コネクテッドカーに求められるセキュリティ対策

杉山 歩　　(株)ヴィッツ

1. はじめに

自動車業界は今，「100 年に 1 度」と言われる変革期にあり，「CASE」と言われる 4 つのキーワードへの対応が求められています。CASE とは，C=Connected（コネクテッド），A=Autonomous（自動運転），S=Shared & Services（シェアリング），E=Electric（電動化）の頭文字で，独ダイムラーの社長が 2016 年のパリモーターショーで発表した経営ヴィジョンです。

しかし，CASE が示す 4 つの変化は自動車に対するハッキングの可能性を高め，その被害を大きくしてしまうなどのリスクを持っています。ここでは，コネクテッドカーを含めた次世代の自動車に考えられるハッキングの脅威と，ハッキングを防ぐために各企業に求められるセキュリティ対策の全体像を紹介します。

2. 次世代自動車に対するハッキング

従来の自動車は他の自動車や製品とはつながらず，独立に動作する“スタンドアローン”な制御システムでした。しかし，コネクテッド化から始まる自動車の変化に伴って，これまで考える必要のなかった様々なハッキングの脅威への対処が必要となります（図 1）。

そのなかでも特に，自動運転システムに対してハッキングがされた場合，走行中の車両の制御が乗っ取られ，交通事故の誘発に繋がる恐れがあります。そのような事態を防ぐため，ハッキングに対抗するためのセキュリティ技術と，自動車業界で培ってきた安全性を担保する技術を組み合わせ，自動運転システムの安全性を担保していく必要があります。

図 1　次世代自動車に考えられるハッキングの脅威

2.1　コネクテッド化に伴う攻撃経路の増加

現在のコネクテッドカーにはサーバやスマートフォンと通信を行い，便利なサービスを提供する機能が搭載されるようになってきています。しかし，これらの新しい機能に対するセキュリティ上の考慮が不足しており，多くの研究者（ホワイトハッカー）から，製品に多くの脆弱性が残っていると指摘されています。

2015年に米FCA US社（旧Chrysler社）の「ジープ・チェロキー」に対するハッキングの手段が公開されていますが，そこでも車両が持つ3GやWi-Fiなどの無線通信IFからアクセス可能な脆弱性を悪用されています。また，このハッキング事例では，無線通信経由（OTA：Over The Air）でECUのソフトウェア更新が可能であったため，「無改造車両に対する遠隔地からのハッキング」の実現に繋がりました（図2）。

2.2　OTAソフトウェア更新の利点／欠点

コネクテッド化により普及が始まっているOTAによるソフトウェア更新は制御プログラムの更新・変更は，サービス／利便性の向上だけでなく，セキュリティ対策としても重要な役割を持っています。

具体的には，制御プログラムに何らかの脆弱性が報告された際にOTA経由で修正パッチを当てることで，ハッキングの脅威から自動車を守ることができます。

しかし，OTAソフトウェア更新機能自体がハッキングされることにより，ハッカーが任意の車の制御プログラムを遠隔から書き換えることが可能になってしまうため，諸刃の剣とも言える機能とも言えます。そのため，OTAソフトウェア更新機能の必要性と危険性を正しく理解し，必要なセキュリティ対策と合わせた導入が必要となります。

OTAソフトウェア更新のセキュリティ対策
- ソフトウェア配布元（サーバ）の認証
- ソフトウェア配布経路の暗号化
- ソフトウェア開発元（デジタル署名）の検証
- ソフトウェアの完全性／新鮮性の検証
- 問題発生時のロールバック機能
- ソフトウェア更新記録の保存　…etc

