NIST Special Publication 800-60
Version 2.0

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

第 I 巻：
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

William C. Barker

情　報　セ　キ　ュ　リ　テ　ィ

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

2004 年 6 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

コンピュータシステム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 と称する。）の情報技術ラボラトリ（ITL:Information Technology Laboratory）は、国の測定基準および標準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、参照データの作成、コンセプト導入の検証、技術的分析を行い、情報技術の開発と生産的利用の拡大に努めている。情報技術ラボラトリの責務は、連邦政府のコンピュータシステムにおいて、費用対効果の高いセキュリティと取り扱いに注意を要する非機密扱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規格とガイドラインを策定することにある。NIST Special Publication800 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、ガイダンス、成果を報告し、産業界、政府機関および教育機関との共同活動についても報告する。

作成機関

NIST は、2002 年の連邦情報セキュリティマネジメント法（FISMA: Federal Information Security Management Act）、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、すべての連邦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、最低要件を含んだ規格およびガイドラインを作成する責任があるが、このような規格およびガイドラインは国家的セキュリティ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）』の要件に一致しており、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。非政府組織が自己責任において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、SP800-60 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）。

この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規格およびガイドラインを否定するものではない。また、これらのガイドラインは、商務長官、行政管理予算局長、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。

NIST Draft Special Publication 800-60
NIST Spec. Publ. 800-60、第 I 巻、57 ページ（2004 年 6 月）

謝辞

本書のドラフトをレビューし作成に貢献してくれた同僚に感謝の意を表したい。入念にレビューをしてくれた Tanya Brewer-Joneas 氏ならびに Shirley Radack 氏には特にお礼を申し上げる。さらに、公共および民間部門からいただいた数多くの貢献にも心より感謝の意を表する。これらの思慮深い建設的なコメントによって、本書の質と実用性が高められた。

注

NIST Special Publication (SP) 800-60 は、順次公開している以下の一連のセキュリティ関連の文書と併せて使用できる。

- FIPS Publication 199 *Standards for Security Categorization of Federal Information and Information System*、2004 年 2 月 (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)
- NIST SP 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems*（最終公開ドラフト）、2004 年 4 月 （連邦政府情報システムのセキュリティに対する承認および認可ガイド）
- NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*（初期公開ドラフト）、2003 年 10 月（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）
- NIST SP 800-53A *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Information Systems*（初期公開ドラフト）、2004 年秋
- NIST SP 800-59 *Guideline for Identifying an Information System as a National Security System*、2003 年 8 月
- FIPS Publication 200[1] *Minimum Security Controls for Federal Information Systems* （2005 年秋公開予定）（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）

7 つの文書からなる本シリーズは、連邦情報システムセキュリティ管理策の選択、特定、採用、評価のための柔軟な枠組みの提供を目指しており、完成すれば、2002 年の連邦情報セキュリティマネジメント法（FISMA）の要件を満たすのに多大な貢献を果たすことが期待される。7 つの文書すべてを同時に発表できないのは残念だが、現在の国際情勢と連邦政府の情報セキュリティに対する高い優先度に鑑み、個々の文書が完成次第、順次発表していくこととした。これらの文書は相互に補強しあうものであり、相互に依存する部分もあるが、ほとんどの場合それぞれが独立した文書として有効に利用できる。

本書は全 2 巻の第 I 巻であり、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に関する基本的ガイドラインを含む。任務別情報タイプごとに推奨するセキュリティ分類およびその根拠について記載した付録は、別巻として公開する。

SP 800-60 の情報タイプおよびセキュリティ影響レベルは、OMB 連邦政府 EA 管理室（Federal Enterprise Architecture Program Management Office）の『*Business Reference Model 2.0*』、NIST SP 800-60 ワークショップの参加者からの意見、および FIPS 199 に基づいている。付録で提供する推奨影響レベル例の根拠は多くの情報源を参考にしたものであるため、用語、構成、および内容に一貫性を持たせるためには、レビュー、コメント、およびそれを反映した修正を何度か繰り返す必要がある。本書のセキュリティ分類が、SP 800-53 のセキュリティ管理策を選択するうえで果たす不可欠な役割、連邦政府の情報システムを保護するためのセキュリティ管理策における重要性から考えれば、これらの管理策を採用するコミュニティに対して本文書を早期に公開する必要があり、そのため、本文書は可能な限り早く公開される運びとなった。

[1] FIPS Publication 200『*Minimum Security Controls for Federal Information Systems*』が 2005 年に出版されれば、これが NIST Special Publication 800-53 にとって代わるものとなり、2002 年の連邦情報セキュリティマネジメント法（FISMA）に従って連邦機関が準拠することが必須の規格となる。

（本ページは意図的に白紙のままとする）

要旨

電子政府法（公法 107-347）第 III 編、2002 年の連邦情報セキュリティマネジメント法（FISMA）は、NIST に対して、以下のものを作成する任務を課している。

- 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、もしく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を勧告するガイドライン
- 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）

本ガイドラインは、上記の 2 番目の任務を踏まえて、連邦政府機関における情報および情報システムの分類を支援するために作成された。本ガイドラインの目的は、情報または情報システムの許可のない開示、改変、または可用性の損失によって生じうる被害とその結果の度合いに応じた、適切なレベルの情報セキュリティの適用を容易にすることにある。本ガイドラインは、ユーザーが『*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*』（FIPS 199）を十分理解していることを前提として記述している。本ガイドラインおよび付録では以下の事項について記述する。

- FIPS 199 によって確立されたセキュリティ分類の用語および定義の概説
- セキュリティ分類プロセスの勧告
- 連邦政府の情報および情報システムのタイプを識別するための方法論の記述
- 一般的な情報タイプの暫定的なセキュリティ影響レベルの提案
- 暫定的な影響レベルの割り付けとの相違をもたらす可能性がある情報属性の考察
- システムの使用、接続性、および集約情報の内容に基づいたシステムのセキュリティ分類の確立方法

一般に、情報のタイプは、ほとんどの政府機関に共通の業務に関連する情報と、各政府機関固有の任務に関する情報に分けられる。本ガイドラインでは、運営、管理、および支援情報を*管理・支援*情報と呼ぶ。管理・支援情報に比べ、任務別情報タイプは各政府機関間での任務共通性がきわめて低いため、本ガイドラインは、任務別情報については管理・支援情報ほど規定しない。本ガイドラインでは、管理・支援情報タイプは具体的に識別するが、任務別情報については情報タイプの識別および影響レベル割り付けの一般的ガイドラインを中心に扱う（*管理・支援*の影響割り付けの例については付録 C、任務別の影響割り付けの例については付録 D で述べる）。

本文書は、指導書というよりむしろリファレンス用の情報資源として作成されたものであり、すべての資料がすべての政府機関にあてはまるとは限らない。本文書は基本的ガイドラインと付録の全 2 巻を収録している。ユーザーには、第 I 巻で提供するガイドラインをレビューしたうえで、付録から各自のシステムおよびアプリケーションに適用される特定の資料を参照していただきたい。

付録に含まれている暫定的な影響割り付けは、影響割り付けとその後のリスクアセスメントにつづくプロセスの最初のステップにすぎない。影響割り付けは、監査人が情報タイプおよび影響割り付けの最終的なチェックリストとして使用することを目的とするものではない。

本ガイドラインで採用した情報タイプ識別の基礎となるのは、OMB 連邦政府 EA 管理室が 2003 年 6 月に公開した資料『*The Business Reference Model Version 2.0 (BRM)*』である。*BRM* は、政府の目的（任務、*国民サービスを指す*）に関する機能、政府がその目的を達成するために使用する仕組み（*提供形態*）、政府の運営に必要な支援機能（*支援サービス*）、および政府の事業のあらゆる分野を支援する資源管理機能（*資源管理*）について記述している。*支援サービス*および*資源管理*機能に関連する情報タイプは、*管理・支援*タイプとして扱われる（OMB *BRM* は時々改訂されるが、*BRM* の変更すべてが本ガイドラインで採用している情報分類法の変更につながるとは限らない）。

そのほかにも、連邦機関の依頼により、いくつかの情報タイプを追加した。付録 C では、*管理・支援情報タイプ* ごとに暫定的に機密性、完全性、および可用性情報分類を勧告し、暫定影響レベルの基本的な根拠を提供する。*国民サービス*および*提供形態*機能に関連する情報タイプは、任務別情報として扱われる。任務別情報タイプの推奨暫定影響レベル、基本的根拠、および暫定割り付けからのずれの根拠の例は付録 D で提供する。

一部の情報は、法律、大統領令、または政府機関の規制により、非開示のための保護が必要なものとして規定されている。連邦政府省庁および機関で取り扱われる情報の秘匿度および／または重大度（これらの用語は付録 A で定義する）を規定する根拠となる法律および大統領令は付録 E で扱う。また、合衆国法典からの個々の引用も記載する。

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

目次

第 I 巻：
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

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

1.0 序論

電子政府法（公法 107-347）第 III 編、2002 年の連邦情報セキュリティマネジメント法（FISMA）は、NIST に対して以下のものを作成する任務を課している。

- 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、もしく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を勧告するガイドライン
- 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）

NIST SP 800-60 の目的は、上記 FISMA 関連の任務の 2 番目、すなわち情報および情報システムのタイプを潜在的なセキュリティ影響に応じて分類するための、ガイドラインを作成することである。本ガイドラインは、政府機関がセキュリティ影響レベルを、(i) 情報（例としてプライバシー、医療、専有、財務、請負業者機密、企業秘密、調査）、および (ii) 情報システム（例として、基幹、任務支援、運営）のタイプに一貫した形でマッピングするのに役立つであろう。

一般に、情報のタイプは、各政府機関固有の任務活動に関する情報と、ほとんどの政府機関に共通する運営、管理、および支援活動に関連する情報に分けられる。本ガイドラインでは、運営、管理、および支援情報を*管理・支援*情報と呼ぶ。*任務別*活動に関連する情報のセキュリティ属性は、各政府機関によって異なることが多く、さらに機関内でも組織によって異なる可能性がある。本ガイドラインでは、*任務別*情報は、政府機関間での共通性が高い*管理・支援*情報とは別に扱う。任務別情報の侵害の結果は運用環境によって異なるため、本ガイドラインは、*任務別*情報については*管理・支援*情報ほど規定しない。同様に、*任務別*情報の秘匿度を左右する情報タイプ、情報の利用、ならびにプログラムおよび任務のライフサイクルの状況に関する専門知識は、その任務情報に責任のある政府機関内（または政府機関内の責任のある組織内）に集中している。本ガイドラインでは、*管理・支援*情報タイプは具体的に定義し、基本的ガイドラインを述べるが、任務別情報の扱いについては、情報タイプの識別および影響レベル割り付けの一般的ガイドラインにとどめる（両クラスの情報タイプの記述および暫定影響割り付けは、付録 C および D でそれぞれ裏づけとなる根拠とともに示す）。

1.1 構成

本ガイドラインは 2 巻に分かれている。第 I 巻では、情報タイプの識別およびセキュリティ分類のガイドラインを示す。第 II 巻は、影響割り付けの例やセキュリティ分類の根拠を記載した付録で構成されている。

第 I 巻では、以下の背景情報およびマッピングのガイドラインを提供する。

- 第 2 章：連邦情報処理標準 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*』[FIPS 199]で識別されているセキュリティ目標および影響レベルの概要
- 第 3 章：影響レベルの選択に用いるプロセス、影響割り付けに関する一般的考慮事項、およびシステム分類のガイドラインの概要
- 第 4 章：*任務別*情報タイプの識別および任務情報に対するセキュリティ影響レベルの割り付けのガイドライン
- 第 5 章：*管理・支援*情報（運営、管理、およびサービス情報）の推奨情報タイプ

第 II 巻は以下の付録を収録している。

- 付録 A：用語集
- 付録 B：参考文献
- 付録 C：*管理・支援*情報（運営、管理、およびサービス情報）の暫定影響割り付けおよび裏づけとなる根拠
- 付録 D：*任務別*情報（任務情報およびサービス提供メカニズム）の暫定影響割り付けおよび裏づけとなる根拠
- 付録 E：秘匿度／重大度を指定する根拠となる法律および大統領令

