FIPS PUB 199

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 セキュリティ分類規格

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

2004 年 2 月

米国商務省 長官
Donald L. Evans

技術管理局 技術担当商務次官
Phillip J. Bond

米国国立標準技術研究所 所長
Arden L. Bement, Jr.

この文書は下記団体によって翻訳監修されています
IPA 独立行政法人 情報処理推進機構 INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
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、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) 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。これらの規定は、商務長官および NIST に対し、連邦政府におけるコンピュータおよびコンピュータ通信システムの利用と管理を改善するという重要な責務を課している。NIST は、情報技術ラボラトリ (Information Technology Laboratory) を通して、これらの分野における規格、およびガイドラインの開発に向けて指導、技術的ガイダンスの提供、および政府の取り組みの調整を行っている。

本 FIPS PUB (連邦情報処理規格) 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。

-- Susan Zevin, Acting Director
Information Technology Laboratory

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。

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 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、以下 FISMA と称す) 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)

本 FIPS PUB 199 は、情報および情報システムの分類に関する規格の策定という上記第 1 の任務に応えるものである。情報および情報システムのセキュリティ分類規格によって、セキュリティを表現する共通の枠組みと理解が提供され、連邦政府は、次の 2 点の対応を促される。 (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、情報セキュリティ導入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、情報セキュリティ方針、手順、および実践の妥当性と有効性に関する正確な報告。上記の第 2 および第 3 の任務には、後続の NIST 規格およびガイドラインによって対処する。

2 適用範囲

これらの規格は、(i) Executive Order 13292 (大統領行政命令 13292) により改正された Executive Order 12958 (大統領行政命令 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、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以外の連邦政府内のすべての情報、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。また、連邦政府機関の職員は、情報および情報システムの分類を実施することを定めた連邦の要件がある場合は必ず、本 FIPS PUB 199 に記述されたセキュリティ分類を使用しなければならない。追加すべきセキュリティ関連項目は、連邦政府各省庁の判断により開発し、使用してよい。州、地方政府および部族政府はもとより、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を検討することができる。これらの規格は、商務長官が承認した時点で発効する。

3 情報および情報システムの分類

本規格は、情報[1]および情報システムの両方のセキュリティ分類を規定する。セキュリティ分類は、組織が割り当てられた任務の達成、資産の保護、法的責任の履行、日常機能の維持、および個人の保護のために必要とする情報および情報システムを脅かす何らかの事象が発生した場合の、組織に対する潜在的影響に基づいたものである。セキュリティ分類は、組織に対するリスクを評価する際に脆弱性および脅威情報と併せて使用するものである。

[1] 情報は、*その情報タイプ*に基づいて分類される。情報タイプとは、情報を特定するカテゴリであり(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)、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、方針、または規定によって定義される。

セキュリティの目的

FISMA は、情報および情報システムに対し 3 つのセキュリティ目的を定義している。

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]

*機密性*の損失とは、情報の不当な開示である。

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]

*完全性*の損失とは、情報の不当な改変または破壊である。

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]

*可用性*の損失とは、情報または情報システムへのアクセスまたは利用への妨害である。

組織および個人に対する潜在的影響

本 FIPS PUB 199 は、セキュリティ侵害 (つまり、機密性、完全性、または可用性の損失) が発生した場合の、組織または個人に対する*潜在的影響*を 3 つのレベルで定義する。これらの定義の適用は、各組織および国家全体の利益に基づいて行わなければならない。

以下の場合、*潜在的影響*は低位である。

– 機密性、完全性、または可用性の損失が、組織活動、組織資産、または個人に限定的な悪影響を及ぼすことが予想されうる[2]。

  詳細説明：限定的な悪影響とは、例えば、機密性、完全性、または可用性の損失が、(i) ある範囲や期間において組織がその基本機能を遂行する能力の低下をもたらし、よって、その機能の有効性が目立って低下する、(ii) 組織の資産に軽微な損害をもたらす、(iii) 財務上の軽微な損失をもたらす、あるいは (iv) 個人に軽微な被害をもたらす可能性があることを意味する。

以下の場合、*潜在的影響*は中位である。

– 機密性、完全性、または可用性の損失が、組織活動、組織資産、または個人に重大な悪影響を及ぼすことが予想されうる。

  詳細説明：重大な悪影響とは、例えば、機密性、完全性、または可用性の損失が、(i) ある範囲や期間において、組織がその基本機能を遂行する機能に重大な低下をもたらし、よってその機能の有効性が著しく低下する、 (ii) 組織資産に重大な損害をもたらす、(iii) 重大な財務上の損失をもたらす、あるいは (iv) 人命の損失や人命への重大な傷害を伴わない重大な被害を個人にもたらす可能性があることを意味する。

