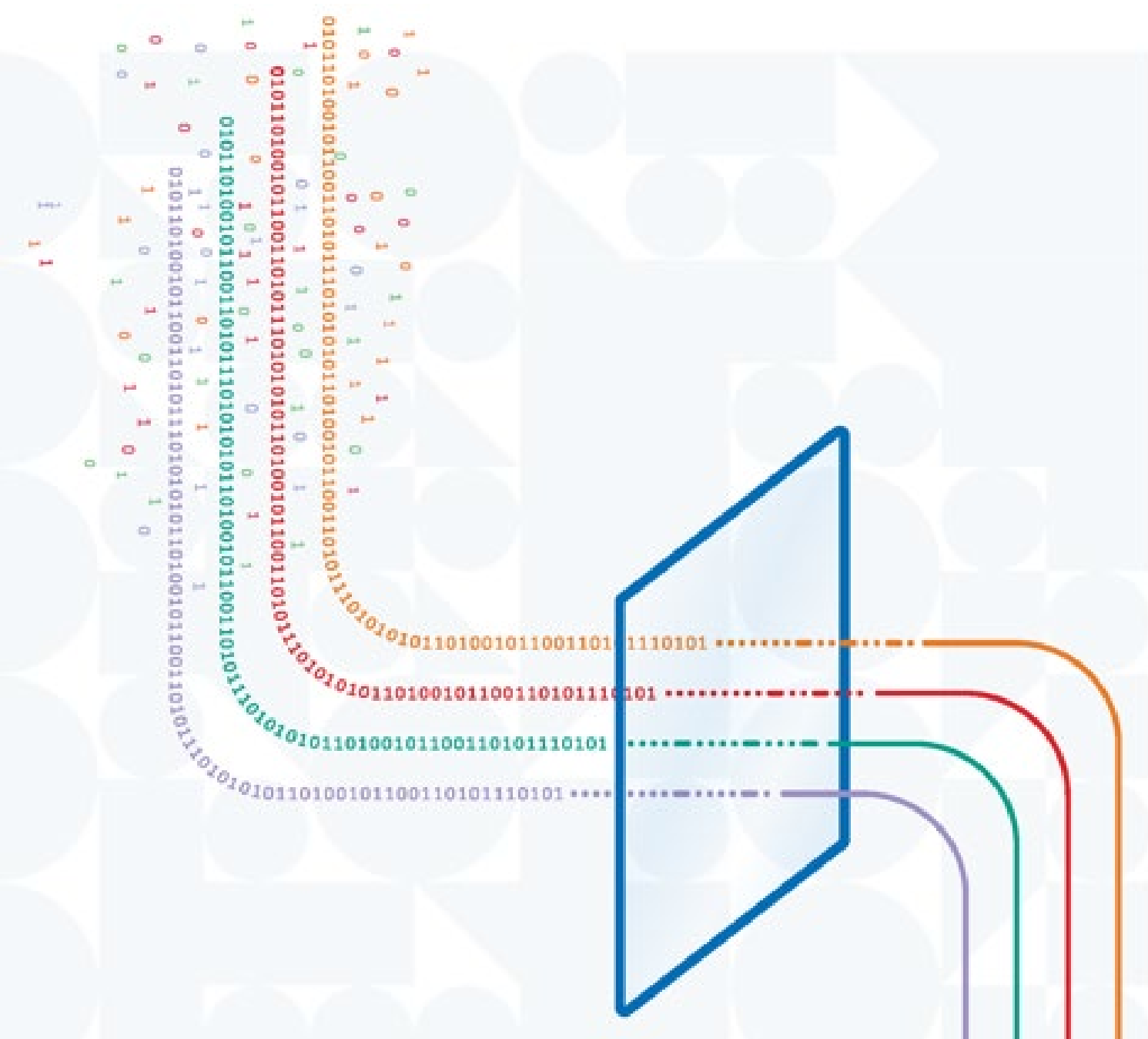


エッジデバイスのための緩和戦略:実務者向けガイド





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エンティティ、製品、サービスを含む、いかなる商業的エンティティ、製品、会社、また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。

目次

対象読者	4
はじめに: エッジに生存する	5
エッジデバイスの概要	6
リスクと脅威	7
ケーススタディ- Cutting Edge	8
枠組みと管理	9
緩和戦略の要約リスト	11
エッジデバイスのための緩和戦略	12
結論	27

対象読者

このガイドは、運用スタッフ、サイバーセキュリティスタッフ及び調達スタッフを対象としている。

- ・ **運用スタッフ**とは、組織のネットワーク内のエッジデバイスの可用性とメンテナンスを担当する実務者を指す。
 - 役割には、ネットワークエンジニア、システム管理者、IT システム/ネットワーク構築者、IT 管理者が含まれる。
- ・ **サイバーセキュリティスタッフ**とは、組織のネットワークにおけるエッジデバイスのセキュリティ面を担当する実務者を指す。これらの実務者は、インシデント対応、脅威検出、脆弱性管理などの活動を行う。
 - 役割には、SOC アナリスト、サイバーセキュリティエンジニア、インシデント対応チームメンバー、脆弱性アナリスト、セキュリティマネージャが含まれる。
- ・ **調達スタッフ**とは、エッジハードウェア及びソフトウェアの選択と購入に従事し、セキュリティ管理が調達プロセスの一部であることを保証する実務者を指す。
 - 役割には、IT 購買管理者、調達担当者、ベンダー関係管理者が含まれる。

はじめに：エッジに生存する

悪意のある行為者は、インターネットと内部ネットワークの間の仲介者として機能する「エッジデバイス」を標的にしている。新たに発見された脆弱性の迅速な悪用は、現在、多くの悪意のある行為者にとって標準的な手法となっている。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ネットワークに対してスキャンと偵察を行い、パッチが適用されていないソフトウェアを見つけ、脆弱なデバイスを悪用する。

このマニュアルでは、「エッジデバイス」という用語を使用している。このガイドでは、「エッジデバイス」という用語は、インターネットに接続されるネットワークハードウェア及び機器を総称して使用する。

目的

このガイドは、ASD による「エッジデバイスの緩和戦略：幹部向けガイド」を実務者向けに拡張したものであり、サイバー脅威に対するセキュリティと強靭性を向上させるためのエッジデバイスの主要な緩和戦略のリストを提供する。これらの戦略は、ベンダーに依存せず、企業ネットワーク及び大規模組織全体で最も一般的なタイプのエッジデバイス及び機器に適用される。

