仮訳

# エッジデバイスのための緩和戦略：幹部向けガイド

悪意のある行為者は、ネットワークへの不正なアクセスを得るために、ますますインターネットに接続されたエッジデバイスを標的にしている。従って、組織は、自身の環境内のエッジデバイスの安全化を優先することが不可欠である。エッジデバイスは、内部の企業ネットワークとインターネットとの間のセキュリティ境界として機能する極めて重要なネットワークコンポーネントである。企業ネットワーク全体に実装されているエッジデバイスで最も一般的に見られるのは、企業ルーター、ファイアウォール及び VPN コンセントレータが含まれる。これらのデバイスは、データトラフィックの管理、セキュリティポリシーの適用、ネットワーク境界を越えたシームレスな通信の実現等、重要な機能を実行する。ネットワークの周辺部に配置され、しばしば「エッジ」と呼ばれる。これらのデバイスは、内部のプライベートネットワークと、インターネットのような信頼されていないパブリックネットワークとの間のインターフェイスとなる。

エッジデバイスを安全にできないことは、インターネットから内部ネットワークへの扉を開いたままにしておくようなものであり、悪意のある行為者がこれらのデバイスを介してネットワークにアクセスできる可能性がある。そこから機密データにアクセスし、運用を中断させる可能性がある。

組織が自身の環境にゼロトラスト原則を適用していない場合、悪意のある行為者は、ネットワークエッジデバイスを介してアクセスするために、さまざまな技術を使用する可能性がある。これは通常、製品セキュリティの実績が乏しいエッジデバイスに対して新たにリリースされた脆弱性を特定し、利用することによって発生する。熟練した悪意のある行為者と熟練していない悪意のある行為者の両方が、インターネットにアクセス可能なエンドポイント及びサービスに対して偵察を行い、脆弱なデバイスを特定し、利用する。

エッジデバイスを不正利用する悪意のある行為者の例には、次のようなものがある。

- PRC state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure (ASD)
- People's Republic of China-Linked Cyber Actors Hide in Router Firmware (CISA)

仮訳

# 適用範囲

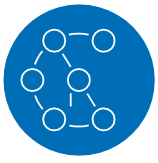
この出版物は、次のパートナー国のサイバーセキュリティ当局に由来する、エッジデバイスを安全にするための既存のガイダンスについてのハイレベルな概要を提供するものである（豪州、カナダ、チェコ共和国、日本、オランダ、ニュージーランド、シンガポール、韓国、英国及び米国）。エッジデバイスを効果的に管理し、安全にするための主要な実行を集約している。このガイダンスは、企業ネットワークの配備、セキュリティ及びメンテナンスの責任者である大規模組織及び重要インフラストラクチャ部門内の幹部を対象としている。

*免責事項：このガイドの情報は、情報提供のみを目的として「現状のまま」提供されている。共同執筆機関は、このドキュメント内でリンクされている主体、製品、サービスを含むいかなる商業的主体、製品、会社又はサービスも支持しない。サービスマーク、商標、製造者又はその他による特定の商業団体、製品、プロセス又はサービスへの言及は、オーサリング機関による支持、推奨又は優遇を構成又は暗示するものではない。*

仮訳

# 緩和戦略の要約

次の表は、ネットワークセキュリティを強化し、脆弱性を緩和することを目的とした、エッジデバイスを保護するための主要な戦略の概要を示すものである。

| | |
|---|---|
|  | **エッジを知る**<br>ネットワークの周辺がどこにあるかを理解し、その周辺に配置されているデバイスを監査するように努める。サポートが終了した（EOL に達した）デバイスを特定し、それらを取り外し、交換する。 |
|  | **セキュア・バイ・デザイン機器を調達する**<br>製品開発中にセキュア・バイ・デザインの原則に従っているメーカーからのエッジデバイスの調達を優先し、調達プロセスの一環として製品セキュリティを明示的に要求する（参考ガイド：https://www.cisa.gov/resources-tools/resources/secure-demand-guide）。配送を追跡し、悪意のある行為者がエッジデバイスを改ざんしていないことの保証を維持する。 |
|  | **セキュリティ強化のガイダンス、更新及びパッチを適用する**<br>特定のベンダーの強化ガイダンスを確認して実装する。既知の脆弱性から保護するために、エッジデバイスにパッチと更新の迅速な適用を確保する。 |
|  | **強力な認証を実装する**<br>弱い認証情報や不十分なアクセス制御による不正アクセスを防止するため、堅固な ID 及びアクセス管理手法を実装する。不正利用から保護するため、エッジデバイス全体にフィッシング耐性のある多要素認証（MFA）を実装する。 |
|  | **不要な機能とポートを無効にする**<br>攻撃を受ける可能性を最小限に抑えるため、エッジデバイスで使用されていない機能やポートを定期的に監査の上、無効にする。 |
|  | **管理インターフェイスを安全にする**<br>管理インターフェイスがインターネットに直接アクセスできないようにすることで、リスクを制限する。 |
|  | **脅威検出のための監視を一元化する**<br>セキュリティインシデントを検出して調査するために、可視性及びログアクセスの一元化を確保する。イベントログもバックアップし、データの冗長性を実装すべきである。 |

