Case Study

国際的法執行機関のHD CCTVネットワーク

cpl.thalesgroup.com/ja

THALES
Building a future we can all trust

THALES
Building a future we can all trust

CCTVネットワーク&監視サービスプロバイダーの大手企業は、欧州の法執行機関のCCTVネットワーク伝送データを保護するために、タレスのセキュアな高速ネットワーク暗号装置を採用しました。

タレスのCNシリーズ高速ネットワーク暗号装置は、CCTVネットワークのパフォーマンスを損なうことなく、認定されたデータセキュリティと完全性を実現しています。

このお客様は、安全な監視情報を提供するスペシャリストです。政府や多国籍企業と連携し、規制、法執行、防衛などの重要なインフラストラクチャ分野において、最も複雑で重要なHD CCTV監視の課題に取り組んでいます。

北欧の法執行機関と共同するにあたり課題となったのは、機密性の高いHD　CCTVストリームを国全体に安全に配信できるセキュアな映像配信インフラストラクチャを設計することでした。

CCTV技術は一般的に、国境、空港、公共建物、軍事基地、石油・ガス施設、公共空間、公共交通システムなどの重要な場所を保護するために使用されています。

近年、CCTVアプリケーションでは、高精細画像のリアルタイムストリーミングに対するニーズが高まっています。これは一部のデータセキュリティシステムにとって課題となっており、通常、画質の低下や、遅延によるストリーミングの遅れが生じたりします。

ライブHDビデオの需要は多くの業界で高まっており、ネットワークビデオトラフィックの急増につながっています。その多くは本質的に機密性が高いため、通信インフラストラクチャ全体で安全かつ効率的にデータを伝送する必要があります。

CCTVデータは、プライバシー侵害、不正データの入力、CCTVデータの完全性に悪影響を及ぼす可能性のある不正アクセスからの保護が必要不可欠です。これらは、法執行や規制遵守のアプリケーションでは特に重要な問題です。

効率的なHDビデオ配信/ストリーミング（通常、大量のデータを含む）では、マルチキャスト伝送プロトコルを使用して、要求したデバイスにのみデータが送信されるようにしています。

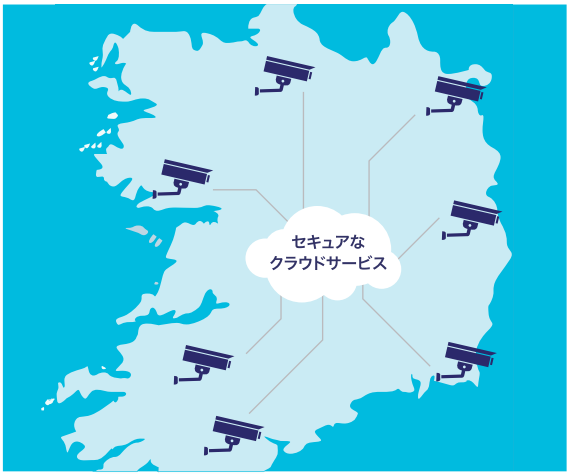

図1 – CCTVネットワーク

別のソリューションの評価

最初に検討されたソリューションのひとつは、通常のレイヤ3（インターネットプロトコル）ルーティングのデータネットワークをベースに、一般的なIPSecセキュリティプロトコルを使用してすべてのトラフィックを暗号化するというものでした。

IPSecは、レイヤ3ルーティングのデータネットワーク環境でデータを保護するための業界標準であり、インターネットのような「ベストエフォート型」ネットワークでの使用に最適化されています。

