NIST Special Publication 800-37
Revision 2

情報システム及び組織のための リスクマネジメントフレームワーク

セキュリティ及びプライバシーのための システムライフサイクルアプローチ

本出版物には、リスクマネジメントフレームワーク（RMF：Risk Management Framework）に対する包括的な更新が含まれている。この更新には、NIST サイバーセキュリティフレームワークの構成要素との整合、プライバシーリスクマネジメントプロセスの統合、システムライフサイクルのセキュリティエンジニアリングプロセスとの整合、サプライチェーンのリスクマネジメントプロセスの取り込みが含まれる。組織は、RMF の中でフレームワーク及びプロセスを補完的な方法で使用し、組織の運営、組織の資産、個人、他の組織、及び国家に対するセキュリティ及びプライバシーリスクを効果的に管理できる。改訂第 2 版には、情報システム所有者がシステムレベルでのリスクマネジメント活動実施のための準備をすることを目的とした、一連の組織全体の RMF タスクが含まれている。その目的は、組織のミッション及びビジネス機能との密接なつながりを確立し、上級幹部、マネージャ、及び運用担当者のコミュニケーションを改善することで、RMF の有効性、効率性、及び費用対効果を高めることである。

ジョイントタスクフォース

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

NIST Special Publication 800-37
Revision 2

情報システム及び組織のための リスクマネジメントフレームワーク

セキュリティ及びプライバシーのための システムライフサイクルアプローチ

ジョイントタスクフォース

本出版物は、https://doi.org/10.6028/NIST.SP.800-37r2 から無料で入手可能である。

2018 年 12 月

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、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）が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、及び公法（P.L.：Public Law）113 条 −283 条に基づく法的責任を果たすために策定したものである。NIST は、連邦政府情報システムに対する最低限の要件を含んだ情報セキュリティ標準及びガイドラインを策定する責務を負う。そうした標準及びガイドラインは、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標準及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（OMB Director）、又はその他の連邦政府担当官の既存の権限を変更するもの、又はそれらに代わるものと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）800−37 改訂第 2 版
NIST SP 800−37、Rev. 2、**全 183 ページ**（2018 年 12 月）CODEN：NSPUE2

本出版物は、https://doi.org/10.6028/NIST.SP.800-37r2 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、機器、又は資料が記載されている場合がある。そうした記載は、NIST による推奨又は承認を意図するものではなく、それらのエンティティ、機器、又は資料が、必ずしも目的のために利用できる最良の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。概念、プラクティス、及び方法論を含む本出版物に記載された情報は、そのような関連出版物の完成前であっても、連邦政府機関によって使用されることがある。したがって、各出版物が完成するまでの間、現行の要件、ガイドライン、及び手順が存在する場合は、それらは引き続き有効である。計画の策定及び移行のために、連邦政府機関は、NIST によるそうした新たな出版物策定の進展を綿密に追うことが望まれる。

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

本出版物に対する意見の送付先：

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 ： Freedom of Information Act） [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、米国の計量と標準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、及び技術分析を開発し、情報技術（IT）の開発と生産的利用を促進している。ITL の責務には、連邦政府情報システムにおける国家安全保障関連情報以外の情報を対象とした、費用対効果の高いセキュリティのための管理、運用、技術、及び物理的な標準とガイドラインを策定することが含まれる。SP 800 シリーズでは、情報システムセキュリティ及びプライバシーに関する ITL の研究、ガイドライン、及び普及の取り組み、並びに産業界、政府、及び学術機関との共同活動について報告している。

概要

本出版物は、リスクマネジメントフレームワーク（RMF）について説明し、情報システム及び組織への RMF の適用に関するガイドラインを提供する。RMF は、セキュリティ及びプライバシーのリスクを管理するための、統制がとれ、構造化された、柔軟なプロセスを提供する。このプロセスには、情報セキュリティの分類化、管理策の選択、実装及びアセスメント、システム及び共通管理策の認可、継続的監視が含まれる。RMF には、組織がこのフレームワークを適切なリスクマネジメントレベルで実行するための準備活動が含まれている。また、RMF は、継続的監視プロセスの実装を通じて、ほぼリアルタイムのリスクマネジメント、並びに、情報システム及び共通管理策の認可を継続的に促進し、ミッション及びビジネスファンクション（ビジネス機能）を支えるシステムについて、リスクマネジメント関連の効率的かつ費用対効果の高い決定を行うために、必要な情報を上級幹部及び管理職に提供し、セキュリティ及びプライバシーをシステム開発ライフサイクルに取り入れている。RMF のタスクを実施することで、システムレベルでの極めて重要なリスクマネジメントプロセスが、組織レベルでのリスクマネジメントプロセスと関連付けられる。さらに、組織の情報システム内に実装され、それらのシステムによって継承される管理策に対する責任と説明責任を確立する。

キーワード

アセスメント、運用認可、使用認可、認可権限のある担当者、分類、共通管理策、共通管理策の認可、共通管理策の提供者、継続的監視、管理策アセッサー、管理策ベースライン、サイバーセキュリティフレームワークプロファイル、ハイブリッド管理策、情報所有者又は情報管理者、情報セキュリティ、監視、継続的認可、実施計画及びマイルストーン、プライバシー、プライバシーアセスメント報告書、プライバシー管理策、プライバシー計画、プライバシーリスク、リスクアセスメント、リスク管理者機能、リスクマネジメント、リスクマネジメントフレームワーク、セキュリティ、セキュリティアセスメント報告書、セキュリティ管理策、セキュリティエンジニアリング、セキュリティ計画、セキュリティリスク、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、サプライチェーンのリスクマネジメント、システム開発ライフサイクル、システム所有者、システムプライバシー責任者、システムセキュリティ責任者、システム固有管理策

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）、及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、並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

Essye B. Miller
Principal Deputy CIO and DoD Senior Information Security Officer

Thomas P. Michelli
Acting Deputy Chief Information Officer for Cybersecurity Information Security Officer

Vicki Michetti
Director, Cybersecurity Policy, Strategy, International, and Defense Industrial Base Directorate

国家情報長官室

John Sherman
Chief Information Officer

Vacant
Deputy Chief Information Officer

Susan Dorr
Director, Cybersecurity Division and Chief

Wallace Coggins
Director, Security Coordination Center

米国国立標準技術研究所

Charles H. Romine
Director, Information Technology Laboratory

Donna Dodson
Cybersecurity Advisor, Information Technology Laboratory

Matt 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

Thomas Michelli
Chair–Defense Community

Susan Dorr–Intelligence Community
Co-Chair

Vicki Michetti
Tri-Chair–Defense Community

Chris Johnson
Tri-Chair–Intelligence Community

Paul Cunningham
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

Ron Ross *NIST, JTF Leader*	Kevin Dulany *DoD*	Peter Duspiva *Intelligence Community*	Kelley Dempsey *NIST*
Taylor Roberts *OMB*	Ellen Nadeau *NIST*	Victoria Pillitteri *NIST*	Naomi Lefkovitz *NIST*
Jordan Burris *OMB*	Charles Cutshall *OMB*	Kevin Herms *OMB*	Carol Bales *OMB*
Jeff Marron *NIST*	Kaitlin Boeckl *NIST*	Kirsten Moncada *OMB*	Jon Boyens *NIST*
Dorian Pappas *CNSS*	Dominic Cussatt *Veterans Affairs*	Esten Porter *The MITRE Corporation*	Celia Paulsen *NIST*
Daniel Faigin *The Aerospace Corporation*	Christina Sames *The MITRE Corporation*	Julie Snyder *The MITRE Corporation*	Martin Stanley *Homeland Security*

また、本出版物の内容の改善において多大なる貢献をいただいた Matt Barrett、Kathleen Coupe、Jeff Eisensmith、Chris Enloe、Ned Goren、Matthew Halstead、Jody Jacobs、Ralph Jones、Martin Kihiko、Raquel Leone の各氏、並びに、コンピュータセキュリティ部門（Computer Security Division）及び応用サイバーセキュリティ部門（Applied Cybersecurity Division）の科学者、エンジニア、研究スタッフにも感謝の意を表したい。特に Jim Foti 氏と NIST ウェブチームの優れた管理上のサポートに対しては、心から感謝する。

さらに、今回の RMF の 更新における新たなアイデアのいくつかについてインスピレーションを与えてくれた、米国空軍（United States Air Force）及び空軍サイバーワークス（Air Force CyberWorx）によって推進される「RMF ネクスト（RMF Next）」イニシアチブに感謝したい。Lauren Knausenberger、Bill Bryant、及び Venice Goodwine の各 氏が率いるワーキンググループには、政府及び業界の代表として、Jake Ames、Chris Bailey、James Barnett、Steve Bogue、Wes Chiu、Kurt Danis、Shane Deichman、Joe Erskine、Terence Goodman、Jason Howe、Brandon Howell、Todd Jacobs、Peter Klabe、William Kramer、Bryon Kroger、Kevin LaSalle、Dinh Le、Noam Liran、Sam Miles、Michael Morrison、Raymond Tom Nagley、Wendy Nather、Jasmine Neal、Ryan Perry、Eugene Peterson、Lawrence Rampaul、Jessica Rheinschmidt、Greg Roman、Susanna Scarveles、Justin Schoenthal、Christian Sorenson、Stacy Studstill、Charles Wade、Shawn Whitney、David Wilcox、Thomas Woodring の各氏が参加していた。

最後に、国内外の公共及び民間分野の個人及び組織からの多大なる貢献にも心から感謝する。彼らの思慮深く建設的な意見は、本出版物の全体的な品質、網羅性、及び有用性を向上させた。

NIST SP 800-37 への過去の貢献者

2005 年当初より、SP 800-37 の過去の各版に貢献いただいた Marshall Abrams、William Barker、Beckie Koonge、Roger Caslow、John Gilligan、Peter Gouldmann、Richard Graubart、John Grimes、Gus Guissanie、Priscilla Guthrie、Jennifer Fabius、Cita Furlani、Richard Hale、Peggy Himes、William Hunteman、Arnold Johnson、Donald Jones、Stuart Katzke、Eustace King、Mark Morrison、Sherrill Nicely、Karen Quigg、George Rogers、Cheryl Roby、Gary Stoneburner、Marianne Swanson、Glenda Turner、及び Peter Williams 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。

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相互接続された複雑な世界が構築されるなか、セキュリティ及びプライバシーのリスク（サプライチェーンリスクを含む）は国民的な議論の大きな部分を占め、非常に重要なトピックであり続けている。公共及び民間分野（米国の重要インフラを含む）内のハードウェア、ソフトウェア、ファームウェア、システムの複雑さが著しく高まっているということは、敵対者が悪用できる攻撃対象領域が大幅に増加していることを意味している。さらに敵対者は、システムの侵入、システム要素の完全性の侵害、重要資産へのアクセス権の取得を行うための攻撃ベクトル及び効果的な手段として、サプライチェーンを利用している。

国防科学評議委員会（Defense Science Board）のレポート「*レジリエントな軍事システム及び高度なサイバー脅威（Resilient Military Systems and the Advanced Cyber Threat）*」[DSB 2013]は、米国政府、米国の重要インフラ、並びに、公共及び民間分野のミッションに不可欠な業務と資産を支えているシステムの脆弱性に関して、厳しいアセスメントを実施している。

> *「…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いるため、少なくとも今後 10 年間、米国は最も有能な米国の敵対者がもたらす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私たちが依存している、根幹をなす情報システム、コンポーネント製品、及びサービスをさらに強化すること－それらのシステム、製品、及びサービスがシステム開発ライフサイクル（SDLC）全体を通じて十分な統合的信頼性を持ち、米国の経済及び国家安全保障上の利益を支えるために必要なレジリエンスを提供できるようにすること－が急務である。システムの近代化、自動化の利用拡大、並びに、連邦政府のシステム及びネットワークの統合、標準化、最適化によって高価値資産の保護を強化すること[OMB M-19-03]が、連邦政府にとって重要な目的である。

大統領令（E.O.：Executive Order）13800 号「*連邦政府のネットワーク及び重要インフラのサイバーセキュリティ強化（Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure）*」[EO 13800]は、連邦政府情報システムの相互接続性の高まりを認識しており、連邦政府機関の事業体のみならず行政府全体に対しても適切なリスクマネジメントを確実に行うよう、各政府機関の長に求めている。この大統領令では以下のように述べられている。

> *「…行政府は米国民のために情報技術（IT）を運用している。その IT 及びデータは、米国政府の持てるすべてのケイパビリティ（能力）を用いて、責任を持ってセキュアにすることが望ましい…」*
>
> *「…サイバーセキュリティリスクマネジメントは、不正アクセス及びその他のサイバー脅威からの IT 及びデータの防御、サイバー脅威に対する認識の維持、IT 及びデータに悪影響をもたらす異常及びインシデントの検知、並びに、インシデントのインパクト軽減、対応、インシデントからの復旧のために実施される、あらゆる活動からなる…」*

行政管理予算局（OMB：Office of Management and Budget）による覚書（Memorandum）M-17-25「*連邦政府のネットワーク及び重要インフラのサイバーセキュリティ強化に関する大統領令の報告ガイダンス（Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure）*」[OMB M-17-25]は、連邦政府機関に対して E.O. 13800 の実装ガイダンスを提供している。この覚書では以下のように述べられている。

> *「…効果的なエンタープライズリスクマネジメントプログラムは、政府機関のミッション及び国民へのサービス提供にインパクトを与え得る潜在的なリスクの認識し、説明するための共通の理解を促進する。このようなリスクには、戦略的リスク、市場リスク、サイバーリスク、法務リスク、資本リ*

スク、風評リスク、政治的リスク、及び運営上の様々なリスク(例えば情報セキュリティリスク、人的資本リスク、ビジネス継続リスク、関連リスクなど)が含まれるが、これらに限定されない…」

「… サイバーセキュリティリスクを効果的にマネジメントするためには、政府機関は情報セキュリティマネジメントプロセスを、戦略プロセス、業務プロセス、及び予算計画プロセスと連携させる必要がある…」

OMB による通達(Circular)A-130「*戦略的リソースとしての情報の管理(Managing Information as a Strategic Resource)*」[OMB A-130]は、連邦政府の情報リソースの保護、及び個人情報(PII)の管理に対する責任を扱っている。Circular A-130 では、本ガイドラインに記述されている RMF を実装すること、及び、プライバシーを RMF プロセスに統合することを政府機関に求めている。この OMB 通達は、情報セキュリティプログラム及びプライバシープログラムの要件を規定する際に、両プログラムが共有された目的に向けて協力することの必要性を以下のように強調している。

「セキュリティ及びプライバシーは独立した別個の分野であるが、両者は密接に関連しており、そのため政府機関は、セキュリティ及びプライバシーのリスクの識別及び管理、並びに、適用可能な要件を順守するために協調的なアプローチをとることが不可欠である….」

NIST Special Publication 800-37 の今回の更新(Revision 2)は、情報システム、組織、及び個人のための次世代型リスクマネジメントフレームワーク(RMF)を策定するという、国防科学評議委員会、大統領令、及び OMB ポリシーの覚書の要求に応えたものである。

今回の更新の主な目的は以下の 7 つである。

- 組織の経営幹部レベル又はガバナンスレベルでのリスクマネジメントプロセス及びリスクマネジメント活動と、組織のシステム及び運用レベルでの個人、プロセス、及び活動との間のより緊密な連携とコミュニケーションを提供すること。
- 重要なリスクマネジメント準備活動をすべてのリスクマネジメントレベルで制度化し、より効果的、効率的、及び費用対効果の高い RMF の実行を促進すること。
- NIST サイバーセキュリティフレームワーク[NIST CSF]を RMF と整合させ、確立された NIST リスクマネジメントプロセスを使用して実装する方法を示すこと。
- プライバシープログラムが責任を負うプライバシー保護のニーズをより適切にサポートするために、プライバシーリスクマネジメントプロセスを RMF に統合すること。
- NIST Special Publication 800-160, Volume 1[SP 800-160 v1]の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と、RMF の関連タスクと整合させることで、統合的信頼性のあるセキュアなソフトウェア及びシステムの開発を促進すること。
- SDLC 全体にわたって、統合的信頼性のないサプライヤ、偽造品の混入、改ざん、無許可生産、窃盗、悪意のあるコードの挿入、及び粗末な製造プラクティス及び開発プラクティスに対処するために、セキュリティ関連のサプライチェーンのリスクマネジメント(SCRM)の概念を RMF に統合すること。
- 従来のベースライン管理策選択アプローチを補完し、NIST Special Publication 800-53, Revision 5 の包括的な管理策カタログの使用をサポートするために、組織によって作成される管理策選択アプローチを可能にすること。

*準備*ステップの追加は、RMF への重要な変更点の 1 つで、より効果的、効率的、かつ費用対効果の高いセキュリティ及びプライバシーのリスクマネジメントプロセスを実現するために取り入れられた。
組織レベル及びシステムレベルでの準備を制度化する主な目的は以下のとおりである。

- 組織レベル及びミッション／ビジネスプロセスレベルの上級幹部及び管理職と、運用レベルのシステム所有者の間の効果的なコミュニケーションを促進すること。
- 全組織的な共通管理策の特定作業と、組織的にテーラリングされた管理策ベースラインの策定を促進し、個々のシステム所有者の作業負荷と、システム開発及び資産保護のコストを軽減すること。
- 組織のシステム、アプリケーション、及びサービスを統合、最適化、標準化するためのエンタープライズアーキテクチャの概念とモデルを使用して、情報技術（IT）及び制御・運用技術（OT）のインフラストラクチャの複雑さを低減すること。
- セキュリティ及びプライバシーのリスクに対処していない不要な機能、並びに、セキュリティ及びプライバシーケイパビリティ（能力）を排除することで、システムの複雑さを低減すること。
- より高度なレベルの保護を必要とする組織の高価値資産（HVA）を特定し、優先順位を付け、リソースを集中させ、そのような資産に対するリスクに見合った対策をとること。

上記の目的を達成することで、組織は RMF の実行を**簡素化**し、リスクマネジメントのための**革新的**なアプローチを採用し、特定のタスクを実行する際の**自動化**レベルを高めることができる。RMF を実装する組織は、以下のことが可能になる。

- 組織内で一貫した出発点から RMF 実行を推進するために、組織レベル及びシステムレベルでの*準備*ステップのタスクとアウトプットを使用する。
- 標準化され、一貫性があり、費用対効果の高いセキュリティ及びプライバシーケイパビリティ（能力）の継承を推進するために、組織レベルで共通管理策を最大限に活用する。
- 組織全体で必要となる認可の数を削減するために、共有又はクラウドベースのシステム、サービス、及びアプリケーションを最大限に活用する。
- セキュリティ及びプライバシー計画の策定速度を上げ、セキュリティ及びプライバシー計画の内容の一貫性を高めるために、組織的にテーラリングされた管理策ベースラインを採用する。
- システムセキュリティエンジニアリングのプロセスで策定されたセキュリティ及びプライバシー要件に基づいて、組織で定義された管理策を採用する。
- セキュリティ分類化、管理策の選択／アセスメント／監視、及び認可プロセスを管理するために、自動化ツールを最大限に活用する。
- 低インパクトのシステムが、システム接続によってより高インパクトのシステムに悪影響を与える可能性がない場合には、低インパクトのシステムにかける労力とリソース関連支出のレベルを下げる。
- 標準化されたハードウェア／ソフトウェアの展開（構成設定を含む）において、RMF の成果物（例：セキュリティ及びプライバシーのアセスメント結果）を最大限に再利用する。
- 不要なシステム、システムコンポーネント、及びサービスを排除し、最小機能の原則を採用することで、IT/OT インフラストラクチャの複雑さを低減する。
- 継続的な認可への移行を優先事項とし、継続的な監視アプローチを使用してコストを削減し、セキュリティプログラム及びプライバシープログラムの効率を高める。

RMF の実行準備は組織によって異なる可能性があることを認識した上で上記の目的を達成することで、組織の全体的な IT/OT フットプリント及び攻撃対象領域を削減し、IT 近代化目標を推進し、リソースを節約し、最も重要な資産及びシステムに保護戦略を集中させるためのセキュリティ活動に優先順位を付け、個人のプライバシー保護を促進することができる。

セキュリティ及びプライバシーのリスクの共通基盤

NIST は標準及びガイドラインの策定において、連邦政府機関、州政府、地方自治体、部族政府、及び民間組織と協議し、不要でコストのかかる重複作業を回避し、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標準及びガイドラインを補完することを確実にしている。NIST は各出版物について透明性のあるパブリックレビュープロセスを実施することに加え、行政管理予算局、国家情報長官室、国防総省、及び国家安全保障システム委員会と協力し、連邦政府の統一されたリスクマネジメントフレームワークを確立してきた。この共通基盤は、組織の運営、組織の資産、個人、他の組織、及び国家に対するセキュリティ及び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と技術を、連邦政府の民間、防衛、情報機関及びその契約事業者に提供する。また、統一されたフレームワークは、アセスメント結果及び認可判断を相互に受け入れるための強固な基盤を提供し、情報の共有及び協力を促進する。NIST は、セキュリティとプライバシーに関する NIST の標準及びガイドラインと、外部の組織が作成した標準及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、公共団体及び民間団体と引き続き協力を続ける。

セキュリティ及びプライバシーのリスクの許容

リスクマネジメントフレームワークは、情報システムの観点と共通管理策の観点の 2 つの観点から、セキュリティ及びプライバシーのリスクに対処する。情報システムについては、組織の運営、組織の資産、個人、他の組織、及び国家に対するセキュリティ及びプライバシーのリスクを許容して、認可権限のある担当者がシステムの運用認可又は使用認可を発行する。共通管理策については、組織の運営、組織の資産、個人、他の組織、及び国家に対するセキュリティ及びプライバシーのリスクを許容して、認可権限のある担当者が、指定された組織システムから継承できる特定の管理策一式について共通管理策の認可を発行する。認可権限のある担当者は、システム認可の一環として、共通管理策の継承に伴うリスクも考慮する。認可の各種類については附属書 F で説明している。

RMF は技術的に中立

RMF は、その方法論をあらゆる種類の情報システム*に変更なしで適用できるように、技術的に中立である（特定の技術に依存しない）ことを意図して設計されている。選択する特定の管理策、管理策実装の詳細、管理策アセスメントの方法及び対象は IT リソースの種類の違いによって異なる可能性があるが、特定の技術に適応させるために RMF プロセスを調整する必要はない。

すべての情報システムは、何らかの種類の情報を処理、保存、又は伝送する。例えば、センサによって収集され監視局に伝送される、遠隔施設の温度情報、無線によって兵器システムのコントローラに伝送される位置座標、遠隔カメラ（地上／衛星）からサーバに伝送される画像、病院のネットワーク経由で患者情報を伝送する医療用 IT デバイスは保護が必要である。これらの情報は、情報を分類して損失のインパクトを判断し、情報の処理が個人のプライバシーにインパクトを与えるかどうかをアセスメントし、利用中の IT リソースに適用可能な管理策を選択及び実装することで保護できる。したがって、クラウドベースのシステム、産業用／プロセス制御システム、兵器システム、サイバーフィジカルシステム、アプリケーション、IoT デバイス、モバイルデバイス／システムには、個別のリスクマネジメントプロセスは必要ではなく、むしろ、既存の RMF プロセスを適用することで特定される、テーラリングされた管理策一式及び具体的な実装詳細が必要である。

RMF は、あらゆる種類のシステム開発アプローチ（アジャイル及び DevOps アプローチを含む）のシステム開発ライフサイクル中に、必要に応じて繰り返し適用される。セキュリティ及びプライバシーの要件及び管理策は、ライフサイクル全体を通じて、開発の進捗に合わせて実装、検証、妥当性確認される。この柔軟性により、RMF は、システム及びシステムコンポーネントの開発において迅速な技術サイクル、イノベーション、及び現時点でのベストプラクティスの使用をサポートできる。

***注**：本出版物は情報システムに関するものである。情報システムとは、デジタル形式か非デジタル形式かにかかわらず、情報の収集、処理、維持、使用、共有、配布、又は廃棄のために体系化された個別の一連の情報リソースである。情報リソースには、情報及び人員、機器、資金、情報技術などの関連リソースが含まれる。したがって、情報システムにはハードウェア、ファームウェア、及びソフトウェアが含まれる場合と含まれない場合がある。

RMF の実行における自動化の利用

組織は、リスクマネジメントフレームワーク（RMF）の各ステップを実施する際のスピード、有効性、及び効率性を高めるために、可能な限り*自動化*を最大限に活用することが望ましい。自動化は、管理策のアセスメント及び継続的監視、タイムリーな意思決定のための認可パッケージの準備、及び継続的認可アプローチの実装において特に有用であり、これらが合わさって、上級幹部によるリアルタイム又はほぼリアルタイムでのリスクベースの意思決定プロセスが促進される。組織は、セキュリティプログラム及びプライバシープログラムにおいて自動化又は自動化されたサポートツールをいつ、どこで、どのように使用するか決定する上で、大きな柔軟性を持っている。状況によっては、管理策の自動アセスメント及び自動監視が不可能又は実行できない可能性がある。

適用範囲及び適用性

本出版物の目的は、組織によるセキュリティ及びプライバシーのリスク管理を促進すること、及び、数ある法律、規制、ポリシーの中でも特に 2014 年の連邦政府情報セキュリティ近代化法（FISMA：Federal Information Security Modernization Act）、1974 年のプライバシー法（Privacy Act）、OMB ポリシー、及び連邦情報処理標準（FIPS：Federal Information Processing Standards）の要件を満たすことである。本出版物の適用範囲は、連邦政府情報システムに関連している。情報システムとは、デジタル形式か非デジタル形式かにかかわらず、情報の収集、処理、維持、使用、共有、配布、又は廃棄のために体系化された個別の一連の情報リソースである。情報リソースには、情報及び人員、機器、資金、情報技術などの関連リソースが含まれる。

RMF は連邦政府での使用が義務付けられているが、あらゆる種類の非連邦政府組織（例：企業、業界、学界）に適用することができる。したがって、州政府、地方自治体、部族政府、及び民間組織は、これらのガイドラインを自主的に必要に応じて利用することが推奨される。さらに、サイバーセキュリティフレームワークを採用及び実装した非連邦政府組織は、そのフレームワークを実行するためのリスクマネジメントプロセスとして、管理策の実装、アセスメント、及び監視、並びに、（リスクベースの意思決定のための）システム認可に不可欠なタスクを規定している RMF を使用することに価値を見出す可能性がある。

リスクの管理

サイバーセキュリティフレームワークの利用

大統領令（E.O）13800 号は、連邦政府機関に対して IT インフラストラクチャ及びシステムを近代化するよう求めており、連邦政府情報システム及びネットワークの相互接続性が高まっていることを認識している。この大統領令はまた、各政府機関の長に対し、*重要インフラのサイバーセキュリティを改善するためのフレームワーク（Framework for Improving Critical Infrastructure Cybersecurity）*（すなわち「サイバーセキュリティフレームワーク」）を使用して、政府機関レベル及び行政府全体でリスクを管理するよう求めている。そして最後に、この大統領令は、組織のサイバーセキュリティリスクを管理する責任及び説明責任を各政府機関の長に課すことで、2014 年の連邦政府情報セキュリティ近代化法（FISMA）を補強している。

サイバーセキュリティフレームワークには、幅広いサイバーセキュリティリスクマネジメントプロセスとともに使用できる柔軟かつリスクベースの実装を提供するために適応性がある。したがって、連邦政府によるサイバーセキュリティフレームワークの実装は OMB 覚書 M-17-25 との一貫性があり、[SP 800-39] 及び NIST Special Publication 800-37 で定義されたリスクマネジメントプロセス及びアプローチの使用を完全にサポートするとともに、それらと一貫性がある。これにより政府機関は、FISMA 及び E.O. 13800 の要件に従うという、同時に発生する義務を果たすことができる。

RMF の各タスクには、サイバーセキュリティフレームワークの特定のセクションへの参照が含まれている。例えば、タスク P-2「*リスクマネジメント戦略*」は、サイバーセキュリティフレームワークコアである[識別機能]と整合性があり、タスク P-4「*組織的にテーラリングされた管理策ベースライン及びサイバーセキュリティフレームワークプロファイル*」は、サイバーセキュリティフレームワークプロファイルの構成要素と整合性がある。また、タスク R-5「*認可の報告*」及びタスク M-5「*セキュリティ及びプライバシーに関する報告*」は、機能、カテゴリ、サブカテゴリのサイバーセキュリティフレームワーク構成要素を使用して、組織全体の OMB 報告及びリスクマネジメントの要件をサポートしている。サブカテゴリの[SP 800-53]管理策とのマッピング表は、https://www.nist.gov/cyberframework/federal-resources で入手できる。

RMF におけるセキュリティ及びプライバシー

組織は、効率を最大化し、重複作業を削減するために、セキュリティ及びプライバシーの問題に関する計画、アセスメント、実施計画及びマイルストーン（POAM：plans of action and milestones）において協調することが推奨される。その目的は、法律、大統領令、指令、規制、ポリシー、標準、又はミッション及びビジネスファンクション（ビジネス機能）から生じるセキュリティ及びプライバシー要件が十分に対応され、適切な管理策の選択、実装、アセスメント、監視が継続的に行われるようにすることである。RMF の重要なステップである認可判断は、認可パッケージ用に生成された、信頼できる実施可能なセキュリティ及びプライバシーの証拠の作成に依存している。費用対効果が高く効率的な方法でそのような証拠を作成することが重要である。

セキュリティ及びプライバシーの証拠を 1 つの認可パッケージにまとめる統一的かつ協調的なアプローチは、認可判断の参考になるセキュリティ及びプライバシーの専門家からの重要情報を得て、認可権限のある担当者をサポートすることになる。このようなアプローチは、最終的には、さらなる書類作業、成果物、又は文書の作成を発生させることではない。むしろ、より多くの情報に基づいたリスクベースの認可判断を促進するであろう、セキュリティ及びプライバシー管理策の実装に対するより大きな可視性を確実にすることである。

目次

正誤表

この表には、SP 800-37 に組み込まれた変更が記載されている。正誤表の更新内容には、本出版物における編集上又は実質的な訂正、明確化、又はその他の軽微な変更が含まれる。

日付	種類	変更内容	ページ

第 1 章

はじめに

セキュリティ及びプライバシーリスクを管理する必要性

組織は、ミッション及びビジネスファンクションを遂行するために情報システム [1] に依存している。ミッション及びビジネスファンクションの成功は、それらのシステムによって処理、保存、伝送される情報の機密性、完全性、可用性、及び個人のプライバシーを保護することにかかっている。情報システムに対する脅威には、機器の故障、環境破壊、ヒューマンエラー又はマシンエラー、及び意図的な攻撃などがある。意図的な攻撃は、高度で、統制が取れ、うまく組織化されていて資金に恵まれていることが多い [2]。情報システムへの攻撃が成功した場合、組織の運営 [3]、組織の資産、個人、他の組織、及び国家に深刻又は壊滅的な損害を与える可能性がある [4]。したがって、組織が常に警戒を怠らず、組織全体の上級管理職、リーダー、及びマネージャが自らの責任を理解して、組織の資産の保護及びリスク [5] の管理に責任を負うことが不可欠である。

組織は、現在の環境に存在する脅威から組織の資産を保護する責任に加えて、情報システムで個人情報（PII）を処理する際に、個人に対するリスクを考慮及び管理する責任を負う [6] [7]。組織が実施する情報セキュリティプログラム及びプライバシープログラムには、PII の機密性、完全性、及び可用性の管理に関して補足する目的がある。多くのプライバシーリスクが、PII の機密性、完全性、又は可用性の喪失につながる不正行為から生じる一方で、その他のプライバシーリスクは、組織によるミッション又は経営目標の達成を可能にする PII の作成、収集、使用、処理、保存、維持、配布、開示、又は廃棄に関わる正当な行為によって生じる。例えば、組織が PII の処理に関する適切な通知を提供せず、個人がそうした処理について知ることができなかったり、PII の正当な開示によっても個人が恥をかいたり、汚名を着せられたりする場合が考えられる。

---

[1] *情報システム*とは、情報の収集、処理、維持、使用、共有、配布、又は廃棄のために体系化された個別の一連の情報リソースである [44 USC 3502]。情報システムという用語に含まれるものの例として、汎用コンピューティングシステム、産業用／プロセス制御システム、サイバーフィジカルシステム、兵器システム、スーパーコンピュータ、指令、制御、及び通信システム、スマートフォン及びタブレットなどのデバイス、環境制御システム、組み込みデバイス／センサ、紙ベースのシステムがある。

[2] 国防科学評議委員会（Defense Science Board）タスクフォースのレポート「*レジリエントな軍事システム及び高度なサイバー脅威（Resilient Military Systems and the Advanced Cyber Threat）*」[DSB 2013]。

[3] 組織の運営には、ミッション、機能、イメージ、及び評判が含まれる。

[4] 有害なインパクトに含まれるものの例として、重要インフラのアプリケーションを支えるシステムへの侵害や、国土安全保障省（Department of Homeland Security）によって定義された政府の運営継続に最も重要なシステムへの侵害がある。

[5] リスクとは、エンティティが潜在的な状況又は事象によって脅かされる度合いの指標である。リスクはまた、その状況又は事象が発生した場合に生じる有害なインパクト、及びその発生の可能性の関数でもある。リスクの種類には、プログラムのリスク、コンプライアンス／規制に関するリスク、財務リスク、法的リスク、ミッション／ビジネスリスク、政治的リスク、セキュリティ及びプライバシーリスク（サプライチェーンリスクを含む）、プロジェクトリスク、風評リスク、安全性リスク、戦略計画リスクなどがある。

[6] [OMB A-130] では、PII を「単独で、又は特定の個人に結び付く、あるいは結び付けることができる他の情報と組み合わせて、個人の身元を識別又は追跡するために使用できる情報」と定義している。

[7] 情報システムが個人の行動又は活動に及ぼす影響よりも、PII の処理によるインパクトが小さい可能性がある場合、組織は、その情報システムとの相互作用によって生じる可能性のある個人へのリスクを考慮することを選択してもよい。そのような影響は、個人の自律性に対するリスクとなり、組織は、情報セキュリティ及びプライバシーリスクに加えて、それらのリスクを管理するための措置を講じる必要がある可能性がある。

プライバシーリスクの管理には、情報セキュリティプログラム及びプライバシープログラムが、PII の機密性、完全性、及び可用性に関するプログラムの目的を相互に補足し合う性質を持っていることから、両プログラム間の緊密な協調が必要である。その一方でプライバシーリスクは、専門的な知識及びアプローチを要する全く別の懸念も生じさせる。したがって、適用可能なプライバシー要件に確実に準拠し、PII の処理に関連する個人へのリスクを管理するために、組織が強固なプライバシープログラムを確立及び維持することも極めて重要である。

セキュリティ及びプライバシーリスクに密接に関連し、その一部でもあるサプライチェーンリスク[8]も、組織にとって懸念が高まっている。サードパーティ又は外部のプロバイダ、及び市販製品（COTS: Commercial-Off-The-Shelf）、システム及びサービスへの依存度が高まっているため、組織のシステムにインパクトを与えるサプライチェーンでの攻撃又は破壊が増加している。そのような攻撃は追跡又は管理が困難であり、組織のシステムに重大、深刻、又は壊滅的な結果をもたらす可能性がある。サプライチェーンのリスクマネジメント（SCRM）は、セキュリティ及びプライバシーリスクマネジメントと重なり合い、調和して機能する。本出版物では、セキュリティ及びプライバシーリスクを管理する包括的なアプローチの促進を支援するために、SCRM に関連するセキュリティ及びプライバシーリスクマネジメントのプラクティスを RMF に統合している。本出版物は主に情報セキュリティ及びプライバシーリスクマネジメントに焦点を当てているが、セキュリティ及びプライバシーリスクマネジメントをサポートする SCRM の概念を、いくつかの領域で具体的に取り上げて強調し、RMF を使用してどう対処できるかを明確にしている。

1.1 背景

NIST は国防総省（Department of Defense）、国家情報長官室（Office of the Director of National Intelligence）、及び国家安全保障システム委員会（Committee on National Security Systems）との協力関係により、情報セキュリティの向上、リスクマネジメントプロセスの強化、組織間の互恵契約[9]の促進を目的とした*リスクマネジメントフレームワーク*（RMF）を策定した。2016 年 7 月、行政管理予算局（OMB：Office of Management and Budget）は通達（Circular）A-130 を改訂し、RMF の下でのプライバシープログラムに対する責任を盛り込んだ。

RMF では、以下によるリスクマネジメントを重視している。システム開発ライフサイクル（SDLC）を通じた情報システムのセキュリティ及びプライバシーのケイパビリティ（能力）開発を促進する[10]、継続的監視プロセスによって、それらのシステムのセキュリティ及びプライバシー態勢に対する状況認識を継続的に維持する、システムの使用及び運用によって生じる、組織の運営、組織の資産、個人、他の組織、及び国家へのリスクの許容に関する決定を容易にするために、上級幹部及び管理職に情報を提供する。RMF とは以下のようなものである。

- リスクに見合った情報及び情報システムの保護を推進するために設計された反復可能なプロセスを提供する。
- セキュリティ及びプライバシーリスクを管理するために必要な、全組織的な準備を重視する。

[8] SCRM 要件は [OMB A-130]、[DODI 5200.44] で公表されている。国家安全保障システム向けの SCRM 要件は [CNSSD505] で公表されている。SCRM 要件は連邦政府 SCRM 政策調整委員会（Federal SCRM Policy Coordinating Committee）でも取り上げられている。

[9] 互恵契約とは、システムリソースを再利用するために互いのセキュリティアセスメント結果を受け入れること、又は、情報を共有するために互いのアセスメントされたセキュリティ態勢を受け入れることについての組織間の合意である。

[10] [SP 800-64] 及び [SP 800-160 v1] は、SDLC におけるセキュリティの考慮事項に関するガイダンスを提供している。

- 情報及びシステムの分類、管理策の選択、実装、アセスメント及び監視、並びに、情報システム及び共通管理策の認可を容易にする。[11]
- 継続的監視プロセスの実装を通じて、ほぼリアルタイムのリスクマネジメント、並びに、システム及び管理策の継続的認可を行うために、自動化の利用を促進する。
- ミッション及びビジネスファンクションを支える情報システムに関して、費用対効果の高い、リスクベースの意思決定を行うために必要となる情報を上級幹部及びマネージャに提供するために、正確かつタイムリーな指標の使用を奨励する。
- セキュリティ及びプライバシーの要件[12]及び管理策を、エンタープライズアーキテクチャ[13]、SDLC、取得プロセス、及びシステムエンジニアリングプロセスに統合することを容易にする。
- 組織レベル及びミッション／ビジネスプロセスレベルでのリスクマネジメントプロセスを、リスクマネジメント担当責任者及びリスク管理者（機能）[14]を通じて、情報システムレベルでのリスクマネジメントプロセスに結び付ける。
- 情報システム内に実装され、それらのシステムによって継承される管理策に対する責任と説明責任を確立する。

RMF は、複雑かつ高度な脅威、進化するミッション及びビジネスファンクション、変化するシステム及び組織の脆弱性を伴う多様な環境においてセキュリティ及びプライバシーリスクを効果的に管理するための動的かつ柔軟なアプローチを提供する。このフレームワークは政策及び技術に関して中立的であるため、IT リソース[15]及び IT 近代化の取り組みの継続的なアップグレードを容易にし、そうした移行期間における極めて重要なミッション及びサービスの確実な提供をサポートし促進する。

1.2 目的及び適用性

本出版物では、RMF について説明し、セキュリティ及びプライバシーリスクを管理し、情報システム及び組織に RMF を適用するためのガイドラインを提供する。このガイドラインは以下の目的で策定された。

- リスク管理者（機能）を通じて、システムに関連するセキュリティ及びプライバシーリスクの管理が、組織のミッション及びビジネス目標、並びに、上級幹部の定めるリスクマネジメント戦略と整合していることを確実にする。
- 適切なリスク対応戦略の実装によって、個人のプライバシー保護と情報及び情報システムのセキュリティ保護を実現する。
- 一貫性があり、情報に基づいた、継続的な認可の判断[16]、互恵契約、セキュリティ及びプライバシー情報の透明性及びトレーサビリティをサポートする。

---

[11] 第 3 章で、RMF の 7 つのステップと関連タスクを説明している。

[12] 第 2.6 節 で、RMF の実行に関する要件と管理策の関係を説明している。

[13] [OMB FEA] は、連邦政府エンタープライズアーキテクチャに関するガイダンスを提供している。

[14] [OMB M-17-25] は、リスクマネジメントに関する役割及び責任についてのガイダンスを提供している。

[15] IT リソースとは、[OMB A-130] に定義されている*情報リソース*の情報技術コンポーネントを指す。

[16] [SP 800-137] は、継続的認可をサポートする、情報セキュリティの継続的監視に関するガイダンスを提供している。今後の出版物では、プライバシーの継続的監視について取り上げる予定である。

- セキュリティ及びプライバシーの要件及び管理策を、エンタープライズアーキテクチャ、SDLC プロセス、取得プロセス、及びシステムエンジニアリングプロセス [17] に統合することを容易にする。
- 連邦政府機関内で重要インフラのサイバーセキュリティを改善するためのフレームワーク（Framework for Improving Critical Infrastructure Cybersecurity）[NIST CSF] の実装を容易にする。[18]

本出版物は、セキュリティ及びプライバシーリスクを組織 [19] が管理できるよう支援すること、並びに、数ある法律、規制、ポリシーの中でも特に 2014 年の連邦情報セキュリティ近代化法（FISMA：Federal Information Security Modernization Act）[FISMA]、1974 年のプライバシー法（Privacy Act）[PRIVACT]、OMB ポリシー、及び指定された連邦情報処理標準（FIPS：Federal Information Processing Standards）の要件を満たすことを目的としている。

本出版物の適用範囲は、連邦政府情報システムに関するものである。情報システムとは、デジタル形式か非デジタル形式かにかかわらず、情報の収集、処理、維持、使用、共有、配布、又は廃棄のために体系化された個別の一連の情報リソースである。情報リソースには、情報及び人員、機器、資金、情報技術などの関連リソースが含まれる。本ガイドラインは、国家安全保障システムのガイドラインを補完するために技術的観点から策定されたものであり、そのようなシステムに対する政策権限を有する適切な連邦政府担当官の承認を得て、当該システムに使用してもよい。州政府、地方自治体、部族政府、及び民間組織は、これらのガイドラインを必要に応じて使用することが推奨される。

1.3 対象読者

本出版物は、情報システムの設計、開発、実装、アセスメント、運用、メンテナンス、及び廃棄に関わる、以下を含む個人に役立つ。

- ミッション又はビジネスの所有に責任又は受託者責任を持つ個人（例：連邦政府機関の長）
- 情報システム、情報セキュリティ、又はプライバシーの管理、監督、又はガバナンスに責任を持つ個人（例：上級幹部、リスク管理者、認可権限のある担当者、最高情報責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者）
- セキュリティ又はプライバシーに関するアセスメントの実施、及び、情報システムの監視に責任を持つ個人（例：管理策アセッサー、監査人、システム所有者）
- セキュリティ又はプライバシーの実装及び運用に責任を持つ個人（例：システム所有者、共通管理策の提供者、情報所有者／情報管理者、ミッション所有者、ビジネスオーナー、セキュリティアーキテクト、プライバシーアーキテクト、システムセキュリティエンジニア、システムプライバシーエンジニア）
- 情報システムの開発及び取得に責任を持つ個人（例：プログラムマネージャ、調達担当者、コンポーネント製品及びシステムの開発者、システムインテグレータ、エンタープライズアーキテクト）

[17] [SP 800-160 v1] は、システムセキュリティエンジニアリング、及び統合的信頼性のあるセキュアなシステムの構築に関するガイドラインを提供している。

[18] [EO 13800] は、連邦政府機関に対し、サイバーセキュリティリスクの管理に [NIST CSF] を使用するよう指示している。

[19] 本出版物において組織という用語は、組織構造内の任意の規模、複雑さ、又は位置付けのエンティティ（例：連邦政府機関、又は必要に応じてその運用要素）を表現するために使用される。

・ロジスティクス又は廃棄に関連する責任を持つ個人（例：プログラムマネージャ、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）

RMF に関連する役割及び責任の包括的なリストと説明については、附属書 D を参照のこと。

1.4 本出版物の構成

本特別出版物の以降の構成は次のとおりである。

・**第 2 章**では、情報システム関連のセキュリティ及びプライバシーリスクマネジメントに関わる概念を説明する。これには、リスクマネジメントに対する全組織的な視点、RMF のステップ及びタスク構造、情報セキュリティプログラム及びプライバシープログラムの関係、並びに RMF における両プログラムへの対応方法、システム及びシステム要素としての情報リソース、認可境界、セキュリティ及びプライバシー態勢、サプライチェーンのリスクマネジメントに関連するセキュリティ及びプライバシーの考慮事項が含まれる。

・**第 3 章**では、RMF のステップの実施に必要なタスクを説明する。これには、組織レベル及び情報システムレベルでの準備、情報及び情報システムの分類、管理策の選択、テーラリング、及び実装、管理策の有効性のアセスメント、情報システム及び共通管理策の認可、管理策の継続的監視、情報システムと組織のセキュリティ及びプライバシー態勢に対する認識の維持が含まれる。

・**補足の附属書**では、RMF の適用に関する以下のような追加の情報及びガイダンスを示している。

- 参考文献
- 用語集
- 略語
- 役割及び責任
- RMF のタスクの概要
- システム及び共通管理策の認可
- 認可境界の考慮事項
- システムライフサイクルの考慮事項

第 2 章

基本的事項

セキュリティ及びプライバシーリスクの管理方法

本章では、組織における情報システム関連のセキュリティ及びプライバシーリスクの管理に関連する基本概念を説明する。これらの概念には、RMF のステップ及びタスク構造、RMF の情報セキュリティプログラム及びプライバシープログラム、情報システム、システム要素、認可境界の設定方法、セキュリティ及びプライバシーの態勢、サプライチェーンに関連するセキュリティ及びプライバシーリスクマネジメントのプラクティスが含まれる。

2.1 全組織的なリスクマネジメント

情報システム関連のセキュリティ及びプライバシーリスクの管理は、組織の戦略的ビジョン及びトップレベルの目標と目的を定める上級幹部から、プロジェクトを計画、実施、管理する中堅リーダー、組織のミッション及びビジネスファンクションを支援するシステムを開発、実装、運用、維持する個人に至るまで、組織全体の関与が必要になる複雑な仕事である。リスクマネジメントは、ミッション及びビジネス計画活動、エンタープライズアーキテクチャ、SDLC プロセス、及びそれらのシステムライフサイクルプロセスに不可欠なシステムエンジニアリング活動など、組織のあらゆる側面に影響を与える全体的な活動である。

図 1 は、*組織*レベル、*ミッション／ビジネスプロセス*レベル、*情報システム*レベルでセキュリティ及びプライバシーリスクに対処する、[SP 800-39] で説明されている多層的なリスクマネジメントアプローチを示している。コミュニケーションと報告は、この 3 つのレベルにまたがる双方向の情報フローであり、リスクが組織全体で対処されることを確実にするためのものである。

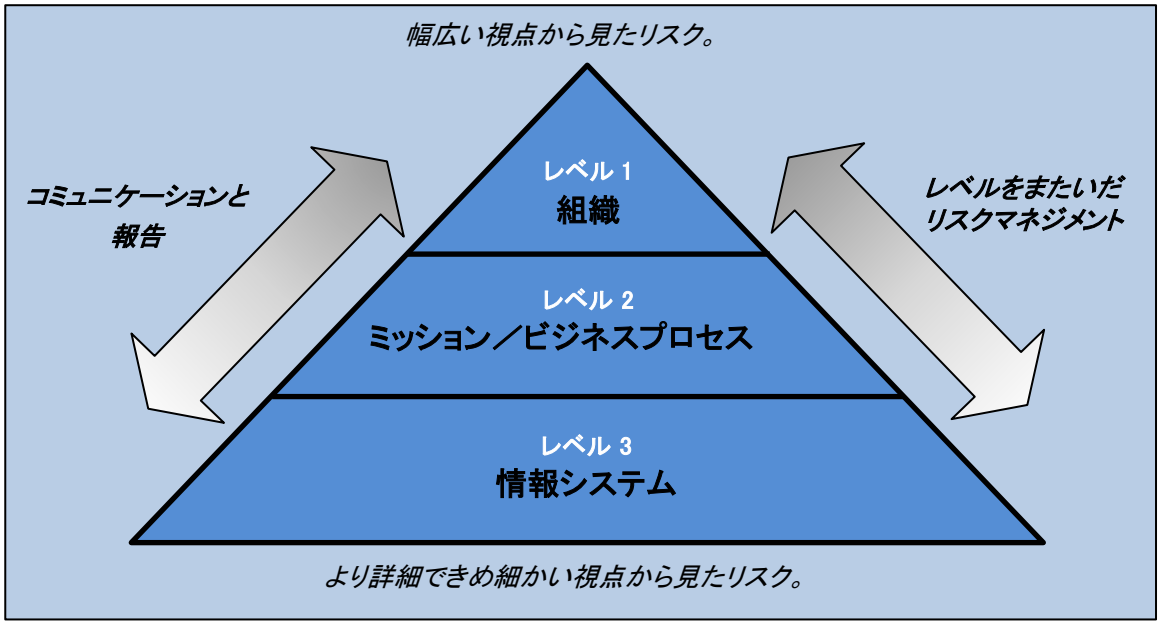

図 1: 全組織的なリスクマネジメントアプローチ

レベル 1 とレベル 2 で実施される活動は、組織が RMF を実行する準備のために極めて重要である。このような準備には、単に特定のシステムの運用や使用に関連するセキュリティ及びプライバシーリスクを管理するだけでなく、組織全体でセキュリティ及びプライバシーリスクを適切に管理するために不可欠な活動を含む、幅広い活動が含まれる。このようなリスクをシステムレベルでどのように管理するかについての決定は、単独で行うことはできない。このような決定は以下と密接に関連している。

- 組織のミッション又は経営目標
- システム、コンポーネント、及びサービスの近代化の取り組み
- エンタープライズアーキテクチャ、並びに、統合、最適化、及び標準化[20]を通じてシステムの複雑さ[21]を管理及び軽減する必要性
- 組織がミッション及びビジネスオペレーションを効果的、効率的、かつ費用対効果の高い方法で遂行できるようにするためのリソースの割り振り

RMF を実行するための組織の準備には、以下のものが含まれる。

- 組織のリスクマネジメントプロセスの役割と責任の割り当て
- リスクマネジメント戦略と組織のリスク許容度の確立
- 情報システムによる支援の対象とするミッション、ビジネスファンクション、及びミッション／ビジネスプロセスの識別
- 情報システムに関心を持つ主要なステークホルダー（組織の内部及び外部）の識別
- 資産（情報資産を含む）の識別と優先順位付け
- 情報システム及び組織に対する脅威の理解
- 個人に対する潜在的なマイナスの影響の理解
- 組織レベル及びシステムレベルのリスクアセスメントの実施
- セキュリティ及びプライバシーの要件の識別及び優先順位付け[22]
- 情報システム及び共通管理策の認可境界の決定[23]
- エンタープライズアーキテクチャの観点から情報システムの定義
- 情報システムによる継承に適した管理策を含むセキュリティ及びプライバシーアーキテクチャの策定

[20] 統合、最適化、及び標準化によってシステムの複雑さを管理することで、敵対者が悪用可能な攻撃対象領域及び技術フットプリントを削減できる。

[21] *エンタープライズアーキテクチャ*は、ミッション、情報、及びミッションの遂行に必要な技術、並びに、ミッションのニーズの変化に応じて新技術を導入するための移行プロセスを定義するものである。これには、ベースラインアーキテクチャ、ターゲットアーキテクチャ、及びシーケンスプラン（順位付け計画）も含まれる。[OMB FEA] は、エンタープライズアーキテクチャを実装するためのガイダンスを提供している。

[22] セキュリティ及びプライバシーの要件は、多くの情報源（法律、大統領令、指令、規制、ポリシー、標準、ミッション／ビジネス／業務の要件など）から得ることができる。

[23] 認可境界は、情報システム及び共通管理策の認可の範囲（すなわち、システムを定義するシステム要素又は継承可能な一連の共通管理策）を決定する。

- セキュリティ及びプライバシーの要件の識別、調整、及び競合の解消
- 情報システム、システム要素、及び組織へのセキュリティ及びプライバシーの要件の割り振り

レベル 1 及び 2 の活動では RMF の実行に向けて組織を準備するのに対し、レベル 3 では*情報システム*の観点からリスクに対処し、組織レベル及びミッション／ビジネスプロセスレベルでのリスク決定によって導かれ、情報を得る。レベル 1 及び 2 でのリスク決定は、システムレベルでの管理策の選択と実装に影響を与える可能性がある。管理策は、エンタープライズアーキテクチャ、セキュリティ又はプライバシーアーキテクチャ、及び組織が策定したテーラリングされた管理策ベースライン又はオーバーレイに従って、システム固有の管理策、ハイブリッド管理策、又は共通（継承）管理策として組織によって指定される。[24]

組織は、管理策が満たすことを意図しているセキュリティ及びプライバシーの要件に対する管理策の*トレーサビリティ（追跡可能性）*を確立する。このようなトレーサビリティを確立することで、システムの設計、開発、実装、運用、メンテナンス、及び廃棄において、すべての要件に対処できるようになる。[25] リスクマネジメント階層の各レベルは、RMF の実行が成功すると恩恵を受けることになり、セキュリティ及びプライバシーリスクを様々な組織レベルで枠組み化、アセスメント、対応、及び監視するリスクマネジメントプロセスの反復的な性質を強化する。

組織レベルで適切なリスクマネジメントの準備がなければ、セキュリティ及びプライバシーの活動のコストが増大し、熟練したセキュリティ及びプライバシーの専門家が余分に必要となり、効果のないソリューションを生み出す可能性がある。例えば、効果的なエンタープライズアーキテクチャの実装に失敗した組織では、情報技術インフラの統合、最適化、及び標準化が困難になる。さらに、アーキテクチャ及び設計の決定の影響は、組織が効果的なセキュリティ及びプライバシーのソリューションを実装する能力に悪影響をおよぼす可能性がある。組織が適切な準備を怠ると、不必要な冗長性、非効率的でコストがかかり脆弱なシステム、サービス、及びアプリケーションをもたらす可能性がある。

2.2 リスクマネジメントフレームワークのステップ及び構造

RMF には、組織がプロセスを実行する準備ができていることを確認するための準備ステップと、6 つの主要なステップから成る、7 つのステップがある。RMF の実行を成功させるためには、7 つのステップすべてが不可欠である。具体的なステップは以下のとおりである。

- **準備**：セキュリティ及びプライバシーリスクを管理するためのコンテキストと優先順位を確立することにより、組織レベル及びシステムレベルの観点から RMF を実行する準備を行う。
- **分類**：システム、及びそのシステムによって処理、保存、及び伝送される情報を、損失のインパクトの分析に基づいて分類する。[26]

[24] 管理策は、リスクマネジメント階層における 3 つのレベルすべてに割り振ることができる。例えば、共通管理策は、組織レベル、ミッション／ビジネスプロセスレベル、又は情報システムレベルで割り振ることができる。

[25] [SP 800-160 v1] は、要件のエンジニアリング及びトレーサビリティに関するガイダンスを提供している。

[26] 損失のインパクトは、リスクアセスメント活動時に考慮される 4 つのリスク要因のうちの 1 つである。他の 3 つの要因は、脅威、脆弱性、及び発生可能性である[SP 800-30]。組織は、情報及びシステムを分類する際にリスクアセスメントの結果を活用する。国家安全保障システムにおいては、分類の一環として、リスク要因に影響する識別の問題を考慮することが重要となる場合がある。例えば、そのシステムで国家機密情報又は諜報情報が処理、保存、又は伝送されるかどうか、米国以外の人間が直接又は間接的にシステムにアクセスするかどうか、システムによって処理、保存、又は伝送される情報が複数のセキュリティドメインにまたがるかどうかなどである。
[CNSSI 1253] は、国家安全保障システムの分類に関する追加情報を提供している。

- **選択**：システムの最初の一連の管理策を選択し、必要に応じて、リスクアセスメントに基づいてリスクを受容可能なレベルまで低減できるように管理策をテーラリングする。
- **実装**：管理策を実装し、システム及びその運用環境内で管理策をどのように使用するかについて記述する。
- **アセスメント**：セキュリティ及びプライバシーの要件に対する適合性の観点から、管理策が正しく実装されているか、意図した通りに運用されているか、及び期待した成果を得られているかを判断するために、管理策をアセスメントする。
- **認可**：組織の運営、組織の資産、個人、他の組織、及び国家に対するリスクが許容可能であるという判断に基づいて、システム又は共通管理策を認可する。
- **監視**：システム及び関連する管理策を継続的に監視する。これには、管理策の有効性のアセスメント、システム及び運用環境に対する変更の文書化、リスクアセスメント及びインパクト分析の実施、システムのセキュリティ及びプライバシーの態勢についての報告が含まれる。

図 2 は、RMF の各ステップを示している。RMF は、図 1 に示されているリスクマネジメント階層のすべてのレベルで機能する。第 3 章では、RMF のステップを実行するのに必要な各タスクの詳細について説明する。

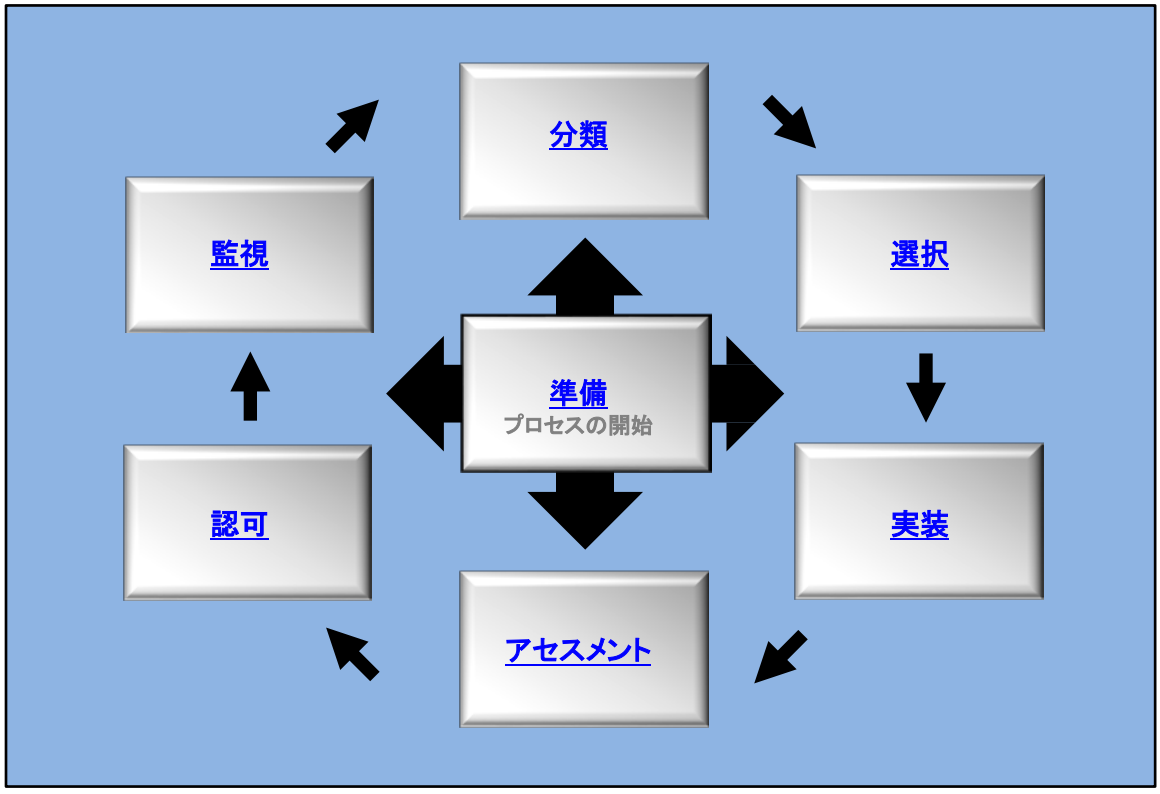

図 2: リスクマネジメントフレームワーク

上記と第 3 章では RMF のステップが順番に記載されているが、*準備*ステップの後は、各ステップを任意の順序で実行できる。*準備*ステップのタスクを完了した後、システム又は一連の共通管理策に対して初めて RMF を実行する組織は、通常、残りのステップを順番に実行する。

しかし、システムの種類、上級幹部によるリスク決定、又はタスク間の反復サイクルやタスクの再検討（アジャイル開発中など）を可能にするために、リスクマネジメントプロセスにおいてこの順序を変える必要が生じる多くのポイントが存在する可能性がある。組織が*監視*ステップに入ると、事象によってステップの不連続な実行が指示されることがある。例えば、リスク又はシステム機能の変化によって、その変化に対処するために RMF の 1 つ以上のステップの再検討を余儀なくされることがある。

RMF の実装における柔軟性

組織は、RMF のすべてのステップ及びタスク（オプションとしてラベル付けされたタスクを除く）を実行することが求められる。ただし、組織がすべての適用要件を満たし、セキュリティ及びプライバシーリスクを効果的に管理している限り、RMF の各ステップ及びタスクの実行方法には大きな柔軟性がある。その目的は、組織が最も効率的、効果的、費用対効果の高い方法で RMF を実装して、効果的なセキュリティ及びプライバシーを促進する方法でミッション及びビジネスのニーズをサポートできるようにすることである。柔軟な実装には、タスクを異なる（場合によっては連続しない）順序で実行する、特定のタスクを他のタスクよりも重視する、又は必要に応じて特定のタスクを組み合わせることが含まれる場合がある。また、RMF タスクの実行を強化するために、サイバーセキュリティフレームワークを使用することも含めることができる。

