AXIS OSハードニングガイド

AXIS OSポータル | AXIS OSリリースノート | AXIS OS知識ベース| AXIS OS YouTubeプレイリスト | セキュリティアドバイザリ

はじめに

Axis Communicationsは、装置の設計、開発、試験に対してサイバーセキュリティ対策を講じて、ハッカーが攻撃に悪用する可能性のある欠陥のリスクを最小限に抑えるよう努めています。ただし、ネットワークやその装置、そしてネットワークがサポートするサービスを保護するには、ベンダーのサプライチェーン全体とエンドユーザー組織が連携する必要があります。環境が安全かどうかは、ユーザー、プロセス、テクノロジーによって決まります。このガイドは、ネットワーク、装置、サービスをセキュアに保つのに役立つように作成されています。

Axis装置に対する最も明白な脅威は、物理的な妨害行為、破壊行為、改ざんです。これらの脅威から製品を保護するには、耐衝撃モデルまたはケーシングを選択し、推奨される方法で取り付けて、ケーブルを保護することが重要です。

Axis装置は、コンピューターや携帯電話と同様、ネットワークエンドポイントです。これらの装置の多くは、接続されているシステムに脆弱性を露呈する可能性のあるWebインターフェースを備えています。このガイドでは、このようなリスクを軽減する方法について説明します。

また、Axisソリューションの導入に携わるすべての人に技術的なアドバイスを提供します。たとえば、推奨される基本設定だけでなく、進化する脅威の状況を考慮した強化ガイドも示します。具体的な設定方法については、必要に応じて製品のユーザーマニュアルを参照してください。AXIS OS 7.10および10.9で、Axis装置のWebインターフェースが更新され、設定パスが変更されています。

Webインターフェースの設定

本ガイドでは、AxisデバイスのWebインターフェースにおけるデバイス設定の構成について説明します。設定パスは、装置にインストールされているAXIS OSのバージョンによって異なります。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション)] > [Security (セキュリティ)] > [IEEE 802.1X]
7.10より前	[Settings (設定)] > [System (システム)] > [Security (セキュリティ)]
≥ 10.9	[System (システム)] > [Security (セキュリティ)]

対象

このガイドは、AXIS OS (LTSまたはアクティブトラック) を実行しているすべてのAXIS OSベースの製品、および4.xxと5.xxを実行しているレガシー製品に適用されます。

CIS保護レベル

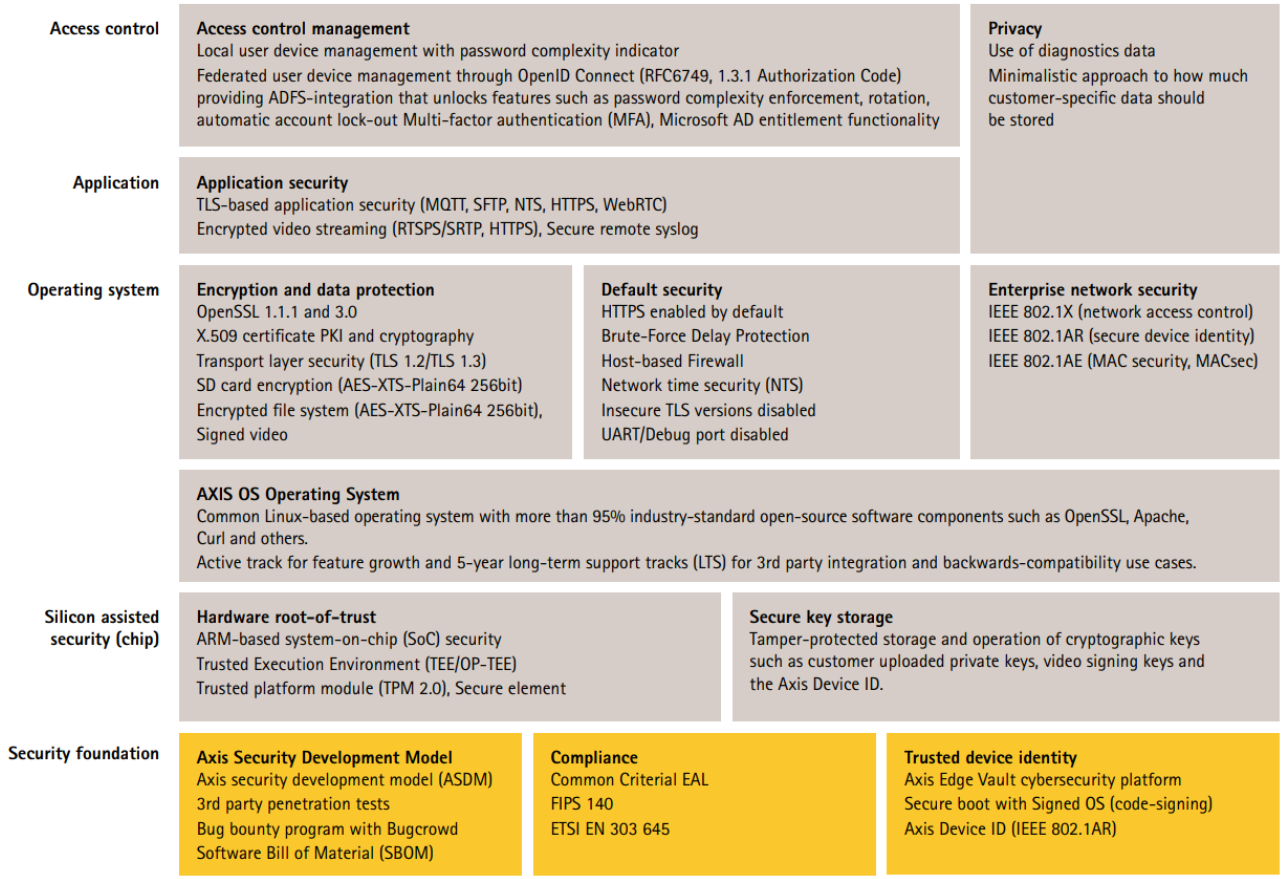
Axisは、Center for Internet Safety (CIS) Controls Version 8で概説されている方法に従って、サイバーセキュリティフレームワークの推奨事項を作成しています。CIS Controlsは、以前はSANS Top 20 Critical Security Controlsと呼ばれていたもので、組織内で最も一般的なサイバーセキュリティリスクのカテゴリに対処することに焦点を当てた、18カテゴリのCritical Security Controls (CSC) を提供しています。

このガイドでは、各強化トピックにCSC番号 (**CSC#**) を付けることで、重要なCritical Security Controlを参照できるようにしています。CSCカテゴリの詳細については、「*18カテゴリのCritical Security Control セキュリティコントロール*」を参照してください。

デフォルトの保護

Axis装置には、デフォルトの保護設定が付属しています。設定する必要のない Security Control がいくつかあります。これらのコントロールは、基本レベルの装置保護を提供し、より広範な強化の基盤として機能します。

AXIS OSセキュリティアーキテクチャー図には、さまざまなレイヤーにわたるAXIS OSサイバーセキュリティ機能の概要が示されています。この図により、セキュリティ基盤、シリコンに支えられたセキュリティ、AXIS OSオペレーティングシステム、アプリケーション、アクセスコントロールレイヤーの包括的な概要を把握することができます。



画像を右クリックして新しいタブで開くと、より見やすくなります。

認証

デフォルトで無効

CSC #4：企業の資産とソフトウェアのセキュアな設定

管理者パスワードが設定されるまで、Axis装置は動作しません。

管理者パスワードを設定した後は、有効なユーザー名とパスワードの認証情報の認証を介してのみ、管理者機能やビデオストリームにアクセスできます。匿名表示や常時マルチキャストモードなど、認証されていないアクセスを可能にする機能を使用することはお勧めしません。

デバイスアクセスの設定方法については、AXIS OS knowledge base (AXIS OS知識ベース) で「デバイスアクセス」を参照してください。

ダイジェスト認証

CSC #3：データ保護

装置にアクセスするクライアントは、ネットワーク経由で送信するときに暗号化する必要があるパスワードを使用して認証されます。したがって、基本認証の代わりにダイジェスト認証のみを使用するか、基本認証とダイジェスト認証の両方を使用することをお勧めします。これにより、ネットワークスニッファーがパスワードを入手するリスクを軽減できます。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション)] > [Advanced (詳細)] > [Plain Config (プレーン設定)] > [Network (ネットワーク)] > [Network HTTP Authentication policy (ネットワークHTTP認証ポリシー)]
7.10より前	[Settings (設定)] > [System (システム)] > [Plain config (プレーン設定)] > [Network (ネットワーク)] > [Network HTTP Authentication policy (ネットワークHTTP認証ポリシー)]
≥ 10.9	[System (システム)] > [Plain config (プレーン設定)] > [Network (ネットワーク)] > [Network HTTP Authentication policy (ネットワークHTTP認証ポリシー)]

ONVIF再生攻撃からの保護

CSC #3：データ保護

再生攻撃からの保護は、Axis装置でデフォルトで有効になっている標準のセキュリティ機能です。その目的は、UsernameToken、有効なタイムスタンプ、nonce、パスワードダイジェストを含む追加のセキュリティヘッダーを追加することで、ONVIFベースのユーザー認証を十分に保護することです。パスワードダイジェストは、パスワード (システムにすでに保存されている)、nonce、タイムスタンプから計算されます。パスワードダイジェストの目的は、ユーザーを検証し、再生攻撃を防ぐことです。そのため、ダイジェストがキャッシュされます。この設定を有効にしておくことをお勧めします。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション)] > [Advanced (詳細設定)] > [Plain Config (プレーン設定)] > [System (システム)] > [Enable Replay Attack Protection (再生攻撃からの保護を有効にする)]
7.10より前	[Settings (設定)] > [System (システム)] > [Plain Config (プレーン設定)] > [WebService (Webサービス)] > [Enable Replay Attack Protection (再生攻撃からの保護を有効にする)]
≥ 10.9	[System (システム)] > [Plain Config (プレーン設定)] > [WebService (Webサービス)] > [Enable Replay Attack Protection (再生攻撃からの保護を有効にする)]

ブルートフォース攻撃を防ぐ

CSC #4：企業の資産とソフトウェアのセキュアな設定
CSC #13：ネットワークの監視と防御

Axis装置には、パスワード推測などのネットワークからの総当たり攻撃を識別してブロックする防止メカニズムが備わっています。この機能は総当たり攻撃による遅延からの保護と呼ばれ、AXIS OS 7.30以降で使用できます。

