NIST Special Publication 800-171
Revision 1

連邦政府外のシステムと組織における管理された非格付け情報の保護

RON ROSS
PATRICK VISCUSO
GARY GUISSANIE
KELLEY DEMPSEY
MARK RIDDLE

本書は、以下より無料で利用可能である：
https://doi.org/10.6028/NIST.SP.800-171r1

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

この文書は以下の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

NIST Special Publication 800-171

連邦政府外のシステムと組織における管理された非格付け情報の保護

RON ROSS
KELLEY DEMPSEY
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

PATRICK VISCUSO
MARK RIDDLE
情報保全監察局
米国国立公文書記録管理局

GARY GUISSANIE
防衛分析研究所
CIO 室補佐
米国国防総省

本書は、以下より無料で利用可能である：
https://doi.org/10.6028/NIST.SP.800-171r1

2016 年 12 月

米国商務省
Penny Pritzker、長官

米国国立標準技術研究所
Willie May、標準技術担当次官兼所長代行

発行機関

本文書は、米国国立標準技術研究所（NIST：National Institute of Standards and Technology、以下、NIST と称す）によって、連邦情報セキュリティ近代化法（FISMA：Federal Information Security Mondernization Act）2014 年、合衆国法典（U.S. Code）第 44 編 第 3541 条 等、公法（P.L.）113-283 に基づく法的責任を推進するために策定された。NIST は、連邦情報システムの最小限の要求事項を含め情報セキュリティ標準及びガイドラインを開発する責務があるが、このような標準及びガイドラインは国家安全保障に適用されてはならず、このようなシステムについての政策的権限を有する適切な連邦機関の明確な承認が必要となる。このガイドラインは、行政管理予算庁（OMB：Office of Management and Budget）による通達（Circular）A-130 号 附属書 IV：鍵の分析セクションで分析されたものとして、第 8 条 b 項(3)、*政府機関の情報システムをセキュア化*、通達 A-130 の要求事項に一致している。補足情報は、通達 A-130 号、附属書 III、*連邦政府の自動化された情報リソースのセキュリティ*で提供される。

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及び拘束力を与えた標準及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たりしてはならない。本文書は、非政府組織が自由意思で使用することもでき、米国における著作権の制約はないが、NIST に帰属する。

National Institute of Standards and Technology Special Publication 800-171
Natl. Inst. Stand. Technol. Spec. Publ. 800-171, 80 pages（December 2016）
CODEN: NSPUE2

本書は、以下から無料で利用可能である： https://doi.org/10.6028/NIST.SP.800-171r1

本文書中で特定される商業的組織、装置、資料は、実験的な手順または概念を適切に説明するためのものである。このような特定は、NIST による推奨または同意を意味するものではなく、これらの組織、資料、または装置が、その目的ために利用可能な最善のものであることを意味している訳ではない。

与えられた法的責任に従い、NIST によって現在開発中のその他の文書への参照が本文書にあるかもしれない。本文書におけるその情報は、概念及び方法論を含め、このような関連文書の完成前であっても連邦政府によって利用されるかもしれない。したがって、それぞれの文書が完成されるまで、現在の要求事項、ガイドライン、及び手順は存在する限り運用の効力を有する。計画及び移行目的に関して、連邦政府は、NIST によるこれらの新しい文書の開発に密接に従うことを希望するかもしれない。

パブリックコメント募集期間中に組織がすべてのドラフト文書をレビューし、NIST へフィードバックを提供するよう奨励する。上記以外のすべての NIST コンピュータセキュリティ部門の文書は、http://csrc.nist.gov/publications において利用可能である。

本文書に対するコメントは以下に提出できます：

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

すべてのコメントは、連邦情報公開法の下で開示の対象となる。

コンピュータシステムの技術に関する報告書

米国国立標準技術研究所（NIST：National Institute of Standards and Technology）の情報技術ラボラトリ（ITL : Information Technology Laboratory）は、米国の度量衡と標準規格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、米国の経済及び社会福祉に貢献している。ITL は、テストの開発、テスト技法の開発、参照データの作成、概念実証の実施及び技術的分析を通じて、情報技術（IT）の開発と生産的利用の発展に努めている。ITL の責務には、連邦政府の情報システムにおいて、国家安全保障に関連する情報以外の情報に対する費用対効果の高いセキュリティとプライバシーを実現するための、技術面、物理面、管理面及び運用面での標準規格及びガイドラインを策定することを含んでいる。本 Special Publication 800 シリーズでは、ITL の学術研究、ガイドラインについて、情報システムのセキュリティ及び産業界、政府機関及び学術機関とのその共同活動における支援活動の取り組みとともに報告する。

要旨

連邦政府外のシステムと組織に存在する管理された非格付け情報（CUI）の保護は、連邦政府機関にとって最も重要なものであり、連邦政府の指定されたミッションとビジネス運用をうまく行うための能力に直接影響を及ぼす可能性がある。本書は、以下のときに CUI の機密性保護についての推奨されるセキュリティ要件を連邦政府機関に対して提供する；このような情報が連邦政府外のシステム及び組織に存在するとき；連邦政府機関が連邦政府機関を代行して情報を収集または維持しない、または政府機関を代行してシステムを利用または運用しないとき；及び CUI リポジトリに列挙された CUI カテゴリまたはサブカテゴリのために許可している法律、政令、または政府全体の政策によって規定される CUI の機密性保護の具体的な保障措置としての要件がないような場合。セキュリティ要件は、CUI を処理し、保存し、または送信するような、あるいはこのようなコンポーネントにセキュリティ保護を提供するような、連邦政府外のシステム及び組織のすべてのコンポーネントに適用される。本要件は、それらの政府機関及び連邦政府外の組織の間で確立される契約書のひな形として、またはその他の合意での連邦政府による利用を意図している。

キーワード

請負業者システム；管理された非格付け情報；CUI リポジトリ；導出されたセキュリティ要件；大統領行政命令 13556；FIPS Publication 199；FIPS Publication 200；FISMA；NIST Special Publication 800-53；連邦政府外のシステム；セキュリティアセスメント；セキュリティ管理策；セキュリティ要件。

謝辞

著者は、本書の全体的な品質、完璧さ、有用性を改善させる思慮深く建設的なコメントを提供した Carol Bales、Matt Barett、Jon Boyens、Devin Casey、Chris Enloe、Jim Foti、Rob Glenn、Rich Graubart、Vicki Michetti、Michael Nieles、Pat O'Reilly、Karen Quigg、Mary Thomas、Matt Scholl、Murugiah Souppaya、及び Pat Toth からの貢献に深く感謝の意を表する。特に、Peggy Himes と Elizabeth Lennon の素晴らしい管理上の技術編集支援に対して感謝の意を表します。

注意書

2014 年版の連邦政府情報セキュリティ近代化法（FISMA）は、以下に対する不正なアクセス、利用、暴露、混乱、改変、または破壊からもたらされるリスクに見合う情報セキュリティ保護を特定し提供することを連邦政府機関に要求する：政府機関によって、または政府機関を代行して収集または維持される情報；または政府機関によって、または政府機関の請負業者によって、または政府機関を代行するその他の組織によって、利用または運用される情報システム。本書は、*連邦政府外の*システム及び組織における管理された非格付け情報（CUI）の*機密性*保護に焦点を当て、またその目的を達成するための具体的なセキュリティ要件を推奨する。FISMA で規定される情報セキュリティ要件はどのようなやり方であっても変更されず、法律のすべての条項、OMB によって制定された政策、及び NIST によって開発された補足のセキュリティ標準規格とガイダンスに適合するための連邦政府機関の責任を変更することはできない。

本書で利用するよう推奨される要件は、FIPS Publication 200 及び NIST SP 800-53 の中位セキュリティ管理策ベースラインから導出され、また CUI 規定（32 CFR Part 2002, *管理された非格付け情報*）に基づいている。本要件とセキュリティ管理策は、FISMA の下で網羅される連邦政府の情報及びシステムの必須の保護を提供するために、時間をかけて決定されてきた。FIPS Publication 200 セキュリティ要件及び NISTSP800-53 セキュリティ管理策に適用される調整基準は、それらの要件と管理策を除外するための承認として解釈されるべきでは***ない*** — むしろ、調整の基準は、連邦政府外のシステム及び組織における不正な暴露からの CUI の保護に焦点を当てている。さらに、セキュリティ要件は、上記列挙された NIST Publications から導出されているので、組織は、それらの具体的な要件が FIPS Publication200 及び SP 800-53 のセキュリティ要件と管理策を自動的に満たすと想定するべきでは***ない***。

*機密性*のセキュリティ対策に追加して、*完全性*と*可用性*の対策方針が包括的な情報セキュリティ施策の制定と維持に関心がある組織にとって高い優先度を持つ。本書の主たる目的が CUI の機密性を保護するための要件を定義することであるが、システムレベルでの下位のセキュリティメカニズムの多くは両方のセキュリティ対策方針を支援するので、機密性と完全性の間には緊密な関係がある。本書の推奨事項に興味があるか適合を要求される組織は、その個別のセキュリティ計画及びセキュリティ管理策の配備が組織のミッションとビジネス運営に対するサイバー及び動力学的（訳注：陸、海、空、宇宙の）範囲の脅威に対処するために必要で十分な保護を提供することを保証するため、附属書 E の中位ベースラインのセキュリティ管理策の完全なリストをレビューすることを強く推奨する。このような脅威への対処は、重要である、なぜなら多くの組織はミッションとビジネス上の成功のための情報技術基盤上に依存しているからである。

本発行文書への期待

2010 年 11 月 4 日付の、大統領行政命令 13556 *管理された非格付け情報* では、管理された非格付け情報（CUI）執行機関として指定された、国立公文書記録管理局（NARA）は、CUI 施策を実施するために必須である、このような行政命令を策定し発行しなければならないと制定した。連邦政府にわたる統一政策と実践を制定するための本任務と CUI 施策のミッションと整合しつつ、NARA は、政府全体の必須の管理策と CUI のマーク付けを制定するような連邦規定を 2016 年に発行しようとしている。本連邦規定は、一度発行されると、CUI 施策によって確立される、標準保障措置、マーク付け、配布、及び管理除外要件を執行府の全体にわたる機関に適用するよう結び付けられる。

*連邦政府情報システム*に関して、中位の機密性影響レベルで CUI を保護するための連邦規定は、OMB によって制定された適用可能な政策及び NIST によって発行された適用可能な政府全体の標準規格及びガイドラインに基づいている。本連邦規定は、OMB と NIST によってすでに制定された、これらの政策、標準規格、及びガイドラインを作成する訳ではない。しかし、本連邦規定は、行政府のいたるところにわたり一貫したやり方で政策の固守及び標準規格とガイドラインの利用を要求し、請負業者を含めて、連邦政府とそれらの連邦政府外のパートナーに対して現在の複雑さを軽減する。

連邦政府内での CUI の保障措置要件の定義に加えて、NARA は、連邦政府外の情報システム及び組織における CUI 保護のセキュリティ要件を定義している—SP 800-171 を NIST と共に作ることによって、連邦政府外の組織におけるそのような要件の潜在的な影響を軽減するようなステップを取る。このアプローチは、連邦政府外の者、請負業者を含めて、政府特有のアプローチの利用を試行するよりもむしろ、すでに行われているシステムや実践を用いてセキュリティ要件に適合するために役立つだろう。連邦政府外の組織が法律及び政令の要件に適合できるように、CUI 保護のための保障措置を一貫して実装できるように、連邦政府外のシステムに調整された、すべての CUI セキュリティニーズの標準化された統一の要件集についても提供するだろう。

最後に、NARA は、CUI 行政機関としての資格で、連邦政府 CUI 規定及び SP 800-171 を含む要求事項を請負業者に適用するような、唯一の連邦調達規則（FAR：Federal Acquisition Regulations）条項を 2017 年に提供することも計画している。これは、さらに、同じ情報に対する連邦政府機関からの異なる要件と矛盾するようなガイダンスは、混乱と非効率性を増大させるため、契約条項の現在の範囲と種別を満たそうとするかなりの数の連邦政府外の組織にとって利益となるような標準化を推進するだろう。CUI FAR 条項は、NIST SP 800-171 のセキュリティ要件の検証と適合要件にも対処する。このような FAR 条項の制定についての正式プロセスが実施されるまで、NIST SP 800-171 は、連邦政府法及び政令の要件と一貫する連邦政府契約において参照されてもよい。もし、必要があれば、SP 800-171 は、連邦政府 CUI 規定と FAR 条項とも一貫性を残すように更新されるだろう。

用語情報システムの定義と用途

法律、規制、または政府全体の政策によって規定されることなしに、本書における用語*情報システム*の使用は、用語*システム*によって置き換えられる。この変更は、例えば以下のようなものを含む情報システムのより幅広い、全体的な定義を反映する：汎用情報システム；産業及びプロセス制御システム；サイバーフィジカルシステム；及び *Internet of Things(IoT)* の一部である個人デバイス。コンピューティングプラットフォームと技術はユビキタスに世界規模で配備が進んでおり、システムやコンポーネントは有線及び無線ネットワークを介して接続され、管理された非格付け情報の紛失や危殆化に対する影響されやすさは、増大している—このような事件からもたらされる悪影響の可能性がある。

重要インフラのサイバーセキュリティの改善のためのフレームワーク

*重要インフラのサイバーセキュリティの改善のための NIST フレームワーク*を実装した、または実装を計画している組織は、本書の附属書 D で、管理された非格付け情報（CUI）セキュリティ要件から NIST SP 800-53 及び ISO/IEC 27001 への直接のマッピングを見つけることができる。一度特定されれば、それらの管理策はサイバーセキュリティフレームワークのコア機能に対応する具体的なカテゴリとサブカテゴリに配置可能である：*識別*、*保護*、*検知*、*応答*、*及び回復*。情報をマッピングしているセキュリティ管理策は、このようなプログラムが NIST または ISO/IEC セキュリティ管理策の周辺で構築されたとき、確立された情報セキュリティプログラムにおけるセキュリティ要件への適合性の実証を希望する組織にとって有用であるに違いない。以下を参照 http://www.nist.gov/cyberframework。

目次

正誤表

本表には、SP 800-171 へ組み込まれた変更が含まれている。正誤表の更新は、本出版における、本来*エディトリアル*または*実質的*のいずれかであるような訂正、明確化、またはその他のマイナーチェンジが含まれる。

日付	種別	変更	ページ

第 1 章
はじめに

管理された非格付け情報の保護の必要性

今日、歴史上のいつにも増して、連邦政府は実運用している情報システム[1]を用いて幅広い範囲の連邦政府の使命とビジネス機能の実施を支援するため外部サービス提供者に依存している。多くの連邦政府の請負業者は、例えば、連邦政府機関への基本的な製品やサービスの提供をサポートするための情報システムにおける機微な連邦政府情報を日常的に処理、保存、送信している(例、クレジットカード及びその他の財務サービスの提供；ウェブ及び電子メールサービスの提供；保全許可のための身元調査の実施；医療データの処理；クラウドサービスの提供；通信、衛星、及び兵器システムの開発)。さらに、連邦政府情報は、州政府及び地方政府、大学、及び独立研究機関のようなエンティティとの間で、頻繁に提供または共有される。*連邦政府外のシステム*[2]及び組織に存在している間の機微な連邦政府情報の保護は、連邦政府機関にとって最も重要であり、重要インフラに関連するその指定された使命とビジネス機能を含めて、連邦政府がその使命とビジネス運営をうまく成し遂げる能力に直接的に影響を及ぼす可能性がある。

連邦政府外のシステム及び組織における非格付け連邦政府情報の保護は、連邦政府機関によって日常的に利用されるような異なった種別の情報を特定するための統制された構造化されたプロセスを提供している連邦政府に依存している。2010 年 11 月 4 日に、大統領は、大統領行政命令 13556、*管理された非格付け情報（Controlled Unclassified Information）*に署名した。本大統領行政命令は、行政機関(省)が保護を要求するような非格付け情報を取り扱う方法を規格化するため、政府全体の管理された非格付け情報（CUI)[3]プログラムを確立し、本プログラム実施する行政機関(局)[4]として国立公文書記録管理局(NARA)を指定した。連邦法、規制、または政府全体の政策に準拠する保障措置または配布管理策を要求するような情報のみが CUI として指定されることがある。

CUI 施策は、手順の標準化によるものと CUI *レジストリ*を介して共通の定義を提供することによるものの両方により、一貫しないマーク付け、不適切な保障措置、及び不必要な制約事項を含むような非格付け情報の管理と保護におけるいくつかの欠如に対処するために設計された。CUI レジストリは、CUI 執行機関による発行を含め、CUI の取り扱いにおける情報、ガイダンス、ポリシー及び要件についてのオンラインリポジトリである。その他の情報の間で、CUI レジストリは、承認された CUI カテゴリとサブカテゴリを特定し、それぞれについて概説を提供し、管理策の基本を特定し、情報のマーク付け、保障措

[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の個別の集まりである。情報システムには、例えば、産業／プロセス制御システム、サイバー・物理的システム、組込みシステム、及びデバイスのような、特化したシステムも含まれる。用語 *システム*には、本発行文書全般において、CUI を処理、格納、または送信できるようなコンピューティングプラットフォームのすべてのタイプを表すために使用される。

[2] *連邦政府情報システム*とは、行政機関（局）によって、行政機関の請負業者によって、または行政機関を代行する別の組織によって利用され運用されるシステムである。このような基準を満たさない情報システムが非連邦情報システムである。

