NIST Special Publication 800-172

Enhanced Security Requirements for Protecting Controlled Unclassified Information

管理対象非機密情報を保護するために強化されたセキュリティ要件

A Supplement to NIST Special Publication 800-171

NIST SP 800-171 への補足

とりあえず、機械翻訳ベースの仮訳バージョン（V 0.2）
By EvaAviation (Kuno) 2021.2.20

ロン ・ロス
ビクトリア ・ピリテリ
ゲイリー・ ギサニー
ライアン・ ワーグナー
リチャード ・グラウバート
デ ブ・ボドー

This Publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-172

February 2021

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

National Institute of Standards and Technology
James K. Olthoff, Acting NIST Director and Acting Under Secretary of Commerce for Standards and Technology

Authority
典拠

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA), 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of the appropriate federal officials exercising policy authority over such systems. This guideline is consistent with requirements of the Office of Management and Budget (OMB) Circular A-130.

この出版物は、米国連邦情報セキュリティ近代化法(FISMA)、44 米国の下での法的責任をさらに高めるために NIST によって開発されました. 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283 NIST は、連邦情報システムの最低要件を含む情報セキュリティ基準およびガイドラインの策定を担当していますが、そのような基準とガイドラインは、そのようなシステムに対する政策権限を行使する適切な連邦当局者の明示的な承認なしに、国家安全保障システムには適用されません。このガイドラインは、管理予算局 (OMB)の Circular A-130 の要件と一致しています。

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, OMB Director, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

この出版物では、法定権限の下で商務長官によって連邦政府機関に義務付けされ拘束力を持つ基準とガイドラインと矛盾するものは何も取られるべきではありません。また、これらのガイドラインは、商務長官、OMB ディレクター、またはその他の連邦当局者の既存の当局を変更または置き換えるものとして解釈されるべきではありません。この出版物は、非政府組織が自発的に使用することができ、米国では著作権の対象となりません。しかし、帰属は NIST によって評価されます。

国立標準技術研究所 SP 800-172
ナットル・インスト・スタンドテクノル。スペック。パブ。
800-172,84 ページ(2021 年 2 月)
コードン: NSPUE2
この資料は、以下から無料で入手できます。
https://doi.org/10.6028/NIST.SP.800-172

Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts, practices, and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review draft publications during the public comment periods and provide feedback to NIST. Many NIST publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

本書では、特定の商業用事業体、設備、または材料を特定して、実験手順または概念を適切に記述することができます。このような識別は、NIST による推薦または承認を意味するものではありませんし、また、エンティティ、材料、または機器が必ずしも目的に最適であることを意味するものではありません。

本書には、その割り当てられた法的責任に従って、NIST が現在開発中の他の出版物への言及があるかもしれません。この出版物の情報は、概念、慣行、方法論を含め、そのようなコンパニオン出版物が完成する前であっても連邦政府機関によって使用される可能性があります。したがって、各パブリケーションが完了するまで、現在の要件、ガイドライン、および手順が存在する場合、それらは動作し続けます。計画と移行の目的のために、連邦政府機関は、NIST によるこれらの新しい出版物の開発に密接に従うことを望むかもしれません。

パブリックコメント期間中に文書の草案を確認し、NIST にフィードバックを提供することをお勧めします。上記以外の多くの NIST 出版物は、https://csrc.nist.gov/publications で入手できます。

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: sec-cert@nist.gov
All comments are subject to release under the Freedom of Information Act (FOIA) [FOIA96].
コメントはすべて情報公開法（FOIA）[FOIA96]に基づき公開対象である。

Reports on Computer Systems Technology
コンピュータシステム技術に関する報告

The National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology (IT). ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost effective security of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information systems security and privacy and its collaborative activities with industry, government, and academic organizations.
国立標準技術研究所（NIST）の情報技術研究所（ITL）は、米国の測定法および規格基盤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、および技術分析を開発し、情報技術（IT）の開発と生産的使用を促進している。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指針を策定することが含まれる。SP 800 シリーズは、情報システムのセキュリティおよびプライバシーに関する ITL の研究、指針、および普及活動とともに、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。

Abstract
要約

The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the Federal Government to successfully conduct its essential missions and functions. This publication provides federal agencies with recommended enhanced security requirements for protecting the confidentiality of CUI: (1) when the information is resident in nonfederal systems and organizations; (2) when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and (3) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category listed in the CUI Registry. The enhanced requirements apply to components of nonfederal systems that process, store, or transmit CUI or that provide security protection for such components when the designated CUI is associated with a critical program or high value asset. The enhanced requirements supplement the basic and derived security requirements in NIST Special Publication 800-171 and are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.
非連邦系および組織に存在する管理対象非機密情報(CUI)の保護は、連邦政府機関にとって最も重要であり、連邦政府が本質的な任務と機能を正常に遂行する能力に直接影響を与える可能性があります。この文書は、以下の各場合に CUI の機密性を保護するための推奨される強化されたセキュリティ要件を連邦政府機関に提供します。(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、または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 カテゴリの認可法、規制、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護要件がない場合。拡張された要件は、CUI を処理、保管、または送信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か、または指定された CUI が重要なプログラムまたは高価値資産に関連付けられている場合に、そのようなコンポーネントのセキュリティ保護を提供します。拡張された要件は、NIST SP

800-171 の基本的および派生セキュリティ要件を補完し、契約車両またはそれらの機関と非連邦組織との間で確立された他の契約上の契約機関によって使用することを意図しています。

Keywords
キーワード

Advanced Persistent Threat; Basic Security Requirement; Contractor Systems; Controlled Unclassified Information; CUI Registry; Derived Security Requirement; Enhanced Security Requirement; Executive Order 13556; FIPS Publication 199; FIPS Publication 200; FISMA; NIST Special Publication 800-53; Nonfederal Organizations; Nonfederal Systems; Security Assessment; Security Control; Security Requirement.

高度な永続的脅威;基本的なセキュリティ要件請負業者システム;管理された非機密情報;CUI レジストリ;派生セキュリティ要件。強化されたセキュリティ要件行政命令 13556;FIPS パブリケーション 199;FIPS パブリケーション 200;フィスマ;NIST 特別刊行 800-53;非連邦組織;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制御;セキュリティ要件。

Acknowledgements
謝辞

The authors also wish to recognize the scientists, engineers, and research staff from the NIST Computer Security and the Applied Cybersecurity Divisions for their exceptional contributions in helping to improve the content of the publication. A special note of thanks to Pat O'Reilly, Jim Foti, Jeff Brewer, Chris Enloe, Ned Goren, and the entire NIST web team for their outstanding administrative support. Finally, the authors also gratefully acknowledge the contributions from individuals and organizations in the public and private sectors, nationally and internationally, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication.

著者らはまた、NIST コンピュータセキュリティと応用サイバーセキュリティ部門の科学者、エンジニア、研究スタッフが、出版物の内容を改善するのに非常に貢献していると認識したいと考えています。 パット・オライリー、ジム・フォティ、ジェフ・ブルワー、クリス・エンロー、ネッド・ゴレン、そして NIST ウェブチーム全体に感謝の気持ちを伝えました。最後に、国内外の官民の個人や組織からの貢献を感謝し、その思慮深く建設的なコメントは、この出版物の全体的な品質、徹底性、有用性を向上させた。

Patent Disclosure Notice
特許開示通知

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have

been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

注意:情報技術研究所(ITL)は、本文書のガイダンスまたは要件を遵守するために使用する必要がある特許請求の保有者に、そのような特許請求を ITL に開示するよう要請しました。しかし、特許の保有者は、特許の ITL の呼び出しに応答する義務を負わないし、ITL は、特許が存在する場合、この出版物に適用することができるかを特定するために特許検索を行っていません。
本公報のガイダンスまたは要件を遵守するために使用が必要な特許請求の特定に関する公表日および次の呼び出しの時点で、ITL に対するそのような特許請求は特定されていません。
本書の使用において特許侵害を回避するためにライセンスが必要とされないことを ITL が表明または暗示するものではありません。

本書の使用方法

This publication is a supplement to NIST Special Publication 800-171 [SP 800-171]. It contains recommendations for enhanced security requirements to provide additional protection for Controlled Unclassified Information (CUI) in nonfederal systems and organizations when such information is associated with critical programs or high value assets. The enhanced security requirements are designed to respond to the advanced persistent threat (APT) and supplement the basic and derived security requirements in [SP 800-171]. While the security requirements in [SP 800-171] focus primarily on confidentiality protection, the enhanced security requirements in this publication address confidentiality, integrity, and availability protection. The enhanced security requirements are implemented in addition to the basic and derived requirements since those requirements are not designed to address the APT. The enhanced security requirements apply to those components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components.

本書は、NIST SP 800-171[SP 800-171]の補足資料です。また、重要なプログラムや価値の高い資産に関連付けられている場合、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)に対する追加の保護を提供するためのセキュリティ要件の強化に関する推奨事項が含まれています。強化されたセキュリティ要件は、高度な永続的な脅威 (APT) に対応し、[SP 800-171] の基本的なセキュリティ要件と派生セキュリティ要件を補完するように設計されています。[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ますが、この資料のセキュリティ要件の強化は機密性、整合性、および可用性の保護に重点を置いています。拡張セキュリティ要件は、APT に対応するように設計されていないので、基本要件と派生要件に加えて実装されます。強化されたセキュリティ要件は、CUI を処理、保存、または送信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これらのコンポーネントに適用されます。

There is no expectation that all of the enhanced security requirements will be selected by federal agencies implementing this guidance. The decision to select a particular set of enhanced security requirements will be based on the mission and business needs of federal agencies and guided and informed by ongoing risk assessments. The enhanced security requirements for nonfederal systems processing, storing, or transmitting CUI associated with critical programs or high value assets will be conveyed to nonfederal organizations by federal agencies in a contract, grant, or other agreement. The application of the enhanced security requirements to subcontractors will also be addressed by federal agencies in consultation with nonfederal organizations.

このガイダンスを実施する連邦政府機関によって、強化されたセキュリティ要件がすべて選択されるとは期待されていません。強化されたセキュリティ要件の特定のセットを選択する決定は、連邦政府機関の使命とビジネスのニーズに基づいており、継続的なリスク評価によって導かれ、通知されます。重要なプログラムまたは高価値資産に関連する CUI の処理、保管、または送信に関する、非連邦政府システムのセキュリティ要件の強化は、契約、補助金、またはその他の合意の中で連邦政府機関によって非連邦組織に伝達されます。下請け業者への強化されたセキュリティ要件の適用は、非連邦組織と協議して連邦政府機関によっても対処されます。

強化されたセキュリティ要件の適用性

The enhanced security requirements are only applicable to a nonfederal system or nonfederal organization as mandated by a federal agency in a contract, grant, or other agreement. The requirements apply to the components of nonfederal systems that process, store, or transmit CUI associated with a critical program or a high value asset or that provide protection for such components. The requirements also apply to services, including externally provided services, that process, store, or transmit CUI, or that provide security protections, for the system requiring enhanced protection. The protection of a specific service to include CUI that is processed, stored or transmitted during the provision of that service, is achieved by implementing the enhanced security requirements for the service, or the system or system components responsible for providing that service.

強化されたセキュリティ要件は、契約、交付金、またはその他の合意の連邦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組織にのみ適用されます。要件は、重要なプログラムまたは高価値資産に関連付けられた CUI を処理、保管、または送信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ます。要件は、強化された保護を必要とするシステムの、外部から提供されるサービス、CUI のプロセス、保存、送信、セキュリティ保護を提供するサービスにも適用されます。特定のサービスを含む CUI を含むサービスの保護は、そのサービスの提供中に処理、保存、または送信される、サービス、またはそのサービスを提供するシステムまたはシステムコンポーネントの強化されたセキュリティ要件を実装することによって実現されます。

In addition to protecting CUI from unauthorized disclosure, the enhanced security requirements have been designed to protect the integrity and availability of CUI. This is achieved by promoting penetration-resistant architectures, damage-limiting operations, and designs to help achieve cyber resiliency and survivability.

The term organizational system is used in many of the enhanced security requirements. It has a specific meaning regarding the applicability of the enhanced requirements as described above. Appropriate scoping considerations for the requirements are important factors in determining protection-related investment decisions and managing security risk for nonfederal organizations that have the responsibility of protecting CUI associated with critical programs and high value assets.

CUI を不正な開示から保護するだけでなく、強化されたセキュリティ要件は CUI の完全性と可用性を保護するように設計されています。これは、侵入に強いアーキテクチャ、損傷を制限する操作、およびサイバーの回復力と生存性を達成するための設計を促進することによって達成されます。

組織システムという用語は、多くの強化されたセキュリティ要件で使用されます。上記のように強化された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プの考慮事項は、保護関連の投資決定を決定し、重要なプログラムと高価値資産に関連する CUI を保護する責任を負う非連邦組織のセキュリティリスクを管理する上で重要な要素です。

FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

重要なインフラサイバーセキュリティを改善するための枠組み

Organizations that have implemented or plan to implement the NIST Framework for Improving Critical Infrastructure Cybersecurity [NIST CSF] can find in Appendix C a mapping of the enhanced security requirements in this publication to the security controls in [SP 800-53]. The security control mappings can be useful to organizations that wish to demonstrate compliance to the security requirements in the context of their established information security programs when such programs have been built using the NIST security controls.

重要なインフラストラクチャサイバーセキュリティを改善するための NIST フレームワークを実装または実装する予定の組織は、付録 C で、この出版物の強化されたセキュリティ要件と[SP 800-53]のセキュリティ制御へのマッピングを見つけることができます。セキュリティ制御マッピングは、NIST セキュリティ制御を使用してプログラムを構築した場合に、確立された情報セキュリティプログラムのコンテキストで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す。

目次

CHAPTER ONE 第 1 章
INTRODUCTION はじめに

管理対象非機密情報を保護する必要性

Today, more than at any time in history, the Federal Government relies on external service providers to help carry out a wide range of federal missions and business functions using information systems.1 Many federal contractors, for example, routinely process, store, and transmit sensitive federal information in their systems to support the delivery of essential products and services to federal agencies (e.g., financial services, providing web and electronic mail services, processing security clearances or healthcare data, providing cloud services, and developing communications, satellite, and weapons systems). Federal information is frequently provided to or shared with entities such as state and local governments, colleges and universities, and independent research organizations. The protection of sensitive federal information while residing in nonfederal systems2 and organizations is of paramount importance to federal agencies and can directly impact the ability of the Federal Government to carry out its designated missions and business operations.

連邦政府は、歴史上のどの時点よりも、情報システムを使用して幅広い連邦ミッションとビジネス機能を実行するのを支援するために、外部サービスプロバイダーに依存しています。たとえば、多くの連邦請負業者は、重要な製品やサービスを連邦政府機関に提供するために、システム内の機密性の高い連邦情報を日常的に処理、保管、送信します(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ヘルスケアデータの処理、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)。連邦政府の情報は、州政府や地方自治体、大学、独立した研究機関など、多くの場合、提供または共有されます。非連邦政府システム 2 および組織に存在している間の機密性の高い連邦情報の保護は、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任務と事業運営を遂行する能力に直接影響を与える可能性があります。

The protection of unclassified federal information in nonfederal systems and organizations is dependent on the Federal Government providing a process for identifying the different types of information that are used by federal agencies. [EO 13556] established a government-wide Controlled Unclassified Information (CUI)3 Program4 to standardize the way that the executive branch handles unclassified information that requires protection.5 Only information that requires safeguarding or dissemination controls pursuant to federal law, regulation, or government-wide policy may be designated as CUI. The CUI Program is designed to address several deficiencies in managing and protecting unclassified information, including inconsistent markings, inadequate safeguarding, and needless restrictions, both by standardizing procedures and by providing common definitions through a CUI Registry [NARA CUI].

非連邦政府システムおよび組織における非機密の連邦情報の保護は、連邦政府機関が使用するさまざまな種類の情報を特定するプロセスを提供する連邦政府に依存しています。[EO 13556] 政府全体の管理対象非機密情報(CUI)3 プログラムを設立し、執行部が保護を必要とする非機密の情報を取り扱う方法を標準化した。連邦法、規制、政府全体の政策に基づく保護または普及管理を必要とする情報のみが CUI に指定できます。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、不整合なマーキング、不十分な保護、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ます。バシーの要件は、適用、法律、行政命令、指令、規制、ポリシー、基準、および処理、保存、または送信される情報の機密性、完全性、可用性を確保し、個人のプライバシーに対するリスクを管理するためのミッションニーズから導き出されます。

The CUI Registry is the online repository of information, guidance, policy, and requirements on handling CUI, including issuances by the National Archives and Records Administration (NARA) CUI Executive Agent. The CUI Registry identifies approved CUI categories, provides general descriptions for each, identifies the basis for controls, and sets out procedures for the use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, reusing, and disposing of the information.

CUI レジストリは、国立公文書記録管理(NARA)CUI エグゼクティブエージェントによる発行を含む、CUI の取り扱いに関する情報、ガイダンス、方針、および要件のオンラインリポジトリです。CUI レジストリは、承認された CUI カテゴリを識別し、それぞれに一般的な説明を提供し、コントロールの基礎を特定し、情報のマーキング、保護、輸送、配布、再利用、および廃棄などの CUI の使用手順を設定します。

[EO 13556] also required that the CUI Program emphasize openness, transparency, and uniformity of government-wide practices, and that the implementation of the program take place in a manner consistent with applicable policies established by the Office of Management and Budget (OMB) and federal standards and guidelines issued by the National Institute of Standards and Technology (NIST). The federal CUI regulation,6 developed by the CUI Executive Agent, provides guidance to federal agencies on the designation, safeguarding, dissemination, marking, decontrolling, and disposition of CUI; establishes self-inspection and oversight requirements; and delineates other facets of the program.

