平成２９年度
戦略的イノベーション創造プログラム
自動走行システム／大規模実証実験
セキュリティ評価ガイドラインドラフト
（成果報告書版）

平成 30 年　2 月

PwC コンサルティング合同会社

株式会社サイバーディフェンス研究所

変更履歴

日付	バージョン	変更内容
2017/11/28	1.0	ドラフト初版発行
2018/1/26	2.0	・評価項目「1.1.4 隠れたインターフェースからの調査」を追加 ・評価項目フォーマットの見直し
2018/2/1	2.1	・評価項目内容の見直し
2018/2/19	3.0	・評価項目に外部委託時の判断ポイントを追記 ・評価項目に評価結果の判断ポイントを追記 ・4.2 評価項目の策定方針を追加

目次

1. はじめに

1.1. 本書の目的

自動走行システムの基盤となる高度な地図情報や地図上にマッピングされる自動車、人、インフラ設備等の情報は、主に外部ネットワークから取得することが想定されている。こうして得られた情報は、自動走行システムによる車両制御に活用する目的で、車両の制御系/情報系の機器に送られるが、このような状況は従来の自動車にはなかったサイバーセキュリティ問題を引き起こす要因にもなっている。

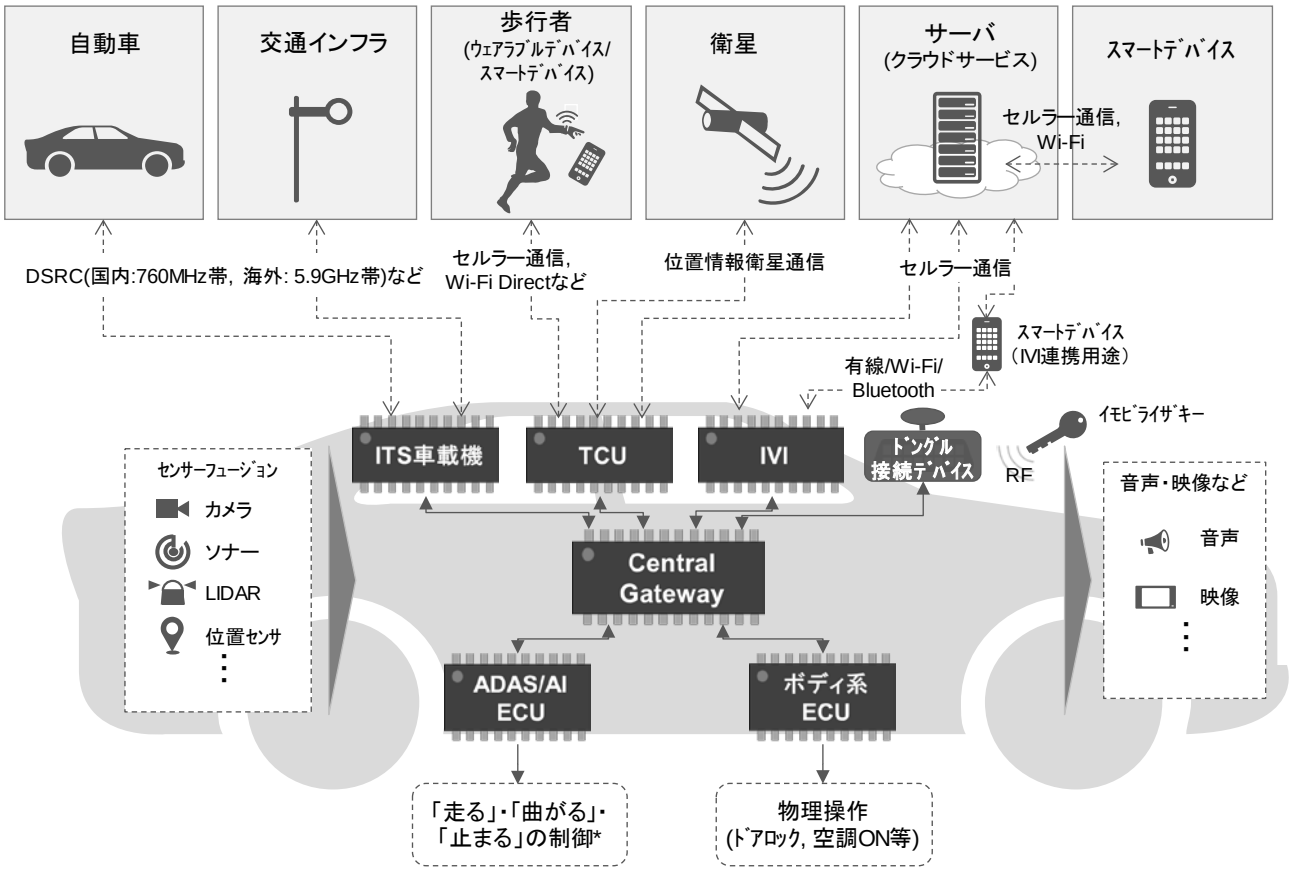
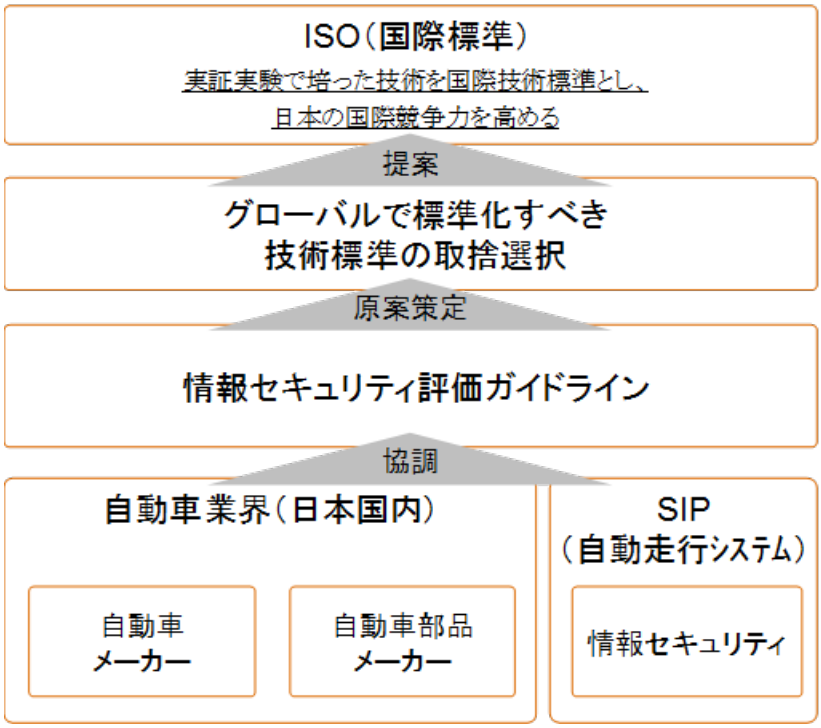


図 1-1　自動走行システムで想定されるシステム図

実際に、2015 年の Black Hat USA における Jeep チェロキーのハッキング報告をはじめ、近年、車両に対するサイバーセキュリティ上の問題について研究者より数多くの報告がなされている。幸い、車両に対するサイバー犯罪や複数の車両に対する攻撃の可能性は現時点で報告されていないもの、自動運転、コネクテッドカーに関する技術開発が急速に進む今、業界として車両のサイバーセキュリティ対策は急務と言える。

一方、100 年に 1 度の自動車産業の変革期と言われ、自動車メーカーのみならず IT 企業も含めた、熾烈な開発競争が進められる現在、日本国内の自動車メーカーが国際競争力を維持し続けるためには、技術開発の協調領域と競争領域を定め、技術分野によっては国内の自動車メーカーが協力し戦略的に開発を進めることも重要である。特に、自動車のサイバーセキュリティの確保は、自動車の安全（セーフティ）にも影響を与えることも考えられるため、最低限満たすべきセキュリティ水準については日本の業界全体の協調領域とすることが適切であり、これにより開発効率の改善を図ることも可能となり、国際的な競争力維持にもつながる。また、定められたセキュリティ対策は、国内の業界における共有にとどめるのではなく、国際標準・標準規格に取り込むことで、不利な技術の普及により競争力を失うことがないよう、戦略的に標準化団体に働きかけることも重要である。



情報セキュリティ評価ガイドラインの国際標準化の狙い

本ガイドはこのような状況にある中で、車両への無線通信を用いた攻撃に対する対ハッキング性能の評価手法を確立することを目的とし、ドラフト版として策定されている。本書に記載される評価手法に沿った評価を実施することで、過去に顕在化した車両インシデント事例と同種の問題に対する予防策がなされていることを明らかにする。また、2019 年度より進められる車両セキュリティ評価方法の標準化においても活用されることを期待している。

1.2. 評価のアプローチ

本ガイドで確立する評価手法は、以下の 3 つのアプローチに沿って策定している。

1. *有効性の確保*
2. *実行性の確保*
3. *メタ評価（開発者評価への還元）*

以下に、各方針の内容と本ガイドでの関連項目について解説する。

- *有効性の確保*

方針	対象車両が実環境で利用・攻撃された場合に発生し得る被害を、明確な証拠と共に明らかにする。
具体的な内容	● 対象車両への攻撃によって発生する実被害を明らかにすることを目的とする。脆弱性の発見のみで、実被害を明らかにしない場合、見つかった脆弱性を修正するか否かの判断が別途必要となり、その後の対策実施を決定する十分な証拠とならないためである。 ● 現実の攻撃環境と同条件で攻撃（評価）を行うものとする。開発組織・開発者のみしか知りえない情報の入手を前提としない。
関連する記載箇所	● 2.1 本書がカバーする既知の車両インシデント 本ガイドで規定する評価の実施で防ぐことができる既知の車両インシデントを記載した。 ● 4.1 評価内容概要評価 ハッカーの攻撃行為と同様の手順にて評価を行うものとした。 具体的には、HW 解析等を行う「偵察」から、実被害を明らかにする「目的の実行」までを手順に記載した。 ● 4.6 評価項目– 4. 目的の実行 現実の攻撃で発生する被害の内容を特定するため、評価内容を脆弱性（候補）の発見にとどめず、攻撃による被害の発生させる、攻撃者にとっての「目的の実行」までを評価項目とした。

- *実行性の確保*

方針	無闇にセキュリティ品質を高めることだけを考慮するのではなく、現実の攻撃者、開発者の実態を踏まえた実行性のある評価とする。
具体的な内容	● 現実の攻撃者の経済原理を考慮した攻撃行為の持続期間や攻撃内容を踏まえて、最低限実施すべき評価内容を明らかにする ● 上記攻撃者想定に加え、実際の評価作業における評価実施者の技術レベル、評価環境・設備の充足度、開発プロセスを合わせて、現実的に実行可能な評価項目とする
関連する記載箇所	● 2.2 想定する評価内容の基準 現実の攻撃者の実態を考慮して、車両セキュリティ耐性の評価として必要な項目として「技術」「設備」「期間」のそれぞれについて基準を設定した。

	● 2.2 想定する評価内容の基準 車両開発プロセスを考慮し、本ガイドを適用し車両評価を行うべき時期を明記している。IT 技術およびセキュリティ技術の進歩は著しい為、一時的な評価実施ではなく、出荷後の定期的評価も推奨している。

● *メタ評価（開発者評価への還元）*

方針	本ガイドで確立する攻撃者視点の評価によって、別途定められる開発者視点のセキュリティ機能評価の手法・ガイドで追加・改善すべき点を明らかにすることを可能とする
具体的な内容	● 攻撃者視点のセキュリティ評価により問題を発見することで、前段の評価である開発者視点評価において不足していた評価観点・項目を明らかにする。 ● 上記の結果、開発時のセキュリティ対策を見直すことができ、対象車両のセキュリティ品質向上につながる。
関連する記載箇所	公開用資料のため、記載内容を削除

1.3. 用語定義

本書で使用する用語とその定義を以下に示す。

No.	用語	用語の定義	用語の定義の目的・理由	定義のベース（引用元を明記）
1	脆弱性	一つ以上の脅威によって付け込まれる可能性のある資産又は管理策の弱点。		vulnerability: weakness of an asset or control （2.16） that can be exploited by one or more threats （2.83）（引用：ISO27000） ・一つ以上の脅威によって付け込まれる可能性のある資産又は管理策の弱点（引用：JIS Q 27000:2014 ぜい弱性）
2	既知の脆弱性	一般公開、もしくは開発者の知りえる脆弱性		
3	公知の脆弱性	一般公開されている脆弱性	既知では一般公開情報と開発者が持つローカルな情報と混在するため、”公知”を定義し、一般公開情報のみの範囲に限定した。	

2. 評価方針および評価条件

2.1. 本書の評価項目がカバーする範囲

本ガイドでは、実際の攻撃者（ハッカー）による攻撃行為に対するセキュリティ耐性の評価を目的としている。つまり、本ガイドで記載する評価手法を実施し、安全性を確認することで、過去に発生したものと同種の車両セキュリティインシデントが発生しないことを確認するものである。

本ガイドが対象とした車両のセキュリティ攻撃事例は以下のとおりに定めた。なお、実際の車両攻撃では、車両から情報を盗み取るためのハードウェア解析やファームウェアの抜き取り、リバースエンジニアリング等の技術を使った攻撃が行われており、本ガイドの評価項目にも反映している。

インシデント事例	インシデント概要
Jeep Cherokee の uConnect 脆弱性	第３者により車両位置の特定やリモートで車両を操作される脆弱性。CellularNetwork 上の開放ポートから車載器に侵入し、CAN コントローラのファームウェア改ざんすることで車両をリモート操作することが可能
BMW の ConnectedDrive 脆弱性	第３者により車両をリモート操作される可能性のある脆弱性。研究者の用意したテレマティクスサーバーから車両に対しドア解錠のコマンドを送ることでドアを解錠することが可能
Tesla ModelS の無線 LAN 脆弱性	第３者により車両をリモート操作される脆弱性。研究者は偽 WiFi スポットを利用して攻撃サイトに誘導する方法を提示したが、Cellular Network を介した攻撃も可能である。その場合、おとりメール等を用いて、ユーザーを攻撃サイトに誘導する。
三菱アウトランダーのモバイルアプリ脆弱性	第３者により空調設定等の環境設置をリモート操作される脆弱性。車内に設置された WiFi スポットにアクセスすることで防犯装置の設定や空調操作をリモート操作することが可能
日産 Nissan Connect EV の脆弱性	一般ユーザーが利用しない開発設定が残存しており、これを利用することでユーザーID,パスワード等の機密情報が外部に漏えいさせることが可能
日産リーフの脆弱性	認証方式に不備があり、スマートフォン⇔サーバーAPI に認証の仕組みが実装されておらず、VIN 下 5 桁が判明すれば他の車両を制御することが可能 ※スマートフォンアプリの脆弱性であるが、車両⇔サーバー、あるいは車両⇔スマートフォンで同様の事象が発生しないか確認する
スバル StarLink の脆弱性	スマートフォンのデバイス認証に使用されるセキュリティトークンには有効期限がなく、窃取された場合、第３者によりドアを解錠させることが可能 ※スマートフォンアプリの脆弱性であるが、車

	両⇔サーバー、あるいは車両⇔スマートフォンで同様の事象が発生しないか確認する
Continental AG の TCU の脆弱性	第３者により TCU がリモート操作される可能性のある脆弱性
マツダの Mazda Connect の脆弱性	車内の USB ポートから任意のコードを実行される脆弱性。AVN のカスタマイズに利用された ※ローカル攻撃であるが、リバースエンジニアリング耐性を図る評価ポイントとして採用
本田技研工業の Honda Connect の脆弱性	車内の USB ポートから任意のコードが実行される脆弱性。AVN のカスタマイズに利用された ※ローカル攻撃であるが、リバースエンジニアリング耐性を図る評価ポイントとして採用

表 2.1-1 本ガイドが対象とした既知の車両インシデント一覧

また具体的なインシデント事例に加え、「戦略的イノベーション創造プログラム　自動走行システム／大規模実証実験」―「脅威分析調査」で明らかにした自動走行システムに係る脅威のうち、早急な対策が求められる重大脅威を踏まえ、車両セキュリティ評価に必要な項目は、本ガイドに反映した。以下、当該脅威分析調査の重大脅威を自動走行システムので想定されるシステム図に図示したものを記載する。

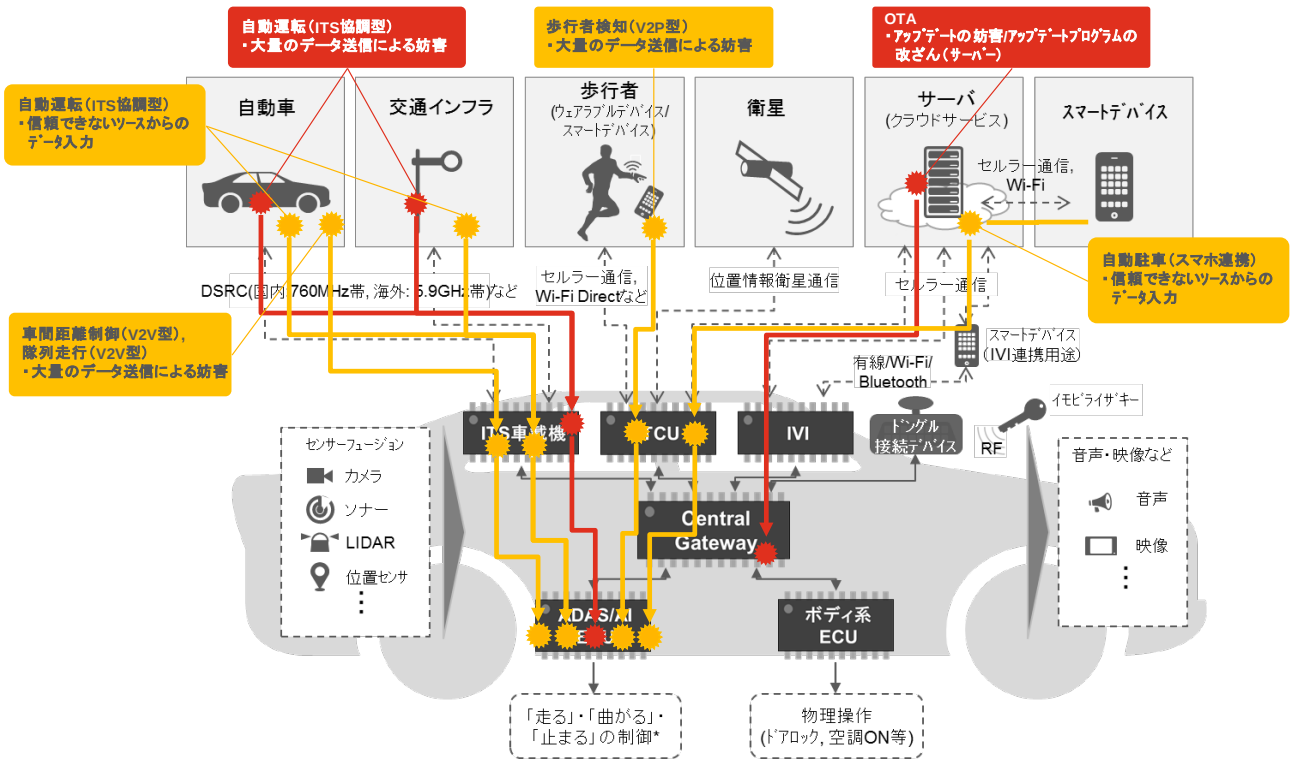


図 2-1-1 脅威分析調査 – 自動走行システム重大脅威（抜粋）

また、具体的な車両インシデントと評価項目の対応は「Appendix 1. 本ガイドと想定脆弱性との関連」を参照のこと。また、車両インシデント以外で項目に盛り込んだものについては、「4.2 評価項目の策定方針」を参照のこと。

2.2. 想定する評価内容の基準

本ガイドで規定する評価内容は、「1.2 評価のアプローチ」－「実行性の確保」に記載のとおり、現実の攻撃者・開発者の実態を考慮し、現実のサイバー攻撃から車両を保護するためにもっとも最適な評価となることを目指している。

具体的には、現実の悪意ある攻撃者と同等な技術・設備・期間を評価項目の基準としており、これらの評価手法を実施することで、「2.1 本書がカバーする既知の車両インシデント」に記載した事例と同種の問題の発生を防止することができる。他方、セキュリティ研究者や専門の研究施設を必要とする評価は対象外としている。このように対象外とする評価項目があることでインシデント発生を懸念することが想定されるが、セキュリティ研究者が車両 OEM 各社との事前調整なしに問題を公知とすることはなく、セキュリティ研究者による報告時に適切な対応をとることで十分対応が可能であると判断した。前提して、車両 OEM 各社はセキュリティインシデントに適切に対応する PSIRT 組織があり運営がなされていることを想定している。

この目的のもと評価項目を設定するにあたり、「評価技術」「評価設備」「評価期間」の項目について以下のように基準を定めた。

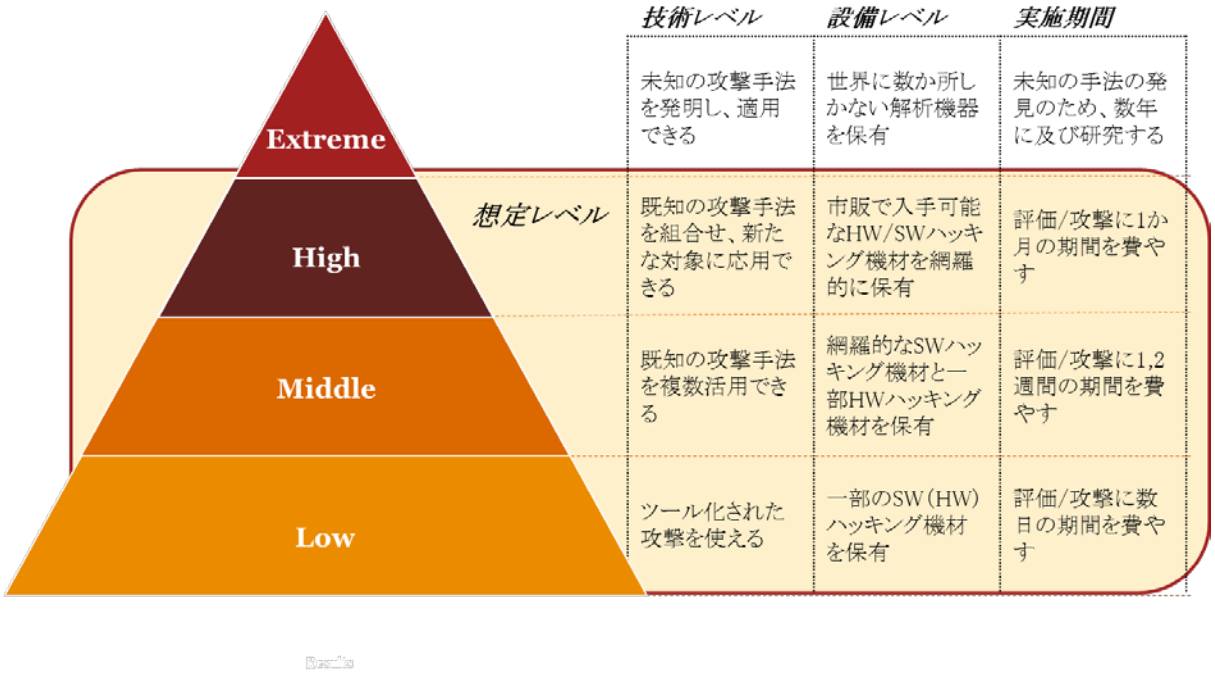


図 2-2　想定する評価内容

以下、定めた基準の詳細と判断の背景を示す。

- 評価技術

・　基準策定の背景

以下に示す通り、車両ハッキングの実際の事例では、車両の購入から始まり、ハードウェア解析、ソフトウェア解析を経たうえで、攻撃コードの作成・実行に至る。報告されたハッキング手法を再現するためには、以下に記載されたハードウェア解析とソフトウェア解析の内容が実施できる技術レベルを有する必要がある。

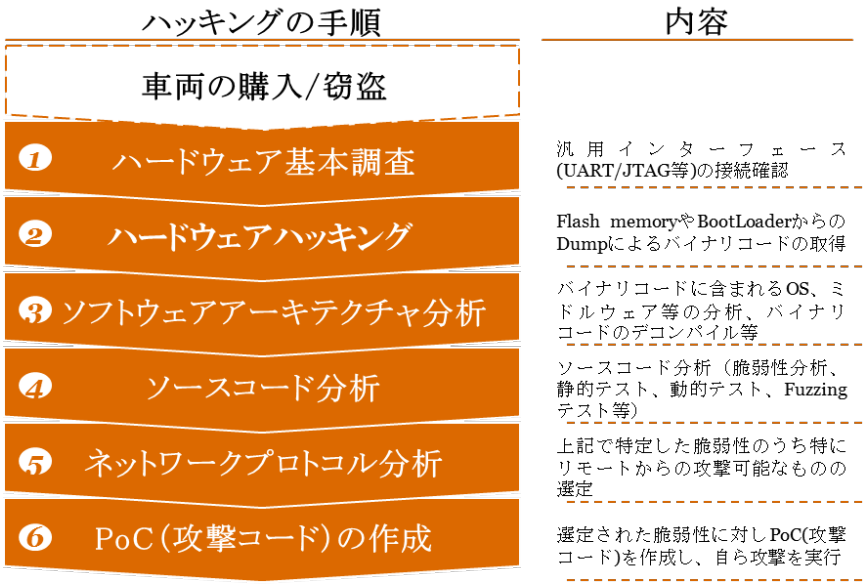


図 2-3 実際のハッキング手順

・　評価の基準

本ガイドでは、「図 2.2-2 実際のハッキング手順」のハッキング手順を追試できる技術力を基準とする。つまり、ハードウェア調査技術から、バイナリコードの解析、攻撃コードの作成ができる技術力を基準とする。これを踏まえた具体的な評価内容は「4.5 評価項目」を参照のこと。

・　評価範囲外

本ガイドでは、実際の攻撃者が有する技術を超えた研究者レベルの技術を使った評価は想定しないものとし、評価対象外とした。

● 評価設備

・　基準策定の背景

実際の車両攻撃者は、内部不正の場合の除き、開発機関や研究機関にある機材を車両攻撃に利用することはできない。また、車両価格を超える機材が攻撃に必要な場合、攻撃行為の経済性が成立せず、多くの場合、より安価な攻撃手法で攻略可能な車両に対する攻撃に移行するためである。

・　評価の基準

本ガイドでは、研究機関にのみ配備されている機材や車両価格を超えるような高額な機材は想定しない。

以下に、本ガイドで必要な評価機材（HW、SW）を示す。これら機材は一般の開発組織（および一般個人）で入手可能なものである。

機材名称	内容	利用する評価項目
Digital Microscope	プリント基板、ICチップの構成を確認するために使用する	1.1.2、1.1.3、1.1.5 1.1.6
Logical Analyzer	デジタル通信信号のモニタリング及びプロトコルのデコードを行うために使用する	1.1.7、1.2.6
HAKKO Soldering Iron station	プリント基板からICチップを剥がすために使用する	1.1.3
Hot-Air Gun	プリント基板からICチップを剥がすために使用する	1.1.3、1.1.5
Bus Pirate	HWインターフェース間で送受信されるデータの内容を確認するために使用する	1.1.3、1.1.6
Jtagulator	プリント基板のJTAGポート、UARTポートのピンレイアウトを診断するために使用する	1.1.2
RIFF BOX 2	JTAGポートからのファームウェアダンプおよびデバッグを実施するために使用する	1.1.6
BeeProg2C	フラッシュメモリからのバイナリファイルの抽出に使用する	1.1.5、1.1.6
Arduino UNO CANBUS Sheild	CANプロトコルの解析を実施するために使用する	1.2.8
Ubertooth One	Bluetoothのパケットをキャプチャするために使用する	1.2.5、2.3.1、2.3.2
USRP N210	SMS解析時にFakeBTSソフトウェアを利用したModem Hackを実施するために使用する（3G/LTE）	1.2.6、2.3.3、2.4.2
Alfa Network AWUS036H	WiFiパケットをキャプチャするために使用する	1.2.2、1.2.3
IDA Pro（x86、ARM32、ARM64）	ファームウェアのリバースエンジニアリングを実施するために使用する	1.1.8
Burp Suite	Webアプリケーションの脆弱性テスト用ツール（本資料ではプロキシサーバーとして使用）	1.2.1、1.2.2、1.2.9 2.2.1、2.2.2
Nessus Vulnerability Scanner	脆弱性診断スキャナ	1.1.5
Metasploit	ペイロード、攻撃コードの作成、あるいは攻撃用Webサイトの作成時に使用する	2.1.1、2.1.2
FTK Imager	バイナリファイルからファイルを取得する際に使用する	1.1.8
enCase	バイナリファイルから機密情報を取得する際に使用する	4.1.1

