AXIS Device Managerによるセキュリティ制御

バージョン1.0

目次

1. イントロダクション

サイバーセキュリティの重要性は監視とセキュリティの分野でますます大きくなっています。効果的なサイバーセキュリティには、防御の深度を確保して、選択する製品や連携するパートナーからお互いに設定する要件に至るまで、あらゆるレベルでIPネットワークを保護することが必要です。

1.1 サイバーセキュリティ保護における3つの層

Axisは次の3つの層から成るサイバーセキュリティ保護を提供します。

1.セキュリティ管理: 直面している脅威を軽減するために必要なセキュリティ管理を適用する必要があります。これは、セキュリティ制御とコストパフォーマンスが高い管理の2つの部分に分けることができます。セキュリティ制御とは、物理的特性、情報、コンピューターシステム、その他の資産に対するセキュリティリスクを回避、検知、抑止、または最小化するために利用される保護手段や対策のことです。

2.脆弱性の管理: これには、悪用されかねない欠陥のリスクを最小化するため、Axisが製品の設計、開発およびテストにサイバーセキュリティのベストプラクティスを適用する際に行うすべての措置が含まれます。Axisは発見された脆弱性を管理し、重大な脆弱性の場合は直ちに修正してセキュリティ勧告を発行します。

3.学習および連携: これは、Axis、お客様、およびお客様のIPネットワークに関わるパートナー様が、直面している脅威、その潜在的な影響、ネットワークを保護する方法に関する明確な共通理解を得て共有することです。

1.2 本書の目的

本アプリケーションガイドでは、AXIS Device Managerを使用してシステムを強化し、セキュリティを高める方法を説明しています。本書は主要な側面に焦点を合わせると同時に、推奨事項を示しています。

1.3 AXIS Device Managerについて

AXIS Device Managerは、設置、セキュリティ、保守といった主要なデバイス管理タスク（下図を参照）をすべて管理するための簡単でコストパフォーマンスが高く安全な方法を提供するオンプレミスのツールです。これは、1つの場所にある最大数千台のAxisデバイス、または複数の場所にあるさらに多くのデバイスを管理するのに適しています。AXIS Device Managerを使用すると、サイバーセキュリティ制御を効率的に展開し、ネットワークデバイスをセキュリティインフラストラクチャに合わせて保護できます。

デバイス管理機能、AXIS Device Manager

設置	保守
> IPアドレスを設定 > デバイスリストをエクスポートして資産を追跡する* > ユーザとパスワードの管理* > ACAPの管理 > ファームウェアのアップグレード* > HTTPS証明書の管理* > IEEE 802.1X証明書の配布* > デバイスへのタグの割り当て	> 装置のステータス > デバイスデータの収集 > デバイスを設定し、複数のデバイスに設定をコピーする > 複数のサーバー/システムへの接続 > 復元ポイント > 工場出荷時の設定を復元する > デバイスの交換 > 証明書の更新と管理* > サイバーセキュリティの強化*

