NIST Special Publication 800-37
Revision 1

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

連邦政府情報システムに対するリスクマネジメントフレームワーク適用ガイド

セキュリティライフサイクルによるアプローチ

JOINT TASK FORCE

情報セキュリティ

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

2010 年 2 月

米国商務省　長官
Gary Locke

米国国立標準技術研究所　所長
Patrick D. Gallagher

コンピュータシステムの技術に関する報告書

米国国立標準技術研究所（NIST: National Institute of Standards and Technology、以下、NISTと称す）の情報技術ラボラトリ（ITL: Information Technology Laboratory）は、国家の測定および標準に関する基盤において技術的リーダーシップを提供することにより、米国の経済と公共福祉に貢献している。情報技術ラボラトリは、テストテスト技法の開発、参照データの作成、実装によるコンセプト実証、技術的分析を通じて、情報技術の開発と生産的利用の発展に努めている。情報技術ラボラトリの責務は、連邦政府の情報システムにおいて、費用対効果の高いセキュリティを施し、国家安全保障にかかわらない情報のプライバシーを確保するための、技術的、物理的、管理的および運用のための標準とガイドラインを策定することにある。NIST Special Publication 800 シリーズでは、情報システムセキュリティにおける情報技術ラボラトリの調査、ガイドライン、普及活動ならびに産業界、政府機関および教育機関との共同活動について報告する。

作成機関および適用範囲

米国国立標準技術研究所（NIST: National Institute of Standards and Technology、以下 NIST と称する）は連邦情報セキュリティマネジメント法（FISMA: Federal Information Security Management Act、以下 FISMA と称す）、公法 107-347 に基づくその法的責任を果たすために、この文書を作成した。NIST は、連邦政府情報システムに対する、最低限の要求事項を含んだ情報セキュリティ標準およびガイドラインを作成する責務があるが、このような標準およびガイドラインは、そのようなシステムに対する政策権限を行使する適切な連邦政府職員による明示的な承認がない限り、国家安全保障にかかわるシステムには適用されない。このガイドラインは、OMB Circular A-130、第 8b(3)項、『Securing Agency Information Systems（政府機関の情報システムの保護）』の要求事項に一致しており、これは A-130 の付録 IV「（Analysis of Key Sections）重要部門の分析」で分析されているとおりである。 補足情報は、A-130、付録 III に記載されている。

本文書における一切は、商務長官が法的権威に基づき連邦政府に対して義務および拘束力を与えた標準および指針を否定するものではない。また、これらの指針は、商務長官、行政管理予算局長、または他のすべての連邦政府当局者の既存の権威に変更を加えたり、これらに取って代わるものと解釈してはならない。本文書は、非政府組織が自由意志で使用することができ、米国における著作権の制約はない。しかしながら、NIST に帰属すると考えてもらえれば幸いである。（翻訳者注：著作権に関するこの記述は、SP800-37 Revision1 の英語の原文のことを言っており、日本語へ翻訳した本文書の著作権は、独立行政法人 情報処理推進機構に帰属する）。

米国国立標準技術研究所、Special Publication 800-37, Revision 1, 93 頁

(2010 年 2 月)

この文書中で特定される商業的組織、装置、資料は、実験手順または概念を適切に説明するためのものである。したがって、NIST による推薦または保証を意味するものではなく、これら組織、資料、または装置が、その目的に関して得られる最善のものであると意味しているわけでもない。

本文書には、現在 NIST が作成中の文書を参照している個所がある。これらの文書は、NIST に割り当てられた法的責任に従って作成しているものである。本文書における概念および方法論を含む情報は、前述の関連文書が完成する前であっても使用してかまわない。したがって、各文書が完成するまでは、既存の要求事項、ガイドラインおよび手順（存在する場合）が引き続き有効である。政府機関は、NIST 発行の文書を、自身のセキュリティ計画の作成および移行に役立てるために、これらの新文書の作成状況を知りたいと考えるかもしれない。

各組織においても、パブリックコメントの募集期間中に、すべての公開ドラフト文書を閲覧し、コメントをNISTへ提出することができる。上記の文書を除き、すべての NIST 刊行物は、http://csrc.nist.gov/publications から入手できる。

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

NISTの標準およびガイドラインへの準拠

FISMAの規定に従って[1]、商務長官は、NISTが策定した標準およびガイドラインに基づいて、連邦政府の情報システムに関する標準およびガイドラインを定めるものとする。商務長官は、連邦政府情報システムの運用の効率性またはセキュリティを向上させるのに必要と判断されたレベルまで、標準への準拠を義務化し、拘束力を与えるものとする。商務長官が定める標準には、情報セキュリティに関する必要最低限の要求事項を示す、さもなければ連邦政府の情報および情報システムのセキュリティを向上させるのに必要となる、情報セキュリティ標準を含めることとする。

- 連邦情報処理基準（FIPS: Federal Information Processing Standards、以下FIPSと称す）は、商務省長官の承認を受け、FISMAに従ってNISTにより発行される。FIPSは、連邦政府機関[2]に義務づけられており、拘束力を持つに至っている。FISMAでは、連邦政府機関がこれらの標準を順守することを求めており、政府機関は、それらの標準の使用を放棄することはできない
- Special Publications は、推奨およびガイダンス文書として、NISTが策定し発行する刊行物である。連邦政府機関は、国家安全保障関連以外のすべてのプログラムとシステムにおいて、FIPSによって義務づけられているそれらのNIST Special Publicationsに従わなければならない。FIPS200 は、SP800-53（修正を含む）の使用を義務づけている。OMB（行政管理予算局）のポリシー（OMB Reporting Instructions for FISMA and Agency Privacy Management（OMB作成のFISMAおよび連邦政府機関のプライバシー保護法に関する報告の手引き）を含む）には、国家安全保障関連以外のすべてのプログラムとシステムに対して、政府機関が特定のNIST Special Publication に従わなければならない旨が記載されている[3]。
- 中間政府機関の報告書（NISTIRs）および ITL 速報など、上記以外のセキュリティ関係の出版物でも、NIST の活動に関する技術情報やその他の情報を提供している。これらの出版物は、OMB（行政管理予算局）によって指定されている場合に限り必須になる。
- NIST のセキュリティ標準およびガイドラインへの準拠に関するスケジュールは、OMB によって規定され、その内容は OMB のポリシー、指令、または覚書（たとえば、FISMA の年次報告に関するガイダンス）に記載されている。

---

[1] 電子政府法（公法第 107-347）は、米国における経済および国家安全保障上の利益に対する情報セキュリティ の重要性を認識している。連邦情報セキュリティマネジメント法と命名された電子政府法第 III 編は、それぞれの組織が、自身の業務および資産をサポートする情報システムに対するセキュリティを提供する、組織全体に渡るプログラムを作成、文書化および導入する必要性を強調している。

[2] 本文書では「政府機関」という用語をより一般的な用語である「組織」の代わりに使用している箇所があるが、これは、その使用が、連邦法または連邦政府ポリシーなどの、その他のソースドキュメントに直接関連する場合に限る。

[3] 連邦政府機関は OMB(行政管理予算局)のポリシーに則り、特定の NIST Special Publications に従わなければならないが、どのようにガイダンスを適用するかについては、政府機関の裁量に任されている。連邦政府機関は、自身の任務／業務上の機能、および運用環境に合わせて、NIST Special Publications が規定するセキュリティ概念および原則を適用する。したがって連邦政府機関が NIST ガイダンスを適用した結果、異なるセキュリティソリューションとなることもあるが、それらのソリューションは受け入れられるものであり、NIST ガイダンスに準拠し、OMB(行政管理予算局)が定める、連邦政府機関の情報システムに対する適切なセキュリティ（Adequate Security）にも適合するものである。連邦政府における情報の共有および透明性の確保は、優先度が高いため、政府機関は、自身の情報セキュリティソリューションを開発する際に、互恵契約（reciprocity）についても考慮する。政府機関が NIST Special Publications に準拠しているかどうかを評価する場合には、監査官、評価者、監査人、およびアセサー(assessor)は、個々のガイダンス文書に記載されているセキュリティ概念および原則の意図を理解し、政府機関が自身の任務／業務上の責任、運用環境、および組織特有の状況に合わせて、どのようにガイダンスを適用したかを考慮するべきである。

謝辞

本文書は、連邦政府向けの統一的な情報セキュリティフレームワークの構築を目的として、民間、防衛、およびインテリジェンスコミュニティの代表からなる Joint Task Force Transformation Initiative Interagency Working Group（以下、省庁間作業グループと称す）によって作成された。プロジェクトリーダーである Ron Ross（NIST）は、献身的な努力をもって本文書の作成に大いに寄与してくれた、米国商務省および国防総省、国家情報局、国家安全保障システム委員会からなるシニアリーダシップチーム、ならびに省庁間作業グループのメンバーに感謝の意を表する。シニアリーダシップチーム、省庁間作業グループのメンバー、および関連組織には、以下に示す方々が含まれる。

米国国防総省

Cheryl J. Roby
Acting Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer

Gus Guissanie
Acting Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance

Dominic Cussatt
Senior Policy Advisor

国家情報局

Honorable Priscilla Guthrie
Intelligence Community Chief Information Officer

Sherrill Nicely
Deputy Intelligence Community Chief Information Officer

Mark J. Morrison
Deputy Associate Director of National Intelligence for IC Information Assurance

Roger Caslow
Lead, C&A Transformation

NIST

Cita M. Furlani
Director, Information Technology Laboratory

William C. Barker
Chief, Computer Security Division

Ron Ross
FISMA Implementation Project Leader

国家安全保障システム委員会

Cheryl J. Roby
Acting Chair, Committee on National Security Systems

Eustace D. King
CNSS Subcommittee Co-Chair (DoD)

William Hunteman
CNSS Subcommittee Co-Chair (DoE)

Joint Task Force Transformation Initiative Interagency Working Group

Ron Ross *NIST, JTF Leader*	Gary Stoneburner *Johns Hopkins APL*	Dominic Cussatt *Department of Defense*	Kelley Dempsey *NIST*
Marianne Swanson *NIST*	Jennifer Fabius Greene *MITRE Corporation*	Dorian Pappas *National Security Agency*	Arnold Johnson *NIST*
Stuart Katzke *Booz Allen Hamilton*	Peter Williams *Booz Allen Hamilton*	Peter Gouldmann *Department of State*	Christian Enloe *NIST*

上記の謝辞に加えて、Peggy Himes および Elizabeth Lennon の両氏には、優れたテクニカルエディティングおよび管理支援をいただいたことにとりわけ感謝したい。また、Beckie Bolton 氏, Marshall Abrams 氏、John Gilligan 氏、Richard Graubart 氏、EstenPorter 氏、Karen Quigg 氏、George Rogers 氏、John Streufert 氏、および Glenda Turner 氏には、本文書の内容の改善に格別な貢献をしてくださったことに感謝する。最後に、国内外の公共および民間部門の個人および団体からいただいた多大な貢献にも心より感謝の意を表する。彼らの建設的で思慮深いコメントによって、本文書の全体的な質と実用性が高められた。

情報セキュリティの共通基盤の構築

公共および民間部門の機関との提携

NIST は、FISMA が要求する標準およびガイドラインを策定するにあたって、他の政府機関および民間部門に助言を求めることにより、情報セキュリティの向上を図り、不要でありかつコスト高につながる努力の重複を避けると同時に、NIST 刊行物が、国家安全保障にかかわるシステムを保護するために採用される標準およびガイドラインへの補足となることを確実にする。NIST は、包括的なパブリックレビューおよび審議プロセス（vetting process）に加えて、米国国家情報局（ODNI）、米国防総省（DOD）、国家安全保障システム委員会（CNSS）と連携して、連邦政府全体にわたる情報セキュリティの共通基盤の構築に努めている。情報セキュリティの共通基盤を利用することで、連邦政府のインテリジェンス部門、防衛部門、および民生部門、ならびに彼らの請負業者は、情報システムの運用および使用により生じる組織の業務や資産、個人、他の組織、および国家に対するリスクを、より一貫性のある統一された方法で管理できるようになる。また、情報セキュリティの共通基盤は、セキュリティ運用認可判断の相互受け入れを実現するための強力な基盤となり、情報の共有を容易にする。NIST はまた、公共および民間部門の機関と連携して、NIST が策定したセキュリティ標準およびガイドラインと、ISO と IEC が策定した 27001 シリーズの ISMS（Information Security Management System）とのマッピングおよび関係の確立に努めている。

目次

序文

「・・・リーダーは、リスクマネジメントプロセスを通じて、サイバースペースを自身が有利になるように利用する敵や、サイバースペースのグローバルな性質を利用して軍事活動、情報収集活動、ビジネス活動における目的を果たそうとする我々自身の取り組みから生じる、米国の利益に対するリスクについて考慮しなければならない。」

「・・・活動計画を策定する際には、脅威、脆弱性、および影響の組み合わせを評価することによって、重要動向を把握し、脅威能力の排除または削減、脆弱性の排除または削減、およびすべてのサイバースペース活動の評価、調整、非対立化を行うために努力を傾けるべき分野を決定しなければならない。」

「あらゆる階層のリーダーは、他のあらゆる分野と同レベルの準備体制およびセキュリティを確保することに責任を負う」

-- THE NATIONAL STRATEGY FOR CYBERSPACE OPERATIONS
OFFICE OF THE CHAIRMAN, JOINT CHIEFS OF STAFF, U.S. DEPARTMENT OF DEFENSE

第 1 章

はじめに

情報セキュリティの必要性とリスクを管理する必要性

組織[4]は、自身の任務および業務上の機能を成功裏に実施するために、情報技術、およびその技術をもとに開発された情報システム[5]に依存している。 情報システムには、その構成要素として、高性能のスーパーコンピュータから、携帯端末および携帯電話まで、さまざまなコンピューティングプラットフォームが含まれる場合がある。また、極めて特殊なシステムおよびデバイス（たとえば、通信システム、産業用／プロセス制御システム、テスト用および較正用デバイス、武器システム、指揮管理システム、環境制御システム）が含まれる場合もある。連邦政府の情報および情報システム[6]は、それらのシステムによって処理、格納、または伝送される情報の機密性、完全性または可用性を侵害することによって、組織の業務（任務、機能、イメージ、および評判を含む）、組織の資産、個人、他の組織、および国家[7]にマイナスの影響を与える可能性のある、深刻な脅威の標的になりやすい。情報および情報システムに対する脅威には、環境破壊、人的ミスまたは機械エラー、および意図的な攻撃が含まれる。今日の、情報システムに対するサイバー攻撃は、積極的であり、統制がとれていて、よくまとめられて、資金に恵まれていて、かつ増え続ける事例によると極めて高度であることが多い。公共および民間部門の情報システムに対する攻撃（複数）が成功した場合、米国の国家安全上の利益および経済安全上の利益に深刻な、または重大な被害が及ぶ可能性がある。これらの脅威の危険性が重大であり、かつ増大していることから、組織内のあらゆる階層のリーダーが、適切な情報セキュリティの確保、および情報システム関連のセキュリティリスク[8]の管理における自身の責務を理解することが必要不可欠になる。

1.1 背景

NIST は、国防総省（DoD）、国家情報局（ODNI）、および国家安全保障システム委員会（CNSS）と協力して、連邦政府およびその請負業者向けの共通の情報セキュリティフレームワークを策定した。この共通フレームワークは、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、および連邦政府機関間の互恵契約（reciprocity）の促進を目的としている。本文書は、Joint Task Force Transformation Initiative Working Group によって作成されたものであり、従来の C&A（Certification and Accreditation：承認および運用認可）プロセスを、6 つのステップからなる RMF（Risk Management Framework：リスクマネジメントフレームワーク）に変換している。改訂されたプロセスは、以下の点に重点をおく: (i) 管理面、運用面、および技術面での最先端のセキュリティ管理策を適用することによって、連邦政府の情報システムに情報セキュリティ機能を組み入れること (ii) 強

[4] 本文書で使用されている「組織」という用語は、組織的な構造（たとえば、連邦政府機関、または、該当する場合、連邦政府機関の運用上のあらゆるエレメント）内のエンティティ（その規模、複雑さ、または位置づけは問わない）を示している。

[5] 情報システムとは、情報の収集、処理、保守、利用、共有、配布、廃棄を目的として編成された、独立した一連の情報資源である。

[6] 連邦政府情報システムとは、執行機関、執行機関の契約者、または執行機関の代わりとなる他の組織によって使用または運用される情報システムである。

[7] 国家に対するマイナスの影響には、たとえば、重要インフラのアプリケーションをサポートする情報システムに対する侵害、または国土安全保障省が規定する、政府の業務継続にとって最も重要な情報システムに対する侵害が含まれる。

[8] リスクとは、発生しうる状況またはイベントによって、エンティティが脅かされる度合いの尺度であり、(i) 当該の状況またはイベントが発生した場合にもたらされると考えられる悪影響と、(ii) 発生の可能性との、関数によって求められる。

化された監視プロセスを通じて、情報システムのセキュリティ状態に関する意識を継続的に維持する (iii) 情報システムの運用および使用により生じる組織の業務や資産、個人、他の組織、および国家に対するリスクを容認するか否かについての判断を容易にするための、重要な情報をシニアリーダーに提供すること。

RMF は、以下の特徴を有する。

- 堅牢で継続的監視プロセスの実施により、リアルタイムに近いリスクマネジメントおよび情報システムの継続的な運用認可の概念を促進する。
- 主要な任務および業務上の機能をサポートす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のに必要な情報をシニアリーダー提供するための、オートメーション（automation）の利用を促進する。
- エンタープライズアーキテクチャおよびシステム開発ライフサイクルに情報セキュリティを組み入れる。
- セキュリティ管理策の選択、実施、アセスメント、および監視、ならびに情報システムの運用認可に重点を置く。
- リスクエグゼクティブ（機能）を通じて、情報システムレベルのリスクマネジメントプロセスを、組織レベルのリスクマネジメントプロセスにリンクする
- 組織の情報システムに導入され、それらのシステムによって継承されるセキュリティ管理策（すなわち、共通管理策）に対する責任と説明責任を定める。

本文書に記載されているリスクマネジメントプロセスでは、C&A の焦点を、従来の静的で手順に沿った活動から、より動的なアプローチへと置き換えている。この動的なアプローチにより、複雑で高度なサイバー脅威、増え続けるシステムの脆弱性、および急速に変化する任務を伴う極めて多様な環境においても、情報システム関連のセキュリティリスクをより効率的に管理できるようになる。

1.2 目的および適用性

本文書の目的は、セキュリティ分類 [9]、セキュリティ管理策の選択および実施、セキュリティ管理策のアセスメント、情報システムの運用認可 [10]、およびセキュリティ管理策の監視といった活動の実施を含む、リスクマネジメントフレームワークを、連邦政府の情報システムに適用するためのガイドラインを提供することにある。本ガイドラインは、次のような目的で作成された。

- 情報システム関連のセキュリティリスクの管理を、組織の任務／業務上の目的、およびリスクエグゼクティブ（機能）を通じてシニアリーダーが定めた全般的なリスク戦略に確実に適合させる。
- 必要なセキュリティ管理策を含む情報セキュリティ要求事項を、組織のエンタープライズアーキテクチャおよびシステム開発ライフサイクルに確実に組み入れる。

[9] FIPS199 は、国家安全保障にかかわらないシステムに対するセキュリティ分類に関するガイダンスを提供する。CNSS Instruction 1253 は、国家安全保障にかかわるシステムに対する同様のガイダンスを提供する。

[10] セキュリティの運用認可とは、情報システムの運用を認可し、合意されたセキュリティ管理策の導入について組織の業務や資産、個人、他の組織、および国家に対するリスクを明示的に受容する、といった組織の上級職員による正式な管理判断である。

- （継続的な監視を通じて）一貫性のある、十分な情報に基づいた、継続的なセキュリティ運用認可判断を支援すると同時に、セキュリティおよびリスクマネジメント関連の情報の透明性、ならびに互恵契約（reciprocity）[11]を支援する。
- 適切なリスク軽減戦略の実施により、連邦政府内の情報および情報システムのセキュリティを向上させる。

本文書は、FISMAの要求事項を満たすものであり、OMB がCircular A-130, Appendix III, Security of Federal Automated Information Resourcesで規定している執行機関 [12]向けの情報セキュリティ要求事項に適合する（あるいは、それらの要求事項を上回る）ものである。本文書に記載されているガイドラインは、44 U.S.C.のセクション 3542 が規定する国家安全保障にかかわるシステムを除き、すべての連邦情報システムに適用される。本ガイドラインは、国家安全保障にかかわるシステムに対する同様のガイドラインについても補足を行えるように、技術的な観点から広範囲にわたって作成されたものであり、そのようなシステムに対する政策権限を行使する適切な連邦政府職員による承認があれば、そのようなシステムに適用することができる。州政府、地方政府、および隊組織はもとより、民間部門の組織においても、必要に応じて本ガイドラインの使用を検討することが推奨される。[13]

1.3 対象となる読者

本文書は、以下の者を含む、連邦政府情報システムの設計、開発、導入、運用、維持管理、および廃棄に関わる個人にとって、有用なものである。

- 任務／業務上のオーナーシップに責任を持つ者、または、受託者責任を持つ者（例：連邦政府機関の長、最高経営責任者、最高財務責任者）
- 情報システムの開発および統合に責任を持つ者（例：プログラムマネージャ、IT 製品の開発者、情報システムの開発者、情報システムのインテグレータ、エンタープライズアーキテクト、情報セキュリティアーキテクト）
- 情報システムおよび／またはセキュリティの管理／監督に責任を持つ者（例：シニアリーダー、リスクエグゼクティブ、運用認可責任者、最高情報責任者、上級情報セキュリティ責任者 [14]）

[11] 互恵契約（reciprocity）とは、情報システムリソースの再利用や、互いのセキュリティ状態の評価結果を受け入れることによる情報の共有を目的として、参加している組織間で、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に合意することをいう。互恵契約(reciprocity)を成立させる最良の方法は、透明性の概念を促進することである（すなわち、情報システムのセキュリティ状態に関する十分な証拠を誰もが入手できるようにすることによって、別組織の運用認可責任者がその証拠を利用して、そのシステム、または、そのシステムが処理、格納、もしくは伝送する情報の運用および使用に関して信頼のおけるリスクベースの意思決定を下せるようにする。）

[12] 執行機関とは、(i) 5 U.S.C., Sec. 101 により規定される執行部門 (ii) 5 U.S.C., Sec. 102 により規定される軍の部局 (iii) 5 U.S.C., Sec. 104(1)により定義される独立機関および (iv) 31 U.S.C., 91 章の規定を全面的に満たしている完全に政府が所有する企業である。本文書において「執行機関(executive agency)」という用語は、「連邦政府機関(federal agency)」という用語と同義である。

[13] FISMA および OMB ポリシーの規定に従って、州政府／地方政府／隊組織、請負業者、または被譲与者が運用する情報システムに対する連邦政府情報システムの相互接続が、連邦政府情報の処理、格納、または伝送を伴う場合には常に、本文書に記載されている情報セキュリティ標準およびガイドラインが適用される。システムの相互接続に関する具体的な情報セキュリティ要求事項および諸条件に関しては、参加組織が策定する Memorandums of Understanding and Interconnection Security Agreements に記載されている。

[14] 政府機関レベルでは、この役職は、政府機関の上級情報セキュリティ責任者（Senior Agency Information Security Officer）として知られている。組織レベルでは、この役職は、最高情報セキュリティ責任者（Chief Information Security Officer）と呼ばれる。

- 情報システムおよびセキュリティ管理策のアセスメントおよび監視に責任を持つ者（例：システム評価者、アセサー／アセスメントチーム、検証および有効性確認を行う第三者アセサー、監査官、または情報システムのオーナー）
- 情報セキュリティの導入および運用に責任を持つ者（例：情報システムのオーナー、共通管理策のプロバイダ、情報のオーナー／スチュワード、任務／業務のオーナー、情報セキュリティアーキテクト、情報システムセキュリティエンジニア／責任者）。

1.4 本文書の構成

本文書は以降、次のように構成されている。

- **第 2 章**では、情報システム関連のセキュリティリスクの管理に関連する基本概念を説明する。内容には次のようなものが含まれる。(i) リスクマネジメントに対する組織全体としての見解、およびリスクマネジメントフレームワークの適用 (ii) システム開発ライフサイクルへの情報セキュリティ要求事項の組み入れ (iii) 情報システム境界の確立、および (iv) システム固有の管理策、ハイブリッド管理策、または共通管理策として分類されたセキュリティ管理策の、情報システムへの割り当て。
- **第 3 章** では、リスクマネジメントフレームワークを情報システムに適用するのに必要なタスクについて記述する。内容には次のようなものが含まれる。(i) 情報および情報システムの分類 (ii) セキュリティ管理策の選択 (iii) セキュリティ管理策の導入 (iv) セキュリティ管理策の有効性のアセスメント (v) 情報システムの運用認可、および(vi) セキュリティ管理策、および情報システムのセキュリティ状態の継続的な監視。
- **（補足）付録** では、リスクマネジメントフレームワークの情報システムへの適用に関する追加情報を提供する。内容には次のようなものが含まれる。(i) 参考文献 (ii) 用語集 (iii) 略語 (iv) 役割と責任 (v) RMF タスクの要約 (vi) 情報システムのセキュリティ運用認可 (vii) 情報システムのセキュリティ状態の監視 (viii) 運用上のシナリオ (ix) 外部環境におけるセキュリティ管理策。

第 2 章

基本項目

情報システム関連のセキュリティリスクの管理

本章では、情報システム関連のセキュリティリスクの管理に関連する基本概念を説明する。これらの概念には次のようなものが含まれる。(i) リスクマネジメントに関する原則およびベストプラクティスを、組織全体にわたる戦略計画の策定における考慮事項、主要な任務および業務プロセス、ならびに組織の支援情報システムに組み入れること (ii) 情報セキュリティ要求事項をシステム開発ライフサイクルに組み入れること (iii) 実用的で有意な情報システム境界を確立すること、および (iv) システム固有の管理策、ハイブリッド管理策、または共通管理策として分類されたセキュリティ管理策を、組織の情報システムに割り当てること。

2.1 統合された組織全体にわたるマネジメント

情報システム関連のセキュリティリスクの管理は、複雑で、多面的な業務であり、組織全体 － すなわち、組織の戦略的ビジョンおよびトップレベルの目標と目的を定めるシニアリーダーから、プロジェクトを計画・管理する中間層のリーダー、ならびにフロントラインにいて組織の主要な任務および業務プロセスを支援する情報システムを開発、導入、運用する個人まで － の関与が必要になる。リスクマネジメントは、組織のあらゆる側面に完全に統合される全体論的な活動とみなすことができる。図 2-1 に、リスクマネジメントにおける 3 層のアプローチを示す。このアプローチでは、(i) 組織レベル (ii) 任務および業務プロセスレベル 、および (iii) 情報システムレベルにおける、リスク関連問題を取り扱っている。[15]

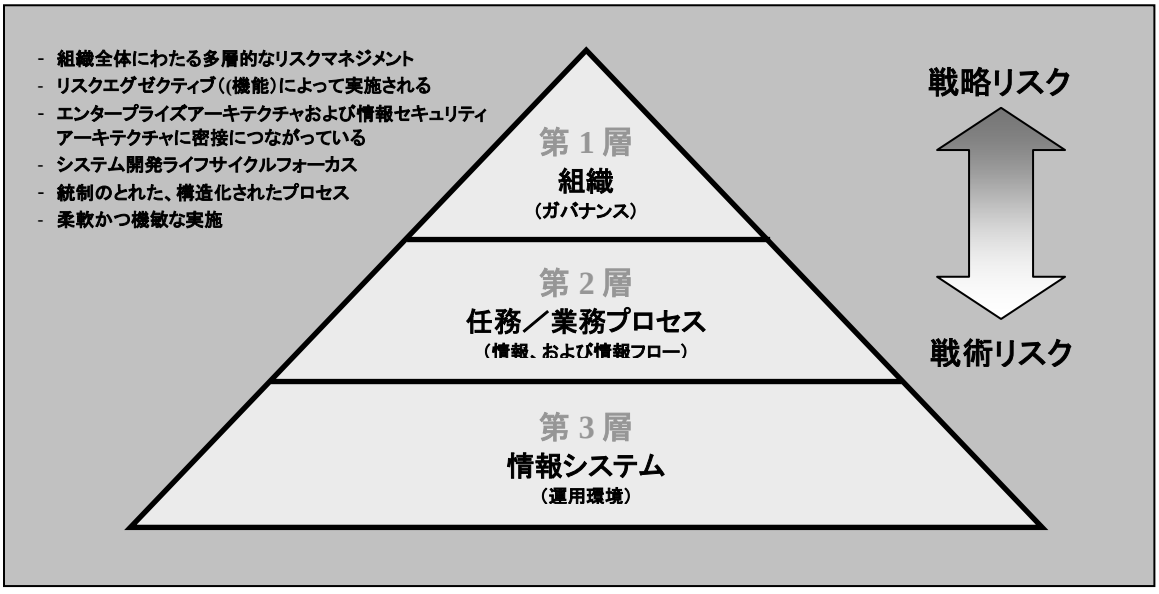

図 2–1: 段階的なリスクマネジメントアプローチ

[15] 2010 年に公開される予定の NIST SP800-39『Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View』は、リスクマネジメントにおける全体論的なアプローチに関するガイダンスとなる。

第 1 層では、以下の項目を含む、包括的なガバナンス構造、および組織全体にわたるリスクマネジメント戦略を開発することによって、組織的観点からリスクに対処する。(i) 情報システム関連のセキュリティリスク、および組織が懸念するその他の種類のリスクを評価するのに使用する予定の、技術と方法論 [16] (ii) リスクアセスメント時に特定されたリスクの重大さを評価するのに使用する予定の、手法と手順 (iii) 特定されたリスクに対処するのに使用する予定の、リスク軽減対策の種類と範囲 (iv) 組織が許容する予定のリスクレベル（すなわち、リスク許容度） (v) 組織の情報システムやその運用環境に対する変更は避けられないことを踏まえて、組織がどのようにしてリスクを継続的に監視するか (vi) リスクマネジメント戦略が効果的に実施されていることを確認するために使用する予定の、監視の度合いと種類。組織が確立する全般的なガバナンス構造の一部であるリスクマネジメント戦略は、プログラム、計画、開発、調達、運用、および監視に責任を持つ、組織内の職員および請負業者に周知される。周知の対象には、たとえば、(i) 運用認可責任者 (ii) 最高情報責任者 (iii) 上級情報セキュリティ責任者 (iv) エンタープライズ／情報セキュリティアーキテクト (v) 情報システムのオーナー／プログラムマネージャ (vi) 情報のオーナー／スチュワード (vii) 情報システムセキュリティ責任者 (viii) 情報システムセキュリティエンジニア (ix) 情報システム開発者およびインテグレータ (x) システムアドミニストレータ (xi) 契約社員、および (xii) ユーザが含まれる。

第 2 層 では、任務および業務プロセスの観点から、リスクに対処する。この層は、**第 1 層**におけるリスク判断によって導かれる。**第 2 層**の活動は、エンタープライズアーキテクチャ [17]と密接に関連しており、以下の項目を含む。(i) 組織の主要な任務および業務プロセス（下部組織が実施する派生的な、または関連のある任務および業務プロセスを含む）を定義する (ii) 組織の目標と目的に照らし合わせて、各任務および業務プロセスに優先順位をつける (iii) 組織が定めた任務および業務プロセスを成功裏に実施するのに必要な情報の種類、および組織内外における当該情報のフローを定義する (iv) 組織全体にわたる情報保護戦略を策定し、高レベルの情報セキュリティ要求事項 [18]を主要な任務および業務プロセスに組み入れる、および (v) 親組織が、リスクのアセスメント、評価、軽減、受容、および監視に関して、下部組織（すなわち、親組織の傘下にある組織）にどの程度の自立性（autonomy）を持たせるかを規定する。

派生的な（あるいは、関連のある）任務および業務プロセスの実施に責任を持つ下部組織では、リスクをアセスメント、評価、軽減、受容および監視する独自の手法に対して既に資金を投じている可能性があるため、親組織は、コストを最小限に抑えるためにも、下部組織の一部または全体に高い自立性（autonomy）を持たせる可能性がある。多様なリスクアセスメント手法が容認される場合、組織は、実現可能な場合には、何らかの手法を用いてリスク関連情報の解釈と統合を行うことによって、異なるリスクアセスメント活動のアウトプットを意味のある形で関連づけることができる。

第 3 層 では、情報システムの観点から、リスクに対処する。この層は、**第 1 層**および**第 2 層**におけるリスク判断によって導かれる。**第 1 層**および**第 2 層**におけるリスク判断は、情報システムレベルで必要となる予防手段および対策（すなわち、セキュリティ管理策）の最終的な選択および導

[16] リスクの種類には、たとえば、(i) プログラム／調達に関するリスク（コスト、スケジュール、パフォーマンス） (ii) コンプライアンスおよび規定に関するリスク (iii) 財政的リスク (iv) 法的リスク (v) 運用（任務／業務）上のリスク (vi) 政治的リスク (vii) プロジェクトに関するリスク (viii) 評判に関するリスク (ix) 安全性に関するリスク (x) 戦略的計画に関するリスク、 および (xi).サプライチェーンに関するリスクが含まれる。

[17] 『Federal Enterprise Architecture Reference Models』と『Segment and Solution Architectures』は、それぞれ、OMB が 2003 年 10 月に公開した Federal Enterprise Architecture (FEA) Program『*FEA Consolidated Reference Model Document,* Version 2.3』、および 2009 年 1 月に公開した『*Federal Segment Architecture Methodology (FSAM)*』に規定されている。

[18] 情報セキュリティ要求事項は、さまざまなソース(たとえば、法律、ポリシー、指令、規定、標準、および組織の任務／業務／運用上の要求事項から入手することができる。組織レベルのセキュリティ要求事項は、情報セキュリティプログラム計画、または同等のドキュメントに記載されている。

入に影響を与える。情報セキュリティ要求事項は、NIST SP800-53 から、管理面、運用面、および技術面での適切なセキュリティ管理策を選択することによって、満たすことができる [19]。セキュリティ管理策は、組織が策定した情報セキュリティアーキテクチャに従って、システム固有の管理策、ハイブリッド管理策、または共通管理策として、情報システムのさまざまなコンポーネントに順を追って割り当てられる。[20] 通常、セキュリティ管理策は、組織が定めたセキュリティ要求事項まで*トレース*することができ、それらの要求事項が情報システムの設計、開発、および導入時に余すところなく満たされていることを確認できるようになっている。セキュリティ管理策は、組織、または、外部のプロバイダによって提供されることが考えられる。外部のプロバイダとの関係は、さまざまな形式で構築される。たとえば、ジョイントベンチャー、ビジネスパートナーシップ、外注契約（すなわち、契約、省庁間の取り決め、業務分野についての取り決めを介して）、ライセンス契約および／またはサプライチェーンの交換などが考えられる。[21]

システム開発ライフサイクルの早い段階で開始されるリスクマネジメントタスクは、情報システムのセキュリティ機能を形成するうえで重要である。リスクマネジメントタスクがシステム開発ライフサイクルの開始、開発、および調達の段階で適切に実施されなかった場合、これらのタスクは必然的にシステム開発ライフサイクルの後の段階で実施されることになり、実施費用も高くなる。いずれの場合も、すべてのタスクは、以下の項目が確実に行われるようにするために、情報システムの運用を開始する前に、あるいは、運用を継続する前に完了すべきである。(i) 情報システム関連のセキュリティリスクに対する適切な対応の継続的な実施 (ii) 組織が定めた一連のセキュリティ管理策が実施されることを前提とし、情報システムの最新のセキュリティ状態を考慮したうえで、運用認可責任者が組織の業務や資産、個人、他の組織、および国家に対するリスクを明確に理解し、受容すること。

図 2-2 に示すリスクマネジメントフレームワーク（RMF）は、情報セキュリティとリスクマネジメント活動をシステム開発ライフサイクルに組み入れるための、統制のとれた構造化されたプロセスを提供する。RMF は、主に、リスクマネジメント階層における**第 3 層**で機能するが、**第 1 層**と**第 2 層**においても、情報のやりとりが行われることがある（たとえば、継続的な運用認可判断からのフィードバックをリスクエグゼクティブ（機能）に提供する、脅威およびリスクに関する最新情報を運用認可責任者および情報システムのオーナーに配布する等）。RMF のステップには、以下の項目が含まれる。

- **分類**－情報システム、およびそのシステムによって処理、格納、および伝送される情報を、影響分析結果に基づいて分類する。[22]
- **選択**－セキュリティ分類結果に基づいて、情報システムに対するベースラインセキュリティ管理策の初期セットを選択する。また、リスク、およびローカルな状況のアセスメント結果に基づいて、必要に応じてセキュリティ管理策ベースラインを調整し、補足する。[23]

[19] 法律、ポリシー、指令、規定、標準、および組織の任務／業務／運用上の要求事項についての考慮を含む RMF の分類ステップは、セキュリティ要求事項の明確化を容易にする。

[20] セキュリティ管理策の割り当ては、リスクマネジメント階層内の 3 つのすべての層で行われる可能性がある。たとえば、共通管理策として識別されたセキュリティ管理策は、組織レベル、任務／業務プロセスレベル、または情報システムレベルで割り当てられる可能性がある。セキュリティ管理策の割り当てに関する詳細は、セクション 2.4 を参照のこと。

[21] 外部サービスプロバイダ、および外部環境へのセキュリティ管理策の供給に関する追加ガイダンスは、付録 I に記載されている。

[22] FIPS199 は、国家安全保障にかかわらないシステムに対するセキュリティ分類に関するガイダンスを提供する。CNSS Instruction 1253 は、国家安全保障にかかわるシステムに対する同様のガイダンスを提供する。

