ホワイトペーパー

Axis Edge Vault

以下の機能により、Axisデバイスの保護を実現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：

— サプライチェーンの保護

— 高信頼性のデバイスID

— 安全な鍵の保管

— ビデオ改ざん検知

4月 2024

概要

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「Axis Edge Vault」により、Axisデバイスを保護することができます。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により、*セキュアブートと署名付きOS*(署名付きオペレーティングシステム) によって確立される強力なRoT（信頼の基点）が確実に実現します。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。

Edge Vaultを搭載したAxisデバイスは、機密情報の盗聴や悪質な抽出を防止することで、お客様がサイバーセキュリティのリスクにさらされることを最小限に抑えます。また、Axis Edge Vaultにより、顧客ネットワーク上でAxisデバイスを信頼して使用することができます。

Axis Edge Vaultサイバーセキュリティプラットフォーム

暗号コンピューティングモジュール	機能	ユースケース
• セキュアエレメント • TPM 2.0 • SoCセキュリティ（TEE）	• セキュアブート • 署名付きOS • AxisデバイスID • 安全なキーストア • 署名付きビデオ • EFS（暗号化ファイルシステム）	• サプライチェーンの保護 • 高信頼性のデバイスID • 安全な鍵の保管 • ビデオの改ざん検知

- **サプライチェーンの保護**：Axis Edge Vaultを有効に機能させるには、RoTとして機能する安全な基盤が必要となります。セキュアブートと署名付きOSがなければ、RoTチェーンを確立することはできません。セキュアブートと署名付きOSの組み合わせにより、暗号で検証されたソフトウェアのチェーンが途切れることがありません。このチェーンは不変メモリ（ブートROM）から始まります。セキュアブートにより、署名付きOS以外ではデバイスを起動できなくなるため、サプライチェーンにおける物理的な改ざんを防止することができます。署名付きOSの場合は、デバイスで新しいデバイスソフトウェアが検証されてからインストールが受け付けられるようになります。完全性が損なわれていること、またはデバイスソフトウェアがAxisによって署名されていないことがデバイスで検知されると、アップグレードは拒否されます。これにより、ソフトウェアの改ざんからデバイスを保護することができます。
- **高信頼性のデバイスID**：デバイスIDの信頼性を確立するには、デバイスの出所を確認できることが鍵となります。Axis Edge Vaultを搭載したデバイスには、生産工程で、工場でプロビジョニングされ、国際規格（IEEE 802.1AR）に準拠した一意のAxisデバイスID証明書が割り当てられます。これがデバイスの出所を証明するパスポートのような役割を果たします。デバイスIDは、Axisルート証明書により署名された証明要素として、セキュリティで保護されたキーストアに安全かつ永続的に格納されます。安全な自動デ

バイスオンボーディングや安全なデバイス識別を目的として、顧客のITインフラストラクチャーでデバイスIDを活用することができます。

- **安全なキーの格納**：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。安全なキーストアにより、Axisデバイス ID や顧客がロードした暗号化情報が保護されるだけでなく、セキュリティ侵害が発生した場合も、不正アクセスや悪質な抽出を防止することができます。
- **ビデオ改ざん検知**：署名付きビデオにより、ビデオファイルの管理のチェーンを証明することなく、映像の証拠が改ざんされていないことを確認できるようになります。セキュリティで保護されたキーストアに安全に格納されている独自のビデオ署名キーにより、各カメラのビデオストリームに署名が追加されます。ビデオが再生されると、Axis の *ファイルプレーヤー* にビデオが改ざんされていないかどうかが表示されます。ビデオに署名が付いていることで、映像を元のカメラまで遡って追跡し、映像がカメラから出た後に改ざんされていないことを確認することが可能となります。

目次

1 はじめに

Axisは業界のベストプラクティスに従って、自社製品にセキュリティを実装しています。これにより、顧客のサイバーセキュリティリスクを最小限に抑えられるだけでなく、顧客ネットワーク内でAxisデバイスを信頼して使用できるようになります。

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「Axis Edge Vault」により、Axisデバイスを保護することができます。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。

本ホワイトペーパーでは、Axisエッジデバイスセキュリティにおける多層アプローチの概要を提示し、一般的なリスクとその防止方法についてご説明します。Axis Edge Vaultを有効に機能させるには、RoTとして機能する安全な基盤が必要となります。そこで、サプライチェーンにおけるAxisデバイスのセキュリティ面を取り上げ、署名付きOS (署名付きオペレーティングシステム) とセキュアブートにより、ソフトウェアの改ざんとサプライチェーンにおける物理的な改ざんを実質的に防止できる理由についてもご説明します。

*https://www.axis.com/support/cybersecurity/resources*には、製品のセキュリティ、公開されている脆弱性、一般的な脅威リスクを軽減するために講じることができる対策に関する詳細情報が記載されています。

本ホワイトペーパーの最終章には、用語集が記載されています。

2 サプライチェーンの保護

Axis Edge Vaultを有効に機能させるには、RoTとして機能する安全な基盤が必要となります。RoTの構築は、デバイスの起動プロセスから始まります。Axisデバイスでは、ハードウェアベースのメカニズム「*セキュアブート*」により、デバイスの起動元となるオペレーティングシステム（AXIS OS）が検証されます。AXIS OSは、ビルドプロセス時に*署名付きOS*を使用して暗号で署名されます。

セキュアブートと署名付きOSは相互に連動しています。これにより、デバイスが展開される前に（デバイスに物理的にアクセスできる人物によって）オペレーティングシステムまたはデバイスソフトウェアが改ざんされていないことが保証されます。また、展開後、侵害された、またはコード署名が付いていないソフトウェアの更新はデバイスにインストールできなくなります。確実に安全な操作を実現するには、暗号で検証されたソフトウェアのチェーンが途切れることのないCoTを確立する必要があります。セキュアブートと署名付きOSの組み合わせにより、これが可能となるのです。

2.1 セキュアブート

セキュアブートとは、暗号で検証されたソフトウェアのチェーンが途切れることのないブートプロセスを実現するメカニズムです。このチェーンは不変メモリ（ブートROM）から始まります。セキュアブートにより、デバイスは承認されたオペレーティングシステムでのみ起動できるようになります。

ブートローダーを検証するブートROMにより、起動プロセスが開始します。その後、セキュアブートはフラッシュメモリから読み込まれた各ソフトウェアコンポーネントについて、組み込まれている署名をリアルタイムで検証します。RoTとして機能するブートROMにより、各署名が検証された場合にのみ、ブートプロセスが続行します。それぞれの

チェーンの部分により次の部分が認証されます。結果として、最終的にLinuxカーネルとルートファイルシステムが検証されるという仕組みです。

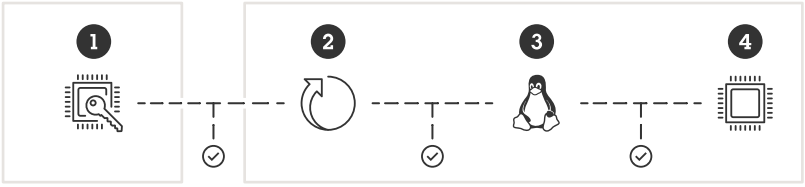

Figure 1. セキュアブートプロセスでは、チェーンの各部分により次の部分が認証されます。これにより、最終的にルートファイルシステムが検証されることになります。