仮訳

# 枠組みと管理

共同執筆機関は、エッジデバイスを効果的に安全なものとし、強化し、管理するためのベストプラクティスのガイダンスを含む組織が使用するための次の出版物を提供する。すべての組織は、エッジデバイスのセキュリティを向上させるために、これらのポリシー、手続及び出版物を確認し、それに従うことが推奨される。組織は、エッジデバイスを安全なものとするため、行動と実装の計画を策定する際に、各国のサイバーセキュリティ当局によって策定された推奨事項の実装を優先すべきである。

次の文書は、このガイド内の緩和策の情報源となる。

| |
|---|
| **豪州通信情報局(ASD)**<br>情報セキュリティマニュアル(ISM)と Essential Eight Maturity Model(E8MM)<br>ASD の ISM は、IT 及び OT システムをサイバー脅威から保護するための包括的な一連のガイドラインを提供する。これには、システムの強化、ネットワーキング及びデバイスの調達に関する基準が含まれる。ISM は、サイバーセキュリティの脅威から保護するための戦略を概説した E8MM と整合している。各戦略には、組織がより高いセキュリティ基準を徐々に達成できるように設計された異なる成熟度レベルがある。 |
| **米国サイバーセキュリティ・インフラセキュリティ庁(CISA)**<br>分野横断的なサイバーセキュリティパフォーマンス目標(CPGs)<br>CISA の CPG は、NIST の CSF（サイバーセキュリティフレームワーク）と整合しており、重要インフラの運用と米国民の両方に対するリスクを有意義に削減することを目的とした、セキュリティ成果についての優先リストを提供する。これらの目標は、セクター固有のリスクに対処するように調整されており、組織に対し、サイバー脅威に対する強靭性を向上させるための具体的で成果に焦点を当てた目標を提供している。 |
| **カナダサイバーセキュリティセンター(CCCS)**<br>分野横断的なサイバーセキュリティ準備目標(CRG)ツールキット<br>CCCS の CRG は、一般的なサイバー脅威から組織を保護するための実用的な枠組みを提供している。これは、CISA のサイバーセキュリティパフォーマンス目標(CPG)及び国立標準技術研究所(NIST)のサイバーセキュリティフレームワーク(CSF)と整合するように設計されており、これらのベースラインの管理策は、組織がサイバーセキュリティリスクを管理及び削減する際の指針となる、安全な設定、インシデント対応、アクセス管理などの基本的な実行を強調している。 |

仮訳

| |
|---|
| **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)**<br>ニュージーランド情報安全マニュアル(NZISM)及び サイバーセキュリティフレームワーク(CSF)<br>NZISM 及び NCSC-NZ の CSF は、ニュージーランド政府及び重要インフラセクター全体の情報システムを安全にするための包括的な管理策と基準を提供している。NZISM 及び CSF は、システムの強化、ネットワーク管理、インシデント対応などの側面をカバーしており、組織が国家安全保障上の要件に沿った強固なサイバーセキュリティ対策を実施することを支援するものになっている。 |
| **National Cyber Security Centre(NCSC-UK)**<br>サイバー評価枠組み(CAF)<br>NCSC の CAF は、組織の重要な機能に基づき、サイバーリスクの影響を受ける程度を評価するための体系的かつ包括的なアプローチを提供し、組織がこれらのリスクに対するサイバー強靭性を構築することを支援するものとなっている。CAF は、ガバナンス、資産管理、システム強靭性などの主要な原則に焦点を当て、組織がその慣行を英国の国家サイバーセキュリティ戦略と整合させることを支援し、組織が不可欠なサービスに対するリスクを緩和することに役立つものとなっている。 |
| **経済産業省（METI-JP）**<br>サイバーセキュリティ経営ガイドライン<br>経済産業省（METI）と独立行政法人情報処理推進機構（IPA）は、経営者のリーダーシップの下でサイバーセキュリティ対策を推進するため、企業経営者向けに「サイバーセキュリティ経営ガイドライン」を提供している。サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「3 原則」、及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要 10 項目」がまとまっている。 |

