NIST SP（特別出版物） **800-171**
Revision 1 （改訂 1）

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**
パトリック・ヴィスクーソ **PATRICK VISCUSO**
ゲーリー・ギサニー **GARY GUISSANIE**
ケリー・デンプシー **KELLEY DEMPSEY**

本出版物は以下から無料で入手可能：
https://doi.org/10.6028/NIST.SP.800-171r1

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

■■■

㈱エヴァアビエーション　info@EvaAviation.com　訳　2017. 03. 24（認証の日）
文書の開示に当たっては事前に NIST から承認を得ております。(2017.05.18)
本文書は、原典に沿ってできるだけ忠実に翻訳するよう努めていますが、 完全性、正確性を保証するものではありません。当社は、本文書に記載されている情報より生じる損失または損 害に対して、いかなる人物あるいは団体についても責任を負うものでは ありません。

NIST SP（特別出版物） **800-171**
Revision（改訂） 1

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
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*）

パトリック・ヴィスクーソ
マーク・リドル
情報セキュリティ監督室
国立公文書館（*NARA*）

ゲーリー・ギサニー
防衛分析研究所
国防総省補佐官

本出版物は以下から無料で入手可能：
https://doi.org/10.6028/NIST.SP.800-171r1

2016 年 **12** 月
2018 年 6 月 7 日までの改訂を含む

米国商務省
ペニー・プリツカー *Penny Pritzker* 長官

米国標準技術研究所（NIST）
ウィリー・メイ *Willie May*、標準・技術担当商務次官および部長

典拠（Authority）

本出版物は、2014 年の FISMA（「連邦情報セキュリティ近代化法」: Federal Information Security Modernization Act of 2014）、合衆国法典（U.S.C.）第 44 編・第 3551 条、および公法（P.L.）113 条-283 条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からなる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システムへの政策権限を執行する関係連邦政府当局者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。この指針は、行政管理予算局（OMB：Office of Management and Budget）通達 A-130 の要件を満たしている。

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。しかしながら、NIST への帰属を明らかにすることには感謝する。

米国標準技術研究所（NIST）特別出版物（SP）800-171　125 ページ（2016 年 12 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.800-171r1

試行的手順や概念を適切に説明するために、文中に一定の商業組織、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、あるいは必然的に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図しているものではない。

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。上記以外のすべてのコンピュータ・セキュリティ部門の出版物は、以下から入手可能である。 http://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
電子メール：sec-cert@nist.gov

全コメントは FIA(Freedom of Information Act)に基づく公開対象となる

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、試験、試験方法、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、連邦政府が指定された任務（mission）および事業運用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、以下の場合における CUI の秘匿性（confidentiality）を保護するための一連の推奨要件を連邦政府機関に提供するものである。すなわち、(i) CUI が非連邦政府組織およびシステムに存在する場合、(ii) 非連邦政府組織が CUI を連邦政府機関を代行して収集・維持しているのではない、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、(iii) CUI の秘匿性は CUI カテゴリーまたはサブカテゴリーを認可する法律、規則、または政府横断のポリシーによって規定され、「CUI レジストリー」に記載されるが、そうした秘匿性を保護するための特定の保全（safeguarding）要件が存在しない場合である。本要件は、CUI を処理、格納、伝送またはそれらの構成要素にセキュリティ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構成要素に適用される。本要件は、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書（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

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）、大統領令（Executive Order）13556、FIPS 出版物 199、FIPS 出版物 200、FISMA, NIST SP 800-53、非連邦政府システム（Nonfederal Systems）、セキュリティ評価（Security Assessment）、セキュリティ管理策（Security Control）、セキュリティ要件（Security Requirement）。

謝辞

著者は、キャロル・ベイルス（Carol Bales）、マット・バレット（Matt Barrett）、ジョン・ボエンズ（Jon Boyens）、デヴィン・ケイシー（Devin Casey）、クリス・エンロー（Chris Enloe）、ジム・フォッティ（Jim Foti）、ロブ・グレン（Rob Glenn）、リッチ・グローバート（Rich Graubart）、ヴィッキー・ミケッティ（Vicki Michetti）、マイケル・ニールス（Michael Nieles）、パット・オーレイリー（Pat O 'Reilly）、カレン・クイグ（Karen Quigg）、メアリー・トーマス（Mary Thomas）、マット・ショル（Matt Scholl）、ムルギ・スパーヤ（Murugiah Souppaya）、およびパット・トス（Pat Toth）の貢献に感謝し、またそれを高く評価する。彼らの思慮深く建設的な意見は、本出版物の全般的な品質、完璧性、および有用性を高めている。ペギー・ハイメス（Peggy Himes）とエリザベス・レノン（Elizabeth Lennon）には、彼らの優れた管理および技術編集支援に対して、心からの感謝を表明する。

注意事項

FISMAは、連邦政府機関が、下記の情報への不正なアクセス、利用、開示、通信の途絶、改ざん、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。すなわち、(i) 政府機関により、または政府機関に代わって、(ii) 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で、収集・維持される情報である。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勧告（recommnend）している。これは、FISMAで規定されている情報セキュリティ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従う責任を変えるものでもない。

本出版物で適用を勧告されている要件は、「FIPS 200」および「NIST SP 800-53」における中位セキュリティ管理基準（baseline）ならびに提案中のCUI規則（32 CFR Part 2002, *「管理対象非機密情報」*）に基づいた（delived from）ものである。セキュリティ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」のセキュリティ要件と「NIST SP 800-53」のセキュリティ管理策に適用される適応規準（tailoring criteria）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、この適応規準は、非連邦政府のシステムと組織における権限のない開示から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「NIST 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 というセキュリティ目的に加えて、*完全性* および *可用性* という目的も、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的を支えているからである。本出版物の勧告に関心を持ち、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セキュリティ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。こうした脅威への対処は重要なことである。なぜなら、多くの組織は、ミッションと事業の成功において、それぞれの情報技術インフラに依存しているからである。

本出版物への期待

2010 年 11 月 04 日付の大統領令 13556『管理対象非機密情報（*CUI:Controlled Unclassified Information*）』では、CUI 執行機関（Executive Agent）として指定された米国国立公文書館（NARA）は CUI プログラムを履行するために必要な指令を開発・発行しなければならない、と定めている。この任務および、連邦政府横断の共通ポリシーと業務手続きを確立するという CUI プログラムのミッションと整合するように、NARA は、2016 年に、CUI に必要とされる政府横断の管理策要件と標記（marking）を確立するための最終版の連邦政府規則を発行している。この連邦政府規則は、一旦制定されると、CUI プログラムによって確立された標準的な保全措置（safeguards）、標記、配付、および管理除外に関する要件は、行政府全機関に統一的に適用することが義務付けられるものになる。

*連邦政府情報システム*に関して、中位秘匿性影響レベルで CUI を保護するための連邦政府規則の要件は、OMB によって設定された適用可能なポリシー、および NIST 発行の適用可能な政府横断の規格と指針に基づいている。この規則が、OMB および NIST によって既に定められているポリシー、規格、および指針を生み出すことにはならない。しかしながら、この提案中の規則は、行政府全体で一貫した方法によるポリシーの厳守と、規格および指針の利用を必要とするものであり、それにより、連邦政府機関およびその契約者を含む非連邦政府パートナーに対して、現時点の複雑さを低減するものになるであろう。

連邦政府内 CUI の保全措置要件の明確化に加えて、NARA は、「SP 800-171」を NIST と共同して開発し、非連邦政府の組織およびシステムに存在する CUI を保護するセキュリティ要件を明確にすることによって、非連邦政府組織に関するこれらの要件の潜在的影響を軽減する措置を講じている。これは、契約者を含む非連邦政府組織が、政府固有の取組み方を使おうとするのではなく、自ら既に構築しているシステムや業務手順等を使うことによってセキュリティ要件に準拠することに役立つであろう。それはまた、非連邦政府のシステムに適応されたすべての CUI セキュリティニーズのための標準化された一律の要件群を提供することになり、非連邦政府組織が、法令および規則上の要件に準拠すること、そして CUI を保護するための保全措置を一貫して実装することを可能にするであろう。

最後に、NARA はまた、CUI 執行機関としての立場で、2017 年に、「連邦政府調達規則」（FAR）の単一条項を提出する計画である。その条項は、提案中の連邦政府 CUI 規則および「SP 800-171」に包含される要件を契約事業者に適用するものである。これは、標準化をさらに促進し、契約条項の現在の範囲と類型に従おうとしている相当数の非連邦政府組織に恩恵をもたらすものになろう。現在は、同一の情報に対して、連邦政府の複数機関から、異なる要件や相反する指導があり、それが混乱や非効率性を生じさせているからである。このような単一 FAR 条項を定める正式プロセスが始まるまでは、「NIST SP 800-171」の要件が、連邦政府法および連邦政府規則の要件に従う連邦政府契約で参照されることになるだろう。なお、必要に応じ「SP 800-171」は、提案中の連邦政府 CUI 規則および FAR 条項との一貫性を保持するために、更新されることがある。

情報システム（Information System）という用語の定義

法、規則、政府横断のポリシーによって規定されないかぎり、本出版物における*情報システム（information system）*という用語は*システム（system）*という用語に置き換えられている。この変更は、汎用情報システム、産業用のプロセス制御システム、サイバーフィジカルシステム、*IoT（Internet of Things）*を構成する個々の装置などを含む情報システムのより広範な、全体論的な定義を反映したものである。コンピュータ処理プラットフォームとテクノロジーはいよいよ全世界にくまなく展開されつつあり、それぞれのシステムおよび構成要素は有線または無線通信により結合されることで、CUI の滅失または毀損による感染性----そうした現象によって有害な結果を招く可能性----は増大している。

重要インフラストラクチャー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『重要インフラストラクチャー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*） 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、「NIST SP 800-53」および「ISO/IEC 27001」のセキュリティ管理策との直接的な対応付け（mapping）を、本出版物の付属書 D に見ることができる。これらの管理策は、識別・保護・検知・対応・回復という「サイバーセキュリティフレームワーク」中核機能に関連付けられた特定のカテゴリーとサブカテゴリーにも対応している。この対応付け情報は、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

NIST SP 800-53 の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://www.nist.gov/file/372651 を参照。

NIST SP 800-171 の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/publications/detail/sp/800-171/rev-1/final を参照。

目次

Errata

This table contains changes that have been incorporated into Special Publication 800-171. Errata updates can include corrections, clarifications, or other minor changes in the publication that are either *editorial* or *substantive* in nature.

DATE	TYPE	CHANGE	PAGE
11-28-2017	Editorial	CAUTIONARY NOTE call out box, third paragraph: Change "publications" to "publication"	iv
11-28-2017	Editorial	EXPECTATIONS FOR THIS PUBLICATION call out box, third paragraph: Change "in compliance" to "comply"	v
11-28-2017	Editorial	FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY call out box: Delete "See http://www.nist.gov/cyberframework."	vii
11-28-2017	Editorial	FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY call out box: Change "Once identified, those controls can be located in" to "These controls are also mapped to"	vii
11-28-2017	Substantive	FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY call out box: Add "Additional Resources – Mapping NIST Special Publication 800-53 security controls to the Cybersecurity Framework: https://www.nist.gov/file/372651. Mapping NIST Special Publication 800-171 requirements to the Cybersecurity Framework: https://www.nist.gov/cyberframework/industry-resources"	vii
11-28-2017	Editorial	Chapter One, Section 1.1, second paragraph, first bullet: Change "moderate confidentiality impact" to "moderate confidentiality"	2
11-28-2017	Editorial	Chapter One, Section 1.1: Replace Footnote 10 with "NIST Special Publication 800-171A provides assessment procedures to help organizations determine compliance to the security requirements in Chapter Three"	2
11-28-2017	Editorial	Chapter One, Section 1.1, fourth paragraph: Change "particular specified" to "specified"	3
11-28-2017	Editorial	Chapter One, Section 1.1, fifth paragraph: Change "as long as" to "if"	3
11-28-2017	Editorial	Chapter One, Section 1.1, fifth paragraph: Delete "all of"	3
11-28-2017	Editorial	Chapter Three, first paragraph: Change "through the use of" to "using"	8
11-28-2017	Editorial	Chapter Three, third paragraph: Change "whether or not" to "whether"	8
11-28-2017	Substantive	Chapter Three, after fourth paragraph: Add call out box "THE MEANING OF ORGANIZATIONAL SYSTEMS"	9
11-28-2017	Substantive	Chapter Three, Section 3.1, Basic Security Requirement 3.1.1: Change "or" to "and"	9
11-28-2017	Substantive	Chapter Three, Section 3.3, Basic Security Requirement 3.3.1: Delete ", protect,"	10
11-28-2017	Substantive	Chapter Three, Section 3.4, Derived Security Requirement 3.4.3: Change "approve/disapprove" to "approve or disapprove"	11
11-28-2017	Substantive	Chapter Three, Section 3.4, Derived Security Requirement 3.4.7: Change "and" to "or"	11
11-28-2017	Substantive	Chapter Three, Section 3.5, Basic Security Requirement 3.5.1: Change "or" to "and"	11
11-28-2017	Substantive	Chapter Three, Section 3.6, Basic Security Requirement 3.6.1: Delete "adequate"	12

DATE	TYPE	CHANGE	PAGE
11-28-2017	Substantive	Chapter Three, Section 3.7, Basic Security Requirement 3.7.2: Delete “effective”	12
11-28-2017	Substantive	Chapter Three, Section 3.9, Basic Security Requirement 3.9.2: Delete “CUI and”	13
11-28-2017	Editorial	Chapter Three, Section 3.10, Derived Security Requirement 3.10.6: Delete “(e.g., telework sites)”	13
11-28-2017	Substantive	Chapter Three, Section 3.14, Basic Security Requirement 3.14.1: Delete “information and”	15
11-28-2017	Substantive	Chapter Three, Section 3.14, Basic Security Requirement 3.14.3: Delete “appropriate”	15
11-28-2017	Editorial	Chapter Three, Section 3.14, Basic Security Requirement 3.14.3: Change “actions” to “action”	15
11-28-2017	Editorial	Appendix A, References: Add URL to 32 CFR Part 2002, Controlled Unclassified Information	17
11-28-2017	Substantive	Appendix A, References (Standards, Guidelines, and Instructions): Add “National Institute of Standards and Technology Special Publication 800-171A (Draft), *Assessing Security Requirements for Controlled Unclassified Information*”	17
11-28-2017	Substantive	Appendix D, Table D-1, Basic Security Requirement 3.1.1: Change “or” to “and”	29
11-28-2017	Substantive	Appendix D, Table D-3, Basic Security Requirement 3.3.1: Delete “, protect,”	33
11-28-2017	Editorial	Appendix D, Table D-3, Basic Security Requirement 3.3.1: Add AU-11 to SP 800-53 mapping	33
11-28-2017	Substantive	Appendix D, Table D-4, Derived Security Requirement 3.4.3: Change “approve/disapprove” to “approve or disapprove”	35
11-28-2017	Substantive	Appendix D, Table D-4, Derived Security Requirement 3.4.7: Change “and” to “or”	36
11-28-2017	Editorial	Appendix D, Table D-4, Derived Security Requirement 3.4.7: Add “programs”	36
11-28-2017	Editorial	Appendix D, Table D-5, Basic Security Requirement 3.5.1: Add IA-3 to SP 800-53 mapping	37
11-28-2017	Substantive	Appendix D, Table D-5, Basic Security Requirement 3.5.1: Change “or” to “and”	37
11-28-2017	Substantive	Appendix D, Table D-6, Basic Security Requirement 3.6.1: Delete “adequate”	39
11-28-2017	Substantive	Appendix D, Table D-6, Derived Security Requirement 3.6.3: Delete IR-3(2) from SP 800-53 mapping	39
11-28-2017	Substantive	Appendix D, Table D-7, Basic Security Requirement 3.7.2: Delete “effective”	40
11-28-2017	Substantive	Appendix D, Table D-8, Derived Security Requirement 3.8.6: Change “information” to “CUI”	41
11-28-2017	Substantive	Appendix D, Table D-9, Basic Security Requirement 3.9.2: Delete “CUI and”	43
11-28-2017	Editorial	Appendix D, Table D-10, Basic Security Requirement 3.10.2: Add PE-4 to SP 800-53 mapping	44
11-28-2017	Editorial	Appendix D, Table D-10, Derived Security Requirement 3.10.6: Delete “(e.g., telework sites)”	44
11-28-2017	Substantive	Appendix D, Table D-14, Basic Security Requirement 3.14.1: Delete “information and”	50

DATE	TYPE	CHANGE	PAGE
11-28-2017	Substantive	Appendix D, Table D-14, Basic Security Requirement 3.14.3: Delete “appropriate”	50
11-28-2017	Editorial	Appendix D, Table D-14, Basic Security Requirement 3.14.3: Change “actions” to “action”	50
11-28-2017	Editorial	Appendix E, Table E-7, IA-3: Change “NCO” to “CUI”	58
11-28-2017	Editorial	Appendix E, Table E-8, IR-3(2): Change “CUI” to “NCO”	59
11-28-2017	Editorial	Appendix E, Table E-11, PE-4: Change “NFO” to “CUI”	62
02-20-2018	Editorial	EXPECTATIONS FOR THIS PUBLICATION call out box, second paragraph: Change “With regard to” to “Regarding”	v
02-20-2018	Editorial	Chapter Two, Section 2.2, Derived Security Requirements, sixth bullet: Change “blacklist” to “blacklisting”	7
02-20-2018	Editorial	Chapter Three, THE MEANING OF ORGANIZATIONAL SYSTEMS call out box: Change “is intended to have” to “has”	9
02-20-2018	Editorial	Chapter Three, THE MEANING OF ORGANIZATIONAL SYSTEMS call out box: Change “security requirements” to “CUI security requirements.”	9
02-20-2018	Substantive	Chapter Three, THE MEANING OF ORGANIZATIONAL SYSTEMS call out box: Change: “—that is, the requirements are applied only to the systems or system components that process, store, or transmit CUI” to “The requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components”	9
02-20-2018	Substantive	Chapter Three, Section 3.1, Derived Security Requirement 3.1.7: Change “audit” to “capture”	9
02-20-2018	Substantive	Chapter Three, Section 3.1, Derived Security Requirement 3.1.7: Add “in audit logs” after “functions”	9
02-20-2018	Editorial	Chapter Three, Section 3.1, Derived Security Requirement 3.1.10: Add “a” before “period”	9
02-20-2018	Substantive	Chapter Three, Section 3.3, Basic Security Requirement 3.3.1: Add “logs and” after “audit”	10
02-20-2018	Substantive	Chapter Three, Section 3.3, Basic Security Requirement 3.3.1: Change “unlawful, unauthorized, or inappropriate” to “unlawful or unauthorized”	10
02-20-2018	Substantive	Chapter Three, Section 3.3, Derived Security Requirement 3.3.3: Change “audited” to “logged”	10
02-20-2018	Substantive	Chapter Three, Section 3.3, Derived Security Requirement 3.3.4: Add “logging” after “audit”	10
02-20-2018	Substantive	Chapter Three, Section 3.3, Derived Security Requirement 3.3.5: Add “record” after “audit”	10
02-20-2018	Substantive	Chapter Three, Section 3.3, Derived Security Requirement 3.3.5: Change “inappropriate” to “unlawful, unauthorized”	10
02-20-2018	Substantive	Chapter Three, Section 3.3, Derived Security Requirement 3.3.6: Add “record” after “audit”	10
02-20-2018	Substantive	Chapter Three, Section 3.3, Derived Security Requirement 3.3.8: Add “logging” before “tools”	10
02-20-2018	Substantive	Chapter Three, Section 3.3, Derived Security Requirement 3.3.9: Add “logging” after “audit”	10
02-20-2018	Substantive	Chapter Three, Section 3.4, Derived Security Requirement 3.4.3: Change “audit” to “log”	11
02-20-2018	Editorial	Chapter Three, Section 3.4, Derived Security Requirement 3.4.8: Change “blacklist” to “blacklisting”	11

DATE	TYPE	CHANGE	PAGE
02-20-2018	Editorial	Chapter Three, Section 3.5, Basic Security Requirement 3.5.2: Delete “those”	11
02-20-2018	Substantive	Chapter Three, Section 3.6, Basic Security Requirement 3.6.2: Change “appropriate” to “designated”	12
02-20-2018	Editorial	Chapter Three, Section 3.11, Derived Security Requirement 3.11.3: Change “assessments of risk” to “risk assessments”	14
02-20-2018	Editorial	Footnote 26: Delete “must” and “appropriately”	14
02-20-2018	Substantive	Chapter Three, Section 3.14, Basic Security Requirement 3.14.2: Change “appropriate” to “designated”	15
02-20-2018	Editorial	Chapter Three, Section 3.14, Derived Security Requirement 3.14.6: Add “,” after “systems”	15
02-20-2018	Substantive	Appendix D: Add call out box “CONSISTENCY IN PUBLICATION CONTENT”	28
02-20-2018	Substantive	Appendix D, Table D-1, Derived Security Requirement 3.1.7: Change “audit” to “capture”	30
02-20-2018	Substantive	Appendix D, Table D-1, Derived Security Requirement 3.1.7: Add “in audit logs” after “functions”	30
02-20-2018	Substantive	Appendix D, Table D-1, Derived Security Requirement 3.1.7, SP 800-53 Security Control Mapping for AC-6(9): Change “Auditing” to “Log”	30
02-20-2018	Editorial	Appendix D, Table D-1, Derived Security Requirement 3.1.10: Add “a” before “period”	30
02-20-2018	Substantive	Appendix D, Table D-3, Basic Security Requirement 3.3.1: Add “logs and” after “audit”	33
02-20-2018	Substantive	Appendix D, Table D-3, Basic Security Requirement 3.3.1: Change “unlawful, unauthorized, or inappropriate” to “unlawful or unauthorized”	33
02-20-2018	Substantive	Appendix D, Table D-3, Derived Security Requirement 3.3.1, SP 800-53 Security Control Mapping for AU-2: Change “Audit Events” to “Event Logging”	33
02-20-2018	Substantive	Appendix D, Table D-3, Derived Security Requirement 3.3.2, SP 800-53 Security Control Mapping for AU-6: Add “Record” after “Audit”	33
02-20-2018	Substantive	Appendix D, Table D-3, Derived Security Requirement 3.3.2, SP 800-53 Security Control Mapping for AU-12: Add “Record” after “Audit”	33
02-20-2018	Substantive	Appendix D, Table D-3, Derived Security Requirement 3.3.3: Change “audited” to “logged”	33
02-20-2018	Substantive	Appendix D, Table D-3, Derived Security Requirement 3.3.3, SP 800-53 Security Control Mapping for AU-2(3): Change “Audit Events” to “Event Logging”	33
02-20-2018	Substantive	Appendix D, Table D-3, Derived Security Requirement 3.3.4: Add “logging” after “audit”	33
02-20-2018	Substantive	Appendix D, Table D-3, Derived Security Requirement 3.3.4, SP 800-53 Security Control Mapping for AU-5: Add “Logging” after “Audit”	33
02-20-2018	Editorial	Appendix D, Table D-3, Derived Security Requirement 3.3.4, SP 800-53 Security Control Mapping for AU-5: Change “Processing” to “Process”	33
02-20-2018	Substantive	Appendix D, Table D-3, Derived Security Requirement 3.3.5: Add “record” after “audit”	33
02-20-2018	Substantive	Appendix D, Table D-3, Derived Security Requirement 3.3.5: Change “inappropriate” to “unlawful, unauthorized”	33