[23] NIST SP800-53 は、国家安全保障にかかわらないシステムに対するセキュリティ管理策の選択に関するガイダンスを提供する。CNSS Instruction 1253 は、国家安全保障にかかわるシステムに対する同様のガイダンスを提供する。

- **実施**－セキュリティ管理策を実施する。また、情報システム、およびその運用環境において、セキュリティ管理策をどのように採用するかについて、記述する。
- **アセスメント**－セキュリティ管理策がどの程度正しく導入されているか、どの程度意図した通りに運用されているか、システムのセキュリティ要求事項に対する適合性の観点から所望の結果をどの程度産出しているかを判断するために、適切なアセスメント手順を用いて、セキュリティ管理策をアセスメントする。
- **運用認可**－情報システムの運用から生じる組織の業務や資産、個人、他の組織、および国家に対するリスクを評価し、そのリスクを受容できると判断した場合に、情報システムの運用を認可する。
- **監視**－情報システムに導入されているセキュリティ管理策を継続的に監視する。これには、管理策の有効性の評価、システムまたはその運用環境に対する変更の文書化、関連する変更によるセキュリティ影響の分析、システムのセキュリティ状態の指定された職員への報告が含まれる。

第 3 章では、RMF の 6 つのステップを実施するのに必要な、各タスクについて詳述する。

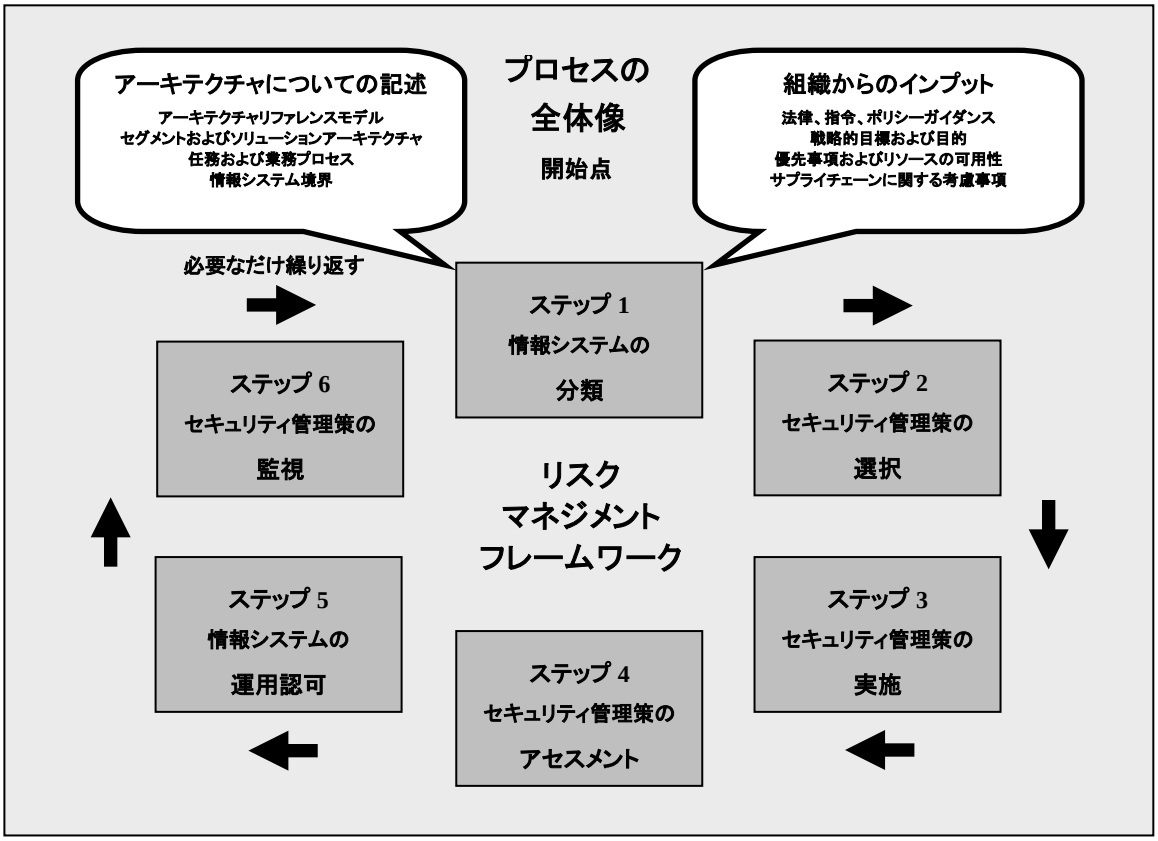

図 2-2: リスクマネジメントフレームワーク

要するに、上述のリスクマネジメントプロセスをどのように採用するかについては、かなりの柔軟性が組織に与えられている。図 2-1 のリスクマネジメントアプローチを階層的に描写するのは便利であるが、プロジェクトおよび組織のダイナミクスの現実は、はるかに複雑である可能性がある。組織のマネジメントスタイルは、トップダウンのコマンドから、仲間同士の合意にいたるまでの、連続体

上の 1 つまたは複数のポイント上に存在するともいえる。組織が、組織のあらゆるレベルにおいてリスクマネジメントを成功裏に行うには、すべてのリスクマネジメントプロセスおよび手順に適用される、一貫性のある効果的なリスクマネジメントアプローチを備えていなければならない。組織の担当者は、本文書に記載されているリスクマネジメントタスクを完遂するのに必要なリソースを特定し、組織内の適切な職員がそれらのリソースを確実に利用できるようにする。リソースの割り当てには、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、それらのタスクを完遂するのに必要な有用な人材を割り当てることの、両方が含まれる。[24]

2.2 システム開発ライフサイクル

運用中のシステム、開発中のシステムおよび何らかの修正または更新が行われているシステムを含むすべての連邦政府情報システムは、通常、システム開発のライフサイクルとして考えられるいずれかの段階に含まれる。[25] 要求事項の定義は、あらゆるシステム開発プロセスにおける重要な要素であり、システム開発ライフサイクルのかなり早い段階（通常は、「開始」フェーズ）で着手することになる。[26] セキュリティ要求事項は、情報システムに課せられる全般的な機能的要求事項および非機能的要求事項（たとえば、品質、保証）のサブセットであり、全般的な機能的要求事項および非機能的要求事項と同時にシステム開発ライフサイクルに組み入れられる。早い段階でセキュリティ要求事項を組み入れかった場合、初期設計に含めることが可能であったセキュリティに関する考慮事項を、システム開発ライフサイクルの後の段階で扱うことになるため、組織にとっては、かなりの出費になる可能性がる。セキュリティ要求事項が、情報システムの他の要求事項にとって不可欠なサブセットであるとみなされ場合、構築されるシステムは、弱点や欠点が少ないシステム、すなわち、将来にわたって悪用される可能性のある脆弱性が少ないシステムになる。.

情報セキュリティ要求事項を早い段階でシステム開発ライフサイクルに組み入れることは、組織にとって、組織の保護戦略を確実に実施するための最も費用対効果が高く効率的な手段となる。また、このような取り組みによって、現行の任務および業務機能を支援する情報システムを開発、導入、運用、および維持管理するために組織が採用するその他の日常的な管理プロセスから、情報セキュリティプロセスが分離されることを回避できる。情報セキュリティ要求事項は、システム開発ライフサイクルに組み入れられるだけでなく、組織内のプログラム、計画、および予算編成活動にも組み入れられ、これにより組織は、必要な時にリソースを利用できるようになり、プログラム／プロジェクトのマイルストーンも完成させることができる。エンタープライズアーキテクチャでは、組織内のこの組み入れ活動に関する記録が一元的に管理される。

採用されるライフサイクルプロセスの種類にかかわらず、組織のシステム開発ライフサイクルプロセスに情報セキュリティ要求事項を確実に組み入れることによって、障害耐性の高い情報システムの開発および導入が容易になり、組織の業務や資産、個人、他の組織、および国家に対するリスクを軽減することができる。これは、「統合されたプロジェクトチーム」[27]という十分に確立された概念によって成し遂げられる。組織の責任者（たとえば、政府機関の長、任務または業務のオーナー、統

[24] リソース要求事項には、自身に割り当てられた責務を効果的に実施できるようにするための、職員に対する訓練にかかる資金の調達が含まれる。

[25] 通常、一般的なシステム開発ライフサイクルには、(i) 開始 (ii) 開発／調達 (iii) インプリメンテーション (iv) 運用／保守 (v) 廃止、といった 5 つのフェーズがある。

[26] 組織は、たとえば、ウォーターフォール、スパイラル、アジャイル開発など、さまざまなシステム開発ライフサイクルプロセスを採用することができる。

[27] 統合されたプロジェクトチームとは、組織の要求事項に適合する情報システムの開発を容易にするための、幅広い技能と役割を有する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。

合されたプロジェクトチームのリーダー、プログラムマネージャ、情報システムのオーナー、運用認可責任者）は、**第 1 層**および**第 2 層**における情報セキュリティ要求事項の初期の定義から、**第 3 層**におけるセキュリティ管理策の選択までの、あらゆる情報システム開発活動において、セキュリティ専門家が不可欠な要素となることを確実にする。このような考慮は、情報システムの設計、開発、導入、運用、維持管理、および廃棄に責任を持つ職員と、リスクの適切な軽減と重要な任務および業務機能の保護に必要な適切なセキュリティ管理策についてシニアリーダーに助言する、情報セキュリティ専門家との間の、緊密な協力関係を助長するために用いられる。.

最後に、組織は、情報セキュリティ関連の目的に必要な類似の情報に課せられる要求事項を満たすために、システム開発ライフサイクルにおいて生成されたセキュリティ関連の情報（たとえば、アセスメント結果、情報システムに関するドキュメント、およびその他のアーチファクト）を最大限に利用する。共通管理策（外部プロバイダが提供するセキュリティ管理策を含む）に関する類似のセキュリティ関連情報は、組織のリスクマネジメントプロセスに投入される。組織によるセキュリティ関連情報の慎重な再利用は、努力の重複の排除、ドキュメント作成の削減、互恵契約（reciprocity）の促進、システム開発ライフサイクルプロセから独立した形でのセキュリティ活動の実施がもたらす不要なコストの回避を実現するための、効果的な手段となる。更に、（セキュリティ関連情報の）再利用は、情報システムの設計、開発、導入、運用、維持管理、および廃棄に使用される情報（セキュリティ関連の考慮事項を含む）の一貫性を向上させる。

2.3 情報システム境界

情報システムのオーナー、運用認可責任者、最高情報責任者、上級情報セキュリティ責任者、および情報セキュリティアーキテクトにとって、最も困難な課題の一つは、組織の情報システムの適切な境界を明確にすることである。[28] 明確に定義された境界によって、組織の情報システムに対する保護範囲（すなわち、組織が、組織の直接的な統制管理（direct management control）のもとで、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）が定まる。対象には、組織の任務および業務プロセスを支援する情報システムの一部である人、プロセス、および情報技術が含まれる。情報システム境界は、セキュリティ計画が作成される前に、セキュリティ分類プロセスとの調整を経て決定される。情報システムの境界が極端に広いと（すなわち、システムコンポーネントの数が多すぎたり、アーキテクチャが不必要に複雑である）、リスクマネジメントプロセスが極めて扱いにくく、複雑になる。境界が極端に制限されると、個別に管理する情報システムの数が増えるため、結果として、情報セキュリティの総費用がつり上がる。後続のセクションでは、適切なシステム境界を確立し、情報システムの運用および使用により生じる情報セキュリティ関連のリスクを管理する費用対効果の高いソリューションを実現するための、一般的なガイドラインを示す。

2.3.1 情報システムの境界の設定

情報システムに割り当てられた一連の情報資源 [29]によって、そのシステムの境界が定まる。組織には、情報システムが何によって構成されるのかに関する決定、および、そのシステムに関連する境界の決定について、大きな柔軟性が与えられている。一連の情報資源が1つの情報システムとして特定される場合、それらの資源は、通常、直接の同じ統制管理下 [30]に置かれる。直接の統制管理下に置くということは、必ずしも中間的な管理が存在しないという意味ではない。複数の情報シス

[28] リスクマネジメントプロセスおよび情報セキュリティに関しては、「情報セキュリティ境界（information system boundary）」という用語は、「認可境界（運用認可が及ぶ範囲）（authorization boundary）」と同義である。

[29] 情報資源は、情報および関連資源（人的資源、設備、資金、情報技術を含む）で構成される。

[30] 情報システムの直接的な統制管理には、予算、計画または運用に関する権限と、それに関連する責任と説明責任が関係する。

テムが、より複雑な情報システムを構成する独立したサブシステム[31]とみなされることもある。 この状況は、小規模の情報システムが、リスクマネジメントを目的として、大規模かつ、より包括的なシステムにまとめられる際に、多くの組織で発生する可能性がある。より大きな規模では、組織が、一連の共通の任務／業務機能を支援する複数の独立した情報システム（地理的に広い範囲にわたって分散されている可能性のある）から成る、一つのシステムを開発することが考えられる。[32]

直接的な統制管理の検討に加えて、情報システムとして識別された情報資源が、下記の特徴を有するかどうかを確認することは、組織にとっても有効な場合がある。

- 同様の任務／業務上の目的または機能を支援し、基本的な運用面での特徴と情報セキュリティ上の要求事項が一致している。
- 同一の一般的な運用環境におかれている（分散型情報システムの場合は、類似の運用環境を有するさまざまな場所に存在している。）[33]

共通性は時間の経過とともに変化する可能性があるため、この判断は、組織が実施する継続的な監視プロセスの一環として、定期的に再検討することになる（セクション 3.6 を参照）。このような検討を行う事は、組織がリスクマネジメントを目的として情報システムの境界を決定する際に有効である場合がある。また、このような検討事項が、組織が利用できる資源の範囲内で効果的な情報セキュリティを推進するために、一般的な意味での境界を確立する、といった柔軟性を制限するものではないということを忘れてはならない。情報システムのオーナーは、システムの境界を設定または変更する場合、運用認可責任者、最高情報責任者、上級情報セキュリティ責任者、情報セキュリティアーキテクト、およびリスクエグゼクティブ（機能）[34]の意見を参考にする。情報システムの境界を確立し、リスクマネジメントの範囲を決定するプロセスは、任務／事業上の要求事項、情報セキュリティに関する技術的な検討課題や組織の計画に関する費用などを検討し、主要担当官らによって十分な話合いが持たれるべき組織全体にわたる活動である。

情報システム上のソフトウェアアプリケーション（たとえば、データベースアプリケーション、Webアプリケーション）も、リスクマネジメントプロセスに含まれる。なぜならば、それらのアプリケーションのセキュリティは、そのシステム全体のセキュリティにとって極めて重要であるからである。[35] ソフトウェアアプリケーションは、それらをホスティングする情報システム（以下、ホスティングシステムと称する）が提供するリソースに依存する。したがって、ホスティングシステムが提供するセキュリティ管理策を活用して、ホスティングされるソフトウェアアプリケーションに基礎レベルの保護を提供することができる（この種の継承が適用される場合に限ってだが）。追加のアプリケーションレベルのセキュリティ管理策は、各ソフトウェアアプリケーションによって、必要に応じて提供される。組織は、個々のソフトウェアアプリケーションに導入されているアプリケーションレベルのセキュリティ管理策を含む、すべてのセキュリティ管理策について、管理および追跡が継続的に行われるようにする。アプリケーションのオーナーは、情報システムのオーナーと協力して、情報セキュリティおよびリスクマネジメント活動がアプリケーション間、およびそれらをホスティングするシステム間で、可能なかぎりシ

[31] サブシステムとは、情報、情報技術および単独または複数の特定の機能を実行する人員によって構成される情報システムの重要なサブディビジョンである。

[32] 複数システムから成るシステムの例としては、FAA（Federal Aviation Administration、連邦航空局）が運営する NAS（National Airspace System、全米航空システム）がある。

[33] 運用環境の類似点には、たとえば、脅威、ポリシー、およびマネジメントに関する考慮が含まれる。

[34] リスクエグゼクティブ（機能）の役割と責任については、付録 D に記載されている。

[35] ソフトウェアアプリケーション、および、それらのアプリケーションをホスティングする情報システムでは、所有者（組織）が異なる場合がある。

ームレスに実施されるようにする。この調整には、たとえば、以下の項目に対する考慮が含まれる。(i) ホスティングされるアプリケーションに対するセキュリティ管理策の選択、導入、アセスメント、および監視 (ii) ホスティングされるアプリケーションに対する変更が、情報システムの全体的なセキュリティ状態、およびそのシステムが支援する任務／業務プロセスにもたらす影響 (iii) 情報システムに対する変更が、ホスティングされるアプリケーションにもたらす影響。ソフトウェアアプリケーションおよび対応するホスティングシステム内に強力な構成管理および構成制御プロセスを導入し、かつ、セキュリティ管理策アセスメントの結果を再利用することによって、アプリケーションに必要な保護が提供される。

ホスティングされるソフトウェアアプリケーションが提供するセキュリティ管理策については、対応するホスティングシステムのセキュリティ計画に記載され、それらの管理策の有効性はリスクマネジメントプロセスにおいて評価される（すなわち、情報システムの初期の運用認可、および、後続の継続的監視プロセスにおいて）。ホスティングシステムの運用が認可された後に、アプリケーションが追加された場合にも、アプリケーションレベルのセキュリティ管理策の有効性の評価が行われる。情報システムのオーナーは、ホスティングされるアプリケーションが、対応するホスティングシステムのセキュリティ状態に影響を及ぼすことのないように、適切な措置を講じる。また、必要に応じて、セキュリティ影響分析を実施するのに必要な情報をアプリケーションのオーナーから取得する。

2.3.2 複雑な情報システムの境界

複雑な情報システムにおけるセキュリティ管理策の適用は、組織にとって大きな難題となることがある。中央集中型の開発、導入、および運用の場合、情報システムのオーナーは、運用認可責任者、上級情報セキュリティ責任者、情報セキュリティアーキテクト、および情報システムセキュリティエンジニアと協力して、情報システムの目的を検証し、複雑なシステムをより管理しやすいサブシステムに分解することができるかどうかを検討する。分散型の開発、導入、および運用の場合、複数のエンティティ（異なるポリシーのもとで活動している可能性がある）がその複雑な情報システムを構成する各サブシステムの開発、導入、および／または運用に携わっている可能性があることを、組織は認識する。このようなシナリオでは、個々のサブシステムが安全に、かつ機能的に連携することを確実にする責任が、組織に課せられる。情報システムを複数のサブシステムとしてとらえ、それぞれのサブシステムの境界を設定することによって、的を絞ったセキュリティ管理策の適用が容易になり、結果として組織は、適切なセキュリティおよ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ことができる。個々のサブシステムのセキュリティ特性についての知識が、必ずしも、（それらのサブシステムによって構成される）複雑な情報システムのセキュリティ特性についての完全な知識をもたらすわけではない。組織は、システムおよびセキュリティエンジニアリングにおけるベストプラクティスを適用し、情報システムの分解についてセキュリティ計画に記載する。

情報セキュリティアーキテクチャは、複雑な情報システムに対するセキュリティ管理策の選択および割り当てプロセスにおいて重要な役割を果たす。これには、サブシステムの主要な内部境界で発生する通信の監視および制御、ならびに、システム全体にわたる共通管理策（セクション 2.4 を参照）の提供が含まれる。システム全体にわたる共通管理策は、当該情報システムの構成要素であり、かつ、それらの管理策を継承する、各サブシステムの要求事項に適合する（あるいは、それらの要求事項を上回る）。セキュリティ管理策の選択および割り当てに関するアプローチの一つに、特定された個々のサブシステム（セクション 2.3.3 に記載されている動的サブシステムを含む）を分類することが挙げられる。各サブシステムを個別に分類したとしても、情報システム全体としての分類が変わることはない。むしろ、そうすることによって、NIST SP800-53 に記載されているセキュリティ管理策を個別に、かつ的を絞って各サブシステムに適用することが可能になり、より高位の影響のセキュリティ管理策をサブシステム全体にわたって導入することを回避できる。別のアプローチとして、

複雑な情報システム内の個々の小規模サブシステムを、より大規模なサブシステムにまとめたうえで、それらの大規模サブシステムに対して個別に分類を行い、必要に応じてそれらの大規模サブシステムにセキュリティ管理策を割り当てるといった方法がある。複雑な情報システム内の各サブシステムは、完結したシステムとして存在する可能性がある一方で、通常は相互に依存し結ばれているため、独立したエンティティとして扱われないことが多い。

特定された各サブシステムに対するセキュリティ分類の結果がそれぞれに異なる場合、組織は、サブシステム間のインターフェース、情報フロー、およびセキュリティ関連の依存関係[36]を慎重に調査し、サブシステムの相互接続における潜在的な脆弱性を削減、または除去するためのセキュリティ管理策を選択する。こうすることで、情報システムを適切に保護することができる[37]。サブシステムの相互接続に関するセキュリティ管理策は、各サブシステムが実施するセキュリティポリシーが異なる場合や、それらのサブシステムを管理する機関がそれぞれに異なる場合にも適用される。セキュリティ管理策がどの程度正しく導入されているか、どの程度意図した通りに運用されているか、その複雑な情報システムのセキュリティ要求事項に対する適合性の観点から望ましい結果をどの程度産出しているかについては、サブシステムレベルのセキュリティ管理策の評価結果をまとめ、サブシステム間のインターフェースに関する問題に対処するシステムレベルでの考察を追加することによって判断することができる。このアプローチにより、サブシステムのセキュリティ分類に従ってアセスメントに費やす作業レベルを測定したり、情報システムレベルのアセスメント結果を再利用することが可能となるため、より的を絞った、費用対効果の高いリスクマネジメントプロセスを構築できる。図 2-3 は、複雑な情報システムの分解の概念を示したものである。

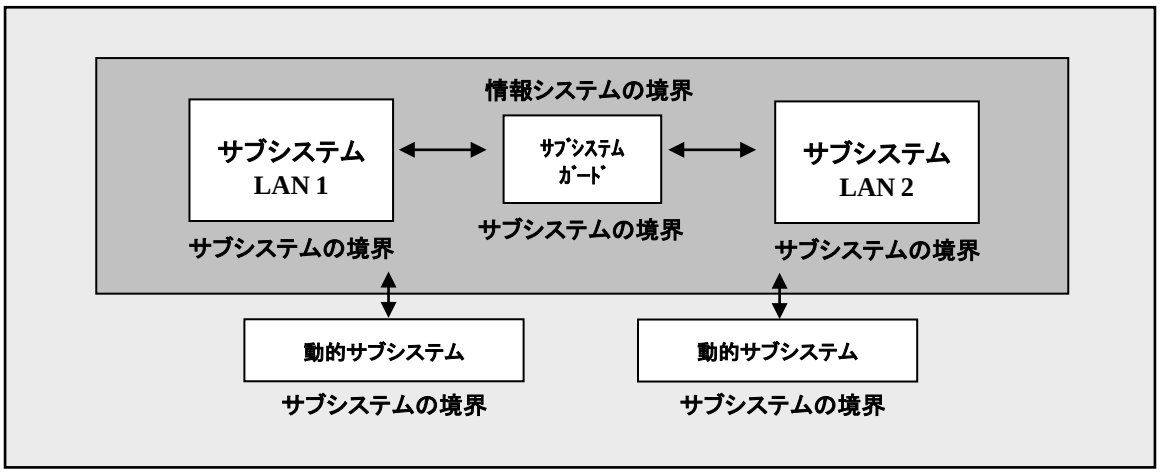

図 2-3: 複雑な情報システムの分解

[36] サブシステムのインターフェースには、ポートとプロトコルが含まれる。情報フローは、サブシステム間で伝送される情報を取り扱う。セキュリティ関連の依存関係とは、あるサブシステムによって実施されるセキュリティ機能／サービスが、それ以外の1つまたは複数のサブシステムにとって必要であることを示す。

[37] サブシステム間のインターフェースの種類や結合の種類によって、複合情報システムに思わぬ弱点および脆弱性が導入される可能性がある。たとえば、組織が有する大規模なイントラネットがエンタープライズサービスによって小規模サブシステムに分解され（たとえば、LAN セグメントなどの、切り離しが可能なサブシステム）、その後個別に分類が行われるとする。この場合、サブシステムレベルの特定の保護者が、当該システムの残りの部分に対して十分な保護を提供できないセキュリティ管理策を誤って選択・導入することによって、イントラネットに対する攻撃を許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ーフェースを慎重に検証し、この分野における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保証する。

上記の例では、2 つのローカルエリアネットワーク間の情報の流れを監視するシステムガードが情報システムに含まれている。この情報システムは、次のように、複数のサブシステムに分けることができる。(i) ローカルエリアネットワーク 1 (ii) ローカルエリアネットワーク 2 (iii) 2 つのネットワークを分離するシステムガード (iv) さまざまな時点でシステムの一部となる、複数の動的サブシステム（セクション 2.3.3 を参照）。情報システム内の各サブシステムは、個別に分類される可能性がある。情報システム全体としてのセキュリティ分類は、個々のサブシステムの分類結果をまとめて考慮したとしても、変わることはない。複雑な情報システム内のすべてのサブシステムに対する初期のセキュリティ管理策アセスメントが完了したら、組織は、次の項目を確実にするための追加措置を講じる。(i) サブシステムアセスメントに含まれなかったセキュリティ管理策の有効性を評価する、および (ii) 情報システムのセキュリティ要求事項に適合する形で、サブシステムを連携させる。[38]

2.3.3 技術の変化および情報システム境界への影響

現在の情報技術およびコンピューティングパラダイムが変化するにつれて、情報システムの境界の確立、ならびに、組織の情報システムが支援する任務および業務プロセスの保護といった従来のタスクが、より複雑になる。特に、ネット中心のアーキテクチャ [39]（たとえば、サービス指向型アーキテクチャ[SOA]、クラウドコンピューティングなど）では、(i) 動的サブシステム、および (ii) 外部サブシステムの 2 つの重要な概念を取り入れている。動的サブシステムと外部サブシステムの概念（後続のセクションに記載されている）は、新しい概念ではないが、ネット中心のアーキテクチャにおけるそれらのサブシステムの引用の普及と、その頻度の増加に伴い、組織が新たな難題に直面する可能性がある。

動的サブシステム

多くの情報システムにおいて、サブシステムに関する決定は、「システムの開始」段階で行われ、システムのライフサイクル全体を通して維持される。しかしながら、場合によっては、なかでもネット中心のアーキテクチャの場合には、システムを構成するサブシステムがライフサイクルのいずれかの段階で存在しないことがある。「システムの開始」よりも後の段階で情報システムに加わるサブシステムもあれば、「システムの終了」よりも前の段階で情報システムを離れるサブシステムもある。一般的に、それらの動的なサブシステムがシステム設計に含まれていて、適切なセキュリティ管理策がセキュリティ計画に反映されている場合には、前述の事態が発生しても、情報システムの外部境界が影響を受けることはない。しかしながら、ライフサイクルのいずれかの時点で境界の内部に存在するサブシステムは、影響を受けることになる。

さまざまな時点で組織の情報システムに加わる動的サブシステムは、組織の直接的な管理下にある場合と、そうでない場合がある。動的サブシステムは、外部プロバイダによって提供される可能性がある（たとえば、契約、省庁間の取り決め、業務分野についての取り決め、ライセンス契約および／またはサプライチェーンについての取り決めなど）。組織は、サブシステムを直接管理するか否かにかかわらず、そのサブシステムに期待される機能について考慮しなければならない。サブシステムを動的に追加または切り離した場合には、情報システム全体の再アセスメントが必要な場合と、そうでない場合がある。再アセスメントが必要か否かは、システム設計においてサブシステムに課

[38] 組織は、以下の事項を実施することができる。(i) 複雑な情報システム全体に対して単独の運用認可を与える（これには、個々のサブシステムのアセスメント結果と、システムレベルの追加アセスメントの結果をまとめることが含まれる）、または、(ii) その情報システムが複数の情報システムによって構成されている場合に、個別に認可された各情報システムを接続することにより生じるリスクを管理するための戦略を実施する。

[39] ネット中心のアーキテクチャは、情報の共有と連携を向上させるためにネットワークで相互接続された人、デバイス、情報およびサービスから成る、継続的に進化する複雑なコミュニティの一部であるサブシステムおよびサービスによって構成される、複雑な情報システムである。ネット中心のアーキテクチャの例として、サービス指向型アーキテクチャ（SOA）が挙げられる。

せられ、セキュリティ計画に記載される、制約および前提条件（たとえば、サブシステムが果たす機能、他のサブシステム、あるいは他の情報システムへの接続など）に基づいて決定される。明確化された制約と前提条件にサブシステムが適合していれば、それらのサブシステムを動的にシステムに追加したり、システムから切り離した場合に、システム全体の再アセスメントを実施する必要はない。

上で述べたように、動的サブシステムの制約と前提条件は、情報システムのデザインおよびセキュリティ計画に反映される。動的サブシステムがその制約と前提条件に適合しているか否かの判断は、リスクマネジメントプロセスの「継続的な監視」段階で行われる。適合に関する判断は、サブシステムの性質（機能、接続、およびサブシステムのプロバイダとの間で確立された相対的な信頼関係を含む）によって手動または自動で行われ、判断のタイミングはシステムに対するサブシステムの接続／切り離し時、またはその前になることが考えられる。

外部サブシステム

ネット中心のアーキテクチャにおいて明白であることが多い、もう一つの特徴として、一部のサブシステム（あるいは、サブシステムのコンポーネント）が、その情報システムを所有し、システムの運用を認可する組織の直接的な管理下にないことが挙げられる。[40] そのような外部サブシステムの性質は、外部のクラウドコンピューティングサービスを利用して情報を処理、格納、伝送する組織から、自身の管理下にあるプラットフォーム上で、なんらかの外部エンティティが開発したアプリケーション／サービスを稼動する組織まで、さまざまである。

付録I（外部環境におけるセキュリティ管理策）に記載されているように、FISMAおよびOMBポリシーは、連邦政府情報を扱う外部プロバイダ、または連邦政府の代わりに情報システムを運用する外部プロバイダに対して、連邦政府機関と同様のセキュリティ要求事項を満たすことを義務づけている。これらのセキュリティ要求事項は、連邦政府情報を格納、処理、または伝送する外部サブシステム、およびそれらの外部サブシステムが提供する、または、それらの外部サブシステムに関連する、あらゆるサービスに適用される。さらに、付録Iでは、外部サービスの使用により生じるリスクが受容できるレベルであること対する保証または信頼は、組織がその外部サービスプロバイダをどれだけ信頼しているかに依る、としている。場合によっては、信頼の度合いが、サービスを保護するのに必要なセキュリティ管理策の導入に関して、および、それらの管理策の有効性に関して提出される証拠に関して、組織が外部サービスプロバイダをどの程度直接管理できるかによって決まる。これ以外にも、外部サービスプロバイダに関して組織がどのような経験を有しているか、および、そのプロバイダが正しい行動を取っていることに関して組織がどの程度の信頼をおいているかなど、他の要素に基づいて信頼の度合いが決まることもある。ネット中心のアーキテクチャでは、信頼の度合いに関する問題を複雑にする可能性のある、さまざまな要因がある。これには、以下のものが含まれる。

- 外部エンティティが所有するものと、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（たとえば、組織が所有するプラットフォームによって、外部エンティティが開発したサービス／アプリケーションソフトウェアまたはファームウェアを実行している場合など）。
- サブシステム／サービスを提供する外部エンティティを組織が管理できる度合いは、極めて限られている場合がある。
- サブシステムの性質および内容は、急速に変化する可能性がある。

[40] ここでいう「サブシステム」という用語には、そのサブシステムが提供するサービスや、そのサブシステムに関連するサービスが含まれる。

- サブシステム／サービスは、きわめて重要な性質をおびているがゆえに、組織の情報システムに迅速に組み入れなければならない場合がある。

上記の要因がもたらす結果として、サブシステムが正しく機能することを検証したり、セキュリティ管理策の有効性を検証するための、従来の手法（たとえば、明確に定義された要求事項、設計分析、導入に先立つテストおよび評価）の一部がネット中心のサブシステム／サービスでは実現不能となる可能性がある。このような場合、組織は、当該サブシステム／サービスを許可する／含めるか否かについての判断材料として、ネット中心のサブシステム／サービスのプロバイダとの間に確立された信頼関係の性質に依存せざるをえなくなる（たとえば、承認されたプロバイダを記したGSAリストの使用）。もう一つの選択肢として、組織は、情報フローまたはプロセスフローの性質に制約を設けることによって、あらゆる潜在的マイナス影響を管理できることが確信できる場合に限って、それらの制約の下でそのサブシステム／サービスの使用を許可することができる。最後に、サブシステム／サービスを提供する外部プロバイダに対する信頼のレベルが期待を下回る場合、組織は、(i) 代替管理策を採用する (ii) より大きなリスクを受け入れる、または (iii) サービスを受けない（すなわち、主要な任務および業務を機能性のレベルを下げて、あるいは、機能性を伴わない形で実施する）。

2.4 セキュリティ管理策の割り当て

情報システムに対して組織が採用できるセキュリティ管理策の種類には、(i) システム固有の管理策（すなわち、特定の情報システムのみにセキュリティ機能を提供する管理策） (ii) 共通管理策（複数の情報システムにセキュリティ機能を提供する管理策） (iii) ハイブリッド管理策（システム固有と共通の、両方の特性を有する管理策）がある。[41] 組織は、自身のエンタープライズアーキテクチャおよび情報セキュリティアーキテクチャに適合するセキュリティ管理策を情報システムに割り当てる。[42] この活動は、運用認可責任者、情報システムのオーナー、最高情報セキュリティ責任者、上級情報セキュリティ責任者、エンタープライズアーキテクト、情報セキュリティアーキテクト、情報システムセキュリティ責任者、共通管理策の提供者、およびリスクエグゼクティブ（機能）が関与する、組織全体にわたる活動として実施される。

情報セキュリティアーキテクチャの一環として、組織には、共通の機能として複数の情報システムを効率的かつ効果的に支援することが可能なセキュリティ管理策（すなわち、共通管理策）を特定し、導入することが推奨される。共通管理策が特定の情報システムを支援するのに使用される場合、それらの管理策は、そのシステムによって「継承された管理策」とみなされる。共通管理策は、組織全体にわたる情報セキュリティの費用対効果と一貫性を向上させ、リスクマネジメント活動を単純化する役割を果たす。各セキュリティ管理策をシステム固有の管理策、ハイブリッド管理策、共通管理策のいずれかの管理策として情報システムに割り当てることによって、組織は、それらの管理策の全般的な開発、実施、アセスメント、認可、および監視に関する責任および説明責任を、組織内の特定のエンティティ（部署、人）に割り当てることになる。

異なる種類の「割り当て」対して、個々の「割り当て」に適したセキュリティ管理策ファミリー（あるいは、セキュリティ管理策）をNIST SP800-53 に記載されている管理策ファミリーから選択するにあ

[41] 情報システムのセキュリティ管理策に関する追加ガイダンスは、NIST SP800-53 に記載されている。

[42] ここでは、以下の項目を実施するために組織が採用するプロセスを指す用語として、「割り当て」を使用している。(i) 各セキュリティ管理策が、システム固有の管理策、ハイブリッド管理策、共通管理策のうち、いずれの管理策として定義されているかを判断する (ii) 特定のセキュリティ機能を提供することに責任を持つ特定の情報システムコンポーネント（たとえば、ルータ、サーバー、リモートセンサー）に、セキュリティ管理策を割り当てる。

たっては、かなりの柔軟性が組織に与えられている。セキュリティ管理策の「割り当て」プロセスには、セキュリティ管理策によってもたらされるセキュリティ機能の割り付けおよび提供が含まれるため、組織は、そのような機能を受ける／提供するすべてのエンティティ間で、効果的なコミュニケーションが行われることを確実にする。このコミュニケーションには、たとえば、共通管理策の運用認可判断の結果、および継続的な監視から得られる情報を、共通管理策を継承する組織内のエンティティがすぐに利用できるようにすること、ならびに、共通管理策になんらかの変更が加えられた場合にその影響を受ける人々に対して、その旨を効果的に伝達することが含まれる。[43] 図 2-4 に、組織におけるセキュリティ管理策の「割り当て」を図解する。この図には、RMFを使用して、シニアリーダー（運用認可責任者を含む）向けに、組織の各情報システムの現在のセキュリティ状態と、それらのシステムが支援する任務および業務プロセスに関する情報を生成する仕組みが含まれている。