だから何？

豪州通信電子局 (ASD) ・豪州サイバーセキュリティセンター (ACSC) は、エッジデバイスの侵害を含むインシデント数の懸念すべき増加を指摘している。エッジデバイスは、インターネット上に晒されており、通常は監視が困難で、ネットワーク上の他の資産にアクセスでき、悪意のある行為者にとって魅力的な侵入ポイントと標的になる。

ASD がオーストラリア全体で実施した最近の研究プロジェクトでは、2 カ月間にわたって 1790 万台のデバイスが一般のインターネットから可視状態にあった。これらのデバイスのうち 212,000 台がエッジデバイスとして識別された¹。

組織がゼロトラストアーキテクチャ (ZTA) を適用する場合でも、このガイダンス内の原則は、企業ネットワーク全体のエッジデバイスに適用されるべきである。ゼロトラストの原則は、境界管理への依存を軽減するが、企業ネットワーク全体の安全なエッジの必要性を排除するものではない。

¹ Analytical Paper: Enterprise Edge Device Environment – Australian Government and Critical Infrastructure Networks', Research on Operational, Critical and Emerging Technology, ACSC (Limited distribution)

エッジデバイスの概要

エッジデバイスとは何か。

エッジデバイスは、企業内ネットワークとインターネットの間のセキュリティ境界として機能する重要なネットワークコンポーネントである。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など、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を接続する。

この文書の原則は、最も実装されているエッジデバイスである企業ルーター、ファイアウォール及びVPN コンセントレータの3つを対象としている。

	企業ルーター ネットワークのエッジとなっているルーターは、内部ネットワークと信頼されていない外部ソース（主にインターネット）との間の着信及び発信トラフィックを方向付けるものである。基本的なセキュリティルールを適用してアクセスを制御しながら、効率的にデータが宛先にルーティングされることを保証する。
	ファイアウォール エッジとなっているファイアウォールは、防御の最前線として機能し、内部ネットワーク及び外部との間のトラフィックを検査及びフィルタリングする。ファイアウォールは、事前に定義されたルールに基づいてトラフィックをブロックし又は許可し、不正アクセスを防止し、特定された悪意のあるアクティビティを阻止することによって、セキュリティポリシーを実施する。
	VPN コンセントレータ エッジとなっているVPN コンセントレータは、インターネットを介して接続するユーザーに対し、暗号化されたトンネルを作成することによって、内部ネットワークへの安全なリモートアクセスを提供する。VPN は、ユーザーを認証し、データを暗号化して、送信中に機密情報が安全に保たれるようにする。

リスクと脅威

なぜエッジを保護するのか

インターネットまたは外部ネットワークに接続している組織は、少くとも1つのエッジデバイスを導入しており、セキュリティへの対応が重要になっている。エッジデバイスは、容易に軽減できる脆弱性を通じて、引き続き悪用されている。これらのデバイスは、従来のネットワーク境界の一部であっても、成熟したゼロトラスト環境内であっても、外部の脅威の表面から直接アクセスできる。組織は、セキュリティ態勢を強化するために積極的な措置を講じなければならない。

インパクト

エッジデバイスが十分に安全でない場合、結果として、損害を与える可能性がある。悪意のある行為者は、エッジデバイスを侵害して初期アクセスを取得し、このアクセスを使用して組織の内部ネットワーク環境に横展開する。このアクセスにより、悪意のある行為者は、システムや重要なサービスの中断、マルウェアの配備、持続化、個人データやその他の機密情報の盗難など、他の目的を達成できる。

これらの悪意のある行為は、組織に対して、金銭的損失、風評被害、法的影響及びその他の重大な損害をもたらす可能性がある。

エッジデバイスの脆弱性がどのように悪用されるかを示す最近の例として、[Cutting Edge](#) キャンペーンがある。このキャンペーンは、重要なセクターを対象とし、VPN 機器のゼロデイ脆弱性を利用して壊滅的な影響を与えた。

[Cutting Edge](#) キャンペーンのケーススタディは、以下に含まれており、悪意のある行為者によって使用される [MITRE ATT&CK テクニック](#) にマッピングされている。

ケーススタディ - Cutting Edge

2023 年 12 月から 2024 年 2 月にかけて、Cutting Edge キャンペーンの背後にいる悪意のある行為者は、防御回避、環境寄生型 (Living-off-the-Land) 技術及び Web シェルとカスタムマルウェアの展開を利用することにより、Ivanti 社 Connect Secure VPN 機器 (以前の Pulse Secure) のゼロデイ脆弱性を不正利用した。

悪意のある行為者は、次の方法で初期アクセスを実行した。

- ・ Ivanti Connect Secure VPN 機器における CVE-2023-46805 及び CVE-2024-21887 を悪用し、認証バイパスとコマンドインジェクションを有効とした。その後、サーバーサイドのリクエストフォージェリ（SSRF）の脆弱性である CVE-2024-21893 が発見され、CVE-2024-21887 [T1554] と結びつけ、最初の 2 つの脆弱性の緩和策をバイパスするために使用された。

悪意のある行為者は、次の方法でプレゼンスを確立した。

- ・ Ivanti 社 Connect Secure 機器の正規ファイルを悪意のあるコードで「トロイの木馬化」することを通じて [T1554]
- ・ Connect Secure VPN から、実行中の設定とキャッシュデータを盗むことを通じて [T1005]
- ・ 脆弱性を利用して、Ivanti 社 Connect Secure VPN ヘリモートファイルのダウンロードすることを通じて [T1105]
- ・ 悪意のあるプラグインを使用し、侵害した Ivanti 社 Secure Connect VPN に対して持続性を維持し、バックドアの展開を可能にすることを通じて [T1055]

悪意のある行為者は、次の方法で認証情報を盗んだ。

- ・ Ivanti 社 Connect Secure 機器の Web SSL VPN コンポーネント上の JavaScript ファイルを変更し、認証情報をキーロギング（記録する）ことを通じて[T1056.001]
- ・ Ivanti 社 Connect Secure のログインページで読み込まれる JavaScript を変更し、入力された認証情報を取得することを通じて[T1056.003]

悪意のある行為者は、次の方法で横方向の移動を達成した

- ・ 以前に盗まれた有効なアカウント認証情報を使用して、内部ネットワークにアクセスすることを通じて [T1078]
- ・ 以前に侵害した認証情報をリモートサービス技術 (SSH、SMB 及び RDP の混合) のために使用することを通じて

