NIST Special Publication 800-172

管理対象非機密情報を保護するための拡張セキュリティ要件

NIST SP 800-171 の補足

RON ROSS
VICTORIA PILLITTERI
GARY GUISSANIE
RYAN WAGNER
RICHARD GRAUBART
DEB BODEAU

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

この文書は以下の団体によって翻訳監修されています

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

NIST Special Publication 800-172

管理対象非機密情報を保護するための拡張セキュリティ要件

NIST SP 800-171 の補足

RON ROSS
VICTORIA PILLITTERI
Computer Security Division
National Institute of Standards and Technology

GARY GUISSANIE
RYAN WAGNER
Institute for Defense Analyses

RICHARD GRAUBART
DEB BODEAU
The MITRE Corporation

2021 年 2 月

U.S. Department of Commerce
Wynn Coggins, Acting Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

発行機関

本出版物は、連邦情報セキュリティ近代化法（FISMA：Federal Information Security Modernization Act）、合衆国法典（U.S.C.）第 44 編第 3551 条以下、および公法（P.L.：Public Law）113 条-283 条に基づく法的責任を受けて米国国立標準技術研究所（NIST：National Institute of Standards and Technology）によって策定された。NIST は、連邦政府情報システムの最小限の要件を含む、情報セキュリティ規格およびガイドラインを策定する責務を負うが、そうした規格およびガイドラインは、国家安全保障システムにおいては、それらのシステムに対して政策権限を行使する適切な連邦政府担当官の明示的な承認なしに適用してはならない。このガイドラインは、行政管理予算局（OMB：Office of Management and Budget）による通達（Circular）A-130 号の要件と一致している。

本出版物のいかなる内容も、法的権限の下で商務長官（Secretary of Commerce）が連邦政府機関に順守を義務付けた基準およびガイドラインを否定するものと解釈されることは望ましくない。また、これらのガイドラインは、商務長官、行政管理予算局長官（OMB Director）、またはその他の連邦政府担当官の既存の権限を変更する、または代わるものとして解釈されることは望ましくない。本出版物は、非政府組織が自由に使用してもよく、米国における著作権の対象外であるが、NIST に帰属する。

米国国立標準技術研究所　特別出版物（Special Publication）800-172
NIST SP 800-172　**84** ページ（2021 年 2 月）

CODEN: NSPUE2

本出版物は、https://doi.org/10.6028/NIST.SP.800-172 から無料で入手可能である。

本出版物では、試行的手順や概念を適切に説明するために、特定の商業エンティティ、装置、または資料が記載されている場合がある。そうした記載は、NIST による推奨または承認を意図するものではなく、目的を達成するうえでそれらのエンティティ、装置、または資料が必ずしも最良なものであるということを意図するものでもない。

本出版物では、NIST が担う法的責任に従って現在策定している他の出版物を参照する場合がある。連邦政府機関は、本出版物に記載の情報を、概念、プラクティス、および方法論を含め、関連出版物の完成前であっても使用してもよい。したがって、現行の要件、ガイドライン、および手順が存在する場合には、各出版物が完成するまでの間、それらは引き続き有効である。計画の策定および移行のために、連邦政府機関は、NIST によるそうした新たな出版物策定の進展を綿密に追うことが望まれる。

各組織は、パブリックコメント期間中に出版物のドラフトをレビューし、NIST にフィードバックを提供することが推奨される。上記の出版物に加え、多くの NIST 出版物が https://csrc.nist.gov/publications から入手可能である。

本出版物に対するご意見は下記まで：

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

寄せられたすべての意見は、情報公開法（FOIA）[FOIA96]に基づき公開対象である。

コンピュータシステム技術に関する報告

米国国立標準技術研究所（NIST）の情報技術研究所（ITL：Information Technology Laboratory）は、米国の計量と規格に関するインフラにおいて技術的リーダーシップを発揮することにより、米国経済と公共福祉を発展させている。また、ITL は、試験、試験方法、参照データ、概念実証の実施、および技術分析を開発し、情報技術（IT）の開発と生産的利用を促進している。ITL の責務には、連邦政府情報システムにおける国家安全保障関連情報以外の情報を対象とした、費用対効果の高いセキュリティのための管理、運用、技術、および物理的な規格とガイドラインを策定することが含まれる。SP 800 シリーズは、情報システムセキュリティおよびプライバシーに関する ITL の研究、ガイドライン、および普及の取り組みならびに産業界、政府、および学術機関との共同活動について報告する。

摘要

非連邦政府システムおよび組織に存在する「機密指定はされていないが管理対象となる情報」（以降、「管理対象非機密情報」または単に「CUI」（CUI：Controlled Unclassified Information）と記述）を保護することは、連邦政府機関にとって最も重要であり、連邦政府が、その不可欠なミッションおよび機能を成功裏に遂行する能力に直接インパクトを及ぼす可能性がある。本出版物は、以下の場合に CUI の機密性を保護するために推奨される拡張セキュリティ要件を連邦政府機関に提供するものである：(1)情報が非連邦政府システムおよび組織に存在している場合、(2)非連邦政府組織が連邦政府機関に代わって情報を収集または維持していない場合や、政府機関に代わってシステムを使用または運用していない場合、および(3)CUI レジストリに記載されている CUI カテゴリーの認可法、規則、または政府全体のポリシーによって規定された CUI の機密性を保護するための特定の保全要件がない場合。拡張要件は、指定された CUI が重要プログラムや高価値資産に関連している場合に、CUI を処理、保存、伝送する非連邦政府システムのコンポーネント、またはそのようなコンポーネントのセキュリティを保護する非連邦政府システムのコンポーネントに適用される。拡張要件は、NIST SP 800-171 の基本および派生セキュリティ要件を補足し、連邦政府機関と非連邦政府組織との間で締結された契約手段またはその他の合意において、連邦政府機関によって使用されることを意図している。

キーワード

持続的標的型攻撃（APT 攻撃）；基本セキュリティ要件；契約事業者システム；管理対象非機密情報；CUI レジストリ；派生セキュリティ要件；拡張セキュリティ要件；大統領令 13556 号；FIPS 199；FIPS 200；FISMA；NIST SP 800-53；非連邦政府組織；非連邦政府システム；セキュリティアセスメント；セキュリティ管理策 ；セキュリティ要件

謝辞

著者らはまた、NIST コンピュータセキュリティ部門（Computer Security Division）および応用サイバーセキュリティ部門（Applied Cybersecurity Division）の科学者、エンジニア、研究スタッフが、本出版物の内容の改善に多大な貢献をしたことを認めたい。Pat O'Reilly、Jim Foti、Jeff Brewer、Chris Enloe、Ned Goren の各氏、およびすべての NIST ウェブチームの優れた管理サポートに心から感謝する。最後に、国内外の公共および民間分野の個人および組織からの貢献に心からの感謝を表明する。彼らの洞察に満ちた建設的な意見は、本出版物の全体的な品質、網羅性、および有用性を高めるものであった。

特許開示に関する通知

通知：情報技術研究所（ITL）は、本出版物のガイダンスや要件に準拠するために使用が必要となる可能性のある特許請求項の所有者に対して、そうした特許請求項を ITL に開示するよう要請している。ただし、特許所有者は、ITL の要請に応じる義務はなく、ITL は、本出版物に適用される可能性のある特許を特定するための特許調査を実施していない。

本出版物の公開日において、および本出版物のガイダンスや要件に準拠するために使用が必要となる可能性のある特許請求項を特定するよう要請を行った時点において、ITL はそうした特許請求項を特定していない。

ITL は、本出版物の使用に際して特許侵害を回避するにはライセンス許諾が不要であることを、明示的にも暗示的にも表明していない。

本出版物の使用方法

本出版物は、NIST SP 800-171[SP 800-171]の補足資料である。非連邦政府システムおよび組織における管理対象非機密情報（CUI）が、重要プログラムまたは高価値資産に関連している場合に、CUI に対する追加の保護を提供するための拡張セキュリティ要件に関する推奨事項が含まれている。拡張セキュリティ要件は、持続的標的型攻撃（APT 攻撃）に対応し、[SP 800-171]の基本セキュリティ要件と派生セキュリティ要件を補足するように設計されている。[SP 800-171]のセキュリティ要件は主に機密性の保護に重点を置いているが、本出版物における拡張セキュリティ要件は機密性、完全性、および可用性の保護に重点を置いている。基本セキュリティ要件と派生セキュリティ要件は、APT 攻撃に対応するように設計されていないため、それらの要件に加えて拡張セキュリティ要件が実装される。拡張セキュリティ要件は、CUI を処理、保存、伝送する非連邦政府システムのコンポーネント、またはそのようなコンポーネントを保護する非連邦政府システムのコンポーネントに適用される。

本ガイダンスを実施する連邦政府機関によって、*すべて*の拡張セキュリティ要件が選択されることは期待されていない。拡張セキュリティ要件の特定のセットを選択する決定は、連邦政府機関のミッションと事業のニーズに基づき、継続的なリスクアセスメントによって導かれ、情報提供される。重要プログラムまたは高価値資産に関連している CUI を処理、保存、伝送する非連邦政府システムに対する拡張セキュリティ要件は、契約、助成金、またはその他の合意によって連邦政府機関から非連邦政府組織に伝達される。*下請事業者*への拡張セキュリティ要件の適用についても、連邦政府機関は非連邦政府組織と協議して対処する。

拡張セキュリティ要件の適用性

*拡張*セキュリティ要件は、契約、助成金、またはその他の合意で連邦政府機関によって義務付けられている非連邦政府システムまたは非連邦政府組織にのみ適用される。要件は、重要プログラムまたは高価値資産に関連している CUI を処理、保存、伝送する非連邦政府システムのコンポーネント、またはそのようなコンポーネントの保護を提供する非連邦政府システムのコンポーネントに適用される。また要件は、CUI を処理、保存、伝送する外部から提供されるサービスや、セキュリティ保護を提供する外部から提供されるサービスを含む、強化された保護を必要とするシステムのサービスにも適用される。サービスの提供中に処理、保存、伝送される CUI を含む特定のサービスの保護は、そのサービス、またはそのサービスの提供を担当するシステムまたはシステムコンポーネントの拡張セキュリティ要件を実装することによって実現される。

拡張セキュリティ要件は CUI を認可されていない開示から保護するだけでなく、CUI の完全性と可用性を保護するように設計されている。これは、侵入耐性アーキテクチャ、被害局限化運用、およびサイバーレジリエンスと生存可能性の実現に役立つ設計を促進することによって達成される。

*組織システム*という用語は、多くの拡張セキュリティ要件で使用されている。上記のように拡張要件の適用性に関しては、特定の意味を有する。要件に対する適切なスコーピングの考慮事項は、重要プログラムと高価値資産に関連している CUI を保護する責任を負う非連邦政府組織が、保護関連の投資決定を判断する上で、また、セキュリティリスクを管理する上で重要な要素である。

重要インフラのサイバーセキュリティを改善するためのフレームワーク

重要インフラのサイバーセキュリティを改善するための NIST フレームワーク [NIST CSF]を実装している、または実装する予定のある組織は、付属書 C で、本出版物の拡張セキュリティ要件と[SP 800-53]のセキュリティ管理策とのマッピングを参照することができる。セキュリティ管理策とのマッピングは、情報セキュリティプログラムが NIST のセキュリティ管理策を使用して構築されている場合に、その確立された情報セキュリティプログラムの状況に即してセキュリティ要件への準拠を実証したい組織にとって有用である。

目次

正誤表

この表には、SP 800-172 に組み込まれた変更が含まれている。正誤表の更新には、本出版物における*編集上*または*実質的*な訂正、明確化、またはその他の軽微な変更が含まれる。正誤表の更新や改訂でまだ公開されていない、本出版物への潜在的な更新（追加の課題や潜在的な訂正を含む）は特定され次第掲載される。SP 800-172 の出版情報を参照のこと。

日付	種類	変更内容	頁

第 1 章

はじめに

管理対象非機密情報を保護する必要性

今日、連邦政府は、情報システムを使用して連邦政府の様々なミッションおよび事業機能を遂行するために、これまでのどの時代よりも外部サービスプロバイダに依存している[1]。例えば、多くの連邦政府の契約事業者は、連邦政府機関への不可欠な製品とサービスの提供をサポートするために、連邦政府の機微情報をシステム内で日常的に処理、保存、伝送している（例えば、金融サービス、ウェブおよび電子メールサービスの提供、セキュリティクリアランスや医療データの処理、クラウドサービスの提供、通信システム、衛星システム、兵器システムの開発など）。連邦政府の情報は、高い頻度で、州政府や地方自治体、単科大学や大学、独立した研究機関などのエンティティに提供されたり、それらのエンティティと共有されたりする。連邦政府の機微情報が、*非連邦政府システム*[2]および組織に存在している間における保護は、連邦政府機関にとって最も重要であり、連邦政府が指定されたミッションおよび事業運営を遂行する能力に直接インパクトを及ぼすことができる。

非連邦政府システムおよび組織における非機密連邦政府情報の保護は、連邦政府機関が使用する様々なタイプの情報を特定するためのプロセスを提供する連邦政府によって左右される。[EO 13556]は、保護を必要とする非機密情報を行政機関が取り扱う方法を標準化するために、政府全体の管理対象非機密情報（CUI）[3]プログラム[4]を確立した[5]。連邦法、規則、または政府全体のポリシーに従って保全措置または配布管理を必要とする情報のみが CUI に指定される。CUI プログラムは、手順を標準化し、CUI レジストリ[NARA CUI]を通じて共通の定義を提供することにより、一貫性のないマーキング、不適切な保全措置、不必要な制限など、非機密情報の管理と保護におけるいくつかの欠陥に対処するように設計されている。

CUI レジストリは、CUI 執行機関である国立公文書記録管理局（NARA）による発行を含む、CUI の取り扱いに関する情報、ガイダンス、ポリシー、および要件に関するオンラインリポジトリである。CUI レジストリは、承認された CUI カテゴリーを特定し、それぞれの一般的な説明を規定し、管理策の基準を明らかにし、情報のマーキング、保全措置、輸送、配布、再利用、および廃棄などの CUI の使用手順を定めている。

[EO 13556]はまた、CUI プログラムが政府全体のプラクティスの開示性、透明性、統一性を重視し、行政管理予算局（OMB）によって確立された適用可能なポリシー、および国立標準技術研究所（NIST）によって発行された連邦規格およびガイドラインと整合性のある方法でプログラムが実施されることを要求した。CUI 執行機関によって策定された連邦 CUI 規則[6]は、CUI の

[1] 情報システムとは、情報の収集、処理、維持、使用、共有、配布、または廃棄のために明確に組織された個別の一連の情報リソースである。情報システムには、産業用制御システム、プロセス制御システム、サイバーフィジカルシステム、IoT システム、組み込みシステム、デバイスなどの特殊なシステムも含まれる。本出版物では、CUI を処理、保存、伝送できるすべてのタイプのコンピューティングプラットフォームを表すために、システムという用語が使用されている。

[2] 連邦政府情報システムとは、執行機関、執行機関の契約事業者、または執行機関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。そのような基準を満たさないシステムは非連邦政府システムである。

[3] 管理対象非機密情報とは、[EO 13526]または先行／後続の大統領令、もしくは[ATOM54]（その後の改正を含む）で機密指定された情報を除く、法律、規則、または政府全体のポリシーが、保全措置または配布管理を行うことを要求している情報である。

[4] 大統領令 13556 号によって確立された CUI プログラムは、法律、規則、および政府全体のポリシーに従った、およびそれらに一致する保全措置または配布管理を必要とする非機密情報を、執行機関が取り扱う方法を標準化している。

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

[6] [32 CFR 2002]は 2016 年 9 月 14 日に公布され、2016 年 11 月 14 日に施行された。

指定、保全、配布、マーキング、管理解除、および廃棄に関するガイダンスを連邦政府機関に提供し、自己検査および監督要件を定め、プログラムの他の側面についての説明している。

特定の状況では、CUI が重要プログラム[7]または高価値資産[8]に関連している場合がある。これらの重要プログラムと高価値資産は、持続的標的型攻撃（APT 攻撃）の潜在的な標的である。APT 攻撃は、サイバー攻撃、物理的手段、欺瞞など、複数の攻撃ベクトルを使用して目的を達成する機会を創出できる専門知識とリソースを備えた敵対者または敵対者グループによる攻撃である。APT 攻撃の目的には、情報を漏出させること;ミッション、機能、プログラム、組織の重要な側面を弱体化または妨害すること;もしくは、将来的にこれらの目的を実行するために自らを配置すること、などを目的として標的組織のインフラ内に足場を確立することが含まれる。。APT 攻撃は、長期間にわたって繰り返しその目的を追求し、攻撃に抵抗する防御側の取り組みに適応し、その目的を実行するために必要な相互作用のレベルを確固として維持する。CUI のカテゴリー自体は、それほど大きな保護を必要としていないが、重要プログラムまたは高価値資産に関連している CUI は、APT 攻撃がそのような情報を標的とする可能性が高く、より大きなリスクにさらされるため、追加の保護が必要となる。

CUI の拡張セキュリティ要件

管理対象非機密情報は、そのような情報が連邦政府機関に属する連邦政府システムに存在する場合でも、非連邦政府組織に属する非連邦政府システムに存在する場合でも、*同じ価値*を有する。したがって、本出版物に記載されている拡張セキュリティ要件は、CUI を保護するために連邦政府機関が使用するガイドラインと一致しており、それを補完している。本要件は、契約、助成金、またはその他の合意において連邦政府機関によって*義務付けられている*非連邦政府システムまたは非連邦政府組織に*のみ適用される*。

組織は、従来の情報技術（IT）システム、運用技術（OT）システム、モノのインターネット（IoT）システム、および産業用 IoT（IIoT）システムを含むあらゆるタイプのシステムに大きく依存しているため、APT 攻撃は米国の国家安全保障および経済安全保障上の利益にとって極めて危険である。これらのタイプのシステムの融合により、*サイバーフィジカルシステム*と呼ばれる新しいクラスのシステムが生まれ、その多くはエネルギー、輸送、防衛、製造、医療、金融、情報通信など、米国の重要インフラの分野に存在する。したがって、重要プログラムまたは高価値資産に関連する上記のいずれかのシステムによって処理、保存、伝送される CUI には、APT 攻撃に対する追加の保護が必要である。

1.1 目的および適用性

本出版物の目的は、(1)CUI が非連邦政府システムおよび組織に存在している場合、(2)非連邦政府組織が連邦政府機関に代わって情報を収集または維持して*いない*場合や、政府機関

[7] 重要プログラムの定義は組織によって異なる場合がある。例えば、国防総省は、重要プログラムを、ケイパビリティとミッションの有効性を大幅に向上させる、または不可欠なシステム／ケイパビリティの期待される有効寿命を延長するプログラムと定義している[DOD ACQ]。

[8] [OMB M-19-03]および[OCIO HVA]を参照。

に代わってシステムを使用または運用して*いない*場合[9]、および(3)CUI レジストリに記載されている CUI カテゴリーの認可法、規則、または政府全体のポリシーによって規定された CUI を保護するための特定の保全要件がない場合における、CUI の*機密性*、*完全性*、および*可用性*を保護するための一連の拡張セキュリティ要件[10]を連邦政府機関に提供することである[11]。拡張セキュリティ要件は、(1)侵入耐性アーキテクチャ、(2)被害局限化運用、および(3)サイバーレジリエンスと生存可能性を達成するための設計を促進することにより、CUI の保護に対処する[12]。拡張セキュリティ要件は、[SP 800-171]の基本セキュリティ要件と派生セキュリティ要件を補足することを目的としており、連邦政府機関と非連邦政府組織との間で締結された契約手段またはその他の合意において、連邦政府機関によって使用される。

拡張セキュリティ要件は、重要プログラムまたは高価値資産に関連している CUI を処理、保存、伝送する、またはそのようなコンポーネント[13]のセキュリティ保護を提供する非連邦政府システムのコンポーネントに適用される。非連邦政府組織が、重要プログラムまたは高価値資産に関連している CUI の処理、保存、伝送のための特定のシステムコンポーネントを指定する場合、それらの組織は、指定されたシステムコンポーネントを別の CUI セキュリティドメインに分離することによって、拡張セキュリティ要件の範囲を限定することができる。分離は、アーキテクチャと設計の概念を適用することによって実現できる（例えば、ファイアウォールやその他の境界保護デバイスを使用してサブネットワークを実装し、情報フロー制御メカニズムを使用するなど）。セキュリティドメインには、物理的な分離、論理的な分離、またはその両方の組み合わせを採用する場合がある。このアプローチは CUI を適切に保護し、組織のセキュリティ態勢を、そのミッション、運営、資産の保護に必要なレベル以上にまで高めることを回避することができる。

本出版物は、組織のどのプログラムまたは資産が重要または*高価値*であると判断されるのかについてのガイダンスは提供していない。これらの決定は、追加の保護のための拡張セキュリティ要件の使用を義務付ける組織によって行われ、法律、大統領令、指令、規則、またはポリシーによって通知され、導かれることができる。さらに、本出版物は、拡張セキュリティ要件の使用を正当化する特定のタイプの脅威または攻撃シナリオに関するガイダンスも提供していない。最後に、すべての拡張セキュリティ要件があらゆる状況で必要になるとは期待されていない。むしろ、選択の決定は、ミッションと事業のニーズとリスクに基づいて組織によって行われる。

---

[9] 連邦政府機関に代わって情報を収集または維持する、もしくは政府機関に代わってシステムを使用または運用する非連邦政府組織は、[FISMA]および[FIPS 200]の要件ならびに[SP 800-53]のセキュリティ管理策に準拠しなければならない([44 USC 3554] (a)(1)(A)を参照)。

[10] 本ガイドラインでは、要件という用語は、特定のシステムや組織における一連の利害関係者保護のニーズを表現するために使用される。利害関係者保護のニーズとそれに対応するセキュリティ要件は、多くのソース（法律、大統領令、指令、規則、ポリシー、基準、ミッションおよび事業のニーズ、またはリスクアセスメントなど）から導出される場合がある。要件という用語には、法的要件とポリシー要件の両方に加えて、他のソースから導出される場合があるより広範な利害関係者保護のニーズの表現も含まれる。これらの要件のすべてをシステムに適用すると、システムに必要な特徴を判断するのに役立つ。

