NIST 特別刊行物 800

NIST SP 800-171r3

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

ビクトリア・ピリッテリ

本書は https://doi.org/10.6028/NIST.SP.800-171r3
から自由に入手できる。

NIST 特別刊行物 800

NIST SP 800-171r3

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

ビクトリア・ピリッテリ

コンピュータ・セキュリティ・ディビジョン

情報技術研究所

本書は以下から無料で入手できる：

https://doi.org/10.6028/NIST.SP.800-171r3

2024 年 5 月

米国商務省 ジーナ・*M*・ライモンド長官

国立標準技術研究所

ローリー・*E*・ロカシオ、*NIST* 理事兼標準技術担当商務次官

本論文では、実験手順を適切に特定するために、商用、非商用を問わず、特定の機器、装置、ソフトウェア、または材料を識別している。このような識別は、NIST によるいかなる製品またはサービスの推奨または保証を意味するものではなく、また識別された材料または装置が必ずしもその目的に対して利用可能な最良のものであることを意味するものでもない。

本書には、NIST がその法定責任に従って現在開発中の他の出版物を参照している場合がある。概念や方法論を含む本書の情報は、そのような関連出版物の完成前であっても、連邦機関によって使用される可能性がある。従って、各出版物が完成するまでは、現行の要求事項、ガイドライン、手順が存在する場合は、それらが引き続き有効である。計画と移行を目的として、連邦機関は NIST によるこれらの新出版物の開発を注意深く見守ることが望ましい。

各組織は、パブリックコメント期間中にすべての出版物のドラフトを検討し、NIST にフィードバックを提供することが推奨される。上記以外の多くの NIST サイバーセキュリティ出版物は、https://csrc.nist.gov/publications で入手できる。

認可

本書は、2014 年連邦情報セキュリティ近代化法（FISMA）（44 U.S.C. § 3551 et seq.、公法（P.L.）113-283）に基づく NIST の法的責任に基づき、NIST が作成したものである。NIST は、連邦情報システムの最低要件を含む情報セキュリティ標準およびガイドラインを策定する責任を負うが、そのような標準およびガイドラインは、そのようなシステムに対する政策権限を行使する適切な連邦政府当局者の明示的な認可がない限り、国家安全保障システムには適用されない。本ガイドラインは、行政管理予算局（OMB）サーキュラーA-130 の要件と一致している。

本書のいかなる内容も、法的認可に基づき商務長官が連邦政府機関に義務付け、拘束力を持たせた標準やガイドラインと矛盾するものであってはならない。また、本ガイドラインは、商務長官、OMB 長官、その他の連邦政府当局者の既存の権限を変更したり、これに取って代わるものと解釈されるべきではない。本書は、非政府組織が任意に使用することができ、米国における著作権の対象ではない。ただし、NIST はその帰属を認める。

NIST テクニカルシリーズ方針

著作権、使用およびライセンスに関する声明

NIST 技術シリーズ出版識別子の構文

出版の履歴

2024-04-23、NIST 編集審査委員会によって承認された。

NIST 特別刊行物 800-171r2 (2020 年 2 月。2021 年 1 月 28 日現在の更新を含む) https://doi.org/10.6028/NIST.SP.800-171r2 を更新する。

この NIST テクニカルシリーズ出版物の引用方法：

Ross R, Pillitteri V (2024) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) NIST SP 800-171r3. https://doi.org/10.6028/NIST.SP.800-171r3.

認可 ORCID iDs

ロン・ロス 0000-0002-1099-9757

ビクトリア・ピリテリ：0000-0002-7446-7506

コメントを投稿する

800-171comments@list.nist.gov

国立標準技術研究所

担当：情報技術研究所コンピュータセキュリティ課

100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

追加情報

関連コンテンツ、更新の可能性、文書の履歴など、本書に関する追加情報は https://csrc.nist.gov/pubs/sp/800/171/r3/final。

すべてのコメントは、情報公開法（FOIA）に基づき公開される。

要旨

管理対象非機密情報（CUI）の保護は、連邦機関にとって最も重要であり、連邦政府がその重要な任務と機能を成功裏に遂行する能力に直接影響を与える可能性がある。本書は、連邦機関に対し、情報が連邦機関以外のシステムおよび組織に常駐している場合に、CUI の機密性を保護するための推奨セキュリティ要件を提供する。要件は、CUI を処理、保管、または送信する連邦政府以外の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の保護を提供するコンポーネントに適用される。本セキュリティ要件は、連邦機関と連邦機関以外の組織との間で締結される契約書ま たはその他の合意において、連邦機関が使用することを意図している。本書は、その関連刊行物である NIST 特別刊行物 800-171A と併せて使用することができ、セキュリティ要件を評価するための包括的な手順を提供する。

キーワード

管理対象非機密情報、大統領令 13556、FIPS 出版物 199、FIPS 出版物 200、FISMA、NIST 特別刊行物 800-53、連邦政府以外の組織、連邦政府以外のシステム、組織 定義パラメータ、セキュリティ評価、セキュリティ管理、セキュリティ要件。

コンピュータ・システム技術に関するレポート

国立標準技術研究所(NIST)の情報技術研究所(ITL)は、国家の測定および標準機構に技術的リーダーシップを提供することにより、米国経済と公共の福祉を促進する。ITL は、情報技術の開発と生産的使用を促進するために、試験、試験方法、参照データ、概念実証実装、技術分析を開発している。ITL の責任には、連邦情報システムにおける国家安全保障関連情報以外のコスト効率の良いセキュリティとプライバシーのための管理、管理、技術、物理的標準とガイドラインの開発が含まれる。Special Publication 800 シリーズは、情報システム・セキュリティに関する ITL の研究、ガイドライン、アウトリーチ活動、および産業界、政府、学術団体との協力活動について報告している。

想定読者

本誌は、官民を問わず、以下のような多様な個人や組織にサービスを提供している：

- CUI の管理と保護に責任を負う連邦政府機関
- CUI を保護する責任を負う連邦政府以外の組織
- システム開発ライフサイクルに責任を持つ個人（プログラムマネジャー、ミッション／ビジネスオーナー、情報所有者／管理者、システム設計者／開発者、システム／セキュリティエンジニア、システムインテグレーターなど）
- 取得または調達に責任を持つ個人（契約担当者など）

- システム、セキュリティ、またはリスクマネジメントや監督責任を有する個人（認可担当者、最高情報責任者、最高情報セキュリティ責任者、システム所有者、情報セキュリティ管理者など）
- セキュリティアセスメント及びモ ニタリングを担当する個人 （監査員、システム評価者、査定者、 アナリスト、独立検証者、検証者な ど）。

上記の役割と責任は、2 つの観点から見ることができる：

- 連邦の視点：事業体：契約書またはその他の種類の協定において、セキュリ ティ要件を設定し、伝達する。
- 連邦政府以外の視点：契約や協定に定められたセキュリティ要件に対応し、これを遵守する事業体

特許開示通知

注意：ITL は、本出版物のガイダンスまたは要件に準拠するために使用が必要となる特許請求の範囲の保有者に対し、当該特許請求の範囲を ITL に開示するよう要請している。ただし、特許権者は ITL の特許募集に応じる義務はなく、ITL は、本出版物に該当する特許があるとしても、それを特定するための特許調査を行っていない。

本書の発行日および、本書のガイダンスまたは要件に準拠するために使用が必要とされる可能性のある特許請求の範囲の識別を求めた後の時点で、ITL にそのような特許請求の範囲は識別されていない。

ITL は、本出版物の使用において特許侵害を回避するためのライセンスが不要であることを表明するものではなく、また示唆するものでもない。

目次

目次 7

謝辞 10

1. 序文 11

1.1. 目的と適用範囲 12

1.2. 本書の構成 13

2. ファンダメンタルズ 14

2.1. セキュリティ要件の前提 14

2.2. セキュリティ要件開発手法 14

3. セキュリティ要件 18

3.1. アクセス制御 18

3.2. 意識向上およびトレーニング 32

3.3. 監査および説明責任 35

3.4. 構成管理 40

3.5. 識別および認証 47

3.6. インシデント対応 53

3.7. 保守 56

3.8. 媒体保護 59

3.9. 職員のセキュリティ 63

3.10. 物理的保護 64

3.11. リスクアセスメント 68

3.12. セキュリティ評価と監視 70

3.13. システムおよび通信の保護 72

3.14. システムおよび情報の完全性 78

3.15. 計画 83

3.16. システムおよびサービスの取得 85

3.17. サプライチェーンのリスクマネジメント 87

参考文献 91

附属書 A. 頭字語 100

附属書 B. 用語集 102

附属書 C. テーラリング基準 109

附属書 D. 組織定義のパラメータ 124

附属書 E. 変更履歴 128

表の一覧

表 1. セキュリティ要件ファミリー 15

表 2. セキュリティ・コントロールの調整基準 109

表 3. アクセス制御（AC） 109

表 4. 意識向上およびトレーニング（AT） 111

表 5. 監査および説明責任（AU） 111

表 6. 評価、認可、モニタリング（CA） 112

表 7. 構成管理（CM） 112

表 8. コンティンジェンシー計画（CP） 113

表 9. 識別および認証（IA） 114

表 10. インシデント対応（IR） 115

表 11. 保守 (MA) 115

表 12. 媒体保護(MP) 116

表 13. 物理的および環境的保護（PE） 116

表 14. 計画（PL） 117

表 15. プログラム・マネジメント（PM） 117

表 16. 職員のセキュリティ（PS）.....119

表 17. PII の処理と透明性（PT）.....119

表 18. リスクアセスメント（RA）.....120

表 19. システムおよびサービスの取得（SA）.....120

表 20. システムおよび通信の保護 (SC).....121

表 21. システムおよび情報の完全性（SI）.....122

表 22. サプライチェーンのリスクマネジメント(SR).....123

表 23.組織定義のパラメータ.....124

表 24.変更履歴.....129

謝辞

本書の全体的な質、徹底性、有用性を向上させるために、官民の個人および組織から建設的なコメントをいただき、多大なご協力をいただいたことに感謝申し上げる。また、認可を受けた NIST の技術編集・制作スタッフ（Jim Foti、Jeff Brewer、Eduardo Takamura、Isabel Van Wyk、Cristina Ritfeld、Derek Sappington、Carolyn Schmidt）にも感謝したい。最後に、プロトタイプの CUI オーバーレイで使用されたコンテンツの最初の調査と開発をしてくれたケリー・デンプシーに感謝の意を表したい。

歴史的貢献

また、本書に歴史的な貢献をしてくれた以下の組織と個人にも謝意を表したい：

- 組織国立公文書記録管理局、国防総省
- 個人キャロル・ベイルズ、マシュー・バレット、ジョン・ボイエンズ、デヴィン・ケイシー、クリスチャン・エンロー、ゲイリー・ギサニー、ペギー・ヒメス、ロバート・グレン、エリザベス・レノン、ヴィッキー・ミケッティ、ドリアン・パパス、カレン・クイッグ、マーク・リドル、マシュー・ショル、メアリー・トーマス、ムルギア・スッパヤ、パトリシア・トス、パトリック・ヴィスクーソ

1. 序文

大統領令（EO）13556[1]は、管理対象非機密情報（CUI）を行政府が取り扱う方法を標準化するための政府全体のプログラムを設立した。[1]EO 13556 は、CUI プログラムが政府全体の慣行の公開性、透明性、および統一性を重視し、 プログラムの実施が行政管理予算局（OMB）の方針および国立標準技術研究所（NIST）の標準およびガイドラインと整合する方法で行われることを要求した。CUI プログラムの執行代理人として、国立公文書記録管理局（NARA）は、CUI の取り扱いに関する情報、ガイダンス、ポリシー、および要件を提供している[4]。これには、承認された CUI のカテゴリーおよび説明、保護および普及管理の基礎、および CUI の使用手順が含まれる。[2]CUI 連邦規則[5]は、CUI の指定、保護、マーキング、普及、管理解除、および処分に関する連邦政府機関へのガイダンスを提供し、自己点検および監督要件を定め、プログラムのその他の側面を定義している。

CUI 規則は、連邦情報システム（[3] ）を使用して CUI を処理、保管、または伝送する連邦機関に対し、NIST 標準およびガイドラインに準拠することを義務付けている。CUI を保護する連邦機関の責任は、そのような情報が連邦機関以外の組織と共有される場合でも変わらない。[4]したがって、連邦機関以外のシステムを使用して連邦機関以外の組織が CUI を処理、保管、または伝送する場合も、同様の保護レベルが必要である。[5]一貫した保護レベルを維持するため、連邦機関以外のシステムおよび組織における CUI を保護するためのセキュリティ要件は、連邦情報処理標準（FIPS 199）公開[6]および FIPS 200[7]に準拠しなければならない。要件は、NIST 特別刊行物（SP）800-53 [8]の管理策に由来する。

---

[1] CUI とは、法律、規則、または政府全体の方針により、保護管理または拡散管理が要求されるあらゆる情報であり、EO 13526 [2]、その前任者または後継者の命令、または改正後の原子力法 [3]に基づき機密扱いとされる情報を除く。 [2]

[2] CUI の使用手順には、情報のマーキング、保護、輸送、配布、再使用、および廃棄が含まれる。

[3] 連邦情報システムとは、行政機関、行政機関の請負業者、または行政機関に代わって他の組織が使用または運用するシステムである。本書では、システムという用語は、CUI の処理、保管、または伝送に関与する人、プロセス、および技術の代表者として使用される。システムには、運用技術（OT）、情報技術（IT）、モノのインターネット（IoT）デバイス、産業用 IoT（IIoT）デバイス、特殊システム、サイバーフィジカルシステム、組込みシステム、およびセンサーが含まれる。

[4] 非連邦組織とは、非連邦システムを所有、運営、維持する事業体である。

[5] 非連邦システムとは、連邦情報システムの基準を満たさないシステムのことである。

1.1. 目的と適用範囲

本書は、CUI[6] の機密性を保護するための推奨セキュリ ティ要件[7] を連邦政府機関に提供するものである。このような情報が連邦政府以外のシス テムおよび組織に常駐しており、CUI レジストリ[4]に記載されている CUI カテゴリーについて、認可法、規 制、または政府全体の方針によって規定された特定の保護要件がない場合、この要件は適用されない。この要件は、連邦機関に代わって情報を収集または管理している、あるいは連邦機関に代わってシステムを使用または運用している連邦機関以外の組織には適用されない。[8]

本書のセキュリティ要件は、CUI を処理、保管、伝送する、またはそのようなコンポーネントの 保護を提供する連邦政府以外のシステムのコンポーネントにのみ適用される。[9]本要件は、連邦機関と非連邦機関との間で締結される契約書またはその他の合意において、連邦機関が使用することを意図している。

要件を適切にスコープすることは、保護関連の投資決定を行い、連邦政府以外の組織のセ キュリティ・リスクをマネジメントする上で重要な要素である。連邦政府以外の組織が、CUI の処理、保存、または送信のためにシステム・コンポーネントを指定する場合、それらの組織は、システム・コンポーネントを別のセキュリティ・ドメインに隔離することによって、セキュリティ要件の範囲を制限することができる。分離は、アーキテクチャおよび設計の概念（例えば、ファイアウォールまたは他の境界保護装置を備えたサブネットワークの実装、情報フロー制御メカニズムの使用）を適用することによって達成する ことができる。セキュリティ・ドメインは、物理的分離、論理的分離、またはその両方の組み合わせを採用することができる。このアプローチにより、CUI に対して適切なセキュリティを提供することができ、組織のミッション、運用、および資産を保護するために必要な範囲を超えて、組織のセキュリティ態勢を増大させることを回避することができる。

---

[6] EO 13526 [2]および 32 CFR 2002 [5]に従い、CUI 保護の範囲は主に機密性に重点が置かれている。しかし、機密性と完全性のセキュリティ目標は、基礎となるセキュリティ・メカニ ズムの多くが両方の目標をサポートするため、密接に関連している。したがって、本書のセキュリティ要件は、不正な開示および改ざんからの CUI の保護に対応する。

[7]セキュリティ要件という 用語は、システムまたは組織の保護ニーズを指す。セキュリティ要件は、法律、大統領令、指令、規制、方針、標準、ミッション及びビジネスニーズ、またはリスクアセスメントから導き出される。

[8] 連邦機関に代わって情報を収集または維持する、あるいは連邦機関に代わってシステムを使用または運用する連邦機関以外の組織は、FISMA [9]の要件を遵守しなければならない。

[9] システム・コンポーネントには、ワークステーション、サーバー、ノートブック・コンピューター、スマートフォン、タブレット、入出カデバイス、ネットワーク・コンポーネント、オペレーティング・システム、仮想マシン、データベース管理システム、アプリケーションなどが含まれる。

1.2. 本書の構成

本特集の残りの部分は以下のように構成されている：

- セクション 2 では、CUI の機密性を保護するためのセキュリティ要件を策定するために使用した前提条件と方法論、要件の形式、および要件を得るために NIST ガイドラインに適用したテーラリング基準について説明する。
- セクション 3 は、連邦政府以外のシステムおよび組織における CUI の機密性を保護するためのセキュリティ要件を列挙している。

以下のセクションでは、CUI の保護をサポートするための追加情報を提供する：

- 参考文献
- 附属書 A：頭字語
- 附属書 B：用語集
- 附属書 C：テーラリング基準
- 附属書 D：組織定義のパラメータ
- 附属書 E：変更履歴

2. ファンダメンタルズ

本セクションでは、連邦政府以外のシステムおよび組織における CUI の機密性を保護するための要件を策定するために使用された前提条件および方法論について説明する。また、SP 800-53 [8]の統制に適用されるテーラリング[10] 基準も含まれる。

2.1. セキュリティ要件の前提

本書のセキュリティ要件は、以下の仮定に基づいている：

- CUI として指定された連邦情報は、そのような情報が連邦または連邦以外のシステムまたは組織に存在するかにかかわらず、同じ価値を持つ。
- CUI の保護に関する法定および規制要件は、連邦および非連邦のシステムおよび組織で一貫している。
- CUI を保護するために実施される保護措置は、連邦政府と連邦政府以外のシステムおよび組織で一貫している。
- CUI の機密性への影響値は中程度以上である。[11]
- 連邦政府以外の組織は、さまざまなセキュリティ・ソリューションの可能性を直接導入することも、外部のサービス・プロバイダを利用してセキュリティ要件を満たすこともできる。

2.2. セキュリティ要件開発手法

SP 800-53B [12]の中程度のベースラインにおける SP 800-53 の管理から始まり、管理は、選択された管理または管理の一部を排除するように調整される：

- 主に連邦政府の責任である、
- CUI の機密保護とは直接関係ない、
- 他の関連する統制によって十分に対処されている、[12] または

---

[10]テーラリングとは、特定の組織目標や目的を達成するために、コントロール・ベースラインを修正するプロセスのことである[13]。

[11] 32 CFR 2002 [5]に従い、CUI は、FIPS 199 [6]の中程度の機密性影響値以上に分類される。ただし、CUI の管理を確立する連邦法、規則、または政府全体の方針が、中程度の管理ベースラインのものとは異なる管理を指定する場合は、適用法、規則、または政府全体の方針に従う。

[12] 「他の関連する管理により適切に対処される」とは、当該管理により提供される保護能力が、同じ管理ファミリーまたは異なる管理ファミリーの他の管理により提供されることを意味する。この調整オプションを使用することにより、連邦政府以外のシステムおよび組織における CUI の保護に影響を与えることなく、要件の潜在的な冗長性を排除することができる。

- 該当しない。

SP 800-171 セキュリティ要件は、CUI の機密性を保護するために必要な管理の代表者である。セキュリティ要件は、表 1 に示すように、17 のファミリーに分類されている。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トピックに関連する要件が含まれている。 例えば、PII 処理及び透明性（PT）ファミリーは、個人を特定できる情報（PII）が CUI のカテゴリであるため、機密性保護に関する追加要件が規定されていないため、含まれていない。プログラム管理(PM)ファミリーは、管理ベースラインと関連付けられていないため、含まれていない。最後に、コンティンジェンシー計画（CP）ファミリーは、可用性を扱うため含まれない。[13]

表 1. セキュリティ要件ファミリー

アクセス管理	保守	セキュリティ評価と監視
意識向上およびトレーニング	媒体保護	システムと通信の保護
監査および説明責任	職員のセキュリティ	システムおよび情報の完全性
構成管理	物理的保護	計画
識別および認証	リスクアセスメント	システムおよびサービスの取得
インシデント対応		サプライチェーンのリスクマネジメント

組織定義パラメータ（ODP）は、特定のセキュリティ要件に含まれている。ODP は、割り当て操作と選択操作を使用して柔軟性を提供し、連邦機関および非連邦 機関が要件内の指定パラメータの値を指定できるようにする。[14]割り当て操作と選択操作は、特定の保護ニーズに基づいてセキュリティ要件をカスタマイズする機能を提供する。ODP の値の決定は、法律、大統領令、指令、規制、ポリシー、標準、ガイダンス、またはミッションやビジネスのニーズによって導かれ、情報を得ることができる。指定されると、組織で定義されたパラメータの値が要件の一部となる。

[13]CP-09 と CP-09(08)は、バックアップ情報の機密性を確保するために例外的に含まれている。

[14]NIST は ODP の値を設定または割り当てない。選択されたセキュリティ要件に対する ODP の値が、連邦機関または連邦機関のコンソーシアムによって正式に設定または割り当てられていない場合は、連邦機関以外の組織がその値を割り当てて要件を完成させる必要がある。

組織定義のパラメータ

組織定義のパラメータは、セキュリティ要件仕様の重要な部分である。ODP は、組織のミッション、ビジネス機能、運用環境、リスク許容度の多様性を考慮し、組織が CUI セキュリティ要件を明確に定義するために必要な柔軟性と具体性の両方を提供する。さらに、ODP は、指定されたセキュリティ要件が満たされているかどうかを判断する際の一貫したセキュリティ評価を支援する。連邦政府機関または連邦政府機関のコンソーシアムが ODP に特定の値または値の範囲を指定していない場合、連邦政府機関以外の組織は、セキュリティ要件を満たす値を割り当てなければならない。

ディスカッションセクションは、各要件に含まれている。このセクションは、SP 800-53 の制御に関する議論セクションから派生したものであり、要件の実装と評価を容易にするための追加情報を提供する。考察セクションは参考であり、規範ではない。これは、要件の範囲を拡張したり、組織が要件を満たすために使用するソリューションに影響を与えることを意図していない。また、例示の使用は想定内であり、網羅的なものではなく、組織が利用可能な潜在的な選択肢を反映するものではない。参考文献のセクションでは、SP 800-53 のソース・コントロール（[15]）、およびセキュリティ要件に記載されているトピックに関する追加情報が記載された NIST 特別刊行物のリストを提供する。典型的なセキュリティ要件の構成と内容は、以下の例に示すとおりである。

03.13.11 暗号保護

CUI の機密性を保護するために使用する場合、以下のタイプの暗号を実装する：[課題：組織で定義された暗号の種類]。

ディスカッション

暗号は、適用法、大統領令、指令、方針、規制、標準、およびガイドラインに従って実装される。CUI の保護には、FIPS Validated 暗号が推奨される。

参考文献

ソース・コントロール SC-13

サポート出版物 FIPS 140-3 [38]

[15]一部の例外を除き、SP800-53 のセキュリティ管理は、政策、技術、部門に中立的であり、管理は情報のライフサイクル全体にわたって情報を保護するために必要な基本的対策に焦点を当てている。

組織という用語は多くのセキュリティ要件で使用されており、その意味は文脈によって異なる。例えば、ODP を含むセキュリティ要件では、組織は、連邦政府機関または非連邦政府機関のいずれかを指し、要件のパラメータ値を設定する。

附属書 C は、セキュリティ要件の作成に使用されたセキュリティ管理の調整基準と、調整プロ セスの結果について記述している。附属書には、SP800-53 に記載された、要求事項をサポートするコントロールのリストと、 調整基準に従って中程度のベースラインから削除されたコントロールが記載されている。

セキュリティ要件を評価する

SP 800-171A [84]は、本書に記載されたセキュリティ要件を評価するための一連の手順を提供する。この評価手順は、SP 800-53A [57]に記載されている手順に基づいている。

3. セキュリティ要件

このセクションでは、以下の機密性を保護するための 17 のセキュリティ要件について説明する。

連邦機関以外のシステムおよび組織における CUI。第 3 節の要件の文脈で使用される場合、システムという用語は、CUI を処理、保存、または伝送する、あるいはそのようなシステムまたはコンポーネントの保護を提供する、連邦政府以外のシステムまたはシステム・コンポーネントと定義される。すべてのセキュリティ要件が CUI に明確に言及しているわけではない。しかし、これらの要件は、処理中、保管中、および異なる場所間での送信中の CUI の保護に直接影響するため、含まれている。

特殊なシステム（例えば、産業用／プロセス制御システム、医療機器、コンピュータ数値制御機械）を含むいくつかのシステムは、特定のセキュリティ要件の適用に制限があるかもしれない。このような問題に対応するため、要件 03.15.02 に反映されているように、システムセキュリティ計画を使用して、セキュリティ要件に対する永続的な例外を記述する。個々の、孤立した、または一時的な欠陥は、要 件 03.12.02 に反映されているように、行動計画とマイルストーンによって管理される。

セキュリティ要件の範囲と適用可能性

本セクションのセキュリティ要件は、CUI を処理、保管、伝送する、またはそのようなコンポー ネントの保護を提供する連邦政府以外のシステムのコンポーネントにのみ適用される。

3.1. アクセス制御

03.01.01 アカウント管理

a. 許可および禁止されるシステムアカウントのタイプを定義する。

b. ポリシー、手順、前提条件、基準に従って、システムアカウントを作成、有効化、変更、無効化、削除する。

c. 指定する：

1. システムの認可ユーザー、
2. グループとロールのメンバーシップ
3. 各アカウントのアクセス認可（すなわち権限）。

d. に基づいてシステムへのアクセスを認可する：

1.有効なアクセス認可と

2.システムの使用目的。

e. システムアカウントの使用を監視する。

f. 以下の場合、システムアカウントを無効にする：

1. 口座の有効期限が切れている、

2. アカウントが[割り当て：組織で定義された期間]非アクティブになっている、

3. アカウントは、もはやユーザーや個人に関連付けられていない、

4. アカウントが組織のポリシーに違反している。

5. 個人に関連する重大なリスクが発見される。

g. アカウント・マネージャーおよび社内の指定された担当者または役割に通知する：

1. [割り当て：組織で定義された期間］アカウントが不要になったとき。

2. [割り当て：組織で定義された期間]ユーザーが終了または移譲されたとき。

3. [割り当て：組織で定義された期間]は、システムの使用状況または個人について知る必要性が変化したときである。

h. 割り当て：組織で定義された期間]操作がないと予想される場合、または[割り当て：組織で定義された状況]が発生した場合、ユーザーがシステムからログアウトすることを義務付ける。

ディスカッション

この要件は、システムとアプリケーションのアカウント管理に焦点を当てている。アカウントタイプ（特権アクセス、非特権アクセスなど）によって決定される以外のアクセス認可の定義と実施については、次のセクションで扱う。

03.01.02.システムアカウントの種類には、個人、グループ、一時、システム、ゲスト、匿名、緊急、開発者、サービスが含まれる。システム・アカウントの管理者権限を必要とするユーザは、そのようなアカウント及び特権アクセスを承認する担当者により、さらに精査を受ける。リスクが高まるため組織が禁止することができるアカウントの種類には、グループ、緊急、ゲスト、匿名、一時が含まれる。

組織は、アカウント、アカウントのタイプ、またはその両方の組み合わせによって、 アクセス権限やその他の属性を定義することができる。アクセスを認可するために必要な他の属性には、時間帯、曜日、及び発信地の制限が含まれる。その他のシステム・アカウント属性を定義する場合、組織は、システム要件（例：シス テムのアップグレード、定期保守）及びミッション及びビジネス要件（例：時差、出張 要件を容易にするためのリモート・アクセス）を考慮する。

重大なセキュリティリスクをもたらすユーザには、認可されたシステム・ア クセスを利用して危害を加えようとする意図、または敵対者が自分を通じて危害 を加えようとしていることを示す信頼できる証拠がある個人が含まれる。リスクの高い個人のシステムアカウントを無効にする場合は、ミッション・オーナー、ビジネス・オーナー、システム管理者、人事マネジャー、法務担当者間の緊密な連携が不可欠である。組織要員または役割の通知期間は、様々である。

非アクティブ時のログアウトは、行動またはポリシーに基づくものであり、定義された期間より長い非アクティブが予想される場合、ログアウトするための物理的な行動をユーザーに要求する。非アクティブ時のログアウトの自動実行は、03.01.10 で扱われている。

参考文献

ソース・コントロール AC-02、AC-02(03)、AC-02(05)、AC-02(13)

サポート出版物 SP 800-46 [14], SP 800-57-1 [15], SP 800-57-2 [16], SP 80057-3 [17], SP 800-77 [18], SP 800-113 [19], SP 800-114 [20], SP 800-121 [21], SP 800-162[22]、SP800-178[23]、SP800-192[24]、IR7874[25]、IR7966[26]。

