ホワイトペーパー

Axis装着式ソリューションのセキュリティ

10月 2026

概要

Axisの装着式システムは、オープンプラットフォームをベースにしているにもかかわらず、非常に高いレベルのシステムセキュリティが備わっています。

カメラ紛失時のセキュリティを確保するため、このカメラは不要なソフトウェアコンポーネントを排除し、最小限のプラットフォームに基づいて構築されています。その代わりに、通常は物理的な脅威にさらされにくいシステムコントローラーに多くの機能を搭載しています。カメラの内部ストレージはAES-256で暗号化されており、データへの不正アクセスを防止しています。証明書を使用したIPv6経由の通信により、カメラは特定のシステムコントローラーまたはシステムのみにデータをオフロードします。

カメラからデータがシステムコントローラーにオフロードされる際は、HTTPSで暗号化されたネットワーク接続が用いられます。データはAES-256で暗号化されたシステムコントローラーのストレージデバイスに一時的に保存され、その後別のHTTPS暗号化接続を通じて、コンテンツ送信先に転送されます。

システムコントローラーのセキュリティと完全性は、FIPS 140-2準拠のTPM（Trusted Platform Module）によってさらに強化されます。装着式システムが他の多くのAxisデバイスと共通するその他の機能としては、署名付きOS、セキュアブート、署名付きビデオなどがあります。

AXIS Body Worn Liveでビデオをライブストリームする場合、組織はAxisホスト (クラウド) またはセルフホスト (オンプレミス) のいずれかによるデプロイを選択できます。いずれの場合も、データは保存時および転送時に暗号化され、完全にエンドツーエンド暗号化されて閲覧者のクライアントに直接送信されます。また、管理者はライブストリームの閲覧が可能なユーザーを、特定のコンピューター、クライアント、およびユーザーの認証情報まで厳格に制御します。

目次

1 頭字語と用語 4
2 はじめに 4
3 カメラ紛失時のセキュリティ 4
4 転送中のデータのセキュリティ 4
5 その他のセキュリティ機能 5
6 AXIS Body Worn Liveによるセキュリティ 6
6.1 Axisがホストするデプロイメント 6
6.2 セルフホスト型デプロイメント 6

1　頭字語と用語

BWC。装着式カメラ

VMS.ビデオ管理システム

EMS.証拠管理システム

コンテンツ送信先：装着式カメラなどからの録画とデータを保存する場所。コンテンツ送信先の例として、ビデオ管理システム、証拠管理システム、メディアサーバーなどがあります。

2　はじめに

Axis装着式システムはオープンプラットフォームに基づいて構築されているため、外部のビデオ管理システムや証拠管理システムと容易に統合することができます。一方で、非常に高レベルのシステムセキュリティを備えています。これは、システム実装のあらゆる段階において、このセキュリティに主要な焦点が当てられているためです。

本ホワイトペーパーでは、Axis装着式システムのコンポーネント間のデータフローの概要についてご説明します。特に、BWCでの録画からコンテンツ送信に至るまで、システムとそのデータを保護するために講じられている対策について説明します。また、2つのデプロイメントモデルにおいて、AXIS Body Worn Liveでライブストリームがどのように暗号化されるかについても説明します。

3　カメラ紛失時のセキュリティ

日常的に使用されるBWC（装着式カメラ）は、常に盗難や破壊行為といった物理的な危険性に曝されます。このような脅威の影響を軽減するために、いくつかのシステム設計機能が採用されており、カメラを紛失した場合でもシステムとデータのセキュリティを維持することができます。

一例として、BWCは他のAxisカメラと比較して、最小限のソフトウェアプラットフォームに基づいて構築されており、不要なソフトウェアコンポーネントはすべて削除されています。カメラとシステムコントローラーはVAPIXをサポートしておらず、FTP、SSH、SNMPといったプロトコルもサポートしていません。また、カメラにはサーバー機能がありません。VMSやEMSといった他のシステムとの統合は、システムコントローラーで処理します。システムコントローラーは通常、カメラほど物理的な脅威にさらされることはありません。