[3] *管理された非格付け情報*は、法律政令、または政府全体のポリシーが安全防護または配布管理を行うことを要求するような情報である、大統領行政命令 13526,*格付けされた国家安全保障情報（Classified National Security Information）*、2009 年 12 月 29 日付、または以前のまたは後継の大統領行政命令、または 1954 年の原子力エネルギー法、その改正を含む、の下で格付けされる情報を除く。

[4] NARA は、NARA の一部門、米国情報保全監察局（ISOO：Information Security Oversight Office）に本権限を委任した。

置、配送、配付、再利用及び廃棄を含むがこれに限らない CUI の利用手順について着手する。

大統領行政命令 13556 は、CUI 施策が政府の実践の公開性、透明性、統一性について強調していること、施策の実施が行政管理予算庁（OMB：Office of Management and Budget）により制定された適用可能な政策と米国国立標準技術研究所（NIST：National Institute of Standards and Technology）により発行された連邦標準規格とガイドラインと一貫したやり方で行われていることについても要求した。CUI 執行機関により策定された、連邦政府 CUI *規定*[5]は、CUI の指定、保障措置、配付、マーク付け、管理除外、及び廃棄に関する連邦政府機関へのガイダンスを提供し、自己点検及び監督要件の確立、及び本施策のその他の断面を描写する。

CUI に対する単一状態セキュリティソリューションを実装する

管理された非格付け情報は、このような情報が連邦政府機関の一部ある連邦政府システムにあっても、非連邦政府組織の一部である非連邦政府システムにあっても、同じ価値がある。それぞれ、本発行文書に含まれるセキュリティ要件は、CUI を保護するために連邦政府機関によって使用される規格とガイドラインに対して一貫しており、補足するものである。

1.1 目的と適用可能性

本書の目的は、CUI が連邦政府外の情報システム及び組織にあるとき； CUI があるような情報システムが使用されない、または連邦政府機関の請負業者またはそれらの機関[6]を代行する組織によって運用されないとき；及び CUI レジストリ[7]に列挙された CUI 分類または小分類について許可している法律、規制、または政府全体の政策によってあらかじめ規定された CUI の機密性を保護するための具体的な安全防護の要件が一切ないような場合に、CUI の*機密性*を保護するための連邦政府機関に推奨されるセキュリティ要件を提供することである。本要件は、CUI を処理し、保存し、または送信するような、またはこのようなコンポーネント[8]のセキュリティ保護を適用するような、連邦政府外のシステムのコンポーネントへのみ適用される。CUI 要件は、適切な契約的な手段またはそれらの機関と連邦政府外の組織との間で確立されたその他の合意において、連邦政府機関による使用を意図している。CUI ガイダンス及び CUI 連邦政府調達令（FAR）[9]において、CUI 行政機関(局)は、

[5] 32CFR Part 2002、*管理された非格付け情報*、が 2016 年 9 月 14 日に発行された；2016 年 11 月 14 日に施行。

[6] 連邦政府機関*を代行して*情報を収集または維持し、または政府機関*を代行して*システムを使用または運用する、非連邦政府組織は、FISMA の要件に、FIPS Publication 200 の要件及び NIST SP 800-53 のセキュリティ管理策を含めて、適合しなければならない(44 USC 3554(a)(1)(A)を参照)。

[7] 本発行文書の要件は、上級政府機関職員が非連邦政府システム及び組織に存在する CUI を含め、彼らの管理下の運用と資産をサポートするような、その情報に対する情報セキュリティを提供するために、FISMA の要件に適合するようにするため、使用可能である。(44 USC 3554(a)(1)（A） 及び 3554(a)(2)を参照)

[8] システム*コンポーネント*には、例えば、以下が含まれる：メインフレーム、ワークステーション、サーバ；入出力デバイス；ネットワークコンポーネント；オペレーティングシステム；仮想マシン；及びアプリケーション。

[9] NARA は、CUI 行政機関としての立場で、提案された連邦政府 CUI 規定及び NISTSP 800-171 の要件を請負業者に適用するような唯一の FAR 条項を 2016 年に提供することを計画している。このような唯一の FAR 条項を制定する正式プロセスが施行されるまで、NIST SP 800-171 のセキュリティ要件は、連邦政府法及び政令の要件と一貫した連邦政府契約において参照されてもよい。

セキュリティ要件[10]への適合性の判断に対処すること。

連邦政府 CUI 規制に従って、CUI を処理し、保存し、または送信するための連邦政府システムを用いる連邦政府機関は、最小限、以下に適合しなければならない(must)：

- 連邦情報処理規格 (FIPS) Pub 199、*連邦政府の情報及び情報システムに対するセキュリティ分類規格　Standards for Security Categorization of Federal Information and Information Systems* (moderate confidentiality impact)[11]
- 連邦情報処理規格 (FIPS) Pub 200、*連邦政府の情報及び情報システム対する最低限のセキュリティ要求事項　Minimum Security Requirements for Federal Information and Information Systems ；*
- NIST Special Publication 800-53、*連邦政府情報システム及び連邦組織のためのセキュリティ管理策とプライバシー管理策 Security and Privacy Controls for Federal Information Systems and Organizations ；及び*
- NIST Special Publication 800-60、*情報及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 Guide for Mapping Types of Information and Information Systems to Security Categories*[12]。

CUI を保護及び CUI の制御を保証するための連邦政府機関の責任は、このような情報が連邦政府外のパートナーと共有されるときも変わらない。従って、CUI が処理され、保存され、または連邦政府外のシステム[13]を用いる*連邦政府外の組織*に送信されるときに同レベルの保護が必要とされる。連邦政府外のシステム及び組織での CUI を保護するための具体的な要件が一貫したレベルの保護を維持するために上記の正式な連邦政府標準及びガイドラインから導出されている。しかし、連邦政府の CUI 規制における保護要件の適用範囲が機密性のセキュリティ対策に限定されること(即ち、完全性と可用性には直接対処していない)、及び NIST 標準及びガイドラインで記述されたセキュリティ要件のいくつかが一意に連邦政府のものであることを特定しつつ、本書の要件が連邦政府外のエンティティ用に*調整*して作られた。

第 2 章で記述された基準の調整は、連邦政府の CUI 規制において記述されるとおり、CUI の保護のための連邦政府の要件を軽減または最小限にすることを意図していない。むしろ、その意図は、連邦政府外の情報システム及び組織内の等価な保護対策を促進することを許容するようなやり方で要件を表明することである。本書に記述されたそれらの要件以外の追加または異なる要件は、このような要件が法律、規制、または政府全体のポリシーに基づいているとき、及び CUI 規定として CUI レジストリにて示されたときにのみ適用されてもよい。特定の規定された分類における CUI のための保護要件の条項は、CUI ガイダンス及

[10] NIST Special Publication 800-171A (2017 年発行が計画されている) 別冊文書は、第 3 章のセキュリティ要件への適合性を組織が決定する支援として、評定手順を提供するだろう。

[11] FIPS Publication 199 は、セキュリティの違反（即ち、機密性の喪失）があるはずの、組織、資産または個人への潜在的な影響の 3 つの値（即ち、低度、中位、高度）について定義している。機密性の喪失が組織の運営、組織の資産または個人への*深刻*で不利な影響を与えると予想される場合、潜在的な影響は、*中位*となる。

[12] NIST Special Publication 800-60 は、CUI レジストリの CUI カテゴリ及びサブカテゴリと整合させるために改訂中である。

[13] *非連邦政府組織*は、非連邦政府情報システムを所有し、運用し、維持するような任意のエンティティである。非連邦政府組織の例には、以下が含まれる：州、地方、及び部族の政府；大学と大学院；請負業者。

び CUI FAR における NARA によって対処されており、契約やその他の合意における具体的な要件として反映される。

CUI の保護を委託された連邦政府外の組織は、CUI の処理、保存、または送信用のシステムまたはコンポーネントを指定し、次にそれらの組織は、それらのシステムまたはコンポーネントのみにセキュリティ要件の適用範囲を制限してもよい。アーキテクチャ設計概念を適用することによって CUI をそれ自体のセキュリティドメインへ隔離することは、最もコスト的に有効であり、連邦政府外の組織にとってセキュリティ要件を満たし、CUI の機密性を保護するために有効なアプローチであるかもしれない。セキュリティドメインは、物理的分離、論理的分離、または両方の組み合わせを採用してもよい。このアプローチは、合理的に適切なセキュリティを CUI に対して提供する、またミッション、運用、及び資産を保護するために通常要求されるようなレベルを超えた組織のセキュリティ姿勢の増加を回避する。連邦政府外の組織は、根拠となる法律、規制、または政府全体のポリシーによって要求または許可される具体的な保護を含めて、CUI 基盤が組織の CUI 関連契約及び／または合意のすべてに対する保護要件を満たす限り、複数の政府契約または合意に対して、同じ CUI 基盤の使用を選択してもよい。

1.2 対象読者

本書は、官及び民間の両方の多様な個人のグループと組織に対して、以下を含めるが、それに限定されない対象に提供することを意図している：

- システム開発ライフサイクルに責任を持つ個人(例、プログラム管理者、ミッション／ビジネスオーナ、情報オーナ／担当者、システム設計者及び開発者、システム／セキュリティ技術者、システムインテグレータ)；
- 取得または調達に責任を持つ個人(例、契約担当官)；
- システム、セキュリティ、またはリスク管理及び監督に責任を持つ個人(例、許可責任者、最高情報責任者、最高情報セキュリティ責任者、システムオーナ、情報セキュリティ管理者)；及び
- セキュリティ評定及び監視に責任を持つ個人(例、監査者、システム評価者、アセッサ、独立検証者／認証者、分析者)。

上記役割と責任は、1 つの異なる視点から見ることができる：*連邦政府の視点*では、契約上の輸送手段またはその他の種別の組織間の合意におけるセキュリティ要件を確立し運搬しているエンティティとして；及び*連邦政府外の視点*では、契約または合意において実施されるセキュリティ要件に対応し、適合しているエンティティとして。

1.3 本特別発行文書の構成

本特別発行文書の残りは、以下のように構成されている：

- 第 2 章は、CUI セキュリティ要件を開発するために利用される前提条件と方法、要件のフォーマットと構造、及び要件を得るための NIST 標準とガイダンスに適用される調整基準について記述する。
- 第 3 章は、連邦政府外の情報システム及び組織における CUI の機密性の保護のためのセキュリティ要件の 14 のファミリについて記述する。

- 補足の附属書は、連邦政府外のシステムと組織における CUI の保護に関連する追加の情報について以下を含めて提供する：一般的な参照情報；定義と用語集；頭字語；NIST Special Publication 800-53 と ISO/IEC 27001 におけるセキュリティ管理策へのセキュリティ要件に関連するマッピングテーブル；及び中位のセキュリティ管理策ベースラインで採用された調整アクションの説明。

第 2 章
基盤

CUI セキュリティ要件を開発するための前提条件と方法

本章は、連邦政府外のシステム及び組織における CUI を保護するためのセキュリティ要件を開発するために使用される前提条件と方法論；基本及び導出された CUI 要件の構造；及び連邦政府情報セキュリティ要件及び管理策へ適用される基準の調整について記述する。

2.1 基本的な前提条件

本発行文書で記述されるセキュリティ要件は、3 つの基盤となる前提条件に基づいて開発された：

- CUI の保護についての法定の及び規制上の要件は、このような情報が連邦政府システムに存在するか、または連邦政府外のシステムに存在するかどうかにかかわらず、それらのシステムが動作するような環境を含めて、*一貫*している；
- CUI を保護するために実装された保障措置は、連邦政府及び連邦政府外のシステムと組織において*一貫*している；及び
- CUI についての機密性影響値は、*中位(moderate)*[14]よりも低くてはならない、これは連邦情報処理標準(FIPS) Publication 199[15]に従う。

上記前提条件は、CUI として指定された連邦政府情報が同じ本質的な*値*と危殆化した場合の潜在的な*悪影響*—このような情報が連邦政府または連邦政府外の組織に存在するかどうかにかかわらず。従って、CUI の機密性保護は、連邦政府機関のミッションとビジネスの成功及び国家の経済及び国家安全保障上の利益に対して重要である。CUI セキュリティ要件の開発に影響も与えている追加の前提条件及び連邦政府外のエンティティとの協力における連邦政府機関の期待は、以下を含む：

- 連邦政府外の組織は、所定の情報技術基盤を有し、CUI を処理、保存、または送信する目的で特別にシステムを開発したり、調達したりする必要はない；
- 連邦政府外の組織は、セキュリティ要件を満たすために十分でもあるようなそれらの情報を保護するために所定の具体的な保障措置を有している；
- 連邦政府外の組織は、セキュリティ要件を満たすため、さまざまな潜在的なセキュリティソリューションを直接的にまたは管理されたサービスの利用を通して実施することが可能である；そして

[14] FIPS Publication 199 で定義された中位影響*値*は、FIPS Publication 200 の中位影響*システム*の一部となるかもしれない、順番に、NIST Special Publication 800-53 の中位セキュリティ管理策ベースラインの利用を調整活動の出発点として要求する。

[15] 32 CFR 2002(g)に従って、CUI は、中位機密性影響値以上に分類される。しかし、CUI の管理策を確立するような連邦政府法、政令、または政府全体のポリシーが中位機密性ベースラインの管理策とは異なる管理策を規定するとき、これらに従うこと。

- 連邦政府外の組織は、セキュリティ要件のすべてを満たすために必要な組織構造または資源を持たないかもしれない、また同等に有効な、特定な要件を満たせないものに対して補うようなセキュリティ対策を代替策として実施するかもしれない。

2.2 セキュリティ要件の開発

連邦政府外のシステム及び組織における CUI の機密性保護のセキュリティ要件は、うまく定義された*基本的セキュリティ要件* セクション及び*導出されたセキュリティ要件*セクションから構成されている。基本的セキュリティ要件は、連邦政府情報及びシステムについての上位レベルかつ基盤セキュリティ要件を提供する、FIPS Publication 200 から得られる。基本的セキュリティ要件を補足する、導出されたセキュリティ要件は、NIST Special Publication 800-53 のセキュリティ管理策から得られる。FIPS Publication 200 中位のベースラインにおけるセキュリティ要件及びセキュリティ管理策を用いて開始しつつ(即ち、連邦政府システム及び組織で CUI に対して要求される最小レベルの保護)、要件と管理策は、以下のような要件、管理策、または管理策の一部を取り除くため、*調整*される：

- 連邦政府独自に(即ち、第一に連邦政府の責任)；
- CUI の機密性保護に直接関連しない；または
- 規定[16]せずとも非連邦組織によって日常的に満たされることが期待される。

附属書 E は、CUI 導出されたセキュリティ要件と上記の CUI 調整基準に基づいて NIST SP800-53 中位ベースラインから取り除かれたそれらの管理策をサポートするようなセキュリティ管理策の完全なリストを提供する。

基本的及び導出されたセキュリティ要件の組み合わせは、連邦政府外のシステム及び組織における CUI の*機密性*保護に関して、FIPS Publication200 及び NIST Special Publication 800-53 の意図を取り込んでいる。附属書 D は、NIST Special Publication 800-53 と ISO/IEC 27001 における関連するセキュリティ管理策へのセキュリティ要件の非形式的なマッピングを提供する。マッピングには、セキュリティ要件のよりよい理解を促進するために含まれ、連邦政府外の組織における追加の要件を課すような意図は*ない*。

*構成管理*ファミリから取られた以下の例は、典型的なセキュリティ要件の構造を説明する：

基本的セキュリティ要件：

- 個別のシステム開発ライフサイクル全体で、組織のシステム（ハードウェア、ソフトウェア、ファームウェア、及び証拠資料（文書）管理を含めて）のベースライン構成とインベントリを確立し、維持する。
- 組織のシステムで採用された情報技術製品のセキュリティ構成設定を確立し、強制（実施）する。

導出されたセキュリティ要件：

- システムへの変更を追跡、レビュー、承認／非承認、及び監査する。
- 実装に先立ち、変更のセキュリティへの影響を分析する。
- システムへの変更に関連する物理的及び論理的なアクセス制約事項を定義し、文書化し、承認し、強

[16] 調整された FIPS Publication 200 セキュリティ要件と NIST SP 800-53 中位セキュリティ管理策ベースラインから開発されたセキュリティ要件は、*包括的な*情報セキュリティプログラムに必要な保障措置のサブセットとして表される。非連邦政府組織におけるこのようなプログラムの強度と品質は、その組織が連邦政府による規定なしに日常的に満たされると期待されるようなセキュリティ要件と管理策を実装するような度合いに依存する。これには、有効なリスクベースの情報セキュリティプログラムをサポートするような、セキュリティポリシー、手順、及び実践の実装が含まれる。非連邦政府組織は、第 3 章のセキュリティ要件の適用範囲外と思われる中位のベースラインのセキュリティ管理策の完全なリストとして、附属書 E 及び SP 800-53 を参照することが推奨される。

制（実施）する。
- 基本的な機能のみを提供するようシステムを構成することによって、最小限の機能の原則を採用する。
- 非基本のプログラム、機能、ポート、プロトコル、及びサービスの使用を制限、無効化、及び防止する。
- 許可されないソフトウェアの使用を防止するために例外による拒否（ブラックリスト）ポリシーを、または許可されたソフトウェアの実行を許可するような例外による許可（ホワイトリスト）ポリシーを適用する。
- 利用者がインストールしたソフトウェアを管理し、監視する。

