サイバーセキュリティ

デバイスのライフサイクル管理

サイバーセキュリティのリスクは、生産から廃棄まで、ネットワークデバイスのライフサイクルのあらゆる段階に存在します。これらのリスクを見過ごすと、業務上の混乱や、データの機密性、完全性、可用性の喪失につながることがあります。そのため、サプライヤーからエンドユーザーに至るまで、すべてのステークホルダーが責任を持ってリスク管理を行うことが極めて重要です。

したがって、デバイスのセキュリティライフサイクルを考慮することが調達において重要です。メーカーは、製品が顧客に届く前、製品が使用されている間、および製品が廃棄されるときの、サイバーセキュリティのリスクを低減する対策を講じる必要があります。

以下のページでは、Axisデバイスのライフサイクルを通してリスクを軽減するためにAxisがサポートするテクノロジー、ツール、ガイダンス、取り組み、プロセスなどについてご紹介します。

セキュリティの基盤: Axis Edge Vault、AXIS OS、Axisセキュリティ開発モデル


生産


物流


実装


使用中


廃棄

セキュリティの基盤 - ハードウェア、ソフトウェア、取り組み

製品の完全性を保護し、最初から脆弱性のリスクを軽減します

Axis Edge Vaultサイバーセキュリティプラットフォーム
このハードウェアベースのプラットフォームは、デバイスのIDと完全性を不正アクセスから保護する機能をサポートしているため、デバイスを安全に起動し、統合して、キーなどの機密データを確実に保護することができます。

オペレーティングシステム、AXIS OS
AXIS OSは、Axisのさまざまなデバイスに対応します。AXIS OSは、脆弱性管理における業界のベストプラクティスを取り入れており、多数の製品にわたりソフトウェアセキュリティ機能とパッチを迅速かつ効率的にリリースするためのプラットフォームを提供します。

Axisセキュリティ開発モデル (ASDM)
ASDMは、ソフトウェアの脆弱性を持つ製品がリリースされるリスクを低減するために、Axisで適用されている方法論です。リスク評価、脅威モデリング、コードの分析、侵入テスト、バグバウンティプログラム、脆弱性のスキャンと管理などが含まれ、ソフトウェア開発にセキュリティへの配慮が確実に組み込まれるよう保証します。

透明性
透明性は、信頼を構築するためのAxisのビジネスの推進方法の重要な要素です。Axisは、共通脆弱性識別子 (CVE) 採番機関です。お客様が適切な措置を講じられるよう、脆弱性について公開し、ステークホルダーに通知しています。また、AXIS OSのソフトウェア部品構成表 (SBOM) を公開しています。

生産と物流

コンポーネントが侵害されるリスクの軽減

- **サプライチェーン:** 重要なコンポーネントは、戦略的サプライヤーから直接調達されます。Axisは製造パートナーと緊密に連携しています。生産工程を監視し、Axisと24時間365日データを共有することで、リアルタイムの分析と透明性を実現します。
- Axis Edge Vault: 生産時にAxisデバイスにインストールされるAxis Edge Vaultには、次の機能が含まれます。
  - **セキュアキーストア。**暗号計算モジュール (セキュアエレメント、Trusted Platform Module、Trusted Execution Environment) により、キーの不正な保管を防止します。
  - **署名付きファームウェア。**インストールしたAXIS OSがAxisの正規品であることを保証します。これにより、デバイスにダウンロード/インストールされる新しいファームウェアも、Axisによって署名されます。
  - **セキュアブート。**デバイスがファームウェアにAxisの署名があることを確認できるようにします。不正なファームウェアや改ざんされたファームウェアを検出すると、起動プロセスが中止され、デバイスの動作が停止します。署名付きファームウェア、セキュアブート、デバイスの工場出荷時状態への初期化を組み合わせることで、デバイスの出荷時における悪意のある改ざんから保護することができます。
  - **Axisデバイス**ID。Axisデバイスの真正性を証明できる、対応キーを備えたデバイス固有の証明書です。IEEE 802.1AR規格に基づくAxisデバイスIDは、ネットワーク上での安全なデバイスの識別とオンボーディングを可能にします。
  - **暗号化されたファイルシステム。**システムインテグレーターからエンドユーザーへの輸送中など、デバイスが使用されていない間に、ファイルシステムに保存されている顧客固有の設定や情報が抜き取られたり改ざんされたりしないように保護します。

実装

不正アクセス、機密データの抜き取り、ネットワークエンドポイント間での改ざんデータの転送につながる可能性のある、侵害された、または適切に強化されていない製品がネットワーク上に設置されるリスクに対処します。

> **工場出荷時状態への初期化:** デバイスを設定する前に、工場出荷時状態への初期化を実行します。これにより、AXIS OSとそのデフォルト設定のみが残り、不要なソフトウェアや設定が完全に削除されていることを保証できます。