BWCの内部ストレージは、AES-256で暗号化されています。これにより、カメラ紛失時におけるデータへの不正アクセスを防止することができます。

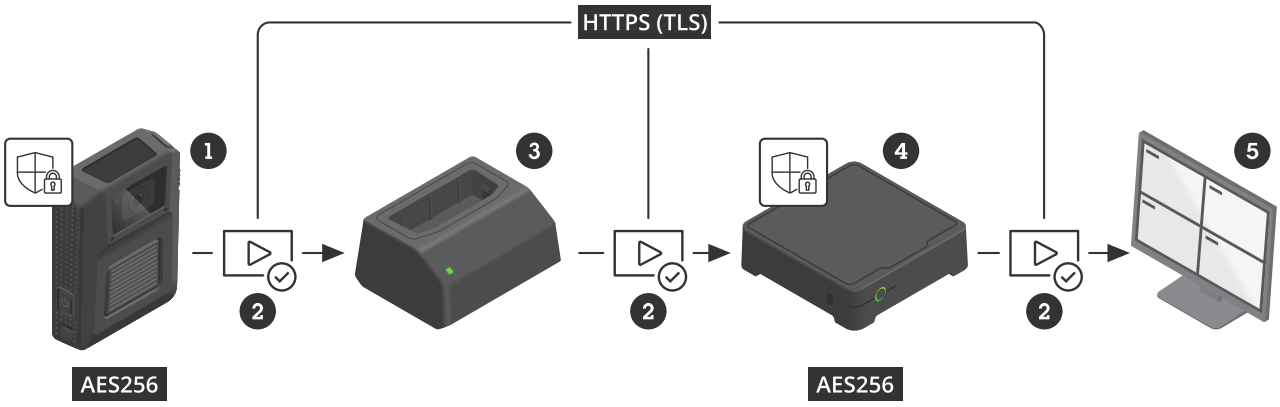
カメラは、カメラが属する特定のシステムコントローラーまたはシステムのみにデータをオフロードします。これは、BWCとシステムコントローラーがIPv6で通信し、証明書を使用するためです。証明書はカメラがドッキングするたびに、システムコントローラーからの最新のものと一致するように自動的に更新されます。

カメラがドッキング解除され、システムから8週間離れている場合、セキュリティ上の理由からセーフモードに入り、接続がロックされます。システムに再度接続するためには、マスターキーのパスフレーズを使用して手動で認証する必要があります。これは、セキュリティ上のリスクを引き起こす可能性がある、紛失していたカメラや長期間ドッキングされていなかったカメラが気づかぬうちに再び追加されてしまうことのないようにするためです。

4　転送中のデータのセキュリティ

通常の使用では、BWCは任務終了後にドッキングされます。BWCには、ビデオとメタデータが格納されています。カメラをドッキングすると、HTTPS（TLSによるHTTP）接続による暗号化ネットワーク経由で、ドッキングステーションを介してすべてのデータがシステムコントローラーにオフロードされます。データは、AES-256により暗号化されたシステムコントローラーのSSDス

トレージデバイスに一時的に保存されます。次に、HTTPS接続経由で、システムコントローラーからデータがコンテンツ送信先に転送されます。



BWC (1) からコンテンツ送信先 (5) への安全なデータ転送と保管

1 *Axis Edge Vault*搭載の*BWC*
2 署名付きビデオ (サイバーセキュリティ機能)
3 ドッキングステーション
4 *Axis Edge Vault*搭載のシステムコントローラー
5 コンテンツ送信先：

コンテンツ送信先が公開暗号化キーを提供している場合、コンテンツ送信先の暗号化キーを使用してBWCとシステムコントローラーのデータを暗号化する機能もサポートしています。この場合、コンテンツ送信先に送信されるデータに追加の暗号化レイヤーが加わります。

5 その他のセキュリティ機能

FIPS 140-2認証TPMを搭載していることで、システムコントローラーのセキュリティと整合性がより強化されます。

BWCとシステムコントローラーは、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であるAxis Edge Vaultが搭載されており、デバイス上のすべてのデータを保護し、いくつかのセキュリティ機能を実現します。例えば、ファイルシステムは暗号化され、キーはAxis Edge Vaultによって保護されます。セキュアブートは、承認されたデバイスソフトウェアでのみデバイスがブートできることを保証します。署名付き*OS*は、ソフトウェアの完全性が損なわれた場合、アップグレードを拒否します。署名付きビデオは、ビデオフレームに暗号化チェックサムを追加することで、追加の保護レイヤーを構築します。これにより、ビデオが録画された特定のAxisカメラまで遡って確実に追跡することができるため、映像が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。

署名付きビデオの詳細については、*developer.axis.com/video-streaming-and-recording/signed-video/*、Axis Edge Vaultの詳細については、*axis.com/solutions/edge-vault*をご覧ください。