表 2.2-1 本ガイドで利用する主な機材一覧

- 評価期間
  - 基準策定の背景

評価設備で記載のとおり、現実の攻撃者は経済原理に従った攻撃を行う。攻撃期間に関しても同様で、特定車両に対して数か月におよぶ攻撃を試行することはせず、攻撃成功を目指してより脆弱な車両を探しだし、攻撃対象を移行する。ただし、セキュリティ攻撃技術の進歩は著しく、新しい

攻撃技術の発明や攻撃ツールの開発・公開により、同じ脆弱性を発見/被害を発生させる場合でも、必要期間は変化（減少）することが考えられる。

・　評価の基準

本ガイドによる１回あたりの評価期間は最大１か月を基準とする。加えて、開発時情報を活用することで、評価項目を絞る・並行実施するなどのテーラリングにより、評価期間を短縮することも想定する。

また、評価実施時期は１度限りとせず、車両出荷後も評価を定期実施することを推奨する。攻撃手法の進歩による新種の攻撃手法に対応するためである。

以下に評価実施時期と目的をまとめた。

評価実施時期	評価目的	評価の特徴
出荷前評価	対象車両が市場に出回る前に既知の車両インシデントと同種のセキュリティ問題が発生しないことを確認する	● 機密度の高い出荷前の車両を評価する必要から、開発者ないし開発者から委託を受けた組織により評価される ● 評価対象が出荷前の完成車両であるため評価にかけられる期間が短くなるケースが多い ● 上記 2 点より、評価項目単位で複数人により並行実施することを想定する。並行作業の実施に必要な場合に限り、開発時の情報を活用する場合がある
出荷後の定期評価	攻撃手法の進化や対象車両の機能アップデートにより、新たに対応が必要となった脆弱性および攻撃によるセキュリティ被害の発生を未然に防ぐ。	● 出荷後の検査となるため、車両そのもの機密性は考慮する必要がない ● 出荷という明確な期限がなくなるため、評価にかけられる期間や評価タイミングに制約が無くなる ● 将来的に評価手法や環境が整備された際には、車両車検時など、ディーラーや整備業者によって評価を実施しても良い。ただし、ユーザーの実車両を評価する際には対象車両を毀損しないよう評価項目・内容を厳に絞る必要がある。

表 2.2-2　評価実施時期

・　評価範囲外

車両セキュリティ研究が目的である場合、車両の評価（攻撃）に数年規模の期間をかける場合がある。このようなセキュリティ研究者による評価（攻撃）は、実被害の発生ではなくセキュリティ攻撃の発明や品質の確認が目的であるため、評価範囲外とした。

最後に、本項で定めた評価内容の基準と評価項目の対応は下記の図 2.2-3 の通り。図 2.2-3 では、本ガイドで評価対象外とした評価項目についても明記した。なお、評価項目の詳細内容は 「4.6 評価項目」を参照のこと。

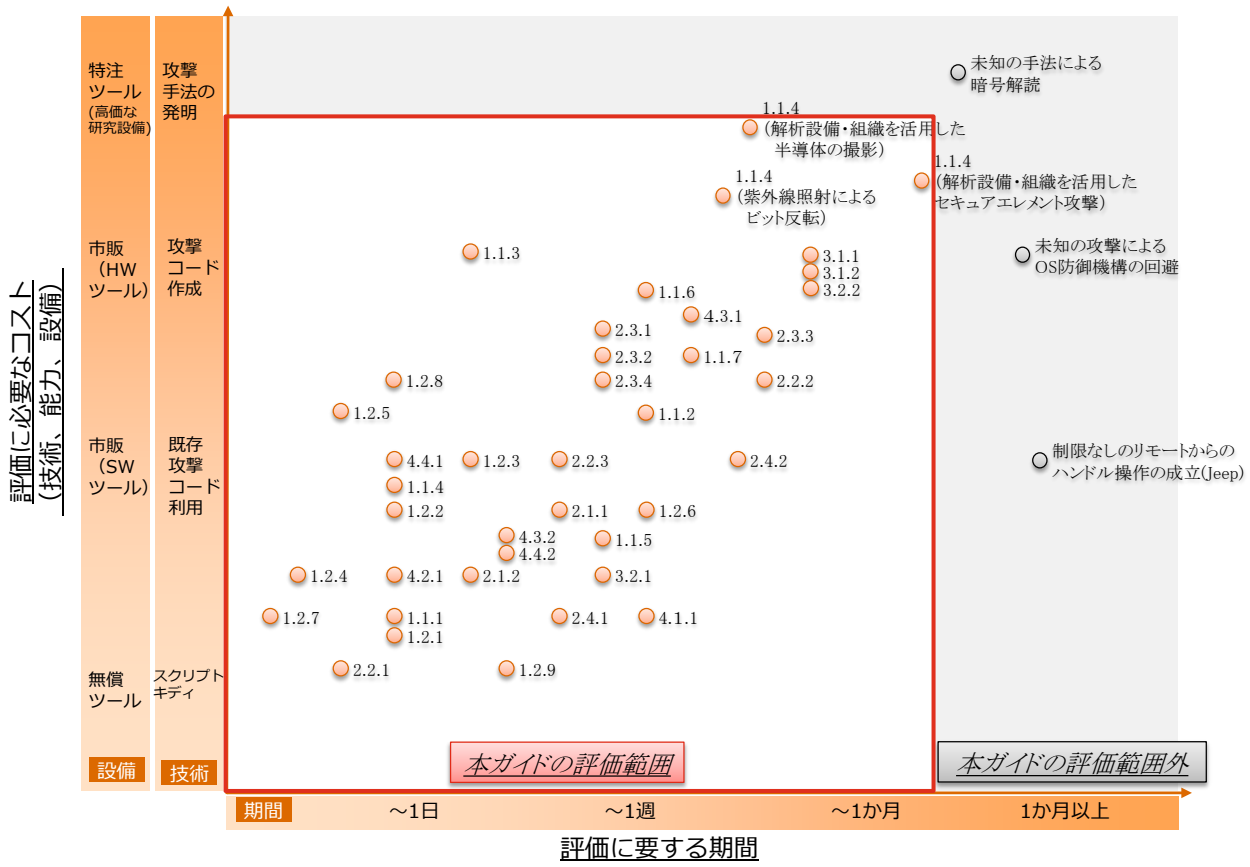


図 2-4 評価基準と評価項目の関連

評価項目	評価項目	評価項目
1.1.1 デバイス取り出し前I/F調査	2.1.1 DrivebyDownload攻撃	3.1.1 コード実行防止機能の回避
1.1.2 デバイス取り出し後I/F調査	2.1.2 ファイル添付攻撃	3.1.2 サンドボックス機構の回避
1.1.3 チップ取り外し後I/F調査	2.2.1 外部WiFiへの自動接続を利用した攻撃	3.2.1 既知の攻撃を試行することによる権限昇格
1.1.4隠れたインターフェースからの調査	2.2.2 偽サーバー誘導による攻撃	3.2.2 強制アクセス制御（MAC）の機構の回避
1.1.5 インターフェース接続	2.2.3 残存開発環境を用いた攻撃	4.1.1 機密情報の漏えい（外部送信）
1.1.6 バイナリ抽出	2.3.1 Bluetooth経由の攻撃	4.2.1 車両のサービス（機能）の停止
1.1.6 バイナリ保護機能確認	2.3.2 BluetoothLE経由の攻撃	4.3.1 制御系ファームウェアの改ざん
1.1.7 リバースエンジニアリング	2.3.3.TCU経由の攻撃	4.3.2 制御系機能の悪用
1.2.1 アプリケーションの通信経路の調査	2.3.4 WiFi(車両内部)経由の攻撃	4.4.1 情報系アプリケーションの改ざん
1.2.2 WiFi(車両外部)の通信傍受	2.4.1 成りすまし攻撃	4.4.2 情報系機能の悪用
1.2.3 WiFi(車両内部)の通信傍受	2.4.2 リプレイ攻撃	
1.2.4 Bluetoothの通信傍受		
1.2.5 BluetoothLEの通信傍受		
1.2.6 TCUの通信傍受		
1.2.7 ブラウザ、HTMLエンジンの調査		
1.2.8 CANメッセージ通信傍受		
1.2.9 アプリケーションの通信傍受		

表 2.2-3 評価項目一覧（名称のみ）

また、「2.1 本書がカバーする既知の車両インシデント」と評価基準・項目との関連について、Jeep Cherokee の uConnect 脆弱性を例として以下に図示する。その他の脆弱性と評価項目との関連は、「Appendix 1. 本ガイドと想定脆弱性との関連」を参照のこと。

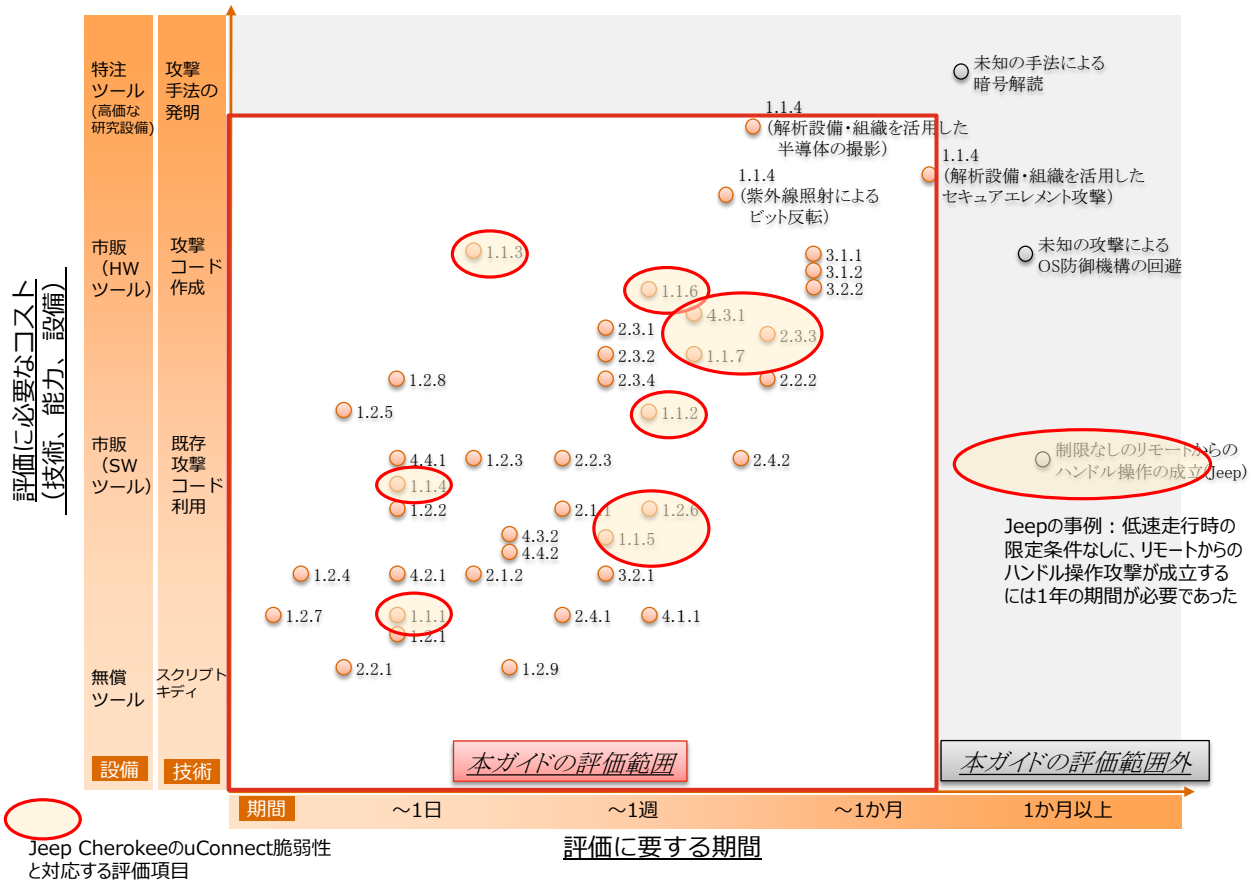


図 2-5 評価項目と Jeep インシデント事例の関係

2.3. 評価実施者

本書が定めるセキュリティ評価は、車両品質に責務を持ちシステムテストを担当する車両 OEM による実施を想定している。

具体的な評価作業においては、車両開発とくにソフトウェア開発における評価作業の経験およびスキルを有することが必要となる。ただし一部の評価項目については、特殊なツールの理解および利用、もしくは、評価結果を正しく判断するために、セキュリティ業務の経験や知見が必要となるものがある。このため、作業効率化のため外部のセキュリティ知見を持つ団体・業者に依頼してもよい。

車両 OEM 自身が評価を実施するか、外部委託するかを判断するため、各評価項目では「外部委託判断」の項目を記載している。各 OEM が保有する人材（技術者）や評価設備と、各評価項目で必要とされるを比較し、見比べ、外部委託実施の判断をすること。

3. 情報セキュリティ　車両評価の位置付け

3.1. 評価の対象範囲

以下に、自動走行車両システムのセキュリティ評価に求められる全ての評価対象範囲を記載する。

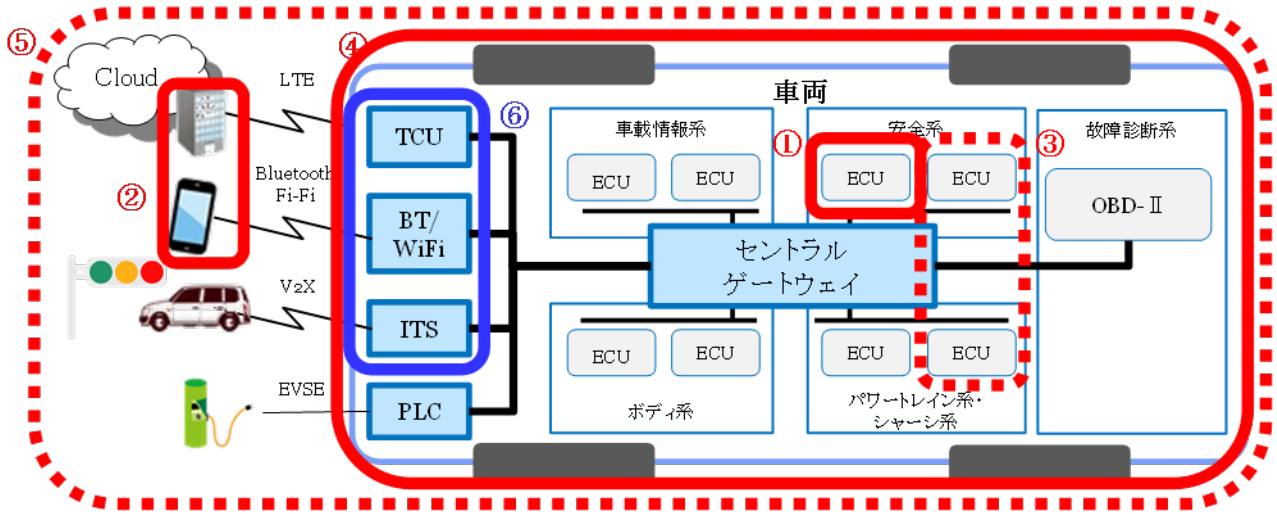


図 3-1 車両システムのセキュリティ評価範囲の全体像

	対象区分	概要
①	単体 ECU/車載機器	単体 ECU/車載機器に対する評価
②	外部エンティティ	車両と接続する専用の Web サーバー及びスマホアプリ等の車両外部のエンティティに対する評価
③	システム機能	自動運転機能等の複数 ECU により実現されるシステム機能に対する評価
④	車両	車両全体に対する評価
⑤	全体システム	外部エンティティや車両に関連する各種リソース（マニュアル、診断ツール等）まで含めた全体システムに対する評価
⑥	外部 IF をもつ車載機器	外部エンティティと IF を持つ車載機器に対する評価

表 3.1-1 車両システムセキュリティ評価の対象区分

上記対象区分のうち、本ガイドでは「⑥外部 IF をもつ車載機器」をアタックサーフェースとし、セントラルゲートウェイまでの範囲を評価対象とする。

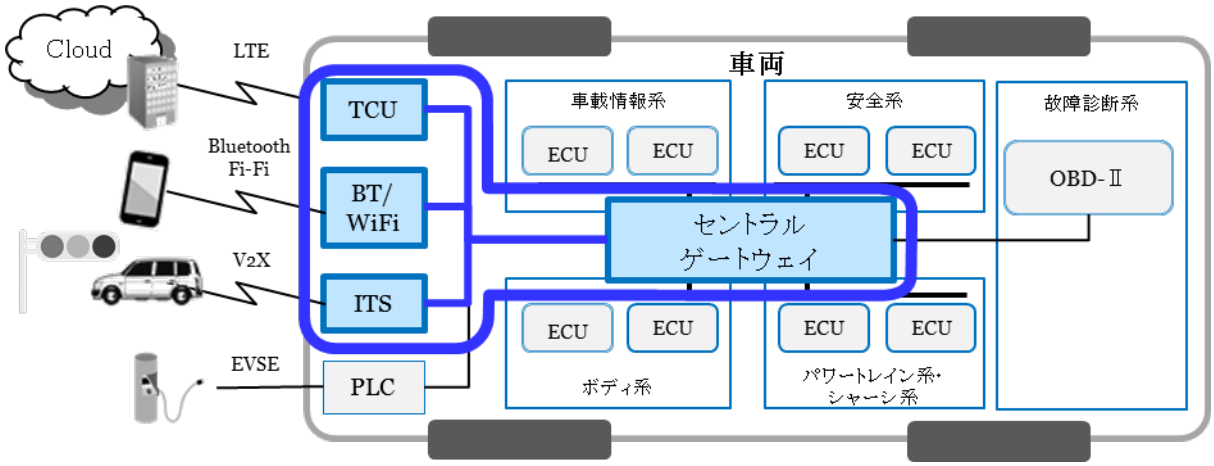


図 3-2 本ガイドの評価対象範囲

3.2. 車両システムの情報セキュリティ評価手法の分類

車両システムのセキュリティ評価において活用される評価手法は以下とおりである。本ガイドではこれら手法のうち、侵入テストによる評価を実施する。

評価種別	種別の説明	評価手法	目的	前提条件	評価結果
ホワイトボックステスト	対象の内部構造(仕様・設計等)を確認、評価する	設計評価	対象が満たすべき*セキュリティ要求を定義*し、要件達成のクライテリアを定義する(サプライヤーへの要求事項)	• 製品企画内容と完成度評価の理解 • システムレベル相当のアーキテクチャ理解	• 機能セキュリティ要求 • 機能セキュリティコンセプト • 技術セキュリティ要求 • 技術セキュリティコンセプト
		機能評価	実装された*セキュリティ機能が対応するセキュリティ要求を満す*ことを確認する	• HW/SWレベルの設計・実装理解 • 設計書等の中間成果物入手	• セキュリティ要件の達成状況の一覧
ブラックボックステスト	対象自体やその動作から問題の有無や原因を解析する	脆弱性テスト	対象に含まれる*脆弱性を網羅的に発見*する。発見した脆弱性毎に対応案を検討する	• 評価対象の入手(部品or車両) • 対象の操作方法の理解(特にECU単位を対象とする場合) • ITセキュリティの知見	• 発見された脆弱性一覧 • 脆弱性毎の想定被害 • 被害への対応案
		侵入テスト	対象への攻撃を試み、*セキュリティ機能の有効性(セキュリティ要件の妥当性)*を測る。より影響度が大きく、より攻略が容易な脆弱性の解析にフォーカス	• 評価対象の入手(車両のみ必須) • 最新のサイバー攻撃手法への知見	• 車両のサイバー攻撃に対する耐性 • 被害内容(深刻度、難易度) • 試行した攻撃内容および手順

表 3.2-1 車両システム評価の評価手法

3.3. 車両評価の位置づけと役割

本ガイドにて確立する評価手法に関して、V 字プロセスにおける位置づけと役割を示す

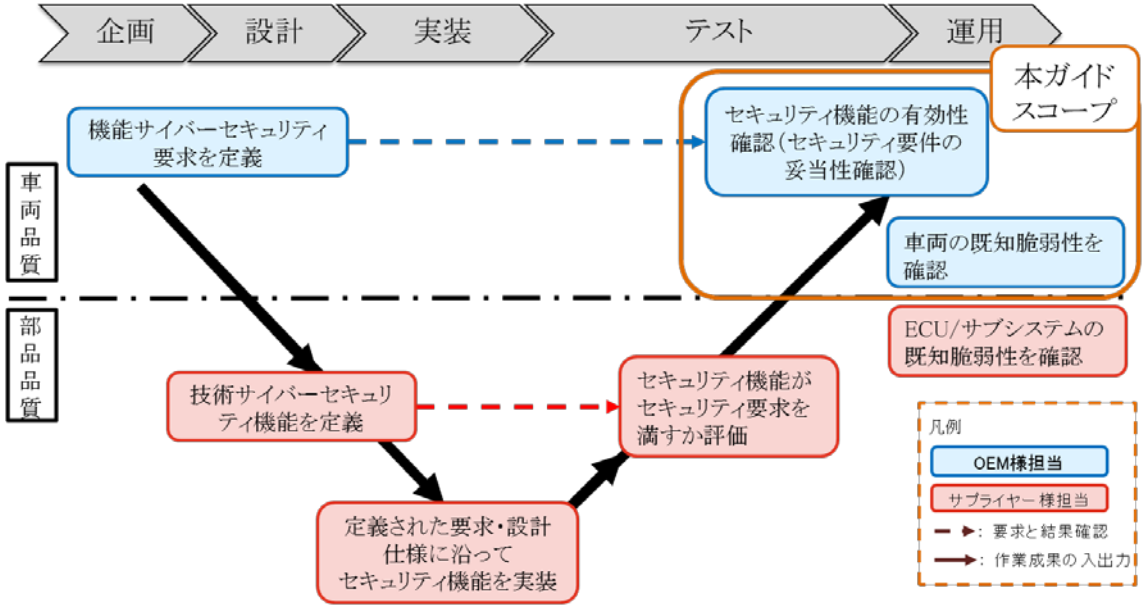


図 3-3 開発 V 字モデルと評価の位置づけ

4. 情報セキュリティ車両評価

4.1. 評価内容概要

本ガイドでの評価手順と評価項目毎の評価内容の概略を示す。

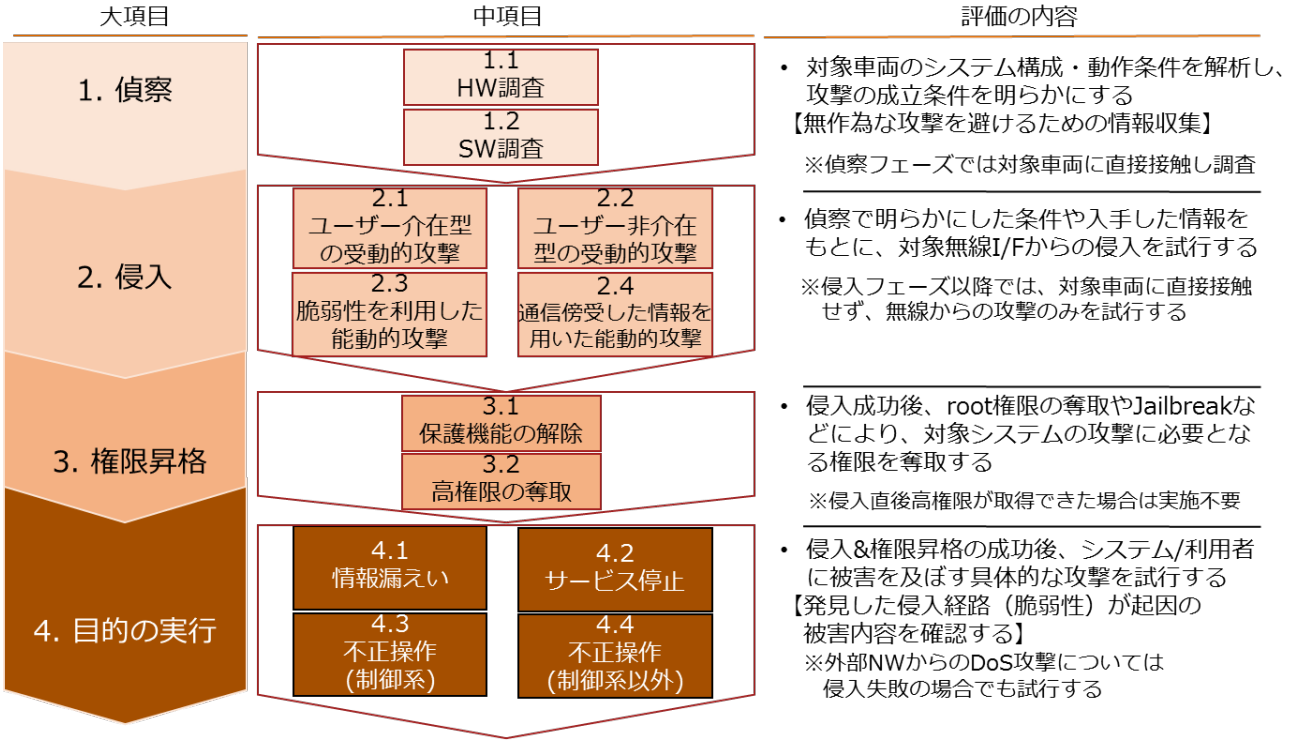


図 4-1　評価手順

4.2. 評価項目の策定方針

各評価における評価項目の策定方針を以下に記載する

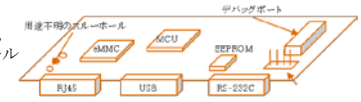
- 1.偵察　－ 1.1 HW 調査

【評価方針】

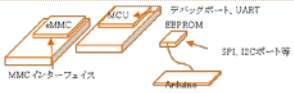
- 搭載HW（車両,デバイス,チップ）が*データ入出力に使うすべてのI/F*からのデータ抽出を試行し、成功した段階でバイナリファイルをリバースし、システムを解析する

【1.1.1 対象I/F】
RJ45, USB, RS-232C等

【1.1.2 対象I/F】
デバッグポート(JTAG等),
UART, 不明なスルーホール

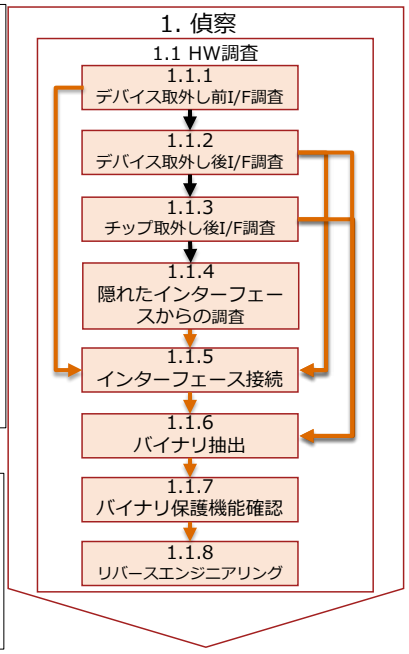


【1.1.3 対象I/F】
デバッグポート,UART（ピン),
MMC I/F, SPI, I2Cポート等



【インシデント以外で取り込んだ評価項目】

- バイナリ抽出にあたり、データ入出力I/F以外からデータ抽出を行う手法を項目化した
  ex.レーザー照射を用いたレジスタビット反転による抽出
  顕微鏡を用いた半導体回路の撮影による抽出
  セキュアエレメントからのデータ抽出、解析

