コネクテッドカーの
セキュリティ保護

ENTRUST

SECURING A WORLD IN MOTION

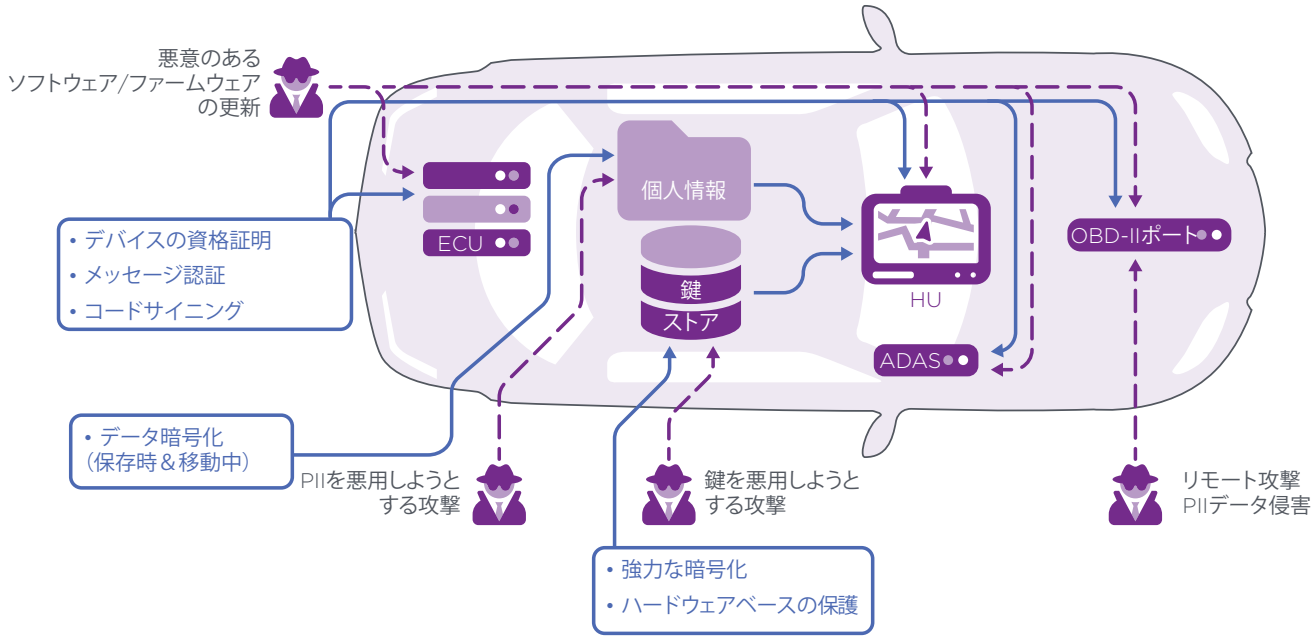
コネクテッドカーのセキュリティ保護

課題：次世代型の自動車がセキュリティ上の脆弱性をもたらす

今日の自動車には、67年型フォード社のマスタングと多くの共通点があるように、Apple社の iPhone とも同様に共通点があります。接続性が向上するにつれて自動車は複雑さを極め、それにより、次のような新たなセキュリティ上の脆弱性と課題が発生することになります。

- 自動車の安全、運用、およびインフォテインメント・システムに送信されるソフトウェアやファームウェアの更新を介した、マルウェアの感染
- 自動車のオンボード診断（OBD-II）ポートに接続されたウィジェットを含む、意図的または無意識のうちに自動車に追加された、安全ではない未承認のコンポーネント
- 大規模な公開鍵基盤（PKI）を設計および構築する、重要なセキュリティ担当者の人材不足
- 遠隔地の工場で未承認の生産が行われることで生じる、減収およびブランドに対する評判の低下

自動車の製造請負先（OEM）とそのサプライヤーは、データ保護戦略を構築するにあたり、Entrustが持つ専門知識と経験に大きな信頼を寄せています。当社のテクノロジーは、業界の進化し続ける需要に合わせて拡張可能であり、堅牢なセキュリティインフラストラクチャを確立するために必要となる、信頼の基点の構築を可能にします。



一部の自動車システムは分離されていることもありますが、脅威に関する調査によると、高度なスキルを持つ攻撃者が脆弱性を見つけ出す恐れがあることから、1つのサブシステムで不正アクセスが発生すると、攻撃者が他のサブシステムにも攻撃を仕掛ける可能性があります。

もう1つの課題は、拡張性のあるセキュリティ・インフラストラクチャの適切な設計に関連しています。具体的には、特定の攻撃から防御するために、接続されたコンポーネントを認証する必要があるということです。