*はサイバーセキュリティ制御に関する機能を示します

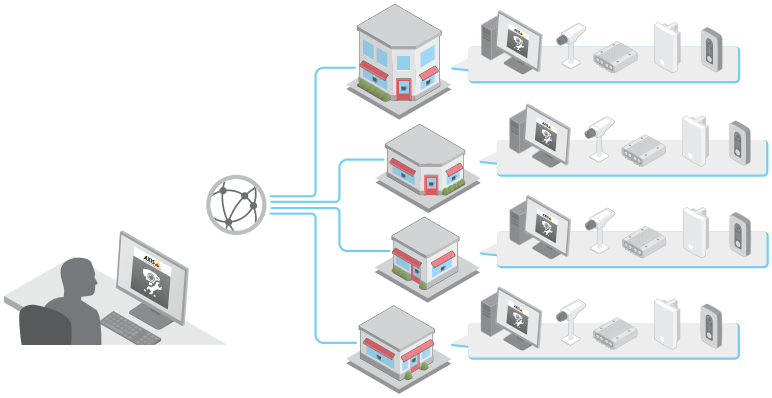


図1. 複数の設置場所の管理

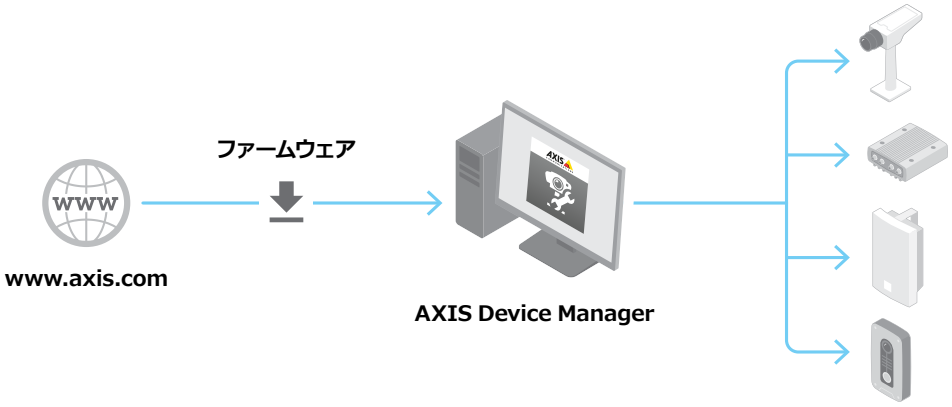


図2. ファームウェアのアップグレード

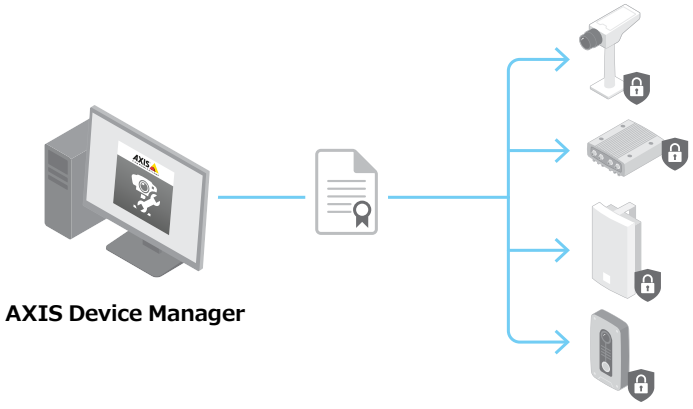


図3. 証明書の管理

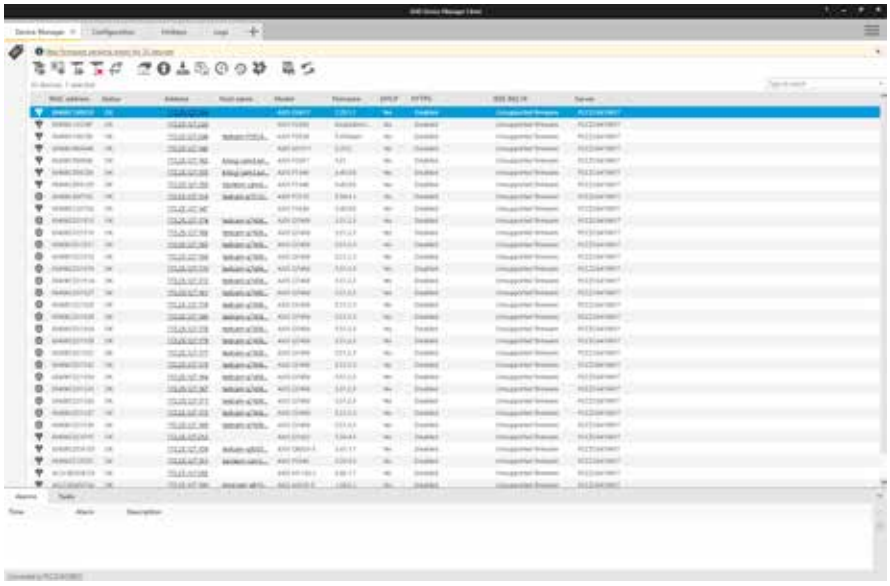
2. デバイスのインベントリ

エンタープライズネットワークのセキュリティ確保における基本的な側面のひとつは、ネットワーク上のデバイスの完全なインベントリを維持することです。全体的なセキュリティポリシーの作成や確認を行う際、重要な資産だけでなく各デバイスに関する知識と明瞭なドキュメントを保持していることが大切です。なぜなら、見落としたデバイスが攻撃者の侵入手段となる可能性があるためです。見落としたデバイスや十分に把握していないデバイスを保護することはできません。