総当たり攻撃に起因する遅延対策として、AXIS OS 11.5以降ではこれがデフォルトで有効化されています。詳細な設定例と推奨事項については、AXIS OS Knowledge Base（AXIS OS知識ベース）に含まれている「*総当たり攻撃による遅延からの保護*」を参照してください。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	N/A
7.10より前	[Settings (設定)] > [System (システム)] > [Plain config (プレーン設定)] > [System (システム)] > [PreventDos Attack (DoS攻撃の防止)]
≥ 10.9	[System (システム)] > [Security (セキュリティ)] > [Prevent brute-force attacks (総当たり攻撃の防止)]

エッジストレージ

CSC #4：企業の資産とソフトウェアのセキュアな設定

CSC #3：データ保護

AXIS OS 12.0以降、マウントされたネットワーク共有に対するデフォルトオプションとしてnoexec (実行不可) マウントオプションが追加されました。これにより、マウントされたネットワーク共有からのバイナリの直接実行が無効化されます。SDカードには、古いAXIS OSバージョンから、すでにこのオプションが追加されています。

さらに、AXIS OS 10.10以降のバージョンのAxisデバイスは、エッジ録画の暗号化されたエクスポートをサポートしています。権限のない個人がエクスポートされたビデオ素材を再生できないようにするため、この機能を使用することをお勧めします。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	N/A
7.10より前	N/A
≥ 10.9	録画

ネットワークセキュリティ

ネットワークプロトコル

CSC #4：企業の資産とソフトウェアのセキュアな設定

Axis装置では、デフォルトで最小限のネットワークプロトコルとサービスのみが有効になります。この表では、それらがどれであるかを確認できます。

プロトコル	ポート	交通	コメント
HTTP	80	TCP	Webインターフェースアクセス、VAPIXおよびONVIF APIインターフェース、エッジツーエッジ通信などの一般的なHTTPトラフィック。*
HTTPS	443	TCP	Webインターフェースアクセス、VAPIXおよびONVIF APIインターフェース、エッジツーエッジ通信などの一般的なHTTPSトラフィック。*
RTSP	554	TCP	Axis装置によってビデオ/音声ストリーミングに使用。
RTP	エフェメラルポート範囲**	UDP	Axis装置によってビデオ/音声ストリーミングに使用。
UPnP	49152	TCP	UPnP検出プロトコル経由でAxis装置を検出するためにサードパーティ製のアプリケーションによって使用。**注：** AXIS OS 12以降、デフォルトで無効化されています。0.
Bonjour	5353	UDP	mDNS検出プロトコル(Bonjour) 経由でAxis装置を検出するためにサードパーティ製のアプリケーションによって使用。
SSDP	1900	UDP	SSDP (UPnP) 経由でAxis装置を検出するためにサードパーティ製のアプリケーションによって使用。**注：** AXIS OS 12以降、デフォルトで無効化されています。0.
WS-Discovery***	3702	UDP	WS-Discoveryプロトコル (ONVIF) 経由でAxis装置を検出するためにサードパーティ製のアプリケーションによって使用。

* エッジツーエッジの詳細については、ホワイトペーパー「*エッジツーエッジテクノロジー*」を参照してください。

** RFC 6056に従って、既定のポート番号の範囲内で自動的に割り当てられます。詳細については、Wikipediaの記事 *「エフェメラルポート」*を参照してください。

*** AXIS OS 12.1以降では、WebService Discovery (WS-Discovery) プロトコルはデフォルトで無効になっています。

可能な限り、使用していないネットワークプロトコルとサービスを無効にすることをお勧めします。デフォルトで使用されるサービスや設定に基づいて有効にできるサービスの完全なリストについては、AXIS OS Knowledge base (AXIS OS 知識ベース) で「*Commonly used network ports (一般的に使用されるネットワークポート)*」を参照してください。

例えば、ネットワークカメラなどのAxis映像監視製品では、音声入出力とマイク機能を手動で有効にする必要がありますが、Axisインターカムやネットワークスピーカーでは、音声入出力とマイク機能が主要な機能であるため、デフォルトで有効になっています。

HTTPSが有効

CSC #3：データ保護

AXIS OS 7.20以降、HTTPSは自己署名証明書を使用してデフォルトで有効になり、セキュアな方法で装置のパスワードを設定できるようになりました。AXIS OS 10.10以降のバージョンでは、自己署名証明書がIEEE 802.1ARセキュアデバイスID証明書に置き換えられています。

AXIS OSでは、工場出荷時の設定状態でサイバーセキュリティの基本レベルを向上させるために、最も一般的なセキュリティ関連のHTTP(S) ヘッダーがデフォルトで有効になっています。AXIS OS 9.80以降のバージョンでは、カスタムHTTPヘッダーVAPIX APIを使用して追加のHTTP(S) ヘッダーを設定できます。

HTTPヘッダーVAPIX APIの詳細については、「*VAPIXライブラリ*」を参照してください。

デフォルトのHTTP(S) ヘッダーの詳細については、AXIS OS knowledge base (AXIS OS知識ベース) で「*Default HTTP(S) headers (デフォルトのHTTP(S) ヘッダー)*」を参照してください。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション)] > [Security (セキュリティ)] > [HTTPS]
7.10より前	[Settings (設定)] > [System (システム)] > [Security (セキュリティ)] > [HTTP and HTTPS (HTTPおよびHTTPS]
≥ 10.9	[System (システム)] > [Network (ネットワーク)] > [HTTP and HTTPS (HTTPおよびHTTPS)]

IEEE 802.1X ネットワークアクセスコントロール

CSC #6：アクセスコントロールの管理
CSC #13：ネットワークの監視と防御

Axis装置は、EAP-TLS方式によるIEEE 802.1Xポートベースのネットワークアクセスコントロールをサポートしています。最適な保護のために、Axis装置を認証する際に、信頼できる認証局 (CA) によって署名されたクライアント証明書を使用することをお勧めします。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション)] > [Security (セキュリティ)] > [IEEE 802.1X]
7.10より前	[Settings (設定)] > [System (システム)] > [Security (セキュリティ)] > [IEEE 802.1X]
≥ 10.9	[System (システム)] > [Security (セキュリティ)] > [IEEE 802.1X]

IEEE 802.1AE MACsec

CSC #3：データ保護
CSC #6：アクセスコントロールの管理

Axisの装置は802.1AE MACsecに対応しています。これは明確に定義されたネットワークプロトコルであり、ネットワークレイヤー2上のポイントツーポイントのイーサネットリンクを暗号的に保護し、2つのホスト間のデータ送信の機密性と完全性を確保します。MACsecはネットワークスタックの低いレイヤー2で動作するため、ネイティブの暗号化機能を提供しないネットワークプロトコル (ARP、NTP、DHCP、LLDP、CDPなど) だけでなく、暗号化機能を提供するネットワークプロトコル (HTTPSやTLS) にも同様に追加のセキュリティレイヤーを提供します。

IEEE 802.1AE MACsec規格では、手動で設定可能な事前共有キー (PSK)/静的CAKモードと、IEEE 802.1X EAP-TLSセッションを使用する自動マスターセッション/動的CAKモードの2つの動作モードについて記述しています。 Axis装置は両方のモードに対応しています。

802.1AE MACsecの詳細と、AXIS OS装置での設定方法については、AXIS OSナレッジベースの*IEEE 802.1AE*を参照してください。

IEEE 802.1ARセキュアデバイスID

CSC #1：企業の資産のインベントリと管理
CSC #13：ネットワークの監視と防御

Axis Edge Vaultを搭載したAxisデバイスでは、ネットワーク規格のIEEE 802.1ARがサポートされています。これにより、生産工程でデバイスにインストールされる一意の証明書「AxisデバイスID」を通じて、Axisデバイスをネットワークに自動的かつ安全にオンボーディングできるようになります。安全なデバイスオンボーディングの例については、「*Secure integration of Axis devices into Aruba networks (Axis装置のArubaネットワークへの安全な統合)*」を参照してください。

詳細については、ホワイトペーパー「*Axis Edge Vault*」を参照してください。Axis装置のデバイスIDを検証するために使用されるAxis Device ID証明書チェーンをダウンロードするには、axis.comで「*公開鍵基盤リポジトリ*」を参照してください。

UART/デバッグインターフェース

CSC #4：企業の資産とソフトウェアのセキュアな設定

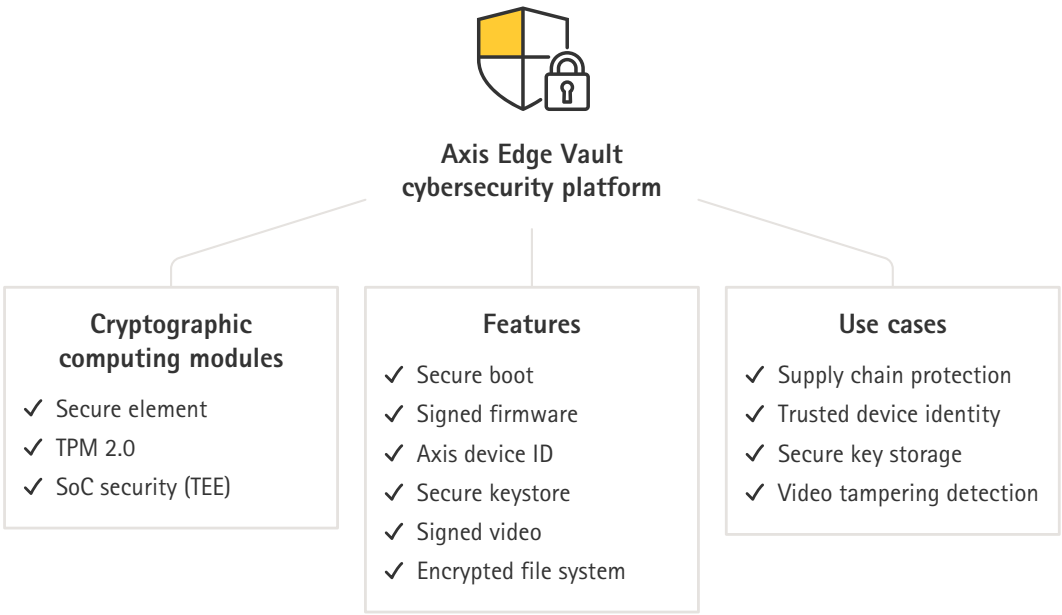
すべてのAxisデバイスは、いわゆる物理UART（Universal Asynchronous Receiver Transmitter）インターフェースを搭載しています。これは「デバッグポート」または「シリアルコンソール」とも呼ばれています。Axisデバイスを徹底的に分解しなければ、インターフェース自体に物理的にアクセスすることはできません。UART/デバッグインターフェースは、Axis社内の研究開発エンジニアリングプロジェクトにおいて、製品開発とデバッグの目的でのみ使用されます。

