TLP:CLEAR

Enhanced Visibility and Hardening Guidance for Communications Infrastructure

通信インフラストラクチャの可視性向上と堅牢化に関するガイダンス【ICT-ISAC Japan 解説追記版】

本ガイダンスには、通信インフラのネットワーク技術者および防御者の方々に対し、可視性の向上とネットワーク機器の堅牢化を図るための重要なポイントがまとめられています。ICT-ISAC Japanでは、本ガイダンスが会員の皆様のみならず、日本の多様な組織における通信インフラの参考に資するよう、翻訳を行った後、ICT-ISAC Japanとして解説を追記しました。翻訳にあたっては、原本に沿ってできる限り忠実に努めましたが、その正確性を保証するものではありません。

[免責事項]
本ガイダンスを雛形として参照することで、セキュリティ改善につながる可能性はありますが、本ガイダンスに記載の内容を遵守すること、あるいは参照したことにより生じるいかなる損失・損害に対しても、ICT-ISAC Japanは一切の責任を負うものではありません。

This document was originally published in English by the United States' Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), and New Zealand's National Cyber Security Centre (NCSC-NZ). It has been translated by a third party and neither CISA, NSA, FBI, ASD, CCCS, NCSC-NZ, nor the U.S. Department of Homeland Security have reviewed the translation. Neither CISA, NSA, FBI, ASD, CCCS, NCSC-NZ, nor DHS are responsible for any errors or omissions relating to this translation. CISA, NSA, FBI, ASD, CCCS, NCSC-NZ have granted permission to ICT-ISAC to use logos and related properties only in a translation which represents a faithful reproduction of the original, and for no other purpose. All other rights reserved. You can find the original English version of this document at CISA.gov.

本ガイダンスは、米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）、国家安全保障局（NSA）、連邦捜査局（FBI）、オーストラリア通信電子局（ASD）傘下のオーストラリアサイバーセキュリティ・センター（ACSC）、カナダサイバーセキュリティセンター（CCCS）、およびニュージーランド国家サイバーセキュリティセンター（NCSC-NZ）によって、当初英語で公開されたものである。

本ガイダンスは第三者によって翻訳されたものであり、CISA、NSA、FBI、ASD、CCCS、NCSC-NZ、および米国国土安全保障省は、当該翻訳をレビューしていない。また、CISA、NSA、FBI、ASD、CCCS、NCSC-NZ、および米国国土安全保障省は、本翻訳に関連するいかなる誤りや漏れについて責任を負わない。

CISA、NSA、FBI、ASD、CCCS、およびNCSC-NZは、原本を忠実に再現した翻訳版においてのみ、ロゴおよび関連資産を使用する許可をICT-ISACに与えているが、それ以外の目的での使用は禁じている。その他すべての権利は留保されている。本文書の英語版原本は、CISA.govにて閲覧可能である。

Contents／目次

Introduction／はじめに

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), and New Zealand's National Cyber Security Centre (NCSC-NZ) warn that People's Republic of China (PRC)-affiliated threat actors compromised networks of major global telecommunications providers to conduct a broad and significant cyber espionage campaign. The authoring agencies are releasing this guide to highlight this threat and provide network engineers and defenders of communications infrastructure with best practices to strengthen their visibility and harden their network devices against successful exploitation carried out by PRC-affiliated and other malicious cyber actors. Although tailored to network defenders and engineers of communications infrastructure, this guide may also apply to organizations with on-premises enterprise equipment. The authoring agencies encourage telecommunications and other critical infrastructure organizations to apply the best practices in this guide.

サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）、国家安全保障局（NSA）、連邦捜査局（FBI）、オーストラリア通信電子局（ASD）の オーストラリアサイバーセキュリティセンター（ACSC）、カナダサイバーセキュリティセンター（CCCS）、ニュージーランド国家サイバーセキュリティセンター（NCSC-NZ）は、中華人民共和国（PRC）関連の脅威アクターが、世界の主要な通信事業者のネットワークを侵害し、広範かつ重大なサイバー諜報活動を展開したと警告している。本ガイダンスは、この脅威を周知するとともに、通信インフラのネットワーク技術者および防御者に対し、可視性の向上とネットワーク機器の堅牢化を図り、中華人民共和国（PRC）関連およびその他の悪意あるサイバーアクターによる侵害を防ぐためのベストプラクティスを提供するために作成した。本ガイダンスは、通信インフラの防御者および技術者を主な対象としているが、オンプレミス型の企業ネットワーク機器を有する組織にも適用可能である。執筆機関は、通信事業者およびその他の重要インフラ組織に対し、本ガイダンスのベストプラクティスを適用することを推奨する。

As of this release date, identified exploitations or compromises associated with these threat actors' activity align with existing weaknesses associated with victim infrastructure; no novel activity has been observed. Patching vulnerable devices and services, as well as generally securing environments, will reduce opportunities for intrusion and mitigate the actors' activity.

本ガイダンスのリリース時点において、これらの脅威アクターの活動に関連して特定された悪用や侵害は、被害者となった組織のインフラストラクチャに内在する既知の脆弱性に起因しており、新たな活動は観測されていない。脆弱なデバイスやサービスへのパッチ適用、および環境全体のセキュリティ強化により、侵入の機会を減らし、脅威アクターの活動を抑制できる。

Strengthening Visibility／可視性向上

In the context of this guide, visibility refers to organizations' abilities to monitor, detect, and understand activity within their networks. High visibility means having detailed insight into network traffic, user activity, and data flow, allowing network defenders to quickly identify threats, anomalous behavior, and vulnerabilities. Visibility is critical for network engineers and defenders, particularly when identifying and responding to incidents.