1 *SoCのブートROM（RoT/信頼の基点）*
2 *ブートローダー*
3 *Linuxカーネル*
4 *ルートファイルシステム*

多くのデバイスでは、下位レベルの機能を変更できない状態に維持することが重要となります。下位レベルのソフトウェアの上に他のセキュリティメカニズムが構築されている場合、セキュアブートが安全なベースレイヤーとして機能します。これにより、そのメカニズムが保護されます。セキュアブートを搭載したデバイスの場合、フラッシュメモリにインストールされているオペレーティングシステムは変更から保護されますが、設定は保護されないままになります。セキュアブートにより、工場出荷時のデフォルト設定後も、デバイスの正常な状態が確実に維持されます。しかし、セキュアブートが有効に機能するには、ブート処理により、オペレーティングシステムがAxisによって署名されていることが検証されなければなりません。

2.2 署名付きOS

Axisの署名付きOSでは、秘密鍵を使用して、Axisによりデバイスソフトウェアイメージにコード署名が行われています。デバイスの起動時に、Axisデバイスのセキュアブートが、デバイスソフトウェアが署名されているかどうかを確認します。デバイスソフトウェアの完全性が損なわれていることをデバイスが検出した場合、デバイスは実行されません。デバイスソフトウェアをアップグレードすると、デバイスの既存の署名付きAXIS OSが、新しいAXIS OSも署名されているかどうかを自動的に確認します。署名されていない場合、アップグレードは拒否されます。

OSのコード署名プロセスは、暗号化ハッシュ値の計算を通じて開始されます。この値はその後、署名がAXIS OSイメージに添付される前に、秘密/公開鍵ペアの秘密鍵を使って署名されます。

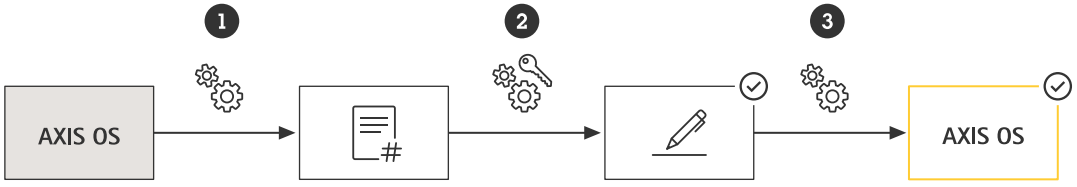

Figure 2. OSのコード署名プロセス。

1 *AXIS OSの暗号化ハッシュ値が生成されます。*

2 ハッシュと秘密鍵を組み合わせて署名が生成されます。
3 署名がAXIS OSのバージョンとバイナリに追加されます。

アップグレードの前に、新しいソフトウェア更新の真正性を検証する必要があります。このプロセスでは、Axis製品に含まれている公開鍵を使用して、ハッシュ値が実際に一致する秘密鍵で署名されていることが検証されます。また、ハッシュ値を計算し、署名の検証済みハッシュ値とこれを比較することで、完全性を検証することができます。署名が無効である場合、またはAXIS OSイメージが改ざんされている場合は、Axisデバイスの起動プロセスが中止されます。

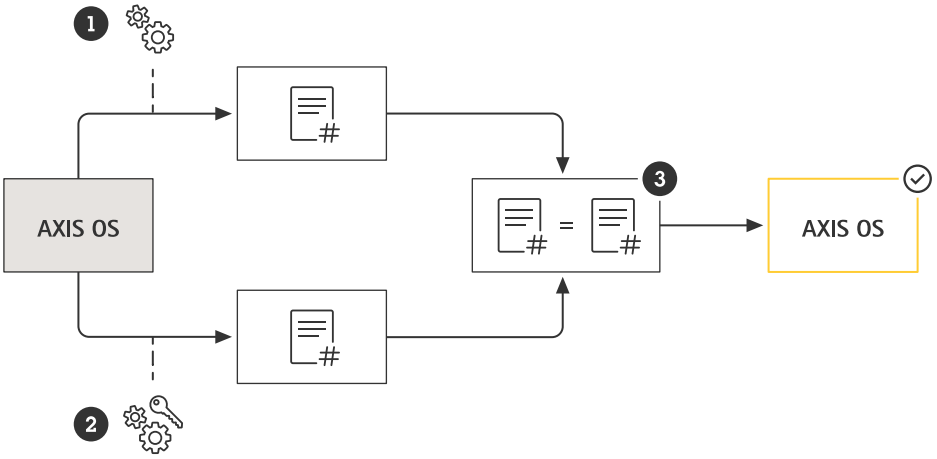

Figure 3. 署名付きOSの検証プロセス。

1 AXIS OSのハッシュ値が計算されます。
2 公開鍵を使用して、署名によりハッシュ値が確認されます。
3 結果が一致した場合にのみ、署名が正常に検証されます。

Axisの署名付きOSは、業界で広く受け入れられているRSA公開鍵暗号化方式をベースにしています。秘密鍵はAxisで厳重に守られている場所に保管され、公開鍵はAxis製品に埋め込まれています。ソフトウェアイメージ全体の完全性は、署名によって保証されています。プライマリ署名により、イメージの解凍中に検証されるいくつかのセカンダリ署名が検証されます。

テストとカスタムビルドを目的として、Axisは個々のデバイスで非生産イメージが受け入れられるメカニズムを実装しています。このイメージは、所有者とAxisの両方の承認を得て、その目的専用のキーを使用してコード署名され、カスタム署名が生成されます。承認済みデバイスに証明書をインストールすると、固有のシリアル番号とチップIDに基づいて、承認済みデバイスでのみ実行できるカスタムイメージの使用が可能となります。カスタム証明書は、署名するキーを保持しているAxisのみが作成することができます。

3 高信頼性のデバイスID

現代のニーズを満たすゼロトラストセキュリティネットワーク（どのトラフィックも決して信頼せず、常に検証するという概念）を実現するには、基本的にデバイスの出所、その信頼性、その接続を検証する機能が必要となります。ネットワークデバイスは、空港でパスポートを提示して本人確認をするのと同じような方法で、その完全性と信頼性を検証できます。

3.1 Axisデバイスによる安全なデバイス識別

国際規格「*IEEE 802.1AR*」には、ネットワークにおけるデバイス識別の自動化と保護方法が定義されています。内蔵された暗号コンピューティングモジュールに通信を転送できれば、規格に従ってデバイスから信頼性の高い識別応答を返すことができます。ネットワークインフラストラクチャーでこの高信頼性の応答を使用すれば、プロビジョニングネットワークへのデバイスのオンボーディングを自動化して保護し、デバイスの初期設定とソフトウェア更新を実施できるようになります。

IEEE 802.1ARに準拠するため、当社は生産工程において、工場でプロビジョニングされたデバイス固有のAxisデバイスID証明書（IEEE 802.1ARに準拠した初期デバイス識別子/IDevID）を大半のデバイスに組み込んでいます。AxisデバイスIDは、デバイスの暗号コンピューティングモジュールにより、セキュリティで保護された耐タンパー性のキーストアに安全に格納されます。Axisデバイスごとに一意に割り当てられているこのIDは、デバイスの出所を証明するためのものです。

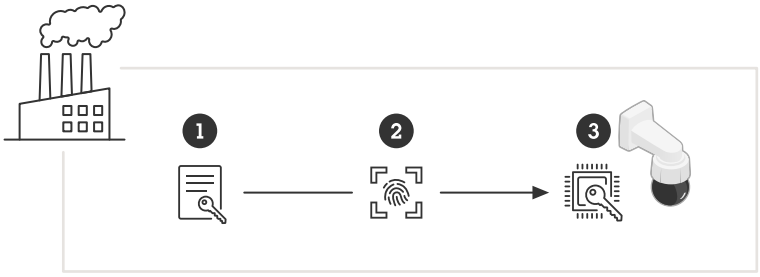

Figure 4. デバイスの製造工程において、一意のAxisデバイスID (2) がデバイスの安全なキーストア (3) に格納されます。

1. *Axisデバイスキーインフラストラクチャー（PKI）*
2. *Axisデバイス*
3. *Axisデバイス（Axisデバイスの暗号コンピューティングモジュールにより、セキュリティで保護された耐タンパー性のキーストアに安全に格納されます）*