使いやすさのために、セキュリティ要件は、14 の*ファミリ*で構成されている。それぞれのファミリには、そのファミリの一般的なセキュリティトピックに関連する要件が含まれている。ファミリは、FIPS Publication 200 に記述された連邦政府情報及びシステムの最小限のセキュリティ要件を用いて密接に整理されている。*コンティンジェンシープラン(緊急時対応計画)*、*システム及びサービス調達*、及び*計画* 要件は、前述の調整の基準[17]のため本発行文書の適用範囲には含まれない。表 1 には、本発行文書で対処されるセキュリティ要件ファミリを列挙している。

表 1：セキュリティ要件ファミリ

ファミリ	ファミリ
アクセス制御	メディア保護
意識向上と訓練	要員のセキュリティ
監査と責任追跡性	物理的保護
構成管理	リスクアセスメント
識別と認証	セキュリティアセスメント
インシデント対応	システムと通信の保護
メンテナンス	システムと情報の完全性

[17] 3 つの例外には以下が含まれる：*緊急時対応計画*ファミリからのシステムバックアップの機密性を保護するための要件（CP-9 から導出）；*計画*ファミリからのシステムセキュリティ計画を策定及び実装するための要件（PL-2 から導出）；*システムとサービス調達*ファミリからのシステムセキュリティエンジニアリングの原則を実装するための要件（SA-8 から導出）。利便性のため、これらの要件は、CUI *メディア保護*、*セキュリティ評価*、*及びシステムと通信保護*の要件ファミリにそれぞれ含まれる。

第 3 章
要件

CUI の機密性を保護するためのセキュリティ要件

本章は、連邦政府外のシステムと組織における CUI の機密性を保護[18]するためのセキュリティ要件の 14 のファミリ(基本的及び導出された要件を含めて）について記述する。基本的及び導出された要件に関連する NIST Special Publication 800-53 からのセキュリティ管理策は、附属書 D[19] でも列挙されている。組織は、セキュリティ要件に関連する追加の、自由な情報（例、参照されるセキュリティ管理策のそれぞれに関連する補足ガイダンス、ISO/IEC セキュリティ管理策へのマッピングテーブル、及び必要に応じて追加のセキュリティ要件の指定を支援するために利用可能なオプションの管理策の一覧）を取得するため、Special Publication 800-53 を利用することができる。この情報は、ミッションとビジネスの要件、運用環境、またはリスクアセスメントとの関連で、要件の明確化または解釈に役立てることが可能である。非連邦組織は、セキュリティ要件を満たすため、直接にまたは管理されたサービスの利用を通して、さまざまな可能性のあるセキュリティソリューションを実装でき、また代替策であるが、特定の要件[20]を満たすことができないものについて補償するような、同様の効果を有するセキュリティ対策を実装してもよい。

非連邦組織は、システムセキュリティ計画において、指定されたセキュリティ要件がどのように満たされるか、または組織計画が要件をどのように満たすかについて記述するべきである。計画にはシステムの境界；運用環境；セキュリティ要件の実装される方法；及びその他のシステムとの関係やコネクションについて記述される。連邦政府外の組織は、実装されないセキュリティ要件がどのように満たされるか、及び計画される軽減策がどのように実装されるかについて記述されるような行動計画を立案するべきである。組織は、システムセキュリティ計画及び行動計画を別文書または統合された文書として任意のフォーマットで文書化することができる。

要求されたとき、システムセキュリティ計画、及びそれに関連する、計画された実装または軽減策についての行動計画は、連邦政府外の組織の実装または計画されたセキュリティ要件の実装を論証するため責任のある連邦政府機関／契約担当官へ提出されるべきである。連邦政府機関は、提出されたシステムセキュリティ計画と行動計画について、連邦政府外の組織によって運用されるシステム上の CUI を処理、保存、または送信するため、及び連邦政府外の組織との合意または契約を進めることが望ましいかどうかの、全体的なリスク管理上の決定への重要な入力として検討するかもしれない。

本発行文書のセキュリティ要件は、連邦政府外の組織の内部システムが CUI を処理、保存、または送信に適用されるべきである。特化したシステム(例、産業／プロセス制御システム、コンピュータ数値制御マシン、医療デバイス)を含めて、何らかのシステムは、特定のセキュリティ要件の適用において、制約または制限があるかもしれない。このような課題に対応するため、シ

---

[18] 本出版文書の目的は CUI の機密性を保護するための要件を定義することであるが、多くの下位のセキュリティメカニズムがシステムレベルにおいて、機密性と完全性の両方のセキュリティ対策方針をサポートするため、機密性と完全性の間には緊密な関係が存在する。従って、完全性の要件（基本または導出のいずれか）は、重要であり、間接的ではあるが、組織が CUI の機密性を保護する能力に影響を及ぼすかもしれない。

[19] 附属書 D のセキュリティ管理策参照は、セキュリティ要件をよりよく理解するために含まれている。管理策参照は、非連邦政府組織に追加の要件を導入することを意図していない。さらに、セキュリティ管理策は連邦政府機関のために開発されたものなので、それらの管理策に対応する補足ガイダンスは、非連邦政府組織には適用できないかもしれない。

[20] 一貫性、透明性、及び互換性を促進するため、組織によって選択された補償的なセキュリティ対策は、以下の例を含めて、*既存の*、かつ*認識された*セキュリティ標準と管理策のセットに基づいたものであるべき、または導出されたものであるべきである：ISO/IEC 27001 または NIST SP 800-53。

ステムセキュリティ計画は、要件 3.12.4 で反映されるものとして、セキュリティ要件への不朽の例外を記述するために使用されるべきである。個別の、孤立した、または一時的な欠乏は、要件 3.12.2 で反映されるとおり、行動計画を通して管理されるべきである。

3.1 アクセス制御

基本的セキュリティ要件

3.1.1 システムアクセスを許可された利用者、許可された利用者を代行して動作するプロセス、またはデバイス(その他のシステムを含めて) に制限する。

3.1.2 システムアクセスを許可された利用者に対して実行が許可された種類のトランザクション及び機能に制限する。

導出されたセキュリティ要件

3.1.3 承認された権限付与に従って CUI のフローを制御する。

3.1.4 共謀のない悪意のあるアクティビティのリスク低減のため、個人の職務を分離する。

3.1.5 具体的なセキュリティ機能と特権アカウントを含め、特権の最小化の原則を採用する。

3.1.6 非セキュリティ機能をアクセスするときは、非特権アカウントまたは役割を使用する。

3.1.7 非特権利用者による特権機能の実行とこのような機能の実行の監査を防止する。

3.1.8 ログイン試行失敗を制限する。

3.1.9 適用可能な CUI 規則と整合性のあるプライバシーとセキュリティの通知を提供する。

3.1.10 非アクティブな時間の経過後、データのアクセス及び閲覧を防止するため、パタンによる不可視化表示を用いてセションロックを使用する。

3.1.11 定義された条件の後、利用者セションを(自動的に) 終了する。

3.1.12 リモートアクセスセションを監視し、制御する。

3.1.13 リモートアクセスセションの機密性を保護するために暗号メカニズムを採用する。

3.1.14 管理されたアクセス制御ポイントを介してリモートアクセスをルーティングする。

3.1.15 特権コマンドのリモート実行とセキュリティ関連情報へのリモートアクセスを許可する。

3.1.16 無線のコネクションを許可する前に無線アクセスを許可する。

3.1.17 認証と暗号化を用いて無線アクセスを保護する。

3.1.18 モバイルデバイスのコネクションを制御する。

3.1.19 モバイルデバイス及びモバイルコンピューティングプラットフォーム[21]上の CUI を暗号化する。

3.1.20 外部システムへのコネクション及び使用を検証し、制御／制限する。

3.1.21 外部システム上での組織のポータブルストレージデバイスの使用を制限する。

3.1.22 公開アクセス可能なシステムにおいて掲載または処理される CUI を制御する。

[21] モバイルデバイスおよびモバイルデバイスコンピューティングプラットフォームには、例えば、スマートフォン、タブレット、電子リーダ、及びノート PC が含まれる。

3.2 意識向上と訓練

基本的セキュリティ要件

3.2.1 組織のシステムの責任者、システム管理者、及び利用者が、彼らのアクティビティに関連するセキュリティリスク及びそれらのシステムのセキュリティに関連する適用可能なポリシー、基準、及び手順について周知されていることを、保証する。

3.2.2 組織の要員が、その割り当てられた情報セキュリティ関連の職務と責任を遂行するために適切に訓練されていることを、保証する。

導出されたセキュリティ要件

3.2.3 内部からの脅威の潜在指標の認識と報告についてのセキュリティ周知訓練を提供する。

3.3 監査と責任追跡性(説明責任)

基本的セキュリティ要件

3.3.1 非合法の、許可されない、または不適切なシステムアクティビティの監視、分析、調査、及び報告を可能とするために必要な範囲で、システム監査記録を作成、保護、及び維持する。

3.3.2 個別のシステム利用者のアクションが、彼らのアクションについての説明責任を維持可能にするよう、それらの利用者に対して一意に追跡が可能であることを保証する。

導出されたセキュリティ要件

3.3.3 監査された事象をレビューし、アップデートする。

3.3.4 監査プロセス失敗の事象においてアラート(警告) を発する。

3.3.5 監査記録のレビュー、分析、及び調査のための報告プロセスを集めて相互の関係を比較し、不適切な、疑わしい、または異常なアクティビティの兆候に対応する。

3.3.6 オンデマンド分析と報告をサポートするため、監査の簡素化と報告書生成を提供する。

3.3.7 監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し同期するようなシステム機能を提供する。

3.3.8 監査情報と監査ツールを不正なアクセス、改変、及び削除から保護する。

3.3.9 監査機能の管理を特権利用者の一部に制限する。

3.4 構成管理

基本的セキュリティ要件

3.4.1 個別のシステム開発ライフサイクル全体で、組織のシステム（ハードウェア、ソフトウェア、ファームウェア、及び文書を含めて）のベースライン構成とインベントリを確立し、維持する。

3.4.2 組織のシステムで採用された情報技術製品のセキュリティ構成設定を確立し、強制（実施）する。

導出されたセキュリティ要件

3.4.3 組織のシステムへの変更を追跡、レビュー、承認／非承認、及び監査する。

3.4.4 実装に先立ち、変更のセキュリティへの影響を分析する。

3.4.5 組織のシステムへの変更に関連する物理的及び論理的なアクセス制約事項を定義し、文書化し、承認し、強制（実施）する。

3.4.6 基本機能のみを提供するように組織のシステムを構成することによって、最小機能の原則を採用する。

3.4.7 非基本プログラム、機能、ポート、プロトコル、及びサービスの使用を制限、無効化、及び防止する。

3.4.8 許可されないソフトウェアの使用を防止するために例外による拒否（ブラックリスト）ポリシーを、または許可されたソフトウェアの実行を許可するような例外による許可（ホワイトリスト）ポリシーを適用する。

3.4.9 利用者がインストールしたソフトウェアを管理し、監視する。

3.5 識別と認証

基本的セキュリティ要件

3.5.1 システム利用者、利用者を代行して動作するプロセス、またはデバイスを識別する。

3.5.2 組織のシステムへのアクセスの許可に対する必要条件として、それらの利用者、プロセス、またはデバイスのアイデンティティを認証(または検証)する。

導出されたセキュリティ要件

3.5.3 複数要素の認証[22]を、特権アカウントへのローカル及びネットワークアクセス[23]のために、及び非特権アカウントへのネットワークアクセスのために、使用する。

3.5.4 特権及び非特権アカウントへのネットワークアクセスのために、リプレイ耐性のある認証メカニズムを採用する。

3.5.5 定義された期間について、識別コードの再利用を禁止する。

3.5.6 定義された非アクティブな期間の後、識別子を無効化する。

3.5.7 新しいパスワードが作成されるとき、最小パスワード複雑性及び文字列の変更を強制(実施)する。

3.5.8 規定された生成回数の間、パスワードの再利用を禁止する。

3.5.9 永久パスワードへ直ちに変更するようなときのシステムログインのために一時的パスワードの使用を許可する。

3.5.10 暗号学的に保護されたパスワードのみを格納及び送信する。

3.5.11 認証情報のフィードバックを目に見えないようにする。

3.6 インシデント対応

基本的セキュリティ要件：

3.6.1 適切な準備、検知、分析、抑制（封じ込め)、リカバリ、及び利用者対応アクティビティを含めて、組織のシステムのための運用上のインシデントハンドリング能力を確立する。

3.6.2 組織の内部及び外部の両方の、適切な担当官及び／または権威に対して、インシデントについて

[22] *複数要素認証* は、2 つ以上の異なる要素を認証達成のために要求する。要素には以下を含む：あなたが知っている何か（例、パスワード／PIN）；あなた持っている何か（例、暗号識別デバイス、トークン）；あなたである何か（例、生体情報)。複数要素認証の要件は、連邦政府個人本人性検証（PIV：Personal Identity Verification）カードまたは国防総省共通アクセスカード（CAC）のようなソリューションを要求するものとして解釈されるべきではない。トークンや生体情報を用いるようなさまざまな複数要素ソリューション（リプレイ耐性を持つものを含む）が市販され、利用可能である。このようなソリューションは、利用者クレデンシャルを格納するハードトークン（例、スマートカード、キーフォブ、またはドングル）またはソフトトークンを採用してもよい。

[23] *ローカルアクセス*は、ネットワークの利用なしに直接の接続を通して通信している利用者（または利用者を代行するプロセス）による情報システムへのアクセスである。*ネットワークアクセス*は、ネットワーク（例、ローカルエリアネットワーク、ワイドエリアネットワーク、インターネット）を通して通信している利用者（または利用者を代行するプロセス）による情報セシステムへのアクセスである。

の追跡、文書化、及び報告を行う。

導出されたセキュリティ要件：
3.6.3 組織のインシデント対応能力をテストする。

3.7 メンテナンス

基本的セキュリティ要件：
3.7.1 組織のシステムにおいてメンテナンスを実施する。[24]

3.7.2 システムメンテナンスを実施するために使用されるツール、手法、メカニズム、及び要員における有効な管理策を提供する。

導出されたセキュリティ要件：
3.7.3 オフサイトのメンテナンスのために除去される装置は、あらゆる CUI についてサニタイズされることを保証する。

3.7.4 組織のシステム内でメディアが使用される前に、悪意のあるコードが入っていないか診断及びテストプログラムを用いてメディアをチェックする。

3.7.5 外部のネットワークコネクションを介した非ローカルメンテナンスセションを確立するため、複数要素の認証を要求し、非ローカルメンテナンスの完了時にこのようなセションを終了する。

3.7.6 必要なアクセス許可なしにメンテナンス要員のメンテナンス活動を監督する。

3.8 メディア保護

基本的セキュリティ要件：
3.8.1 紙及びディジタルの両方の、CUI を含む、システムメディアを保護する(即ち、物理的に制御及びセキュアに格納する)。

3.8.2 システムメディア上の CUI へのアクセスを許可された利用者に制限する。

3.8.3 廃棄または再利用のために手放す前に、CUI を含むシステムメディアをサニタイズまたは破壊する。

導出されたセキュリティ要件：
3.8.4 CUI のマーク表示と配付制限が必要なメディアに対して表示を行う。[25]

3.8.5 CUI を含むメディアへのアクセスを制御し、管理エリアの外部への持ち出し中のメディアの説明責任を維持する。

3.8.6 代替の物理的予防手段による保護がない限り、持ち出し中はディジタルメディア上に格納された CUI の機密性を保護するための暗号学的メカニズムを実装する。

3.8.7 システムコンポーネント上の取り外し可能なメディアの使用を管理する。

3.8.8 ポータブルストレージデバイスに識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。

[24] 一般に、システムメンテナンス要件は、*可用性*のセキュリティ対策方針をサポートする傾向がある。しかし、不適切なシステムメンテナンスまたはメンテナンス実行時の不具合は、CUI の不正な暴露をもたらす可能性がある、すなわち、その情報の機密性を危殆化する。

[25] 本要件の実装は、32 CFR、Part 2002、及び CUI レジストリにおけるマーク付けガイダンスの完成を条件としている。

3.8.9　保存場所にあるバックアップ CUI の機密性を保護する。

3.9　人的セキュリティ

基本的セキュリティ要件

3.9.1　CUI を含む組織のシステムへのアクセスを許可する前に、個人を審査する。

3.9.2　離職または配置転換等の人事措置の間と後で、CUI 及び CUI を含む組織のシステムが保護されることを保証する。

導出されたセキュリティ要件：なし

3.10　物理的保護

基本的セキュリティ要件：

3.10.1　組織のシステム、装置、及びそれぞれの運用環境への物理的アクセスを許可された個人に制限する。

3.10.2　物理的設備を保護し、監視し、組織のシステムの基盤をサポートする。

導出されたセキュリティ要件：

3.10.3　訪問者をエスコートし、訪問者の活動を監視する。

3.10.4　物理的アクセスの監査ログを維持する。

3.10.5　物理的アクセスデバイスを制御し、管理する。

3.10.6　代替の作業サイト(例、テレワークのサイト)での CUI に対する防護対策を強制(実施)する。

3.11　リスクアセスメント

基本的セキュリティ要件：

3.11.1　組織のシステムの運用と関連する CUI の処理、ストレージ、または送信からの結果として、組織の運用(ミッション、職務、イメージ、または風評を含めて)、組織の資産、及び個人に対するリスクを定期的にアセスメントする。