仮訳

## セキュア・バイ・デザインなエッジデバイスの調達

組織は、あらゆるエッジデバイスを調達する前に、全てのセキュリティ上の懸念が考慮され、対処されていることを確保するために、原産国を含む製造業者とその製品を評価しなければならい。セキュア・バイ・デザインの実践に従って開発された技術を選択することは、組織が、機密性、完全性及び可用性を維持し、コストのかかるイベントを緩和し、強靭な企業ネットワークを構築することを支援するものとなる。

共同執筆機関は、エッジデバイスを調達する際のガイダンスとして、次の出版物を推奨している。

- Choosing Secure and Verifiable Technologies: Secure-by-Design Foundations(ASD)
- Secure-by-Design Foundations（ASD）
- Cyber supply chain: An approach to assessing risk(CCCS)
- Supply chain security guidance(NCSC-UK)
- Secure-by-Design（CISA）
- Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Econosystem(CISA 及び FBI)

なお、日本における JC-STAR ラベルを有する製品のようなラベル又は認証された製品を選択することは、組織が適切なセキュリティ措置を備えた製品を調達するのに役立つであろう。

さらに、共同執筆機関は、すべてのエッジデバイス製造業者に対して、製品を設計によって安全にすること（secure by design）を奨励している。製造業者は、自身の製品において、既定において安全な機能を実装する方法についてのガイダンスとして、CISA の「Secure by Design Alert:Security Design Improvements for SOHO Device Manufacturers」を確認し、CISA の「Secure by Design Pledge」に参加することができる。この誓約は、自身の製品の脆弱性の存在を減らし、透明性を以て脆弱性について報告するという目標を含む、自身の製品をより安全にするために製造業者が達成すべき特定の目標を概説するものとなっている。

## ネットワークのセグメント化と分離

ネットワークのセグメント化と分離は、ネットワーク内の不正アクセスの可能性のある経路や横展開の可能性のある経路を制限することによって組織の環境を保護するため、極めて重要である。

同アプローチは、機密システムを隔離することによって、サイバー脅威に対する防御を強

仮訳

化し、侵害の影響を最小限に抑え、相互接続されたシステム全体にわたり強靭性のある運用を確保する。共同執筆機関は、ネットワークのセグメント化と分離に関するガイダンスとして、次の出版物を推奨している。

- Implementation Network Segmentation and Segregation (ASD)
- A zero trust approach to security architecture (CCCS)
- Baseline security requirements for network security zones (version 2.0)-ITSP.80.022 (CCCS)
- Preventing Lateral Movement (NCSC-UK)
- CPGs: Securing Network Infrastructure Devices、Zero Trust Maturity Model、Layering Network Security Through Segmentation Infographic (CISA)
- Reducing the risk of network compromises (NSA)

## ゲートウェイの強化

ゲートウェイの強化は、組織がゲートウェイサービスを設計、調達、運用、維持又は廃棄するのを支援することを目的としている。ゲートウェイは、異なるセキュリティドメインを分離する境界システムであり、組織が異なるセキュリティドメイン間のデータ転送のためのセキュリティポリシーを実施できるようにするものである。提携したサイバーセキュリティ当局は、組織がサイバーセキュリティの課題に対処し、ゲートウェイセキュリティを強化するために十分な情報に基づいたリスクに基づく決定を行うことを支援するよう努めている。

共同執筆機関は、ゲートウェイの強化に関するガイダンスとして、次の出版物を推奨している。

- Gateway Security Guidance Package (ASD)
- Top 10 IT security actions to protect Internet connected networks and information (CCCS)
- Trusted Internet Connections (TIC) (CISA)
- Network Infrastructure Security Guidance, Hardening Network Devices (NSA)

## スマートインフラストラクチャでのエッジデバイスの安全

エッジデバイスは、最新のスマートインフラストラクチャにおいて重要な役割を果たし、スマートテクノロジー間のデータフローと通信をサポートする重要な接続ポイントとして機能する。共同執筆機関は、スマートインフラストラクチャでエッジデバイスを保護するためのガイダンスとして、次の出版物を推奨している。

