ホワイトペーパー

Axisネットワーク音声のサイバーセキュリティ

9月 2025

概要

相互接続された現在の社会において、機密性の高い情報を保護し、業務効率を維持するためには、音声通信システムのセキュリティ確保が極めて重要です。ネットワークに接続された音声システムは、不正なアクセス、盗聴、サービス拒否攻撃、マルウェア、ソフトウェアのエクスプロイトなど、数多くの脅威に直面します。Axisは、既存のインフラストラクチャーにシームレスに統合できる、信頼性、拡張性、ロバストな保護を提供する最先端のセキュリティソリューションによってこれらのリスクに対応しています。

Axisは、暗号化、認証、セキュアなソフトウェア更新、アクセスコントロール、システムのハードニング、イベントログを取り入れた、セキュリティ・バイ・デザインのアプローチを採用しています。SIPS、SRTP、HTTPS、IEEE 802.1AEなどのセキュアなプロトコルにより、セキュアな通信とデータ転送を可能にしています。

Axisの音声管理ソフトウェアは、ロールベースアクセス制御、セキュアなオンボーディング、包括的なイベントログ機能を提供し、オンプレミスとクラウドベースの両方の展開に対応します。

これらのセキュリティレイヤーを活用することで、Axisネットワーク音声システムは、サイバー脅威に対するエンドツーエンドの保護を提供します。

目次

1　はじめに

音声システムは、小売店舗、運輸、公共安全、教育などのさまざまな産業分野で、通信、セキュリティ、業務効率において重要な役割を果たしています。これらのシステムは、サイバー攻撃の標的となりやすく、ロバストなセキュリティ対策が不可欠です。音声システムが不正にアクセスされると、深刻な影響が広範囲に及ぶ可能性があります。

このホワイトペーパーでは、Axisのスピーカーと音声システムがこのような課題に対処するために採用している主なセキュリティレイヤーについて考察します。

2　リスクの把握

さまざまな業界でネットワークに接続された音声ソリューションの導入が増えるにつれて、セキュリティ対策が不十分なシステムに関連する潜在的なリスクが著しく高まっています。

ネットワークに接続された音声システムは、複数の種類の脅威に晒される可能性があります。

- **不正なアクセス。** 保護されていない音声デバイスは、悪意のある攻撃者が遠隔からアクセスし、スピーカーを操作したり、不正なアナウンスを流したり、業務を妨害する可能性があります。
- **盗聴やデータ傍受。** ネットワークに接続された音声システムは、有線または無線ネットワークを介して機密性の高い音声データを送信することがあります。暗号化されていないと、攻撃者によって会話が傍聴されたり記録される可能性があり、プライバシーの侵害、産業スパイ活動、または機密情報の悪用につながる恐れがあります。
- **サービス拒否 (DoS) 攻撃。** 攻撃者がネットワーク接続されたスピーカーや音声サーバーに過剰なトラフィックを集中させ、システムの過負荷やサービスの中断を引き起こす可能性があります。このような攻撃によって、重要な局面で緊急通信システムの機能不能になる恐れがあります。
- **マルウェアおよびランサムウェア攻撃。** 従来のITインフラストラクチャーと同様に、ネットワークに接続された音声デバイスもマルウェアやランサムウェアによって不正にアクセスされる可能性があります。攻撃者はデバイスをロックダウンしてその対価として金銭の支払いを要求したり、不正にアクセスしたシステムから広範なネットワークを攻撃する可能性があります。
- **ソフトウェアのエクスプロイトとサプライチェーン上の脆弱性。** パッチが適用されていないセキュリティ上の脆弱性を持つ古いオペレーティングシステムでは、音声デバイスがエクスプロイトされてコントロールが奪われる恐れがあります。さらに、セキュアでないサプライチェーン管理は、導入前に脆弱性を生み、最初からシステムが攻撃を受けやすい状態になる恐れがあります。

3　Axisネットワーク音声の利点

Axisは、既存のインフラストラクチャーにシームレスに統合できる最先端のスピーカーとシステムのセキュリティソリューションを提供します。オープンアーキテクチャによって、さまざまなシステムやプロトコルに対応します。Axisシステムは柔軟性に優れ、小規模の導入から大企業規模のネットワークまで、組織のニーズに合わせて拡張できるように設計されています。Axisはオンプレミス型とクラウドベースの両方の音声管理システムを提供しています。