導出されたセキュリティ要件：

3.11.2　定期的に、及び組織のシステムとアプリケーションに影響する新しい脆弱性が識別されるときに、それらのシステム及びアプリケーションの脆弱性についてスキャンする。

3.11.3　リスクのアセスメントに従い、脆弱性を修正する。

3.12　セキュリティアセスメント

基本的セキュリティ要件：

3.12.1　管理策がそれらのアプリケーションにおいて有効であるかどうかを決定するために、組織のシステムにおけるセキュリティ管理策を定期的にアセスメントする。

3.12.2　欠陥を修正し、組織のシステムにおける脆弱性を軽減し、または取り除くために設計された行動計画を策定し、実施する。

3.12.3　管理策の継続的な有効性を保証するため、継続的にセキュリティ管理策を監視する。

3.12.4 システムの境界、システムの運用環境、セキュリティ要件の実装方法、及び他のシステムとの関係または他のシステムへのコネクションについて記述した、システムセキュリティ計画[26]を策定、文書、及び定期的に更新する。

導出されたセキュリティ要件：なし

3.13 システムと通信の保護

基本的セキュリティ要件：

3.13.1 外部の境界及びシステムの鍵となる内部境界における通信（即ち、組織のシステムによって送信または受信される情報）を監視し、制御し、保護する。

3.13.2 組織のシステム内の有効な情報セキュリティを促進するような、アーキテクチャ設計、ソフトウェア開発手法、及びシステムエンジニアリングの原則を採用する。

導出されたセキュリティ要件：

3.13.3 利用者機能をシステム管理機能と分離する。

3.13.4 共有システム資源を介した、不正な予期せぬ情報の転送を防止する。

3.13.5 内部ネットワークから物理的にまたは論理的に分離される、公開アクセス可能なシステムコンポーネント用には、サブネットワークを実装する。

3.13.6 デフォルトでネットワーク通信トラフィクを拒否し、また例外によってネットワーク通信トラフィクを許可する(即ち、すべて拒否、例外で許可)。

3.13.7 リモートデバイスが、組織のシステムとの非リモートコネクションの確立と同時に、外部ネットワークの資源への何らかの他のコネクションを介して通信することを防止する。

3.13.8 代替の物理的予防手段による保護がない限り、持ち出し中に CUI の不正な暴露を防止するために暗号学的メカニズムを実装する。

3.13.9 セション終了時または定義された非アクティブな時間の経過後に、通信セションに対応するネットワークコネクションを終了する。

3.13.10 組織のシステムで採用された暗号のための暗号鍵を確立し、管理する。

3.13.11 CUI の機密性を保護するために使用されるとき、FIPS 認証された暗号を採用する。

3.13.12 共同コンピューティングデバイスのリモートからの活性化を禁止し[27]、使用中のデバイスの兆候をデバイスに存在する利用者に提供する。

3.13.13 モバイルコードの使用を管理し監視する。

3.13.14 VoIP 技術の使用を管理し、監視する。

3.13.15 通信セションの真正性を保護する。

3.13.16 保存された CUI の機密性を保護する。

3.14 システムと情報の完全性

基本的セキュリティ要件：

[26] システムセキュリティ計画の詳細についての所定のフォーマットまたは規定のレベルは定められていない。しかし、組織は、3.12.4 の必須の情報がそれらの計画において適切に伝えられることを保証しなければならない。

[27] ビデオ会議を活性化するために他者を呼び出したり、接続したりする参加者に信頼を置くような、ビデオ会議専用システムは、除外される。

3.14.1　タイムリーなやり方で情報及びシステムフローを識別し、報告し、訂正する。

3.14.2　組織のシステム内の適切な場所で、悪意のあるコードから保護を提供する。

3.14.3　システムセキュリティ警報及びアドバイザリを監視し、適切な対応アクションを取る。

導出されたセキュリティ要件：

3.14.4　新しいリリースが利用可能となったとき、悪意のあるコードからの保護メカニズムをアップデートする。

3.14.5　組織のシステムの定期的スキャン、及びファイルがダウンロードされ、開かれ、または実行されるような、外部情報源からのファイルのリアルタイムスキャンを実行する。

3.14.6　内向き及び外向きの通信トラフィクを含めて、攻撃や潜在的な攻撃の兆候を検知するため、組織のシステムを監視する。

3.14.7　組織のシステムの不正な使用を識別する。

NARA, CUI 要件、及び FAR 条項

大統領行政命令 13556、管理された非格付け情報、2010 年 11 月 4 日付、は CUI プログラムを制定し、大統領行政命令への適合を保証するために活動する大統領行政命令の執行行政機関として国立公文書記録管理局（NARA）を指定した。CUI 行政機関は、監督責任と要件の決定と同様に請負業者への NIST SP 800-171 の要件の適用のため、2017 年の 1 つの連邦調達令（FAR）を制定すると予測されている。行政機関は、32 CFR Part 2002 における連邦政府機関の監督を包含するようにも対処する。連邦政府の監督へのアプローチは、統一 CUI FAR 条項、将来の理解、及び連邦政府機関とそれらの非連邦政府情報共有パートナー間の合意を通して決定される。

附属書 A
参照文書

法律、大統領行政命令、政令、指令、標準及びガイドライン[28]

法令、大統領行政命令、及び政令

1. Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014.
http://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf
2. 大統領行政命令 13556, Controlled Unclassified Information, November 2010.
http://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf
3. 大統領行政命令 13636, Improving Critical Infrastructure Cybersecurity, February 2013.
http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
4. 32 CFR Part 2002, *Controlled Unclassified Information*, September 2016.

標準、ガイドライン、及び指令

1. National Institute of Standards and Technology Federal Information Processing Standards Publication 199 (as amended), Standards for Security Categorization of Federal Information and Information Systems.
http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
2. *National Institute of Standards and Technology Federal Information Processing Standards Publication 200 (as amended), Minimum Security Requirements for Federal Information and Information Systems.*
http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
3. National Institute of Standards and Technology Special Publication 800-53 (as amended), *Security and Privacy Controls for Federal Information Systems and Organizations*.
http://doi.org/10.6028/NIST.SP.800-53r4
4. National Institute of Standards and Technology Special Publication 800-60 (as amended), *Guide for Mapping Types of Information and Information Systems to Security Categories*, Volume 1.
http://doi.org/10.6028/NIST.SP.800-60v1r1
5. National Institute of Standards and Technology Special Publication 800-60 (as amended), *Guide for Mapping Types of Information and Information Systems to Security Categories*, Volume 2.
http://doi.org/10.6028/NIST.SP.800-60v2r1
6. National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity* (as amended).
http://www.nist.gov/cyberframework
7. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2013, *Information technology -- Security techniques -- Information security management systems -- Requirements*, September 2013.
8. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27002:2013, *Information technology -- Security techniques -- Code of practice for information security controls*, September 2013.
9. Committee on National Security Systems Instruction 4009 (as amended), *National Information Assurance Glossary*.
https://www.cnss.gov

その他の情報源

1. National Archives and Records Administration, *Controlled Unclassified Information Registry*.
https://www.archives.gov/cui/registry/category-list

[28] 具体的な発行日または改訂版数の付いていない本セクションの参照文書は、それらの出版物の最も最新のアップデートを参照すると想定される。

附属書 B

用語集

共通用語と定義

附属書 B は、SP 800-171 で利用されるセキュリティ用語の定義を提供する。本用語集で特に定義されることなしに、本出版で資料されるすべての用語は、CNSS Instruction 4009、*米国国家情報保証 用語集* に含まれる定義と一貫している。

政府機関（agency）	*行政機関（局）（executive agency）*を参照。
アセスメント（assessment）	*セキュリティ管理策アセスメント（security Control Assessment）*を参照。
アセッサ（assessor）	*セキュリティ管理策アセッサ（security Control Assessor）*を参照。
監査ログ（audit log） [CNSSI 4009]	所与の期間のシステムアクセスの記録と実行された操作を含めて、情報システム活動の時系列順の記録。
監査記録（audit record）	監査事象に関連する監査ログにおける個別のエントリ。
認証（authentication） [FIPS 200, adapted]	情報システムの資源へアクセスを許可する前に、しばしば利用者、プロセス、またはデバイスの識別を検証すること。
可用性（availability） [44 U.S.C., Sec.3542]	情報へのアクセス及び情報の活用についてタイムリーかつ信頼性をもって保証すること。
ベースライン構成	所与の時点で正式にレビューされ合意された、変更管理手順を介してのみ変更可能な、システム内の情報システムの文書化された一連の仕様または構成項目。
ブラックリスト（blacklisting）	以下を特定するために利用されるプロセス：(i) 情報システムにおいて実行することが許可されないソフトウェアプログラム；または（ii）禁止された URL／ウェブサイト。
機密性（confidentiality） [44 U.S.C., Sec.3542]	個人のプライバシー及び専有情報の保護のための手段を含め、情報アクセスと開示における許可された制限の維持。
構成管理（configuration management）	システム開発ライフサイクル全体を通しての情報技術製品と情報システムの設定についての初期化、変更及び監視を介して、それらの製品及びシステムの完全性の確立と維持に焦点を当てた活動の集まり。
構成設定（configuration settings）	セキュリティ法律及び／または情報システムの機能に影響を与えるような、ハードウェア、ソフトウェアまたはファームウェアを変更可能な一連のパラメタ。

管理された区域（controlled area）	提供された物理的及び手続き的保護が、情報及び／または情報システム保護のために確率された要件を満たすために十分であるという確信をその組織が持つような任意の区域または空間。
管理された非格付け情報 （controlled unclassified information）[E.O. 13556]	法律政令、または政府全体のポリシーが安全防護または配布管理を行うことを要求するような情報、大統領行政命令 13526, *格付けされた国家安全保障情報*、2009 年 12 月 29 日付、または以前のまたは後継の大統領行政命令、または 1954 年の原子力エネルギー法、その改正を含む、の下で格付けされる情報を除く。
CUI カテゴリまたはサブカテゴリ（CUI categories or subcategories）[Title 32 CFR, Part 2002]	法律、政令、または政府全体のポリシーが安全防護または配布の管理を要求するような情報の種別で、CUI 行政機関（局）が承認し、CUI レジストリにリスト掲載したもの。
CUI 行政機関（局）CUI Executive Agent [Title 32 CFR, Part 2002]	国立公文書記録管理局（NARA）のことで、行政機関（省）にわたる CUI プログラムを実施し、大統領行政命令 13556 に適合するための連邦政府機関の活動を監督する。NARA は、情報セキュリティ監督局（ISOO：Information Security Oversight Office）の長として本権限を委任されている。
CUI プログラム（CUI program）[Title 32 CFR, Part 2002]	行政機関（省）にわたるプログラムで、連邦政府機関による CUI 取り扱いを標準化するもの。本プログラムは、大統領行政命令 13556、32 CFR Part 2002、及び CUI レジストリによって制定され、CUI に対する規則、組織及び手順を含む。
CUI レジストリ（CUI registry）[Title 32 CFR, Part 2002]	CUI の取り扱いに関するすべての情報、ガイダンス、ポリシー、及び要件についてのオンラインリポジトリで、CUI 行政機関（局）によるすべての発行を含む。その他の情報の間に、CUI リポジトリは、承認された CUI カテゴリ及びサブカテゴリ特定し、それぞれについての概説を提供し、管理策の基本を特定し、また CUI の利用手順を設定する、以下を含むがそれに限らない：情報のマーク付け、保障措置、配送、配布、再利用、及び廃棄。
運用の環境（environment of operation）[NIST SP 800-37, adapted]	情報システムで情報を処理、保存、及び送信する際の物理的な周辺。
行政機関（局）executive agency [41 U.S.C., Sec. 403]	5 U.S.C., Sec. 105 で規定された連邦機関；5 U.S.C., Sec. 102 で規定された軍事機関；5 U.S.C., Sec. 104(1)で定義された独立機関；及び 31 U.S.C., Chapter 91 の条項の対象となる完全に政府保有の法人。

外部情報システム（またはコンポーネント） external system (or component)	組織によって制定された権限付与の境界の外部にあり、その組織が必須のセキュリティ管理策またはセキュリティ管理策の有効性のアセスメントの適用について直接管理しないような、情報システムまたは情報システムのコンポーネント。
外部情報システムサービス （external system service）	その組織の情報システムの権限付与境界の外部に実装され（即ち、その組織の情報システムにより利用されるが、その組織の情報システムの一部でない）、その組織が通常必須のセキュリティ管理策の適用またはセキュリティ管理策の有効性のアセスメントを介して直接の管理を行わないような、情報システムサービス。
外部情報システムサービスプロバイダ （external system service provider）	さまざまな消費者—生産者関係を通してある組織への外部情報システムサービスの提供者で、以下を含むがそれに限定されない：ジョイントベンチャー；ビジネスパートナーシップ；外部委託協定（即ち、契約、政府機関間の合意、ビジネス協定の類を介して）；ライセンス契約；及び／またはサプライチェイン取引。
外部ネットワーク （external network）	その組織によって管理されていないネットワーク。
連邦政府機関 （federal agency）	*行政機関（局）*を参照。
連邦政府情報システム （federal information system） [40 U.S.C., Sec.11331]	行政機関（局）によって、行政機関の請負業者によって、または行政機関を代行する別の組織によって利用され、運用される、情報システム。
FIPS 認証済み暗号 （FIPS-validated cryptography）	FIPS Publication 140-2（その改正を含む）で規定される要件を満たすために、暗号モジュール認証プログラム（CMVP）によって認証された暗号モジュール。CMVP 認証に先立つものとして、その暗号モジュールは、暗号アルゴリズム認証プログラム（CAVP）による認証テストに合格した暗号アルゴリズム実装を採用するよう要求されている。*NSA 承認済み暗号*を参照。
ファームウェア （firmware）	ハードウェア—通常は読み出し専用メモリ（ROM）またはプログラム可能読み出し専用メモリ（PROM）に保存されたコンピュータプログラムとデータで、そのプログラムとデータは、プログラムの実行中に動的に書き込み、または改変ができないもの。
ハードウェア （hardware）	情報システムの物理的コンポーネント。*ソフトウェア*及び*ファームウェア*を参照。
影響 （impact）	情報または情報システムの機密性、完全性、または可用性の喪失が及ぼす、組織の運用、組織の資産、個人、その他の組織、または国（合衆国の国家安全保障上の利害を含む）に対する影響。
影響値 （impact value）	低度、中位、または高度の値として表現されるような、情報（例、CUI）の機密性の危殆化からもたらされる評定された潜在的な影響。

インシデント（incident） [FIPS 200,adapted]	情報システムまたはそのシステムが処理、保存、または送信する情報の機密性、完全性、または可用性を実際にまたは潜在的に危険にさらすような事象、またはセキュリティポリシー、セキュリティ手順、または受け入れ可能な利用ポリシーの違反または違反の差し迫った脅威を成す事象。
情報（information）	任意のメディアまたは形態の事実、データまたは意見のような通信または知識の表現で、テキスト、数字、画像、地図、談話、または音声映像を含む。
情報フロー制御（information flow control）	システム内の情報転送がセキュリティポリシーの違反とならないことを保証するための手続き
情報資源（information resources） [44U.S.C.,Sec.3502]	要員、装置、資金、及び情報技術のような、情報と関連する資源。
情報セキュリティ（information security） [44U.S.C.,Sec.3542]	機密性、完全性及び可用性を提供するために許可されないアクセス、利用、暴露、混乱、改変、または破壊からの情報と情報システムの保護。
情報システム（information system） [44U.S.C.,Sec.3502]	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の個別の集まり。
情報技術（information technology） [40U.S.C.,Sec.1401]	行政機関によって、自動化調達、データまたは情報の保存、操作、管理、移動、制御、表示、スイッチ、交換、送信、受信において利用されるような、任意の装置または相互接続されたシステムまたは装置のサブシステム。前文の目的のため、その装置が行政機関によって直接利用されるか、または以下のような行政機関との契約の下で請負業者によって利用される場合、装置は行政機関によって利用されることになる：(i) このような装置の利用を要求する；または (ii) あるサービスの性能の点で、またはある製品の供給の点で、かなりの程度まで、このような装置の利用を要求する。用語*情報技術*には、コンピュータ、補助的な装置、ソフトウェア、ファームウェア、及び同様の手順、サービス（サポートサービスを含めて）、及び関連する資源が含まれる。
インサイダー脅威（insider threat）	内部の者が米国のセキュリティに害をなすために、故意に無意識に脅威
完全性（integrity） [44U.S.C.,Sec.3542]	不適切な情報改変または破壊に対する保護、及び情報否認防止と真正性の保証を含む。