本ガイドラインは、指導書というよりむしろリファレンス用の情報資源として作成されたものであり、すべての資料がすべての政府機関にあてはまるとは限らない。ユーザーは、本ガイドラインの最初の 3 章の序説、用語、およびプロセスに関する資料をレビューされたい。また、任務情報（第 4 章）ならびに運営、管理、およびサービス情報（第 5 章）の影響レベルの割り付けのガイドラインのレビューも推奨する。そのうえで、残りのガイドラインから各自のシステムまたはアプリケーションに適用される資料のみを参照する必要がある。暫定影響レベルの割り付けおよびレビューを支援するための資料は、付録 C、D、および E に収録されている。

1.2 適用範囲

本勧告は、*国家的セキュリティシステム*以外のすべての連邦システムに適用される。*国家的セキュリティシステム*とは、*国家セキュリティ*情報を蓄積、処理、または伝達するものである[2]。

[2] FISMA では、*国家的セキュリティシステム*を、政府機関または政府機関の意向を受けた請負業者、あるいは政府機関の意向を受けた別の組織が使用または運用する情報システム（あらゆる電気通信システムを含む）であって、(i) その機能、運用、もしくは利用が、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を伴うか、あるいは軍事または諜報任務の直接的遂行にとってきわめて重要である（ただし、例えば給与、財務、物流、人事管理などのアプリケーションに使用される日常の運営または業務用のアプリケーションシステムは除く）、または (ii) 機密情報を取り扱う情報システムと定義している。[公法 107-347, Section 3542 (b)(2)(A)を参照]

付録に含まれている暫定影響割り付けは、影響割り付けの最初のステップにすぎず、その後のリスクアセスメントプロセスでのレビューも推奨する。この暫定的影響割り付けは、監査人が情報タイプおよび影響割り付けの最終的なチェックリストとして使用することを目的とするものではない。

（本ページは意図的に白紙のままとする）

2.0 情報および情報システムのセキュリティ分類

本ガイドラインで情報タイプとマッピングするセキュリティ分類、セキュリティ目標、および影響レベルは、連邦情報処理規格 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*』（FIPS 199）で定義されているものである。また、本ガイドラインの使用の範囲も FIPS 199 に記述されているものである。本ガイドラインの使い勝手を考慮して、FIPS 199 の内容の一部を本章に引用する。

ほとんどの連邦政府機関には、その情報および／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により生じると予想される潜在的影響レベルまたは損害規模を想定するための専門知識と情報ベースを有している。FIPS 199 では、侵害の確率を算定する試みなどのアセスメントの結果ではなく、侵害により生じると予想される損害規模の結果に基づいてセキュリティ分類を規定している。

本ガイドライン SP 800-60 の付録では、特定の情報タイプの暫定影響レベルを勧告する。また、それらの勧告暫定レベルの根拠をいくつか提供するとともに、勧告暫定レベルより高いまたは低い影響レベルの割り付けとなる可能性があるいくつかの事柄について考察する。

多くの政府機関に共通する*管理・支援*情報に関連する影響レベルは、それに関連する任務別情報に強く影響される。つまり、きわめて重要である、あるいは重要な機密にかかわる任務別情報タイプとともに使用される政府機関共通の情報は、あまり重要でない任務別情報タイプとともに使用される政府機関共通の情報より影響レベルが高くなる可能性がある。各組織は、暫定情報影響レベルを各自の運用環境の枠組みのなかでレビューした結果に従って、その影響レベルをそのまま利用するか、修正する。情報の影響レベルは、組織の運用環境の枠組みに従って定義するしかない。ある組織または運用の枠組みのなかでは影響が低い情報タイプでも、別の組織または運用の枠組みのなかでは高い影響レベルを持つ可能性がある。

一般に、情報システムは多くのタイプの情報を取り扱う。それらの情報タイプがすべて同じ影響レベルを持つとは限らない。情報タイプによっては、侵害された場合、ほかの情報タイプよりもシステムの機能性や政府機関の任務を大きく脅かすものもあろう。システムの影響レベルの査定は、システムの任務および機能の枠組みのなかで行うだけでなく、さらにコンポーネント情報タイプの集合に基づいて行わなければならない。

2.1 セキュリティ分類とセキュリティ目標（FIPS 199 の内容）

2.1.1 セキュリティ分類

FIPS 199 は、情報[3]と情報システムの両方のセキュリティ分類を規定している。セキュリティ分類は、組織がその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特定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く。セキュリティ分類は、組織に対するリスクを査定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。

[3] 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、組織により、あるいは場合によっては特定の法律、大統領令、指令、方針、または規制により定義された情報の特定のカテゴリである（例：プライバシー、医療、専有、財務、調査、請負業者機密、セキュリティ管理）。

FIPS 199 では、連邦情報および情報システムの保護に関連して、3 つのセキュリティ目標（機密性、完全性、可用性）ごとに 3 つの潜在的影響レベル（低位、中位、高位）を規定している。

2.1.2 セキュリティ目標と潜在的損失のタイプ

連邦情報セキュリティマネジメント法および FIPS 199 では、情報および情報システムに対して 3 つのセキュリティ目的（機密性、完全性、可用性）を定義している。

2.1.2.1 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。

2.1.2.2 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。

2.1.2.3 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。

2.2 影響アセスメント（FIPS 199 の内容）

セキュリティ侵害が発生した場合の組織または個人への*潜在的影響*のレベルに関する FIPS 199 の定義の適用は、各組織および国家全体の利益の枠組みのなかで行わなければならない。

2.2.1 影響レベル

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、組織の運営、組織の資産、または個人に**限定的な**悪影響を及ぼすと予想されうる[4]。

  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。

[4] 個人に対する悪影響は、個人が法律の下に権利を与えられているプライバシーの損失を含むが、これらに限定されない。

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、組織の運営、組織の資産、または個人に**重大な**悪影響を及ぼすと予想されうる。

  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) 組織の資産に重大な損害をもたらす、(iii) 財務上の重大な損失をもたらす、あるいは (iv) 人命の損失または人命にかかわる重大な傷害を伴わない重大な損害を個人に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**高位**である。

– 機密性、完全性、または可用性の損失が、組織の運営、組織の資産、または個人に**致命的または壊滅的な**悪影響を及ぼすと予想されうる。

  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) 組織の資産に甚大な損害をもたらす、(iii) 財務上の甚大な損失をもたらす、あるいは (iv) 人命の損失または人命にかかわる重大な傷害を伴う致命的または壊滅的な損害を個人にもたらす可能性があることを意味する。

2.2.2 情報タイプ別に確立するセキュリティ分類

FIPS 199 では、情報タイプのセキュリティ分類は、ユーザー情報とシステム情報[5]の両方に関連づけられ、また電子媒体・非電子媒体両方の情報に適用できるとしている。FIPS 199 は、情報システムに適切なセキュリティ分類を考慮する際にも参照できる。情報タイプ別に適切なセキュリティ分類を適用するには、特定の情報タイプに関連のあるセキュリティ目標ごとに*潜在的影響*を決定することが必ず必要となる。情報タイプのセキュリティ分類 (SC: Security Category)の一般化された書式は、以下のとおりである。

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

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」[6]である。

[5] システム情報（例えば、ネットワーク経路表、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、情報システムが処理している最も重要な、または最も機密にかかわるユーザー情報に相応のレベルで保護しなければならない。

[6] 潜在的影響値「*該当なし*」は、セキュリティ目標「機密性」にのみ適用される。

3.0 影響レベルの割り付けとセキュリティ分類

3.1 情報タイプとセキュリティ管理策および影響レベルへのマッピング

本サブセクションでは、情報タイプおよび情報システムをセキュリティ管理策および影響レベルにマッピングする段階的な方法論を提供する。セキュリティレベルの割り付けは、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*』に基づく。本文書は、ユーザーが FIPS 199 を読み、その内容を十分理解していることを前提としている。

図 1 にセキュリティ分類プロセスを示し、セキュリティ分類がどのようにセキュリティ管理策の選択プロセスに適合するかを示す。本プロセスは、情報システムごとに実行される。

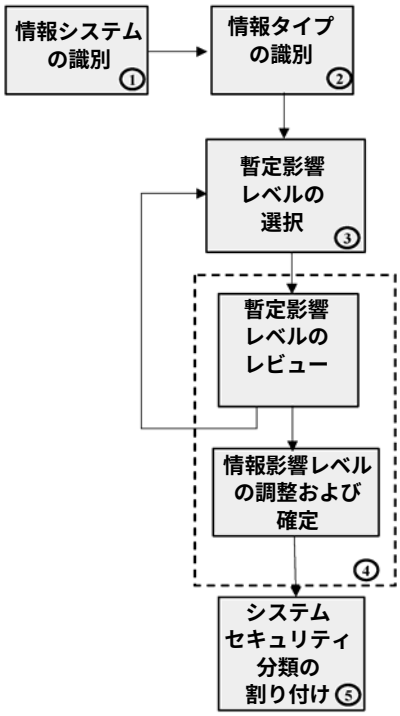

図 1：SP 800-60 のセキュリティ分類プロセス

1. 情報システムの識別：情報システムには、一般支援システム、主要アプリケーション、ローカルシステム、特殊用途システムなどがある。政府機関は、セキュリティ分類のため、システム識別に関する各自の方針を策定する。一般に、システムはセキュリティ境界に接する[7]。

2. 情報タイプの識別：ユーザーは、システムごとに入力、蓄積、処理、および／または出力されるすべての情報タイプを識別する[7]。

[7] 計画中／提案中のシステムの情報タイプおよびセキュリティ境界については、いくつかの前提条件を置かなければならない。

3. 暫定影響レベルの選択：ユーザーは、識別した情報タイプごとに暫定影響レベルを選択する。（例については付録 C および D を参照）。

4. 暫定影響レベルのレビューと調整：ユーザーは、レビュー対象のシステムに関連する組織、環境、任務、利用、および接続性に基づいて、ユーザーの情報タイプに対して勧告されている暫定影響レベルの適切性をレビューする。

   暫定影響レベルのレビュー後、必要に応じて影響レベルを調整する。

5. システムセキュリティ分類の割り付け：次に、レビュー対象のシステムに関連する機密性、完全性、および可用性への影響レベルを確立する。当てはめられた情報タイプの影響レベルを、各システムにおいて、またシステムによって処理されるすべての情報をまとめたままでレビューする。まとまった情報全体での機密性、完全性、または可用性の損失は、単体の情報タイプのそれより重大な結果になる可能性がある。また、システムのアクセス制御情報とその保護および呼び出しを行うシステムソフトウェアのいずれも、システムの完全性および可用性属性、さらにはレビュー対象のシステムが接続されたほかのシステムへのアクセスに影響を及ぼす可能性がある。

セキュリティ分類プロセスの完了後は、本プロセスで得られた機密性、完全性、および可用性影響レベルの決定を、システムリスクアセスメントおよび各システムに必要な一連のセキュリティ管理策の選択への入力に使用することができる。各システムセキュリティ分類に対して勧告されている最低限のセキュリティ管理策は、NIST SP 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*』に記載されている。

図 2 に、情報セキュリティ構想における NIST のセキュリティ標準およびガイドラインの役割を示す。これらの出版物で文書化されたセキュリティ分類プロセスは、以下のプロセスの入力となる。

- NIST SP 800-30『*IT システムのためのリスクマネジメントガイド*』で定義され、NIST SP 800-37『*連邦政府情報システムのセキュリティに対する承認および認可ガイド*』で特定された承認および認可プロセスで実施されるリスクアセスメント

- NIST SP 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*』（および同タイトルの将来の FIPS）で定義されたセキュリティ管理策の選択および実施

- NIST SP 800-18『*IT システムのためのセキュリティ計画策定ガイド*』および NIST SP 800-34『*IT システムのための緊急時対応計画ガイド*』で特定されたセキュリティ計画

- NIST SP 800-37 で特定されたシステム承認および認可
- NIST SP 800-37 および NIST SP 800-26『*IT システムのためのセキュリティ自己アセスメントガイド*』で特定されたシステム変更の影響レビュー