[11] 本出版物の要件は、政府機関の責任者が、その管理下にある、非連邦政府システムおよび組織に存在する CUI を含む、運営および資産をサポートする情報に対して情報セキュリティを提供する FISMA 要件に準拠するために使用することができる（[44 USC 3554] (a)(1)(A)および(a)(2)を参照）。

[12] 機密性の保護を達成するために使用される手段の完全性と可用性を保護することは、本出版物の範囲内である。本出版物の明確な目的の範囲外ではあるが、APT 攻撃は、CUI としてカテゴライズされるミッションまたはビジネスソフトウェアなどの、ミッションや事業機能が依存する CUI の完全性と可用性を侵害することにより、組織、個人、または国家に損害を与えようとする場合がある。

[13] システムコンポーネントには、メインフレーム、ワークステーション、サーバ、入出力デバイス、サイバーフィジカルコンポーネント、ネットワークコンポーネント、モバイルデバイス、オペレーティングシステム、仮想マシン、およびアプリケーションが含まれる。

1.2 対象読者

本出版物は、公共および民間部門の以下に該当する個人や組織を対象としている。

- システム開発ライフサイクルの責任者（プログラムマネージャー、ミッションオーナー、事業オーナー、情報オーナー、情報スチュワード、システム設計者、システム開発者、システムエンジニア、セキュリティエンジニア、システムインテグレータ、など）
- システム、セキュリティ、またはリスクマネジメントおよび監督の責任者（認可権限のある担当者、最高情報責任者、最高情報セキュリティ責任者、システムオーナー、情報セキュリティマネージャー、など）
- セキュリティアセスメントおよび監視の責任者（監査人、システム評価者、アセッサー、独立した検証および妥当性確認者、アナリストなど）
- 購買または調達の責任者（契約担当官、など）

上記の役割と責任は、異なる二つの視点から見ることができる。一つは、契約手段またはその他のタイプの組織間合意においてセキュリティ要件を確立し、伝達するエンティティとしての*連邦政府の視点*であり、もう一つは、契約または合意に定められたセキュリティ要件に対応し、それに準拠するエンティティとしての*非連邦政府の視点*である。

1.3 本出版物の構成

本出版物の第 2 章以降は、次のように構成される。

- **第 2 章**では、CUI を保護するための拡張セキュリティ要件の策定に使用される基本的な前提事項、要件の構成と構造、および要件の適用における柔軟性について説明する。
- **第 3 章**では、非連邦政府システムおよび組織における CUI を保護するための拡張セキュリティ要件の 14 のファミリーについて説明する。
- 補足資料である付属書は、CUI の保護に関連する追加情報を提供する。これらには、参照資料、用語集、略語、およびマッピング表が含まれる。マッピング表では、拡張セキュリティ要件を[SP 800-53]のセキュリティ管理策に関連付けており、また、拡張セキュリティ要件が侵入耐性アーキテクチャ、被害局限化運用、およびサイバーレジリエンスと生存可能性のための設計を促進するかどうかを示している。

第 2 章

基本的事項

拡張セキュリティ要件を策定するための前提事項

本章では、非連邦政府システムおよび組織における CUI を保護するための拡張セキュリティ要件を策定するために使用されるアプローチについて説明する。また、拡張セキュリティ要件の構成と構造についても説明し、付属書 C のセキュリティ管理策マッピング表へのリンクを提供する。

2.1 策定アプローチ

本出版物で説明する拡張セキュリティ要件は、次の 4 つの基本的な前提事項に基づいて策定されている。

- CUI の保護に関する法的および規則上の要件は、そのような情報が連邦政府または非連邦政府のシステムおよび組織に存在するかどうかにかかわらず、*一貫している*。
- CUI を保護するために実施される保全措置は、連邦政府および非連邦政府のシステムならびに組織において*一貫している*。
- CUI のインパクト値は少なくとも[FIPS 199]「*中(moderate)*」である[14]。

重要プログラムまたは高価値資産に関連している CUI を保護するには、追加の保護が必要である[15]。

- これらの前提事項は、CUI が連邦政府組織または非連邦政府組織のどちらに存在するかどうかにかかわらず、CUI は同じ*価値*であり、侵害された場合には、*有害なインパクト*を及ぼす可能性がある、という概念を補強する。拡張セキュリティ要件の策定と、非連邦政府組織と協力する際の連邦政府機関の期待にもインパクトを及ぼす追加の前提事項には、次のようなものが含まれる。非連邦政府組織は、自らの情報を保護するための特定の保全措置を講じている。これは、拡張セキュリティ要件を満たすのに十分な場合もある。
- 非連邦政府組織は、様々なセキュリティソリューションを直接実装するか、外部サービスプロバイダ(マネージドサービスなど)を使用して、拡張セキュリティ要件を満たすことができる。
- 非連邦政府組織は、特定の拡張セキュリティ要件を満たすために必要な組織構造またはリソースを持っていない場合があり、要件の意図を満たすために代替的であるが同等に効果的なセキュリティ対策を実装する場合がある。
- 連邦政府機関は、適切な契約またはその他の合意で、適用される拡張セキュリティ要件に対して組織が定めるパラメータを規定する。

[14] [32 CFR 2002]に従って、CUI は少なくとも「中」の機密性インパクト値にカテゴライズされる。ただし、CUI の管理策を定める連邦法、規則、または政府全体のポリシーで、「中」の機密性ベースラインの管理策とは異なる管理策が指定されている場合は、これらに従う。

[15] 重要プログラムや高価値資産に関連している CUI は、APT 攻撃の標的となる可能性が高く、より大きなリスクにさらされるため、そうした CUI を保護するには、追加の保護が必要となる。

拡張セキュリティ要件は、相互に支援し補強する3つのコンポーネントを含む多次元の多層防御戦略の基盤を提供する：(1)*侵入耐性アーキテクチャ*、(2)*被害局限化運用*、および(3)*サイバーレジリエンスと生存可能性*のための設計[SP 800-160-2]。この戦略は、組織によって実装された最善の保護措置にもかかわらず、APT 攻撃が境界防御を侵害またはブリーチし、防御側のシステム内に悪意のあるコードを展開する方法を見つける場合があることを認識している。このような状況が発生した場合、組織は、敵対者を検知し、打ち負かし、混乱させ、欺き、誤解させ、防止する、すなわち、敵対者の戦術的優位性を取り除き、組織の重要プログラムと高価値資産を保護するための保全措置と対策にアクセスできなければならない。図 1 は、多次元的な資産防御戦略の一部として実装された場合の、拡張セキュリティ要件の補完的な性質を示している。

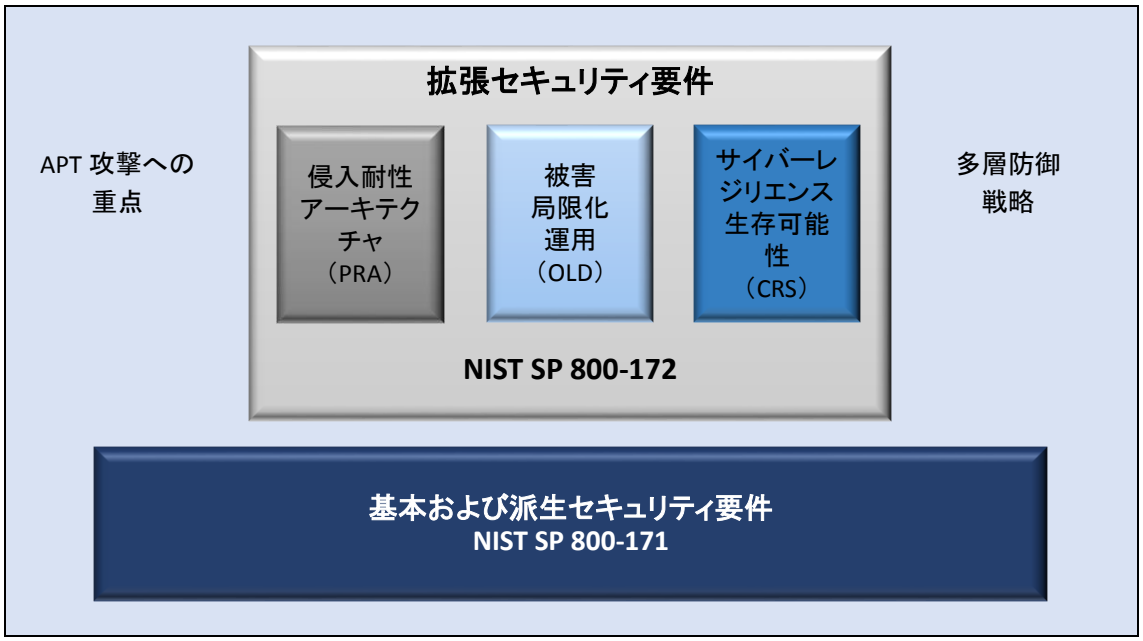

図 1：多次元（多層）防御戦略

拡張セキュリティ要件は包括的に実装できるが、組織は、包括的なリスクマネジメント戦略の一環として、セキュリティ要件のサブセットを選択しても良い。ただし、選択プロセスに影響を与える特定の要件の間には依存関係がある。拡張セキュリティ要件は、連邦政府機関と非連邦政府組織との間で締結された契約手段またはその他の合意において、連邦政府機関によって使用されることを意図している。選択された要件に関する具体的な実装ガイダンスは、そうした契約手段または合意によって連邦政府機関から非連邦政府組織に提供することができる。

拡張セキュリティ要件は、[SP 800-53]のセキュリティ管理策から派生している。この要件は、高度なサイバー脅威からのサイバー攻撃から情報（および、特に CUI）を保護し、攻撃を受けている間のシステムや組織のサイバーレジリエンスを確保するための方法を表している。拡張セキュリティ要件は、APT 攻撃に対処するために不可欠な次の主要な要素に焦点を当てている。

- 脅威中心のアプローチをセキュリティ要件仕様に適用する。
- システムおよびネットワークのセグメンテーション技術、仮想マシン、およびコンテナを使用して、論理的および物理的な分離をサポートするシステムおよびセキュリティアーキテ

クチャを採用する[16]。

- 最も重要または機微な操作に対して二重認可の管理策を実装する。
- 永続的なストレージを、隔離されたエンクレーブ（enclave）またはドメインに限定する。
- システムとネットワークに対する接続のための準拠（comply-to-connect）アプローチを実装する。
- システムおよびシステムコンポーネントへの変更に対応するための信頼できるソースを確立することにより、構成管理要件を拡張する。
- 組織のシステムおよびシステムコンポーネントを既知の状態に定期的にリフレッシュまたはアップグレードするか、新しいシステムまたはコンポーネントを開発する。
- 高度な分析機能を備えたセキュリティオペレーションセンターを採用し、組織のシステムの継続的な監視と保護をサポートする。
- 敵対者が意思決定に使用する情報、敵対者が漏出させようとする情報の価値と真正性、または敵対者が活動している環境に関して、敵対者を混乱させ、誤解させる欺瞞を使用する。

2.2 構成および構造

拡張セキュリティ要件は、基本要件と派生要件のファミリーに一致する 14 の*ファミリー*に構成されている。各ファミリーには、ファミリーの一般的なセキュリティの主題に関連する要件が含まれている。ファミリーは、[FIPS 200]における連邦政府情報および情報システムの最小限のセキュリティ要件と密接に関わっている。*緊急時対応計画*、*システムおよびサービスの取得*、および*計画*に関するセキュリティ要件は、[SP 800-171]のテーラリング基準のため、本出版物の範囲内には含まれていない。表 1 は、本出版物で取り上げられているセキュリティ要件ファミリーを示している[17]。

表 1：セキュリティ要件ファミリー

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

[16] [SP 800-160-1]は、システムおよびセキュリティアーキテクチャの策定に関するガイダンスを提供している。
[17] 「監査および説明責任」、「メンテナンス」、「媒体保護」、および「物理的保護」のファミリーは、現時点では、拡張セキュリティ要件を含んでいない。

拡張セキュリティ要件の構造は、[SP 800-171]の基本および派生セキュリティ要件に類似している。一部の要件では、組織が指定されたパラメータに対して特定の値を規定できるようにすることで、さらなる柔軟性が提供されている。柔軟性は、特定の要件に組み込まれた*設定*および*選択*操作を使用して実現される。設定および選択操作は、組織の保護のニーズに基づいて、拡張セキュリティ要件をカスタマイズするケイパビリティを提供する。組織が定めるパラメータ値の決定は、法律、大統領令、指令、規則、ポリシー、基準、ガイダンス、ミッションまたは事業ニーズによって導かれ、情報提供される。リスクアセスメントとリスク許容度も、要件のパラメータ値を規定する上で重要な要素である。一度指定されると、設定および選択操作の値は要件の一部になる[18]。

各拡張セキュリティ要件に続いて、*詳解セクション*は、要件の実装を促進するための追加情報を提供する。この情報は、主に[SP 800-53]のセキュリティ管理策の詳解セクションから得られたもので、CUI を保護するために使用される管理策の実装に使用できるメカニズムと手順について、組織がより理解を深めることができるようにするために提供されている。詳解セクションは、情報提供のみを目的としており、拡張セキュリティ要件の範囲を拡張することを意図したものでは**ない**。詳解セクションには、有益な*参照情報*も含まれている。

最後に、*保護戦略と敵対者への効果*のセクションでは、特に、脅威イベントの発生の可能性、脅威イベントが損害を与える能力、およびその損害の程度を低減させることによって、拡張セキュリティ要件の実装がリスクに及ぼす潜在的影響について説明する。敵対者に対する望ましい影響として、5 つの高レベルの影響（*リダイレクト*、*排除*、*防止*、*限定*、および*暴露*）を特定することができる。それぞれの敵対者への効果はさらに分解され、具体的なリスクに対するインパクトと期待される結果が含まれる。これらの敵対者への効果は、[SP 800-160-2]および付属書 D に記載されている。

設定および選択操作

指定された拡張セキュリティ要件における*設定*および*選択*操作のパラメータ値は、管轄連邦政府機関によって決定される。ただし、パラメータ値は非連邦政府組織と調整することが望ましい。これは、パラメータ値が、非連邦政府組織またはシステム内の特定の特性、属性、または条件（システムアーキテクチャ、設計、実装など）に左右される状況を反映している。

基本要件や派生要件と同様に、拡張セキュリティ要件は、要件のソースである[SP 800-53]のセキュリティ管理策にマッピングされている。表 C-1 から表 C-14 に記載されているマッピングは、情報提供のみを目的として提供されており、関連する管理策は追加の要件を提供していないことに注意されたい[19]。

[18] 要件（特定のパラメータ値を含む）は、契約、助成金、またはその他の合意で連邦政府機関によって表明される。パラメータ値は、システムアーキテクチャ、設計、または実装に関する潜在的な問題に対処するために、非連邦政府組織と調整することが望ましい。

[19] 表 C-1 から表 C-14 のセキュリティ管理策は[SP 800-53]から引用されている。

図 2 は、拡張セキュリティ要件の例を示している。

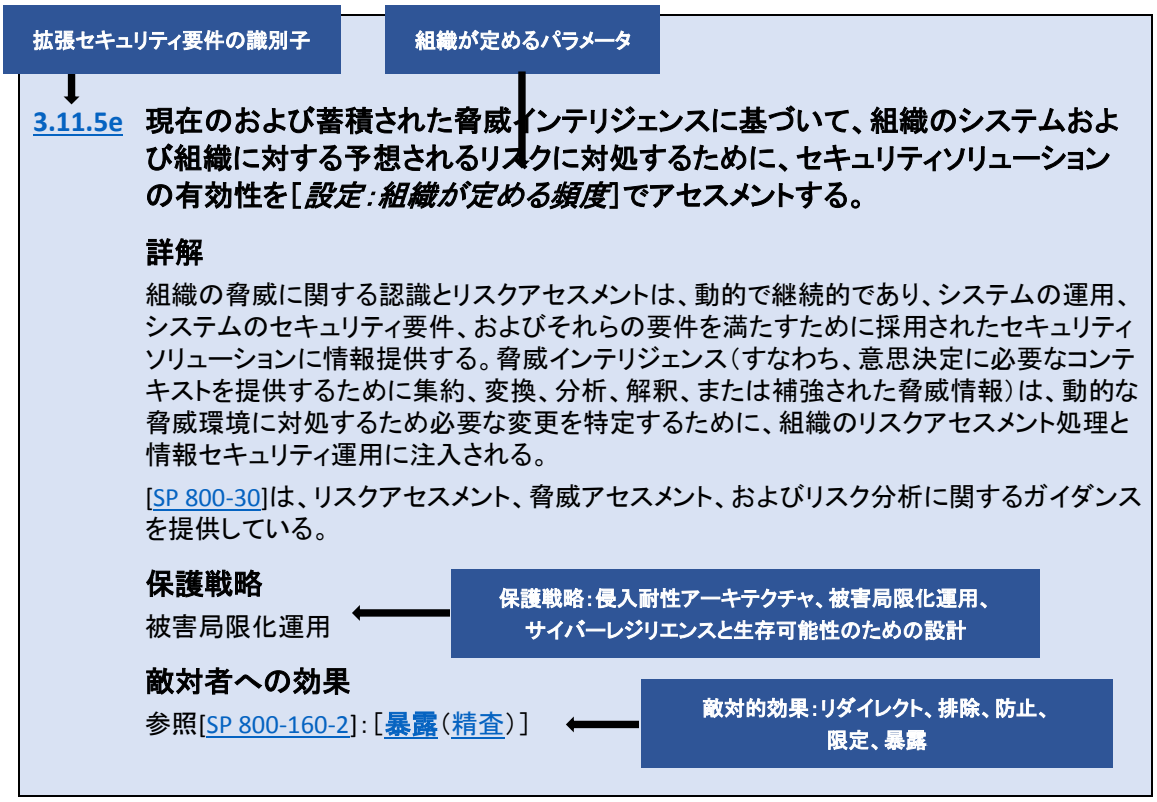

図 2:拡張セキュリティ要件の例

2.3 柔軟な適用

拡張セキュリティ要件は、重要プログラムまたは高価値資産に関連している CUI を保護するために、必要に応じて適用される。連邦政府機関は、重要プログラムまたは高価値資産に関連している CUI を処理、保存、伝送する非連邦政府システムのコンポーネント;そのようなコンポーネントを保護する非連邦政府システムのコンポーネント;または、そのようなコンポーネントへの直接的な攻撃経路を提供する(例えば、システムコンポーネント間の信頼関係が確立されているため)非連邦政府システムのコンポーネント、に対して拡張セキュリティ要件を適用しているなど、必要な保護が達成されている場合に限り、適用を限定しても良い[20]。

*すべての*拡張セキュリティ要件が各連邦政府機関によって選択されることは期待されていない。拡張セキュリティ要件を選択する決定は、政府機関、政府機関のグループ、または連邦政府(すなわち、連邦政府エンティティ)の特定のミッションと事業保護のニーズに基づいて行われ、継続的なリスクアセスメントによって導かれ、情報提供される。重要プログラムまたは高価値資産に関連している CUI を処理、保存、伝送する非連邦政府システムのための拡張セキュリティ要件の選択は、契約、助成金、またはその他の合意で連邦政府エンティティから非連邦政府組織に伝達される。*下請事業者*への拡張セキュリティ要件の適用に関しても、連

[20] システムコンポーネントには、メインフレーム、ワークステーション、サーバ、入出力デバイス、ネットワークコンポーネント、オペレーティングシステム、仮想マシン、アプリケーション、サイバーフィジカルコンポーネント(プログラマブルロジックコントローラ(PLC)や医療デバイスなど)、モバイルデバイス(スマートフォンやタブレットなど)が含まれる。

邦政府エンティティが非連邦政府組織と協議して対処される。

拡張セキュリティ要件の中には、組織が内部で満たすことが困難またはコストが高すぎるものがある。このような場合、外部サービスプロバイダ[21]の活用により要件を満たすことができる。サービスには以下が含まれるが、これらに限定されない。

- 脅威インテリジェンス[22]
- 脅威および敵対者のハンティング
- システム監視およびセキュリティ管理[23]
- IT インフラ、プラットフォーム、ソフトウェアサービス
- 脅威、脆弱性、リスクのアセスメント
- 対応および復旧[24]
- サイバーレジリエンス[25]

最後に、拡張セキュリティ要件に関連する具体的な実装ガイダンスは、本出版物の範囲外である。組織は、拡張セキュリティ要件を満たすために使用される方法、技法、技術、およびアプローチについて最大限の柔軟性を有している[26]。

連邦政府機関向けの実装に関するヒント

1. 非連邦政府システムまたは組織の CUI を保護するために必要な一連の拡張セキュリティ要件を**選択する**。
2. 政府機関によって選択された一連の拡張セキュリティ要件で、設定および選択操作（該当する場合）を**完了する**。
3. 必要に応じて、非連邦政府組織向けの実装ガイダンスを**策定する**。
4. 非連邦政府組織との政府契約またはその他の合意に、拡張セキュリティ要件と実装ガイダンスを**含める**。

[21] これらのサービスは、親組織または監督組織（例えば、下請事業者にサービスを提供する主契約事業者）またはサードパーティ（例えば、クラウドサービスプロバイダ）によって提供することができる。
[22] [SP 800-150]は、脅威情報と脅威インテリジェンスを区別している。脅威情報とは、組織が脅威から組織自身を防御する、または脅威行為者の行為を検知するのに役立つ可能性のある、脅威に関連するあらゆる情報である。脅威インテリジェンスとは、リスクベースの意思決定プロセスに必要なコンテキストを提供するために集約、変換、分析、解釈、または補強された脅威情報である。
[23] マネージドセキュリティサービスプロバイダ（MSSP）は、複数の顧客または下位組織に代わってアナリストがセキュリティ関連のデータフローを監視するオフサイトのセキュリティオペレーションセンター（SOC）を提供することができる。最適なサービスは、境界防御の監視にとどまらず、組織のシステムやネットワークの奥深くからシステムコンポーネント、デバイス、エンドポイントデータを監視する。
[24] 場合によっては、MSSP 組織は、検知および対応のマネージドサービス（MDR）プロバイダと同様に、統合されたセキュリティ関連の管理およびインシデント対応サービスを提供する。あるいは、対応および復旧サービスを別々に取得することもできる。
[25] [SP 800-160-2]は、サイバーレジリエントなシステムに関するガイダンスを提供している。
[26] このようなガイダンスは、連邦政府機関と非連邦政府組織との間で締結された契約手段またはその他の合意に含めることができる。

