［ハードウェアセキュリティの最新動向］

⑥ 自動車サイバーセキュリティの基本 ―車載ネットワークと攻撃例―

基般

Camille Gay | 産業技術総合研究所

自動車におけるセキュリティの懸念

2015 年に FCA 社の Jeep Cherokee に 3G ネットワーク経由で勝手に遠隔操作される可能性のある脆弱性がセキュリティリサーチャーにより発表され，約 140 万台の車両がリコールされた．その事件が広くメディアに報道され，自動車のセキュリティ対策の必要性が初めて世間に知られた．しかし，自動車セキュリティは決して新しい研究分野ではない．自動車にまつわる犯罪は昔から多く存在している．車上荒らし，自動車盗難，自動車部品の偽造，不正改造，メータ改ざんの詐欺等といった迷惑行為が毎日世界中に発生している．また，盗難車は別の犯罪を実行するために使われることが多いので，車の所有者の問題だけではなく，深刻な社会問題でもある．

最近，自動運転のアルゴリズムや運転支援システムの開発が進み，車の ECU（Electronic Control Unit，電子制御機器）が制御できる範囲が広がっている．たとえばステアリングやブレーキ等の致命的な装置が高機能のコンピュータに制御されるようになった．それらのコンピュータが仮に攻撃者に乗っ取られれば，重大な事故を起こせる可能性がある．言い換えると，ECU の脆弱性のインパクトが劇的に上がったといえる．一方，車を Bluetooth，Wi-Fi，インターネット等に接続する“コネクテッドカー”の通信機能が普及してきた．加えて，車と車を接続する“V2V”（Vehicle to Vehicle）の通信機能や，車とインフラを接続する“V2X”（Vehicle to X）の通信機能も実証実験の段階にまで進んでいる．車は電子機器のない機械的な乗り物から，スマートフォンに劣らない接続性を持つ複雑な電子ネットワークに変化した．それらの機能を実現するためには，多くのハードウェア技術やソフトウェア技術が必要である．図 -1 に示す通り，車に脆弱性が潜在する可能性のあるコンポーネントが多くなり，車に脆弱性が存在する確率も劇的に上がった．

自動運転とコネクテッドカーの時代に備え，自動車メーカもビジネスモデルを変えている．自動車を製造するだけでなく，モビリティのディジタルサービスを提供する会社に変化している．そのため，車は乗客の個人情報を多く発生させる・取り扱う乗り物になりつつある．従来の自動車法規に加え，個人情報保護規制に対応する必要が生じた．近年，「ハッカーに遠隔されないか」や「自分の個人情報が車から流出するのではないか」等と，世間から深刻に心配されるようになり，自動車メーカのセキュリティ対策が注目を浴びている．

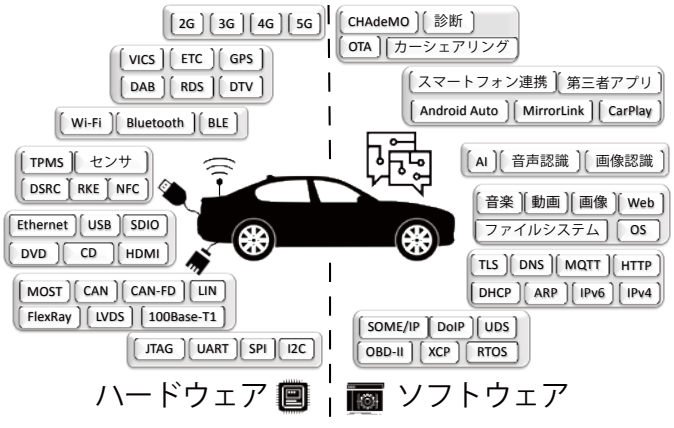

図 -1　車が攻撃を受ける可能性のある機能の例

自動車業界特有の課題

セキュアな車を開発するには，自動車業界は多くの課題を解決する必要がある．まず，自動車業界は複雑なエコシステムでできている．車載ネットワークは多くの ECU で構成されているが，ECU を設計しているのはティア 1 の企業（自動車メーカに直接納入する一次サプライヤ）である．また，それらの ECU に使われるハードウェアやソフトウェアを開発しているのはティア 2 の企業（ティア 1 の企業へ自社製品を供給する二次サプライヤ）である．自動車メーカ・ティア 1・ティア 2 はお互い完全に情報を共有していないため，自動車のセキュリティ対策を管理することは簡単ではない．

