ネットワークストリームの暗号化

ネットワークビデオを暗号化する理由と方法

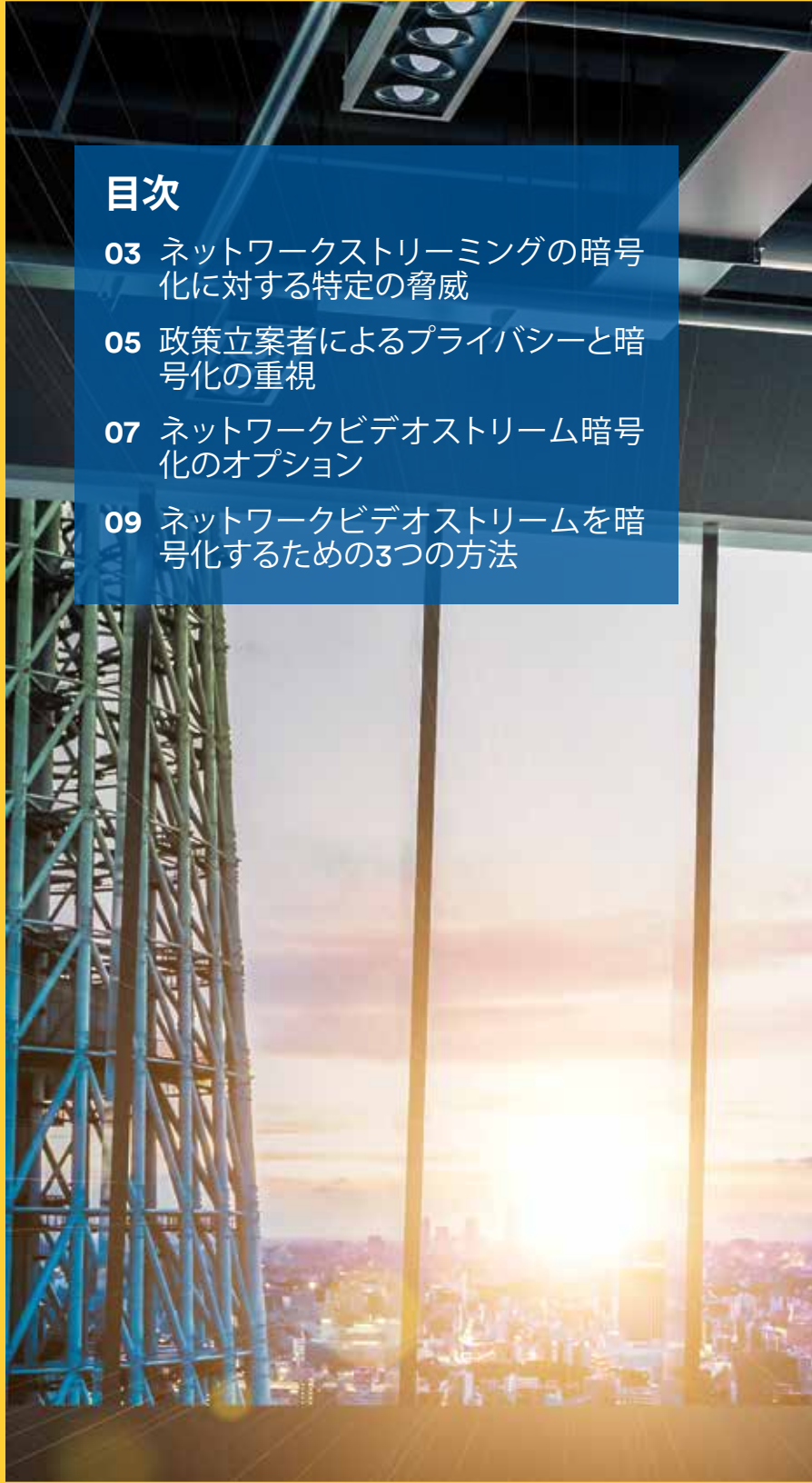
Genetec™ AXIS COMMUNICATIONS

ネットワークビデオカメラ、管理ソフトウェア、およびクライアント間の通信の保護

セキュリティシステムのあらゆる側面 (通信、サーバー、データ) を保護することは、今日のビジネスにとってますます重要になっています。また、これに伴い物理セキュリティとサイバーセキュリティの統合も推進されています。組織の物理セキュリティ、サイバーセキュリティを問わず、その責任者の業務は、保護する必要がある資産とリソースを継続的に特定することです。これにより、最も防止が必要と思われる脅威と、外部および内部の脅威を防止、検出、修復するための方法を評価することができます。