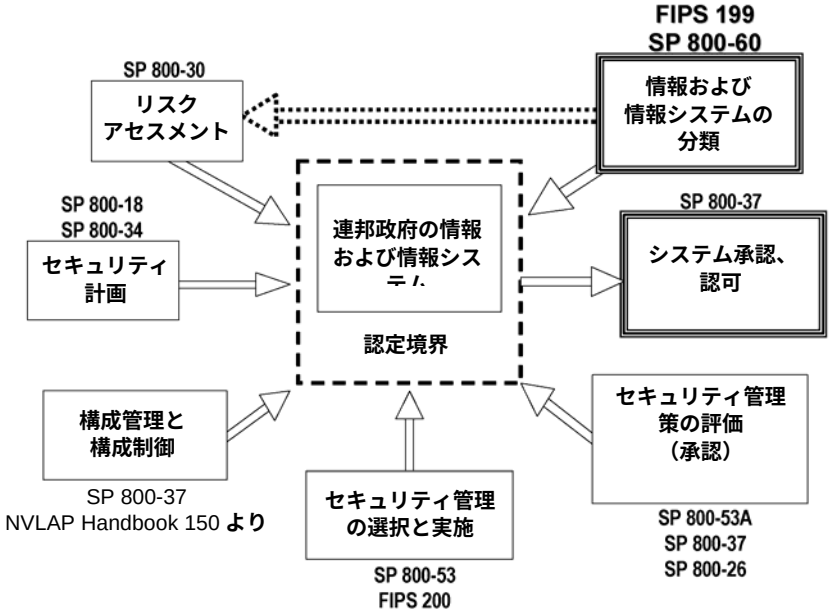

図 2：情報セキュリティ構想における FIPS 199 および SP 800-60 の役割

3.2 情報タイプの識別

以下は、情報タイプの識別に用いることができるとして提案された方法論である。

- レビュー対象のシステムによって実施される基本的な業務分野（管理・支援）または任務分野（任務別）を識別する
- 業務分野または任務分野ごとに、システムの目的を機能の観点から表す運用または業務項目を識別する
- 各運用分野または業務項目を実施するのに必要な下位機能を識別する
- 識別した下位機能に関連する基本情報タイプを選択する
- 必要に応じて、特別な扱い（許可のない開示または伝播に関してなど）をするように法律、大統領令、または政府機関の規制で義務づけられた、システムによって処理される情報タイプを識別する。本情報は、情報タイプまたはシステムの影響レベルの調整に使用することができる。

「業務分野」は、政府活動を、政府の目的、その目的を達成するために使用する仕組み、政府活動の実施に必要な支援機能、および政府の事業のあらゆる分野を支援する資源管理機能に関する高次のカテゴリに区分する。「業務分野」は、「運用分野」または「業務項目」に細分される。

「運用分野」または「業務項目」は、機能の観点から政府の目的を表す、あるいは政府が国民サービスを効果的に提供するために実施しなければならない支援機能を表す。政府の目的および政府がその目的を達成するために使用する仕組みに関する*業務項目*は、任務別となる傾向がある。任務別情報タイプの暫定リストは、付録 D で提供する。

政府活動の実施に必要な支援機能および資源管理機能に関する*業務項目*は、ほとんどの政府機関に共通する傾向がある。行政管理予算局（OMB: Office of Management and Budget）の連邦政府 EA 管理室（Federal Enterprise Architecture Program Management Office）の資料『*The Business Reference Model Version 2.0 (BRM)*』で識別されている管理・支援業務項目は、本文書の第 5 章に記載する。これらの「業務項目」のそれぞれの定義は、付録 C で提供する。

*下位機能*は、各運用分野または業務項目においてシステムサービスが提供する基本的な操作である。任務別業務項目のコンポーネントである下位機能の例は、付録 D でいくつか記述する。*BRM* で業務項目ごとに識別されている管理・支援下位機能は、第 5 章に記載し、付録 C で定義する。また、記載した下位機能ごとに情報タイプを識別する（OMB *BRM* は時々改訂されることがあるが、*BRM* の変更がすべて本ガイドラインで採用している情報分類法の変更につながるとは限らない）。

特定の情報タイプに対して秘匿度または重大性の保護要件を規定する根拠となる法律および大統領令は、付録 E に記載する。

本ガイドラインでは、多数の情報タイプを識別し、*BRM* の Version 2.0 に基づいて分類しているが、おそらく単一のシステムによって処理されるのは、識別したタイプのうちのほんのわずかである。また、各システムは、記載されている情報タイプのいずれかにうまく分類されない情報を取り扱う可能性がある。本ガイドラインで識別する一連の情報タイプを選択した後、レビュー対象の各システムによって処理される情報をレビューして、影響アセスメントのために追加のタイプを識別する必要があるかどうかを確かめたほうがよい。

3.3 暫定的影響レベルの選択

管理・支援情報タイプの機密性、完全性、および可用性への暫定影響レベルは、付録 C で提案する。また、いくつかの任務別情報タイプの暫定影響レベル割り付けの例は、付録 D で提供する。システムによって処理される情報タイプが本ガイドラインによって分類されていない場合、その影響を初めに決めるには、FIPS 199 の規格に基づいて行う必要があろう。

3.3.1 FIPS 199 のセキュリティ分類規格

政府機関は、本ガイドラインに記載されていない情報タイプを識別しても、付録 C（管理・支援情報タイプ）または付録 D（任務別情報タイプ）から暫定影響レベルを選択しなくてもよい。前記の場合、政府機関は、表 1「連邦政府の情報および情報システムの分類」に示す FIPS 199 の規格を用いて暫定影響レベルを決定する。

表 1：連邦政府の情報および情報システムの分類

セキュリティ目標	潜在的影響 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］	許可のない情報の開示が、組織の運営、組織の資産、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。	許可のない情報の開示が、組織の運営、組織の資産、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。	許可のない情報の開示が、組織の運営、組織の資産、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］	許可のない情報の改変または破壊が、組織の運営、組織の資産、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。	許可のない情報の改変または破壊が、組織の運営、組織の資産、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。	許可のない情報の改変または破壊が、組織の運営、組織の資産、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中断・途絶が、組織の運営、組織の資産、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中断・途絶が、組織の運営、組織の資産、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中断・途絶が、組織の運営、組織の資産、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。

政府機関は、機密性、完全性、および可用性の侵害の潜在的影響について、表 1 から適切な値を選択し、調整することにより、情報タイプおよび情報システムにセキュリティ分類を割り付けることができる。影響の選択およびその後のセキュリティ分類の責任者は、みずからが責任を負う各システムが受信、処理、蓄積、および／または生成する各情報タイプに、表 1 が提供する規格を適用する。一般に、セキュリティ分類は、レビュー対象のシステムが受信、処理、蓄積、および／または生成する、最も機密にかかわるまたは最も重要な情報に基づいて決定される。

3.3.2 FIPS 199 に基づく影響レベル選択の例

情報タイプおよびシステムの例に対する、FIPS 199 に基づく影響選択およびセキュリティ分類の例を以下に示す。

例 1：Web 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。Web

SC 公開情報 ＝ {(機密性，該当なし)，(完全性，中位)，(可用性，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 調査情報 ＝ {(機密性，高位)，(完全性，中位)，(可用性，高位)}

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 管理情報 ＝ {(機密性，低位)，(完全性，低位)，(可用性，低位)}

一般に、影響アセスメントは、セキュリティ侵害の結果を低減するために用いられる仕組みに依存しない。

3.3.3 影響レベルの選択に関するそのほかの要因

FIPS 199 の判断基準に基づいてローカルなアプリケーションの影響レベルおよびセキュリティ分類を想定する場合、政府機関は、各情報タイプのセキュリティ影響に関して以下の質問および要因を考慮することが推奨される。

共通機密性要因：

表 1 に要約した FIPS 199 の影響の分類規格を使用して、以下の質問に対する回答に関連して情報タイプごとに低位／中位／高位の影響を評価する。

- 悪意のある敵対者がその情報をどのように使用して、機関の活動、機関の資産、または個人に限定的／重大／致命的な損害を与える可能性があるか。

- 悪意のある敵対者がその情報を使用して、どのように許可のない情報の改変、情報の破壊、またはシステムサービスの妨害につながる可能性がある機関の資産を制御し、その結果、機関の活動、機関の資産、または個人に限定的／重大／致命的な損害をもたらす可能性があるか。

- 許可のないその情報タイプの要素の開示／伝播は、法律、大統領令、または機関の規制に違反することになるか。

機密性への影響レベルを決定する際には、情報タイプの利用およびそのタイプに属するさまざまな既知の情報を考慮する。

共通完全性要因：

表 1 に要約した FIPS 199 の影響の分類規格を使用して、情報タイプごとに、(i) そのタイプに属するさまざまな既知の情報 (ii) レビュー対象のシステムによる情報の各利用の許可されない改変または破壊に伴う低位／中位／高位の影響 について評価する。

情報の許可のない改変または破壊は多様な形態を取りうる。改変は巧妙で検出が困難である場合、大規模に発生する場合もある。情報の改変およびそれにより起こる結果は、非常に広範囲にわたると想定することができる。以下は、情報が偽造または改変された結果についてほんの一部の例を示している。

- 政府機関への公共の信頼の低下

- 財務利益の不正な計上

- 不正または不正確な手順が公表されたことによる混乱または論争の発生

- 不正または虚偽の方針による混乱または論争の誘発

- 人事決定への影響

- 法執行または法的手続きへの干渉または操作

- 立法への影響行使

- 政府の情報または施設への許可のないアクセス

ほとんどの場合、完全性の侵害の最も重大な影響は、改変された情報に基づいて何らかの活動が行われたとき、または改変された情報がほかの組織または一般人に伝播されたときに発生する。

完全性の損失が検出されないことは、多くの情報タイプにとって壊滅的な結果をもたらす可能性がある。完全性の侵害の結果は、直接的（例：財務帳簿、医療警告、または犯罪記録の改変）、または間接的（例：機密にかかわる情報または個人情報への許可のないアクセスの容易化や、情報または情報システムサービスへのアクセス妨害）であることがある。情報および情報システムへの書込み権限のあるアクセスの悪用は、政府機関の任務に多大な損害を与える可能性があり、さらに政府機関のシステムをほかのシステムへの攻撃の踏み台として利用するために用いられる可能性もある。

多くの場合、政府機関の任務機能および政府機関への公共の信頼に対する情報の許可のない改変または破壊は、限定的と予想される。そうでない場合、完全性の侵害は人命の危険またはそのほかの致命的な結果を招く場合がある。決定的に時間に依存する情報の場合、その影響は特に致命的なものとなる可能性がある。

共通可用性要因：

表 1 に要約した FIPS 199 の影響分類規格を使用して、情報タイプごとに、(i) そのタイプに属するさまざまな既知の情報 (ii) レビュー対象のシステムによる情報の各利用の可用性の損失に伴う低位／中位／高位の影響について評価する。

多くの情報タイプおよび情報システムの場合、可用性に関する影響レベルは情報またはシステムが利用できない期間の長さに依存する。可用性の損失が検出されないと、多くの情報タイプにとって壊滅的な結果をもたらす可能性がある。例えば、予算執行、緊急時対応計画、運用の継続性、サービス復旧、債権回収、租税管理、人事管理、給与管理、セキュリティ管理、在庫管理、物流管理、会計情報などに関するデータベースの永久的な損失は、ほぼすべての政府機関にとって壊滅的なものとなるだろう。当該データベースを完全に復元するには、多大な時間と費用がかかることになる。政府機関の活動の中断・途絶は、重大もしくは致命的なものとなろう。

可用性の侵害が限られた時間の場合は、政府機関の任務機能および政府機関への公共の信頼に対する悪影響は、ほとんどの場合、限定的なものであろう。その一方で、時間に決定的に依存する情報タイプの場合、機関の資産、運用、または要員に（あるいは公共福祉に）重大な損害が及ぶ前に可用性が回復する可能性は低い。このような特性のために、可用性に対する影響レベルの度合いは、ほとんどの場合、その情報が時間に決定的に依存するかどうかの度合いである。

3.4 情報への影響レベルのレビューおよび調整／確定

政府機関は、特に第 5 章または付録 D で推奨するセキュリティ分類の影響レベルを暫定的レベルとして適用する場合、レビュー対象のシステムに関連する組織、環境、任務、利用、および接続性に関連づけて、暫定影響レベルの適切性をレビューする。本文書のセクション 3.3 で示した FIPS 199 の規格は、暫定的影響レベルの調整または確定に関する判断の基礎として使用する。機密性、完全性、および可用性影響レベルは、レビューの過程で何回でも調整することができる。すべての情報タイプのレビューおよび調整プロセスが完了したら、情報タイプ別の影響レベルのマッピングを確定することができる。

特定のタイプの情報の侵害の影響は、政府機関間によって、または運用状況によって異なる場合がある。また、その情報タイプの影響は、ライフサイクル全体にわたって変化する可能性がある。例えば、契約期間中は機密性影響レベルが*中位*である契約情報は、契約が完了したら影響レベルが*低位*になる可能性がある。方針情報は、方針策定プロセスでは機密性影響レベルと完全性影響レベルがともに*中位*であっても、方針が実施されたら機密性影響レベルが*低位*になり（完全性影響レベルは*中位*のまま)、さらにその方針が用いられなくなったら機密性影響レベルと完全性影響レベルがいずれも*低位*になる可能性がある。