実装の柔軟性は、管理策の*選択*、組織のセキュリティ及びプライバシーのニーズを満たすための管理策の*テーラリング*、又は SDLC 全体での管理策アセスメントの実施にも適用できる。例えば、管理策の選択、テーラリング、実施、及びアセスメントは、システムの開発中に段階的に行うことができる。管理策のテーラリングを実施することで、セキュリティ及びプライバシーのソリューションを組織の具体的なミッション、ビジネスファンクション、リスク、及び運用環境に合わせて確実にカスタマイズするのに役立つ。最終的に、RMF の実行に固有の柔軟性は、組織がミッション及びビジネスの成功のために依存しているシステムと、それらのシステムで情報が処理される個人の保護に役立つ、効果的なセキュリティ及びプライバシーを促進する。

注：RMF は継続的な認可を重視する SDLC プロセスであるため、組織は、リスクのアセスメント及び*準備（システムレベル）*のステップで説明されているタスクに基づいて、どの RMF ステップを開始（又は再開始）するかを柔軟に決定できる。適切な RMF ステップを決定するには、システムの現在の状態のアセスメント、システムに対して既に完了している活動のレビュー、提案されるステップの識別と RMF へのタスクの登録、リスクが許容可能であることを確認するためのギャップ分析、決定の文書化、ステークホルダーへの通知、認可権限のある担当者（又はその他の関連する意思決定者）からの承認が必要である。

図 1 のリスクマネジメントアプローチは階層的に示されているが、通常、プロジェクト及び組織の力学はより複雑なものである。組織が選択するリスクマネジメントアプローチは、トップダウンの指令型から同僚間での分権的コンセンサス型まで、状況に応じて異なる。ただし、いずれの場合も、組織では、*組織*レベルから*情報システム*レベルまで、全組織的なリスクマネジメントプロセスに一貫したアプローチを適用して使用している。連邦政府職員は、本出版物に記載されているリスクマネジメントタスクを完了するために必要なリソースを識別及びセキュアにし、それらのリソースを適切な職員が利用できるようにする。リソースの割り振りには、リスクマネジメントタスクを実施するための資金調達と、それらのタスクを達成するのに必要な有能な人材を割り当てることが含まれる。

RMF の各ステップには、*目的*ステートメント、定義された一連の*成果*、及びそれらの成果を達成するために実行する一連の*タスク*がある。これらの成果は、様々なリスクマネジメントレベルによって達成できる。すなわち、組織全体に共通する成果もあれば、システム又はミッション／ビジネスユニットに焦点を当てた成果もある。

図 3 は、RMF の*準備*ステップ（組織レベル）の目的ステートメントと成果の例を示している。

3.1 準備

目的

*準備*ステップの目的は、組織における組織レベル、ミッション及びビジネスプロセスレベル、並びに、情報システムレベルでの極めて重要な活動を実施することで、組織が*リスクマネジメントフレームワーク*を使用してセキュリティ及びプライバシーリスクを管理するための準備を支援することである。

準備タスク（組織レベル）

表 1 は、*組織*レベルでの RMF の*準備*ステップのタスクと期待される成果の概要を示している。また、適用可能なサイバーセキュリティフレームワークの構成要素も示している。

表 1：準備タスクと成果（組織レベル）

タスク	成果
タスク P-1 リスクマネジメント役割	・ リスクマネジメントフレームワークを実行する個人が識別され、そのための主要な役割が割り当てられている。［*サイバーセキュリティフレームワーク*: **ID.AM-6**; **ID.GV-2**］
タスク P-2 リスクマネジメント戦略	・ 組織のリスク許容度の決定及び表明が含まれた組織のリスクマネジメント戦略が確立されている。 ［*サイバーセキュリティフレームワーク*: **ID.RM**; **ID.SC**］
タスク P-3 リスクアセスメント（組織）	・ 組織全体のリスクアセスメントが完了している、又は既存のリスクアセスメントが更新されている。 ［*サイバーセキュリティフレームワーク*: **ID.RA**; **ID.SC-2**］
タスク P-4 組織的にテーラリングされた管理策ベースライン及びサイバーセキュリティフレームワークプロファイル（オ	・ 組織的にテーラリングされた管理策ベースライン及び／又はサイバーセキュリティフレームワークプロファイルが確立され、利用可能になっている。 ［*サイバーセキュリティフレームワーク*: **プロファイル**］
タスク P-5 共通管理策の識別	・ 組織システムによって継承可能な共通管理策が識別され、文書化され、公開されている。
タスク P-6 インパクトレベルの優先順位付け（オプション）	・ 同じインパクトレベルを持つ組織システムの優先順位付けが実施されている。 ［*サイバーセキュリティフレームワーク*: **ID.AM-5**］
タスク P-7 継続的監視戦略（組織）	・ 管理策の有効性を監視するための組織全体の戦略が策定され、実装されている。 ［*サイバーセキュリティフレームワーク*: **DE.CM**; **ID.SC-4**］

RMF のタスク、責任、及び補助的な役割の概要表へのクイックリンク。

図 3：リスクマネジメントフレームワークのタスク構造

各タスクには、タスクの実行に必要となる一連の潜在的なインプットと、タスクの実行によって生成されることが期待される一連のアウトプットが含まれている。[27] さらに、各タスクには、そのタスクに関連するリスクマネジメント役割及び責任、並びに、タスクが実行される SDLC の段階が記述されている。[28] 詳解セクションでは、理解を容易にし、効果的なタスク実行を推進できるように、タスクに関連する情報が提供されている。最後に、RMF タスクの説明の後に、各タスクの補足情報を組織に提供するための参考文献一覧を示している。該当する場合、参考文献には RMF タスクに関連するシステムセキュリティエンジニアリングタスクも識別されている。[29] 図 4 は、標準的な RMF タスクの構造を示している。

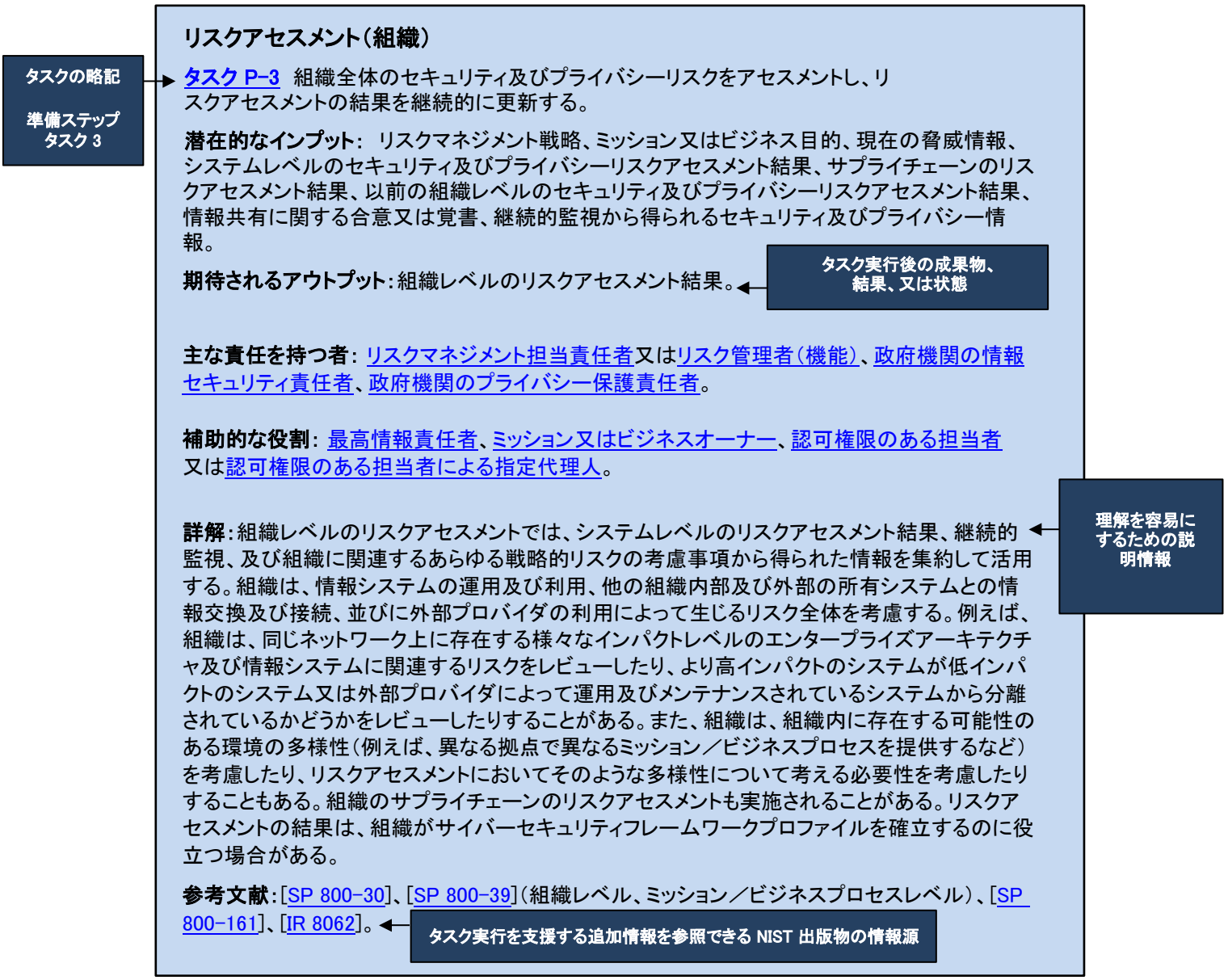

図 4: リスクマネジメントフレームワークのタスク構造

[27] タスクの*潜在的なインプット*は、必ずしも前のタスクの*期待されるアウトプット*から得られるとは限らない。これは、RMF ステップが必ずしも順番に実行されるわけではなく、順次的な依存関係が壊れることによって起こり得ることである。

[28] 附属書 D では、タスクで識別された各役割と責任について説明を提供している。

[29] [SP 800-160 v1] では、ライフサイクルベースのシステムセキュリティエンジニアリングプロセスについて説明している。

2.3 RMF における情報セキュリティ及びプライバシー

OMB CIRCULAR A-130：情報セキュリティとプライバシーの統合

2016 年に OMB は通達（Circular）A-130 号を改訂した。この通達では、連邦政府の情報、人員、機器、資金、情報技術リソース、及びそれらを支えるインフラとサービスの計画、予算、ガバナンス、取得、及び管理に関する一般方針を定めている。この通達は、連邦政府の情報リソースを保護し、個人情報（PII）を管理する責任について説明している。この通達では、情報セキュリティプログラム及びプライバシープログラムの要件の規定において、両プログラムが共有された目的に向けて協調することの必要性を以下のように強調している。

> *セキュリティ及びプライバシーは独立した別個の分野であるが、両者は密接に関連しており、政府機関は、セキュリティ及びプライバシーリスクの識別及び管理、並びに、適用可能な要件への準拠のために協調的なアプローチをとらなければならない。*

[OMB A-130] では、このガイドラインに記載されている RMF を実装することを組織に要求している。2016 年に改訂された通達では、OMB は組織に対して、プライバシーを RMF プロセスに統合することも要求している。

> *RMF は、情報セキュリティ、プライバシー、及びリスクマネジメントの活動を SDLC に統合するための、統制のとれた、構造化されたプロセスを提供する。この通達では、RMF を使用して、通常は「情報セキュリティ」という用語の「機密性」の目的に含まれるものを超えるプライバシーリスクを管理することを組織に要求している。多くのプライバシーリスクは PII の不正アクセス又は漏えいに関連しているが、プライバシーリスクは PII の作成、収集、使用、保持を含む他の活動、PII の品質又は完全性が不十分であること、及び適切な通知、透明性、又は参加の欠如が原因で生じることもある。*

ガイドラインのこのセクションでは、RMF における情報セキュリティプログラム及びプライバシープログラムの*関係*について説明している。ただし、OMB のポリシーの下では、組織は、組織のミッション及び状況を考慮した上で、最も効果的な方法でプライバシーを RMF に統合するという柔軟性を保持する。

RMF を実行するには、情報セキュリティプログラム及びプライバシープログラムの間の密接な協力が必要である。情報セキュリティプログラム及びプライバシープログラムにはそれぞれ異なる目的があるが、それらの目的は重なる部分があり、補完的である。情報セキュリティプログラムは、機密性、完全性、及び可用性を提供するために、情報及び情報システムを不正アクセス、不正利用、漏えい、破壊、改ざん、又は破棄（すなわち、不正なシステム活動又は行動）から保護する責任を負う。プライバシープログラムは、適用されるプライバシー要件に確実に準拠し、PII の作成、収集、使用、処理、配布、保存、維持、開示、又は廃棄（総称して「処理」と呼ぶ）に関連する個人へのリスクを管理する責任を負う[30]。
RMF のステップを実行する準備を行う際、組織は、プロセスのすべてのステップで両分野の目的が確実に達成されるように、2 つのプログラム間の協力を最も効果的に促進及び制度化する方法を検討する。

[30] プライバシープログラムは、情報システムとの相互作用によって生じる可能性のある個人へのリスクを考慮することもある。この場合、PII の処理は、情報システムが個人の行動又は活動にもたらす影響よりもインパクトが小さい可能性がある。そのような影響は、個人の自律性に対するリスクとなり、組織は、情報セキュリティ及びプライバシーリスクに加えて、それらのリスクを管理するための措置を講じる必要がある可能性がある。

情報システムが PII を処理する場合、組織の情報セキュリティプログラム及びプライバシープログラムは、不正なシステム活動又は行動から発生する可能性のある個人へのリスクを管理する責任を分担している。このため、セキュリティ管理策を選択、実装、アセスメント、及び監視する際には、この 2 つのプログラムが協力する必要がある[31]。しかし、情報セキュリティプログラム及びプライバシープログラムには、PII の機密性、完全性、及び可用性の管理に関して補完的な目的があるが、PII をセキュアにするだけでは個人のプライバシー保護を達成することはできない。

すべてのプライバシーリスクが、PII の不正アクセス又は漏えいなどの不正なシステム活動又は行動から生じるわけではない。プライバシーリスクの中には、情報セキュリティの範囲を超える、認可された活動が原因で生じるものもある。例えば、プライバシープログラムは、PII の作成、収集、使用、及び保持、PII の品質又は完全性が不十分であること、及び適切な通知、透明性、又は参加の欠如が原因で生じる、個人へのリスクを管理する責任を負う。したがって、適用されるプライバシー要件に確実に準拠し、PII の認可された処理及び不正な処理によるプライバシーリスクを管理するために、組織のプライバシープログラムは、プライバシー管理策の選択、実装、アセスメント、及び監視も行う[32]。

[OMB A-130] は、*プライバシー管理策*を、適用されるプライバシー要件に確実に準拠し、プライバシーリスクを管理するために政府機関内で採用される行政上、技術的、及び物理的な予防手段、と定義している。プライバシー管理策は、システム及びその情報の機密性、完全性、及び可用性を保護するために、情報システム又は組織に対して予防手段又は対策として通達で規定されている*セキュリティ管理策*とは異なる。組織の情報セキュリティプログラム及びプライバシープログラムは、不正なシステム活動又は行動から生じる個人へのリスクを管理する責任を分担しているため、セキュリティの目的とプライバシーの目的の両方を達成する管理策は、プライバシー管理策であり、セキュリティ管理策でもある。本ガイドラインでは、このような両方の目的を達成する管理策を単に「管理策」と呼んでいる。本ガイドラインで*管理策*という用語とともに「プライバシー」及び「セキュリティ」という記述語を使用している場合、特定の目的のために管理策を選択、実施、及びアセスメントする状況における管理策を指している。

本出版物に記載されているリスクマネジメントプロセスは、セキュリティプログラム及びプライバシープログラムに同様に適用される。ただし、セキュリティプログラム及びプライバシープログラムが管理する必要があるリスクは、重なる部分がある領域も、そうでない領域もある。したがって、組織のあらゆるレベルでプライバシーとセキュリティの責任者間の効果的な協力を促進するために、組織がプライバシーとセキュリティの相互作用を理解することが重要である。

---

[31] 例えば、*分類*ステップのタスク C-2 では、情報システムのインパクトレベルを判断するために、プライバシープログラム及びセキュリティプログラムが連携して、PII の機密性、完全性、又は可用性の喪失によって生じる組織の運営、組織の資産、個人、他の組織、及び国家に対する潜在的な有害なインパクトを考慮する。その結果得られたインパクトレベルにより、*選択*ステップのタスク S-1 でセキュリティ管理策ベースラインが選択される。

[32] 認可を受けて PII を処理する場合に関連するプライバシーリスクを軽減するために、異なる管理策を選択する必要がある場合がある。例えば、個人に関する特定の情報が公開された場合に、その個人が恥ずかしい思いをしたり、汚名を着せられたりするリスクがあるかもしれない。暗号化は、PII の漏えいを防ぐことができるが、復号化と PII へのアクセスを認可された当事者への公開に関連するプライバシーリスクには対処できない。このプライバシーリスクを軽減するには、組織は認可された当事者に情報の復号化を許可するリスクをアセスメントする必要があり、場合によっては、そのリスクを軽減する管理策を選択する必要がある。このような例では、組織は、個人が公開に関する組織のプラクティスを理解し、このアクセスについて選択を行使できるような管理策を選択したり、個人から情報を切り離すために、差分プライバシー又はプライバシー強化の暗号技術を使用したりすることがある。

2.4 システム及びシステム要素

本出版物では、RMF の実行については情報システムの法令上の定義を使用する。しかし、SDLC プロセスのコンテキストで情報システムを記述し、それらのシステムのコンポーネント内でセキュリティ及びプライバシーのケイパビリティがどのように実装されるかを記述することが重要である。したがって、RMF を実行する組織は、情報システム開発のライフサイクルを広く見渡し、アーキテクチャ及びエンジニアリングの概念とのコンテキスト上の関係と連携を提供する。これにより、セキュリティ及びプライバシーリスク（サプライチェーンリスクを含む）にライフサイクル全体を通じて適切な詳細レベルで対処し、このようなケイパビリティを確実に実現されるようになる。[ISO 15288] は、情報システム及びその運用環境でシステムが相互作用するエンティティについての技術展望を提供している[33]。

連邦法が情報システムを、情報の収集、処理、維持、使用、共有、配布又は廃棄のために体系化された個別の情報リソースのセットと定義しているように、[ISO 15288] は*システム*を、1 つ以上の所定の目的を達成するために体系化された、相互作用する要素のセットと定義している。情報システムを構成する情報リソースに情報及びその他のリソース（人員、機器、資金、情報技術など）が含まれるように、システム要素には技術又は機械の要素、人的要素、及び物理的又は環境的な要素が含まれる。システム内の各*システム要素*[34] は、指定された要件を満たし、ハードウェア、ソフトウェア、又はファームウェア[35]、物理構造又はデバイス、又は人、プロセス、ポリシー、及び手順を介して実装される場合がある。個々のシステム要素又はシステム要素の組み合わせは、規定されたシステム要件を満たすことができる。システム要素間の相互接続により、それらの要素が必要に応じて相互作用し、システム要件で規定されたケイパビリティを生み出せるようになる。最終的に、すべてのシステムは、システム及びその運用に影響を及ぼす環境内で運用される。

認可境界は、リスクマネジメント及び説明責任を促進するために、RMF の実行のためのシステム[36]を定義している。システムは、システムライフサイクル中にサポートを提供する 1 つ以上の*イネーブリングシステム*によってサポートされることがある。イネーブリングシステムは、システムの認可境界内に含まれておらず、システムの運用環境に存在するとは限らない。イネーブリングシステムは、システムに共通の（すなわち、継承された）管理策を提供することも、識別サービス及び認証サービス、ネットワークサービス、又は監視機能など、システムで使用されるあらゆる種類のサービス又は機能を含めることもできる。最後に、システムが運用環境内で相互作用する*他のシステム*がある。他のシステムも認可境界外にあり、システムが提供するサービスの受益側である場合もあれば、単に何らかの一般的な相互作用があるだけの場合もある[37]。

---

[33] [SP 800-160 v1] では、SDLC の一部として、システムセキュリティエンジニアリングを取り上げている。

[34] 本出版物では、*システム要素*と*情報リソース*という用語は同じ意味で使用されている。44 U.S.C. Sec. 3502 で定義されている情報リソースには、情報及び人員、機器、資金、情報技術などの関連リソースが含まれる。法律によって、システムは個別の情報リソースのセットで構成されている。

[35] *システムコンポーネント*という用語は、ハードウェア、ソフトウェア、又はファームウェアを介して実装される*システム要素*を指す。

[36] 歴史的に、NIST では*認可境界*という用語と*システム境界*という用語を同じ意味で使用してきた。明確性と正確性を高め、標準化された用語を使用するために、現在、認可境界という用語は、認可権限のある担当者によって操作又は使用が認可されるシステムを構成するシステム要素（すなわち、認可の範囲）のセットを指すために排他的に使用されている。また、認可境界は、継承目的で認可される共通管理策のセットを指す場合もある。

[37] イネーブリングシステム及びその他のシステムのリスクマネジメント及び説明責任は、それぞれの認可境界内で対処される。

図 5 は、システムの概念図と、システム、システム要素、イネーブリングシステム、その他のシステム、及び運用環境の間の関係を示している[38]。

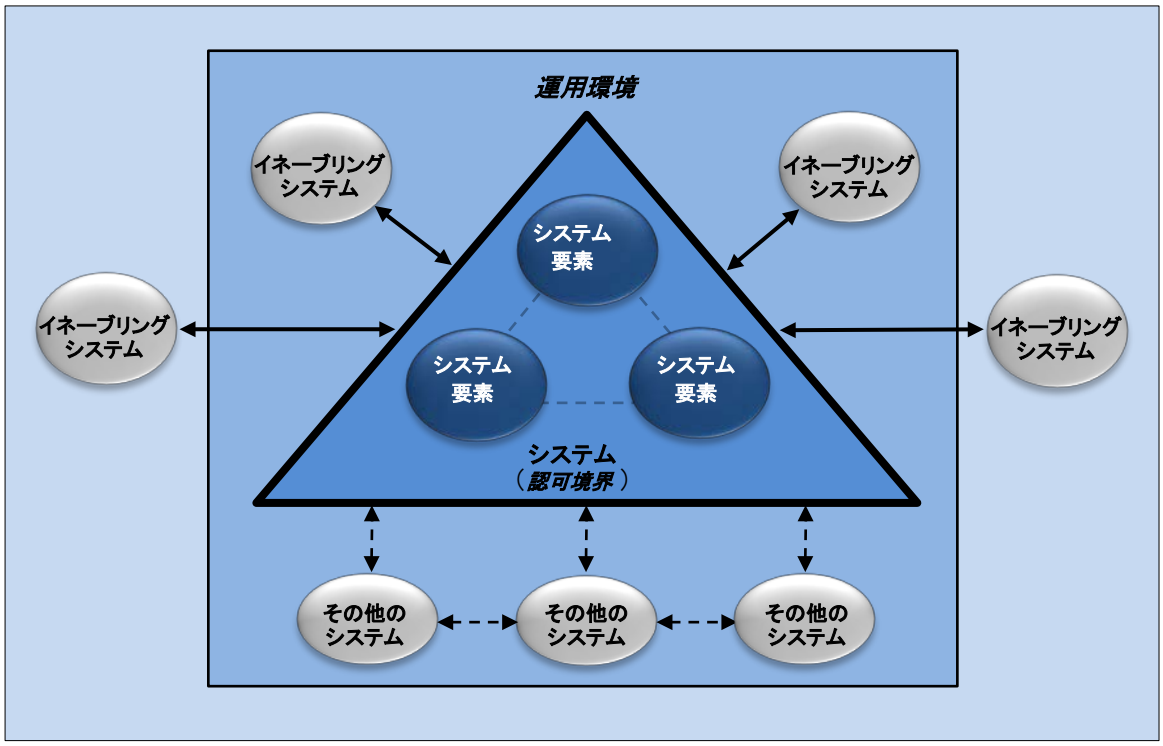

図 5: システムの概念図

運用環境の特定の部分が認可境界に含まれる（すなわち、認可の「範囲内」であると判断される）が、他の部分は除外される場合がある。例えば、システム要素の保護を提供する施設（すなわち、運用環境）がシステムの認可の範囲内にあると判断された場合、物理的及び環境的な保護管理策（例えば、エントリポイントでの物理的アクセス制御、境界保護デバイス）は認可境界に含まれるため、システムセキュリティ計画に含まれる。施設がシステムに継承される共通管理策として物理的及び環境的な保護を提供している場合、運用環境はシステムの範囲外となり、システムの認可境界に含まれない[39]。

また、システムは、拡張された運用環境の一部ではあるが、システムの認可の範囲外にあるイネーブリングシステム又はその他のシステムと通信したり、その他の相互作用を行ったりすることもある[40]。運用環境のどの部分が認可境界内にあるかは、組織が判断する。通常、これらの判断はシステムに固有であり、文脈に依存する。

---

[38] *システム*、*システム要素*、*イネーブリングシステム*、*その他のシステム*、*運用環境*という用語は、情報技術（IT）及び制御・運用技術（OT）に関してそのどちらかに依存するものではない。

[39] *共通管理策*は、管理策を継承するシステムのセキュリティ及びプライバシーの計画で参照される。

[40] システムと認可境界外にあるイネーブリングシステム又はその他のシステムとの間の接続及び情報交換について、組織はそのような接続及び情報交換によってもたらされるリスクを考慮する。

2.5 認可境界

認可境界は、情報システムに対する保護範囲（すなわち、組織が、組織の直接的な管理下で、あるいは組織の責任の範囲内で、何を保護することに同意するか）を設定するものである [41]。認可境界には、組織のミッション及びビジネスファンクションをサポートする各システムの一部である人、プロセス、及び情報技術（すなわち、システム要素）が含まれる。認可境界が広すぎる（すなわち、含まれるシステム要素又はコンポーネントの数が多すぎる）と、リスクマネジメントプロセスが不必要に複雑になる。逆に、認可境界を限定しすぎる（すなわち、含まれるシステム要素又はコンポーネントが少なすぎる）と、個別に管理しなければならないシステムの数が増えるため、組織の情報セキュリティ及びプライバシーのコストが不必要に増大する可能性がある。

システムの認可境界は、RMF の*準備タスク（システムレベル）*のタスク P-11 で設定される。組織は、システムの認可境界を構成する要素を柔軟に決定できる。認可境界内に含まれる一連のシステム要素が、システム（すなわち、認可の範囲）を定義する。一連のシステム要素がシステムの認可境界として識別される場合、それらの要素は、一般的に同じ直接的な管理下にある [42]。認可境界を決定する際のその他の考慮事項には、次のようなシステム要素を特定することが含まれる。

- 同じミッション又はビジネスファンクションをサポートする。
- 運用特性と、セキュリティ及びプライバシーの要件が類似している。
- 類似の種類の情報（例えば、同じインパクトレベルで分類されている）を処理、保存、及び伝送する [43]。
- 同じ運用環境に存在する（又は、分散型システムの場合、運用環境が類似している様々な場所に存在する）。

認可境界の範囲は、組織が実施する継続的監視プロセスの一環として、定期的に再検討される。上記の考慮事項は、組織がリスクの管理を目的として認可境界を決定する際に有用である可能性があるが、この考慮事項は、組織の利用可能なリソースで効果的なセキュリティ及びプライバシーを推進するための認可境界を設定する際の組織の柔軟性を制限することを意図していない。

認可境界を設定するプロセスは、リスクマネジメントに大きな影響を及ぼすため、主要な参加者間の調整を必要とする全組織的な活動である。このプロセスでは、ミッション及びビジネスの要件、セキュリティ及びプライバシーの要件、及び組織にかかるコストが考慮される。

---

[41] 情報システムとは、デジタル形式か非デジタル形式かにかかわらず、情報の収集、処理、使用、共有、維持、配布、又は廃棄のために体系化された個別の情報リソースのセットである。情報リソースには、情報及び人員、機器、資金、情報技術など関連リソースが含まれる。情報システムには、ハードウェア、ファームウェア、及びソフトウェアが含まれる場合と含まれない場合がある。

[42] 情報システムの直接的な管理下における管理策には、予算、計画、又は運用に関する権限、及びそれらに関連する*責任*及び*説明責任*が含まれる。直接的な管理下における管理策は、必ずしもマネジメント（訳注：経営層）が介在しないということを意味するとは限らない。

[43] システムに複数のインパクトレベルの情報が含まれている場合、そのシステムは、最も高いインパクトレベルに分類される。[FIPS 199] 及び [FIPS 200] を参照のこと。

附属書 G では、複雑なシステム及びソフトウェアアプリケーションの境界を含む、認可境界を決定するための追加情報及び考慮事項を提供している。

効果的な認可境界

*システム*及び*共通管理策*のための有意義な認可境界を設定することは、組織が実施する最も重要なリスクマネジメント活動の 1 つである。認可境界は、外部プロバイダのシステム、コンポーネント、及びサービスの使用を含む、情報リソース及び個人のプライバシーを保護するための、認可権限のある担当者の責任及び説明責任の具体的な範囲を定める。有意義な認可境界を設定することは、組織のミッション及びビジネスの成功を確実にするための土台となる。

2.6 要件及び管理策

RMF を実行する前に、セキュリティ及びプライバシーの要件の概念、及び要件と管理策の関係を理解することが重要である。*要件*という用語は、様々なコンテキストで使用できる。連邦政府の情報セキュリティ及びプライバシーポリシーに関するコンテキストでは、この用語は通常、組織に課される情報セキュリティ及びプライバシーに関する義務を指すために使用される。例えば、OMB による通達（Circular）A-130 は、連邦政府機関に対して、情報リソースを管理する際に準拠しなければならない一連の情報セキュリティ及びプライバシーの要件を課している。本ガイドラインでは、連邦政府政策というコンテキストでの要件という用語の使用に加えて、特定のシステム又は組織に対するステークホルダーの一連の保護ニーズを表すために、より広い意味で*要件*という用語を使用している。ステークホルダー保護のニーズとそれに対応するセキュリティ及びプライバシーの要件は、多くの情報源（例えば、法律、大統領令、指令、規制、ポリシー、標準、ミッション及びビジネスのニーズ、又はリスクアセスメント）から導き出される場合がある。本ガイドラインで使用される*要件*という用語には、法律上の要件とポリシーの要件の両方に加えて、他の情報源から導き出される可能性があるより広範な一連のステークホルダー保護のニーズの表現も含まれる。これらすべての要件をシステムに適用すると、セキュリティ、プライバシー、及びアシュアランスを含むシステムに必要な特性を決定するのに役立つ。

組織は、セキュリティ及びプライバシーの要件が SDLC のどこで何の目的で採用されるかに応じて、それらの要件をさらに細かいカテゴリに分類することを選択できる。組織は、ステークホルダー保護のニーズを満たすためにシステム又は組織が提供しなければならないケイパビリティについて記述するために、*ケイパビリティ要件*という用語を使用することがある。さらに、組織はシステムの特定のハードウェア、ソフトウェア、及びファームウェアコンポーネントに関連するシステム要件を*仕様要件*と呼ぶことがある。仕様要件とは、管理策のすべて又は一部を実装するケイパビリティ、及び（すなわち、検証、妥当性確認、テスト、及び評価プロセスの一環として）アセスメントされる可能性があるケイパビリティである。
最後に、組織は*作業ステートメント*要件という用語を使用して、運用上又はシステム開発中に実施しなければならない活動を指す可能性がある。

*管理策*は、組織が特定のセキュリティ及びプライバシーに関する目的を達成し、組織のステークホルダー保護のニーズを反映するのに適切な予防手段及び保護ケイパビリティの記述と見なすことができる。

管理策は、システム要件を満たすために組織によって選択及び実装される。管理策には、技術的、行政上、及び物理的な側面を含めることができる。場合によっては、管理策の選択及び実装には、*派生要件*又は実体化された管理策パラメータ値の形で、組織による追加の仕様が必要になる可能性がある。派生要件と管理策パラメータ値は、SDLC 内の特定の管理策に適切なレベルの実装詳細を提供するために必要になる可能性がある。

コンテキスト依存型要件

組織が識別したセキュリティ及びプライバシーの要件及びリスクは、そのリスクに対応するために必要なセキュリティ管理策及びプライバシー管理策の必要性をもたらす。組織によって選択された管理策は、システムエンジニアリングのコンテキストにおける仕様要件及び作業ステートメント要件の両方をもたらす。これは、SDLC プロセスの一環としてシステムエンジニアが要件を策定、導出、分解する方法の重要な側面である。このように、組織はシステムのライフサイクル中に、セキュリティ及びプライバシーの要件を様々な粒度及び具体性で管理する。管理策は、組織が改良したり拡張したりすることができる保護ケイパビリティの高レベルなステートメントを提供することで、ライフサイクルにおいて重要な役割を果たす。

2.7 セキュリティ及びプライバシー態勢

RMF の目的は、SDLC 全体を通じて、情報システム、組織、及び個人が適切に保護されること、並びに、認可権限のある担当者がシステムの運用又は使用、又は共通管理策の提供に関して、信頼できるリスクベースの意思決定を行うために必要な情報を入手することを支援することである。認可権限のある担当者にとってリスクベースの意思決定を行う際の重要な側面は、情報システムのセキュリティ及びプライバシー態勢、及びそれらのシステムで継承可能な共通管理策を理解することである。セキュリティ及びプライバシー態勢は、組織のシステムの運用又は使用に関して組織の防御を管理し、適用されるプライバシー要件に準拠してプライバシーリスクを管理し、状況の変化に応じて対応するための情報アシュアランスリソース（人員、ハードウェア、ソフトウェア、ポリシー、手順など）及びケイパビリティに基づいて、組織内の情報システム及び情報リソース（人員、機器、資金、情報技術など）の状況を表すものである。

情報システム及び組織のセキュリティ及びプライバシー態勢は、システム固有の管理策、ハイブリッド管理策、及び共通管理策をアセスメント及び継続監視することによって、継続的に決定される [44]。管理策アセスメント及び監視活動は、組織が選択した管理策が正しく実装され、意図したとおりに運用され、法律、大統領令、規制、指令、ポリシー、標準、又はミッション及びビジネスの要件に対応したセキュリティ及びプライバシーの要件を満たしていることの証拠を提供する。認可権限のある担当者は、組織の運営及び資産、個人、他の組織、又は国家に対するリスクが許容可能であるかどうかを、組織のリスクマネジメント戦略及び組織のリスク許容度に基づいて判断するため、セキュリティ及びプライバシー態勢を使用する [45]。

[44] 管理策の監視は [SP 800-39] で定義されている組織全体のリスクマネジメントアプローチの一部である。
[45] RMF の*準備（組織レベル）*ステップの*タスク P-2* を参照。

2.8 サプライチェーンのリスクマネジメント

組織では、ミッション及びビジネスファンクションを実施するために、外部プロバイダから提供される製品、システム、及びサービスにますます依存するようになっている。組織は、そのようなコンポーネント製品、システム、及びサービスを使用する際に発生するリスクに対して責任及び説明責任を負う [46]。外部プロバイダとの関係は、例えば、合弁事業、業務提携、様々な種類の正式合意（契約、省庁間の合意、一連のビジネス合意、ライセンス合意など）、又は外部委託協定などを通じて、様々な方法で確立することができる。

外部プロバイダからの製品、システム、及びサービスへの依存度の高まりと、それらのプロバイダとの関係の性質により、組織にとってのリスクが高まっている。リスクは、偽造品、不正な製造、改ざん、盗難、悪意のあるソフトウェア及びハードウェアの挿入、サプライチェーンにおける製造及び開発の不適切なプラクティス（組織がその環境におけるリスクをより適切に管理できるようなセキュリティ又はプライバシーのケイパビリティを構築できないことを含む）などの、脅威事象の起こりやすさ及び有害なインパクトに基づいて増加する可能性がある。

サプライチェーンのリスクは、システム要素、システム、組織、セクター、又は国で固有のもの、又は体系的である可能性がある。1 つのシステム内でのシステム要素又はサービスの単独使用によって、組織にとって受容可能なリスクが生じることもあるが、システム、組織、セクター、又は国家全体で一般的に又は広範囲に使用すると、リスクが受容できないレベルまで高まる可能性がある。これらのリスクは、多くの場合、製品及びサービスのサプライチェーンがグローバルに分散していること、及び取得した技術がどのように開発、統合、及び展開されているかに関して組織の可視性及び理解度が低下していることに関連している。これには、取得した製品、システム、及びサービスの完全性、セキュリティ、レジリエンス、プライバシーのケイパビリティ、及び品質を保証するために使用されるプロセス、手順、及びプラクティスが含まれる。

サプライチェーンのリスクに対処するために、組織は、SCRM 活動を方向付けるための重要な手段となる SCRM ポリシーを策定する。SCRM ポリシーは、適用される法律、大統領令、指令、ポリシー、規制からのガイド及び情報に基づいて、適用される組織のポリシー（取得及び調達、情報セキュリティ及びプライバシー、物流、品質、サプライチェーンなど）をサポートする。このポリシーは、組織の戦略計画における目標及び目的、ミッション及びビジネスファンクション、内部及び外部の顧客要件に対処するものである。また、SCRM と組織のリスクマネジメント及び SDLC プロセスとの統合ポイントも定める。最後に、SCRM ポリシーは、組織内の SCRM の役割及び責任、それらの役割間の依存関係、及び役割間の相互作用を定める。SCRM の役割は、調達、リスクアセスメントの実施、サプライチェーン脅威インテリジェンスの収集、リスクベースの軽減策の識別と実装、監視機能の実施に関する責任を規定する。

[46] [OMB A-130] では、サプライチェーンリスクを定義し、連邦政府機関に対して、リスクが適切に管理されるように、SDLC 全体を通してすべてのリソース計画及び管理活動でサプライチェーンのセキュリティ問題を考慮するように要求している。

[FISMA] 及び [OMB A-130] は、連邦政府の情報を扱う外部プロバイダ、又は連邦政府の代理としてシステムを運用する外部プロバイダに対して、連邦政府機関と同じセキュリティ及びプライバシーの要件を満たすことを義務づけている。連邦政府の情報を処理、保存、又は伝送するシステムの管理策を含む外部プロバイダに課せられるセキュリティ及びプライバシーの要件は、契約又はその他の正式な合意で表明される。RMF はサプライチェーンのリスク管理に効果的に使用できる[47]。図 5 のシステムの概念図は、サプライチェーンのあらゆる要素に対するセキュリティ、プライバシー、及びリスクマネジメント活動を手引きし、情報を提供している。RMF のすべてのステップは、*認可*ステップを除いて、非連邦政府の外部プロバイダによって実行される可能性がある。すなわち、リスクの受容は、連邦政府固有の責任であり、上級管理職が責任及び説明責任を負う。認可の決定は、外部プロバイダからのコンポーネント製品、システム、及びサービスの取得及び使用に関連するリスクマネジメントに直接関連している[48]。[OMB A-130] では、組織に対して SCRM 計画を策定し実装することも要求している[49]。

サプライチェーンリスクの管理は複雑で多面的な仕事であり、内外のステークホルダーとの信頼関係の構築及びコミュニケーションなど、組織全体での協調した取り組みが必要である。SCRM 活動には、該当するリスクの識別及びアセスメント、適切な緩和策の決定、選択された緩和策を文書化するための適切な SCRM 計画の策定、及び SCRM 計画に対するパフォーマンスの監視が含まれる。サプライチェーンは組織間及び組織内で異なるため、SCRM 計画は個々のプログラム、組織、及び運用の状況に合わせてテーラリングされる。テーラリングされた計画は、システムが「目的に適合している」かどうかを判断するための基礎を提供するため、それに応じて管理策をテーラリングする必要がある。テーラリングされた SCRM 計画は、組織が、ミッション及びビジネスの要件及びリスク環境に基づいて、最も重要なミッション及びビジネスファンクションにリソースを集中させるのに役立つ。

外部プロバイダから製品、システム、又はサービスを取得することによるリスクを許容できるかという判断は、組織がそのプロバイダから得ることのできるアシュアランス[50]のレベルによって決まる。アシュアランスのレベルは、製品、システム、又はサービスの保護に必要な管理策に関して、組織が外部プロバイダに対して実施できる管理の程度と、それらの管理策の有効性を示すためにプロバイダが提示する証拠に基づいている。

管理の程度は、契約又はサービス内容合意書の具体的な条件によって確立される。組織によっては、外部プロバイダに対するセキュリティ及びプライバシーの要件を規定する契約手段又はその他の合意を通じて、広範な管理を行っている。これに対し、コモディティサービス又は市販製品（COTS）を購入しているために、管理が制限される組織もある。

[47] *サプライチェーンリスク*とは、情報又は情報システムの機密性、完全性、又は可用性の喪失により生じるリスクを意味しており、組織の運営（ミッション、機能、イメージ、又は評判を含む）、組織の資産、個人、他の組織、及び国家に及ぶ可能性がある有害なインパクトを表す[OMB A-130]。システム要素が PII を処理する場合、SCRM のプラクティスでは情報セキュリティ及びプライバシーリスクの両方に対処する。

[48] 連邦政府情報システムの*認可*（すなわち、リスクの受容）は連邦政府の固有の責任であるが、これは、サプライチェーンのあらゆるレベルで連邦政府以外の組織の上級管理職がセキュリティ及びプライバシーリスクを管理するために使用できる基礎的な概念である。

[49] [SP 800-161] は、SCRM 計画に関するガイダンスを提供している。

[50] 外部プロバイダが提供するアシュアランスのレベルは様々であり、高いアシュアランスを提供するプロバイダ（例えば、共通のビジネスモデル及び目標を共有する合弁事業のビジネスパートナー）もいれば、アシュアランスが低く、リスク源の多いプロバイダ（例えば、ある市場分野ではビジネスパートナーであり、別の市場分野では競争相手となる）もいる。

アシュアランスのレベルは、必要な管理策が実装されていること、及び管理策の有効性に関する判断が信頼できるものであることを組織に納得させる、その他の多くの要因にも基づくことができる。例えば、確立された事業部門（line-of-business）の関係を通じて組織に提供される、認可された外部クラウドサービスによって、組織のリスク許容度の範囲内でサービスの信頼レベルが提供されることがある。最終的に、外部プロバイダのコンポーネント製品、システム、及びサービスの使用によって生じるリスクに対応する責任は、組織及び認可権限のある担当者が負うことになる。組織では、システムのセキュリティ又はプライバシーリスクに関連する問題を扱う場合には、外部プロバイダとの間で適切な*信頼の連鎖*が確立されていることが求められる。

サプライチェーンのリスクマネジメント戦略及び計画

組織は、 SCRM の戦略及び計画の詳細をどのように文書するかについて、柔軟性を有している。レベル 1 及びレベル 2（組織レベル及びミッション／ビジネスプロセスレベル）の SCRM 戦略の詳細は、組織の情報セキュリティプログラム計画、又は別の組織レベル及び／又はミッション／ビジネスプロセスレベルの SCRM 戦略に文書化することができる。レベル 3（情報システムレベル）の SCRM 計画の詳細は、情報システムセキュリティ計画又は別のシステムレベルの SCRM 計画に文書化することができる。SCRM 戦略のテンプレートは、[SP 800-161] で提供されている。

第 3 章

プロセス

リスクマネジメントフレームワークのタスクの実行

本章では、RMF を構成するステップ及び関連タスクと、そのようなタスクを実施する選択された個人又はグループ（定義された組織の役割）を説明する。組織は、リスクマネジメントの役割 [51] を、可能な限り常に、SDLC のために定義された補完的又は類似の役割に合わせ、ミッション及びビジネスファンクション（ビジネス機能）と一致させる。RMF タスクは、組織の SDLC プロセスと同時に、又はその一部として実行される。RMF タスクを SDLC プロセスと同時に実行することは、組織が情報セキュリティ及びプライバシーリスクの管理プロセスを SDLC プロセスに効果的に統合するのに役立つ。さらに、RMF で求められている期待されるアウトプット（例えば、セキュリティ及びプライバシー計画、アセスメント報告書、行動計画及びマイルストーン）は、組織内で実施されている SDLC プロセスから日常的に取得でき、RMF の実装のためだけに開発する必要はない可能性がある。

RMF と SDLC の連携

最善の RMF の実装とは、組織によって実行される日常的な SDLC プロセスと区別がつかないようなものである。つまり、RMF タスクは、SDLC プロセスで進行中の活動と密接に連携し、セキュリティ及びプライバシー保護を組織のシステムにシームレスに統合することを確実にする。そして、SDLC プロセスによって生成される成果物を最大限に活用して、組織の上級幹部による信頼できるリスクベースの意思決定を容易にするために必要な証拠を、認可パッケージで作成する。

RMF タスクの実装プロセスは、組織によって異なる場合がある。各タスクは順番に発生するが、リスクマネジメントプロセスの中には、初回のタスク実行とタスク再検討の間の反復サイクルの必要性を含め、この順番から逸脱する必要がある点が多く存在する可能性がある。例えば、管理策アセスメントの結果がシステム所有者及び共通管理策の提供者による一連の改善措置をもたらし、その結果、選択されている管理策の再アセスメントが必要となる可能性がある。管理策の監視によって、システム及びその運用環境に対する変更の追跡、情報セキュリティ及びプライバシー影響のアセスメント、管理策の再アセスメント、改善措置の実施、及びシステム及び組織のセキュリティ及びプライバシー態勢の報告というサイクルを生成することができる。

より効果的、効率的、又は費用対効果が高い場合には、順番に発生するというタスクの性質から逸脱する機会が他にもある場合がある。例えば、管理策アセスメントタスクは管理策の実装タスクの後に記載されているが、組織は、システムのセキュリティ計画及びプライバシー計画に記載されているすべての管理策の完全な実装に先立って、それらが実装されるとすぐに管理策のアセスメントを開始してもよい。管理策が実装された直後にアセスメントすると、組織は、（後で実装される可能性がある）システムのハードウェア、ファームウェア、又はソフトウェアコンポーネントに実装される管理策のアセスメントよりも先に、施設内の物理的及び環境的保護管理策をアセスメントすることになる場合がある。タスクの順序に関係なく、システムの運用を開始

[51] 附属書 D で、組織のリスクマネジメントと RMF の実行に関わる主要な参加者の役割及び責任を説明している。本出版物で定義されている多くのリスクマネジメント役割には、SDLC プロセスで定義されている対応する役割がある。

する前の最終的な活動は、認可権限のある担当者による、リスクの明確な受容である。

RMF のステップ及び関連タスクは、SDLC の適切なフェーズで、新規開発システム及び既存システムに適用できる。新規及び既存システムに対して、組織は、RMF の実行を準備するために、指定されたタスクが完了していることを確実にする。既存システムの場合、組織は、セキュリティ分類化及び（PII を処理する情報システムの場合は）プライバシーリスクアセスメントが完了しており適切であること、及び必要な管理策が選択され、テーラリングされ、実装されていることを確認する。

RMF のステップ及び関連タスクを既存システムに適用することは、組織のセキュリティ及びプライバシーリスクが効果的に管理されているかどうかを判断するためのギャップ分析の役割を果たすことができる。管理策の欠陥は、新規開発システムの場合と同様の方法で、RMF の実装、アセスメント、認可、及び監視のステップで対処することができる。ギャップ分析で欠陥が検出されず、現在有効な認可がある場合、組織は RMF の継続的監視ステップに直接移行できる。現在の認可が有効ではない場合には、組織はアセスメント、認可、及び監視の各ステップを通常の順序で続行する。

タスクの委任

各 RMF タスクの「*主たる*責任者」の節で規定されている役割は、タスクの完了を確実にする責任を負う。主たる責任を持つ役割は、タスクの「*詳解*」の節又は附属書 D で委任が具体的に禁止されている場合を除き、タスクを完了することも、タスクの完了を又は 1 人以上の*補助的な*役割にタスクの完了を委任してもよい。タスクの完了が委任される場合、そのタスクの主たる責任を持つ役割はタスクの完了に対して引き続き責任を負う。

RMF 実装を効率化するためのヒント

- 組織内で RMF を実行するための一貫した出発点を促進するために、組織レベル及びシステムレベルの*準備*ステップのタスクとアウトプットを使用する。
- 標準化され、一貫性があり、費用対効果の高いセキュリティ及びプライバシーケイパビリティ（能力）の継承を促進するために、*共通管理策*を最大限に活用する。
- 組織の認可の数を削減するために、適用可能な場合には*共有*又は*クラウドベース*のシステム、サービス、及びアプリケーションを最大限に活用する。
- セキュリティ及びプライバシー計画の策定速度を上げ、セキュリティ及びプライバシー計画の内容の一貫性を促進し、組織全体の脅威に対処するために、*組織的にテーラリングされた管理策ベースライン*を採用する。
- システムセキュリティエンジニアリングプロセスで作成されたセキュリティ及びプライバシー要件に基づいて、*組織が定義した管理策*を採用する。
- セキュリティ分類化、管理策の選択、アセスメント及び監視、及び認可プロセスを管理するために、*自動化されたツール*を最大限に活用する。
- 低インパクトシステムが、システム接続によってより高インパクトのシステムに悪影響を与える可能性がない場合には、*低インパクト*システムの労力とリソース支出のレベルを下げる。
- 構成設定を含む、標準化されたハードウェア／ソフトウェアの展開において、RMF の成果物（例えば、セキュリティ及びプライバシーのアセスメント結果）を最大限に*再利用*する。
- 不要なシステム、システム要素、及びサービスを排除し、*最小機能*の原則を採用することで、IT/OT インフラストラクチャの*複雑さ*を低減する。
- *継続的な認可*に移行し、*継続的な監視*アプローチを使用してコストを削減し、セキュリティ及びプライバシープログラムの効率を高める。

明確に定義されたセキュリティ及びプライバシー要件の策定

RMF は SDLC に基づくプロセスであり、情報システム又は組織のセキュリティ及びプライバシー要件が満たされることを確実にするのに役立てるために効果的に使用することができる。明確で一貫性があり、曖昧さのないセキュリティ及びプライバシー要件を定義することは、RMF の実行を成功させるための重要な要素である。要件は SDLC の早い段階で上級幹部と協力して定義され、取得及び調達プロセスに統合される。例えば、組織は[SP 800-160 v1]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、最初の一連のセキュリティ及びプライバシー要件を定義し、次に、この要件を満たすための一連の管理策*を選択できる。要件又は管理策は、組織がシステム、システムコンポーネント、又はサービスを取得する際に、提案依頼書又はその他の契約合意書に記載することができる。要件は、新しい機能が継続的に導入されるアジャイル開発方法論などを使用して、ライフサイクル全体で追加することもできる。

セキュリティ要件の識別、調整、及び競合を解消し、その後、組織のセキュリティ管理策の選択の情報を提供するために、NIST *サイバーセキュリティフレームワーク*[NIST CSF]（即ち、コア、プロファイル）を使用することもできる。サイバーセキュリティフレームワークプロファイルは、サイバーセキュリティ活動と組織のミッション／ビジネス目標の間のリンクを提供することができ、RMF 全体でのリスクベースの意思決定をサポートする。プロファイルは、管理策の選択及びテーラリング活動の情報を提供するための出発点として使用してもよいが、適切な管理策が選択されていることを確実にするためには、さらなる評価が必要となる。組織によっては、セクター、業界、又は組織全体の要件を識別、調整、及び競合を解消する NIST *システムセキュリティエンジニアリング*の出版物と組み合わせてサイバーセキュリティフレームワークを使用することを選択してもよい。その後、要件をさらに洗練させ、組織の業務、資産、個人を保護するのに役立つ統合的信頼性のあるセキュアなソリューションを得るために、システムエンジニアリングアプローチを採用する。

* プライバシー管理策の選択及びプライバシーリスクの管理についての具体的なガイダンスについては、第 2.3 節を参照。

組織及びシステムの準備

準備によって、リスクマネジメントプロセスの効率的、効率的、及び費用対効果の高い実行を実現できる。*準備*ステップの主な目的には、以下が含まれる。

- 経営トップ及び経営幹部と、システム所有者及びオペレータの間のより良いコミュニケーションを促進する。
  - 組織の優先順位を、システムレベルでのリソースの割り振り及び優先順位付けに合わせる。
  - 規定された組織のリスク許容度の範囲内での管理策の選択及び実装に関して、受容可能な限度を伝える。
- 各システム所有者の作業負荷と、システム開発及び保護のコストを軽減するために、共通管理策の組織全体での識別及び組織的にテーラリングされた管理策ベースラインの策定を促進する。
- エンタープライズアーキテクチャの概念及びモデルを適用して、システム、アプリケーション、及びサービスを統合、標準化、及び最適化することで、IT インフラストラクチャの複雑さを軽減する。
- より高いレベルの保護を必要とする高価値資産([OMB M-19-03]で定義)を識別し、優先順位付けし、リソースを投入する。
- システム固有のタスクに対するシステムの準備を促進する。

これらの目的が達成されると、組織の情報技術のフットプリント及び攻撃対象領域を大幅に削減し、IT 近代化の目的を促進し、保護戦略を最も重要な資産及びシステムに集中させるためのセキュリティ及びプライバシー活動に優先順位が付けられるようになる。

最後に、組織レベルでの準備ステップの一部のタスクはオプションとして指定される。これらのタスクは RMF の実装を、より効果的、効率的、及び費用対効果の高いものにするための追加オプションを組織に提供するために含まれている。

3.1 準備 [52]

目的

*準備*ステップの目的は、組織が*リスクマネジメントフレームワーク*を使用してセキュリティ及びプライバシーリスクを管理するための準備を支援するために、組織における組織レベル、ミッション及びビジネスプロセスレベル、並びに情報システムレベルでの重要な活動を実施することである。

準備タスク – 組織レベル [53]

表 1 は、*組織*レベルでの RMF *準備*ステップのタスクと期待される成果の概要を示している。また、適用可能なサイバーセキュリティフレームワークの構成要素も示している。

表 1:準備タスクと成果 – 組織レベル

タスク	成果
タスク P-1 リスクマネジメント役割	・リスクマネジメントフレームワークを実行する個人が識別され、そのための主要な役割が割り当てられている。 [*サイバーセキュリティフレームワーク*: **ID.AM-6、ID.GV-2**]
タスク P-2 リスクマネジメント戦略	・組織のリスク許容度の決定及び表明が含まれた組織のリスクマネジメント戦略が確立されている。 [*サイバーセキュリティフレームワーク*: **ID.RM、ID.SC**]
タスク P-3 リスクアセスメント – 組織	・組織全体のリスクアセスメントが完了している、又は既存のリスクアセスメントが更新されている。 [*サイバーセキュリティフレームワーク*: **ID.RA、ID.SC-2**]
タスク P-4 組織的にテーラリングされた管理策ベースライン及びサイバーセキュリティフレームワークプロファイル(オプション)	・組織にテーラリングされた管理策ベースライン及び／又はサイバーセキュリティフレームワークプロファイルが確立され、利用可能になっている。 [*サイバーセキュリティフレームワーク*: **プロファイル**]
タスク P-5 共通管理策の識別	・組織システムによって継承可能な共通管理策が識別、文書化、及び公開されている。
タスク P-6 インパクトレベルの優先順位付け(オプション)	・インパクトレベルが同じ組織システムの優先順位付けが実施されている。 [*サイバーセキュリティフレームワーク*: **ID.AM-5**]
タスク P-7 継続的監視戦略 –組織	・管理策の有効性を監視するための組織全体の戦略が策定され、実装されている。 [*サイバーセキュリティフレームワーク*: **DE.CM、ID.SC-4**]

RMF のタスク、責任、及び補助的な役割の概要表へのクイックリンク。

[52] *準備*ステップは、セキュリティ、プライバシー、及びサプライチェーンのプログラムで既に実施されている活動を活用して、費用対効果の高い一貫したリスクマネジメントプロセスを組織全体で実行できるようにするために、組織全体のガバナンスと適切なリソースを確保することの重要性を強調することを意図している。

[53] 使いやすさのため、準備活動は組織レベルの準備と情報システムレベルの準備に分類されている。

リスクマネジメント役割

タスク P-1　セキュリティ及びプライバシーリスクマネジメントに関する特定の役割を識別し、個人に割り当てる。

潜在的なインプット：組織のセキュリティ及びプライバシーポリシー及び手順、組織図。

期待されるアウトプット：文書化されたリスクマネジメントフレームワーク役割の割り当て。

主たる責任者：政府機関の長、最高情報責任者、政府機関のプライバシー保護責任者。

補助的な役割を果たす者：認可権限のある担当者又は認可権限のある担当者による指定代理人、リスクマネジメント担当責任者又はリスク管理者（機能）、政府機関の情報セキュリティ責任者。

詳解：リスクマネジメントプロセスの主要な参加者の役割と責任については、附属書 D に記載されている。役割と責任には、必要に応じて、組織の内部又は外部の担当者を含めてもよい。組織には異なるミッション、機能、及び組織構造があるため、リスクマネジメント役割の命名規則や、組織内の担当者間での具体的な責任の割り振り方法が異なる場合がある（例えば、複数の担当者が 1 つの役割を担う、又は 1 人の担当者が複数の役割を兼任する）。いずれの場合でも、基本的なリスクマネジメント機能は同じである。組織は、同じ個人を複数のリスクマネジメント役割に割り当てる場合には、利益相反がないことを確実にする。例えば、認可権限のある担当者は、自らが認可するシステム又は共通管理策のシステム所有者又は共通管理策の提供者の役割を担うことはできない。さらに、セキュリティ及びプライバシーの複数の役割を組み合わせる場合、2 つの分野が異なる専門知識を必要とする場合があり、状況によっては優先順位が競合する可能性があるため、注意が必要である。一部の役割（例えば、管理策アセッサー、リスク管理者（機能）、システム管理者）は、個人ではなくグループ又はオフィスに割り振られる場合がある。

参考文献：[SP 800-160 v1]（人材管理プロセス）、[SP 800-181]、[NIST CSF]（コア[識別機能]）。

リスクマネジメント戦略

タスク P-2　リスク許容度の決定を含む、組織のリスクマネジメント戦略を確立する。

潜在的なインプット：組織のミッションステートメント、組織のポリシー、組織のリスクの前提条件、制約条件、優先順位、及びトレードオフ。

期待されるアウトプット：リスクマネジメント戦略及び、情報セキュリティ及びプライバシーリスクを含む、リスク許容度ステートメント。

主たる責任者：政府機関の長。

補助的な役割を果たす者：リスクマネジメント担当責任者又はリスク管理者（機能）、最高情報責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者。

詳解：リスク許容度とは、組織が受容可能なリスク又は不確実性の度合いである。リスク許容度は、組織のリスクマネジメントプロセスのすべての部分に影響し、組織全体で上級幹部又は管理職によって行われるリスクマネジメントの決定に直接影響を与え、これらの決定に重要な制約を与える。リスクマネジメント戦略は、セキュリティ及びプライバシーリスクをどのように構成、アセスメント、対応、及び監視するかを含め、リスクベースの意思決定を導き、情報を提供する。リスクマネジメント戦略は、1 つの文書で構成される場合もあれば、セキュリティ及びプライバシーリスクマネジメントに関する個別の文書で構成される場合もある[54]。リスクマネジメント戦略は、投資及び運用に関する決定に使用される脅威、前提条件、制約条件、優先事項、トレードオフ、及びリスク許容度を明確にする。この戦略には、組織の業務、組織の資産、個人、他の組織、及び国家に対するセキュリティ及びプライバシーリスク（サプライチェーンリスクを含む）を、上級幹部及び管理職がどのように管理するかについての戦略レベルの決定及び考慮事項が含まれる。リスクマネジメント戦略には、組織のリスク許容度の表現、受容可能なリスクアセスメント方法論及びリスク対応戦略、組織全体でセキュリティ及びプライバシーリスクを一貫して評価するプロセス、及び長期にわたってリスクを監視するためのアプローチが含まれる。
組織がリスクマネジメント戦略、ポリシー、手順、及びプロセスを定義及び実装する際には、SCRM の考

[54] 個別のサプライチェーンのリスクマネジメント戦略文書は、サプライチェーンのリスクマネジメント計画と呼ばれる。

慮事項を含めることが重要である。セキュリティ及びプライバシーリスクマネジメント戦略は、セキュリティ及びプライバシープログラムを、組織のエンタープライズリスクマネジメント戦略で設定されたマネジメント管理システムと結び付ける[55]。

参考文献:[SP 800-30]、[SP 800-39](組織レベル)、[SP 800-160 v1](リスクマネジメント、意思決定マネジメント、品質アシュアランス、品質マネジメント、プロジェクトアセスメント及び管理策プロセス)、[SP 800-161]、[IR 8062]、[IR 8179](重要度分析プロセス B)、[NIST CSF](コア[識別機能])。

リスクアセスメント – 組織

タスク P-3 組織全体のセキュリティ及びプライバシーリスクをアセスメントし、リスクアセスメントの結果を継続的に更新する。

潜在的なインプット:リスクマネジメント戦略、ミッション又はビジネスの目標、最新の脅威情報、システムレベルのセキュリティ及びプライバシーリスクアセスメント結果、サプライチェーンのリスクアセスメント結果、以前の組織レベルのセキュリティ及びプライバシーリスクアセスメント結果、情報共有合意書又は覚書、継続的監視からのセキュリティ及びプライバシー情報。

期待されるアウトプット:組織レベルのリスクアセスメント結果。

主たる責任者: リスクマネジメント担当責任者又はリスク管理者(機能)、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者。

補助的な役割を果たす者: 最高情報責任者、ミッション又はビジネスオーナー、認可権限のある担当者又は認可権限のある担当者による指定代理人。

詳解:組織レベルのリスクアセスメントでは、システムレベルのリスクアセスメント結果、継続的監視、及び組織に関連するあらゆる戦略的リスクの考慮事項から得られた情報を集約して活用する。組織は、情報システムの運用及び使用、他の内部及び外部の所有システムとの情報交換及び接続、並びに外部プロバイダの利用によるリスクの全体を考慮する。例えば、組織は、同じネットワーク上に存在する様々なインパクトレベルのエンタープライズアーキテクチャ及び情報システムに関連するリスクをレビューしたり、より高インパクトのシステムが低インパクトのシステム又は外部プロバイダによって運用及びメンテナンスされているシステムから分離されているかどうかをレビューしたりする場合がある。また、組織は、組織内に存在する可能性のある環境の多様性(例えば、異なるミッション/ビジネスプロセスを提供する異なる拠点)を考慮したり、リスクアセスメントにおいてそのような多様性の説明責任を負う必要性を考慮したりする場合もある。組織のサプライチェーンのリスクアセスメントも実施される場合がある。リスクアセスメントの結果は、組織がサイバーセキュリティフレームワークプロファイルを確立するのに役立つ場合がある。

