# べからず集

## 車載器編

～失敗しないための事例集～

Ver. 1.0

平成29年5月29日

CCDS セキュリティガイドラインWG
車載 SWG

# 目次構成

| 章 | No | |
|---|---|---|
| 1 | | はじめに |
| 2 | | 失敗しないための事例集 |
| | 01 | パスワードは推測されにくいものになっていますか？ |
| | 02 | パスワードは変更できるようになっていますか？ |
| | 03 | 必要のないTelnetポートは閉じていますか？ |
| | 04 | 外部からアクセス可能なデータについて、情報の種類毎による設定とその設定に合ったアクセス制限が施されていますか？ |
| | 05 | バッファオーバーフローを発生させないようにしていますか？ |
| | 06 | 接続されている機器の実行権限をきちんと確認していますか？ |
| | 07 | 整備ツールや診断ツールが攻撃に使われることを前提に考えられていますか？ |
| | 08 | アフターマーケット機器を接続することで新たな脆弱性が付加される可能性を認識していますか？ |
| | 09 | 電波が弱ければ大丈夫と思っていませんか？ |
| | 10 | 同じ暗号鍵を共通で使用していませんか？ |
| | 11 | キーレスエントリーのIDコードが盗まれないと思っていませんか？ |
| | 12 | Bluetoothでの接続は安全だと過信していませんか？ |
| | 13 | 自動車内部で使う無線通信に暗号化を忘れていませんか？ |
| | 14 | 車載器に認証なしに簡単にアクセスできるようになっていませんか？ |
| | 15 | ジャミングされるという可能性を考えていますか？ |
| | 16 | 運転支援システムに使うセンサ情報は信頼できますか？ |
| | 17 | 車外からの不必要な通信に対してオープンな接続になっていませんか？ |
| | 18 | 遠隔からの攻撃に対する脆弱性が高まっていることを認識していますか？ |
| | 19 | つながれる機器のセキュリティレベルが低い場合があることを認識していますか？ |
| | 20 | 外部から攻撃を受けても、システムの安全性が確保できるようになっていますか？ |
| | | 参考文献 |

# 1. はじめに

昨年リリースした「製品分野別セキュリティガイドライン：車載器編」では、車載器やシステムの開発に関わる企業の開発者を主な対象として、車載器において適切なセキュリティ対策を実施するためのガイドラインを１８項目の指針という形でまとめた。また、脅威事例の評価に必要なリスク評価手法を調査し、国内外の発表文献から集めた脅威事例を使い、実際にリスク評価を行い傾向分析の結果を示した。しかしながら、具体的な対策等を示したガイドラインとはなっておらず、指針をもとに何をしたらよいかがイメージしにくいものであった。そこで、過去に起こった車載器に対する攻撃事例やIT分野の事例から、脆弱性のもととなった失敗事例を参考に、「べからず集：車載器編　～失敗しないための事例集～」としてまとめた。

# 2. 失敗しないための事例集

## ■ 01 パスワードは推測されにくいものになっていますか？

パスワードを知られてしまうと、正当な権限を持たない者に自動車システムの機能を「不正利用」される脅威が高まる。設計の段階で、推測されやすいパスワードや短いパスワードの設定を回避する対策等が必要である。また、初期パスワードのまま使い続けないことや、定期的なパスワードの変更をユーザに推奨する等の配慮も必要である。

【失敗事例】

電気自動車の専用アプリの脆弱性を利用し、インターネット経由で、他人の自動車のエアコンやファンを作動させたり、運転履歴を取得したりした事例。専用アプリのAPIには認証の仕組みが実装されておらず、個々の自動車に割り当てられた車両識別番号の下5ケタさえ分かれば自動車にアクセスし制御することができた。