悪意のある行為者は、検出を回避するために、次のような複数の技術を利用した。

- ・ ロギングを無効にし、compcheckresult.cgi コンポーネントを変更して、Ivanti 社 Connect Secure に組み込まれている Integrity Checker 除外リスト編集することを通じて [T1562.001]
- ・ 侵害した Ivanti 社 Connect Secure VPN 上のファイルのタイムスタンプ（修正、アクセス、作成及び変更時間）を変更することを通じて [T1070.006]

このケーススタディの詳細な分析は、次の場所にある。[Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways](#)

枠組みと管理

組織は、エッジデバイスを保護するための行動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施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) 情報セキュリティマニュアル (ISM) と Essential Eight Maturity Model (E8MM) 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) 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) 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靱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) 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 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。
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) 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) 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)

サイバー評価枠組み(CAF)

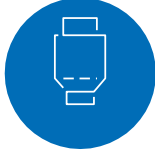
NCSC の CAF は、組織の重要な機能に基づき、サイバーリスクの影響を受ける程度を評価するための体系的かつ包括的なアプローチを提供し、組織がこれらのリスクに対するサイバー強靱性を構築することを支援するものとなっている。CAF は、ガバナンス、資産管理、システム強靱性などの主要な原則に焦点を当て、組織がその慣行を英国の国家サイバーセキュリティ戦略と整合させることを支援し、組織が不可欠なサービスに対するリスクを緩和することに役立つものとなっている。

経済産業省 (METI-JP)

サイバーセキュリティ経営ガイドライン

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。

緩和戦略の要約リスト

	エッジを知る 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 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。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 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 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 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 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 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。

エッジデバイスのための緩和戦略

次の主要な緩和戦略のリストは、主に、企業ネットワークに対する不正利用の成功をもたらすエッジデバイスに関する一般的な問題に対処することに焦点を当てている。これらの戦略は、いかなる連続的な重要性のレベルにおいても優先順位付けされているものではない。

これらの戦略は、可能な場合には、サイバーセキュリティフレームワーク (CSF) による関連する部分の管理策を補完するものである。パートナー国は、可能であれば、これらの緩和策を採用するか、互換性があれば、これらの管理策を別の CSF と同等のものにマッピングすることが歓迎される。

エッジを知る

組織は、エッジデバイスを保護する前に、これらエッジデバイスがネットワーク周辺のどこに位置し、どのような役割を果たしているかを知る必要がある。豪州通信情報局 (ASD) の運用の経験によれば、しばしば、組織はネットワークエッジと存在するサービスについての理解及び可視性が限られていたことが示唆されている。

組織は、以下を認識しておくべきである。

- ・ エッジデバイスは、情報通信技術 (ICT) 環境では広く理解されていない、比較的小さな役割を果たすことができること
- ・ エッジデバイスが、様々な理由から、企業の資産管理コンソールの外に存在していることが検出されていること
- ・ エッジデバイスは、既知又は必要以上のサービスをインターネットに提供している可能性があること

例：

- ・ 使用されていないときに VPN インターフェイスをインターネットに公開したままにする統合ファイアウォール機器
- ・ ネットワークに対して運用又は管理インターフェイスをオープンにしたままのエッジデバイス

エッジデバイスがどこに存在するかを知ることは、それらを保護するための最初のステップ

ASD のサイバーハイジーン改善計画 (CHIPs) に登録されている事業体は、CHIPs レポートを使用してこの作業を通知できる。このプログラムに参加していない組織は、インターネットからネットワークエッジがどのように見えているかの可視性を向上させるため、攻撃面の監視機能の開発を検討するべきである。



セキュア・バイ・デザイン機器を調達する

エッジデバイスにおけるサイバーサプライチェーンセキュリティリスクの管理は、製品ライフサイクルのすべての段階でセキュリティを優先するベンダーからのデバイス調達から始まる。組織は、セキュリティに対するコミットメントが実証されているベンダーを選択することで、脆弱な又は侵害されたハードウェア及びソフトウェアをネットワークに導入するリスクを最小限に抑えることができる。

ベンダーを評価する

IT 機器は、セキュア・バイ・デザイン及びセキュア・バイ・デフォルトの原則、可能な場合には、メモリ安全性の高いプログラミング言語の使用及びその他の安全なプログラミング実行及び製品のセキュリティの維持に対するコミットメントを実証したベンダーから選択される。

主要な枠組の管理策、出版物や規約: ISM-1857; NIST CSF; NIST SP 800-53, Rev. 5; NIST SP 800-161r1upd1

調達チームは、エッジデバイスのベンダーを選択する際には注意を払うべきである。これには、ベンダーのパッチリリースの履歴や、新たに発見された脆弱性への対応時間の確認が含まれる。セキュリティの脆弱性を開示する際のベンダーの透明性と、それらに対処した履歴を評価するべきである。理想的には、ベンダーは、エッジデバイスの強化ガイダンスを作成することにコミットし、セキュア・バイ・デザイン及びセキュア・バイ・デフォルトの製品設計を採用しているべきである。

日本における [JC-STAR ラベル](#) を有する又はカナダにおける [CC 認証を有する製品](#) のような、ラベル付け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。

ベンダーリスクを管理する

CISO は、組織のサイバーサプライチェーンリスクの管理活動を監督する。

主要な枠組の管理策、出版物や規約: ISM-0731; NZISM-3.2.14.C.01; NIST SP 800-161r1upd1

サプライチェーンセキュリティの重要な部分は、特定のベンダーに関連する可能性のある地理的リスク、地政学的リスク及びサプライチェーンリスクを理解することである。各ベンダーの製造プロセス、地理的な場所及びサプライチェーンの依存性が、組織に許容できないリスクをもたらすかどうかを評価すること。サプライチェーンに予期しない脆弱性や中断が発生した場合に、代替のサプライヤ又は二次的なソースが単一のベンダーへの依存を減らすかどうかを検討すること。

安全に配送する

アプリケーション、IT 設備、OT 設備及びサービスは、その完全性を維持する方法で提供される。

主要な枠組の管理策、出版物や規約: ISM-1790; NZISM-12.7.18.C.02; NZISM- 12.1.35.C.01; NZISM-12.1.34.C.02; NISTCSF; NISTSP800-53, Rev.5; NISTSP800-161r1upd1