内部ネットワーク（internal network）	セキュリティ管理策の確立、維持、及びプロビジョニングが組織の従業員または請負業者の直接の管理下にある；または組織が管理する複数の端点間で実装される暗号カプセル化または同様なセキュリティ技術が同様な効果を提供する（機密性と完全性に関して）であるようなネットワーク。内部ネットワークは通常組織所有のものであるが、組織が所有しないが組織の管理下にあるものかもしれない。
最小限の特権（least privilege）	それぞれのエンティティがその機能を実行するために必要な最小限のシステム資源と権限を保証されるようにセキュアリティアーキテクチャが設計されるべき原理。
ローカルアクセス（local access）	ネットワークの利用なしに直接の接続を介して通信している、利用者（または利用者を代行するプロセス）による組織の情報システムへのアクセス。
悪意のあるコード（malicious code）	情報システムの機密性、完全性、または可用性に不利な影響を与えるような、許可されない処理を実行することを意図したソフトウェアまたはファームウェア。ウィルス、ワーム、トロイの木馬、またはホストに感染するその他のコードベースのエンティティ。スパイウェアと何らかの形態のアドウェアについても、悪意のあるコードの例である。
メディア（media）[FIPS 200]	物理メディアまたは書き物で、以下を含むがそれに限定されない：情報システム内で、情報が記録され、保存され、印刷されたような、磁気テープ、光ディスク、磁気ディスク、大規模集積回路（LSI）メモリチップ、及び印刷物（ただし、表示メディアは含まない）。
モバイルコード（mobile code）	明示的なインストールまたは受信者による実行なしに、リモートの情報システムから取得され、ネットワークを介して送信され、ローカル情報システム上で実行されたソフトウェアプログラムまたはプログラムの一部。
モバイルデバイス（mobile device）	以下のような、可搬のコンピューティングデバイス：(i) 個人によって容易に持ち運び可能なように小さい形状のもの；（ii）物理的接続なしに操作するよう設計されたもの（例、無線での情報の送信または受信）；(iii) ローカルで処理、取り外し可能でないまたは取り外し可能なデータストレージ；及び（iv）電源内蔵。モバイルデバイスには音声通信機能、情報を取り込むことを可能にする基盤上のセンサ、及び／または離れた場所でのローカルデータを同期するビルトイン機能が含まれる。例としてはスマートホン、タブレット、及び電子リーダが含まれる。
多要素認証（multifactor authentication）	認証を達成するために 2 つ以上の異なる要素を用いた認証。要素には、あなたが知っている何か（例、パスワード／PIN）；あなた持っている何か（例、暗号識別デバイス、トークン）；あなたである何か（例、バイオメトリック）を含む。*認証コード*を参照。

連邦政府外の情報システム（nonfederal information system）	連邦政府情報システムの基準を満たさないような情報システム。
連邦政府外の組織（nonfederal organization）	連邦政府外の情報システムを所有し、運用し、または維持するエンティティ。
連邦政府外のシステム nonfederal system	連邦政府システムの基準を満たさないようなシステム
ネットワーク（network）	相互接続されたコンポーネントの集まりと共に実装された情報システム。このようなコンポーネントには、ルータ、ハブ、ケーブル、通信制御器、鍵配付センタ、及び技術的な管理デバイスが含まれるかもしれない。
ネットワークアクセス（network access）	ネットワーク（例、ローカルエリアネットワーク、ワイドエリアネットワーク、インターネット）を介して通信している利用者（または利用者を代行するプロセス）による情報システムへのアクセス。
非ローカルメンテナンス（nonlocal maintenance）	ネットワークまたは外部ネットワーク（例、インターネット）または内部ネットワークを通して通信している個人によって行われるメンテナンス活動。
on behalf of (an agency) [32 CFR Part 2002]	A situation that occurs when: (i) a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information; and (ii) those activities are not incidental to providing a service or product to the government.
組織（organization） [FIPS 200, Adapted]	組織的な構造内の任意の規模、複雑さ、または位置付けのエンティティ。
ポータブルストレージデバイス（portable storage device）	情報システムに対して挿入可能で、取り外し可能な、情報システムコンポーネントで、データまたは情報（例、テキスト、ビデオ、音声、及び／または画像データ）を保存するために使用されるもの。このようなコンポーネントは、通常磁気、高額または半導体デバイス（例、フロッピーディスク、コンパクト／ディジタルビデオディスク、フラッシュ／サムドライブ、外部ハードディスクドライブ、及び不揮発性メモリを内蔵するようなフラッシュメモリカード／ドライブ）上に実装される。
潜在的な影響（potential impact） [FIPS 199]	機密性、完全性、または可用性の喪失は、以下を引き起こすと想定される：組織の運営、組織の資産または個人に対して（i）*限定された*不利な影響（FIPS Publication 199 低度）；（ii）*深刻な*不利な影響（FIPS Publication 199 中位）；または（ii）*厳しい*または*壊滅的な*不利な影響（FIPS Publication 199 高度）。

特権アカウント（privileged account）	特権ユーザの権限を付与された情報システムアカウント。
特権ユーザ（privileged user）	通常の利用者が実行を許可されないようなセキュリティ関連の機能を実行することを許可されている（ゆえに、信頼されている）利用者。
記録（records）	組織及び情報システムが意図した通り実行されていることを検証するための基礎として提供される、実行された活動の証拠または達成された結果（例、様式、報告書、テスト結果）の記録（自動化された及び／または手動の）。関連するデータフィールドの単位へ参照するためにも利用される（すなわち、プログラムによってアクセス可能で特定の項目についての完全な情報を含むような、一団のデータフィールド）。
リモートアクセス（remote access）	外部ネットワーク（例、インターネット）を通して通信している利用者（または利用者を代行するプロセス）による組織の情報システムへのアクセス。
リモートメンテナンス（remote maintenance）	外部ネットワーク（例、インターネット）を通して通信している個人によって行われるメンテナンス活動。
リプレイ耐性（replay resistance）	Protection against the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access
リスク（risk）[FIPS 200, Adapted]	あるエンティティが潜在的な環境または事象、及び通常は以下の機能による脅威を持つような程度についての尺度：(i) 環境または事象が発生する場合発生する不利な影響；及び (ii) 出来事の確からしさ。 情報システム関連のセキュリティリストは、情報または情報システムの機密性、完全性、または可用性の喪失から発生するようなリスクであり、組織的な運用（ミッション、機能、イメージ、または評判を含む）、組織の資産、個人、その他の組織、及び国家への潜在的な不利な影響を反映する。
リスクアセスメント（risk assessment）	情報システムの運用からもたらされる、組織的な運用（ミッション、機能、イメージ、評判を含む）、組織の資産、個人、その他の組織、及び国家に対するリスクを特定するプロセス。
サニタイゼ—ション（sanitization）	通常は何らかの形態の無害化、異常な手段の両方によって、回復不能なメディア上に書かれたデータを表示するために取られるアクション。 データ回復が可能でないようにメディアから情報削除する処理。すべての格付けされたレベル、マーク付け、及び活動ログの削除を含む。

セキュリティ（security）	情報システムの利用に対する脅威によって直面するリスクに関わらずそのミッションまたは重要な機能を企業が実行することを可能とするような保護的な対策の確立と維持からもたらされるような状態。保護的対策には、企業のリスク管理アプローチの一部を構成するべき抑止力、回避、防止、検知、回復、及び訂正の組み合わせが含まれてもよい。
セキュリティアセスメント（security assessment）	*セキュリティ管理策アセスメント*を参照。
セキュリティ管理策（security control）[FIPS 199, Adapted]	情報の機密性、完全性、及び可用性を保護するため、定義された一連のセキュリティ要件を満たすように設計された情報システムまたは組織についてあらかじめ規定された保障措置または対策。
セキュリティ管理策アセスメント（security control assessment）[FIPS 199, Adapted]	管理策がどの程度。正しく実装され、意図した通り運用され、情報システムまたは組織に対するセキュリティ要件の満足に関する望ましい結果を生成しているかを決定するための、セキュリティ管理策のテストまたは評価。
セキュリティ機能（security functionality）	組織の情報システムまたはそれらのシステムが動作する環境内で実装された、セキュリティ関連の特徴、機能、メカニズム、サービス、手順及びアーキテクチャ。
セキュリティ機能（security functions）	システムセキュリティポリシーの強制に責任のある、保護の基礎となるコードとデータの分離をサポートしている、情報システムのハードウェア、ソフトウェア、及び／またはファームウェア。
セキュリティ関連（security relevance）	Functions or mechanisms that are relied upon, directly or indirectly, to enforce a security policy that governs confidentiality, integrity, and availability protections.
分散トンネリング（split tunneling）	The process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices (e.g., a networked printer) at the same time as accessing uncontrolled networks.
補足ガイダンス（supplemental guidance）	セキュリティ管理策またはセキュリティ拡張管理策のための追加の説明情報を提供するために利用されるステートメント。
システム（system）	*情報システム*を参照。

システムコンポーネント（system component）[NIST SP 800-128, adapted]	A discrete, identifiable information technology asset (hardware, software, firmware) that represents a building block of a system. System components include commercial information technology products.
システムセキュリティ計画（system security plan）	A document that describes how an organization meets the security requirements for a system or how an organization plans to meet the requirements. In particular, the system security plan describes the system boundary; the environment in which the system operates; how the security requirements are implemented; and the relationships with or connections to other systems.
システムサービス（system service）	A capability provided by a system that facilitates information processing, storage, or transmission.
脅威（threat）[CNSSI 4009, Adapted]	情報システムを通して、情報の許可されないアクセス、破壊、暴露、改変、及び／またはサービスの拒否を介して、組織の運用（ミッション、機能、イメージ、または評判を含む）、組織の資産、個人、その他の組織、または国家に不利な影響を与える可能性のある状況または事象。
利用者（user）[CNSSI 4009, Adapted]	情報システムをアクセスする権限を付与された、個人、または個人を代行する（システム）処理。
ホワイトリスト（whitelisting）	以下を特定するために利用される処理：(i) 情報システム上で実行する権限を付与されているソフトウェアプログラム；または (ii) 許可された URL／ウェブサイト。
ワイヤレス技術（wireless technology）	Technology that permits the transfer of information between separated points without physical connection.

附属書 C

頭字語

共通の略語

CFR	Code of Federal Regulations (米国連邦行政規則集)
CIO	Chief Information Officer (最高情報責任者)
CNSS	Committee on National Security Systems (米国国家安全保障システム委員会)
CUI	Controlled Unclassified Information (管理された非格付け情報)
FIPS	Federal Information processing Standards (米国連邦情報処理規格)
FISMA	Federal Information Security Modernization Act (米国連邦情報セキュリティ近代化法)
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission (国際標準化機構／国際電気標準会議)
ISOO	Information Security Oversight Office (情報保全監察局)
ITL	Information Technology Laboratory (NIST 情報技術ラボラトリ)
NARA	National Archives and Records Administration (米国国立公文書記録管理局)
NFO	Nonfederal Organization (連邦政府外の組織)
NIST	National Institute of Standards and Technology (米国国立標準技術研究所)
OMB	Office of Management and Budget (行政管理予算庁)
SP	Special Publication (特別発行文書)

附属書 D

マッピング表

CUI セキュリティ要件のセキュリティ管理策へのマッピング

表 D-1 から D-14 は、セキュリティ要件の NIST SP 800-53 の関連するセキュリティ管理策への非形式的なマッピングを提供する。マッピングテーブルは、情報提供目的のみのために含まれており、第 3 章で定義された要件を超えたセキュリティ要件を伝えることを意図していない。さらに、セキュリティ管理策が連邦政府機関のために開発されたゆえに、それらの管理策に対応する補足ガイダンスは、連邦政府外の組織に適用されなくてもよい。ある場合には、関連するセキュリティ管理策には、CUI を保護するために要求されるものを超えた追加の想定を含み、第 2 章の基準を用いて調整される。表には、SP 800-53 から附属書 A、ISO/IEC 27001 の関連する管理策までのセキュリティ管理策の 2 番目のマッピングを含まれることもある。NIST から ISO/IEC へのマッピングは、SP 800-53 附属書 A から得られる。アスタリスク(*)は、ISO/IEC 管理策が NIST 管理策の意図を十分に満たさないことを示す。CUI のための調整のため、基本または導出されたセキュリティ要件の満足は、NIST SP 800-53 からの対応するセキュリティ管理策または拡張管理策が満たされたことを意味しない、なぜなら CUI の機密性の保護に基本的でないような管理策または拡張管理策の具体的なエレメントがそれらの要件に反映されていないからである。

NIST *重要インフラのサイバーセキュリティ改善のフレームワーク*を実装した、または実装する計画の組織は、フレームワークのコア機能：識別、保護、検知、応答、及び回復に対応するカテゴリ及びサブカテゴリの等価な管理策を配置するため、NIST SP 800-53 及び ISO/IEC 27001 のセキュリティ管理策へのセキュリティ要件のマッピングを利用することが可能である。セキュリティ管理策マッピング情報は、確立した情報セキュリティプログラムにおけるセキュリティ要件への適合を実証したい組織は、このようなプログラムが NIST または ISO/IEC セキュリティ管理策を取り込んで構築されたときに役立てることが可能である。

表 D-1：アクセス制御要件のセキュリティ管理策へのマッピング

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
3.1 アクセス制御				
基本セキュリティ要件				
3.1.1 システムアクセスを許可された利用者、許可された利用者を代行して動作するプロセス、またはデバイス(その他のシステムを含めて）に制限する。 3.1.2 システムアクセスを許可された利用者に対して実行が許可された種類のトランザクション及び機能に制限する。	AC-2	アカウント管理	A.9.2.1	利用者登録及び登録抹消
			A.9.2.2	利用者アクセスの提供（provisioning）
			A.9.2.3	特権的アクセス権の管理
			A.9.2.5	利用者アクセス権のレビュー
			A.9.2.6	アクセス権の削除又は修正
	AC-3	アクセス制御の実施	A.6.2.2	テレワーキング
			A.9.1.2	ネットワーク及びネットワークサービスへのアクセス
			A.9.4.1	情報へのアクセス制限
			A.9.4.4	特権的なユーティリティプログラムの使用
			A.9.4.5	プログラムソースコードへのアクセス制御
			A.13.1.1	ネットワーク管理策
			A.14.1.2	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮
			A.14.1.3	アプリケーションサービスのトランザクションの保護
			A.18.1.3	記録の保護
	AC-17	リモートアクセス	A.6.2.1	モバイル機器の方針
			A.6.2.2	テレワーキング
			A.13.1.1	ネットワーク管理策
			A.13.2.1	情報転送の方針と手順
			A.14.1.2	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮
導出されたセキュリティ要件				
3.1.3 承認された権限付与に従ってCUIのフローを制御する。	AC-4	情報フロー制御の実施	A.13.1.3	ネットワークの分離
			A.13.2.1	情報転送の方針と手順

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
			A.14.1.2	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮
			A.14.1.3	アプリケーションサービスのランザクションの保護
3.1.4 共謀のない悪意のあるアクティビティのリスク低減のため、個人の職務を分離する。	AC-5	職務の分離	A.6.1.2	職務の分離
3.1.5 具体的なセキュリティ機能と特権カウントを含め、特権の最小化の原則を採用する。	AC-6	特権の最小化	A.9.1.2	ネットワーク及びネットワークサービスへのアクセス
			A.9.2.3	特権的アクセス権の管理
			A.9.4.4	特権的なユーティリティプログラムの使用
			A.9.4.5	プログラムソースコードへのアクセス制御
	AC-6(1)	特権の最小化 *セキュリティ機能へのアクセスを許可する*	直接のマッピングなし	
	AC-6(5)	特権の最小化 *特権アカウント*	直接のマッピングなし	
3.1.6 非セキュリティ機能をアクセスするときは、非特権アカウントまたは役割を使用する。	AC-6(2)	特権の最小化 *非セキュリティ機能の非特権アクセス*	直接のマッピングなし	
3.1.7 非特権利用者による特権機能の実行とこのような機能の実行の監査を防止する。	AC-6(9)	特権の最小化 *特権機能の利用の監査*	直接のマッピングなし	
	AC-6(10)	特権の最小化 *特権機能の実行を非特権利用者に禁止する*	直接のマッピングなし	
3.1.8 ログイン試行失敗を制限する。	AC-7	ログイン試行の失敗	A.9.4.2	セキュリティに配慮したログオン手順
3.1.9 適用可能な CUI 規則と整合性のあるプライバシーとセキュリティの通知を提供する。	AC-8	システムの利用に関する通知	A.9.4.2	セキュリティに配慮したログオン手順
3.1.10 非アクティブな時間の経過後、データのアクセス及び閲覧を防止するため、パタンによる不可視化表示を用いてセションロックを使用する。	AC-11	セションのロック	A.11.2.8	無人状態にある利用者装置
			A.11.2.9	クリアデスク・クリアスクリーン方針
	AC-11(1)	セションのロック *パタンによる不可視化表示*	直接のマッピングなし	
3.1.11 定義された条件の後、利用者セションを（自動的に）終了する。	AC-12	セションの終了	直接のマッピングなし	