しかし、レイヤ3でのデータ保護にはいくつかの制限があります。特に、 HD　CCTVフィードの高性能配信が必要な場合です。

速度制限、遅延、過剰なネットワークオーバーヘッドは、画質、ネットワークパフォーマンス、そしてデータセキュリティ全体に影響します。

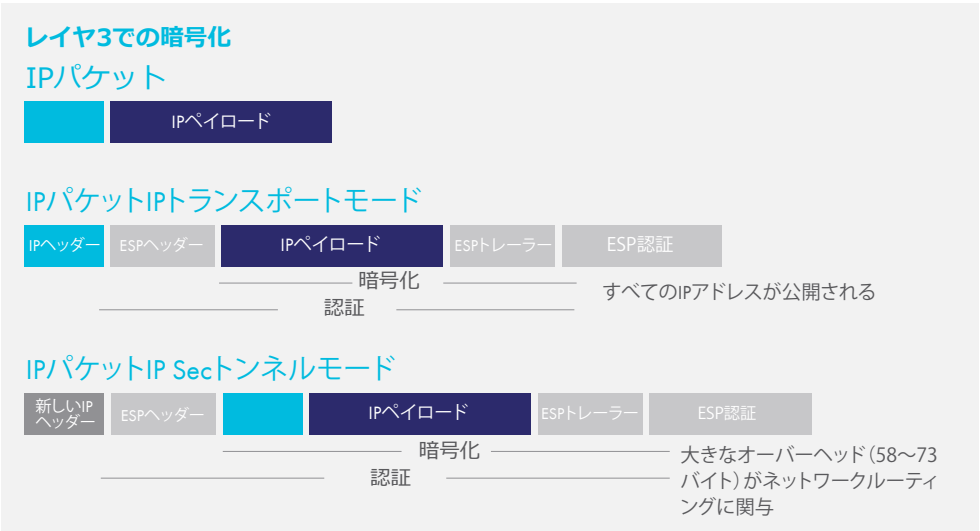

図2 – IPSec暗号化のオーバーヘッド

レイヤ3での暗号化は、クライアントの厳しい基準を満たすために必要なセキュアで高パフォーマンスのソリューションを提供できません。

また、レイヤ3で暗号化する際、その複雑さから技術的な問題も発生します。これらの制限を克服するために、IPSec暗号化ソリューションでは通常、ネットワーク帯域幅を増やす必要があり（最大30%）、これにはかなりのコストがかかります。

マルチキャスト伝送

マルチキャストの保護にレイヤ3での暗号化を採用することには問題があります。なぜなら、基盤となるネットワークに、PIM（Protocol-Independent Multicast）ルーティングファミリーなどのマルチトラフィックをサポートするための追加のルーティングプロトコルが必要となるからです。

これらのプロトコルは、IPSec暗号化との同時使用が必要な場合、さらなる複雑さをもたらします。実際には、マルチキャストIPトラフィックの多くがGRE（Generic Routing Encapsulation）トンネルを使用してカプセル化され、ユニキャストトラフィックの暗号化が容易になるものの、オーバーヘッドがはるかに高くなります。したがって、レイヤ3で暗号化する場合、基盤となるデータネットワークと装置には、より高度な仕様が求められます。

大規模なマルチキャスト展開でのデータ配信は非効率的であり、これらの「隠れた」コストがソリューション選定の重要な要因となりました。

タレスのセキュアな高速ネットワーク暗号ソリューション

レイヤ3ネットワークリンクを介して暗号化された複数ロケーションのCCTVデータを伝送することには制限と欠点があると判明したため、別のネットワークアーキテクチャが必要になりました。

タレスは、イーサネット層で高速に暗号化を行うレイヤ2のWANサービスをベースにした代替案を提案しました。タレスCNシリーズのセキュアな高速ネットワーク暗号装置は、ネットワークデータにオーバーヘッドを追加せず、遅延がほぼゼロで、他のネットワーク資産に影響を与えません。

タレスの高速ネットワーク暗号装置は、レイヤ2において、はるかにシンプルな「セットアンドフォーゲット（初期設定だけの）」実装と継続的な管理を提供し、技術的にも財政的にもはるかに効率的なソリューションとなります。

タレスの暗号化ソリューションは、メトロイーサネットE-LAN、E-LINE、E-TREE、レイヤ2 MPLS（VPLS）、または単純なポイントツーポイントのダークファイバーやWDM（波長分割多重）接続などのネットワークサービス向けに最適化されています。