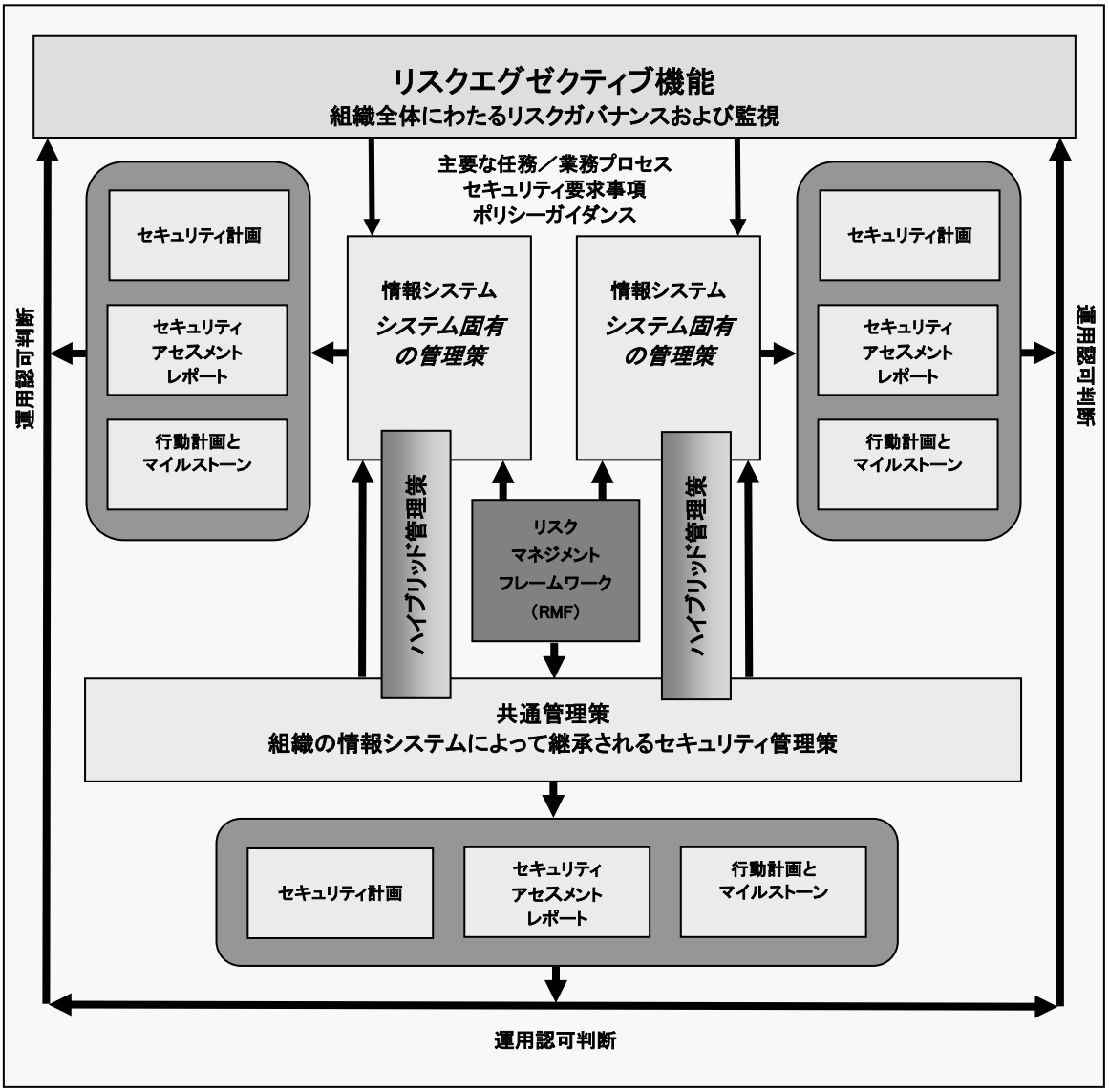

図 2-4: セキュリティ管理策の割り当て

[43] 共通（継承された）管理策のセキュリティ状態に関するコミュニケーションは、共通管理策の提供者が組織にとって内部である／外部であるにかかわらず必要不可欠である。外部環境におけるセキュリティ管理策に依存する組織が利用できるガイダンスは、付録 I に記載されている。その内容には、セキュリティ関連の適切な情報が外部プロバイダから組織に伝達されることを確実にするための、契約上の合意および約定の種類が含まれる。

第 3 章

プロセス

リスクマネジメントフレームワークの各タスクの実施

この章では、リスクマネジメントフレームワーク（RMF）を政府機関の情報システムに適用するプロセスについて記述する。[44] このプロセスには、明確な定義付けがされた組織上の任務の中から選択された任務を担う個人またはグループ（リスクエグゼクティブ[機能]、運用認可責任者、運用認可責任者が指名した代理人、最高情報責任者、上級情報セキュリティ責任者、エンタープライズアーキテクト、情報セキュリティアーキテクト、情報のオーナー／スチュワード、情報システムのオーナー、共通管理策の提供者、情報システムセキュリティ責任者、セキュリティ管理策アセサー）によって実行されるべき、明確な定義付けがされたリスク関連のタスクが含まれる。[45] 本文書内で定義付けがされているリスクマネジメントに関する役割の多くは、組織が実施する日常的なシステム開発ライフサイクルプロセスに関して定義付けがされている、いずれかの役割に対応している。主要な任務／業務プロセスに適合している場合で、かつ可能な場合は常に、組織は、リスクマネジメントに関する役割と、システム開発ライフサイクルプロセス向けに定義付けがされた類似の（または補足的な）役割との、対応づけを行う。RMFタスクは、適切な依存関係を考慮したうえで、システム開発ライフサイクルプロセスと共に、または、その一部として、実行される。これにより組織は、情報システム関連のセキュリティリスクを管理するプロセスをシステム開発ライフサイクルプロセスに効果的に組み入れることができる。

個々のRMFタスクに関する記述には、そのタスクを実施することに一義的な責任を負う個人またはグループ、そのタスクの完遂を支援するのに必要となる補助的な役割、そのタスクとの関連が最も深いシステム開発ライフサイクル上のフェーズ、そのタスクがどのように実行されるかを示す補足ガイダンス、および、そのタスクに関連する情報を提供する刊行物またはウェブサイトへの適切な参照が含まれる。[46] 組織が実行すべき主要なリスクマネジメント関連活動をまとめるために、RMFの各ステップに対して、マイルストーンチェックポイントが用意されている。マイルストーンチェックポイントには、組織に対する一連の質問事項が含まれていて、RMFの特定のステップに含まれる重要な活動が次のステップに進む前に完了していることを確認できるようになっている。

RMF タスク（複数）を実施するプロセス（すなわち、タスクが発生し実行される順序および形式、主要な／補助的な役割の名称、アーチファクトの名称およびフォーマット）は、組織によって、さまざまである。RMF の各タスクは、システム開発ライフサイクルの適切なフェーズにおいて実施される。RMF の各タスクは、シーケンシャルな順序で現れるが、リスクマネジメントプロセスの多くの地点で、シーケンシャルな順序からの逸脱が必要となる場合がある（タスクと再訪されるタスク間の、反復サイクルの必要性を含む）。たとえば、セキュリティ管理策アセスメントの結果が、情報システムのオーナーによる是正活動の誘因となり、その結果セキュリティ管理策の再アセスメントが必要になること

[44] 本文書に記載されているリスク管理プロセスは、連邦政府内の多くの利益共同体（たとえば、民間、防衛、およびインテリジェンスコミュニティを含む）のニーズを満たすために調整することができる。この調整によって、RMF に関連するリスクマネジメント概念を関係組織および情報システムに最も適した形で適用するための、柔軟性が組織に与えられる。

[45] 組織のリスクマネジメントプロセスに関与する主要な関係者の役割および責任については、付録 D に記載されている。

[46] 参照は、以下の条件が満たされる場合に、RMF タスクリストに含まれる。(i) 通常、その参照が、国家安全保障にかかわるシステムと、そうでないシステムの、両方に適用される (ii) 国家安全保障にかかわらないシステムに対する参照であり、それと同等の、または、補足的な参照が、国家安全保障にかかわるシステム向けに用意されている (iii) その参照が、NIST が発行する特定の標準またはガイダンスの実施に関する、特定の国家安全保障コミュニティガイダンスに関連している。

がある。情報システムに導入されているセキュリティ管理策の監視を行うことによって、システムやその運用環境に対する変更の追跡、セキュリティ影響分析の実施、是正活動の実施、セキュリティ管理策の再アセスメント、ならびにシステムのセキュリティ状態についての報告といった、サイクルが発生する可能性がある。上記以外でも、RMF タスクのシーケンシャルな性質から逸脱することが効率的であり、かつ、費用対効果も高い場合には、そのようにすることが考えられる。たとえば、セキュリティ管理策アセスメントタスクは、セキュリティ管理策実施タスクの後にリストアップされるが、組織によっては、セキュリティ計画に記載されているすべての管理策の実施を待たずに、特定の管理策を実施直後にアセスメントすることを選択する場合がある。この場合、（後に実施される可能性がある）情報システムのハードウェアおよびソフトウェアコンポーネントに導入されているセキュリティ管理策のアセスメントの前に、施設内で、物理的および環境的保護管理策のアセスメントが実施される可能性がある。タスクの順序付けがどうなっているかにかかわらず、情報システムの運用を開始する前に実施すべき最後のステップは、運用認可責任者がリスクを明示的に受容することである。

RMF の各ステップ、および関連する各タスクは、新規開発した情報システムおよびレガシーシステムの両方に適用することができる。レガシーシステムでは、RMF のステップ 1 から 3 を用いて、セキュリティ分類が完了していて、かつ、適切であること、および、必要なセキュリティ管理策の選択と割り当てが完了していることを確認する。レガシーシステムに RMF の最初の 3 つのステップを適用することは、必要、かつ十分なセキュリティ管理策（すなわち、システム固有の管理策、ハイブリッド管理策、および共通管理策）の選択および割り当てが適切に行われたかどうかを判断するための、ギャップ分析とみなすことができる。セキュリティ管理策の弱点および欠陥が発見された場合には、新規開発システムと同様に、RMF のステップ 3 から 6 を用いて対処することができる。ギャップ分析を実施中に、セキュリティ管理策の弱点または欠陥が発見されなかった場合で、かつ、現時点で有効なセキュリティ運用認可が存在する場合、組織は、RMF の最後のステップである「継続的な監視」に進むことができる。現時点で有効なセキュリティ運用認可が存在しない場合は、RMF のステップ 4 から 6 を実施する。

セキュリティ分類プロセスは、RMF タスクの実施に必要な作業レベルに影響を与える。セキュリティ分類によって示されるとおり、組織内の最も重要な／機密性の高い業務と資産を支援する情報システムにおいては、適切な情報セキュリティとリスク軽減を実現するためにも、最大レベルの注意と取り組みが必要となる。RMF タスク（複数）の大半は、適切な契約上の合意やその他の約定を結ぶことによって、外部プロバイダに実行させることができる（付録 I を参照）。RMF の各タスクの概要をまとめた表は、付録 E に記載されている。

リスクマネジメントフレームワークの適用

リスクマネジメントフレームワークおよび関連する RMF タスクは、**情報システムのオーナー**と**共通管理策の提供者**の両方に適用される。情報システムの運用認可を支援するのに加えて、RMF タスクは、組織の情報システムが継承する共通管理策の選択、開発、実施、アセスメント、運用認可、および継続的な監視を支援する。共通管理策の提供者（組織にとって内部・外部の両方）による RMF タスクの実施により、共通管理策によって提供されるセキュリティ機能が、情報の保護に関する彼らのニーズに適した保証レベルで、情報システムオーナーによって継承される。このアプローチでは、情報システムおよび、それらのシステムを支援するインフラに導入されるセキュリティ管理策の有効性の重要性を認識している。

RMF の各タスクは、**シーケンシャル**に記述されているが、組織は、組織が確立したマネジメントおよびシステム開発ライフサイクルプロセスに適合させるために、あるいは、タスクの実施に関して、より費用対効果が高く効率的なソリューションを実現するために、シーケンシャルな構造からの逸脱を選択してもよい。タスクの順序付けがどうなっているかにかかわらず、情報システムの運用を開始する前に実施すべき最後のステップは、運用認可責任者がリスクを明示的に受容することである。組織は、RMF の特定のタスクを反復する形で実施したり、システム開発ライフサイクルの異なるフェーズにおいて実施することもできる。たとえば、セキュリティ管理策アセスメントは、システム開発時、システム導入時、およびシステム運用／保守時（継続的な監視の一環として）に実施される可能性がある。

組織は、組織内の選択されたプロセスおよび活動の熟成度に基づいて、RMF の特定のタスクに対しては、大きな**労力**をかけて、残りのタスクに対しては、より少ないリソースを割り当ててもよい。RMF は、ライフサイクルをベースしているため、情報システムやその運用環境に対する変更を組織がどのように管理するかによっては、時間の経過とともに多くのタスクを再訪する必要性が生じる。情報システムに対する情報セキュリティ関連リスクの管理は、シニアリーダーが実施する、組織全体にわたる大規模のリスクマネジメント活動の一部とみなされている。RMF によって、情報システムの運用および使用により生じるリスクを軽減するための統制のとれた構造化されたアプローチと、極めて動的な運用環境において組織の主要な任務および業務を支援するのに必要な柔軟性と機敏さとの、両方が同時に提供されなければならない。

3.1 RMF ステップ 1ー情報システムの分類

セキュリティ分類

タスク 1-1: 情報システムを分類し、セキュリティ分類の結果をセキュリティ計画に記載する。

主な責任を持つ者: 情報システムのオーナー、情報のオーナー／スチュワード

補助的な役割: リスクエグゼクティブ（機能）、運用認可責任者または指名された代理人、最高情報責任者、上級情報セキュリティ責任者、情報システムセキュリティ責任者

SDLCのフェーズ: 開始（コンセプト／要求事項の定義）

補足ガイダンス: セキュリティ分類プロセスは、情報システムのオーナーと情報のオーナー／スチュワードが、組織内の適切な職員（すなわち、任務／業務機能および／またはリスクマネジメントに責任を持つシニアリーダー）と連携・協調して実施する。セキュリティ分類プロセスは、エンタープライズアーキテクチャと情報セキュリティアーキテクチャを考慮した、組織全体にわたる活動として実施される。これにより、個々の情報システムが、組織の任務および業務上の目的に基づいて分類される。セキュリティ分類プロセスの結果は、情報システムに導入する適切なセキュリティ管理策の選択、および、該当する場合には、システムに対する最低限の保証要件に影響を与える。組織には、情報システムを複数のサブシステムに分解することによって、より効率的、かつ効果的にセキュリティ管理策をシステムに割り当てるといった選択肢もある。そのためのアプローチの一つに、特定された個々のサブシステム（動的サブシステムを含む）を分類することが挙げられる。各サブシステムを個別に分類したとしても、情報システム全体としての分類が変わることはない。むしろ、そうすることによって、NIST SP800-53 に記載されているセキュリティ管理策を個別に各サブシステムに割り当てることが可能になり、より高位の影響のセキュリティ管理策をサブシステム全体にわたって導入することを回避できる。別のアプローチとして、情報システム内の個々の小規模サブシステムを、より大規模なサブシステムにまとめたうえで、それらの大規模サブシステムに対して個別に分類を行い、必要に応じてそれらの大規模サブシステムにセキュリティ管理策を割り当てるといった方法がある。セキュリティ分類に関する情報は、セキュリティ計画のシステムの識別に関するセクションに記載される、または、セキュリティ計画の添付文書に含まれる。リスクエグゼクティブ（機能）は、組織のリスクマネジメント戦略に関するガイダンス、および関連情報を運用認可責任者に提供する（たとえば、組織が採用するリスクアセスメント方法論、特定されたリスクの評価、リスク軽減アプローチ、組織が定めたリスク許容度、長期にわたってリスクを監視するためのアプローチ、現行の情報システムが直面している既知のリスクの集約、リスクに関するその他の情報源）。セキュリティ分類に関する決定では、組織の業務、組織の資産、個人、他の組織、および国家に対する潜在的なマイナスの影響を考慮する。

参考文書: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-59, 800-60; CNSS Instruction 1253。

情報システムに関する記述

タスク 1-2: 情報システム（システム境界を含む）について説明し、その内容をセキュリティ計画に記載する。

主な責任を持つ者: 情報システムのオーナー

補助的な役割: 運用認可責任者または指名された代理人、上級情報セキュリティ責任者、情報のオーナー／スチュワード、情報システムセキュリティ責任者

SDLCのフェーズ: 開始（コンセプト／要求事項の定義）

補足ガイダンス: 情報システムに関する記述は、セキュリティ計画のシステムの識別に関するセクションに記載されるか、セキュリティ計画の添付文書に含まれるか、あるいは、システム開発ライフサイクルの一環として生成される情報の、その他の標準的な情報源から参照される。情報の重複は、可能な場合には常に、回避する。セキュリティ計画における詳細さのレベルは組織によって決定され、通常は、情報システムのセキュリティ分類に対応する。システム開発ライフサイクルにおいて、および RMF の各タスクの実施時に利用可能になった情報は、システムに関する記述に追加される場合がある。システムに関する記述には、たとえば、以下の項目が含まれる。

- 情報システムの記述的なフルネーム（対応する略称を含む）
- 情報システムに割り当てられた一意の識別子（番号またはコードであるのが一般的）
- 情報システムのオーナーと運用認可責任者（連絡先情報を含む）
- 情報システムを管理、所有、および／または制御する親組織、または運営組織
- 情報システムの設置場所および運用環境

- 情報システムのバージョンまたはリリースナンバー
- 情報システムの目的、機能、および能力、ならびに、システムが支援する任務／業務プロセス
- 情報システムがどのようにしてエンタープライズアーキテクチャと情報セキュリティアーキテクチャに組み込まれるか
- 調達やシステム開発ライフサイクルに関する、情報システムの状態
- 情報および情報システムのセキュリティ分類プロセスの結果
- 情報システムが処理、格納、および伝送する情報の種類
- リスクマネジメントおよびセキュリティ運用認可を目的として設定される情報システムの境界
- 情報システムのセキュリティに影響を与える適用される法律、指令、方針、規制、または基準
- 情報システムのアーキテクチャに関する記述（ネットワークトポロジーを含む）
- 情報システムに含まれるハードウェア／ファームウェアデバイス
- 情報システム上のシステムおよびアプリケーションソフトウェア
- ハードウェア、ソフトウェア、およびシステムのインターフェース（内部および外部）
- 情報システムに関連する（静的および動的）サブシステム
- 情報システム内の情報のフローおよび経路（インプットとアウトプットを含む）
- クロスドメインデバイス／要求事項
- 外部情報システムと通信するための、ネットワーク接続に関するルール
- 相互接続された情報システムおよび、それらのシステムの識別子
- 情報の処理、伝送、および格納に使用される暗号化技術
- 暗号鍵の管理に関する情報（公開鍵基盤、認証局など）
- 情報システムのユーザ（該当する場合、関係組織、アクセス権限、特権、市民権が含まれる）
- 情報システムのオーナーシップ／運営（たとえば、政府が所有・運営するシステム、政府が所有し、請負業者が運営するシステム、請負業者が所有・運営するシステム、連邦政府以外[州政府および地方政府、被譲与者]）
- セキュリティが認可された日付と、認可が終了する日付
- インシデント対応に関する連絡窓口
- 組織が必要とするその他の情報

参考文書: なし。

情報システムの登録

タスク 1-3: 組織内の適切な計画局／管理局に情報システムを登録する。

主な責任を持つ者: 情報システムのオーナー

補助的な役割: 情報システムセキュリティ責任者

SDLCのフェーズ: 開始（コンセプト／要求事項の定義）

補足ガイダンス: 登録プロセスは、情報システムインベントリに含まれる情報システム（および、該当する場合は、サブシステム）を特定することから始まり、情報システムと、そのシステムを所有、管理、および／または制御する親組織または運営組織との関係を確立する。情報システムの登録では、組織の方針に従って、セキュリティ計画のシステムの識別に関するセクションに記載されている情報を使用して、次の事項を親組織または運営組織に通知する。(i) 当該情報システムの存在 (ii) システムの主な特徴 (iii) システムの継続的な運用が組織にもたらすセキュリティ上の影響。情報システムの登録によって、適用される法律、大統領令、指令、ポリシー、基準、ガイダンス、または規則に準拠したセキュリティ状況報告に必要な、効果的な管理／追跡ツールが、組織に提供される。より動的なサブシステム（ネット中心のアーキテクチャにおけるサブシステム）は、システム開発ライフサイクルのいずれかのフェーズにて存在しない可能性がある。そのようなサブシステムは、明確な定義付けがされた情報システムのサブセットとして登録されるか、あるいは、実現可能な限り多くの情報を含めることが可能な手法を用いて、サブシステムの登録が行われる。動的サブシステムに関する情報の中には、そのサブシステムが情報システムに姿を現わす前に、既知の情報となるものもある（たとえば、セキュリティ計画に記載されている前提条件および制約など）。しかしながら、より詳細な情報は、そのサブシステムが姿を現わすまで知りえない可能性がある。

参考文書: なし。

マイルストーンチェックポイント #1

- 組織は、情報システム（そのシステムが処理、格納、および伝送する情報を含む）の**セキュリティ分類**を完了したか？
- 情報システムのセキュリティ分類プロセスの結果は、組織の**エンタープライズアーキテクチャ**、および**組織の任務／業務プロセスの保護**に対するコミットメントに適合するものであるか？
- セキュリティ分類プロセスの結果は、組織の**リスクマネジメント戦略**を反映しているか？
- 組織は情報システムの**特徴**を適切に記述しているか？
- 組織は、情報システムの管理、説明責任、調整、および監視を目的として、そのシステムの**登録**を完了しているか？

3.2 RMF ステップ 2ーセキュリティ管理策の選択

共通管理策の明確化

タスク 2-1: 組織の情報システムに対する共通管理策として組織が提供しているセキュリティ管理策を明確にし、セキュリティ計画（またはそれと同等の文書）に記載する。

主な責任を持つ者: 最高情報責任者または上級情報セキュリティ責任者、情報セキュリティアーキテクト、共通管理策の提供者

補助的な役割: リスクエグゼクティブ（機能）、運用認可責任者または指名された代理人、情報システムのオーナー、情報システムセキュリティエンジニア

SDLCのフェーズ: 開始（コンセプト／要求事項の定義）

補足ガイダンス: 共通管理策は、組織の単独または複数の情報システムによって継承されるセキュリティ管理策である。共通管理策は、情報セキュリティアーキテクトの協力のもと、最高情報責任者および／または上級情報セキュリティ責任者によって明確化され、それらの管理策の開発、実施、アセスメント、および監視の責任は、組織内の特定のエンティティに割り当てられる。共通管理策が情報システム内に存在する場合、情報システムのオーナーが共通管理策の提供者であることも考えられる。組織が共通管理策を特定する際には、情報システムのオーナーに助言を求めることによって、継承される管理策が提供するセキュリティ機能によって、適切な保護が提供されることを保証する。組織が提供する共通管理策が、それらの管理策を継承する情報システムに対して十分な保護を提供できない場合には、そのシステムのオーナーがシステム固有の管理策やハイブリッド管理策によってそれらの共通管理策を補足して、システムに必要な保護を実現する、および／または、より大きなリスクを受け入れる。共通管理策を継承する情報システムのオーナーは、それらの管理策の実施について個々のセキュリティ計画に記載するか、あるいは、共通管理策の提供者のセキュリティ計画に含まれる、共通管理策についての記述への参照を含める。組織は、共通管理策の明確化およびセキュリティ管理策の選択をシステム開発ライフサイクルの後のフェーズに先送りしてもよい。共通管理策が情報システム内に存在しない場合（たとえば、物理的および環境的保護管理策、人的セキュリティ管理策など）、組織は、それらの管理策の運用認可責任者として、組織内の単独または複数の上級職員または管理職者を選定する。運用認可責任者は、共通管理策の提供者によって提供され、組織の情報システムによって継承されるセキュリティ管理策を導入することにより生じる、組織の業務や資産、個人、他の組織、および国家に対するリスクを受容することに責任を持つ。共通管理策の提供者は、以下の項目の実施に責任を負う。(i) 共通管理策についてセキュリティ計画（または、組織が提供する同等の文書）に記載する (ii) 共通管理策を確実に導入・実施し、それらの管理策の有効性が、資格を持ち、組織が求めるレベルの独立性を有するアセサーによって確実に評価されるようにする (iii) 評価結果をセキュリティアセスメントレポートに記載する (iv) 有効でないとみなされたすべての共通管理策（すなわち、受容できない弱点または欠陥を有する管理策）に対する行動計画とマイルストーンを作成する (v) 組織指定の運用認可責任者による、共通管理策の運用認可を受ける (vi) 共通管理策の有効性を継続的に監視する。

共通管理策のセキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーン（または、そうした情報の要約）は、それらの管理策に対する責任と説明責任を負う上級職員または管理職者によってレビュー・承認された後に、情報システムのオーナー（共通管理策を継承するシステムのオーナー）が利用できるようになる。通常、共通管理策は組織内の複数の情報システムを支援するため、組織は、この情報が共通管理策の提供者によって最新に保たれるようにする。共通管理策のセキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーンは、組織内の運用認可責任者が、自身の情報システムのセキュリティ運用認可プロセスにおいてリスクに基づいた決定を行うために使用する。共通管理策の使用については、それらの管理策を継承する情報システムのセキュリティ計画に記載される。組織は、共通管理策の状態が変化した場合で、かつ、それにより共通管理策が提供する（かつ、共通管理策に期待される）保護にマイナスの影響が及ぶ場合に、その旨を迅速に配信する能力が、管理策の提供者に備わっていることを確認する。共通管理策の提供者は、継承された共通管理策に問題が発生した場合に、その旨を迅速に情報システムオーナーに知らせることができる（たとえば、特定の共通管理策のアセスメントまたは再アセスメントの結果によって、その管理策になんらかの欠陥があることが示された場合、新たな脅威または攻撃手法が出現し、その脅威または攻撃手法からの保護に関する共通管理策の有効性が低下した場合）。可能な場合には、組織内の各情報システムで使用されている特定の共通管理策についての記録を維持する自動化されたマネジメントシステムを導入することが推奨される。そうすることで、情報システムのオーナーとの迅速なコミュニケーションを取るための、共通管理策の提供者の能力が向上する。共通管理策が、組織にとって外部のエンティティ（たとえば、共有サービスプロバイダ／外部サービスプロバイダなど）によって組織（および組織の情報システム）に提供される場合には、導入される管理策の有効性に関する情報を組織が得られるようにするための取り決めが、

外部／共有サービスプロバイダとの間で交わされる。共通管理策の有効性に関して外部組織から得た情報は、運用認可判断を下す際に考慮される。

参考文書: FIPS Publications 199, 200; NIST Special Publications 800-30, 800-53; CNSS Instruction 1253。

セキュリティ管理策の選択

タスク 2-2: 情報システムに導入するセキュリティ管理策を選択し、それらの管理策について、セキュリティ計画に記載する。

主な責任を持つ者: 情報セキュリティアーキテクト、情報システムのオーナー

補助的な役割: 運用認可責任者または指名された代理人、情報のオーナー／スチュワード、情報システムセキュリティ責任者、情報システムセキュリティエンジニア

SDLCのフェーズ: 開始（コンセプト／要求事項の定義）

補足ガイダンス: セキュリティ管理策は、情報システムのセキュリティ分類に基づいて選択される。セキュリティ管理策の選択プロセスには、必要に応じて、以下の項目が含まれる。(i) 一連のベースラインセキュリティ管理策を選択する (ii) スコーピング、パラメータ化、および代替管理策ガイダンスを適用して、ベースラインセキュリティ管理策を調整する (iii) 必要な場合、リスクアセスメント（正式なものと、そうでないもの）結果と、ローカルな状況（運用環境、組織固有のセキュリティ要求事項、脅威に関する具体的な情報、費用対効果分析結果、または特別な状況を含む）に基づいた組織固有のニーズを満たすために、追加的な管理策および／または管理強化策をよって調整済みのベースラインセキュリティ管理策を補足する、および (iv) 必要に応じて、最低限の保証要件を示す。組織は、セキュリティ管理策の選択プロセスにおいて下された決定事項（たとえば、調整、補足などに関して）を、健全な根拠とともに、セキュリティ計画に記載する。セキュリティ計画には、情報システムのセキュリティ要求事項の概要が十分に詳細なレベルで記載されていて、選択されたセキュリティ管理策がそれらの要求事項を満たすか否かを、組織が判断できるようになっている。セキュリティ計画には、実施すべきセキュリティ管理策のリストに加えて、各管理策がその情報システムの状況に応じて何を意図して適用されるかについての記述が十分な詳細さで記載される。これは、管理策が意図したとおりに実施されるようにするためにも重要である。組織は、セキュリティ管理策の選択プロセスにおいて、監視に関する戦略を策定し、継続的な監視プロセスの計画作成に着手することができる。この戦略には、たとえば、特定のセキュリティ管理策の変わりやすさ（volatility）や、それらの管理策に対する適切な監視頻度など、監視に関する基準が含まれる場合がある。セキュリティ管理策の変わりやすさ、およびセキュリティ管理策の監視頻度については、管理策の選択時に対処し、そこで得た情報を継続的な監視プロセスへのインプットとすることもできる。監視戦略は、リアルタイムに近いリスクマネジメントと継続的な運用認可（タスク 2-3 を参照）の概念を支援するために、セキュリティ計画に含めることができる。共通管理策を継承する情報システムのオーナーは、それらの管理策の実施について個々のセキュリティ計画に記載するか、あるいは、共通管理策の提供者のセキュリティ計画に含まれる、共通管理策についての記述への参照を含める（タスク 2-1 を参照）。情報システムのオーナーは、彼らが所有する個々のシステムが継承する共通管理策が適切であるか否かの判断を下す際に、共通管理策の提供者が用意したセキュリティ運用認可パッケージを参照することができる。

情報システムに対するサブシステムの動的な追加や切り離しが可能なネット中心のアーキテクチャを採用する場合、組織は、情報システムのセキュリティ計画に以下の項目を含める。(i) 動的サブシステムの機能についての記述 (ii) サブシステムに導入されるセキュリティ管理策 (iii) 動的サブシステムの機能、および、それらのサブシステムに導入されるセキュリティ管理策の機能に関する制限／前提条件 (iv) 動的サブシステムに導入されるセキュリティ管理策が正しく機能することと、他のサブシステムとの、依存関係 (v) 動的サブシステムがセキュリティ計画、前提条件、および制約に適合するか否かを判断するための手順 (vi) 動的サブシステムおよび関連するセキュリティ管理策によってもたらされる、情報システムに導入されている既存のセキュリティ管理策への影響。動的サブシステムを含めることによって、情報システム、または、現時点で特定されているサブシステムのうち、一部のサブシステムに影響が生じる可能性がある一方で、動的サブシステムが、その情報システムまたは他のサブシステムのセキュリティに影響を与えるとは限らない。つまり、すべてのサブシステムがセキュリティ面でつながっているわけではない。ネット中心のアーキテクチャに対する、セキュリティ計画上予想される制限を超える変更は許可されない、または、変更が承認される前に再アセスメントが必要となる場合がある。セキュリティ管理策が共通管理策として指定された場合、組織は、リスクマネジメントプロセスを支援するのに十分な情報を情報システムのオーナーおよび運用認可責任者が確実に利用できるようにする。セキュリティサービスが外部プロバイダによって提供される場合（たとえば、契約、省庁間の取り決め、業務分野についての取り決め、ライセンス契約および／またはサプライチェーンの取り決めなどを介して）、組織は、以下の項目を実施する。 (i) 組織に提供される外部サービスを定義する (ii) 組織のセキュリティ要求事項

に応じて外部サービスがどのように保護されるかについて説明する、ならびに (iii) 外部サービスの利用により生じる、組織の業務や資産、個人、他の組織、および国家に対するリスクが許容範囲内に収まることに対する保証を得る。また、組織は、複雑な情報システム内の複製されたサブシステムによって、一般的な脅威源が利用する可能性のある一般的な脆弱性が導入される可能性についても考慮し、必要な場合には、リスク軽減策として組織が依存する可能性のある「システムの冗長（redundancy）」を無効にする。システムを構成する複数のサブシステムのうち、一つのサブシステムに対するセキュリティインシデントが発生した場合、その影響はカスケード化し、他の多くのサブシステムに同時に影響を与える可能性がある。

参考文書: FIPS Publications 199, 200; NIST Special Publications 800-30, 800-53; CNSS Instruction 1253。

監視戦略

タスク 2-3: セキュリティ管理策の有効性、ならびに、情報システムおよびシステムの運用環境に対して提案されている、あるいは、実際に実施された変更を継続的に監視するための、戦略を策定する。

主な責任を持つ者: 情報システムのオーナーまたは共通管理策の提供者

補助的な役割: リスクエグゼクティブ（機能）、運用認可責任者または指名された代理人、最高情報責任者、上級情報セキュリティ責任者、情報のオーナー／スチュワード、情報システムセキュリティ責任者

SDLCのフェーズ: 開始（コンセプト／要求事項の定義）

補足ガイダンス: 情報システムに導入される、または情報システムによって継承されるセキュリティ管理策の継続的な監視は、リスクマネジメントの重要な側面である。効果的な監視戦略は、システム開発ライフサイクルの早い段階（すなわち、システム設計または COTS（民生品）の購入に関する決定の段階）で策定される。厳格な継続的監視プログラムを実施することによって、組織は、長期にわたって情報システムのセキュリティ状態を把握し、変化する脅威、脆弱性、テクノロジー、および任務／業務機能を伴う極めて動的な運用環境において、初期のセキュリティ運用認可を維持することができる。自動化ツールと支援データベースを用いてセキュリティ管理策を継続的に監視することによって、情報システムに対するリアルタイムに近いリスクマネジメントが容易になる。効果的な監視プログラムには、(i) 構成管理および構成制御プロセス (ii) 情報システムおよびシステムの運用環境に対して提案されている、あるいは、実際に実施された変更がもたらすセキュリティ影響の分析 (iii) 情報システムに導入される、または情報システムによって継承されるセキュリティ管理策（動的サブシステムに導入される管理策を含む）のアセスメント、および (iv) 組織内の適切な職員へのセキュリティ状況の報告。情報システムの継続的監視戦略によって、監視すべきセキュリティ管理策、監視頻度、および管理策のアセスメントアプローチが特定される。この戦略によって、情報システムに対する変更の監視方法、セキュリティ影響分析の実施方法、およびセキュリティ状況報告に関する要求事項（報告を受ける者を含む）が明確になる。.

