NIST Special Publication 800-18
改訂第 1 版

連邦情報システムのための セキュリティ計画策定ガイド

Marianne Swanson
Joan Hash
Pauline Bowen

情　報　セ キ ュ リ テ ィ

コンピュータセキュリティ部門
情報技術ラボラトリ
米国国立標準技術研究所
Gaithersburg, MD 20899-8930

2006 年 2 月

米国商務省　長官
Carlos M. Gutierrez

米国国立標準技術研究所　所長
William Jeffrey

この文書は下記団体によって翻訳監修されています

情報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、テストの実施、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と国家安全保障にかかわらない情報のプライバシ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、コンピュータ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、普及活動と、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

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、2002 年施行の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推進するために、この文書を作成した。

NIST は、すべての連邦政府機関の運営および資産に適切な情報セキュリティをもたらすために、最低限の要求事項を含んだ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国家安全保障に関わるシステムには適用されない。このガイドラインは、行政管理予算局（OMB; Office of Management and Budget）Circular A-130、第 8b(3)項、『政府機関の情報システムの保護（Securing Agency Information Systems）』の要求事項に一致しており、これは A-130 の付録 IV「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。

このガイドラインは連邦政府機関が使用する目的で作成されている。非政府組織が自由意志で使用することもでき、著作権の制約はない（翻訳者注：著作権に関するこの記述は、SP800-18 の英語の原文のことを言っており、日本語へ翻訳した本書の著作権は、独立行政法人情報処理推進機構および NRI セキュアテクノロジーズ株式会社に帰属する）。

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。

本文書中で言及される商業的組織、装置、資料は、実験手順あるい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、あるいは装置が、その目的に関して得られる最善のものであることを意味しているわけでもない。

謝辞

NIST は、NIST Special Publication 800-18 *Guide for Developing Security Plans for Information Technology System*（情報技術システムのためのセキュリティ計画策定ガイド）初版の作成者に謝意を表する。初版を本改訂版のベースとして使用した。また、本文書をレビューしコメントを寄せてくれたすべての NIST 職員にも感謝の意を表する。

目次

本書の概要

システムセキュリティ計画の目的は、情報システム資源の保護対策の改善である。連邦システムはすべて、何らかのレベルの機密性の高さを持ち、それに対する保護は、管理上の良き慣行として行われるべきものである。システムの保護は、システムセキュリティ計画の中で文書化しなければならない。システムセキュリティ計画を策定することは、行政管理予算局（OMB）Circular A-130 “Management of Federal Information Resources” 、Appendix III “Security of Federal Automated Information Resources”および E-Government Act の第Ⅲ編である FISMA の要求事項である。

システムセキュリティ計画の目的は、システムに対するセキュリティ要求事項の概観を提供し、これらの要求事項を満たすために設定または計画されている管理策について記述することである。システムセキュリティ計画はまた、システムにアクセスするすべての個人の責任および期待される行動を明確に記述する。システムセキュリティ計画は、システムに対する適切で費用対効果の高いセキュリティ保護策を計画するための構造化されたプロセスを文書化したものと考えるべきである。システムセキュリティ計画は、情報のオーナー、システムのオーナー、政府機関の上級情報セキュリティ責任者（SAISO）を含む、システムに関する責任を有するさまざまな管理者から提供される情報を反映すべきである。追加情報は、本文書の主なセクションの記述が適切に網羅され、かつ容易に識別可能である限り基本計画に含めてもよく、構成および書式は、各政府機関のニーズに応じて作り変えてもよい。

資源の保護を計画に適切に反映させるために、上級管理責任者はシステムの運用認可を行わなければならない。情報処理システムの運用認可を管理責任者が行うことによって、重要な品質管理が実現される。システムの運用を許可することで、管理者は関連するリスクを受容することになる。

管理者による運用認可は、管理的、運用的、技術的管理策の評価に基づいて行われるべきである。システムセキュリティ計画はセキュリティ管理策を確立し文書化するので、評価報告と行動計画およびマイルストーンにより補完されて、運用認可の基礎を形成する。さらに、管理策を定期的に見直すことも将来の認可に貢献するはずである。再認可は、情報システムにおける処理に重大な変更があった場合には必ず行うが、少なくとも 3 年に一度は行うべきである。

1. はじめに

今日、技術環境が急速に変化しているため、連邦政府機関はその情報と情報システムを保護するために最低限のセキュリティ管理策を採用することを求められている。FIPS（Federal Information Processing Standard：連邦情報処理規格）200、*Minimum Security Requirements for Federal Information and Information Systems（連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項）*は、連邦政府の情報および情報システムに関する最低限のセキュリティ要求事項を 17 のセキュリティ領域について規定している。連邦政府機関は、NIST Special Publication 800-53、*Recommended Security Controls for Federal Information Systems*（連邦政府情報システムにおける推奨セキュリティ管理策）に記載されたセキュリティ管理策を導入することによって、FIPS 200 で規定された最低限のセキュリティ要件を満たさなければならない。NIST SP 800-53 には、情報システムに対して規定された管理的、運用的、および技術的な保護手段や対抗策が含まれている。選定または計画した管理策は、システムセキュリティ計画の中で文書化しなければならない。本文書は、連邦政府機関が連邦情報システムに対するシステムセキュリティ計画を作成する際の指針を提供する。

1.1 背景

E-Government Act の第Ⅲ編、Federal Information Security Management Act（FISMA：連邦情報セキュリティマネジメント法、以下、FISMA と称す）は、各連邦政府機関がその機関全体を対象とした情報セキュリティプログラムを開発、文書化、および実施することを義務付けている。この情報セキュリティプログラムは、他の政府機関、請負業者またはその他の情報源が提供または管理するものも含め、政府機関の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。システムセキュリティ計画は、システム開発ライフサイクル（SDLC）を支援する重要な活動であり、システムに起こるさまざまな事象を契機としてシステムの最新の状態を正確に反映するように改訂されるべきである。システムセキュリティ計画は、情報システムに対するセキュリティ要求事項をまとめ、これらの要求事項を満たすために実施または計画されているセキュリティ管理策について記述する。システムセキュリティ計画はまた、情報システムに対するセキュリティに関するその他の重要な文書（リスクアセスメント、活動計画およびマイルストーン、承認決定書、プライバシー影響アセスメント、緊急時対応計画、構成管理計画、セキュリティ設定チェックリスト、システム相互接続協定など）を必要に応じて参照する場合もある。

1.2 対象とする読者

組織内のセキュリティプログラムマネージャー、システムオーナー、およびセキュリティ要員は、システムセキュリティ計画のプロセスを理解しなければならない。さらに、情報システムの利用者とシステム要件定義の担当者も、システムセキュリティ計画のプロセスを十分理解しているべきである。情報システムの導入および管理担当者は、それぞれの担当システムに適用するセキュリティ管理策の実施に関与しなければならない。本文書の指針は、システムセキュリティ計画を準備する方法について基本的な情報を提供する。この指針は、さまざまな組織構成に適用できるように設計されており、セキュリティ計画に関する活動に責任を負う担当者が参照するためのものである。

1.3 本文書の構成

本文書は、情報システムセキュリティ計画を作成するための一連の活動と概念を紹介する。本文書の内容を以下に簡単に示す。

- ***第1章***には、システムセキュリティ計画のプロセスに関する背景情報、対象とする読者、FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems*（連邦政府の情報および情報システムに対するセキュリティ分類規格）に関する情報、情報システムのさまざまな分類の説明、本文書に関連する NIST 文書、システムセキュリティ計画の作成に関する役割と責任の説明がある。
- ***第2章***では、政府機関がシステム境界を設定するプロセスで保有する情報システムの棚卸しの方法について述べる。また、共通セキュリティ管理策の明確化と詳細調査の指針についても説明する。
- ***第3章***では、システムセキュリティ計画の作成ステップについて説明する。
- ***付録A*** は、システムセキュリティ計画のテンプレートである。
- ***付録B*** は、用語および定義の用語集である。
- ***付録C*** は、本文書を補足する参考文献のリストである。

1.4 システムの資産目録と連邦情報処理規格（FIPS 199）

FISMA によれば、政府機関は情報システムの棚卸しを実施する必要がある。システムセキュリティ計画アクティビティの最初のステップとして、情報システム資産目録に含まれるすべての情報システムを FIPS 199 に従って分類すべきである。

FIPS 199 は、各連邦政府機関が準拠することが必須の標準であり、連邦政府機関が収集・維持するすべての情報および情報システムを分類し、その脅威レベルに基づいた適切な情報セキュリティを提供するために使われる。。情報および情報システムに対するセキュリティ分類規格は、セキュリティについて表現する共通の枠組みと理解を提供するものであり、これによって連邦政府は以下のことを推進する。(i) 民間、国家安全保障、緊急時対応、国土安全保障、および法執行機関などのコミュニティ全体における情報セキュリティへの取り組みの調整を含む、情報セキュリティプログラムの効果的な管理監視。ならびに (ii) 行政管理予算局（OMB：Office of Management and Budget）および連邦議会への、情報セキュリティポリシー、手順、および実践の妥当性と有効性に関する一貫性のある報告。

1.5 主要アプリケーション、一般支援システム、非主要アプリケーション

すべての情報システムをシステムセキュリティ計画の対象として、主要アプリケーション[1]か一般支援システム[2]のラベルを付けなければならない。非主要アプリケーション[3]に対するセキュリティ管理策は、通常それらを運用する一般支援システムまたは主要アプリケーションが提供するため、非主要アプリケーションに対する特定のシステムセキュリティ計画を作成する必要はない。非主要アプリケーションが主要アプ

[1] OMB Circular A-130、付録 III は、主要アプリケーションを、アプリケーション内の情報の損失、誤用、または不当なアクセスや改変によって発生するリスクと損害の大きさのために、セキュリティに対する特別な注意が必要なアプリケーションであると定義している。

[2] OMB Circular A-130、付録 III は、一般支援システムを、共通の機能を共有する同一の直接統制管理下にある相互接続された一連の情報資源であると定義している。通常、ハードウェア、ソフトウェア、情報、データ、アプリケーション、通信、および人が含まれる。

[3] NIST Special Publication 800-37 は、非主要アプリケーションを、主要アプリケーション（アプリケーション内の情報の損失、誤用、またはそれらの情報に対する許可されていないアクセスや改変によって発生するリスクと損害の大きさのために、セキュリティに対する特別な注意が必要なアプリケーション）以外のアプリケーションであると定義している。非主要アプリケーションは通常、一般支援システムの一部として含まれる。

リケーションや一般支援システムに接続されていない場合、その非主要アプリケーションと設置場所が同じ、または、サポートする組織が同じである一般支援システムのセキュリティ計画中で、その非主要アプリケーションについて簡単に説明すべきである。追加情報は第 2 章に記載されている。

1.6 関連する他の NIST 文書

システムセキュリティ計画を作成するためには、NIST のセキュリティ標準およびガイドラインを十分理解しておく必要がある。本文書の読者は、NIST FIPS 199 に記述されている情報システムの分類に関する要件と方法を理解するだけでなく、NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*（連邦政府情報システムにおける推奨セキュリティ管理策）および FIPS 200 *Minimum Security Requirements for Federal information and Information System*（連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項）に記述されている所定のシステムに対して必要最低限のセキュリティ管理策を実施するにあたっての要件を理解することが不可欠である。

セキュリティ計画の準備を直接サポートしている他の重要な NIST 文書には、NIST SP 800-30 *Risk Management Guide for Information Technology Systems*（IT システムのためのリスクマネジメントガイド）および NIST SP 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems*（連邦政府情報システムのセキュリティに関する承認および運用認可のガイド）がある。全ての文書は NIST Computer Security Resource Center のウェブサイト（http://csrc.nist.gov/）から入手可能である。