03.01.02 アクセスの強制

適用されるアクセス制御ポリシーに従い、CUI およびシステムリソースへの論理アクセスに対する認可を実施する。

ディスカッション

アクセス管理ポリシーは、組織システムにおける能動的な事業体または主体（すなわち、ユーザーまたはユーザーに代わって行動するシステムプロセス）と受動的な事業体またはオブジェクト（すなわち、デバイス、ファイル、レコード、ドメイン）との間のアクセスを制御する。システムアクセスの種類には、リモートアクセスや、インターネットなどの外部ネットワークを通じて通信するシステムへのアクセスが含まれる。アクセス強制メカニズムは、CUI の保護を強化するために、アプリケーションおよびサービス・レベルでも採用すること

ができる。これは、システムがミッションおよびビジネス機能を支援する多くのアプリケーションおよびサービスをホストできることを認識するものである。アクセス管理ポリシーは、03.15.01 に定義されている。

参考文献

ソース・コントロール AC-03

サポート出版物 SP 800-46 [14], SP 800-57-1 [15], SP 800-57-2 [16], SP 80057-3 [17], SP 800-77 [18], SP 800-113 [19], SP 800-114 [20], SP 800-121 [21], SP 800-162[22]、SP800-178[23]、SP800-192[24]、IR7874[25]、IR7966[26]。

03.01.03 情報の流れの施行

システム内および接続されたシステム間の CUI の流れを制御するために、承認された認可を実施する。

ディスカッション

情報フロー管理は、CUI がシステム内およびシステム間で（誰が情報へのアクセスを許可されるかとは対照的に）通過できる場所を、その情報へのその後のアクセスに関係なく規制する。フロー制御の制限には、CUI が平文でインターネットに送信されないようにすること、組織内から発信されたと主張する外部コミュニケーション・トラフィックをブロックすること、内部ウェブ・プロキシ・サーバからでないインターネットへの要求を制限すること、データ構造とコンテンツに基づいて組織間の CUI 転送を制限することなどが含まれる。

組織間で CUI を移転する場合、情報の流れがどのように強制されるかを規定する合意を必要と する場合がある（03.12.05 を参照）。異なるセキュリティ・ポリシーを持つ異なるセキュリティ・ドメインを代表するシス テム間で CUI を移転することは、そのような移転が 1 つまたは複数のドメインのセキュリティ・ ポリシーに違反するリスクをもたらす。このような状況では、情報所有者またはスチュワードが、相互接続されたシステム間の指 定されたポリシー実施ポイントにおいてガイダンスを提供する。組織は、特定のセキュリティ・ポリシーを実施する必要がある場合、特定のアーキテ クチャ・ソリューションを義務付けることを検討する。強制には、相互接続されたシステム間の CUI 転送の禁止（すなわち、情報アクセスのみを許可する）、一方向の情報フローを強制するハードウェア機構の採用、セキュリティ属性とセキュリティラベルを再割り当てする信頼できる格付け変更機構の実装などが含まれる。

組織は一般的に、情報フロー制御ポリシーと実施メカニズムを使用して、指定されたソースと宛先間の CUI のフローを制御する。

(システム内および相互接続されたシステム間のネットワーク、個人、デバイスなど)。フロー制御は、情報または情報経路の特性に基づいて行われる。保護は境界保護デバイス（暗号化トンネル、ルータ、ゲートウェイ、ファイアウォールなど）で行われ、ルールセットを使用したり、システムサービスを制限するコンフィグレーション設定を確立したり、ヘッダ情報に基づくパケットフィルタリング機能を提供したり、メッセージコンテンツに基づくメッセージフィルタリング機能を提供したりする（キーワード検索の実装や文書の特性の使用など)。組織はまた、情報フロー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（すなわち、ハード ウェア、ファームウェア、およびソフトウェアコンポーネント）の信頼性も考慮する。

参考文献

ソース・コントロール AC-04

サポート出版物 SP 800-160-1[11]、SP 800-162[22]、SP 800-178[23]。

03.01.04 職務の分離

a. 分離が必要な個人の職務を識別する。

b. 職務分掌をサポートするために、システムへのアクセス認可を定義する。

ディスカッション

職務の分離は、認可された特権の濫用の可能性に対処し、共謀を伴わない悪意ある活動のリスクを低減する。職務の分離には、ミッション機能とサポート機能とを異なる個人または役割で分担すること、システムサポート機能を異なる個人または役割で実施すること（例えば、品質保証、構成管理、ネットワークセキュリティ、システム管理、評価、プログラミング)、アクセス管理機能を管理する要員が監査機能も管理しないようにすることなどが含まれる。職務分掌違反はシステム及びアプリケーションのドメインにまたがる可能性があるため、組織は職務分掌に関する方針を策定する際に、システム及びシステム構成要素全体を考慮する。この要件は、03.01.02.

参考文献

ソース・コントロール AC-05

サポート出版物 SP 800-162［22]、SP 800-178［23]。

03.01.05 最小特権

a. ユーザー（またはユーザーに代わって行動するプロセス）に対して、割り当てられた組織的タスクを達成するために必要な認可されたシステムアクセスのみを許可する。

b. 課題：組織で定義されたセキュリティ機能」及び「課題：組織で定義されたセキュリティ関連情報」へのアクセスを認可する。

c. ユーザーのロールまたはクラスに割り当てられた権限を確認する[*Assignment*：組織が定めた頻度]で、そのような特権の必要性を検証する。

d. 必要に応じて、権限を再割り当てまたは削除する。

ディスカッション

認可組織は、ユーザーとシステムプロセスの特定の職務と認可されたアクセスについて、最小特権の原則を採用する。最小特権は、システムの開発、実装、および運用に適用される。組織は、最小特権を達成するために、追加のプロセス、役割、およびシステムアカウントの作成を検討する。セキュリティ機能には、システム・アカウントの確立と権限の割り当て、ソフトウェアのインストール、アクセス認可の構成、監査対象イベントの設定、脆弱性スキャン・パラメータの確立、侵入検知パラメータの確立、監査情報の管理が含まれる。セキュリティ関連情報には、脅威・脆弱性情報、ルータやファイアウォールのフィルタリング・ルール、セキュリティ・サービスの構成パラメータ、セキュリティ・アーキテクチャ、暗号鍵管理情報、アクセス管理リスト、監査情報などがある。

参考文献

ソース・コントロール AC-06、AC-06(01)、AC-06(07)、AU-09(04) 補助出版物：なし

03.01.06 最小特権 - 特権アカウント

a. システム上の特権アカウントを[割り当て*:* 組織で定義された職員または役割]に制限する。

b. 特権アカウントを持つユーザ（またはロール）が、非セキュリティ機能または非セキュリティ情報にアクセスするときは、非特権アカウントを使用することを義務付ける。

ディスカッション

特権アカウントとは、非特権アカウントには制限されているリソース（セキュ リティ機能やセキュリティ関連情報を含む）にアクセスするための昇格した特権 を与えられたアカウント

を指す。これらのアカウントは、通常、システム管理者アカウントまたはスーパーユーザーアカウントと表現される。例えば、システムの動作を変更する可能性のあるコマンドを実行するなどの特権機能を実行するためには、特権アカウントが必要になることが多い。特権アカウントを特定の職員または役割に制限することで、認可されたユーザのみがセキュリティ機能またはセキュリティ関連情報にアクセスし、操作できるようにする。そのようなアクセスが不要な場合に非特権アカウントの使用を要求することで、セキュリティ機能またはセキュリティ関連情報への不正なアクセスや操作を制限することができる。

参考文献

ソース・コントロール AC-06(02), AC-06(05)

サポート出版物：なし

03.01.07 最小特権 - 特権機能

a. 非特権ユーザーが特権機能を実行できないようにする。

b. 特権機能の実行を記録する。

ディスカッション

特権機能には、システムアカウントの確立、システム整合性チェックの実 施、パッチ適用操作の実施、システム構成設定の変更、暗号鍵管理操作などがある。非特権ユーザーは、特権機能を実行する認可を持っていない。侵入検知・防止機構や悪意あるコード保護機構を回避することは、非特権ユーザーからの保護を必要とする特権機能の例である。この要件は、03.01.01 における認可特権の定義と、03.01.02 における特権の強制によって達成される条件を表している。

特権機能の悪用は、認可されたユーザーによる意図的なものであれ意図的でないものであれ、あるいはシステム・アカウントを侵害した無許可の外部事業体によるものであれ、組織に重大な悪影響を及ぼしかねない深刻かつ継続的な問題である。特権機能の使用を検知することは、このような悪用を検知し、高度な持続的脅威や内部脅威によるリスクを軽減する一つの方法である。

参考文献

ソース・コントロール AC-06(09), AC-06(10)

サポート出版物：なし

03.01.08 ログオンに失敗する

a. 割り当て：組織で定義された数]の連続した無効なログオン試行を、[割り当て：組織で定義された期間]中に制限する。

b. 自動的に [選択（*1* つ以上）：アカウントまたはノードを [割り当て：組織で定義された期間] ロックする；管理者が解除するまでアカウントまたはノードをロックする；次のログオンプロンプトを遅延させる；システム管理者に通知する；その他のアクションを取る] 失敗した試行の最大回数を超えると、自動的に [選択（*1* つ以上）：アカウントまたはノードを [割り当て：組織で定義された期間] ロックする。

ディスカッション

サービス拒否の可能性があるため、ほとんどの場合、自動システムロックアウトは一時的なものであり、組織によって設定された（すなわち、遅延アルゴリズムを使用した）所定の時間経過後に自動的に解除される。組織は、各コンポーネントの能力に基づいて、異なるシステムコンポーネントに対して異なる遅延アルゴリズムを採用することができる。システムログオンの失敗に対する応答は、システムレベルおよびアプリケーションレベルで実装することができる。

ユーザー名とパスワードに加えて秘密の質問に答えるようユーザーに促す、（完全なロックアウトではなく）ユーザー機能を制限したロックダウンモードを起動する、指定したインターネットプロトコル（IP）アドレスからのみログオンできるようにする、自動化された攻撃を防ぐために CAPTCHA を要求する、場所、時間帯、IP アドレス、デバイス、媒体クセス管理（MAC）アドレスなどのユーザープロファイルを適用する、などの組織定義のアクションが取られる可能性がある。

参考文献

ソース・コントロール AC-07

サポート出版物 SP 800-63-3[27]、SP 800-124[28]。

03.01.09 システム使用通知

システムへのアクセスを許可する前に、適用される CUI 規則と一致するプライバシーとセキュリティに関する通知を含むシステム使用通知メッセージを表示する。

ディスカッション

システム使用通知は、メッセージまたは警告バナーを使用して実装することができる。メッセージまたは警告バナーは、個人が CUI を処理、保管、または伝送するシス テムにログイ

ンする前に表示される。システム使用通知は、人間のユーザとのログオン・インタフェースを介したアクセスに使用され、 人間のインタフェースが存在しない場合は必要ない。組織は、最初のネットワーク・ログオン後にアプリケーションまたは他のシステム・リソースにアクセスするために、二次使用通知が必要かどうかを検討する。自動化されたシステムメッセージの代わりに、ポスターまたはその他の印刷物を使用してもよい。この要件は、03.15.03 に関連している。

参考文献

ソース・コントロール AC-08

サポート出版物：なし

03.01.10 デバイスロック

a. 選択*(1* つ以上*):* [割り当て*:* 組織で定義された期間]非アクティブの後、デバイスロックを開始する。

b. 確立された本人確認および認証手順を使用してユーザがアクセスを再確立するま で、デバイス・ロックを保持する。

c. デバイスロックにより、これまでディスプレイに表示されていた情報を、一般に閲覧可能な画像で隠す。

ディスカッション

デバイスロックは、ユーザーがシステムのすぐ近くから離れるが、不在の一時的な性質のためにログアウトしたくないときに、システムへのアクセスを防ぐために取られる一時的なアクションである。デバイスロックは、オペレーティングシステムレベルまたはアプリケーションレベルで実装することができる。ユーザーによるデバイスロックは、行動またはポリシーに基づくものであり、デバイスロックを開始するためにユーザーが物理的な行動を起こすことを要求する。デバイスロックは、システムからのログアウトの代用としては認められない（例えば、組織が終業時にユーザにログアウトを要求する場合）。一般に閲覧可能な画像には、スクリーンセーバで使用されるパターン、無地、写真画像、時計、バッテリ残量インジケータ、または管理対象非機密情報が表示されないことを条件とする空白画面などの静的または動的画像を含めることができる。

参考文献

ソース・コントロール AC-11、AC-11(01)

サポート出版物：なし

03.01.11 セッション終了

割り当て：セッション切断を必要とする組織定義の条件またはトリガーイベント]の後に、ユーザーセッションを自動的に終了する。

ディスカッション

この要件は、03.13.09 のコミュニケーションセッションに関連するネットワーク接続の終了（すなわち、ネットワークからの切断）とは対照的に、ユーザーが開始した論理セッションの終了に対処するものである。論理セッションは、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）がシ ステムにアクセスするたびに開始される。論理セッションは、ネットワークセッションを終了させることなく終了させることができる。セッションの終了は、セッションが終了した後も継続するようにユーザー（つまりセッションの所有者）によって作成されたプロセスを除き、ユーザーの論理セッションに関連付けられたすべてのシステムプロセスを終了する。自動セッション終了を必要とする条件やトリガーイベントには、組織で定義されたユーザーの非アクティブ期間、システム使用の時間帯制限、特定のタイプのインシデントに対する標的型対応などがある。

参考文献

ソース・コントロール AC-12

サポート出版物：なし

03.01.12 リモートアクセス

a. 許可されるリモートシステムアクセスの種類ごとに、使用制限、構成要件、接続要件を確立する。

b. そのような接続を確立する前に、各タイプのリモートシステムアクセスを認可する。

c. 認可・管理されたアクセス管理ポイントを経由してシステムへのリモートアクセスを行う。

d. 特権コマンドのリモート実行と、セキュリティ関連情報へのリモートアクセスを認可する。

ディスカッション

リモート・アクセスとは、インターネットなどの外部ネットワークを介して通信するシステム（またはユーザーに代わって動作するプロセス）へのアクセスのことである。リモートアクセス方法を検知・管理することで、組織は攻撃を検知し、リモートアクセスポリシーの遵守を保証することができる。管理されたアクセス・コントロール・ポイントを経由してリモート・アクセスをルーティングすることで、そのような接続に対する明示的な制御が強化され、システムへの不正アクセスに対する感受性が低下する。

システムへのリモート・アクセスは、敵対者に悪用され得る重大な潜在的脆弱性を意味する。特権コマンドの実行や、リモートアクセスによるセキュリティ関連情報へのアクセスを制限することで、組織のエクスポージャーを低減し、敵対者による脅威への感受性を低下させることができる。特権コマンドとは、システム上で人間が実行するコマンドであり、セキュリティ機能やセキュリティ関連情報を含むシステムの制御、監視、管理に関与する。セキュリティ関連情報とは、システムのセキュリティ・ポリシーの実施やコードとデータの分離の維持に失敗する可能性があるような形で、セキュリティ機能の動作やセキュリティ・サービスの提供に影響を与える可能性がある情報のことである。特権コマンドは、機密、セキュリティ上重要、またはセキュリティに関連するシステム機能を実行する能力を個人に与える。

参考文献

ソース・コントロール AC-17、AC-17(03)、AC-17(04)

サポート出版物 SP 800-46［14］、SP 800-77［18］、SP 800-113［19］、SP 800-114［20］、SP 800-121［21］、IR 7966［26］。

03.01.13 削除

03.13.08 までに対処する。

03.01.14 削除

03.01.12 に組み込んだ。

03.01.15 削除

03.01.12 に組み込んだ。

03.01.16 ワイヤレス・アクセス

a. システムへの各タイプの無線アクセスについて、使用制限、構成要件、接続要件を確立する。

b. 接続を確立する前に、システムへの各種無線アクセスを認可すること。

c. 使用目的でない場合は、発行や配備の前にワイヤレスネットワーク機能を無効にする。

d. 認証と暗号化を使用して、システムへのワイヤレスアクセスを保護する。

ディスカッション

無線ネットワーク機能は、敵対者に悪用される可能性のある重要な脆弱性を表している。システムへの無線アクセスのための使用制限、構成要件、および接続要件を確立することは、アクセス認可の決定をサポートする基準を提供する。これらの制限および要件は、無線技術を介した無許可のシステム・アクセスに対する感受性を低減する。ワイヤレスネットワークは、認証保護と相互認証を提供する認証プロトコルを使用する。組織は、システムへのワイヤレス・アクセスを保護するために、個人とデバイスを認証する。小型フォーム・ファクタのモバイル・デバイス（スマートフォン、タブレット、スマート・ウオッチなど）を含む、システムへのワイヤレス・アクセスの可能性があるさまざまなデバイスに特別な注意が払われる。システム・コンポーネントに組み込んだ。ワイヤレス・ネットワーキング機能は、敵対者に悪用される可能性のある脆弱性を表している。ユーザとデバイスの強力な認証、強力な暗号化、および必須ミッションまたはビジネス機能に必要のない無線機能を無効にすることで、無線技術に関わる敵による脅威の影響を受けにくくすることができる。

参考文献

ソース・コントロール AC-18、AC-18(01)、AC-18(03)

サポート出版物 SP 800-94［29］、SP 800-97［30］、SP 800-124［28］。

03.01.17 削除

03.01.16 に組み込んだ。

03.01.18 モバイル機器のアクセス管理

a. モバイル機器の使用制限、構成要件、接続要件を定める。

b. モバイル機器のシステムへの接続を認可する。

c. モバイルデバイス上の CUI の機密性を保護するために、フルデバイスまたはコンテナベースの暗号化を導入する。

ディスカッション

モバイルデバイスは、一人で持ち運べるような小型のフォームファクターを持ち、物理的な接続なしに動作するように設計され、ローカル、非リムーバブル、またはリムーバブルのデータストレージを持ち、自己完結型の電源を含むコンピューティングデバイスである。モバイルデバイスの機能には、デバイスが情報を取得できるようにするオンボードセンサー、音声通信機能、および／またはローカルデータを遠隔地と同期させるための内蔵機能が含まれる。例としては、スマートフォン、スマートウォッチ、タブレットなどがある。モバイルデバイスは通常、一個人に関連付けられる。モバイル・デバイスの処理、記憶、伝送能力は、デバイスの性質や意図される目的によっては、ノートブック・システムやデスクトップ・システムと同等であったり、そのサブセットであったりする。組織によっては、ノートブックコンピュータをモバイルデバイスと見なす場合もある。モバイル・デバイスの保護と管理は、行動またはポリシーに基づくものであり、管理区域の外では、そのようなデバイスを保護し管理するために、ユーザーが物理的な行動をとることを要求する。管理区域とは、CUI を保護するために設定された要件を満たすために、組織が物理的または手続き的な管理を提供するスペースのことである。

異なる特性や能力を持つ多種多様なモバイルデバイスがあるため、組織的な制限は、そのようなデバイスの異なるクラスまたはタイプによって異なる可能性がある。モバイル・デバイスの使用制限、構成要件、および接続要件には、構成管理、デバイスの認証、必須の保護ソフトウェアの実装、デバイスの悪意のあるコードのスキャン、ウイルス保護ソフトウェアの更新、重要なソフトウェアの更新とパッチのスキャン、オペレーティング・システムと場合によってはその他のソフトウェアの整合性チェックの実施、不要なハードウェアの無効化などが含まれる。モバイル・デバイスでは、セキュア・コンテナは、エンタープライズ・アプリケーションや情報を個人アプリやデータから分離するように設計されたソフトウェア・ベースのデータ分離を提供する。コンテナには複数のユーザー・インターフェイスが表示されることがあるが、最も一般的なものの 1 つは、電子メール、連絡先、カレンダーなどのビジネス生産性アプリケーション・スイートへのポータルとして機能するモバイル・アプリケーションである。組織は、モバイル・デバイス上の CUI の機密性を保護するために、フルデバイス暗号化またはコンテナ・ベースの暗号化を採用することができる。

参考文献

ソース・コントロール AC-19、AC-19(05)

サポート出版物 SP 800-46[14]、SP 800-114[31]、SP 800-124[28]。

03.01.19 削除

03.01.18 に組み込んだ。

03.01.20 外部システムの使用

a. 特別に認可されていない限り、外部システムの使用を禁止する。

b. 認可された個人によるシステムの使用やアクセスを許可する前に、外部システムで満たすべきセ キュリティ要件を以下のように設定する：[割り当て：組織が定義したセキュリティ要件]。

c. 認可された個人が外部システムを使用して組織システムにアクセスすること、または CUI を処理、保管、送信することを、以下の場合にのみ許可する：

   1. 組織のシステムセキュリティ計画で規定されている外部システムのセキュリティ要件が満たされていることを検証する。

   2. 外部システムをホストする事業体との間で、承認されたシステム接続または処理契約を保持する。

d. 認可された個人による、組織が管理するポータブルストレージデバイスの外部システムでの使用を制限する。

ディスカッション

外部システムとは、組織の一部ではないが、組織が使用するシステムである。このようなシステムには、個人所有のシステム、システムコンポーネント、またはデバイス、商業施設や公共施設にある個人所有のコンピューティングおよび通信デバイス、連邦政府以外の組織が所有または管理するシステム、および請負業者が管理するシステムが含まれる。組織には、あらゆる種類の外部システムまたは特定の種類の外部システムの使用を禁止するオプションがある（例えば、組織所有でない外部システムの使用を禁止する）。条件は、外部システムを所有、運用、または保守する事業体との間に確立された信頼関係と一致し、共有責任の説明を含む。

認可された個人には、組織要員、請負業者、または組織システムへのアクセスを認可され、組織がシステムアクセスに関する特定の行動ルールを課す権限を持つその他の個人が含まれる。組織が認可個人に課す制限は、組織間の信頼関係によって異なる場合がある。組織は、外部システムが必要なセキュリティ要件を満たしていることを保証する必要がある。この要件は、03.16.03 に関連している。

参考文献

ソース・コントロール AC-20、AC-20(01)、AC-20(02)

サポート出版物：なし

03.01.21 削除

03.01.20 に組み込んだ。

03.01.22 一般にアクセス可能なコンテンツ

a. 認可された個人を訓練し、一般にアクセス可能な情報に CUI が含まれないようにする。

b. 一般にアクセス可能なシステムのコンテンツに CUI がないか確認し、そのような情報が発見された場合は削除する。

ディスカッション

適用法、大統領令、指令、方針、規制、標準、ガイドラインに従い、一般市民は、CUI を含む非公開情報にアクセスすることは認可されていない。

参考文献

ソース・コントロール AC-22

サポート出版物：なし

3.2. 意識向上およびトレーニング

03.02.01 識字率向上およびトレーニング

a. システムユーザにセキュリティリテラシートレーニングを提供する：

1. 新規ユーザーに対する初回トレーニングの一環として、またその後は［割り当て：組織が定めた頻度］で実施する、

2. システムの変更または［割り当て：組織で定義されたイベント］の後に必要な場合、および

3. インサイダー脅威、ソーシャル・エンジニアリング、ソーシャル・マイニングの指標を認識し、報告する。

b. セキュリティリテラシートレーニングの内容 [担当*:* 組織が定めた頻度] と [担当*:* 組織が定めたイベント] を更新する。

ディスカッション

組織は、システムユーザ（マネージャ、上級管理職、システム管理者、請負業者を含む）に対して、基本レベルおよび上級レベルのセキュリティリテラシートレーニングを提供し、ユーザの知識レベルをテストする手段を提供する。組織は、特定の組織要件、要員に認可されたアクセス先のシステム、作業環境（テレワークなど）に基づいて、リテラシー教育の内容を決定する。内容には、セキュリティの必要性の理解、およびセキュリティを維持しインシデントに対応するためにユーザに求められる行動が含まれる。また、運用セキュリティの必要性と CUI の取り扱いについても扱う。

セキュリティ意識の向上手法には、ポスターの掲示、セキュリティに関する注意事項が刻まれた備品の提供、電子メールによる勧告や組織職員からの通知の生成、ログオン画面メッセージの表示、ポッドキャスト、ビデオ、ウェビナーを使用した意識向上イベントの実施などがある。セキュリティリテラシートレーニングは、適用法、指令、規制、方針に沿った頻度で実施する。リテラシー研修の内容を定期的に更新することで、内容の適切性が保たれる。リテラシー研修の内容を更新するきっかけとなる出来事には、評価や監査の結果、セ キュリティインシデントや侵害、適用法、大統領令、指令、規則、ポリシー、標準、ガ イドラインの変更などがある。

インサイダー脅威の潜在的な指標や前兆となる可能性のある行動には、過度に長期的な職務上の不満、職務遂行に必要でない情報へのアクセスの試み、財源への説明のつかないアクセス、同僚従業員へのセクシャルハラスメントやいじめ、職場での暴力、その他組織の方針、手順、規則、指令、慣行に対する重大な違反などがある。組織は、インサイダー脅威の認識に関するトピックを役割に合わせて調整することを検討することができる（例えば、管理者向けのトレーニングはチームメンバーの行動の具体的な変化に焦点を当て、従業員向けのトレーニングはより一般的な観察に焦点を当てることができる）。

ソーシャル・エンジニアリングとは、個人を欺き、情報を開示させたり、システ ムを侵害、危殆化、またはその他の悪影響を与えるような行動を取らせようとす る試みである。ソーシャルエンジニアリングには、フィッシング、口実、なりすまし、おとり、見返り、スレッドジャッキング、ソーシャル媒体悪用、尾行などが含まれる。ソーシャルマイニングとは、将来の攻撃に利用される可能性のある組織に関する情報を収集する試みである。セキュリティリテラシーのトレーニングには、内部脅威の潜在的な指標、ソーシャルエンジニアリングやデータマイニングの潜在的な事例や実際の事例に関する従業員や管理職の懸念を、確立されたポリシーと手順に従い、適切な組織のチャネルを通じてコミュニケーションする方法が含まれる。

参考文献

ソース・コントロール AT-02, AT-02(02), AT-02(03)

サポート出版物 SP 800-50[32]、SP 800-160-2[10]。

03.02.02 役割に基づくトレーニング

a. 組織の要員に対して、役割に応じたセキュリティトレーニングを実施する：

   1. システムまたは CUI へのアクセスを認可する前、割り当てられた職務を遂行する前、およびその後[割り当て：組織で定義された頻度]。

   2. システムの変更または［割り当て：組織で定義されたイベント］の後に必要な場合。

b. 役割に応じたトレーニング内容[割り当て：組織で定義された頻度]と次の[割り当て：組織で定義されたイベント]を更新する。

ディスカッション

組織は、各人に割り当てられた職務、役割、責任、及び要員がアクセスを認可されているシス テムのセキュリティ要件に基づいて、セキュリティ教育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、ソフトウエア開発者、システムインテグレータ、取得／調達担当者、システム管理者及びネットワーク管理者、構成管理及び監査活動を実施する要員、独立した検証及び妥当性確認を実施する要員、セキュリティ評価者、システムレベルのソフトウエアにアクセスできる要員に対して、それぞれの担当職務に特化したセキュリティ関連の技術トレーニングを提供する。

包括的な役割ベースのトレーニングは、物理的、要員的、技術的な管理をカバーする管理、運用、技術的な役割と責任を扱う。このような訓練には、定義されたセキュリティ役割のための方針、手順、ツール、成果物を含めることができる。また、組織は、組織の情報セキュリ ティプログラムの範囲内で、業務及びサプライチェーンのセキュリティに関連する 責任を個人が遂行するために必要な研修も提供する。

参考文献

ソース・コントロール AT-03

サポート出版物 SP 800-161［33]、SP 800-181［34]。

03.02.03 削除

03.02.01 に組み込んだ。

3.3. 監査および説明責任

03.03.01 イベントログ

a. システム内のロギング用に選択された以下のイベントタイプを指定する：[割り当て：組織定義のイベントタイプ]。

b. ロギングのために選択されたイベントタイプをレビューし、更新する[割り当て：組織定義の頻度]。

ディスカッション

イベントとは、非合法または未承認のシステム活動を含む、システムにおける観察可能なあらゆる発生である。組織は、ロギング機能が必要とされるイベントタイプを識別する。これには、特定の継続的な監査ニーズを満たすために、システムのセキュリ ティとシステムが動作する環境に関連するイベントが含まれる。イベント・タイプには、パスワードの変更、特権機能の実行、システムに関連する失敗したログオンまたはアクセス、管理者権限の使用、またはサードパーティ認証情報の使用を含めることができる。ログ記録が必要なイベントタイプを決定する際、組織は、各セキュリティ要件に適切なシステ ム監視と監査を考慮する。イベントの種類を定義するとき、組織は、分散したトランザクションベースのプロセス（例え ば、複数の組織に分散したプロセス）のステップや、サービス指向アーキテクチャやクラウドベースのアーキテク チャで発生するアクションなど、関連するイベントをカバーするために必要なロギングを考慮する。