DATE	TYPE	CHANGE	PAGE
02-20-2018	Substantive	Appendix D, Table D-3, Derived Security Requirement 3.3.5, SP 800-53 Security Control Mapping for AU-6(3): Add “Record” after “Audit” (two instances)	33
02-20-2018	Substantive	Appendix D, Table D-3, Derived Security Requirement 3.3.6: Add “record” after “audit”	33
02-20-2018	Substantive	Appendix D, Table D-3, Derived Security Requirement 3.3.6, SP 800-53 Security Control Mapping for AU-7: Add “Record” after “Audit”	33
02-20-2018	Substantive	Appendix D, Table D-3, Derived Security Requirement 3.3.8: Add “logging” before “tools”	33
02-20-2018	Substantive	Appendix D, Table D-3, Derived Security Requirement 3.3.9: Add “logging” after “audit”	34
02-20-2018	Substantive	Appendix D, Table D-4, Derived Security Requirement 3.4.3: Change “audit” to “log”	34
02-20-2018	Editorial	Appendix D, Table D-4, Derived Security Requirement 3.4.8: Change “blacklist” to “blacklisting”	36
02-20-2018	Editorial	Appendix D, Table D-5, Basic Security Requirement 3.5.2: Delete “those”	37
02-20-2018	Substantive	Appendix D, Table D-6, Basic Security Requirement 3.6.2: Change “appropriate” to “designated”	39
02-20-2018	Substantive	Appendix D, Table D-6, Basic Security Requirement 3.6.2: Delete “organizational”	39
02-20-2018	Substantive	Appendix D, Table D-6, Basic Security Requirement 3.6.2: Add “both internal and external to the organization” after “authorities”	39
02-20-2018	Substantive	Appendix D, Table D-8, Derived Security Requirement 3.8.6: Delete “outside of controlled areas”	41
02-20-2018	Editorial	Appendix D, Table D-11, Derived Security Requirement 3.11.3: Change “assessments of risk” to “risk assessments”	45
02-20-2018	Substantive	Appendix D, Table D-14, Basic Security Requirement 3.14.2: Change “appropriate” to “designated”	50
02-20-2018	Editorial	Appendix D, Table D-14, Derived Security Requirement 3.14.6: Add “,” after “systems”	50
02-20-2018	Substantive	Appendix E, Table E-3, Security Control AU-5: Add “Logging” after “Audit”	54
02-20-2018	Editorial	Appendix E, Table E-3, Security Control AU-5: Change “Processing” to “Process”	54
06-07-2018	Editorial	Chapter One, Section 1.2, first paragraph, first sentence: Change “is intended to serve” to “serves”	4
06-07-2018	Editorial	Chapter One, Section 1.2, first paragraph, first sentence: Change “:” to “individuals with:”	4
06-07-2018	Editorial	Chapter One, Section 1.2, first paragraph, all four bullets: Delete “Individuals with”	4
06-07-2018	Editorial	Chapter One, Section 1.3, third bullet: Change “and an explanation of the tailoring actions employed on the moderate security control baseline.” to “an explanation of the tailoring actions applied to the moderate security control baseline;”	4
06-07-2018	Substantive	Chapter One, Section 1.3, third bullet: Add “and an expanded discussion about each security requirement.”	4
06-07-2018	Editorial	Chapter Two, Section 2.1, second paragraph, first bullet: Delete “the purpose of”	5

DATE	TYPE	CHANGE	PAGE
06-07-2018	Editorial	Chapter Two, Section 2.1, second paragraph, fourth bullet: Change "particular requirement" to "requirement"	5
06-07-2018	Editorial	Chapter Two, Section 2.2, fifth paragraph, fourth sentence: Delete "aforementioned"	7
06-07-2018	Editorial	Chapter Three, first paragraph, change "particular requirement" to "requirement"	8
06-07-2018	Substantive	Chapter Three, Introduction section after fourth paragraph: Add "Appendix F provides expanded information on the CUI security requirements. Hyperlinks in the CUI requirements below provide direct accessibility to the discussion section in the appendix."	9
06-07-2018	Editorial	Chapter Three, Section 3.1, Derived Security Requirement 3.1.21: Delete "organizational"	10
06-07-2018	Editorial	Chapter Three, Section 3.2, Basic Security Requirement 3.2.2: Delete "organizational" and "adequately"	10
06-07-2018	Substantive	Appendix A, References (Legislation, Executive Orders, and Regulations): Add "Executive Order 13526, Classified National Security Information, December 2009. https://www.archives.gov/isoo/policy-documents/cnsi-eo.html"	17
06-07-2018	Editorial	Appendix A, References (Standards, Guidelines, and Instructions), National Institute of Standards and Technology Federal Information Processing Standards Publication 199: Delete "(as amended)"	17
06-07-2018	Editorial	Appendix A, References (Standards, Guidelines, and Instructions), National Institute of Standards and Technology Federal Information Processing Standards Publication 199: Add "February 2004"	17
06-07-2018	Editorial	Appendix A, References (Standards, Guidelines, and Instructions), National Institute of Standards and Technology Federal Information Processing Standards Publication 200: Delete "(as amended)"	17
06-07-2018	Editorial	Appendix A, References (Standards, Guidelines, and Instructions), National Institute of Standards and Technology Federal Information Processing Standards Publication 200: Add "March 2006"	17
06-07-2018	Editorial	Appendix A, References (Standards, Guidelines, and Instructions), National Institute of Standards and Technology Special Publication 800-53: Delete "(as amended)"	17
06-07-2018	Editorial	Appendix A, References (Standards, Guidelines, and Instructions), National Institute of Standards and Technology Special Publication 800-53: Add "Revision 4"	17
06-07-2018	Editorial	Appendix A, References (Standards, Guidelines, and Instructions), National Institute of Standards and Technology Special Publication 800-53: Add "April 2013"	17
06-07-2018	Editorial	Appendix A, References (Standards, Guidelines, and Instructions), National Institute of Standards and Technology Special Publication 800-60, Volume 1: Delete "(as amended)"	17
06-07-2018	Editorial	Appendix A, References (Standards, Guidelines, and Instructions), National Institute of Standards and Technology Special Publication 800-60, Volume 1: Add "Revision 1"	17
06-07-2018	Editorial	Appendix A, References (Standards, Guidelines, and Instructions), National Institute of Standards and Technology Special Publication 800-60, Volume 1: Add "August 2008"	17
06-07-2018	Editorial	Appendix A, References (Standards, Guidelines, and Instructions), National Institute of Standards and Technology Special Publication 800-60, Volume 2: Delete "(as amended)"	17

DATE	TYPE	CHANGE	PAGE
06-07-2018	Editorial	Appendix A, References (Standards, Guidelines, and Instructions), National Institute of Standards and Technology Special Publication 800-60, Volume 2: Add “Revision 1”	17
06-07-2018	Editorial	Appendix A, References (Standards, Guidelines, and Instructions), National Institute of Standards and Technology Special Publication 800-60, Volume 2: Add “August 2008”	17
06-07-2018	Editorial	Appendix A, References (Standards, Guidelines, and Instructions), National Institute of Standards and Technology Special Publication 800-171A: Delete “(Draft)”	17
06-07-2018	Editorial	Appendix A, References (Standards, Guidelines, and Instructions), National Institute of Standards and Technology Special Publication 800-171A: Add “, June 2018”	17
06-07-2018	Substantive	Appendix B, Glossary: Add “**security domain**” and “A domain that implements a security policy and is administered by a single authority.”	25
06-07-2018	Editorial	Appendix D, Table D-1, Derived Security Requirement 3.1.21: Delete “organizational”	31
06-07-2018	Editorial	Appendix D, Table D-2, Basic Security Requirement 3.2.2: Delete “organizational” and “adequately”	32
06-07-2018	Substantive	Add Appendix F, “Discussion”	69-108

（株）エヴァアビエーション info@EvaAviation.com 訳の改訂版（2019.01）について

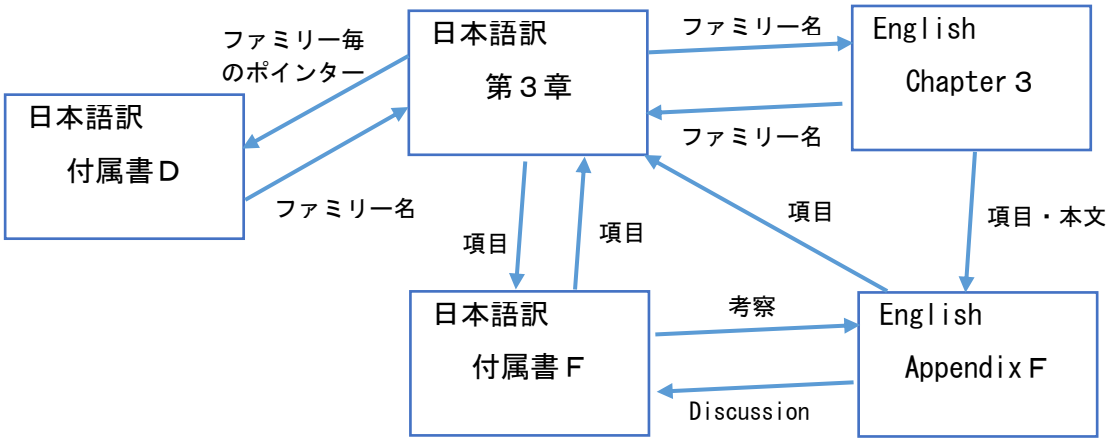
先（2017.03.24）に（株）エヴァアビエーションから発行された日本語訳の文書は NIST SP 800-171 Revision 1（2016.12）にもとづいて作成されたが、その後 NIST にて継続的に改訂が進められ、特に「付属書 F」が付加されたことから日本語訳の文書の改訂が必要になったと判断し、SP 800-171 Revision 1（2018.06.07）にもとづく日本語訳の文書の改訂を行った。今回の改訂にあたり、編集上の訂正の他、先の版のいくつかの訳語の見直しを行っている。見直した訳語の主なものを以下に示す。

i　access control　　アクセス制御　→　アクセス管理
　理由：システムによる制御と人による管理を含む場合の差異を表現した

ii　confidentiality　　機密性　→　秘匿性
　理由：非機密（unclassified）情報の機密性の保護という論理矛盾的な表現を避けるため。また、機密は情報の性質も示しており、措置を取ることを明示的に意味する秘匿の方が適切とした。

iii　safeguards　　保護措置　→　保全措置
　理由：protect との差異を明確に表現した。

また、NSIT の改訂で新たに第３章の 14 ファミリーと付属書 D の、および第３章の個々の要件項目と付属書 F とのハイパーリンクが設けられたのでそれに対応すると共に、日本語訳の改訂版では第３章と付属書 F を英日対訳形式としたことに伴う英日文書間のハイパーリンクを設けたので、その関連を以下に図示する。



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ーに依存して、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。たとえば、多くの連邦政府との契約者は、それぞれのシステムで、要注意（sensitive）連邦政府情報を日常的に処理、格納、通信することで連邦政府機関にとって必須の製品やサービスの納入を支えている（たとえば、クレジットカードおよびその他の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、機密取扱許可のための身元調査実施、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）。さらに、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期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、重要インフラに関連する任務および機能を含めて、指定された任務および事業運営（business operations）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。

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、連邦政府によって日常的に使われる様々なタイプの情報を識別するための構造化され統制のとれたプロセスを、連邦政府が提供できるかどうかにかかっている。2010 年 11 月 4 日、大統領は大統領令 13556『EO 13556,管理対象非機密情報』（CUI：Controlled Unclassified Information）に署名した。この大統領令は、保護を必要とする非機密情報を執行部門（executive branch）が取り扱う方法を標準化するために、政府横断の CUI プログラム[3]を設け、そしてこのプログラムを履行する執行機関（Executive Agent）[4]に国立公文書館（NARA： National Archives and Records Administration）を

---

[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資源の集合である。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、格納、または伝送することができるすべて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、大統領令 13526「EO 13526,機密国家安全保障情報」（*Classified National Security Information*）December 29, 2009（または以前の、または後継の大統領令）、または改訂を含む 1954 年の原子力エネルギー法（Atomic Energy Act)で機密扱い（classified）にされた情報を除く。

[4] NARA は本権限を NARA の一部門である米国情報セキュリティ監督局（ISOO:Information Security Oversight Office）に委任している。

指定した。連邦法、規則、または政府横断のポリシーに従って保全や配布制限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、一貫性のない標記、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、手順の標準化おおび「CUI レジストリー（CUI *Registry*）」 を通じた共通定義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、指導、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、様々な情報を処理する中で、特に、承認済 CUI 区分（categories）および下位区分（subcategories）を識別し、それぞれに一般的説明を規定し、管理策の基礎を明らかにし、また CUI を使う手順を設定している。これには、情報の標記、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。

大統領令 13356 はまた、CUI プログラムが、開示性、透明性、および政府全体の実践の画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標準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 執行機関によって開発された連邦政府 CUI 規則 [5]は、CUI の指定、保全、配布、標記、解除、および処分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 目的と適用性

本出版物の目的は、下記の期間において、CUI の *秘匿性* を守るための推奨要件を、連邦政府機関に提供することである。すなわち、(i) CUI が非連邦政府システムおよび組織に存在している期間、(ii) CUI が存在するシステムが連邦政府機関の契約者またはその連邦政府機関を代理するその他の組織[6]によって使用または運用されていない 期間、および(iii) CUI の秘匿性は、CUI カテゴリーまたはサブカテゴリーを認可する法律、規則、または政府横断ポリシーによって規定され、「CUI レジストリー」[7]に記載されるが、そうした秘匿性を保護するための特定の保全要件が存在しない場合である。本要件は、CUI を処理、格納、または伝送する非連邦政府システムの構成要素[8]だけに適用され、あるいはそれらの構成要素にセキュリティ保護を提供する非連邦政府システムの構成要素だけに適用される。本 CUI 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

[5] 32 CFR Part 2002,『管理対象非機密情報』が 2016 年 9 月 14 日に制定、2016 年 11 月 14 日に施行された。

[6] 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）の要件に従わなければならない。それには、FIPS 200 の最低限のセキュリティ要件、および NIST SP 800-53 のセキュリティ管理策が含まれる。 （44 USC 3554(a)(1)(A)参照）

[7] 本出版物に示す要件は、上級政府機関職員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 要件に適合した情報セキュリティ措置のために利用できる。

[8] システムの構成要素 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入出力装置、③ネットワーク構成要素、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。

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：Federal Acquisition Regulation）[9]の中で、CUI 執行機関は CUI 要件[10]への準拠性判断を行う。

CUI を処理、格納、または通信する連邦政府システムを使う連邦政府機関は、提案中の連邦政府 CUI 規則に従って、 最低限、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のセキュリティカテゴリー企画』（中位秘匿性）[11]。
- 「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』[12]。

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 によって CUI が処理・格納・伝送される時にも、類似レベルの保護が必要とされる[13]。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、上述の連邦政府標準規格と指針から引き出される。しかしながら、提案中の連邦政府 CUI 規則にある保全要件の範囲が、秘匿性というセキュリティ目的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）、そして NIST の規格および指針に示されている FISMA 関連の要件の一部が一意的に連邦政府用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適応されている。

第 2 章で説明される適応規準は、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し、または 最小限にすることを意図していない。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（safeguarding measures）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

[9] NARA は、CUI 執行機関としての立場で、2017 年に、連邦政府 CUI 規則および「NIST SP 800-171」の要件を契約者に適用する単一条項を提出する計画である。このような単一 FAR 条項を制定する正式プロセスが始まるまでは、連邦政府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るだろう。

[10] NIST SP 800-171A は、組織が第 3 章のセキュリティ要件への適合性を判断する上で助けとなる評価手順を提供している。

[11] FIPS 199 は、万一セキュリティの欠陥（たとえば秘匿性の欠損）が存在した場合における、組織、資産、または個人に対する 3 種類の潜在的影響（低位、中位、高位）を規定している。この潜在的影響は、秘匿性の欠損が、組織の運営、組織の資産、または個人に対して重大な悪影響をおよぼすと予想できる場合には「中位」（*moderate*） になる。

[12] NIST SP 800-60 は、CUI レジストリーにある CUI カテゴリーおよびサブカテゴリーとの整合性を取るために改訂中である。

[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、および契約者が含まれる。

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、または政府横断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だけである。特定カテゴリー内への CUI 保全要件の規定は、NARA の CUI 指針および CUI FAR の中で NARA によって検討され、また契約やその他の合意書における具体的な要件として反映されることになる。

CUI 保護を受託した非連邦政府組織が、CUI の処理・格納・伝送用に、特定のシステムやシステム構成要素を指定する場合、それらの組織はその特定のシステムや構成要素へのセキュリティ要件の範囲を限定する可能性がある。アーキテクチャー設計の原則や概念を適用することによって、CUI をそれ自身のセキュリティドメインへ隔離することが（たとえば、ファイアウォールその他の境界保護デバイスを備えたサブネットワークの実装）、非連邦組織が要件を満たし、CUI の秘匿性を守る上でもっともコスト効果があり、効率的な取り組み方であるかもしれない。セキュリティドメインでは、物理的分離、論理的分離、または両方の組み合わせを利用することもある。この取り組み方では、以下が可能である。すなわち、(i) CUI に適したセキュリティを合理的に提供すること、そして (ii) 組織のミッションおよび事業運用と資産を保護するために、その組織が通常必要とするレベルを超えたところまで、その組織のセキュリティ体制を拡大しなければならないことを回避することである。CUI インフラストラクチャーが、認可法、規則、または政府横断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書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 インフラストラクチャーの使用を選択できる。

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・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ーなど）。
- 購買（acquisition）または調達（procurement）責任を有する（契約担当官など）。
- 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（認可担当官、 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）。
- セキュリティの評価・確認責任を有する（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、(i) 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 (ii) 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、それに従う組織体としての非連邦政府の観点 である。

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、セキュリティ要件の開発に用いられる前提条件と方法論、要件の形式と構造、および要件を獲得するために NIST 規格および指針に適用される適応規準について記述する。
- 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 保護に関連した付加情報を提供する。それには以下が含まれる。 (A) 一般的参照情報、(B) 定義および用語集、(C) 本出版物で使われる頭字語、(D)セキュリティ要件を「NIST SP 800-53」と「ISO/IEC 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適応措置の説明、および (F) 各セキュリティ要件に関する詳細な考察（discussion）。

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、 (i) 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および (ii) 基本および派生セキュリティ要件の構造および連邦政府情報セキュリティ要件と管理策に適用される適応規準を記述する。

2.1 基本的前提条件

本出版物で記述されるセキュリティ要件は、 以下の３つの基礎的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 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 のための秘匿性影響値は、「連邦情報処理規格（FIPS）199」[14]に従い、中位[15]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、潜在的な*悪影響*をもたらす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影響をおよぼし、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備えており、必ずしも CUI を処理・格納・伝送するためにシステムを開発・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。

[14] FIPS 199 で定義されている中位影響値 は、FIPS 200 では中位影響度システム の一部になる可能性があるが、その代わり、適応措置の出発点として、NIST 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。

[15] 32 CFR 2002(g) に従い中位秘匿性影響値以上に分類されている。しかしながら、連邦政府法、規則、または政府横断的なポリシーが CUI を管理する上で、中位秘匿性ベースラインの管理策とは異なる規定がなされる場合には、これに従うものとする。

- 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、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、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。

CUI に対する単一（single stage）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標準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、明確に定義された構造を持ち、それは以下で構成される。 すなわち、(i) *基本（basic）セキュリティ要件*の節と、(ii) *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 から入手される。FIPS 200 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、NIST SP 800-53 のセキュリティ管理策から取り入れられている。要件と管理策は、「FIPS 200」のセキュリティ要件および中位ベースラインの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）で始まり、以下の要件、管理策、または管理策の一部を削除するように適応されている。

- 連邦政府固有のもの（すなわち主に連邦政府の責任であるもの）
- CUI の秘匿性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[16]

[16] 適応された FIPS Publication 200 のセキュリティ要件および NIST SP 800-53 の中位セキュリティ管理策ベースラインから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、および実践手続きの実装が含まれる。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 適応規準に基づいて「NIST SP 800-53」の中位ベースラインから削除されたセキュリティ管理策に関する完全なリストを提供する。

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「NIST SP 800-53」の意図を捉えることができる。付属書 D は、「NIST SP 800-53」および「ISO/IEC 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、セキュリティ要件のより良い理解を促進するためであって、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。

構成管理 ファミリーの以下の例は、典型的なセキュリティ要件の構造を説明（illustrates）している。

基本セキュリティ要件

- 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資産目録（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（establish）し、維持する。
- 組織のシステムで採用された情報技術製品のセキュリティ構成設定を規定し、実施（enforce）する。

派生セキュリティ要件

- 組織のシステムに対する変更を追跡、見直し、承認/非承認し、記録（log）する。
- 変更実施に先立って、セキュリティへの影響を分析する。
- 組織のシステム変更に関する物理的・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。
- 必須能力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。
- 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し、無効化し、防止する。
- 「例外による拒否」（ブラックリスト登録（blacklisting））ポリシーを適用して権限の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（permit）」（ホワイトリスト登録（whitelisting））ポリシーを適用して権限のあるソフトウェア実行を許可する（allow）。
- ユーザーがインストールしたソフトウェアを管理（control）し、確認（monitor）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、適応規準に従い、本出版物の範囲には含まれない[17]。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。

[17] 3 つの例外には以下が含まれる。すなわち、(i) 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、(ii)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（CP-9 からの導出） (iii)システムおよびサービス取得ファミリー にお

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	記憶媒体の保護
意識向上と訓練	要員のセキュリティ
監査と説明責任	物理的保護
構成管理	リスク評価
識別と認証	セキュリティ評価
インシデント対応	システムと通信の保護
メンテナンス	システムと情報の完全性

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。便宜上、これらの要件は、それぞれ CUI の記憶媒体の保護、セキュリティ評価, およびシステムと通信の保護ファミリーに含まれている。

CHAPTER THREE

THE REQUIREMENTS

SECURITY REQUIREMENTS FOR PROTECTING THE CONFIDENTIALITY OF CUI

This chapter describes fourteen families of security requirements (including basic and derived requirements) for protecting the confidentiality of CUI in nonfederal systems and organizations.[18] The security controls from NIST Special Publication 800-53 associated with the basic and derived requirements are also listed in Appendix D. [19] Organizations can use Special Publication 800-53 to obtain additional, non-prescriptive information related to the security requirements (e.g., supplemental guidance related to each of the referenced security controls, mapping tables to ISO/IEC security controls, and a catalog of optional controls that can be used to help specify additional security requirements if needed). This information can help clarify or interpret the requirements in the context of mission and business requirements, operational environments, or assessments of risk. Nonfederal organizations can implement a variety of potential security solutions either directly or using managed services, to satisfy the security requirements and may implement alternative, but equally effective, security measures to compensate for the inability to satisfy a requirement. [20]

Nonfederal organizations should describe in a system security plan, how the specified security requirements are met or how organizations plan to meet the requirements. The plan describes the system boundary; the operational environment; how the security requirements are implemented; and the relationships with or connections to other systems. Nonfederal organizations should develop plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format.

THE MEANING OF ORGANIZATIONAL SYSTEMS

The term *organizational system* is used in many of the CUI security requirements in NIST Special Publication 800-171. This term has a specific meaning regarding the scope of applicability for the CUI security requirements. The requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. The appropriate scoping for the security requirements is an important factor in determining protection-related investment decisions and managing security risk for nonfederal organizations that have the responsibility of safeguarding CUI.

[18] While the purpose of this publication is to define requirements to protect the confidentiality of CUI, there is a close relationship between confidentiality and integrity since many of the underlying security mechanisms at the system level support both security objectives. Thus, the integrity requirements (either basic or derived) may have a significant, albeit indirect, effect on the ability of an organization to protect the confidentiality of CUI.

[19] The security control references in Appendix D are included to promote a better understanding of the security requirements. The control references are not intended to impose additional requirements on nonfederal organizations. Moreover, because the security controls were developed for federal agencies, the supplemental guidance associated with those controls may not be applicable to nonfederal organizations.