第 3 章

要件

持続的標的型攻撃（APT 攻撃）に対する拡張セキュリティ要件

この章では、APT 攻撃[27]から非連邦政府システムおよび組織における CUI の機密性、完全性、および可用性を保護するための拡張セキュリティ要件について説明する。拡張セキュリティ要件は、CUI の特定のカテゴリーや項目に対しては必要とされていない。しかし、連邦政府機関が、CUI が重要プログラムまたは高価値資産に関連していると判断した場合[28]、そのような情報およびそのような情報を処理、保存、伝送するシステムは APT 攻撃の潜在的な標的であるため、強化された保護が必要になる場合がある。拡張セキュリティ要件を通じて表現されるこのような保護は、契約、助成金、またはその他の合意において連邦政府機関によって義務付けられている。[SP 800-171]に含まれる基本要件と派生要件は APT 攻撃に対応するようには策定されていないため、それらの要件に加えて拡張セキュリティ要件が実装される[29]。

それぞれの拡張セキュリティ要件に関連して、要件が 3 つの保護戦略領域（侵入耐性アーキテクチャ、被害局限化運用、サイバーレジリエンスと生存可能性のための設計）のうち、どの領域をサポートしているのか、および、要件が敵対者にどのような潜在的影響を与えるのかが識別されている。この情報は、要件が適切かどうかを組織が確認する際に役立つように含まれている。理想的には、選択した要件は、3 つの戦略領域でバランスが取れていることが望ましい。1 つの領域にのみ該当する要件を選択した場合、APT 攻撃に対処するための対応戦略のバランスが崩れてしまう可能性がある。同様に、敵対者への潜在的影響に関して、組織は、特定のミッションや事業目的を考慮して、敵対者に対して可能な限り広範な一連の影響を与えるようにすることが望ましい。

[27] [SP 800-39]は、APT 攻撃を、高度なレベルの専門知識と莫大なリソースを保有し、サイバー攻撃、物理攻撃、詐欺などの複数の攻撃ベクトルを使用して目的を達成する機会を生み出す敵対者、と定義している。

[28] [OMB M-19-03]を参照。

[29] 拡張セキュリティ要件は、[NTCTF]で説明されている脅威に対処するために策定された。

3.1 アクセス制御

拡張セキュリティ要件

3.1.1e **重要または機微なシステムおよび組織の運営を実行するために、二重認可を採用する。**

詳解

二重認可は、二者管理としても知られ、インサイダー脅威に関連するリスクを低減する。二重認可は、特定のコマンド、措置、または機能を実行するために、二人の認可された個人の承認を必要とする。例えば、組織は二重認可を採用して、資格のある二人の個人が承認しない限り、選択したシステムコンポーネント（ハードウェア、ソフトウェア、ファームウェアなど）または情報の変更を行えないようにすることを確実にする。これらの個人は、提案された変更が、承認された変更の正しい実装であるかどうかを判断するためのスキルと専門知識を有しており、それらの変更に対しても責任を負う。別の例として、特権コマンドの実行に二重認可を採用する場合がある。共謀のリスクを軽減するために、組織は、割り当てられた二重認可の職務をローテーションし、インサイダー脅威のリスクを減らすことを考慮する。二重認可は、技術的または手続き的な手段を介して実装することができ、順次または並行して実施することができる。

保護戦略

侵入耐性アーキテクチャ; 被害局限化運用

敵対者への効果

参照[SP 800-160-2]: [**排除**（先制）; **防止**（徒労）]

3.1.2e **システムおよびシステムコンポーネントへのアクセスを、組織により所有、支給、または発行された情報リソースのみに制限する。**

詳解

組織により所有、支給、または発行されていない情報リソースには、他の組織が所有するシステムまたはシステムコンポーネントおよび個人所有のデバイスがある。非組織の情報リソースは、組織に重大なリスクをもたらし、「接続のための準拠（comply-to-connect）」ポリシーを採用する能力、または組織のシステムの完全性を確保するためのコンポーネントまたはデバイス証明技法を実装する能力を複雑なものにする。

保護戦略

侵入耐性アーキテクチャ

敵対者への効果

参照[SP 800-160-2]: [**排除**（先制）; **防止**（封じ込め、徒労）]

3.1.3e **接続されたシステムのセキュリティドメイン間の情報フロー制御のために、[*設定：組織が定めるセキュアな情報転送ソリューション*]を採用する。**

詳解

組織は、システム内の指定された発信元と宛先の間、および接続されたシステム間の情報フローを制御するために情報フロー制御ポリシーと実施のメカニズムを採用する。フロー制御は、情報または情報パス、あるいはその両方の特性に基づいている。例えば、境界保護デバイスでは、ルールセットを採用したり、システムサービスを制限する構成設定を確立したり、ヘッダー情報に基づいてパケットフィルタリングケイパビリティを提供したり、メッセージの内容に基づいてメッセージフィルタリングケイパビリティを提供したりすることで実施される。組織は、情報フローの実施に重要なフィルタリングおよび検査のメカニズム（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）の統合的信頼性についても検討する。

異なるセキュリティポリシーを有する異なるセキュリティドメインのシステム間で情報を転送す

ると、そのような転送が 1 つまたは複数ドメインのセキュリティポリシーに違反するリスクが生じる。このような状況では、情報オーナーまたはスチュワードは、接続されたシステム間の指定されたポリシー実施拠点におけるガイダンスを提供する。組織は、異なるセキュリティドメイン内のシステム間で論理的または物理的な分離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。実施には、接続されたシステム間の情報転送を禁止すること、一方向の情報フローを実施するためのハードウェアによるメカニズムを採用すること、別のセキュリティドメインまたは接続されたシステムから情報を受け入れる前に書き込み許可を検証すること、およびセキュリティ属性とラベルを再設定するための信頼性のある再評価のメカニズムを実装することなどが含まれる。

セキュアな情報転送ソリューションには、多くの場合、次の 1 つ以上の特性が含まれている: セキュリティドメインを横断する場合のクロスドメインソリューションの利用、送信者と受信者の相互認証（ハードウェアベースの暗号技術の利用）、転送中および保存時のデータの暗号化、他のドメインからの分離、情報転送のロギング（ファイルタイトル、ファイルサイズ、ファイルの暗号化ハッシュ、送信者、受信者、転送時刻および転送 IP アドレス、受信時刻および受信 IP アドレスなど）。

保護戦略

侵入耐性アーキテクチャ

敵対者への効果

参照[SP 800-160-2]: [**排除**（先制）; **防止**（封じ込め、徒労）]

3.2 意識向上およびトレーニング

拡張セキュリティ要件

3.2.1e **ソーシャルエンジニアリング、持続的標的型攻撃の行為者、ブリーチ、および疑わしい行動からの脅威の認識と対応に重点を置いた意識向上トレーニングを[*設定：組織が定める頻度*]で提供する。意識向上トレーニングを[*設定：組織が定める頻度*]で、または脅威に重大な変更がある場合に、更新する。**

詳解

APT 攻撃行為を検知し、攻撃行為の有効性を低下させる効果的な方法は、個人に対して特定の意識向上トレーニングを提供することである。十分な訓練を受けセキュリティ意識の高い要員は、電子メールまたは Web アプリケーションを介した悪意のあるコードインジェクションから組織を保護する多層防御戦略の一環として用いられる別の組織的な保全措置を提供する。脅威に対する意識向上トレーニングには、ウェブサイト、電子メール、広告ポップアップ、記事、ソーシャルエンジニアリングなど APT 攻撃者が組織に侵入する様々な方法について、個人を教育することが含まれる。トレーニングには、疑わしい電子メールを見分ける技法、セキュアでない設定でのリムーバブルシステムの使用、職場外の敵対者による個人への潜在的な標的化の可能性などを含めることができる。特に脅威は絶えず、そしてしばしば急速に進化しているため、意識向上トレーニングを定期的にアセスメントおよび更新して、トレーニングが適切で効果的であることを確実にする。

[SP 800-50]は、セキュリティ意識向上およびトレーニングプログラムに関するガイダンスを提供している。

保護戦略

被害局限化運用

敵対者への効果

参照[SP 800-160-2]: [**防止**（徒労）; **暴露**（検知）]

3.2.2e **[*設定：組織が定める役割*]に対する意識向上トレーニングに現在の脅威シナリオに沿った実践的な演習を含め、トレーニングに関与する個人およびその監督者にフィードバックを提供する。**

詳解

意識向上トレーニングは、脅威の戦術、技法、手順（TTP）にテーラリングした実践的な演習によって補完される場合に最も効果的となる。実践的な演習の例としては、認可されていないアクセスや情報収集を目的としたソーシャルエンジニアリングの試みや、悪意のある電子メールの添付ファイルの開封やスピアフィッシング攻撃を介した悪意のある Web リンクの呼び出しによる有害なインパクトをシミュレートすることなどが含まれる。ユーザの望ましい行動を強化するためには、迅速なフィードバックが不可欠である。トレーニング結果、特に重要な役割を担う職員の失敗は、潜在的に深刻な問題を示している可能性がある。上級管理職にそのような状況を認識させ、適切な改善措置を講じることが重要である。

[SP 800-181]は、仕事の役割を介したサイバーセキュリティの仕事を説明する用語集と分類を含む、役割ベースのセキュリティトレーニングに関するガイダンスを提供している。

保護戦略

被害局限化運用

敵対者への効果

参照[SP 800-160-2]：[**防止**（徒労）；**暴露**（検知）]

3.3 監査および説明責任

拡張セキュリティ要件

監査および説明責任に関する拡張セキュリティ要件はない。

3.4 構成管理

拡張セキュリティ要件

3.4.1e 承認および実装されたシステムコンポーネントに対して信頼できるソースおよび説明責任を提供するために、信頼できるソースおよびリポジトリを確立し維持する。

詳解

信頼できるソースおよびリポジトリの確立および維持には以下が含まれる。(1)承認されたハードウェア、ソフトウェア、ファームウェアのシステムコンポーネントのインベントリ；(2)承認されたシステムベースライン構成および構成変更；(3)検証されたシステムソフトウェアおよびファームウェア；(4)システムイメージおよび／またはスクリプトなど。信頼できるソースは、リポジトリ内のソフトウェア、構成、またはデータに対する変更や変更の試みをロギングするための完全性の管理策を実装する。さらに、リポジトリへの変更は、変更管理手順の対象とし、変更を要求するユーザの認証を要求する。状況によっては、このような変更に対して、組織は二重認可を要求してもよい。リポジトリを更新する場合、および既知の信頼できるソースからシステムをリフレッシュする場合に、変更が正当であることを確実にするために、ソフトウェアの変更は、完全性と真正性について定期的にチェックされる。リポジトリ内の情報は、規定された構成ベースラインへの準拠を示したり、規定された構成ベースラインからの逸脱を識別したり、信頼できるソースからシステムコンポーネントを復元したりするために使用される。自動化されたアセスメントの観点から、信頼できるソースから提供されるシステム記述は、望ましい状態と呼ばれる。望ましい状態は、準拠または逸脱をチェックするために、実際の状態と比較される。[SP 800-128]は、セキュリティ構成設定や構成変更管理など、セキュリティ構成管理に関するガイダンスを提供している。

[IR 8011-1]は、システムおよびシステムコンポーネントの構成をアセスメントするための自動化サポートに関するガイダンスを提供している。

保護戦略

侵入耐性アーキテクチャ；サイバーレジリエンスと生存可能性のための設計

敵対者への効果

参照[SP 800-160-2]：[**防止**（徒労）；**限定**（短縮）；**暴露**（検知）]

3.4.2e **誤った構成または認可されていないシステムコンポーネントを検知するために、自動化されたメカニズムを採用する。検知後、パッチ適用、再構成、またはその他の緩和策を促進するために、[*選択（1 つ以上）：コンポーネントを取り除く；コンポーネントを検疫または修復ネットワークに配置する*]。**

詳解

CUI の処理、保存、伝送、保護に使用されるシステムコンポーネントは、信頼できるソース（ハードウェアおよびソフトウェアインベントリ、関連するベースライン構成など）に対して監視およびチェックされる。自動化されたアセスメントの観点から、信頼できるソースにより提供されるシステム記述は、望ましい状態と呼ばれる。望ましい状態は、準拠または逸脱をチェックするために、自動化されたツールを使用して実際の状態と比較される。不明なシステムコンポーネントや、承認された構成から逸脱しているシステムコンポーネントに対するセキュリティ対応には以下を含めることができる。(1)そのコンポーネントを取り除くこと；(2)システム機能または処理を停止すること；(3)パッチ適用、再構成、またはその他の緩和策を促進するためにシステムコンポーネントを検疫ネットワークまたは修復ネットワークに配置すること；(4)組織が定める構成アイテムに認可されていない変更があった場合に、アラート告および／または通知を職員に発行すること。対応は、自動化、手動、または手続き型にすることできる。システムから取り除かれたコンポーネントは、信頼できるソースによって確立された信頼できる構成ベースラインから再構築される。

[IR 8011-1]は、システム構成をアセスメントするための自動化サポートの利用に関するガイダンスを提供している。

保護戦略

侵入耐性アーキテクチャ

敵対者への効果

参照[SP 800-160-2]：[**排除**（抹消、先制）；**防止**（封じ込め）；**暴露**（検知）]

3.4.3e **システムコンポーネントの最新かつ完全で的確なすぐに利用可能なインベントリを維持するために、自動化された検出および管理ツールを採用する。**

詳解

システムコンポーネントインベントリには、コンポーネントの説明責任に必要なシステム固有の情報、および信頼されたソースに従って構成アイテムを識別、管理、監視、検証するためのサポートを提供するために必要なシステム固有の情報が含まれる。システムコンポーネントの効果的な説明責任を果たすために必要な情報には、システム名、ハードウェアおよびソフトウェアコンポーネントのオーナー、ハードウェアインベントリの仕様書、ソフトウェアのライセンス情報、ソフトウェアのバージョン番号、およびネットワークコンポーネントの場合は、マシン名とネットワークアドレスが含まれる。インベントリの仕様書には、製造元、サプライヤ情報、コンポーネントのタイプ、受領日、費用、モデル、シリアル番号、および物理的な設置場所が含まれる。組織は、また、ハードウェアおよびソフトウェアインベントリツール、構成管理ツール、ネットワーク管理ツールなどのシステムに対する信頼された（すなわち、最新で、完全で、正確で、利用可能な）ベースライン構成を実装および維持するために、自動化されたメカニズムを利用する。ツールを使用して、オペレーティングシステムのバージョン番号、アプリケーション、インストールされているソフトウェアのタイプ、および現在のパッチレベルを追跡できる。

保護戦略

侵入耐性アーキテクチャ

敵対者への効果

参照[SP 800-160-2]：[**暴露**（検知）]

3.5 識別および認証

拡張セキュリティ要件

3.5.1e **暗号をベースとしたリプレイ攻撃耐性のある双方向認証を使用してネットワーク接続を確立する前に、[*設定：組織が定めるシステムおよびシステムコンポーネント*]を識別および認証する。**

詳解

システム、コンポーネント、およびデバイス間の、暗号をベースとしたリプレイ攻撃耐性のある認証は、スプーフィング（いわゆる、虚偽のアイデンティティ主張）による認可されていないアクセスのリスクに対応する。この要件は、クライアント間認証、サーバ間認証、およびデバイス認証（モバイルデバイスを含む）に適用される。認証トランザクションの暗号鍵は、オーセンティケータアプリケーションで使用できる適切にセキュアなストレージ（キーチェーンストレージ、トラステッドプラットフォームモジュール［TPM：Trusted Platform Module］、高信頼実行環境［TEE：Trusted Execution Environment］、セキュアなエレメントなど）に保管される。すべての接続ポイントで認証要件を義務付けることは実用的でない可能性があるため、このような要件は、定期的に、またはネットワーク接続の初期ポイントでのみ適用してもよい。

［SP 800-63-3］は、アイデンティティおよびオーセンティケータのマネジメントに関するガイダンスを提供している。

保護戦略

侵入耐性アーキテクチャ

敵対者への効果

参照［SP 800-160-2］：［**排除**（否定）；**暴露**（検知）］

3.5.2e **多要素認証または複雑なアカウント管理をサポートしていないシステムおよびシステムコンポーネントに、パスワードの生成、保護、ローテーション、管理のための自動化されたメカニズムを採用する。**

詳解

静的パスワードや個人識別番号（PIN：Personal Identification Numbers）が使用されている状況（例えば、あるシステムコンポーネントが、多要素認証、またはユーザ毎に別々のシステムアカウントやロギングなどの複雑なアカウント管理をサポートしていない場合）では、自動化されたメカニズム（パスワードマネージャーなど）は、ユーザアカウントとデバイスアカウントの強力で異なるパスワードを自動的に生成、ローテーション、管理、保管することができる。例えば、ルータには 1 つの管理者アカウントがあるかもしれないが、組織には通常、複数のネットワーク管理者が存在する。したがって、アクセス管理と説明責任が問題となる。パスワードマネージャーは、自動化されたパスワードローテーション（この例ではルータパスワード）などの技法を使用して、特定のユーザが一時的なパスワードををチェックアウトし、そのパスワードをチェックインしてアクセスを終了することで、一時的にデバイスにアクセスできるようにする。パスワードマネージャーは、これらの動作を同時にロギングする。パスワードマネージャーを使用する場合のリスクの 1 つは、デバイスが生成するパスワードの一群を敵対者が標的にする可能性があることである。したがって、これらのパスワードはセキュアに管理することが重要である。パスワードを保護する方法には、パスワードマネージャーへの多要素認証、暗号化、またはセキュアなハードウェア（ハードウェアセキュリティモジュールなど）の使用が含まれる。

［SP 800-63-3］は、パスワードの生成と管理に関するガイダンスを提供している。

保護戦略

侵入耐性アーキテクチャ

敵対者への効果

参照[SP 800-160-2]：[**防止**（遅延、徒労）]

3.5.3e **システムコンポーネントが、既知で、認証されており、適切に構成された状態、または信頼プロファイル内でない限り、組織のシステムに接続することを禁止する自動化または手動／手続き型のメカニズムを採用する。**

詳解

システムコンポーネントおよびコンポーネント構成の識別および認証は、例えば、コンポーネントの暗号ハッシュを介して決定することができる。これは、デバイスの認証、および既知の動作状態または信頼プロファイルとしても知られている。ユーザ認証方法、デバイスのタイプ、物理的な場所などの要素に基づく信頼プロファイルは、様々なタイプのデータに対する動的な認可の決定を行うために使用される。デバイスの認証が識別および認証の手段である場合、デバイスのパッチ適用と更新は、パッチ適用と更新がセキュアに行われ、他のデバイスの識別および認証を中断しないように、構成管理プロセスを介して処理することが重要である。

[IR 8011-1]は、自動化サポートを使用してシステム構成をアセスメントする方法に関するガイダンスを提供している。

保護戦略

侵入耐性アーキテクチャ

敵対者への効果

参照[SP 800-160-2]：[**排除**（先制）；**暴露**（検知）]

3.6 インシデント対応

拡張セキュリティ要件

3.6.1e **[*設定：組織が定める期間*]運営するセキュリティオペレーションセンターのケイパビリティを確立し維持する。**

詳解

セキュリティオペレーションセンター（SOC：Security Operations Center）は、組織のセキュリティオペレーションおよびコンピュータネットワーク防御の中心である。SOC の目的は、組織のシステムやネットワーク（すなわち、サイバーインフラ）を継続的に防御および監視することである。SOC は、サイバーセキュリティインシデントをタイムリーに、検知、分析、対応する責任を負う。SOC には、スキルのある技術職員および運用職員（セキュリティアナリスト、インシデント対応職員、システムセキュリティエンジニアなど）を配置する。場合によっては、1 日 24 時間、週 7 日間運営する。また、複数のソースからのセキュリティ関連イベントのデータを監視、融合、関連付け、分析、対応するために、技術的管理策、マネジメント管理策、運用管理策（監視、スキャン、フォレンジックツールなど）を実装する。イベントデータのソースには、境界防御、ネットワークデバイス（ゲートウェイ、ルータ、スイッチなど）、エンドポイントエージェントのデータフィードが含まれる。SOC は、組織がシステムと組織のセキュリティ態勢を決定するのに役立つ包括的な状況認識ケイパビリティを提供する。SOC のケイパビリティは、様々な方法で取得できる。大規模な組織では専用の SOC を実装してもよく、小規模な組織では SOC のケイパビリティを提供するためにサードパーティ組織を利用してもよい。

[SP 800-61]は、インシデント対応に関するガイダンスを提供している。[SP 800-86]および[SP 800-101]は、フォレンジック技法をインシデント対応に統合するためのガイダンスを提供している。[SP 800-150]は、サイバー脅威情報の共有に関するガイダンスを提供している。[SP 800-184]は、サイバーセキュリティイベントの復旧に関するガイダンスを提供している。

保護戦略

被害局限化運用

敵対者への効果

参照[SP 800-160-2]：[**限定**（短縮、低減）；**暴露**（検知）]