1.7 システムセキュリティ計画に関する責任

政府機関は、システムセキュリティ計画策定プロセスに関する方針を作成すべきである。システムセキュリティ計画は、常に変化する文書であり、セキュリティ管理策を実施するための定期的な見直し、修正、活動計画、およびマイルストーンを必要とする。誰が計画を見直し、計画を最新の状態に保ち、計画されたセキュリティ管理策を確認するのかについての要点をまとめた手順を用意すべきである。さらに、システムに対するセキュリティ承認および運用認可プロセスを進める前に、システムセキュリティ計画の策定とレビューを行うことを手順の要求事項に含めるべきである。

セキュリティ承認および運用認可プロセスにおいて、システムセキュリティ計画の分析、更新、受け入れを行う。承認者は、システムセキュリティ計画に記述されているセキュリティ管理策が、その情報システムに対して指定されている FIPS 199 セキュリティ分類に適合していることを確認するとともに、システムセキュリティ計画、リスクアセスメント、または同等の文書において、脅威と脆弱性の明確化および初期リスク判定が明確化され文書化されていることを確認する。セキュリティ承認の結果は、リスクの再評価、修復活動の追跡に必要な活動計画およびマイルストーン（POA&M）の作成、ならびにシステムセキュリティ計画の更新に使用され、ひいては認可責任者が運用認可の判断を下す際に事実に基づいた根拠を提供する。承認および運用認可プロセスに関する追加情報については、NIST SP 800-37 を参照されたい。図 1 は、セキュリティ計画プロセスの主な入力と出力を示している。

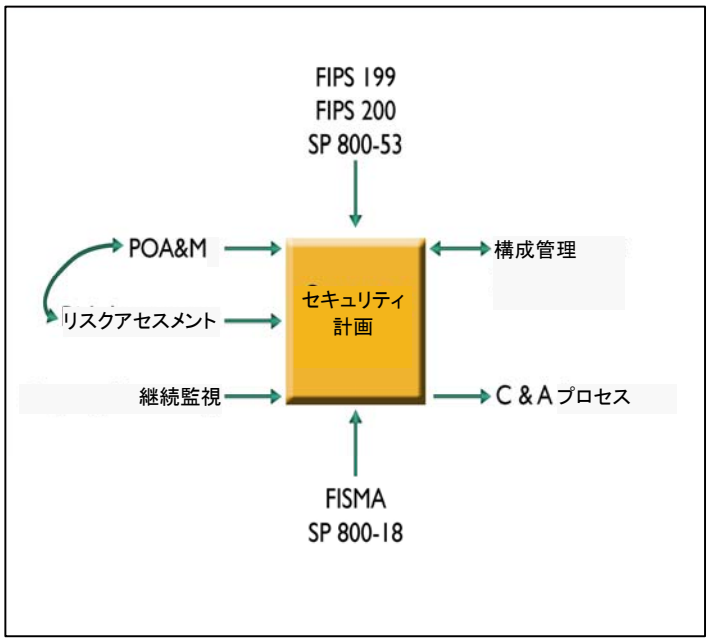

図 1:セキュリティ計画プロセスの入力と出力

この節で述べる役割と責任は、情報システムセキュリティ計画特有のものである。政府機関の多岐にわたるミッションと組織構造を踏まえれば、セキュリティ計画関連の役割に対する命名規則や、政府機関職員への関連する責任の割り当て方(たとえば、1 つの役割を複数の担当者に、または複数の役割を 1 人の担当者に割り当てるなど[4])が異なる場合がある。

1.7.1 最高情報責任者

最高情報責任者(CIO)[5]は、その政府機関全体の情報セキュリティプログラムの作成と保守に責任を持つ政府機関の職員であり、システムセキュリティ計画について次の責任を負う。

- システムセキュリティ計画に対して CIO の責任を果たす、政府機関の上級情報セキュリティ責任者(SAISO)を任命する。

[4] 1 人の担当者がセキュリティ計画プロセスで複数の役割を果たす場合は、その担当者が十分なレベルの独立性を維持するとともに、利害の衝突に巻き込まれないように注意すべきである。

[5] 連邦政府機関が正式な CIO の職位を設けていない場合、FISMA は関連する責任を同等の政府機関の職員が受け持つ必要があるとしている。

- システムセキュリティ計画策定のための、情報セキュリティポリシー、手順、および管理手法を作成し維持管理する。

- 共通のセキュリティ管理策の明確化、実施、および評価について管理する。

- システムセキュリティ計画に対する重要な責任を持つ要員に対して確実に訓練を実施する。

- 政府機関の上級責任者がシステムセキュリティ計画に対する責任を遂行するのを支援する。

- 政府機関に適用する共通セキュリティ管理策を明確化し調整する。

1.7.2 情報システムのオーナー

情報システムのオーナー[6]は、情報システムの総合的な調達、開発、統合、修正、または運用と保守に責任を持つ政府機関の職員である。情報システムのオーナーは、システムセキュリティ計画に対する次の責任を負う。

- 情報のオーナー、システム管理者、情報システムセキュリティ責任者、政府機関の上級情報セキュリティ責任者、および機能の「最終利用者」と連携してシステムセキュリティ計画を策定する。

- システムセキュリティ計画を保守し、合意済みのセキュリティ要求事項に従ってシステムが、確実に配備され運用されるようにする。

- システム利用者およびサポート要員が、必要なセキュリティ訓練（例：行動規程の教育）を確実に受けられるようにする。

- 重大な変更が行われたときに必ずシステムセキュリティ計画を更新する。

- 共通セキュリティ管理策の明確化、実施、および評価を支援する。

1.7.3 情報のオーナー

情報のオーナーは、特定の情報に対する法的または運用上の権限を持ち、その生成、収集、処理、伝達、および廃棄の管理策を確立する責任を負う政府機関の職員である。情報のオーナーは、システムセキュリティ計画に対する以下の責任を負う。

[6] 情報システム所有者の役割は、特定の政府機関および情報システムのシステム開発ライフサイクル段階に応じてさまざまに解釈されうる。情報システム所有者を、プログラム管理者またはビジネス／資産／ミッションの所有者としてとらえる政府機関もある。

- 対象データ／情報の適切な使用および保護に関する規則（行動規程）を確立する。[7]

- 情報が記録されている情報システムに対するセキュリティ要件やセキュリティ管理策に関して、情報システム所有者に入力を提供する。

- 情報システムへのアクセス権を誰に与えるか、どのような種類の特権やアクセス権を与えるかを決定する。

- 情報が存在する場所の明確化とそれに対する共通セキュリティ管理策の評価を支援する。

1.7.4 政府機関の上級情報セキュリティ責任者（SAISO）

政府機関の上級情報セキュリティ責任者（SAISO）は、政府機関の情報システムオーナーおよび情報システムセキュリティ責任者に対する、CIO の主な連絡役としての責任を負う政府機関の職員である。SAISO は、システムセキュリティ計画について次の責任を負う。

- システムセキュリティ計画に対して CIO の責任を果たす。

- システムセキュリティ計画の作成、見直し、受け入れを、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、および運用認可責任者と調整する。

- 共通セキュリティ管理策の明確化、実施、および評価の調整をする。

- システムセキュリティ計画の作成や見直しを行うのに必要な専門資格（訓練や経験を含む）を持っている。

1.7.5 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責任者は、SAISO、認可責任者、管理責任者、または情報システム所有者から、情報システムやプログラムに対する適切な運用上のセキュリティポリシーを確実に維持する責任を与えられた政府機関の職員である。情報システムセキュリティ責任者は、システムセキュリティ計画について次の責任を負う。

- 政府機関の上級情報セキュリティ責任者が実施する共通セキュリティ管理策の明確化、実施、および評価を支援する。

[7] 情報所有者は、データ／情報を他の組織と共有する場合にもその責任を負う。

- システムセキュリティ計画の作成および更新に積極的な役割を果たすだけでなく、システムに対する変更を情報システムのオーナーと調整し、その変更がセキュリティに与える影響を評価する。

1.7.6 運用認可責任者

運用認可責任者（指定認可権限者と呼ぶ政府機関もある）は、連邦政府機関の運営、連邦政府機関の資産、または個人に対するリスクを許容できるレベルに維持しながら、情報システムを運用する公式な責任を負う権限を持つ上級管理責任者または幹部である[8]。運用認可責任者は、システムセキュリティ計画について次の責任を負う。

- システムセキュリティ計画を承認する。
- 情報システムの運用を認可する。
- 特定の条件下で情報システムの運用に暫定的な承認を与える。
- 容認できないセキュリティリスクが存在する場合は、情報システムの運用認可を与えない（システムがすでに運用されている場合は運用を停止する）。

1.8 行動規程

行動規程は、OMB Circular A-130 付録 III で要求されている、NIST SP 800-53 に含まれるセキュリティ管理策である。行動規程には、システムにアクセスする全担当者の責任と期待される行動を明確に記述すべきである。この規程は、それと整合しない行動や、規程に適合しないときの結果を明示し、システムへのアクセス認可を与える前に全利用者が利用できるようにすべきである。規程書には各利用者の受領を確認する署名ページを設けて、利用者が行動規程を読み、理解し、従うことに同意したことを明らかにする必要がある。行動規程に同意するのに電子署名を使用してもよい。

図 2 は、OMB Circular A-130 付録 III から引用した、代表的な行動規程に含むべき項目例のリストである。これらは単なる例であり、詳細および内容については政府機関に裁量の余地がある。行動規程を作成する際には、すべての利用者が行動規程を読み、理解し、従うことに同意することによって自分の活動に責任を持たせることがその目的であることを忘れてはいけない。行動規程は、セキュリティポリシーや手順の手引の全面的なコピーではなく、以下の図に記述された管理策のいくつかを高いレベルで取り上げるべきである。

[8] 政府機関によっては、上級責任者と最高情報責任者が共同で運用認可責任者となる場合もある。その場合は、上級責任者が最高情報責任者より前に情報システムの運用を認可する。

行動規程に含まれる管理策の例

- 全利用者の責任、期待されるシステムの利用法、および行動を明確に記述する
- 相互接続に関して該当する制限を記述する
- サービスの提供および復旧の優先度を定義する
- 規程に従わない行動の結果を記述する
- 以下の項目を取り上げる
  - 在宅勤務
  - ダイヤルインアクセス
  - インターネットへの接続
  - 著作物の利用
  - 政府装置の私的な使用
  - システム特権と担当者の説明責任の割り当ておよび制限
  - パスワードの利用
  - データベースの探索および情報の暴露

図 2:行動規程の例

1.9 システムセキュリティ計画の承認

組織の方針には、システムセキュリティ計画の承認と、計画の提出のために作成された手順に誰が責任を負うのかを明確に規定すべきである。その手順には、政府機関が必要とする特別な覚書きの言語やその他の文書交付が含まれる。通常は、承認および運用認可プロセスが実施される前に、システムオーナーとは独立の、指定された運用認可責任者が計画を承認する。

2. システム境界の分析とセキュリティ管理策

システムセキュリティ計画の策定が可能になる前に、情報システムとそのシステム内に存在する情報を FIPS 199 の影響分析に基づいて分類しなければならない。それにより、資産目録にあるどのシステムを主要アプリケーションまたは一般支援システムに論理的に分けられるかの判断ができるようになる。システム境界を引く場合、および初期の一連のセキュリティ管理策(ベースライン管理策)を選択する場合には、FIPS 199 が規定する影響レベルを考慮しなければならない。その後、ベースライン管理策を、リスクアセスメントおよび組織固有のセキュリティ要件、固有の脅威情報、費用対効果分析、補完的管理策の利用可能性、特別な状況などのローカルな条件に基づいて手直しすることができる。システム固有の管理策ではなく、政府機関レベルで対応する管理策を明確化するため、システムセキュリティ計画を準備する前に、ベースライン管理策を手直しする段階の考慮点の 1 つである共通セキュリティ管理策を明確化しなければならない。このような共通セキュリティ管理策は、参照情報としてシステムセキュリティ計画に組み込むことができる。

