FIPS PUB 200

Federal Information Processing Standards Publication (連邦情報処理規格)

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

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

2006 年 3 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

独立行政法人 情報処理推進機構
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

NRI SECURE TECHNOLOGIES

まえがき

米国国立標準技術研究所（National Institute of Standards and Technology 、以下、NISTと称す) FIPS PUB シリーズ（Federal Information Processing Standards Publication: 連邦情報処理規格、以下 FIPS と称す）は、Federal Information Security Management Act of 2002 (2002年施行の連邦情報セキュリティマネジメント法)の規定のもとに採択され公布される、公式の規格文書シリーズである。本 FIPS PUB に対するコメントを歓迎する。コメントは、「Director, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900」宛に送付されたい。

-- CITA M. FURLANI, ACTING DIRECTOR
INFORMATION TECHNOLOGY LABORATORY

本文書は、原典に沿ってできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありません。翻訳監修主体は本文書に記載されている情報より生じる損失または損害に対して、いかなる人物あるいは団体にも責任を負うものではありません。

作成機関

FIPS PUB シリーズは、Information Technology Management Reform Act of 1996 (1996 年施行の情報技術マネジメント改革法)(Public Law 104-106) の第 5131 条および Federal Information Security Management Act of 2002 (2002 年施行の連邦情報セキュリティマネジメント法) (Public Law 107-347) に従って、商務長官の承認を受けた後、NIST によって発行される。

FIPS PUB 200

2006 年 3 月 9 日

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のための規格の公布について

FIPS PUB シリーズは、Federal Information Security Management Act of 2002 (2002 年施行の連邦情報セキュリティマネジメント法)に従って、商務長官の承認を受けた後、NIST によって発行される。

1. 規格の名称

FIPS Publication 200 (以下、FIPS PUB 200 と称す):*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*

2. 規格の分類

情報セキュリティ

3. 概要

第 107 回連邦議会を通過し、2002 年 12 月に大統領の署名により法律として成立した E-Government Act of 2002 (2002 年施行の電子政府法) (Public Law 107-347) は、米国の経済および国家安全保障における情報セキュリティの重要性を認めたものである。E-Government Act の第 III 編である Federal Information Security Management Act (連邦情報セキュリティマネジメント法、以下 FISMA と称す) は、各連邦政府において連邦政府の業務と情報資産を支援する情報および情報システムにセキュリティを提供するための組織横断的なプログラムを開発し、文書化し、導入する必要性を強調している。これらの情報および情報システムは、他の連邦政府、委託先、またはそれ以外の関係者によって提供または管理されるものを含む。FISMA は、次の連邦規格を公布することを命じている。(i) リスクレベルに基づいた適切なレベルの情報セキュリティを提供するために、連邦政府の情報および情報システムをセキュリティ分類するための規格 (ii) (i)の規格に従って分類された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関する規格。 本規格は、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ついて述べたものである。

4. 承認者

商務省長官

5. 維持管理機関

商務省、NIST 情報技術ラボラトリ

6. 適用範囲

本規格は、(i) 連邦政府内のすべての情報、但し、Executive Order 13292 (大統領令 13292) により改正された Executive Order 12958 (大統領令 12958)、またはそれ以前のすべての命令、あるいは Atomic Energy Act of 1954 (1954 年施行の原子力法。その改正を含む) に準拠して、不当な開示からの保護を必要とすることが決定され、機密扱いとすることを示すためのマーク付けが行われた情報を除く、ならびに (ii) 44 United States Code Section 3542(b)(2) に定義された国家的セキュリティシステムに指定された情報システム以外のすべての連邦情報システムに適用すべきものである。本規格は、国家的セキュリティシステムのための同様の規格を補完するために技術的視野に立って開発されたものである。連邦政府機関はもとより、州、地方政府および部族政府、合衆国の重要インフラを構成する民間部門の組織も、これら規格を適宜使用することが推奨される。

7. 仕様

FIPS PUB 200:*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*

8. 導入

本規格は、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ついて、17 のセキュリティ関連分野にわたり規定したものである。連邦政府機関は、NIST の 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）の最新版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、本規格で規定された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。