3.6.2e **[*設定：組織が定める期間*]内に、組織が展開できるサイバーインシデント対応チームを確立し維持する。**

詳解

サイバーインシデント対応チーム（CIRT）は、サイバーインシデントをアセスメントし、文書化し、対応する専門家のチームであり、組織のシステムを迅速に復旧し、将来のインシデントを回避するために必要な管理策を実装できるようにする。CIRT の職員には、例えば、フォレンジックアナリスト、悪意のあるコードのアナリスト、システムセキュリティエンジニア、リアルタイム運用職員などが含まれる。インシデント対応ケイパビリティには、エビデンスの迅速なフォレンジック保存、侵入の分析と侵入への対応が含まれる。チームメンバーはフルタイムでも、フルタイムでなくてもよいが、必要な期間内に対応できる必要がある。チームの規模と専門分野は、既知の脅威と予想される脅威に基づく。チームは通常、迅速な識別、検疫、緩和、復旧に必要なソフトウェアとハードウェア（フォレンジックツールなど）を事前に装備し、エビデンスを保存し、法執行機関や防諜機関カウンターインテリジェンスの利用のために証拠の保全と過程管理（chain of custody）を維持する方法に精通している。一部の組織では、CIRT を組織横断のエンティティとして実装することも、セキュリティオペレーションセンター（SOC）の一部として実装することもできる。

[SP 800-61]は、インシデント対応に関するガイダンスを提供している。[SP 800-86]および[SP 800-101]は、フォレンジック技法をインシデント対応に統合するためのガイダンスを提供している。[SP 800-150]は、サイバー脅威情報の共有に関するガイダンスを提供している。[SP 800-184]は、サイバーセキュリティイベントの復旧に関するガイダンスを提供している。

保護戦略

被害局限化運用

敵対者への効果

参照[SP 800-160-2]：[**排除**（抹消）；**防止**（封じ込め、徒労）；**限定**（短縮、低減）；**暴露**（精査）]

3.7 メンテナンス

拡張セキュリティ要件

メンテナンスに関する拡張セキュリティ要件はない。

3.8 媒体保護

拡張セキュリティ要件

媒体保護に関する拡張セキュリティ要件はない。

3.9 職員のセキュリティ

拡張セキュリティ要件

3.9.1e **個人に対して[*設定：組織が定める拡張した職員のスクリーニング*]を実施し、[*設定：組織が定める頻度*]で個人の職位と CUI へのアクセスを再アセスメントする。**

詳解

職員のセキュリティは、行い、誠実さ、判断力、忠誠心、信頼性、安定性の評価またはアセスメントに基づいて、信頼できる要員を提供する規律である。身元調査の程度は、個人がその職位と CUI へのアクセスによってもたらすことができるリスクのレベルに見合ったものとする。連邦政府は、連邦政府の施設やシステムにアクセスする個人に対し、信頼できる要員を確保するための身元調査プロセスでリソース、情報、技術を用いる。これらのスクリーニングプロセスは、連邦政府機関と非連邦政府組織との間で締結された契約手段またはその他の合意により非連邦政府システムまたは組織に存在する CUI を含む、連邦政府情報にアクセスする人の全部または一部に拡張してもよい。

セキュリティを目的とした拡張した職員のスクリーニングの例としては、追加の経歴チェックが含まれる。職員の再アセスメント活動には、適用される法律、大統領令、指令、ポリシー、規則、および割り当てられた職位に必要なアクセスレベルに対して規定された具体的な判定基準を反映する。

保護戦略

被害局限化運用

敵対者への効果

参照[SP 800-160-2]: [**排除**(抹消); **防止**(徒労)]

3.9.2e **CUI にアクセスする個人について敵対的情報が発生または取得された場合、組織のシステムが保護されていることを確実にする。**

詳解

CUI にアクセスする個人について敵対的情報が発生または取得され、その個人が CUI を含むシステムへのアクセスを継続するべきかどうか疑問を投げかけられている場合、敵対的情報が解決されるまでの間、CUI を保護するための措置(例えば、当該個人によるそれ以上のアクセスを排除または限定する、当該個人のアクションを監査するなど)を取る。

保護戦略

被害局限化運用

敵対者への効果

参照[SP 800-160-2]: [**限定**(低減)]

3.10 物理的保護

拡張セキュリティ要件

物理的保護に関する拡張セキュリティ要件はない。

3.11 リスクアセスメント

拡張セキュリティ要件

3.11.1e **リスクアセスメントの一環として、組織のシステム、セキュリティアーキテクチャ、セキュリティソリューションの選択、監視、脅威ハンティング、対応および復旧措置の策定をガイドし、情報を提供するために、[*設定:組織が定める脅威インテリジェンスのソース*]を採用する。**

詳解

敵対者、特に APT 攻撃の絶え間ない進化と高度化により、敵対者が組織のシステムを侵害し、ブリーチに成功する可能性が高まっている。したがって、脅威インテリジェンスは、システム開発ライフサイクル全体を通じて、リスクマネジメント処理の各ステップに統合することができる。このリスクマネジメントプロセスには、システムセキュリティ要件の定義、システムおよびセキュリティアーキテクチャの開発、セキュリティソリューションの選択、監視（脅威ハンティングを含む）、および修復の試みが含まれる。

[SP 800-30]は、リスクアセスメントに関するガイダンスを提供している。[SP 800-39]では、リスクマネジメント処理に関するガイダンスを提供している。[SP 800-160-1]は、セキュリティアーキテクチャとシステムセキュリティエンジニアリングに関するガイダンスを提供している。[SP 800-150]は、サイバー脅威情報の共有に関するガイダンスを提供している。

保護戦略

被害局限化運用

敵対者への効果

参照[SP 800-160-2]：[**排除**（否定）；**防止**（徒労）；**暴露**（検知）]

3.11.2e **[*設定：組織が定めるシステム*]における侵害の兆候を捜索し、既存の管理策を回避する脅威を検知、追跡、および妨害するために、[*選択（1 つ以上）：*[*設定：組織が定める頻度*]；[*設定：組織が定めるイベント*]]でサイバー脅威ハンティング活動を実施する。**

詳解

脅威ハンティングは、ファイアウォール、侵入検知および防御システム、サンドボックス内での悪意のあるコードの隔離、セキュリティ情報イベント管理（SIEM：Security Information and Event Management）の技術とシステムなど、従来の保護対策とは対照的な能動的な防御手段である。サイバー脅威ハンティングでは、組織のシステム、ネットワーク、インフラを積極的に検索し、高度な脅威を探し出す。その目的は、攻撃シーケンスのできるだけ早い段階でサイバー敵対者を追跡し、混乱させ、組織の対応のスピードと精度を測定できるほどにまで向上させることである。侵害の兆候は、ホストまたはネットワークレベルで組織のシステム上に識別された侵害によるフォレンジック調査の対象であり、異常なネットワークトラフィック、異常なファイルの変更、悪意のあるコードの存在などが含まれる可能性がある。

脅威ハンティングチームは既存の脅威インテリジェンスを使用し、新しい脅威情報を作成する場合がある。この新しい脅威情報は同業組織、情報共有分析機関（ISAO：Information Sharing and Analysis Organizations）、情報共有分析センター（ISAC：Information Sharing and Analysis Centers）、および関連する政府部局および政府機関と共有される場合がある。脅威の兆候、署名、戦術、技法、手順、その他の侵害の兆候は、セキュリティインシデント対応のための非営利国際調整協力機関、米国コンピュータ緊急対応チーム（US-CERT）、防衛産業基盤サイバーセキュリティ情報共有（DIB CS）プログラム、CERT コーディネーションセンター（CERTCC）など、政府および非政府の協同活動組織を通じて入手できる場合がある。

[SP 800-30]では、脅威とリスクアセスメント、リスク分析、およびリスクモデリングに関するガイダンスを提供している。[SP 800-160-2]では、システムセキュリティエンジニアリングとサイバーレジリエンスに関するガイダンスを提供している。[SP 800-150]では、サイバー脅威情報の共有に関するガイダンスを提供している。

保護戦略

被害局限化運用

敵対者への効果

参照[SP 800-160-2]：[**排除**（抹消）；**限定**（短縮、低減）；**暴露**（検知、精査）]

3.11.3e **アナリストをサポートし、組織、システム、システムコンポーネントに対するリスクを予測および特定するために、高度な自動化と分析ケイパビリティを採用する。**

詳解

適切なリソースを持つセキュリティオペレーションセンター（SOC）またはコンピュータインシデント対応チーム（CIRT）は、高度な自動化と分析ケイパビリティを採用してデータを分析しない限り、セキュリティツールやアプライアンスの急増によって生成される情報量に圧倒される可能性がある。高度な自動化と予測分析ケイパビリティは、通常、人工知能の概念と機械学習によってサポートされる。例としては、自動化されたワークフロー操作、自動化された脅威の検出と対応（広範な収集、コンテキストベースの分析、適応型対応ケイパビリティを含む）、機械支援の意思決定ツールなどがある。

[SP 800-30]は、リスクアセスメントとリスク分析に関するガイダンスを提供している。

保護戦略

被害局限化運用

敵対者への効果

参照[SP 800-160-2]：直接的な影響なし

3.11.4e 選択したセキュリティソリューション、セキュリティソリューションの根拠、およびリスクの決定をシステムセキュリティ計画で文書化または参考文献目録として作成する。

詳解

システムセキュリティ計画では、セキュリティ要件を一連のセキュリティ管理策とソリューションに関連付ける。計画では、管理策とソリューションがどのようにセキュリティ要件を満たすかについて記述する。APT 攻撃が懸念される場合に選択される拡張セキュリティ要件については、セキュリティ計画は、脅威とリスクアセスメントおよび、セキュリティソリューションのリスクベースの選択との間のトレーサビリティを提供する。これには、セキュリティ関連の主要なアーキテクチャおよび設計上の決定に対する代替案の関連分析と理論的根拠の詳解が含まれる。このレベルの詳細化は、脅威が変化するにつれて重要になり、リスクの再アセスメントと以前のセキュリティ上の決定の根拠が必要になる。

外部サービスプロバイダをシステムセキュリティ計画に組み込む場合、組織は提供されるサービスのタイプ（例えば、サービスとしてのソフトウェア、サービスとしてのプラットフォームなど）、接続ポイントとタイプ（ポートとプロトコルを含む）、サービスプロバイダとの間の情報フローの性質とタイプ、およびサービスプロバイダによって実装されるセキュリティ管理策を記述する。安全性を重要視すべきシステムの場合、組織は、安全性がセキュリティソリューションを実装しない主な理由である状況（すなわち、ソリューションは脅威に対処するのには適切だが、安全上の懸念を引き起こす状況）を文書化する。

[SP 800-18]では、システムセキュリティ計画の策定に関するガイダンスを提供している。

保護戦略

侵入耐性アーキテクチャ

敵対者への効果

参照[SP 800-160-2]：直接的な影響なし

3.11.5e 現在のおよび蓄積された脅威インテリジェンスに基づいて、組織のシステムおよび組織に対して予想されるリスクに対処するために、セキュリティソリューションの有効性を[*設定：組織が定める頻度*]でアセスメントする。

詳解

組織の脅威に関する認識とリスクアセスメントは、動的で継続的であり、システムの運用、システムのセキュリティ要件、およびそれらの要件を満たすために採用されたセキュリティソリューションに情報提供する。脅威インテリジェンス（すなわち、意思決定に必要なコンテキストを提供するために集約、変換、分析、解釈、または補強された脅威情報）は、動的な脅威環境に対処するため必要な変更を特定するために、組織のリスクアセスメント処理と情報セキュリティ運用に注入される。

[SP 800-30]は、リスクアセスメント、脅威アセスメント、およびリスク分析に関するガイダンスを提供している。

保護戦略

被害局限化運用

敵対者への効果

参照[SP 800-160-2]：[**暴露**（精査）]

3.11.6e 組織のシステムおよびシステムコンポーネントに関連するサプライチェーンリスクをアセスメント、対応、および監視する。

詳解

サプライチェーンのイベントには、妨害、欠陥コンポーネントの使用、偽物の挿入、窃取、悪意のある開発プラクティス、不適切な配信プラクティス、悪意のあるコードの挿入などがある。これらのイベントはシステムとその情報に重大なインパクトを与える可能性があり、したがって、組織の運営（ミッション、機能、イメージ、評判など）、組織の資産、個人、その他の組織、および国家にも有害なインパクトを与える可能性がある。サプライチェーン関連のイベントは、故意ではない場合もあれば悪意のある場合もありシステムのライフサイクルのどの時点でも発生する可能性がある。サプライチェーンリスクの分析は、サプライチェーンリスクの緩和が必要なシステムやコンポーネントを組織が特定するのに役立つ。

[SP 800-30]は、リスクアセスメント、脅威アセスメント、およびリスク分析に関するガイダンスを提供している。[SP 800-161]は、サプライチェーンのリスクマネジメントに関するガイダンスを提供している。

保護戦略

侵入耐性アーキテクチャ

敵対者への効果

参照[SP 800-160-2]：[**排除**（先制）：**暴露**（検知）]

3.11.7e 組織のシステムおよびシステムコンポーネントに関連するサプライチェーンリスクを管理するための計画を策定し；[*設定：組織が定める頻度*]で計画を更新する。

詳解

外部プロバイダからの製品、システム、サービスへの依存度の高まりは、それらのプロバイダとの関係の性質と共に、組織に対するリスクのレベルを高めている。リスクを高める可能性のある脅威行為には、偽造品の挿入または使用、認可されていない生産、改ざん、窃取、悪意のあるソフトウェアおよびハードウェアの挿入、サプライチェーンにおける不十分な製造および開発プラクティスなどが含まれる。サプライチェーンリスクは、システム要素またはコンポーネント、システム、組織、業界、または国家内で固有または体系的である可能性がある。サプライチェーンのリスクマネジメントは、信頼関係を構築し、社内外の利害関係者とのコミュニケーションを図るために、組織全体で協調的な取り組みを必要とする多面的な取り組みである。サプライチェーンのリスクマネジメント（SCRM：Supply chain risk management）活動には、リスクの特定とアセスメント、適切な緩和措置の決定、選択した緩和措置を文書化するための SCRM 計画の策定、計画に対する実績の監視が含まれる。SCRM 計画は、ライフサイクルベースのシステムセキュリティエンジニアリング処理の一部として実装されるセキュリティ設計原則の適用を含む、統合的信頼性、セキュアで、レジリエントなシステムおよびシステムコンポーネントを開発するための要件に対応する。

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

保護戦略

侵入耐性アーキテクチャ

敵対者への効果

参照[SP 800-160-2]：[**排除**（先制）；**防止**（徒労）]

3.12 セキュリティアセスメント

拡張セキュリティ要件

3.12.1e 自動化されたスキャンツールと、対象分野の専門家によるアドホックテストを活用して、[*設定：組織が定める頻度*]で侵入テストを実施する。

詳解

侵入テストは、敵対者に悪用される可能性のある脆弱性を特定するために、システムや個々のシステムコンポーネントに対して行われる特殊なタイプのアセスメントである。侵入テストは、自動化された脆弱性スキャンに勝る。侵入テストは、ネットワーク、オペレーティングシステム、およびアプリケーションレベルのセキュリティに関する技術的な専門知識を含む特定のスキルと経験を持つ、侵入テスト担当者やチームによって実施される。侵入テストは、脆弱性を検証したり、指定された制約の範囲内の敵対者に対するシステムの侵入耐性を判断するために使用できる。そのような制約には、時間、リソース、およびスキルが含まれる。組織は、レッドチーム演習で侵入テストを補足することもできる。レッドチームは、組織に対する攻撃を実行する際の敵対者の行動を再現しようと試み、セキュリティ関連の弱点や欠陥の詳細な分析を提供する。

組織は脆弱性分析の結果を利用して、侵入テスト活動をサポートすることができる。侵入テストは、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に対して内部または外部で実行でき、物理的制御および技術的制御を実行できる。侵入テストの標準的な方法には、システムの完全な知識に基づく事前テスト分析、事前テスト分析に基づく潜在的な脆弱性のテスト前の特定、および脆弱性の悪用可能性を判断するためのテストが含まれる。すべての関係者は、侵入テストの開始前に、指定された交戦規定に同意する。組織は、侵入テストとレッドチーム演習（使用する場合には）の交戦規定を、敵対者が使用する可能性があると予想されるツール、技法、および手順と関連付ける。侵入テストまたはレッドチーム演習は、組織ベースの場合もあれば組織の外部の場合もある。いずれの場合も、チームが仕事をするために必要なスキルとリソースを持っており、そのアセスメントにおいて客観的であることが重要ある。

[SP 800-53A]は、セキュリティアセスメントの実施に関するガイダンスを提供している。

保護戦略

侵入耐性アーキテクチャ；被害局限化運用

敵対者への効果

参照[SP 800-160-2]：[**防止**（徒労）；**暴露**（検知）]

3.13 システムおよび通信の保護

拡張セキュリティ要件

3.13.1e 悪意のあるコードの伝播の程度を減らすために、[*設定：組織が定めるシステムコンポーネント*]に多様性を作る。

詳解

組織は、多くの場合、コストを削減し、運用や使用を促進するために、同種の情報技術環境を使用する。ただし、同種の環境では、共通モードの障害や同一のシステムコンポーネント（すなわち、ハードウェア、ソフトウェア、ファームウェア）間で悪意のあるコードの伝播が可能になるため、APT 攻撃の作業も促進される。このような環境では、システムコンポーネントの 1 つのインスタンス化で機能する敵対者の戦術、技法、手順（TTP）は、そのようなコンポーネントが何回複製されるかや、アーキテクチャ内でどれだけ離れて設置されるかに関係なく、他の同一の

コンポーネントのインスタンス化でも同様に機能する。組織のシステム内の多様性を高めることは、特定の技術の潜在的な悪用や侵害のインパクトを軽減する。このような多様性は、サプライチェーン攻撃によって引き起こされる障害を含む、共通モードの障害から保護する。また、多様性は、敵対者が 1 つのシステムコンポーネントを侵害するために使用する TTP が、他のシステムコンポーネントに対して有効となる可能性を軽減し、その結果、計画された攻撃を正常に完了するための敵対者の作業要因を増加させる。異種または多様な情報技術環境では、敵対者が多様なコンポーネントに対して異なる TTP を開発して展開する必要があるため、悪意のあるコードを伝播する作業がより困難になる。

この要件を満たすことは、組織が複数のバージョンのオペレーティングシステム、アプリケーション、ツール、および通信プロトコルを取得および管理する必要があることを意味するものではない。しかし、組織的に決定された特定の重要な、システムコンポーネントにおける多様性の使用は、APT 攻撃に対する効果的な対策となる可能性がある。さらに、APT 攻撃に対抗するためではなく、組織はすでに多様性を実践している可能性がある。例えば、単に各ベンダが異なる時間や頻度で新しい悪意のあるコードパターンの更新を発行する可能性があるという理由で、組織がインフラの様々な部分で多様なウイルス対策製品を採用することは一般的である。同様に、一部の組織は、サーバレベルで 1 つのベンダの製品を採用し、エンドユーザレベルで別のベンダの製品を採用している。多様性の別の例は、アドレス空間配置のランダム化（ASLR）を提供する製品に存在する。このような製品は、共通のソフトウェアの実装を変形して様々なインスタンスを生成することで、総合的な多様性の形態をもたらしている。最後に、組織は、複数の仮想プライベートネットワーク（VPN：virtual private network）ベンダを使用して、あるベンダの VPN を別のベンダの VPN 内にトンネリングすることを選択できる。小規模な組織では、システムコンポーネントの多様性を実現することは困難であり、おそらく実用的ではないと思うかもしれない。また、組織は、多様なシステムコンポーネントの採用によってシステムに導入される可能性のある脆弱性も考慮する。

[SP 800-160-1]は、セキュリティエンジニアリングのプラクティスとセキュリティ設計の概念に関するガイダンスを提供している。[SP 800-160-2]は、サイバーレジリエントなシステムとシステムコンポーネントの開発に関するガイダンスを提供している。[SP 800-161]は、サプライチェーンのリスクマネジメントに関するガイダンスを提供している。

保護戦略

サイバーレジリエンスと生存可能性のための設計

敵対者への効果

参照[SP 800-160-2]：[**リダイレクト**（阻止）；**排除**（先制）；**防止**（封じ込め、デグレード、遅延、徒労）；**限定**（短縮、低減）]

3.13.2e 運用にある程度の予測不可能性を導入するために、組織のシステムおよびシステムコンポーネントに[*設定：組織が定める、システムとシステムコンポーネントの変更および変更の頻度*]を実装する。

詳解

敵対者によるサイバー攻撃は、攻撃対象領域に関するある程度の予測可能性と一貫性を前提としている。攻撃対象領域とは、攻撃者がシステム、システム要素、または環境に侵入したり、影響を与えたり、データを抽出したりすることを試みることができる、システム、システム要素、または環境の境界上の一連のポイントである。攻撃対象領域を変更すると、環境の予測可能性が低下し、敵対者が攻撃を計画したり実行したりすることが困難になる。また、攻撃の全体的な有効性にインパクトを与えたり、敵対者の可観察性を高めたりするような可能性のある誤算を敵対者が引き起こす可能性がある。予測不能性は、一見ランダムに見える時間や状況に変更を加える（例えば、クレデンシャルが有効な時間をランダムに短縮する）ことによって達成できる。ランダム性は、システムを攻撃から守るために組織が取る行動に関して、敵対者の不確実性のレベルを高める。このような措置は、敵対者が、重要または不可欠な組織のミッションや事業機能をサポートするシステムコンポーネントを、正確に標的にする能力を妨げる可能性がある。不確実性により、敵対者が攻撃を開始したり、継続したりする前に躊躇する可能性もある。ランダム性を伴う技法には、特定の日常的な行動処理を 1 日の異なる時間帯に実行すること、様々な情報技術を採用すること、様々なサプライヤを使用すること、組織の職員の役割と責任をローテーションする方法などが含まれる。

保護戦略

サイバーレジリエンスと生存可能性のための設計

敵対者への効果

参照[SP 800-160-2]：[**排除**（先制、否定）；**防止**（遅延、徒労）；**暴露**（検知）]