[20] To promote consistency, transparency, and comparability, compensatory security measures selected by organizations should be based on or derived from *existing* and *recognized* security standards and control sets, including, for example: ISO/IEC 27001 or NIST Special Publication 800-53.

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 のセキュリティ要件ファミリー（基本要件と派生要件を含む）について記述する [18]。基本要件と派生要件に関連する NIST 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[19]。 各組織は、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（参照されるセキュリティ管理策それぞれに関連する補足ガイダンス、ISO/IEC セキュリティ管理策への対応付け表、必要に応じて付加的セキュリティ要件の特定に役立てるために使える管理策オプションの一覧表など）を入手するために、「SP 800-53」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、またはリスク評価との関連で、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[20]。

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）を作成し、指定されたセキュリティ要件がどのように満たされているか、または組織が要件をどのように満たす計画であるかについて記述する必要がある。この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。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、および計画される軽減措置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）を作成する必要がある。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る。

「組織のシステム」の意味

*組織のシステム*という用語は、NIST SP 800-171の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、CUI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。

[18] 本出版物の主要目的は、CUI の秘匿性を保護する要件の定義であるが、秘匿性と完全性の間には密接な関係がある。というのは、システムレベルにおいて基礎と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的を支えているからである。したがって、完全性の要件（基本要件または派生要件のいずれか）は、ある組織が CUI の秘匿性を保護する能力に、間接的ではあるが、大きな効果を持つ可能性がある。

[19] 付属書 D でセキュリティ管理策を参照しているのは、セキュリティ要件のより良い理解を促進するためである。このセキュリティ管理策への参照は、非連邦政府組織に付加的要件を課すことを意図したものではない。さらに、セキュリティ管理策は、連邦政府機関用に開発されたものであるため、これらのセキュリティ管理策関連の補足ガイダンスは、非連邦政府組織には適用できないこともある。

[20] 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/IEC 27001 や NIST 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なければならない。

When requested, the system security plan and any associated plans of action for any planned implementations or mitigations should be submitted to the responsible federal agency/contracting officer to demonstrate the nonfederal organization's implementation or planned implementation of the security requirements. Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization.

The security requirements in this publication should be applied to the nonfederal organization's internal systems processing, storing, or transmitting CUI. Some systems, including specialized systems (e.g., industrial/process control systems, Computer Numerical Control machines, medical devices), may have restrictions or limitations on the application of certain security requirements. To accommodate such issues, the system security plan, as reflected in Requirement 3.12.4, should be used to describe any enduring exceptions to the security requirements. Individual, isolated, or temporary deficiencies should be managed though plans of action, as reflected in Requirement 3.12.2.

Appendix F provides expanded information on the CUI security requirements. Hyperlinks in the CUI requirements below provide direct accessibility to the discussion section in the appendix.

3.1 ACCESS CONTROL

Basic Security Requirements

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Derived Security Requirements

3.1.3 Control the flow of CUI in accordance with approved authorizations.

3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.

3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.

3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

3.1.8 Limit unsuccessful logon attempts.

3.1.9 Provide privacy and security notices consistent with applicable CUI rules.

3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

3.1.11 Terminate (automatically) a user session after a defined condition.

3.1.12 Monitor and control remote access sessions.

3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

3.1.14 Route remote access via managed access control points.

3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.

求めに応じ、システムセキュリティ計画書およびそれに関連する、実装または軽減措置に関する実施計画書は、非連邦政府組織の実装または計画されたセキュリティ要件を論証するために、責任連邦政府機関／契約担当官に提出される必要がある。連邦政府機関は、提出されたシステムセキュリティ計画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全体的な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ろう。

本出版物のセキュリティ要件は、非連邦政府組織の内部システムがCUI を処理、保存、または伝送するため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、コンピュータ数値制御マシン、医療デバイス)を含めて、何らかのシステムは特定のセキュリティ要件の適用に際し、制約または制限があるかもしれない。このような課題に対応するため、シ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必要がある。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必要がある。

付属書 F は、CUI セキュリティ要件の詳細（expanded）情報を提供している。 以下の CUI 要件の項目番号からのハイパーリンクにより、付属書 F の対応する考察（discussion）の節（section）に直接アクセスできる。

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、権限のあるユーザー、権限のあるユーザーの代理として動作するプロセスおよび（その他のシステムを含む）装置に限定する。

3.1.2 システムへのアクセスは、権限のあるユーザーが実行を許可されている各種のトランザクションおよび機能に限定する。

派生セキュリティ要件

3.1.3 承認された権限に従って、CUI の一連の取扱い手続き（flow）を管理する。

3.1.4 共謀のない有害行動のリスクを減らすため、個人の職務を分離する。

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。

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。

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（audit logs）に取り込む（capture）。

3.1.8 ログオン試行失敗回数を限定する。

3.1.9 適用される CUI 規則に則って、プライバシーおよびセキュリティ通知する。

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。

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）終結させる。

3.1.12 リモートアクセスセションを監視し、管理する。

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。

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。

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に権限を付与する。

3.1.16 Authorize wireless access prior to allowing such connections.

3.1.17 Protect wireless access using authentication and encryption.

3.1.18 Control connection of mobile devices.

3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.[21]

3.1.20 Verifyand control/limit connections to and use of external systems.

3.1.21 Limit use of portable storage devices on external systems.

3.1.22 Control CUI posted or processed on publicly accessible systems.

Mapping access control requirements to controls

3.2 AWARENESS AND TRAINING

Basic Security Requirements

3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

Derived Security Requirements

3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Mapping awareness and training requirements to controls

3.3 AUDIT AND ACCOUNTABILITY

Basic Security Requirements

3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

Derived Security Requirements

3.3.3 Review and update logged events.

3.3.4 Alert in the event of an audit logging process failure.

3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting.

3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

[21] Mobile devices and mobile computing platforms include, for example, smartphones, tablets, E-readers, and notebook computers.

3.1.16 ワイヤレスアクセスの接続を許可する前に、そうしたアクセスに権限を付与する。

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。

3.1.18 モバイル装置の接続を管理する。

3.1.19 モバイル装置およびモバイルコンピューティングプラットフォーム[21]上の CUI を暗号化する。

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

3.1.21 外部システム上での可搬型記憶装置の使用を制限する。

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。

「アクセス管理」要件から付属書 D の管理策への対応付け

3.2 意識向上と訓練

基本セキュリティ要件

3.2.1 組織のシステムの管理者（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、規格および手続き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 要員が、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。

派生セキュリティ要件

3.2.3 インサイダーによる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。

「意識向上と訓練」要件から付属書 D の管理策への対応付け

3.3 監査と説明責任

基本セキュリティ要件

3.3.1 非合法的または権限の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。

派生セキュリティ要件

3.3.3 ログされた事象を見直し、最新情報にする。

3.3.4 監査ログ取得（logging）プロセスが失敗した場合に警告を発する。

3.3.5 非合法的または権限のない、疑わしいまたは異常な活動の徴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。

3.3.6 オンデマンドでの分析・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。

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・同期させるシステム機能を提供する。

3.3.8 監査情報および監査ログ取得ツールを、不正なアクセス・改ざん・削除から保護する。

[21] モバイル装置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、e-リーダー、およびノートパソコンを含む。

3.3.9 Limit management of audit logging functionality to a subset of privileged users.

Mapping audit and accountability requirements to controls

3.4 CONFIGURATION MANAGEMENT

Basic Security Requirements

3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.

Derived Security Requirements

3.4.3 Track, review, approve or disapprove, and log changes to organizational systems.

3.4.4 Analyze the security impact of changes prior to implementation.

3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

3.4.8 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

3.4.9 Control and monitor user-installed software.

Mapping configuration management requirements to controls

3.5 IDENTIFICATION AND AUTHENTICATION

Basic Security Requirements

3.5.1 Identify system users, processes acting on behalf of users, and devices.

3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

Derived Security Requirements

3.5.3 Use multifactor authentication[22] for local and network access[23] to privileged accounts and for network access to non-privileged accounts.

3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

[22] *Multifactor authentication* requires two or more different factors to achieve authentication. The factors include: something you know (e.g., password/PIN); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). The requirement for multifactor authentication should not be interpreted as requiring federal Personal Identity Verification (PIV) card or Department of Defense Common Access Card (CAC)- like solutions. A variety of multifactor solutions (including those with replay resistance) using tokens and biometrics are commercially available. Such solutions may employ hard tokens (e.g., smartcards, key fobs, or dongles) or soft tokens to store user credentials.

[23] *Local access* is any access to a system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network. *Network access* is any access to a system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

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。

「監査と説明責任」要件から付属書 D の管理策への対応付け

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資産目録（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。

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、ログする。

3.4.4 変更実施に先立って、セキュリティへの影響を分析する。

3.4.5 組織のシステム変更に関する物理的・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。

3.4.6 必須能力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。

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。

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権限の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権限のあるソフトウェア実行を許可する。

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）し確認（monitor）する。

「構成管理」要件から付属書 D の管理策への対応付け

3.5 識別と認証

基本セキュリティ要件

3.5.1 システムのユーザー、 ユーザーの代理として動作するプロセス、および装置を識別する。

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、プロセスまたは装置のアイデンティティを認証（authenticate）（または検証（verify））する。

派生セキュリティ要件

3.5.3 多要素認証[22]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[23]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。

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。

---

[22] *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、(i) 人が記憶しているもの（パスワード/PIN など）、(ii) 人が所持しているもの（暗号識別装置、トークンなど）、あるいは (iii) 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格納するために、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。

[23] *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（またはユーザーの代理とし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（またはユーザーの代理とし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 Prevent reuse of identifiers for a defined period.

3.5.6 Disable identifiers after a defined period of inactivity.

3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.

3.5.8 Prohibit password reuse for a specified number of generations.

3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.

3.5.10 Store and transmit only cryptographically-protected passwords.

3.5.11 Obscure feedback of authentication information.

Mapping identification and authentication requirements to controls

3.6 INCIDENT RESPONSE

Basic Security Requirements

3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

Derived Security Requirements

3.6.3 Test the organizational incident response capability.

Mapping incident response requirements to controls

3.7 MAINTENANCE

Basic Security Requirements

3.7.1 Perform maintenance on organizational systems.[24]

3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

Derived Security Requirements

3.7.2 Ensure equipment removed for off-site maintenance is sanitized of any CUI.

3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.

Mapping maintenance requirements to controls

[24] In general, system maintenance requirements tend to support the security objective of *availability*. However, improper system maintenance or a failure to perform maintenance can result in the unauthorized disclosure of CUI, thus compromising *confidentiality* of that information.

3.5.5 定められた期間、識別子の再利用を防止する。

3.5.6 定められた非アクティブな期間が過ぎた後、識別子を無効化する。

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

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格納・伝送する。

3.5.11 認証情報のフィードバックを隠す。

「識別と認証」要件から付属書 D の管理策への対応付け

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、回復およびユーザー対応を含め、組織のシステムに運用状態のインシデント対応能力を確立する。

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職員および/または機関に報告する。

派生セキュリティ要件

3.6.3 組織のインシデント対応能力をテストする。

「インシデント対応」要件から付属書 D の管理策への対応付け

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[24]。

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、および要員を管理する。

派生セキュリティ要件

3.7.3 現場外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。

3.7.4 診断および試験プログラムが入っている記憶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検査する。

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。

3.7.6 必要なアクセス権限を持たないメンテナンス要員のメンテナンス活動を監督する。

「メンテナンス」要件から付属書 D の管理策への対応付け

[24] 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的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、結果的に権限のない 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。

3.8 MEDIA PROTECTION

Basic Security Requirements

3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

3.8.2 Limit access to CUI on system media to authorized users.

3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.

Derived Security Requirements

3.8.4 Mark media with necessary CUI markings and distribution limitations.[25]

3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

3.8.7 Control the use of removable media on system components.

3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.

3.8.9 Protect the confidentiality of backup CUI at storage locations.

Mapping media protection requirements to controls

3.9 PERSONNEL SECURITY

Basic Security Requirements

3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.

3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Derived Security Requirements

None.

Mapping personnel security requirements to controls

3.10 PHYSICAL PROTECTION

Basic Security Requirements

3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.

Derived Security Requirements

3.10.3 Escort visitors and monitor visitor activity.

3.10.4 Maintain audit logs of physical access.

3.10.5 Control and manage physical access devices.

3.10.6 Enforce safeguarding measures for CUI at alternate work sites.

Mapping physical protection requirements to controls

[25] The implementation of this requirement is per marking guidance in the 32 CFR, Part 2002, and the CUI Registry.

3.8 記憶媒体の保護

基本セキュリティ要件

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

3.8.2 システム記憶媒体上の CUI へのアクセスを、権限を有するユーザーに限定する。

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。

派生セキュリティ要件

3.8.4 CUI の標記と配布制限が必要な記憶媒体にはその旨を標記する[25]。

3.8.5 CUI を含む記憶媒体へのアクセスを管理し、管理区域外での輸送中は、記憶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、デジタル記憶媒体上に格納された 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可搬型記憶媒体の使用を管理する。

3.8.8 可搬型記憶装置の所有者を識別できない時には、そうした記憶装置の使用を禁止する。

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。

「記憶媒体の保護」要件から付属書 D の管理策への対応付け

3.9 要員のセキュリティ

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権限を与えるに先立って、個人を審査する。

3.9.2 退職や異動などの人事処理中、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。

「要員のセキュリティ」要件から付属書 D の管理策への対応付け

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、権限のある個人に限定する。

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。

派生セキュリティ要件

3.10.3 訪問者をエスコートし、その活動を確認する。

3.10.4 物理的アクセスの監査ログを保持する。

3.10.5 物理的アクセス装置を管理・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。

「物理的保護」要件から付属書 D の管理策への対応付け

[25] 本要件の実装は、32 CFR、Part 2002、および CUI レジストリーのマーク標示ガイダンスによる条件である。

3.11 RISK ASSESSMENT

Basic Security Requirements

3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

Derived Security Requirements

3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

3.11.3 Remediate vulnerabilities in accordance with risk assessments.

Mapping risk assessment requirements to controls

3.12 SECURITY ASSESSMENT

Basic Security Requirements

3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.[26]

Derived Security Requirements

None.

Mapping security assessment requirements to controls

3.13 SYSTEM AND COMMUNICATIONS PROTECTION

Basic Security Requirements

3.13.1 Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

Derived Security Requirements

3.13.3 Separate user functionality from system management functionality.

3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.

3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

[26] There is no prescribed format or specified level of detail for *system security plans*. However, organizations ensure that the required information in 3.12.4 is conveyed in those plans.

3.11 リスク評価

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、格納、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評価する。

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。

3.11.3 リスク評価（risk assessments）に従って、脆弱性を取り除く。

「リスク評価」要件から付属書 D の管理策への対応付け

3.12 セキュリティ評価

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評価し、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・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確認する。

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[26]。

「セキュリティ評価」要件から付属書 D の管理策への対応付け

派生セキュリティ要件：無し

3.13 システムと通信の保護

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・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。

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。

3.13.4 共有システム資源を経由した、不正な情報転送や意図せぬ情報転送を防止する。

3.13.5 内部ネットワークから物理的・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

[26] *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規定はない。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。

3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems.

3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

3.13.12 Prohibit remote activation[27] of collaborative computing devices and provide indication of devices in use to users present at the device.

3.13.13 Control and monitor the use of mobile code.

3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

3.13.15 Protect the authenticity of communications sessions.

3.13.16 Protect the confidentiality of CUI at rest.

Mapping system and communications protection requirements to controls

3.14 SYSTEM AND INFORMATION INTEGRITY

Basic Security Requirements

3.14.1 Identify, report, and correct system flaws in a timely manner.

3.14.2 Provide protection from malicious code at designated locations within organizational systems.

3.14.3 Monitor system security alerts and advisories and take action in response.

Derived Security Requirements

3.14.4 Update malicious code protection mechanisms when new releases are available.

3.14.5 Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

3.14.7 Identify unauthorized use of organizational systems.

Mapping system and information integrity requirements to controls

[27] Dedicated video conferencing systems, which rely on one of the participants calling or connecting to the other party to activate the video conference, are excluded.

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）。

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。

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 の不正な開示を防止するために、暗号メカニズムを実装する。

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。

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。

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。

3.13.12 協働コンピューティング装置のリモートからの活性化[27]を禁止し、その装置に存在するユーザーに対して使用中の装置を表示する。

3.13.13 モバイルコードの使用を管理・監視する。

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・監視する。

3.13.15 通信セションの正当性（Authenticity）を保護する。

3.13.16 通信停止中の CUI の秘匿性を保護する。

「システムと通信の保護」要件から付属書 D の管理策への対応付け

3.14 システムと情報の完全性

基本セキュリティ要件

3.14.1 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警報（alert）および通報（advisory）を監視し、対応措置を講ずる。

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。

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徴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。

3.14.7 組織のシステムの不正使用を特定（identify）する。

「システムと情報の完全性」要件から付属書 D の管理策への対応付け

[27] 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。

NARA, SECURITY REQUIREMENTS, AND THE FAR CLAUSE

Executive Order 13556, *Controlled Unclassified Information*, November 4, 2010, established the CUI Program and designated the National Archives and Record Administration (NARA) as its Executive Agent to implement the Order and to oversee agency actions to ensure compliance with the Order. The CUI Executive Agent anticipates establishing a single Federal Acquisition Regulation (FAR) clause in 2017 to apply the security requirements of NIST Special Publication 800-171 to contractor environments as well as to determine oversight responsibilities and requirements. The Executive Agent also addresses its oversight of federal agencies in the 32 CFR Part 2002. The approaches to federal oversight will be determined through the uniform CUI FAR clause, future understandings, and any agreements between federal agencies and their nonfederal information-sharing partners.

NARA、*CUI* の要件と *FAR* 条項

2010 年 11 月 4 日付の EO 13556（大統領令 13556）『*管理対象非機密情報*』は、CUI プログラムを制定し、この命令を履行する執行機関として国立公文書館（NARA）を指定し、本命令に従うことを保証するように政府機関の行動を確認している。契約者については、CUI 執行機関は、「NIST SP 800-171」の要件を契約者環境に適用し、監督責任と要件を決定するために、2016 年に「連邦政府調達規則」（FAR：Federal Acquisition Regulation）の単一条項を制定することになっている。CUI 執行機関はまた、32 CFR Part 2002「連邦規則集」（CFR：Code of Federal Regulations）へ組み入れるための提案中の規則の中で、連邦政府機関の監督に取り組む。監督への取り組み方は、統一された CUI FAR 条項、今後の意思疎通、および連邦政府機関とその非連邦政府情報共有パートナーの間の合意を通じて決定されることになるだろう。

付属書 A
参照資料

法律、大統領令、規則、指令、規格、および指針[28]

法律、大統領令、および規則

1. 2014 年「連邦情報セキュリティ近代化法」 (P.L. 113-283)、2014 年 12 月。
http://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf
2. 大統領令 13526 、『機密安全保障情報』、 2009 年 12 月。
https://www.archives.gov/isoo/policy-documents/cnsi-eo.html
3. 大統領令 13556 、『管理対象非機密情報』、 2010 年 11 月。
http://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf
4. 大統領令 13636、『重要インフラ・サイバーセキュリティの改良』、2013 年 2 月。
http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
5. 32 CFR Part 2002、『管理対象非機密情報』、2016 年 9 月。
https://www.gpo.gov/fdsys/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf

規格、指針、および指令

1. 米国標準技術研究所（NIST）連邦情報処理規格（FIPS）199、『連邦政府の情報および情報システムのセキュリティ分類のための規格』2004 年 2 月。
https://doi.org/10.6028/NIST.FIPS.199
2. 米国標準技術研究所（NIST）連邦情報処理規格（FIPS）200、『連邦政府の情報および情報システムのための最小セキュリティ要件』、2006 年 3 月。
https://doi.org/10.6028/NIST.FIPS.200
3. 米国標準技術研究所（NIST）特別出版物（SP）800-53 改訂 4、『連邦政府組織および情報システムのためのセキュリティおよびプライバシー管理策』、2013 年 4 月。
https://doi.org/10.6028/NIST.SP.800-53r4
4. 米国標準技術研究所（NIST）特別出版物（SP）800-60 改訂 1 、『セキュリティ区分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ダンス』第 1 巻、2008 年 8 月。
https://doi.org/10.6028/NIST.SP.800-60v1r1
5. 米国標準技術研究所（NIST）特別出版物（SP）800-60 改訂 1、『セキュリティ区分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ダンス』第 2 巻、2008 年 8 月。
https://doi.org/10.6028/NIST.SP.800-60v2r1

[28] 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。

6. 米国標準技術研究所（NIST）特別出版物（SP）800-171A、『管理対象非機密情報に対するセキュリティ要件への対応状況の評価』、2018 年 6 月。
https://doi.org/10.6028/NIST.SP.800-171A

7. 米国標準技術研究所（NIST）、『重要インフラ・サイバーセキュリティ改善のためのフレームワーク』（修正版）。
https://www.nist.gov/cyberframework

8. ISO/IEC 27001:2013、『情報技術 -- セキュリティ技術 - 情報セキュリティマネジメントシステム（ISMS）-- 要件』September, 2013

9. ISO/IEC 27002:2013、『情報技術 -- セキュリティ技術 - 情報セキュリティ管理策のための実施計画（Code of practice for information security controls）』September, 2013

10. 国家セキュリティシステム委員会 指令 4009（修正版）、『国家情報保証用語解説』。
https://www.cnss.gov

その他情報源

1. 米国国立公文書館（NARA）、『CUI レジストリー』。
https:// www.archives.gov /cui/registry/category-list

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定義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）	*executive agency*（執行機関） を参照のこと。
assessment （評価）	*Security Control Assessment*（セキュリティ管理策評価） を参照のこと。
assessor （評価者）	*Security Control Assessor*（セキュリティ管理策評価者）を参照のこと。
audit log （監査ログ） [CNSSI 4009]	システム活動の日付順の記録。所与の期間に実施されたシステム評価および運用の記録を含む。
audit record （監査記録）	監査された事象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、または装置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 3542 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。
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・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。
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 3542 節]	情報のアクセスおよび開示について、権限を与えられた制限を存続させること。個人のプライバシーおよび所有権の情報を保護する手段を含む。
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・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・確認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ーの集合。
controlled area （管理区域）	規定された物理的および手順的な保護が、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、または政府横断のポリシーが、保全または配布制限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 or subcategories **(CUI** 区分または下位区分） [Title 32 CFR,Part 2002]	法律、規則、または政府横断のポリシーが、保全または配布制限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** 執行機関職員） [Title 32 CFR,Part 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 に準拠しているかどうかを監督する国立公文書館（ 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） [Title 32 CFR,Part 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 のための規則、組織、および手順が含まれる。