監視・監査要件は、他のシステムニーズとバランスをとることができる。例えば、成功した場合も失敗した場合も、すべてのファイル・アクセスをログに記録する機能がシステムには必要だが、システム・パフォーマンスに潜在的な負担がかかるため、特定の状況下でのみその機能を有効にする必要があると、組織が判断する場合がある。組織がログに記録するイベントタイプは、時間の経過とともに変更される可能性がある。ログに記録されるイベント・タイプのセットを見直し、更新することは、現在のイベント・タイプ・セットが適切であり続けることを確実にするために必要である。

参考文献

ソース・コントロール AU-02

サポート出版物 SP 800-92 [35]

03.03.02 監査記録の内容

a. 監査記録に以下の内容を含める：

1. どのような出来事が起きたか
2. イベントが発生した時期
3. イベントが発生した場所
4. イベントのソース
5. イベントの結果
6. その事象に関連する個人、主体、対象、事業体のアイデンティティ

b. 必要に応じて、監査記録のための追加情報を提供する。

ディスカッション

監査機能をサポートするために必要な監査記録の内容には、タイムスタンプ、送信元アドレスと宛先アドレス、ユーザーまたはプロセス識別、イベントの説明、ファイル名、および呼び出されたアクセス管理またはフロー制御ルールが含まれる。イベントの結果には、イベントの成否の指標とイベント固有の結果（例えば、イベント発生後のシ ステムのセキュリティ状態）を含めることができる。組織が監査記録で考慮する詳細情報には、特権コマンドの全文記録や、グループ・アカウント・ユーザの個々の ID が含まれる。

参考文献

ソース・コントロール au-03, au-03(01)

サポート出版物：なし

03.03.03 監査記録生成的

a. 03.03.01 および 03.03.02 で指定された、選択されたイベントタイプおよび監査記録内容の監査記録を生成する。

b. 監査記録は、記録保存方針と一致する期間保存する。

ディスカッション

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む、様々な抽象レベルで生成することができる。適切な抽象化レベルを選択することは、監査ロギング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ことができる。監査記録に生成された情

報を追加する機能は、監査記録の内容を構成するシステム機能に依存する。組織は、起動されたアクセス管理またはフロー制御ルール、およびグループ・アカウント・ユーザーの個々の ID を含む、監査記録における追加情報を考慮することができる。組織はまた、監査レコードの追加情報を、監査要件に明示的に必要な情報のみに制限することを検討してもよい。

参考文献

ソース・コントロール AU-11、AU-12

サポート出版物 SP 800-92 [35]

03.03.04 監査ロギング・プロセスの失敗への対応

a. 監査ロギングプロセスが失敗した場合、[割り当て：組織で定義された期間]内に組織の要員または役割に警告する。

b. 以下の追加アクションを取る：*[*割り当て：組織定義の追加アクション]。

ディスカッション

監査ロギング・プロセスの障害には、ソフトウェアやハードウェアのエラー、監査ログの取り込み機構の障害、監査ログの記憶容量に達するか、それを超えることなどが含まれる。対応措置には、最も古い監査記録の上書き、システムのシャットダウン、監査記録の生成停止が含まれる。組織は、障害の種類、障害の場所、障害の重大度、またはそのような要因の組み合わせに基づいて、監査ログ記録プロセスの障害に対する追加のアクションを定義することを選択できる。監査ロギングプロセスの障害がストレージに関連する場合、対応は、監査ログストレージリポジトリ（すなわち、監査ログが保存される明確なシステムコンポーネント）、監査ログが存在するシステム、組織の総監査ログストレージ容量（すなわち、すべての監査ログストレージリポジトリを合わせたもの）、またはこれら 3 つすべてに対して実施される。組織は、指定された役割または担当者に警告を発した後、追加の措置を取らないことを決定することができる。

参考文献

ソース・コントロール AU-05

サポート出版物：なし

03.03.05 監査記録のレビュー、分析、報告

a. 不適切または異常な活動の兆候と潜在的な影響について、システム監査記録をレビューし、分析する [担当業務：組織が定めた頻度*]*。

b. 調査結果を組織の担当者または役割に報告する。

c. 組織全体の状況認識を得るために、異なるリポジトリ間で監査記録を分析し、関連付ける。

ディスカッション

監査記録のレビュー、分析、及び報告は、組織が実施する情報セキュリティロギングを対象とし、アカウントの使用、リモートアクセス、無線接続、構成設定、保守ツールの使用及び非ローカル保守、システムコンポーネントのインベントリ、モバイルデバイスの接続、機器の搬入及び搬出、物理的アクセス、温度及び湿度、システムインターフェースにおけるコミュニケーション、並びにモバイルコードの使用の監視から生じるロギングを含むことができる。発見された事項は、インシデント対応チーム、ヘルプデスク、セキュリティまたはプライバシーオフィスなどの事業体に報告することができる。組織が監査記録のレビューや分析を禁止されているか、そのような活動を実施できない場合、レビューや分析は、そのような権限を付与された他の組織が実施することができる。監査記録のレビュー、分析、及び報告の範囲、頻度、及び／又は深さは、受け取った新情報に基 づき、組織のニーズに合わせて調整することができる。監査記録のレビュー、分析、及び報告のプロセスを関連付けることは、監査記録が集合的により完全な事象の把握を確実にするのに役立つ。

参考文献

ソース・コントロール au-06, au-06(03)

サポート出版物 SP 800-86［36］、SP 800-101［37］。

03.03.06 監査記録の削減とレポート生成的

a. 監査記録のレビュー、分析、報告要件、およびインシデントの事後調査をサポートする、監査記録の削減および報告書生成機能を導入する。

b. 監査記録の元の内容と時間順序を保存する。

ディスカッション

監査記録は 03.03.03 で生成される。監査記録の縮小と報告書の生成は、監査記録の生成の後に行われる。監査記録の縮小は、収集された監査情報を操作し、分析者にとってより意味のある要約形式に整理するプロセスである。監査記録削減及び報告書生成の能力は、監査活動を行う同じシステム又は事業体から生まれるとは限らない。監査記録の削減機能には、例えば、監査記録中の異常な行動を特定するための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含めることができる。システムが提供するレポート生成機能は、カスタマイズ可能なレポートの生成に役立つ。監査記録のタイムスタンプの粒度が不十分な場合、監査記録の時間順序は重大な問題となり得る。

参考文献

ソース・コントロール AU-07

サポート出版物：なし

03.03.07 タイムスタンプ

a. 内部システムクロックを使用して、監査記録のタイムスタンプを生成する。

b. 割り当て：組織が定義した時間測定の粒度]を満たし、協定世界時（UTC）を使用するか、UTC からの固定ローカル時間オフセットを持つか、またはタイムスタンプの一部としてローカル時間オフセットを含む監査記録のタイムスタンプを記録する。

ディスカッション

システムによって生成されるタイムスタンプには、日付と時刻が含まれる。時刻は、グリニッジ標準時（GMT）を現代的に継承した協定世界時（UTC）、または UTC からオフセットされたローカルタイムで表されることが多い。時間計測の粒度とは、システム・クロックと基準クロックの同期の度合いを指す（例えば、数百ミリ秒から数十ミリ秒以内に同期するクロック）。組織は、システム・コンポーネントに対して異なる時間粒度を定義することができる。タイムサービスは、他のセキュリティ機能（アクセス管理、認証など）にとって重要であり、それらの機能をサポートするために使用されるメカニズムの性質に依存する。

参考文献

ソース・コントロール AU-08

サポート出版物：なし

03.03.08 監査情報の保護

a. 監査情報と監査ロギングツールを不正アクセス、変更、削除から保護する。

b. 監査ログの管理機能へのアクセスを、特権ユーザまたはロールのサブセットのみに認可する。

ディスカッション

監査情報には、監査記録、監査ログ設定、監査レポート、個人を特定できる情報など、システム活動を正常に監査するために必要な情報が含まれる。監査ロギングツールは、監査およびロギング活動を実施するために使用されるプログラムおよび装置である。監査情報の保護は、技術的な保護に重点を置き、監査ロギングツールにアクセスし実行する能力を認可された個人に制限する。監査情報の物理的保護は、媒体および物理的保護要件によって対処される。

システムに対する特権的なアクセス権を持ち、そのシステムによる監査の対象でもある個人または役割は、監査活動を阻害したり監査記録を変更したりすることによって、監査情報の信頼性に影響を与える可能性がある。特権アクセスを監査関連特権とその他の特権の間でさらに定義することを要求することにより、監査関連特権を持つユーザまたはロールの数を制限する。

参考文献

ソース・コントロール au-09, au-09(04)

サポート出版物：なし

03.03.09 削除

03.03.08 に組み込んだ。

3.4. 構成管理

03.04.01 ベースライン設定

a. 構成管理の下で、システムの現在のベースライン構成を開発し、維持する。

b. システムのベースライン構成を見直し、更新する：

組織で定義された頻度]、およびシステムコンポーネントが設置または変更されたとき。

ディスカッション

システムおよびシステム構成要素のベースライン構成には、接続性、運用、およびコミュニケーションの側面が含まれる。ベースライン構成は、文書化され、正式にレビューされ、システムまたはシステム内の構成項目の仕様として合意されたものである。ベースライン・構成は、将来のシステムの構築、リリース、変更の基礎となるもので、システム・コンポーネント、運用手順、ネットワーク・トポロジー、システム・アーキテクチャにおけるコンポーネントの配置に関する情報が含まれる。ベースライン・構成を維持するには、システムの経

年変化に応じて新しいベースラインを作成する必要がある。システムのベースライン構成は、現在のエンタープライズ・アーキテクチャを反映する。

参考文献

ソース・コントロール CM-02

サポート出版物 SP 800-124[28]、SP 800-128[41]、IR 8011-2[42]、IR 8011-3[43]。

03.04.02 構成設定

a. 運用要件に合致した最も制限的なモードを反映する、システムの以下の構成設定を確立し、文書化し、実装する：*[*割り当て：組織が定義した構成設定]。

b. 確立された構成設定からの逸脱を識別し、文書化し、承認する。

ディスカッション

構成設定とは、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・コンポーネントで変更可能で、システムのセキュリティ態勢や機能に影響を与えるパラメータのセットである。セキュリティ関連の構成設定は、システム（サーバ、ワークステーションなど）、入出力デバイス（スキャナ、コピー機、プリンタなど）、ネットワークコンポーネント（ファイアウォール、ルータ、ゲートウェイ、音声・データスイッチ、無線アクセスポイント、ネットワークアプライアンス、センサなど）、オペレーティングシステム、ミドルウェア、アプリケーションに対して定義することができる。

セキュリティ・パラメータとは、システムのセキュリティ状態に影響を与えるパ ラメータであり、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む。セキュリティ・パラメータには、レジストリ設定、アカウント、ファイル、ディレクトリの権限設定（すなわち権限）、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、組織全体の構成設定を確立し、その後、システム固有の構成設定を導き出す。確立された設定は、システムの構成ベースラインの一部となる。

共通セキュア構成（セキュア構成チェックリスト、ロックダウンおよびハードニングガイド、セキュ リティ参照ガイド、セキュリティ技術実装ガイドとも呼ばれる）は、特定の情報技術プラットフォーム／製品 のセキュア構成設定と、運用要件を満たすためにそれらのシステムコンポーネントを構成するための指示を 規定する、認知され、標準化され、確立されたベンチマークを提供する。共通のセキュアな構成は、情報技術製品の開発者、製造事業者、ベンダー、コンソーシ ア、学術界、産業界、連邦政府機関、官民のその他の組織など、さまざまな組織によって 開発される。

参考文献

ソース・コントロール CM-06

サポート出版物 SP 800-70［44］、SP 800-126［45］、SP 800-128［41］。

03.04.03 構成変更管理

a. 構成管理されるシステムへの変更の種類を定義する。

b. システムに対して提案された構成管理上の変更をレビューし、セキュリ ティへの影響を明示的に考慮した上で、そのような変更を承認又は不承認とする。

c. 承認された構成管理された変更をシステムに実施し、文書化する。

d. システムに対する構成管理された変更に関連する活動を監視し、レビューする。

ディスカッション

構成変更管理とは、システムに対する変更の追跡、レビュー、承認または不承認、および変更履歴を記録することを指す。具体的には、システムのアップグレードや修正を含む、システムに対する変更の体系的な提案、正当化、実装、テスト、レビュー、および処分が含まれる。

構成変更管理には、システム・コンポーネント（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、モバイル機器など）およびシステムの構成項目に関するベースライン構成の変更、構成設定の変更、予定外の不正な変更、脆弱性を是正するための変更が含まれる。この要件は、03.04.04 に関連する。

参考文献

ソース・コントロール CM-03

サポート出版物 SP 800-124［28］、SP 800-128［41］。

03.04.04 影響分析

a. システムに対する変更を分析し、変更実施前にセキュリティへの潜在的影響を判断する。

b. システムのセキュリティ要件が、システム変更実施後も引き続き満たされていることを検証する。

ディスカッション

この影響分析には、システムセキュリティ計画、方針及び手順をレビューしてセキュリ ティ要件を理解すること、システム設計文書及び運用手順をレビューしてシステムの 変更がシステムのセキュリティ状態にどのような影響を及ぼす可能性があるかを理解すること、 システムの変更がサプライチェーンパートナーに及ぼす影響を利害関係者とともにレビューすること、システムの潜在的な変更によって新たなリスクがどのように生じるか及びそれらのリスクを 軽減する能力を決定することが含まれる。影響分析には、変更の影響を理解し、追加的なセキュリ ティ要件が必要かどうかを判断するためのリスクアセスメントも含まれる。システムの変更は、以前に実施された保障措置及び対策に影響を及ぼす可能性がある。この要件は 03.04.03 に関連する。システムに対するすべての変更が構成管理されているわけではない。

参考文献

ソース・コントロール cm-04, cm-04(02)

サポート出版物 SP 800-128 [41]

03.04.05 変更のためのアクセス制限

システムへの変更に伴う物理的および論理的なアクセス制限を定義し、文書化し、承認し、実施する。

ディスカッション

システムのハードウェア、ソフトウェア、ファームウェア・コンポーネント、またはシステムに関連する運用手順の変更は、システムのセキュリティに重大な影響を及ぼす可能性がある。したがって、組織は、変更を開始する目的で、資格を有し認可された個人のみがシステムにアクセスすることを許可する。アクセス制限には、物理的および論理的なアクセス管理、ソフトウェア・ライブラリ、 ワークフローの自動化、媒体・ライブラリ、抽象的なレイヤ（すなわち、変更をシステ ムに直接実装するのではなく、外部インタフェースに実装する）、および変更ウィンドウ（すなわち、 変更は指定された時間帯にのみ発生する）が含まれる。

参考文献

ソース・コントロール CM-05

サポート出版物 FIPS 140-3[38]、FIPS 180-4[39]、SP 800-128[41]。

03.04.06 最小機能

a. ミッションに必要な機能のみを提供するようにシステムを構成する。

b. 以下の機能、ポート、プロトコル、接続、およびサービスの使用を禁止または制限する：*[*割り当て：組織で定義された機能、ポート、プロトコル、接続、およびサービス]。

c. システムをレビューする [課題*:* 組織が定義した頻度] 不要な機能、または安全でない機能、ポート、プロトコル、接続、およびサービスを特定する。

d. 不要または安全でない機能、ポート、プロトコル、接続、サービスを無効化または削除する。

ディスカッション

システムは様々な機能やサービスを提供できる。デフォルトで日常的にプロバイダとして提供される機能やサービスの中には、組織の重要なミッション、機能、または運用をサポートするために必要でないものもある。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かもしれない。しかし、そうすると、1 つのコンポーネントが提供するサービスを制限するよりもリスクが増大する。実行可能な場合、組織はコンポーネントごとに機能を単一機能に制限する。

組織は、システムまたはシステムコンポーネントが提供する機能およびサービスをレビューし、どの機能およびサービスが削除候補であるかを決定する。組織は、使用されていない、または不要な物理的・論理的ポートおよびプロトコルを無効化し、デバイスの不正接続、情報の転送、トンネリングを防止する。組織は、ネットワーク・スキャニング・ツール、侵入検知・保護システム、およびエンドポイント保護システム（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）を採用して、禁止されている機能、ポート、プロトコル、システム接続、およびサービスの使用を特定し、防止することができる。

ブルートゥース、ファイル転送プロトコル（FTP）、ピアツーピアネットワーキングなどは、組織が排除、制限、無効化を検討するプロトコルの一例である。

参考文献

ソース・コントロール cm-07, cm-07(01)

サポート出版物 SP 800-160-1[11]、SP 800-167[46]。

03.04.07 削除

03.04.06 および 03.04.08 に組み込んだ。

03.04.08 認可ソフトウェア - 例外による許可

a. システム上での実行が認可されたソフトウェアプログラムを識別する。

b. システム上で認可されたソフトウェアプログラムの実行について、すべて拒否し、例外を認めるポリシーを実装する。

c. 認可されたソフトウェアプログラムのリストを見直し，更新する［担当部署が定めた頻度］。

ディスカッション

必要な権限が与えられていれば、ユーザは組織のシステムにソフトウェアをインストールできる。インストールされるソフトウェアの管理を維持するために、組織は、ソフトウェアのインストー ルに関して許可されるアクションと禁止されるアクションを識別する。許可されるソフトウェアのインストールには、既存のソフトウェアのアップデートやセキュリティパッチ、組織が承認した「アプリストア」からの新しいアプリケーションのダウンロードなどが含まれる。ユーザがインストールしたソフトウェアをガバナンスするために選択されるポリシーは、組織が開発したもの、または何らかの外部事業体から提供されたものである。ポリシーの実施方法には、手続き的な方法と自動化された方法がある。

認可されたソフトウェアプログラムは、特定のバージョンに制限されたり、 特定のソースから提供されたりすることがある。包括的な認可ソフトウェアプロセスを容易にし、アプリケーションレベルの認可ソ フトウェアをバイパスする攻撃に対する保護の強度を高めるために、ソフトウェアプ ログラムは異なる詳細レベルに分解され、監視されることがある。これらのレベルには、アプリケーション、アプリケーション・プログラミング・インタフェース、アプリケーション・モジュール、スクリプト、システム・プロセス、システム・サービス、カーネル機能、レジストリ、ドライバ、ダイナミック・リンク・ライブラリが含まれる。

参考文献

ソース・コントロール CM-07(05)

サポート出版物 SP 800-160-1[11]、SP 800-167[46]。

03.04.09 削除

03.01.05、03.01.06、03.01.07、03.04.08、03.12.03 による。

03.04.10 システムコンポーネントのインベントリ

a. システムコンポーネントのインベントリを作成し、文書化する。

b. システムコンポーネントのインベントリをレビューし、更新する [担当業務：組織が定めた頻度]。

c. インストール、削除、システムアップデートの一環として、システムコンポーネントインベントリを更新する。

ディスカッション

システム・コンポーネントとは、システムを構成する個別の識別可能な資産（すなわち、ハード ウェア、ソフトウェア、ファームウェア要素）である。組織は、すべてのシステムのコンポーネントを含む、一元化されたシステムコンポーネ ントインベントリを実施することができる。そのような状況では、組織は、インベントリに、コンポーネントの説明責任に必要なシステム固有情報が含まれていることを保証する。システム・コンポーネントの効果的な説明責任に必要な情報には、システム名、ソフトウ ェア所有者、ソフトウェア・バージョン番号、ソフトウェア・ライセンス情報、ハ ードウェア・インベントリ仕様、および（ネットワーク接続されたコンポーネントについては） すべての実装プロトコル（IPv4、IPv6 など）のマシン名とネットワーク・アドレスが含 まれる。インベントリ仕様には、コンポーネントのタイプ、物理的な場所、受領日、製造事業者、コスト、モデル、シリアル番号、サプライヤー情報が含まれる。

参考文献

ソース・コントロール cm-08, cm-08(01)

サポート出版物 SP 800-124[28]、SP 800-128[41]、IR 8011-2[42]、IR 8011-3[43]。

03.04.11 インフォメーション・ロケーション

a. CUI の場所と、情報が処理され保存されるシステム・コンポーネントを特定し、文書化する。

b. CUI が処理され保管されるシステムまたはシステム・コンポーネントの場所の変更を文書化する。

ディスカッション

情報ロケーションは、情報フロー管理、アクセス管理、情報管理などの適切な保護メカニズムを提供できるように、CUI が処理され保管されている特定のシステム・コンポーネント、および CUI にアクセスできるユーザーを理解する必要性に対処する。

参考文献

ソース・コントロール CM-12

サポート出版物：なし

03.04.12 高リスク地域のシステムおよびコンポーネントの構成

a. リスクの高い場所に出張する個人に対して、以下の構成を持つシステムまたはシステムコンポーネントを発行する：[割り当て：組織が定義したシステム構成]。

b. 出張から帰ったら、システムまたはコンポーネントに以下のセキュリティ要件を適用する。

ディスカッション

システムまたはシステム・コンポーネントがリスクの高い地域に行くことが分かっている場合、脅威の増大に対抗するために追加のセキュリティ要件が必要になることがある。組織は、出張に出発する個人および出張から戻る個人が使用するシステムまたはシステム・コンポーネントに保護措置を講じることができる。対策には、懸念される場所かどうかを判断すること、コンポーネントに必要な構成を定義すること、旅行を開始する前にコンポーネントが意図したとおりに構成されていることを確認すること、旅行が完了した後に追加の対策を講じることなどが含まれる。例えば、リスクの高い地域に行くシステムは、ハードディスクをサニタイズし、アプリケーションを制限し、より厳格な構成設定にすることができる。旅行から戻ったモバイル・デバイスに適用される措置には、物理的な改ざんの兆候がないかデバイスを検査し、デバイス・ストレージをパージして再イメージングすることが含まれる。

参考文献

ソース・コントロール CM-02(07)

サポート出版物 SP 800-124［28］、SP 800-128［41］。

3.5. 識別および認証

03.05.01 ユーザーの識別と認証

a. システム・ユーザーを一意に識別・認証し、その一意の識別を、そのユーザーの代理として行動するプロセスに関連付ける。

b. 割り当て：再認証を必要とする組織で定義された状況または状況]が発生した場合は、認証 を再実行する。

ディスカッション

システムユーザーには、システムへのアクセスを認可された個人（または個人に代わって行動するシステムプロセス）が含まれる。通常、個人の識別子は、その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。システム・プロセスは、グループおよびロールの代理として実行されるため、組織は、 グループ・アカウントにおける個人の一意な識別、または個人の活動の説明責任を必要とする場 合がある。ユーザの一意な識別と認証は、すべてのシステム・アクセスに適用される。組織は、パスワード、物理的認証子、バイオメトリクス、またはそれらの組み合わせを使用して、 ユーザの認証を行う。組織は、役割、認証子、または資格情報が変更されたとき、特権機能の実行が発生したとき、 一定期間経過後、または定期的になど、特定の状況で個人を再認証することがある。

参考文献

ソース・コントロール： IA-02,IA-11

サポート出版物 SP 800-63-3 [27]

03.05.02 機器の識別と認証

システム接続を確立する前に、［識別：組織で定義されたデバイスまたはデバイスの種類］を一意に識別し、認証する。

ディスカッション

一意のデバイス間識別および認証が必要なデバイスは、タイプ、デバイス、またはタ イプとデバイスの組み合わせによって定義される。組織定義のデバイス・タイプには、組織が所有しないデバイスが含まれる。システムは、ローカル・エリア・ネットワークおよびワイド・エリア・ネットワーク上のデバイスを識別および認証するために、デバイス識別用の共有既知情報（媒体・アクセス管理[MAC]、伝送制御プロトコル／インターネット・プロトコル[TCP/IP]アドレスなど）または組織認証ソリューション（電気電子学会[IEEE]802.1x および拡張可能認証プロトコル[EAP]、EAP-トランスポート・レイヤー・セキュリティ[TLS]認証付き RADIUS サーバ、Kerberos など）を使用する。公開鍵基盤（PKI）と、交換された証明書の証明書失効チェックを、認証の一部として含めることができる。

参考文献

ソース・コントロール IA-03

サポート出版物 SP 800-63-3 [27]

03.05.03 多要素認証

特権アカウントおよび非特権アカウントへのアクセスに多要素認証を導入する。

ディスカッション

この要件は、ユーザ・アカウントに適用される。多要素認証では、認証を達成するために 2 つ以上の異なる要素を使用する必要がある。認証要素は、「知っているもの」（個人識別番号[PIN]など）、「持っているもの」（暗号化秘密 鍵などの物理的認証子など）、または「いるもの」（バイオメトリクスなど）と定義される。物理的認証手段を特徴とする多要素認証ソリューションには、時間ベースまたはチャレンジ・ レスポンス出力を提供するハードウェア認証手段、およびスマート・カードが含まれる。組織は、システム・レベルでの認証に加えて、アプリケーション・レベルでの認証メカニズ ムを採用して、情報セキュリティを強化することができる。

ソース・コントロール IA-02(01),IA-02(02)

サポート出版物 SP 800-63-3 [27]

03.05.04 リプレイ耐性認証

特権アカウントおよび非特権アカウントへのアクセスについて、リプレイ耐性認証メカニズムを実装する。

ディスカッション

認証プロセスは、以前の認証メッセージを記録または再生することで認証に 成功することが現実的でない場合、リプレイ攻撃に抵抗する。リプレイ耐性のある技術には、時間同期またはチャレンジ・レスポンス・ ワンタイム認証などの、ノンスまたはチャレンジを使用するプロトコルがある。

参考文献

ソース・コントロール IA-02(08)

サポート出版物 SP 800-63-3 [27]

03.05.05 識別子の管理

a. 個人、グループ、役割、サービス、またはデバイス識別子を割り当てるために、組織の職員または役割から認可を受ける。

b. 個人、グループ、役割、サービス、デバイスを識別する識別子を選択し、割り当てる。

c. 識別子の再利用を防止する。

d. 各個人を以下のように一意に識別して、個人識別子を管理する。

[識別：個人の状態を識別する組織定義の特性]。

ディスカッション

識別子は、ユーザー、ユーザーの代理を務めるプロセス、およびデバイスに提供される。識別子の再利用を禁止することで、以前に使用された個人、グループ、役割、サービス、またはデバイスの識別子が、異なる個人、グループ、役割、サービス、またはデバイスに割り当てられることを防ぐ。

個人のステータスを識別する特性には、請負業者、外国人、および非組織ユーザーが含まれる。これらの特性によって個人のステータスを識別することで、組織の要員がコミュニ ケーションしている相手に関する情報が得られる。例えば、従業員にとって、電子メールメッセージ上の個人の一人が請負業者であることを知ることは有益である。

参考文献

ソース・コントロール IA-04,IA-04(04)

03.05.06 削除

SP 800-53 [8]との整合性。

03.05.07 パスワード管理

a. 一般的に使用されているパスワード、予想されるパスワード、または漏洩したパスワードのリストを維持し、[割り当て*:* 組織が定義した頻度]および組織パスワードの漏洩が疑われる場合にリストを更新する。

b. ユーザがパスワードを作成または更新する際に、パスワードがよく使用される、予想される、または漏洩したパスワードのリストにないことを確認する。

c. パスワードの送信は、暗号的に保護されたチャネルのみで行う。

d. パスワードは暗号化された形で保存する。

e. アカウント回復後の最初の使用時に新しいパスワードを選択する。

f. パスワードに対して、以下の構成ルールと複雑さルールを適用する：*[*割り当て：組織で定義された構成と複雑さのルール]。

ディスカッション

パスワード・ベース認証は、1 要素認証または多要素認証で使用されるパスワードに適 用される。長いパスワードまたはパスフレーズは、短いパスワードよりも望ましい。強制的な構成ルールは、セキュリティ上の利点はわずかであるが、使い勝手は低下する。しかし、組織は、特定の状況下で、パスワード生成のための特定のルール（例えば、最小 文字長）を確立し、強制することを選択することができる。例えば、パスワードを忘れた場合、アカウントの回復が発生することがある。暗号的に保護されたパスワードには、パスワードの塩付け一方向暗号ハッシュが含まれる。よく使われるパスワード、危殆化したパスワード、または予想されるパスワードのリストには、過去の侵害コーパスから得られたパスワード、辞書的な単語、反復的または連続的な文字が含まれる。リストには、サービス名、ユーザー名、およびその派生語など、文脈に特有な単語が含まれる。システム・ログオン直後に一時的なパスワードを恒久的なパスワードに変更することで、必要な強 度の認証メカニズムが早い機会に実装され、認証者が危険にさらされる可能性が低くなる。長いパスワードやパスフレーズを使用して、パスワードの複雑性を高めることができる。

参考文献

ソース・コントロール IA-05(01)

サポート出版物 SP 800-63-3

03.05.08 削除

SP 800-53 [8]との整合性。

03.05.09 削除

SP 800-53 [8]との整合性。

03.05.10 削除

03.05.07 に組み込んだ。

03.05.11 認証フィードバック

認証プロセスにおいて、認証情報のフィードバックが不明瞭である。

ディスカッション

認証フィードバックは、権限のない個人が認証メカニズムを侵害できるような情報を提供しない。たとえば、比較的大きなモニタを持つデスクトップまたはノートブック・システムの場合、この 脅威は重大である可能性がある（一般にショルダー・サーフィンと呼ばれる）。小さなディスプレイを持つモバイル・デバイスの場合、この脅威はそれほど大きくないかも しれな