本ガイダンスにおいて、可視性とは、組織がネットワーク内の活動を監視し、検知し、そして理解する能力を指す。
高い可視性とは、ネットワークトラフィック、ユーザー活動、およびデータフローに関する詳細な洞察を有している状態であり、これによりネットワーク防御者は、脅威、異常な挙動、および脆弱性を迅速に特定できることを意味する。
可視性は、ネットワーク技術者と防御者にとって、特にインシデントの特定と対応において極めて重要である。

解説
本ガイダンスで取り上げている可視性向上と堅牢化のポイント (1) デバイス、特にエッジデバイスは乗っ取られる可能性がある ● 構成設定情報は一元管理しているところから各デバイスに配信すること。デバイス自体を、その構成における信頼できる唯一の情報源として扱ってはならない。(P.6) ● あるデバイスが侵害された際の横展開（ラテラルムーブメント）を防ぐため、OOB管理用ネットワーク内でのデバイス間の横方向（直接）の管理接続を許可しないこと。(P.10) ● 自己署名証明書ではなく、PKI（公開鍵基盤）に基づく証明書を使用すること。(P.14) (2) ネットワーク通信は盗聴あるいはハイジャックされる可能性がある ● 管理用ネットワークには、運用のデータフロー用ネットワークとは物理的に分離された、アウトオブバンド（OOB）管理用ネットワークを利用すべきである。(P.10) ● 通信は可能な限り最大限に、エンドツーエンドで暗号化を徹底すること。(P.12) ● SNMPを利用する場合は、暗号化と認証を備えたSNMPv3のみを利用すること。(P.13) ● 暗号化要件を遵守したSSHバージョン2.0のみを使用すること。(P.14)

Monitoring／モニタリング

Network Engineers／ネットワーク技術者

- Closely scrutinize and investigate any configuration modifications or alterations to network devices such as switches, routers, and firewalls outside of the change management process. Implement comprehensive alerting mechanisms to detect unauthorized changes to the network, including unusual route updates, enabled weak protocols, and configuration changes (i.e., changes to users and Access Control Lists [ACLs]).
- ネットワーク機器（スイッチ、ルーター、ファイアウォールなど）に対する、変更管理プロセス外での構成変更や修正は、厳密に精査し、調査すること。また、異常な経路更新、脆弱なプロトコルの有効化、および構成変更（ユーザーやアクセス制御リスト [ACL] の変更など）を含む、ネットワークへの不正な変更を検出するための包括的なアラート機構を導入すること。
    - Store configurations centrally and push to devices. Do not allow devices to be the trusted source of truth for their configuration. Monitor configuration and, if feasible, test and override on a frequent basis.
    - 構成設定情報は一元管理しているところから各デバイスに配信すること。デバイス自体を、その構成における信頼できる唯一の情報源として扱ってはならない。構成設定を監視し、可能であれば頻繁にテストを実施し、設定情報を上書き（強制適用）すること。

解説（用語）
ネットワーク技術者とは ネットワークの設計、実装、維持管理を担当する。本ガイダンスにおける主な役割は、セキュリティ要件を具体的なネットワーク構成や設定に落とし込むこと。 ネットワーク防御者とは セキュリティ運用、脅威検知、インシデント対応を担当する。本ガイダンスにおける主な役割は、可視性を利用して脅威を特定し、阻止すること。

- Implement a strong network flow monitoring solution. This solution should allow for network flow data exporters and the associated collectors to be strategically centered around key ingress and egress locations that provide visibility into inter-customer traffic.
- 強力なネットワークフロー監視ソリューションを導入すること。このソリューションでは、ネットワークフローデータのエクスポート機能を持つ機器と、それに関連する収集機を、顧客間のトラフィックを可視化できる主要な入口および出口地点に戦略的に配置する必要がある。

解説（参考情報）
ネットワークフローデータのエクスポート機能の具体的な事例に関する参考資料 ● Cisco NetFlowコンフィギュレーション https://www.cisco.com/c/dam/global/ja_jp/td/docs/security/stealthwatch/netflow/Cisco_NetFlow_Configuration.pdf

- If feasible, limit exposure of management traffic to the Internet. Only allow management via a limited and enforced network path, ideally only directly from dedicated administrative workstations.
- 可能であれば、管理トラフィック（ネットワーク機器やサーバの設定・監視などを行う通信）がインターネットにさらされないように制限すること。管理作業は、強制的に制限したネットワーク経路のみを通じて許可し、理想的には管理ワークステーション（DAWs: Dedicated Administrative Workstations）からの直接接続のみに限定すること。

- Monitor user and service account logins for anomalies that could indicate potential malicious activity. Validate all accounts and disable inactive accounts to reduce the attack surface. Monitor logins occurring internally and externally from the management environment.
- ユーザーアカウントおよびサービスアカウント（管理アカウント）のログインを監視し、潜在的な悪意ある活動を示す異常がないかを確認すること。アタックサーフェスを減らすため、すべてのアカウントを（定期的に）検証し、非アクティブなアカウントは無効にすること。管理用区画の内部および外部の双方からのログインを監視対象とすること。

- Implement secure, centralized logging with the ability to analyze and correlate large amounts of data from different sources. Encrypt any logging traffic destined for a remote destination via IPsec, TLS, or any other available encrypted transport options. Additionally, store copies of logs off-site to ensure they cannot be modified or deleted. Enable logging and auditing on devices and ensure logs can be offloaded from the device.
- 安全で中央集約型のロギングを導入し、異なるソースからの大量のデータを分析・相関解析できるようにすること。リモート送信されるロギングトラフィックは、IPsec、TLS、またはその他の利用可能な暗号化された転送オプションを使用して暗号化すること。さらに、ログが改ざんまたは削除されないよう、ログのコピーをオフサイト（別拠点）に保管すること。デバイス上でのロギングと監査機能を有効にし、ログがデバイスから確実に外部転送できるように設定すること。

- If possible, implement a Security Information and Event Management (SIEM) tool to analyze and correlate logs and alerts from the routers for rapid identification of security incidents.
- 可能であれば、ルーターからのログとアラートを分析・相関解析し、セキュリティインシデントを迅速に特定するために、SIEM（Security Information and Event Management）ツールを導入すること。