3.13.3e 敵対者を混乱させ誤解させるために、[*設定：組織が定める技術的および手続き的手段*]を採用する。

詳解

誤認誘導（misdirection）、汚染（tainting）、偽情報配備（disinformation）、またはその組み合わせを含む、敵対者を混乱させ誤解させるために使用できる多くの技法とアプローチがある。欺瞞は、敵対者が意思決定に使用する情報、敵対者が漏出させようとする情報の価値と真正性、敵対者が活動を望む、または必要とする環境に関して、敵対者を混乱させ、誤解させるために使用できる。このような行動は、標的組織の有意義な偵察を行う敵対者の能力を防止し、システム内、またはあるシステムから別のシステムに横方向に移動したりする敵対者の能力を遅延またはデグレードさせ、CUI を含むシステムまたはシステムコンポーネントから敵対者を逸らし、防御側に対する敵対者の可観性を高める可能性があり、敵対者の存在とその TTP を明らかにすることができる。誤認誘導は、悪意のあるコードを逸らし、敵対者の TTP を安全に検査できる仮想サンドボックスを提供する欺瞞環境（例えば、欺瞞ネット）を通じて達成できる。汚染とは、組織が攻撃者に漏出させたいデータを組織のシステムまたはシステムコンポーネントに組み込むことである。汚染は、情報が組織から盗み出されたか、不適切に削除されたかを組織が判断することができ、漏出の性質や敵対者の場所に関する情報を組織に提供する可能性がある。偽情報配備は、システムの状態や組織の防御のタイプに関する偽情報を意図的に、敵対者が利用できるようにすることで実現できる。いかなる偽情報配備活動も、そのような活動を必要とする関連する連邦政府機関と調整され、認可されたユーザへの偽 CUI の偶発的な暴露を限定する計画を含めることが望ましい。偽情報配備は、戦術的（例えば、防御側が敵対者の行動を追跡するために使用できる偽のクレデンシャルを利用可能にする）にも戦略的（例えば、偽の CUI を実際の CUI に散在させる、敵対者の再利用を妨害する、リバースエンジニアリング、正当な CUI の悪用を妨害する、したがって、漏出された情報の価値に対する敵対者の信頼を損ない、その後、そのような漏出を制限する）にも使用される可能性がある。

[SP 800-160-2]は、サイバーレジリエントなシステムとシステムコンポーネントの開発に関するガイダンスを提供している。

保護戦略

サイバーレジリエンスと生存可能性のための設計

敵対者への効果

参照[SP 800-160-2]：[**リダイレクト**（阻止、逸らし、欺き）；**排除**（先制、否定）；**防止**（遅延、徒労）；**暴露**（検知）]

3.13.4e [*選択：（1 つ以上）：[設定：組織が定める物理的分離技法]；[設定：組織が定める論理的分離技法]*]を組織のシステムおよびシステムコンポーネントに採用する。

詳解

システムアーキテクチャの一部として実装された物理的および論理的な分離技法（後述）の組み合わせは、CUI の認可されていないフローを限定し、システムの攻撃対象領域を減らし、セキュアでなければならないシステムコンポーネントの数を制限し、敵対者の動きを妨げることが出来る。一連の管理されたインタフェースを使用して実装すると、組織のシステムおよびコンポーネントの物理的および論理的な分離技法により、CUI を追加の保護を実装できる個別のセキュリティドメインに分離することができる。管理または管理目的を含め、管理されたインタフェース間（すなわち、複数のセキュリティドメイン間）の通信は、通信が組織内に留まっている場合でもリモートアクセスを構成する。境界保護メカニズムを使用してシステムコンポーネントを分離することで、個々のコンポーネントの保護を強化し、それらのコンポーネント間の情報フローをより効果的に制御できる。この強化された保護は、敵対的なサイバー攻撃やエラーに

対する潜在的な危害と脆弱性を制限する。分離の程度は、選択した境界保護メカニズムによって異なる。境界保護メカニズムには、システムコンポーネントを物理的に分離したネットワークまたはサブネットワークに分離するルータ、ゲートウェイ、およびファイアウォール；仮想化およびマイクロ仮想化技術；個別の暗号化キーを使用してシステムコンポーネント間の情報フローの暗号化；サブネットワークを分離するクロスドメインデバイス；完全な物理的分離（すなわち、エアギャップ）が含まれる。

システムアーキテクチャには、論理的分離、部分的な物理的および論理的分離、またはサブシステム間および CUI とその他のリソースを保存、処理、伝送、または保護するリソース間のシステム境界での完全な物理的分離が含まれる。例としては、次のようなものがある。

- *論理的分離*：CUI のフローにタグ付け、監視、制限するタグ付け、デジタル著作権管理（DRM）、およびデータ損失防止（DLP）；ホスト上の CUI およびその他の情報を分離する仮想マシンまたはコンテナ；および CUI やその他の情報をネットワーク上で分離する仮想ローカルエリアネットワーク（VLAN）
- *部分的な物理的および論理的分離*：物理的に、または暗号化によって分離されたネットワーク、データセンター内の専用ハードウェア、および(a)ドメイン外のリソースに直接アクセスできない可能性のあるセキュアなクライアント（すなわち、クロスエンクレーブ接続を備えたすべてのアプリケーションは、非武装地帯[DMZ：demilitarized zone]または内部の保護されたエンクレーブでホストされるリモート仮想アプリケーションとして実行される）、(b)二重認可以外のファイル転送ケイパビリティを持たないリモート仮想化アプリケーションまたは仮想デスクトップを介したアクセスするセキュアなクライアント、または(c)専用のクライアントハードウェア（ゼロクライアントまたはシンクライアントなど）またはマルチレベルセキュア（MLS：multi-level secure）の使用が承認されたハードウェアを採用しているセキュアなクライアント。
- *完全な物理的分離*：専用（共有されていない）クライアントおよびサーバハードウェア；クライアントとサーバ用の、物理的に分離されたスタンドアロンのエンクレーブ；(a)公開鍵基盤（PKI：Public Key Infrastructure）ベースの暗号技術を使用したエンドツーエンドの暗号化によるネットワークトラフィックを論理的に分離する（VLAN の使用など）、(b)他のネットワークからの物理的分離。

分離技法は、脅威、保護される情報、および保護のためのオプションのコストのバランスをとるリスクマネジメントの観点に基づいて選択される。アーキテクチャおよび設計の決定は、セキュリティ要件と選択したソリューションによって導かれ、通知される。組織は、採用される分離技法の統合的信頼性を考慮し（例えば、論理的分離は、実行される機能のために高価値の標的と考えられる可能性のある情報技術に依存している）、独自の脆弱性のセットを導入する。

[SP 800-160-1]はシステムセキュリティエンジニアリングのプラクティスとセキュリティ設計の概念を使用して、統合的信頼性、セキュアで、サイバーレジリエントなシステムの開発に関するガイダンスを提供している。

保護戦略

侵入耐性アーキテクチャ；サイバーレジリエンスと生存可能性のための設計

敵対者への効果

参照[SP 800-160-2]：[**排除**（先制、否定）；**防止**（封じ込め、デグレード、遅延、徒労）；**限定**（低減）]

3.13.5e [*設定：組織が定めるシステム機能またはリソース*]を[*設定：組織が定める頻度*]で配布および再配置する。

詳解

処理およびス保存場所の変更（移動標的防御とも呼ばれる）は、仮想化、分散処理、複製などの技法を使用して APT 攻撃に対処する。これにより、組織は、重要なミッションや事業機能をサポートするシステムコンポーネントを再配置できるようになる。処理活動の場所や保存場

所を変更すると、敵対者の標的化活動にある程度の不確実性をもたらす。標的化の不確実性は、敵対者の作業要因を増やし、組織のシステムに対する侵害やブリーチをより困難で時間のかかるものにする。また、敵対者が組織のリソースを見つけようとしている間に、諜報活動の様相を不用意にさらす可能性も高くなる。移動標的防御を採用するその他のオプションには、IP アドレス、ドメインネームシステム（DNS）名、ネットワークトポロジの変更などがある。移動標的防御は、絶えず変化する防御すべきシステムを持つ防御側の作業要因も増大させる可能性がある。したがって、組織は管理ツールとセキュリティツールを更新し、追加の作業要因に適応するように職員をトレーニングする。

この要件に対処するもう 1 つの方法は、断片化である。これは、情報を取得し、それを複数のコンポーネント（例えば分散データベース間）にわたって断片化／分割することが含まれる。このようなアクションは、情報データセットの単一コンポーネントの侵害（認可されていない漏出）がデータ全体の侵害につながることはないことを意味する。データセット全体を完全に侵害するには、敵対者はすべてのデータセットを見つけようと努力する必要がある。

保護戦略

サイバーレジリエンスと生存可能性のための設計

敵対者への効果

参照[SP 800-160-2]：[**排除**（先制、否定）；**防止**（遅延、徒労）；**暴露**（検知）]

3.14 システムおよび情報の完全性

拡張セキュリティ要件

3.14.1e 信頼の基点（root of trust）メカニズムまたは暗号化された署名を使用して、[*設定：組織が定めるセキュリティ上重要または不可欠なソフトウェア*]の完全性を検証する。

詳解

破損したソフトウェアは、敵対者が組織のシステムの正常な機能を損なったり妨害したりするために使用する主な攻撃ベクトルであるため、組織のセキュリティ上重要または不可欠なソフトウェアの完全性を検証することは、重要なケイパビリティである。システム開発ライフサイクル全体を通じてソフトウェアの完全性を検証する方法は多数ある。信頼の基点メカニズム（例えば、セキュアブート、TPM（Trusted Platform Module）、UEFI（Unified Extensible Firmware Interface））は、信頼されたコードのみがブート処理中に実行されることを検証する。このケイパビリティは、システムコンポーネントに変更を適用する前に、ファームウェアに対する更新の完全性と真正性を検証し、認可されていない処理によるブートファームウェアの変更を防ぐことで、システムコンポーネントが組織のシステムのブートファームウェアの完全性を保護するのに役立つ。暗号化された署名の採用により、CUI を保存、処理、伝送する重要かつ不可欠なソフトウェアの完全性と真正性が保証される。暗号化された署名には、デジタル署名、および非対称暗号化を使用した署名付きハッシュの計算と適用、ハッシュの生成に使用される鍵の機密性の保護、および公開鍵を使用したハッシュ情報の検証が含まれる。ハードウェアの信頼基点は、よりセキュアであると見なされる。この要件は、3.4.1e および 3.4.3.e をサポートする。

[FIPS 140-3]は、暗号モジュールのセキュリティ要件を提供している。[FIPS 180-4]および[FIPS 202]は、セキュアなハッシュ規格を提供している。[FIPS 186-4]はデジタル署名の規格を提供している。[SP 800-147]は BIOS 保護ガイダンスを提供している。[NIST TRUST]は、信頼の基点プロジェクトに関するガイダンスを提供している。

保護戦略

侵入耐性アーキテクチャ

敵対者への効果

参照[SP 800-160-2]：[**排除**（否定）；**防止**（徒労）；**暴露**（検知）]

3.14.2e 異常な動作や疑わしい動作がないか、組織のシステムとシステムコンポーネントを継続的に監視する。

詳解

監視は、組織のシステムおよびシステムコンポーネントに関連する、異常な、疑わしい、または認可されていない行為や状態を特定するために使用される。このような行為や状態には、異常な内部システム通信トラフィック、情報の認可されていないエクスポート、外部システムへの信号伝送、大容量ファイルの転送、長時間の永続的接続、予期しない場所からの情報へのアクセスの試行、使用中の異常なプロトコルとポート、および疑わしい悪意のある外部アドレスとの通信の試行が含まれる。

物理的、時間的、または地理位置の監査記録情報とシステムからの監査記録の相関関係は、組織が異常な行動の例を特定するのに役立つ場合がある。例えば、特定のシステムへの論理アクセスに対する個人の ID と、その論理アクセスが発生したときに当該個人が施設にいなかったという追加情報との相関関係は、異常な行動を示している。

[SP 800-61]は、インシデント対応に関するガイダンスを提供している。[SP 800-83]は、悪意のあるコードによるインシデントの防止と処理に関するガイダンスを提供している。[SP 800-92]は、コンピュータセキュリティログの管理に関するガイダンスを提供している。[SP 800-94]は、侵入検知と防御に関するガイダンスを提供している。[SP 800-137]は、システムの継続的な監視に関するガイダンスを提供している。

保護戦略

サイバーレジリエンスと生存可能性のための設計

敵対者への効果

参照[SP 800-160-2]：[**暴露**（検知）]

3.14.3e [*設定：組織が定めるシステムおよびシステムコンポーネント*]が、指定された拡張セキュリティ要件の範囲に含まれていること、または目的別のネットワークに分離されていることを確実にする。

詳解

組織のインベントリには、情報技術（IT：Information Technology）、モノのインターネット（IoT：Internet of Things）、運用技術（OT：Operational Technology）、産業用 IOT（IIoT：Industrial Internet of Things）など、様々なシステムやシステムコンポーネントが含まれている場合がある。IT、OT、IoT、および IIoT の融合は、組織の攻撃対象領域を著しく増大させ、対処が困難な攻撃ベクトルを提供する。侵害された IoT、OT、IIoT システムコンポーネントは、CUI（例えば、重要プログラムをサポートするために製造されたオブジェクトの仕様またはパラメータ）を処理する組織の IT システムに対する攻撃の起点として機能する可能性がある。一部の IoT、OT、IIoT システムコンポーネントは CUI を保存、伝送、処理することができる。現世代の IoT、OT、IIoT システムコンポーネントのほとんどは、基本的なプロパティとしてセキュリティを考慮して設計されておらず、セキュリティ機能性をサポートするように構成できない場合がある。このようなシステムコンポーネントとの間の接続は、通常、暗号化されておらず、必要な認証を提供せず、監視もされずログに記録もされない。したがって、これらのコンポーネントは、重大なサイバー脅威をもたらす。IoT、OT、IIoT のセキュリティ機能のギャップは、暗号化、認証、セキュリティスキャン、およびログ記録機能を提供できる中間のシステムコンポーネントを採用することで対処できる—したがって、コンポーネントがインターネットからアクセス可能となるのを防ぐ。ただし、そのような緩和策のオプションが常に使用できるまたは実行可能であるとは限らない。IoT、OT、IIoT デバイスの一部は、不可欠なミッションや事業機能のために、が必要になる可能性があるため、状況はさらに複雑である。そのような場合、サイバー攻撃の影響を受けにくくするために、そのようなデバイスをインターネットから隔離する必要がある。

[SP 800-160-1]は、セキュリティエンジニアリングのプラクティスとセキュリティ設計の概念に関するガイダンスを提供している。

保護戦略

侵入耐性アーキテクチャ

敵対者への効果

参照[SP 800-160-2]：[**排除**（先制、否定）；**防止**（封じ込め、デグレード、遅延、徒労）；**限定**（低減）；**暴露**（検知）]

3.14.4e [*設定：組織が定めるシステムおよびシステムコンポーネント*]を既知の信頼できる状態から[*設定：組織が定める頻度*]でリフレッシュする。

詳解

この要件は、敵対者の標的化ケイパビリティ（すなわち、攻撃する絶好の機会）を減少させることによって、APT 攻撃からのリスクを緩和する。選択されたシステムコンポーネントに非永続性という概念を実装することにより、組織は、組織のシステムやシステムが動作する環境の脆弱性を悪用するのに十分な時間を敵対者に与えない特定の期間、既知の状態のコンピューティングリソースを提供できる。APT 攻撃は、ケイパビリティ、意図、および標的化に関する最高レベルの高度な脅威であるため、組織は長期間にわたって一定の割合の攻撃が成功すると想定している。非永続性のシステムコンポーネントおよびシステムサービスは、保護された情報を使用して必要に応じて起動され、定期的にまたはセッションの終了時に終了する。非永続性は、システムを侵害またはブリーチしようとする敵対者の作業要因を増加させる。

非永続性は、システムコンポーネントをリフレッシュする（例えば、定期的にコンポーネントを再イメージングしたり、様々な一般的な仮想化技法を使用したりする）ことによって実現できる。非永続的なサービスは、「コードとしてのインフラ（Infrastructure as Code）」を使用して実装でき、コンテナ、仮想マシン、または物理マシン上の処理の新しいインスタンス（永続または非永続）を自動的に構築、構成、テスト、展開、および管理することができる。システムコンポーネントとサービスの定期的なリフレッシュでは、コンポーネントやサービスの侵害が発生したかどうかを組織が判断する必要はない（多くの場合、判断が困難な場合がある）。選択したシステムコンポーネントおよびサービスのリフレッシュは、攻撃の拡散または意図されたインパクトを防ぐのに十分な頻度で行われるが、システムが不安定になるような頻度では行われない。格好の無防備な時間帯を悪用する敵対者の能力を妨げるために、定期的にリフレッシュが行われる場合がある。

システムコンポーネントの再イメージングには、既知の信頼できるソースからのファームウェア、オペレーティングシステム、およびアプリケーションの再インストールが含まれる。また、再イメージングには、パッチのインストール、構成設定の再適用、既知の信頼できるソースからのシステムまたはアプリケーションデータのリフレッシュも含まれる。

保護戦略

侵入耐性アーキテクチャ

敵対者への効果

参照[SP 800-160-2]：[**排除**（抹消、先制、否定）；**防止**（デグレード、遅延、徒労）；**限定**（短縮、低減）]

3.14.5e 永続的な組織のストレージの場所のレビューを[*設定：組織が定める頻度*]で実施し、不要になった CUI を削除する。

詳解

プログラム、プロジェクト、契約が進展するにつれて、一部の CUI が不要になる場合がある。不要になった CUI が永続的なストレージからセキュアに削除されることを確実にするために定期的およびイベント関連（例えば、プロジェクトの完了時など）のレビューが行われる。削除は、連邦政府記録保持ポリシーおよび廃棄スケジュールと一致する。情報を必要以上に長く保持すると、その情報は、重要プログラムや HVA 情報を漏出させようと探し回る敵対者の潜在的な標的になる。システム関連情報の不必要な保持は、敵対者に、組織のシステムを介した偵察や横方向の移動に役立つ情報を提供する。あるいは、保持しなければならないが、現在の活動には必要のない情報はオンラインストレージから削除され、セキュアな場所にオフラ

インで保存され、ネットワークを介して個人が情報へ認可されていないアクセスをする可能性を排除する。CUI の削除により、情報は読み取り不能、解読不能、および復旧不能になる。

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

保護戦略

侵入耐性アーキテクチャ

敵対者への効果

参照[SP 800-160-2]: [**排除**(抹消、先制、否定); **防止**(デグレード、遅延、徒労); **限定**(短縮、低減)]

3.14.6e **侵入検知と脅威ハンティングをガイドし、情報を提供するために、[*設定:組織が定める外部組織*]から取得した脅威の兆候に関する情報と効果的な緩和策を使用する。**

詳解

組織が経験した特定の脅威イベント(例えば TTP、標的など)に関連する脅威情報、組織が特定のタイプの脅威に対して効果的であると判断した脅威の緩和策、脅威インテリジェンス(すなわち、発生する可能性のある脅威に関する兆候と警告)は、信頼できる組織から入手され共有される。この脅威情報は、組織のセキュリティオペレーションセンター(SOC:Security Operations Centers)で使用され、監視機能に組み込むことができる。脅威情報の共有には、脅威共有コンソーシアム、政府-商業協同組合、および政府-政府協同組合(例えば、CERTCC、CISA/US-CERT、FIRST、ISAO、DIB CS プログラムなど)に参加している組織からの脅威の兆候、署名、敵対者の TTP が含まれる。機密情報に基づくが、組織の侵入検知システムに容易に組み込むことができる非機密の兆候は、適格な非連邦政府組織が政府のソースから入手することができる。

保護戦略

被害局限化運用

敵対者への効果

参照[SP 800-160-2]: [**暴露**(検知、精査、公開)]

3.14.7e **[*設定:組織が定める検証方法または技法*]を使用して、[*設定:組織が定めるセキュリティ上重要または不可欠なソフトウェア、ファームウェア、ハードウェアコンポーネント*]の正確性を検証する。**

詳解

検証方法には、ソフトウェア、ファームウェア、およびハードウェアコンポーネントの正確性を判断する際に、様々な厳密さの程度がある。例えば、フォーマル検証には、ソフトウェアプログラムがフォーマルなプロパティまたはプロパティのセットを満たしていることを証明することが含まれる。フォーマル検証の性質は、一般的に時間がかかり、商用のオペレーティングシステムやアプリケーションには採用されていない。そのため、暗号化プロトコルの検証など、非常に限定的な用途にのみ適用される可能性がある。ただし、ソフトウェア、ファームウェア、またはハードウェアコンポーネントのセキュリティプロパティがフォーマル検証されている場合そのようなコンポーネントは、より高い保証と統合的信頼性を提供し、フォーマル検証されていない同様のコンポーネントよりも優先される。

[SP 800-160-1]はシステムセキュリティエンジニアリングのプラクティスとセキュリティ設計の概念を使用して、統合的信頼性、セキュアで、サイバーレジリエントなシステムの開発に関するガイダンスを提供している。

保護戦略

侵入耐性アーキテクチャ

敵対者への効果

参照[SP 800-160-2]：[**排除**（否定）；**防止**（徒労）；**暴露**（検知）]

参照資料

法律、大統領令、規則、指示、基準、およびガイドライン[30]

法律および大統領令	
[ATOM54]	Atomic Energy Act (P.L. 83-703), August 1954. https://www.govinfo.gov/app/details/STATUTE-68/STATUTE-68-Pg919
[FOIA96]	Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996. https://www.govinfo.gov/app/details/PLAW-104publ231
[FISMA]	Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.govinfo.gov/app/details/PLAW-113publ283
[40 USC 11331]	Title 40 U.S. Code, Sec. 11331, Responsibilities for Federal information systems standards. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title40/USCODE-2017-title40-subtitleIII-chap113-subchapIII-sec11331
[44 USC 3502]	Title 44 U.S. Code, Sec. 3502, Definitions. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapI-sec3502
[44 USC 3552]	Title 44 U.S. Code, Sec. 3552, Definitions. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapII-sec3552
[44 USC 3554]	Title 44 U.S. Code, Sec. 3554, Federal agency responsibilities. 2017 ed. https://www.govinfo.gov/app/details/USCODE-2017-title44/USCODE-2017-title44-chap35-subchapII-sec3554
[EO 13526]	Executive Order 13526 (2009) Classified National Security Information. (The White House, Washington, DC), DCPD-200901022, December 29, 2009. https://www.govinfo.gov/app/details/DCPD-200901022
[EO 13556]	Executive Order 13556 (2010) Controlled Unclassified Information. (The White House, Washington, DC), DCPD-201000942, November 4, 2010. https://www.govinfo.gov/app/details/DCPD-201000942
ポリシー、規則、および指令	
[32 CFR 2002]	32 CFR Part 2002, Controlled Unclassified Information, September 2016. https://www.govinfo.gov/app/details/CFR-2017-title32-vol6/CFR-2017-title32-vol6-part2002/summary
[OMB A-130]	Office of Management and Budget (2016) Managing Information as a Strategic Resource. (The White House, Washington, DC), OMB Circular A-130, July 2016.