[EO 13556]また、CUI プログラムは、政府全体の慣行の開放性、透明性、均一性を重視し、管理予算局(OMB)および国立標準技術研究所(NIST)が発行した連邦基準とガイドラインによって確立された適用可能な政策と一致する方法で実施することを要求した。CUI 執行機関が開発した連邦 CUI 規制(6)は、CUI の指定、保護、普及、マーキング、制御解除、および処分に関するガイダンスを連邦政府機関に提供します。自己検査および監督要件を確立する。プログラムの他のファセットを示します。

In certain situations, CUI may be associated with a critical program7 or a high value asset.8 These critical programs and high value assets are potential targets for the advanced persistent threat (APT). An APT is an adversary or adversarial group that possesses the expertise and resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors, including cyber, physical, and deception. The APT objectives include establishing a foothold within the infrastructure of targeted organizations for purposes of exfiltrating information; undermining or impeding critical aspects of a mission, function, program, or organization; or positioning itself to carry out these objectives in the future. The APT pursues its objectives repeatedly over an extended period, adapts to defenders' efforts to resist it, and is determined to maintain the level of interaction needed to execute its objectives. While the category of CUI itself does not require greater protection, CUI associated with critical programs or high value assets is at greater risk because the APT is more likely to target such information and therefore requires additional protection.

特定の状況では、CUI は重要なプログラムまたは高価値資産に関連付けられることがあります。これらの重要なプログラムと価値の高い資産は、高度な永続的な脅威(APT)の潜在的なターゲットです。APT は、サイバー、物理的、詐欺など、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持つ敵対者または敵対者グループです。APT の目標には、情報を浸透させる目的で対象となる組織のインフラストラクチャ内に足がかりを設けるというものがあります。ミッション、機能、プログラム、または組織の重要な側面を損なう、または妨げる。または将来的にこれらの目的を実行するために自分自身を位置づけます。APT は、長期間にわたって目的を繰り返し追求し、それに抵抗するディフェンダーの努力に適応し、その目的を実行するために必要なインタラクションのレベルを維持することを決意しています。CUI 自体のカテゴリは、大きな保護を必要としませんが、重要なプログラムや価値の高い資産に関連付けられている CUI は、APT がこのような情報を対象とする可能性が高く、したがって、追加の保護を必要とする、より大きなリスクがあります。

Controlled Unclassified Information has the same value, whether such information is resident in a federal system that belongs to a federal agency or a nonfederal system that belongs to a nonfederal organization. Accordingly, the enhanced security requirements in this publication are consistent with and complementary to the guidelines used by federal agencies to protect CUI. The requirements are only applicable to a nonfederal system or nonfederal organization as mandated by a federal agency in a contract, grant, or other agreement.

管理対象非機密情報は、そのような情報が連邦機関に属する連邦政府システムまたは非連邦組織に属する非連邦政府システムに存在しているかどうか、*同じ値*を有する。したがって、この文書の強化された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、補完的です。この要件は、契約、交付、またはその他の契約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組織にのみ*適用されます*。

The APT is extremely dangerous to the national and economic security interests of the United States since organizations are very dependent on systems of all types, including traditional Information Technology (IT) systems, Operational Technology (OT) systems, Internet of Things

APT は、従来の情報技術(IT)システム、オペレーショナルテクノロジー(OT)システム、モノのインターネットを含むすべてのタイプのシステムに非常に依存しているため、米国の国家および経済安全保障上の利益にとって非常に危険です。

(IoT) systems, and Industrial IoT (IIoT) systems. The convergence of these types of systems has brought forth a new class of systems known as cyber-physical systems, many of which are in sectors of U.S. critical infrastructure, including energy, transportation, defense, manufacturing, healthcare, finance, and information and communications. Therefore, CUI that is processed, stored, or transmitted by any of the above systems related to a critical program or high value asset requires additional protection from the APT.

(IoT)と産業 IoT(IIoT)システムを使用します。このような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、ヘルスケア、金融、情報通信などの米国の重要インフラの分野にあります。したがって、重要な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、または送信される CUI は、APT からの追加の保護を必要とします。

1.1 PURPOSE AND APPLICABILITY 目的と適用性

The purpose of this publication is to provide federal agencies with a set of enhanced security requirements9 for protecting the confidentiality, integrity, and availability of CUI: (1) when the CUI is resident in a nonfederal system and organization, (2) when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency,10 and (3) where there are no specific safeguarding requirements for protecting the CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category listed in the CUI Registry.11 The enhanced security requirements address the protection of CUI by promoting: (1) penetration-resistant architecture, (2) damage-limiting operations, and (3) designs to achieve cyber resiliency and survivability.12 The enhanced security requirements are intended to supplement the basic and derived security requirements in [SP 800-171] and are for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

この文書の目的は、CUI の機密性、完全性、可用性を保護するための強化されたセキュリティ要件を連邦政府機関に提供することです: (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)非連邦組織が連邦機関に代わって情報を収集または維持していない場合、または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、10 および(3)CUI レジストリに記載されている CUI カテゴリの認可法、規制、または政府全体のポリシーによって規定されている CUI を保護するための特定の保護要件がない場合。11 強化されたセキュリティ要件は、(1)侵入耐性アーキテクチャ、(2)損傷制限操作、サイバーの回復力と生存性を達成するための設計の促進によって CUI の保護に対処します。 12 強化されたセキュリティ要件は、[SP 800-171]の基本的なセキュリティ要件と派生セキュリティ要件を補完することを目的としており、これらの機関と非連邦組織との間で確立された契約車両またはその他の協定で連邦政府機関が使用するためのものです。

The enhanced security requirements apply to components13 of nonfederal systems that process, store, or transmit CUI associated with a critical program or a high value asset or that provide security protection for such components. If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI associated with a critical program or a high value asset, those organizations may limit the scope of the enhanced security requirements by isolating the designated system components in a separate CUI security domain.

セキュリティ要件の強化は、重要なプログラムまたは高価値資産に関連付けられた CUI を処理、保存、または送信する非連邦政府システムのコンポーネント 13 に適用されるか、そのようなコンポーネントのセキュリティ保護を提供します。非連邦組織が、重要なプログラムまたは高価値資産に関連付けられた CUI の処理、保管、または伝送に対して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、強化されたセキュリティ要件の範囲を制限できます。

Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. This approach can provide adequate protection for the CUI and avoid increasing the organization's security posture to a level beyond that which it requires for protecting its missions, operations, and assets.

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達成できます (たとえば、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)。セキュリティドメインは、物理的な分離、論理的分離、またはその両方の組み合わせを使用できます。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体制を、その任務、運用、資産の保護に必要なレベル以上にまで増やすことを避けることができます。

This publication does not provide guidance on which organizational programs or assets are determined to be critical or of high value. Those determinations are made by the organizations mandating the use of the enhanced security requirements for additional protection and can be informed and guided by laws, executive orders, directives, regulations, or policies. Additionally, this publication does not provide guidance on specific types of threats or attack scenarios that justify the use of the enhanced security requirements. Finally, there is no expectation that all of the enhanced security requirements will be needed in every situation. Rather, the selection decisions will be made by organizations based on mission and business needs and risk.

この資料では、どの組織のプログラムまたは資産が重要または価値が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ません。これらの決定は、追加の保護のための強化された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、執行命令、指令、規制、またはポリシーによって通知され、導かれます。また、この資料では、特定の種類の脅威や、強化されたセキュリティ要件の使用を正当化する攻撃シナリオに関するガイダンスも提供していません。最後に、すべての状況で強化されたセキュリティ要件が必要になることは期待していません。むしろ、選択の決定は、ミッションとビジネスのニーズとリスクに基づいて組織に

よって行われます。

1.2 TARGET AUDIENCE ターゲットオーディエンス

This publication serves individuals and organizations in the public and private sectors with:

- System development life cycle responsibilities (e.g., program managers, mission or business owners, information owners or stewards, system designers and developers, system and security engineers, systems integrators);
- System, security, or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, chief information security officers, system owners, information security managers);
- Security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, independent verifiers or validators, analysts); and
- Acquisition or procurement responsibilities (e.g., contracting officers).

この出版物は、公共および民間部門の個人や組織に以下のサービスを提供します。

- システム開発のライフ サイクル の責任（例: プログラムマネージャ、 ミッション またはビジネス オーナー、情報所有者 またはスチュワード、 システム 設計者 および 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ー）
- システム、セキュリティ、またはリスク管理および監督責任（例:職員、最高情報責任者、最高情報セキュリティ責任者、システム所有者、情報セキュリティマネージャーの認可）
- セキュリティ 評価 および 監視 責任（監査人、 システム 評価者、 査定人、 独立した検証者または検証者、アナリストなど）および
- 取得または調達の責任（契約担当者など）

The above roles and responsibilities can be viewed from two distinct perspectives: the federal perspective, as the entity establishing and conveying the security requirements in contractual vehicles or other types of inter-organizational agreements, and the nonfederal perspective, as the entity responding to and complying with the security requirements set forth in contracts or agreements.

上記の役割と責任は、契約車両またはその他の組織間契約におけるセキュリティ要件を確立して伝達するエンティティとして、および契約または契約に定めるセキュリティ要件に対応し、遵守するエンティティとして、連邦政府の視点と非連邦の視点の 2 つの異なる視点から見ることができます。

1.3 ORGANIZATION OF THIS SPECIAL PUBLICATION 本特別刊行物の構成

The remainder of this special publication is organized as follows:

- Chapter Two describes the basic assumptions used to develop the enhanced security requirements for protecting CUI, the organization and structure of the requirements, and the flexibility in applying the requirements.
- Chapter Three describes the 14 families of enhanced security requirements for protecting CUI in nonfederal systems and organizations.
- Supporting appendices provide additional information related to the protection of CUI.

この特別な資料の残りの部分は、次のように編成されています。

- 第 2 章では、CUI を保護するための強化されたセキュリティ要件の開発に使用される基本的な前提、要件の編成と構造、および要件の適用における柔軟性について説明します。
- 第 3 章では、非連邦政府システムおよび組織における CUI を保護するための強化された

セキュリティ要件の 14 ファミリーについて説明します。

- 付属の付録をサポートすると、CUI の保護に関連する追加情報が提供されます。

These include the References, Glossary, Acronyms, and Mapping Tables relating the enhanced security requirements to the security controls in [SP 800-53] and whether the requirements promote penetration-resistant architecture, damage-limiting operations, and designing for cyber resiliency and survivability.

これらには、 [SP 800-53] のセキュリティ制御に対するセキュリティ要件の強化に関連する参照、用語集、略語、およびマッピング表、およびその要件が侵入耐性アーキテクチャ、損傷制限操作、およびサイバー復元性と存続性の設計を促進するかどうかが含まれます。

CHAPTER TWO 第 2 章
THE FUNDAMENTALS 基礎
強化されたセキュリティ要件を開発するための前提

This chapter describes the approach used to develop the enhanced security requirements to protect CUI in nonfederal systems and organizations. It also covers the organization and structure of the enhanced security requirements and provides links to the security control mapping tables in Appendix C.

この章では、非連邦政府システムや組織の CUI を保護するための強化されたセキュリティ要件を開発するために使用されるアプローチについて説明します。また、強化されたセキュリティ要件の編成と構造についても説明し、付録 C のセキュリティ制御マッピングテーブルへのリンクを提供します。

2.1 開発・アプローチ
The enhanced security requirements described in this publication have been developed based on four fundamental assumptions:

- Statutory and regulatory requirements for the protection of CUI are consistent, whether such information resides in federal or nonfederal systems and organizations.
- Safeguards implemented to protect CUI are consistent in federal and nonfederal systems and organizations.
- The impact value for CUI is no less than [FIPS 199] moderate.14
- Additional protections are necessary to protect CUI associated with critical programs or high value assets.15

この資料で説明する強化されたセキュリティ要件は、次の 4 つの基本的な前提に基づいて開発されています。

- CUI の保護に関する法的および規制上の要件は、連邦または非連邦のシステムおよび組織に存在するかどうかに関わらず一貫しています。
- CUI を保護するために実施されるセーフガードは、連邦および非連邦のシステムおよび組織において一貫しています。
- CUI の影響値は [FIPS 199] 中程度以上です。14
- 重要なプログラムや高価値資産に関連する CUI を保護するために、追加の保護が必要です。15

The assumptions reinforce the concept that CUI has the same value and potential adverse impact if compromised, whether such information is located in a federal or a nonfederal organization. Additional assumptions that also impact the development of the enhanced security requirements and the expectation of federal agencies in working with nonfederal organizations include:

この仮定は、CUI が連邦組織または非連邦組織に存在するかどうかにかかわらず、侵害された場合と同じ価値と潜在的な悪影響を及ぼすという概念を強化します。 強化されたセキュリティ要件の開発に影響を与える追加の仮定と、連邦政府機関が非連邦組織と協力する際の期待も次のとおりです。

- Nonfederal organizations have specific safeguarding measures in place to protect their information, which may also be sufficient to satisfy the enhanced security requirements.
- Nonfederal organizations can implement a variety of security solutions directly or using external service providers (e.g., managed services) to satisfy the enhanced security requirements.
- Nonfederal organizations may not have the necessary organizational structure or resources to

satisfy a particular enhanced security requirement and may implement alternative but equally effective security measures to satisfy the intent of the requirement.

- Federal agencies define, in appropriate contracts or other agreements, the organization-defined parameters for applicable enhanced security requirements.
- 非連邦政府機関は、情報を保護するための特定の保護措置を講じているため、強化されたセキュリティ要件を満たすのに十分な場合もあります。
- 非連邦政府機関は、さまざま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ー（マネージドサービスなど）を使用して、強化されたセキュリティ要件を満たすことができます。
- 非連邦政府機関は、特定の強化されたセキュリティ要件を満たすために必要な組織構造やリソースを持っていない可能性があり、要件の意図を満たすために代替的で同様に効果的なセキュリティ対策を実施する可能性があります。
- 連邦政府機関は、適切な契約または他の契約において、組織定義のパラメータを、適用可能な強化されたセキュリティ要件に定義します。

The enhanced security requirements provide the foundation for a multidimensional, defense-in-depth protection strategy that includes three mutually supportive and reinforcing components:

強化されたセキュリティ要件は、相互に支持され、強化されるコンポーネントを含む多次元の多層防御保護戦略の基盤を提供します。

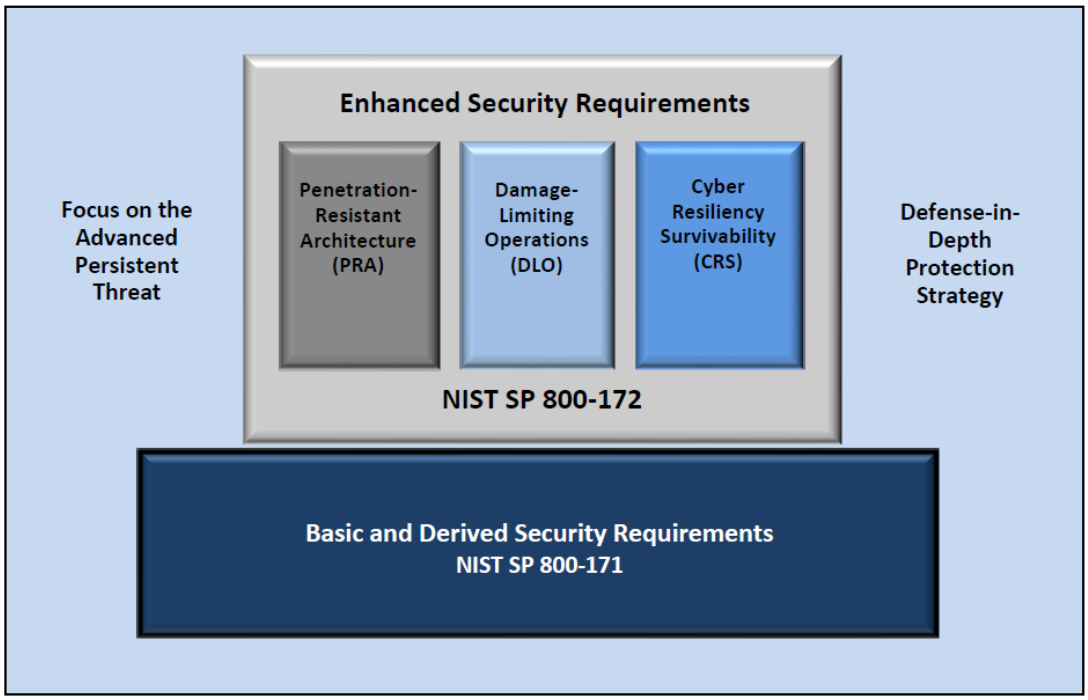

FIGURE 1: MULTIDIMENSIONAL (DEFENSE-IN-DEPTH) PROTECTION STRATEGY

(1) penetration-resistant architecture, (2) damage-limiting operations, and (3) designing for cyber resiliency and survivability [SP 800-160-2]. This strategy recognizes that despite the best protection measures implemented by organizations, the APT may find ways to compromise or breach boundary defenses and deploy malicious code within a defender's system. When this situation occurs, organizations must have access to safeguards and countermeasures to detect, outmaneuver, confuse, deceive, mislead, and impede the adversary—that is, removing the adversary's tactical advantage and protecting the organization's critical programs and high value assets. Figure 1 shows the complementary nature of the enhanced security requirements when implemented as part of a

multidimensional asset protection strategy.