カメラユーザーが現場で録画ビデオを表示するには、AXIS Body Worn Assistantアプリケーションを使用しなければなりません。アプリケーションが有効になっている場合、BWCはアプリケーションに直接ビデオをストリーミングしますが、アプリケーションを実行しているデバイスのキャッシュやメモリーにビデオ素材を保存することはありません。また、ビデオストリームにはオーバーレイが表示され、二次的な録画デバイスによるキャプチャを抑止します。それでも録画が行われた場合、オーバーレイを介して、BWCユーザーまで遡ってビデオクリップを追跡することが可能となります。BWCのUSB-C対応コネクターは、ビデオの表示、削除、オフロードに使用することはできません。

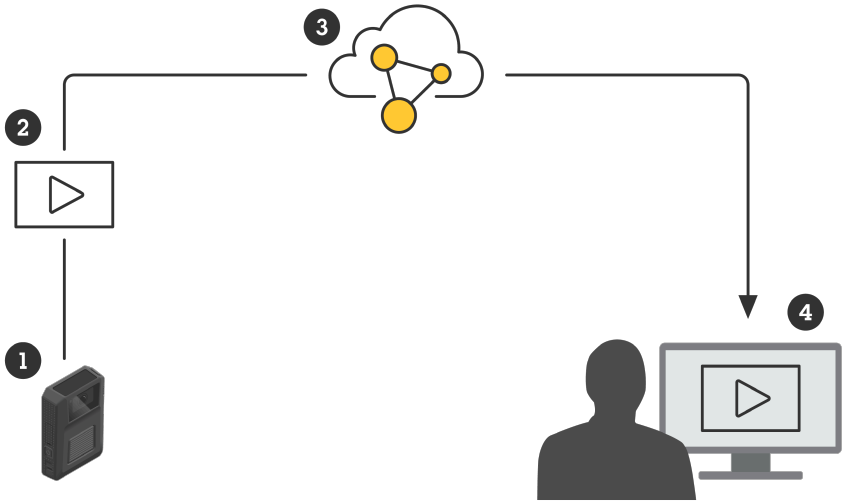
6 AXIS Body Worn Liveによるセキュリティ

AXIS Body Worn Liveは、Axis装着式カメラのライブデータにアクセスできるアプリケーションです。AXIS Body Worn Liveは、ビデオ、音声、位置座標などのデータのライブストリームをユーザーに提供することで、進行中のインシデントに関する比類ない状況認識を可能にします。インフラストラクチャーやデータ主権に関するさまざまな組織の要件に対応するため、以下の2つの導入モデルが用意されています。Axisによるホストおよびセルフホスト。

デプロイメントモデルに関わらず、装着式カメラシステムの管理者は、管理者はライブストリームの閲覧が可能なユーザーを完全に監理することができます。データは、管理者が明示的に承認した閲覧者のみが復号化してビデオを閲覧できるように暗号化されます。また、管理者は、データの完全性を保護するために、ロールに基づいてアクセス権を取り消すこともできます。Axisがホストするデプロイメントでは、閲覧者は承認されたWebブラウザ、VMS、および正しいユーザー認証情報にアクセスできる必要があります。セルフホスト型のデプロイメントでは、閲覧者はローカルネットワークおよび正しい認証情報にアクセスできる必要があります。Axisを含むその他のユーザーはライブストリームにアクセスできず、Axisはユーザーが作成したエンドツーエンド暗号化キーにアクセスすることはできません。

6.1 Axisがホストするデプロイメント

クラウドベースのサービスとして使用する場合、AXIS Body Worn Liveにホストされているすべてのデータおよびファイルは、保存時にAES-256を使用して暗号化されます。すべての通信チャンネルは、信頼性の高い認証局によって署名された証明書を使用し、TLSによるHTTPSで保護されています。転送時の暗号化に加え、AXIS Body Worn Liveは、XChaCha20-Poly1305 暗号スイートを用いて、真のエンドツーエンド暗号化層を追加します。