[30] この節の参照資料は、特定の出版日や版数が記載されていない場合、それらの出版物の最新の更新版を指すものとする。

https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[OMB M-19-03] Office of Management and Budget (2018) Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program. (The White House, Washington, DC), OMB Memorandum M-19-03, December 10, 2018. https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf

[CNSSI 4009] Committee on National Security Systems (2015) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Fort George G. Meade, MD), CNSS Instruction 4009. https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[OCIO HVA] Office of the Federal Chief Information Officer (2019), The Agency HVA Process. https://policy.cio.gov/hva/process

基準、ガイドライン、および報告書

[FIPS 140-3] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

[FIPS 180-4] 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

[FIPS 186-4] National Institute of Standards and Technology (2013) Digital Signature Standard (DSS). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 186-4. https://doi.org/10.6028/NIST.FIPS.186-4

[FIPS 199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[FIPS 200] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200

[FIPS 202] National Institute of Standards and Technology (2015) SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 202. https://doi.org/10.6028/NIST.FIPS.202

[SP 800-30] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

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

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

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

[SP 800-53A] Joint Task Force Transformation Initiative (2014) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 4, Includes updates as of December 18, 2014. https://doi.org/10.6028/NIST.SP.800-53Ar4

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

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

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

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

[SP 800-88] Kissel RL, Regenscheid AR, Scholl MA, Stine KM (2014) Guidelines for Media Sanitization. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-88, Rev. 1.

https://doi.org/10.6028/NIST.SP.800-88r1

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

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

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

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

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

[SP 800-147] Cooper DA, Polk T, Regenscheid AR, Souppaya MP (2011) BIOS Protection Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-147. https://doi.org/10.6028/NIST.SP.800-147

[SP 800-150] Johnson CS, Waltermire DA, Badger ML, Skorupka C, Snyder J (2016) Guide to Cyber Threat Information Sharing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-150. https://doi.org/10.6028/NIST.SP.800-150

[SP 800-160-1] Ross RS, Oren JC, McEvilley M (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. https://doi.org/10.6028/NIST.SP.800-160v1

[SP 800-160-2] Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2019) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 2. https://doi.org/10.6028/NIST.SP.800-160v2

[SP 800-161] Boyens JM, Paulsen C, Moorthy R, Bartol N (2015) Supply Chain Risk

Management Practices for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161. https://doi.org/10.6028/NIST.SP.800-161

[SP 800-171] Ross RS, Pillitteri VY, Dempsey KL, Riddle M, Guissanie G (2020) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171, Rev. 2. https://doi.org/10.6028/NIST.SP.800-171r2

[SP 800-181] 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 Special Publication (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1

[SP 800-184] Bartock M, Scarfone KA, Smith MC, Witte GA, Cichonski JA, Souppaya MP (2016) Guide for Cybersecurity Event Recovery. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-184. https://doi.org/10.6028/NIST.SP.800-184

[IR 8011-1] Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 1: Overview. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 1. https://doi.org/10.6028/NIST.IR.8011-1

その他の出版物およびウェブサイト

[DOD ACQ] Department of Defense, Defense Acquisition University (2020), DAU Glossary of Defense Acquisition Acronyms and Terms. https://www.dau.edu/glossary/Pages/Glossary.aspx

[GAO 19-128] U.S. Government Accountability Office (2018) Weapons Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities. (GAO, Washington, DC), Report to the Committee on Armed Services, U.S. Senate, GAO 19-128. https://www.gao.gov/assets/700/694913.pdf

[NARA CUI] National Archives and Records Administration, *Controlled Unclassified Information (CUI) Registry*. https://www.archives.gov/cui

[NIST CSF] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[NIST TRUST] National Institute of Standards and Technology (2019) *Roots of Trust Project*. https://csrc.nist.gov/projects/hardware-roots-of-trust

[NTCTF] National Security Agency (2018) NSA/CSS Technical Cyber Threat Framework, Version 2 (National Security Agency, Fort George G. Meade, MD). https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-nsa-css-technical-cyber-threat-framework.pdf

[Richards09] Richards MG, Hastings DE, Rhodes DH, Ross AM, Weigel AL (2009) Design for Survivability: Concept Generation and Evaluation in Dynamic Tradespace Exploration. *Second International Symposium on Engineering Systems* (Massachusetts Institute of Technology, Cambridge, MA). https://pdfs.semanticscholar.org/3734/7b58123c16e84e2f51a4e172ddee0a8755c0.pdf

付属書 A

用語集

一般的な用語と定義

付属書 A は、NIST 特別出版物（SP）800-172 で使用されているセキュリティに関する用語の定義を提供する。この用語集で別段に定義されていない限り、本出版物で使用されているすべての用語は[CNSSI 4009]*National Information Assurance Glossary* に含まれている定義と一致する。

持続的標的型攻撃（APT 攻撃） (advanced persistent threat) [SP 800-39]	高度なレベルの専門知識と莫大なリソースを保有し、例えば、サイバー攻撃、物理攻撃、詐欺などの複数の攻撃ベクトルを使用して目的を達成する機会を生み出す敵対者。APT 攻撃の目的には、通常、情報を漏出させること、ミッション、プログラム、組織の重要な側面を弱体化または妨害すること、もしくは、将来的にこれらの目的を実行するために自らを配置することを目的として、標的組織の IT インフラ内に足場を確立し拡張することなどが含まれる。持続的標的型攻撃は、長期間にわたって繰り返しその目的を追求し、攻撃に抵抗する防御側の取り組みに適応し、その目的を実行するために必要な相互作用のレベルを確固として維持する。
政府機関 (agency) [OMB A-130]	執行機関または省、軍事部門、連邦政府法人、連邦政府管理法人、または連邦政府の行政府におけるその他の機関、または独立した規制機関。
アセスメント (assessment)	*セキュリティ管理策アセスメント*（*security control assessment*）を参照。
アセッサー (assessor)	*セキュリティ管理策アセッサー*（*security control assessor*）を参照。
攻撃対象領域 (attack surface) [GAO 19-128]	攻撃者がシステム、システム要素、または環境に侵入したり、影響を与えたり、データを抽出したりすることを試みることができる、システム、システム要素、または環境の境界上の一連のポイント。
監査記録 (audit record)	監査されたイベントに関連する監査ログの個々のエントリ。
認証 (authentication) [FIPS 200, Adapted]	多くの場合、システム内のリソースへのアクセスを許可するための前提条件として、ユーザ、プロセス、またはデバイスのアイデンティティを検証すること。
可用性 (availability) [44 USC 3552]	情報へのタイムリーで信頼性の高いアクセスと使用を確保すること。
ベースライン構成 (baseline configuration)	特定の時点で正式にレビューおよび合意された、変更管理手順によってのみ変更できる、システムまたはシステム内の構成アイテムに関する文書化された仕様のセット。

双方向認証 (bidirectional autentication)	2 つの当事者が同時に相互に行う認証。相互認証または二方向認証とも呼ばれる。
境界 (boundary)	システムの物理的または論理的境界。
コンポーネント (component)	*システムコンポーネント*(*system component*)を参照。
機密性 (confidentiality) [44 USC 3552]	個人のプライバシーおよび専有情報を保護するための手段を含む、情報へのアクセスおよび開示に関する認可された制限を維持すること。
構成管理 (configuration management)	システム開発ライフサイクル全体を通して、情報技術製品およびシステムの構成を初期化、変更、監視するためのプロセスを管理することによって、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合。
構成設定 (configuration settings)	ハードウェア、ソフトウェア、またはファームウェアで変更することができる、システムのセキュリティ態勢や機能性に影響を与える一連のパラメータ。
管理対象非機密情報 (controlled unclassified information) [EO 13556]	2009 年 12 月 29 日発行の大統領令 13526 号「*機密指定された国家安全保障情報*(*Classified National Security Information*)」または先行／後継の大統領令、もしくは 1954 年原子力法(その後の改正を含む)で機密指定された情報を除く、法律、規則、または政府全体のポリシーが、保全措置または配布管理を行うことを要求している情報。
重要プログラム(または技術) (critical program (or technology)) [DOD ACQ]	ケイパビリティとミッションの有効性を大幅に向上させる、または不可欠なシステム／ケイパビリティの期待される有効寿命を延長するプログラム。
CUI カテゴリー (CUI categories) [32 CFR 2002]	法律、規則、または政府全体のポリシーが、政府機関に対して保全措置または配布管理を行うことを要求または許可している情報のタイプで、CUI 執行機関が承認し、CUI レジストリに記載されているもの。
CUI 執行機関 (CUI Executive Agent) [32 CFR 2002]	大統領令 13556 号に準拠するために行政機関全体の CUI プログラムを実施し、連邦政府機関のアクションを監督する、国立公文書記録管理局(NARA)。NARA は、この権限を情報安全保障監督局(ISOO)局長に委任している。
CUI プログラム (CUI program) [32 CFR 2002]	すべての連邦政府機関による CUI の取扱いを標準化するための行政機関全体のプログラム。CUI プログラムには、大統領令 13556 号、32 CFR Part 2002、および CUI レジストリによって確立されている規定、編成、手順が含まれる。
サイバーフィジカルシステム (cyber-physical system)	統合された物理特性と論理を通して機能するように設計された、相互作用するデジタル、アナログ、物理、および人的なコンポーネント。

サイバーレジリエンス (cyber resiliency) [SP 800-160-2]	サイバーリソースを使用している、またはサイバーリソースによって有効化されるシステムの悪条件、ストレス、攻撃、または侵害を予測、抵抗、復旧、適応する能力。
被害局限化運用 (damage-limiting operations)	敵対者によるシステム侵害を検知する組織の能力を最大化するために、および、そのような侵害の影響(検知された侵害と検知されなかった侵害の両方)を局限化するために、システムのケイパビリティを使用する手続き上および運用上の手段。
多層防御 (defense-in-depth)	人、技術、運用のケイパビリティを統合して、組織の複数のレイヤーとミッションにわたって可変の障壁を確立する情報セキュリティ戦略。
サイバーレジリエンスと生存可能性のための設計 (designing for cyber resiliency and survivability)	ミッションや事業運営を最大化するために、サイバーリソースの侵害に備え、抵抗、復旧、適応するためのケイパビリティを提供するシステム、ミッション、および事業機能を設計すること。
詳解 (discussion)	セキュリティ管理策や拡張セキュリティ管理策に関する追加の説明情報を提供するために使用される記述。
偽情報配備 (disinformation)	システムや組織のセキュリティ態勢やサイバー準備態勢の状態に関して、敵対者を誤解させ混乱させるために、故意に欺瞞的な情報を敵対者に提供するプロセス。
二重認可 (dual authorization) [CNSSI 4009, Adapted]	実施されているタスクに関して誤った、または認可されていないセキュリティ手順を検知することが可能な、少なくとも二人の認可された人の存在とアクションを要求することにより、特定のリソースへの個々のアクセスを禁止するように設計された保存と取扱いのシステム。
拡張セキュリティ要件 (enhanced security requirements)	NIST SP 800-171 の基本および派生セキュリティ要件に加えて実装されるセキュリティ要件。追加のセキュリティ要件は、相互に支援し補強する 3 つのコンポーネント:(1)侵入耐性アーキテクチャ、(2)被害局限化運用、および(3)サイバーレジリエンスと生存可能性のための設計、を含む多層防御戦略の基盤を提供する。
執行機関 (executive agency) [OMB A-130]	合衆国法典第 5 編第 101 条(5 U.S.C. Sec. 101)で指定された執行部門、合衆国法典第 5 編第 102 条(5 U.S.C. Sec. 102)で指定された軍事部門、合衆国法典第 5 編第 104 条 1 項(5 U.S.C. Sec. 104(1))で規定された独立組織、合衆国法典第 31 編第 91 章(31 U.S.C. Chapter 91)の規定の対象である政府完全所有法人。
外部システム(またはコンポーネント)	組織が定めた認可境界の外にあり、通常、必要なセキュリティ管理策の適用またはセキュリティ管理策の有効性のアセスメン

(external system (or component))	トを組織が直接管理していないシステムまたはシステムのコンポーネント。
外部ネットワーク (external network)	当該組織によって管理されていないネットワーク。
連邦政府機関 (federal agency)	*執行機関*(*executive agency*)を参照。
連邦政府情報システム (federal information system) [40 USC 11331]	執行機関、執行機関の契約事業者、または執行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。
ファームウェア (firmware)	ハードドウェアに保存されたコンピュータプログラムとデータ。通常、読み取り専用メモリ(ROM)やプログラム可能な読み取り専用メモリ(PROM)に保存され、プログラムの実行中にプログラムとデータを動的に書き込んだり変更したりすることができない。*ハードウェア*(*hardware*)と*ソフトウェア*(*software*)を参照。
フォーマル検証 (formal verification)	数学的推論と数学的証明(すなわち、数学の形式手法)を使用して、システムが、望ましいプロパティ、動作、または仕様を満たしている(すなわち、システムの実装は設計の忠実な表現である)ことを検証する体系的なプロセス。
ハードウェア (hardware)	システムの有形な物理コンポーネント。*ソフトウェア*(*software*)と*ファームウェア*(*firmware*)を参照。
高価値資産 (high value asset) [OMB M-19-03]	次のカテゴリーの 1 つ以上に関連する場合における、連邦政府情報または連邦政府情報システムとしての指定。 - *情報価値* – 情報、もしくは情報を処理、保存、伝送する情報システムが、政府またはその敵対者にとって高い価値がある。 - *ミッション不可欠* – 情報または情報システムを所有する政府機関が、大統領政策指令 40 号(PPD-40)の国家継続性ポリシー(National Continuity Policy)に従って承認された主要ミッション不可欠機能(PMEF: Primary Mission Essential Functions)を、情報または情報システムなしでは予想されるタイムライン内に達成することができない。 - *連邦民間企業に不可欠(FCEE:)* – 情報または情報システムが、連邦民間企業のセキュリティとレジリエンスを維持する上で重要な機能を果たす。
インパクト (impact)	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、組織の運営、組織の資産、個人、他の組織、または国家(米国の国家安全保障上の利益を含む)に及ぼす影響。プライバシーに関しては、情報システムが PII を取扱う際に個人が経験する可能性のある悪影響。
インパクト値 (impact value) [FIPS 199]	情報の機密性、完全性、または可用性の侵害から生じる可能性のある最悪のケースをアセスメントした潜在的インパクトを「低」、「中」、「高」の値で表したもの。

インシデント (incident) [44 USC 3552]	法的権限なしに、情報または情報システムの機密性、完全性、または可用性を実際にまたは差し迫って危険にさらす出来事；あるいは、法律、セキュリティポリシー、セキュリティ手順、または利用ポリシーの違反または違反の差し迫った脅威を構成する出来事。
産業用 IoT (industrial internet of things)	産業および製造業の事業プロセスとアプリケーションを強化するために、ネットワーク化され、インターネット接続を使用するセンサ、機器、機械、およびその他のデバイス。
情報 (information) [OMB A-130]	テキスト、数値、グラフィック、地図、叙述、電子、または視聴覚形式を含む、あらゆる媒体または形態の事実、データ、意見などの知識の伝達または表現。
情報フロー制御 (information flow control)	システム内の情報転送がセキュリティポリシーに違反して行われないようにするための手順。
情報リソース (information resources) [44 USC 3502]	人事、装置、資金、情報技術などの情報および関連リソース。
情報セキュリティ (information security) [44 USC 3552]	機密性、完全性、可用性を提供するために、情報およびシステムを認可されていないアクセス、使用、開示、中断、変更、または破壊から保護すること。
情報システム (information system) [44 USC 3502]	情報の収集、処理、維持、使用、共有、配布、または廃棄のために組織された個別の一連の情報リソース。
情報技術 (information technology) [OMB A-130]	政府機関によるデータまたは情報の自動取得、保存、分析、評価、操作、管理、移動、制御、表示、切り替え、交換、送信、または受信で使用される、あらゆるサービス、装置、または相互接続された装置のシステムやサブシステム。本定義の目的においては、政府機関が直接使用するサービスや装置、もしくは、その使用（またはサービスの実施や製品の提供においてかなりの程度その使用）を必要とする政府機関との契約に基づいて契約事業者が使用するサービスや装置が含まれる。情報技術には、コンピュータ、補助装置（セキュリティと監視に必要な映像周辺機器、入力、出力、および記憶デバイスを含む）、コンピュータの中央処理装置によって制御されるように設計された周辺装置、ソフトウェア、ファームウェアおよび類似の手順、サービス（クラウドコンピューティングおよびヘルプデスクサービス、または装置やサービスのライフサイクルの任意のポイントをサポートするその他の専門サービスを含む）、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、契約事業者が取得した装置は含まれない。
コードとしてのインフラ (infrastructure as code)	物理的なハードウェア構成やインタラクティブな構成ツールを採用するのではなく、機械判読可読な構成ファイルを使用して組織の IT インフラスを管理およびプロビジョニングするプロセス。
インサイダー脅威 (insider threat)	インサイダーが、米国のセキュリティに損害を与えるために、故意または無意識に、認可されたアクセスを使用する脅威。この脅威には、スパイ活動、テロ、認可されていない開示、機関のリ

	ソースやケイパビリティの喪失または劣化による米国への損害が含まれまる。
完全性 (integrity) [44 USC 3552]	不適切な情報の変更または破壊から保護すること。情報の否認防止および真正性の確保を含む。
内部ネットワーク (internal network)	セキュリティ管理策の確立、維持、およびプロビジョニングが、組織の従業員または契約事業者の直接の管理下にある、または、組織が管理するエンドポイント間に実装された暗号カプセル化または類似のセキュリティ技術が(機密性と完全性に関して)同じ影響をもたらすネットワーク。内部ネットワークは通常、組織が所有しているが、組織が所有していない場合でも、組織が管理している場合がある。
IoT(モノのインターネット) (internet of things)	ハードウェア、ソフトウェア、ファームウェア、およびアクチュエータを含むデバイスのネットワーク。これにより、デバイスは接続、相互作用、およびデータと情報の自由な交換が可能となる。
悪意のあるコード (malicious code)	システムの機密性、完全性、または可用性に有害なインパクトを及ぼす認可されていないプロセスを実行することを目的としたソフトウェアまたはファームウェア。ホストに感染するウイルス、ワーム、トロイの木馬、またはその他のコードベースのエンティティ。スパイウェアや一部のアドウェアも悪意のあるコードの例である。
媒体 (media) [FIPS 200]	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、大規模集積回路(LSI)メモリチップ、および印刷物(ただし、ディスプレイ媒体は除く)を含むが、これらに限定されない物理デバイスまたは書き込み面。
誤認誘導 (misdirection)	欺瞞リソースや環境を維持および採用し、敵対者の行為をそれらのリソースや環境に向けるプロセス。
モバイルデバイス (mobile device)	個人が一人で簡単に持ち運べるような小さなフォームファクタを有し、物理的な接続なしで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)、取り外し可能または不可能なローカルのデータストレージを持ち、内臓電源を備えている、ポータブルコンピューティングデバイス。また、モバイルデバイスには、音声通信ケイパビリティ、デバイスが情報をキャプチャすることを可能にする搭載センサ、ローカルデータを遠隔地と同期させるための組み込み機能などが含まれる場合がある。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含まれる。
移動標的防御 (moving target defense)	攻撃者に対して不確実性と明らかな複雑さを高め、絶好の機会を減らし、探査と攻撃労力のコストを増加させるために、複数のシステム次元にわたって変化を制御するという概念。
多要素認証 (multi-factor authentication)	認証を実現するために 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(暗号識別デバイス、トークンなど)、または自分自身の特性(生体認証など)が含まれる。 *オーセンティケータ*(*authenticator*)を参照。

相互認証 (mutual authentication)	トランザクションに関与する双方のエンティティが相互に検証を行うプロセス。*双方向認証*(*bidirectional authentication*)を参照。
非連邦政府組織 (nonfederal organization)	非連邦政府システムを所有、運用、または維持するエンティティ。
非連邦政府システム (nonfederal system)	連邦政府システムの基準を満たしていないシステム。
ネットワーク (network)	相互接続されたコンポーネントの集合で実装されたシステム。そのようなコンポーネントには、ルータ、ハブ、ケーブル、通信制御装置、主要な配布センター、および技術的制御デバイスが含まれる。
ネットワークアクセス (network access)	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)を介して通信するユーザ(またはユーザに代わって動作するプロセス)によるシステムへのアクセス。
(政府機関)に代わって (on behalf of (an agency)) [32 CFR 2002]	(i)非行政機関のエンティティが、連邦政府情報を処理、保存、伝送する目的で、情報システムを使用または運用する、もしくは情報を維持または収集する場合、および、(ii)これらの活動が、政府にサービスや製品を提供することに付随するものではない場合、に生じる状況。
運用技術 (operational technology)	物理デバイスの直接的な制御と監視を通じて、物理プロセスの変更を検知または引き起こすために使用されるシステムのハードウェア、ソフトウェア、およびファームウェアコンポーネント。
組織 (organization) [FIPS 200, Adapted]	組織構造内の任意のサイズ、複雑さ、または位置付けのエンティティ。
侵入耐性アーキテクチャ (penetration-resistant architecture)	敵対者が組織システムを侵害し、システム内での永続的な存在を実現する機会を限定するために、技術や手順を使用するアーキテクチャ。
職員のセキュリティ (personnel security) [SP 800-53]	統合的信頼性を必要とする職務および責任について、個人の行い、誠実さ、判断力、忠誠心、信頼性、安定性をアセスメントする規律。
潜在的インパクト (potential impact) [FIPS 199]	機密性、完全性、または可用性の損失は、組織の運営、組織の資産、または個人に対して、(i)*限定的*な悪影響(FIPS 199「低」);(ii)*深刻*な悪影響(FIPS 199「中」);あるいは、(iii)*重大*または*壊滅的*な悪影響(FIPS 199「高」)を及ぼすと予想される。
特権アカウント (privileged account)	特権ユーザの権限を持つシステムアカウント。
特権ユーザ (privileged user)	一般ユーザが実行することを認可されていないセキュリティ関連機能を実行することを認可されている(したがって信頼されている)ユーザ。