9. 発効日

本規格は直ちに発効する。連邦政府機関は、発効日から 1 年以内に本規格に準拠することとする。

10. 留意事項

NIST Special Publication 800-53 で定義されたセキュリティ管理策を用いることは、本規格の要求事項であり、それにより、情報システムに対し最先端の予防手段と対抗策を導入することになる。SP800-53 のセキュリティ管理策は、最低でも 1 年に 1 度は NIST によって見直しされ、(i) 管理策を導入することによって得た経験 (ii) 連邦政府機関におけるセキュリティ要求事項に対する変化 (iii) 利用可能な新たなセキュリティ技術 を反映して、適宜、改正および拡張が行われる。低位、中位および高位に定義された最低限のセキュリティ管理策のベースライン（基準値）も、時間の経過や、セキュリティレベルの上昇、連邦政府機関内でリスクを緩和するための最適慣行の変化に従って変更されることが予想される。セキュリティ管理策のカタログに対する追加、削除または修正案や、NIST Special Publication 800-53 のセキュリティ管理策のベースラインに対する変更案は、厳格な公的検討のプロセスにより、政府や民間の意見を得て、変更に対する合意が形成される。連邦政府機関は、その変更に全面的に準拠するまでに、最終公布日から 1 年を上限とする期間が与えられるが、準拠するための行動にすぐにとりかかることが推奨される。

11. 免責事項

商務省長官によって FIPS への準拠は必須と定められており、それを猶予するいかなる条項も FISMA では規定していない。

12. 規格の入手について

本規格は、NIST コンピュータセキュリティ部門のウェブサイト http://csrc.NIST.gov/publications より入手可能である。

目次

1. 目的

第 107 回連邦議会を通過し、2002 年 12 月に大統領の署名により法律として成立した E-Government Act of 2002 (2002 年施行の電子政府法) (Public Law 107-347) は、米国の経済および国家安全保障における情報セキュリティの重要性を認めたものである。E-Government Act の第 III 編である FISMA は、NIST に対して、以下の開発を含め、規格とガイドラインの策定に関する責務を課すものである。

- リスクレベルに基づいた適切なレベルの情報セキュリティを提供するために、連邦政府機関により、または連邦政府機関のために、収集、維持されるすべての情報および情報システム[1]を分類する際に使用すべき規格
- 各分類に含めるべき情報および情報システムのタイプに関するガイドライン
- 上記の各分類の情報および情報システムに対する最低限の情報セキュリティ要求事項 (例えば、管理的、運用的、技術的管理策など)

2004 年の 2 月に商務省の長官によって承認された FIPS PUB 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) は、FISMA[2]が規定する 2 つの必須のセキュリティ規格のうち最初に策定されたものである。必須のセキュリティ規格の 2 番目となる FIPS PUB 200 は、連邦政府の執行機関を支援する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とそれを満たすために必要な管理策をリスクに応じて選択するプロセスについて規定している。本規格は、情報セキュリティのための最低限の最適慣行レベルを設定することにより、連邦政府機関内で、さらに安全な情報システムを開発し、導入し、運用することを促進する。また、最低限のセキュリティ要求事項に合致する、情報システムに対するセキュリティ管理策を選択し、特定する際に、一貫性があり、他に勝るとも劣らない、反復可能なアプローチを提供する。

2. 情報システムの影響レベル

FIPS PUB 199 では政府機関に対し、セキュリティ目的である機密性、完全性および可用性それぞれに対する影響レベルを低位、中位あるいは高位として自らの情報システムを分類することを求めている。それぞれのセキュリティ目的に対して割り当てられた潜在的影響値は、これらの情報システムに格納された情報それぞれに対し割り当てられたセキュリティ分類のうち最高値 (高水準マーク[3]) となる[4]。情報システムのセキュリティ分類 (SC: Security Category) を表す一般的な形式は以下のとおりである。

$$SC_{\text{情報システム}} = \{(\textbf{機密性}, \textit{影響}), (\textbf{完全性}, \textit{影響}), (\textbf{可用性}, \textit{影響})\}$$

ここで、潜在的な影響の許容値は、「低位」、「中位」、「高位」である。

ある情報システムに対する機密性、完全性および可用性の潜在的影響値は、常に同じではないことがあるため、その情報システムの全体的な影響レベルを判断するためには、高水準マークの考え方が用いられなければならない。従って、*影響レベルが低位であるシステム*では、3 つのセキュリティ目的に対する影響レベルはすべて低位である。*影響レベルが中位であるシステム*では、3 つのセキュリティ目的に対する影響レベルの少なくとも 1 つは中位であり、中位以上の影響値を示すセキュリティ目的は存在しない。そして*影響レベルが高位であるシステム*では、セキュリティ目的に対する影響レベルの少なくとも 1 つが高位である。情報システムの影響レベルに関する判断は、最低限のセキュリティ要求事項を検討し、情報システムに対して適切なセキュリティ管理策を選択する前に完了していなければならない。

---

1 情報システムとは、情報の収集、処理、維持、利用、共有、配布または廃棄のために体系化された情報資源それぞれの独立した集合である。情報資源には、情報および人員、設備、資金、情報技術などの情報に関連する資源が含まれる。