(1)侵入抵抗性アーキテクチャ、(2)損傷制限操作、および(3)サイバーの回復性と生存性のための設計 [SP 800-160-2]。この戦略は、組織が実施する最善の保護対策にもかかわらず、APT が防御を侵害または侵害し、防御者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可能性があることを認識しています。このような状況が発生した場合、組織は、敵対者を検出、打ち負かす、混乱、欺き、誤解を招き、妨害する、つまり不利益な戦術的優位性を取り除き、組織の重要なプログラムと価値の高い資産を保護するためのセーフガードと対策にアクセスできる必要があります。図 1 は、多次元資産保護戦略の一部として実装された場合の、強化されたセキュリティ要件の相補的な性質を示しています。

While the enhanced security requirements can be implemented comprehensively, organizations may—as part of their overarching risk management strategy—select a subset of the security requirements. However, there are dependencies among certain requirements which will affect the selection process. The enhanced security requirements are intended for use by federal agencies in the contractual vehicles or other agreements established between those agencies and nonfederal organizations. Specific implementation guidance for the selected requirements can be provided by federal agencies to nonfederal organizations in such contractual vehicles or agreements.

強化されたセキュリティ要件を包括的に実装できますが、組織は包括的なリスク管理戦略の一環として、セキュリティ要件のサブセットを選択できます。ただし、選択プロセスに影響を与える特定の要件間の依存関係があります。強化されたセキュリティ要件は、契約車両またはそれらの機関と非連邦組織との間で確立された他の契約で連邦政府機関によって使用することを目的としています。選択した要件に関する具体的な実装ガイダンスは、連邦政府機関が、このような契約車両または契約で非連邦政府機関に提供することができます。

The enhanced security requirements are derived from the security controls in [SP 800-53]. The requirements represent methods for protecting information (and CUI, in particular) against cyber-attacks from advanced cyber threats and for ensuring the cyber resiliency of systems and organizations while under attack. The enhanced security requirements focus on the following key elements, which are essential to addressing the APT:

強化された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ます。この要件は、高度なサイバー脅威からサイバー攻撃から情報(特に CUI)を保護し、攻撃を受けている間にシステムや組織のサイバー復元性を確保するための方法を表しています。強化されたセキュリティ要件は、APT に対処するために不可欠な次の重要な要素に焦点を当てています。

- Applying a threat-centric approach to security requirements specification;
- Employing system and security architectures that support logical and physical isolation using system and network segmentation techniques, virtual machines, and containers;16
- Implementing dual authorization controls for the most critical or sensitive operations;
- Limiting persistent storage to isolated enclaves or domains;
- Implementing a comply-to-connect approach for systems and networks;
- Extending configuration management requirements by establishing authoritative sources for addressing changes to systems and system components;
- Periodically refreshing or upgrading organizational systems and system components to a known state or developing new systems or components;
- Employing a security operations center with advanced analytics to support continuous monitoring and protection of organizational systems; and
- Using deception to confuse and mislead adversaries regarding the information they use for

decision-making, the value and authenticity of the information they attempt to exfiltrate, or the environment in which they are operating.

- 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。
- 最も重要な操作または機密性の高い操作に対して二重承認制御を実装する。
- 分離されたエンクレーブまたはドメインへの永続的なストレージの制限
- システムとネットワークに対する接続への準拠アプローチの実装
- システムおよびシステムコンポーネント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。
- 組織システムおよびシステムコンポーネントを定期的に更新またはアップグレードして、既知の状態にしたり、新しいシステムまたはコンポーネントを開発したりすること。
- 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、組織システムの継続的な監視と保護をサポートする。および
- 詐欺を使用して、意思決定に使用する情報、漏えいしようとする情報の価値と信頼性、または彼らが操作している環境に関して、敵対者を混乱させ、誤解を与える。

2.2 ORGANIZATION AND STRUCTURE 統制の構造と組織

The enhanced security requirements are organized into 14 families consistent with the families for basic and derived requirements. Each family contains the requirements related to the general security topic of the family. The families are closely aligned with the minimum security requirements for federal information and information systems in [FIPS 200]. The security requirements for contingency planning, system and services acquisition, and planning are not included within the scope of this publication due to the tailoring criteria in [SP 800-171]. Table 1 lists the security requirement families addressed in this publication.17

強化されたセキュリティ要件は、基本要件と派生要件に合わせて一致する 14 のファミリーに編成されます。各ファミリーには、ファミリーの一般的なセキュリティ トピックに関連する要件が含まれています。ファミリーは[FIPS 200]の連邦情報および情報システムの最低限のセキュリティ要件と密接に一致しています。コンティンジェンシー計画、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]の調整基準のため、この資料の範囲内には含まれません。表ファミリーの資料で扱うセキュリティ要件ファミリーを示します。

ファミリー	
アクセス制御	メディア 保護
意識 と トレーニング	人事 セキュリティ
監査 と 説明責任	物理的 な保護
構成 管理	リスク アセスメント
識別 と 認証	セキュリティ アセスメント
インシデント 対応	システム と 通信 の保護
メンテナンス	システム と 情報 の整合性

TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

表 1：セキュリティおよびプライバシー制御ファミリー

The structure of an enhanced security requirement is similar to the basic and derived security requirements in [SP 800-171]. For some requirements, additional flexibility is provided by allowing organizations to define specific values for the designated parameters. Flexibility is achieved using assignment and selection operations embedded within certain requirements. The assignment and selection operations provide the capability to customize the enhanced security requirements based on organizational protection needs. Determination of organization-defined parameter values can be guided and informed by laws, executive orders, directives, regulations, policies, standards, guidance, or mission or business needs. Risk assessments and risk tolerance are also important factors in defining the values for requirement parameters. Once specified, the values for the assignment and selection operations become part of the requirement.18

強化された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似ています。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定義できるようにすることで、さらに柔軟性が提供されます。柔軟性は、特定の要件に組み込まれた割り当ておよび選択操作を使用して実現されます。割り当ておよび選択操作は、組織の保護のニーズに基づいて、強化されたセキュリティ要件をカスタマイズする機能を提供します。組織定義のパラメータ値の決定は、法律、執行命令、指令、規制、ポリシー、基準、ガイダンス、またはミッションまたはビジネスニーズによって導かれ、情報を得ることができます。リスク評価とリスク許容度も、要件パラメータの値を定義する上で重要な要素です。指定すると、割当および選択操作の値が要件の一部になります。

Following each enhanced security requirement, a discussion section provides additional information to facilitate the implementation of the requirement. This information is primarily derived from the security controls discussion sections in [SP 800-53] and is provided to give organizations a better understanding of the mechanisms and procedures that can be used to implement the controls used to protect CUI. The discussion section is informational only. It is not intended to extend the scope of the enhanced security requirements. The discussion section lso includes informative references.

各拡張セキュリティ要件に従って、要件の実装を容易にするための追加情報を説明するセクションが示されています。この情報は、主に[SP 800-53] のセキュリティ制御の説明のセクションから導き出され、CUI を保護するために使用されるコントロールの実装に使用できるメカニズムと手順について組織に理解を与えるために提供されます。考察は情報提供のみであり、強化されたセキュリティ要件の範囲を拡張するためのものではありません。考察には、有益な参考文献が含まれています。

Finally, a protection strategy and adversary effects section describe the potential effects of implementing the enhanced security requirements on risk, specifically by reducing the likelihood of the occurrence of threat events, the ability of threat events to cause harm, and the extent of that harm. Five high-level, desired effects on the adversary can be identified: redirect, preclude, impede, limit, and expose. Each adversary effect is further decomposed to include specific impacts on risk and expected results. These adversary effects are described in [SP 800-160-2] and in Appendix D.

最後に、保護戦略と敵対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、脅威イベントが害を引き起こす可能性、およびその害の程度を減らすことによって、セキュリティ要件の強化を実装することの潜在的な影響について説明します。敵対者に対する 5 つの高レベルの望ましい影響を特定することができます:リダイレクト、妨害、妨害、制限、および暴露。各不利益な効果はさらに分解され、リスクに対する具体的な影響と予想される結果が含まれます。これらの敵対の影響については、[SP 800-160-2]および付録 D に記載されています。

ASSIGNMENT AND SELECTION OPERATIONS
割り当ておよび選択操作

The parameter values for assignment and selection operations in designated enhanced security requirements are determined by the cognizant federal agency. However, the parameter values should be coordinated with the nonfederal organization. This reflects situations in which the parameter values are dependent on specific characteristics, attributes, or conditions within the nonfederal organization or system (e.g., system architecture, design, or implementation).
指定された強化されたセキュリティ要件における割り当ておよび選択操作のパラメータ値は、認識連邦機関によって決定されます。ただし、パラメータ値は非連邦組織と調整する必要があります。これは、パラメータ値が、非連邦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)に依存している状況を反映しています。

Similar to the basic and derived requirements, the enhanced security requirements are mapped to the security controls in [SP 800-53], the source from which the requirements were derived. The mappings, which can be found in tables C-1 through C-14, are provided for informational purposes only, noting that the related controls do not provide additional requirements.19

基本要件と派生要件と同様に、強化されたセキュリティ要件は、要件の派生元である [SP 800-53] のセキュリティ管理策にマッピングされます。テーブル C-1 から 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、関連するコントロールには追加の要件は提供されないことに注意してください。

18 The requirements, including specific parameter values, are expressed by a federal agency in a contract, grant, or other agreement. The parameter values should be coordinated with nonfederal organizations to address potential system architecture, design, or implementation issues.: 特定のパラメータ値を含む要件は、契約、交付金、またはその他の契約で連邦政府機関によって表されます。パラメータ値は、潜在的なシステム アーキテクチャ、設計、または実装の問題に対処するために、非連邦組織と調整する必要があります。

19 The security controls in Tables C-1 through C-14 are taken from [SP 800-53]. 表 C-1 から C-14 までのセキュリティ管理策は [SP 800-53] から取得されます。

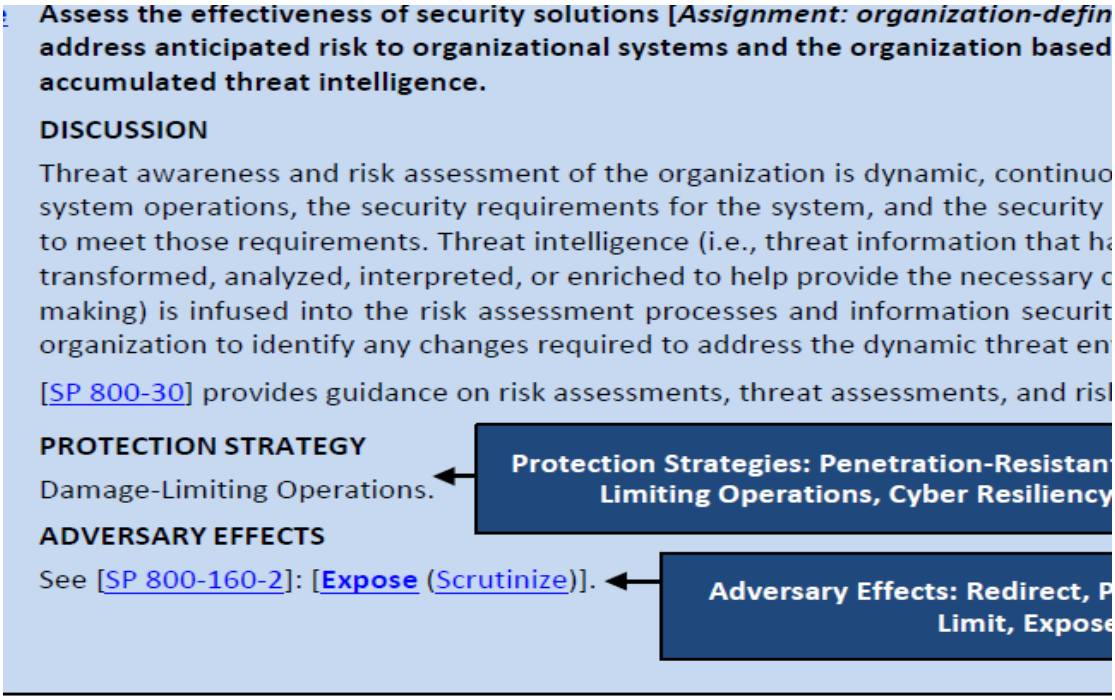

FIGURE 2: ENHANCED SECURITY REQUIREMENT EXAMPLE

2.3 FLEXIBLE APPLICATION 柔軟なアプリケーション

The enhanced security requirements are applied, as necessary, to protect CUI associated with a critical program or a high value asset. Federal agencies may limit application as long as the needed protection is achieved, such as by applying the enhanced security requirements to the components of nonfederal systems that process, store, or transmit CUI associated with a critical program or high value asset; provide protection for such components; or provide a direct attack path to such components (e.g., due to established trust relationships between system components).20

必要に応じて、セキュリティ要件の強化が適用され、重要なプログラムまたは高価値資産に関連付けられた CUI を保護します。連邦政府機関は、重要なプログラムまたは高価値資産に関連する CUI を処理、保存、または送信する非連邦政府システムのコンポーネントに対して強化されたセキュリティ要件を適用するなど、必要な保護が達成される限り、アプリケーションを制限することができます。このようなコンポーネントの保護を提供する。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)。

There is no expectation that all of the enhanced security requirements will be selected by every federal agency. The decision to select enhanced security requirements will be based on the specific mission and business protection needs of the agency, group of agencies, or the federal government (i.e., federal entity) and will be guided and informed by ongoing assessments of risk. The selection of enhanced security requirements for a nonfederal system processing, storing, or transmitting CUI associated with a critical program or a high value asset will be conveyed to the nonfederal organization by the federal entity in a contract, grant, or other agreement. The application of the enhanced security requirements to subcontractors will also be addressed by the federal entity in consultation with the nonfederal organization.

強化されたセキュリティ要件のすべてがすべての連邦機関によって選択されるとは期待されていません。強化されたセキュリティ要件を選択する決定は、機関、機関のグループ、または連邦政府(すなわち、連邦機関)の特定の使命とビジネス保護のニーズに基づいており、継続的なリスク評価によって導かれ、通知されます。重要なプログラムまたは高価値資産に関連する非連邦政府システムの処理、保存、または CUI の送信に関する強化されたセキュリティ要件の選択は、契約、補助金、またはその他の契約で連邦機関によって非連邦組織に伝達されます。

下請け業者への強化されたセキュリティ要件の適用は、非連邦組織と協議して連邦機関によっても対処されます。

---

20 System components include mainframes, workstations, servers, input and output devices, network components, operating systems, virtual machines, applications, cyber-physical components (e.g., programmable logic controllers [PLC] or medical devices), and mobile devices (e.g., smartphones and tablets). 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)や医療機器など)、モバイルデバイス(スマートフォンやタブレットなど)が含まれます。

Certain enhanced security requirements may be too difficult or cost prohibitive for organizations to meet internally. In these situations, the use of external service providers21 can be leveraged to satisfy the requirements. The services include but are not limited to:

強化されたセキュリティ要件の一部は、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場合があります。このような場合、外部サービス プロバイダーの使用を利用して要件を満たすことができます。サービスには以下が含まれますが、これらに限定されません。

- Threat intelligence22
- Threat and adversary hunting
- System monitoring and security management23
- IT infrastructure, platform, and software services
- Threat, vulnerability, and risk assessments
- Response and recovery24
- Cyber resiliency25
- インテリジェンス 22
- 脅威と敵対狩り
- システム監視とセキュリティ管理 23
- IT インフラストラクチャ、プラットフォーム、ソフトウェアサービス
- 脅威、脆弱性、リスク評価
- 応答と回復 24
- サイバー復元力 25

Finally, specific implementation guidance associated with the enhanced security requirements is beyond the scope of this publication. Organizations have maximum flexibility in the methods, techniques, technologies, and approaches used to satisfy the enhanced security requirements.26

最後に、強化された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、このドキュメントの範囲外です。組織は、強化されたセキュリティ要件を満たすために使用される方法、技術、技術、およびアプローチに最大限の柔軟性を持っています。

IMPLEMENTATION TIPS FOR FEDERAL AGENCIES
連邦政府機関向けの実装に関するヒント

1. Select the set of enhanced security requirements needed to protect CUI in the nonfederal system or organization.
2. Complete the assignment and selection operations (where applicable) in the set of enhanced security requirements selected by the agency.
3. Develop implementation guidance for nonfederal organizations if desired or needed.
4. Include the enhanced security requirements and implementation guidance in federal contracts or other agreements with nonfederal organizations.