参考文献:[SP 800-30]、[SP 800-39](組織レベル、ミッション/ビジネスプロセスベル)、[SP 800-161]、[IR 8062]。

[55] [OMB A-123]を参照。

組織的にテーラリングされた管理策ベースライン及びサイバーセキュリティフレームワークプロファイル（オプション）

タスク P-4 組織的にテーラリングされた管理策ベースライン、及び／又はサイバーセキュリティフレームワークプロファイルを確立、文書化、及び公開する。

潜在的なインプット：組織的にテーラリングされた管理策ベースラインの使用を指示する、文書化されたセキュリティ及びプライバシー要件、ミッション又はビジネス目標、エンタープライズアーキテクチャ、セキュリティアーキテクチャ、プライバシーアーキテクチャ、システムレベルのリスクアセスメント結果、共通管理策の提供者及び継承に利用可能な共通管理策のリスト、NIST Special Publication 800-53B 管理策ベースライン。[56]

期待されるアウトプット：承認又は指示された組織的にテーラリングされた管理策ベースラインのリスト、[NIST CSF]プロファイル。

主たる責任者：ミッション又はビジネスオーナー、リスクマネジメント担当責任者又はリスク管理者（機能）。

補助的な役割を果たす者：最高情報責任者、認可権限のある担当者又は認可権限のある担当者による指定代理人、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者。

詳解：リスクを軽減するための一連の特殊な管理策に対する組織のミッション又はビジネスニーズに対処するため、組織全体で使用できる組織的にテーラリングされた管理策ベースラインを策定してもよい[57]。組織的にテーラリングされた管理策ベースラインは、[SP 800-53B]で説明されている確立された管理策ベースラインから得られた、完全に規定された一連の管理策、拡張管理策、及び補足ガイダンスを提供する。テーラリングプロセスは、[SP 800-160 v1]で説明されている要件エンジニアリングプロセスによっても導かれ、情報を得ることができる。組織は、[SP 800-53B]の初期の管理策ベースラインを作成するために使用された特定の前提条件との相違がある場合、テーラリングされた管理策ベースラインの概念を使用できる。これには、例えば、組織に特定のセキュリティ又はプライバシーリスクがある場合、特定のミッション又はビジネスニーズがある場合、又は初期ベースラインで対処されていない環境で運用することを計画している場合が含まれる。

組織的にテーラリングされた管理策ベースライン及びオーバーレイは、リスクに見合った情報保護を継続しながら、組織の要件に対応する管理策を追加又は除外する機会を提供することで、NIST 管理策ベースラインを補完する。組織は、管理策の適用可能性を記述すること、及び特定の技術、ミッション又はビジネスファンクション、業務、システム、運用環境、及び運用モードの種類、及び法的又は規制上の要件の解釈を提供することによって管理策ベースラインをカスタマイズするために、テーラリングされたベースライン及びオーバーレイを使用できる。複数のカスタマイズされたベースラインは、異種システムを持つ組織（例えば、運用又は処理特性が異なるシステム、又はミッション又はビジネス特性が異なるシステムを保守している組織）に役立つ場合がある。

組織的にテーラリングされたベースラインは、特定の利益共同体が同意する管理策及び拡張管理策における割り当て又は選択ステートメントに対する組織が定める管理策パラメータの値を確立することができ、また、必要に応じて補足ガイダンスを拡張することもできる。テーラリングされたベースラインは、[SP 800-53B]で識別されているベースラインより厳しくても厳しくなくてもよく、複数のシステムに適用される。

組織の外部で策定されたテーラリングされたベースラインは、特定の法律、大統領令、指令、規制、ポリシー、又は規格によって使用が義務付けられている場合もある。状況によっては、テーラリングされたベースラインの開発者又はテーラリングされたベースラインの発行機関によって、テーラリング活動が制限または限定される場合がある。

---

[56] NIST Special Publication 800-53（Revision 5）では、管理策カタログと、これまで同出版物に含まれていた管理策ベースラインを区別している。新しい関連出版物 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*』（*Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations*）は、推奨されるベースラインを定義している。NIST Special Publication 800-53B は、RMF の関連タスク全体で参照されている。

[57] テーラリングされた管理策ベースラインは、*オーバーレイ*と呼ばれる場合もある。 オーバーレイは、利益共同体（この場合は組織）にサービスを提供するテーラリングされたベースラインであるため、組織的にテーラリングされた管理策ベースラインは、組織全体のオーバーレイに似ている。

テーラリングされたベースライン（又はオーバーレイ）は、クラウド及び共有システム、サービス、及びアプリケーション、産業用制御システム、プライバシー、国家安全保障システム、兵器又は宇宙ベースのシステム、高価値資産、[58] モバイルデバイスマネジメント、連邦政府公開鍵基盤、及びプライバシーリスクのための利益共同体によって策定されてきた。
また、組織は、1 つ以上のサイバーセキュリティフレームワーク*プロファイル*を策定することからも恩恵を受けることができる場合もある。サイバーセキュリティフレームワークプロファイルは、サイバーセキュリティの成果を組織のミッション又はビジネスの要件、リスク許容度、及びリソースに合わせるために、フレームワークコアのサブカテゴリを使用する [59]。組織レベル又はミッション／ビジネスプロセスレベルでのサイバーセキュリティの成果の優先順位付けされたリストは、システムレベルでの一貫性があるリスクベースの意思決定を促進する上で役立つ可能性がある。適用されるサイバーセキュリティフレームワークプロファイルで識別されたサブカテゴリは、前述のテーラリングされた管理策ベースラインの策定を導き、情報を提供することにも使用できる。

参考文献：[SP 800-53]、[SP 800-53B]、[SP 800-160 v1]（ビジネス又はミッション分析及びステークホルダーのニーズ及び要件定義プロセス）、[NIST CSF]（コア、プロファイル）。

共通管理策の識別

タスク P-5 組織システムによる継承に利用可能な、組織全体の共通管理策を識別、文書化、及び公開する。

潜在的なインプット：文書化されたセキュリティ及びプライバシー要件、既存の共通管理策の提供者及び関連するセキュリティ及びプライバシー計画、情報セキュリティ及びプライバシープログラム計画、組織レベル及びシステムレベルのセキュリティ及びプライバシーリスクアセスメント結果。

期待されるアウトプット：共通管理策の提供者及び継承に利用可能な共通管理策のリスト、共通管理策の実装の説明（インプット、期待される動作、及び期待されるアウトプットを含む）を提供するセキュリティ及びプライバシー計画（又は同等の文書）。

主たる責任者：政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者。

補助的な役割を果たす者：ミッション又はビジネスオーナー、リスクマネジメント担当責任者又はリスク管理者（機能）、最高情報責任者、認可権限のある担当者又は認可権限のある担当者による指定代理人、共通管理策の提供者、システム所有者。

詳解：共通管理策とは、1 つ以上の情報システムによる継承に利用可能な管理策である。[60]
共通管理策には、例えば、物理的及び環境的保護の管理策、システム境界及び監視の管理策、職員のセキュリティの管理策、ポリシー及び手順、取得の管理策、アカウント及びアイデンティティ管理の管理策、監査ログ及び説明責任の管理策、又は一般の人々からのプライバシーに関する問い合わせを受ける際の苦情管理の管理策など、任意の[SP 800-53]の管理策ファミリーの管理策を含めることができる。組織は一連の共通管理策を識別、選択し、これらの管理策を共通管理策の提供者として指定された組織エンティティに割り振る。共通管理策は、ホストする場所、システムアーキテクチャ、及び組織の構造など、様々な要因によって異なる場合がある。組織全体の共通管理策のリストでは、これらの要素が考慮される。共通管理策はまた、組織の様々なレベル（例えば、法人、部門、又は政府機関レベル、局又はサブコンポーネントレベル、又は個々のプログラムレベル）でも識別することができる。組織は、情報システムによって継承可能な共通管理策のリストを 1 つ以上作成してもよい。ある要件が、1 つの共通管理策では完全には満たされない場合がある。そのような場合、その共通管理策はハイブリッド管理策と見なされ、管理策の要件のどの部分が継承のためにこの共通管理策によって提供され、どの部分がシステムレベルで提供されるかを規定することを含め、組織によってそのように注記される。

[58] [OMB M-19-03]を参照。

[59] [NIST CSF]、第 2.3 節を参照。

[60] 共通管理策は、組織のシステムによる継承に利用可能になる前に、指定された認可権限のある担当者によって*認可*される。各種認可の説明については、附属書 F を参照。

共通管理策の提供元が複数ある場合、組織は共通管理策の提供者（即ち、管理策を提供するのは誰で、例えば共有サービス、特定のシステム、又は特定の種類のアーキテクチャ内など、どのような場所を介して提供するか）、及び、どのシステム又はシステムの種類が管理策を継承できるかを規定する。共通管理策リストはシステム所有者に伝達されるため、システム所有者は、継承によって組織から利用可能なセキュリティ及びプライバシーケイパビリティを認識する。システム所有者は、システムによって継承される共通管理策をアセスメントしたり、共通管理策の実装の詳細を文書化したりする必要はない。これは共通管理策の提供者の責任である。同様に、共通管理策の提供者は、提供する共通管理策を継承するシステムのシステムレベルの詳細を可視化する必要はない。

リスクアセスメントの結果は、共通管理策を識別する際に、継承可能な管理策が組織のシステム及びその運用環境のセキュリティ及びプライバシー要件を満たしているかどうかを判断するために使用できる（潜在的な単一障害点の識別を含む）。組織が提供する共通管理策が、これらの管理策を継承する情報システムにとって不十分であると判断された場合、システム所有者は、システムに必要な保護を得られるようにシステム固有の管理策又はハイブリッド管理策で共通管理策を補完するか、組織の確認と承認を得てより大きなリスクを受容することができる。

共通管理策の提供者は、共通管理策として指定された管理策を実装、アセスメント、及び監視するためのRMF ステップを実行する。共通管理策の提供者は、共通管理策が情報システム内に存在する場合、システム所有者になる場合もある。組織は、共通管理策の認可権限のある担当者として上級職員又は管理職を選定する。政府機関のプライバシー保護責任者は、共通プライバシー管理策を指定する責任、及び組織のプライバシープログラム計画にそれらを文書化する責任を負う。認可権限のある担当者は、組織のシステムに継承された共通管理策の使用によって生じるセキュリティ及びプライバシーリスクを受容する責任を負う。

共通管理策の提供者は、共通管理策をセキュリティ及びプライバシー計画（又は組織によって規定される同等の文書）に文書化すること、共通管理策が実装され、資格を持つアセッサーによって有効性が確実にアセスメントされ、アセスメントの所見がアセスメント報告書に確実に文書化されること、受容できない欠陥があると判断され、改善の対象となった共通管理策の行動計画及びマイルストーンを作成すること、指定された認可権限のある担当者から共通管理策の認可を受けること、及び管理策の有効性を継続的に監視することの責任を負う。共通管理策の計画、アセスメント報告書、及び行動計画及びマイルストーン（又はこれらの情報の要約）は、システム所有者が利用できるようになっており、認可権限のある担当者は、共通管理策を継承するシステムの認可の決定を導き、情報を提供するために使用することができる。共通管理策の認可に関する情報については、タスク R-4 及び附属書 F を参照。

参考文献：[SP 800-53]。

インパクトレベルの優先順位付け（オプション）[61]

タスク P-6 インパクトレベルが同じ組織システムに優先順位を付ける。

潜在的なインプット：組織のシステムのセキュリティ分類化情報、システムに関する記述、組織レベル及びシステムレベルのリスクアセスメント結果、ミッション又はビジネス目標、サイバーセキュリティフレームワークプロファイル。

期待されるアウトプット：低インパクト、中インパクト、及び高インパクトのサブカテゴリに優先順位が付けられた組織のシステム。

主たる責任者：リスクマネジメント担当責任者又はリスク管理者（機能）。

[61] 組織は、より細かなインパクトの指定のために組織的にテーラリングされた管理策ベースライン、例えば、低～中レベルのシステムと高～中レベルのシステムを対象とした組織的にテーラリングされた管理策ベースラインを策定するために、このタスクをオプションの RMF の*準備 – 組織レベル*ステップのタスク P4 と組み合わせて使用できる。

補助的な役割を果たす者: 政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、ミッション又はビジネスオーナー、システム所有者、最高情報責任者、認可権限のある担当者又は認可権限のある担当者による指定代理人。

詳解:このタスクは、組織のシステムの分類が完了した後にのみ実行される(タスク C1 を参照)。このタスクでは、組織が最初に、[FIPS 199]及び[FIPS 200]に従って分類された各情報システムに最高水準の概念を適用する必要がある [62]。最高水準の概念を適用すると、結果としてシステムは低インパクト、中インパクト、又は高インパクトとして指定される。リスクベースの意思決定のためにシステムのインパクトの指定をさらに細かくしたい組織は、各インパクトレベル内でシステムの優先順位付けを行うために、このタスクを使用することができる [63]。例えば、組織は、それぞれの中インパクトシステムを、低 – 中インパクトシステム、中 – 中インパクトシステム、及び高 – 中インパクトシステムという 3 つの新しいサブカテゴリのいずれかに割り当てることにより、中インパクトシステムに優先順位を付けてもよい。高 – 中インパクトシステムは中 – 中インパクトシステムよりも優先順位が高く、低 – 中インパクトシステムは中 – 中インパクトシステムよりも優先順位が低い。中インパクトシステムの優先順位付けは、識別されたリスクに対応する際に、管理策の選択と管理策ベースラインのテーラリングに関して、より多くの情報に基づいた決定を行う機会を組織に与える。

インパクトレベルの優先順位付けは、組織のミッション又はビジネスの業務にとって重要又は不可欠なシステムを決定するためにも使用できるため、組織は複雑さ、集約、及びシステムの相互接続の要因に焦点を当てることができる。このようなシステムは、例えば、高インパクトシステムを*低 – 高インパクト*システム、*中 – 高インパクト*システム、及び*高 – 高インパクト*システムに優先順位付けすることによって識別することができる。インパクトレベルの優先順位付けはどの組織レベルでも実施でき、個々のシステム所有者から報告されたセキュリティ分類化データに基づいている。インパクトレベルの優先順位付けは、追加のより細かなインパクトレベルに対応する適切な一連の管理策を指定するために、組織的にテーラリングされた管理ベースラインの策定を必要とする場合がある。

組織は、インパクトレベルの優先順位付けタスクをサポートするために、サイバーセキュリティフレームワーク*プロファイル*を使用できる。適用可能なサイバーセキュリティフレームワークプロファイルで定義されたミッション及びビジネス目標、及び優先順位付けされた成果は、同じインパクトレベルのシステム間の相対的な優先順位を区別するのに役立つ。サイバーセキュリティフレームワークプロファイルは、組織のミッション／ビジネス目標の優先順位に基づいて編成することができ、これらの目標には、相対的な優先順位が割り当てられる。例えば、人と環境の安全の目標が、プロファイルのコンテキストに関連する 2 つの最も重要な目標である場合がある。この例では、タスク P-6 を実行する際に、人の安全という目標に関連するシステムには、同じインパクトレベルだが人の安全という目標には関連しないシステムよりも高い優先順位が付けられる場合がある。

参考文献:[FIPS 199]、[FIPS 200]、[SP 800-30]、[SP 800-39](組織及びシステムレベル)、[SP 800-59]、[SP 800-60 v1]、[SP 800-60 v2]、[SP 800-160 v1](システム要件の定義プロセス)、[IR 8179](重要度分析プロセス B)、[CNSSI 1253]、[NIST CSF](コア[識別機能]、プロファイル)。

継続的監視戦略 – 組織

タスク P-7 管理策の有効性を継続的に監視するための組織全体の戦略を策定し、実装する。

潜在的なインプット:リスクマネジメント戦略、組織レベル及びシステムレベルのリスクアセスメント結果、組織のセキュリティ及びプライバシーポリシー。

期待されるアウトプット:実装された組織の継続的監視戦略。

主たる責任者: リスクマネジメント担当責任者又はリスク管理者(機能)。

[62] 国家安全保障システムを運用する組織は、*最高水準*の概念を適用しない[CNSSI 1253] の分類ガイダンスに従う。
[63] 組織は、[FIPS 199] で定義されているインパクトレベルにさらに細かさを追加するために、組織が定める代替の分類化アプローチの使用を選択することもできる。

補助的な役割を果たす者: 最高情報責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、ミッション又はビジネスオーナー、システム所有者、認可権限のある担当者又は認可権限のある担当者による指定代理人。

詳解:リスクマネジメントの重要な側面は、組織全体のセキュリティ及びプライバシー態勢、及び組織のシステム内に実装された、又は組織のシステムによって継承された管理策の有効性を継続的に監視する能力である。[64] このような監視を効率的かつ費用対効果の高い方法で実行するためには、組織全体の継続的監視戦略が不可欠である。継続的監視戦略には、例えば、サプライヤの外国人による所有、支配、又は影響(FOCI:Foreign Ownership, Control, or Influence)の定期的なレビュー、在庫予測の監視、又はサプライヤの継続的監査の要求など、サプライチェーンリスクの考慮事項を含めることもできる。堅牢で包括的な継続的監視プログラムの実装は、組織が情報システムのセキュリティ及びプライバシー態勢を理解するのに役立つ。また、初期のシステム又は共通管理策の認可後の、継続的な認可を容易にする。これには、ミッション又はビジネスファンクション、ステークホルダー、技術、脆弱性、脅威、リスク、及びシステム、コンポーネント、又はサービスのサプライヤの変化の可能性が含まれる。

組織の継続的監視戦略は、組織、ミッション/ビジネスプロセス、及び情報システムの各レベルでの監視要件に対処する。継続的監視戦略では、組織全体で実装された管理策の最小監視頻度を識別し、管理策の継続的なアセスメントアプローチを定義し、継続的なアセスメントの実施方法(例えば、自動化ツールの使用、及び管理、監視を自動化できない管理策の継続的なアセスメントの指示)を記述する。継続的監視戦略では、報告書の受領者を含め、セキュリティ及びプライバシーに関する報告の要件を定義してもよい。管理策監視の最小頻度を決定する基準は、組織の担当者(例えば、リスクマネジメント担当責任者又はリスク管理者(機能)、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、最高情報責任者、システム所有者、共通管理策の提供者、認可権限のある担当者又は指定代理人)と協力して確立される。組織のリスクアセスメントは、監視の頻度を導き、知らせるために使用できる。

自動化の使用は、監視プロセスの一環としての管理策アセスメントの頻度及び量の増加を促進する。自動化ツール及びサポートデータベースを使用した継続的な管理策の監視は、情報システムのほぼリアルタイムのリスクマネジメントを容易にし、継続的な認可及びリソースの効率的な使用をサポートする。リスクマネジメント担当責任者又はリスク管理者(機能)は、管理策の監視の最小頻度を含む継続的監視戦略を承認する。

参考文献:[SP 800-30]、[SP 800-39](組織、ミッション又はビジネスプロセス、システムレベル)、[SP 800-53]、[SP 800-53A]、[SP 800-137]、[SP 800-161]、[IR 8011 v1]、[IR 8062]、[NIST CSF](コア[識別、検知機能])、[CNSSI 1253]。

ミッション/ビジネスプロセス(レベル 2)の考慮事項

ミッション/ビジネスプロセスの考慮事項は、RMF の*準備 – 組織レベル*ステップ及び RMF の*準備 – システムレベル*ステップで、ミッション/ビジネスプロセスの懸念事項を規定し、主な役割又は補助的な役割のミッション又はビジネスオーナーを識別し、ミッション又はビジネス目標を識別することにより、対処される。RMF の*準備 – システムレベル*ステップのタスク P-8 及びタスク P-9 は、システムレベル特有の焦点で実施されるミッション/ビジネスプロセスレベルのタスクである。

[64] 管理策の有効性の監視は、管理策アセスメントの一種である。[SP 800-53A]、[SP 800-137]、及び[IR 8011 v1]はそれぞれ、監視、管理策の有効性アセスメントの実施、及び管理策の有効性アセスメントの自動化に関する追加情報を提供している。

準備タスク – システムレベル

表 2 は、*システムレベル*での RMF の*準備*ステップのタスク及び期待される成果の概要を示している。また、適用可能なサイバーセキュリティフレームワークの構成要素も示している。

表 2:準備タスクと成果 – システムレベル

タスク	成果
タスク P-8 ミッション又はビジネスの焦点	· システムがサポートすることを意図しているミッション、ビジネスファンクション、及びミッション／ビジネスプロセスが識別されている。 [*サイバーセキュリティフレームワーク*: **プロファイル、実装ティア、ID.BE**]
タスク P-9 システムステークホルダー	· システムに利害関係を有するステークホルダーが識別されている。 [*サイバーセキュリティフレームワーク*: **ID.AM、ID.BE**]
タスク P-10 資産の識別	· ステークホルダーの資産が識別され、優先順位が付けられている。 [*サイバーセキュリティフレームワーク*: **ID.AM**]
タスク P-11 認可境界	· 認可境界(即ち、システム)が決定されている。
タスク P-12 情報の種類	· システムによって処理、保存、及び伝送される情報の種類が識別されている。 [*サイバーセキュリティフレームワーク*: **ID.AM-5**]
タスク P-13 情報ライフサイクル	· 情報ライフサイクルのすべての段階が、システムによって処理、保存、又は伝送される情報の種類ごとに識別され、理解されている。 [*サイバーセキュリティフレームワーク*: **ID.AM-3、ID.AM-4**]
タスク P-14 リスクアセスメント – システム	· システムレベルのリスクアセスメントが完了しているか、既存のリスクアセスメントが更新されている。 [*サイバーセキュリティフレームワーク*: **ID.RA、ID.SC-2**]
タスク P-15 要件の定義	· セキュリティ及びプライバシー要件が定義され、優先順位が付けられている。 [*サイバーセキュリティフレームワーク*: **ID.GV、PR.IP**]
タスク P-16 エンタープライズアーキテクチャ	· エンタープライズアーキテクチャ内でのシステムの配置が決定されている。
タスク P-17 要件の割り振り	· セキュリティ及びプライバシー要件が、システム及びシステム運用環境に割り振られている。 [*サイバーセキュリティフレームワーク*: **ID.GV**]
タスク P-18 システムの登録	· 管理、説明責任、調整、及び監督の目的でシステムが登録されている。 [*サイバーセキュリティフレームワーク*: **ID.GV**]

RMF のタスク、責任、及び補助的な役割の概要表へのクイックリンク。

ミッション又はビジネスの焦点

タスク P-8　システムがサポートすることを意図しているミッション、ビジネスファンクション、及びミッション／ビジネスプロセスを識別する。

潜在的なインプット:組織のミッションステートメント、組織のポリシー、ミッション／ビジネスプロセス情報、システムステークホルダー情報、サイバーセキュリティフレームワークプロファイル、提案依頼書又は他の取得文書、運用の概念。

期待されるアウトプット:システムでサポートする予定のミッション、ビジネスファンクション、及びミッション／ビジネスプロセス。

主たる責任者: ミッション又はビジネスオーナー。

補助的な役割を果たす者: 認可権限のある担当者又は認可権限のある担当者による指定代理人、システム所有者、情報所有者又は情報管理者、最高情報責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者。

システム開発ライフサイクルのフェーズ: 新規 – 開始(概念／要件の定義)。
既存 – 運用／保守。

詳解:組織のミッション又はビジネスファンクションは、これらのミッション及びビジネスファンクションを実施するために作成されるミッション又はビジネスプロセスの設計と開発に影響を与える。ミッション及びビジネスファンクションの優先順位付けは、投資戦略、資金調達の決定、リソースの優先順位付け、及びリスク決定を推進する—したがって、既存のエンタープライズアーキテクチャと、関連するセキュリティ及びプライバシーアーキテクチャの開発に影響を与える。システムのセキュリティ及びプライバシーの観点から組織のミッション、ビジネスファンクション、及びミッション／ビジネスプロセスをより詳しく理解するために、ステークホルダーから情報が引き出される。

参考文献:[SP 800-39](組織及びミッション／ビジネスプロセスレベル)、[SP 800-64]、[SP 800-160 v1](ビジネス又はミッション分析、ポートフォリオマネジメント、及びプロジェクト計画プロセス)、[NIST CSF](コア[識別機能])、[IR 8179](重要度分析プロセス B)。

システムステークホルダー

タスク P-9 システムの設計、開発、実装、アセスメント、運用、保守、又は廃棄に利害関係を有するステークホルダーを識別する。

潜在的なインプット:組織のミッションステートメント、ミッション又はビジネス目標、システムでサポートする予定のミッション、ビジネスファンクション、及びミッション／ビジネスプロセス、他のミッション／ビジネスプロセスの情報、組織のセキュリティ及びプライバシーポリシー及び手順、組織図、システムに利害関係があり、システムの意思決定の責任を負う個人又はグループ(内部又は外部)に関する情報。

期待されるアウトプット:システムステークホルダーのリスト。

主たる責任者: ミッション又はビジネスオーナー、システム所有者。

補助的な役割を果たす者: 最高情報責任者、認可権限のある担当者又は認可権限のある担当者による指定代理人、情報所有者又は情報管理者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、最高取得責任者。

システム開発ライフサイクルのフェーズ: 新規 – 開始(概念／要件の定義)。
既存 – 運用／保守。

詳解:ステークホルダーには、システムのライフサイクル—システムの設計、開発、実装、配送、運用、及び維持—を通じてシステムに利害関係を有する個人、組織、又は代表者が含まれる。また、サプライチェーンのすべての側面も含まれる。ステークホルダーは、同じ組織に存在する場合もあれば、複数の異なる組織が情報システムに共通の利害関係を有する場合には、複数の異なる組織に存在する場合もある。例えば、クラウドベースのシステム、共有サービスシステム、又はシステムに対するブリーチや侵害によって組織に悪影響が及ぶ可能性があるあらゆるシステムの開発中、運用中、及び保守中、あるいはサプライチェーンに関連する様々な考慮事項のために、このような状況が発生する場合がある。ステークホルダー間のコミュニケーションは、セキュリティ及びプライバシー要件が満たされ、懸念及び問題が迅速に対処され、リスクマネジメントプロセスが効果的に実施されることを確実にするために、RMF のすべてのステップ及び SDLC 全体で重要である。

参考文献:[SP 800-39](組織レベル)、[SP 800-64]、[SP 800-160 v1](ステークホルダーのニーズ及び要件定義プロセス及びポートフォリオマネジメントプロセス)、[SP 800-161]、[NIST CSF](コア[識別機能])。

資産の識別

タスク P-10 保護する必要がある資産を識別する。

潜在的なインプット:情報システムでサポートするミッション、ビジネスファンクション、及びミッション／ビジネスプロセス、ビジネスインパクト分析、内部ステークホルダー、システムステークホルダーの情報、システムの情報、システムとやりとりする他のシステムに関する情報。

期待されるアウトプット:一連の保護される資産。

主たる責任者: システム所有者。

補助的な役割を果たす者: 認可権限のある担当者又は認可権限のある担当者による指定代理人、ミッション又はビジネスオーナー、情報所有者又は情報管理者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、システム管理者。

システム開発ライフサイクルのフェーズ: 新規 – 開始(概念／要件の定義)。
既存 – 運用／保守。

詳解:資産とは、ミッション又はビジネス目標の達成に有用な有形又は無形のものである。有形資産は性質が物理的なものであり、物理的／環境的な要素(例えば、非デジタル情報、建造物、施設)、人的要素、及び技術／機械の要素(例えば、ハードウェア要素、メカニズム、ネットワーク)が含まれる。これとは対照的に、無形資産は性質が物理的ではなく、ミッション及びビジネスプロセス、機能、デジタル情報及びデータ、ファームウェア、ソフトウェア、及びサービスが含まれる。情報資産には有形資産と無形資産があり、ミッション又はビジネスファンクションの実施、サービスの提供、及びシステム管理／運用に必要な情報、管理対象非機密情報及び国家機密情報、及び情報システムに関連するあらゆる形態の文書が含まれる可能性がある。無形資産には、組織のイメージ又は評判、システムによって情報が処理される個人のプライバシー権益も含まれる可能性がある。組織は、保護のために考慮すべきステークホルダー資産の範囲を定義する。保護する必要がある資産は、ステークホルダーの懸念と、資産が使用されるコンテキストに基づいて識別される。これには、組織のミッション又はビジネスファンクション、システムとやりとりする他のシステム、及びミッション又はビジネスファンクションもしくはシステムによって資産が活用されるステークホルダーが含まれる。資産は、システムセキュリティ及びプライバシー計画で文書化することができる。

参考文献:[SP 800-39](組織レベル)、[SP 800-64]、[SP 800-160 v1](ステークホルダーのニーズ及び要件定義プロセス)、[IR 8179](重要度分析プロセス C)、[NIST CSF](コア[識別機能])、[NARA CUI]。

認可境界

タスク P-11 システムの認可境界を決定する。

潜在的なインプット:システム設計文書、ネットワーク図、システムステークホルダーの情報、資産の情報、ネットワーク及び／又はエンタープライズアーキテクチャの図、組織構造(チャート、情報)。

期待されるアウトプット:文書化された認可境界。

主たる責任者: 認可権限のある担当者。

補助的な役割を果たす者: 最高情報責任者、システム所有者、ミッション又はビジネスオーナー、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、エンタープライズアーキテクト。

システム開発ライフサイクルのフェーズ: 新規 – 開始(概念／要件の定義)。
既存 – 運用／保守。

詳解:認可境界は、情報システムの保護範囲(即ち、組織が、そのマネジメント管理策の下で、又はその責任の範囲内で、保護することに同意するもの)を確立する。 認可境界は、ミッション、マネジメント、又は予算上の責任に基づき、システム所有者からのインプットを得て、認可権限のある担当者が決定する(附属書 F を参照)。特に低インパクトシステムが高インパクトシステムに接続されている場合、又は外部プロバイダがシステムの運用又は保守に責任を負う場合には、説明責任及びセキュリティ分類化のために、認可境界の明確な描写が重要である。各システムには、1 つ以上の目的を達成し、組織のミッション及びビジネスプロセスをサポートするために編成された、一連の要素(即ち、情報リソース)[65]

[65] システム要素は、ハードウェア、ソフトウェア、又はファームウェア、物理的構造又はデバイス、もしくは個人、プロセス、又は手順によって実装される。*システムコンポーネント*という用語は、特にハードウェア、ソフトウェア、及びファームウェアによって実装されるシステム要素を指すために使用される。

が含まれている。各システム要素は、組織が、規定されたセキュリティ及びプライバシー要件を満たすことができるような方法で実装される。システム要素には、人的要素、技術／機械の要素、及び物理的／環境的な要素が含まれる。

システムという用語は、一連のシステム要素、システム要素の相互接続、及び RMF 実装の焦点となる環境を定義するために使用される（図 5 を参照）。システムは、説明責任を確保するために、単一の認可境界内に含まれる。PII を処理するシステムでは、プライバシー及びセキュリティプログラムが連携して、認可境界の共通理解を深める。効果的なリスクアセスメントを実施し、適切な管理策を選択するため、プライバシー及びセキュリティプログラムは、何が認可境界を構成するかについての明確かつ一貫した理解を提供する。認可境界と、それを超えると何が起きるかを理解することは、選択された管理策とその実装方法に影響を与える可能性がある。例えば、システムの機能に PII の外部共有が含まれる場合、システムから伝送される PII に対して堅牢な暗号化の管理策が選択される場合がある。

同様に、外部プロバイダによって部分的又は全体的に管理、保守、又は運用されているシステムについては、認可境界を明確に記述した合意によって、説明責任が確保される。プライバシー及びセキュリティプログラムは、認可境界の共通理解を深めるために、プロバイダと連携する。外部プロバイダとの正式な合意（例えば、契約）は、何が認可境界を構成するのかを明確にするために使用される場合がある。このような境界を理解しておくことで、サプライチェーンリスクを管理するための適切な管理策の選択が容易になる。

参考文献：[SP 800-18]、[SP 800-39]（システムレベル）、[SP 800-47]、[SP 800-64]、[SP 800-160 v1]（システム要件の定義プロセス）、[NIST CSF]（コア[識別機能]）。

情報の種類

タスク P-12 システムによって処理、保存、及び伝送される情報の種類を識別する。

潜在的なインプット：システム設計文書、保護される資産、ミッション／ビジネスプロセスの情報、システム設計文書。

期待されるアウトプット：システムの情報の種類のリスト。

主たる責任者：システム所有者、情報所有者又は情報管理者。

補助的な役割を果たす者：ミッション又はビジネスオーナー、システムセキュリティ責任者、システムプライバシー責任者。[66]

システム開発ライフサイクルのフェーズ：新規 – 開始（概念／要件の定義）。
既存 – 運用／保守。

詳解：組織のミッション、ビジネスファンクション、及びミッション／ビジネスプロセスをサポートするために必要な情報の種類の識別は、システムのセキュリティ及びプライバシー計画において重要なステップであり、セキュリティ分類化を決定するための前提条件である。[NARA CUI] は、法律、規制、又は政府全体のポリシーに従って、管理対象非機密情報（CUI）プログラムの一部として保護を必要とする情報の種類を定義している。組織は、CUI レジストリ又は [SP 800-60 v2] で定義されていない組織のミッション、ビジネスファンクション、及びミッション／ビジネスプロセスをサポートために必要な追加の情報の種類を定義してもよい。識別された情報の種類は、情報所有者又は情報管理者によって確認され、システムセキュリティ及びプライバシー計画に文書化される。

参考文献：[OMB A-130]、[NARA CUI]、[SP 800-39]（システムレベル）、[SP 800-60 v1]、[SP 800-60 v2]、[NIST CSF]（コア[識別機能]）。

[66] システムプライバシー責任者は、情報システムで PII が処理される場合にのみ、主たる責任を持つ役割となる。

情報ライフサイクル

タスク P-13 システムによって処理、保存、又は伝送される情報の種類ごとに、情報ライフサイクルのすべての段階を識別し、理解する。

潜在的なインプット:システムでサポートする予定のミッション、ビジネスファンクション、及びミッション／ビジネスプロセス、システムステークホルダーの情報、認可境界の情報、システムとやりとりする他のシステムに関する情報(情報交換／接続に関する合意など)、システム設計文書、システム要素の情報、システム情報の種類のリスト。

期待されるアウトプット:システム内で情報が通過する段階に関する文書、例えば、情報ライフサイクル全体においてシステムで情報がどのように構造化又は処理されるかを示すデータマップやモデルなど。このような文書には、データフロー図、エンティティ関係図、データベーススキーマ、及びデータディクショナリが含まれる。

主たる責任者: 政府機関のプライバシー保護責任者、システム所有者、情報所有者又は情報管理者。

補助的な役割を果たす者: 最高情報責任者、ミッション又はビジネスオーナー、セキュリティアーキテクト、プライバシーアーキテクト、エンタープライズアーキテクト、システムセキュリティエンジニア、プライバシーエンジニア。

システム開発ライフサイクルのフェーズ: 新規 – 開始(概念／要件の定義)。
既存 – 運用／保守。

詳解:情報ライフサイクルは、情報が通過する段階を示すものであり、通常、作成又は収集、処理、配布、使用、保存、及び廃棄として特徴付けられ、破棄及び削除も含まれる[OMB A-130]。ライフサイクルのすべての段階で各情報の種類がどのように処理されるかを識別し理解することは、組織が情報を保護するための考慮事項を識別し、組織のセキュリティ及びプライバシーリスクアセスメントに情報を提供し、管理策の選択と実装に情報を提供するのに役立つ。情報ライフサイクルの識別及び理解は、例えば、組織が情報を収集又は作成する権限を持ち、インパクトレベルに応じた情報の処理に関するルールを策定し、情報共有の合意を形成し、情報の保存と廃棄に関する保持スケジュールに従うことを確実にするのに役立つプラクティスの採用を容易にする。

データマップなどのツールを使用することで、組織は情報がどのように処理されているかを理解できるため、どこでセキュリティ及びプライバシーリスクが発生する可能性があるか、どこで最も効果的に管理策が適用されるかを、より適切にアセスメントできる。情報がシステムに出入りする方法はセキュリティ及びプライバシーリスクアセスメントに影響を与える可能性があるため、組織は、認可境界の適切な描写及び情報システムと他のシステムの間の相互作用を考慮することが重要である。システムの要素は、このようなリスクアセスメントをサポートするのに十分な細かさで識別される。

情報ライフサイクルを識別し、理解することは、情報が SDLC のフェーズのいずれかでシステムによって処理される可能性があるため、セキュリティ及びプライバシーリスクアセスメントに特に関連する。例えば、SDLC のテスト及び統合フェーズでは、実データ(即ち、ライブデータ)を処理するとセキュリティ及びプライバシーリスクが発生する可能性があるが、代替データ(即ち、合成データ)を使用すると、リスクを軽減しつつ、システムのテストという観点では同等のメリットが得られる可能性がある。

参考文献:[OMB A-130]、[OMB M-13-13]、[NARA RECM]、[NIST CSF](コア[識別機能])、[IR 8062]。

リスクアセスメント – システム

タスク P-14 システムレベルのリスクアセスメントを実施し、リスクアセスメント結果を継続的に更新する。

潜在的なインプット:保護される資産、システムでサポートする予定のミッション、ビジネスファンクション、及びミッション／ビジネスプロセス、ビジネスインパクト分析又は重要度分析、システムステークホルダーの情報、システムとやりとりする他のシステムに関する情報、プロバイダの情報、脅威の情報、データマップ、システム設計文書、サイバーセキュリティフレームワークプロファイル、リスクマネジメント戦略、組織レベルのリスクアセスメント結果。

期待されるアウトプット:セキュリティ及びプライバシーリスクアセスメント報告書。

主たる責任者: システム所有者、システムセキュリティ責任者、システムプライバシー責任者。

補助的な役割を果たす者: リスクマネジメント担当責任者又はリスク管理者(機能)、認可権限のある担当者又は認可権限のある担当者による指定代理人、ミッション又はビジネスオーナー、情報所有者又は情報管理者、管理策アセッサー。

システム開発ライフサイクルのフェーズ: 新規 – 開始(概念／要件の定義)。
既存 – 運用／保守。

詳解:このタスクでは、各種のリスクが完全にアセスメントされることを確実にするために、組織がセキュリティ及びプライバシーリスクアセスメントを実施する必要がある場合がある。セキュリティリスクのアセスメントには、資産に影響を与える脅威源及び脅威事象の識別 [67]、資産が脅威に対して脆弱であるかどうか、及びどのように脆弱であるか、資産の脆弱性が脅威によって悪用される可能性、及び資産の損失のインパクト(又は結果)の識別が含まれる。リスクアセスメントの重要な部分として、資産の損失の悪いインパクト又は結果に基づいて、資産の優先順位付けを行う。損失の意味は、損失の結果(即ち、損失の悪いインパクト)を判断できるようにするため、資産の種類ごとに定義される。損失の結果は、有形(例えば、金銭的、産業的被害)又は無形(例えば、評判)であり、資産に関連する部分的な損失から全体的な損失までの連続体を構成する。情報の損失の解釈には、例えば、所有権の喪失、破壊、又は精度又は正確さの損失が含まれる場合がある。機能又はサービスの損失は、制御の損失、アクセス可能性の損失、通常の機能、パフォーマンス、又は動作を提供する能力の損失、もしくは機能、パフォーマンス、又は動作のレベルの低下をもたらす限定的なケイパビリティの損失として解釈される場合がある。侵害の物理的な結果には、予定外の生産停止、産業機器の損傷、現場での死傷者、環境災害、及び公共の安全に対する脅威を含めることができる。資産の優先順位付けは、資産の価値、物理的な結果、交換にかかるコスト、重要度、イメージや評判へのインパクト、又はユーザ、協力組織、あるいはミッション又ビジネスパートナーからの信頼に基づく。資産の優先順位は、リソースの割り振り、メカニズムの強度の決定、及びアシュアランスレベルの定義における優先度に変換される。

プライバシーリスクアセスメントは、PII を処理する際にシステムが行っている特定の処理が、個人に悪影響を及ぼす可能性、及び個人に対する潜在的インパクトを判断するために実施される [68]。これらの悪影響は、PII を処理する情報システムの機密性、完全性、又は可用性の損失につながる不正な活動から発生するか、又は認可された活動の副産物として発生する可能性がある。プライバシーリスクアセスメントは、文脈的要因の影響を受ける。文脈的要因には、特定の要素又は全体としての PII の機微性レベル、システムを使用する、又はシステムとやり取りする組織の種類、及びプライバシーに関して個人が組織に対して持っている認識、処理の性質及び目的に関する個人の理解、及び個人のプライバシー権益、個人の理解又は行動に影響を与える技術的専門知識又は人口統計学的特性が含まれる可能性があるが、これらに限定されない。個人に対するプライバシーリスクは、個人がシステムと関わる意思決定に影響を与え、それによってミッション又はビジネス目標に影響を与える、又は組織に法的責任、風評被害のリスク、又は他の種類のリスクを生み出す場合がある。組織へのインパクトは、プライバシーリスクではない。しかし、これらのインパクトは、組織の意思決定を導き、情報を提供し、さらに、リスク対応の優先順位付け及びリソース割り振りに影響を与えることができる。

[67] さらに、脅威インテリジェンス、脅威分析、及び脅威のモデル化の使用は、敵対的なサイバー攻撃、機器の故障、自然災害、怠慢や過失による誤りを含む様々な脅威に対する組織の影響の受けやすさを軽減するために必要なセキュリティケイパビリティを組織が開発するのに役立つ。

[68] [IR 8062]は、プライバシーリスクマネジメント及びプライバシーリスクアセスメントを実施するためのプライバシーリスクモデルを紹介している。

リスクアセスメントは、システム、システム要素、又はサービスの開発、実装、保守、管理、運用、又は廃棄のために外部プロバイダを利用することによって損失が発生する可能性と、その損失の潜在的なインパクトを判断するためにも実施される。インパクトは、即自的なもの（例えば、物理的な盗難）、又は継続的なもの（例えば、盗難窃盗により、敵対者が重要な機器を複製する能力）である場合がある。インパクトは、固有（エンデミック）（例えば、単一のシステムに限定される）、又はと全体的（システミック）（例えば、特定の種類のシステムコンポーネントを使用するすべてのシステムを含む）である場合がある。サプライチェーンのリスクアセスメントでは、システム又はシステム要素の廃棄、又は外部プロバイダの利用から発生する可能性がある脆弱性を考慮する。サプライチェーンの脆弱性には、偽造品の利用、マルウェアの挿入、又は低品質システムにつながるトレーサビリティと説明責任の欠如が含まれる場合がある。外部プロバイダの利用は、システム、システム要素、及びサービスがどのように開発、展開、及び保守されるかについての可視性及び制御の損失につながる可能性がある。有害なサプライチェーン事象の脅威、脆弱性、及び潜在的インパクトを明確に理解することは、組織がサプライチェーンリスクとリスク許容度の適切なバランスを取るのに役立つ。サプライチェーンのリスクアセスメントには、サプライヤ監査、レビュー、及びサプライチェーンのインテリジェンスからの情報を含めることができる。組織は、サプライチェーンのリスクアセスメントにおけるプロバイダとの協力に関する戦略を含む、情報を収集するための戦略を策定する。このような協力は、組織がプロバイダからの情報を活用し、冗長性を軽減し、リスク対応のための潜在的な行動方針を識別し、プロバイダの負荷を軽減するのに役立つ。

リスクアセスメントは SDLC 全体を通じて実施され、様々な RMF のステップ及びタスクをサポートする。リスクアセスメントの結果は、セキュリティ及びプライバシー要件定義；分類の決定；管理策の選択、テーラリング、実装、及びアセスメント；認可の決定；リスク対応のための潜在的な行動方針及び優先順位付け；及び継続的監視戦略を知らせるために使用される。組織は、リスクアセスメントの実施形式（リスクアセスメントの範囲、厳格さ、及び手続きを含む）と結果の報告方法を決定する。

参考文献：[FIPS 199]、[FIPS 200]、[SP 800-30]、[SP 800-39]（組織レベル）、[SP 800-59]、[SP 800-60 v1]、[SP 800-60 v2]、[SP 800-64]、[SP 800-160 v1]（ステークホルダーのニーズ及び要件定義プロセス及びリスクマネジメントプロセス）、[SP 800-161]（アセスメント）、[IR 8062]、[IR 8179]、[NIST CSF]（コア[識別機能]）、[CNSSI 1253]。

要件の定義

タスク P-15 システム及び運用環境に関するセキュリティ及びプライバシー要件を定義する。

潜在的なインプット：システム設計文書、組織レベル及びシステムレベルのリスクアセスメント結果、ステークホルダーの既知の保護される資産、システムでサポートする予定のミッション、ビジネスファンクション、及びミッション／ビジネスプロセス、システムステークホルダーの情報、ビジネスインパクト分析又は重要度分析、システムステークホルダーの情報、PII の情報ライフサイクルのデータマップ、サイバーセキュリティフレームワークプロファイル、システムとやりとりする他のシステムに関する情報、サプライチェーンの情報、脅威の情報、システムに適用される法律、大統領令、指令、規制、又はポリシー、リスクマネジメント戦略。

期待されるアウトプット：文書化されたセキュリティ及びプライバシー要件。

主たる責任者：ミッション又はビジネスオーナー、システム所有者、情報所有者又は情報管理者、システムプライバシー責任者。[69]

[69] システムプライバシー責任者は、情報システムで PII が処理される場合にのみ、主たる責任を持つ役割となる。

補助的な役割を果たす者: 認可権限のある担当者又は認可権限のある担当者による指定代理人、システムセキュリティ責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、最高取得責任者、セキュリティアーキテクト、プライバシーアーキテクト、エンタープライズアーキテクト。

システム開発ライフサイクルのフェーズ: 新規 – 開始(概念／要件の定義)。
既存 – 運用／保守。

詳解: 保護ニーズは、ミッション又はビジネスニーズをサポートしながら、セキュリティ及びプライバシーリスクを受容可能なレベルまで低減するために、システムに必要な保護ケイパビリティを表したものである。保護ニーズには、システムのセキュリティ特性[70]と、意図した運用環境及びシステムライフサイクルの全フェーズにおけるシステムのセキュリティ動作が含まれる。保護ニーズは、ステークホルダーの優先事項、対立に対応したステークホルダー間の交渉の結果、相反する優先事項、矛盾、及び表明された目的を反映しており、本質的に主観的である。保護ニーズは、これらのニーズに関連する根拠、前提条件、及び制約を後で参照できることを確実にし、セキュリティ及びプライバシー要件へのトレーサビリティを提供するために文書化される。セキュリティ及びプライバシー要件[71]は、SDLC の全フェーズ、関連するライフサイクルプロセス、及びシステムに関連する資産の保護にわたる保護ニーズの正式で、より詳細な表現を構成する。セキュリティ及びプライバシー要件は、多くの情報源(例えば、法律、大統領令、指令、規制、ポリシー、標準、ミッション及びビジネスのニーズ、又はリスクアセスメント)から得られる。セキュリティ及びプライバシー要件は、システムに必要な特性を正式に表現する上で重要な部分である[72]。セキュリティ及びプライバシー要件は、システムの管理策の選択及びこれらの管理策に関連するテーラリング活動を導き、情報を提供する。

組織はサイバーセキュリティフレームワークを使用して、セキュリティ及びプライバシー要件を管理し、これらの要件を組織のために定義されたサイバーセキュリティフレームワーク*プロファイル*で表現することができる。例えば、フレームワークコアの*機能* – *カテゴリ* – *サブカテゴリ*の構造を使用して、複数の要件を調整することができ、更に競合を解決することもできる。その後、プロファイルを使用して、RMF *準備 – 組織レベル*ステップ、タスク P-4 で説明されている組織的にテーラリングされた管理策ベースラインの開発に情報を提供することができる。

参考文献: [SP 800-39](組織レベル)、[SP 800-64]、[SP 800-160 v1](ステークホルダーのニーズ及び要件定義プロセス)、[SP 800-161](マルチティアリスクマネジメント)、[IR 8179]、[NIST CSF](コア[防御、検知、対応、復旧機能]、プロファイル)。

エンタープライズアーキテクチャ

タスク P-16 エンタープライズアーキテクチャ内でのシステムの配置を決定する。

潜在的なインプット: セキュリティ及びプライバシー要件、組織レベル及びシステムレベルのリスクアセスメント結果、エンタープライズアーキテクチャの情報、セキュリティアーキテクチャの情報、プライバシーアーキテクチャの情報、資産の情報。

期待されるアウトプット: 更新されたエンタープライズアーキテクチャ、更新されたセキュリティアーキテクチャ、更新されたプライバシーアーキテクチャ、クラウドベースのシステム及び共有システム、サービス、又はアプリケーションの使用計画。

---

[70] 例えば、基本的なセキュリティ特性は、システムが規定された動作、相互作用、及び成果のみを示すことである。

[71] *要件*という用語は、個別の意味を持つ可能性がある。例えば、法律及びポリシーの要件は、組織が順守しなければならない義務を課す。しかし、セキュリティ及びプライバシー要件は、システムの保護ニーズから導き出されたものであり、これらの保護ニーズは、法律又はポリシーの要件、ミッション又はビジネスのニーズ、リスクアセスメント、又はその他のソースから導き出すことができる。

[72] セキュリティ及びプライバシー要件には、*アシュアランス*要件を含めることもできる。アシュアランスとは、悪意の意図の有無に関わらず、あらゆる形態の逆境において、システムがセキュリティ及びプライバシーに関する統合的信頼性を維持する能力について確信を持つことである。

主たる責任者: ミッション又はビジネスオーナー、エンタープライズアーキテクト、セキュリティアーキテクト、プライバシーアーキテクト。

補助的な役割を果たす者: 最高情報責任者、認可権限のある担当者又は認可権限のある担当者による指定代理人、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、システム所有者、情報所有者又は情報管理者。

システム開発ライフサイクルのフェーズ: 新規 – 開始(概念／要件の定義)。
既存 – 運用／保守。

詳解:エンタープライズアーキテクチャは、ミッション／ビジネスプロセス及び情報リソースの有効性を最大化し、ミッション及びビジネスの成功を達成するために使用される管理プラクティスである。エンタープライズアーキテクチャは、情報システムの初期設計及び開発に含まれる情報技術及び制御・運用技術をより深く理解することができ、脅威がますます高度化する環境において、これらのシステムのレジリエンスと生存性を達成するための前提条件となるものである。また、エンタープライズアーキテクチャは、組織が情報及び技術資産を統合、標準化、及び最適化する機会も提供する。効果的に実装されたアーキテクチャは、より透明性が高いシステムを生み出し、その結果、理解及び保護が容易になる。また、エンタープライズアーキテクチャは、投資から測定可能なパフォーマンスの向上への明確なつながりも確立する。エンタープライズアーキテクチャ内でのシステムの位置付けは、システムに接続されている(内部及び外部の)他のシステムについての可視性及び理解を高めるため重要であり、システム保護レベルを高めるためのセキュリティドメインを確立することにも使用することができる。

セキュリティアーキテクチャ及びプライバシーアーキテクチャは、エンタープライズアーキテクチャの不可欠な部分である。これらのアーキテクチャは、セキュリティ及びプライバシー要件の実装に関連するエンタープライズアーキテクチャの部分を表している。セキュリティ及びプライバシーアーキテクチャの主な目的は、組織のシステムにおいて、セキュリティ及びプライバシー要件が一貫して費用対効果の高い方法で満たされ、リスクマネジメント戦略と整合していることを確実にすることである。セキュリティ及びプライバシーアーキテクチャは、組織の戦略的目標及び目的から、保護ニーズ及びセキュリティ及びプライバシー要件を経て、人、プロセス、技術によって提供される特定のセキュリティ及びプライバシーソリューションまでのトレーサビリティを容易にするロードマップを提供する。

参考文献:[SP 800-39](ミッション／ビジネスプロセスレベル)、[SP 800-64]、[SP 800-160 v1](システム要件の定義プロセス)、[NIST CSF](コア[識別機能]、プロファイル)、[OMB FEA]。

要件の割り振り

タスク P-17 セキュリティ及びプライバシー要件を、システム及び運用環境に割り振る。

潜在的なインプット:組織レベル及びシステムレベルのリスクアセスメント結果、文書化されたセキュリティ及びプライバシー要件、組織レベル及びシステムレベルのリスクアセスメント結果、共通管理策の提供者及び継承に利用可能な共通管理策のリスト、システムに関する記述、システム要素の情報、システムコンポーネントのインベントリ、関連する法律、大統領令、指令、規制、及びポリシー。

期待されるアウトプット:システム、システム要素、及び運用環境に割り振られたセキュリティ及びプライバシー要件のリスト。

主たる責任者: セキュリティアーキテクト、プライバシーアーキテクト、システムセキュリティ責任者、システムプライバシー責任者。

補助的な役割を果たす者: 最高情報責任者、認可権限のある担当者又は認可権限のある担当者による指定代理人、ミッション又はビジネスオーナー、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、システム所有者。

システム開発ライフサイクルのフェーズ: 新規 – 開始(概念／要件の定義)。
既存 – 運用／保守。

詳解:セキュリティ及びプライバシー要件は、組織、システム、システム要素、及び／又は運用環境の管理策の選択と実装を導き、情報を提供するために割り振られる[73]。
要件の割り振りは、管理策の実装先される場所を識別する。要件の割り振りは、リソースを節約し、共通管理策又はシステムレベルの管理策の特定のシステム要素への実装が必要な保護ケイパビリティ(能力)を提供する場合、複数のシステム又はシステム要素に要件が実装されないことを確実にすることによって、リスクマネジメントプロセスを合理化するのに役立つ。

参考文献:[SP 800-39](組織、ミッション／ビジネスプロセス、及びシステムレベル)、[SP 800-64]、[SP 800-160 v1](システム要件の定義プロセス)、[NIST CSF](コア[識別機能]、プロファイル)、[OMB FEA]、

システムの登録

タスク P-18 組織の計画部門又は管理部門にシステムを登録する。

潜在的なインプット:システムの登録に関する組織のポリシー、システム情報。

期待されるアウトプット:組織のポリシーに従って登録されたシステム。

主たる責任者: システム所有者。

補助的な役割を果たす者: ミッション又はビジネスオーナー、最高情報責任者、システムセキュリティ責任者、システムプライバシー責任者。

システム開発ライフサイクルのフェーズ: 新規 – 開始(概念／要件の定義)。
既存 – 運用／保守。

詳解:組織のポリシーに従ったシステムの登録は、システム開発の計画又は既存のシステムの存在、システムの主な特性、及びシステムの運用及び使用によって組織にもたらすと予想されるセキュリティ及びプライバシーの影響を、監督組織に通知する役割りを果たす。システムの登録は、エンタープライズアーキテクチャへのシステムの導入、リスクに見合った保護の実装、及び適用される法律、大統領令、指令、規制、ポリシー、又は標準に従ったセキュリティ及びプライバシー態勢の報告を容易にする管理及び追跡ツールを組織に提供する。システムの登録プロセスの一環として、組織はシステムを組織全体のシステムインベントリに追加する。*分類*ステップが完了すると、システムの登録情報はセキュリティ分類化及びシステムの特徴の情報によって更新される。

参考文献:なし。

[73] 情報システムの運用環境とは、システムが情報を処理、保存、及び伝送する物理的な環境を指す。例えば、*セキュリティ要件*は、システムが配置され運用される施設に割り振られる。これらのセキュリティ要件は、[SP 800-53]の物理的セキュリティ管理策によって満たすことができる。

3.2 分類 [74]

目的

分類ステップの目的は、組織のシステムの機密性、完全性、及び可用性の喪失、及びこれらのシステムによって処理、保存、及び伝送される情報に関して、組織の業務及び資産、個人、他の組織、及び国家への悪影響を判断することで、組織のリスクマネジメントプロセス及びタスクに情報を提供することである。

分類のタスク

表 3 は、RMF *分類*ステップのタスク及び期待される成果の概要を示している。
また、適用可能なサイバーセキュリティフレームワークの構成要素も示している。

表 3:分類のタスクと成果

タスク	成果
タスク C-1 システムに関する記述	・ システムの特徴が記述及び文書化されている。[*サイバーセキュリティフレームワーク*:**プロファイル**]
タスク C-2 セキュリティ分類化	・ 組織によって識別された情報の種類で表された、システムによって処理される情報を含む、システムのセキュリティ分類化が完了している。 [*サイバーセキュリティフレームワーク*:**ID.AM-1**、**ID.AM-2**、**ID.AM-3**、**ID.AM-4**、**ID.AM-5**] ・ セキュリティ分類化の結果が、セキュリティ、プライバシー、及び SCRM の計画に文書化されている。 [*サイバーセキュリティフレームワーク*:**プロファイル**] ・ セキュリティ分類化の結果が、エンタープライズアーキテクチャ及び組織のミッション、ビジネスファンクション、及びミッション／ビジネスプロセスの保護への取り組みと整合している。 [*サイバーセキュリティフレームワーク*:**プロファイル**] ・ セキュリティ分類化の結果が、組織のリスクマネジメント戦略を反映している。
タスク C-3 セキュリティ分類化のレビュー及び承認	・ 組織の上級幹部によってセキュリティ分類化の結果がレビューされ、分類の決定が承認されている。

RMF のタスク、責任、及び補助的な役割の概要表へのクイックリンク。

システムに関する記述

タスク C-1 システムの特徴を文書化する。

潜在的なインプット:システムの設計及び要件の文書、認可境界の情報、システム、システム要素、及び運用環境に割り振られたセキュリティ及びプライバシー要件のリスト、システム要素によって制御される物理的プロセス又は他のプロセス、システム要素の情報、システムコンポーネントのインベントリ、インベントリ及びサプライヤの情報を含むシステム要素のサプライチェーンの情報、セキュリティ分類化、システムによって処理、保存、及び伝送される情報の情報ライフサイクルのデータマップ、システムの用途、ユーザ、及び役割についての情報。

[74] RMF *分類化*ステップは、セキュリティ管理策を選択するための前提条件である。しかし、プライバシーに関しては、プライバシー管理策の選択を導き、情報を提供する組織によって考慮される他の要因がある。これらの要因については、RMF *準備 – システムレベル*ステップのタスク P-15 で説明されている。

期待されるアウトプット：文書化されたシステムに関する記述。

主たる責任者：システム所有者。

補助的な役割を果たす者：認可権限のある担当者又は認可権限のある担当者による指定代理人、情報所有者又は情報管理者、システムセキュリティ責任者、システムプライバシー責任者。

システム開発ライフサイクルのフェーズ：新規 – 開始（概念／要件の定義）。
既存 – 運用／保守。

詳解：システムの特徴に関する記述は、セキュリティ及びプライバシー計画に記載されるか、計画の添付ファイルに含まれるか、又は SDLC の一環として生成される情報のために他の標準的な情報源で参照される。情報の重複は、可能な限り回避される。セキュリティ及びプライバシー計画の詳細レベルは組織によって決定され、システムのセキュリティ分類化及びセキュリティ及びプライバシーリスクアセスメントに見合ったものとなる。情報は、システムライフサイクル中、RMF ステップの実行中に利用可能になった時、又はシステムの特徴の変更に伴って、システムに関する記述に追加又は更新される場合がある。

組織がセキュリティ及びプライバシー計画に追加できる様々な種類の記述情報の例には、以下のものがある。システムの記述名及びシステム識別子；システムのバージョン又はリリース番号；製造業者及びサプライヤの情報；システムの責任を負う個人；システムの連絡先情報；システムを管理、所有、制御する組織；システムの場所；システムの目的及びサポートされるミッション／ビジネスプロセス；エンタープライズアーキテクチャへのシステムの統合方法；SDLC フェーズ；分類化プロセス及びプライバシーリスクアセスメントの結果；認可境界；個人のプライバシー及びシステムのセキュリティに影響を与える法律、指令、ポリシー、規制、又は標準；ネットワークトポロジを含むシステムのアーキテクチャの記述；情報の種類；システムの一部であるハードウェア、ファームウェア、及びソフトウェアコンポーネント；ハードウェア、ソフトウェア、及びシステムインタフェース（内部及び外部）；システム内の情報フロー；外部システムとの通信のためのネットワーク接続ルール；相互接続されたシステム及びこれらのシステムの識別子；システム要素によって制御される物理的又はその他のプロセス、コンポーネント、及び機器；システムユーザ（所属、アクセス権、特権、市民権を含む）；サプライチェーンにおけるシステム来歴；保守及びその他の関連合意；システムの交換用コンポーネントの潜在的サプライヤ、代替の互換システムコンポーネント；交換用システムコンポーネントのインベントリにおける数と場所；システムの所有権及び運用（政府所有、政府運用；政府所有、請負業者運用；請負業者所有、請負業者運用；連邦政府外[州及び地方自治体、被譲与者]）、インシデント対応の連絡窓口；認可日及び認可の満了日；継続的な認可のステータス。システムの登録情報は、システムの特徴情報によって更新される（タスク P-18 を参照）。

参考文献：[SP 800-18]、[NIST CSF]（コア[識別機能]）。

セキュリティ分類化

タスク C-2　システムを分類し、セキュリティ分類化の結果を文書化する。

潜在的なインプット：リスクマネジメント戦略、組織のリスク許容度、認可境界（即ち、システム）の情報、組織レベル及びシステムレベルのリスクアセスメント結果、システムによって処理、保存、又は伝送される情報の種類、システム、システム要素、及び運用環境に割り振られたセキュリティ及びプライバシー要件のリスト、システムを運用するための組織の権限又は目的、ビジネスインパクト分析又は重要度分析、システムでサポートされるミッション、ビジネスファンクション、及びミッション／ビジネスプロセスに関する情報。

期待されるアウトプット：各情報の種類及び各セキュリティ目的について決定したインパクトレベル（機密性、完全性、可用性）、情報の種類のインパクトレベルの最高水準に基づくセキュリティ分類化。

主たる責任者：システム所有者、情報所有者又は情報管理者。

補助的な役割を果たす者：リスクマネジメント担当責任者又はリスク管理者（機能）、最高情報責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、認可権限のある担当者又は認可権限のある担当者による指定代理人、システムセキュリティ責任者、システムプライバシー責任者。