ネットワークの完全性をサポートするには、製造時点から最終設置までのエッジデバイスの配送を保護することが重要である。出荷又は取り扱い中に改ざんされたデバイスは、組織のネットワークインフラストラクチャに重大な脆弱性をもたらす可能性がある。これらのリスクを緩和するために、調達担当者はサプライチェーン全体で適切な完全性チェックメカニズムを確保すべきである。

サプライチェーンを追跡する

サプライチェーンの可視性システムを実装することにより、デバイスを生産地点から最終設置地点まで追跡するのに役立つ。デバイスの配送状況をリアルタイムで追跡し、透明性のあるレポートを提供するサプライヤーと提携することで、配送されたデバイスの完全性を確保できる。

信頼性と完全性を評価する

ネットワークデバイスは、初めて使用される前に、信頼されたファームウェアでフラッシュ（書き直し）されます。

主要な枠組の管理策、出版物や規約: ISM-1800; NZISM-12.4.6.C.01; NIST SP 800-161r1upd1; CISA CPG 2.Q

組織は、エッジデバイスを受け取ったときに、ハードウェアとソフトウェアの両方を徹底的に検査して、改ざん又は操作の兆候がないかどうかを確認すべきである。これには、改ざん防止包装が無傷であることの確認を含むことができる。

サイバーサプライチェーン妨害攻撃（cyber supply chain interdiction attack）、ベンダー開発環境への侵害その他のサイバーサプライチェーンリスクに起因する悪意のあるファームウェアの導入は、エッジデバイスを初めて使用する前に、信頼できる方法でベンダーから入手した信頼できるファームウェアを使用してネットワークデバイスをフラッシュ（書き直し）することで緩和できる。

展開前にデフォルトの認証情報を確認する

ネットワークデバイスのデフォルトアカウント又は認証（事前設定されたアカウントを含む）が変更される。

主要な枠組の管理策、出版物や規約: ISM-1304; NZISM-14.1.10.C.02; CISA CPG 2.A; CCCSCRG-2.0

デフォルトの認証情報を提供するベンダー製品ではなく、認証情報の作成が必要なベンダー製品を選択することが推奨される。デバイスの製造元によって提供されるデフォルトの認証情報は、広く知られていることが多く、悪意のある行為者の主要な標的となる。新しいデバイスの初期セットアップ中に必ずこれらを変更し、既存のエッジデバイス全体でもデフォルトの認証情報を監査して、一度に変更を行う。



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

エッジデバイスを強化し、最新のセキュリティパッチで最新の状態に保つことはネットワークのセキュリティを維持する上で重要な役割を果たす。

特定のベンダー強化ガイダンスをレビューし実装する

IT 機器は、ASD 及びベンダーの強化ガイダンスを使用することで強化される。競合が発生した場合は、最も制限の厳しいガイダンスが優先される。

主要な枠組の管理策、出版物や規約: ISM-1858; NZISM-22.2.14.C.05; NIST National Checklist Program

特定のエッジデバイス及び機器には、固有のベースラインセキュリティに関して様々なレベルの成熟度がある。デフォルトの設定で配備されると、悪意のある行為者がアクセスする可能性がある。

多くのエッジデバイスではこのセキュリティリスクを最小限に抑えるために、エッジデバイスを承認された安全な状態で構成できるようにする設定を有している。ベンダーは、ユーザーがエッジデバイスの構成を強化するのに役立つ強化ガイダンスを作成することがよくある。

エッジデバイスを設置する前に、このベンダー強化ガイダンスの適用を優先する及び／又はインターネットセキュリティセンター(CIS)のベースライン強化ガイダンスを確認すること ([CIS Center for Internet Security](#))。

侵害されたエッジデバイスを特定する

組織は、アップデートやパッチを適用する前に、特に脆弱性が積極的に悪用されていることがわかっている場合には、エッジデバイスがすでに侵害されているかどうかを評価しなければならない。

パッチは、脆弱性自体に対処するだけで、システム上の攻撃者の存在には対処するものではないため、パッチを適用しても、すでに侵害されたデバイスを修復することはできない。

パッチ適用の前後又は組織のサポートが終了した(EOL)デバイスを使用していた場合や、積極的に悪用された脆弱性に対するパッチ適用が遅れている場合には、セキュリティスタッフがこれらのデバイスの Indicators of Compromise (IoC) を徹底的に調査することが推奨される。

侵害されたデバイスに緩和策又はパッチを適用すると、一時的に実装されていたセキュリティ制御が誤って削除され、デバイスが再び脆弱になる可能性がある。このような場合、組織は、侵害の重大性と調査に利用できる資源に応じて、どの措置を講じるべきかを検討すべきである。最新のアップデートを適用するか、すでにアクセスを

取得している可能性のある敵を特定して排除するかの間で、リスクを比較検討する必要がある。

侵害が検知された場合は、さらなるガイダンスのため、ベンダー及びサイバーセキュリティ当局からの支援を求めること。オーストラリアの組織は、[ReportCyber](#) を通じてサイバー犯罪、セキュリティインシデント、不正使用を報告すべきである。あなたの報告により、犯罪活動が妨害され、オーストラリアをより安全にするのに役立つ。

現在のパッチバージョンを維持する

運用スタッフ及びサイバーセキュリティスタッフは、エッジデバイスを更新する前にセキュリティ問題が公表されるのを待つべきではない。サポートされているベンダーリリースの最新バージョンでエッジデバイスを維持することは重要である。その理由は次のとおり。

- ・ベンダーは、更新に重要なセキュリティ修正が含まれていることを常に公表するわけではない。特に、ベンダー自身のチームによって脆弱性が発見され、修正された場合はそうである。
- ・ベンダーは、サポートされている最新バージョンのソフトウェアに対して、アドバイス、緩和及びパッチを優先する。サポートされているバージョンの最新リリースを使用している組織は、パッチと、関連するガイダンスをより早く入手できる可能性がある。
- ・組織が最新のリリースを使用していない場合、パッチの適用はより困難になる可能性がある。デバイスのソフトウェアが長期間にわたって最新ではないため、中間のパッチやその他のプロセスの適用が必要になる場合や、更新中にエッジデバイスの停止時間が増加する可能性がある。