本ドキュメントの目的

本ガイドは、暗号化が映像、音声およびデータのネットワークストリーミングを安全に保つしくみの概要を提供することを目的としています。



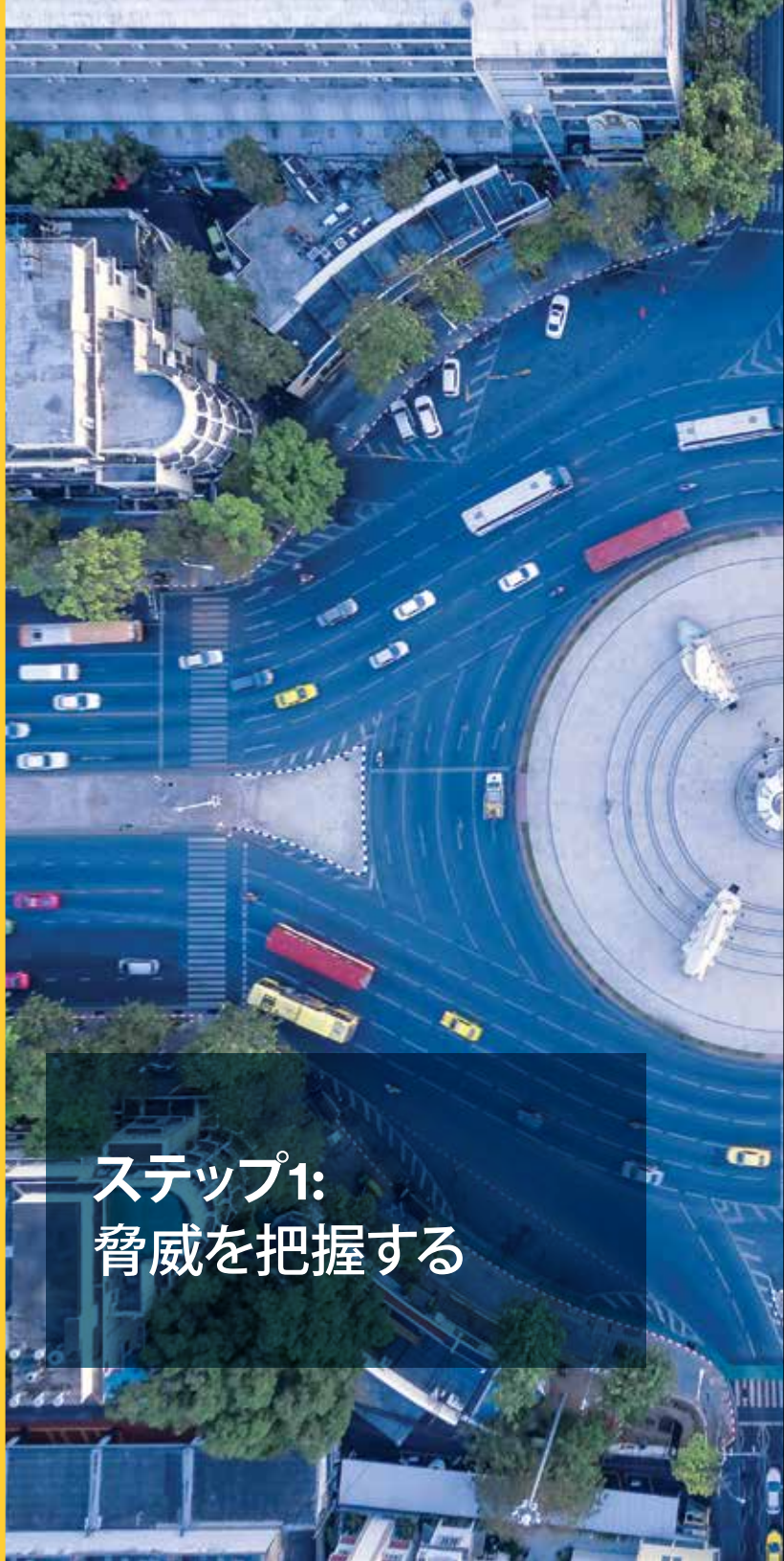
目次

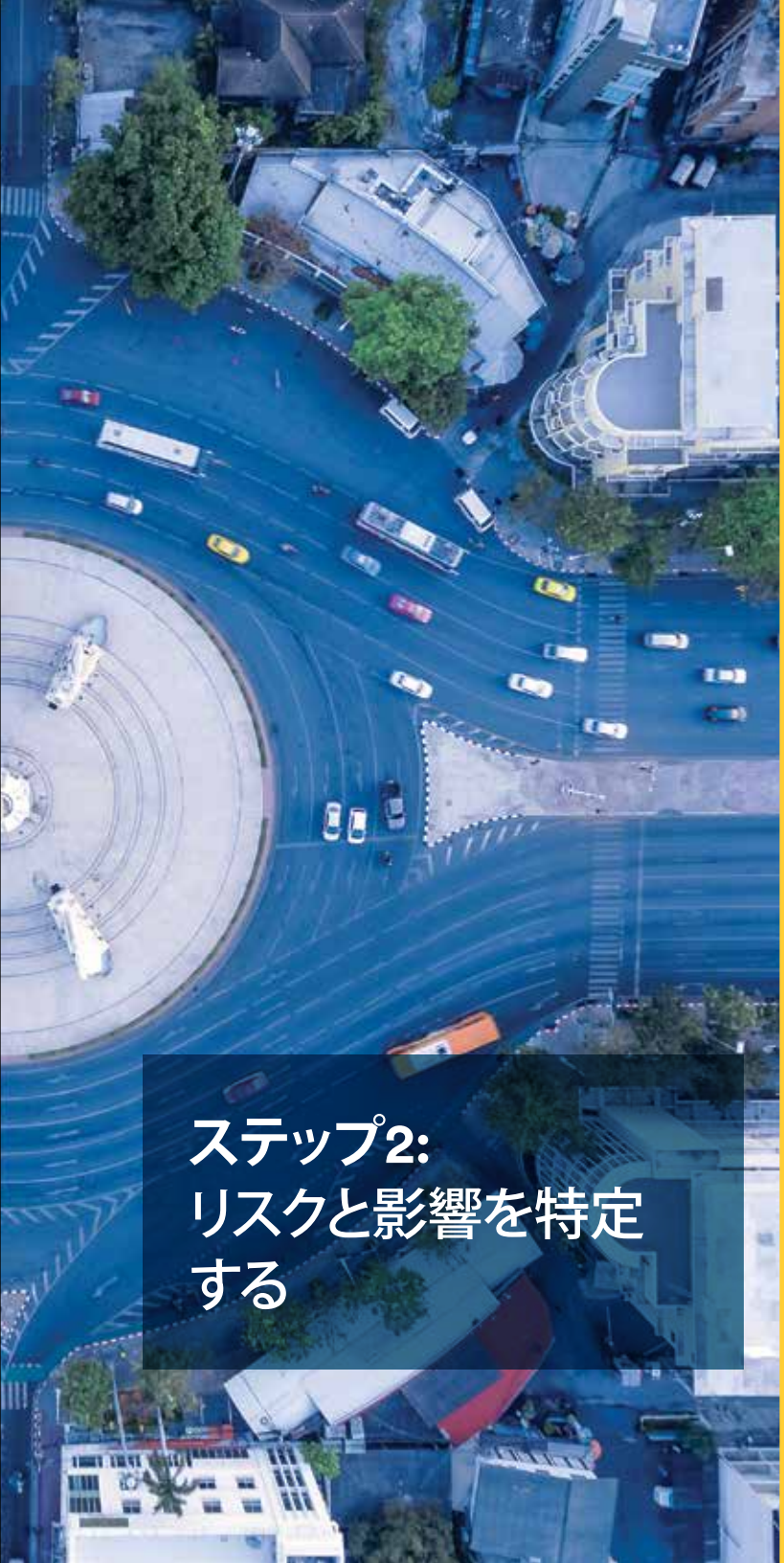
第一章

ネットワークストリーミングの暗号化に対する特定の脅威

ネットワーク上に存在するあらゆるものと同様に、IPセキュリティソフトウェア、システム、およびデバイスは、さまざまな攻撃の影響を受けやすい状態にあります。まずは、ネットワークストリーミングにおける潜在的な脅威を把握する必要があります。以下は、主な外部脅威の一部です。

