NIST SP（特別出版物） **800-171**
Revision 2（改訂 2）

非連邦政府組織およびシステムにおける管理対象非機密情報（CUI）の保護

ロン・ロス **RON ROSS**
ヴィクトリア・ピリッテリー **VICTORIA PILLITTERI**
ケリー・デンプシー **KELLEY DEMPSEY**
マーク・リドル **MARK RIDDLE**
ゲイリー・ギッサニー **GARY GUISSANIE**

本出版物は以下から無料で入手可能：
https://doi.org/10.6028/NIST.SP.800-171r2

コンピュータ セキュリティ

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

NIST SP（特別出版物） **800-171**
Revision 2（改訂 2）

非連邦政府組織およびシステムにおける管理対象非機密情報（CUI）の保護

ロン・ロス
ヴィクトリア・ピリッテリー
ケリー・デンプシー
コンピュータ・セキュリティ部
米国標準技術研究所（*NIST*）

マーク・リドル
情報セキュリティ監督室
国立公文書記録管理局（*NARA*）

ゲイリー・ギッサニー
国防分析研究所（*IDA*）

本出版物は以下から無料で入手可能：
https://doi.org/10.6028/NIST.SP.800-171r2

2020 年 2 月
2021 年 1 月 28 日更新

米国商務省
ウィルバー・ロス, Jr.、長官

米国標準技術研究所（NIST）
ウォルター・コパン、標準・技術担当商務次官、部長

典拠（Authority）

本出版物は、FISMA（「連邦情報セキュリティ近代化法」：Federal Information Security Modernization Act）、合衆国法典（U.S.C.）第 44 編 第 3551 条等、および公法（P.L.）113 -283 に基づく法定責任にもとづき、NIST（米国標準技術研究所：National Institute of Standards and Technology）によって作成された。NIST は、連邦政府情報システムのための最小限の要件を含め情報セキュリティ規格（standards）および指針(guidelines)を作成する責任を負うが、これらの規格および指針は国家安全保障に係るシステムへの政策権限を執行する関係連邦政府担当官による明示された承認なしにそれらのシステムに適用してはならない。このガイドライン（指針）は、行政管理予算局（OMB：Office of Management and Budget）通達 A-130 の要件に一致している。

本出版物に記載されているものは、商務長官による法的権限により連邦政府機関に命じられ、義務付けられるとした規格および指針を否定するように解釈されてはならない。また、これらの指針は、商務長官、行政管理予算局長、またはその他のすべての連邦政府当局者の既存の権限を変更、あるいはそれらを置換するものと解釈されてはならない。本出版物は、非政府組織が任意に使用できるとともに米国における著作権の対象外である。NIST への帰属を示すことは評価される。

米国標準技術研究所（NIST）特別出版物（SP）800-171 改訂 2 113 頁（2020 年 2 月）
CODEN：NSPUE2
本出版物は以下より無料で入手可能：
https://doi.org/10.6028/NIST.SP.800-171r2

試行的手順や概念を適切に説明するために、文中に一定の商業エンティティ、装置、または資料が特定されることがある。そうした特定は、NIST による推奨や是認を意味するものではなく、エンティティ、資料、装置が必ずしもその目的に利用可能な最善のものであるということを意味しているものでもない。

また本出版物では、与えられた法定責任に従って NIST が現在開発中のその他の出版物を参照することがある。本出版物にある情報は、概念、実践例、および方法論を含め、そのような関連出版物の完成以前であっても連邦政府機関によって使用されることがある。したがって、それぞれの出版物が完成されるまでの間、その時点において運用している要件、指針、および手順が別に存在する場合には、それらは有効であり続ける。計画策定および移行の目的のためには、連邦政府機関は NIST によるこれらの新しい出版物の作成に密接に添うことになろう。

各組織は、指定されたパブリックコメント公募期間中に出版物の草稿を見直し、NIST へフィードバックを提供することは奨励される。上記のもの以外の多くの NIST 出版物は、以下から入手可能である。
https://csrc.nist.gov/publications

本出版物へのコメント提出先は以下である。

米国標準技術研究所（NIST）
情報技術研究所、コンピュータ・セキュリティ部
20899-8930 MD（メリーランド州）、ゲイサーズバーグ、ビューロー・ドライブ 100
e メール：**sec-cert@nist.gov**

全てのコメントは情報自由法（FOIA：Freedom of Information Act)[FOIA96]に基づく公開対象である

コンピュータシステム技術に関する報告

国立標準技術研究所（NIST）の情報技術研究所（ITL：Information Technology Laboratory）は、米国の計測・標準インフラへの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および社会福祉に貢献している。ITL は情報技術（IT）の開発ならびに生産的利用を促進するために、テスト、テスト方法、参照データ、概念実証（POC）、および技術分析等を研究している。ITL は、連邦政府情報システムにおける国家安全保障関連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およびプライバシーのための管理、運営、技術、物理的な規格および指針の開発に責任を持っている。本特別出版物 SP 800 シリーズは、情報システムのセキュリティに関する ITL の調査研究、指針、普及活動ならびに産業界、政府、および学術機関との協働活動について報告するものである。

摘要（Abstract）

非連邦政府のシステムおよび組織に存在する「機密指定はされてないが管理対象となる情報」（以降、管理対象非機密情報または単に CUI（CUI：Controlled Unclassified Information）と記述）を保護（protecting）することは連邦政府機関にとって極めて重要であり、連邦政府が必須なミッションおよび業務を成功裏に遂行する能力に直接的な影響をおよぼす可能性がある。本出版物は、以下の場合に CUI の秘匿性（confidentiality）を保護するための推奨セキュリティ要件を連邦政府機関に提供するものである：すなわち、(1) CUI が非連邦政府組織およびシステムに存在する場合;(2) 非連邦政府組織が CUI を連邦政府機関の代行として収集・維持していない場合、あるいはシステムを連邦政府機関に代わって使用または運用しているのではない場合；および、(3) CUI レジストリーにリストされている CUI カテゴリーに対する認可法、規則、または政府全体のポリシーによって規定されている CUI の秘匿性を保護するための具体的な保全（safeguarding）要件が無い場合である。本要件は、CUI を処理、保存、および／または伝送する、あるいはそれらのコンポーネントに保護機能を提供する非連邦政府のシステムおよび組織の全てのコンポーネントに適用される。本セキュリティ要件は、連邦政府機関と非連邦政府組織の間で締結された契約手段またはその他の合意（agreement）の中で、連邦政府機関によって使われることを意図している。

キーワード

基本セキュリティ要件（Basic Security requirement）；契約事業者システム（Contractor Systems）；管理対象非機密情報（Controlled Unclassified Information）；CUI レジストリー（CUI Registry）；派生セキュリティ要件（Derived Security Requirement）；大統領令（Executive Order）13556；FIPS 出版物 199；FIPS 出版物 200；FISMA；NIST SP 800-53；非連邦政府組織；非連邦政府システム（Nonfederal Systems）；セキュリティアセスメント（Security Assessment）；セキュリティ管理策（Security Control）；セキュリティ要件（Security Requirement）。

登録商標

謝辞

著者は、コンピュータ・セキュリティ部門と応用サイバーセキュリティ部門の科学者、技術者、および研究スタッフが本出版物の内容の改善に役立つ優れた貢献をしたことを認めたい。
パット・オーレイリー（Pat O 'Reilly）、ジム・フォッティ（Jim Foti）、ジェフ・ブリュワー（Jeff Brewer）、および NIST ウェブチームの傑出した管理サポートに特別な感謝を捧げる。
最後に、著者はまた、国内外の公共部門と民間部門の個人と組織からの貢献に感謝する。その思慮深く建設的なコメントにより、この出版物の全体的な品質、徹底性、および有用性が向上した。

NIST SP800-171 へのこれまでの貢献

著者たちは 2015 年 6 月の開始以来、特別出版物 800-171 のこれまでの版に貢献した下記を含む多くの方々に謝意を表する。

記

キャロル・ベイルズ（Carol Bales）、マシュー・バレット（Matthew Barrett）、ジョン・ボエンズ（Jon Boyens）、デヴィン・ケイシー（Devin Casey）、クリスチャン・エンロー（Christian Enloe）、ペギー・ハイムズ（Peggy Himes）、ロバート・グレン（Robert Glenn）、エリザベス・レノン（Elizabeth Lennon）、ヴィッキー・ミケッティ（Vicki Michetti）、ドリアン・パッパス（Dorian Pappas）、カレン・クイッグ（Karren Quigg）、メアリー・トーマス（Mary Thomas）、マシュー・ショール（Matthew Scholl）、ムルギア・スッパヤ（Murugiah Souppaya）、パトリシア・トス（Patricia Toth）、パトリック・ヴィスクーソ（Patrck Viscuso）。

特許開示通知

注意：情報技術研究所（ITL）は、本出版物のガイダンスまたは要件に準拠するために使用することが必要となる可能性のある特許権の所有者に、そのような特許権を ITL に開示することを求めている。ただし、特許の保有者は ITL による特許の開示要求に対応する義務はなく、ITL は、この出版物に適用される可能性のある特許を特定するための特許調査を行っていない。

なお、本出版物のガイダンスまたは要件に準拠するために使用することが必要となる可能性のある特許権を特定するための、公開日およびそれ以降の案内の中では、今のところ ITL にそのような特許権は特定されていない。

また ITL は、本出版物の使用における特許侵害を回避するためにライセンスが必要でないということは表明あるいは暗示していない。

注意事項

2014年の 連邦政府情報セキュリティ近代化法[FISMA] は、連邦政府機関に対し、 (1) 政府機関により、または政府機関に代わって収集・維持される情報；あるいは (2) 政府機関により、または政府機関の契約事業者により、あるいは政府機関を代理するその他の組織によって使用・運用される情報システムへの認可されてないアクセス、使用、開示、通信の途絶（disruption）、変更、または毀損から生ずるリスクに対応した情報セキュリティ保護を特定し、提供することを求めている。本出版物は、*非連邦政府* のシステムおよび組織における「管理対象非機密情報」（CUI）の *秘匿性* の保護に焦点を当て、その目標を達成するためのセキュリティ要件を推奨（recommend）している。これは、[FISMA] で規定されている要件をどのような形においても変更するものではなく、また連邦政府機関が、法令の全条項、OMB によって設定されたポリシー、および NIST によって開発された支援セキュリティ規格および指針に準拠するための責任を変えるものでもない。

本出版物で適用を推奨されている要件は、[FIPS 200] および [SP 800-53] における中位セキュリティ管理策ベースラインならびに提案中のCUI規則 [32 CFR 2002] に基づいた（derived from）ものである。当該要件および管理策は、[FISMA]で扱われている連邦政府の情報およびシステムに必須の保護要件を提供するために、時間をかけて規定されたものである。[FIPS 200] の要件と[SP 800-53]の管理策に適用されるテーラリング基準（tailoring criteria：削除または調整基準）は、それらの要件および管理策の排除を是認するものと解釈***されてはならず***、むしろ、このテーラリング基準は、非連邦政府のシステムと組織における認可されてない開示からCUIを保護することに焦点を当てるものである。さらに、このセキュリティ要件は、上に挙げたNIST出版物から派生しているものであるため、各組織は、それらの要件を満たしても、[FIPS 200] および[SP 800-53] のセキュリティの要件と管理策を自動的に満たすものになると推定***してはならない***。

*秘匿性 （confidentiaity）*というセキュリティ目標に加えて、*完全性 （integrity）*および*可用性 （availability）*という目標も、包括的な情報セキュリティ施策の確立・維持に携わる組織にとっては高い優先事項である。本出版物の主要目的は、CUIの秘匿性を保護する要件を規定することであるが、秘匿性と完全性の間には密接な関係が存在する。というのは、システムレベルの基礎になるセキュリティメカニズムの多くが双方のセキュリティ目標を支えているからである。したがって、本出版物の基本セキュリティ要件および派生セキュリティ要件は、CUIの認可されてない開示だけでなく認可されてない変更から保護することも提供している。本出版物の推奨要件に関心を持ち、あるいはそれに準拠することを求められる組織は、付属書Eにある中位ベースラインの管理策に関する記載事項全体を見直し、組織の個別セキュリティ計画とセキュリティ管理策の展開が、組織のミッションと事業運営に対する多様なサイバー脅威および物理的脅威に対処する上で、必要かつ十分な保護を提供するものであることを確実にすることが強く勧められる。

CUI セキュリティ要件

本出版物に含まれる推奨セキュリティ要件は、連邦政府機関から契約、認可、またはその他の合意で義務付けられている場合にのみ、非連邦政府の組織またはシステムに適用される。当該セキュリティ要件は、CUI を処理、保存、または伝送する、またはそのようなコンポーネントのセキュリティ保護を提供する非連邦政府システムのコンポーネントに適用される。

重要インフラのサイバーセキュリティを改善するためのフレームワーク

NIST の『重要インフラのサイバーセキュリティを改善するためのフレームワーク』（*NIST Framework for Improving Critical Infrastructure Cybersecurity* [NIST CSF]）を実装している組織や、実装を計画している組織は、管理対象非機密情報（CUI）セキュリティ要件と、[SP 800 - 53]および[ISO 27001]のセキュリティ管理策との直接的な対応付け（mapping）を、付属書 D に見ることができる。これらの管理策は、識別・防御・検知・対応・復旧という「サイバーセキュリティフレームワーク」の中核機能に関連付けられたカテゴリーとサブカテゴリーにも対応している。この対応付けは、セキュリティ要件への準拠性を論証（demonstrate）したい組織にとっては、それぞれの組織が整えた情報セキュリティ対策が NIST や ISO/IEC のセキュリティ管理策に沿って構築されている場合には、有用なものとなろう。

追加情報源

セキュリティ管理策とサイバーセキュリティフレームワークとの対応付けについては https://csrc.nist.gov/publications/detail/nistir/8170/archive/2017-05-12 を参照。

CUI セキュリティ要件とサイバーセキュリティフレームワークとの対応付けについては https://csrc.nist.gov/projects/cybersecurity-framework/informative-reference-catalog/details/ 1 を参照。

目次

正誤表

本表は特別出版物（SP）800-171 に組み込まれた変更が含まれている。正誤表の更新には、*編集上（Editorial）*のまたは*本質的（Substantive）*な内容の修正、説明、または出版上のその他の小さな変更が含まれる場合がある。

発行日	タイプ	変更内容	頁

第 1 章

はじめに

管理対象非機密情報（CUI）を保護する必要性

現在、連邦政府は、歴史上これまでになく外部のサービスプロバイダに依存して、多様な連邦政府の任務および事業機能を遂行するために情報システム[1]を運用している。連邦政府との契約事業者の多くは、要注意（sensitive）連邦政府情報を処理、保存、および伝送することで連邦政府機関にとって必須な製品やサービスの納入を支えている（たとえば、金融サービスの提供、web および電子メールサービスの提供、身元調査または健康管理データの処理、クラウドサービスの提供、通信・衛星・兵器システムの開発など）。連邦政府の情報は、州および地方政府、単科大学および総合大学、そして独立調査機関などの組織に頻繁に提供され、またそれらと共有されている。*非連邦政府のシステム*[2]および各組織に存在している間における要注意連邦政府情報の保護は、連邦政府機関にとって極めて重要であり、連邦政府が、指定された任務および事業運営（business operations）を遂行する能力に、直接的なインパクトをおよぼす可能性がある。

非連邦政府のシステムおよび各組織内の非機密連邦政府情報を保護できるかどうかは、連邦政府によって使われる様々なタイプの情報を識別するためのプロセスを、連邦政府が提供できるかどうかにかかっている。[EO 13556]は、保護を必要とする非機密情報（CUI）[3]を執行部門（executive branch）が取り扱う方法を標準化するために、政府全体の CUI プログラム[4]を設けた。連邦法、規則、または政府全体のポリシーに従って保全措置や配布管理を必要とする情報だけが、CUI として指定されることができる。 CUI プログラムは、一貫性のないマーキング、不十分な保全、不必要な制限など、非機密情報を管理・保護する上でのいくつかの欠陥に対処することを意図している。その方法は、手順の標準化および CUI レジストリー[NARA CUI]を通じた共通規定の提供の双方による。CUI レジストリーは、CUI の取扱に関する情報、ガイダンス、ポリシー、および要件のためのオンラインリポジトリであり、CUI 執行機関によって発行されるものを含む。CUI レジストリーは、特に、承認済 CUI カテゴリーを識別し、それぞれに一般的説明を規定し、管理策の基準を明らかにし、また CUI を使う手順を設定している。これには、情報のマーキング、保全、移動、配布、再利用、廃棄が含まれるが、それに限定されるものではない。

---

[1] 「情報システム」（*information system*）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明示的に組織された個別の情報リソースの集合である。情報システムには、産業/プロセス制御システム、サイバーフィジカルシステム、組込みシステム、およびデバイスなど特化したシステムも含まれる。「システム」という用語は本出版物では CUI を処理、保存、または伝送することができるすべてのタイプの情報処理プラットフォームを示すものとして用いられている。

[2] 「連邦政府情報システム」とは、執行機関、執行機関の契約事業者、または執行機関を代理する別組織によって利用され、あるいは運用されるシステムである。この規準を満たさないシステムは、「非連邦政府システム」（*nonfederal system*）である。

[3] 「管理対象非機密情報」は、法、規則、または政府全体のポリシーが保全または配布管理を要求するような情報であり、改訂を含む［EO 13526］または以前のあるいは後継の大統領令、または［ATOM 54］で機密扱い（classified）にされた情報を除く。

[4] ［EO 13556］は CUI プログラムを実施する執行機関として国立公文書記録管理局（NARA）を指定した。

[EO 13356] はまた、CUI プログラムが、開示性、透明性、および政府全体のプラクティス（対応する業務）の統一性を重視すること、そしてプログラムの履行が、行政管理予算局（OMB：Office of Management and Budget）によって定められた適用可能なポリシーと、米国標準技術研究所（NIST：National Institute of Standards and Technology）によって発行される連邦規格および指針と整合性のある方法で行われることを求めている。CUI 執行機関によって策定（developed）された連邦政府 CUI *規則*は、CUI の指定、保全、配布、マーキング、解除（decontrolling）、および処分（disposition）に関して連邦政府機関にガイダンスを提供し、自己点検と監督要件を定め、またプログラムのその他の側面について正確に概説している。

1.1 目的および適用性

本出版物の目的は、以下の場合に CUI の*秘匿性*を保護するための推奨セキュリティ要件[6]を連邦政府機関に提供することである：すなわち、(1) CUI が非連邦政府組織およびシステムに存在する場合；(2) 非連邦政府組織が CUI を連邦政府機関の代行として収集・維持して*いない*場合、あるいはシステムを連邦政府機関に代わって使用または運用して*いるのではない*場合；[7]および、(3) CUI レジストリーにリストされている CUI カテゴリーに対する認可法、規則、または政府全体のポリシーによって規定されている CUI の秘匿性を保護するための具体的な保全要件が無い場合である。[8]

本要件は、CUI を処理、保存、または伝送する非連邦政府システムのコンポーネント[9]あるいはそれらのコンポーネントにセキュリティ保護を提供する非連邦政府システムのコンポーネントに適用される。非連邦政府組織が CUI の処理、保存、または伝送のために特定のシステムコンポーネントを指定する場合、それらの組織は、指定されたシステムコンポーネントを別の CUI

[5] [32 CFR Part 2002]2016 年 9 月 14 日に発行され、2016 年 11 月 14 日発効した。

[6] *要件*という用語は、さまざまな文脈で使用される。連邦政府の情報セキュリティおよびプライバシーの保護政策（ポリシー）に関連して、この用語は通常、組織に課せられる情報セキュリティおよびプライバシーの保護義務を指すために使用される。たとえば、OMB A-130 は、連邦政府機関が情報リソースを管理する際に準拠しなければならない一連の情報セキュリティとプライバシーの保護要件を課している。連邦政府の政策の文脈での要件という用語の使用に加えて、要件という用語はこのガイドラインではより広い意味で使用され、特定のシステムまたは組織に対する一連の利害関係者の保護ニーズという表現を指している。利害関係者の保護ニーズとそれに対応するセキュリティ要件は、多くの情報源（法律、行政命令、指令、規則、ポリシー、規格、ミッションとビジネスのニーズ、リスクアセスメントなど）から導き出される場合がある。本ガイドラインで使用される要件という用語には、法的要件とポリシー要件の両方、および他のソースから派生する可能性のある幅広い一連の利害関係者の保護ニーズの表現が含まれる。これらの要件はすべて、システムに適用された場合、システムに必要な特性を決定するのに役立つ。

[7] 連邦政府機関を*代行して*情報を収集・維持する非連邦政府組織、または連邦政府機関を*代理して*システムを運用・使用する非連邦政府組織は、「連邦情報セキュリティ近代化法」（FISMA：Federal Information Security Modernization Act）の要件に準拠しなければならない。それには、[FIPS 200] の要件、および[SP 800-53] のセキュリティ管理策が含まれる。（参照：44 USC 3554(a)(1)(A)）

[8] 本出版物に示す要件は、政府機関の担当官が非連邦政府システムおよび組織に存在する CUI を含め、彼らの管理下の資産および運用を支援する情報に対する[FISMA]要件に準拠した情報セキュリティ措置のために利用できる。

[9] システム*コンポーネント*には、たとえば、(1) メインフレーム、ワークステーション、サーバー；(2) 入出力デバイス；(3) ネットワークコンポーネント；(4) オペレーティングシステム；(5) バーチャル・マシン；および(6) アプリケーションが含まれる。

セキュリティドメインに分離することにより、セキュリティ要件の範囲を制限できる。分離は、アーキテクチャーと設計の概念を適用することで実現できる（例えば、ファイアウォールやその他の境界保護デバイスを使用してサブネットワークを実装し、情報フロー制御メカニズムを使用する）。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する場合がある。このアプローチにより、CUI に適切なセキュリティを提供し、組織のセキュリティ態勢を、ミッション、運用、および資産を保護するために必要なレベルを超えて増加させることを回避できる。本出版物で推奨されるセキュリティ要件は、連邦政府機関と非連邦政府組織の間で締結される該当する契約手段またはその他の合意書の中で、連邦政府機関によって使われることを意図している。CUI ガイダンスおよび CUI 連邦政府調達規則（FAR）[10]では、CUI 執行機関がセキュリティ要件[11]への準拠性判断を行う。

CUI を処理、保存、または伝送する連邦政府システムを使う連邦政府機関は、連邦政府 CUI 規則に従って、 少なくとも、以下に準拠しなければならない。

- 連邦情報処理規格（FIPS）199『連邦政府情報および情報システム（中位秘匿性）[12]のセキュリティカテゴリー化に関する規格』
- 連邦情報処理規格（FIPS）200『連邦政府情報および情報システムに関する最低限のセキュリティ要件』
- NIST SP 800-53『連邦政府情報システムおよび組織のためのセキュリティおよびプライバシー管理策』
- NIST SP 800-60『セキュリティカテゴリーに対して情報および情報システムのタイプを対応付けするためのガイド』

CUI を保護し、CUI を確実に管理するという連邦政府機関の責任は、そうした情報が非連邦政府パートナーと共有される期間においても変わらない。したがって、非連邦政府のシステムを使用する非連邦政府組織[13]によって CUI が処理、保存、または伝送される時にも、類似レベルの保護が必要とされる。非連邦政府組織およびシステムにある CUI を保全するための具体的な要件は、一貫した保護レベルを維持するために、上述の連邦政府規格と指針から引き出される。しかしながら、連邦政府 CUI 規則の保全要件の範囲が、秘匿性のセキュリティ目標に限定されていること（すなわち完全性や可用性に直接対処していないこと）、および NIST の規格および指針に示されているセキュリティ要件の一部が連邦政府独自のものであることを認識した上で、本出版物の要件は非連邦政府の組織向けにテーラリングされている。

[10] NARA は、CUI 執行機関として、連邦政府 CUI 規則および「NIST SP 800-171」の要件を契約事業者に適用する単一条項を提出する計画である。このような FAR 条項が施行されるまでは、連邦法および規則の要件に従う連邦政府契約に際して NIST SP 800-171 のセキュリティ要件が参照されることになろう。

[11] [SP 800-171A] は、組織が第 3 章のセキュリティ要件への準拠性を判断するアセスメント手順を提供している。

[12] [FIPS 199] は、セキュリティがブリーチ（たとえば秘匿性の欠損）した場合における、組織、資産、または個人に対する 3 種類の潜在的インパクト（低位（low）、中位（moderate）、高位（high））を規定している。

[13] *非連邦政府組織* とは、非連邦政府のシステムを所有、運用、または維持する組織すべてのことである。非連邦政府組織の例には、州政府・地方政府・部族政府、単科大学・総合大学、および契約事業者が含まれる。

第２章で説明されるテーラリング基準は、提案中の連邦政府 CUI 規則に示されている CUI の保全のための連邦政府要件を縮小、または 最小限にすることは意図していない。その意図はむしろ、非連邦政府のシステムおよび組織内で同等の保全手段を可能にし、また促進するような方法で、その要件を示すことであり、中位の秘匿性に求められる CUI の保護レベルを弱めることではない。本出版物で記述される要件以外の追加要件や別途要件が適用される可能性があるのは、そうした要件が法律、規則、または政府全体のポリシーに基づいている時と、CUI レジストリーに特定 CUI（CUI-specified）と指定されている時、あるいは基本 CUI（CUI Basic）[14]の秘匿性を中位以上の要件とする合意が成立した時である。特定カテゴリー内への CUI 保全要件の規定は、(1) 国立公文書記録管理局（NARA）の CUI ガイダンスおよび CUI FAR の中で NARA によって検討されている；また（2）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ことになる。 CUI インフラが、認可法、規則、または政府全体のポリシーによって要求される、または許可された特定の保全要件を含むその組織の CUI 関連の契約または合意のための保全要件を満たしている場合、非連邦政府組織は、複数の政府契約や合意書に対して同一の CUI インフラを使用できる。

1.2 対象読者

本出版物は、以下の公共部門と民間部門双方の組織ならびに個人の様々なグループに役立つものであるが、それらの者に限定されるものではない。

- システムの開発ライフサイクルに責任を有する（プログラム管理者、ミッション／事業オーナー、情報オーナー／管理者、システム設計者および開発者、システム／セキュリティ技術者、システムインテグレータなど)。
- 購買（acquisition）または調達（procurement）責任を有する者（契約責任者など)。
- システム、セキュリティ、またはリスク管理および監督に責任を有する（認可担当者、 CIO（最高情報責任者)、CSO（最高情報セキュリティ責任者)、システムオーナー、情報セキュリティ管理者など)。
- セキュリティアセスメントおよび監視責任を有する（監査人、システム評価者、アセッサー、独立検証者／確認者、分析者など)。

上記の役割と責任は、異なる二つの観点から見ることができる。すなわち、(1) 契約手段またはその他のタイプの組織間合意書におけるセキュリティ要件を確立し、伝達する組織体としての連邦政府の観点、および (2) 契約書または合意書に示されたセキュリティ要件に対応し、それに準拠する組織体としての*非連邦政府の観点*である。

[14] 基本 CUI（CUI Basic）は CUI レジストリーに規定されている［NARA CUI］。

1.3 本出版物の構成

本出版物は、これ以降、以下のように構成されている。

- 第２章では、(1) CUI の秘匿性を保護するためのセキュリティ要件の開発に用いられる基本的な前提条件と方法論；(2) 要件の形式と構造、および要件を取得するために NIST 規格および指針に適用されるテーラリング基準について説明する。
- 第３章では、非連邦政府組織およびシステムにおいて、CUI の秘匿性を保護する 14 のセキュリティ要件ファミリーについて記述する。
- 補足の付属書では、非連邦政府組織およびシステムにおける CUI 保護に関連した以下の付加情報を提供する：(A) 一般的参照情報；(B) 規定および用語集；(C) 本出版物で使われる頭字語；(D)セキュリティ要件を[SP 800-53]と[ISO 27001]のセキュリティ管理策に関連付ける対応付け表； (E) 中位セキュリティ管理策ベースラインに充てられたテーラリング措置。

第２章
基礎
セキュリティ要件開発のための前提条件と方法論

本章では、(1) 非連邦政府のシステムおよび組織における CUI を保護する推奨セキュリティ要件の開発に使われる基本的前提条件と方法論；(2) 基本および派生セキュリティ要件の構造；および (3) 連邦政府情報セキュリティ要件と管理策に適用されるテーラリング基準を説明する。

2.1 基本的（basic）前提条件

本出版物で記述される推奨セキュリティ要件は、 以下の３つの基礎的（fundamental）前提条件を基にして開発されている。

- CUI を保護するための法令および規則上の要件は、その情報が連邦政府システムに存在する場合も、あるいはそのシステムが運用されている環境を含めて、それが非連邦政府システムに存在する場合も *首尾一貫*（consistent）している。
- CUI を保護するために実装される保全措置は、連邦政府と非連邦政府双方のシステムおよび組織で *首尾一貫* している。
- CUI のための秘匿性インパクト値は、[FIPS 199]の *中位*[15,16]より低いことはない。

上記の前提は、CUI に指定された連邦政府情報は、その情報が連邦政府と非連邦政府のどちらの組織に存在する場合においても同一の本質的な *価値* を持ち、またそれが危殆化した場合には、*有害なインパクト*をもたらす可能性があるという基本的考え方を補強するものである。それ故に、CUI の秘匿性を保護することは、連邦政府機関のミッションおよび事業の成功にとって、そして米国の経済および国家安全保障の利益にとって極めて重要である。セキュリティ要件の開発にインパクトをおよぼし、また非連邦政府組織とともに活動する連邦政府機関の期待にも影響をおよぼす付加的前提条件には、以下が含まれる。

- 非連邦政府組織は、情報技術インフラを適所に備えており、必ずしも CUI を処理、保存、または伝送するためにシステムを開発あるいは取得する必要はない。
- 非連邦政府組織は、自らの情報を保護する個別の保全手段を保有しており、それはセキュリティ要件を満たす上で十分である可能性がある。
- 非連邦政府組織は、あらゆるセキュリティ要件を満たすために必要な組織構造や資源を保有していないかもしれないが、要件を満たせないことを補償（compensate）するために、

[15] [FIPS 199] で規定されている中位インパクト *値*は、[FIPS 200] では中位インパクト *システム*の一部になる可能性があるが、その代わりテーラリング措置の出発点として [SP 800-53] の中位セキュリティ管理策ベースラインの使用を必要とする。

[16] [32 CFR 2002]に従って CUI は中位の秘匿性インパクト値以上に区分される。しかしながら、CUI の統制を確立する連邦法、規則または政府全体のポリシーが中位の秘匿性ベースラインとは異なる管理策を指定している場合はこれらに従う。

同様に有効なセキュリティ手段（security measures）を代替策（alternative）として実装することができる。

- 非連邦政府組織は、セキュリティ要件を満たすために、直接的に、あるいはマネージドサービス（managed services）を利用することで、必要性が考えられる様々なセキュリティソリューションを実装することができる。