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
3.1.12 リモートアクセスセッションを監視し、制御する。	AC-17(1)	リモートアクセス *自動化された監視／管理*	直接のマッピングなし	
3.1.13 リモートアクセスセッションの機密性を保護するために暗号メカニズムを採用する。	AC-17(2)	リモートアクセス *暗号化を用いた機密性／完全性の保護*	直接のマッピングなし	
3.1.14 管理されたアクセス制御ポイントを介してリモートアクセスをルーティングする。	AC-17(3)	リモートアクセス *管理されたアクセス制御ポイント*	直接のマッピングなし	
3.1.15 特権コマンドのリモート実行とセキュリティ関連情報へのリモートアクセスを許可する。	AC-17(4)	リモートアクセス *特権コマンド／アクセス*	直接のマッピングなし	
3.1.16 無線のコネクションを許可する前に無線アクセスを許可する。	AC-18	無線アクセスの制限	A.6.2.1	モバイル機器の方針
			A.13.1.1	ネットワーク管理策
			A.13.2.1	情報転送の方針と手順
3.1.17 認証と暗号化を用いて無線アクセスを保護する。	AC-18(1)	無線アクセス *認証と暗号化*	直接のマッピングなし	
3.1.18 モバイルデバイスのコネクションを制御する。	AC-19	携帯機器に対するアクセス制御	A.6.2.1	モバイル機器の方針
			A.11.2.6	構外にある装置及び資産のセキュリティ
			A.13.2.1	情報転送の方針と手順
3.1.19 モバイルデバイスおよびモバイルコンピューティングプラットフォーム上の CUI を暗号化する。	AC-19(5)	携帯機器に対するアクセス制御 *デバイス全体／コンテナベースの暗号化*	直接のマッピングなし	
3.1.20 外部システムへのコネクション及び使用を検証し、制御／制限する。	AC-20	外部情報システムの利用	A.11.2.6	構外にある装置及び資産のセキュリティ
			A.13.1.1	ネットワーク管理策
			A.13.2.1	情報転送の方針と手順
	AC-20(1)	外部情報システムの利用 *許可された利用の制限*	直接のマッピングなし	
3.1.21 外部システム上での組織のポータブルストレージデバイスの使用を制限する。	AC-20(2)	外部情報システムの利用 *ポータブルストレージデバイス*	直接のマッピングなし	
3.1.22 公開アクセス可能なシステムにおいて掲載または処理される CUI を制御する。	AC-22	公的アクセス可能なコンテンツ	直接のマッピングなし	

表 D- 2：意識向上と訓練要件のセキュリティ管理策へのマッピング

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
3.2 意識向上と訓練				
基本セキュリティ要件				
3.2.1 組織のシステムの責任者、システム管理者、及び利用者が、彼らのアクティビティに関連するセキュリティリスク及びそれらのシステムのセキュリティに関連する適用可能なポリシー、基準、及び手順について周知されていることを、保証する。 3.2.2 組織の要員が、その割り当てられた情報セキュリティ関連の職務と責任を遂行するために適切に訓練されていることを、保証する。	AT-2	セキュリティの意識向上	A.7.2.2	情報セキュリティの意識向上、教育及び訓練
			A.12.2.1	マルウェアに対する管理策
	AT-3	ロールベースのセキュリティトレーニング	A.7.2.2*	情報セキュリティの意識向上、教育及び訓練
導出されたセキュリティ要件				
3.2.3 内部からの脅威の潜在指標の認識と報告についてのセキュリティ周知訓練を提供する。	AT-2(2)	セキュリティの意識向上 *内部の脅威*	直接のマッピングなし	

表 D- 3：監査と責任追跡性要件のセキュリティ管理策へのマッピング

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
3.3 監査と責任追跡性				
基本セキュリティ要件				
3.3.1 非合法の、許可されない、または不適切な情報システムアクティビティの監視、分析、調査、及び報告を可能とするために必要な範囲で、情報システム監査記録を作成、保護、及び維持する。 3.3.2 個別の情報システム利用者のアクションが、彼らのアクションについての説明責任を維持可能にするよう、それらの利用者に対して一意に追跡が可能であることを保証する。	AU-2	監査対象のイベント	*直接のマッピングなし*	
	AU-3	監査記録の内容	A.12.4.1*	イベントログ取得
	AU-3(1)	監査記録の内容 *追加の監査情報*	*直接のマッピングなし*	
	AU-6	監査記録の監視、分析、及び報告	A.12.4.1	イベントログ取得
			A.16.1.2	情報セキュリティ事象の報告
			A.16.1.4	情報セキュリティ事象の評価と決定
	AU-12	監査の生成	A.12.4.1	イベントログ取得
			A.12.4.3	実務管理者および運用担当者の作業ログ
導出されたセキュリティ要件				
3.3.3 監査された事象をレビューし、アップデートする。	AU-2(3)	監査対象のイベント *レビューとアップデート*	*直接のマッピングなし*	
3.3.4 監査プロセス失敗の事象においてアラート（警告）を発する。	AU-5	監査処理エラーへの対応	*直接のマッピングなし*	
3.3.5 監査記録のレビュー、分析、及び調査のための報告プロセスを集めて相互の関係を比較し、不適切な、疑わしい、または異常なアクティビティの兆候に対応する。	AU-6(3)	監査記録の監視、分析、及び報告 *監査リポジトリとの相互の関連付け*	*直接のマッピングなし*	
3.3.6 オンデマンド分析と報告をサポートするため、監査情報の簡素化と報告書生成を提供する。	AU-7	監査量の低減と報告書の作成	*直接のマッピングなし*	
3.3.7 監査記録のタイムスタンプを生成するための正式な情報源を用いて、内部システムクロックを比較し同期するような情報システム機能を提供する。	AU-8	タイムスタンプ	A.12.4.4	クロックの同期
	AU-8(1)	タイムスタンプ *権威ある時刻ソースとの同期*	*直接のマッピングなし*	
3.3.8 監査情報と監査ツールを不正なアクセス、改変、及び削除から保護する。	AU-9	監査情報の保護	A.12.4.2	ログ情報の保護
			A.12.4.3	実務管理者および運用担当者の作業ログ
			A.18.1.3	記録の保護

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策
3.3.9 監査機能の管理を特権利用者の一部に制限する。	AU-9(4)	監査情報の保護 *特権利用者のサブセットによるアクセス*	*直接のマッピングなし*

表 D- 4：構成管理要件のセキュリティ管理策へのマッピング[29]

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
3.4 構成管理				
基本セキュリティ要件				
3.4.1 個別のシステム開発ライフサイクル全体で、組織のシステム（ハードウェア、ソフトウェア、ファームウェア、及び文書を含めて） のベースライン構成とインベントリを確立し、維持する。 3.4.2 組織のシステムで採用された情報技術製品のセキュリティ構成設定を確立し、強制 （実施）する。	CM-2	ベースライン構成	直接のマッピングなし	
	CM-6	構成設定	直接のマッピングなし	
	CM-8	情報システムコンポーネントのインベントリ	A.8.1.1	資産目録
			A.8.1.2	資産の管理責任
	CM-8(1)	情報システムコンポーネントのインベントリ *インストレーション／除去中のアップデート*	直接のマッピングなし	
導出されたセキュリティ要件				
3.4.3 組織のシステムへの変更を追跡、レビュー、承認／非承認、及び監査する。	CM-3	構成変更管理	A.12.1.2	変更管理
			A.14.2.2	システムの変更管理手順
			A.14.2.3	オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー
			A.14.2.4	パッケージソフトウェアの変更に対する制限
3.4.4 実装に先立ち、変更のセキュリティへの影響を分析する。	CM-4	構成変更の監視	A.14.2.3	オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー
3.4.5 組織のシステムへの変更に関連する物理的及び論理的なアクセス制約事項を定義し、文書化し、承認し、強制（実施）する。	CM-5	変更のためのアクセス制限	A.9.2.3	特権的アクセス権の管理
			A.9.4.5	プログラムソースコードへのアクセス制御
			A.12.1.2	変更管理
			A.12.1.4	開発環境、試験環境及び運用環境の分離
			A.12.5.1	運用システムに関わるソフトウェアの導入
3.4.6 基本機能のみを提供するように組織のシステムを構成することによって、最小機能の原則を採用する。	CM-7	機能の最小化	A.12.5.1*	運用システムに関わるソフトウェアの導入
3.4.7 非基本プログラム、機能、ポート、プロトコル、及びサービス	CM-7(1)	機能の最小化 *定期的なレビュー*	直接のマッピングなし	

[29] CM-7(5)、機能の最小化ホワイトリストポリシーは、CUI を含む情報システムに対してより大きな保護を望む組織に対して、CM-7(4)、機能の最小化ブラックリストポリシーの代替策として列挙されている。CM-7(5)は、NIST SP 800-53 に従って高度なセキュリティ管理策ベースラインの連邦政府情報システムにおいてのみ要求される。

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
の使用を制限、無効化、及び防止する。	CM-7(2)	機能の最小化 *プログラム実行の防止*	直接のマッピングなし	
3.4.8 許可されないソフトウェアの使用を防止するために例外による拒否 （ブラックリスト） ポリシーを、または許可されたソフトウェアの実行を許可するような例外による許可 （ホワイトリスト） ポリシーを適用する。	CM-7(4)	機能の最小化 *許可されないソフトウェア／ブラックリスト*	直接のマッピングなし	
	CM-7(5)	機能の最小化 *許可されたソフトウェア／ホワイトリスト*	直接のマッピングなし	
3.4.9 利用者がインストールしたソフトウェアを管理し、監視する。	CM-11	利用者がインストールしたソフトウェア	A.12.5.1	運用システムに関わるソフトウェアの導入
			A.12.6.2	ソフトウェアのインストレーションの制限

表 D- 5：識別と認証要件のセキュリティ管理策へのマッピング[30]

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
3.5 識別と認証				
基本セキュリティ要件				
3.5.1 システム利用者、利用者を代行して動作するプロセス、またはデバイスを識別する。 3.5.2 組織のシステムへのアクセスの許可に対する必要条件として、それらの利用者、プロセス、またはデバイスのアイデンティティを認証(または検証)する。	IA-2	ユーザ識別及び認証	A.9.2.1	利用者登録と登録抹消
	IA-5	認証コードの管理	A.9.2.1	利用者登録と登録抹消
			A.9.2.4	利用者の秘密認証情報の管理
			A.9.3.1	秘密認証情報の利用
			A.9.4.3	パスワード管理システム
導出されたセキュリティ要件				
3.5.3 複数要素の認証 を、特権アカウントへのローカル及びネットワークアクセス のために、及び非特権アカウントへのネットワークアクセスのために、使用する。	IA-2(1)	ユーザ識別及び認証 *特権アカウントへのネットワークアクセス*	*直接のマッピングなし*	
	IA-2(2)	ユーザ識別及び認証 *非特権アカウントへのネットワークアクセス*	*直接のマッピングなし*	
	IA-2(3)	ユーザ識別及び認証 *特権アカウントへのローカルアクセス*	*直接のマッピングなし*	
3.5.4 特権及び非特権アカウントへのネットワークアクセスのために、リプレイ耐性のある認証メカニズムを採用する。	IA-2(8)	ユーザ識別及び認証 *特権アカウントへのネットワークアクセスーリプレイ耐性*	*直接のマッピングなし*	
	IA-2(9)	ユーザ識別及び認証 *非特権アカウントへのネットワークアクセスーリプレイ耐性*	*直接のマッピングなし*	
3.5.5 定義された期間について、識別コードの再利用を禁止する。	IA-4	識別子の管理	A.9.2.1	利用者登録と登録抹消

[30] IA-2(9)は、SP 800-53 中位セキュリティ管理策に現在含まれていないが、次回の更新でベースラインに追加されるだろう。非特権アカウントのためのリプレイ耐性機能なしの複数要素認証の採用は、CUI を伝送している情報システムにとって、重大な脆弱性を作り込む。

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
3.5.6 定義された非アクティブな期間の後、識別コードを無効化する。	IA-4	識別子の管理	A.9.2.1	利用者登録と登録抹消
3.5.7 新しいパスワードが作成されるとき、最小パスワード複雑性及び文字列の変更を強制（実施）する。	IA-5(1)	認証コードの管理 *パスワードベース認証*	*直接のマッピングなし*	
3.5.8 規定された生成回数の間、パスワードの再利用を禁止する。				
3.5.9 永久パスワードへ直ちに変更するようなときのシステムログインのために一時的パスワードの使用を許可する。				
3.5.10 暗号学的に保護されたパスワードのみを格納及び送信する。				
3.5.11 認証情報のフィードバックを不可視化する。	IA-6	認証コードのフィードバック	A.9.4.2	セキュリティに配慮したログオン手順

表 D- 6：インシデント対応要件のセキュリティ管理策へのマッピング

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
3.6 インシデント対応				
基本セキュリティ要件				
3.6.1 適切な準備、検知、分析、抑制（封じ込め）、リカバリ、及び利用者対応アクティビティを含めて、組織のシステムのための運用上のインシデントハンドリング能力を確立する。 3.6.2 組織の内部及び外部の両方の、適切な担当官及び／または権威に対して、インシデントについての追跡、文書化、及び報告を行う。	IR-2	インシデント対応のトレーニング	A.7.2.2*	情報セキュリティの意識向上、教育及び訓練
	IR-4	インシデントの対応	A.16.1.4	情報セキュリティ事象の評価及び決定
			A.16.1.5	情報セキュリティインシデントへの対応
			A.16.1.6	情報セキュリティインシデントからの学習
	IR-5	インシデントの監視	直接のマッピングなし	
	IR-6	インシデントの報告	A.6.1.3	関係当局との連絡
			A.16.1.2	情報セキュリティ事象の報告
	IR-7	インシデント対応の支援	直接のマッピングなし	
導出されたセキュリティ要件				
3.6.3 組織のインシデント対応能力をテストする。	IR-3	インシデント対応のテストと実習	直接のマッピングなし	
	IR-3(2)	インシデント対応のテストと実習 *関連する計画との調整*	直接のマッピングなし	

表 D- 7：メンテナンス要件のセキュリティ管理策へのマッピング

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
3.7 メンテナンス				
基本セキュリティ要件				
3.7.1 組織のシステムにおいてメンテナンスを実施する。 3.7.2 システムメンテナンスを実施するために使用されるツール、手法、メカニズム、及び要員における有効な管理策を提供する。	MA-2	定期的な保守	A.11.2.4* A.11.2.5*	装置の保守 資産の移動
	MA-3	保守ツール	直接のマッピングなし	
	MA-3(1)	保守ツール *ツールを検査する*	直接のマッピングなし	
	MA-3(2)	保守ツール *メディアを検査する*	直接のマッピングなし	
導出されたセキュリティ要件				
3.7.3 オフサイトメンテナンスのために除去された装置は、あらゆる CUI についてサニタイズされることを保証する。	MA-2	定期的な保守	A.11.2.4* A.11.2.5*	装置の保守 資産の移動
3.7.4 組織のシステム内でメディアが使用される前に、悪意のあるコードが入っていないか診断及びテストプログラムを用いてメディアをチェックする。	MA-3(2)	保守ツール	直接のマッピングなし	
3.7.5 外部のネットワークコネクションを介した非ローカルメンテナンスセションを確立するため、複数要素の認証を要求し、非ローカルメンテナンスの完了時にこのようなセションを終了する。	MA-4	遠隔保守	直接のマッピングなし	
3.7.6 必要なアクセス許可なしにメンテナンス要員のメンテナンス活動を監督する。	MA-5	保守要員	直接のマッピングなし	

表 D- 8：メディアの保護要件のセキュリティ管理策へのマッピング[31]

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
3.8 メディア保護				
基本セキュリティ要件				
3.8.1 紙及びディジタルの両方の、CUI を含む、システムメディアを保護する(即ち、物理的に制御及びセキュアに格納する)。 3.8.2 システムメディア上の CUI へのアクセスを許可された利用者に制限する。 3.8.3 廃棄または再利用のために手放す前に、CUI を含むシステムメディアをサニタイズまたは破壊する。	MP-2	メディアへのアクセス	A.8.2.3	資産の取扱い
			A.8.3.1	取外し可能なメディアの管理
			A.11.2.9	クリアデスクとクリアスクリーンの方針
	MP-4	メディアの保管	A.8.2.3	資産の取扱い
			A.8.3.1	取外し可能なメディアの管理
			A.11.2.9	クリアデスク・クリアスクリーン方針
	MP-6	メディア上の記録の抹消とメディアの廃棄	A.8.2.3	資産の取扱い
			A.8.3.1	取外し可能なメディアの管理
			A.8.3.2	メディアの処分
			A.11.2.7	装置のセキュリティを保った処分又は再利用
導出されたセキュリティ要件				
3.8.4 CUI のマーク表示と配付制限が必要なメディアに対して表示を行う。	MP-3	メディアへのラベル付け	A.8.2.2	情報のラベル付け
3.8.5 CUI を含むメディアへのアクセスを制御し、管理エリアの外部への持ち出し中のメディアの説明責任を維持する。	MP-5	メディアの輸送	A.8.2.3	資産の取扱い
			A.8.3.1	取外し可能なメディアの管理
			A.8.3.3	物理的メディアの輸送
			A.11.2.5	資産の移動
			A.11.2.6	構外にある装置及び資産のセキュリティ
3.8.6 代替の物理的予防手段による保護がない限り、持ち出し中はディジタルメディア上に格納された CUI の機密性を保護するための暗号学的メカニズムを実装する。	MP-5(4)	メディアの輸送 *暗号学的保護*	直接のマッピングなし	
3.8.7 システムコンポーネント上の取り外し可能なメディアの使	MP-7	メディアの利用	A.8.2.3	資産の取扱い

[31] CP-9、*情報システムのバックアップ*、は緊急時対応計画ファミリが CUI セキュリティ要件に含まれなかったので、メディアの保護ファミリに含まれる。

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
用を管理する。			A.8.3.1	取外し可能なメディアの管理
3.8.8 ポータブルストレージデバイスに識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。	MP-7(1)	メディアの利用 *所有者以外の利用を禁止*	直接のマッピングなし	
3.8.9 保存場所にあるバックアップ CUI の機密性を保護する。	CP-9	情報システムのバックアップ	A.12.3.1	情報のバックアップ
			A.17.1.2	情報セキュリティ継続の実装
			A.18.1.3	記録の保護