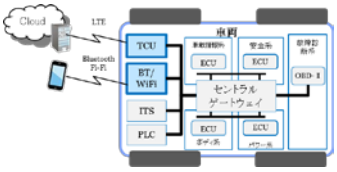


➢ 1.偵察 － 1.2 SW 調査

【評価方針】

- 車両システムが持つ下記の無線通信（当該機能を有するコンポーネント）を対象として通信傍受を試行し、侵入・なりすましに必要な情報を入手する

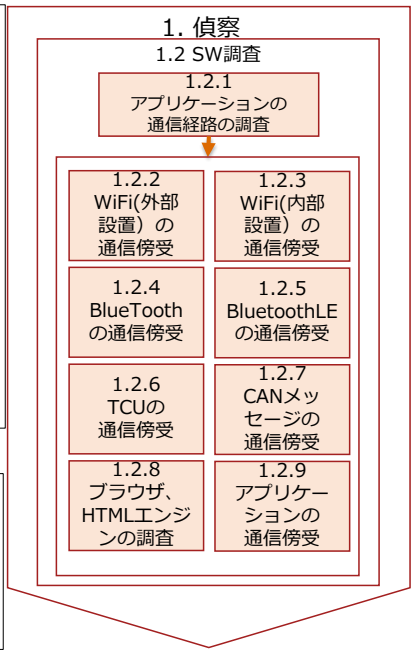
【対象通信】
- TCU(3G/4G)
- WiFi
- Bluetooth



- 上記無線I/Fを利用するすべてのアプリケーションに対して、送受信データの傍受を試行し、侵入・なりすましに必要な情報を入手する

【インシデント以外で取り込んだ評価項目】

- Bluetooth関連について、Bosch社のBluetoothドングル等の車両部品システムにインシデント事例があり、それら内容を項目化した



➢ 2.侵入

【評価方針】

- 無線I/Fを経由した攻撃を試行し、システムのコンソールが利用できる段階までの攻撃（侵入）を行う
- 攻撃方法に影響を与える「車両NWアクセス条件」、「搭乗者関与」を軸に攻撃パターンを分類

搭乗者関与 / NWアクセス	搭乗者の介在を必要とする攻撃（人を罠に嵌める）	搭乗者が不要な自動化された攻撃（機械を罠に嵌める）
外部NWから車両への直接接続しない（外部からのレスポンスのみ）	攻撃プログラムの実行開始を人の操作に頼る攻撃 評価項目 2.1	システムが自動アクセスする対象を攻撃者の意図で誘導する 評価項目 2.2
外部NWから車両への直接アクセスが可能	(N/A)	各種I/Fの脆弱性をつく攻撃(評価項目 2.3) 通信傍受した情報を使う攻撃(評価項目2.4)

【インシデント以外で取り込んだ評価項目】

- Bluetooth関連について、Bosch社のBluetoothドングル等の車両部品システムにインシデント事例があり、それら内容を項目化した
- ITセキュリティで攻撃事例および被害の多い標的型攻撃を考慮するものと判断し、「ファイル添付攻撃」「偽サーバー誘導による攻撃」を項目化した

➢ 3.権限昇格

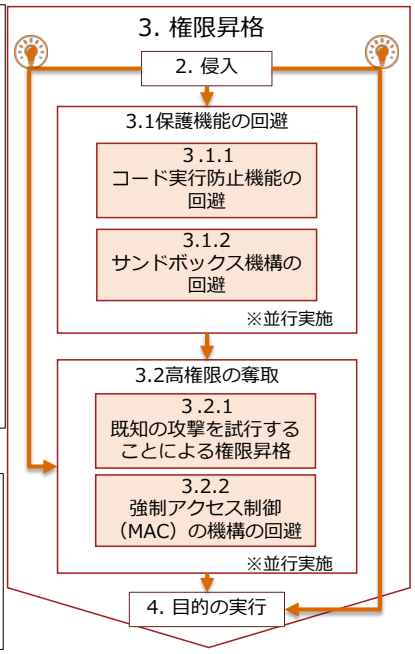
【評価方針】

- 任意コード実行が失敗した際のエラー状態に応じて、当該原因の回避策を試行する
- 任意コード実行の失敗の状態と原因は以下のとおり

失敗の状態	評価項目	失敗の原因	防御機構例
実行できない	3.1.1.	意図した位置にコードが存在しない	ASLR
		コード実行禁止のセグメントに配置	DEP、Nxbit
攻撃対象にアクセスできない	3.1.2.	コード実行が管理された領域に配置された	サンドボックス
実行が途中で停止する	3.2.1.	実行権限の不足	一般アクセス管理
	3.2.2.	強制アクセス制御による停止	SELinux

【インシデント以外で取り込んだ評価項目】

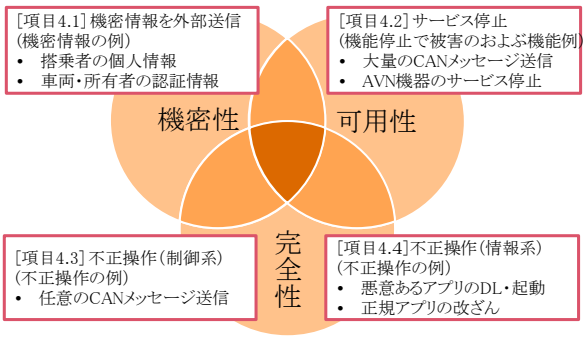
- IoT製品（特にスマートデバイス）でのJailBreak事例を踏まえ、今後車両セキュリティで同種の問題が発生することを考慮し、各項目化した



➢ 4.目的の実行

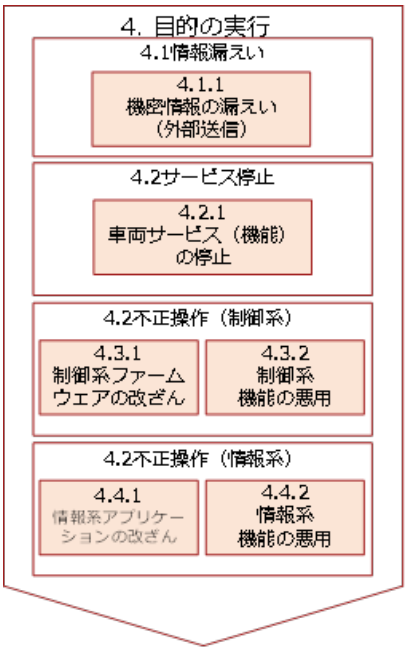
【評価方針】

- セキュリティ特性(CIA:機密性、完全性、可用性)の各観点で、システムに被害を及ぼす攻撃を実行する



【インシデント以外で取り込んだ評価項目】

- 特になし
(既知の車両インシデントでは攻撃後に機密性、完全性、可用性それぞれの観点で攻撃が実行されている)



4.3. 評価項目一覧

本ガイドの評価項目の一覧を示す。

カテゴリ(大項目)	カテゴリ	評価項目	確認項目
	1.1 HW調査	1.1.1 デバイス取り出し前I/F調査	1.1.1.1 USBポート接続確認
			1.1.1.2 RJ45ポート接続確認
			1.1.1.3 RS-232Cポート接続確認
		1.1.2 デバイス取り出し後I/F調査	1.1.2.1目視による確認
			1.1.2.2 マルチメータによる確認
			1.1.2.3 ポートファジングツールを用いた確認
		1.1.3 チップ取り外し後I/F調査	1.1.3.1 MCUのチップ調査
			1.1.3.2 EEPROMのチップ調査
			1.1.3.3 NANDフラッシュ、eMMCのチップ調査
		1.1.4隠れたインターフェースからの調査	1.1.4.1 公開情報からのスペック調査
			1.1.4.2専門業者への解析依頼
		1.1.5 インターフェース接続	1.1.5.1 イーサネットからのパスワード認証の確認
			1.1.5.2 イーサネットから脆弱性診断スキャン
			1.1.5.3 シリアルからのパスワード認証の確認
			1.1.5.4 シリアルからのBootLoaderの確認
			1.1.5.5 NANDフラッシュ、eMMCからのコンソール取得
			1.1.5.6 root権限の取得
		1.1.6 バイナリ抽出	1.1.6.1 root取得後のバイナリ抽出
			1.1.6.2 ADBからのバイナリ抽出
			1.1.6.3 BootLoaderからのバイナリ抽出
			1.1.6.4 デバッグポートからのバイナリ抽出
			1.1.6.5 EEPROMからのバイナリ抽出
			1.1.6.6 NANDフラッシュ、eMMCからのバイナリ抽出
		1.1.7 バイナリ保護機能確認	1.1.7.1 マニュアルによる調査
			1.1.7.2 目視によるバイナリファイルの調査
			1.1.7.3 EEPROMからの鍵の入手
			1.1.7.4 RAMからの鍵の抽出
			1.1.7.5 暗号処理モジュールからの鍵の抽出
			1.1.7.6 暗号化方式の確認
			1.1.7.7 別の車載器からの鍵の抽出

カテゴリ（大項目）	カテゴリ	評価項目	確認項目
1.偵察	1.1 HW調査	1.1.8 リバースエンジニアリング	1.1.8.1 ファイルシステムの調査
			1.1.8.2 逆アセンブラの実行
			1.1.8.3 逆コンパイラの実行
	1.2 SW調査	1.2.1 アプリケーションの通信経路の調査	1.2.1.1 通信経路の調査
		1.2.2 WiFi（車両外部）の通信傍受	1.2.2.2外部へのアクセス先の確認
			1.2.2.2待ち受けポートの確認
			1.2.2.3 SSL暗号化の確認
			1.2.2.4 認証情報の確認
			1.2.2.5 リプレイ、成りすまし防止情報の解析
		1.2.3 WiFi（車両内部）の通信傍受	1.2.3.1 アクセス先ポート確認
			1.2.3.2 SSL暗号化の確認
			1.2.3.3 認証情報の解析
			1.2.3.4 リプレイ防止情報の解析
			1.2.3.5 認証方式の確認
			1.2.3.6 パスワード規則性の推測
			1.2.3.7 WiFiパスワードの解析
		1.2.4 Bluetoothの通信傍受	1.2.4.1 BluetoothMACアドレスが検出可能なタイミングの確認
			1.2.4.2 ペアリング方式の確認
			1.2.4.3 Bluetoothプロファイルの調査
		1.2.5 BluetoothLEの通信傍受	1.2.5.1 スマートフォン⇔車載間のBLE通信傍受
			1.2.5.2 キーフォブ⇔車載間のBLE通信傍受
		1.2.6 TCUの通信傍受	1.2.6.1 公開IPアドレススキャン
			1.2.6.2 ATコマンドを利用したオーバーフロー攻撃
			1.2.6.3 ATコマンドを利用したDDoS攻撃
		1.2.7 ブラウザ、HTMLエンジンの調査	1.2.7.1 ブラウザアプリの選別
			1.2.7.2 バージョンの取得
		1.2.8 CANメッセージ通信傍受	1.2.8.1 CANメッセージキャプチャツールの設置
			1.2.8.2 CANメッセージの送受信
		1.2.9 アプリケーションの通信傍受	1.2.9.1 プロキシ用端末の証明書のインストール
			1.2.9.2 キャプチャ内容の確認
2.侵入	2.1 ユーザー介在型の受動的攻撃	2.1.1 DrivebyDownload攻撃	2.1.1.1 ブラウザの脆弱性確認
			2.1.1.2 攻撃用Webサイトへのアクセス
			2.1.1.3 Webサイトから攻撃の反応確認
		2.1.2 ファイル添付攻撃	2.1.2.1 リバースシェルの配布
			2.1.2.2 リバースシェルのダウンロード
			2.1.2.3 リバースシェルの実行
	2.2 ユーザー非介在型の受動的攻撃	2.2.1 外部WiFiへの自動接続を利用した攻撃	2.2.1.1 マニュアルベースの確認
			2.2.1.2 バイナリファイルの確認
			2.2.1.3 接続確認
		2.2.2 偽サーバー誘導による攻撃	2.2.2.1 アプリケーションの脆弱性調査
			2.2.2.2 アプリケーションの実行
			2.2.2.3 攻撃の確認
		2.2.3 残存開発環境を用いた攻撃	2.2.3.1 用途不明の通信経路の調査
			2.2.3.2 WiFiへの接続
			2.2.3.3 通信ログ確認
	2.3 脆弱性を利用した能動的攻撃	2.3.1 Bluetooth経由の攻撃	2.3.1.1 MACアドレスの入手
			2.3.1.2 APIの脆弱性を利用した攻撃
			2.3.1.3 プロトコルの脆弱性を利用した攻撃
		2.3.2 BluetoothLE経由の攻撃	2.3.2.1 MACアドレスの入手
			2.3.2.2 APIの脆弱性を利用した攻撃
			2.3.2.3 プロトコルの脆弱性を利用した攻撃
		2.3.3.TCU経由の攻撃	2.3.3.1 TCU側サービスAPIの脆弱性を利用した攻撃
			2.3.3.2 機器の脆弱性を利用した攻撃
		2.3.4 WiFi（車両内部）経由の攻撃	2.3.4.1 公開ポートからのログイン
			2.3.4.2 スマートフォンの解析
			2.3.4.3 APIソースコードの解析
	2.4 通信傍受した情報を用いた能動的攻撃	2.4.1 成りすまし攻撃	2.4.1.1 サーバーを経由した成りすまし攻撃
			2.4.1.2 BluetoothLEからの成りすまし攻撃
			2.4.1.3 WiFi（内部設置）からの成りすまし攻撃
			2.4.1.4 成りすまし攻撃の対策確認
		2.4.2 リプレイ攻撃	2.4.2.1 サーバー⇒TCUパケットをリプレイ
			2.4.2.2 BluetoothLEデバイス⇒車両パケットをリプレイ
			2.4.2.3 WiFiデバイス⇒車両（WiFi内部設置）パケットをリプレイ
			2.4.2.4 リプレイ攻撃への対策確認

カテゴリ（大項目）	カテゴリ	評価項目	確認項目
3. 権限昇格	3.1 保護機能の回避	3.1.1 コード実行防止機能の回避	3.1.1.1 NXビットの確認
			3.1.1.2 ASLRの確認
			3.1.1.3 SSPの確認
			3.1.1.4 PIEの確認
			3.1.1.5 RELRO-FULLの確認
			3.1.1.6 既知の脆弱性を利用したデータ実行保護機能の確認
		3.1.2 サンドボックス機構の回避	3.1.2.1 ファイルシステムの制限の確認
			3.1.2.2 システムコールの制限の確認
			3.1.2.3 既知の脆弱性を利用したサンドボックスの回避
	3.2 高権限の奪取	3.2.1 既知の攻撃を試行することによる権限昇格	3.2.1.1 root権限の昇格
		3.2.2 強制アクセス制御（MAC）の機構の回避	3.2.2.1 強制アクセス制御の確認
			3.2.2.2 強制アクセス制御の回避
4.目的の実行	4.1 情報漏えい	4.1.1 機密情報の漏えい（外部送信）	4.1.1.1 機密情報の調査
			4.1.1.2 外部へのデータ送信
	4.2 サービスの停止	4.2.1 車両のサービス（機能）の停止	4.2.1.1 プロセス強制終了による車両サービスの停止
			4.2.1.2 CPU負荷上昇による車両サービスの停止
			4.2.1.3 ネットワーク負荷上昇による車両サービスの停止
			4.2.1.4 ディスク負荷上昇による車両サービスの停止
	4.3 不正操作（制御系）	4.3.1 制御系ファームウェアの改ざん	4.3.1.1 チェックサムによるアップデート保護の回避
			4.3.1.2 デジタル署名によるアップデート保護の回避
			4.3.1.3 ファームウェアのダウングレード
		4.3.2 制御系機能の悪用	4.3.2.1 CANメッセージを実行するAPIの調査
			4.3.2.2 APIを利用した制御系の操作
	4.4 不正操作（情報系）	4.4.1 情報系アプリケーションの改ざん	4.4.1.1 監視項目の確認
			4.4.1.2 セーフティシステムの無効化
			4.4.1.3 暗号化方式の確認
			4.4.1.4 デジタル署名を改ざんした状態でのアプリケーション起動
			4.4.1.5 異なるユーザーのデジタル署名を付与した状態でのアプリケーション起動
		4.4.2 情報系機能の悪用	4.4.2.1 アプリケーションを実行するAPIの調査
			4.4.2.2 APIを利用した情報系の操作

表 4.3-1 評価項目一覧

4.4. 評価項目フォーマットの説明

各評価項目の記載フォーマットを以下に示す。

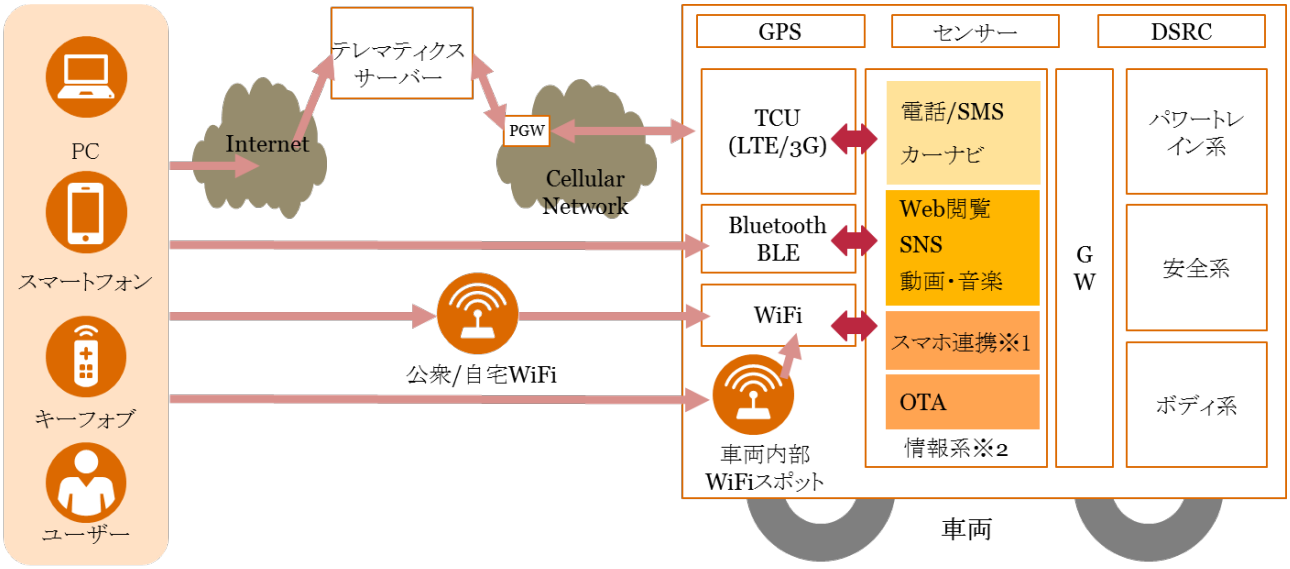
項目	記載内容
項目番号	項目番号を記載
項目名	小項目名称を記載
目的	評価項目の目的を記載する
実施タイミング	どこの開発段階で評価されるのかプロセスと紐付けを明確にする．本ガイドの評価は車両システムテスト時の実施を基本とする。ただし、評価期間の短縮のためにテーラリングの一環として、一部の項目を単体テスト時等に実施する場合がある。
想定実施工数（作業量）	評価する際の環境構築、技術習得、評価時間、結果判定に必要となる工数を記載する.ここには全体の工数を記載する※別途フォーマットを準備
前提条件	他の評価項目の結果により実施有無が決定する項目の場合、その前提となるテスト項目の内容を記載する 例）項目ｘｘにおいて、問題が検出された場合に実施する
入力情報	評価実施に当たって必要となる以下の情報を必要に応じて記載する 評価の実施に必要となる仕様情報

	他のテスト項目の結果
実施条件	評価を実施する際のターゲットの接続状態や、動作状態に条件が存在する場合にそれを記載する 実施すべきテストパターンを記載する
外部委託判断	評価実施時で必要となる技術・設備要件を記載する これにより当該項目実施を外部委託する際の判断基準とする
事前作業	評価を行う前に必要な環境準備の概要を記載する
確認事項	評価項目において確認すべき観点を具体的に記述する 各観点に連番（1.、2.、・・・）をつける
取得エビデンス	実行結果として取得すべきデータ
事前作業実施例	事前作業の手順を具体的に記載する
実施例	具体的な評価実施方法を 1 つ以上記載する 番号は「確認事項」の番号と合わせる 同じ「確認事項」の番号で複数の実施方法を記載する場合は、サブ番号（1-1.、1-2.、・・・）を振る
結果判断	評価を実施した結果、評価結果を判断するための観点を記載する。評価実施を外部委託した場合についても本項目の内容をもとに受け入れ確認すること。 判断に足る情報が集まらない場合、引き続き実施例の作業を継続する、もしくは、外部委託先に追加調査を依頼する
開発評価観点	攻撃を防ぐために推奨する設計上の考慮点
備考	評価を実施する上での注意点や、ツールや手順の参考情報を記載する 商用ツール含めて全て記載すること.ガイドへの掲載判断は別途行う

4.5. 評価対象プラットフォーム

以下に本評価において想定する車両システムのモデル図を示す。

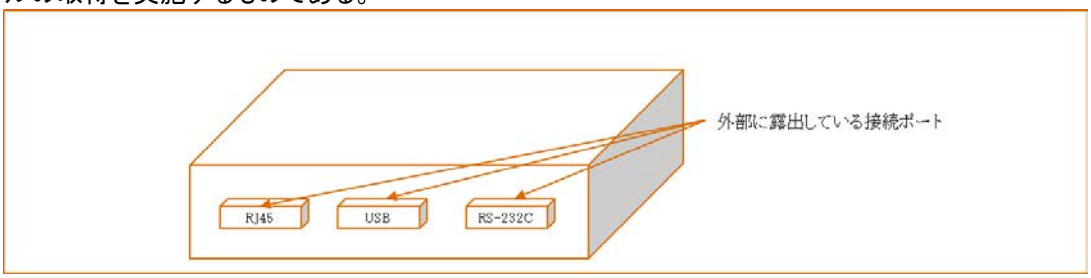
- ユーザー（搭乗者）はキーフォブ、スマートフォン、PC を用いてテレマティクスサーバーあるいは直接車両にアクセスし、外部 I/F（TCU、Bluetooth/BLE、WiFi）を経由して情報系 OS 上で稼働する各アプリケーションと通信を行う
- 情報系と制御系（パワートレイン系、安全系、ボディ系等）は直接ネットワーク接続されておらず、GatewayECU によって隔てられている
- 評価項目ごとに情報系プラットフォームとして実績の多い Linux を前提としたコマンドライン等の参考例を記載しているが、評価項目としては QNX、Android 等他のプラットフォームにも適用可能



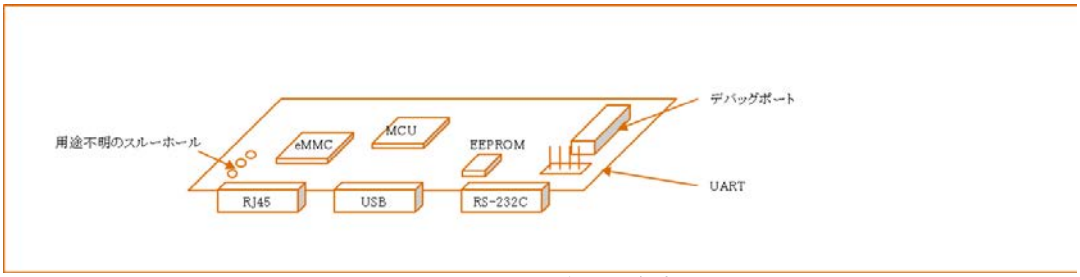
※1 Android Auto、Car Play、MirrorLink、SDL 等

※2 Linux（Automotive Grade Linux 等）、QNX、Android 等、インフォテイメント系 OS

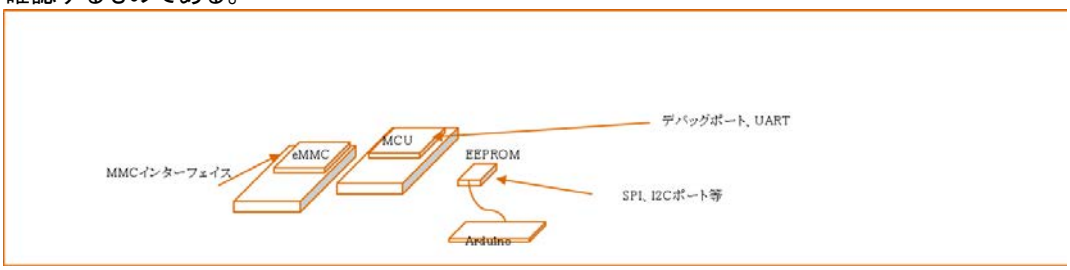
4.6. 評価項目

項目	記載内容
項目番号	1.1.1
項目名	デバイス取り外し前 I/F 調査
目的	外部ポートからコンソールを取得する
実施タイミング	車両システムテスト時
想定実施工数（作業量）	8 時間未満
前提条件	特になし
入力情報	車載器マニュアル（取り付けマニュアル、操作マニュアル） サービスモードへの変更方法
実施条件	対象車載器に電源が供給され、使用可能な状態であること コンソール取得用のツールが準備できていること
外部委託判断	本項目は OEM が実施することを推奨する。 なお、実施にあたり Linux OS のネットワークコマンドを理解していることを前提する。
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目は、デバイスの外殻を取り外すことなく、外部に露出したポートを調査することで、コンソールの取得を実施するものである。  以下の確認項目を実行し、コンソールを取得できるか確認する **1. ユーザー接続ポートからのコンソール接続確認** 1.1 USB ポート接続確認（1.1.1.1） コンソールが取得できた場合「1.1.5 インターフェース接続」に進む 1.2 RJ45 ポート接続確認（1.1.1.2） コンソールが取得できた場合「1.1.5 インターフェース接続」に進む 1.3 RS-232C ポート接続確認（1.1.1.3） コンソールが取得できた場合「1.1.5 インターフェース接続」に進む 確認項目のいずれも該当しない場合、あるいはコンソールが取得できない場合、以下に進む 「1.1.2 デバイス取り外し後の I/F 調査」 「1.1.3 取り外し後 I/F 調査」
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット） ・ 取り付け位置を示した写真 ・ 背面パネルの配線図を示した写真
事前作業実施例	公開用資料のため、記載内容を削除

実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発評価観点	車内に露出しているユーザー接続ポートはアクセサリー接続など最低限のサービスに制限していることを確認する。 またサービス仕様上問題ない場合、接続には何らかの認証を有することが望ましい。
備考	・ Android Studio（Androud SDK） https://developer.android.com/studio/index.html?hl=ja