3.5 システムセキュリティ分類

システムによって処理される個々の情報タイプごとに影響レベルを選択し終えたら、システムセキュリティ分類を割り付ける必要がある。

3.5.1 FIPS 199 のシステム分類プロセス

FIPS 199 では、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としている。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 。

情報システムは、プログラムと情報の両方からなる。情報システム内で実行されるプログラム（システムプロセス）は、情報の処理、蓄積、および伝送を容易にするものであり、組織が任務に関連する必須の機能および操作を実行するのに必要なものである。これらのシステム処理機能も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。ただし、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する*最悪*の潜在的影響により分類することとし、よって情報システムのセキュリティ分類に際してシステムプロセスを考慮する必要性をなくす。

これは、以下の認識によるものである。

- 完全性、可用性、ならびにパスワードや暗号鍵などの重要情報の場合はシステムレベルの処理機能および情報の機密性を最高水準で保護するという基本的な要件
- 完全性、機密性、および可用性間の強い相互依存性

このため、FIPS 199 では、「該当なし」の値は、システムによって処理される特定の情報タイプには適用できるが、その値を情報システムのセキュリティ目標に割り付けることはできないと指摘している。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。

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 情報システム ＝ {(機密性，*影響*)，(完全性，*影響*)，(可用性，*影響*)}

ここで、潜在的影響の許容値は「低位」、「中位」、「高位」である。

システム例 1：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 契約情報 ＝ {(機密性，中位)，(完全性，中位)，(可用性，低位)}

および

SC 管理情報 ＝ {(機密性，低位)，(完全性，低位)，(可用性，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 調達システム ＝ {(機密性，中位)，(完全性，中位)，(可用性，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。

システム例 2：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。

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

および

SC 管理情報 ＝ {(機密性，低位)，(完全性，低位)，(可用性，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。

SC SCADA システム ＝ {(機密性，低位)，(完全性，高位)，(可用性，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。

SC SCADA システム **＝ {(機密性，中位)，(完全性，高位)，(可用性，高位)}**

3.5.2 システム分類のガイドライン

一般に、システムに対する影響レベルは、システムの情報タイプの集合に関連するセキュリティ目的（機密性、完全性、および可用性）における最高値または潜在的影響の最大値である。*情報システム*は通常、さまざまな情報タイプ（例：プライバシー、医療、専有、財務、請負業者機密）を取り扱う。これらの情報タイプはそれぞれセキュリティ分類の対象となる。場合によっては、システムのセキュリティ分類が、システムによって処理されるあらゆる情報タイプの影響レベルよりも高くなることがある。システム全体のセキュリティ分類が通常、それを構成する情報タイプのセキュリティ分類より高くなる主な要因は、集約、接続性、およびきわめて重要なシステム機能にある。本章では、集約、きわめて重要な機能性、およびそのほかのシステム要因がシステムセキュリティ分類に影響を及ぼす可能性について、いくつかの一般的指針を提供する。

影響割り付けプロセスでは、機密度／重大度の経時的変化を計算に入れる必要があろう。情報によっては、時間がたつとその秘匿度を失うものもあれば（例：公表後の経済／商品予測）、ある時点で特に重要になるものもある（例：航空機の着陸操作中の空港進入区域内の気象データ）。

システムレベルの影響アセスメントに関する決定には、さまざまな利害関係者（例：経営陣、運用要員、セキュリティ専門家）が関与する必要があろう。システムレベルの影響を判断する際、情報集約、きわめて重要なシステム機能、およびそのほかの要因を考慮する。

3.5.2.1 集約

情報によっては、単独では秘匿度がほとんど、または全くないが、集約したら秘匿度が高くなるものがある。場合によっては、大量の単一の情報タイプを集約したら、機密にかかわるパターンおよび／または計画が明らかになったり、機密にかかわるシステムまたはきわめて重要なシステムへのアクセスが容易になったりする可能性がある。そのほかにも、一見無害と思われる異なるタイプの情報の集約が、同様の効果を示す場合がある。一般に、特定のデータ要素の秘匿度は、単独でよりも情報が集まることによって高くなることが多い（例：口座番号と個人および／または機関の識別情報の関連づけ）。データ集約・推論ツールの入手可能性の向上、日常の運用への採用、および高度化はいずれも急速に進んでいる。情報集約に付随する秘匿度または重大度が高まったことがレビューによって明らかになった場合、システム分類を個々の情報タイプに関連する影響によって示されるレベルより高い値に調整する必要があろう。

3.5.2.2 きわめて重要なシステムの機能性

いくつかの情報タイプに対する侵害は、システムの基本機能に対しては影響が低位であっても、全体としてみた場合、その侵害に対する潜在的影響の値は、はるかに深刻なものである可能性がある。

- 問題のシステムが接続されているほかのシステム
- そのシステムの情報に依存するほかのシステム

影響が低位の情報のみを取り扱うシステムのアクセス制御情報は当初、低位の影響属性しか持たないとみなされるかもしれない。しかし、そのシステムへのアクセスがほかのシステムへの何らかの形でのアクセスする（例：ネットワークを介して）可能性がある場合、当該の間接アクセスが発生しうるすべてのシステムの秘匿度および重大性属性を考慮する必要がある。同様に、情報によっては、一般に低位の秘匿度および／または重大性属性のものであっても、きわめて機密にかかわる機能またはきわめて重要な機能に到達するために、ほかのシステムによってその情報が使用されることもありうる（例：航空交通管制における気象情報の利用や、商業飛行情報の利用による軍事輸送システムの識別)。データの完全性、可用性、時間的枠組み、またはそのほかの枠組みの損失は、壊滅的な結果をもたらす可能性がある。

3.5.2.3 そのほかのシステム要因

Web ページの完全性

ほとんどの連邦機関は、誰もがアクセスできる Web ページを開設している。それらの公開 Web ページの大多数では、サイトと閲覧者間の対話を可能にしている。情報提供のみの Web サイトもあれば、Web サイトを介して書類を提出できる場合や（例：サービス申請や求職)、サイトが商取引の媒体となる場合もある。外部との通信に影響を及ぼす情報（例：Web ページ、電子メール）の許可のない改変または破壊は、政府機関の活動および／または政府機関に対する公共の信頼に悪影響を及ぼす可能性がある。ほとんどの場合、損害は比較的短期間で回復することができ、限定的である（影響レベルは*低位*)。そのほかの場合（例：非常に大規模な不正行為や、諜報／セキュリティコミュニティコンポーネントに属する Web ページの改変)では、政府機関の任務機能および／または政府機関に対する公共の信頼に対する損害が重大なものとなる可能性がある。前記の場合、公開 Web ページの許可のない改変または破壊に伴う完全性への影響は最低でも*中位*ということになろう。

システム可用性の壊滅的損失

主要資産の物理的破壊と論理的破壊のいずれも、資産の回復に非常に多額の出費を要する、および／または復旧に長時間を要する結果となる可能性がある。情報システム能力の永久的な喪失／利用不能は、機関の活動を著しく阻害し、さらに直接的な公共サービスにかかわる場合には、連邦機関に対する公共の信頼に致命的な悪影響を及ぼす可能性がある。特に大規模システムの場合、システム可用性の壊滅的損失は、結果的に可用性への影響が*高位*となることを FIPS 199 の規格は示唆している。システム可用性の影響レベルを*高位*とする（また、その結果としてシステムセキュリティ分類を*高位*とする）かどうかは、そのシステムによって処理される情報タイプの影響レベルよりもむしろシステムの費用および重大性属性によって決まる。

きわめて重要なインフラストラクチャおよび主要国家資産

情報システムが果たす任務、または取り扱う情報がきわめて重要な国家基盤または主要国家資産のセキュリティに影響を及ぼす場合、その侵害によってもたらされる損害に特に細心の注意を払う必要がある。この場合、セキュリティへの影響としては、物理的またはサイバーセキュリティ保護メカニズムの有効性の大幅な低下や、きわめて重要なインフラストラクチャおよび／または主要資産へのテロリストの攻撃が容易になることなどがあげられる。したがって、機密性、完全性、または可用性の損失が以下のようなインフラストラクチャのコンポーネントおよび資産に悪影響をもたらす場合、その影響レベルを慎重に判断するべきである。

きわめて重要なインフラストラクチャ

- 農業および食糧（農場および食品加工工場を含む）
- 水（連邦の貯水池および地方自治体の下水処理施設を含む）
- 公衆衛生（病院および連邦保健機関を含む）
- 救急サービス（連邦、州、および地方自治体の対応部署を含む）
- 防衛施設および防衛産業基盤
- 電気通信（交換および伝送／ケーブル設備を含む）
- エネルギー（発電・送電設備および石油／ガス生産・輸送設備を含む）
- 輸送（航空、鉄道、幹線道路、パイプライン、海運、および公共輸送機関）
- 銀行／金融（連邦サービスおよび連邦預金保険公社（FDIC）加盟機関を含む）
- 化学工業／危険物（例：化学プラント）
- 郵便および運送施設

主要資産

- 原子力発電所
- 国定史跡および国家の象徴
- ダム
- 政府施設
- 商業資産

2002 年 11 月 25 日に成立した公法 107-296 の第 211～215 条、*2002 年の重要情報基盤法*（合衆国法典第 6 編第 131～134 条として法令化）では、「きわめて重要な基盤（インフラストラクチャ）情報」という用語を、通常公開されない、きわめて重要なインフラストラクチャまたは保護されたシステムのセキュリティに関係する情報を意味すると定義している。同法では、重要なインフラストラクチャや保護されたシステムのセキュリティ、分析、警告、相互依存性調査、復旧、復元、またはそのほかの情報目的のために連邦機関が使用するようにと、任意で提出された、きわめて重要なインフラストラクチャ情報（提出者または提出組織の識別情報を含む）、について、同法によって定義された明示的宣言を伴う場合、以下のとおり定めている。

(1) 合衆国法典第 5 編第 552 条（一般に情報自由法と呼ばれる）に基づく開示から除外しなければならない
(2) 政策決定当局者との一方的情報伝達に関する機関の規則または司法の見解に従ってはならない
(3) 当該の情報が善意で提出された場合、連邦法または州法に基づいて提起された民事訴訟において、当該の政府機関、そのほかの連邦、州、または地方当局、あるいは第三者が、当該の情報の提出者または提出組織の書面による同意なしに直接使用してはならない
(4) 合衆国の公務員または職員が、本法の目的以外の目的で、当該の情報の提出者または提出組織の書面による同意なしに使用または開示してはならない[8]
(5) 州または地方の政府もしくは政府機関に提供された場合、情報または記録の開示を義務づける州または地方の法律に基づいて提供すること、さもなければ、州または地方の政府もしくは政府機関が当該の情報の提出者または提出組織の書面による同意なしに開示または配付すること、あるいはきわめて重要なインフラストラクチャまたは保護システムの保護もしくは犯罪行為の捜査または訴追の促進以外の目的で使用してはならない

なお、企業秘密の保護など、法律の定めるところにより適用される特権または保護の適用除外には当たらない。

プライバシー情報

*2002 年の電子政府法*は、*1974 年のプライバシー法*のプライバシー保護要件を強化した。これらの公法の条項により、連邦政府機関は、個人に関する情報の収集、伝播、または開示に対して明確な責任を負う[9]。

2003 年 9 月 29 日の OMB 覚え書き『OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002』は、2002 年の電子政府法のプライバシー規定を実施するものである。その指針は、氏名、住所、電話番号、社会保障番号、および電子メールアドレスなど、認識できる形で個人を識別する情報に適用される。OMB は、政府機関の長に対して、「個人情報の保護をアメリカ国民に保証するために、個人が電子的に提供する情報を政府がどのように取り扱うかを記述する」ように指示した。これらの公法および行政方針を受けて、「許可のない開示」の定義を広げる必要がある。新しい定義には、プライバシー法および方針によってプライバシー保護情報の共有が禁止されている連邦政府機関のあいだで、プライバシー保護情報を*形態を問わず*共有することも含める。ほとんどのプライバシー規制が情報の共有または開示に重点を置いていることから、本ガイドラインではプライバシーの考慮を機密性影響レベルに影響を及ぼす特殊要因として扱う。各情報タイプに対して機密性影響レベルを確立する際、責任者は許可のないプライバシー情報の開示の結果を考慮しなければならない（連邦の方針および／または法律の違反に関して）。