Axisはソフトウェア開発においてセキュリティ・バイ・デザインのアプローチを採用しています。Axis Security Development Model (ASDM) フレームワークによって、ソフトウェア開発ライフサイクル全体にセキュリティを統合し、脆弱性のリスクを低減するプロセスとツールを定義しています。ASDMは継続的に改善されています。

改善に向けた多数のインプットの一つとして、さまざまなセキュリティ関連規格を定期的に評価してASDMにマッピングしています。Axisのソフトウェアは、EUのGDPR (一般データ保護規則) を含む、データプライバシーとセキュリティに関する厳格な業界基準を満たしています。

4 スピーカーおよびシステムのセキュリティの主な特徴

Axisネットワーク音声では、セキュリティがデバイスと管理システムに組み込まれます。

暗号化と認証

- 暗号化はTLS 1.2および1.3によって音声データのセキュアな転送を実現し、許可されていない第三者による情報の傍受やアクセスを防止します。
- 認証は許可されたデバイスとユーザーのみがデバイスとソリューション全体にアクセスできることを保証します。

セキュアなデバイスソフトウェア更新

- セキュアブート (ほとんどの製品) とデジタル署名付きパッチにより、検証済みデバイスソフトウェアのみインストールされることが保証されます。これにより、システムが悪意のあるコードから保護されます。

アクセスコントロール

- AXIS Audio Manager ProとAXIS Audio Manager Centerは、ロールベースアクセス制御 (RBAC) を採用し、システムへのアクセスを許可されたユーザーのみに制限します。
- 一元管理により、IT管理者は権限を効果的に監視、管理できます。

システムのハードニング

- デフォルト設定は最適化されており、アウトオブザボックスのセキュリティで脆弱性を低減します。
- 追加の設定オプションにより、特定のユースケースに基づいたカスタマイズが可能です。AXIS OSハードニングガイド (*help.axis.com/axis-os-hardening-guide*) で技術的なアドバイスを提供しています。

イベントのログと監視

- 包括的なログにより、システムアクティビティが可視化されます。リアルタイムの脅威検知とフォレンジック分析に役立ちます。

5 システム全体のセキュリティ

Axisネットワーク音声では、セキュリティがデバイスと管理システムに組み込まれます。セキュアプロトコルがデバイスと管理ソフトウェア間の通信で高度なセキュリティを実現します。

5.1 デバイスのセキュリティ

すべてのAxisスピーカーは、Axisデバイス専用に設計されたデバイスソフトウェアAXIS OSで動作します。これにより、長期的な価値、サイバーセキュリティ、ワールドクラスの統合が実現します。AXIS OSにより、AxisスピーカーはAxisエコシステムからロバストなセキュリティ機能を継承します。これにより、すべてのデバイスで一貫性と信頼性が確保され、あらゆるデプロイにおいてエンドツーエンドの保護を提供します。セキュリティ機能には、暗号化ファイルシステムや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 (*axis.com/solutions/edge-vault*) が含まれています。

Axis Edge Vaultは、Axisデバイスの完全性を保護し、暗号鍵に基づくセキュアな運用を可能にします。 これにより、IEEE 802.1ARに準拠するAxisデバイスIDの検証と、IEEE 802.1XおよびHTTPSを介したゼロトラストネットワークにおけるデバイスのセキュアなオンボーディングの活用が可能になります。Axis Edge Vaultの使用により、デバイスを安全に起動し、統合でき、暗号鍵などの機密情報が確実に保護されます。

Axis Edge Vaultにより、受け取ったAxisデバイスが物理的なサプライチェーンで改ざんや不正アクセスされていないことを確認できます。Axis Edge Vaultは信頼の連鎖を確立し、暗号的に検証されたソフトウェアの途切れない連鎖を保証します。たとえば、*署名付きOS*の機能は、デバイスソフ