- Ensure logging takes place at all levels of the environment, network operating system, application, and software levels, as it pertains to network devices.
- ネットワークデバイスに関わるすべてのレベルでロギングが確実に行われるようにすること。ロギングの対象には、環境全体、ネットワークオペレーティングシステム、アプリケーション、およびソフトウェアが含まれる。

- Establish a baseline of normal network behavior and define rules on security appliances to alert on abnormal behavior.
- ネットワークの正常な振る舞い（動作）のベースラインを確立し、異常な振る舞いを検知してアラートを発するためのルールをSEIM等のセキュリティアプライアンスに定義（設定）すること。

解説（参考情報）
イベントログの取扱いに関する参考資料 ● イベントログと脅威検知のベストプラクティス https://www.cyber.go.jp/pdf/policy/kokusai/Provisional_Translation_JP_ASD_LOTL_Guidance.pdf

- Ensure the inventory of devices and firmware in the environment are up to date to enable effective visibility and monitoring.
- デバイスおよびファームウェアのインベントリが常に最新の状態であることを確認し、これにより効果的な可視性と監視を実現すること。

- Implement a monitoring and network management capability that, at a minimum, enforces configuration management, automates routine administrative functions, and alerts on changes detected within the environment, such as connections and user and account activity.
- 最低限、構成管理を実施し、定型的な管理業務を自動化するとともに、接続やユーザー、アカウントの活動など、環境内で検出された変更に対してアラートを発する監視およびネットワーク管理機能を導入すること。

    - Establish understanding of the architecture of infrastructure and production enclaves, as well as where the two environments meet or are segregated. Map and understand boundary and ingress/egress points of the network management enclave.
    - インフラストラクチャ区画と本番用区画（production enclaves）のアーキテクチャを明確に把握し、これら二つの環境が結合または分離されている箇所を明確にすること。また、ネットワーク管理用区画（network management enclave）の境界と入口/出口とを対応付け、明確にしておくこと。

    - Understand which assets should be forward facing and remove those that should not be forward facing. Closely monitor all devices that accept external connections from outside the corporate network and investigate any configurations that do not comply with known good configurations, such as open ports, services, or unexpected Generic Routing Encapsulation (GRE) or IPsec tunnel usage. Threat actors have been observed taking advantage of external-facing vulnerable services and features; therefore, proper visibility of network and security operations is vital.
    - どの資産が外部に公開すべきもの（forward facing）であり、どの資産がそうでないかを明確にし、非公開とすべき資産は除外すること。組織ネットワーク外からの外部接続を受け入れるすべてのデバイスを厳密に監視し、オープンポート、サービス、予期せぬGRE（Generic Routing Encapsulation）やIPsecトンネルの使用など、既知の適切な設定に準拠しない構成がないかを調査し把握すること。攻撃者が外部に面した脆弱なサービスや機能を悪用している事例が確認されているため、ネットワークおよびセキュリティ運用における適切な可視性の確保が不可欠である。

解説（用語）
GRE（Generic Routing Encapsulation） Ciscoが開発し、RFC2784などで標準化されたトンネリングプロトコル

    - If appropriate, implement a packet capture capability as part of the broader visibility effort for the enterprise. Determine capture location(s) and retention policies based on organizational demands.
    - 組織全体の可視性向上の一環として、必要に応じてパケットキャプチャ機能を実装すること。キャプチャの取得場所とデータの保持ポリシーは、組織の要件に基づいて決定しておくこと。

Hardening Systems and Devices／
システムとデバイスの堅牢化

Hardening device and network architecture is a defense-in-depth strategy. Reducing vulnerabilities, improving secure configuration habits, and following best practices limit potential entry points for PRC-affiliated and other cyber threats.

デバイスおよびネットワークアーキテクチャの堅牢化は、多層防御（Defense-in-Depth）戦略のひとつである。脆弱性を減らし、安全な構成維持の習慣を改善し、ベストプラクティスに従うことで、中華人民共和国（PRC）関連およびその他のサイバー脅威に対する潜在的な侵入経路を制限することが可能となる。

Protocols and Management Processes／
プロトコルと管理プロセス

Network Engineers／ネットワーク技術者

- Use an out-of-band management network that is physically separate from the operational data flow network. Ensure that management of network infrastructure devices can only come from the out-of-band management network. In addition, confirm that the out-of-band management network does not allow lateral management connections between devices to prevent lateral movement in the case that one device becomes compromised. Ensure device management is physically isolated from the customer and production networks. When properly implemented, out-of-band management can mitigate many threat actor tactics, techniques, and procedures (TTPs).
- 管理用ネットワークには、運用のデータフロー用ネットワークとは物理的に分離された、アウトオブバンド（OOB）管理用ネットワークを利用すべきである。ネットワークインフラのデバイス管理は、このOOB管理用ネットワークからのみ実行できるように徹底すること。さらに、あるデバイスが侵害された際の横展開（ラテラルムーブメント）を防ぐため、OOB管理用ネットワーク内でのデバイス間の横方向（直接）の管理接続を許可しないこと。デバイスの管理は、顧客用ネットワークおよび本番用ネットワークから物理的に隔離されていることを確実にする。OOB管理が適切に実装されていれば、脅威アクターのTTP（戦術、技術、手順）の多くを軽減することが可能となる。

解説（用語）
アウトオブバンド（OOB）管理 out-of-band management サーバーやネットワーク機器を、通常のデータ通信経路とは別の専用経路を使って管理する手法 インバンド管理 in-band management サーバーやネットワーク機器を、通常のデータ通信経路と同じ経路を使って管理する手法

- Implement a strict, default-deny ACL strategy to control inbound and egressing traffic. Ensure all denied traffic is logged. For maximum depth, implement on separate devices from those implementing other security controls.
- 流入および流出するトラフィックを制御するために、デフォルト拒否（default-deny）を原則とする厳格なACL（アクセス制御リスト）戦略を実装すること。拒否されたトラフィックは、そのすべてを確実にログとして記録すること。防御の多層性を最大化するため、このACL制御は、他のセキュリティ制御を実装しているデバイスとは別のデバイスで実装することが望ましい。