デバイスのインベントリは、エンタープライズネットワークの保護において不可欠なステップとなります。AXIS Device Managerは、次の点で役立ちます。

> 監査や事故応答者と共に作業する際にネットワークデバイスの現在の完全なインベントリに簡単にアクセスできます
> デバイスの完全なリストを取得し、合計数、種類、モデル番号などによって並べ替えることができます
> ネットワーク上の各デバイスのステータスを確認できます

推奨事項
AXIS Device Managerには、Axisネットワークデバイスのリアルタイムのインベントリに自動的にアクセスする手段が備わっています。デバイスを自動的に識別し、リストを表示して並べ替えることができます。重要な機能として、タグを使用し、独自の条件に基づいてデバイスをグループ化したり並べ替えたりできます。これにより、容易にネットワーク上のすべてのAxisデバイスの概要を把握してドキュメント化することができます。



AXIS Device Managerではデバイスのインベントリが分かりやすく表示されます。

3. アカウントとパスワードに関するポリシー

認証と権限の制御は、ネットワークリソースの保護において重要な部分です。ポリシーを実装することは、比較的長い期間において不意または意図的な誤用のリスクを減らすのに役立ちます。ひとつの主要な部分は、パスワード侵害のリスクを減らすことです。強力なパスワードを設定することは重要ですが、デバイスパスワードは組織内で拡散する可能性があります。その場合、パスワードを入手できる人物を制御することはできなくなります。AXIS Device Managerを使用すると、Axisデバイスの複数のアカウントとパスワードを容易に管理できます。

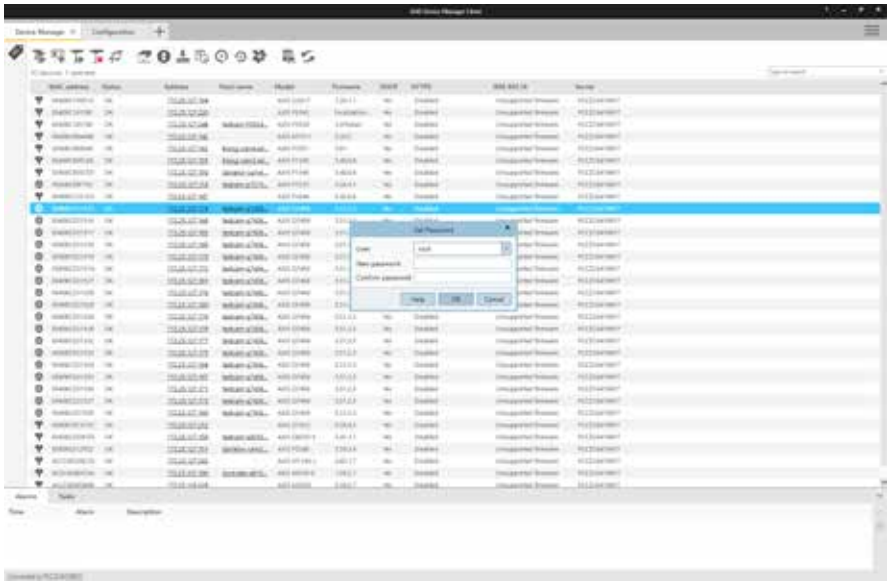
デバイス内で複数のユーザーアカウントを持つ必要がある理由
> 異なるユーザータイプ (マシンと人間) の権限レベルを制御できる
> root (マスター) パスワードが侵害されるリスクを減らすことができる
> あるユーザータイプの認証情報を、他のユーザーに影響を与えずにリセットできる

AXIS Device Managerにおける権限の処理
AXIS Device Managerでは、Axisデバイスの複数アカウントがサポートされており、各アカウントは3種類の権限レベルである閲覧者、オペレーター、管理者に分類されます。各権限がAxisネットワークカメラ用に管理できる内容は次のとおりです。