CUI registry （**CUI** レジストリー） [Title 32 CFR,Part 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 CUI カテゴリーおよびサブ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、マーク付け（標記）および取扱い手続きのガイダンスを含む。
environment of operation （運用環境） [NIST SP 800-37, Adapted]	あるシステムが情報を処理・格納・通信する物理的な周辺状況。
executive agency （執行機関） [合衆国法典・第 41 編・第 403 節]	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、そして合衆国法典・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（または構成要素））	組織によって定められた権限境界外にあるシステムまたはシステムの構成要素、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評価への直接的な統制力を、その組織が通常持たないシステムまたはシステムの構成要素。
external system service （外部システムサービス）	組織のシステムの権限境界外で実行されるシステムサービス（すなわち組織のシステムによって使われるが、組織のシステムの一部ではないサービス）、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評価への直接的な統制力を、その組織が通常持たないシステムサービス。
external system service provider （外部システムサービスプロバイダー）	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、合弁事業、ビジネスパートナー、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）、ライセンス契約、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**の暗号）	「FIPS 140-2」（修正版）に明記された要件を満たすために、「暗号モジュール認証プログラム」（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プログラム」（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）	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格納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）	システムの物理的構成要素。*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 （識別子）	個人のアイデンティティおよびそれに伴う属性を表す固有のデータ。
impact （影響）	組織の運用、組織の資産、個人、その他の組織、または国家（米国の国家安全保障利益を含む）に対して、情報またはシステムの秘匿性、完全性、または可用性の欠如がおよぼす効力。
impact value （影響値）	情報（CUI など）の秘匿性が危険に晒されることから生ずる、評価された潜在的影響のことであり、低位・中位・高位という値で表現される。
incident （インシデント） [FIPS 200,Adapted]	あるシステム、またはそのシステムが処理・格納・通信する情報の、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）	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（情報の一連の取り扱い手続（flow）の管理）	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続き
information resources（情報資源）[合衆国法典・第 44 編・第 3502 節]	情報、そして要員、装備、資金、および情報技術などの関連資源。
information security（情報セキュリティ）[合衆国法典・第 44 編・第 3542 節]	秘匿性、完全性、および可用性の提供を目的とした、権限のないアクセス、使用、開示、途絶、修正、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、維持、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資源の集合体。
information technology（情報技術）[合衆国法典・第 40 編・第 1401 節]	執行機関によるデータまたは情報の自動的取得、格納、操作、管理、移動、制御、表示、転換、交換、伝送、または受領に使われる装置、あるいは相互接続された装置のシステムまたはサブシステム。前文の趣旨において、装備が執行機関に使われるのは、装備が執行機関に直接使われる場合と、以下を必要とする執行機関との契約の下で契約者によって使われる場合とがある。 すなわち、(i) その装置の使用を必要とする執行機関、または (ii) あるサービスの遂行またはある製品の供給において、その装置の使用を相当程度必要とする執行機関である。この「*情報技術*」という用語には、コンピュータ、補助装置、ソフトウェア、ファームウェア、そして類似の手順、（支援サービスを含む）サービス、そして関連資源が含まれる。
insider threat（内部の脅威）	内部の者が、故意または無意識に、権限のある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、不正な露出によって、あるいは当局の資源や能力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 3542 節]	不適切な情報変更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、(i) セキュリティ管理策の確立・維持・提供が、組織の被雇用者または契約者の直接管理下にあるネットワーク、あるいは (ii) 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）同一の効果を提供す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）	各エンティティがその機能を実行するために必要な最小のシステム資源と権限を付与されるべくセキュリティアーキテクチャーが設計される原理。
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（またはユーザーの代理として作用するプロセス）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）	あるシステムの秘匿性、完全性、または可用性に悪影響を持つことになる、権限のないプロセスの遂行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 （記憶媒体） [FIPS 200]	システムの中で、情報が記録、格納、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、物理的装置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 （モバイル装置）	以下のような携帯型コンピューティング装置。すなわち、 (i) 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、(ii) 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、(iii) 取外し不能または取外し可能なローカルデータ・記憶を有するもの、そして (iv) 内蔵型電源を包含するもの。モバイル装置には、音声通信能力、当該装置の情報捕捉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、(i) 人が記憶しているもの（パスワード/PIN など）、(ii) 人が所持しているもの（暗号識別装置、トークンなど）、あるいは (iii) 人自身に存在するもの（生体認証情報）である。認証符号（*Authenticator*） 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）	相互接続された構成要素の集合によって実行されるシステム。そうした構成要素には、ルーター、ハブ、敷設ケーブル、遠隔通信制御装置、主要配電センター、および回線統制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（またはユーザーの代理として作用するプロセス）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) （(執行機関）の代理として） [FIPS 200（修正版）]	以下の場合に生ずる状況：(i) 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ために処理、格納、転送する；（ii）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。
portable storage device （可搬型記憶装置）	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）を格納するために使われるシステムの構成要素。そうした構成要素は通常、磁気、光学、または半導体装置（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 （潜在的影響） [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 (i) 限定された 悪影響（FIPS 199：低位）、 (ii) 重大な 悪影響（FIPS 199：中位）、(iii) 深刻 または破局的な 悪影響（FIPS 199：高位）である。
privileged account （特権アカウント）	特権ユーザーの権限を持つシステムアカウント。
privileged user （特権ユーザー） [CNSSI 4009]	通常のユーザーは実行する権限を与えられないセキュリティ関連機能を実行する権限を与えられ（それ故、信頼され）ているユーザー。
records （記録）	実行された活動の証拠、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（またはユーザーの代理として作用するプロセス）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。

risk （リスク） [FIPS 200（修正版）]	ある実体が、潜在的な周辺事情または事象によって脅かされる程度の尺度であり、通常は以下の相関的要素である。すなわち、(i) 周辺事業または事象が発生した場合に現れる可能性のある悪影響、そして (ii) その発生の見込みである。システム関連のセキュリティリスクとは、情報またはシステムの秘匿性、完全性、または可用性の欠損から生ずるリスクであり、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、および国家への潜在的悪影響を反映している。
risk assessment （リスク評価）	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 （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、記憶媒体に書かれたデータを回復不能にさせるための措置。 データ回復が可能でないように、記憶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、標記、および作動ログが含まれる。
security （セキュリティ）	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、その組織が自らの任務（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、回復、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 （セキュリティ評価）	*Security Control Assessment*（セキュリティ管理策評価） を参照のこと。
security control （セキュリティ管理策） [FIPS 199（修正版）]	組織の情報の秘匿性・完全性・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評価）[CNSSI 4009（改良版）]	あるシステムまたは組織のセキュリティ要件への対処に関して、保護が、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試験または評価。
security domain（セキュリティ領域）[CNSSI 4009（改良版）]	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 functionality（セキュリティ機能性）	組織のシステムの中で、またはそのシステムが作動する環境の中で実行される、セキュリティ関連の特性、機能、メカニズム、サービス、手順、およびアーキテクチャー。
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。
security relevance（セキュリティ関連）	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
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装置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。
supplemental guidance（捕捉指導）	セキュリティ管理策またはセキュリティ管理策強化版のための付加的説明情報の提供に使われる言明。
system（システム）	*Information System*（情報システム） を参照のこと。
system component（システム構成要素）[NIST SP 800-128, Adapted]	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システの境界；セキュリティ要件がどのように実装されているか：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）	情報を処理、格納、または通信する機能を備えたシステムによって提供される能力。
threat （脅威） [CNSSI 4009（改良版）]	情報への権限のないアクセス、破壊、開示、修正、およびサービス拒否の一つまたはそれ以上を介したシステムによって、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、または国家に、悪い影響をおよぼす潜在性を持つ周辺事情または事象。
user （ユーザー） [CNSSI 4009（改良版）]	あるシステムへアクセスする権限を与えられた個人、または権限を与えられた個人の代理として作用する（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地点間の情報通信を可能にする技術。

付属書 C

頭字語

共通省略語

CFR	Code of Federal Regulations （連邦規則集）
CIO	Chief Information Officer （最高情報責任者）
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）
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）
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）
ITL	Information technology Laboratory （情報技術研究所）
NARA	National Archives and Records Administration （国立公文書館）
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）

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、NIST SP 800-53 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対応付けを提供する。この対応付け表は、情報提供だけを目的としており、第 3 章 で定義された要件を越えた付加的セキュリティ要件を伝えることを意図したものではない。さらに、このセキュリティ管理策は、連邦政府機関用に開発されたものであるため、これらのセキュリティ管理策関連の補足ガイダンスは、非連邦政府組織には適用できないものがある。場合によっては、この関連セキュリティ管理策には CUI を保護するために必要とされるものを越えた、追加が見込まれるものを含んでおり、そうした関連セキュリティ管理策は、第 2 章 の規準を使って適応されている。本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、適用可能である。本表には、「SP 800-53」から、ISO/IEC 27001 付属書 A の関連する管理策に至るまでの、セキュリティ管理策の二次的な対応付けも含まれる。NIST から ISO/IEC への対応付けは、「SP 800-53」の付属書 H から入手できる。 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。CUI への適応に起因して、基本または派生セキュリティ要件が満たされているからと言って、それは「NIST SP 800-53」の対応するセキュリティ管理策やセキュリティ管理策強化版（control enhancement）が満たされていることを意味 *しない* ことに注意することも重要である。というのは、CUI の秘匿性保護に必須ではない管理策または管理策強化版の要素の中には、本要件に反映されていないものもあるからである。

『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 NIST フレームワーク』 を実装し、または実装を計画している組織は、「NIST SP 800-53」および「ISO/IEC 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、このフレームワークの中核機能、すなわち識別、保護、検知、対応、および回復に関連した区分および下位区分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、本セキュリティ管理策の対応付けに関する情報は有用なものとなろう。

出版物の一貫性について

NISTは、そのコンテンツが最新のものであり、提供されているコミュニティにとって適切であることを確実にするために出版物の更新を続けている。これらの更新が進行中であるため、本書で参照されている内容が他のNISTの出版物と矛盾する場合がある。たとえば、この付属書の NIST SP 800-53で選択されたセキュリティ管理策と管理策強化版の名前は、その出版物への改訂予定のものを反映している。この不一致は一時的なものであり、参照された出版物が完成した時点で解決される。

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、権限のあるユーザー、権限のあるユーザーの代理として動作するプロセスおよび（その他のシステムを含む）装置に限定する。 **3.1.2** システムへのアクセスは、権限のあるユーザーが実行を許可されている各種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	モバイル機器の方針
			A.6.2.2	テレワーキング
			A.13.1.1	ネットワーク管理策
			A.13.2.1	情報転送の方針および手順
			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	承認された権限に従って、CUI の一連の取扱い手続き（flow）を管理する。	AC-4	情報フローの強制	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 共謀のない有害行動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（audit logs）に取り込む（capture）。	AC-6 (9)	最小特権 特権機能の使用をログする	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 規則に則って、プライバシーおよびセキュリティ通知する。	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	無人状態にある利用者装置
			A.11.2.9	クリアデスク・クリアスクリーン方針
	AC-11 (1)	セションロックパターン隠蔽ディスプレイ	直接対応付け無し	
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	AC-12	セション終結	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
動的に）終結させる。			
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に権限を付与する。	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、そうしたアクセスに権限を付与する。	AC-18	無線アクセス	A.6.2.1	モバイル装置ポリシー
			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 モバイル装置の接続を管理する。	AC-19	モバイル装置のアクセス管理	A.6.2.1	モバイル機器の方針
			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 モバイル装置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)	モバイル装置のアクセス管理 装置/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/制限する。	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 権限を与えられた使用を限定	直接対応付け無し	
3.1.21 外部システム上での組織の可搬型記憶装置の使用を制限する。	AC-20 (2)	外部システムの使用 携帯型記憶装置	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と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 意識向上と訓練				
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、規格および手続き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** 要員が、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の訓練	A.7.2.2	情報セキュリティの意識向上、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*	情報セキュリティの意識向上、教育および訓練
派生セキュリティ要件				
3.2.3 インサイダーによる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の訓練 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と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 監査と説明責任				
基本セキュリティ要件				
3.3.1 非合法的または権限の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	監査事象	直接対応付け無し	
	AU-3	イベントログの内容	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	情報セキュリティ事象の報告
			A.16.1.4	情報セキュリティ事象の評価および決定
	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	証拠収集
派生セキュリティ要件				
3.3.3 **ログ**された事象を見直し、最新情報にする。	AU-2 (3)	イベントログされた事象の見直しと更新	直接対応付け無し	
3.3.4 監査ログ取得（logging）プロセスが失敗した場合に警告を発する。	AU-5	監査ログ処理失敗への対応	直接対応付け無し	
3.3.5 非合法的または権限のない、疑わしいまたは異常な活動の徴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・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	
	AU-8	タイムスタンプ	A.12.4.4	クロックの同期

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・同期させるシステム機能を提供する。	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、不正なアクセス・改ざん・削除から保護する。	AU-9	監査情報の保護	A.12.4.2 A.12.4.3	ログ情報の保護 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[29]

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資産目録（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	システム構成要素の在庫	A.8.1.1	資産目録
			A.8.1.2	資産の管理責任
	CM-8 (1)	システム構成要素の在庫 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、セキュリティへの影響を分析する。	CM-4	セキュリティ影響分析	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
	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

[29] 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 SPP 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	
3.4.5 組織のシステム変更に関する物理的・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，試験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 必須能力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権限の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権限のあるソフトウェア実行を許可する。	CM-7 (4)	最小機能性 権限のないソフトウェア/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 権限のないソフトウェア/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）し確認（monitor）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 A.12.6.2	運用システムに関わるソフトウェアの導入 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と認証要件の対応付け[30]

セキュリティ要件	**NIST SP 800-53** 関連セキュリティ管理策		**ISO/IEC 27001** 関連セキュリティ管理策	
3.5 識別と認証				
基本セキュリティ要件				
3.5.1 システムのユーザー、ユーザーの代理として動作するプロセス、および装置を識別する。	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	装置の識別と認証	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、プロセスまたは装置のアイデンティティを認証（authenticate）（または検証（verify））する。	IA-5	認証符号の管理	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)	識別と認証（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)	識別と認証（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)	識別と認証（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)	識別と認証（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	

[30] 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。再生防止能力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)	識別と認証（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、識別子の再利用を防止する。	IA-4	識別子の管理	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、識別子を無効化する。	IA-4	識別子の管理	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)	認証符号の管理 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格納・伝送する。				
3.5.11 認証情報のフィードバックを隠す。	IA-6	認証符号のフィードバック	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、回復およびユーザー対応を含め、組織のシステムに運用状態のインシデント対応能力を確立する。 **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職員および/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*	情報セキュリティの意識向上、教育および訓練
	IR-4	インシデント取り扱い	A.16.1.4	情報セキュリティ事象の評価および決定
			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 情報セキュリティ事象の報告
	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能力をテストする。	IR-3	インシデント対応試験	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、および要員を管理する。	MA-2	被管理メンテナンス	A.11.2.4*	装置の保守
			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	直接対応付け無し	
	MA-3 (2)	検査ツール メンテナンスツール 検査ツール	直接対応付け無し	
派生セキュリティ要件				
3.7.3 現場外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*	装置の保守
			A.11.2.5*	資産の移動
3.7.4 診断および試験プログラムが入っている記憶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検査する。	MA-3 (2)	メンテナンスツール	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 必要なアクセス権限を持たないメンテナンス要員のメンテナンス活動を監督する。	MA-5	メンテナンス要員	直接対応付け無し	

表 D-8：セキュリティ管理策に対する記憶媒体の保護要件の対応付け[31]

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 記憶媒体の保護				
基本セキュリティ要件				
3.8.1 紙とデジタル双方とも、CUI を含むシステムの記憶媒体を保護する（すなわち、セキュアに格納し物理的に管理する）。 **3.8.2** システム記憶媒体上の CUI へのアクセスを、権限を有するユーザーに限定する。 **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。	MP-2	記憶媒体アクセス	A.8.2.3	資産の取扱い
			A.8.3.1	取外し可能な媒体の管理
			A.11.2.9	クリアデスク・クリアスクリーン方針
	MP-4	記憶媒体格納	A.8.2.3	資産の取扱い
			A.8.3.1	取外し可能な媒体の管理
			A.11.2.9	クリアデスク・クリアスクリーン方針
	MP-6	記憶媒体の情報除去	A.8.2.3	資産の取扱い
			A.8.3.1	取外し可能な媒体の管理
			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 の標記と配布制限が必要な記憶媒体にはその旨を標記する。	MP-3	記憶媒体への標記	A.8.2.2	情報のラベル付け
3.8.5 CUI を含む記憶媒体へのアクセスを管理し、管理区域外での輸送中は、記憶媒体に関する説明責任を維持する。	MP-5	記憶媒体の輸送	A.8.2.3	資産の取扱い
			A.8.3.1	取外し可能な媒体の管理
			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

[31] 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、「記憶媒体の保護」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	
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、デジタル記憶媒体上に格納された 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)	記憶媒体の輸送 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可搬型記憶媒体の使用を管理する。	MP-7	記憶媒体の使用	A.8.2.3	資産の取扱い
			A.8.3.1	取外し可能な媒体の管理
3.8.8 可搬型記憶装置の所有者を識別できない時には、そうした記憶装置の使用を禁止する。	MP-7 (1)	記憶媒体の使用 所有者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要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 要員のセキュリティ				
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権限を与えるに先立って、個人を審査する。 **3.9.2** 退職や異動などの人事処理中、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-3	要員審査	A.7.1.1	選考
	PS-4	要員解雇	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
	PS-5	要員異動	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、権限のある個人に限定する。 **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	出力装置のアクセス管理	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、その活動を確認する。	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 物理的アクセス装置を管理・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評価要件の対応付け

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 リスク評価				
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、格納、または通信から生ずる、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評価する。	RA-3	リスク評価	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 リスク評価（risk assessments）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評価要件の対応付け

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 セキュリティ評価				
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評価し、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・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確認する。	CA-2	セキュリティ評価	A.14.2.8	システムセキュリティの試験
			A.18.2.2	情報セキュリティのための方針群および標準の順守
			A.18.2.3	技術的順守のレビュー
	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と通信の保護要件の対応付け[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	
3.13 システムと通信の保護				
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・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、不正な情報転送や意図せぬ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・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。	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
			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

[32] 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、「システムと通信の保護」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	
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 遠隔装置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 の不正な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	
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

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	
3.13.10 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 協働コンピューティング装置のリモートからの活性化[33]を禁止し、その装置に存在するユーザーに対して使用中の装置を表示する。	SC-15	共同コンピューティング装置	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・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・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 通信セションの正当性（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

[33] 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。

表 **D-14**：セキュリティ管理策に対するシステムと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 システムと情報の完全性				
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警報（alert）および通報（advisory）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	情報セキュリティ事象の報告
	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	セキュリティ警報、注意報、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徴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 組織のシステムの不正使用を特定（identify）する。	SI-4	システムの監視	直接対応付け無し	

付属書 E

適応規準

中位セキュリティ管理策ベースラインおよび適応措置の一覧表

本付属書は、第 3 章に記述されたセキュリティ要件について、「FIPS 200」とともにその情報源の一つである「NIST SP 800-53」中位ベースラインにあるセキュリティ管理策の完全なリストを提供する。表 E-1 から表 E-17 には、NIST および NARA によって規定された適応規準に従って、中位ベースラインのセキュリティ管理策に基づいて遂行されている（ファミリー毎の）適応措置が含まれる[34]。この適応措置は、「FISP 200」のセキュリティ要件から得られた基本セキュリティ要件を補完する CUI 派生セキュリティ要件の開発を容易にした[35]。

中位ベースラインからセキュリティ管理策またはセキュリティ管理策強化版（enhancement）を削減する主要な規準は以下の 3 つである。

- 管理策または管理策強化版は、連邦政府固有のものである（主に連邦政府の責任）。
- 管理策または管理策強化版は、CUI の秘匿性保護に直接関係していない[36]。
- 管理策または管理策強化版は、明確化し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[37]。

表 E-1 から表 E-17 で使われる以下の記号は、講じられる特定の適応措置を示し、あるいは適応措置が必要とされないことを示す。

適応記号	適応規準
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	明確化し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。
CUI	CUI 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、セキュリティ管理策強化版、または管理策/管理策強化版の特定要素に反映されており、またそれらに起因している。

[34] 各組織は、「NIST SP 800-53」付属書 I で定義されているとおりに、CUI 秘匿性と同じもの を構築するために、付属書 E の情報を使うことができる。

[35] 同じ適応規準は、「FIPS 200」のセキュリティ要件にも適用され、第 3 章および付属書 D で説明されている CUI 基本セキュリティ要件をもたらしている。

[36] 本出版物の主要目的は、CUI の秘匿性を保護する要件の定義であるが、秘匿性と完全性のセキュリティ目的の間には密接な関係がある。それ故、権限のない開示に対する保護を支える「NIST SP 800-53」中位ベースラインのほとんどのセキュリティ管理策は、権限のない変更に対する保護も支えている。

[37] CUI の保護に関して「NIST SP 800-53」の中位ベースラインから適応されたセキュリティ管理策（すなわち、表 E-1 から表 E-17 で NCO または NFO と標示された管理策）は、組織の包括的セキュリティプログラムの一部として包含されることも多い。

表 **E-1**：アクセス管理の管理策のための適応措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		適応措置
AC-1	アクセス管理の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	モバイル装置用のアクセス管理	CUI
AC-19 (5)	モバイル装置用のアクセス管理 ｜ 装置/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 ｜ 権限を与えられた使用の限定	CUI
AC-20 (2)	外部システムの使用 ｜ 携帯型記憶装置	CUI
AC-21	情報の共有	FED
AC-22	公開の情報内容	CUI

表 **E-2**：意識向上と訓練の管理策のための適応措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		適応措置
AT-1	セキュリティ意識向上・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の訓練	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	ロール・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**：監査と説明責任の管理策のための適応措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		適応措置
AU-1	監査および説明責任のポリシーおよび手順	NFO
AU-2	監査事象	CUI
AU-2 (3)	監査事象 | 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	監査集積能力	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**：セキュリティ評価と認可の管理策のための適応措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		適応措置
CA-1	セキュリティ評価および認可のポリシーおよび手順	NFO
CA-2	セキュリティ評価	CUI
CA-2 (1)	セキュリティ評価 ｜ 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 ｜ 独立評価	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適応措置[38]

NIST SP 800-53 中位ベースラインセキュリティ管理策		適応措置
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、構成要素、および装置を構成	NFO
CM-3	構成変更管理	CUI
CM-3 (2)	構成変更管理 ｜ 変更を試験/確認/文書化	NFO
CM-4	セキュリティ影響分析	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	システム構成要素の在庫	CUI
CM-8 (1)	システム構成要素の在庫 ｜ 設置/除去時の更新	CUI
CM-8 (3)	システム構成要素の在庫 ｜ 非認可構成要素の自動検知	NCO
CM-8 (5)	システム構成要素の在庫 ｜ 構成要素の非重複記述	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

[38] CM-7 (5)「 最小機能 ホワイトリスト登録 」は、「NIST SP 800-53」に従って、中位セキュリティ管理ベースラインには入ってない。しかしながら、これは、ブラックリスト登録 に対する選択的かつ強力なポリシー代替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適応措置[39]

NIST SP 800-53 中位ベースラインセキュリティ管理策		適応措置
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	緊急時対応計画の試験	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/完全性の試験	NCO
CP-10	システムの回復および再構成	NCO
CP-10 (2)	システムの回復および再構成 ｜ トランザクションの復旧	NCO

[39] 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 は、付属書 D の表 D-8「記憶媒体の保護」 ファミリーに包含されている。

表 **E-7**：識別と認証の管理策のための適応措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		適応措置
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)	識別と認証（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)	認識と認証（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)	識別と認証（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)	識別と認証（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)	識別と認証（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)	識別と認証（組織のユーザー）｜リモートアクセス（分離装置）	FED
IA-2 (12)	識別と認証（組織のユーザー）｜*PIV* クレデンシャルの受領	FED
IA-3	装置の識別と認証	CUI
IA-4	識別子の管理	CUI
IA-5	認証符号の管理	CUI
IA-5 (1)	認証符号の管理｜パスワードベース認証	CUI
IA-5 (2)	認証符号の管理｜*PKI* ベース認証	FED
IA-5 (3)	認証符号の管理 ｜対面（*IN-PERSON*）または信頼されたサードパーティー登録	FED
IA-5 (11)	認証符号の管理｜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	識別と認証（非組織ユーザー）	FED
IA-8 (1)	識別と認証（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)	識別と認証（非組織ユーザー） ｜サードパーティークレデンシャルの受領	FED
IA-8 (3)	識別と認証（非組織ユーザー）｜*FICAM* 承認済み製品の使用	FED
IA-8 (4)	識別と認証（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適応措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		適応措置
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	インシデント対応試験	CUI
IR-3 (2)	インシデント対応試験 | 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適応措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		適応措置
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	メンテナンス要員	CUI
MA-6	時宜を得たメンテナンス	NCO

表 **E-10**：記憶媒体の保護の管理策のための適応措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		適応措置
MP-1	記憶媒体の保護ポリシーおよび手順	NFO
MP-2	記憶媒体へのアクセス	CUI
MP-3	記憶媒体への標記	CUI
MP-4	記憶媒体の格納	CUI
MP-5	記憶媒体の輸送	CUI
MP-5 (4)	記憶媒体の輸送 ｜ 暗号保護	CUI
MP-6	記憶媒体の情報除去	CUI
MP-7	記憶媒体の使用	CUI
MP-7 (1)	記憶媒体の使用 ｜ 所有者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適応措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		適応措置
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	通信媒体用のアクセス管理	CUI
PE-5	出力装置用のアクセス管理	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	電力設備と敷設ケーブル	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・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適応措置

NIST SP 800-53 中位ベースラインセキュリティ管理		適応措置
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	実施規定	NFO
PL-4 (1)	実施規定 | 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**：要員のセキュリティの管理策のための適応措置

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

表 **E-14**：リスク評価の管理策のための適応措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		適応措置
RA-1	リスク評価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	リスク評価	CUI
RA-5	脆弱性検査（scanning）	CUI
RA-5 (1)	脆弱性検査 ｜ ツール能力の更新	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適応措置[40]

NIST SP 800-53 中位ベースラインセキュリティ管理策		適応措置
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試験および評価	NFO

[40] 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 は、付属書 D の「システムおよび通信保護」ファミリーの中のセキュリティ管理にグループ化されている。

表 **E-16**：システムと通信の保護の管理策のための適応措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		適応措置
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)	境界保護 ｜デフォルト設定による拒否/例外による許可	CUI
SC-7 (7)	境界保護 ｜ 遠隔装置へのスプリットトンネリング（*Sprit Tunneling*）を防止	CUI
SC-8	通信の秘匿性と完全性	CUI
SC-8 (1)	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	CUI
SC-10	ネットワークの切断	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装置	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	セキュアネーム/アドレス解決サービス（Secure Name / Address Resolution Service）	NFO
SC-21	セキュアネーム/アドレス解決サービス（Secure Name / Address Resolution Service）	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**：システムと情報の完全性の管理策のための適応措置

NIST SP 800-53 中位ベースラインセキュリティ管理策		適応措置
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警報	NFO
SI-5	セキュリティ警報、注意報、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

APPENDIX F

DISCUSSION

IMPLEMENTING AND ASSESSING CUI SECURITY REQUIREMENTS

Tables F-1 through F-14 provide discussion intended to facilitate implementing and assessing the CUI security requirements in NIST Special Publication 800-171. This information is derived primarily from the security controls and discussion in NIST Special Publication 800-53. It is provided to give assessors a better understanding of the mechanisms and procedures used to implement the safeguards employed to protect CUI. The discussion is *not* intended to extend the security requirements or the scope of the assessments of those requirements. NIST publications identified in the following tables are available at https://csrc.nist.gov/publications.