- **ネットワークスニッフィング (盗聴):** 通信中のデバイス2台と同じネットワークへのアクセスを持つ敵対者は、データパケットをキャプチャーすることができます。機密データや重要データを問わず、保護されていないあらゆるデータは、容易に侵害されてしまいます。
- **ネットワークスプーフィング (リソースの完全性):** 悪意のあるコンピューターは、ネットワークリソースになりすまし、通信相手を欺いて機密情報を漏えいさせたり、データ (完全性) を改ざんしたりできます。
- **中間者攻撃 (情報の完全性):** トラフィックのリダイレクトや傍受が可能な敵対者は、二者間の通信を改ざんすることができます。





ステップ2: リスクと影響を特定する

影響度とリスクレベル

情報セキュリティ管理システムの規格群、ISO 27000では、データおよびサービスを機密情報、私的情報および公共情報に分類しています。各リスク分類は、その潜在的な影響力に基づいています。例えば、1つの映像システムでは映像システムのアセットを次のように分類できます。

- ライブ映像は公共情報に分類されます (公共とは、一般的な公共と、組織内での公共、両方を意味します)。ライブ映像が一般に公開される場合、危険性は限定されます。
- 録画は私的情報に分類されます。録画されたインシデントの一部は機密情報を含んでいる可能性があるため、特定の組織にのみアクセス権が与えられます。
- システム設定、アカウントおよびパスワードは機密情報に分類されます。組織内の特定の個人のみにアクセス権が与えられます。

ポリシー設定における2つのステップ

アクシスとジGenetec社では、企業内に導入されたすべてのネットワーク技術に関連するセキュリティポリシーを作成することを推奨しています。このポリシーにより、ネットワーク内のどのデータが機密であるかを定義し、転送中に適切に保護できるようにする必要があります。

第二章

政策立案者によるプライバシーと暗号化の重視

政府によって制定された法律、業界固有の標準や基準の変更への準拠。EU一般データ保護規則から生じる最新の要件を満たす必要性、または機密性の高い個人データを保護する必要性。新しいオンラインの脅威。セキュリティ、運用システムおよび管理システムの統一に対する要求。これらの要素はすべて、個人データとビデオストリームを保護する必要性に影響を与えます。

プライバシー、完全性および情報源は今日の重要な課題

監視ビデオでは、機密性の高い個人データとプライバシーの保護も考慮する必要があり、これはEU一般データ保護規則 (GDPR) でも示されています。この規則は、個人データの使用方法と保護方法に関して、欧州連合 (EU) および欧州経済地域 (EEA) 内のデータ主体の権利を強化することを目的としています。ほとんどの場合、「個人データ」という用語は、特定されたまたは特定可能な自然人に関する情報を意味します。これには、映像が含まれます。

そのため、ビデオ映像では、アクティビティやアクセスを制限できることが非常に重要です。録画やストリームされた映像へのアクセスにも、プライバシーを確保するため高い安全性と保護が求められます。使用するソリューションにかかわらず、以下の3つの側面が重要です。

プライバシー：個人の身元情報を保護し、その機密性を保持する

完全性：映像が改ざんされていないことを実証する

情報源：映像が適切なソースによるものであることを実証する

通常、データの完全性、機密性、そして情報源の保証は、Hyper Text Transfer Protocol Secure (HTTPS) およびTransport Layer Security (TLS) を使用して管理されます。

第三章

ネットワークビデオストリーム暗号化のオプション

業界標準への準拠は、ネットワークセキュリティとネットワークビデオの転送管理における主要推進力の1つです。ただし今日では、一般的にネットワーク上を流れるすべてのセキュリティデータを暗号化することが推奨されており、すべてのリソースを認証する必要があります。