項目	記載内容
項目番号	1.1.2
項目名	デバイスの取り外し後 I/F 調査
目的	プリント基盤を確認し、内部ポートからコンソールあるいはデバックポートを取得する
実施タイミング	車両システムテスト時 （テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）
想定実施工数（作業量）	1～5 日
前提条件	「1.1.1 デバイス取り外し前 I/F 調査」でコンソールが取得できなかった場合に実施する
入力情報	対象チップのマニュアル（ピンレイアウト記載のもの）
実施条件	対象車載器が取り外された状態であること 対象車載器に電源が供給され、使用可能な状態であること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. チップメーカーのマニュアルからピンレイアウト構成を理解できる人材が確保できない 2. 本項目に必要な機材（マルチメータ、ポートファジングツール）準備および運用することができない
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目は、プリント基板からバイナリファイル取得対象となるチップを選定した上で、露出したピンヘッダ・スルーホールからバイナリファイルの取得を実施するものである。  以下の項目を順番に確認し、コンソールあるいはデバッグポートの有無を確認する **1. 視認が容易なポートからの取得** 1.1 目視による確認（1.1.2.1） UART ポートが確認できた場合、「1.1.5 インターフェース接続」に進む デバッグポートが確認できた場合、「1.1.6 バイナリ抽出」に進む 1.2 マルチメータによる確認（1.1.2.2） UART ポートが確認できた場合、「1.1.5 インターフェース接続」に進む デバッグポートが確認できた場合、「1.1.6 バイナリ抽出」に進む **2. 視認が困難なポートからの取得** 2.1 ポートファジングツールを用いた確認（1.1.2.3） UART ポートが確認できた場合、「1.1.5 インターフェース接続」に進む デバッグポートが確認できた場合、「1.1.6 バイナリ抽出」に進む 確認項目のいずれからもコンソール、デバッグポートが確認できない場合、「1.1.3 チップ取り外し後 I/F 調査」に進む
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット） ・ プリント基板を示した写真
事前作業実施例	公開用資料のため、記載内容を削除

実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発評価観点	基盤上に不要な外部入出力ポートを露出していないことを確認する
備考	・ Reverse Engineering Serialports http://www.devttys0.com/2012/11/reverse-engineering-serial-ports/ ・ Jtagulator http://www.grandideastudio.com/jtagulator/

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>1.1.3</td></tr>
<tr><td>項目名</td><td>チップ取り外し後 I/F 調査</td></tr>
<tr><td>目的</td><td>チップをプリント基板から剥がし、チップの足から直接バイナリファイルを取得できるか確認する</td></tr>
<tr><td>実施タイミング</td><td>車両システムテスト時
（テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）</td></tr>
<tr><td>想定実施工数（作業量）</td><td>1～5 日</td></tr>
<tr><td>前提条件</td><td>「1.1.2 デバイス取り外し後 I/F 調査」においてデバッグポート、UART ポートが確認できなかったチップがある場合に実施する</td></tr>
<tr><td>入力情報</td><td>対象チップのマニュアル（ピンレイアウト記載のもの）
対象チップの一覧（1.1.2 で確認済みのもの）</td></tr>
<tr><td>実施条件</td><td>対象車載器が取り外された状態であること
対象チップが取り外されていること
対象チップのデータ抽出に必要な機器の準備が完了していること</td></tr>
<tr><td>外部委託条件</td><td>以下いずれかの条件に該当する場合、外部への委託を検討する
1.　チップの取り外し（ソルダリング）の実施経験のある人材が確保できない
2.　ソケットアダプタ、ヒートガン等対象チップのチップ取り外しに必要な機器が準備できない</td></tr>
<tr><td>事前作業</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>確認事項</td><td>本項目は、チップをプリント基板から剥がし、チップの足から直接バイナリファイルを取得できるか確認するものである。
 

確認対象チップのタイプによって応じて 1～3 へ進む。

<table>
<tr><th>番号</th><th>チップ</th></tr>
<tr><td>1</td><td>MPU（フラッシュメモリ内蔵タイプ）</td></tr>
<tr><td>2</td><td>EEPROM</td></tr>
<tr><td>3</td><td>NAND フラッシュ、eMMC</td></tr>
</table>

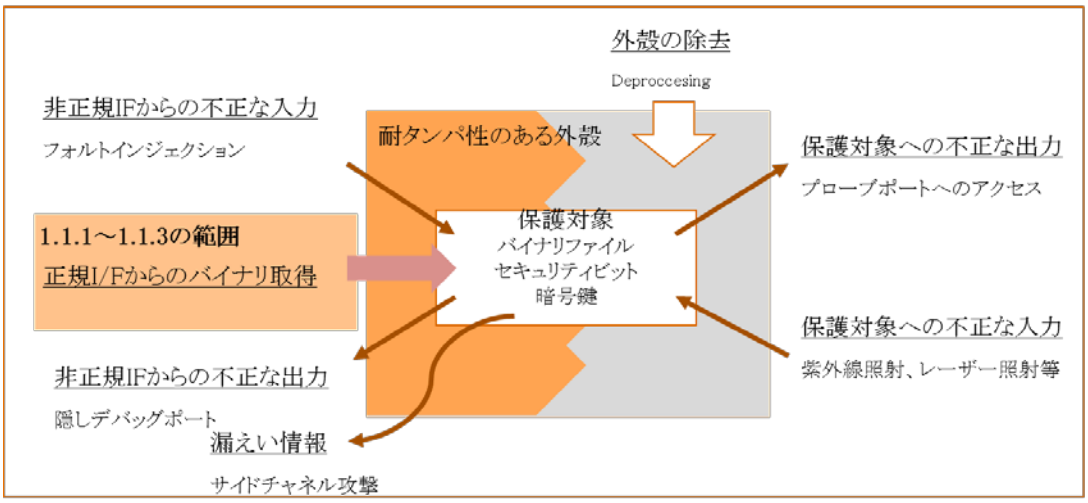
1. MCU のチップ調査（1.1.3.1）
剥がした MCU の調査を行う。デバッグポートが確認できた場合、「1.1.6 バイナリの抽出」に進む。

2. EEPROM のチップ調査（1.1.3.2）
剥がした EEPROM の調査を行う。インターフェース（SPI、I2C 等）が確認できた場合、「1.1.6 バイナリの抽出」に進む。

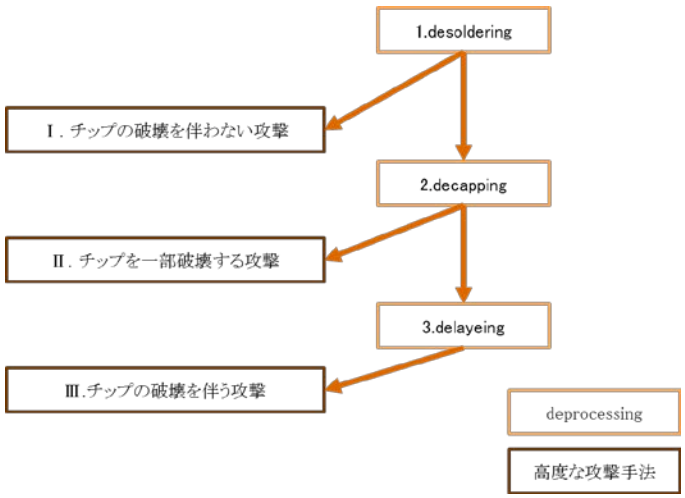
3. NAND フラッシュ、eMMC のチップ調査（1.1.3.3）
剥がした NAND フラッシュ、eMMC の調査を行う。チップをソケットアダプタに取り付け後、「1.1.6 バイナリ抽出」に進む。

確認対象のチップ毎、チップのタイプがいずれにも該当しない場合、あるいは、確認が成功しない場合、「1.1.4 隠れたインターフェースからの調査」に進む。</td></tr>
<tr><td>取得エビデンス</td><td>・　実行したコマンド一覧
・　GUI 画面の出力（スクリーンショット）</td></tr>
</table>

	・ プリント基板を示した写真 ・ ソケットアダプタを示した写真
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発評価項目	製品仕様上問題ない場合、チップのデバックポートを無効化する。もしくはデバックポートからの読み込みを禁止し、書き込みのみを許可する 重要な情報が含まれているチップが、BGA 等物理的にアクセスしにくいことを確認する
備考	・ 富士通：パッケージの体系/形状/構造 http://edevice.fujitsu.com/jp/datasheet/readmej/contents2.pdf ・ Samsung：Galaxy S3 dead repair by changing EMMC https://www.youtube.com/watch?v=rOYo9AcUQQI ・ HAKKO：こて先選択ガイド https://www.hakko.com/japan/tip_selection/work_qfp_removing.html ・ ケイ・ワーク http://www.kei-all.co.jp/

項目	記載内容
項目番号	1.1.4
項目名	隠れたインターフェースからの調査
目的	セキュリティ対策が施されているチップからバイナリファイルを抽出できるか確認する
実施タイミング	車両システムテスト時 （テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）
想定実施工数（作業量）	1～5 日
前提条件	1.1.2、1.1.3、1.1.5、1.1.6 においてバイナリファイルが取得できない、あるいは暗号化を解読できない場合に実施する
,	対象チップのマニュアル 対象チップのセキュリティ対策を記載した公開技術資料
実施条件	各手法に必要な資機材の準備が完了していること
外部委託条件	本項目は基本的に外部委託することを推奨する
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目は JTAG、UART 等の正規インターフェースではない、隠れたインターフェースから特別な設備を使用してバイナリファイルを取得できるかを確認するための評価項目である。  最初に各チップメーカーの公開技術資料と対象チップが認証制度を受けているかどうか調べ、バイナリファイルの取得の可能性のある攻撃が判明した場合は、専門の外部業者にチップの解析依頼を行う。具体的な確認項目は以下のとおり。 **1. 公開情報からのスペック調査（1.1.4.1）** 1.1 チップメーカー公開資料からの調査 1.2 認証制度からの調査 **2. 専門業者への解析依頼（1.1.4.2）** **【確認実施のために必要な補足事項】** 本項目で想定する攻撃手法および、参考とする国際評価基準を以下に示す。 **a. 想定される攻撃手法**

セキュリティ対策が施されたチップを攻撃するためには、チップのセキュリティ対策を解除するDeprocessing を実施する必要がある。



a.1 各 Deprocessing および想定レベル

各 Deprocessing 工程に必要機材、スキルおよび想定レベルを以下に示す。

名称/想定レベル	説明	必要機材
Desoldering /Middle～High	チップをプリント基板から剥がし、専用のソケットアダプタに移植する	・ソルダリングステーション ・ソケットアダプタ ・マイクロニードル ・デジタルマイクロスコープ ・X線非破壊検査装置等
Decapping /High～Extreme	チップのモールドをくり抜き、ボンディングワイヤーを除去し化学洗浄することで、半導体回路を表面にさらす。 または半導体回路上面がセキュリティレイヤで覆われていた場合、レイヤーをレーザー切断、あるいはマイクロニードルで除去する。	・グラインダー ・化学実験器具 ・モールドの材質に合わたエッチングを行うための化学薬品（硫酸、水酸化ナトリウム等） ・金属顕微鏡 ・Micro Probe Station 等
Delayering /Extreme	層間絶縁膜等、半導体積層構造の一部を観察可能な状態まで除去する。	Decapping の機材に加え ・走査電子顕微鏡 ・集束イオンビーム（FIB） ・レーザー照射装置等

a.2 各攻撃手法の想定レベル

各攻撃手法想定レベルを以下に示す。チップの状態に応じて以下の3つに分類した。

Ⅰ. チップの破壊を伴わない攻撃
Ⅱ. チップを一部破壊する攻撃
Ⅲ. チップの破壊を伴う攻撃

チップの状態/想定レベル	手法	説明	備考
Ⅰチップの破壊を伴わない攻撃/ High	隠しデバッグポートへのアクセス（BGA）	チップ裏側のプリント基板からデバッグポートへのピンに物理的に穴をあけ、デバッグポートへアクセスすることでバイナリファイルを抽出する	Desolding 作業に加え、各攻撃手法に関する専門知識および機材の運用経験が必要
	不正グリッチによるフォルトインジェクション攻撃	電源ラインに不正な電力、細かいパルスを入力して悪用可能な異常動作を誘発させることで、code protection を解除し、バイナリファイルを抽出する	
	サイドチャネル攻撃	電力消費あるいは電磁波照射の特徴的な変化を通して漏れた情報を観察	

				することでセキュアブート時に使用される暗号鍵を取得する	
		Ⅱチップを一部破壊する攻撃/ High～Extreme	紫外線照射による bit 反転	UV-EPROM,EPROM の register bit に紫外線を照射し、code protection を解除することでバイナリファイルを抽出する	高度な Deprocessing 作業に加え、数百 nm 単位の半導体のプローブポートにアクセスするための Probe Station の運用経験が必要。また物理セキュリティレイヤが存在する場合、これを除去することは非常に困難であるため、Extreme とする
			Probing による read 端子読み取り	チップ内の配線もしくは端子に物理的な Probe を当て、機密情報の読み出しを行うことでバイナリファイルを抽出する	
			Probing による Logic 変更による確認	チップ内の配線もしくは端子に物理的な Probe を当て、外部から電圧を与え、デバッグポートへのアクセスを解放させることで、バイナリファイルを抽出する	
		Ⅲチップの破壊を伴う攻撃(回路を破壊する)/ Extreme	回路のイメージング	チップ裏側からフローティングゲートに対し電子ビームを当て、2 次電子を測定することでバイナリファイルのビット配列を取得する	極めて高度な Deprocessing 作業に加え、イメージングで得られた画像から半導体回路を解析可能な設計知識と数十 nm レベルの精度で回路を照射するレーザー照射機器等の運用経験が必要
			レーザー照射によるフォルトインジェクション攻撃	チップ内のデバッグ回路の配線をレーザーで編集(破壊・蒸着)し、ロジックを変化させることで機密情報の読み出しができるか確認する	
			集束イオンビーム(FIB)による配線編集による確認	チップ内のデバッグ回路の配線を FIB で編集(破壊・蒸着)し、デバッグポートへのアクセスを解放させることで、機密情報の読み出しができるか確認する	

b. 暗号モジュールの要求規格 ISO/IEC19790

ISO/IEC 19790 は暗号モジュール要求規格であり、実装機能に応じてレベルを定義する。ソフトウェア要求(対象鍵、非対称鍵等の暗号強度)の他に、物理セキュリティ要求(物理セキュリティ、非侵入セキュリティ)についても以下の通り定義されている。この規格に従ったセキュリティチップの認証制度(FIPS140、JCMVP 等) があり、認可されたチップは公開されているため、公開情報から検索することで、該当チップのセキュリティ実装を確認することが可能。

※試験項目によっては各専門業間で検証方法で統一がされておらず、場合によっては実施しない可能性があるため後述の専門業者に問い合わせが必要。

セキュリティレベル	説明	必要なセキュリティ実装(2012 年版)
1	市販品として求められる基本的なセキュリティ要求事項を満たすレベル。セキュリティ確保のための物理的なメカニズムは要求されないレベル。	なし
2	セキュリティレベル 1 に加え、タンパ証跡(暗号モジュールを開封した跡が 残るようなシールなど)に関する要求事項を加えたレベル。	・開封検知機構 ・ホールやスリットからの侵入防止
3	セキュリティレベル 2 に加え、タンパ検出・応答(暗号モジュールを開封したことを 検出しデータ消去などの応答をする)に関する要求事項を加えたレベル。	・開封防止機構 ・チップの強固なコーティング ・プローブアクセス防御 ・メンテナンスアクセスの検知 グリッチ攻撃耐性(温度、電力) サイドチャネル攻撃耐性
4	セキュリティレベル 3 に加え、いかなる物理的な攻撃に対してもタンパ検出・応答 をするように完全に暗号モジュール部分を被覆保護する物理的メカニズムを 加えたレベル さらに 正常に動作する電圧 温度の範囲を超えた環境条件 変動加えたレベル。さらに、正常に動作する電圧・温度の範囲を超えた環境条件・変動 に関する要求事項も追加されている。	・グリッチ攻撃防御機構(温度、電力、クロック) ・その他あらゆる物理攻撃に対するタンパ耐性

取得エビデンス	・ チップメッカ―提供のホワイトペーパー ・ 認証チップの調査結果
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発評価項目	チップが耐タンパ性などの物理的な対策を有しているか確認する
備考	・ 独立行政法人 情報処理推進機構技術本部セキュリティセンター：ハードウェアセキュリティ―IoT の時代に向けて https://www.trustedcomputinggroup.org/wp-content/uploads/JRF/%5bJRFWS%5dDec2015_3.%20IPA_S.%20Sato_Presen+ForWeb.pdf.pdf ・ IPA：ハードウェア脆弱性評価の最新技術動向に関するセミナー https://www.ipa.go.jp/security/jisec/seminar/documents/hw_semi_20160204_1.pdf ・ Chipworks Inc：The State-of-the-Art in IC Reverse Engineering https://www.iacr.org/archive/ches2009/57470361/57470361.pdf ・ 財団法人 日本規格協会情報技術標準化研究センター：耐タンパ性調査研究委員会報告書 https://www.ipa.go.jp/security/enc/CRYPTREC/fy15/documents/INSTAC_rep.pdf ・ ケンブリッジ大学：Physical Attacks on Tamper Resistance: Progress and Lessons http://www.cl.cam.ac.uk/~sps32/ARO_2011.pdf ・ レンセラー工科大学：CSCI4974/6974 hrdware reverse Engineering http://security.cs.rpi.edu/courses/hwre-spring2014/Lecture15_Antitamper.pdf

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>1.1.5</td></tr>
<tr><td>項目名</td><td>インターフェース接続</td></tr>
<tr><td>目的</td><td>コンソール接続し、root 権限を取得する（ファームウェア抜き取りが可能な状態とする）</td></tr>
<tr><td>実施タイミング</td><td>車両システムテスト時
（テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）</td></tr>
<tr><td>想定実施工数（作業量）</td><td>8 時間未満</td></tr>
<tr><td>前提条件</td><td>前段の評価項目でコンソールを取得済み
あるいは NAND フラッシュ、eMMC のチップのバイナリファイルを取得済み</td></tr>
<tr><td>入力情報</td><td>対象チップのマニュアル（ピンレイアウトが記載のもの）</td></tr>
<tr><td>実施条件</td><td>対象車載器に電源が供給され、使用可能な状態であること
root の取得に必要な環境の準備が完了していること</td></tr>
<tr><td>外部委託条件</td><td>以下いずれかの条件に該当する場合、外部への委託を検討する
1.　公開済みの攻撃コードを実行できる経験を有する人材が確保できない
2.　脆弱性スキャナ等、root の取得に必要な環境の準備が準備できない</td></tr>
<tr><td>事前作業</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>確認事項</td><td>条件に応じて 1～4 へ進む。ログイン（コマンドプロンプト）の取得に成功した場合、【4. root の取得】に進む。

<table>
<tr><th>番号</th><th>条件</th></tr>
<tr><td>1</td><td>イーサネットからコンソールを取得済み</td></tr>
<tr><td>2</td><td>シリアルポートまたは UART からシリアルコンソールを取得済み</td></tr>
<tr><td>3</td><td>ADB コンソールを取得済み</td></tr>
<tr><td>4</td><td>NAND フラッシュ、eMMC のチップのバイナリファイルを取得済み</td></tr>
</table>

1. イーサネットからのコンソール確認

1.1 イーサネットからのパスワード認証の確認（1.1.5.1）
ログインに成功した場合、【4. root の取得】に進む

1.2 イーサネットからの脆弱性診断スキャン（1.1.5.2）
ログインに成功した場合、【4.root の取得】に進む

2. シリアルからのコンソールの確認

2.1 シリアルからのパスワード認証の確認 （1.1.5.3）
ログインに成功した場合、【4. root の取得】に進む

2.2 シリアルからの BootLoader の確認（1.1.5.4）
BootLoader のコマンドプロンプトが確認できた場合、「1.1.6 バイナリ抽出」に進む

3. ADB からのコンソール確認

ADB の場合、パスワードなしでログイン可能であるため、そのまま【4. root の取得】に進む。
※本項目は作業は発生しない。

4. NAND フラッシュ、eMMC のチップからのコンソール取得（1.1.5.5）

NAND フラッシュ、eMMC のファイルを改ざんすることでコンソールの取得を行う。既にバイナリファイルの抽出に成功していることが前提のため、コンソールの取得後は、「2. 侵入」の実施を検討する。

5. root 権限の取得（1.1.5.6）</td></tr>
</table>

	既知の脆弱性を利用して root 権限を取得する。成功した場合、「1.1.6 バイナリ抽出」に進む。 確認項目のいずれも成功しない場合、いかのいずれかに進む。 「1.1.2 デバイス取り出し後 I/F 調査」 「1.1.3 チップ取り外し後 I/F 調査」 「1.1.4 隠れたインターフェースからの調査」
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット） ・ プリント基板を示した写真
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発評価項目	外部 IF からのアクセスにはアクセス制限、もしくは、ユーザー認証などの制限を設けること
備考	・ adb コマンド https://developer.android.com/studio/command-line/adb.html?hl=ja ・ JVN 脆弱性情報提供データベース http://jvndb.jvn.jp/index.html ・ 攻撃コード提供サイト Exploit-db https://www.exploit-db.com/

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>1.1.6</td></tr>
<tr><td>項目名</td><td>バイナリ抽出</td></tr>
<tr><td>目的</td><td>対象デバイスより、バイナリファイルを抽出する</td></tr>
<tr><td>実施タイミング</td><td>車両システムテスト時
（テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）</td></tr>
<tr><td>想定実施工数（作業量）</td><td>1～5 日</td></tr>
<tr><td>前提条件</td><td>いずれかの条件を満たす場合に実施する
・ コンソールから root 権限を取得済み
・ コンソールから BootLoader を取得済み
・ デバックポートを取得済み
・ チップのインターフェイスにアクセスできる状態であること</td></tr>
<tr><td>入力情報</td><td>対象 BootLoader のマニュアル（コマンド記載のもの）
対象チップのマニュアル（ピンレイアウトが記載のもの）
対象チップの開発環境のマニュアル</td></tr>
<tr><td>実施条件</td><td>ハードウェアタイプに応じたバイナリファイル取得環境が準備済みであること</td></tr>
<tr><td>外部委託条件</td><td>以下いずれかの条件に該当する場合、外部への委託を検討する
1. Linux の基礎的な操作経験およびプログラムツールの操作経験を有する人材が確報できない
2. ハードウェアタイプに応じたバイナリファイル取得環境の準備が準備できない</td></tr>
<tr><td>事前作業</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>確認事項</td><td>接続状態に応じて1～6 に進む。

<table>
<tr><th>番号</th><th>接続状態</th></tr>
<tr><td>1</td><td>root 権限を取得済み</td></tr>
<tr><td>2</td><td>ADB ポートを取得済み</td></tr>
<tr><td>3</td><td>BootLoader を取得済み</td></tr>
<tr><td>4</td><td>デバックポートを取得済み</td></tr>
<tr><td>5</td><td>EEPROM をチップから剥がし、ダンプ用マイコンに装着済み</td></tr>
<tr><td>6</td><td>NAND フラッシュ、eMMC をチップから剥がし、ソケットアダプタに装着済み</td></tr>
</table>

1. root 取得後のバイナリ抽出（1.1.6.1）

root 権限を取得後、外部記憶媒体あるいはネットワーク経由でバイナリファイルを転送する
バイナリファイルが抽出できた場合、「1.1.7 バイナリ保護機能確認」に進む

2. ADB からのバイナリ抽出（1.1.6.2）

ADB のバックアップコマンドを用いてバイナリファイルの抽出を行う。
バイナリファイルが抽出できた場合、「1.1.7 バイナリ保護機能確認」に進む

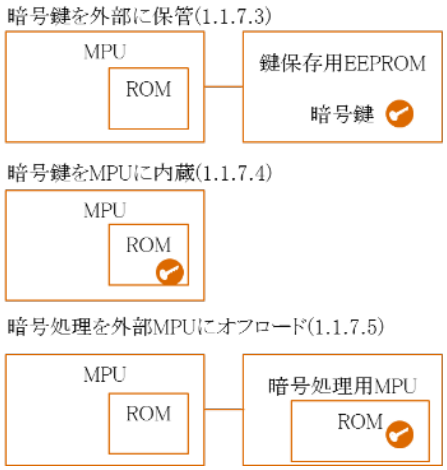
3. BootLoader からのバイナリ抽出（1.1.6.3）

BootLoader のメモリダンプコマンドを利用してバイナリファイルの抽出を行う。
バイナリファイルが抽出できた場合、「1.1.7 バイナリ保護機能確認」に進む

4. デバッグポートからのバイナリ抽出（1.1.6.4）

プログラミングツールを用いて、バイナリファイルの抽出を行う。
バイナリファイルが抽出できた場合、「1.1.7 バイナリ保護機能確認」に進む</td></tr>
</table>

	5. EEPROM からのバイナリ抽出（1.1.6.5） SPI、I2C 等のインターフェース経由で EEPROM のバイナリファイルの抽出を行う。 バイナリファイルが抽出できた場合、「1.1.7 バイナリ保護機能確認」に進む **6. NAND フラッシュ、eMMC からのバイナリ抽出（1.1.6.6）** プログラミングツールを用いてのバイナリファイルの抽出を行う。 バイナリファイルが抽出できた場合、「1.1.7 バイナリ保護機能確認」に進む 確認項目のいずれも該当しない場合、「1.1.4 隠れたインターフェースからの調査」に進む
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット） ・ プリント基板を示した写真
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	ROM を持つチップにはハードウェアプロテクションが実装されていることを確認し、チップを選定する。
備考	・ Arduino IDE https://www.arduino.cc/en/main/softwar ・ Using Arduino with an I2C EEPROM※一部コード修正 https://playground.arduino.cc/Code/I2CEEPROM ・ ケイ・ワーク http://www.kei-all.co.jp/ ・ ELNIC：BeePlog2 http://www.elnec.co.jp/beeprog2.html

項目	記載内容
項目番号	1.1.7
項目名	バイナリ保護機能確認
目的	バイナリファイルに暗号化、難読化が施されているか確認し、暗号化、難読化を解除する
実施タイミング	車両システムテスト時 （テーラリング対応：該当バイナリファイルのビルド成果物の単体テスト結果を活用しても良い）
想定実施工数（作業量）	1～5 日
前 提 条 件	バイナリファイルが抽出済みである場合に実施する
入力情報	対象チップのマニュアル（セキュリティ機能が記載のもの）
実施条件	バイナリファイル確認用の環境が準備済みであること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. 組み込み系プログラムの開発経験のある人材が確保できない 2. 暗号に関する知識および解析経験のある人材が確保できない 3. 組み込み機器開発環境やプログラミングツールが準備できない
事前作業	公開用資料のため、記載内容を削除
確認事項	マニュアルレベルで暗号化、難読化の有無を調査し、暗号化、難読化が認められる場合、【2. 暗号化難読化の解読】に進む。 【2. 暗号化難読化の解読】では以下の暗号処理の場所、保管場所の方式に応じて鍵の抽出を行う。  （参考情報） BMW ConnectedDrive 搭載車両の TCU では、サーバーへのメッセージ送信に上図の「暗号処理を外部 MPU にオフロード」する方式を採用しており、複数車両で同じ暗号鍵を使用していた。車両1台から鍵を抽出することで、他の BMW 車両の通信の解読が可能であったことから、鍵の使いまわし状況についても本項目で確認する。 **1. 暗号化、難読化の確認** 1.1 マニュアルによる調査（1.1.7.1） 暗号化、難読化の有無を確認 1.2 目視によるバイナリファイルの調査（1.1.7.2） **2. 暗号化、難読化の解読** 2.1 EEPROM からの鍵の入手（1.1.7.3）