いが、キーボードが小さいために入力エラーが発生する可能性が高くなることとのバランスをとる必要がある。したがって、認証のフィードバックを不明瞭にする手段は、適宜選択される。フィードバックの不明瞭化には、ユーザが入力デバイスにパスワードを入力する際にアスタリスクを 表示する方法や、フィードバックを一定時間表示した後に完全に不明瞭化する方法がある。

参考文献

ソース・コントロール IA-06

サポート出版物：なし

03.05.12 認証管理

a. 最初の認証子配布の一環として、認証子を受け取る個人、グループ、役割、サービス、またはデバイスの ID を検証する。

b. 組織が発行する認証子について、認証の初期コンテンツを確立する。

c. 最初の認証子の配布、紛失、危殆化または破損した認証子、および認証子の失効に関する管理 手続きを確立し、実施する。

d. 初回使用時にデフォルトの認証を変更する。

e. 認証の変更または更新は、[割り当て：組織で定義された頻度]または以下のイベントが発生したときに行う：[割り当て：組織定義のイベント]。

f. 認証コンテンツを不正な開示や改ざんから保護する。

ディスカッション

認証には、パスワード、暗号化装置、バイオメトリクス、証明書、ワンタイムパスワード装置、ID バッジなどがある。初期認証子コンテンツは、認証子の実際のコンテンツである（例えば、初期パスワード）。対照的に、認証子コンテンツに対する要件には、特定の特性が含まれる。認証子管理は、さまざまな認証子特性（パスワードの複雑性と構成規則、時間同期ワンタイムトークン の検証時間ウィンドウ、バイオメトリクス認証の検証段階における拒否許容数など）に対する組織 定義の設定および制限によってサポートされる。

認証の保護要件は、個人が所有する認証については 03.15.03、組織システムに保存される認証につい ては 03.01.01、03.01.02、03.01.05、03.13.08 によって実施することができる。これには、ハッシュ化または暗号化された形式で保存されたパスワード、または管理者権限でア クセス可能なハッシュ化または暗号化されたパスワードを含むファイルが含まれる。認

証子を保護するために、認証子の所有権を維持し、認証子を他者と共有せず、紛失、盗難、危殆化した 認証子を直ちに報告するなどの措置を取ることができる。

開発者は、初期インストールと構成を可能にするために、工場出荷時のデフォルト認証 本人情報とともにシステム・コンポーネントを提供することがある。デフォルト認証本人は、しばしばよく知られ、容易に発見可能であり、重大なリスクをもたらす。認証の管理には、不要になった場合の一時的なアクセスのための認証の発行と取り消しが含 まれる。長いパスワードまたはパスフレーズを使用することで、認証を定期的に変更する必要性が なくなる場合がある。

参考文献

ソース・コントロール IA-05

サポート出版物 SP 800-63-3 [27]

3.6. インシデント対応

03.06.01 インシデントハンドリング

インシデント対応計画に合致し、準備、検知・分析、封じ込め、根絶、復旧を含むインシデントハンドリング能力を導入する。

ディスカッション

インシデント関連情報は、監査監視、ネットワーク監視、物理的アクセス監視、ユーザー及び管理者報告、報告されたサプライチェーンイベントなど、様々な情報源から得ることができる。効果的なインシデントハンドリング能力には、ミッション及びビジネス所有者、システム所有者、人事部、物理的及び人的セキュリティ部、法務部、業務担当者、調達部など、多くの事業体間の調整が必要である。

参考文献

ソース・コントロール IR-04

サポート出版物 SP 800-50 [32]、SP 800-61 [47]、SP 800-161 [33]。

03.06.02 インシデントの監視、報告、および対応支援

a. システムのセキュリティインシデントを追跡し、文書化する。

b. 疑わしいインシデントを、[割り当て*:* 組織が定義した期間]内に組織のインシデント対応能力に報告する。

c. インシデント情報を[認可：組織で定義された当局]に報告する。

d. インシデント対応サポートリソースを提供し、インシデントのハンドリングと報告について、システムユーザーに助言と支援を提供する。

ディスカッション

インシデントの文書化には、インシデントの詳細、傾向、ハンドリングを評価するだけでなく、各インシデントに関する記録、インシデントのステータス、フォレンジックに必要なその他の関連情報を維持することが含まれる。インシデント情報は、ネットワーク監視、インシデント報告、インシデント対応チーム、ユーザからの苦情、サプライチェーンパートナー、監査監視、物理的アクセス監視、ユーザおよび管理者の報告など、多くの情報源から得ることができる。03.06.01 は、監視に適切なインシデントの種類に関する情報を提供する。報告されるインシデントの種類、報告の内容と適時性、および報告権限は、適用法、大統領令、指令、規制、方針、標準、およびガイドラインを反映する。インシデント情報は、リスクアセスメント、セキュリティアセスメントの有効性、取得のセキュリティ要件、技術製品の選定基準に反映される。組織が提供するインシデント対応支援リソースには、ヘルプデスク、アシスタンス・グループ、インシデント対応チケットを開設・追跡するための自動発券システム、必要に応じてフォレンジック・サービスや消費者救済サービスへのアクセスが含まれる。

参考文献

ソース・コントロール IR-05、IR-06、IR-07

サポート出版物 SP 800-61［47］、SP 800-86［36］。

03.06.03 インシデント対応テスト

インシデント対応能力の有効性をテストする［割り当て：組織が定めた頻度］。

ディスカッション

組織は、インシデント対応能力をテストし、その有効性を判断し、潜在的な弱点や欠陥を特定する。インシデント対応テストには、チェックリストの使用、ウォークスルーまたは机上演習、シミュレーショ ンが含まれる。インシデント対応テストには、組織運営、組織資産、および個人に対するインシデント対応の影響の判定を含めることができる。定性的および定量的データは、インシデント対応プロセスの有効性を判断するのに役立つ。

参考文献

ソース・コントロール IR-03

サポート出版物 SP 800-84 [48]

03.06.04 インシデント対応トレーニング

a. 割り当てられた役割と責任に沿ったインシデント対応トレーニングを、システムユーザーに提供する：

   1. インシデント対応の役割や責任を担うようになってから、またはシステムアクセスを獲得してから、[割り当て*:* 組織が定義した期間]以内に行う、

   2. システムの変更によって必要とされる場合

   3. *[*割り当て：組織で定義された頻度]以降。

b. インシデント対応トレーニングの内容[課題：組織で定めた頻度]および次の[課題：組織で定めた事象*]*を見直し、更新する。

ディスカッション

インシデント対応訓練は、適切な内容と詳細レベルがそのような訓練に含まれるように、組織要員の割り当てられた役割と責任に関連付けられる。例えば、ユーザはインシデントの認識方法や連絡先を知るだけでよいかもしれないが、システム管理者はインシデントの処理方法に関する追加訓練が必要かもしれないし、インシデント対応者はデータ収集技術、フォレンジック、報告、システム復旧、システム復元に関する特定の訓練を受けるかもしれない。インシデント対応訓練には、外部および内部ソースからの不審な活動を特定し報告するためのユ ーザー訓練が含まれる。ユーザーに対するインシデント対応訓練は、03.02.02 の一部として提供されることがある。インシデント対応研修内容の更新の原因となる出来事には、インシデント対応計画のテスト、実際のインシデントへの対応、監査または評価の結果、または適用法、大統領令、方針、指令、規制、標準、ガイドラインの変更が含まれる。

参考文献

ソース・コントロール IR-02

サポート出版物 SP 800-86［36］、SP 800-137［49］。

03.06.05 インシデント対応計画

a. 以下のようなインシデント対応計画を策定する：

   1. インシデント対応能力を導入するためのロードマップを組織に提供する、

   2. インシデント対応能力の構造と組織を記述する、

3. インシデント対応能力が組織全体にどのように適合するかについて、高レベルのアプローチを提供する、
4. 報告すべきインシデントを定義する、
5. インシデント情報の共有に取り組む。
6. 事業体、要員、または役割に責任を指定する。

b. インシデント対応計画のコピーを、指定されたインシデント対応要員（氏名および／または役割で識別）および組織要素に配布する。

c. インシデント対応計画を更新し、計画の実施、実行、またはテスト中に発生したシステムおよび組織の変更または問題に対処する。

d. インシデント対応計画を不正な開示から保護する。

ディスカッション

組織は、インシデント対応に対する協調的アプローチを開発し、実施することが重要である。組織の使命と業務機能が、インシデント対応能力の構成を決定する。インシデント対応能力の一部として、組織は、外部のサービスプロバイダーやサプライチェーンに関与する他の組織を含む外部組織との情報の連携と共有を考慮する。

参考文献

ソース・コントロール IR-08

サポート出版物 SP 800-86［36］、SP 800-137［49］。

3.7. 保守

03.07.01 削除

NCO に再分類された。

03.07.02 削除

03.07.04 および 03.07.06 に組み込んだ。

03.07.03 削除

03.08.03 に組み込んだ。

03.07.04 保守ツール

a. システム保守ツールの使用を承認、管理、監視する。

b. 媒体をシステムで使用する前に、診断プログラムやテストプログラムで悪意のあるコードがないかチェックする。

c. 機器に CUI がないことを確認する、機器をサニタイズまたは破壊する、あるいは機器を施設内に保持することにより、CUI を含むシステム保守機器の持ち出しを防止する。

ディスカッション

保守ツールの承認、管理、監視、レビューによって、システムの診断や修理に使用され るツールに関連するセキュリティ関連の問題に対処する。保守ツールには、パケットスニファだけでなく、ハードウェアやソフトウェアの診断・テスト機器も含まれる。保守ツールは、プレインストールされたもの、保守要員とともに媒体で持ち込まれたもの、クラウドベースのもの、ウェブサイトからダウンロードされたものなどがある。診断およびテスト・プログラムは、意図的であれ無意識であれ、悪意のあるコードをシステム内に持ち込む潜在的な手段である。媒体検査の例としては、診断・テストプログラムおよび媒体の暗号ハッシュまたはデジタル署名のチェックがある。

組織が診断プログラム及びテストプログラムを含む媒体を検査し、その媒体にも悪意のあるコードが含まれていると判断した場合、インシデントハンドリングのポリシー及び手順に準拠してインシデントが処理される。システム保守ツールの定期的なレビューにより、時代遅れのツール、サポートされていないツール、無関係なツール、または使用されなくなったツールの承認を取り消すことができる。保守ツールは、保守をサポートし、システムの一部とみなされるハードウェアおよびソフトウェア・コンポーネントには対応していない。

参考文献

ソース・コントロール MA-03, MA-03(01), MA-03(02), MA-03(03)

サポート出版物 SP 800-88 [50]

03.07.05 非ローカル保守

a. 非ローカル保守・診断活動を承認し、監視する。

b. 非ローカル保守および診断セッションの確立において、多要素認証とリプレイ耐性を実装する。

c. 非ローカル保守が完了したら、セッションとネットワーク接続を終了する。

ディスカッション

非ローカル保守・診断活動は、外部または内部ネットワークを通じてコミュニケーションする個人によって行われる。ローカル保守および診断活動は、システムの場所に物理的に存在し、ネットワーク接続を介してコミュニ ケーションを行わない個人によって実施される。非局所保守および診断セッションを確立するために使用される認証技術は、03.05.01 の要件を反映する。

参考文献

ソース・コントロール MA-04

サポート出版物 SP 800-63-3[27]、SP 800-88[50]。

03.07.06 保守要員

a. 保守要員の認可プロセスを確立する。

b. 認可された保守組織または要員のリストを保守する。

c. システムの保守を行う非保護要員が、必要なアクセス認可を持っていることを確認する。

d. 必要なアクセス認可と技術的能力を持つ組織要員を指名し、必要なアクセス認可を持たない要員の保守活動を監督させる。

ディスカッション

保守要員とは、システム上でハードウェアまたはソフトウェアの保守を行う個人を指し、03.10.01 は、保守業務によってシステムの物理的保護境界内に入ることになる個人の物理的アクセスに対処する。監督する個人の技術的能力は、システム上で実行される保守に関連し、必要なアクセス認可を有することは、システム上およびシステム近傍での保守に関連する。認可された保守要員として事前に識別されていない個人（製造事業者、コンサルタント、シス テム・インテグレータ、ベンダーなど）は、ほとんどまたはまったく予告なしに保守を実施 する必要がある場合など、システムへの特権的なアクセスが必要になることがある。組織は、リスクアセスメントに基づいて、これらの個人に一時的クレデンシャルを発行すること を選択できる。一時的なクレデンシャルは、1 回限りの使用または非常に限定された期間の使用である。

参考文献

ソース・コントロール MA-05

サポート出版物：なし

3.8. 媒体保護

03.08.01 媒体・ストレージ

CUI を含むシステム媒体を物理的に管理し、安全に保管する。

ディスカッション

システム・媒体には、デジタル・媒体と非デジタル・媒体がある。デジタル・媒体には、ディスケット、フラッシュ・ドライブ、磁気テープ、外付けまたは取り外し可能なソリッド・ステート・ドライブまたは磁気ドライブ、コンパクト・ディスク、デジタル多用途ディスクが含まれる。非デジタル・媒体には、紙やマイクロフィルムが含まれる。保管された媒体を物理的に管理することには、目録の作成、個人が図書館に媒体を貸出および返却できるようにする手順の確立、保管された媒体の説明責任の維持が含まれる。安全な保管には、施錠された引き出し、机、キャビネット、または管理された媒体・ライブラリーが含まれる。管理区域は、情報およびシステムの保護のために確立された要件を満たすための物理的および手続き上の管理を提供する。サニタイズ技術（例えば、破壊、暗号的消去、クリア、およびパージ）は、権限のない個人への CUI の開示を防止する。サニタイズ・プロセスは、情報が検索または再構築できないように、媒体から CUI を除去する。

参考文献

ソース・コントロール MP-04

サポート出版物 SP 800-88［50］、SP 800-111［51］。

03.08.02 媒体・アクセス

システム・媒体上の CUI へのアクセスを認可された職員または役割に制限する。

ディスカッション

システム・媒体には、デジタル・媒体と非デジタル・媒体が含まれる。システム・媒体上の CUI へのアクセスは、そのような媒体を物理的に管理することにより制限することができる。これには、インベントリの実施、個人が媒体を媒体・ライブラリに貸し出し、返却できるようにする手順の確保、および保存された媒体の説明責任の維持が含まれる。デジタル・媒体の場合、CUI へのアクセスは、暗号化手段を使用することによ って制限することができる。保管中または静止中のデータの暗号化については、03.13.08 に記載されている。

参考文献

ソース・コントロール MP-02

サポート出版物 SP 800-111 [51]

03.08.03 媒体のサニタイズ

CUI を含むシステム・媒体は、廃棄、組織管理外へのリリース、または再利用のためのリリースの前にサニタイズする。

ディスカッション

媒体のサニタイズは、廃棄または再利用の対象となるデジタルおよび非デジタ ル媒体に適用され、その媒体がリムーバブルであるか否かを問わない。例えば、スキャナー、複写機、プリンター、ノートブック・コンピューター、モバイル・デバイス、ワークステーション、ネットワーク・コンポーネント、および非デジタル・媒体のデジタル・媒体が含まれる。サニタイゼーション・プロセスは、情報が検索または再構築できないように、媒体から CUI を除去する。サニタイズ技術（暗号による消去、クリア、パージ、破壊など）は、そのような媒体が再利用されたり、廃棄のために公開されたりする際に、権限のない個人への CUI の開示を防ぐ。NARA の方針は、CUI を含む媒体のサニタイズプロセスを管理し、媒体に他の方法が適用できない場合、破棄を要求することがある。

参考文献

ソース・コントロール MP-06

サポート出版物 SP 800-88 [50]

03.08.04 媒体・マーキング

CUI を含むシステム・媒体には、配布制限、取り扱い上の注意、適用される CUI マーキングを示すためにマークを**付ける。**

ディスカッション

システム媒体には、デジタル媒体と非デジタル媒体が含まれる。マーキング（Marking）とは、人間が読み取り可能なセキュリティ属性の使用または適用を指す。ラベリングとは、内部システムデータ構造に対するセキュリティ属性の使用をいう。デジタル・媒体には、ディスケット、磁気テープ、外付けまたは取り外し可能なソリッド・ステート・ドライブまたは磁気ドライブ、フラッシュ・ドライブ、コンパクト・ディスク、デジタル多用途ディスクが含まれる。非デジタル媒体には、紙とマイクロフィルムが含まれる。CUI は、そのような情報のマーキング、保護、および配布要件とともに NARA によって定義される。

参考文献

ソース・コントロール MP-03

サポート出版物：なし

03.08.05 媒体・トランスポート

a. 管理区域外への輸送中、CUI を含むシステム媒体を保護・管理する。

b. 管理区域外への輸送中、CUI を含むシステム・媒体の説明責任を維持する。

c. CUI を含むシステム媒体の輸送に関連する活動を文書化する。

ディスカッション

システム・媒体には、デジタル・媒体と非デジタル・媒体がある。デジタル・媒体には、フラッシュ・ドライブ、ディスケット、磁気テープ、外付けまたは取り外し可能なソリッド・ステート・ドライブまたは磁気ドライブ、コンパクト・ディスク、デジタル多用途ディスクが含まれる。非デジタル・媒体には、マイクロフィルムと紙が含まれる。管理区域は、CUI およびシステムを保護するために設定された要件を満たす物理的または手 続的手段を組織が提供するスペースである。輸送中の媒体保護には、暗号化および／または施錠されたコンテナを含めることができる。媒体の輸送に関連する活動には、輸送のために媒体を解放すること、媒体が適切な輸 送プロセスに入ることを確実にすること、および実際の輸送が含まれる。認可された輸送要員および宅配要員には、組織の外部の個人が含まれる場合がある。輸送中の媒体のアカウンタビリティの維持には、輸送活動を認可された要員に制限すること、媒体が輸送システムを移動する際に輸送活動の記録を追跡または入手し、紛失、破壊、改ざんを防止および検知することが含まれる。この要件は、03.13.08 及び 03.13.11 に関連する。

参考文献

ソース・コントロール：MP-05、SC-28

サポート出版物 SP 800-111 [51]

03.08.06 削除

03.13.08 までに対処する。

03.08.07 媒体利用

a. 割り当て：組織で定義された種類のシステム媒体]の使用を制限または禁止する。

b. 識別可能な所有者のいないリムーバブル・システム・媒体の使用を禁止する。

ディスカッション

媒体へのユーザーアクセスを制限する要件 03.08.01 とは対照的に、この要件は、外付けハードドライブ、フラッシュドライブ、スマートディスプレイなど、特定のタイプの媒体の使用を制限または禁止する。組織は、技術的および非技術的な手段（例えば、方針、手順、行動規則）を使用して、システム媒体の使用を管理することができる。例えば、組織は、ワークステーションに物理的なケージを使用して外部ポートへのアクセスを禁止したり、デバイスの挿入、読み取り、書き込みの機能を無効にしたり、削除したりすることで、ポータブルストレージデバイスの使用を管理することができる。

組織は、ポータブル・ストレージ・デバイスの使用を、組織から提供されたデバイス、他の承認された組織から提供されたデバイス、および個人所有でないデバイスを含む、承認されたデバイスのみに制限することができる。組織はまた、書き込み可能なポータブル・デバイスの使用を禁止するなど、デバイスの種類に基づいてポータブル・ストレージ・デバイスの使用を管理し、そのようなデバイスへの書き込み機能を無効にするか削除することによって、この制限を実施することもできる。外部システムにおける、組織が管理するシステム媒体の使用制限には、媒体の使用方法と使用条件についての制限が含まれる。リムーバブル・システム・媒体に識別可能な所有者（個人、組織、プロジェクトなど）を要求することで、組織は、媒体の既知の脆弱性（悪意のあるコードの挿入など）に対処する責任と説明責任を割り当てることができ、そのような技術を使用するリスクが低減する。

参考文献

ソース・コントロール MP-07

サポート出版物 SP 800-111 [51]

03.08.08 削除

03.08.07 に組み込んだ。

03.08.09 システム・バックアップ - 暗号保護

a. バックアップ情報の機密性を保護する。

b. バックアップ保管場所における CUI の不正な開示を防止するため、暗号化メカニズムを導入**する。**

ディスカッション

暗号化メカニズムの選択は、バックアップ情報の機密性を保護する必要性に基づいている。ハードウェア・セキュリティ・モジュール（HSM）デバイスは、暗号鍵を保護・管理し、暗号処

理を提供する。暗号処理（暗号化、復号化、署名の生成と検証など）は通常、HSM デバイス上で行われ、多くの実装では暗号処理のためのハードウェアアクセラレーション機構が提供される。この要件は 03.13.11 に関連する。

参考文献

ソース・コントロール CP-09、CP-09(08)

サポート出版物 SP 800-34[52]、SP 800-130[53]、SP 800-152[54]。

3.9. 職員のセキュリティ

03.09.01 人事選考

a. システムへのアクセスを認可する前に、個人を選別する。

b. 再選考を必要とする組織定義の条件]に従って、個人を再選考する。

ディスカッション

職員のセキュリティ・スクリーニング活動には、システムへのアクセスを認可する前、またはシステ ム・アクセスを昇格させる前に、個人の行動、誠実さ、判断力、忠誠心、信頼性、安定性（すなわち、個 人の信頼性）を評価することが含まれる。スクリーニングおよび再スクリーニング活動は、適用される連邦法、大統領令、 指令、方針、規則、および割り当てられた職務に必要なアクセス・レベルに対して設定された基準を反映 する。

参考文献

ソース・コントロール PS-03

サポート出版物 SP 800-181 [34]

03.09.02 職員の解雇および異動

a. 個人の雇用が終了した場合：

   1. 割り当て：組織が定義した期間]内にシステムアクセスを無効にする、

   2. 個人に関連付けられた認証およびクレデンシャルを停止または取り消す。

   3. セキュリティ関連のシステムプロパティを取得する。

b. 個人が組織内の他のポジションに配置転換または異動される場合：

   1. システムおよび施設に対する現行の論理的および物理的アクセス認可の継続的な運用上の必要性を検討し、確認する。

2. 運用上の必要性の変化に応じて、アクセス認可を変更する。

ディスカッション

セキュリティ関連のシステム財産には、ハードウェア認証トークン、シス テム管理技術マニュアル、鍵、ID カード、ビルパスが含まれる。退社時の面談では、退社した個人が、元従業員であることによって課されるセキュリテ ィ上の制約を理解し、組織の財産に対する説明責任が達成されるようにする。退 職者面談におけるセキュリティの話題には、将来の雇用や非開示契約に対する潜在的な 制約を個人に思い出させることが含まれる。退社面談は、上司の不在、病気、職務放棄に関連する場合を含め、個人によっては常に可能であるとは限らない。

理由があって解雇された個人には、解雇アクションをタイムリーに実行することが不可欠である。組織は、解雇される個人に通知する前に、解雇される個人のアカウントを無効にすることを検討してもよい。この要件は、人事措置が永続的である場合、または保護が必要なほど期間が延長される場合に、個人の配置転換または異動に適用される。組織内の他の職位への異動または再任に必要とされる保護には、古い身分証明書、鍵、およびビ ルパスの返却と新しい発行、システムアクセス認可（すなわち、特権）の変更、システムア カウントの閉鎖と新しいアカウントの確立、以前のシステムアカウントで以前の職場で個人がア クセスしていた公式記録へのアクセスの提供などが含まれる。

参考文献

ソース・コントロール：PS-04、PS-05

サポート出版物：なし

3.10. 物理的保護

03.10.01 物理的アクセス認可

a. システムが存在する施設へのアクセスを認可された個人のリストを作成し、承認し、維持する。

b. 施設にアクセスするための認可クレデンシャルを発行する。

c. 施設アクセスリスト[割り当て：組織が定義した頻度]を見直す。

d. アクセスが不要になった場合、施設アクセスリストから個人を削除する。

ディスカッション

施設は、CUI を処理、保管、または伝送するシステムまたはシステム・コンポーネントを含む 1 つ以上の物理的な場所を含むことができる。物理的アクセス認可は、従業員および訪問者に適用される。永続的な物理的アクセス認可クレデンシャルを持つ個人は、訪問者とはみなされない。認可クレデンシャルには、ID バッジ、ID カード、およびスマート・カードが含まれる。組織は、適用法、大統領令、指令、規制、ポリシー、標準、およびガイドラインに準拠して認可クレデン シャルの強度を決定する。物理的なアクセス認可は、一般にアクセス可能であると指定されている施設内の特定のエリアへの アクセスには必要ない場合がある。

参考文献

ソース・コントロール PE-02

サポート出版物：なし

03.10.02 物理的アクセスの監視

a. システムが存在する施設への物理的アクセスを監視し、物理的セキュリティインシデントを検知し対応する。

b. 物理的アクセスログを[割り当て：組織が定めた頻度]で、かつ[割り当て：組織が定めた事象または事象の潜在的兆候]が発生した時点でレビューする。

ディスカッション

施設は、CUI を処理、保管、または伝送するシステムまたはシステム・コンポーネントを含む 1 つ以上の物理的な場所を含むことができる。物理的アクセス監視には、組織施設内の公にアクセス可能な区域が含まれる。物理的アクセス監視の例には、警備員、ビデオ監視装置（すなわち、カメラ）、およびセンサー装置が含まれる。物理的アクセスログをレビューすることは、不審な活動、異常な事象、または潜在的な脅威を 識別するのに役立つ。アクセスログが自動化されたシステムの一部である場合、このレビューは監査ログ管理によってサポートされる。インシデント対応機能には、物理的セキュリティインシデントの調査およびインシデントへの対応が含まれる。インシデントには、通常の勤務時間外のアクセス、通常アクセスされないエリアへの繰り返し のアクセス、異常な長時間のアクセス、連続しないアクセスなど、セキュリティ違反や不審な物理 的アクセス活動が含まれる。

参考文献

ソース・コントロール PE-06

サポート出版物：なし

03.10.03 削除

03.10.07 に組み込んだ。

03.10.04 削除

03.10.07 に組み込んだ。

03.10.05 削除

03.10.07 に組み込んだ。

03.10.06 代替作業現場

a. 従業員が使用できる代替作業場所を決定する。

b. 代替作業現場において、以下のセキュリティ要件を採用する： [課題：組織が定義したセキュリティ要件]。

ディスカッション

代替作業場所には、従業員の私邸や、組織が指定したその他の施設が含まれる。代替作業現場は、有事作戦中に容易に利用できる代替場所を提供することができる。組織は、特定の代替作業場所や作業場所の種類に対して、その場所で行われる業務関連の活動に応じて、異なるセキュリティ要件を定義することができる。要件の有効性を評価し、代替作業場所でのインシデントを伝える手段を提供することは、組織の緊急時計画活動を支援する。

参考文献

ソース・コントロール PE-17

サポート出版物 SP 800-46［14]、SP 800-114［20]。

03.10.07 物理的アクセス管理

a. システムが存在する施設への出入り口において、以下の方法により物理的なアクセス認可を実施する：

   1. 施設へのアクセスを許可する前に、個々の物理的アクセス認可を検証すること。

   2. 物理的なアクセス管理システム、装置、または警備員を使って出入りを管理すること。

b. 出入口の物理的アクセス監査ログを維持すること。

c. 訪問者をエスコートし、訪問者の行動を管理する。

d. 安全な鍵、組み合わせ、その他の物理的アクセス装置。

e. 権限のない個人が CUI にアクセスできないよう、出力機器への物理的アクセスを管理する。

ディスカッション

この要件は、CUI を処理、保管、または伝送するシステムまたはシステム・コンポーネントを含む物理的な場所を対象とする。組織は、専門のセキュリティ・スタッフまたは管理スタッフを含め、必要な警備員のタイプを決定する。物理的アクセス装置には、鍵、ロック、組み合わせ、バイオメトリック・リーダ、カード・リーダが含まれる。物理的アクセス管理システムは、適用法、大統領令、指令、方針、規制、標準、およびガ イドラインに準拠する。組織は、採用する監査ログの種類に柔軟性がある。監査ログは、手続き的なもの、自動化されたもの、またはそれらを組み合わせたものである。物理的アクセスポイントには、外部アクセスポイント、補足的アクセス管理を必要とするシステ ムへの内部アクセスポイント、またはその両方が含まれる。物理的アクセス管理は、従業員および訪問者に適用される。永続的な物理的アクセス認可を持つ個人は、訪問者とはみなされない。

出力機器への物理的アクセスを管理することとしては、キーパッドまたはカードリーダーによるアクセス制御を備えた施錠された部屋またはその他の安全な区域に出力機器を設置し、認可された個人のみにアクセスを許可すること、職員が監視できる場所に出力機器を設置すること、モニターまたはスクリーンフィルターを設置すること、およびヘッドホンを使用することが挙げられる。出力機器の例としては、モニター、プリンター、スキャナー、ファクシミリ、オーディオ機器、コピー機などがある。