3.　セキュリティの法規化／標準化動向

2015年にジープ・チェロキーがハッキングされて以降，自動車業界全体でセキュリティ対策の法規化／標準化が急ピッチで進んでいます。

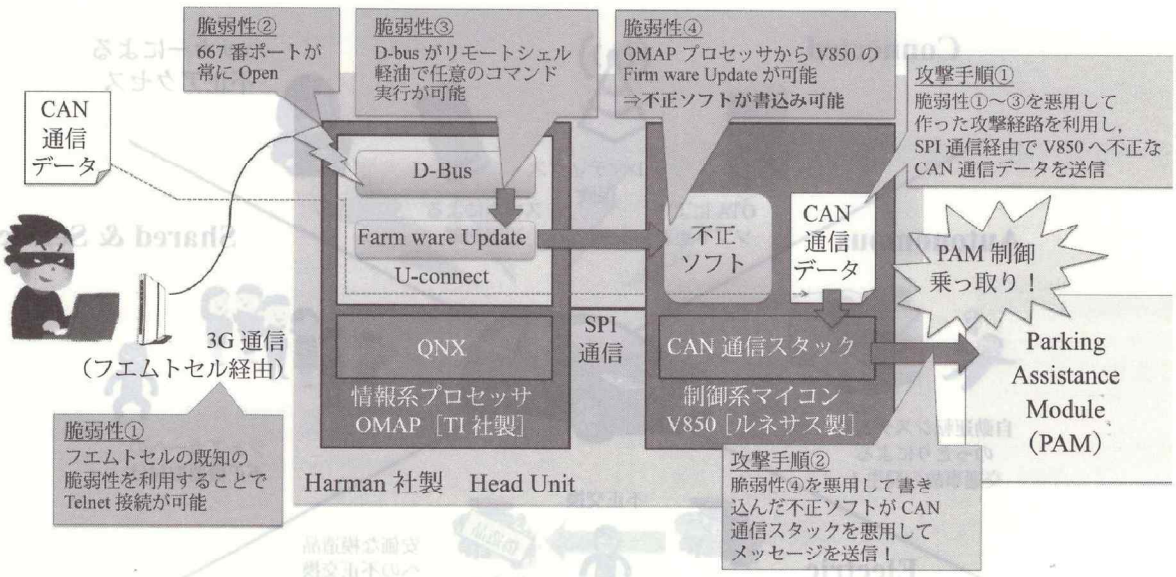

図2　ジープ・チェロキーのハッキング手段

ここでは標準化の代表事例としてISO/SAE 21434を，法規化の代表事例としてWP29（World Forum for Harmonization of Vehicle Regulations）の動向を紹介します。

3.1 ISO/SAE 21434による標準規格

現在，自動車向けセキュリティ規格“ISO/SAE 21434”の策定が開始され，自動車のライフサイクル全体（製品企画～廃棄まで）を通じて，セキュリティ対策の実現に必要な実施事項が規格要求として策定が進んでいます。

ISO/SAE 21434で規定される要求は，SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systemsをベースに，情報セキュリティにおける評価基準を定めたISO 15408などの内容を取り込む形で議論されています。

ISO/SAE 21434およびベースとなるSAE J3061は，自動車にサイバーセキュリティマネジメントシステムを適用するために，自動車向け機能安全規格であるISO 26262と類似したフレームワークを取っており，特に開発フェーズにおいてはISO 26262のアウトプットと一貫性が取れるような構成となっています。

ただし，自動車の生産・運用・廃棄に関するフェーズでは，市場に流通している自動車の脆弱性／インシデント対応として，フィールド監視による情報収集から修正パッチを当てる仕組み（OTAを含む）の構築や，中古車販売を行う際の個人情報の保護や自動車の廃棄を行う際に暗号鍵が漏洩しないように削除する仕組みの構築など，機能安全にはないセキュリティ特有の要求が策定される見込みです。

なお，ISO/SAE 21434のベースとなるSAE J3061と，ITシステム向けISO 15408や制御システム向けIEC 62443を比較すると，一部SAE J3061では規定されていない内容があります。具体的には，ISO 15408ではPart2で機能セキュリティコンポーネントという形で，対象製品に搭載するセキュリティ機能に関する要求が定義されています。これは制御システム向けのセキュリティ規格であるIEC 62443でも同様です。しかし，SAE J3061では自動車開発で実施すべき活動については要求されていますが，自動車に搭載すべきセキュリティ機能については要求として明記されていません。

そのため，自動車に搭載するセキュリティ機能を検討する際には，ISO 15408などの他のセキュリティ規格や米国のNHTSA（National Highway Traffic Safety Administration）などが発行しているガイドラインを参照する必要があります。

3.2 WP29による各国法規の国際調和

自動車に対するセキュリティ対策の検討が各国／各団体で進んでいるなか，その基準に大きな乖離が発生しない様，WP29にて，自動運転車（コネクテッドカー）の情報セキュリティ対策の議論が進んでいます。

WP29では傘下に設置されたITS/AD（Intelligent Transport Systems / Automated Driving）が，2016年にCybersecurity And Data protectionに関するガイドラインを発行しています。その後，自動運転車のサイバーセキュリティとOTAに関するタスクフォース（TF-CS/OTA）が発足し，日本とイギリスが共同議長となり活動を進めています。その中で，当初はRecommendation化の議論が進んでいましたが，2018年頃よりRegulation化に向けての議論へ変化しつつあります。

TF-CS/OTAではすべての車両（カテゴリーL, M, N, O, R, S, および，T）を対象に，車両の型式認証時に「サイバーセキュリティマネジメントシステム（CSMS）の実施」を評価することが要件案として挙がっています。この要件を満たすためには，例えばISO/SAE 21434にて規定されているセキュリティ活動が，サプライチェーン全体（OEM～サプライヤまで）を通して正しく適用しなければなりません。

WP29 TF-CS/OTAの法規案が成立した際には，法規適用の猶予期間内にCSMSの適用ができていないと，車両の販売ができなくなる可能性もあるため，法規要件の議論状況を注視しながら，適用の準備を進める必要があります。