CUI に対する単一（single state）セキュリティ対策（solution）の実装

CUI は、このような情報が連邦政府機関の一部で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*。したがって、本出版物に含まれる推奨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およびガイドラインと矛盾なく、補完するものである。

2.2 セキュリティ要件の開発

非連邦政府システムおよび組織において CUI の秘匿性を保護するためのセキュリティ要件は、明確に規定された構造を持ち、それは以下で構成される。 すなわち、 (1) *基本（basic）セキュリティ要件* の節（section）と、(2) *派生（derived）セキュリティ要件*の節である。基本セキュリティ要件は [FIPS 200] から得られており、これは、連邦政府の情報およびシステムのための高位かつ基礎的なセキュリティ要件を提供するものである。派生セキュリティ要件は、基本セキュリティ要件を補完（supplement）するものであり、[SP 800-53] のセキュリティ管理策から取り入れられており、その中位ベースラインのセキュリティ要件とセキュリティ管理策（すなわち、連邦政府システムおよび組織の CUI に求められる最低限の保護レベル）を基に、以下の基準に該当する要件、管理策、または管理策の一部をテーラリング（削除または調整）されている。

- 連邦政府固有のもの（すなわち一義的に連邦政府の責任であるもの）
- CUI の秘匿性の保護に直接関係しないもの
- 明確化しなくても非連邦政府組織によって日常的に満たされると期待されるもの[17]

[17] テーラリングされた[FIPS 200] のセキュリティ要件および[SP 800-53] の中位セキュリティ管理策ベースラインから開発される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全手段のサブセットとして表されている。非連邦政府組織におけるそうしたプログラムの強度と品質の良し悪しは、その組織が、連邦政府に指定されることなしに日常的に満たすことを期待されるセキュリティ要件と管理策を、どの程度実装できるかにかかっている。これには、リスクベースの効果的な情報セキュリティプログラムを支える、セキュリティポリシー、手順、およびプラクティス（対応する業務）の実装が含まれる。非連邦政府組織には、第 3 章 のセキュリティ要件の範囲外と思われる中位ベースラインのセキュリティ管理策の全リストとして、付属書 E および[SP 800-53]を参照することが推奨される。

付属書 E は、CUI 派生セキュリティ要件を支えるセキュリティ管理策と、上述された CUI テーラリング基準に基づいて中位ベースラインから削除または調整されたセキュリティ管理策に関するリストを提供する。

基本セキュリティ要件と派生セキュリティ要件を組み合わせることで、非連邦政府のシステムと組織にある CUI の秘匿性保護に関して、[FIPS 200]および[SP 800-53]の意図を把握することができる。付属書 D は、[SP 800-53]および[ISO 27001]の中の関連するセキュリティ管理策に対する、セキュリティ要件の非公式な対応付けを提供する。この対応付けは、CUI セキュリティ要件のより良い理解を促進するためのものであって、非連邦政府組織に付加的な要件を課することを意図したものではない。

以下の*媒体保護*ファミリーの例は、CUI 要件の構造を例解（illustrates）している。

基本セキュリティ要件

3.8.1	紙とデジタル双方とも、CUI を含むシステムの媒体を保護する（すなわち、セキュアに保存し物理的に管理する）。
3.8.2	システム媒体上の CUI へのアクセスを、認可されたユーザーに限定する。
3.8.3	CUI を含むシステムの媒体を廃棄または再利用する前に、サニタイズ（情報除去）または破壊する。

派生セキュリティ要件

3.8.4	CUI のマーキングと配布制限が必要な媒体にはその旨をマーキングする。
3.8.5	CUI を含む媒体へのアクセスを管理し、管理区域外での輸送中は、媒体に関する説明責任を維持する。
3.8.6	代替的な物理的保全措置によって保護されている場合を除き、デジタル媒体上に保存された CUI の秘匿性を輸送時に保護するため、暗号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リムーバブル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のオーナーを識別できない時には、そうしたストレージデバイスの使用を禁止する。
3.8.9	保管場所にあるバックアップ CUI の秘匿性を保護する。

使い易さの観点からセキュリティ要件は 14 の*ファミリー*に体系化されている。各ファミリーには、そのファミリーの一般的なセキュリティ項目に関係する要件が含まれている。各ファミリーは[FIPS 200] で説明されている連邦政府情報およびシステムのための最小セキュリティ要件に沿って調整（aligned）されている。*緊急時対応計画*（*contingency planning*）作成、*システムおよびサービスの取得*、および*計画作成*要件は、テーラリング基準に従い、本出版物

の範囲には含まれない[18]。表１に本出版物で扱われるセキュリティ要件ファミリーを示す。

表１：セキュリティ要件ファミリー

ファミリー	ファミリー
アクセス管理	媒体保護
意識向上および訓練	職員のセキュリティ
監査および説明責任	物理的保護
構成管理	リスクアセスメント
識別および認証	セキュリティアセスメント
インシデント対応	システムおよび通信の保護
メンテナンス	システムおよび情報の完全性

*詳解（discussion）*セクションは、CUI セキュリティ要件の実装とアセスメントを容易にするための追加情報として各要件のすぐ後に記載されている。この情報は、主として[SP 800-53]のセキュリティ管理策の詳解セクションから導出されたもので、CUI を保護するために適用される管理策を実装するために用いられるメカニズムと手順を、組織がよりよく理解するために提供されている。なお、詳解セクションはあくまでも*参考情報*であり、*規範的*ではなく、要件の範囲を拡張したり、要件を満たすために組織が使用するソリューションに影響を与えることは意図されてない。例示の使用は概念的であり、網羅的ではなく、組織が適用可能なオプションを反映しているものでもない。図１に、基本的なセキュリティ要件である 3.8.1 と、それに対応する詳解セクションおよび参考資料を例示する。

[18] 3 つの例外には以下が含まれる。すなわち、(1) *緊急事態対応計画*ファミリーにおけるシステムバックアップ（CP-9 からの導出）の秘匿性保護要件、(2) *計画*ファミリーにおけるシステムセキュリティ計画書を策定および実装するための要件（PL-2 からの導出） (3) システムおよびサービス取得ファミリー におけるシステムセキュリティエンジニアリングの原則（SA-8 からの導出）を実装する要件である。当該要件は、それぞれ、CUI の*媒体保護*、*セキュリティアセスメント*, *およびシステムおよび通信の保護*ファミリーに含められている

3.8.3 CUI を含むシステムの記憶媒体を廃棄または再利用する前に、サニタイズ（情報除去）または破壊する。

詳解

この要件は、処分または再利用の対象となるデジタルおよび非デジタルのすべてのシステム記憶媒体に適用される。例として、ワークステーション、ネットワークコンポーネント、スキャナー、コピー機、プリンター、ノートパソコン、モバイルデバイスに見られるデジタル記憶媒体と、紙やマイクロフィルムなどの非デジタル記憶媒体があげられる。サニタイズプロセスでは、情報の取り出しや再現ができないような形で、情報が記憶媒体から削除される。消去、除去、暗号化消去、破壊を含むサニタイズ技法は、記憶媒体が再利用または処分される際に、認可されてない個人に情報が漏えいすることを防止する。

組織は、サニタイズが必要な記憶媒体に対して、当該記憶媒体に他の手段を適用できない場合には破壊が必要となる可能性を認識した上で、適切なサニタイズ手法を決定する。組織は、パブリックドメインにある情報や公開可能な（releasable）、または再利用や処分のために提供され、組織や個人に有害なインパクトを及ぼさないと見なされる情報を保存している記憶媒体に対しては、サニタイズ技法および手順を自由に採用することができる。非デジタル媒体のサニタイズには、たとえば、媒体を破壊することやドキュメントからCUIを削除することに加えて、ドキュメントから単語やセクションを削除する場合と同等の効果が得られるように、ドキュメント内の選択した単語やセクションを編集して隠蔽することが含まれる。NARAのポリシーおよびガイダンスは、CUIのサニタイズプロセスの管理を規定している。

[SP 800-88] は、記憶媒体のサニタイズに関するガイダンスを提供する。

図１：CUI セキュリティ要件の様式と構造

第３章

要件

CUI の秘匿性を保護するためのセキュリティ要件

本章では、非連邦政府のシステムおよび組織にある CUI の秘匿性を保護するための 14 の推奨セキュリティ要件ファミリーについて記述する[19]。基本要件と派生要件に関連する[SP 800-53] のセキュリティ管理策は、付属書 D にも記載されている[20]。 各組織は、推奨セキュリティ要件に関連する本文書での規定外の追加情報（例えば、参照されるセキュリティ管理策それぞれの詳解セクションにおける解説的な情報、[ISO 27001]セキュリティ管理策への対応付け表、必要に応じて付加的セキュリティ要件の特定に利用可能な管理策オプションの一覧表（catalog）など）を入手するために、NIST 出版物を利用することができる。この情報は、ミッションおよび事業の要件、運用環境、またはリスクアセスメントとの関連で、要件を明確化し、または解釈することに役立てることができる。非連邦政府組織は、セキュリティ要件を満たすために、直接またはマネージドサービスを利用して、様々な潜在的セキュリティソリューションを実装することができ、また要件を満たせない場合にはそれを補償すべく、代替的ではあるが同様に有効なセキュリティ手段を実装することができる[21]。

詳解セクションについて

各 CUI 要件に付されている詳解セクションは*参考情報（informative）*であり、*規範的（normative）*ではなく、要件の範囲を拡張したり、要件を満たすために組織が使用するソリューションに影響を与えることは意図されてない。加えて、例示の使用は概念的であり、網羅的ではなく、組織が適用可能なオプションを反映しているものでもない。

非連邦政府組織は、システムセキュリティ計画書（SSP : system security plan）に、セキュリティ要件がどのように満たされており、または組織が要件をどのように満たす計画で、既知および想定される脅威に対処することについて記述する。このシステムセキュリティ計画書にはシステムの範囲、運用環境、セキュリティ要件の実装方法およびその他のシステムとの関係や連接について記述される。また非連邦政府組織は、実装されていないセキュリティ要件がどのように満たされるか、および計画される緩和策がどのように実装されるかについて記述する実施計画書（PoA : plan of action）を作成する。各組織はシステムセキュリティ計画書および実施計画書は別文書または統合された文書など任意の様式で文書化することができ

[19]システムレベルの基礎となるセキュリティメカニズムの多くが、双方の目標を支えているため、秘匿性と完全性のセキュリティ目標は密接に関連している。したがって、本出版物の基本および派生セキュリティ要件は、CUI の認可されてない開示および認可されてない変更からの保護を提供している。

[20]付属書 D でセキュリティ管理策を参照しているのは、推奨セキュリティ要件のより良い理解を促進するためのものであり、要件の範囲を拡大するためのものではない。

[21] 一貫性、透明性、および両立性を促進するために、各組織が代替的セキュリティ手段を選択する場合には、たとえば[ISO 27001] や [SP 800-53]などを含め、*承認済の既存*のセキュリティ規格や管理策のセットを基にあるいはそれらから導出されたものである。

る。[22]要求があった場合、システムセキュリティ計画書（またはその抜粋）および計画された実装または軽減策に関する実施計画書は、非連邦政府組織のセキュリティ要件の実装または計画された実装を実証するために、責任のある連邦政府機関／契約担当官に提出される。連邦政府機関は、提出されたシステムセキュリティ計画書と実施計画書について、非連邦政府組織によって運用されるシステム上の CUI を処理、保存、または伝送する上で、および非連邦政府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といったリスク管理上の意思決定への重要な入力情報として検討することになる。

本出版物の推奨セキュリティ要件は、CUI を処理、保存、または伝送する、またはそのようなコンポーネントを保護する非連邦政府組織のシステムのコンポーネントのみに適用されるものである。特化したシステム(例、産業／プロセス制御システム、医療機器、コンピュータ数値制御マシンなど)を含む、一部のシステムでは特定のセキュリティ要件について適用が限定される場合がある。

このような課題に対応するため、システムセキュリティ計画書は、要件 3.12.4 に反映されるものとして、セキュリティ要件への例外事項を記述するために使用される。個別の、独立した、あるいは一時的な不充足要件は、要件3.12.2 で反映されるものとして、実施計画書により管理される。

「組織のシステム（organizational systems）」の意味

*組織のシステム*という用語は、本文書における推奨CUIセキュリティ要件の多くで使用されている。この用語は、当該セキュリティ要件の適用範囲に関する特定の意味を持っている。本要件は、CUIを処理、保存、または伝送する非連邦政府システムのコンポーネント、またはそ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コンポーネントにのみ適用されるものである。セキュリティ要件の適用に関して適切な範囲を見極めること（scoping）は、CUIの保全責任を持つ非連邦政府組織において保護関連の投資判断を決定し、セキュリティリスクを管理する上で重要な要素である。

3.1 アクセス管理

基本セキュリティ要件

3.1.1 システムへのアクセスは、認可されたユーザー、認可されたユーザーに代わって動作するプロセスおよび（その他のシステムを含む）デバイスに限定する。

詳解

アクセス管理ポリシー（たとえば、アイデンティティまたは役割ベースのポリシー、制御マトリックス、暗号化など）は、能動的なエンティティまたはサブジェクト（すなわち、ユーザーまたはユーザーに代わって動作するプロセス）と受動的なエンティティまたはサブジェクト（たとえば、デバイス、ファイル、レコード、ドメインなど）との間におけるシステム内のアクセスを管理するものである。アクセス管理の実施メカニズムは、更なる情報セキュリティを提供するために、アプリケーションレベルおよびサービスレベルで採用することができる。その他のシステムには、組織内部のシステムと外部のシステムが含まれる。このセキュリティ要件は、システムとアプリケーションの両方のアカウント管理に焦点を当てている。アカウントのタイプ（たとえば、特権や非特権など）によって決定されるアクセス認可以外のアクセス認可の規定および実施は 3.1.2 で扱われる。

[22] [NIST CUI]は、システムセセキュリティ計画書と実施計画書のテンプレートを含む SP 800-171 の補足資料を提供する。

3.1.2 システムへのアクセスは、認可されたユーザーが実行を許可されているタイプのトランザクションおよび機能に限定する。

詳解

組織は、アクセス特権やその他の属性を、アカウント、アカウントのタイプ、またはそれらの組み合わせによって規定してよい。システムアカウントのタイプには、個人アカウント、共有アカウント、グループアカウント、システムアカウント、ゲスト、匿名アカウント、非常時アカウント、開発者、製造者、ベンダーアカウント、仮アカウントなどが含まれる。アクセスを許可する際に求められるその他の属性には、時間帯、曜日、発信場所に対する制限がある。組織はその他の属性を規定する際、システムに関連する要件（たとえば、システムアップグレード、定期メンテナンスなど）およびミッションや事業に関連する要件（たとえば、時差、顧客からの要求、移動（旅行）に関する要件をサポートするリモートアクセスなど）について考慮する。

派生セキュリティ要件

3.1.3 承認された認可に従って、CUI のフロー（flow）を管理する。

詳解

情報フロー管理は、情報がシステム内およびシステム間を移動（travel）できる場所（情報にアクセスできる者ではなく）を、その情報への後続のアクセスを明示的に考慮せず制御する。情報フロー管理の規制には以下が含まれる：(1) エクスポートが制限されている情報を平文でインターネットに移動できないようにすること；(2) 組織内からのトラフィックであると主張する外部からのトラフィックをブロックすること；(3) 内部の web プロキシサーバーからではないインターネットへのリクエストを禁止すること；ならびに、(4) データ構造およびコンテンツに基づいて組織間での情報転送を限定すること。

組織は通常、情報フロー管理ポリシーと実施メカニズムを使用して、システム内および相互接続されたシステム間の指定された送信元と宛先（ネットワーク、個人、デバイスなど）間の情報のフローを管理する。フローの管理は、情報または情報パスの特性に基づいている。ルールセットを使用する、またはシステムサービスを制限する構成設定を確立する境界保護デバイス（ゲートウェイ、ルータ、ガード、暗号化トンネル、ファイアウォールなど）で実施され、ヘッダー情報に基づくパケットフィルタリングケイパビリティ（機能、能力）またはメッセージコンテンツに基づくメッセージフィルタリングケイパビリティ（キーワード検索の実装やドキュメント特性の使用など）を提供する。組織は、情報フローの実施に重要なフィルタリングおよび検査メカニズム（ハードウェア、ファームウェア、ソフトウェアコンポーネントなど）の信頼性も考慮する。

異なるセキュリティポリシーを持つ異なるセキュリティドメインを表すシステム間で情報を伝送すると、そのような伝送が一つ以上のドメインセキュリティポリシーに違反するリスクが生ずる。このような状況では、情報のオーナーまたは管理者（stewards）は、相互接続されたシステム間の指定されたポリシー実施ポイントでガイダンスを提供する。組織は、特定のセキュリティポリシーを適用する必要がある場合は、特定のアーキテクチャソリューションの義務化を検討する。実施には以下が含まれる：(1)相互接続されたシステム間の情報転送を禁止する（つまり、アクセスのみを許可する）；(2)ハードウェアメカニズムを使用して一方向の情報フローを実施する；(3)セキュリティ属性とセキュリティラベルを再割り当てするための統合的信頼性のある再格付け（regrading）メカニズムの実装。

3.1.4 共謀が関与しない場合の有害行為のリスクを減らすため、個人の職務を分離する。

詳解

職務の分離は、認可された特権が悪用される可能性に対処し、共謀が関与しない場合の有害行為のリスクを減らすために役立つ。職務の分離には (1) ミッション関連の機能とシステムサポート関連の機能を異なる個人や役割に割り当てること；(2) 異なる個人がシステムサポートの機能（たとえば、構成管理、品質保証および品質試験、システム管理、プログラミング、おおびネットワークセキュリティなど）を実施すること；および(3) アクセス管理機能を管理するセキュリティ担当者が監

査機能の管理も行わないようにすること、などが含まれる。職務の分離に対する違反は、システムやアプリケーションドメインにまで及ぶ恐れがあるため、職務の分離に関するポリシーを策定する際、組織は、組織のシステムとシステムコンポーネントを全体的に検討する。

3.1.5 特定のセキュリティ機能および特権アカウントを含め、最小特権の原則を採用する。

詳解

組織は、ユーザーおよびプロセスの特定の職務およびアクセス認可に対して、最小特権の原則を採用する。最小特権の原則は、組織の必要なミッションを達成するために、または業務上の機能を果たすために必要な最小限の認可を付与することを目標として適用される。組織は、最小特権を実現するために、必要に応じて、追加のプロセス、役割、およびシステムアカウントを作成することを検討する。また、組織は、組織のシステムの開発、実装、および運用にも最小特権の原則を適用する。セキュリティ機能には、システムアカウントの作成、ログ取得されるイベントの設定、侵入検知パラメータの設定、アクセス認可（許可または特権）の設定などが含まれる。

スーパーユーザーアカウントを含め、特権アカウントとは、市販の様々なタイプのオペレーティングシステムにおいてシステムアドミニストレーターと通常呼ばれるアカウントである。特権アカウントを特定の職員または役割に制限することで、日常業務担当のユーザーが特権的な情報や機能にアクセスすることを防止する。組織は、この要件を適用するにあたって、組織が重要なセキュリティパラメータのシステム構成を管理する能力を保持し、且つ、リスクを十分に軽減できる場合に限り、ローカルアカウントとドメインアカウントの特権を区別してもよい。

3.1.6 非セキュリティ機能にアクセスする時には、非特権アカウントまたは役割を使用する。

詳解

この要件は、特権アカウントまたは役割で操作する際の情報漏えいを限定するものである。役割をセキュリティ要件の対象に含めたことによって、組織が役割ベースのアクセス管理などのアクセス管理ポリシーを実装する場合や、役割の変更が、特権アカウントと非特権アカウント間の変更によってもたらされる保証と同等の保証を、ユーザーおよびユーザーに代わって動作するプロセスのアクセス認可を変更する際に提供する場合も、このセキュリティ要件が適用される。

3.1.7 非特権ユーザーが特権機能を実行することを防止し、そのような機能の実行を監査ログに取り込む（capture）。

詳解

特権機能には、システムアカウントの作成、システムの完全性チェックの実施、パッチ適用操作の実行、暗号鍵の管理活動の管理、などが含まれる。非特権ユーザーとは、適切な認可を持たない個人のことを指す。非特権ユーザーからの保護が必要な特権機能の例には、侵入検知および防止メカニズムを回避することや、悪意のあるコードからの保護メカニズムを回避することなどがあげられる。なお、このセキュリティ要件は、3.1.2.で規定される特権によって実現される状態を示している。

認可されたユーザーによる意図的なまたは意図しない特権機能の誤用、または危殆化されたシステムアカウントを持つ外部の認可されてないエンティティによる特権機能の誤用は、常に深刻な懸念であり、組織に著しい有害なインパクトを及ぼしかねない。特権機能の使用をログ取得することは、そうした誤用を検知する 1 つの方法でもあり、インサイダー脅威および持続的標的型攻撃（APT 攻撃）からのリスクを軽減するのに役立つ。

3.1.8 ログオン試行失敗回数を限定する。

詳解

このセキュリティ要件は、ログオンがローカル接続であるかネットワーク接続を介しているかを問わず適用される。サービスの拒否の可能性があることから、多くの場合、システムが行う自動ロックアウトは一時的なものであり、組織が設定した所定の期間の後に自動で解除される（遅延アルゴリズム）。遅延アルゴリズムが選択された場合、組織は、各コンポーネントのケイパビリティに基づいて、異なるシステムコンポーネントごとに別のアルゴリズムを採用してもよい。ログオン試行の

失敗に対する対応は、オペレーティングシステムレベルおよびアプリケーションレベルで実装してもよい。

3.1.9 適用される CUI のルールに則って、プライバシーおよびセキュリティ通知を提示する。

詳解

システム利用通知は、個人が組織のシステムにログインする前に表示されるメッセージや警告バナーを使用して実装することができる。システム利用通知は、人間のユーザーがログオンインタフェースを介してアクセスする場合にのみ使用され、人によるインタフェースを介したアクセスがない場合は必要ない。組織は、ネットワークに最初にログオンした後、アプリケーションやシステムのその他の資源にアクセスする際に、第２のシステム利用通知が必要か否かを、リスク対応状況のアセスメントに基づいて検討する。第２のシステム利用通知が必要な場合、システムの自動バナーの代わりにポスターまたはその他の印刷物を使用してもよい。組織は警告バナーの内容に関して法務部門と協議し、法制度面の審査と承認を得る。

3.1.10 非アクティブ状態が一定時間経過後のデータのアクセスおよび閲覧を防止するために、隠蔽用パターンの表示によるセションロックを使用する。

詳解

セションロックは、ユーザーが作業を中断してシステム近傍から離れる際、退席が一時的なものであることからログアウトすることを望まない場合に取られる一時的なアクションである。セションロックは、通常、オペレーティングシステムのレベルで（ただし、アプリケーションレベルでも）セションアクティビティを決定できる場所に実装される。セションロックは、たとえば、組織がユーザーに対して１日の終わりにログアウトすることを要求する場合などは、システムログアウトの代わりとして認められない。

隠蔽用パターンの表示には静的または動的な画像が含まれ、たとえば、スクリーンセーバ、真画像、無地、時計、バッテリー残量表示、またはブランクスクリーンなどがある。また、これらの何れの画像も CUI を含まないという注意警告を、追加で表示する。

3.1.11 規定された条件が成立した場合には、ユーザーセションを（自動的に）終了させる。

詳解

このセキュリティ要件は、通信セションに関連するネットワーク接続の終了（ネットワークからの切断）についてではなく、ユーザーが開始した論理セションの終了について取り扱う。（ローカルアクセス、ネットワークアクセス、およびリモートアクセスの）論理セションは、ユーザー（またはユーザーに代わって動作するプロセス）が組織のシステムにアクセスすると開始される。そうしたユーザーセションは、ネットワークセションを切断することなく終了させることができる（よって、ユーザーのアクセスを終了させる）。セションの終了によって、ユーザーの論理セションに関連するすべてのプロセスが終了する。ただし、ユーザー（すなわち、セションのオーナー）が、セションの終了後も継続するように特別に作成したプロセスは除外される。セションの自動終了を要する条件または引き起こすイベントには、組織が規定したユーザーの非アクティブな時間、特定のタイプのインシデントに対象を絞った対応、および時間帯によるシステム利用の制限などがある。

3.1.12 リモートアクセスセションを監視し、管理する。

詳解

リモートアクセスとは、ユーザー（またはユーザーに代わって動作するプロセス）が外部ネットワーク（たとえば、インターネット）を経由して組織のシステムに通信するアクセスである。リモートアクセスには、ダイアルアップ、ブロードバンド、ワイヤレスなどが含まれる。組織は、多くの場合、暗号化した仮想プライベートネットワーク（VPN）を採用して、リモート接続に対する秘匿性を強化する。暗号化した VPN の使用によってアクセスが非リモートになるわけではないが、適切な管理策を設けて（たとえば、秘匿性保護のために暗号技法を導入して）VPN を使用した場合、組織がそうした接続を事実上内部ネットワークとして扱うことができるほどの十分な保証が提供され

る。暗号化トンネルを備えた VPN は、悪意のあるコード検知のためにネットワーク通信トラフィックを監視するケイパビリティに影響を及ぼす。

リモートアクセスセションの自動監視および管理機能は、さまざまなシステムコンポーネント（たとえば、サーバー、ワークステーション、ノートパソコン、スマートフォン、タブレットなど）に対するリモートユーザーの接続行為を監査することによって、組織におけるサイバー攻撃の検知を可能にし、リモートアクセスに関するポリシーに継続的に準拠することができるようにする。

[SP 800-46]、[SP 800-77]、および [SP 800-113] は、セキュアなリモートアクセスおよび仮想プライベートネットワークに関するガイダンスを提供する。

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

詳解

暗号技術の規格には、FIPS 認証暗号技術と NSA 承認暗号技術が含まれる。

参照：[NIST CRYPT]、[NIST CAVP]、[NIST CMVP]、NSA 暗号規格。

3.1.14 管理されたアクセス制御ポイント経由でリモートアクセスをルーティングする。

詳解

管理された（managed）アクセス制御ポイント経由でリモートアクセスをルーティングすることにより、リモートアクセス接続に対する明確な組織の管理が強化され、CUI の認可されてない開示を誘発するような、組織のシステムへの認可されてないアクセスを受けにくくする。

3.1.15 特権コマンドのリモート実行およびセキュリティ関連情報へのリモートアクセスを認可する。

詳解

特権コマンドとは、人為的な（対話式なまたは人の代理として動作するプロセスを介した）コマンドであり、セキュリティ機能および関連するセキュリティ関連情報を含むシステムの制御、監視、または管理（administration）に関与するシステムに対して実行される。セキュリティ関連情報とは、システムのセキュリティポリシーが実施されない、またはコードとデータの分離が維持されないといった状況を引き起こすような形で、セキュリティ機能の動作またはセキュリティサービスの提供にインパクトを与える可能性のあるシステム内のあらゆる情報のことを指す。特権コマンドにより、個人は、要注意（sensitive）システム機能、セキュリティが重要な（security-critical）システム機能、またはセキュリティ関連のシステム機能を実行することができる。リモートからのそうしたアクセスを管理することにより、認可されてない個人が、組織のシステムに対して深刻なまたは壊滅的な被害を及ぼしかねない特権コマンドを自由に実行できないようにする。なお、システムの完全性に影響を及ぼすことができる場合、セキュリティ機能自体に直接インパクトを及ぼさないにしても、セキュリティ機能を迂回する手段を可能にするため、セキュリティ関連としてみなされる。

3.1.16 ワイヤレスアクセスの接続を許可する前に、そうしたアクセスを認可する。

詳解

システムへのワイヤレスアクセスの使用に関する制限および設定／接続要件を定めることにより、組織がワイヤレスアクセスの許可に関する意思決定を行う際に決定の根拠となる基準が提供される。そうした制限および要件によって、システムは認可されてないアクセスを受けにくくなる。ワイヤレスネットワークは、クレデンシャルの保護および相互認証を提供する認証プロトコルを使用する。

[SP 800-97] は、セキュアなワイヤレスネットワークに関するガイダンスを提供する

3.1.17 認証および暗号を使用してワイヤレスアクセスを保護する。

詳解

組織は、個人およびデバイスを認証して、システムに対するワイヤレスアクセスを保護する。特に、組織のシステムにワイヤレスでアクセスする可能性のある IoT の一部である様々なデバイスに注意する。

参照：[NIST CRYPTO]。

3.1.18 モバイルデバイスの接続を管理する。

詳解

モバイルデバイスとは、(1) 1 人の個人が簡単に持ち運べる小型のフォームファクタ（物理的な規格）を有し；(2) 物理的な接続なしで動作する（たとえば、ワイヤレスで情報の送受信を行う）ように設計され；(3) 非リムーバブルまたはリムーバブルなローカルデータストレージを有し；かつ、(4) 電源を内蔵している、コンピューティングデバイスのことである。モバイルデバイスには、音声通信ケイパビリティ、モバイルデバイスが情報を取り込むための内臓センサー、またはローカルデータを 離れた所にあるものと同期させる組み込み特性が含まれることがある。モバイルデバイスは、たとえばスマートフォン、電子書籍リーダー、タブレットなどである。

異なる技術的特性およびケイパビリティを備える様々なモバイルデバイスが存在するため、異なるタイプのデバイスごとに組織の制限を変更してもよい。モバイルデバイスの使用に対する制限および実装に関するガイダンスには：(1) デバイスの識別および認証、構成管理、必須の保護ソフトウェアの実装（たとえば悪意のあるコードの検知やファイアウォールなど）；(2) 悪意のあるコードをスキャンするデバイス；(3)ウイルス対策ソフトウェアの更新の実施；(4) 重要なソフトウェアの更新スキャン、パッチ検出のためのスキャンの実施；(5) 主要オペレーティングシステム（および常駐ソフトウェアと考えられるもの）の完全性チェックの実施；ならびに(6)不必要なハードウェア（たとえば、無線ハードウェアや赤外線ハードウェアなど）の無効化などが含まれる。モバイルデバイスに適切なセキュリティを設けることは、本セキュリティ要件の対象外であり、モバイルデバイスのための管理策は、CUI に関するその他のセキュリティ要件に反映されている。

[SP 800-124] は、モバイルデバイスのセキュリティに関するガイダンスを提供する。

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[23]上の CUI を暗号化する。

詳解

組織は、モバイルデバイスおよびコンピューティングプラットフォーム上の CUI の秘匿性を保護するために、デバイス全体の暗号化またはコンテナベースの暗号化を採用することができる。コンテナベースの暗号化は、データや情報をより細かく暗号化し、ファイル、レコード、フィールドなどのデータ構造を選択して暗号化することができる。

参照：[NIST CRYPTO]。

3.1.20 外部システムへの接続および使用を検証（verify）し、管理／限定する。

詳解

外部システムとは、セキュリティ要件およびセキュリティ管理策の適用に関して、またはシステムやシステムコンポーネントで実装される管理策の有効性の判定に関して、組織が直接管理できない、また、直接の認可を持たないシステムやシステムのコンポーネントである。外部システムには、個人が所有するシステム、コンポーネント、またはデバイスに加え、商業または公共施設に置かれる民有のコンピューティングデバイスおよび通信デバイスなどが含まれる。このセキュリティ