AXIS OS 10.10以前のバージョンのAxis装置では、UART/デバッグインターフェースはデフォルトで有効になっていますが、認証されたアクセスが必要であり、認証されていない間は機密情報が公開されることはありません。AXIS OS 10.11以降、UART/デバッグインターフェースはデフォルトで無効になっています。インターフェースを有効にする唯一の方法は、Axisが提供する装置固有のカスタム証明書を使用してロックを解除することです。

Axis Edge Vault

Axis Edge Vaultは、Axis装置を保護するハードウェアベースのサイバーセキュリティプラットフォームとなります。これは、エッジデバイスセキュリティに関する専門知識を駆使して、暗号コンピューティングモジュール（セキュアエレメントやTPM）とSoCセキュリティ（TEEやセキュアブート）に基づき構築された強力な基盤により成り立っています。Axis Edge Vaultは、セキュアブートと署名付きファームウェアによって確立された強力な信頼元に基づいています。こうした機能により、暗号で検証されたソフトウェアのCoT（信頼チェーン）が途切れることがありません。どのような操作でも、安全性の確保はこのCoTにかかっています。

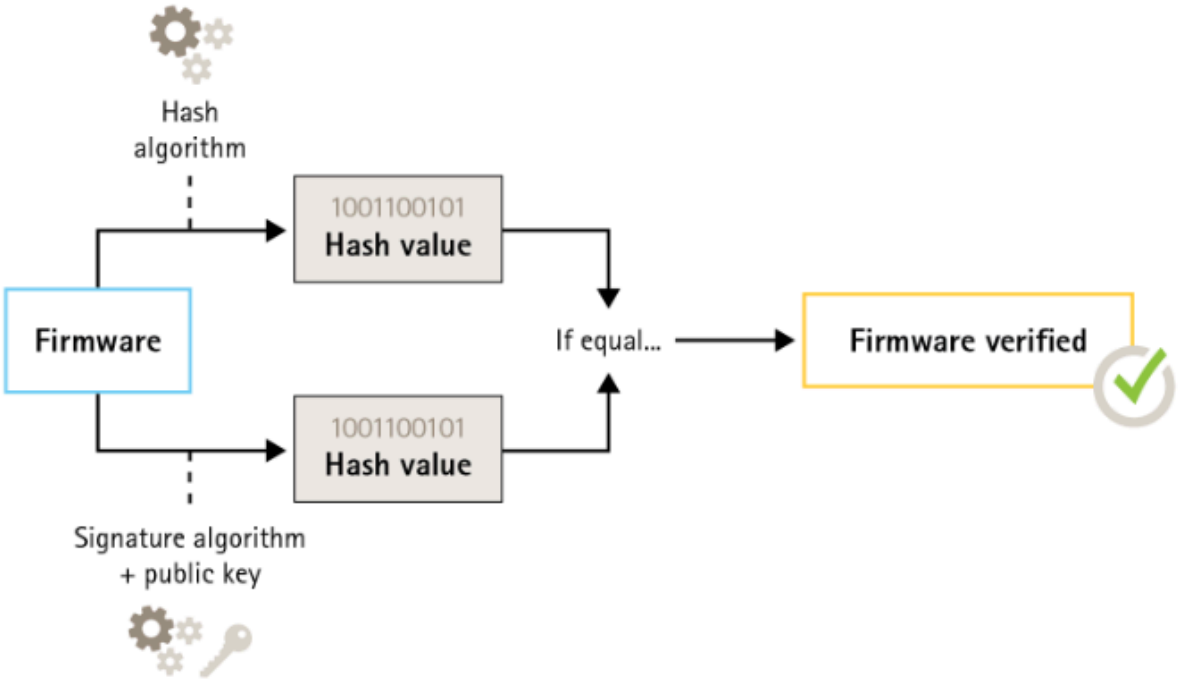
Axis Edge Vaultを搭載したAxisデバイスを利用すれば、機密情報の傍受や悪質な抽出を防止することができるため、顧客のサイバーセキュリティリスクを最小限に抑えることが可能となります。また、Axis Edge Vaultにより、Axis装置がお客様のネットワーク内で信頼できるユニットであることが確実になります。



署名付きファームウェア

CSC #2：ソフトウェア資産のインベントリと管理

バージョン9.20.1以降、AXIS OSには署名が追加されています。デバイスのAXIS OSバージョンがアップグレードされるたびに、暗号署名検証を通じてデバイスで更新ファイルの完全性がチェックされ、改ざんされているファイルは拒否されます。これにより、攻撃者がユーザーを誘導して危険なファイルをインストールさせるのを防止できます。

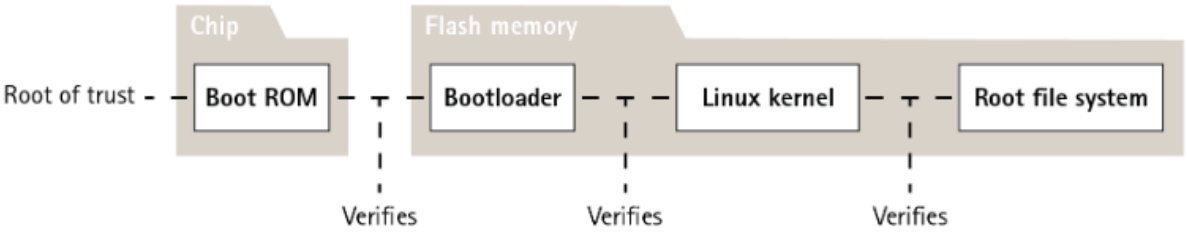


詳細については、ホワイトペーパー「*Axis Edge Vault*」を参照してください。

セキュアブート

CSC #2：ソフトウェア資産のインベントリと管理

ほとんどのAxis装置には、装置の完全性を保護するためのセキュアブートシーケンスがあります。セキュアブートにより、改ざんされたAxis装置の導入を防ぐことができます。

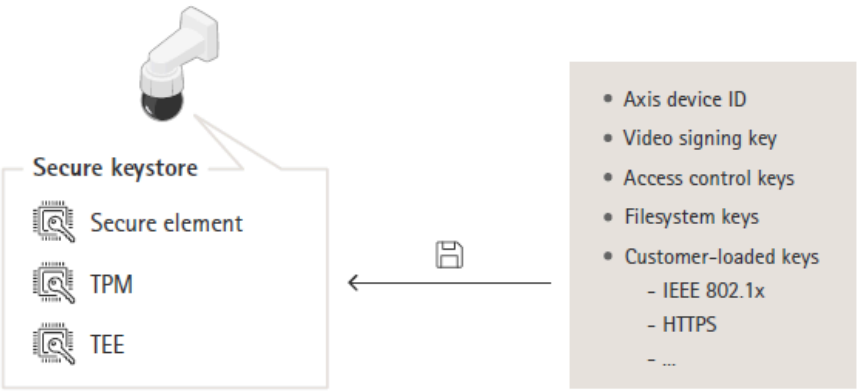


詳細については、ホワイトペーパー「*Axis Edge Vault*」を参照してください。

安全なキーストア

CSC #6：アクセスコントロールの管理

安全なキーストアにより、耐タンパー性能を備えたハードウェアベースの暗号情報ストレージが実現します。AxisデバイスIDと顧客がアップロードした暗号情報を保護すると同時に、セキュリティ侵害が発生した場合の不正アクセスや悪意のある抽出も防ぎます。セキュリティ要件に応じて、Axis装置は、TPM 2.0 (Trusted Platform Module)、セキュアエレメント、TEE (Trusted Execution Environment) などのモジュールを1つまたは複数搭載できます。



詳細については、ホワイトペーパー「*Axis Edge Vault*」を参照してください。

暗号化ファイルシステム

CSC #3：データ保護

悪意のある攻撃者は、フラッシュメモリをマウント解除し、フラッシュリーダー装置を通じてアクセスすることで、ファイルシステムから情報を抽出しようとする可能性があります。ただし、Axis装置は、だれかがファイルシステムに物理的にアクセスしたり盗んだりした場合に、悪意のあるデータの流出や設定の改ざんからファイルシステムを保護できます。Axis装置の電源がオフの場合、ファイルシステム上の情報はAES-XTS-Plain64 256bitで暗号化されます。セキュアブートプロセス中、読み書き可能なファイルシステムは復号化され、Axis装置でマウントして使用できるようになります。

詳細については、ホワイトペーパー「*Axis Edge Vault*」を参照してください。

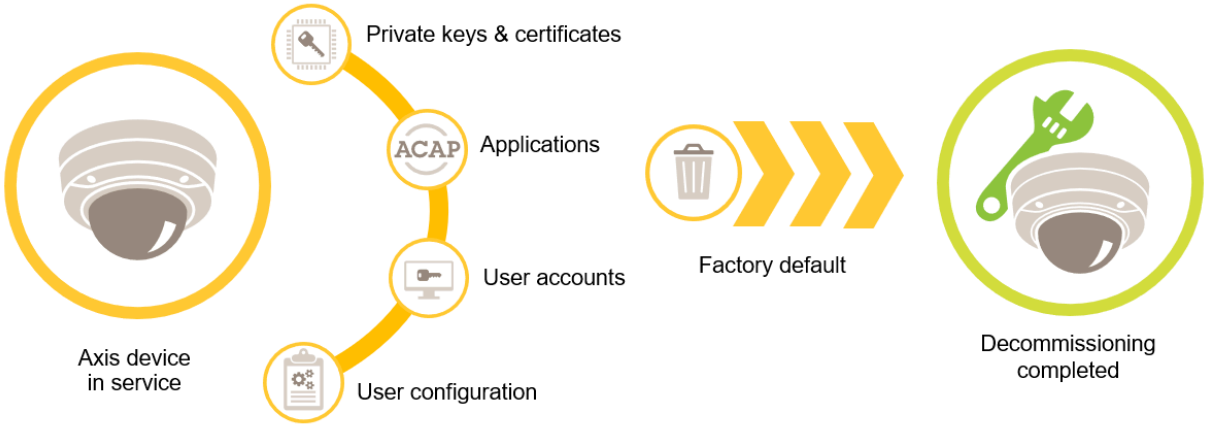
運用停止

CSC #3：データ保護

Axis装置は揮発性メモリと不揮発性メモリの両方を使用します。揮発性メモリに保存されている情報は装置を電源から外すと消去されますが、不揮発性メモリに保存されている情報は残り、起動時に再び使用できるようになります。データポインターを単に削除して、保存されたデータがファイルシステムから見えないようにするという一般的な方法は避けています。そのため、出荷時の設定へのリセットが必要になります。NANDフラッシュメモリでは、UBI機能 [Remove Volume (ボリュームの削除)] が使用されます。ストレージブロックがもう使用されていないという信号を送信するeMMCフラッシュメモリには、これに相当する機能が使用されます。その場合、ストレージコントローラーにより、必要に応じてそれらのストレージブロックが消去されます。