システム開発ライフサイクルのフェーズ：新規 – 開始（概念／要件の定義）。
既存 – 運用／保守。

詳解：セキュリティ分類化の決定では、情報の機密性、完全性、又は可用性の喪失から生じる、組織の業務、組織の資産、個人、他の組織、及び国家に対する潜在的な悪いインパクトを考慮する。組織は、 最高水準の概念に基づいてシステムに対して単一のインパクトレベルを設定するための[FIPS 200]（国家安全保障システム以外の場合）、又は機密性、完全性、及び可用性のセキュリティ目的ごとに異なる 3 つのインパクト値を設定するための[CNSSI 1253]（国家安全保障システムの場合）のいずれかを使用して、柔軟にセキュリティ分類化を実施する。セキュリティ分類化プロセスは、システム所有者及び情報所有者又は情報管理者が、ミッション、ビジネスファンクション、又はリスクマネジメントの責任を負う上級幹部及び管理職の協力及び連携して実施する。協力及び連携は、組織のミッション及びビジネス目標に基づいて個々のシステムが分類されることを確実にするのに役立つ。システム所有者及び情報所有者又は情報管理者は、セキュリティリスクアセスメント（及びシステムが PII を処理する場合はプライバシーリスクアセスメント）の結果を、セキュリティ分類化の決定の一部として考慮する。この決定はリスクマネジメント戦略と整合している。分類化プロセスの結果は、システムのセキュリティ管理策の選択に影響を与える。セキュリティ分類化の情報は、システムセキュリティ計画に文書化されるか、又は計画の添付ファイルとして含まれ、システムが PII を処理する場合は、プライバシー計画で相互参照できる。

システムのセキュリティ分類化の結果は、同一インパクトレベルのシステムのインパクトレベルの優先順位付けを容易にするために、組織によってさらに改良することができる（タスク P-6 を参照）。組織が実施したインパクトレベルの優先順位付けの結果は、システム所有者による管理策の選択及びテーラリングの決定に役立てることができる。

参考文献：[FIPS 199]、[FIPS 200]、[SP 800-30]、[SP 800-39]（システムレベル）、[SP 800-59]、[SP 800-60 v1]、[SP 800-60 v2]、[SP 800-160 v1]（ステークホルダーのニーズ及び要件定義及びシステム要件の定義プロセス）、[IR 8179]、[CNSSI 1253]、[NIST CSF]（コア[識別機能]）。

セキュリティ分類化のレビュー及び承認

タスク C-3 セキュリティ分類化の結果及び決定をレビューし、承認する。

潜在的なインプット：情報の種類及び各セキュリティ目的（機密性、完全性、可用性）ごとに決定されたインパクトレベル、情報の種類のインパクトレベルの最高水準に基づくセキュリティ分類化、組織の高価値資産のリスト。

期待されるアウトプット：システムのセキュリティ分類化の承認。

主たる責任者：認可権限のある担当者又は認可権限のある担当者による指定代理人、政府機関のプライバシー保護責任者。[75]

[75] 政府機関のプライバシー保護責任者は、情報システムで処理される情報が PII と見なされるかどうかの判断に参加し、そのようなシステムの分類のレビュー及び承認に関与する。

補助的な役割を果たす者: リスクマネジメント担当責任者又はリスク管理者（機能）、最高情報責任者、政府機関の情報セキュリティ責任者。

システム開発ライフサイクルのフェーズ: 新規 – 開始（概念／要件の定義）。
既存 – 運用／保守。

詳解: PII を処理する情報システムについては、認可権限のある担当者のレビューの前に、政府機関のプライバシー保護責任者がセキュリティ分類化の結果と決定をレビューし、承認する。[76]
セキュリティ分類化の結果及び決定は、情報システムに対して選択されているセキュリティ分類が、組織のミッション及びビジネスファンクション、並びに、これらのミッション及びファンクションを適切に保護するニーズと整合していることを確実にするために、認可権限のある担当者又は指定代理人によってレビューされる。認可権限のある担当者又は指定代理人は、分類化の結果及び決定を、組織の他のすべてのシステムの分類の決定とどのように整合させるかを含め、組織全体の観点からレビューする。認可権限のある担当者は、リスクマネジメント担当責任者又はリスク管理者（機能）と協力して、システムの分類の決定が、組織のリスクマネジメント戦略と整合し、高価値資産の要件を満たしていることを確実にする。承認プロセスの一部として、認可権限のある担当者は、RMF *選択*ステップで発生するシステムのベースラインのテーラリング活動の制限に関して、システム所有者に具体的なガイダンスを提供することができる（タスク S-2 を参照）。セキュリティ分類化の決定が承認されない場合、システム所有者は分類化プロセスを繰り返すためのステップを開始し、調整された結果を認可権限のある担当者又は指定代理人に再提出する。その後、システムの登録情報は承認されたセキュリティ分類化情報で更新される（タスク P-18 を参照）。

参考文献: [FIPS 199]、[SP 800-30]、[SP 800-39]（組織レベル）、[SP 800-160 v1]（ステークホルダーのニーズ及び要件定義プロセス）、[CNSSI 1253]、[NIST CSF]（コア[識別機能]）。

[76] 政府機関のプライバシー保護責任者の責任については[OMB A-130]で説明されている。

3.3 選択

目的

選択ステップの目的は、組織の業務及び資産、個人、他の組織、及び国家に対するリスクに見合った情報システム及び組織の保護に必要な管理策を選択、テーラリング、及び文書化することである。

選択のタスク

表 4 は、RMF *選択*ステップのタスク及び期待される成果の概要を示している。また、適用可能なサイバーセキュリティフレームワークの構成要素も提供されている。

表 4：選択のタスクと成果

タスク	成果
タスク S-1 管理策の選択	・ リスクに見合ったシステム保護に必要な管理策ベースラインが選択されている。 ［*サイバーセキュリティフレームワーク*：**プロファイル**］
タスク S-2 管理策のテーラリング	・ 管理策がテーラリングされ、テーラリングされた管理策ベースラインが作成されている。 ［*サイバーセキュリティフレームワーク*：**プロファイル**］
タスク S-3 管理策の割り振り	・ 管理策がシステム固有、ハイブリット、又は共通管理策として指定されている。 ・ 特定のシステム要素（即ち、機械的、物理的、及び人的要素）に管理策が割り振られている。 ［*サイバーセキュリティフレームワーク*：**プロファイル**、**PR.IP**］
タスク S-4 計画された管理策の実装の文書化	・ 管理策及び関連するテーラリング活動が、セキュリティ及びプライバシー計画又は同等の文書に文書化されている。 ［*サイバーセキュリティフレームワーク*：**プロファイル**］
タスク S-5 継続的監視戦略 – システム	・ 組織のリスクマネジメント戦略を反映した、システムの継続的監視戦略が策定されている。 ［*サイバーセキュリティフレームワーク*：**ID.GV**、**DE.CM**］
タスク S-6 計画のレビュー及び承認	・ リスクに見合ったシステム及び運用環境の保護に必要な管理策の選択を反映したセキュリティ及びプライバシー計画が、認可権限のある担当者によってレビューされ、承認されている。

RMF のタスク、責任、及び補助的な役割の概要表へのクイックリンク。

管理策の選択

タスク S-1　システム及び運用環境のための管理策を選択する。

潜在的なインプット：セキュリティ分類化、組織レベル及びシステムレベルのリスクアセスメント結果、システム要素の情報、システムコンポーネントのインベントリ、システム、システム要素及び運用環境に割り振られたセキュリティ及びプライバシー要件のリスト、システム又はシステム要素の外部プロバイダに割り振られた契約上の要件のリスト、ビジネスインパクト分析又は重要度分析、リスクマネジメント戦略、組織のセキュリティ及びプライバシーポリシー、連邦政府又は組織によって承認又は義務付けられたベースライン又はオーバーレイ、サイバーセキュリティフレームワークプロファイル。

期待されるアウトプット:システム及び運用環境のために選択された管理策。

主たる責任者: システム所有者、共通管理策の提供者。

補助的な役割を果たす者: 認可権限のある担当者又は認可権限のある担当者による指定代理人、情報所有者又は情報管理者、システムセキュリティエンジニア、プライバシーエンジニア、システムセキュリティ責任者、システムプライバシー責任者。

システム開発ライフサイクルのフェーズ: 新規 – 開発／調達。
既存 – 運用／保守。

詳解:管理策の初期の選択には、*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の 2 種類のアプローチが使用できる。ベースライン管理策の選択アプローチでは、グループ、組織、又は利益共同体の保護ニーズに対応するために特別に構築された、事前定義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、及び情報システムの保護のための出発点として機能する。連邦政府の管理策ベースラインは[SP 800-53B]で提供されている。システムのセキュリティ分類化(タスク C-2 を参照)及び、ステークホルダーの保護ニーズ、法律、大統領令、規制、ポリシー、指令、指示、及び標準から得られるセキュリティ要件(タスク P-15 を参照)は、セキュリティ管理策ベースラインの選択の情報を提供するのに役立つ。プライバシーリスクアセスメント(タスク P-14 を参照)及び、ステークホルダーの保護ニーズ、法律、大統領令、規制、ポリシー、指令、指示、及び標準から得られるプライバシー要件(タスク P-15 を参照)は、プライバシー管理策ベースラインの選択の情報を提供するのに役立つ。プライバシープログラムは、認可されていないシステムの活動又は動作と、認可されている活動の両方から生じるプライバシーリスクを管理するために、セキュリティ及びプライバシー管理策ベースラインを使用する。事前に定義された管理策ベースラインが選択された後、組織は、提供されたガイダンスに従ってベースラインをテーラリングする(タスク S-2 を参照)。ベースライン管理策の選択アプローチは、広範な利益共同体全体で一貫性を提供することができる。

組織が作成する管理策の選択アプローチは、組織が事前に定義された一連の管理策から開始しないため、ベースラインの選択アプローチとは異なる。むしろ、組織は独自の選択プロセスを使用して管理策を選択する。これは、システムが高度に専門化されている場合(例えば、兵器システム又は医療機器)、又は目的又は範囲が限定されている場合(例えば、スマートメーター)に必要となる場合がある。このような状況では、広範な管理策ベースラインから事前に定義された一連の管理策から開始し、その後テーラリングプロセスで管理策を除外する(即ち、トップダウンアプローチ)のではなく、システムに対する一連の特定の管理策を選択する(即ち、ボトムアップアプローチ)方が、組織にとって効率的かつ費用対効果が高い場合がある。

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の両方で、組織は、ライフサイクルに基づくシステムエンジニアリングプロセス(例えば、RMF *準備 – システムレベル*ステップのタスク P-15 で説明されている[ISO 15288]、[SP 800-160 v1])を使用して、明確に定義された一連のセキュリティ及びプライバシー要件を策定する。このプロセスでは、(組織が管理策ベースラインから開始するか、独自の選択プロセスから一連の管理策を作成するかに関わらず)要件を満たす一連の管理策の選択を導き、情報を提供するために使用できる一連の要件が作成される。同様に、組織は、一連の組織固有のセキュリティ及びプライバシー要件を表し、結果として[SP 800-53]の管理策の選択を導き、情報を提供するサイバーセキュリティフレームワーク*プロファイル*を策定するために、[NIST CSF]を使用することができる。また、組織が作成する管理策の選択アプローチでは、テーラリングが必要となる場合もある(タスク S-2 を参照)。組織はシステムごとに管理策の選択するために 1 つのアプローチを選択する必要はないが、状況に応じて異なるアプローチを使用してもよい。

参考文献:[FIPS 199]、[FIPS 200]、[SP 800-30]、[SP 800-53]、[SP 800-53B]、[SP 800-160 v1](システム要件の定義、アーキテクチャ定義、及び設計定義プロセス)、[SP 800-161](対応及び第 3 章)、[IR 8062]、[IR 8179]、[CNSSI 1253]、[NIST CSF](コア[識別、保護、検知、対応、復旧機能]、プロファイル)。

管理策のテーラリング

タスク S-2 システム及び運用環境のために選択した管理策をテーラリングする。

潜在的なインプット：初期の管理策ベースライン、組織レベル及びシステムレベルのリスクアセスメント結果、システム要素の情報、システムコンポーネントのインベントリ、システム、システム要素、及び運用環境に割り振られたセキュリティ及びプライバシー要件のリスト、ビジネスインパクト分析又は重要度分析、リスクマネジメント戦略、組織のセキュリティ及びプライバシーポリシー、連邦政府又は組織が承認した又は義務付けたオーバーレイ。

期待されるアウトプット：システム及び運用環境のテーラリングされた管理策のリスト（即ち、テーラリングされた管理策ベースライン）。

主たる責任者：システム所有者、共通管理策の提供者。

補助的な役割を果たす者：認可権限のある担当者又は認可権限のある担当者による指定代理人、情報所有者又は情報管理者、システムセキュリティエンジニア、プライバシーエンジニア、システムセキュリティ責任者、システムプライバシー責任者。

システム開発ライフサイクルのフェーズ：新規 – 開発／調達。
既存 – 運用／保守。

詳解：適用可能な管理策ベースラインを選択した後、組織は、様々な要因（例えば、ミッション又はビジネスファンクション、脅威、セキュリティ及びプライバシーリスク許容度（サプライチェーンリスクを含む）、システムの種類、リスク許容度）に基づいて、管理策をテーラリングする。テーラリングプロセスには、管理策ベースラインの共通管理策の識別及び指定（タスク P-5 を参照）、残りのベースライン管理策へのスコーピングの考慮事項の適用、必要に応じて代替管理策の選択、割り当て又は選択ステートメントのいずれかを使用した組織が定める管理策パラメータへの値の割り当て、追加の管理策によるベースラインの補足、及び管理策の実装実装のための仕様情報の提供、が含まれる[77]。組織は、テーラリングの決定に必要な正当化の理由又は裏付けとなる根拠に含める詳細の量を決定する。例えば、高インパクトシステム又は高価値資産[78]に関連するスコーピングの決定の正当化の理由又は裏付けとなる根拠は、低インパクトシステムの同様の決定よりも高い特殊性が必要とする場合がある。このような決定は、組織のミッション及びビジネスファンクション、ステークホルダーのニーズ、及び関連する法律、大統領令、規制、指令、又はポリシーと整合している。SDLC 及び SCRM に関連する管理策は、情報システムが目的に適合（fit-for-purpose）[79]しているかどうかを判断する際の根拠を提供し、それに応じてテーラリングされる必要がある。

組織は、テーラリングプロセスを導き、情報を提供するためにリスクアセスメントを使用する。セキュリティリスクアセスメントからの脅威情報は、関連するコストと利益を含むセキュリティ管理策の選択に関する組織の決定に影響を与える可能性がある、敵対者のケイパビリティ（能力）、意図、及び標的に関する情報を提供する。情報システムが PII を処理する場合、その中の文脈的要因を含むプライバシーリスクアセスメントもテーラリングに影響を与える[80]。リスクアセスメント結果は、共通管理策を識別し、継承可能な管理策がシステムとその運用環境のセキュリティ及びプライバシー要件を満たしているかどうかを判断する際にも活用される。組織によって提供される共通管理策が、管理策を継承するシステムに対して十分な保護を提供しない場合、システム所有者は、システム固有管理策又はハイブリッド管理策で共通管理策を補完して必要な保護レベルを達成するか、又は認可権限のある担当者に対してリスクのより大きな受容を推奨することができる。組織は管理策をテーラリングする際に、連邦政府又は組織が指示又は承認したオーバーレイ、テーラリングされたベースライン、又はサイバーセキュリティフレームワークプロファイルを考慮してもよい（タスク P-4 を参照）。

参考文献：[FIPS 199]、[FIPS 200]、[SP 800-30]、[SP 800-53]、[SP 800-53B]、[SP 800-160 v1]（システム要件の定義、アーキテクチャ定義、及び設計定義プロセス）、[SP 800-161]（対応及び第 3 章）、[IR 8179]、[CNSSI 1253]、[NIST CSF]（コア[識別、防御、検知、対応、復旧機能]、プロファイル）。

[77] テーラリングプロセスについては、[SP 800-53B]に詳しく記載されている。

[78] 高価値資産の詳細については、[OMB M-19-03]及び[OCIO HVA]を参照。

[79] [ISO 15288]は、*目的に適合（fit-for-purpose）*を、「適正な」システムが作成され、顧客のニーズを満たしていることを、ステークホルダーに提示されるサービスのアセスメントを通じて実証する SDLC の妥当性確認プロセスの成果として説明している。

[80] [IR 8062]は、プライバシーリスクモデルにおけるコンテキストとその機能についての詳解を提供している。

管理策の割り振り

タスク S-3 セキュリティ及びプライバシー管理策を、システム及び運用環境に割り振る。

潜在的なインプット:セキュリティ分類化、組織レベル及びシステムレベルのリスクアセスメント結果、システムの登録に関する組織のポリシー、エンタープライズアーキテクチャ、セキュリティ及びプライバシーアーキテクチャ、セキュリティ及びプライバシー要件、システム、システム要素、及び運用環境に割り振られたセキュリティ及びプライバシー要件のリスト、共通管理策の提供者及び継承に利用可能な共通管理策のリスト、システムに関する記述、システム要素の情報、システムコンポーネントのインベントリ、関連する法律、大統領令、指令、規制、及びポリシー。

期待されるアウトプット:システム、システム要素、及び運用環境に割り振られたセキュリティ及びプライバシー管理策のリスト。

主たる責任者: セキュリティアーキテクト、プライバシーアーキテクト、システムセキュリティ責任者、システムプライバシー責任者。

補助的な役割を果たす者: 最高情報責任者、認可権限のある担当者又は認可権限のある担当者による指定代理人、ミッション又はビジネスオーナー、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、システム所有者。

システム開発ライフサイクルのフェーズ: 新規 – 開始(概念/要件の定義)。
既存 – 運用/保守。

詳解:組織は、管理策をシステム固有、ハイブリッド、又は共通として指定し、セキュリティ又はプライバシーのケイパビリティ(能力)を提供する責任を負うシステム要素(即ち、機械的、物理的、又は人的要素)にその管理策を割り振る。管理策は、組織のエンタープライズアーキテクチャ及びセキュリティ又はプライバシーアーキテクチャ、並びに、割り振られたセキュリティ及びプライバシー要件と整合するシステム又は組織に割り振られる。すべての管理策をすべてのシステム要素に割り振る必要はない。特定のセキュリティ及びプライバシーケイパビリティ(能力)を提供する管理策は、そのケイパビリティ(能力)を必要とするシステム要素にのみ割り振られる。セキュリティ分類化、プライバシーリスクアセスメント、セキュリティ及びプライバシーアーキテクチャ、及び管理策の割り振りが連携することで、セキュリティ及びプライバシー保護とシステムのミッションベースの機能との間の適切なバランスを実現するのに役立つ。

システム、システム要素、及び運用環境に割り振られたセキュリティ及びプライバシー要件(タスク P-17 を参照)は、システム要素への管理策の割り振りを導き、情報を提供する。RMF *準備 – 組織レベル*ステップ(タスク P-5 を参照)中に、組織によって使用可能になった共通管理策が継承のために選択され、ハイブリッド管理策も選択される。共通管理策は、組織に割り振られたセキュリティ及びプライバシー要件を満たし、1 つ以上のシステムに継承される保護ケイパビリティ(能力)を提供する。ハイブリッド管理策は、システム及び組織に割り振られたセキュリティ及びプライバシー要件を満たし、1 つ以上のシステムに部分的に継承される保護ケイパビリティ(能力)を提供する。最後にシステム固有管理策は、システムに割り振られたセキュリティ及びプライバシー要件を満たし、そのシステムに保護ケイパビリティ(能力)を提供する。管理策は、システム内のすべての要素ではなく、特定のシステム要素に割り振ることができる。例えば、監査ログの管理に関連するシステム固有管理策は、ログ管理サーバに割り振られ、すべてのシステム要素に実装する必要はない場合がある。

参考文献:[SP 800-39](組織、ミッション/ビジネスプロセス、及びシステムレベル)、[SP 800-64]、[SP 800-160 v1](システム要件の定義、アーキテクチャ定義、及び設計定義プロセス)、[NIST CSF](コア[識別機能]、プロファイル)、[OMB FEA]。

計画された管理策の実装の文書化

タスク S-4 システム及び運用環境のための管理策を、セキュリティ及びプライバシー計画に文書化する。

潜在的なインプット:セキュリティ分類化、組織レベル及びシステムレベルのリスクアセスメント結果(セキュリティ、プライバシー、及び/又はサプライチェーン)、システム要素の情報、システムコンポーネントのインベントリ、ビジネスインパクト分析又は重要度分析、システム、システム要素、及び運用環境に割り振られたセキュリティ及びプライバシー要件のリスト、リスクマネジメント戦略、システム及び運用環境のために選択された管理策のリスト、組織のセキュリティ、プライバシー、及び SCRM のポリシー。

期待されるアウトプット:システムのセキュリティ及びプライバシー計画。

主たる責任者: システム所有者、共通管理策の提供者。

補助的な役割を果たす者: 認可権限のある担当者又は認可権限のある担当者による指定代理人、情報所有者又は情報管理者、システムセキュリティエンジニア、プライバシーエンジニア、システムセキュリティ責任者、システムプライバシー責任者。

システム開発ライフサイクルのフェーズ: 新規 – 開発/調達。
既存 – 運用/保守。

詳解:セキュリティ及びプライバシー計画には、システムのセキュリティ及びプライバシー要件と、これらの要件を満たすために選択された管理策の概要が含まれる。この計画には、システムのコンテキストで選択された各管理策の意図された適用を、管理策を正しく実装し、その後管理策の有効性をアセスメントするために十分な詳細レベルで記述する。管理策文書には、システム固有管理策及びハイブリッド管理策の実装方法、及びシステムの機能に関する計画及び期待を記述する。この記述には、システムのハードウェア、ソフトウェア、又はファームウェアコンポーネントに実装される管理策について、通常、計画されたインプット、期待される動作、及び必要に応じて期待されるアウトプットが含まれる。共通管理策も計画で識別される。継承された共通管理策の実装の詳細を提供することは要求されていない。このような詳細は、むしろ共通管理策の提供者の計画で提供され、システム所有者が利用できるようになっている。ハイブリッド管理策の場合、組織はシステムレベルの計画で、共通管理策の提供者によって提供される部分と、システムレベルで実装される部分を規定する。

組織は、セキュリティ及びプライバシー計画を組み込んだ統合計画を策定しても、個別の計画を維持してもよい。統合計画を策定する場合、プライバシープログラムはセキュリティプログラムと連携し、PII の機密性、完全性、及び可用性の管理に関して保護を提供する管理策の選択が計画に反映されること、及び管理策の実装、アセスメント、及び監視の役割及び責任を明確にするが描写されることを確実にする。個別のシステムセキュリティ計画及びプライバシー計画では、組織は、すべての計画で管理策を相互参照し、説明責任及び認識を維持するのに役立てる。プライバシー計画(又は統合計画)がレビューのために認可権限のある担当者又は指定代理人に提供される前に、政府機関のプライバシー保護責任者はその計画(又は統合計画)をレビューし、承認する(タスク S-6 を参照)。組織はセキュリティ及びプライバシー計画に相当する文書、例えば、システムエンジニアリング又はシステムライフサイクルの成果物又は文書に、管理策の選択とテーラリングに関する情報を文書化してもよい。

計画された管理策の実装の文書化は、システムの導入前後の決定のトレーサビリティを可能にする。可能な限り、組織は、管理策文書の冗長性を減らし、効率性と費用対効果を向上させるために、(同一又は類似のシステム又はシステム要素を採用しているベンダ又は他の組織によって作成された)既存の文書を参照し、自動化サポートツールを使用し、組織全体で調整する。また、この文書はプラットフォームの依存関係にも対処し、必要なケイパビリティ(能力)がどのように達成されるのかを、管理策の実装及びアセスメントをサポートするのに十分な詳細レベルで説明するために必要な追加情報を含んでいる。管理策の実装のための文書は、ハードウェア及びソフトウェアの開発、及びシステムセキュリティ及びプライバシーエンジニアリング分野のベストプラクティスに従っており、SDLC における活動の文書化のために確立されたポリシー及び手順とも整合する。特定の状況では、プライバシーリスクを引き起こす方法でセキュリティ管理策が実装される可能性がある。 プライバシープログラムは、プライバシーリスクの考慮事項の文書化と、そのようなリスクの軽減を目的とした実装をサポートする。

メカニズムをベースにした管理策の場合、組織は、製造業者、ベンダ、及びシステムインテグレータから提供される、又は入手可能な機能仕様書を利用する。これには、管理策の策定、実装、アセスメント、及び監視中に組織を支援する可能性があるあらゆる文書が含まれる。特定の管理策の場合、組織は、適切な組織エンティティ（例えば、物理セキュリティ部門、施設部門、記録管理部門、人事管理部門）から管理策の実装の情報を入手する。組織が確立したエンタープライズアーキテクチャとセキュリティ及びプライバシーアーキテクチャは、管理策の計画及び実装に使用される組織的アプローチを導き、情報を提供するため、プロセスを文書化することは、セキュリティ及びプライバシー要件を満たす上でのトレーサビリティを確実にするのに役立つ。

参考文献：[FIPS 199]、[FIPS 200]、[SP 800-18]、[SP 800-30]、[SP 800-53]、[SP 800-64]、[SP 800-160 v1]（システム要件の定義、アーキテクチャ定義、及び設計定義プロセス）、[SP 800-161]（対応及び第 3 章）、[IR 8179]、[CNSSI 1253]、[NIST CSF]（コア[識別、防御、検知、対応、復旧機能]、プロファイル）。

継続的監視戦略 ―システム

タスク S-5　組織の継続的監視戦略と整合し、それを補完する、管理策の有効性を監視するためのシステムレベルの戦略を策定し、実装する。

潜在的なインプット：組織のリスクマネジメント戦略、組織の継続的監視戦略、組織レベル及びシステムレベルのリスクアセスメント結果、セキュリティ及びプライバシー計画、組織のセキュリティ及びプライバシーポリシー。

期待されるアウトプット：継続的な認可の時間ベースのトリガーを含む、システムの継続的監視戦略。

主たる責任者：システム所有者、共通管理策の提供者。

補助的な役割を果たす者：リスクマネジメント担当責任者又はリスク管理者（機能）、最高情報責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、認可権限のある担当者又は認可権限のある担当者による指定代理人、情報所有者又は情報管理者、セキュリティアーキテクト、プライバシーアーキテクト、システムセキュリティエンジニア、プライバシーエンジニア、システムセキュリティ責任者、システムプライバシー責任者。

システム開発ライフサイクルのフェーズ：新規 – 開発／調達。
既存 – 運用／保守。

詳解：リスクマネジメントの重要な側面は、情報システム内に実装された、又は情報システムによって継承された管理策の継続的な監視である。システムレベルでの効果的な継続的監視戦略は、SDLC の早期（即ち、システムの初期設計又は調達決定段階）に、組織の継続的監視戦略と連携して策定及び実装される。システムレベルの継続的監視戦略は、組織の継続的監視戦略と整合しており、これを補足する。システムレベルの戦略は、組織の継続的監視戦略及び実装の一部として監視が提供されない管理策の監視に対処する。システムレベルの戦略では、組織レベルの戦略が対処していない管理策の監視頻度が識別し、このような管理策をアセスメントするために使用するアプローチを定義する。システムレベルの継続的監視戦略は、組織の監視戦略と整合しており、システム及び運用環境[81]に対する変更をどのように監視するか、リスクアセスメントをどのように実施するか、及び、報告書の受領者を含むセキュリティ及びプライバシー態勢の報告要件を定義する。システムレベルの継続的監視戦略は、セキュリティ及びプライバシー計画に含めることができる。[82]

[81] 運用環境（サプライチェーンを含む）に対する変更によって、脆弱性が生じる可能性ある（例えば、ソフトウェアパッチの利用可能性、サービス、保守、修理部品、又はその他のサポートを提供するサプライヤの所有権の変更）。

[82] プライバシーの継続的監視（PCM）戦略には、すべてのリスクマネジメントレベル（即ち、組織、ミッション／ビジネスプロセス、及びシステム）で組織全体に実装された、使用可能なすべてのプライバシー管理策が含まれる。この戦略では、適用されるプライバシー要件への準拠を確実にし、プライバシーリスクを管理するのに十分な、組織が定めるアセスメント頻度を各管理策に割り当てることで、管理策が継続的に監視されることを確実にする。新しいシステムの開発中に、PCM 戦略に含まれていないプライバシー管理策を作成又は使用する必要がある場合は、提案されるユースケースに対してその管理策が適切であるかどうかを判断するために政府機関のプライバシー保護責任者に相談する。新しいプライバシー管理策を実装することを決定した場合は、組織が定める監視頻度で新しい管理策を含めるように組織の PCM 戦略が更新される。

組織の継続的監視戦略によって対処されない管理策については、システムレベルの継続的監視戦略で、実装後に監視される管理策の監視頻度を決定する基準、及びこれらの管理策の継続的なアセスメントの計画を識別する。この基準は、システム所有者又は共通管理策の提供者が、他の組織の担当者（例えば、認可権限のある担当者又は指定代理人；リスクマネジメント担当責任者又はリスク管理者（機能）；政府機関の情報セキュリティ責任者；政府機関のプライバシー保護責任者；及び最高情報責任者）と協力して確立する。システムレベルでの頻度の基準には、組織の優先順位と、組織の業務及び資産、個人、他の組織、及び国家に対するシステムの重要性を反映する。変動しやすい管理策（即ち、管理策又は管理策の実装が時間の経過と共に変化する可能性が高い）[83]、組織の保護ニーズの特定の側面にとって極めて重要な管理策、又は行動計画及びマイルストーンで識別された管理策の場合、より頻繁なアセスメントが必要な場合がある。継続的監視中の管理策アセスメントのアプローチには、初期の認可の決定をサポートしたアセスメント手順と結果の再利用、システム要素のステータスの検出、及び履歴データと運用データの分析が含まれる場合がある。

認可権限のある担当者又は指定代理人は、継続的監視戦略と各管理策の監視の最小頻度を承認する。戦略の承認は、セキュリティ及びプライバシー計画の承認と併せて取得できる。管理策の監視は、SDLC の運用フェーズの開始時に開始され、廃止フェーズまで継続される。

参考文献：[SP 800-30]、[SP 800-39]（組織、ミッション又はビジネスプロセスシステムレベル）、[SP 800-53]、[SP 800-53A]、[SP 800-137]、[SP 800-161]、[IR 8011 v1]、[CNSSI 1253]、[NIST CSF]（コア[検知機能]）。

計画のレビュー及び承認

タスク S-6 システム及び運用環境のセキュリティ及びプライバシー計画をレビューし、承認する。

潜在的なインプット：セキュリティ及びプライバシー計画、組織レベル及びシステムレベルのリスクアセスメント結果。

期待されるアウトプット：認可権限のある担当者によって承認されたセキュリティ及びプライバシー計画。

主たる責任者：認可権限のある担当者又は認可権限のある担当者による指定代理人。

補助的な役割を果たす者：リスクマネジメント担当責任者又はリスク管理者（機能）、最高情報責任者、最高取得責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者。

システム開発ライフサイクルのフェーズ：新規 – 開発／調達。
既存 – 運用／保守。

[83] 変動性は、システムのハードウェア、ソフトウェア、及びファームウェアの要素に実装される管理策において最もよく見られる。例えば、オペレーティングシステム、データベースシステム、アプリケーション、又はネットワークルータを交換又はアップグレードすると、ベンダ又は相手先ブランド供給業者が提供しているセキュリティ管理策が変更される場合がある。また、組織のミッション、ビジネスファンクション、脅威、リスク、及びリスク許容度の変更に伴い、構成設定の調整が必要となる場合もある。

詳解:リスクマネジメント担当責任者又はリスク管理者(機能)、最高情報責任者、政府機関の情報セキュリティ責任者、及び政府機関のプライバシー保護責任者のサポートを得て、認可権限のある担当者又は指定代理人が実施するセキュリティ及びプライバシー計画のレビューでは、計画が完全で一貫性があり、システムのセキュリティ及びプライバシー要件を満たしているかどうかを判断する。このレビュー結果に基づき、認可権限のある担当者又は指定代理人は、セキュリティ及びプライバシー計画の変更を推奨してもよい。計画が受け入れられないものである場合、システム所有者又は共通管理策の提供者が計画を適宜変更する。計画が受け入れられるものである場合、認可権限のある担当者又はその指定代理人が計画を承認する。

セキュリティ及びプライバシー計画の承諾は、SDLC 及びリスクマネジメントプロセスにおける重要なマイルストーンを表す。認可権限のある担当者又は指定代理人は、計画を承認することで、一連の管理策(即ち、システム固有、ハイブリッド、又は共通管理策)と、システム及びその運用環境のセキュリティ及びプライバシー要件を満たすために提案された管理策の実装の記述に同意する [84]。計画の承認により、リスクマネジメントプロセスを RMF *実装*ステップに進めることができる。また、計画の承認は、残りの RMF ステップを正常に完了するために必要な労力のレベルを確立し、システム又は個々のシステム要素の取得のためのセキュリティ及びプライバシーの仕様の基盤を提供する。

参考文献:[SP 800-30]、[SP 800-53]、[SP 800-160 v1](システム要件の定義、アーキテクチャ定義、及び設計定義のプロセス)。

[84] 認可権限のある担当者によるシステムセキュリティ計画の初期レビュー及び承認後、後続のあらゆる認可に関連する行為(例えば、再認証又は継続的な認可)は、システムセキュリティ計画が認可パッケージに含まれているため、固有のレビュー及び承認を提供する。

3.4 実装

目的

実装ステップの目的は、システム及び組織のセキュリティ及びプライバシー計画における管理策を実装し、管理策の実装の具体的な詳細をベースライン構成に文書化することである。

実装のタスク

表 5 は、RMF *実装*ステップのタスク及び期待される成果の概要を示している。
また、適用可能なサイバーセキュリティフレームワークの構成要素も提供されている。

表 5：実装のタスクと成果

タスク	成果
タスク I-1 管理策の実装	· セキュリティ及びプライバシー計画で規定された管理策が実装されている。 ［*サイバーセキュリティフレームワーク*: **PR.IP-1**］ · システムセキュリティ及びプライバシー計画における管理策を実装するために、システムセキュリティ及びプライバシーエンジニアリング方法論が使用されている。 ［*サイバーセキュリティフレームワーク*: **PR.IP-2**］
タスク I-2 管理策の実装情報の更新	· 計画された管理策の実装に対する変更が文書化されている。 ［*サイバーセキュリティフレームワーク*: **PR.IP-1**］ · 管理策の実装中に得られた情報に基づいて、セキュリティ及びプライバシー計画が更新されている。 ［*サイバーセキュリティフレームワーク*: **プロファイル**］

RMF のタスク、責任、及び補助的な役割の概要表へのクイックリンク。

管理策の実装

タスク I-1　セキュリティ及びプライバシー計画における管理策を実装する。

潜在的なインプット：承認されたセキュリティ及びプライバシー計画、システム設計文書、組織のセキュリティ及びプライバシーポリシー及び手順、ビジネスインパクト分析又は重要度分析、エンタープライズアーキテクチャの情報、セキュリティアーキテクチャの情報、プライバシーアーキテクチャの情報、システム、システム要素、及び運用環境に割り振られたセキュリティ及びプライバシー要件のリスト、システム要素の情報、システムコンポーネントのインベントリ、組織レベル及びシステムレベルのリスクアセスメント結果。

期待されるアウトプット：実装された管理策。

主たる責任者：システム所有者、共通管理策の提供者。

補助的な役割を果たす者：情報所有者又は情報管理者、セキュリティアーキテクト、プライバシーアーキテクト、システムセキュリティエンジニア、プライバシーエンジニア、システムセキュリティ責任者、システムプライバシー責任者、エンタープライズアーキテクト、システム管理者。

システム開発ライフサイクルのフェーズ: 新規 – 開発／調達、実装／アセスメント
既存 – 運用／保守。

詳解:組織は、セキュリティ及びプライバシー計画に記載されているとおりに管理策を実装する。管理策の実装は、組織のエンタープライズアーキテクチャ及び関連するセキュリティ及びプライバシーアーキテクチャと整合している。組織は管理策を実装する際に、システムセキュリティ及びプライバシーエンジニアリングの方法論、概念、原則を含むベストプラクティスを使用する。リスクアセスメントは、管理策の実装に様々な技術やポリシーを使用する場合のコスト、利益、リスクのトレードオフに関する決定を導き、情報を提供する。また、組織は、連邦政府又は組織のポリシーに従って、必須の構成設定が確立され、システム要素に実装されていることを確実にする。組織がシステム要素にどのような管理策が実装されるかを直接的に制御できない場合、例えば市販製品(COTS)では、組織は、認定を受けた独立した第三者機関のアセスメント施設(例えば、NIST Cryptographic Module Validation Program Testing Laboratories、National Information Assurance Partnership Common Criteria Testing Laboratories)によってテスト、評価、又は検証されたシステム要素の使用を検討する。テスト、評価、及び検証では、製品を特定の構成内で、及び分離して検討する。管理策の実装では、セキュリティ機能性とアシュアランスを維持しながら、製品をどのようにシステムに統合されるかに対処する。

組織は、管理策を実装する際に、必要に応じてアシュアランス要件にも対処する。アシュアランス要件は、管理策が正しく実装され、意図されたとおりに運用され、システムのセキュリティ及びプライバシー要件を満たすことに関して期待どおりの成果を出すという信頼度を高めるために、管理策の開発者と実装担当者が実施する活動を対象にする。アシュアランス要件は、管理策の設計、開発、及び実装の品質に対処するものである。[85]

システムに継承される共通管理策については、システムセキュリティ及びプライバシーエンジニアが、システムセキュリティ及びプライバシー担当者のサポートを得て、共通管理策の提供者と連携して共通管理策を実装するための最も適切な方法を決定する。システム所有者は、システムに継承される共通管理策の妥当性について判断する際に、共通管理策の提供者が作成した認可パッケージを参照することができる。実装中に、システムに継承されるように前もって選択された共通管理策が、システムの規定されたセキュリティ又はプライバシー要件を満たしていないと判断される場合がある。共通管理策が、その管理策を継承するシステムの要件を満たしていない場合、又は共通管理策に受け入れ難い欠陥がある場合、システム所有者は、実装すべき代替管理策又は補足管理策を識別する。システム所有者は、システムに必要な保護を実現するために、システム固有管理策又はハイブリッド管理策で共通管理策を補完することができる。又は、組織の同意と承認を得て、より大きなリスクを受容することができる。リスクアセスメントは、システムと共通管理策の間のセキュリティ又はプライバシー要件のギャップが、システムに関連するリスクにどのように影響するか、及び特定のリスクを軽減するための代替管理策又は補足管理策のニーズに優先順位を付ける方法を決定する場合がある。

RMF のタスクの適用に認められている柔軟性に矛盾することなく、組織はシステムの開発及び実装時に最初の管理策アセスメントを実施する。SDLC の開発及び実装フェーズと並行してこのようなアセスメントを実施することで、欠陥の早期識別が容易になり、是正措置を開始するための費用対効果の高い方法が提供される。これらのアセスメント中に発見された問題は、認可権限のある担当者に解決を委ねることができる。最初の管理策アセスメントの結果は、アセスメントの遅延やコストがかかる繰り返しを避けるために、認可ステップ中で使用することもできる。その後 SDLC の他のフェーズで再利用されるアセスメント結果は、組織によって確立された再利用の要件を満たしている[86]。

[85] [SP 800-53] は、アシュアランス関連のセキュリティ及びプライバシー管理策のリストを提供している。

[86] アセスメントとアセスメント結果の再利用の詳細については、RMF *アセスメント*ステップ及び [SP 800-53A] を参照。

参考文献:[FIPS 200]、[SP 800-30]、[SP 800-53]、[SP 800-53A]、[SP 800-160 v1](実装、統合、検証、及び移行プロセス)、[SP 800-161]、[IR 8062]、[IR 8179]。

管理策の実装情報の更新

タスク I-2 管理策の「実装された」状態に基づいて、計画された管理策の実装に対する変更を文書化する。

潜在的なインプット:セキュリティ及びプライバシー計画、管理策の実装作業からの情報。

期待されるアウトプット:アセッサーによる使用には十分な実装の詳細で更新されたセキュリティ及びプライバシー計画、システム構成ベースライン。

主たる責任者: システム所有者、共通管理策の提供者。

補助的な役割を果たす者: 情報所有者又は情報管理者、セキュリティアーキテクト、プライバシーアーキテクト、システムセキュリティエンジニア、プライバシーエンジニア、システムセキュリティ責任者、システムプライバシー責任者、エンタープライズアーキテクト、システム管理者。

システム開発ライフサイクルのフェーズ: 新規 – 開発／調達、実装／アセスメント
既存 – 運用／保守。

詳解:セキュリティ及びプライバシー計画とシステム設計文書における管理策の実装の詳細にもかかわらず、計画どおりに管理策を実装することは必ずしも実現可能ではない。そのため、管理策の実装が実施されると、セキュリティ及びプライバシー計画は、実装された管理策の実装の詳細で更新される。更新には、計画されたインプット、期待される動作、及び管理策のアセスメントをサポートするのに十分な詳細を持つ期待されるアウトプットへの変更を含む、実装された管理策の改訂された記述が含まれる。「実装された」管理策の情報を文書化することは、管理策にいつ変更があったのか、それらの変更が認可されているのか、及びこの変更がシステム及び組織のセキュリティ及びプライバシー態勢に及ぼすインパクトを判断するためのケイパビリティ(能力)の提供にとって不可欠である。

参考文献:[SP 800-53]、[SP 800-128]、[SP 800-160 v1](実装、統合、検証、及び移行、構成管理プロセス)。

3.5 アセスメント

目的

アセスメントステップの目的は、実装のために選択された管理策が正しく実装され、意図したとおりに運用され、システム及び組織のセキュリティ及びプライバシー要件を満たすことに関して期待どおりの成果を出しているかどうかを判断することである。

アセスメントのタスク

表 6 は、RMF *アセスメント*ステップのタスク及び期待される成果の概要を示している。また、適用可能なサイバーセキュリティフレームワークの構成要素も提供されている。

表 6:アセスメントのタスクと成果

タスク	成果
タスク A-1 アセッサーの選択	・ 管理策アセスメントを実施するアセッサー又はアセスメントチームが選択されている。 ・ 選択したアセッサー又はアセスメントチームに対して、適切なレベルの独立性が得られている。
タスク A-2 アセスメント計画	・ アセスメントの実施に必要な文書が、アセッサー又はアセスメントチームに提供されている。 ・ セキュリティ及びプライバシーアセスメント計画が策定及び文書化されている。 ・ 管理策アセスメントに対する期待と必要な労力のレベルを確立するために、セキュリティ及びプライバシーアセスメント計画がレビューされ、承認されている。
タスク A-3 管理策アセスメント	・ セキュリティ及びプライバシー計画に従って管理策アセスメントが実施されている。 ・ リスクマネジメントプロセスをタイムリーかつ費用対効果の高いものにするために、以前のアセスメントのアセスメント結果を再利用できる機会が検討されている。 ・ アセスメントの時間、有効性、効率性を高めるために、管理策アセスメントの実施で自動化が最大限に活用されている。
タスク A-4 アセスメント報告書	・ 所見及び推奨事項を記載したセキュリティ及びプライバシーアセスメント報告書が作成されている。
タスク A-5 改善措置	・ システム及び運用環境に実装された管理策の欠陥に対処するための改善措置が実施されている。 ・ アセスメント及びその後の改善措置に基づいて行われた管理策の実装の変更を反映するために、セキュリティ及びプライバシー計画が更新されている。 [*サイバーセキュリティフレーム ワーク*:**プロファイル**]
タスク A-6 行動計画及びマイルストーン	・ セキュリティ及びプライバシーアセスメント報告書で識別された受容できないリスクに対する改善計画を詳述した行動計画及びマイルストーンが策定されている。 [*サイバーセキュリティフレーム ワーク*:**ID.RA-6**]

RMF のタスク、責任、及び補助的な役割の概要表へのクイックリンク。

アセッサーの選択

タスク A-1 実施する管理策アセスメントの種類に適したアセッサー又はアセスメントチームを選択する。

潜在的なインプット：セキュリティ、プライバシー、及び SCRM の計画、プログラムマネジメント管理策の情報、共通管理策の文書、組織のセキュリティ及びプライバシープログラム計画、SCRM 戦略、システム設計文書、エンタープライズ、セキュリティ、及びプライバシーアーキテクチャの情報、システムに適用されるセキュリティ、プライバシー、及び SCRM のポリシー及び手順。

期待されるアウトプット：管理策アセスメントの実施の責任を負うアセッサー又はアセスメントチームの選択。

主たる責任者：認可権限のある担当者又は認可権限のある担当者による指定代理人。

補助的な役割を果たす者：最高情報責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者。

システム開発ライフサイクルのフェーズ：新規 – 開発／調達、実装／アセスメント
既存 – 運用／保守。

詳解：組織は、管理策アセッサーの選択において、必要な技術的専門知識と独立性のレベル[87]の両方を考慮する[88]。組織は、管理策アセッサーが、効果的なアセスメント計画を策定し、プログラムマネジメント、システム固有、ハイブリッド、及び共通管理策のアセスメントを必要に応じて実施するために必要なスキル及び技術的な専門知識を有していることを確実にする。これには、リスクマネジメントの概念及びアプローチに関する一般的な知識、及び実装されたハードウェア、ソフトウェア、及びファームウェアコンポーネントに関する包括的な知識及び経験が含まれる。アセスメントケイパビリティ（能力）が一元管理される組織では、政府機関の情報セキュリティ責任者が、組織のシステムのセキュリティ管理策アセッサー又はアセスメントチームを選択し管理する責任を負う場合がある。セキュリティ及びプライバシーの目的を達成するために管理策を実装される場合があるため、組織は、セキュリティ管理策アセッサーとプライバシー管理策アセッサーの間で必要となる協力の度合いを検討する。

組織は、管理策のセルフアセスメントを実施するか、又は独立した管理策アセッサーのサービスを受けることができる。独立したアセッサーとは、公平なアセスメントを実施できる個人又はグループである。公平性とは、管理策の有効性の決定、又はシステム、共通管理策、又はプログラムマネジメント管理策の開発、運用、維持、又は管理に関して、認識された、又は実際の利益相反がアセッサーにないことを意味する。認可権限のある担当者は、適用される法律、大統領令、指令、規制、ポリシー、又は標準に基づいて、アセッサーの独立性のレベルを決定する。認可権限のある担当者は、アセッサーの独立性に関する決定を導き、情報を提供するのに役立てるために、監察総監室、最高情報責任者、政府機関のプライバシー保護責任者、及び政府機関の情報セキュリティ責任者と協議する。

システムプライバシー責任者は、プライバシー管理策が正しく実装され、意図したとおりに運用され、適用されるプライバシー要件への準拠を確実にし、プライバシーリスクの管理に十分であるかどうかを判断するためのアセスメント方法論と評価基準を識別する責任を負う。政府機関のプライバシー保護責任者は、プライバシー管理策のアセスメントを実施し、アセスメント結果を文書化する責任を負う。組織の判断により、プライバシー管理策は独立したアセッサーによってアセスメントされる場合がある。しかし、すべての場合において、政府機関のプライバシー保護責任者は、独立したアセッサーによって実施されるプライバシー機能を含め、組織のプライバシープログラムに対して責任及び説明責任を負う。政府機関のプライバシー保護責任者は、認可権限のある担当者にプライバシー情報を提供する責任を負う。

参考文献：[FIPS 199]、[SP 800-30]、[SP 800-53A]、[SP 800-55]。

---

[87] [OMB A-130]に従い、プライバシープログラム及びプラクティスの独立した評価は必要ない。ただし、組織は、組織の判断で、独立したプライバシーアセスメントを実施することを選択してもよい。

[88] 組織によっては、システムライフサイクル中の最も早い機会での管理策アセスメントをサポートするために、RMF アセスメントステップよりも前に管理策アセッサーを選択する場合がある。アセッサーの早期の識別及び選択により、組織は、アセスメント範囲に合意することを含め、アセスメント活動の計画を立てることができる。システムセキュリティエンジニアリングアプローチを実装する組織は、システムライフサイクル全体にわたって発生する検証活動及び妥当性確認活動をサポートするために、アセッサーを早期に選択することでもメリットを得る場合がある。

アセスメント計画

タスク A-2 実装された管理策のアセスメントを行うための計画を策定、レビュー、及び承認する。

潜在的なインプット：セキュリティ、プライバシー、及び SCRM の計画、プログラムマネジメント管理策の情報、共通管理策の文書、組織のセキュリティ及びプライバシープログラム計画、SCRM 戦略、システム設計文書、サプライチェーンの情報、エンタープライズ、セキュリティ及びプライバシーアーキテクチャの情報、システムに適用されるセキュリティ、プライバシー、及び SCRM のポリシー及び手順。

期待されるアウトプット：認可権限のある担当者によって承認されたセキュリティ及びプライバシーアセスメント計画。

主たる責任者：認可権限のある担当者又は認可権限のある担当者による指定代理人、管理策アセッサー。

補助的な役割を果たす者：政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、システム所有者、共通管理策の提供者、情報所有者又は情報管理者、システムセキュリティ責任者、システムプライバシー責任者。

システム開発ライフサイクルのフェーズ：新規 – 開発／調達、実装／アセスメント
既存 – 運用／保守。

詳解：セキュリティ及びプライバシーアセスメント計画は、セキュリティ及びプライバシー計画、プログラムマネジメント管理策の文書、及び共通管理策の文書に含まれる実装情報に基づいて、管理策アセッサーによって策定される。組織は、システム又は組織のために単独の統合セキュリティ及びプライバシーアセスメント計画を策定することを選択してもよい。統合アセスメント計画では、管理策アセスメントの役割及び責任を明確にする。アセスメント計画では、管理策アセスメントの目的と、各管理策固有のアセスメント手順も提供する。アセスメント計画には、組織が実施するアセスメントの種類を反映させる。例えば、開発テスト及び評価；独立機関による検証（正当性確認と妥当性確認）；サプライチェーンを含む監査、システム及び共通管理策の認可又は再認可をサポートするアセスメント；プログラムマネジメント管理策アセスメント；継続的監視；及び改善措置の後で実施されるアセスメントが含まれる。

アセスメント計画は、計画が組織のセキュリティ及びプライバシーの目的と整合していること、継続的監視とほぼリアルタイムのリスクマネジメントをサポートする手順、手法、技法、ツール、及び自動化を採用していること、及び費用対効果が高いことを確実にするために、認可権限のある担当者又は認可権限のある担当者による指定代理人によってレビューされ、承認される。承認されたアセスメント計画は、管理策アセスメントに対する期待と、アセスメントの労力のレベルを確立する。承認されたアセスメント計画は、管理策の有効性を判断するために適切なリソースが適用されることを確実にすると同時に、そのような判断をする上で必要なアシュアランスレベルを提供することを確実にするのに役立つ。管理策が契約、省庁間協定、事業協定、ライセンス契約、又はサプライチェーン協定を通じて外部プロバイダによって提供される場合、組織はセキュリティ及びプライバシーアセスメント計画及びアセスメントの結果又は証拠をプロバイダにすることができる。

参考文献：[SP 800-53A]、[SP 800-160 v1]（検証及び妥当性確認プロセス）、[SP 800-161]、[IR 8011 v1].

管理策アセスメント

タスク A-3 アセスメント計画に記述されたアセスメント手順に従って、管理策のアセスメントを行う。

潜在的なインプット：セキュリティ及びプライバシーアセスメント計画、セキュリティ及びプライバシー計画、外部アセスメント又は監査結果（該当する場合）。

期待されるアウトプット：完了した管理策アセスメント及び関連するアセスメントの証拠。

主たる責任者：管理策アセッサー。

補助的な役割を果たす者：認可権限のある担当者又は認可権限のある担当者による指定代理人、システム所有者、共通管理策の提供者、情報所有者又は情報管理者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、システムセキュリティ責任者、システムプライバシー責任者。

システム開発ライフサイクルのフェーズ：新規 – 開発／調達、実装／アセスメント
既存 – 運用／保守。

詳解：管理策アセスメントでは、選択された管理策がどの程度正しく実装され、意図したとおりに運用され、システム及び組織のセキュリティ及びプライバシー要件を満たすことに関して期待どおりの成果を出しているかが判断される。システム所有者、共通管理策の提供者、及び／又は組織は、アセスメント計画に規定されたアセスメント手順を使用して実装された管理策をアセスメントするために、アセッサーの技術スキルと専門知識に依存し、識別された脆弱性又は受容できないリスクを軽減又は排除するために、管理策の欠陥にどのように対処するかについての推奨事項を提供する。政府機関のプライバシー保護責任者は、プライバシー管理策の管理策アセッサーの役割を果たし、システム運用の前にプライバシー管理策の初回のアセスメントを実施し、その後は、プライバシー要件への準拠を確実にし、プライバシーリスクを管理するのに十分な頻度で定期的に管理策をアセスメントする責任を負う[89]。セキュリティ及びプライバシーの両方の目的を達成するために実装される管理策は、セキュリティ及びプライバシー管理策アセッサーの間である程度の協力を必要とする場合がある。アセッサーの所見は、管理策が意図したとおりに運用されているかどうか、及び管理策の欠陥[90]がアセスメント中に発見されたかどうかを事実に基づいて報告するものである。

管理策アセスメントは、SDLC 中の実行可能な早い段階、できれば開発フェーズで実施される。この種のアセスメントは開発テスト及び評価と呼ばれ、管理策が正しく実装され、及び確立された情報セキュリティ及びプライバシーアーキテクチャと整合していることを妥当性確認する。開発テスト及び評価の活動には、例えば、設計とコードのレビュー、回帰テスト、アプリケーションのスキャンが含まれる。SDLC 中の早い段階で識別された欠陥は、より費用対効果が高い方法で解決することができる。アセスメントは、潜在的なサプライヤ又はプロバイダをアセスメントするために、組織が合意又は契約を締結して開発フェーズを開始する前に、調達プロセス中の調達先の選択に先立って必要となる場合がある。SDLC 中に実施された管理策アセスメントの結果は、不必要な遅延やコストがかかるアセスメントの繰り返しを避けるために、認可プロセス中に（組織が定めた再利用基準と整合して）使用することもできる。組織は、アセスメントのスピード、有効性、効率性を向上し、組織のシステムのセキュリティ及びプライバシー態勢の継続的監視をサポートするために、管理策アセスメントを実施するための自動化を最大限に活用できる。

開発プロセス全体を通じて管理策を適用及びアセスメントすることは、反復型開発プロセスに適している場合がある。反復型開発プロセス（アジャイル開発など）が採用される場合、各サイクルが完了するたびに反復型アセスメントが実施される場合がある。同様のプロセスは、システムで使用される市販の IT 製品の管理策のアセスメントに使用される。組織は、セキュリティ及びプライバシー計画のすべての管理策の完全な実装の前に、管理策のアセスメントを開始することを選択してもよい。そうする方がより効率的又は対費用効果が高い場合は、このような段階的なアセスメントが適している。

[89] 政府機関のプライバシー保護責任者は、適用されるポリシーに従ってアセスメント機能を委任することができる。
[90] 脅威エージェントによって悪用される可能性がある管理策の欠陥のみが、脆弱性と見なされる。

共通管理策（即ち、システムに継承される管理策）は、（共通管理策の提供者又は組織によって選ばれたアセッサーによって）個別にアセスメントされ、システムレベルのアセスメントの一部としてアセスメントする必要はない。

組織は、管理策が実装されている情報システム及び運用環境、及び管理策のアセスメントに必要な文書、記録、成果物、テスト結果、及びその他の資料にアセッサーがアクセスできることを確実にする。これには、契約、省庁間協定、事業協定、ライセンス契約、又はサプライチェーン協定を通じて外部プロバイダによって実装される管理策が含まれる。アセッサーは、認可権限のある担当者によって決定された、必要な程度の独立性を有する [91]。継続的監視プロセスにおけるアセッサーの独立性は、継続的な認可及び再認可をサポートするためのアセスメントの再利用を容易にする。

リスクマネジメントプロセスの効率性と費用対効果を高めるため、組織は、組織全体のアセスメントポリシーの一部として、又はセキュリティ及びプライバシープログラム計画の中で、アセスメント結果を再利用するための妥当かつ適切な基準を確立することを選択してもよい。例えば、最近のシステム監査で、選択された管理策の有効性に関する情報が得られた可能性がある。また、市販の情報技術製品のセキュリティ及びプライバシー機能をテスト及び評価する外部プログラム（例えば、Common Criteria Evaluation and Validation Program 及び NIST Cryptographic Module Validation Program）から、以前のアセスメント結果を再利用する機会がもたらされる場合がある。システム開発者又はベンダの以前のアセスメント結果が利用可能な場合、管理策アセッサーは、適切な状況下でこれらの結果をアセスメントに組み込んでもよい。さらに、SDLC の前のステージ（ユニットテスト、機能テスト、受け入れテスト）で別の形式のアセスメント中に管理策の実装がアセスメントされた場合、組織は努力の重複を減らすために、それらの結果の再利用の可能性を検討してもよい。そして最後に、アセスメント結果は、互恵契約をサポートするために再利用することができる。例えば、使用認可をサポートするアセスメント結果を再利用できる（附属書 F を参照）。アセスメント結果の再利用に関する追加情報は、[SP 800-53A]で入手可能である。

参考文献：[SP 800-53A]、[SP 800-160 v1]（検証及び妥当性確認プロセス）、[IR 8011 v1]。

アセスメント報告書

タスク A-4　管理策アセスメントによって得られた所見及び推奨事項を文書化したアセスメント報告書を準備する。

潜在的なインプット：完了した管理策アセスメント及び関連するアセスメントの証拠。

期待されるアウトプット：アセッサーの所見及び推奨事項を詳述している、完成したセキュリティ及びプライバシーアセスメント報告書。

主たる責任者：管理策アセッサー。

補助的な役割を果たす者：システム所有者、共通管理策の提供者、システムセキュリティ責任者、システムプライバシー責任者。

システム開発ライフサイクルのフェーズ：新規 – 開発／調達、実装／アセスメント
既存 – 運用／保守。

詳解：セキュリティ及びプライバシー管理策のアセスメント結果は、実装された管理策の欠陥の修正に関する推奨事項を含め、管理策アセッサーによってアセスメント報告書 [92]に文書化される。組織は、単一の統合されたセキュリティ及びプライバシーアセスメント報告書を作成してもよい。アセスメント報告書は、認可権限のある担当者のために作成される、システム又は共通管理策の認可パッケージの主要な文書である。アセスメント報告書には、情報システム内で実装された、又は情報システムによって継承された管理策の有効性を判断するために必要な、アセッサーの所見に基づく情報が含まれる。アセスメント報告書は、認可権限のある担当者が組織の業務及び資産、個人、他の組織、及び国家に対するリスクを判断する際の重要な要素である。アセスメント報告書で提供される形式と詳細のレベルは、実施される管理策アセスメントの種類、例えば、開発テスト及び評価；独立した検証（正当性確認と妥当性確認）；情報システ

[91] [OMB A-130]に従い、プライバシープログラム及びプラクティスの独立した評価は必要ない。ただし、組織の判断で、組織は独立したプライバシーアセスメントを実施することを選択してもよい。

[92] 同等の報告書がアセスメント報告書に含まれるべき要件を満たしている場合、この同等の報告書自体がアセスメント報告書の構成要素となる。

ム又は共通管理策の認可又は再認可をサポートする独立したアセスメント；改善措置後のアセスメント；独立した評価又は監査；及び継続的監視中のアセスメント、に適している。また、報告形式は組織が規定してもよい。

システム開発ライフサイクル中に得られた管理策アセスメント結果は、中間報告書に文書化され、最終的なセキュリティ及びプライバシーアセスメント報告書に含まれる。SDLC の関連フェーズからのアセスメント結果を文書化した中間報告書を作成することで、アセスメント報告書が進化する文書であるという概念が強化される。中間報告書は、必要に応じて、最終的なアセスメント報告書に情報を提供するために使用される。組織は、管理策アセスメントの所見からエグゼクティブサマリを作成することを選択してもよい。エグゼクティブサマリは、組織の認可権限のある担当者及びその他の利害関係者に、アセスメント、所見、及び管理策の欠陥の対処するための推奨事項の概要を含むアセスメント報告書の要約を提供する。

参考文献：[SP 800-53A]、[SP 800-160 v1]（検証及び妥当性確認プロセス）。

改善措置

タスク A-5 管理策に対する初期段階の改善措置を実施し、改善された管理策を再アセスメントする。

潜在的なインプット：所見及び推奨事項を記載した、完了したセキュリティ及びプライバシーアセスメント報告書、セキュリティ及びプライバシー計画、セキュリティ及びプライバシーアセスメント計画、組織レベル及びシステムレベルのリスクアセスメント結果。

期待されるアウトプット：セキュリティ及びプライバシーアセスメント報告書に基づいて完了した初期段階の改善措置、アセスメントチームによる、実装に対する変更の再アセスメント、更新されたセキュリティ及びプライバシーアセスメント報告書、管理策の実装に対する変更を含む、更新されたセキュリティ及びプライバシー計画。

主たる責任者：システム所有者、共通管理策の提供者、管理策アセッサー。

補助的な役割を果たす者：認可権限のある担当者又は認可権限のある担当者による指定代理人、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、リスクマネジメント担当責任者又はリスク管理者（機能）、情報所有者又は情報管理者、システムセキュリティエンジニア、プライバシーエンジニア、システムセキュリティ責任者、システムプライバシー責任者。

システム開発ライフサイクルのフェーズ：新規 – 開発／調達、実装／アセスメント
既存 – 運用／保守。

詳解：セキュリティ及びプライバシーアセスメント報告書には、システム開発中に解決できなかった、又は開発後に発見された管理策の欠陥が記述される。このような管理策の欠陥は、セキュリティ及びプライバシーリスク（サプライチェーンのリスクを含む）をもたらす可能性がある。管理策アセスメント中に得られた所見は、組織のリスク許容度及び優先順位に基づくリスク対応を容易にする情報を提供する。認可権限のある担当者は、システム所有者又はその他の組織の担当者と相談及び調整して、特定の所見が重大で受容できないリスクを示しており、緊急の改善措置が必要であると判断してもよい。さらに、既存のリソースを利用して迅速かつ容易に改善可能なアセスメントの所見に関して、初期段階の改善措置を実施することが可能かつ現実的である場合がある。