2.1 システム境界

システムに対するセキュリティ境界は、情報システムに情報資源[9]を一意的に割り当てるプロセスによって定義される。政府機関は、情報システムを構成する要素(主要アプリケーションや一般支援システム)を決める上で大きな裁量の余地を持つ。一連の情報資源が情報システムとして識別されたら、通常それらの資源は、同一の直接統制管理下に置かれるべきである。直接統制管理[10]とは、必ずしも介在的な管理が存在しないことではない。1 つの情報システムに複数の *サブシステム*が含まれることも考えられる。

サブシステムとは、1 つまたはそれ以上の特定の機能を実行する情報、情報技術、および要員からなる情報システムの主要な下位区分つまりコンポーネントのことである。通常、それぞれのサブシステムは同一の管理権限下に置かれ、単一のシステムセキュリティ計画に含まれる。図 3 は、3 つのサブシステムがある一般支援システムを示している。

直接統制管理の検討のほかに、政府機関が以下の基準に従って情報資源を 1 つの情報システムとして識別できるかどうかを検討することは有益な場合がある。

- 同一の機能またはミッションの目標を持ち、基本的に同一の運用特性およびセキュリティニーズを持つ。

[9] 情報資源は、情報および関連する資源(例:要員、装置、資金、情報技術)からなる。

[10] 直接統制管理には通常、予算、プログラムまたは運用の権限および関連する責任が含まれる。新しい情報システムの場合、統制管理は情報システムの開発と配備のための予算/プログラムの権限および責任を持つことと解釈できる。現時点で連邦政府のインベントリにある情報システムの場合、統制管理は情報システムの日々の運用と保守に対する予算/運用権限を持つことと解釈できる。

- 同一の一般運用環境の中に設置されている（分散情報システムの場合は、類似した運用環境を持つさまざまな場所に設置されている）。

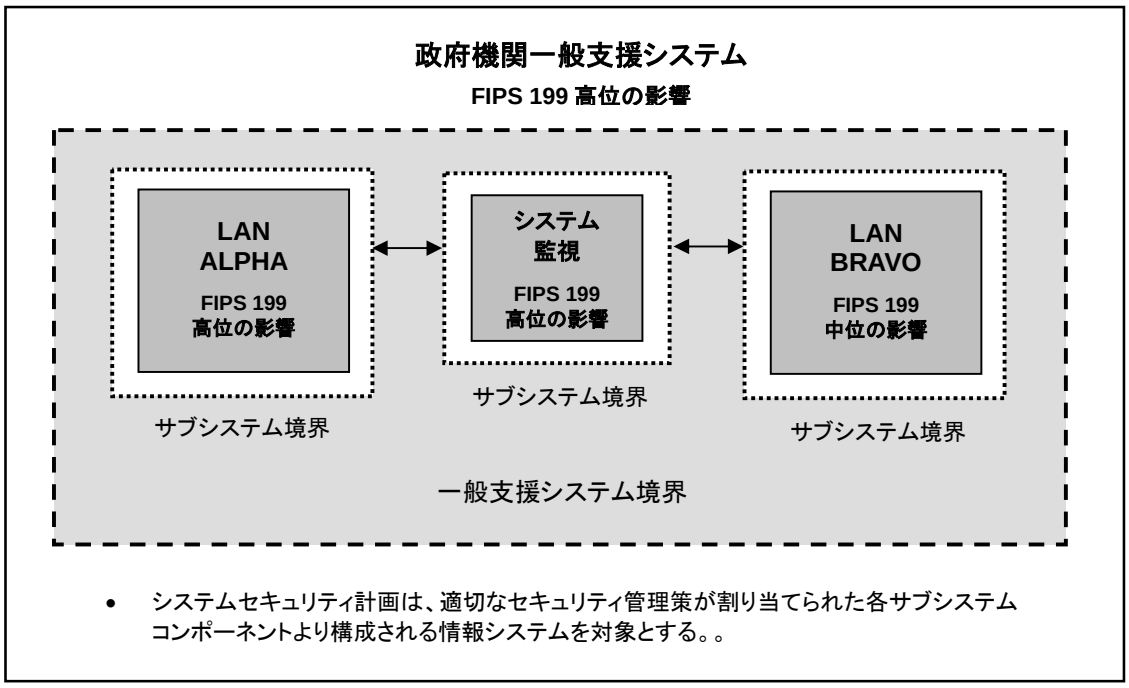

図 3:大規模で複雑な情報システムの構成要素

前述の検討事項は、政府機関が運用認可を目的として情報システムの境界を決定するのに有益な場合もあるが、利用可能な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の境界を設定する際に、政府機関の裁量の余地を制限するものと考えてはならない。運用認可責任者および政府機関の上級情報セキュリティ責任者は、情報システムの境界を設定する際に、将来の情報システムのオーナーと協議すべきである。政府機関の情報システムおよび関連するセキュリティ上の影響に境界を設定するプロセスは、すべての主要な関係者間で慎重な協議を必要とする政府機関レベルの活動であり、政府機関のミッション／業務要件、情報セキュリティに関する技術検討事項、政府機関にかかるプログラムコストを考慮しなければならない。

FIPS 199 は、セキュリティ侵害（機密性、完全性、または可用性の損失）が発生した場合の組織、資産、または個人に対する潜在的影響に基づいて、情報システムに対するセキュリティ分類を定義している。FIPS 199 のセキュリティ分類は、情報および情報システムの重大性つまり機密の高さ、および政府機関のミッションを達成する上でのシステムの重要性に従って政府機関の情報システムを区分することによって、情報システムの境界を定義する際に重要な役割を果たす可能性がある。これは、FIPS 199 で規定するさまざまな影響レベルが 1 つの情報システムに存在する場合に特に重要である。FIPS 199 では、さまざまな影響レベルを持つ非主要アプリケーション／サブシステムを一般支援システムや主要アプリケーションにグループ化する場合、十分な境界保護（例：ファイアウォールや暗号化）が高位の影響レベルを持つサブシステムやアプリケーションの周りに設けられていない限り、その情報システムを最高水準つまり高位の影響レベルに分類するということが規定されている。さらに、共有資源（一般支援システムまたは主要アプリケーション全体で共有するネットワーク、通信、および物理アクセス）は、高位の影響レベルに分類される情報システムとして十分に保護される保証がなければならない。影響の大きいシステムを隔離することにより、システムのセキュリティが高まるだけでなく、そのようなレベルのセキュリ

ティを必要としない多くのアプリケーション／システムを保護するのに必要な資源の量が少なくなる。NIST SP 800-53 は、FIPS 199 の 3 つの影響レベルに関連する 3 つのセキュリティ管理策のベースライン（低位、中位、および高位）を規定している。影響レベルが高くなるにつれて、最低限の保証要件も多くなる。ある情報システムが FIPS 199 のさまざまな影響レベルを持つ場合、報告書（FISMA 年次報告書）上、そのシステムはその情報システムが持つ最高の影響レベルに分類される。

2.2 主要アプリケーション

連邦政府のアプリケーションはすべて価値を有し、一定レベルの保護を必要とする。あるアプリケーションは、含まれる、処理する、蓄積する、または送信する情報のため、あるいは政府機関のミッションに対する重大性のために、管理者による特別の監督を必要とする。これらのアプリケーションが主要アプリケーションである。主要アプリケーションは、FIPS 199 の影響レベルが中位か高位であると考えられる。OMB Circular A-130 は、「主要情報システム」とは、政府機関のミッションにとっての重要性、高額の開発、運用または保守費用、あるいは政府機関のプログラム、財務、資産、またはその他の資源の管理に果たす重要な役割から、管理者による特別な注意を必要とする情報システムであると定義している。主要アプリケーションは、これの定義によれば、主要情報システムである。

主要アプリケーションとは、容易に識別可能なセキュリティ上の考慮事項とニーズが存在する、明確に定義された機能を果たすシステムである（例：電子資金振替決済システム）。主要アプリケーションは、多数の個別プログラムとハードウェア、ソフトウェア、および電気通信コンポーネントから構成される可能性がある。これらのコンポーネントは、特定のミッションに関連する機能のサポートに重点を置いた、単一のソフトウェアアプリケーションまたはハードウェアとソフトウェアの組合せのいずれでもよい。主要アプリケーションはまた、すべてが単一のミッション機能（例：給与計算または人事）に関係する場合は、複数の個別アプリケーションから構成されることもある。システムが主要アプリケーションとして定義され、かつアプリケーションが別の組織の一般支援システム上で実行される場合、主要アプリケーションのオーナーはリスクの受け入れに対する責任とともに、以下の責任を負う。

- 一般支援システムのオーナーに、そのアプリケーションが極めて重要であることを通知し、具体的なセキュリティ要求事項を提供する。

- 主要アプリケーションのシステムセキュリティ計画のコピーを一般支援システムの運用者に提供する。

- 一般支援システムのシステムセキュリティ計画のコピーを要求し、それによってアプリケーションと情報に対する十分な保護が与えられることを確認する。

- 主要アプリケーションのシステムセキュリティ計画の中に、一般支援システムのセキュリティ計画への参照を含める。

2.3 一般支援システム

一般支援システムとは、共通の機能を共有する同一の直接統制管理下にある、一連の相互接続された情報資源である。一般支援システムには通常、ハードウェア、ソフトウェア、情報、データ、アプリケーション、通信、ファシリティ、および人が含まれ、さまざまな利用者および／またはアプリケーションに支援を提供する。一般支援システムの例[11]には、次のものがある。

- 支店をサポートするスマートターミナルを含む LAN
- バックボーン（例：政府機関全体にわたる）
- 通信ネットワーク
- オペレーティングシステムおよびユーティリティを含む政府機関のデータ処理センター
- 戦術的な無線ネットワーク
- 情報処理サービスの共有ファシリティ

一般支援システムのセキュリティ分類は、システムの重大性つまり機密の高さ、および一般支援システムがサポートしている主要アプリケーションによって、FIPS 199 の影響レベルが低位、中位、または高位となる場合がある。一般支援システムは、特別な注意が必要な場合、開発、運用、または保守の費用が高額である場合、およびシステム／情報が政府機関のプログラム管理に重要な役割を担っている場合に主要情報システムと見なされる。一般支援システムが主要情報システムである場合、そのシステムの FIPS 199 の影響レベルは中位または高位である。

主要アプリケーションは、一般支援システムをホストコンピュータにすることができる。一般支援システムの計画は、主要アプリケーションのシステムセキュリティ計画を参照すべきである。

2.4 非主要アプリケーション

政府機関は、そのアプリケーションのどれが非主要アプリケーションであるか、管理者としての判断を行い、非主要アプリケーションのセキュリティ要件が、該当する一般支援システムに対するシステムセキュリティ計画の一部として、場合によっては該当する主要アプリケーションに対するシステムセキュリティ計画の一部として、確実に取り上げられるようにすることを求められている。非主要アプリケーションのセキュリティ管理策の大部分が、その非主要アプリケーションが置かれている一般支援システムか主要アプリケーションから提供されることが一般的である。その場合、一般支援システムか主要アプリケーションの情報システムオーナーが、非主要アプリケーションの情報システムオーナーであり、システムセキュリティ計画の策定に責任を負う。非主要アプリケーション固有の追加セキュリティ管理策は、システムセキュリティ計画の付録またはパラグラフとして文書化すべきである。非主要アプリケーションのオーナー（情報のオーナーと同じことが多い）は、追加した管理策を記述した付録またはパラグラフを作成す