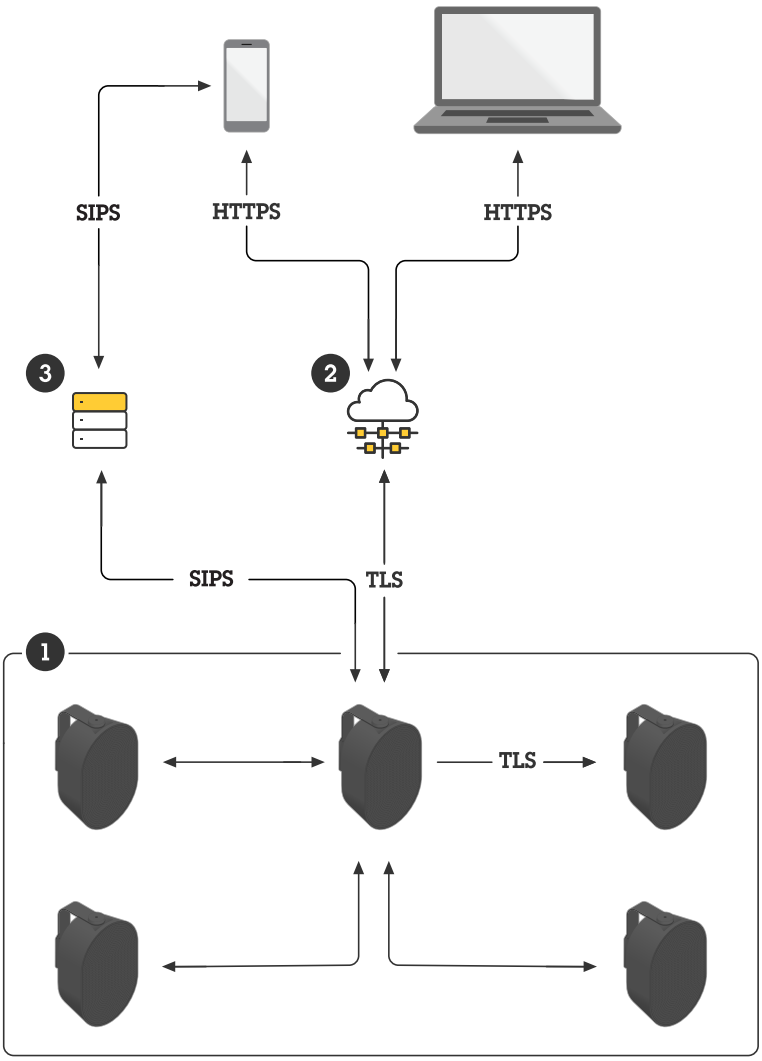
トウェアがAxis製であり、Axisの署名付きのアップデートのみがインストールされることを保証します。

5.2 セキュリティプロトコル

Axisのデバイスとシステムは、セキュアな通信、転送、ストリーミングのためにオープンプロトコルを使用します。

- **SIPS** (SIP Secure): TLS (Transport Layer Security) を組み込むことによって標準のSIP (Session Initiation Protocol) を強化します。これによってIP PBXとVoIP電話の間にセキュアな接続が確立されます。セキュアな接続が確立されると、SRTP (Secure Real-Time Transport Protocol) が音声データを暗号化し、インターネット経由での転送のためにセキュアなIPパケットに変換します。これにより、送信側 (IP電話システム) から受信側 (スピーカー) までエンドツーエンドの暗号化が提供されます。

  AxisシステムはSIPSとSRTPを活用することで、音声データと接続設定そのものを保護します。つまり、音声ストリームと接続の詳細 (発信者IDや受信者など) が完全に暗号化され、ピアツーピアのセキュアな通信チャンネルのロバスト性が確保されます。
- **マルチキャストコントローラー**: Axisスピーカーのマルチキャストコントローラー機能によって、SRTP経由で送信されるマルチキャスト音声ストリームのセキュアな受信が可能になります。これにより、グループ通信が確実に暗号化されます。
- **Transmit.cgiとreceive.cgi**: これらのVAPIX APIは、HTTPS経由の暗号化されたポイントツーポイント通信におけるセキュアな音声ストリーム送受信方法を提供します。CGI (Common Gateway Interface) は、Webサーバーと外部プログラム間の通信を指定する標準プロトコルです。
- **RTSPS** (Real-Time Streaming Protocol Secure): サーバーとクライアント間のリアルタイムメディアストリームの確立と管理に使用されるネットワーク制御プロトコルです。不正アクセスを防ぐために暗号化を利用し、セキュアな音声ストリーミングをサポートします。
- **HTTPS**: あらゆる通信において機密性と完全性を維持するため、すべてのAPIはHTTPSで保護されています。
- **IEEE 802.1AE**: MACsec (Media Access Control Security) としても知られ、基本的にネットワークレイヤー2でAES-128がネットワーク通信を暗号化するネットワークプロトコルです。HTTPS、RTSPS、SIPSと組み合わせると、ネットワークトラフィックは実質的に二重暗号化され、ネットワークセキュリティが大幅に強化されます。