導入後に監視すべきセキュリティ管理策の選択、および監視頻度の決定に関する基準は、組織内の選定された職員（たとえば、運用認可責任者または指名された代理人、最高情報責任者、上級情報セキュリティ責任者、およびリスクエグゼクティブ（機能）が含まれる）の協力のもと、情報システムのオーナーまたは共通管理策の提供者によって定められる。この選択基準は、組織の業務や資産、個人、他の組織、および国家に対する情報システムの優先事項と重要性を反映したものである。変化しやすい（すなわち、時間の経過とともに変化する可能性が最も高い）セキュリティ管理策、組織の保護戦略の特定の側面にとって極めて重要である管理策、または、現行の行動計画とマイルストーンに記載されている管理策については、その機能の重要性と監視ツールの能力に適合する頻度でアセスメントが実施される。セキュリティ管理策アセスメントの頻度とボリュームが増加した場合にも、自動化ツールを使えば容易に対処できる。

情報システムによって継承されるセキュリティ管理策（すなわち、共通管理策）のアセスメント頻度を決定するプロセスには、共通管理策の提供者をどれだけ信頼できるかについての組織の判断が含まれる。組織が実施するリスクアセスメント（正式なものと、そうでないもの）の結果も、監視すべきセキュリティ管理策を選択し、それらの管理策に対する監視頻度を決定する際に、使用できる。継続的な監視段階におけるセキュリティ管理策アセスメントアプローチには、情報システムコンポーネントのステータスの把握、運用履歴データの分析、および初期の運用認可判断を支援したアセスメント手順と結果の再利用が含まれる場合がある。

継続的に監視すべき一連のセキュリティ管理策および監視活動の頻度を含む、監視戦略は、運用認可責任者または指名された代理人によって承認される。監視戦略の承認は、セキュリティ計画の承認と併せて得ることも可能である。セキュリティ管理策の監視は、システム開発ライフサイクル全体を通して実施される。セキュリティ管理策が動的サブシステムを伴う情報システムに導入されている場合、システム開発ライフサイクルの初期に存在しなかったサブ

システムについての説明が、監視戦略を持ってなされる。動的サブシステムに対する効果的な監視戦略によって、(i) サブシステムの追加や切り離しのたびに情報システムの再運用認可を求めることによって不要な、あるいは現実的でない負担を組織に負わせる (ii) 一度受け入れたシステム全体のセキュリティ状態について妥協する、といったことを実施しない場合に生じるリスクとの、適切なバランスを実現することができる。

参考文書: NIST Special Publications 800-30, 800-39, 800-53; 800-53A; CNSS Instruction 1253。

セキュリティ計画の承認

タスク 2-4: セキュリティ計画をレビューし、承認する。

主な責任を持つ者: 運用認可責任者または指名された代理人

補助的な役割: リスクエグゼクティブ（機能）、最高情報責任者、上級情報セキュリティ責任者

SDLCのフェーズ: 開発／調達

補足ガイダンス: 上級情報セキュリティ責任者、最高情報責任者、およびリスクエグゼクティブ（機能）の支援をもとに、運用認可責任者または指名された代理人が実施するセキュリティ計画の独立したレビューは、その計画が完全であり、一貫性があり、かつ、その情報システムのセキュリティ要求事項を満たしているか否かの判断を支援する。また、セキュリティ計画のレビューでは、計画または運用に関して入手可能なドキュメントが最大限に活用され、このレビューによって、セキュリティ計画に記載されているセキュリティ管理策が意図したとおりに実施された場合に生じる組織の業務や資産、個人、他の組織、および国家に対する潜在的なリスクがセキュリティ計画によって正確に、かつ、効果的に明確化されているか否かの判断も支援される。このような独立したレビューや分析の結果をもとに、運用認可責任者または指名された代理人、最高情報責任者、上級情報セキュリティ責任者、またはリスクエグゼクティブ（機能）は、セキュリティ計画の変更を推奨する場合がある。セキュリティ計画が受容できないと考えられる場合、運用認可責任者または指名された代理人は、情報システムのオーナー（または共通管理策の提供者）が次に適切な活動を実施することができるように、その計画を差し戻す。セキュリティ計画が受容できると考えられる場合には、運用認可責任者または指名された代理人がその計画を承認する。セキュリティ計画の受容は、リスクマネジメントプロセスとシステム開発ライフサイクルの両方の主要なマイルストーンを表している。セキュリティ計画を承認することによって、運用認可責任者または指名された代理人は、情報システムのセキュリティ要求事項を満たすために提案されている一連のセキュリティ管理策（システム固有の管理策、ハイブリッド管理策、および／または共通管理策）に同意することになる。この承認によって、リスクマネジメントプロセスは RMF の次のステップ（すなわち、セキュリティ管理策の実施）に進むことができる。セキュリティ計画が承認されることによって、RMF の残りのステップを成功裏に完了させるのに必要な作業レベルが定まり、情報システム、サブシステム、またはコンポーネントの調達に関するセキュリティ仕様のベースが提供される。

参考文書: NIST Special Publications 800-30, 800-53; CNSS Instruction 1253。

マイルストーンチェックポイント #2

- 組織は、すべてのセキュリティ管理策を、システム固有の管理策、ハイブリッド管理策、または共通管理策として、**情報システム**に割り当てているか？
- 組織は、セキュリティ管理策の選択プロセスを通知・誘導するにあたって、自身の**リスクアセスメント**（正式なものと、そうでないもの）を用いたか？
- 組織は、情報システム、およびそのシステムが継承するすべての共通管理策に対する**運用認可責任者**を明確にしているか？
- 組織は、セキュリティ管理策が実施された場合に、組織の業務や資産、個人、他の組織、および国家に対するリスクが十分に軽減されることを確実にするための、ベースラインセキュリティ管理策の**調整**および**補足**を行っているか？
- 組織は、情報システムに導入されている、または情報システムによって継承されたセキュリティ管理策の**最低限の保証要件**を取り扱っているか？
- 組織は、**共通管理策を特定する**際に、それらの継承される管理策が提供するセキュリティ機能によって、適切な保護が提供されることを確実にするために、情報システムのオーナーに助言を求めているか？
- 組織は、共通管理策のセキュリティ管理策ベースラインが、共通管理策を継承する情報システムのベースラインよりも低い場合に、システム固有の管理策またはハイブリッド管理策によって、**共通管理策**を**補足**しているか？
- 組織は、**外部プロバイダ**から継承したセキュリティ管理策について、文書化しているか？
- 組織は、組織のリスクマネジメント戦略、および重要な任務／業務機能の保護に対する組織のコミットメントを反映した、情報システムの**継続的監視戦略**（システム固有の管理策、ハイブリッド管理策、および共通管理策に導入されているセキュリティ管理策の有効性の監視を含む）を策定しているか？?
- システム固有の管理策、ハイブリッド管理策、および共通管理策を含むセキュリティ計画は、組織内の適切な責任者によって**承認**されているか？

3.3 RMF ステップ 3ーセキュリティ管理策の実施

セキュリティ管理策の実施

タスク 3-1: セキュリティ計画に記載されているセキュリティ管理策を実施する。

主な責任を持つ者: 情報システムのオーナーまたは共通管理策の提供者

補助的な役割: 情報のオーナー／スチュワード、情報システムセキュリティ責任者、情報システムセキュリティエンジニア

SDLCのフェーズ: 開発／調達、インプリメンテーション

補足ガイダンス: セキュリティ管理策の実施は、組織のエンタープライズアーキテクチャおよび情報セキュリティアーキテクチャに適合している。情報セキュリティアーキテクチャは、情報システム、および、組織によって定義されたあらゆるサブシステムにセキュリティ管理策（たとえば、セキュリティメカニズムおよびサービスが含まれる）を割り当てるための、リソースとして機能する。情報システム（サブシステムを含む）に導入する予定のセキュリティ管理策は、特定のセキュリティ機能を提供することに責任を持つシステムコンポーネントに割り当てられる。すべてのセキュリティ管理策をいずれかのサブシステムに割り当てる必要はない。サブシステムの分類、情報セキュリティアーキテクチャ、およびセキュリティ管理策の割り当ては、適切なバランスの実現を実現するために連携する必要がある。一部のセキュリティ管理策を共通管理策またはハイブリッド管理策として割り当てることは、このアーキテクチャプロセスの一環である。情報システムにおいてセキュリティ管理策を実施する際には、システムおよびソフトウェアエンジニアリングに関する方法論、セキュリティエンジニアリングの原理、セキュアなコーディング技法を含む、ベストプラクティスを用いる。また、組織は、連邦政府のポリシーおよび組織のポリシーに従って、各IT製品の必須の設定を定めて、そのような設定が確実に行われるようにする（たとえば、Federal Desktop Core Configuration（連邦政府のデスクトップ基準））。情報システムセキュリティエンジニアは、情報システムセキュリティ責任者の支援のもと、情報セキュリティ要求事項を把握・改良し、洗練された要求事項を意図的なセキュリティ設計またはセキュリティ構成を通じて各IT製品およびシステムに確実に組み入れることを可能にする、健全なセキュリティエンジニアリングプロセスを導入する。組織は、入手可能な場合には、承認された第三者アセスメント機関によってテスト、評価、または有効性の確認が行われたIT製品の使用を検討する。これに加えて、組織は、該当する場合には、セキュリティ管理策の実施時に求められる最低限の保証要件を満たさなければならない。保証要件は、セキュリティ管理策の開発者および実施者が定める活動および行動を対象としており、管理策が正しく導入されていること、意図したとおりに運用されていること、情報システムのセキュリティ要求事項に対する適合性の観点から望まれる結果を産出していることに対する信頼の度合いを向上させるために適用される。保証要件は、情報システムのセキュリティ機能の設計、開発、および実施の品質を取り扱う。より高位の影響のシステム（すなわち、標的となりうる高価値のシステム）の場合で、かつ、具体的で信用できる脅威情報によって高度なサイバー攻撃の可能性が示される場合、追加的な保証手段についても検討する。組織は、共通管理策間およびシステム固有の管理策間の統合および／またはインターフェースに関連する、実施関連のすべての問題について考慮する。

情報システムによって継承される共通管理策については、情報システムセキュリティエンジニアが、情報システムセキュリティ責任者の支援のもと、共通管理策の提供者と協力して、組織の情報システムに最も適した適用方法を決定する。管理面および運用面での管理策の中には、IT製品、サービス、およびシステムへの正式な組み入れが不要なものもある。運用面および／または技術面での管理策の種類によっては、あらかじめ選択された共通管理策を情報システムが最大限に活用することを可能にするために、コンポーネント、製品、またはサービスの追加が必要となる。仮に共通管理策の選択が据え置きになっていた場合、情報システムによって継承される共通管理策の特定については、システム開発ライフサイクルの現時点ならより適切な判断を下せるか否かを見極めるためにも、再訪される。情報システムのオーナーは、彼らが所有する個々のシステムにおける共通管理策の実施が適切であるか否かを判断する際に、共通管理策の提供者が用意した運用認可パッケージを参照することができる。共通管理策を継承する情報システムの保護に関するニーズを満たすことができない共通管理策、または、受容できない弱点または欠陥を有する共通管理策については、情報システムのオーナーが、実施すべき代替管理策または補足管理策を特定する。組織および組織の請負業者は、情報システムの開発および導入段階で最大限に、かつ、RMF の各タスクを適用するうえで許容される柔軟性に適合する形で、セキュリティ管理策の初期アセスメント（開発段階におけるテストおよび評価ともいわれる）を実施する。システム開発ライフサイクルの開発および導入段階と並行してセキュリティ管理策のアセスメントを実施することにより、弱点と欠陥を早期に特定することができると同時に、是正措置を開始するための費用対効果の最も高い手法が組織に提供される。これらのアセスメント時に発見された問題は、必要に応じて、早期解決のために運用認可責任者にゆだねられる。セキュリティ管理策の初期のアセスメントの結果は、アセスメントの遅延や、コスト高につながるアセスメントの重複を避けるために、セキュリティ運用認可プロセスにおいて

使用されることもある。システム開発ライフサイクルの他のフェーズにおいても引き続き再利用されるアセスメント結果は、組織が定める再利用に関する要求事項（独立性を含む）を満たさなければならない。

参考文書: FIPS Publication 200; NIST Special Publications 800-30, 800-53, 800-53A; CNSS Instruction 1253; Web: SCAP.NIST.GOV。

セキュリティ管理策の文書化

タスク 3-2: 必要に応じて、セキュリティ管理策の実施について、機能面での記述（予定しているインプット、予想される挙動、および予想されるアウトプットを含む）と併せて、セキュリティ計画に記載する。

主な責任を持つ者: 情報システムのオーナーまたは共通管理策の提供者

補助的な役割: 情報のオーナー／スチュワード、情報システムセキュリティ責任者、情報システムセキュリティエンジニア

SDLCのフェーズ: 開発／調達、インプリメンテーション

補足ガイダンス: システム固有の管理策、ハイブリッド管理策、および共通管理策がどのように実施されるかについては、セキュリティ管理策に関するドキュメントに記載される。このドキュメントは、情報システムの全体的な機能に関する計画および予想を形式化したものである。セキュリティ管理策の実施に関する機能的記述には、通常、情報システムのハードウェア、ソフトウェア、またはファームウェアコンポーネントに導入されている、技術面での管理策に対する、予定しているインプット、予想される挙動、および予想されるアウトプット（該当する場合）が含まれる。セキュリティ管理策の実施に関するドキュメントによって、情報システムの導入前後に下された決定事項への追跡が可能になる。情報システムに関するドキュメントの作成に必要な作業レベルは、組織の任務、業務機能、および運営に関して、情報システムがどのような目的と範囲で機能し、どのような影響をもたらすかに適合する。可能な限り、組織は、既存のドキュメント（ベンダーによって供給されるものと、同じ（あるは類似の）情報システムを導入している他の組織によって供給されるもの）を参照し、自動化された支援ツールを利用すると同時に、最大限のコミュニケーションを確保することによって、セキュリティ管理策の実施の全体的な効率と費用対効果を向上させる。プラットフォームの依存関係も取り扱うこのドキュメントには、セキュリティ管理策に必要なセキュリティ機能が、どのようにして管理策のアセスメントを支援するのに十分な詳細さをもって実現されるかについての記述に必要な、あらゆる追加的情報が含まれる。セキュリティ管理策の実施に関するドキュメント作成は、ハードウェアおよびソフトウェア開発、ならびにシステム／セキュリティエンジニアリング分野の最優良事例に従うものとし、組織が定めたシステム開発ライフサイクル活動の文書化に関するポリシーおよび手順に適合する。組織は、メカニズムをベースにした技術面でのセキュリティ管理策に関して可能な場合で、かつ、実用的な場合には、ハードウェアベンダー、ソフトウェアベンダー、および／またはシステムインテグレータが提供する（あるいは、彼らから入手できる）機能仕様書（管理策のアセスメントおよび監視時に、組織を支援する可能性のある、セキュリティ関連のドキュメントを含む）を最大限に活用する。同様に、管理面および運用面での管理策に関しては、組織内の適切なエンティティ（たとえば、施設整備室、人材オフィス、物理的セキュリティオフィスなど）から、セキュリティ管理策の実施に関する情報を入手する。組織が策定したエンタープライズアーキテクチャおよび情報セキュリティアーキテクチャは、セキュリティ管理策の実施に用いられるアプローチに大きな影響を与える。したがって、このプロセスに関するドキュメントを用意することによって、組織の情報セキュリティ要求事項を満たすうえでの追跡可能性の確保が容易になる。

参考文書: NIST Special Publication 800-53; CNSS Instruction 1253。

マイルストーンチェックポイント #3

- 組織は、エンタープライズアーキテクチャおよび情報セキュリティアーキテクチャに準拠する形で、セキュリティ管理策をシステム固有の管理策、ハイブリッド管理策、または共通管理策として**割り当てているか**？
- 組織は、IT製品を情報システムに組み入れる際に、および、セキュリティ計画に記載されているセキュリティ管理策を実施する際に、健全な**情報システムおよびセキュリティエンジニアリング方法論**を使用していることを示しているか？
- 組織は、組織の情報システムによって継承された**共通管理策**がどのように実施されているかについて文書化しているか？
- 組織は、**システム固有の**セキュリティ管理策および**ハイブリッド**管理策が、具体的なテクノロジーおよびプラットフォームの依存関係を考慮したうえで、情報システムにおいてどのように実施されているかについて文書化しているか？
- 組織は、セキュリティ管理策を実施する際に、**最低限の保証要件**を考慮しているか？

3.4 RMF ステップ 4ーセキュリティ管理策のアセスメント

アセスメントの準備

タスク 4-1: セキュリティ管理策のアセスメント計画を策定、レビューし、承認する。

主な責任を持つ者: セキュリティ管理策アセサー

補助的な役割: 運用認可責任者または指名された代理人、最高情報責任者、上級情報セキュリティ責任者、情報システムのオーナーまたは共通管理策の提供者、情報のオーナー／スチュワード、情報システムセキュリティ責任者

SDLCのフェーズ: 開発／調達、インプリメンテーション

補足ガイダンス: セキュリティアセスメント計画は、セキュリティ管理策アセスメントの目的、アセスメントの実施方法に関する詳細なロードマップ、およびアセスメント手順を提供する。セキュリティアセスメント計画は、組織が実施するアセスメントのタイプ（たとえば、開発段階におけるテストおよび評価、第三者による検証および有効性確認、セキュリティ運用認可／再運用認可を支援するアセスメント、監査、継続的な監視、是正活動後のアセスメント）を反映する。システム開発ライフサイクルの開発／調達、インプリメンテーションの段階と並行してセキュリティ管理策のアセスメントを実施することにより、弱点と欠陥を早期に特定することができると同時に、是正活動を開始するための費用対効果の最も高い手法が組織に提供される。これらのアセスメント時に発見された問題は、必要に応じて、早期解決のために運用認可責任者にゆだねられる。システムの開発およびインプリメンテーションの段階で実施されるセキュリティ管理策アセスメントの結果は、システムフィールディングの遅延、またはコスト高につながるアセスメントの重複を避けるために、セキュリティ運用認可プロセスにおいて使用されることもある（ただし、再利用に関する基準を満たすことが前提となる）。セキュリティアセスメント計画は、組織内の適切な職員によってレビュー・承認され、その計画が組織のセキュリティ目的に適合していること、継続的な監視およびリアルタイムに近いリスクマネジメントの概念を支援する最新のツール、技法、手順、および自動化を採用していること、アセスメント用に割り当てられたリソースに関して費用対効果が高いことが確認される。セキュリティアセスメント計画の承認には、(i) セキュリティ管理策アセスメントに関する適切な予想を立てる、および (ii) セキュリティ管理策のアセスメントに必要な作業レベルを決定する、といった 2 つの目的がある。承認されたセキュリティアセスメント計画は、セキュリティ管理策の有効性の判断に適切なレベルのリソースが確実に割り当てられることを支援する。セキュリティ管理策が外部プロバイダによって組織に提供される場合（たとえば、契約、省庁間の取り決め、業務分野についての取り決め、ライセンス契約および／またはサプライチェーンの取り決めなどを介して）、組織は、そのプロバイダからセキュリティアセスメント計画を入手する。

組織は、セキュリティ管理策アセサーを選択するにあたって、必要な技術的専門知識と独立性レベルの両方について考慮する。組織は、システム固有の管理策、ハイブリッド管理策、および共通管理策のアセスメントを成功裏に実施するのに必要なスキルと技術的専門知識が、セキュリティ管理策アセサーに備わっていることを確認する。これには、組織が採用する特定のハードウェア、ソフトウェア、およびファームウェアコンポーネントに関する知識と経験が含まれる。独立したアセサーとは、情報システムに導入されている、または、情報システムによって継承されるセキュリティ管理策を公平に評価することができる、個人、またはグループのことである。「公平」とは、アセサーが、情報システムの開発、運用および／または管理に関して、あるいは、セキュリティ管理策の有効性の判断に関して、認識された、あるいは実際の、あらゆる利害の衝突とは無縁の者であることを意味する。独立したセキュリティ管理策アセスメントサービスは、組織内の他のエレメントから調達する、あるいは、組織外の公的部門または民間部門に委託することができる。契約によるアセスメントサービスは、情報システムのオーナーが契約プロセスに直接関与していないこと、あるいはセキュリティ管理策のアセスメントを実施するアセサーの独立性が、不当な影響を受けてないことが確認できる場合に、独立しているとみなされる。運用認可責任者または指名された代理人は、情報システムのセキュリティ分類プロセスの結果、および、組織の業務や資産、個人、他の組織、および国家に対する最終的なリスクに基づき、セキュリティ管理策アセサーに求められる独立性のレベルを決定する。運用認可責任者は、設定した独立性のレベルが、生成されるアセスメント結果が妥当であること、また、情報システムの運用の開始または継続を許可するか否かについてのリスクベースの判断に利用できることを保証するのに十分なレベルであるかを判断する。特別な状況にある場合（たとえば、情報システムを所有する組織の規模が小さい場合、または組織の構成上、システムのオーナーの指揮のもとで働く開発担当者、運用担当者および／または管理担当者による、セキュリティ管理策のアセスメントが求められる場合など）、アセスメントプロセスの独立性を実現するために、独立した専門家チームを採用することもできる。この場合、そのチームが、アセスメント結果の慎重なレビューと分析を通じて、結果の完全性、一貫性、および正確さを検証することになる。運用認可責任者は、上述のような特別な状況において下された、アセサーの独立性に関するあらゆる決定事項がもたらす影響について、監査官室（the Office of the Inspector General）、上級情報セキュリティ責任者および最高情報責任者との間で十分な話し合いを持つべきである。この話し

合いは、各セキュリティアセスメントを実施する前に行われるか、あるいは、特別な状況に関する基準を満たす、すべての情報システムに適用される、特別な状況に関する組織のポリシーおよびアプローチを組織が定める際に、一度だけ行われることが考えられる。初期および後続のセキュリティ運用認可を支援するセキュリティ管理策アセスメントは、独立したアセサーによって実施される。

参考文書: NIST Special Publication 800-53A。

セキュリティ管理策のアセスメント

タスク 4-2: セキュリティアセスメント計画に記載されているアセスメント手順に従ってセキュリティ管理策をアセスメントする。

主な責任を持つ者: セキュリティ管理策アセサー

補助的な役割: 情報システムのオーナーまたは共通管理策の提供者、情報のオーナー／スチュワード、情報システムセキュリティ責任者

SDLCのフェーズ: 開発／調達、インプリメンテーション

補足ガイダンス: セキュリティ管理策がどの程度正しく導入されているか、どの程度意図した通りに運用されているか、システムのセキュリティ要求事項に対する適合性の観点から所望の結果をどの程度産出しているかを判断するために、管理策のアセスメントが行われる。セキュリティ管理策のアセスメントは、システム開発ライフサイクルにおいて、可能な限り早い段階（情報システムの開発段階が好ましい）で実施される。この種のアセスメントは、開発段階におけるテストおよび評価といわれるもので、必要なセキュリティ管理策が正しく導入されていることと、組織が定めた情報セキュリティアーキテクチャに適合しているかを確認することを目的としている。開発段階におけるテストおよび評価活動には、たとえば、設計およびコードのレビュー、アプリケーションのスキャン、および回帰試験が含まれる。システム開発ライフサイクルの早い段階で特定された弱点や欠陥は、後続の段階に進む前に、より迅速に、かつ、費用面でもはるかに効果的に、解決できる。その目的は、情報セキュリティアーキテクチャおよびセキュリティ管理策を前もって特定し、システムの設計およびテストを通じて、それらの管理策の導入の有効性を確認することにある。

情報システムオーナーは、以下の目的を果たすために、アセサーの技術的専門知識と判断に頼る。(i) セキュリティアセスメント計画に記載されているアセスメント手順を用いて、情報システムに導入される、または情報システムによって継承されるセキュリティ管理策をアセスメントする、(ii) 管理策の弱点または欠陥を修正し、特定された脆弱性を排除または削減するための、具体的な推奨事項を示す。アセサーの結論は、セキュリティ管理策のアセスメント時に発見された弱点および欠陥を、公平な立場で事実に基づき報告したものでなければならない。組織には、以下の項目を支援するために、セキュリティ管理策のアセスメント向けに用意されている自動化された支援ツールを最大限に活用することが推奨される。(i) アセスメントのスピードと、全体的な有効性および効率性を向上させる、および (ii) 組織の情報システムのセキュリティ状態を継続的に監視するといった考えを支援する。アジャイル開発などの反復的な開発プロセスが採用される場合、通常、各サイクルの実施ごとに、反復的なアセスメントが実施されることになる。情報システムに導入されているCOTS（民生）IT製品に導入されているセキュリティ管理策をアセスメントするのに、同様のプロセスを用いることができる。反復的な開発が採用されない場合にも、セキュリティ計画にリストアップされているすべてのセキュリティ管理策の完全な実施を待たずに、各セキュリティ管理策をアセスメントすることを選択してもよい。この種の段階的なアセスメントは、他のアセスメントよりも高い効率または費用対効果が期待できる場合に、実施すべきである。たとえば、ハードウェアおよびソフトウェアに導入されている技術面でのセキュリティ管理策をアセスメントする前に、ポリシー、手順、および計画をアセスメントしてもよい。多くの場合、共通管理策（すなわち、情報システムによって継承されるセキュリティ管理策）のアセスメントは、システムに導入されているセキュリティ管理策のアセスメントよりも先に実施することができる。

組織は、アセサーが以下の項目にアクセスできるようにする。(i) アセスメント対象のセキュリティ管理策を導入している情報システムやその運用環境 (ii) それらのセキュリティ管理策をアセスメントするのに必要な、適切なドキュメント、記録、アーチファクト、テスト結果、およびその他の資料。さらに、アセサーには、運用認可責任者が定めるレベルの独立性を有することが求められる（付録 D.13 と付録 F.4 を参照）。初期および後続のセキュリティ運用認可を支援するセキュリティ管理策アセスメントは、独立したアセサーによって実施される。継続的な監視におけるアセサーの独立性は、必須ではないが、再運用認可が必要な場合のアセスメント結果の再利用を容易にする。セキュリティ管理策が外部プロバイダによって提供される場合（たとえば、契約、省庁間の取り決め、業務分野についての取り決め、ライセンス契約および／またはサプライチェーンの取り決めなどを介して）、組織は、アセサーによる、セキュリティ管理策を導入している情報システム／運用環境、および、アセスメントを実施するのに必要な適切な情報へのアクセスを保証する。また、組織は、外部プロバイダによって実施された可能性のある、既存のアセスメントに関連する

あらゆる情報を入手し、組織が定めた再利用に関する基準に従って可能な場合には常に、そうしたアセスメント情報を再利用する。情報システムに関する記述は、通常、セキュリティ計画のシステムの識別に関するセクションに記載されるか、参照として含まれるか、あるいは、セキュリティ計画の添付文書として含まれる。手順、レポート、ログ、およびセキュリティ管理策の実施に関する証拠を示す記録などの補足的な資料についても、セキュリティ計画に記載される。可能な限りタイムリーで、かつ、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には、以前に実施されたアセメントの結果を再利用することが推奨される（ただし、そうすることが妥当であり、かつ適切な場合に限られるが）。たとえば、最近実施された情報システムの監査によって、選択されたセキュリティ管理策の有効性に関する情報が生成された可能性がある。以前に実施されたアセメントの結果を再利用する別の機会として、市販のIT製品のセキュリティ機能をテストおよび評価するプログラムの実施がある。また、システム開発者から以前に実施されたアセメントの結果を入手できる場合には、セキュリティ管理策アセサーが、適切な状況において、それらの結果を現行のアセスメントに組み入れてもよい。最後に、アセスメント結果の再利用は、互恵契約（reciprocity）を支援するために行われる場合もある（可能であれば）。

参考文書: NIST Special Publication 800-53A。

セキュリティアセスメントレポート

タスク 4-3: セキュリティ管理策のアセスメントを通じて発見された問題、導かれた結論および推奨事項を文書化した、セキュリティアセスメントレポートを用意する。

主な責任を持つ者: セキュリティ管理策アセサー

補助的な役割: 情報システムのオーナーまたは共通管理策の提供者、情報システムセキュリティ責任者

SDLCのフェーズ: 開発／調達、インプリメンテーション

補足ガイダンス: セキュリティ管理策のあらゆる弱点または欠陥を修正するための推奨事項を含む、アセスメント結果は、セキュリティアセスメントレポートに記載される。セキュリティアセスメントレポートは、運用認可責任者向けに策定されるセキュリティ運用認可パッケージ内の構成要素である、3 つの主要ドキュメントのうちの一つである。セキュリティアセスメントレポートにはアセサーからの情報が含まれていて、アセサーの見解をもとに、情報システムに導入される、または情報システムによって継承されるセキュリティ管理策の有効性を判断できるようになっている。運用認可権限者にとってセキュリティアセスメントレポートは、組織の業務や資産、個人、他の組織および国家に対するリスクを特定するための重要な要素である。セキュリティ管理策アセスメントの結果は、当該アセスメントに適した詳細レベルで文書化しなければならない。この際、文書の書式は、組織および／または連邦政府のポリシーが規定する報告書式に従う。報告書式は、組織が実施するアセスメントの種類にも適したものでなければならない（たとえば、開発段階におけるテストおよび評価、自己評価、第三者による検証および有効性確認、セキュリティ運用認可プロセスまたは後続の再運用認可を支援する第三者アセスメント、継続的な監視におけるアセスメント、是正活動後のアセスメント、第三者による監査／評価など）。

システム開発時に得たセキュリティ管理策アセスメントの結果は、中間レポートに記載され、最終的なセキュリティアセスメントレポートに含められる。これは、セキュリティアセスメントレポートが進化するドキュメントであり、システム開発ライフサイクルの関連するすべてのフェーズにおいて生成されたアセスメント結果（継続的な監視段階で生成された結果を含む）を含んでいるといった概念を支援する。組織は、セキュリティ管理策のアセスメント時に生成された結果の詳細から、エグゼクティブサマリを作成してもよい。エグゼクティブサマリは、運用認可権限者に対して、アセスメントの主要部分、重要な結果の概要、および／またはセキュリティ管理策の弱点と欠陥を克服するための推奨事項にフォーカスをあてた、セキュリティアセスメントレポートの簡略版を提供する。

参考文書: NIST Special Publication 800-53A。

是正活動

タスク 4-4: セキュリティアセスメントレポートに記載されている結論と推奨事項に基づいて、セキュリティ管理策に対する初期の是正活動を実施し、是正された管理策（複数）を適宜、再アセスメントする。

主な責任を持つ者: I 情報システムのオーナーまたは共通管理策の提供者、セキュリティ管理策アセサー

補助的な役割: 運用認可責任者または指名された代理人、最高情報責任者、上級情報セキュリティ責任者、情報のオーナー／スチュワード、情報システムセキュリティ責任者、情報システムセキュリティエンジニア、セキュリティ管理策アセサー

SDLCのフェーズ: 開発／調達、インプリメンテーション

補足ガイダンス: セキュリティアセスメントレポートによって、情報システムに導入される、または情報システムによって継承されるセキュリティ管理策の弱点および欠陥のうち、システム開発時に合理的に解決できなかった弱点と欠陥への可視性がもたらされる。セキュリティ管理策のアセスメント時に生成された結果は、組織の優先順位に従ってリスクを軽減するための統制のとれた、構造化されたアプローチを容易にする。情報システムのオーナーと共通管理策の提供者が、組織の選ばれた職員（たとえば、情報システムセキュリティエンジニア、運用認可責任者が指名する代理人、最高情報責任者、上級情報セキュリティ責任者、情報のオーナー／スチュワードなど）の協力を得て特定のアセスメント結果について検討した結果、組織に重大なリスクをもたらすような重要なものではないと判断することもある。反対に、特定のアセスメント結果が実際に重大であり、緊急の是正活動が必要であると、組織の担当者が判断することもある。いずれにせよ組織は、アセサーの結論をレビューし、結果の重大さ、あるいは深刻さ（すなわち、組織の業務や資産、個人、他の組織、および国家に対する潜在的なマイナスの影響）および、それらの結果がさらなる調査または是正措置が必要なほど重大なものであるかどうかを自ら判断しなければならない。セキュリティ管理策のアセスメント時に生成された結果に基づく最新のリスクアセスメント、および、リスクエグゼクティブ（機能）からのあらゆるインプットは、初期の是正活動と、それらの活動の優先順位の決定を支援する。組織の資源が組織の優先事項に従って効果的に割り当てられることを確実にするためには、シニアリーダーによるリスク軽減プロセスへの関与が必要となる場合がある。資源の効果的な割り当てでは、組織の最も重要かつ機密に関わる任務および業務機能を支援する情報システムに対して、または、最も深刻なリスクの要因となる欠陥を修正する活動に対して、最初に資源が割り当てられる。セキュリティ管理策の弱点または欠陥を修正した後は、修正された管理策の有効性を再アセスメントする。セキュリティ管理策の再アセスメントは、修正された管理策がどの程度正しく導入されているか、どの程度意図した通りに運用されているか、システムのセキュリティ要求事項に対する適合性の観点から所望の結果をどの程度産出しているかを判断するための活動である。アセサーは、元のアセスメント結果が変更にならないように注意を払いながら、再アセスメントの結果をもって、セキュリティアセスメントレポートを更新する。セキュリティ計画は、セキュリティ管理策アセスメントの結果、および実施されたあらゆる是正活動に基づいて更新される。更新されたセキュリティ計画は、最終的なセキュリティ管理策（初期アセスメント後に、是正活動に関する推奨事項に従って、情報システムのオーナーまたは共通管理策の提供者によって変更が加えられたもの）の実際の状態を反映したものでなければならない。アセスメントが完了した時点で、セキュリティ計画には、導入されたセキュリティ管理策（代替管理策を含む）の正確なリストと内容、および残存する脆弱性のリストが含まれる。

組織は、セキュリティアセスメントレポートへの随意的な付録を用意して、運用認可責任者に提出することができる。この随意的な付録によって、アセサーの初期の結論に応じる機会が、情報システムのオーナーおよび共通管理策の提供者に与えられる。この付録には、たとえば、アセサーの結論に応じて情報システムのオーナーまたは共通管理策の提供者が実施した、初期の是正活動に関する情報が含まれる場合があり、また、アセサーの結論に対するオーナーの見解（たとえば、追加の説明資料、特定の結論に対する反論、および記録の修正が含まれる）が提供されることもある。セキュリティアセスメントレポートへの随意的な付録によって、元のレポートに記載されているアセサーの初期の結論に、なんらかの形で変更が加わったり、影響がもたらされることはない。この付録に記載されている情報は、運用認可責任者がリスクベースの運用認可判断を行う際に考慮される。組織は、アセスメント時に特定されたセキュリティ管理策の弱点と欠陥に対してどのような措置を取るべきかを決定する際に、問題解決プロセスを採用してもよい。問題解決プロセスは、脆弱性および関連するリスク、ならびにフォールスポジティブへの対処を支援し、システム固有の管理策、ハイブリッド管理策、および共通管理策の現行の有効性を含む、情報システムのセキュリティ状態に関する有用な情報を運用認可責任者に提供する。問題解決プロセスは、（組織が）重要な項目のみを特定し、行動計画とマイルストーンに含めることも支援する。

参考文書: NIST Special Publications 800-30, 800-53A。

マイルストーンチェックポイント #4

- 組織は、情報システムに導入される、または情報システムによって継承されるセキュリティ管理策をアセスメントするための、包括的な**計画**を策定しているか？
- アセスメント計画は、組織内の適切な職員によって**レビュー・承認されているか**？
- 組織は、組織のセキュリティ管理策アセスメントに適したアセサーの**独立性**レベルを定めているか？
- 組織は、効果的なセキュリティ管理策アセスメントの実施のためにアセサーが必要とする、**アセスメント関連**の重要な補足**資料**を用意しているか？
- 組織は、以前に実施されたアセスメントまたは他のソースからの**アセスメント結果**を**再利用**する機会を検討しているか？
- アセサーは、組織が定めたアセスメント計画に従って**セキュリティ管理策アセスメント**を完了したか？
- 組織は、アセサーから、適切な結論と推奨事項を含む、完結した**セキュリティアセスメントレポート**を受け取ったか？
- 組織は、セキュリティアセスメントレポートに記載されている結論と推奨事項に基づいて、情報システムおよびシステムの運用環境における最も重要な弱点および欠陥に対処するのに必要な**是正活動**を実施したか？
- 組織は、セキュリティアセスメントレポートに記載されている結論と推奨事項、ならびに、情報システムおよびシステムの運用環境に対する後続のあらゆる変更に基づいて、適切な**セキュリティ計画**を更新したか？

3.5 RMF ステップ 5ー情報システムの運用認可

行動計画とマイルストーン

タスク 5-1: セキュリティアセスメントレポートに記載されている結論と推奨事項に基づいて、行動計画とマイルストーンを作成する（ただし、既に実施されたすべての是正活動を除く）。

主な責任を持つ者: 情報システムのオーナーまたは共通管理策の提供者

補助的な役割: 情報のオーナー／スチュワード、情報システムセキュリティ責任者

SDLCのフェーズ: インプリメンテーション

補足ガイダンス: 運用認可責任者向けに情報システムのオーナーまたは共通管理策の提供者が作成する行動計画とマイルストーンは、セキュリティ運用認可パッケージの構成要素である、3 つの主要ドキュメントのうちの一つである。行動計画とマイルストーンは、(i) セキュリティ管理策のアセスメント時に確認されたあらゆる弱点または欠陥の是正、および (ii) 情報システムに残存する脆弱性への対応のために計画される、具体的なタスクについて記述したものである。行動計画とマイルストーンは、(i) 情報システムを導入する前に、あるいは後に、完了させることが推奨されるタスク (ii) それらのタスクを達成するのに必要なリソース (iii) タスクに見合ったすべてのマイルストーン (iv) マイルストーンの完了予定日の確認に役立つ。行動計画とマイルストーンは、運用認可責任者が、セキュリティ管理策のアセスメント時に発見された弱点または欠陥に対する是正処置の進捗を確認するために用いられる。セキュリティ管理策のアセスメント時に発見されたセキュリティ上のあらゆる弱点および欠陥は、効果的な追跡記録を維持するためにも、セキュリティアセスメントレポートに記載される。組織は、適用される法律、大統領令、指令、方針、基準、ガイダンス、または規制に従って、セキュリティ管理策アセスメントの結果をもとに具体的な行動計画とマイルストーンを作成する。アセスメント時、または、運用認可パッケージを運用認可責任者に提出する前に修正された弱点または欠陥に関しては、行動計画とマイルストーンに含める必要はない。

組織は、組織全体を通して一貫性のある、優先順位付がなされたリスク軽減アプローチを容易にする、行動計画およびマイルストーンを作成するための戦略を定義する。この戦略により、以下の項目に基づいた、行動計画とマイルストーンを作成することができる。(i) 情報システムのセキュリティ分類 (ii) セキュリティ管理策の具体的な弱点または欠陥 (iii) セキュリティ管理策において特定された弱点または欠陥の重大性（すなわち、それらの弱点または欠陥が、情報システムの全体的なセキュリティ状態、組織のリスクへの暴露、または自身の任務／業務機能を果たすための組織の能力に及ぼす直接的／間接的な影響）、ならびに (iv) セキュリティ管理策において特定された弱点または欠陥に対処するためのリスク軽減アプローチ（組織に対して提案されているもの）（たとえば、リスク軽減活動の優先順位付け、リスク軽減活動に必要なリソースの割り当て）。リスクアセスメントによって、行動計画とマイルストーンに含まれる項目に対する優先順位付けプロセスが導かれる。

参考文書: OMB Memorandum 02-01; NIST Special Publications 800-30, 800-53A。

セキュリティ運用認可パッケージ

タスク 5-2: セキュリティ運用認可パッケージをまとめて、運用認可責任者に提出し、裁定を仰ぐ。

主な責任を持つ者: 情報システムのオーナーまたは共通管理策の提供者

補助的な役割: 情報システムセキュリティ責任者、セキュリティ管理策アセサー

SDLCのフェーズ: インプリメンテーション.