参考文献

ソース・コントロール PE-03、PE-05

サポート出版物：なし

03.10.08 送信のアクセス管理

組織施設内のシステム配電線および送電線への物理的アクセスを管理する。

ディスカッション

システムの配電線や送電線に適用される保護措置は、偶発的な損傷、混乱、物理的な改ざんを防ぐ。このような対策は、盗聴や暗号化されていない伝送の改ざんを防ぐためにも必要な場合がある。システムの配電線および送電線への物理的アクセスを管理するために使用される保護

手段には、切断または施錠された予備ジャック、施錠された配線クロゼット、電線管またはケーブルトレイによる配線保護、盗聴センサーなどがある。

参考文献

ソース・コントロール PE-04

サポート出版物：なし

3.11. リスクアセスメント

03.11.01 リスクアセスメント

a. CUI の処理、保管、送信に起因する不正開示のリスク（サプライチェーンリスクを含む）をアセスメントする。

b. リスクアセスメントを更新する［割り当て：組織が定めた頻度］。

ディスカッション

システム境界の確立は、CUI の不正開示のリスクをアセスメントするための前提条件である。リスクアセスメントは、システムの運用及び使用、並びに CUI の不正な開示に基づき、組織の運用及び資産に対する脅威、脆弱性、可能性、及び悪影響を考慮する。リスクアセスメントは、外部の関係者（例えば、組織のためにシステムを運用する請負業者、サービスプロバイダー、システムにアクセスする個人、アウトソーシング事業体）からのリスクも考慮する。リスクアセスメントは、組織レベル、ミッション又はビジネスプロセ スレベル、システムレベル、及びシステム開発ライフサイクルのどの段階においても 実施することができる。リスクアセスメントには、供給業者又は請負業者及びそれらが提供するシステム、シス テムコンポーネント又はシステムサービスに関連するサプライチェーンに関連するリ スクが含まれる。

参考文献

ソース・コントロール RA-03、RA-03(01)、SR-06

サポート出版物 SP 800-30[55]、SP 800-161[33]。

03.11.02 脆弱性の監視とスキャン

a. システムの脆弱性を監視し、スキャンする [識別*:* 組織が定義した頻度]。

b. システムの脆弱性を[課題*:* 組織が定義した対応時間]以内に是正する。

c. システムの脆弱性をスキャン対象として更新する [識別*:* 組織が定義した頻度]、および新しい脆弱性が識別され報告されたときに更新する。

ディスカッション

組織は、システム構成要素に必要な脆弱性スキャンを決定し、脆弱性の潜在的な発生源（ネットワーク接続されたプリンタ、スキャナ、コピー機など）を見落とさないようにする。カスタムソフトウエアの脆弱性分析には、静的分析、動的分析、バイナリ分析などの追加アプローチが必要になる場合がある。組織は、ソースコードレビューやツール（例えば、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、バイナリアナライザ）において、これらのアプローチを使用することができる。脆弱性スキャンには、パッチレベルのスキャン、ユーザーやデバイスがアクセスすべきでない機能、ポート、プロトコル、サービスのスキャン、不適切に設定された、あるいは不正に動作するフロー制御メカニズムのスキャンが含まれる。

相互運用性を促進するために、組織は、脆弱性を CVE（Common Vulnerabilities and Exposures）の命名規則で表現するスキャン・ツールの使用を検討する。脆弱性情報の情報源としては、Common Weakness Enumeration（CWE）リスト、National Vulnerability Database（NVD）、Common Vulnerability Scoring System（CVSS）などもある。

参考文献

ソース・コントロール RA-05、RA-05(02)

サポート出版物 SP 800-40[56]、SP 800-53A[57]、SP 800-70[44]、SP 800-115[58]、SP 800-126[45]。

03.11.03 削除

03.11.02 に組み込んだ。

03.11.04 リスク対応

セキュリティ評価、監視、監査から得られた結果に対応する。

ディスカッション

この要件は、行動計画およびマイルストーン（POAM）項目を生成する前に、 リスクに対する適切な対応策を決定する必要性に対処するものである。POAM 項目が必要ないように、リスクを直ちに低減することが可能な場合もある。しかし、リスクへの対応が識別されたリスクを軽減することであり、その軽減が直ちに完了できない場合には、POAM 項目が生成される。

参考文献

ソース・コントロール RA-07

サポート出版物 SP 800-30［55］、SP 800-37［59］、SP 800-39［60］、SP 800-1601［11］。

3.12. セキュリティ評価と監視

03.12.01 セキュリティ・アセスメント

システム及びその運用環境のセキュリティ要件を評価し、要件が満たされて いるかどうかを判断する［課題：組織が定めた頻度］。

ディスカッション

セキュリティ要件を評価することによって、組織は、必要な保護措置や対策が正しく実装され、意図したとおりに運用され、望ましい結果を生み出しているかどうかを判断する。セキュリティアセスメントは、システムの弱点を特定し、リスクに基づく意思決定に必要な識別情報を提供する。セキュリティアセスメント報告書は、報告書の正確性と完全性を判断するために組織が必要と判断した十分な詳細さで、アセスメント結果を文書化する。セキュリティアセスメントの結果は、実施するアセスメントの種類に適した個人または役割にプロバイダされる。

参考文献

ソース・コントロール CA-02

サポート出版物 SP 800-53[8]、SP 800-53A[57]、SP 800-37[59]、SP 800-115[58]。

03.12.02 行動計画とマイルストーン

a. システムの行動計画とマイルストーンを策定する：
    1. セキュリティ評価で指摘された弱点や欠陥を是正するために計画した是正措置を文書化する。
    2. 既知のシステム脆弱性を低減または排除する。
b. の調査結果に基づき、既存の行動計画とマイルストーンを更新する：
    1. セキュリティ評価、
    2. 監査またはレビュー
    3. 継続的な監視活動。

ディスカッション

行動計画とマイルストーン（POAM）は、組織の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 POAM を使用して、満たされていないセキュリティ要 件をどのように満たすか、計画した低減策をどのように実施するかを記述する。組織は、システムセキュリティ計画と POAM を、別個の文書として、または組み合わせた文書として、どのような形式でも文書化することができる。連邦機関は、連邦機関以外がホストするシステム上で CUI を処理、保管、または伝送するかどうかに関するリスク・ベースの決定のインプットとして、システム・セキュリティ計画および POAM を考慮することができる。

参考文献

ソース・コントロール CA-05

サポート出版物 SP 800-37 [59]

03.12.03 継続的モニタリング

継続的な監視とセキュリティ評価を含む、システムレベルの継続的なモニタリング戦略を策定し、実施する。

ディスカッション

システムレベルの継続的なモニタリングは、リスクマネジメントの意思決定を支援するために、システ ムのセキュリティ状況を継続的に認識することを容易にする。継続的かつ継続的という用語は、組織がリスクベースの意思決定を支援するのに十分な頻度でシステムをアセスメントし、監視することを意味する。セキュリティ要件の種類によって、必要な監視頻度が異なる場合がある。

参考文献

ソース・コントロール CA-07

サポート出版物 SP 800-37[59]、SP 800-39[60]、SP 800-53A[57]、SP 800-115[58]、SP 800-137[49]。

03.12.04 削除

03.15.02 に組み込んだ。

03.12.05 情報交換

a. 選択（*1* つ以上）：相互接続セキュリティ合意書、情報交換セキュリティ合意書、覚書または合意書、サービスレベル合意書、ユーザ合意書、非開示合意書、その他の種類の合意書]を使用して、システムと他のシステムとの間の CUI の交換を承認し、管理する。

b. 交換契約の一部として、各システムのインターフェイス特性、セキュリティ要件、責任を文書化する。

c. 交換契約を見直し、更新する［担当業務：組織の定める頻度］。

ディスカッション

情報交換は、組織の内外を問わず、2 つ以上のシステム間の情報交換に適用される。組織は、セキュリティ要件やポリシーが異なる可能性のある他のシステムとシステ ムが情報を交換する際に生じる、新たな脅威や脅威の増大に関するリスクを考慮する。選択される協定の種類は、情報を交換する組織間の関係（政府対政府、企業対企業、政府対企業、政府または企業、政府または企業対個人など）や、他のシステムのユーザによる組織システムへのアクセスレベルなどの要因に基づいている。協定の種類には、情報交換セキュリティ協定、相互接続セキュリティ協定、覚書または合意書、サービスレベル協定、または他の種類の協定を含めることができる。

組織は、特に連邦機関と連邦機関以外の組織（サービスプロバイダー、請負業者、シ ステム開発者、システムインテグレーターなど）との間で確立された情報交換につい て、合意情報を正式な契約に組み込むことができる。交換契約に含まれる情報の種類には、各システムのインターフェイス特性、セキュ リティ要件、管理、および責任が含まれる。

参考文献

ソース・コントロール CA-03

サポート出版物 SP 800-47 [83]

3.13. システムおよび通信の保護

03.13.01 境界の保護

a. システムに対する外部管理インターフェイスおよびシステム内の主要な内部管理インターフェイスにおけるコミュニケーションを監視および制御する。

b. 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、一般にアクセス可能なシステムコンポーネント用にサブネットワークを実装する。

c. 外部システムとの接続は、組織のセキュリティ・アーキテクチャに従って配置された境界保護デバイスで構成される、管理されたインターフェイスを介してのみ行う。

ディスカッション

管理されたインターフェースには、ゲートウェイ、ルーター、ファイアウォール、ネットワーク・ベースの悪質コード分析、仮想化システム、セキュリティ・アーキテクチャ内に実装された暗号化トンネルなどがある。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、非武装地帯または DMZ と呼ばれる。組織システム内のインタフェースを制限または禁止することには、外部ウェブトラフィックを管理インタフェース内の指定ウェブサーバに制限すること、内部アドレスを偽装していると思われる外部トラフィックを禁止すること、外部アドレスを偽装していると思われる内部トラフィックを禁止することなどが含まれる。

参考文献

ソース・コントロール SC-07

サポート出版物 SP 800-41[64]、SP 800-125B[65]、SP 800-160-1[11]、SP 800-189[67]、SP 800-207[66]。

03.13.02 削除

下士官に再分類された。

03.13.03 削除

03.01.01、03.01.02、03.01.03、03.01.04、03.01.05、03.01.06、03.01.07 で扱う。

03.13.04 共有システムリソース内の情報

共有システムリソースを介した、不正で意図しない情報転送を防止する。

ディスカッション

共有システムリソースを介した不正かつ意図しない情報転送を防止することで、以前のユーザーまたはロール（または以前のユーザーまたはロールの代理を務めるプロセス）の行為によって生成された情報を、リソースがシステムに解放された後に共有システムリソースへのアクセスを取得した現在のユーザーまたはロール（または現在のユーザーまたはロールの代理を務める現在のプロセス）が利用できるようにする。共有システムリソース内の情報は、暗号化された情報表現にも適用される。他の文脈では、共有システムリソース内の情報の制御は、オブジェクトの再利用および残留情報の保護と呼ばれる。共有システムリソース内の情報は、名目上

削除されたデータの残存表現、情報フロー制限に違反するために共有システムリソースが操作される秘密チャネル（ストレージチャネルやタイミングチャネルを含む）、単一ユーザーまたは単一ロールしか存在しないシステム内のコンポーネントを指す、情報の残存には対処しない。

参考文献

ソース・コントロール SC-04

サポート出版物：なし

03.13.05 削除

03.13.01 に組み込んだ。

03.13.06 ネットワークコミュニケーション - デフォルトで拒否 - 例外で許可

デフォルトでネットワーク・コミュニケーション・トラフィックを拒否し、例外的にネットワーク・コミュニケーション・トラフィックを許可する。

ディスカッション

この要件は、システム境界およびシステム内の識別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・コミュニケーション・トラフィックに適用される。ネットワーク・コミュニケーション・トラフィック・ポリシーでは、必要かつ承認された接続のみが許可されるようにする。

参考文献

ソース・コントロール SC-07(05)

サポート出版物 SP 800-41[64]、SP 800-77[18]、SP 800-189[67]。

03.13.07 削除

03.01.12、03.04.02、03.04.06 で扱われている。

03.13.08 送信および保管の機密性

送信中および保管中の CUI の不正な開示を防止するための暗号化メカニズムを導入する。

ディスカッション

この要件は、内部および外部ネットワークと、サーバー、ノートブック・コンピューター、デスクトップ・コンピューター、モバイル・デバイス、プリンター、コピー機、スキャナー、フ

ァクシミリ、無線機など、CUI を送信できるあらゆるシステム・コンポーネントに適用される。保護されていないコミュニケーション経路は、傍受や改ざんの影響を受けやすい。暗号化は、送信中および保管中の不正な開示から CUI を保護する。送信中の CUI の機密性を保護する暗号化メカニズムには、TLS および IPsec が含まれる。保管中の情報（すなわち、静止状態の情報）とは、CUI が処理中または転送中でないときの CUI の状態を指し、内部または外部のストレージ・デバイス、ストレージ・エリア・ネットワーク・デバイス、およびデータベースに存在する。ストレージ内の CUI の保護は、ストレージ・デバイスのタイプやそのデバイスへのアクセス頻度ではなく、むしろ情報の状態に焦点を当てる。この要件は 03.13.11 に関連する。

参考文献

ソース・コントロール SC-08、SC-08(01)、SC-28、SC-28(01)

サポート出版物 FIPS 140-3 [38], FIPS 197 [68], SP 800-46 [14], SP 800-52 [69], SP 800-56A [73], SP 800-56B [74], SP 800-56C [75], SP 800-57-1 [15], SP 800-57-2 [16]、sp 800-57-3 [17]、sp 800-77 [18]、sp 800-111[51]、sp 800-113[19]、sp 800-114[20]、sp 800-121[21]、sp 800-124[28]、sp 800-177[70]。

03.13.09 ネットワーク切断

セッションの終了時、または[割り当て*:* 組織が定義した期間]非アクティブになった後に、コミュニケーションセッションに関連付けられたネットワーク接続を終了する。

ディスカッション

この要件は、内部および外部ネットワークに適用される。コミュニケーション・セッションに関連するネットワーク接続の終了には、オペレーティング・システム・レベルで TCP/IP アドレスまたはポート・ペアの割り当てを解除すること、または複数のアプリケーション・セッションが単一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割り当てを解除することが含まれる。非アクティブの時間帯は、組織によって設定されることがあり、ネットワーク・アクセスのタイプ別または特定のネットワーク・アクセスの時間帯を含む。

参考文献

ソース・コントロール SC-10

サポート出版物：なし

03.13.10 暗号鍵の確立と管理

以下の鍵管理要件に従って、システム内の暗号鍵を確立し、管理する：*[*割り当て：鍵の生成、配布、保管、アクセス、破棄に関する組織定義の要件]。

ディスカッション

暗号鍵は、手動の手順または手動の手順をサポートする自動化されたメカニズムのいずれかを使用して確立および管理することができる。組織は、適用される連邦法、大統領令、適切なオプション、レベル、パラメー タを規定するポリシー、指令、標準に従い、鍵確立および管理の要件を満たす。この要件は、03.13.11 に関連する。

参考文献

ソース・コントロール SC-12

サポート出版物 FIPS 140-3[38]、SPA 800-56A[73]、SPA 800-56B[74]、SPA 800-56C[75]、SPA 800-57-1[15]、SPA 800-57-2[16]、SPA 800-57-3[17]、SPA 800-63-3[27]。

03.13.11 暗号保護

CUI の機密性を保護するために、以下のタイプの暗号を実装する：*[*課題：組織で定義された暗号の種類]。

ディスカッション

暗号は、適用法、大統領令、指令、規制、方針、標準、およびガイドラインに従って実装される。CUI の保護には、FIPS Validated 暗号が推奨される。

参考文献

ソース・コントロール SC-13

サポート出版物 FIPS 140-3 [38]

03.13.12 コラボレーティブ・コンピューティング・デバイスとアプリケーション

a. 以下の例外を除き、コラボレーションコンピューティングデバイスおよびアプリケーションのリモートアクティベーションを禁止する：*[*割り当て：リモート起動が許可される組織定義の例外]。

b. 機器に物理的に居合わせた利用者に、利用を明示する。

ディスカッション

協働コンピューティング機器には、ホワイトボード、マイク、カメラが含まれる。会議ソフトウェアが使用されている場合、カメラおよびマイクを含むノートブックコンピュータ、スマートフォン、ディスプレイモニター、およびタブレットは、共同コンピューティングデバイスの一部とみなされる。使用の表示には、共同コンピューティングデバイスが起動されたときに、ユーザーに通知すること（録画中であることやマイクがオンになったことを示すポップアップメニューなど）が含まれる。専用ビデオ会議システムは、通常、参加者の一人がビデオ会議を起動するために相手方に電話をかけるか接続することに依存するため、除外される。デバイスの使用を防ぐ解決策としては、ウェブカメラのカバーやマイクを無効にするボタンなどがある。

参考文献

ソース・コントロール SC-15

サポート出版物：なし

03.13.13 モバイルコード

a. 許容されるモバイルコードとモバイルコード技術を定義する。

b. モバイルコードの使用を認可、監視、管理する。

ディスカッション

モバイルコードには、リモートシステムから取得され、ネットワークを介して送信され、取得者が明示的にインストールまたは実行することなくローカルシステム上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一部が含まれる。モバイルコードの使用に関する決定は、コードが悪意を持って使用された場合にシステムに損害を与える可能性に基づいて行われる。モバイルコードの技術には、Java アプレット、JavaScript、HTML5、VBScript、WebGL が含まれる。使用制限と実装ガイドラインは、サーバーにインストールされ、個々のワークステーションやデバイス（ノートブック・コンピューター、スマートフォン、スマートデバイスを含む）にダウンロードされ実行されるモバイルコードの選択と使用に適用される。モバイルコードのポリシーと手順は、システム内で容認できないモバイルコードの開発、取得、使用を防止するために取られる措置に対処するもので、これには、モバイルコードが信頼できるソースによってデジタル署名されていることを要求することも含まれる。

参考文献

ソース・コントロール SC-18

サポート出版物 SP 800-28 [71]

03.13.14 削除

技術に特化している。

03.13.15 セッション認証

通信セッションの認証を保護する。

ディスカッション

セッションの認証の保護は、パケットレベルではなく、セッションレベルでの通信の保護に取り組む。このような保護は、通信セッションの両端において、相手の継続的な身元と送信された情報の正当性を信頼する根拠を確立する。認証の保護には、中間者攻撃、セッション・ハイジャック、およびセッションへの偽情報の挿入に対する保護が含まれる。

参考文献

ソース・コントロール SC-23

サポート出版物 SP 800-52[69]、SP 800-77[18]、SP 800-95[72]、SP 800-113[19]。

03.13.16 削除

03.13.08 に組み込んだ。

3.14. システムおよび情報の完全性

03.14.01 欠陥の修復

a. システムの欠陥を識別し、報告し、修正する。

b. セキュリティに関連するソフトウエアとファームウ ェアのアップデートを、アップデートがリリースさ れてから「割り当て：組織で定義した期間」内にインストー ルする。

ディスカッション

組織は、発表されたソフトウェアやファームウェアの欠陥の影響を受けるシステムを特定し、それらの欠陥に起因する潜在的脆弱性を含め、情報セキュリティの責任を負う指定要員にその情報を報告する。セキュリティ関連の更新には、パッチ、サービスパック、ホットフィックス、アンチウイルス署名が含まれる。組織は、セキュリティの評価、継続的なモニタリング、インシデント対応活動、システ ムエラーハンドリングにおいて発見された欠陥に対処する。シ

ステムの欠陥を是正する際に、利用可能なリソース（CWE や CVE データベースなど）を活用できる。セキュリティに関連するソフトウェアとファームウェアをアップデートするための組織定義の期 間は、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重大性）を含む、 様々な要因に基づいて変化する可能性がある。欠陥の是正の種類によっては、他の種類よりも多くのテストを必要とする場合がある。

参考文献

ソース・コントロール SI-02

サポート出版物 SP 800-39［60］、SP 800-40［56］、SP 800-128［41］。

03.14.02 悪意のあるコードの保護

a. システムの入口と出口に悪意のあるコード保護メカニズムを実装し、悪意のあるコードを検知して根絶する。

b. 構成管理ポリシーと手順に従い、新しいリリースが利用可能になると、悪意のあるコード保護メカニズムを更新する。

c. 悪意のあるコード保護メカニズムを設定する：

   1. ファイルのダウンロード、オープン、または実行時に、エンドポイントまたはシステムの出入口で、システムのスキャン [割り当て*:* 組織が定義した頻度]、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を実行する。

   2. 悪意のあるコードの検知に応じて、悪意のあるコードをブロック、隔離、またはその他の低減措置を講じる。

ディスカッション

悪意のあるコードの挿入は、システムの脆弱性を悪用することで発生する。悪意のあるコードは、電子メール、インターネット、ポータブル・ストレージ・デバイスなど、さまざまな方法でシステムに挿入される可能性がある。悪意のあるコードには、ウイルス、ワーム、トロイの木馬、スパイウェアなどがある。悪意のあるコードは、さまざまな形式でエンコードされたり、圧縮ファイルや隠しファイルに含まれたり、ステガノグラフィなどの技術を使ってファイルに隠されたりする。悪意のあるコードは、市販のソフトウェアやカスタムメイドのソフトウェアに存在する可能性があり、論理爆弾、バックドア、組織のミッションやビジネス機能に影響を及ぼす可能性のある他のタイプの攻撃を含む可能性がある。システムの定期的なスキャンや、ファイルがダウンロードされたり、開かれたり、実行されたりする際に、外部ソースから

のファイルをリアルタイムでスキャンすることで、悪意のあるコードを検知することができる。また、悪意のあるコード保護メカニズムは、異常な動作や予期せぬ動作についてシステムを監視し、適切な措置を講じることもできる。

悪意あるコードの保護技術には、シグネチャベースの技術と非シグネチャベースの技術がある。非シグネチャベースの検知メカニズムには、悪意のあるコードの特徴や動作を検知、分析、記述し、シグネチャがまだ存在しない、または既存のシグネチャが有効でない可能性のあるコードに対する制御を提供するためにヒューリスティックを使用する人工知能技術が含まれる。アクティブなシグネチャがまだ存在しない、あるいは有効でない可能性のある悪意のあるコードには、ポリモーフィックな悪意のあるコード（複製時にシグネチャを変更するコード）が含まれる。非シグネチャ・ベースのメカニズムには、レピュテーション・ベースの技術が含まれる。不正なコードの実行を防ぐには、浸透した構成管理、悪用防止ソフトウエア、ソフトウエアの完全性制御も効果的な場合がある。

悪意のあるコードが検知方法や技術によって検知できない場合、組織は、ソフトウェアが意図した機能のみを実行することを確実にするために、安全なコーディングの実践、構成管理と制御、信頼できる調達プロセス、および監視の実践に頼ることができる。組織は、悪意のあるコードの検知に応じて、異なる対応が正当化されると判断することができる。例えば、組織は、スキャン中に悪意のあるコードが検知された場合、悪意のあるダウンロードが検知された場合、またはファイルを開こうとしたり実行しようとしたときに悪意のあるアクティビティが検知された場合に取るべきアクションを定義することができる。

参考文献

ソース・コントロール SI-03

サポート出版物 SP 800-83[76]、SP 800-125B[65]、SP 800-177[70]。

03.14.03 セキュリティ警告、勧告、指令

a. 外部組織からのシステムセキュリティ警告、勧告、指示を継続的に受信する。

b. 必要に応じて、内部システムのセキュリティ警告、勧告、指令を生成し、周知する。

ディスカッション

システム・セキュリティに関する警告や勧告の情報源は数多く公開されている。

国土安全保障省のサイバーセキュリティ・インフラセキュリティ庁（CISA）、国家安全保障局（NSA）、連邦捜査局（FBI）は、連邦政府全体および連邦政府以外の組織の状況認識を維持す

るために、セキュリティ・アラートとアドバイザリを生成している。ソフトウェア・ベンダー、サブスクリプション・サービス、業界の情報共有・分析センター（ISAC）もセキュリティ・アラートとアドバイザリーを提供することがある。セキュリティ指令の遵守は、これらの指令の多くが重要な性質を持ち、指令が適時に実施されなけ れば、組織の運営や資産、個人、他の組織、国家に直ちに悪影響を及ぼす可能性があるため、 不可欠である。

参考文献

ソース・コントロール SI-05

サポート出版物 SP 800-161 [33]

03.14.04 削除

03.14.02 に組み込んだ。

03.14.05 削除

03.14.02 までに対応する。

03.14.06 システム・モニタリング

a. システムを監視して検知する：

   1. 攻撃と潜在的な攻撃の指標

   2. 不正な接続。

b. システムの不正使用を識別する。

c. インバウンドおよびアウトバウンドのコミュニケーション・トラフィックを監視し、異常または不正な活動や状況を検知する。

ディスカッション

システム・モニタリングには、外部モニタリングと内部モニタリングがある。内部モニタリングには、システム内部で発生する事象の観察が含まれる。外部モニタリングには、システム境界で発生するイベントの観察が含まれる。組織は、監査記録の活動をリアルタイムで観察することによって、またはアクセスパターン、アク セスの特徴、その他のアクションなどの他のシステム側面を観察することによって、システムを監視 することができる。監視目的は、事象の決定の指針となる。

システム監視能力は、様々なツールや技術（例えば、監査記録監視ソフトウェア、侵入検知システム、侵入防止システム、悪意のあるコード保護ソフトウェア、スキャンツール、ネットワ

ーク監視ソフトウェア）によって達成される。モニタリング・デバイスの戦略的な場所としては、選択された境界の場所や、重要なアプリケーションをサポートするサーバー・ファームの近くがあり、管理されたシステム・インターフェースにそのようなデバイスが採用されている。収集される情報の監視の粒度は、組織の監視目的と、そのような目的をサポートするシステムの能力に基づいている。

システム接続には、ネットワーク接続、リモート接続、ローカル接続がある。ネットワーク接続とは、ネットワーク（ローカルエリアネットワーク、インターネットなど）を通じてコミュニケーションするデバイスとの接続のことである。リモート接続とは、外部ネットワーク（インターネットなど）を通じてコミュニケーションするデバイスとの接続のことである。ネットワーク接続、リモート接続、ローカル接続は、有線でも無線でも構わない。

インバウンドおよびアウトバウンドのコミュニケーション・トラフィックに関連する異常または不正な活動または状態には、システム内に悪意のあるコードが存在するか、システム・コンポーネント間で伝播していること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シグナリングが含まれる。悪意のあるコードの識別は、潜在的に侵害されたシステムを識別するために使用される。システム監視の種類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ことがある。

参考文献

ソース・コントロール Si-04、Si-04(04)

サポート出版物 SP 800-61[47]、SP 800-83[76]、SP 800-92[35]、SP 800-94[29]、SP 800-137[49]、SP 800-177[70]。

03.14.07 削除

03.14.06 に組み込んだ。

03.14.08 情報管理と保持

適用法、大統領令、指令、規制、方針、標準、ガイドライン、および運用要件に従って、システム内の CUI およびシステムから出力される CUI を管理し、保持する。

ディスカッション

連邦機関は、非連邦組織に対するデータ保持要件を検討する。契約または協定が終了した後も連邦政府以外のシステム上に CUI を保持することは、それらのシステムの攻撃対象領域を拡大

し、情報が漏洩するリスクを増大させる。NARA は、記録保持およびスケジュールに関する連邦政策およびガイダンスを提供する。

参考文献

ソース・コントロール SI-12

サポート出版物：なし

3.15. 計画

03.15.01 方針と手続き

a. CUI の保護に関するセキュリティ要件を満たすために必要な方針および手順を策定し、文書化し、組織の要員または役割に周知する。

b. 方針および手順を見直し、更新する［担当業務：組織で定める頻度］。

ディスカッション

この要件は、CUI を保護するための方針および手順を扱う。ポリシーおよび手順は、セキュリティ保証に貢献し、CUI セキュリティ要件の各ファミリに対応する必要がある。ポリシーは、組織のセキュリティ・ポリシーの一部として含めることも、セキュリティ要件の各ファミリーに対応する個別のポリシーで代表することもできる。手順は、ポリシーをどのように実施するかを記述するものであり、手順の対象である個人または役割を対象とすることができる。手順は、システムセキュリティ計画に文書化することも、1 つまたは複数の個別の文書に文書化することもできる。

参考文献

ソース・コントロール AC-01、AT-01、AU-01、CA-01、CM-01、IA-01、IR-01、MA-01、MP-01、PE-01、PL-01、PS-01、RA-01、SA-01、SC-01、Si-01、SR-01

サポート出版物 SP 800-12[61]、SP 800-100[62]。

03.15.02 システム・セキュリティ計画

a. 次のようなシステム・セキュリティ計画を策定する：

1. システムの構成要素を定義する；
2. システムによって処理、保存、伝送される情報の種類を識別する；
3. 組織にとって懸念される、システムに対する具体的な脅威を記述する；