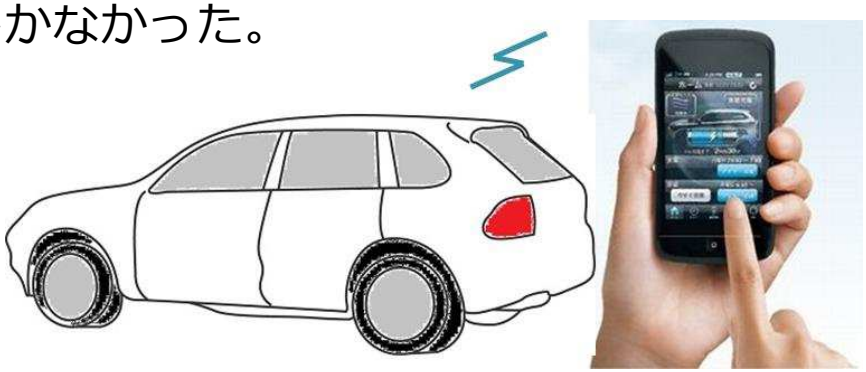
# 2. 失敗しないための事例集

■ 02 パスワードは変更できるようになっていますか？

更新の手間や管理の容易さの面から固定パスワードを利用する場合も多いが、一度パスワードが知られてしまうと、正規ユーザと同じ権限を持つこととなり不正利用をゆるしてしまう。また、パスワードをハードコードすると、それらの情報を攻撃者にさらしてしまう危険性があり、パスワードの漏えいにつながるため注意が必要である。

【失敗事例】

PHEV車に搭載された無線LANアクセスポイントのパスワードが、単純で非常に短いため容易に解読可能であった。このためモバイルアプリで遠隔操作できる機能がハッキングされ、車のライトやエアコンを付けたり盗難警報を解除された。この事例では無線LANアクセスポイントのパスワードが変更できない仕様になっていたため、当面の対策としてモバイルアプリの使用停止をユーザに注意喚起するしかなかった。



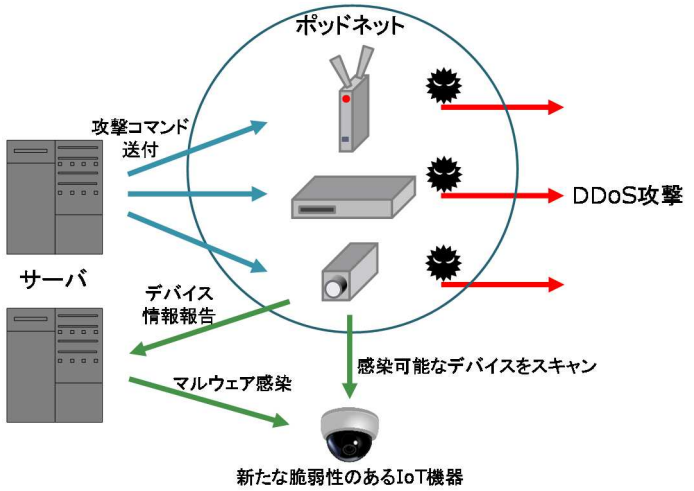
# 2. 失敗しないための事例集

## ■ 03 必要のないTelnetポートは閉じていますか？

IoT機器がマルウェアに感染し、大規模ボットネットに組み込まれ、「DDoS攻撃」（分散型サービス妨害攻撃）の踏み台に使用されるという事例が近年増加している。マルウェアに感染して攻撃の踏み台とならないためには、TelnetポートやSSHポート等、必要のないポートは閉じて、デフォルトのままユーザ名やパスワードを使わない等の注意が必要である。

【失敗事例】

2016年9月に発生した史上空前のDDoS攻撃では、不十分なIoT機器のセキュリティを悪用してマルウェアを感染させ、攻撃の踏み台として利用した。
これらの踏み台にされたIoT機器では、
Telnetポートを開いたままにしており、
「root」とか「admin」等良く使われるパスワードをデフォルトのまま使っていた。このマルウェアは初期設定で良く使用されるユーザ名とパスワードのリストを持っており、
Telnetポートを使用するIPアドレスをランダムにスキャンし、脆弱なIoT機器を見つけ出してはマルウェアを拡散させていた。