補足ガイダンス: セキュリティ運用認可パッケージには、(i) セキュリティ計画 (ii) セキュリティアセスメントレポート、および (iii) 行動計画とマイルストーンが含まれる。運用認可責任者は、リスクベースの運用認可判断を行う際に、これらの主要なドキュメントに含まれる情報を利用する。特定のセキュリティ機能を備えるために共通管理策を継承する情報システムに関しては、共通管理策に対するセキュリティ運用認可パッケージ、またはそのようなドキュメントへの参照も、情報システムのセキュリティ運用認可パッケージに含まれる。セキュリティ管理策が外部プロバイダによって組織に提供される場合（たとえば、契約、省庁間の取り決め、業務分野についての取り決め、ライセンス契約および／またはサプライチェーンの取り決めなどを介して）、組織は、運用認可責任者がリスクベースの判断を行うのに必要な情報が、そのプロバイダによって提供されていることを確認する。

運用認可活動を実施する運用認可責任者のリクエストに応じて、追加の情報がセキュリティ運用認可パッケージに含まれる場合もある。セキュリティ運用認可パッケージの内容は、連邦政府のポリシーおよび組織のポリシーに従っ

て適切に保護される。組織には、セキュリティ運用認可パッケージの内容を用意・管理するための、自動化された支援ツールを使用することが推奨される。このようなツールによって、組織内の各情報システムの現行のセキュリティ状況に関する、運用認可責任者向けの情報を維持管理・更新するための効果的な手段が、組織に与えられる。セキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーンに対する秩序だった、統率のとれたタイムリーな更新は、リアルタイムに近いリスクマネジメントと継続的な運用認可の概念を支援する。また、（必要に応じて）費用対効果の優れた有意な再運用認可活動も支援する。組織は、運用認可パッケージに含まれる主要ドキュメントの更新に対して、厳密なバージョン管理を行う。自動化ツールと支援データベースを使用することによって、組織の運用認可責任者と他のシニアリーダーは、システム固有の管理策、ハイブリッド管理策、および共通管理策の現行の有効性を含む、情報システムのセキュリティ状況に対する意識を維持することができる。

参考文書: なし。

リスクの判断

タスク 5-3: 組織の業務（任務、機能、イメージ、または評判を含む）、組織の資産、個人、他の組織、または国家に対するリスクを判断する。

主な責任を持つ者: 運用認可責任者または指名された代理人

補助的な役割: リスクエグゼクティブ（機能）、上級情報セキュリティ責任者

SDLCのフェーズ: インプリメンテーション

補足ガイダンス: 運用認可責任者または指名された代理人は上級情報セキュリティ責任者の協力のもと、情報システムのオーナーまたは共通管理策の提供者が提供する、情報システム（あるいは、そのシステムが継承する共通管理策）の最新のセキュリティ状態に関する情報、ならびに、あらゆる残存リスクに対応するための推奨事項に関する情報を評価する。組織は、脅威、脆弱性、および潜在的な影響、ならびにリスク軽減に関する推奨事項の分析結果に関する必要な情報を提供するために、リスクアセスメント（正式なものと、そうでないもの）を自身の自由裁量によって採用する。リスクエグゼクティブ（機能）は、運用認可責任者に対して、情報システムの運用および使用により生じる組織の業務や資産、個人、他の組織、および国家に対するリスクについての最終的な判断に必要な情報も提供する。リスク関連情報には、情報システムが支援する組織の任務および／または業務機能の重要性と、組織のリスクマネジメント戦略が含まれる。リスクマネジメント戦略には、通常、以下の項目が含まれる。(i) 組織においてリスクをアセスメントする方法（すなわち、どのようなツール、技法、手順、および方法論を用いるか）(ii) アセスメントされたリスクの重大さの評価方法 (iii) 組織の情報システムおよび他のソースより生じる既知のリスクの集約 (iv) リスク軽減アプローチ (v) 組織のリスク許容度、および (vi) 長期にわたってリスクを監視する方法。リスクに関する最終的な判断を下す際に、運用認可責任者または指名された代理人は、リスクエグゼクティブ（機能）から得た情報や、セキュリティ運用認可パッケージ（すなわち、セキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーン）に含まれる、情報システムのオーナーまたは共通管理策の提供者が提供する情報を考慮する。逆に、RMF を実効することによって得られる情報システム関連のセキュリティリスク情報は、リスクエグゼクティブ（機能）が、組織全体にわたるリスクマネジメント戦略を考案・更新する際に利用できるようになっている。

参考文書: NIST Special Publications 800-30, 800-39。

リスクの受容

タスク 5-4: 組織の業務、組織の資産、個人、他の組織、または国家に対するリスクが受容できるかどうかを判断する。

主な責任を持つ者: 運用認可責任者

補助的な役割: リスクエグゼクティブ（機能）、運用認可責任者が指名する代理人、上級情報セキュリティ責任者

SDLCのフェーズ: インプリメンテーション

補足ガイダンス: リスクを明示的に受容することは、運用認可責任者の責任であり、この任務を組織内の他の職員に委譲することはできない。運用認可責任者が組織の業務（任務、機能、イメージ、または評判を含む）、組織の資産、個人、他の組織、または国家に対するリスクが受容できるか否かを判断する場合には、多くの要素について考慮する。セキュリティに関する考慮と、任務および業務上のニーズとのバランスを取ることは、受容可能な運用認可判断を実現するためには不可欠である。運用認可責任者は、すべての関連情報をレビューし、適宜、組織のリスク

エグゼクティブ（機能）を含む他の職員に助言を求めた後に、情報システムおよびシステムが継承する共通管理策に対する運用認可判断を下す。セキュリティ運用認可の判断は、セキュリティ運用認可パッケージの内容と、必要に応じて、組織の主要な職員（リスクエグゼクティブ（機能）を含む）から得たあらゆる情報をもとに行われる。セキュリティ運用認可パッケージは、情報システムに導入される、または情報システムによって継承されるセキュリティ管理策の現行の有効性を含む、情報システムのセキュリティ状態に関連する情報を提供する。運用認可責任者向けに定められた包括的なリスクガイダンスを含む、リスクエグゼクティブ（機能）からの情報（以前に作成された運用認可責任者向けの包括的なリスクガイダンス）は、運用認可判断（たとえば、組織のリスク許容度、任務および業務上の具体的な要求事項、情報システム間の依存関係、および情報システムに直接関連しないリスクの種類など）に関連し影響を与える可能性がある、組織規模の追加情報を運用認可責任者に提供する。リスクエグゼクティブ（機能）からの情報は、文書化され、セキュリティ運用認可判断の一部となる。リスクエグゼクティブ（機能）からの情報を含む、セキュリティ運用認可判断は、情報システムのオーナーおよび共通管理策の提供者に伝達され、組織内の関係者（たとえば、相互接続されている各システムのオーナーおよび運用認可責任者、最高情報責任者、情報のオーナー／スチュワード、シニアマネージャなど）が利用できるようになる。

運用認可判断に関するドキュメントは、運用認可責任者が下した最終的なセキュリティ運用認可判断を情報システムのオーナーまたは共通管理策の提供者、および、必要であれば組織内の他の職員に伝達する役割を果たす。運用認可判断文書には、以下の情報が含まれる。(i) 運用認可判断 (ii) 運用認可のための諸条件、および (iii) 運用認可の満了日。セキュリティ運用認可判断は、情報システムのオーナーに対し、そのシステムの運用が (i) 認可されたこと (ii) 認可されないこと、のいずれかを示す。運用認可のための諸条件には、情報システムの運用に関して、または、共通管理策の導入に関して、情報システムのオーナーまたは共通管理策の提供者が順守しなければならないあらゆる制限や制約が記載されている。運用認可責任者が定める運用認可の満了日は、いつセキュリティ運用認可の期限が切れるかを示す。継続的監視プログラムが十分に堅牢であり、情報システムのセキュリティ状態、および情報システムに導入される、または情報システムによって継承されるセキュリティ管理策の現行の有効性に関する継続的なリスク判断およびリスク受容活動を実施するのに必要な情報が、運用認可責任者に提供されることが保証される場合には、運用認可の満了日を設けなくてもよい。

運用認可の満了日は、運用認可の最大期間を規定することもある連邦政府／組織のポリシーによって左右される。たとえば、情報システムの運用認可の最大期間が 3 年だとする。この場合、組織は、その期間内に、情報システムに導入される、または情報システムによって継承されるセキュリティ管理策のサブセットをアセスメントするための、継続的監視戦略を策定する。この戦略によって、個々のセキュリティ計画に記載されているすべてのセキュリティ管理策が、運用認可から 3 年が過ぎる前に少なくとも 1 度はアセスメントされることになる。ここでいう管理策には、外部から組織の情報システムに導入されるあらゆる共通管理策も含まれる。セキュリティ管理策のアセスメントが、必要なレベルの独立性を有する資格を持つアセサーによって、連邦政府／組織のポリシー、適切なセキュリティ標準およびガイドライン、ならびに運用認可責任者のニーズに沿って実施される場合には、それらのアセスメント結果を累積的に再運用認可に適用することができ、これによって、継続的な運用認可の概念が支援される。継続的な運用認可および正式な再運用認可に関する組織のポリシーは、（そうすることが求められる場合）連邦政府の指令、規定、および／またはポリシーに準拠する。

運用認可の判断文書は、裏付けとなるドキュメントを含むオリジナルのセキュリティ運用認可パッケージに添付されて情報システムのオーナーまたは共通管理策の提供者に伝送される。運用認可の判断文書とオリジナルの運用認可パッケージを受領した時点で、情報システムのオーナーまたは共通管理策の提供者が運用認可のための諸条件を受け入れたことになり、彼らはそれらの条件を満たした後に、その旨を運用認可責任者に通知する。組織は、情報システムと共通管理策の両方に対する運用認可文書を、組織の適切な職員（たとえば、共通管理策を継承する情報システムのオーナー、リスクエグゼクティブ（機能）、最高情報責任者、上級情報セキュリティ責任者、情報システムセキュリティ責任者など）が利用できるようにする。運用認可文書（特に、情報システムの脆弱性を扱っている情報）は、(i) 連邦政府のポリシーおよび組織のポリシーに従って、マーク付けと適切な保護がされなければならない、かつ、(ii) 組織の記録保管ポリシーに従って、保管されなければならない。運用認可責任者は、情報システムのオーナーまたは共通管理策の提供者が、運用認可の一部として定められた諸条件に従っていることを継続的に監視にする。

参考文書: NIST Special Publication 800-39。

マイルストーンチェックポイント #5

- 組織は、情報システムおよびシステムの運用環境に残存する弱点と欠陥への対応における組織の優先順位を反映した、**行動計画とマイルストーン**を策定しているか？
- 組織は、セキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーン（該当する場合）を含む、主要なドキュメントをすべて備えた、適切な**運用認可パッケージ**を策定しているか？
- 運用認可責任者による最終的な**リスク判断**と**リスク受容**は、組織が策定し、リスクエグゼクティブ（機能）によって伝達されるリスクマネジメント戦略を反映しているか？
- **運用認可判断**は、情報システムのオーナーおよび共通管理策の提供者を含む、組織内の適切な職員に伝達されているか？

3.6 RMF ステップ 6－セキュリティ管理策の監視

情報システムやその運用環境に対する変更

タスク 6-1: 情報システムおよびシステムの運用環境に対して提案されている、あるいは、実際に実施された変更がもたらすセキュリティへの影響を判断する。

主な責任を持つ者: 情報システムのオーナーまたは共通管理策の提供者

補助的な役割: リスクエグゼクティブ（機能）、運用認可責任者または指名された代理人、上級情報セキュリティ責任者、情報のオーナー／スチュワード、情報システムセキュリティ責任者

SDLCのフェーズ: 運用／保守

補足ガイダンス: 情報システムは、ハードウェア、ソフトウェア、またはファームウェアのアップグレード、およびシステムが存在し稼動する周辺環境に対する修正が行われるため、常に変化する。情報システムやその運用環境に対する変更を統制、管理、文書化するための統制のとれた、構造化されたアプローチは、効果的なセキュリティ管理策監視プログラムにとって不可欠な要素である。そのような監視活動を支援するために、組織は厳格な構成管理および構成制御プロセスを確立する。ハードウェア、ソフトウェア、またはファームウェアに対する具体的な変更に関するあらゆる情報（バージョンナンバー／リリースナンバー、新たに追加された、あるいは修正された機能／能力についての説明、セキュリティの導入に関するガイダンスなど）を記録することが重要である。情報システムの運用環境に対するすべての変更（たとえば、ホスティングするネットワークと施設に対する変更、任務／業務を遂行するためのシステムの利用に関する変更、脅威の変化など）、または、組織のリスクマネジメント戦略に対する変更を記録することも重要である。情報システムのオーナーおよび共通管理策の提供者は、上述の変更がもたらす可能性のあるセキュリティ上の影響を評価する際に、これらの情報を利用する。情報システムまたはシステムの運用環境に対して提案されている、あるいは、実際に実施された変更を文書化し、これらの変更によってもたらされる可能性があるシステムまたは組織のセキュリティ状態への影響を評価することが、セキュリティ管理策の監視および長期にわたるセキュリティ運用認可の維持の重要な側面となる。一般的に、情報システムに対する変更は、そのような変更がもたらすセキュリティ上の影響を評価する前に行われることはない。組織には、情報システムやその運用環境に対する変更を管理する際に、自動化ツールを最大限に利用することが推奨される。

組織が実施するセキュリティ影響分析では、情報システムまたはシステムの運用環境に対して提案されている変更（あるいは実際に実施された変更）がシステムのセキュリティ状態に与えると予測される（あるいは与えた）影響の度合いを判断する。情報システムやその運用環境に対する変更によって、現在実施されているセキュリティ管理策（システム固有の管理策、ハイブリッド管理策、および共通管理策を含む）に影響がもたらされる、システムに新たな脆弱性が生じる、または以前は必要ではなかった新たなセキュリティ管理策が必要になることがある。セキュリティ影響分析の結果が、情報システムに対して提案されている、あるいは、実際に実施された変更が、情報システムのセキュリティ状態に影響を与えると予測されるあるいは、与えたことを示している場合には、是正措置が発動され、適切なドキュメント（セキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーン）が訂正・更新される。情報システムのオーナーまたは共通管理策の提供者は、情報システムまたはシステムの運用環境に対してセキュリティに関わる変更を実施する前に、組織の適切な職員／エンティティ（たとえば、構成制御委員会、上級情報セキュリティ責任者、情報システムセキュリティ責任者など）に助言を求める。運用認可責任者または指名された代理人は、上級情報セキュリティ責任者およびリスクエグゼクティブ（機能）の協力のもと、訂正・更新されたセキュリティアセスメントレポートを使用して、正式な再運用認可活動が必要であるか否かを判断する。情報システムまたはシステムの運用環境に対する最も日常的な変更については、組織の継続的監視プログラムによって管理することができ、これにより、継続的な運用認可とリアルタイムに近いリスクマネジメントの概念が支援される。セキュリティ影響分析は、継続的なリスクアセスメントの一環として実施される。運用認可責任者または指名された代理人は、リスクエグゼクティブ（機能）の協力のもと、残存するリスクについての判断事項を必要に応じて確認する。組織のリスク状況に大きな変化が生じた場合には、リスクエグゼクティブ（機能）が運用認可責任者に通知する。

参考文書: NIST Special Publications 800-30, 800-53A。

継続的なセキュリティ管理策アセスメント

タスク 6-2: 組織が定めた監視戦略に従って、情報システムに導入される、または情報システムによって継承される技術面、管理面、および運用面でのセキュリティ管理策の中から選択された、管理策のサブセットをアセスメントする。

主な責任を持つ者: セキュリティ管理策アセサー

補助的な役割: 運用認可責任者または指名された代理人、情報システムのオーナーまたは共通管理策の提供者、情報のオーナー／スチュワード、情報システムセキュリティ責任者

SDLCのフェーズ: 運用／保守

補足ガイダンス: 組織は、初期のセキュリティ運用認可の期間内に、情報システムに導入される、または情報システムによって継承されるすべてのセキュリティ管理策をアセスメントする。初期の運用認可に続き、組織は、継続的な監視期間中にセキュリティ管理策（管理面、運用面、および技術面での管理策を含む）のサブセットを継続的にアセスメントする。監視すべきセキュリティ管理策の選択、およびそれらの管理策に対する監視頻度の決定は、情報システムのオーナーまたは共通管理策の提供者が策定し、運用認可責任者および上級情報セキュリティ責任者によって承認される、監視戦略に基づいて行われる。継続的なセキュリティ管理策アセスメントでは、アセサーが、運用認可責任者が定めるレベルの独立性を有することが求められる（付録 D.13 と付録 F.4 を参照）。初期および後続のセキュリティ運用認可を支援するセキュリティ管理策アセスメントは、独立したアセサーによって実施される。継続的な監視におけるアセサーの独立性は、必須ではないものの、プロセスを効率化し、再運用認可が必要な場合に、アセスメント結果の再利用を可能にする。組織は、今年度のアセスメント結果を、FISMA の年次的なセキュリティ管理策アセスメント要件に適合させるために用いることができる。本要件を満たすために、組織は、以下に示す活動のいずれかから得られるアセスメント結果を利用することができるが、これらに限定されるわけではない。(i) 情報システムの運用認可、継続的な運用認可、および正式な再運用認可（必要な場合）の一環として実施されるセキュリティ管理策アセスメント、(ii) 継続的監視活動、または (iii) システム開発ライフサイクルプロセスまたは監査の一環として行われる情報システムのテストと評価の結果（ただし、テスト、評価、または監査の結果は現時点のものとし、セキュリティ管理策の有効性についての判断に関連があり、必要なレベルの独立性を有するアセサーから入手したものであることが前提）。既存のセキュリティアセスメント結果は、それらが有効である限り再利用され、必要に応じて追加的なアセスメントによって補足される。アセスメント情報の再利用は、費用対効果の高い、完全に統合されたセキュリティプログラムの構築には不可欠である。このようなセキュリティプログラムによって、情報システムのセキュリティ状態の判断に必要な、証拠の作成が可能になる。セキュリティ管理策アセスメントを支援する自動化ツールを使用することによって、組織が策定する監視戦略に適合する高頻度、かつ大量のアセスメントが容易になる。

参考文書: NIST Special Publication 800-53A。

継続的な是正活動

タスク 6-3: 継続的監視活動の結果、リスクアセスメント結果、および行動計画とマイルストーンにリストアップされている重要な項目に基づいて、是正活動を実施する。

主な責任を持つ者: 情報システムのオーナーまたは共通管理策の提供者

補助的な役割: 運用認可責任者または指名された代理人、情報のオーナー／スチュワード、情報システムセキュリティ責任者、情報システムセキュリティエンジニア、セキュリティ管理策アセサー

SDLCのフェーズ: 運用／保守

補足ガイダンス: 継続的な監視期間中にアセサーが生成したアセスメント情報は、最新のセキュリティアセスメントレポートとして、情報システムのオーナーおよび共通管理策の提供者に提供される。情報システムのオーナーまたは共通管理策の提供者は、行動計画とマイルストーンにリストアップされている重要な項目と、セキュリティ管理策の継続的な監視期間中に生成された結論に対する是正活動を開始する。セキュリティ管理策のアセサーが、適切な是正活動に関する推奨事項を示す場合がある。リスクアセスメント（正式なものと、そうでないもの）は、継続的な是正活動の実施に関する情報を、組織的判断を行う者に提供する。継続的な監視プロセスにおいて修正／強化／追加されたセキュリティ管理策については、アセサーによる再アセスメントが行われる。これは、弱点または欠陥を排除する、あるいは特定されたリスクを軽減するための、適切な是正活動が確実に実施されるようにするためにも、重要である。

参考文書: NIST Special Publications 800-30, 800-53, 800-53A; CNSS Instruction 1253。

重要な更新

タスク 6-4: 継続的監視プロセスの結果に基づいて、セキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーンを更新する。

主な責任を持つ者: 情報システムのオーナーまたは共通管理策の提供者

補助的な役割: 情報のオーナー／スチュワード、情報システムセキュリティ責任者

SDLCのフェーズ: 運用／保守

補足ガイダンス: 情報システムの運用および使用により生じるリスクに対する、リアルタイムに近いマネジメントを容易にするために、組織は、セキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーンを継続的に更新する。更新されたセキュリティ計画は、情報システムのオーナーまたは共通管理策の提供者が実施するリスク軽減活動に基づいた、セキュリティ管理策に対するすべての変更を反映したものとなる。更新されたセキュリティアセスメントレポートは、セキュリティ計画および導入されている管理策に対する変更後の、セキュリティ管理策の有効性を判断するために実施される、追加のアセスメント活動を反映したものとなる。更新された行動計画とマイルストーンには、(i) 計画にリストアップされている重要な項目の進捗状況についての報告 (ii) セキュリティ影響分析またはセキュリティ管理策の監視中に発見された脆弱性に対する言及 (iii) 情報システムのオーナーまたは共通管理策の提供者が、それらの脆弱性にどのように対処しようとしているかに関する記述が含まれる。これらの主要な更新がもたらす情報は、情報システム（および、システムによって継承される共通管理策）の最新のセキュリティ状態に対する意識を向上させるのに役立つと同時に、継続的な運用認可およびリアルタイムに近いリスクマネジメントのプロセスを支援する。

リスクマネジメント関連の情報に対する更新の頻度は、情報システムのオーナー、共通管理策の提供者、および運用認可責任者が、連邦政府のポリシーおよび組織のポリシーに従って自由に設定することができる。情報システム（および、システムによって継承される共通管理策）のセキュリティ状態に関する情報の更新は、正確、かつ、タイムリーに行わなければならない。なぜならば、このような情報が、継続的なセキュリティ関連活動と、組織内の運用認可責任者や他のシニアリーダーによる意思決定に影響を与えるからである。自動化された支援ツールと、組織全体にわたる効果的なセキュリティプログラムマネジメントプラクティスを用いることによって、運用認可責任者は、システム固有の管理策、ハイブリッド管理策、および共通管理策の現行の有効性を含む、情報システムの最新のセキュリティ状態に容易にアクセスできる。

セキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーンに含まれる重要な情報を更新する際には、監視、管理、および監査のために必要となる元の情報が改変されたり、破壊されることがないように注意する。厳密な構成管理および構成制御に関する手順（バージョンの管理を含む）を用いて情報に対する変更を長期にわたって追跡するための効果的な手法を用意することは、(i) 組織の情報セキュリティ活動の透明性を確保し、(ii) 各セキュリティ関連活動に対する個別の説明責任がなされるようにし、かつ (iii) 組織の情報セキュリティプログラムの最新動向について理解を深めるために、必要である。

参考文書: NIST Special Publication 800-53A。

セキュリティ状況の報告

タスク 6-5: 監視戦略に従って、継続的に、情報システムのセキュリティ状況（情報システムに導入されるセキュリティ管理策、および情報システムによって継承されるセキュリティ管理策の有効性を含む）を運用認可責任者および組織内の他の適切な職員に報告する。

主な責任を持つ者: 情報システムのオーナーまたは共通管理策の提供者

補助的な役割: 情報システムセキュリティ責任者

SDLCのフェーズ: 運用／保守

補足ガイダンス: 監視活動の結果は、監視戦略に従って継続的に記録されると同時に、運用認可責任者への報告がなされる。セキュリティ状況の報告は、(i) イベント駆動型（情報システムやその運用環境に変更があった場合、またはシステムへの侵害が発生した場合） (ii) 時間駆動型（たとえば、週ごとに、月ごとに、3カ月ごとに）、または (iii) その両方（イベントおよび時間駆動型）であることが考えられる。セキュリティ状況の報告は、運用認可責任者をはじめとする組織内のシニアリーダーに対して、導入されているセキュリティ管理策の有効性を含む、情報システムのセキュリティ状態に関する極めて重要な情報を提供する。セキュリティ状況の報告には、情報システムのオーナーまたは共通管理策の提供者が採用する継続的監視活動についての記述が含まれる。また、セキュリティ状況の報告は、セキュリティ管理策のアセスメント、セキュリティ影響分析、およびセキュリティ管理策の監視中に発見された、情報システムおよびシステムの運用環境の脆弱性について、ならびに情報システムのオーナーまたは共通管理策の提供者が、それらの脆弱性にどのように対処しようとしているかについても言及する。セキュリティ状況の報告に関する広さ、深さ、および形式については、大きな自由度と柔軟性が組織に与えられている。セキュリティ状況の報告では、組織に最も適していると考える形式がとられる。その目的は、組織の任務および業務機能の観点から、情

報システムおよびシステムの運用環境の最新のセキュリティ状態を伝達する、シニアリーダーとの間の継続的なコミュニケーションの効率化と費用対効果の向上にある。少なくともセキュリティ状況の報告には、セキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーンに対する主な変更についての要約が含まれる。自動化された管理ツールを使用することで、セキュリティ状況の報告を効率よく、かつ、タイムリーに行うことができる。セキュリティ状況の報告の頻度は、連邦政府のポリシーおよび組織のポリシーに従って、組織の自由裁量で決定される。状況の報告は、適切な間隔で行われ、情報システムに関するセキュリティ関連の重要な情報（情報システムに導入されている、または、情報システムによって継承されるセキュリティ管理策の現在の有効性に関する情報を含む）が伝送されるが、その頻度は、不必要な作業が発生しない程度に設定される。運用認可責任者は、上級情報セキュリティ責任者およびリスクエグゼクティブ（機能）の協力のもと、セキュリティ状況報告書の内容を参考に、正式な再運用認可が必要であるか否かを判断する。セキュリティ状況報告書は、連邦政府のポリシーおよび組織のポリシーに従って、適切なマーク付け、保護、および取り扱いがなされる。組織の判断によって、セキュリティ状況報告書を、セキュリティ関連のすべての弱点または欠陥を修正する活動の文書化に関する、FISMA 報告要件を満たすのを支援するために用いることができる。この状況報告は、継続的に行われることを目的としたものであり、初期の運用認可判断のために提供される情報に関連する、所要時間、費用、および形式を求めるものであると解釈すべきではない。むしろ、この報告は、報告を行う目的が達成させるように、かつ、費用対効果が最も高くなるように実施される。

参考文書: NIST Special Publication 800-53A。

継続的なリスク判断および受容

タスク 6-6: 監視戦略に従って、情報システムのセキュリティ状況に関する報告内容（情報システムに導入される、または情報システムによって継承されるセキュリティ管理策の有効性を含む）を継続的に見直すことによって、組織の業務、組織の資産、個人、他の組織、または国家に対するリスクが、ひきつづき受容可能か否かを判断する。

主な責任を持つ者: 運用認可責任者

補助的な役割: リスクエグゼクティブ（機能）、運用認可責任者が指名する代理人、上級情報セキュリティ責任者

SDLCのフェーズ: 運用／保守

補足ガイダンス: 運用認可責任者または指名された代理人は、情報システムのセキュリティ状況に関する報告内容（導入されているセキュリティ管理策の有効性を含む）を継続的に見直すことによって、組織の業務や資産、個人、他の組織、または国家が現在直面しているリスクを特定する。運用認可責任者は、適宜、運用認可責任者が指名した代理人、上級情報セキュリティ責任者、およびリスクエグゼクティブ（機能）から情報を入手し、現存するリスクが受容可能か否かを判断して、情報システムのオーナーまたは共通管理策の提供者に適切な指示を出す。セキュリティ状況に関する情報を取得、編成、定量化、視覚的に表示、および維持管理する自動化された支援ツールを使用することで、組織全体にわたるリスク状況に対するリアルタイムに近いリスクマネジメントの概念が推進される。メトリクスとダッシュボードを使用することで、組織は、自動化ツールが生成したデータを整理して、その結果を分かりやすいフォーマットで組織内のさまざまなレベルの意思決定者に提供することができるため、リスクベースの判断を行うための組織の能力が向上する。組織が直面しているリスクは、セキュリティ状況報告書が提供する情報に基づいて、時間の経過とともに変化する可能性がある。変化する状況が、情報システムに関連する任務上／業務上のリスクにどのような影響を与えるかを判断することは、適切なセキュリティを維持するうえで不可欠である。継続的なリスク判断とリスク受容を実施することで、運用認可責任者は、長期にわたってセキュリティ運用認可を維持することができる。正式な再運用認可活動は、連邦政府のポリシーまたは組織のポリシーに従って発生するものであり、不必要に実施されることはない。運用認可責任者は、最新のリスク判断および受容結果をリスクエグゼクティブ（機能）に伝達する。

参考文書: NIST Special Publications 800-30, 800-39。

情報システムの切り離しおよび廃止

タスク 6-7: 必要に応じて、情報システムの廃止戦略を実施する。この戦略は、システムがサービスから切り離された時に必要となる活動を実施するためのものである。

主な責任を持つ者: 情報システムのオーナー

補助的な役割: リスクエグゼクティブ（機能）、運用認可責任者が指名する代理人、上級情報セキュリティ責任者、情報のオーナー／スチュワード、情報システムセキュリティ責任者

SDLCのフェーズ: Disposal.

補足ガイダンス: 連邦政府の情報システムが運用から外された場合に実施すべきリスクマネジメント関連の活動は、数多く存在する。組織は、情報システムの切り離しと廃止を取り扱うすべてのセキュリティ管理策（媒体のサニタイズ（記録の抹消）、構成管理および構成制御）を確実に実施する。組織の追跡管理システム（在庫システムを含む）に対しては、サービスから除外される情報システムコンポーネントが示されるようにするための更新が行われる。セキュリティ状況報告書は、情報システムの最新の状況を反映したものとなる。廃止された情報システムにホスティングされていたユーザおよびアプリケーションのオーナーは、適宜、（廃止に関する）通知を受けることになり、セキュリティ管理策のすべての継承関係について、それらの関係がもたらす影響を判断するための見直しと評価が行われる。この作業は、情報システムから切り離されたサブシステム、または廃止されたサブシステムにも適用される。サブシステムの切り離し／廃止がもたらす影響は、そのサブシステムが常駐していた情報システム（動的なサブシステムの場合には、そのサブシステムが能動的に導入された情報システム）全般の運用に対する影響の観点から評価される。

参考文書: NIST Special Publications 800-30, 800-53A。

マイルストーンチェックポイント #6

- 組織は、継続的監視戦略に従って、導入されている**セキュリティ管理策**の有効性を含む、**情報システム**やその**運用環境**に対する変更を効果的に監視しているか？
- 組織は、情報システムおよびシステムの運用環境において特定された変更がもたらす**セキュリティ上の影響**を効果的に分析しているか？
- 組織は、監視戦略に従って**セキュリティ管理策の継続的なアセスメント**を実施しているか？
- 組織は、情報システムおよびシステムの運用環境において特定された弱点と欠陥を克服するに必要な**是正活動**を継続的に実施しているか？
- 組織は、情報システムおよびシステムの運用環境の**セキュリティ状況**を運用認可責任者、および組織内の指定された他のシニアリーダーに報告するための、効果的なプロセスを実施しているか？
- 組織は、継続的監視活動に基づいて、**リスクマネジメント**に関するきわめて重要な**ドキュメント**を更新しているか？
- 運用認可責任者は、効果的な継続的監視活動を採用し、最新のリスク判断および受容結果を情報システムのオーナーおよび共通管理策の提供者に伝達することによって、**継続的なセキュリティ運用認可**を実施しているか？

付録 A

参考文献

法律、ポリシー、指令、指示、基準、およびガイドライン

法律

1. E-Government Act [includes FISMA] (P.L. 107-347), 2002 年 12 月.
2. Federal Information Security Management Act (P.L. 107-347, Title III), 2002 年 12 月.
3. Paperwork Reduction Act (P.L. 104-13), 1995 年 5 月.

ポリシー、指令、指示

1. Committee on National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, 2006 年 6 月.
2. Committee on National Security Systems (CNSS) Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, 2009 年 10 月.
3. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, 2000 年 11 月.
4. Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, 2001 年 10 月.

基準

1. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, 2004 年 2 月.
2. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, 2006 年 3 月.

ガイドライン

1. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, 2006 年 2 月.
2. National Institute of Standards and Technology Special Publication 800-27, Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, 2004 年 6 月.
3. National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, 2002 年 7 月.
4. National Institute of Standards and Technology Special Publication 800-39 (Second Public Draft), *Managing Risk from Information Systems: An Organizational Perspective*, 2008 年 4 月.

5. National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, 2009 年 8 月.

6. National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, 2008 年 7 月.

7. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, 2003 年 8 月.

8. National Institute of Standards and Technology Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, 2008 年 8 月.

9. National Institute of Standards and Technology Special Publication 800-70, Revision 1, *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*, 2009 年 9 月.

付録 B

用語集

用語とその定義

この付録では、SP800-37 で用いられているセキュリティ用語の定義を示す。特に明記しない限り、本文書で使用されるすべての用語は、国家安全保障システム委員会（CNSS: Committee for National Security Systems）の指示 4009、国家情報保証に関する用語集（National Information Assurance Glossary）の定義に従うものとする。

適切なセキュリティ (Adequate Security) [OMB Circular A-130, Appendix III]	情報の消失、誤用／悪用、情報への不正アクセスもしくは、改ざんがもたらす危険性や被害の大きさに比例するセキュリティ。これには、管理面、人事面、運用面、および技術面での費用対効果の優れた管理策を導入することによって、政府機関が使用するシステムおよびアプリケーションが効率的に機能することと、適切な機密性、完全性、および可用性が提供されることを保証することが含まれる。
政府機関 (Agency)	＜執行機関（Execution Agency）＞を参照。
割り当て (Allocation)	各セキュリティ管理策がシステム固有の管理策、ハイブリッド管理策、または共通管理策のうち、いずれの管理策として定義されているかを判断するのに用いられるプロセス。 特定のセキュリティ機能を提供することに責任を持つ情報システムコンポーネント（たとえば、ルータ、サーバー、リモートセンサーなど）にセキュリティ管理策を割りつけるのに用いられるプロセス。
アプリケーション (Application)	情報システムにホスティングされるソフトウェアプログラム。
アセスメント (Assessment)	＜セキュリティ管理策アセスメント（Security Control Assessment）＞を参照。
アセサー (Assessor)	＜セキュリティ管理策アセサー（Security Control Assessor）＞を参照。
保証 (Assurance)	情報システムへの意図されたセキュリティ管理策一式の適用が有効であることに対する信頼の根拠。
運用認可 (Authorization (to operate))	情報システムの運用認可。情報システムの運用を認可し、合意されたセキュリティ管理策の導入について組織の業務（任務、機能、イメージまたは評判を含む）、組織の資産、個人、他の組織、および国家に対するリスクを明示的に受容する、といった組織の高官による正式な管理判断。

認可境界（運用認可が及ぶ範囲） (Authorization Boundary)	運用認可責任者によって認可されるべき情報システムのすべてのコンポーネント（情報システムが接続されているシステムであっても、個別に運用認可を受けたものは含まない）。
運用認可プロセス (Authorize Processing)	＜運用認可（Authorization）＞を参照。
運用認可責任者 (Authorizing Official)	組織の業務（任務、機能、イメージまたは評判を含む）、組織の資産、個人、他の組織、および国家に対する（容認レベルの）リスクを受容し、情報システムの運用に正式な責任を負う政府機関の高官。
運用認可責任者が指名する代理人 (Authorizing Official Designated Representative)	セキュリティ運用認可に関連する必要な活動を運用認可責任者に代わって実施・調整する職員。
可用性 (Availability) [44 U.S.C., Sec. 3542]	情報へのタイムリーで信頼のおけるアクセスと利用の確保。
最高情報責任者 (Chief Information Officer) [PL 104-106, Sec. 5125(b)]	以下の項目に責任を負う、政府機関の高官： (i) 法律、大統領令、指令、ポリシー、規定や政府機関の上層部によって定められた優先順位に基づいた方法で情報技術が調達され、情報資源が管理されていることを確実にするために、政府機関の執行部の長官や政府機関の他の上級管理職に対して助言や様々な支援を提供すること。 (ii) 政府機関のための健全で統合された情報技術アーキテクチャの開発、維持および導入促進。 (iii) 政府機関のすべての主要情報資源管理プロセスに関して、効果的かつ効率的な設計および運用を促進する。この活動には、政府機関の作業プロセスの改良も含まれる。 注：連邦政府の下位組織では、政府機関レベルの最高情報責任者が担うセキュリティ責務と類似の責務を担う個人を示す用語として、「最高情報責任者」を用いる場合がある。
最高情報セキュリティ責任者 (Chief Information Security Officer)	＜政府機関の上級情報セキュリティ責任者（Senior Agency Information Security Officer）＞を参照。
共通管理策 (Common Control)	単独または複数の情報システムによって継承されるセキュリティ管理策。＜セキュリティ管理策の継承（Security Control Inheritance）＞を参照。
共通管理策の提供者 (Common Control Provider)	共通管理策の開発、実施、アセスメント、および監視に責任を持つ職員（すなわち、情報システムによって継承されるセキュリティ管理策）。

代替管理策 (Compensating Security Controls)	NIST SP 800-53 に記載されている影響度が低位、中位または高位のベースライン内の推奨管理策の代わりに採用できる、管理面、運用面、および技術面での管理策（すなわち、保護手段または対策）であり、情報システムに対して NIST の管理策と同等の（または匹敵する）保護を提供する。
機密性 (Confidentiality) [44 U.S.C., Sec. 3542]	個人のプライバシーや占有情報の保護手段を含む情報へのアクセスや公開の制限（正式に認定されたもの）を保持すること。
構成管理 (Configuration Control) [CNSSI 4009]	ハードウェア、ファームウェア、ソフトウェアに対する変更管理（変更の文書化を含む）プロセス。情報システムが導入される前後、または導入中に不適切な変更が加えられることで、システムが被害に遭うことを、このプロセスにより、防ぐことができる。
管理されたインターフェース (Controlled Interface)	セキュリティポリシーを実施し、相互接続されている情報システム間の情報のフローを制御する一連のメカニズムを備えた境界。.
対抗策／対策 (Countermeasures) [CNSSI 4009]	情報システムの脆弱性を削減するための活動、手段、手順、技術または、これ以外の対策。セキュリティ管理策（security control）および保護手段（safeguard）と同義。
クロスドメインソリューション (Cross Domain Solution)	管理されたインターフェースの一種。手動／自動による、異なるセキュリティドメイン間での情報へのアクセスや情報の転送を可能にする。
ドメイン (Domain) [CNSSI 4009]	共通のセキュリティポリシー、セキュリティモデル、またはセキュリティアーキテクチャの規定に従って、リソースへのアクセス権を有する一連のシステムリソース、または一連のシステムエンティティを含む、環境またはコンテクスト。＜セキュリティドメイン（Security Domain）＞を参照。
動的サブシステム (Dynamic Subsystem)	情報システムの実行段階において一時的に存在するサブシステム。動的なサブシステムを使用するアーキテクチャには、サービス指向型アーキテクチャやクラウドコンピューティングアーキテクチャなどがある。
運用環境 (Environment of Operation)	情報システムによる情報の処理、格納、および伝送が行われる物理的な環境。
政府機関(Executive Agency) [41 U.S.C., Sec. 403]	5 U.S.C., Sec. 101 で特定する執行部門、5 U.S.C., Sec. 102 で特定する軍の部局、5 U.S.C., Sec. 104（1）で定義される独立機関および 31 U.S.C., 91 章の規定を全面的に満たしている完全に政府が所有する企業。
外部情報システム（またはコンポーネント） (External Information System (or Component))	組織の認可が及ぶ範囲外にある情報システムまたは情報システムを構成するコンポーネント。通常、組織は、これらのシステムやコンポーネントに対して、必要なセキュリティ管理策の適用や、セキュリティ管理策の有効性のアセスメントに関する直接的な制御を行うことはできない。