IEEE 802.1ARは、ネットワークアクセスコントロールに関するIEEE 802.1X規格に基づいています。これにより、Axisデバイスでは、事前選択されたAxisデバイスIDがデフォルトで有効化されています。そのため、工場出荷時の状態でも802.1X対応のITインフラストラクチャーを通じてAxisデバイスの安全な識別と認証が可能となります。

Axisデバイス証明書は、さまざまな暗号化設定（2048ビットRSA、4096ビットRSA、ECC-P256）で提供されています。これはデフォルトで有効化されているため、IEEE 802.1Xネットワークアクセスコントロールと HTTPSを介して、安全なデバイスの接続と識別が実現します。

製造工程においてAxisデバイスIDを工場でプロビジョニングできるように、AxisはIEEE 802.1ARに準拠した独自の公開鍵インフラストラクチャー（PKI）を実装しています。Axisデバイスは、中間証明書によって署名されてから、Axisルート証明書による署名が行われます。ルートCAと中間CAが、地理的に離れた暗号コンピューティングモジュールにそれぞれ安全に格納されます。これにより、Axis生産施設でセキュリティ侵害が発生した場合も、悪

質な抽出を防止することができるのです。Axis PKIインフラストラクチャーの詳細については、*www.axis.com/support/public-key-infrastructure-repository*をご覧ください。

Figure 5. 製造工程でAxisデバイスIDを工場でプロビジョニングできるように、Axisは IEEE 802.1ARに準拠した公開鍵インフラストラクチャー（PKI）を実装しています。製品のシリアル番号が組み込まれた証明書であるAxisデバイスID (1) は、Axisデバイス ID中間CA (2) によって署名され、この中間CAはAxisデバイスIDルートCA (3) によって署名されます。専用のハードウェアセキュリティモジュール（HSM）は、工場での安全なプロビジョニングに使用されます。

A 照合
B 署名

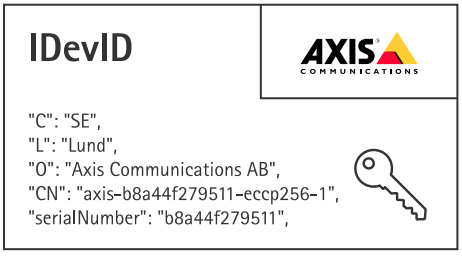

Figure 6. Axisデバイス IDの例。

3.2 安全なネットワークオンボーディング

購入したAxisデバイスには、使用を開始する前に手動で検査を実行することができます。デバイスを視覚的に検査し、Axis製品のルックアンドフィールに関する予備知識を活かせば、そのデバイスがAxis製であることを確信できるはずです。しかし、この種の検査を行うには、デバイスに物理的にアクセスできる状況が必要です。では、ネットワーク経由でデバイスと通信している場合は、正当なデバイスと通信していることをどのように確認し、そのIDを検証すればよいのでしょうか？ネットワークでつながっている機器やサーバーにインストールされているソフトウェアに対して物理的な検査を行うことはできません。この場合、まず安全にプロビジョニングできる閉じたネットワーク経由で新しいデバイスと通信することが、一般的なセキュリティ対策とされています。

AxisデバイスIDにより、そのデバイスが確かにAxis製であること、そしてデバイスへのネットワーク接続が実際にそのデバイスによるものであることを証明する暗号学的に検証可能な手段を得ることができます。IEEE 802.1Xネットワークの認証プロセス時にAxisデバイスIDを使用して、プロビジョニングネットワークにアクセスすることができます。Axisデバイスが実稼働ネットワークに移動される前に、プロビジョニングネットワークでさらなるソフトウェアの更新とAxisデバイスの設定が実行されます。

AxisデバイスIDを使用することで、デバイスのインストールと設定においてコスト効率の高い自動制御を利用できるため、全体的なセキュリティが強化されるだけでなく、デバイス展開にかかる時間を短縮することができます。

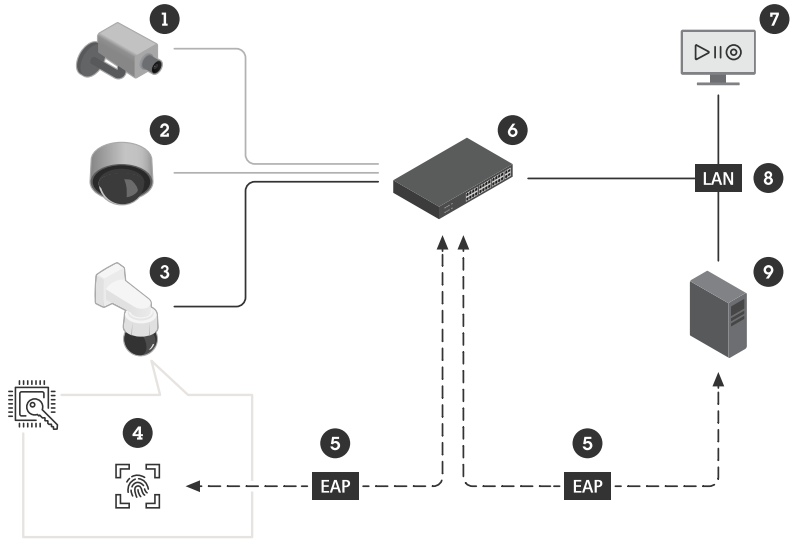

Figure 7. 安全なネットワークオンボーディング。Axisデバイス (3) がネットワーク (8) とVMS (7) で自動的に受け入れられるように認証サーバー (9) を設定することができます。これは、デバイスのシリアル番号とAxisデバイスID (4) を指紋または認証として使用することによって可能になります。

1. *承認されていないデバイス（手動でオンボードする必要があります）*
2. *サードパーティ製のデバイス*
3. *Axisデバイス*
4. *AxisデバイスID（セキュリティで保護された耐タンパー性のキーストアに安全に格納されます）*
5. *AxisデバイスID証明書によるAxisデバイスの802.1X EAP-TLSネットワーク認証*
6. *マネージドスイッチ（認証システム）*
7. *VMS（デバイス検証）*
8. *802.1Xで保護されたLAN*
9. *RADIUS（ネットワーク認証サーバー）*

Figure 8. オンボーディングプロセスに関する詳細説明。安全なデバイスIDのIEEE 802.1ARには、RADIUSサーバー (3) を使用して、IEEE 802.1X EAP要求（EAP-TLS）経由でデバイス (1) を識別し、ネットワークへのデバイスアクセスを許可する方法が定義されています。

1. *Axisデバイス*
2. *マネージドスイッチ（認証システム）*
3. *RADIUSサーバー（ネットワーク認証サーバー）*

A 新しい接続
B EAP要求ID
C EAP応答ID（AxisデバイスID証明書、IEEE 802.1AR IDevIDを含む）
D RADIUSアクセス要求
E RADIUSアクセスチャレンジ
F EAP成功

追加の内蔵の信頼ソースを提供することとは別に、AxisデバイスIDにより、デバイスを追跡する手段が得られ、ゼロトラストネットワークの原則に従って定期的な検証と認証を実現することができます。