[23] 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には、たとえば、スマートフォン、タブレットを含む。

要件は、組織のシステムからのクラウドサービス（たとえば、IaaS、PaaS、SaaS など）へのアクセスを含め、CUI を処理、保存、または伝送する外部システムの使用も対象とする。

組織は、セキュリティポリシーおよびセキュリティ手順に則り、外部システムの使用に関する条件を定める。条件としては、少なくとも外部システムから組織のシステムにアクセスできるアプリケーションのタイプを定める。外部システムのオーナーと条件を定めることができない場合は、組織は、外部システムを使用する組織の職員に対して制限を設けることがある。

このセキュリティ要件は、外部システムを使用する個人（たとえば契約事業者や提携パートナーなど）が組織のシステムにアクセスしなければならない場合があることを踏まえている。そのような状況において、組織のシステムが危殆化しないように、被害を与えないように、またはその他の方法で害を及ぼさないように、外部システムが必要な管理策を備えていることを、組織は確証する必要がある。必要な管理策が効果的に実装されているかは、組織が求める保証水準または信頼水準に応じて、サードパーティの独立した対応状況のアセスメント、証明、またはその他の手段によって検証することができる。

なお、「外部」とは通常、組織が直接管理できない場合、および、権限のない場合を指すが、必ずしもこの限りではない。組織全体における CUI の保護に関して、組織のシステムには CUI を処理するシステムと、処理しないシステムとがあり得る。CUI を処理するシステムでは、CUI に対するアクセス制限が設けられることがあり、この制限はシステム間で適用される。よって、所与のシステムからすると、組織内のその他のシステムは「外部」とみなされる。

3.1.21 外部システム上でのポータブルストレージデバイスの使用を限定する。

詳解

組織が管理するポータブルストレージデバイスを外部システムで使用する際の限定には、そうしたデバイスの使用を全面的に禁止することや、そうしたデバイスの使用方法と使用条件を制限することなどが含まれる。なお、「外部」とは通常、組織が直接管理できない、また、権限のない場合を指すが、必ずしもこの限りではない。組織全体における CUI の保護に関して、組織のシステムには CUI を処理するシステムと、処理しないシステムとがあり得る。CUI を処理するシステムの中には、システム間で適用される CUI のアクセス制限が設けられる可能性がある。よって、所与のシステムからすると、組織内のその他のシステムは「外部」とみなされる。

3.1.22 公衆アクセス可能なシステム上に掲載または処理される CUI を管理する。

詳解

法律、大統領令、指令、方針、規定、または規格により、一般人は、非公開情報（たとえば、プライバシー保護法の下で保護されている情報、CUI、機密情報など）へのアクセスは認可されてない。本セキュリティ要件は、識別または認証なしで一般人が通常アクセスできる組織によって管理されているシステムについて取り扱う。情報を公衆アクセス可能なシステムに掲載する前に、非公開情報が含まれていないかその中身が確認される。

3.2 意識向上および訓練

基本セキュリティ要件

3.2.1 組織のシステムの管理者（managers）、システムアドミニストレーターおよびユーザーが、組織のシステムのセキュリティに関連する適用ポリシー、規格、および手順ならびに彼らの活動に関連するセキュリティリスクについて認識していることを確実にする。

詳解

組織は、組織の具体的な要件および職員がアクセスを認可されているシステムに基づいて、セキュリティ意識向上および訓練の内容および頻度を決定するとともに、セキュリティ意識向上の技法を決定する。訓練には、情報セキュリティの必要性に加え、セキュリティを維持し、疑われるセキュリティインシデントに対応するユーザーの措置について、基本的な理解を深める内容が含まれる。また、運用上のセキュリティの必要性についても意識向上させる。セキュリティ意識向上の技法に

ついては、(1) 正式な訓練の実施；(2) セキュリティの注意喚起が記されたグッズの提供；(3) 組織の担当者からの電子メールによる勧告や通知；(4) ログオン画面におけるメッセージの表示；(5) セキュリティ意識向上に関するポスターの掲示；および (6) 情報セキュリティ意識向上イベントの実施などが含まれる。

[SP 800-50] は、セキュリティ意識向上および訓練プログラムに関するガイダンスを提供する。

3.2.2 職員が、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ように訓練されていることを確実にする。

詳解

組織は、個人に割り当てられた職務、役割、責任とともに、組織のセキュリティ要件および職員がアクセス認可されているシステムに基づいて、セキュリティ意識向上訓練の内容と頻度を決定する。さらに、組織は、システム開発者、エンタープライズアーキテクト、セキュリティアーキテクト、購買／調達部門担当者、ソフトウェア開発者、システム開発者、システムインテグレータ、システムネットワークアドミニストレーター、ネットワークアドミニストレーター、構成管理および監査活動を行う職員、独立した検証と確認を行う職員、セキュリティアセスメントならびにシステムレベルのソフトウェアにアクセスできるその他の職員に対して、各々の割り当てられた職務に特別に合わせたセキュリティ関連技術に関する訓練を提供する。

包括的な役割ベースの訓練は、管理面、運用面、技術面の役割ならびに物理的、人的、技術的な管理策を網羅する責任について取り扱う。役割ベースの訓練には、たとえば、セキュリティに関連して規定された役割のための、ポリシー、手順、ツールおよび成果物などを含むことができる。また、組織の情報セキュリティプログラムという面においては、個人が運用面およびサプライチェーンのセキュリティに関連した各自の役割を果たすことができるよう、必要な研修が提供される。

[SP 800-181] は、職場での役割ベースの情報セキュリティ研修に関するガイダンスを提供する。また,[SP 800-161]は、サプライチェーンのリスクマネジメントに関するガイダンスを提供する。

派生セキュリティ要件

3.2.3 インサイダー脅威の潜在的兆候を認識し、報告するためのセキュリティ意識向上訓練を行う。

詳解

インサイダー脅威の潜在的兆候および予想される前兆には：(1) 長期にわたる仕事への多大な不満；(2)業務の遂行に不必要な情報へのアクセスの試行；(3) 金融資産の無断使用；(4) 同僚に対するいじめやセクシュアルハラスメント；(5) 職場内暴力；および (6) 組織のポリシー、手順、指示、ルール、プラクティス（対応する業務）に対する重大な違反、などの行動が含まれる。セキュリティ意識向上訓練では、インサイダー脅威の潜在的兆候に関する懸念について、一般職員と管理職員が、いかに組織の定められたポリシーおよび手順に従い適切な手段を通じて情報交換を行うかを取り上げる。組織は、インサイダー脅威に対する意識向上について、役割に合わせてトピックを変更してよい（たとえば、管理者を対象とした訓練では、チームメンバーの行動における特別な変化を重視する一方、従業員を対象とした訓練では、より一般的な概説に重点を置く）。

3.3 監査および説明責任

基本セキュリティ要件

3.3.1 非合法的または認可されてないシステム行為に関する監視、分析、調査、報告を可能にするために必要な範囲で、システム監査ログおよび記録を作成し保持する。

詳解

イベントとは、非合法的または認可されてないシステム行為を含め、システム内で発生する観察可能なあらゆる行為を指す。組織は、ログ取得機能が必要なイベントタイプを、システムのセキュ

リティおよび特定の継続的監査ニーズに対応するためにそれらのシステムの運用環境に関係する重要なイベントとして識別する。イベントタイプには、パスワードの変更、システムへのログオンやアクセスの失敗、管理者特権の使用、またはサードパーティのクレデンシャルの使用などがある。ログ取得されるイベントタイプを決定するうえで組織は、各 CUI セキュリティ要件に適切な監視および監査を検討する。監視および監査の要件と、システムのその他の必要事項とはバランスを取ることができる。たとえば、組織は、ファイルへのアクセスが成功／失敗したかに関わらずすべてのアクセスをログ取得するケイパビリティ（機能、能力）をシステムに求める一方で、このようなケイパビリティは、システム性能に負担をかける可能性があることから、特定の状況以外は有効化しないようにする場合がある。

監査記録は、情報がネットワークを通過する際のパケットレベルを含め、さまざまな抽象レベルで生成することができる。適切な抽象レベルを選択することは、監査ログ取得ケイパビリティの重要な側面であり、問題の根本原因の特定を促進する。組織は、イベントタイプを規定する際、トランザクションベースの分散しているプロセス（たとえば、複数の組織にわたって分散されているプロセスなど）のステップおよびサービス指向アーキテクチャーまたはクラウドベースのアーキテクチャーで発生するアクションなど、関連するイベントを網羅するために必要なログ取得を検討する。

このセキュリティ要件を満たすために必要な監査記録の内容には、タイムスタンプ、送信元アドレス、送信先アドレス、ユーザーまたはプロセス ID、イベントの説明、成功または失敗判定、関連ファイル名、および、実施されるアクセス管理規則または情報の一連の取り扱い手続の管理ルールなどが含まれる。イベントの結果には、イベントの成功または失敗の表示およびイベント固有の結果（たとえば、イベント発生後におけるシステムのセキュリティ状態）を含むことができる。

組織が監査記録において検討する詳細な情報には、特権コマンドの全テキスト、グループアカウントユーザーの個人 ID などがある。組織は、追加の監査ログ情報を、特定の監査要件を満たすために明らかに必要な情報のみに限定することを検討する。情報を限定することで、誤解を招く恐れのある情報や知りたい情報の検索をより困難にしかねない情報は除かれ、監査証跡および監査ログの使用を容易にする。監査ログは、組織のリスクベースの意思決定を促進する重要な情報を提供するために、必要に応じて幾度も見直され分析される。

[SP 800-92] は、セキュリティログの管理に関するガイダンスを提供する。

3.3.2 個々のシステムユーザーの行動が、そのユーザーに対して一意に追跡可能であり、ユーザーが自らの行動に説明責任を負わせられるようにする。

詳解

このセキュリティ要件は、監査イベントと個人の行動を可能な範囲で結び付けるために必要な情報が、監査記録の内容に含まれるようにすることを目標とする。この追跡可能性（traceability）のために、組織がログ取得を検討する対象には、アカウント利用の監視結果、リモートアクセス、ワイヤレス接続、モバイルデバイスの接続、構成設定、システム境界における通信、メンテナンスツールの使用、非ローカルメンテナンス、温度と湿度、装置の搬入および撤去、システムコンポーネントのインベントリ（inventory）、モバイルコードの使用、ならびにインターネット音声通話（VoIP）の使用などが含まれる。

派生セキュリティ要件

3.3.3 ログ取得されたイベントを見直し、更新する。

詳解

このセキュリティ要件は、ログ取得されたイベントのうち、何れのイベントを継続的に一覧に含めるかを定期的に見直すことを目標とする。組織によりログ取得されたイベントのタイプは、時間の経過と共に変化することがある。ログ取得されたイベントのタイプ一式を見直し、更新することによって、必要かつ十分な最新の一式が維持される。

3.3.4 監査ログ取得プロセスが失敗した場合にアラートを発する。

詳解

監査ログ取得プロセスの失敗には、ソフトウェアおよびハードウェアエラー、監査記録収集メカニズムの不具合とともに、監査記録のストレージ容量が上限に達するか、または上限を超えることなどがあげられる。このセキュリティ要件は、監査記録データを保存する各リポジトリ（すなわち、監査記録が保存される別個のシステムコンポーネント）、監査記録の全データを保存する組織のストレージ容量（すなわち、監査記録データを保存するすべてのリポジトリの合計）およびこれらの両方に適用される。

3.3.5 非合法的、認可されてない、疑わしい、または異常な行為の兆候を調査し対応するために、監査記録の見直し、分析および報告のプロセスを相互に関連づける。

詳解

監査記録のレビュー、分析、およびレポート作成プロセスを相互に関連付けることによって、これらが独立して動作するのではなく集合的に動作するようになる。組織のシステムのアセスメントにあたり、このセキュリティ要件は、相互の関連付けがシステムレベルで適用されているか、またはシステムすべてにわたり組織レベルで適用されているかに左右されない。

3.3.6 オンデマンドでの分析および報告をサポートするための監査記録の集約および報告書生成機能を提供する。

詳解

監査記録の集約とは、収集した監査情報を操作して、そうした情報を分析者にとってより意味のあるものにするために要約形式にまとめるプロセスである。監査記録の集約および報告書の生成ケイパビリティは、必ずしも監査活動を実施する同じシステムまたは組織のエンティティから生じるとは限らない。たとえば、監査記録の中から異常な行動を割り出す高度なデータフィルターを備えた最新のデータマイニング技法を、監査記録の集約ケイパビリティに含むことができる。システムが提供する報告書の生成ケイパビリティは、カスタマイズ可能な報告書を作成することができる。監査記録のタイムスタンプの粒度が十分でない場合は、監査記録の時系列が重要な問題となる可能性がある。

3.3.7 監査記録にタイムスタンプを生成するために、内部システムクロックを信頼できるタイムソース（時刻提供者）と比較および同期させるシステムケイパビリティを提供する。

詳解

内部システムクロックはタイムスタンプを生成するために使用され、日付と時刻が含まれる。時刻は、GMT（グリニッジ平均時）を継承したUTC（協定世界時）で表示される、または現地時刻がUTCからの時差付きで表示される。時間単位の粒度は、システムクロックと基準クロックが、たとえば、数百ミリ秒または数十ミリ秒以内で同期しているなど、同期の程度を表す。組織は、システムコンポーネントごとに異なる時間の粒度を定めることができる。アクセス管理と識別および認証などその他のセキュリティケイパビリティをサポートするメカニズムの性質によっては、タイムスタンプのサービスは、それらのケイパビリティにとっても重要な場合がある。このセキュリティ要件は、複数のシステムクロックを有するシステムおよびネットワークを介して接続されるシステムのために、タイムスタンプの一貫性を確保する。

参照：[IETF5905]。

3.3.8 監査情報および監査ログ取得ツールを、認可されてないアクセス、変更、および削除から保護する。

詳解

監査情報には、システム活動を適切に監査するために必要なすべての情報（たとえば、監査記録、監査ログ設定、監査報告書など）が含まれる。監査ログ取得ツールとは、監査活動および監査ログ取得活動を実行するうえで使用されるプログラムおよびデバイスのことである。このセキュリティ要件は、監査情報の技術的な保護を対象とし、監査ログ取得ツールにアクセスし実行できる個人を

認可された個人に限定する。監査情報の物理的な保護については、媒体保護に関する要件ならびに物理的および環境保護に関する要件で取り扱われる。

3.3.9 監査ログ取得機能の管理を特権ユーザーの一部の者に限定する。

詳解

システムへの特権アクセスを持つ個人が、そのシステムにおける監査の対象である場合、監査ログ取得活動の妨害または監査記録の改ざんによって監査情報の信頼性に影響を及ぼす場合がある。このセキュリティ要件は、特権アクセスをさらに監査関連の特権とその他の特権とに分けるように定め、監査関連の特権を持つユーザーを限定する。

3.4 構成管理

基本セキュリティ要件

3.4.1 個々のシステム開発ライフサイクル全体にわたり、組織が持つシステムの基本構成およびインベントリ（ハードウェア、ソフトウェア、ファームウェアおよび文書を含む）を規定し、維持する。

詳解

基本構成とは、システムまたはそのシステムの構成品目に関する正式に審査、および合意され文書化された仕様のことを指す。基本構成は、システムの将来的な開発、リリース、および変更の基盤となる。基本構成には、(1)システムコンポーネントに関する情報（たとえば、ワークステーション、ノートパソコン、サーバー、ネットワークコンポーネント、またはモバイルデバイスにインストールされている標準ソフトウェアパッケージ；(2)オペレーティングシステムとアプリケーションの現在のバージョン番号と更新およびパッチ情報；および(3)構成設定と構成パラメータなど)、ネットワークの接続形態、およびシステムアーキテクチャーにおけるシステムコンポーネントの論理的配置、が含まれる。システムの基本構成は、現在のエンタープライズアーキテクチャーを反映したものである。時間の経過と共に組織のシステムは変更されるため、効果的な基本構成を維持するには、新たに基本要素を規定する必要がある。基本構成の維持には、変更が生じた際、セキュリティリスクおよび規定した基本構成からの逸脱に基づき基本構成を見直し更新することが含まれる。

組織は、組織の複数のシステムのコンポーネントを集約したシステムコンポーネントの総合目録を導入することができる。そうした場合、組織は、コンポーネントの適切な説明責任を確保するために必要なシステム特有の情報（たとえばシステムの関連性やシステムオーナーなど）が、作成された目録に必ず含まれているようにする。システムコンポーネントの効果的な説明責任に必要とされる情報には、ハードウェア目録の詳細、ソフトウェアライセンス情報、ソフトウェアのバージョン番号、コンポーネントオーナー、ネットワークコンポーネント、また、ネットワークデバイスの場合はマシン名とネットワークアドレスなどがある。目録の詳細には、製造者、デバイスのタイプ、型式、シリアル番号、および物理的位置が含まれる。

[SP 800-128]は、セキュリティを重視した構成管理に関するガイダンスを提供する。

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規定し、実施する。

詳解

構成設定は、システムのハードウェア、ソフトフェア、またはファームウェアコンポーネントにおいて変更可能なパラメータの一式であり、システムのセキュリティ態勢または機能性に影響する。セキュリティに関連する構成設定を規定できる情報技術製品には、メインフレームコンピュータ、サーバー、ワークステーション、入出力デバイス（たとえば、スキャナー、コピー機、プリンターなど)、ネットワークコンポーネント（たとえば、ファイアウォール、ルータ、ゲートウェイ、音声およびデータスイッチ、ワイヤレスアクセスポイント、ネットワーク機器、センサーなど)、オペレーティングシステム、およびアプリケーションなどがある。

セキュリティパラメータはシステムのセキュリティ状態にインパクトを与えるパラメータであり、その他のセキュリティ要件を満たすために必要なパラメータも含まれる。セキュリティパラメータには：(1) レジストリーの設定；(2) アカウントファイルディレクトリの許可設定；および(3) 機能、ポート、プロトコル、リモート接続の設定などがある。組織は、組織全体にわたる構成設定を定め、その後、システムに関する特定の構成設定を派生させる。規定した設定は、システム構成基本要素の一部となる。

共通セキュア構成（セキュリティ構成チェックリスト、ロックダウンおよび堅牢化のガイド、セキュリティリファレンスガイド、セキュリティ技術実装ガイドとも称される）は、広く認知され、標準化され、確立された基準（benchmark）を提供し、この基準は特定の情報技術プラットフォームまたは情報技術製品のセキュアな構成設定とともに、運用要件を満たすシステムコンポーネントの設定方法を示す。共通セキュア構成はさまざまな組織、情報技術製品の開発者、製造者、ベンダー、合併企業、産学官機関、およびその他の公共および民間組織などによって策定される。

[SP 800-70]、[SP 800-128] は、セキュリティ構成設定に関するガイダンスを提供する。

派生セキュリティ要件

3.4.3 組織のシステムに対する変更を追跡、見直し、承認または非承認し、ログ取得する。

詳解

変更の追跡、見直し、承認／非承認、ログ取得は、構成変更管理と呼ばれる。組織のシステムの構成変更管理には、システムアップグレートや修正を含む、システムに対する変更の体系的な提案、正当性の提示、実装、テスト、審査、破棄などを伴う。構成変更管理では、システムのコンポーネントと構成項目の基本構成の変更、情報技術製品（たとえば、オペレーティングシステム、アプリケーション、ファイアウォール、ルータ、モバイルデバイスなど）の構成設定の変更、予定外のまたは認可されていない変更、および脆弱性を改善するための変更が対象とされる。

システムの構成変更を管理するプロセスには、構成管理委員会（Configuration Control Boards）や変更諮問委員会（Change Advisory Boards）による、提案されたシステムへの変更の審査および承認が含まれる。新たに開発されたシステムや大幅にアップグレードされたシステムの場合は、組織は、開発組織の代表を構成管理委員会や変更諮問委員会に参加させることを検討する。変更に関する監査ログには、システムへの変更前後の活動および変更を実施する際必要な活動が含まれる。

[SP 800-128]は、構成変更管理に関するガイダンスを提供する。

3.4.4 変更実施に先立って、セキュリティへのインパクトを分析する。

詳解

情報セキュリティに対して責任を負う組織の職員（たとえば、システムアドミニストレーター、システムセキュリティ責任者、システムセキュリティ管理者、システムセキュリティ技術者など）は、セキュリティへインパクト分析を実施する。セキュリティインパクト分析は、システムへの変更および関連するセキュリティへのインパクトを分析するために必要なスキルと技術的専門知識を有する個人によって実施される。セキュリティインパクト分析には、セキュリティ計画書を審査して、セキュリティ要件を理解すること、およびシステム設計書を審査して、管理策の実装方法ならびに特定の変更がどのように管理策にインパクトを与えるかを理解することが含まれる。また、セキュリティインパクト分析には、変更によるインパクトをより良く理解し、追加の管理策が必要かを決定するためのリスクアセスメントも含まれる。

[SP 800-128]は、構成変更管理およびセキュリティ影響分析に関するガイダンスを提供する。

3.4.5 組織のシステム変更に関する物理的および論理的アクセス制限（restrictions）を明確に定め、文書化し、承認し、実施する。

詳解

システムのハードウェア、ソフトウェア、またはファームウェアコンポーネントへの変更は、システムのセキュリティ全般に重大な影響を与える可能性があることから、組織は、認可された適格な個人に対してのみ、アップグレードおよび修正を含む変更を実施する目的でシステムにアクセスすることを許可する。ソフトウェアライブラリへの変更も、アクセス制限の対象である。

アクセス制限には、物理的および論理的なアクセス管理に関する要件、ワークフローの自動化、メディアライブラリ、抽象化層（たとえば、変更はシステムに直接実施されるのではなく、外部インタフェースに実施される）、および変更可能時間（たとえば、変更は指定された時間内にのみ行われる）などがある。セキュリティを考慮することに加えて、アクセス制限は、構成管理を効果的に実施するうえで必須なものとして、適切な注意が払われることが一般に認識されている。

[SP 800-128] は、構成変更管理に関するガイダンスを提供する。

3.4.6 必須なケイパビリティ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り、 最小機能性の原則を採用する。

詳解

システムは様々な機能やサービスを提供することができる。初期設定で機械的に提供される機能やサービスには、組織の必須なミッション、機能、または運営を必ずしも支援しない機能やサービスも含まれている。単一のシステムコンポーネントから複数のサービスを提供することは便利な場合もあるが、そうすることによって、提供されるサービスが単一のシステムコンポーネントによるものに限定されるため、リスクが高くなる。組織は可能な限り、コンポーネントの機能性を、各コンポーネントにつき単一の機能に限定する。

組織は、システムやシステムコンポーネントが提供する機能やサービスを見直して、削除の候補に入れる機能やサービスを決定する。組織は、認可されてないデバイスの接続、情報転送、およびトンネリングを防止するため、使用していないまたは不必要な物理的および論理的ポート、およびプロトコルを無効にする。組織は、ファイアウォールやホストベースの侵入検知システムなどの、ネットワークスキャンツール、侵入検知および防止システム、およびエンドポイント保護策を活用して、禁止されている機能、ポート、プロトコルおよびサービスの使用を特定し、防止する。

3.4.7 必須でないプログラム、機能、ポート、プロトコルおよびサービスの使用を制限、無効化または防止する。

詳解

必須でないソフトウェア（プログラム）の使用制限には、(1)プログラム実行を承認できる役割の限定；(2)自動実行の禁止；(3)プログラムのブラックリスト登録とホワイトリスト登録；または(4)同時に実行されるプログラムインスタンス数に対する制限などがある。組織は、いずれの機能、ポート、プロトコル、および／またはサービスを制限するかについて、セキュリティを基に決定する。組織が使用を防止、制限、または無効化することを検討するプロトコルには、Bluetooth、ファイル転送プロトコル（FTP）、および P2P ネットワークが例としてあげられる。

3.4.8 「例外による拒否」（ブラックリスト登録）ポリシーを適用して認可されてないソフトウェアの使用を防止する、あるいは「全拒否、例外による許可」（ホワイトリスト登録）ポリシーを適用して認可されたソフトウェアの実行を許可する。

詳解

システム上で実行が許可されていないソフトウェアプログラムを識別するために使用されるプロセスは、一般にブラックリスト登録と称され、システム上で実行が許可されているソフトウェアプログラムを識別するために使用されるプロセスは、一般にホワイトリスト登録と称される。ソフトウェアプログラムの実行制限に関して、両者のポリシーのうち、ホワイトリスト登録の方がよりポリシー強度が高い。組織は、ホワイトリスト登録に加えて、たとえば、暗号チェックサム、デジタル署名、またはハッシュ関数を使用してホワイトリストに登録されたソフトウェアプログラムの完全性を検証することを検討する。

[SP 800-167] は、アプリケーションのホワイトリスト登録に関するガイダンスを提供する。

3.4.9 ユーザーがインストールしたソフトウェアを管理（control）し監視する。

詳解

ユーザーは、必要な特権を付与されている場合、組織のシステムにソフトウェアをインストールすることができる。組織は、インストールされたソフトウェアに対する管理を維持するため、ソフトウェアのインストールに関して許可される行動と禁止される行動をポリシーによって特定する。許可されるソフトウェアのインストールには、既存ソフトウェアの更新やセキュリティパッチ、および組織が承認している「app ストア」からのアプリケーションなどが含まれる。禁止されるソフトウェアのインストールには、開発過程が不明なまたは疑わしいソフトウェアや、悪意のある可能性があると組織がみなすソフトウェアなどが含まれる。ユーザーがインストールするソフトウェアを規定するポリシーにおいて、組織が選択するポリシーは、組織が策定してもよいし、もしくは外部のエンティティが提供してもよい。ポリシーの実施方法には、手続きによる方法、自動的な方法、またはこの両方が含まれる。

3.5 識別および認証

基本セキュリティ要件

3.5.1 システムのユーザー、ユーザーに代わって動作するプロセス、およびデバイスを識別する。

詳解

一般的なデバイス識別子（identifiers：以下 ID）には、MAC アドレス、IP アドレス、またはデバイスに一意のトークン ID などがある。個人の ID の管理は、共有のシステムアカウントには適用されない。個人の ID は通常、個人に割り当てられたシステムアカウントに関連するユーザー名である。組織は、グループアカウントにおいて個人の活動に対する詳細な説明責任を確保するために、個人の一意の ID を求める場合がある。更に、このセキュリティ要件は、システムアカウントには必ずしも関連していない個人の ID も対象とする。ID が必要な組織のデバイスは、タイプによって、デバイスによって、またはタイプとデバイスの組み合わせによって定めることができる。

[SP 800-63-3] は、デジタルアイデンティティに関するガイダンスを提供する。

3.5.2 組織のシステムへのアクセスを許可する前提条件として、ユーザー、プロセス、またはデバイスのアイデンティティを認証（authenticate）（または検証（verify））する。

詳解

個人のオーセンティケータ（authenticator：認証子）には、以下の、パスワード、キーカード、暗号デバイス、ワンタイムパスワードデバイスなどが含まれる。オーセンティケータの初期の内容は、たとえば、初期パスワードなどの、オーセンティケータの実際の内容である。これに対し、オーセンティケータの内容についての要件には、パスワードの最低限の長さなどがある。開発事業者は、初期インストールおよび構成設定を可能にするために、システムコンポーネントに対して工場のデフォルトの認証クレデンシャルを設定して出荷する。デフォルトの認証クレデンシャルは多くの場合、周知のため、容易に見破られ、重大なセキュリティリスクを招く。

システムは、さまざまなオーセンティケータの特性に関して組織が定めた設定および制限によって、オーセンティケータの管理をサポートする。組織が定める設定および制限には、パスワードの最低限の長さ、時刻同期方式のワンタイムトークンの検証時間、生体認証の検証時に許容される拒否回数などがある。オーセンティケータの管理では、リモートメンテナンスなどに必要な一時的アクセスのためのオーセンティケータを発行するとともに、このオーセンティケータが必要でなくなった場合に失効させることが含まれる。デバイスのオーセンティケータは、証明書やパスワードなどである。

[SP 800-63-3] は、デジタルアイデンティティに関するガイダンスを提供する。

派生セキュリティ要件

3.5.3 多要素認証[24]を特権アカウントによるローカルおよびネットワークアクセス[25]ならびに非特権アカウントによるネットワークアクセスに使用する。

詳解

多要素認証では、認証に２つ以上の異なる要素を使用する必要がある。要素は、(1) 知識情報（たとえば、パスワードや暗証番号など）；(2) 所持情報（たとえば、暗号識別デバイスやトークンなど）；および (3) 生体情報（たとえば、バイオメトリクスなど）、と定義されている。物理的なオーセンティケータを特徴とする多要素認証ソリューションには、時間ベースまたはチャレンジレスポンス方式のオーセンティケータを提供するハードウェアオーセンティケータおよびスマートカードなどがある。ユーザーをシステムレベルで（つまり、ログオン時に）認証することに加え、組織はさらなる情報セキュリティを備えるために、必要に応じて、アプリケーションレベルにおいても認証メカニズムを採用することができる。

組織のシステムへのアクセスには、ローカルアクセスまたはネットワークアクセスがある。ローカルアクセスとは、ユーザー（またはユーザーに代理わって動作するプロセス）が組織のシステムへアクセスする際、ネットワークを使用せず直接接続するようなアクセスのことを指す。一方、ネットワークアクセスとは、ユーザー（またはユーザーに代わって動作するプロセス）が組織のシステムへアクセスする際、ネットワークを使用するアクセス（すなわち、非ローカルアクセス）のことを指す。リモートアクセスは、外部ネットワークを介した通信を伴うネットワークアクセスの一つのタイプである。組織が管理するエンドポイントと組織が管理しないもののネットワーク接続のために、暗号化された仮想プライベートネットワークを使用する場合、情報の秘匿性保護の観点から、内部ネットワークとして扱われる場合がある。

[SP 800-63-3] は、デジタルアイデンティティに関するガイダンスを提供する。

3.5.4 特権および非特権アカウントによるネットワークアクセスに、リプレイ耐性のある認証メカニズムを採用する。

詳解

前回の認証メッセージの記録または再送による認証が実施できない場合、認証プロセスは、リプレイ攻撃に耐えることができる。リプレイ攻撃に耐性のある技法には、時刻同期方式またはチャレンジレスポンス方式のワンタイムオーセンティケータなどの、ナンス（number used once（一度だけ使用される使い捨ての数字）：ノンスとも言う）やチャレンジを使用するプロトコルがある。

[SP 800-63-3] は、デジタルアイデンティティに関するガイダンスを提供する。

---

[24] *多要素認証* は、認証を成就するために２つまたはそれ以上の異なる要素を必要とする。要素には以下が含まれる。すなわち、(1) 人が記憶しているもの（パスワード／PIN など）；(2) 人が所持しているもの（暗号識別デバイス、トークンなど）；あるいは (3) 人自身に存在するもの（生体認証情報）である。多要素認証のための要件が、連邦政府の「個人アイデンティティ検証」（PIV：Personal Identity Verification ）カードや、国防総省の「共通アクセスカード」（CAC：Common Access Card）のようなソリューションを必要とすると解釈してはならない。トークンや生体認証を使う（再生防止によるものを含めて）様々な多要素認証ソリューションは、商業ベースで入手可能である。そのようなソリューションでは、ユーザーのクレデンシャルを保存するために、トークン（スマートカード、キーフォブ、またはドングルなど）やソフトトークンを採用することもある。