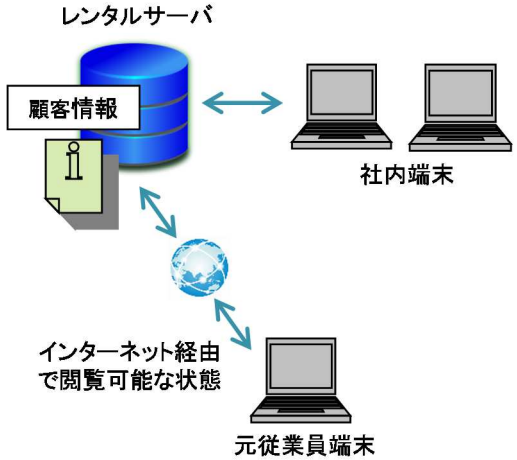


# 2. 失敗しないための事例集

■ 04 外部からアクセス可能なデータについて、情報の種類毎による設定とその設定に合ったアクセス制限が施されていますか？

車載器の場合、一般の顧客がアクセス可能な情報以外に、カーディーラー等の保守員がアクセスするメインテナンス情報や、開発者が扱う設計情報等がある。これらの情報に対しては、情報の種類毎にアクセス制限を設け、適切な関係者のみ閲覧できるようにする必要がある。

【失敗事例】
情報の種類毎にアクセス制限を設けていなかった為、元従業員によって無断で顧客情報18万件及び営業の秘密情報が不正に社外に持ち出され、インターネット上にその情報が公開されてしまった。



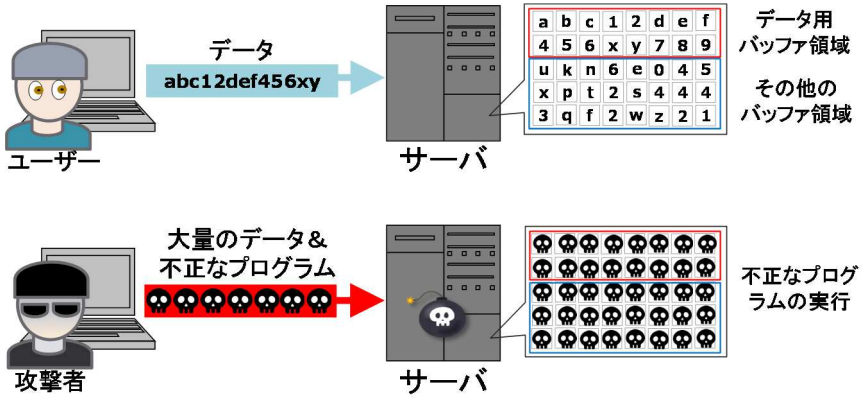
# 2. 失敗しないための事例集

■ 05 バッファオーバーフローを発生させないようにしていますか？

バッファオーバーフローは、大量のデータを入力することで、用意された領域以外のメモリ領域まで上書きされ、プログラムが誤動作を起こす脆弱性のことである。車載器の設計段階において、バッファオーバーフローを避けるには、入力されたデータをバッファに書き込む前に、データサイズがバッファサイズを超えていないことを確認する等の注意が必要である。

【失敗事例】

2000年1月、科学技術庁のホームページが乗っ取られ、Webサイトが書換えられる事件が起こった。この事件ではバッファオーバーフローを用いて悪意のあるプログラムをサーバに侵入させ、管理者権限で実行中のアプリケーションからそのプログラムから呼び出すことで、管理者権限を奪取しWebサイトを改ざんした。



# 2. 失敗しないための事例集

## ■ 06 接続されている機器の実行権限をきちんと確認していますか？

ディーラや保険会社、中古車販売業者等が、自社のサービスに利用するため独自の機器を接続し使用する場合が多い。保守やメインテナンス等で使用する機器との接続も含め、接続されている機器の実行により重大なインシデントに繋がる可能性のある場合は、接続される機器の正当性や実行権限の確認、実行のための多重認証等を設ける等の配慮が必要である。

【失敗事例】

2010年3月、米国テキサス州オースチンで、中古車販売業者が設置した遠隔イモビライザーを悪用し、突然100台以上の自動車のエンジンがかからなくなったり、警告ホーンが鳴り続け止められなくなったりする事件が発生した。この販売店がローン販売した自動車には、返済が滞ったユーザに自動車を利用させなくするために遠隔イモビライザーが装着されていた。この遠隔イモビライザーは、その販売店の従業員が操作用のパソコンを使ってWebサーバにアクセスすれば集中的に停止処理を操作できた。この事件では解雇された従業員が別の従業員のIDとパスワードを入手して不正に操作を行っていた。