[11] ここに示した例は一般支援システムの一部であり、最終的なリストではない。

ることができる。一般支援システムまたは主要アプリケーションの完全なシステムセキュリティ計画は、情報のオーナーと共有すべきである。

非主要アプリケーションの FIPS 199 セキュリティ分類は、低位または中位である。ただし、十分な境界保護のないシステム上に非主要アプリケーションがある場合、その非主要アプリケーションのホストコンピュータまたは相互接続されたシステムが必要とする最低限のベースライン管理策を導入しなければならない。

2.5 セキュリティ管理策

FIPS 200 は、連邦政府の情報および情報システムに対する 17 項目の最低限のセキュリティ要求事項を規定している。これらの要件は、連邦政府の情報および情報システムの管理、運用、および技術のそれぞれの側面における機密性、完全性、および可用性の保護に関する広範でバランスの取れた情報セキュリティプログラムを示している。政府機関は、NIST SP 800-53 および情報システムの指定された影響レベルに従って選択したセキュリティ管理策を適用することによって、この規格に示される最低限のセキュリティ要求事項を満たさなければならない。政府機関は、この規格に示された条件に従ってその裁量でセキュリティ管理策のベースラインを手直しできる。手直しのための活動には、(i) 詳細調査ガイダンスの適用、(ii) 補完的管理策の規定、および (iii) 許容される場合には、セキュリティ管理策について政府機関が定義するパラメータの規定が含まれる。システムセキュリティ計画の策定に際しては、すべての手直し作業を文書化しておくべきである。

2.5.1 詳細調査ガイダンス

詳細調査ガイダンスによって、NIST SP 800-53 が規定するベースラインセキュリティ管理策における、個々のセキュリティ管理策の適用および導入に関する特定の条件が政府機関に与えられる。次に示すいくつかの考慮事項が、政府機関によるベースラインセキュリティ管理策の適用方法に影響を及ぼす可能性がある。システムセキュリティ計画は、どのセキュリティ管理策が詳細調査ガイダンスを採用したのかを明確化するとともに、検討した考慮事項の種別に関する記述を含むべきである。詳細調査ガイダンスを適用するには、情報システムの運用認可責任者による見直しと承認を受けなければならない。

技術に関連する考慮点—

– 特定の技術（例：無線、暗号技術、公開鍵インフラストラクチャ）を参照するセキュリティ管理策は、情報システム内でこれらの技術を使用している、または使用する必要がある場合にのみ適用できる。

– 最低限のセキュリティ要求事項が対象とするセキュリティ機能を提供する情報システムコンポーネントに対してのみそのセキュリティ管理策が適用できる。

– 自動化メカニズムによって明示的または黙示的にサポートされるセキュリティ管理策では、そのメカニズムがまだ存在しない場合、あるいは市販または政府の既製製品として容易に入手できない場合、そのようなメカニズムを開発する必要はない。自動化メカニズムがすぐには利用できない場合や技術的に実現できない場合、非自動化メカニズムまたは手順によって実施される補完的なセキュリティ管理策を使用して、最低限のセキュリティ要求事項を満たすことになる。

共通セキュリティ管理策に関連する考慮点—

– 政府機関が共通管理策として指定したセキュリティ管理策は、ほとんどの場合、情報システムのオーナー以外の組織内エンティティにより管理される。ベースラインセキュリティ管理策に含まれるすべての管理策は、政府機関が共通セキュリティ管理策により対応するか、情報システムのオーナーが対応しなければならない。ただし、共通管理策の指定に関する判断が、情報システムに対する最低限のセキュリティ要求事項を満たすのに必要なセキュリティ管理策を提供するという政府機関の責任に影響を与えてはならない。（共通管理策に関する追加情報は、第 2.5.3 節にある）

公衆回線を介してアクセスされる情報システムに関連する考慮点—

– 公衆回線を介してアクセスされる情報システムに関連するセキュリティ管理策は、注意深く検討して慎重に適用しなければならない。なぜなら、指定されたセキュリティ管理策のベースラインに含まれるセキュリティ管理策（例：人的セキュリティ管理策、識別および認証の管理策）の中には、公衆回線を介して情報システムにアクセスする利用者には適用されないものがあるためである。[12]

インフラストラクチャに関連する考慮点—

– 政府機関の施設（例：施錠や警備員などの物理的アクセス管理、温度、湿度、照明、火災、電力に対する環境管理）に関するセキュリティ管理策は、施設のうち情報システムを直接保護／サポートするもの、または情報システム（電子メールやウェブサーバ、サーバファーム、データセンター、ネットワークノード、管理されたインタフェース装置、通信装置など、その情報テクノロジ資産を含む）に関連する部分にのみ適用可能である。

[12] 例えば、ベースラインセキュリティ管理策では、公衆回線サービスを提供する情報システムを維持、サポートする組織要員の識別と認証を要求しているが、公衆回線を介してそれらの情報システムにアクセスし一般公開されている情報を入手する利用者には、それと同じ管理策は要求されないことがある。一方、公衆回線を介して情報システムにアクセスし、自分の秘密／個人情報にアクセスする利用者には識別と認証を要求しなければならない。

拡張性に関連する考慮点—

– セキュリティ管理策は、管理策を実施する特定の政府機関の規模や複雑性および情報システムの影響レベルに従って拡張できる。拡張性は、セキュリティ管理策を実施する際の範囲と深さに関するものである。 特定の使用環境にセキュリティ管理策を拡張する際には、費用効率のよい、リスクベースのアプローチによるセキュリティ管理策の実施を確実に行うために、慎重な検討が求められる。[13]

リスクに関連する考慮点—

– 機密性、完全性、または可用性に関するセキュリティ目標に独自に対応するセキュリティ管理策は、より低位のベースライン内の対応する管理策にレベルを下げることが可能である（または、低位のベースラインに定義されていない場合は適宜修正または削除できる）。ただし、レベルを下げる活動が以下の条件を満たす場合に限る。(i) 高位レベル[14]に移る前に、対応する機密性、完全性、または可用性のセキュリティ目標について FIPS 199 のセキュリティ分類と整合していること、(ii) 政府機関のリスクアセスメントの裏付けがあること、および (iii) 情報システム内のセキュリティ関連情報に影響を与えないこと。[15]

2.5.2 補完的管理策

補完的なセキュリティ管理策は、低位、中位、または高位のセキュリティ管理策のベースラインで事前に規定されている管理策の代わりに政府機関が採用する管理的・運用的・技術的管理策であり、情報システムに対して等価または同等の保護を提供するものである。政府機関が情報システムに対して補完的なセキュリティ管理策を採用するのは、次の条件を満たす場合のみである。(i) 政府機関が NIST SP 800-53 のセキュリティ管理策カタログから補完的管理策を選択する (ii) 補完的管理策が、情報システムに対して同等のセキュリティ機能あるいは保護レベルをいかにして提供するかについて、完全で納得できる理論的根拠と正当化できる理由を政府機関が示している (iii) 情報システムに補完的管理策を適用することに伴うリスクを政府機関が評価し、正式に受け入れる。補完的なセキュリティ管理策を使用するにあたっては見直しを行い、システムセキュリティ計画の中で文書化し、情報システムの運用認可責任者による承認を得なければならない。

[13] 例えば、影響レベルが中位または高位の情報システムを持つ大規模かつ複雑な組織では、緊急時対応計画が非常に長くなり、実施に関する大量の詳細な記述をその中に含む場合がある。これとは対照的に、影響レベルが低位の情報システムを持つ小規模な組織の緊急時対応計画は大幅に短くなり、実施に関する詳細記述もはるかに少なくなると考えられる。

[14] 「高位レベル」の概念を採用する場合、いくつかのセキュリティ目標（機密性、完全性、または可用性）の影響レベルが高くなっている可能性がある。そのため、それらのセキュリティ目標に独自に対応するセキュリティ管理策のレベルも同様に引き上げられることになる。したがって、組織は許容できる範囲で適切なレベルの引き下げを行い、費用効率がよくリスクに基づいたセキュリティ管理策を確実に適用するように考慮しなければならない。

[15] システムレベルのセキュリティ関連情報（例：パスワードファイル、ネットワーク経路テーブル、暗号鍵管理情報）は、情報システム内の利用者レベルの情報と区別しなければならない。情報システム内のセキュリティ管理策には、利用者レベルおよびシステムレベル情報の両方に対する機密性と完全性のセキュリティ目標に対応するために使用されるものもある。組織は、機密性または完全性に関するセキュリティ管理策のレベルを下げる場合には、情報システム内のセキュリティ関連情報に影響を与えないように注意しなければならない。

2.5.3 共通セキュリティ管理策

情報セキュリティプログラムを政府機関全体で見渡すと、1 つ以上の政府機関の情報システムに適用できる共通セキュリティ管理策を容易に明確にすることができる。共通セキュリティ管理策は以下のものに適用できる。(i) あらゆる政府機関の情報システム、(ii) 特定サイトの情報システムのグループ（場合によってはサイトの認証／承認という用語に関連）、(iii) 複数の運用サイトに配備された共通の情報システム、サブシステム、またはアプリケーション（共通のハードウェア、ソフトウェア、および／またはファームウェア）（場合によっては種別の認証／承認という用語に関連）。共通セキュリティ管理策は通常、CIO、SAISO、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（共通ハードウェア、ソフトウェア、および／またはファームウェアに対する共通セキュリティ管理策の場合は、開発担当プログラム管理者も）が関与する政府機関全体の共同プロセスの実施中に明確化され、以下の特性を持つ。

- 共通セキュリティ管理策の開発、実施、評価は、政府機関の責任者または組織の部署（その共通セキュリティ管理策を導入または使用するシステムの情報システムのオーナーを除く）に割り当てられる。

- 共通セキュリティ管理策の評価結果は、管理策が適用される政府機関情報システムのセキュリティ承認および運用認可プロセスの裏付けとして使用できる。

情報システムの保護に必要な管理的および運用的管理策（例：緊急時対応計画、インシデント対応、セキュリティの意識向上および訓練、人的セキュリティ、物理的セキュリティの各管理策）の多くは、共通セキュリティ管理策の優れた候補となりうる。その目的は、政府機関が指定した共通セキュリティ管理策の作成、実施、および評価を一元管理し、その後それらの共通セキュリティ管理策が適用される情報システムのオーナーと評価結果を共有することによって、セキュリティコストを削減することである。共通管理策に指定されていないセキュリティ管理策は*システム固有管理策*と考えられ、情報システムのオーナーが責任を負う。システムセキュリティ計画では、どのセキュリティ管理策が共通セキュリティ管理策に指定されているか、どの管理策がシステム固有の管理策に指定されているかを明確に識別すべきである。

システムセキュリティ計画策定の効率を高めるために、共通セキュリティ管理策をいったん文書化した上で、政府機関内の情報システムに対するそれぞれのシステムセキュリティ計画に追記する、あるいは取り込むべきである。セキュリティ計画には、共通管理策の実施に責任を持つ担当者を記載すべきである。システムセキュリティ計画策定プロセスにおいて、共通管理策を最大限効果的に適用できるかどうかは、以下の要因によって決まる。

- 政府機関が共通セキュリティ管理策を明確にするための固有の指針の作成、文書化、および伝達を行っていること。

- 政府機関が、共通セキュリティ管理策の明確化と見直しを調整し、共通管理策の指定について合意を得る責任を、CIO や SAISO など、セキュリティプログラムに責任を持つ管理責任者に対して割り当てていること。

- システム所有者が、共通管理策の使用を含めたシステムセキュリティ計画プロセスの概要の説明を受けたこと。

- プロセスの一部として、明確化された共通管理策分野に関する政府機関内の専門家に助言を得ていること。

また、管理策の一部が共通で他の部分はシステム固有と考えられる場合、政府機関はセキュリティ管理策に複合状態を割り当てることもある。たとえば、IR-1（インシデント対応の方針と手順）のセキュリティ管理策については、方針部分を共通と見なし、手順部分はシステム固有と見なす政府機関があるかもしれない。複合セキュリティ管理策は、管理策をさらに改良するためのテンプレートとしても使用できる。たとえば、ある政府機関では、CP-2（緊急時対応計画）のセキュリティ管理策を、すべての情報システムの一般化した緊急時対応計画のマスターテンプレートとして選択し、個々の情報システムのオーナーが、システム固有の課題に応じてこれを適宜手直しする場合などが考えられる。