1. 非連邦システムまたは組織の CUI を保護するために必要な強化されたセキュリティ要件のセットを選択します。
2. 機関によって選択された強化されたセキュリティ要件のセットで、割り当ておよび選択操作 (該当する場合) を完了します。
3. 必要に応じて、非連邦組織の実装ガイダンスを作成します。
4. 連邦契約または非連邦組織との他の協定に、強化されたセキュリティ要件と実装ガイダンスを含める。

---

21 These services can be provided by a parent or supervisory organization (e.g., a prime contractor providing services to a subcontractor) or a third party (e.g., a cloud service provider). これらのサービスは、親または監督組織(例えば、下請け業者にサービスを提供する主要な請負業者)または第三者(例えば、クラウドサービスプロバイダー)によって提供することができる。

22[SP 800-150] makes a distinction between threat information and threat intelligence. Threat information is any information related to a threat that might help an organization protect itself against that threat or detect the activities of a threat actor. Threat intelligence is threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for risk-based decision-making processes. [SP 800-150] は、脅威情報と脅威インテリジェンスを区別します。脅威情報とは、脅威から組織を保護したり、脅威アクターの活動を検出したりするのに役立つ脅威に関連する情報です。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、または強化された脅威情報です。

23 A managed security services provider (MSSP) can provide an off-site security operations center (SOC) in which analysts monitor security-relevant data flows on behalf of multiple customers or subordinate organizations. The best services go beyond monitoring perimeter defenses and additionally monitor system components, devices, and endpoint data from deep within organizational systems and networks 管理セキュリティ サービス プロバイダー (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 セキュリティ オペレーション センター (SOC) を提供できます。最適なサービスは、境界防御を監視するだけでなく、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 データを監視します。

24 In some cases, MSSP organizations provide integrated security-related management and incident response services, similar to a managed detection and response (MDR) services provider. Alternatively, response and recovery services may be obtained separately. 場合によっては、MSSP 組織は、管理された検出および応答 (MDR) サービス プロバイダーと同様に、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します。あるいは、応答および回復サービスは別々に得られてもよい。

25[SP 800-160-2] provides guidance on cyber resilient systems. [SP 800-160-2]は、サイバーレジリエントシステムに関するガイダンスを提供します。

26 Such guidance can be included in the contractual vehicles or other agreements established between federal agencies and nonfederal organizations. このようなガイダンスは、連邦機関と非連邦組織との間で確立された契約車両またはその他の協定に含めることができます。

CHAPTER THREE 第 3 章 要件

ENHANCED SECURITY REQUIREMENTS FOR THE ADVANCED PERSISTENT THREAT
高度な永続的脅威に対する強化されたセキュリティ要件

This chapter describes enhanced security requirements to protect the confidentiality, integrity, and availability of CUI in nonfederal systems and organizations from the APT.27

The enhanced security requirements are not required for any particular category or article of CUI. However, if a federal agency determines that CUI is associated with a critical program or a high value asset,28 the information and the system processing, storing, or transmitting such information are potential targets for the APT and, therefore, may require enhanced protection.

Such protection, expressed through the enhanced security requirements, is mandated by a federal agency in a contract, grant, or other agreement. The enhanced security requirements are implemented in addition to the basic and derived requirements contained in [SP 800-171] since the basic and derived requirements are not designed to address the APT.29

この章では、APT.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強化されたセキュリティ要件について説明します。

CUI の特定のカテゴリまたはアーティクルに対して、セキュリティ要件の強化は必要ありません。しかし、連邦政府機関が CUI が重要な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 の情報とシステムの処理、保存、または送信は APT の潜在的なターゲットであり、したがって、強化された保護が必要になる可能性があります。

強化されたセキュリティ要件を通じて表明されたこのような保護は、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。基本要件と派生要件は APT.29 に対応するように設計されていないので、[SP 800-171] に含まれる基本要件と派生要件に加えて、セキュリティ要件の強化が実装されています。

Associated with each enhanced security requirement is an identification of which of the three protection strategy areas (i.e., penetration-resistant architecture, damage-limiting operations, and designing for cyber resiliency and survivability) the requirement supports and what potential effects the requirement has on an adversary. This information is included to assist organizations in ascertaining whether the requirement is appropriate. Ideally, the requirements selected should be balanced across the three strategy areas. Selecting requirements that fall exclusively in one area could result in an unbalanced response strategy for dealing with the APT.

Similarly, with regard to potential effects on adversaries, organizations should attempt to have as broad a set of effects on an adversary as possible, given their specific mission or business objectives.

各強化されたセキュリティ要件に関連付けられているのは、3 つの保護戦略領域 (侵入耐性アーキテクチャ、損傷制限操作、サイバー復元性と生存性の設計) のうち、どの領域をサポートしているか、および要件が敵に与える潜在的な影響を識別することです。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情報です。理想的には、選択した要件は、3 つの戦略領域でバランスを取る必要があります。1 つの領域に排他的に該当する要件を選択すると、APT に対処するためのアンバランス対応戦略が生じる可能性があります。

同様に、潜在的な不利益な影響に関しては、組織は、特定の使命やビジネス目標を考えると、敵対者に対して可能な限り広範な影響を及ぼすようにすべきです。

27 [SP 800-39] defines the APT as an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors, including cyber, physical, and deception. [SP 800-39]は、サイバー、物理的、詐欺を含む複数の攻撃ベクトルを使用して目標を達成する機会を創出することを可能にする高度なレベルの専門知識と重要なリソースを持つ敵対者として APT を定義します。

28 [OMB M-19-03]を参照してください。

29 The enhanced security requirements have been developed to help address the threats described in [NTCTF]. [NTCTF] で説明されている脅威に対処するために、強化されたセキュリティ要件が開発されました。

Enhanced Security Requirements

3.1.1e Employ dual authorization to execute critical or sensitive system and organizational operations.：システムや組織の操作を実行するために二重承認を採用すること。

DISCUSSION 考察

Dual authorization, also known as two-person control, reduces risk related to insider threats. Dual authorization requires the approval of two authorized individuals to execute certain commands, actions, or functions. For example, organizations employ dual authorization to help ensure that changes to selected system components (i.e., hardware, software, and firmware) or information cannot occur unless two qualified individuals approve and implement such changes. These individuals possess the skills and expertise to determine if the proposed changes are correct implementations of the approved changes, and they are also accountable for those changes.

Another example is employing dual authorization for the execution of privileged commands. To reduce the risk of collusion, organizations consider rotating assigned dual authorization duties to reduce the risk of an insider threat. Dual authorization can be implemented via either technical or procedural measures and can be carried out sequentially or in parallel.

二重承認は、2 人の制御とも呼ばれ、インサイダーの脅威に関連するリスクを軽減します。二重承認では、特定のコマンド、アクション、または機能を実行するために、2 人の権限を持つ個人の承認が必要です。たとえば、組織は二重認証を採用して、2 人の資格のある担当者が承認して実装しない限り、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) や情報の変更を行えないようにします。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持っており、それらの変更に対しても責任があります。

別の例として、特権コマンドの実行に二重認証を使用する場合があります。共謀のリスクを軽減するために、組織は、インサイダーの脅威のリスクを減らすために、割り当てられた二重承認義務をローテーションすることを検討します。二重認証は、技術的または手続き的な手段を介して実施することができ、順次または並行して実行することができます。

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture; Damage-Limiting Operations.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Preempt); **Impede** (Exert)].

3.1.2e Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.：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、組織が所有、プロビジョニング、または発行された情報リソースのみに制限すること。

DISCUSSION 考察

Information resources that are not owned, provisioned, or issued by the organization include systems or system components owned by other organizations and personally owned devices. Non-organizational information resources present significant risks to the organization and complicate the ability to employ a “comply-to-connect” policy or implement component or device attestation techniques to ensure the integrity of the organizational system.組織が所有、プロビジョニング、または発行していない情報リソースには、他の組織や個人所有のデバイスが所有するシステムまたはシステム コンポーネントが含まれます。組織以外の情報リソースは、組織に重大

なリスクを与え、組織システムの整合性を確保するために「接続に準拠する」ポリシーを採用したり、コンポーネントまたはデバイスの構成証明技術を実装したりする機能を複雑にします。

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Preempt); **Impede** (Contain, Exert)].

3.1.3e- Employ [*Assignment: organization-defined secure information transfer solutions*] to control information flows between security domains on connected systems. : [割り当て: 組織定義の安全な情報転送ソリューション]に、接続されたシステム上のセキュリティドメイン間の情報フロー制御を採用すること。

DISCUSSION 考察

Organizations employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations within systems and between connected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content. Organizations also consider the trustworthiness of filtering and inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.

組織は、情報フロー制御ポリシーと実施メカニズムを採用して、システム内の指定された送信元と送信先間、および接続されたシステム間の情報の流れを制御します。フロー制御は、情報や情報パスの特性に基づいています。強制は、たとえば、ルール セットを使用する境界保護デバイス、またはシステム サービスを制限する構成設定を確立する、ヘッダー情報に基づくパケット フィルタリング機能を提供する、メッセージの内容に基づくメッセージ フィルタリング機能を提供する境界保護デバイスで発生します。また、組織は、情報フローの実施に不可欠なフィルタリングおよび検査メカニズム(ハードウェア、ファームウェア、ソフトウェアコンポーネントなど)の信頼性も考慮しています。

Transferring information between systems in different security domains with different security policies introduces the risk that the transfers violate one or more domain security policies. In such situations, information owners or information stewards provide guidance at designated policy enforcement points between connected systems. Organizations mandate specific architectural solutions when required to enforce logical or physical separation between systems in different security domains. Enforcement includes prohibiting information transfers between connected systems, employing hardware mechanisms to enforce one-way information flows, verifying write permissions before accepting information from another security domain or connected system, and implementing trustworthy regrading mechanisms to reassign security attributes and labels.

異なるセキュリティ ポリシーを使用して、異なるセキュリティ ドメイン内のシステム間で情報を転送すると、転送を 1 つ以上のドメイン セキュリティ ポリシーに違反するリスクが生じます。このような状況では、情報所有者または情報スチュワードは、接続されたシステム間の指定されたポリシー施行ポイントでガイダンスを提供します。組織では、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に、特定のアーキテクチャ ソリューションを義務付けています。強制には、接続システム

間の情報転送の禁止、ハードウェア メカニズムによる一方向の情報フローの強制、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の情報を受け入れる前の書き込みアクセス許可の検証、およびセキュリティ属性とラベルを再割り当てするための信頼できる再採点メカニズムの実装が含まれます。

Secure information transfer solutions often include one or more of the following properties: use of cross-domain solutions when traversing security domains, mutual authentication of the sender and recipient (using hardware-based cryptography), encryption of data in transit and at rest, isolation from other domains, and logging of information transfers (e.g., title of file, file size, cryptographic hash of file, sender, recipient, transfer time and Internet Protocol [IP] address, receipt time, and IP address).

セキュリティ情報転送ソリューションには、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 ソリューションの使用、送信者と受信者の相互認証 (ハードウェア ベースの暗号化を使用)、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、情報転送の記録 (ファイルのタイトル、ファイル サイズ、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、転送時間、および IP アドレスの 1 つ以上が含まれます) が含まれます。受信時刻、および IP アドレス)。

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Preempt); **Impede** (Contain, Exert)].

3.2 AWARENESS AND TRAINING 意識とトレーニング

Enhanced Security Requirements

3.2.1e- Provide awareness training [*Assignment: organization-defined frequency*] focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training [*Assignment: organization-defined frequency*] or when there are significant changes to the threat.：ソーシャル エンジニアリング、高度な永続的な脅威アクター、侵害、および不審な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 [割り当て: 組織定義の頻度] を提供すること。;トレーニングの更新 [割り当て: 組織定義の頻度]、または脅威に重大な変更がある場合。

DISCUSSION 考察

An effective method to detect APT activities and reduce the effectiveness of those activities is to provide specific awareness training for individuals. A well-trained and security-aware workforce provides another organizational safeguard that can be employed as part of a defense-in-depth strategy to protect organizations against malicious code injections via email or web applications. Threat awareness training includes educating individuals on the various ways that APTs can infiltrate organizations, including through websites, emails, advertisement pop-ups, articles, and social engineering. Training can include techniques for recognizing suspicious emails, the use of removable systems in non-secure settings, and the potential targeting of individuals by adversaries outside the workplace. Awareness training is assessed and updated periodically to ensure that the training is relevant and effective, particularly with respect to the threat since it is constantly, and often rapidly, evolving.

APT 活動を検出し、その活動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トレーニングを提供することです。十分な訓練を受けたセキュリティに対応した従業員は、多層防御戦略の一部として使用できる別の組織的な保護手段を提供し、電子メールや Web アプリケーションを介して悪意のあるコードインジェクションから組織を保護します。

脅威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、AT が組織に侵入するさまざまな方法に関する個人の教育が含まれます。トレーニングには、疑わしい電子メールを認識する手法、安全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のターゲット設定の可能性などがあります。意識トレーニングは定期的に評価され、更新され、特に脅威が絶えず急速に進化しているため、トレーニングが関連性と効果的であることを確認します。

[SP 800-50] provides guidance on security awareness and training programs.

[SP 800-50]セキュリティの認識とトレーニングプログラムに関するガイダンスを提供します。

PROTECTION STRATEGY 保護戦略

Damage-Limiting Operations.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Impede** (Exert); **Expose** (Detect)].

3.2.2e Include practical exercises in awareness training for [*Assignment: organization-defined roles*] that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.：現在の脅威シナリオに沿った[割り当て: 組織定義の役割]啓発トレーニングに実践的な演習を含め、トレーニングに関与する個人とその上司にフィードバックを提供すること。

DISCUSSION 考察

Awareness training is most effective when it is complemented by practical exercises tailored to the tactics, techniques, and procedures (TTP) of the threat. Examples of practical exercises include unannounced social engineering attempts to gain unauthorized access, collect information, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links. Rapid feedback is essential to reinforce desired user behavior. Training results, especially failures of personnel in critical roles, can be indicative of a potentially serious problem. It is important that senior management are made aware of such situations so that they can take appropriate remediating actions.

意識トレーニングは、脅威の戦術、テクニック、手順(TTP)に合わせた実践的な演習によって補完される場合に最も効果的です。実際の演習の例としては、未発表のソーシャルエンジニアリングの試みにより、不正なアクセスを取得したり、情報を収集したり、スピアフィッシング攻撃、悪意のある Web リンクを介して悪意のある電子メールの添付ファイルを開いたり、呼び出しを行ったりする悪影響をシミュレートする試みが含まれます。迅速なフィードバックは、必要なユーザーの行動を強化するために不可欠です。トレーニング結果、特に重要な役割を担う人員の障害は、潜在的に深刻な問題を示している可能性があります。適切な改善措置を講じるためには、上級管理職に対してそのような状況を認識させることが重要です。

SP800-181]レキシコンや分類など、ロール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ます。
仕事の役割を通じたサイバーセキュリティ作業を記述します。

PROTECTION STRATEGY 保護戦略

Damage-Limiting Operations.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Impede** (Exert); **Expose** (Detect)].

3.3 AUDIT AND ACCOUNTABILITY

Enhanced Security Requirements

There are no enhanced security requirements for audit and accountability.

3.4 CONFIGURATION MANAGEMENT

Enhanced Security Requirements

3.4.1e Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.：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とアカウンタビリティを提供するために、信頼できるソースとリポジトリを確立および維持すること。

DISCUSSION 考察

The establishment and maintenance of an authoritative source and repository includes a system component inventory of approved hardware, software, and firmware; approved system baseline configurations and configuration changes; and verified system software and firmware, as well as images and/or scripts. The authoritative source implements integrity controls to log changes or attempts to change software, configurations, or data in the repository. Additionally, changes to the repository are subject to change management procedures and require authentication of the user requesting the change. In certain situations, organizations may also require dual authorization for such changes. Software changes are routinely checked for integrity and authenticity to ensure that the changes are legitimate when updating the repository and when refreshing a system from the known, trusted source. The information in the repository is used to demonstrate adherence to or identify deviation from the established configuration baselines and to restore system components from a trusted source. From an automated assessment perspective, the system description provided by the authoritative source is referred to as the desired state. The desired state is compared to the actual state to check for compliance or deviations. [SP 800-128] provides guidance on security configuration management, including security configuration settings and configuration change control.

権限のあるソースとリポジトリの確立と保守には、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 インベントリが含まれます。承認されたシステムベースライン構成および構成変更。検証されたシステムソフトウェアとファームウェア、画像やスクリプト。権限のあるソースは、リポジトリ内のソフトウェア、構成、またはデータの変更や変更をログに記録するための整合性制御を実装します。さらに、リポジトリへの変更は変更管理手順の対象となり、変更を要求するユーザーの認証が必要です。状況によっては、このような変更に対して、組織で二重の承認が必要になる場合もあります。ソフトウェアの変更は、リポジトリを更新するとき、および既知の信頼できるソースからシステムを更新する際に、変更が正当であることを確認するために、整合性と信頼性について定期的にチェックされます。リポジトリ内の情報は、確立された構成基準への準拠を示したり、確立された構成基準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ます。自動評価の観点からは、権限のあるソースによって提供されるシステム記述は、目的の状態と呼ばれます。希望の状態は、実際の状態と比較され、コンプライアンスまたは偏差をチェックします。[SP 800-128] では、セキュリティ構成の設定や構成変更制御など、セキュリティ構成管理に関するガイダンスを提供します。

[IR 8011-1] provides guidance on automation support to assess system and system component configurations.

[IR 8011-1] では、システムおよびシステム コンポーネントの構成を評価するための自動化

サポートに関するガイダンスを提供します。

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture; Designing for Cyber Resiliency and Survivability.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Impede** (Exert); **Limit** (Shorten); **Expose** (Detect)].

3.4.2e- Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, [*Selection (one or more): remove the components; place the components in a quarantine or remediation network*] to facilitate patching, re-configuration, or other mitigations.：自動メカニズムを使用して、構成ミスや無許可のシステムコンポーネントを検出すること。検出後、[選択(1つ以上): コンポーネントを削除し、コンポーネントを検疫または修復ネットワークに配置して、パッチ適用、再構成、またはその他の緩和策を実施すること。

DISCUSSION 考察

System components used to process, store, transmit, or protect CUI are monitored and checked against the authoritative source (i.e., hardware and software inventory and associated baseline configurations). From an automated assessment perspective, the system description provided by the authoritative source is referred to as the desired state. Using automated tools, the desired state is compared to the actual state to check for compliance or deviations. Security responses to system components that are unknown or that deviate from approved configurations can include removing the components; halting system functions or processing; placing the system components in a quarantine or remediation network that facilitates patching, re-configuration, or other mitigations; or issuing alerts and/or notifications to personnel when there is an unauthorized modification of an organization-defined configuration item. Responses can be automated, manual, or procedural. Components that are removed from the system are rebuilt from the trusted configuration baseline established by the authoritative source.