2 本文書で参照している NIST のセキュリティ規格およびガイドラインは、http://csrc.NIST.gov から入手可能である。

3 高水準マークの考え方は、セキュリティ目的である機密性、完全性および可用性の間に重要な依存性があるために採用される。多くの場合、1つのセキュリティ目的を侵害することは、最終的にこれ以外のセキュリティ目的にも影響を及ぼすためである。

4 800-60、Guide for Mapping types of Information and Information Systems to Security Categories (情報および情報システムのタイプとセキュリティ分類のマッピングガイド) は、情報および情報システムに対しセキュリティ分類を割り付ける際の導入ガイダンスを提供するものである。

3. 最低限のセキュリティ要求事項

最低限のセキュリティ要求事項は、連邦情報システムの機密性、完全性および可用性を保護し、これらのシステムによって処理、格納および発信される情報に関する 17 のセキュリティ関連分野を網羅している。セキュリティ関連分野には次のような内容が含まれる。 (i) アクセス制御 (ii) 意識向上およびトレーニング (iii) 監査および責任追跡性 (iv) 承認、認可およびセキュリティ評価 (v) 構成管理 (vi) 緊急時対応計画 (vii) 識別および認証 (viii) インシデント対応 (ix) 保守 (x) 記録媒体の保護 (xi) 物理的および環境的な保護 (xii) 計画 (xiii) 人的セキュリティ (xiv) リスクアセスメント (xv) システムおよびサービスの調達 (xvi) システムおよび通信の保護 (xvii) システムおよび情報の完全性。この 17 の分野は、連邦政府の情報および情報システムの管理、運用および技術面を扱い、情報セキュリティプログラムが広範で、バランスの取れた状態であることを表している。

ポリシーや手順は、情報セキュリティプログラムを連邦政府の組織全体に効果的に導入し、連邦政府の情報および情報システムを保護するために採用されたセキュリティ管理策が成功するための重要な役割を果たしている。従って、組織は、本規格に示す最低限のセキュリティ要求事項を統制するために正式に文書化されたポリシーと手続きを作成、配布し、それらの導入が効果的であることを確実にしなければならない。

最低限のセキュリティ要求事項の詳細

アクセス管理 (AC: Access Control)：組織は、権限を付与されたユーザーや権限を付与されたユーザーのために代行するプロセスの情報システムへのアクセスを制限するとともに、デバイス (他の情報システムを含む) や権限を付与されたユーザーに実行が許可されるトランザクション (処理) と機能の種類についても制限しなければならない。

意識向上およびトレーニング (AT: Awareness and Training)：組織は、次の 2 項目を確実に行わなければならない。
(i) 組織の情報システムの管理者やユーザーに対し、自らの活動に関連するセキュリティリスクと組織の情報システムのセキュリティに関して適用される法律、大統領令、指令、方針、規格、指示、規定または手順を認識させること。
(ii)組織の人員に対し、その担当する情報セキュリティ関連の任務や責任を果たすための適切な訓練を施すこと。

監査および責任追跡性 (AU: Audit and Accountability)：組織は、次の 2 項目を確実に行わなければならない。
(i) 非合法的／不正または不適切な情報システムの活動を監視、分析、調査および報告するために必要な情報システムの監査記録が作成され、保護および維持されていること。
(ii) それぞれの情報システムのユーザー活動の一意的な追跡を可能にすることにより、ユーザー自らの活動に対する説明責任を持つことができること。

承認、認可およびセキュリティ評価 (CA: Certification, Accreditation and Security Assessments)：組織は、次の 4 項目を確実に行わなければならない。
(i) 組織の情報システムのセキュリティ管理策を定期的に評価し、その管理策が自らのアプリケーションにとって効果的であることを判断すること。
(ii) 組織の情報システムの欠陥の修正と脆弱性の削減または解消のための活動計画を作成し導入すること。
(iii) 組織の情報システムの運用とその他の関連情報システムとの接続を承認すること。
(iv) 情報システムのセキュリティ管理策を継続的に監視することにより、その管理策を継続的に有効にすること。

構成管理 (CM: Configuration Management)：組織は、次の 2 項目を確実に行わなければならない。
(i) 組織の情報システム (ハードウェア、ソフトウェア、ファームウェアおよびその文書化を含む) の基本的な構成とその一覧表をそれぞれのシステム開発のライフサイクル全体について設定し、維持すること。
(ii) 組織の情報システムに採用されている情報技術製品のセキュリティ構成を設定し、実行すること。