複数のオープンプロトコルによるセキュアな通信を実現するネットワーク音声システム。

1 *AXIS Audio Manager Edge: Axis*スピーカーに統合されたオンプレミス型音声管理
2 *AXIS Audio Manager Center:* ハイブリッドクラウドによる一元的な音声管理
3 パートナー*PBX*

5.3 音声管理ソフトウェアのセキュリティ

5.3.1 オンプレミスソリューション

Axisのオンプレミスソリューションは、オンサイトの複数のスピーカー間でのゾーニング、優先順位付け、セキュアな通信を管理できるように設計されています。

AXIS Audio Manager Edge。この管理ソフトウェアは、Axisのすべてのネットワーク音声スピーカーに組み込まれています。これによって、それぞれのスピーカーが独立したソフトウェア管理サーバーを必要としない完全なオールインワンサウンドシステムになります。AXIS Audio Manager Edgeは、20ゾーン以下、200台以下のデバイスで構成される複雑性の低いプロジェクト管理向けです。

- デバイス間の暗号化をサポートしています。デフォルトの暗号化方式は自己署名証明書によるTLSですが、デバイスに信頼された証明書をインストールし、サイトのシステム設定でTLS認証を有効にすることをお勧めします。これにより中間者攻撃に対する保護が提供されます。
- ローカルサイトへのデバイスのセキュアなオンボーディングを可能にします。初期設定はHTTPS経由でデバイスの認証情報を使用して行われます。その後、デバイス間の通信にはMQTT

(TLS-PSK) が使用され、デバイス間の音声ストリームなどの暗号化されたRTPデータの送信にはSRTPが使用されます。

- HTTPS API経由でオペレーショナルユースケースに外部システムへのアクセスを提供します。

AXIS Audio Manager Pro。この管理ソフトウェアは、より大規模で高度なプロジェクトを対象としています。1つのインターフェースで多数のゾーン (500以上) とデバイス (5000台以上) を管理できます。AXIS Audio Manager Proでは、長期スケジュール設定と高度な優先度設定を容易に行うことができます。

- システムへのアクセスを許可されたユーザーのみに制限するロールベースアクセス制御が含まれており、Active Directory統合をサポートしています。
- デバイスのセキュアなオンボーディングを可能にします。
- 詳細イベントと監査ログが含まれています。これは、システムアクティビティの包括的な記録を提供し、管理者は変更の追跡、動作の監視、問題のトラブルシューティングに役立てることができます。

5.3.2 クラウドベースのソリューション

AXIS Audio Manager Centerは、マルチサイトシステムのリモート管理と監視のためのサービスで、少数のサイトから数千のサイトまで拡張可能です。各ローカルサイトで、AXIS Audio Manager Edgeと共に使用します。これは、クラウドベースとオンプレミスの両方のコンポーネントを採用した、便利で安定したハイブリッドクラウドソリューションです。

AXIS Audio Manager Centerは、管理を簡素化し、一元管理を実現し、デバイスのセキュアなオンボーディングを処理します。1回のサインオンで、選択したサイトやゾーンへのアナウンス、BGM、広告のスケジュールを設定できるため、ユーザーの作業負荷が大幅に軽減されます。主なセキュリティ機能には以下が含まれます。

- ロールベースアクセス制御 (RBAC): システムへのアクセスを許可されたユーザーのみに制限します。
- 一元ユーザー管理: 効率的な管理のために*My Axis*またはActive Directoryのユーザー/グループをサポートします。ローカルユーザーは必要ありません。
- セキュアなオンボーディング: 各デバイスにインストールされた固有の証明書を使用して、クラウドからの信頼性のあるデバイスのオンボーディングを簡素化します。
- セキュアなエンドツーエンド設定の簡素化: 証明書の処理を含むSIPSのセキュアな設定が可能になります。
- ヘルスモニタリングと通知: システムの健全性に対する統合監視と、潜在的な問題に対する即時アラートを提供します。
- セキュアな通信: クラウドとデバイス間のすべての通信はTLS経由で暗号化され、相互TLS (双方向認証) によりロバストなセキュリティが確保されます。
- リモートアクセス: どこからでもローカルサイトへのセキュアなリモートアクセスを可能にします。

T10225475_JA/JA/M1.13/2509

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。

© 2025 — 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。