Axis装置を廃棄する場合は、装置を工場出荷時の設定にリセットすることをお勧めします。これにより、装置の不揮発性メモリーに保存されたすべてのデータが消去されます。

工場出荷時の状態に初期化するコマンドを実行しても、データが直ちに消去されるわけではありません。デバイスが再起動すると、そのシステム起動中にデータが消去されます。 そのため、工場出荷時の状態に初期化するコマンドを実行するだけでは不十分です。データを確実に消去するには、電源を切る前に、デバイスを再起動させて、その起動を完了させる必要があります。



AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション)] > [Maintenance (メンテナンス)] > [Default (デフォルト)]
7.10より前	[Settings (設定)] > [System (システム)] > [Maintenance (メンテナンス)] > [Default (デフォルト)]
≥ 10.9	「Maintenance (メンテナンス)」> [Default (デフォルト)]

この表には、不揮発性メモリに保存されているデータに関する詳細情報が含まれています。

情報とデータ	工場出荷時の設定後に消去
VAPIXおよびONVIFのユーザー名とパスワード	必要
証明書と秘密鍵	必要
自己署名証明書	必要
TPMとAxis Edge Vaultに保存されている情報	必要
WLAN設定とユーザー/パスワード	必要
カスタム証明書*	なし
SDカード暗号化キー	必要
SDカードデータ**	なし
ネットワーク共有設定とユーザー/パスワード	必要
ネットワーク共有データ**	なし
ユーザー設定***	必要
アップロードされたアプリケーション (ACAP)****	必要
本番データと有効期間統計*****	なし

アップロードされたグラフィックとオーバーレイ	必要
RTCクロックデータ	必要

* 署名付きファームウェアのプロセスでは、カスタム証明書が使用されます。これにより、ユーザーがAXIS OSをアップロードできるようになります（他の事柄も行うことができます）。
** エッジストレージ（SDカード、ネットワーク共有）に保存されている録画と画像は、ユーザーが別途削除する必要があります。詳細については、AXIS OS Knowledge Base（AXIS OS知識ベース）に含まれている*「Axis SDカードの初期化」*を参照してください。
*** アカウントの作成からネットワーク、O3C、イベント、画像、PTZ、システム設定に至るまで、ユーザーが行ったすべての設定が含まれます。
**** プリインストールされていたアプリケーションはデバイスに残りますが、こうしたアプリケーションでユーザーが行った設定はすべて消去されます。
***** 本番データ（キャリブレーション、生産に関する802.1AR証明書）と有効期間統計には、機密性のない情報とユーザーに関連しない情報が含まれます。

基本的な強化

基本的な強化は、Axis装置の保護の最小推奨レベルです。基本的な強化の課題は「エッジで構成可能」ということになります。これは、サードパーティ製のネットワークインフラストラクチャー、ビデオ、証拠管理システム (VMS、EMS)、機器、アプリケーションにさらに依存することなく、Axisデバイスで直接設定できることを意味します。

工場出荷時の設定

CSC #4：企業の資産とソフトウェアのセキュアな設定

装置を設定する前に、工場出荷時の設定になっていることを確認してください。ユーザーデータから装置を消去したり、使用を停止したりする必要がある場合には、装置を工場出荷時の設定にリセットすることも重要です。詳細については、を参照してください。

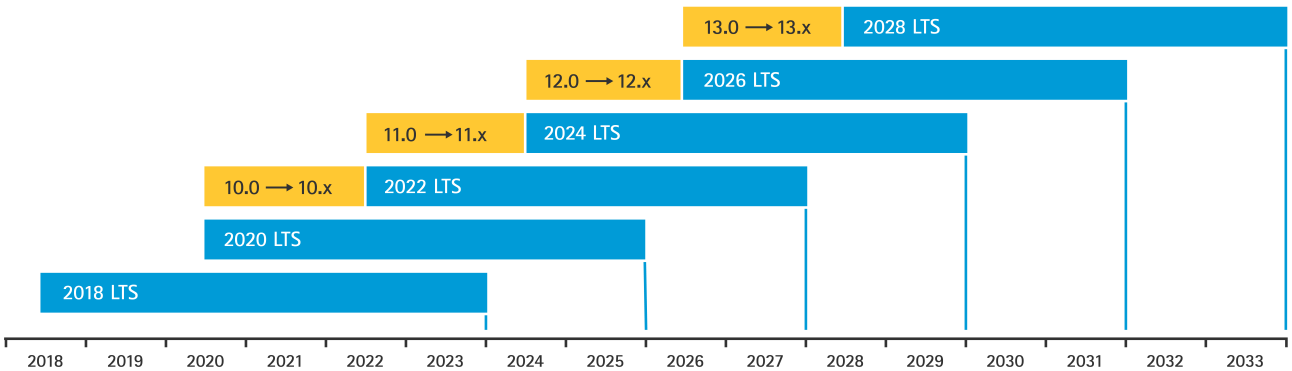
AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション)] > [Maintenance (メンテナンス)] > [Default (デフォルト)]
7.10より前	[Settings (設定)] > [System (システム)] > [Maintenance (メンテナンス)] > [Default (デフォルト)]
≥ 10.9	「Maintenance (メンテナンス)」> [Default (デフォルト)]

最新のAXIS OSへのアップグレード

CSC #2：ソフトウェア資産のインベントリと管理

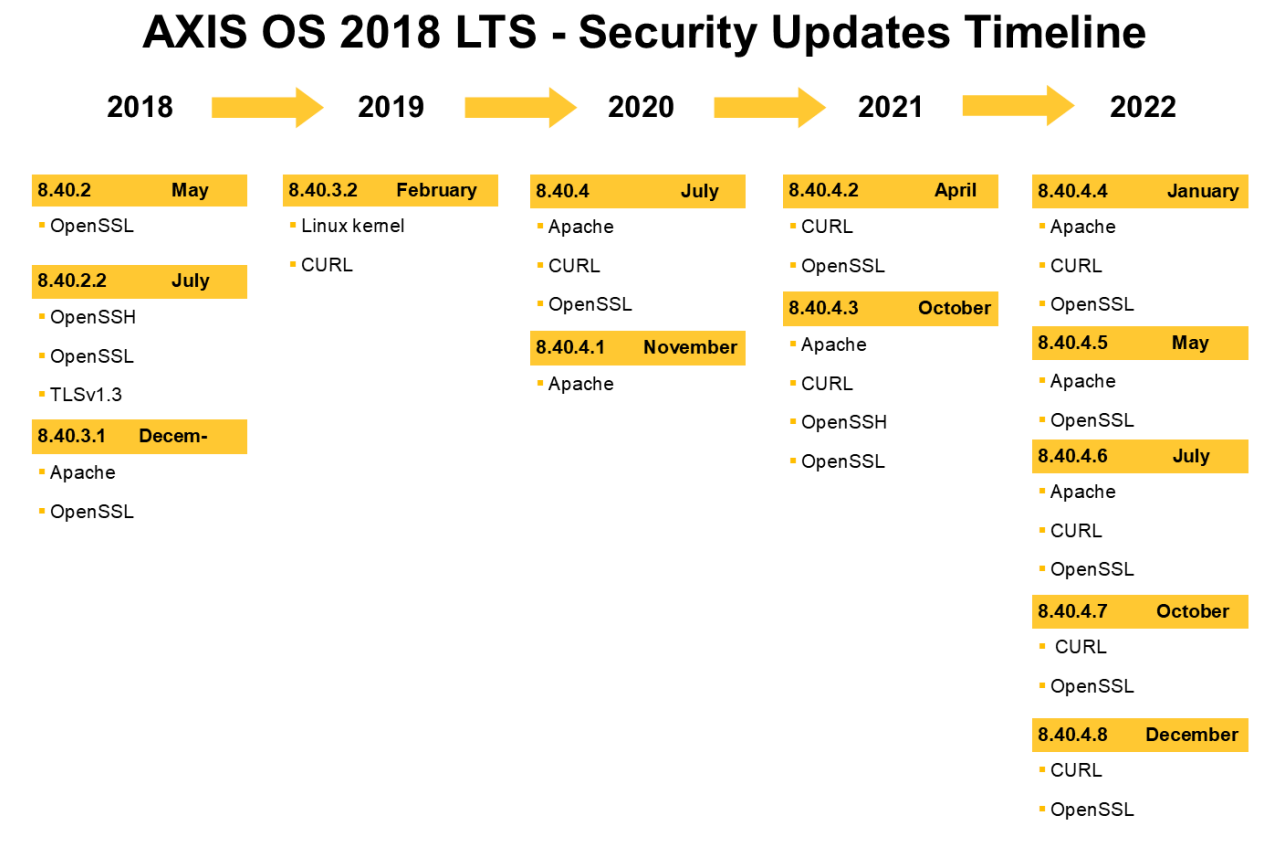
ソフトウェアにパッチを適用することは、サイバーセキュリティの重要な側面です。攻撃者は、一般的に知られている脆弱性を悪用しようとすることが多く、パッチが適用されていないサービスにネットワークアクセスした場合、その試みが成功する可能性があります。既知の脆弱性に対するセキュリティパッチが含まれている場合があるため、常に最新のAXIS OSを使用するようにしてください。特定のバージョンのリリースノートには、重要なセキュリティ修正が明示的に記載されている場合がありますが、すべての一般的な修正が記載されているわけではありません。

Axisは、アクティブトラックとLTS（長期サポート）トラックの2種類のAXIS OSトラックを提供しています。どちらのタイプにも最新の重要な脆弱性パッチが含まれていますが、互換性問題のリスクを最小限に抑えることが目的であるため、LTSトラックには新機能は含まれていません。詳細については、AXIS OS情報で「*AXIS OS lifecycle (AXIS OSライフサイクル)*」を参照してください。



Axisは、重要な新機能、バグ修正、セキュリティパッチに関する情報など、今後のリリースの予定をお知らせしています。詳細については、AXIS OS情報で「*Upcoming releases (リリース予定)*」を参照してください。axis.comの「ファームウェア」にアクセスして、装置用のAXIS OSをダウンロードしてください。