[25] *ローカルアクセス* とは、ネットワークを使うことなしに、直接的な接続を介して通信するユーザー（またはユーザーに代わって動作するプロセス）によるシステムへのアクセスのことである。ネットワークアクセスとは、ネットワーク（LAN、WAN、インターネットなど）を介して通信するユーザー（またはユーザーに代わって動作するプロセス）によるシステムへのアクセスのことである。

3.5.5 規定された期間、ID の再利用を防止する。

詳解

ID は、ユーザー、ユーザーに代わって動作するプロセス、またはデバイス（3.5.1 参照）に付与される。ID の再利用の防止とは、以前に使用された個人、グループ、役割、またはデバイスの ID が別の個人、グループ、役割、またはデバイスに割り当てられることを防止することを意味する。

3.5.6 規定された非アクティブな期間が過ぎた後、ID を無効化する。

詳解

個人の ID は、攻撃者が非アクティブな ID を不当に利用し、検知されることなく組織のデバイスにアクセスする可能性があるため、組織の情報にリスクをもたらす。非アクティブなアカウントのオーナーは、自身のアカウントへの認可されてないアクセスがなされたかどうかに気付かない場合がある。

3.5.7 新しいパスワードが作成される際には、パスワードの最小限の複雑性と文字の変更を強制する。

詳解

このセキュリティ要件は、個人が、個人のオーセンティケータまたはグループのオーセンティケータとしてパスワードを使用する際の単一要素認証に適用され、また、パスワードが多要素認証の一部として使用される場合にも、同様に適用される。変更文字数は、現在のパスワードの文字列の総数に対して変更が必要な文字数を意味する。パスワードに対するブルートフォース（総当たり）攻撃を回避するために、組織は、パスワードにソルトを付与することを検討する。

3.5.8 指定された生成回数の間、パスワードの再利用を禁ずる。

詳解

パスワードの有効期間に関する制限は、一時的なパスワードには適用されない。

3.5.9 システムログオン時、常用（permanent）パスワードに即時変更することを条件として一時的パスワードの使用を許可する。

詳解

システムへのログオン後、一時的なパスワードが即座に常用のパスワードに変更されることにより、認証メカニズムの必要な強度が早急に実装され、オーセンティケータが危殆化される可能性を低くする。

3.5.10 暗号技術で保護されたパスワードのみを保存および伝送する。

詳解

暗号技術で保護されたパスワードは、ソルトが付与された一方向ハッシュにより暗号化されたパスワードの使用などである。

参照：[NIST CRYPTO]。

3.5.11 認証情報のフィードバックを隠す。

詳解

システムからのフィードバックは、認可されてない個人が認証メカニズムを危殆化することを許すような情報を提供しない。システムまたはシステムコンポーネントのタイプによっては、たとえば、モニター画面が比較的大きいデスクトップパソコンまたはノートパソコンでは、（ショルダーサーフィン（訳注：対象者の肩越しにディスプレイをのぞき見て、認可されてない情報を入手すること）と称される）脅威が深刻な場合がある。ディスプレイが小さいモバイルデバイスなどの、その他のタイプのシステムまたはシステムコンポーネントの場合は、この脅威はさほど深刻でない一方、キーボードが小さいため、入力ミスの可能性が高くなる。したがって、オーセンティケータのフィードバックを隠す手段は、システムの種類に応じて選択される。オーセンティケータのフィー

ドバックを隠す手段には、ユーザーが入力デバイスにパスワードを入力する際にアスタリスクを表示させることや、完全に隠す前の極めて限定された時間しかフィードバックを表示しないこと、などが含まれる。

3.6 インシデント対応

基本セキュリティ要件

3.6.1 準備、検知、分析、抑制、復旧およびユーザー対応活動を含め、組織のシステムに運用状態のインシデント対応ケイパビリティを確立する。

詳解

インシデント対応ケイパビリティ（機能、能力）は、組織のシステムのケイパビリティおよびそれらのシステムによって支援されている組織のミッション／事業プロセスに依存したものであることを、組織は認識する。組織は、インシデント対応を、ミッション／事業プロセスおよびシステムの定義、設計、開発の一環とみなす。インシデントに関連する情報は、監査活動による監視（audit monitoring）、ネットワーク監視、物理的アクセスの監視、ユーザーレポート、管理者レポート、報告されたサプライチェーンのイベント、などのさまざまな情報源から入手することができる。効果的なインシデント対応ケイパビリティには、ミッション／事業オーナー、システムオーナー、認可担当者、人事部、物理的および職員セキュリティ部、法務部、業務職員、調達部、およびリスクエグゼクティブなどの、組織の多数のエンティティ間の連携を伴う。

ユーザー対応活動の一環として、組織はインシデント対応訓練を提供する。訓練は、適切な内容と詳細レベルで構成されるように、組織の職員に割り当てられた役割と責任に直接関連付けられる。たとえば、(1) 一般のユーザーは、システム上のインシデントをどのように見分け、誰に報告すべきかのみを知っていればよいが（need to know）；(2) システム管理者は、インシデントの対応方法や解決方法に関する追加の訓練を必要とする場合があり；(3) インシデント対応者は、フォレンジック（forensics：法的証拠収集）捜査、報告、システム復旧、修復に関するより具体的な訓練を受けることがある。インシデント対応訓練には、外部ソースおよび内部ソースからの疑わしい行為の識別／報告に関するユーザー向け訓練が含まれる。ユーザー対応活動には、ヘルプデスクサポート、ヘルプグループ、フォレンジック捜査サービスへのアクセス、または必要に応じて消費者救済サービスなどの、インシデント対応の補助も含まれる。

[SP 800-61]はインシデント対応に関するガイダンスを提供する。[SP 800-86]、[SP 800-101] は、フォレンジック技法を組み込んだインシデント対応に関するガイダンスを提供する。[SP 800-161]はサプライチェーンのリスクマネジメントに関するガイダンスを提供する。

3.6.2 インシデントを追跡、文書化し、組織内外の指定された担当者および／または機関に報告する。

詳解

システムのセキュリティインシデントの追跡および文書化には、各インシデントについての記録、インシデントの状態、フォレンジック捜査に必要なその他の関連情報を維持することに加えて、インシデントの詳細、傾向、対応を対応状況の評価することが含まれる。インシデント情報は、インシデント報告、インシデント対応チーム、監査活動による監視、ネットワーク監視、物理的アクセスの監視、ユーザーレポート、管理者レポートなどのさまざまな情報源から入手することができる。

インシデント報告は、組織内の固有なインシデント報告要件および組織に課された公的なインシデント報告要件に対応する。悪意のあるコードが含まれている可能性のある疑わしい電子メールを受信した場合などに、セキュリティインシデントの発生が疑われ、報告される場合がある。報告されるセキュリティインシデントのタイプ、報告の内容と適時性、および指定の報告先機関は、適用される法律、大統領令、指令、規定、および方針を反映する。

[SP 800-61] は、インシデント対応に関するガイダンスを提供する。

派生セキュリティ要件

3.6.3 組織のインシデント対応ケイパビリティをテストする。

詳解

組織は、インシデント対応ケイパビリティの全般的な有効性を判定し、潜在的な弱点または欠陥を特定するために、インシデント対応ケイパビリティをテストする。インシデント対応のテストには、チェックリストの使用、実地検証、机上演習、シミュレーション（平行および完全割り込み型の双方とも）、および包括的な演習などが含まれる。インシデント対応のテストでは、インシデント対応が組織の運営（たとえば、ミッションケイパビリティの低下など）、組織の資産、個人に与える影響も判定される。

[SP 800-84] は、情報技術ケイパビリティのためのテストプログラムに関するガイダンスを提供する。

3.7 メンテナンス

基本セキュリティ要件

3.7.1 組織のシステムのメンテナンスを行う[26]。

詳解

このセキュリティ要件は、システムのメンテナンスプログラムの情報セキュリティに関する側面を取り扱い、ローカルまたは非ローカルエンティティが実施する、あらゆるシステムコンポーネント（ハードウェア、ファームウェア、アプリケーションを含む）に対するあらゆるタイプのメンテナンスに適用される。システムメンテナンスには、スキャナー、コピー機、プリンターなど、情報処理やデータまたは情報保持に直接関連しないコンポーネントも含まれる。

3.7.2 システムのメンテナンスを実行するために用いられるツール、技法、メカニズム、および職員を管理する。

詳解

このセキュリティ要件は、セキュリティに関連したメンテナンスツールの問題に対応するものであり、CUI を処理、保存、または伝送する組織のシステム境界の外部にあり、特にそれらのシステムの動作を診断および修理するために用いられるメンテナンスツールを対象とする。組織は、メンテナンスツールに対して実施する管理策を柔軟に決定することができ、そうしたツールの利用の承認、管理、および監視を管理策に含むことができる。メンテナンスツールは、悪意のあるコードを意図的にまたは意図せずに、施設および組織のシステムに持ち込むための手段になる可能性がある。メンテナンスツールには、ハードウェア、ソフトウェア、およびファームウェアアイテム、たとえば、ハードウェアやソフトウェアの診断装置、ハードウェアやソフトウェアのパケットスニファなどが含まれる。

派生セキュリティ要件

3.7.3 **オフサイト**（off-site）で行われるメンテナンスのために取り外される装置からすべての CUI がサニタイズ（情報除去）されていることを確実にする。

詳解

[26] 一般に、システムメンテナンス要件は、*可用性* というセキュリティ目標を助ける傾向にある。しかしながら、不適切なシステムメンテナンスや、メンテナンス実施の失敗は、結果的に認可されてない CUI の開示をもたらし、その情報の *秘匿性* を危殆化する可能性がある。

この要件は、オフサイトで実施されるシステムメンテナンスの情報セキュリティに関する側面を取り扱い、ローカルまたは非ローカルエンティティが実施する、あらゆるシステムコンポーネント（アプリケーションを含む）に対するあらゆるタイプのメンテナンス（たとえば、委託メンテナンス、保証期間メンテナンス、社内メンテナンス、ソフトウェア保全契約によるメンテナンスなど）に適用される。

[SP 800-88] は、媒体のサニタイズに関するガイダンスを提供する。

3.7.4 診断およびテストプログラムが入っている媒体を組織のシステムで使用する前に、悪意のあるコードの有無をチェックする。

詳解

メンテナンス診断およびテストプログラムが入っている媒体の検査時に、媒体に悪意のあるコードが含まれていることが判定された場合、組織は、インシデント対応ポリシーおよび手順に則ってインシデント対応する。

3.7.5 外部ネットワーク接続を介して非ローカルメンテナンスセションを確立する際には多要素認証を要求し、非ローカルメンテナンスの完了時にはその接続を切断する。

詳解

非ローカルメンテナンスおよび診断活動とは、外部ネットワークを介して通信する個人によって実施される行為を指す。これらの非ローカルメンテナンスおよび診断セションを確立する際に使用される認証技法は、3.5.3 に記載のネットワークアクセス要件を反映する。

3.7.6 必要なアクセス認可のないメンテナンス職員のメンテナンス行為を監督（supervise）する。

詳解

このセキュリティ要件は、組織のシステム上でハードウェアまたはソフトウェアのメンテナンスを実施する個人に適用される。メンテナンスの職務を遂行するために、システムの物理的な保護領域内に配置される個人（たとえば、用務員や施設メンテナンス職員など）の物理的なアクセスについては、3.10.1 で取り扱われる。情報技術製造者、ベンダー、コンサルタント、システムインテグレータなどの、認可されたメンテナンス職員として事前に特定されていない個人は、たとえば、ほとんどあるいはまったく通知無しでメンテナンス活動を行う必要がある場合に、組織のシステムへの特権アクセスを必要とすることがある。組織は、リスクアセスメントに基づき、そうした個人に対して一時的なクレデンシャルを発行してもよい。一時的なクレデンシャルは、一度かぎりまたは非常に限定された期間のみ使用することができる。

3.8 媒体保護

基本セキュリティ要件

3.8.1 紙とデジタル双方とも、CUI を含むシステムの媒体を保護する（すなわち、セキュアに保存し物理的に管理する）。

詳解

システム媒体には、デジタル媒体と非デジタル媒体とがある。デジタル媒体には、ディスケット、磁気テープ、外付けおよびリムーバブル HDD、フラッシュドライブ、CD、および DVD などが含まれ、非デジタル媒体には、紙やマイクロフィルムなどが含まれる。デジタル媒体の保護には、メディアライブラリ内の CD やフラッシュドライブに保存されている設計仕様書にアクセスできる個人を、プロジェクトリーダーと開発チームのメンバーに限定することが含まれる。システム媒体の物理的な管理には、在庫を確認すること、保存されている媒体の説明責任を維持すること、および、個人がメディアライブラリから媒体を借り出しおよび返却できるようにする手順が整っていることの確認が含まれる。安全な保管場所には、鍵付きの引き出し、机、キャビネット、または管理されたメディアライブラリなどが含まれる。

システム媒体上の CUI へのアクセスは、そうした装置を物理的に管理することによって、在庫を確認すること、個人がメディアライブラリから媒体を借り出しおよび返却できるようにする手順を定めること、保存されているすべての媒体の説明責任を維持すること、などによって、限定することができる。

[SP 800-111]は、エンドユーザーデバイスのためのストレージ暗号化技術に関するガイダンスを提供する。

3.8.2 システム媒体上の CUI へのアクセスを、認可されたユーザーに限定する。

詳解

システム媒体へのアクセスは、物理的な管理システム媒体および安全な保管場所によって、限定することができる。システム媒体の物理的な管理には、在庫管理をすること、保存されているすべての媒体の説明責任を維持すること、および、個人がメディアライブラリからシステム媒体を借り出しおよび返却できるようにするための手順が整っていることを確認すること、などが含まれる。安全な保管場所には、鍵付きの引き出し、机、キャビネット、または管理されたメディアライブラリなどがある。

3.8.3 CUI を含むシステムの媒体を廃棄または再利用する前に、サニタイズ（情報除去）または破壊する。

詳解

この要件は、廃棄または再利用の対象となるデジタルおよび非デジタルのすべてのシステム媒体に適用される。例としては：(1) ワークステーション、ネットワークコンポーネント、スキャナー、コピー機、プリンター、ノートパソコン、モバイルデバイスに見られるデジタル媒体；および、(2) 紙やマイクロフィルムなどの非デジタル媒体が含まれる。サニタイズ（情報除去）プロセスでは、情報の取得または再構築ができないような形で、情報が媒体から削除される。消去、除去、暗号化消去、破壊を含むサニタイズ技法は、媒体が再利用または廃棄のために手放される（released）際に、認可されてない個人に情報が漏えいすることを防止する。

組織は、サニタイズが必要な媒体に対して、他の方法（methods）を適用できない場合には破壊が必要となる可能性があることを認識した上で、適切なサニタイズ方法を決定する。組織は、収容されているすべての（containing）情報がパブリックドメインにあるか、公開可能であるか、再利用または廃棄された場合に組織または個人に有害なインパクトを及ぼさないと思われる情報である媒体に対しても、サニタイズ技法および手順を自由に採用することができる。非デジタル媒体のサニタイズには、媒体を破壊することやドキュメントから CUI を削除することに加えて、ドキュメントから単語またはセクションを削除する場合と同等の効果が得られるように、ドキュメント内の選択された単語またはセクションを編集して隠すことが含まれる。NARA のポリシーおよびガイダンスは、CUI のサニタイズプロセスを管理している。

[SP 800-88] は、媒体のサニタイズに関するガイダンスを提供する。

派生セキュリティ要件

3.8.4 CUI のマーキングと配布制限が必要な媒体にはその旨をマーキングする[27]。

[27] 本要件の実装は、[32 CFR 2002]、および[NARA CUI]のマーク標示ガイダンスに従っている。標準フォーム（SF）902（約 2.125 インチ x1.25 インチ）および SF 903（約 2.125 インチ x.625 インチ）は、ハードドライブや USB デバイスなどの CUI を含むメディアで使用できる。どちらのフォームも https://www.gsaadvantage.gov から入手できる。SF 902：NSN 7540-679-3318。SF 903：NSN 7540-01-679-3319。

詳解

「*セキュリティマーキング*（標記）」という用語は、人が読むことが可能なセキュリティ属性を適用することや使用することを意味する。システム媒体には、デジタル媒体と非デジタル媒体とがある。システム媒体へのマーキングは、適用される連邦法、大統領令、指令、方針および規則を反映する。

参照：[NARA MARK]。

3.8.5 CUI を含む媒体へのアクセスを管理し、管理区域外での輸送中は、媒体に関する説明責任を維持する。

詳解

管理区域とは、組織が、システムおよび情報を保護するために設定した要件を満たす、物理的または手続き上の管理策を提供する区域または場所のことを指す。輸送中の媒体の説明責任を維持する管理策には、鍵のかかったコンテナまたは暗号化が含まれる。暗号メカニズムは、使用されるメカニズムに応じた秘匿性および完全性の保護を提供する。輸送に関連する活動には、たとえば、実際の輸送とともに、輸送のために媒体を取り外すこと、媒体を適切な輸送処理に確実に移すこと、などが含まれる。実際の輸送において、認可された輸送および配達職員は、組織外部の個人であってもよい。輸送中の媒体の説明責任を維持するには、輸送活動を認可された職員に制限すること、および、媒体が輸送システムを移動する際の輸送活動の明確な記録を追跡および取得して、紛失、破壊、または改ざんを防止および検出することが含まれる。

3.8.6 代替的な物理的保全措置によって保護されている場合を除き、デジタル媒体上に保存された CUI の秘匿性を輸送時に保護するため、暗号メカニズムを実装する。

詳解

このセキュリティ要件は、ポータブルストレージデバイス（たとえば、USB メモリスティック、DVD、CD、外付けまたはリムーバブル HDD など）に適用される。

参照：[NIST CRYPTO]。

[SP 800-111] は、エンドユーザーデバイスのためのストレージ暗号化技術に関するガイダンスを提供する。

3.8.7 システムコンポーネント上のリムーバブルメディア（可搬型媒体）の使用を管理する。

詳解

このセキュリティ要件は、ユーザーによる媒体へのアクセスを制限する 3.8.1 の要件とは異なり、特定のタイプの媒体をシステム上で使用することを禁止し、たとえば、フラッシュドライブや外付け HDD の使用を制限または禁止する。組織は、システム媒体の使用を管理するために、技術的なまたは非技術的な管理策（たとえば、ポリシー、手順、および行動ルールなど）を採用することができる。組織は、ワークステーション上に物理的なケージを使用して特定の外部ポートの利用を禁止したり、ポータブルストレージデバイスの挿入、読み出し、書き込み機能を無効化または削除したりすることによって、そのようなデバイスの使用を管理する。

組織はまた、ポータブルストレージデバイスの使用を、組織が提供するデバイス、承認されたその他の組織が提供するデバイス、および私有でないデバイス、などを含む、承認されたデバイスに限定する。最後に、組織は、ポータブルストレージデバイスの使用をデバイスのタイプに基づいて管理することができ、書き込み可能なポータブルデバイスの使用を禁止し、デバイスへの書き込みケイパビリティを無効化または削除することによってそうした管理を実施する。

3.8.8 ポータブルストレージデバイスのオーナーを識別できない時には、そうしたデバイスの使用を禁止する。

詳解

ポータブルストレージデバイスのオーナー（たとえば、個人、組織、またはプロジェクト）の識別を義務付けることで、デバイスの知られている脆弱性（たとえば、悪意のあるコードの挿入）に対処する責任と説明責任の割り当てが可能になり、ポータブルストレージデバイスの使用から生じる全体的なリスクを抑えることができる。

3.8.9 保管場所にあるバックアップ CUI の秘匿性を保護する。

詳解

組織は、指定の保管場所にあるバックアップ情報の秘匿性を保護するために、暗号メカニズムまたは代わりの物理的管理策を採用することができる。CUI を含んでいるバックアップ情報には、システムレベルの情報とユーザーレベルの情報とがある。システムレベルの情報には、システム状態情報、オペレーティングシステムソフトウェア、アプリケーションソフトウェア、およびライセンスなどがある。ユーザーレベルの情報には、システムレベルの情報以外の情報が含まれる。

3.9 職員のセキュリティ

基本セキュリティ要件

3.9.1 CUI を含む組織のシステムへのアクセス認可に先立って、個人を審査する。

詳解

人事セキュリティスクリーニング（審査）活動には、CUI を含む組織システムへのアクセスを承認する前の、個人の行動、完全性、判断、忠誠心、信頼性、および安定性（つまり、個人の信頼性）のアセスメントが含まれる。この審査活動は、適用される連邦法、大統領令、指令、方針、規則、ならびに割り当てられた職位（positions）に必要なアクセスのレベルに応じて定められた特定の基準を反映する。

3.9.2 退職や異動などの人事措置中、およびその後において、CUI を含む組織のシステムが保護されていることを確実にする。

詳解

人事措置中および人事措置後における CUI の保護には、システム関連資産の返却および退職者面談の実施が含まれる。システム関連資産は、ハードウェア認証トークン、ID カード、システム管理技術マニュアル、鍵、入館証などである。退職者面談では、退職者に元従業員として課されるセキュリティ上の制約を理解させ、システム関連資産に対する適切な説明責任が達成されるようにする。退職者面談で扱われるセキュリティ関連のトピックには、守秘義務契約や退職後の職業選択に対する制約について、退職者に再認識させることを含めることができる。退職者のなかには、たとえば、就業放棄、病気、上司の不在などの理由から、退職者面談を実施できない者もいる。正当な理由により退職する個人に対して、退職措置を適時に実施することは必須である。組織は、特定の状況において、退職者に通知する前に退職者のシステムアカウントを無効にすることを検討する。

このセキュリティ要件は、個人の異動または転勤が恒久的である場合や、そうした人事措置が保護措置を要するほど長期的な場合に適用される。組織は、異動または転勤が恒久的か長期的かを問わず、そうした人事措置のタイプに適した CUI の保護措置を規定する。転勤や、組織内の他の職務への異動の際に必要な保護措置には、(1)古い鍵、ID カード、入館証を返却させ、新たな鍵、ID カード、入館証を発行すること；(2)システムへのアクセス認可（つまり、特権）を変更すること；(3)システムアカウントを削除し新たにアカウントを作成すること；および、(4)個人が前の勤務地において前のアカウントでアクセスしていた公式な記録に対してはアクセスを可能にすること、などが含まれる。

派生セキュリティ要件：無し

3.10 物理的保護

基本セキュリティ要件

3.10.1 組織のシステム、装置、およびそれぞれの運用環境への物理的アクセスを、認可された個人に限定する。

詳解

このセキュリティ要件は、従業員、訪問者、および恒久的な物理的アクセス認可のクレデンシャルを保持する個人に適用される。認可された個人は、バッジ、ID カード、スマートカードなどのクレデンシャルを保持する。組織は、適用される法律、指令、方針、規定、規格、手順および指針に則り、認証クレデンシャルの必要な強度を決定する。このセキュリティ要件は、一般にアクセス可能でない施設内の指定エリアに対してのみ適用される。

装置への物理的なアクセスの限定には、(1) 装置を鍵がかかった部屋またはその他の安全なエリアに配置して、認可された個人にのみアクセスを許可すること；および、(2) 装置を組織の職員が監視できる場所に配置することなどが含まれる。装置には、コンピューティングデバイス、外付け HDD、ネットワークデバイス、モニター、プリンター、コピー機、スキャナー、ファックス機器、オーディオデバイスなどがある。

3.10.2 組織のシステムの物理的施設および支援インフラを保護し、監視する。

詳解

物理的なアクセスの監視には、組織の施設内の一般にアクセス可能なエリアが含まれる。これは、たとえば、(1) 警備員の採用；(2) センサーデバイスの使用；または、(3) カメラなどのビデオ監視装置の使用などによって実施することができる。支援インフラとしては、システムの配電線、伝送回線、電力線などがある。支援インフラに適用されるセキュリティ管理策には、事故による損傷、障害、および物理的な不正行為を防止する。そのような管理策は、暗号化されていない通信の盗聴や改変を防止するために必要な場合がある。支援インフラへの物理的アクセスを管理するために使用される管理策には、たとえば、(1) 鍵がかかった配線用ボックス；(2) 分離したまたは鍵がかかった予備ジャッキ；(3) 導管やケーブルトレイによる配線の保護；および、(4) 通信傍受センサーなどがある。

派生セキュリティ要件

3.10.3 訪問者をエスコートし、その活動を監視する。

詳解

恒久的な物理的アクセス認可のクレデンシャルを持つ個人は、訪問者としてみなされない。訪問者の活動の監視には、監査ログを使用することができる。

3.10.4 物理的アクセスの監査ログを保持する。

詳解

組織は、使用する監査ログのタイプを柔軟に選択することができる。監査ログは、手続き的（たとえば、施設にアクセスした個人が書き込まれたログ）、自動的（たとえば、PIV カードによって示される ID の保存）、またはそれらの組み合わせであってよい。物理的なアクセスポイントには、施設へのアクセスポイント、補足的なアクセス管理が必要なシステムやシステムコンポーネントに対す

る施設内部のアクセスポイント、またはそれらの両方が含まれる。システムコンポーネント（たとえば、ワークステーション、ノートパソコンなど）は、組織がそうしたデバイスへのアクセスを保護している場合に限り、一般にアクセス可能として指定されたエリアに置くことができる。

3.10.5 物理的アクセスデバイスを管理（control）および監督（manage）する。

詳解

物理的アクセスデバイスには、鍵、ロック、それらの組み合わせ、およびカードリーダーなどが含まれる。

3.10.6 代替作業サイトにおける CUI の保全措置を実施する。

詳解

代替作業サイトは、公共施設や従業員の自宅などであることがある。組織は、そうした場所で行われる業務関連活動に応じて、特定の代替作業サイトまたはそのタイプごとに異なるセキュリティ要件を規定する。

[SP 800-46]、[SP 800-114] は、テレワーク時のエンタープライズセキュリティおよびユーザーセキュリティに関するガイダンスを提供する。

3.11 リスクアセスメント

基本セキュリティ要件

3.11.1 組織のシステム運用、および CUI に関連する処理、保存、または伝送から生ずる、組織運営（ミッション、機能、イメージ、評判を含む）、組織資産、および個人に対するリスクを定期的にアセスメントする。

詳解

システム境界を明確に定義することは、効果的なリスクアセスメントの前提条件である。そうしたリスクアセスメントは、組織のシステムの運用および使用に基づいて、組織運営、組織資産、および個人にもたらされる脅威、脆弱性、可能性、およびインパクトを考慮する。リスクアセスメントは、外部関係者（たとえば、サービスプロバイダ、組織の代理としてシステムを運用する契約事業者、組織のシステムにアクセスする個人、および外部委託先など）がもたらすリスクも考慮する。正式なまたは略式のリスクアセスメントは、組織レベル、ミッション／事業プロセスレベル、またはシステムレベルで実施されるとともに、システム開発ライフサイクルのあらゆる段階でも実施することができる。

[SP 800-30] は、リスクアセスメントの実施に関するガイダンスを提供する。

派生セキュリティ要件

3.11.2 システムおよびアプリケーションの脆弱性スキャンを定期的に、かつ、それらのシステムおよびアプリケーションに影響する新たな脆弱性が特定された場合に実施する。

詳解

組織は、ネットワーク接続されたプリンター、スキャナー、コピー機などの脆弱性の要因となり得るシステムコンポーネントも見落とさないよう、すべてのシステムコンポーネントに対して、必要な脆弱性スキャン実施を決定する。スキャンの対象となる脆弱性は、新たな脆弱性が発見、公表、および新たなスキャン方法が開発され次第、即座に更新される。このプロセスにより、システム内の潜在的な脆弱性は、可能な限り迅速に特定され、対処される。カスタムソフトウェアアプリケーションの脆弱性の分析では、静的解析、動的解析、バイナリ解析、およびこれらの 3 つの手段の混合など、追加の手段が必要な場合がある。組織は、それらの解析手段を、ソースコードレビューお

よびさまざまなツール（たとえば、静的解析ツール、ウェブベースのアプリケーションスキャナー、バイナリ解析ツールなど）に採用することができる。脆弱性のスキャンには：(1) パッチレベルのスキャン；(2) ユーザーまたはデバイスがアクセスを許可されていない機能、ポート、プロトコル、およびサービスのスキャン；ならびに、(3) 設定が誤っている、または不適当に動作している情報の一連の取り扱い手続の管理メカニズムのスキャンがある。

相互運用性を促進するために、組織は、CVE（Common Vulnerabilities and Exposures：共通脆弱性識別子）の命名規則によって脆弱性を表現し、システムの脆弱性の存在を判定する OVAL（Open Vulnerability Assessment Language：脆弱性アセスメント言語）を使用するスキャンツール、つまり、SCAP（Security Content Automation Protocol：セキュリティ設定共通化手順）認定の製品の採用を検討する。脆弱性情報に関する情報源には、CWE（Common Weakness Enumeration：共通脆弱性タイプ）のリストや NDV（National Vulnerability Database：脆弱性情報データベース）などがある。

レッドチーム演習などのセキュリティアセスメントは、スキャンが必要な潜在的な脆弱性の要因を更に特定する。組織は、また、脆弱性のインパクトを CVSS（Common Vulnerability Scoring System：共通脆弱性対応状況の評価システム）によって表現するスキャンツールを使用することも検討する。特定の状況において、脆弱性スキャンはその性質上、干渉的であったり、スキャン対象のシステムコンポーネントが特に高い要注意情報を含んでいたりすることがある。選択されたシステムコンポーネントに対して特権的なアクセスを認可することによって、徹底的な脆弱性スキャンが促進され、そうしたスキャンの要注意性が保護される。

[SP 800-40] は、脆弱性の管理に関するガイダンスを提供する。

3.11.3 リスクアセスメントに従って、脆弱性を取り除く。

詳解

たとえば、3.11.2 の要件に対応して実施されたスキャンを介して発見された脆弱性は、関連のリスクアのセスメントを考慮した上で修正される。リスクを考慮することで、修正の優先順位、および特定の脆弱性の解消において予期される労力が左右される。

3.12 セキュリティアセスメント

基本セキュリティ要件

3.12.1 組織のシステムのセキュリティ管理策を定期的にアセスメントし、その管理策の適用が有効かどうかを判断する。

詳解

組織は、システム開発ライフサイクルの一環として、組織のシステムのセキュリティ管理策およびそれらのシステムの運用環境をアセスメントする。セキュリティ管理策とは、セキュリティ要件に対応するため、組織が実装する保全措置や対策のことである。実装されたセキュリティ管理策をアセスメントすることによって、組織は、保全措置や対策が整っており、意図した通りに運用されているかを確認する。セキュリティ管理策のアセスメントでは、(1) 情報セキュリティが、組織のシステムに組み込まれていること；(2) 開発の早期の段階で弱点および欠陥を特定していること；(3) リスクベースの意思決定に必須な情報を提供していること；および、(4) 脆弱性緩和手順に準拠していることを確認する。セキュリティ管理策のアセスメントは、システムセキュリティ計画書の記載に従って、実装されたセキュリティ管理策に対して実施される。