表 D- 9：人的セキュリティ要件のセキュリティ管理策へのマッピング

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
3.9 人的セキュリティ				
基本的セキュリティ要件				
3.9.1 CUI を含む組織のシステムへのアクセスを許可する前に、個人を審査する。 3.9.2 離職または配置転換等の人事措置の間と後で、CUI 及び CUI を含む組織のシステムが保護されることを保証する。	PS-3	要員に対する審査	A.7.1.1	選考
	PS-4	要員の解雇	A.7.3.1	雇用の終了又は変更に関する責任
			A.8.1.4	資産の返却
	PS-5	人事異動	A.7.3.1	雇用の終了又は変更に関する責任
			A.8.1.4	資産の返却
導出されたセキュリティ要件	なし			

表 D- 10：物理的保護要件のセキュリティ管理策へのマッピング

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
3.10 物理的保護				
基本的セキュリティ要件				
3.10.1 組織のシステム、装置、及びそれぞれの運用環境への物理的アクセスを許可された個人に制限する。 3.10.2 物理的設備を保護し、監視し、組織のシステムの基盤をサポートする。	PE-2	物理的アクセス権限	A.11.1.2*	物理的入場管理策
	PE-5	表示メディアへのアクセス制御	A.11.1.2	物理的入場管理策
			A.11.1.3	オフィス、部屋及び施設のセキュリティ
	PE-6	物理的アクセスの監視	直接のマッピングなし	
導出されたセキュリティ要件				
3.10.3 訪問者をエスコートし、訪問者の活動を監視する。	PE-3	物理的アクセス制御	A.11.1.1	物理的セキュリティ境界
3.10.4 物理的アクセスの監査ログを維持する。			A.11.1.2	物理的入場管理策
3.10.5 物理的アクセスデバイスを制御し、管理する。			A.11.1.3	オフィス、部屋及び施設のセキュリティ
3.10.6 代替の作業サイト(例、テレワークのサイト)での CUI に対する防護対策を強制(実施)する。	PE-17	代替作業拠点	A.6.2.2	テレワーク
			A.11.2.6	構外にある装置及び資産のセキュリティ
			A.13.2.1	情報輸送の方針及び手順

表 D- 11：リスクアセスメント要件のセキュリティ管理策へのマッピング

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
3.11 リスクアセスメント				
基本的セキュリティ要件				
3.11.1 組織のシステムの運用と関連する CUI の処理、ストレージ、または送信からの結果として、組織の運用(ミッション、職務、イメージ、または風評を含めて)、組織の資産、及び個人に対するリスクを定期的にアセスメントする。	RA-3	リスクアセスメント	A.12.6.1*	技術的ぜい弱性の管理
導出されたセキュリティ要件				
3.11.2 定期的に、及び組織のシステムとアプリケーションに影響する新しい脆弱性が識別されるときに、それらのシステム及びアプリケーションの脆弱性についてスキャンする。	RA-5	脆弱性のスキャン	A.12.6.1*	技術的ぜい弱性の管理
	RA-5(5)	脆弱性のスキャン *特権アクセス*	直接のマッピングなし	
3.11.3 リスクアセスメントに従い、脆弱性を修正する。	RA-5	脆弱性のスキャン	A.12.6.1*	技術的ぜい弱性の管理

表 D- 12：セキュリティアセスメント要件のセキュリティ管理策へのマッピング

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
3.12 セキュリティアセスメント				
基本的セキュリティ要件				
3.12.1 管理策がそれらのアプリケーションにおいて有効であるかどうかを決定するために、組織のシステムにおけるセキュリティ管理策を定期的にアセスメントする。 3.12.2 欠陥を修正し、組織のシステムにおける脆弱性を軽減し、または取り除くために設計された行動計画を策定し、実施する。 3.12.3 管理策の継続的な有効性を保証するため、継続的にセキュリティ管理策を監視する。 3.12.4 システムの境界、システムの運用環境、セキュリティ要件の実装方法、及び他のシステムの関係または他のシステムとのコネクションについて記述するような、システムセキュリティ計画を策定、文書及び定期的に更新する。	CA-2	セキュリティア評価	A.14.2.8	システムセキュリティの試験
			A.18.2.2	情報セキュリティのための方針群及び標準の順守
			A.18.2.3	技術的順守のレビュー
	CA-5	行動計画とマイルストン	直接のマッピングなし	
	CA-7	継続的な監視	直接のマッピングなし	
	PL-2	システムセキュリティ計画	A.6.1.2	情報セキュリティリスクアセスメント
導出されたセキュリティ要件	なし			

表 D- 13：システム及び通信の保護要件のセキュリティ管理策とのマッピング[32]

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
3.13 システムと通信の保護				
基本的セキュリティ要件				
3.13.1 外部の境界及びシステムの鍵となる内部境界における通信（即ち、組織のシステムによって送信または受信される情報）を監視し、制御し、保護する。 3.13.2 組織のシステム内の有効な情報セキュリティを促進するような、アーキテクチャ設計、ソフトウェア開発手法、及びシステムエンジニアリングの原則を採用する。	SC-7	境界保護	A.13.1.1	ネットワーク管理策
			A.13.1.3	ネットワークの分離
			A.13.2.1	情報転送の方針及び手順
			A.14.1.3	アプリケーションサービスのトランザクションの保護
	SA-8	セキュリティエンジニアリングの原則	A.14.2.5	セキュリティに配慮したシステム構築の原則
導出されたセキュリティ要件				
3.13.3 利用者機能をシステム管理機能と分離する。	SC-2	アプリケーションの分離	直接のマッピングなし	
3.13.4 共有システム資源を介した、不正な予期せぬ情報の転送を防止する。	SC-4	残存情報	直接のマッピングなし	
3.13.5 内部ネットワークから物理的にまたは論理的に分離される、公開アクセス可能なシステムコンポーネント用には、サブネットワークを実装する。	SC-7	境界保護	A.13.1.1	ネットワーク管理策
			A.13.1.3	ネットワークの分離
			A.13.2.1	情報転送の方針及び手順
			A.14.1.3	アプリケーションサービスのトランザクションの保護
3.13.6 デフォルトでネットワーク通信トラフィクを拒否し、また例外によってネットワーク通信トラフィクを許可する（即ち、すべて拒否、例外で許可）。	SC-7(5)	境界保護 *デフォルトで拒否／例外で許可*	直接のマッピングなし	
3.13.7 リモートデバイスが、組織のシステムとの非リモートコネクションの確立と同時に、外部ネットワークの資源への何らかの他のコネクションを介して通信することを防止する。	SC-7(7)	境界保護 *リモートデバイスのスプリットトンネルを禁止*	直接のマッピングなし	

[32] SA-8、*セキュリティエンジニアリングの原則*、はシステム及びサービスの調達ファミリはセキュリティ要件に含まれていなかったので、システム及び通信の保護ファミリに含まれる。

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
3.13.8 代替の物理的予防手段による保護がない限り、持ち出し中に CUI の不正な暴露を防止するために暗号学的メカニズムを実装する。	SC-8	伝送する情報の完全性	A.8.2.3	資産の取扱い
			A.13.1.1	ネットワーク管理策
			A.13.2.1	情報転送の方針及び手順
			A.13.2.3	電子的メッセージ通信
			A.14.1.2	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮
			A.14.1.3	アプリケーションサービスのトランザクションの保護
	SC-8(1)	伝送する情報の完全性 *暗号学的保護または代替の物理的保護*	直接のマッピングなし	
3.13.9 セション終了時または定義された非アクティブな時間の経過後に、通信セションに対応するネットワークコネクションを終了する。	SC-10	ネットワークの切断	A.13.1.1	ネットワーク管理策
3.13.10 組織のシステムで採用された暗号のための暗号鍵を確立し、管理する。	SC-12	暗号鍵の確立と管理	A.10.1.2	鍵管理
3.13.11 CUI の機密性を保護するために使用されるとき、FIPS 認証された暗号を採用する。	SC-13	暗号化の利用	A.10.1.1	暗号による管理策の利用方針
			A.14.1.2	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮
			A.14.1.3	アプリケーションサービスのトランザクションの保護
			A.18.1.5	暗号化機能に対する規制
3.13.12 共同コンピューティングデバイスのリモートからの活性化を禁止し、使用中のデバイスの兆候をデバイスに存在する利用者に提供する。	SC-15	共同コンピューティングデバイス	A.13.2.1*	情報転送の方針及び手順
3.13.13 モバイルコードの使用を管理し、監視する。	SC-18	モバイルコード	直接のマッピングなし	
3.13.14 VoIP 技術の使用を管理し監視する。	SC-19	ボイスオーバーインターネットプロトコル (VoIP)	直接のマッピングなし	

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
3.13.15 通信セションの真正性を保護する。	SC-23	セションの真正性	直接のマッピングなし	
3.13.16 保存された CUI の機密性を保護する。	SC-28	保存情報の保護	A.8.2.3*	資産の取扱い

表 D- 14：システム及び情報の完全性要件のセキュリティ管理策へのマッピング

CUI セキュリティ要件	NIST SP 800-53 関連セキュリティ管理策		ISO/IEC 27001 関連セキュリティ管理策	
3.14 システムと情報の完全性				
基本セキュリティ要件				
3.14.1 タイムリーなやり方で情報及びシステムフローを識別し、報告し、訂正する。 3.14.2 組織のシステム内の適切な場所で、悪意のあるコードから保護を提供する。 3.14.3 システムセキュリティ警報及びアドバイザリを監視し、適切な対応アクションを取る。	SI-2	欠陥の修正	A.12.6.1	技術的ぜい弱性の管理
			A.14.2.2	システムの変更管理手順
			A.14.2.3	オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー
			A.16.1.3	情報セキュリティ弱点の報告
	SI-3	悪意のコード(不正プログラム) からの保護	A.12.2.1	マルウェアに対する管理策
	SI-5	セキュリティ警報と勧告	A.6.1.4*	専門組織との連絡
導出されたセキュリティ要件				
3.14.4 新しいリリースが利用可能となったとき、悪意のあるコードからの保護メカニズムをアップデートする。	SI-3	悪意のコード(不正プログラム) からの保護	A.12.2.1	マルウェアに対する管理策
3.14.5 組織のシステムの定期的スキャン、及びファイルがダウンロードされ、開かれ、または実行されるような、外部情報源からのファイルのリアルタイムスキャンを実行する。				
3.14.6 内向き及び外向きの通信トラフィクを含めて、攻撃や潜在的な攻撃の兆候を検知するため、組織のシステムを監視する。	SI-4	情報システムの監視ツールと監視技法	直接のマッピングなし	
	SI-4(4)	情報システムの監視ツールと監視技法 *内向きと外向きの通信トラフィク*	直接のマッピングなし	
3.14.7 組織のシステムの不正な使用を識別する。	SI-4	情報システムの監視ツールと監視技法	直接のマッピングなし	

附属書 E

基準の調整

CUI 中位のセキュリティ管理策ベースラインのリスト作成とアクションの調整

本附属書は、第 3 章に記述された最終版 CUI セキュリティ要件についての FIPS Publication 200 に沿った情報源のひとつとして、NIST SP 800-53 中位ベースラインのセキュリティ管理策の完全なリストを提供する。表 E-1 から E-17 は、NIST 及び NARA によって制定された基準の調整に従って、中位ベースラインのセキュリティ管理策について実行されることになるアクションの調整を含む。[33] アクションの調整は、FIPS Publication 200 のセキュリティ要件から得られる基本セキュリティ要件を補足するような CUI 導出セキュリティ要件の作成を促進した。[34]

以下を含めて、中位ベースラインからのセキュリティ管理策または拡張管理策を軽減するような、３つの主たる基準がある—

- 管理策または拡張管理策が、連邦政府専用である（即ち、主として連邦政府の責任）;
- 管理策または拡張管理策が、CUI の機密性保護に直接関連しない[35]、または
- 管理策または拡張管理策が規定なしに連邦政府外の組織によって日常的に満たされると想定される。[36]

以下のシンボルは、表 E-1 から E-17 で、特定のアクションの調整がなされるよう規定するため、または要求されたアクションの調整がないとき、使用される。

調整のシンボル	基準の調整
NCO	CUI の機密性保護に直接関連しない
FED	連邦政府専用、主として連邦政府の責任である
NFO	規定なしに連邦政府外の組織によって日常的に満たされると想定される
CUI	CUI 基本または導出されたセキュリティ要件が反映され、かつセキュリティ管理策、拡張管理策または管理策／拡張管理策の具体的なエレメントに対してトレース可能である

[33] 組織は、NIST SP 800-53、附属書 I で定義されるとおり CUI 機密性*オーバーレイ*を構築するため、附属書 E の情報を利用できる。
[34] 同様の*調整基準* が、第 2 章と附属書 D に記述される CUI 基本セキュリティ要件をもたらしている FIPS Publication 200 のセキュリティ要件に適用された。
[35] 本書の主たる目的は CUI の機密性保護するための要件を定めることであるが、機密性と完全性のセキュリティ対策の間には緊密な関係がある。ゆえに、許可されない暴露に対する保護をサポートするような NIST SP 800-53 の中位ベースラインのほとんどのセキュリティ管理策は、許可されない改変に対する保護についてもサポートする。
[36] CUI の保護に関する SP 800-53 の中位ベースラインから調整されたセキュリティ管理策(即ち、表 E-1 から E-17 での NCO,または NFO のいずれかのマークを特に付けられた管理策) は、組織の包括的なセキュリティプログラムの一部としてしばしば含まれる。

表 E-1：アクセス制御のアクション調整

NIST SP 800-53 中位ベースラインセキュリティ管理策		アクションの調整
AC-1	アクセス制御方針と手順	NFO
AC-2	アカウント管理	CUI
AC-2(1)	*アカウント管理 ／ 自動化システムアカウント管理*	NCO
AC-2(2)	*アカウント管理 ／ 一時的／緊急時アカウントの抹消*	NCO
AC-2(3)	*アカウント管理 ／ 非アクティブなアカウントの無効化*	NCO
AC-2(4)	*アカウント管理 ／ 自動化監査アクション*	NCO
AC-3	アクセス制御の実施	CUI
AC-4	情報フロー制御の実施	CUI
AC-5	職務の分離	CUI
AC-6	特権の最小化	CUI
AC-6(1)	*特権の最小化 ／ セキュリティ機能へのアクセスを許可する*	CUI
AC-6(2)	*特権の最小化 ／ 非セキュリティ機能の非特権アクセス*	CUI
AC-6(5)	*特権の最小化 ／ 特権アカウント*	CUI
AC-6(9)	*特権の最小化 ／ 特権機能の利用の監査*	CUI
AC-6(10)	*特権の最小化 ／ 特権機能の実行を非特権利用者に禁止する*	CUI
AC-7	ログイン試行の失敗	CUI
AC-8	システムの利用に関する通知	CUI
AC-11	セションのロック	CUI
AC-11(1)	*セションのロック ／ パタンによる不可視化表示*	CUI
AC-12	セションの終了	CUI
AC-14	識別または認証なしでの許可されたアクション	FED
AC-17	リモートアクセス	CUI
AC-17(1)	*リモートアクセス ／ 自動化された監視／管理*	CUI
AC-17(2)	*リモートアクセス ／ 暗号化を用いた機密性／完全性の保護*	CUI
AC-17(3)	*リモートアクセス ／ 管理されたアクセス制御ポイント*	CUI
AC-17(4)	*リモートアクセス ／ 特権コマンド／アクセス*	CUI
AC-18	無線アクセス	CUI
AC-18(1)	*無線アクセス ／ 認証と暗号化*	CUI
AC-19	モバイルデバイスのアクセス制御	CUI
AC-19(5)	*モバイルデバイスのアクセス制御 ／ デバイス全体／コンテナベースの暗号化*	CUI
AC-20	外部情報システムの利用	CUI
AC-20(1)	*外部情報システムの利用 ／ 許可された利用の制限*	CUI
AC-20(2)	*外部情報システムの利用 ／ ポータブルストレージデバイス*	CUI
AC-21	情報共有	FED
AC-22	公共アクセス可能なコンテンツ	CUI

表 E-2：意識向上と訓練の管理策のアクション調整

NIST SP 800-53 中位ベースラインセキュリティ管理策		アクションの調整
AT-1	セキュリティの意識向上と訓練の方針と手順	NFO
AT-2	セキュリティの意識向上と訓練	CUI
AT-2(2)	*セキュリティの意識向上 ／ 内部犯行の脅威*	CUI
AT-3	役割ベースのセキュリティ訓練	CUI
AT-4	セキュリティ訓練記録	NFO