初期段階の改善措置が実施された場合、アセッサーは管理策を再アセスメントする。管理策の再アセスメントでは、改善された管理策がどの程度正しく実装され、意図したとおりに運用され、システム及び組織のセキュリティ及びプライバシー要件を満たすことに関して期待どおりの成果を出しているかを判断する。 アセッサーは、再アセスメントの所見でアセスメント報告書を更新するが、元のアセスメント結果は変更しない。セキュリティ及びプライバシー計画は、管理策アセスメントの所見及び実施されたすべての改善措置に基づいて更新される。更新された計画には、初期段階のアセスメント後の管理策の状態、及びシステム所有者又は共通管理策の提供者が改善措置の推奨事項に対処する際に行ったすべての変更が反映される。管理策アセスメントが完了すると、セキュリティ及びプライバシー計画には、代替管理策を含め、実装されている管理策の正確な記述が含まれる。

組織は、システム所有者と共通管理策の提供者が初期段階のアセスメントの所見に対応する機会を提供する、セキュリティ及びプライバシーアセスメント報告書の補遺を作成することができる。この補遺には、例えば、システム所有者又は共通管理策の提供者がアセッサーの所見に対応して実施した初期段階の改善措置に関する情報を含めてもよい。補遺は、所見に対するシステム所有者又は共通管理策の提供者の視点を提供することもできる。これには、追加の説明資料の提供、特定の所見に対する反論、及び記録の訂正が含まれる可能性がある。この補遺によって、報告書に記載された初期段階のアセッサーの所見を変更する、又は影響を与えることはない。補遺で提供された情報は、リスクベースの認可に関する決定を行う際に、認可権限のある担当者によって考慮される。組織は、アセスメント中に識別された管理策の欠陥に関して実施すべき初期段階の活動を決定するプロセスを実装する。このプロセスは、脆弱性及びリスク、誤検出、及びシステム固有の管理策、ハイブリッド管理策、共通管理策の継続的な有効性を含む、システム及び組織のセキュリティ及びプライバシー態勢に関する有用な情報を認可権限のある担当者に提供するその他の要因に対処することができる。また、この問題解決プロセスにより、実質的な項目のみが識別され、行動計画及びマイルストーンに移行されることを確実にすることができる。

システムレベルの管理策アセスメントからの所見は、システムのリスクアセスメント及び組織のリスクアセスメントの更新を必要とする場合がある [93]。更新されたリスクアセスメント、及びリスクマネジメント担当責任者又はリスク管理者（機能）からのインプットは、初期段階の改善措置及びこれらの活動の優先順位を決定する。システム所有者及び共通管理策の提供者は、システム又は組織のリスクアセスメントに基づいて、特定の所見が重要ではなく、重大なセキュリティ又はプライバシーリスクを示すものではないと判断する場合がある。このような所見は、セキュリティ及びプライバシーアセスメント報告書に保持され、監視ステップ中に監視される。認可権限のある担当者は、アセッサーの所見をレビューして理解し、システムの運用又は共通管理策の使用の結果生じるセキュリティ又はプライバシーリスク（サプライチェーンのリスクを含む）を受容する責任を負う。

いかなる場合でも、組織はアセッサーの所見をレビューし、その所見の重要性、及びその所見が更なる調査又は改善を必要とするかどうかを判断する。最も重要なミッション及びビジネスファンクションをサポートするシステムにリソースを提供する、又は最も大きなリスクをもたらす欠陥を修正するなど、組織のリソースが組織の優先順位に従って効果的に割り振られることを確実にするために、軽減プロセスへの上級幹部の関与が必要となる。

参考文献：[SP 800-53A]、[SP 800-160 v1]（検証及び妥当性確認プロセス）。

行動計画及びマイルストーン

タスク A-6 アセスメント報告書の所見及び推奨事項に基づいて、行動計画及びマイルストーンを準備する。

潜在的なインプット：更新されたセキュリティ又はプライバシーアセスメント報告書、更新されたセキュリティ又はプライバシー計画、組織レベル又はシステムレベルのリスクアセスメント結果、組織のリスクマネジメント戦略及びリスク許容度。

[93] リスクアセスメントは、SDLC 全体を通じて、組織レベル、ミッション／ビジネスレベル、及びシステムレベルで必要に応じて実施される。リスクアセスメントは RMF *準備 － 組織レベル*ステップ、タスク P-3 及び RMF *準備 － システムレベル*ステップ、タスク P-14 の一部として規定される。

期待されるアウトプット：セキュリティ又はプライバシーアセスメント報告書に記載されている改善すべき所見を詳述した行動計画及びマイルストーン。

主たる責任者：システム所有者、共通管理策の提供者。

補助的な役割を果たす者：情報所有者又は情報管理者、システムセキュリティ責任者、システムプライバシー責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、管理策アセッサー、最高取得責任者。

システム開発ライフサイクルのフェーズ：新規 – 実装／アセスメント。
既存 – 運用／保守。

詳解：行動計画及びマイルストーンは、認可パッケージの一部として含まれている。行動計画及びマイルストーンには、管理策のアセスメント中及び継続的監視中に識別された管理策の欠陥を修正するために計画された活動を記述する。行動計画及びマイルストーンには、システムの認可の前又は後に完了することを推奨する達成すべきタスク、タスクの達成に必要なリソース、タスクを達成するために設定されたマイルストーン、及びマイルストーンとタスクの完了予定日が含まれる。行動計画及びマイルストーンは、識別された欠陥を修正するために計画された改善措置に関する合意が得られていることを確実にするために、認可権限のある担当者によってレビューされる。その後、活動の完了の進捗状況を監視するために使用される。欠陥は、認可権限のある担当者によって残留リスクとして受容されるか、あるいはアセスメント中又は認可権限のある担当者への認可パッケージの提出前に是正される。認可権限のある担当者によって欠陥が残留リスクとして受容された場合、行動計画及びマイルストーンの記入は必要ない。ただし、アセスメント又は監視中に識別された欠陥はアセスメント報告書に文書化され、有効な監査証跡を維持するために自動化されたセキュリティ／プライバシー管理報告ツール内に保持することができる。組織は、管理策アセスメント、監査、及び継続的監視から得られたアセスメント結果に基づき、適用される法律、大統領令、指令、ポリシー、規制、標準、又はガイダンスに従って、行動計画及びマイルストーンを策定する。

組織は、組織全体で統一されたリスク軽減のための優先順位付けされたアプローチを使用する、行動計画及びマイルストーン策定プロセスを策定するための一貫したプロセスを実装する。リスクアセスメントは、行動計画及びマイルストーンに含まれる項目の優先順位付けプロセスを導く。このプロセスは、行動計画及びマイルストーンが以下から情報提供されることを確実にする：システムのセキュリティ分類化及びセキュリティ、プライバシー、及びサプライチェーンのリスクアセスメント；管理策の特定の欠陥；識別された管理策の欠陥の重要度（即ち、欠陥がシステムのセキュリティ及びプライバシー態勢、ひいては組織のリスク曝露、又は組織のミッション又はビジネスファンクションを遂行する能力に与える直接的又は間接的影響）；及び識別された管理策の欠陥に対処するために提案されたリスク軽減アプローチ（例えば、リスク軽減措置の優先順位付け及びリスク軽減リソースの割り振り）。リスク軽減リソースには、例えば、人員、新しいハードウェア又はソフトウェア、及びツールが含まれる。

参考文献：[SP 800-30]、[SP 800-53A]、[SP 800-160 v1]（検証及び妥当性確認プロセス）、[IR 8062]。

3.6 認可

目的

*認可*ステップの目的は、システム運用又は共通管理策の使用に基づいて、組織の業務及び資産、個人、他の組織、又は国家に対するセキュリティ及びプライバシーリスク（サプライチェーンのリスクを含む）が受容可能であるかどうかの判断を上級管理職員に義務付けることで、組織の説明責任を提供することである。

認可のタスク

表 7 は、RMF *認可*ステップのタスク及び予想される成果の概要を示している。
また、適用可能なサイバーセキュリティフレームワークの構成要素も提供されている。

表 7：認可のタスクと成果

タスク	成果
タスク R-1 認可パッケージ	・ 認可権限のある担当者に提出する認可パッケージが作成されている。
タスク R-2 リスクの分析及び判断	・ リスク許容度を含むリスクマネジメント戦略を反映した、認可権限のある担当者によるリスク判断が示されている。
タスク R-3 リスク対応	・ 判断されたリスクに対するリスク対応が提供されている。 ［*サイバーセキュリティフレームワーク*: **ID.RA-6**］
タスク R-4 認可の決定	・ システム又は共通管理策の認可が承認又は却下されている。
タスク R-5 認可の報告	・ 認可の決定、重大な脆弱性、及びリスクが組織の担当者に報告されている。

RMF のタスク、責任、及び補助的な役割の概要表へのクイックリンク。

認可パッケージ

タスク R-1　認可パッケージを作成し、認可の決定のために認可権限のある担当者に提出する。

潜在的なインプット：セキュリティ及びプライバシー計画、セキュリティ及びプライバシーアセスメント報告書、行動計画及びマイルストーン、必要に応じて、裏付けとなるアセスメントの証拠又はその他の文書。

期待されるアウトプット：認可パッケージ（エグゼクティブサマリを含む）。認可権限のある担当者に提出するためにセキュリティ及びプライバシー管理ツール [94] から生成してもよい。

主たる責任者：システム所有者、共通管理策の提供者、政府機関のプライバシー保護責任者。[95]

[94] 組織は、認可パッケージ及び認可プロセスをサポートするセキュリティ及びプライバシー情報の準備、作成、及び伝送に自動化ツールを最大限に活用することが推奨される。ハードコピーの文書を削減又は撤廃するために利用できる、多くの市販のガバナンス、リスク、コンプライアンス（GRC）ツールを採用することができる。

[95] 政府機関のプライバシー保護責任者は、PII を処理する情報システムに関与する。

補助的な役割を果たす者: システムセキュリティ責任者、システムプライバシー責任者、政府機関の情報セキュリティ責任者、管理策アセッサー。

システム開発ライフサイクルのフェーズ: 新規 – 実装／アセスメント。
既存 – 運用／保守。

詳解: 認可パッケージ [96] には、セキュリティ及びプライバシー計画、セキュリティ及びプライバシーアセスメント報告書、行動計画及びマイルストーン、及びエグゼクティブサマリが含まれる。認可権限のある担当者の要請に応じて、認可パッケージに追加情報を含めることができる。組織は、認可パッケージの情報の更新の際に、バージョン及び変更管理を維持する。計画、アセスメント報告書、及び行動計画及びマイルストーンのタイムリーな更新を継続的に提供することは、ほぼリアルタイムのリスクマネジメントと継続的な認可の概念をサポートし、必要に応じて、再認可措置に使用することができる。

政府機関のプライバシー保護責任者は、認可権限のある担当者がリスク判断及びリスク受容の決定を行う前に、適用されるプライバシー要件への準拠を確実にし、プライバシーリスクを管理するために、PII を処理するシステムの認可パッケージをレビューする。

認可パッケージ内の情報は、認可権限のある担当者が情報に基づいたリスクベースの意思決定を行うために使用される。管理策が契約、省庁間協定、事業協定、ライセンス契約、又はサプライチェーン協定を通じて外部プロバイダによって実装される場合、組織は、リスクベースの意思決定を行うために必要な情報がプロバイダから入手可能となることを確実にする。
認可パッケージは、認可権限のある担当者にハードコピー又は電子データで提供される場合もあれば、自動化されたセキュリティ／プライバシー管理報告ツールを使用して生成される場合もある。組織は、認可パッケージの内容を準備及び管理する際に、自動化されたサポートツールを使用することができる。自動化されたサポートツールは、組織内の情報システムの継続的なセキュリティ及びプライバシー態勢に関する認可権限のある担当者のための情報を維持、更新するための効果的な手段を提供する。

情報システムが継続的な認可を受けている場合、最も効率的かつタイムリーな方法で情報を提供するために、認可パッケージは自動化された報告書を通じて認可権限のある担当者に提示される [97]。認可権限のある担当者にアセスメント報告書で提示される情報は、情報セキュリティ及びプライバシーの継続的監視プログラムの情報を使用して、組織が決定した形式及び頻度で生成される。

認可権限のある担当者に提示されるアセスメント報告書には、システム固有の管理策、ハイブリッド管理策、又は共通管理策の欠陥に関する情報（即ち、アセッサーによって判断された満足する所見以外の情報）が含まれる。認可権限のある担当者は、実行可能な場合はいつでも、自動化されたセキュリティ／プライバシー管理報告ツール又はその他の自動化手法を使用して、セキュリティ及びプライバシー計画と行動計画及びマイルストーンにアクセスする。認可文書は、組織のリスクマネジメント目的に従って、自動プロセス又は手動プロセスを使用して、組織が定義した頻度で更新される [98]。

[96] 同等の報告書が認可パッケージに含まれるものの要件を満たしている場合、この同等の報告書自体が認可パッケージを構成する。

[97] 認可パッケージのすべてのコンポーネントを完全自動化することが目的であるが、組織は、完全自動化状態への移行の様々な段階、即ち認可パッケージの特定の部分は自動化された手段で利用可能でき、その他の部分は手動でのみ利用できるという状態である可能性がある。

[98] 組織は、認可権限のある担当者が自動化によって利用できるセキュリティ及びプライバシー情報の詳細レベル及び提示形式を決定する。詳細レベル及び形式に関する決定は、認可権限のある担当者の意思決定ニーズに合わせてテーラリングされたセキュリティ及びプライバシー情報の自動提示による組織のニーズに基づく。例えば、詳細なセキュリティ及びプライバシー情報が組織の運用レベルで生成及び収集され、その後、この情報が分析、抽出され、自動化を使用して要約又はハイライトされた形式で認可権限のある担当者に提示される場合がある。

参考文献:[OMB A-130]、[SP 800-18]、[SP 800-160 v1](リスクマネジメントプロセス)、[SP 800-161](SCRM 計画)。

リスクの分析及び判断

タスク R-2 システムの運用又は使用、あるいは共通管理策の提供によるリスクを分析し、判断する。

潜在的なインプット:認可パッケージ、裏付けとなるアスメントの証拠又は必要に応じてその他の文書、リスクマネジメント担当責任者又はリスク管理者(機能)から提供される情報、組織のリスクマネジメント戦略及びリスク許容度、組織レベル又はシステムレベルのリスクアセスメント結果。

期待されるアウトプット:リスク判断。

主たる責任者: 認可権限のある担当者又は認可権限のある担当者による指定代理人。

補助的な役割を果たす者: リスクマネジメント担当責任者又はリスク管理者(機能)、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者。

システム開発ライフサイクルのフェーズ: 新規 – 実装/アセスメント。
既存 – 運用/保守。

詳解:認可権限のある担当者又は指定代理人が、政府機関の情報セキュリティ責任者及び政府機関のプライバシー保護責任者(PII を処理する情報システムの場合)と協力して、管理策アセッサー、システム所有者、又は共通管理策の提供者から提供された認可パッケージの情報を分析し、リスクに関する最終的な判断を下す。認可権限のある担当者がリスクを徹底的に理解することを確実にするために、管理策アセッサー、システム所有者、又は共通管理策の提供者とのさらなる協議が必要な場合がある。

リスクの分析及び判断に影響を与える可能性がある情報[99]を提供するために、リスクアセスメントが採用される。リスクマネジメント担当責任者又はリスク管理者(機能)は、システムの運用又は共通管理策の使用によって生じる、組織の業務及び資産、個人、他の組織、及び国家に対するリスクの最終的な判断で考慮される追加情報を認可権限のある担当者に提供してもよい。追加情報には、例えば、組織のリスク許容度、システムと管理策の間の依存関係、ミッション及びビジネスの要件、システムでサポートするミッション又はビジネスファンクションの重要度、又はリスクマネジメント戦略が含まれる場合がある。

認可権限のある担当者は、リスクを判断する際に、リスクマネジメント担当責任者又はリスク管理者(機能)から提供される情報、又はシステム所有者又は共通管理策の提供者から認可パッケージで提出される情報を分析する。リスクマネジメント担当責任者又はリスク管理者(機能)から提供された追加情報は、文書化され、関連する範囲で認可の決定の一部として含まれる(タスク R-4 を参照)。認可権限のある担当者は、リスクマネジメント担当責任者又はリスク管理者(機能)のインプットに注釈を付けるために、自動化されたセキュリティ/プライバシー管理報告ツールを使用してもよい。

システムが継続的な認可を受けて運用されている場合、リスク判断タスクは実質的に変更されない。認可権限のある担当者は、システムの現在のセキュリティ及びプライバシー態勢を判断するために、自動化されたセキュリティ/プライバシー管理報告ツールから提供される関連するセキュリティ及びプライバシー情報を分析する。

参考文献:[OMB A-130]、[SP 800-30]、[SP 800-39](組織、ミッション/ビジネスプロセス、及びシステムレベル)、[SP 800-137]、[SP 800-160 v1](リスクマネジメントプロセス)、[IR 8062]。

[99] [SP 800-30]は、セキュリティリスクアセスメントの実施に関するガイダンスを提供している。[IR 8062]は、プライバシーリスクアセスメント及び関連するリスク要因に関する情報を提供している。

リスク対応

タスク R-3 判断されたリスクへの対応として望ましい行動方針を識別し、実装する。

潜在的なインプット：認可パッケージ、リスク判断、組織レベル及びシステムレベルのリスクアセスメント結果。

期待されるアウトプット：判断されたリスクに対するリスク対応。

主たる責任者：認可権限のある担当者又は認可権限のある担当者による指定代理人。

補助的な役割を果たす者：リスクマネジメント担当責任者又はリスク管理者（機能）、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、システム所有者又は共通管理策の提供者、情報所有者又は情報管理者、システムセキュリティエンジニア、プライバシーエンジニア、システムセキュリティ責任者、システムプライバシー責任者。

システム開発ライフサイクルのフェーズ：新規 – 実装／アセスメント。
既存 – 運用／保守。

詳解：リスクが分析及び判断された後、組織は、リスクの受容又はリスクの軽減を含む様々な方法でリスクに対応することができる。リスク対応として望ましい行動方針を決定するのに役立てるために、既存のリスクアセスメント結果及びリスク対応手法を使用してもよい [100]。リスクへの対応が軽減の場合、計画された軽減措置が行動計画及びマイルストーンに含まれ、これを使用して追跡される。リスクが軽減されると、、アセッサーが管理策を再アセスメントする。管理策の再アセスメントでは、改善された管理策がどの程度正しく実装され、意図したとおりに運用され、システム及び組織のセキュリティ及びプライバシー要件を満たす上で期待どおりの成果を出しているかを判断する。アセッサーは、再アセスメントの所見でアセスメント報告書を更新するが、元のアセスメント結果は変更しない。セキュリティ及びプライバシー計画は、管理策アセスメントの所見及び実施されたすべての改善措置に基づいて更新される。更新された計画には、初期段階のアセスメント後の管理策の状態、及び改善措置の推奨事項に対処する際のシステム所有者又は共通管理策の提供者によるすべての変更が反映される。

管理策の再アセスメントが完了すると、セキュリティ及びプライバシー計画には、代替管理策を含め、実装されている管理策の正確な記述が含まれる。リスクへの対応が受容の場合、アセスメントプロセスで発見された欠陥は、セキュリティ及びプライバシーアセスメント報告書に文書化されたままになり、リスク要因の変化が監視される [101]。リスクを受容することができるのは認可権限のある担当者のみであるため、認可権限のある担当者は、アセスメント報告書と行動計画及びマイルストーンをレビューし、識別されたリスクを認可前に軽減する必要があるかどうかを判断する責任を負う。リスク対応のための最も適切な行動方針の決定には、何らかの形式での優先順位付けが含まれる場合がある。一部のリスクは、組織にとって、他のリスクよりも、より大きな懸念事項となる場合がある。このような場合、優先順位が低いリスクよりも優先順位が高いリスクに対処するために、より多くのリソースを割り当てる必要がある可能性がある。リスク対応の優先順位付けは、必ずしも優先順位が低いリスクが無視されることを意味しない。むしろ、優先順位の低いリスクへの対応に割り当てられるリソースが少なくなる、又は優先順位の低いリスクへの対応が後になることを意味する可能性がある。リスクベースの意思決定プロセスの重要な部分は、リスク対応に関わらず、ある程度の残留リスクが存在することを認識することである。組織は、組織のリスク許容度に基づいて、受容できる残留リスクの程度を判断する。

参考文献：[SP 800-30]、[SP 800-39]（組織、ミッション／ビジネスプロセス、及びシステムレベル）、[SP 800-160 v1]（リスクマネジメントプロセス）、[IR 8062]、[IR 8179]、[NIST CSF]（コア[識別機能]）。

[100] [SP 800-39]は、リスク対応に関する追加情報を提供している。

[101] 4 つのセキュリティリスク要因は、脅威、脆弱性、起こりやすさ、及びインパクトである。[SP 800-30]及び[SP 800-39]は、セキュリティリスクアセスメント及び関連するリスク要因に関する情報を提供している。[IR 8062]及び 2.3 節は、プライバシーリスク要因及びプライバシーリスクアセスメント実施に関する追加情報を提供している。

認可の決定

タスク R-4 情報システムの運用又は使用、あるいは共通管理策の提供又は使用によるリスクが受容可能かどうかを判断する。

潜在的なインプット：判断されたリスクに対するリスク対応。

期待されるアウトプット：運用認可、使用認可、共通管理策の認可、運用認可の拒否、使用認可の拒否、共通管理策の認可の拒否。

主たる責任者：認可権限のある担当者。

補助的な役割を果たす者：リスクマネジメント担当責任者又はリスク管理者（機能）、最高情報責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、認可権限のある担当者による指定代理人。

システム開発ライフサイクルのフェーズ：新規 – 実装／アセスメント。
既存 – 運用／保守。

詳解：リスクの明確な受容は、認可権限のある担当者の責任であり、組織内の他の担当者に委任することはできない。認可権限のある担当者は、組織の業務（ミッション、機能、イメージ、及び評判を含む）及び資産、個人、他の組織、又は国家に対するリスクが受容可能であるかどうかを判断する際に、多くの要因を考慮する。セキュリティ及びプライバシーの考慮事項と、ミッション及びビジネスのニーズとのバランスを取ることが、受容可能なリスクベースの認可の決定を達成する上で最も重要である [102]。認可権限のある担当者は、認可パッケージ内の情報、他の組織の担当者からのインプット（タスク R-2 を参照）、及び認可の決定に影響を与える可能性があるその他の関連情報をレビューした後、システム又は組織指定の共通管理策の認可の決定を発行する。認可パッケージは、システム又は共通管理策のセキュリティ及びプライバシー態勢に関する最新の情報を提供する。

認可権限のある担当者は、情報システム又は共通管理策の最終的な認可の決定を行う前に、リスクマネジメント担当責任者又はリスク管理者（機能）に相談する。組織のシステム間及び外部システムとの間には潜在的に大きな依存関係があるため、個々のシステムの認可の決定では、現在の残留リスク、組織の行動計画及びマイルストーン、及び組織のリスク許容度を考慮する。

認可の決定は、認可権限のある担当者によって、システム所有者又は共通管理策の提供者、及び必要に応じて他の組織の担当者に伝達される [103]。認可の決定では、運用認可の諸条件、認可の満了日又は時間駆動型認可の頻度、提供されている場合はリスクマネジメント担当責任者又はリスク管理者（機能）からのインプット、及び共通管理策の認可の場合は共通管理策でサポートするシステムのインパクトレベルも伝達する。

システムの場合、認可の決定は、システム所有者に対して、システムの運用又は使用が認可されるか、又は認可されないかを示す。共通管理策の場合、認可の決定は、共通管理策の提供者及び継承するシステムのシステム所有者に対して、共通管理策の提供が認可されるか、又は認可されないかを示す。共通管理策の認可の諸条件は、システム所有者又は共通管理策の提供者が従わなければならない、システムの運用又は管理策に課される特定の制限または限定についての説明を提供する。

---

[102] セキュリティ及びプライバシーの考慮事項とミッション及びビジネスのニーズのバランスを取ることは、受容可能なリスクに基づく認可の決定を達成する上で最も重要であるが、認可権限のある担当者及び政府機関のプライバシー保護責任者が、PII、及び PII を処理する情報システムの適切な保護に関する最終決定に達することができない場合ある。[OMB A-130]は、このような事例を解決する方法に関するガイダンスを提供している。

[103] 組織は、実現可能な場合は常に、自動化されたセキュリティ／プライバシー管理報告ツールを使用すること、システム及び共通管理策の認可パッケージを作成すること、及び継続的な認可においてこれらの認可パッケージを保守することが推奨される。自動化ツールは、文書化のコストを大幅に削減し、意思決定者にとって重要な情報を生成するスピードと効率を上げ、重要なリスクマネジメント情報を更新するためのより効果的な手段を提供することができる。特定の管理策は自動化ツールの使用に適さないため、このような状況では手動による方法が許容されることが認識されている。

認可の満了日は、認可権限のある担当者によって設定され、認可がいつ失効するかを示す。組織は、システムが継続的な認可の下で運用されている場合、即ち、システムのセキュリティ及びプライバシー態勢、及びシステム内で採用された又はシステムによって継承された管理策の継続的な有効性に関して、継続的なリスク判断及びリスク受容活動を実施するために必要な情報を認可権限のある担当者に提供するのに十分なほど継続的監視プログラムが堅牢で成熟している場合、認可の満了日をなくしてもよい。

認可の決定は認可パッケージに含まれ、システム所有者又は共通管理策の提供者に送られる。システム所有者又は共通管理策の提供者は、認可の決定及び認可パッケージを受けとると、認可の諸条件を承認し、実装する。組織は、組織の担当者（共通管理策を継承するシステム所有者、最高情報責任者、リスクマネジメント担当責任者又はリスク管理者（機能）、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、及びシステムセキュリティ及びプライバシー担当者など）が、システム及び共通管理策の認可の決定を含む認可パッケージが利用可能となることを確実にする。認可権限のある担当者は、継続的監視（タスク M-2 を参照）の一環として、システム所有者又は共通管理策の提供者が、確立された認可の諸条件に従っていることを継続的に検証する。

システムが継続的な認可の下で運用されている場合、認可権限のある担当者は、システムの運用又は使用を継続すること、又は継承のための共通管理策の提供を継続することのリスクを明確に理解して受容する責任及び説明責任を負い続ける。継続的な認可の場合、認可の満了日の代わりに認可の頻度が規定される。認可権限のある担当者は、継続的監視戦略の一環として組織が定義した特定の時間駆動型認可の頻度で情報をレビューし、システムの継続的な運用又は共通管理策の提供のリスクが依然として受容可能かどうかを判断する。リスクが依然として受容可能である場合、認可権限のある担当者は組織のプロセスに従って受容を承認する。受容可能ではない場合、認可権限のある担当者は、リスクがもはや受容できないことを示し、更なるリスク対応又は認可の完全な拒否を要求する。

組織は、認可権限のある担当者による継続的なリスク受容を伝達及び承認するプロセスの手続きレベルを決定する。認可権限のある担当者は、継続的な運用認可、継続的な共通管理策の認可、又は継続的な使用認可のために、システム所有者又は共通管理策の提供者が従うべき諸条件を引き続き確立し、伝達してもよい。認可の諸条件は、自動認可の決定の一部として、自動管理報告ツールを通じて伝達される場合がある。

管理策アセスメントが必要なレベルの独立性 [104] を有する資格のあるアセッサーによって実施される場合、アセスメント結果は継続的な認可をサポートし、再認可に適用される場合がある。継続的な認可及び再認可に関する組織のポリシーは、法律、大統領令、指令、規制、及びポリシーと整合する。

附属書 F は、認可の決定、認可の種類、及び認可パッケージの準備に関するガイダンスを提供している。

参考文献：[SP 800-39]（組織、ミッション／ビジネスプロセス、及びシステムレベル）、[SP 800-160 v1]（リスクマネジメントプロセス）。

[104] [OMB A-130]に従い、プライバシープログラムと実施項目の独立した評価は必要ない。ただし、組織の判断で、組織は独立したプライバシーアセスメントを実施することを選択してもよい。

認可の報告

タスク R-5 認可の決定、及び重大なセキュリティ又はプライバシーリスクを示す管理策の欠陥を報告する。

潜在的なインプット:認可の決定。

期待されるアウトプット:システム又は一連の共通管理策の認可の決定を示す報告書、組織のシステムの登録における認可ステータスに関する注釈。

主たる責任者: 認可権限のある担当者又は認可権限のある担当者による指定代理人。

補助的な役割を果たす者: システム所有者又は共通管理策の提供者、情報所有者又は情報管理者、システムセキュリティ責任者、システムプライバシー責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者。

システム開発ライフサイクルのフェーズ: 新規 – 実装／アセスメント。
既存 – 運用／保守。

詳解:認可権限のある担当者は、システム及び共通管理策の認可の決定を、指名された組織の担当者に報告する。これにより、個々のリスク決定を、組織の業務及び資産、個人、他の組織、及び国家に対する組織全体のセキュリティ及びプライバシーリスクのコンテキストで見ることができる。報告は、組織が認可機能を組織内の政府機関の長よりも下のレベルに委任している状況でのみ行われる。認可権限のある担当者はまた、アセスメント及び継続的監視中に気付いた、重大なセキュリティ又はプライバシーリスクを示す悪用可能な欠陥(即ち、脆弱性)も報告する。組織は、報告対象の重大なセキュリティ又はプライバシーリスクを構成するものを決定し、組織のポリシーに反映する。重大な脆弱性又はリスクを示す欠陥は、[NIST CSF]のサブカテゴリ、カテゴリ、及び機能を使用して報告することができる。認可の決定は、組織の判断で、組織全体のシステムの登録プロセスの一部として追跡及び反映してもよい(タスク P-18 を参照)。

参考文献:[SP 800-39](組織、ミッション／ビジネスプロセス、及びシステムレベル)、[SP 800-160 v1](意思決定マネジメント及びプロジェクトアセスメント及び管理策プロセス)、[NIST CSF](コア[識別、防御、検知、対応、及び復旧機能])。

3.7 監視

目的

監視ステップの目的は、リスクマネジメントの決定をサポートするため、情報システム及び組織のセキュリティ及びプライバシー態勢に関する継続的な状況認識を維持することである。

監視のタスク

表 8 は、RMF *監視*ステップのタスク及び予想される成果の概要を示している。
また、適用可能なサイバーセキュリティフレームワークの構成要素も提供されている。

表 8:監視のタスクと成果

タスク	成果
タスク M-1 システム及び環境に対する変更	・ 情報システム及び運用環境が、継続的監視戦略に従って監視されている。 [*サイバーセキュリティフレームワーク*: DE.CM、ID.GV]
タスク M-2 継続的なアセスメント	・ 管理策の有効性の継続的なアセスメントが、継続的監視戦略に従って実施されている。 [*サイバーセキュリティフレームワーク*: ID.SC-4]
タスク M-3 継続的なリスク対応	・ 継続的監視活動のアウトプットが分析され、適切に対応されている。 [*サイバーセキュリティフレームワーク*: RS.AN]
タスク M-4 認可パッケージの更新	・ リスクマネジメント文書が、継続的監視活動に基づいて更新されている。 [*サイバーセキュリティフレームワーク*: RS.IM]
タスク M-5 セキュリティ及びプライバシーに関する報告	・ セキュリティ及びプライバシー態勢を、認可権限のある担当者及びその他の上級幹部及び管理職に報告するプロセスが実施されている。
タスク M-6 継続的な認可	・ 認可権限のある担当者が、継続的監視活動の結果を使用して継続的な認可を実施し、リスク判断及びリスク受容の決定の変更を伝達している。
タスク M-7 システムの廃棄	・ 必要に応じてシステムの廃棄戦略が策定され、実装されている。

RMF のタスク、責任、及び補助的な役割の概要表へのクイックリンク。

システム及び環境に対する変更

タスク M-1　情報システム及びその運用環境の変更を監視し、システムのセキュリティ及びプライバシー態勢に影響を及ぼす変更がないかを確認する。

潜在的なインプット:組織の継続的監視戦略、組織の構成管理ポリシー及び手順、認可されていないシステム変更に対処する組織のポリシー及び手順、セキュリティ又はプライバシー計画、構成変更要求／承認、システム設計文書、セキュリティ及びプライバシーアセスメント報告書、行動計画及びマイルストーン、自動化された監視ツール及び手動監視ツールからの情報。

期待されるアウトプット：更新されたセキュリティ及びプライバシー計画、更新された行動計画及びマイルストーン、更新されたセキュリティ及びプライバシーアセスメント報告書。

主たる責任者：システム所有者又は共通管理策の提供者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者。

補助的な役割を果たす者：リスクマネジメント担当責任者又はリスク管理者（機能）、認可権限のある担当者又は認可権限のある担当者による指定代理人、情報所有者又は情報管理者、システムセキュリティ責任者、システムプライバシー責任者。

システム開発ライフサイクルのフェーズ：新規 – 運用／保守。
既存 – 運用／保守。

詳解：システム及び運用環境は、技術的又は機械的要素、人的要素、物理的又は環境的要素で発生する変更に伴って常に変化する状態にある。技術又は機械的要素の変更には、例えば、ハードウェア、ソフトウェア、又はファームウェアのアップグレードが含まれる。人的要素の変更には、例えば、スタッフの離職又は人員削減が含まれる。また、周囲の物理的及び環境的要素の変更には、例えば、施設の場所又は施設を保護する物理的アクセス制御の変更が含まれる。外部プロバイダによる変更は検出が困難な場合がある。システム及び運用環境の変更を管理、制御、及び文書化するための規律ある構造化されたアプローチ、及び認可の諸条件の順守は、セキュリティ及びプライバシープログラムの不可欠な要素である。組織は、構成及び変更管理をサポートするために、構成管理及び制御プロセスを確立する。[105]

組織内での一般的な活動は、システム又は運用環境の変更をもたらし、システムのセキュリティ及びプライバシー態勢に重大な影響を与える可能性がある。例としては、ハードウェアの設置又は廃棄、構成の変更、確立された構成変更管理プロセス外でのパッチのインストールがある。不正な変更は、敵対者による意図的な攻撃又は認可された職員による不注意なエラーによって発生する場合がある。組織は、確立された構成管理プロセスを順守することに加えて、システムに対する不正な変更を監視し、発生した不正な変更に関する情報を分析して、不正な変更の根本原因を特定する。不正な変更の監視に加えて、組織は、システムのプライバシー態勢に影響を与える認可された変更がないか、システム及び運用環境を継続的に監視する。[106]

不正な変更（又は、システムのプライバシー態勢に影響を与える認可された変更）の根本原因が特定されると、組織はそれに応じて対応する（タスク M-3 を参照）。例えば、不正な変更の根本原因が敵対的な攻撃であると判断された場合、インシデント対応プロセスの開始、侵入検知防止ツール及びファイアウォールの構成の調整、又は将来の攻撃リスクを低減するための追加管理策又はより強力な管理策の実装など、複数の活動が実施される可能性がある。不正な変更の根本原因が、スタッフが確立された構成管理プロセスを順守しなかったことであると判断された場合は、特定の個人に対する改善トレーニングが必要となる可能性がある。

参考文献：[SP 800-30]、[SP 800-128]、[SP 800-137]、[IR 8062]。

[105] [SP 800-128]は、セキュリティに焦点を当てた構成管理（SecCM）に関するガイダンスを提供している。なお、[SP 800-128]で説明している SecCM プロセスには、関連する監視ステップが含まれていることに留意。

[106] 認可されたシステム動作と不正な（認可されていない）システム動作の違いについては、第 2.3 節のセキュリティ及びプライバシーの説明を参照。

継続的なアセスメント

タスク M-2 継続的監視戦略に従って、システム内に実装された、及びシステムによって継承された管理策をアセスメントする。

潜在的なインプット:組織の継続的監視戦略及びシステムレベルの継続的監視戦略(該当する場合)、セキュリティ及びプライバシー計画、セキュリティ及びプライバシーアセスメント計画、セキュリティ及びプライバシーアセスメント報告書、行動計画及びマイルストーン、自動化された監視ツール及び手動監視ツールからの情報、組織レベル及びシステムレベルのリスクアセスメント結果、外部アセスメント又は監査結果(該当する場合)。

期待されるアウトプット:更新されたセキュリティ及びプライバシーアセスメント報告書。

主たる責任者: 管理策アセッサー。

補助的な役割を果たす者: 認可権限のある担当者又は認可権限のある担当者による指定代理人、システム所有者又は共通管理策の提供者、情報所有者又は情報管理者、システムセキュリティ責任者、システムプライバシー責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者。

システム開発ライフサイクルのフェーズ: 新規 – 運用/保守。
既存 – 運用/保守。

詳解:システム又は共通管理策の最初の認可後、組織は、すべての管理策を継続的にアセスメントする。管理策の有効性の継続的なアセスメントは、組織の継続的監視活動の一部である。各管理策の監視頻度は、組織の継続的監視戦略(タスク P-7 を参照)に基づいており、システムレベルの継続的監視戦略(タスク S-5 を参照)によって補完することができる。認可の決定の一部として認可権限のある担当者によって規定された諸条件の順守も監視される(タスク M-1 を参照)。継続的監視の一部として生成された情報は関連付けられ、分析され、上級幹部へ報告されるので、継続的な管理策のアセスメントが継続される。

継続的な管理策のアセスメントのために、アセッサーは、認可権限のある担当者によって決定された必要なレベルの独立性を有する [107]。継続的監視中のアセッサーの独立性は、プロセスに効率性をもたらし、継続的な認可をサポート及び再認可が必要な場合にアセスメント結果の再利用することを可能にする場合がある。

FISMA の年次セキュリティアセスメントの要件を満たすために、組織は、認可、継続的な認可、又は再認可中;又は、継続的監視中;あるいは SDLC 又は監査の一環としてのシステムのテスト及び評価中に生じた管理策アセスメントのアセスメント結果を使用することができる(ただし、そのアセスメント結果が最新で、管理策の有効性の判断に関連し、必要なレベルの独立性を有するアセッサーによって得られたものであることが条件)。既存のアセスメント結果は、組織によって確立された再利用ポリシーに沿って再利用され、必要に応じて追加のアセスメントによって補完される。アセスメント結果の再利用は、情報システム及び組織のセキュリティ態勢を判断するために必要な証拠を作成できる、費用対効果の高いセキュリティプログラムを実現するのに役立つ。最後に、管理策アセスメントをサポートするための自動化の使用は、アセスメントの頻度、量、範囲の拡大を容易にする。

参考文献:[SP 800-53A]、[SP 800-137]、[SP 800-160 v1](検証、妥当性確認、運用、及び保守プロセス)、[IR 8011 v1]。

継続的なリスク対応

タスク M-3 継続的な監視活動及びリスクアセスメントの結果、並びに、行動計画及びマイルストーンの未実施項目に基づいて、リスクに対応する。

[107] [OMB A-130]に従い、プライバシープログラム及びプラクティスの独立した評価は要求されていない。ただし、組織の判断で、組織は独立したプライバシーアセスメントを採用することを選択してもよい。

潜在的なインプット：セキュリティ及びプライバシーアセスメント報告書、組織レベル及びシステムレベルのリスクアセスメント結果、セキュリティ及びプライバシー計画、行動計画及びマイルストーン。

期待されるアウトプット：軽減措置又はリスク受容の決定、更新されたセキュリティ及びプライバシーアセスメント報告書。

主たる責任者：認可権限のある担当者、システム所有者、共通管理策の提供者。

補助的な役割を果たす者：リスクマネジメント担当責任者又はリスク管理者（機能）、政府機関のプライバシー保護責任者、認可権限のある担当者による指定代理人、情報所有者又は情報管理者、システムセキュリティ責任者、システムプライバシー責任者、システムセキュリティエンジニア、プライバシーエンジニア、セキュリティアーキテクト、プライバシーアーキテクト。

システム開発ライフサイクルのフェーズ：新規 – 運用／保守。
既存 – 運用／保守。

詳解：継続的監視中にアセッサーによって作成されたアセスメント情報は、更新されたアセスメント報告書、又は自動化されたセキュリティ／プライバシー管理及び報告ツールからの報告書を通じて、システム所有者及び共通管理策の提供者に提供される。認可権限のある担当者は、アセスメントの所見に対する適切なリスク対応を判断するか、システム所有者及び共通管理策の提供者によって提案された対応を承認する。その後、システム所有者及び共通管理策の提供者が、適切なリスク対応を実装する。リスク対応が受容の場合、所見は、セキュリティ及びプライバシーアセスメント報告書に文書化されたままとなり、リスク要因の変化が監視される。リスク対応が軽減の場合、計画された軽減措置は、行動計画及びマイルストーンに含まれ、これを使用して追跡される。認可権限のある担当者によって要求された場合、管理策アセッサーは、改善措置の推奨事項を提供する場合がある。改善措置の推奨事項は、自動化されたセキュリティ／プライバシー管理報告ツールによって提供される場合もある。組織のリスクアセスメント（タスク P-3）及びシステムレベルのリスクアセスメントの結果（タスク P-14）は、継続的なリスク対応に関する決定を導き、情報を提供する。継続的なリスク対応の一環として修正、拡張、又は追加された管理策は、新規、修正された、又は拡張された管理策が正しく実装され、意図したとおりに運用され、システム及び組織のセキュリティ及びプライバシー要件を満たす上で期待どおりの成果を出していること確実にするために、アセッサーによって再アセスメントされる。

参考文献：[SP 800-30]、[SP 800-53]、[SP 800-53A]、[SP 800-137]、[SP 800-160 v1]（リスクマネジメントプロセス）、[IR 8011 v1]、[IR 8062]、[NIST CSF]（コア[対応機能]）。

認可パッケージの更新

タスク M-4　継続的監視プロセスの結果に基づいて、計画、アセスメント報告書、並びに、行動計画及びマイルストーンを更新する。

潜在的なインプット：セキュリティ及びプライバシーアセスメント報告書、組織レベル及びシステムレベルのリスクアセスメント結果、セキュリティ及びプライバシー計画、行動計画及びマイルストーン。

期待されるアウトプット：更新されたセキュリティ及びプライバシーアセスメント報告書、[108] 更新された行動計画及びマイルストーン、更新されたリスクアセスメント結果、更新されたセキュリティ及びプライバシー計画。

主たる責任者：システム所有者、共通管理策の提供者。

補助的な役割を果たす者：情報所有者又は情報管理者、システムセキュリティ責任者、システムプライバシー責任者、政府機関のプライバシー保護責任者、政府機関の情報セキュリティ責任者。

システム開発ライフサイクルのフェーズ：新規 – 運用／保守。
既存 – 運用／保守。

[108] 同等の報告書がアセスメント報告書に含まれるべき要件を満たしている場合（例えば、セキュリティ又はプライバシー管理報告ツールから生成された報告書）、この同等の報告書自体がアセスメント報告書の構成要素となる。

詳解：ほぼリアルタイムのリスクマネジメントを実現するために、組織は、セキュリティ及びプライバシー計画、セキュリティ及びプライバシーアセスメント報告書、及び行動計画及びマイルストーンを継続的に更新する。計画の更新は、システム所有者又は共通管理策の提供者によって実施されるリスク軽減活動に基づいた管理策の修正を反映している。管理策アセスメント報告書の更新は、計画の実装詳細に基づいて管理策の有効性を判断するために実施された追加のアセスメント活動を反映している。行動計画及びマイルストーンは、現時点での未実施項目の進展に基づいて更新され、管理策の有効性の監視の一環として発見されたセキュリティ及びプライバシーリスクに対処し、システム所有者又は共通管理策の提供者がこれらのリスクにどのように対処しようとしているかを説明する。更新された情報は、システムのセキュリティ及びプライバシー態勢、及びシステムによって継承される共通管理策に対する認識を高め、これにより、ほぼリアルタイムのリスクマネジメント及び継続的な認可プロセスをサポートする。

リスクマネジメント情報の更新頻度は、連邦政府及び組織のポリシーに従い、システム所有者、共通管理策の提供者、及び認可権限のある担当者の判断によるものであり、組織又はシステムレベルの継続的監視戦略と整合している。システムのセキュリティ及びプライバシー態勢及びシステムによって継承される管理策に関する情報の更新は、提供される情報が認可権限のある担当者又は組織内の他の上級幹部による継続的な活動及び決定に影響を与えるため、正確かつタイムリーである。自動化されたサポートツール及び組織全体でのセキュリティ及びプライバシープログラムマネジメントのプラクティスの使用は、認可権限のある担当者がシステムの現在のセキュリティ及びプライバシー態勢に容易にアクセスできることを確実にする。現在のセキュリティ及びプライバシー態勢への容易なアクセスは、継続的監視及び継続的な認可をサポートし、組織の業務及び資産、個人、他の組織、及び国家に対するリスクのほぼリアルタイムの管理が促進する。

組織は、セキュリティ及びプライバシー計画、アセスメント報告書、及び行動計画及びマイルストーンを更新する際に、監督、管理、及び監査のために必要な情報が修正又は破棄されないことを確実にする。構成管理手順を通じてシステムへの変更を追跡する効果的な手法を提供することは、組織のセキュリティ及びプライバシー活動における透明性とトレーサビリティの達成、セキュリティ又はプライバシー活動に対する個人の説明責任の獲得、及び組織のセキュリティ及びプライバシープログラムの最新動向の理解のために必要である。

参考文献：[SP 800-30]、[SP 800-53A]。

セキュリティ及びプライバシーに関する報告

タスク M-5　組織の継続的監視戦略に従い、システムのセキュリティ及びプライバシー態勢を、認可権限のある担当者及び他の組織の担当者に継続的に報告する。

潜在的なインプット：セキュリティ及びプライバシーアセスメント報告書、行動計画及びマイルストーン、組織レベル及びシステムレベルのリスクアセスメント結果、組織レベル及びシステムレベルの継続的監視戦略、セキュリティ及びプライバシー計画、サイバーセキュリティフレームワークプロファイル。

期待されるアウトプット：セキュリティ及びプライバシー態勢に関する報告書。[109]

主たる責任者：システム所有者、共通管理策の提供者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者。

補助的な役割を果たす者：システムセキュリティ責任者、システムプライバシー責任者。

システム開発ライフサイクルのフェーズ：新規 – 運用／保守。
既存 – 運用／保守。

[109] 同等の報告書がセキュリティ及びプライバシー態勢に関する報告書に含まれるべき要件を満たしている場合（例えば、セキュリティ又はプライバシー管理報告ツールから生成された報告書）、この同等の報告書が態勢に関する報告書の構成要素となる。

詳解：監視活動の結果は、組織の継続的監視戦略に従って、文書化され、認可権限のある担当者及び選択された他の組織の担当者に継続的に報告される。セキュリティ及びプライバシー態勢に関する報告書を受け取る可能性のある他の組織の担当者には、例えば、最高情報責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、リスクマネジメント担当責任者又はリスク管理者（機能）、情報所有者又は情報管理者、インシデント対応担当の役割、及び緊急時対応計画担当の役割が含まれる。セキュリティ及びプライバシー態勢に関する報告は、事象駆動型、時間駆動型、又は事象及び時間駆動型にすることができる [110]。この報告書は、実装された管理策の有効性を含む、システムのセキュリティ及びプライバシー態勢に関する情報を、認可権限のある担当者及び他の組織の担当者に提供する。セキュリティ及びプライバシー態勢に関する報告書には、システム所有者又は共通管理策の提供者によって採用された継続的監視活動が記述される。また、この報告書には、管理策アセスメント、監査、及び継続的監視中に発見されたシステム及び運用環境のセキュリティ及びプライバシーリスクに関する情報、及び、システム所有者又は共通管理策の提供者によるこれらのリスクへの対応方法の計画も含まれる。

組織は、セキュリティ及びプライバシー態勢に関する報告書の範囲、深さ、手続き、書式、形式について柔軟性を有している。目標は、システム及び運用環境の現在のセキュリティ及びプライバシー態勢並びに現在の態勢が個人、組織のミッション、及びビジネスファンクションにどのように影響するかを伝えながら、認可権限のある担当者及び必要に応じてその他の組織の担当者と効率的で継続的なコミュニケーションを図ることである。少なくとも、セキュリティ及びプライバシー態勢に関する報告書には、前回の報告以降に生じた、セキュリティ及びプライバシー計画、セキュリティ及びプライバシーアセスメント報告書、及び行動計画及びマイルストーンの変更を要約する。組織による自動化されたセキュリティ／プライバシー管理報告ツール（例えば、ダッシュボード）の使用は、セキュリティ及びプライバシー態勢に関する報告の有効性と適時性を促進する。

セキュリティ及びプライバシー態勢に関する報告書の頻度は、組織の判断に委ねられており、連邦政府及び組織のポリシーに従う。報告書は、システム又は共通管理策に関するセキュリティ及びプライバシー情報を伝送するために適切な間隔で発生するが、不要な労力やコストを生じるほど頻繁ではない。認可権限のある担当者は、再認可措置が必要かどうかを判断するために、セキュリティ及びプライバシー態勢に関する報告書を使用し、リスクマネジメント担当責任者又はリスク管理者（機能）、政府機関の情報セキュリティ責任者、及び政府機関のプライバシー保護責任者と相談する。

セキュリティ及びプライバシー態勢に関する報告書は、連邦政府又は組織のポリシーに従って、評価され、保護され、取り扱われる。セキュリティ及びプライバシー態勢に関する報告書は、セキュリティ及びプライバシー上の弱点又は欠陥の改善措置を文書化することに関する FISMA の報告要件を満たすために使用することができる。セキュリティ及びプライバシー態勢に関する報告は、継続的に実施されることを意図しており、最初の認可のために提供された情報に関連する時間、費用、及び手続きを必要とすると解釈すべきではない。むしろ、報告は、報告の目的の達成と整合する費用対効果が高い方法で実施される。

参考文献：[SP 800-53A]、[SP 800-137]、[NIST CSF]（コア[識別、防御、検知、対応、復旧機能]）。

継続的な認可

タスク M-6 リスクが依然として受容可能かどうかを判断するために、システムのセキュリティ及びプライバシー態勢を継続的にレビューする。

潜在的なインプット：リスク許容度、セキュリティ及びプライバシー態勢に関する報告書、行動計画及びマイルストーン、組織レベル及びシステムレベルのリスクアセスメント結果、セキュリティ及びプライバシー計画。

期待されるアウトプット：リスク判断、継続的な運用認可、継続的な使用認可、継続的な共通管理策の認可、継続的な運用認可の拒否、継続的な使用認可の拒否、継続的な共通管理策の認可の拒否。

[110] 時間駆動型及び事象駆動型の認可及び報告に関する追加情報ついては、附属書 F を参照。

主たる責任者: 認可権限のある担当者。

補助的な役割を果たす者: リスクマネジメント担当責任者又はリスク管理者(機能)、最高情報責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、認可権限のある担当者による指定代理人。

システム開発ライフサイクルのフェーズ: 新規 – 運用／保守。
既存 – 運用／保守。

詳解:継続的な認可アプローチを採用するために、組織は、実装された管理策を継続的にアセスメントするための組織レベル及びシステムレベルの継続的監視プロセスを導入する[111]。継続的監視プロセスから得られた所見及び結果は、ほぼリアルタイムのリスクベースの意思決定をサポートするために、認可権限のある担当者に有用な情報を提供する。タスク R-4 のガイダンスに従い、認可権限のある担当者又は指定代理人は、組織の業務及び資産、個人、他の組織、及び国家に対する現在のリスクを判断するために、システムのセキュリティ及びプライバシー態勢(実装された管理策の有効性を含む)を継続的にレビューする。認可権限のある担当者は、現在のリスクが受容可能かどうかを判断し、システム所有者又は共通管理策の提供者に適切な指示を与える。認可権限のある担当者が、リスクが依然として継続的運用のための受容可能なレベルであると判断する場合、又はリスクが継続的運用のための受容可能なレベルではなくなったかを判断し、運用認可、使用認可、又は共通管理策の認可の拒否を発行する場合がある。

報告書には、セキュリティ又はプライバシーリスク要因の変更が示されている場合があるので、セキュリティ及びプライバシー態勢に関する報告書で提供される情報に基づいてリスクが変更される場合がある。状況の変化が組織のリスク及び個人のリスクにどのように影響するかを判断することは、プライバシーリスクを管理し、適切なセキュリティを維持する上で不可欠である。継続的なリスク判断及びリスク受容を実施することで、認可権限のある担当者は、システム及び共通管理策の認可を長期にわたって維持し、継続的な認可に移行することができる。再認可措置は、連邦政府又は組織のポリシー従ってのみ行われる。認可権限のある担当者は、更新されたリスク判断及びリスク受容の結果を、リスクマネジメント担当責任者又はリスク管理者(機能)に伝達する。

セキュリティ及びプライバシー態勢の情報を取得、整理、定量化、視覚表示、及び維持管理するための自動化サポートツールを使用することで、組織のリスク態勢に関連するほぼリアルタイムのリスクマネジメントが促進される。測定基準及びダッシュボードの使用は、データを自動化された方法で統合し、分かりやすい形式で組織内の様々なレベルの意思決定者に提供することで、リスクベースの意思決定を行う組織のケイパビリティ(能力)を向上させる。

参考文献:[SP 800-30]、[SP 800-39](組織、ミッション／ビジネスプロセス、及びシステムレベル)、[SP 800-55]、[SP 800-160 v1](リスクマネジメントプロセス)、[IR 8011 v1]、[IR 8062]。

システムの廃棄

タスク M-7 システムの廃棄戦略を実装し、システムが運用から除外される際に必要な措置を実行する。

潜在的なインプット:セキュリティ及びプライバシー計画、組織レベル及びシステムレベルのリスクアセスメント結果;システムコンポーネントのインベントリ。

期待されるアウトプット:廃棄戦略、更新されたシステムコンポーネントのインベントリ、更新されたセキュリティ又はプライバシー計画。

主たる責任者: システム所有者。

補助的な役割を果たす者: 認可権限のある担当者又は認可権限のある担当者による指定代理人、情報所有者又は情報管理者、システムセキュリティ責任者、システムプライバシー責任者、リスクマネジメント担当責任者又はリスク管理者(機能)、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者。

システム開発ライフサイクルのフェーズ: 新規 – 適用なし。
既存 – 廃棄。

[111] 継続的な認可及び継続的監視の追加情報については、附属書 F を参照。

詳解：システムが運用から除外される際には、様々なリスクマネジメント活動が必要になる。組織は、システムの廃棄に対処する管理策が実装されていることを確実にする。例としては、媒体のサニタイズ、構成管理及び制御、コンポーネントの真正性、及び記録の保存がある。サービスから除外されるシステムを示すために、組織の追跡及びマネジメントシステム（インベントリシステムを含む）が更新される。セキュリティ及びプライバシー態勢に関する報告書には、システムのセキュリティ及びプライバシー状況が反映される。廃棄されるシステムでホストされているユーザ及びアプリケーション所有者に必要に応じて通知され、すべての管理策の継承関係がレビューされ、インパクトがアセスメントされる。このタスクは、運用から除外されるシステム要素にも適用される。システムを運用から除外する組織は、除外を反映するために、情報システムのインベントリを更新する。システム所有者及びセキュリティ担当者は、廃棄されたシステムが、該当する連邦法、規制、指令、ポリシー、及び標準を順守していることを確実にする。

参考文献：[SP 800-30]、[SP 800-88]、[IR 8062].