4. 企業に必要なセキュリティの取り組み

自動車に対してCSMSを適用するためには，① 自動車に搭載するセキュリティ対策を決定し，② 自動車の

本来機能上にセキュリティ対策を脆弱性なく設計・実装し，③ 自動車の販売後にもセキュリティ対策を維持できる仕組みを構築する必要があります。これらの取り組みはそれぞれ単独で完結するものではなく，それぞれの活動を連携させて，自動車に対するセキュリティ対策として構築する必要があります（図 3）。

4.1　脅威分析によるセキュリティ対策の導出

自動車に対するハッキングによる脅威を防ぐためには，まず自動車に対して脅威分析を行い，脅威を防ぐためのセキュリティ技術を導出する必要があります。

その際に脅威分析の対象を明確化して範囲を絞り，脅威分析を発散させないための「方針」の定義が重要となります。

セキュリティ対策の方針は，業界動向（過去のハッキング事例を含む）や規格／法規を考慮した上で，想定する脅威と考えられるリスクを比較し，どこまでのセキュリティ対策を実施するかを明確化する必要があります。

その上で，ハッカーにはシステム上の最も弱い箇所（攻撃しやすい箇所）が狙われることを考慮して脅威分析を実施し，その結果から弱い箇所を特定して対策を施すための要求仕様を定義します。

セキュリティ要求を定義する際には，規格やガイドラインに記載されているセキュリティ機能を参考にすることができます。セキュリティ機能は，異なる規格であってもほぼ同じ機能要求を示していますが，規格毎に記載粒度や表現が異なるため，目的や工程毎に参照する要求を使い分けることができます。

ここでは具体例として，ISO 15408 Part2 に定義されている SFR（セキュリティ機能要求）の一覧と，制御システム向けセキュリティ規格である

IEC 62443 3-3 に定義されている FR（Foundational Requirements）/ SR（System Requirements），および，NHTSA が発行しているセキュリティガイドライン（Cybersecurity Best Practices for Modern Vehicles）に定義されている自動車に適用すべきセキュリティ要求を比較し，規格毎の特徴を整理した事例の一部を紹介します（図 4）。

これらの規格／ガイドラインを比較すると，IEC 62443 の要求はセキュリティの 3 特性である“CIA”との対応が取りやすいことから脅威に対抗するためのセキュリティ対策技術の導出に利用しやすいことがわかります。それに対して，ISO 15408 の要求はセキュリティ対策の設計＆実装時に脆弱性を残さないためのポイントが要求として定義されています。それらのセキュリティ規格と比較すると，NHTSA のガイドラインは自動車業界の人間からすると理解しやすい記述になっていますが，必要な要求が全て書かれているわけではないことに注意が必要です。

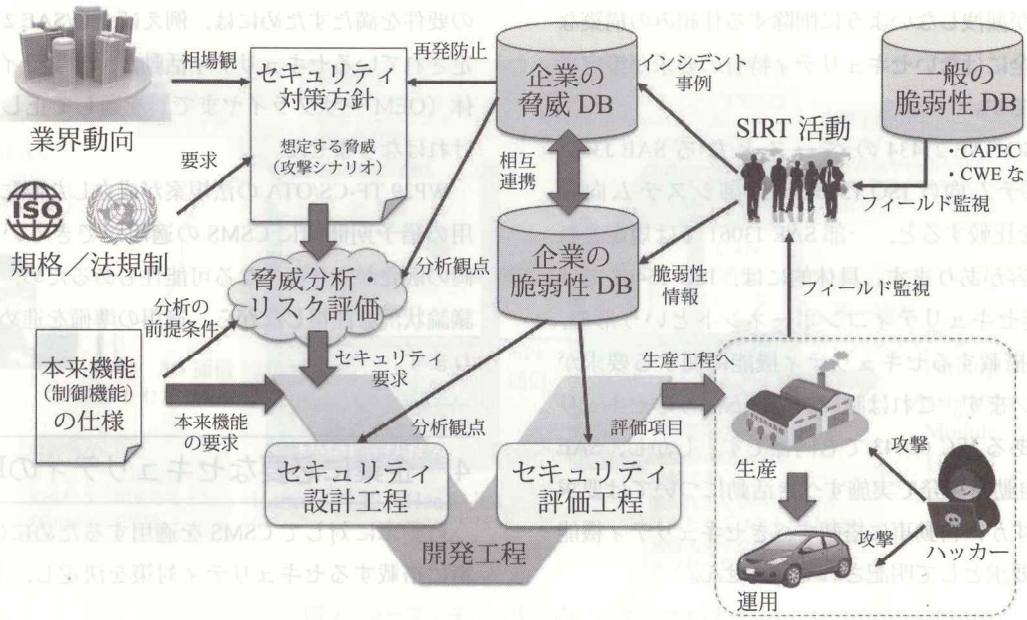

図 3　自動車に対するセキュリティ対策の全体像