ネットワークストリーミングを保護するには、カメラコンポーネント、ビデオ管理システム、および通信ストリームが移動するネットワークインフラにセキュリティを実装する必要があります。IPネットワークを介して送信される映像のセキュリティ確保には、さまざまなセキュリティレベルがあります。ネットワークの強化には、認証された通信ストリームの確立と維持、設定ファイルへのデジタル署名、データとビデオストリームの暗号化、あらゆるコンポーネント間の信号伝達が必要です。これらのセキュリティ機能はすべてのネットワークに必要というわけではありませんが、セキュリティレベルの向上に選択肢を提供します。

もちろん、各保護形式にはコストが伴い、通常はさまざまなワークフロールーティンが必要です。多くの場合、より高度な保護形式はより高度なルーティンを必要とし、コストの上昇を招きます。

ユニキャスト vs. マルチキャスト

ユニキャスト伝送とマルチキャスト伝送は、一般的にネットワークを介して、カメラからその宛先に映像をストリーミングする際に使用される2つの方法です。各映像伝送方法にはそれぞれ長所と短所があり、各システムの機能要件によってどちらの伝送方法が最適か決定されます。一般的には、以下のように分けられます。

- **ユニキャストストリーミング**は、ネットワークビデオのストリームにおいて最も一般的な方法です。各クライアントは、1つのメディアストリームを要求します。この伝送方法は、すべてのネットワークパケットがクライアントに配信されることを保証します。
- **マルチキャストストリーミング**は、パケットをブロードキャストして、複数のクライアントが同じビデオストリームを表示できるようにします。複数のクライアントが同じビデオストリームを表示する場合に、より効果的な方法です。マルチキャストでは、ネットワークの途絶が発生するため、すべてのクライアントがすべてのパケットを受信することは保証されません。ビデオストリームに対する影響は非常に限られており、多くの場合気づくことはありません。

ネットワークインフラとシステムの使用方法によって、使用する方法が決まります。

第四章

ネットワークビデオストリームを暗号化するための3つの方法

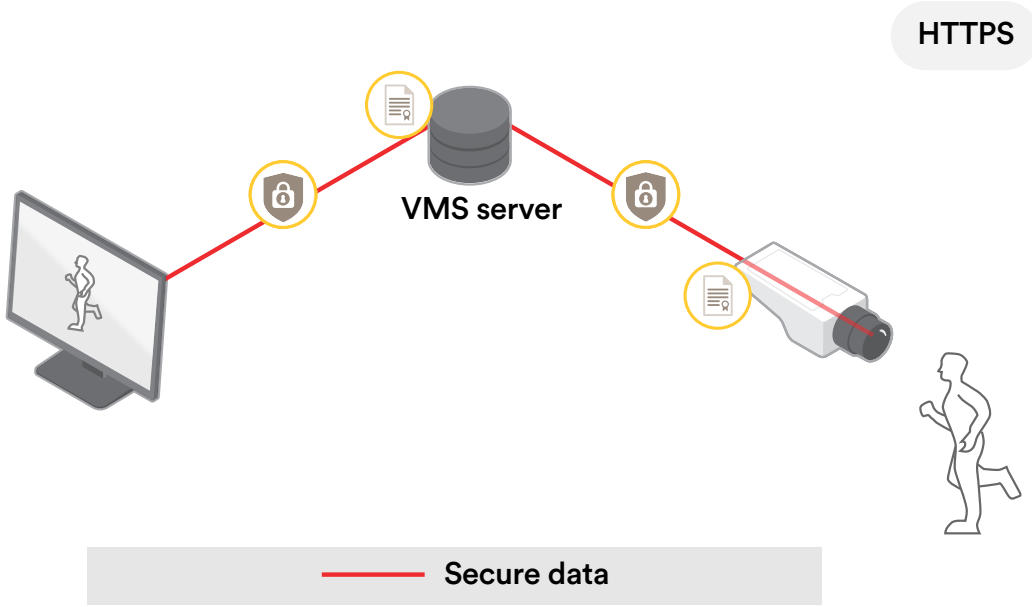
HTTPS

HTTPSは、クライアントとサーバー間のトラフィックの暗号化に使用される標準の保護です。TLS (Transport Layer Security) は、HTTPトラフィックをトンネリングする安全なチャネルを作成するために使用されます。サーバーに認証局 (CA) によって署名された証明書がある場合、クライアントはカメラになりすました悪意のあるコンピューターではなく、正当なサーバーにアクセスしていることを確認することができます。

