Case Study

三菱電機株式会社 三田製作所：タレスのLuna HSMによる暗号管理の導入でECUへのSW書き込みプロセスのセキュリティを大幅強化

cpl.thalesgroup.com

THALES
Building a future we can all trust

車は進化を続けています。

電気自動車、AD（自動運転）、およびADAS（先進運転支援システム）が普及期に入り、OTA（Over The Air）で車と外部との双方向通信を行いながら、メンテナンスしたり性能を高めたりするSDV（Software Defined Vehicle：ソフトウェア定義型自動車）も実用化しつつあります。

しかし、ソフトウェアで制御され、通信でアップデートされる車は、外部からの乗っ取りや情報漏洩などのリスクにさらされることになり、これまで以上に高度なセキュリティが要求されます。

兵庫県の三菱電機株式会社 三田製作所では、ADAS製品を電子制御するECU（Electric Control Unit）と呼ばれるマイコンにソフトウェアを書き込むプロセスに、タレスのLuna HSMを導入して大きく改革。ECUのソフトウェア開発から生産に至るライフサイクルを、一貫して強固に守る体制づくりに成功し、工場で実稼働させています。

選定のポイント

三田製作所では、高度化・多様化する車の進化を支えるADAS／ADに関わる多様な車両制御製品を、「安全・安心・快適・環境」をコンセプトとして開発しています。

注目を集める製品のひとつが、DMS（ドライバーモニタリングシステム）。車内に搭載したカメラでドライバーの状態をモニタリングし、居眠りやわき見運転を検知して警告を発するなどのアプローチで、安全運転をサポートするシステムです。

ADAS製品は、ECUが電子制御します。DMSの中枢を担うのも、車内カメラに組み込むECUであり、そのECUに書き込まれるソフトウェア（ファームウェア）です。

ECUのサイバーセキュリティは近年特に重視されており、UN-R155 / UN-R156、ISO / SAE2134などの国際規格を日本も積極的に取り入れています。

三田製作所でも、2022年秋、DMSを搭載しているOEM（三田製作所の顧客である自動車メーカーのこと）から、ECUの設計・生産工程の改革が求められました。

OEMが提示した条件は、AES （Advanced Encryption Standard：高度暗号化規格）の米国標準であるNIST FIPS 197を満たすことなど、多岐にわたりました。特に具体的に指示されたのが、開発中のソフトウェアは外部ネットワークと接続可能なサーバーに保存しないこと、設計と生産ラインとのソフトウェアのやり取りには暗号化を用いること、そして暗号鍵自身も保存するときには必ず暗号化することなどの要件でした。

三田製作所はさっそく、プロセス改革に取り組みました。

セキュリティ対策を講じてはいますが、社内サーバーは各種規格に抵触する懸念があるため、利用しないことを決断。PC端末と暗号処理をベースにセキュリティ・プロセスを再構築しました。

暗号処理については、様々な方法を検討しましたが、最終的に、HSMで発行・管理する強固な鍵で暗号鍵のライフサイクル全体を管理することにしました。

タレスのHSMを選定したのは、耐タンパ性に優れ、プロテクトできるレベルが高いなど、機能面で他社製品よりも優れていたからです。同じ価格帯で比べたときにセキュリティレベルが高いため、相対的に少ない投資でより良いシステムを構築できます。

また、三田製作所と同様に自動車関連製品を製造している同社の他の事業所でタレスHSMの導入実績があることが決定打となりました。生産ラインの暗号鍵管理に使って、実際に成果を上げているという実績を評価したのです。

機種としては、FIPS 140-2レベル3 認証を取得済みで、UN-R155/156にも対応しており、導入しやすい、小型フォームファクタのLuna USB HSMを選択しました。

ソリューション

「ソフトウェアは、設計エリアから生産ラインへの受け渡しプロセスを完全に暗号化する。暗号鍵はHSM内で作成し、鍵自身も暗号化した状態で保存する」。このプロセス改革はOEMから支持され、2023年秋からは新しいDMSの生産システムが順調に実働しています。

設計エリアには、Luna HSMとPCで「鍵生成装置」を構築。書き込むソフトウェアを暗号化したうえで、生産ラインの「鍵管理サーバー」へ構内LANで送ります。

生産ラインの「鍵管理サーバー」も、Luna HSMとPCで構成されています。ここで暗号データを復号してソフトウェア書き込みPCへ渡し、ECUへの書き込みへと進みます。