	2.2 RAM からの鍵の抽出（1.1.7.4） 2.3 暗号処理モジュールからの鍵の抽出（1.1.7.5） 2.1～2.3 にて鍵の抽出に成功後、暗号方式および、別の車載器において同じ鍵が使用されているかどうか確認する。 2.4 暗号化方式の確認（1.1.7.6） 2.5 別の車載器からの鍵の抽出（1.1.7.7） 暗号化、難読化が施されていない場合、「1.1.8 リバースエンジニアリング」に進む。 暗号化、難読化が解除できない場合は「1.1.4 隠れたインターフェースからの調査」に進む。
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	ファームウェア全体を暗号化し、暗号化を解除する鍵はセキュアエレメントに保存していることを確認する。 複数の車両において暗号化に用いる鍵が共用されていないことを確認する。 容易に解読されにくい暗号化方式で暗号化していることを確認する。
備考	・ Sniffing SPI data from my Current Cost EnviR http://jack-kelly.com/sniffing_spi_data_from_my_current_cost_envir ・ 組込機器の診断を紹介 http://io.cyberdefense.jp/entry/2016/05/31/%E7%B5%84%E8%BE%BC%E6%A9%9F%E5%99%A8%E3%81%AE%E8%A8%BA%E6%96%AD%E3%82%92%E7%B4%B9%E4%BB%8B_2/2 ・ STM32L4 システムメモリ保護 http://www.st.com/content/ccc/resource/sales_and_marketing/presentation/product_presentation/07/3f/d9/5d/ca/96/49/c0/19.STM32L4-Security-Memories%20Protections%20Final_JP.pdf/files/19.STM32L4-Security-Memories%20Protections%20Final_JP.pdf/jcr:content/translations/ja.19.STM32L4-Security-Memories%20Protections%20Final_JP.pdf ・ Beemer, Open Thyself! – Security vulnerabilities in BMW's ConnectedDrive https://www.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-ConnectedDrive-2540957.html ・ 電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト） http://www.cryptrec.go.jp/list/cryptrec_ciphers_list_2016.pdf

項目	記載内容
項目番号	1.1.8
項目名	リバースエンジニアリング
目的	バイナリファイルをソースコードに逆コンパイルする
実施タイミング	車両システムテスト時 （テーラリング対応：該当バイナリファイルのビルド成果物の単体テスト結果を活用しても良い）
想定実施工数（作業量）	6～10 日
前提条件	バイナリファイルを取得済みであり、バイナリファイルの保護機能がない、または、暗号・難読化を復号済みである場合に実施する
入力情報	対象チップのマニュアル（メモリマップが記載のもの）
実施条件	逆アセンブル、逆コンパイル実行環境が準備済みであること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. バイナリファイルの解析経験を有する人材が確保できない 2. 逆アセンブル、逆コンパイル実行環境が準備できない
事前作業	公開用資料のため、記載内容を削除
確認事項	以下の項目を順に実施する **1. ファイルシステムの調査（1.1.8.1）** **2. 逆アセンブラの実行（1.1.8.2）** **3. 逆コンパイラの実行（1.1.8.3）** 実施完了後、「2. 侵入」を実施する
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	非常に重要な処理部分については、リバースエンジニアリング対策（難読化など）を施す
備考	・ HEY-RAYS：逆アセンブラツール IDA pro https://www.hex-rays.com/products/ida/ ・ AccecssData：フォレンジックツール AccessData FTK Imager http://www.accessdata.com/product-download ・ ARM 向け逆アセンブラツール GNU ARM Embedded Toolchain https://launchpad.net/gcc-arm-embedded/+download ・ ARM：ARM アーキテクチャ http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.dui0471kj/pge1358786959461_00012.html ・ ルネサス：ユーザーズマニュアル ハードウェア編 : RZ/A1L https://www.renesas.com/ja-jp/document/hw-manual?hwLayerShowFlg=true&prdLayerId=186376&layerName=RZ%252FA1L&coronrService=document-prd-search&hwDocUrl=%2Fja-jp%2Fdoc%2Fproducts%2Fmpumcu%2Fdoc%2Frz%2Fr01uh0437jj0300_rz_a1l.pdf&hashKey=263bafbe81ff3b6014fc83012ee731d7

項目	記載内容
項目番号	1.2.1
項目名	アプリケーションの通信経路の調査
目的	アプリケーションがどのような I/F を通して外部と通信しているか調査する 本項目は、車両と外部がどのサービスと通して接続されているかを調査するための補助項目である。そのためセキュリティ評価そのものの項目ではないが、以降の評価項目につながる調査のため独立した項目として記載する
実施タイミング	車両システムテスト時
想定実施工数（作業量）	8 時間未満
前提条件	特になし
入力情報	車載器の操作マニュアル メーカーWeb サイト
実施条件	車載器に電源が供給され、使用可能な状態であること
外部委託条件	本項目は OEM が実施することを推奨する。
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目は、車両と外部がどのサービスと通して接続されているかを調査するための補助項目である。インターネット等の公開情報を通して車載システムの接続先を調査する。 **1. 通信経路の調査（1.2.1.1）** 1.1 オープンソースからの調査 1.2 搭乗者なしのケース 1.3 搭乗者ありのケース 本項目が終了した後、1.2.2 以降に進む。
取得エビデンス	・　調査したオープンソース情報 ・　車両 GUI 画面の出力
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	公開する必要のない情報が外部公開されていないことを確認する
備考	

項目	記載内容
項目番号	1.2.2
項目名	WiFi（車両外部）の通信傍受
目的	車外に設置された WiFi スポットと車両間の通信を傍受する
実施タイミング	車両システムテスト時 （テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）
想定実施工数（作業量）	8 時間未満
前提条件	「1.2.1 アプリケーションの通信経路の調査」で、WiFi（車両外部）通信の存在が確認されていること
入力情報	特になし
実施条件	WiFi の通信傍受に必要な環境の準備が完了していること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. WiFi ネットワークのパケット解析経験を有する人材が確保できない 2. WiFi の通信傍受に必要な PC や WiFi アダプタの準備ができない
事前作業	公開用資料のため、記載内容を削除
確認事項	WiFi 経由で外部に通信するパケットをキャプチャし、攻撃に応用できる情報が含まれているか解析する。 **1. WiFi スポットへの通信傍受** 1.2 車載器側の WiFi 設定の変更 1.2 WiFi 通信の傍受を行う **2. パケット解析** 2.1 外部へのアクセス先の確認（1.2.2.1） 外部へのアクセス先 2.2 待ち受けポートの確認（1.2.1.2） 車両側待ち受けポートの有無 2.3 SSL 暗号化の確認（1.2.2.3） SSL 暗号化の有無 2.4 認証情報の解析（1.2.2.4） 外部接続時に使用したと想定される認証情報（パスワード等） 外部接続時に送信した個人情報とみなせる情報 2.5 リプレイ、成りすまし防止情報の解析（1.2.2.5） 特定のバイト位置がシーケンシャルに変化するもの 特定のバイト位置に 128bit、256bit 等固定サイズのデータがランダムに変化するもの
取得エビデンス	・ 検証環境の全体構成を示した写真 ・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	車載から外部への通信上、機密情報を含んだ通信は暗号化する

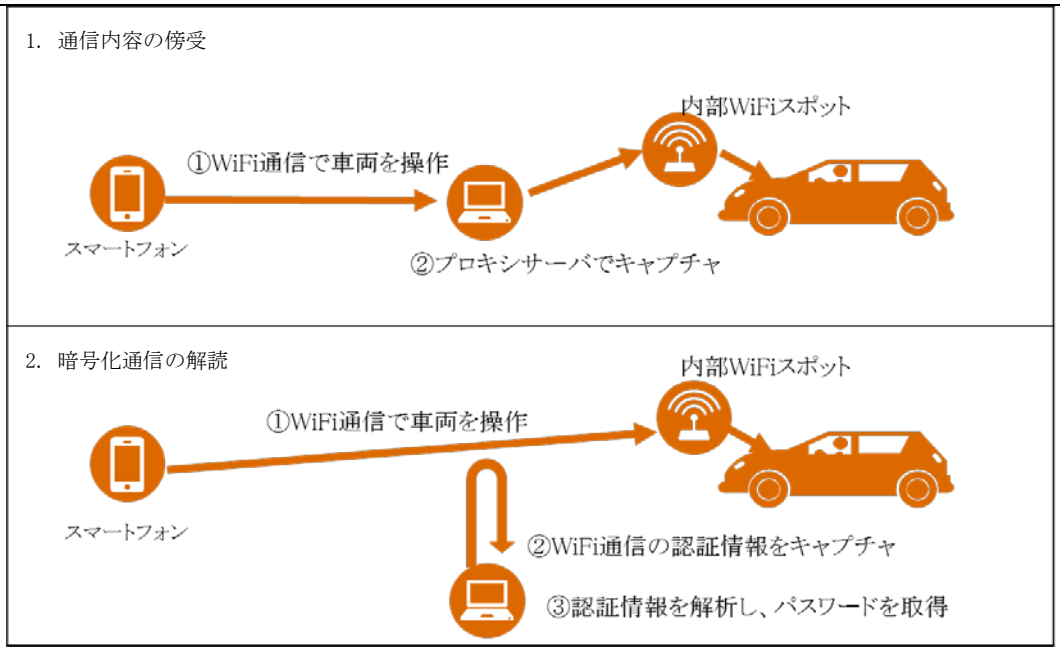
	同一処理を実行する通信メッセージであっても、リプレイ攻撃などを避けるため毎回異なるデータとなるように設計する
備考	

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>1.2.3</td></tr>
<tr><td>項目名</td><td>WiFi（車両内部）の通信傍受</td></tr>
<tr><td>目的</td><td>車両内部設置の WiFi スポットと外部との通信傍受および暗号化の解除を行う</td></tr>
<tr><td>実施タイミング</td><td>車両システムテスト時
（テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）</td></tr>
<tr><td>想定実施工数（作業量）</td><td>1～5 日</td></tr>
<tr><td>前提条件</td><td>「1.2.1 アプリケーションの通信経路の調査」で、WiFi（車両内部）通信の存在が確認されている、および、車両内部の WiFi スポットに接続可能なアプリの存在が確認されていること</td></tr>
<tr><td>入力情報</td><td>接続に必要な WiFi の SSID、およびパスワード情報（マニュアル記載のものがある場合）</td></tr>
<tr><td>実施条件</td><td>車両内部の WiFi スポットに接続できる専用アプリが用意されていること
WiFi の通信解析および通信傍受に必要な環境の準備が完了していること</td></tr>
<tr><td>外部委託条件</td><td>以下いずれかの条件に該当する場合、外部への委託を検討する
1.　WiFi ネットワークのパケット解析経験を有する人材が確保できない
2.　WiFi の通信傍受に必要な環境の準備ができない</td></tr>
<tr><td>事前作業</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>確認事項</td><td>本手順では専用アプリから車両内部の WiFi スポットに対する通信の傍受と暗号化の解除を行う。

車両内に設置された WiFi スポットは搭乗者の利便性向上のためのアクセスポイントとして利用されるほか、車両をリモート操作にも利用される。インシデント事例として WiFi のパスワード解析を攻撃の起点として利用された経緯があることから、本項目では公開情報からパスワードを推測できるか、規則性の有無についても確認する。（1.2.3.6）

<table>
<tr><th>項番</th><th>インシデント</th><th>用途</th><th>認証・暗号化方式</th><th>内容</th></tr>
<tr><td>1</td><td>Jeep Cheroke</td><td>搭乗者のスマートフォンのアクセスポイントとして利用</td><td>WPA-PSK</td><td>有償オプションとして車内 WiFi スポットが提供されており、UConnect の初回起動日時を seed 値としてパスワード（PSK）が自動生成されるため、車の購入時期が判明できればパスワードを推測することが可能であった。</td></tr>
<tr><td>2</td><td>三菱アウトランダーPHEV</td><td>車外にいる車両オーナーが車両をリモート操作するために使用</td><td>WPA-PSK</td><td>パスワード（PSK）はユーザーマニュアルに記載されており、公開されていないものの短くて単純なものであり、GPU を用いたパスワードクラッキングにより4日程度で解析可能であった。</td></tr>
</table>

なお、本評価項目においては、接続用専用アプリはスマートフォンアプリを想定している。通信の傍受にはプロキシサーバーを経由し、通信の暗号化解除には WiFi 通信傍受兼パスワード解析環境を用いる。</td></tr>
</table>



1. 通信内容の傍受

1.1 車両の操作

1.2 アクセス先ポート確認(1.2.3.1)
車両側待ち受けポートの有無

1.3 SSL 暗号化の確認(1.2.3.2)
SSL 暗号化の有無

1.4 認証情報の解析(1.2.3.3)
外部接続時に使用したと想定される認証情報(パスワード等)
外部接続時に送信した個人情報とみなせる情報

1.5 リプレイ防止情報の解析(1.2.3.4)
特定のバイト位置がシーケンシャルに変化するもの
特定のバイト位置に 128bit、256bit 等固定サイズのデータがランダムに変化するもの

2. 暗号化通信の解読

2.1 認証方式の確認(1.2.3.5)
パスワード認証使用の有無

2.2 パスワード規則性の推測(1.2.3.6)
パスワードの容易性について確認する

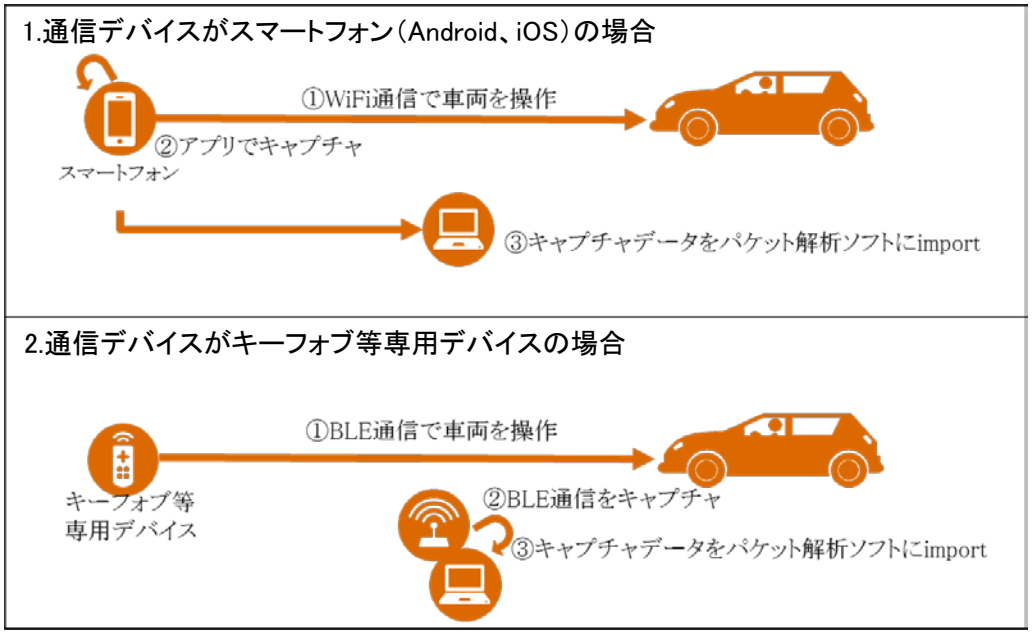
2.3 パケットキャプチャの開始

2.4 WiFi パスワードの解析(1.2.3.7)
WiFi パスワードが解析可能であることを確認する

取得エビデンス	・ 検証環境の全体構成を示した写真 ・ 実行したコマンド一覧 ・ GUI 画面の出力(スクリーンショット)

事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	車載から外部への通信上、機密データを含んだ通信は暗号化していることを確認する
備考	・ IOActive：Remote Exploitation of an Unaltered Passenger Vehicle https://ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf ・ Pentest Partners:Hacking the Mitsubishi Outlander PHEV hybrid https://www.pentestpartners.com/security-blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/

項目	記載内容
項目番号	1.2.4
項目名	Bluetooth の通信傍受
目的	車載器の Bluetooth 対応プロファイルを調査する
実施タイミング	車両システムテスト時 （テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）
想定実施工数（作業量）	8 時間未満
前提条件	「1.2.1 アプリケーションの通信経路の調査」で、Bluetooth 通信の存在が確認されていること
入力情報	特になし
実施条件	Bluetooth のプロファイル調査環境の準備が完了していること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. Bluetooth プロファイルの解析経験を有する人材が確保できない 2. Bluetooth のプロファイル調査環境が準備できない
事前作業	公開用資料のため、記載内容を削除
確認事項	Bluetooth デバイスを利用した攻撃の実現可能性を調査するため、以下の3点を確認する。 1. Bluetooth の MAC アドレスが取得可能か 2. 搭乗者の介入なしにペアリング可能か 3. どのようなプロファイルを使用しているのか **1. BluetoothMAC アドレスが検出可能なタイミングの確認（1.2.4.1）** **2. ペアリング方式の確認（1.2.4.2）** **3. Bluetooth プロファイルの調査（1.2.4.3）**
取得エビデンス	・ 検証環境の全体構成を示した写真 ・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	ユーザーの介在が不要なペアリング方式を採用していないことを確認する
備考	

項目	記載内容
項目番号	1.2.5
項目名	BluetoothLE の通信傍受
目的	BLE を利用したデバイスと車両間の通信を傍受する
実施タイミング	車両システムテスト時 （テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）
想定実施工数（作業量）	8 時間未満
前提条件	「1.2.1 アプリケーションの通信経路の調査」で、BluetoothLE（BLE）通信の存在が確認されていること
入力情報	特になし
実施条件	BLE の通信傍受に必要な環境の準備が完了していること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. BluetoothLE のパケット解析経験を有する人材が確保できない 2. Ubertooth 等 BLE の通信傍受に必要な環境が準備できない
事前作業	公開用資料のため、記載内容を削除
確認事項	車載器にアクセスする方式に応じて以下いずれかを実施 **1. スマートフォン⇔車載間の BLE 通信傍受（1.2.5.1）** **2. キーフォブ⇔車載間の BLE 通信傍受（1.2.5.2）** 
取得エビデンス	・ 検証環境の全体構成を示した写真 ・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	BLE 通信においてペアリングを必須とする、もしくは、メッセージを暗号化しておくこと
備考	・ パケット解析ソフト WireShark https://www.wireshark.org/download.html ・ Bluetooth/BLE キャプチャデバイス Ubertooth

	https://github.com/greatscottgadgets/ubertooth

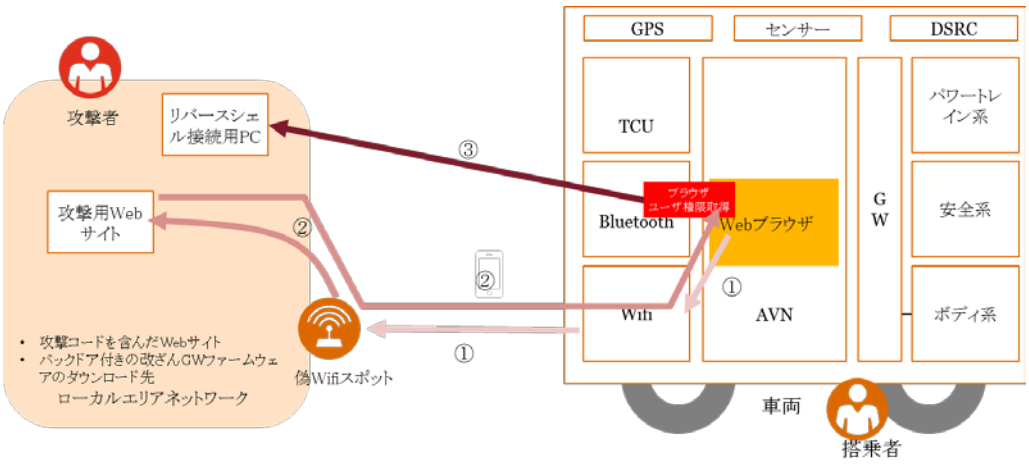
項目	記載内容
項目番号	1.2.6
項目名	TCU の通信傍受
目的	セルラーネットワークを利用した対車両間の通信を傍受する
実施タイミング	車両システムテスト時 (テーラリング対応:該当 ECU の単体テスト時の結果を活用しても良い)
想定実施工数(作業量)	1～5 日
前提条件	「1.2.1 アプリケーションの通信経路の調査」で、セルラー通信の存在が確認されていること
入力情報	TCU の IMSI
実施条件	セルラーネットワークの通信傍受に必要な環境の準備が完了していること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. セルラーネットワークの解析環境の構築経験を有する人材が確保できない 2. セルラーネットワークのパケット解析経験を有する人材が確保できない 3. セルラーネットワークの解析に必要な機材および、電波対策を施した専用室が用意できない
事前作業	公開用資料のため、記載内容を削除
確認事項	IMSI Catcher を用いたセルラーネットワークの通信傍受が各国の法執行機関により行われている。IMSI Catcher は正規の基地局(BTS)と端末(MS)の間の通信を中継し、強度の低い暗号方式(A5/0 or A5/1)に誘導させることで通信を復号する。また、海外のハッキング事例においては GSM アーキテクチャを実装したオープンソースの BTS を用いて車載器とインターネット上のテレマティクスサーバーの中間者攻撃に活用されている。(BMW ConnectedDrive)しかしながらどちらとも 2G 回線(GSM)を前提としたものであり、GSM 規格を採用していない日本ではこれらの機器は利用できない。  IMSI Catcher「Stringray」 https://en.wikipedia.org/wiki/Stingray_phone_tracker そのため本項目では国内の回線に即した 3G の検証用基地局を構築するが、通信の傍聴は行わず、セルラーネットワーク上端末(Mobile Station)を識別するための ID(IMSI)を取得することを目標とする。また、TCU のコンソールが取得済みあれば、セルラーネットワーク内の通信端末および TCU 同士で取得した IMSI 情報から通信ができるかどうか確認する。 **1. セルラーネットワーク上の通信傍受** 1.1 公開 IP アドレススキャン(1.2.6.1) 1.2 AT コマンドを利用したオーバーフロー攻撃(1.2.6.2) 1.3 AT コマンドを利用した DDoS 攻撃(1.2.6.3)
取得エビデンス	・ 検証環境の全体構成を示した写真 ・ 実行したコマンド一覧

	・ GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	車載器の IP アドレスを外部インターネットに公開していないことを確認する 1つのプログラムの機能不全が全体に影響を与えないことを確認する セルラーネットワーク通信に流れる機密情報を暗号化していることを確認する
備考	・ OpenBTS http://openbts.org

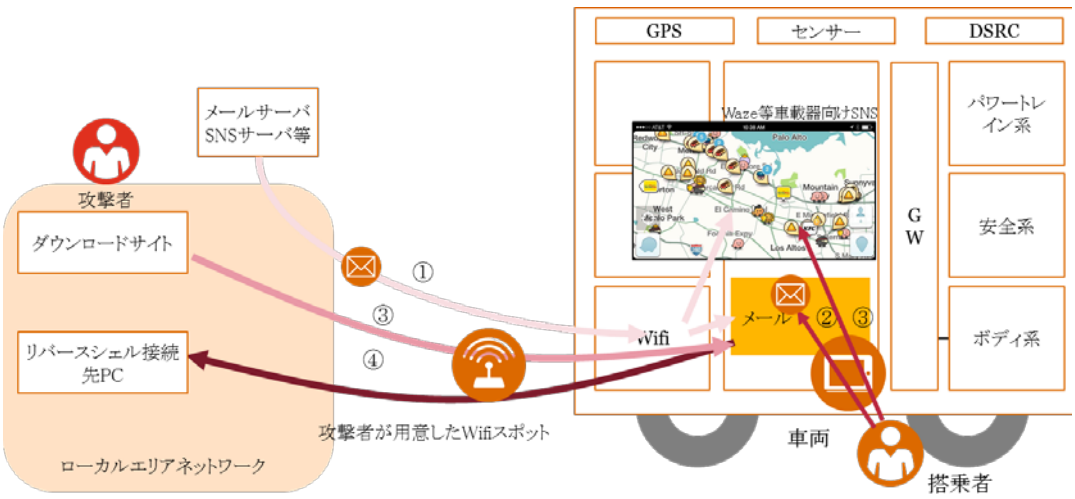
項目	記載内容
項目番号	1.2.7
項目名	使用ブラウザ、HTML エンジンの調査
目的	ブラウザあるいは HTML レンダリングエンジンの脆弱性を調べるために、フィンガープリントを取得する
実施タイミング	車両システムテスト時 （テーラリング対応：該当ソフトウェアの単体テスト結果を活用しても良い）
想定実施工数（作業量）	8 時間未満
前提条件	「1.2.1 アプリケーションの通信経路の調査」で、ブラウザもしくは HTML レンダリングエンジンの利用が確認されていること
入力情報	フィンガープリント取得サイトの URL
実施条件	車載器（AVN を想定）のブラウザがインターネット接続できること
外部委託条件	本項目は OEM が実施することを推奨する。
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目はブラウザあるいは HTML の脆弱性を突いた攻撃が実行可能か判断するために、フィンガープリントを取得しバージョン等を調査するものである。インシデント事例では、車載器ブラウザのフィンガープリントを取得し、該当 HTML レンダリングエンジン（QtWebKit）を確認した後、同エンジンの脆弱性（CVE-2011-3928）を利用して車載器に侵入した。（2016 Tesla） 参考）Tesla Model S 車載ブラウザの User-Agent 公開用資料のため、記載内容を削除 **1. ブラウザアプリの選別（1.2.7.1）** **2. バージョンの取得（1.2.7.2）**
取得エビデンス	・ GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	最新バージョンのソフトウェアを利用していることを確認する
備考	・ ブラウザフィンガープリント取得サイト：Panopticlick https://panopticlick.eff.org ・ Keen Security Lab（tencent）：FREE-FALL: HACKING TESLA FROM WIRELESS TO CAN BUS https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf

項目	記載内容
項目番号	1.2.8
項目名	CAN メッセージの通信傍受
目的	車載器から出力される CAN メッセージの通信の傍受を行う
実施タイミング	車両システムテスト時 （テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）
想定実施工数（作業量）	8 時間未満
前提条件	「1.2.1 アプリケーションの通信経路の調査」で、車載器に CAN ポートあるいは ODB Ⅱ ポートが存在すると確認されていること
入力情報	特になし
実施条件	CAN メッセージキャプチャツールが用意できていること
外部委託条件	本項目は OEM が実施することを推奨する。
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目は「1.2.1 アプリケーションの通信経路の調査」で、CAN ポートが存在しており、かつアプリケーションの操作によって CAN メッセージが発行されることが公開情報から判明している場合、同 CAN メッセージを利用した攻撃を行うための準備事項として CAN メッセージ通信傍受を行うものである。例としてスマートフォンから遠隔地に停車している車両のドアをロックする機能等、制御系に何等かのアクションを与える場合に実施する。 **1. CAN メッセージキャプチャツールの設置（1.2.8.1）** **2. CAN メッセージの送信（1.2.8.2）**
取得エビデンス	・　実行したコマンド一覧 ・　GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	特になし
備考	・　python-can-monitor https://github.com/alexandreblin/python-can-monitor ・　sparkfun ：CAN-BUS Shield https://www.sparkfun.com/products/13262

項目	記載内容
項目番号	1.2.9
項目名	アプリケーションの通信傍受
目的	外部プロキシサーバーを通して暗号前の HTTP 通信を傍受する
実施タイミング	車両システムテスト時 （テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）
想定実施工数（作業量）	1～5 日
前提条件	「1.1 HW 調査」によりコンソールを取得していること 「1.2.1 アプリケーションの通信経路の調査」で、通信アプリケーションの存在が確認されていること
入力情報	特になし
実施条件	参照先のプロキシサーバーの構築が完了していること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. WiFi ネットワークのパケット解析経験を有する人材が確保できない 2. WiFi の通信傍受に必要なプロキシサーバーの準備ができない
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目では、車載器（AVN または TCU）をプロキシ用端末に接続することで、暗号前の HTTP 通信を傍受する。また、車載器に任意の証明書をインストールできるかも確認する。 **1. プロキシ用端末の証明書のインストール（1.2.9.1）** **2. キャプチャ内容の確認（1.2.9.2）**
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	不要なサーバー証明書のインポートを制限していることを確認する 車載から外部への通信上、機密データを含んだ通信は暗号化していることを確認する
備考	・ プロキシサーバー Fiddler https://www.telerik.com/fiddler ・ 脆弱性診断ツール：Burp Suite Scanner https://portswigger.net/burp