- Employ strong network segmentation via the use of router ACLs, stateful packet inspection, firewall capabilities, and demilitarized zone (DMZ) constructs. Separation via virtual local area networks (VLANs) and, if possible, private VLANs (PVLAN) will provide additional granular logical separation. This should be done as part of a broader defense-in-depth approach that protects and isolates different device groups.
- 強固なネットワークセグメンテーション（ネットワーク分離）を実現するため、ルーターのACL、ステートフルパケットインスペクション、ファイアウォール機能、およびDMZ（非武装地帯）の構築を活用すること。VLAN、そして可能であればPVLAN（プライベートVLAN）を利用することで、よりきめ細かな論理的隔離を実現できる。このVLANによる分離策は、デバイスグループの保護と隔離を目的とした、広範な多層防御アプローチの一環として実施すべきである。

    - Place externally facing services, such as Domain Name System (DNS), web servers, and mail servers, in a DMZ to provide segmentation from the internal LAN and backend resources.
    - DNS、Webサーバー、メールサーバーなどの外部公開サービスは、DMZ（非武装地帯）上に配置し、内部LANやバックエンドリソースから分離すること。

    - Additionally, as a general strategy, put devices with similar purposes in the same VLAN.
    - また、一般的な戦略として、類似した目的を持つデバイスは同じVLAN上に配置すべきである。

    - For example, place all user workstations from a certain team in one VLAN, while putting another team with different functions in a separate VLAN.
    - 例えば、特定のチームのすべてのユーザーワークステーションは一つのVLAN上に配置し、機能が異なる別のチームには別のVLANを割り当てること。

    - Do not manage devices from the internet. Only allow device management from trusted devices on trusted networks. Use dedicated administrative workstations (DAWs) connected to dedicated management zones.
    - デバイスの管理をインターネット経由で実施してはならない。デバイス管理は、信頼できるネットワーク上の信頼できるデバイスからのみ許可すること。このため、専用の管理区画（dedicated management zones）に接続された専用の管理ワークステーション（DAWs: Dedicated Administrative Workstations）を使用すること。

- Harden and secure virtual private network (VPN) gateways by limiting external exposure, if possible, and limiting the port exposure to what is minimally required (for example udp/500, udp/4500 and protocol type 50 (ESP)). Ensure all VPNs are configured to only use strong cryptography for key exchange, authentication, and encryption.[1]
- VPNゲートウェイを堅牢化し、保護すること。可能であれば、VPNゲートウェイの外部への公開を制限し、開放するポートも必要最小限（例：UDP/500、UDP/4500、プロトコルタイプ50（ESP））に絞り込むこと。すべてのVPNが、鍵交換、認証、および暗号化に強力な暗号方式のみを使用するように構成されていることを確認すること [1]。

    - Disable unused VPN features and cryptographic algorithms to prevent exploitable weaknesses.
    - 悪用可能な脆弱性を防ぐため、未使用のVPN機能および暗号アルゴリズムは無効にすること。

- Ensure that traffic is end-to-end encrypted to the maximum extent possible.
- 通信は可能な限り最大限に、エンドツーエンドで暗号化を徹底すること。

解説
暗号化を徹底することの中には、次に示すような施策の適用も考えられる。 PKIの認証局が攻略される可能性への対策 ● mTLS（相互TLS認証） 接続する二者間でTLSプロトコルを使って相互に認証し合う ● 認証局証明書の固定化 偽サーバーへの接続防止 ● SSHサーバー鍵の検証

- As a management policy, control access to device Virtual Teletype (VTY) lines with an ACL to restrict inbound lateral movement connections.
- 管理方針として、デバイスの仮想テレタイプ（VTY）接続へのアクセスをACLで制御し、インバウンド（内向け）の横展開接続を制限すること。

    - Additionally, disable outbound connections to mitigate against lateral movement. Monitor for changes as adversaries can modify this configuration on compromised devices to allow outbound connections.
    - 加えて、（攻撃者による）横展開を低減するため、アウトバウンド（外向けの）接続は無効にすること。攻撃者は侵害したデバイス上でアウトバウンド（外向けの）接続の設定を変更し、外部接続を許可する可能性があるため、本設定の変更は監視対象とすること。

解説（用語）
仮想テレタイプ（VTY） ネットワークデバイス（ルーターやスイッチ）で使用される論理インターフェースの一種。sshなど、ネットワーク経由でデバイスにリモートアクセスし、コマンドラインインターフェース（CLI）を操作するために使用する。

- Ensure all authentication, authorization, and accounting (AAA) logging is securely sent to a centralized logging server with modern confidentiality, integrity, and authentication (CIA) protections.
- AAA（認証、認可、アカウンティング）に関するすべてのログは、最新のCIA（機密性、完全性、可用性）保護を兼ね備えた中央集約型のロギングサーバーに安全に送信されるように徹底すること。
  [注] 原文には confidentiality, integrity, and authentication (CIA) と記載されているが、文脈より authentication は availability であると想定して翻訳している。

- If using Simple Network Management Protocol (SNMP), ensure only SNMP v3 with encryption and authentication is used, along with ACL protections against unnecessary public exposure. Ensure configuration with the most secure cryptographic options supported by the hardware.
- SNMPを利用する場合は、暗号化と認証を備えたSNMPv3のみを利用すること。また、不要な外部公開を防ぐために、ACLによるアクセス制御を適用すること。設定時には、ハードウェアがサポートする最も安全な暗号オプションを用いてSNMPによる監視を構成することを徹底する。

解説
SNMPv2/v3の利用については、運用面で、次のような情報が共有されている。 ● SNMPv2 のセキュリティ形骸化と使われない SNMPv3 https://www.si1230.com/computer/%E7%9B%A3%E8%A6%96/snmpv2-security-and-unused-snmpv3/ ● SNMP バージョン: V1、V2c、または V3 — ネットワーク セキュリティに最適なのはどれですか? https://www.logicmonitor.jp/blog/whats-with-the-different-snmp-versions-s1-v2c-v3