[2] 個人に対する悪影響は、個人が法律のもとに権利を与えられているプライバシーの損失を含むが、これらに限定されるものではない。

以下の場合、*潜在的影響*は高位である。

– 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。

詳細説明：致命的または壊滅的な悪影響とは、例えば、機密性、完全性、または可用性の損失が、(i) ある範囲や期間において、組織がその基本機能の 1 つ以上を遂行することができず、任務遂行能力に致命的な低下または損失がもたらされる、(ii) 組織資産に甚大な損害をもたらす、(iii) 甚大な財務上の損失をもたらす、あるいは (iv) 人命の損失や人命への重大な傷害を伴う致命的または壊滅的な被害を個人にもたらす可能性があることを意味する。

情報タイプ別に適用されるセキュリティ分類

情報タイプのセキュリティ分類は、利用者情報とシステム情報[3]の両方に関連するものであり、電子形式または非電子形式の情報に適用することができる。また、情報タイプのセキュリティ分類は、情報システムのセキュリティ分類を検討する際のインプット（情報）として使用することもできる（以下の情報システムのセキュリティ分類の記述を参照）。情報タイプのセキュリティ分類を適切に評価するには、特定の情報タイプに関連する各セキュリティ目的ごとに*潜在的影響*を判断することが基本として必要である。

情報タイプのセキュリティ分類 (SC: Security Category) の一般化された表現形式は、以下のとおりである。

$$SC_{\text{情報タイプ}} = \{(\text{機密性}, \textit{影響}), (\text{完全性}, \textit{影響}), (\text{可用性}, \textit{影響})\}$$

ここで、潜在的影響の許容値は、「低位」、「中位」、「高位」、または「該当なし」[4]である。

例 1：ウェブサーバ上で*公開情報*を管理している組織が、機密性の損失による潜在的影響はなく（つまり、機密性要件には該当なし）、完全性の損失による潜在的影響は中位であり、可用性の損失による潜在的影響は中位であると判断したとする。この情報タイプのセキュリティ分類 (SC) の結果は、以下の式で表現される。

$$SC_{\text{公開情報}} = \{(\text{機密性}, \text{該当なし}), (\text{完全性}, \text{中位}), (\text{可用性}, \text{中位})\}$$

例 2：極秘の*調査情報*を管理している法の執行組織が、機密性の損失による潜在的影響は高位であり、完全性の損失による潜在的影響は中位であり、可用性の損失による潜在的影響は中位であると判断したとする。この情報タイプのセキュリティ分類 (SC)の結果 は、以下の式で表現される。

$$SC_{\text{調査情報}} = \{(\text{機密性}, \text{高位}), (\text{完全性}, \text{中位}), (\text{可用性}, \text{中位})\}$$

例 3：日常の*管理情報*（プライバシー関連情報以外）を管理している財務組織が、機密性の損失による潜在的影響は低位であり、完全性の損失による潜在的影響は低位であり、可用性の損失による潜在的影響は低位であると判断したとする。この情報タイプのセキュリティ分類 (SC)の結果 は、以下の形式で表現される。

$$SC_{\text{管理情報}} = \{(\text{機密性}, \text{低位}), (\text{完全性}, \text{低位}), (\text{可用性}, \text{低位})\}$$

[3] システム情報 (例えば、ネットワークルーチン表、パスワードファイル、暗号鍵管理情報) は、機密性、完全性、および可用性を保証するために、情報システムによって処理、格納、または伝送される最も重要または機密に関わる利用者情報に相応のレベルで保護されなければならない。

[4] 潜在的影響値における*該当なし*は、セキュリティ目的「機密性」にのみ適用される。

情報システムに適用されるセキュリティ分類

情報システムのセキュリティ分類を判断するには、もう少し詳しい分析が必要であり、情報システム上に存在するすべての情報タイプのセキュリティ分類を考慮しなければならない。情報システムの場合、それぞれのセキュリティ目的 (機密性、完全性、可用性) に関し指定される潜在的影響値は、情報システム上に存在する情報の各タイプごとに判断されたセキュリティ分類の中で最も高い値 (つまり、最高水準) でなければならない[5]。

情報システムのセキュリティ分類 (SC: Security Category) の一般化された表現形式は、以下のとおりである。

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

ここで、潜在的影響の許容値は、「低位」、「中位」、または「高位」である。

情報システムのセキュリティ分類を評価する場合、「*該当なし*」の値は、いかなるセキュリティ目的にも指定することはできないことに留意されたい。これは、情報システムの運用時においては、システムレベルでの処理機能および機密情報を保護することが基本的要件であるため、情報システムの機密性、完全性、および可用性が失なわれた時には、低位レベル (つまり、最低水準)の潜在的影響が存在するとの認識による。

例 4:ある業務請負企業において、大規模なシステム調達の際に使用される情報システムは、契約の前段階の契約機密情報と日常的に用いられる管理情報の両方を含んでいる。その業務請負企業内の管理者が、(i) 機密に関わる契約情報に関して、機密性の損失による潜在的影響は中位であり、完全性の損失による潜在的影響は中位であり、可用性の損失による潜在的影響は低位であると判断し、(ii) 日常的管理情報 (非プライバシー関連情報) に関して、機密性の損失による潜在的影響は低位であり、完全性の損失による潜在的影響は低位であり、可用性の損失による潜在的影響は低位であると判断したとする。これらの情報タイプのセキュリティ分類 (SC: Security Category) の結果は、以下の式で表現される。

$$SC_{\text{契約情報}} = \{(\text{機密性}, \text{中位}), (\text{完全性}, \text{中位}), (\text{可用性}, \text{低位})\}$$