CUI の処理、保存、送信、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、関連ベースライン設定など) に対して監視およびチェックされます。自動評価の観点からは、権限のあるソースによって提供されるシステム記述は、目的の状態と呼ばれます。自動化ツールを使用すると、希望の状態が実際の状態と比較され、コンプライアンスまたは偏差がチェックされます。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応答には、コンポーネントの削除が含まれる場合があります。システム機能または処理の停止。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し、パッチ適用、再構成、またはその他の緩和策を容易にします。組織定義の構成項目が不正に変更された場合に、警告や通知を担当者に発行する。応答は、自動化、手動、または手続きにできます。システムから削除されたコンポーネントは、権限のあるソースによって確立された信頼された構成基準から再構築されます。

[IR 8011-1] provides guidance on using automation support to assess system configurations.

[IR 8011-1]は、オートメーションサポートを使用してシステム構成を評価する方法に関するガイダンスを提供します。

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Expunge, Preempt); **Impede** (Contain); **Expose** (Detect)].

3.4.3e- Employ automated discovery and management tools to maintain an up-to-date, complete,accurate, and readily available inventory of system components.：自動検出および管理ツールを使用して、システムコンポーネントの最新の完全かつ正確なインベントリを維持すること。

DISCUSSION 考察

The system component inventory includes system-specific information required for component accountability and to provide support to identify, control, monitor, and verify configuration items in accordance with the authoritative source. The information necessary for effective accountability of system components includes the system name, hardware and software component owners, hardware inventory specifications, software license information, software version numbers, and—for networked components—the machine names and network addresses. Inventory specifications include the manufacturer, supplier information, component type, date of receipt, cost, model,serial number, and physical location. Organizations also use automated mechanisms to implement and maintain authoritative (i.e., up-to-date, complete, accurate, and available) baseline configurations for systems that include hardware and software inventory tools, configuration management tools, and network management tools. Tools can be used to track version numbers on operating systems, applications, types of software installed, and current patch levels.

システム コンポーネントインベントリには、コンポーネントのアカウンタビリティに必要なシステム固有の情報、および権限のあるソースに従って構成項目を識別、制御、監視、および検証するためのサポートが含まれます。システム コンポーネントの効果的なアカウンタビリティに必要な情報には、システム名、ハードウェアおよびソフトウェア コンポーネントの所有者、ハードウェア インベントリの仕様、ソフトウェア ライセンス情報、ソフトウェア バージョン番号、およびネットワーク コンポーネントのコンピュータ名とネットワーク アドレスが含まれます。在庫の仕様には、製造元、サプライヤー情報、コンポーネントタイプ、入庫日、コスト、モデル、シリアル番号、および物理的な場所が含まれます。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して、信頼性のある (最新の、完全、正確、使用可能な) 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使用します。ツールを使用して、オペレーティング システム、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種類、および現在のパッチレベルのバージョン番号を追跡できます。

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Expose** (Detect)].

3.5 IDENTIFICATION AND AUTHENTICATION

Enhanced Security Requirements

3.5.1e-Identify and authenticate [*Assignment: organization-defined systems and system components*] before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant.：暗号ベースで再生に抵抗力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、[割り当て: 組織定義システムとシステム コンポーネント] を識別および認証すること。

DISCUSSION 考察

Cryptographically-based and replay-resistant authentication between systems, components, and

devices addresses the risk of unauthorized access from spoofing (i.e., claiming a false identity). The requirement applies to client-server authentication, server-server authentication, and device authentication (including mobile devices). The cryptographic key for authentication transactions is stored in suitably secure storage available to the authenticator application (e.g., keychain storage, Trusted Platform Module [TPM], Trusted Execution Environment [TEE], or secure element).

暗号ベースのシステム、コンポーネント、およびデバイス間の認証は、なりすましによる不正アクセス(つまり、偽のアイデンティティを主張する)のリスクに対処します。要件は、クライアント/サーバー認証、サーバーサーバー認証、およびデバイス認証 (モバイル デバイスを含む) に適用されます。認証トランザクションの暗号化キーは、認証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に格納されます (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]、トラステッド実行環境 [TEE]、またはセキュアな要素)。

Mandating authentication requirements at every connection point may not be practical, and therefore, such requirements may only be applied periodically or at the initial point of network connection.

[SP 800-63-3] provides guidance on identity and authenticator management.

すべての接続ポイントでの認証要件の義務付けは実用的では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できます。

[SP 800-63-3]では、ID および認証システムの管理に関するガイダンスを提供しています。

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Negate); **Expose** (Detect)].

3.5.2e- Employ automated mechanisms for the generation, protection, rotation, and management of passwords for systems and system components that do not support multifactor authentication or complex account management.：多要素認証や複雑なアカウント管理をサポートしないシステムおよびシステムコンポーネントのパスワードの生成、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こと。

DISCUSSION 考察

In situations where static passwords or personal identification numbers (PIN) are used (e.g., certain system components do not support multifactor authentication or complex account management, such as separate system accounts for each user and logging), automated mechanisms (e.g., password managers) can automatically generate, rotate, manage, and store strong and different passwords for users and device accounts. For example, a router might have one administrator account, but an organization typically has multiple network administrators. Therefore, access management and accountability are problematic. A password manager uses techniques such as automated password rotation (in this example, for the router password) to allow a specific user to temporarily gain access to a device by checking out a temporary password and then checking the password back in to end the access. The password manager simultaneously logs these actions. One of the risks in using password managers is that an adversary may target the collection of passwords that the device generates. Therefore, it is important that these passwords are secured. Methods for protecting passwords include the use of multi-factor authentication to the password manager, encryption, or secured

hardware (e.g., a hardware security module).

静的なパスワードや暗証番号 (PIN) が使用されている場合 (たとえば、ユーザーごとに別々のシステム アカウントやログ記録など、多要素認証や複雑なアカウント管理をサポートしていないシステム コンポーネントなど)、自動化されたメカニズム (パスワード マネージャなど) は、ユーザーとデバイス アカウントの強力で異なるパスワードを自動的に生成、回転、管理、および格納できます。たとえば、ルーターには 1 つの管理者アカウントが割り振られますが、組織には通常、複数のネットワーク管理者が存在します。したがって、アクセス管理とアカウンタビリティは問題になります。パスワード マネージャは、自動パスワード ローテーション (この例ではルーターパスワード) などの手法を使用して、一時的なパスワードをチェックアウトし、パスワードを再びチェックインしてアクセスを終了することで、特定のユーザーが一時的にデバイスにアクセスできるようにします。パスワード マネージャは、これらのアクションを同時にログに記録します。パスワード マネージャを使用する場合のリスクの 1 つは、敵対者がデバイスによって生成されるパスワードの収集を対象とする可能性があるということです。したがって、これらのパスワードはセキュリティで保護することが重要です。パスワードを保護する方法には、パスワード マネージャ、暗号化、またはセキュリティで保護されたハードウェア (ハードウェア セキュリティ モジュールなど) に対する多要素認証の使用が含まれます。

[SP 800-63-3] provides guidance on password generation and management.

[SP800-63-3]では、パスワードの生成と管理に関するガイダンスを提供します。

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Impede** (Delay, Exert)].

3.5.3e-Employ automated or manual/procedural mechanisms to prohibit system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state, or in a trust profile.：コンポーネントが既知、認証済み、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、システム コンポーネントが組織のシステムに接続することを禁止する自動または手動/手続き型のメカニズムを採用すること。

DISCUSSION 考察

Identification and authentication of system components and component configurations can be determined, for example, via a cryptographic hash of the component. This is also known as device attestation and known operating state or trust profile. A trust profile based on factors such as the user, authentication method, device type, and physical location is used to make dynamic decisions on authorizations to data of varying types. If device attestation is the means of identification and authentication, then it is important that patches and updates to the device are handled via a configuration management process such that the patches and updates are done securely and do not disrupt the identification and authentication of other devices.
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と認証は、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、デバイスの構成証明と既知の動作状態または信頼プロファイルとも呼ばれます。ユーザー、認証方法、デバイスの種類、物理的な場所などの要因に基づく信頼プロファイルを使用して、さまざまな種類のデータに対する承認に対する動的な決定を行います。デバイスの認証が識別と認証の手段である場合、デバイスのパッチと更新は、パッチと更新が安全に行われ、他のデバイスの識別と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す。

[IR 8011-1] provides guidance on using automation support to assess system configurations.
[IR 8011-1]は、オートメーションサポートを使用してシステム構成を評価する方法に関するガイダンスを提供します。

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Preempt); **Expose** (Detect)].

3.6 INCIDENT RESPONSE

Enhanced Security Requirements

3.6.1e- Establish and maintain a security operations center capability that operates [*Assignment:organization-defined time period*]. : 割当て: 組織定義の期間]セキュリティオペレーションセンター機能の運用を確立および維持すること。

DISCUSSION 考察

A security operations center (SOC) is the focal point for security operations and computer network defense for an organization. The purpose of the SOC is to defend and monitor an organization's systems and networks (i.e., cyber infrastructure) on an ongoing basis. The SOC is also responsible for detecting, analyzing, and responding to cybersecurity incidents in a timely manner. The SOC is staffed with skilled technical and operational personnel (e.g., security analysts, incident response personnel, systems security engineers); in some instances operates 24 hours per day, seven days per week; and implements technical, management, and operational controls (e.g., monitoring, scanning, and forensics tools) to monitor, fuse, correlate, analyze, and respond to security-relevant event data from multiple sources. Sources of event data include perimeter defenses, network devices (e.g., gateways, routers, and switches), and endpoint agent data feeds. The SOC provides a holistic situational awareness capability to help organizations determine the security posture of the system and organization. An SOC capability can be obtained in many ways. Larger organizations may implement a dedicated SOC while smaller organizations may employ third-party organizations to provide such a capability.

セキュリティ オペレーション センター (SOC) は、組織のセキュリティ運用とコンピュータ ネットワークの防御の中心です。SOC の目的は、組織のシステムやネットワーク(サイバーインフラストラクチャ)を継続的に守り、監視することです。また、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出、分析、対応する責任もあります。SOC には熟練した技術および運用スタッフ(セキュリティアナリスト、インシデント対応担当者、システムセキュリティエンジニアなど)が配置されています。場合によっては、1 日 24 時間、週 7 日の動作をします。また、複数のソースからのセキュリティ関連のイベント データを監視、ヒューズ、関連付け、分析、および対応するための技術的、管理、運用管理 (監視、スキャン、フォレンジックツールなど) を実装します。イベント データのソースには、境界部の防御、ネットワーク デバイス (ゲートウェイ、ルーター、スイッチなど)、エンドポイント エージェント データ フィードなどがあります。SOC は、全体的な状況認識機能を提供し、組織がシステムと組織のセキュリティ体制を決定するのに役立ちます。SOC 機能は、さまざまな方法で得ることができます。大規模な組織では専用の SOC を実装し、小規模な組織ではサードパーティの組織を使用してこのような機能を提供することができます。

[SP 800-61] provides guidance on incident handling. [SP 800-86] and [SP 800-101] provide guidance on integrating forensic techniques into incident response. [SP 800-150] provides guidance on cyber threat information sharing. [SP 800-184] provides guidance on cybersecurity event recovery.

[SP 800-61] では、インシデント処理に関するガイダンスを提供します。[SP 800-86] および

[SP 800-101] では、フォレンジック技術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ます。[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ます。[SP 800-184] では、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ます。

PROTECTION STRATEGY 保護戦略

Damage-Limiting Operations.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Limit** (Shorten, Reduce); **Expose** (Detect)].

3.6.2e- Establish and maintain a cyber incident response team that can be deployed by the organization within [*Assignment: organization-defined time period*]. : [割り当て: 組織定義期間]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、維持すること。

DISCUSSION 考察

A cyber incident response team (CIRT) is a team of experts that assesses, documents, and responds to cyber incidents so that organizational systems can recover quickly and implement the necessary controls to avoid future incidents. CIRT personnel include, for example, forensic analysts, malicious code analysts, systems security engineers, and real-time operations personnel. The incident handling capability includes performing rapid forensic preservation of evidence and analysis of and response to intrusions. The team members may or may not be full-time but need to be available to respond in the time period required. The size and specialties of the team are based on known and anticipated threats. The team is typically pre-equipped with the software and hardware (e.g., forensic tools) necessary for rapid identification, quarantine, mitigation, and recovery and is familiar with how to preserve evidence and maintain chain of custody for law enforcement or counterintelligence uses. For some organizations, the CIRT can be implemented as a cross- organizational entity or as part of the Security Operations Center (SOC).

サイバー インシデント対応チーム (CIRT) は、サイバー インシデントを評価、文書化、対応する専門家チームで、組織システムが迅速に復旧し、今後のインシデントを回避するために必要な制御を実装できるようにします。CIRT の担当者には、たとえば、フォレンジック アナリスト、悪意のあるコード アナリスト、システム セキュリティ エンジニア、リアルタイム運用担当者などが含まれます。インシデント処理機能には、証拠の迅速なフォレンジック保存と、侵入の分析と対応が含まれます。チーム メンバーはフルタイムの場合とない場合がありますが、必要な期間内に対応できる必要があります。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いています。チームは通常、迅速な識別、検疫、軽減、回復に必要なソフトウェアとハードウェア(法医学ツールなど)を事前に装備しており、証拠を保存し、法執行機関やカウンターインテリジェンスの使用のために親権の連鎖を維持する方法に精通しています。一部の組織では、CIRT は組織間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ます。

[SP 800-61] provides guidance on incident handling. [SP 800-86] and [SP 800-101] provide guidance on integrating forensic techniques into incident response. [SP 800-150] provides guidance on cyber threat information sharing. [SP 800-184] provides guidance on cybersecurity event recovery.

[SP 800-61] では、インシデント処理に関するガイダンスを提供します。[SP 800-86] および [SP 800-101] では、フォレンジック技術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ます。[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ます。[SP 800-184] では、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ます。

PROTECTION STRATEGY 保護戦略

Damage-Limiting Operations.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Expunge); **Impede** (Contain, Exert); **Limit** (Shorten, Reduce); **Expose** (Scrutinize)].

3.7 MAINTENANCE

Enhanced Security Requirements

There are no enhanced security requirements for maintenance.

3.8 MEDIA PROTECTION

Enhanced Security Requirements

There are no enhanced security requirements for media protection.

3.9 PERSONNEL SECURITY

Enhanced Security Requirements

3.9.1e- Conduct [*Assignment: organization-defined enhanced personnel screening*] for individuals and reassess individual positions and access to CUI [*Assignment: organization-defined frequency*].：個人に対して[割り当て:組織定義の強化された人員審査]を実施し、個人のポジションと CUI へのアクセスを再評価する[割り当て:組織定義頻度]こと。

DISCUSSION 考察

Personnel security is the discipline that provides a trusted workforce based on an evaluation or assessment of conduct, integrity, judgment, loyalty, reliability, and stability. The extent of the vetting is commensurate with the level of risk that individuals could bring about by their position and access to CUI. For individuals accessing Federal Government facilities and systems, the Federal Government employs resources, information, and technology in its vetting processes to ensure a trusted workforce. These screening processes may be extended all or in part to persons accessing federal information, including CUI that is resident in nonfederal systems and organizations through contractual vehicles or other agreements established between federal agencies and nonfederal organizations.

Examples of enhanced personnel screening for security purposes include additional background checks. Personnel reassessment activities reflect applicable laws, executive orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.

人事セキュリティは、行動、誠実性、判断力、忠誠心、信頼性、安定性の評価または評価に基づいて、信頼できる労働力を提供する規律です。審査の程度は、個人が CUI への位置と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ています。連邦政府の施設やシステムにアクセスする個人のために、連邦政府は、信頼できる労働力を確保するために、その審査プロセスでリソース、情報、技術を採用しています。これらの審査プロセスは、連邦機関と非連邦機関との間で締結された契約車両またはその他の協定を通じて非連邦政府システムや組織に存在する CUI を含む、連邦情報にアクセスする人物の全部または一部に拡張することができます。

セキュリティを目的とした人員審査の強化例としては、追加の身元調査が含まれます。人事

再評価活動には、適用される法律、執行命令、指令、ポリシー、規制、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定められている具体的な基準が反映されます。

PROTECTION STRATEGY 保護戦略

Damage-Limiting Operations.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Expunge); **Impede** (Exert)].

3.9.2e- Ensure that organizational systems are protected if adverse information develops or is obtained about individuals with access to CUI.：**有害な情報が CUI にアクセスできる個人に関して発生または取得された場合、組織システムが保護されていることを確認すること。**

DISCUSSION 考察

If adverse information develops or is obtained about an individual with access to CUI which calls into question whether the individual should have continued access to systems containing CUI, actions are taken (e.g., preclude or limit further access by the individual, audit actions taken by the individual) to protect the CUI while the adverse information is resolved.

有害な情報が発生するか、または個人が CUI を含むシステムへの継続的なアクセスを持つべきかどうか疑問に問う CUI へのアクセスを持つ個人について取得された場合、有害な情報が解決されている間に CUI を保護するための措置(例えば、個人によるさらなるアクセスを排除または制限する)が取られる。

PROTECTION STRATEGY 保護戦略

Damage-Limiting Operations.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Limit** (Reduce)].

3.10 PHYSICAL PROTECTION

Enhanced Security Requirements

There are no enhanced security requirements for physical protection.

3.11 RISK ASSESSMENT

Enhanced Security Requirements

3.11.1e- Employ [*Assignment: organization-defined sources of threat intelligence*] as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.：**評価の一環として[割り当て: 組織定義の脅威インテリジェンスのソース]を採用し、組織システム、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、脅威の調査、対応および回復活動の開発を説明し、周知すること。**

DISCUSSION 考察

The constant evolution and increased sophistication of adversaries, especially the APT, makes it more likely that adversaries can successfully compromise or breach organizational systems. Accordingly,

threat intelligence can be integrated into each step of the risk management process throughout the system development life cycle. This risk management process includes defining system security requirements, developing system and security architectures, selecting security solutions, monitoring (including threat hunting), and remediation efforts.