通常、映像はRTP (Real-time Protocol) を使用して送信されます。暗号化された映像の場合、クライアントはHTTPS経由でRTPストリームを要求する必要があります。HTTPS (TLS) は、さまざまなタイプの暗号を使用できます。最も一般的に使用されている暗号は、AES (Advanced Encryption Standard) で、128ビットまたは256ビットの鍵長を用います。

アクシスのカメラには自己署名証明書があらかじめインストールされており、HTTPSが有効になっています。そのため、クライアントは即座にHTTPSを使用してカメラにアクセスすることができます。スプーフィングの脅威がある場合は、証明書をCA署名付き証明書に置き換える必要があります。

多数のエッジベースIPカメラを展開するエンタープライズレベルのシステムでは、通常この作業に多大な時間がかかり、管理が困難です。AXIS Device Manager (ADM) ソフトウェアはカメラのCAとして機能し、VMSのトラストポイントを作成することができます。AXIS Device Managerを使用してCA署名付き証明書を展開および更新することで、1つのサイトで最大2千台のAxisカメラを、または複数のサイトで数千台のAxisカメラを、バッチで効率的に管理できます。これにより、Webインターフェースを使用して一度に1台のカメラを手動で管理する場合と比較して、時間を大幅に節約できます。

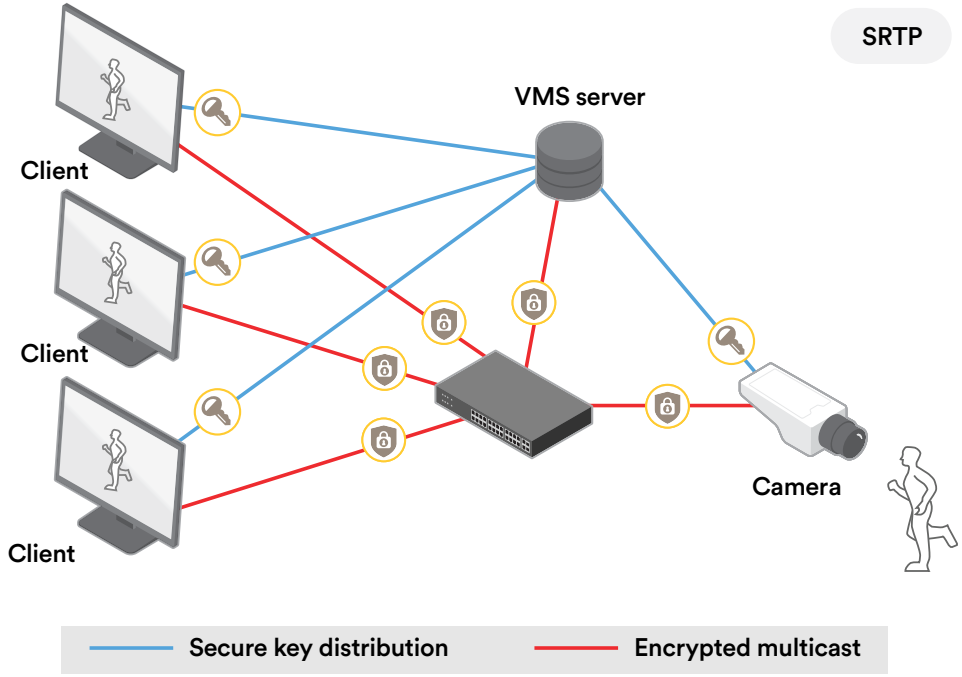


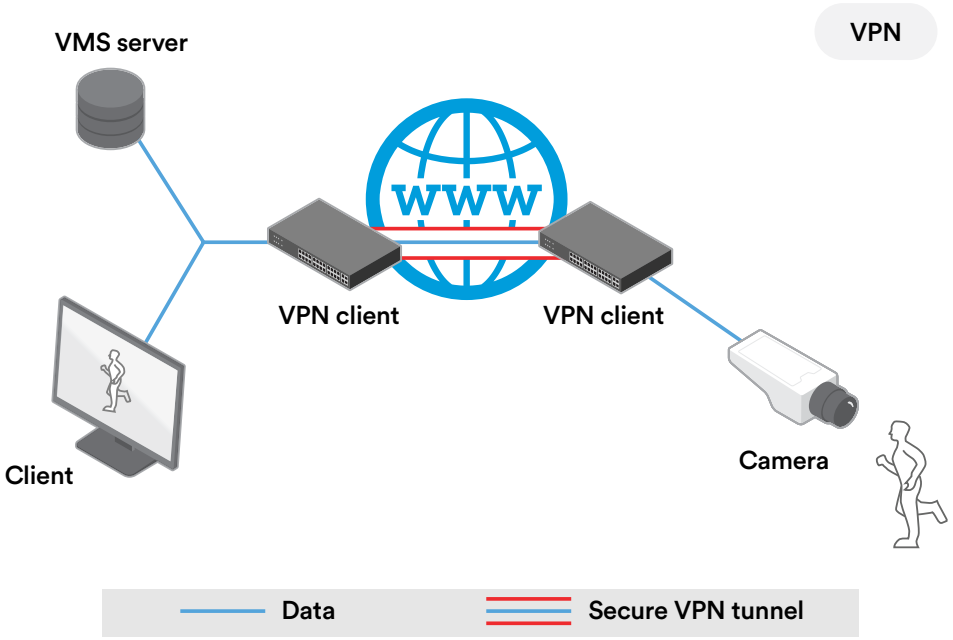
Secure Real-time Protocol (SRTP)

SRTPは、Real-time Transport Protocol (RTP)の拡張プロトコルです。データ転送におけるポイントツーポイントおよびマルチポイントの両方に使用されます。

HTTPSがクライアントとサーバー間にトンネルを作成する間、SRTPは各RTPパケットを暗号化します。つまり、SRTPはストリーミングメディアの暗号化にのみ使用できます。クライアントがカメラの管理作業 (設定の変更など) を行う必要がある場合は、HTTPSを使用する必要があります。

SRTPはHTTPSと同じ暗号、通常は鍵長128ビットのAESを使用します。