閲覧者権限を持つユーザーは、映像にアクセスしてPTZを制御できます。オペレーター権限を持つユーザーは、カメラの設定とビデオストリームプロファイルを最適化できます。管理者は、アカウントの管理、ネットワーク設定の変更、デバイス内の複数のサービスの制御を行うことができます。カメラにアクセスする権限ごとに独自のアカウントが必要です。

推奨する手順

> カメラをVMSに追加する前に、AXIS Device Managerに追加することをお勧めします。
> AXIS Device Managerで、すべてのカメラを選択し、「vms」または類似した名前の新しいユーザーアカウントを作成して強力なパスワードを設定します。権限はVMSの要件に合わせる必要があり、オペレーターまたは管理者にすることができます (メーカーにお問い合わせください)。
> 定義した「vms」アカウントとパスワードを指定して、デバイスをVMSに追加します。
> AXIS Device Managerに戻り、すべてのカメラを再び選択して、「root」アカウントのパスワードを新しい強力なパスワードにリセット (変更) します。「root」アカウントのパスワードは限られた数の個人 (AXIS Device Managerのユーザー) だけが知っている必要があります。
> 組織内のだれかが保守またはトラブルシューティングタスク用にWebブラウザー経由でデバイスにアクセスしなければならない場合は、rootパスワードを与えないようにします。AXIS Device Managerを使用して、選択したデバイス用に管理者またはオペレーターの権限を持つ新しい (一時的な) アカウントを作成します。タスクが完了したら、AXIS Device Managerを使用して一時アカウントを削除します。
> AXIS Device Managerでは、ローカル管理者に加えてドメインユーザーとグループがサポートされます。AXIS Device Managerサーバーをホストするマシンだけを使用してAXIS Device Managerクライアントにアクセスする場合は、ローカル管理者を使用できます。システムを保守するユーザーがリモートクライアントを使用する場合は、ドメインユーザーの使用をお勧めします。



AXIS Device Managerにおけるユーザー権限とパスワードの変更。

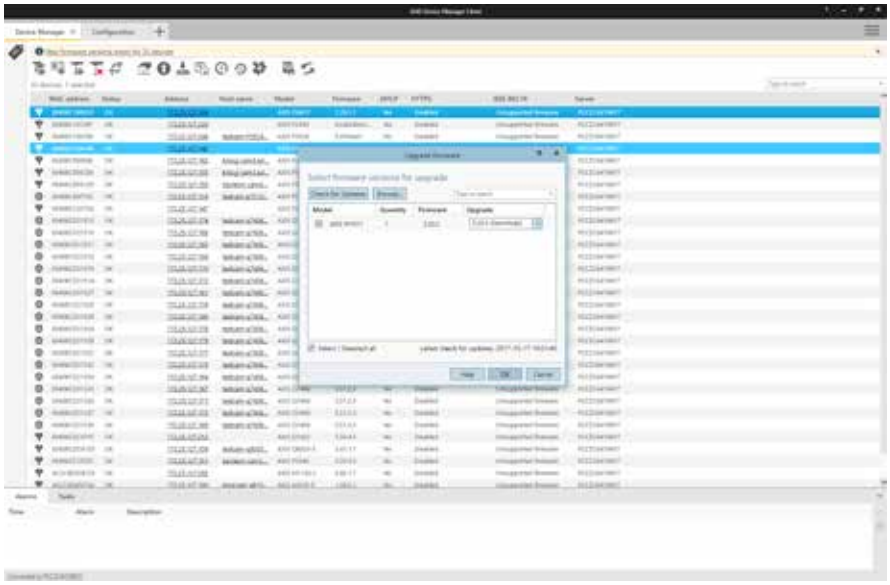
4. ファームウェアのアップグレード

最新のファームウェアには既知の脆弱性に対するパッチが含まれています。攻撃者は既知の脆弱性を利用しようとする場合があるため、常に最新のソフトウェアを使用することは不可欠です。重要な点として、新しいファームウェアを迅速に展開することにより、運用能力が向上し、新しいリリースアップグレードを手動でロールアウトする際のボトルネックがなくなります。AXIS Device Managerはwww.axis.comに接続し、最新の適用可能なファームウェアやサービスリリースをダウンロードします。インターネットからネットワークに直接ダウンロードすることを望まない場合は、アップグレードをUSBスティックに保存した後でAXIS Device Managerクライアントにアップロードできます。また、新しいファームウェアが入手可能かどうかが表示されるため、Axisデバイスへの素早い展開を実行できます。