項目	記載内容
項目番号	2.1.1
項目名	DrivebyDownload 攻撃
目的	車載器のブラウザの脆弱性を攻撃する Web サイトを構築し、同サイトに誘導させることで、攻撃が成立するか確認する
実施タイミング	車両システムテスト時 （テーラリング対応：該当ソフトウェアの単体テスト結果を活用しても良い）
想定実施工数（作業量）	1～5 日
前提条件	ネットワーク通信機能を有すること 車載器（AVN を想定）にブラウザが存在すること
入力情報	車載器のブラウザおよび HTML レンダリングエンジンのバージョン
実施条件	攻撃用の外部 WiFi スポットの準備が完了していること リバースシェル接続用 PC の準備が完了していること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. 公開された攻撃コードの中に必要なペイロードを埋め込む能力を有する人材が確保できない 2. 攻撃に必要な PC や WiFi 環境の準備ができない
事前作業	公開用資料のため、記載内容を削除
確認事項	【本評価項目の背景となる既知セキュリティインシデント】 車載器のブラウザの脆弱性を利用してリモートから車載器に侵入するケースが報告されている（2016 Tesla）。ブラウザはゼロベースで作られることはなく、汎用的な HTML レンダリングエンジンをベースにしたものが多い。そのため、PC やスマートフォン用のブラウザで発見された脆弱性が車載器にも存在し、同じ攻撃が再現できる可能性が高い。 本項目では車載器のブラウザの脆弱性を攻撃する Web サイトを構築し、同サイトに誘導させることで、攻撃が成立するか確認する。 ① 搭乗者が攻撃用 Web サイトにアクセスする ② ブラウザの脆弱性を利用した攻撃コードを送信し、リモートシェルを実行させる ③ リバースシェルにより、攻撃者は車載器のアクセス権限を取得する  本評価項目では、ブラウザの脆弱性の存在を確認後、評価実施者による操作で、車載器ブラウザから攻撃用 Web サイトにアクセスし、その結果を確認する。 **1. ブラウザの脆弱性確認（2.1.1.1）** **2. 攻撃の実施** 2.1 攻撃用 Web サイトへのアクセス（2.1.1.2）

	2.2 Web サイトから攻撃の反応確認(2.1.1.3) 攻撃コードの実行結果に応じて以下の項目に進む。 a. シェルの取得に失敗した場合、 「3.1 保護機能の回避」に進む b. リバースシェル接続用 PC からシェルが取得できた場合 「3.2 高権限の奪取」に進む c. root 権限(特権機能を有するユーザー)としてシェルが取得できた場合 「4. 目的の実行」に進む
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力(スクリーンショット)
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	「3.1 保護機能の回避」に含まれる脆弱性緩和対策が施されていることを確認する サービスが利用できるリソースを必要最低限にとどめていることを確認する
備考	・ Keen Security Lab(tencent) : FREE-FALL: HACKING TESLA FROM WIRELESS TO CAN BUS https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf ・ JVN 脆弱性情報提供データベース http://jvndb.jvn.jp/index.html ・ 脆弱性情報提供サイト Exploit-db https://www.exploit-db.com/

項目	記載内容
項目番号	2.1.2
項目名	ファイル添付攻撃
目的	車載器にリバースシェルを含んだファイルを送信し、搭乗者にリバースシェルを開かせることで車両に侵入できるかどうか確認する
実施タイミング	車両システムテスト時 （テーラリング対応：該当ソフトウェアの単体テスト結果を活用しても良い）
想定実施工数（作業量）	1～5 日
前提条件	ネットワーク通信機能を有すること AVN のバイナリファイルを入手済みであること 車載器（AVN を想定）にリバースシェルを配布する仕組み（ブラウザメール、SNS 等のアプリ）が存在すること
入力情報	車載器のマニュアル
実施条件	検証用 WiFi スポットの準備が完了していること リバースシェル接続用 PC の準備が完了していること リバースシェルダウンロード環境の準備が完了していること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. Metasploit 等、エキスプロイトツールの使用経験を有する人材が確保できない 2. 攻撃に必要な PC や WiFi 環境の準備ができない
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目は一般的な IT システムと同じ標的型攻撃を模した攻撃によって車両に侵入できるかどうか評価するものである。 具体的には Waze（ウェイズ）の様な車載器向け SNS や e メールを媒体として、リバースシェル（遠隔操作プログラム）のダウンロード先に誘導する。搭乗者がリバースシェルをダウンロードし、タッチスクリーンパネルから実行することを契機として、車両への侵入を試みるものである。 ①メール、SNS で攻撃者が用意した URL を送る、あるいはリバースシェルを添付する ②ユーザーは受信した URL をクリックし、リバースシェルをダウンロードする ③ダウンロードされたリバースシェルをユーザーが実行（タップ）する ④リバースシェルにより、攻撃者は車載器のアクセス権限を取得する  siliconbeat ：Google’s Waze expanding carpool program http://www.siliconbeat.com/2017/02/22/googles-waze-expanding-carpool-program/ 本評価項目の主要な観点は以下とおり。 ・ 攻撃者がリバースシェルを車載器側に配布することができるか ・ 搭乗者がリバースシェルをダウンロードすることができるか、 ・ ダウンロードしたリバースシェルを実行できるか

	1. 攻撃の実施 1.1 リバースシェルの配布（2.1.2.1） 1.2 リバースシェルのダウンロード（2.1.2.2） 1.3 リバースシェルの実行（2.1.2.3）
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	ユーザーインターフェースからの実行ファイルの実行を禁止していることを確認する。 製品仕様上、実行ファイルの実行が禁止できない場合、実行のための何らかの制限・認証を用意すること
備考	・ Waze https://www.waze.com/ja/

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>2.2.1</td></tr>
<tr><td>項目名</td><td>外部 WiFi への自動接続を利用した攻撃</td></tr>
<tr><td>目的</td><td>デフォルトで自動接続する WiFi 接続設定が存在するか確認する</td></tr>
<tr><td>実施タイミング</td><td>車両システムテスト時
（テーラリング対応：該当ソフトウェアの単体テスト結果を活用しても良い）</td></tr>
<tr><td>想定実施工数（作業量）</td><td>8 時間未満</td></tr>
<tr><td>前提条件</td><td>ネットワーク通信機能を有すること
AVN のバイナリファイルを入手済みであること
車載器（AVN を想定）にブラウザが存在すること</td></tr>
<tr><td>入力情報</td><td>車載器のマニュアル</td></tr>
<tr><td>実施条件</td><td>検証用 WiFi スポットの準備が完了していること</td></tr>
<tr><td>外部委託条件</td><td>以下いずれかの条件に該当する場合、外部への委託を検討する
1.　WiFi の設定方法（特に wpa_suplicant）を理解した人材が確保できない</td></tr>
<tr><td>事前作業</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>確認事項</td><td>【本評価項目の背景となる既知セキュリティインシデント】
搭乗者向けのサービスとして EV 充電スポット付近に無償の WiFi スポットを設け、車両が近づいた際、自動接続できるサービスが提供されており、それが、車載器のブラウザを攻撃用 Web サイトへ誘導する手段として利用されたケースが存在する。（2016 tesla）。

本項目ではデフォルト設定で自動接続可能な WiFi 接続機能（設定）が存在するか調査する。

①対象車両付近に WiFi スポットを設置する
②車両は自動的に WiFI スポットに接続する
 
 

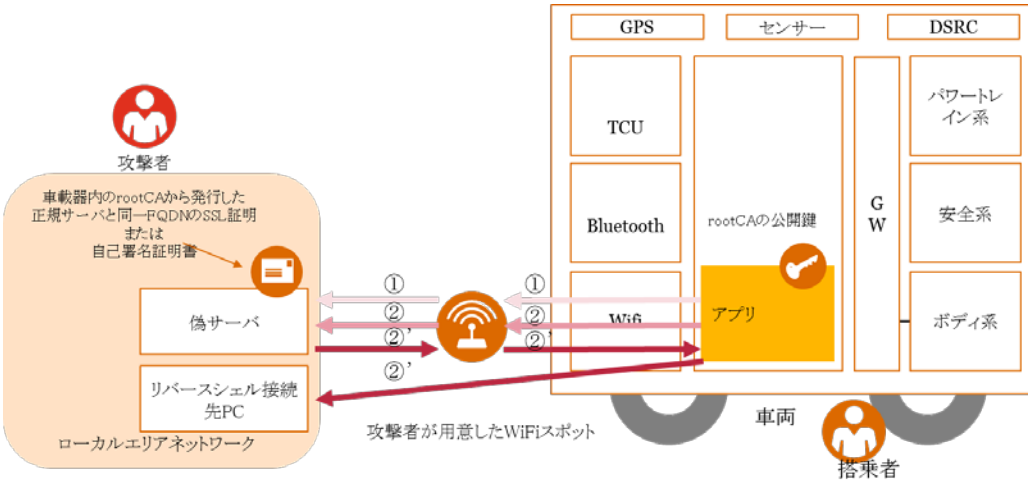
本評価項目では、マニュアルベースおよび実機の設定ファイルを調査し、自動接続設定を確認する。公衆無線 LAN として提供されている暗号化方式の内、WPA パーソナル方式を用いた自動接続が有効である場合を対象とし、同じ設定をもつ WiFi スポットを用意する。そのうえで、実際に車両機器が自動接続されるかを確認する。

公衆無線 LAN の主な暗号化・認証方式
<table>
<tr><td colspan="2">暗号化方式</td><td>WPA パーソナル</td><td colspan="4">WPA エンタープライズ</td></tr>
<tr><td colspan="2">認証方式</td><td>PSK</td><td>EAP-SIM</td><td>EAP-TTLS</td><td>EAP-TLS</td><td>PEAP</td></tr>
<tr><td rowspan="2">認証対象</td><td>サーバー側</td><td rowspan="2">認証は行われない。パスワードの入力で通信暗号化に必要な鍵がサーバー、クライアント間で自動生成される</td><td>証明書</td><td>証明書</td><td>証明書</td><td>証明書</td></tr>
<tr><td>クライアント側</td><td>SIM</td><td>証明書</td><td>パスワード</td><td>パスワード</td></tr>
</table>

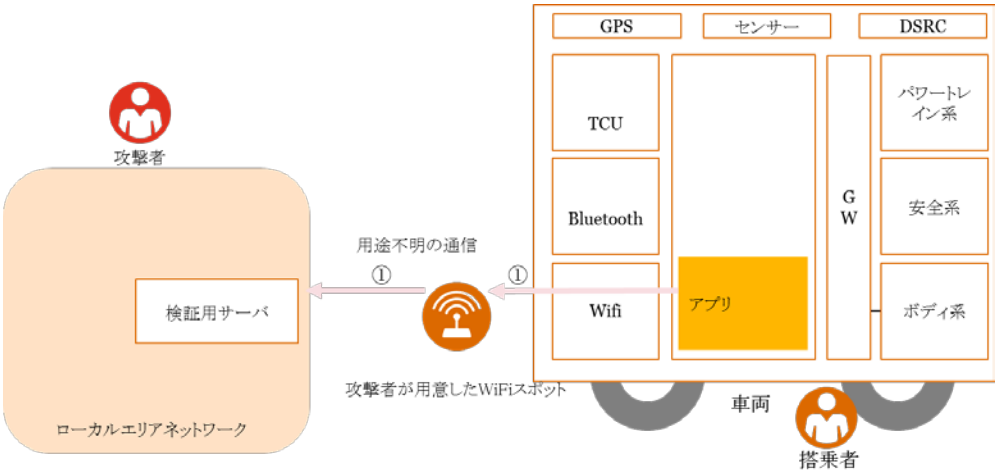
本項目は以下の流れで実施する。</td></tr>
</table>

	1. マニュアルベースの確認(2.2.1.1) **2. 設定ファイルの確認(2.2.1.2)** **3. 接続確認(2.2.1.3)**
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力(スクリーンショット)
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	認証不要、もしくは、固定パスワードの WiFi スポットには自動接続しないことを確認する 自動接続させる場合、EAP-SIM 認証を用いること
備考	・ Keen Security Lab(tencent):FREE-FALL: HACKING TESLA FROM WIRELESS TO CAN BUS https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf ・ archLinux:WPA supplicant https://wiki.archlinux.jp/index.php/WPA_supplicant

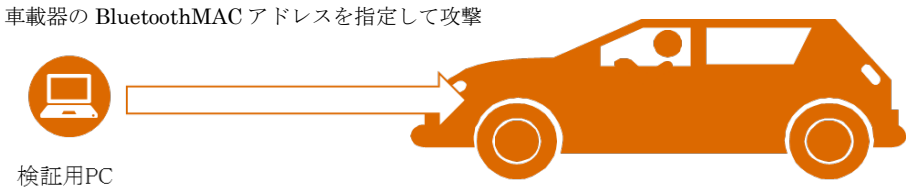
項目	記載内容
項目番号	2.2.2
項目名	偽サーバー誘導による攻撃
目的	アプリケーションを偽サーバーに誘導し、脆弱性を突く攻撃コードを実行する
実施タイミング	車両システムテスト時 （テーラリング対応：該当ソフトウェアの単体テスト結果を活用しても良い）
想定実施工数（作業量）	6～10 日
前提条件	WiFi 通信機能を有すること AVN のバイナリファイルを入手済みであること Web サーバーに接続するアプリケーションが存在すること
入力情報	車載器のマニュアル アプリケーションが接続するサーバー情報（FQDN など）
実施条件	検証用 WiFi スポットの準備が完了していること 攻撃 Web サイト環境の準備が完了していること リバースシェル接続用 PC の準備が完了していること リバースシェルダウンロード環境の準備が完了していること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. 小規模のプライベート PKI 環境の構築経験を有する人材が確保できない 2. WebView を利用したモバイルアプリケーションの開発経験を有する人材が確保できない 3. 静的コード解析の経験を有する人材が確保できない 4. 攻撃に必要な PC や WiFi 環境の準備ができない
事前作業	公開用資料のため、記載内容を削除
確認事項	【本評価項目の背景となる既知セキュリティインシデント】 発行元を確認できない SSL 証明書を用いたサーバーにアクセスする場合、PC 版ブラウザでは下図のとおり、ユーザーに注意喚起を促すため、悪意あるサーバーへの接続を防ぐことができる。しかしながらスマートフォンのアプリケーションには発行元不明の証明書であっても注意喚起を行わずに、そのまま受け入れてしまう脆弱性が多数報告されている。車載器（AVN）ではスマートフォン同様に、サードパーティ製のアプリケーションを実行しているケースが多いため、アプリケーションごとに証明書受け入れの挙動を確認する。  本項目は、ブラウザ以外でインターネット接続する車載器（主に AVN を対象）のアプリケーションを対象とする。 ブラウザ以外のアプリケーションはアクセス先が固定されている可能性が高く、攻撃サイトに誘導することが困難である。そこで、アクセス先と同一 FQDN に設定した偽サーバーを用意し、攻撃者が用意した WiFi スポットを通して当該サーバーに誘導する。偽サーバーから攻撃コードをリプライすることで、下図「②機密情報の取得」、あるいは「②’ シェル取得」を試みる。

	① アプリケーションが偽サーバーにアクセス。SSL 通信の場合、偽サーバー側が用意した SSL 証明書を用いて暗号化通信を行う ② アプリケーションは偽サーバーにパスワード等の機密情報を送信 ②’ アプリケーションに対し攻撃コードを返信。リバースシェルにより、車載器のアクセス権限を取得する  正規アプリケーションが SSL 通信を利用している場合、サーバー接続には SSL 証明書が必要である。そこで以下のいずれかのパターンで偽サーバー用の SSL 証明書を発行する。 a. 車載器にインストールされている rootCA から本物サーバーと同一 FQDN のサーバー証明書を発行してもらう b. 本物サーバーと同一 FQDN のサーバー証明書を自己署名で発行する（通称「オレオレ証明書」を発行する） 本評価項目では、本物サーバーと同一 FQDN の偽サーバー（攻撃用 Web サーバー）に誘導させ、各攻撃の結果を確認し、結果に応じて次の項目に進む。 **1. アプリケーションの脆弱性調査（2.2.2.1）** **2. 攻撃の実施（2.2.2.2 および 2.2.2.3）** 攻撃方法および攻撃コードの実行結果に応じて以下の項目に進む。 a. 認証情報 の取得に成功 「2.4.1 成りすまし攻撃」へ進む b. シェル取得に失敗 「3.1 保護機能の回避」に進む c. シェル取得に成功 「3.2 高権限の奪取」に進む d. root 権限（特権機能を有するユーザー）としてのシェル取得に成功 「4. 目的の実行」に進む
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	アプリケーションの構築にブラウザエンジンを利用する場合、脆弱性のないバージョンを利用する 証明書～ルート証明書間の信頼チェーンを正しく検証する
備考	・ セキュアプログラミング講座

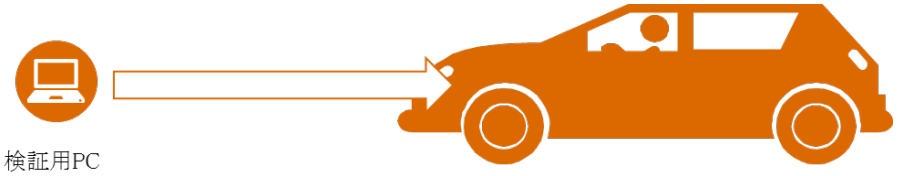
	https://www.ipa.go.jp/security/awareness/vendor/programmingv2/clanguage.html ・ Android アプリのセキュア設計・セキュアコーディングガイド www.jssec.org/dl/android_securecoding.pdf

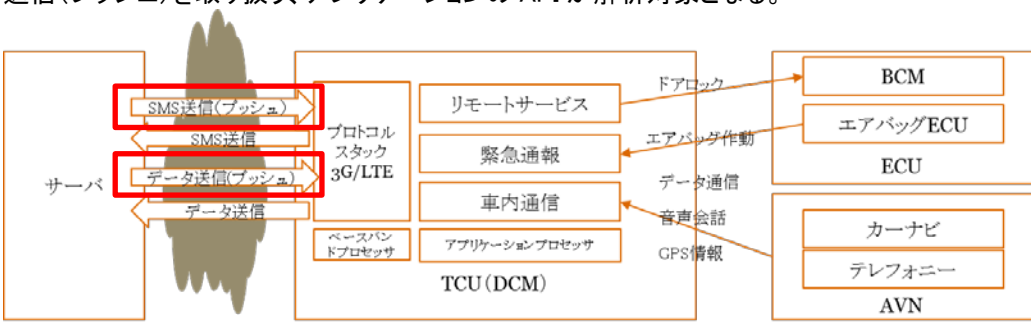
項目	記載内容
項目番号	2.2.3
項目名	残存機能を用いた攻撃
目的	通常使用しない用途不明の通信経路から情報の取得を試みる
実施タイミング	車両システムテスト時
想定実施工数(作業量)	1～5 日
前提条件	AVN のバイナリファイルを入手済みであること Web に接続するアプリケーションが存在すること
入力情報	AVN のバイナリファイル 用途不明の Web サーバー情報(FQDN など)
実施条件	検証用 WiFi スポットの準備が完了していること 検証用サーバーの準備が完了していること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. 静的コード解析の経験を有する人材が確保できない 2. 攻撃に必要な PC や WiFi 環境の準備ができない
事前作業	公開用資料のため、記載内容を削除
確認事項	【本評価項目の背景となる既知セキュリティインシデント】 セキュリティ研究者がカーナビゲーションのソースコードにハードコードされていた用途不明の通信先ドメイン(閉塞中)を買い取り、サーバーを開設したところ、通信が復旧し、ユーザー名、パスワード、VIN、位置情報等の機密情報が漏えいした事例(2017 Nissan)が存在している。 本項目は、通常の利用では使用されることのない用途不明の通信先がアプリケーション内に含まれている場合を想定し、その通信経路を復元させることでパスワード等の認証情報が漏えいしないことを確認するものである。 ①アプリケーションの用途不明の通信内容を確認するため、通信先と同一 FQDN の検証用サーバーを構築 ②アプリケーションを検証用サーバーに接続させ、通信内容を傍受し、機密情報がないか確認する  本評価項目では、用途不明の通信先サーバーを復元・アクセスを試行し、当該サーバーのアクセスログを調査することで、認証情報等が含まれているかを確認する。 **1. 用途不明の通信経路の調査(2.2.3.1)** **2. 接続の確認** 2.1 WiFi への接続(2.2.3.2)

	2.2 通信ログ確認(2.2.3.3)
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力(スクリーンショット)
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	不要なコード、機能を含めたままリリースしていないことを確認する
備考	・ DEFCON25:Driving Down the Rabbit Hole https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20presentations/DEFCON-25-Jesse-Michael-and-Mickey-Shkatov-Driving-Down-the-Rabbit-Hole.pdf

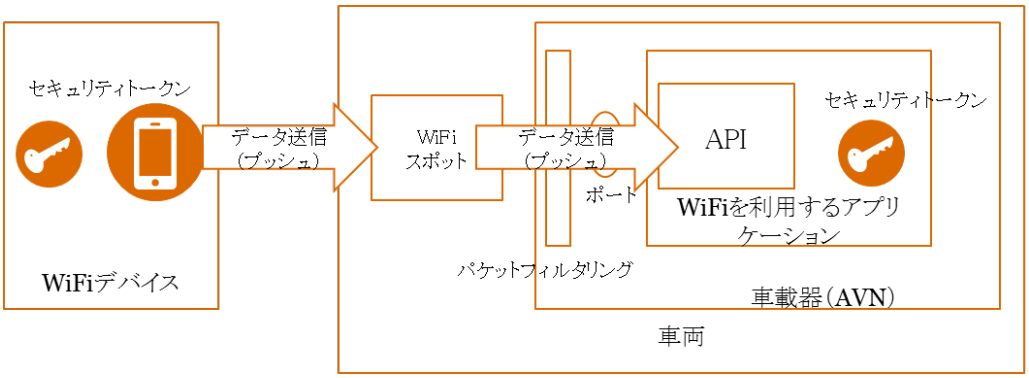
項目	記載内容
項目番号	2.3.1
項目名	Bluetooth 経由の攻撃
目的	Bluetooth の脆弱性を利用した攻撃
実施タイミング	車両システムテスト時 （テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）
想定実施工数（作業量）	1～5 日
前提条件	Bluetooth を利用しているアプリケーションが存在すること 「1.2.4 Bluetooth の通信傍受」にて Bluetooth のプロファイルとペアリング方式を調査済みであること
入力情報	AVN のバイナリファイル Bluetooth のペアリング方式
実施条件	Bluetooth 検証用環境の準備が完了していること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. 静的コード解析の経験を有する人材が確保できない 2. 脆弱性を利用した攻撃用の Bluetooth のパケットを作成可能な人材が確保できない 3. MAC アドレスの調査に必要な Ubertooth 等のキャプチャツールの準備ができない
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目は、Bluetooth プロトコルスタックの既知の脆弱性を利用した攻撃を行う。  本評価項目では、Bluetooth の MAC アドレス入手後、Bluetooth ペアリング方式が JustWork あるいは、車載器側の情報提供なしにペアリングが成立することを確認する。ペラリングが成立する場合、【2. API の脆弱性を利用した攻撃】を実施する。 **1. MAC アドレスの入手（2.3.1.1）** **2. API の脆弱性を利用した攻撃（2.3.1.2）** 「1.2.4 Bluetooth の通信傍受」によって得られたプロファイルに対し攻撃コードを作成し、攻撃を試みる。攻撃コードの実行結果に応じて以下の項目に進む。 a. 認証情報 の取得に成功 「2.4.1 成りすまし攻撃」へ進む b. シェル取得に失敗 「3.1 保護機能の回避」に進む c. シェル取得に成功 「3.2 高権限の奪取」に進む d. root 権限（特権機能を有するユーザー）としてのシェル取得に成功 「4. 目的の実行」に進む **3. プロトコルの脆弱性を利用した攻撃（2.3.1.3）** 入手した攻撃コードを利用して、検証用 PC から車載器を攻撃する。攻撃の結果に応じて以下の項目に進む。 a.DDoS 攻撃が成功 「4.2 サービスの停止」に進む

	b.機密情報の取得に成功 「2.4.1 成りすまし攻撃」へ進む c.シェルの取得に失敗 「3.1 保護機能の回避」に進む d.シェルの取得に失敗 「3.2 高権限の奪取」に進む e.root 権限の取得に成功 「4. 目的の実行」に進む
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	既知の脆弱性のないソフトウェアスタックを利用していることを確認する
備考	・ Bluetooth FTP 転送ツール https://github.com/GNOME/gnome-bluetooth/tree/master/sendto ・ Bluetooth の脆弱性「Blueborne」解説サイト https://www.armis.com/blueborne/ ・ MAC アドレス検索サイト：HWAddress https://hwaddress.com/ ・ Bluetooth/BLE キャプチャデバイス：Ubertooth ※MAC アドレスの入手に必要 https://github.com/greatscottgadgets/ubertooth ・ JVN 脆弱性情報提供データベース http://jvndb.jvn.jp/index.html ・ 脆弱性情報提供サイト Exploit-db https://www.exploit-db.com/

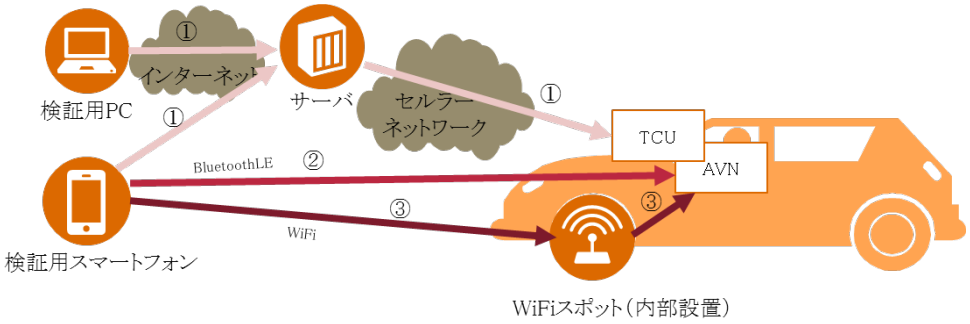
項目	記載内容
項目番号	2.3.2
項目名	BluetoothLE 経由の攻撃
目的	BluetoothLE の脆弱性を利用した攻撃
実施タイミング	車両システムテスト時 （テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）
想定実施工数（作業量）	1～5 日
前提条件	BluetoothLE を利用しているアプリケーションが存在すること 「1.2.5 BluetoothLE の通信傍受」にて BluetoothLE の通信を傍受済みであること
入力情報	AVN のバイナリファイル
実施条件	BluetoothLE 検証用環境の準備が完了していること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. 静的コード解析の経験を有する人材が確保できない 2. 脆弱性を利用した攻撃用の GATT のパケットを作成可能な人材が確保できない 3. MAC アドレスの調査に必要な Ubertooth 等のキャプチャツールの準備ができない
事前準備	公開用資料のため、記載内容を削除
確認事項	本項目は、Bluetooth プロトコルスタックの既知の脆弱性を利用した攻撃を行う。 車載器の BluetoothMAC アドレスを指定して攻撃  本評価項目では、Bluetooth の MAC アドレス入手後、【2. API の脆弱性を利用した攻撃】以降を実施する。 **1. MAC アドレスの入手（2.3.2.1）** **2. API の脆弱性を利用した攻撃（2.3.2.2）** **3. プロトコルの脆弱性を利用した攻撃（2.3.2.3）**
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	受信するデータに制限を設けていることを確認する
備考	・ MAC アドレス検索サイト：HWAddress https://hwaddress.com/ ・ hcitool and gatttool example https://github.com/pcborenstein/bluezDoc/wiki/hcitool-and-gatttool-example ・ BlueZ D-Bus GATT API description https://git.kernel.org/pub/scm/bluetooth/bluez.git/tree/doc/gatt-api.txt