セキュリティアセスメントレポートにはアセスメント結果が記載される。このアセスメント結果は、組織がレポートの的確性（accuracy）および正確性（completeness）を判断する上で、また、セキュリティ管理策が正しく実装され、意図したとおりに運用され、そして、セキュリティ要件を満たすような望ましい結果をもたらしているかを判断する上で、組織が必要とみたす範囲で詳細に記載される。セキュリティアセスメントの結果は、実施されたアセスメントのタイプに応じて該当する個人または役割に提供される。

組織は、セキュリティアセスメントの結果はセキュリティ管理策の有効性を判断するうえで最新かつ適切なものであることと、一定のレベルの独立性を有するアセッサーによってセキュリティアセ

スメントが行われて結果が出されることを保証する。組織は、システムのライフサイクルを通じてセキュリティ態勢を維持するために、脆弱性のスキャンやシステムの監視などのその他のタイプのアセスメント活動を使用することができる。

[SP 800-53] は、システムおよび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に関するガイダンスを提供する。

[SP 800-53A] は、セキュリティアセスメント計画書の作成およびアセスメントの実施に関するガイダンスを提供する

3.12.2 組織のシステムの欠陥を修正し、脆弱性を軽減または排除することを意図した実施計画書を作成し、実施する。

詳解

実施計画書は、情報セキュリティプログラムにおいて重要な文書である。組織は、実装されていないセキュリティ要件をいかに適合するか、および計画された緩和策をいかに実装するかを示す実施計画書を作成する。組織は、システムセキュリティ計画書と実施計画書を別の文書または集合的な文書として、選択したあらゆる形式で記述することができる。

連邦政府機関は、非連邦政府組織によってホスティングされるシステム上の CUI を処理、保存、または伝送するかについて総合的なリスク管理の決定を行う際に、提出されたシステムセキュリティ計画書と実施計画書を、重要なインプットとして考慮し、そうした非連邦政府組織と合意または契約を結ぶことが望ましいかを検討することがある。 [NIST CUI]は実施計画書のテンプレートを含む特別出版物 SP 800-171 の補足資料を提供する。

3.12.3 システムのセキュリティ管理策が継続的に有効であることを確実にするため、その管理策を継続的に監視する。

詳解

継続的な監視プログラムは、脅威や脆弱性ならびに組織のリスク管理の決定を支援する情報セキュリティに対する継続的な認識向上を促進する。「継続的」および「現在進行中の」という用語は、組織がセキュリティ管理策および情報セキュリティ関連リスクを、リスクに基づく決定を支援するのに十分な頻度で、対応状況をアセスメントし分析することを意味する。継続的な監視プログラムの結果に対して、組織は適切なリスク対応措置を講じる。レポートやダッシュボードによって、継続的にセキュリティ情報にアクセスできるようにすることで、組織の担当者は、効果的にかつ迅速にリスク管理の決定を行うことができる。

自動化は、ハードウェア、ソフトウェア、およびファームウェアの目録とその他のシステム情報のより頻繁な更新を支援する。継続的な監視のアウトプットが、具体的で、測定可能で、実用的で、関連性があり、タイムリーな情報を提供するようにフォーマット化されている場合、セキュリティ管理策の有効性はさらに向上する。特定の監視の必要性を含む監視要件は、他の要件でも参照される場合がある。

[SP800-137] は、継続的監視に関するガイダンスを提供する。

3.12.4 システムの境界、運用環境、セキュリティ要件の実装方法、および他のシステムとの関係または他のシステムへの接続について記述したシステムセキュリティ計画書を作成し、文書化し、定期的に更新する[28]。

詳解

[28] *システムセキュリティ計画書*の所定の様式または詳細なレベルの指定はない。しかしながら、組織は 3.12.4 で求められる要件がそれらの計画書によって伝えられることを保証する。

システムセキュリティ計画書は、セキュリティ要件を一式のセキュリティ管理策に関連づける。システムセキュリティ計画書は、セキュリティ管理策がどのようにしてセキュリティ要件を満たすかを概略的に記述するものであって、管理策の設計や実装に関する技術的な詳細を示すものではない。システムセキュリティ計画書には、計画書の意図に明確に従った設計と実装を可能にするために十分な情報、および、計画書の意図通りに導入された場合、その後のリスクの判定を可能にするために十分な情報が含まれる。セキュリティ計画書は単一の文書である必要はなく、既に存在するドキュメントを含めたさまざまな文書と組み合わせることができる。効果的なセキュリティ計画書は、より詳細な情報が得られるポリシー、手順、およびその他の文書（たとえば、設計および実装仕様書）を広く参照する。これによって、セキュリティ計画書に関連した文書化要件は少なくなり、セキュリティ関連情報は、エンタープライズアーキテクチャー、システム開発ライフサイクル、システムエンジニアリング、および調達に関連した、その他の設定された管理／運用の分野において維持される。

連邦政府機関は、非連邦政府組織によってホスティングされるシステム上の CUI を処理、保存、または伝送するかについて総合的なリスク管理の決定を行う際に、提出されたシステムセキュリティ計画書と実施計画書を、重要なインプットとして考慮し、そうした非連邦政府組織と合意または契約を結ぶことが望ましいかを検討することがある。

[SP 800-18] は、セキュリティ計画書の作成に関するガイダンスを提供する。[NIST CUI]は実施計画書のテンプレートを含む特別出版物 SP 800-171 の補足資料を提供する。

派生セキュリティ要件：無し

3.13 システムおよび通信の保護

基本セキュリティ要件

3.13.1 通信（すなわち、組織のシステムによって送受信される情報）を、組織のシステムの外部境界および主要な内部境界において監視、管理、および保護する。

詳解

通信は、境界コンポーネントにおいて、また、組織のシステム内のインタフェースを制限または禁止することによって、監視、管理、保護することができる。境界コンポーネントは、システムのセキュリティアーキテクチャー内で実装されるゲートウェイ、ルータ、ファイアウォール、ガード、ネットワークベースの悪意のあるコード分析システム、ネットワークベースの仮想化システム、または暗号化トンネルなど（たとえば、ファイアウォールを保護するルータや保護されたサブネットワーク上のアプリケーションゲートウェイなど）を含む。組織のシステム内のインタフェースの制限または禁止には、管理されたインタフェースにおいて指定されたウェブサーバーへの外部ウェブ通信トラフィックを制限することや、内部アドレスにスプーフィング（いわゆる、虚偽のアイデンティティ主張）していると思われる外部トラフィックを禁止すること、が含まれる。

組織は、商用通信サービスの利用に関するセキュリティ要件を実装する際は、そうしたサービスが共用される性質を持つ点に注意する。商用通信サービスは通常、サービスに加入しているすべての法人顧客が共用するネットワークコンポーネントおよび総合管理システムを基盤にしており、サードパーティが提供するアクセス回線またはその他のサービス要素を含むこともある。そうした通信サービスは、契約上のセキュリティ保障条項にもかかわらず、さらなるリスクをもたらす要因になり得る。

[SP 800-41] は、ファイアウォールおよびファイアウォールポリシーに関するガイダンスを提供する。[SP 800-125B] は、仮想化技術のセキュリティに関するガイダンスを提供する。

3.13.2 組織のシステム内で効果的な情報セキュリティを促進するような、アーキテクチャー設計、ソフトウェア開発技法、およびシステムエンジニアリングの原則を採用する。

詳解

組織は、新たに開発されるシステムや大幅なアップグレートが行われるシステムに対してシステムセキュリティエンジニアリングの原則を採用する。レガシーシステムについては、組織は、それらのシステムのハードウェア、ソフトウェア、およびハードウェアの現在の状態を踏まえて、システムのアップグレードおよび修正に対して可能な範囲でシステムセキュリティエンジニアリングの原則を適用する。システムセキュリティエンジニアリングの概念および原則を適用することによって、信頼できセキュアかつ復元力（レジリエンス）の高いシステムやシステムコンポーネントの開発が促進され、障害、危険、脅威にさらされにくくする。それらの概念および原則には、たとえば、(1) 層構造の保護を開発すること；(2) 設計の基盤としてセキュリティポリシー、アーキテクチャー、管理策を確立すること；(3) セキュリティ要件をシステム開発ライフサイクルに組み込むこと；(4) 、物理的および論理的井なセキュリティ境界を描くこと；(5) セキュアなソフトウェア開発の方法について開発者を訓練すること；ならびに、(6) 脅威をモデル化して、ユースケース、脅威エージェント、攻撃ベクトル、攻撃パターン、およびリスク緩和のために必要な相殺管理策を特定すること、などがある。セキュリティエンジニアリングの概念および原則を適用した組織では、信頼できるセキュアなシステム、システムコンポーネント、およびシステムサービスの開発が促進され、許容可能な水準までリスクを軽減し、また、十分な情報に基づいてリスク管理に関する決定を下すことができる。

[SP 800-160-1] は、システムセキュリティエンジニアリングに関するガイダンスを提供する。

派生セキュリティ要件

3.13.3 システム管理機能からユーザー機能を分離する。

詳解

システム管理機能には、データベース、ネットワークコンポーネント、ワークステーション、またはサーバーなどの管理に必要な機能が含まれ、通常、特権ユーザーのアクセス権が必要である。ユーザー機能とシステム管理機能との分離は、物理的なまたは論理的な分離を含む。システム管理機能とユーザー機能の分離は、(1) 異なるコンピュータ、異なる中央処理装置、異なるオペレーティングシステムのインスタンス、異なるネットワークアドレスを使用することにより；(2) 仮想化技法を使用することにより；または(3) 必要に応じてこれらやほかの方法を組み合わせることにより実施することができる。こうしたタイプの分離には、他のシステム資源の利用者に対して別の認証手段を使用するウェブ管理インタフェースがある。システム管理機能とユーザー機能の分離は、異なるドメイン上の管理インタフェースを追加のアクセス管理によって分離することを含む

3.13.4 共有システム資源を経由した、認可されてない情報転送や意図しない情報転送を防止する。

詳解

共有システム資源（たとえば、レジスタ、キャッシュメモリ、メインメモリ、ハードディスク）の情報の管理は、一般的に、オブジェクトの再利用や残存情報の保護とも呼ばれる。このセキュリティ要件は、共有システム資源がシステムに開放された後、そうしたシステム資源にアクセスする現在のユーザーまたは役割（または、現在のユーザーまたは役割に代わって動作する現在のプロセス）が、前のユーザーまたは役割のアクション（または前のユーザーまたは役割に代わって動作するプロセスのアクション）によって生成された情報を利用できないように防止する。このセキュリティ要件は、暗号化された情報にも適用される。一方、(1) 名目上は削除されたデータの残存表現を指す情報の残留性；(2) 情報フローの制限に違反するように共有リソースが操作される隠れチャネル（ストレージチャネルまたはタイミングチャネルを含む）；または、(3) 単一のユーザーまたは役割しかないシステム内のコンポーネントは、このセキュリティ要件の対象ではない。

3.13.5 内部ネットワークから物理的または論理的に分離された、公開（Publicly）アクセス可能なシステムコンポーネント用のサブネットワークを実装する

詳解

内部ネットワークから物理的または論理的に分離されたサブネットワークは、非武装地帯（DMZ）と呼ばれる。DMZ は通常、ルータ、ゲートウェイ、ファイアウォールなどの境界管理デバイスや技法、またはクラウドベースの技術を用いて実装される。

[SP 800-41]は、ファイアウォールおよびファイアウォールポリシーに関するガイダンスを提供する。[SP 800-125B] は、仮想化技術のセキュリティに関するガイダンスを提供する。

3.13.6 デフォルト設定によりネットワーク通信トラフィックを拒否、また例外によりネットワーク通信トラフィックを許可する（すなわち、全拒否、例外による許可）。

詳解

このセキュリティ要件は、システム境界およびシステム内の特定のポイントにおける、インバウンドおよびアウトバウンドのネットワーク通信トラフィックに適用される。全拒否、例外による許可のネットワーク通信トラフィックポリシーによって、必須かつ承認された接続のみが許可されるようになる。

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接続を確立することと同時に、外部ネットワーク内にある資源へその他何らかの接続（すなわち、スプリットトンネリング）を介して通信することを防止する。

詳解

スプリットトンネリングは、プリンターやファイルサーバーなどのローカルのシステム資源に通信するリモートのユーザーにとって望ましい場合がある。しかし、スプリットトンネリングは、認可されてない外部からの接続を許してしまうため、システムは攻撃に対して脆弱になり、組織の情報は漏出され易くなる。このセキュリティ要件は、構成設定によってリモートデバイス（たとえば、ノートパソコン、スマートフォン、およびタブレットなど）で実装され、ユーザーが構成する構成設定を自由に変更できなくすることで、リモートデバイスでのスプリットトンネリングを無効化する。このセキュリティ要件は、リモートデバイス内のスプリットトンネリング（またはスプリットトンネリングを許可する構成設定）を検知することによって、また、リモートデバイスがスプリットトンネリングを使用している場合には接続を禁止することによって、システムにおいて実装される。

3.13.8 代替的な物理的保全措置によって保護されている場合を除き、伝送中の CUI の認可されてない開示を防止するために、暗号メカニズムを実装する。

詳解

このセキュリティ要件は、内部および外部ネットワークならびに、サーバー、ノートパソコン、デスクトップパソコン、モバイルデバイス、プリンター、コピー機、スキャナー、ファックス機器など、情報を伝送できるあらゆるシステムコンポーネントに適用される。管理された境界の物理的保護下にない通信経路は、傍受や改変の双方を受けやすい。組織が、完全な専用サービス（すなわち、個々の顧客のニーズに特化したサービス）ではなく、商品サービスとして通信サービスを提供する民間プロバイダに頼っている場合、通信の秘匿性のために必要な管理策の実装に関して、必要な保証を得ることが困難な場合がある。そうした状況において組織は、標準的な商用通信サービスパッケージの中で、どのようなタイプの秘匿性サービスが利用可能であるかを確認する。適切な契約を介した必要な保全措置およびその保全措置の効果に対する保障を得ることが不可能または現実的でない場合、組織は補完的な保全措置を実装する、もしくは、リスクの増大を明示的に受け入れる。代替的な物理的保全措置には、たとえば、配布媒体を電子的または物理的な傍受から保護し、伝送中の情報の秘匿性を確保する PDS（保護された配布システム）がある。

参照：[NIST CRYPTO]。

3.13.9 通信セション終了時、または規定された非アクティブ時間経過後、そのセションに関連するネットワーク接続を切断する。

詳解

このセキュリティ要件は、内部ネットワークおよび外部ネットワークに適用される。通信セションに関連するネットワーク接続の切断には、オペレーティングシステムレベルで関連する TCP/IP アドレスまたはポートのペアの割当てを解除することや、複数のアプリケーションセションが単一のオペレーティングシステムレベルのネットワーク接続を使用している場合は、アプリケーションレベルでネットワークの割当てを解除すること、などが含まれる。ユーザーの非アクティブな時間は組織が設定してもよく、ネットワークアクセスのタイプごとや特定のネットワーク向けに時間を設定することができる。

3.13.10 組織のシステムで採用される暗号技術のための暗号鍵を設定し、管理する。

詳解

暗号鍵の管理および設定は、手動の手順または手動の手順に支援されるメカニズムを使用して実施することができる。組織は、適用される連邦法、大統領令、方針、指令、規制および規格に則って暗号鍵管理に関する要件を規定し、適切なオプション、レベル、およびパラメータを指定する。

[SP 800-56A]、[SP 800-57-1] は、暗号鍵のメンテナンスに関するガイダンスを提供する。

3.13.11 CUI の秘匿性保護には、FIPS 認証された暗号技術を採用する。

詳解

暗号技術は、CUI の保護、デジタル署名の提供、ならびに、認可された個人がそのような情報に必要な取扱許可は得ているものの、正式なアクセス許可を得ていない場合における情報の分離などの、多くのセキュリティソリューションをサポートするために使用することができる。暗号技術は、乱数の生成およびハッシュの生成のためにも使用できる。暗号規格には、FIPS 認証暗号技術および／または NSA 承認暗号技術がある。

参照：[NIST CRYPTO];[NIST CAVP]および[NIST CMVP]。

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[29]を禁止し、そのデバイスに存在するユーザーに対して使用中のデバイスを表示する。

詳解

共同コンピューティングデバイスは、ネットワーク化されたホワイトボード、カメラ、マイクロフォンなどである。使用の表示には、共同コンピューティングデバイスが活性化された時のユーザーへの信号が含まれる。ビデオ会議の参加者の一方が他方の参加者を呼び出して、または接続してビデオ会議が開始する、専用ビデオ会議システムは、この要件の対象から除かれる。

3.13.13 モバイルコードの使用を管理および監視する。

詳解

モバイルコード技術には、Java、JavaScript、ActiveX、Postscript、PDF、Flash animations、VBScript などがある。組織のシステムにモバイルコードを使用するかに関しては、モバイルコードが悪意をもって使用された場合にシステムに被害を及ぼす可能性に基づいて決定される。使用制限と実装ガイダンスは、サーバーにインストールされるモバイルコードの選択および使用、ならびに、個々のワークステーション、ノートパソコン、およびデバイス（たとえば、スマートフォン）にダウンロードされ実行されるモバイルコードの選択および使用、に対して適用される。モバイルコードに関するポリシーおよび手順は、信頼できるソースのデジタル署名をモバイルコードに付与することを義務付けることによって、許容できないモバイルコードの開発や取得、ならびにそうしたモバイルコードがシステムに挿入されることを防止する。

[29] ビデオ会議を活性化するために一人の参加者が他者を呼び出したり接続したりする専用ビデオ会議システムは除く。

[SP 800-28] は、モバイルコードに関するガイダンスを提供する。

3.13.14 インターネットプロトコルによる音声通信（VoIP）技術の使用を管理および監視する。

詳解

VoIP は、基本電話サービス（POTS, Plain Old Telephone Service）（すなわち、標準的な電話サービス）と比較して、種々の要件、特徴、機能性、可用性、およびサービスが限定されている。一方、その他の電話サービスは、総合サービスデジタル網（ISDN, Integrated Services Digital Network）や光ファイバー分散データインタフェース（FDDI, Fiber Distributed Data Interface）などの、高速デジタル通信回線に基づいている。POTS と POTS 以外のサービスの主な違いは、その速度と帯域幅にある。VoIP 技術の使用制限と実装ガイダンスは、VoIP 技術が悪意をもって使用された場合にシステムに被害を及ぼす可能性に基づいており、VoIP に関連する脅威に対応する。VoIP に対する脅威は、インターネットベースのあらゆるアプリケーションに内在する脅威と類似している。

[SP 800-58]は VoIP のガイダンスを提供する。

3.13.15 通信セションの真正性（Authenticity）を保護する。

詳解

真正性の保護には、中間者攻撃、セションハイジャック、または、通信セションへの偽情報の挿入などに対する保護が含まれる。このセキュリティ要件は、パケットレベルではなくセションレベルでの通信（たとえば、ウェブベースのサービスを提供するサービス指向アーキテクチャーでのセション）の保護を対象とする要件であり、通信セションの両側で、相手側の身元と伝送される情報の有効性を信頼するための根拠を確立する。

[SP 800-77]、[SP 800-95]、[SP 800-113] は、セキュアな通信セションに関するガイダンスを提供する。

3.13.16 通信停止中の CUI の秘匿性を保護する。

詳解

通信停止中の情報とは、処理中や伝送中ではなく、システムの特定のコンポーネントとしてストレージデバイスに位置している情報の状態をさす。通信停止中の保護で注意すべきは、ストレージデバイスのタイプやアクセスの頻度ではなく、情報の状態である。組織は、暗号メカニズムやファイル共有スキャンの使用を含め、様々なメカニズムを使用して秘匿性の保護を実現することができる。組織は、また、通信停止中の情報に含まれる悪意のあるコードを特定する継続的な監視や、通信停止中の情報を十分に保護できない場合はオンラインストレージの代わりにセキュアなオフラインのストレージを使用するなど、その他の管理策を採用してもよい。

参照：[NIST CRYPTO]。

3.14 システムおよび情報の完全性

基本セキュリティ要件

3.14.1 システムの欠陥をタイムリーに特定し、報告し、修正する。

詳解

組織は、ソフトウェアやファームウェアの公表された欠陥によって影響を受けるシステムと、それらの欠陥から生じる潜在的な脆弱性を特定し、そうした情報を指定の情報セキュリティ担当者に報告する。セキュリティ関連の更新には、パッチ、サービスパック、ホットフィックス、アンチウイルス署名などがある。組織は、セキュリティアセスメント、継続的な監視、インシデント対応活動、およびシステムエラー処理時に発見された欠陥にも対応する。組織は、組織のシステムで発見された欠陥を解決する際、CWE（Common Weakness Enumeration：共通脆弱性タイプ）データベースまたは CVE（Common Vulnerabilities and Exposure：共通脆弱性識別子）データベースなどの利用可能なリソース資料を活用することができる。

組織は、セキュリティ関連ソフトウェアおよびハードウェアの更新を行う時期を、更新の重要性（すなわち、発見された欠陥に関連する脆弱性の深刻度）を含む様々な要因に基づいて設定する。欠陥解決のタイプによっては、他の解決のタイプよりも多くテストを要することがある。

[SP 800-40]は、パッチ管理技術に関するガイダンスを提供する。

3.14.2 組織のシステム内の指定された場所で、悪意のあるコードからの保護機能を提供する。

詳解

このセキュリティ要件において、指定された（designated）場所とは、システムの入り口と出口とを指し、ファイアウォール、リモートアクセスサーバー、ワークステーション、電子メールサーバー、ウェブサーバー、プロキシサーバー、ノートパソコン、モバイルデバイスなどが含まれる。悪意のあるコードには、ウイルス、ワーム、トロイの木馬、スパイウェアなどがある。悪意のあるコードは、様々な形式（たとえば、UUENCODE、Unicode）でエンコードされ、圧縮ファイルや隠しファイルに含まれる、または、ステガノグラフィーなどの技法を用いてファイルに隠される。悪意のあるコードは、ウェブへのアクセス、電子メール、電子メールの添付物、および、ポータブルストレージデバイスを含む、様々な方法でシステムに挿入され得る。悪意のあるコードの挿入は、システムの脆弱性の悪用によって発生する。

悪意のあるコードからの保護メカニズムには、アンチウイルス署名の規定やレピュテーション（評判）ベース技術などが含まれる。悪意のあるコードの影響を限定または抑制する様々な技術や方法が存在する。広範囲の構成管理および包括的なソフトウェアの完全性の管理は、認可されてないコードの実行防止に有効な場合がある。悪意のあるコードは、市販のソフトウェアに加えて、カスタムソフトウェアにも存在することがある。そうした悪意のあるコードには、組織のミッション／事業機能に影響を及ぼしかねない、論理爆弾、バックドア、およびその他のタイプのサイバー攻撃などがある。悪意のあるコードに対する従来の保護メカニズムは、常にそうしたコードを検知できるわけではない。こうした状況において、組織は、代わりにセキュアコーディングプラクティス、構成管理および制御、信頼できる調達プロセス、監視プラクティスなどに頼り、ソフトウェアが意図した機能以外の機能を実行しないようにするなどその他の保全措置が含まれる。

[SP 800-83] は、マルウェア感染インシデントの防止に関するガイダンスを提供する。

3.14.3 システムのセキュリティアラートおよび勧告を監視し、対応措置を講ずる。

詳解

システムのセキュリティアラート（警報）およびアドバイザリ（勧告）は、一般に利用可能なソースが多数ある。たとえば、米国国土安全保障省の CISA（Cybersecurity and Infrastructure Security Agency）は、連邦政府全体および非連邦政府機関全体の状況に関する意識向上を維持するために、セキュリティアラートおよび勧告を作成している。ソフトウェアベンダー、加入サービス、および業界の ISAC（情報共有分析センター）もまた、セキュリティアラートおよび勧告を提供することがある。対応措置には、たとえば、外部のミッション／事業パートナー、サプライチェーンパートナー、外部のサービスプロバイダ、同業他社または支援組織などの、適切な外部組織に通知することが含まれる。

[SP 800-161]はサプライチェーンのリスクマネジメントに関するガイダンスを提供する。

派生セキュリティ要件

3.14.4 悪意のあるコードからの保護メカニズムが新たにリリースされた場合、更新する。

詳解

悪意のあるコードからの保護メカニズムには、アンチウイルス署名の規定やレピュテーションベース技術などが含まれる。悪意のあるコードの影響を限定または抑制する様々な技術や方法が存在する。広範囲の構成管理および包括的なソフトウェアの完全性の管理は、認可されてないコードの実行防止に有効な場合がある。悪意のあるコードは、市販のソフトウェアに加えて、カスタムソフトウェアにも存在することがある。論理爆弾、バックドア、およびその他のタイプのサイバー攻撃な

ど悪意のあるコードは、組織のミッション／事業機能に影響を及ぼしかねない。悪意のあるコードに対する従来の保護メカニズムは、常にそうしたコードを検知できるわけではない。こうした状況において、組織は、代わりにセキュアコーディングプラクティス、構成管理および制御、信頼できる調達プロセス、監視プラクティスなど、その他の保全措置に頼り、ソフトウェアが意図した機能以外の機能を実行しないようにする。

3.14.5 組織のシステムの定期的スキャンを実行すると共に、外部ソースからのファイルのリアルタイムスキャンを、ファイルがダウンロードされ、開かれ、実行される都度実行する。

詳解

組織のシステムの定期的スキャンおよび外部ソースからのファイルのリアルタイムスキャンにより、悪意のあるコードを検知することができる。悪意のあるコードは、様々な形式（たとえば、UUENCODE、Unicode）でエンコードされ、圧縮ファイルまたは隠しファイルに含まれる、または、ステガノグラフィーなどの技法を用いてファイルに隠される。悪意のあるコードは、たとえばウェブへのアクセス、電子メール、電子メールの添付物、およびポータブルストレージデバイスを含む、様々な方法でシステムに挿入され得る。悪意のあるコードの挿入は、システムの脆弱性を悪用して発生する。

3.14.6 攻撃および潜在的攻撃の兆候を検知するために、出入する通信トラフィックを含めて組織のシステムを監視する。

詳解

システム監視には、外部監視と内部監視とがある。外部監視は、システム境界で発生するイベント（すなわち、境界防御と境界保護の一部）の観測を含む。内部監視は、システム内で発生するイベントの観測を含む。組織は、たとえば、リアルタイムで監査記録活動を観測することによって、または、アクセスパターン、アクセスの特徴、その他の活動などのシステムのその他の側面を観測することによって、システムを監視することができる。監視目標によって、観測されるイベントが決定される。システム監視ケイパビリティは、さまざまなツールや技法（たとえば、侵入検知システム、侵入防止システム、悪意コード防御ソフトウェア、スキャンツール、監査記録監視ソフトウェア、ネットワーク監視ソフトウェア）によって実現される。監視デバイスの戦略的な配置場所には、選択された境界や、重要なアプリケーションを支援するサーバーファームの付近などがある。この時、監視デバイスは管理されたシステムインタフェースで採用される。収集する監視情報の詳細さの度合いは、組織の監視目標とその目標を支援するシステムのケイパビリティに基づいて決定される。

システム監視は、継続監視およびインシデント対応プログラムの不可欠な要素である。システム監視からの出力データは、継続監視およびインシデント対応プログラムへの入力データとして使用される。ネットワーク接続とは、ネットワーク（たとえば、ローカルエリアネットワークやインターネット）を介して通信するデバイスとのあらゆる接続である。リモート接続とは、外部ネットワーク（たとえば、インターネット）を介して通信するデバイスとのあらゆる接続である。ローカル接続、ネットワーク接続、およびリモート接続は、有線またはワイヤレスのいずれもあり得る。

出入りする通信トラフィックに関連する異常なまたは認可されてない行為や状態には、システム内に存在する悪意のあるコードまたはシステムコンポーネント間で伝播する悪意のあるコードを示す内部トラフィック、情報の認可されてないエクスポート、または外部システムへの信号などが含まれる。悪意のあるコードのエビデンスは、危殆化された可能性のあるシステムまたはシステムコンポーネントを特定するために使用される。特定のタイプのシステム監視の必要性を含む、システム監視要件は、他の要件で参照される場合がある。

[SP 800-94] は、侵入検知システムおよび侵入防止システムに関するガイダンスを提供する。

3.14.7 組織のシステムの認可されてない使用を特定（identify）する。

詳解

システム監視には、外部および内部監視が含まれる。システム監視は、組織のシステムの認可されてない使用を検知することができる。システム監視は、継続的な監視およびインシデント対応プロ

グラムの不可欠な要素である。監視は、さまざまな技法（たとえば、侵入検知システム、侵入防止システム、悪意を防御するソフトウェア、スキャンツール、監査記録監視ソフトウェア、ネットワーク監視ソフトウェア）によって実現される。システム監視からの出力データは、継続監視および対応プログラムへの入力データとして使用される。

出入りする通信トラフィックに関連する異常なまたは認可されてない行為や状態には、システム内に存在する悪意のあるコードの存在を示す内部トラフィック、またはシステムコンポーネント間での伝播、情報の認可されてないエクスポート、または外部システムへの信号などが含まれる。悪意のあるコードのエビデンスは、危殆化された疑いのあるシステムまたはシステムコンポーネントを特定するために使用される。特定のタイプのシステム監視の必要性を含む、システム監視要件は、他の要件で参照される場合がある。

[SP 800-94] は、侵入検知システムおよび侵入防止システムに関するガイダンスを提供する。

付属書 A
参照資料

法律、大統領令、規則、指示、規格、および指針[30]

法律、大統領令

[ATOM54] Atomic Energy Act (P.L. 83-703), August 1954.
「原子力法」1954年（または「原子力エネルギー法」の訳もある。）
https://www.govinfo.gov/app/details/STATUTE-68/STATUTE-68-Pg919

[FOIA96] Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996.
米国「情報公開法」（1967年施行、1996年「電子文書情報公開法」に改訂。「（電子）情報自由法」の訳もある。）
https://www.govinfo.gov/app/details/PLAW-104publ231

[FISMA] Federal Information Security Modernization Act (P.L. 113-283), December 2014.
「連邦情報セキュリティ近代化法」（2002年制定の「連邦情報セキュリティマネージメント法」から改訂）
https://www.govinfo.gov/app/details/PLAW-113publ283

[40 USC 11331] Title 40 U.S. Code, Sec. 11331, Responsibilities for Federal information systems standards. 2017 ed.
合衆国法典（U.S.C.）第40編 第11331条「連邦情報システム規格に対する責任」2017年版
https://www.govinfo.gov/app/details/USCODE-2017-title40/USCODE-2017-title40-subtitleIII-chap113-subchapIII-sec11331