# 2. 失敗しないための事例集

■ 07 整備ツールや診断ツールが攻撃に使われることを前提に考えられていますか？

整備業者などから低価格の診断ツールを求める声に応じ、使いやすいアフターマーケットプログラミングツールやサービスツールを低価格で開発・販売する新しい業界が誕生している。これらのツールは正規販売代理店を通さなくてもインターネットで購入することができ、攻撃者が整備ツールや診断ツールを容易に入手することができるようになっている。そこで、これらのツールを用いた攻撃も想定しておく必要がある。

【失敗事例】
2012年4月、電子ロック式自動車の合鍵を作製する「イモビライザーテスター」と呼ばれるツールが悪用され、自動車が盗まれる被害が日本で報じられた。本来、このツールはキーを紛失した場合に使用されるもので、盗難防止装置（イモビライザー）が装着された自動車に、新たに電子キーのデータを登録することができる。
「イモビライザーテスター」の正規品は数十万円で販売されているが、最近では中国製の類似品が数万円で販売されている。盗まれた自動車はいったんドアを開けられ、OBD-IIポートにイモビライザーテスターを接続された後、合鍵が追加されていた。

# 2. 失敗しないための事例集

■ 08 アフターマーケット機器を接続することで新たな脆弱性が付加される可能性を認識していますか？

近年、自動車のOBD-II端子に接続し、燃費管理や安全運転評価を行う機器がいくつも販売されおり、これらの機器の脆弱性を利用して攻撃を行う事例が報告されている。現在はカーナビやドライブレコーダ等、多種多様なアフターマーケット機器を自動車に搭載することができるが、これらの機器を接続することで、新たな脆弱性が付加される可能性を認識する必要がある。

【失敗事例】
アメリカの保険会社が走行距離に応じた自動車保険サービスを展開しており、その保険料算定ツールとして、OBD-II端子に接続する装置を配布していた。この装置は携帯電話網を使って利用者の運転情報を保険会社に送信する機能を持っていた。攻撃者はこの装置の脆弱性を利用し、スマートフォンから特殊なSMSを送ることによりOBD-II経由で車内ネットワークに侵入し、ワイパーやブレーキを操作することに成功した

# 2. 失敗しないための事例集

■ 09 電波が弱ければ大丈夫と思っていませんか？

スマートキーシステムは、ハンドルの鍵穴にキーを差し込むことなく、エンジンを始動できる便利な仕組みであるが、このシステムが「信号増幅攻撃」という手法でハッキングされ自動車が盗難される事例が報告されている。自動車が発信するスマートキー認証用の電波が微弱である為、車体周辺の狭く限られた範囲しか電波は届かないから大丈夫という前提の裏を突いた攻撃手法である。

【失敗事例】

スマートキーシステムでは、自動車からの信号を受信したスマートキーが、自動車へ応答信号を返すことで、正規のキーを持ったドライバーが自動車の周辺にいると認識し、ドアの開錠やエンジンの始動を許可する仕組みである。「信号増幅攻撃」は自動車からの信号を増幅し、遠隔地のスマートキーの傍に信号を中継し、あたかもドライバーが自動車の周辺にいるように偽装してエンジンを始動させるという窃盗手口である

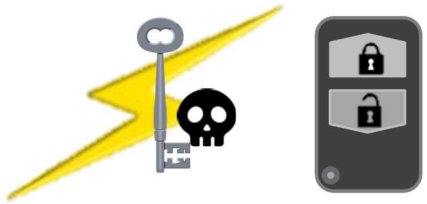
# 2. 失敗しないための事例集

■ 10 同じ暗号鍵を共通で使用していませんか？

欧州の大手自動車メーカーが1995年以降に販売したほぼ全ての自動車で、自動車のドアを開錠するキーレスエントリーシステムの脆弱性が見つかった 。過去20年間に発売された約１億台の自動車で、キーレスエントリーシステムの暗号化通信に、わずか４つの共通鍵を使用していた。共通鍵が判明しただけでは、容易にキーレスエントリーシステムをハッキングできるわけではないが、1億台にも及ぶ自動車が危険に晒される可能性があるとしている。