自動車のOEMとそのサプライヤーは、暗号ベースのデジタル署名が最も強力な認証を提供することを認識していますが、これには証明書と基盤となる鍵の管理および保護も必要となります。接続されたコンポーネントの急速な増加により、PKIによってサポートされた、大規模かつ安全な鍵管理が必要となってきました。

ソリューションがもたらすメリット：

- 接続されたコンポーネントの信頼性を保証
- コードの更新を改ざんから保護
- ファームウェアとソフトウェアコードが社内ポリシーに準拠していることを保証
- PKIの整合性、パフォーマンス、扱いやすさを保証
- 顧客サービスと収益源を改善する機会を提供
- 未承認の誤った生産工程からの保護

さらに、ソフトウェアやファームウェアの更新は、さまざまな家庭用電化製品では一般的ですが、自動車のOEMやサプライヤーにとっては新たな領域です。このような更新はますます必要になっており、今日では通常、販売代理店にて実行されるため、コストがかさみ顧客に負担を与えています。

接続されたコンポーネントにコードの更新を送信するにあたり、無線（OTA）で配信する場合でも、サービスセンターで配信する場合でも、悪意のある動作や意図しないエラーが発生する可能性があります。適切なセキュリティプロトコルがなければ、破損したコードが自動車に導入される恐れがあります。また、製造業者は、コードが組織のポリシーに準拠していることを保証する必要があります。

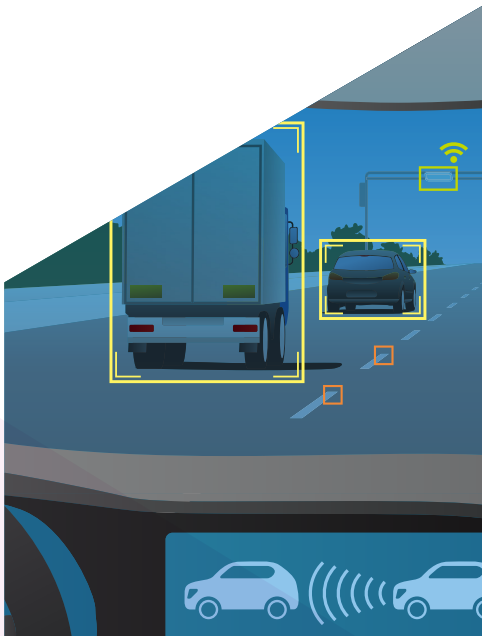
さらに、システムとデータを制御することの難しさもあり、セキュリティを取り巻く状況はますます複雑化してきています。その例として、次のようなものが挙げられます。

- 多くの消費者に支持されている法令を修正する権利により、自動車メーカーは、修理のために代理店以外の整備士が自動車システムにアクセスすることを許可する必要があり、セキュリティ上の懸念をもたらす可能性がある
- 消費者は、新たなOBD-IIポートデバイスによって提供される機能（保険割引のためのテレメトリ追跡、10代のドライバーの追跡など）を望んでいるが、自動車メーカーは、自動車環境へのなじみのない製品の導入を歓迎していない

コネクテッドカーは大量のデータを生成するため、課題が発生します。具体的には、次のようなものが挙げられます。

- メンテナンスの追跡やOBD-IIポートに接続された消費者向けデバイスに使用できるテレメトリデータは、地域ごとのプライバシー規制に従い、移動中または静止時に保護する必要がある
- 接続されたコンポーネントによって送信されるデータは、信頼できるソースから送信されたものであることを確認するために、認証される必要がある
- データ保護は不可欠であるが、分析を妨げるものであってはいけない

さらに複雑さを増加させるものとして、2017年に生産車両に初めて導入された車車間通信および路車間（V2X）通信は、まもなく標準となる予定で、これにより製造業者には、必要な技術を特定して実装することが求められます。移動中の自動車は、輸送エコシステムの他の参加者との間で、テレメトリデータを安全に配信および受信できる必要があります。