および

$$SC_{\text{管理情報}} = \{(\text{機密性}, \text{低位}), (\text{完全性}, \text{低位}), (\text{可用性}, \text{低位})\}$$

この情報システムのセキュリティ分類の結果は、以下の式で表現される。

$$SC_{\text{調達システム}} = \{(\text{機密性}, \text{中位}), (\text{完全性}, \text{中位}), (\text{可用性}, \text{低位})\}$$

これは、調達システム上に存在する情報タイプの、各セキュリティ目的におけるレベルの最高値または潜在的影響の最大値を表すものである。

[5] 情報システムはプログラムと情報の両方によって構成されている。情報システム内で実行中のプログラム (つまり、システムプロセス) は、情報の処理、格納、および伝送を容易にするものであり、組織が任務に関する基本的な機能を遂行したり、操作したりするために必要である。これらのシステム処理機能もまた保護する必要があり、同様にセキュリティ分類の対象となりうる。しかしながら、簡素化のために、情報システムに関連するすべての情報タイプのセキュリティ分類においては、情報システム全体に対して適切と思われる*最悪のケース*を想定して、潜在的影響を評価するものである。これによって情報システムのセキュリティ分類を評価するにあたって、システムプロセスを考慮する必要性を取り除くものである。

例 5：ある発電所は、大規模軍事施設への配電を制御する SCADA (監視制御データ収集) システムを備えている。その SCADA システムは、リアルタイムセンサデータと日常的管理情報の両方を含んでいる。その発電所の管理者が、(i) SCADA システムによって収集されるセンサデータに関して、機密性の損失による潜在的影響はないが、完全性の損失による潜在的影響は高位であり、可用性の損失による潜在的影響は高位であると判断し、(ii) そのシステムによって処理される管理情報に関して、機密性の損失による潜在的影響は低位であり、完全性の損失による潜在的影響は低位であり、可用性の損失による潜在的影響は低位であると判断したとする。これらの情報タイプのセキュリティ分類 (SC: Security Category) は、以下の式で表現される。

$$\mathbf{SC}_{\text{センサデータ}} = \{(\text{機密性}, \text{該当なし}), (\text{完全性}, \text{高位}), (\text{可用性}, \text{高位})\}$$

および

$$\mathbf{SC}_{\text{管理情報}} = \{(\text{機密性}, \text{低位}), (\text{完全性}, \text{低位}), (\text{可用性}, \text{低位})\}$$

この情報システムのセキュリティ分類の結果は、以下の形式で表現される。

$$\mathbf{SC}_{\text{SCADA システム}} = \{(\text{機密性}, \text{低位}), (\text{完全性}, \text{高位}), (\text{可用性}, \text{高位})\}$$

これは、SCADA システム上に存在する情報タイプの、各セキュリティ目的におけるレベルの最高値または潜在的影響の最大値を表すものである。また、その発電所の管理者が、システムレベルの情報または処理機能が不当に開示されるセキュリティ侵害が発生した場合を想定し、情報システムに対する潜在的影響に関するより現実的な見通しを反映し、機密性の損失による潜在的影響を低位から中位に引き上げることを選択したとする。その場合、この情報システムの最終的なセキュリティ分類は、以下の形式で表現される。

$$\mathbf{SC}_{\text{SCADA システム}} = \{(\text{機密性}, \text{中位}), (\text{完全性}, \text{高位}), (\text{可用性}, \text{高位})\}$$

表 1 に、各セキュリティ目的 (機密性、完全性、および可用性) に対する潜在的影響の定義を要約する。

表 1：セキュリティ目的に対する潜在的影響の定義

	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。

付録 A　用語および定義

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]

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]

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使用または運用されている情報システム。**[40 U.S.C., SEC. 11331]

情報 (INFORMATION)：**情報タイプの実体。**

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、配信、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、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、**(1) **そのような装置を使用する必要がある場合、または** (2) **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、大統領行政命令、大統領令、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]

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) **大統領行政命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]

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 (保護手段または対抗策)。

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

付録 B　参考文献

[1] Privacy Act of 1974 (Public Law 93-579), September 1975. (1975 年 9 月施行のプライバシー保護法)

[2] Paperwork Reduction Act of 1995 (Public Law 104-13), May 1995. (1995 年 5 月施行の文書業務削減法)

[3] OMB Circular (行政管理予算局通達) A-130, Transmittal Memorandum #4, (通達メモ第 4 号), *Management of Federal Information Resources, November 2000*.

[4] Information Technology Management Reform Act of 1996 (Public Law 104-106), August 1996. (1996 年 8 月施行の情報技術マネジメント改革法)

[5] Federal Information Security Management Act of 2002. (Public Law 107-347), December 2002. (2002 年 12 月施行の連邦情報セキュリティマネジメント法)