ハードウェアセキュリティの分野では，極端な温度での対策は難しいと言われている．一般的に使われている IC カード（クレジットカード等，きわめて薄い半導体集積回路がプラスチックに埋め込まれた認証用のカード）の使用温度範囲は−25 ～ 85℃であるのに対し，車に使われる部品（いわゆる車載グレード部品）の使用温度範囲は最大で−40 ～ 150℃である．IC カード等は極端な温度では動作停止が許されるが，車は極端な温度であっても動作停止・誤動作すれば，乗客の命を危険にさらしてしまう．また，車には非常に高い信頼性が求められている．IC カードの読み取りエラーは，誰でも経験したことはあるだろう．しかし，車のエラーは事故につながる可能性があるため，IC カードと同じ失敗率は許されない．

IC カード等は，故障した場合は交換すれば済む．しかし，車は原因不明の事故に遭った場合，ECU に不具合があったことが疑われる．その不具合の原因を究明するため，不具合解析ができる環境を保障する必要がある．一方，攻撃者に製品が解析されないよう，開発用の機能を無効化したり，ソフトウェアを難読化したりすることがよく用いられるセキュリティ対策（リバースエンジニアリング対策）である．しかし，不具合解析をしやすい環境では，製品を解析しにくくするリバースエンジニアリングの対策は実装しにくい．

広い使用温度範囲で高い信頼性を保障できる対策は高額になる傾向があり，低コストでの量産が求められるある車での採用は一般に難しい．一方，セキュリティレベルが低すぎると，脆弱性が悪用され，リコールや集団訴訟につながるリスクもある．うまくバランスをとることが自動車業界の会社には求められている．

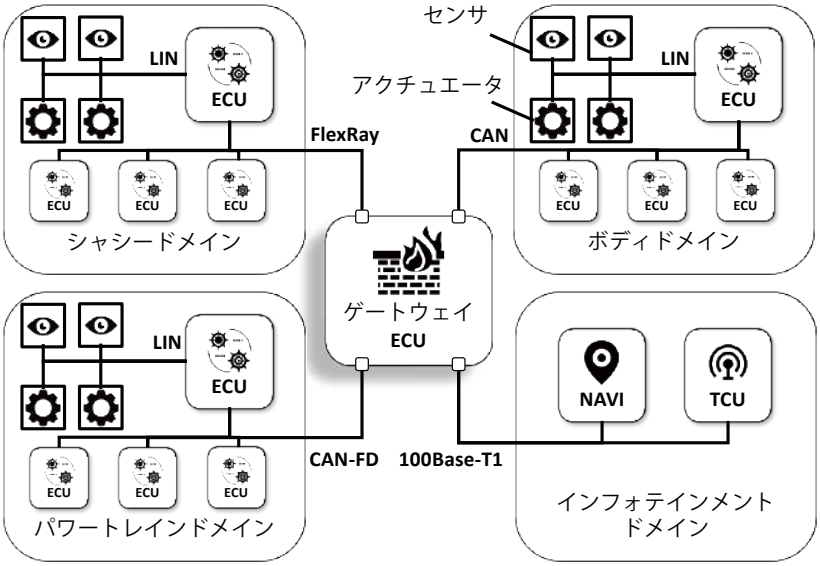

図 -2　車載ネットワークの例

車載ネットワークの概要

現代の車の車載ネットワークの代表例を図 -2 に示す．車は多くの ECU で構成されている．それぞれの ECU に役割が与えられている．たとえば，ブレーキはブレーキ ECU により制御されている．役割を果たすためには，センサとアクチュエータが必要である．ケーブル線の本数を最小限に抑えるため，センサとアクチュエータを同一の LIN バス（Local Interconnect Network）に接続することが多い．また，ECU と ECU の