附属書 A

参考文献

法律、ポリシー、指令、規制、標準、及びガイドライン

法律及び大統領令	
[32 CFR 2002.4]	Title 32 Code of Federal Regulations, Sec. 2002.4, *Definitions*.2018 ed. https://www.govinfo.gov/app/details/CFR-2018-title32-vol6/CFR-2018-title32-vol6-sec2002-4
[40 USC 11331]	Title 40 U.S. Code, Sec. 11331, *Responsibilities for Federal information systems standards*. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title40/USCODE-2017-title40-subtitleIII-chap113-subchapIII-sec11331
[44 USC 3301]	Title 44 U.S. Code, Sec. 3301, *Definition of records*. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap33-sec3301
[44 USC 3502]	Title 44 U.S. Code, Sec. 3502, *Definitions*. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapI-sec3502
[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
[44 USC 3554]	Title 44 U.S. Code, Sec. 3554, *Federal agency responsibilities*. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapII-sec3554
[44 USC 3601]	Title 44 U.S. Code, Sec. 3601, *Definitions*. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap36-sec3601
[PRIVACT]	Privacy Act (P.L. 93-579), December 1974. https://www.govinfo.gov/app/details/STATUTE-88/STATUTE-88-Pg1896
[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/app/details/PLAW-104publ231
[FISMA]	Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.govinfo.gov/app/details/PLAW-113publ283
[EO 13800]	Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 2017. https://www.govinfo.gov/app/details/FR-2017-05-16/2017-10004

ポリシー、規制、指令、及び指示	
[OMB A-123]	Office of Management and Budget Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/ m-16-17.pdf
[OMB A-130]	Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource*, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
[OMB M-13-13]	Office of Management and Budget Memorandum M-13-13, *Open Data Policy-Managing Information as an Asset*, May 2013. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf
[OMB M-17-25]	Office of Management and Budget Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-17-25.pdf
[OMB M-19-03]	Office of Management and Budget Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program*, December 2018. https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf
[CNSSI 1253]	Committee on National Security Systems Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, March 2014. https://www.cnss.gov/CNSS/issuances/Instructions.cfm
[CNSSI 4009]	Committee on National Security Systems Instruction 4009, *Committee on National Security Systems (CNSS) Glossary*, April 2015. https://www.cnss.gov/CNSS/issuances/Instructions.cfm
[CNSSD 505]	Committee on National Security Systems Directive 505, *Supply Chain Risk Management*, August 2017. https://www.cnss.gov/CNSS/issuances/Directives.cfm
[OCIO HVA]	Office of the Federal Chief Information Officer, *The Agency HVA Process*. https://policy.cio.gov/hva/process
[DODI 5200.44]	Department of Defense Instruction 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks* (TSN), July 2017. http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf
標準、ガイドライン、及び報告書	
[IEEE 610.12]	Institute of Electrical and Electronics Engineers (IEEE) Std. 610.12-1990, *IEEE Standard Glossary of Software Engineering Terminology*, December 1990. https://ieeexplore.ieee.org/iel1/2238/4148/00159342.pdf

[ISO 15026-1] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15026-1:2013, *Systems and software engineering—Systems and software assurance—Part 1: Concepts and vocabulary*, May 2015. https://www.iso.org/standard/62526.html

[ISO 15288] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15288:2015, *Systems and software engineering—Systems life cycle processes*, May 2015. https://www.iso.org/standard/63711.html

[ISO 15408-1] International Organization for Standardization/International Electrotechnical Commission 15408-1:2009, *Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model*. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

[ISO 15408-2] International Organization for Standardization/International Electrotechnical Commission 15408-2:2008, *Information technology—Security techniques—Evaluation criteria for IT security—Part 2: Security functional requirements*. https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf

[ISO 15408-3] International Organization for Standardization/International Electrotechnical Commission 15408-3:2008, *Information technology—Security techniques—Evaluation criteria for IT security—Part 3: Security assurance requirements*. https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

[ISO 27001] International Organization for Standardization/International Electrotechnical Commission 27001:2013, *Information Technology—Security techniques—Information security management systems—Requirements*. https://www.iso.org/standard/54534.html

[ISO 29148] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 29148:2011, *Systems and software engineering—Life cycle processes—Requirements engineering*, December 2011. https://www.iso.org/standard/45171.html

[FIPS 199] National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. https://doi.org/10.6028/NIST.FIPS.199

[FIPS 200] National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. https://doi.org/10.6028/NIST.FIPS.200

[SP 800-18] National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006. https://doi.org/10.6028/NIST.SP.800-18r1

[SP 800-30] National Institute of Standards and Technology Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, September 2012. https://doi.org/10.6028/NIST.SP.800-30r1

[SP 800-39] National Institute of Standards and Technology Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011. https://doi.org/10.6028/NIST.SP.800-39

[SP 800-47] National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002. https://doi.org/10.6028/NIST.SP.800-47

[SP 800-53] National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013. https://doi.org/10.6028/NIST.SP.800-53r4

[SP 800-53A] National Institute of Standards and Technology Special Publication 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, July 2008. https://doi.org/10.6028/NIST.SP.800-53Ar4

[SP 800-55] National Institute of Standards and Technology Special Publication 800-55, Revision 1, *Performance Measurement Guide for Information Security*, December 2014. https://doi.org/10.6028/NIST.SP.800-55r1

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

[SP 800-60 v1] National Institute of Standards and Technology Special Publication 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008. https://doi.org/10.6028/NIST.SP.800-60v1r1

[SP 800-60 v2] National Institute of Standards and Technology Special Publication 800-60, Volume 2, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices*, August 2008. https://doi.org/10.6028/NIST.SP.800-60v2r1

[SP 800-61] National Institute of Standards and Technology Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide*, August 2012. https://doi.org/10.6028/NIST.SP.800-61r2

[SP 800-64] National Institute of Standards and Technology Special Publication 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, October 2008. https://doi.org/10.6028/NIST.SP.800-64r2

[SP 800-82] National Institute of Standards and Technology Special Publication 800-82, Revision 2, *Guide to Industrial Control Systems (ICS) Security*, May 2015. https://doi.org/10.6028/NIST.SP.800-82r2

[SP 800-88] National Institute of Standards and Technology Special Publication 800-88, *Guidelines for Media Sanitization*, December 2014. https://doi.org/10.6028/NIST.SP.800-88r1

[SP 800-128] National Institute of Standards and Technology Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011. https://doi.org/10.6028/NIST.SP.800-128

[SP 800-137] National Institute of Standards and Technology Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011. https://doi.org/10.6028/NIST.SP.800-137

[SP 800-160 v1] National Institute of Standards and Technology Special Publication 800-160, Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, November 2016. https://doi.org/10.6028/NIST.SP.800-160v1

[SP 800-161] National Institute of Standards and Technology Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, April 2015. https://doi.org/10.6028/NIST.SP.800-161

[SP 800-181] National Institute of Standards and Technology Special Publication 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, August 2017. https://doi.org/10.6028/NIST.SP.800-181

[IR 8011 v1] National Institute of Standards and Technology Interagency Report 8011, Volume 1, *Automation Support for Security Control Assessments: Overview*, June 2017. https://doi.org/10.6028/NIST.IR.8011-1

[IR 8062] National Institute of Standards and Technology Internal Report 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, January 2017. https://doi.org/10.6028/NIST.IR.8062

[IR 8179] National Institute of Standards and Technology Internal Report 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components*, April 2018. https://doi.org/10.6028/NIST.IR.8179

その他の出版物及びウェブサイト

[DSB 2013] Department of Defense, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, January 2013. https://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf

[NARA CUI] National Archives and Records Administration, *Controlled Unclassified Information (CUI) Registry*. https://www.archives.gov/cui

[NARA RECM] National Archives and Records Administration, *NARA Records Management Guidance and Regulations*. https://www.archives.gov/records-mgmt/policy/guidance-regulations.html

[NIST CSF] National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), Version 1.1, April 2018. https://www.nist.gov/cyberframework

[OMB FEA] Office of Management and Budget, *Federal Enterprise Architecture (FEA)*. https://obamawhitehouse.archives.gov/omb/e-gov/fea

付属書 B
用語集

共通の用語とその定義

附属書 B では、Special Publication 800-37 で使用されている用語の定義を示す。本出版物で使用されて用語の出典は、適宜引用する。引用元が記載されていない場合、定義の出典は Special Publication 800-37 である。

適切なセキュリティ（adequate security） [OMB A-130]	情報の不正アクセス、不正利用、漏えい、破壊、改ざん、破棄から生じるリスクに見合ったセキュリティ保護。これには、政府機関に代わって運用される情報、政府機関が使用する情報システム及びアプリケーションが、費用対効果の優れたセキュリティ管理策を適用することによって、効率的に機能し、適切な機密性、完全性、及び可用性の保護を提供することを保証することが含まれる。
政府機関（agency） [OMB A-130]	行政機関又は省庁、軍事部門、連邦政府法人、連邦政府が管理する法人、又は連邦政府の行政機関内のその他の施設、又は独立した規制機関。
割り振り（allocation）	組織が情報システム又はその運用環境にセキュリティ要件やプライバシー要件を割り当てたり、セキュリティ又はプライバシーケイパビリティを提供することに責任を持つ特定のシステム要素（ルータ、サーバ、リモートセンサなど）に管理策を割り当てたりするために使用するプロセス。
アプリケーション（application）	情報システムにおいて運用されるソフトウェアプログラム。
アセスメント（assessment）	*管理策アセスメント（control assessment）又はリスクアセスメント（risk assessment）*を参照。
アセスメント計画（assessment plan）	管理策アセスメントの目的、及びそのようなアセスメントの実施方法に関する詳細なロードマップ。
アセッサー（assessor）	セキュリティ又はプライバシーのアセスメントの実施に責任を持つ個人、グループ、又は組織。
設定ステートメント（assignment statement）	組織が、管理策又は拡張管理策に対して組織が定める特定の値を設定できるようにする管理策パラメータ（例えば、通知を受け取る役割のリストやテスト頻度の値を設定するもの）。 組織が定める管理策パラメータ（organization-defined control parameters）及び選択ステートメント（selection statement）を参照。

アシュアランス（assurance） [ISO 15026, Adapted]	[セキュリティ又はプライバシーに関する] 主張が達成された、又は今後達成されるであろうという正当な信用の根拠。 *注 1：*通常、アシュアランスは一連の特定の主張に関連して得られる。そのような主張の範囲及び焦点は様々であり（例えば、セキュリティに関する主張、安全に関する主張）、これらの主張自体が相互に関連している場合もある。 *注 2：*アシュアランスは、主張を裏付けるための信頼できる証拠を生み出す技術及び方法によって得られる。
監査ログ（audit log） [CNSSI 4009]	特定の期間に実行されたシステムアクセス及び操作の記録を含む、システム活動の時系列の記録。
監査証跡（audit trail）	セキュリティ関連のトランザクションにおける特定の操作、手順、又は事象に関連する、又はそれらに至るまでの一連の活動を、開始から結果まで再構成して調査する時系列の記録。
認証（authentication） [FIPS 200]	ユーザ、プロセス、又はデバイスの ID の検証。多くの場合、システム内のリソースへのアクセスを許可するための前提条件となる。
真正性（authenticity）	本物であり、検証及び信頼できる特性。伝送、メッセージ、又はメッセージ発信者の妥当性に対する信用。 *認証（authentication）*を参照。
認可境界（authorization boundary） [OMB A-130]	認可権限のある担当者によって運用を認可される、情報システムのすべてのコンポーネント。これには、情報システムが接続されている、個別に認可されたシステムは含まれない。
認可パッケージ（authorization package） [OMB A-130]	情報システムの運用又は指定された一連の共通管理策の提供を認可するかどうかを決定するために、認可権限のある担当者が使用する必要不可欠な情報。認可パッケージには、少なくとも、エグゼクティブサマリ、システムセキュリティ計画、プライバシー計画、セキュリティ管理策アセスメント、プライバシー管理策アセスメント、行動計画及びマイルストーンが含まれる。
運用認可（authorization to operate） [OMB A-130]	合意された一連のセキュリティ及びプライバシー管理策の実施に基づき、情報システムの運用を認可し、政府機関の業務（ミッション、機能、イメージ、又は評判を含む）、政府機関の資産、個人、他の組織、及び国家に対するリスクを明示的に受容するために、連邦政府の高官によって下される管理上の正式な決定。認可は、政府機関の情報システムによって継承される共通管理策にも適用される。

使用認可 **（authorization to use）**	別の組織によって生成された既存の認可パッケージ内の情報に基づいて情報システム、サービス、又はアプリケーションの使用を認可し、システム、サービス、又はアプリケーションへの合意された一連の管理策の導入に基づいて政府機関の業務（ミッション、機能、イメージ、又は評判を含む）、政府機関の資産、個人、他の組織、及び国家に対するリスクを明示的に受容するために、認可権限のある担当者によって行われる管理上の正式な決定。 *注：*使用認可は、通常、クラウド及び共有のシステム、サービス、アプリケーションに適用され、ある組織（顧客組織と呼ぶ）が別の組織（プロバイダ組織と呼ぶ）によって生成された既存の認可パッケージ内の情報を受け入れることを選択した場合に使用される。
認可権限のある担当者 **（authorizing official）** [OMB A-130]	政府機関の業務（ミッション、機能、イメージ、又は評判を含む）、政府機関の資産、個人、他の組織、及び国家に対する受容可能なリスクレベルで、情報システムの運用、又は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、連邦政府の高官又は幹部。
認可権限のある担当者による指定代理人 **（authorizing official designated representative）**	認可プロセスに関連する必要な活動の実施及び調整において、認可権限のある担当者の代理として行動する組織の担当者（訳注：連邦政府職員）。
可用性（availability） [44 USC 3552]	タイムリーで信頼性の高い、情報へのアクセス及び情報の使用を確保すること。
ベースライン（baseline）	*管理策ベースライン（control baseline）*を参照。
ベースライン構成 **（baseline configuration）** [SP 800-128, Adapted]	システム又はシステム内の構成アイテムに関する仕様の文書化されたセット。特定の時点で正式にレビュー及び合意されたもので、変更管理手順によってのみ変更できる。
ケイパビリティ（能力） **（capability）**	技術的手段、物理的手段、及び手続き上の手段によって実施される、相互に補強し合う管理策の組み合わせ。このような管理策は、通常、共通の情報セキュリティ又はプライバシーの目的を達成するために選択される。
ケイパビリティ要件 **（capability requirement）**	組織又はシステムがステークホルダーのニーズを満たすために提供しなければならないケイパビリティ（能力）を記述する要件の一種。 *注：*情報セキュリティ及びプライバシーに関連するケイパビリティ要件は、ステークホルダーの保護ニーズとそれに対応するセキュリティ要件及びプライバシー要件から導き出される。
信頼の連鎖 **（chain of trust）** **（サプライチェーン）** **（supply chain）**	消費者と提供者の関係にある各参加者が、そのコンポーネント製品、システム、及びサービスを適切な保護を提供するような、サプライチェーンの相互作用における一定レベルの信頼。

最高情報責任者（chief information officer） [OMB A-130]	政府機関の戦略的目標及び情報リソース管理目標を達成するような方法で、政府機関のために IT が取得され、情報リソースが管理されることを確実にするために、政府機関の長官及びその他の上級管理職員に助言やその他の支援を提供する政府高官。一般市民の情報収集の負担を軽減することを含む、政府機関による情報ポリシーと情報リソースの管理責任の順守、迅速・効率的・効果的な実施を実現する責任を負う。
最高情報セキュリティ責任者（chief information security officer）	*政府機関の情報セキュリティ責任者（Senior Agency Information Security Officer）*を参照。
国家機密情報（classified information）	*国家機密安全保障情報（classified national security information）*を参照。
国家機密安全保障情報（classified national security information） [CNSSI 4009]	大統領令（E.O.）13526 又はそれに先行する命令に従って、漏えいから保護する必要があると判断された情報。文書形式の場合には機密扱いであることを示すマークが付いている。
コモディティサービス（commodity service）	商用サービスプロバイダが、大規模かつ多様な消費者集団に提供するシステムサービス。コモディティサービスを取得する又は受ける組織は、プロバイダの管理構造と運用についての可視性が限られているため、そのような組織は、サービスレベル契約を交渉できる場合があるが、通常、特定の管理策の実装をプロバイダに要求することはできない。
共通管理策（common control） [OMB A-130]	複数の情報システム又はプログラムによって継承されるセキュリティ管理策又はプライバシー管理策。
共通管理策の提供者（common control provider）	共通管理策（すなわち、組織システムによって継承される管理策）の開発、実装、アセスメント、及び監視の責任を負う組織の担当者。
コモンクライテリア（common criteria） [CNSSI 4009]	製品及びシステムのセキュリティ機能及びアシュアランス要件を規定するための包括的かつ厳密な方法を提供する管理文書。
代替管理策（compensating controls）	NIST Special Publication 800-53 に記載されているベースラインの管理策の代わりに実装されるセキュリティ管理策及びプライバシー管理策で、システム又は組織に対して同等又は同様の保護を提供する。
コンポーネント（component）	*システムコンポーネント（system component）*を参照。
機密性（confidentiality） [44 USC 3552]	個人のプライバシー及び機密情報を保護するための手段を含む、情報へのアクセス及び開示に関する認可された制限を維持すること。
構成変更管理（configuration control） [CNSSI 4009]	システムの実装前、実装中、及び実装後の不適切な変更から情報システムを保護するために、ハードウェア、ファームウェア、ソフトウェア、及び文書への変更を管理するプロセス。

構成アイテム（**configuration item**）[SP 800-128]	構成管理用に指定され、構成管理プロセスにおいて単一のエンティティとして扱われるシステムコンポーネントの集合体。
構成管理（**configuration management**）[SP 800-128]	システム開発ライフサイクル全体を通じて、情報技術製品及びシステムの構成を初期化、変更、及び監視するプロセスを管理することによって、情報技術製品及びシステムの完全性を確立し維持することに焦点を当てた活動の集まり。
構成設定（**configuration settings**）[SP 800-128]	システムのセキュリティ態勢及び／又は機能に影響を及ぼす、ハードウェア、ソフトウェア、又はファームウェアで変更できるパラメータのセット。
継続的監視（**continuous monitoring**）	組織のリスク決定を支援するために、継続的な認識を維持すること。
継続的監視プログラム（**continuous monitoring program**）	実装されたセキュリティ管理策を通じて容易に入手できる情報を利用して、事前に設定された指標に従って情報を収集するために確立されたプログラム。 *注:*プライバシー及びセキュリティの継続的監視の戦略及びプログラムは、同じもの、又は異なる戦略及びプログラムにすることもできる。
管理策（**control**）	*セキュリティ管理策（security control）及びプライバシー管理策（privacy control）*を参照。
管理策アセスメント（**control assessment**）	管理策が正しく実装されているか、意図した通りに運用されているか、情報システム又は組織のセキュリティ要件又はプライバシー要件を満たすことに関して期待される成果をどの程度得られているかを判断するための、情報システム又は組織の管理策のテスト又は評価。
管理策アセッサー（**control assessor**）	管理策アセスメントの実施に責任を持つ個人、グループ、又は組織。アセッサー（assessor）を参照。
管理策ベースライン（**control baseline**）	法律、規制、又はポリシーの要求事項を満たすとともに、リスク管理を目的とした保護ニーズに対処するために、情報又は情報システムに適用される一連の管理策。
管理策の指定（**control designation**）	管理策を 3 種類の管理策（共通管理策、ハイブリッド管理策、又はシステム固有管理策）のいずれかに割り当てるプロセス。
管理策の有効性（**control effectiveness**）	特定の管理策が情報セキュリティ又はプライバシーリスクの低減に貢献しているかどうかを示す尺度。
拡張管理策（**control enhancement**）	管理策に追加の関連する機能性を組み込むため、管理策の強度を高めるため、又は管理策へのアシュアランスの追加を行なうための、管理策の拡張。
管理策の継承（**control inheritance**）	システム又はアプリケーションが、それらのシステム又はアプリケーションに責任を負うエンティティ以外のエンティティ（システム又はアプリケーションが設置されている組織の内部又は外部のエンティティ）によって開発、実装、アセスメント、認可、及び監視される管理策（又は管理策の一部）の保護を受けている状況。*共通管理策（common control）*を参照。

管理策パラメータ（control parameter）	*組織が定める管理策パラメータ（organization-defined control parameter）*を参照。
管理対象非機密情報（controlled unclassified information） [32 CFR 2002.4]	政府が作成又は保有する情報、又はあるエンティティが政府のために、あるいは政府の代わりに作成又は保有する情報のうち、法律、規制、又は政府全体のポリシーにより、政府機関が保護管理策又は配布管理策を使用して取り扱うことを要求又は許可している情報。ただし、CUI には、行政府以外の機関のエンティティが自身のシステム内で保有及び管理している国家機密情報や情報のうち、行政府の機関又はその代理で活動するエンティティから得たものではない情報、又ははそれらのために作成又は保有されていたものではない情報は含まれない。
対策（countermeasures） [FIPS 200]	システムの脆弱性を低減するための活動、デバイス、手順、技術、又はその他の対策。*セキュリティ管理策*（security control）及び*予防手段*（safeguard）と同義。
サイバーセキュリティ（cybersecurity） [OMB A-130]	コンピュータ、電子通信システム、電子通信サービス、有線通信、及び電子通信（これらに含まれる情報を含む）の可用性、完全性、認証、機密性及び否認防止を実現するために、これらの損害防止、保護、及び復旧を行うこと。
サイバーセキュリティフレームワーク（cybersecurity framework） [NIST CSF]	サイバーセキュリティリスクを低減するためのリスクベースのアプローチであり、フレームワークコア、フレームワークプロファイル、及びフレームワークインプリメンテーションティアの 3つの部分で構成される。
サイバーセキュリティフレームワークのカテゴリ（cybersecurity framework category） [NIST CSF]	機能をプログラム上のニーズ及び特定の活動と密接に結びついたサイバーセキュリティ成果グループに細分化したもの。
サイバーセキュリティフレームワークコア（cybersecurity framework core） [NIST CSF]	重要インフラ分野に共通し、特定の成果を中心に編成された、一連のサイバーセキュリティ活動及び参考資料。フレームワークコアは、機能、カテゴリ、サブカテゴリ、及び参考資料という 4種類の要素で構成される。
サイバーセキュリティフレームワーク機能（cybersecurity framework function） [NIST CSF]	フレームワークの主要コンポーネントの 1つ。機能は、基本的なサイバーセキュリティ活動をカテゴリ及びサブカテゴリに整理するための最高レベルの構造を提供する。「識別（Identify）」、「防御（Protect）」、「検知（Detect）」、「対応（Respond）」、及び「復旧（Recover）」の 5つの機能がある。
サイバーセキュリティフレームワークプロファイル（cybersecurity framework profile） [NIST CSF]	特定のシステム又は組織がフレームワークのカテゴリ及びサブカテゴリから選択した成果の表現。

サイバーセキュリティフレームワークのサブカテゴリ（cybersecurity framework subcategory） [NIST CSF]	カテゴリを、技術的及び／又は管理上の活動の特定の成果に細分化したもの。
派生要件（derived requirements） [SP 800-160 v1]	上位レベルの要件から暗示された、又は変換された要件。 *注 1：*暗示された要件は、どの要件ベースラインにも含まれていないためアセスメントできない。エンジニアリングプロセス全体を通して要件を分解することで、暗示された要件が明示的になる。これにより、それらの要件を適切なベースラインに記述及び取り込めるようになり、関連するアセスメント基準を記述できるようになる。 *注 2：*派生要件は、少なくとも 1つの上位レベルの要件に遡らなければならない。
検知（CSF 機能）（detect（CSF function）） [NIST CSF]	サイバーセキュリティ事象の発生を識別するための適切な活動を策定及び実装すること。
開発者（developer）	システム、システムコンポーネント、又はシステムサービスの開発者又は製造者、システムインテグレータ、ベンダ、及び製品の再販業者を含む一般用語。システム、コンポーネント、又はサービスの開発は、組織内部で、又は外部エンティティを介して行われる可能性がある。
事業体（enterprise） [CNSSI 4009]	定義されたミッション／目標及び定義された境界を持ち、そのミッションを遂行するためにシステムを使用し、自らのリスク及びパフォーマンスを管理する責任を持つ組織。事業体は、取得、プログラムマネジメント、人事、財務管理、セキュリティ、システム、情報及びミッションの管理といったビジネスの側面のすべて又は一部で構成される場合がある。*組織*（organization）を参照。
エンタープライズアーキテクチャ（enterprise architecture） [44 USC 3601]	戦略的情報資産基盤であり、ミッション、ミッション遂行に必要な情報、ミッション遂行に必要な技術、及び変化するミッションニーズに対応した新技術実装の移行プロセスを規定したもの。ベースラインアーキテクチャ、ターゲットアーキテクチャ、及び**シーケンスプラン**を含む。
運用環境（environment of operation） [OMB A-130]	情報システムが情報を処理、保存、及び伝送する物理的環境。
事象（event） [SP 800-61, Adapted]	ネットワーク又は情報システムにおける観察可能なあらゆる出来事。
行政機関（executive agency） [OMB A-130]	合衆国法典第 5 編第 101 条（5 U.S.C. Sec. 101）で規定された行政部門、合衆国法典第 5 編第 102 条（5 U.S.C. Sec. 102）で規定された軍事部門、合衆国法典第 5 編第 104 条 1 項（5 U.S.C. Sec. 04（1））で規定された独立組織、合衆国法典第 31 編第 91 章（31 U.S.C. Chapter 91）の規定の対象である政府完全所有法人。
外部システム（又はコンポーネント）（external system（or component））	組織が設定した認可境界の外側にあるシステム又はシステム要素であり、通常、組織はこれらのシステム又はシステム要素に対して、必要な管理策の適用や管理策の有効性のアセスメントを直接制御できない。

外部システムサービス（external system service）	組織システムの認可境界の外側で実施されるシステムサービス（すなわち、組織システムによって使用されるが、そのシステムの一部ではないサービス）であり、通常、組織はこれらのサービスに対して、必要な管理策の適用や管理策の有効性のアセスメントを直接制御できない。
外部システムサービスプロバイダ（external system service provider）	様々な消費者と製造者の関係を通じて、組織に外部システムサービスを提供するプロバイダ。これには、合弁事業、業務提携、外部委託協定（すなわち、契約、省庁間協定、事業協定などによるもの）、ライセンス契約、及び／又はサプライチェーンの交換などが含まれるが、これらに限定されない。
外部ネットワーク（external network）	当事者である組織によって管理されていないネットワーク。
連邦政府機関（federal agency）	*行政機関*（executive agency）を参照。
連邦政府エンタープライズアーキテクチャ（federal enterprise architecture） [OMB FEA]	米国行政管理予算局（Office of Management and Budget）によって策定された、政府全体を改善するためのビジネスベースのフレームワーク。連邦政府を市民中心、成果重視、及び市場ベースに転換するための取り組みを促進することを目的としている。
連邦政府情報システム（federal information system） [40 USC 11331]	行政機関、行政機関の請負業者、又は行政機関の代わりとなる他の組織によって使用又は運用される情報システム。
ファームウェア（firmware） [CNSSI 4009]	ハードウェアに保存されたコンピュータプログラム及びデータ。通常、読み取り専用メモリ（ROM）又はプログラム可能な読み取り専用メモリ（PROM）に保存され、プログラムの実行中にプログラム及びデータを動的に書き込んだり変更したりすることができない。*ハードウェア*（hardware）及び*ソフトウェア*（software）を参照。
ハードウェア（hardware） [CNSSI 4009]	システムの有形な物理コンポーネント。*ソフトウェア*（software）及び*ファームウェア*（firmware）を参照。
高インパクトシステム（high-impact system） [FIPS 200]	少なくとも 1つのセキュリティ目的（すなわち、機密性、完全性、又は可用性）に対して FIPS Publication 199 の潜在的インパクト値「高」が設定されているシステム。
ハイブリッド管理策（hybrid control） [OMB A-130]	一部は共通管理策として、また一部はシステム固有管理策として情報システムのために実装されるセキュリティ管理策又はプライバシー管理策。*共通管理策*（common control）及びシステム*固有管理策*（system-specific control）を参照。
識別（CSF 機能）（identify（CSF function）） [NIST CSF]	サイバーセキュリティ事象の発生を識別するための適切な活動を策定及び実装すること。

インパクト（impact）	セキュリティに関しては、情報又はシステムの機密性、完全性、又は可用性の喪失が、組織の業務、組織の資産、個人、他の組織、又は国家（米国の国家安全保障上の利益を含む）に及ぼす影響。プライバシーに関しては、情報システムが個人情報（PII）を処理する際に対象の個人が経験する可能性のある有害事象。
インパクトレベル（impact level）	*インパクト値*（impact value）を参照。
インパクト値（impact value） [FIPS 199]	情報の機密性、完全性、又は可用性の侵害から生じる可能性がある、アセスメントした最悪のケースの潜在的インパクトを「低」、「中」、「高」の値で表したもの。
インシデント（incident） [44 USC 3552]	法的権限なしに、情報又は情報システムの機密性、完全性、又は可用性を実際に危険にさらす又は今にも危険にさらそうとする出来事、あるいは、法律、セキュリティポリシー、セキュリティ手順、又は許容される利用ポリシーの違反又は違反の差し迫った脅威を構成する出来事。
独立機関による検証（正当性確認と妥当性確認）（independent verification and validation） [CNSSI 4009]	要件が正しく定義されていることを確認（すなわち検証）し、システムが要求される機能要件とセキュリティ要件を正しく実装していることを確認（すなわち妥当性確認）するために、客観的な第三者によって実施される（ソフトウェア及び／又はハードウェアの）包括的なレビュー、分析、及びテスト。
産業用制御システム（industrial control system） [SP 800-82]	監視制御及びデータ取得（SCADA）システム、分散制御システム（DCS）、及び産業分野や重要インフラに存在するプログラマブルロジックコントローラ（PLC）などの他の制御システム構成など、いくつかの種類の制御システムを包含する一般用語。産業用制御システムは、産業上の目的（製造、物質又はエネルギーの輸送など）を達成するために一緒に作用する（電気、機械、油圧、空気圧などの）制御コンポーネントの組み合わせで構成される。
情報（information） **[OMB A-130]**	テキスト、数値、グラフィック、地図、叙述、電子、又は視聴覚形式を含む、あらゆる媒体又は形態での、事実、データ、意見などの知識の伝達又は表現。
情報ライフサイクル（information life cycle） [OMB A-130]	情報が通過する全段階。通常、作成又は収集、処理、配布、利用、保存、及び廃棄として特徴付けられ、破棄及び削除も含まれる。
情報所有者（information owner）	特定の情報に対する法的又は運用上の権限を持ち、その情報の生成、収集、処理、配布及び廃棄に関する管理策を確立する責任を有する職員。
情報リソース（information resources） [44 USC 3502]	人員、装置、資金、情報技術などの情報及び関連リソース。
情報セキュリティ（information security） [44 USC 3552]	機密性、完全性、及び可用性を提供するために、情報及びシステムを不正アクセス、不正利用、漏えい、破壊、改ざん、破棄から保護すること。

情報セキュリティアーキテクチャ（information security architecture） [OMB A-130]	事業体のセキュリティプロセス、セキュリティシステム、職員及び組織のサブユニットの構造と動作を記述し、事業体のミッションと戦略的計画との整合性を示す、エンタープライズアーキテクチャに組み込まれた不可欠な部分。セキュリティアーキテクチャ（security architecture）を参照。
情報セキュリティプログラム計画（information security program plan） [OMB A-130]	組織全体の情報セキュリティプログラムのセキュリティ要件の概要を提供し、それらの要件を満たすために導入又は計画されているプログラムマネジメント管理策及び共通管理策について説明する正式な文書。
情報セキュリティリスク（information security risk） [SP 800-30]	情報及び／又はシステムへの不正アクセス、不正利用、漏えい、破壊、改ざん、破棄の可能性によってもたらされる、組織の業務（ミッション、機能、イメージ、又は評判を含む）、組織の資産、個人、他の組織、及び国家に対するリスク。
情報管理者（information steward）	特定の情報に対する法的又は運用上の権限を持ち、その情報の生成、収集、処理、配布及び廃棄に関する管理策を確立する責任を有する政府機関の職員。
情報システム（information system） [44 USC 3502]	情報の収集、処理、維持、使用、共有、配布、又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。
情報システムの境界（information system boundary）	*認可境界*（authorization boundary）を参照。
情報システムセキュリティ責任者（information system security officer） [CNSSI 4009]	情報システム又はプログラムに関する運用上の適切なセキュリティ態勢を維持することに責任を持つ個人。
情報システムセキュリティ計画（information system security plan） [OMB A-130]	情報システムのセキュリティ要件の概要を示し、これらの要件を満たすために既に実施されている、又は計画されているセキュリティ管理策を記述する正式な文書。
情報技術（information technology） [OMB A-130]	政府機関によるデータ又は情報の自動取得、保存、分析、評価、操作、管理、移動、制御、表示、切り替え、交換、伝送、又は受信で使用される、あらゆるサービス、機器、又は相互接続されたシステム又はサブシステム。本定義において、そのようなサービス又は機器は、政府機関が直接使用する。或いは、そのようなサービス又は機器を（例えば、サービス実行や製品設置において一定程度）使用する必要がある場合、政府機関の請負業者が契約に基づいて使用する。 情報技術には、コンピュータ、付属機器（セキュリティと監視に必要な画像処理周辺装置、入力装置、出力装置、及び記憶装置を含む）、コンピュータの中央処理装置（CPU）によって制御されるように設計された周辺機器、ソフトウェア、ファームウェア及び類似の手順、サービス（機器やサービスのライフサイクルの任意の時点をサポートするクラウドコンピューティング及びヘルプデスクサービス、又はその他の専門サービスを含む）、及び関連リソースが含まれる。情報技術には、その使用を必要としない

	契約に付随して、請負業者が取得した機器は含まれない。
情報技術製品 **（information technology product）**	*システムコンポーネント*（system component）を参照。
情報の種類（information type） [FIPS 199]	組織によって、又は場合によっては特定の法律、大統領令、指令、ポリシー、又は規制によって定義された特定の分類の情報（プライバシー、医療、機密、財務、調査、請負業者機密、セキュリティ管理など）。
インタフェース（interface） **[CNSSI 4009]**	相互作用が発生する独立したシステム又はモジュール間の共通境界。
完全性（integrity） **[44 USC 3552]**	改ざんや破壊から情報を保護すること。情報の否認防止及び真正性の確保を含む。
共同認可 **（joint authorization）**	認可権限のある担当者が複数関与する認可。
低インパクトシステム **（low-impact system）** [FIPS 200]	3つのセキュリティ目的（すなわち、機密性、完全性、及び可用性）すべてに対して FIPS Publication 199 の潜在的インパクト値「低」が設定されているシステム。
媒体（media） [FIPS 200]	システム内で情報が記録、保存、又は印刷される磁気テープ、光ディスク、磁気ディスク、大規模集積回路メモリチップ、及び印刷物（ただし、ディスプレイ媒体は除く）を含む物理デバイス又は書き込み面。
中インパクトシステム **（moderate-impact system）** [FIPS 200]	少なくとも 1つのセキュリティ目的（すなわち、機密性、完全性、又は可用性）に対して FIPS Publication 199 の潜在的インパクト値「中」が設定され、どのセキュリティ目的にも潜在的インパクト値「高」が設定されていないシステム。
国家安全保障システム **（national security system）** [44 USC 3552]	政府機関、又は政府機関の請負業者、又は政府機関に代わって他の組織が使用又は運用するあらゆるシステム（電気通信システムを含む）で－（i）システムの機能、運用、又は使用が、諜報活動を伴う、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、兵器又は兵器システムの不可欠な部分である機器を伴う、又は、軍事又は諜報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、及び人事管理アプリケーションなどの日常的な管理及び業務アプリケーションに使用されるシステムを除く）、又は、（ii）国防又は外交政策上の利益のために機密扱いとされ続けるように、大統領令又は議会制定法によって確立された基準の下で明確に認可されている情報のために確立された手順によって常時保護されているシステム。
ネットワーク（network）	相互接続されたコンポーネントの集合で実装されたシステム。このようなコンポーネントには、ルータ、ハブ、ケーブル、通信制御装置、鍵配布センター、及び技術制御装置が含まれる。
ネットワークアクセス **（network access）**	ネットワーク（ローカルエリアネットワーク、ワイドエリアネットワーク、及びインターネットなど）を介して通信するユーザ（又はユ

	ーザの代理として動作するプロセス）によるシステムへのアクセス。
制御・運用技術（operational technology）	物理環境と相互作用する（又は物理環境と相互作用するデバイスを管理する）プログラム可能なシステム又はデバイス。これらのシステム／デバイスは、デバイス、プロセス、事象の監視及び／又は制御を通じて、直接的な変化を検知したり引き起こしたりする。例としては、産業用制御システム、ビル管理システム、防火システム、及び物理的アクセス制御メカニズムがある。
制御・運用技術（operations technology）	*制御・運用技術*（operational technology）を参照。
組織（organization） [FIPS 200, Adapted]	組織構造（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、又は必要に応じて、それらの運用要素など）内の任意の規模、複雑さ、又は位置付けのエンティティ。
組織的にテーラリングされた管理策ベースライン（organizationally-tailored control baseline）	オーバーレイ及び／又はシステム固有の管理策のテーラリングを使用して、定義された概念的な（タイプの）情報システムに合わせて調整された管理策ベースラインであり、1 つ以上の組織内の複数のシステムに対する管理策を選択する際に使用することを目的としている。
組織が定める管理策パラメータ（organization-defined control parameter）	組織が定める値を割り当てるか、管理策又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実体化することができる管理策又は拡張管理策の可変部分。
オーバーレイ（overlay） [OMB A-130]	セキュリティ又はプライバシー管理策、拡張管理策、補足ガイダンス、及びテーラリングプロセス中に採用されるその他の補足情報の仕様で、セキュリティ管理策ベースラインを補完（及び、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。
個人情報（personally identifiable information） [OMB A-130]	単独で、又は特定の個人にリンクされている、又はリンク可能な他の情報と組み合わされた時に、個人の身元を識別又は追跡するために使用できる情報。
実施計画及びマイルストーン（plan of action and milestones）	達成する必要があるタスクを識別する文書。計画の要素を達成するために必要なリソース、タスクを達成するためのすべてのマイルストーン、及びそのマイルストーンの完了予定日の詳細を示している。
潜在的インパクト（potential impact） [FIPS 199]	機密性、完全性、又は可用性の喪失は、組織の業務、組織の資産、又は個人に対して、限定的な悪影響（FIPS Publication 199「低」）、深刻な悪影響（FIPS Publication 199「中」）、あるいは、重大又は壊滅的な悪影響（FIPS Publication 199「高」）を及ぼすと予想される。

プライバシーアーキテクト（privacy architect）	個人のプライバシーを保護するために必要なシステムプライバシー要件が、リファレンスモデル、セグメントアーキテクチャ並びにソリューションアーキテクチャ、及び個人情報を処理する情報システムを含むエンタープライズアーキテクチャのあらゆる側面において適切に対処されていることを保証する責任を有する個人、グループ、又は組織。
プライバシーアーキテクチャ(privacy architecture)	事業体のプライバシー保護プロセス、技術的手段、人員及び組織のサブユニットの構造と動作を記述し、事業体のミッションと戦略的計画との整合性を示す、エンタープライズアーキテクチャに組み込まれた不可欠な部分。
プライバシー管理策（privacy control） [OMB A-130]	適用されるプライバシー要件への準拠を確保し、プライバシーリスクを管理するために政府機関内で採用される行政上、技術的、及び物理的な予防手段。 注：管理策は、複数の目的を達成するために選択することができる。セキュリティ及びプライバシーの両方の目的を達成するために選択された管理策では、組織の情報セキュリティプログラム及びプライバシープログラムとの間で、ある程度の連携が必要になる。
プライバシー管理策アセスメント（privacy control assessment） [OMB A-130]	管理策が正しく実装され、意図したとおりに動作し、適用されるプライバシー要件に確実に準拠し、プライバシーリスクを管理するのに十分かどうかを判断するための、プライバシー管理策のアセスメント。プライバシー管理策アセスメントは、アセスメントであると同時に、アセスメントのプロセス及び成果を詳述した正式な文書でもある。
プライバシー管理策ベースライン（privacy control baseline）	個人のプライバシー保護ニーズに対処するために、関心のあるグループ、組織、又はコミュニティによって特別に集められた、又はまとめられた管理策の集合。
プライバシー影響アセスメント（privacy impact assessment） [OMB A-130]	情報が、以下の目的のためにどのように取り扱われるかについての分析。プライバシーに関して適用される法的、規制、及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、及び廃棄することのリスク及び影響を判定する、並びに、プライバシーに対する潜在的な懸念を軽減するために、情報の取り扱いに対する保護及び代替プロセスを調査及び評価する。プライバシー影響アセスメントは、分析であると同時に、分析のプロセスと成果を詳述した正式な文書でもある。
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実装又は計画されている情報システム又は運用環境に対して選択されたプライバシー管理策を詳述し、その管理策がどのように実装されたか方法を詳述し、その管理策のアセスメントに使用する方法論及び測定基準を記述する正式な文書。
プライバシー態勢（privacy posture）	プライバシー態勢とは、情報アシュアランスリソース（人員、ハードウェア、ソフトウェア、ポリシー、手順など）、及び適用されるプライバシー要件に準拠し、プライバシーリスクを管理し、状況の

	変化に対応するためのケイパビリティに基づいて、組織内の情報システム及び情報リソース（人員、機器、資金、情報技術など）の状況を表すもの。
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及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、及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実施又は計画されているプログラムマネジメント管理策及び共通管理策を含む、政府機関のプライバシープログラムの概要を記載した正式な文書。
プライバシー要件（privacy requirement）	プライバシーに関して適用される法律、大統領令、指令、ポリシー、標準、規制、手順、及び／又はミッション／ビジネスのニーズから派生した、情報システム又は組織に適用される要件。 *注:* プライバシー要件（privacy requirement ）という用語は、ハイレベルの政策活動から、システム開発及びエンジニアリング分野におけるローレベルの実装活動まで、様々な文脈で使用できる。
プライバシー情報（privacy information）	情報システム又は組織のプライバシー態勢を記述する情報。
防御（CSF 機能）（protect（CSF function）） [NIST CSF]	重要インフラサービスを確実に提供するための適切な予防手段を策定及び実装すること。
来歴（provenance）	システム又はシステムコンポーネント及び関連データの起源、開発、所有権、場所、及び変更の年表。また、システム、コンポーネント、又は関連データとやりとりする、又はそれらを変更するために使用される職員及びプロセスも含まれる場合がある。
互恵契約（reciprocity）	システムリソースを再利用するために互いのセキュリティアセスメントを受け入れること、及び／又は情報を共有するために互いのアセスメントされたセキュリティ態勢を受け入れることについての参加組織間の合意。
記録（records） [44 USC 3301]	米国政府の組織、機能、ポリシー、決定、手順、運用、又はその他の活動の証拠として、又はそれらに含まれるデータの情報価値を理由として、連邦法に基づいて、又は公共事業の取引に関連して連邦政府機関によって作成又は受領され、その政府機関又はその合法的な後継者によって保存される、又は保存するのにふさわしい、形式又は特性を問わないすべての記録情報。
復旧（CSF 機能）（recover（CSF function）） [NIST CSF]	レジリエンスのための計画を維持し、サイバーセキュリティ事象によって損なわれたケイパビリティ又はサービスを回復するための適切な活動を策定及び実装すること。
レジリエンス（resilience） [CNSSI 4009]	変化する状況に備え、適応し、混乱に耐えて迅速に回復する能力。レジリエンスには、意図的な攻撃、事故、又は自然発生の脅威やインシデントに耐え、それらから回復する能力が含まれる。
対応（CSF 機能）（respond（CSF function）） [NIST CSF]	検知されたサイバーセキュリティ事象に対処するための適切な活動を策定及び実施すること。

リスク（risk） [OMB A-130]	潜在的な状況又は事象によってエンティティが脅かされる度合いの指標であり、通常、以下に応じて変化する。(i) 状況又は事象が発生した場合に生じる有害なインパクト又は損害の大きさ、及び(ii) 発生の可能性。
リスクアセスメント（risk assessment） [SP 800-30]	システムの運用により生じる、組織の業務（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、及び国家へのリスクを識別するプロセス。
リスク管理者（機能）（risk executive（function）） [SP 800-39]	リスクマネジメント担当責任者が主導する組織内の個人又はグループで、個々のシステムに対するセキュリティリスクの考慮事項（それらのシステムに関する認可判断を含む）を、組織のミッション及びビジネスファンクションを遂行する上での組織の全体的な戦略的目標及び目的に照らして組織全体の観点から捉えられるよう支援したり、個々のシステムからのリスクの管理が組織全体にわたって一貫し、組織のリスク許容度を反映し、ミッション／ビジネスの成功に影響を及ぼす他の組織的リスクと共に考慮されるよう支援したりする。
リスクマネジメント（risk management） [OMB A-130]	政府機関の業務（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、その他の組織、及び国家に対するリスクを管理するためのプログラム及びサポートプロセス。リスク関連活動のコンテキストの確立、リスクのアセスメント、判定されたリスクへの対応、及びリスクの長期監視が含まれる。
リスク軽減（risk mitigation） [CNSSI 4009]	リスクマネジメントプロセスから推奨された適切なリスク低減管理策／対策の優先順位付け、評価、及び実施。
リスク対応（risk response） [OMB A-130]	政府機関の業務、政府機関の資産、個人、その他の組織、又は国家に対するリスクの受容、回避、軽減、共有、又は移転。
サニタイズ（sanitization） [SP 800-88]	所定の努力レベルでは媒体上の対象データへのアクセスを実行不可能にするプロセス。消去、除去、及び破壊は、媒体をサニタイズするために実行できる措置である。
スコーピングの考慮事項（scoping considerations）	管理策ベースラインにおける管理策の適用可能性と実装に関する具体的な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／規制、技術、物理インフラ、システム要素の割り振り、運用／環境、パブリックアクセス、拡張性、共通管理策、及びセキュリティ目的が含まれる。
セキュリティ（security） [CNSSI 4009]	システムの使用に対する脅威によってもたらされるリスクにもかかわらず、組織がそのミッション又は重要な機能を遂行できるようにする保護対策を確立及び維持することによって生じる状態。保護対策は、抑止、回避、防止、検知、復旧、及び修正の組み合わせを含むことができ、組織のリスクマネジメントアプローチの一部を形成することが望ましい。
セキュリティアーキテクト（security architect）	組織の中核的なミッション及びビジネスプロセスを保護するために必要な情報セキュリティ要件が、リファレンスモデル、セグメントアーキテクチャ及びソリューションアーキテクチャ並びにそれらのミッション及びビジネスプロセスをサポートする情報システムを含むエンタープライズアーキテクチャのあらゆる側面におい

	て、適切に対処されることに責任を有する個人、グループ、又は組織。
セキュリティアーキテクチャ（security architecture） [SP 800-39]	事業体のセキュリティプロセス、情報セキュリティシステム、人員及び組織のサブユニットの構造と動作を記述し、事業体のミッションと戦略的計画との整合性を示す、エンタープライズアーキテクチャに組み込まれた不可欠な部分。*情報セキュリティアーキテクチャ*（information security architecture）を参照。
[SP 800-160 v1]	データ及び情報をどのように保護しなければならないかという観点に基づいて、システムのセキュリティドメインをどのように分割するか、及びセキュリティドメイン内及びセキュリティドメイン間でどのようにセキュリティポリシーを適用するかについての情報を伝える、システムアーキテクチャの一連の物理的及び論理的なセキュリティ関連表現（すなわち、ビュー）。 *注:* セキュリティアーキテクチャは、セキュリティドメイン、セキュリティドメイン内のセキュリティ関連要素の配置、セキュリティ関連要素間の相互接続と信頼関係、及びセキュリティ関連要素間の動作と相互作用を反映したものである。セキュリティアーキテクチャは、システムアーキテクチャと同様に、様々な抽象化レベル及び様々な範囲で表現されることがある。
セキュリティ分類化（security categorization）	情報又はシステムのセキュリティ分類を決定するプロセス。セキュリティ分類化の方法は、国家安全保障システムについてはCNSSI 第 1253 号に、国家安全保障システム以外についてはFIPS Publication 199 に記載されている。 *セキュリティ分類*（security category）を参照。
セキュリティ分類（security category） [OMB A-130]	情報又は情報システムの機密性、完全性、又は可用性の喪失が政府機関の業務、政府機関の資産、個人、その他の組織、及び国家に及ぼす潜在的インパクトのアセスメントに基づく、情報又は情報システムの特性化。
セキュリティ管理策（security control） [OMB A-130]	情報システム及びその情報の機密性、完全性、及び可用性を保護するために、情報システム又は組織に対して規定された予防手段又は対策。
セキュリティ管理策アセスメント（security control assessment） [OMB A-130]	情報システム又は組織のセキュリティ要件を満たすことに関して、管理策が正しく実装されている程度、意図した通りに運用されている程度、及び期待される成果を生み出している程度を判断するための、セキュリティ管理策のテスト又は評価。
セキュリティ管理策ベースライン（security control baseline） [OMB A-130]	インパクトが「低」、「中」、又は「高」の情報システムに対して規定された一連の最低限のセキュリティ管理策。*管理策ベースライン*（control baseline）も参照。
セキュリティ目的（security objective） [FIPS 199]	機密性、完全性、又は可用性。
セキュリティ計画（security plan）	*情報システムセキュリティ計画*（information system security plan）を参照。

セキュリティ態勢（**security posture**）[CNSSI 4009]	情報アシュアランスリソース（人員、ハードウェア、ソフトウェア、ポリシーなど）、及び事業体の防御を管理したり状況の変化に対応したりするためのケイパビリティに基づく、事業体のネットワーク、情報、及びシステムのセキュリティ状況。*セキュリティ状況*（security status）と同義。
セキュリティ要件（**security requirement**）[FIPS 200, Adapted]	処理、保存、又は伝送される情報の機密性、完全性、及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、ポリシー、標準、指示、規制、手順、及び／又はミッション／ビジネスのニーズから派生した、情報システム又は組織に課せられる要件。 *注:*セキュリティ要件は、ハイレベルの政策活動から、システム開発及びエンジニアリング分野におけるローレベルの実装活動まで、様々な文脈で使用できる。
セキュリティ情報（**security information**）	システムのセキュリティポリシーの適用に失敗したり、コード及びデータの分離の維持に失敗したりするような方法で、セキュリティ機能の動作又はセキュリティサービスの提供に影響を及ぼす可能性のあるシステム内の情報。
選択ステートメント（**selection statement**）	管理策又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、組織が値を選択できるようにする管理策パラメータ（例えば、活動を制限するか、禁止するかのいずれかを選択する）。 *設定ステートメント*（assignment statement）及び*組織が定める管理策パラメータ*（organization-defined control parameter）を参照。
政府機関の情報セキュリティ責任者（**senior agency information security officer**）[44 USC 3544]	FISMA の下で最高情報責任者の責任を遂行し、政府機関の認可権限のある担当者、情報システム所有者、及び情報システムセキュリティ責任者に対する最高情報責任者の主たる連絡役としての役割を果たす職員。
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、及びポリシーの順守、政府機関におけるプライバシーリスクの管理、法律、規則、及びその他の政策に関する提案の策定と評価における政策決定における中心的役割を含む、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政府高官。
リスクマネジメント担当責任者（**senior accountable official for risk management**）[OMB M-17-25]	各政府機関の長が指名する政府高官。組織のすべての領域に対するビジョンを持ち、情報セキュリティマネジメントプロセスと戦略プロセス、運用プロセス、及び予算計画プロセスとの連携に責任を持つ。
ソフトウェア（**software**）[CNSSI 4009]	実行中に動的に書き込まれたり変更されたりする可能性のあるコンピュータプログラム及び関連データ。
仕様書（**specification**）[IEEE 610.12]	システム又はコンポーネントの要件、設計、動作、又はその他の特性を完全、正確、かつ検証（妥当性確認）可能な方法で規定した文書であり、多くの場合、これらの規定が満たされているかどうかを判断するための手順も示されている。*仕様要件*

（specification requirement）を参照。

仕様要件（specification requirement）	管理策の全部又は一部を実装し、アセスメントされる可能性のある（すなわち、検証、妥当性確認、テスト、及び評価のプロセスの一環として）特定のケイパビリティの仕様を提供する、要件の一種。
作業ステートメント要件（statement of work requirement）	運用上又はシステム開発中に実行される処置を表す要件の一種。
サブシステム（subsystem）	情報システムの主要な下位区分又は要素であり、情報、情報技術、及び人員で構成され、1 つ以上の特定の機能を果たす。
サプライチェーン（supply chain） [OMB A-130]	製品及びサービスの調達から始まり、製品及びサービスの設計、開発、製造、加工、出荷、及び取得者への配送に至るまで、複数の階層の開発者間で関連付けられた一連のリソース及びプロセス。
サプライチェーンリスク（supply chain risk） [OMB A-130]	情報又は情報システムの機密性、完全性、又は可用性の喪失から生じ、組織の業務（ミッション、機能、イメージ、又は評判を含む）、組織の資産、個人、他の組織、及び国家に対する潜在的な悪影響を反映するリスク。
サプライチェーンのリスクマネジメント（supply chain risk management） [OMB A-130]	情報通信技術製品及びサービスのサプライチェーンにおける、グローバルかつ分散型の性質に関連するリスクを識別、アセスメント、及び軽減するプロセス。
システム（system） [CNSSI 4009]	一連の特定の機能を実現するために、相互作用又は相互依存によって結合及び調整されたリソース及び手順の組織化された集合。*情報システム*（information system）参照。 *注:* システムには、産業用／プロセス制御システム、電話交換及び構内交換機（PBX）システム、環境制御システムなどの特殊なシステムも含まれる。
[ISO 15288]	1 つ以上の明示された目的を達成するために編成された、相互作用する要素の組み合わせ。 *注 1:* システムには多くの種類がある。例えば、汎用及び特殊用途の情報システム、指令・制御・通信システム、暗号モジュール、中央処理装置（CPU）及びグラフィックスプロセッサボード、産業用／プロセス制御システム、飛行制御システム、武器、標的、及び射撃管制システム、医療機器及び治療システム、金融・銀行・商品取引システム、ソーシャルネットワーキングシステムなどがある。 *注 2:* システムの定義における相互作用要素には、ハードウェア、ソフトウェア、データ、人間、プロセス、施設、材料、及び自然発生の物理的エンティティが含まれる。 *注 3:* システムの定義には、システム・オブ・システムズが含まれる。
システム境界（system boundary）	*認可境界*（authorization boundary）を参照。

システムコンポーネント（system component） [SP 800-128]	システムの構成要素を表す個別の識別可能な情報技術資産。ハードウェア、ソフトウェア、及びファームウェアを含むことがある。
システム要素（system element） [ISO 15288]	システムを構成する一連の要素のメンバー。 *注 1:* システム要素となり得るものには、個別のコンポーネント、製品、サービス、サブシステム、システム、インフラ、又は事業体がある。 *注 2:* システムの各要素は、規定された要件を満たすように実装される。 *注 3:* この用語の再帰的な性質により、システム（system）という用語は、個別のコンポーネントを指す場合にも、大規模かつ複雑で地理的に分散したシステム・オブ・システムズを指す場合にも、同様に適用できる。 *注 4:* システム要素は、データ／情報を操作するハードウェア、ソフトウェア、ファームウェア、運用環境内の物理構造、デバイス及びコンポーネント、及びシステム要素を操作、維持、サポートするための人、プロセス、及び手順によって実装される。 *注 5:* システム要素（System elements）及び情報リソース（information resources）（44 U.S.C. Sec. 3502 及び本出版物で定義）は、本出版物で使用されている限りにおいて交換可能な用語である。
システム開発ライフサイクル（system development life cycle）	システムに関連する活動の範囲。システムの開始、開発及び取得、実装、運用及び保守、最終的に別のシステムの開始を引き起こすシステムの廃棄が含まれる。
システムプライバシー責任者（system privacy officer）	システム又はプログラムの適切な運用上のプライバシー態勢を維持する責任を割り当てられた個人。
システムプライバシーエンジニア（systems privacy engineer）	システムプライバシーエンジニアリング活動を実施する責任を割り当てられた個人。
システムプライバシーエンジニアリング（systems privacy engineering）	プライバシー要件を把握して改善し、目的のあるプライバシー設計又は構成を通じてそれらの要件を情報技術コンポーネント製品及び情報システムに確実に統合するプロセス。
システムセキュリティエンジニア（systems security engineer）	システムセキュリティエンジニアリング活動を実施する責任を割り当てられた個人。
システムセキュリティエンジニアリング（systems security engineering）	セキュリティ要件を把握して改善し、目的のあるセキュリティ設計又は構成を通じてそれらの要件を情報技術コンポーネント製品及び情報システムに確実に統合するプロセス。

システムセキュリティ責任者（system security officer）	情報システム又はプログラムに関する運用面での適切なセキュリティ態勢を維持する責任を割り当てられた個人。
システムセキュリティ計画（system security plan）	*情報システムセキュリティ計画*（information system security plan）を参照。
システム関連のプライバシーリスク（system-related privacy risk） [OMB A-130]	政府機関による個人情報の作成、収集、利用、処理、保存、維持、配布、公開、及び廃棄に関連する、個人に対するリスク。リスク（risk）を参照。
システム関連のセキュリティリスク（system-related security risk） [SP 800-30]	情報又はシステムの機密性、完全性、又は可用性の喪失により生じるリスクで、組織（資産、ミッション、機能、イメージ、又は評判を含む）、個人、他の組織、及び国家に及ぼすインパクトを考慮したもの。リスク（risk）を参照。
システム固有管理策（system-specific control） [OMB A-130]	システムレベルで実装され、他の情報システムに継承されない、情報システムのセキュリティ管理策又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した結果生じる一連の管理策。*テーラリング*（tailoring）を参照。
テーラリング（tailoring） [OMB A-130]	共通管理策の識別及び指定、スコーピングの考慮事項の適用、代替管理策の選択、組織が定めるセキュリティ管理策パラメータへの特定の値の設定、追加のセキュリティ管理策又は拡張管理策によるベースラインの補足、及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管理策ベースラインが変更されるプロセス。テーラリングプロセスはプライバシー管理策にも適用できる。
脅威（threat） [SP 800-30]	情報の不正アクセス、破壊、漏えい、改ざん、及び／又はサービス妨害によって、システムを通じて組織の業務、組織の資産、個人、他の組織、又は国家に有害なインパクトをもたらす可能性のある状況又は事象。
脅威源（threat source） [FIPS 200]	脆弱性を意図的に悪用することを目的とした意図及び方法、又は偶発的に脆弱性をもたらす可能性がある状況及び方法。*脅威エージェント*（threat agent）を参照。
統合的信頼性（trustworthiness） [CNSSI 4009]	特定のタスクを実行し、割り当てられた責任を果たすために、当該エンティティの資格、ケイパビリティ、及び信頼性を他者に信用させる人又は事業体の属性。
統合的信頼性（trustworthiness）（システム）	情報システム（システムの構築に使用される情報技術コンポーネントを含む）が、あらゆる脅威や個人のプライバシーに対して、システムで処理、保存、又は伝送される情報の機密性、完全性、及び可用性を維持することが期待できる度合い。
信頼できる情報システム（trustworthy information system） [OMB A-130]	運用環境において発生が予想される環境破壊、ヒューマンエラー、構造的な障害、及び意図的な攻撃にもかかわらず、規定されたリスクレベルの範囲内で運用できると考えられる情報システム。

システムユーザ（system user）	システムへのアクセスを認可された、個人、又は個人の代理として動作する（システム）プロセス。
脆弱性（vulnerability） [CNSSI 4009]	脅威源によって悪用される又はもたらされる可能性がある、情報システム、システムセキュリティ手順、内部管理策、又は実装における弱点。 *注:* 弱点（weakness）という用語は、欠陥（deficiency）と同義である。弱点は、セキュリティ及び／又はプライバシーリスクにつながる可能性がある。
脆弱性アセスメント（vulnerability assessment） [CNSSI 4009]	セキュリティ対策の妥当性を判定し、セキュリティの欠陥を識別し、提案されたセキュリティ対策の有効性を予測するためのデータを提供し、実装後にそのような対策の妥当性を確認するための、情報システム又は製品の体系的な検査。

附属書 C

略語

一般的な略語

CIO	最高情報責任者（Chief Information Officer）
CNSS	国家安全保障システム委員会（Committee on National Security Systems）
CNSSI	国家安全保障システム委員会指示 （Committee on National Security Systems Instruction）
CNSSP	国家安全保障システム委員会ポリシー （Committee on National Security Systems Policy）
CUI	管理対象非機密情報（Controlled Unclassified Information）
DoD	国防総省（Department of Defense）
EO	大統領令（Executive Order）
FedRAMP	連邦リスク承認管理プログラム （Federal Risk and Authorization Management Program）
FIPS	連邦情報処理規格（Federal Information Processing Standards）
FISMA	連邦情報セキュリティ近代化法 （Federal Information Security Modernization Act）
FOCI	外国人による所有、支配、又は影響（Foreign Ownership, Control, or Influence）
GRC	ガバナンス・リスク・コンプライアンス（Governance Risk Compliance）
GSA	一般調達局（General Services Administration）
IEC	国際電気標準会議（International Electrotechnical Commission）
IEEE	米国電気電子学会（Institute of Electrical and Electronics Engineers）
ISCM	情報セキュリティの継続的監視（Information Security Continuous Monitoring）
IT	情報技術（Information Technology）
IR	内部報告書（Internal Report） 又は省庁間報告書（Interagency Report）
ISO	国際標準化機構（International Organization for Standardization）
NARA	国立公文書記録管理局（National Archives and Records Administration）
NIST	国立標準技術研究所（National Institute of Standards and Technology）
NSA	国家安全保障局（National Security Agency）
ODNI	国家情報長官官房（Office of the Director of National Intelligence）
OMB	行政管理予算局（Office of Management and Budget）
OT	制御・運用技術（Operations Technology）

PCM	プライバシーの継続的監視（Privacy Continuous Monitoring）
PII	個人情報（Personally Identifiable Information）
PL	公法（Public Law）
RMF	リスクマネジメントフレームワーク（Risk Management Framework）
SCRM	サプライチェーンのリスクマネジメント（Supply Chain Risk Management）
SDLC	システム開発ライフサイクル（System Development Life Cycle）
SecCM	セキュリティを重視した構成管理（Security-focused Configuration Management）
SP	特別出版物（Special Publication）

附属書 D

役割及び責任

リスクマネジメントプロセスの主要な参加者

以下の節では、組織のリスクマネジメントプロセスに関与する主要な参加者の役割及び責任について説明する [112]。組織には様々なミッション、ビジネスファンクション、及び組織構造があることを認識すると、リスクマネジメントの役割の命名規則や、リスクマネジメントの責任が組織の職員にどのように割り振られるか（例えば、複数人で 1 つの役割を担当する、又は 1 人で複数の役割を担当する）には違いがある可能性がある [113]。しかし、基本的な機能は同じである。本出版物で説明する RMF の適用は柔軟であり、組織は、セキュリティ及びプライバシーリスクを最適な方法で管理するために、それぞれの組織構造の内部における特定のタスクの目的を効果的に達成することができる。本出版物内で定義されている多くのリスクマネジメントの役割は、組織が実施する SDLC プロセスにおいて対応する役割がある。組織は、可能な場合は常に、組織のリスクマネジメントの役割を、SDLC で定義された類似の（又は補完的な）役割に合わせる [114]。

認可権限のある担当者

*認可権限のある担当者*は、システムの運用、組織のシステムに継承される共通管理策の提供、又は外部プロバイダからのシステム、サービス、又はアプリケーションの使用に対する責任及び説明責任を正式に引き受ける権限を持つ高官又は幹部である。認可権限のある担当者は、組織の業務、組織の資産、及び個人に対するセキュリティ及びプライバシーリスクを受容することができる唯一の組織の担当者である [115]。通常、認可権限のある担当者は、システムの予算を監督する、又は、システムによってサポートされるミッション及び／又はビジネスの業務の責任を負う。したがって、認可権限のある担当者は、そのようなセキュリティリスク及びプライバシーリスクを理解し、受容するのに見合う権限レベルを持つ管理職である。認可権限のある担当者は、計画、合意又は了解の覚書、行動計画及びマイルストーンを承認し、情報システム又は運用環境の重大な変更が再認可を必要とするかどうかを判断する。

認可権限のある担当者は、認可プロセス中に、共通管理策の提供者、システム所有者、最高情報責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、システムセキュリティ及びプライバシー責任者、管理策アセッサー、リスクマネジメント担当責任者／リスク管理者（機能）、及びその他の関係者と活動を調整する。組織におけるミッション／ビジネスプロセス、パートナーシップの協定、及び共有サービスの利用の複雑さが増してきたことに伴い、システムには共同で認可権限を持つ職員が関与することも可能である [116]。その場合、共同認可権限のある担当者間で合意が形成され、セキュリティ及びプライバシー計画で文書化される。認可権限のある担当者は、認可権限のある担当者による指定代理人に委任された認可活動及び

[112] 組織は、リスクマネジメントプロセスをサポートする他の役割を定義してもよい。

[113] 組織は、同じ個人を複数のリスクマネジメント役割に割り当てる場合、利害の衝突がないようにする。RMF の*準備（組織レベル）*ステップのタスク P-1 を参照。

[114] 例えば、SDLC におけるシステム開発者又はプログラムマネージャの役割はシステム所有者の役割に合わせることができ、SDLC におけるミッション又はビジネスオーナーの役割は認可権限のある担当者の役割に合わせることができる。[SP 800-64]は、SDLC における情報セキュリティに関するガイダンスを提供している。

[115] [FIPS 200]で説明されている認可権限のある担当者の責任及び説明責任は、他の組織及び国家に対するリスクを含めるように [SP 800-53]で拡張された。

[116][OMB A-130]は、認可権限のある担当者及び共同認可権限のある担当者に関する追加情報を提供している。

機能が指定されたとおりに実施されることを確実にする責任及び説明責任を負う。連邦政府機関の場合、認可権限のある担当者の役割は、米国政府の固有の機能であり、政府職員にのみ割り当てられる。

認可権限のある担当者による指定代理人

*認可権限のある担当者による指定代理人*は、認可権限のある担当者によって指名され、認可権限のある担当者の代理で情報システム及び組織に対するリスクの管理に関連する日々の活動を調整及び実施する権限が付与された組織の担当者である。これには、RMF の実行に関連する多くの活動を実施することが含まれる。認可権限のある担当者から指定代理人に委任できない唯一の活動は、認可の判断及び関連する認可判断文書への署名（すなわち、リスクの受容）である。

最高取得責任者

*最高取得責任者*は、政府機関の取得活動の管理を通じて政府機関のミッションが達成されるように、政府機関の長及び他の政府機関職員に助言及び支援するために、政府機関の長によって指名される組織の担当者である。最高取得責任者は、取得活動及びプログラムのパフォーマンスを監視し、政府機関内で取得の意思決定を行うための明確な権限、説明責任、及び責任の系統を確立し、政府機関の取得ポリシーの方向性及び実施を管理し、調達する資産又はサービスの性質を考慮して最高価値の要件を満たすために、責任ある供給源からの完全かつ開かれた競争を促進するポリシー、手順、及びプラクティスを確立する。最高取得責任者は、組織の調達及び取得においてセキュリティ及びプライバシー要件が確実に定義されるように、ミッション又はビジネスオーナー、認可権限のある担当者、リスクマネジメント担当責任者、システム所有者、共通管理策の提供者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、及びリスク管理者（機能）と調整する。

最高情報責任者

最高情報責任者 [117] は、政府機関の情報セキュリティ責任者の指名、セキュリティ要件に対処するためのセキュリティポリシー、手順、及び管理手法の策定及び保守、セキュリティに重要な責任を担う職員の監督、及びそれらの職員が適切に訓練されていることの確認、政府の上級職員のセキュリティ責任に関する支援、及び是正措置の進捗を含む、組織のセキュリティプログラムの有効性に関する政府機関の長への報告の責任を負う組織の担当者である。最高情報責任者は、リスクマネジメント担当責任者、リスク管理者（機能）、及び政府機関の情報セキュリティ責任者のサポートを得て、認可権限のある担当者及び指定代理人と緊密に連携し、以下のことを確実にする。

[117] 組織が正式に最高情報責任者を指名していない場合、[FISMA]は、関連する責任を同等の組織の担当者が担当することを要求している。

- 組織のすべてのシステム及び運用環境に対する適切なセキュリティにつながる、組織全体のセキュリティプログラムが効果的に実装されている。
- セキュリティ及びプライバシー（サプライチェーンを含む）のリスクマネジメントに関する考慮事項が、プログラミング／計画／予算編成サイクル、エンタープライズアーキテクチャ、SDLC、及び取得に統合されている。
- 組織のシステム及び共通管理策が、承認されたシステムセキュリティ計画の対象であり、現行の認可を保有している。
- 組織全体で必要とされるセキュリティ活動が、効率的で費用対効果の高い、タイムリーな方法で実施されている。
- セキュリティ活動に関する報告が一元化されている。