- Introduction to Securing Smart Places (ASD)
- VPNs (CCCS)

仮訳

- Connected Community (CCCS)
- VPNs：Network Architectures (NCSC-UK)
- Cybersecurity Best Practices for Smart Cities (CISA)

## イベントログと脅威検出

悪意のある行為者がネットワーク内に足場を確立すると、彼らは、組み込まれているツールとシステムプロセスを活用して目的を達成することを含む、環境寄生型（Living Off the Land）技術を使用できる。これにより、ネットワーク防御者が悪意のある活動と正当な活動とを区別することが困難になる。これらの技術から防御するには、可視性を可能にし、脅威を検出するための包括的なイベントログとネットワーク遠隔情報収集（telemetry）が重要である。

侵害が発生した又は発生した疑いがある場合、堅固なロギングは、組織が脅威や侵入を効果的に監視するのに役立つ。共同執筆機関は、脅威及び侵入の監視に関するガイダンスとして、次の出版物を推奨している。

- Best Practice for Event Logging and Threat Detection (ASD)
- Introduction to logging for security purposes (NCSC-UK)
- Cross-sector CPGs (CISA)
- Network security logging and monitoring (CCCS)

## レガシーエッジデバイス

ソフトウェアがメーカーによってサポート又は更新されなくなると、エッジデバイスは最終的にレガシーハードウェア又は EOL（サポートが終了)となる。EOL に達したエッジデバイス、特にメーカーによってサポートされなくなったエッジデバイスは、サイバー脅威に対してより脆弱になる可能性がある。サイバー脅威に対して安全であることを確保するため、ソフトウェアがサポートされているバージョンにアップグレードするか、EOL に達したエッジデバイスを交換することが極めて重要である。

共同執筆機関は、古くなったエッジデバイスに関連するリスクの理解、評価及び管理に関するガイダンスとして、次の出版物を推奨している。

- Managing the Risk of Legacy IT (ASD)
- Obsolete products (CCCS)
- Obsolete products (NCSC-UK)
- Understanding Patches and Software Updates (CISA)

仮訳

# 更なる情報及び連絡先

組織は、エッジデバイスの安全化やエッジデバイスに対するサイバーセキュリティのベストプラクティスの実装に関連する追加のガイダンス、情報源又は特定の問い合わせについては、それぞれの国のサイバーセキュリティ当局に連絡することが推奨される。

**豪州通信情報局(ASD)**
問い合わせは、ASD のウェブサイト www.cyber.gov.au にアクセスするか、オーストラリアのサイバーセキュリティホットライン 1300 CYBER1(1300 292 371)にお電話下さい。

**カナダサイバーセキュリティセンター(CCCS)**
CCCS はカナダの組織を支援しています。出版物やガイダンスについては www.cyber.gc.ca にアクセスするか、1-833-CYBER-88 経由で CCCS に連絡するか、contact@cyber.gc.ca に電子メールで連絡してください。

**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)**
NCSC-NZ はニュージーランドの組織を支援しています。ガイダンスとリソースについては www.ncsc.govt.nz にアクセスするか、info@ncsc.govt.nz に電子メールを送信してください。

**国家サイバーセキュリティセンター(NCSC-UK)**
英国を拠点とする組織の場合、NCSC は www.ncsc.gov.uk で包括的なリソースを提供しています。NCSC の連絡先ページには、問い合わせの詳細が記載されています。又は、電子メールで inquiries@ncsc.gov.uk までお問い合わせください。

**米国土安全保障省サイバーセキュリティ・インフラ庁(CISA)**
CISA は、米国を拠点とする組織をサポートしています。www.cisa.gov にアクセスしてリソースを入手するか、central@cisa.gov の電子メールで連絡してください。疑わしい又は悪意のあるサイバーアクティビティを CISA に報告するには、CISA のインシデント報告フォーム又は 24/7 オペレーションセンター(report@cisa.gov)を使用するか、1-844-Say-CISA(1-844-729-2472)に電話してください。

**内閣サイバーセキュリティセンター（NISC）**
問合せは以下のサイトにアクセスしてください
https://www.kantei.go.jp/jp/forms/nisc_opinion.html（NISC）

**JPCERT コーディネーションセンター (JPCERT/CC)**
JPCERT/CC にインシデントレポートを提出するには、info@jpcert.or.jp まで電子メールを送信してください。