TABLE F-1: DISCUSSION ON ACCESS CONTROL REQUIREMENTS

3.1.1	**SECURITY REQUIREMENT** Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	DISCUSSION Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for both systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses non-privileged) are addressed in requirement 3.1.2.
3.1.2	**SECURITY REQUIREMENT** Limit system access to the types of transactions and functions that authorized users are permitted to execute.
	DISCUSSION Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. System account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, and temporary. Other attributes required for authorizing access include, for example: restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations may consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission or business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements).
3.1.3	**SECURITY REQUIREMENT** Control the flow of CUI in accordance with approved authorizations.
	DISCUSSION Information flow control regulates where information can travel within a system and between systems (as opposed to who can access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example: keeping export- controlled information from being transmitted in the clear to the Internet; blocking outside traffic that claims to be from within the organization; restricting requests to the Internet that are not from

付属書 F

考察 CUI に関するセキュリティ要件の実装および対応状況の評価

表 F-1 から F-14 は、NIST SP 800-171 の CUI に関するセキュリティ要件の実装および対応状況の評価を容易にするための考察を提供するものである。これらの情報は、主として NIST SP 800-53 のセキュリティ管理策と考察から派生されたものであり、CUI 保護のために採用された保全措置を実装する際に使用される仕組みや手続きに関して、対応状況の評価を行う者がより良く理解できるようにするために提供されるものである。なお、本考察はセキュリティ要件そのものまたはそれらの要件に対する対応状況の評価の範囲を拡大することは意図していない。また、以下の表中に示された NIST の出版物は、https://csrc.nist.gov/publications から入手可能である。

表 F-1：「アクセス管理」要件に関する考察

3.1.1	**セキュリティ要件** システムへのアクセスは、権限のあるユーザー、権限のあるユーザーの代理として動作するプロセスおよび（その他のシステムを含む）装置に限定する。
	考察 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の代理とし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、装置、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。アカウントの種類（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権限以外のアクセス権限の定義および実施は3.1.2で扱われる。
3.1.2	**セキュリティ要件** システムへのアクセスは、権限のあるユーザーが実行を許可されている各種のトランザクションおよび機能に限定する。
	考察 組織は、アクセス特権やその他の属性を、アカウント、アカウントの種類、またはそれらの組み合わせによって定義してよい。システムアカウントの種類には、たとえば、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求められるその他の属性には、たとえば、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定義する際、システムに関連する要件（たとえば、定期メンテナンスやシステムアップグレードなど）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）について考慮することができる。
3.1.3	**セキュリティ要件** 承認された権限に従って、CUIの一連の取扱い手続き（flow）を管理する。
	考察 情報の一連の取り扱い手続の管理は、（情報にアクセスすることができる人を規定するのではなく）システム内およびシステム間において情報を伝達できる範囲を規定する。一方、そうした情報へのその後のアクセスに関しては、明示的に規定しない。情報の管理には、たとえば、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伝送できないようにすること、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、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、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制限すること、などの制限が含まれる。

	the internal web proxy server; and limiting information transfers between organizations based on data structures and content. Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within systems and between interconnected systems. Flow control is based on characteristics of the information or the information path. Enforcement occurs in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict system services, provide a packet- filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering and inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Transferring information between systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: prohibiting information transfers between interconnected systems (i.e., allowing access only); employing hardware mechanisms to enforce one-way information flows; and implementing trustworthy regrading mechanisms to reassign security attributes and security labels.
3.1.4	**SECURITY REQUIREMENT** Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
	DISCUSSION Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: dividing mission functions and system support functions among different individuals or roles; conducting system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and ensuring that security personnel administering access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of organizational systems and system components when developing policy on separation of duties.
3.1.5	**SECURITY REQUIREMENT** Employ the principle of least privilege, including for specific security functions and privileged accounts.
	DISCUSSION Organizations employ the principle of least privilege for specific duties and authorized accesses for users and processes. The principle of least privilege is applied with the goal of authorized privileges no higher than necessary to accomplish required organizational missions or business functions. Organizations consider the creation of additional processes, roles, and system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational systems. Security functions include, for example, establishing system accounts, setting events to be logged, setting intrusion detection parameters, and configuring access authorizations (i.e., permissions, privileges). Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information or functions. Organizations may differentiate in the application of this requirement between allowed privileges for local accounts and for domain accounts provided organizations retain the

	組織では通常、システム内および相互接続されたシステム間における指定された送信元と送信先（たとえばネットワーク、個人、装置など）との間の情報の一連の取り扱い手続を管理するため、情報の一連の取り扱い手続の管理ポリシーおよび実施メカニズムを採用する。情報の一連の取り扱い手続は、情報および情報経路の特性に基づいて管理される。情報の一連の取り扱い手続の管理は、境界保護装置（たとえば、ゲートウェイ、ルーター、ガード、暗号化トンネル、ファイアウォールなど）において実施される。境界保護装置とは、システムサービスを制限する一連の規則を採用する、またはシステムサービスを制限する構成設定を構築する装置や、ヘッダー情報に基づいたパケットフィルタリング機能やメッセージのコンテンツに基づいたメッセージフィルタリング機能（たとえば、キーワード検索を実装するまたはドキュメントの特性を使用する機能）を提供する装置である。組織は、情報の一連の取り扱い手続の管理の実施に不可欠なフィルタリングおよび検査メカニズム（たとえば、ハードウェアコンポーネント、ファームウェアコンポーネント、ソフトウェアコンポーネントなど）の信頼性についても検討する。 異なるセキュリティポリシーを有する異なるセキュリティドメインのシステム間で情報がやり取りされる場合、1つ以上のドメインセキュリティポリシーが違反されるリスクが生じる。そのような状況において、情報のオーナー／スチュワード（管理者）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点におけるガイダンスを提供する。また、組織は、特定のセキュリティポリシーの実施が必要な場合において、特定のアーキテクチャー解決策を義務付けることを検討する。セキュリティポリシーの実施には、たとえば、相互接続されたシステム間での情報のやり取りを禁止する（つまり、アクセスのみを許可する）こと、情報の一連の取り扱い手続を一方向に強制するハードウェアメカニズムを採用すること、ならびに、セキュリティ属性とセキュリティラベルを再度割り当てる信頼できるメカニズムを実装すること、などが含まれる。
3.1.4	**セキュリティ要件** 共謀のない有害行動のリスクを減らすため、個人の職務を分離する。
	考察 職務の分離は、権限を付与された特権が悪用される可能性に対処し、共謀のない有害行動のリスクを減らすために役立つ。たとえば、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、異なる個人がシステムサポートの機能（たとえば、システム管理、プログラミング、構成管理、品質保証・品質試験、ネットワークセキュリティなど）を実施すること、また、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、などが職務の分離に含まれる。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	**セキュリティ要件** 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。
	考察 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権限に対して、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権限を付与することを目的として適用される。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・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、たとえば、システムアカウントの作成、ログに出力する事象の設定、不正侵入検知パラメータの設定、アクセス権限（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、市販の様々な種類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要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。

	ability to control system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.
3.1.6	**SECURITY REQUIREMENT** Use non-privileged accounts or roles when accessing nonsecurity functions.
	DISCUSSION This requirement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.
3.1.7	**SECURITY REQUIREMENT** Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
	DISCUSSION Privileged functions include, for example, establishing system accounts, performing system integrity checks, conducting patching operations, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and intrusion prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users. Note that this requirement represents a condition to be achieved by the definition of authorized privileges in 3.1.2. Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat.
3.1.8	**SECURITY REQUIREMENT** Limit unsuccessful logon attempts.
	DISCUSSION This requirement applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are, in most cases, temporary and automatically release after a predetermined period established by the organization (i.e., a delay algorithm). If a delay algorithm is selected, organizations may employ different algorithms for different system components based on the capabilities of the respective components. Responses to unsuccessful logon attempts may be implemented at the operating system and the application levels.
3.1.9	**SECURITY REQUIREMENT** Provide privacy and security notices consistent with applicable CUI rules.
	DISCUSSION System use notifications can be implemented using messages or warning banners displayed before individuals log in to organizational systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Based on an assessment of risk, organizations consider whether a secondary system use notification is needed to access applications or other system resources after the initial network logon. Where necessary, posters or other printed materials may be used in lieu of an automated system banner. Organizations should consult with the Office of the General Counsel for legal review and approval of warning banner content.

3.1.6	**セキュリティ要件** 非セキュリティ機能にアクセスする際は、非特権アカウントまたは役割を使用する。
	考察 このセキュリティ要件は、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防止するものである。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の代理として動作するプロセスのアクセス権限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	**セキュリティ要件** 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（audit logs）に取り込む（capture）。
	考察 特権機能には、たとえば、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、適切な権限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・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があげられる。なお、このセキュリティ要件は、3.1.2.で定義される特権によって実現される状態を示している。 権限のある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、またはシステムアカウントに不正侵入した外部の権限を持た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、組織に著しい悪影響を及ぼしかねない。特権機能の使用を記録することは、そうした誤用を検知する1つの方法でもあり、内部の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	**セキュリティ要件** ログオン試行失敗回数を限定する。
	考察 このセキュリティ要件は、ログオンがローカル接続またはネットワーク接続を介しているかを問わず適用される。サービスが拒否される可能性があることから、多くの場合、システムが引き起こす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機能に基づいて、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よい。ログオン試行の失敗に対する応答は、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よい。
3.1.9	**セキュリティ要件** 適用されるCUI規則に則って、プライバシーおよびセキュリティ通知する。
	考察 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ーフェースを介してアクセスする場合にのみ使用され、人によるインター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、リスク対応状況の評価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、法的面の審査と承認を得るべきである。

3.1.10	**SECURITY REQUIREMENT** Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
	DISCUSSION Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of the system but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined, typically at the operating system level (but can also be at the application level). Session locks are not an acceptable substitute for logging out of the system, for example, if organizations require users to log out at the end of the workday. Pattern-hiding displays can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey controlled unclassified information.
3.1.11	**SECURITY REQUIREMENT** Terminate (automatically) a user session after a defined condition.
	DISCUSSION This requirement addresses the termination of user-initiated logical sessions in contrast to the termination of network connections that are associated with communications sessions (i.e., disconnecting from the network). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on system use.
3.1.12	**SECURITY REQUIREMENT** Monitor and control remote access sessions.
	DISCUSSION Remote access is access to organizational systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example: dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate safeguards (e.g., employing encryption techniques for confidentiality protection), may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. VPNs with encrypted tunnels can affect the capability to adequately monitor network communications traffic for malicious code. Automated monitoring and control of remote access sessions allows organizations to detect cyber- attacks and help to ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of system components (e.g., servers, workstations, notebook computers, smart phones, and tablets). NIST Special Publications 800-46, 800-77, and 800-113 provide guidance on secure remote access and virtual private networks.

3.1.10	**セキュリティ要件** 非アクティブな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。
	考察 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においてセション・アクティビティが見られる場合に実行される（ただし、アプリケーションレベルにおいて実行することもできる）。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、写真画像、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	**セキュリティ要件** 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）終結させる。
	考察 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（またはユーザーの代理とし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、たとえば、組織が規定したユーザーの非アクティブな時間、特定の種類のインシデントに対する対応、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	**セキュリティ要件** リモートアクセスセションを監視し、管理する。
	考察 リモートアクセスとは、ユーザー（またはユーザーの代理とし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、たとえば、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、適切な保全措置を設けて（たとえば、秘匿性保護のために暗号技術を導入して）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、ネットワーク通信トラフィックを悪意のあるコード検知のために監視する能力に影響を及ぼす。 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活動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。 NIST SP 800-46、SP 800-77、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	**SECURITY REQUIREMENT** Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
	DISCUSSION Generally applicable cryptographic standards include FIPS-validated cryptography and NSA- approved cryptography. See NIST Cryptographic Standards; NIST Cryptographic Module Validation Program; NIST Cryptographic Algorithm Validation Program; NSA Cryptographic Standards.
3.1.14	**SECURITY REQUIREMENT** Route remote access via managed access control points.
	DISCUSSION Routing all remote access through managed access control points enhances explicit, organizational control over such connections, reducing the susceptibility to unauthorized access to organizational systems resulting in the unauthorized disclosure of CUI.
3.1.15	**SECURITY REQUIREMENT** Authorize remote execution of privileged commands and remote access to security- relevant information.
	DISCUSSION A privileged command is a human-initiated (interactively or via a process operating on behalf of the human) command executed on a system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information. Security-relevant information is any information within the system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Privileged commands give individuals the ability to execute sensitive, security-critical, or security-relevant system functions. Controlling such access from remote locations helps to ensure that unauthorized individuals are not able to execute such commands freely with the potential to do serious or catastrophic damage to organizational systems. Note that the ability to affect the integrity of the system is considered security-relevant as that could enable the means to by-pass security functions although not directly impacting the function itself.
3.1.16	**SECURITY REQUIREMENT** Authorize wireless access prior to allowing such connections.
	DISCUSSION Establishing usage restrictions and configuration/connection requirements for wireless access to the system provides criteria for organizations to support wireless access authorization decisions. Such restrictions and requirements reduce the susceptibility to unauthorized access to the system through wireless technologies. Wireless networks use authentication protocols which provide credential protection and mutual authentication. NIST Special Publications 800-48 and 800-97 provide guidance on secure wireless networks.

3.1.13	**セキュリティ要件** 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。
	考察 一般的に適用される暗号標準は、FIPS認証の暗号およびNSA承認の暗号である。 詳細は、NIST 暗号標準（Cryptographic Standards）、NIST 暗号モジュール認証制度（Cryptographic Module Validation Program）、NIST 暗号アルゴリズム認証制度（Cryptographic Algorithm Validation Program）、NSA 暗号標準（Cryptographic Standards）を参照。
3.1.14	**セキュリティ要件** 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。
	考察 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の不正な開示を誘発するような組織のシステムへの不正アクセスを受けにくくする。
3.1.15	**セキュリティ要件** 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に権限を付与する。
	考察 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・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影響を及ぼす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、取扱いに注意すべきシステム機能、セキュリティに重要なシステム機能、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、権限のない個人が、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影響を及ぼさないにしても、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	**セキュリティ要件** ワイヤレスアクセスの接続を許可する前に、そうしたアクセスに権限を付与する。
	考察 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、システムは不正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。 NIST SP 800-48 、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	**SECURITY REQUIREMENT** Protect wireless access using authentication and encryption.
	DISCUSSION Organizations can authenticate individuals and devices to help protect wireless access to the system. Special attention should be given to the wide variety of devices that are part of the Internet of Things with potential wireless access to organizational systems. See NIST Cryptographic Standards.
3.1.18	**SECURITY REQUIREMENT** Control connection of mobile devices.
	DISCUSSION A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, or built-in features for synchronizing local data with remote locations. Examples of mobile devices include smart phones, e-readers, and tablets. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different types of devices. Usage restrictions and implementation guidance for mobile devices include, for example: configuration management; device identification and authentication; implementation of mandatory protective software (e.g., malicious code detection, firewall); scanning devices for malicious code; updating virus protection software; scanning for critical software updates and patches; conducting primary operating system (and possibly other resident software) integrity checks; and disabling unnecessary hardware (e.g., wireless, infrared). The need to provide adequate security for mobile devices goes beyond this requirement. Many safeguards for mobile devices are reflected in other CUI security requirements. NIST Special Publication 800-124 provides guidance on mobile device security.
3.1.19	**SECURITY REQUIREMENT** Encrypt CUI on mobile devices and mobile computing platforms.
	DISCUSSION Organizations can use full-device encryption or container-based encryption to protect the confidentiality of CUI on mobile devices and computing platforms. Container-based encryption provides a more fine-grained approach to the encryption of data and information including, for example, encrypting selected data structures such as files, records, or fields. See NIST Cryptographic Standards.
3.1.20	**SECURITY REQUIREMENT** Verify and control/limit connections to and use of external systems.
	DISCUSSION External systems are systems or components of systems for which organizations typically have no direct supervision and authority over the application of security requirements and controls or the determination of the effectiveness of implemented safeguards on those systems. External systems include, for example, personally owned systems or devices and privately-owned computing and communications devices resident in commercial or public facilities. This requirement also addresses the use of external systems for the processing, storage, or transmission of CUI, including accessing

3.1.17	**セキュリティ要件** 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。
	考察 組織は、個人および装置を認証して、システムに対するワイヤレスアクセスを保護することができる。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装置に対して注意が必要である。 詳細は、NIST 暗号標準（Cryptographic Standards）を参照すること。
3.1.18	**セキュリティ要件** モバイル装置の接続を管理（control）する。
	考察 モバイル装置とは、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、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、非可搬型または可搬型のローカルなデータ記憶装置を有し、かつ、電源を内蔵しているコンピュータデバイスのことである。モバイル装置には、音声通信機能、モバイル装置が情報を取得するための内臓センサー、またはローカルデータをリモート位置と同期させる組み込み機能も含まれることがある。モバイル装置は、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機能を備える様々なモバイル装置が存在するため、異なる種類の装置ごとに組織の制限を変更してもよい。モバイル装置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、たとえば、構成管理、装置の識別・認証、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）、悪意のあるコードを検知する装置のスキャン、ウイルス対策ソフトウェアのアップデート、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、主要オペレーティングシステムの完全性チェックの実施、ならびに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。モバイル装置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、モバイル装置のための数多くの保全措置は、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。 NIST SP 800-124 は、モバイル装置のセキュリティに関するガイダンスを提供する。
3.1.19	**セキュリティ要件** モバイル装置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。
	考察 組織は、モバイル装置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使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、たとえば、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。 詳細は、NIST 暗号標準（Cryptographic Standards）を参照すること。
3.1.20	**セキュリティ要件** 外部システムへの接続および使用を検証（verify）し、管理／制限する。
	考察 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保全措置の有効性の判定に関して、組織が直接管理できない、また、直接の権限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、たとえば、個人が所有するシステムまたは装置に加え、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装置および通信装置などが含まれる。このセキュリティ要件は、組織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・格納・伝送する外部システムの使用も対象とする。

	cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational systems. Organizations establish terms and conditions for the use of external systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum, the types of applications that can be accessed on organizational systems from external systems. If terms and conditions with the owners of external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems. This requirement recognizes that there are circumstances where individuals using external systems (e.g., contractors, coalition partners) need to access organizational systems. In those situations, organizations need confidence that the external systems contain the necessary safeguards so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required safeguards have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the assurance or confidence level required by organizations. Note that while “external” typically refers to outside of the organization’s direct supervision and authority, that is not always the case. Regarding the protection of CUI across an organization, the organization may have systems that process CUI and others that do not. And among the systems that process CUI there are likely access restrictions for CUI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered “external" to that system.
3.1.21	**SECURITY REQUIREMENT** Limit use of portable storage devices on external systems.
	DISCUSSION Limits on the use of organization-controlled portable storage devices in external systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used. Note that while “external” typically refers to outside of the organization’s direct supervision and authority, that is not always the case. Regarding the protection of CUI across an organization, the organization may have systems that process CUI and others that do not. And among the systems that process CUI there are likely access restrictions for CUI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered “external" to that system.
3.1.22	**SECURITY REQUIREMENT** Control CUI posted or processed on publicly accessible systems.
	DISCUSSION In accordance with laws, Executive Orders, directives, policies, regulations, or standards, the public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act, CUI, and proprietary information). This requirement addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Individuals authorized to post CUI onto publicly accessible systems are designated. The content of information is reviewed prior to posting onto publicly accessible systems to ensure that nonpublic information is not included.

	組織は、セキュリティポリシーおよびセキュリティ手続きに則り、外部システムの使用に関する条件を定める。条件は、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種類を少なくとも定める。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要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（たとえば請負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、組織のシステムを危険にさらさないように、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保全措置を備えていることを、組織は確証する必要がある。必要な保全措置が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、たとえば第三者の独立した対応状況の評価、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、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	**セキュリティ要件** 外部システム上での可搬型記憶装置の使用を制限する。
	考察 組織が管理する可搬型記憶装置を外部システムで使用する際の制限には、たとえば、そうした装置の使用を全面的に禁止することや、そうした装置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。
3.1.22	**セキュリティ要件** 公衆（publicly）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。
	考察 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）にアクセスする権限を持たない。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。

TABLE F-2: DISCUSSION ON AWARENESS AND TRAINING REQUIREMENTS

3.2.1	**SECURITY REQUIREMENT** Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
	DISCUSSION Organizations determine the content and frequency of security awareness training and security awareness techniques based on the specific organizational requirements and the systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, formal training, offering supplies inscribed with security reminders, generating email advisories or notices from organizational officials, displaying logon screen messages, displaying posters, and conducting information security awareness events. NIST Special Publication 800-50 provides guidance on security awareness and training programs.
3.2.2	**SECURITY REQUIREMENT** Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.
	DISCUSSION Organizations determine the content and frequency of security training based on the assigned duties, roles, and responsibilities of individuals and the security requirements of organizations and the systems to which personnel have authorized access. In addition, organizations provide system developers, enterprise architects, security architects, acquisition/procurement officials, software developers, system developers, system or network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards. Such training can include, for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. NIST Special Publication 800-181 provides guidance on role-based information security training in the workplace.
3.2.3	**SECURITY REQUIREMENT** Provide security awareness training on recognizing and reporting potential indicators of insider threat.
	DISCUSSION Potential indicators and possible precursors of insider threat include behaviors such as: inordinate, long-term job dissatisfaction; attempts to gain access to information that is not required for job performance; unexplained access to financial resources; bullying or sexual harassment of fellow employees; workplace violence; and other serious violations of organizational policies, procedures, directives, rules, or practices. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role (e.g., training for managers may be focused on specific changes in behavior of team members, while training for employees may be focused on more general observations).