[44 USC 3502] Title 44 U.S. Code, Sec. 3502, Definitions. 2017 ed.
合衆国法典 第44編 第3502条「定義」2017年版
https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapI-sec3502

[44 USC 3552] Title 44 U.S. Code, Sec. 3552, Definitions. 2017 ed.
合衆国法典 第44編 第3552条「定義」2017年版
https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapII-sec3552

[44 USC 3554] Title 44 U.S. Code, Sec. 3554, Federal agency responsibilities. 2017 ed.
合衆国法典 第44編 第3554条「連邦政府機関の責任」2017年版
https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapII-sec3554

[30] 本節において特定の発行日や改訂版数のない参照出版物は、当該出版物の最新の更新版を参照しているものとする。

[EO 13526] Executive Order 13526 (2009) Classified National Security Information. (The White House, Washington, DC), DCPD-200901022, December 29, 2009.
大統領令 13526「国家安全保障機密情報」2009年
https://www.govinfo.gov/app/details/DCPD-200901022

[EO 13556] Executive Order 13556 (2010) Controlled Unclassified Information. (The White House, Washington, DC), DCPD-201000942, November 4, 2010.
大統領令13556「管理対象非機密情報」2010年
https://www.govinfo.gov/app/details/DCPD-201000942

ポリシー、規則、指令、および指示

[32 CFR 2002] 32 CFR Part 2002, Controlled Unclassified Information, September 2016.
連邦規則集 vol 6（国土安全保障）title32 part 2002「管理対象非機密情報」2016年
https://www.govinfo.gov/app/details/CFR-2017-title32-vol6/CFR-2017-title32-vol6-part2002/summary

[OMB A-130] Office of Management and Budget (2016) Managing Information as a Strategic Resource. (The White House, Washington, DC), OMB Circular A-130, July 2016.
合衆国行政管理予算局「戦略資源としての情報管理」2016年
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[CNSSI 4009] Committee on National Security Systems (2015) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Fort George G. Meade, MD), CNSS Instruction 4009.
「国家安全保障委員会（CNSS）用語集 2015年」CNSS 指示 4009
https://www.cnss.gov/CNSS/issuances/Instructions.cfm

規格、指針（ガイドライン）、および報告書

[ISO 27001] International Organization for Standardization/International Electrotechnical Commission (2013) Information Technology—Security techniques— Information security management systems—Requirements. (International Organization for Standardization, Geneva, Switzerland), ISO/IEC 27001:2013.
ISO/IEC 27001 2013年「情報技術-セキュリティ技法-情報セキュリティ管理システム-要件」
https://www.iso.org/standard/54534.html

[FIPS 199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199.
「連邦政府情報および情報システムのセキュリティカテゴリー化に関するNIST規格」FIPS 199 米商務省 2004年
https://doi.org/10.6028/NIST.FIPS.199

[FIPS 200] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information

Processing Standards Publication (FIPS) 200.
「連邦政府情報および情報システムに対する最小限のセキュリティ要件に関するNIST規格」FIPS 200 米商務省 2006年
https://doi.org/10.6028/NIST.FIPS.200

[SP 800-18] Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1.
NIST特別出版物（SP）800-18「連邦情報システムのセキュリティ計画の策定に関するガイド」rev.1 2006年
https://doi.org/10.6028/NIST.SP.800-18r1

[SP 800-28] Jansen W, Winograd T, Scarfone KA (2008) Guidelines on Active Content and Mobile Code. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-28, Version 2.
NIST SP 800-28「アクティブコンテンツとモバイルコードの利用に関するガイドライン」2008年
https://doi.org/10.6028/NIST.SP.800-28ver2

[SP 800-30] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1.
NIST SP 800-30「リスクアセスメントの実施に関するガイド」rev.1 2012年
https://doi.org/10.6028/NIST.SP.800-30r1

[SP 800-39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.
NIST SP 800-39「情報セキュリティリスク管理の策定：組織、ミッション、および情報システムの考え方」2011年
https://doi.org/10.6028/NIST.SP.800-39

[SP 800-40] Souppaya MP, Scarfone KA (2013) Guide to Enterprise Patch Management Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 3.
NIST SP 800-40「パッチおよび脆弱性管理の策定に関するガイド」rev.3 2013年
https://doi.org/10.6028/NIST.SP.800-40r3

[SP 800-41] Scarfone KA, Hoffman P (2009) Guidelines on Firewalls and Firewall Policy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-41, Rev. 1.
NIST SP 800-41「ファイアウォールとその防護ポリシーの策定に関するガイドライン」rev.1 2009年
https://doi.org/10.6028/NIST.SP.800-41r1

[SP 800-46] Souppaya MP, Scarfone KA (2016) Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. (National Institute of

Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-46, Rev. 2.
NIST SP 800-46「企業におけるテレワーク、リモートアクセスおよび個人使用デバイスの使用に関するガイド」rev.2 2016年
https://doi.org/10.6028/NIST.SP.800-46r2

[SP 800-50] Wilson M, Hash J (2003) Building an Information Technology Security Awareness and Training Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-50.
NIST SP 800-50「情報技術セキュリティ意識向上および訓練プログラムの策定」2003年
https://doi.org/10.6028/NIST.SP.800-50

[SP 800-53] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015.
NIST SP 800-53「連邦政府組織と情報システムにおけるセキュリティおよびプライバシー管理策」rev.4 2013年、2015年更新を含む
https://doi.org/10.6028/NIST.SP.800-53r4

[SP 800-53A] Joint Task Force Transformation Initiative (2014) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 4, Includes updates as of December 18, 2014.
NIST SP 800-53A「連邦政府組織と情報システムにおけるセキュリティおよびプライバシー管理策のアセスメント：効果的なアセスメント計画の策定について」rev.4 2014年、2014更新を含む
https://doi.org/10.6028/NIST.SP.800-53Ar4

[SP 800-53B] Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-53B.
NIST SP 800-53B「連邦政府組織と情報システムにおける管理策ベースラインと適用に関するガイダンス」
[Forthcoming]. 近日登場

[SP 800-56A] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R (2018) Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56A, Rev. 3.
NIST SP 800-56A「離散対数暗号を用いたペアーワイズキー確立スキームの推奨」rev.3 2018年
https://doi.org/10.6028/NIST.SP.800-56Ar3

[SP 800-57-1] Barker EB (2016) Recommendation for Key Management, Part 1: General. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-57 Part 1, Rev. 4.
NIST SP 800-57-1「鍵管理方式の推奨」rev.1 2016年

https://doi.org/10.6028/NIST.SP.800-57pt1r4

[SP 800-58] Kuhn R, Walsh TJ, Fries S (2005) Security Considerations for Voice Over IP Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-58.
NIST SP 800-58「VoIPシステムのセキュリティに関する考慮事項」rev.3 2005年
https://doi.org/10.6028/NIST.SP.800-58

[SP 800-60-1] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1.
NIST SP 800-60-1「情報および情報システムのタイプとセキュリティカテゴリーとのマッピングのためのガイド」第１巻 rev.1 2008年
https://doi.org/10.6028/NIST.SP.800-60v1r1

[SP 800-60-2] Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 2, Rev. 1.
NIST SP 800-60-2「情報および情報システムのタイプとセキュリティカテゴリーとのマッピングのためのガイド」第２巻 rev.1 2008年
https://doi.org/10.6028/NIST.SP.800-60v2r1

[SP 800-61] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61, Rev. 2.
NIST SP 800-61「コンピュータセキュリティインシデント対応ガイド」rev.2 2012年
https://doi.org/10.6028/NIST.SP.800-61r2

[SP 800-63-3] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Includes updates as of December 1, 2017.
NIST SP 800-63-3「デジタルアイデンティティのガイドライン」2017年更新を含む
https://doi.org/10.6028/NIST.SP.800-63-3

[SP 800-70] Quinn SD, Souppaya MP, Cook MR, Scarfone KA (2018) National Checklist Program for IT Products: Guidelines for Checklist Users and Developers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-70, Rev. 4.
NIST SP 800-70「IT製品の国家的チェックリストプログラム：チェックリスト利用者と開発者のためのガイドライン」rev.4 2018年
https://doi.org/10.6028/NIST.SP.800-70r4

[SP 800-77] Frankel SE, Kent K, Lewkowski R, Orebaugh AD, Ritchey RW, Sharma SR (2005) Guide to IPsec VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-77.

NIST SP 800-77「IPセキュリティアーキテクチャー（IPsec）およびVPNに関するガイド」2005年
https://doi.org/10.6028/NIST.SP.800-77

[SP 800-83] Souppaya MP, Scarfone KA (2013) Guide to Malware Incident Prevention and Handling for Desktops and Laptops. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-83, Rev. 1.
NIST SP 800-83「デスクトップおよびラップトップコンピュータ向けのマルウェアインシデント防止と取り扱いのためのガイド」rev.1 2013年
https://doi.org/10.6028/NIST.SP.800-83r1

[SP 800-84] Grance T, Nolan T, Burke K, Dudley R, White G, Good T (2006) Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-84.
NIST SP 800-84「IT計画およびIT対応ケイパビリティに向けたテスト、トレーニング（訓練）、エクササイズ（演習）プログラムのためのガイド」2006年
https://doi.org/10.6028/NIST.SP.800-84

[SP 800-86] Kent K, Chevalier S, Grance T, Dang H (2006) Guide to Integrating Forensic Techniques into Incident Response. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-86.
NIST SP 800-86「インシデント対応におけるフォレンジック技法の統合のためのガイド」2006年
https://doi.org/10.6028/NIST.SP.800-86

[SP 800-88] Kissel RL, Regenscheid AR, Scholl MA, Stine KM (2014) Guidelines for Media Sanitization. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-88, Rev. 1.
NIST SP 800-88「媒体のサニタイズに関するガイドライン」rev.1 2014年
https://doi.org/10.6028/NIST.SP.800-88r1

[SP 800-92] Kent K, Souppaya MP (2006) Guide to Computer Security Log Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-92.
NIST SP 800-92「コンピュータセキュリティログ管理に関するガイド」2006年
https://doi.org/10.6028/NIST.SP.800-92

[SP 800-94] Scarfone KA, Mell PM (2007) Guide to Intrusion Detection and Prevention Systems (IDPS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-94.
NIST SP 800-94「侵入検知および侵入防止システム（IDPS）に関するガイド」2007年
https://doi.org/10.6028/NIST.SP.800-94

[SP 800-95] Singhal A, Winograd T, Scarfone KA (2007) Guide to Secure Web Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-95.
NIST SP 800-95「セキュアなWebサービスに関するガイド」2007年
https://doi.org/10.6028/NIST.SP.800-95

[SP 800-97] Frankel SE, Eydt B, Owens L, Scarfone KA (2007) Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-97.
NIST SP 800-97「堅固なセキュリティのワイヤレスネットワークの確立」2007年
https://doi.org/10.6028/NIST.SP.800-97

[SP 800-101] Ayers RP, Brothers S, Jansen W (2014) Guidelines on Mobile Device Forensics. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-101, Rev. 1.
NIST SP 800-101「モバイルデバイスのフォレンジックスに関するガイドライン」2014年
https://doi.org/10.6028/NIST.SP.800-101r1

[SP 800-111] Scarfone KA, Souppaya MP, Sexton M (2007) Guide to Storage Encryption Technologies for End User Devices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-111.
NIST SP 800-111「エンドユーザーデバイスのストレージ暗号化技術に関するガイド」2007年
https://doi.org/10.6028/NIST.SP.800-111

[SP 800-113] Frankel SE, Hoffman P, Orebaugh AD, Park R (2008) Guide to SSL VPNs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-113.
NIST SP 800-113「SSL、VPNに関するガイド」2008年
https://doi.org/10.6028/NIST.SP.800-113

[SP 800-114] Souppaya MP, Scarfone KA (2016) User's Guide to Telework and Bring Your Own Device (BYOD) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-114, Rev. 1.
NIST SP800-114「テレワークおよび個人所有デバイス（BYOD）の持ち込みに関する利用者向けガイド」2016年
https://doi.org/10.6028/NIST.SP.800-114r1

[SP 800-124] Souppaya MP, Scarfone KA (2013) Guidelines for Managing the Security of Mobile Devices in the Enterprise. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-124, Rev. 1.
NIST SP 800-124「企業内のモバイルデバイスのセキュリティ管理のためのガイドライン」2013年
https://doi.org/10.6028/NIST.SP.800-124r1

[SP 800-125B] Chandramouli R (2016) Secure Virtual Network Configuration for Virtual Machine (VM) Protection. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-125B.
NIST SP 800-125B「仮想マシン（VM）のセキュアな仮想ネットワーク構成」2016年
https://doi.org/10.6028/NIST.SP.800-125B

[SP 800-128] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128.
NIST SP 800-128「情報システムのセキュリティにフォーカスした構成管理に関するガイド」2011年
https://doi.org/10.6028/NIST.SP.800-128

[SP 800-137] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137.
NIST SP 800-137「連邦政府組織と情報システムのための情報セキュリティに関する継続的監視（ISCM）」2011年
https://doi.org/10.6028/NIST.SP.800-137

[SP 800-160-1] Ross RS, Oren JC, McEvilley M (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018.
NIST SP 800-160-1「システムセキュリティエンジニアリング：信頼できるセキュアなシステムのエンジニアリングにおける学際的アプローチに関する考慮事項」Vol.1 2016年、2018年の更新を含む
https://doi.org/10.6028/NIST.SP.800-160v1

[SP 800-161] Boyens JM, Paulsen C, Moorthy R, Bartol N (2015) Supply Chain Risk Management Practices for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161.
NIST SP 800-161「連邦政府組織と情報システムのためのサプライチェーンのリスクマネジメントプラクティス」2015年
https://doi.org/10.6028/NIST.SP.800-161

[SP 800-167] Sedgewick A, Souppaya MP, Scarfone KA (2015) Guide to Application Whitelisting. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-167.
NIST SP 800-167「アプリケーションのホワイトリスト化ガイド」2015年
https://doi.org/10.6028/NIST.SP.800-167

[SP 800-171A] Ross RS, Dempsey KL, Pillitteri VY (2018) Assessing Security Requirements

for Controlled Unclassified Information. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171A.

NIST SP 800-171A「管理対象非機密情報（CUI）のセキュリティ要件の適合状況アセスメント」2018年

https://doi.org/10.6028/NIST.SP.800-171A

[SP 800-181] Newhouse WD, Witte GA, Scribner B, Keith S (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181.

NIST SP 800-181「国立サイバーセキュリティ教育機構（NICE）におけるサイバーセキュリティ実務者のフレームワーク」2017年

https://doi.org/10.6028/NIST.SP.800-181

その他の出版物およびウェブサイト

[IETF 5905] Mills D, Martin J (ed.), Burbank J, Kasch W (2010) Network Time Protocol Version 4: Protocol and Algorithms Specification. (Internet Engineering Task Force), IETF Request for Comments (RFC) 5905.

IETF RFC 5905「ネットワーク時刻プロトコル第４版：プロトコルとアルゴリズム仕様」2010年

https://doi.org/10.17487/RFC5905

[NARA CUI] National Archives and Records Administration (2019) *Controlled Unclassified Information (CUI) Registry*.

NARA「CUIレジストリー」2019年

https://www.archives.gov/cui

[NARA MARK] National Archives and Records Administration (2016) Marking Controlled Unclassified Information, Version 1.1. (National Archives, Washington, DC).

https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf

CUI Notice 2019-01, Controlled Unclassified Information Coversheets and Labels.

NARA「CUIのマーキング」V1.1 2019年

https://www.archives.gov/files/cui/documents/20190222-cui-notice-2019-01-coversheet-label.pdf

[NIST CAVP] National Institute of Standards and Technology (2019) *Cryptographic Algorithm Validation Program*.

NIST「暗号アルゴリズム認証制度」2019年

https://csrc.nist.gov/projects/cavp

[NIST CMVP] National Institute of Standards and Technology (2019) *Cryptographic Module Validation Program*.

NIST「暗号モジュール認証制度」2019年

https://csrc.nist.gov/projects/cmvp

[NIST CRYPTO] National Institute of Standards and Technology (2019) *Cryptographic Standards and Guidelines*.

NIST「暗号技術規格およびガイドライン」2019年
https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines

[NIST CSF] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD).
NIST「重要インフラにおけるサイバーセキュリティ改善フレームワーク」v1.1 2018年
https://doi.org/10.6028/NIST.CSWP.04162018

[NIST CUI] National Institute of Standards and Technology (2019) *Special Publication 800-171 Publication and Supporting Resources*.
NIST「SP800-171 出版および支援リソース」
https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

付属書 B

用語解説

共通用語および定義

付属書 B では、「SP 800-171」で使われるセキュリティに関する専門用語の定義を定める。本用語解説で特段の規定がある場合を除いて、本出版物で使われるすべての用語は、CNSS 指令 4009『米国国家情報保証用語解説』CNSS Instruction 4009, に含まれる定義に一致する。

agency （政府機関） [OMB A-130]	行政機関または部局、軍事部局、連邦政府法人、連邦政府が管理する法人、または連邦政府の行政機関にあるその他の施設、または独立した規制機関。
assessment （アセスメント）	*Security Control Assessment*（セキュリティ管理策アセスメント） を参照のこと。
assessor （アセッサー）	*Security Control Assessor*（セキュリティ管理策アセッサー）を参照のこと。
audit log （監査ログ）	特定の機関に実行されたシステムアクセスおよび操作の記録を含む、システムアクティビティの時系列の記録。
audit record （監査記録）	監査されたイベントに関連する監査ログ内の個々の記載。
authentication （認証） [FIPS 200,Adapted]	多くの場合、システム内の資源へのアクセスを許可する前提条件として、ユーザー、プロセス、またはデバイスのアイデンティティを照合すること。
availability （可用性） [合衆国法典・第 44 編・第 3552 節]	情報に対する適時かつ信頼できるアクセス、およびその使用を確実にすること。
advanced persistent threat （持続的標的型攻撃） [SP 800-39]	高度な専門知識と重要なリソースを備え、サイバー攻撃、物理攻撃、欺瞞などの複数の攻撃ベクトルを使用して目標を達成する機会を生み出す敵対者。これらの目標には通常、(1) 情報の漏出、ミッション、プログラム、または組織の重要な側面の弱体化または妨害を目的として、対象組織の IT インフラ内に足場を確立および拡張すること；または (2) 将来的にこれらの目標を実行するためにそれ自体を配置することなどが含まれる。持続的標的型攻撃は、(1)その目標を長期間にわたって繰り返し追求し；(2) 防御側のそれに抵抗するための努力に適応し；および、(3)その目標を実行するために必要な相互作用のレベルを維持すべく決定されている。

baseline configuration （ベースライン構成）	あるシステムに関して文書化された仕様群、またはあるシステム内の構成品目のことであり、所与の時点において正式に見直しおよび合意されており、また変更管理手順を通じてのみ変更し得るもの。
bidirectional authentication （双方向認証）	同時にお互いを認証する 2 つのパーティ。 相互認証または双方向認証とも呼ばれる。
blacklisting （ブラックリスト登録）	システムまたは禁止された URL（Universal Resource Locators）／ウェブサイト上で実行することを許可されていないソフトウェアプログラムを特定するために使用されるプロセス。
confidentiality （秘匿性） [合衆国法典・第 44 編・第 3552 節]	個人のプライバシーおよび所有権のある情報を保護する手段を含む、情報へのアクセスおよび開示について、認可された制限を存続させること。
configuration management （構成管理）	情報技術製品およびシステムの完全性を確立および維持することに焦点を当てた活動の集合。システム開発ライフサイクル全体を通して、それらの製品およびシステムの構成を初期化、変更、および監視するプロセスを管理することによって行われる。
configuration settings （構成設定）	システムのセキュリティ態勢や機能性に影響をおよぼすハードウェア、ソフトウェア、またはファームウェアの中で変更することができるパラメータの集合。
controlled area （管理区域）	規定された物理的および手続き的な保護が、情報やシステムを保護するために確立された要件を十分に満たしているという信頼を、組織が持っている区域または空間。
controlled unclassified information （管理対象非機密情報） [E.O. 13556]	法律、規則、または政府全体のポリシーが、保全または配布管理を求める情報であり、2009 年 12 月 29 日付の大統領令 13526『*機密国家安全保証情報*』、または先行命令もしくは後継命令、あるいは 1954 年付の『原子力法』（修正版）に区分される情報は除かれる。
CUI categories （**CUI** カテゴリー（区分）） [32 CFR 2002]	法律、規則、または政府全体のポリシーが、保全または配布管理を求める情報のタイプ、および CUI 執行機関が承認し、CUI レジストリーに列挙した情報のタイプ。
CUI Executive Agent （**CUI** 執行機関） [32 CFR 2002]	執行機関横断の CUI プログラムを実装し、連邦政府機関の行動が大統領令 13556 を遵守しているかどうかを監督する国立公文書記録管理局（ NARA ： National Archives and Records Administration）。NARA は、米国情報セキュリティ監督局（ISOO）部長にその権限を委任している。

CUI program （**CUI** プログラム） [32 CFR 2002]	連邦政府機関による CUI の取り扱いを標準化するための執行機関全体におよぶプログラム。このプログラムには、大統領令 13556『32 CFR Part 2002』および CUI レジストリーによって制定された CUI のためのルール、組織、および手順が含まれる。
CUI registry （**CUI** レジストリー） [32 CFR 2002]	CUI の取扱に関するすべての情報、ガイダンス、ポリシー、ならびに要件に関するオンラインリポジトリ、32 CFR Part 2002 を除く、CUI 執行機関によって発行されるすべてのものを含んでいる。とりわけ、CUI レジストリーでは、承認されたすべての CUI カテゴリーを識別するとともに、それぞれについての概説、管理策の根拠、マーキング（標記）、および取扱い手順のガイダンスを含む。
cyber-physical systems （サイバーフィジカルシステム）	統合された物理学およびロジックを通じて機能するように設計された、相互作用するデジタル、アナログ、物理、および人間のコンポーネント。
dual authorization （二重認可） [CNSSI 4009, Adapted]	実行中のタスクに関し、それぞれが誤った、または認可されてないセキュリティ手順を検知できる、少なくとも 2 人の認可された人物の存在とアクションを要求することにより、特定のリソースへの個別のアクセスを禁止するように設計された保存と処理のシステム。
executive agency （執行機関） [OMB A-130]	合衆国法典・第 5 編・第 105 節で特定された行政省；合衆国法典・第 5 編・第 102 節で特定された軍事省；合衆国法典・第 5 編・第 104(1)節で規定された独立機関；および合衆国法典・第 31 編・第 91 章の規定に従う政府全額出資法人。
external system (or component) （外部 システム（またはコンポーネント））	組織によって定められた認可境界外にあるシステムまたはシステムのコンポーネント、そして必要とされるセキュリティ管理策の適用や、セキュリティ管理策の有効性アセスメントへの直接的な統制力を当該組織が通常では持たないシステムまたはシステムコンポーネント。
external system service （外部システムサービス）	組織のシステムの認可境界の外側に実装され、通常、組織が必要な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直接管理できないシステムサービス（つまり、組織のシステムによって使用されるが、組織のシステムの一部ではないサービス）。
external system service provider （外部システムサービスプロバイダ）	消費者-生産者の様々な関係を通じた、ある組織への外部システムサービスの提供者。この関係には、(1) 合弁事業、(2) ビジネスパートナー、(3) アウトソーシング協定（すなわち、契約、機関間合意、事業分野協定などを通したもの）、(4) ライセンス契約、(5) サプライチェーン取決めなどが含まれるが、それに限定されない。

external network （外部ネットワーク）	当該組織によって管理されないネットワーク。
federal agency （連邦政府機関）	*executive agency*（執行機関）を参照のこと。
federal information system （連邦政府情報システム） [合衆国法典・第 40 編・第 11331 節]	執行機関、執行機関の契事業約者、または執行機関の代理としての別組織によって使用され、あるいは運用される情報システム。
FIPS-validated cryptography （FIPS 認証暗号技術）	「FIPS 140-2」（修正版）で特定された要件を満たすために、「暗号モジュール認証制度」（CMVP： Cryptographic Module Validation Program）によって正当性確認（認証）された暗号モジュール。CMVP 認証の前提条件として、暗号モジュールは、「暗号アルゴリズム認証制度」（CAVP：Cryptographic Algorithm Validation Program）によって成功裏に認証試験に合格した暗号アルゴリズムを実装することが求められる。*NSA-Approved Cryptography*（*NSA* 承認暗号）を参照のこと。
firmware （ファームウェア） [CNSSI 4009]	通常は読取専用メモリー（ROM）またはプログラム可能読取専用メモロー（PROM）の中でハードウェアに保存されるコンピュータプログラムおよびデータ。その結果、プログラムとデータは、プログラム実行時に動的に書き出しや修正を行えない。
hardware （ハードウェア） [CNSSI 4009]	システムの物理的コンポーネント。*Software*（ソフトウェア）および *Firmware*（ファームウェア）を参照のこと。
identifier （ID）	個人のアイデンティティおよびそれに伴う属性を代表する固有のデータ。名前またはカード番号は、ID の例。 特定のエンティティ、オブジェクト、またはグループを示すためにシステムによって使用される一意のラベル。
impact （インパクト）	セキュリティに関して、情報またはシステムの秘匿性、完全性、または可用性の喪失が組織の運営、組織の資産、個人、他の組織、または国家（米国の国家安全保障上の利益を含む）に及ぼす影響。プライバシーに関して、情報システムが PII を処理するときに個人が受ける可能性のある有害な影響。
impact value （インパクト値） [FIPS 199]	情報の秘匿性、保全性、可用性が危殆化されることから生ずる、アセスメントされたワーストケースの潜在的インパクトであり、低位（low）、中位（moderate）、高位（high）という値で表現される。

incident （インシデント） [44 USC 3552]	あるシステム、またはそのシステムが処理、保存、または伝送する情報の、秘匿性、完全性、または可用性を、実際にまたは潜在的に危険に晒す出来事；あるいはセキュリティポリシー、セキュリティ手順、または利用規定（acceptable use policy）の違反、または差し迫った違反の恐れを構成する出来事。
information （情報） [OMB A-130]	テキスト、数値、図形、地図、口述、または視聴覚を含めて、あらゆる媒体または形式における、事実、データ、または意見などの知識の伝達または表象。
information flow control （情報フロー（一連の取り扱い手続）管理）	システム内の情報転送がセキュリティポリシー違反にならないことを確実にする手順。
information resources （情報リソース） [合衆国法典・第 44 編・第 3502 節]	職員、装置、資金、および情報技術などの情報および関連リソース。
information security （情報セキュリティ） [合衆国法典・第 44 編・第 3552 節]	秘匿性、完全性、および可用性の提供を目標とした、認可されてないアクセス、使用、開示、途絶、変更、または破壊からの、情報およびシステムの保護。
information system （情報システム） [合衆国法典・第 44 編・第 3502 節]	情報の収集、処理、メンテナンス、使用、共有、配布、または廃棄のために組織された個別の情報リソースの集合体。
information technology （情報技術） [OMB A-130]	執行機関によるデータまたは情報の自動的取得、保存、分析、評価、操作、管理、移動、制御、表示、転換、交換、伝送、または受信に使われるサービス、装置、あるいは相互接続された装置のシステムまたはサブシステム。この定義の目的上、そのようなサービスまたは装置は、(1)政府機関が直接使用する場合、またはその使用を必要とする政府機関との契約に基づいて契約事業者が使用する場合のもの；あるいは、(2)それがどうしても必要な場合には、サービスの実行または製品の提供における使用の場合のものである。また情報技術には、コンピュータ、付属装置（画像周辺機器、入力、出力、およびセキュリティと監視に必要なストレージデバイスを含む）、コンピュータの中央処理装置によって制御されるように設計された周辺装置、ソフトウェア、ファームウェアおよび同様の手順、サービス（クラウドコンピューティングやヘルプデスクサービス、または装置やサービスのライフサイクルの任意のポイントをサポートするその他の専門サービスなど）、および関連リソースを含む。 なお、情報技術には、その使用を必要としない契約に付随して契約事業者が取得した装置は含まれない。

insider threat （インサイダー脅威）	内部の者（インサイダー）が、故意または無意識に、認可されたアクセスを行うことで米国のセキュリティに害をなす可能性の脅威。この脅威には、スパイ行為、テロリズム、認可されてない開示によって、あるいは当局の資源やケイパビリティを喪失または低減させることで、米国に与えるダメージを含む。
integrity （完全性） [合衆国法典・第 44 編・第 3552 節]	不適切な情報改変や破壊の防止であり、情報の否認防止と真正性の保証が含まれる。
internal network （内部ネットワーク）	以下のようなネットワークである。すなわち、(1) セキュリティ管理策の確立、維持、および提供が、組織の被雇用者または契約事業者の直接管理下にあるネットワーク、あるいは (2) 組織管理の端点間に実装された暗号カプセル化または類似のセキュリティ技術が、（少なくとも秘匿性と完全性に関して）同一の影響を与えるネットワークである。内部ネットワークは通常、組織が所有するものであるが、組織所有ではなく、組織が管理しているものであることもある。
least privilege （最小限の特権）	セキュリティアーキテクチャーは、各エンティティに、その機能を実行するために必要な最小限のシステム認可とリソースが付与されるように設計されているという原則。
local access （ローカルアクセス）	ネットワークを使うことなしに、ダイレクトコネクションを介して通信するユーザー（またはユーザーに代わって動作するプロセス）による、組織所有のシステムへのアクセス。
malicious code （悪意のあるコード）	システムの秘匿性、完全性、または可用性に有害なインパクトを及ぼすことになる、認可されてないプロセス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。ホストコンピュータに感染する、ウイルス、ワーム、トロイの木馬、またはその他のコードベースのエンティティ。 スパイウェアおよびある種のアドウェアも、悪意のあるコードの例である。
media （媒体） [FIPS 200]	システムの中で、情報が記録、保存、印刷される、磁気テープ、光ディスク、磁気ディスク、大規模集積回路（LSI）メモリーチップ、および印刷出力（ディスプレイ媒体は含まれない）を含む、物理的デバイスまたは文書表面であるが、それらに限定されるものではない。