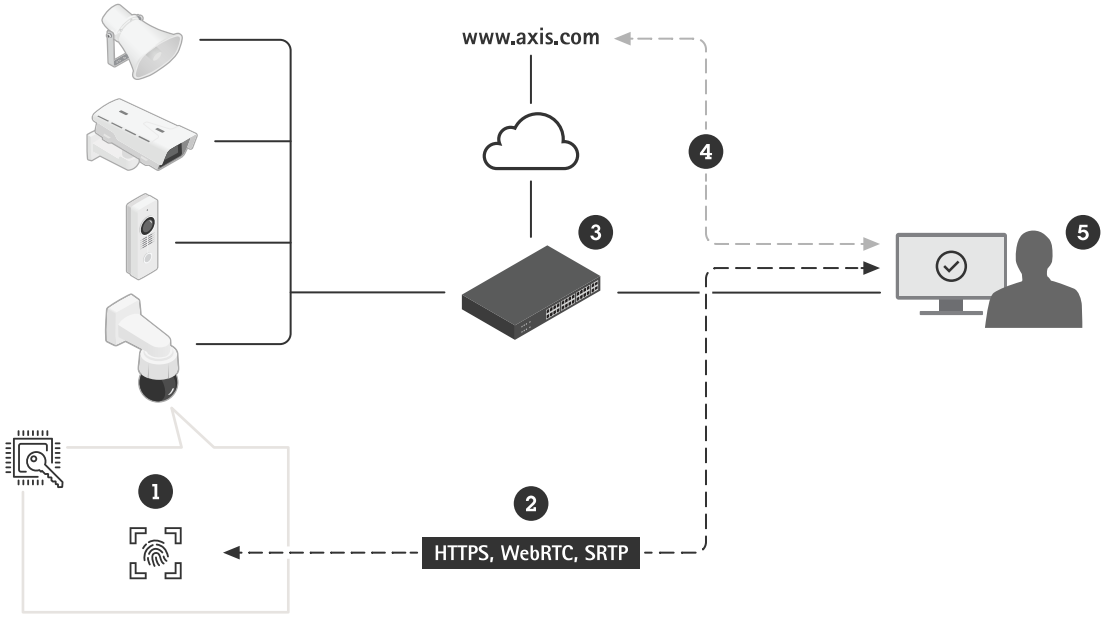

Figure 9. デバイスが安全にオンボードされると、他のシステム領域にあるソフトウェアアプリケーション (5) で、AxisデバイスID (1) と暗号化操作を使用して、さまざまなTLSベースの通信 (2) でデバイスが検証および認証されます。AxisデバイスIDは、公開されているAxisデバイスIDルートCA証明書 (4) によって検証することが可能です。

1 Axisデバイス ID（セキュリティで保護された耐タンパー性のキーストアに安全に格納されます）
2 TLSベースの通信（HTTPS、WebRTC、SRTP）
3 マネージドスイッチ
4 Axis デバイス ID ルート CA 証明書 (www.axis.com/support/public-key-infrastructure-repositoryからダウンロード可能)
5 VMSまたはその他のソフトウェア（デバイス検証）

4 安全な鍵の保管

従来から、機密性の高いX.509暗号化情報（秘密鍵）は、デバイスのファイルシステムに格納されるようになっています。これは、ユーザーアカウントのアクセスポリシーのみによって保護されます。ユーザーアカウントは簡単に侵害されるものではないため、これに

より基本的な保護が得られるわけです。しかし、セキュリティ侵害が発生すると、この暗号化情報が保護されず、攻撃者にアクセスされることになります。

セキュリティの観点から、暗号化情報を保存・保護するためには、安全なキーストアが必要となります。当社の仕組みでは、AxisデバイスIDと署名付きビデオに含まれている機密性の高い暗号化情報が安全なキーストアに格納されるだけでなく、顧客がロードした情報も同じ方法で保護することができるのです。

4.1 安全なキーストア

機密性の高い暗号化情報（秘密鍵）は、耐タンパー性能を備えたハードウェアベースの安全なデバイスのキーストアに格納されます。そのため、万が一セキュリティ侵害が発生しても、悪質な抽出を防止することができます。また、秘密鍵は使用中であっても、安全なキーストアにより継続的に保護されます。攻撃者は安全なキーストアにアクセスすることはできません。また、ネットワークトラフィックの傍受、IEEE 802.1Xキー経由でのネットワークへのアクセス、他の秘密鍵の抽出を行うこともできません。

ハードウェアベースの暗号コンピューティングモジュールを通じて、安全なキーストアが実現します。セキュリティ要件に応じて、Axisデバイスには、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。

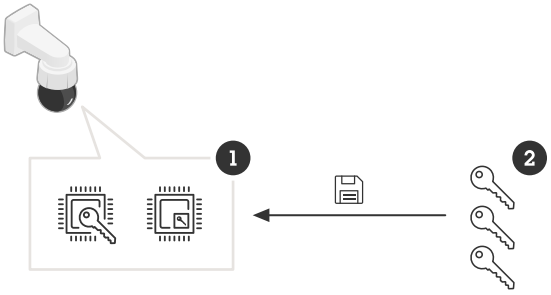

Figure 10. 安全なキーストア (1) により、秘密鍵 (2) が保護され、暗号化操作を安全に実行することができます。

1 *安全なキーストア（セキュアエレメント、TPM、[SoCの] TEEなど）*
2 *秘密鍵（AxisデバイスID、ビデオ署名キー、アクセスコントロールキー、ファイルシステムキー、顧客がロードしたキー [IEEE 802.1XやHTTPSなど] など）*

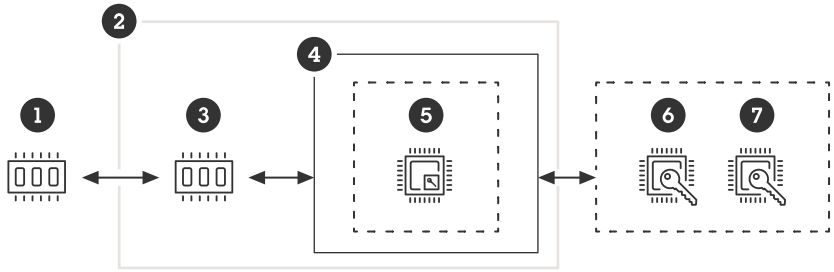

Figure 11. Axis Edge Vaultを搭載したデバイスには、ハードウェア暗号コンピューティングモジュール (セキュアエレメント (6) および TPM (7)) がSoCのメインプロセッサ (4) のすぐ横に

PCBマウントされています。TEE (5) は、SoCのメインプロセッサの安全な実行環境です。SoC内蔵のブートROM (3) は、セキュアブートを実行し、フラッシュメモリ (1) からの署名付きOSソフトウェアイメージのみがデバイスの起動に使用されるようにする役割を果たします。

1. *フラッシュメモリ (署名付きOS、読み取り/書き込み可能ファイルシステム用)*
2. *SoC*
3. *ブートROM (セキュアブート用)*
4. *CPU*
5. *TEE (安全なキーストア用)*
6. *セキュアエレメント (安全なキーストア用)*
7. *TPM (安全なキーストア用)*

TPM、セキュアエレメント、TEEはいずれも、秘密鍵の保護と暗号化操作の安全な実行を実現するテクノロジーです。万が一セキュリティ侵害が発生しても、これらのテクノロジーにより不正アクセスや悪質な抽出を防止することができます。