外部情報システムサービス (External Information System Service)	組織の情報システムの運用認可が及ぶ範囲外で実施される情報システムサービス（すなわち、組織の情報システムによって利用されるサービスではあるが、そのシステムの一部ではないもの）。通常、組織は、これらのシステムに対して、必要なセキュリティ管理策の適用や、セキュリティ管理策の有効性のアセスメントに関する直接的な制御を行うことはできない。
外部情報システムサービスプロバイダ (External Information System Service Provider)	組織に対して、多様な消費者－提供者の関係に基づき、外部情報システムサービスを提供する者。消費者－提供者の関係には、ジョイントベンチャー、ビジネスパートナーシップ、外注契約（すなわち、契約、省庁間の取り決め、業務分野についての取り決めを介して）、ライセンス契約および／またはサプライチェーンの交換などが含まれるが、これらに限られるわけではない。
連邦政府機関 (Federal Agency)	＜執行機関（Executive Agency）＞を参照。
連邦政府の情報システム (Federal Information System) [40 U.S.C., Sec. 11331]	執行機関、執行機関の契約者、または執行機関の代わりとなる他の組織によって使用または運用される情報システム。
影響度が高位のシステム (High-Impact System) [FIPS 200]	FIPS 199 に従って分類を行った結果、少なくとも 1 つのセキュリティ目的（機密性、完全性、または可用性）の潜在的な影響度が高位であると判断された情報システム。
ハイブリッドセキュリティ管理策 (Hybrid Security Control)	情報システムに導入されているセキュリティ管理策の一種。共通管理策としての役割と、システム固有の管理策としての役割を併せ持つ。 ＜共通管理策（Common Control）＞と＜システム固有のセキュリティ管理策（System-Specific Security Control）＞を参照。
情報 (Information) [FIPS 199]	情報のタイプ実体。
情報システムのオーナー (Information Owner) [CNSSI 4009]	特定の情報に対する法的権限または運用権限を持ち、その情報の生成、収集、処理、配布および廃棄に関する管理策の制定に責任を負う高官。
情報資源 (Information Resources) [44 U.S.C., Sec. 3502]	情報および関連資源（人的資源、設備、資金、情報技術など）。
情報セキュリティ (Information Security) [44 U.S.C., Sec. 3542]	機密性、完全性および可用性を確保するために、情報と情報システムを不正アクセス、誤用／悪用、意図しない公開、中断・途絶、改ざんまたは破壊から保護すること。

情報セキュリティアーキテクト (Information Security Architect)	リファレンスモデル、セグメントおよびソリューションアーキテクチャ、ならびに組織の主要な任務および業務プロセスを支援する最終的な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すべての側面において、組織の主要な任務および業務プロセスを保護するのに必要な情報セキュリティ要求事項が十分に考慮されることに責任を持つ、個人、グループ、または組織。
情報セキュリティポリシー (Information Security Policy) [CNSSI 4009]	組織がどのように情報を管理、保護し配布すべきかを定めている指令、規定、規則および慣行を一つにまとめたもの。
情報セキュリティプログラム計画 (Information Security Program Plan)	組織全体にわたる情報セキュリティプログラムに課せられるセキュリティ要求事項の概要を提供し、これらの要求事項を満たすために既に導入されている、または導入が計画されているプログラムマネジメント管理策および共通管理策を記述する正式な文書。
情報スチュワード (Information Steward)	その情報がどのエンティティまたはソースによって発信、作成、または収集されたかにかかわらず、国家全体に属するすべての連邦政府情報を慎重に、かつ信頼できる形で管理することを支援する個人またはグループ。情報スチュワードは、連邦政府のエレメントおよび連邦政府の顧客が連邦政府の情報に最大限にアクセスできることを保証する。この際、FISMA の規定に従って情報を保護する義務と、セキュリティに関する政府機関のポリシー、指令、規定、基準、およびガイダンスのうち、関連するすべてのものとのバランスを考慮しなければならない。
情報システム (Information System) [44 U.S.C., Sec. 3502]	情報の収集、処理、メンテナンス、利用、共有、配布または廃棄のために編成された情報資源の独立した集まり。
情報システムの境界 (Information System Boundary)	＜認可境界（運用認可が及ぶ範囲）（Authorization Boundary）＞を参照。
情報システムのオーナー（または、プログラムマネージャ） (Information System Owner (or Program Manager))	情報システム全体の調達、開発、統合、訂正または運用とメンテナンスの担当責任官。
情報システムセキュリティエンジニア (Information System Security Engineer)	情報システムセキュリティエンジニアリング活動の実施に責任を持つ個人。
情報システムセキュリティエンジニアリング (Information System Security Engineering)	情報セキュリティ要求事項を把握・改良し、洗練された要求事項を意図的なセキュリティ設計またはセキュリティ構成を通じて各ITコンポーネント製品および情報システムに確実に組み入れることを可能にするプロセス。

情報システム関連のセキュリティリスク (Information System-related Security Risks)	情報または情報システムの機密性、完全性、または可用性の喪失により生じるリスク。情報システム関連のセキュリティリスクの評価では、組織（資産、任務、機能、イメージ、または評判を含む）、個人、他の組織、および国家に及ぶ影響が考慮される。＜リスク（Risk）＞を参照。
情報システムセキュリティ責任者 (Information System Security Officer) [CNSSI 4009]	情報システムまたはプログラムに関する運用面での適切なセキュリティ状況を維持することに責任を持つ個人。
情報技術 (Information Technology) [40 U.S.C., Sec. 1401]	データまたは情報の自動的な入手、格納、操作、管理、移動、制御、表示、切り替え、交換、送信、または受信のために政府機関の執行部門によって利用される機器、相互接続されたシステムまたは機器のサブシステム。上記の文章が示す目的のために、執行部門が機器を直接用いる場合には、機器は執行部門によって使用され、契約者が執行部門と以下のような契約を結んでいる場合には、機器は契約者によって使用される。(i) そのような機器の使用が要求されている (ii) サービスの実行や製品の設置において、そのような機器をかなりの程度使用することが要求されている。情報技術の定義には、コンピュータ、補助機器、ソフトウェア、ファームウェアや類似の手続き、サービス（補助サービスを含む）および関連するリソースが含まれる。
情報の種類 (Information Type) [FIPS 199]	組織あるいは、状況によっては、特定の法律、大統領令、指令、ポリシーまたは規制などによって定められている情報の具体的な分類（例：プライバシー、医療、占有、財務、調査、契約者機密、セキュリティ管理など）。
完全性 (Integrity) [44 U.S.C., Sec. 3542]	不正な改ざんまたは破壊から情報を保護すること。（情報の否認防止および真正性の確保を含む）
ジョイント運用認可 (Joint Authorization)	複数の運用認可責任者によるセキュリティ運用認可。
影響度が低位のシステム (Low-Impact System) [FIPS 200]	FIPS 199 に従って分類を行った結果、すべてのセキュリティ目的（機密性、完全性、または可用性）の潜在的影響度が低位であると判断された情報システム。
管理面における管理策 (Management Controls) [FIPS 200]	情報システムのリスク管理やセキュリティの管理に的を絞ったセキュリティ管理策（例：予防手段または対策）。
影響度が中位のシステム (Moderate-Impact System) [FIPS 200]	FIPS 199 に従って分類を行った結果、少なくとも 1 つのセキュリティ目的（機密性、完全性、または可用性）の潜在的影響度が中位であり、潜在的影響度が高位のセキュリティ目的がひとつもないと判断された情報システム。

国家安全保障にかかわるシステム (National Security System) [44 U.S.C., Sec. 3542]	政府機関、政府機関の委託業者または政府機関の代わりとなる他の組織によって使用される／運用されるすべての情報システム（すべての通信システムを含む）とは (i) システムの機能、運用、利用が、インテリジェンス活動、国家安全保障にかかわる暗号活動、軍隊の指揮統制、武器または武器システムの一部として一体化した機器に関連するシステム、または、軍隊またはインテリジェンス任務の達成に直結する重要なシステム（日常的な管理業務や業務アプリケーションに用いられる、例えば、給与、財務、物流および人材管理のアプリケーションを除く）。 (ii) 特定の手順に従って常に保護されるシステム。ここでいう特定の手順とは、大統領令、あるいは議会制定法が定める基準に従って判断した結果、国家防衛や外交政策上の利益の観点から機密にすることが特別に許可された情報を対象として確立された手順である。
ネット中心のアーキテクチャ (Net-centric Architecture)	情報の共有と連携を向上させるためにネットワークで相互接続された人、デバイス、情報およびサービスから成る、継続的に進化する複雑なコミュニティの一部であるサブシステムおよびサービスによって構成される、複雑な情報システム。サブシステムおよびサービスは、同じエンティティが開発または所有する場合と、そうでない場合がある。また、一般的に、複数のシステムから成る複雑なシステムのライフサイクル全体を通して存在し続けるわけではない。このアーキテクチャの例として、サービス指向型アーキテクチャやクラウドコンピューティングアーキテクチャがある。
運用面における管理策 (Operational Controls) [FIPS 200]	情報システムに対するセキュリティ管理策で、（システムによって導入・実行されるセキュリティ管理策とは対照的に）主に人によって導入され実行されるセキュリティ管理策(予防手段または、対策ともいう）。
組織 (Organization) [FIPS 200, Adapted]	組織的な構造（たとえば、連邦政府機関、または、該当する場合、連邦政府機関の運用上のあらゆるエレメント）内のエンティティ（その規模、複雑さ、または位置づけは問わない）。
行動計画とマイルストーン (Plan of Action and Milestones) [OMB Memorandum 02-01]	達成すべきタスクを明確化する文書：行動計画とマイルストーンは、計画の中の項目の達成に必要な資源、タスクに見合ったすべてのマイルストーン、およびそのマイルストーンの完了予定日を詳述したものである。
潜在的影響 (Potential Impact) [FIPS 199]	低位： 機密性、完全性または可用性の喪失が、組織の業務、組織の資産または個人に対し*僅かな*マイナスの影響を及ぼすことが予想される。 中位：機密性、完全性または可用性の喪失が、組織の業務、組織の資産または個人に対し*重大な*マイナスの影響を及ぼすことが予想される。 高位： 機密性、完全性または可用性の喪失が、組織の業務、組織の資産または個人に対し*重度*のまたは*壊滅的な*マイナスの影響を及ぼすことが予想される。

互恵契約 (Reciprocity)	情報システムリソースの再利用や、互いのセキュリティ状態の評価結果を受け入れることによる情報共有を目的として、参加している組織間で、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に合意すること。
リスク (Risk) [FIPS 200, Adapted]	発生しうる状況またはイベントによって、エンティティが脅かされる度合いの尺度であり、通常、(i) 当該の状況またはイベントが発生した場合にもたらされると考えられる悪影響と、(ii) 発生の可能性との、関数によって求められる。 [注:情報システム関連のセキュリティリスクとは、情報または情報システムの機密性、完全性、または可用性の喪失により生じるリスクであり、組織の業務(任務、機能、イメージ、または評判を含む)、組織の資産、個人、他の組織、および国家に及ぶ可能性があるマイナスの影響を表す。国家に対するマイナスの影響には、たとえば、極めて重要なインフラアプリケーションを支援する情報システムに対する侵害、または、国土安全保障省が規定する政府機関の業務の継続にとって不可欠な情報システムに対する侵害が含まれる。]
リスクアセスメント (Risk Assessment)	情報システムの運用により生じる、組織の業務(任務、機能、イメージ、評判を含む)、組織の資産、個人、他の組織、および国家へのリスクを特定するプロセス。リスクマネジメントの一部であり、リスク分析と同義で、脅威や脆弱性の分析などが含まれる。リスクアセスメントでは、計画中、または実施中のセキュリティ管理策による、リスクや脆弱性の軽減を考慮する。
リスクエグゼクティブ(機能) (Risk Executive (Function))	以下の項目が確実に行われることを支援する、組織内の個人またはグループ。(i) 個々の情報システムに対するセキュリティリスク関連の考慮事項(運用認可判断を含む)が、組織の任務および業務機能を実施するうえでの、組織全体的な戦略的目標および目的と照らし合わせて、組織全体的な観点から捉えられるようにすること、ならびに (ii) 情報システム関連のセキュリティリスクの管理が、組織全体にわたって一貫していて、組織のリスク許容度を反映すると同時に、任務／業務の成功の妨げとなる他のリスクとともに考慮されること。
リスクマネジメント (Risk Management) [FIPS 200, Adapted]	情報システムの運用により生じる、組織の業務(任務、機能、イメージ、評判を含む)、組織の資産、個人、他の組織、および国家へのリスクを管理するプロセス。これには、(i) リスクアセスメントの実施、(ii) リスク軽減戦略の実施、および (iii) 情報システムのセキュリティ状態を継続的に監視するための技術および手続きの採用が含まれる。
予防手段 (Safeguards) [CNSSI 4009]	情報システムに対して規定されたセキュリティ要求事項(すなわち、機密性、完全性および可用性)を満たすために指定された保護対策。予防手段には、セキュリティ機能、管理規約、人的セキュリティや物理的な構築物、領域やデバイスのセキュリティなどが含まれる。セキュリティ管理策や対策と同義。

セキュリティ運用認可 (Security Authorization)	＜運用認可（Authorization）＞を参照。
セキュリティ分類 (Security Categorization)	情報または情報システムのセキュリティ分類を決定するプロセス。国家安全保障にかかわるシステムと、そうでないシステムのセキュリティ分類に関する方法論については、それぞれ、CNSS Instruction 1253 と FIPS 199 に記載されている。
セキュリティ管理策 (Security Controls) [FIPS 199]	システムとその情報の機密性、完全性および可用性を保護するために、情報システムに対して規定された、管理、運用および技術の各側面からの管理策（すなわち、予防手段または対策）。
セキュリティ管理策アセスメント (Security Control Assessment)	セキュリティ管理策がどの程度正しく導入されているか、どの程度意図した通りに運用されているか、システムのセキュリティ要求事項に対する適合性の観点から所望の結果をどの程度産出しているかを判断するための、情報システムの管理、運用、技術の各側面からのセキュリティ管理策のテストおよび／または評価。
セキュリティ管理策アセサー (Security Control Assessor)	セキュリティ管理策アセスメントの実施に責任を持つ個人、グループ、または組織。
セキュリティ管理策の継承 (Security Control Inheritance)	情報システムまたはアプリケーションが、それらのシステムまた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（システムまたはアプリケーションが設置されている組織にとって内部または外部のエンティティ）によって開発、実施、アセスメント、運用認可、監視されるセキュリティ管理策の保護を受けている状況。＜共通管理策（Common Control）＞を参照。
セキュリティドメイン (Security Domain) [CNSSI 4009]	セキュリティポリシーを実施するドメイン。単独の機関によって管理される。
セキュリティ影響分析 (Security Impact Analysis)	情報システムに対する変更が、システムのセキュリティ状態にどの程度の影響を与えたかを判断するために、運用認可責任者によって実施される分析。
セキュリティ目的 (Security Objective) [FIPS 199]	機密性、完全性または可用性。
セキュリティ計画 (Security Plan)	情報システムまたは情報セキュリティプログラムのセキュリティ要求事項の概要を示し、これらの要求事項を満たすために既に導入されている、または導入が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。＜システムセキュリティ計画（System Security Plan）＞または＜情報セキュリティプログラム計画（Information Security Program Plan）＞を参照。
セキュリティポリシー (Security Policy) [CNSSI 4009]	セキュリティサービスの提供に関する一連の基準。

セキュリティ要求事項 (Security Requirements) [FIPS 200]	処理、格納または伝送されている情報の機密性、完全性および可用性を確保するために、情報処理システムに課される要求事項。これらの要求事項は、適用される法律、大統領令、指令、方針、基準、指示、規定、手順または組織の任務／事業事例から導出される。
政府機関の上級情報セキュリティ責任者 (Senior (Agency) Information Security Officer) [44 U.S.C., Sec. 3544]	FISMA が規定する最高情報責任者の職責を果たす責任を有する高官で、最高情報責任者の、政府機関の運用認可責任者、情報システムのオーナーおよび情報システムセキュリティ責任者との最初の連絡窓口としての役割を果たす担当官。 注：連邦政府の下位組織では、政府機関の上級情報セキュリティ責任者が担う責務と類似の責務を担う個人を示す用語として「上級情報セキュリティ責任者」または「最高情報セキュリティ責任者」を用いる場合がある。
上級情報セキュリティ責任者 (Senior Information Security Officer)	＜政府機関の上級情報セキュリティ責任者（Senior Agency Information Security Officer）＞を参照。
サブシステム (Subsystem)	情報システムの主要な一部分（下位システム）であり、情報、情報技術、人員で構成され、ひとつまたは複数の特定の役割を果たす。
システム (System)	＜情報システム（Information System）＞参照。
システムセキュリティ計画 (System Security Plan) [NIST SP 800-18]	情報システムのセキュリティ要求事項の概要を示し、これらの要求事項を満たすために既に導入されている、または導入が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。
システム固有のセキュリティ管理策 (System-Specific Security Control)	共通セキュリティ管理策としては指定されていない情報システムのセキュリティ管理策、または、情報システムに導入される予定のハイブリッド管理策の一部。
調整済みのセキュリティ管理策ベースライン (Tailored Security Control Baseline)	セキュリティ管理策ベースラインに調整ガイダンスを適用することによって得られる一連のセキュリティ管理策。＜調整（Tailoring）＞を参照。
調整 (Tailoring)	セキュリティ管理策ベースラインを、以下の活動を通じて修正すること。(i) スコーピングガイダンスの適用、(ii) 代替管理策の指定(必要な場合)、(iii) 明示的な代入ステートメントと選択ステートメントを使用して、組織が定めたセキュリティ管理策パラメータの値を指定（可能な場合）。
技術面での管理策 (Technical Controls) [FIPS 200]	情報システムのセキュリティ管理策であって、システムのハードウェア、ソフトウェアまたはファームウェアに搭載されているメカニズムを経由して、主として情報システムによって導入および実行されるセキュリティ管理策（すなわち予防手段または対策）。

脅威 (Threat) [CNSSI 4009, Adapted]	組織の業務（任務、機能、イメージまたは評判を含む）、組織の資産、個人、他の組織、または国家にマイナスの影響をもたらす可能性のある状況または事象。要因としては、情報システムに対する不正アクセス、破壊、公開、情報の改ざんおよび／またはサービス妨害(DoS)などがある。
脅威源 (Threat Source) [FIPS 200]	脆弱性の意図的な悪用を目的とした意図および方法、または脆弱性の偶発的なきっかけとなる可能性のある状況や方法。脅威要因(threat agent)と同義である。
脆弱性 (Vulnerability) [CNSSI 4009]	情報システム、システムセキュリティ手順、内部統制または実装に存在する弱点で、脅威源によって悪用される、あるいは脅威源によってもたらされるもの。
脆弱性のアセスメント (Vulnerability Assessment) [CNSSI 4009]	情報システムにおける脆弱性の正式な説明と評価。

付録 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)
DoD	国防総省 (Department of Defense)
FIPS	連邦情報処理規格 (Federal Information Processing Standards)
FISMA	連邦情報セキュリティマネジメント法 (Federal Information Security Management Act)
NIST	米国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	国家情報局 (Office of the Director of National Intelligence)
OMB	行政管理予算局 (Office of Management and Budget)
RMF	リスクマネジメントフレームワーク (Risk Management Framework)

付録 D

役割と責任

リスクマネジメントプロセス参加する主要関係者

本セクションでは、組織のリスクマネジメントプロセスに関与する主な担当官の役割と責任について記述する。[47] 組織には様々な任務があり、その構成も組織によって異なることを理解すれば、リスクマネジメントにかかわる役職名や、それに関する責任が組織の職員にどのように割り当てられるか（たとえば、複数の担当者にひとつの役割を割り当てる、一人の担当者に複数の役割を割り当てる、など）も異なることがあるということがわかる。[48] しかしながら、基本的な機能は同じである。本文書に記載されているリスクマネジメントフレームワークは、組織が、情報システム関連のセキュリティリスクを最も良い方法で管理し、それぞれの組織構造の内部における固有のタスクの意図を効果的に達成できるような柔軟性を持たせている。本文書内で定義付けがされているリスクマネジメントに関する役割の多くは、組織が実施する日常的なシステム開発ライフサイクルプロセスに関して定義付けがされている、いずれかの役割に対応している。組織は、可能な場合は常に、リスクマネジメントに関する役割と、システム開発ライフサイクルプロセス向けに定義付けがされた類似の（または補足的な）役割との、対応づけを行う。[49]

D.1 政府機関の長（最高経営責任者）（HEAD OF AGENCY（CHIEF EXECUTIVE OFFICER））

政府機関の長（または、最高経営責任者）は、組織の最高レベルの上級職員または管理職者であり、(i) 政府機関によって、または、政府機関の代わりとなる他の組織によって収集または維持管理される情報、ならびに (ii) 政府機関、政府機関の契約者、または政府機関の代わりとなる他の組織によって使用または運用される情報システムへの、不正アクセス、誤用／悪用、意図しない公開、中断・途絶、改ざんまたは破壊によってもたらされる危険性や被害の大きさ（すなわち、影響）に比例する、情報セキュリティ上の保護を提供することに全責任を負う。また、以下の項目が確実に実施されるようにすることも、政府機関の長の責任である。(i) 戦略的／運用上の計画策定プロセスに、情報セキュリティマネジメントプロセスを統合する (ii) 組織の上級職員が、自身の管理下にある業務と資産を支援する情報および情報システムに対する、情報セキュリティを提供する、ならびに (iii) 関連する法律、ポリシー、指令、指示、基準、およびガイドラインが規定する情報セキュリティ要求事項に適合することを支援するための十分な訓練を受けた職員を確保する。強力なポリシーを開発・実施することによって、政府機関の長は、情報セキュリティに対する組織のコミットメント、およびリスクの効果的な管理と組織が遂行する主要な任務／業務機能の保護に必要な措置に対する組織のコミットメントを確立する。政府機関の長は、情報セキュリティに関する適切な説明責任を果たし、情報セキュリティプログラムの監視と向上を積極的に支援し、監督する。情報セキュリティに対するシニアリーダーのコミットメントは、組織内に一定レベルの善管注意義務を確立し、任務および業務の成功に向けた風潮を促進するうえで重要である。

---

[47] 組織は、リスクマネジメントプロセスを支援する他の役割（例：施設管理者、人事部長、システムアドミニストレータなど）の定義付けを行うことができる。

[48] リスクマネジメントプロセスにおいて、一人の担当者が複数の役割を担う場合、この担当者には、適切な独立性が担保され、利益相反に抵触しないよう留意しなければならない。

[49] たとえば、システム開発ライフサイクルにおけるシステム開発者またはプログラムマネージャの役割は、情報システムのオーナーに、任務のオーナー／マネージャは運用認可責任者に対応づけることができる。また、システム／ソフトウェアエンジニアは、情報システムセキュリティエンジニアに対する補足的な役割を担う。

D.2 リスクエグゼクティブ（機能）（RISK EXECUTIVE（FUNCTION））

リスクエグゼクティブ（機能）は、以下の項目が確実に行われることを支援する、組織内の個人またはグループである。(i) 個々の情報システムに対するリスク関連の考慮事項（運用認可判断を含む）が、組織の主要な任務および業務機能を実施するうえでの、組織全体的な戦略的目標および目的と照らし合わせて、組織全体的な観点から捉えられるようにすること、ならびに (ii) 情報システム関連のセキュリティリスクの管理が、組織全体にわたって一貫していること、組織のリスク許容度を反映すること、および任務／業務の成功の妨げとなる他のリスクと併せて考慮されること。リスクエグゼクティブ（機能）は、組織内のシニアリーダーと連携して、以下の項目を実施する。

- リスクに対処するための、組織全体にわたる、包括的かつ全体論的なアプローチ（すなわち、組織の総合された業務に関して、社員の理解を深めることを可能にするアプローチ）を提供する。
- 組織が実施すべきリスク軽減戦略を策定する。これには、組織全体に関わる情報セキュリティ関連のリスクに対する戦略的展望が含まれる。[50]
- 運用認可責任者をはじめとするシニアリーダー間でのリスク関連情報の共有を促進する。
- P リスクの受容に関する一貫性のある、効果的な判断を支援するために、組織全体にわたるすべてのリスクマネジメント関連活動（たとえば、セキュリティ分類など）を監視する。
- 任務および業務の成功に必要なすべての要素が、運用認可判断において考慮されるようにする。
- 組織の業務と資産、個人、他の組織、および国家に対するすべてのリスク源（集約されたリスクを含む）について把握するための、組織全体にわたるフォーラムを開催する。
- 運用認可責任者間の協調と連携を促進する。これには、責任の共有を必要とする運用認可活動が含まれる。
- 外部プロバイダが提供する情報とサービスを使用して組織の任務／業務機能を支援することに対する共同責任について、必要とされる可視性を確保し、適切な意思決定機関まで段階的に通知する。
- 組織が責任を負う情報システムの運用および使用により生じる、情報へのリスクの集約に基づいて、組織のリスク状態を特定する。

リスクエグゼクティブ（機能）は、具体的な組織構造、あるいは、組織内の特定の個人またはグループに割り当てられた正式な責務を担うわけではない。政府機関／組織の長は、リスクエグゼクティブ（機能）を保持こともできれば、その機能を他の職員またはグループ（たとえば、経営指導委員会など）に委託することもできる。リスクエグゼクティブ（機能）は、米国政府から付与された権限を持ち、その役割は政府職員に対してのみ割り当てられるべきものである。

D.3 最高情報責任者（CHIEF INFORMATION OFFICER）

最高情報責任者 [51]とは、次のような項目に責任を負う組織の職員である。(i) 上級情報セキュリティ責任者の指名。 (ii) 適用され得るすべての要求事項に対応するための情報セキュリティポリシ

[50] 運用認可判断を下す運用認可責任者の見解が、時には、狭い（または、局所的である）場合がある（たとえば、運用認可責任者が、そうした判断から生じるリスクについて十分に理解していなかったり、そのようなリスクを明示的に受け入れていない場合など）。

[51] 組織が、正式に最高情報責任者を任命していない場合、FISMA は、その役職に準ずる職員によって、関連する責務が扱われ

ーや手順、コントロール技術の作成と維持。 (iii) 情報セキュリティについて重要な責任を担う職員の監視と、それらの職員が十分な訓練を受けていることの確認。 (iv) 組織の上級職員のセキュリティ責任に関する支援。 (v) 他の上級職員と協力し、復旧活動の進捗を含む組織の情報セキュリティプログラムの全般的な有効性を、年に一回政府機関の長へ報告すること。最高情報責任者は、リスクエグゼクティブ（機能）と上級情報セキュリティ責任者の助力を得て、運用認可責任者および運用認可責任者が指名する代理人と連携することにより、以下の項目が確実に行われるようにする。

- 組織全体にわたる情報セキュリティプログラムの効果的な導入。結果として、組織のすべての情報システム、およびそれらのシステムの運用環境に対する適切なセキュリティが確保される。
- 情報セキュリティに関する考慮事項の、企画／計画／予算編成のサイクル、エンタープライズアーキテクチャ、および調達／システム開発ライフサイクルへの組み入れ。
- 情報システムが承認されたセキュリティ計画の中で取り上げられること、また、その運用が認可されること。
- 組織全体にわたって必要とされる情報セキュリティ関連活動がタイムリーに、かつ効率的で費用対効果の優れた方法で実施されること。
- 適切な情報セキュリティ関連活動の一元的な報告。

また、最高情報責任者と運用認可責任者は、組織内で定められた優先順位に基づき、組織の任務および業務機能を支援する各情報システムの保護に特化したリソースの適切な割当てを決定する。選択された情報システムによっては、最高情報責任者が運用認可責任者として、または他の上級職員と共に選択された共同運用認可責任者として指名されることがある。最高情報責任者は、米国政府から付与された権限を持ち、その役割は政府職員に対してのみ割り当てられるべきものである。

D.4 情報のオーナー／スチュワード（INFORMATION OWNER/STEWARD）

情報のオーナー／スチュワードは、特定の情報に関する法的権限、管理上の権限、または運用上の権限を持ち、その情報の生成、収集、処理、配布および廃棄についてのポリシーと手順を制定することに責任を負う組織の職員である。[52] 情報が共有される環境では、情報のオーナー／スチュワードが、対象となる情報の適切な利用と保護のための規則（たとえば、行動規範）を制定することに責任を負う。この責任は、情報を共有する（あるいは提供する）相手が別の組織であっても存続する。情報システムによって処理、格納、または伝送される情報のオーナー／スチュワードは、情報システムのオーナーである場合もあれば、そうではない場合もある。さらに、一つの情報システムが複数の情報オーナー／スチュワードからの情報を含んでいることもある。情報のオーナー／スチュワードは、自身の情報を処理、格納、または伝送する情報システムのセキュリティ要求事項およびセキュリティ管理策に関する入力情報を、情報システムのオーナーに提供する。

ることを要求している。

[52] 連邦政府情報は国の資産であり、特定の政府機関またはその下位組織に属するものではない。そうした考えから連邦政府機関の多くは、情報のオーナーシップの実践から情報のスチュワードシップの実践へと移行するためのポリシー、手順、プロセス、およびトレーニングを用意している。情報のスチュワードシップは、その情報がどのエンティティまたはソースによって発信、作成、または収集されたかにかかわらず、国家全体に属するすべての連邦政府情報を慎重に、かつ信頼できる形で管理することである。情報スチュワードは、連邦政府のエレメントおよび連邦政府の顧客が連邦政府の情報に最大限にアクセスできることを保証する。この際、FISMA の規定に従って情報を保護する義務と、セキュリティに関する政府機関のポリシー、指令、規定、基準、およびガイダンスのうち、関連するすべてのものとのバランスを考慮しなければならない。

D.5 上級情報セキュリティ責任者（SENIOR INFORMATION SECURITY OFFICER）

上級情報セキュリティ責任者は、次の項目に責任を負う組織の職員である。(i) FISMA が定める最高情報責任者としてのセキュリティ責任を負う。 (ii) 政府機関の運用認可責任者、情報システムのオーナー、共通管理策の提供者、および情報システムのセキュリティ担当者が最高情報責任者に報告する際、報告を取り次ぐ第一の窓口としての役割を果たす。上級情報セキュリティ責任者には、(i) 情報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（トレーニングおよび経験を含む）を有すること。 (ii) 情報セキュリティに関わる職務を主要な職務とし、その職務を維持すること (iii) ミッションおよびリソースを持つ一つの部門を率いて、組織が FISMA の要求事項に従って、より安全な情報および情報システムを構築できるように支援することが求められる。上級情報セキュリティ責任者（または、その支援スタッフ）は、運用認可責任者が指名する代理人として、またはセキュリティ管理策アセサーとして従事することもある。上級情報セキュリティ責任者は、米国政府から付与された権限を持ち、その役割は政府職員に対してのみ割り当てられるべきものである。

D.6 運用認可責任者（AUTHORIZING OFFICIAL）

運用認可責任者は、情報システムの運用により生じる組織の業務や資産、個人、他の組織、および国家へのリスクを受容可能なレベルに収めることに正式な責任を負う上級職員または管理職者である。[53] 通常、運用認可責任者は、情報システムの予算を監視する権限を持っているか、あるいは、システムが支援する任務／業務に責任を負う。運用認可責任者は、セキュリティの運用認可を行うことで、情報システムの運用により生じるセキュリティ上のリスクに対する説明責任を負う。したがって、運用認可責任者は、そのような情報システム関連のセキュリティリスクを把握・受容するのに見合ったレベルの権限を持つ管理職にある。また、運用認可責任者は、セキュリティ計画、協定書または覚書、および行動計画とマイルストーンの承認と、情報システムまたはその運用環境に対する重大な変更が発生した場合の再運用認可の必要性の判断が求められる。運用認可責任者は、受容できないリスクが存在する場合には、情報システムの運用を認可しない（システムが既に運用されている場合は、その運用を停止する）こともできる。運用認可責任者は、セキュリティ運用認可プロセスにおいて、リスクエグゼクティブ（機能）、最高情報責任者、上級情報セキュリティ責任者、共通管理策の提供者、情報システムのオーナー、情報システムセキュリティ責任者、セキュリティ管理策アセサー、およびこれ以外の利害関係者との連携を図る。任務／業務プロセスの複雑化や、パートナーシップに関する取り決めの複雑化、ならびに外部／共有サービスの利用により、一つの情報システムに複数の運用認可責任者が関与することも考えられるようになった。一つの情報システムに複数の運用認可責任者が関与する場合、それらの運用認可責任者同士で同意した内容が、システムセキュリティ計画において文書化される。運用認可責任者は、運用認可責任者が指名する代理人に委任されるセキュリティ運用認可に関連するすべての活動と機能が、確実に実施されることに責任を持つ。運用認可責任者は、米国政府から付与された権限を持ち、その役割は政府職員に対してのみ割り当てられるべきものである。

D.7 運用認可責任者が指名する代理人 （AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE）

運用認可責任者が指名する代理人は、セキュリティ運用認可プロセスに関連して必要となる日々の活動を運用認可責任者の代わりに調整し、実施する個人である。運用認可責任者に指名さ

[53] FIPS200 に記載されている運用認可責任者の責務を拡張したものが、NIST SP800-53 に記載されているが、これには、他の組織および国家に対するリスクが含まれている。

れた代理人には、セキュリティ運用認可プロセスの計画やリソースの調達、セキュリティ計画の承認、行動計画とマイルストーンの承認とその実施状況の監視、ならびに、リスクアセスメントおよび／またはリスク判断に関する特定の意思決定を行う権限が、運用認可責任者によって与えられている。指名代理人は、最終的な運用認可パッケージを作成し、セキュリティ運用認可判断文書に運用認可責任者の署名を得たのちにそのパッケージを組織内の適切な職員に送付するという一連の作業を要求されることもある。指名代理人が運用認可責任者から委譲されない唯一の権限が、セキュリティ運用認可の判断と関連する運用認可判断文書への署名（すなわち、組織の業務や資産、個人、他の組織、および国家に対するリスクの受容）である。

D.8 共通管理策の提供者（COMMON CONTROL PROVIDER）

共通管理策の提供者は、共通管理策（すなわち、情報システムによって継承されるセキュリティ管理策）の開発、実施、アセスメント、および監視に責任を持つ個人、グループ、または組織である。[54] 共通管理策の提供者は、以下の項目の実施に責任を負う。(i) 組織が明確化した共通管理策についてセキュリティ計画（あるいは、組織が提供する同等の文書）に記載する (ii) 必要な共通管理策アセスメントが、資格を持ち、組織が定めるレベルの独立性を有するアセサーによって確実に実施されるようにする (iii) 評価結果をセキュリティアセスメントレポートに記載する (iv) 弱点または欠陥を有するすべての管理策に対する行動計画とマイルストーンを策定する。共通管理策のセキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーン（あるいは、そうした情報の要約）は、それらの管理策の監視に責任を負う上級職員または管理職者によってレビュー・承認された後に、それらの管理策を継承する情報システムのオーナーが利用できるようになる。.