mobile code （モバイルコード）	受信者による明示的なインストール行為なしに、遠隔システムから入手され、ネットワークを越えて送信され、そしてローカルシステムで実行されるソフトウェアプログラムまたはプログラムの部分。
mobile device （モバイルデバイス）	以下のような携帯型コンピューティングデバイス。すなわち、(1) 小型形状因子であり、その結果、一人で容易に持ち運びできるもの；(2) 物理的接続なしに（無線送受信情報など）作動することを意図しているもの；(3) 取外し不能または取外し可能なローカルデータストレージを有するもの；および (4) 内蔵型電源を包含するもの。モバイルデバイスには、音声通信ケイパビリティ、当該デバイスの情報の取り込みを可能にする搭載センサー、そしてローカルデータを遠隔地と同期させる組込型特性も含まれることがある。例として、スマートフォン、タブレット、および電子ブックリーダーがある。
multifactor authentication （多要素認証）	認証を成就するために２つまたはそれ以上の異なる要素を使う認証。要素には以下が含まれる。すなわち、(1) 人が記憶しているもの（パスワード／PIN など）；(2) 人が所持しているもの（暗号識別デバイス、トークンなど）；あるいは (3) 人自身に存在するもの（生体認証情報）である。オーセンティケータ（*Authenticator*） を参照のこと。
mutual authentication （相互認証） [CNSSI 4009]	相互に確認するトランザクションに関与する両方のエンティティのプロセス。 双方向認証を参照のこと。
nonfederal organization （非連邦政府組織）	非連邦政府のシステムを所有、運用、または維持する主体。
nonfederal system （非連邦政府システム）	連邦政府システムの規準を満たさないシステム。
network （ネットワーク）	相互接続されたコンポーネントの集合によって実行されるシステム。そうしたコンポーネントには、ルータ、ハブ、敷設ケーブル、遠隔通信制御装置、主要配電センター、および回線制御装置が含まれることがある。
network access （ネットワークアクセス）	ネットワーク（LAN、WAN、インターネットなど）を介して通信するユーザー（またはユーザーに代わって動作するプロセス）によるシステムへのアクセス。

nonlocal maintenance （非ローカルメンテナンス）	外部ネットワーク（インターネットなど）または内部ネットワークのどちらかのネットワークを通じて通信する個人によって実施されるメンテナンス活動。
on behalf of (an agency) （（政府機関）の代理として） [32 CFR 2002]	以下の場合に生ずる状況： （1）情報システムを非執行機関の部局のエンティティが使用または運用する、または連邦政府情報を維持あるいは収集する目的で処理、保存、または伝送する；(2) 政府向けにサービス提供または製造するための付随的ではない活動。
organization （組織） [FIPS 200（修正版）]	ある組織的構造内にある、あらゆる規模、複雑性、または位置標定を持つエンティティ。
personnel security （職員のセキュリティ） [SP 800-53]	信頼性を必要とする義務と責任について、個人の行動、誠実さ、判断、忠誠、信頼性、および安定性をアセスメントする規範（discipline）。
portable storage device （ポータブルストレージデバイス）	システムに挿入でき、また取り外すことができ、そしてデータまたは情報（テキスト、映像、音声、画像データなど）を保存するために使われるシステムコンポーネント。そうしたコンポーネントは通常、磁気、光学、または半導体デバイス（フロッピーディスク、コンパクト／デ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、そして不揮発性メモリーを含むフラッシュメモリーカード／ドライブなど）に実装される。
potential impact （潜在的インパクト） [FIPS 199]	以下の状態が予想される秘匿性、完全性、または可用性の欠損。すなわち、組織の運用、組織の資産、または個人に対する (1) 限定的な有害な影響（FIPS 199：低位）； (2) 容易ならざる有害な影響（FIPS 199：中位）；(3) 深刻 または破局的な 有害な影響（FIPS 199：高位）である。
privileged account （特権アカウント）	特権ユーザーとして認可されたシステムアカウント。
privileged user （特権ユーザー）	通常のユーザーには実行が認可されないセキュリティ関連機能の実行が認可され（それ故、信頼され）たユーザー。

records （記録）	実行された活動のエビデンス、または達成された結果の（自動化および人力の双方または一方による）記録であり、組織やシステムが意図された通りに実行していることを確認する基礎となるもの。関連するデータフィールド単位（すなわち、プログラムがアクセスでき、また特定項目に関する完全な情報群を含むデータフィールドグループ）を参照するためにも使われる。
remote access （リモートアクセス）	外部ネットワーク（インターネットなど）を通じて通信するユーザー（またはユーザーに代わって動作するプロセス）による、組織所有のシステムへのアクセス。
remote maintenance （リモートメンテナンス）	外部ネットワーク（インターネットなど）を通じて通信する個人によって実施されるメンテナンス活動。
replay resistance （リプライ耐性）	送信された認証情報またはアクセス管理情報のキャプチャと、その後の認可されてない効果（effect）の生成または認可されてないアクセスの取得を目的とした再送信に対する保護。
risk （リスク） [OMB A-130]	あるエンティティが、潜在的な周辺事情またはイベントによって脅かされる程度の尺度であり、通常は以下の関数である。すなわち、(1) 周辺事情またはイベントが発生した場合に現れる有害なインパクト、または被害の程度；および (2) その発生の可能性である。
risk assessment （リスクアセスメント） [SP 800-30]	システムの運用から生ずる、組織の運用（ミッション、機能、心象、または評判を含む）、組織の資産、個人、その他の組織、および国家へのリスクを特定するプロセスである。リスク管理の一部であり、脅威および脆弱性分析を組み入れ、計画中または実施中のセキュリティ管理策によってもたらされる軽減を考慮に入れる。リスク分析と同義。
sanitization （サニタイゼイション／情報除去）	通常の手段により、また情報除去の形態によっては変則的な手段により、媒体に書かれたデータを復旧不能にさせるための措置。データ復旧が可能でないように、媒体から情報を取除くプロセス。これには、すべての機密区分ラベル、マーキング、および活動ログが含まれる。

security （セキュリティ） [CNSSI 4009]	ある組織のシステム使用への脅威によって課せられるリスクがあるにもかかわらず、その組織が自らのミッションや重要機能の実行を可能にする保護手段を確立・維持することから生ずる状態。保護手段は、抑止、回避、防止、検知、復旧、および補正の組み合わせを伴い、その組織のリスク管理アプローチの一部を形成するものでなければならない。
security assessment （セキュリティアセスメント）	*Security Control Assessment*（セキュリティ管理策アセスメント） を参照のこと。
security control （セキュリティ管理策） [OMB A-130]	組織の情報の秘匿性、完全性、および可用性を保護すること、そして定められたセキュリティ要件群を満たすことを意図して、システムまたは組織のために規定された保全措置または対抗手段。
security control assessment （セキュリティ管理策アセスメント） [OMB A-130]	情報システムまたは組織へのセキュリティ要件の対処に関して、管理策が、正しく実装され、意図通りに機能し、所望の結果を生み出している程度を判断するための、セキュリティ管理策のテストまたは評価(evaluation)。
security domain （セキュリティ領域） [CNSSI 4009, Adapted]	セキュリティポリシーを実装し、単一の機関によって管理される領域。
security functions （セキュリティ機能）	システムのセキュリティポリシーを強制し、セキュリティ保護の基礎となるコードやデータの遮断を支える責任を果たす、システムのハードウェア、ソフトウェア、およびファームウェアのうちの一つまたはそれ以上。
split tunneling （スプリットトンネリング）	リモートユーザーあるいはデバイスがシステムと非リモート接続すると同時に何らかの他の接続を介して外部ネットワークに存在する資源に通信することを可能とするプロセス。このネットワークアクセス方式は、管理されていないネットワークにアクセスしたままリモートデバイス（たとえば、ネットワーク印刷装置など）にアクセスすることができる。直接または間接的に、秘匿性、完全性、可用性を保護するセキュリティポリシーを実施するための関連する機能
system （システム）	*Information System*（情報システム） を参照のこと。

system component（システムコンポーネント）[SP 800-128]	システムを組み立てる要素としての、独立した、識別可能な情報技術資産（ハードウェア、ソフトウェア、ファームウェア）。システムコンポーネントには市販情報技術製品を含む。
system security plan（システムセキュリティ計画書）	組織がいかにシステムに対するセキュリティ要件に適合しているか、あるいは適合させる計画であるかを記述する文書。特に、このシステムセキュリティ計画書では（1）システの境界；(2) セキュリティ要件がどのように実装されているか；(3) 他のシステムとの関係あるいは接続、について記述する。
system service（システムサービス）	情報の処理、保存、または伝送を容易にするシステムによって提供されるケイパビリティ。
threat（脅威）[SP 800-30]	情報への認可されてないアクセス、破壊、開示、変更、およびサービス拒否の一つまたはそれ以上を介し、システムを通じて、組織の運営、組織の資産、個人、その他の組織、または国家に、有害なインパクトをおよぼす可能性のある周辺事情またはイベント。
system user（システムユーザー）	あるシステムへのアクセスが認可された個人、または認可された個人に代わって動作する（システム）プロセス。
whitelisting（ホワイトリスト登録）	システムまたは許可された URL／ウェブサイト上で実行することを許可されたソフトウェアプログラムを識別するために使用されるプロセス。
wireless technology（ワイヤレス技術）	物理的な接続なしに、離れたポイント間で情報を転送できるようにするテクノロジー。 ワイヤレス技術には、マイクロ波、パケットラジオ（超高周波または超高周波）、802.11x、および Bluetooth が含まれる。

付属書 C

頭字語

共通省略語

CFR	Code of Federal Regulations （連邦規則集）
CNSS	Committee on National Security Systems （国家セキュリティシステム委員会）
CUI	Controlled Unclassified Information （管理対象非機密情報）
CISA	Cybersecurity and Infrastructure Security Agency （サイバーセキュリティインフラストラクチャセキュリティ庁）
DMZ	Demilitarized Zone （非武装地帯／公開外部接続ネットワーク環境）
FAR	Federal Acquisition Regulation （連邦調達規則）
FIPS	Federal Information Processing Standards （連邦情報処理規格）
FISMA	Federal Information Security Modernization Act （連邦情報セキュリティ近代化法）
IoT	Internet of Things （機器類のインターネット）
IP	Internet Protocol （インターネットプロトコル）
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 （米国情報セキュリティ監督局）
IT	Information Technology （情報技術）
ITL	Information technology Laboratory （情報技術研究所）

NARA	National Archives and Records Administration （国立公文書記録管理局）
NFO	Nonfederal Organization （非連邦政府組織）
NIST	National Institute of Standards and Technology （米国標準技術研究所）
OMB	Office of Management and Budget （行政管理予算局）
SP	Special Publication （特別出版物）
VoIP	Voice over Internet Protocol （IP 音声通信技術）

付属書 D

対応付け表（MAPPING TABLES）

セキュリティ管理策に対するセキュリティ要件の対応付け

表 D-1 から表 D-14 は、本出版物の基本および派生セキュリティ要件に関連する[SP 800-53][31]のセキュリティ管理策の対応付け表である。この対応付け表は、理解を助けるための情報提供が目的であり、第 3 章に規定されている要件を超える追加のセキュリティ要件を与えるものではない。場合によっては、本セキュリティ管理策には CUI を保護するために求められるもの以外の、追加の期待が含まれており、そうした関連セキュリティ管理策は、第 2 章 の基準（criteria）を使ってテーラリングされている。本出版物のセキュリティ要件に関連するセキュリティ管理策の部分だけが、適用可能なものである。また、本表には２つ目の対応付け表として、[ISO27001] の関連する管理策についても、対応付けを示している。アスタリスク（*）は、ISO/IEC の管理策が、NIST 管理策の意図を完全には満たしていないことを示すものである。本出版物のセキュリティ要件を策定に際におこなわれたテーラリング措置の結果、CUI の機密性を保護するためには必須でない管理策または拡張（enhancement）管理策の特定の要素は、それらの要件に反映されていないため、基本要件または派生要件が満足されているからと言って、対応する[SP 800-53]のセキュリティ管理策または拡張管理策も満たされているということにはならない。

[NIST CSF] を実装し、または実装を計画している組織は、[SP 800-53]および[ISO 27001]のセキュリティ管理策に対するセキュリティ要件の対応付けを使って、このサイバーセキュリティフレームワークの中核機能、すなわち：識別、防御、検知、対応、および復旧に関連したカテゴリーおよびサブカテゴリーの中にある同等の保護を位置付けることができる。本セキュリティ要件への準拠性の実証を望む組織にとって、確立した情報セキュリティプログラムが NIST や ISO/IEC のセキュリティ管理策を中心に構築されている場合には、本管理策の対応付けに関する情報は有用なものとなろう。

[31] 表 D-1～D-14 のセキュリティ管理策は、NIST 特別出版物 SP 800-53、Rev.4 のものである。これらのテーブルは、NIST 特別出版物 SP 800-35rev.5 と整合性のある中位のセキュリティ管理策ベースラインへの更新を提供する[SP 800-53B]の公開時に更新される。中位ベースラインへの変更は、第 3 章の基本および派生セキュリティ要件に対する将来の更新に影響する。

表 **D-1**：セキュリティ管理策に対するアクセス管理要件の対応付け

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 アクセス管理				
基本セキュリティ要件				
3.1.1 システムへのアクセスは、認可されたユーザー、認可されたユーザーに代わって動作するプロセスおよび（その他のシステムを含む）デバイスに限定する。 **3.1.2** システムへのアクセスは、認可されたユーザーが実行を許可されているタイプのトランザクションおよび機能に限定する。	AC-2	アカウント管理	A.9.2.1	利用者登録および登録削除
			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	アクセス権の削除または修正
	AC-3	アクセス実施	A.6.2.2	テレワーキング
			A.9.1.2	ネットワークおよ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管理
			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	モバイルデバイスの方針
			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	情報転送の方針および手順
			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

派生セキュリティ要件				
3.1.3 承認された認可に従って、CUI のフローを管理する。	AC-4	情報フローの実施	A.13.1.3	ネットワークの分離
			A.13.2.1	情報転送の方針および手順
			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
			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

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	
3.1.4 共謀が関与しない場合の有害行為のリスクを減らすため、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 特定のセキュリティ機能および特権アカウントを含め、最小特権の原則を採用する。	AC-6	最小特権	A.9.1.2	ネットワークおよ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管理
	AC-6 (1)	最小特権 セキュリティ機能へのアクセスを認可	直接対応付け無し	
	AC-6 (5)	最小特権 特権アカウント	直接対応付け無し	
3.1.6 非セキュリティ機能にアクセスする時には、非特権アカウントまたは役割を使用する。	AC-6 (2)	最小特権 非セキュリティ機能への非特権アクセス	直接対応付け無し	
3.1.7 非特権ユーザーが特権機能を実行することを防止し、そのような機能の実行を監査ログに取り込む（capture）。	AC-6 (9)	最小特権 特権機能の使用をログ取得する	直接対応付け無し	
	AC-6 (10)	最小特権 非特権ユーザーが特権機能を実行することを禁止	直接対応付け無し	
3.1.8 ログオン試行失敗回数を限定する。	AC-7	不成功なログオンの試み	A.9.4.2	セキュリティに配慮したログオン手順
3.1.9 適用される CUI のルールに則って、プライバシーおよびセキュリティ通知を提示する。	AC-8	システム使用の通告	A.9.4.2	セキュリティに配慮したログオン手順
3.1.10 非アクティブ状態が一定時間経過後のデータのアクセスおよび閲覧を防止するために、隠蔽用パターンの表示によるセションロックを使用する。	AC-11	セションロック	A.11.2.8	無人状態にあるユーザー装置
			A.11.2.9	クリアデスクおよびクリアスクリーン方針
	AC-11 (1)	セションロックパターン隠蔽ディスプレイ	直接対応付け無し	

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
3.1.11 規定された条件が成立した場合には、ユーザーセションを（自動的に）終了させる。	AC-12	セション終結	直接対応付け無し
3.1.12 リモートアクセスセションを監視し、管理する。	AC-17 (1)	リモートアクセス 自動化監視／管理	直接対応付け無し
3.1.13 リモートアクセスセションの秘匿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 暗号を使った秘匿性の保護／完全性	直接対応付け無し
3.1.14 管理されたアクセス制御ポイント経由で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	直接対応付け無し

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	
3.1.15 特権コマンドのリモート実行およびセキュリティ関連情報へのリモートアクセスを認可する。	AC-17 (4)	遠隔アクセス 特権コマンド／アクセス	直接対応付け無し	
3.1.16 ワイヤレスアクセスの接続を許可する前に、そうしたアクセスを認可する。	AC-18	無線アクセス	A.6.2.1	モバイルデバイスポリシー
			A.13.1.1	ネットワーク管理
			A.13.2.1	情報転送のポリシーおよび手順
3.1.17 認証および暗号を使用してワイヤレスアクセスを保護する。	AC-18 (1)	無線アクセス 認証と暗号	直接対応付け無し	
3.1.18 モバイルデバイスの接続を管理する。	AC-19	モバイル装置のアクセス管理	A.6.2.1	モバイルデバイスの方針
			A.11.2.6	構外にある装置および資産のセキュリティ
			A.13.2.1	情報転送のポリシーおよび手順
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)	モバイルデバイスのアクセス管理 デバイス／筐体ベースの完全暗号	直接対応付け無し	
3.1.20 外部システムへの接続および使用を検証（verify）し、管理／限定する。	AC-20	外部システムの使用	A.11.2.6	構外の装置およ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	情報転送の方針および手順
	AC-20 (1)	外部システムの使用 認可された使用を限定	直接対応付け無し	
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限定する。	AC-20 (2)	外部システムの使用 ポータブルストレージデバイス	直接対応付け無し	
3.1.22 公衆アクセス可能なシステム上に掲載または処理される CUI を管理する。	AC-22	公開の情報内容	直接対応付け無し	

表 **D-2**：セキュリティ管理策に対する意識向上および訓練要件の対応付け

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 意識向上および訓練				
基本セキュリティ要件				
3.2.1 組織のシステムの管理者（manager）、システムアドミニストレーターおよびユーザーが、組織のシステムのセキュリティに関連する適用ポリシー、規格、および手順ならびに彼らの活動に関連するセキュリティリスクについて認識していることを確実にする。 **3.2.2** 職員が、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ように訓練されていることを確実にする。	AT-2	セキュリティ意識向上訓練	A.7.2.2	情報セキュリティ意識向上、教育および訓練
			A.12.2.1	マルウェアに対する管理策
	AT-3	役割ベースのセキュリティ訓練	A.7.2.2*	情報セキュリティ意識向上、教育および訓練
派生セキュリティ要件				
3.2.3 インサイダー脅威の潜在的兆候を認識し、報告するためのセキュリティ意識向上訓練を行う。	AT-2 (2)	セキュリティ意識向上訓練 インサイダー脅威	直接対応付け無し	

表 **D-3**：セキュリティ管理策に対する監査および説明責任要件の対応付け

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 監査および説明責任				
基本セキュリティ要件				
3.3.1 非合法的または認可されてないシステム活動に関する監視、分析、調査、報告を可能にするために必要な範囲で、システム監査ログおよび記録を作成し保持する。 **3.3.2** 個々のシステムユーザーの行動が、そのユーザーに対して一意に追跡可能であり、ユーザーが自らの行動に説明責任を負わせられるようにする。	AU-2	イベントログ取得	直接対応付け無し	
	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 *付加的監査情報*	*直接対応付け無し*	
	AU-6	監査記録の点検、分析、および報告	A.12.4.1	イベントログ取得
			A.16.1.2	情報セキュリティイベントの報告
			A.16.1.4	情報セキュリティイベントのアセスメントおよび決定
	AU-11	監査記録保持	A.12.4.1	イベントログ取得
			A.12.4.3	業務管理者及び運用担当者の作業ログ
	AU-12	監査記録生成	A.12.4.1	イベントログ取得
			A.16.1.7	エビデンスの収集
派生セキュリティ要件				
3.3.3 **ログ取得**されたイベントを見直し、更新する。	AU-2 (3)	イベントログ取得されたイベントの見直しと更新	直接対応付け無し	
3.3.4 監査ログ取得プロセスが失敗した場合にアラートを発する。	AU-5	監査ログ取得処理失敗への対応	直接対応付け無し	
3.3.5 非合法的または認可されてない、疑わしいまたは異常な行為の兆候を調査し対応するために、監査記録の見直し、分析および報告のプロセスを相互に関連づける。	AU-6 (3)	監査記録の点検、分析、および報告 監査記録リポジトリを相互に関連づけ	直接対応付け無し	
3.3.6 オンデマンドでの分析および報告をサポートするための監査記録の集約および報告書生成機能を提供する。	AU-7	監査記録情報の集約および報告書生成	直接対応付け無し	
3.3.7 監査記録にタイムスタン	AU-8	タイムスタンプ	A.12.4.4	クロックの同期

	プを生成するために、内部システムクロックを信頼できるタイムソース（時刻提供者）と比較および同期させるシステムケイパビリティを提供する。	AU-8 (1)	タイムスタンプ 信頼できるタイムソース（時刻提供者）との同期	直接対応付け無し
	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
3.3.8	監査情報および監査ログ取得ツールを、認可されてないアクセス、変更、およ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
3.3.9	監査ログ取得機能の管理を特権ユーザーの一部の者に限定する。	AU-9 (4)	監査情報の保護 特権ユーザーの少人数によるアクセス	直接対応付け無し

表 D-4：セキュリティ管理策に対する構成管理要件の対応付け[32]

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 個々のシステム開発ライフサイクル全体にわたり、組織が持つシステムの基本構成およびインベントリ（ハードウェア、ソフトウェア、ファームウェアおよび文書を含む）を規定し、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規定し、実施する。	CM-2	ベースライン構成	直接対応付け無し	
	CM-6	構成設定	直接対応付け無し	
	CM-8	システムコンポーネントのインベントリ	A.8.1.1	インベントリ
			A.8.1.2	資産のオーナー
	CM-8 (1)	システムコンポーネントのインベントリ 設置／除去時の更新	直接対応付け無し	
派生セキュリティ要件				
3.4.3 組織のシステムに対する変更を追跡、見直し、承認または非承認し、ログ取得する。	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 変更実施に先立って、セキュリティへのインパクトを分析する。	CM-4	セキュリティインパクト分析	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 組織のシステム変更に	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

[32] CM-7 (5) 「最小機能性ホワイトリスト登録ポリシー」は、CUI を包含するシステムへの保護強化を望む組織のために、CM-7 (4) 「最小機能性ブラックリスト登録ポリシー」に対する代替の一つとして列挙されている。CM-7 (5) は、「NIST SP 800-53」に従って、高いセキュリティ管理ベースラインにある連邦政府システムにだけ要求される。

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	
関する物理的および論理的アクセス制限を明確に定め、文書化し、承認し、実施する。			A.9.4.5	プログラムソースコードへのアクセス管理
			A.12.1.2	変更管理
			A.12.1.4	開発環境，テスト環境および運用環境の分離
			A.12.5.1	運用システムに関わるソフトウェアの導入

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	
3.4.6 必須なケイパビリティだけを提供するように組織のシステムを構成することにより、 最小機能性の原則を採用する。	CM-7	最小機能性	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 必須でないプログラム、機能、ポート、プロトコルおよびサービスの使用を制限、無効化または防止する。	CM-7 (1)	最小機能性 周期的見直し	直接対応付け無し	
	CM-7 (2)	最小機能性 プログラム実行を防止	直接対応付け無し	
3.4.8 「例外による拒否」（ブラックリスト登録）ポリシーを適用して認可されてないソフトウェア使用を防止する、あるいは「全拒否、例外による許可」（ホワイトリスト登録）ポリシーを適用して認可されたソフトウェア実行を許可する。	CM-7 (4)	最小機能性 認可されてないソフトウェア／ブラックリスト登録	直接対応付け無し	
	CM-7 (5)	最小機能性 認可されてないソフトウェア／ホワイトリスト登録	直接対応付け無し	
3.4.9 ユーザーがインストールしたソフトウェアを管理（control）し監視する。	CM-11	ユーザー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ールの制限

表 **D-5**：セキュリティ管理策に対する識別および認証要件の対応付け[33]

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 識別および認証				
基本セキュリティ要件				
3.5.1 システムのユーザー、ユーザーに代わって動作するプロセス、およびデバイスを識別する。	IA-2	識別および認証（組織のユーザー）	A.9.2.1	利用者登録および登録削除
	IA-3	デバイスの識別および認証	直接対応付け無し	
3.5.2 組織のシステムへのアクセスを許可する前提条件として、ユーザー、プロセスまたはデバイスのアイデンティティを認証（authenticate）（または検証（verify））する。	IA-5	オーセンティケータの管理	A.9.2.1	利用者登録および登録削除
			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
派生セキュリティ要件				
3.5.3 多要素認証を特権アカウントによるローカルおよびネットワークアクセスならびに非特権アカウントによるネットワークアクセスに使用する。	IA-2 (1)	識別および認証（組織のユーザー） 特権アカウントへのネットワークアクセス	直接対応付け無し	
	IA-2 (2)	識別および認証（組織のユーザー） 非特権アカウントへのネットワークアクセス	直接対応付け無し	
	IA-2 (3)	識別および認証（組織のユーザー） 特権アカウントへのローカルアクセス	直接対応付け無し	
3.5.4 特権および非特権アカウントによるネットワークアクセスに、リプレイ耐	IA-2 (8)	識別および認証（組織のユーザー） 特権アカウント（再生防止）へのネットワークアクセス	直接対応付け無し	

[33] IA-2(9)は、「NIST SP 800-53」の中位セキュリティ管理ベースラインに現在はない。ただし、次回の更新でベースラインに追加されることになっている。再生防止ケイパビリティなしに非特権アカウントに多要素認証を採用することは、CUI を通信するシステムに重大な脆弱性を生じさせる。

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	
性のある認証メカニズムを採用する。	IA-2 (9)	識別および認証（組織のユーザー） 非特権アカウント（再生防止）へのネットワークアクセス	直接対応付け無し	
3.5.5 定められた期間、ID の再利用を防止する。	IA-4	ID の管理	A.9.2.1	利用者登録および登録削除
3.5.6 定められた非アクティブな期間が過ぎた後、ID を無効化する。	IA-4	ID の管理	A.9.2.1	利用者登録および登録削除
3.5.7 新しいパスワードが作成される際には、パスワードの最小限の複雑性と文字の変更を強制する。	IA-5 (1)	オーセンティケータの管理 パスワードベース認証	直接対応付け無し	
3.5.8 指定された生成回数の間、パスワードの再利用を禁ずる。				
3.5.9 システムログオン時、常用（permanent）パスワードに即時変更することを条件として一時的パスワードの使用を許可する。				
3.5.10 暗号技術で保護されたパスワードのみを保存および伝送する。				
3.5.11 認証情報のフィードバックを隠す。	IA-6	オーセンティケータのフィードバック	A.9.4.2	セキュリティに配慮したログオン手順

表 **D-6**：セキュリティ管理策に対するインシデント対応要件の対応付け

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 準備、検知、分析、抑制、復旧およびユーザー対応活動を含め、組織のシステムに運用状態のインシデント対応ケイパビリティを確立する。 **3.6.2** インシデントを追跡、文書化し、組織内外の指定された担当者および／または機関に報告する。	IR-2	インシデント対応訓練	A.7.2.2*	情報セキュリティ意識向上、教育および訓練
	IR-4	インシデント取り扱い	A.16.1.4	情報セキュリティイベントのアセスメントおよび決定
			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	インシデント監視	直接対応付け無し	
	IR-6	インシデント報告	A.6.1.3 A.16.1.2	関係当局との連絡 情報セキュリティイベントの報告
	IR-7	インシデント対応の補佐	直接対応付け無し	
派生セキュリティ要件				
3.6.3 組織のインシデント対応ケイパビリティをテストする。	IR-3	インシデント対応テスト	直接対応付け無し	

表 **D-7**：セキュリティ管理策に対するメンテナンス要件の対応付け

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 組織のシステムのメンテナンスを行う。 **3.7.2** システムのメンテナンスを実行するために使われるツール、技法、メカニズム、および職員を管理する。	MA-2	被管理メンテナンス	A.11.2.4*	装置のメンテナンス
			A.11.2.5*	資産の移動
	MA-3	メンテナンスツール	直接対応付け無し	
	MA-3 (1)	メンテナンスツール 検査ツール	直接対応付け無し	
	MA-3 (2)	メンテナンスツール 検査媒体	直接対応付け無し	
派生セキュリティ要件				
3.7.3 オフサイトで行われるメンテナンスのために取り外される装置からすべての CUI がサニタイズ（情報除去）されていることを確実にする。	MA-2	被管理メンテナンス	A.11.2.4*	装置のメンテナンス
			A.11.2.5*	資産の移動
3.7.4 診断およびテストプログラムが入っている媒体を組織のシステムで使用する前に、悪意のあるコードの有無をチェックする。	MA-3 (2)	メンテナンスツール 検査媒体	直接対応付け無し	
3.7.5 外部ネットワーク接続を介して非ローカルメンテナンスセションを確立する際には多要素認証を要求し、非ローカルメンテナンスの完了時にはその接続を切断する。	MA-4	非ローカルメンテナンス	直接対応付け無し	
3.7.6 必要なアクセス認可のないメンテナンス職員のメンテナンス活動を監督する。	MA-5	メンテナンス職員	直接対応付け無し	

表 D-8：セキュリティ管理策に対する媒体保護要件の対応付け[34]

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 媒体保護				
基本セキュリティ要件				
3.8.1 紙とデジタル双方とも、CUI を含むシステムの媒体を保護する（すなわち、セキュアに保存し物理的に管理する）。 3.8.2 システム媒体上の CUI へのアクセスを、認可されたユーザーに限定する。 3.8.3 CUI を含むシステムの媒体を廃棄または再利用する前に、サニタイズ（情報除去）または破壊する。	MP-2	媒体アクセス	A.8.2.3	資産の取扱い
			A.8.3.1	リムーバブルメディアの管理
			A.11.2.9	クリアデスクおよびクリアスクリーン方針
	MP-4	媒体の保管	A.8.2.3	資産の取扱い
			A.8.3.1	リムーバブルメディアの管理
			A.11.2.9	クリアデスクおよびクリアスクリーン方針
	MP-6	媒体の情報除去	A.8.2.3	資産の取扱い
			A.8.3.1	リムーバブルメディアの管理
			A.8.3.2	媒体の処分
			A.11.2.7	装置のセキュリティを保った処分または再利用
派生セキュリティ要件				
3.8.4 CUI のマーキングと配布制限が必要な媒体にはその旨をマーキングする。	MP-3	媒体へのマーキング	A.8.2.2	情報のラベル付け
3.8.5 CUI を含む媒体へのアクセスを管理し、管理区域外での輸送中は、媒体に関する説明責任を維持する。	MP-5	媒体の輸送	A.8.2.3	資産の取扱い
			A.8.3.1	リムーバブルメディアの管理
			A.8.3.3	物理的媒体の輸送
			A.11.2.5	資産の移動
			A.11.2.6	構外にある装置および資産のセキュリティ

[34] セキュリティ要件に「緊急時対応計画作成」ファミリーが含まれなかったため、CP-9「情報システムのバックアップ」が、「媒体保護」ファミリーに包含されている。

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	
3.8.6	代替的な物理的保全措置によって保護されている場合を除き、デジタル媒体上に保存された CUI の秘匿性を輸送時に保護するため、暗号メカニズムを実装する。	MP-5 (4)	媒体の輸送暗号の保護	直接対応付け無し	
3.8.7	システムコンポーネント上のリムーバブルメディアの使用を管理する。	MP-7	媒体の使用	A.8.2.3	資産の取扱い
				A.8.3.1	リムーバブルメディアの管理
3.8.8	ポータブルストレージデバイスのオーナーを識別できない時には、そうしたデバイスの使用を禁止する。	MP-7 (1)	媒体の使用 オーナーがいない場合の使用を禁止	直接対応付け無し	
3.8.9	保管場所にあるバックアップ CUI の秘匿性を保護する。	CP-9	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施
				A.18.1.3	記録の保護