常に最新のファームウェアバージョンを実行する必要がある理由

> ネットワークとデバイスは、既知の脆弱性 (特に、重大な脆弱性) に対する最新のパッチによって保護されます

> デバイスが更新されることにより、最新のパフォーマンス改善が適用されると共に既知のバグや欠陥が解決されます
> 最新の機能や機能拡張に即座にアクセスできます



AXIS Device Managerによるファームウェアのアップグレードは、画面上の通知と直感的なダイアログボックスによってシンプルに行うことができます。

5. さらに強化する方法

適切なユーザー/パスワードのポリシーに加え、最新のファームウェアバージョンを適用したデバイスの実行により、デバイスの一般的なリスクは軽減されます。『Axis強化ガイド』では、大規模な組織や重要な組織でリスクを減らすためのその他の方法を説明しています。これは、使用が許可されていないサービスの無効化と、攻撃や侵入の兆候を検知して監視するのに役立つサービスの有効化が含まれます。

AXIS Device Managerにより、これらのポリシーを展開するプロセスは簡単になります。Axisでは、基本的な推奨設定用の設定テンプレートを提供しています。詳細については、次のURLをご覧ください。
www.axis.com/products/axis-device-manager/support-and-documentation.

Axis強化ガイドに従ってデバイスを強化する方法
> www.axis.com/products/axis-device-manager/support-and-documentationから強化テンプレート設定ファイルをダウンロードします
> 設定ファイルを編集し、該当する項目を選択します
> デバイスを選択します
> 右クリックして、[Configure Devices | Configure… (デバイスの設定 | 設定…)] を選択します
> [Configuration File (設定ファイル)] をクリックして、ダウンロードしたファイルを選択します
> 必要に応じて設定を調整します

6. 認証局サービス

認証局 (CA) は、デジタル証明書をサーバー、クライアント、ユーザーに発行するサービスです。CAにはパブリックCAとプライベートCAがあります。通常、ComodoやSymantec (旧Verisign) などのパブリックに信頼されたCAは、パブリックWebサイトや電子メールなどのパブリックサービスに使用されます。

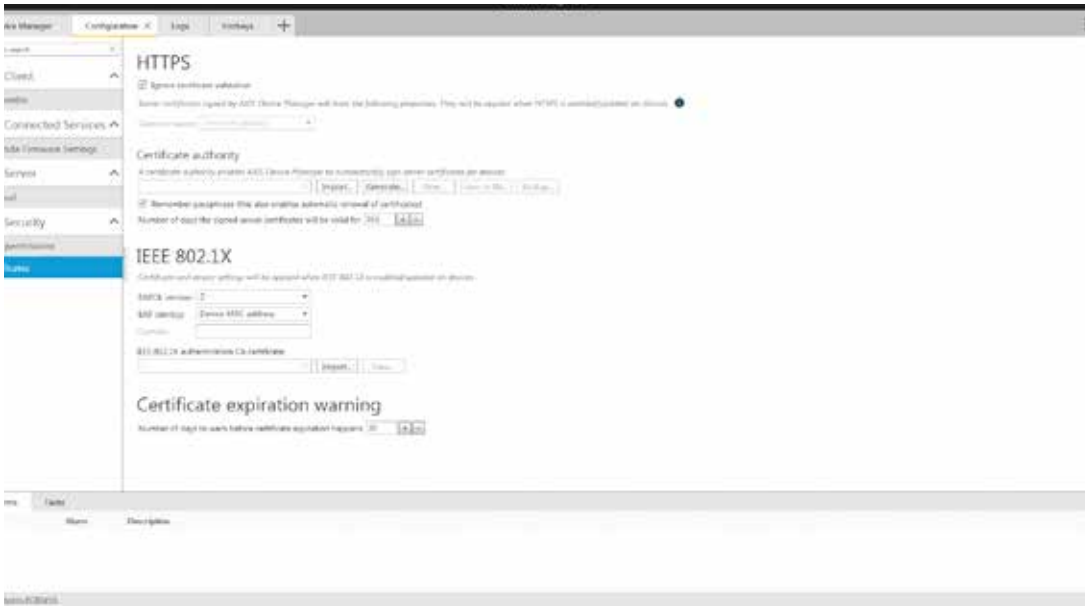
プライベートCA (通常はアクティブディレクトリ/証明書サービス) は、社内/プライベートネットワークサービス用の証明書を発行します。映像管理システムでは、これは主にHTTPS (Hyper Text Transfer Protocol Secure) (ネットワークの暗号化) とIEEE 802.1X (ネットワークアクセス制御) に使用されます。AXIS Device ManagerにはAxisデバイス用のCAサービスが含まれており、プライベートルートCAまたはプライベート中間CA (エンタープライズPKI (Public Key Infrastructure) の一部) として動作できます。