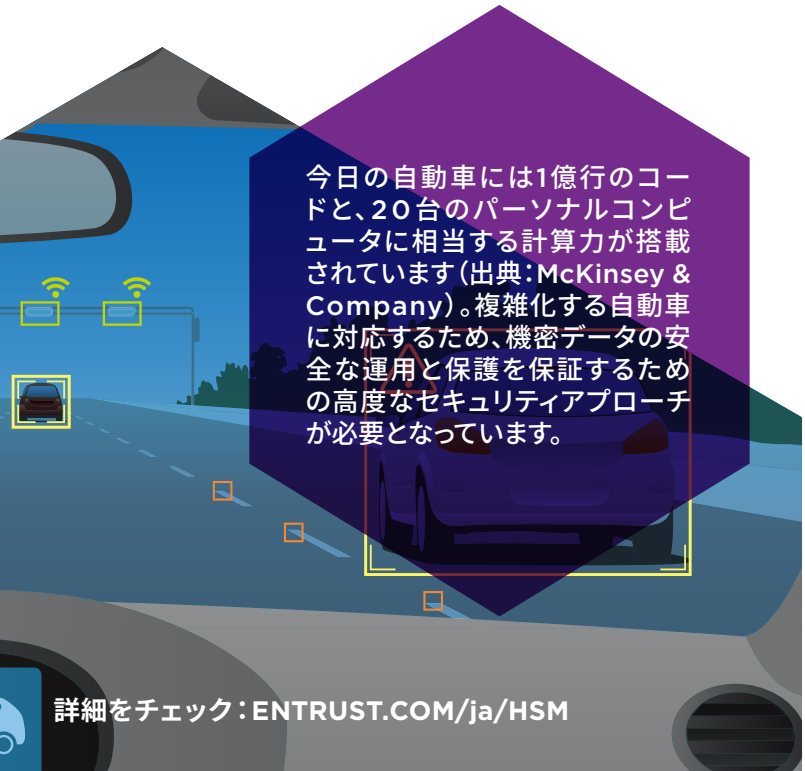
ソリューション：Entrust nShield HSM、コードサイニング、およびPKIサポート

現代の自動車がもたらすセキュリティに関するさまざまな課題に対処するために、Entrust nShield®ハードウェア・セキュリティ・モジュール（HSM）を使用することで、製造業者は、最初の製造時に導入されたものであっても、交換品として導入されたものであっても、接続された各コンポーネントにユニークなIDを与えることができます。このセキュリティシステムは、非常に強力な暗号化処理、鍵の保護、および鍵の管理を使用して以下を可能にします。

- 各コンポーネントに対する強力な認証
- V2Xエコシステムの一部として、および、メンテナンスの追跡などのアプリケーション向けの、テレメトリデータの信頼度の高い通信
- 承認されたコードの更新
- 効果的なPKIの基盤構築
- 不正かつ欠陥のある生産に対するより強力な防御機能

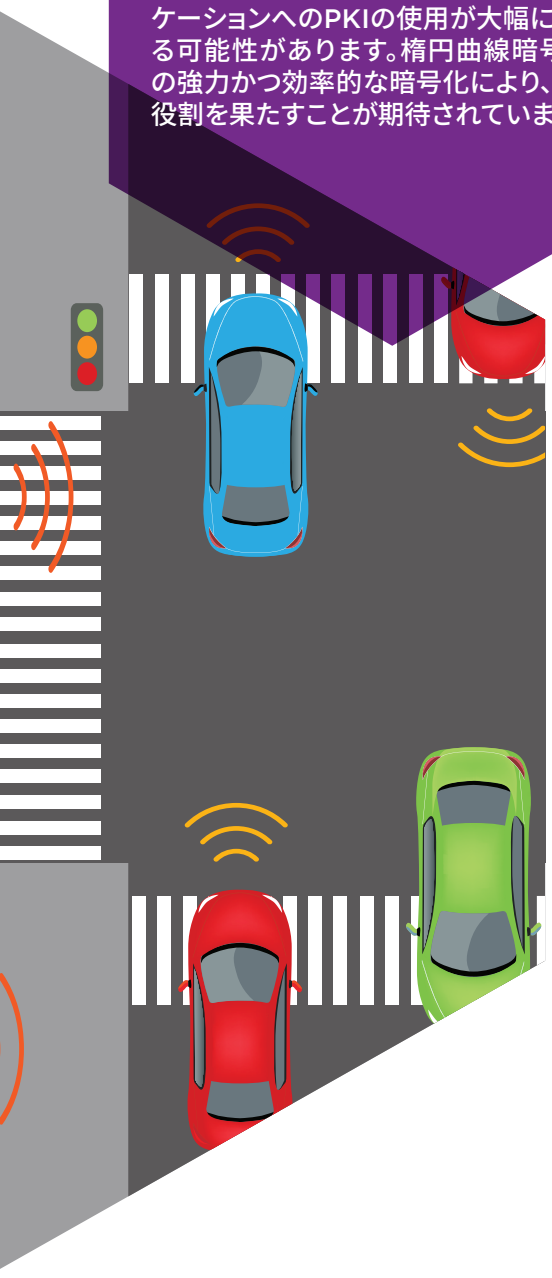
接続されたコンポーネントのデジタル資格情報を確立するための最も安全かつ業界で認められた方法は、ハードウェア・セキュリティ・モジュールを使用して、基盤となる鍵を作成および保護することから始まります。製造業者は、Entrust nShieldと補助的なセキュリティアプリケーションを組み合わせることで、鍵要素および関連するデジタル証明書のプロビジョニングを制御し、それぞれが、承認されたコードのみを使用してロードされるようにすることができます。また、地理的に分散したサプライチェーンであっても、生産されるユニット数とそれぞれに組み込まれるコードを制御することで、偽造を防ぐことができます。さらに、自動車の最終検査の一環として、必要なすべての証明書が確実に配置されるようにすることで、品質管理が強化されるというメリットも享受することができます。