【失敗事例】

研究者たちは自動車の内部ネットワーク内の部品をリバースエンジニアリングすることで、何百万台の自動車で共有される暗号鍵を抽出できることを発見した。その後、無線ハードウェアを使用しワイヤレスキーが発する信号を一度だけ盗聴することで、元のワイヤレスキーのクローンを作成し、何度でも自動車のドアを施錠・解錠することができた。



# 2. 失敗しないための事例集

## ■ 11 キーレスエントリーのIDコードが盗まれないと思っていませんか？

自動車のキーレスエントリーシステムでは、IDコードの傍受による不正解錠の対策として、ローリングコードによるセキュリティ方式が多くの自動車メーカーで採用されるようになった。ローリングコードによるセキュリティ方式は、送信するIDコードを毎回変化させ、攻撃者に傍受されたとしても、次で使えないという仕組みを用いて安全性を高めている。しかしながら、この安全と考えられていた方式も、安価なツールでコードを盗み解錠できることが発表された。

【失敗事例】

DEF CON23で米国のセキュリティ研究者が自動車のキーレスエントリーを破るツールを発表した。このツールはリモコンキーの電波が自動車に到達するのを妨害すると同時に、１回目の開錠用コードを傍受し記録する。ユーザーが解錠できないため再度リモコンキーを押した際に、1回目の開錠用コードを自動車に送信すると同時に、2回目の開錠用コードを傍受し記録する。この結果、自動車のユーザは正常に開錠できたと思い込まされ、2回目の開錠用コードが盗まれたことに気が付かない。ユーザが自動車を離れた後、攻撃者はツールに記録した2回目の開錠用コードを使って自動車に侵入することができる。自動車のユーザに2回開錠操作を行わせるだけで、ドア開錠用コードを入手することができる攻撃手法である。

# 2. 失敗しないための事例集

## ■ 12 Bluetoothでの接続は安全だと過信していませんか？

Bluetoothは数m～数10m程度の比較的近距離にある機器間の通信に使用されるワイヤレス技術であり、パソコンやPDA、スマートフォン等に搭載され、周辺機器も含め広く普及している。しかしながら、これらの機器で利用されているBluetooth技術に脆弱性が多数存在することが指摘されている。Bluetoothのプライバシと接続認証は一定のセキュリティを保持するが、そのプロトコルについては脆弱性が報告されており、対策としては遅れを取っている。そのような状況であるにも関わらず、医療機器や車載器にも利用されるようになり、これらを利用する場合には、セキュリティを考慮した利用方法を意識しなければ、極めて深刻な事態も起こり得る可能性がある。

【失敗事例】
サイバーセキュリティとハッキングの会議であるGrrCON 2012にて、Chris Roberts氏はオスロ市街地に駐車してあったタクシーの車列で、BluetoothのPINを解読して接続し、特定のCANバスメッセージを送り、タクシーのトランスミッションをニュートラルにすることができるという報告をした

# 2. 失敗しないための事例集

■ 13 自動車内部で使う無線通信に暗号化を忘れていませんか？

TPMS（Tire Pressure Monitoring System）はタイヤの空気圧を監視し、無線通信を利用して車体側の受信機に情報を送り、運転手に異常を知らせるシステムで、2007年から米国でTPMSの装着が義務化されている。TPMSのように自動車内部の非常に狭い範囲で使用する無線通信であっても、傍受や悪用されることを想定し暗号化などセキュリティ面での対応を行う必要がある。