このグラフは、Axis装置を常に最新の状態に保つことの重要性を示しています。



AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション)] > [Maintenance (メンテナンス)] > [Upgrade Server (サーバーのアップグレード)]
7.10より前	[Settings (設定)] > [System (システム)] > [Maintenance (メンテナンス)] > [Firmware upgrade (ファームウェアのアップグレード)]
≥ 10.9	[Maintenance (メンテナンス)] > [Firmware upgrade (ファームウェアのアップグレード)]

専用アカウントの作成

CSC #4：企業の資産とソフトウェアのセキュアな設定
CSC #5：アカウント管理

Axisデバイスには、管理者アカウントとクライアントユーザーアカウントという2種類のアカウントがあります。デバイス管理を目的とした第一次アカウントとなる管理者アカウントは、管理タスクのみに使用することが重要となります。デバイス設定時に、管理者アカウントのユーザー名とパスワードを作成する必要があります。

管理者アカウントの他に、日常業務の操作を行うためのクライアントユーザーアカウントを作成します。このアカウントの権限は制限されています。これにより、デバイスを安全に管理でき、デバイス管理者のパスワードが漏洩するリスクが軽減されます。クライアントユーザーアカウントは、完全な管理者権限が必要とならないタスクに使用する必要があります。

いずれのアカウントの場合も、パスワードを作成する際は、NISTやBSIなどのガイドラインに示されているパスワードの推奨事項に従うことが勧められます。こうしたガイドラインでは、新規パスワードには十分な文字数が含まれている複雑なものを選択することが求められています。Axis装置は、64文字までのパスワードをサポートしています。8文字より短いパスワードは弱いと見なされます。

詳細については、*AXIS OS knowledge base (AXIS OS知識ベース) で「IDとアクセス管理」*を参照してください。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [Basic Setup (基本設定)] > [Users (ユーザー)]
7.10より前	[Settings (設定)] > [System (システム)] > [Users (ユーザー)]
≥ 10.9	[System (システム)] > [Users (ユーザー)]
≥ 11.6	[System (システム)] > [Accounts (アカウント)]

Webインターフェースへのアクセスを無効にする

CSC #4：企業の資産とソフトウェアのセキュアな設定

CSC #5：アカウント管理

Axis装置には、ユーザーが標準のWebブラウザー経由で装置にアクセスできるWebサーバーがあります。Webインターフェースは、設定、メンテナンス、トラブルシューティングを目的としています。これは、クライアントとして使用してビデオを視聴するなど、日常の作業を目的としたものではありません。

日常の作業でAxis装置とのやり取りを許可する必要があるクライアントは、ビデオ管理システム (VMS) や装置管理およびAXIS Device Managerなどの管理ツールのみです。システムユーザーには、Axis装置への直接アクセスを絶対に許可しないでください。

AXIS OS 9.50以降、Axis装置のWebインターフェースを無効にできます。Axis装置をシステムに導入 (つまりAXIS Device Managerに追加) したら、組織内の人がWebブラウザー経由で装置にアクセスできるオプションを削除することをお勧めします。これにより、装置アカウントのパスワードが組織内で共有されている場合、追加のセキュリティ層が作成されます。より安全なオプションは、高度なIDアクセス管理 (IAM) アーキテクチャ、より優れたトレーサビリティ、アカウント漏洩の防護機能を提供する専用アプリケーションを通じて、Axis装置へのアクセスを排他的に設定することです。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	N/A
7.10より前	[Settings (設定)] > [System (システム)] > [Plain config (プレーン設定)] > [System (システム)] > [Web Interface Disabled (Webインターフェース無効)]
≥ 10.9	[System (システム)] > [Plain config (プレーン設定)] > [System (システム)] > [Web Interface Disabled (Webインターフェース無効)]

ネットワーク、日付、時刻の設定の構成

CSC #4：CSC #8：監査ログの管理
CSC #12：ネットワークインフラストラクチャーの管理

Axisデバイスの機能を良好かつ安全に維持するために、デバイスのネットワーク、日付、時刻の設定を適切に構成することが重要となります。こうした設定により、ネットワーク通信、ログ記録、証明書の検証など、デバイスの動作のさまざまな側面に影響が及ぼされます。

装置のIP設定は、IPv4/IPv6、静的または動的 (DHCP) ネットワークアドレス、サブネットマスク、デフォルトルーターなどのネットワーク設定によって異なります。新しいコンポーネントを追加する際は、必ずネットワークトポロジを確認してください。ネットワークの到達可能性を確保するため、またDHCPサーバーのように攻撃に脆弱であり得るネットワークサーバーへの依存を最小限に抑えるために、静的IPアドレス構成を使用することが勧められます。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [Basic Setup (基本設定)] > [TCP/IP]
7.10より前	[Settings(設定)] > [System (システム)] > [TCP/IP]
≥ 10.9	[System (システム)] > [Network (ネットワーク)]

システムログを維持し、デジタル証明書を検証する上で、またHTTPS、IEEE、802.1xといったサービスを有効化する上で、正確に時間の管理を行うことが不可欠となります。そのため、デバイスの時計をNTP（Network Time Protocol）サーバーまたはNTS（Network Time Security）サーバーと同期することが勧められます。AXIS OS 11.1には、NTS（Network Time Security）が追加されています。NTSはNTP（Network Time Protocol）を暗号化した安全なプロトコルです。精度を高め、潜在的な障害に対応するために、複数のタイムサーバーを設定することが勧められます。ローカルタイムサーバーをホストできない場合は、パブリックNTPまたはNTSサーバーを使用することを検討してください。Axis装置でのNTP/NTSの詳細については、AXIS OS knowledge base (AXIS OS知識ベース) で「*NTP and NTS (NTPとNTS)*」を参照してください。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [Basic Setup (基本設定)] > [Date & Time (日付と時間)]
7.10より前	[Settings (設定)] > [System (システム)] > [Date and time (日付と時刻)]
≥ 10.9	[System (システム)] > [Date and time (日付と時刻)]
≥ 11.6	[System (システム]) >[Time and location (時刻と場所)]

エッジストレージ暗号化

CSC #3：データ保護

SDカード

録画を保存するセキュアデジタル (SD) カードがAxisデバイスでサポートされている場合、またはこれが使用されている場合は、暗号化を適用することが勧められます。これにより、取り外したSDカードに保存されているビデオを権限のない個人が再生できなくなります。

Axis装置のSDカード暗号化の詳細については、AXIS OS knowledge base (AXIS OS知識ベース) で「*SD card support (SDカードのサポート)*」を参照してください。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup(設定)] > [System Options (システムオプション)] > [Storage (ストレージ)]
7.10より前	[Settings (設定)] > [System (システム)] > [Storage (ストレージ)]
≥ 10.9	[System (システム)] > [Storage (ストレージ)]

ネットワーク共有（NAS）
ネットワーク接続ストレージ (NAS) を録画装置として使用する場合は、アクセスが制限されたロックされた領域に保管し、ハードディスクの暗号化を有効にすることをお勧めします。Axis装置は、ビデオ録画を保存するためにNASに接続するためのネットワークプロトコルとして、SMBを利用します。SMBの以前のバージョン (1.0および2.0) ではセキュリティや暗号化が提供されませんが、新しいバージョン (2.1以降) ではセキュリティや暗号化が提供されるため、本番環境で新しいバージョンを使用することをお勧めします。

Axis装置をネットワーク共有に接続するときの適切なSMBの設定の詳細については、AXIS OS knowledge base (AXIS OS知識ベース) で「*Network share (ネットワーク共有)*」を参照してください。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup(設定)] > [System Options (システムオプション)] > [Storage (ストレージ)]
7.10より前	[Settings (設定)] > [System (システム)] > [Storage (ストレージ)]
≥ 10.9	[System (システム)] > [Storage (ストレージ)]

アプリケーション (ACAP)

CSC #4：企業の資産とソフトウェアのセキュアな設定

Axis装置にアプリケーションをアップロードして、機能を拡張できます。それらの多くには、特定の機能を操作するための独自のユーザーインターフェースが付属しています。アプリケーションは、AXIS OSが提供するセキュリティ機能を使用する場合があります。

Axis装置には、*Axisセキュリティ開発モデル (ASDM)* に従ってAxisが開発した複数のアプリケーションがプリロードされています。Axisアプリケーションの詳細については、axis.comで「*分析機能*」を参照してください。

サードパーティ製のアプリケーションの場合は、運用とテストの観点からそのセキュリティに関する証拠の提出を依頼したり、一般的なベストプラクティスのセキュリティ開発モデルに従って開発されているかどうかについてベンダーに問い合わせたりすることをお勧めします。サードパーティ製のアプリケーションで見つかった脆弱性は、サードパーティ製のベンダーに直接報告する必要があります。

信頼できるアプリケーションのみを操作し、使用していないアプリケーションはAxis装置から削除することをお勧めします。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [Applications (アプリケーション)]
7.10より前	[Setup (設定)] > [Apps (アプリ)]
≥ 10.9	アプリ

使用していないサービス/機能を無効にする

CSC #4：企業の資産とソフトウェアのセキュアな設定

使用していないサービスや機能が直ちにセキュリティ上の脅威になるわけではありませんが、不必要なリスクを軽減するために、使用していないサービスや機能を無効にすることをお勧めします。使用していない場合に無効にできるサービスと機能の詳細については、このまま読み進めてください。

使用していない物理ネットワークポート

AXIS OS 11.2以降、AXIS S3008などの複数のネットワークポートを備えた装置には、ネットワークポートのPoEとネットワークトラフィックの両方を無効にするオプションが用意されています。使用していないネットワークポートを放置してアクティブのままにすると、重大なセキュリティリスクが生じます。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	N/A
7.10より前	N/A
≥ 11.2	[System (システム)] > [Power over Ethernet]

ネットワーク検出プロトコル

Bonjour、UPnP、ZeroConf、WS-Discovery、LLDP/CDPなどの検出プロトコルは、ネットワーク上でAxis装置とそのサービスを簡単に見つけられるようにするサポートサービスです。装置を導入してVMSに追加した後、検出プロトコルを無効にして、Axis装置がネットワーク上でその存在を通知しないようにすることをお勧めします。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション] > [Advanced (詳細設定] > [Plain Config (プレーン設定] > [Network (ネットワーク)] > [Network Bonjour Enabled, Network UPnP Enabled, Network ZeroConf Enabled, Network UPnP NATTraversal Enabled (ネットワークBonjour有効、ネットワークUPnP有効、ネットワークZeroConf有効、ネットワークUPnP NATTraversal有効]*
	N/A
7.10より前	[Settings (設定)] > [System (システム)] > [Plain Config (プレーン設定] > [Network (ネットワーク)] > [Network Bonjour Enabled, Network UPnP Enabled, Network ZeroConf Enabled, Network UPnP NATTraversal Enabled (ネットワークBonjour有効、ネットワークUPnP有効、