敵対者、特に APT の絶え間ない進化と高度化により、敵対者が組織システムを侵害したり侵害したりする可能性が高まります。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、リスク管理プロセスの各ステップに統合できます。このリスク管理プロセスには、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 (脅威の検出を含む)、および修復作業が含まれます。

[SP 800-30] provides guidance on risk assessments. [SP 800-39] provides guidance on the risk management process. [SP 800-160-1] provides guidance on security architectures and systems security engineering. [SP 800-150] provides guidance on cyber threat information sharing.

[SP 800-30] では、リスク評価に関するガイダンスを提供しています。[SP 800-39] では、リスク管理プロセスに関するガイダンスを提供します。[SP 800-160-1]には、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が用意されています。[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ます。

PROTECTION STRATEGY 保護戦略

Damage-Limiting Operations.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Negate); **Impede** (Exert); **Expose** (Detect)].

3.11.2e- Conduct cyber threat hunting activities [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined event]] to search for indicators of compromise in [Assignment: organization-defined systems] and detect, track, and disrupt threats that evade existing controls.：サイバー脅威の狩猟活動を実施 [選択(1 つ以上):[割り当て:組織定義頻度];[割り当て: 組織定義イベント]][割り当て: 組織定義システム]で妥協の指標を検索し、既存の制御を回避する脅威を検出、追跡、および妨害すること。

DISCUSSION 考察

Threat hunting is an active means of defense that contrasts with traditional protection measures, such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandboxes, and Security Information and Event Management (SIEM) technologies and systems. Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. The objective is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses. Indicators of compromise are forensic artifacts from intrusions that are identified on organizational systems at the host or network level and can include unusual network traffic, unusual file changes, and the presence of malicious code.

脅威の検出は、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) のテクノロジとシステムなど、従来の保護対策とは対照的な積極的な防御手段です。サイバー脅威の検出には、組織システム、ネットワーク、インフラストラクチャを積極的に検索し、高度な脅威を探し出します。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、組織の対応の速度と精度を測定可能に改善することです。侵害の指標は、ホストまたはネットワーク レベルで組織システムで識別される侵入によるフォレンジック アーティファクト

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ります。

Threat hunting teams use existing threat intelligence and may create new threat information, which may be shared with peer organizations, Information Sharing and Analysis Organizations (ISAO), Information Sharing and Analysis Centers (ISAC), and relevant government departments and agencies. Threat indicators, signatures, tactics, techniques, procedures, and other indicators of compromise may be available via government and non-government cooperatives, including Forum of Incident Response and Security Teams, United States Computer Emergency Response Team, Defense Industrial Base Cybersecurity Information Sharing Program, and CERT Coordination Center.

脅威の調査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可能性があり、ピア組織、情報共有分析機関 (ISAO)、情報共有分析センター (ISAC)、および関連する政府機関と共有される可能性があります。脅威指標、署名、戦術、テクニック、手順、その他の妥協指標は、インシデント対応およびセキュリティチームのフォーラム、米国コンピュータ緊急対応チーム、防衛産業基地サイバーセキュリティ情報共有プログラム、CERT 調整センターなど、政府および非政府の協同組合を通じて利用可能です。

[SP 800-30] provides guidance on threat and risk assessments, risk analyses, and risk modeling. [SP 800-160-2] provides guidance on systems security engineering and cyber resiliency. [SP 800-150] provides guidance on cyber threat information sharing.

[SP 800-30] では、脅威とリスクの評価、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ます。[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復元に関するガイダンスを提供しています。[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ます。

PROTECTION STRATEGY 保護戦略

Damage-Limiting Operations.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Expunge); **Limit** (Shorten, Reduce); **Expose** (Detect, Scrutinize)].

3.11.3e- Employ advanced automation and analytics capabilities in support of analysts to predict and identify risks to organizations, systems, and system components.：高度な自動化機能と分析機能を使用して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こと。

DISCUSSION 考察

A properly resourced Security Operations Center (SOC) or Computer Incident Response Team (CIRT) may be overwhelmed by the volume of information generated by the proliferation of security tools and appliances unless it employs advanced automation and analytics to analyze the data. Advanced automation and predictive analytics capabilities are typically supported by artificial intelligence concepts and machine learning. Examples include Automated Workflow Operations, Automated Threat Discovery and Response (which includes broad-based collection, context-based analysis, and adaptive response capabilities), and machine-assisted decision tools.

高度な自動化と分析を使用してデータを分析しない限り、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、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ります。高度な自動化機能と予測分析機能は、通常、人工知能の概念と機械学習

によってサポートされます。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応答 (広範なコレクション、コンテキストベースの分析、適応型応答機能を含む)、マシン支援の意思決定ツールなどがあります。

[SP 800-30] provides guidance on risk assessments and risk analyses.

[SP 800-30] では、リスク評価とリスク分析に関するガイダンスを提供しています。

PROTECTION STRATEGY 保護戦略

Damage-Limiting Operations.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: No direct effects.

3.11.4e- Document or reference in the system security plan the security solution selected, the rationale for the security solution, and the risk determination.：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、およびリスク決定をシステムセキュリティ計画に文書化または参照すること。

DISCUSSION 考察

System security plans relate security requirements to a set of security controls and solutions. The plans describe how the controls and solutions meet the security requirements. For the enhanced security requirements selected when the APT is a concern, the security plan provides traceability between threat and risk assessments and the risk-based selection of a security solution, including discussion of relevant analyses of alternatives and rationale for key security-relevant architectural and design decisions. This level of detail is important as the threat changes, requiring reassessment of the risk and the basis for previous security decisions.

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制御とソリューションに関連付けます。計画では、コントロールとソリューションがセキュリティ要件を満たす方法について説明します。APT が懸念される場合に選択されるセキュリティ要件の強化について、セキュリティ計画は、脅威とリスクの評価と、セキュリティ ソリューションのリスクベースの選択の間のトレーサビリティを提供します。このレベルの詳細は、脅威の変化に応じて重要であり、リスクの再評価と以前のセキュリティ上の決定の基礎が必要になります。

When incorporating external service providers into the system security plan, organizations state the type of service provided (e.g., software as a service, platform as a service), the point and type of connections (including ports and protocols), the nature and type of the information flows to and from the service provider, and the security controls implemented by the service provider. For safety critical systems, organizations document situations for which safety is the primary reason for not implementing a security solution (i.e., the solution is appropriate to address the threat but causes a safety concern).

外部サービス プロバイダーをシステム 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種類 (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)、接続のポイントと種類 (ポートとプロトコルを含む)、サービス プロバイダーとの間の情報フローの性質と種類、およびサービス プロバイダーによって実装されるセキュリティ制御を指定します。安全に重要なシステムの場合、セキュリティ ソリューションを実装しない主な理由は安全に関する状況を文書化します (つまり、ソリューションは脅威に対処するのに適切ですが、安全上の懸念が生じます)。

[SP 800-18] provides guidance on the development of system security plans.

[SP 800-18] では、システム セキュリティ計画の開発に関するガイダンスを提供します。

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: No direct effects.

3.11.5e- Assess the effectiveness of security solutions [*Assignment: organization-defined frequency*] to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.：現在および蓄積された脅威インテリジェンスに基づいて、組織システムおよび組織に対する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評価する **[割り当て: 組織定義の頻度]**こと。

DISCUSSION 考察

Threat awareness and risk assessment of the organization are dynamic, continuous, and inform system operations, security requirements for the system, and the security solutions employed to meet those requirements. Threat intelligence (i.e., threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to help provide the necessary context for decision-making) is infused into the risk assessment processes and information security operations of the organization to identify any changes required to address the dynamic threat environment.

組織の脅威認識とリスク評価は、動的で継続的なシステム運用、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るセキュリティ ソリューションを通知します。脅威インテリジェンス (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、強化された脅威情報) は、組織のリスク評価プロセスと情報セキュリティ操作に注がれ、動的な脅威環境に対処するために必要な変更を特定します。

[SP 800-30] provides guidance on risk assessments, threat assessments, and risk analyses.

[SP 800-30] では、リスク評価、脅威評価、およびリスク分析に関するガイダンスを提供します。

PROTECTION STRATEGY 保護戦略

Damage-Limiting Operations.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Expose** (Scrutinize)].

3.11.6e- Assess, respond to, and monitor supply chain risks associated with organizational systems and system components.：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評価、対応、監視すること。

DISCUSSION 考察

Supply chain events include disruption, use of defective components, insertion of counterfeits, theft, malicious development practices, improper delivery practices, and insertion of malicious code. These events can have a significant impact on a system and its information and, therefore, can also adversely impact organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. The supply chain-related events may be unintentional

or malicious and can occur at any point during the system life cycle. An analysis of supply chain risk can help an organization identify systems or components for which additional supply chain risk mitigations are required.

サプライチェーンイベントには、中断、欠陥コンポーネントの使用、偽造品の挿入、盗難、悪意のある開発慣行、不適切な配信方法、悪意のあるコードの挿入などがあります。これらのイベントはシステムとその情報に大きな影響を与える可能性があるため、組織の運営（ミッション、機能、イメージ、評判など)、組織資産、個人、その他の組織、および国家に悪影響を及ぼす可能性があります。サプライチェーン関連のイベントは、意図しないイベントや悪意のあるイベントであり、システムのライフサイクル中の任意の時点で発生する可能性があります。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軽減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ちます。

[SP 800-30] provides guidance on risk assessments, threat assessments, and risk analyses. [SP 800-161] provides guidance on supply chain risk management.

[SP 800-30] では、リスク評価、脅威評価、およびリスク分析に関するガイダンスを提供します。[SP 800-161] では、サプライチェーンのリスク管理に関するガイダンスを提供しています。

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Preempt); **Expose** (Detect)].

3.11.7e- Develop a plan for managing supply chain risks associated with organizational systems and system components; update the plan [*Assignment: organization-defined frequency*].：組織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すること。計画を更新する [割り当て: 組織定義の頻度]こと。

DISCUSSION 考察

The growing dependence on products, systems, and services from external providers, along with the nature of the relationships with those providers, present an increasing level of risk to an organization. Threat actions that may increase risk include the insertion or use of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain. Supply chain risks can be endemic or systemic within a system element or component, a system, an organization, a sector, or the Nation. Managing supply chain risk is a multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with both internal and external stakeholders. Supply chain risk management (SCRM) activities involve identifying and assessing risks, determining appropriate mitigating actions, developing SCRM plans to document selected mitigating actions, and monitoring performance against plans. SCRM plans address requirements for developing trustworthy, secure, and resilient systems and system components, including the application of the security design principles implemented as part of life cycle-based systems security engineering processes.

外部プロバイダーからの製品、システム、サービスへの依存度が高まり、これらのプロバイダーとの関係の性質が高まり、組織に対するリスクのレベルが高まっています。リスクを増大させる可能性のある脅威のアクションには、偽造品の挿入または使用、不正な生産、改ざん、盗難、悪意のあるソフトウェアやハードウェアの挿入、サプライチェーンでの製造および開発の不十分な慣行などがあります。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、セクター、または国家内で固有または全身的である可能性

があります。サプライチェーンリスクの管理は、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事業です。サプライチェーンリスク管理(SCRM)の活動には、リスクの特定と評価、適切な軽減措置の決定、選択した軽減措置を文書化するための SCRM 計画の策定、計画に対するパフォーマンスの監視が含まれます。SCRM 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 プロセスの一部として実装されるセキュリティ設計原則の適用など、信頼性、安全性、および回復性の高い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計画です。

[SP 800-161] provides guidance on supply chain risk management.

[SP 800-161] では、サプライチェーンのリスク管理に関するガイダンスを提供しています。

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Preempt); **Impede** (Exert)].

3.12 SECURITY ASSESSMENT

Enhanced Security Requirements

3.12.1e- Conduct penetration testing [*Assignment: organization-defined frequency*], leveraging automated scanning tools and ad hoc tests using subject matter experts.：ペネトレーションテストを実施し[割り当て:組織定義の頻度]、自動化されたスキャンツールと、主題の専門家を使用したアドホックテストを活用すること。

DISCUSSION 考察

Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Penetration testing goes beyond automated vulnerability scanning. It is conducted by penetration testing agents and teams with particular skills and experience that include technical expertise in network, operating system, and application-level security. Penetration testing can be used to validate vulnerabilities or determine a system's penetration resistance to adversaries within specified constraints. Such constraints include time, resources, and skills. Organizations may also supplement penetration testing with red team exercises. Red teams attempt to duplicate the actions of adversaries in carrying out attacks against organizations and provide an in-depth analysis of security-related weaknesses or deficiencies.

侵入テストは、敵対者が悪用する可能性のある脆弱性を特定するために、システムまたは個々のシステム コンポーネントに対して行われる特殊な種類の評価です。侵入テストは、自動化された脆弱性スキャンを超えています。侵入テストエージェントと、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チームによって実施されます。侵入テストを使用して、脆弱性を検証したり、指定された制約内の敵対者に対するシステムの侵入抵抗を判断したりできます。このような制約には、時間、リソース、およびスキルが含まれます。組織は、赤のチーム演習で侵入テストを補完することもできます。レッドチームは、組織に対する攻撃を実行する不利益な行動を複製し、セキュリティ関連の弱点や欠陥を詳細に分析しようとします。

Organizations can use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted internally or externally on the hardware, software, or firmware components of a system and can exercise both physical and technical controls. A standard method for penetration testing includes pretest analysis based on full knowledge of the system, pretest

identification of potential vulnerabilities based on the pretest analysis, and testing designed to determine the exploitability of vulnerabilities. All parties agree to the specified rules of engagement before the commencement of penetration testing. Organizations correlate the rules of engagement for penetration tests and red teaming exercises (if used) with the tools, techniques, and procedures that they anticipate adversaries may employ. The penetration testing or red team exercises may be organization-based or external to the organization. In either case, it is important that the team possesses the necessary skills and resources to do the job and is objective in its assessment.

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できます。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 コンポーネントで内部または外部で実施でき、物理的および技術的な制御の両方を実行できます。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事前確認、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ます。すべての当事者は、侵入テストの開始前に、指定された契約規則に同意します。組織は、侵入テストと赤のチーミング演習 (使用する場合) のエンゲージメントのルールを、敵対者が使用する可能性があると予想されるツール、テクニック、および手順と関連付けます。ペネトレーション テストまたは赤のチーム演習は、組織ベースまたは組織の外部の場合があります。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ち、その評価において客観的である必要があります。

[SP 800-53A] provides guidance on conducting security assessments.

[SP 800-53A] では、セキュリティ評価の実施に関するガイダンスを提供しています。

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture; Damage-Limiting Operations.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Impede** (Exert); **Expose** (Detect)].

3.13 SYSTEM AND COMMUNICATIONS PROTECTION

Enhanced Security Requirements

3.13.1e- Create diversity in [*Assignment: organization-defined system components*] to reduce the extent of malicious code propagation. : [割り当て: 組織定義システムコンポーネント] で多様性を作り、悪意のあるコードの伝達の程度を減らすこと。

DISCUSSION 考察

Organizations often use homogenous information technology environments to reduce costs and to simplify administration and use. However, a homogenous environment can also facilitate the work of the APT, as it allows for common mode failures and the propagation of malicious code across identical system components (i.e., hardware, software, and firmware). In these environments, adversary tactics, techniques, and procedures (TTP) that work on one instantiation of a system component will work equally well on other identical instantiations of the component regardless of how many times such components are replicated or how far away they may be placed in the architecture. Increasing diversity within organizational systems reduces the impact of potential exploitations or compromises of specific technologies. Such diversity protects against common mode failures, including those failures induced by supply chain attacks. Diversity also reduces the likelihood that the TTP adversaries use to compromise one system component will be effective against other system components, thus increasing the adversary's work factor to successfully complete the planned attacks. A heterogeneous or diverse information technology environment makes the task of propagating malicious code more difficult, as the adversary needs to develop and deploy different TTP for the diverse components.

組織は、多くの場合、同種の情報技術環境を使用して、コストを削減し、管理と使用を簡素化します。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 (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達が可能になるため、APT の作業を容易にすることもできます。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に使用する敵対的な戦術、テクニック、および手順 (TTP) は、コンポーネントが何回複製されるか、またはアーキテクチャ内に配置される距離に関係なく、コンポーネントの他の同一のインスタンス化でも同様に機能します。組織システム内の多様性の増大により、特定の技術の悪用や侵害の影響が軽減されます。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、コモンモードの障害から保護します。また、ダイバーシティは、TTP の敵が 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可能性を他のシステム コンポーネントに対して有効にする可能性を減らし、それによって、計画された攻撃を正常に完了するための敵の作業要素を増加させます。異種または多様な情報技術環境では、悪意のあるコードを伝播する作業が困難になります。

Satisfying this requirement does not mean that organizations need to acquire and manage multiple versions of operating systems, applications, tools, and communication protocols. However, the use of diversity in certain critical, organizationally determined system components can be an effective countermeasure against the APT. In addition, organizations may already be practicing diversity, although not to counter the APT. For example, it is common for organizations to employ diverse anti-virus products at different parts of their infrastructure simply because each vendor may issue updates to new malicious code patterns at different times and frequencies. Similarly, some organizations employ products from one vendor at the server level and products from another vendor at the end-user level. Another example of diversity occurs in products that provide address space layout randomization (ASLR). Such products introduce a form of synthetic diversity by transforming the implementations of common software to produce a variety of instances. Finally, organizations may choose to use multiple virtual private network (VPN) vendors, tunneling one vendor’s VPN within another vendor’s VPN. Smaller organizations may find that achieving diversity in system components is challenging and perhaps not practical. Organizations also consider the vulnerabilities that may be introduced into the system by the employment of diverse system components.