緊急時対応計画 (CP: Contingency Planning)： 組織は、緊急時における対応、バックアップオペレーションや組織の情報システムの災害後の復旧計画を作成、維持し、効果的に導入し、緊急事態における重要な情報資源や継続的なオペレーションの可用性を確保しなければならない。

識別および認証 (IA: Identification and Authentication)：組織は、組織の情報システムへアクセスを許可する前提条件として、情報システムのユーザー、ユーザーを代行する手順またはデバイスを識別し、認証しなければならない。

インシデント対応（IR: Incident Response）：組織は、次の 2 項目を確実に行わなければならない。
(i) 適切な準備、検知、分析、隔離、回復およびユーザーの対応活動を含む組織の情報システムのインシデント対応運用能力を構築すること。
(ii) インシデントを追跡し、文書化したものを適切な組織の関係者および／または承認権限のある者に報告すること。

保守（MA: Maintenance）：組織は、次の 2 項目を確実に行わなければならない。
(i) 組織の情報システムに対する定期的かつタイムリーな保守を実施すること。
(ii) 情報システムの保守を実行するために用いるツール、技術、メカニズムや人員の効果的な管理を整備すること。

記録媒体の保護（MP: Media Protection）：組織は、次の 3 項目を確実に行わなければならない。
(i) 紙と電子ベース双方の情報システムの媒体を保護すること。
(ii) 情報および情報システムの媒体への承認されたユーザーのアクセスを制限すること。
(iii) 情報システムの媒体を廃棄または再利用する前に、その内容を完全に消去または物理的に破壊すること。

物理的および環境的保護（PE: Physical and Environmental Protection）：組織は、次の 5 項目を確実に行わなければならない。
(i) 承認された個人に対し、情報システム、設備とそれぞれのオペレーション環境への物理的なアクセスを制限すること。
(ii) 物理的な施設を保護し、情報システムのためのインフラを維持すること。
(iii) 情報システムの支援ユーティリティを整備すること。
(iv) 環境的な危険から情報システムを保護すること。
(v) 情報システムが含まれる設備に適切な環境的管理を整備すること。

計画（PL: Planning）：組織は、セキュリティ計画を作成し、文書化し、定期的な更新を行い、その計画を導入しなければならない。また、その計画には、組織の情報システムに対する既存または、計画中のセキュリティ管理策と情報システムにアクセスする個人の行動規範が記載されていること。

人的セキュリティ（PS: Personnel Security）：組織は、次の 3 項目を確実に行わなければならない。
(i) 組織内で責任のある地位を与えられている個人（関係機関のサービスプロバイダを含む）が、信頼のおける人物であり、その地位について設定されたセキュリティ基準を満たしていること。
(ii) 解雇または、異動などの人事的措置中またはその措置の完了後の組織の情報や情報システムが保護されていること。
(iii) 組織のセキュリティ方針や、手順に順守できなかった人員に対する正式な罰則が採用されていること。

リスクアセスメント（RA: Risk Assessment）：組織は、組織の情報システムのオペレーションや組織情報の関連処理、格納または発信が組織のオペレーション（任務、機能、印象または、評判を含む）にもたらすリスクを定期的に評価しなければならない。

システムおよびサービスの調達（SA: System and Services Acquisition）：組織は、次の 3 項目を確実に行わなければならない。
(i) 組織の情報システムを適切に保護するために、十分な資源を割り当てること。
(ii) 情報セキュリティの検討事項を盛り込んだシステム開発のライフサイクルを採用すること。
(iii) ソフトウェアの利用や、設定の制限を設けること。
(iv) 組織が外部委託する際の情報、アプリケーションおよび／またはサービスを保護するために、外注先のプロバイダが適切なセキュリティ対策を行っていること。

システムおよび通信の保護（SC: System and Communications Protection）：組織は、次の 2 項目を確実に行わなければならない。
(i) 情報システムの外部との境界および、主要な内部との境界における組織的な通信（例：組織の情報システムによって発信または、受信した情報）を監視、管理および保護すること。
(ii) 組織の情報システムにおける効果的な情報セキュリティを促進する構造設計、ソフトウェア開発技術とシステムエンジニアリングの原則を採用すること。

システムおよび情報の完全性（SI: System and Information integrity）：組織は、次の 3 項目を確実に行わなければならない。
(i) 情報や情報システムの欠陥をタイムリーに特定し、報告および訂正すること。
(ii) 組織の情報システムの適切な箇所に悪質なプログラムからの保護策を備えること。
(iii) 情報システムのセキュリティ警告やアドバイザリを監視し、それに対応する適切な活動を行うこと。