AXIS OSバージョン	Webインターフェースの設定パス
	ネットワークZeroConf有効、ネットワークUPnP NATTraversal有効]*
	[Settings (設定)] > [System (システム)] > [Plain config (プレーン設定)] > [WebService (Webサービス)] > [Discovery Mode (検出モード)]
≥ 10.9	[Settings (設定)] > [Plain Config (プレーン設定)] > [ネットワーク] > [Bonjour Enabled, UPnP Enabled, ZeroConf Enabled (Bonjour有効、UPnP有効、ZeroConf有効)]
	[System (システム)] > [Plain config (プレーン設定)] > [WebService (Webサービス)] > [DiscoveryMode (検出モード)] > [Enable WS-Discovery discoverable mode (WS-Discovery検出可能モードを有効にする]
≥ 11.11	System (システム) > Network (ネットワーク) > Network discovery protocols (ネットワーク検出プロトコル) > LLDP and CDP (LLDPおよびCDP)**

* この機能はAXIS 10.12から削除され、それ以降のバージョンでは使用できません。

** LLDPとCDPを無効にすると、PoE電力ネゴシエーションに影響する可能性があります。

古いTLSバージョン

Axis装置を本番環境に導入する前に、古くて期限切れになっている、セキュアでないTLSバージョンを無効にすることをお勧めします。通常、古いTLSバージョンはデフォルトで無効になっていますが、TLS 1.2およびTLS 1.3をまだ実装していないサードパーティ製のアプリケーションに下位互換性を提供するために、Axis装置で有効になっている可能性があります。

旧式のTLSバージョンはAXIS OS 12.0から削除されたため、それ以降のバージョンでは利用できません。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション)] > [Advanced (詳細)] > [Plain Config (プレーン設定)] > [HTTPS] > [Allow TLSv1.0 and/or Allow TLSv1.1 (TLSv1. 0/TLSv1.1を許可する)]
7.10より前	[Setup (設定)] > [System (システム)] > [Plain Config (プレーン設定)] > [HTTPS] > [Allow TLSv1.0 and/or Allow TLSv1.1 (TLSv1. 0/TLSv1.1を許可する)]
≥ 10.9	[System (システム)] > [Plain Config (プレーン設定)] > [HTTPS] > [Allow TLSv1.0 and/or Allow TLSv1.1 (TLSv1. 0/TLSv1.1を許可する)]

スクリプトエディター環境

スクリプトエディター環境へのアクセスを無効にすることをお勧めします。スクリプトエディターは、トラブルシューティングとデバッグの目的でのみ使用します。

スクリプトエディターはAXIS OS 10.11から削除され、それ以降のバージョンでは使用できません。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	N/A
7.10より前	[Settings (設定)] > [System (システム)] > [Plain config (プレーン設定)] > [System (システム)] > [Enable the script editor (editcgi) (スクリプトエディター (editcgi) を有効にする)]
≥ 10.9	[System (システム)] > [Plain config (プレーン設定)] > [System (システム)] > [Enable the script editor (editcgi) (スクリプトエディター (editcgi) を有効にする)]

HTTP(S)サーバーヘッダー

デフォルトでは、Axis装置は、ネットワーク上のクライアントとのHTTP(S) 接続中に、現在のApacheおよびOpenSSLバージョンを通知します。この情報は、特定のAXIS OSバージョンにおける未解決の脆弱性のより詳細なレポートを提供するため、ネットワークセキュリティスキャナーを定期的に使用する場合に便利です。

HTTP(S) サーバーヘッダーを無効にして、HTTP(S) 接続中の情報露出を減らすことができます。ただし、装置を常に最新の状態に保ち、Axisが推奨する方法に従って装置を操作する場合にのみ、ヘッダーを無効にすることをお勧めします。

HTTP(S) サーバーヘッダーを無効にするオプションは、AXIS OS 10.6以降から使用できます。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	N/A
7.10より前	[Settings (設定)] > [System (システム)] > [Plain config (プレーン設定)] > [System (システム)] > [HTTP Server Header Comments (HTTPサーバーヘッダーコメント)]
≥ 10.9	[System (システム)] > [Plain config (プレーン設定)] > [System (システム)] > [HTTP Server Header Comments (HTTPサーバーヘッダーコメント)]

音声

ネットワークカメラなどのAxis映像監視向け製品では、音声入出力およびマイク機能はデフォルトで無効になっています。音声機能が必要な場合は、使用前に有効にする必要があります。Axisインターカムやネットワークスピーカーなど、音声入出力とマイク機能が主要な機能であるAxis製品では、音声機能がデフォルトで有効になっています。

音声機能を使用しない場合は、無効にすることをお勧めします。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション)] > [Advanced (詳細設定)] > [Plain Config (プレーン設定)] > [Audio (音声)] > [Audio A* (音声A*)] > [Enabled (有効)]
7.10より前	[Settings (設定)] > [Audio (音声)] > [Allow audio (音声を許可)]
≥ 10.9	[Audio (音声)] > [Device settings (装置設定)]

SDカードスロット

Axis装置は通常、ビデオ録画のローカルエッジストレージを提供するために、1枚以上のSDカードをサポートしています。SDカードを使用しない場合は、SDカードスロットを完全に無効にすることをお勧めします。SDカードスロットを無効にするオプションは、AXIS OS 9.80以降から使用できます。

詳細については、AXIS OS knowledge base (AXIS OS知識ベース) で「*Disabling the SD card* (SDカードを無効にする) 」を参照してください。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	N/A
7.10より前	[Settings (設定)] > [System (システム)] > [Plain config (プレーン設定)] > [Storage (ストレージ)] > [SD Disk Enabled (SDディスク有効)]
≥ 10.9	[System (システム)] > [Plain config (プレーン設定)] > [Storage (ストレージ)] > [SD Disk Enabled (SDディスク有効)]

FTPアクセス

FTPは、安全性の低い通信プロトコルです。これは、トラブルシューティングとデバッグ目的にのみ使用されるプロトコルです。AXIS OS 11.1以降、OSからFTPアクセスが排除されたため、それ以降のバージョンではこれを利用することはできません。トラブルシューティングの目的では、FTPアクセスを無効にし、セキュアなSSHアクセスを使用することをお勧めします。

SSHの詳細については、AXIS OSポータルで「*SSHアクセス*」を参照してください。FTPを使用したデバッグオプションの詳細については、AXIS OSポータルで「*FTPアクセス*」を参照してください。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション)] > [Plain Config (プレーン設定)] > [Network (ネットワーク)] >[FTP Enabled (FTP有効)]
7.10より前	[Settings (設定)] > [System (システム)] > [Plain config (プレーン設定)] > [Network (ネットワーク)] > [FTP Enabled (FTP有効)]
≥ 10.9	[System (システム)] > [Plain config (プレーン設定)] > [Network (ネットワーク)] > [FTP Enabled (SSH有効)]

SSHアクセス

SSHは、トラブルシューティングとデバッグの目的にのみ使用されるセキュアな通信プロトコルです。AXIS OS 5.50以降のAxisデバイスでサポートされています。SSHアクセスを無効化することが勧められます。

SSHを使用したデバッグオプションの詳細については、AXIS OS knowledge base (AXIS OS知識ベース) で「*SSH access (SSHアクセス)*」を参照してください。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション)] > [Plain Config (プレーン設定)] > [Network (ネットワーク)] >[SSH Enabled (SSH有効)]
7.10より前	[Settings (設定)] > [System (システム)] > [Plain config (プレーン設定)] > [Network (ネットワーク)] > [SSH Enabled (SSH有効)]
≥ 10.9	[System (システム)] > [Plain config (プレーン設定)] > [Network (ネットワーク)] > [SSH Enabled (SSH有効)]

Telnetアクセス

Telnetは、トラブルシューティングとデバッグの目的のみに使用される、セキュアでない通信プロトコルです。これは、AXIS OS 5.50以前のバージョンを搭載しているAxisデバイスでサポートされています。Telnetアクセスを無効化することが勧められます。

AXIS OSバージョン	Webインターフェースの設定パス
5.50より前	手順については、AXIS OS knowledge base (AXIS OS知識ベース) で「*Device access (デバイスアクセス)*」を参照してください。
7.10より前	N/A
7.10より前	N/A
≥ 10.9	N/A

ARP/Ping

ARP/Pingは、AXIS IP Utilityなどのツールを使用してAxis装置のIPアドレスを設定する方法でした。この機能はAXIS OS 7.10から削除され、それ以降のバージョンでは使用できません。AXIS OS 7.10以前のバージョンを搭載したAxis装置では、この機能を無効にすることをお勧めします。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション)] > [Advanced (詳細設定)] > [Plain Config (プレーン設定)] > [Network (ネットワーク)] >[ARP/Ping]
7.10より前	N/A
≥ 10.9	N/A

USB

AXIS OS 12.1以降、AXIS D1110にはUSBポートを無効化するオプションが備わっています。使用していないUSBポートを放置してアクティブのままにすると、重大なセキュリティリスクが生じます。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	N/A
7.10より前	N/A
≥ 12.1	[System (システム)]> > [Accessories (アクセサリー)]> [USB Configuration (USB設定)]

ホストベースのファイアウォール

CSC #1：企業の資産のインベントリと管理
CSC #4：企業の資産とソフトウェアのセキュアな設定
CSC #13：ネットワークの監視と防御

AXIS OS 11.9以降に導入されているホストベースのファイアウォールはセキュリティ機能です。これにより、IPアドレスやTCP/UDPポート番号経由の入力トラフィックを制御するルールを作成することができます。これが、デバイスやそのサービスへの不正アクセスの防止につながります。

デフォルトポリシーを「拒否」に設定した場合、権限のあるすべてのクライアント (VMSおよび管理クライアント) やポートを必ずリストに追加してください。

AXIS OSバージョン	Webインターフェースの設定パス
≥ 11.9	[Setup (設定)] > [Security (セキュリティ)] > [Firewall (ファイアウォール)]

IPアドレスフィルタリング

AXIS OS 11.8以前のバージョンを搭載したデバイスでは、IPアドレスフィルタリングによって、許可されていないクライアントからのアクセスが防止されます。承認済みネットワークホストのIPアドレスが許可されるように、または未承認のIP アドレスが拒否されるようにデバイスを設定することが勧められます。