政府機関による共通セキュリティ管理策の実施に関連するシステム固有の課題については、すべて情報システムのオーナーが責任を負う。これらの課題は、個々の情報システムに対するシステムセキュリティ計画の中で明確化し記述する。SAISO は CIO に代わり、指定された共通セキュリティ管理策の開発と実施に責任を持つ政府機関の職員（例：施設管理者、拠点管理者、人事管理者）と調整して、必要な管理策を確実に導入し、評価を行い、関係する情報システムのオーナーとの間で評価結果を共有すべきである。

セキュリティ管理策を共通セキュリティ管理策とシステム固有のセキュリティ管理策に分けることは、政府機関における管理策の開発および実施コストの大幅な削減につながる。また、政府機関全体にわたるセキュリティ管理策のより一貫した適用にもつながる。さらに、セキュリティの承認および運用認可プロセスにおいても、同様に大幅なコスト削減を実現できる。すべての情報システムで共通セキュリティ管理策の評価を行うのではなく、政府機関レベルで実施される共通セキュリティ管理策の最新の評価結果の中から、適切なものを承認プロセスに利用することができる。政府機関全体で評価結果を再利用し共有するアプローチによって、政府機関が実施するセキュリティ承認および運用認可の効率を大幅に向上させ、セキュリティプログラムのコストを著しく削減することができる。

セキュリティ管理策を共通セキュリティ管理策とシステム固有の管理策に分けるという概念は単純明快で直観的であるが、政府機関内でこの原理を適用するには計画、調整、そして忍耐が必要である。政府機関がこのアプローチをまさに実施し始めた段階であるか、または部分的にしか実施していない場合、セキュリティ管理の区分やそれに関連する評価結果の再利用から最大の効果を得るまでに、多少の時間を要する可能性がある。政府機関の情報システムの多くが共通セキュリティ管理策に依存する可能性があるので、共通セキュリティ管理策に欠陥があった場合は、これらの管理策に依存するシステムの運用から生ずる政府機関レベルのリスクが著しく増大する恐れがある。

3. 計画の作成

本文書の残りの部分は、システムセキュリティ計画を策定する際の手引きである。その中には、計画の策定に取り組む上で従うべき論理手順、推奨される構成と内容、最新の NIST 文書を最大限に活用してシステムセキュリティ計画策定活動を効果的に支援する方法などが含まれる。この活動を開始する前に、情報システムセキュリティ計画の管理方法やアクセス方法に関する政府機関の方針を確立しておくべきである。

3.1 システムの名称と識別子

システムセキュリティ計画に記述する最初の項目は、システムの名称と識別子である。OMB Circular A-11 が要求しているように、それぞれのシステムに名称と一意の識別子を割り当てることにより、政府機関は、政府機関に関する情報およびシステムに固有のセキュリティ尺度を容易に収集することができるようになるだけでなく、システムの実装と性能に関するすべての要件の完全な追跡を容易に行うことができるようになる。この識別子は、システムが存続する間は変更せず、システムの使用に関する監査ログにも（システムの識別子として）記載すべきである。

3.2 システムの分類

政府機関のシステム資産目録で識別される各システムは、FIPS 199 を使用して分類しなければならない。
199. NIST Special Publication 800-60、*Guide for Mapping Types of Information and Information Systems to Security Categories* は、この活動を完了するための実施上の指針を規定している。
FIPS 199 による分類のまとめは表 1 を参照されたい。

3.3 システムのオーナー

各システムのシステムセキュリティ計画では、指定されたシステムオーナーを明確にしなければならない。システムオーナーは、システムの主要連絡先（POC）であり、システム固有のシステム開発ライフサイクル（SDLC）に関する活動をを調整する責任を負う。システムオーナーは、システムの能力および機能について専門的知識を持っていることが重要である。システムオーナーの割り当ては書面に文書化すべきであり、計画には以下の連絡先情報を含めるべきである。

- 名前
- 役職
- 政府機関
- 住所
- 電話番号
- 電子メールアドレス

	潜在的影響		
セキュリティ目的	低位	中位	高位
機密性 しかるべき承認を受けて情報へのアクセスと開示に対して制限を設けること。これには、個人のプライバシーと機密情報の保護手段が含まれる。 [44 U.S.C., Sec. 3542]	情報の不当な開示が、組織活動、組織資産、または個人に**限定的な**悪影響を及ぼすことが予想されうる。	情報の不当な開示が、組織活動、組織資産、または個人に**重大な**悪影響を及ぼすことが予想されうる。	情報の不当な開示が、組織活動、組織資産、または個人に**致命的または壊滅的な**悪影響を及ぼすことが予想されうる。
完全性 不適切な情報改変または破壊から情報を保護すること。これには情報の否認防止および真正性の保証が含まれる。 [44 U.S.C., Sec. 3542]	情報の不当な改変または破壊が、組織活動、組織資産、または個人に**限定的な**悪影響を及ぼすことが予想されうる。	情報の不当な改変または破壊が、組織活動、組織資産、または個人に**重大な**悪影響を及ぼすことが予想されうる。	情報の不当な改変または破壊が、組織活動、組織資産、または個人に**致命的または壊滅的な**悪影響を及ぼすことが予想されうる。
可用性 タイムリーかつ信頼性の高い方法で情報にアクセスでき、利用できることを保証すること。 [44 U.S.C., Sec. 3542]	情報または情報システムへのアクセスまたは利用の妨害が、組織活動、組織資産、または個人に**限定的な**悪影響を及ぼすことが予想されうる。	情報または情報システムへのアクセスまたは利用の妨害が、組織活動、組織資産、または個人に**重大な**悪影響を及ぼすことが予想されうる。	情報または情報システムへのアクセスまたは利用の妨害が、組織活動、組織資産、または個人に**致命的または壊滅的な**悪影響を及ぼすことが予想されうる。

表 1：FIPS 199 による分類

3.4 運用認可責任者

各システムに対するシステムセキュリティ計画では、運用認可責任者を明確にしなければならない。運用認可責任者は、情報システム（主要アプリケーションまたは一般支援システム）の運用を認可し、システムに関連する未解決のリスクを受け入れる権限を持つ上級管理責任者である。運用認可責任者の割り当ては文書化すべきであり、計画には第 3.3 節での記載と同じ連絡先情報を含めなければならない。

3.5 その他の指定連絡先

このセクションには、システムの特性や操作に関する問い合わせに対応できる、他の主要連絡先担当者の名前を含めるべきである。このセクションに記載する各担当者について、第 3.3 節での記載と同じ情報を含めるべきである。

3.6 セキュリティに対する責任の割り当て

政府機関内で、それぞれのシステムに責任を持つ担当者を割り当てなければならない。この割り当てには、さまざまな方法がある。政府機関によっては、SAISO に全面的な責任を委任することも考えられる。SAISO が、各主要コンポーネントに割り当てられたセキュリティ責任者のサブネットから支援を受けることもよくある。これらのセキュリティ責任者に、その権限の範囲内のすべてのシステムに対するセキュリティ要求事項に対処する権限を与えてもよい。それ以外に、この責任を政府機関の構成と職責に基づくという方法で割当てるモデルも考えられる。それらの担当者についても、第 3.3 節での記載と同じ連絡先情報を提供すべきである。最も重要な点は、この責任を職員の職位記述書か委任覚書のいずれかに、書面で正式に記述しておくことである。

3.7 システムの運用状態

システムの運用状態を、下記のうちの 1 つかそれ以上を用いて表示する。2 つ以上の状態が選択されている場合は、システムのどの部分がどの状態にあるのかを記述する。

- *運用中*－システムは実働中である。
- *開発中*－システムは設計、開発、または導入中である。
- *大規模な修正の実施中*－システムは大規模な改造または移行を実施中である。

システムが開発中または大規模な修正を実施中である場合には、当面のセキュリティ要求事項が確実に含まれるようにするために、使用した方法に関する情報を記載する。システムがセキュリティライフサイクルのどこにあるのかに応じて、計画の対応する節に具体的な管理策を含める。

3.8 情報システムの種別

計画のこの節で、システムが主要アプリケーションなのか一般支援システムなのかを示す。システムに非主要アプリケーションが含まれている場合、計画の「概説／目的」節でそれらについて記述する。政府機関に情報システム種別のその他の分類がある場合は、テンプレートを修正して他の分類を含める。

3.9 概要／目的

システムの機能と目的に関する簡単な記述（1～3 パラグラフ）を用意する（例：経済指標、政府機関に対するネットワークサポート、ビジネス調査データ分析、作柄報告支援）。

システムが一般支援システムの場合は、一般支援システムによってサポートされるすべてのアプリケーションを列挙する。アプリケーションが主要アプリケーションであるかないかを明記し、該当する場合は一意の名称／識別子を含める。各アプリケーションの機能および処理する情報を記述する。利用者組織がシステム所有者の政府機関の内部か外部かにかかわらず、その一覧を含める。

3.10 システム環境

技術的なシステムの簡単な（1～3 パラグラフ）概要を記載する。パーソナルデジタルアシスタント（PDA）や無線技術の使用など、特別なセキュリティ問題を引き起こす環境要因または技術要因を含める。通常、運用環境には以下のものがある。

- **スタンドアロンまたはスモールオフィス／ホームオフィス（SOHO）環境**は、家庭向けまたは業務目的で使用される小規模で非公式なコンピュータ施設のことである。スタンドアロンには、ラップトップ、モバイル装置、ホームコンピュータから、在宅勤務システム、小規模企業、および企業の小規模な支店まで、各種の小規模な環境や装置が含まれる。

- **管理された環境またはエンタープライズ環境**は通常、定義され体系化された一連のハードウェアおよびソフトウェア構成を持つ、大規模な政府機関システムである。この環境は、一元管理されるワークステーションやサーバから構成されるのが一般的であり、ファイアウォールやその他のネットワークセキュリティ装置によってインターネットから保護されている。

- **カスタム環境**には、セキュリティの機能や程度が他の環境と適合しないシステムが含まれる。カスタム環境の代表的なものには、**セキュリティ制約のある特殊機能環境とレガシー環境**の 2 つがある。

  -- **セキュリティ制約のある特殊機能環境** セキュリティ制約がある特殊機能環境には、攻撃やデータ露出のリスクが高く、機能よりもセキュリティが優先されるシステムやネットワークが含まれる。これは、大きな脅威にさらされる環境で、システムが限定的または特殊な（汎用的なワークステーションやシステムではなく）機能を持つことを想定している。そのようなシステムには、外部に面したファイアウォールや公開ウェブサーバのようなシステム、あるいはデータの内容やミッションの目的が極めて重要であるために、他の有益なシステム属性(レガシーアプリケーションや他のシステムとの相互運用性など)にマイナスの影響が及ぶ可能性があっても、セキュリティを積極的に優先させるトレードオフが勝るシステムがある。セキュリティ制約がある特殊機能環境は、他の環境のサブセットとなる場合もある。

  -- **レガシー環境** レガシー環境は、過去の安全性の低い通信メカニズムを利用している可能性がある、旧来のシステムまたはアプリケーションが含まれる。レガシー環境で運用する他のマシンでは、セキュリティの設定を緩和して、レガシーシステムやアプリケーションと通信できるようにしなければならない場合がある。レガシー環境は、スタンドアロン環境または管理された環境のサブセットになる場合がある。[16]