レイヤ2の暗号化は、イーサネットネットワークのデータリンク層で行われます。そのため、イーサネットペイロードは暗号化されますが、イーサネットヘッダー（MACアドレスとVLAN識別子を含む）は変更されません。サービスプロバイダーのネットワーク上での伝送が可能となります。

イーサネットペイロードはIPヘッダーとIPペイロードを完全にカプセル化し、これらも暗号化されるため、送信データ内のすべてのIPアドレスが隠れるというセキュリティ上の利点があります。

レイヤ2での暗号化は、フレームごとのオーバーヘッドがほぼゼロで、最大10Gbpsの速度で100%の暗号化スループットを実現できます。

また、暗号化はデータリンク層で行われるため、マルチキャストやブロードキャストトラフィックを暗号化するための特別な設定やプロトコルが不要になります。

レイヤ2ネットワークでの効率的なマルチキャストデータ伝送を確保するために、多くの場合、IGMPやMLDなどのプロトコルがホストとルーター間に導入されます。また、ネットワークスイッチは、IGMPのやり取りをリッスンするためにIGMPモニタリングを実行し、IPマルチキャストストリームを必要とするリンクのマップを維持することができます。

このメカニズムでは、必要な場所にのみフレームを配信するため、データネットワークの効率が維持されます。IGMP/MLDトラフィックを（必要に応じて）バイパスできるようにすることで、レイヤ2暗号装置は、ネットワークの運用に根本的な変更を加える必要なく、最大の効率で稼働し続けることを可能にします。