4. システムの運用環境と、他のシステムまたはシステムコンポーネントへの依存関係または接続を記述する；
5. システムのセキュリティ要件の概要を提供する；
6. セキュリティ要求事項を満たすために実施されている、または計画されている保護手段を記述する；
7. システムの役割と責任を果たす個人を識別する。
8. CUI の保護に必要なその他の関連情報を含む。

b. システムセキュリティ計画をレビューし，更新する [担当者*:* 組織が定めた頻度]。

c. システムのセキュリティ計画を不正な開示から保護する。

ディスカッション

システム・セキュリティ計画は、CUI を処理、保存、送信するシステムの主要な特性、およびシステムおよび情報がどのように保護されるかを提供する。システムセキュリティ計画は、計画の意図及び計画が意図されたとおりに実施された場合のその後のリスクの決定に明確に適合する設計及び実施を可能にするのに十分な情報を含む。システムセキュリティ計画は、既に存在する文書も含めて、文書の集合体とすることができる。効果的なシステムセキュリティ計画は、追加的な詳細情報を提供する方針、 手順、文書（設計仕様書など）を参照する。これにより、セキュリティプログラムに関連する文書化要件が軽減され、エ ンタープライズアーキテクチャ、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、取得に関連する他の確立された管理領域または運用領域において、セ キュリティ情報が維持される。

参考文献

ソース・コントロール PL-02

サポート出版物 SP 800-18 [63]

03.15.03 行動規則

a. システムの使用と CUI の保護に関する責任と期待される行動を記述したルールを確立する。

b. システムへのアクセスを必要とする個人にルールを提供する。

c. CUI およびシステムへのアクセスを認可する前に、行動規範を読み、理解し、遵守することに同意することを示す文書化された確認書を個人から受領すること。

d. 行動規範を見直し、更新する［担当業務：組織が定める頻度］。

ディスカッション

行動規則は、システム・ユーザーに対するアクセス協定の一種である。

組織は、個々のユーザーの役割と責任に基づいて、CUI の取り扱いに関する行動ルールを検討し、特権ユーザーに適用されるルールと一般ユーザーに適用されるルールを区別する。

参考文献

ソース・コントロール PL-04

サポート出版物 SP 800-18 [63]

3.16. システムおよびサービスの取得

03.16.01 セキュリティ工学の原則

システム及びシステムコンポーネントの開発又は変更に、以下のシステムセ キュリティ工学の原則を適用する：*[*課題：組織で定義されたシステムセキュリティ工学の原則]を適用する。

ディスカッション

組織は、新規開発システムにシステムセキュリティ工学の原則を適用する。レガシーシステムについては、ハードウェア、ソフトウエア、ファームウェアの各コンポーネントの現状を考慮して、実行可能な範囲でシステムセ キュリティ工学の原則をシステムの変更に適用する。システムセキュリティ工学の原則を適用することで、信頼でき、安全で、レジリエンスに優れたシス テムを開発し、混乱、危険、脅威に対する組織の感受性を低減することができる。例としては、階層的な保護の開発、システム設計の基礎となるセキュリティポリシー、アーキテ クチャ及び制御の確立、システム開発ライフサイクルへのセキュリティ要件の組み込み、物理的 及び論理的セキュリティ境界の明確化、信頼できる安全なソフトウエアの構築方法に関する開発者のトレー ニングの徹底、ユースケース、脅威エージェント、攻撃ベクトル及びパターン、設計パターン、リスク 軽減に必要な補償制御を特定するための脅威モデリングの実施などがある。セキュリティ工学の原則を適用する組織は、信頼できる安全なシステム、システムコンポー ネント、システムサービスの開発を促進し、リスクを許容可能なレベルまで低減し、情報に基づくリスクマネジメントの決定を行うことができる。

参考文献

ソース・コントロール SA-08

サポート出版物 SP 800-160-1[11]、SP 800-160-2[10]、SP 800-207[66]。

03.16.02 サポートされないシステムコンポーネント

a. システムコンポーネントのサポートが開発者、ベンダー、製造事業者から受けられなくなった場合、そのコンポーネントを交換する。

b. 交換が不可能なサポート対象外のコンポーネントについて、リスク低減またはサポート継続のための代替ソースの選択肢を提供する。

ディスカッション

システム・コンポーネントのサポートには、ソフトウェア・パッチ、ファームウェア・ アップデート、交換部品、保守契約などが含まれる。サポートされていないコンポーネントの例としては、ベンダーが重要なソフトウエア・パッチや製品のアップデートを提供しなくなった場合などがあり、その結果、敵対的なサンプルが、インストールされているコンポーネントの弱点や欠陥を悪用する機会が生じる可能性がある。サポート対象外のシステム・コンポーネントを交換する例外として は、より新しい技術が利用できない場合や、システムが孤立しているため交換用コンポーネントのインストールが選択肢にない場合など、 重要な任務または業務機能を提供するシステムが挙げられる。

代替サポート源は、製造事業者、開発者、またはベンダーによるサポートが終了したシステムコンポー ネントが、組織のミッションやビジネス機能にとって不可欠である場合に、そのようなコンポー ネントに対して継続的なサポートを提供する必要性に対処するものである。必要であれば、組織は、重要なソフトウエアコンポーネントのカスタマイズパッチを開発することによって社内でサポートを確立するか、契約関係を通じてサポート対象外のコンポーネントに継続的なサポートを提供する外部サービスプロバイダのサービスを得ることができる。このような契約関係には、オープンソースソフトウェアの付加価値ベンダーも含まれる。サポートされていないシステム・コンポーネントを使用することによるリスクの増大は、そのようなコンポーネントを公衆ネットワークや管理されていないネットワークに接続することを禁止したり、その他の形で隔離することを実施することによって低減することができる。

参考文献

ソース・コントロール SA-22

サポート出版物：なし

03.16.03 外部システムサービス

a. CUI の処理、保管、または伝送に使用される外部システムサービスのプロバイダに対し、以下のセキュリティ要件に準拠することを要求する：[割当て：組織定義のセキュリティ要件)。

b. 外部サービスプロバイダとの責任分担を含め、外部システムサービスに関するユーザーの役割と責任を定義し、文書化する。

c. 外部サービスプロバイダによるセキュリティ要件遵守を継続的に監視するためのプロセス、方法、技法を導入する。

ディスカッション

外部システムサービスは、外部のサービスプロバイダーによって提供される。組織は、ビジネス・パートナーシップ、契約、省庁間協定、業務提携、ライセンス契約、ジョイント・ベンチャー、サプライ・チェーン交換など、様々な方法で外部サービス・プロバイダとの関係を構築する。外部システム・サービスの利用によるリスクをマネジメントする責任は、CUI の保護を担当する組織にある。サービスレベル契約は、期待されるパフォーマンスを定義し、測定可能な結果を記述し、不履行の場合の救済、低減、および対応要件を特定する。特定の機能、ポート、プロトコル、および当該サービスの提供に使用されるサービスに関する外部サービス・プロバイダからの情報は、特定の機能およびサービスを制限すること、または特定のポートおよびプロトコルをブロックすることに伴うトレードオフを理解する必要がある場合に有用である。この要件は 03.01.20 に関連している。

参考文献

ソース・コントロール SA-09

サポート出版物 SP 800-160-1[11]、SP 800-161[33]。

3.17. サプライチェーンのリスクマネジメント

03.17.01 サプライチェーンのリスクマネジメント計画

a. システム、システムコンポーネント、またはシステムサービスの研究開発、設計、製造、取得、引渡し、統合、運用、保守、および廃棄に関連するサプライチェーンリスクの管理計画を策定する。

b. サプライチェーンのリスクマネジメント計画を見直し、更新する。

c. サプライチェーンのリスクマネジメント計画を不正な開示から保護する。

ディスカッション

外部プロバイダの製品、システム、サービスへの依存と、それらプロバイダとの関係の性質は、 組織に増大するレベルのリスクをもたらす。セキュリティリスクを増大させる脅威行為には、不正生産、偽造品の挿入又は使用、改ざん、サプライチェーンにおける不適切な製造及び開発慣行、窃盗、悪意のあるソフトウェア、ファームウェア及びハードウェアの挿入が含まれる。サプライチェーンリスクは、システム、部品、サービスの中に常在することもあれば、組織的に存在することもある。サプライチェーンのリスクマネジメントは、複雑で多面的な事業であり、信頼関係を構築し、社内外の利害関係者とコミュニケーションを図るために、組織全体で協調して取り組む必要がある。

サプライチェーンのリスクマネジメント（SCRM）活動には、リスクの特定とアセスメント、適切なリスク対応アクションの決定、対応アクションを文書化するための SCRM 計画の策定、及び計画に対する実績のモニタリングが含まれる。システムレベルの SCRM 計画は、実施に特化したものであり、制約、ポリシーの実施、要求事項、及び意味合いを提供する。独立したものとすることも、システムセキュリティ計画に組み込むこともできる。SCRM 計画は、SCRM 要件の管理、実施及び監視と、ミッション及びビジネ ス機能を支援するためのシステム開発ライフサイクル全体にわたるシステムの 開発又は維持に対処する。サプライチェーンは組織間及び組織内で大きく異なる可能性があるため、 SCRM 計画は個々のプログラム、組織及び運用の状況に合わせて調整される。

参考文献

ソース・コントロール SR-02

サポート出版物 SP 800-30[55]、SP 800-39[60]、SP 800-161[33]、SP 800-181[34]。

03.17.02 取得戦略、ツール、および方法

サプライチェーンリスクを特定、保護、軽減するための取得戦略、契約ツール、調達方法を開発し、実施する。

ディスカッション

取得プロセスは、サプライチェーンを保護するための重要な手段を提供する。システム又はシステム・コンポーネントの最終用途を不明瞭にすること、ブラインド購入 を利用すること、改ざん不可能な包装を要求すること、信頼された又は管理された流通を利用す ること等、多くの有用な手段や手法が利用可能である。サプライチェーン・リスクアセスメントの結果は、その状況に最も適用可能な戦略、ツール、及び 方法を示すことができる。ツールや手法は、システ

ムのライフサイクル全体を通じて、不正生産、盗難、改ざん、偽造品の挿入、悪意のあるソフトウエアやバックドアの挿入、不適切な開発行為に対する保護を提供することができる。

組織はまた、サプライヤがセーフガードを実施するためのインセンティブをプロバイダに提供し、サプライヤのプロセス及びセキュリティ慣行の透明性を促進し、汚染された又は偽造された部品の禁止に対処する契約文言を提供し、信頼できないサプライヤからの購入を制限することを検討する。組織は、サプライチェーンのリスク、利用可能な低減戦略、及びそのプログラムをいつ採用すべきかについて、要員に対する研修、教育及び意識向上プログラムを提供することを検討する。開発計画、文書、証拠をレビューし、保護する方法は、組織のセキュリティ要 件に見合ったものである。契約において、文書保護の要件を規定することができる。

参考文献

ソース・コントロール SR-05

サポート出版物 SP 800-30[55]、SP 800-161[33]。

03.17.03 サプライチェーンの要件とプロセス

a. サプライチェーンの要素やプロセスにおける弱点や欠陥を特定し、対処するためのプロセスを確立する。

b. システム、システムコンポーネント、またはシステムサービスに対するサプライチェーンリスクから保護し、サプライチェーンに関連する事象による被害や結果を抑制するために、以下のセキュリティ要件を実施する：*[*割り当て：組織が定義したセキュリティ要件)。

ディスカッション

サプライチェーン要素には、システム及びシステム構成要素の研究、開発、設計、製造、取得、引渡し、統合、運用、保守及び廃棄のために採用される組織、事業体又はツールが含まれる。サプライチェーンプロセスには、ハードウェア、ソフトウェア、ファームウェア、及びシステム開発プロセス、出荷及び取扱い手順、物理的セキュリティプログラム、人的セキュリティプログラム、構成管理ツール、技術、及び出所を維持するための手段、又はシステム及びシステム構成要素の開発、取得、保守、及び廃棄に関連するその他のプログラム、プロセス、又は手順が含まれる。サプライチェーンの要素やプロセスは、組織、システムインテグレーター、または外部のサービスプロバイダーによって提供される。サプライチェーン要素又はプロセスの脆弱性又は欠陥は、敵対者に悪用される可能性のある潜在的な脆弱性を表し、組織に危害を加え、その中核的使命又は事業機能を遂行する能力に影響を与える。

参考文献

ソース・コントロール SR-03

サポート出版物 SP 800-30[55]、SP 800-161[33]。

参考文献

[1] 大統領令 13556（2010 年）管理対象非機密情報。(ホワイトハウス、ワシントン DC)、DCPD-201000942、2010 年 11 月 4 日。https://www.govinfo.gov/app/details/DCPD-201000942。

[2] 大統領令 13526 (2009) 国家安全保障機密情報。(The White House, Washington, DC), DCPD-200901022, December 29, 2009.https://www.govinfo.gov/app/details/DCPD-200901022。

[3] 原子力法（P.L.83-703）、1954 年 8 月。https://www.govinfo.gov/app/details/STATUTE-68/STATUTE-68-Pg919。

[4] National Archives and Records Administration (2019) 管理対象非機密情報（CUI）登録簿。https://www.archives.gov/cui で入手できる。

[5] 32 CFR Part 2002（2016）、管理対象非機密情報（CUI）、2016 年 9 月。https://www.govinfo.gov/content/pkg/CFR-2018-title32-vol6/pdf/CFR-2018title32-vol6-part2002.pdf。

[6] 国立標準技術研究所（2004）連邦情報および情報システムのセキュリティ分類標準。(U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[7] 国立標準技術研究所（2006）連邦情報および情報システムに対する最低セキュリティ要件。(U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200

[8] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-53, Rev. 5, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5.

[9] 連邦情報セキュリティ近代化法（P.L.113-283)、2014 年 12 月。https://www.govinfo.gov/app/details/PLAW-113publ283。

[10] Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2021) Developing Cyber-Resilient Systems : A Systems Security Engineering Approach.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-160, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-160v2r1.

[11] Ross R, Winstead M, McEvilley M (2022) Engineering Trustworthy Secure Systems.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-160, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-160v1r1.

[12] Joint Task Force (2020) Control Baselines for Systems and Organizations.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-53B, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53B.

[13] 行政管理予算局サーキュラーA-130「戦略的資源としての情報の管理」（2016 年 7 月）。https://www.whitehouse.gov/wpcontent/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf。

[14] Souppaya MP, Scarfone KA (2016) Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.(国立標準技術研究所、メリーランド州ゲイサーズバーグ）、NIST 特別刊行物（SP）800-46、改訂 2.https://doi.org/10.6028/NIST.SP.800-46r2

[15] Barker EB (2020) 鍵管理のすすめ：パート 1 - 一般。(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-57 Part 1, Rev. 5. https://doi.org/10.6028/NIST.SP.800-57pt1r5.

[16] Barker EB, Barker WC (2019) 鍵管理のすすめ：パート 2 - 鍵管理組織のベストプラクティス。(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-57 Part 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-57pt2r1.

[17] Barker EB, Dang QH (2015) Recommendation for Key Management, Part 3: ApplicationSpecific Key Management Guidance.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-57 Part 3, Rev. 1. https://doi.org/10.6028/NIST.SP.800-57pt3r1.

[18] Barker EB, Dang QH, Frankel SE, Scarfone KA, Wouters P (2020) Guide to IPsec VPNs.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-77, Rev. 1. https://doi.org/10.6028/NIST.SP.800-77r1.

[19] Frankel SE, Hoffman P, Orebaugh AD, Park R (2008) Guide to SSL VPNs.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-113. https://doi.org/10.6028/NIST.SP.800-113。

[20] Souppaya MP, Scarfone KA (2016) User's Guide to Telework and Bring Your Own Device (BYOD) Security.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-114, Rev. 1. https://doi.org/10.6028/NIST.SP.800-114r1.

[21] Padgette J, Bahr J, Holtmann M, Batra M, Chen L, Smithbey R, Scarfone KA (2017) Guide to Bluetooth Security.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-121, Rev. 2, Includes updates as January 19, 2022. https://doi.org/10.6028/NIST.SP.800-121r2-upd1.

[22] Hu VC, Ferraiolo DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone KA (2014) Guide to Attribute Based Access Control (ABAC) Definition and Considerations.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-162, Includes updates as of August 2, 2019. https://doi.org/10.6028/NIST.SP.800-162.

[23] Ferraiolo DF, Hu VC, Kuhn R, Chandramouli R (2016) A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications : Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC). (National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-178. https://doi.org/10.6028/NIST.SP.800-178.

[24] Yaga DJ, Kuhn R, Hu VC (2017) Verification and Test Methods for Access Control Policies/Models.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-192. https://doi.org/10.6028/NIST.SP.800-192.

[25] Hu VC, Scarfone KA (2012) Guidelines for Access Control System Evaluation Metrics.(National Institute of Standards and Technology, Gaithersburg, MD）、NIST Interagency or Internal Report (IR) 7874。https://doi.org/10.6028/NIST.IR.7874。

[26] Ylonen T, Turner P, Scarfone KA, Souppaya MP (2015) Security of Interactive and Automated Access Management Using Secure Shell (SSH).(National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7966.

https://doi.org/10.6028/NIST.IR.7966

[27] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-63-3, Includes updates as of March 2, 2020. https://doi.org/10.6028/NIST.SP.800-63-3.

[28] Howell G, Franklin JM, Sritapan V, Souppaya M, Scarfone K (2023) Guidelines for Managing the Security of Mobile Devices in the Enterprise.(National Institute of Standards and Technology, Gaithersburg, MD）, NIST 特別刊行物 (SP) 800-124, Rev. 2.

https://doi.org/10.6028/NIST.SP.800-124r2

[29] Scarfone KA, Mell PM (2007) Guide to Intrusion Detection and Prevention Systems (IDPS).(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-94。https://doi.org/10.6028/NIST.SP.800-94。

[30] Frankel SE, Eydt B, Owens L, Scarfone KA (2007) Wireless Robust Security Networks : A Guide to IEEE 802.11i.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-97。

https://doi.org/10.6028/NIST.SP.800-97

[31] Souppaya MP, Scarfone KA (2016) User's Guide to Telework and Bring Your Own Device (BYOD) Security.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-114, Rev. 1. https://doi.org/10.6028/NIST.SP.800-114r1.

[32] Wilson M, Hash J (2003) Building an Information Technology Security Awareness and Training Program.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-50。https://doi.org/10.6028/NIST.SP.800-50。

[33] Boyens JM, Smith A, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-161, Rev. 1. https://doi.org/10.6028/NIST.SP.800-161r1.

[34] Petersen R, Santos D, Smith MC, Wetzel KA, Witte G (2020) Workforce Framework for Cybersecurity (NICE Framework).(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1.

[35] Kent K, Souppaya MP (2006) Guide to Computer Security Log Management.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-92。https://doi.org/10.6028/NIST.SP.800-92。

[36] Kent K, Chevalier S, Grance T, Dang H (2006) Guide to Integrating Forensic Techniques into Incident Response.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-86。https://doi.org/10.6028/NIST.SP.800-86。

[37] Ayers RP, Brothers S, Jansen W (2014) Guidelines on Mobile Device Forensics.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-101, Rev. 1. https://doi.org/10.6028/NIST.SP.800-101r1.

[38] 国立標準技術研究所（2019）暗号モジュールのセキュリティ要件。(米国商務省、ワシントン D.C.)、連邦情報処理標準刊行物（FIPS）140-3。 https://doi.org/10.6028/NIST.FIPS.140-3

[39] National Institute of Standards and Technology (2015) Secure Hash Standard (SHS). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 180-4. https://doi.org/10.6028/NIST.FIPS.180-4.

[40] 国立標準技術研究所（2015）SHA-3 標準：Permutation-Based Hash and Extendable-Output Functions.(米国商務省、ワシントン D.C.）、連邦情報処理標準刊行物（FIPS）202。 https://doi.org/10.6028/NIST.FIPS.202

[41] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-128, Includes updates as of October 10, 2019. https://doi.org/10.6028/NIST.SP.800-128.

[42] Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments：第 2 巻：ハードウェア資産管理。(National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 2. https://doi.org/10.6028/NIST.IR.8011-2.

[43] Dempsey KL, Eavy P, Goren N, Moore G (2018) Automation Support for Security Control Assessments：第 3 巻：ソフトウェア資産管理。(National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 3. https://doi.org/10.6028/NIST.IR.8011-3.

[44] Quinn SD, Souppaya MP, Cook MR, Scarfone KA (2018) National Checklist Program for IT Products：チェックリストの利用者と開発者のためのガイドライン。(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-70, Rev. 4. https://doi.org/10.6028/NIST.SP.800-70r4.

[45] Waltermire DA, Quinn SD, Booth H, III, Scarfone KA, Prisaca D (2018) The Technical Specification for the Security Content Automation Protocol (SCAP)：SCAP Version 1.3. (National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-126, Rev. 3. https://doi.org/10.6028/NIST.SP.800-126r3.

[46] Sedgewick A, Souppaya MP, Scarfone KA (2015) Guide to Application Whitelisting.(National Institute of Standards and Technology, Gaithersburg, MD）、NIST 特別刊行物（SP）800-167https://doi.org/10.6028/NIST.SP.800-167。

[47] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide.(National Institute of Standards and Technology, Gaithersburg, MD）, NIST 特別刊行物 (SP) 800-61, Rev. 2. https://doi.org/10.6028/NIST.SP.800-61r2.

[48] Grance T, Nolan T, Burke K, Dudley R, White G, Good T (2006) Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-84。https://doi.org/10.6028/NIST.SP.800-84。

[49] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-137. https://doi.org/10.6028/NIST.SP.800-137.

[50] Kissel RL, Regenscheid AR, Scholl MA, Stine KM (2014) Guidelines for Media Sanitization.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-88, Rev. 1. https://doi.org/10.6028/NIST.SP.800-88r1.

[51] Scarfone KA, Souppaya MP, Sexton M (2007) Guide to Storage Encryption Technologies for End User Devices.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-111. https://doi.org/10.6028/NIST.SP.800-111.

[52] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-34, Rev. 1, Includes updates as of November 11, 2010. https://doi.org/10.6028/NIST.SP.800-34r1.

[53] Barker EB, Smid ME, Branstad DK, Chokhani S (2013) A Framework for Designing Cryptographic Key Management Systems.(National Institute of Standards and Technology, Gaithersburg, MD）、NIST 特別刊行物（SP）800-130。https://doi.org/10.6028/NIST.SP.800-130。

[54] Barker EB, Branstad DK, Smid ME (2015) A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS).(National Institute of Standards and Technology, Gaithersburg, MD）、NIST 特別刊行物（SP）800-152。https://doi.org/10.6028/NIST.SP.800-152。

[55] 統合タスクフォース変革イニシアティブ（2012）リスクアセスメント実施のためのガイド。(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1.

[56] Souppaya MP, Scarfone KA (2022) エンタープライズパッチ管理計画ガイド：技術の予防保守。(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-40, Rev. 4. https://doi.org/10.6028/NIST.SP.800-40r4.

[57] Joint Task Force Transformation Initiative (2022) Assessing Security and Privacy Controls in Information Systems and Organizations.(National Institute of Standards and Technology,

Gaithersburg, MD), NIST 特別刊行物 (SP) 800-53A, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53Ar5.

[58] Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical Guide to Information Security Testing and Assessment.(National Institute of Standards and Technology, Gaithersburg, MD）、NIST 特別刊行物（SP）800-115。https://doi.org/10.6028/NIST.SP.800-115。

[59] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations : A System Life Cycle Approach for Security and Privacy.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2.

[60] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39.

[61] Nieles M, Pillitteri VY, Dempsey KL (2017) An Introduction to Information Security.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-12, Rev. 1. https://doi.org/10.6028/NIST.SP.800-12r1.

[62] Bowen P, Hash J, Wilson M (2006) Information Security Handbook : A Guide for Managers.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-100, Includes updates as of March 7, 2007. https://doi.org/10.6028/NIST.SP.800-100.

[63] Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-18, Rev. 1. https://doi.org/10.6028/NIST.SP.800-18r1.

[64] Scarfone KA, Hoffman P (2009) Guidelines on Firewalls and Firewall Policy.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-41, Rev. 1. https://doi.org/10.6028/NIST.SP.800-41r1.

[65] Chandramouli R (2016) Secure Virtual Network Configuration for Virtual Machine (VM) Protection.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-125B. https://doi.org/10.6028/NIST.SP.800-125B.

[66] Rose S, Borchert O, Mitchell S, Connelly S (2017) Zero Trust Architecture.(National Institute of Standards and Technology, Gaithersburg, MD）、NIST 特別刊行物（SP）800-207。https://doi.org/10.6028/NIST.SP.800-207。

[67] Sriram K, Montgomery D (2019) レジリエンスに優れたドメイン間トラフィック交換：BGP セキュリティと DDoS 低減。(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-189. https://doi.org/10.6028/NIST.SP.800-189.

[68] National Institute of Standards and Technology (2001) Advanced Encryption Standard (AES). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 197, updated May 9, 2023. https://doi.org/10.6028/NIST.FIPS.197-upd1。

[69] McKay KA, Cooper DA (2019) Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-52, Rev. 2. https://doi.org/10.6028/NIST.SP.800-52r2.

[70] Rose SW, Nightingale S, Garfinkel SL, Chandramouli R (2019) Trustworthy Email.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-177, Rev. 1. https://doi.org/10.6028/NIST.SP.800-177r1.

[71] Jansen W, Winograd T, Scarfone KA (2008) Guidelines on Active Content and Mobile Code.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-28, Version 2. https://doi.org/10.6028/NIST.SP.800-28ver2.

[72] Singhal A, Winograd T, Scarfone KA (2007) Guide to Secure Web Services.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-95。https://doi.org/10.6028/NIST.SP.800-95。

[73] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R (2018) Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-56A, Rev. 3. https://doi.org/10.6028/NIST.SP.800-56Ar3.

[74] Barker EB, Chen L, Roginsky A, Vassilev A, Davis R, Simon S (2019) Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-56B, Rev. 2. https://doi.org/10.6028/NIST.SP.800-56Br2.

[75] Barker EB, Chen L, Davis R (2020) Recommendation for Key-Derivation Methods in KeyEstablishment Schemes.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-56C, Rev. 2. https://doi.org/10.6028/NIST.SP.80056Cr2.

[76] Souppaya MP, Scarfone KA (2013) Guide to Malware Incident Prevention and Handling for Desktops and Laptops.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-83, Rev. 1. https://doi.org/10.6028/NIST.SP.800-83r1.

[77] Tracy MC, Jansen W, Scarfone KA, Butterfield J (2007) Guidelines on Electronic Mail Security.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-45, Version 2. https://doi.org/10.6028/NIST.SP.800-45ver2.

[78] 国家安全保障システム委員会（2022）国家安全保障システム委員会（CNSS）用語集。(国家安全保障局、フォート・ジョージ・G・ミード、メリーランド州)、CNSS Instruction 4009。https://www.cnss.gov/CNSS/issuances/Instructions.cfm で入手可能である。

[79] Title 44 U.S. Code, Sec. 3552, Definitions.2017 年版。https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35subchapII-sec3552。

[80] Title 40 U.S. Code, Sec. 11331, Responsibilities for Federal information systems standards.2017 年版。https://www.govinfo.gov/app/details/USCODE-2017title40/USCODE-2017-title40-subtitleIII-chap113-subchapIII-sec11331 にて入手可能。

[81] Title 44 U.S. Code, Sec. 3502, Definitions.2017 年版。https://www.govinfo.gov/app/details/USCODE-2021-title44/USCODE-2021-title44-chap35subchapI-sec3502。

[82] Chandramouli R, Rose SW (2013) Secure Domain Name System (DNS) Deployment Guide.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-81-2. https://doi.org/10.6028/NIST.SP.800-81-2.

[83] Dempsey K, Pillitteri V, Regenscheid A (2021) Managing the Security of Information Exchanges.(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-47, Rev. 1. https://doi.org/10.6028/NIST.SP.800-47r1.

[84] Ross R, Pillitteri V (2024) Assessing Security Requirements for Controlled Unclassified Information（管理対象非機密情報のセキュリティ要件の評価）。(National Institute of Standards and Technology, Gaithersburg, MD), NIST 特別刊行物 (SP) 800-171A, Rev. 3. https://doi.org/10.6028/NIST.SP.800-171Ar3.