ベンダーのセキュリティアドバイザリーの情報を得られる状態にしてお

く

殆どのエッジデバイスの製造元は、脆弱性とそれに対応するパッチを詳述したセキュリティアドバイザリーをリリースしている。運用スタッフ及びサイバーセキュリティスタッフは、次のようなベンダーとの通信経路を通じて、これらのアドバイザリーに関する情報を常に入手しておくことが重要である。

- ・ベンダーのセキュリティ情報- 製造元の通知を購読
- ・RSS (Really Simple Syndication) フィード- RSS フィードは、新しいパッチが利用可能になったときに IT スタッフに通知するように設定しておくべきである。
- ・電子メールアラート- 電子メールアラートを購読して、新しいパッチが公表されたときに通知を受信する。

脆弱性が判明していて、パッチがまだ配信されていない場合、ベンダーは、通常、パッチの開発中に他の緩和策を推奨する。組織は、パッチが利用可能になるのを待つ間、こうした緩和策を実施すべきである。

自動更新を検討する

可能な場合、組織はエッジデバイスの自動更新を設定することを検討するべきである。システムに迅速にパッチが適用されない場合、侵害のリスクは重大となる。ASD は、エッジデバイスの脆弱性を数週間、数ヶ月、そして数年間も放置してしまうようなパッチが見落とされる可能性があることを観察してきた。自動アップデートを導入することで、パッチが迅速に適用され、脆弱性の開示からパッチ適用までの時間が短縮される。また、パッチを適用し忘れるというシナリオもなくなる。

しかし、自動パッチ適用には、アップデートが運用に与える影響をテストする機会がないなど、潜在的な可用性リスクが生じる。したがって、運用担当者は、ファームウェアやソフトウェアの自動アップデートを有効にすることのメリットとリスクを、事前に検討すべきである。

運用担当者、サイバーセキュリティ担当者、または調達担当者は、ベンダーに、設定のバックアップ、自動ロールバック、復元ポイントなど、ベンダーがすでに実装しているメカニズムを理解するために問い合わせるべきである。

自動更新がサポートされていない又は使用されていない場合、運用スタッフ及びサイバーセキュリティスタッフは、以下を行う必要がある。

- ・ ベンダーのセキュリティ勧告を受信し、点検し、対応することを保証する
- ・ ベンダーの更新を定期的に確認する
- ・ 必要に応じて、重要なパッチを適用するためのメンテナンスの機会をスケジュールする

実世界の例

Fortinet FortiOS の脆弱性 (CVE-2018-13379) は、パッチ適用の遅れのリスクを示している。パッチが発行されてから 2 年が経過しても、多くのデバイスが脆弱なままであった。脆弱性に対する悪意のある行為者の新たな関心は、政府部門及び商業部門の両方で重大な侵害につながった²。

緩和されていない脆弱性をスキャンする

脆弱性スキャナは、インターネットに接続されたサーバー及びインターネットに接続されたネットワークデバイスのオペレーティングシステムの脆弱性に関して、欠如しているパッチ更新を特定するために、少なくとも毎日使用される。

² On 3 April 2021, ASD released an alert reminding organisations that APT groups had been observed exploiting CVE-2018-13379. Later, in September 2021, ASD received a report of a successful exploitation of CVE-2018-13379 against an Australian entity. Despite being vulnerable for more than 2 years, the victim's device had not been patched. [ASD Cyber Threat Report 2022-2023 | Cyber.gov.au](#)

主要な枠組の管理策、出版物や規約：ISM-1701； NIST SP 800-161r1upd1, CCCS
CRG-1.1

パッチ又は更新をエッジデバイスへ適用するには、資産検出ツールや同等の機能を備えた脆弱性スキャナなどの自動資産検出方法を使用して、環境内のすべての資産を定期的に識別することが重要である。

資産の検出後、特定されたエッジデバイスは、最新の脆弱性データベースを備えた脆弱性スキャナを使用して、欠如しているパッチや更新スキャンできる。理想的には、脆弱性スキャンは自動化された方法で実行され、インターネットに接続されたネットワークデバイスに対して少なくとも毎日実行される必要がある。

サポートが終了した（EOL に達した）デバイスを管理する

サポートが終了した（EOL に達した）エッジデバイスは、ベンダーがセキュリティの更新やパッチを提供しなくなったため、特に脆弱である。組織は、EOL に達したエッジデバイスを使用すべきではない。

エッジデバイスのインベントリ（一覧）とそれぞれのサポート計画を維持すること。どのエッジデバイスが EOL の期日に近づいているかを定期的に確認し、EOL となる前にそれらを削除／交換する計画を立てる。

文書化されていない（インベントリに上がっていない）エッジデバイスがないか、ネットワークを積極的にスキャンすること。これらも EOL に達している可能性がある。直ちに EOL に達したデバイスの交換ができない場合は、

1. システムの観点からリスクを特定し、十分な情報に基づいた判断を下す。
2. リスクを低減する可能性のある代償的コントロールを探す。
3. 交換の計画／スケジュールを特定する

しかし、エッジデバイスのように脆弱なデバイスをパブリックネットワークにアクセス可能な状態にしておくリスクもあるため、製造中止となったエッジデバイスは直ちに交換することを強く推奨する。

リスクが緩和されていない EOL デバイスに依存すると、侵害のリスクが大幅に増大する。これらのリスクに関する更なるガイダンスは、[Managing the Risks of Legacy IT: Executive Guidance](#) にて参照可能である。



強力な認証を実装する

エッジデバイスを侵害する最も一般的な攻撃ベクターの1つは、デフォルトの認証情報、脆弱な認証、または不十分な ID 及びアクセスの管理を悪用することである。特に、VPN コンセントレータ等のユーザーログインを定期的にサポートするエッジデバイスでは、それが当てはまる。

悪意のある行為者がパスワードスプレー攻撃、クレデンシャル（認証）スタッフィング攻撃、情報窃取型マルウェア（[InfoStealer](#)）のようなマルウェアの使用、その他の技術により、認証を取得するかどうかにかかわらず、弱い認証は、不正アクセスへの扉を開き、ネットワーク全体を侵害する可能性がある。

一元的な認証のリスクとメリットを理解する

Active Directory などの集中型認証システムは、エッジデバイス認証が企業のプライマリアイデンティティストアにリンクされている場合又は1つの ID プロバイダ (IDP) が複数のセキュリティゾーンにわたって使用されている場合、組織の攻撃面を増大させる。エッジデバイスは、公共の場に面し、インターネットからアクセス可能であることからリスクが高いと考えられている。従って、組織のコーポレート AD フォレスト又は同等の認証 (authentication)、認可 (authorization) 及びアカウンティング (accounting) (AAA) ソリューションからエッジデバイスを分離することが重要である。