項目	記載内容
項目番号	2.3.3
項目名	TCU 経由の攻撃
目的	TCU の脆弱性を利用した攻撃
実施タイミング	車両システムテスト時
想定実施工数(作業量)	6～10 日
前提条件	TCU のバイナリが取得済みであること 車載器同士で SMS が送受信可能である、またはセルラーネットワーク内の通信端末(PC、モバイル端末等)から車載器に通信可能であること
入力情報	車載器の IMSI TCU バイナリファイル
実施条件	検証用無線基地局の準備が完了していること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. 静的コード解析の経験を有する人材が確保できない 2. セルラーネットワークの解析環境の構築経験を有する人材が確保できない 3. セルラーネットワークのパケット解析経験を有する人材が確保できない 4. セルラーネットワークの解析に必要な機材および、電波対策を施した専用室が用意できない
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目は TCU の API を解析することにより、外部から直接侵入できるかどうか確認するものである。TCU は通信装置としての役割のほか、内部に独立したアプリケーションが存在するため、アプリケーションの役割を理解した上でソースコードの解析を行う必要がある。 以下に TCU の想定モデル図を示す。下図においては赤枠で囲った SMS 送信(プッシュ)、データ送信(プッシュ)を取り扱う、アプリケーションの API が解析対象となる。  本評価項目では、攻撃コードを含む SMS を TCU に対して送付する。また機器自体に既知の脆弱性があり攻撃コードが公開されている場合は、それを実行する。 **1. TCU 側サービス API の脆弱性を利用した攻撃(2.3.3.1)** セルラーネットワーク内の通信端末(検証用 PC)あるいは別の車載器から対象車載器に対し攻撃コードを送信する。攻撃の結果に応じて各項目へ進む。 a.DDoS 攻撃が成功した場合 「4.2 サービスの停止」に進む b 機密情報の取得に成功した場合 「2.4.1 成りすまし攻撃」へ進む c. シェルの取得に失敗した場合 「3.1 保護機能の回避」に進む d. リバースシェル接続用 PC からシェルが取得できた場合 「3.2 高権限の奪取」に進む

	e. root 権限（特権機能を有するユーザー）としてシェルが取得できた場合 「4. 目的の実行」に進む 攻撃に失敗した場合、成りすまし及びリプレイ防止対策が施されている可能性があるため、「2.4.1 成りすまし攻撃」、「2.4.2 リプレイ攻撃」に進む。 **2. 機器の脆弱性を利用した攻撃（2.3.3.2）** TCU にリモートから実行可能な既知の脆弱性がある場合、攻撃コードを作成し実行する。以下は過去に公開された TCU の脆弱性であり、類似の脆弱性があるか確認する。
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	受信するデータに制限を設けていることを確認する 既知の脆弱性が存在する機器を使用しないこと
備考	・ JVN 脆弱性情報提供データベース http://jvndb.jvn.jp/index.html ・ 脆弱性情報提供サイト Exploit-db https://www.exploit-db.com/ ・ DEFCON25：Driving Down the Rabbit Hole https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20presentations/DEFCON-25-Jesse-Michael-and-Mickey-Shkatov-Driving-Down-the-Rabbit-Hole.pdf

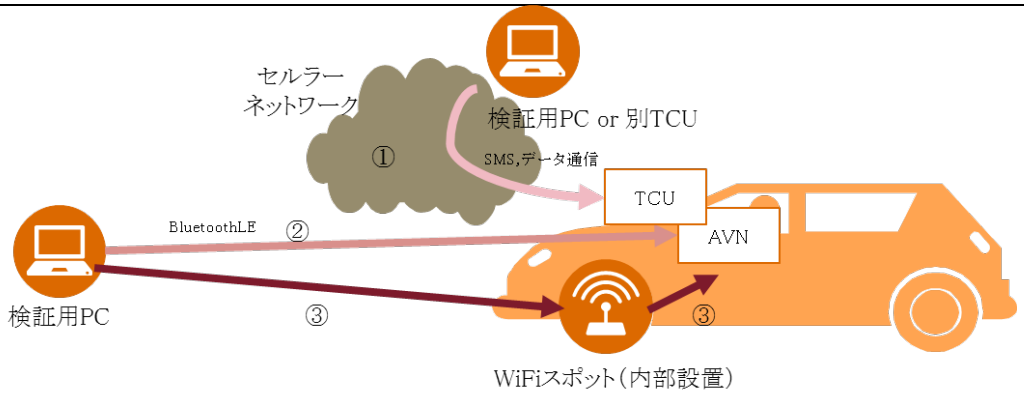
項目	記載内容
項目番号	2.3.4
項目名	WiFi（内部設置）経由の攻撃
目的	車両内部に設置された WiFi スポットの脆弱性を利用した攻撃
実施タイミング	車両システムテスト時 （テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）
想定実施工数（作業量）	1～5 日
前提条件	「1.2.3 WiFi（車両内部）の通信傍受」において WiFi の SSID、パスワードが解析済みであること
入力情報	特になし
実施条件	リバースシェル接続用 PC の準備が完了していること WiFi デバイス（専用アプリをインストールしたスマートフォン）の準備が完了していること スマートフォンのフォレンジック環境の準備が完了していること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. スマートフォンアプリの静的コード解析の経験を有する人材が確保できない 2. 攻撃に必要な PC や WiFi 環境の準備ができない
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目は車両内部に設置された WiFi スポットを通じて外部デバイスと通信するアプリケーションの API を解析することにより、外部から車載器へ侵入できるかどうか確認するものである。 以下に WiFi（内部設置）のモデル図を示す。 ①認証情報がハードコードされせるているか ②どのファイルを用いて WiFi デバイスの認証を行っているか ③リプレイ対策への規則性の有無  本評価項目では、車載器側に待ち受けポートが存在する場合、ログインを実施する。ログインが失敗した場合、ソースコードの解析を行い、脆弱なコードがないか確認する。 **1. 公開ポートからのログイン（2.3.4.1）** ログインに成功した場合、ユーザーの権限に応じた項目へ進む。 a. 一般ユーザーの場合 「3.2 高権限の奪取」に進む b. root 権限の場合 「4. 目的の実行」に進む **2. API の脆弱性を利用した攻撃（2.3.4.1、2.3.4.2）** 攻撃に成功した場合、結果に応じた項目へ進む a. DDoS 攻撃が成功した場合

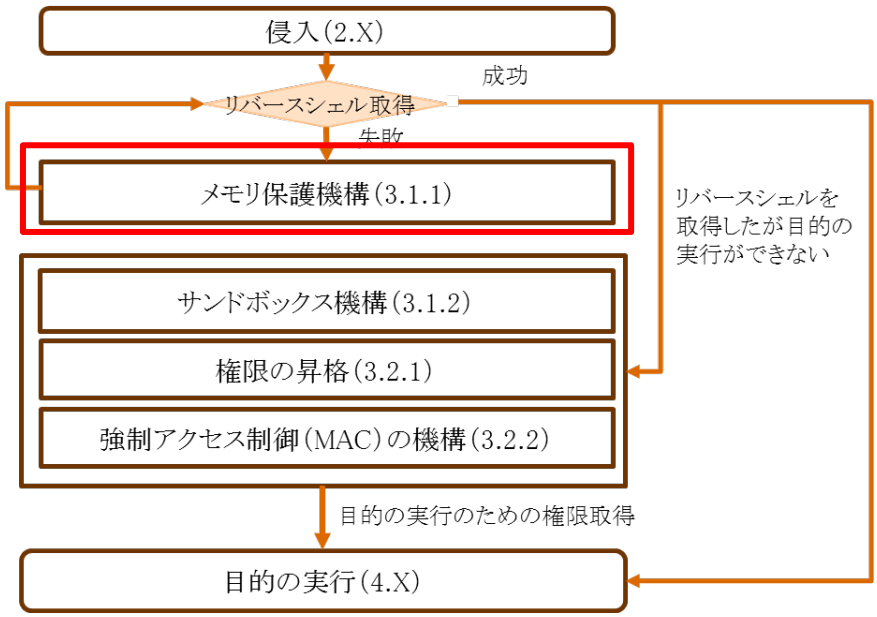
	「4.2 サービスの停止」に進む b. 機密情報の取得に成功した場合 「2.4.1 成りすまし攻撃」へ進む c. リバースシェルの取得に失敗した場合 「3.1 保護機能の回避」に進む d. 一般ユーザーとしてリバースシェルが取得できた場合 「3.2 高権限の奪取」に進む e. root 権限としてリバースシェルが取得できた場合 「4. 目的の実行」に進む
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット）
事前作業時実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	受信するデータに制限を設けていることを確認する クライアントが車載へ通信する場合、端末に対し、多要素（端末認証、ユーザー認証等）で認証する
備考	・ apktool https://ibotpeaches.github.io/Apktool/install/ ・ Dex2jar https://sourceforge.net/projects/dex2jar/

項目	記載内容
項目番号	2.4.1
項目名	成りすまし攻撃
目的	入手したユーザーID、パスワードを用いて正規ユーザーと同じ操作が実行できるか確認する。
実施タイミング	車両システムテスト時 （テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）
想定実施工数（作業量）	1～5 日
前提条件	認証情報と想定されるデータを取得済みであること
入力情報	各種認証情報（想定されるもの）
実施条件	検証用のスマートフォン、PC の準備が完了していること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. メッセージ認証（HMAC、CMAC 等）やデジタル署名に関する知識を有する人材が確保できない
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目はパケットキャプチャ等により傍受した認証情報（厳密には認証情報であると想定されるもの）を用いて、正規ユーザーと同じ操作が実行できるか確認する。 攻撃経路は以下3パターンを想定しており、攻撃者が用意した PC あるいはスマートフォンから正規アプリケーションを用いて車両の操作を行う。 なお、本項目は「2. 侵入」の評価項目の一部であるが、侵入と同時に「4. 目的の実行」の内容を含むため、本項目の評価結果を「4. 目的の実行」の項目で使うことはない。 ① 傍受した認証情報を用いてサーバーにアクセスし、車両に対し操作を行う ② 傍受した認証情報を用いて BluetoothLE 経由で、車両に対し操作を行う ③ 傍受した認証情報を用いて WiFi 経由で、車両に対し操作を行う  本評価項目では、「1.2 SW 調査」で通信傍受した認証情報を用いてサーバーに接続し、期待される操作が実行できるか確認する。 **1. 成りすまし攻撃** 1.1. サーバーを経由した TCU への成りすまし攻撃（2.4.1.1） 1.2. BluetoothLE からの成りすまし攻撃（2.4.1.2） 1.3. WiFi（内部設置）からの成りすまし攻撃（2.4.1.3） 傍受した認証情報を利用して車両を操作できない場合、成りすまし対策が車両、スマートフォン、サーバー間で取られていることを確認する。 **2.成りすまし攻撃の対策確認（2.4.1.4）**

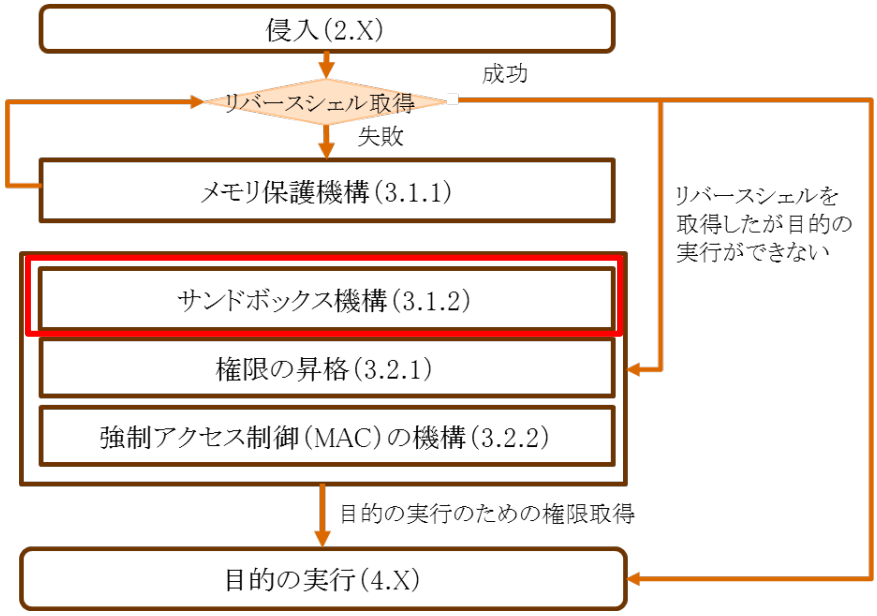
	なお、以下の項目は本項目の評価対処外とする WiFi（外部設置）：外部から車両に対するプッシュ型通信を行う通信経路を検証対象とするため除外 Bluetooth：ペアリング（暗号化）が前提であり、通信傍受ができないため除外
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット） ・ 同一のサービスに利用される複数車両の暗号鍵の比較結果
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	クライアントが車載へ通信する場合、デバイスに対し、多要素（デバイス認証、ユーザー認証等）で認証する サーバーの成りすましによる攻撃を防ぐため、共通する鍵情報は車両ごとに一意のものを使用する
備考	

項目	記載内容
項目番号	2.4.2
項目名	リプレイ攻撃
目的	命令コードを含んだパケットデータを受信および再送すること同じ操作が複数回実行されるか確認する
実施タイミング	車両システムテスト時 （テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）
想定実施工数（作業量）	6～10 日
前提条件	（TCU 関係の評価） ・ TCU のバイナリ取得により TCU のメッセージの解析が可能であること ・ 車載器同士で SMS が送受信可能である、またはセルラーネットワーク内の通信端末（PC、モバイル端末等）から車載器に通信可能であること （WiFi 関係の評価） ・ WiFi デバイスと WiFi（内部設置）の間で SSL による暗号化を行っていないこと ・ 「1.2.3 WiFi（車両内部）の通信傍受」において、通信傍受が成功していること （Bluetooth 関係の評価） ・ BluetoothLE デバイスと車両の間でペアリングを行っていない事 ・ 「1.2.3 WiFi（車両内部）の通信傍受」において WiFi の SSID、パスワードが解析済みであること
入力情報	車載器の IMSI BluetoothMAC アドレス TCU のバイナリファイル
実施条件	検証用の PC、WiFi、Bluetooth 通信環境の準備が完了していること
外部委託作業	以下いずれかの条件に該当する場合、外部への委託を検討する 1. WiFi のパケット解析経験を有する人材が確保できない 2. GATT のパケットを作成可能な人材が確保できない 3. 攻撃に必要な PC や WiFi、Bluetooth 環境の準備ができない
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目は命令コードを含んだパケットデータを受信および再送することで、複数回同じ操作が実行されるか確認する。 攻撃経路は以下 3 パターンを想定する。攻撃者が用意した PC あるいは別 TCU を用いてパケットデータを再送する。 なお、本項目は「2. 侵入」の検証項目の一部であるが、侵入と同時に「4. 目的の実行」の内容を含むため、本項目の評価結果を「4. 目的の実行」の項目で使うことはない。 ① サーバーから TCU に送信されるメッセージを検証用 PC からリプレイすることで車両の操作を行う ② BLE デバイスから車両に送信されるパケットを検証用 PC からリプレイすることで車両の操作を行う ③ スマートフォンから車両（WiFi 内部設置）に送信されるパケットを検証用 PC からリプレイすることで車両の操作を行う

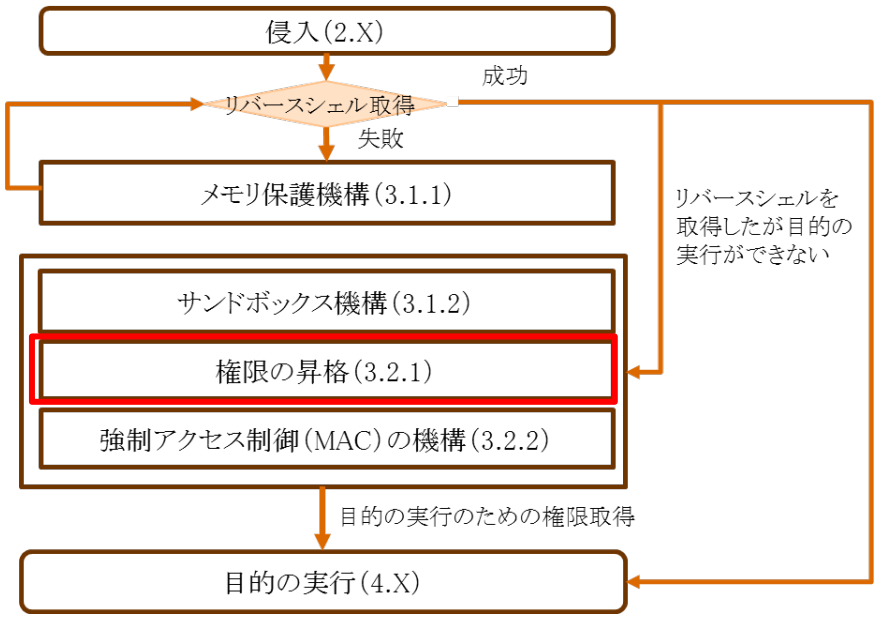
	 本評価項目では、「1.2 SW 調査」で傍受したメッセージを再送することで、期待される操作が実行できるか確認する。 **1. リプレイ攻撃** 1.1 サーバー⇒TCU パケットをリプレイ(2.4.2.1) 1.2 BLE デバイス⇒車両パケットをリプレイ(2.4.2.2) 1.3 WiFi デバイス⇒車両(WiFi 内部設置)パケットをリプレイ(2.4.2.3) リプレイ攻撃が失敗する場合、リプレイ対策が車両、BLE デバイス(検証用 PC)、サーバー間で取られているかどうか確認する。 **2. リプレイ攻撃への対策確認(2.4.2.4)** リプレイ攻撃対策の実装方法をコード解析することにより確認する。 なお、以下の項目は本項目の評価対処外とする WiFi(外部設置)外部から車両へのプッシュ型通信を行う通信経路を検証対象とするため除外 Bluetooth:プッシュ型であるが、ペアリング(暗号化)が前提。通信傍受ができないため除外
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力(スクリーンショット)
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	第3者がキャプチャしたメッセージを再送しても同じ操作が実行されないよう対策を施すこと
備考	・ hcitool and gatttool example https://github.com/pcborenstein/bluezDoc/wiki/hcitool-and-gatttool-example

項目	記載内容
項目番号	3.1.1
項目名	コード実行防止機能の回避
目的	脆弱性を利用した攻撃に対する保護機能が有効であるかどうか確認する
実施タイミング	車両システムテスト時 （テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）
想定実施工数（作業量）	6～10 日
前提条件	「2. 侵入」において脆弱性を利用した攻撃を実施したが、リバースシェルの取得には失敗した場合
入力情報	チップの型番
実施条件	対象デバイス上でコンソールを取得できており、コマンド操作が可能であること 対象チップのクロスコンパイラ環境の準備が完了していること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1.　対象 OS カーネルのセキュリティ実装に関する知識を有する人材が確保できない
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目はメモリの保護機能が有効でペイロードの実行に失敗した原因を調査し、既知脆弱性がある場合には保護機能を回避する手段がないか調査するものである。 Linux 環境には攻撃を受けても、その攻撃を緩和させるための多層構造の防御機構を採用している。本項目では最初の防御機構となるメモリ保護機構を調査する。  Linux 環境における保護対象となるメモリ区分と攻撃防止対策は以下のとおりである。 <table><tr><th>メモリ区分</th><th>スタック領域</th><th>MMAP 領域 共有ライブラリ</th><th>ヒープ領域/vDSO</th><th>実行ファイル</th></tr><tr><td>保護/緩和方式</td><td colspan="3">NX ビット ASLR SSP</td><td>PIE RELRO-FULL</td></tr></table>

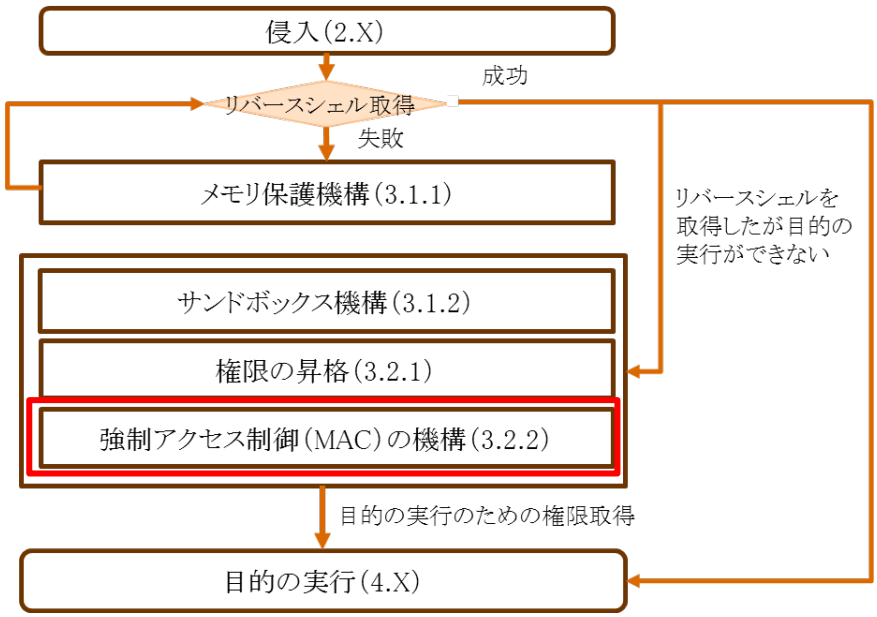
	本評価項目では、各メモリ保護機能の実装状態を確認するほか、保護機能を回避可能な既知脆弱性がないか調査を行う。 **1.メモリ保護機能の確認** 1.1 NX ビットの確認(3.1.1.1) 1.2 ASLR の確認(3.1.1.2) 1.3 SSP の確認(3.1.1.3) 1.4 PIE の確認(3.1.1.4) 1.5 RELRO-FULL の確認(3.1.1.5) **2. 既知の脆弱性を利用したデータ実行保護機能の回避(3.1.1.6)** 【ファイルフォーマットについて】 確認方法は実行バイナリにより異なるが、本項目では ARM 環境の Linux、UNIX における標準 ELF フォーマットを想定する。 参考)ARM 環境における実行ファイルフォーマットの調査方法 公開用資料のため、記載内容hを削除
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力(スクリーンショット)
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	メモリ領域に応じた脆弱性緩和機能を有効にする
備考	・ ARM アーキテクチャ http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.dui0471kj/pge1358786959461_00012.html ・ GNU ARM Embedded Toolchain https://launchpad.net/gcc-arm-embedded/+download ・ Anatomy of a Program in Memory https://manybutfinite.com/post/anatomy-of-a-program-in-memory/

項目	記載内容
項目番号	3.1.2
項目名	サンドボックス機構の回避
目的	脆弱性を利用した攻撃に対する無効化機能（サンドボックス）が有効であるかどうか確認する
実施タイミング	車両システムテスト時 （テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）
想定実施工数（作業量）	6～10 日
前提条件	「2. 侵入」において脆弱性を利用した攻撃を実施したが、シェルの取得には失敗した場合 または 「2. 侵入」において脆弱性を利用した攻撃を実施し、シェルの取得には成功しているが、「4.目的の実行」のための権限が不足している場合
入力情報	特になし
実施条件	対象デバイス上でコンソールを取得できており、コマンド操作が可能であること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1.　対象 OS カーネルのセキュリティ実装に関する知識を有する人材が確保できない
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目はペイロードの実行に失敗した原因を調査し、既知脆弱性がある場合にはペイロード実行が失敗した原因（保護機能）を回避できる手段がないか調査するものである。 本項目では、システムの多層構造の防御機構の内、サンドボックス機構を確認する。前項目のメモリ保護機能を突破し、リバースシェルの取得に成功した状態を想定する。  本評価項目では、サンドボックス実装として、以下2つの実装状況を調査するほか、実装されているサンドボックス機構を確認し、既知の回避策がないか調査を行う。 ・　ファイルシステムによるアクセス制御 ・　システムコールによるアクセス制限 **1. ファイルシステムの制限の確認（3.1.2.1）** **2. システムコールのの制限の確認（3.1.2.2）** **3. 既知の脆弱性を利用したサンドボックスの回避（3.1.2.3）**

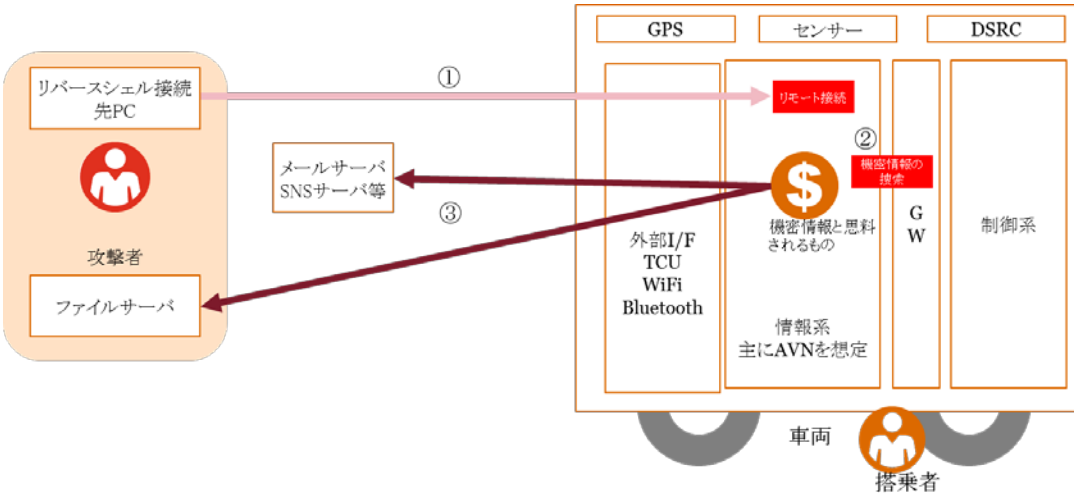
取得エビデンス	・　実行したコマンド一覧 ・　GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	アプリケーション/プログラム事に利用できるリソースを必要最低限にとどめていることを確認する
備考	

項目	記載内容
項目番号	3.2.1
項目名	既知の攻撃を試行することによる権限昇格
目的	既知の脆弱性を用いて目的の実行に必要な権限に昇格する（JailBreak 等の実施）
実施タイミング	車両システムテスト時 （テーラリング対応：該当 ECU の単体テスト時の結果を活用しても良い）
想定実施工数（作業量）	1～5 日
前提条件	「2. 侵入」において、シェル取得には成功しているが、「4.目的の実行」のための権限が不足している場合
入力情報	OS、カーネルのバージョン情報
実施条件	対象デバイス上でコンソールを取得できており、コマンド操作が可能であること ダウンロードサーバーの準備が完了していること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1.　公開された攻撃コードの中に必要なペイロードを埋め込む能力を有する人材が確保できない
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目は「4. 目的の実行」に必要な権限が不足する場合に実行するものである。 攻撃コードの実行が成立した場合であっても、システムリソースの利用が制限され目的の実行ができない可能性がある。本項目では既知の脆弱性を利用したローカルエクスプロイトにより特権ユーザーである root 権限に昇格することを目標とする。  本評価項目では、root 権限の取得が可能な、既知の回避策の有無を調査し、存在する場合は攻撃を試みる。 **1 root 権限の昇格（3.2.1.1）**
取得エビデンス	・　実行したコマンド一覧 ・　GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	既知の脆弱性がないバージョンの OS やミドルウェアを利用していることを確認する
備考	・　JVN 脆弱性情報提供データベース