附属書 A. 頭字語

CFR	Code of Federal Regulations	連邦規則
CISA	Cybersecurity and Infrastructure Security Agency	サイバーセキュリティ・インフラセキュリティ庁
CUI	Controlled Unclassified Information	管理対象非機密情報
CVE	Common Vulnerabilities and Exposures	一般的な脆弱性とエクスポージャー
CVSS	Common Vulnerability Scoring System	共通脆弱性スコアリングシステム
CWE	Common Weakness Enumeration	共通の弱点列挙
DMZ	Demilitarized Zone	非武装地帯
EAP	Extensible Authentication Protocol	拡張可能認証プロトコル
FIPS	Federal Information Processing Standards	連邦情報処理標準
FISMA	Federal Information Security Modernization Act	連邦情報セキュリティ近代化法
FTP	File Transfer Protocol	ファイル転送プロトコル
GMT	Greenwich Mean Time	グリニッジ標準時
HSM	Hardware Security Module	ハードウェア・セキュリティ・モジュール
IEEE	Institute of Electrical and Electronics Engineers	電気電子技術者協会
IIoT	Industrial Internet of Things	産業用モノのインターネット
IoT	Internet of Things	モノのインターネット
ISOO	Information Security Oversight Office	情報セキュリティ監視室
IT	Information Technology	情報技術
LSI	Large-Scale Integration	大規模な統合
MAC	Media Access Control	媒体クセス管理
NARA	National Archives and Records Administration	国立公文書記録管理局
NVD	National Vulnerability Database	全国脆弱性データベース
ODP	Organization-Defined Parameter	組織定義のパラメータ
OT	Operational Technology	運用技術
PII	Personally Identifiable Information	個人を特定できる情報
PIN	Personal Identification Number	個人識別番号
PROM	Programmable Read-Only Memory	プログラマブル読み出し専用メモリー
ROM	Read-Only Memory	読み出し専用メモリー
SCAP	Security Content Automation Protocol	セキュリティ・コンテンツ・オートメーション・プロトコル

SCRM	Supply Chain Risk Management	サプライチェーンのリスクマネジメント
TCP/IP	Transmission Control Protocol/Internet Protocol	伝送制御プロトコル／インターネット・プロトコル
TLS	Transport Layer Security	トランスポート層のセキュリティ
UTC	Coordinated Universal Time	協定世界時

附属書 B. 用語集

附属書 B は、SP 800-171r3 で使用される用語の定義を提供する。定義は、特に断りのない限り、国家情報保証用語集[78]に含まれる定義と一致している。

agency	行政機関	連邦政府行政府の行政機関、省庁、軍部、連邦政府法人、連邦政府管理法人、その他の施設、または独立規制機関。[13]
assessment	アセスメント	セキュリティ管理評価を参照。
assessor	アセッサー	セキュリティ管理評価者を参照のこと。
audit log	監査ログ	ある期間に実行されたシステム・アクセスや操作の記録を含む、システム活動の時系列的な記録。
audit record	監査記録	監査対象イベントに関連する監査ログ内の個々のエントリ。
authentication	認証	システム内のリソースへのアクセスを許可する前提条件として、ユーザー、プロセス、またはデバイスの ID を検証すること。[7、適合]。
availability	可用性	情報へのタイムリーで信頼できるアクセスと利用を確保すること。[79]
advanced persistent threat	高度な持続的脅威	高度なレベルの専門知識と重要な資源を保有し、例えばサイバー、物理的、欺瞞を含む複数の攻撃ベクトルを使用することにより、目的を達成する機会を創出することを可能にする敵対者。これらの目的には、通常、情報の流出、ミッション、プログラム、または組織の重要な側面の弱体化または阻害、あるいは将来的にこれらの目的を実行するための位置づけを目的として、標的とする組織の IT インフラ内に足場を確立し、拡張することが含まれる。高度な永続的脅威は、長期間にわたって繰り返しその目的を追求し、それに抵抗しようとする防御側の努力に適応し、その目的を実行するために必要な相互作用のレベルを維持しようと決意する。[60]
authenticator	オーセンティケーター	請求者が所有し管理する何か（通常は暗号モジュールまたはパスワード）で、請求者の ID を認証するために使用される。これは以前はトークンと呼ばれていた。
baseline configuration	ベースライン構成	文書化されたシステムまたはシステム内の構成項目の仕様のセットで、ある時点で正式にレ ビューされ合意され、変更管理手順によってのみ変更できるもの。
common secure configuration	共通セキュア構成	特定の情報技術プラットフォーム／製品の安全な構成設定を規定し、運用要件を満たすようにそれらのシステム・コンポーネントを構成するための指示を示す、認知され、標準化され、確立されたベンチマーク。これらのベンチマークは、セキュリティ構成チェックリスト、ロックダウン及びハードニングガイド、セキュリティ参照ガイド、セキュリティ技術実装ガイドとも呼ばれる。
confidentiality	機密性	個人のプライバシーや専有情報を保護するための手段を含め、情報へのアクセスや情報開示に関する認可された制限を維持する。[79]
configuration management	構成管理	システム開発ライフサイクルを通じて、情報技術製品およびシステムの構成を初期化、変更、監視するプロセスを管理することにより、情報技術製品およびシステムの完全性を確立し、維持することに焦点を当てた活動の集まり。
configuration settings	構成設定	ハードウェア、ソフトウェア、ファームウェアにおいて変更可能なパラメータの集合であって、システムのセキュリティ態勢及び／又は機能に影響を与えるもの。
controlled area	管理領域	情報またはシステムを保護するために設定された要件を満たすために、提供される物理的・手続き的な保護が十分であると組織が確信している領域または空間。

controlled unclassified information	管理対象非機密情報	法律、規制、または政府全体の方針により、保護または拡散の管理が要求される情報。ただし、2009 年 12 月 29 日付の大統領令 13526「国家安全保障情報（Classified National Security Information）」、またはその前身もしくは後継の命令、または 1954 年原子力法（Atomic Energy Act of 1954）に基づき分類される情報は除く。[1]
CUI Executive Agent	CUI エグゼクティブ・エージェント	国立公文書記録管理局（NARA）は、行政府全体の CUI プログラムを実施し、行政命令 13556 を遵守するための連邦機関の行動を監督する。NARA はこの権限を情報セキュリティ監督局（Information Security Oversight Office: ISOO）局長に委任している。[5]
CUI program	CUI プログラム	すべての連邦機関による CUI の取り扱いを標準化するための行政府全体のプログラムである。このプログラムには、大統領令 13556、32 CFR Part 2002、および CUI レジストリによって確立された CUI に関する規則、組織、および手順が含まれる。[5]
CUI registry	CUI レジストリ	32CFR パート 2002 以外の CUI エグゼクティブ・エージェントによって発行されたすべてを含む、CUI の取り扱いに関するすべての情報、ガイダンス、ポリシー、および要件のオンライン・リポジトリである。他の情報の中でも、CUI レジストリは、承認されたすべての CUI カテゴリーを特定し、各カテゴリーの一般的説明を提供し、管理の基礎を特定し、マーキングを確立し、取り扱い手順のガイダンスを含む。[5]
cyber-physical systems	サイバーフィジカルシステム	相互作用するデジタル、アナログ、物理的、および人間のコンポーネントで、統合された物理学と論理によって機能するように設計されている。
executive agency	執行機関	連邦法典第 5 編第 101 条に規定される行政部門、連邦法典第 5 編第 102 条に規定される軍事部門、連邦法典第 5 編第 104 条(1)に定義される独立施設、および連邦法典第 31 編第 91 条の規定に完全に従う完全所有の政府法人。
external network	外部ネットワーク	組織によって管理されていないネットワーク。
external service provider	外部サービスプロバイダ	外部システム・サービス・プロバイダーを参照のこと。
external system (or component)	外部システム（またはコンポーネント）	組織が設定した権限境界の外部にあり、要求されるセキュリティ管理の適用又はセキュリティ管理の有効性の評価について、通常、組織が直接管理できないシステム又はシステムの構成要素。
external system service	外部システムサービス	組織システムの認可境界の外部に実装されるシステムサービス（すなわち、組織システムによって使用されるが、組織システムの一部ではないサービス）であって、要求されるセキュリティ管理策の適用又はセキュリティ管理策の有効性の評価について、通常、組織が直接的な統制を持たないもの。
external system service provider	外部システム・サービス・プロバイダ	外部システムサービスのプロバイダ 合弁事業、業務提携、アウトソーシングの取決め（すなわち、契約、省庁間取決め、 業務提携）、ライセンス契約、及び／又はサプライチェーン交換など、様々な消費者と 生産者の関係を通じて、組織に外部システムサービスを提供する。[8]
facility	施設	情報を処理、保存、伝送するシステムまたはシステム・コンポーネントを含む 1 つ以上の物理的な場所。
federal agency	連邦政府機関	行政機関を参照のこと。
federal information system	連邦情報システム	行政機関、行政機関の請負業者、または行政機関に代わって他の組織が使用または運用する情報システム。[80]

FIPS-validated cryptography	FIPS 認証暗号	暗号モジュール検証プログラム（CMVP）によって検証され、FIPS パブリケーション 140-3（修正後）に規定された要件を満たす暗号モジュール。CMVP 検証の前提条件として、暗号モジュールは、暗号アルゴリズム検証プログラム （CAVP）による検証テストに合格した暗号アルゴリズム実装を採用することが要求される。NSA 承認暗号を参照のこと。
firmware	ファームウェア	ハードウェアに格納されたコンピュータ・プログラムおよびデータ。通常、読み取り専用メモリ （ROM）またはプログラマブル読み取り専用メモリ（PROM）に格納される。ハードウェアとソフトウェアを参照のこと。[78]
hardware	ハードウェア	システムの物理的な構成要素。ソフトウェアおよびファームウェアを参照のこと。[78]
identifier	識別	人の身元および関連する属性を表すために使用される一意のデータ。名前やカード番号は識別子の例である。特定の実体、物体、またはグループを示すためにシステムで使用される一意のラベル。
impact	インパクト	セキュリティに関しては、情報またはシステムの機密性、完全性、または可用性の喪失が、組 織運営、組織資産、個人、他の組織、または国家（米国の国家安全保障上の利益を含む）に及ぼす影響 をいう。プライバシーに関しては、情報システムが個人の PII を処理する際に個人が経験する可能性のある悪影響。
impact value	影響値	情報の機密性、完全性、または可用性が損なわれた場合に生じうる潜在的な影響について、最悪のケースを低、中、または高の値で評価したもの。[6]
incident	インシデント	情報又は情報システムの機密性、完全性又は可用性を、合法的な権限なしに、実際に又は差し迫っ て危険にさらす、又は法律、セキュリティ・ポリシー、セキュリティ手順、許容される利用方 針に対する違反又は違反の差し迫った脅威を構成する出来事。[79]
information	情報	事実、データ、意見などの知識を、文字、数値、図形、地図、物語、電子的、または視聴覚的な形式を含むあらゆる媒体または形式で伝達または表現すること。[13]
information flow control	情報フロー制御	システム内の情報伝達がセキュリティ・ポリシーに違反しないことを保証する手順。
information resources	情報資源	情報及び関連する資源（人員、設備、資金、情報技術など）をいう。[81]
information security	情報セキュリティ	機密性、完全性、可用性を提供するために、不正なアクセス、使用、開示、中断、変更、破壊から情報とシステムを保護すること。[79]
information system	情報システム	情報の収集、処理、維持、使用、共有、普及、または処分のために組織された情報資源の個別集合。[81]
information technology	情報技術	データまたは情報の自動的な取得、保存、分析、評価、操作、管理、移動、制御、表示、切替、交換、送信または受信に使用されるサービス、機器または相互接続されたシステムまたは機器のサブシステム。本定義において、このようなサービスまたは機器は、省庁が直接使用する場合、または省庁との契約に基づいて請負業者が使用する場合であって、その使用が義務付けられている場合、または重要な範囲において、サービスの履行または製品の提供において使用される場合をいう。情報技術には、コンピュータ、付属機器（画像周辺機器、セキュリティおよび監視に必要な入力、出力、記憶装置を含む）、コンピュータの中央処理装置によって制御されるように設計された周辺機器、ソフトウェア、ファームウェア、および類似の手順、サービス（クラウドコンピューティング、ヘルプデスクサービス、または機器やサービスのライフサイ

		クルの任意の時点をサポートするその他の専門的サービスを含む）、および関連リソースが含まれる。情報技術には、その使用を必要としない契約に付随して請負業者が取得する機器は含まれない。[13]
insider threat	内部脅威	インサイダー（insider） インサイダーが許可されたアクセス権を故意または無意識に使用して、米国のセキュリ ティに危害を加える脅威。この脅威には、スパイ活動、テロ行為、不正な情報開示、または部局の資源や能力の損失や低下による米国への損害が含まれる。
integrity	完全性	不適切な情報の改ざんや破壊から保護し、情報の否認防止と真正性を確保することを含む。[79]
internal network	内部ネットワーク	セキュリティ管理の確立、維持、および提供が、組織の従業員または請負業者の直接管理下にあるネットワーク、または、組織が管理するエンドポイント間で実装される暗号カプセル化または類似のセキュリティ技術が、（機密性と完全性に関して）同じ効果を提供するネットワーク。内部ネットワークは通常、組織が所有するものであるが、組織が所有するものでない一方で、組織が管理するものである場合もある。
least privilege	最小特権	セキュリティ・アーキテクチャは、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限のシステム権限とリソースが付与されるように設計されるという原則。
malicious code	悪意のあるコード	悪意のあるコード システムの機密性、完全性、可用性に悪影響を及ぼす不正な処理を実行することを意図したソフトウ ェアまたはファームウェア。悪意のあるコードの例には、ウイルス、ワーム、トロイの木馬、スパイウェア、ある種のアドウェア、またはホストに感染するその他のコードベースのエンティティが含まれる。
media	媒体	システム内で情報が記録、保存、または印刷される、磁気テープ、光ディスク、磁気ディスク、大規模集積（LSI）メモリ・チップ、印刷物（ただし、ディスプレイ・媒体は含まない）を含むが、これらに限定されない物理的なデバイスまたは書き込み面。[7]
mobile code	モバイルコード	リモートシステムから取得したソフトウェアプログラムまたはプログラムの一部がネットワークを介して送信され、受信者による明示的なインストールまたは実行なしにローカルシステム上で実行されること。
mobile device	モバイル・デバイス	ポータブルコンピューティングデバイスとは、一個人が容易に持ち運べるような小型のフォームファクターを持ち、物理的な接続なしに動作するように設計され（例えば、無線で情報を送受信する）、ローカルで取り外し不可能な、または取り外し可能なデータストレージを持ち、自己完結型の電源を含む。モバイルデバイスは、音声通信機能、デバイスが情報を取得できるようにするオンボードセンサー、またはローカルデータを遠隔地と同期させる内蔵機能を含む場合もある。例えば、スマートフォン、タブレット、電子書籍リーダーなどがある。
multi-factor authentication	多要素認証	認証を達成するために、2 つ以上の異なる要素を使用する認証。要素には、知っているもの（PIN、パスワードなど）、持っているもの（暗号化識別デバイ ス、トークンなど）、または自分自身であるもの（バイオメトリクスなど）が含まれる。認証子を参照のこと。
network	ネットワーク	相互接続されたコンポーネントの集合体で実装されるシステム。このようなコンポーネントには、ルーター、ハブ、ケーブリング、電気通信コ ントローラー、鍵配布センター、技術制御装置などが含まれる。

network access	ネットワーク・アクセス	ネットワーク（ローカル・エリア・ネットワーク、ワイド・エリア・ネットワーク、イン ターネットなど）を通じて通信するユーザー（またはユーザーの代理を務めるプロセ ス）によるシステムへのアクセス。
nonfederal organization	連邦政府以外の組織	連邦政府以外のシステムを所有、運用、または保守する事業体。
nonfederal system	非連邦システム	連邦システムの基準を満たさないシステム。
nonlocal maintenance	非ローカル保守	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を通じて通信する個人によって行われる保守活動。
NSA-approved cryptography	NSA 承認暗号	承認されたアルゴリズム、特定環境における機密情報および／または管理された非機密情 報の保護のために承認された実装、およびそれを支える鍵管理インフラストラクチャで構成され る暗号技術。[8]
on behalf of (an agency)	を代表して	以下の場合に発生する状況： (i)行政機関以外の組織が、連邦情報を処理、保管、または送信する目的で、情報システ ムを使用または運用し、あるいは情報を維持または収集する場合。[5]
organization	組織	規模、複雑さ、組織構造内の位置づけを問わない。[7, 適応]。
organization-defined parameter	組織定義のパラメータ	セキュリティ要件の可変部分であり、要件の一部として組織定義の値を割り当てることによって、テーラリングプロセス中に組織によってインスタンス化される。[8, 適応済み]。
overlay	オーバーレイ	セキュリティまたはプライバシーの管理、管理の強化、補足ガイダンス、その他の支援情報の仕様で、セキュリティ管理ベースラインを補完する（さらに洗練する）ことを意図したもので、テーラリングプロセス中に採用される。オーバレイ仕様は、元のセキュ リティ対策基本方針よりも厳しい場合もあれば、緩い場合もあり、複数の情報システムに適用することができる。[13]
personnel security	職員のセキュリティ	信頼性を必要とする職務や責任について、個人の行動、誠実さ、判断力、忠誠心、信頼性、安定性を評価する学問分野。[8]
portable storage device	ポータブル・ストレージ・デバイス	システムに挿入したり、システムから取り外したりすることができ、情報やデータ（テキスト、ビデオ、オーディオ、画像データなど）を保存するために使用されるシステム・コンポーネント。このようなコンポーネントは通常、磁気、光学、またはソリッドステート・デバイス（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、外付けソリッドステート・ドライブ、外付けハード・ディスク・ドライブ、不揮発性メモリを含むフラッシュ・メモリ・カード／ドライブなど）に実装される。
potential impact	潜在的影響	機密性、完全性、または可用性の喪失は、以下のような影響を及ぼすと予想される： (i)限定的な悪影響（FIPS パブリケーション 199 の「低」）、(ii)深刻な悪影響（FIPS パブリケーシ ョン 199 の「中」）、または(iii)組織の運営、組織の資産、または個人に対する深刻または壊滅的な悪 影響（FIPS パブリケーション 199 の「高」）。[6]
privileged account	特権アカウント	特権ユーザの権限を持つシステム・アカウント。
privileged user	特権ユーザー	一般ユーザが実行する権限を持たないセキュリティ関連機能を実行する権限を与えられている（したがって、信頼されている）ユーザ。
records	記録	組織とシステムが意図したとおりに機能していることを検証するための基礎となる、実行された活動や達成された結果の証拠（帳票、報告書、テスト結果など）の記録（自動および／または手動）。また、関連するデータフィールドの単位（すなわち、

		プログラムによってアクセス可能で、特定の項目に関する情報の完全なセットを含むデータフィールドのグループ）を指す場合にも使用される。
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を務めるプロセス）による組織システムへのアクセス。リモートアクセスの方法には、ダイヤルアップ、ブロードバンド、無線がある。
remote maintenance	リモート保守	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が行う保守活動。
replay resistance	リプレイ耐性	不正な効果を生じさせたり、不正なアクセスを得る目的で、送信された認証またはアクセ ス制御情報のキャプチャとその後の再送信に対する保護。
risk	リスク	潜在的な状況または事象によってエンティティが脅かされる程度を示す尺度であり、通常、 以下の関数である： (i)その状況や事象が発生した場合に生じるであろう悪影響、すなわち損害の大きさ、及び(ii)発生の可能性の関数である。[13]
risk assessment	リスクアセスメント	システムの運用に起因する、組織の業務（使命、機能、イメージ、評判を含む）、組織の資産、個人、他の組織、及び国家に対するリスクを特定するプロセス。[55]
sanitization	サニタイゼーション	サニタイゼーション（Sanitization） 媒体に書き込まれたデータを、通常の手段及び（ある種のサニタイゼー ションの場合は）特別な手段によって回復不可能にするために行われる措置。 データ復元が不可能となるように媒体から情報を除去するプロセスで、すべての機密ラベ ル、マーキング、活動ログの除去を含む。
security	セキュリティ	システムの利用に対する脅威がもたらすリスクにもかかわらず、組織がその使命または重要な機能を遂行することを可能にする保護手段を確立し、維持することによって生じる状態。保護手段には、抑止、回避、予防、検知、回復、及び是正の組合せが含まれることがあり、これらは組織のリスク管理手法の一部を形成する必要がある。[78]
security assessment	セキュリティ評価	セキュリティ管理評価を参照。
security control	セキュリティ・コントロール	システム及びその情報の機密性、完全性及び可用性を保護するために、情報システム又は組織に対して規定される保護措置又は対策。[13]
security control assessment	セキュリティ・コントロール評価	情報システムまたは組織のセキュリティ要件を満たすために、セキュリティ管理策がどの程度正しく実装され、意図したとおりに動作し、望ましい結果を生み出しているかを判断するために、セキュリティ管理策をテストまたは評価すること。[13]
security domain	セキュリティ・ドメイン	セキュリティポリシーを実施し、単一の権限によって管理されるドメイン。[78, 適応]。
security functions	セキュリティ機能	システム・セキュリティ・ポリシーを実施し、保護の基礎となるコードとデータの分離をサポートする責任を負う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。
security requirement	セキュリティ要件	適用される法律、行政命令、指令、規制、方針、基準、手順、または、処理、保存、伝送される情報の機密性、完全性、可用性を確保するためのミッション／ビジネス・ニーズから導き出される、システムまたは組織に課される要件。[7, 適応済み] [8, 適応済み]。
system	システム	情報システムを参照のこと。
system component	システムコンポーネント	情報システム（information system） システムの構成要素であり、ハードウェア、ソフトウェア、ファームウェアを 含むことがある、個別の識別可能な情報技術資産。[41]

system security plan	システムセキュリティ計画	システム・セキュリティ計画（System Security Plan） 組織がシステムのセキュリティ要件をどのように満たすか、または満たす予定かを記述した文書。特に、システム・セキュリティ計画には、システムの境界、システムが動作する環境、どのようにセキュリティ要件を満たすか、他のシステムとの関係や他のシステムとの接続が記述される。
system service	システムサービス	情報処理、保存、伝送を容易にするシステムによって提供される機能。
threat	脅威	不正アクセス、破壊、開示、情報の変更、及び／又はサービス拒否によって、システムを通じて組織の運営、組織の資産、個人、他の組織、又は国家に悪影響を及ぼす可能性のある状況又は事象。[55]
system user	システムユーザー	システムへのアクセスを許可された、個人に代わって行動する個人または（システム）プロセス。

附属書 C. テーラリング基準

この附属書では、CUI セキュリティ要求事項の作成に使用されたセキュリティ管理の調整基準について説明する。表 2 に、利用可能な調整オプションと省略形の調整記号を示す。表 3 から表 22 は、第 3 章のセキュリティ要件を得るために、SP 800-53 モデレート・ベースライン [12]の管理策に適用される調整アクションを規定している。管理及び管理強化は、SP 80053 の特定の管理文言及び補足資料にオンラインでアクセスできる NIST Cybersecurity and Privacy Reference Tool にハイパーリンクされている。

表 2. セキュリティ・コントロールの調整基準

記号	基準
NCO	この管理は CUI の機密保護とは直接関係ない。
FED	その管理は主に連邦政府の責任である。
ORC	CUI の機密保護に関する統制の結果は、他の関連する統制によって適切にカバーされている。[16]
N/A	コントロールは適用されない。
CUI	この管理は CUI の機密保護に直接関係する。

表 3. アクセス制御（AC）

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
AC-01	方針と手続き	CUI	03.15.01
AC-02	アカウント管理	CUI	03.01.01
AC-02(01)	口座管理｜自動システム口座管理	NCO	-
AC-02(02)	口座管理｜自動化された臨時・緊急口座管理	NCO	-
AC-02(03)	アカウント管理｜アカウントを無効にする	CUI	03.01.01
AC-02(04)	アカウント管理｜自動監査アクション	NCO	-
AC-02(05)	アカウント管理｜非アクティブ時のログアウト	CUI	03.01.01
AC-02(13)	アカウントマネジメント｜リスクの高い人のアカウントを無効にする	CUI	03.01.01
AC-03	アクセス・エンフォースメント	CUI	03.01.02
AC-04	情報の流れの施行	CUI	03.01.03

[16] SP 800-53 のセキュリティ管理は、組織のシステムを保護し、深層防衛の概念をサポートするために必要なセ キュリティ能力の包括的なセットを提供する。セキュリティ管理策の中には、他の関連する管理策によってカバーされている類似または重複するセキュリティトピックを扱っているものもある。これらの管理策は、調整基準において ORC として指定されている。

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
AC-05	職務の分離	CUI	03.01.04
AC-06	最小特権	CUI	03.01.05
AC-06(01)	最小特権｜セキュリティ機能へのアクセスを認可する。	CUI	03.01.05
AC-06(02)	最小特権｜非セキュリティ機能のための非特権アクセス	CUI	03.01.06
AC-06(05)	最小特権｜特権アカウント	CUI	03.01.06
AC-06(07)	最小特権｜ユーザー権限の見直し	CUI	03.01.05
AC-06(09)	最小特権｜特権機能の使用を記録する	CUI	03.01.07
AC-06(10)	最小特権｜非特権ユーザーによる特権機能の実行を禁止する	CUI	03.01.07
AC-07	ログオンに失敗した	CUI	03.01.08
AC-08	システム利用通知	CUI	03.01.09
AC-11	デバイスロック	CUI	03.01.10
AC-11(01)	デバイスロック｜パターン隠しのディスプレイ	CUI	03.01.10
AC-12	セッション終了	CUI	03.01.11
AC-14	本人確認や認証なしに許される行為	FED	-
AC-17	リモートアクセス	CUI	03.01.02
AC-17(01)	リモートアクセス｜監視と管理	NCO	-
AC-17(02)	リモートアクセス｜暗号化による機密性と完全性の保護	CUI	03.13.08
AC-17(03)	リモートアクセス｜管理型アクセス・コントロール・ポイント	CUI	03.01.12
AC-17(04)	リモートアクセス｜特権コマンドとアクセス	CUI	03.01.12
AC-18	無線アクセス	CUI	03.01.16
AC-18(01)	無線アクセス｜認証と暗号化	CUI	03.01.16
AC-18(03)	ワイヤレスアクセス｜ワイヤレスネットワークを無効にする	CUI	03.01.16
AC-19	モバイル機器のアクセス管理	CUI	03.01.18
AC-19(05)	モバイルデバイスのアクセス管理｜フルデバイスまたはコンテナベースの暗号化	CUI	03.01.18
AC-20	外部システムの利用	CUI	03.01.20
AC-20(01)	外部システムの使用｜認可使用の制限	CUI	03.01.20
AC-20(02)	外部システムの使用｜ポータブル・ストレージ・デバイス - 使用の制限	CUI	03.01.20
AC-21	情報共有	FED	-

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
AC-22	一般にアクセス可能なコンテンツ	CUI	03.01.22

表 4. 意識向上およびトレーニング（AT）

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
AT-01	方針と手続き	CUI	03.15.01
AT-02	識字率向上およびトレーニング	CUI	03.02.01
AT-02(02)	意識向上およびトレーニング｜インサイダーの脅威	CUI	03.02.01
AT-02(03)	意識向上およびトレーニング｜ソーシャルエンジニアリングおよびマイニング	CUI	03.02.01
AT-03	役割ベースのトレーニング	CUI	03.02.02
AT-04	トレーニング記録	NCO	-

表 5. 監査および説明責任（AU）

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
AU-01	方針と手続き	CUI	03.15.01
AU-02	イベントログ	CUI	03.03.01
AU-03	監査記録の内容	CUI	03.03.02
AU-03(01)	追加監査情報	CUI	03.03.02
AU-04	監査ログの保存容量	NCO	-
AU-05	監査ロギング・プロセスの失敗への対応	CUI	03.03.04
AU-06	監査記録のレビュー、分析、報告	CUI	03.03.05
AU-06(01)	監査記録のレビュー、分析、レポーティング｜自動化されたプロセスの統合	NCO	-
AU-06(03)	監査記録のレビュー、分析、レポーティング｜監査記録リポジトリを関連付ける	CUI	03.03.05
AU-07	監査記録の削減とレポート生成的	CUI	03.03.06
AU-07(01)	監査記録の削減とレポート生成的｜自動処理	NCO	-
AU-08	タイムスタンプ	CUI	03.03.07
AU-09	監査情報の保護	CUI	03.03.08
AU-09(04)	監査情報の保護｜一部の特権ユーザによるアクセス	CUI	03.03.08
AU-11	監査記録の保持	CUI	03.03.03
AU-12	監査記録生成的	CUI	03.03.03

表 6. 評価、認可、モニタリング（CA）

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
CA-01	方針と手続き	CUI	03.15.01
CA-02	コントロール・アセスメント	CUI	03.12.01
CA-02(01)	統制評価｜独立評価機関	NCO	-
CA-03	情報交換	CUI	03.12.05
CA-05	行動計画とマイルストーン	CUI	03.12.02
CA-06	認可	FED	-
CA-07	連続モニタリング	CUI	03.12.03
CA-07(01)	継続的モニタリング｜第三者評価	NCO	-
CA-07(04)	継続的モニタリング｜リスクモニタリング	NCO	-
CA-09	システム内部の接続	NCO	-

表 7. 構成管理（CM）

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
CM-01	方針と手続き	CUI	03.15.01
CM-02	ベースライン構成	CUI	03.04.01
CM-02(02)	ベースライン設定｜正確性と最新性のための自動化サポート	NCO	-
CM-02(03)	ベースライン・構成｜以前の構成の保持	NCO	-
CM-02(07)	ベースライン構成｜システムおよびコンポーネントを高リスク領域用に構成する	CUI	03.04.12
CM-03	構成変更管理	CUI	03.04.03
CM-03(02)	構成変更管理｜変更のテスト、検証、文書化	NCO	-
CM-03(04)	設定変更管理｜セキュリティとプライバシーの代表者	NCO	-
CM-04	影響分析	CUI	03.04.04
CM-04(02)	影響分析｜コントロールの検証	CUI	03.04.04
CM-05	変更のためのアクセス制限	CUI	03.04.05
CM-06	構成設定	CUI	03.04.02
CM-07	最低機能	CUI	03.04.06
CM-07(01)	最低機能｜定期レビュー	CUI	03.04.06