例えば、Golden Ticket [[T1558. 001](#)] と SID History を組み合わせることによって、悪意のある行為者は、チケット認可チケット (TGT) を偽造して、同じフォレスト内の他のドメインにアクセスできる。フォレスト間の信頼が存在する場合は、他のフォレストにもアクセスできる。詳細については、ASD の「Active Directory の侵害の検出と緩和（[Detecting and mitigating Active Directory compromises](#)）」を参照のこと。

ASD は、エッジデバイス認証を不正利用する [APT40](#) や [Volt Typhoon](#) などの高度な持続的脅威 (APTs) を観察した。これらの悪意のある行為者は、エッジデバイスが企業のプライマリアイデンティティストアを使用している又はリンクしている集中型認証システムを不正利用することによって、横展開と認証情報のダンプを行っている。このシナリオについて具体的に観察されることの1つは、コーポレートディレクトリに対してライトウェイト・ディレクトリ・アクセス・プロトコル (LDAP) を使用して検索が可能なエッジデバイス上のサービスアカウントである。

これらのリスクは一般的であるが、集中型認証システムは、きめ細かなアクセス制御、デバイス管理プレーンの分離、集中型認証サービスの堅固な強化など、様々なセキュリティ上の利点も提供する。これらの対策は、横展開リスクを制限するとともに、個人の責任追跡性、同期されたアカウント失効、効率的な認証管理、ログ記録、異常検出等の利点を提供することができる。

組織は、当該リスクを効果的に管理するために、集中型認証について、弱みとセキュリティ上の強みの両方を考慮し、それに応じてアプローチを調整するべきである。

Active Directory を超える代替の AAA ソリューションは、特定の脆弱性に対処しながら、同様の利点を提供する可能性がある。集中型 AAA の構成を安全にするための詳細なアプローチについては、米国家安全保障局（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（[Network Infrastructure Security Guide](#)）を参照のこと。

ローカル認証情報を保護する

ローカルアカウントを使用するエッジデバイスは、特権アクセス管理 (PAM) システム又は認証情報の管理サービスを使用して管理する必要がある。これらのソリューションでは、シナリオに応じ、使用した度に認証情報を循環させることができるため、認証が長期にわたって露見されるリスクを軽減できる。

多要素認証 (MFA) により認証を強固にする

システムのユーザーを認証するために使用される多要素認証は、フィッシングに対して耐性がある。

主要な枠組の管理策1、出版物や規約: ISM-1682; CISA CPG 2.H, CCCS CRG-2.7

VPN ゲートウェイのシナリオのように、エッジデバイスがインターネットに公開されたログイン・インターフェイスを持つ必要がある場合、フィッシングに対して耐性のある多要素認証 (MFA) を有効にすることは、様々なセキュリティ枠組みとベストプラクティス全体にわたる重要な管理策である。可能であれば、フィッシングに対して耐性のある MFA を実装することで、クレデンシャルスタッフィング攻撃や総当たり攻撃に対する強力な保護を提供し、他のパスワード再利用による不正利用を現実的な手段ではないようにする。

MFA がサポートされていない場合は、適切な単一要素認証を使用する

システムが多要素認証をサポートできない場合は、代わりにパスフレーズを使用した単一要素認証が実装される。

主要な枠組の管理策1、出版物や規約: ISM-1682; CISA CPG 2.H, CCCS CRG-2.7

フィッシングに耐性のある MFA がデバイスでサポートされていない場合は、単一要素認証は、現地のサイバーセキュリティ当局からの最新のパスワード又はパスフレーズの複雑さと長さに関するアドバイスに基づき、実現されるべきである。

オーストラリアの組織では、単一要素認証に使用されるパスフレーズは、少なくとも 4 つのランダムな単語で、合計の最小長は 15 文字である必要がある（組織に対してより厳しい要件が適用される場合を除く）。システムがパスフレーズをサポートしていない場合は、絶対的な最後の手段として、システムでサポートされている最も強力なパスワードの長さと複雑さを実装する必要がある。

認証情報は、決して再利用してはならない。

パスワードの保存に強力な保護を適用する

システムに保存された認証は、パスワードマネージャ、ハードウェアセキュリティモジュール、又はデータベース内への保存前のソルト、ハッシュ及びストレッチングにより保護される。

主要な枠組の管理策, 出版物や規約: ISM-1402; CCCS CRG-2.10

エッジデバイスに認証情報を保存する場合、認証情報の窃取から守るため、安全なハッシュ・アルゴリズムを使用することが重要である。パスワード保存アルゴリズムが、ブルートフォース攻撃に対して脆弱でないことを確保するには、次のようなアルゴリズムを回避すること。

- ・ MD5 のような古くて安全性の低いアルゴリズムを使用する
- ・ ハッシュ関数の反復回数を 1 回又は少ない回数とする
- ・ 暗号化ハッシュ関数ではなく、カスタムなエンコーディングでパスワードを保存するという、過去使われていた方法を使用する



不要な機能とポートを無効にする

最新のエッジデバイスで利用可能な機能の多くはオプションであり、しばしば、組織によって使用されていない機能であるが、既定で有効になっている。監査を実行し、組織によって使用されていない機能を無効にすると、デバイスの攻撃面が減少する。

一般的に、公開されるサービスには、次のようなものがある。

- ・ VPN インターフェイス: 多くのセキュリティ関連のエッジデバイスには VPN 機能があり、既定で VPN サービスを提供する。VPN 機能が使用されていない場合は、サービスを無効にして、インターネットから当該サービスをブロックすること。
- ・ アプリケーション・プログラミング・インタフェース (API): 多くのエッジデバイスでは、既定で有効になっている API がある。これらが使用されておらず、可能な場合は、API を無効にすること。
- ・ 簡易ネットワーク管理プロトコル (SNMP): SNMP がモニタリングに必要な場合は、SNMPv3 を設定し、承認されたエンドポイントからの SNMP のみを許可し、他のバージョンのプロトコルを無効にする。SNMPv3 は、古いバージョンに対する不正利用から保護するため、暗号化と強力な認証をサポートしている。
- ・ デバイス管理インターフェイス: 多くのエッジデバイスでは、デバイス管理用のインターフェイスが既定で開いている場合がある。これらのインターフェイスは、デバイスを構成している間、適切なアクセス管理の背後に配置する必要がある。これらのインターフェイス、特に Web で実装されている場合は、インターネットからブロックされるべきである。
- ・ インターネットプロトコル・バージョン: 組織は、インターネットプロトコルの 1 つのバージョンを排他的に使用すべきである。使用されていないバージョンを無効にすることは、攻撃対象領域を最小限に抑え、使用されているバージョンが悪意のあるアクターによって悪用されないようにするのに役立つ。