D.9 情報システムのオーナー（INFORMATION SYSTEM OWNER）

情報システムのオーナーは、情報システムの調達、開発、統合、修正、運用、メンテナンス、および廃棄に責任を負う組織の職員である。[55] 情報システムのオーナーは、ユーザコミュニティの運用に関する利害（すなわち、任務上、業務上、または運用上の要求事項を満たすために、情報システムにアクセスする必要があるユーザ）を代表し、情報セキュリティ要求事項への適合を確実にすることに責任を負う。情報システムのオーナーは、情報システムセキュリティ責任者の協力のもと、セキュリティ計画の作成とメンテナンスに責任を負い、合意されたセキュリティ管理策に従ったシステムの配備と運用が確実に行われるようにしなければならない。情報システムのオーナーは、情報のオーナー／スチュワードの協力のもと、誰が情報システムにアクセスできるのか（およびどのような特権種別またはアクセス権に基づいてアクセスできるのか）を決定する[56]とともに、システムユーザやサポート要員が所定のセキュリティトレーニング（行動規範など）を確実に受講できるようにする責任も負う。情報システムのオーナーは、運用認可責任者が提供するガイダンスをもとに、セキュリティ運用認可を行うことの必要性を組織内の適切な職員に通知し、その作業を行うために十分なリ

[54] 組織が共通管理策の提供者を複数抱える場合があるが、これは、情報セキュリティに関する責務を組織全体にわたってどのように割り当てるかによって変わってくる。共通管理策が情報システムに内在する場合は、そのシステムのオーナーが共通管理策の提供者になることもある。共通管理策については、セクション 2.4 に記載されている。

[55] 情報システムのオーナーは、情報システムの中心としての役割を果たす。そのような立場にある情報システムのオーナーは、オーナーとして、また、システムの各コンポーネントのオーナーと運用認可プロセス間の連絡窓口としての機能を果たす。システムコンポーネントには、たとえば、(i) アプリケーション、ネットワーク、サーバー、またはワークステーション (ii) そのシステムが処理、格納、または伝送する情報のオーナー／スチュワード、ならびに (iii) そのシステムが支援する任務／業務機能のオーナーが含まれる。情報システムのオーナーのことをプログラムマネージャ、または業務／資産のオーナーと呼ぶ組織もある。

[56] 情報システム内の特定の情報に誰がアクセスできるのか（およびどのような特権種別またはアクセス権に基づいてアクセスできるのか）を決定する責任、情報のオーナー／スチュワードに課せられる場合もある。

ソースが利用できるようにして、セキュリティ管理策アセサーに対して、必要な情報システムへのアクセス、情報、および関連文書を確実に提供する。情報システムのオーナーは、セキュリティ管理策アセサーからセキュリティアセスメントの結果を受け取る。脆弱性を排除または削減するために適切な対策を実施した後、情報システムのオーナーは運用認可パッケージをまとめ、運用認可責任者もしくは運用認可責任者が指名する代理人に提出し、裁定を仰ぐ。[57]

D.10 情報システムセキュリティ責任者（INFORMATION SYSTEM SECURITY OFFICER）

情報システムセキュリティ責任者[58]は、情報システムに関わる運用上の適切なセキュリティ状態が確実に維持されるようにすることに責任を負う個人である。したがって、情報システムのオーナーと緊密に連携する。情報システムセキュリティ責任者は、情報システムのセキュリティに関するすべての事柄（技術面およびその他）について、筆頭アドバイザーとしての役割も果たす。情報システムセキュリティ責任者は、情報システムのセキュリティ面を管理するために必要な詳細な知識や専門技術を持っており、多くの組織では、システムの日常のセキュリティに関する業務上の責務が割り当てられている。この職責には、物理的および環境的保護、人的セキュリティ、事故対応、セキュリティトレーニングとセキュリティ意識向上も含まれる場合があるが、これらに限られるわけではない。情報システムセキュリティ責任者は、システムのセキュリティポリシーと手順の作成を支援したり、それらのポリシーと手順への遵守を確実にするための作業を要求されることがある。情報システムセキュリティ責任者は、情報システムのオーナーと緊密な連携を取りながら、セキュリティ計画の作成や更新だけでなく、システムに対する変更の管理やコントロールおよび、これらの変更によるセキュリティの影響の評価を含む、システムおよ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。

D.11 情報セキュリティアーキテクト（INFORMATION SECURITY ARCHITECT）

情報セキュリティアーキテクトは、リファレンスモデル、セグメントおよびソリューションアーキテクチャ、ならびに組織の主要な任務および業務プロセスを支援する最終的な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すべての側面において、組織の主要な任務および業務プロセスを保護するのに必要な情報セキュリティ要求事項が十分に考慮されることに責任を持つ、個人、グループ、または組織である。情報セキュリティアーキテクトは、エンタープライズアーキテクトと、情報システムセキュリティエンジニアとの間の連絡窓口としての役割を果たす。また、情報システムのオーナー、共通管理策の提供者、および情報システムセキュリティ責任者と連携して、各セキュリティ管理策をシステム固有の管理策、ハイブリッド管理策、または共通管理策に分類して、システムに割り当てる。さらに、情報システムセキュリティ責任者と緊密な連携を取りながら、運用認可責任者、最高情報責任者、上級情報セキュリティ責任者、およびリスクエグゼクティブ（機能）に対して、広範囲にわたるセキュリティ関連事項（たとえば、情報システムの境界の設定、情報システムの弱点と欠陥の重大性の評価、行動計画とマイルストーン、リスク軽減アプローチ、セキュリティアラート、特定された脆弱性によってもたらされる可能性のあるマイナスの影響が含まれる）について助言する。

[57] 組織が自らのセキュリティ運用認可活動をどのように組織化しているかによって、運用認可責任者はセキュリティ運用認可パッケージに必要な情報の編集・統合を行うために、情報システムのオーナー以外の個人を指名する場合がある。この場合、指名された個人は、情報システムのオーナーとともに、運用認可に必要な情報の編集・統合作業の調整を行わなければならない

[58] 組織は、情報システムセキュリティ責任者と類似の責務を担う（または、情報セキュリティプログラムの監視に責任を持つ）情報システムセキュリティマネージャまたは情報セキュリティマネージャを、複数の情報システムセキュリティ責任者のうちの一人として定義することもできる。この場合、組織の自由裁量で、各情報システムセキュリティ責任者が情報システムセキュリティマネージャまたは情報セキュリティマネージャに直接報告を行うことが考えられる。

D.12 情報システムセキュリティエンジニア（INFORMATION SYSTEM SECURITY ENGINEER）

情報システムセキュリティエンジニアは、情報システムセキュリティエンジニアリング活動の実施に責任を持つ個人、グループ、または組織である。情報システムセキュリティエンジニアリングは、情報セキュリティ要求事項を把握・改良し、洗練された要求事項を、セキュリティの意図的な体系化／設計／開発／構成を通じて各ITコンポーネント製品および情報システムに効率的に組み入れることを可能にするプロセス。情報システムセキュリティエンジニアは、組織の情報システムを設計・開発している、あるいは、レガシーシステムをアップグレードしている開発チーム（たとえば、統合されたプロジェクトチーム）にとって、不可欠な存在である。情報システムセキュリティエンジニアは、情報システムにおいてセキュリティ管理策を実施する際には、ソフトウェアエンジニアリングに関する方法論、システム／セキュリティエンジニアリングの原理、セキュアな設計、セキュアなアーキテクチャ、およびセキュアなコーディング技法を含む、ベストプラクティスを用いる。システムセキュリティエンジニアは、情報セキュリティアーキテクト、上級情報セキュリティ責任者、情報システムのオーナー、共通管理策の提供者、および情報システムセキュリティ責任者との間で、自身のセキュリティ関連活動を調整する。

D.13 セキュリティ管理策アセサー（SECURITY CONTROL ASSESSOR）

セキュリティ管理策アセサー[59]は、情報システムに導入される、または情報システムによって継承される管理面、運用面、および技術面でのセキュリティ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、または組織である。このような包括的なアセスメントでは、管理策の全体的な有効性（すなわち、セキュリティ管理策がどの程度正しく導入されているか、どの程度意図した通りに運用されているか、システムのセキュリティ要求事項に対する適合性の観点から所望の結果をどの程度産出しているか）を判断する。また、セキュリティ管理策アセサーは、情報システムおよびその運用環境において発見された弱点または欠陥の重大性を評価すると同時に、特定された脆弱性を克服するための是正活動を推奨する。以上のような責務に加え、セキュリティ管理策アセサーは、アセサーによる評価結果と結論を含む、最終的なセキュリティアセスメントレポートを用意する。セキュリティ管理策アセスメントを開始する前に、アセサーはセキュリティ計画のアセスメントを実施する。これにより、定められたセキュリティ要求事項を満たすために情報システムに導入すべき一連のセキュリティ管理策が、セキュリティ計画を通じて確実に提供される。

アセサーに求められる独立性のレベルは、セキュリティ管理策アセスメントの具体的な条件によって定まる。たとえば、セキュリティ管理策のアセスメントが、運用認可判断または継続的な運用認可を支援する目的で実施される場合、運用認可責任者は、連邦政府のポリシー、指令、基準、およびガイドラインに従って要求される独立性のレベルについて、明示的な判断を下す。アセサーの独立性は、以下の項目を確実に実施するうえで、重要な要素となる (i) アセスメントプロセスの公正さや公平さを維持する (ii) セキュリティアセスメント結果の信頼性について判断する (iii) 運用認可責任者が十分な情報に基づいたリスクベースの運用認可判断を行うのに必要な、最も客観的な情報を確実に受け取れるようにする。情報システムのオーナーおよび共通管理策の提供者は、(i) 情報システムに導入されている、または、情報システムによって継承されるセキュリティ管理策を、セキュリティアセスメント計画に記載されているアセスメント手順を用いて評価する、および (ii) 管理策の弱点または欠陥をどのように訂正するか、また、特定された脆弱性にどのように対処するか、につ

[59] セキュリティ管理策アセサーは、組織によっては承認エージェントと呼ばれることがある。組織の自由裁量により、セキュリティ管理策アセスメントの結果と結論に対する事後処理および分析についての追加の任務／責務が、セキュリティ管理策アセサーに与えられることもある。

いての具体的な推奨事項を示すことについては、アセサーのセキュリティに関する専門的な知識や技術的な判断に委ねている。

付録 E

RMF の各タスクの要約

主な責任と補助的な役割の一覧

RMF タスク	主な責任を持つ者	補助的な役割
RMF ステップ 1: 情報システムの分類		
タスク 1-1 **セキュリティ分類** 情報システムを分類し、セキュリティ分類の結果をセキュリティ計画に記載する。	情報システムのオーナー 情報のオーナー／スチュワード	リスクエグゼクティブ（機能） 運用認可責任者または指名された代理人 最高情報責任者 上級情報セキュリティ責任者 情報システムセキュリティ責任者
タスク 1-2 **情報システムに関する記述** 情報システム（システム境界を含む）について説明し、その内容をセキュリティ計画に記載する。	情報システムのオーナー	運用認可責任者または指名された代理人 上級情報セキュリティ責任者 情報のオーナー／スチュワード 情報システムセキュリティ責任者
タスク 1-3 **情報システムの登録** 組織内の適切な計画局／管理局に情報システムを登録する。	情報システムのオーナー	情報システムセキュリティ責任者
RMF ステップ 2:セキュリティ管理策の選択		
タスク 2-1 **共通管理策の明確化** 組織の情報システムに対する共通管理策として組織が提供しているセキュリティ管理策を明確にし、セキュリティ計画（またはそれと同等の文書）に記載する。	最高情報責任者 または 上級情報セキュリティ責任者 情報セキュリティアーキテクト 共通管理策の提供者	リスクエグゼクティブ（機能） 運用認可責任者または指名された代理人 情報システムのオーナー 情報システムセキュリティエンジニア
タスク 2-2 **セキュリティ管理策の選択** 情報システムに導入するセキュリティ管理策を選択し、それらの管理策について、セキュリティ計画に記載する。	情報セキュリティアーキテクト 情報システムのオーナー	運用認可責任者または指名された代理人 情報のオーナー／スチュワード 情報システムセキュリティ責任者 情報システムセキュリティエンジニア

RMF タスク	主な責任を持つ者	補助的な役割
タスク 2-3 **監視戦略** セキュリティ管理策の有効性、ならびに、情報システムおよびシステムの運用環境に対して提案されている、あるいは、実際に実施された変更を、継続的に監視するための、戦略を策定する。	情報システムのオーナー または 共通管理策の提供者	リスクエグゼクティブ（機能） 運用認可責任者または指名された代理人 最高情報責任者 上級情報セキュリティ責任者 情報のオーナー／スチュワード 情報システムセキュリティ責任者
タスク 2-4 **セキュリティ計画の承認** セキュリティ計画をレビューし、承認する。	運用認可責任者 または 指名された代理人	リスクエグゼクティブ（機能） 最高情報責任者 上級情報セキュリティ責任者
RMF ステップ 3：セキュリティ管理策の実施		
タスク 3-1 **セキュリティ管理策の実施** セキュリティ計画に記載されているセキュリティ管理策を実施する。	情報システムのオーナー または 共通管理策の提供者	情報のオーナー／スチュワード 情報システムセキュリティ責任者 情報システムセキュリティエンジニア
タスク 3-2 **セキュリティ管理策の文書化** 必要に応じて、セキュリティ管理策の実施について、機能面での記述（予定しているインプット、予想される挙動、および予想されるアウトプットを含む）と併せて、セキュリティ計画に記載する。	情報システムのオーナー または 共通管理策の提供者	情報のオーナー／スチュワード 情報システムセキュリティ責任者 情報システムセキュリティエンジニア
RMF ステップ 4：セキュリティ管理策のアセスメント		
タスク 4-1 **アセスメントの準備** セキュリティ管理策のアセスメント計画を策定、レビューし、承認する。	セキュリティ管理策アセサー	運用認可責任者または指名された代理人 最高情報責任者 上級情報セキュリティ責任者 情報システムのオーナーまたは共通管理策の提供者 情報のオーナー／スチュワード 情報システムセキュリティ責任者
タスク 4-2 **セキュリティ管理策のアセスメント** セキュリティアセスメント計画に記載されているアセスメント手順に従ってセキュリティ管理策をアセスメントする。	セキュリティ管理策アセサー	情報システムのオーナーまたは共通管理策の提供者 情報のオーナー／スチュワード 情報システムセキュリティ責任者

RMF タスク	主な責任を持つ者	補助的な役割
タスク 4-3 **セキュリティアセスメントレポート** セキュリティ管理策のアセスメントを通じて発見された問題、導かれた結論および推奨事項を文書化した、セキュリティアセスメントレポートを用意する。	セキュリティ管理策アセサー	情報システムのオーナーまたは共通管理策の提供者 情報システムセキュリティ責任者
タスク 4-4 **是正活動** セキュリティアセスメントレポートに記載されている結論と推奨事項に基づいて、セキュリティ管理策に対する初期の是正活動を実施し、是正された管理策（複数）を適宜、再アセスメントする。	情報システムのオーナー または 共通管理策の提供者 セキュリティ管理策アセサー	運用認可責任者または指名された代理人 最高情報責任者 上級情報セキュリティ責任者 情報のオーナー／スチュワード 情報システムセキュリティ責任者 情報システムセキュリティエンジニア
RMF ステップ 5: 情報システムの運用認可		
タスク 5-1 **行動計画とマイルストーン** セキュリティアセスメントレポートに記載されている結論と推奨事項に基づいて、行動計画とマイルストーンを作成する（ただし、既に実施されたすべての是正活動を除く）。	情報システムのオーナー または 共通管理策の提供者	情報のオーナー／スチュワード 情報システムセキュリティ責任者
タスク 5-2 **セキュリティ運用認可パッケージ** セキュリティ運用認可パッケージをまとめて、運用認可責任者に提出し、裁定を仰ぐ。	情報システムのオーナー または 共通管理策の提供者	情報システムセキュリティ責任者 セキュリティ管理策アセサー
タスク 5-3 **リスクの判断** 組織の業務（任務、機能、イメージ、または評判を含む）、組織の資産、個人、他の組織、または国家に対するリスクを判断する。	運用認可責任者 または 指名された代理人	リスクエグゼクティブ（機能） 上級情報セキュリティ責任者
タスク 5-4 **リスクの受容** 組織の業務、組織の資産、個人、他の組織、または国家に対するリスクが受容できるかどうかを判断する。	運用認可責任者	リスクエグゼクティブ（機能） 運用認可責任者が指名する代理人 上級情報セキュリティ責任者

RMF タスク	主な責任を持つ者	補助的な役割
RMF ステップ 6: セキュリティ管理策の監視		
タスク 6-1 **情報システムやその運用環境に対する変更** 情報システムおよびシステムの運用環境に対して提案されている、あるいは、実際に実施された変更がもたらすセキュリティへの影響を判断する。	情報システムのオーナー または 共通管理策の提供者	リスクエグゼクティブ（機能） 運用認可責任者または指名された代理人 上級情報セキュリティ責任者 情報のオーナー／スチュワード 情報システムセキュリティ責任者
タスク 6-2 **継続的なセキュリティ管理策アセスメント** 組織が定めた監視戦略に従って、情報システムに導入される、または情報システムによって継承される技術面、管理面、および運用面でのセキュリティ管理策の中から選択された管理策のサブセットをアセスメントする。	セキュリティ管理策アセサー	運用認可責任者または指名された代理人 情報システムのオーナーまたは共通管理策の提供者 情報のオーナー／スチュワード 情報システムセキュリティ責任者
タスク 6-3 **継続的な是正活動** 継続的監視活動の結果、リスクアセスメント結果、および行動計画とマイルストーンにリストアップされている重要な項目に基づいて是正活動を実施する。	情報システムのオーナー または 共通管理策の提供者	運用認可責任者または指名された代理人 情報のオーナー／スチュワード 情報システムセキュリティ責任者 情報システムセキュリティエンジニア セキュリティ管理策アセサー
タスク 6-4 **重要な更新** 継続的監視プロセスの結果に基づいて、セキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーンを更新する。	情報システムのオーナー または 共通管理策の提供者	情報のオーナー／スチュワード 情報システムセキュリティ責任者
タスク 6-5 **セキュリティ状況の報告** 監視戦略に従って、継続的に、情報システムのセキュリティ状況（情報システムに導入されるセキュリティ管理策、および情報システムによって継承されるセキュリティ管理策の有効性を含む）を運用認可責任者および組織内の他の適切な職員に報告する。	情報システムのオーナー または 共通管理策の提供者	情報システムセキュリティ責任者

RMF タスク	主な責任を持つ者	補助的な役割
タスク 6-6 **継続的なリスク判断および受容** 監視戦略に従って、情報システムのセキュリティ状況に関する報告内容（情報システムに導入される、または情報システムによって継承されるセキュリティ管理策の有効性を含む）を継続的に見直すことによって、組織の業務、組織の資産、個人、他の組織、または国家に対するリスクが、ひきつづき受容可能か否かを判断する	運用認可責任者	リスクエグゼクティブ（機能） 運用認可責任者が指名する代理人 上級情報セキュリティ責任者
タスク 6-7 **情報システムの切り離しおよび廃止** 必要に応じて、情報システムの廃止戦略を実施する。この戦略は、システムがサービスから切り離された時に必要となる活動を実施するためのものである。	情報システムのオーナー	リスクエグゼクティブ（機能） 運用認可責任者が指名する代理人 上級情報セキュリティ責任者 情報のオーナー／スチュワード 情報システムセキュリティ責任者

付録 F

セキュリティ運用認可

運用認可判断および裏付けとなる証拠

本付録には、セキュリティ運用認可プロセスに関する情報を記載している。これには、(i) 運用認可パッケージの内容 (ii) 運用認可判断の種類 (iii) 運用認可判断文書の内容 (iv) 継続的な監視プロセスを通じた運用認可の維持および再運用認可のための諸条件。

F.1 運用認可パッケージ（AUTHORIZATION PACKAGE）

セキュリティ運用認可パッケージは、セキュリティ管理策アセスメントの結果を文書にしたものであり、情報システムの運用、または指定された共通管理策一式を認可するか否かについて、運用認可責任者がリスクベースの判断を行うために必要不可欠な情報を提供するものである。最高情報責任者または運用認可責任者が具体的に指定しない限り、情報システムのオーナーまたは共通管理策の提供者が、運用認可パッケージのまとめと編集およびその提出に責任を負う。情報システムのオーナーまたは共通管理策の提供者は、セキュリティ運用認可のパッケージを作成している間に、情報システムセキュリティ責任者、セキュリティ管理策アセサー、上級情報セキュリティ責任者、およびリスクエグゼクティブ（機能）から必要な情報を受け取る。セキュリティ運用認可パッケージ [60]には、次の文書が含まれる。

- セキュリティ計画
- セキュリティアセスメントレポート
- 行動計画とマイルストーン

情報システムのオーナーまたは共通管理策の提供者によって作成されるセキュリティ計画とは、情報システムのセキュリティ要求事項を要約したものであり、それらの要求事項に適合し、既に組み入れられた、または組み入れが計画されているセキュリティ管理策を記載したものである。セキュリティ計画は、情報システムに導入される、または情報システムによって継承される各セキュリティ管理策がどのように実施されているか、あるいは、どのように実施する予定であるかについて理解するのに十分な情報を提供する。[61] セキュリティ計画には、リスクアセスメント、プライバシー影響評価、システムの相互接続に関する同意書、緊急時対応計画、セキュリティ設定、設定の管理計画、事故対応計画、および継続的な監視戦略などの、リスクおよびセキュリティに関するその他のドキュメントが、付録、または、適切な情報源への参照として含まれる場合がある。組織は、セキュリティ運用認可プロセスにおけるリアルタイムに近いリスクマネジメントを実現するために、情報システムに導入される、または情報システムによって継承されるセキュリティ管理策への変更が必要となる

[60] 運用認可責任者は、セキュリティ運用認可パッケージに含まれるべき裏付けとなる追加のドキュメント、または参考文献を決定する。セキュリティ運用認可パッケージに含まれる情報は、政府機関のポリシーおよび組織のポリシーに従って適切な対策によって保護される。

[61] セキュリティ計画は、単独の、または複数のレポジトリに含まれる概念的な情報の集まりである。これには、システム開発ライフサイクル全体を通して生成される、種々の情報源から得られるドキュメント（電子的、または、ハードコピー）が含まれる。たとえば、共通管理策を継承する情報システムのオーナーは、セキュリティ管理策の実施について個別のセキュリティ計画に記載することもできれば、共通管理策の提供者が作成したセキュリティ計画に含まれるセキュリティ管理策への参照を用意することもできる。

イベントが発生した場合には、セキュリティ計画を更新する。セキュリティ計画の更新をひき起こすイベントには、たとえば、(i) 情報システムに内在する脆弱性のスキャン、または、運用環境の脆弱性のアセスメント (ii) 新しい脅威に関する情報 (iii) 情報システムに対する侵害が発生した後に、現在導入されているセキュリティ管理策について発見された弱点または欠陥 (iv) 以前に実施されたセキュリティ分類プロセスの結果を無効にする、任務の優先順位の再定義、または業務上の目的の再定義、ならびに、(v) 情報システムに対する変更（たとえば、新しいハードウェア、ソフトウェア、またはファームウェアの追加、さらなる接続の確立など）および、システムの運用環境に対する変更（たとえば、新たな施設への移動など）。

セキュリティ管理策アセサーによって作成されるセキュリティアセスメントレポートは、セキュリティ計画に記載されているセキュリティ管理策の実施に関する評価結果を示すものであり、これにより、どの程度正しく導入されているか、どの程度意図した通りに運用されているか、システムのセキュリティ要求事項に対する適合性の観点から所望の結果をどの程度産出しているかを判断することができる。セキュリティアセスメントレポートには、セキュリティ管理策において特定されたあらゆる弱点または欠陥に対して、推奨される是正活動の一覧を収容することもできる。[62] セキュリティ運用認可プロセスにおけるリアルタイムに近いリスクマネジメントの実現を支援するセキュリティアセスメントレポートは、情報システムに導入される、または情報システムによって継承されるセキュリティ管理策に変更が生じた場合には常に、更新される。[63] セキュリティアセスメントレポートを更新することによって、セキュリティ管理策の有効性に関する情報システムのオーナー、共通管理策の提供者、および運用認可責任者の適切な意識が保たれる。セキュリティ管理策の全体的な有効性は、情報システムの最終的なセキュリティ状態、およびリスクの明示的な受容に関する意思決定に影響を与える。

情報システムのオーナーまたは共通管理策の提供者によって作成される行動計画とマイルストーンには、次のことを目的として、導入を計画中の対策が記載されている。 (i) セキュリティ管理策のアセスメント時に確認された弱点または欠陥の是正 (ii) 情報システムの既知の脆弱性への対処。[64] 行動計画とマイルストーンの内容および構造は、リスクエグゼクティブ（機能）の一部として策定されるリスクマネジメント戦略に基づいて決定され、組織が定める行動計画とマイルストーンプロセス、および連邦政府のポリシー、指令、覚書、または規定が定めるあらゆる要求事項に適合する。最も効果的な行動計画とマイルストーンには、情報システムに導入されている、または情報システムによって継承されたセキュリティ管理策において特定された、実際の弱点または欠陥一式が含まれる。情報システム、およびそれらのシステムが導入されている環境のほとんどにおいて、利用可能なリソースが現実的に対処できる脆弱性を上回る脆弱性が存在することが想定されるため、組織は、組織全体にわたって一貫性のある、優先順位付けがなされたリスク軽減アプローチを容易にするための、行動計画とマイルストーンの策定と実施に関する戦略を立てるべきである。この戦略によって、行動計画とマイルストーンが以下の項目に基づいたものになる。

- 情報システムのセキュリティ分類
- セキュリティ管理策の具体的な弱点または欠陥

[62] 組織は、セキュリティ管理策アセスメントにおいて生成された詳細な結果から要旨を作成してもよい。この要旨は、運用認可権限者に対して、アセスメントの主要部分、重要な結果の概要、および／またはセキュリティ管理策の弱点と欠陥を克服するための推奨事項にフォーカスをあてた、セキュリティアセスメントレポートの簡略版となる。

[63] 組織は、運用認可パッケージ内の重要なドキュメントが更新される際には、厳密なバージョン管理を行う。

[64] 組織は、セキュリティ管理策に弱点または欠陥を是正するために導入される対策を行動計画とマイルストーンに記載してもよい。そうすることで、完了済みのアクションについての履歴が提供される。

- セキュリティ管理策において特定された弱点または欠陥の重大性（すなわち、それらの弱点または欠陥が、情報システムの全体的なセキュリティ状態、ならびに、組織のリスクへの暴露[65]に及ぼす直接的／間接的な影響）
- 提案されている、セキュリティ管理策に関して特定された弱点または欠陥に対処するためのリスク軽減アプローチ（たとえば、リスク軽減活動の優先順位付け、リスク軽減に必要なリソースの割り当て）、および
- セキュリティ管理策の弱点または欠陥の一部の受容に関する組織の根拠。[66]

行動計画と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各情報システムのセキュリティ分類によって導かれる。たとえば組織が、初期の段階で、リスク軽減用リソースの大半を影響度が高位の情報システムに割り当てることを決定する場合がある。理由としては、影響度が高位の情報システムにおける弱点または欠陥の是正を怠ると、組織の任務または業務に最も重大なマイナスの影響が及ぶ可能性があるからである。組織は、組織によるリスクアセスメント、およびリスクエグゼクティブ（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、弱点または欠陥の優先順位付けを行う。したがって影響度が高位のシステムにおいても、影響度が中位または低位のシステムと同様に、そのシステムの弱点または欠陥の優先順位を反映したリストが用意されることになる。一般的に行動計画とマイルストーンでは、常に、優先順位付けがなされた各システム内の弱点または欠陥のうち、優先度が最も高いものを取り扱うことになる。

セキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーンが完成したら、情報システムのオーナーまたは共通管理策の提供者は、最終的なセキュリティ運用認可パッケージを運用認可責任者またはその運用認可責任者に指名された代理人に提出する。図 F-1 は、セキュリティ運用認可パッケージの主な構成要素を図示したものである。

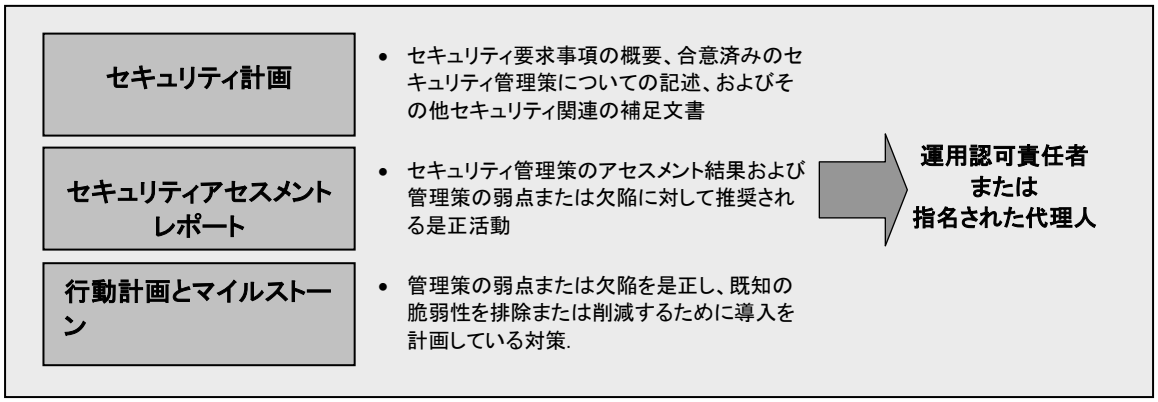

FIGURE F-1:　SECURITY AUTHORIZATION PACKAGE

F.2 運用認可判断（AUTHORIZATION DECISIONS）

運用認可判断は、運用認可パッケージの内容（組織のリスクエグゼクティブ（機能）からの情報、および運用認可責任者が必要とする追加の補足文書を含む）に基づいて行われる。セキュリティ運用認可パッケージは、情報システムのセキュリティ状態に関する包括的な情報を提供する。リスク

[65] 一般的に、リスクへの暴露は、組織の業務や資産、個人、他の組織、または国家に対する潜在的なマイナスの影響によって組織が脅かされる度合いを示す。

[66] 組織は、セキュリティ管理策の弱点または欠陥の受容に関する根拠を文書化する。

エグゼクティブ（機能）からのインプット（リスクマネジメント戦略から抽出した、以前に確立された包括的なリスクガイダンスを含む）は、運用認可責任者に対して、最終的な運用認可判断（たとえば、組織のリスク許容度、組織の全体的なリスク軽減戦略、主要な任務および業務上の要求事項、情報システム間の依存関係、継続的なリスクの監視に関する要求事項、情報システムまたはシステムの運用環境に直接関わらない他の種類のリスク）に関連し、かつ、影響を与える可能性のある追加情報を提供する。リスクエグゼクティブ（機能）からのインプットは文書化され、運用認可判断の一部となる。組織は、リスクマネジメント戦略、およびリスクエグゼクティブ（機能）から得られるリスク関連のガイダンスが、運用認可責任者の運用認可判断にどのような影響を与えるかについて、判断する。セキュリティ運用認可の判断は、情報システムのオーナーおよび共通管理策の提供者に伝えられ、組織内の選択された職員（たとえば、共通管理策を継承する情報システムのオーナー、相互接続されたシステムの運用認可に責任を持つ運用認可責任者、最高情報責任者、上級情報セキュリティ責任者、情報のオーナー／スチュワード）が利用できるようになる。運用認可責任者によって行われる運用認可判断には、次の 2 つのタイプがある。

- 運用の認可 [67]
- 運用の不許可

運用の認可

運用認可パッケージ、およびリスクエグゼクティブ（機能）が提供するあらゆる追加情報を精査した後に、運用認可責任者が組織の業務や資産、個人、他の組織、および国家に対するリスクが受容できると判断した場合には、情報システムまたは組織の各情報システムが継承する共通管理策に対して運用認可が発行される。その情報システムの運用が認可される期限は、運用認可責任者が定める諸条件に従って決定される。[68] 組織の特定の情報システムにとって共通管理策の提供者が外部の者である場合、この運用認可判断結果は、彼らの管理下にある共通管理策がその情報システムによって継承されることについて認可が与えられたことを意味する。運用認可の満了日も、運用認可の条件のうちの1つとして運用認可責任者によって設定される。運用認可の満了日は、情報システムに導入される、または情報システムによって継承されるセキュリティ管理策を含む、情報システムのセキュリティ状態に関する懸念の度合いが向上した場合に、それを反映するために、運用認可責任者によって調整される。運用認可の満了日が、連邦政府のポリシーまたは組織のポリシーが規定する運用認可期間を超えることはない。

運用認可責任者は、リスクマネジメントフレームワークの実施中に確認された脆弱性を排除または削減するための、具体的な活動を行う（ただし、それらの脆弱性が運用認可判断の一部として明示的に受容されている場合を除く。） また、情報システムのオーナーまたは共通管理策の提供者は、導入されているセキュリティ管理策の現時点の有効性と、弱点または欠陥を是正／排除するためのすべての活動の進捗を監視するために、繰り返しが可能で統制のとれた、構造化されたプロセスを構築する。情報システムのオーナーによって提出された行動計画とマイルストーンは、セキュリティ管理策のアセスメント時に確認された欠陥および弱点の是正の進捗を監視する運用認可責任者によって使用される。

[67] テストのための暫定的な運用認可とは、特別な種類の運用認可判断であり、情報システムを特定の期間にわたって実際の運用データ（すなわち、ライブデータ）を使用してテストするといった明白な目的のもとで、当該システムの特定の環境における運用を許可するものである。テストのための暫定的な運用認可は、特定のテスト目的を達成するために、そのような運用環境またはライブデータが必要とされる場合に限り、運用認可責任者によって与えられる。

[68] 組織によっては、「暫定的な運用認可」という用語を使用することがある。暫定的な運用認可は、情報システムに重大な弱点または欠陥が存在するものの、任務上の必要性から当該システムの運用を開始する必要がある、あるいは、当該システムの運用を継続する必要がある場合に、運用認可責任者がリスクの増加を受容することを意味する。

運用の不許可

運用認可パッケージ、およびリスクエグゼクティブ（機能）が提供するあらゆる追加情報を精査した後に、運用認可責任者が組織の業務や資産、個人、他の組織、および国家に対するリスクが受容できないと判断した場合で、かつ、リスクを受容できるレベルまで軽減するための措置を直ちに講じることができない場合には、情報システムまたは組織の各情報システムが継承する共通管理策に対して、運用の不認可が発行される。その情報システムの運用は認可されず、運用は開始されない。その情報システムが、現在稼働中である場合には、すべての活動を停止することになる。組織の特定の情報システムにとって共通管理策の提供者が外部の者である場合、この運用認可判断結果は、彼らの管理下にある共通管理策がその情報システムによって継承されることについて認可が与えられなかったことを意味する。運用の認可を受けることができないということは、情報システムに導入される、または情報システムによって継承されるセキュリティ管理策に重大な弱点または欠陥があることを示している。運用認可責任者または運用認可責任者に指名された代理人は、情報システムのオーナーまたは共通管理策の提供者と共同で、行動計画とマイルストーンを見直して、確認された弱点または欠陥を是正するための対策が確実に実施されるようにしなければならない。

運用の不許可の特別なケースとして、運用認可の撤回がある。運用認可責任者は、次の項目に対する違反行為が発生した場合に、いつでも、以前に下した運用認可判断を撤回することができる。(i) 連邦政府／組織のセキュリティポリシー、指令、規定、基準、ガイダンス、または慣行、 あるいは (ii) 組織が定める運用認可のための諸条件。たとえば、効果的な継続的監視プログラムが維持されていないことが、運用認可判断を撤回する根拠となる可能性がある。運用認可責任者は、セキュリティ運用認可を撤回する前に、リスクエグゼクティブ（機能）と上級情報セキュリティ責任者の助言を求めるべきである。

F.3 運用認可の判断文書（AUTHORIZATION DECISION DOCUMENT）

運用認可の判断文書は、最終的なセキュリティ運用認可判断を運用認可責任者から情報システムのオーナーまたは共通管理策の提供者に、また、必要な場合には、組織内のその他の主要な職位に伝える役割を果たす。運用認可の判断文書には、以下の情報が含まれる。

- 運用認可の判断
- 運用認可のための諸条件
- 運用認可の満了日
- リスクエグゼクティブ（機能）から得られる情報（提供される場合）

セキュリティ運用認可判断は、その情報システムの運用が (i) 認可されたこと、(ii) 認可されなかったこと、のいずれかを示すものである。共通管理策に関しては、「運用の認可」という判断は、それらの管理策が組織の情報システムによって継承されることについての認可が与えられたことを意味する。運用認可のための諸条件は、情報システムの運用に関して、あるいは、共通管理策の導入に関して情報システムのオーナーまたは共通管理策の提供者に課せられる、あらゆる制限／制約を記述したものである。運用認可責任者が定める運用認可の満了日は、いつセキュリティ運用認可の期限が切れて、再運用認可が必要となるかを示す。運用認可責任者が指名した代理人は、必要に応じて、運用認可の判断文書に運用認可に関する推奨事項を添えて、運用認可責任者に提出する。運用認可の判断文書は、オリジナルの認可パッケージに添付されて情報システムのオー

ナーまたは共通管理策の提供者に戻される。[69] 運用認可の判断文書と運用認可パッケージを受領した時点で、情報システムのオーナーまたは共通管理策の提供者が運用認可のための諸条件を受け入れたことになり、彼らはそれらの条件を満たした後に、その旨を運用認可責任者に通知する。情報システムのオーナーまたは共通管理策の提供者が、運用認可の判断文書と認可パッケージの原本を保管する。[70] 組織は、組織内の適切な職員（たとえば、共通管理策を継承する情報システムのオーナー、リスクエグゼクティブ（機能）、最高情報責任者、上級情報セキュリティ責任者、情報システムセキュリティ責任者）が、情報システムの運用認可文書および共通管理策の運用認可文書を確実に利用できるようにする。セキュリティ運用認可文書の内容（特に、情報システムの脆弱性に関する情報）は、(i) 政府機関／組織のポリシーに従い、マーク付けと適切な保護がなされて、かつ、(ii) 組織の記録保管ポリシーに従って保管される。運用認可責任者は、運用認可の一部として設定された諸条件が、情報システムのオーナーまた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確認する。

F.4 継続的な運用認可（ONGOING AUTHORIZATION）

組織のシステム開発ライフサイクルプロセスに統合された堅牢で、かつ包括的な継続監視[71]戦略によって、組織は、継続的なリスクマネジメントを促進させると同時に、再運用認可が必要になった場合に、必要なリソースも大幅に減らすことができる。オートメーションや最先端のツール、技法、手順の使用により、セキュリティ管理策および情報システムやその運用環境に対する変更の継続的な監視を、ほぼリアルタイムに実施することができる。運用認可責任者のニーズに従って監視が実施された場合、結果として、次の項目についての判断に必要な重要な情報が生成される。(i) 情報システムの最新のセキュリティ状態（当該システムに導入されている、または当該システムによって継承されたセキュリティ管理策の有効性を含む） (ii) 組織の業務、組織の資産、個人、他の組織、および国家にもたらされるリスク (iii) システムの継続的な運用、または組織の情報システムによって継承された共通管理策の継続的な使用を認可するか否か。