4.2 コモンクライテリアとFIPS 140

暗号コンピューティングモジュールは、CC EAL（コモンクライテリア評価レベル）とFIPS 140規格（レベル1～4）を使用して認定されます。暗号操作の正確性と完全性を判断し、自己検証、耐タンパー性能、他の耐性といったさまざまな改ざん手段を検証するために、こうした認証が使用されます。認証に関する情報については、Axisデバイスのデータシートまたは*Axisプロダクトセレクター*をご覧ください。Axisは、少なくともコモンクライテリアEAL4やFIPS 140-2/3レベル2/3に従って認定されたハードウェア暗号コンピューティングモジュールを組み込むことを定めています。

4.2.1 コモンクライテリア

コモンクライテリア（CC）（正式名称：情報技術セキュリティ評価のためのコモンクライテリア/Common Criteria for Information Technology Security Evaluation）は、IT製品のセキュリティ認証に関する国際規格（ISO/IEC 15408）です。コモンクライテリアはセキュリティ評価のフレームワークを提供するもので、このフレームワークの中でメーカーや実装者はセキュリティの機能や保証の要件を指定することができます。コモンクライテリアでは、セキュリティターゲット（ST）やプロテクションプロファイル（PP）などの概念が定義されています。

提示されたセキュリティターゲットは、認定独立試験機関による評価を経て、コモンクライテリアのデータベースに認証製品として一覧されます。試験機関による評価の要件と完全性の評価保証レベル（EAL）は、機能テストを行う最も基本的なEAL 1から形式的検証済み設計とテストを行う最も厳格なEAL 7までの7段階に分けられています。コモンクライテリアは、オペレーティングシステム、ファイアウォール、TPM、パスポートなどさまざまな製品が対象となります。

コモンクライテリアの認証要件に関する詳細については、コモンクライテリアのWebサイト（ *www.commoncriteriaportal.org/*）をご覧ください。

4.2.2 FIPS 140

FIPS (米国連邦情報処理標準) 140-2および140-3は、NIST (米国国立標準技術研究所) が発行し、米国およびカナダの連邦政府によって要件として採用されている、暗号コンピューティングモジュールおよび暗号アルゴリズムの使用に関する情報セキュリティ標準です。FIPS 140-3は、FIPS 140-2の更新版として2019年にFIPS 140-2に取って代わります。

NIST認定の試験研究所が検証を行い、モジュールシステムとモジュールの暗号化が正しく実装されていることを保証します。認証を取得するには、暗号コンピューティングモジュール、承認されたアルゴリズム、承認された動作モードの文書化（説明、仕様、検証）および起動テストが必要となります。

お客様は、自社の製品が政府の仕様に従って動作することを保証できます。これにより、お客様は政府機関による監査が行われる際も、安心することができます。FIPS 140の規制を受けていない組織は、その製品が政府によって定義された標準に準拠していることが保証されます。FIPS 140-2とFIPS 140-3の認証要件に関する詳細については、NISTのWebサイト（*www.nist.gov*）をご覧ください。

システム全体が FIPS 140に準拠するためには、システムのすべてのコンポーネントがFIPS 140に準拠する必要があります。例えば、ビデオ管理システムや録画サーバー、カメラなどの接続されているデバイスが準拠する必要があります。デバイスは、ソフトウェア認定モジュールまたはハードウェア認定モジュールの少なくともいずれかが使用されている場合、FIPS 140に準拠していることになります。

AXIS OSバージョン12以降を搭載したAxisデバイスは、FIPS 140認定のソフトウェアベース (OpenSSL) Axis暗号化モジュールを備えています。新しいAxisデバイスのほとんどには、FIPS 140認定のハードウェア暗号化モジュールとソフトウェアベースの暗号化モジュールの両方が組み込まれています。これにより、HTTPSやIEEE 802.1Xなどのソフトウェアベースのアプリケーションをオペレーティングシステムレベルで提供するためのソフトウェア認定モジュールと、安全な鍵の保管用のハードウェア認定モジュールを併用する最適なソリューションが実現します。

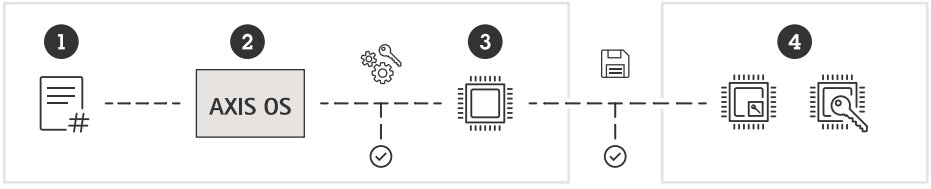

Figure 12. AxisデバイスでのFIPS 140準拠の暗号化ソフトウェアおよびハードウェアモジュールの使用。アプリケーション (1) は、AxisデバイスのAXIS OS (2) に組み込まれた Axis暗号化モジュールを通じて提供されます。Axis暗号化モジュールは、SoC (3) および/または組み込みハードウェアベースの暗号化コンピューティングモジュール (4) を使用して対称および非対称の暗号化処理を実行し、安全な鍵の保管を実現します。

1 *暗号化を必要とするアプリケーション、またはTLSベースのアプリケーション (HTTPS、webRTC、802.1Xなど)*
2 *ソフトウェアベースの暗号化モジュールが組み込まれたAXIS OS (NIST証明書: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4621)*
3 *SoC*
4 *ハードウェアベースの組み込み暗号コンピューティングモジュール*

4.3 秘密鍵の保護

攻撃者は秘密鍵を抽出できれば、HTTPSで暗号化されたネットワークトラフィックを傍受すること、またデバイスのなりすましにより、802.1Xで保護されたネットワークにアクセスすることが可能となります。

Axisデバイスでは、さまざまなTLS（Transport Layer Security）ベースのプロトコルがサポートされているため、これにより安全な通信が実現します。AxisデバイスID (IEEE 802.1AR)、

HTTPS (ネットワーク暗号化)、802.1X (ネットワークアクセスコントロール) は、X.509暗号化情報保護に基づいています。

TLSのX.509デジタル証明書の構造には、証明書およびネットワークの2つのホスト間の通信に使用される公開鍵と秘密鍵のペアが含まれます。安全なキーストアに格納される秘密鍵は、これがデータ復号化に使用されている間も、キーストアから出ることはありません。実際の証明書と公開鍵は既知であるため、Axisデバイスで共有でき、データ暗号化に使用されます。

4.4 アクセスコントロールキーの保護

ハードウェアで保護されたキーストレージが重要であることを示す別の例として、OSDP（Open Supervised Device Protocol）セキュアチャネルなど、Axisアクセスコントロールソリューションで使用される暗号化情報の保護が挙げられます。

広く使用されているAES-128ベースの暗号化や認証方式がサポートされているOSDPセキュアチャネルにより、リーダーなどの周辺機器とドアコントローラーの間の通信が保護されます。

相互認証の開始時に、ドアコントローラーやリーダーで共有されるAES対称キーであるSCBK（Secure Channel Base Key）が使用されます。続いて、セッションキー一式が生成され、ドアコントローラーとリーダー間の通信データが暗号化されるという仕組みです。

真のエンドツーエンドセキュリティを実現するには、マスターキー（MK）とSCBKがAxisネットワークドアコントローラーの安全なキーストアに格納されている必要があります。マスターキーから、接続されているAxisリーダーごとに一意のSCBKキーが生成されます。また、インストール段階でAxisリーダーに安全に配布される個々のSCBKが、リーダーの安全なキーストアに格納されている必要があります。通常、リーダーはドアの安全でない側に設置されるため、これがより重要となります。