未使用のポートを閉じる

ネットワークデバイス上の未使用の物理ポートは無効であること。

主要な枠組の管理策, 出版物や規約: ISM-0534; NZISM-22.3.11.C.01; CISACPG 2.B; NIST SP 800-53, Rev. 5, CCCSCRG-2.17

エッジデバイスには、様々なサービスをサポートする複数のオープンポートが付属していることが多く、組織の環境には必要ない場合がある。オープンポートの数を減らすことで、デバイスが潜在的な脅威にさらされる可能性を最小限に抑えることができる。

エッジデバイスで開いているポートを定期的に監査して、必要なサービスのみが有効になっていることを確認する。アクティブに使用されていないポート又はサービスは無効にすること。



管理インターフェイスを安全にする

エッジデバイス上の管理インターフェイスとサービスを安全にすることは、悪意のある行為者が悪用できる攻撃面を最小限にするために重要である。

アクセス制御リストを適用する

承認されていないネットワークデバイスその他の IT 機器との接続を防止するために、ネットワークアクセス制御がネットワークに実装されていること。

主要な枠組の管理策、出版物や規約： ISM-0520; NZISM-18.1.13.C.01; CISACPG 2.B; NIST CSF; NIST SP 800-53, Rev. 5

エッジデバイスにネットワークアクセス制御リスト (ACL) を実装すると、特定のポート及びサービスと通信できるユーザーを制限するのに役立つ。ACL は、エッジデバイスの管理インターフェイスにアクセスできる IP アドレス又はネットワークに関する厳密な管理を提供する。

専用の管理インターフェイスを使用する

可能な限り、エッジデバイスは、プライマリデータインターフェイスから分離された専用の管理インターフェイスを使用するように装備されるべきである。管理トラフィックを通常のネットワークトラフィックから分離する (コントロールプレーンをデータプレーンから分離するともいう) ことで、機密性の高い管理機能の露出が減少し、権限を与えられた運用スタッフとサイバーセキュリティスタッフだけがこれらの重要なインターフェイスにアクセスできるようになる。

管理インターフェイスをインターネットに公開しない

IT 設備のネットワーク管理インターフェイスは、インターネットに直接公開されないこと。

主要な枠組の管理策、出版物や規約： ISM-1863; CCCS CRG-2.21, [CISA Binding Operational Directive \(BOD\) 23-02: Implementation Guidance for Mitigating the Risk from Internet - Exposed Management Interfaces](#)

管理インターフェイスには、telnet、簡易ネットワーク管理プロトコル (SNMP)、セキュアシェル (SSH)、Web ベースの管理インターフェイス (標準及び非標準ポート) 及び既存の Web インターフェイスのアプリケーションプログラミングインターフェイス (API) エンドポイントなどのサービスが含まれる。

ベンダーのセキュリティ構成に関するアドバイスでは、当該様々な管理インターフェイスとそれぞれに推奨される構成オプションについて説明がなされるべきである。

管理インターフェイスは、インターネットに公開されるように設計されていない。これは、インターネットに接続するように構築されたインターフェイスと比較して、管理インターフェイスにおいて重大な脆弱性が発生する頻度が高いことから明らか

である。これらの管理インターフェイスがインターネットに公開されないようにすることが不可欠である。

実世界の例

脅威グループ [BackdoorDiplomacy](#) は、F5 BIG-IP の脆弱性である [CVE-2020-5902](#) を不正利用して、公開された管理インターフェイスに Linux バックドアを仕込んだ。これは、公共に面している機器 [\[T1190\]](#) を不正利用する例です。

攻撃対象範囲は、管理インターフェイスを 1 つの管理ネットワークに集約することによっても広がる。この攻撃対象範囲は、プライベート仮想 LAN(VLAN)を実装し、悪意のある行為者の横展開を防止することによって縮小できる。この管理トラフィックは、適切に設定された ACL を使用してファイアウォールで終了する必要がある。

ネットワークのセグメント化を検討する

ネットワークのセグメント化は、ネットワークを安全にするための重要な実行である。組織は、ネットワークをより小さく分離したセグメントに分割することで、トラフィックの流れを制御し、機密データへのアクセスを制限し、侵害時の横展開の可能性を制限できる。

十分なフィルタリングルールを使用したセグメント化は、攻撃対象範囲を縮小し、違反を封じ込め、悪意のある活動を検出する可能性を高め、悪意のある行為者が特権をエスカレートさせて横展開することを困難にする。

このセグメンテーションを作るために、レイヤー 4（トランスポート層）ファイアウォールなどのエッジデバイスが使われることがある。そのほかの状況では、エッジデバイスは電子メールセキュリティゲートウェイのようにレイヤー 7（アプリケーション層）の機能を実行する場合もある。最新のファイアウォールのような、収斂型のエッジデバイスは、特に小規模な環境では、両方の機能を実行する場合がある。例えば、1 つの収斂型のセキュリティエッジデバイスは、ほとんどのネットワークトラフィックに対してレイヤー 4 ゲートウェイとして動作するが、VPN 及び電子メールサービスに対してレイヤー 7 ゲートウェイとしても動作する。

エッジデバイスが使用される展開シナリオは多岐にわたり、エッジデバイスのタイプ、機能とも多種多様であるため、それぞれの事例に対して簡潔なアドバイスを提供することは困難である。

ネットワークセグメント化の構成をめぐる安全なアーキテクチャと設計を理解するためのさらなる情報源については、ACSC の次のガイダンスを参照のこと。

- ・ [Guidelines for Networking](#)
- ・ [Gateway Security Guidance Package: Gateway Security Principles](#)
- ・ [Managing the Risks of Legacy IT: Practitioner Guidance](#)

脅威検出のための監視を一元化する

エッジデバイス上の潜在的な脅威を検出するには、効果的なログ記録と監視が極めて重要である。ログ収集を一元化することで、より効率的な分析と脅威の検出が可能になり、悪意のある行為者が検出につながる可能性のあるログを削除するプロセスを複雑にする。