なお、「鍵管理サーバー」は、バックアップシステムをつないで二重化しています。冗長構成を構築しやすいのも、Luna HSMの特長です。

三田製作所は、HSMを利用することで、OEMが求めるハイレベルなプロセス改革を短期間で実現し、OEMの了解も獲得して、タイムリーに実稼働させることができました。

DMS市場は、今後急速な伸びが予想されます。

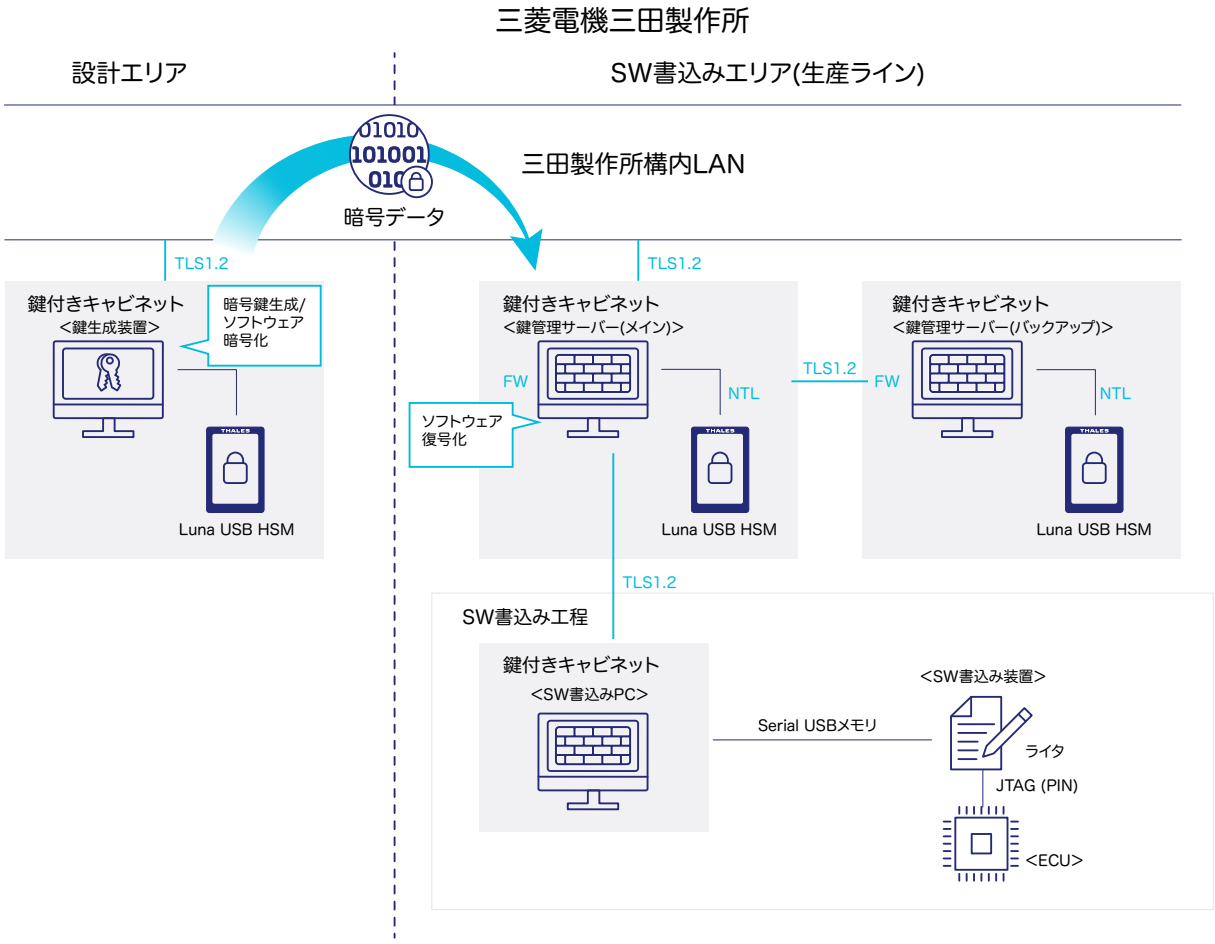
三田製作所は今後も、セキュリティの最新技術を積極的に取り込みながら、OEMごとに異なるセキュリティ管理要求へ柔軟に対応して、DMS市場の技術革新を牽引し、ひいては、ADAS市場全体の拡大に貢献していこうとしています。

Thales Luna USB HSMについて

Luna USB HSMは、USBインターフェースを備えたポータブルアプライアンスで、業界をリードする鍵管理を提供します。耐タンパ性を備えたハードウェア内にすべての暗号化された鍵マテリアルを保存することにより、高保証の鍵保護を提供します。小型フォームファクタとオフラインの鍵ストレージ機能が、本製品の特徴です。ビジネスクリティカルな鍵をセキュアなオフライン環境で保護する必要がある場合に最適で、データ、アプリケーション、デジタルIDを保護してリスクを低減し規制コンプライアンスを確保するために、製造業、政府機関、金融機関、大企業によって広く使用されています。

「自動車業界の大きな流れとしては、利便性が高まれば高まるほど、セキュリティ強化が求められることは必須です。OEMからより高いレベルのセキュリティ要求があったとき、タイムリーに要望を満たせるような製品を、タレスにはどんどん開発していただきたい。HSMに限定せず、より総合的でより高いレベルのセキュリティ・ソリューション提供を期待します。」

– 三菱電機株式会社 三田製作所
DMSソフトウェア設計部門 セキュリティ機能担当



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。

課題

- カーエレクトロニクス製品はECUが電子制御する。ECUに書き込むソフトウェア（ファームウェア）のセキュリティ確保がますます重要に
- ECUにソフトウェアを書き込むプロセスの刷新を、OEMが要望
- データの暗号化のみならず、暗号鍵そのものの暗号化など、OEMの要求は具体的でハイレベルだった

ソリューション

- ネットワークを介することなく、専用ハードウェアで発行・管理する鍵で暗号鍵のライフサイクル全体を管理できることからHSMを採用
- 採用を検討したタレスのHSMは、耐タンパ性に優れ、プロテクトできるレベルが高い。同じ価格帯で比べた時に、他社製品よりもセキュリティレベルが高かった
- 機種は、小型フォームファクタのLuna USB HSMを選定。FIPS 140-2レベル3認証を取得済みで、UN-R155/156にも対応しており、導入しやすい。

メリット

- 設計と生産ラインとのソフトウェアのやり取りには暗号化を用い、暗号鍵自身も保存するときには必ず暗号化するという要件を満たし、AESのNIST FIPS 197にも準拠したセキュリティ・プロセスを、比較的に短期間でシンプルに構築できた
- すべての暗号処理は、耐タンパ性を備えたFIPS認証取得済みのハードウェア内で行われ、ソフトウェア開発から実装までセキュアなライフサイクルを実現
- HSMを利用していることで、セキュリティレベルの高さをOEMに認知してもらえた
- タイムリーにプロセス改革が行えたことで、DMSの開発・製造が停滞することなく、順調に行えた

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。