間の情報交換も多く行われている．たとえば，ブレーキペダルの状態を，ストップランプを制御する ECU に知らせる必要がある．ECU 間の通信のために設計された通信手段には，CAN（Controller Area Network），CAN-FD（CAN with Flexible Data-rate）と FlexRay がある．また，高速通信の車載用通信手段では，MOST（Media Oriented Systems Transport）と 100Base-T1（Automotive Ethernet）が現在の主な選択肢である．

ECU の数が多ければ多いほど，通信量が上がり信頼性が下がるため，ECU をドメイン（サブネットワーク）で分ける考え方が最も浸透している．図 -2 では，よく使用されるドメイン分けを示している．シャシードメインは車の曲がる・止まる機能を実現している．パワートレインドメインはエンジンやトランスミッションの機能を実現している．ボディドメインはドア，窓，エアコンや照明の機能を実現している．インフォテインメントドメインは通信量の多い NAVI とテレマティクス機能を実現している．なお，ドメインをまたぐ ECU 間の通信も必要である．上記のブレーキペダルとストップランプの例では，シャシードメインとボディドメインをまたぐ必要がある．そのため，それぞれのドメインを接続するセントラルゲートウェイが使われている．ゲートウェイはドメインをまたぐメッセージを厳格にフィルタリングするべきではあるが，実際の車両では必ずしもそのように実装されているとは限らない．

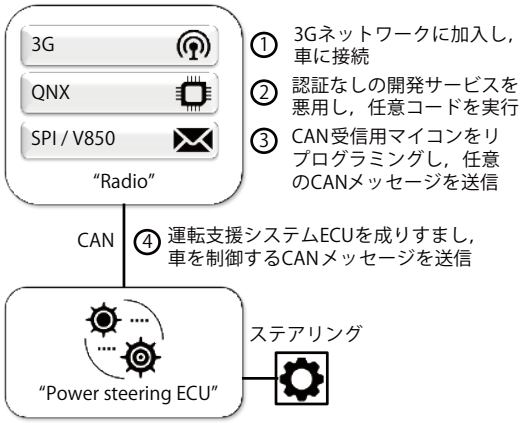

図 -3　Jeep Cherokee 攻撃の概要

実際にあった脆弱性の報告の例

2015 年 Jeep Cherokee（3G からの攻撃例）

2015 年に報告された Jeep の脆弱性 [1] をここで簡単に説明する．攻撃の流れを図 -3 で示す．

①車との遠隔通信手段を確保

Jeep Cherokee の NAVI が接続していた 3G ネットワークには，通信ポートの制限や，クライアントとクライアントの間の通信の制限がなかった．結果として，同じ 3G ネットワークに加入していた研究者は遠距離でも車に接続できた．

② NAVI に任意のコードを実行

NAVI にファイアウォールが設定されず，認証なしの開発用のサービスが稼働していたため，NAVI に任意のコードを実行できた．

③ CAN 通信モジュールに任意のコードを実行

NAVI には CAN バス受信専用のマイコンが搭載されていた．本来，任意のメッセージを送信する機能はなかったが，そのマイコンに認証なしのリプログラミング機能があったことを悪用し，任意のメッセージを送信できるファームウェアで研究者がリプログラミングできた．

④ステアリング ECU 等にメッセージを送信

車にゲートウェイ ECU がなく，NAVI とステアリング ECU は同一の CAN バスに接続されていた．また，CAN バスのメッセージの認証がなかったため，“曲がれ”の命令を送れば，車が曲がった．

2017 年 Tesla Model S　（Wi-Fi からの攻撃例）

2017 年に報告された Tesla Model S の近距離遠隔操作の脆弱性 [2] をここで簡単に説明する．攻撃の流れを図 -4 で示す．

①車との無線通信手段を確保

NAVI に Wi-Fi 機能があり，ディーラーの Wi-Fi ネットワークに自動的に接続する仕様になっていた．しかし，共通のパスワード“abcd123456”での弱い認証しかなかった．成りすましの Wi-Fi ネットワークを立ち上げ，車から接続してもらうことで，通信手段を確保できた．