IPアドレスを許可する場合は、VMSサーバーと管理クライアントを含め、すべての承認済みクライアントをリストに追加してください。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション)] > [Security (セキュリティ)] > [IP Address Filter (IPアドレスフィルター)]
7.10より前	[Settings(設定)] > [System (システム)] > [TCP/IP] > [IP address filter (IPアドレスフィルター)]
10.9 — 11.8	[Settings(設定)] > [Security (セキュリティ)] > [IP address filter (IPアドレスフィルター)]

注

ネットワークアクセス試行に関するより詳細なログを有効化すると、他のネットワークホストからの不要なアクセス試行を特定することが可能となります。**[System (システム)]** > **[Plain config (プレーン設定)]** > **[Network (ネットワーク)]** の順に移動して、[Network Filter Log (ネットワークフィルターログ)] に移動すると、より詳細なログを有効化することができます。

HTTPS

CSC #3：データ保護

AXIS OS 7.20以降を搭載したAxisデバイスでは、HTTPとHTTPSがデフォルトで有効化されています。HTTP経由でのアクセスの場合は、暗号化が全く行われないために安全性が低くなります。HTTPSでは、クライアントとAxisデバイス間のトラフィックが暗号化されます。Axis装置のすべての管理タスクにはHTTPSを使用することをお勧めします。

設定方法については、とを参照してください。

HTTPSのみ

Axis装置は、HTTPSのみを使用するように設定することをお勧めします (HTTPアクセスは不可)。これにより、HSTS (HTTP Strict Transport Security) が自動的に有効になり、装置のセキュリティがさらに向上します。

AXIS OS 7.20以降、Axis装置には自己署名証明書が付属しています。自己署名証明書は設計上信頼できませんが、初期設定時や公開鍵基盤 (PKI) が使用できない場合にAxis装置にセキュアにアクセスするには十分です。可能であれば、自己署名証明書を削除し、選択したPKI機関が発行した適切な署名付きクライアント証明書に置き換える必要があります。AXIS OS 10.10以降、自己署名証明書はIEEE 802.1ARセキュアデバイスID証明書に置き換えられました。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション)] > [Security (セキュリティ)] > [HTTPS]
7.10より前	[Settings (設定)] > [System (システム)] > [Security (セキュリティ)] > [HTTP and HTTPS (HTTPおよびHTTPS]
≥ 10.9	[System (システム)] > [Network (ネットワーク)] > [HTTP and HTTPS (HTTPおよびHTTPS)]

HTTPS暗号

Axis装置は、TLS 1.2およびTLS 1.3暗号スイートをサポートし使用して、HTTPS接続をセキュアに暗号化します。使用する特定のTLSバージョンと暗号スイートは、Axis装置に接続するクライアントによって異なり、それに応じてネゴシエーションされます。AXIS OSの定期更新では、Axis装置で使用可能な暗号のリストが更新される場合がありますが、実際の暗号設定は変更されません。暗号設定の変更は、Axis装置を工場出荷時の設定に戻すか、ユーザー設定を手動で行うことにより、ユーザーが開始する必要があります。AXIS OS 10.8以降では、ユーザーがAXIS OSの更新を行うと、暗号のリストが自動的に更新されます。

TLS 1.2以下

TLS 1.2以下を使用する場合、Axis装置の再起動後に使用されるHTTPS暗号を指定できます。選択できる暗号に制限はありませんが、セキュリティ強化のため、以下のいずれかまたはすべての強力な暗号を選択することをお勧めします。

```
ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:ECDHE-RSA-CHACHA20-POLY1305
```

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション)] > [Advanced (詳細設定)] > [Plain Config (プレーン設定)] > [HTTPS] > [Ciphers (暗号)]
7.10より前	[Settings (設定)] > [System (システム)] > [Plain config (プレーン設定)] > [HTTPS] > [Ciphers (暗号)]
≥ 10.9	[System (システム)] > [Plain config (プレーン設定)] > [HTTPS] > [Ciphers (暗号)]

TLS 1.3

デフォルトでは、TLS 1.3仕様に従った強力な暗号スイートのみが使用できます。

```
TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_256_GCM_
SHA384
```

これらのスイートはユーザーが設定することはできません。

アクセスログ

CSC #1：企業の資産のインベントリと管理
CSC #8：監査ログの管理

アクセスログは、Axis装置にアクセスするユーザーの詳細なログを提供するため、監査とアクセスコントロール管理の両方が容易になります。この機能を有効にし、リモートsyslogサーバーと組み合わせて、Axis装置がログを中央のログ環境に送信できるようにすることをお勧めします。これにより、ログメッセージの保存とその保存期間が簡素化されます。

詳細については、AXIS OS knowledge base (AXIS OS知識ベース) で「*Device access logging (デバイスアクセスログ)*」を参照してください。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション)] > [Advanced (詳細設定)] > [Plain Config (プレーン設定)] > [System (システム)] > [Access log (アクセスログ)]
7.10より前	[Settings (設定)] > [System (システム)] > [Plain Config (プレーン設定)] > [System (システム)] > [Access log (アクセスログ)]
≥ 10.9	[System (システム)] > [Plain Config (プレーン設定)] > [System (システム)] > [Access log (アクセスログ)]

物理的改ざん防止アクセサリー

CSC #1：企業の資産のインベントリと管理
CSC #12：ネットワークインフラストラクチャーの管理

Axisは、Axis装置の物理的な保護を強化するために、オプションのアクセサリーとして物理的な侵入/改ざん防止スイッチを提供しています。これらのスイッチは、警告をトリガーでき、選択したクライアントにAxis装置が通知や警告を送ることができるようにします。

使用できる改ざん防止アクセサリーの詳細については、以下を参照してください。

- *AXIS TA8501 Physical Tampering Switch*
- *AXIS Dome Intrusion Switch C*
- *AXISドアスイッチ A*

拡張強化

拡張強化の手順は、とで説明している強化のトピックに基づいています。ただし、デフォルトおよび基本的な強化手順をAxis装置に直接適用することはできますが、拡張強化の対象にはベンダーのサプライチェーン全体、エンドユーザー組織、基盤となるITインフラストラクチャーやネットワークインフラストラクチャーを積極的に含める必要があります。

インターネットとネットワークへの露出の抑制

CSC #12：ネットワークインフラストラクチャーの管理

Axisデバイスをパブリックwebサーバーとして公開しないこと、また他の方法で不明なクライアントにデバイスへのネットワークアクセスを許可しないことが勧められます。ビデオ管理ソフトウェア（VMS）を使用していない小規模組織や個人、または遠隔地からビデオにアクセスする必要のある小規模組織や個人には、AXIS Camera Station Edgeが適切な選択肢となります。

AXIS Camera Station Edgeは、Windows、iOS、Androidで無料で利用することができます。これを活用することで、デバイスをインターネットに公開せずに、安全かつ容易なビデオへのアクセスを実現することができます。詳細については、*axis.com/products/axis-camera-station-edge*を参照してください。

注

VMSを使用している組織の場合は、VMSベンダーにリモートビデオアクセスのベストプラクティスについて相談してください。

ネットワークデバイスおよび関連するインフラストラクチャーとアプリケーションを分離することで、ネットワークへの露出リスクが削減されます。

Axisデバイス、関連インフラストラクチャー、関連アプリケーションは、本番ネットワークやビジネスネットワークから分離されているローカルネットワークに隔離することが勧められます。

基本的な強化を適用するには、多層のネットワークセキュリティメカニズムを追加して、ローカルネットワークとそのインフラストラクチャー (ルーター、スイッチ) を不正アクセスから保護します。これには、VLANセグメンテーション、ルーティング機能の制限、サイト間またはWANアクセスのVPN、ネットワークレイヤー2/3ファイアウォールの配置、アクセスコントロールリスト（ACL）などが含まれます。

基本的な強化を拡張するには、ディープパケットインスペクションや侵入検知といった高度なネットワーク検査テクノロジーを適用します。これにより、ネットワーク内で発生する脅威の防御能力が強化されます。通常、拡張ネットワーク強化には、特殊なソフトウェアやハードウェアアプライアンスが必要となることに注意してください。

ネットワークの脆弱性のスキャン

CSC #1：企業の資産のインベントリと管理
CSC #12：ネットワークインフラストラクチャーの管理

ネットワークセキュリティスキャナーを使用して、ネットワーク装置の脆弱性評価を実行できます。脆弱性評価の目的は、潜在的なセキュリティ脆弱性や設定ミスを体系的に確認することです。

Axis装置とその関連インフラストラクチャーの脆弱性評価を定期的に実行することをお勧めします。スキャンを開始する前に、使用できる最新のAXIS OSバージョン (LTSまたはアクティブトラック) に、Axis装置が更新されていることを確認してください。

また、スキャンレポートを確認し、Axis装置の既知の誤検出を除外することをお勧めします。これについては、「*AXIS OS脆弱性スキャナーガイド*」を参照してください。レポートと追加のコメントをヘルプデスクチケットに記入して、axis.comで「*Axisサポート*」に送信してください。

信頼できる公開鍵基盤 (PKI)

CSC #3：データ保護

CSC #12：ネットワークインフラストラクチャーの管理

パブリックまたはプライベートの認証局 (CA) によって信頼され、署名されたWebサーバー証明書とクライアント証明書をAxis装置に導入することをお勧めします。検証済みの信頼チェーンが構成されたCA署名付き証明書により、HTTPS経由での接続時に表示されるブラウザの証明書警告を排除することができます。また、CA署名付き証明書により、ネットワークアクセスコントロール（NAC）ソリューションを展開する際に、Axisデバイスの真正性が保証されます。これにより、Axis装置になりすましたコンピューターからの攻撃のリスクが軽減されます。

組み込みのCAサービスが付属するAXIS Device Managerを使用して、署名付き証明書をAxis装置に発行できます。

リモートsyslog

CSC #8：監査ログの管理

すべてのログメッセージを暗号化して中央のsyslogサーバーに送信するように、Axis装置を設定できます。これにより監査が容易になり、意図的に、悪意を持って、または意図せずに、Axis装置でログメッセージが削除されるのを防止できます。企業のポリシーによっては、装置ログの保持期間を延長することもできます。

さまざまなAXIS OSバージョンでリモートsyslogサーバーを有効にする方法の詳細については、AXIS OS knowledge base (AXIS OS知識ベース) で「*Syslog*」を参照してください。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	手順については、AXIS OSポータルで「*Syslog*」を参照してください。
7.10より前	[Settings(設定)] > [System (システム)] > [TCP/IP]
≥ 10.9	[System (システム)] > [Logs (ログ)]