[8] 犯罪行為の捜査または訴追の促進が目的である場合、あるいは会計検査院の職務遂行の過程で上院、下院、または会計検査院長に情報を開示する場合を除く。
[9] OMB による個人の定義は、「合衆国国民または永住が合法的に認められた外国人」である。政府機関は、プライバシー法および電子政府法の保護対象を、企業、個人事業主、外国人などに拡大することを選択してもよい。

なお、プライバシー情報を扱う管理・支援情報タイプは 4 種類である。

現在、政府機関は、識別可能な情報を含む IT システムを開発する前、または識別可能な情報を電子的に収集する前に、新しいプライバシー影響アセスメント（PIA）を実施することが義務づけられている。個人を特定できる情報を政府機関が取り扱う方法を変更することによって新たなプライバシーリスクが生じる場合、PIA を更新しなければならない。影響を受ける政府機関は、その電子プライバシー関連の活動について毎年報告することが義務づけられている。

政府機関は、その Web サイトにおいて、来訪者に以下のことを告知することが義務づけられる。

- 情報の提出が自発的である場合
- 自発的に提出された個人データを政府機関が使用することに承諾を与える方法
- プライバシー法およびそのほかの適用法が来訪者に認める権利

政府機関の Web サイトでは、以下のことを開示することが義務づけられる。

- 収集する情報の種類
- 情報収集の目的および収集した情報の利用法
- 収集した情報の共有の有無および共有先
- 収集した情報に適用されるプライバシーセーフガード

プライバシー侵害の影響は、ひとつには関連する法律および方針の違反に対する刑罰に依存する。ほとんどの場合、影響は*中位*の範囲に分類される。分類をレビューして、影響の決定に際して侵害の結果が十分に考慮されていることを保証する。

企業秘密

許可のない企業秘密の開示を明確に禁止している法律がいくつかある（例：合衆国法典第 7 編第 6 章第 II 節第 136 条 h や合衆国法典第 42 編第 6A 章第 XII 節第 E 部第 300j-4 条(d)(1)）。一般に、企業秘密を蓄積、伝達、または処理するシステムには、最低でも*中位*の機密性影響レベルを割り付ける。

（本ページは意図的に白紙のままとする）

4.0 任務別情報に対する影響レベル割り付けのガイドライン

本章では、任務別情報タイプを識別するプロセスと、許可のない当該情報の開示、改変、または利用不可の影響を特定するプロセスを記述する。任務別情報は、任務情報と政府がその任務を達成するために使用する仕組みに関連する情報の両方を含む。任務別情報タイプは、本質的に、個々の省庁および政府機関に固有か、あるいは一連の特定省庁および政府機関に固有のものである。多くの省庁および政府機関に共通する運営および管理情報タイプについては、第 5 章「管理・支援情報のタイプ別影響レベル」で述べる。

4.1 任務別情報タイプの識別

連邦政府は、さまざまな情報タイプを調達、生成、処理、および蓄積する。連邦政府の情報および情報システムのタイプとセキュリティ目標および影響レベルへのマッピングにおける最初のステップは、情報分類法の開発、つまり情報タイプのカタログの作成である[10]。

ほとんどの連邦政府の情報および多くの情報システムは、サービス提供のために直接使用される。政府機関レベルで任務別情報タイプを確立するアプローチの 1 つは、まずその政府機関の業務分野および任務分野を文書化することである。その後、各業務分野および任務分野の遂行に必要な主要下位機能を定義できる。例えば、政府機関によって遂行される任務の 1 つに法執行がある。その政府機関の法執行任務の一部である下位機能として、犯罪捜査および監視、犯罪者逮捕、犯罪者拘禁、市民保護、犯罪防止、資産保護などがあげられる。これらの下位機能がそれぞれ 1 つの情報タイプに該当することもありうる。任務別情報システムによって実行されるいくつかの業務分野と任務分野、およびその構成要素である下位機能については、付録 D「任務別情報および情報システムの影響決定の例」で識別する。

各システムの所有者、または所有者によって指名された担当者は、そのシステムに蓄積され、そのシステムによって処理、または生成される情報タイプを識別する責任がある。任務別情報の場合、責任者は、管理、運用、およびセキュリティの利害関係者と協調して、その政府機関によって遂行される包括的な一連の業務項目および任務分野、ならびに政府機関の業務の遂行および／または政府機関の任務の達成に必要な機能および下位機能をまとめる。業務項目または任務分野の下位機能がそれぞれ、1 つの情報タイプに該当する[11]。

[10] 分類活動に付随する課題の 1 つは、どこまで細分化するかを決定することである。カテゴリが広範すぎると、影響レベル割り付けのガイドラインは大まかすぎて役に立たない可能性が高い。とはいえ、各政府機関によって処理される情報の要素ごとにガイドラインを提供しようとした場合、ガイドラインは扱いにくくなり、頻繁な変更が必要になるおそれがある。

[11] 付録 D では、OMB 連邦政府 EA 管理室の『*Business Reference Model 2.0*』で識別されている業務項目および下位機能に基づいて、連邦政府の任務情報タイプを提供する。

4.2 任務別情報の影響アセスメント

直接サービス任務は、任務別情報および情報システムの影響レベルおよびセキュリティ目標を想定する際の基本リファレンス枠を提供する。許可のない情報の開示、完全性の侵害、およびサービス妨害の結果は、提供または支援されるサービスの性質および受益者（集団）ごとに定義される。すべての政府機関は少なくとも 1 つの任務を遂行し、付録 D に記載されたサービス提供メカニズムの少なくとも 1 つを採用している。また、いくつかの任務分野にわたってさまざまな任務を遂行している機関もある。直接サービスシステムは、任務別情報（例：任務情報）だけでなく、政府機関共通の*管理・支援*情報も取り扱う。

影響の決定に責任を負う団体は、システムごとに識別した各任務別情報タイプに、影響レベルおよびそれを反映したセキュリティ分類を割り付けなければならない。このとき、セクション 2.1.2 で識別したセキュリティ目標および潜在的損失のタイプに対して、セクション 2.2.1 で識別した影響選択基準を使用する。最終的なシステムセキュリティ分類は、そのシステムに蓄積され、そのシステムによって処理、または生成される各情報タイプの影響レベルのほかに、セクション 3.5 で述べた要因に基づく。

機密性目標に固有の要因は、特別な扱いを受ける情報である（例：合衆国法典第 5 編第 552A 条、1974 年のプライバシー法の適用対象となる情報）。当該の情報を蓄積、処理、または生成するあらゆる情報システムには、そのほかの考慮事項にかかわらず、何らかの最低限の機密性影響レベルを割り付けなければならない。前述の情報の例としては、企業秘密法の適用対象となる情報、プライバシー法の適用対象となる情報、エネルギー省の*セーフガード*の対象となる情報、内国歳入庁の公式使用限定情報、環境保護庁の機密業務情報（例：有害物質規制法、資源保全再生法、包括的環境対処補償責任法の適用対象）などがある。これらの法律および規制の規定のいくつかは、付録 E「秘匿度／重大度を確立する根拠となる法律および大統領令」に記載されている。

5.0 管理・支援情報のタイプ別影響レベル

ほとんどの連邦政府情報および多くのシステムは、国民サービスの提供のために直接使用するのではなく、主に資源管理またはサービス提供を支援することを目的としている。本章では、連邦政府情報の一連の情報タイプを勧告する。*管理・支援*情報タイプに対して推奨する暫定的なセキュリティ分類は、その裏づけとなる根拠とともに付録 C で示す。第 4 章で述べたように、情報タイプは OMB 連邦政府 EA 管理室が 2003 年 6 月に公開した資料『*The Business Reference Model Version 2.0 (BRM)*』に基づいて識別する。*BRM* には、4 つの業務分野にわたって 39 の政府業務項目が記述されている。業務分野とは、以下に関する高次のカテゴリである。

- 政府の目的（*任務*または*国民サービス*）
- 政府がその目的を達成するために使用する仕組み（*提供形態*）
- 政府の運営に必要な支援機能（*サービス提供支援*）、および
- 政府の事業のあらゆる分野を支援する資源管理機能（*資源管理*）

*サービス提供支援*および*資源管理*業務分野は、全体で 13 の業務項目で構成される。*BRM* では、その業務項目を 63 の下位機能に細分している。*サービス提供支援*および*資源管理*業務分野はほとんどの連邦政府機関に共通であり、本ガイドラインではそれらの各下位機能に関連する情報は、*管理・支援*情報タイプとして識別されている[12]。プライバシー情報を扱う 4 つの*管理・支援*情報タイプ、および行政機能情報を扱う 1 つの*管理・支援*情報タイプの定義が追加されている。すべての*管理・支援*情報タイプに関する機密性、完全性、および可用性の暫定的情報分類は付録 C で勧告する。また、推奨する暫定影響レベルに関する提案の基礎となる根拠も付録 C に記述する。そのほかにも、各政府機関で追加の情報タイプを識別し、それらのタイプに影響レベルを割り付けることが必要になるかもしれない。

任務別情報の場合と同様に、*管理・支援*情報および情報システムのタイプとセキュリティ目標および影響レベルへのマッピングにおける最初のステップは、そのシステムに蓄積され、そのシステムによって処理、または生成される情報タイプを識別することである。その次のステップは、適用される情報タイプごとに影響レベルおよびそれを反映したセキュリティ分類を選択することである。このとき、セクション 2.1.2 で識別したセキュリティ目標の枠組みのなかで、セクション 2.2.1 で識別した基準を使用する。システムセキュリティ分類は、そのシステムに蓄積され、そのシステムによって処理、または生成される情報タイプごとの各セキュリティ目標に関連する影響レベルのほかに、システムレベルの影響の想定を左右する追加要因に基づく（セクション 3.5 を参照）。

[12] *国民サービス*および*提供形態*業務項目の下位機能に関連する情報タイプは政府機関固有であり、第 4 章「任務別情報に対する影響レベル割り付けの指針」で扱う。

例えば、構成およびセキュリティポリシー実施情報は、パスワードファイル、ネットワークアクセスルール、そのほかのハードウェアおよびソフトウェア構成設定、その情報システムのデータ、プログラム、および／またはプロセスへのアクセスに影響を及ぼす可能性がある資料などを含む。当該の一連の情報およびプロセスは、システムの情報およびプロセスの破損、誤使用、または乱用につながる可能性があるため、最低でも低位の機密性影響レベルが適用される。

表 2 に、*管理・支援*業務項目および情報タイプを示す。

表 2：管理・支援業務項目および情報タイプ
サービス提供を支援する情報

管理・監督
是正措置（方針／規制）
プログラム評価
プログラム監視

規制整備
方針・ガイドライン策定
パブリックコメント追跡
規制作成
規則公表

計画作成・資源割り当て
予算編成
資本計画
エンタープライズアーキテクチャ
戦略計画
予算執行
人員計画
管理改善

内部リスク管理・低減
緊急時対応計画
運用継続
サービス復旧

公報
顧客サービス
公式情報伝播
成果のアウトリーチ活動
広報活動

歳入徴収
債権回収
受益者負担金徴収
連邦資産売却

立法関係
立法追跡
立法証明
法案作成
議会連絡

一般政府
中央財政運用
立法機能
行政機能
中央資産管理
中央人事管理
租税管理
中央記録・統計管理
収入情報
個人識別・認証
受給資格事象情報
代理受取人情報

政府資源管理情報

人的資源管理
給付管理
人事管理
給与管理・経費精算
人的資源訓練・開発
セキュリティ資格管理
職員募集・採用

運営管理
施設・車両・装置管理
ヘルプデスクサービス
セキュリティマネジメント
出張旅行
職場方針策定・管理

情報・技術管理
システム開発
ライフサイクル／変更管理
システム保守
IT インフラストラクチャ保守
IT セキュリティ
記録保管
情報管理

財務管理
会計
予算・財務
支払い
徴収・未収
資産・負債管理
報告・情報

サプライチェーン管理
物品調達
在庫管理
物流管理
サービス調達

5.1 サービス提供を支援する情報

サービスの提供を支援する業務と資源管理業務の両方に使用されているほとんどの情報システムは、表 2 で識別した 8 つのイタリック体の*サービス提供支援*業務項目の 1 つ以上に関係する。以下に、*サービス提供支援*下位機能に関連する各情報タイプを記述する。機密性、完全性、および可用性の暫定影響レベルは、付録 C.2「サービス提供支援機能」で勧告する。