このように、OSDPセキュアチャネルキーが、ハードウェアで保護された環境の両端で保護される仕組みとなります。そのため、万が一セキュリティ侵害が発生しても、悪質な抽出を防止することができます。

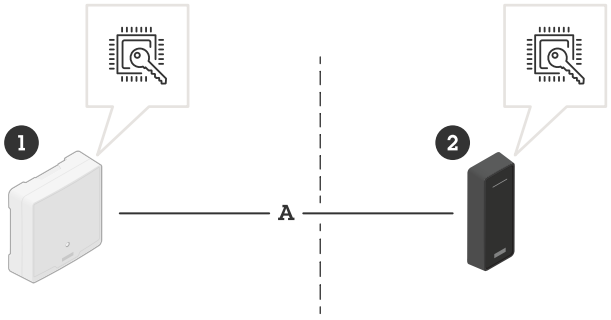

Figure 13. アクセスコントロールにおける安全なキーストアにより、エンドツーエンドセキュリティが実現します。マスターキーと個々のSCBKはそれぞれ、ドアの両側にあるデバイスの安全なキーストアに格納されます。

1　ドアの安全な側に設置するAxisドアコントローラー
2　ドアの安全でない側に設置するAxisリーダー
A　OSDPセキュアチャンネル通信

4.5 ファイルシステムキーの保護

動作中のAxisデバイスには、顧客固有設定と情報が含まれています。事前構成サービスを提供するディストリビューターやシステムインテグレーターから顧客への出荷などで、Axisデバイスが輸送中の状態にある場合も同様です。攻撃者がAxisデバイスに物理的にアクセスできれば、フラッシュメモリーを取り外し、フラッシュリーダーデバイス経由でアクセスすることで、ファイルシステムから情報を抽出できる可能性があります。そのため、Axisデバイスが窃盗された場合や侵害された場合を考慮して、読み取り/書き込み可能なファイルシステムから機密情報が抽出されないように、また設定が改ざんされないように保護することが非常に重要となります。

安全なキーストアにより、ファイルシステムに強力な暗号化を適用することで、悪質な情報の抽出や設定の改ざんを防止することができます。Axisデバイスの電源がオフの場合は、ファイルシステムの情報が暗号化された状態となります。起動プロセス中に、読み取り/書き込み可能なファイルシステムがAES-XTS-Plain64 256ビットキーで復号化されます。これにより、ファイルシステムのマウントが可能となり、Axisデバイスで使用できるようになります。ファイルシステムの暗号化キーは、工場出荷時のデフォルトでデバイスごとに一意に生成され、その後もソフトウェアの更新ごとに再生成されます。デバイスのライフサイクルを通じて、キーが同じになることはありません。

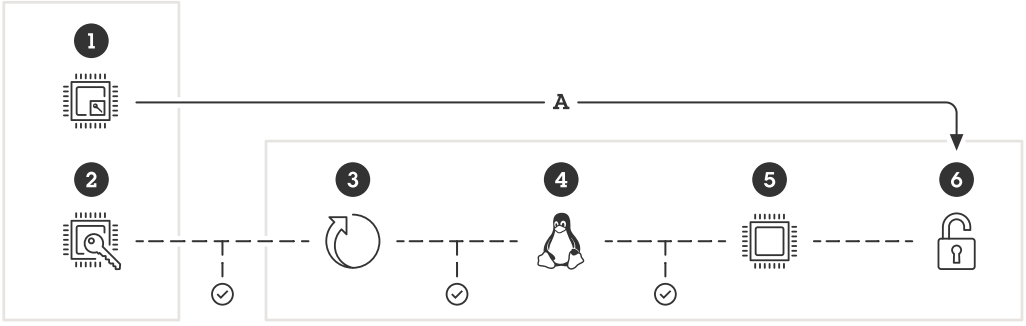

Figure 14. TEE (1) とブートROM (2) はSoCに内蔵されています。ブートプロセス時に、読み書き可能なファイルシステム (6) が（TEE によって）復号化されます。これにより、Axisデバイスでファイルシステムがマウントされて使用可能な状態となります。ブートプロセスでは、ブートローダー (3)、Linuxカーネル (4)、ルートファイルシステム (5) というチェーンの各部が検証され、フラッシュメモリにある次のサブシステムが認証されます。これにより、最終的にルートファイルシステムが検証されることになります。

1 TEE
2 ブートROM
3 ブートローダー
4 Linuxカーネル
5 ルートファイルシステム
6 読み書き可能なファイルシステム
A TEEにより、読み書き可能なファイルシステムが復号化される

5 映像改ざん防止

セキュリティ業界では、監視カメラで撮影された映像は、真正性と信頼性を備えているということが大前提となっています。署名付きビデオは、証拠としての映像の信頼性を維持し、さらに強化するために開発された機能です。映像の真正性を検証する機能により、カメラから転送された後の映像が編集または改ざんされていないことを確認する手段が得られます。

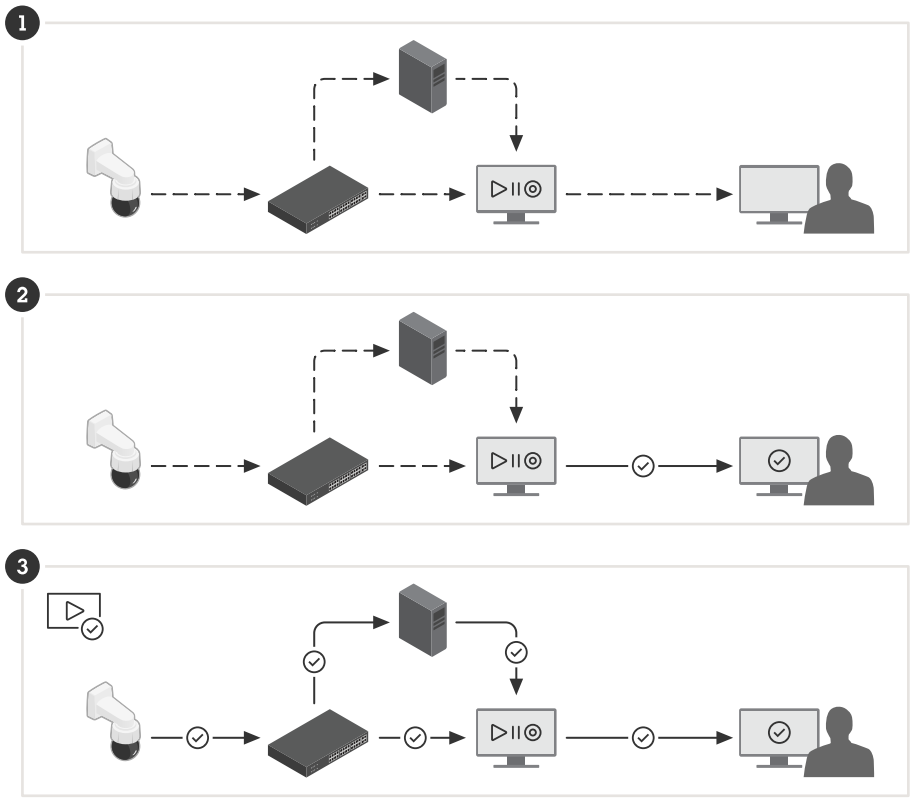

Figure 15. 映像の真正性の検証。

1 *カメラの録画を再生する人物に到達するまで、映像は多くの地点を通過します。熟練した攻撃者なら、いずれかの転送地点で映像を改ざんすることができます。*
2 *エクスポート時に、VMSによる透かしが映像に追加されるため、いくつかの転送地点での検証が可能となりますが、早期の段階で映像が改ざんされていないという保証を得ることはできません。*
3 *署名付きビデオは、映像がカメラからエクスポートされて、録画を見る人物に到達するまでの間、いずれの転送地点でもその映像が改ざんされていないことを確認する手段を提供します。映像が録画されたデバイスまで遡って追跡することが可能となります。*