継続的な監視により、再運用認可活動に必要なリソース関連の支出を、認可期間にわたって分散させることが可能になる。その最終目的は、「継続的な運用認可」の実現 － すなわち、運用認可責任者が、情報システムの最新のセキュリティ状態（当該システムに導入されている、または当該システムによって継承されたセキュリティ管理策の有効性を含む）についての十分な知識を持ち続けることで、システムの継続運用の受容の可否を継続的なリスク判断の結果に基づいて判断できること、また、受容できない場合には、追加のリスクを十分に軽減するために再度実施する必要がある、リスクマネジメントフレームワークのステップ（単独または複数）を特定できることにある。情報システムやその運用環境に対する変更がもたらす潜在的なリスクを管理するのに必要な情報が、継続的監視プロセスによって運用認可責任者に提供される状況下では、正式な再運用認可活動の実施は避けられる。組織は、状況報告書、および継続的監視プロセスにおいて生成されたセキュリティ状況に関する情報を最大限に利用して、実施が求められている正式な再運用認可活動に必要な作業レベルを最小限に抑える。正式な再運用認可活動は、連邦政府のポリシーまたは組織のポリシーに従って、運用認可責任者の自由裁量によって実施される。正式な再運用認可活動が必要な場合、組織は、継続的な監視において、ならびに、現時点で有効な運用認可プロセスにおいて生成されたセキュリティ関連およびリスク関連の情報を最大限に利用する。

---

[69] 運用認可の判断文書は、真正性を保証するためにも、電子的に署名される可能性がある。

[70] 組織は、リスクマネジメントに関するドキュメント（セキュリティ運用認可プロセスに関連するアーチファクトを含む）の作成、配布、およびアーカイブを支援する自動化ツールを採用してもよい。

[71] 継続的な監視については、付録 G に記載されている。

いったん開始された再運用認可活動は、「時間駆動型」あるいは「イベント駆動型」のいずれかに分類される。時間駆動型の再運用認可は、運用認可の満了日を迎えた時点で実施される。運用認可の満了日は、運用認可の最大期間を規定することもある連邦政府／組織のポリシー、および運用認可責任者が定める要求事項によって左右される。たとえば、情報システムの運用認可の最大期間が 3 年だとする。この場合、組織は、その期間内に、情報システムに導入される、または情報システムによって継承されるセキュリティ管理策のサブセットをアセスメントするための、継続的監視戦略を策定する。この戦略によって、個々のセキュリティ計画に記載されているすべてのセキュリティ管理策が、運用認可から 3 年が過ぎる前に少なくとも 1 度はアセスメントされることになる。ここでいう管理策には、外部から組織の情報システムに導入されるあらゆる共通管理策も含まれる。セキュリティ管理策のアセスメントが、必要なレベルの独立性を有する資格を持つアセサーによって、連邦政府／組織のポリシー、適切なセキュリティ標準およびガイドライン、ならびに運用認可責任者のニーズに沿って実施される場合には、それらのアセスメント結果を累積的に再運用認可に適用することができ、これによって、継続的な運用認可の概念も支援される。[72] 再運用認可活動は、運用認可パッケージ（すなわち、セキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーン）に記載されているセキュリティ状況関連情報を更新するだけで済む場合もある。続いて運用認可責任者は、組織の業務や資産、個人、他の組織、および国家に対するリスクの判断および受容に関する最新の情報に基づいて、最新の運用認可判断文書に署名する。[73]

情報システムまたはその運用環境に大幅な変更が生じた場合、継続的な監視および運用認可によって対処される場合を除き、イベント駆動型の再運用認可が実施される。大幅な変更とは、「情報システムのセキュリティ状態に影響を与える可能性の高い変更」と定義される。情報システムに対する大幅な変更には、たとえば、(i) 新規のあるいは更新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あるいはアプリケーションのインストール (ii) システムのポート、プロトコル、あるいはサービスに対する変更 (iii) 新規のあるいは更新されたハードウェアプラットフォームのインストール (iv) 暗号モジュールあるいはサービスに対する変更 (v) セキュリティ管理策に対する変更が含まれる。システムの運用環境に対する大幅な変更の例としては、たとえば、(i) 新たな施設への移動 (ii) 主要な任務および業務機能の追加 (iii) 組織が特定の脅威源に狙われているといった、具体的で信用できる脅威情報を入手 (iv) 新規のあるいは修正された法律、指令、ポリシー、または規定の制定が含まれる。[74] 正式な再運用認可活動が発動された場合、組織は、その変更による影響を受けるセキュリティ管理策のみに的を絞ると同時に、可能であれば常に、以前に実施されたアセスメントの結果を再利用する。情報システムやその運用環境に対する日常的な変更の多くは、組織の継続的監視プログラムによって取り扱われるため、結果として継続的な運用認可の概念が支援される。効果的な監視プログラムを通じて、組織は、再運用認可活動に要する全般的な費用と作業レベルを大幅に削減することができる。

運用認可責任者が代わった場合、新たに就任した運用認可責任者は、最新の運用認可判断文書、運用認可パッケージ、および継続的監視活動を通じて作成されたあらゆる最新のドキュメントを見直す。新たに就任した運用認可責任者が、現時点で文書化されているリスクを受容する場合、新しい運用認可判断文書に署名する。そうすることで、その運用認可責任者が、情報システム、または組織の情報システムによって継承される共通管理策に対する責任と説明責任を委譲し、組織の業

[72] NIST SP800-53A では、セキュリティ関連の情報をセキュリティ運用認可、継続的な運用認可、および再運用認可に再利用する際に満たすべき諸条件を記載している。

[73] 正式な再運用認可活動を開始するか否かの判断には、リスクエグゼクティブ（機能）および上級情報セキュリティ責任者が提供する情報の利用が含まれる。

[74] 先に挙げた変更の例が「大幅な変更」とみなされるのは、それらの変更が「大幅な変更」の定義において定められている閾値にあてはまる場合に限られる。

務や資産、個人、他の組織、および国家に対するリスクを明示的に受容したことになる。新たに就任した運用認可責任者が、前回の運用認可の結果（特定されたリスクを含む）を受容しない場合、再運用認可活動を開始するか、あるいは、オリジナルの運用認可を継続させるのに必要となる諸条件を新たに定める（ただし、オリジナルの運用認可の満了日を引き延ばさないことが前提）。情報システム、または組織の情報システムによって継承される共通管理策の再利用についての判断が必要な場合には、再運用認可活動に要する時間と費用を最小限に抑えるためにも、運用認可関連情報を最大限に再利用することが強く推奨される。[75]

F.5 タイプ運用認可（TYPE AUTHORIZATION）

タイプ運用認可は、指定された運用環境において、同一の情報システムまたはサブシステム（ハードウェア、ソフトウェア、ファームウェア、および／またはアプリケーションを含む）の同一の複製物を採用することについての正式な認可判断である。[76] この種の運用認可は、複数拠点に導入されている同一の情報システムに対するアーチタイプ（共通）の運用認可パッケージとして、単独の運用認可パッケージ（すなわち、セキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーン）のみの作成を許可するものである。これには、各拠点において担当組織が満たすべき導入および設定に関する一連の要求事項、あるいは運用上のセキュリティニーズが添付される。タイプ運用認可は、情報システムによって継承されるサイト固有の管理策（たとえば、物理的および環境的な保護管理策、人的セキュリティ管理策など）に対する認可と併せて使用される。[77] 第3章に一覧表示されているRMFタスクは、システム固有の管理策、ハイブリッド管理策、および共通管理策の導入に関連する運用認可活動を取り扱っている。

F.6 運用認可アプローチ（AUTHORIZATION APPROACHES）

組織は、セキュリティ運用認可を計画・実施する際に、次のような異なる3つのアプローチから適切なものを選択することができる。(i) 単独の運用認可責任者による運用認可 (ii) 複数の運用認可責任者による運用認可 (iii) 既存の運用認可の活用。[78] 1番目のアプローチは、本付録に定義されている従来型の運用認可プロセスであり、情報システムに対する責任と説明責任は、シニアリーダー職にある単独の職員が負う。また、この職員は、組織の業務や資産、個人、他の組織、または国家に影響を与える可能性のある、情報システム関連のセキュリティリスクも受容する。

2番目のアプローチは、ジョイント運用認可と呼ばれるもので、同一組織あるいは異なる組織から選抜された複数の職員が、情報システムの運用認可に対する関心を共有する場合に採用される。これらの職員は、情報システムに対する連帯責任と説明責任を負うことになり、組織の業務や資産、個人、他の組織、および国家にマイナスの影響を与える可能性のある情報システム関連のセキュリティリスクを共同で受容する。運用認可プロセスは、1番目のアプローチと似ているが、本質的な違いは、複数の運用認可責任者が認可に加わることである。ジョイント運用認可のアプローチを選択した複数組織は、共同でRMFの各タスク（付録Hを参照）を計画・実行し、合意事項と各タスクの実

[75] 正式な再運用認可活動を開始すべきか否かの判断は、さまざまな要因に基づくことがある。それらの要因には、たとえば、運用認可パッケージが提供する前回の運用認可に関する情報の受容性、前回の運用認可判断から起算した経過期間、新たに就任した運用認可責任者のリスク許容度、および組織の最新の要求事項／優先事項が含まれる。

[76] タイプ運用認可の例としては、たとえば、(i) 世界中の複数拠点に導入されている特定の標準的な金融システムに導入予定のハードウェアおよびソフトウェアに対する認可 (ii) 組織内のすべてのオペレーティングユニットに設置されている共通のワークステーションまたはオペレーティング環境（すなわち、ハードウェア、OS、ミドルウェア、およびアプリケーション）がある。

[77] 通常、サイト固有の管理策は、共通管理策として組織に導入される。

[78] 運用認可アプローチは、情報システム、ならびに、組織内の単独または複数の情報システムによって継承されるセキュリティ管理策の両方に適用することができる。

施の進捗について文書化する。ジョイント運用認可の成功には、セキュリティ分類、セキュリティ管理策の選択、有効性を判断するための管理策アセスメント計画の作成を共同で行うことが必要である。ジョイント運用認可に関する具体的な諸条件は、ジョイント運用認可に参加する組織によって定められる。これらの諸条件には、たとえば、リスクの継続的な判断および受容のためのプロセスが含まれる。ジョイント運用認可が有効であり続けるには、認可に参加している複数の運用認可責任者間の合意と、連邦政府／組織のポリシーが定める要求事項への適合が必須になる。

3番目のアプローチは、レバレッジド運用認可と呼ばれるもので、ある連邦政府機関[79]が、他の連邦政府機関（以下、オーナー組織[80]と称する）が有する情報資源（たとえば、情報システムや、そのシステムが提供するサービス）を使用する必要があり、かつ、オーナー組織によって作成された既存の運用認可パッケージに含まれる情報の一部、あるいはすべてを受容する場合に、採用される。オーナー組織によって作成された既存の運用認可パッケージを活用する側の組織（以下、レバレッジング組織と称する）は、自組織に対するリスクを判断するための材料として、オーナー組織が作成した運用認可パッケージをレビューする。[81] レバレッジング組織は、運用認可パッケージをレビューする際に、運用認可の結果が生成されてからどれくらいの期間が経過しているか、（運用認可パッケージに記載されている運用環境と実際の運用環境が異なる場合）の運用環境の差異、および処理／格納／伝送される情報の重要性／機密性、ならびに、レバレッジング組織全体の全般的なリスク許容度などのリスク因子について考慮する。運用認可パッケージに情報が不足している箇所がある、あるいは、導入されているセキュリティ対策がリスクを受容できるレベルまで軽減するのに十分でないと判断される場合、レバレッジング組織は、セキュリティ対策やセキュリティ関連情報の追加の必要性について、オーナー組織と協議する。[82] セキュリティ対策の追加には、たとえば、セキュリティ管理策の数の増加、追加のアセスメントの実施、代替管理策の実施、または情報システムやそのシステムが提供するサービスの使用に関して制約を設けることが含まれる。セキュリティ関連情報には、たとえば、運用認可パッケージに記載されていない情報システムの使用またはアセスメントに関して、オーナー組織が発見した情報などが含まれる。追加のセキュリティ対策やセキュリティ関連情報は、レバレッジング組織、情報システムの開発者、その他の外部関係者、あるいはそれらの組み合わせによって提供される場合がある。

レバレッジド運用認可のアプローチによって、大幅なコスト削減のための機会が与えられると同時に、費用と時間がかかる可能性のあるレバレッジング組織による運用認可プロセスを省略できる。レバレッジング組織は、必要な場合、オーナー組織から入手した運用認可パッケージに含まれる情報をもとに、運用認可判断文書およびリファレンスを作成する。追加のセキュリティ対策を導入した場合、レバレッジング組織は、それらの対策を文書化し、オーナー組織が作成したオリジナルの運用認可パッケージに対する付録として添付する。この付録には、必要に応じて、セキュリティ計画、セキュリティアセスメントレポート、および／または行動計画とマイルストーンへの更新が含まれる。上述した従来の運用認可プロセスとの一貫性を保つために、レバレッジング組織内のシニアリーダ

[79] この状況において、連邦政府機関には、その連邦政府機関に従属するすべての組織が含まれる。たとえば、NISTは米商務省の下部組織である。

[80] 「オーナー組織」という用語は、運用認可パッケージを所有する連邦政府機関または下部組織を示す。情報システムを所有する組織と、運用認可パッケージを所有する組織が同一でない場合がある（たとえば、システム／サービスが外部プロバイダによって提供される場合など）。

[81] 運用認可パッケージ（セキュリティ計画、セキュリティアセスメントレポート、行動計画とマイルストーン、および運用認可判断文書を含む）の共有は、すべての関係者（すなわち、オーナー組織とレバレッジング組織）が合意した諸条件の下で実現が可能になる。

[82] オーナー組織との間の協議には、他の組織が加わる場合がある（たとえば、情報システム／サービスの一部あるいはすべてが、外部プロバイダによってオーナー組織に提供されている場合など）。

一職にある単独の職員は、組織の業務や資産、個人、他の組織、および国家に影響を与える可能性のある情報システム関連のセキュリティリスクの受容に関して、責任と説明責任を負う。レバレッジド運用認可が有効であり続けるには、レッジング組織が情報システム関連のセキュリティリスクを受容することと、その運用認可が連邦政府／組織のポリシーが規定する要求事項に適合することが必須になる。そのためには、オーナー組織によって実施された継続的監視活動から得られる情報（たとえば、セキュリティ計画、セキュリティアセスメントレポート、行動計画とマイルストーン、およびセキュリティ状況報告書に対する更新の内容）の共有が必要となる。すべての関係者のセキュリティを向上させるために、レッジング組織は、オーナー組織が生成した運用認可結果を補足するためにレッジング組織が実施した、RMF 関連活動から得た結果を、オーナー組織との間で共有してもよい。

上述した 3 つの運用認可アプローチでは、いずれの場合も外部プロバイダが関与するリスクマネジメント関連活動（RMF の各タスクを含む）は、付録Hと付録Iに記載されているガイダンスに従って実施される。

付録 G

継続的な監視

情報システムのセキュリティ状態の管理および追跡

情報システムの運用および使用により生じる、情報に対するリスクを管理するうえで重要な側面には、システムに導入されている、またはシステムによって継承されたセキュリティ管理策の継続的な監視が含まれる。[83] 導入されているセキュリティ管理策に対する徹底したポイントインタイムアセスメントの実施は必要ではあるが、組織がセキュリティ上の善管注意義務を果たしていることを示すための十分な条件にはならない。効果的な情報セキュリティプログラムには、システム開発ライフサイクルに組み入れられた厳格な継続的監視プログラムも含まれる。そのような厳格な継続的監視プログラムの目的は、導入されているセキュリティ管理策一式に変更が生じることは避けられないことを踏まえたうえで、それらの管理策の有効性が、時間が経過しても維持されているか否かを判断することにある。継続的な監視は、ハードウェア、ソフトウェア、ファームウェア、または運用環境に対する変更により生じる情報システムに対するセキュリティ影響に対処するための、実証済みの技法である。設計と管理に優れた継続的監視プログラムを通じて、組織は、静的なセキュリティ管理策アセスメントおよびリスク判断プロセスを動的なプロセスに変化させることができる。この動的なプロセスによって、適切なリスク軽減活動を実施し、情報システムの運用に関する費用対効果の高い、リスクベースの判断を下すために必要となる、セキュリティ状況に関する重要、かつ、リアルタイムに近い情報が組織の職員に提供される。継続的監視プログラムは、セキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーンに対する効果的な更新メカニズムを組織に提供する。

G.1 監視戦略（MONITORING STRATEGY）

組織は、情報システムやその運用環境に対して提案されている、あるいは、実際に実施された、すべての変更を考慮したうえで、管理策セットの変更または補足についての潜在的なニーズを含む、セキュリティ管理策の有効性を継続的に監視するための戦略を策定し、プログラムを実施する。その継続的監視プログラムは、組織のシステム開発ライフサイクルに組み入れられる。厳格な継続的監視プログラムは、情報システムのオーナーおよび共通管理策の提供者、最高情報責任者、上級情報セキュリティ責任者、および運用認可責任者による積極的な関与が必要となる。厳格な継続的監視プログラムを実施することによって、組織は、(i) 情報システムのセキュリティ状態を継続的に追跡し、かつ (ii) 変化する脅威、脆弱性、テクノロジー、および任務／業務プロセスを伴う極めて動的な運用環境において、初期のセキュリティ運用認可を維持することができる。自動化された支援ツールを用いてセキュリティ管理策を継続的に監視することによって、リアルタイムに近いリスクマネジメントが容易になり、かつ、セキュリティ運用認可活動の採用方法についても、過去に比べて大幅な変化が示されることになる。情報システムにおけるリアルタイムに近いリスクマネジメントは、自動化された支援ツールを使用して RMF の種々のステップ（運用認可関連活動を含む）を実行することによって、容易に実現できる。情報システムのセキュリティ状態の判断を支援する脆弱性走査ツールやシステムおよびネットワーク監視ツールなどの自動化された支援ツールに加えて、組織は、自動化されたセキュリティマネジメント・報告ツールを使用して、運用認可パッケージ内の主要ドキュメント（セキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーンを含む）を更新することができる。運用認可パッケージ内のドキュメントは、「生きたドキュメント」として扱わ

[83] 組織内の継続的監視プログラムには、セキュリティインシデントの監視プログラムまたはセキュリティイベントの監視プログラムとは異なる活動が含まれる。

れ、情報システムのセキュリティ状態に影響を与える可能性のある実際のイベントに基づいて更新される。

リアルタイムに近いリスクマネジメントでは、適時性が極めて重要になる。組織には、意思決定者によるタイムリーなレビューと意思決定を支援するために、入手可能な情報を整理統合し、動向報告書や他の種類のダッシュボードによる視覚化の形式で表示できるようにしておくことが推奨される。リアルタイムに近いリスクマネジメント環境への移行では、時間の経過とともに自動化された支援ツールの使用を増やすことが必要となるだろう。なぜならば、組織は、利用できるリソースに応じて前述の技法を自身の情報セキュリティプログラムに組み入れるからである。

組織全体にわたる効果的な継続的監視プログラムには、次のような項目が含まれる。

- 組織の情報システムに対する構成管理および構成制御プロセス
- 組織の情報システムやその運用環境に対して提案されている、あるいは、実際に実施された変更がもたらすセキュリティ影響の分析 [84]
- 組織が定めた継続的監視戦略 [85]に基づいた、選択されたセキュリティ管理策（システム固有の管理策、ハイブリッド管理策、および共通管理策含む）のアセスメント
- 組織内の適切な職員に対するセキュリティ状況の報告 [86]
- 情報システム関連のセキュリティリスクの継続的な管理への、運用認可責任者による積極的な関与

構成管理および構成制御に関しては、情報システムやその運用環境に対して提案されている、あるいは、実際に実施された変更を文書化し、続いて、それらの変更が情報システムの全体的なセキュリティ状態にもたらす影響を評価にすることが重要となる。通常、情報システムやその運用環境は、常に変化する（たとえば、ハードウェア、ソフトウェア、またはファームウェアのアップグレード、組織の任務および業務プロセスの再定義、ならびに新たな脅威の発見などを通じて）。日常的なシステム開発ライフサイクルプロセスの一環として情報システムに対する変更を文書化して、それらの変更が情報システムのセキュリティ状態にもたらす可能性のある影響を評価することは、継続的な監視、最新の運用認可の維持、および再運用認可に関する判断（必要な場合）を支援するうえで重要である。

[84] 継続的監視活動の主な焦点は、情報システムに導入される、または情報システムによって継承されるセキュリティ管理策の有効性に置かれるが、システムの運用環境には、継続的な監視を必要とする他の重要な外部因子が存在する。これらの因子には、たとえば、組織の任務または業務プロセスに対する変更、脅威スペース（threat space）の変化、および以前に受容したリスク（複数）に対する許容度の変化が含まれる。

[85] 自動化ツールを使用することで、組織は、手動プロセスを用いた場合よりも多くのセキュリティ管理策を継続的に監視できる。結果として、組織は、自動化ツールの使用頻度を増やすことによって、より多くのセキュリティ管理策を監視する可能性がある。

[86] セキュリティ状況の報告に関する広さ、深さ、および形式については、大きな自由度と柔軟性が組織に与えられている。セキュリティ状況報告書には、少なくとも、セキュリティ計画、セキュリティアセスメントレポート、および行動計画とマイルストーンに対する主要な変更についての全容または要約が含まれる。組織の判断によって、情報システムのセキュリティ状況報告書を、すべてのセキュリティ関連の弱点または欠陥を修正する活動の文書化に関する FISMA の報告要件を満たすのを支援するために用いることができる。

G.2 監視すべきセキュリティ管理策の選択（SELECTION OF SECURITY CONTROLS FOR MONITORING）

どのセキュリティ管理策を監視するかの選択と、どの程度の頻度で監視を行うかについて判断基準は、運用認可責任者または指名された代理人、最高情報責任者、上級情報セキュリティ責任者、およびリスクエグゼクティブ（機能）の協力のもと、情報システムのオーナーまたは共通管理策の提供者によって定められる。確立された選択基準は、組織の業務や資産、個人、他の組織、および（FIPS 199 または CNSS Instruction 1253 に従って）国家に対する当該情報システム（あるいは、共通管理策の場合、それらの管理策を継承する情報システム）の優先順位および重要性を反映したものとなる。組織は、監視すべきセキュリティ管理策を選択し、それらの管理策に対する監視プロセスの頻度を決定するために、最新のリスクアセスメント結果（脅威や脆弱性に関する最新情報を含む）、サイバー攻撃の前歴、前回のセキュリティアセスメントの結果、および運用上の要求事項を使用してもよい。

セキュリティ管理策の監視における優先権は、最も変化が激しい管理策と、組織の行動計画とマイルストーンに記載されている管理策に与えられる。セキュリティ管理策の変わりやすさ（volatility）は、導入後に、その管理策が一定期間にわたってどれくらいの頻度で変化する可能性が高いかを示す一つの尺度である。たとえば、特定の組織のセキュリティポリシーおよび手順が年ごとに変化する可能性は少ないと判断される場合、その組織のセキュリティ管理策は、変化が少ない管理策とみなされるだろう。一方で、情報システムのハードウェア、ソフトウェア、および／またはファームウェアコンポーネントが頻繁に変わることによる直接的な影響、または副次的な影響を受けやすいアクセス制御やその他の（技術面での）セキュリティ管理策は、変化が多い管理策とみなされるだろう。行動計画とマイルストーンに記載されているセキュリティ管理策も、継続的監視プロセスにおいて優先権が与えられる管理策である。なぜなら、それらの管理策は、効果が薄いとみなされた管理策であるからである。また、組織は、監視すべきセキュリティ管理策を選択し、それらの管理策に対する監視の頻度を決定する際に、既知の攻撃ベクター（すなわち、脅威源によって利用される特定の脆弱性）を含む、脅威に関する具体的な情報も考慮する。運用認可責任者または指名された代理人は、監視活動の頻度はもとより、継続的に監視すべきセキュリティ管理策を承認する。

G.3 主要ドキュメントの更新および状況報告（KEY DOCUMENT UPDATES AND STATUS REPORTING）

継続的な監視の結果は、セキュリティ計画、セキュリティアセスメントレポート、および達成項目と行動計画に対するすべての必要な更新という観点から検討されなければならない。なぜなら、これらのドキュメントは、将来のリスクマネジメント活動をガイドするため用いられるからである。更新されたセキュリティ計画は、情報システムのオーナーまたは共通管理策の提供者が実施するリスク軽減活動に基づいた、セキュリティ管理策に対するすべての変更を反映したものとなる。更新されたセキュリティアセスメントレポートは、セキュリティ計画と、導入されている管理策に対する変更後の、セキュリティ管理策の有効性を判断するためにアセサーが実施する、追加のアセスメント活動を反映したものとなる。更新された行動計画とマイルストーンには、(i) 計画にリストアップされている重要な項目の進捗状況についての報告　(ii) セキュリティ影響分析またはセキュリティ管理策の監視中に発見された脆弱性に対する言及　(iii) 情報システムのオーナーまたは共通管理策の提供者が、それらの脆弱性にどのように対処しようとしているかに関する記述が含まれる。監視活動の結果は、状況報告書の形式で運用認可責任者に継続的に報告される。組織内の他の主要な職員（たとえば、リスクエグゼクティブ（機能）、上級情報セキュリティ責任者）は、必要な場合に、あるいはそのような要請があった場合に、継続的監視活動の結果を受け取る。自動化された支援ツールと、組織全体にわたる効果的なセキュリティプログラムマネジメントプラクティスを用いることによって、運用認可責任者は、運用認可パッケージに含まれる最新のドキュメントにいつでもアクセスできるようになる

と同時に、情報システムの最新のセキュリティ状態の把握、リスクマネジメントの支援、および再運用認可に関する判断に必要な重要な情報の提供が可能になる。セキュリティ管理策、および情報システムやその運用環境に対する変更の監視は、システム開発ライフサイクル全体を通して継続的に実施される。監視結果の要約は、上級情報セキュリティ責任者およびリスクエグゼクティブ（機能）に提供される。

付録 H

運用上のシナリオ

さまざまな環境へのリスクマネジメントフレームワークの適用

多様な潜在的ビジネス関係を伴う現代のコンピュータ環境において、情報システムの運用および使用により生じる、情報に対するリスクを管理することは、組織にとって難題となることがある。ビジネス関係は、さまざまな形式で構築・維持される。たとえば、ジョイントベンチャー、ビジネスパートナーシップ、外注契約（すなわち、契約、業務分野についての取り決め、省庁間の取り決めや省庁内の取り決めを介して）、ライセンス契約、およびサプライチェーンの交換などが考えられる。[87] リスクマネジメントフレームワーク（RMF）は、連邦政府の情報システムにのみ適用される。RMFの各ステップおよび関連するタスクを組織がどのように実施するかを左右する運用上のシナリオには、次のような 2 つの異なる種類がある。

- 連邦政府機関 [88]によって使用または運用される情報システム
- 連邦政府機関の代わりとなる他の組織 [89]によって使用または運用される情報システム

シナリオ 1: 連邦政府機関によって使用または運用される情報システムの場合、そのシステムの境界は、当該政府機関によって定められる。その政府機関は、情報システムの運用認可を含む、すべての RMF タスクを実施する。また、情報システムに導入される、または情報システムによって継承されるセキュリティ管理策を管理し続ける。

シナリオ 2: 連邦政府機関の代わりとなる他の組織によって使用または運用される情報システムの場合、そのシステムの境界は、連邦政府機関が、連邦政府機関に代わって当該システムを使用または運用する他の組織と共同で定めることになる。また、そのようなシステムは、以下に示す状況のいずれかに当てはまる。

- その組織が連邦政府機関と契約を結んでいる場合、連邦政府機関が政府機関としての責務の一環として実施するタスクを除くすべてのRMFタスクを、その組織（以下、請負組織と称する）が実施することになる。[90] 当該政府機関は、請負組織に対して、必要に応じてRMF関連の情報を提供し、請負組織が実施するすべてのRMFタスクに対する厳格な管理を維持する。請負組織は、連邦政府機関の運用認可責任者が運用認可判断を下す際に必要となる、適切な証拠をセキュリティ運用認可パッケージに含める。
- 他の連邦政府機関（以下、請負政府機関と称する）が、当該連邦政府機関に代わってその情報システムを使用または運用する場合、その情報システムの運用認可を含むすべての RMF タスクを、請負政府機関が実施することになる。両当事者が運用認可についての責任の共有に合意

[87] NIST SP800-53 には、外部サービスプロバイダとの間の関係を含む、外部環境におけるセキュリティ管理策の適用および使用に関する追加的なガイダンスが記載されている。

[88] ここでいう連邦政府機関には、連邦政府機関に従属する組織が含まれる。

[89] 連邦政府機関の代わりに情報システムを使用または運用する組織、もしくは連邦政府機関の下部組織には、たとえば、その他の連邦政府機関やそれらの連邦政府機関の下部組織、州または地方の政府機関、請負業者、および学術機関が含まれる。

[90] 組織は、RMF の特定のタスクの実施に関する要求事項が、適切な契約内容に確実に含まれるようにする。これには、（該当する場合）独立したアセスメントに対する要求事項が含まれる。

した場合、その情報システムの運用認可はジョイント運用認可となることもある。一つの連邦政府機関が複数の連邦政府機関に代わって情報システムを使用または運用する場合、ジョイント運用認可には、関係するすべての政府機関が参加することになる。

付録 I

外部環境におけるセキュリティ管理策

パートナーシップ、外部委託、およびサプライチェーンに関する考慮事項

組織が、重要な任務およびビジネス機能を実施するために、外部プロバイダが提供する情報システムサービスに依存することが多くなっている。外部情報システムサービスとは、組織が、自身の情報システムに対して定めた認可境界（運用認可が及ぶ範囲）外で実施されるサービス。これらの外部サービスは、組織の情報システムによって利用される可能性のあるサービスではあるが、そのシステムの一部ではない。場合によっては内部情報システムの機能のすべてが、外部情報システムサービスによって置き換えられることもある。外部プロバイダが提供するサービスの使用により生じるリスクに対する責任と説明責任は、それらのサービスを使用する組織が負うことになる。また、そのリスクが、運用認可責任者または組織が受容できるレベルを超えたものである場合、組織は代替管理策を実施することでリスクに対処する。

外部サービスプロバイダとの関係は、さまざまな形式で構築される。たとえば、ジョイントベンチャー、ビジネスパートナーシップ、外注契約（すなわち、契約、省庁間の取り決め、業務分野についての取り決めを介して）、ライセンス契約および／またはサプライチェーンの交換などが考えられる。外部サービスプロバイダへの依存度が増し、それらのプロバイダとの新たな関係が構築されるにつれ、組織は、特に情報システムセキュリティの分野において、新たな難題を抱えることになった。そうした難題には、以下の項目が含まれる。

- 組織に提供される外部サービスの種類を定義すること
- 組織が定めるセキュリティ要求事項に従って外部サービスがどのように保護されるかについて記述すること
- 外部サービスの使用により生じる組織の業務や資産、個人、他の組織、および国家に対するリスクが、受容できる範囲内に収まることに対する、必要な保証を得る。

FISMAおよびOMBポリシーは、連邦政府の情報を扱う外部プロバイダ、または連邦政府の代わりに情報システムを運用する外部プロバイダに対して、連邦政府機関と同様のセキュリティ要求事項を満たすことを義務づけている。外部プロバイダに課せられるセキュリティ要求事項（連邦政府の情報を処理、格納、伝送する情報システムに導入すべきセキュリティ管理策を含む）は、適切な契約書またはその他の正式な合意書に記載される。組織は、外部プロバイダに対して、セキュリティ運用認可ステップの除く、すべてのRMFステップの実施を要求することができる。セキュリティ運用認可ステップは、外部情報システムサービスの使用に関連するリスクの管理に直結する、連邦政府が本来果たすべき責務である。[91]

外部サービスの使用により生じるリスクが受容できるレベルであること対する保証または信頼は、組織がその外部サービスプロバイダをどれだけ信頼しているかに依る。[92] 場合によっては、サービ

[91] この文脈において、特定の連邦政府機関が外部プロバイダである場合、その政府機関が情報システムの運用認可を含むすべての RMF タスクを実施することが考えられる（付録 H を参照）。

[92] 組織が外部のサービスプロバイダをどれだけ信頼するかは、プロバイダごとに大きく異なる。例えば、組織の高い信頼を得るプロバイダ（例：共通のビジネスモデルや目的を持つ共同事業者）もあれば、リスク要因が大きいために高い信頼を得られないプロバイダ（例：ある市場部門ではビジネスパートナーだが、他の市場部門では競合相手にもなる場合など）もある。

スの保護に必要なセキュリティ管理策の採用に関して、また、それらの管理策の有効性を証明する証拠の提出に関して、組織が外部サービスプロバイダをどれだけ直接管理できるかに基づくこともある。外部のサービスプロバイダをどれだけ管理できるかは、通常、プロバイダとの契約やサービス内容合意書（SLA）の諸条件によって定められ、契約の範囲は、広範囲のもの（例：詳細なセキュリティ管理要件を定めた契約書または同意書をプロバイダと交わす）から非常に限られたもの（例：商用通信サービスなどの汎用サービス[93]を受けるための、契約またはサービス内容合意書の利用）までさまざまである。この他にも、信用度は、必要不可欠なセキュリティ管理策が採用されていること、また、その管理策が有効であることを組織に納得させることができるなど、他の要因から導き出されることがある。たとえば、確固たる取引関係を通じて個別に認可を受けて組織に提供される外部情報システムサービスは、運用認可責任者が定める受容可能なリスクの範囲内に収まる場合に、ある程度の信頼を与えると考えられる。

外部プロバイダによるサービスの供給は、そのサービスに責任を負う外部組織と、サービスを受ける組織間に、明示的な合意が無い状態で、サービスが提供される可能性がある。契約書やサービス内容合意書などによる明示的な合意が可能な場合、組織は、契約書（または合意書）を作成し、契約者に対して、NIST SP 800-53に記載されているセキュリティ管理策の使用を要求すべきである。組織が外部サービスプロバイダに対して明示的な合意を要求できる立場にない場合（例：サービスに関する責任が組織に課せられている場合や、そのサービスが汎用サービスである場合など）、組織は、セキュリティに関するサービスの機能について明確な条件を設定する。組織が、中央集中型の調達手段（たとえば、一般調達局（General Services Administration）、あるいは、その他の任意／必須の調達組織との間の政府全体的な契約）を通じて情報システムサービスあるいは情報システムテクノロジーを調達している場合、契約書の作成者側が外部プロバイダとの間で組織が定めるレベルの信頼（必須のセキュリティ管理策の定義、およびそれらの管理策の提供に関する保障レベルを含む）を構築・維持した方が、そうでない場合よりも高い効率と費用対効果を実現できる可能性がある。中央集中型の契約を通じて情報システムサービスあるいは情報システムテクノロジーを調達している組織は、調達元が定めた信頼レベルを活用できる。これにより、そうした信頼を築くのに必要な活動を高い費用をかけて繰り返すといったことが回避される。[94] 組織と外部プロバイダと間の契約が、当該組織による積極的な関与を求める場合がある。たとえば組織が、契約によって、サービスプロバイダが推奨する、公開鍵による暗号化が可能なクライアントソフトウェアをインストールするよう求められることがある。

最終的に、外部情報システムサービスの使用により生じる受容できないリスクを十分に軽減する責任は、運用認可責任者にある。組織は、外部サービスプロバイダとの間で情報システムセキュリティに関するさまざまな問題が扱われる場合には、外部サービスプロバイダとの間に適切なトラストチェーンが構築されることを求めなければならない。トラストチェーンの構築には、外部サービスを提供するそれぞれのプロバイダが、複雑になりがちな消費者—提供者の関係において、サービスに対する適切な保護を行っていることが、組織によって確認され、その状態が維持されることが求められる。消費者—提供者の関係に関与する事業体の数が多い場合や、これらの事業体同士の関係の種類によっては、トラストチェーンの構築が非常に困難な場合がある。外部のサービスプロ

[93] 通常、汎用サービスを提供する営利目的のプロバイダは、広範囲のさまざまな顧客層を対象に、共有可能な資源およびデバイスのコンセプトに基づき、ビジネスモデルおよびサービスを構築する。したがって組織がプロバイダから受けるサービスが組織専用のサービスでない場合、サービスに依存する情報システムを適切に保護するには、補足的なセキュリティ管理策に大きく頼らざるをえない可能性がある。組織のリスクアセスメントやリスク軽減活動を行う際には、この点を考慮しなければならない。

[94] たとえば、調達元が、契約書が定める具体的な諸条件の元で連邦政府に外部サービスを提供する情報システムに対して運用認可を行う場合がある。契約書が定める諸条件の元で情報システムサービスをリクエストする政府機関は、そうしたサービスを調達する際に、情報システムの再運用認可を行う必要はない（ただし、そのリクエストに、組織の契約の範囲外のサービスが含まれる場合を除く）。

バイダは、自身が提供すべきサービスを他の外部組織に委託することがあり、この場合トラストチェーンの構築がさらに複雑になり、管理が困難になる。サービスの性質によっては、プロバイダに大きな信頼を寄せることは浅はかであるといわざるをえない場合がある。これは、プロバイダ自身に信用がないというよりは、当該サービスに内在するリスクが大きいためである。外部のサービスおよび／またはサービスプロバイダとの間で十分なレベルの信頼を構築することができない場合、組織は、(i) 代替管理策を採用する (ii) より大きなリスクを受け入れる、あるいは (iii) そのサービスを受けない（すなわち、任務および業務を機能性のレベルを下げて、あるいは、機能性を全く伴わない形で実施する）。