- Disable all unnecessary discovery protocols, such as Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP). If they are required, only enable on the necessary interfaces.
- Cisco Discovery Protocol (CDP) や Link Layer Discovery Protocol (LLDP) など、不要なディスカバリープロトコルはすべて無効にすること。もし利用が必須な場合は、必要なインターフェース上でのみ有効化すること。

- Ensure Transport Layer Security (TLS) v1.3 is used on any TLS-capable protocols to secure data in transit over a network.[2] Ensure TLS is configured to only use strong cryptographic cipher suites.[3]
- ネットワーク上で転送されるデータを保護するため、TLS対応プロトコルにおいては、必ずTLSv1.3を利用すること [2]。その際、強力な暗号化スイートのみを使用するよう設定すること [3]。

    - Use Public Key Infrastructure (PKI)-based certificates instead of self-signed certificates.
    - 自己署名証明書ではなく、PKI（公開鍵基盤）に基づく証明書を使用すること。

    - Implement a robust process to renew certificates before they expire.
    - 証明書が有効期限切れとなる前に更新するための、堅牢な（業務）手順を実装すること。

解説（参考情報）
TLSのセキュリティ設定に関する参考情報 ● SSL Server Test (Powered by Qualys SSL Labs) https://www.ssllabs.com/ssltest/ ● TLS暗号設定ガイドライン 安全なウェブサイトのために（暗号設定対策編） https://www.ipa.go.jp/security/crypto/guideline/ssl_crypt_config.html

- Disable Internet Protocol (IP) source routing.
- IPソースルーティングは無効にすること。

- Disable Secure Shell (SSH) version 1. Ensure only SSH version 2.0 is used with the following cryptographic considerations.[2] For more information on acceptable algorithms, see NSA's Network Infrastructure Security Guide.
- SSHバージョン1は無効にし、以下の暗号化要件を遵守したSSHバージョン2.0のみを使用すること [2]。許容される暗号化アルゴリズムに関する詳細は、NSAのネットワークインフラストラクチャセキュリティガイドを参照のこと。

    - Configure with minimally a 3072-bit RSA key.
    - 鍵長が最低でも、3072ビットのRSA鍵を設定すること。

    - Configure with minimally a 4096 Diffie-Hellman key size (group 16).
    - 鍵サイズが最低でも、4096ビットのDiffie-Hellman鍵（グループ16）を設定すること。

- When possible, apply secure authentication to protocols and services which allow it, such as Network Time Protocol (NTP), Terminal Access Controller Access-Control System (TACACS+), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Hot Standby Router Protocol (HSRP). Similarly, disable any unauthenticated management protocols or functions, such as Cisco Smart Install.
- 可能であれば、NTP、TACACS+、OSPF、BGP、HSRPなど、認証機能を有するプロトコルやサービスには、安全な認証方法を適用すること。同様に、Cisco Smart Installのように、認証を必要としない管理プロトコルや機能は無効にすること。

- Use secure cryptographic building blocks when building VPNs such as [3]:
- VPNを構築する際は、[3] に挙げられているような安全な暗号構成要素（cryptographic building blocks）を使用すること。

    - Key Exchange:
    - 鍵交換：
        - Diffie-Hellman Group 15 with 3072-bit Modular Exponential (MODP)
        - Diffie-Hellman Group 16 with 4096-bit Modular Exponential (MODP)
        - Diffie-Hellman Group 20 with 384-bit Elliptic Curve Group (ECP)
    - Encryption: AES-256
    - 暗号化：AES-256
    - Hashing: SHA-384 or SHA-512
    - ハッシュ：SHA-384または、SHA-512

- Ensure that no default passwords are used.
- デフォルトのパスワードは一切使用しないこと。

    - Change all default passwords on first use.
    - すべてのデフォルトパスワードは初回利用時に変更すること。
    - Ensure no passwords are reset back to the default.
    - パスワードのリセット時に、デフォルトパスワードに戻らないことを確認すること。

- Confirm the integrity of the software image in use by using a trusted hashing calculation utility, if available.
- 可能であれば、信頼できるハッシュ計算ユーティリティを使用し、使用するソフトウェアイメージの完全性を確認すること。

    - If a utility is unavailable, calculate a hash of the software image on a trusted administration workstation and compare against the vendor's published hashes on an authenticated site as a trusted source of truth. This may require engaging the device's maintenance contract to access source of truth hash values. For additional security, copy the image to a forensic workstation and calculate the hash value to compare against the vendor's published hashes.
    - 信頼できるハッシュ計算のユーティリティが利用できない場合、信頼できる管理ワークステーション上で、ソフトウェアイメージのハッシュ値を計算し、認証済みのサイトで公開されているベンダーのハッシュ値（信頼できる情報源）と比較すること。情報源となるハッシュ値にアクセスするためには、当該デバイスの保守契約が必要となる場合がある。さらなるセキュリティ強化のため、ソフトウェアイメージをフォレンジック用ワークステーションにコピーし、ハッシュ値を計算して、ベンダー公開値と比較することも推奨される。

解説（用語）
管理用ワークステーション ネットワーク機器やサーバーなどの管理対象システムを安全かつ信頼できる方法で操作・設定するための専用のコンピュータ フォレンジック用ワークステーション サイバーインシデント発生時やセキュリティ監査のために、デジタル証拠を収集・分析するために用意された、高度な隔離・保全機能を持つ専用のコンピュータ

Network Defenders／ネットワーク防御者

- Disable any unnecessary, unused, exploitable, or plaintext services and protocols, such as Telnet, File Transfer Protocol (FTP), Trivial FTP (TFTP), SSH v1, Hypertext Transfer Protocol (HTTP) servers, and SNMP v1/v2c. Ensure any required internet-exposed services are adequately protected by ACLs and are fully patched.
- Telnet、FTP、TFTP（Trivial FTP）、SSHv1、HTTPサーバー、SNMP v1/v2cなど、不要、未使用、悪用可能、あるいは平文（暗号化されていない）で利用されるサービスやプロトコルは、すべて無効にすること。インターネットに公開される必要最小限のサービスについては、ACLによってアクセス制御を適切に行い、必要なパッチが完全に適用されていることを確認すること。