AESは対称鍵を使用するため、映像の製作者側と消費者側の両方が鍵を知る必要があります。Genetec社とアクシスのSRTPソリューションは、この鍵をクライアントやカメラに安全に配布するソリューションを提供します。鍵は毎分更新され、すべてのクライアントとカメラ間で確実に鍵が同期されるようにします。





仮想プライベートネットワーク (VPN)

VPNはセキュアなトンネルを構築し、多くの場合、2つのリモートネットワーク (サイト) を安全にリンクさせるために使用されます。VPNは、ポイントツーポイントトンネリングプロトコル (PPTP)、インターネットプロトコルセキュリティ (IPsec)、OpenVPNなど、さまざまな方法で異なるプロトコルを使用して実装できます。

一般的にVPNは、ネットワークビデオシステムのリモートカメラへの接続を保護するために使用されます。インターネット、都市ネットワーク、またはモバイル4Gを介して接続されたカメラなどが挙げられます。HTTPSも同じ目的のために使用できます。主な違いは、HTTPSがさまざまな種類の攻撃に対してカメラのパブリックIPアドレスを公開することです。VPNソリューションは、カメラにローカルIPアドレスを提供し、トラフィックを暗号化しながら露出を低減します。

効果的なサイバーセキュリティ保護を目的とした提携

Genetec社とアクシスは、お客様と地域社会がセキュアなセキュリティソリューションを確保できるよう、取り組んでいます。この取り組みの1つは、それぞれのデバイス、ソフトウェア、およびシステムを強化するための効果的なソリューションを見つけることです。たとえば、各強化ガイドには、セキュリティコントロールを適用するための明確な手段が記載されています。さらに、この緊密な連携により、お客様はAxis強化ガイドに記載されたAxisカメラを保護するためのさまざまな推奨事項を、直接Genetec Security Centerで自動的に実装することができます。

Genetec社とアクシスが連携し、セキュリティデバイスとシステムのセキュリティをサポートするもう1つの方法が、知識の共有です。本ガイドでは、ネットワークビデオテクノロジーのセキュリティポリシーを作成するための2つのステップと、セキュリティシステムとネットワーク間の通信を保護するための暗号化において弊社が提供する3つのオプションについて説明しています。

連絡先

ジェネテック・ジャパン株式会社

www.genetec.com/jp
salesjapan@genetec.com

アクシスコミュニケーションズ株式会社

axis.com/ja-jp
info-jp@axis.com