Case Study

ネットワーク暗号化により、自動運転データ収集センターと処理センター間の大量データ転送の安全性を確保

cpl.thalesgroup.com

THALES
Building a future we can all trust

アナリストは、完全自動運転車の年間販売台数が2035年までに1,200万台に達すると予測しています。自動車のコネクテッド化が進む中、自動車メーカーは膨大なデータパケットを収集することで、顧客行動を活用し、製品性能を理解し、故障を予測するためのインサイトを引き出しています。自動車メーカーとモビリティ企業は、そのデータの保護とプライバシーの保護という大きな課題に直面しています。このケーススタディでは、データを収集するIT企業、データを保管および分析するデータセンタープロバイダー、そしてタレスHSE（高速ネットワーク暗号化システム）との間の連携を探ります。タレスHSEは、自動運転車から収集されたデータの収集サイトと処理センター間の移動中データを保護します。

ビジネスニーズ ― IoTデータ保護

自動運転・先進運転支援システムのソフトウェア開発会社は、テスト車両から大量のデータを収集しています。この開発会社の目標は、自動化のSense-Think-Actモデルを使用して、自動運転車が人間よりも上手に運転できるようにすることです。自動運転車の良い動作、悪い動作、卓越した動作を研究することで、日々その目標の実現に近づいています。IoTのユースケースにより、ネットワークはますます複雑化し、多層化しています。かつてネットワークは独立したデータセンターを中心に構成されていましたが、現在ではクラウド、広範なアプリケーション、複数のデバイス（このユースケースでは自動車）に分散されています。

こうした課題に対応するため、このソフトウェア開発会社は、車両から常時収集されるペタバイト規模のデータを収集、処理するソリューションを必要としていました。ソリューションには、柔軟でスケーラブルなプラットフォームが必要でした。ビッグデータを専門とする多国籍企業が、データ分析と処理のための収集センターを提供しています。データ収集に加え、自動車とデータセンター間を行き来するデータを保護することも不可欠でした。IPsec VPNを使用した移動中データの保護はコストと時間がかかり、膨大な量のデータを移動するようには作られていません。

ソリューション ― 移動中データの暗号化

データセンタープロバイダーは、タレスのCN6140 Multilink Network Encryptor (CN6140) を選択し、この高速暗号化ソリューションを自社のサービス（ホスティングおよびその他のサービス）にパッケージ化し、マネージドサービスとしてソフトウェア開発会社に販売しました。IPsecの代わりにネットワーク暗号化システムを導入するという決定は、パフォーマンス、セキュリティ、予算のニーズに基づいてなされましたが、タレスの暗号化システムは、この3つのニーズすべてにおいて競合製品に勝っていました。タレスの高保証のネットワーク暗号化システムを使用して移動中データを暗号化することで、車両とデータセンター間を移動するデータが漏洩したり操作されたりすることがなくなります。

CN6140は、このようにスケーラビリティに対する要求が高くパフォーマンスが重視される環境に理想的なソリューションです。CN6140は、最大限のセキュリティとパフォーマンスを提供する高保証の高速暗号化ソリューションであり、最高レベルのセキュリティ標準に認定されています。

メリット ― セキュリティ、スピード、スケーラビリティ

タレスCN6140は、柔軟性とスケーラビリティに対する顧客のニーズを満たすと同時に、コスト削減とパフォーマンスの向上を実現しました。

パフォーマンス

CN6140は、高パフォーマンスのマルチリンク暗号化システムであり、全二重モードでパケットロスを発生させることなく、フルスピードで動作します。最大40 Gbps (4x10) のスケーラブルかつ高保証の移動中データの暗号化を実現します。

スケーラビリティ

CN6140により、データセンタープロバイダーは1台のコスト効率の高いマルチチャネルアプライアンスで、4x1 Gbpsから4x10 Gbpsまで拡張することが可能になりました。同プロバイダーは10 Gbpsから開始しており、40Gbpsまで拡張する予定です。この暗号化システムは、マルチポート設計により、最大40Gbps（4x10 Gbps）の可変速度ライセンスを備え、設置が容易で非常にコストパフォーマンスに優れています。デ

バイスは、メンテナンス、機能強化、セキュリティアップデートのために、現場で容易にフィールドアップグレード可能です。

セキュリティ

世界で最もセキュアな組織から信頼されている耐タンパ性を備えたCN6140は、コモンクライテリアEA4+およびFIPS 140-2 Level 3の要件を満たしており、標準ベースのエンドツーエンド認証付暗号化とクライアント側の鍵管理をサポートしています。

役割分掌

物理的および仮想的な職務分掌により、許可されたユーザーのみが暗号鍵にアクセスできるようにします。暗号鍵は、デバイスの耐タンパ性エンクロージャ内のハードウェアにて安全に生成および保管されます。物理的に鍵を抜き取ろうとする不正が試みられた場合、デバイスのゼロ化が発生します。

コスト

データセンタープロバイダーの最大の懸念はコストでした。IPsecでは、データエグレストラフィックのオーバーヘッドが30%増加することも珍しくなく、これがコストの増加につながります。IPsecからタレスHSEに切り替えることで、データセンタープロバイダーは、コストを削減し、パフォーマンスと帯域幅を向上させるとともに、最新のネットワーク用に構築されたスケーラブルかつ高保証の暗号化によって移動中データを保護することができました。

タレスについて

皆様が信頼して個人情報を預けている事業者の多くは、そのデータを保護するためにタレスのテクノロジーを採用しています。データセキュリティに関して組織が決断を求められる局面は次々と増え続けています。その局面が暗号化戦略の策定、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、デジタルトランスフォーメーションの推進と保護をタレスはお手伝いします。

決断の瞬間のための、確実なテクノロジー。

cpl.thalesgroup.com

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。