表 F-2：「意識向上と訓練」要件に関する考察

3.2.1	**セキュリティ要件** 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、規格および手続き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。
	考察 組織は、組織の具体的な要件および要員がアクセス権限を有するシステムに基づいて、セキュリティ意識向上と訓練の内容および頻度を決定するとともに、セキュリティ意識を向上させる手法を決定する。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を向上させる。セキュリティ意識を向上させる手法については、たとえば、正式な訓練の実施、セキュリティの注意喚起が記されたグッズの提供、組織の職員からの電子メールによる勧告や通知、ログオン画面におけるメッセージの表示、ポスターの掲示、および情報セキュリティ意識向上イベントの実施などがあげられる。 NIST SP 800-50 は、セキュリティ意識の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	**セキュリティ要件** 要員が、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。
	考察 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要員がアクセス権限を有す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・調達部門職員、ソフトウェア開発者、システム開発者、システム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・監査担当者、独立した検証と確認を行う要員、セキュリティ対応状況の評価者、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要員に対して、各々の割り当てられた職務に特別に合わせた適切な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・技術的な保全措置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、手続き、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。 NIST 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。
3.2.3	**セキュリティ要件** インサイダーによる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。
	考察 インサイダーによる脅威の潜在的兆候および予想される前兆には、長期にわたる仕事への多大な不満、業務の遂行に不必要な情報へのアクセスの試行、金融資産の無断使用、同僚に対するいじめやセクシュアル・ハラスメント、職場内暴力、組織のポリシー・手続き・指令・規則・慣行に対する重大な違反、などの振る舞いが含まれる。セキュリティ意識向上訓練では、インサイダーによる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続き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、インサイダーによる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、管理職員を対象とした訓練では、チームメンバーの振る舞いにおける特別な変化を重視する一方、一般職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）。

TABLE F-3: DISCUSSION ON AUDIT AND ACCOUNTABILITY REQUIREMENTS

3.3.1	**SECURITY REQUIREMENT** Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
	DISCUSSION An event is any observable occurrence in a system, which includes unlawful or unauthorized system activity. Organizations identify event types for which a logging functionality is needed as those events which are significant and relevant to the security of systems and the environments in which those systems operate to meet specific and ongoing auditing needs. Event types can include, for example, password changes, failed logons or failed accesses related to systems, administrative privilege usage, or third-party credential usage. In determining event types that require logging, organizations consider the monitoring and auditing appropriate for each of the CUI security requirements. Monitoring and auditing requirements can be balanced with other system needs. For example, organizations may determine that systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit logging capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of event types, the logging necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented or cloud-based architectures. Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the system after the event occurred). Detailed information that organizations may consider in audit records includes, for example, full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit log information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest. Audit logs are reviewed and analyzed as often as needed to provide important information to organizations to facilitate risk-based decision making. NIST Special Publication 800-92 provides guidance on security log management.
3.3.2	**SECURITY REQUIREMENT** Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.
	DISCUSSION This requirement ensures that the contents of the audit record include the information needed to link the audit event to the actions of an individual to the extent feasible. Organizations consider logging for traceability including, for example, results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, use of maintenance tools, nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, system component inventory, communications at the system boundaries, use of mobile code, and use of VoIP.

表 F-3：「監査と説明責任」要件に関する考察

3.3.1	**セキュリティ要件** 非合法的または権限の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。
	考察 事象とは、非合法的または権限のないシステム活動を含め、システム内で発生する観察可能なあらゆる活動を指す。組織は、システムのセキュリティおよびシステムの運用環境に関係する重要な事象を、ログに出力すべき事象としてみなし、特定の継続的監査の必要性に対応する。事象の種別には、たとえば、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、または第三者のクレデンシャルの使用などがある。ログに出力される事象の種別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・監査を検討する。監視・監査要件と、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する機能をシステムに求める一方で、このような機能は、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、監査ログ取得機能の重要な側面であり、問題の根本原因の特定を容易にする。組織は、事象の種別を定義する際、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、関連する事象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、たとえば、タイムスタンプ、送信元アドレス、送信先アドレス、ユーザー識別子、プロセス識別子、事象の説明、成功判定、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規則などが含まれる。事象の結果には、事象の成功判定または失敗判定および事象固有の結果（たとえば、事象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、たとえば、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円滑に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。 NIST 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	**セキュリティ要件** 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。
	考察 このセキュリティ要件は、監査事象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的とする。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、たとえば、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、モバイル装置の接続、構成設定、メンテナンスツールの使用、非ローカルメンテナンス、物理的アクセス、温度・湿度、機器の搬入・撤去、システムコンポーネントの一覧表（inventory）、システム境界における通知、モバイルコードの使用、ならびにVoIPの使用などが含まれる。

3.3.3	**SECURITY REQUIREMENT** Review and update logged events.
	DISCUSSION The intent of this requirement is to periodically re-evaluate which of the logged events will continue to be included in the list of events to be logged. Over time, the event types that are logged by organizations may change. Reviewing and updating the set of logged event types periodically is necessary to ensure that the current set remains necessary and sufficient.
3.3.4	**SECURITY REQUIREMENT** Alert in the event of an audit logging process failure.
	DISCUSSION Audit logging process failures include, for example, software/hardware errors, failures in the audit record capturing mechanisms, and audit record storage capacity being reached or exceeded. This requirement applies to each audit record data storage repository (i.e., distinct system component where audit records are stored), the total audit record storage capacity of organizations (i.e., all audit record data storage repositories combined), or both.
3.3.5	**SECURITY REQUIREMENT** Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
	DISCUSSION Correlating these processes helps to ensure that they do not operate independently, but rather collectively. Regarding the assessment of a given organizational system, the requirement is agnostic as to whether this correlation is applied at the system level or at the organization level across all systems.
3.3.6	**SECURITY REQUIREMENT** Provide audit record reduction and report generation to support on-demand analysis and reporting.
	DISCUSSION Audit record reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or organizational entities conducting auditing activities. Audit record reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can help generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the time stamp in the record is insufficient.
3.3.7	**SECURITY REQUIREMENT** Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
	DISCUSSION Internal system clocks are used to generate time stamps, which include date and time. Time is expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication,

3.3.3	**セキュリティ要件** ログされた事象を見直し、最新情報にする。
	考察 このセキュリティ要件は、ログされた事象のうち、何れの事象を継続的に一覧に含めるかを定期的に見直すことを目的とする。組織によりログされた事象の種別は、時間の経過と共に変化することがある。事象の種別の一式を見直し、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	**セキュリティ要件** 監査ログ取得（logging）プロセスが失敗した場合に警告を発する。
	考察 監査ログ取得プロセスの失敗には、たとえば、ソフトウェア／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	**セキュリティ要件** 非合法的または権限のない、疑わしいまたは異常な活動の徴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。
	考察 これらのプロセスを相互に関連付けることによって、これらのプロセスは、独立して動作するのではなく一体的に動作するようになる。組織のシステムを対応状況の評価するにあたり、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	**セキュリティ要件** オンデマンドでの分析・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。
	考察 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は、必ずしも監査を実施する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挙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術を、監査記録の集約機能に含むことができる。システムが提供する報告書の生成機能は、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細かさ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り得る。
3.3.7	**セキュリティ要件** 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・同期させるシステム機能を提供する。
	考察 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。時間単位の細かさは、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細かさを定めることができる。アクセス制御および識別・認証などその他のセキュリティ機能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、それらの機能にとっても不可欠な場合がある。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

	depending on the nature of the mechanisms used to support those capabilities. This requirement provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network. See IETF Network Time Protocol.
3.3.8	**SECURITY REQUIREMENT** Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
	DISCUSSION Audit information includes all information (e.g., audit records, audit log settings, and audit reports) needed to successfully audit system activity. Audit logging tools are those programs and devices used to conduct audit and logging activities. This requirement focuses on the technical protection of audit information and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by media protection and physical and environmental protection requirements.
3.3.9	**SECURITY REQUIREMENT** Limit management of audit logging functionality to a subset of privileged users.
	DISCUSSION Individuals with privileged access to a system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit logging activities or modifying audit records. This requirement specifies that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.

	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。 詳細は、IETFのネットワークタイムプロトコル（Network Time Protocol）を参照すること。
3.3.8	**セキュリティ要件** 監査情報および監査ログ取得ツールを、不正なアクセス・改ざん・削除から保護する。
	考察 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装置のことである。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権限のある個人に限定する。監査情報の物理的な保護については、記憶媒体の保護に関する要件ならびに物理的・環境保護に関する要件で取り扱われる。
3.3.9	**セキュリティ要件** 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。
	考察 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。

TABLE F-4: DISCUSSION ON CONFIGURATION MANAGEMENT REQUIREMENTS

3.4.1	**SECURITY REQUIREMENT** Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
	DISCUSSION This requirement establishes baseline configurations for systems and system components including communications and connectivity aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-upon sets of specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and changes to systems. Baseline configurations include information about system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and update and patch information on operating systems and applications; and configuration settings and parameters), network topology, and the logical placement of those components within the system architecture. Baseline configurations of systems reflect the current enterprise architecture. Maintaining effective baseline configurations requires creating new baselines as organizational systems change over time. Baseline configuration maintenance includes reviewing and updating the baseline configuration when changes are made based on security risks and deviations from the established baseline configuration Organizations can implement centralized system component inventories that include components from multiple organizational systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., system association, system owner). Information deemed necessary for effective accountability of system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location. NIST Special Publication 800-128 provides guidance on security-focused configuration management
3.4.2	**SECURITY REQUIREMENT** Establish and enforce security configuration settings for information technology products employed in organizational systems.
	DISCUSSION Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers, workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, devices, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security parameters are those parameters impacting the security state of systems including the parameters required to satisfy other security requirements. Security parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the systems configuration baseline. Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product

表 F-4：「構成管理」要件に関する考察

3.4.1	**セキュリティ要件** 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資産目録（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。
	考察 このセキュリティ要件により、システムの通信・接続の側面を含め、システムおよびシステムコンポーネントの基本（baseline）構成が既定される。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・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、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、またはモバイル装置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；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・パッチ情報；および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。基本構成の保守には、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所有者など）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、たとえば、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、コンポーネント所有者、ネットワークコンポーネント、また、ネットワーク装置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、たとえば、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。 NIST 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	**セキュリティ要件** 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。
	考察 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状況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定義できる情報技術製品には、たとえば、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、入出力装置（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、ルーター、ゲートウェイ、音声・データスイッチ、装置、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影響す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、たとえば、レジストリーの設定、アカウント・ファイル・ディレクトリの許可設定、および機能・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・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

	developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. NIST Special Publications 800-70 and 800-128 provide guidance on security configuration settings.
3.4.3	**SECURITY REQUIREMENT** Track, review, approve or disapprove, and log changes to organizational systems.
	DISCUSSION Tracking, reviewing, approving/disapproving, and logging changes is called configuration change control. Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled and unauthorized changes, and changes to remediate vulnerabilities. Processes for managing configuration changes to systems include, for example, Configuration Control Boards or Change Advisory Boards that review and approve proposed changes to systems. For new development systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards or Change Advisory Boards. Audit logs of changes include activities before and after changes are made to organizational systems and the activities required to implement such changes. NIST Special Publication 800-128 provides guidance on configuration change control.
3.4.4	**SECURITY REQUIREMENT** Analyze the security impact of changes prior to implementation.
	DISCUSSION Organizational personnel with information security responsibilities (e.g., system administrators, system security officers, system security managers, and systems security engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills and technical expertise to analyze the changes to systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security requirements and reviewing system design documentation to understand the implementation of safeguards and how specific changes might affect the safeguards. Security impact analyses may also include risk assessments to better understand the impact of the changes and to determine if additional safeguards are required. NIST Special Publication 800-128 provides guidance on configuration change control and security impact analysis.
3.4.5	**SECURITY REQUIREMENT** Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.
	DISCUSSION Any changes to the hardware, software, or firmware components of systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes, including upgrades and modifications. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access control requirements, workflow automation, media libraries, abstract layers (e.g., changes implemented into external interfaces rather than directly into systems), and change windows (e.g., changes occur only during specified times). In addition to security concerns, commonly-accepted due diligence for configuration

	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、たとえば、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・民間組織などによって策定される。 NIST 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。
3.4.3	**セキュリティ要件** 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、ログする。
	考察 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、試験、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、ルーター、モバイル装置など）の構成設定の変更、予定外または不正な変更、および脆弱性を解消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、たとえば、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・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。 NIST 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	**セキュリティ要件** 変更実施に先立って、セキュリティへの影響を分析する。
	考察 情報セキュリティに対して責任を負う組織の要員（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、セキュリティ影響分析を実施する。セキュリティ影響分析は、システムへの変更および関連するセキュリティへの影響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。セキュリティ影響分析には、たとえば、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、保全措置の実装方法ならびに特定の変更がどのように保全措置に影響するかを理解することが含まれる。また、セキュリティ影響分析には、変更の影響をより良く理解し、追加の保全措置が必要かを決定するためのリスク対応状況の評価も含まれる。 NIST 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	**セキュリティ要件** 組織のシステム変更に関する物理的・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。
	考察 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、権限のある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、たとえば、物理的・論理的アクセス制御に関する要件、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、外部インター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

	management includes access restrictions as an essential part in ensuring the ability to effectively manage the configuration. NIST Special Publication 800-128 provides guidance on configuration change control.
3.4.6	**SECURITY REQUIREMENT** Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.
	DISCUSSION Systems can provide a wide variety of functions and services. Some of the functions and services routinely provided by default, may not be necessary to support essential organizational missions, functions, or operations. It is sometimes convenient to provide multiple services from single system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per component. Organizations review functions and services provided by systems or components of systems, to determine which functions and services are candidates for elimination. Organizations disable unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of devices, transfer of information, and tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host- based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.
3.4.7	**SECURITY REQUIREMENT** Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
	DISCUSSION Restricting the use of nonessential software (programs) includes, for example, restricting the roles allowed to approve program execution; prohibiting auto-execute; program blacklisting and whitelisting; or restricting the number of program instances executed at the same time. The organization makes a security-based determination which functions, ports, protocols, and/or services are restricted. Bluetooth, FTP, and peer-to-peer networking are examples of protocols organizations consider preventing the use of, restricting, or disabling.
3.4.8	**SECURITY REQUIREMENT** Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
	DISCUSSION The process used to identify software programs that are not authorized to execute on systems is commonly referred to as blacklisting. The process used to identify software programs that are authorized to execute on systems is commonly referred to as whitelisting. Whitelisting is the stronger of the two policies for restricting software program execution. In addition to whitelisting, organizations consider verifying the integrity of whitelisted software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of whitelisted software can occur either prior to execution or at system startup. NIST Special Publication 800-167 provides guidance on application whitelisting.
3.4.9	**SECURITY REQUIREMENT** Control and monitor user-installed software.
	DISCUSSION Users can install software in organizational systems if provided the necessary privileges. To maintain control over the software installed, organizations identify permitted and prohibited

	て、アクセス制限は、構成管理を効果的に実施するうえで欠かせないものとして、適切な注意が払われることが一般に認識されている。 NIST 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	**セキュリティ要件** 必須能力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。
	考察 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、組織の根幹的なミッション、機能、または事業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、不正な装置の接続、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・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・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	**セキュリティ要件** 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。
	考察 必須ではないソフトウェア（プログラム）の使用制限には、たとえば、プログラム実行を承認できる役割の限定、自動実行の禁止、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・無効化することを検討するプロトコルには、Bluetooth、FTP、およびP2Pネットワークが例としてあげられる。
3.4.8	**セキュリティ要件** 「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権限の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権限のあるソフトウェア実行を許可する。
	考察 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。 NIST 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	**セキュリティ要件** ユーザーがインストールするソフトウェアを管理（control）し確認（monitor）する。
	考察 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

	actions regarding software installation through policies. Permitted software installations include, for example, updates and security patches to existing software and downloading applications from organization-approved “app stores.” Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization- developed or provided by some external entity. Policy enforcement methods include procedural methods, automated methods, or both.

	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、たとえば、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「アプリ・ストア」からのアプリケーションのダウンロードなどが含まれる。禁止されるソフトウェアのインストールには、たとえば、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。

TABLE F-5: DISCUSSION ON IDENTIFICATION AND AUTHENTICATION REQUIREMENTS

3.5.1	**SECURITY REQUIREMENT** Identify system users, processes acting on behalf of users, and devices.
	DISCUSSION Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the user names associated with the system accounts assigned to those individuals. Organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity. In addition, this requirement addresses individual identifiers that are not necessarily associated with system accounts. Organizational devices requiring identification may be defined by type, by device, or by a combination of type/device. NIST Special Publication 800-63 provides guidance on digital identities.
3.5.2	**SECURITY REQUIREMENT** Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.
	DISCUSSION Individual authenticators include, for example, passwords, key cards, cryptographic devices, and one-time password devices. Initial authenticator content is the actual content of the authenticator, for example, the initial password. In contrast, the requirements about authenticator content include, for example, the minimum password length. Developers ship system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. NIST Special Publication 800-63 provides guidance on digital identities.
3.5.3	**SECURITY REQUIREMENT** Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
	DISCUSSION Multifactor authentication requires the use of two or more different factors to authenticate. The factors are defined as something you know (e.g., password, personal identification number [PIN]); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). Multifactor solutions that feature physical authenticators include, for example, hardware authenticators providing time-based or challenge-response authenticators and smart cards. In addition to authenticating users at the system level (i.e., at logon), organizations may also employ authentication mechanisms at the application level, when necessary, to provide increased information security. Access to organizational systems is defined as local access or network access. Local access is any access to organizational systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. The use of encrypted virtual private networks for

表 F-5：「識別と認証」要件に関する考察

3.5.1	**セキュリティ要件** システムのユーザー、あるいはユーザーの代理として動作するプロセスまたは装置を識別する。
	考察 一般的な装置識別子には、たとえば、MAC（メディアアクセス管理）、IP（インターネットプロトコル）アドレス、または装置に一意のトークン識別子などがある。個人の識別子の管理は、共有のシステムアカウントには適用されない。個人の識別子は通常、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、個人の一意の識別子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必ずしも関連しない個人の識別子も対象とする。識別子が必要な組織の装置は、種類によって、装置によって、または種類と装置の組み合わせによって定めることができる。 NIST SP 800-63 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	**セキュリティ要件** 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、プロセスまたは装置のアイデンティティを認証（authenticate）（または検証（verify））する。
	考察 個人の認証子（authenticator）には、たとえば、パスワード、キーカード、暗号装置、ワンタイムパスワード装置などが含まれる。認証子の初期の内容は、たとえば、初期パスワードなどの、認証子の実際の内容である。これに対し、認証子の内容についての要件には、たとえば、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、さまざまな認証子の特性に関して組織が定めた設定および制限によって、認証子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、たとえば、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。認証子の管理では、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認証子を発行するとともに、この認証子が必要でなくなった場合に失効させることが含まれる。装置の認証子は、たとえば、証明書やパスワードなどである。 NIST SP 800-63 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。
3.5.3	**セキュリティ要件** 多要素認証を特権アカウントによるローカルアクセス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。
	考察 多要素認証では、認証の際に2種類以上の異なる要素を使用することが求められる。それらの要素は、知識情報（たとえば、パスワードや暗証番号など）、所持情報（たとえば、暗号識別装置やトークンなど）、および生体情報（たとえば、バイオメトリクスなど）と定義される。物理的な認証子を特徴とする多要素認証ソリューションには、たとえば、時間ベースまたはチャレンジ・レスポンス方式の認証子を提供するハードウェア認証子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（またはユーザーの代理とし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（またはユーザーの代理とし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種である。組織が管理するエンドポイントと

	network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks with regard to protecting the confidentiality of information traversing the network. NIST Special Publication 800-63 provides guidance on digital identities.
3.5.4	**SECURITY REQUIREMENT** Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
	DISCUSSION Authentication processes resist replay attacks if it is impractical to successfully authenticate by recording or replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as time synchronous or challenge-response one-time authenticators. NIST Special Publication 800-63 provides guidance on digital identities.
3.5.5	**SECURITY REQUIREMENT** Prevent reuse of identifiers for a defined period.
	DISCUSSION Identifiers are provided for users, processes acting on behalf of users, or devices (3.5.1). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.
3.5.6	**SECURITY REQUIREMENT** Disable identifiers after a defined period of inactivity.
	DISCUSSION Inactive identifiers pose a risk to organizational information because attackers may exploit an inactive identifier to gain undetected access to organizational devices. The owners of the inactive accounts may not notice if unauthorized access to the account has been obtained.
3.5.7	**SECURITY REQUIREMENT** Enforce a minimum password complexity and change of characters when new passwords are created.
	DISCUSSION This requirement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are used as part of multifactor authenticators. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords.
3.5.8	**SECURITY REQUIREMENT** Prohibit password reuse for a specified number of generations.
	DISCUSSION Password lifetime restrictions do not apply to temporary passwords.

	組織が管理しないエンドポイントとの間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、ネットワークを通過する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。 NIST SP 800-63 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	**セキュリティ要件** 特権アカウント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。
	考察 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術には、たとえば、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認証子などの、ナンス（number used once（一度だけ使用される使い捨ての数字））やチャレンジを使用するプロトコルがある。 NIST SP 800-63 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。
3.5.5	**セキュリティ要件** 定められた期間、識別子の再利用を防止する。
	考察 識別子は、ユーザー、ユーザーの代理として動作するプロセス、または装置（3.5.1参照）に付与される。識別子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、または装置の識別子が別の個人、グループ、役割、または装置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	**セキュリティ要件** 定められた非アクティブな期間が過ぎた後、識別子を無効化する。
	考察 個人の識別子は、攻撃者が非アクティブな識別子を不当に利用し、検知されることなく組織の装置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所有者は、アカウントが不正にアクセスされても気が付かない場合がある。
3.5.7	**セキュリティ要件** 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。
	考察 このセキュリティ要件は、個人が、個人の認証子またはグループの認証子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	**セキュリティ要件** 指定された生成回数の間、パスワードの再利用を禁ずる。
	考察 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	**SECURITY REQUIREMENT** Allow temporary password use for system logons with an immediate change to a permanent password.
	DISCUSSION Changing temporary passwords to permanent passwords immediately after system logon ensures that the necessary strength of the authentication mechanism is implemented at the earliest opportunity, reducing the susceptibility to authenticator compromises.
3.5.10	**SECURITY REQUIREMENT** Store and transmit only cryptographically-protected passwords.
	DISCUSSION Cryptographically-protected passwords include, for example, salted one-way cryptographic hashes of passwords. See NIST Cryptographic Standards.
3.5.11	**SECURITY REQUIREMENT** Obscure feedback of authentication information.
	DISCUSSION The feedback from systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems or system components, for example, desktop or notebook computers with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with small displays, this threat may be less significant, and is balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring authenticator feedback includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it.