これらのサービス支援機能は、連邦政府の業務を支援するための重要な方針、計画、および管理基盤を提供する際に必要であり、日常的に使用される。*サービス提供を支援する*業務分野に関連する情報の侵害に伴うセキュリティ影響を想定する際には、そのサービス支援機能によって最終的に支援される直接サービス任務およびその受益者が重要な要因となる。

5.1.1 管理・監督

管理・監督情報は、連邦政府および外部ビジネスパートナーの業務およびプログラムが、適用される法律および規制を遵守していることを保証し、浪費、不正、および悪用を防止するために使用される。

5.1.1.1 是正措置情報タイプ

是正措置情報は、所定の法律、規制、または方針を遵守していないことが判明したプログラムの修正に必要な是正機能をサポートする。機密性、完全性、および可用性に対する影響レベルは、ほとんどの場合、是正措置情報の、許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、所定の法律、規制、または方針を遵守していないことが判明した内部または外部のプログラムを修正する主管政府機関の能力に関するものである。

5.1.1.2 プログラム評価情報タイプ

プログラム評価情報は、内部および外部のプログラムの有効性分析、および是正措置の妥当性を判断することをサポートする。ほとんどの場合、機密性、完全性、および可用性影響レベルは、プログラム評価情報の、許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、内部および外部のプログラムの有効性を分析し、適切な是正措置を決定する主管政府機関の能力に関するものである。

5.1.1.3 プログラム監視情報タイプ

プログラム監視情報は、内部および外部のプログラムの有効性、ならびに適用される法律、規制、および方針の遵守の程度を判断するのに必要なデータ収集活動をサポートする。ほとんどの場合、影響レベルはプログラム監視情報の、許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、データ収集活動を実行する主管政府機関の能力に関するものである。これらの活動は、内部および外部のプログラムの有効性、ならびに関連する法律、規制、および方針の遵守の程度を決定する。

5.1.2 規制整備

規制整備情報は、法律を施行するための規制、方針、およびガイドラインの策定における立法プロセスへの情報の提供に関連する活動をサポートする。

5.1.2.1 方針・ガイドライン策定情報タイプ

方針・ガイドライン策定情報は、規制の解釈および実施を支援するガイドラインの作成および普及をサポートする。ほとんどの場合、方針およびガイドライン策定任務遂行能力の損失が公共福祉に及ぼす影響は、即座ではなく遅れて現れると予想されるため、結果として人命または主要国家資産の損失が発生する可能性は比較的低い。ほとんどの場合、影響レベルは方針・ガイドライン情報の、許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、規制の解釈および実施を支援するガイドラインを作成および普及する主管政府機関の能力に関するものである。

5.1.2.2 パブリックコメント追跡情報タイプ

パブリックコメント追跡情報は、規制案に関するパブリックコメントの募集、維持、および回答活動をサポートする。ほとんどの場合、影響レベルはパブリックコメント追跡情報の、許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、規制案に関するパブリックコメントを募集、維持、および回答する主管政府機関の能力に関するものである。

5.1.2.3 規制作成情報タイプ

規制作成情報は、規制案および最終的な規制の調査および起草活動をサポートする。ほとんどの場合、影響レベルは規制作成情報の、許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、規制案および最終的な規制を調査および起草する主管政府機関の能力に関するものである。

5.1.2.4 規則公表情報タイプ

規則公表情報は、連邦官報および連邦規制集による規則案または最終的な規則の公表に関連するすべての活動をサポートする。ほとんどの場合、影響レベルは規則公表情報の、許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、連邦官報および連邦規則集で規則案または最終的な規則を公表する主管政府機関の能力に関するものである。

5.1.3 計画作成・資源割り当て

計画作成・資源割り当て情報は、戦略的方向の決定、変更を可能にするためのプログラムおよびプロセスの識別および確立、ならびにそれらのプログラムおよびプロセスのあいだでの資源（資本および労働力）の割り当て活動をサポートする。

5.1.3.1 予算編成情報タイプ

予算編成情報は、将来の支出の優先度を決定し、目標の期間における将来の財源および歳出の個別予測を作成するためのすべての活動をサポートする。これには、プログラムの有効性を査定し、予算優先度を決定するための実績情報の収集および使用を含む。ほとんどの場合、影響レベルは予算編成情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、将来の支出の優先度を決定し、目標の期間における将来の財源および歳出の個別予測を作成する主管政府機関の能力に関するものである。

5.1.3.2 資本計画情報タイプ

資本計画情報は、資本的経費に対して適切な投資が選択されることを保証するためのプロセスをサポートする。ほとんどの場合、影響レベルは資本計画情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、資本的経費に対して適切な投資が選択されることを保証する主管政府機関の能力に関するものである。

5.1.3.3 エンタープライズアーキテクチャ情報タイプ

エンタープライズアーキテクチャ情報は、現在の状態の記述、ならびに目標の状態および組織の人、プロセス、および技術の移行戦略を定義するための確立されたプロセスをサポートする。ほとんどの場合、影響レベルはエンタープライズアーキテクチャ情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、現在の状態の記述、ならびに目標の状態および組織の人、プロセス、および技術の移行戦略を定義する主管政府機関の能力に関するものである。

5.1.3.4 戦略計画情報タイプ

戦略計画情報は、長期最終目標の決定およびその目標を達成するための最良の手法の識別をサポートする。ほとんどの場合、影響レベルは戦略計画情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、長期目標を決定しその目標を達成するための最良の手法を識別する主管政府機関の能力に関するものである。

5.1.3.5 予算執行情報タイプ

予算執行情報は、政府機関の経費の日常的な要求および支出負担、請求書、請求をめぐる紛争の解決、調停、サービスレベル契約、および分担経費の配分をサポートする。ほとんどの場合、影響レベルは予算執行情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、政府機関の経費の日常的な要求および支出負担、請求書、請求をめぐる紛争の解決、調停、サービスレベル契約、および分担経費の配分を管理する主管政府機関の能力に関するものである。

5.1.3.6 人員計画情報タイプ

人員計画情報は、政府機関の戦略目標の達成に必要な人員の能力の識別およびその要件を満たすための戦略の開発プロセスをサポートする。ほとんどの場合、影響レベルは人員計画情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、政府機関の戦略目標の達成に必要な人員の能力の識別およびその要件を満たすための戦略の開発を行う主管政府機関の能力に関するものである。

5.1.3.7 管理改善情報タイプ

管理改善情報は、業務プロセスの現在の効率を評価し、リエンジニアリングまたはリストラクチャリングの機会を識別するためのすべての取り組みをサポートする。ほとんどの場合、影響レベルは管理改善情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、業務プロセスの現在の効率を評価し、リエンジニアリングまたはリストラクチャリングの機会を識別する主管政府機関の能力に関するものである。

5.1.4 内部リスク管理・低減

内部リスク管理・低減情報は、リスクにさらされることの分析および適切な対抗策の決定プロセスに関するすべての活動をサポートする。内部リスク管理・低減活動に関連するほとんどの情報に対するリスクは、広範囲のきわめて重要なインフラストラクチャおよび主要国家資産に関する侵害／損害への抵抗力および損害からの回復に本質的に影響を及ぼす可能性がある。

5.1.4.1 緊急時対応計画情報タイプ

緊急時対応計画情報は、損害を与える事象に対する計画、対応、およびその低減に必要な活動をサポートする。ほとんどの場合、影響レベルは緊急時対応計画情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、損害を与える事象に対する計画、対応、および低減を行う主管政府機関の能力に関するものである。

5.1.4.2 運用継続情報タイプ

運用継続情報は、きわめて重要なシステムおよびプロセスの識別、ならびに壊滅的な事象が発生した場合でも、それらのシステムおよびプロセスが利用可能であることを保証するのに必要な計画および準備に関連する活動をサポートする。ほとんどの場合、影響レベルは運用継続情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、重要システムおよびプロセスの識別、ならびに壊滅的な事象が発生した場合でも、それらのシステムおよびプロセスが利用可能であることを保証するのに必要な計画および準備を実行する主管政府機関の能力に関するものである。

5.1.4.3 サービス復旧情報タイプ

サービス復旧情報は、火災や地震などの大災害発生後の運用再開計画の作成に必要な内部活動をサポートする。ほとんどの場合、影響レベルはサービス復旧情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、火災や地震などの大災害発生後の運用再開計画を作成する主管政府機関の能力に関するものである。

5.1.5 公報

公報情報は、国民サービス、公共政策、および／または国益を直接支援する連邦政府機関、国民、および利害関係者のあいだの情報交換および情報伝達に関する活動をサポートする。

5.1.5.1 顧客サービス情報タイプ

顧客サービス情報は、政府の顧客に対する情報および支援の提供およびその管理に関連する活動をサポートする。ほとんどの場合、影響レベルは顧客サービス情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、政府の顧客に対する情報および支援の提供およびその管理を行う主管政府機関の能力に関するものである。

5.1.5.2 公式情報伝播情報タイプ

公式情報伝播情報は、各種媒体（例：ビデオ、書類、Web など）を利用して政府公式情報を外部の利害関係者に提供する取り組みをサポートする。ほとんどの場合、影響レベルは公式情報伝播情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、各種媒体（例：ビデオ、書類、Web など）を利用して政府公式情報を外部の利害関係者に提供する主管政府機関の能力に関するものである。

5.1.5.3 成果のアウトリーチ活動情報タイプ

成果のアウトリーチ活動情報は、政府サービスの成果および一般向けプログラムのマーケティングをサポートする。一般向けプログラムは、意識を向上させこれらのサービスおよびプログラムの顧客／受益者数の増加を図るためのものである。ほとんどの場合、影響レベルは成果のアウトリーチ活動情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、政府サービスの成果、および意識を向上させこれらのサービスおよびプログラムの顧客／受益者数の増加を図るための一般向けプログラムをマーケティングする主管政府機関の能力に関するものである。

5.1.5.4 広報情報タイプ

広報情報は、国民の懸念事項に効果的に対応することによって、組織のイメージを向上させるための取り組みをサポートする。ほとんどの場合、影響レベルは広報情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、国民の懸念事項に効果的に対応することによって組織のイメージを向上させる主管政府機関の能力に関するものである。

5.1.6 歳入徴収

歳入徴収情報は、すべての収入源からの政府収入の徴収を含む。

注：徴税は、一般政府任務分野の租税管理情報タイプの項で説明する。

5.1.6.1 債権回収情報タイプ

債権回収情報は、国外および国内の合衆国政府の債務者からの代金回収に関連する活動をサポートする。ほとんどの場合、機密性、完全性、および可用性影響レベルは、債権回収情報の、許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、国外および国内の合衆国政府の債務者からの代金を適切かつ効率的に回収する主管政府機関の能力に関するものである。

5.1.6.2 受益者負担金徴収情報タイプ

受益者負担金徴収情報は、政府サービスの提供および政府所有物または資源（例：国立公園）の利用に対して個人または組織に課される負担金の徴収をサポートする。ほとんどの場合、影響レベルは受益者負担金徴収情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、政府サービスの提供および政府所有物または資源の利用に対して個人または組織に課される負担金の徴収を正確かつ効率的に実施、統制、および達成する主管政府機関の能力に関するものである。

5.1.6.3 連邦資産売却情報タイプ

連邦資産売却情報は、連邦政府が管理する商品価値を持った非内部資産で、民間部門に売却されるものの調達、監督、追跡、および売却に関連する活動をサポートする。ほとんどの場合、影響レベルは連邦資産売却情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、連邦政府が管理する商品価値を持った非内部資産で、民間部門に売却されるものを適切かつ効率的に調達、監督、追跡、および売却する主管政府機関の能力に関するものである。

5.1.7 立法関係

立法関係の情報は、連邦政府の立法部門による一般法の立案、追跡、および改正を目的とする活動をサポートする。

5.1.7.1 立法追跡情報タイプ

立法追跡情報は、構想から採択までの立法の追跡をサポートする。ほとんどの場合、影響レベルは立法追跡情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、構想から採択まで立法を追跡する主管政府機関の能力に関するものである。

5.1.7.2 立法証明情報タイプ

立法証明情報は、構想から採択までの立法に対する賛成または反対の証言／証拠の提供に関連する活動をサポートする。ほとんどの場合、影響レベルは立法証明情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、構想から採択までの立法に対する賛成または反対の証言／証拠を提供する主管政府機関の能力に関するものである。