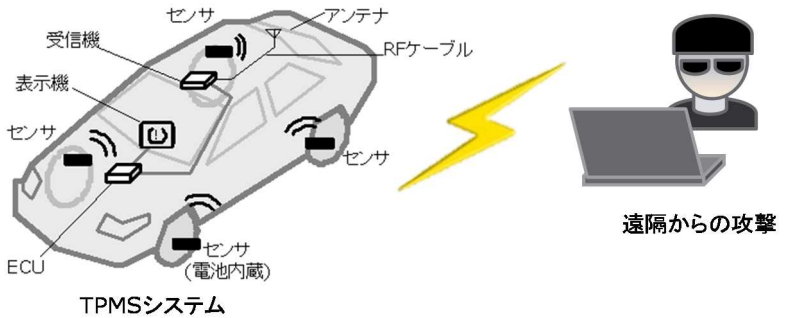
【失敗事例】

TPMSの脆弱性を指摘する論文が2010年に米国で発表された 。

1．TPMSでは通信メッセージは暗号化されていないため、盗聴・解析が容易。

2．タイヤのバルブに装着した空気圧測定装置は32bitの固有のIDを持つとともに自動車本体から40m離れても無線通信が可能なため、路肩や高架橋等で測定すれば、特定の自動車がいつ通過したかを記録することができる。

3．TPMSの空気圧報告メッセージになりすますことができ、いつでも警告灯を点灯させることができる。



TPMSシステム

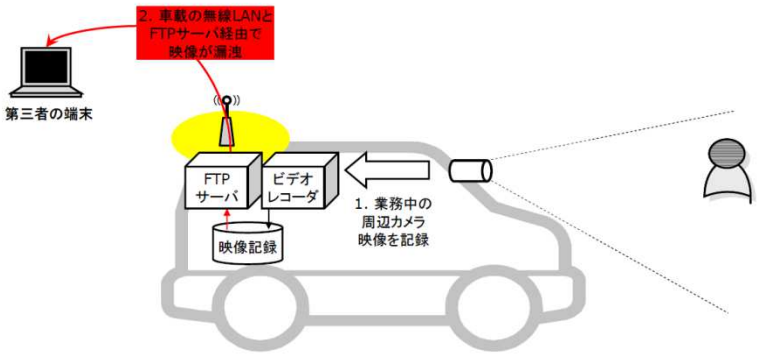
# 2. 失敗しないための事例集

## ■ 14 車載器に認証なしに簡単にアクセスできるようになっていませんか？

自動車にカメラが搭載され様々な用途に利用されている。バックモニター等の安全確認や運転支援用途だけでなく、ドライブレコーダのように車載カメラで撮影された映像や音声等を記録として残す機能を持つものもある。これらの機器に遠隔から簡単にアクセスできると、記録された映像や音声を通じ個人情報の漏洩につながる恐れがある。

【失敗事例】

米国で、ある自治体の警察用パトロールカーのビデオレコーダの映像記録が、車載の無線LAN アクセスポイントとFTP サーバを経由して漏洩する問題があった。車載ビデオレコーダの記録映像が、内蔵しているFTP サーバを通じて認証なしで取り出せるようになっていることが原因だった。記録映像には、停車させられた自動車のナンバーや、取り締まりを受けた市民の顔等が含まれていると考えられ、プライバシ情報の漏えいや、犯罪等への関与を疑われる等の誤解につながる可能性がある。



# 2. 失敗しないための事例集

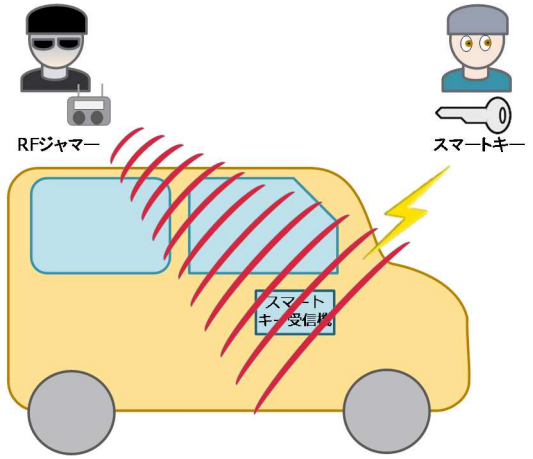
■ 15 ジャミングされるという可能性を考えていますか？

南アフリカでは、ユーザの不注意を利用し、「RFジャマー」を使った自動車の盗難が増加している。「RFジャマー」とは、スマートキーからの信号をジャミングし、自動車の施錠をブロックするもの。スマートキーが使う周波数を、攻撃者がジャミングに使いにくい周波数帯に変えるか、施錠確認をキー自体にフィードバックする等の対策が考えられる。