5.1 署名付きビデオ

Axisがプロアクティブにオープンソースで開発した署名付きビデオ機能により、ビデオストリームの署名に基づき映像が改ざんされていないこと保証し、映像を生成したカメラまで遡って追跡することでその出所を検証することが可能となります。これにより、ビデオファイルの管理のチェーンを証明することなく、映像の真正性を証明することができます。

防犯カメラシステムによって事件が録画されると、警察はエクスポートされた映像ファイルをUSBスティックで受け取り、それをEMS（証拠管理システム）に保存することができます。カメラから映像をエクスポートする際、警察は映像が正しく署名されていることを確認できます。後にその映像を起訴手続きに使用する場合、裁判所はその映像がいつ、どのカメラで撮影されたものか、また映像のフレームが変更・削除されていないかを管理およ

び検証することができます。Axisの*ファイルプレーヤー*を使用すれば、映像のコピーを取得したユーザーなら誰でもこの情報を再生することができます。

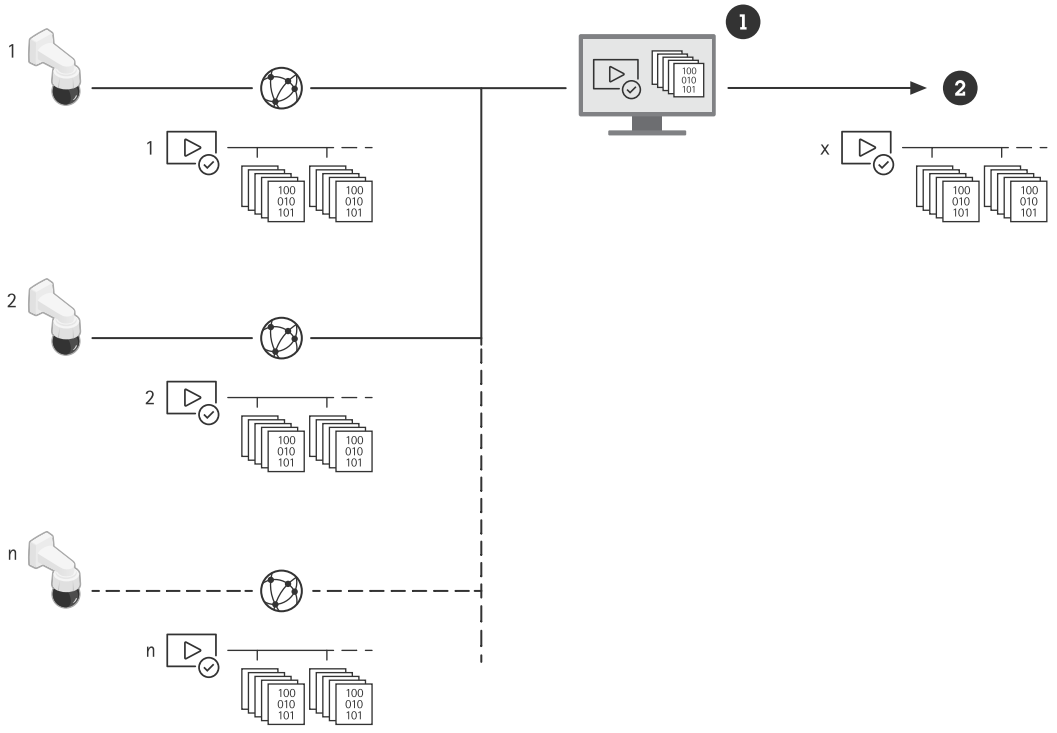

Figure 16. 署名はカメラ内ですでに追加されているため、映像のソースから最終的な使用までのすべての段階でコンテンツを検証することが可能となります。

1 VMS
2 CD/USB/Web/電子メールへのビデオのエクスポート

それぞれのカメラで、安全なキーストアに格納されている一意のビデオ署名キーが使用され、ビデオストリームに署名が追加されます。メタデータを含め、各ビデオフレームの

ハッシュが計算され、結合されたハッシュへの署名が追加されるという仕組みです。この署名は、ストリームの専用メタデータフィールド（SEIヘッダー）に保存されます。

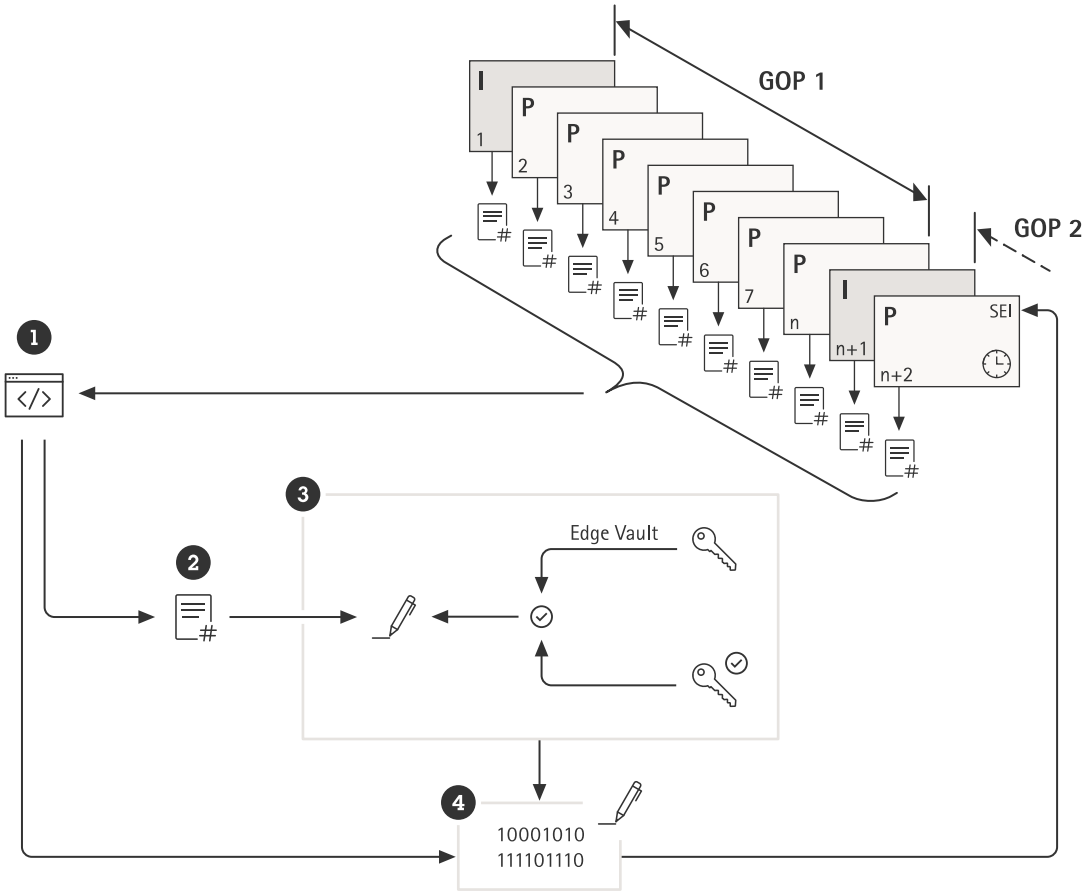

Figure 17. 映像のストリームに署名が追加される仕組みの図示。GOP（Group Of Pictures）の各フレームのコンテンツが、メタデータのハッシュ (1) と共にハッシュ化されます。これにより、GOPハッシュ (2) が生成されます。このハッシュは、デバイス固有のビデオ署名キーと証明キーを使用してEdge Vault (3) で署名されます。次に、デジタル署名 (4) とメタデータ (1) が、ストリームと共に伝送される後続のSEIヘッダーに追加されます。