強力な認証を実施することで、コンポーネントはOTAソフトウェアおよびファームウェアの更新を受け取ることができます。これにより製造業者には、更新を発行するコストを削減しながら、新たな収益源を開拓し、新機能の導入に対するドライバーの満足度を高めることができるという、大きな機会がもたらされます。



詳細をチェック：ENTRUST.COM/ja/HSM

メッセージを共有する自動車とインフラストラクチャ要素を効率的に検証する必要があるため、運輸業界において、V2Xアプリケーションへの PKIの使用が大幅に拡大する可能性があります。楕円曲線暗号は、その強力かつ効率的な暗号化により、重要な役割を果たすことが期待されています。



Entrustのコードサイニング

コード更新の整合性を確認し、ソフトウェアの改ざんに関連するリスクから防御するためのベストプラクティスは、HSMによって保護された秘密署名鍵を使用して安全性の高い署名プロセスで、コードが署名されていることを保証することです。

Entrustのコードサイニングソリューションには、nShield HSMとEntrust nShieldプロフェッショナルサービスを組み合わせています。nShieldは、個人の署名鍵に改ざんを防止する認定された保護を提供し、重要なデジタル署名プロセスを実行するための安全なプラットフォームを提供します。

公開鍵基盤に対するサポート

自動車メーカーおよびサプライヤーの大規模な業務を考慮すると、デジタル証明書を管理し、署名鍵を保護するためのソリューションが必要です。業界をリードする当社のPKIパートナーと連携する場合でも、サポートのためにnShieldプロフェッショナルサービスを利用する場合でも、Entrust nShield HSMは、規模や複雑さを問わず、ニーズを満たすことができるPKIの導入を実現します。証明書の発行プロセスを保護し、署名鍵を積極的に管理することで、証明書の紛失や盗難を防ぎ、デジタルセキュリティに対する信頼性の高い基盤を構築することができます。nShield HSMは、独立機関によって認定された耐タンパ性デバイスであり、組織内の非常に機密性の高い鍵やビジネスプロセスを保護するために使用され、PKIのベストプラクティスとして広く認識されています。

自動車メーカーでのPKIの導入ユースケースには、下記のものがあります。

- 製造工程で挿入されるデジタル証明書を含む、接続されたコンポーネントの信頼性の保証
- OTAの更新：ソフトウェアとファームウェアの更新パッケージは暗号化および署名され、車両に配布されます
- V2Xアプリケーション：CAが証明書を発行および管理するための信頼できるソースとして機能し、コンポーネントが本物であることを検証します

大量の証明書と堅牢なPKIが必要になるV2Xのユースケースは、注目に値します。また、輸送コミュニティの主要な組織（米国国道交通局、欧州委員会合同調査センターなど）が、強力かつ効率的な暗号化を実現するために、V2Xへの楕円曲線暗号の採用を推奨していることも注目すべき点です。

自動車会社から信頼されているEntrust

Entrustの顧客には、北米の上位3社のOEMのうち2社、およびヨーロッパの主要サプライヤーの3分の2が含まれます。

まとめ

自動車メーカーはEntrust nShield HSMを使用することで、接続されたコンポーネントごとにユニークIDを確立し、接続されていないコンポーネントやコード更新のリスクから保護することができます。また、Entrust nShield HSMとプロフェッショナルサービスは、製造業者が使用するPKIの整合性、パフォーマンス、および管理性を保証できるようサポートします。

当社が提供する自動車のセキュリティ戦略推進サポートについては、**www.entrust.com/ja**をご覧ください。

Entrust nShield
HSMの詳細はこちら：

HSMinfo@entrust.com
entrust.com/ja/HSM

ENTRUSTについて

Entrust は信頼できる認証、支払い、データ保護を実現することで、動き続ける世界をセキュアにしています。今日、支払いや国際取引、電子政府サービスへのアクセス、そして企業ネットワークへの認証において世界中でより安全で円滑なユーザ体験が求められています。Entrust はこれらの要となる部分において、他に類を見ない幅広いデジタルセキュリティとID発行ソリューションを提供しています。2,500人を超える従業員、グローバルパートナーネットワーク、そして150カ国以上におよぶ顧客に支えられ、世界で最も信頼されている組織から信頼されています。

詳細は下記URLをご覧ください。
entrust.com/ja/HSM

お問い合わせ：
HSMinfo@entrust.com