3.5.9	**セキュリティ要件** 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。
	考察 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、認証子の安全性が損なわれる可能性を低くする。
3.5.10	**セキュリティ要件** 暗号技術で保護されたパスワードのみを格納・伝送する。
	考察 暗号技術で保護されたパスワードは、たとえば、ソルトが付与され、一方向ハッシュにより暗号化されたパスワードなどである。 詳細は、NIST 暗号標準（Cryptographic Standards）を参照すること。
3.5.11	**セキュリティ要件** 認証情報のフィードバックを隠す。
	考察 システムからのフィードバックは、権限のない個人が認証メカニズムのセキュリティを脅かすことを許可してしまう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によっては、たとえば、モニター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、情報を不正に入手すること）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装置などの、その他の種類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、認証子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。認証子のフィードバックを隠す手段には、たとえば、ユーザーが入力装置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ら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。

TABLE F-6: DISCUSSION ON INCIDENT RESPONSE REQUIREMENTS

3.6.1	**SECURITY REQUIREMENT** Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
	DISCUSSION Organizations recognize that incident handling capability is dependent on the capabilities of organizational systems and the mission/business processes being supported by those systems. Organizations consider incident handling as part of the definition, design, and development of mission/business processes and systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user and administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive. As part of user response activities, incident response training is provided by organizations and is linked directly to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the system; system administrators may require additional training on how to handle or remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification/reporting of suspicious activities from external and internal sources. User response activities also includes incident response assistance which may consist of help desk support, assistance groups, and access to forensics services or consumer redress services, when required. NIST Special Publication 800-61 provides guidance on incident handling. NIST Special Publications 800-86 and 800-101 provide guidance on integrating forensic techniques into incident response.
3.6.2	**SECURITY REQUIREMENT** Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.
	DISCUSSION Tracking and documenting system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Reporting incidents addresses specific incident reporting requirements within an organization and the formal incident reporting requirements for the organization. Suspected security incidents may also be reported and include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, Executive Orders, directives, regulations, and policies. NIST Special Publication 800-61 provides guidance on incident handling.

表 F-6：「インシデント対応」要件に関する考察

3.6.1	**セキュリティ要件** 適切な準備、検知、分析、抑制、回復およびユーザー対応を含め、組織のシステムに運用状態のインシデント対応能力を確立する。
	考察 インシデント対応能力は、組織のシステムの能力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さまざまな情報源、たとえば、監査、ネットワーク監視、物理的なアクセス監視、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事象、などから入手することができる。効果的なインシデント対応には、たとえば、ミッション／事業担当者、システムオーナー、承認担当職員、人事部、物理・要員セキュリティ部、法務部、業務要員、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、組織の要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、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、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る。また、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活動の識別・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。 NIST SP 800-86、SP 800-101 は、フォレンジック捜査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。
3.6.2	**セキュリティ要件** インシデントを追跡、文書化し、組織内外の指定された職員および/または機関に報告する。
	考察 システムのセキュリティインシデントの追跡・文書化には、たとえば、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さまざまな情報源、たとえば、インシデント報告、インシデント対応チーム、監査、ネットワーク監視、物理的なアクセス監視、ユーザーレポート、管理者レポートなど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。たとえば、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種類、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。 NIST 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。

3.6.3	**SECURITY REQUIREMENT** Test the organizational incident response capability.
	DISCUSSION Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel and full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response. NIST Special Publication 800-84 provides guidance on testing programs for information technology capabilities.

3.6.3	**セキュリティ要件** 組織のインシデント対応能力をテストする。
	考察 組織は、インシデント対応能力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、インシデント対応能力をテストする。インシデント対応能力のテストには、たとえば、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・完全割り込み型）、および包括的な演習などが含まれる。テストでは、インシデント対応が組織の業務、組織の資産、個人に与える影響（たとえば、ミッション実施能力の低下など）も判定される。 NIST SP 800-84 は、情報技術能力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。

TABLE F-7: DISCUSSION ON MAINTENANCE REQUIREMENTS

3.7.1	**SECURITY REQUIREMENT** Perform maintenance on organizational systems.
	DISCUSSION This requirement addresses the information security aspects of the system maintenance program and applies to all types of maintenance to any system component (including hardware, firmware, applications) conducted by any local or nonlocal entity. System maintenance also includes those components not directly associated with information processing and data or information retention such as scanners, copiers, and printers.
3.7.2	**SECURITY REQUIREMENT** Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
	DISCUSSION This requirement addresses security-related issues with maintenance tools that are not within the organizational system boundaries that process, store, or transmit CUI, but are used specifically for diagnostic and repair actions on those systems. Organizations have flexibility in determining the controls in place for maintenance tools, but can include approving, controlling, and monitoring the use of such tools. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and into organizational systems. Maintenance tools can include hardware, software, and firmware items, for example, hardware and software diagnostic test equipment and hardware and software packet sniffers.
3.7.3	**SECURITY REQUIREMENT** Ensure equipment removed for off-site maintenance is sanitized of any CUI.
	DISCUSSION This control addresses the information security aspects of system maintenance that is performed off-site and applies to all types of maintenance to any system component (including applications) conducted by a local or nonlocal entity (e.g., in-contract, warranty, in- house, software maintenance agreement). NIST Special Publication 800-88 provides guidance on media sanitization.
3.7.4	**SECURITY REQUIREMENT** Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
	DISCUSSION If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with incident handling policies and procedures.
3.7.5	**SECURITY REQUIREMENT** Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
	DISCUSSION Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through an external network. Authentication techniques used in the establishment of these nonlocal maintenance and diagnostic sessions reflect the network access requirements in 3.5.3.

表 F-7：「メンテナンス」要件に関する考察

3.7.1	**セキュリティ要件** 組織のシステムのメンテナンスを行う。
	考察 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）に対するあらゆる種類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	**セキュリティ要件** 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、および要員を管理する。
	考察 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・格納・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・修正するために使用さ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、そうしたツールの使用の承認・管理・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機器、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。
3.7.3	**セキュリティ要件** 現場外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。
	考察 このセキュリティ要件は、現場外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）に対するあらゆる種類のメンテナンス（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 NIST 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。
3.7.4	**セキュリティ要件** 診断および試験プログラムが入っている記憶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検査する。
	考察 メンテナンス診断および試験プログラムが入っている記憶媒体の検査時に、記憶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続きに則ってこのインシデントに対応する。
3.7.5	**セキュリティ要件** 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。
	考察 非ローカルメンテナンスおよび診断とは、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活動を指す。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術は、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	**SECURITY REQUIREMENT** Supervise the maintenance activities of maintenance personnel without required access authorization.
	DISCUSSION This requirement applies to individuals performing hardware or software maintenance on organizational systems, while 3.10.1 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, consultants, and systems integrators, may require privileged access to organizational systems, for example, when required to conduct maintenance activities with little or no notice. Organizations may choose to issue temporary credentials to these individuals based on organizational risk assessments. Temporary credentials may be for one-time use or for very limited time periods.

3.7.6	**セキュリティ要件** 必要なアクセス権限を持たないメンテナンス要員のメンテナンス活動を監督する。
	考察 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要員など）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ーなどの、権限のあるメンテナンス要員として事前に特定されていない個人は、たとえば、通知無しでメンテナンスを行う必要がある場合に、組織のシステムへの特権的なアクセスを必要とすることがある。組織は、リスク対応状況の評価に基づき、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られた期間のみ使用することができる。

TABLE F-8: DISCUSSION ON MEDIA PROTECTION REQUIREMENTS

3.8.1	**SECURITY REQUIREMENT** Protect (i.e. physically control and securely store) system media containing CUI, both paper and digital.
	DISCUSSION System media includes digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Protecting digital media includes, for example, limiting access to design specifications stored on compact disks or flash drives in the media library to the project leader and any individuals on the development team. Physically controlling system media includes, for example, conducting inventories, maintaining accountability for stored media, and ensuring procedures are in place to allow individuals to check out and return media to the media library. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. Access to CUI on system media can be limited by physically controlling such media, which includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. NIST Special Publication 800-111 provides guidance on storage encryption technologies for end user devices.
3.8.2	**SECURITY REQUIREMENT** Limit access to CUI on system media to authorized users.
	DISCUSSION Access can be limited by physically controlling system media and secure storage. Physically controlling system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library.
3.8.3	**SECURITY REQUIREMENT** Sanitize or destroy system media containing CUI before disposal or release for reuse.
	DISCUSSION This requirement applies to all system media, digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include: digital media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal. Organizations determine the appropriate sanitization methods, recognizing that destruction may be necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, destruction, removing CUI from a document, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document. NARA policy and guidance control the sanitization process for controlled unclassified information.

表 F-8：「記憶媒体の保護」要件に関する考察

3.8.1	**セキュリティ要件** 紙とデジタル双方とも、CUIを含むシステムの記憶媒体を保護する（すなわち、セキュアに格納し物理的に管理する）。
	考察 システム記憶媒体には、デジタル記憶媒体と非デジタル記憶媒体とがある。デジタル記憶媒体には、たとえば、ディスケット、磁気テープ、外付け・可搬型HDD、フラッシュドライブ、CD、およびDVDなどが含まれ、非デジタル記憶媒体には、たとえば、紙やマイクロフィルムなどが含まれる。デジタル記憶媒体の保護には、たとえば、メディアライブラリ内のCDやフラッシュドライブに格納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。システム記憶媒体の物理的な管理には、たとえば在庫を確認すること、保存されている記憶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記憶媒体を借り出し・返却できるようにする手続きを定めること、などが含まれる。安全な保管場所には、たとえば、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。 システム記憶媒体上の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、たとえば、在庫を確認すること、個人がメディアライブラリから記憶媒体を借り出し・返却できるようにする手続きを定めること、保存されているすべての記憶媒体の説明責任を維持すること、などによって、制限することができる。 NIST SP 800-111は、エンドユーザー装置のための記憶装置暗号化技術に関するガイダンスを提供する。
3.8.2	**セキュリティ要件** システム記憶媒体上のCUIへのアクセスを、権限を有するユーザーに限定する。
	考察 システム記憶媒体へのアクセスは、物理的な管理および安全な保管場所によって、制限することができる。システム記憶媒体の物理的な管理には、たとえば在庫管理をすること、保存されているすべての記憶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記憶媒体を借り出し・返却できるようにするための手続き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、たとえば、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	**セキュリティ要件** 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。
	考察 この要件は、記憶媒体が可搬型と見なされるかどうかにかかわらず、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、スキャナー、コピー機、プリンター、ノートパソコン、ワークステーション、ネットワークコンポーネント、モバイル装置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（情報除去）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手法は、記憶媒体が再利用または処分される際に、権限の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、他の手段を適用できない場合には廃棄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に公開できる情報を含んでいる記憶媒体に対して、承認されたサニタイズ手法および手続きを自由に採用することができる。また、再利用や処分された場合に組織や個人に負の影響を及ぼさないと思われる情報を含んでいる記憶媒体に対しても、承認されたサニタイズ手法および手続きを自由に採用することができる。非デジタル記憶媒体のサニタイズには、たとえば、記憶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すことが

	See NARA Sanitization Policy and Guidance. NIST Special Publication 800-88 provides guidance on media sanitization.
3.8.4	**SECURITY REQUIREMENT** Mark media with necessary CUI markings and distribution limitations.
	DISCUSSION The term *security marking* refers to the application or use of human-readable security attributes. System media includes digital and non-digital media. Marking of system media reflects applicable federal laws, Executive Orders, directives, policies, and regulations. See NARA Marking Handbook.
3.8.5	**SECURITY REQUIREMENT** Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
	DISCUSSION Controlled areas are areas or spaces for which organizations provide physical or procedural safeguards to meet the requirements established for protecting systems and information. Safeguards to maintain accountability for media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization. Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering.
3.8.6	**SECURITY REQUIREMENT** Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
	DISCUSSION This requirement applies to portable storage devices (e.g., USB memory sticks, digital video disks, compact disks, external or removable hard disk drives). NIST Special Publication 800-111 provides guidance on storage encryption technologies for end user devices. See NIST Cryptographic Standards.
3.8.7	**SECURITY REQUIREMENT** Control the use of removable media on system components.
	DISCUSSION In contrast to requirement 3.8.1, which restricts user access to media, this requirement restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to control the use of system media. Organizations may control the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling or removing the ability to insert, read, or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved

	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規定する。 詳細は、NARA サニタイズポリシーおよびガイダンス を参照すること。NIST 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。
3.8.4	**セキュリティ要件** CUIの標記と配布制限が必要な記憶媒体にはその旨を標記する。
	考察 「*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。システム記憶媒体には、デジタル記憶媒体と非デジタル記憶媒体とがある。システム記憶媒体への標記は、適用される連邦法、大統領令、指令、方針および規定を反映する。 詳細は、NARA マーキングハンドブックを参照すること。
3.8.5	**セキュリティ要件** CUIを含む記憶媒体へのアクセスを管理し、管理区域外での輸送中は、記憶媒体に関する説明責任を維持する。
	考察 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保全措置を提供する区域または場所のことを指す。輸送中の記憶媒体の説明責任を維持する保全措置には、たとえば、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・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、輸送のために記憶媒体を取り外すこと、記憶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、権限のある輸送要員および配達員は、組織外部の個人であってもよい。輸送時の記憶媒体の説明責任を維持するには、たとえば、輸送活動を権限のある要員に制限すること、および、記憶媒体が輸送システムによって輸送される際、輸送活動の明確な記録を追跡・取得することを含み、これにより、紛失・破壊・改ざんが防止され、検知される。
3.8.6	**セキュリティ要件** 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、デジタル記憶媒体上に格納された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。
	考察 このセキュリティ要件は、可搬型記憶装置（たとえば、USBメモリスティック、DVD、CD、外付けまたは可搬型HDDなど）に適用される。NIST SP 800-111は、エンドユーザー装置のための記憶装置暗号化技術に関するガイダンスを提供する。 詳細は、NIST 暗号標準（Cryptographic Standards）を参照すること。
3.8.7	**セキュリティ要件** システムコンポーネント上の可搬型記憶媒体の使用を管理する。
	考察 このセキュリティ要件は、ユーザーによる記憶媒体へのアクセスを制限する3.8.1の要件とは異なり、特定の種類の記憶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、システム記憶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保全措置（たとえば、ポリシー、手続き、行動規則など）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、可搬型記憶装置の挿入・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、可搬型記憶装置の使用を管理する。 組織はまた、可搬型記憶装置の使用を、たとえば、組織が提供する装置、承認されたその他の組織が提供する装置、および私有でない装置、などを含む、承認された装置に限定する。

	organizations, and devices that are not personally owned. Finally, organizations may control the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices.
3.8.8	**SECURITY REQUIREMENT** Prohibit the use of portable storage devices when such devices have no identifiable owner.
	DISCUSSION Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., insertion of malicious code).
3.8.9	**SECURITY REQUIREMENT** Protect the confidentiality of backup CUI at storage locations.
	DISCUSSION Organizations can employ cryptographic mechanisms or alternative physical safeguards to protect the confidentiality of backup information at designated storage locations. Backed-up information containing CUI may include system-level information and user-level information. System-level information includes, for example, system-state information, operating system software and application software, and licenses. User-level information includes information other than system- level information.

	る。最後に、組織は、可搬型記憶装置の使用を装置の種類に基づいて管理することができ、たとえば、書き込み可能な可搬型記憶装置の使用を禁止し、装置への書き込み機能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	**セキュリティ要件** 可搬型記憶装置の所有者を識別できない時には、そうした記憶装置の使用を禁止する。
	考察 可搬型記憶装置の所有者（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、装置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、可搬型記憶装置の使用から生じるリスクを抑えることができる。
3.8.9	**セキュリティ要件** 保管場所にあるバックアップCUIの秘匿性を保護する。
	考察 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保全措置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、たとえば、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。

TABLE F-9: DISCUSSION ON PERSONNEL SECURITY REQUIREMENTS

3.9.1	**SECURITY REQUIREMENT** Screen individuals prior to authorizing access to organizational systems containing CUI.
	DISCUSSION Personnel screening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.
3.9.2	**SECURITY REQUIREMENT** Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.
	DISCUSSION Protecting CUI during and after personnel actions may include, for example, return of system-related property and exit interviews. System-related property includes, for example, hardware authentication tokens, identification cards, system administration technical manuals, keys, and building passes. Exit interviews ensure that individuals who have been terminated understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors. For termination actions, timely execution is essential for individuals terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals that are being terminated prior to the individuals being notified. This requirement applies to reassignments or transfers of individuals when the personnel action is permanent or of such extended durations as to require protection. Organizations define the CUI protections appropriate for the types of reassignments or transfers, whether permanent or extended. Protections that may be required for transfers or reassignments to other positions within organizations include, for example, returning old and issuing new keys, identification cards, and building passes; closing system accounts and establishing new accounts; changing system access authorizations (i.e., privileges); and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

表 F-9：「要員のセキュリティ」要件に関する考察

3.9.1	**セキュリティ要件** CUIを含む組織のシステムへのアクセス権限を与えるに先立って、個人を審査する。
	考察 要員の審査は、適用される連邦法、大統領令、指令、方針、規定、ならびに割り当てられた職務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	**セキュリティ要件** 退職や異動などの人事処理中、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。
	考察 人事処理中および人事処理後におけるCUIの保護には、たとえば、システム関連資産の返却および退職者面談が含まれる。システム関連資産は、たとえば、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、たとえば、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、退職処理を適宜に実施することは極めて重要である。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、そうした人事処理が保護策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、そうした人事処理の種類に適したCUIの保護策を定義する。転勤や、組織内の他の職務への異動の際に必要な保護には、たとえば、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、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、システムへのアクセス権限（つまり、特権）を変更すること、および、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。

TABLE F-10: DISCUSSION ON PHYSICAL PROTECTION REQUIREMENTS

3.10.1	**SECURITY REQUIREMENT** Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
	DISCUSSION This requirement applies to organizational employees, individuals with permanent physical access authorization credentials, and visitors. Authorized individuals have credentials which include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, directives, policies, regulations, standards, procedures, and guidelines. This requirement applies only to areas within facilities that have not been designated as publicly accessible. Limiting physical access to equipment may include, for example, placing equipment in locked rooms or other secured areas and allowing access to authorized individuals only, and placing equipment in locations that can be monitored by organizational personnel. Computing devices, external hard disk drives, networking devices, monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of equipment.
3.10.2	**SECURITY REQUIREMENT** Protect and monitor the physical facility and support infrastructure for organizational systems.
	DISCUSSION Monitoring of physical access includes publicly accessible areas within organizational facilities. This can be accomplished, for example, by the employment of guards; the use of sensor devices; or the use of video surveillance equipment such as cameras. Examples of support infrastructure include system distribution, transmission, and power lines. Security safeguards applied to the support infrastructure prevent accidental damage, disruption, and physical tampering. Such safeguards may also be necessary to help prevent eavesdropping or modification of unencrypted transmissions. Safeguards used to control physical access to support infrastructure include, for example, locked wiring closets; disconnected or locked spare jacks; protection of cabling by conduit or cable trays; and wiretapping sensors.
3.10.3	**SECURITY REQUIREMENT** Escort visitors and monitor visitor activity.
	DISCUSSION Individuals with permanent physical access authorization credentials are not considered visitors. Audit logs can be used to monitor visitor activity.
3.10.4	**SECURITY REQUIREMENT** Maintain audit logs of physical access.
	DISCUSSION Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to systems or system components requiring supplemental access controls, or both. Components of systems (e.g., workstations, notebook computers) may be in areas designated as publicly accessible with organizations safeguarding access to such devices.

表 F-10：「物理的保護」要件に関する考察

3.10.1	**セキュリティ要件** 組織のシステム、機器、およびそれぞれの運用環境への物理的アクセスを、権限のある個人に限定する。
	考察 このセキュリティ要件は、組織の従業員、訪問者、および恒久的な物理的アクセス権限のクレデンシャルを保持する個人に適用される。権限のある個人は、たとえば、バッチ、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、手続きおよび指針に則り、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。 機器への物理的なアクセスの制限には、たとえば、機器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、権限のある個人にのみアクセスを許可することや、機器を組織の要員が監視できる場所に配置することなどが含まれる。機器には、コンピュータデバイス、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、ファックス装置、オーディオ装置などがある。
3.10.2	**セキュリティ要件** 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。
	考察 物理的なアクセスの監視は、組織の施設内の一般にアクセス可能なエリアを対象とする。これは、たとえば、警備員の採用、センサー装置の使用、またはカメラなどの監視機器の使用などによって実施することができる。支援インフラは、システムの配電線、伝送回線、電力線などである。支援インフラに適用されるセキュリティ面の保全措置は、事故による損傷、障害、および物理的な改ざんを防止する。そうした保全措置は、暗号化されていない通信の盗聴や改ざん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保全措置には、たとえば、鍵がかかった配線用ボックス、分離したまたは鍵がかかった予備ジャッキ、導管やケーブルトレイによる配線の保護、および、通信傍受センサーなどがある。
3.10.3	**セキュリティ要件** 訪問者をエスコートし、その活動を確認する。
	考察 恒久的な物理的アクセス権限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。訪問者の活動の確認には、監査ログを使用することができる。
3.10.4	**セキュリティ要件** 物理的アクセスの監査ログを保持する。
	考察 組織は、使用する監査ログの種類を柔軟に選択することができる。監査ログは、手続き的なログ（たとえば、施設にアクセスした個人とそのアクセス時間が書き込まれたログ）、自動的なログ（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、組織がそうした装置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	**SECURITY REQUIREMENT** Control and manage physical access devices.
	DISCUSSION Physical access devices include, for example, keys, locks, combinations, and card readers.
3.10.6	**SECURITY REQUIREMENT** Enforce safeguarding measures for CUI at alternate work sites.
	DISCUSSION Alternate work sites may include, for example, government facilities or private residences of employees. Organizations may define different security requirements for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. NIST Special Publications 800-46 and 800-114 provide guidance on enterprise and user security when teleworking.

3.10.5	**セキュリティ要件** 物理的アクセス装置を管理・監督する。
	考察 物理的アクセス装置には、たとえば、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	**セキュリティ要件** 代替作業サイトにおけるCUIの保全措置を実施する。
	考察 代替作業サイトは、たとえば、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種類ごとに異なるセキュリティ要件を定義する。 NIST 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。

TABLE F-11: DISCUSSION ON RISK ASSESSMENT REQUIREMENTS

3.11.1	**SECURITY REQUIREMENT** Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.
	DISCUSSION Clearly defined system boundaries are a prerequisite for effective risk assessments. Such risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations, organizational assets, and individuals based on the operation and use of organizational systems. Risk assessments also consider risk from external parties (e.g., service providers, contractors operating systems on behalf of the organization, individuals accessing organizational systems, outsourcing entities). Risk assessments, either formal or informal, can be conducted at the organization level, the mission or business process level, or the system level, and at any phase in the system development life cycle. NIST Special Publication 800-30 provides guidance on conducting risk assessments.
3.11.2	**SECURITY REQUIREMENT** Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
	DISCUSSION Organizations determine the required vulnerability scanning for all system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. The vulnerabilities to be scanned are readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This process ensures that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in source code reviews and in a variety of tools (e.g., static analysis tools, web-based application scanners, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms. To facilitate interoperability, organizations consider using products that are Security Content Automated Protocol (SCAP)-validated, scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention, and that use the Open Vulnerability Assessment Language (OVAL) to determine the presence of vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). Security assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). In certain situations, the nature of the vulnerability scanning may be more intrusive or the system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates thorough vulnerability scanning and protects the sensitive nature of such scanning. NIST Special Publication 800-40 provides guidance on vulnerability management.