4. セキュリティ管理策の選択

組織は、NIST の Special Publication 800-53 "*Recommended Security Controls for Federal Information Systems*（連邦政府の情報システムのための推奨セキュリティ管理策[5]）"に記載の適切なセキュリティ管理策と保証要求事項を選択することにより、本規格におけ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。組織の情報システムに対し、*適切なセキュリティ*[6]を構築するための適切なセキュリティ管理策および保証要求事項の選択プロセスは、マネジメントや組織内のオペレーションに携わる人員が関与するリスクに基づいた多角的な活動である。FIPS PUB 199 に規定されているように、連邦政府の情報および情報システムのセキュリティ分類は、リスク管理プロセス[7]の第一段階である。セキュリティ分類のプロセスに続き、組織は、本規格が示す最低限のセキュリティ要求事項を満たすように、自らの情報システムに対し適切なセキュリティ管理策を選択しなければならない。選択されたセキュリティ管理策セットは、セキュリティ分類のプロセスで組織の情報システムに割り付けられた影響レベルと関連づけられ、NIST Special Publication 800-53 のセキュリティ管理策のベースライン（基準値）を自らの組織の情報システムにあわせて調整したうえで[8]、次の 3 つの影響レベルのうちの 1 つを含まなければならない。

— *影響レベルが低位である情報システム*では、組織は、最低限、NIST Special Publication 80-53 において定義された低位ベースラインのセキュリティ管理策を採用し、それを自組織の情報システムにあわせて調整し、低位ベースラインの最低限の保証要求事項を確実に満たすようにしなければならない。

— *影響レベルが中位である情報システム*では、組織は、最低限、NIST Special Publication 800-53 において定義された中位ベースラインのセキュリティ管理策を採用し、それを自組織の情報システムにあわせて調整し、中位ベースラインの最低限の保証要求事項を確実に満たすようにしなければならない。

— *影響レベルが高位である情報システム*では、組織は、最低限、NIST Special Publication 800-53 において定義された高位ベースラインのセキュリティ管理策を採用し、それを自組織の情報システムにあわせて調整し、高位ベースラインの最低限の保証要求事項を確実に満たすようにしなければならない。

組織は、それぞれのベースラインにおけるすべてのセキュリティ管理策を採用しなければならない。但し、特例として、NIST の Special Publication 800-53 に記載された調整のためのガイダンスに基づき許可された場合を除く。

組織全体の適切なセキュリティを構築するための費用対効果の高い、リスクに基づいた取り組みを確実にするために、セキュリティベースラインを調整する活動は、組織の適切な関係者によって統制され、承認されなければならない（適切な関係者の例として、chief information officers（最高情報責任者）、senior agency information security officers（政府機関情報セキュリティ局高官）、authorizing officials（承認権限者）または、authorizing officials designated representatives（承認権限者が指定する代表者）などが挙げられる）。このような調整の結果採用されたセキュリティ管理策は、情報システムのセキュリティ計画として文書化されなければならない。

[5] 組織は、セキュリティ管理策の選択プロセスにおいて、NIST Special Publication 800-53 の改訂に応じ、その最新版を使用しなければならない。
[6] The Office of Management and Budget (OMB) Circular A-130（行政管理予算局通達 A-130）付録第 III 編では、「適切なセキュリティ」を情報の消失、不正使用、不正アクセスまたは改ざんがもたらすリスクや、損害の大きさに見合ったセキュリティとして定義している。
[7] セキュリティの分類は、chief information officer（最高情報責任者）、senior agency information security officers（政府機関情報セキュリティ局高官）、authorizing officials（承認権限者）（accreditation authorities（認可権限者）とも呼ばれる）、information system owners（情報システムの所有者）や、information owners（情報の所有者）を含み、かつこれに限らず senior-level organizational officials（上級レベルの組織関係者）が関与する企業全体の活動として達成されなければならない。
[8] セキュリティベースラインの調整のためのガイダンスは、NIST Special Publication 800-53 に規定されている。

付録 A: 用語および定義

認可 (ACCREDITATION) : 情報システムの運用認可、および、合意したセキュリティ管理策の導入における政府機関のオペレーション (任務、機能、印象あるいは評判を含む) や、政府機関の資産または個人に対するリスクの明示的な受容に関する政府機関の上級管理者による公式的判断。

適切なセキュリティ (ADEQUATE SECURITY) : 情報の消失、不正使用、不正アクセス、改ざんがもたらすリスクや損害に見合ったセキュリティ。[行政管理予算局通達 A-130、付録第 III 編]