- Conduct port-scanning and scanning of known internet-facing infrastructure to ensure no additional services are accessible across the network or from the internet. Remove unnecessary internet-facing infrastructure, monitor necessary internet-facing infrastructure, and continuously validate the architecture.
- インターネットに接続されている既存インフラについては、ポートスキャンおよびネットワークスキャンを実施し、ネットワーク全体、またはインターネットから予期せずアクセスできるサービスが存在しないことを確認すること。不要なインターネット公開インフラは排除し、必要な公開インフラは監視しつつ、アーキテクチャの妥当性を継続的に検証すること。

    - Routers with an active shell environment—even if they have not been tampered with—have significantly more listeners running at the operating system (OS) level compared to the software level.
    - シェル環境を有効化したルーターは、たとえ改ざんが行われていない場合でも、ソフトウェアレベルの管理機能が公開する限定的な待ち受けポートに比べ、オペレーティングシステム層で遥かに多数のリスナー（サービス待ち受けソケット・ポート）が稼働していることに留意すべきである。

Network defenders and network engineers should ensure close collaboration and open communication to accomplish the following:

ネットワーク防御者とネットワーク技術者は、以下の事項を達成するために、密接な連携とオープンなコミュニケーションを確保すべきである。

- Ensure all networking configurations are stored, tracked, and regularly audited for compliance with security policies and best practices.
- セキュリティポリシーおよびベストプラクティスへの準拠状況を確認できるよう、すべてのネットワーク構成情報が保存、追跡され、定期的に監査できる状態にあること。

    - Whenever networking configurations are transmitted for storage, tracking, and troubleshooting, confirm that they are sent using encrypted protocols. Additionally, be sure they are not attached to plaintext emails or sent via FTP or TFTP.
    - ネットワーク構成情報を保存、追跡、またはトラブルシューティングのために転送する際は、必ず暗号化プロトコルを利用すること。また、それらを平文のメールに添付したり、FTPやTFTP経由でやり取りしたりしないことを徹底すること。

- Monitor for vendor end-of-life (EOL) announcements for hardware devices, operating system versions, and software, and upgrade as soon as possible.
- ハードウェア、OS（のバージョン）、ソフトウェアに関するベンダーのサポート終了（EOL）の発表を継続的に注視し、可能な限り速やかにアップグレード（または、デバイス更新）を実施すること。

- Implement a change management system that anticipates both routine and emergency patching. Continuously monitor for vendor vulnerability and patch announcements and ensure patches are applied in a timely manner. Ensure use of vendor recommended version of the operating system for the features and capabilities required.
- 定期的及び緊急を要するパッチ適用に対応できる変更管理システムを導入すること。ベンダーによる脆弱性およびパッチ公開の情報を継続的に注視し、適切なタイミングでパッチが適用できる体制を確保すること。要求される機能と性能を満たすために、ベンダーが推奨するOSのバージョンを使用すること。

    - Test and validate patches as part of the change and patch management processes.
    - 変更管理およびパッチ適用管理のプロセスの一環として、パッチのテストと検証を実施すること。

- As part of a broader password policy, store passwords with secure hashing algorithms.
- 包括的なパスワードポリシーの一部として、パスワードは安全なハッシュアルゴリズムを用いて保存すること。

    - Passwords should meet complexity requirements and should be stored using one-way hashing algorithms or, if available, unique keys. Follow National Institute of Standards and Technologies guidelines when creating password policies.
    - パスワードは推測しづらくするため複雑性の要件を満たす必要があり、一方向性のハッシュアルゴリズム、あるいは利用可能であれば、ユニークな鍵を用いて保存する必要がある。パスワードポリシーを作成する際は、NIST（米国標準技術研究所）のガイドライン（NIST SP 800-63 Digital Identity Guidelines）に従うこと。

解説
if available, unique keys. は、固有鍵（PWマネージャーのような複数機器のパスワードを集中管理）ではなく、少なくとも、パスワードファイル毎にユニークな鍵を使用して保存することであると想定される。このため、「パスワードは推測しづらくするため複雑性の要件を満たす必要があり、一方向性のハッシュアルゴリズム、あるいは利用可能であれば、ユニークな鍵を用いて保存する必要がある。」と翻訳している。

- Require phishing-resistant multi-factor authentication (MFA) for all accounts that access company systems, networks, and applications, including sensitive administrative access to routers. MFA should use a combination of credentials and a phishing-resistant secondary verification method, such as hardware-based PKI or FIDO authentication, to ensure secure access and prevent unauthorized entry.
- 組織のシステム、ネットワーク、およびアプリケーションにアクセスする、すべてのアカウント、特にルーターへの機密性の高い管理アクセスに対して、フィッシングへの耐性を持つ多要素認証（MFA）を必須とすること。MFAは、安全なアクセスを確保し、不正な侵入を防ぐため、認証情報（クレデンシャル） と、ハードウェアベースのPKIや FIDO認証などのフィッシング耐性のある別の検証方法（別の要素）とを組み合わせて使用すべきである。

- As part of a broader identity and access management policy, use local accounts only for emergencies and change the passwords after each use. Verify that each use was authorized and expected. For everyday management of network infrastructure, use a centralized AAA server that supports multi-factor authentication requirements; however, ensure the AAA server is not linked to the primary corporate identity store.
- 包括的なIDおよびアクセス管理ポリシーの一環として、ローカルアカウントは緊急時のみに利用し、使用後は毎回必ずパスワードを変更すること。その利用に関して、利用することが承認され、想定されたものであるかを確認すること。ネットワークインフラの日常的な管理には、多要素認証（MFA）をサポートする中央集約型のAAA（認証、認可、アカウンティング）サーバーを利用すること。ただし、このAAAサーバーは、組織の主要なID管理システムとは連携させないこと。

- Limit session token durations and require users to reauthenticate when the session expires.
- セッショントークンの有効期限を制限し、セッションの期限切れ時にはユーザーに再認証を要求すること。