5.1.7.3 法案作成情報タイプ

法案作成情報は、連邦議会の立法行為を条件として作成または改正する法案の起草をサポートする。ほとんどの場合、影響レベルは法案作成情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、連邦議会の立法行為を条件として作成または改正する法案を起草する主管政府機関の能力に関するものである。

5.1.7.4 議会連絡情報タイプ

議会連絡活動情報は、連邦機関と米国議会間の公式関係のサポートに関連するすべての活動をサポートする。ほとんどの場合、影響レベルは議会連絡情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、米国議会との公式関係をサポートする主管政府機関の能力に関するものである。

5.1.8 一般政府

一般政府情報は、立法および行政活動、中央の財政、人事、および資産活動の提供、ならびにほかのサービス支援分野に合理的に分類できないサービスの提供を含む、連邦政府の一般諸経費をサポートする。一般に、ほかのサービス支援分野または情報タイプに密接に関連するすべての活動は、一般政府の一部として記載するのではなく、それらのサービス支援分野または情報タイプに含める。当該サービス支援分野は、中央政府の管理活動のために用意されたものであり、ほとんどの政府機関固有の管理活動はここには含まれないはずである。ただし、ほかのサービス支援機能とは異なり、特定の組織に関連する一般政府情報タイプがある（例：中央人事管理の場合は人事管理局）。

5.1.8.1 中央財政運用情報タイプ

中央財政運用情報は、指定された組織が政府の意向を受けて実行する財政運用をサポートする[13]。ほとんどの場合、影響レベルは中央財政運用情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、指定された組織が政府の意向を受けて実行する財政運用に関するものである。中央財政運用に関連する一部の情報および情報システムへの影響は、きわめて重要な銀行および金融インフラストラクチャのセキュリティに影響を及ぼす可能性がある。結果として人命または主要国家資産の損失が発生する可能性は一般的に低い。

5.1.8.2 立法機能情報タイプ

立法機能情報は、租税裁判所、議会図書館、および政府印刷局の回転資金を除く立法部門の経費に関連するサービス支援活動をサポートする。ほとんどの場合、影響レベルは立法サービス支援情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、租税裁判所、議会図書館、および政府印刷局の回転資金を除く立法部門の経費に関連するサービス支援活動を提供する主管政府機関の能力に関するものである。

[13] 税関連の機能は、租税管理情報タイプに関連する。

5.1.8.3 行政機能情報タイプ

行政機能[14]情報は、行政府の運用をサポートする。影響レベルは、行政府の機能に関する行政情報タイプの許可のない開示、改変、または可用性の損失による影響に基づく。

5.1.8.4 中央資産管理情報タイプ

中央資産管理情報は、一般調達局の運用のほとんどをサポートする。ほとんどの場合、影響レベルは中央資産管理情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、連邦政府によって使用されるオフィスビル、車両、機械類、ならびにそのほかの資本資産および消耗品を調達、提供、および一元管理する一般調達局の能力に関するものである。

5.1.8.5 中央人事管理情報タイプ

中央人事管理情報は、人事管理局（OPM）および関連諸機関の運用活動のほとんどをサポートする。ほとんどの場合、影響レベルは中央人事管理情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、資格任用制の原則に基づいて良質かつ多様な連邦職員を組織する人事管理局の能力に関するものである。中央人事管理情報は、人的資源管理およびコンサルティングサービス、教育および指導力開発サービス、調査サービスなどを含む。

5.1.8.6 租税管理情報タイプ

租税管理情報は、内国歳入法の実施およびアメリカ国内外における租税徴収に関連する活動をサポートする。ほとんどの場合、影響レベルは租税管理情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、内国歳入法の実施およびアメリカ国内外における租税徴収を行う指定機関の能力に関するものである。

5.1.8.7 中央記録・統計管理情報タイプ

中央記録・統計管理情報は、連邦政府全体の公式文書、統計、および記録の運用に関する活動をサポートする。本情報タイプは、国立公文書館（NARA）が行う記録管理や商務省が行うデータ収集など、連邦政府全体としての記録および統計の管理に関連する情報および情報システムを含めるためのものである[15]。

---

[14] OMB の『Business Reference Model』では、「行政機能」は、大統領府（EOP）の機能に加えて一般政府機関の行政機能も含むように範囲が拡大された。EOP のみの行政機能については、付録 D「任務別情報および情報システムの影響決定の例」で扱う。

[15] 多くの政府機関は、特定の業務機能に関する記録および統計管理を行っているので、記録および統計管理はその業務機能に関連するサービス支援、管理、または任務分野にマッピングされる。中央記録・統計管理情報タイプは、連邦政府全体に代わって実行される機能を目的としている。

ほとんどの場合、影響レベルは中央記録・統計管理情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、連邦政府全体の公式文書、統計、および記録を管理する主管政府機関の能力に関するものである。

5.1.8.8 収入情報

収入情報は、個人が補足的所得保障または RSDI（退職 (Retirement)、遺族(Survivor)、障害保険(Disability benefits)）第 II 編制度から受給するまたは受給しない権利がある退職給付金、遺族給付金、または障害給付金の額の決定を支援するのに必要なすべての賃金、自営業収入、貯蓄型データ、およびそのほかの金融資産情報をサポートする。ほとんどの場合、影響レベルは収入情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、国民の受給資格および負担を識別し、国民の識別情報を盗難から保護し、連邦政府を不正行為から保護する、連邦政府の能力に関するものである。

5.1.8.9 個人識別・認証情報

個人識別・認証情報は、連邦給付金の受給資格を持つ可能性があるすべての人を確実に列挙および識別し、連邦機関がその本人に対して支払いまたは連絡を行っていることを合理的に保証できるようにするのに必要な情報を含む。本情報は、個々の国民の社会保障番号、氏名、誕生日、出生地、両親の氏名などを含む[16]。ほとんどの場合、影響レベルは個人識別・認証情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、個人に対する連絡および支払いがその本人に対して行われていると判断する連邦機関の能力に関するものである。

5.1.8.10 受給資格事象情報

受給資格事象情報は、死亡などの事象とその発生日に関する情報、障害事象の発生日と当該障害の程度を合理的に証明できる関連データ、退職給付金受給のための年齢証明、主たる受給者の補助者としてのみ給付金を受け取る権利がある配偶者および／または子供の誕生および関係、ならびに給付金の請求処理に必要なそのほかの関連情報を含む。これはまた、第 XVI 編（補足的所得保障制度）および最近改正されたメディケア制度の新しい医薬品規定に関連するすべての収入関連給付の管理に必要な収入関連情報も含む。ほとんどの場合、影響レベルは受給資格事象情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、個人の政府給付金受給資格を証明する連邦政府の能力に関するものである。

[16] 政府と機密または支払いに関するビジネスを行う個人は、当該のデータを使用して、適用される指令によって規定されたレベルに合わせて身元を証明しなければならない。

5.1.8.11 代理受取人情報

代理受取人情報は、自己の資金を管理できないすべての連邦政府給付金受給者に関する代理受取人の必要性の判断に必要な情報、および代理受取人となる人を決定するために収集されるデータを含む。これはまた、給付金が受給資格者の福祉のために適切に利用されていることを合理的に保証するのに必要な責任追跡性情報も含む。ほとんどの場合、影響レベルは代理受取人情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、給付金が受給資格者の福祉のために適切に使用されていることを確認する連邦政府の能力に関するものである。

5.2 政府資源管理情報

*政府資源管理情報*業務分野は、連邦政府が効果的に活動できるようにする事務処理支援活動を含む。*政府資源管理情報*には、表 2 の見出し「政府資源管理」の下にイタリック体で識別した 5 つの業務項目がある。以下に、*政府資源管理情報*下位機能に関連する各情報タイプを記述する。サービス提供支援情報の機密性、完全性、および可用性の侵害の暫定影響レベルは、付録 C.3「政府資源管理情報」で勧告する。多くの省庁および政府機関は、それぞれ独自の支援システムを運用している。そうでない省庁および政府機関は、ほかの組織から少なくともいくつかの支援サービスを調達している。いくつかの政府機関は、直接サービス任務の遂行においてほかの政府省庁および機関を支援することを主な任務としている。前述のとおり、運営・管理情報およびシステムのセキュリティ目標および影響は、支援される直接サービスおよび受益者の性質によって決定される。

5.2.1 人的資源管理

人的資源情報は、要員の募集および管理に関連するすべての活動をサポートする。

5.2.1.1 給付管理情報タイプ

給付管理情報は、退職、医療、障害、保険など、連邦職員が受給資格を持つ給付金の管理をサポートする。ほとんどの場合、影響レベルは給付管理情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、退職、医療、障害、保険など、連邦職員が受給資格を持つ給付金を管理する主管政府機関の能力に関するものである。

5.2.1.2 人事管理情報タイプ

人事管理情報は、人事措置、職員追跡、職位分類・管理、懲戒／苦情処理、昇進・表彰、労務関係などの機能を含む、連邦職員の全般的な管理をサポートする。ほとんどの場合、影響レベルは人事管理情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、主管政府機関による連邦職員の管理能力に関するものである。

5.2.1.3 給与管理・経費精算情報タイプ

給与管理・経費精算情報は、連邦職員報酬の管理および決定をサポートする[17]。ほとんどの場合、影響レベルは給与管理・経費精算情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、主管政府機関による連邦職員の報酬管理および決定能力に関するものである。

5.2.1.4 人的資源訓練・開発情報タイプ

人的資源訓練・開発情報タイプは、正規の教育、技術訓練、またはそのほかの教育手段による職員の積極的な能力開発をサポートする。ほとんどの場合、影響レベルは人的資源訓練・開発情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、正規の教育、技術訓練、またはそのほかの教育手段による職員の能力開発を行う主管政府機関の能力に関するものである。

5.2.1.5 セキュリティ資格管理情報タイプ

セキュリティ資格管理情報は、職員、請負業者、およびそのほかの人による連邦の建物への入場、連邦サービスの利用、および機密にかかわる情報へのアクセスが許可済みであることの保証に関連するプロセスをサポートする。これは、資格決定、バッジ支給、権限追跡、およびセキュリティ検証サービスを含む。セキュリティ資格管理に関連する一部の情報および情報システムへの影響は、きわめて重要なインフラストラクチャおよび主要国家資産のセキュリティに影響を及ぼす可能性がある。また、セキュリティ資格管理に関連する多くの情報は国家安全保障（本ガイドラインの範囲外）に関連するが、本ガイドラインで用いるセキュリティ資格管理は国家安全保障用途に限定されない。ほとんどの場合、影響レベルはセキュリティ資格情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、連邦の情報および施設に関するアクセス資格決定、バッジ支給、資格追跡、およびセキュリティ検証サービスを管理する主管政府機関の能力に関するものである。

5.2.1.6 職員募集・採用情報タイプ

職員募集・採用情報は、組織内の増員および欠員補充のための積極的な求人および雇用をサポートする。ほとんどの場合、影響レベルは職員募集・採用情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、組織内の増員および欠員補充のための積極的な求人および雇用を行う主管政府機関の能力に関するものである。

[17] 給与および経費の実際の支払いについては、*支払い*情報タイプを参照。

5.2.2 運営管理

運営管理情報は、内部インフラストラクチャの日常の管理および保守をサポートする。運営情報は通常、定型的であり影響は比較的低位であるが、運営管理情報のなかには、非常に機密にかかわる情報（例：核物質またはそのほかの危険物の物流管理、セキュリティマネジメント情報、およびセキュリティ資格管理情報）や、きわめて重要な情報（例：時間に決定的に依存する運用の支援に必要な在庫管理および物流管理情報）もある。*国家セキュリティ情報*はすべて本ガイドラインの範囲外である（*国家セキュリティ情報／システム*の定義については、付録 A「用語集」を参照）。機密情報を取り扱わない日常運営管理情報システムは通常、たとえ軍事または諜報任務の直接的遂行にとってきわめて重要であっても、*国家的セキュリティシステム*には指定されない。

5.2.2.1 施設・車両・装置管理情報タイプ

施設・車両・装置管理情報は、連邦政府の所有物とみなされるオフィスビル、車両、機械類、およびそのほかの資本資産の保守、管理、および運用をサポートする。ほとんどの場合、影響レベルは施設・車両・装置管理情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、連邦政府の所有物とみなされるオフィスビル、車両、機械類、およびそのほかの資本資産を保守、管理、および運用する主管政府機関の能力に関するものである。施設、車両、および装置管理に関連する一部の情報および情報システムへの影響は、いくつかの主要国家資産（例：原子力発電所、ダム、およびそのほかの政府施設）のセキュリティに影響を及ぼす可能性がある。