政府機関 (AGENCY) : (i) 政府説明責任局 (ii) 連邦選挙管理委員会 (iii) コロンビア特別区の政府や米国の領土や所有区およびその一区画または (iv) 国防に関する調査や製品の製造に従事する研究機関など政府が所有し、契約者によって運営される設備を除くすべての執行部門、軍事部門、政府関連法人、政府管理法人、これ以外の政府の行政府 (大統領の執務室を含む) または独立調整機関。[44 U.S.C., SEC. 3502]

認証 (AUTHENTICATION) : 多くの場合、情報システムにおける情報源へのアクセスを許可するための前提条件となる、ユーザー、プロセス、デバイスの識別情報の確認。

認可権限者 (AUTHORIZING OFFICIAL) : 政府機関のオペレーション (任務、機能、印象または、評判を含む) や、政府機関の資産または個人に対するリスクを受容し、情報システムの運用認可に公式の責任を負う、認可権限を持つ官吏。*同義語として Accreditation Authority (認可権限者) がある。*

可用性 (Availability) : 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]

承認 (CERTIFICATION) セキュリティ認可を支援するために作成された、情報システムの管理的、運用的、技術的管理策の総合的評価。セキュリティ管理策が正しく導入されているか、意図された通りの運用であるか、そのシステムに対するセキュリティ要求事項に合致する期待通りの成果が上がっているか、という点に関し、その達成度を判断する。

最高情報責任者 (CHIEF INFORMATION OFFICER) : とは、次の 3 項目に責任を負う政府機関の関係者である。(i) 執行機関の上官や、政府機関のそれ以外の上級管理者に対する勧告や支援を提供し、法律、大統領令、指令、方針、規定および政府機関の上官によって制定された優先順位に準拠する方法で情報技術が調達され、情報源が管理されていること; (ii) 政府機関にとって健全かつ完全な情報技術アーキテクチャーを開発し、維持管理し、その導入を促進すること、および; (iii) 作業プロセスの向上などを含む、政府機関のすべての重要な情報資源を管理するプロセスの効果的かつ有効な設計およびオペレーションの推進。[44 U.S.C., SEC.5125 (b)]

最高情報セキュリティ責任者 (CHIEF INFORMATION SECURITY OFFICER) : 政府機関情報セキュリティ局高官 (Senior Agency Information Security Officer) の項参照。[44 U.S.C., SEC.3542]

機密性 (CONFIDENTIALITY) : 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]

対抗策 (COUNTERMEASURES) : 情報システムの脆弱性を削減するための活動、デバイス、手順、技術またはこれ以外の手段。[CNSS Instruction 4009]*セキュリティ管理策 (Security Control) や予防手段 (Safeguards) と同義。*

環境 (ENVIRONMENT) : 情報システムの開発、オペレーションおよびメンテナンスに影響を及ぼす外部的な手順、条件および目的。[CNSS Instruction 4009]

執行機関 (EXECUTIVE AGENCY) : 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。[41 U.S.C., SEC. 403]

連邦政府機関 (FEDERAL AGENCY) : 政府機関の項参照。

連邦情報システム (FEDERAL INFORMATION SYSTEM) : 執行機関、執行機関の請負企業、または執行機関に代わるその他の組織によって執行機関のために使用または運用されている情報システム。[40 U.S.C., SEC. 11331]

影響レベルが高位であるシステム (HIGH-IMPACT SYSTEM) : 最低でも1つのセキュリティ目的 (例: 機密性、完全性または可用性) における影響レベルが、FIPS PUB 199 の潜在的影響値の高位を示す情報システム。

インシデント (INCIDENT) : 情報システムの機密性、完全性または可用性あるいはシステムが処理、格納または発信する情報を、実際もしくは潜在的に危険におとしめる事象。あるいはセキュリティ方針、セキュリティ手順、利用が容認できる方針の侵害または侵害に差し迫る脅威を構成する事象。

情報 (INFORMATION) : 情報タイプの実体。[FIPS Publication 199]

情報の所有者 (INFORMATION OWNER) : 特定の情報に関する制定法または運用に関する権限および情報の生成、収集、処理、普及や廃棄に関する統制を整備する責任が伴う関係者。[CNSS Instruction 4009]

情報資源 (INFORMATION RESOURCES) : 情報および要員、装置、資金、情報技術などの情報に関連する資源。[44 U.S.C., SEC. 3502]

情報セキュリティ (INFORMATION SECURITY) : 機密性、完全性、可用性を維持するための、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。[44 U.S.C., SEC. 3542]

情報システム (INFORMATION SYSTEM) : 情報の収集、処理、保守、利用、共有、配布、廃棄のために統合された情報資源の独立した集合体。[44 U.S.C., SEC. 3502]

情報システム所有者 (INFORMATION SYSTEM OWNER) : 情報システムの全面的な調達、開発、統合、修正または運用および保守に責任を持つ関係者。[CNSS Instruction 4009 Adapted]