表 **D-9**：セキュリティ管理策に対する職員のセキュリティ要件の対応付け

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 職員のセキュリティ				
基本セキュリティ要件				
3.9.1 CUI を含む組織のシステムへのアクセスの認可に先立って、個人を審査する。	PS-3	職員審査	A.7.1.1	選考
	PS-4	職員解雇	A.7.3.1	雇用の終了または変更に関する責任
			A.8.1.4	資産の返却
3.9.2 退職や異動などの人事措置中、およびその後において、CUI を含む組織のシステムが保護されていることを確実にする。	PS-5	職員異動	A.7.3.1	雇用の終了または変更に関する責任
			A.8.1.4	資産の返却
派生セキュリティ要件	無し			

表 **D-10**：セキュリティ管理策に対する物理的保護要件の対応付け

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				
基本セキュリティ要件				
3.10.1　組織のシステム、装置、およびそれぞれの運用環境への物理的アクセスを、認可された個人に限定する。 **3.10.2**　組織のシステムの物理的施設および支援インフラを保護し、監視する。	PE-2	物理的アクセスの認可	A.11.1.2*	物理的入退管理策
	PE-4	伝送手段のアクセス管理	A.11.1.2	物理的入退管理策
			A.11.2.3	配線のセキュリティ
	PE-5	出力デバイスのアクセス管理	A.11.1.2	物理的入退管理策
			A.11.1.3	オフィス，部屋および施設のセキュリティ
	PE-6	物理的アクセスの監視	直接対応付け無し	
派生セキュリティ要件				
3.10.3　訪問者をエスコートし、その活動を監視する。	PE-3	物理的アクセス管理	A.11.1.1	物理的セキュリティ境界
			A.11.1.2	物理的入退管理策
3.10.4　物理的アクセスの監査ログを保持する。			A.11.1.3	オフィス，部屋および施設のセキュリティ
3.10.5　物理的アクセスデバイスを管理および監督する。				
3.10.6　代替作業サイトにおける CUI の保全措置を実施する。	PE―17	代替作業サイト	A.6.2.2	テレワーキング
			A.11.2.6	構外にある装置および資産のセキュリティ
			A.13.2.1	情報転送の方針および手順

表 **D-11**：セキュリティ管理策に対するリスクアセスメント要件の対応付け

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				
基本セキュリティ要件				
3.11.1 組織のシステム運用、および CUI に関連する処理、保存、または伝送から生ずる、組織運営（ミッション、機能、イメージ、評判を含む）、組織資産、およ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
派生セキュリティ要件				
3.11.2 システムおよびアプリケーションの脆弱性スキャンを定期的に、かつ、それらのシステムおよびアプリケーションに影響する新たな脆弱性が特定された場合に実施する。	RA-5	脆弱性精査	A.12.6.1*	技術的脆弱性の管理
	RA-5 (5)	脆弱性精査 特権アクセス	直接対応付け無し	
3.11.3 リスクアセスメントに従って、脆弱性を取り除く。	RA-5	脆弱性精査	A.12.6.1*	技術的脆弱性の管理

表 **D-12**：セキュリティ管理策に対するセキュリティアセスメント要件の対応付け

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				
基本セキュリティ要件				
3.12.1 組織のシステムのセキュリティ管理策を定期的にアセスメントし、その管理策の適用が有効かどうかを判断する。 **3.12.2** 組織のシステムの欠陥を修正し、脆弱性を軽減または排除することを意図した実施計画書を作成し、実施する。 **3.12.3** システムのセキュリティ管理策が継続的に有効であることを確実にするため、その管理策を継続的に監視する。	CA-2	セキュリティアセスメント	A.14.2.8	システムセキュリティのテスト
			A.18.2.2	情報セキュリティのための方針群および規格への準拠性
			A.18.2.3	技術的準拠性のレビュー
	CA-5	実施計画と中間目標	直接対応付け無し	
	CA-7	継続的監視	直接対応付け無し	
3.12.4 システムの境界、運用環境、セキュリティ要件の実装方法、および他のシステムとの関係または他のシステムへの接続について記述したシステムセキュリティ計画書を作成し、文書化し、定期的に更新する。	PL-2	システムセキュリティ計画	A.6.1.2	Information security coordination（情報セキュリティの調整）
派生セキュリティ要件	無し			

表 D-13：セキュリティ管理策に対するシステムおよび通信の保護要件の対応付け[35]

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 システムおよび通信の保護				
基本セキュリティ要件				
3.13.1 通信（すなわち、組織のシステムによって送受信される情報）を、組織のシステムの外部境界および主要な内部境界において監視、管理、および保護する。 3.13.2 組織のシステム内で効果的な情報セキュリティを促進するような、アーキテクチャー設計、ソフトウェア開発技法、およ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 A.13.1.3	ネットワーク管理策 ネットワークの分離
			A.13.2.1	情報転送の方針および手順
			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
派生セキュリティ要件				
3.13.3 システム管理機能からユーザー機能を分離する。	SC-2	アプリケーションパーティショニング	直接対応付け無し	
3.13.4 共有システム資源を経由した、認可されてない情報転送や意図しない情報転送を防止する。	SC-4	共有資源内の情報	直接対応付け無し	
3.13.5 内部ネットワークから物理的または論理的に分離された、公開（Publicly）アクセス可能なシステムコ	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	情報転送の方針および手順

[35] セキュリティ要件に「システムおよびサービス取得」ファミリーが含まれなかったため、SA-8「セキュリティエンジニアリング原則」が、「システムおよび通信の保護」ファミリーに包含されている。

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	
ンポーネント用のサブネットワークを実装する。			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　デフォルト設定によりネットワーク通信トラフィックを拒否、また例外によりネットワーク通信トラフィックを許可する（すなわち、全拒否、例外による許可）。	SC-7 (5)	境界保護 デフォルト設定による拒否／例外による許可	直接対応付け無し	
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接続を確立することと同時に、外部ネットワーク内にある資源へその他何らかの接続（すなわち、スプリットトンネリング）を介して通信することを防止する。	SC-7 (7)	境界保護 リモートデバイスへのスプリットトンネリング（*Split Tunneling*）を防止	直接対応付け無し	
3.13.8　代替的な物理的保全措置によって保護されている場合を除き、移送中の CUI の認可されてない開示を防止するために、暗号メカニズムを実装する。	SC-8	通信の秘匿性と完全性	A.8.2.3 A.13.1.1	資産の取扱い ネットワーク管理策
			A.13.2.1	情報転送の方針および手順
			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)	通信の秘匿性と完全性 暗号による保護、または代替的な物理的保護	直接対応付け無し	

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	
3.13.9 通信セション終了時、または定められた非アクティブ時間経過後、そのセションに関連するネットワーク接続を切断する。	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る暗号技術のための暗号鍵を設定し、管理する。	SC-12	暗号鍵の設定と管理	A.10.1.2	鍵管理
3.13.11 CUI の秘匿性保護には、FIPS 認証された暗号技術を採用する。	SC-13	暗号の保護	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、そのデバイスに存在するユーザーに対して使用中のデバイスを表示する。	SC-15	共同コンピューティングデバイス	A.13.2.1*	情報転送の方針および手順
3.13.13 モバイルコードの使用を管理および監視する。	SC-18	モバイルコード	直接対応付け無し	
3.13.14 インターネットプロトコルによる音声通信（VoIP）技術の使用を管理および監視する。	SC-19	インターネットプロトコル経由音声通信（VoIP）	直接対応付け無し	
3.13.15 通信セションの真正性（Authenticity）を保護する。	SC-23	セションの真正性	直接対応付け無し	
3.13.16 通信停止中の CUI の秘匿性を保護する。	SC-28	停止時の情報の保護	A.8.2.3*	資産の取扱い

表 **D-14**：セキュリティ管理策に対するシステムおよび情報の完全性要件の対応付け

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 システムおよび情報の完全性				
基本セキュリティ要件				
3.14.1　システムの欠陥をタイムリーに特定し、報告し、修正する。 **3.14.2**　組織のシステム内の指定された場所で、悪意のあるコードからの保護機能を提供する。 **3.14.3**　システムのセキュリティアラートおよび勧告を監視し、対応措置を講ずる。	SI-2	欠陥の改善	A.12.6.1	技術的脆弱性の管理
			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	情報セキュリティイベントの報告
	SI-3	悪意のあるコードからの保護	A.12.2.1	マルウェアに対する管理策
	SI-5	セキュリティアラート、勧告、および指令	A.6.1.4*	専門組織（special interest group）との連絡
派生セキュリティ要件				
3.14.4　悪意のあるコード保護メカニズムが新たにリリースされた場合、更新する。	SI-3	悪意のあるコードからの保護	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を実行すると共に、外部ソースからのファイルのリアルタイムスキャンを、ファイルがダウンロードされ、開かれ、実行される都度実行する。				
3.14.6　攻撃および潜在的攻撃の兆候を検知するために、出入する通信トラフィックを含めて組織のシステムを監視する。	SI-4	システムの監視	直接対応付け無し	
	SI-4 (4)	システムの監視 出入する通信トラフィック	直接対応付け無し	
3.14.7　組織のシステムの認可されてない使用を特定（identify）する。	SI-4	システムの監視	直接対応付け無し	

付属書 E

テーラリング基準

中位セキュリティ管理策ベースラインおよびテーラリング措置の一覧表

本付属書は、第 3 章に示されている CUI セキュリティ要件の策定に際して使用された[FIPS 200]とともにその情報源の一つとした[SP 800-53][36]中位ベースラインにあるセキュリティ管理策のリストを提示している。表 E-1 から表 E-17 には、NIST および NARA によって確立されたテーラリング（除外または調整）基準に従って、管理策に対して実行された特定のテーラリング措置が示されている。このテーラリング措置により、基本セキュリティ要件を補足する CUI 派生セキュリティ要件の開発が促進された[37]。 SP 800-53 中位ベースラインからセキュリティ管理策または拡張管理策をテーラリングする主な基準は以下の 3 つである。

- この管理策または拡張管理策は、連邦政府固有のものである（主に連邦政府の責任）。
- この管理策または拡張管理策は、CUI の秘匿性保護に直接関係していない[38]。
- この管理策または拡張管理策は、規定がなくても非連邦政府の組織により日常的に満たされると期待される[39]。

表 1 に示されている以下の記号は、表 E-1 から表 E-17 で講じられた特定のテーラリング措置、あるいはテーラリング措置が必要でなかったことを示す。

表 1 ：テーラリング措置を表す記号

テーラリング記号	テーラリング基準
NCO	CUI の秘匿性保護に直接関係しない。
FED	連邦政府固有、主に連邦政府の責任。
NFO	規定がなくても非連規定邦政府の組織により日常的に満たされると期待される。
CUI	CUI の基本または派生セキュリティ要件は、セキュリティ管理策、拡張管理策、または管理策／拡張管理策の特定要素を反映しており、対応関係をたどることができる。

[36] NIST Special Publication 800-53、Revision 4 から取得されている。なお、これらの表は、[SP 800-53B]の公開時に更新され、NIST Special Publication 800-53、Revision 5 に準拠する中位のセキュリティ管理策ベースラインへの更新を提供する予定である。中位のベースラインへの変更は、第 3 章の基本および派生セキュリティ要件の将来の更新に影響する。

[37] *同じテーラリング基準*が[FIPS 200]のセキュリティ要件にも適用され、第 3 章に示されている CUI 基本セキュリティ要件となっている。

[38] この文書の主な目的は、CUI の秘匿性を保護するための要件を規定することであるが、秘匿性と完全性のセキュリティ目標の間には密接な関係がある。したがって、[SP 800-53]中位ベースラインのセキュリティ管理策は、認可されてない開示に対する保護をサポートするとともに、認可されてない変更に対する保護もサポートする。

[39] 中位ベースラインからテーラリングによって除外されたセキュリティ管理策（つまり、NCO または NFO のいずれかとして特別にマークされ、表 E-1 から E-17 の濃い青色の網掛けで強調表示された管理策）は、多くの場合、組織の包括的なセキュリティプログラムの一部として含まれている。

表 **E-1**：アクセス管理の管理策のためのテーラリング措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		テーラリング措置
AC-1	アクセス管理ポリシーおよび手順	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／緊急アカウントの除去	NCO
AC-2 (3)	アカウント管理 ｜ 無効、非活動アカウント	NCO
AC-2 (4)	アカウント管理 ｜ 自動化監査行動	NCO
AC-3	アクセス実施	CUI
AC-4	情報フローの実施	CUI
AC-5	職務の分離	CUI
AC-6	最小特権	CUI
AC-6 (1)	最小特権 ｜ セキュリティ機能へのアクセス認可	CUI
AC-6 (2)	最小特権 ｜ 非セキュリティ機能への非特権アクセス	CUI
AC-6 (5)	最小特権 ｜ 特権アカウント	CUI
AC-6 (9)	最小特権 ｜ 特権機能の使用監査	CUI
AC-6 (10)	最小特権 ｜ 非特権ユーザーの特権機能実行の禁止	CUI
AC-7	不成功なログオンの試み	CUI
AC-8	システム使用の通告	CUI
AC-11	セションロック	CUI
AC-11 (1)	セションロック ｜ パターン隠蔽ディスプレイ	CUI
AC-12	セション終結	CUI
AC-14	識別または認証なしに許可される行動	FED
AC-17	リモートアクセス	CUI
AC-17 (1)	リモートアクセス ｜ 自動化監視／管理	CUI
AC-17 (2)	リモートアクセス ｜ 暗号使用の秘匿性／完全性の保護	CUI
AC-17 (3)	リモートアクセス ｜ 被管理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	CUI
AC-19	モバイルデバイスのアクセス管理	CUI
AC-19 (5)	モバイルデバイスのアクセス管理 ｜デバイス／筐体ベースの完全暗号	CUI
AC-20	外部システムの使用	CUI
AC-20 (1)	外部システムの使用 ｜認可された使用の限定	CUI
AC-20 (2)	外部システムの使用 ｜ポータブルストレージデバイス	CUI
AC-21	情報の共有	FED
AC-22	公開の情報内容	CUI

表 **E-2**：意識向上および訓練の管理策のためのテーラリング措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		テーラリング措置
AT-1	セキュリティ意識向上および訓練のポリシーおよび手順	NFO
AT-2	セキュリティ意識向上訓練	CUI
AT-2 (2)	セキュリティ意識向上 | インサイダー脅威	CUI
AT-3	役割ベースのセキュリティ訓練	CUI
AT-4	セキュリティ訓練の記録	NFO

表 **E-3**：監査および説明責任の管理策のためのテーラリング措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		テーラリング措置
AU-1	監査および説明責任のポリシーおよび手順	NFO
AU-2	監査イベント	CUI
AU-2 (3)	監査イベント ｜ 見直しおよび更新	CUI
AU-3	監査記録の内容	CUI
AU-3 (1)	監査記録の内容 ｜ 付加的監査情報	CUI
AU-4	監査保存容量	NCO
AU-5	監査ログ取得処理失敗への対応	CUI
AU-6	監査の点検、分析、および報告	CUI
AU-6 (1)	監査の点検、分析、および報告 ｜ 処理の統合	NCO
AU-6 (3)	監査の点検、分析、および報告 ｜ 監査リポジトリの相関	CUI
AU-7	監査情報の集約および報告生成	CUI
AU-7 (1)	監査情報の集約および報告生成 ｜ 自動処理	NCO
AU-8	タイムスタンプ	CUI
AU-8 (1)	タイムスタンプ ｜ 信頼できるタイムソース（時刻提供者）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 ｜ 特権ユーザーの一部によるアクセス	CUI
AU-11	監査記録の保存	NCO
AU-12	監査生成	CUI

表 **E-4**：セキュリティアセスメントと認可の管理策のためのテーラリング措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		テーラリング措置
CA-1	セキュリティアセスメントおよび認可のポリシーおよび手順	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 ｜ 独立アセッサー	NFO
CA-3	システム相互接続	NFO
CA-3 (5)	システム相互接続 ｜ 外部システム接続の制限	NFO
CA-5	実施計画と中間目標	CUI
CA-6	セキュリティ認可	FED
CA-7	継続的監視	CUI
CA-7 (1)	継続的管理 ｜ 独立アセスメント	NFO
CA-9	内部システム接続	NFO

表 **E-5**：構成管理の管理策ためのテーラリング措置[40]

NIST SP 800-53 中位ベースラインセキュリティ管理策		テーラリング措置
CM-1	構成管理のポリシーおよび手順	NFO
CM-2	ベースライン構成	CUI
CM-2 (1)	ベースライン構成 ｜ 見直しおよび更新	NFO
CM-2 (3)	ベースライン構成 ｜ 以前の構成の保持	NCO
CM-2 (7)	ベースライン構成 ｜ 高リスク区域用にシステム、コンポーネント、およびデバイスを構成	NFO
CM-3	構成変更管理	CUI
CM-3 (2)	構成変更管理 ｜ 変更をテスト／確認／文書化	NFO
CM-4	セキュリティインパクト分析	CUI
CM-5	変更のためのアクセス制限	CUI
CM-6	構成設定	CUI
CM-7	最小機能性	CUI
CM-7 (1)	最小機能 ｜ 周期的見直し	CUI
CM-7 (2)	最小機能 ｜ プログラム実行の防止	CUI
CM-7(4)(5)	最小機能 ｜ 非認可または認可ソフトウェア／ブラックリスト登録またはホワイトリスト登録	CUI
CM-8	システムコンポーネントのインベントリ	CUI
CM-8 (1)	システムコンポーネントのインベントリ ｜ 設置／除去時の更新	CUI
CM-8 (3)	システムコンポーネントのインベントリ ｜認可されてないコンポーネントの自動検知	NCO
CM-8 (5)	システムコンポーネントのインベントリ ｜ コンポーネントの非重複記述	NFO
CM-9	構成管理の計画	NFO
CM-10	ソフトウェア用途の制限	NCO
CM-11	ユーザーがインストールしたソフトウェア	CUI

[40] CM-7(5)「最小機能*ホワイトリスト登録*」は、「NIST SP800-53」によれば、中位セキュリティ管理策ベースラインには入っていない。しかしながら、これは、*ブラックリスト登録*に代わる選択的かつ強力なポリシーとして提供されている。

表 **E-6**：緊急時対応計画作成の管理策のためのテーラリング措置[41]

NIST SP 800-53 中位ベースラインセキュリティ管理策		テーラリング措置
CP-1	緊急時対応計画作成のポリシーおよび手順	NCO
CP-2	緊急時対応計画	NCO
CP-2 (1)	緊急時対応計画 ｜ 関連計画との調整	NCO
CP-2 (3)	緊急時対応計画 ｜必須なミッション／事業機能の再開	NCO
CP-2 (8)	緊急時対応計画 ｜ 重要資産の特定	NCO
CP-3	緊急時対応の訓練	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 ｜ 関連計画との調整	NCO
CP-6	代替保管サイト	NCO
CP-6 (1)	代替保管サイト ｜ 主サイトからの分離	NCO
CP-6 (3)	代替保管サイト ｜ アクセス容易性	NCO
CP-7	代替処理サイト	NCO
CP-7 (1)	代替処理サイト ｜ 主サイトからの分離	NCO
CP-7 (2)	代替処理サイト ｜ アクセス容易性	NCO
CP-7 (3)	代替処理サイト ｜ サービス優先順位	NCO
CP-8	遠隔通信サービス	NCO
CP-8 (1)	遠隔通信サービス ｜ サービス提供優先順位	NCO
CP-8 (2)	遠隔通信サービス ｜ 単一障害発生点	NCO
CP-9	システムのバックアップ	CUI
CP-9 (1)	システムのバックアップ ｜ 信頼性／完全性のテスト	NCO
CP-10	システムの復旧および再構成	NCO
CP-10 (2)	システムの復旧および再構成 ｜ トランザクションの復旧	NCO

[41] CP-9 は、「緊急時対応計画作成」ファミリーがセキュリティ要件に含まれていなかったため、付録 D の「媒体保護」ファミリーのセキュリティ管理策に包含されている。

表 **E-7**：識別および認証の管理策のためのテーラリング措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		テーラリング措置
IA-1	識別および認証のポリシーおよび手順	NFO
IA-2	識別および認証（組織のユーザー）	CUI
IA-2 (1)	識別および認証（組織のユーザー） ｜特権アカウントへのネットワークアクセス	CUI
IA-2 (2)	認識および認証（組織のユーザー） ｜非特権アカウントへのネットワークアクセス	CUI
IA-2 (3)	識別および認証（組織のユーザー） ｜特権アカウントへのローカルアクセス	CUI
IA-2 (8)	識別および認証（組織のユーザー） ｜特権アカウント（再生防止）へのネットワークアクセス	CUI
IA-2 (9)	識別および認証（組織のユーザー） ｜非特権アカウント（再生防止）へのネットワークアクセス	CUI
IA-2 (11)	識別および認証（組織のユーザー）｜リモートアクセス（分離デバイス）	FED
IA-2 (12)	識別および認証（組織のユーザー）｜*PIV* クレデンシャルの受領	FED
IA-3	デバイスの識別および認証	CUI
IA-4	ID の管理	CUI
IA-5	オーセンティケータの管理	CUI
IA-5 (1)	オーセンティケータの管理｜パスワードベース認証	CUI
IA-5 (2)	オーセンティケータの管理｜*PKI* ベース認証	FED
IA-5 (3)	オーセンティケータの管理 ｜対面（*IN-PERSON*）または信頼されたサードパーティ登録	FED
IA-5 (11)	オーセンティケータの管理｜ハードウェアトークンベース認証	FED
IA-6	認証符号のフィードバック	CUI
IA-7	暗号モジュール認証	FED
IA-8	識別および認証（非組織ユーザー）	FED
IA-8 (1)	識別および認証（非組織ユーザー） ｜他の機関からの *PIV* クレデンシャルの受領	FED
IA-8 (2)	識別および認証（非組織ユーザー） ｜サードパーティのクレデンシャルの受領	FED
IA-8 (3)	識別および認証（非組織ユーザー）｜*FICAM* 承認済み製品の使用	FED
IA-8 (4)	識別および認証（非組織ユーザー）｜*FICAM* 発行プロファイルの使用	FED

表 **E-8**：インシデント対応の管理策のためのテーラリング措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		テーラリング措置
IR-1	インシデント対応のポリシーおよび手順	NFO
IR-2	インシデント対応訓練	CUI
IR-3	インシデント対応テスト	CUI
IR-3 (2)	インシデント対応テスト ｜ 関連計画との調整	NCO
IR-4	インシデント取扱	CUI
IR-4 (1)	インシデント取扱 ｜ 自動化インシデント取扱プロセス	NCO
IR-5	インシデント監視	CUI
IR-6	インシデント報告	CUI
IR-6 (1)	インシデント報告 ｜ 自動化報告	NCO
IR-7	インシデント対応の補佐	CUI
IR-7 (1)	インシデント対応の補佐 ｜ 情報／支援の可用性に対する自動支援	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ためのテーラリング措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		テーラリング措置
MA-1	システムメンテナンスのポリシーおよび手順	NFO
MA-2	被管理メンテナンス	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 ｜ 検査ツール	CUI
MA-3 (2)	メンテナンスツール ｜ 検査媒体	CUI
MA-4	非ローカルメンテナンス	CUI
MA-4 (2)	非ローカルメンテナンス ｜ 非ローカルメンテナンスの文書化	NFO
MA-5	メンテナンス職員	CUI
MA-6	時宜を得たメンテナンス	NCO

表 **E-10**：媒体保護の管理策のためのテーラリング措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		テーラリング措置
MP-1	媒体の保護ポリシーおよび手順	NFO
MP-2	媒体へのアクセス	CUI
MP-3	媒体へのマーキング	CUI
MP-4	媒体の保管	CUI
MP-5	媒体の輸送	CUI
MP-5 (4)	媒体の輸送 ｜ 暗号保護	CUI
MP-6	媒体の情報除去	CUI
MP-7	媒体の使用	CUI
MP-7 (1)	媒体の使用 ｜ オーナーがいない場合の使用を禁止	CUI

表 **E11**：物理的および環境的保護の管理策のためのテーラリング措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		テーラリング措置
PE-1	物理的および環境的保護のポリシーおよび手順	NFO
PE-2	物理的アクセスの認可	CUI
PE-3	物理的アクセスの管理	CUI
PE-4	通信媒体のアクセス管理	CUI
PE-5	出力デバイスのアクセス管理	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 ｜ 侵入警報／監視装置	NFO
PE-8	訪問者のアクセス記録	NFO
PE-9	電力装置と敷設ケーブル	NCO
PE-10	緊急遮断	NCO
PE-11	非常用電源	NCO
PE-12	非常用照明	NCO
PE-13	防火	NCO
PE-13 (3)	防火 ｜ 自動消火	NCO
PE-14	温度および湿度管理	NCO
PE-15	水害保護	NCO
PE-16	引渡および撤去	NFO
PE-17	代替作業サイト	CUI

表 **E-12**：計画作成の管理策のためのテーラリング措置

NIST SP 800-53 中位ベースラインセキュリティ管理		テーラリング措置
PL-1	セキュリティ計画作成のポリシーおよび手順	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｜他の組織との計画／調整	NFO
PL-4	行動ルール	NFO
PL-4 (1)	行動ルール｜ソーシャルメディアおよびネットワーキングの制限	NFO
PL-8	情報セキュリティアーキテクチャー	NFO

表 **E-13**：職員のセキュリティの管理策のためのテーラリング措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		テーラリング措置
PS-1	職員のセキュリティポリシーおよび手順	NFO
PS-2	地位リスク（Position Risk）明示	FED
PS-3	職員審査	CUI
PS-4	職員解雇	CUI
PS-5	職員異動	CUI
PS-6	アクセス協定	NFO
PS-7	サードパーティ職員のセキュリティ	NFO
PS-8	職員制裁規定	NFO

表 **E-14**：リスクアセスメントの管理策のためのテーラリング措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		テーラリング措置
RA-1	リスクアセスメントのポリシーおよび手順	NFO
RA-2	セキュリティのカテゴリー化	FED
RA-3	リスクアセスメント	CUI
RA-5	脆弱性検査（scanning）	CUI
RA-5 (1)	脆弱性検査 ｜ ツールケイパビリティの更新	NFO
RA-5 (2)	脆弱性検査 ｜ 頻繁に／新たな精査に先行して／特定された時に更新	NFO
RA-5 (5)	脆弱性検査 ｜ 特権アクセス	CUI

表 **E-15**：システムとサービス取得の管理策のためのテーラリング措置[42]

NIST SP 800-53 中位ベースラインセキュリティ管理策		テーラリング措置
SA-1	システムおよびサービス取得のポリシーおよび手順	NFO
SA-2	資源の配分	NFO
SA-3	システム開発ライフサイクル	NFO
SA-4	取得プロセス	NFO
SA-4 (1)	取得プロセス ｜ セキュリティ管理策の機能特性	NFO
SA-4 (2)	取得プロセス ｜ セキュリティ管理策のための企画／実施情報	NFO
SA-4 (9)	取得プロセス ｜ 機能／ポート／プロトコル／使用中サービス	NFO
SA-4 (10)	取得プロセス ｜ 承認済み *PIV* 製品の使用	NFO
SA-5	システムの文書化	NFO
SA-8	セキュリティエンジニアリング原則	CUI
SA-9	外部システムサービス	NFO
SA-9 (2)	外部システム ｜ 機能／ポート／製品／サービスの特定	NFO
SA-10	ディベロッパー構成管理	NFO
SA-11	ディベロッパーセキュリティのテストおよび評価	NFO

[42] 「システムとサービス取得」ファミリーはセキュリティ要件に含まれなかったため、SA-8 は、付属書 D の「システムおよび通信の保護」ファミリーのセキュリティ管理策に包含されている。

表 **E-16**：システムおよび通信の保護の管理策のためのテーラリング措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		テーラリング措置
SC-1	システムおよび通信保護のポリシーおよび手順	NFO
SC-2	アプリケーションパーティショニング	CUI
SC-4	共有資源内の情報	CUI
SC-5	サービス拒否（DoS）に対する保護	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 ｜ 外部遠隔通信サービス	NFO
SC-7 (5) SC-7 (7)	境界保護 ｜デフォルト設定による拒否／例外による許可 境界保護 ｜ リモートデバイスへのスプリットトンネリング（*Sprit Tunneling*）を防止	CUI CUI
SC-8	通信の秘匿性と完全性	CUI
SC-8 (1) SC-10	通信の秘匿性および完全性 ｜ 暗号によるまたは代替的な物理的保護 ネットワークの切断	CUI CUI
SC-12	暗号鍵の設定と管理	CUI
SC-13	暗号の保護	CUI
SC-15	共同コンピューティングデバイス	CUI
SC-17	公開鍵インフラ証明書	FED
SC-18	モバイルコード	CUI
SC-19	インターネットプロトコル経由音声通信（VoIP）	CUI
SC-20 SC-21	セキュアネーム／アドレス解決サービス（Secure Name / Address Resolution Service） セキュアネーム／アドレス解決サービス（Secure Name / Address Resolution Service）	NFO NFO
SC-22	ネーム／アドレス解決サービス用のアーキテクチャーおよび規定	NFO
SC-23	セションの真正性	CUI
SC-28	停止時の情報の保護	CUI
SC-39	プロセスの遮断	NFO

表 **E-17**：システムおよび情報の完全性の管理策のためのテーラリング措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		テーラリング措置
SI-1	システムおよび情報の完全性のポリシーおよび手順	NFO
SI-2	欠陥の改善	CUI
SI-2 (2)	欠陥の改善 ｜ 自動化された欠陥改善ステイタス	NCO
SI-3	悪意のあるコードに対する保護	CUI
SI-3 (1)	悪意のあるコードに対する保護 ｜ 集中管理	NCO
SI-3 (2)	悪意のあるコードに対する保護 ｜ 自動更新	NCO
SI-4	システムの監視	CUI
SI-4 (2)	システムの監視 ｜ リアルタイム用の自動化ツール	NCO
SI-4 (4)	システムの監視 ｜ 出入通信トラフィック	CUI
SI-4 (5)	システムの監視 ｜ システム生成によるアラート	NFO
SI-5	セキュリティアラート、勧告、および指令	CUI
SI-7	ソフトウェア、ファームウェア、および情報の完全性	NCO
SI-7 (1)	ソフトウェア、ファームウェア、および情報の完全性 ｜ 完全性チェック	NCO
SI-7 (7)	ソフトウェア、ファームウェア、および情報の完全性 ｜ 探知と対応の統合	NCO
SI-8	スパムに対する保護	NCO
SI-8 (1)	スパムに対する保護 ｜ 集中管理	NCO
SI-8 (2)	スパムに対する保護 ｜ 自動更新	NCO
SI-10	情報インプットの認証	NCO
SI-11	エラーの取扱	NCO
SI-12	情報の取扱および保持	FED
SI-16	記憶保護	NFO