5.2.2.2 ヘルプデスクサービス情報タイプ

ヘルプデスクサービス情報は、政府職員の技術的および運営上の質問に回答するサービスセンターの管理をサポートする。ほとんどの場合、影響レベルはヘルプデスクサービス情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、政府職員の技術的および運営上の質問に回答するサービスセンターを管理する主管政府機関の能力に関するものである。

5.2.2.3 セキュリティマネジメント情報タイプ

セキュリティマネジメント情報は、組織の要員、資産、および施設の物理的保護をサポートする。ほとんどの場合、影響レベルはセキュリティマネジメント情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、主管政府機関の要員、資産、および施設の物理的保護能力に関するものである。セキュリティマネジメントに関連する一部の情報および情報システムへの影響は、いくつかのきわめて重要なインフラストラクチャ要素および主要国家資産（例：原子力発電所、ダム、およびそのほかの政府施設）のセキュリティに影響を及ぼす可能性がある。セキュリティ情報に関連する影響レベルは、保護対象の資産に関係する人命への潜在的脅威に直接関連する。例えば、影響レベルは、テロリストによるダムまたは原子力発電所への侵入が一般人にもたらす結果に基づく場合がある。

5.2.2.4 出張旅行情報タイプ

出張旅行情報は、組織職員の業務に関連する出張旅行の計画、準備、および監視に関連する活動をサポートする。ほとんどの場合、影響レベルは出張旅行情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、組織職員の業務に関連する出張旅行を計画、準備、および監視する主管政府機関の能力に関するものである。

5.2.2.5 職場方針策定・管理情報タイプ*（政府機関内のみ）*

職場方針策定・管理情報は、服装規定、時間報告要件、在宅勤務などの職場方針の策定および伝播に必要なすべての活動をサポートする。ほとんどの場合、影響レベルは職場方針策定・管理情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、服装規定、時間報告要件、在宅勤務などの職場方針を策定および伝播する主管政府機関の能力に関するものである。

5.2.3 情報・技術管理

情報・技術管理情報は、国民サービスの支援または実現に必要な情報技術（IT）資源およびシステムの調整をサポートする。一般に、IT システムの運用に関連する情報への影響は、たとえそのシステムによって処理される任務関連情報すべてが一般公開用であっても、考慮する必要がある。完全性および可用性と機密性とでは、関連する課題が異なる可能性がある。公表済みの情報は当然、機密性保護を必要としない。一方、一般人に配布済みの情報のコピーについては、完全性および可用性を保護し続けることはできない。情報のコピーの完全性および可用性を保証し続けるには、組織の管理下にある情報システム内に保存しておくしかない。

5.2.3.1 システム開発情報タイプ

システム開発情報は、組織内でのソフトウェアアプリケーション設計および開発に関連するすべての活動をサポートする。ほとんどの場合、影響レベルはシステム開発情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、主管政府機関の組織内でのソフトウェアアプリケーション設計および開発能力に関するものである。

5.2.3.2 ライフサイクル／変更管理情報タイプ

ライフサイクル／変更管理情報は、資産、方法論、システム、または手順などの政府機関資源の変更の設計および実施の進展、構成、および要員異動を円滑化するプロセスをサポートする。ほとんどの場合、影響レベルはライフサイクル／変更管理情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、資産、方法論、システム、または手順などの政府機関資源の変更の設計および実施の進展、構成、および要員異動を円滑化する主管政府機関の能力に関するものである。

5.2.3.3 システム保守情報タイプ

システム保守情報は、組織内で設計したソフトウェアアプリケーションの保守に関連するすべての活動をサポートする。ほとんどの場合、影響レベルはシステム保守情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、組織内で設計したソフトウェアアプリケーションを保守する主管政府機関の能力に関するものである。

5.2.3.4 IT インフラストラクチャ管理情報タイプ

IT インフラストラクチャ保守情報は、自動化のニーズ（例：オペレーティングシステム、アプリケーションソフトウェア、プラットフォーム、ネットワーク、サーバー、プリンタなど）に効果的に対応するための IT インフラストラクチャの計画、設計、導入、および保守をサポートする。IT インフラストラクチャ保守はまた、情報システム構成およびセキュリティポリシー実施情報も含む。本情報には、パスワードファイル、ファイルアクセステーブル、ネットワークアクセスルール（ファイルおよび／またはスイッチ設定の導入を含む）、ハードウェアおよびソフトウェア構成設定、ならびにその情報システムのデータ、プログラム、および／またはプロセスへのアクセスに影響を及ぼす可能性がある資料が含まれる。ほとんどの場合、影響レベルは IT インフラストラクチャ保守情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、自動化のニーズ（例：オペレーティングシステム、アプリケーションソフトウェア、プラットフォーム、ネットワーク、サーバー、プリンタなど）に効果的に対応するための IT インフラストラクチャの計画、設計、導入、および保守を行う主管政府機関の能力に関するものである。IT インフラストラクチャ保守情報に関連する影響レベルは、そのインフラストラクチャ内で処理される情報に主に依存する（5.2.3.5「IT セキュリティ情報」および 5.2.3.7「情報管理情報」を参照）。IT インフラストラクチャ保守はまた、情報システム構成およびセキュリティポリシー実施情報も含む。

5.2.3.5 IT セキュリティ情報タイプ

IT セキュリティ情報は、識別、認証、否認防止などのサービスをカバーするセキュリティポリシー、手順、および管理策を作成および定義することによって、連邦のデータおよびシステムのセキュリティ保護に関連するすべての機能をサポートする。ほとんどの場合、影響レベルは IT セキュリティ情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、識別、認証、否認防止などのサービスをカバーするセキュリティポリシー、手順、および管理策を作成および定義することによって、連邦のデータおよびシステムのセキュリティを保護する主管政府機関の能力に関するものである。

5.2.3.6 記録保管情報タイプ

記録保管情報は、政府機関の公式文書および記録の管理にかかわる運用をサポートする。ほとんどの場合、影響レベルは記録保管情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、主管政府機関の公式文書および記録の保存、追跡、把握、維持、検索、および伝播能力に関するものである。*国家セキュリティ情報*および*国家的セキュリティシステム*は、本ガイドラインの範囲外である。

5.2.3.7 情報管理情報タイプ

情報管理情報は、情報収集、蓄積、伝播、および破壊の調整、ならびに情報管理に関する方針、ガイドライン、および標準の管理をサポートする。ほとんどの場合、影響レベルは情報管理情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、主管政府機関の日常の情報収集、蓄積、伝播、および破壊プロセス、ならびに情報管理に関する方針、ガイドライン、および標準の管理の実行能力に関するものである。

5.2.4 財務管理

財務管理情報は、すべての政府の歳入、財源、および歳出の正確、効率的、透明、かつ効果的な処理を可能にする一連の会計慣例および手順全体をサポートする。一般に、財務管理情報に関連する機密性の影響は、許可のない情報の開示によって暴露される可能性がある特定のプロジェクト、プログラム、および／または技術の秘匿度に関連する。不正の成功などの完全性の侵害は、政府機関のイメージに影響を及ぼす可能性がある。財務管理情報の永久的な喪失／利用不可は、機関の活動を不能にする可能性がある。

5.2.4.1 資産・負債管理情報タイプ

資産・負債管理情報は、連邦政府の資産および負債の管理に関する会計サポートを提供する。資産・負債管理活動は、連邦プログラムの総費用および総収入、ならびにその各種要素、活動、および出力結果を評価する。資産・負債管理は、活動費用の検証可能な報告による正確なプログラム評価情報、達成度評価、および財務諸表の提供に不可欠である。ほとんどの場合、影響レベルは資産・負債管理情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、連邦政府の資産および負債の管理に関する会計サポートを提供する主管政府機関の能力に関するものである。

5.2.4.2 レポート・インフォメーション情報タイプ

レポート・インフォメーション情報は、財務情報ならびに財務取引の報告および分析を提供する。財務報告情報は、受託者としての管理者の役割、予算編成・執行機能、プログラム実施およびプログラム決定の財務的管理、ならびに内部および外部報告要件の支援に必要な活動をサポートする。ほとんどの場合、影響レベルは財務報告情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、財務情報ならびに財務取引の報告および分析を提供する政府機関の能力に関するものである。

5.2.4.3 予算・財務情報タイプ

予算・財務情報は、計画・プログラム、予算、執行結果・成果の作成、ならびに直接および立替支出権限に基づく予算割当・分配、資金振替、投資、およびそのほかの資金調達メカニズムによる連邦プログラムおよび運用の資金調達を含む連邦予算プロセスの管理をサポートする。

予算・財務管理情報は、組織が割当額または承認額を超える資金を債務返済に充当したり、支出したりしないことを保証するシステムの確立をサポートする。ほとんどの場合、影響レベルは予算・財務情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、主管政府機関の計画・プログラム、予算、執行結果・成果の作成能力、ならびに直接および立替支出権限に基づく予算割当・分配、資金振替、投資、およびそのほかの資金調達メカニズムによる連邦プログラムおよび活動の資金調達能力に関するものである。

5.2.4.4 会計情報タイプ

会計情報は、適用される連邦基準（例：財務会計基準委員会（FASAB）、財務省、OMB、会計検査院（GAO）など）に基づく連邦資金および連邦歳出予算支出（例：給与や経費、運用や保守、調達、運転資本、資金運用など）の維持管理に関連する資産、負債、資金残高、収入、および支出の会計をサポートする。ほとんどの場合、影響レベルは会計情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、適用される連邦標準に基づいて連邦資金および連邦歳出予算支出を維持管理する政府機関の能力に関するものである。

5.2.4.5 支払い情報タイプ

支払い情報は、物品およびサービスに対する支払い、あるいは社会保障手当、給付金、補助金、助成金、貸付金、または賠償金の支給のための、さまざまな仕組みを通した連邦の公人／私人、連邦機関、州／地方政府、国際機関、および民間部門への連邦資金の支出を含む。支払管理は、組織によって、または組織に代わって行われるすべての支払いの適切な管理を提供する。これには、契約書、購入注文書、およびそのほかの拘束力のある文書に基づくベンダーへの支払い、各種制度に基づく州政府への支払い、給与および経費精算のための職員への支払い、実行された清算可能な作業に対するほかの連邦機関への支払い、連邦給付金を受給する国民個人への支払い、連邦融資の借入者への支払いが含まれるが、必ずしもこれらに限定されない。ほとんどの場合、影響レベルは支払い情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、組織によって、または組織に代わって行われるすべての支払いの適切な管理を提供する主管政府機関の能力に関するものである。

5.2.4.6 徴収・未収情報タイプ

徴収・未収情報は、売却またはサービスに対する預託、資金振替、および収入を含む。未収管理は、政府債権の認識および記録、債権の徴収のためのフォローアップ活動の実施、ならびに現金収入の記録に関する活動をサポートする。ほとんどの場合、影響レベルは徴収・未収情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、政府債権の認識および記録、債権の徴収のためのフォローアップ活動の実施、ならびに現金収入の記録を行う主管政府機関の能力に関するものである。

5.2.5 サプライチェーン管理

サプライチェーン管理情報は、物品およびサービスの購入、追跡、および全般的管理をサポートする。

5.2.5.1 物品調達情報タイプ

物品調達情報は、連邦政府が使用する物品、製品、および資本資産の調達をサポートする。ほとんどの場合、影響レベルは物品調達情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、連邦政府が使用する物品、製品、および資本資産を調達する政府機関の能力に関するものである。

5.2.5.2 在庫管理情報タイプ

在庫管理情報は、調達した資産および資源の数量、品質、および所在に関する情報の追跡をサポートする。ほとんどの場合、影響レベルは在庫管理情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、調達した資産および資源の数量、品質、および所在に関する情報を追跡する政府機関の能力に関するものである。

5.2.5.3 物流管理情報タイプ

物流管理情報は、要員およびその資源の可用性および所在に関する計画および追跡をサポートする。ほとんどの場合、影響レベルは物流管理情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、要員およびその資源の可用性および所在に関する計画および追跡を行う政府機関の能力に関するものである。

5.2.5.4 サービス調達情報タイプ

サービス調達情報は、民間部門の請負業者およびサービス提供者の監督および／または管理をサポートする。ほとんどの場合、影響レベルはサービス調達情報の許可のない開示、改変、または可用性の損失による影響に基づく。この情報は、民間部門の請負業者およびサービス提供者の監督および管理を行う政府機関の能力に関するものである。