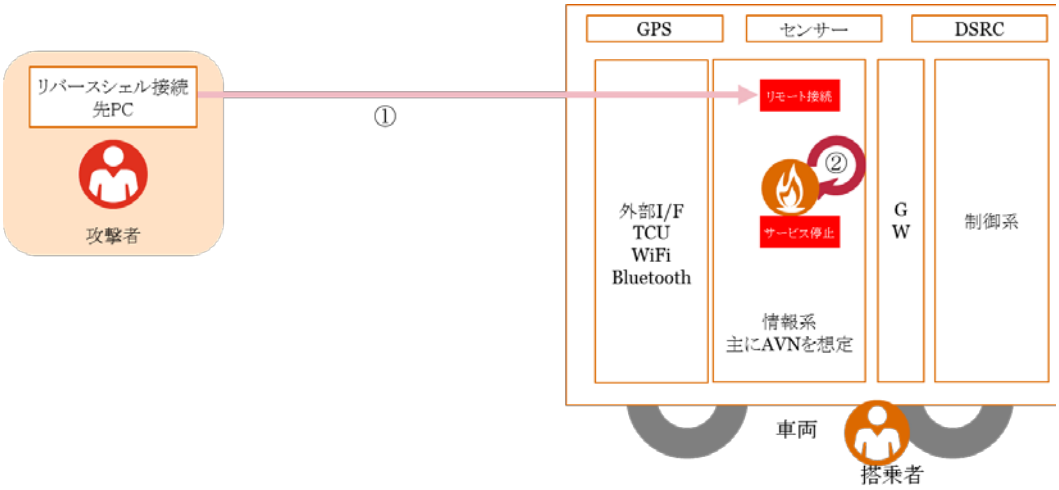
	http://jvndb.jvn.jp/index.html ・ 脆弱性情報提供サイト Exploit-db https://www.exploit-db.com/

項目	記載内容
項目番号	3.2.2
項目名	強制アクセス制御(MAC)の機構の回避
目的	強制アクセス制御が有効であるかどうか確認する
実施タイミング	車両システムテスト時 (テーラリング対応:該当 ECU の単体テスト時の結果を活用しても良い)
想定実施工数(作業量)	6～10 日
前提条件	「2. 侵入」において、シェルの取得には成功しているが、「4.目的の実行」のための権限が不足している場合
入力情報	OS、カーネルのバージョン情報
実施条件	対象デバイス上でコンソールを取得できており、コマンド操作が可能であること ダウンロードサーバーの準備が完了していること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. 公開された攻撃コードの中に必要なペイロードを埋め込む能力を有する人材が確保できない 2. OS カーネルに対する深い知識を有する人材が確保できない
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目は特権ユーザーを取得できた場合であっても、「4. 目的の実行」に必要なリソース、プログラムへのアクセスが制限されている場合に実行する。 想定する環境としては、強制アクセス制御(MAC)が適用された環境下で特権ユーザーであってもリソース制限を受け、目的の実行を達成できない場合が相当する。強制アクセス制御の実装は Linux の場合、SMACK、SE Linux 、AppArmor、TOMOYO Linux 等が存在する。Automotive Grade Linux は SMACK、Android は SE Linux、Tesla においては AppArmor を採用している。  本評価項目では、強制アクセス制御設定の有無を判断し、既知の回避策があれば攻撃を試みる。 **1. 強制アクセス制御の確認(3.2.2.1)** **2. 強制アクセス制御の回避(3.2.2.2)**
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力(スクリーンショット)
事前作業実施例	公開用資料のため、記載内容を削除

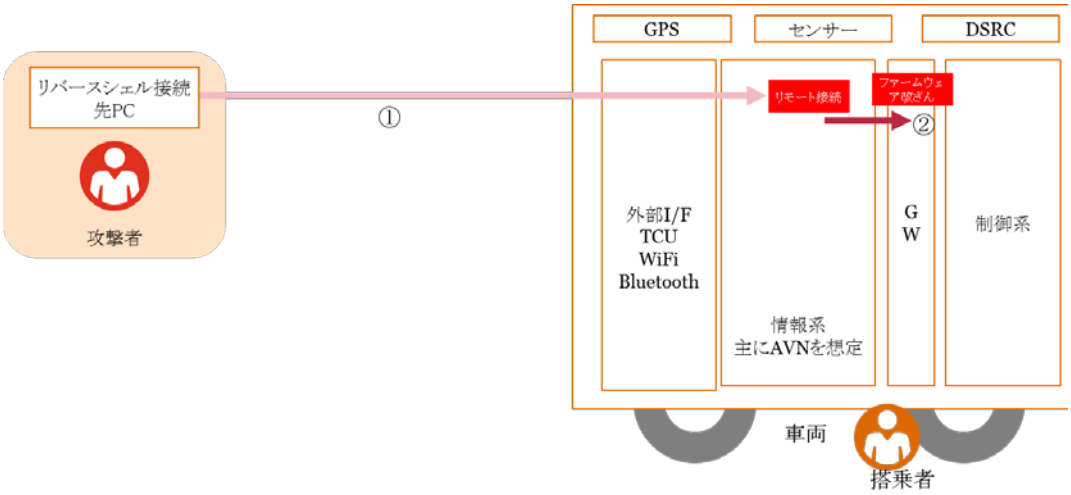
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	強制アクセス制御が有効であることを確認する 既知の脆弱性がないバージョンの OS やミドルウェアを利用していることを確認する
備考	・ JVN 脆弱性情報提供データベース http://jvndb.jvn.jp/index.html ・ 脆弱性情報提供サイト Exploit-db https://www.exploit-db.com/

項目	記載内容
項目番号	4.1.1
項目名	機密情報の漏えい（外部送信）
目的	車載器内に保管された機密情報を外部に送信できるかどうか確認する
実施タイミング	車両システムテスト時
想定実施工数（作業量）	1～5 日
前提条件	「3.2 高権限の奪取」に成功している、あるいは「2.侵入」時に root 権限を取得済みである
入力情報	アップロードサーバーの URL
実施条件	フォレンジック用 PC の準備が完了していること 対象車載器に電源が供給され、使用可能な状態であること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1.　デジタルフォレンジックの経験を有する人材が確保できない 2.　外部へデータを送信するためのファイルサーバー等の環境を準備することができない
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目は、攻撃者が車載器へ侵入できた場合に、機密情報を外部に送信できるか確認するものである。 ①　「2. 侵入」「3. 権限昇格」で車載器（主に AVN を想定）にリモート接続 ②　機密情報を捜索 ③　車載器にインストールされたソーシャルアプリまたはファイルサーバーを用いて機密情報を外部に送信  本評価項目では、車載器（AVN を想定）のバイナリファイルから機密情報と想定されるデータを抽出し（4.1.1.1）、外部へ送信する（4.1.1.2）。 外部へ送信する方法はアプリに SNS やメール、オンラインストレージが存在すればそれを優先的に使用する。存在しない場合、アップロード用のファイルサーバーを構築し、WiFi 経由でアップロードすることを試みる。 **1. 機密情報の調査（4.1.1.1）** **2. 外部へのデータ送信（4.1.1.2）**
取得エビデンス	・　実行したコマンド一覧 ・　GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除

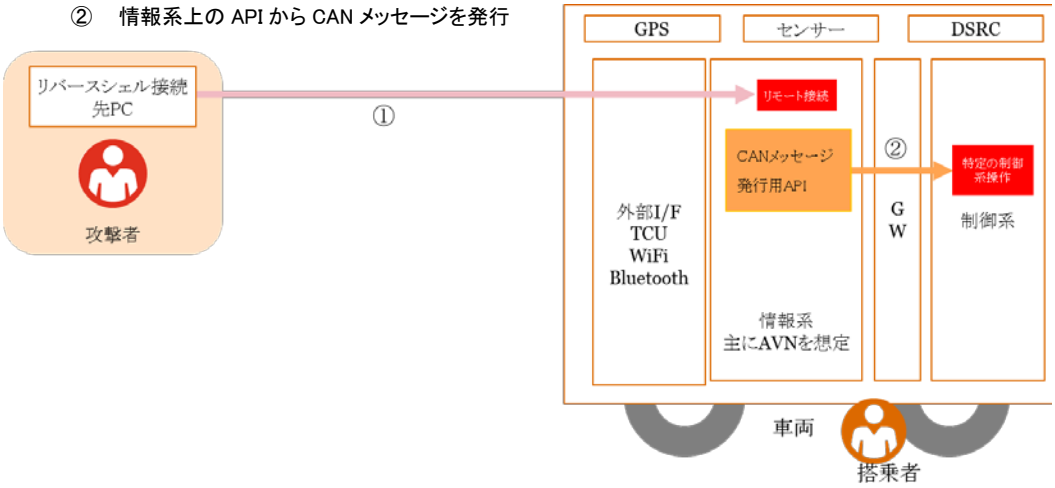
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	機密情報は暗号化を施し、容易に取り出せないことを確認する パケットフィルタリング機能を用いて外部および内部からのアクセスを制限することを確認する
備考	・ フォレンジックツール encase www.guidancesoftware.com/encase-forensic ・ データベース閲覧ソフト popSQLite https://www.eonet.ne.jp/~pup/software.html ・ FTP サーバーの設定 : Vsftpd https://www.server-world.info/query?os=Ubuntu_16.04&p=ftp

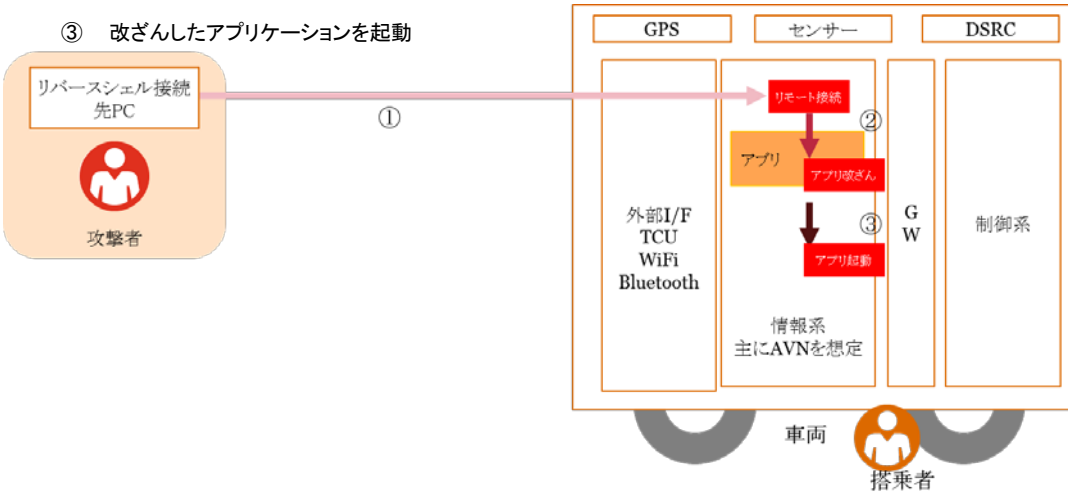
項目	記載内容
項目番号	4.2.1
項目名	車両のサービス(機能)の停止
目的	車両サービスを停止できるか確認する
実施タイミング	車両システムテスト時
想定実施工数(作業量)	8 時間未満
前提条件	「3.2 高権限の奪取」に成功している、あるいは「2.侵入」時に root 権限を取得済みである
入力情報	車載器上の OS および実行可能なコマンドに関する情報
実施条件	対象車載器に電源が供給され、使用可能な状態であること
外部委託条件	本項目は OEM が実施することを推奨する。 なお、実施にあたり Linux OS のコマンドを理解していることを前提する。
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目は攻撃者が車載器へ侵入できた場合に、車両サービス正常稼働の影響について確認するものである。 ① 「2. 侵入」「3. 権限昇格」で車載器(主に AVN を想定)にリモート接続 ② 車両(情報系)のサービス(機能)の停止させるコマンドを実行  以下 1～4 の観点で攻撃を試行した結果、[サービス状態]に挙げる悪影響が発生するか確認する。 **1.プロセス強制終了による車両サービスの停止(4.2.1.1)** **2.CPU 負荷上昇による車両サービスの停止(4.2.1.2)** **3.ネットワーク負荷上昇による車両サービスの停止(4.2.1.3)** **4.ディスク負荷上昇による車両サービスの停止(4.2.1.4)** [サービス状態] a.著しくレスポンスが低下する b.画面が固まったまま動かない c.通信ができない

取得エビデンス	・　実行したコマンド一覧 ・　GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	1つのプログラムの機能不全が全体に影響を与えないことを確認する プログラムの機能不全を自動回復する機能があることを確認する
備考	

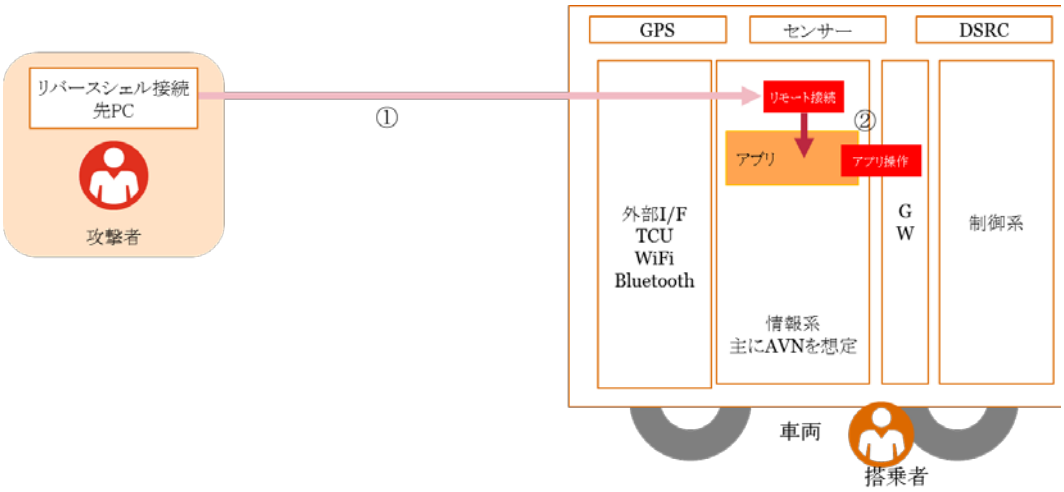
項目	記載内容
項目番号	4.3.1
項目名	制御系ファームウェアの改ざん
目的	制御系ファームウェアを改ざんできるか確認する
実施タイミング	車両システムテスト時
想定実施工数(作業量)	6～10 日
前提条件	「3.2 高権限の奪取」に成功している、あるいは「2.侵入」時に root 権限を取得済みである
入力情報	正規サーバーからダウンロードした制御系ファームウェア(セントラルゲートウェイを想定) 正規サーバーからダウンロードした旧バージョンの制御系ファームウェア(セントラルゲートウェイを想定)
実施条件	改ざんファームウェアにデジタル署名を付与するために必要な環境の準備が完了していること AVN 側に GW のファームウェアアップデートプログラムが存在していること 対象車載器に電源が供給され、使用可能な状態であること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. 静的コード解析の経験を有する人材が確保できない 2. 小規模のプライベート PKI 環境の構築経験を有する人材が確保できない
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目は制御系を不正操作するための手段として、セントラルゲートウェイ(以下、GW と記載する)のファームウェアを改ざんできるか確認するものである。 ① 「2．侵入」「3．権限昇格」で車載器（主に AVN を想定）にリモート接続 ② 改ざんしたファームウェアで GW をアップデート  改ざん検知手段は以下 2 パターンを想定しており、本評価項目ではこれらの回避を試行する。 a. チェックサム方式 b. デジタル署名方式 また、ファームウェアのダウングレードを禁止する機能の有無についても確認する。 **1. チェックサムによるアップデート保護の回避(4.3.1.1)** **2. デジタル署名によるアップデート保護の回避(4.3.1.2)** **3. ファームウェアのダウングレード(4.3.1.3)**

取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット）
事前作業実例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	ファームウェアには発行元の電子署名を付与し、事前に正規の署名か検証していることを確認する セキュアエレメントを用いたファームウェア改ざん検知を行っていることを確認する ファームウェアのダウングレードを制限していることを確認する
備考	・ 電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト） http://www.cryptrec.go.jp/list/cryptrec_ciphers_list_2016.pdf ・ Verifying Boot https://source.android.com/security/verifiedboot/

項目	記載内容
項目番号	4.3.2
項目名	制御系機能の悪用
目的	情報系が持つ制御系への命令パスを悪用して制御系を故意に操作することができるか確認する
実施タイミング	車両システムテスト時
想定実施工数(作業量)	1～5 日
前提条件	「3.2 高権限の奪取」に成功している、あるいは「2.侵入」時に root 権限に昇格済みである
入力情報	特になし
実施条件	対象車載器に電源が供給され、使用可能な状態であること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. CAN メッセージの仕様を利用している人材が確保できない 2. 静的コード解析の経験を有する人材が確保できない
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目は、攻撃者が車載器へ侵入できた際、情報系機器が持つ制御系への命令パスを悪用して制御系を故意に操作することができるか確認するものである。 情報系から制御系へのアクセスは API を通して間接的に CAN メッセージを発行することを想定している。そのため最初に情報系（AVN、TCU）に CAN メッセージを発行できる API が用意されているか調査する。API が存在していた場合、同 API を用いて制御系を操作できるかどうか確認する。 ① 「2.侵入」「3.権限昇格」で車載器（主に AVN を想定）にリモート接続 ② 情報系上の API から CAN メッセージを発行  本項目は以下の流れで実施する。 **1. CAN メッセージを実行する API の調査（4.3.2.1）** **2. API を利用した制御系の操作（4.3.2.2）**
取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	重要な機能に関する API 呼び出しについては呼び出し元の認証する（MAC 認証など）
備考	

項目	記載内容
項目番号	4.4.1
項目名	情報系アプリケーションの改ざん
目的	改ざんアプリケーションで起動できるか確認する
実施タイミング	車両システムテスト時
想定実施工数(作業量)	8 時間未満
前提条件	「3.2 高権限の奪取」に成功している、あるいは「2.侵入」時に root 権限を取得済みである
入力情報	AVN 内のアプリケーションファイル
実施条件	デジタル署名を確認、削除、付与できる検証用 PC が構築済みであること 対象車載器に電源が供給され、使用可能な状態であること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1. モバイルアプリケーションの開発経験を有する人材が確保できない 2. 小規模のプライベート PKI 環境の構築経験を有する人材が確保できない
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目は情報系を不正操作するための手段として、改ざんしたアプリケーションをダウンロードし実行できるか確認するものである。 アプリケーションの実行には改ざん防止のためデジタル署名の確認が行われていることを想定している。 ① 「2. 侵入」「3. 権限昇格」で車載器(主に AVN を想定)にリモート接続 ② 情報系上のアプリケーションを改ざん ③ 改ざんしたアプリケーションを起動  本項目は以下の流れで実施する。 **1 セーフティシステムの確認** 1.1 監視項目の確認(4.4.1.1) 1.2 セーフティシステムの無効化(4.4.1.2) **2. 暗号化方式の確認(4.4.1.3)** **3. デジタル署名を改ざんした状態でのアプリケーション起動(4.4.1.4)** **4. 異なるユーザーのデジタル署名を付与した状態でのアプリケーション起動(4.4.1.5)**

取得エビデンス	・ 実行したコマンド一覧 ・ GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	電子署名されたアプリケーションのみ起動を許可していることを確認する
備考	・ 電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト） http://www.cryptrec.go.jp/list/cryptrec_ciphers_list_2016.pdf

項目	記載内容
項目番号	4.4.2
項目名	情報系機能の悪用
目的	アプリケーションの命令パスを悪用して情報系を故意に操作することができるか確認する
実施タイミング	車両システムテスト時
想定実施工数(作業量)	1～5 日
前提条件	「3.2 高権限の奪取」に成功している、あるいは「2.侵入」時に root 権限を取得済みである
入力情報	特になし
実施条件	対象車載器に電源が供給され、使用可能な状態であること
外部委託条件	以下いずれかの条件に該当する場合、外部への委託を検討する 1.　静的コード解析の経験を有する人材が確保できない
事前作業	公開用資料のため、記載内容を削除
確認事項	本項目は攻撃者が車載器へ侵入できた際、アプリケーションを制御する API を悪用することで情報系を故意に操作できるかどうか確認するものである。  本項目は以下の流れで実施する。 **1. アプリケーションを実行する API の調査（4.4.2.1）** **2. API を利用した情報系の操作（4.4.2.2）**
取得エビデンス	・　実行したコマンド一覧 ・　GUI 画面の出力（スクリーンショット）
事前作業実施例	公開用資料のため、記載内容を削除
実施例	公開用資料のため、記載内容を削除
結果判断	公開用資料のため、記載内容を削除
開発検討項目	重要な機能に関する API 呼び出しについては呼び出し元の認証をする（MAC認証など）
備考	・　AGL Application Framework: A Quick Tutorial http://docs.automotivelinux.org/docs/apis_services/en/dev/reference/af-main/4-quick-tutorial.html

5. 参考文献

[1] JASO TP15002 自動車―情報セキュリティ分析ガイド, 公益社団法人自動車技術会, 2015.
[2]（一財）日本自動車研究所：Ｖ２Ｘ等車外情報の活用にかかるセキュリティ技術の研究・開発プロジェクト, 平成 27 年度戦略的イノベーション創造プログラム, 2016
[3] 360 独角兽团队（UnicornTeam）, “硬件安全攻防大揭秘”, 2016
[4] Hiroshi Hashimoto, “JasPar’s activity towards the standardization of CyberSecurity”, escar Asia, 2017.
[5] Yuval Weisglass, “PRACTICAL ATTACK ON CAN MESSAGE AUTHENTICATION”, escar Asia, 2017.
[6] Dr. Frederic Stumpf, “A Holistic Approach to Automotive Security With Security in the Fast Lane”, escar Asia, 2017.
[7] 野口大輔, “Automotive Grade Linux のセキュリティリスク”, escar Asia, 2017.
[8] NIST SP 800-30 Revision 1, Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology, 2012.
[9] 自動車の情報セキュリティへの取組みガイド, Information-technology Promotion Agency Japan, 2013.
[10] ISO 26262, “Road vehicles. Functional safety”, 2011 （10 parts）.
[11] “Cybersecurity Best Practices for Modern Vehicles”, National Highway Traffic Safety Administration, 2016
[12] 360 独角兽团队（UnicornTeam）, “智能汽车安全攻防大揭秘”, 2017
[13] 360 独角兽团队（UnicornTeam）, “无线电安全攻防大揭秘”, 2016
[14] 佐藤 眞司,”ハードウェアセキュリティ―IoT の時代に向けて”, Information-technology Promotion Agency Japan, 2015.
[15] Randy Torrance and Dick James, “The State-of-the-Art in IC Reverse Engineering”, Conference on Cryptographic Hardware and Embedded Systems, 2009
[16] 耐タンパー性調査研究委員会報告書, 財団法人 日本規格協会 情報技術標準化研究センター, 2003
[17] Dr. Sergei Skorobogatov, “Physical Attacks on Tamper Resistance: Progress and Lessons”, 2nd ARO Special Workshop on HW Assurance, 2011
[18] Bulent Yener, “CSCI4974/6974 hrdware reverse Engineering”, Rensselaer Polytechnic Institute, 2014

6. Appendix

Appendix 1. 本ガイドと想定脆弱性との関連

本ガイドの評価項目の一覧と本ガイドで想定する既知の車両インシデント（脆弱性）との関連を示す。なお、各脆弱性の詳細は「2.1 本書がカバーする既知の車両インシデント」を参照のこと。

評価項目	*Jeep Cherokee の uConnect 脆弱性*	*BMW の ConnectedDrive 脆弱性*	*Tesla ModelS の無線 LAN 脆弱性*	*三菱アウトランダーのモバイルアプリ脆弱性*	*日産 Nissan Connect EV の脆弱性*
1.1.1 デバイス取り出し前 I/F 調査	△	△	△		△
1.1.2 デバイス取り出し後 I/F 調査	△	△	△		△
1.1.3 チップ取り外し後 I/F 調査	△	△	△		△
1.1.4 隠れたインターフェースからの調査					
1.1.5 インターフェース接続	△		△		
1.1.6 バイナリ抽出	○	○	○		
1.1.7 バイナリ保護機能確認		○			
1.1.8 リバースエンジニアリング	○	△	○		○
1.2.1 アプリケーションの通信経路の調査					
1.2.2 WiFi（車両外部）の通信傍受			△		
1.2.3 WiFi（車両内部）の通信傍受	○			○	
1.2.4 Bluetooth の通信傍受					
1.2.5 BluetoothLE の通信傍受					
1.2.6 TCU の通信傍受	○	○			
1.2.7 ブラウザ、HTML エンジンの調査			○		
1.2.8 CAN メッセージ通信傍受					
1.2.9 アプリケーションの通信傍受					
2.1.1 DrivebyDownload 攻撃			○		
2.1.2 ファイル添付攻撃					
2.2.1 外部 WiFi への自動接続を利用した攻撃			○		
2.2.2 偽サーバー誘導による攻撃					
2.2.3 残存開発環境を用いた攻撃					○
2.3.1 Bluetooth 経由の攻撃					
2.3.2 BluetoothLE 経由の攻撃					
2.3.3.TCU 経由の攻撃	○				
2.3.4 WiFi（車両内部）経由				○	

の攻撃					
2.4.1 成りすまし攻撃		○		○	
2.4.2 リプレイ攻撃					
3.1.1 コード実行防止機能の回避					
3.1.2 サンドボックス機構の回避					
3.2.1 既知の攻撃を試行することによる権限昇格			○		
3.2.2 強制アクセス制御（MAC）の機構の回避			○		
4.1.1 機密情報の漏えい（外部送信）	○				○
4.2.1 車両のサービス（機能）の停止					
4.3.1 制御系ファームウェアの改ざん	○		○		
4.3.2 制御系機能の悪用		○		○	
4.4.1 情報系アプリケーションの改ざん					
4.4.2　情報系機能の悪用			○		

評価項目	*日産リーフの脆弱性*	*スバル StarLink の脆弱性*	*Continental AG の TCU の脆弱性*	*マツダの Mazda Connect の脆弱性*	*本田技研工業 Honda Connect の脆弱性*
1.1.1 デバイス取り出し前 I/F 調査				○	○
1.1.2 デバイス取り出し後 I/F 調査					
1.1.3 チップ取り外し後 I/F 調査					
1.1.4 隠れたインターフェースからの調査					
1.1.5 インターフェース接続				○	○
1.1.6 バイナリ抽出				△	△
1.1.7 バイナリ保護機能確認					
1.1.8 リバースエンジニアリング				△	△
1.2.1 アプリケーションの通信経路の調査					
1.2.2 WiFi（車両外部）の通信傍受	△	△			
1.2.3 WiFi（車両内部）の通信傍受					
1.2.4 Bluetooth の通信傍受					
1.2.5 BluetoothLE の通信傍受					
1.2.6 TCU の通信傍受					
1.2.7 ブラウザ、HTML エンジンの調査					
1.2.8 CAN メッセージ通信傍受					
1.2.9 アプリケーションの通信傍受		△			
2.1.1 DrivebyDownload 攻撃					

2.1.2 ファイル添付攻撃					
2.2.1 外部 WiFi への自動接続を利用した攻撃					
2.2.2 偽サーバー誘導による攻撃					
2.2.3 残存開発環境を用いた攻撃					
2.3.1 Bluetooth 経由の攻撃					
2.3.2 BluetoothLE 経由の攻撃					
2.3.3.TCU 経由の攻撃			○		
2.3.4 WiFi（車両内部）経由の攻撃					
2.4.1 成りすまし攻撃	○	○			
2.4.2 リプレイ攻撃					
3.1.1 コード実行防止機能の回避					
3.1.2 サンドボックス機構の回避					
3.2.1 既知の攻撃を試行することによる権限昇格					
3.2.2 強制アクセス制御（MAC）の機構の回避					
4.1.1 機密情報の漏えい（外部送信）					
4.2.1 車両のサービス（機能）の停止					
4.3.1 制御系ファームウェアの改ざん					
4.3.2 制御系機能の悪用	○	○			
4.4.1 情報系アプリケーションの改ざん				○	○
4.4.3　情報系機能の悪用				○	○