表 E-3：監査と責任追跡性の管理策のアクション調整

NIST SP 800-53 中位ベースラインセキュリティ管理策		アクションの調整
AU-1	監査と責任追跡性方針と手順	NFO
AU-2	監査対象の事象	CUI
AU-2(3)	*監査対象の事象 ／ レビューとアップデート*	CUI
AU-3	監査記録の内容	CUI
AU-3(1)	*監査記録の内容 ／ 追加の監査情報*	CUI
AU-4	監査記録の保存容量	NCO
AU-5	監査処理の不具合に対する対応	CUI
AU-6	監査記録のレビュー、分析、及び報告	CUI
AU-6(1)	*監査記録のレビュー、分析、及び報告 ／ プロセス統合*	NCO
AU-6(3)	*監査記録のレビュー、分析、及び報告 ／ 監査リポジトリとの相互の関連付け*	CUI
AU-7	監査量の低減と報告書の作成	CUI
AU-7(1)	*監査量の低減と報告書の作成 ／ 自動生成処理*	NCO
AU-8	タイムスタンプ	CUI
AU-8(1)	*タイムスタンプ ／ 権威ある時刻ソースとの同期*	CUI
AU-9	監査情報の保護	CUI
AU-9(4)	*監査情報の保護 ／ 特権利用者の一部によるアクセス*	CUI
AU-11	監査記録の保持	NCO
AU-12	監査情報の生成	CUI

表 E-4：セキュリティアセスメントと権限付与の管理策のアクション調整

NIST SP 800-53 中位ベースラインセキュリティ管理策		アクションの調整
CA-1	セキュリティアセスメントと権限付与の方針と手順	NFO
CA-2	セキュリティアセスメント	CUI
CA-2(1)	*セキュリティアセスメント ／ 独立したアセッサ*	NFO
CA-3	情報システムの接続	NFO
CA-3(5)	*情報システムの接続 ／ 外部システム接続の制限*	NFO
CA-5	行動計画とマイルストン	CUI
CA-6	セキュリティに関する運用許可	FED
CA-7	継続的な監視	CUI
CA-7(1)	*継続的な監視 ／ 独立したアセッサ*	NFO
CA-9	内部の情報システムの接続	NFO

表 E-5：構成管理の管理策のアクション調整[37]

NIST SP 800-53 中位ベースラインセキュリティ管理策		アクションの調整
CM-1	構成管理の方針と手順	NFO
CM-2	ベースライン構成	CUI
CM-2(1)	*ベースライン構成 ／ レビューとアップデート*	NFO
CM-2(3)	*ベースライン構成 ／ 以前の構成の維持*	NCO
CM-2(7)	*ベースライン構成 ／ 高リスク区域のシステム、コンポーネント、またはデバイスの構成*	NFO
CM-3	構成変更管理	CUI
CM-3(2)	*構成変更管理 ／ テスト／検証／文書の変更*	NFO
CM-4	セキュリティ上の影響分析	NFO
CM-5	構成変更のためのアクセス制限	CUI
CM-6	構成設定	CUI
CM-7	機能の最小化	CUI
CM-7(1)	*機能の最小化 ／ 定期的なレビュー*	CUI
CM-7(2)	*機能の最小化 ／ プログラム実行の防止*	CUI
CM-7(4)(5)	*機能の最小化 ／ 許可されない、または許可される祖父音ウェア ／ ブラックリスト または ホワイトリスト*	CUI
CM-8	情報システムコンポーネントのインベントリ	CUI
CM-8(1)	*情報システムコンポーネントのインベントリ ／ インストール／除去中のアップデート*	CUI
CM-8(3)	*情報システムコンポーネントのインベントリ ／ 自動化された許可されないコンポーネント検知*	NCO
CM-8(5)	*情報システムコンポーネントのインベントリ ／ コンポーネントの重複しないアカウント管理*	NFO
CM-9	構成管理計画	NFO
CM-10	ソフトウェア利用上の制限	NCO
CM-11	利用者によりインストールされたソフトウェア	CUI

[37] CM-7(5)、機能の最小化*ホワイトリスト*、は NIST SP 800-53 にしたがって、中位セキュリティ管理策にはない。しかし、*ブラックリスト*へのオプションの、より強い代替方針として提供される。

表 E-6：緊急時対応計画の管理策のアクション調整[38]

NIST SP 800-53 中位ベースラインセキュリティ管理策		アクションの調整
CP-1	緊急時対応計画の方針と手順	NCO
CP-2	緊急時対応計画	NCO
CP-2(1)	*緊急時対応計画 ／ 関連する計画との調整*	NCO
CP-2(3)	*緊急時対応計画 ／ 基本的ミッション ／ ビジネス機能の復旧*	NCO
CP-2(8)	*緊急時対応計画 ／ 重要な資産の特定*	NCO
CP-3	緊急時対応訓練	NCO
CP-4	緊急時対応計画のテスト	NCO
CP-4(1)	*緊急時対応計画のテスト ／ 関連する計画と調整*	NCO
CP-6	代替保管拠点	NCO
CP-6(1)	*代替保管拠点 ／ 主たる拠点との分離*	NCO
CP-6(3)	*代替保管拠点 ／ アクセス性*	NCO
CP-7	代替処理拠点	NCO
CP-7(1)	*代替処理拠点 ／ 主たる拠点との分離*	NCO
CP-7(2)	*代替処理拠点 ／ アクセス性*	NCO
CP-7(3)	*代替処理拠点 ／ サービスの優先度*	NCO
CP-8	通信サービス	NCO
CP-8(1)	*通信サービス ／ サービスプロビジョンの優先度*	NCO
CP-8(2)	*通信サービス ／ 単一障害点*	NCO
CP-9	情報システムのバックアップ	CUI
CP-9(1)	*情報システムのバックアップ ／ 信頼性／完全性のテスト*	NCO
CP-10	情報システムの復旧と再構築	NCO
CP-10(2)	*情報システムの復旧と再構築 ／ トランザクションの復旧*	NCO

[38] CP-9 は、緊急時対応計画ファミリが CUI セキュリティ要件に含まれなかったので、附属書 D のメディア保護ファミリのセキュリティ管理策とともにグループ化されている。

表 E-7：識別と認証の管理策のアクション調整

NIST SP 800-53 中位ベースラインセキュリティ管理策		アクションの調整
IA-1	識別と認証の方針と手順	NFO
IA-2	識別と認証 （組織の利用者）	CUI
IA-2(1)	*識別と認証 （組織の利用者）／ 特権アカウントへのネットワークアクセス*	CUI
IA-2(2)	*識別と認証（組織の利用者）／ 非特権アカウントへのネットワークアクセス*	CUI
IA-2(3)	*識別と認証（組織の利用者）／ 特権アカウントへのローカルアクセス*	CUI
IA-2(8)	*識別と認証（組織の利用者）／ 特権アカウントへのネットワークアクセス － リプレイ耐性あり*	CUI
IA-2(9)	*識別と認証（組織の利用者）／ 非特権アカウントへのネットワークアクセス － リプレイ耐性あり*	CUI
IA-2(11)	*識別と認証（組織の利用者）／ リモートアクセス － デバイスを分離*	FED
IA-2(12)	*識別と認証（組織の利用者）／ PIV クレデンシャルの受入れ*	FED
IA-3	デバイスの識別と管理	NCO
IA-4	識別子の管理	CUI
IA-5	認証コードの管理	CUI
IA-5(1)	*認証コードの管理 ／ パスワードベース認証*	CUI
IA-5(2)	*認証コードの管理 ／ PKI ベース認証*	FED
IA-5(3)	*認証コードの管理 ／ 本人または信頼される第三者の登録*	FED
IA-5(11)	*認証コードの管理 ／ ハードウェアトークンベース認証*	FED
IA-6	認証コードのフィードバック	CUI
IA-7	暗号モジュール認証	FED
IA-8	識別と認証（組織外の利用者）	FED
IA-8(1)	*識別と認証（組織外の利用者）／ 他の政府機関からの PIV クレデンシャルの受入れ*	FED
IA-8(2)	*識別と認証（組織外の利用者）／ 第三者のクレデンシャルの受入れ*	FED
IA-8(3)	*識別と認証（組織外の利用者）／ FICAM 承認された製品の利用*	FED
IA-8(4)	*識別と認証（組織外の利用者）／FICAM 発行されたプロファイルの利用*	FED

表 E-8：インシデント対応の管理策のアクション調整

NIST SP 800-53 中位ベースラインセキュリティ管理策		アクションの調整
IR-1	インシデント対応の方針と手順	NFO
IR-2	インシデント対応の訓練	CUI
IR-3	インシデント対応のテスト	CUI
IR-3(2)	*インシデント対応のテスト ／ 関連する計画との調整*	CUI
IR-4	インシデントの対応	CUI
IR-4(1)	*インシデントの対応 ／ 自動化されたインシデント対応処理*	NCO
IR-5	インシデントの監視	CUI
IR-6	インシデントの報告	CUI
IR-6(1)	*インシデントの報告 ／自動化された報告書作成*	NCO
IR-7	インシデント対応の支援	CUI
IR-7(1)	*インシデント対応の支援 ／ 情報／サポートの利用可能性についての自動化支援*	NCO
IR-8	インシデント対応計画	NFO

表 E-9：メンテナンスの管理策のアクション調整

NIST SP 800-53 中位ベースラインセキュリティ管理策		アクションの調整
MA-1	システムメンテナンスの方針と手順	NFO
MA-2	管理されたメンテナンス	CUI
MA-3	メンテナンスツール	CUI
MA-3(1)	*メンテナンスツール ／ ツールの検査*	CUI
MA-3(2)	*メンテナンスツール ／ メディアの検査*	CUI
MA-4	遠隔メンテナンス	CUI
MA-4(2)	*遠隔メンテナンス ／ 遠隔メンテナンスについての文書化*	NFO
MA-5	メンテナンス要員	CUI
MA-6	タイムリーなメンテナンス	NCO

表 E-10：メディア保護の管理策のアクション調整

NIST SP 800-53 中位ベースラインセキュリティ管理策		アクションの調整
MP-1	メディア保護の方針と手順	NFO
MP-2	メディアへのアクセス	CUI
MP-3	メディアのマーク付け	CUI
MP-4	メディアの保管	CUI
MP-5	メディアの輸送	CUI
MP-5(4)	*メディアの輸送 ／ 暗号学的な保護*	CUI
MP-6	メディアのサニタイゼ―ション	CUI
MP-7	メディアの利用	CUI
MP-7(1)	*メディアの利用 ／ 所有者以外の利用を禁止*	CUI

表 E-11：物理的及び環境的な保護の管理策のアクション調整

NIST SP 800-53 中位ベースラインセキュリティ管理策		アクションの調整
PE-1	物理的及び環境的な保護の方針と手順	NFO
PE-2	物理的アクセス権限付与	CUI
PE-3	物理的アクセス制御	CUI
PE-4	送信メディアのアクセス制御	NFO
PE-5	出力デバイスのアクセス制御	CUI
PE-6	物理的アクセスの監視	CUI
PE-6(1)	*物理的アクセスの監視 ／ 侵入アラーム／監視装置*	NFO
PE-8	来訪者のアクセス記録	NFO
PE-9	電源装置及び配線	NCO
PE-10	非常時遮断	NCO
PE-11	非常時電源	NCO
PE-12	非常時照明	NCO
PE-13	防火	NCO
PE-13(3)	*防火 ／ 自動消火機能*	NCO
PE-14	温度及び湿度の管理	NCO
PE-15	浸水の損害からの保護	NCO
PE-16	荷物の搬入と搬出	NFO
PE-17	代替作業拠点	CUI

表 E-12：計画の管理策のアクション調整

NIST SP 800-53 中位ベースラインセキュリティ管理策		アクションの調整
PL-1	セキュリティ計画作成の方針と手順	NFO
PL-2	システムセキュリティ計画	NFO
PL-2(3)	*システムセキュリティ計画 ／ その他の組織エンティティとの調整*	NFO
PL-4	行動規則	NFO
PL-4(1)	*行動規則 ／ ソーシャルメディアとネットワーク構築の制限*	NFO
PL-8	情報セキュリティアーキテクチャ	NFO

表 E-13：人的セキュリティの管理策のアクション調整

NIST SP 800-53 中位ベースラインセキュリティ管理策		アクションの調整
PS-1	人的セキュリティの方針と手順	NFO
PS-2	職位リスクの指定	FED
PS-3	要員に対する審査	CUI
PS-4	要員の解雇	CUI
PS-5	人事異動	CUI
PS-6	アクセス契約	NFO
PS-7	サードパーティ要員セキュリティ	NFO
PS-8	要員の処罰	NFO

表 E-14：リスクアセスメントの管理策のアクション調整

NIST SP 800-53 中位ベースラインセキュリティ管理策		アクションの調整
RA-1	リスクアセスメントの方針と手順	NFO
RA-2	セキュリティ分類	FED
RA-3	リスクアセスメント	CUI
RA-5	脆弱性のスキャン	CUI
RA-5(1)	*脆弱性のスキャン ／ アップデートツールの機能*	NFO
RA-5(2)	*脆弱性のスキャン ／ 定期的／新しいスキャンの前に／識別されたときに行われるアップデート*	NFO
RA-5(5)	*脆弱性のスキャン ／ 特権アクセス*	CUI

表 E-15：システム及びサービス調達の管理策のアクション調整[39]

NIST SP 800-53 中位ベースラインセキュリティ管理策		アクションの調整
SA-1	システムとサービスの調達の方針と手順	NFO
SA-2	資源の割り当て	NFO
SA-3	システム開発のライフサイクル	NFO
SA-4	調達プロセス	NFO
SA-4(1)	*調達プロセス ／ セキュリティ管理策の機能特性*	NFO
SA-4(2)	*調達プロセス ／ セキュリティ管理策の設計／実装の情報*	NFO
SA-4(9)	*調達プロセス ／ 使用中の機能／ポート／プロトコル／サービス*	NFO
SA-4(10)	*調達プロセス ／ 承認されたPIV製品の利用*	NFO
SA-5	情報システムの文書化	NFO
SA-8	システムエンジニアリングの原則	CUI
SA-9	外部情報システムサービス	NFO
SA-9(2)	*外部情報システムサービス ／ 機能／ポート／プロトコル／サービスの識別*	NFO
SA-10	開発者の構成管理	NFO
SA-11	開発者のセキュリティテストと評価	NFO

[39] SA-8は、*システム及びサービスの調達*ファミリがセキュリティ要件に含まれなかったので、附属書Dの*システム及び通信の保護*ファミリのセキュリティ管理策と共にグループ化されている。

表 E-16：システム及び通信の保護の管理策のアクション調整

NIST SP 800-53 中位ベースラインセキュリティ管理策		アクションの調整
SC-1	システム及び通信の保護の方針と手順	NFO
SC-2	アプリケーションの分離	CUI
SC-4	共有資源の情報	CUI
SC-5	サービス妨害（DoS）からの保護	NCO
SC-7	境界保護	CUI
SC-7(3)	*境界保護 ／ アクセスポイント*	NFO
SC-7(4)	*境界保護 ／ 外部通信サービス*	NFO
SC-7(5)	*境界保護 ／ デフォルト拒否／例外許可*	CUI
SC-7(7)	*境界保護 ／ リモートデバイスのスプリットトンネル禁止*	CUI
SC-8	送受信される情報の機密性と完全性	CUI
SC-8(1)	*送受信される情報の機密性と完全性 ／ 暗号化または代替の物理的保護*	CUI
SC-10	ネットワークの切断	CUI
SC-12	暗号鍵の確立と管理	CUI
SC-13	暗号学的保護	CUI
SC-15	共同コンピューティングデバイス	CUI
SC-17	公開鍵基盤証明書	FED
SC-18	モバイルコード	CUI
SC-19	ボイスオーバーインターネットプロトコル（VoIP）	CUI
SC-20	セキュアネーム／アドレスレゾリューションサービス（権威のある情報源）	NFO
SC-21	セキュアネーム／アドレスレゾリューションサービス（リカーシブまたはキャッシュレゾルバ）	NFO
SC-22	ネーム／アドレスレゾリューションサービスのアーキテクチャ及び初期設定	NFO
SC-23	セションの真正性	CUI
SC-28	保存情報の保護	CUI
SC-39	プロセス分離	NFO

表 E-17：システム及び情報の完全性の管理策のアクション調整

NIST SP 800-53 中位ベースラインセキュリティ管理策		アクションの調整
SI-1	システム及び情報の完全性に対する方針と手順	NFO
SI-2	欠陥の修正	CUI
SI-2(2)	*欠陥の修正 ／ 自動化された欠陥修正の状態*	NCO
SI-3	悪意のあるコード（不正プログラム）からの保護	CUI
SI-3(1)	*悪意のあるコード（不正プログラム）からの保護 ／ 集中管理*	NCO
SI-3(2)	*悪意のあるコード（不正プログラム）からの保護 ／ 自動アップデート*	NCO
SI-4	情報システムの監視	CUI
SI-4(2)	*情報システムの監視 ／ リアルタイム分析用の自動化されたツール*	NCO
SI-4(4)	*情報システムの監視 ／ 内向きと外向きの通信トラフィク*	CUI
SI-4(5)	*情報システムの監視 ／ システムにより生成された警告*	NFO
SI-5	セキュリティ警報、勧告、指令	CUI
SI-7	ソフトウェア、ファームウェア、及び情報の完全性	NCO
SI-7(1)	*ソフトウェア、ファームウェア、及び情報の完全性 ／ 完全性チェック*	NCO
SI-7(7)	*ソフトウェア、ファームウェア、及び情報の完全性 ／ 検出と応答の統合*	NCO
SI-8	スパムからの保護	NCO
SI-8(1)	*スパムからの保護 ／ 集中管理*	NCO
SI-8(2)	*スパムからの保護 ／ 自動アップデート*	NCO
SI-10	情報入力の妥当性確認	NCO
SI-11	エラー処理	NCO
SI-12	情報の取り扱いと保持	FED
SI-16	メモリ保護	NFO