【失敗事例】

スマートキーを用いてドアロックをする際、ドアロックが成功したことを確かめるには、目視でウィンカーの点滅やドアロック時の音を確認するか、ドアノブを操作して施錠の確認を行う。

「RFジャマー」により自動車の施錠をブロックされているときに、このようにドアロックの確認を怠ると、施錠をしないまま自動車を離れることになる。この結果、攻撃者の自動車への侵入を許し、車内に置いてあったノートパソコンや携帯電話、現金といった貴重品を盗まれることになる。最悪の場合、自動車そのものが盗まれてしまう。



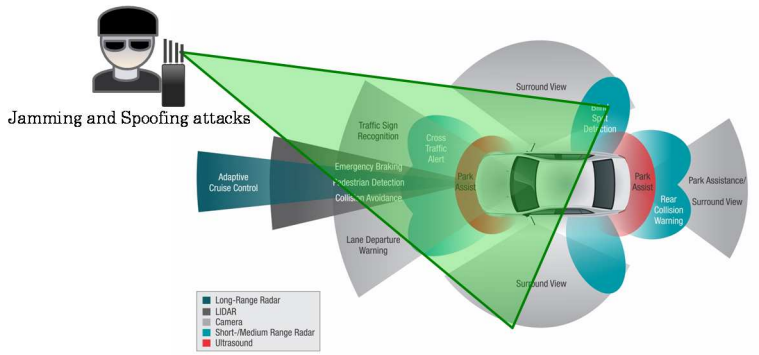
# 2. 失敗しないための事例集

## ■ 16 運転支援システムに使うセンサ情報は信頼できますか？

近年、ドライバーの安全運転や運転操作ミス軽減をサポートするため運転支援システムを搭載した自動車が増えている。これらの技術にはカメラやミリ波レーダ、超音波センサ等が用いられている。今後、より高度な自律運転技術を搭載した自動車へと進化していくなら、これらセンサ情報の信頼性が重要となり、外部からの攻撃に対するセンサのセキュリティリスクを考える必要がある。

【失敗事例】

DEF CON24で中国の研究者が車載センサへの攻撃に関する発表をした。運転支援システムを搭載した車の、ミリ波レーダ、超音波センサ、前方監視カメラの各センサに対し、非接触型の攻撃を行い検証した。
各センサのセキュリティを検証するため、ジャミング攻撃による妨害に対する耐性や、やなりすまし攻撃による機器の誤動作や誤検出を測定した。検証の結果、これらのセンサに対してジャミング攻撃やなりすまし攻撃が行われることで、自動車システムに障害が発生しクラッシュや被害につながる可能性を指摘している。



Major ADAS sensor types and typical vehicle positions

# 2. 失敗しないための事例集

■ 17 車外からの不必要な通信に対してオープンな接続になっていませんか？

ワシントン大学のKohno 准教授らは2011年のKohno 論文で、現代の自動車には広範囲な攻撃経路があり、これらを間接的な物理アクセス、短距離無線アクセス、および長距離無線アクセスの3つのカテゴリに大別し自動車の脅威モデルを作って分析している。この中で、CDプレーヤー、Bluetooth、携帯電話等を介して、遠隔からの攻撃が可能なことを発見した。論文では「自動車の外部とのインターフェイスが、迷惑な通信に対してオープンになっていることに驚いた。その結果、攻撃を受ける経路が大幅に広がった。」と述べている。

【失敗事例】
ワシントン大学Kohno 准教授らは2011年のKohno 論文で遠隔から車載LANに任意のコマンドを注入することに成功している。具体的には、携帯電話網を経由して遠隔から自動車のテレマティクス端末に3Gの音声回線経由でアナログモデム接続し、CAN (Controller Area Network)バスにコマンドを中継するIRCクライアントソフトウェアを実行させた。その後遠隔からIRCチャットの形でIRCクライアントに命令し、任意のCANメッセージをCANバスに注入した。2011年のKohno 論文では実際の試験は行われていないが、CANバスへの制御命令によりほとんどの制御が可能だと指摘している。