表 F-11：「リスク評価」要件に関する考察

3.11.1	**セキュリティ要件** 組織のシステム運用、およびCUIに関連する処理、格納、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評価する。
	考察 システムの境界を明確に定義することは、効果的なリスク対応状況の評価の前提条件である。そうしたリスク対応状況の評価は、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、および影響を考慮する。リスク対応状況の評価は、外部関係者（たとえば、サービスプロバイダー、組織の代理としてシステムを運用する請負業者、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対応状況の評価は、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。 NIST SP 800-30 は、リスク対応状況の評価の実施に関するガイダンスを提供する。
3.11.2	**セキュリティ要件** 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。
	考察 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・公表され次第、または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、たとえば、パッチレベルのスキャン、ユーザーまたは装置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、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、脆弱性の存在を判定するOVAL（Open Vulnerability Assessment Language：セキュリティ検査言語）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）認定の製品の使用を検討する。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対応状況の評価は、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、脆弱性の影響を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取扱いに注意すべき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許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秘匿性が保護される。 NIST 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	**SECURITY REQUIREMENT** Remediate vulnerabilities in accordance with risk assessments.
	DISCUSSION Vulnerabilities discovered, for example, via the scanning conducted in response to 3.11.2, are remediated with consideration of the related assessment of risk. The consideration of risk influences the prioritization of remediation efforts and the level of effort to be expended in the remediation for specific vulnerabilities.

3.11.3	**セキュリティ要件** リスク評価に従って、脆弱性を取り除く。
	考察 たとえば、3.11.2の要件を満たすために実施されたスキャンを介して発見された脆弱性は、関連のリスク評価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。

TABLE F-12: DISCUSSION ON SECURITY ASSESSMENT REQUIREMENTS

3.12.1	**SECURITY REQUIREMENT** Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
	DISCUSSION Organizations assess security controls in organizational systems and the environments in which those systems operate as part of the system development life cycle. Security controls are the safeguards or countermeasures organizations implement to satisfy security requirements. By assessing the implemented security controls, organizations determine if the security safeguards or countermeasures are in place and operating as intended. Security control assessments ensure that information security is built into organizational systems; identify weaknesses and deficiencies early in the development process; provide essential information needed to make risk-based decisions; and ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls as documented in system security plans. Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Organizations can choose to use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of systems during the life cycle. NIST Special Publication 800-53A provides guidance on developing security assessment plans and for conducting assessments. NIST Special Publication 800-53 provides guidance on security and privacy controls for systems and organizations.
3.12.2	**SECURITY REQUIREMENT** Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
	DISCUSSION The plan of action is a key document in the information security program. Organizations develop plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format. Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization.
3.12.3	**SECURITY REQUIREMENT** Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
	DISCUSSION Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms *continuous* and *ongoing* imply that organizations assess and analyze security controls and information security- related risks at a frequency sufficient to support risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Providing access

表 F-12：「セキュリティ評価」要件に関する考察

3.12.1	**セキュリティ要件** 組織のシステムのセキュリティ管理策を定期的に評価し、その管理策の適用が有効かどうかを判断する。
	考察 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評価する。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評価することによって、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評価では、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、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、リスクベースの意思決定に必要な重要情報を提供していること、また、脆弱性緩和手続きを順守していること、を確認する。セキュリティ管理策の評価は、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。 セキュリティ評価レポートには対応状況の評価結果が記載される。この評価結果は、組織がレポートの正確性・完全性を判断する上で、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。セキュリティ評価の結果は、実施された評価の種類に応じて該当する個人または役割に提供される。 組織は、セキュリティ評価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評価者によってセキュリティ評価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状態を維持するために、脆弱性のスキャンやシステムの監視などのその他の種類の評価活動を使用することができる。 NIST SP 800-53A は、セキュリティ評価計画書の作成および評価の実施に関するガイダンスを提供する NIST 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。
3.12.2	**セキュリティ要件** 組織のシステムの欠陥を修正し、脆弱性を軽減・排除することを意図した実施計画書を作成し、実施する。
	考察 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・格納・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。
3.12.3	**セキュリティ要件** 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確認（monitor）する。
	考察 継続的な確認プログラムは、脅威や脆弱性に対する継続的な意識、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を高める。「*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、対応状況を評価し分析することを意味する。継続的確認プログラムの結果に対して、組織は適切なリスク対応処置を講じる。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

	to security information on a continuing basis through reports or dashboards gives organizational officials the capability to make more effective and timely risk management decisions. Automation supports more frequent updates to hardware, software, firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Monitoring requirements, including the need for specific monitoring, may also be referenced in other requirements. NIST Special Publication 800-137 provides guidance on continuous monitoring.
3.12.4	**SECURITY REQUIREMENT** Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.
	DISCUSSION System security plans relate security requirements to a set of security controls. System security plans also describe, at a high level, how the security controls meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls. Security plans contain sufficient information to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk if the plan is implemented as intended. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization. NIST Special Publication 800-18 provides guidance on developing security plans.

	職員は、より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。継続的確認のアウトプットが詳細な・重要な・実用的な・迅速な・関連する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をさらに高める。特定の確認の必要性を含め、確認要件は、他の要件で参照される場合がある。 NIST SP800-137 は、継続的確認に関するガイダンスを提供する。
3.12.4	**セキュリティ要件** 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。
	考察 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、管理策の具体的な設計や実装に関する技術的な詳細を示すものではない。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文書、手続き文書、およびその他の文書（たとえば、設計・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・格納・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 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。

TABLE F-13: DISCUSSION ON SYSTEM AND COMMUNICATIONS PROTECTION REQUIREMENTS

3.13.1	**SECURITY REQUIREMENT** Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
	DISCUSSION Communications can be monitored, controlled, and protected at boundary components and by restricting or prohibiting interfaces in organizational systems. Boundary components include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a system security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Restricting or prohibiting interfaces in organizational systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security requirements associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. NIST Special Publication 800-41 provides guidance on firewalls and firewall policy. NIST Special Publication 800-125 provides guidance on security for virtualization technologies.
3.13.2	**SECURITY REQUIREMENT** Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
	DISCUSSION Organizations apply systems security engineering principles to new development systems or systems undergoing major upgrades. For legacy systems, organizations apply systems security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems. The application of systems security engineering concepts and principles helps to develop trustworthy, secure, and resilient systems and system components and reduce the susceptibility of organizations to disruptions, hazards, and threats. Examples of these concepts and principles include developing layered protections; establishing security policies, architecture, and controls as the foundation for design; incorporating security requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; and performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk. Organizations that apply security engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk-management decisions. NIST Special Publication 800-160 provides guidance on systems security engineering.
3.13.3	**SECURITY REQUIREMENT** Separate user functionality from system management functionality.
	DISCUSSION System management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from system management functionality is physical or

表 F-13：「システムと通信の保護」要件に関する考察

3.13.1	**セキュリティ要件** 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・保護する。
	考察 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ーフェースを制限・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、たとえば、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、ルーター、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ー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ーフェースの制限・禁止には、たとえば、管理されたインター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トラフィックを制限することや、内部アドレスになりすま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、第三者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。NIST 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。 NIST SP 800-125 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	**セキュリティ要件** 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。
	考察 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、層構造の保護を開発すること、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、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、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、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容易になり、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。 NIST SP 800-160 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。
3.13.3	**セキュリティ要件** システム管理機能からユーザー機能を分離する。
	考察 システム管理機能には、たとえば、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

	logical. Organizations can implement separation of system management functionality from user functionality by using different computers, different central processing units, different instances of operating systems, or different network addresses; virtualization techniques; or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.
3.13.4	**SECURITY REQUIREMENT** Prevent unauthorized and unintended information transfer via shared system resources.
	DISCUSSION The control of information in shared system resources (e.g., registers, cache memory, main memory, hard disks) is also commonly referred to as object reuse and residual information protection. This requirement prevents information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to any current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. This requirement also applies to encrypted representations of information. This requirement does not address information remanence, which refers to residual representation of data that has been nominally deleted; covert channels (including storage or timing channels) where shared resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.
3.13.5	**SECURITY REQUIREMENT** Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
	DISCUSSION Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones (DMZs). DMZs are typically implemented with boundary control devices and techniques that include, for example, routers, gateways, firewalls, virtualization, or cloud-based technologies. NIST Special Publication 800-41 provides guidance on firewalls and firewall policy. NIST Special Publication 800-125 provides guidance on security for virtualization technologies.
3.13.6	**SECURITY REQUIREMENT** Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
	DISCUSSION This requirement applies to inbound and outbound network communications traffic, both at the system boundary and at identified points within the system. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.
3.13.7	**SECURITY REQUIREMENT** Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).
	DISCUSSION Split tunneling might be desirable by remote users to communicate with local system resources such as printers or file servers. However, split tunneling would allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. This requirement is implemented in remote devices (e.g., notebook computers,

	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、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、または仮想化技術を使用することによって、もしくは必要に応じてこれらの技術やほかの技術を組み合わせて実施することができる。こうした種類の分離には、たとえば、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ーフェースがある。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ーフェースを追加のアクセス制御によって分離することを含む
3.13.4	**セキュリティ要件** 共有システム資源を経由した、不正な情報転送や意図せぬ情報転送を防止する。
	考察 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の代理とし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の代理とし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、表面上は削除されたが残っているデータの残存情報、共有資源が操作され情報の一連の取り扱い手続の制限に違反するようにする隠れチャネル（ストレージチャネル、タイミングチャネルを含む）、または、一人のユーザーまたは単一の役割用のシステムコンポーネントは、このセキュリティ要件の対象ではない。
3.13.5	**セキュリティ要件** 内部ネットワークから物理的・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。
	考察 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、たとえば、ルーター、ゲートウェイ、ファイアウォールなどの境界管理装置や技術、またはクラウドベースの技術を用いて実装される。 NIST 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。NIST SP 800-125 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	**セキュリティ要件** 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）。
	考察 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、必要不可欠な承認された接続のみが許可されるようになる
3.13.7	**セキュリティ要件** リモート装置が、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。
	考察 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、権限の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、組織の情報は盗まれやすくなる。このセキュリティ要件は、構成設定によってリモート装置（たとえば、ノートパソコンやタブレットなど）で実装され、ユーザーが構成する。

	tablets) through configuration settings to disable split tunneling in those devices, and by preventing configuration settings from being readily configurable by users. This requirement is implemented in the system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling.
3.13.8	**SECURITY REQUIREMENT** Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
	DISCUSSION This requirement applies to internal and external networks and any system components that can transmit information including, for example, servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, and facsimile machines. Communication paths outside the physical protection of a controlled boundary are susceptible to interception and modification. Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed safeguards for transmission confidentiality. In such situations, organizations determine what types of confidentiality services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary safeguards and assurances of the effectiveness of the safeguards through appropriate contracting vehicles, organizations implement compensating safeguards or explicitly accept the additional risk. An example of an alternative physical safeguard is a protected distribution system (PDS) where the distribution medium is protected against electronic or physical intercept, thereby ensuring the confidentiality of the information being transmitted. See NIST Cryptographic Standards.
3.13.9	**SECURITY REQUIREMENT** Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
	DISCUSSION This requirement applies to internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address or port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of user inactivity may be established by organizations and include, for example, time periods by type of network access or for specific network accesses.
3.13.10	**SECURITY REQUIREMENT** Establish and manage cryptographic keys for cryptography employed in organizational systems.
	DISCUSSION Cryptographic key management and establishment can be performed using manual procedures or mechanisms supported by manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, and standards, specifying appropriate options, levels, and parameters. NIST Special Publications 800-56 and 800-57 provide guidance on cryptographic key maintenance.

	成設定を自由に変更できなくすることで、リモート装置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、リモート装置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、リモート装置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	**セキュリティ要件** 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の不正な開示を防止するために、暗号メカニズムを実装する。
	考察 このセキュリティ要件は、内部・外部ネットワークならびに、情報を伝送できるあらゆるシステムコンポーネント、たとえば、サーバー、ノートパソコン、デスクトップパソコン、モバイル装置、プリンター、コピー機、スキャナー、ファックス装置などに適用される。管理された境界の物理的保護下にない通信経路は、傍受や改ざんを受けやすい。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保全措置の実装に関して、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。 詳細は、NIST 暗号標準（Cryptographic Standards）を参照すること。
3.13.9	**セキュリティ要件** 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。
	考察 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、たとえば、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、たとえば、ネットワークアクセスの種類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	**セキュリティ要件** 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。
	考察 暗号鍵の管理および設定は、手動の手続きまたは手動の手続き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、指令、規定、方針および規格に則って暗号鍵管理に関する要件を定義し、適切なオプション、レベル、およびパラメータを指定する。 NIST SP 800-56 、SP 800-57 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	**SECURITY REQUIREMENT** Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
	DISCUSSION Cryptography can be employed to support many security solutions including, for example, the protection of controlled unclassified information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on other security requirements, organizations define each type of cryptographic use and the type of cryptography required (e.g., FIPS-validated cryptography). See NIST Cryptographic Standards; NIST Cryptographic Module Validation Program; NIST Cryptographic Algorithm Validation Program.
3.13.12	**SECURITY REQUIREMENT** Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
	DISCUSSION Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Indication of use includes, for example, signals to users when collaborative computing devices are activated. Dedicated video conferencing systems, which rely on one of the participants calling or connecting to the other party to activate the video conference, are excluded.
3.13.13	**SECURITY REQUIREMENT** Control and monitor the use of mobile code.
	DISCUSSION Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Decisions regarding the use of mobile code in organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Usage restrictions and implementation guidance apply to the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations, notebook computers, and devices (e.g., smart phones). Mobile code policy and procedures address controlling or preventing the development, acquisition, or introduction of unacceptable mobile code in systems, including, for example, requiring mobile code to be digitally signed by a trusted source. NIST Special Publication 800-28 provides guidance on mobile code.
3.13.14	**SECURITY REQUIREMENT** Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.
	DISCUSSION VoIP has different requirements, features, functionality, availability, and service limitations when compared with Plain Old Telephone Service (POTS) (i.e., the standard telephone service that most homes use). In contrast, other telephone services are based on high-speed, digital communications lines, such as Integrated Services Digital Network (ISDN) and Fiber Distributed Data Interface (FDDI). The main distinctions between POTS and non-POTS services are speed and bandwidth. To address the threats associated with VoIP, usage restrictions and implementation guidelines are based on the potential for the VoIP technology to cause damage to the system if it is used maliciously. Threats to VoIP are similar to those inherent with any Internet-based application.

3.13.11	**セキュリティ要件** CUIの秘匿性保護には、FIPS認証された暗号技術を採用する。
	考察 暗号技術は、CUIの保護、デジタル署名の提供、ならびに、権限のある個人が情報の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解決策を支援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することができる。一般的に適用される暗号標準には、FIPS認証の暗号技術およびNSA承認の暗号技術がある。この管理策は、組織に対して暗号技術の使用を義務付けるものではないが、その他のセキュリティ要件により暗号技術が求められる場合、組織は、暗号の用途と必要な暗号技術（たとえば、FIPS認証の暗号技術）の種類をそれぞれ定義する。 詳細は、NIST 暗号標準（Cryptographic Standards）、NIST 暗号モジュール認証制度（Cryptographic Module Validation Program）、NIST 暗号アルゴリズム認証制度（Cryptographic Algorithm Validation Program）を参照すること。
3.13.12	**セキュリティ要件** 協働コンピューティング装置のリモートからの活性化を禁止し、その装置に存在するユーザーに対して使用中の装置を表示する。
	考察 協働コンピューティング装置は、たとえば、ネットワークで結ばれたホワイトボード、カメラ、マイクロフォンなどである。装置の使用を表示するには、たとえば、協働コンピューティング装置が作動した時に、信号によってユーザーに通知する。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	**セキュリティ要件** モバイルコードの使用を管理・監視する。
	考察 モバイルコード技術には、たとえば、Java、JavaScript、ActiveX、Postscript、PDF、Shockwave movies、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、および装置（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続きは、たとえば、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。 NIST 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	**セキュリティ要件** 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・監視する。
	考察 VoIPには、基本電話サービス（POTS, Plain Old Telephone Service）（すなわち、家庭で通常使用される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、およびサービスの制限事項がある。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。

	NIST Special Publication 800-58 provides guidance on Voice Over IP Systems.
3.13.15	**SECURITY REQUIREMENT** Protect the authenticity of communications sessions.
	DISCUSSION Authenticity protection includes, for example, protecting against man-in-the-middle attacks, session hijacking, and the insertion of false information into communications sessions. This requirement addresses communications protection at the session versus packet level (e.g., sessions in service- oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. NIST Special Publications 800-52, 800-77, 800-95, and 800-113 provide guidance on secure communications sessions.
3.13.16	**SECURITY REQUIREMENT** Protect the confidentiality of CUI at rest.
	DISCUSSION Information at rest refers to the state of information when it is not in process or in transit and is located on storage devices as specific components of systems. The focus of protection at rest is not on the type of storage device or the frequency of access but rather the state of the information. Organizations can use different mechanisms to achieve confidentiality protections, including the use of cryptographic mechanisms and file share scanning. Organizations may also employ other safeguards including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved or continuous monitoring to identify malicious code at rest. See NIST Cryptographic Standards.

	NIST SP800-58 は、VoIPシステムに関するガイダンスを提供する。
3.13.15	**セキュリティ要件** 通信セションの正当性（Authenticity）を保護する。
	考察 正当性の保護には、たとえば、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。 NIST SP 800-52、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	**セキュリティ要件** 通信停止中のCUIの秘匿性を保護する。
	考察 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記憶装置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、記憶装置の種類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、たとえば、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、その他の保全措置を採用してもよい。 詳細は、NIST 暗号標準（Cryptographic Standards）を参照すること。

TABLE F-14: DISCUSSION ON SYSTEM AND INFORMATION INTEGRITY REQUIREMENTS

3.14.1	**SECURITY REQUIREMENT** Identify, report, and correct system flaws in a timely manner.
	DISCUSSION Organizations identify systems that are affected by announced software and firmware flaws including potential vulnerabilities resulting from those flaws, and report this information to designated personnel with information security responsibilities. Security-relevant updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations can take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational systems. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types of remediation. NIST Special Publication 800-40 provides guidance on patch management technologies.
3.14.2	**SECURITY REQUIREMENT** Provide protection from malicious code at designated locations within organizational systems.
	DISCUSSION Designated locations include system entry and exit points which may include, for example, firewalls, remote-access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. NIST Special Publication 800-83 provides guidance on malware incident prevention.
3.14.3	**SECURITY REQUIREMENT** Monitor system security alerts and advisories and take action in response.
	DISCUSSION There are many publicly available sources of system security alerts and advisories. The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government and in nonfederal organizations. Software vendors, subscription services, and relevant industry information sharing and analysis centers (ISACs) may also provide security alerts and advisories. Examples of response actions

表 F-14：「システムと情報の完全性」要件に関する考察

3.14.1	**セキュリティ要件** システムの欠陥をタイムリーに特定し、報告し、修正する。
	考察 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アップデートには、たとえば、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、セキュリティ対応状況の評価、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）またはCVE（Common Vulnerabilities and Exposure：共通脆弱性識別子）の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アップデートを行う時期を、たとえば、アップデートの重要性（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。欠陥解決の種類によっては、他の解決の種類よりも多く試験を要することがある。NIST 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	**セキュリティ要件** 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。
	考察 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、たとえば、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、モバイル装置などが含まれる。悪意のあるコードには、たとえば、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術を使用し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、可搬型記憶装置を含む、様々な方法でシステムに挿入され得る。悪意のあるコードは、システムの脆弱性を不正に利用して挿入される。 悪意のあるコードからの保護メカニズムには、たとえば、アンチウイルス署名の定義や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抑えるまたは削除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、不正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、組織の任務（mission）／事業機能に影響を及ぼしかねない、たとえば、論理爆弾、バックドア、およびその他の種類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、代わりにその他の保全措置、たとえば、セキュアコーディング、構成管理・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。 NIST 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	**セキュリティ要件** システムのセキュリティ警報および通報を監視し、対応措置を講ずる。
	考察 システムのセキュリティ警報および通報は、一般に利用可能なソースが多数ある。US-CERT（United States Computer Emergency Readiness Team：米国コンピュータ緊急対策チーム）は、連邦政府機関および非連邦政府機関全体で状況認識を維持するために、セキュリティ警告および通報を作成する。ソフトウェアベンダー、加入サービス、および業界の

	include notifying relevant external organizations, for example, external mission/business partners, supply chain partners, external service providers, and peer or supporting organizations.
3.14.4	**SECURITY REQUIREMENT** Update malicious code protection mechanisms when new releases are available.
	DISCUSSION Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended.
3.14.5	**SECURITY REQUIREMENT** Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.
	DISCUSSION Periodic scans of organizational systems and real-time scans of files from external sources can detect malicious code. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. Many technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended.
3.14.6	**SECURITY REQUIREMENT** Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
	DISCUSSION System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system. Organizations can monitor systems, for example, by observing audit record activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. System monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices

	ISAC（情報共有分析センター）もまた、セキュリティ警告および通報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ー、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。
3.14.4	**セキュリティ要件** 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。
	考察 悪意のあるコードからの保護メカニズムには、たとえば、アンチウイルス署名の定義や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抑えるまたは削除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、不正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、組織の任務（mission）／事業機能に影響を及ぼしかねない、たとえば、論理爆弾、バックドア、およびその他の種類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、代わりにその他の保全措置、たとえば、セキュアコーディング、構成管理・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。
3.14.5	**セキュリティ要件** 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。
	考察 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術を使用し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、および可搬型記憶装置を含む、様々な方法でシステムに挿入され得る。悪意のあるコードは、システムの脆弱性を不正に利用して挿入される。 悪意のあるコードからの保護メカニズムには、たとえば、アンチウイルス署名の定義や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抑えるまたは削除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、不正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、組織の任務（mission）／事業機能に影響を及ぼしかねない、たとえば、論理爆弾、バックドア、およびその他の種類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、代わりにその他の保全措置、たとえば、セキュアコーディング、構成管理・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。
3.14.6	**セキュリティ要件** 攻撃および潜在的攻撃の徴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。
	考察 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事象（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事象の観測を含む。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。監視目的によって、観測される事象が決定される。システム監視機能は、さまざまなツールや技術

	include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices being employed at managed system interfaces. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of systems to support such objectives. System monitoring is an integral part of continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Unusual or unauthorized activities or conditions related to inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other requirements. NIST Special Publication 800-94 provides guidance on intrusion detection and prevention systems.
3.14.7	**SECURITY REQUIREMENT** Identify unauthorized use of organizational systems.
	DISCUSSION System monitoring can detect unauthorized use of organizational systems. System monitoring includes external and internal monitoring. System monitoring is an integral part of continuous monitoring and incident response programs; it is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Output from system monitoring serves as input to continuous monitoring and incident response programs. Unusual or unauthorized activities or conditions related to inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other requirements. NIST Special Publication 800-94 provides guidance on intrusion detection and prevention systems.

	（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。監視装置の戦略的な配置場所には、たとえば選択された境界や、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、監査装置は管理されたシステムインター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、組織の監視目的とその目的を支援するシステムの能力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）を介して通信する装置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）を介して通信する装置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不正な活動や状態には、たとえば、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、情報の不正なエクスポート、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形跡は、安全性が損なわ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。特定の種類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。 NIST 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	**セキュリティ要件** 組織のシステムの不正使用を特定（identify）する。
	考察 システム監視は、組織のシステムの不正使用を検知することができる。システム監視には、外部監視と内部監視とがある。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り、さまざまなツールや技術（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。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。 出入りする通信トラフィックに関連する異常なまたは不正な活動や状態には、たとえば、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、情報の不正なエクスポート、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形跡は、安全性が損なわ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。特定の種類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。 NIST 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。