CA署名証明書は、IEEE 802.1X (クライアント) とHTTPS (サーバー) の両方の証明書に使用されます。

HTTPS
HTTPSは安全なバージョンのHTTPであり、クライアントとサーバーの間の通信が暗号化されます。自己署名証明書により、十分な暗号化接続が実現されます。自己署名証明書とCA署名証明書の間で、暗号化レベルに違いはありません。異なるのは、自己署名証明書では攻撃者のコンピューターが正当なサーバーのふりをしようとするネットワークなりすましに対する保護が行われないことです。CA署名証明書では、アクセス先が信頼されたデバイスであることをクライアントが認証するための信頼ポイントが追加されます。映像を暗号化するには、ビデオクライアント (VMS) でHTTPSによる映像のリクエスト (RTP over RTSP over HTTPS) がサポートされている必要があります。

IEEE 802.1X
802.1Xとも呼ばれるこの標準は、許可されていないネットワークデバイスがローカルネットワークにアクセスすることを防止します。ネットワーク (およびそのリソース) へのアクセスを許可される前に、デバイスは自身を認証する必要があります。MACアドレス　(MACフィルタリング)、ユーザー/パスワード、クライアント証明書などの様々な認証方法を使用できます。使用する方法はシステムの所有者が決定します。選択する方法は脅威、リスク、コストによって異なります。

802.1Xインフラストラクチャの運用はひとつの投資であり、マネージドスイッチと追加サーバー（通常はRADIUS (Remote Authentication Dial-In User Service)) が必要です。クライアント証明書を使用するには、クライアント証明書を発行できるCA（プライベートまたはパブリック）が必要です。ほとんどの場合、このインフラストラクチャには保守または監視する人員が必要です。



AXIS Device Managerにおける証明書の設定。

7. 証明書ライフサイクルの管理

証明書ライフサイクルの管理は、証明書の発行、インストール、検査、修正、更新に関係するすべてのプロセスとタスクを長期間にわたってコスト効率に優れた方法で処理する手段のひとつです。AXIS Device Managerでは、管理者が次の処理を行うことを許可することによって証明書を効率的に管理できます。

> 別のCAが利用できない場合にCA署名証明書を発行する
> IEEE 802.1X証明書を容易に配布する
> HTTPS証明書を容易に展開する
> 証明書の有効期限を監視する
> 証明書を有効期限の前に容易に更新する

プライベートルートCAとプライベート中間CAに関する推奨事項
Axisデバイスを一般人向けのパブリックサーバーとして公開することは推奨されていません。そのため、パブリックCAをプライベートリソース用に使用することはコストパフォーマンスが良くありません。

HTTPSの場合、信頼されたカメラにアクセスしていることを検証する必要があるクライアントはVMSサーバーだけです。ライブおよび録画された映像はVMSサーバーから提供されるため、オペレータークライアントがカメラに直接アクセスすることはありません。この状況では、カメラサーバー証明書を既存のエンタープライズPKIに組み込むことの価値は限定的なものとなります。

AXIS Device ManagerをプライベートCAとして使用するのは、最もコストパフォーマンスが優れたソリューションです。ルートCA証明書が生成された後、AXIS Device Manager証明書をVMSサーバーの証明書ストアにインストールしてください。他のクライアントが(保守やトラブルシューティングのために) カメラに直接アクセスする場合は、それらのクライアントにもAXIS Device ManagerルートCAをインストールします。

