cpl.thalesgroup.com

THALES
Building a future we can all trust

APACの自動車技術メーカー、サプライチェーンのセキュリティをデジタル技術で確保

アジア太平洋地域の複数の自動車メーカーにソリューションを提供している、ある大手自動車技術サプライヤーは、モノのインターネット（IoT）接続デバイスの広範な採用を皮切りに、大規模なデジタル化のプロセスを進めていました。

IoTは現在、コネクテッドカー、自動車メンテナンスシステム、自動運転車、車載インフォテインメントとテレマティクス、フリートマネジメントなど、自動車製造において幅広い役割を果たしています。製造環境にIoTインフラストラクチャを追加することで、製造コストを削減し、サプライチェーンの効率を向上させ、デバイスのライフサイクルを適切に管理できます。しかしながら、これらのアプリケーションはインターネット通信に依存しているため、ハッキングの影響も受けやすくなっています。

課題

この大手自動車技術サプライヤーは、重要な自動車部品サプライチェーンのセキュリティを確保して、外部ハッキング、マルウェアを防ぎ、機密情報を保護する必要がありました。同サプライヤーのITチームは、これを実現するには、組織に暗号鍵管理の完全なオンプレミス制御が必要であると考えました。

さらに、自動車メーカーの分散したサプライチェーンの配置を考慮すると、ソリューションは、複数の場所に柔軟に実装できる必要があり、アジア太平洋地域全体の複数のOEMメーカーをサポートする必要がありました。

ソリューション

この自動車技術サプライヤーは、対処の必要性を感じていたデータセキュリティのあらゆる側面について数十年の経験を有するタレスを選定しました。

同自動車サプライヤーのデジタルセキュリティチームは、暗号鍵の信頼の基点として、FIPS 140-2 Level 3検証済みのThales ProtectServerハードウェアセキュリティモジュール（HSM）を導入しました。

ProtectServer HSMは、NIST SP800-90 TRNGをサポートしており、暗号鍵の生成のためにオンプレミスに展開されます。ProtectServer HSMには、安全な暗号化処理を高保証で実行する暗号化モジュールが含まれています。このアプライアンスは、物理的攻撃から保護する改ざん防止セキュリティを備えた堅牢なスチールケースを備えています。暗号鍵、個人識別番号、その他のデータなど、機密性の高い情報の保存と処理に、最高レベルの物理的および論理的保護を提供します。そのため、暗号鍵がHSMの外部に平文形式で公開されることはありません。

ProtectServer HSMは、同自動車技術サプライヤーに、他のソフトウェアでは得られないレベルのセキュリティを提供すると同時に、政府の規制や業界団体のセキュリティ要求を満たす認定レベルの機密性と整合性を提供しました。

結果

このアジア太平洋地域の自動車技術サプライヤーは、次の方法によって製造とそのサプライチェーンのセキュリティをデジタル技術で確保することができました。

- 運用要件を満たす必要性に応じて、複数の製造拠点およびサプライヤー拠点でのオンプレミス展開の組み合わせを通した、柔軟な公開鍵基盤（PKI）とHSMの運用を構築。
- サプライヤーの製造業務全体にわたる、自動車部品の暗号鍵管理に対する信頼性の高いオンプレミス制御により、製造のセキュリティを確保。
- 複数の国の製造拠点と外部サプライヤー両方のサプライチェーン全体で、グローバルにシームレスな展開を確保。

タレスについて

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な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順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を保護するためにタレスに頼ることができます。

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 – 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。