# 2. 失敗しないための事例集

■ 18 遠隔からの攻撃に対する脆弱性が高まっていることを認識していますか？

2016年3月、米連邦捜査局(FBI)は米運輸省道路交通安全局と共同で「自動車は遠隔からのサイバー攻撃に対してますます脆弱性が高まっている」という報告を行った。この報告書の中で、自動車の無線通信機能や、USB/Bluetooth/Wi-Fi 経由で自動車に接続される携帯電話やタブレット等のモバイル端末や、ODB-IIの診断ポートを介して車両に接続されるサードパーティー製の端末に、脆弱性が内在する可能性を指摘している。

【失敗事例】
報告書では、研究者が購入した自動車の無線モジュールの複数の脆弱性を特定し、セルラー方式の無線通信機能とユーザがオプションで利用可能なWi-Fiホットスポット通信機能を対象とした攻撃法を開発した悪用例の記載があった。Wi-Fi経由の攻撃は、自動車から約100フィート以内の範囲に限られていたが、セルラー方式による接続であれば、研究者は通信事業者の全国ネットワークのどこからでも、自動車と通信し攻撃を行うことができた。更にこの無線モジュールは自動車のCANバスに接続されており自動車の不正操作に成功した。通信事業者は報告が発表される前に車両通信で用いられる特定ポートへのアクセスを遮断したが、結果的に自動車メーカーは約150万台のリコールを行った。

# 2. 失敗しないための事例集

■ 19 つながれる機器のセキュリティレベルが低い場合があることを認識していますか？

IoT機器は分野毎に必要とされる安心・安全レベルが異なり、機器毎にもセキュリティ対策の実施レベルが異なる。自分たちの開発している車機器に対して十分なレベルのセキュリティ対策を施したとしても、接続される機器に脆弱性があると弱いところから攻撃され、想定したセキュリティレベルを担保できない。機器同士が連携してサービスされるIoTの時代には、システム全体のセキュリティレベルを、一番低いレベルの機器に合わせざる得ないことを考える必要がある。

【失敗事例】
欧州の車メーカーが、特定のアプリを使ってWi-Fi経由で車のデータをダウンロードできるサービスを開始した。このシステムにでは、車のデータにアクセス可能なWi-Fiルータが組み込まれており、初期設定のパスワードは車の車両識別番号 (VIN) だった。このシステムを利用すれば、自動車の走行速度、平均燃費量、次回のオイル交換や保守サービスまでの日数等、スマートフォンから自動車に接続して20種類以上のパラメータを読み取ることができるだけでなく、自動車の所有者をこのシステムから締め出すことさえ可能なことが判明した。

# 2. 失敗しないための事例集

■ 20 外部から攻撃を受けても、システムの安全性が確保できるようになっていますか？

自動車は衝突防止ブレーキ等の運転支援システムの搭載で、電子システムが自動車制御の主要機能を担うような制御の高度化や高性能化が進んでいる。今後、自動運転の実現に向けて更に高度な制御システムや車外との通信機能が搭載されていくとすると、故障や誤操作による機能安全面での対応だけでなく、これらのシステムや機能が外部から攻撃を受けても、システム全体の安全性を確保できるよう、セキュリティ面での対応が必須となる。

【失敗事例】
Black hat USA 2016でのCharlie Miller 氏とChris Valasek 氏の報告によると、自動車に対する遠隔攻撃の最終目標は、自動車のネットワークにCANメッセージを注入することによる物理的な制御だが、強制的に実行できるアクションには多くの制限がある。例えば自動車が特定の速度以下でないと、ブレーキを無効にしたりステアリングを回したりすることができない等である。そこで両氏は、パーキングアシストシステムや車間距離調節機能を利用し、これらの制限の多くを回避することで、自動車の制動、ステアリング、および加速システムを制御するCANメッセージ注入の新しい方法を実証した。