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しません。しかし、特定の重要な、組織的に決定されたシステムコンポーネントにおける多様性の使用は、APT に対する効果的な対策であり得る。さらに、組織はすでに多様性を実践しているかもしれませんが、APT に対抗する必要はありません。たとえば、各ベンダーが異なる時間や頻度で新しい悪意のあるコード パターンの更新プログラムを発行する可能性があるため、組織がインフラストラクチャのさまざまな部分で多様なウイルス対策製品を採用するのが一般的です。同様に、一部の組織では、サーバー レベルで 1 つのベンダーの製品を使用し、エンド ユーザー レベルで別のベンダーの製品を使用します。ダイバーシティの別の例は、アドレス空間レイアウトのランダム化 (ASLR) を提供する製品で発生します。このような製品は、共通のソフトウェアの実装を変革してさまざまなインスタンスを生成することで、合成多様性の形態を導入します。最後に、組織は、複数の仮想プライベート ネットワーク (VPN) ベンダーを使用して、あるベンダーの VPN を別のベンダーの VPN 内でトンネリングすることを選択できます。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、実用的ではない可能性があります。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します。

[SP 800-160-1] provides guidance on security engineering practices and security design concepts.

[SP 800-160-2] provides guidance on developing cyber resilient systems and system components.

[SP 800-161] provides guidance on supply chain risk management.

[SP 800-160-1] では、セキュリティ エンジニアリングの実践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ます。

[SP 800-160-2] は、サイバー復元力のある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ます。

[SP 800-161] では、サプライチェーンのリスク管理に関するガイダンスを提供しています。

PROTECTION STRATEGY 保護戦略

Designing for Cyber Resiliency and Survivability.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Redirect** (Deter); **Preclude** (Preempt); **Impede** (Contain, Degrade, Delay, Exert); **Limit** (Shorten, Reduce)].

3.13.2e- Implement the following changes to organizational systems and system components to introduce a degree of unpredictability into operations: [*Assignment: organization-defined changes and frequency of changes by system and system component*]. : 組織システムおよびシステムコンポーネントに以後の変更を施し、ある程度の予測不能性を運用に導入すること。

DISCUSSION 考察

Cyber-attacks by adversaries are predicated on the assumption of a certain degree of predictability and consistency regarding the attack surface. The attack surface is the set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from the system, system element, or environment. Changes to the attack surface reduce the predictability of the environment, making it difficult for adversaries to plan and carry out attacks, and can cause the adversaries to make miscalculations that can either impact the overall effectiveness of the attacks or increase the observability of the attackers.

敵対者によるサイバー攻撃は、攻撃面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ます。攻撃面とは、システム、システム要素、または攻撃者がシステム、システム要素、または環境に対してデータを入力、影響を及ぼしたり、または抽出を試みることができる環境の境界上のポイントの集合です。攻撃対象の表面を変更すると、環境の予測可能性が低下し、敵対者が攻撃の計画や実行を困難にし、攻撃の全体的な有効性に影響を与えたり、攻撃者の観察可能性を高めたりする可能性のある誤算が発生する可能性があります。

Unpredictability can be achieved by making changes in seemingly random times or circumstances (e.g., by randomly shortening the time when the credentials are valid). Randomness introduces increased levels of uncertainty for adversaries regarding the actions that organizations take to defend their systems against attacks. Such actions may impede the ability of adversaries to correctly target system components that support critical or essential organizational missions or business functions. Uncertainty may also cause adversaries to hesitate before initiating attacks or continuing attacks. Techniques involving randomness include performing certain routine actions at different times of day, employing different information technologies, using different suppliers, and rotating the roles and responsibilities of organizational personnel.

予測不能は、一見ランダムな時間や状況を変更することによって達成できます(例えば、資格情報が有効な時間をランダムに短縮することによって)。ランダム性は、組織が攻撃からシステムを守るために取る行動に関して、敵対者にとって不確実性のレベルを高めます。このような行為は、敵対者が重要なまたは不可欠な組織のミッションやビジネス機能をサポートするシステムコンポーネントを正しくターゲットにする能力を妨げる可能性があります。また、攻撃を開始したり、攻撃を続けたりする前に、敵対者が躊躇する可能性もあります。ランダム性を伴う手法には、特定の日常的なアクションを 1 日の異なる時間帯に実行すること、さまざまな情報技術を採用すること、異なるサプライヤーを使用すること、組織の担当者の役割と責

任をロールする方法などがあります。

PROTECTION STRATEGY 保護戦略

Designing for Cyber Resiliency and Survivability.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Preempt, Negate); **Impede** (Delay, Exert); **Expose** (Detect)].

3.13.3e- Employ [*Assignment: organization-defined technical and procedural means*] to confuse and mislead adversaries.：敵対者を混乱させ誤解させる[割り当て:組織定義の技術的および手続き上の手段]を採用すること。

DISCUSSION 考察

There are many techniques and approaches that can be used to confuse and mislead adversaries, including misdirection, tainting, disinformation, or a combination thereof. Deception is used to confuse and mislead adversaries regarding the information that the adversaries use for decision-making, the value and authenticity of the information that the adversaries attempt to exfiltrate, or the environment in which the adversaries desire or need to operate. Such actions can impede the adversary's ability to conduct meaningful reconnaissance of the targeted organization, delay or degrade an adversary's ability to move laterally through a system or from one system to another system, divert the adversary away from systems or system components containing CUI, and increase observability of the adversary to the defender—revealing the presence of the adversary along with its TTPs. Misdirection can be achieved through deception environments (e.g., deception nets), which provide virtual sandboxes into which malicious code can be diverted and adversary TTP can be safely examined. Tainting involves embedding data or information in an organizational system or system component which the organization desires adversaries to exfiltrate. Tainting allows organizations to determine that information has been exfiltrated or improperly removed from the organization and potentially provides the organization with information regarding the nature of exfiltration or adversary locations. Disinformation can be achieved by making false information intentionally available to adversaries regarding the state of the system or type of organizational defenses. Any disinformation activity is coordinated with the associated federal agency requiring such activity, and should include a plan to limit incidental exposure of the false CUI to authorized users. Disinformation can be employed both tactically (e.g., making available false credentials that the defender can use to track adversary actions) and strategically (e.g., interspersing false CUI with actual CUI, interfering with an adversary's re-use, reverse engineering and exploitation of legitimate CUI, thus undermining the adversary's confidence in the value of the exfiltrated information, and subsequently causing them to limit such exfiltration).

誤った方向、汚染、情報漏えい、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術とアプローチがあります。欺瞞は、敵対者が意思決定に使用する情報、敵対者が流出しようとする情報の価値と真正性、または敵対者が望むまたは操作する必要がある環境に関して、敵対者を混乱させ、誤解を招くために使用されます。このような行動は、敵対者が標的となる組織の有意義な偵察を行う能力を妨げる可能性がある。敵対者がシステムを横方向に移動したり、あるシステムから別のシステムに横方向に移動したり、敵対者を CUI を含むシステムやシステムコンポーネントから遠ざけ、不利益な防御能力を高める能力を遅らせたり劣化させたりします。詐欺ネット)は、悪意のあるコードを流用し、不利益な TTP を安全に検査することができる仮想サンドボックスを提供します。汚染とは、組織が敵対者に浸透させたい組織システムまたはシステムコンポーネントにデータまたは情報を埋め込むことです。汚染により、組織は情報が組織から流出または不適切に削除されたと判断し、流出や不利益な場所の性質に関する情報を組織に提供する可能性があります。誤った情報は、システムの状態や組織の防御の種類に関して、敵対者に意図的に虚偽の

情報を提供することによって達成することができます。いかなる情報漏えい活動も、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、権限のあるユーザーへの偽 CUI の偶発的な暴露を制限する計画を含める必要があります。情報漏えいは、戦術的に(例えば、擁護者が敵対行為を追跡するために使用できる偽の資格情報を利用可能にする)と戦略的に(例えば、実際の CUI と偽の CUI を散在させ、不利益な再利用、リバースエンジニアリング、正当な CUI の搾取を妨害し、その後、その結果を引き起こす不利益な信頼を損なう)の両方で採用することができます。

[SP 800-160-2] provides guidance on developing cyber resilient systems and system components.

[SP 800-160-2] は、サイバー復元力のある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ます。

PROTECTION STRATEGY 保護戦略

Designing for Cyber Resiliency and Survivability.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Redirect** (Deter, Divert, Deceive); **Preclude** (Preempt, Negate); **Impede** (Delay, Exert); **Expose** (Detect)].

3.13.4e- Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components. : [選択: (1 つ以上): [割り当て: 組織定義の物理的分離手法]、[割り当て: 組織定義の論理的分離手法]]を組織システムおよびシステムコンポーネントに採用すること。

DISCUSSION 考察

A mix of physical and logical isolation techniques (described below) implemented as part of the system architecture can limit the unauthorized flow of CUI, reduce the system attack surface, constrain the number of system components that must be secure, and impede the movement of an adversary. When implemented with a set of managed interfaces, physical and logical isolation techniques for organizational systems and components can isolate CUI into separate security domains where additional protections can be implemented. Any communications across the managed interfaces (i.e., across security domains), including for management or administrative purposes, constitutes remote access even if the communications remain within the organization.

システムアーキテクチャの一部として実装される物理的および論理的な分離技術 (後述) の組み合わせにより、CUI の不正なフローを制限し、システム攻撃の表面を減らし、安全にする必要のあるシステム コンポーネントの数を制限し、不利益な移動を妨げる可能性があります。一連の管理インターフェイ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術により、CUI を別々のセキュリティドメインに分離して、追加の保護を実装できます。管理または管理目的を含め、管理インターフェイス (セキュリティドメイン間) を介した通信は、通信が組織内に残っている場合でもリモートアクセスを構成します。

Separating system components with boundary protection mechanisms allows for the increased protection of individual components and more effective control of information flows between those components. This enhanced protection limits the potential harm from and susceptibility to hostile cyber-attacks and errors. The degree of isolation can vary depending on the boundary protection mechanisms selected. Boundary protection mechanisms include routers, gateways, and firewalls separating system components into physically separate networks or subnetworks; virtualization and micro-virtualization techniques; encrypting information flows among system components using

distinct encryption keys; cross-domain devices separating subnetworks; and complete physical separation (i.e., air gaps).

境界保護機構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ます。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害と感受性を制限します。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ります。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ー、ゲートウェイ、およびファイアウォールが含まれます。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 コンポーネント間で情報フローを暗号化する。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)。

System architectures include logical isolation, partial physical and logical isolation, or complete physical isolation between subsystems and at system boundaries between resources that store, process, transmit, or protect CUI and other resources. Examples include:

システムアーキテクチャには、論理分離、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の完全な物理的分離、および CUI とその他のリソースを格納、処理、送信、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ます。例としては、次のようなものがあります。

- Logical isolation: Data tagging, digital rights management (DRM), and data loss prevention (DLP) that tags, monitors, and restricts the flow of CUI; virtual machines or containers that separate CUI and other information on hosts; and virtual local area networks (VLAN) that keep CUI and other information separate on networks.
- 論理的分離: CUI のフローにタグ付け、監視、および制限を加えるデータタグ付け、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。および仮想ローカル エリア ネットワーク (VLAN)により、CUI やその他の情報をネットワーク上で分離します。
- Partial physical and logical isolation: Physically or cryptographically isolated networks, dedicated hardware in data centers, and secure clients that (a) may not directly access resources outside of the domain (i.e., all applications with cross-enclave connectivity execute as remote virtual applications hosted in a demilitarized zone [DMZ] or internal and protected enclave), (b) access via remote virtualized applications or virtual desktop with no file transfer capability other than with dual authorization, or (c) employ dedicated client hardware (e.g., a zero or thin client) or hardware approved for multi-level secure (MLS) usage.
- 部分的な物理的および論理的分離: 物理的または暗号的に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リティクライアント(つまり、クロスエンクレーブ接続を持つすべてのアプリケーションは、非武装地帯[DMZ]または内部および保護されたエンクレーブでホストされているリモート仮想アプリケーションとして実行される)、(b)リモートアクセス、または (c) 専用のクライアント ハードウェア (例えば、ゼロまたはシン クライアント) またはマルチレベル セキュア (MLS) の使用が承認されたハードウェアを使用します。
- Complete physical isolation: Dedicated (not shared) client and server hardware; physically isolated, stand-alone enclaves for clients and servers; and (a) logically separate network traffic (e.g., using a VLAN) with end-to-end encryption using Public Key Infrastructure (PKI)-based cryptography or (b) physical isolation from other networks.
- 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ー ハードウェア。クライアントとサーバー用の、物理的に分離されたスタンドアロンのエンクレーブ。(a) 公開キー基盤 (PKI) ベースの暗号化または (b) 他のネットワークからの物理的な分離を使用したエンドツーエンド暗号化と(VLAN を使用する)ネットワーク トラフィックを論理的に分離します。

Isolation techniques are selected based on a risk management perspective that balances the threat, the information being protected, and the cost of the options for protection. Architectural and design decisions are guided and informed by the security requirements and selected solutions.

Organizations consider the trustworthiness of the isolation techniques employed (e.g., the logical isolation relies on information technology that could be considered a high value target because of the function being performed), introducing its own set of vulnerabilities.

分離手法は、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管理の観点に基づいて選択されます。アーキテクチャと設計の決定は、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、通知されます。

組織は、使用される分離技術の信頼性を考慮し (たとえば、論理的な分離は、実行される機能のために高い価値のターゲットと考えられ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します。

[SP 800-160-1] provides guidance on developing trustworthy, secure, and cyber resilient systems using systems security engineering practices and security design concepts.

[SP 800-160-1] システムセキュリティエンジニアリングの実践とセキュリティ設計コンセプトを使用して、信頼性、安全、およびサイバーに対する回復力のあるシステムの開発に関するガイダンスを提供します。

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture; Designing for Cyber Resiliency and Survivability.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Preempt, Negate); **Impede** (Contain, Degrade, Delay, Exert); **Limit** (Reduce)].

3.13.5e- Distribute and relocate the following system functions or resources [*Assignment: organization-defined frequency*]: [*Assignment: organization-defined system functions or resources*]. : 以後のシステム機能またはリソースを配分および再配置すること [割り当て: 組織定義頻度]: [割り当て: 組織定義システム機能またはリソース]

DISCUSSION 考察

Changing processing and storage locations (also referred to as moving target defense) addresses the APT by using techniques such as virtualization, distributed processing, and replication. This enables organizations to relocate system components that support critical missions and business functions. Changing the locations of processing activities or storage sites introduces a degree of uncertainty into the targeting activities of adversaries. Targeting uncertainty increases the work factor of adversaries making compromises or breaches to organizational systems more difficult and time-consuming. It also increases the chances that adversaries may inadvertently disclose aspects of their tradecraft while attempting to locate organizational resources. Other options for employing moving target defense include changing IP addresses, Domain Name System (DNS) names, or network topologies. Moving target defense can also increase the work factor for defenders who have a constantly changing system to defend. Accordingly, organizations update their management and security tools and train personnel to adapt to the additional work factor.

処理とストレージの場所の変更 (移動対象防御とも呼ばれます) は、仮想化、分散処理、レプリケーションなどの手法を使用して APT に対応します。これにより、重要なミッションやビジネス機能をサポートするシステムコンポーネントを組織が再配置できるようになります。処理活動や保管場所の場所を変更すると、不利益なターゲティング活動に不確実性が生

じます。不確実性をターゲットにすることは、敵対者が組織システムに対する妥協や侵害をより困難で時間のかかるものにする作業要因を増大させます。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、誤ってトレードクラフトの側面を開示する可能性も高まります。移動対象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ります。ターゲットディフェンスを動かすと、絶えず変化するシステムを持つディフェンダーが防御する作業要素を増やすこともできます。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、追加の作業要素に適応するように担当者をトレーニングします。

Another way of addressing this requirement is by fragmentation. This involves taking information and fragmenting/partitioning it across multiple components (e.g., across a distributed database).

Such actions mean that the compromise (unauthorized exfiltration) of any single component of the information data set will not result in the compromise of the entire data. To fully compromise the entire data set, the adversary would have to work harder to try to locate all of the data sets.

この要件に対処するもう 1 つの方法は、断片化です。これには、情報を取り、複数のコンポーネント(分散データベース間など)にわたって情報を断片化/パーティション分割することが含まれます。

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 (無許可の流出) がデータ全体の侵害を引き起こさないことを意味します。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ります。

PROTECTION STRATEGY 保護戦略

Designing for Cyber Resiliency and Survivability.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Preempt, Negate); **Impede** (Delay, Exert); **Expose** (Detect)].

3.14 SYSTEM AND INFORMATION INTEGRITY システムと情報の整合性

Enhanced Security Requirements

3.14.1e- Verify the integrity of [*Assignment: organization-defined security critical or essential software*] using root of trust mechanisms or cryptographic signatures.：信頼メカニズムまたは暗号署名のルートを使用して、[割り当て: 組織定義のセキュリティ クリティカルまたは不可欠なソフトウェア] の整合性を確認すること。

DISCUSSION 考察

Verifying the integrity of the organization's security-critical or essential software is an important capability since corrupted software is the primary attack vector used by adversaries to undermine or disrupt the proper functioning of organizational systems. There are many ways to verify software integrity throughout the system development life cycle. Root of trust mechanisms (e.g., secure boot, trusted platform modules, Unified Extensible Firmware Interface [UEFI]), verify that only trusted code is executed during boot processes. This capability helps system components protect the integrity of boot firmware in organizational systems by verifying the integrity and authenticity of updates to the firmware prior to applying changes to the system component and preventing unauthorized processes from modifying the boot firmware. The employment of cryptographic signatures ensures the integrity and authenticity of critical and essential software that stores, processes, or transmits, CUI. Cryptographic signatures include digital signatures and the computation and application of signed hashes using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information. Hardware roots of trust are considered to be more secure. This requirement supports 3.4.1e and 3.4.3.e.