記録 (records)	実行された活動のエビデンス、または達成された結果（フォーム、レポート、テスト結果など）の記録（自動および手動）。これは、組織とシステムが意図した通りに実行されていることを検証するための基礎となる。関連するデータフィールド単位（すなわち、プログラムからアクセスすることができ、特定のアイテムに関する完全な情報セットを含むデータフィールドグループ）を参照するためにも使用される。
リモートアクセス (remote access)	外部ネットワーク（インターネットなど）を介して通信するユーザ（またはユーザに代わって動作するプロセス）による組織システムへのアクセス。
リプレイ耐性 (replay resistance)	認可されていない影響を及ぼすことや、認可されていないアクセスを行うことを目的として、伝送された認証またはアクセス制御情報がキャプチャされ、その後に再送信されることに対する保護。
リスク (risk) [OMB A-130]	エンティティが潜在的な状況またはイベントによって脅かされる程度の尺度で、通常、以下の関数である。(i)状況またはイベントが発生した場合に生じる有害なインパクトまたは損害の規模；および(ii)発生の可能性。
リスクアセスメント (risk assessment) [SP 800-30]	システムの運用から生じる、組織の運営（ミッション、機能、イメージ、評判を含む）、組織の資産、個人、他の組織、および国家に対するリスクを識別するプロセス。
信頼の基点 (roots of trust) [NIST TRUST]	特定の重要なセキュリティ機能を実行する、信頼性の高いハードウェア、ファームウェア、およびソフトウェアコンポーネント。信頼の基点は本質的に信頼されているため、設計上セキュアでなければならない。信頼の基点は、セキュリティと信頼を構築するための強固な基盤を提供する。
サニタイズ (sanitization)	媒体に書き込まれたデータを、通常の手段および一部の形式のサニタイズでは特別な手段によって復旧できないようにするために実行されるアクション。 媒体から情報を削除して、データ復旧ができないようにするプロセス。
セキュリティ (security)	システムの使用に対する脅威によってもたらされるリスクにもかかわらず、組織がそのミッションや重要機能を実行できるよう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、組織のリスクマネジメントアプローチの一部を形成することが望ましい抑止、回避、防止、検知、復旧、修正の組み合わせが含まれる場合がある。
セキュリティアセスメント (security assessment)	*セキュリティ管理策アセスメント*（*security control assessment*）を参照。
セキュリティ管理策 (security control) [OMB A-130]	情報システムとその情報の機密性、完全性、可用性を保護するために、情報システムまたは組織のために定められた保全措置または対策。
セキュリティ管理策アセスメント	セキュリティ管理策が正しく実装され、意図した通りに運用され、情報システムまたは組織のセキュリティ要件を満たすこと

(security control assessment) [OMB A-130]	に関して望ましい結果を生み出している程度を判定するための、セキュリティ管理策のテストまたは評価。
セキュリティドメイン (security domain) [CNSSI 4009, Adapted]	セキュリティポリシーを実装し、単一の権限によって管理されるドメイン。
セキュリティ機能 (security functions)	システムの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。
セキュリティソリューション (security solution)	システムまたはシステムコンポーネントに対する指定されたセキュリティ要件を満たすために、組織が行う主要な設計、アーキテクチャ、および実装の選択。
生存可能性 (survivability) [Richards09]	有限期間の障害が価値の提供（すなわち、コストにおける利害関係者の利益）に与えるインパクトを最小限に抑えるシステムの能力（障害の可能性または規模を低減させることによって達成される）；障害時および障害後において最低限許容可能なレベルの価値提供を満たすこと；および／またはタイムリーな復旧。
システム (system)	*情報システム*（*information system*）を参照。
システムコンポーネント (system component) [SP 800-128]	システムの構成要素を表す個別の識別可能な情報技術資産。ハードウェア、ソフトウェア、およびファームウェアを含む。
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しているのか、または要件を満たすために組織がどのように計画しているのかを記述する文書。システムセキュリティ計画は、特に、システム境界、システムが動作する環境、セキュリティ要件の実装方法、および他のシステムとの関係または接続について記述する。
システムサービス (system service)	情報の処理、保存、伝送を促進するシステムによって提供されるケイパビリティ。
戦術、技法、手順（TTP） (tactics, techniques, and procedures (TTP)) [SP 800-150]	行為者の行動。戦術は、行動の最上位レベルの記述であり、技法は、戦術との関連で行動のより詳細な記述を提供し、手順は、技法との関連で行動の下位レベルの非常に詳細な記述を提供する。
汚染 (tainting)	組織が情報の漏出についてアラートを受けられるようにするために、情報、システムまたはシステムコンポーネントに隠れたケイパビリティを組み込むプロセス。
脅威 (threat) [SP 800-30]	情報の認可されていないアクセス、破壊、開示、変更、および／またはサービス妨害により、システムを通じて、組織の運営、組織の資産、個人、他の組織、または国家に有害なインパクトを与える可能性のある状況または事象。

脅威情報 (threat information) [SP 800-150]	組織が脅威から組織自身を防御する、または行為者の行為を検知するのに役立つ可能性のある、脅威に関連するあらゆる情報。脅威情報の主なタイプには、兆候、TTP、セキュリティアラート、脅威インテリジェンスレポート、およびツール構成が含まれる。
脅威インテリジェンス (threat intelligence) [SP 800-150]	意思決定プロセスに必要なコンテキストを提供するために集約、変換、分析、解釈、または補強された脅威情報。

付属書 B

略語

一般的な略語

ASLR	Address Space Layout Randomization （アドレス空間配置のランダム化）
APT	Advanced Persistent Threat （持続的標的型攻撃）
BIOS	Basic Input/Output System （基本入出力システム）
CERT	Computer Emergency Response Team （コンピュータ緊急対応チーム）
CERTCC	CERT Coordination Center （CERT コーディネーションセンター）
CFR	Code of Federal Regulations （連邦規則集）
CIRT	Cyber Incident Response Team （サイバーインシデント対応チーム）
CISA	Cybersecurity and Infrastructure Security Agency （サイバーセキュリティ・インフラストラクチャセキュリティ庁）
CNSS	Committee on National Security Systems （国家安全保障システム委員会）
CRS	Cyber Resiliency and Survivability （サイバーレジリエンスと生存可能性）
CSF	Cyber Security Framework （サイバーセキュリティフレームワーク）
CUI	Controlled Unclassified Information （管理対象非機密情報）
DIB	Defense Industrial Base （防衛産業基盤）
DIB CS	Defense Industrial Base Cybersecurity Sharing （防衛産業基盤サイバーセキュリティ情報共有）
DLO	Damage-Limiting Operations （被害局限化運用）
DMZ	Demilitarized Zone （非武装地帯）
DNS	Domain Name System （ドメインネームシステム）
DRM	Digital Rights Management （デジタル著作権管理）

EO Executive Order
（大統領令）

FIPS Federal Information Processing Standards
（連邦情報処理規格）

FIRST Forum of Incident Response and Security Teams
（セキュリティインシデント対応のための非営利国際調整協力機関）

FISMA Federal Information Security Modernization Act
（連邦情報セキュリティ近代化法）

FOIA Freedom of Information Act
（情報公開法）

GAO Government Accountability Office
（会計検査院）

HVA High Value Asset
（高価値資産）

IIoT Industrial Internet of Things
（産業用 IoT）

IoT Internet of Things
（モノのインターネット）

IP Internet Protocol
（インターネットプロトコル）

ISAC Information Sharing and Analysis Centers
（情報共有分析センター）

ISAO Information Sharing and Analysis Organizations
（情報共有分析機関）

ISOO Information Security Oversight Office
（情報安全保障監督局）

IT Information Technology
（情報技術）

ITL Information Technology Laboratory
（情報技術研究所）

MDR Managed Detection and Response
（検知および対応のマネージドサービス）

MSSP Managed Security Services Provider
（マネージドセキュリティサービスプロバイダ）

MLS Multilevel Secure
（マルチレベルセキュア）

NARA National Archives and Records Administration
（国立公文書記録管理局）

NIST National Institute of Standards and Technology
（国立標準技術研究所）

NISTIR NIST Interagency or Internal Report
（NIST 機関間／内部報告書）

OMB Office of Management and Budget
（行政管理予算局）

OT Operational Technology
（運用技術）

PIN Personal Identification Number
（個人識別番号）

PKI Public Key Infrastructure
（公開鍵基盤）

PLC Programmable Logic Controller
（プログラマブルロジックコントローラ）

PRA Penetration-Resistant Architecture
（侵入耐性アーキテクチャ）

ROI Return On Investment
（投資収益率）

SCRM Supply Chain Risk Management
（サプライチェーンのリスクマネジメント）

SIEM Security Information and Event Management
（セキュリティ情報イベント管理：サイバー攻撃対策ツール）

SOC Security Operations Center
（セキュリティオペレーションセンター）

SP Special Publication
（特別出版物）

TEE Trusted Execution Environment
（高信頼実行環境）

TPM Trusted Platform Module
（トラステッドプラットフォームモジュール）

TTP Tactics, Techniques, and Procedures
（戦術、技法、手順）

USC United States Code
（合衆国法典）

US-CERT United States Computer Emergency Response Team
（米国コンピュータ緊急対応チーム）

VLAN Virtual Local Area Network
（仮想ローカルエリアネットワーク）

付属書 C

マッピング表

管理策および保護戦略に対する拡張セキュリティ要件のマッピング

表 C-1 から表 C-14 は、[SP 800-53]のセキュリティ管理策に対する拡張セキュリティ要件のマッピングを提供している[31]。さらに、これらの表は、拡張セキュリティ要件が侵入耐性アーキテクチャ（PRA）、被害局限化運用（DLO）、サイバーレジリエンスと生存可能性（CRS）のための設計、またはそれらの組み合わせを促進するかを識別している。マッピング表は、情報提供のみを目的として含まれており、第 3 章で規定されているセキュリティ要件を超える追加のセキュリティ要件を付与するものではない。場合によっては、セキュリティ管理策には、CUI を保護するために必要なものを超えるさらなる期待が含まれている。セキュリティ要件に関連するセキュリティ管理策の部分のみが適用される。拡張要件を満たしていることは、対応する NIST セキュリティ管理策または拡張管理策も満たしていることを意味するものではない。

[NIST CSF]を実装している、または実装を計画している組織は、マッピング表を使用して、サイバーセキュリティフレームワーク（Cybersecurity Framework）のコア機能：識別（Identify）、保護（Protect）、検知（Detect）、対応（Respond）、および復旧（Recover）に関連するカテゴリーとサブカテゴリーの同等の管理策を見つけることができる。マッピング情報は、組織の確立された情報セキュリティプログラムが NIST のセキュリティ管理策を中心に構築されている場合に、そうしたプログラムの一環としてセキュリティ要件への準拠を実証したい組織にとって有用である。

[31] 表 C-1 から表 C-14 のセキュリティ管理策は、NIST SP 800-53 改訂第 5 版から引用されている。

表 C-1:「アクセス制御」要件のマッピング

セキュリティ要件		多層防御戦略			NIST SP800-53 *関連セキュリティ要件*	
		PRA	DLO	CRS		
3.1.1e	重要または機微なシステムおよび組織の運営を実行するために、二重認可を採用する。	x	x		AC-3(2)	アクセス実施 *二重認可*
					AU-9(5)	監査情報の保護 *二重認可*
					CM-5(4)	変更に対するアクセス制限 *二重認可*
					CP-9(7)	システムバックアップ *削除や破壊に対する二重認可*
					MP-6(7)	媒体のサニタイズ *二重認可*
3.1.2e	システムおよびシステムコンポーネントへのアクセスを、組織により所有、支給、または発行された情報リソースのみに制限する。	x			AC-20(3)	外部システムの使用 *組織が所有していないシステム — 使用制限*
3.1.3e	接続されたシステムのセキュリティドメイン間の情報フロー制御のために、[*設定:組織が定めるセキュアな情報転送ソリューション*]を採用する。	x			AC-4	情報フローの実施
					AC-4(1)	情報フローの実施 *オブジェクトのセキュリティおよびプライバシー属性*
					AC-4(6)	情報フローの実施 *メタデータ*
					AC-4(8)	情報フローの実施 *セキュリティおよびプライバシーポリシーフィルター*
					AC-4(12)	情報フローの実施 *データタイプ識別子*
					AC-4(13)	情報フローの実施 *ポリシー関連サブコンポーネントへの分解*
					AC-4(15)	情報フローの実施 *容認されない情報の検知*

表 C-2:「意識向上およびトレーニング」要件のマッピング

セキュリティ要件		多層防御戦略			NIST SP800-53 *関連セキュリティ要件*	
		PRA	DLO	CRS		
3.2.1e	ソーシャルエンジニアリング、持続的標的型攻撃の行為者、ブリーチ、および疑わしい行動からの脅威の認識と対応に重点を置いた意識向上トレーニングを[*設定:組織が定める頻度*]で提供する。意識向上トレーニングを[*設定:組織が定める頻度*]で、または脅威に重大な変更がある場合に、更新する。		x		AT-2	リテラシートレーニングおよび意識向上
					AT-2(3)	リテラシートレーニングおよび意識向上 *ソーシャルエンジニアリングおよびマイニング*
					AT-2(4)	リテラシートレーニングおよび意識向上 *疑わしい通信および異常なシステム動作*
					AT-2(5)	リテラシートレーニングおよび意識向上 *持続的標的型攻撃(APT 攻撃)*
					AT-2(6)	リテラシートレーニングおよび意識向上 *サイバー脅威環境*
3.2.2e	[*設定:組織が定める役割*]に対する意識向上トレーニングに現在の脅威シナリオに沿った実践的な演習を含め、トレーニングに関与する個人およびその監督者にフィードバックを提供する。		x		AT-2(1)	リテラシートレーニングおよび意識向上 *実践的な演習*
					AT-6	トレーニングのフィードバック

表 C-3:「監査および説明責任」要件のマッピング

セキュリティ要件	多層防御戦略			NIST SP800-53 *関連セキュリティ要件*
	PRA	DLO	CRS	
監査およびと説明責任に関する拡張セキュリティ要件はない。				

表 C-4:「構成管理」要件のマッピング

セキュリティ要件		多層防御戦略			NIST SP800-53 *関連セキュリティ要件*	
		PRA	DLO	CRS		
3.4.1e	承認および実装されたシステムコンポーネントに対して信頼できるソースおよび説明責任を提供するために、信頼できるソースおよびリポジトリを確立し維持する。	x		x	CM-2	ベースライン構成
					CM-3	構成変更管理
					CM-8	システムコンポーネントのインベントリ
					SI-14(1)	非永続性 *信頼できるソースからのリフレッシュ*
3.4.2e	誤った構成または認可されていないシステムコンポーネントを検知するために、自動化されたメカニズムを採用する。検知後、パッチ適用、再構成、またはその他の緩和策を促進するために、[*選択(1つ以上):コンポーネントを取り除く;コンポーネントを検疫または修復ネットワークに配置する*]。	x			CM-2	ベースライン構成
					CM-3	構成変更管理
					CM-3(5)	構成変更管理 *自動化されたセキュリティ対応*
					CM-3(8)	構成変更管理 *構成変更の防止または制限*
3.4.3e	システムコンポーネントの最新かつ完全で的確なすぐに利用可能なインベントリを維持するために、自動化された検出および管理ツールを採用する。	x			CM-2(2)	ベースライン構成 *的確性および最新性サポートの自動化*
					CM-8(2)	システムコンポーネントのインベントリ *自動化されたメンテナンス*

表 C-5:「識別および認証」要件のマッピング

セキュリティ要件		多層防御戦略			NIST SP800-53 *関連セキュリティ要件*	
		PRA	DLO	CRS		
3.5.1e	暗号をベースとしたリプレイ攻撃耐性のある双方向認証を使用してネットワーク接続を確立する前に、[*設定:組織が定めるシステムおよびシステムコンポーネント*]を識別および認証する。	x			IA-2(8)	識別および認証(組織のユーザ) *アカウントへのアクセス ― リプレイ攻撃耐性*
					IA-3	デバイスの識別および認証
					IA-3(1)	デバイスの識別および認証 *暗号双方向認証*
3.5.2e	多要素認証または複雑なアカウント管理をサポートしていないシステムおよびシステムコンポーネントに、パスワードの生成、保護、ローテーション、管理のための自動化されたメカニズムを採用する。	x			IA-5(18)	オーセンティケータ管理 *パスワードマネージャー*
3.5.3e	システムコンポーネントが、既知で、認証されており、適切に構成された状態、または信頼プロファイル内でない限り、組織のシステムに接続することを禁止する自動化または手動/手続き型のメカニズムを採用する。	x			CM-8(3)	システムコンポーネントのインベントリ *認可されていないコンポーネントの自動化された検知*
					IA-3(4)	デバイスの識別および認証 *デバイス証明*
					SI-4(22)	システム監視 *認可されていないネットワークサービス*

表 C-6:「インシデント対応」要件のマッピング

セキュリティ要件		多層防御戦略			NIST SP800-53 *関連セキュリティ要件*	
		PRA	DLO	CRS		
3.6.1e	[*設定:組織が定める期間*]運営するセキュリティオペレーションセンターのケイパビリティを確立し維持する。		x		IR-4(14)	インシデント対応 *セキュリティオペレーションセンター*
3.6.2e	[*設定:組織が定める期間*]内に、組織が展開できるサイバーインシデント対応チームを確立し維持する。		x		IR-4(11)	インシデント対応 *統合インシデント対応チーム*
					IR-7	インシデント対応支援

表 C-7:「メンテナンス」要件のマッピング

セキュリティ要件	多層防御戦略			NIST SP800-53 *関連セキュリティ要件*
	PRA	DLO	CRS	
メンテナンスに関する拡張セキュリティ要件はない。				

表 C-8:「媒体保護」要件のマッピング

セキュリティ要件	多層防御戦略			NIST SP800-53 *関連セキュリティ要件*
	PRA	DLO	CRS	
媒体保護に関する拡張セキュリティ要件はない。				

表 C-9:「職員のセキュリティ」要件のマッピング

セキュリティ要件		多層防御戦略			NIST SP800-53 *関連セキュリティ要件*	
		PRA	DLO	CRS		
3.9.1e	個人に対して[*設定:組織が定める拡張した職員のスクリーニング*]を実施し、[*設定:組織が定める頻度*]で個人の職位と CUI へのアクセスを再アセスメントする。		x		PS-3	職員のスクリーニング
					SA-21	開発者のスクリーニング
3.9.2e	CUI にアクセスする個人について敵対的情報が発生または取得された場合、組織のシステムが保護されていることを確実にする。		x		PS-3	職員のスクリーニング
					SA-21	開発者のスクリーニング

表 C-10:「物理的保護」要件のマッピング

セキュリティ要件	多層防御戦略			NIST SP800-53 *関連セキュリティ要件*
	PRA	DLO	CRS	
物理的保護に関する拡張セキュリティ要件はない。				

表 C-11：「リスクアセスメント」要件のマッピング

セキュリティ要件	多層防御戦略			NIST SP800-53 *関連セキュリティ要件*	
	PRA	DLO	CRS		
3.11.1e リスクアセスメントの一環として、組織のシステム、セキュリティアーキテクチャ、セキュリティソリューションの選択、監視、脅威ハンティング、対応および復旧措置の策定をガイドし、情報を提供するために、[*設定：組織が定める脅威インテリジェンスのソース*]を採用する。		x		PM-16	脅威認識プログラム
				PM-16(1)	脅威認識プログラム *脅威インテリジェンスを共有するための自動化された手段*
				RA-3(3)	リスクアセスメント *動的脅威認識*
3.11.2e [*設定：組織が定めるシステム*]における侵害の兆候を捜索し、既存の管理策を回避する脅威を検知、追跡、および妨害するために、[*選択（1 つ以上）*：[*設定：組織が定める頻度*]；[*設定：組織が定めるイベント*]]でサイバー脅威ハンティング活動を実施する。		x		RA-10	脅威ハンティング
				SI-4(24)	システム監視 *侵害の徴候*
3.11.3e アナリストをサポートし、組織、システム、システムコンポーネントに対するリスクを予測および特定するために、高度な自動化と分析ケイパビリティを採用する。		x		RA-3(4)	リスクアセスメント *予測的サイバー分析*
				SI-4(24)	システム監視 *侵害の徴候*
3.11.4e 選択したセキュリティソリューション、セキュリティソリューションの根拠、およびリスクの決定をシステムセキュリティ計画で文書化または参考文献目録として作成する。	x			AC-4	情報フローの実施
				CA-3	情報交換
				CM-8	システムコンポーネントのインベントリ
				PL-2	システムセキュリティおよびプライバシー計画
				PL-8	セキュリティおよびプライバシーアーキテクチャ
				SC-7	境界保護
3.11.5e 現在のおよび蓄積された脅威インテリジェンスに基づいて、組織のシステムおよび組織に対して予想されるリスクに対処するために、セキュリティソリューションの有効性を[*設定：組織が定める頻度*]でアセスメントする。		x		RA-3	リスクアセスメント
				RA-3(3)	リスクアセスメント *動的脅威認識*
3.11.6e 組織のシステムおよびシステムコンポーネントに関連するサプライチェーンリスクをアセスメント、対応、および監視する。	x			RA-3	リスクアセスメント
				RA-3(1)	リスクアセスメント *サプライチェーンのリスクアセスメント*

3.11.7e	組織のシステムおよびシステムコンポーネントに関連するサプライチェーンリスクを管理するための計画を策定し；[*設定：組織が定める頻度*]で計画を更新する。	x			SR-2	サプライチェーンのリスクマネジメント計画