[16] システム環境の詳しい説明については、NIST Special Publication 800-70、*Security Configuration Checklists Program for IT Products -- Guidance for Checklists Users and Developers*（*IT 製品のためのセキュリティ設定チェックリストプログラム - チェックリスト利用者と開発者のための手引き)*を参照されたい。

3.11 システム相互接続／情報共有

システム相互接続とは、情報資源の共有を目的とした 2 つ以上の IT システムの直接接続である。システム相互接続が適切に保護されなければ、接続されたすべてのシステムおよびそれらが蓄積、処理、または送信するデータが危険にさらされる結果となる可能性がある。システム相互接続および情報共有に関連する脆弱性について、システム所有者、情報所有者、および管理者ができるだけ多くの情報を入手することが重要である。これは、そのような脆弱性を軽減するのに必要な適切な管理策を選択する上で不可欠である。異なる組織が所有または運用するデータを共有するシステムの間（ワークステーション／デスクトップまたは公衆回線を介してアクセスされるシステムの間ではなく）で相互接続セキュリティ協定（ISA）、了解事項覚書（MOU）、または合意事項覚書（MOA）を取り交わす必要がある。政府機関が、セキュリティ要求事項への適合を保証する承認と署名を必要とする厳密なシステム開発ライフサイクルを管理し実施する場合、ISA は内部の政府機関システムには必要ない。相互接続に関する追加情報は、NIST SP 800-47、*Security Guide for Interconnecting Information Technology Systems（情報システムの相互接続に関するセキュリティガイド）*を参照されたい。

この節では、異なる組織が所有または運用するシステム間の***相互接続ごと***に、他のシステムとの接続または情報共有の認可に関する以下の情報を記述する。

- システムの名称
- 組織
- 相互接続種別（インターネット、ダイヤルアップなど）
- 相互接続の認可（MOU/MOA、ISA）
- 合意日付
- FIPS 199 による分類
- システムの承認および運用認可の状況
- 運用認可責任者の名前と役職

相互接続の多い政府機関では、上記の情報を含む表形式にするのが望ましい情報の表示方法である場合がある。

3.12 システムに影響する法律、規程、および政策

システム、およびシステムが保持、伝送、または処理する情報の機密性、完全性、または可用性に対する具体的な要求事項を確立した法律、規程、または政策をすべて列挙する。政府機関の一般的なセキュリティ要求事項は、すべてのシステムに対するセキュリティを義務付けるものなので、列挙する必要はない。各政府機関は、システムセキュリティ計画に含める法律、規程、および政策のレベルを決定すべきである。例として、1974 年施行のプライバシー保護法や、処理する情報（例：税または国勢調査情報）に関する特定の法律または規程がある。システムがプライバシー保護法に従って記録を処理する場合は、プライバシー保護法の記録システムの番号と表題、およびそのシステムがコンピュータマッチングアクティビティに使用されるかどうかを含める。

3.13 セキュリティ管理策の選択

適用可能なセキュリティ管理策のベースライン（影響レベルが低位、中位、または高位の情報システム）に対する NIST SP 800-53 セキュリティ管理策の実施方法、または実施の計画方法を文書化する準備として、ベースラインに含まれるセキュリティ管理策を見直し、場合によっては手直しすべきである。個々の管理策の適用性の判断または手直しには、第 2.5.1 節で説明した詳細調査ガイドラインを使用すべきである。さらに、多数のシステムまたはその政府機関全体に共通する管理策を明確化した上で、計画の中で文書化すべきである。共有管理策の決定、文書化、および調整の方法に関する指針は、第 2.5.3 節を参照されたい。*十分なセキュリティ*[17]を達成するために、適切なセキュリティ管理策を選択して詳細調査ガイダンスを適用するプロセスは、政府機関内の管理者および運用要員が関与する多角的かつリスクに基づく活動であり、計画のセキュリティ管理策部分を記述する前に実施すべきである。

– *影響レベルが低位*の情報システムでは、政府機関は、最低限の管理策として NIST SP 800-53 で定義されているセキュリティ管理策の低位ベースラインからセキュリティ管理策を採用しなければならない。また、低位ベースラインに伴う最低限の保証要件を確実に満たさなければならない。

– *影響レベルが中位*の情報システムで、政府機関は、最低限の管理策として NIST SP 800-53 で定義されているセキュリティ管理策の中位ベースラインからセキュリティ管理策を採用しなければならない。また、中位ベースラインに伴う最低限の保証要件を確実に満たさなければならない。

– *影響レベルが高位*の情報システムでは、政府機関は、最低限の管理策として NIST SP 800-53 で定義されているセキュリティ管理策の高位ベースラインからセキュリティ管理策を採用しなければならない。また、高位ベースラインに伴う最低限の保証要件を確実に満たさなければならない。

3.14 最低限のセキュリティ管理策

ここまででセキュリティ管理策を選択、手直しし、共通管理策を明確にしたので、それぞれの管理策について記述する。記述には、1) セキュリティ管理策の表題、2) セキュリティ管理策の実施方法または実施計画の方法、3) 適用した詳細調査ガイダンスおよび考慮点の種別を含め、4) セキュリティ管理策が共通管理策であるか、管理策の実施責任者は誰であるかを示すべきである。

[17] 行政管理予算局（OMB） Circular A-130 付録 III では、十分なセキュリティとは、情報の損失、誤用、または情報への不当なアクセスや改変によって発生するリスクと損害の大きさに見合ったセキュリティであると定義されている。

セキュリティ管理策カタログ（NIST SP 800-53 付録 F）に示すセキュリティ管理策は、その分類と構成が明確に定義されている。セキュリティ管理策は、管理策の選択および特定を行うプロセスで簡単に使用できるようにクラスおよびファミリに分類されている。セキュリティ管理策には 3 つの一般的クラス（管理、運用、技術[18]）がある。各ファミリには、ファミリのセキュリティ機能と関連するセキュリティ管理策が含まれる。各管理策ファミリを一意に識別するために、標準化された 2 文字の識別子が割り当てられている。表 2 にセキュリティ管理策カタログにおけるクラスとファミリ、および対応するファミリ識別子を示す。

クラス	ファミリ	識別子
管理	リスクアセスメント	RA
管理	計画	PL
管理	システムおよびサービスの調達	SA
管理	承認、運用認可、およびセキュリティ評価	CA
運用	人的セキュリティ	PS
運用	物理的および環境的な保護	PE
運用	緊急時対応計画	CP
運用	構成管理	CM
運用	保守	MA
運用	システムおよび情報の完全性	SI
運用	記録媒体の保護	MP
運用	インシデント対応	IR
運用	意識向上およびトレーニング	AT
技術	識別および認証	IA
技術	アクセス制御	AC
技術	監査および責任追跡性	AU
技術	システムおよび通信の保護	SC

表 2：セキュリティ管理策のクラス、ファミリ、および識別子

システムセキュリティ計画を準備するために、次にセキュリティ管理クラスの指定（管理、運用、技術）を分かりやすく定義する。

管理的管理策は、情報システムの管理およびシステムに対するリスクの管理に重点を置いたものである。これは通常、管理者が対処する技法や懸念事項である。***運用的管理策***は、主に、人により（システムによってではなく）導入され、実行されるメカニズムに重点を置くセキュリティの方法をいう。この管理策は、特定のシステム（またはシステムのグループ）のセキュリティを改善するために設けられる。これは技術的または特化された専門知識を必要とすることが多く、技術的管理策だけでなく管理者の行動にしばしば依存する。***技術的管理策***は、コンピュータシステムが実行するセキュリティ管理策に重点を置いたも

[18] NIST SP 800-53 に示すセキュリティ管理策ファミリは、3 つのセキュリティ管理策クラス（管理、運用、技術）のいずれか 1 つと関連付けられている。ファミリは、そのファミリに含まれる管理策の主な特性に対応するクラスに割り当てられる。しかし、セキュリティ管理策の多くは論理的に複数のクラスに関連付けることができる。例えば、緊急時対応計画に含まれる方針および手順の管理策である CP-1 のクラスは、運用に分類されているが、セキュリティ管理とも矛盾しない特性を持つ。

のである。この管理策によって、許可されていないアクセスや誤用に対する自動化された保護が提供され、セキュリティ違反の検出が容易になり、アプリケーションおよびデータに対するセキュリティ要件がサポートされる。

3.15 完了日および承認日

システムセキュリティ計画の完了日を記入すべきである。完了日は、計画を定期的に見直して更新するたびに更新すべきである。システムを更新する場合は、バージョン番号を追加すべきである。システムセキュリティ計画には、運用認可責任者または指定運用認可承認者がその計画を承認した日付も含めるべきである。承認文書（承認書、承認覚書）は、ファイルに記録するか、計画の一部として添付すべきである。

3.16 システムセキュリティ計画の継続的保守

情報システムセキュリティ計画の作成後、計画を定期的に評価するとともに、システムの状態、機能、設計などに関するあらゆる変更を見直して、システムに関する正しい情報が確実に計画に反映され続けることが重要である。この文書とその正確さは、システム承認活動にとって極めて重要である。必要であれば、少なくとも年 1 回はすべての計画を見直して更新すべきである。見直し対象の事項には以下のものが考えられる。

- 情報システムオーナーの変更
- 情報セキュリティ担当者の変更
- システムアーキテクチャの変更
- システム状態の変更
- システム相互接続の追加／削除
- システム適用範囲の変更
- 運用認可責任者の変更
- 承認および運用認可状態の変更

付録 A：情報システムセキュリティ計画のサンプルテンプレート

以下のサンプルは例としてのみ提供するものである。政府機関が他の形式を使用し、本指針にない部分を反映させてそれを更新することを選択してもよい。これは必須の形式ではない。多数の政府機関および情報セキュリティサービスプロバイダが、情報システムセキュリティ計画の策定と提示のためにさまざまなアプローチを整備して実施し、柔軟性に対する独自のニーズに合わせることもあると理解している。

情報システムセキュリティ計画のテンプレート

1. **情報システムの名称／表題**:
   - システムに割り当てられた一意の識別子および名称。

2. **情報システムの分類**:
   - FIPS 199 による適切な分類を識別する。

	低位		**中位**		**高位**

3. **情報システムのオーナー**:
   - システムのオーナーである担当者の名前、役職、政府機関、住所、電子メールアドレス、および電話番号。

4. **運用認可責任者**:
   - 運用認可責任者として指名されている上級管理責任者の名前、役職、政府機関、住所、電子メールアドレス、および電話番号。

5. **その他の指定連絡先**:
   - 必要な場合、その他の主な担当者の役職、住所、電子メールアドレス、電話番号などを列挙する。

6. **セキュリティに対する責任の割り当て**:
   - システムのセキュリティに対する責任を負う担当者の名前、役職、住所、電子メールアドレス、および電話番号。

7. **情報システムの運用状態**:
   - システムの運用状態を示す。2 つ以上の状態が選択されている場合は、システムのどの部分がどの状態にあるのかを記述する。

	運用中		**開発中**		**大規模な 修正中**

8. **情報システム種別**:
   - システムが主要アプリケーションか一般支援システムかを示す。システムに非主要アプリケーションが含まれる場合は、それを第 9 節「システムの概要／目的」に列挙する。

	主要アプリケーション		**一般支援 システム**

9. システムの概要／目的

- システムおよび情報処理の機能または目的を記述する。

10. システム環境

- 技術的なシステムの概要を記述する。主なハードウェア、ソフトウェア、および通信機器を含める。

11. システム相互接続／情報共有

- 相互接続されるシステムとシステム識別子（必要な場合）を列挙し、システム、名称、組織、システム種別（主要アプリケーションまたは一般支援システム）を示すとともに、ISA/MOU/MOA がファイルに記録されているかどうか、相互接続に合意した日付、FIPS 199 による分類、C&A の状態、および認可責任者の名前を示す。