破損したソフトウェアは、組織システムの適切な機能を損なったり妨害したりするために敵対者が使用する主な攻撃方法であるため、組織のセキュリティクリティカルまたは不可欠なソフトウェアの整合性を検証することは重要な機能です。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整合性を検証する方法は多数あります。信頼メカニズムのルート(例えば、セキュアブート、信頼されたプラットフォームモジュール、統一された拡張ファームウェアインターフェイス(UEFI)))は、信頼されたコードのみがブートプロセス中に実行されることを確認します。この機能は、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整合性と信頼性を確認し、承認されていないプロセスがブート ファームウェアを変更するのを防ぐことで、組織のシステムのブートファームウェアを変更するのを防ぐことで、組織のシステムのブートファームウェアの整合性を保護するのに役立ちます。暗号署名の採用により、CUI を格納、処理、または送信する重要かつ重要なソフトウェアの完全性と信頼性が保証されます。暗号化署名には、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キーの機密性の保護、および公開キーを使用したハッシュ情報の検証が含まれます。信頼のハードウェアルートは、より安全であると考えられます。この要件は、3.4.1e および 3.4.3.e をサポートします。

[FIPS 140-3] provides security requirements for cryptographic modules. [FIPS 180-4] and [FIPS 202] provide secure hash standards. [FIPS 186-4] provides a digital signature standard. [SP 800-147] provides BIOS protection guidance. [NIST TRUST] provides guidance on the roots of trust project.

[FIPS 140-3] は、暗号モジュールのセキュリティ要件を提供します。[FIPS 180-4]および[FIPS 202]は、安全なハッシュ標準を提供します。[FIPS 186-4]はデジタル署名規格を提供します。[SP 800-147]には BIOS 保護ガイダンスが含まれています。[NIST TRUST]は、信頼プロジェクトのルーツに関するガイダンスを提供しています。

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Negate); **Impede** (Exert); **Expose** (Detect)].

3.14.2e- Monitor organizational systems and system components on an ongoing basis for anomalous or suspicious behavior.：組織システムとシステム コンポーネントを継続的に監視し、異常な動作や疑わしい動作を監視すること。

DISCUSSION 考察

Monitoring is used to identify unusual, suspicious, or unauthorized activities or conditions related to organizational systems and system components. Such activities or conditions can include unusual internal systems communications traffic, unauthorized exporting of information, signaling to external systems, large file transfers, long-time persistent connections, attempts to access information from unexpected locations, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.

監視は、組織のシステムやシステム コンポーネントに関連する、不審な、または不正なアクティビティや状態を特定するために使用されます。このようなアクティビティや条件には、異常な内部システム通信トラフィック、情報の不正なエクスポート、外部システムへの通知、大規模なファイル転送、長時間の永続的な接続、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ます。

The correlation of physical, time, or geolocation audit record information to the audit records from

systems may assist organizations in identifying examples of anomalous behavior. For example, the correlation of an individual's identity for logical access to certain systems with the additional information that the individual was not present at the facility when the logical access occurred is indicative of anomalous behavior.

物理的、時間的、または地理位置情報の監査レコード情報とシステムからの監査レコード情報の関連付けは、組織が異常な動作の例を特定するのに役立ちます。たとえば、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施設に存在しなかった追加情報との相関関係は、異常な動作を示します。

[SP 800-61] provides guidance on incident handling. [SP 800-83] provides guidance for malicious code incident prevention and handling. [SP 800-92] provides guidance on computer security log management. [SP 800-94] provides guidance on intrusion detection and prevention. [SP 800-137] provides guidance on continuous monitoring of systems.

[SP 800-61] では、インシデント処理に関するガイダンスを提供します。[SP 800-83] は、悪意のあるコードの問題の防止と処理に関するガイダンスを提供します。[SP 800-92] では、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ます。[SP 800-94] では、侵入検知と防御に関するガイダンスを提供します。[SP 800-137] では、システムの継続的な監視に関するガイダンスを提供します。

PROTECTION STRATEGY 保護戦略

Designing for Cyber Resiliency and Survivability.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Expose** (Detect)].

3.14.3e- Ensure that [*Assignment: organization-defined systems and system components*] are included in the scope of the specified enhanced security requirements or are segregated in purpose-specific networks. : [割り当て: 組織定義システムおよびシステム コンポーネント] が、指定された強化されたセキュリティ要件の範囲に含まれているか、目的固有のネットワークに分離されていることを確認すること。

DISCUSSION 考察

Organizations may have a variety of systems and system components in their inventory, including Information Technology (IT), Internet of Things (IoT), Operational Technology (OT), and Industrial Internet of Things (IIoT). The convergence of IT, OT, IoT, and IIoT significantly increases the attack surface of organizations and provides attack vectors that are challenging to address. Compromised IoT, OT, and IIoT system components can serve as launching points for attacks on organizational IT systems that handle CUI. Some IoT, OT, and IIoT system components can store, transmit, or process CUI (e.g., specifications or parameters for objects manufactured in support of critical programs).

組織では、情報技術 (IT)、モノのインターネット (IoT)、運用技術 (OT)、産業用モノのインターネット (IIoT) など、さまざまなシステムやシステム コンポーネントを在庫に含める場合があります。IT、OT、IoT、および IIoT の統合により、組織の攻撃対象領域が大幅に増加し、対処が困難な攻撃のベクトルが提供されます。侵害された IoT、OT、および IIoT システム コンポーネントは、CUI を処理する組織の IT システムに対する攻撃の開始点として機能します。一部の IoT、OT、および IIoT システム コンポーネントは CUI を格納、送信、または処理できます (例えば、重要な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)。

Most of the current generation of IoT, OT, and IIoT system components are not designed with security as a foundational property and may not be able to be configured to support security functionality. Connections to and from such system components are generally not encrypted, do not provide the

necessary authentication, are not monitored, and are not logged. Therefore, these components pose a significant cyber threat. Gaps in IoT, OT, and IIoT security capabilities may be addressed by employing intermediary system components that can provide encryption, authentication, security scanning, and logging capabilities—thus, preventing the components from being accessible from the Internet. However, such mitigation options are not always available or practicable. The situation is further complicated because some of the IoT, OT, and IIoT devices may be needed for essential missions and business functions. In those instances, it is necessary for such devices to be isolated from the Internet to reduce the susceptibility to cyber-attacks.

現代の世代の IoT、OT、および IIoT システム コンポーネントのほとんどは、セキュリティを基盤として設計されておらず、セキュリティ機能をサポートするように構成できない場合があります。このようなシステム コンポーネントとの接続は、一般に暗号化されず、必要な認証を提供せず、監視されず、ログに記録されません。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引き起こします。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仲介システム コンポーネントを採用することで対処できるため、コンポーネントがインターネットからアクセスできなくなります。ただし、このような緩和オプションは、常に使用できる、または実行可能であるとは限りません。重要なミッションやビジネス機能のために、IoT、OT、IIoT デバイスの一部が必要になる可能性があるため、状況はさらに複雑になります。そのような場合、サイバー攻撃に対する感受性を減らすために、こ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ります。

[SP 800-160-1] provides guidance on security engineering practices and security design concepts.

800-160-1] では、セキュリティ エンジニアリングの実践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ます。

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Preempt, Negate); **Impede** (Contain, Degrade, Delay, Exert); **Limit** (Reduce); **Expose** (Detect)].

3.14.4e- Refresh [*Assignment: organization-defined systems and system components*] from a known,trusted state [*Assignment: organization-defined frequency*]. : 既知の信頼された状態から [割り当て: 組織定義システムとシステム コンポーネント] を更新する [割り当て: 組織定義の頻度]こと。

DISCUSSION 考察

This requirement mitigates risk from the APT by reducing the targeting capability of adversaries (i.e., the window of opportunity for the attack). By implementing the concept of non-persistence for selected system components, organizations can provide a known state computing resource for a specific time period that does not give adversaries sufficient time to exploit vulnerabilities in organizational systems and the environments in which those systems operate. Since the APT is a high-end, sophisticated threat regarding capability, intent, and targeting, organizations assume that over an extended period, a percentage of attacks will be successful. Non-persistent system components and system services are activated as required using protected information and are terminated periodically or at the end of sessions. Non-persistence increases the work factor of adversaries attempting to compromise or breach systems.

この要件は、不利益な標的化能力(すなわち、攻撃の機会の窓)を減らすことによって、APT からのリスクを軽減します。選択し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、組織は特定の期間に既知の状態コンピューティング リソースを提供し、組織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時間を確保できません。APT は、能力、意図、および標的化に関する高度な脅威であるため、組織は長期間にわたって攻撃の割合が成功すると想定しています。非永続システムコンポーネントおよびシステム・サービスは、保護情報を使用して必要に応じて活動化され、定期的に、またはセッションの終了時に終了されます。非永続性は、システムを侵害または侵害しようとする不利益な作業要因を増加させます。

Non-persistence can be achieved by refreshing system components (e.g., periodically reimaging components or using a variety of common virtualization techniques). Non-persistent services can be implemented using “Infrastructure as Code” to automatically build, configure, test, deploy, and manage containers, virtual machines, or new instances of processes on physical machines (both persistent or non-persistent). Periodic refreshes of system components and services do not require organizations to determine whether compromises of components or services have occurred (something that may often be difficult to determine). The refresh of selected system components and services occurs with sufficient frequency to prevent the spread or intended impact of attacks but not with such frequency that it makes the system unstable. Refreshes may be done periodically to hinder the ability of adversaries to exploit optimum windows of vulnerabilities.

非持続性は、システムコンポーネントを更新することによって達成できます(例えば、定期的にコンポーネントを再イメージングするか、さまざまな一般的な仮想化技術を使用して)。非永続的なサービスは、物理マシン上のコンテナ、仮想マシン、またはプロセスの新しいインスタンス (永続または非永続的の両方) を自動的に構築、構成、テスト、デプロイ、および管理するために、「コードとしてのインフラストラクチャ」を使用して実装できます。システム コンポーネントとサービスの定期的な更新では、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ありません (多くの場合、判断が困難な場合があります)。選択したシステムコンポーネントおよびサービスの更新は、攻撃の拡散または意図された影響を防ぐのに十分な頻度で行われますが、システムが不安定になるような頻度ではありません。敵対者が脆弱性の最適なウィンドウを悪用する能力を妨げるために、定期的に更新が行われる可能性があります。

The reimaging of system components includes the reinstallation of firmware, operating systems, and applications from a known, trusted source. Reimaging also includes the installation of patches, reapplication of configuration settings, and refresh of system or application data from a known, trusted source.

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ます。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更新も含まれます。

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Expunge, Preempt, Negate); **Impede** (Degrade, Delay, Exert); **Limit** (Shorten, Reduce)].

3.14.5e- Conduct reviews of persistent organizational storage locations [*Assignment: organization-defined frequency*] and remove CUI that is no longer needed.：永続的な組織の保管場所のレビューを実施する [割り当て: 組織定義の頻度]、不要になった CUI を削除すること。

DISCUSSION 考察

As programs, projects, and contracts evolve, some CUI may no longer be needed. Periodic and event-related (e.g., at project completion) reviews are conducted to ensure that CUI that is no longer required is securely removed from persistent storage. Removal is consistent with federal records retention policies and disposition schedules. Retaining information for longer than it is needed makes the information a potential target for adversaries searching for critical program or HVA information to exfiltrate. The unnecessary retention of system-related information provides adversaries information that can assist in their reconnaissance and lateral movement through organizational systems. Alternatively, information which must be retained but is not required for current activities is removed from online storage and stored offline in a secure location to eliminate the possibility of individuals gaining unauthorized access to the information through a network. The purging of CUI renders the information unreadable, indecipherable, and unrecoverable.

プログラム、プロジェクト、契約が進化するにつれて、一部の CUI が不要になる場合があります。定期的なイベント関連のレビュー(例えば、プロジェクトの完了時)は、不要になった CUI が永続的なストレージから安全に削除されることを確実にするために行われます。削除は、連邦記録保持ポリシーおよび廃棄スケジュールと一致します。必要以上に長く情報を保持すると、重要なプログラムや HVA 情報を検索する敵対者が情報を漏らす潜在的なターゲットになります。システム関連情報の不必要な保持は、組織システムを通じた偵察や横移動に役立つ敵対者情報を提供します。また、オンライン・ストレージから保存する必要があるが、必要とされない情報はオンライン・ストレージから削除され、オフラインで安全な場所に保管され、ネットワークを介して個人が不正に情報にアクセスする可能性を排除します。CUI の削除により、情報は読み取り不能、解読不能、および回復不能になります。

[SP 800-88] provides guidance on media sanitization.

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Expunge, Preempt, Negate); **Impede** (Degrade, Delay, Exert); **Limit** (Shorten, Reduce)].

3.14.6e- Use threat indicator information and effective mitigations obtained from [*Assignment: organization-defined external organizations*] to guide and inform intrusion detection and threat hunting.：侵入検知と脅威の検出を誘導し、情報を提供するために[割り当て: 組織定義の外部組織]から得られる脅威インジケータ情報と効果的な軽減策を使用すること。

DISCUSSION 考察

Threat information related to specific threat events (e.g., TTPs, targets) that organizations have experienced, threat mitigations that organizations have found to be effective against certain types of threats, and threat intelligence (i.e., indications and warnings about threats that can occur) are sourced from and shared with trusted organizations. This threat information can be used by organizational Security Operations Centers (SOC) and incorporated into monitoring capabilities.

組織が経験した特定の脅威イベント (TTP、ターゲットなど) に関連する脅威情報、特定の種類の脅威に対して組織が効果的であることが判明した脅威の軽減、脅威インテリジェンス(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発信および共有されます。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) で使用され、監視機能に組み込まれます。

Threat information sharing includes threat indicators, signatures, and adversary TTPs from organizations participating in threat-sharing consortia, government-commercial cooperatives, and government-government cooperatives (e.g., CERTCC, CISA/US-CERT, FIRST, ISAO, DIB CS Program).

Unclassified indicators, based on classified information but which can be readily incorporated into organizational intrusion detection systems, are available to qualified nonfederal organizations from government sources.

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、政府と政府の協同組合(CERTCC、CISA/US-CERT、ファースト、ISAO、DIB CS プログラム)に参加している組織からの脅威指標、署名、敵対者 TTP が含まれます。

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指標は、政府の情報源から適格な非連邦組織に利用可能です。

PROTECTION STRATEGY 保護戦略

Damage-Limiting Operations.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Expose** (Detect, Scrutinize, Reveal)].

3.14.7e- Verify the correctness of [Assignment: organization-defined security critical or essential software, firmware, and hardware components] using [Assignment: organization-defined verification methods or techniques]. : **[割り当て: 組織定義の検証方法または技術] を使用して、[割り当て: 組織定義のセキュリティ クリティカルまたは重要なソフトウェア、ファームウェア、ハードウェア コンポーネント] の正確さを確認すること。**

DISCUSSION 考察

Verification methods have varying degrees of rigor in determining the correctness of software, firmware, and hardware components. For example, formal verification involves proving that a software program satisfies some formal property or set of properties. The nature of formal verification is generally time-consuming and not employed for commercial operating systems and applications. Therefore, it would likely only be applied to some very limited uses, such as verifying cryptographic protocols. However, in cases where software, firmware, or hardware components exist with formal verification of the component's security properties, such components provide greater assurance and trustworthiness and are preferred over similar components that have not been formally verified.

検証方法では、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、さまざまな程度の厳しさがあります。たとえば、正式な検証では、ソフトウェア プログラムが正式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します。正式な検証の性質は、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ません。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ります。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 コンポーネントがコンポーネントのセキュリティ プロパティを正式に検証する場合、そのようなコンポーネントは、より高い保証と信頼性を提供し、正式に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ます。

[SP 800-160-1] provides guidance on developing trustworthy, secure, and cyber resilient systems using systems security engineering practices and security design concepts.

[SP 800-160-1] システムセキュリティエンジニアリングの実践とセキュリティ設計コンセプトを使用して、信頼性、安全、およびサイバーに対する回復力のあるシステムの開発に関す

るガイダンスを提供します。

PROTECTION STRATEGY 保護戦略

Penetration-Resistant Architecture.

ADVERSARY EFFECTS 不利益な影響

See [SP 800-160-2]: [**Preclude** (Negate); **Impede** (Exert); **Expose** (Detect)].

REFERENCES

LAWS, EXECUTIVE ORDERS, REGULATIONS, INSTRUCTIONS, STANDARDS, AND GUIDELINES[30]

LAWS AND EXECUTIVE ORDERS

[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

POLICIES, REGULATIONS, AND DIRECTIVES

[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

[30] References in this section without specific publication dates or revision numbers are assumed to refer to the most recent updates to those publications.

[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. 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

STANDARDS, GUIDELINES, AND REPORTS

[FIPS 140-3] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, DC), 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, DC), 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, DC), 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, DC), 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, DC), 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, DC), 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. 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 WT, 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, Graubart R, Bodeau D, McQuaid R (2019) Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. (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] Newhouse WD, Witte GA, Scribner B, Keith S (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181. 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 (NISTIR) 8011, Vol. 1. https://doi.org/10.6028/NIST.IR.8011-1

MISCELLANEOUS PUBLICATIONS AND WEBSITES

[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 (2019) *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