情報技術 (INFORMATION TECHNOLOGY) : 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、送信または受信に用いられるあらゆる装置また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。 (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。[40 U.S.C., SEC. 1401]

情報タイプ (INFORMATION TYPE): 組織によって、あるいは場合により特定の法律、大統領令、指令、方針または規定によって定義された情報の特定のカテゴリ (例えば、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): 不適切な情報の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]

影響レベルが低位である影響システム (LOW-IMPACT SYSTEM) : 3つすべてのセキュリティ目的 (例: 機密性、完全性および可用性) における影響レベルが、FIPS PUB 199 の潜在的影響値の低位を示す情報システム。

管理的コントロール (MANAGEMENT CONTROLS) : リスクの管理および情報システムセキュリティの管理に焦点を置いたセキュリティ管理策 (例: 予防手段または、対抗策)。

記録媒体（MEDIA）：情報システムの物理的なデバイスすなわち情報を記録、格納または印刷するために書き込む磁気テープ、光学ディスク、磁気ディスク、大規模集積回路（LSI）のメモリチップ、プリントアウト（表示用の媒体は含まない）などを含むが、これらに限らない。

影響レベルが中位である影響システム（MODERATE-IMPACT SYSTEM）：最低 1 つのセキュリティ目的（機密性、完全性または可用性）における影響レベルが、FIP PUB S199 の潜在的影響値の中位を示し、FIPS PUB 199 の潜在的影響値の高位を示すものがない情報システム。

国家的セキュリティ情報（NATIONAL SECURTY INFORMATION）：Executive Order 13292（大統領令 13292）により改正された Executive Order 12958 (大統領令 12958）またはそれ以前のすべての命令、あるいは Atomic Energy Act of 1954 (1954 年施行の原子力法)（その改正を含む）に従い、不当な開示からの保護を必要とすることが決定され、そのように分類されていることを示すためのマーク付けがされた情報。

国家的セキュリティシステム (NATIONAL SECURITY SYSTEM)：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政府機関のために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、諜報活動、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諜報任務の直接的遂行にとって極めて重要なもの (ただし、例えば給与計算、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) 大統領令または議会立法によって制定された規格のもとに、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。[44 U.S.C., SEC. 3542]

運用的管理策（OPERATIONAL CONTROL）：最初は、（システムとは異なり）要員によって導入され、実行される情報システムのセキュリティ管理策（例：予防手段または、対抗策）。

組織（ORGANIZATION）：連邦政府機関、または妥当な範囲での連邦政府機関のあらゆるオペレーションの単位。

潜在的な影響（POTENTIAL IMPACT）：組織の活動、組織の資産または個人に限定的な悪影響、重大もしくは壊滅的な悪影響を及ぼすことが予想される場合の機密性、完全性または可用性の損失。[FIPS Publication 199]

記録（RECORDS）：物理的な形式や特徴にかかわりなく、すべての本、紙、地図、写真、コンピュータが判読可能な物質またはその他の文書資料など、合衆国政府の政府機関の連邦法によってあるいは公務の執行に関連して作成もしくは受領され、組織、機能、方針、判断、手続き、オペレーションまたは政府のこれ以外の活動あるいはそれらデータの情報としての価値のために証拠として、その政府機関またはその正当な後継者によって保存されるまたは、保存するのが適切であると思われるもの。[44 U.S.C., SEC. 3301]

リスク（RISK）：情報システムのオペレーションを前提とする脅威の潜在的な影響およびその脅威が発生し得る可能性が組織活動（任務、機能、印象または評判を含む）、組織資産または個人にもたらす影響のレベル。

リスク管理（RISK MANAGEMENT）：情報システムの運用がもたらす組織活動（任務、機能、印象または評判を含む）、組織資産または個人に対するリスク管理のプロセスと（i）リスク評価 (ii)リスク緩和策の導入 （iii）情報システムのセキュリティの状態を継続的に監視する技術と手順の採用を含む。

予防手段（SAFEGUARDS）：その情報システムに特有のセキュリティ要求事項（例：機密性、完全性および可用性）に合致する所定の保護策。予防手段には、セキュリティ特性、管理者による制限、人的セキュリティと物理的構造、分野およびデバイスのセキュリティが含まれることがある。[CNSS Instruction 4009 Adapted]*セキュリティ管理策及び対抗策と同義*。

無害化（SANITIZATION）：情報の回復を不可能にするなど媒体から情報を除去するプロセス。これには、すべてのラベル、マークや活動ログの除去が含まれる。[CNSS Instruction 4009 Adapted]