最高情報責任者及び認可権限のある担当者は、組織の優先順位に基づいて、組織のミッション及びビジネスファンクションをサポートするシステムの保護に特化したリソースの割り振りを決定する。個人情報を処理する情報システムについては、最高情報責任者及び認可権限のある担当者は、これらのシステムの保護に特化したリソースの割り振りに関する決定を政府機関のプライバシー保護責任者と調整する。選択されたシステムによっては、最高情報責任者が認可権限のある担当者、又は組織の他の上級職員との共同認可権限のある担当者として指名されることがある。最高情報責任者の役割は、米国政府の固有の機能であり、政府職員にのみ割り当てられる。

共通管理策の提供者

*共通管理策の提供者*は、共通管理策（すなわち、組織のシステムによって継承される管理策）の実装、アセスメント、及び監視に責任を持つ個人、グループ、又は組織である [118]。共通管理策の提供者は、組織が定義した共通管理策をセキュリティ及びプライバシー計画（又は組織が規定した同等の文書）で確実に文書化すること、共通管理策の必要なアセスメントが適切なレベルの独立性を確保した有資格のアセッサーによって確実に実施されるようにすること、アセスメント結果を管理策アセスメント報告書で文書化すること、及び欠陥のある管理策に対して行動計画及びマイルストーンを作成することの責任も負う。セキュリティ及びプライバシー計画、セキュリティ及びプライバシーアセスメント報告書、及び共通管理策の行動計画及びマイルストーン（又は、そのような情報の要約）は、それらの管理策に対する説明責任及び認可権限のある担当者によってレビュー及び承認された後に、共通管理策を継承するシステムのシステム所有者が利用できるようになる。

政府機関のプライバシー保護責任者は、どのプライバシー管理策を共通管理策として扱うことができるかを指定する責任を負う。共通管理策として指定されたプライバシー管理策は、組織のプライバシープログラム計画で文書化される [119]。政府機関のプライバシー保護責任者は、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実施又は計画されている共通管理策に対して監督責任を負い、これらの管理策をアセスメントする責任を負う。

[118] 組織は、セキュリティ及びプライバシー責任を組織全体でどのように割り振るかに応じて、複数の共通管理策の提供者を持つことができる。共通管理策が組織のシステム内に存在する場合、共通管理策の提供者が*システム所有者*になることもある。

[119] プライバシープログラム計画は、プライバシープログラムの構造、政府機関のプライバシー保護責任者及びその他のプライバシー担当者及びスタッフの役割、プライバシープログラムの戦略的目標及び目的、プライバシープログラム専用のリソース、及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実施又は計画されているプログラムマネジメント管理策及び共通管理策を含む、政府機関のプライバシープログラムの概要を記載した正式な文書である。

組織の判断で、共通管理策として指定されたプライバシー管理策は、独立したアセッサーによってアセスメントされる場合がある。しかし、いずれの場合も、政府機関のプライバシー保護責任者は、独立したアセッサーによって行われるプライバシー機能を含め、組織のプライバシープログラムに対する責任及び説明責任を保持する。プライバシー計画及びプライバシー管理策アセスメント報告書は、共通管理策として指定されたプライバシー管理策を継承するシステムのシステム所有者が利用できる。

管理策アセッサー

*管理策アセッサー*は、管理策の有効性（すなわち、管理策が正しく実装され、意図した通りに運用され、システム及び組織のセキュリティ及びプライバシー要件を満たすことに関して期待した成果を生み出している度合い）を判断するために、実装済みの管理策及び拡張管理策の包括的なアセスメントの実施に責任を持つ、個人、グループ、又は組織である。システムについては、実装されたシステム固有の管理策と、ハイブリッド管理策のシステムによって実装された部分がアセスメントされる。共通管理策については、実装された共通管理策と、ハイブリッド管理策の共通管理策によって実装された部分がアセスメントされる。システム所有者及び共通管理策の提供者は、セキュリティ及びプライバシーの専門知識とアセッサーの判断に基づき、セキュリティ及びプライバシーアセスメント計画で規定されているアセスメント手順を使用して、実装された管理策をアセスメントする。アセスメントを効果的に実施するためには、特定の管理策の要件又は技術に関する専門知識によって細分化された複数の管理策アセッサーが必要となる場合がある。管理策アセスメントを開始する前に、アセッサーはセキュリティ及びプライバシー計画をレビューし、アセスメント計画の策定を促進する。管理策アセッサーは、システム、運用環境、及び共通管理策において発見された欠陥の重大性をアセスメントし、特定された脆弱性に対処するための是正処置を推奨することができる。システムレベルの管理策アセスメントでは、管理策アセッサーは継承された管理策はアセスメントせず、ハイブリッド管理策のシステムによって実装された部分のみをアセスメントする。管理策アセッサーは、アセスメントの結果及び所見を含む、セキュリティ及びプライバシーアセスメント報告書を準備する。

アセッサーの独立性に必要なレベルは、法律、大統領令、指令、規則、ポリシー、標準、又はガイドラインに基づき、認可権限のある担当者によって決定される。管理策アセスメントが、認可判断又は継続的な認可をサポートする目的で実施される場合、認可権限のある担当者は、必要な独立性の程度について明確に判断する。アセッサーの独立性は、公平かつ公正なアセスメントプロセスを維持し、アセスメント結果の信ぴょう性を判断し、認可権限のある担当者が情報に基づいたリスクベースの認可判断を行うのに必要な客観的な情報を確実に受け取れるようにするための要素である。

政府機関のプライバシー保護責任者は、プライバシー管理策のアセスメント及び認可権限のある担当者へのプライバシー情報の提供の責任を負う。組織の判断で、プライバシー管理策は独立したアセッサーによってアセスメントされる場合がある。しかし、いずれの場合も、政府機関のプライバシー保護責任者は、独立したアセッサーによって行われるプライバシー機能を含め、組織のプライバシープログラムに対する責任及び説明責任を保持する。

エンタープライズアーキテクト

*エンタープライズアーキテクト*は、組織内のリーダー及び対象分野の専門家と協力して、組織のミッション及びビジネスファンクション、ミッション／ビジネスプロセス、情報、及び情報技術資産（IT 資産）の全体像を構築する責任を負う個人又はグループである。情報セキュリティ及びプライバシーに関して、エンタープライズアーキテクトは以下のことを行う。

- 効果的なセキュリティ及びプライバシーソリューションを促進するエンタープライズアーキテクチャ戦略を実装する。
- エンタープライズアーキテクチャ内のシステム／システム要素の最適な配置を決定し、システムとエンタープライズアーキテクチャの間のセキュリティ及びプライバシーの問題に対処するために、セキュリティ及びプライバシーアーキテクトと調整する。
- IT インフラの複雑さを軽減し、セキュリティを容易にできるように支援する。
- エンタープライズアーキテクチャに関連する適切な管理策の実装及び初期構成ベースラインの決定を支援する。
- 認可境界の決定及びシステム要素への管理策の割り振りを促進するために、システム所有者及び認可権限のある担当者と協力する。
- リスク管理者（機能）の一部としての役割を果たす。
- 組織のリスクマネジメント戦略及びシステムレベルのセキュリティ及びプライバシー要件を、プログラム、計画、及び予算編成の活動、SDLC、取得プロセス、セキュリティ及びプライバシー（サプライチェーンを含む）のリスクマネジメント、及びシステムエンジニアリングプロセスに統合することを支援する。

政府機関の長

*政府機関の長*は、組織の業務及び資産、個人、他の組織、及び国家に対するリスク―すなわち、政府機関によって、又は政府機関の代理で行動する他の組織によって収集又は維持管理される情報、並びに政府機関、政府機関の請負業者、又は政府機関の代理で行動する他の組織によって使用又は運用される情報システムの不正アクセス、不正利用、漏えい、破壊、改ざん、又は破棄によってもたらされるリスクに見合った、情報セキュリティ上の保護を提供する責任及び説明責任を負う。また、政府機関の長は、プライバシーの利益が保護され、PII（個人情報）が組織内で責任を持って管理されることを保証する責任を負う、組織の高官でもある。
政府機関の長は以下のことを保証する。

- 情報セキュリティ及びプライバシーマネジメントプロセスが、戦略的及び運用上の計画策定プロセスに統合されている
- 組織の高官が、自身の管理下にある業務及び資産をサポートする情報及びシステムに対する情報セキュリティを提供する
- 適用されるプライバシー要件への確実な準拠、プライバシーリスクの管理、及び組織のプライバシープログラムについて責任及び説明責任を負う、政府機関のプライバシー保護責任者が指名されている
- 組織は、法律、大統領令、ポリシー、指令、指示、標準、ガイドラインのセキュリティ及びプライバシー要件への準拠を支援するための適切な訓練を受けた職員を有している

政府機関の長は、セキュリティ及びプライバシーリスクを効果的に管理し、組織が遂行するミッション及びビジネスファンクションを保護するために必要な組織のコミットメント及び活動を確立する。政府機関の長は、セキュリティ及びプライバシーの説明責任を確立し、セキュリティ及びプライバシープログラムの監視及び改善を積極的に支援し、監督する。セキュリティ及びプライバシーに対する上級幹部のコミットメントは、組織内に一定レベルのデューディリジェンスを確立し、ミッション及びビジネスの成功に向けた環境を推進する。

情報所有者又は情報管理者

*情報所有者又は情報管理者*は、特定の情報に関する法的権限、管理上の権限、又は運用上の権限を持ち、その情報の生成、収集、処理、配布、及び廃棄に関するポリシー及び手順を確立することに責任を負う連邦政府職員である。情報共有環境では、情報所有者／管理者は、情報の適切な利用及び保護のための規則を確立することに責任を負い、情報が他の組織と共有される、又は他の組織に提供される場合であっても、その責任を保持する。システムで処理、保存、又は伝送される情報の所有者／管理者は、システム所有者と同一人物である場合もあれば、そうではない場合もある。個々のシステムには、複数の情報所有者／管理者からの情報が含まれる場合がある。情報所有者／管理者は、情報が処理、保存、又は伝送されるシステムのセキュリティ及びプライバシー要件と管理策に関するインプットを、システム所有者に提供する。

ミッション又はビジネスオーナー

*ミッション又はビジネスオーナー*は、特定のミッション又は事業部門に対する責任を持ち、それらのミッション又は事業部門をサポートする組織システムのセキュリティ又はプライバシー上の関心を持つ、組織内の高官又は管理職である。ミッション又はビジネスオーナーは、組織のミッション及びビジネスプロセスの確立と、組織のミッション及びビジネス運営の実施を確実に成功させるための保護ニーズとセキュリティ及びプライバシー要件を確立する上で重要な役割を持つ主要なステークホルダーである。ミッション及びビジネスオーナーは、リスクマネジメント戦略に不可欠なインプットを提供したり、SDLC で積極的な役割を果たしたりするほか、認可権限のある担当者の役割を果たすこともある。

リスク管理者（機能）

*リスク管理者（機能）*は、リスクマネジメントに対して包括的な組織全体のアプローチを提供する、組織内の個人又はグループである。リスク管理者（機能）は、リスクマネジメント担当責任者が主導し、上級幹部、管理職、マネージャ、ミッション／ビジネスオーナー、最高情報責任者、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、システム所有者、共通管理策の提供者、エンタープライズアーキテクト、セキュリティアーキテクト、システムセキュリティ又はプライバシーエンジニア、システムセキュリティ又はプライバシー責任者、組織のミッション／ビジネスの成功に既得権を持つステークホルダーの共通リスクマネジメントリソースとして機能する。リスク管理者（機能）は、米国政府の固有の機能であり、政府職員にのみ割り当てられる。

リスク管理者（機能）は、システムのリスクに関する考慮事項（システムの認可判断、システムによって継承される共通管理策を含む）が、コアミッション及びビジネスファンクションを遂行する上での組織の戦略的目標及び目的に関する組織全体の観点から考慮されることを確実にする。リスク管理者（機能）は、リスクマネジメントが組織全体で一貫していること、リスクマネジメントに組織のリスク許容度が反映されていること、及びミッション／ビジネスを確実に成功させるために他の種類のリスクがリスクマネジメントで考慮されていることを確実にする。

リスク管理者（機能）は、組織内の上級幹部及び管理職と調整して、以下のことを行う。

- リスクマネジメントの役割及び責任を確立する。
- 組織のセキュリティリスクの戦略的な視点を提供し[120]、組織のリスク判断（リスクの枠組み化、アセスメント、対応、長期にわたる監視の方法を含む）を手引きし、情報を提供する、組織全体の*リスクマネジメント戦略*を策定して実装する。

[120] 認可権限のある担当者は、認可判断を下す際に、認可決定によって生じる組織全体のリスクを十分に理解したり、明確に受容したりすることなく、狭い視点又は局所的な視点を持つことがある。

- リスクに対処するための包括的で組織全体の全体的なアプローチ―組織の統合された業務をより深く理解するためのアプローチ―を提供する。
- 組織のシステム及びシステム運用環境に関する脅威、脆弱性、セキュリティ及びプライバシーリスク（サプライチェーンリスクを含む）の情報を管理する。
- あらゆる種類のリスク及びリスク源（集約リスクを含む）を検討するための組織全体のフォーラムを設置する。
- 組織が責任を負うシステムの運用及び使用、並びにそれぞれの運用環境から生じる集約リスクに基づいて、組織のリスク態勢を識別する。
- 一貫性のある効果的なリスクベースの意思決定が確実に行われるようにするために、組織が実施するリスクマネジメント活動を監督する。
- 組織の戦略的な視点及びその統合された業務に関するリスクについての幅広い理解を深める。
- 効果的な手段を確立し、組織内部及び外部の主要なステークホルダー（例えば、認可権限のある担当者、その他の上級幹部）との間でリスク情報を伝達及び共有するための中心的な役割を果たす。
- リスクの枠組み化、アセスメント、対応、及び監視に関して、親組織によって認められている下位組織の自律性の度合いを規定する。
- 責任の共有を必要とする認可活動（例えば、共同認可）を含めるよう、認可権限のある担当者間の協力と連携を促進する。
- 組織の業務及び資産、個人、他の組織、及び国家に対するすべてのリスク源（集約リスクを含む）について検討するための、組織全体にわたるフォーラムを提供する。

- 認可判断において、ミッション及びビジネスの成功に必要なすべての要素が確実に考慮されるようにする。
- 外部プロバイダを利用して組織のミッション及びビジネスファンクションをサポートすることに対する責任の共有が、必要な可視性を得て、適切な意思決定機関に昇格するようにする。

リスク管理者（機能）は、特定の組織構造も、組織内の特定の個人又はグループに割り当てられた正式な責任も想定していない。政府機関又は組織の長は、リスク管理者（機能）を保持すること、又はその機能を委任することを選択してもよい。リスク管理者（機能）には、組織の戦略的目標及び目的、組織のミッション／ビジネスファンクション、技術的な可能性及び制約事項、並びに組織の業務を形成する主要な任務及びガイダンスを理解するために、スキル、専門知識、及び視点の組み合わせが必要となる。この必要とされる組み合わせを提供するために、リスク管理者（機能）は、1 人の個人又は 1 つの部門（専門スタッフによってサポートされる）、又は指定されたグループ（例えば、リスク委員会、エグゼクティブ運営委員会、経営幹部会議）によって満たされることができる。リスク管理者（機能）は、効率性と有効性を促進するような方法で、組織のガバナンス構造に適合する。

セキュリティ又はプライバシーアーキテクト

*セキュリティ又はプライバシーアーキテクト*は、組織のミッション及びビジネスファンクション並びに個人のプライバシーを保護するために必要なステークホルダーの保護ニーズ及びそれに対応するシステム要件が、リファレンスモデル、セグメントアーキテクチャ、及びソリューションアーキテクチャ（ミッション及びビジネスプロセスをサポートするシステム）を含むエンタープライズアーキテクチャにおいて適切に対処されることを確実にする責任を負う個人、グループ、又は組織である。セキュリティ又はプライバシーアーキテクトは、エンタープライズアーキテクトとシステムセキュリティ又はプライバシーエンジニアとの間の主たる連絡役としての役割を果たし、システム所有者、共通管理策の提供者、及びシステムセキュリティ又はプライバシー責任者と管理策の割り振りに関する調整を行う。

セキュリティ又はプライバシーアーキテクトは、システムセキュリティ又はプライバシー責任者と協力して、様々なセキュリティ及びプライバシー問題について、認可権限のある担当者、最高情報責任者、リスクマネジメント担当責任者又はリスク管理者（機能）、政府機関の情報セキュリティ責任者、及び政府機関のプライバシー保護責任者に対して助言を行う。例としては、認可境界の確立、セキュリティ又はプライバシーアラートの確立、システム又は管理策に存在する欠陥の重大度のアセスメント、行動計画及びマイルストーンの策定、リスク軽減アプローチの作成、識別された脆弱性又はプライバシーリスクによる潜在的なマイナスの影響などがある。

セキュリティアーキテクト及びプライバシーアーキテクトが別々の役割である場合、一般的に、セキュリティアーキテクトは、機密性、完全性、及び可用性を提供するために、不正なシステム活動又は行動から情報及び情報システムを保護するエンタープライズアーキテクチャの側面に責任を負う。プライバシーアーキテクトは、プライバシー要件に確実に準拠し、PII の処理に関連する個人のプライバシーリスクを管理するエンタープライズアーキテクチャの側面に責任を負う。セキュリティアーキテクト及びプライバシーアーキテクトの責任は、PII のセキュリティを保護するエンタープライズアーキテクチャの側面については重なり合っている。

リスクマネジメント担当責任者

*リスクマネジメント担当責任者*は、組織内のリスク管理者（機能）を主導及び管理する個人であり、情報セキュリティ及びプライバシーリスクマネジメントプロセスを戦略プロセス、運用プロセス、及び予算計画プロセスと整合させる責任を負う。リスクマネジメント担当責任者は、政府機関の長、又は政府機関の長によって指名された個人である。リスクマネジメント担当責任者は、リスク管理者（機能）の組織構造及び責任を決定し、政府機関の長と調整して、リスク管理者（機能）を保持したり、その機能を他の連邦政府職員又はグループに委任したりしてもよい。リスクマネジメント担当責任者は、米国政府の固有の機能であり、政府職員にのみ割り当てられる。

政府機関の情報セキュリティ責任者

*政府機関の情報セキュリティ責任者*は、FISMA の下で最高情報責任者のセキュリティの責任を遂行する責任を負う組織の担当者であり、組織の認可権限のある担当者、システム所有者、共通管理策の提供者、及びシステムセキュリティ責任者に対する最高情報責任者の主たる連絡役としての役割を果たす。また、政府機関の情報セキュリティ責任者は、政府機関のプライバシー保護責任者と調整して、プライバシーと情報セキュリティプログラムの間の調整を確実に行う責任も負う。政府機関の情報セキュリティ責任者は、トレーニング及び経験を含む、セキュリティプログラムの機能を管理するのに必要な専門的な能力を有し、第一義的な責任としてセキュリティの義務を維持し、FISMA の要件に従った信頼性が高くセキュアな情報及びシステムを実現するために組織を支援する特定のミッション及びリソースを持つ部門を率いる。政府機関の情報セキュリティ責任者は、認可権限のある担当者による指定代理人として、あるいはセキュリティ管理策アセッサーとしての役割を果たすこともある。政府機関の情報セキュリティ責任者の役割は、米国政府の固有の機能であり、政府職員にのみ割り当てられる。また、組織は、政府機関の情報セキュリティ責任者を情報セキュリティ責任者又は最高情報セキュリティ責任者と呼ぶこともある。

政府機関のプライバシー保護責任者

*政府機関のプライバシー保護責任者*は、適用されるプライバシー要件に確実に準拠し、プライバシーリスクを管理するための機関全体の責任及び説明責任を負う高官又は管理職である。政府機関のプライバシー保護責任者は、特に、以下のことに対して責任を負う。

- プライバシー及び情報セキュリティ活動の調整を確実にするために、政府機関の情報セキュリティ責任者と調整する。
- 個人情報を作成、収集、使用、処理、保存、維持、配布、開示、又は廃棄する情報システムの分類をレビューし、承認する。
- どのプライバシー管理策をプログラムマネジメント、共通管理策、システム固有の管理策、及びハイブリッドプライバシー管理策として扱うかを指定する。
- プライバシー管理策が正しく実施され、意図したとおりに動作し、適用されるプライバシー要件に確実に準拠し、プライバシーリスクを管理するのに十分であるかを判断するための、アセスメント方法及び測定基準を識別する。
- 認可、再認可、又は継続的な認可の前に、情報システムのプライバシー計画をレビューして承認する。
- プライバシー要件に確実に準拠し、プライバシーリスクを管理するために、個人情報を作成、収集、使用、処理、保存、維持、配布、開示、又は廃棄する情報システムの認可パッケージをレビューする。
- 政府機関で選択され実装されたすべてのプライバシー管理策の継続的な有効性を検証するために、プライバシー管理策アセスメントを実施し、その結果及び文書化する。
- プライバシーリスクの継続的な認識を維持し、プライバシー要件への準拠を確実にし、プライバシーリスクを管理するのに十分な頻度でプライバシー管理策をアセスメントするための、プライバシーの継続的監視プログラムを確立して維持する。

政府機関のプライバシー保護責任者の役割は、米国政府の固有の機能であり、政府職員にのみ割り当てられる。

システム管理者

*システム管理者*は、システム又は特定のシステム要素の設定及び保守に責任を負う個人、グループ、又は組織である。システム管理者の責任には、ハードウェア及びソフトウェアのインストール、構成、及び更新、ユーザアカウントの設定及び管理、バックアップ、リカバリ、及び再構成活動の監督又は実施、管理策の実装、組織のセキュリティ及びプライバシーポリシー及び手順の順守及び実施などが含まれる。システム管理者の役割には、他の種類のシステム管理者（例えば、データベース管理者、ネットワーク管理者、ウェブ管理者、アプリケーション管理者）が含まれる。

システム所有者

*システム所有者*は、システムの調達、開発、統合、修正、運用、保守、及び廃棄に責任を負う組織の担当者である[121]。システム所有者は、ユーザコミュニティ（すなわち、ミッション、ビジネス、又は業務要件を満たすためにシステムにアクセスする必要があるユーザ）の業務上の利害に対処する責任、及びセキュリティ要件に確実に準拠する責任を負う。システム所有者は、システムセキュリティ及びプライバシー保護責任者と調整して、セキュリティ及びプライバシー計画の策定及び維持に責任を負い、選択され実装された管理策に従ってシステムが確実に運用されるようにする。

システム所有者は、情報所有者／管理者と調整して、誰がシステムにアクセスできるのか（及び、どのような種類の特権又はアクセス権を持つか）を決定する[122]。システム所有者は、システムユーザ及びサポート担当者が必要なセキュリティ及びプライバシートレーニングを確実に受けるようにする。システム所有者は、認可権限のある担当者が提供するガイダンスに基づいて、認可を実施することの必要性を組織の担当者に通知し、その作業に利用可能なリソースを確保し、必要なシステムアクセス権、情報、及び文書を管理策アセッサーに提供する。システム所有者は、管理策アセッサーからセキュリティ及びプライバシーアセスメントの結果を受け取る。脆弱性又はセキュリティ及びプライバシーリスクを軽減又は除去するための適切なステップを実行した後、システム所有者は認可パッケージを作成し、そのパッケージを認可権限のある担当者又は認可権限のある担当者による指定代理人に提出し、裁定を仰ぐ[123]。

[121] 組織は、システム所有者をプログラムマネージャ又はビジネス／アセットオーナーと呼ぶことがある。

[122] 組織のシステム内の特定の情報に誰がアクセスできるのか（及び、どのような種類の特権又はアクセス権を持つか）を決定する責任は、情報所有者／管理者が負う場合がある。

[123] 認可権限のある担当者は、認可パッケージの情報を収集・整理するために、システム所有者以外の個人を指名することを選択してもよい。この場合、指名された個人が、システム所有者と情報の収集及び整理活動を調整する。

システムセキュリティ又はプライバシー責任者

システムセキュリティ又はプライバシー責任者 [124] は、組織のシステムに対してセキュリティ及びプライバシー態勢が維持されることを確実にする責任を負う個人であり、システム所有者と緊密に連携して作業する。また、システムセキュリティ又はプライバシー責任者は、システムの管理に関連する技術的及びその他のあらゆる事柄の主要なアドバイザーとしての役割も果たす。システムセキュリティ又はプライバシー責任者は、組織のシステムのセキュリティ又はプライバシーの側面を管理するための知識及び専門知識を持っており、多くの組織では、システムセキュリティ又はプライバシーの日々の運用に対する責任が割り当てられる。この責任には、物理的及び環境的保護、職員のセキュリティ、インシデント対応、セキュリティ及びプライバシーに関するトレーニング及び意識向上も含まれる場合があるが、これらに限定されない。

システムセキュリティ又はプライバシー責任者は、システムレベルのセキュリティ及びプライバシーポリシー及び手順の策定を支援し、それらのポリシー及び手順に確実に準拠するよう求められる場合がある。システムセキュリティ又はプライバシー責任者は、システム所有者と緊密に調整して、セキュリティ及びプライバシー計画の策定及び更新、システムに対する変更の管理及び制御、及びそれらの変更によるセキュリティ又はプライバシーへの影響のアセスメントを含む、システム及びその運用環境の監視において積極的な役割を果たすことが多い。

システムセキュリティ責任者とシステムプライバシー責任者が別々の役割である場合、一般的に、システムセキュリティ責任者は機密性、完全性、及び可用性を提供するために、不正なシステム活動又は行動から情報及び情報システムを保護するというシステムの側面に対して責任を負う。システムプライバシー責任者は、プライバシー要件に確実に準拠し、PII の処理に関連する個人のプライバシーリスクを管理するというシステムの側面に対して責任を負う。システムセキュリティ責任者とシステムプライバシー責任者の責任は、PII のセキュリティを保護するというシステムの側面については重なる部分がある。

システムユーザ

*システムユーザ*は、割り当てられた職務を遂行するために情報及び情報システムへのアクセスを認可された個人、又は個人の代理として動作する（システム）プロセスである。システムユーザの責任には、組織のシステムの許容される使用を規定する組織のポリシーを順守すること、組織が提供する情報技術リソースを定められた目的のみに使用すること、異常な、又は疑わしいシステム動作を報告することが含まれるが、これらに限定されない。

システムセキュリティ又はプライバシーエンジニア

*システムセキュリティ又はプライバシーエンジニア*は、SDLC の一環としてシステムセキュリティ又はプライバシーエンジニアリング活動を実施する責任を負う個人、グループ、又は組織である。システムセキュリティ及びプライバシーエンジニアリングは、システムのセキュリティ及びプライバシー要件を把握及び改良し、セキュリティ又はプライバシーの体系化、設計、開発、及び構成を通じて、それらの要件がシステム及びシステム要素に効果的に統合されることを確実にするプロセスである。

[124] 組織は、*システムセキュリティマネージャ*又は*セキュリティマネージャ*の役割を、システムセキュリティ責任者と同様の責務を負う役割、又はセキュリティプログラムを監督する責任を負う役割として定義することがある。このような場合には、組織の判断で、各システムセキュリティ責任者がシステムセキュリティマネージャ又はセキュリティマネージャに直接報告を行ってもよい。組織は、プライバシーに関する同等の責任を、適切な、対象分野の専門知識を持つ別の個人に割り当ててもよい。

システムセキュリティ又はプライバシーエンジニアは開発チームの一員であり、組織のシステムの設計及び開発、又は既存のシステムのアップグレードを行うだけでなく、継続的監視の要件がシステムレベルで確実に対処されるようにする。システムセキュリティ又はプライバシーエンジニアは、管理策を実装する際に、ソフトウェアエンジニアリングの方法論、システム及びセキュリティ又はプライバシーのエンジニアリングの原則、セキュアな、又はプライバシーを強化する設計、セキュアな、又はプライバシーを強化するアーキテクチャ、及びコーディング技法などのベストプラクティスを採用する。システムセキュリティ又はプライバシーエンジニアは、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、セキュリティ及びプライバシーアーキテクト、システム所有者、共通管理策の提供者、及びシステムセキュリティ又はプライバシー責任者と、セキュリティ及びプライバシーに関する活動を調整する。

システムセキュリティエンジニアとプライバシーエンジニアが別々の役割である場合、一般的に、システムセキュリティエンジニアは機密性、完全性、及び可用性を提供するために、不正なシステム活動又は行動からの情報及び情報システムの保護に関連する活動に責任を負う。プライバシーエンジニアは、プライバシー要件への確実な準拠、及び PII の処理に関連する個人のプライバシーリスクの管理に関連する活動に責任を負う。システムセキュリティエンジニアとプライバシーエンジニアの責任は、PII のセキュリティの保護に関連する活動については重なる部分がある。

附属書 E

RMF の各タスクの概要

RMF のタスク、責任、補助的な役割

表 E-1：準備のタスク、責任、補助的な役割

RMF タスク	主たる責任者	補助的な役割を果たす者
組織レベル		
タスク P-1 **リスクマネジメント役割** セキュリティ及びプライバシーリスクマネジメントに関する特定の役割を識別し、個人に割り当てる。	・政府機関の長 ・最高情報責任者 ・政府機関のプライバシー保護責任者	・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・リスクマネジメント担当責任者、又はリスク管理者（機能） ・政府機関の情報セキュリティ責任者
タスク P-2 **リスクマネジメント戦略** リスク許容度の判断を含む、組織のリスクマネジメント戦略を確立する。	・政府機関の長	・リスクマネジメント担当責任者、又はリスク管理者（機能） ・最高情報責任者 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者
タスク P-3 **リスクアセスメント – 組織** 組織全体のセキュリティ及びプライバシーリスクをアセスメントし、リスクアセスメントの結果を継続的に更新する。	・リスクマネジメント担当責任者、又はリスク管理者（機能） ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者	・最高情報責任者 ・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・ミッション又はビジネスオーナー
タスク P-4 **組織的にテーラリングされた管理策ベースライン及びサイバーセキュリティフレームワークプロファイル（オプション）** 組織的にテーラリングされた管理策ベースライン、及び／又はサイバーセキュリティフレームワークプロファイルを確立、文書化、及び公開する。	・ミッション又はビジネスオーナー ・リスクマネジメント担当責任者、又はリスク管理者（機能）	・最高情報責任者 ・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者

RMF タスク	主たる責任者	補助的な役割を果たす者
タスク P–5 **共通管理策の識別** 組織システムによる継承に利用可能な、組織全体の共通管理策を識別、文書化、及び公開する。	・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者	・ミッション又はビジネスオーナー ・リスクマネジメント担当責任者、又はリスク管理者（機能） ・最高情報責任者 ・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・共通管理策の提供者 ・システム所有者
タスク P–6 **インパクトレベルの優先順位付け（オプション）** インパクトレベルが同じ組織システムに優先順位を付ける。	・リスクマネジメント担当責任者、又はリスク管理者（機能）	・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者 ・ミッション又はビジネスオーナー ・システム所有者 ・最高情報責任者 ・認可権限のある担当者、又は認可権限のある担当者による指定代理人
タスク P–7 **継続的監視戦略 – 組織** 管理策の有効性を継続的に監視するための組織全体の戦略を策定し、実装する。	・リスクマネジメント担当責任者、又はリスク管理者（機能）	・最高情報責任者 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者 ・ミッション又はビジネスオーナー ・システム所有者 ・認可権限のある担当者、又は認可権限のある担当者による指定代理人
システムレベル		
タスク P–8 **ミッション又はビジネスの重点領域** システムがサポートすることを意図しているミッション、ビジネスファンクション、及びミッション／ビジネスプロセスを識別する。	・ミッション又はビジネスオーナー	・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・システム所有者 ・情報所有者又は情報管理者 ・最高情報責任者 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者
タスク P–9 **システムステークホルダー** システムの設計、開発、実装、アセスメント、運用、保守、又は廃棄に利害関係を有するステークホルダーを識別する。	・ミッション又はビジネスオーナー ・システム所有者	・最高情報責任者 ・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・情報所有者又は情報管理者 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者 ・最高取得責任者

RMF タスク	主たる責任者	補助的な役割を果たす者
タスク P-10 **資産の識別** 保護する必要がある資産を識別する。	・システム所有者	・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・ミッション又はビジネスオーナー ・情報所有者又は情報管理者 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者 ・システム管理者
タスク P-11 **認可境界** システムの認可境界を決定する。	・認可権限のある担当者	・最高情報責任者 ・ミッション又はビジネスオーナー ・システム所有者 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者 ・エンタープライズアーキテクト
タスク P-12 **情報の種類** システムによって処理、保存、及び伝送される情報の種類を識別する。	・システム所有者 ・情報所有者又は情報管理者	・システムセキュリティ責任者 ・システムプライバシー責任者 ・ミッション又はビジネスオーナー
タスク P-13 **情報ライフサイクル** システムによって処理、保存、又は伝送される情報の種類ごとに、情報ライフサイクルのすべての段階を識別し、理解する。	・政府機関のプライバシー保護責任者 ・システム所有者 ・情報所有者又は情報管理者	・最高情報責任者 ・ミッション又はビジネスオーナー ・セキュリティアーキテクト ・プライバシーアーキテクト ・エンタープライズアーキテクト ・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
タスク P-14 **リスクアセスメント – システム** システムレベルのリスクアセスメントを実施し、リスクアセスメント結果を継続的に更新する。	・システム所有者 ・システムセキュリティ責任者 ・システムプライバシー責任者	・リスクマネジメント担当責任者、又はリスク管理者（機能） ・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・ミッション又はビジネスオーナー ・情報所有者又は情報管理者 ・システムセキュリティ責任者
タスク P-15 **要件の定義** システム及び運用環境に関するセキュリティ及びプライバシー要件を定義する。	・ミッション又はビジネスオーナー ・システム所有者 ・情報所有者又は情報管理者 ・システムプライバシー責任者	・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者 ・システムセキュリティ責任者 ・最高取得責任者 ・セキュリティアーキテクト ・プライバシーアーキテクト ・エンタープライズアーキテクト

RMF タスク	主たる責任者	補助的な役割を果たす者
タスク P-16 **エンタープライズアーキテクチャ** エンタープライズアーキテクチャ内でのシステムの配置を決定する。	・ミッション又はビジネスオーナー ・エンタープライズアーキテクト ・セキュリティアーキテクト ・プライバシーアーキテクト	・最高情報責任者 ・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者 ・システム所有者 ・情報所有者又は情報管理者
タスク P-17 **要件の割り振り** セキュリティ及びプライバシー要件を、システム及び運用環境に割り振る。	・セキュリティアーキテクト ・プライバシーアーキテクト ・システムセキュリティ責任者 ・システムプライバシー責任者	・最高情報責任者 ・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・ミッション又はビジネスオーナー ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者 ・システム所有者
タスク P-18 **システムの登録** 組織の計画部門又は管理部門にシステムを登録する。	・システム所有者	・ミッション又はビジネスオーナー ・最高情報責任者 ・システムセキュリティ責任者 ・システムプライバシー責任者

表 E-2：分類のタスク、責任、補助的な役割

RMF タスク	主たる責任者	補助的な役割を果たす者
タスク C-1 **システムに関する記述** システムの特徴を文書化する。	システム所有者	・ 認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・ 情報所有者又は情報管理者 ・ システムセキュリティ責任者 ・ システムプライバシー責任者
タスク C-2 **セキュリティ分類化** システムを分類し、セキュリティ分類化の結果を文書化する。	・ システム所有者 ・ 情報所有者又は情報管理者	・ リスクマネジメント担当責任者、又はリスク管理者（機能） ・ 最高情報責任者 ・ 政府機関の情報セキュリティ責任者 ・ 認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・ システムセキュリティ責任者 ・ システムプライバシー責任者
タスク C-3 **セキュリティ分類化のレビュー及び承認** セキュリティ分類化の結果及び決定をレビューし、承認する。	・ 認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・ 政府機関のプライバシー保護責任者 （PII を処理するシステムの場合）	・ リスクマネジメント担当責任者、又はリスク管理者（機能） ・ 最高情報責任者 ・ 政府機関の情報セキュリティ責任者

表 E-3：選択のタスク、責任、補助的な役割

RMF タスク	主たる責任者	補助的な役割を果たす者
タスク S-1 **管理策の選択** システム及び運用環境のための管理策を選択する。	・システム所有者 ・共通管理策の提供者	・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・情報所有者又は情報管理者 ・システムセキュリティエンジニア ・プライバシーエンジニア ・システムセキュリティ責任者 ・システムプライバシー責任者
タスク S-2 **管理策のテーラリング** システム及び運用環境のために選択された管理策をテーラリングする。	・システム所有者 ・共通管理策の提供者	・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・情報所有者又は情報管理者 ・システムセキュリティエンジニア ・プライバシーエンジニア ・システムセキュリティ責任者 ・システムプライバシー責任者
タスク S-3 **管理策の割り振り** セキュリティ及びプライバシー管理策を、システム及び運用環境に割り振る。	・セキュリティアーキテクト ・プライバシーアーキテクト ・システムセキュリティ責任者 ・システムプライバシー責任者	・最高情報責任者 ・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・ミッション又はビジネスオーナー ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者 ・システム所有者
タスク S-4 **計画された管理策の実装の文書化** システム及び運用環境のための管理策を、セキュリティ及びプライバシー計画に文書化する。	・システム所有者 ・共通管理策の提供者	・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・情報所有者又は情報管理者 ・システムセキュリティエンジニア ・プライバシーエンジニア ・システムセキュリティ責任者 ・システムプライバシー責任者
タスク S-5 **継続的監視戦略 – システム** 組織の継続的監視戦略と整合し、かつそれを補完する、管理策の有効性を監視するためのシステムレベルの戦略を策定し、実装する。	・システム所有者 ・共通管理策の提供者	・リスクマネジメント担当責任者、又はリスク管理者（機能） ・最高情報責任者 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者 ・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・情報所有者又は情報管理者 ・セキュリティアーキテクト ・プライバシーアーキテクト ・システムセキュリティエンジニア ・プライバシーエンジニア ・システムセキュリティ責任者 ・システムプライバシー責任者

RMF タスク	主たる責任者	補助的な役割を果たす者
タスク S-6 **計画のレビュー及び承認** システム及び運用環境のセキュリティ及びプライバシー計画をレビューし、承認する。	・ 認可権限のある担当者、又は認可権限のある担当者による指定代理人	・ リスクマネジメント担当責任者、又はリスク管理者（機能） ・ 最高情報責任者 ・ 政府機関の情報セキュリティ責任者 ・ 政府機関のプライバシー保護責任者 ・ 最高取得責任者

表 E-4：実装のタスク、責任、補助的な役割

RMF タスク	主たる責任者	補助的な役割を果たす者
タスク I-1 **管理策の実装** セキュリティ及びプライバシー計画における管理策を実装する。	・システム所有者 ・共通管理策の提供者	・情報所有者又は情報管理者 ・セキュリティアーキテクト ・プライバシーアーキテクト ・システムセキュリティエンジニア ・プライバシーエンジニア ・システムセキュリティ責任者 ・システムプライバシー責任者 ・エンタープライズアーキテクト ・システム管理者
タスク I-2 **管理策の実装情報の更新** 管理策の「実際の実装」状況に基づいて、計画された管理策の実装に対する変更を文書化する。	・システム所有者 ・共通管理策の提供者	・情報所有者又は情報管理者 ・セキュリティアーキテクト ・プライバシーアーキテクト ・システムセキュリティエンジニア ・プライバシーエンジニア ・システムセキュリティ責任者 ・システムプライバシー責任者 ・エンタープライズアーキテクト ・システム管理者

表 E-5:アセスメントのタスク、責任、補助的な役割

RMF タスク	主たる責任者	補助的な役割を果たす者
タスク A-1 **アセッサーの選択** 実施する管理策アセスメントの種類に適したアセッサー又はアセスメントチームを選択する。	・認可権限のある担当者、又は認可権限のある担当者による指定代理人	・最高情報責任者 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者
タスク A-2 **アセスメント計画** 実装された管理策のアセスメントを行うための計画を策定、レビュー、及び承認する。	・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・管理策アセッサー	・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者 ・システム所有者 ・共通管理策の提供者 ・情報所有者又は情報管理者 ・システムセキュリティ責任者 ・システムプライバシー責任者
タスク A-3 **管理策アセスメント** アセスメント計画に記述されたアセスメント手順に従って、管理策のアセスメントを行う。	・管理策アセッサー	・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・システム所有者 ・共通管理策の提供者 ・情報所有者又は情報管理者 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者 ・システムセキュリティ責任者 ・システムプライバシー責任者
タスク A-4 **アセスメント報告書** 管理策アセスメントによって得られた所見及び推奨事項を文書化したアセスメント報告書を準備する。	・管理策アセッサー	・システム所有者 ・共通管理策の提供者 ・システムセキュリティ責任者 ・システムプライバシー責任者
タスク A-5 **改善措置** 管理策に対して初期段階の改善措置を実施し、改善された管理策を再アセスメントする。	・システム所有者 ・共通管理策の提供者 ・管理策アセッサー	・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者 ・リスクマネジメント担当責任者、又はリスク管理者(機能) ・情報所有者又は情報管理者 ・システムセキュリティエンジニア ・プライバシーエンジニア ・システムセキュリティ責任者 ・システムプライバシー責任者

RMF タスク	主たる責任者	補助的な役割を果たす者
タスク A-6 **行動計画及びマイルストーン** アセスメント報告書の所見及び推奨事項に基づいて、行動計画及びマイルストーンを準備する。	・ システム所有者 ・ 共通管理策の提供者	・ 情報所有者又は情報管理者 ・ システムセキュリティ責任者 ・ システムプライバシー責任者 ・ 政府機関の情報セキュリティ責任者 ・ 政府機関のプライバシー保護責任者 ・ 最高取得責任者 ・ 管理策アセッサー

表 E-6：認可のタスク、責任、補助的な役割

RMF タスク	主たる責任者	補助的な役割を果たす者
タスク R-1 **認可パッケージ** 認可パッケージを作成し、認可の決定のために認可権限のある担当者に提出する。	・システム所有者 ・共通管理策の提供者	・システムセキュリティ責任者 ・システムプライバシー責任者 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者 ・管理策アセッサー
タスク R-2 **リスクの分析及び判断** システムの運用又は使用、あるいは共通管理策の提供によるリスクを分析し、判断する。	・認可権限のある担当者、又は認可権限のある担当者による指定代理人	・リスクマネジメント担当責任者、又はリスク管理者（機能） ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者
タスク R-3 **リスク対応** 判断されたリスクへの対応として望ましい行動方針を識別し、実装する。	・認可権限のある担当者、又は認可権限のある担当者による指定代理人	・リスクマネジメント担当責任者、又はリスク管理者（機能） ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者 ・システム所有者、又は共通管理策の提供者 ・情報所有者又は情報管理者 ・システムセキュリティエンジニア ・プライバシーエンジニア ・システムセキュリティ責任者 ・システムプライバシー責任者
タスク R-4 **認可の決定** 情報システムの運用又は使用、あるいは共通管理策の提供又は使用によるリスクが受容可能かどうかを判断する。	・認可権限のある担当者	・リスクマネジメント担当責任者、又はリスク管理者（機能） ・最高情報責任者 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者 ・認可権限のある担当者による指定代理人
タスク R-5 **認可の報告** 認可の決定、及び重大なセキュリティ又はプライバシーリスクを示す管理策の欠陥を報告する。	・認可権限のある担当者、又は認可権限のある担当者による指定代理人	・システム所有者、又は共通管理策の提供者 ・情報所有者又は情報管理者 ・システムセキュリティ責任者 ・システムプライバシー責任者 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者

表 E-7: 監視のタスク、責任、補助的な役割

RMF タスク	主たる責任者	補助的な役割を果たす者
タスク M-1 **システム及び環境に対する変更** 情報システム及びその運用環境の変更を監視し、システムのセキュリティ及びプライバシー態勢に影響を及ぼす変更がないかを確認する。	・システム所有者、又は共通管理策の提供者 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者	・リスクマネジメント担当責任者、又はリスク管理者（機能） ・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・情報所有者又は情報管理者 ・システムセキュリティ責任者 ・システムプライバシー責任者
タスク M-2 **継続的なアセスメント** システム内に実装される管理策及びシステムによって継承される管理策を、継続的監視戦略に従ってアセスメントする。	・管理策アセッサー	・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・システム所有者、又は共通管理策の提供者 ・情報所有者又は情報管理者 ・システムセキュリティ責任者 ・システムプライバシー責任者 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者
タスク M-3 **継続的なリスク対応** 継続的な監視活動及びリスクアセスメントの結果、並びに、行動計画及びマイルストーンの未実施項目に基づいて、リスクに対応する。	・認可権限のある担当者 ・システム所有者 ・共通管理策の提供者	・リスクマネジメント担当責任者、又はリスク管理者（機能） ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者、認可権限のある担当者による指定代理人 ・情報所有者又は情報管理者 ・システムセキュリティ責任者 ・システムプライバシー責任者 ・システムセキュリティエンジニア ・プライバシーエンジニア ・セキュリティアーキテクト ・プライバシーアーキテクト
タスク M-4 **認可パッケージの更新** 継続的監視プロセスの結果に基づいて、計画、アセスメント報告書、並びに、行動計画及びマイルストーンを更新する。	・システム所有者 ・共通管理策の提供者	・情報所有者又は情報管理者 ・システムセキュリティ責任者 ・システムプライバシー責任者 ・政府機関のプライバシー保護責任者 ・政府機関の情報セキュリティ責任者

RMF タスク	主たる責任者	補助的な役割を果たす者
タスク M-5 **セキュリティ及びプライバシーに関する報告** 組織の継続的監視戦略に従い、認可権限のある担当者及び他の組織の担当者に対して、システムのセキュリティ及びプライバシー態勢を継続的に報告する。	・システム所有者 ・共通管理策の提供者 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者	・システムセキュリティ責任者 ・システムプライバシー責任者
タスク M-6 **継続的な認可** システムのセキュリティ及びプライバシー態勢を継続的にレビューし、リスクが依然として受容可能かどうかを判断する。	・認可権限のある担当者	・リスクマネジメント担当責任者、又はリスク管理者（機能） ・最高情報責任者 ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者 ・認可権限のある担当者による指定代理人
タスク M-7 **システムの廃棄** システムの廃棄戦略を実装し、システムを運用から外す際に必要な措置を講ずる。	・システム所有者	・認可権限のある担当者、又は認可権限のある担当者による指定代理人 ・情報所有者又は情報管理者 ・システムセキュリティ責任者 ・システムプライバシー責任者 ・リスクマネジメント担当責任者、又はリスク管理者（機能） ・政府機関の情報セキュリティ責任者 ・政府機関のプライバシー保護責任者

附属書 F

システム及び共通管理策の認可

認可の決定及び裏付けとなる証拠

本附属書では、認可の種類、認可パッケージの内容、認可の決定、認可の決定文書、継続的な認可、再認可、事象駆動型トリガー及び重大な変更、原型認可及び施設認可、及び認可アプローチを含む、システム及び共通管理策の認可プロセスに関する情報を提供する。

認可の種類

認可とは、上級管理職員である*認可権限のある担当者*が、情報システム又はシステムによって継承される共通管理策の現在のセキュリティ及びプライバシー態勢を記述したセキュリティ及びプライバシー情報をレビューするプロセスである。認可権限のある担当者はこの情報を使用して、システム運用又は共通管理策提供のミッション／ビジネスリスクが受容可能であるかどうかを判断し、受容可能であればそのリスクを明示的に受容する。セキュリティ及びプライバシー情報は、自動化されたセキュリティ／プライバシー管理報告ツールからの報告書で構成されることがある認可パッケージで、認可権限のある担当者に提出される [125]。システム及び共通管理策の認可は、RMF *認可*ステップの一部として行われる。システム認可又は共通管理策の認可は、以下に定義される初期の認可、継続的な認可、又は再認可のいずれかとなり得る。

- *初期の認可*は、システム又は共通管理策の完全なゼロベースレビューに基づく初期（起動時）のリスク判断及びリスク受容の決定と定義される。システムのゼロベースレビューには、実装されているすべてのシステムレベル管理策（ハイブリッド管理策のシステムレベル部分を含む）のアセスメントと、セキュリティ及びプライバシー計画で規定されている、継承された共通管理策のセキュリティ状況のレビューが含まれる [126]。共通管理策（システムベースの共通管理策以外）のゼロベースレビューには、1 つの共通管理策又は一連の共通管理策の提供に寄与する適用可能な管理策（例えば、ポリシー、運用手順、実装情報）のアセスメントが含まれる。
- *継続的な認可*は、組織のミッション／ビジネス要件及び組織のリスク許容度に従って、合意及び文書化された頻度で実施される、後続の（その後の）リスク判断及びリスク受容の決定と定義される。継続的な認可は時間駆動型又は事象駆動型の認可プロセスである。認可権限のある担当者には、継続的システム運用又は共通管理策の提供のミッション／ビジネスリスクが受容可能であるかどうかを判断するために、ほぼリアルタイムのセキュリティ及びプライバシー態勢に関する必要な情報が提供される。継続的な認可は、基本的にセキュリティ及びプライバシーリスクの継続的な理解及び継続的な受容に関連しており、強固な継続的監視プログラムに依存している。

[125] [SP 800-137]は、自動化されたセキュリティ管理報告ツールに関する情報を提供している。今後の出版物では、プライバシー管理及び報告ツールについて取り上げる予定である。

[126] システムのゼロベースレビューでは、そのシステムによる継承に利用可能な共通管理策のゼロベースレビューは必要ない。共通管理策は、これらの管理策の提供に関連するリスクを受容する、個別の認可権限のある担当者によって、個別の認可プロセスで認可される。共通管理策を含むセキュリティ及びプライバシー計画のレビューは、組織のシステムによって継承され、システムに関連するリスクベースの意思決定にこの情報を考慮に入れている管理策の現在の状態を理解する上で必要である。

- *再認可*は、初期の認可の後で行われる静的で単一の時点でのリスク判断及びリスク受容の決定と定義される。一般に、再認可活動は時間駆動型又は事象駆動型である。ただし、継続的な認可では、再認可はほとんどの場合、認可権限のある担当者が以前に受容したリスクレベルを超えるセキュリティ及びプライバシーリスクをもたらす事象に対応して、認可権限のある担当者によって開始される、又はリスクマネジメント担当責任者又はリスク管理者（機能）によって指示される事象駆動型の活動である。再認可は、初期の認可で実施されるレビューに類似した、システム又は共通管理策のレビューで構成される。再認可は、システム又は共通管理策の完全なゼロベースレビューを開始するか、再認可をもたらした事象の種類に基づいて対象を絞ったレビューを開始するかを認可権限のある担当者が選択できるため、初期の認可とは異なる。再認可は継続的な認可プロセスとは別個の活動である。しかし、継続的監視プログラムから生成されるセキュリティ及びプライバシー情報は、再認可をサポートするために活用される場合がある。再認可活動では、組織の情報セキュリティ及びプライバシーの継続的監視戦略のレビュー及び変更が必要となる場合があり、結果的にこれが継続的な認可に影響する可能性がある。

認可パッケージ

*認可パッケージ*は、管理策アセスメントの結果の記録を提供し、システム又は共通管理策の運用を認可するかどうかに関するリスクベースの意思決定を行うために必要な情報を、認可権限のある担当者に提供する [127]。システム所有者又は共通管理策の提供者が、認可パッケージの開発、編集、及び提出の責任を負う。これには、自動化されたセキュリティ／プライバシー管理報告ツールで生成された報告書から入手可能な情報が含まれる。システム所有者又は共通管理策の提供者は、認可パッケージの準備中に、多数の情報源（例えば、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、リスクマネジメント担当責任者又はリスク管理者（機能）、管理策アセッサー、システムセキュリティ又はプライバシー責任者、及び継続的監視プログラム）からインプットを受け取る。認可パッケージ [128] には以下が含まれる。

- エグゼクティブサマリ
- セキュリティ及びプライバシー計画 [129] [130]
- セキュリティ及びプライバシーアセスメント報告書 [131]
- 行動計画及びマイルストーン

[127] システムベースではない共通管理策の認可パッケージには、セキュリティ又はプライバシー計画が含まれていない場合があるが、共通管理策の実装詳細の記録が含まれている。

[128] 認可権限のある担当者は、認可パッケージに必要となる可能性のある追加の補足情報、成果物、又は参考文献を決定する。追加の文書には、リスクアセスメント、緊急時対応計画、又は SCRM 計画が含まれる場合がある。

[129] [SP 800-18]は、システムセキュリティ計画のガイダンスを提供している。プライバシー計画のガイダンスは、プライバシー計画に特化した、計画されている出版物で取り上げる予定である。

[130] [OMB A-130]に従い、情報システムセキュリティ計画及びプライバシー計画を統合して 1 つの総合文書にしてもよい。

[131] [SP 800-53A]は、セキュリティアセスメント報告書のガイダンスを提供している。プライバシーアセスメント報告書のガイダンスについては、今後の出版物で扱われる予定である。

エグゼクティブサマリは、認可パッケージのセキュリティ及びプライバシー情報の概要を提供する。エグゼクティブサマリでは、情報システム及びシステムが運用される環境の保護に関連するリスクマネジメントの問題を識別し、強調する。エグゼクティブサマリは、組織の業務及び資産、個人、他の組織、及び国家に対するセキュリティ及びプライバシーリスクを理解するために認可権限のある担当者に必要とされる極めて重要な情報を提供する。エグゼクティブサマリの情報は、認可権限のある担当者が、システムの運用及び使用、又は組織のシステムによって継承される共通管理策の提供に関して、情報に基づいたリスクベースの意思決定を行うために使用できる。

セキュリティ及びプライバシー計画は、セキュリティ及びプライバシー要件の概要を提供し、これらの要件を満たすために導入されている管理策又は予定されている管理策を記述する[132]。これらの計画は、システム内に実装されている管理策の意図する実装又は実際の実装を理解するための十分な情報を提供し、継承された共通管理策を介して実装された管理策を示す。さらに、プライバシー計画では、管理策のアセスメントに使用される方法論及び測定基準を記述する。セキュリティ及びプライバシー計画には、附属書又は参考文献として、プライバシー影響アセスメント、相互接続に関するセキュリティ合意書、セキュリティ及びプライバシー構成、緊急時対応計画、構成管理計画、サプライチェーンのリスクマネジメント計画、インシデント対応計画、及びシステムレベルの継続的監視戦略などの追加文書を含めてもよい。セキュリティ及びプライバシー計画は、システム内に実装された管理策又はシステムが継承した管理策に対する変更を決定づける事象が発生するたびに更新される。

セキュリティ及びプライバシーアセスメント報告書は、管理策アセッサーによって準備されるか、又は自動化されたセキュリティ／プライバシー管理報告ツールによって生成され、セキュリティ及びプライバシー要件を満たすことに関して管理策が正しく実装され、意図したとおりに運用され、望ましい成果がどの程度生み出されているかを判断するための、セキュリティ及びプライバシー計画で識別された管理策の実装のアセスメントの所見及び結果を提供する。アセスメント報告書には、管理策で識別された欠陥に対し推奨される是正処置が含まれる場合がある[133]。認可権限のある担当者はこの報告書をレビューし、適切なリスク対応を決定する[タスク R-3]。

認可プロセスにおけるほぼリアルタイムのリスクマネジメントの目的をサポートするため、システム内に実装された管理策又はシステムが継承した管理策に対する変更が行われるたびに、アセスメント報告書は継続的に更新される[134]。アセスメント報告書の更新により、システム所有者、共通管理策の提供者、及び認可権限のある担当者は、管理策の有効性に対する認識を確実に維持する。管理策の有効性は、システムのセキュリティ及びプライバシー態勢、及びリスクの明示的な受容に関する意思決定に直接影響を与える。

[132] 情報システムセキュリティ計画及びプライバシー計画は、1 つの総合文書に統合してもよい。

[133] エグゼクティブサマリは、アセスメントの主要部分、所見の概要、並びにセキュリティ及びプライバシー管理策の欠陥に対処するための推奨事項に焦点をあてた、セキュリティ及びプライバシーアセスメント報告書の要約版を認可権限のある担当者に提供する。

[134] リスクマネジメントに関する決定を容易にするためにアセスメント所見の継続的な追跡及び対応の望ましい成果が、（使用する特定のプロセスよりも）重視されるため、組織は、組織の内部プロセスと整合しているあらゆる形式又は手法を使用して、セキュリティアセスメント報告書の情報を管理及び更新できる。

行動計画及びマイルストーンには、アセスメント中に識別された管理策の欠陥を修正し、既知の脆弱性又はセキュリティ及びプライバシーリスクに対処するために計画された措置を記述する[135]。行動計画及びマイルストーンの内容と構造は、リスク管理者（機能）の一部として策定されたリスクマネジメント戦略から情報が提供され、連邦法、大統領令、ポリシー、指令、又は標準で定められた要件を含む、組織により確立された行動計画及びマイルストーンのプロセスと整合している。システム及びシステムが運用される環境に、利用可能なリソースが現実的に対処できるよりも多くの脆弱性がある場合、組織は、組織全体にわたって一貫性のある、優先順位付けされたリスク軽減アプローチを促進する行動計画及びマイルストーンを策定及び実装する。優先順位付けされた一貫性のあるリスク軽減アプローチは、行動計画及びマイルストーンが以下基づいていることを確実にする。

- システムのセキュリティ分類化及び、セキュリティ、プライバシー、及びサプライチェーンのリスクアセスメント
- 管理策の具体的な欠陥
- 管理策の欠陥の重大性（すなわち、それらの欠陥が、システムのセキュリティ及びプライバシー態勢並びに組織のリスクレベルに及ぼす可能性がある直接的又は間接的な影響）[136]
- 管理策で識別された欠陥に対処するための組織のリスク軽減アプローチ
- 管理策の特定の欠陥を受容する根拠

行動計画及びマイルストーンに関する組織の戦略は、リスク軽減活動の影響を受けるシステムのセキュリティ分類化によって導かれ、情報が提供される。例えば、組織は、最初に、リスク軽減のリソースを影響が最も大きいシステムに割り振ることを決定する場合がある。影響が最も大きいシステムの既知の欠陥の是正ができないと、組織のミッション又はビジネスファンクションに最も重大な悪影響が及ぶ可能性があるからである。組織は、リスクアセスメントから得られる情報、及びリスク管理者（機能）の一部として策定されるリスクマネジメント戦略から得られる情報を利用して、欠陥に優先順位を付ける。したがって、影響が大きいシステムには、そのシステムの欠陥の優先順位付けされたリストがあり、影響が中程度のシステム及び影響が小さいシステムについても同様である。

認可の決定

認可の決定は認可パッケージの内容に基づいて行われる。認可権限のある担当者が行うことができる認可の決定は 4 種類ある。

- 運用認可
- 共通管理策の認可
- 使用認可
- 認可の拒否

[135] 行動計画及びマイルストーンの軽減措置の結果として変更が行われた場合、システムセキュリティ計画はこの変更に基づいて更新される。

[136] 一般にリスクレベルとは、組織の業務及び資産、個人、他の組織、又は国家に対する潜在的な悪影響によって組織が脅かされる度合いを示す。

運用認可

認可権限のある担当者が認可パッケージのレビュー後に、組織の業務、組織の資産、個人、他の組織、又は国家に対するリスクが受容可能であると判断した場合、情報システムに対して*運用認可*が発行される。そのシステムは、認可権限のある担当者が設定した条件に基づいて、指定された期間運用することが認可される。*認可の満了日*は、認可権限のある担当者によって認可の条件として設定される。認可の満了日は、システムのセキュリティ及びプライバシー態勢に関する懸念の高まりを反映するために、認可権限のある担当者がいつでも調整できる。例えば、認可権限のある担当者は、すべての管理策を完全に導入する前に運用環境でのシステムのテストが必要な場合に、短期間に限りシステムの運用を認可してもよい（すなわち、運用認可は、テストの目的を達成するために必要な期間に限定される）[137]。認可権限のある担当者は、論理アクセス及び物理アクセスを最小限のユーザ数に限定する、システム使用期間を制限する、拡張又は強化された監査ロギング、スキャン、及び監視を採用する、又は本番環境テストに必要な機能のみにシステム機能を限定する、などの運用制限を含めることを選択してもよい。システムが本番環境でテストする準備ができている場合には管理策の多くが既に導入されているはずであるため、認可権限のある担当者は、完全実装又は部分的に実装されている管理策のアセスメントの結果を考慮する。システムが継続的な認可を受けている場合、時間駆動型の認可の頻度が規定される。さらに、運用認可のレビューの必要性をもたらす有害な事象が発生する可能性がある[138]。

共通管理策の認可

*共通管理策の認可*は、システムの運用認可に類似している。認可権限のある担当者が共通管理策の提供者から提出された認可パッケージをレビューした後に、組織の業務、組織の資産、個人、他の組織、又は国家に対するリスクが受容可能であると判断した場合、共通管理策の認可が発行される。組織が選択した共通管理策の実装、アセスメント、及び認可が完了していること、及び組織のシステムによる継承が可能であることを示すのは、共通管理策の提供者の責任である。また、共通管理策の提供者は、管理策を継承するシステム所有者が適切な文書及びツールにアクセスできるようにする責任も担う。

共通管理策は、認可権限のある担当者及び組織が定めた諸条件に従って、特定期間だけ認可される。*認可の満了日*は、初期の共通管理策の認可の条件つとして、認可権限のある担当者によって設定される。この満了日は、継承可能な共通管理策のセキュリティ及びプライバシー態勢に関する懸念の度合いを反映するために、認可権限のある担当者がいつでも調整できる。管理策が継続的な認可を受けている場合は、時間駆動型の認可の頻度が規定される。どの種類の認可でも、有害な事象が発生すると、共通管理策の認可のレビューの必要性をもたらす可能性がある。システムに実装された共通管理策の場合、これらの管理策はシステムの運用認可の一部として認可を受けるため、個別の共通管理策の認可は必要ない[139]。