システムの名称	組織	種別	合意（ISA/MOU/MOA）	日付	FIPS 199 による分類	C&A の状態	運用認可責任者

12. 関連する法律／規程／政策

- システム内のデータの機密性、完全性、または可用性に対する具体的な要求事項を定めた法律または規程をすべて列挙する。

13. 最低限のセキュリティ管理策

NIST SP 800-53 から該当する最低限のセキュリティ管理策ベースライン（低位、中位、高位の影響レベル）を選択した上で、適用可能なベースラインに含まれる最低限のセキュリティ管理策のすべての実施方法または実施計画の方法を詳細に記述する。この記述には以下の情報を盛り込むべきである。1) セキュリティ管理策の表題、2) セキュリティ管理策の実施方法または実施計画の方法、3) 適用した詳細調査ガイダンスおよび考慮点の種別、および 4) セキュリティ管理策が共通管理策であるか、管理策の実施責任者は誰であるかの記述。

14. 情報システムセキュリティ計画の完了日： _____

- 計画の完了日を記入する。

15. 情報システムセキュリティ計画の承認日：_____

- システムセキュリティ計画が承認された日付を記入し、承認文書が添付またはファイルに記録されているかどうかを示す。

付録 B:用語集

一般的な用語と定義

運用認可 (Accreditation) [NIST SP 800-37]	政府機関の上級責任者が与える公式の管理者意思決定。情報システムの運用を認可し、政府機関の活動(ミッション、機能、イメージ、または評判など)、政府機関の資産、または担当者に対するリスクを合意済みのセキュリティ管理策の集合体の導入に基づいて明示的に受け入れる。
認可び境界 (Accreditation Boundary) [NIST SP 800-37]	運用認可責任者が認可する、情報システムのすべてのコンポーネント。ただし、情報システムが接続されていて単独で認可を受けるシステムは除く。CNSS 指示 4009、および中央情報長官指令(DCID)6/3 に定義されている用語「セキュリティ境界(security perimeter)」と同義。
運用認可権限者 (Accrediting Authority)	運用認可責任者(Authorizing Official)を参照。
十分なセキュリティ (Adequate Security) [OMB Circular A-130、付録 III]	情報の損失、誤用、または不当なアクセスや改変によるリスクおよび損害の大きさに見合ったセキュリティ。
政府機関 (Agency)	執行機関(Executive Agency)を参照。
認証 (Authentication)	利用者、プロセス、または装置の識別情報を検証すること。多くの場合、情報システム内の資源へのアクセスを許可するための必要条件となる。
真正性 (Authenticity)	真正のものであり、検証が可能で、信頼できるという特性。送信、メッセージまたはメッセージの発信者の有効性に対する信頼。認証(Authentication)を参照。
認可手続き (Authorize Processing)	運用認可(Accreditation)を参照。
運用認可責任者 (Authorizing Official) [NIST SP 800-37]	政府機関の活動(ミッション、機能、イメージ、または評判など)、政府機関の資産または担当者に対して、許容可能なレベルのリスクで情報システムを運用する責任を公式に負う権限を持つ責任者。
可用性 (Availability) [44 U.S.C., Sec. 3542]	タイムリーかつ信頼性の高い方法で情報にアクセスでき、利用できることを保証すること。

承認 (Certification) [NIST SP 800-37]	情報システムでの管理的、運用的、および技術的なセキュリティ管理策に対する包括的な評価。システムに対するセキュリティ要求事項を満たすという観点から、管理策が正しく導入され、意図したとおりに運用され、期待した効果が上げられているかの度合いを判断し、セキュリティ承認を裏付ける。
承認代行者 (Certification Agent) [NIST SP 800-37]	セキュリティ承認の実施に責任を持つ担当者、グループ、または組織。
最高情報責任者 (Chief Information Officer) [44 U.S.C., Sec. 5125(b)]	以下に対して責任を持つ政府機関の職員。 (i) 執行機関の長および政府機関のその他の上級管理要員に助言やその他の援助を提供し、情報技術が獲得され、情報資源が法律、大統領行政命令、大統領令、政策、規定、および政府機関の長が定めた優先順位に従って管理されていることを確認する。 (ii) 政府機関に対する妥当で統合された情報技術のアーキテクチャを開発、保守し、その実現を容易にする。 (iii) 政府機関の作業プロセスの改善など、政府機関のすべての主要な情報資源管理プロセスの効果的かつ効率的な設計と運用を推進する。
共通セキュリティ管理策 (Common Security Control) [NIST SP 800-37]	1 つ以上の政府機関の情報システムに適用可能なセキュリティ管理策。以下の特性を持つ。(i) 管理策の開発、導入、および評価を責任者または組織の要素（情報システム所有者を除く）に割り当て、(ii) 管理策の評価結果を使用して、管理策を適用する政府機関の情報システムのセキュリティ承認および運用認可プロセスを支援する。
補完的セキュリティ管理策 (Compensating Security Controls)	NIST SP 800-53 に記述された低、中、高位のベースラインでの推奨管理策の代わりに組織が採用する、管理的・運用的・技術的管理策（保護手段または対抗策）。情報システムに対して同等または同程度の保護を提供する。
機密性 (Confidentiality) [44 U.S.C., Sec. 3542]	しかるべき承認を受けて情報へのアクセスと開示に対して制限を設けること。これには、個人のプライバシーと機密情報の保護手段が含まれる。

構成管理 (Configuration Control) [CNSS Inst. 4009]	ハードウェア、ファームウェア、ソフトウェアおよび資料に対する改変を管理するプロセス。システムの導入前、導入中、および導入後の不適切な改変から情報システムを確実に保護する。
対抗策 (Countermeasures) [CNSS Inst. 4009]	情報システムの脆弱性を低減する活動、装置、手順、手法、その他の手段。セキュリティ管理策（security control）および保護手段（safeguard）と同義。
執行機関 (Executive Agency) [41 U.S.C., Sec. 403]	5 U.S.C., Section 101 で特定されている行政機関、5 U.S.C., Section 102 で特定されている軍事機関、5 U.S.C., Section 104(1)で定義されている独立（行政）組織、および、31 U.S.C., Chapter 91 の規定に完全に準拠する100%政府所有の企業。
連邦エンタープライズアーキテクチャ (Federal Enterprise Architecture) [FEA Program Management Office]	政府全体の向上を目指して行政管理予算局が開発した、ビジネスに基づく枠組み。連邦政府を国民主体、成果重視、市場を基盤としたものに転換に対する取り組みを促進するもの。
連邦情報システム (Federal Information System) [40 U.S.C., Sec. 11331]	執行機関、執行機関の請負業者、または執行機関に代わるその他の組織によって使用または運用されている情報システム。
一般支援システム (General Support System) [OMB Circular A-130、付録 III]	共通の機能を共有する同じ直接統制管理下にある、相互接続された情報資源の集合体。通常、ハードウェア、ソフトウェア、情報、データ、アプリケーション、通信、および人を含む。
影響レベル高のシステム (High-Impact System)	セキュリティ目標（機密性、完全性、可用性）の少なくとも 1 つに対して FIPS 199 の潜在的影響レベル「高」が設定されている情報システム。
情報のオーナー (Information Owner) [CNSS Inst. 4009]	特定の情報に対する法的または運用上の権限、ならびに情報の生成、収集、処理、配信、および廃棄の管理策を確立する責任を有する職員。
情報資源 (Information Resources) [44 U.S.C., Sec. 3502]	要員、装置、資金、情報技術などの、情報および関連する資源。

情報セキュリティ (Information Security) [44 U.S.C., Sec. 3542]	機密性、完全性、可用性を提供するための、不当なアクセス、使用、開示、妨害、改変、あるいは破壊に対する、情報および情報システムの保護。
情報セキュリティポリシー (Information Security Policy) [CNSS Inst. 4009]	組織が情報を管理、保護、および配布する方法を規定する、指令、規定、規則、慣例などを集めたもの。
情報システム (Information System) [44 U.S.C., Sec. 3502] [OMB Circular A-130、付録 III]	情報の収集、処理、保守、利用、共有、配信、廃棄のために統合された、情報資源の独立した集合体。
情報システムのオーナー (Information System Owner) （またはプログラムマネージャ (Program Manager)） [CNSS Inst. 4009、改訂]	情報システムの総合的な調達、開発、統合、改変、または運用と保守の責任者。
情報システム セキュリティ責任者 (Information System Security Officer) [CNSS Inst. 4009、改訂]	政府機関の上級情報セキュリティ責任者、認可責任者、管理責任者、または情報システム所有者から、情報システムまたはプログラムに対する適切な運用上のセキュリティポリシーを確保する責任を与えられた担当者。
情報技術 (Information Technology) [40 U.S.C., Sec. 1401]	執行機関による、データまたは情報の自動的な取得、保存、操作、管理、移動、制御、表示、切り換え、交換、送信、受信に用いられる、あらゆる装置あるいは相互接続された装置のシステムまたはサブシステム。装置は、前文の目的で、執行機関が直接使用するか、あるいは以下の条件で執行機関と請負契約を結んだ請負企業が使用する。その条件とは、(i) そのような装置を使用する必要がある場合、または (ii) サービスの提供または製品の供給時にかなりの度合いでそのような装置を使用する必要がある場合。情報技術という用語には、コンピュータ、補助装置、ソフトウェア、ファームウェアおよび類似の手順、サービス（サポートサービスを含む）、および関連する資源が含まれる。

情報タイプ (Information Type) [FIPS 199]	組織によって、あるいは場合により特定の法律、大統領行政命令、大統領令、政策、または規定によって定義された、情報の特定のカテゴリ（例：プライバシー、医療、知財、財務、調査、契約者機密、セキュリティ管理）。
完全性 (Integrity) [44 U.S.C., Sec. 3542]	不適切な情報改変または破壊から情報を保護すること。これには情報の否認防止および真正性の保証が含まれる。
ラベル (Label)	セキュリティラベル（Security Label）を参照。
影響レベル低のシステム (Low-Impact System)	3 つのセキュリティ目標（機密性、完全性、可用性）のすべてに対して FIPS 199 の潜在的影響レベル「低」が設定されている情報システム。
主要アプリケーション (Major Application) [OMB Circular A-130、付録 III]	アプリケーション内の情報の損失、誤用、または不当なアクセスや改変によるリスクおよび損害の大きさのために、セキュリティに対する特別な注意が必要なアプリケーション。注：連邦のアプリケーションはすべて一定のレベルの保護を必要とする。ただし、含まれる情報によっては、特別な管理監督を必要とし、主要アプリケーションとみなされるべきものもある。その他のアプリケーションには、それを運用するシステムが十分なセキュリティを提供すべきである。
主要情報システム (Major Information System) [OMB Circular A-130]	政府機関のミッションにとっての重要性、高額な開発、運用、保守費用、または政府機関のプログラム、財務、資産、その他の資源の管理に果たす重要な役割から、管理者による特別な注意が必要な情報システム。
管理的管理策 (Management Controls) [NIST SP 800-18]	リスク管理と情報システムセキュリティ管理に重点を置いた情報システムに適用されるセキュリティ管理策（保護手段と対抗策）。
MAC アドレス (Media Access Control Address)	IEEE 802 に基づく、ネットワーク上の各コンポーネントを一意に識別するハードウェアアドレス。IEEE802 標準には準拠せず OSI 参照モデルに準拠するネットワーク上では、ノードアドレスをデータリンク制御（DLC）アドレスと呼ぶ。
非主要アプリケーション (Minor Application)	主要アプリケーション以外のアプリケーションで、その内の情報の損失、誤用、または不当なアクセスや改変によるリスクおよび損害の大きさのために、セキュリティに対する特別な注意が必要なアプリケーション。非主要アプリケーションは通常、一般支援システムの一部として含まれる。
モバイルコード (Mobile Code)	遠隔情報システムから取得するか、ネットワークを横切って送信され、受信者が明示的にインストールまたは実行することなくローカル情報システム上で実行されるソフトウェアプログラムまたはその一部。