セキュリティ分類 (SECURITY CATEGORY) : 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): 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管理的、運用的、技術的管理策 (予防手段または対抗策)。

セキュリティ管理策のベースライン (SECURITY CONTROL BASELINE) : 影響レベルが低位、中位または、高位である情報システムに対する最低限のセキュリティ管理策。

セキュリティ目的 (SECURITY OBJECTIVE): 機密性、完全性、または可用性。

セキュリティ計画 (SECURITY PLAN) : システムセキュリティ計画の項を参照。

セキュリティ要求事項 (SECURITY REQUIREMENTS) : 処理、格納または発信されている情報の機密性、完全性および可用性を確実にするために必要な摘要法、大統領令、指令、方針、基準、指示、規定、手順または組織の任務／事業などから導出された情報処理システムに課される要求事項。

政府機関情報セキュリティ局高官 (SENIOR AGENCY INFORMATION SECURITY OFFICER) : FISMA で規定される最高情報責任者としての役割を果たし、政府機関の承認権限者、情報システムの所有者および情報システムのセキュリティ関係者との最初の連絡窓口としての任務も行う関係者。[44 U.S.C., Sec. 3544]

システム (SYSTEM) : 情報システムの項を参照。

システムセキュリティ計画 (SYSTEM SECURITY PLAN) : 情報システムのセキュリティ要求事項の概要を規定し、これらの要求事項と、順守する所定の、あるいは計画中のセキュリティ管理策を記述する正式な文書。[NIST Special Publication 800-18, Revision 1]

技術的管理策 (TECHNICAL CONTROL) : 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搭載するメカニズムから情報システムによって最初に導入され、実行される情報システムのセキュリティ管理策 (例: 予防手段または対抗策)。

脅威 (THREAT) : 不正アクセス、破壊、不正公開、情報の改ざんおよび／またはサービス拒否攻撃 (DoS 攻撃) などによって情報システムから組織の活動 (任務、機能、印象や評判を含む)、組織の資産または個人に悪影響を及ぼす可能性がある状況または事象。脅威源は、特定の情報システムの脆弱性を巧みに利用する可能性もある。[CNSS Instruction 4009 Adapted]

脅威源 (THREAT SOURCE) : 脆弱性の意図的な搾取を対象とした目的や方法もしくは脆弱性を故意に誘発することがある状況や方法。*脅威要因 (Security Agent) と同義*。

ユーザー (USER) : 情報システムへのアクセスを認可された個人または (システムの) プロセス。[CNSS Instruction 4009]

脆弱性 (VULNERABILITY) : 脅威源によって搾取または誘発されることがある情報システム、システムセキュリティ手順、内部管理や導入における脆弱箇所。[CNSS Instruction 4009 Adapted]

付録 B: 参考文献

[1] Committee for National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, May 2003 (国家安全保障システム委員会指示 4009、国家の情報保証に関する用語集、2003 年 5 月)

[2] E-Government Act of 2002 (Public Law 107-347), December 2002 (2002 年度電子政府法(一般法 107-347)、2002 年 12 月)

[3] Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004 (FIPS 199、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、2004 年 2 月)

[4] Federal Information Security Management Act of 2002 (Public Law 107-347, Title III), December 2002 (2002 年度連邦情報セキュリティマネジメント法(一般法 107-347、第 III 編)、2002 年 12 月)

[5] Information Technology Management Reform Act of 1996 (Public Law 104-106) August 1996 (1996 年度情報技術マネジメント改革法(一般法 104-106)、1996 年 8 月)

[6] National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006 (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作成ガイド"、2006 年 2 月)

[7] National Institute of Standards and Technology Special Publication 800-53, Recommended Security Controls for Federal Information Systems, February 2005 (NIST Special Publication 800-53、"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"、2005 年 2 月)

[8] National Institute of Standards and Technology Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004 (NIST Special Publication 800-60、"情報および情報システムのタイプとセキュリティ分類のマッピングガイド"、2004 年 6 月)

[9] Office of Management and Budget, Circular A-130, Transmittal Memorandum #4 *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, November 2000 (行政管理予算局通達 A-130、通達メモ第 4 号、連邦政府の情報源の管理、第 III 編、連邦政府の自動情報資源のセキュリティ、2000 年 11 月)

付録 C： 参考文献

CIO:： Chief Information Officer （最高情報責任者）

CNSS： Committee for National Security Systems （国家安全保障システム委員会）

FIPS： Federal Information Processing Standards （連邦情報処理規格）

FISMA： Federal Information Security Management Act （連邦情報セキュリティマネジメント法）

NIST： National Institute of Standards and Technology （米国国立標準技術研究所）

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

USC： United States Code （合衆国法典）