② NAVI に任意のコードを実行

Wi-Fi 接続後，NAVI が自動的に Web ページをロードしていたが，JavaScript の実行エンジンにソフトウェア脆弱性があり，NAVI で任意のコードを実行できた．また，Linux の公知脆弱性を悪用することで権限上昇し，車載ネットワーク内のイーサネットに任意のメッセージを送受信できた．

③ゲートウェイ ECU に任意のコードを実行

イーサネット接続先のゲートウェイ ECU に，弱い認証の診断機能があり，ゲートウェイ ECU で任意のコマンドが実行できた．

④ ECU 等にメッセージを送信

制御 ECU には共通パスワードを平文で送る弱い認証しかなかったため，制御 ECU のリプログラミングができた．

脆弱性対策と正しい考え方

上記の攻撃の流れをどう防止できるかをここで考える．まず，自動車のセキュリティ対策は，自動車の車両以外でも考える必要がある．ネットワークの通信制限があれば Jeep の攻撃はそもそも成立しなかった．また，セキュリティ対策は，用途に合わせて選ぶ必要がある．前述の Tesla の場合，Wi-Fi の PSK 認証（共通パスワード認証）を採用していたが，MGT 認証（会社向けの認証）を採用していれば Wi-Fi での攻撃は成立しなかった．特に，車を含む IoT 機器は，**全デバイスに共通するパスワード・共通鍵に基づく対策は原則採用しない**方が望ましい．また，車の寿命は 10 年と一般的に言われているが，暗号アルゴリズムにも寿命がある．車がビンテージカーになったときのセキュリティ対策の有効性も考える必要がある．

なお，ここで紹介した攻撃がどれもいろいろなリプログラミング機能を悪用していたとはいえ，リプログラミング機能そのものはセキュリティ対策としても非常に重要である．Jeep の車には遠隔リプログラミング機能（通称 OTA ― Over the Air）がなく，リコールせざるを得ない状態に陥った．一方，Tesla の車には OTA 機能があり，リコールせずに対応ができた．素早い対応が称賛され，顧客からの信頼度も上がった．コネクテッドカーには，**強い認証性を備えた OTA 機能が必要不可欠である**．そして，その **OTA 機能を活用する脆弱性報告対応チームの育成**も重要である．ハッカーの技術は日々進化している．インターネットで車の情報だけでなく，解析用のソフトウェアや，車と通信をするための安価なハードウェアも共有している．自動車業界は秘密主義だから解析されないだろと思うのは禁物である．どんな対策も突破されるかもしれないと思い，**同じ目的の複数の対策を実装するという**考え方が重要である．

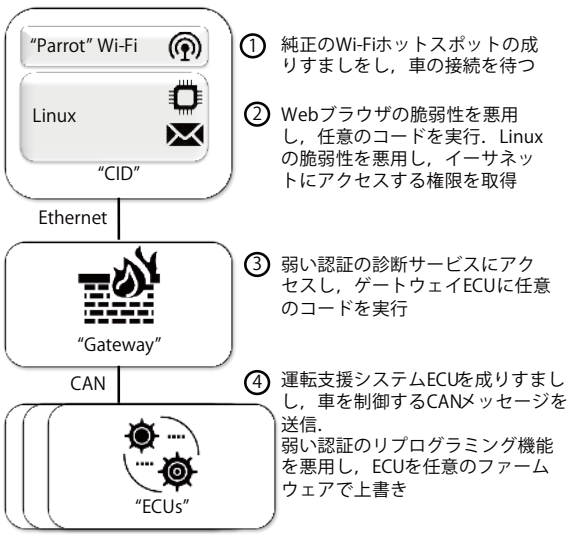

図 -4　2017 年　Tesla Model S 攻撃の概要

参考文献

1) Miller, C. and Valasek, C. : Remote Exploitation of an Unaltered Passenger Vehicle, Black Hat USA (2015).
2) Nie, S., Liu, L. and Du, Y.: Free-Fall : Hacking Tesla from Wireless to CAN Bus, Black Hat USA (2017).

(2020 年 2 月 4 日受付)

Camille Gay　camille.gay@aist.go.jp

産業技術総合研究所サイバーフィジカルセキュリティ研究センター CPSEC 客員研究員．トヨタ自動車（株）コネクティッド先行開発部セキュリティグループ シニア・リサーチャー．