1 *デバイス固有のメタデータ（ハードウェアID、AXIS OSのバージョン、シリアル番号、証明レポート*）およびストリームのメタデータ（GOPカウンターとフレームハッシュ）*
2 *GOPハッシュ*
3 *Axis Edge Vault*
4 *デジタル署名*

** 証明レポート（第三者認証）を使用して、署名に使用された鍵ペアの出所と発行元を検証することができます。鍵の構成証明を検証することで、鍵が特定のデバイスのハードウェアに安全に保管されていることを確認することが可能となります。これにより、ビデオの出所を保護することができるのです。*

デバイス固有の証明キーを使用して証明されたデバイス固有のビデオ署名キーにより、実際の署名が行われます。証明レポートは開始時にストリームに添付され、その後、定期的な間隔（通常は1時間ごと）を置いて添付されます。メタデータには各フレームのハッシュが含まれているため、どのフレームが正しいかを確認することができます。署名を完了するには、ビデオのGOP構造を保護する必要があります。次のGOPの最初のIフレームのハッ

シュを署名に含めることで、これを保護することができます。これにより、検知不可能なフレームのカットや並び替えを防止することが可能となります。万がーストリーミング中にフレームが失われるという事態、または保存中にコンテンツが破損するというような事態が発生した場合も、同様にフラグが立てられます。

6 用語集

Axisデバイス ID：対応するキーにより、Axisデバイスの真正性を証明できるデバイス固有の証明書。Axisデバイスには、安全なキーストアに格納されているAxisデバイスIDによって工場でプロビジョニングされています。AxisデバイスIDは、ネットワークにおけるデバイス識別の自動化と保護方法を規定する国際規格「IEEE 802.1AR」（初期デバイス識別子/IDevID）に基づいています。

Axis Edge Vault：Axisデバイス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。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。

証明書：公開鍵と秘密鍵のペアにより、出所と特性を証明する署名付き文書。証明書は認証局（CA）により署名されています。システムでCAが信頼済みであれば、CAが発行した証明書も信頼済みとなります。

認証局（CA）：証明書チェーンのRoT（信頼の基点）。基礎となる証明書の信頼性と真実性を証明するために使用されます。

コモンクライテリア（CC）：IT製品のセキュリティ認証に関する国際規格。正式名称は「情報技術セキュリティ評価のためのコモンクライテリア（Common Criteria for Information Technology Security Evaluation）」（ISO/IEC 15408）となります。

FIPS 140：暗号コンピューティングモジュールに関するセキュリティ要件の仕様を規定する米国連邦標準規格。FIPS（連邦情報処理標準）140 は、モジュールの改ざんリスクの軽減を目的として、暗号モジュールの設計および実装に関する要件を規定しています。

不変ROM（読み取り専用メモリー）：信頼済みの公開鍵および署名の比較に使用されるプログラムを安全に格納する読み取り専用メモリー。上書きできないようになっています。

プロビジョニング：ネットワークに接続するデバイスを準備および装備するプロセス。これには、中心点からデバイスへの設定データとポリシー設定の配信が含まれます。デバイスには鍵と証明書が付属しています。

公開鍵の暗号化：非対称暗号化システム。受信者の*公開鍵*を使用して誰でもメッセージを暗号化できますが、*秘密鍵*を使用してメッセージを復号化できるのは受信者のみとなります。メッセージの暗号化と署名の両方に使用できます。

セキュアブート：デバイス起動時に不正なソフトウェアの読み込みを防止する機能。セキュアブートでは、署名付きOSが使用されます。これにより、認可されているAxisソフトウェア以外でデバイスを起動することはできなくなります。

セキュアエレメント：ハードウェアベースの暗号コンピューティングモジュール。耐タンパー性能を備え、ストレージへの秘密鍵の保管および暗号操作の安全な実行を実現する。TPMとは異なり、セキュアエレメントのハードウェアインターフェースとソフトウェアインターフェースは標準化されておらず、メーカー固有となります。

安全なキーストア：秘密鍵の保護および暗号操作の安全な実行が可能となる耐タンパー性の環境。これにより、セキュリティ侵害が発生した場合も、不正アクセスや悪質な抽出を防止することができます。セキュリティ要件に応じて、Axisデバイスには、ハードウェアで保護された安全なキーストアが可能となるハードウェアベースの暗号コンピューティングモジュールを1つまたは複数搭載することができます。

署名付きOS (署名付きオペレーティングシステム)：ファイルイメージが信頼済み機関によってデジタルコード署名されたデバイスソフトウェア。署名付きOSは、デバイスが信頼できるソフトウェアイメージからのみ起動することを保証するためのセキュアブートプロセスの要件です。AXIS OSベースの製品では、デバイスが更新を実行する前に、デバイスソフトウェアイメージの完全性と真正性を検証します。

署名付きビデオ：証拠としてのビデオの信頼性を維持および強化する機能。署名付きビデオにより、ビデオ改ざんの検知と真正性の確認が可能となり、ビデオが損傷していないことを証明することができます。特定のAxisカメラまで遡って追跡することが可能です。署名付きビデオの署名キーは、Axisデバイスの安全なキーストアに格納されています。

TLS（Transport Layer Security）：ネットワークトラフィックを保護するプロトコル。TLSにより、HTTPSなどの安全な通信プロトコルが実現します。

TEE（Trusted Execution Environment）：耐タンパー性能を備えたハードウェアベースのストレージへの秘密鍵の保管および暗号操作の安全な実行を実現する環境。セキュアエレメントやTPMとは異なり、TEEは、SoC（システムオンチップ）のメインプロセッサーからは独立した安全なハードウェア分離実行環境です。

TPM（Trusted Platform Module）：ハードウェアベースの暗号コンピューティングモジュール。耐タンパー性能を備え、ストレージへの秘密鍵の保管および暗号操作の安全な実行を実現する。TPM は国際標準規格に則ったコンピューター部品で、その仕様は*TCG（Trusted Computing Group）*により策定されています（TPM 1.2、TPM 2.0）。

ゼロトラストセキュリティ：高度なセキュリティ制御の実現を目的として、接続されたデバイスとITインフラストラクチャー（ネットワーク、コンピューター、サーバー、クラウドサービス、アプリケーションなど）間の反復的な識別、検証、相互認証の必要性を唱えるITセキュリティの最新アプローチ。

T10190380/ja/M3.5/2404

Axis Communicationsについて

Axisはセキュリティとビジネスパフォーマンスを向上させるソリューションを生み出すことで、 よりスマートで安全な世界の実現を目指しています。 ネットワークテクノロジー企業として、 また業界のリーダーとして、Axisはビデオ監視、 アクセスコントロール、インターコム、音声システムなどのソリューションを提供しています。 これらのソリューションは インテリジェントな分析アプリケーションによって強化され、高品質のトレーニングに支えられています。

Axisは50ヶ国以上に約4,000人の熱意にあふれた従業員を擁し、 世界中のテクノロジーおよびシステムインテグレーションパートナーと連携することで、 カスタマーソリューションをお届けしています。 Axisは1984年に設立され、本社は スウェーデンのルンドにあります。