802.1Xの場合、カメラには自身をRADIUSサーバーに認証するためのクライアント証明書が必要です。エンタープライズPKI/CAの管理者に依頼して中間CA証明書を生成した後、AXIS Device Managerにインストール可能なPKCS#12 (P12) 証明書としてエクスポートしてください。

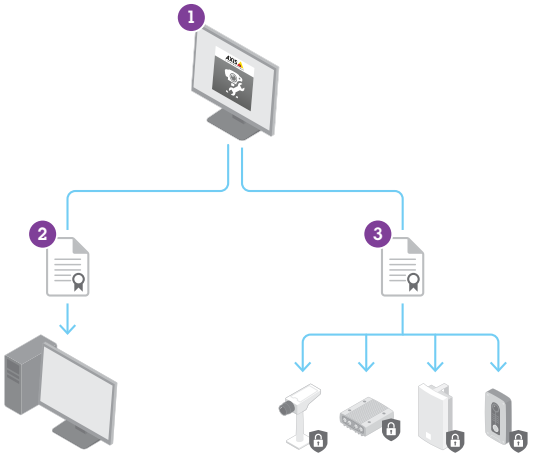


図4、左: HTTPS証明書の管理に含まれる事柄:
1) AXIS Device Managerで中間またはルートCA証明書を生成する。2) CA証明書をVMSにエクスポートする。3) サーバー証明書をデバイスにアップロードする。

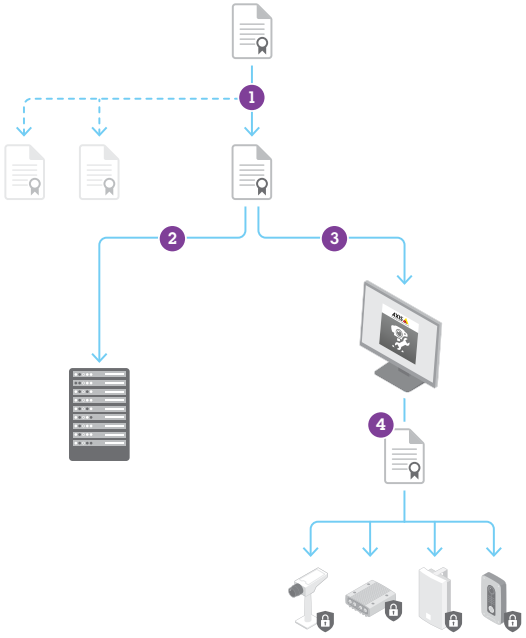


図5、右: IEEE 802.1X証明書の配布に含まれる事柄: 1) 中間CAおよびクライアント証明書を生成する。2) CA証明書をRADIUSサーバーにインストールする。3) AXIS Device ManagerでCA証明書をインポートする。4) CAおよびクライアント証明書をデバイスにアップロードする。

8. まとめ

セキュリティ管理とセキュリティ制御は、効果的なサイバーセキュリティアプローチの実装における重要な部分です。これらはいずれも継続的なプロセスであり、IPネットワークに影響を与える可能性のある潜在的な脅威を軽減するため、明瞭なステータスを維持し、適切な処置を実施する必要があります。AXIS Device Managerは、デバイスを管理すると同時にネットワークのセキュリティを高めることのできるツールです。詳細やサポートについては、お近くのAxis代理店にお問い合わせいただくか、www.axis.comをご覧ください。

Axis Communicationsについて

Axisは、インテリジェントなセキュリティソリューションを通じて、よりスマートで安全な環境の実現を目指しています。ネットワークビデオ市場をけん引するリーダーとして、Axisはオープンプラットフォームを基盤とした革新的なネットワーク製品を次々と開発し、製品化しています。また、パートナーとのグローバルな連携体制を通じて、お客様に高い価値を提供します。Axisでは、長年にわたってパートナーと協力関係を築いてきました。こうしたパートナーに向け、Axisは蓄積された知見と、既存および新規市場における画期的なネットワーク製品を提供しています。

また、世界の50か国以上に2,700人を超える熱意にあふれた従業員を擁し、9万社以上のパートナーから成るグローバルネットワークに支えられています。1984年に設立されたAxisはスウェーデンに本社を置き、NASDAQ Stockholmに株式上場しています（ティッカーシンボルAXIS）。

より詳しい情報はwww.axis.comをご覧ください。