[137] 以前は、テストのための暫定的な認可と呼ばれていた。

[138] 事象駆動型のトリガーに関する追加情報については後述する。

[139] 特定の状況では、システム所有者は、共通管理策として公式に指定されていない可能性がある他の組織のシステムから管理策を継承することを選択してもよい。承認された共通管理策の提供者以外から管理策を継承するシステム所有者は、このような管理策を提供するシステムが、有効な運用認可を持つことを確実にする。また、管理策を継承するシステムの認可権限のある担当者にも、この継承が知らされる。

使用認可

*使用認可*は、ある組織（以下、顧客組織と呼ぶ）が、連邦政府組織（プロバイダ組織と呼ぶ）によって運用が認可された情報システムに対して、別の組織（連邦政府又は連邦政府以外）によって作成された既存の認可パッケージの情報を受け入れることを選択した場合に採用される [140]。使用認可は、異なる認可権限のある担当者の権限の下でシステムの相互利益を促進するメカニズムである。使用認可は、運用認可の代わりに、顧客組織の認可権限のある担当者によって発行される。使用認可を発行する職員は、運用認可又は共通管理策の認可を発行する認可権限のある担当者と同等の、リスクマネジメントに対する責任及び権限を有する。[141]

プロバイダ組織からの認可パッケージの情報の受け入れは、互恵契約の一種であり、共有システム、サービス、又はアプリケーションを使用する必要性に基づいている。顧客組織は、別の連邦組織（すなわち、プロバイダ組織）から有効な運用認可が発行された後にのみ、使用認可を発行できる [142]。プロバイダ組織による運用認可は、提供されるシステム、サービス、又はアプリケーションのリスク受容のステートメント（表明）である。顧客組織による使用認可は、顧客の情報に関して、システム、サービス、又はアプリケーションを使用する際のリスク受容のステートメントである。使用認可は、大幅なコスト削減の機会を提供し、コスト及び時間がかかる可能性がある顧客組織による認可プロセスを回避する。

使用認可では、リスクを判断するための基本的な根拠として、プロバイダ組織からの認可パッケージを顧客組織がレビューする必要がある [143]。顧客組織は認可パッケージをレビューする際、認可結果が作成されてからの経過時間、運用環境（認可パッケージに反映されている環境と異なる場合）、処理、保存、又は伝送される情報のインパクトレベル、及び顧客組織の全体的なリスク許容度などの様々なリスク要因を考慮する。顧客組織が共有システム、アプリケーション、又はサービスを 1 つ以上のシステムと統合することを計画している場合には、顧客組織は、そうすることのリスクを考慮する。

---

[140] *プロバイダ組織*という用語は、共有システム、サービス、又はアプリケーションを提供及び／又は認可パッケージを所有及び維持する（すなわち、共有システム、サービス、又はアプリケーションの運用認可を付与されている）連邦政府機関又は下部組織を指す。 認可パッケージを所有する組織が、例えば、共有システム、サービス、又はアプリケーションが外部プロバイダから提供される状況では、共有システム、サービス、又はアプリケーションを所有していない場合がある。

[141] クラウド又は共有システム、サービス、又はアプリケーションを提供する組織による管理策の選択及びベースラインのテーラリング措置に関連するリスクベースの意思決定では、このようなクラウド又は共有システム、サービス、又はアプリケーションを使用する可能性がある顧客組織の保護ニーズを考慮することが望ましい。したがって、クラウド又は共有システム、サービス、又はアプリケーションをホストする組織は、これらのタイプの環境における運用の共有リスクを考慮することが望ましい。

[142] 連邦政府によるリスク及び認可の管理プログラム（FedRAMP）の一部として一般調達局（GSA）によって発行される暫定的な（運用）認可は、クラウドベースのシステム、サービス、又はアプリケーションの使用認可の発行を希望する顧客組織にとって、有効な運用認可と見なされる。

[143] 認可パッケージ（セキュリティ及びプライバシー計画、セキュリティ及びプライバシーアセスメント報告書、行動計画及びマイルストーン、認可の決定文書を含む）の共有は、すべての当事者（すなわち、顧客組織及びサービスプロバイダ組織）により合意された条件に基づいて行われる。

顧客組織は、プロバイダ認可パッケージの情報が不十分である、又は受容可能なリスクレベルを設定する上で不十分な管理策が導入されていると判断した場合、顧客組織はプロバイダ組織と交渉し、追加の管理策又はセキュリティ、プライバシー、又はサプライチェーン情報を要求してもよい。追加の管理策の要求には、例えば、リスク削減のための管理策の補完、代替管理策の実装、追加又はより厳格なアセスメントの実施、又は、提供されるシステム、アプリケーション、又はサービスの使用に関する制約の確立が含まれる可能性がある。追加情報の要求には、例えば認可パッケージに反映されていないシステムの使用時にプロバイダ組織が作成又は発見した情報が含まれる可能性がある。プロバイダ組織が要求された管理策を提供しない場合、顧客組織はリスクを受容可能なレベルに軽減するための追加の管理策を実装することを選択してもよい。追加の管理策は、顧客組織が責任を負うその他のすべての管理策とともに、文書化、実装、アセスメント、認可、及び監視される。

顧客組織は、共有又はクラウドシステム、アプリケーション、又はサービスのセキュリティ及びプライバシー態勢に満足し（現在の認可パッケージに反映されている）、共有又はクラウドシステム、アプリケーション、又はサービスを使用するリスクが十分に軽減されたら、共有システム、サービス、又はアプリケーションを使用することで発生するセキュリティ又はプライバシーリスクを顧客組織が明確に理解し、受容する使用認可を発行する[144]。最終的には、顧客組織は、顧客組織の業務及び資産、個人、他の組織、又は国家に対してインパクトを与える可能性のあるリスクに対する責任と説明責任を負う。

使用認可では満了日は不要であるが、顧客組織が共有又はクラウドシステム、アプリケーション、又はサービスを使用する上でのセキュリティ及びプライバシーリスクを引き続き受容し、プロバイダ組織によって発行された運用認可が、連邦政府及び組織のポリシーにより定められている要件を満たしている場合は、使用認可は有効であり続ける。プロバイダ組織が実施する監視活動からの情報が継続的に共有されるようにすること、及び、プロバイダのセキュリティ及びプライバシー態勢に影響を与える可能性があるシステム、アプリケーション、又はサービスに重大な変更が発生した場合に、プロバイダ組織が顧客組織に通知することを確実にすることは、顧客組織の義務である。必要であれば、使用認可の決定の際に、顧客組織が使用するプロバイダ組織のシステム、サービス、又はアプリケーションのセキュリティ及びプライバシー態勢をレビューするための時間駆動型又は事象駆動型のトリガーを規定してもよい。顧客組織の情報を侵害する、又は顧客組織の情報に悪影響を及ぼす重大な事象が発生した場合、プロバイダ組織は顧客組織に通知する[145]。

[144] [FISMA] に従い、各政府機関の長は、政府機関によって、又は政府機関の代理として収集又は保守される情報、及び政府機関又は政府機関の請負業者によって使用又は運用される情報システムの不正アクセス、不正利用、漏えい、破壊、改ざん、又は破棄により生じるリスクに見合った情報セキュリティの保護を提供する責任を負う。[OMB A-130] には、セキュリティ及びプライバシーリスクの受容に関する組織の責任が記載されている。

[145] 顧客組織は、提供されるシステムに関するセキュリティ態勢の情報が適切に共有されるようにするため、プロバイダ組織との合意／合意事項の覚書、契約、又はその他の種類の合意を作成してもよい。

図 F-1 は、組織のシステム及び共通管理策に適用できる認可の決定の種類と、認可プロセスにおけるリスクマネジメントの役割を示している。

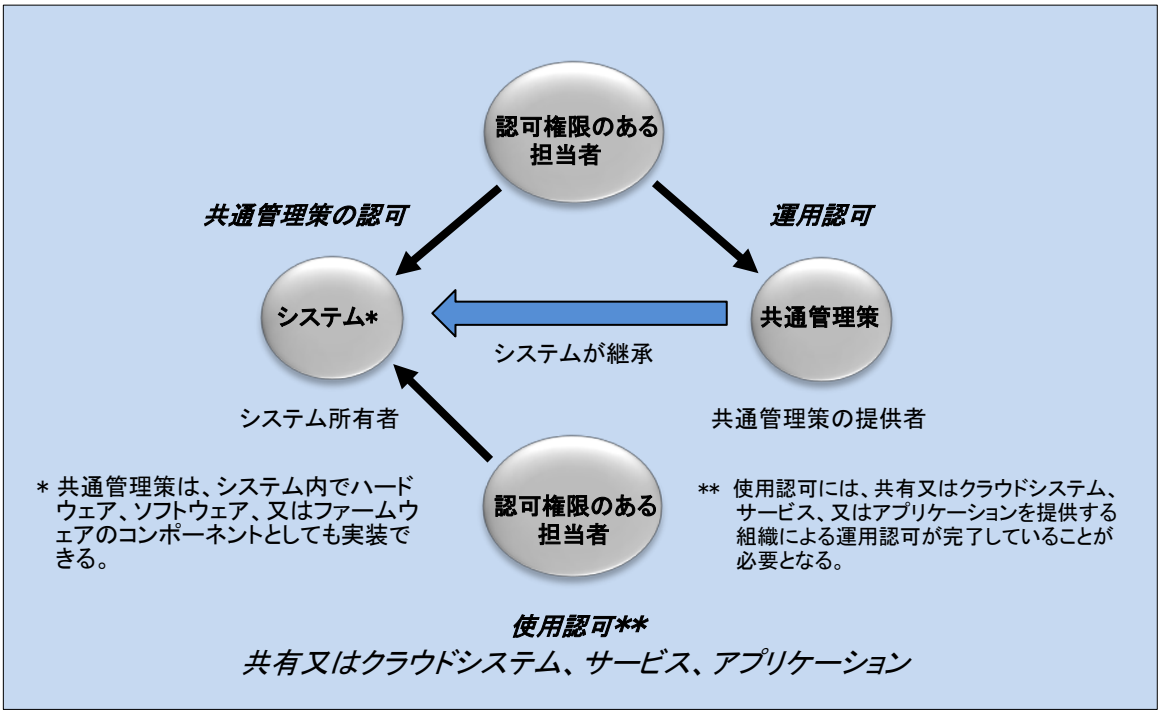

図 F-1：認可の決定の種類

認可の拒否

認可権限のある担当者が、リスクマネジメント担当責任者又はリスク管理者（機能）から提供されたすべてのインプットを含む認可パッケージをレビューした後に、組織の業務、資産、個人、他の組織、及び国家に対するリスクが受容できない、及びリスクを受容可能なレベルに軽減するための措置を直ちに講じることができないと判断した場合には、認可は付与されない。*認可の拒否*とは、情報システムの運用が認可されず、運用開始されないこと、共通管理策をシステムに提供することが認可されないこと、又はプロバイダのシステムが顧客組織による使用を認可されないことを意味する。システムが現在運用中である場合、すべての活動が停止される。認可を受けられないということは、管理策に重大な欠陥があることを意味する。

認可権限のある担当者又は指定代理人は、システム所有者又は共通管理策の提供者と協力して行動計画及びマイルストーンを見直し、欠陥を是正するための対策が確実に実施されるようにする。認可の拒否の特殊なケースとして、*認可の撤回*がある。

認可権限のある担当者は、連邦政府又は組織のポリシー、指令、規制、標準、ガイダンスに対する違反、又は認可の諸条件に対する違反がある場合に、以前に下した認可の決定を撤回できる。例えば、有効な継続的監視プログラムが維持されていないことが、認可の決定の撤回の根拠となり得る。

認可の決定情報

認可の決定は認可権限のある担当者からシステム所有者、共通管理策の提供者、及びその他の主要な組織の担当者に伝送される。認可の決定には以下の情報が含まれる。

- 認可の決定
- 認可の諸条件
- 時間駆動型の認可の頻度又は認可の満了日
- 認可の決定のレビューをもたらす可能性がある事象（存在する場合）
- 共通管理策の場合、これらの管理策でサポートされる[FIPS 199]インパクトレベル

認可の決定は、システムの運用又は使用が認可されているかどうか、又は共通管理策がシステム所有者に提供されること及び組織システムに継承されることが認可されているかどうかを示す。認可の諸条件は、システム所有者が従わなければならない、システムの運用に課されたあらゆる制限事項又は制約事項、又はその代わりとして、共通管理策の提供者が従わなければならない、共通管理策の実装に課された制限事項又は制約事項を提供する。システム又は共通管理策が継続的な認可を受けていない場合、認可権限のある担当者が設定した認可の満了日は、認可が失効し、再認可が必要となる時期を示す。認可の決定文書は元の認可パッケージとともにシステム所有者又は共通管理策の提供者に送られる[146]。

認可の決定及び認可パッケージを受領すると、システム所有者及び共通管理策の提供者は認可の諸条件を承認し、実装し、順守する。システム所有者及び共通管理策の提供者は、認可の決定と認可パッケージを保持する[147]。組織は、要求があった場合に、組織の担当者が認可文書を確実に利用できるようにする。システムの脆弱性、プライバシーリスク、管理策の欠陥に関する機密情報を含む認可パッケージの内容は、連邦政府及び組織の記録保持ポリシーに従ってマーク付けされ、保護される。認可の決定情報は、組織の記録保管ポリシーに従って保持される。認可権限のある担当者は、認可の一部として設定された諸条件が、システム所有者又は共通管理策の提供者によって順守されていることを継続的に検証する。

[146] 認可の決定文書は真正性を確実にするためにデジタル署名にしてもよい。

[147] 組織は、認可プロセスに関連する成果物を含めるために、リスクマネジメント情報の作成、配布、及びアーカイブをサポートする自動化ツールを採用することを選択してもよい。

使用認可の決定

使用認可は運用認可の簡略版であり、以下のものが含まれる。

- リスク受容のステートメント
- プロバイダ組織の共有クラウド又はシステム、アプリケーション、又はサービス（存在する場合）のセキュリティ及びプライバシー態勢のレビューするための時間駆動型又は事象駆動型トリガー

使用認可は、運用認可の代わりに顧客組織の認可権限のある担当者が発行する。この認可権限のある担当者は、運用認可又は共通管理策の認可を発行する認可権限のある担当者と同等のレベルのリスクマネジメントの責任及び権限を有する。リスク受容のステートメントは、共有又はクラウドシステム、サービス、又はアプリケーションによる、又はこれらを介して処理、保存、又は伝送される顧客組織の情報に関して、共有システム、サービス、又はアプリケーションの使用から生じるセキュリティ及びプライバシーリスクを明示的に受容することを示すものである。

継続的な認可

継続的監視戦略[148]は、効果的かつ効率的なリスクマネジメントを継続的に促進する。リスクマネジメントは、システム及びその運用環境に対する変更及び管理策の継続的な監視するための自動化ツール及び実践的ツール、技法、手順を使用することで、*ほぼリアルタイム*に実施することができる。認可権限のある担当者のニーズに基づいた継続的監視は、システムのセキュリティ及びプライバシー態勢[149]を判断するために必要な情報を生成し、組織の業務及び資産、個人、他の組織、及び国家に対するリスクが明らかにする。最終的に、継続的な監視は、システムの継続的運用又は組織のシステムが継承した共通管理策の継続的使用を認可するかどうかという認可権限のある担当者の決定を導き、情報を提供する。

継続的監視は、認可権限のある担当者が、継続的リスク判断に基づいて継続的運用が受容できるかどうかを判断するため、及び受容できない場合には、増加するリスクに効果的に対応するために RMF のどのステップを再考する必要があるかを判断するために、システムの現在のセキュリティ及びプライバシー態勢に関する十分な知識を維持している*継続的な認可*の状態を達成するのに役立つ。継続的監視プログラムが、システム又はその運用環境に対する変更により生じるリスクの管理に必要な情報を認可権限のある担当者に提供している状況では、再認可は不要である。再認可が必要な場合、組織は、継続的監視プロセス中に作成されたシステムのセキュリティ及びプライバシー態勢に関する状況報告書及び関連情報を最大限に活用して、効率化を図る。

システム又は共通管理策が継続的な認可を受けている場合、システム又は共通管理策は、継続的監視プログラムにより生成されたセキュリティ及びプライバシー情報を活用して、時間駆動型及び／又は事象駆動型で認可される場合がある。システム及び共通管理策は、組織レベル及びシステムレベルの継続的監視戦略の一部として定められた認可の頻度に従って、時間駆動型で認可される。システム及び共通管理策は、組織が定めたトリガー事象が発生するまで、事象駆動型で認可される。認可が時間駆動型又は事象駆動型のいずれであっても、認可権限のある担当者は、特定されたリスクの継続的な受容を承認する。組織は、認可権限のある担当者によるこのような承認に必要な手続きレベルを決定する。

---

[148] [SP 800-137] は、情報セキュリティの継続的監視の追加ガイダンスを提供している。プライバシーの継続的監視のガイダンスについては、今後の出版物で提供される予定である。

[149] 効率性を高めるため、情報セキュリティの継続的監視（ISCM）及びプライバシーの継続的監視（PCM）戦略を 1 つの統一された継続的監視戦略に統合してもよい。同様に、ISCM 及び PCM プログラムを 1 つの統一された継続的監視プログラムに統合してもよい。

継続的な認可の実装の条件

RMF が組織全体に効果的に適用され、組織が堅牢な継続的監視プログラムを実装している場合、システムは静的な特定時点での認可プロセスから、動的なほぼリアルタイムでの継続的な認可プロセスへ移行してもよい。そのためには、以下の条件を満たさなければならない。

- 継続的な認可の対象として検討されるシステム又は共通管理策が、システム又は共通管理策の完全なゼロベースレビューに基づいて初期の認可を受けている[150]。
- 組織の継続的監視戦略及び NIST の標準及びガイドラインに従って、組織により規定された適切な厳密さ及び必要な頻度で、実装された管理策を監視する組織の継続的監視プログラムが実施されている[151]。

組織は、この 2 つの条件が満たされていること、及びシステム又は共通管理策を継続的な認可へ移行することを規定するプロセスを確立し実装する。このプロセスには、認可権限のある担当者が、システム又は共通管理策が現在、継続的な認可プロセスによって管理されていることを承認し、そのプロセスに関連するすべての活動の実施の責任を受け入れることが含まれる。継続的な認可への移行は、認可権限のある担当者が新たな認可の決定を発行することによって文書化される[152]。継続的監視プロセスを通じて生成されたセキュリティ及びプライバシー情報は、セキュリティ及びプライバシー管理報告ツールによって認可権限のある担当者及び他の組織の担当者にタイムリーに提供される。このようなツールは、システム及び共通管理策の継続的な認可に関するリスクベースの意思決定を容易にする。

情報の生成、収集、及び独立性に関する要件

継続的な認可をサポートするため、管理策のセキュリティ及びプライバシー情報は、組織の継続的監視戦略で規定された頻度で生成及び収集される。セキュリティ及びプライバシー情報は、管理策の種類及び目的、並びにアセスメントに求められる厳格さに基づき、自動化ツール又はその他のアセスメント手法を使用して収集してもよい。自動化ツールは、認可権限のある担当者によるリスク判断をサポートするのに十分なセキュリティ及びプライバシー情報を生成しない場合がある。自動化ツールは、様々な理由（例えば、ツールがすべての管理策又は管理策のすべての部分の情報を生成しない、追加のアシュアランスが必要である、ツールが特定の技術又はプラットフォームに関する情報は生成しない）で、十分なサポートを提供しない場合がある。このような場合には、セキュリティ及びプライバシー情報の自動生成におけるギャップを埋めるため、組織が決めた頻度で手動での管理策アセスメントが実施される。手動生成されたアセスメント結果は、組織が適切と判断した方法で、認可権限のある担当者に提供される。

[150] システム所有者及び認可権限のある担当者は、共通管理策の提供者によって実施されたアセスメントから継承された共通管理策に関するセキュリティ及びプライバシー情報を活用する。

[151] [SP 800-53] 及び [SP 800-53A] は、セキュリティアセスメント及び監視の適切な厳格さに関するガイダンスを提供している。今後の出版物では、プライバシーアセスメントについて取り上げる予定である。

[152] 継続的な認可へ移行する前に、組織は認可の満了日を含む認可の決定文書を持っている。新たな認可の決定文書を要求することによって、システム又は共通管理策が現在、継続的な認可のもとにあるために、これらの管理策は初期の認可文書に規定されている満了日に拘束されないことが明確にされる。

中インパクトシステム及び高インパクトシステムの継続的な認可をサポートするため、認可権限のある担当者に提供されるセキュリティ及びプライバシー情報は、手動生成か自動生成かに依らず、組織によって確立された独立性の要件を満たすエンティティによって作成及び分析される。政府機関のプライバシー保護責任者は、プライバシー管理策のアセスメント及び認可権限のある担当者へのプライバシー情報の提供の責任を負う。組織の判断で、プライバシー管理策は独立したアセッサーによってアセスメントされる場合がある。独立したアセッサーは、監視対象の組織のシステム及び共通管理策の開発、実装、アセスメント、運用、又は管理に関して、公平であり、認識された利害の衝突又は実際の利害の衝突がない。

継続的な認可の頻度

[SP 800-53]セキュリティ管理策 CA-6、Part c は、システム及びシステムによって継承されるすべての管理策の認可が、組織が定めた頻度で更新されることを規定している。この管理策のこの部分は、継続的な認可の概念を強化している。CA-6 に(継続的監視戦略の一部として定められたセキュリティ及びプライバシーアセスメント及び監視の頻度の判断と共に)従い、組織は、認可権限のある担当者がセキュリティ又はプライバシー管理報告ツール又は手動プロセスを使用してセキュリティ及びプライバシー情報をレビューする頻度を決定する [153]。報告ツール又は手動プロセスからのほぼリアルタイムの情報は、システム運用又は共通管理策提供に伴うミッション又はビジネスリスクが引き続き受容可能であるかどうかを判断するために使用される。[SP 800-137]は、アセスメント及び監視の頻度の判断の基準を提供している。

継続的な認可では、*時間駆動型*の認可トリガーとは、認可権限のある担当者が、前述したようにセキュリティ及びプライバシー情報をレビューし、システム(又は共通管理策)の継続的運用を認可することを組織が判断する頻度を指す。時間駆動型の認可トリガーは、システムのインパクトレベルなど、組織が定めた様々な要因に基づくことができる。時間駆動型のトリガーが発生すると、認可権限のある担当者は、継続的な組織のミッション又はビジネスリスクを判断し、組織のリスク許容度に基づいてこのようなリスクが受容可能であるかどうか、及び継続的運用の承認が正当であるかどうかを判断するために、自身が責任及び説明責任を負うシステムのセキュリティ及びプライバシー情報をレビューする。組織のセキュリティ及びプライバシー管理報告ツールによってサポートされる継続的監視プロセスは、継続的な認可をサポートするためセキュリティ及びプライバシー情報をレビューする時期が来たことを責任及び説明責任を負う認可権限のある担当者に通知するための適切な機能を提供する。

[153] *継続的な認可*と*継続的アセスメント*は異なる概念であるが密接に関連している。組織は(リスクを継続的に理解して受容することにつながる)継続的な認可アプローチを採用するために、実装されている管理策を継続的にアセスメントする組織レベル及びシステムレベルの継続的監視プロセスを導入しなければならない。継続的監視プロセスの所見及び結果は、ほぼリアルタイムのリスクベースの意思決定をサポートする情報を認可権限のある担当者に提供する。

時間駆動型の認可トリガーとは対照的に、*事象駆動型*トリガーでは、認可権限のある担当者によるセキュリティ及びプライバシー情報の即時レビューが必要となる。組織は、継続的な認可及び再認可に対して事象駆動型*トリガー*(すなわち、組織が事前に定められた方法で対応するよう促す指標又はきっかけ)を定義してもよい。継続的な認可で事象駆動型トリガーが発生すると、認可権限のある担当者は、政府職員(例えば、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、システム所有者、共通管理策の提供者、システムセキュリティ又はプライバシー責任者)又は自動化ツールから、システム又は共通管理策の即時レビューを必要とする定義されたトリガー事象が発生したという通知を受ける。認可権限のある担当者は、即時レビューが必要であると自主的に判断してもよい。事象駆動型トリガーのレビューは、組織の継続的監視戦略で定義された時間駆動型の頻度のレビューに加えて実施され、残留リスクが組織のリスク許容度の受容可能な範囲内にある場合に、継続的な認可中に発生する[154]。

静的認可から継続的な認可への移行

継続的監視の目的は、自動化された手段又は手動による手段を問わず、効果的なリスクベースの意思決定を行うために必要な情報を認可権限のある担当者に提供するのに十分な頻度で、管理策を監視することである[155]。しかし、監視のかなりの部分が自動化によって達成されない場合、現在の静的認可アプローチから効果的かつ効率的な継続的な認可アプローチへ移行することは、実現可能でも実用的でもないであろう。自動化ツールが使用可能になり、より多くの数の管理策が自動化された手段で監視されるようになるにつれて、セキュリティ及びプライバシー情報を生成するための段階的なアプローチが移行中に必要となる可能性がある。組織は、自動化ツールからセキュリティ及びプライバシー情報を生成することから始め、手動アセスメントから追加情報を生成することでギャップを埋めてもよい。自動監視機能が追加されると、プロセスを調整することができる。

静的認可プロセスから動的な継続的な認可プロセスへの移行には、かなりの検討及び計画が必要となる。組織が検討してもよい方法論の 1 つは、システムのセキュリティ分類化に基づいて、移行に段階的アプローチをとることである。低インパクトシステムのリスク許容度は、中インパクトシステム又は高インパクトシステムよりも大きい可能性が高いため、最初に低インパクトシステムに継続的監視及び継続的な認可を実装すると、移行が容易になる可能性がある。低インパクトシステムから開始する段階的アプローチによって、組織は、中インパクトシステム及び高インパクトシステムに継続的監視及び継続的な認可プロセスを実装する際に、学んだ教訓を取り入れることができる。学んだ教訓を取り入れることで、継続的監視及び継続的な認可の実装を、組織内のシステムへのインパクトレベルが最も低いものからインパクトレベルが最も高いものまで、一貫して進めることが容易となる。組織は、システムをサブシステム又はシステム要素に分割し、その後、システム全体の完全な移行の準備ができる(その時点で、認可権限のある担当者はシステムが継続的な認可プロセスにより管理されていることを認める)まで、これらのサブシステム又はシステム要素を継続的な認可に 1 セグメントずつ移行するという段階的実装アプローチを採用することを検討してもよい。

[154] 特定のトリガー事象によって開始される即時レビューは、組織が確立した監視頻度及びレビューが組織内でどのように構成されているかに基づいて、時間駆動型の監視活動と同時に(すなわち、連動して)発生する場合がある。効率化を図るために、事象駆動型のレビューと時間駆動型のレビューに同じ報告構造を使用してもよい。

[155] プライバシーの継続的監視とは、プライバシーリスクの継続的認識を維持し、適用されるプライバシー要件に確実に準拠し、プライバシーリスクを管理するために十分な頻度でプライバシー管理策をアセスメントすることを意味する。

再認可

再認可措置は、連邦政府又は組織のポリシーに従って、認可権限のある担当者の判断で行われる [156]。再認可措置が必要な場合、組織は、現在有効な継続的監視プロセスの一環として作成されたセキュリティ及びプライバシーリスク情報を最大限に利用する。再認可措置が開始された場合、時間駆動型又は事象駆動型のいずれかとなる。時間駆動型の再認可は、認可の満了日（規定されている場合）を迎えた時点で発生する。システムが継続的な認可を受けている場合 [157]、時間駆動型の再認可は必要ない場合がある。しかし、継続的監視プログラムが継続的な認可を十分にサポートするほど十分に包括的でない場合、認可権限のある担当者が最大認可期間を規定することができる。認可の満了日は、連邦政府及び組織のポリシー、並びに認可権限のある担当者の要件によって導かれ、情報が提供される。

継続的な認可においては、組織の受容可能なリスク許容度を超えたリスクをもたらす事象が発生した場合、再認可が必要となる場合がある。例えば、継続的監視プログラムの侵害／インシデント、又は不備、又は重大な問題がある場合には、再認可の正当な理由となる可能性がある。再認可措置では、継続的監視戦略のレビュー及び変更が必要となる場合があり、これが継続的な認可に影響を与える可能性がある。

再認可に関連するセキュリティ及びプライバシーアセスメントでは、組織は継続的監視プログラムにより生成されたセキュリティ及びプライバシー情報を活用して、手動アセスメントによってギャップを埋める。組織は、より高いレベルのアシュアランスが必要な状況で、自動生成されたアセスメント情報を、手動で生成された情報で補完してもよい。セキュリティ管理策アセスメントが、必要な独立性を有する適格なアセッサーによって実施され、適切なセキュリティ標準及びガイドラインを使用しており、認可権限のある担当者のニーズに基づいている場合には、アセスメント結果を再認可に適用することができる [158]。

政府機関のプライバシー保護責任者は、プライバシー管理策のアセスメントの責任を負い、これらのアセスメントの結果は累積的に再認可に適用できる。独立したアセッサーは、組織の判断でプライバシー管理策をアセスメントしてもよい。、政府機関のプライバシー保護責任者は、認可権限のある担当者が再認可に関する決定を下す前に、個人情報（PII）を処理する情報システムの認可パッケージをレビュー及び承認する。再認可措置は、特定の問題又は継続的な問題のみに焦点をあてたセキュリティ及びプライバシー計画、セキュリティ及びプライバシーアセスメント報告書、及び行動計画及びマイルストーンの更新と同程度に単純なものとなるか、又は初期の認可と同程度に包括的なものとなる可能性がある。

[156] 正式な再認可の開始の決定には、政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、及びリスクマネジメント担当責任者／リスク管理者（機能）からのインプットが含まれる。

[157] 継続的な認可アプローチでは、継続的監視戦略で規定された頻度で、実装されているすべてのセキュリティ管理策を監視する継続的監視プログラムが導入されている必要がある。

[158] [SP 800-53A] には、認可活動をサポートするためにセキュリティ情報を再利用できる場合の具体的な条件が説明されている。

認可権限のある担当者は、現時点でのリスク判断と、組織の業務及び資産、個人、他の組織、及び国家に対するリスクの受容に基づいて更新された認可の決定文書に署名する。システム又は組織のシステムによって継承される共通管理策の再認可が決定されるすべての状況において、再認可作業にかかる時間とコストを最小限に抑えるため、（組織の再利用ポリシーに基づき）認可情報を最大限に再利用することが推奨される。

事象駆動型トリガー及び重大な変更

組織は、継続的な認可及び再認可の両方に対して事象駆動型*トリガー*（すなわち、組織が事前に定められた方法で対応するよう促す指標又はきっかけ）を定義する。事象駆動型トリガーには以下が含まれるが、これらに限定されない。

- 新たな脅威、脆弱性、プライバシーリスク、又はインパクト情報
- 継続的監視プログラムからの所見及び欠陥の数の増加
- 新しいミッション／ビジネスの要件
- 認可権限のある担当者の変更
- リスクアセスメントの所見における重大な変更
- システム、共通管理策、又は運用環境の重大な変更
- 運用システムのセキュリティ又はプライバシーリスクに影響を与えるサプライチェーンの変更
- 組織のしきい値の超過

認可権限のある担当者に変更があった場合、新任の認可権限のある担当者は、現在の認可の決定文書、認可パッケージ、継続的監視活動から更新されたすべての文書、又は自動化されたセキュリティ／プライバシー管理報告ツールからの報告書をレビューする。新任の認可権限のある担当者が、現在のリスクは受容可能であると判断した場合、その担当者は新たな認可の決定文書又は更新された認可の決定文書に署名し、システム及び共通管理策の責任及び責任説明が正式に移譲される。そうすることで、新任の認可権限のある担当者は、組織の業務及び資産、個人、他の組織、及び国家に対するリスクを明示的に受容することになる。新任の認可権限のある担当者が現在のリスクを受容できないと判断した場合、認可活動（すなわち、継続的な認可又は再認可）を開始することができる。あるいは、新任の認可権限のある担当者は、元の認可を継続するための新しい諸条件を設定してもよいが、元の認可の満了日を延長することはできない（継続的な認可を受けていない場合）。

重大な変更は、システムのセキュリティ又はプライバシー態勢に大きく影響を与える可能性がある変更と定義される。事象駆動型の認可活動をもたらす可能性があるシステムに対する重大な変更には、以下のものが含まれるが、これらに限定されない。

- 新規又はアップグレードされたオペレーティングシステム、ミドルウェアコンポーネント、又はアプリケーションのインストール
- システムのポート、プロトコル、又はサービスの変更
- 新規又はアップグレードされたハードウェアプラットフォームのインストール
- PII を含む情報の処理方法の変更
- 暗号モジュール又はサービスの変更
- システムによって処理、保存、又は伝送される情報の種類の変更

- セキュリティ及びプライバシー管理策の変更

事象駆動型の認可活動をもたらす可能性がある運用環境に対する重大な変更には、以下のものが含まれるが、これらに限定されない。

- 新しい施設への移転
- 新しい中核的なミッション又はビジネスファンクションの追加
- 組織が脅威源の標的にされているという具体的で信頼できる脅威情報の取得
- 新規又は改正された法律、指令、ポリシー又は規制の制定

上記の変更の例は、システムのセキュリティ及びプライバシー態勢に影響を及ぼす可能性がある変更を表している場合にのみ、重大な変更となる。組織は、様々な要因（ミッション及びビジネスのニーズ、脅威及び脆弱性の情報、システム運用環境、プライバシーリスク、セキュリティ分類化など）に基づいて、何が重大な変更であるかの基準を確立する。

リスクアセスメントの結果又はインパクト分析の結果は、システム又は共通管理策の変更が重大な変更であり、認可活動をもたらすかどうかを決定するために使用される場合がある。認可活動が開始された場合、組織は変更の影響を受ける特定の管理策のみをその対象とし、可能な限り、以前のアセスメント結果を再利用する。効果的な監視プログラムは、認可活動の全体的なコスト及び労力のレベルを大幅に削減することができる。システム又はその運用環境に対する変更のほとんどは、継続的監視プログラム及び継続的な認可によって対処することができる。

原型認可及び施設認可

原型認可 [159] は、システムの原型（すなわち、共通）バージョンに対して、単一の認可パッケージの策定を許可する正式な認可の決定である。これには、例えば、特定の運用環境（例えば、特定の場所でホスト組織によって提供されるシステムのインストール及び構成の要件、又は運用セキュリティ及びプライバシーのニーズ）で使用するために複数の場所に展開されるハードウェア、ソフトウェア、又はファームウェアのコンポーネントが含まれる。原型認可は、定められた環境にシステムが展開され、かつシステムが、同一のシステムアーキテクチャのインスタンス、ソフトウェア、同一の情報の種類、機能的に同一のハードウェア、同一の方法で処理される情報、同一の管理策実装、又は同一の構成の、同一のインスタンスで構成される場合に適切である。原型認可は、認可されたサイト固有の管理策 [160] 又は以下で説明する施設認可と組み合わせて使用される。原型認可は、システム開発に責任を負う認可権限のある担当者によって発行され [161]、運用認可を表す。システムが展開されているサイト又は施設では、サイト又は施設のシステムの責任を負う認可権限のある担当者が、システム展開のリスクを受容し、使用認可を発行する。使用認可は、原型システムの認可パッケージ及び施設の共通管理策の情報を活用する。

[159] 原型認可の例には、複数の場所に展開される標準的な金融システムのハードウェア及びソフトウェアアプリケーションに対する認可、又は組織内のすべての業務ユニットに展開される共通のワークステーション又は運用環境（すなわち、ハードウェア、オペレーティングシステム、及びアプリケーション）に対する認可が含まれる。

[160] サイト固有の管理策は、通常、組織によって*共通管理策*として実装される。例えば、物理的及び環境的保護管理策や職員のセキュリティ管理策が含まれる。

[161] 一般に、原型認可は、顧客向けの標準化されたハードウェア及びソフトウェアのケイパビリティ（能力）の開発の責任を負う組織によって発行され、受領側の組織に「すぐに利用可能な（turn key）」ソリューションとして供給される。このような認可を発行する上級幹部は、開発側の認可権限のある担当者と呼ばれることがある。

*施設認可*は、定義された運用環境内に存在する 1 つ以上のシステムをサポートするために、その運用環境に実装される特定の管理策に焦点をあてた正式な認可の決定である。施設認可は、施設内の共通管理策を扱っており、定義された環境内に存在するシステムが共通管理策を継承し、影響を受けるシステムのセキュリティ及びプライバシー計画で施設の認可パッケージを参照できるようにする。共通管理策は、特定のシステムを特定施設内に配置することが適切かどうかについてのリスク判断を容易にするために、規定されたインパクトレベルで提供される[162]。物理的管理策及び環境的管理策は施設認可で扱われるが、その他の管理策、例えば、施設の境界保護、施設の緊急時対応計画及びインシデント対応計画、又は施設職員のトレーニング及び意識向上並びに職員審査、も含まれる可能性がある。施設の認可権限のある担当者は、施設内に存在するシステムが継承できる共通管理策を記述するために、共通管理策の認可を発行する。

従来型認可及び共同認可

組織は、認可を計画及び実施する際に、2 種類のアプローチのいずれかを選択できる。これには、*単独の*認可権限のある担当者による認可と*複数の*認可権限のある担当者による認可が含まれる[163]。最初のアプローチは、本附属書で定義されている従来型認可プロセスであり、上級幹部の地位にある単独の組織の担当者が、システム又は共通管理策の責任及び説明責任を負う。この組織の担当者は、組織の業務、組織の資産、個人、他の組織、又は国家に有害なインパクトをもたらす可能性があるセキュリティ及びプライバシーリスクを受容する。

2 番目のアプローチである*共同認可*は、同一組織又は複数組織に属する複数の組織の担当者が、システム認可に対し共通の利害を有している場合に採用される。これらの組織の担当者はシステムに対し共同で責任及び説明責任を負い、組織の業務及び資産、個人、他の組織、及び国家有害なインパクトをもたらす可能性があるセキュリティ及びプライバシーリスクを共同で受容する。認可権限のある担当者が複数追加されるという本質的な違いはあるが、単独の認可権限のある担当者のアプローチと類似の認可プロセスに従う。共同認可アプローチを選択する組織には、RMF のタスクの計画と実施に共同で取り組み、タスクの実装における合意事項と進捗状況を文書化することが期待される。

共同認可を成功させるためには、セキュリティ分類化、管理策の選択及びテーラリング、有効性を判断するための管理策アセスメント計画、行動計画及びマイルストーン、及びシステムレベルの継続的監視戦略における協力が必要である。共同認可の諸条件は、継続的なリスク判断及び受容のプロセスを含む、共同認可の参加関係者によって定められる。共同認可は、認可権限のある担当者の間で合意が得られており、かつこの認可が連邦政府又は組織のポリシーが確立した特定の要件を満たしている場合にのみ有効である。[SP 800-53] の管理策 CA-6(1)の「*共同認可 - 組織内*」(*Joint Authorization – Same Organization*)及び CA-6(2)「*共同認可 - 組織間*」(*Joint Authorization – Different Organizations*)に、共同認可の要件が説明されている。

[162] 例えば、施設が中インパクトとして分類される場合、高インパクトシステム又はシステム要素をその運用環境に配置することが適切ではない場合がある。

[163] 認可アプローチは、システム及び組織のシステムによって継承される共通管理策に適用することができる。

附属書 G

認可境界に関する考慮事項

複雑なシステム、アプリケーション、及び変化する技術の影響

本附属書では、複雑なシステム及びソフトウェアアプリケーションの認可境界を決定するための追加の考慮事項を提供する。また、組織が情報リソースのために外部プロバイダを利用する場合の、認可境界に関するガイダンスも含まれている。第 3 章で説明した基本的な RMF のステップ及びタスクは、 組織がセキュリティ及びプライバシーリスクを管理し、、第 1 章で論じた法律、大統領令、及び OMB ポリシーを順守できるようにするために、3 つのシナリオすべてに適用できる。

複雑なシステムの認可境界

複雑なシステムの認可境界の決定は、組織にとって大きな課題を提示する可能性がある。複雑なシステムは、個々のサブシステムの集合と見なすことができる。サブシステムは、1 つ以上の特定の機能を果たすシステム要素で構成される、システムの主要な下位区分である。図 G-1 は、複雑なシステムの概念を示している。

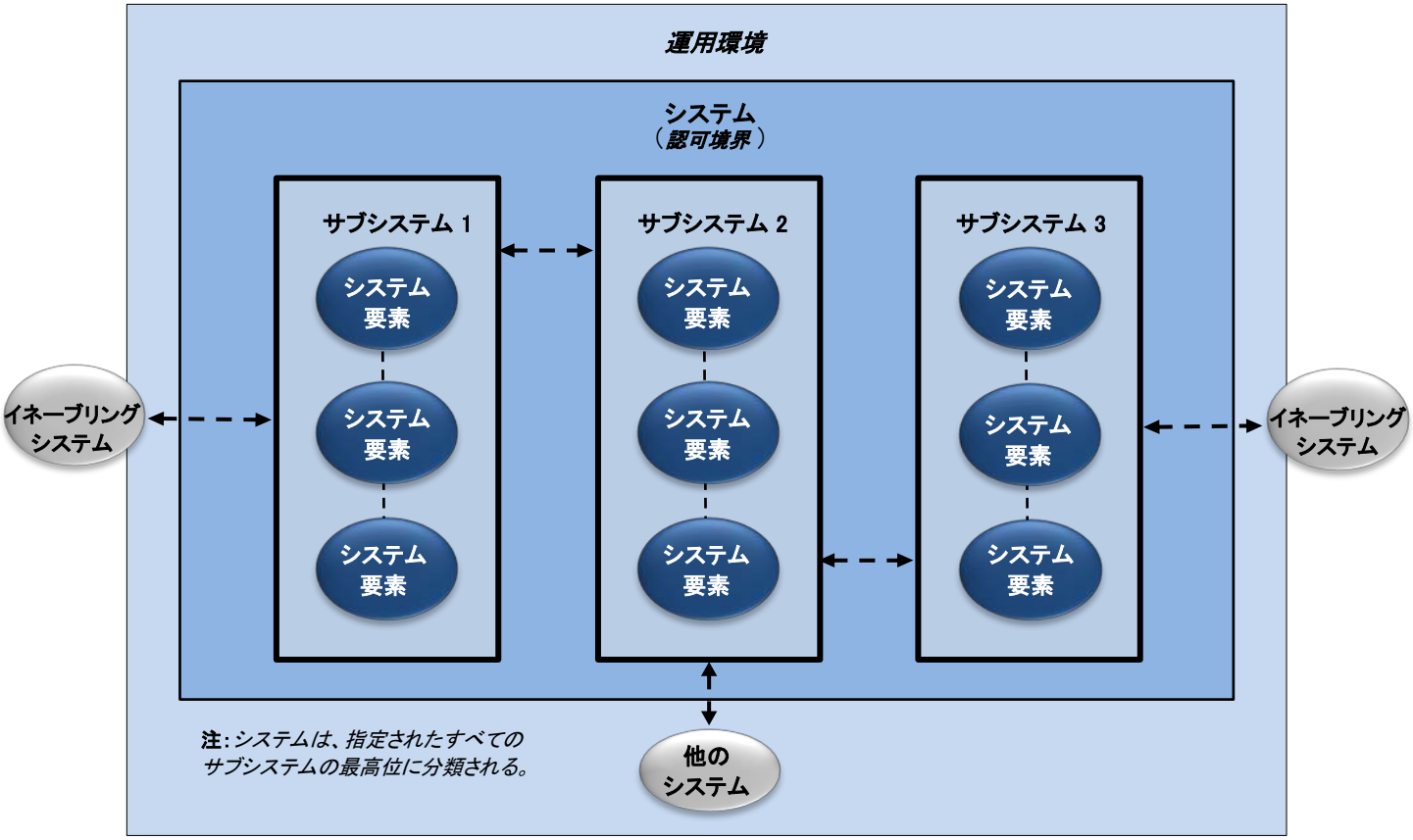

図 G-1：複雑なシステムの概念図

組織は、複雑なシステムを一連の管理可能なシステム要素に分割するために、又は類似のミッションをサポートするが別々に識別されるほど明らかに異なる要素を識別するために、サブシステムの概念を用いることができる。各サブシステムは（認可境界とは異なる）独自の境界を持ち、すべてのサブシステムを含む包括的な認可境界内で定義することができる。

例えば、組織は、効果的なリスクマネジメント及びリソースマネジメントという 2 つの目的を達成するために、同じ直接的なマネジメント管理策の下にある複数のシステム、あるいは、類似のミッション又はビジネスファンクションを持つ複数のシステムを 1 つのシステムにまとめることが有益だと判断する場合がある。また、組織は、一連の共通のミッション又はビジネスファンクションをサポートする（広範囲の地理的領域に分散した）複数の独立したシステムで構成されるシステムを開発する場合もある。同様に、システムは、システムの管理、及びリスクベースの意思決定（例えば、分類の決定、テーラリングの決定、管理策の割り振りの決定）を容易にするため及びサポートするために、複数のサブシステムに分割することができる。

システムをサブシステムに分割する（すなわち、分割統治する）ことによって、適切なセキュリティ、個人のプライバシーの保護、及び費用対効果の高いリスクマネジメントプロセスを実現するための、的を絞った管理策の適用が容易になる。また、複雑なシステムを複数のサブシステムに分割することは、ドメイン分離及びネットワークセグメンテーションという重要なセキュリティ概念もサポートする。これは、高価値資産を扱う場合に重要となる可能性がある。システムがサブシステムに分割される場合、組織は、サブシステムごとにセキュリティ及びプライバシー計画を策定するか、又は、同じセキュリティ及びプライバシー計画でシステムとサブシステムに対処するかを選択してもよい。

情報セキュリティアーキテクチャ及びプライバシーアーキテクチャは、複雑なシステムをサブシステムに分割するプロセスで重要な役割を果たす。これには、サブシステム間の内部境界における通信の監視及び制御、並びに、構成要素であるサブシステムのセキュリティ及びプライバシー要件を満たす又は上回る管理策の選択、割り振り、及び実施が含まれる。管理策の選択及び割り振りの一つアプローチは、識別された各サブシステムを個別に分類することである（タスク C-2 を参照）。しかし、各サブシステムを個別に分類しても、システム全体の分類は変わらない。むしろ、各サブシステムを個別に分類することで、システム全体により影響の大きい管理策を展開する代わりに、サブシステムが[SP 800-53]から個別の、より的を絞った管理策の割り振りを受けることが可能になる（タスク P-17 及びタスク S-3 を参照）。別のアプローチとして、システム内の小さなサブシステムを、より大きなサブシステムにまとめ、統合されたサブシステムをそれぞれ分類し、必要に応じてサブシステムに管理策を割り振る。複雑なシステム内のサブシステムは、完結したシステムとして存在する場合もあるが、通常は相互に依存及び接続しているため、独立したエンティティとして扱われないことが多い。

識別されたサブシステムのセキュリティ分類が異なる場合（例えば、低インパクトと高インパクト）、組織は、サブシステムのインタフェース [164]、情報フロー、並びに、サブシステム間でのセキュリティ及びプライバシーの依存関係を調査し、潜在的な脆弱性を排除又は削減するために、サブシステムの相互接続に適切な管理策を選択する。

[164] サブシステム間のインタフェースの種類及び結合の種類は、複雑なシステムに不注意による脆弱性をもたらす可能性がある。例えば、大規模な組織のイントラネットが、より小規模のサブシステム（例えば、LAN セグメントなどの切り離しが可能なシステム）に分解され、その後個別に分類された場合、システムレベルの特定の保護が、当該システムの他の部分に対して十分に強力でない管理策が誤って選択及び実装されることによって、イントラネットに対する攻撃ベクトルを曝露してしまう可能性がある。このような状況を回避するために、組織は、サブシステム間のインタフェースを慎重に調査し、この分野の潜在的な脆弱性を排除するための適切な措置を講じることによって、情報システムが適切に保護されることを確実にする。

これは、システムが適切に保護されることを確実にする。サブシステムの相互接続に関する管理策は、サブシステムが異なるセキュリティ及びプライバシーポリシーを実装している場合、又は、異なる機関によって管理されている場合にも採用される。選択した管理策がどの程度正しく実装され、意図した通りに運用し、複雑なシステムのセキュリティ及びプライバシー要件を満たすことに関して望ましい成果を生み出しているかについては、システムレベルの管理策アセスメントをまとめ、インタフェースの問題に対処するための考慮事項を追加することによって判断できる。複合的なアプローチは、セキュリティ分類に従ってアセスメントの労力のレベルを増減し、システムレベルのアセスメント結果の再利用を可能にすることで、的を絞った、費用対効果の高いリスクマネジメントプロセスを促進する。

ソフトウェアアプリケーションの認可境界

認可境界には、ハードウェア、ファームウェア、及びソフトウェアを含むすべてのシステム要素が含まれる。ソフトウェア要素には、アプリケーション（例えば、データベースアプリケーション、カスタマイズされたビジネスアプリケーション、Web アプリケーション）、ミドルウェア、及びオペレーティングシステムが含まれる。ソフトウェア要素は、ソフトウェアがホストされている情報システムの一部として、又は、ホスティングシステムから管理策を継承するアプリケーションのみからなるシステム又はサブシステムの一部として、認可境界に含まれる。ソフトウェアアプリケーションは、ホスティングシステムから提供されるリソースに依存する場合があるため、ホストされているアプリケーションに基本レベルの保護を提供するのを支援するために、ホスティングシステムから提供される管理策を活用できる。アプリケーションレベルの追加の管理策は、必要に応じて各ソフトウェアアプリケーションによって提供される。アプリケーション所有者は、セキュリティ及びプライバシー要件がアプリケーションとホスティングシステムの間で確実に満たされるようにするために、システム所有者と協調する。システム所有者とアプリケーション所有者との協調には、例えば、アプリケーションの管理策の選択、実装、アセスメント、及び監視に関する検討、アプリケーションへの変更がシステム及び組織のセキュリティ及びプライバシー態勢に及ぼす影響、及びシステムへの変更がホストされているアプリケーションに及ぼす影響が含まれる。

認可境界と外部プロバイダ

外部システム及び外部サービスプロバイダの概念は新しいものではないが、それらの現在の普及及び利用頻度は、組織に重大で新たな課題を提示する可能性がある。システム要素、サブシステム、又はシステム全体が、その運用を認可する組織の直接管理の範囲外にある場合がある。そのような外部システムの性質は、連邦政府情報の処理、保存、及び伝送に外部クラウドコンピューティングサービスを採用している組織から、何らかの外部エンティティによって開発されたアプリケーション又はサービスを自らの管理下のプラットフォームでホストできるようにしている組織まで、様々である可能性がある[165]。

連邦政府情報セキュリティ近代化法（FISMA：Federal Information Security Modernization Act）及び行政管理予算局（OMB：Office of Management and Budget）のポリシーでは、連邦政府情報を処理、保存、又は伝送する外部プロバイダ、又は、連邦政府の代理として情報システムを運用する外部プロバイダに対して、連邦政府機関と同じセキュリティ及びプライバシー要件を満たすよう求めている。連邦政府のセキュリティ及びプライバシー要件は、連邦政府情報を保存、処理、又は伝送する外部システム、及び外部システムによって提供される、又は外部システムに関連するあらゆるサービスにも適用される。さらに、外部プロバイダを利用することによるリスクが受容可能なレベルであるというアシュアランス又は確信は、組織がプロバイダに置く信頼に依存する。

[165] 一般調達局（GSA：General Services Administration）が運営する、連邦政府によるリスク及び認可の管理プログラム（FedRAMP：Federal Risk and Authorization Management Program）は、クラウドの認可境界の決定に関するガイダンスを提供している。

場合によっては、信頼のレベルは、連邦政府情報を保護する、及び個人のプライバシーを保護するために必要な管理策の採用に関して、組織がプロバイダに及ぼすことのできる直接的な管理の量に基づいている。

信頼のレベルは、これらの管理策の有効性に関して、外部プロバイダ又は独立したアセッサーによって提出された証拠に基づく場合もある。他の例では、組織が外部プロバイダと以前に経験したこと、及び、プロバイダが正しい行動をとっているという組織の確信など、他の要因に基づく場合がある。外部プロバイダとの信頼のレベルを複雑にする要因には、様々なものがある。

- 外部プロバイダが所有するものと、組織が所有するものの区分けが、はっきりしない場合がある（例えば、外部プロバイダによって開発されたアプリケーション、ソフトウェアモジュール、又はファームウェアを、組織が所有するプラットフォームで実行している場合）。
- 組織が外部プロバイダに対して持つ管理の度合いは、極めて限られている場合がある。
- システム、サブシステム、サービス、又はアプリケーションの性質及び内容は、急速に変化する可能性がある。
- システム、サブシステム、サービス、又はアプリケーションは、極めて重要な性質を持っているため、組織のシステムに迅速に組み込む必要がある場合がある。

上記の要因の結果として、システム、サブシステム、アプリケーション、又はサービスが正しく機能することの検証及び妥当性確認、並びに、実装された管理策の有効性の検証及び妥当性確認を行うために組織が使用する従来の手法（例えば、明確に定義された要件、設計分析、導入前のテスト及び評価、管理策のアセスメント、及び継続的監視）の一部が実行不可能になる可能性がある。その結果、組織は、連邦政府情報を処理、保存、又は伝送するシステム又はサブシステムの使用認可あるいは運用認可を発行するかどうかを判断する根拠として、外部プロバイダとの信頼関係の性質に依存することに委ねる可能性がある（例えば、承認済みプロバイダを記載した GSA のリストの使用）。あるいは、組織は、組織が判断した情報交換リスクが受容可能である場合にのみ、外部から提供されたシステム又はサービスの利用を許可する可能性がある。

最終的に、外部プロバイダの信頼のレベルが十分なアシュアランスを提供しない場合、組織は、代替管理策を採用するか、より大きなリスクを受容するか、より統合的信頼性が高い外部プロバイダと契約するか、又はサービスを取得しない（すなわち、機能性のレベルを下げた、又はまったく機能性を持たない可能性のある状態でミッション及びビジネスの業務を遂行する）。

外部プロバイダによる管理策及びアセスメントの活用

組織は、外部プロバイダによる管理策及びアセスメント結果を活用しようとする際は、注意を払うことが望ましい。外部プロバイダによって実装される管理策は、提供される範囲、対象、及びケイパビリティの点で、[SP 800-53] の管理策と異なる場合がある。NIST は、そのカタログにある管理策と、[ISO 27001] のセキュリティ管理策とのマッピング、並びに [ISO 15408-2] 及び [ISO 15408-3] のセキュリティ要件とのマッピングを提供している。しかし、このようなマッピングは本質的に主観的なものであり、外部プロバイダによって対応される管理策及び要件が組織の保護ニーズを満たすかどうかを判断するために組織が慎重にレビューすることが望ましい。また、異なる標準又はガイドライン間のマッピングも、各出版物の範囲及び目的が異なる可能性に対処していない。

外部プロバイダによる、セキュリティ及びプライバシーのアセスメント結果を使用又は活用しようとする場合にも、同様の注意を払うことが望ましい。アセスメントの種類、厳格さ、及び範囲はプロバイダによって大きく異なる可能性がある。さらに、プロバイダが採用するアセスメント手順、及び、アセスメントを行うアセッサーの独立性は、組織がアセスメント結果を活用する前にレビュー及び検討することが望ましい極めて重要な問題である。

認可権限のある担当者による効果的なリスク判断は、外部プロバイダによって選択及び実装される管理策の透明性、並びに、それらのプロバイダによって作成されるアセスメント証拠の質及び有効性に依存する。透明性は、組織の資産を適切に保護するために必要なアシュアランスを得るために不可欠である。

附属書 H

システムライフサイクルに関する考慮事項

RMF の実行に影響を与える他の要因

運用中のシステム、開発中のシステム、及び、修正又はアップグレードが行われているシステムを含むすべてのシステムは、SDLC のいずれかの段階にある[166]。要件の定義は SDLC プロセスの重要な部分であり、*開始*段階で開始する[167]。セキュリティ及びプライバシー要件は、システムに割り振られる機能的及び非機能的[168]な要件の一部である。セキュリティ及びプライバシー要件は、他の要件と同時に SDLC に組み込まれる。セキュリティ及びプライバシー要件が早期に統合されなかった場合、初期の設計に含めることができたはずのセキュリティ及びプライバシーの懸念事項に対処するために、組織がライフサイクルの後半で多額の費用を負担する可能性がある。セキュリティ及びプライバシー要件が SDLC の初期の段階で定義され、他のシステム要件と統合されている場合、結果として生じるシステムには欠陥が少なくなり、したがって、将来悪用される可能性のあるプライバシーリスク又はセキュリティ脆弱性が少なくなる。

セキュリティ及びプライバシー要件を SDLC に統合することは、組織の保護戦略を確実に実施するための最も効果的、効率的、及び費用対効果が高い手段である。また、セキュリティ及びプライバシープロセスが、進行中のミッション及びビジネスファンクションをサポートするシステムを開発、実装、運用、及び保守するために組織が利用する他のプロセスから分離されていないことを確実にする。SDLC にセキュリティ及びプライバシー要件を組み込むことに加え、要件は、組織のプログラム、計画、及び予算編成活動にも統合され、必要な時にリソースが利用でき、プログラム及びプロジェクトのマイルストーンが完了するようにするのに役立てる。エンタープライズアーキテクチャは、組織内のこのような統合に関する一元化された記録を提供する。

システム開発ライフサイクルにおけるリスクマネジメント

リスクマネジメント活動は SDLC の初期に開始し、ライフサイクルを通じで継続する。これらの活動は、システムにおけるセキュリティ及びプライバシーのケイパビリティ（能力）の形成を支援すること、必要な管理策が実装され、セキュリティ及びプライバシーリスクが継続的に適切に対処されていることを確実にすること、認可権限のある担当者が、組織の運営、組織の資産、個人、他の組織、及び国家へのリスクを受容するために、現在のシステムのセキュリティ及びプライバシー態勢を確実に理解することにおいて重要である。

セキュリティ及びプライバシー要件を SDLC に確実に統合することは、組織の運営、組織の資産、個人、他の組織、及び国家に対するセキュリティ及びプライバシーリスク（サプライチェーンリスクを含む）を低減するための、よりレジリエントなシステムの開発及び実装を容易にするのに役立つ。

[166] SDLC には、開始、開発及び取得、実装、運用及び保守、廃棄という 5 つの段階がある。[SP 800-64] は、SDLC に関するガイダンスを提供している。

[167] 組織は様々な開発プロセス（ウォーターフォール、スパイラル、アジャイルなど）を採用する場合がある。

[168] 非機能的な要件には、例えば、品質及びアシュアランスに関する要件が含まれる。

これは、統合されたプロジェクトチーム [169] の概念を用いることで達成することができる。連邦政府職員は、SDLC 活動にセキュリティ及びプライバシーの専門家を確実に参加させる。このようなチームの統合により、システムの設計、開発、実装、アセスメント、運用、保守、及び廃棄に責任を負う人員と、セキュリティ及びプライバシーリスクを十分に軽減して組織のミッション及びビジネスファンクションを保護する上で必要な管理策について上級幹部に助言を与えるセキュリティ及びプライバシー専門家との間の協力レベルの向上が促進される。

最後に、組織は、SDLC プロセス中に生成されたセキュリティ及びプライバシー関連の情報を最大限に利用して、他のセキュリティ及びプライバシーに関する目的に必要な類似の情報に対する要件を満たす。セキュリティ及びプライバシー情報の再利用は、作業の重複及び文書化の重複を減らし、相互利益を促進し、セキュリティ及びプライバシー活動が SDLC プロセスから独立して実施される場合の不要なコストを回避する、効果的な手段である。再利用は、セキュリティ及びプライバシーの考慮事項を含む、システムの開発、実装、アセスメント、運用、保守、及び廃棄における情報の一貫性を促進する。

[169] 統合されたプロジェクトチームとは、組織の要件を満たすシステムの開発を容易にするために、幅広い技能及び役割を持つ複数の個人によって構成される、分野横断的なエンティティである。

アーキテクチャ及びエンジニアリングの重要性

セキュリティアーキテクト、プライバシーアーキテクト、システムセキュリティエンジニア及びプライバシーエンジニアは、SDLC 及び RMF の実行の成功において極めて重要な役割を果たすことができる。セキュリティアーキテクト及びプライバシーアーキテクト、並びにセキュリティエンジニア及びプライバシーエンジニアは、情報システムにおける管理策の選択及び実装に関する技術的な助言を*システム所有者*及び*認可権限のある担当者*に提供し、事業体全体のリスクベースの意思決定を導き、情報を提供する。

セキュリティアーキテクト及びプライバシーアーキテクト:

- ミッション及びビジネスプロセスを保護するのに必要なセキュリティ及びプライバシー要件が、リファレンスモデル、セグメントアーキテクチャ及びソリューションアーキテクチャ並びにミッション及びビジネスプロセスをサポートするシステムを含むエンタープライズアーキテクチャのあらゆる側面において、適切に対処されていることを確実にする。
- エンタープライズアーキテクトと、システムセキュリティエンジニア及びプライバシーエンジニアの間の主たる連絡窓口となる。
- 管理策の割り振りに関して、システム所有者、共通管理策の提供者、システムセキュリティ及びプライバシー責任者と調整する。
- セキュリティ及びプライバシーに関する様々な問題について、認可権限のある担当者、最高情報責任者、リスクマネジメント担当責任者／リスク管理者（機能）、政府機関の情報セキュリティ責任者、及び、政府機関のプライバシー保護責任者に助言する。

セキュリティエンジニア及びプライバシーエンジニア:

- 意図的なセキュリティ又はプライバシーの体系化、設計、開発及び構成を通じて、セキュリティ及びプライバシー要件がシステム及びシステム要素に統合されることを確実にする。
- システムに管理策を実装する際に、ベストプラクティスを採用する。これには、ソフトウェアエンジニアリングの方法論の利用、システムセキュリティエンジニアリング又はプライバシーエンジニアリングの原則の利用、セキュアな、又はプライバシーを強化する設計、アーキテクチャ、あるいはコーディング技法の利用、が含まれる。
- 政府機関の情報セキュリティ責任者、政府機関のプライバシー保護責任者、システム所有者、共通管理策の提供者、セキュリティアーキテクト及びプライバシーアーキテクト、システムセキュリティ又はプライバシー責任者とともに、セキュリティ及びプライバシー活動を調整する。