Axisがホストするデプロイメントにおけるエンドツーエンド暗号化による安全なライブストリーム

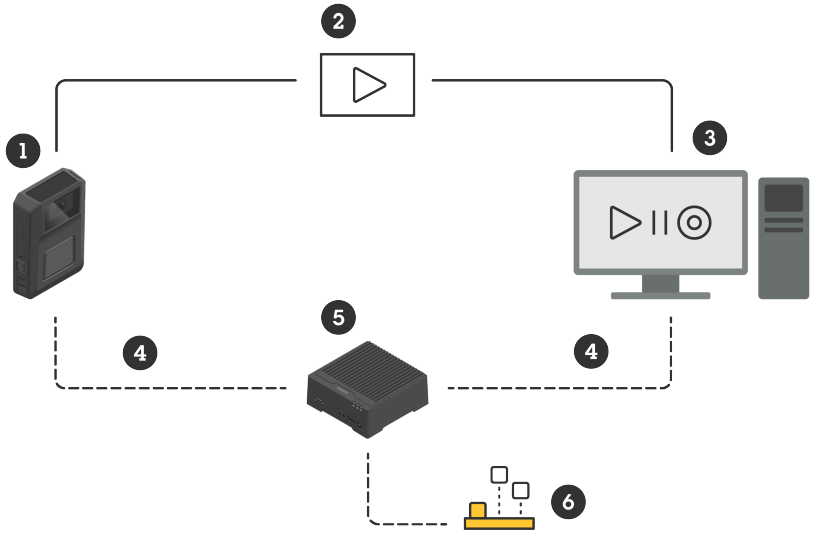
1. 装着式ボディカメラがライブビデオやその他のデータを収集します。データはカメラ内ですでに暗号化されています。
2. ライブストリーミング *(*エンドツーエンド暗号化*)*。
3. *Axis*がホストするクラウド。データおよびファイルは*AES-256*を使用して暗号化されます。
4. *Web*クライアント。データは閲覧者の*Web*ブラウザで復号化されます。

6.2 セルフホスト型デプロイメント

インフラストラクチャーを自組織の管理下にあるネットワーク環境内に完全に留めておくことを求める厳格なポリシーを持つ組織では、サーバーアプリケーションのAXIS Body Worn Live, Self Hostedをデバイスにローカルインストールすることができます。このサーバーデバイスとして、

AXIS W401 Body Worn Activation KitまたはAXIS D3110 Mk II Connectivity Hubを利用できます。ローカルサーバーデバイスには、ビデオや機密データが保存されることはなく、その役割は接続の維持に限定されます。カメラと統合システム間でメディアを送信するための通信チャンネルは、DTLS 1.0以降を使用して保護されています。サーバーと統合システム間でシグナリングやイベントを送信するための通信チャンネルは、顧客から提供された証明書を含むHTTPSとTLS 1.2以降を使用して保護されています。

セルフホストバージョンを使用してデータをストリームする場合、ローカルサーバーは、サーバーとBWCの間で証明書ベースの認証を用いたWebRTCシグナリングを安全に設定します。これが確立されると、BWCと閲覧者のWebRTCクライアント (VMSなど) の間に、暗号化されたピアツーピア接続が直接確立されます。ビデオストリームは、中間ストレージを使用せずにこの暗号化接続を介して直接送信されるため、不正な傍受が防止されます。システムは、インターネットへのアクセスを必要としない、閉じたセグメント化されたネットワークで動作するように設計されており、外部からの脅威に対する攻撃対象領域が最小限に抑えられています。



セルフホスト型デプロイメントにおける安全なライブストリーミング

1. 装着式ボディカメラがライブビデオやその他のデータを収集します。データはカメラ内ですでに暗号化されています。
2. *Peer-to-Peer (P2P)* ストリーミング *(*暗号化*)*。
3. 閲覧者の*WebRTC*クライアント。
4. *WebRTC*シグナリング。
5. *AXIS Body Worn Live, Self Hosted*サーバーデバイス。
6. *AXIS Body Worn Live, Self Hosted*サーバーアプリ。これは*WebRTC*シグナリングを設定するために使用されます。

T10155258_JA/JA/M10.2/2610

Axis Communicationsについて

Axisは、セキュリティ、安全性、運用効率、ビジネスインテリジェンスを向上させることで、よりスマートでより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、また業界をけん引するリーダーとして、Axisは映像監視、アクセスコントロール、インターコム、音声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、インテリジェントアプリケーションによって強化され、質の高いトレーニングによってサポートされています。

Axisは50ヶ国以上に5,000人を超える熱意にあふれた従業員を擁し、世界中のテクノロジーパートナーや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年に創業し、本社はスウェーデン・ルンドにあります。

© 2020 — 2026 Axis Communications AB. AXIS COMMUNICATIONS、AXIS、ARTPEC、VAPIXは、スウェーデンおよびその他の国で登録されたAxis ABの登録商標です。その他のすべての商標は、それぞれの所有者に帰属します。記載内容は予告なく変更されることがあります。