表 C-12：「セキュリティアセスメント」要件のマッピング

セキュリティ要件	多層防御戦略			NIST SP800-53 *関連セキュリティ要件*	
	PRA	DLO	CRS		
3.12.1e 自動化されたスキャンツールと、対象分野の専門家によるアドホックテストを活用して、[*設定：組織が定める頻度*]で侵入テストを実施する。	x	x		CA-8	侵入テスト
				SR-6(1)	サプライヤのアセスメントおよびレビュー *テストおよび分析*

表 C-13:「システムおよび通信の保護」要件のマッピング

セキュリティ要件	多層防御戦略			NIST SP800-53 *関連セキュリティ要件*	
	PRA	DLO	CRS		
3.13.1e 悪意のあるコードの伝播の程度を減らすために、[*設定:組織が定めるシステムコンポーネント*]に多様性を作る。			x	PL-8	セキュリティおよびプライバシーアーキテクチャ
				SA-17(9)	開発者のセキュリティおよびプライバシーのアーキテクチャおよび設計 *設計の多様性*
				SC-27	プラットフォームに依存しないアプリケーション
				SC-29	異質性
				SC-29(1)	異質性 *仮想化技法*
				SC-47	代替通信経路
3.13.2e 運用にある程度の予測不可能性を導入するために、組織のシステムおよびシステムコンポーネントに[*設定:組織が定める、システムとシステムコンポーネントの変更および変更の頻度*]を実装する。			x	SC-30(2)	秘匿化および誤認誘導 *ランダム性*
3.13.3e 敵対者を混乱させ誤解させるために、[*設定:組織が定める技術的および手続き的手段*]を採用する。			x	SC-8(4)	伝送の機密性および完全性 *通信の秘匿化またはランダム化*
				SC-26	デコイ
				SC-30	秘匿化および誤認誘導
				SC-30(2)	秘匿化および誤認誘導 *ランダム性*
				SI-20	汚染
3.13.4e [*選択:(1 つ以上):[設定:組織が定める物理的分離技法];[設定:組織が定める論理的分離技法]*]を組織のシステムおよびシステムコンポーネントに採用する。	x		x	SC-7	境界保護
				SC-7(13)	境界保護 *セキュリティツール、メカニズム、およびサポートコンポーネントの分離*
				SC-7(21)	境界保護 *システムコンポーネントの分離*
				SC-7(22)	境界保護 *異なるセキュリティドメインに接続するための個別のサブネット*
				SC-25	シンノード
3.13.5e [*設定:組織が定めるシステム機能またはリソース*]を[*設定:組織が定める頻度*]で配布および再配置する。			x	SC-30(3)	秘匿化および誤認誘導 *処理場所および保管場所の変更*

表 C-14:「システムおよび情報の完全性」要件のマッピング

セキュリティ要件	多層防御戦略			NIST SP800-53 *関連セキュリティ要件*	
	PRA	DLO	CRS		
3.14.1e 信頼の基点(root of trust)メカニズムまたは暗号化された署名を使用して、[*設定:組織が定めるセキュリティ上重要または不可欠なソフトウェア*]の完全性を検証する。	x			SI-7(6)	ソフトウェア、ファームウェア、および情報の完全性 *暗号保護*
				SI-7(9)	ソフトウェア、ファームウェア、および情報の完全性 *ブートプロセスの確認*
				SI-7(10)	ソフトウェア、ファームウェア、および情報の完全性 *ブートファームウェアの保護*
3.14.2e 異常な動作や疑わしい動作がないか、組織のシステムとシステムコンポーネントを継続的に監視する。			x	AU-6(6)	監査記録のレビュー、分析、および報告 *物理的監視との相関*
				SI-4(4)	システム監視 *インバウンドおよびアウトバウンド通信のトラフィック*
				SI-4(7)	システム監視 *疑わしいイベントへの自動応答*
				SI-4(11)	システム監視 *通信トラフィック異常の分析*
				SI-4(13)	システム監視 *トラフィックおよびイベントのパターンの分析*
				SI-4(18)	システム監視 *トラフィックおよび秘密の漏出の分析*
				SI-4(19)	システム監視 *個人のリスク*
				SI-4(20)	システム監視 *特権ユーザ*
3.14.3e [*設定:組織が定めるシステムおよびシステムコンポーネント*]が、指定された拡張セキュリティ要件の範囲に含まれていること、または目的別のネットワークに分離されていることを確実にする。	x			AC-3	アクセス実施
				AC-4	情報フローの実施
				SA-8	セキュリティおよびプライバシーエンジニアリングの原則
				SC-2	システムおよびユーザ機能の分離
				SC-3	セキュリティ機能の分離
				SC-49	ハードウェアによる分離およびポリシーの実施
3.14.4e [*設定:組織が定めるシステムおよびシステムコンポーネント*]を既	x			SI-14	非永続性
				SI-14(1)	非永続性

	知の信頼できる状態から[*設定:組織が定める頻度*]でリフレッシュする。					*信頼できるソースからのリフレッシュ*
					SI-14(2)	非永続性 *非永続的情報*
					SI-14(3)	非永続性 *非永続的接続性*
3.14.5e	永続的な組織のストレージの場所のレビューを[*設定:組織が定める頻度*]で実施し、不要になったCUIを削除する。	x			SC-28(2)	保管中の情報の保護 *オフラインストレージ*
					SI-14(2)	非永続性 *非永続的情報*
3.14.6e	侵入検知と脅威ハンティングをガイドし、情報を提供するために、[*設定:組織が定める外部組織*]から取得した脅威の兆候に関する情報と効果的な緩和策を使用する。		x		PM-16(1)	脅威認識プログラム *脅威インテリジェンスを共有するための自動化された手段*
					SI-4(24)	システム監視 *侵害の徴候*
					SI-5	セキュリティのアラート、勧告、および指令
3.14.7e	[*設定:組織が定める検証方法または技法*]を使用して、[*設定:組織が定めるセキュリティ上重要または不可欠なソフトウェア、ファームウェア、ハードウェアコンポーネント*]の正確性を検証する。	x			SA-17	開発者のセキュリティおよびプライバシーのアーキテクチャおよび設計

付属書 D

敵対者への効果

脅威イベントとリスクに対する潜在的影響

サイバーレジリエンスソリューションは、特に、脅威イベント[32]の発生の可能性、脅威イベントが損害を与える能力、およびその損害の程度を低減させることによって、リスクに何らかの影響を及ぼす場合にのみ関係する[33]。サイバーレジリエンスについて示されるシステムアーキテクチャ、設計、実装、および運用の分析のタイプには、組織が懸念する脅威シナリオの一部である脅威イベントに対して、代替策がどのような影響を及ぼす可能性があるかについての考慮を含むことができる。

敵対的な脅威からシステムを保護するという観点から、敵対者に対する望ましい影響として、5 つの高レベルな影響（*リダイレクト*、*排除*、*妨止*、*限定*、および*暴露*）を特定することができる。これらの影響は議論には役立つが、多くの場合、有効性に関する具体的な尺度の規定を促進するにはあまりにも一般的である。したがって、影響に関するより具体的な以下の分類が定義される。

- **リダイレクト**をサポートするための*阻止*、*逸（そ）らし*、*欺き*
- **排除**をサポートするための*否定*、*先制*、*抹消*
- **防止**をサポートするための*封じ込め*、*デグレード*、*遅延*、*徒労*
- **限定**をサポートするための*短縮*、*低減*
- **暴露**をサポートするための*検知*、*公開*、*精査*

これらの影響は戦術的（すなわち、特定の脅威イベントまたはシナリオに対して局所的）ではあるが、その繰り返しの成果が戦略的な影響をもたらす可能性がある。

表 D-1 は、影響を定義し、各影響がリスクをどのように軽減できるかを示し、攻撃から保護するためのサイバーレジリエンス技法を実装するための特定のアプローチの使用が、どのように特定された影響をもたらすことができるかを示している[34]。防御側という用語は、保護機能の提供または適用に責任を負う組織または組織のスタッフを指している。可能性とインパクトは減らすことができるが、リスクは排除できないことに留意すべきである。したがって、否定、検知、または抹消などの完全性を示唆する名称を持つものであっても、完全な影響は想定できない。

[32] 脅威イベントという用語は、望ましくない結果やインパクトを引き起こす可能性のあるイベントまたは状況を指す。脅威イベントは、敵対的または非敵対的な脅威ソースのいずれかによって引き起される可能性がある。ただし、この節では、敵対的脅威、特にその脅威イベントを敵対者の行為として識別できる APT 攻撃に対する影響に重点を置いている。

[33] 様々なリスクモデルが有効で有用である一方で、ほとんどのモデルにおいて次の 3 つの要素が共通している：(1)発生の可能性（すなわち、一連の相互依存イベントで構成される脅威イベントまたは脅威シナリオが敵対者によって発生または開始される可能性）、(2)インパクトの可能性（すなわち、脅威イベントまたは脅威シナリオが脆弱性、弱点、および素因条件につながる可能性）、(3)およびインパクトレベル[SP 800-30]。

[34] サイバーレジリエンス技法とアプローチの詳細については、[SP 800-160-2]の付属書 H を参照。

表 D-1：サイバーレジリエンス技法が敵対的脅威イベントに及ぼす影響

意図された影響	リスクへのインパクト	期待される結果
リダイレクト（阻止、逸（そ）らし、欺きを含む） 防御側が選択したリソースから脅威イベントを遠ざける。	発生の可能性を低減し、（より少ない程度まで）インパクトの可能性を低減する。	• 敵対者の試みが停止する。 • 敵対者は、誤った標的に設定し、誤った情報を与えられたりして行動する。
阻止 敵対者に恐怖（例えば、身元が特定される恐怖や報復を受ける恐怖）を植え付けること、あるいはそれらの行為が意図された影響を達成するのではないかという疑念（例えば、標的の存在への疑念）を抱かせることによって、さらなる行為を行うことを思いとどまらせる。	発生の可能性を低減する。	• 敵対者は行為を停止または中断する。 **例**：防御側は、偽情報を配備して、組織が実際よりも攻撃を検知する能力が高く、大規模な反撃を開始することを厭わないように見せかける。したがって、敵対者は、検知と報復を恐れて、攻撃を開始しないことを選択する。
逸（そ）らし 脅威イベントを防御側が選択したリソースに向けさせる。	発生の可能性を低減する。	• 敵対者は、防御側が選択したリソースに対する行為に焦点を定めなおす。 • 敵対者は、防御側の権限外（例えば、他の組織）の標的に行為を向ける。 • 敵対者は、防御側が標的として選択していないリソースに影響を与えない。 **例**：防御側は、信頼されていない外部エンティティが相互にやり取りできるインターネットから見えるエンクレーブ（enclave）と、信頼されたサプライヤ、パートナー、または顧客（事前定義されたセグメンテーション）のVPNを介してのみアクセス可能なプライベートなエンクレーブを保持する。 **例**：防御側は、重要なリソースを隠すために非永続型の情報と難読化を使用し、サイバーリソースの機能的再配置と偽情報を組み合わせて、敵対者の行動が重要なリソースに損害を与えることができないサンドボックス化されたエンクレーブに敵対者を誘い込む。
欺き 敵対者を、防御されたシステム、ミッション、組織、または防御側のケイパビリティや TTP（戦術、技法、手順：Tactics, Techniques and Procedure）に関する虚偽の情報を信じるように仕向ける。	発生の可能性を低減する、および／または、インパクトの可能性を低減する。	• 敵対者が攻撃の根拠としている前提が誤っているため、敵対者の労力が無駄になる。 • 敵対者は虚偽の情報に基づいて行動を起こすので、その情報を得ていたことが明らかになる。 **例**：防御側は、計画しているサイバーセキュリティへの投資に関する虚偽の情報（偽情報）を戦略的に配備する。その結果、敵対者のマルウェア開発は、存在しないサイバーセキュリティ保護に対抗することに焦点を当てさせられることによって無駄になる。 **例**：防御側は選択的に仕掛けられた虚偽の情報（偽情報）とハニーネット（誤認誘導）を使用

意図された影響	リスクへのインパクト	期待される結果
		して、敵対者が仮想サンドボックスにマルウェアを集中させると同時に、実際のリソースを隠すために難読化を使用する。
排除（抹消、先制、否定を含む） 脅威イベントにインパクトがないことを確認する。	発生の可能性を低減する、および／または、インパクトの可能性を低減する。	• 敵対者の労力やリソースは、適用できないか、無駄になる。
抹消 安全でない、正しくない、または破損していることがわかっている、または疑わしいリソースを削除する。	同じ脅威シナリオでの後続のイベントへのインパクトの可能性を低減する。	• 誤動作、不適切な動作、または疑わしいリソースが通常の動作に復元される。 • 敵対者は、敵対者向けの脅威メカニズム（例えば、悪意のあるコードなど）が削除されるため、一定期間ケイパビリティを失う。 • 敵対者が制御するリソースは、被害がひどくなるので、完全に再構築されないと、機能を実行したり、使用できる状態に復元したりすることはできない。 **例**：防御側は仮想化を使用して、重要なソフトウェア（非永続的なサービス）を既知の正常なコピーからランダムな間隔でリフレッシュする（一時的な予測不可能性）。その結果、ソフトウェアに埋め込まれたマルウェアが削除される。
先制 脅威イベントが発生する可能性のある、または攻撃が予測される状態を未然に防ぐか、回避する。	発生の可能性を低減する。	• 敵対者のリソースを適用できない、または敵対者が行為を行うことができない（例えば、敵対者が要求する資源が破壊されたりアクセス不能になったりするため）。 **例**：不要なネットワーク接続が無効になっている（非永続的な接続）ため、そのインタフェースを介した攻撃を行うことができない。 **例**：リソースの位置が変更（資産の可動性）されるため、新しい場所では脅威イベントの影響を受けることはない。
否定 脅威イベントがインパクトを及ぼすとは予想できない条件を作成する。	インパクトの可能性を低減する。	• 敵対者は攻撃を仕掛けることはできるが、部分的にも成功することはない。敵対者がその攻撃の根拠とした前提がもはや有効ではなくなるため、敵対者の労力は無駄になり、その結果、意図された影響を達成することができなくなる。 **例**：重要なソフトウェアの微妙なバリエーション（合成の多様性）が実装され、その結果、敵対者のマルウェアが標的のソフトウェアを侵害できなくなる。
防止（封じ込め、デグレード、遅延、徒労を含む） 脅威イベントが有害なインパクトや結果を引き起こすことをより困難にする。	インパクトの可能性を低減し、インパクトのレベルを低減する。	• 敵対者の行為は範囲が制限され、完全な影響を達成できず、敵対者のタイムラインに従って行われず、敵対者が計画していたよりも大きなリソースを必要とする。
封じ込め 脅威イベントの影響を、限られたリソースセットに限	インパクトのレベルを低減する。	• 敵対者は、計画よりも少ないリソースに影響を与える可能性がある。敵対者の目標を達成するという点で、敵対者にとっての行為の

意図された影響	リスクへのインパクト	期待される結果
定する。		価値は低減される。 **例**：防御側組織は、内部ファイアウォールと論理的に分離されたネットワーク（動的セグメンテーション）の組み合わせに変更を加えて、マルウェアの検知に応じてエンクレーブを分離し、マルウェアの影響は最初に感染したエンクレーブのみに限定される。
デグレード 脅威イベントの予想される結果を減少する。	インパクトの可能性を低減、および／または、インパクトのレベルを低減する。	• 敵対者が標的とするすべてのリソースが影響を受けるわけではない、あるいは標的とするリソースは、敵対者が求めているよりも影響を受ける程度が低い。 **例**：防御側は、エンドユーザシステムと一部の重要なサーバの両方で、複数のブラウザとオペレーティングシステム（アーキテクチャの多様性）を使用している。その結果、特定のソフトウェアを標的にしたマルウェアは、標的となるシステムのサブセットしか侵害できず、ミッションまたは事業機能を完了するために十分な数が引き続き可動している。
遅延 脅威イベントが有害なインパクトを及ぼすまでに必要な時間を長くする。	インパクトの可能性を低減、および／または、インパクトのレベルを低減する。	• 敵対者は意図された影響を達成するが、意図された期間内ではない。 **例**：リソースに割り当てられた保護手段（アクセス制御、暗号化など）は、リソースの重要度（多層防御の調整）に基づいて、数と強度が増加する。認証チャレンジの頻度はランダムに変化（時間的な予測不能）し、より重要なリソースの頻度が高くなる。その結果、攻撃者が標的とするリソースの侵害に成功するには、より多くの時間がかかる。
徒労 敵対者が特定の結果を達成するために必要な労力またはリソースのレベルを上げる。	インパクトの可能性を低減する。	• 敵対者は、追加の労力やリソースが必要であると判断した場合に、計画された、または部分的に完了した行為を断念する。 • 敵対者は、より多くのリソースを適用することによってのみ、目的の時間枠で意図された影響を達成する。したがって、敵対者の投資収益率（ROI）は減少する。 • 敵対者は、将来の使用のために予約する予定であった TTPs を明らかにする。 **例**：防御側は、追加の緩和策（多層防御の調整）により、中程度の重要度のコンポーネントの防御を強化する。これらを克服するために、敵対者は、より価値の高い防御側の標的に対して使用するために予約する予定であったTTPを調整し、展開しなければならない。 **例**：防御側は、有効だが役に立たない大量の情報をデータストアに追加し（難読化）、敵対者はさらなるアクションを実行する前に、より多くのデータを漏出させて分析する必要がある。
限定（短縮と低減を含む） 時間、システム リソース、および/またはミッションま	インパクトのレベルを低減し、同じ脅威シナリオにおける後続	• 敵対者の有効性は制限されている。

意図された影響	リスクへのインパクト	期待される結果
たは事業へのインパクトの観点から、それらが引き起こす被害や影響を限定することで、現実化した脅威イベントの結果を制限する。	イベントのインパクトの可能性を低減する。	
短縮 脅威イベントの有害な影響の持続時間を限定する。	インパクトのレベルを低減する。	• 敵対者の行為が防御側のリソースに影響を与える期間は限定されている。 **例**：防御側は、タイムクリティカルなコンポーネントに対して多様なサプライヤ（サプライチェーンの多様性）を採用している。その結果、敵対者の攻撃が原因で、あるサプライヤがシャットダウンした場合、防御側は他のサプライヤの使用を増やすことができるため、重要なコンポーネントがない状態である時間を短縮できる。
低減 脅威イベントによる被害の程度を減少する。被害の程度は、幅（すなわち、影響を受けるリソースの数）と深さ（すなわち、特定のリソースに対する損害のレベル）の 2 つの次元がある。	インパクトのレベルを低減する。	• 敵対者の行為によるミッションまたは事業運営への被害のレベルは、影響を受けるすべてのリソースの部分的な復元または再構成によって低減される。 **例**：破損または疑わしいと判断されたリソース（完全性チェック、動作の検証）は、機能が制限された古い、破損していないリソース（保護されたバックアップと復元）から復元される。 • 敵対者の行為によるミッションまたは事業運営への被害のレベルは、影響を受けるリソースの一部を完全に復元または再構成することにより低減される。 **例**：組織は、侵害された 3 つのリソースのうちのいずれかを削除し、同じまたは同等のミッションまたは事業機能に対して新しいリソース（交換、専門化）を提供する。
暴露（検知、精査、公開を含む） 同一または類似の環境での、脅威イベントと、複製または類似の可能性のある脅威イベントに対する無知によるリスクを低減する。	インパクトの可能性を低減する。	• 防御側が脅威インテリジェンスを開発し、共有することによってより適切に準備を整えることができているので、敵対者はステルスの利点を失う。
検知 イベントが発生している、発生した、または（兆候、警告、前兆行為に基づいて）発生しようとしているという事実を検出または識別することにより、脅威イベントまたはその影響を特定する。	インパクトの可能性を低減し、（対応に応じて）インパクトのレベルを低減する。	• 敵対者の行為は防御的な反応の影響を受けやすくなる。 **例**：防御側は、多くの場合、ランダムな時間（時間的な予測不能）でセンサを組織からの共通の出口に移動（センサの機能的な再配置）し、これをビーコントラップ（汚染）の使用と組み合わせる。その結果、防御側は敵対者が機微情報を漏出させる試みを素早く検知できる。
精査 脅威イベントと脅威イベン	インパクトの可能性を低減する。	• 敵対者は、不確実性、混乱、および疑いの利点を失う。

意図された影響	リスクへのインパクト	期待される結果
トに関連するアーティファクト（特に脆弱性の悪用パターン、素因となる条件、および脆弱性）を分析して、より効果的な検知とリスク対応を通知する。		• 防御側は、敵対者の行為に関連するアーティファクト（悪意のあるコードなど）と影響、および行為に固有の観察結果と他の行為（実行可能な場合）との相関を含む敵対者の行為の分析に基づいて、敵対者をよりよく理解するため、敵対者の TTP を認識することができる。 **例**：防御側はハニーネット（誤認誘導）を展開し、防御側による攻撃を誘い、防御側が安全な環境で TTP を適用できるようにする。防御側は、ハニーネットでキャプチャされたマルウェアを分析（マルウェアおよびフォレンジック分析）して、攻撃者の TTP の性質を判断し、適切な防御を開発できるようにする。
公開 共通、共同、または調整されたリスク対応をサポートするために、利害関係者のコミュニティ全体でリスク要因と改善アプローチの相対的な有効性に関する認識を高める。	特に将来のインパクトの可能性を低減する。	• 敵対者は驚きと否認の可能性という利点を失う。 • ある組織のシステムを侵害して、別の組織を攻撃する敵対者の能力は、利害関係者のコミュニティ全体（例えば、同じ行為者または行為者たちによる攻撃が予想される特定のセクターをサポートするすべてのコンピュータセキュリティインシデント対応チーム全体）での敵対者の特性と行動に対する認識が高まるにつれて損なわれる。 **例**：防御側は脅威情報の共有に参加し、動的に更新される脅威インテリジェンスデータフィード（動的脅威モデル）を使用して行動（順応的管理）を通知する。