    - Conduct audits to determine the standard session duration for each role to implement session expirations.
    - セッションの有効期限を適切に設定するため、役割（ロール）ごとに標準的なセッション時間を決定するための監査を実施すること。

- Implement a Role-Based Access Control (RBAC) strategy that assigns users to a specific role with defined and inherited permissions to better control and manage what users can do.
- ユーザーが実行できる操作を適切に制御ならびに管理するため、RBAC（ロールベース・アクセス制御）戦略を導入し、定義済みかつ継承された権限を持つ特定のロールをユーザーに割り当てること。

- Remove any unnecessary accounts and periodically review accounts to verify that they continue to be needed. Apply the principle of least privilege to make sure accounts only have the minimum permissions necessary to complete their tasks. Additionally, continuously monitor accounts in use.
- 不要なアカウントは削除し、定期的にアカウントを棚卸して継続的な必要性を確認すること。最小限の権限を付与する原則を適用し、各アカウントが業務遂行に必要な最低限の権限のみを有するように設定すること。また、使用中のアカウントについては継続的に監視すること。

Cisco-Specific Guidance／シスコ製品向けガイダンス

Organizations in the communications sector should be aware that the authoring agencies have observed Cisco-specific features often being targeted by, and associated with, these PRC cyber threat actors' activity. To address the risk of exploitation by these specific threat actors, the authoring agencies urge organizations to apply the following hardening best practices to all Cisco operating systems. For additional information, see Cisco's IOS XE Hardening Guide and Guide to Securing NX-OS Software Devices.

本ガイダンスの執筆機関の観測によると、Cisco固有の機能は、中華人民共和国（PRC）関連のサイバー脅威アクターの関与が認められる活動の主な標的となっている。通信分野にかかわる組織はこの点に留意すべきである。これらの特定の脅威アクターによる悪用リスクに対処するために、本ガイダンスの執筆機関は、すべてのCiscoのオペレーティングシステムに対し、以下の堅牢化（ハードニング）のベストプラクティスを適用することを強く推奨する。詳細については、Ciscoの「IOS XEハードニングガイド」および「NX-OSソフトウェアデバイスのセキュリティ確保ガイド」を参照のこと。

- Disable Cisco's Smart Install service using no vstack.
- "no vstack" コマンドを利用して、Cisco Smart Installサービスを無効にすること。

- If not required, disable the guestshell access using guestshell disable for those versions which support the guestshell service.
- ゲストシェルサービスをサポートするバージョンにおいては、必要がなければ、"guest shell disable" コマンドを使用してゲストシェルの機能を無効にすること。

- Disable all non-encrypted web management capabilities. If web management is required, configure servers in compliance with vendor recommended security settings and software images.
- 暗号化されていないウェブ管理機能はすべて無効にすること。ウェブ管理が必要な場合は、ベンダーが推奨するセキュリティ設定およびソフトウェアバージョンに従って、（ウェブ管理機能を提供する）サーバーを構築すること。

    - Always disable the underlying non-encrypted web server using no ip http server. If web management is not required, disable all of the underlying web servers using no ip http server and no ip http secure-server.
    - 標準で稼働している（システムに組み込まれた）暗号化されていないウェブサーバーは、"no ip http server" コマンドを使用して常に無効にすること。ウェブ管理機能自体が不要であれば、"no ip http server" および "no ip http secure-server" の両コマンドを実行し、すべてのウェブサーバー機能を無効にすること。

- Disable telnet and ensure it is not available on any of the VTY lines by configuring all VTY stanzas with transport input ssh and transport output none.
- telnet を無効化し、すべての仮想テレタイプ（VTY）接続の設定で "transport input ssh" および "transport output none" を指定することにより、VTY接続のいずれからもtelnetが利用できないように構成すること。

- To securely store passwords on Cisco devices, organizations should:
- シスコ製のデバイスにパスワードを安全に保存するために、組織は次のことを実施すべきである。

    - Use Type-8 passwords when possible.
    - 可能であれば、Type-8 のパスワードを利用すること。

    - Avoid use of deprecated hashing or password types when storing passwords, such as Type-5 or Type-7.
    - Type-5やType-7など、非推奨のハッシュまたはパスワードタイプをパスワード保存時に使用しないこと。

    - If supported, secure the TACACS+ key as a Type-6 encrypted password.
    - サポートされている場合は、TACACS+の鍵をType-6で暗号化されたパスワードとして安全に保護すること。

解説（用語）

Type-0：平文
Type-4：PBKDF2 (Password-Based Key Derivation Function version 2)
Type-5：MD5ハッシュアルゴリズム
Type-6：128ビットAES（可逆暗号化）
Type-7：公開されている既知の鍵を用いた単純なアルファベット置換によるVigenere暗号
Type-8：PBKDF2、SHA-256、80ビットソルト、20,000回の反復を使用しハッシュする暗号アルゴリズム
Type-9：SCRYPTハッシュアルゴリズム

Table: Cisco password types

Password type	Ability to crack	Vulnerability severity	NSA recommendation
Type 0	Immediate	Critical	**Do not use**
Type 4	Easy	Critical	**Do not use**
Type 5	Medium	Medium	**Not NIST approved, use only when Types 6, 8, and 9 are not available**
Type 6	Difficult	Low	**Use only when reversible encryption is needed, or when Type 8 is not available**
Type 7	Immediate	Critical	**Do not use**
Type 8	Difficult	Low	**Recommended**
Type 9	Difficult	Low	**Not NIST approved**