セキュアビデオストリーミング (SRTP/RTSPS)

CSC #3：データ保護

AXIS OS 7.40以降を搭載しているAxisデバイスでは、SRTP/RTSPSとも呼ばれるRTP経由のセキュアビデオストリーミングがサポートされています。SRTP/RTSPSでは、安全なエンドツーエンドの暗号化転送方法が用いられるため、承認済みクライアント以外はAxisデバイスからビデオストリームを受信できなくなります。ビデオ管理システム (VMS) がSRTP/RTSPSをサポートしている場合は、SRTP/RTSPSを有効にすることをお勧めします。利用可能であれば、非暗号化RTPビデオストリーミングの代わりにSRTPを使用してください。

注

SRTP/RTSPSはビデオストリームデータのみを暗号化します。管理設定タスクでは、このタイプの通信を暗号化するためにHTTPSのみを有効にすることをお勧めします。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	[Setup (設定)] > [System Options (システムオプション)] > [Advanced (詳細設定)] > [Plain Config (プレーン設定)] > [Network (ネットワーク)] >[RTSPS]
7.10より前	[Settings (設定)] > [System (システム)] > [Plain config (プレーン設定)] > [Network (ネットワーク)] > [RTSPS]
≥ 10.9	[System (システム)] > [Plain config (プレーン設定)] > [Network (ネットワーク)] > [RTSPS]

署名付きビデオ

CSC #3：データ保護

AXIS OS 10.11以降、Axis Edge Vaultを搭載したAxis装置は、署名付きビデオをサポートしています。署名付きビデオを使用すると、Axis装置はビデオストリームに署名を追加して、ビデオが改ざんされていないことを確認し、ビデオを作成した装置までさかのぼってその出所を検証できます。ビデオ管理システム (VMS) または証拠管理システム (EMS) は、Axis装置から提供されたビデオの信ぴょう性を検証することもできます。

詳細については、ホワイトペーパー「*Axis Edge Vault*」を参照してください。署名付きビデオの信ぴょう性を検証するために使用されるAxisルート証明書を見つけるには、AXIS OS knowledge base (AXIS OS知識ベース) で「*Device access (デバイスアクセス)* 」を参照してください。

AXIS OSバージョン	Webインターフェースの設定パス
7.10より前	N/A
7.10より前	N/A
≥ 10.9	[System (システム)] > [Plain config (プレーン設定)] > [Image (画像)] > [SignedVideo (署名付きビデオ)]

クイックスタートガイド

クイックスタートガイドでは、AXIS OS 5.51以降のバージョンでAxis装置を強化するときに構成する必要がある設定の概要を示します。このガイドでは、で説明している強化に関するトピックを取り上げていますが、のトピックは、ケースバイケースで広範かつお客様固有の設定が必要なため、取り上げていません。

AXIS Device Managerを使用して、迅速かつコスト効率の高い方法で、複数のAxis装置を強化することをお勧めします。装置の設定に別のアプリケーションを使用する必要がある場合、または少数のAxis装置の強化のみが必要な場合は、VAPIX APIを使用することをお勧めします。

よくある設定ミス

注

以下に示すよくある設定ミスは、Axisデバイスの攻撃対象領域を拡大し、サイバーセキュリティ防御層を減少させる可能性があり、デバイスの悪用、誤用、または安全でない動作のリスクの増大につながります。

インターネットに露出したデバイス
CSC #12：ネットワークインフラストラクチャーの管理

Axis装置をパブリックWebサーバーとして公開したり、その他の方法で未知のクライアントに装置へのネットワークアクセスを許可したりすることはお勧めしません。詳細については、を参照してください。

非常に一般的なパスワード
CSC #4：企業の資産とソフトウェアのセキュアな設定
CSC #5：アカウント管理

すべての装置に共通のパスワードを使用するのではなく、装置ごとに固有のパスワードを使用することを強くお勧めします。手順については、とを参照してください。

匿名アクセス
CSC #4：企業の資産とソフトウェアのセキュアな設定
CSC #5：アカウント管理

匿名ユーザーがログイン認証情報を提供せずに装置のビデオや設定にアクセスできるようにすることはお勧めしません。詳細については、を参照してください。

安全な通信の無効化
CSC #3：データ保護

パスワードが暗号化されずに転送されるHTTPや基本認証など、セキュアでない通信およびアクセス方法を使用して装置を操作することはお勧めしません。詳細については、を参照してください。推奨設定については、を参照してください。

古いAXIS OSバージョン
CSC #2：ソフトウェア資産のインベントリと管理

LTSまたはアクティブトラックのいずれかで、利用可能な最新のAXIS OSバージョンを使用してAxis装置を操作することを強くお勧めします。どちらのトラックでも、最新のセキュリティパッチとバグ修正が提供されます。詳細については、を参照してください。

VAPIX APIによる基本的な強化

VAPIX APIを使用すると、で説明されているトピックに基づいてAxis装置を強化できます。この表では、Axis装置のAXIS OSバージョンに関係なく、すべての基本的な強化設定を見つけることができます。

セキュリティを強化するために一部の機能が削除されたため、装置のAXIS OSバージョンでは一部の設定が使用できなくなっている可能性があります。VAPIX呼び出しを発行したときにエラーが発生した場合は、その機能がAXIS OSバージョンで使用できなくなっていることを示している可能性があります。

目的	VAPIX API呼び出し
*使用していないネットワークポートでのPOEを無効にする**	`http://ip-address/axis-cgi/nvr/poe/setportmode.cgi?port=X&enabld=no`
*使用していないネットワークポートでのネットワークトラフィックを無効にする***	`http://ip-address/axis-cgi/network_settings.cgi { "apiVersion": "1.17", "method": "setDeviceConfiguration", "params": { "deviceName": "eth1.1", "staticState": "down" } }`
Bonjour検出プロトコルを無効にする	`https://ip-address/axis-cgi/param.cgi?action=update&Network.Bonjour.Enabled=no`
UPnP検出プロトコルを無効にする	`https://ip-address/axis-cgi/param.cgi?action=update&Network.UPnP.Enabled=no` `https://ip-address/axis-cgi/param.cgi?action=update&Network.UPnP.NATTraversal.Enabled=no`
WebService検出プロトコルを無効にする	`https://ip-address/axis-cgi/param.cgi?action=update&WebService.DiscoveryMode.Discoverable=no`
ワンクリッククラウド接続 (O3C) を無効にする	`https://ip-address/axis-cgi/param.cgi?action=update&RemoteService.Enabled=no`
装置のSSHメンテナンスアクセスを無効にする	`https://ip-address/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no`
装置のFTPメンテナンスアクセスを無効にする	`https://ip-address/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no`
ARP-Ping IPアドレス設定を無効にする	`https://ip-address/axis-cgi/param.cgi?action=update&Network.ARPPingIPAddress.Enabled=no`
Zero-Conf IPアドレス設定を無効にする	`http://ip-address/axis-cgi/param.cgi?action=update&Network.ZeroConf.Enabled=no`

HTTPSのみを有効にする	`https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.admin=https`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.operator=https`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.viewer=https`

TLS 1.2およびTLS 1.3のみを有効にする	`https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS1=no` `https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS11=no`

目的	VAPIX API呼び出し
TLS 1.2セキュア暗号の設定	`https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.Ciphers=ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384`

*総当たり攻撃からの保護を有効にする****	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.ActivatePasswordThrottling=on`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSBlockingPeriod=10`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageCount=20`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageInterval=1`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteCount=20`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteInterval=1`

スクリプトエディター環境を無効にする	`https://ip-address/axis-cgi/param.cgi?action=update&System.EditCgi=no`
ユーザーアクセスログの向上を有効にする	`https://ip-address/axis-cgi/param.cgi?action=update&System.AccessLog=On`
ONVIF再生攻撃からの保護を有効にする	`https://ip-address/axis-cgi/param.cgi?action=update&WebService.UsernameToken.ReplayAttackProtection=yes`
装置のWebインターフェースへのアクセスを無効にする	`https://ip-address/axis-cgi/param.cgi?action=update&System.WebInterfaceDisabled=yes`
HTTP/OpenSSLサーバーヘッダーを無効にする	`https://ip-address/axis-cgi/param.cgi?action=update&System.HTTPServerTokens=no`

匿名ビューアとPTZアクセスを無効にする	`https://ip-address/axis-cgi/param.cgi?action=update&root.Network.RTSP.ProtViewer=password`
	`https://ip-address/axis-cgi/param.cgi?action=update&root.System.BoaProtViewer=password`
	`https://ip-address/axis-cgi/param.cgi?action=update&root.PTZ.BoaProtPTZOperator=password`

目的	VAPIX API呼び出し
ACAPアプリケーションを必要とするroot権限のインストールを防ぐ	`http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowRoot&value=false`
署名なしACAPアプリケーションのインストールを防ぐ	`http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowUnsigned&value=false`

*「port=X」の「X」を実際のポート番号に置き換えます。例：「port=1」とすると、ポート1が無効化されます。「port=2」とすると、ポート2が無効化されます。
**「eth1.1」の「1」を実際のポート番号に置き換えます。例：「eth1.1」とすると、ポート1が無効化されます。「eth1.2」とすると、ポート2が無効化されます。
*** 1秒以内にログイン試行の失敗が20回発生すると、クライアントIPアドレスが10秒間ブロックされます。30秒のページ間隔内で後続のリクエストが失敗するたびに、DoSブロック期間がさらに10秒延長されます。

AXIS Device Manager (Extend) による基本的な強化

AXIS Device ManagerとAXIS Device Manager Extendを使用して、で説明されているトピックに基づいてAxis装置を強化できます。この設定*ファイル*を使用します。その設定は、にリストされているものと同じです。

セキュリティを強化するために一部の機能が削除されたため、装置のAXIS OSバージョンでは一部の設定が使用できなくなっている可能性があります。AXIS Device ManagerとAXIS Device Manager Extendは、これらの設定を自動的に強化設定から削除します。

注

設定ファイルをアップロードすると、Axis装置はHTTPSのみに設定され、Webインターフェースは無効になります。パラメーターを削除または追加するなど、必要に応じて設定ファイルを変更できます。

セキュリティ通知

Axis製品、ソリューション、サービスで新たに発見された脆弱性や、Axis装置をセキュアに保つ方法に関する情報を受け取るには、*Axisセキュリティ通知サービス*に加入することをお勧めします。