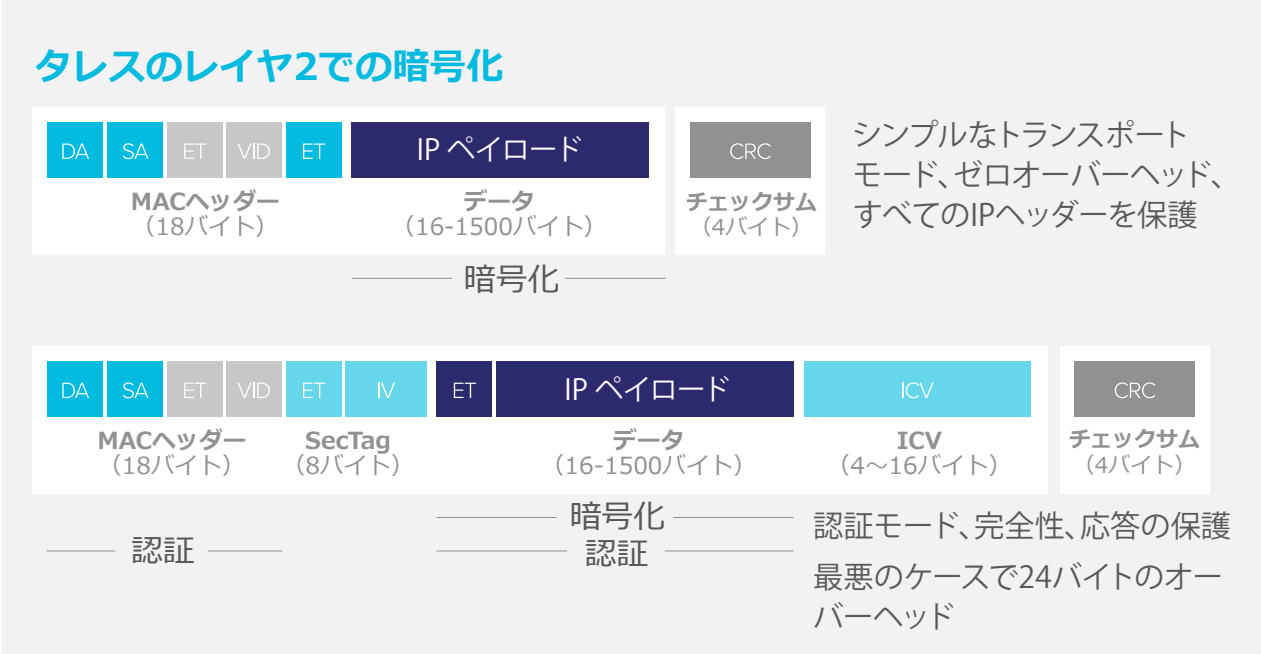

図3 – イーサネット暗号化のオーバーヘッド

お客様のメリット

このCCTVサービスプロバイダーがタレスのソリューションを導入する決め手となったのは、タレスのセキュアな高速ネットワーク暗号装置によるパフォーマンス上のメリットとネットワーク効率の高さでした。

タレスCNシリーズ高速ネットワーク暗号装置は、北欧全域の100以上のエンドポイントから送信されるデータを保護するために採用されました。

遅延、ネットワークオーバーヘッド、技術的な複雑さを最小限に抑えることで、タレスのCNシリーズ高速ネットワーク暗号装置はお客様が使用できる帯域幅を最大化し、管理時間とコストの両方を削減します。

タレスのセキュアな高速ネットワーク暗号装置は、認定された情報セキュリティを提供し、マルチキャストとユニキャストの両方のトラフィック配信のためにネットワークパフォーマンスを最大化します。シンプルな自動の「ゼロタッチ」鍵管理により、大規模な展開にも暗号化を効率的に拡張できます。

タレス独自のテクノロジーである、ネットワークトラフィックをワイヤースピードでカットスルー処理する専用ハードウェア暗号化エンジンは、ほぼゼロの遅延を実現します。

耐タンパ性を備えたシャーシは、すべての暗号鍵とユーザー資格情報を政府認定レベルで保護します。

タレスのCNシリーズ高速ネットワーク暗号装置は、すべての主要な国際的独立試験機関（FIPS、コモンクライテリア、CAPS、NATO）の認定を取得しています。

タレスのリモート管理ソフトウェア「CM7」を使用すると、多数の暗号装置を簡単かつ安全に管理できます。このツールは、SNMPv3　　を利用し、暗号化されたイーサネットポートを使用したアウトオブバンドまたはインバンドのいずれかのリモート管理を簡単かつ安全に行えるようにします。

メリットのまとめ

柔軟性:
タレス独自のFPGA（フィールドプログラマブルゲートアレイ）技術により、柔軟なカスタマイズが可能です。

相互運用性:
すべてのCNシリーズ高速ットワーク暗号装置は相互運用性があり、効率的な長期投資を実現します。

影響ゼロ:
タレスのCNシリーズ高速ネットワーク暗号装置は、他のネットワーク資産に影響を与えず、導入時にネットワークの変更を必要としません。

信頼性:
タレスの高速ネットワーク暗号装置は、最も要求の厳しい24時間365日の稼働環境においても、99.999%の稼働率を実現します。

アップグレード性:
各種CNシリーズ高速ネットワーク暗号装置の多くは、現場で交換およびアップグレード可能なコンポーネントを備えています。

拡張性:
他の暗号化ソリューションとは異なり、タレスのCNシリーズ高速ネットワーク暗号装置は、最大300接続まで拡張可能です。

タレスについて

皆様が信頼を寄せ、プライバシー保護を任せている企業は、その大切なデータを守るためにタレスの力を活用しています。データセキュリティにおいて、組織が直面する重要な課題は日々増え続けています。それが暗号化戦略の構築や、クラウドへの移行、コンプライアンス要件の遵守のいずれであっても、タレスは皆様のデジタルトランスフォーメーションを確実に保護するためのパートナーです。

図4 – CN6010高速ネットワーク暗号装置

cpl.thalesgroup.com/ja
お問い合わせ先 – Email: cpl.jpsales@thalesgroup.com
すべてのオフィスの所在地と連絡先情報につきましては、cpl.thalesgroup.com/ja/contact-usをご覧ください。