詳細は、NSA: Cisco Password Types: Best Practices を参照のこと

Incident Reporting／インシデント報告

- U.S. organizations: If suspicious activity is identified, contact your local FBI field office or the FBI's Internet Crime Complaint Center (IC3). Cyber incidents can also be reported to CISA by calling 1-844-Say-CISA (1-844-729-2472), emailing report@cisa.dhs.gov, or reporting online at cisa.gov/report. For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov.
- 米国：疑わしい活動を特定した場合、最寄りのFBI支局またはFBIインターネット犯罪苦情センター（IC3）に連絡すること。サイバーインシデントは、1-844-Say-CISA（1-844-729-2472）に電話するか、report@cisa.dhs.govにメールを送信するか、cisa.gov/reportでのオンライン報告により、CISAに報告することもできる。NSAのクライアント要件または一般的なサイバーセキュリティに関するお問い合わせは、Cybersecurity_Requests@nsa.govに連絡すること。

- Australian organizations: Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.
- オーストラリア：サイバーセキュリティインシデントの報告、およびアラートや勧告へのアクセスについては、cyber.gov.auにアクセスするか、1300 292 371（1300 CYBER 1）に電話まで。

- Canadian organizations: Report incidents by emailing CCCS at contact@cyber.gc.ca.
- カナダ：CCCS（contact@cyber.gc.ca）にメールでインシデントを報告まで。

- New Zealand organizations: Report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654.
- ニュージーランド：サイバーセキュリティインシデントを incidents@ncsc.govt.nz に報告するか、04 498 7654に電話まで

解説
サイバーセキュリティインシデントの報告は、各国の指定された窓口に連絡してください。 日本の場合には、次の連絡先への報告・相談を検討してください。 ● 独立行政法人情報処理推進機構セキュリティセンター サイバーセキュリティ 相談・届出窓口一覧 https://www.ipa.go.jp/security/support/soudan.html ● 一般社団法人JPCERTコーディネーションセンター(JPCERT/CC) インシデント対応依頼 https://www.jpcert.or.jp/form/

Secure by Design／セキュア・バイ・デザイン

The authoring agencies urge software manufacturers to incorporate secure by design principles into their software development lifecycle to strengthen the security posture of their customers. Software manufacturers should prioritize secure by design configurations to eliminate the need for customer implementation of hardening guidelines. Additionally, customers should demand that the software they purchase is secure by design. For more information on secure by design, see CISA's Secure by Design webpage. Customers should refer to CISA's Secure by Demand guidance for additional product security considerations.

執筆機関は、ソフトウェア開発事業者に対し、顧客のセキュリティ態勢を強化するため、ソフトウェア開発ライフサイクルに「セキュア・バイ・デザイン」の原則を組み込むことを強く推奨する。ソフトウェア開発事業者は、「セキュア・バイ・デザイン」に基づいた設計を優先し、顧客が堅牢化のガイドラインを実装する必要性を排除すべきである。また、顧客も、購入するソフトウェアが「セキュア・バイ・デザイン」に基づいていることを要求すべきである。「セキュア・バイ・デザイン」に関する詳細については、CISAのウェブページを参照のこと。製品セキュリティに関するさらなる検討事項については、CISAの「Secure by Demand」ガイダンスを参照のこと。

解説（参考情報）
セキュアバイデザイン、セキュアバイデフォルトに関する参考情報 • サイバーセキュリティリスクのバランスを変える：セキュアバイデザイン、セキュアバイデフォルトの原則とアプローチ https://www.cyber.go.jp/pdf/policy/kokusai/Provisional_Translation_JP_Principles_Approaches_for_Security-by-Design-Default_October.pdf

Resources／資料

- CISA: Cross-Sector Cybersecurity Performance Goals
- Joint Guide: Best Practices for Event Logging and Threat Detection
- NSA: Network Infrastructure Security Guide
- NSA, CISA, and FBI: People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices
- NSA: Hardening Network Devices
- NSA: Performing Out-of-Band Network Management
- NSA: Cisco Password Types: Best Practices
- NSA: Cisco Smart Install Protocol Misuse
- CCCS: Cryptographic Algorithms for UNCLASSIFIED, PROTECED A, and PROTECTED B Information – ITSP.40.111
- NIST: Special Publication 800-52: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
- NIST: Special Publication 800-77: Guide to IPsec VPNs

References／参考文献

[1] CCCS: Guidance on Securely Configuring Network Protocols
[2] NSA: Network Infrastructure Security Guide
[3] CNSS: Committee on National Security Systems Policy (CNSSP)-15

Disclaimer／免責事項

The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring agencies. Additionally, the information in this document is provided “as-is” and without warranties or representations of any kind. The users of this information shall have no recourse against the authoring parties for any loss, liability, damage or cost that may be suffered or incurred at any time arising from the use of information in this document, including but not limited to loss of data or interruption of business.

執筆機関は、本ガイダンス内でリンクされているものを含め、いかなる特定の商業団体、製品、企業、またはサービスも推奨するものではない。サービスマーク、商標、製造元、その他の方法による特定の商業団体、製品、プロセス、またはサービスへの言及についても、執筆機関による推奨、推薦、または優遇を構成あるいは示唆するものではない。さらに、本ガイダンスの情報は「現状のまま（as-is）」提供し、いかなる種類の保証や表明も伴わない。本情報の利用者は、本ガイダンス内の情報の利用に起因して生じ得るいかなる損失、責任、損害、費用（データの損失や業務の中断を含むがこれらに限定されない）についても、執筆当事者に対して一切の法的措置を講じる権利を有さない。

解説について
解説については、ICT-ISAC Japan 情報共有WGによって追記したものであり、本ガイダンス執筆機関による推奨、推薦、または優遇を構成あるいは示唆するものではありません。 ● 解説には、解釈に関連する補足説明などを記載している。 ● 解説（用語）には、用語の補足説明を記載している。 ● 解説（参考情報）には、関連する情報源を提示している。

Acknowledgements／謝辞

Cisco and Google Cloud Security contributed to this guidance.
本ガイダンスは、CiscoおよびGoogle Cloud Securityの協力を得て作成された。

Version History／改訂履歴

December 3, 2024: Initial version.
2024年12月3日：初版発行
2025年11月11日：ICT-ISAC Japan 情報共有WG　日本語翻訳、翻訳版レビュー
2026年3月7日：「ICT-ISAC Japan 解説追記版」公開の承諾を受領、免責事項を追記