> **デバイスの最新ファームウェアの確認:** 生産から実装までに時間が経っている場合があるため、AxisのWebサイトで特定のデバイスに対する最新のバグ修正を含む最新のファームウェアを確認することをお薦めします。

> **AxisデバイスID:** Axisの正規デバイスのみをネットワークに実装するため、IEEE 802.1X認証を使用して、またはHTTPSプロトコルを介して安全なネットワーク接続を確立するときにAxisデバイスIDを確認することができます。IEEE 802.1Xネットワークでは、AxisデバイスIDを使用してセキュリティを強化し、導入時間を短縮することができます。

> **セキュアキーストア:** 暗号化計算モジュールを使用するセキュアキーストアは、AxisデバイスIDや顧客がロードしたキーなどの機密情報を保持し、デバイスが侵害された場合でも、不正アクセスや機密情報の悪意のある抜き取りを防止します。

> **暗号化されたファイルシステム:** デバイスが使用されていないときに、ファイルシステムに保存されているデータが抜き取られたり、改ざんされたりすることを防ぎます。

> **強化ガイド (Hardening Guide):** AxisのWebサイトのAXIS OSポータルから入手できるAXIS OS強化ガイドは、一般的な脅威に対処するための基本的な設定を定め、ベストプラクティスと技術的アドバイスを提供します。また、ビデオ管理ソフトウェアのAXIS Camera StationやAxisネットワークスイッチの強化ガイドもあります。

> **AXIS OSセキュリティスキャナーガイド:** Axisでは、Axisデバイスのセキュリティスキャンを実行して、脆弱性や脆弱な設定の影響を受けていないかどうかを確認することをお薦めしています。AXIS OSセキュリティスキャナーガイドでは、スキャナーからの特定の通知を解決する方法に関する推奨事項と、一般的な「誤検出」の概要について説明しています。

> **AXIS Device Manager:** このツールは、Axisデバイスをローカルで効率的に設定・管理できるようにします。デバイスの認証情報の管理、証明書の展開、使用されていないサービスの無効化、AXIS OSのアップグレードなど、インストールおよびセキュリティタスクのバッチ処理を可能にします。


生産


物流


実装


使用中


廃棄

使用中

既知の脆弱性を持つファームウェアの実行、認証されていないファームウェアによるデバイスの更新、安全な設定の未更新によるリスクに対処します

> **ファームウェアのアップグレード:** AXIS OSのアクティブトラックまたは長期サポート (LTS) トラックのいずれかを使用してファームウェアを最新の状態に保ち、Axisデバイスのサイバーセキュリティを維持することが重要です。無償で提供されるいずれかのトラックを使用したファームウェアの更新には、セキュリティパッチが含まれます。署名付きファームウェアは、Axisの正規ファームウェアのみをインストールできるようにします。

> **AXIS Device Manager Extend:** AXIS Device Managerを補完するこのツールは、Axisデバイスのリモート管理を可能にし、デバイスのファームウェアのアップグレードなど、メンテナンス作業の拡張を簡素化します。

> **脆弱性管理:** Axisでは、登録された方に脆弱性などのセキュリティに関する情報を配信するセキュリティ通知サービスを提供しています。

> **AXIS OSフォレンジックガイド:** このガイドは、Axisデバイスが設置されている周辺ネットワークやITインフラに対するサイバーセキュリティ攻撃が発生した場合に、Axisデバイスのフォレンジック分析を行う方に向けた技術的アドバイスを提供します。

> **署名付きビデオ:** 対応カメラでこの機能を有効にすると、ビデオストリームがデバイスから送信される前にビデオに暗号署名が追加され、視聴者はビデオが改ざんされていないかどうかを確認することができます。これは、捜査や起訴において特に重要です。

廃棄

サポートが終了し、パッチが適用されていない既知の脆弱性を持つデバイスのリスクや、廃棄後にデバイスに機密データが残るリスクに対処します

> **ファームウェアのサポート終了日:** Axis.com上の多くの製品のサポートWebページには、特定の製品のファームウェアのサポート終了日が記載されており、お客様は製品の廃止や交換を適時に計画することができます。

> **AXIS Device Manager Extend:** 製品の製造・販売中止やサポート終了に関する情報など、システム内のすべてのデバイスの保証状況を簡単に把握することができます。この情報により、デバイスの廃止に備え、サポートされていないデバイスがもたらすリスクを排除することができます。

> **ガイダンス:** AxisのWebサイトのAXIS OSポータルでは、Axisデバイスの廃止に関するガイダンスを提供しています。デバイスを工場出荷時状態に初期化することで、すべての設定とデータが消去されます。

詳しくは、こちらのサイトをご覧ください: www.axis.com/ja-jp/about-axis/cybersecurity