ホワイトペーパー

Axis装着式カメラ

システムセキュリティ

6月 2023

概要

オープンプラットフォームがベースとなっていますが、Axisの装着式システムには非常に高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、最小限のプラットフォームに基づいて構築されたカメラには、不要なソフトウェアコンポーネントが一切含まれていません。その代わりに、通常は物理的な脅威に曝されにくいシステムコントローラーに多くの機能が配置されています。また、カメラの内部ストレージがAES-256で暗号化されています。これにより、データへの不正アクセスを防止することができます。証明書を使用したIPv6経由の通信により、カメラからは特定のシステムコントローラーまたはカメラが属しているシステムのみにデータをオフロードすることができます。

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。

FIPS 140-2認証TPM（Trusted Platform Module）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。装着式システムの他の機能として、署名付きファームウェア、セキュアブート、署名付きビデオなどが挙げられます。こうした機能は、他多くのAxisデバイスにも搭載されています。

AXIS Body Worn Liveを通じて映像をライブストリーミングする際には、保存中・転送中のデータおよび閲覧者のWebブラウザにあるデータが暗号化されます。これはまた、プロトコル「XChaCha20-Poly1305」を使用して、エンドツーエンドで暗号化されます。さらに、特定のコンピューター、Webブラウザ、ユーザー認証情報など、ライブストリームを視聴できるユーザーを管理者が制御することができます。

目次

1 頭字語＆用語の解説

BWC：装着式カメラ（Body Worn Camera）

VMS：ビデオ管理システム（Video Management System）

EMS：証拠管理システム（Evidence Management System）

コンテンツ送信先（コンテントデスティネーション）：装着式カメラなどでキャプチャーされた録画やデータが保存される場所。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挙げられます。

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の全段階において、システムとそのデータの保護を目的として講じられている対策をご紹介します。追加のセキュリティに関する考慮事項など、さまざまなストレージメディアに関する内容も含まれています。

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。こうした脅威の影響を軽減することを目的として、いくつかのシステム設計機能が導入されています。これにより、カメラを紛失した場合も、システムとデータのセキュリティを維持することが可能となります。

一例として、他のAxisカメラとは異なり、BWCは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いることが挙げられます。つまり、不要なソフトウェアコンポーネントはすべて排除されているということです。カメラとシステムコントローラーにはVAPIXが搭載されておらず、FTP、SSH、SNMPといったプロトコルもサポートされていません。また、カメラにはサーバー機能が備わっていません。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経由で処理します。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曝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。

カメラからは特定のシステムコントローラーまたはカメラが属しているシステムのみにデータをオフロードすることができます。証明書を使用したIPv6経由の通信により、BWCとシステムコントローラー間で通信が図られます。カメラを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情報と一致するように証明書が自動的に更新されます。

4週間以上カメラをドッキングしない状態が続くと、猶予期間として8週間システムコントローラーで古い証明書が受け入れられます。これ以上の期間カメラがシステムから離れた状態が続いた場合は、マスターキーのパスフレーズを使用して、カメラを手動でシステムに受け入れさせる必要があります。紛失していたカメラや長期間ドッキングされていな

かったカメラが不用意に再び追加されると、セキュリティ上のリスクが発生するため、これは一種のセキュリティ対策となります。

4 転送中のデータのセキュリティ

一般的な使用では、任務終了後に使用者がBWCをドッキングします。これには、ビデオとメタデータが含まれています。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。

