と拡張管理策、(2)オーバーレイの特定の特徴と前提事項に基づいて、どの管理策および拡張管理策が選択されるか、または選択されないかについての表示(3)第 2.4 節で提供されるテーラリングガイダンスまたは組織固有のガイダンス、(4)パラメータ値を含む、選択した管理策と拡張管理策、(5)適用される法律、大統領令、指令、指示、規則、ポリシー、または基準への参照、を含んでもよい。

オーバーレイによる管理策仕様

組織は、テーラリングプロセスの一部としてオーバーレイの管理策と拡張管理策の包括的な表現を提供する。これには、(1)特定の管理策または拡張管理策を選択する、または選択しないことの正当性、(2)オーバーレイの特徴とオーバーレイの使用が意図される環境を含めるように、管理策の詳解セクションへの変更、(3)管理策の選択または設定操作における固有のパラメータ値、(4)管理策または拡張管理策によって満たされる特定の法的または規則要件（FISMA に加えて）、(5)必要に応じて、代替管理策の推奨、(6)追加の機能性を規定、メカニズムの強度を変更、もしくは実装オプションを追加または制限することによって、管理策または拡張管理策のケイパビリティを拡張するガイダンス、を含んでもよい。

テーラリングの考慮事項

組織は、特定のシステム、システムコンポーネント、または技術に適用される一連の管理策および拡張管理策を判定する際に、テーラリングプロセス中に考慮すべき情報をシステムオーナーおよび認可権限のある担当者に提供する。これは、第 3 章の管理策ベースラインが前提とする運用環境とは異なる環境で使用されるオーバーレイに特に重要である。さらに、組織は、ベースラインの管理策とオーバーレイ仕様との間で生じる場合がある不一致に対応するために、管理策ベースラインに適用される複数のオーバーレイの使用に関するガイダンスを提供することができる。

用語と定義

組織は、オーバーレイに関する固有の用語と定義を提供する。オーバーレイに固有の用語または定義がない場合は、その旨をこのセクションに記載する。

追加情報または指示

組織は、これより前のセクションで取り上げられていないオーバーレイに関連する追加情報または指示を提供する。