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
CM-07(02)	最小機能｜プログラムの実行を防ぐ	ORC	-
CM-07(05)	最小機能｜認可ソフトウェア - 例外的に許可する	CUI	03.04.08
CM-08	システム・コンポーネント・インベントリー	CUI	03.04.10
CM-08(01)	システム・コンポーネント・インベントリ｜インストールと取り外し時のアップデート	CUI	03.04.10
CM-08(03)	システム部品のインベントリ｜未承認部品の自動検知	NCO	-
CM-09	構成管理計画	NCO	-
CM-10	ソフトウェアの使用制限	NCO	-
CM-11	ユーザー・インストール・ソフトウェア	ORC	-
CM-12	情報ロケーション	CUI	03.04.11
CM-12(01)	情報ロケーション｜情報ロケーションを支援する自動化ツール	NCO	-

表 8. コンティンジェンシー計画（CP）

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
CP-01	方針と手続き	NCO	-
CP-02	コンティンジェンシー・計画	NCO	-
CP-02(01)	コンティンジェンシー・計画｜関連計画との調整	NCO	-
CP-02(03)	コンティンジェンシー計画｜ミッションとビジネス機能の再開	NCO	-
CP-02(08)	コンティンジェンシー計画｜重要資産の識別	NCO	-
CP-03	コンティンジェンシートレーニング	NCO	-
CP-04	コンティンジェンシー・計画のテスト	NCO	-
CP-04(01)	コンティンジェンシー・計画のテスト｜関連計画の調整	NCO	-
CP-06	代替保管場所	NCO	-
CP-06(01)	代替保管場所｜プライマリー・サイトの分離	NCO	-
CP-06(03)	代替保管場所｜アクセシビリティ	NCO	-
CP-07	代替処理施設	NCO	-
CP-07(01)	代替処理サイト｜プライマリー・サイトの分離	NCO	-
CP-07(02)	代替処理サイト｜アクセシビリティ	NCO	-
CP-07(03)	代替処理サイト｜サービスの優先順位	NCO	-

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
CP-08	電気通信サービス	NCO	-
CP-08(01)	電気通信サービス｜優先サービス規定	NCO	-
CP-08(02)	電気通信サービス｜単一障害点	NCO	-
CP-09	システム・バックアップ	CUI	03.08.09
CP-09(01)	システムのバックアップ｜信頼性と完全性のテスト	NCO	-
CP-09(08)	システムバックアップ｜暗号保護	CUI	03.08.09
CP-10	システムの復旧と再構築	NCO	-
CP-10(02)	システムの復旧と再構築｜トランザクションの復旧	NCO	-

表 9. 識別および認証（IA）

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
IA-01	方針と手続き	CUI	03.15.01
IA-02	識別および認証（組織ユーザー）	CUI	03.05.01
IA-02(01)	識別および認証（組織ユーザー）｜特権アカウントへの多要素認証	CUI	03.05.03
IA-02(02)	識別と認証（組織ユーザー）｜非特権アカウントへの多要素認証	CUI	03.05.03
IA-02(08)	識別および認証（組織ユーザー）｜アカウントへのアクセス - 耐リプレイ性	CUI	03.05.04
IA-02(12)	識別および認証（組織ユーザ）｜PIV クレデンシャルの受け入れ	FED	-
IA-03	デバイスの識別と認証	CUI	03.05.02
IA-04	識別子の管理	CUI	03.05.05
IA-04(04)	識別子の管理｜ユーザーのステータスを識別する	CUI	03.05.05
IA-05	認証管理	CUI	03.05.12
IA-05(01)	認証者管理｜パスワード・ベース認証	CUI	03.05.07
IA-05(02)	認証管理｜公開鍵ベース認証	FED	-
IA-05(06)	認証管理｜認証子の保護	FED	-
IA-06	認証フィードバック	CUI	03.05.11
IA-07	暗号モジュール認証	FED	-
IA-08	識別および認証（非組織ユーザー）	FED	-
IA-08(01)	識別および認証（非組織ユーザ）｜他機関からの PIV クレデンシャルの受け入れ	FED	-

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
IA-08(02)	識別および認証（非組織ユーザー）｜外部認証者の受け入れ	FED	-
IA-08(04)	認証（非組織ユーザー）｜定義されたプロファイルの使用	FED	-
IA-11	認証のやり直し	CUI	03.05.01
IA-12	身元確認	FED	-
IA-12(02)	身元確認｜身元証拠	FED	-
IA-12(03)	身元確認｜身元証拠の検証と検証	FED	-
IA-12(05)	身元証明｜住所確認	FED	-

表 10. インシデント対応（IR）

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
IR-01	方針と手続き	CUI	03.15.01
IR-02	インシデント対応トレーニング	CUI	03.06.04
IR-03	インシデント対応テスト	CUI	03.06.03
IR-03(02)	インシデント対応テスト｜関連計画との調整	NCO	-
IR-04	インシデントハンドリング	CUI	03.06.01
IR-04(01)	インシデントハンドリング｜自動化されたインシデントハンドリング・プロセス	NCO	-
IR-05	インシデント・モニタリング	CUI	03.06.02
IR-06	インシデント報告	CUI	03.06.02
IR-06(01)	インシデント・レポーティング｜自動化されたレポーティング	NCO	-
IR-06(03)	インシデント報告｜サプライチェーン・コーディネーション	NCO	-
IR-07	インシデント対応支援	CUI	03.06.02
IR-07(01)	インシデント対応支援｜情報の可用性とサポートの自動化サポート	NCO	-
IR-08	インシデント対応計画	CUI	03.06.05

表 11. 保守 (MA)

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
MA-01	システム保守の方針と手順	CUI	03.15.01
MA-02	保守管理	NCO	-

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
MA-03	保守ツール	CUI	03.07.04
MA-03(01)	保守用具｜点検用具	CUI	03.07.04
MA-03(02)	保守ツール｜媒体を検査する	CUI	03.07.04
MA-03(03)	保守ツール｜不正な取り外しを防ぐ	CUI	03.07.04
MA-04	非ローカル保守	CUI	03.07.05
MA-05	保守要員	CUI	03.07.06
MA-06	適時保守	NCO	-

表 12. 媒体保護(MP)

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
MP-01	方針と手続き	CUI	03.15.01
MP-02	媒体・アクセス	CUI	03.08.02
MP-03	媒体・マーキング	CUI	03.08.04
MP-04	媒体・ストレージ	CUI	03.08.01
MP-05	媒体輸送	CUI	03.08.05
MP-06	媒体のサニタイゼーション	CUI	03.08.03
MP-07	媒体利用	CUI	03.08.07

表 13. 物理的および環境的保護（PE）

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
PE-01	方針と手続き	CUI	03.15.01
PE-02	物理的アクセス認可	CUI	03.10.01
PE-03	物理的アクセス管理	CUI	03.10.07
PE-04	送信のアクセス管理	CUI	03.10.08
PE-05	出力機器のアクセス管理	CUI	03.10.07
PE-06	物理的アクセスを監視する	CUI	03.10.02
PE-06(01)	物理的アクセスの監視｜侵入アラームと監視装置	NCO	-
PE-08	ビジター・アクセス記録	NCO	-
PE-09	電力設備とケーブル配線	NCO	-

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
PE-10	緊急シャットオフ	NCO	-
PE-11	非常用電源	NCO	-
PE-12	非常用照明	NCO	-
PE-13	防火対策	NCO	-
PE-13(01)	防火｜検知システム - 自動作動と通知	NCO	-
PE-14	環境制御	NCO	-
PE-15	水害保護	NCO	-
PE-16	搬入・搬出	NCO	-
PE-17	代替勤務地	CUI	03.10.06

表 14. 計画（PL）

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
PL-01	方針と手続き	CUI	03.15.01
PL-02	システムのセキュリティとプライバシー計画	CUI	03.15.02
PL-04	行動規範	CUI	03.15.03
PL-04(01)	行動規範｜ソーシャル媒体と外部サイト・アプリの利用制限	NCO	-
PL-08	セキュリティとプライバシーのアーキテクチャ	NCO	-
PL-10	ベースラインの選択	FED	-
PL-11	ベースライン・テーラリング	FED	-

表 15. プログラム・マネジメント（PM）

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
PM-01	情報セキュリティ・プログラム計画	N/A	-
PM-02	情報セキュリティ・プログラム・リーダーの役割	N/A	-
PM-03	情報セキュリティとプライバシーに関するリソース	N/A	-
PM-04	行動計画とマイルストーンのプロセス	N/A	-
PM-05	システム・インベントリ	N/A	-
PM-05(01)	システム・インベントリ｜個人を特定できる情報のインベントリ	N/A	-
PM-06	パフォーマンスの指標	N/A	-

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
PM-07	エンタープライズ・アーキテクチャ	N/A	-
PM-07(01)	エンタープライズ・アーキテクチャ｜オフロード	N/A	-
PM-08	重要インフラ計画	N/A	-
PM-09	リスクマネジメント戦略	N/A	-
PM-10	認可プロセス	N/A	-
PM-11	ミッションとビジネス・プロセスの定義	N/A	-
PM-12	インサイダー脅威プログラム	N/A	-
PM-13	セキュリティとプライバシーの労働力	N/A	-
PM-14	テスト、トレーニング、モニタリング	N/A	-
PM-15	セキュリティとプライバシーの団体と協会	N/A	-
PM-16	脅威認識プログラム	N/A	-
PM-16(01)	脅威認識プログラム｜脅威インテリジェンスを共有する自動化された手段	N/A	-
PM-17	外部システム上の管理対象非機密情報の保護	N/A	-
PM-18	プライバシー・プログラム計画	N/A	-
PM-19	プライバシー・プログラム・リーダーの役割	N/A	-
PM-20	プライバシー・プログラム情報の普及	N/A	-
PM-20(01)	プライバシープログラム情報の周知｜ウェブサイト、アプリケーション、デジタルサービスにおけるプライバシーポリシー	N/A	-
PM-21	開示の会計処理	N/A	-
PM-22	個人を特定できる情報の品質管理	N/A	-
PM-23	データガバナンス会議体	N/A	-
PM-24	データ・インテグリティ委員会	N/A	-
PM-25	試験、訓練、研究に使用される PII の最小化	N/A	-
PM-26	苦情管理	N/A	-
PM-27	プライバシー	N/A	-
PM-28	リスクの枠組み	N/A	-
PM-29	リスクマネジメント・プログラムの指導者の役割	N/A	-
PM-30	サプライチェーンのリスクマネジメント戦略	N/A	-
PM-30(01)	サプライチェーンのリスクマネジメント戦略｜重要品目または基幹品目のサプライヤー	N/A	-

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
PM-31	継続的モニタリング戦略	N/A	-
PM-32	ポーズ	N/A	-

表 16. 職員のセキュリティ（PS）

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
PS-01	方針と手続き	CUI	03.15.01
PS-02	ポジション リスク指定	FED	-
PS-03	人事選考	CUI	03.09.01
PS-04	人事解雇	CUI	03.09.02
PS-05	人事異動	CUI	03.09.02
PS-06	アクセス契約	NCO	-
PS-07	社外職員のセキュリティ	NCO	-
PS-08	人事上の制裁	NCO	-
PS-09	ポジション詳細	FED	-

表 17. PII の処理と透明性（PT）

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
PT-01	方針と手続き	N/A	-
PT-02	個人を特定できる情報を処理する認可	N/A	-
PT-02(01)	個人を特定できる情報を処理する認可｜データタグ付け	N/A	-
PT-02(02)	個人を特定できる情報を処理する認可｜オートメーション	N/A	-
PT-03	個人を特定できる情報の処理目的	N/A	-
PT-03(01)	個人を特定できる情報処理の目的｜データタギング	N/A	-
PT-03(02)	個人を特定できる情報処理の目的｜自動化	N/A	-
PT-04	同意	N/A	-
PT-04(01)	同意｜テーラーメイドの同意	N/A	-
PT-04(02)	同意｜ジャストインタイム・コンセント	N/A	-
PT-04(03)	同意｜撤回	N/A	-
PT-05	プライバシー	N/A	-

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
PT-05(01)	プライバシー通知｜ジャストインタイム通知	N/A	-
PT-05(02)	プライバシー通知｜個人情報保護法に関する声明	N/A	-
PT-06	記録システムのお知らせ	N/A	-
PT-06(01)	システム・オブ・レコードのお知らせ｜定期的な使用	N/A	-
PT-06(02)	記録制度通知｜免責規定	N/A	-
PT-07	個人を特定できる情報のカテゴリー	N/A	-
PT-07(01)	個人を特定できる情報のカテゴリー｜社会保障番号	N/A	-
PT-07(02)	個人を特定できる情報のカテゴリー｜はじめに 修正情報	N/A	-
PT-08	コンピューター・マッチングの条件	N/A	-

表 18. リスクアセスメント（RA）

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
RA-01	方針と手続き	CUI	03.15.01
RA-02	セキュリティの分類	FED	-
RA-03	リスクアセスメント	CUI	03.11.01
RA-03(01)	リスクアセスメント｜サプライチェーンリスクアセスメント	CUI	03.11.01
RA-05	脆弱性の監視とスキャン	CUI	03.11.02
RA-05(02)	脆弱性の監視とスキャン｜スキャンする脆弱性をアップデートする	CUI	03.11.02
RA-05(05)	脆弱性の監視とスキャン｜特権アクセス	ORC	-
RA-05(11)	脆弱性の監視とスキャン｜情報公開プログラム	NCO	-
RA-07	リスク対応	CUI	03.11.04
RA-09	クリティカリティ分析	NCO	-

表 19. システムおよびサービスの取得（SA）

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
SA-01	方針と手続き	CUI	03.15.01
SA-02	リソースの配分	NCO	-
SA-03	システム開発ライフサイクル	NCO	-

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
SA-04	取得プロセス	NCO	-
SA-04(01)	取得プロセス｜コントロールの機能特性	NCO	-
SA-04(02)	取得プロセス｜統制の設計と実施に関する情報	NCO	-
SA-04(09)	取得プロセス｜使用している機能、ポート、プロトコル、サービス	NCO	-
SA-04(10)	取得プロセス｜承認された PIV 製品の使用	FED	-
SA-05	システム・ドキュメント	NCO	-
SA-08	セキュリティとプライバシー工学の原則	CUI	03.16.01
SA-09	外部システム・サービス	CUI	03.16.03
SA-09(02)	外部システムサービス｜機能、ポート、プロトコル、サービスの識別	ORC	-
SA-10	開発者構成管理	NCO	-
SA-11	デベロッパーのテストと評価	NCO	-
SA-15	開発プロセス、標準、ツール	NCO	-
SA-15(03)	開発プロセス・標準・ツール｜クリティカリティ分析	NCO	-
SA-22	サポートされていないシステムコンポーネント	CUI	03.16.02

表 20. システムおよび通信の保護 (SC)

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
SC-01	方針と手続き	CUI	03.15.01
SC-02	システムとユーザー機能の分離	ORC	-
SC-04	共有システム・リソース内の情報	CUI	03.13.04
SC-05	サービス拒否保護	NCO	-
SC-07	バウンダリー・プロテクション	CUI	03.13.01
SC-07(03)	バウンダリー・プロテクション｜アクセスポイント	ORC	-
SC-07(04)	バウンダリー・プロテクション｜外部通信サービス	ORC	-
SC-07(05)	バウンダリー・プロテクション｜デフォルトで拒否 - 例外で許可	CUI	03.13.06
SC-07(07)	バウンダリー・プロテクション｜リモート・デバイスのためのスプリット・トンネリング	ORC	-

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
SC-07(08)	バウンダリー・プロテクション｜認証されたプロキシサーバーにトラフィックをルーティングする	ORC	-
SC-08	伝送の機密性と完全性	CUI	03.13.08
SC-08(01)	伝送の機密性と完全性｜暗号による保護	CUI	03.13.08
SC-10	ネットワーク切断	CUI	03.13.09
SC-12	暗号鍵の確立と管理	CUI	03.13.10
SC-13	暗号保護	CUI	03.13.11
SC-15	コラボレーション・コンピューティング・デバイスとアプリケーション	CUI	03.13.12
SC-17	公開鍵基盤証明書	FED	-
SC-18	モバイルコード	CUI	03.13.13
SC-20	セキュアな名前/住所解決サービス（権威ソース）	NCO	-
SC-21	セキュアな名前/アドレス解決サービス（再帰的またはキャッシュ・リゾルバ）	NCO	-
SC-22	名前/アドレス解決サービスのアーキテクチャとプロビジョニング	NCO	-
SC-23	セッション認証	CUI	03.13.15
SC-28	安静時情報の保護	CUI	03.13.08
SC-28(01)	静止状態の情報保護｜暗号による保護	CUI	03.13.08
SC-39	プロセスの分離	NCO	-

表 21. システムおよび情報の完全性（SI）

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
SI-01	方針と手続き	CUI	03.15.01
SI-02	欠陥の修復	CUI	03.14.01
SI-02(02)	欠陥の修復｜自動欠陥修復ステータス	NCO	-
SI-03	悪意のあるコードの保護	CUI	03.14.02
SI-04	システム監視	CUI	03.14.06
SI-04(02)	システム監視｜リアルタイム分析のための自動化ツールとメカニズム	NCO	-
SI-04(04)	システム監視｜インバウンドとアウトバウンドのコミュニケーション交通	CUI	03.14.06
SI-04(05)	システム監視｜システム生成的アラート	NCO	-

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
SI-05	セキュリティ・アラート、勧告、指令	CUI	03.14.03
SI-07	ソフトウェア、ファームウェア、情報の完全性	NCO	-
SI-07(01)	ソフトウェア、ファームウェア、情報の完全性｜完全性チェック	NCO	-
SI-07(07)	ソフトウェア、ファームウェア、情報の完全性｜検知と対応の統合	NCO	-
SI-08	スパム保護	ORC	-
SI-08(02)	スパム保護｜自動アップデート	NCO	-
SI-10	情報入力の検証	NCO	-
SI-11	エラー処理	NCO	-
SI-12	情報管理と保持	CUI	03.14.08
SI-16	メモリー保護	NCO	-

表 22. サプライチェーンのリスクマネジメント(SR)

NIST SP 800-53 中程度のベースライン		基準	セキュリティ要件
SR-01	方針と手続き	CUI	03.15.01
SR-02	サプライチェーンのリスクマネジメント計画	CUI	03.17.01
SR-02(01)	サプライチェーンのリスクマネジメント計画｜SCRM チームの設立	NCO	-
SR-03	サプライチェーン・コントロールとプロセス	CUI	03.17.03
SR-05	獲得戦略、ツール、方法	CUI	03.17.02
SR-06	サプライヤーの評価とレビュー	CUI	03.11.01
SR-08	通知契約	NCO	-
SR-10	システムまたはコンポーネントの検査	NCO	-
SR-11	コンポーネントの認証	NCO	-
SR-11(01)	部品の認証｜模倣品・海賊版対策トレーニング	NCO	-
SR-11(02)	コンポーネントの認証｜コンポーネントのサービスと修理のための構成・コントロール	NCO	-
SR-12	部品廃棄	ORC	-

附属書 D. 組織定義のパラメータ

この附属書では、第 3 章のセキュリティ要件に含まれる組織定義パラメータ（ODP）を列挙する。ODP は、アクセス管理（AC）ファミリーの ODP を含む最初の要求事項から始まり、サプライチェーンのリスクマネジメント（SR）ファミリーの ODP を含む最後の要求事項で終わる、要求事項ファミリーごとに順番に列挙されている。

表 23.組織定義のパラメータ

セキュリティ要件	組織定義パラメータ	
03.01.01	03.01.01.f.02	[割り当て：組織が定義した期間]。
03.01.01	03.01.01.g.01	[割り当て：組織が定義した期間]。
03.01.01	03.01.01.g.02	[割り当て：組織が定義した期間]。
03.01.01	03.01.01.g.03	[割り当て：組織が定義した期間]。
03.01.01	03.01.01.h	[割り当て：組織が定義した期間]。
03.01.01	03.01.01.h	[割り当て：組織が定義した状況]。
03.01.05	03.01.05.b	[割り当て：組織で定義されたセキュリティ機能]。
03.01.05	03.01.05.b	[割り当て：組織で定義されたセキュリティ関連情報]。
03.01.05	03.01.05.c	[割り当て：組織定義の頻度]。
03.01.06	03.01.06.a	[割り当て：組織で定義された職員または役割]。
03.01.08	03.01.08.a	[割り当て：組織で定義された番号]。
03.01.08	03.01.08.a	[割り当て：組織が定義した期間]。
03.01.08	03.01.08.b	[選択（*1* つまたは複数）：アカウントまたはノードを[割り当て]のためにロックする： 管理者が解除するまでアカウントまたはノードをロックする。次のログオンプロンプトを遅延させる。]
03.01.10	03.01.10.a	[選択（*1* つ以上）：[割り当て：組織で定義された期間] 非アクティブになった後にデバイスロックを開始する。]
03.01.11	03.01.11	[割り当て：セッション切断を必要とする組織定義の条件またはトリガーイベント]。
03.01.20	03.01.20.b	[割り当て：組織で定義されたセキュリティ要件]。
03.02.01	03.02.01.a.01	[割り当て：組織定義の頻度]。
03.02.01	03.02.01.a.02	[割り当て：組織定義のイベント]。
03.02.01	03.02.01.b	[割り当て：組織定義の頻度]。
03.02.01	03.02.01.b	[割り当て：組織定義のイベント]。

セキュリティ要件	組織定義パラメータ	
03.02.02	03.02.02.a.01	[割り当て：組織定義の頻度]。
03.02.02	03.02.02.a.02	[割り当て：組織定義のイベント]。
03.02.02	03.02.02.b	[割り当て：組織定義の頻度]。
03.02.02	03.02.02.b	[割り当て：組織定義のイベント]。
03.03.01	03.03.01.a	[割り当て：組織定義のイベントタイプ]。
03.03.01	03.03.01.b	[割り当て：組織定義の頻度]。
03.03.04	03.03.04.a	[割り当て：組織が定義した期間]。
03.03.04	03.03.04.b	[割り当て：組織定義の追加アクション]。
03.03.05	03.03.05.a	[割り当て：組織定義の頻度]。
03.03.07	03.03.07.b	[割り当て：時間測定の組織定義の粒度]。
03.04.01	03.04.01.b	[割り当て：組織定義の頻度]。
03.04.02	03.04.02.a	[割り当て：組織定義の構成設定]。
03.04.06	03.04.06.b	[割り当て：組織で定義された機能、ポート、プロトコル、接続、および/またはサービス]。
03.04.06	03.04.06.c	[割り当て：組織定義の頻度]。
03.04.08	03.04.08.c	[割り当て：組織定義の頻度]。
03.04.10	03.04.10.b	[割り当て：組織定義の頻度]。
03.04.12	03.04.12.a	[割り当て：組織定義のシステム構成]。
03.04.12	03.04.12.b	[割り当て：組織で定義されたセキュリティ要件]。
03.05.01	03.05.01.b	[割り当て：再認証を必要とする組織定義の状況または状況]。
03.05.02	03.05.02	[割り当て：組織で定義されたデバイスまたはデバイスのタイプ]。
03.05.05	03.05.05.c	[割り当て：組織が定義した期間]。
03.05.05	03.05.05.d	[識別：個人の状態を識別する組織定義の特性]。
03.05.07	03.05.07.a	[割り当て：組織定義の頻度]。
03.05.07	03.05.07.f	[割り当て：組織で定義された構成と複雑さのルール]。
03.05.12	03.05.12.e	[割り当て：組織定義の頻度]。

セキュリティ要件	組織定義パラメータ	
03.05.12	03.05.12.e	[割り当て：組織定義のイベント]。
03.06.02	03.06.02.b	[割り当て：組織が定義した期間]。
03.06.02	03.06.02.c	[認可：組織で定義された権限]。
03.06.03	03.06.03	[割り当て：組織定義の頻度]。
03.06.04	03.06.04.a.01	[割り当て：組織が定義した期間]。
03.06.04	03.06.04.a.03	[割り当て：組織定義の頻度]。
03.06.04	03.06.04.b	[割り当て：組織定義の頻度]。
03.06.04	03.06.04.b	[割り当て：組織定義のイベント]。
03.08.07	03.08.07.a	[割り当て：組織が定義するシステム・媒体のタイプ]。
03.09.01	03.09.01.b	[割り当て：再選考を必要とする組織定義の条件]。
03.09.02	03.09.02.a.01	[割り当て：組織が定義した期間]。
03.10.01	03.10.01.c	[割り当て：組織定義の頻度]。
03.10.02	03.10.02.b	[割り当て：組織定義の頻度]。
03.10.02	03.10.02.b	[割り当て：組織で定義された事象または事象の潜在的兆候]。
03.10.06	03.10.06.b	[割り当て：組織で定義されたセキュリティ要件]。
03.11.01	03.11.01.b	[割り当て：組織定義の頻度]。
03.11.02	03.11.02.a	[割り当て：組織定義の頻度]。
03.11.02	03.11.02.b	[割り当て：組織定義の応答時間]。
03.11.02	03.11.02.c	[割り当て：組織定義の頻度]。
03.12.01	03.12.01	[割り当て：組織定義の頻度]。
03.12.05	03.12.05.a	[選択（1 つ以上）：相互接続セキュリティ契約、情報交換セキュリティ契約、覚書または合意書、サービスレベル契約、ユーザー契約、機密保持契約、その他の種類の契約]。
03.12.05	03.12.05.c	[割り当て：組織定義の頻度]。
03.13.09	03.13.09	[割り当て：組織が定義した期間]。
03.13.10	03.13.10	[割り当て：鍵の確立と管理に関する組織定義の要件]。

セキュリティ要件	組織定義パラメータ	
03.13.11	03.13.11	[課題：組織で定義された暗号の種類】。]
03.13.12	03.13.12.a	[割り当て：リモート起動が許可される組織定義の例外]。
03.14.01	03.14.01.b	[割り当て：組織が定義した期間]。
03.14.02	03.14.02.c.01	[割り当て：組織定義の頻度]。
03.15.01	03.15.01.b	[割り当て：組織定義の頻度]。
03.15.02	03.15.02.b	[割り当て：組織定義の頻度]。
03.15.03	03.15.03.d	[割り当て：組織定義の頻度]。
03.16.01	03.16.01	[課題：組織で定義されたシステムセキュリティ工学の原則]。
03.16.03	03.16.03.a	[割り当て：組織で定義されたセキュリティ要件]。
03.17.01	03.17.01.b	[割り当て：組織定義の頻度]。
03.17.03	03.17.03.b	[割り当て：組織で定義されたセキュリティ要件]。

附属書 E. 変更履歴

本書は、初版（2020 年 2 月、2021 年 1 月 28 日更新）からの以下の変更点を織り込んでいる：

- 第 1 項と第 2 項の序文情報を簡素化し、分かりやすさと理解を改善した。
- SP 800-53B [12]の中程度の基本方針及び附属書 C の調整措置のセキュリティ対策を反映するように、第 3 章のセキュリティ要件及びファミリを修正した。
- 基本的なセキュリティ要件と派生的なセキュリティ要件の区別を廃止した。
- セキュリティ要件の具体性を向上させ、曖昧さをなくし、実装の有効性を改善し、 評価の範囲を明確にした
- 一部のセキュリティ要件に ODP（Organization-Defined Parameter：組織定義パラメータ）を導入し、柔軟性を高めて組織のリスクマネジメントを支援する。
- セキュリティ要件を可能な限りグループ化することで、 理解を深め、実装と評価の効率を向上させる
- 時代遅れで冗長なセキュリティ要件を削除した
- 新しいセキュリティ要件が追加された
- セキュリティ要件にタイトルを追加
- セキュリティー要件に関する議論のセクションを再編成し、スリム化した。
- 新しいカテゴリーを追加した：その他の関連コントロール（ORC）と N/A（N/A）を追加した。
- 附属書 C の調整基準を使用して、SP 800-53B 中程度のベースラインの選択された管理を再分類した。
- SP 800-53 のセキュリティ管理に関する文言との整合性を図るため、セキュリティ要件を改訂した。
- 参考文献、略語、用語集のセクションの構成を見直し、より明確で使いやすくした。
- 附属書 C のテーラリング表を、セキュリティ要件の変更と整合するよう修正した。
- セキュリティ要件に関する組織定義のパラメータを列挙した新しい附属書を追加した。

表 24 に、本書に組み込んだ。変更点を示す。正誤表の更新には、編集的または実質的な性質の、出版物の修正、明確化、その他の小さな変更が含まれる。正誤表更新または正式な改訂版としてまだ公表されて

いない、追加問題や修正の可能性を含む本書の更新の可能性は、識別され次第掲載される。本報告書の発行の詳細を参照のこと。本書の現在のリリースには、正誤表の更新は含まれていない。

表 24.変更履歴

出版物 ID	日付	編集の種類	変更	ロケーション