リアルタイムでログ記録を一元化する

エッジデバイスからのログイベントは、集中型システムにリアルタイムで送信されるべきである。ログの転送に必要なデータのみが送信されるように、エッジデバイスからログ収集ポイントへのアクセスを制限されるよう、別のファイアウォールなど、エッジデバイスに依存しない制御が用いられるべきである。

イベントログの保存と完全性を安全にする

集中型イベントロギングファシリティが実装されること。イベントログは、発生した後できるだけ早くファシリティに送信されること。

主要な枠組の管理策、出版物や規約: ISM-1405; NZISM-16.6.12.C.03; CISA CPG 2.U, CCCS CRG-2.16

ログは、転送中及び保存中の両方で保護され、承認されていないアクセス、変更又は削除から保護されることを確保しなければならない。イベントログは、承認されたユーザーによるアクセス及び分析を可能にするために、データレイクやSIEMシステムなどの一元化された設備に保存されるべきである。

ログ・アグリゲータ及びログ・パーサーは、入力検証を使用すべきである。エッジデバイスのログ記録で考慮すべき重要な管理策は、エッジデバイスがログの変更又は削除を許可するアクセスを有するべきではないということである。これは、悪意のある行為者が搾取の証拠を改ざんすることを防ぐ。

イベントログと脅威検出のより包括的な詳細については、共同署名がなされた「[イベントログと脅威検知のためのベストプラクティス](#)」を参照のこと。

予期されるイベントのプロファイルを作成する

インターネットとエッジデバイスとの間、加えて、エッジデバイスと他の内部システムとの間の通常の活動がどのように見えるかについての基本的な理解を有しておくことが重要である。

エッジデバイス上の一定の活動は、リスクが高いと考えられており、できるだけ早く調査する必要がある。たとえば、予期しない活動が含まれる場合がある。

- ・ 設定の変更
- ・ 再起動
- ・ ACL の変更
- ・ パスワードの変更

- ・ トンネル/トラフィック転送
- ・ 送信接続(Web、ファイル転送プロトコル)
- ・ インターネットへの大量のデータ転送
- ・ シリアル化エラー

エッジデバイスと内部ネットワークとの間の特定の相互作用についても、直ちに調査すべきである。例えば、以下のとおり

- ・ エッジデバイスが内部のネットワーク認証(例えば、エッジデバイスがLDAP 検索を実行できるようにするためのAD アカウント)を使用して設定された場合。このアカウントは、通信するように設定されたホスト以外のホストにアクセスした場合にアラートを発するべきである。
- ・ エッジデバイスが通常通信しないホストに向けられたネットワークトラフィック
さらに、ファイアウォールのルール集のいずれかのルールに違反するネットワークトラフィックのイベントログとアラートを生成することは、ファイアウォールの障害又はファイアウォールの設定変更が原因でネットワークに入りこんでくる疑わしいトラフィックや悪意のあるトラフィックを識別するのに役立つ。

いかなる侵害についても当局を関与させる

不規則で疑わしい活動が発見された場合、セキュリティスタッフは、ベンダー及びサイバーセキュリティ当局に積極的に報告すべきである(オーストラリアの組織の場合には、ASD が該当。[Report and recover/Cyber.gov.au](https://www.cyber.gov.au/report-and-recover))。ASD は、組織が悪意のある行動を理解したり、ゼロデイ脆弱性を捕捉したりすることを支援することができる。

これらの活動の特定は、組織にネットワークオペレーションセンター(NOC)又はセキュリティオペレーションセンター(SOC)がある場合、検出エンジニアリングシナリオとして優先されるべきである。これらの脅威モデル化は、使用された戦術、技術及び手順(TTPs)を特定するために何を分析すべきかをチームが発見するのに役立つ可能性がある。

結論

エッジデバイスは、内部ネットワークとインターネットとの間の極めて重要な接点として機能するが、トラフィックを管理し、セキュリティポリシーを実施する上で重要な役割を果たすことから、ますます悪意のある行為者の標的になっている。組織がデジタルインフラストラクチャを拡張するのに伴い、これらのデバイスのセキュリティを最優先事項としなければならない。このガイドにおける戦略は、エッジデバイス及びエッジデバイスと相互に作用しているネットワークの全体にわたる強靭性を構築することを目的とした実行集である。

その他のガイダンス

ASD のリソース

- Mitigation strategies for edge devices: executive guidance
- Identifying Cyber Supply Chain Risks
- Choosing secure and verifiable technologies
- Cyber Supply Chain Risk Management
- Gateway hardening package
- Secure your Wi-Fi and router
- Identifying and Mitigating Living Off the Land Techniques
- Cybersecurity Best Practices for Smart Cities
- Guidelines for System Hardening
- Managing the Risks of Legacy IT: Practitioner Guidance
- Best practices for event logging and threat detection
- Network hardening
- Implementing Network Segmentation and Segregation

米国の CISA のリソース

- Cybersecurity Performance Goals (CPGs)
- Secure by Design Alert: Security Design Improvements for SOHO Device Manufacturers
- Secure-by-Design
- Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem
- Securing Network Infrastructure Devices
- Zero Trust Maturity Model
- Layering Network Security Through Segmentation Infographic

- Trusted Internet Connections (TIC)
- Understanding Patches and Software Updates
- CISA Binding Operational Directive (BOD) 23-02: Implementation Guidance for Mitigating the
- Risk from Internet-Exposed Management Interfaces

NIST のリソース

- Cybersecurity Framework (CSF)
- SP 800-53, Rev. 5
- SP 800-161r1upd1
- National Checklist Program

カナダ CCCS のリソース

CCCS は、可能な限り、組織が CSE の IT セキュリティ対策のトップ 10 に従って「インターネットゲートウェイの統合、監視、および保護」に努めることを推奨している

- Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089)

日本経済産業省のリソース

Japan Cyber STAR (JC-STAR) : セキュリティ要件適合評価及びラベリング制度は、日本のラベリングスキームであり、独自の基準に基づいて IoT 製品が適合要件（セキュリティ技術要件）に適合していることを確認します。また、ETSI EN 303 645 や NISTIR 8425 などの国内および国際基準と調和しています。

詳細については、[Japan Cyber STAR \(JC-STAR\) | IPA, METI](#) をご覧ください。