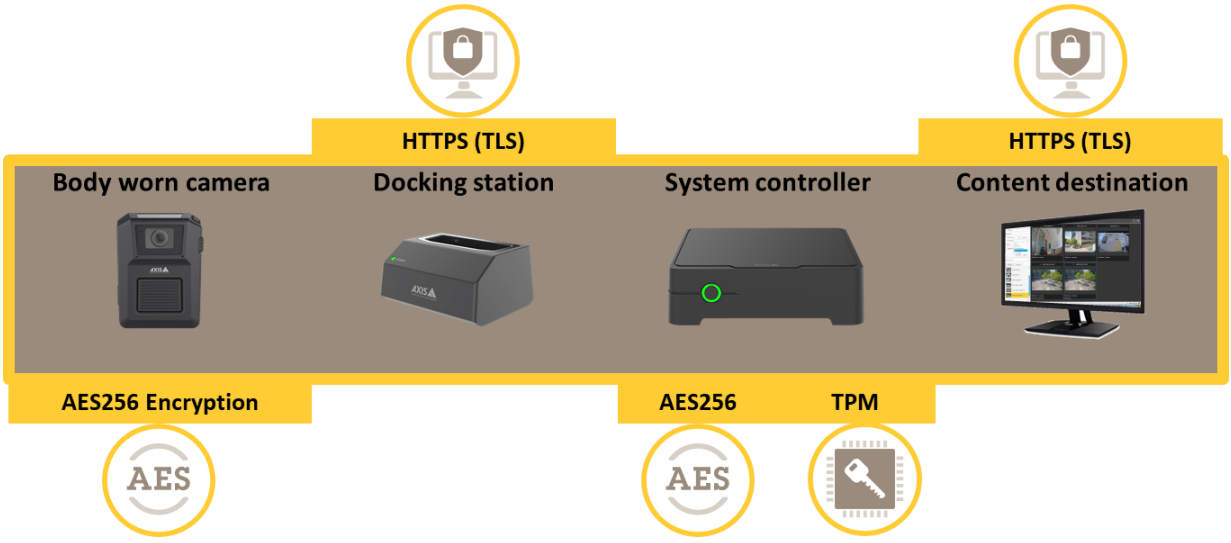

Figure 1. データストレージ＆BWCからコンテンツ送信先への安全なデータ転送

コンテンツ送信先で公開暗号化キーが提供される場合は、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されています。これにより、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。システムコントローラーには、*セキュアブート*も備わっています。これにより、承認されたファームウェア以外ではデバイスを起動できなくなります。

また、システムコントローラーとBWCには*署名付きファームウェア*が備わっているため、ファームウェアの完全性が損なわれていることがデバイスで検知されると、ファームウェアのアップグレードが拒否されます。

*署名付きビデオ*では、ビデオフレームに暗号化チェックサムが追加されるため、より強力な保護レイヤーが構築されます。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、*www.axis.com/developer-community/signed-video*、Axisのサイバーセキュリティ機能の詳細については、*www.axis.com/solutions/built-in-cybersecurity-features*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れば、BWCからビデオがアプリケーションに直接ストリーミングされますが、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要素が保存されることはないため、後から第三者がこれにアクセスすることはできません。別の録画デバイスでビデオがキャプチャーされるのを防止するため、ビデオストリームにオーバーレイを追加することができます。この場合は、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

アプリケーション「AXIS Body Worn Live」により、Axis装着式カメラのライブデータにアクセスすることができます。AXIS Body Worn Liveを利用することで、ユーザーはビデオや音声、また位置座標といった他のデータのライブストリームにアクセスできるため、進行中の事件や事態に対する優れた状況認識を得ることができます。当初、これはクラウドベースのサービスとして提供されていました。

AXIS Body Worn Liveにより、保存中（ストレージ内）と転送中のデータの暗号化だけでなく、カメラと閲覧者のWebブラウザ間における完全なエンドツーエンドの暗号化が実現します。

AXIS Body Worn Liveでホストされるデータとファイルはすべて、AES-256で暗号化されます。すべての通信チャネルは、HTTPS（TLSによるHTTP）接続で保護され、信頼済み認証局（CA）によって署名された証明書が使用されます。また、AXIS Body Worn Liveでは、プロトコル「XChaCha20-Poly1305」を使用して、真のエンドツーエンド暗号化が実現することで、追加のレイヤーによりセキュリティが強化されます。

装着式カメラシステムの管理者は、ライブストリームを視聴できる人物を完全に制御することができます。暗号化されたデータを復号化して動画を視聴できるのは、管理者が承認した閲覧者のみとなります。閲覧者は、適切なコンピューター、適切なWebブラウザ、適切なユーザー認証情報を備えている必要があります。このライブストリームには、他者は誰も、Axisすらもアクセスすることはできません。管理者はアクセス権を取り消すこともできます。

T10155258/ja/M2.4/2306

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。