モバイルコード技術 (Mobile Code Technologies)	モバイルコードを生成、使用するためのメカニズムを提供するソフトウェア技術（例：Java、JavaScript、ActiveX、VBScript）。
影響レベル中のシステム (Moderate-Impact System)	セキュリティ目標（機密性、完全性、可用性）の少なくとも 1 つに対して FIPS 199 の潜在的影響レベル「中」が設定され、どのセキュリティ目標に対しても「高」が設定されていない情報システム。
国家安全保障緊急時対応電気通信サービス (National Security Emergency Preparedness Telecommunications Services) [47 C.F.R., Part 64, AppA]	準備状態を維持するため、あるいは、国民に対する傷害または損害、資産の損害または喪失を引き起こす、あるいは合衆国の国家安全保障または緊急時対応体制を悪化させるまたは脅かす、あるいはその恐れがあるあらゆる事象や危機（地域内、国家的、または国際的なもの）への対処・管理を行うために使用される電気通信サービス。
国家安全保障に関わる情報 (National Security Information)	大統領行政命令第 13292 号によって修正された大統領行政命令第 12958 号、またはそれ以前のすべての命令、または 1954 年の原子力法修正条項に従って、不当な開示に対する保護が必要であると判断され、その機密状態を示す表示のある情報。
国家安全保障に関わるシステム (National Security System) [44 U.S.C., Sec. 3542]	政府機関または政府機関の請負企業、または政府機関に代わる他の組織が使用または運用する、以下の特徴を有する（あらゆる電気通信システムを含む）情報システムのすべて。(i) その機能、運用、あるいは利用が、情報収集活動、国家安全保障に関連する暗号作成活動、軍隊の指揮統制、武器および武器システムに不可欠な部分となっている装置に関わるか、あるいは、軍事または情報収集業務の直接的遂行にとって極めて重要なもの（ただし、たとえば給与計算、財務、物流、人事管理アプリケーションなど、日常の管理業務やビジネスのアプリケーションに用いられるようなシステムは除く）あるいは、(ii) 大統領行政命令または議会立法によって制定された基準のもとに、国防または外交政策上機密にすべきであることが特に許可された情報に対して確立された手順により常に保護がなされるもの。
否認防止 (Non-repudiation) [CNSS Inst. 4009]	情報の送信者には配達証明が、受信者には送信者の識別情報が提供されたという保証。これによって、送信者と受信者のいずれも後日情報を処理したことを否認できない。
運用的管理策 (Operational Controls) [NIST SP 800-18]	主に、人により（システムによってではなく）導入され実行される情報システムに適用されるセキュリティ管理策（保護手段と対抗策）。

行動計画およびマイルストーン (Plan of Action and Milestones) [OMB Memorandum 02-01]	達成する必要がある任務を明確化する文書。計画の要素を達成するために必要な資源、任務を達成するためのマイルストーン、およびそのための完了予定日程を詳細に記述する。
潜在的影響 (Potential Impact) [FIPS 199]	機密性、完全性、または可用性の損失によって、(i) 限定的な悪影響（FIPS 199 影響レベル低）、(ii) 重大な悪影響（FIPS 199 影響レベル中）、(iii) 致命的または壊滅的な悪影響（FIPS 199 影響レベル高）が、組織の運営、組織の資産、または個人に生じると予想される。
プライバシー影響評価 (Privacy Impact Assessment) [OMB Memorandum 03-22]	以下の目的のために情報がどのように扱われるかの分析。(i) 取り扱い方法が、プライバシーに関して準拠すべき法律、規定、および政策の要件に適合していることを確認すること、(ii) 電子情報システム内で情報を識別可能な形で取得、保守、および配布することのリスクと影響を判断すること、および (iii) プライバシーに対する潜在リスクを軽減するための保護と情報を処理する代替プロセスを検討し評価すること。
保護配送システム (Protective Distribution System)	十分な保護手段や対抗策（例：音響的、電気的、電磁的、物理的）を備え、暗号化されていない情報の送信に使用できるワイヤーラインまたは光ファイバーシステム。
記録 (Records)	実施したアクティビティまたは得られた結果の確証（例：書類、報告、テスト結果）を記録すること。組織および情報システムが意図したとおりに機能していることを検証する際の基礎となる。また、関連するデータフィールド（プログラムがアクセスできる、特定の項目についての完全な情報の集合体を含むデータフィールドのグループ）内の構成単位を参照するためにも用いられる。
リモートアクセス (Remote Access)	情報システムセキュリティ境界の外部と通信する利用者（または情報システム）によるアクセス。
遠隔保守 (Remote Maintenance)	情報システムセキュリティ境界の外部と通信する担当者が行う保守アクティビティ。
リスク (Risk) [NIST SP 800-30]	脅威の潜在的影響および脅威が発生する可能性を前提として、情報システムの運用によってもたらされる政府機関の運営（ミッション、機能、イメージ、または評判など）、政府機関の資産、または担当者に対する影響レベル。

リスクアセスメント (Risk Assessment) [NIST SP 800-30]	政府機関の活動（ミッション、機能、イメージ、または評判を含む）、政府機関の資産、または個人に対するリスクを特定し、発生確率、もたらされる影響、およびこの影響を軽減する追加的なセキュリティ管理策を判断するプロセス。リスクマネジメント（Risk Management）の一部であり、リスク分析（Risk Analysis）と同義である。脅威分析および脆弱性分析を含む。
リスクマネジメント (Risk Management) [NIST SP 800-30]	情報システムの運用による、政府機関の活動（ミッション、機能、イメージ、または評判を含む）、政府機関の資産、または個人に対するリスクを管理するプロセス。これには、リスクアセスメント、費用対効果分析、セキュリティ管理策の選択、実施、評価、およびシステム運用のための正式認可が含まれる。このプロセスでは、有効性、効率、および法律、大統領令、政策、または規定による制約を考慮する。
保護手段 (Safeguards) [CNSS Inst. 4009、改訂]	情報システムに対して定められたセキュリティ要求事項（機密性、完全性、可用性）を満たすために規定された保護手段。保護手段には、セキュリティ機能、管理上の制約、人的セキュリティ、ならびに物理的構造、領域、および装置のセキュリティなどが含まれる場合がある。セキュリティ管理策（Security Controls）および対抗策（Countermeasures）と同義。
サニタイズ (Sanitization) [CNSS Inst. 4009、改訂]	情報を復旧できないように記録媒体から削除するプロセス。すべてのラベル、マーク、活動ログを削除する作業が含まれる。
詳細調査ガイダンス (Scoping Guidance)	管理策ベースライン内の個々のセキュリティ管理策の適用範囲と導入について、技術、基盤、外部アクセス、拡張性、共通セキュリティ管理策、およびリスクに関する具体的な考慮点を組織に提供する。
セキュリティ分類 (Security Category) [FIPS 199]	情報または情報システムの機密性、完全性、または可用性の損失が組織活動、組織資産、または個人に及ぼす潜在的影響の評価に基づく、情報または情報システムの特性付け。
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、可用性を保護するために、情報システムに対し規定された統制・運用・技術管理（保護手段または対抗策）。
セキュリティ管理策ベースライン (Security Control Baseline)	影響レベル低、影響レベル中、および影響レベル高の情報システムに対して定義された最低限のセキュリティ管理策の集合体。
セキュリティ管理強化 (Security Control Enhancements)	(i) 基本管理策に付加的な関連機能を組み込む、および (ii) 基本管理策を強化する、またはどちらか一方のセキュリティ機能のステートメント。

セキュリティ影響分析 (Security Impact Analysis) [NIST SP 800-37]	政府機関の職員が実施する分析で、多くの場合セキュリティ承認および運用認可プロセスの継続的監視段階で、情報システムの変更がシステムのセキュリティ状態に与える影響の度合いを判断する。
セキュリティラベル (Security Label)	情報システムに関連するデータ構造または出力媒体への明示的または黙示的なマーク付け。マークには、FIPS 199 セキュリティ分類、あるいはその中に含まれる情報の配布制限や取り扱いに関する警告を示す。
セキュリティ目的 (Security Objective)	機密性、完全性、または可用性。
セキュリティ境界 (Security Perimeter)	運用認可境界（Accreditation Boundary）を参照。
セキュリティ計画 (Security Plan)	システムセキュリティ計画（System Security Plan）を参照。
セキュリティ要求事項 (Security Requirements)	処理、保存、または伝送される情報の機密性、完全性、および可用性を確保するための法律、大統領行政命令、大統領令、政策、指示、規定、または組織（ミッション）の必要性に由来する、情報システムに課される要件。
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 に定められた最高情報責任者の責務を遂行し、最高情報責任者から政府機関の認可責任者、情報システム所有者、および情報システムセキュリティ責任者への連絡役を務める責任者。
スパイウェア (Spyware)	情報システムに秘密裏かつ不正にインストールされ、個人または組織に知られずにその情報を収集するソフトウェア。
サブシステム (Subsystem)	情報、情報技術、および 1 つ以上の特定の機能を実行する要員からなる、情報システムの主要な下位区分またはコンポーネント。
システム (System)	情報システム（Information System）を参照。
システム固有セキュリティ管理策 (System-specific Security Control) [NIST SP 800-37]	情報システムに対するセキュリティ管理策のうち、共通セキュリティ管理策に指定されていないもの。
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件の概要と、これらの要件を満たすために設置済みまたは設置が計画されているセキュリティ管理策について記述した公式の文書。

技術的管理策 (Technical Controls) [NIST SP 800-18]	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含まれるメカニズムにより、主に情報システムにより導入および実行される、情報システムに対するセキュリティ管理策（保護手段と対抗策）。
脅威 (Threat) [CNSS Inst. 4009、改訂]	不当なアクセス、破壊、開示、改変、および／またはサービス妨害によって、情報システムを介して政府機関の活動（ミッション、機能、イメージ、または評判を含む）、政府機関の資産、または担当者に悪影響を及ぼす可能性のあるあらゆる状況または事象。
脅威要因／脅威源 (Threat Agent/Source) [NIST SP 800-30]	(i) 脆弱性を故意に悪用することを目指す意図および手法、あるいは (ii) 脆弱性が偶発的に衝かれる状況および手法、のいずれか。
脅威のアセスメント (Threat Assessment) [CNSS Inst. 4009]	情報システムに対する脅威の形式的な記述およびアセスメント。
高信頼経路 (Trusted Path)	システムセキュリティポリシーをサポートするのに必要な信頼性を備え、利用者が（入力装置を介して）情報システムのセキュリティ機能と直接通信できるメカニズム。このメカニズムは、利用者または情報システムのセキュリティ機能のみが有効化でき、信頼できないソフトウェアはこれをまねることができない。
利用者 (User) [CNSS Inst. 4009]	情報システムへのアクセスが許可されている担当者または（システム）プロセス。
脆弱性 (Vulnerability) [CNSS Inst. 4009、改訂]	脅威源によってつけこまれるか衝かれるおそれがある情報システム、システムセキュリティの手順、内部制御、または導入での弱点。
脆弱性アセスメント (Vulnerability Assessment) [CNSS Inst. 4009]	情報システムにおける脆弱性の形式的な記述および評価。

付録 C:参考文献

Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems,* December 2003.

Federal Information Processing Standards Publication 200, *Security Controls for Federal Information System*, (projected for publication February 2006).

Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.

National Institute of Standards and Technology Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.

National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005.

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

National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

National Institute of Standards and Technology Special Publication 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle*, June 2004.

National Institute of Standards and Technology Special Publication 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005.

National Institute of Standards and Technology Special Publication 800-70, *Security Configuration Checklists Program for IT Products -- Guidance for Checklists Users and Developers*, May 2005.

Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.