SYNOPSYS®

平成２９年度成果報告書

戦略的イノベーション創造プログラム（ＳＩＰ）自動走行システム 大規模実証実験 情報セキュリティ実証実験

国立研究開発法人新エネルギー・産業技術総合開発機構

委託先：日本シノプシス合同会社

目次

まえがき

近年、自動車のシステムに対する侵入テスト手法が多数研究開発されている。しかしながら、自動車の侵入テストについては、自動車メーカーごとに異なる車両システムであるため、侵入テストの手順が標準化し辛いことが課題である。このため、本実証前調査では、ある車両システムに対する(1) セキュリティ評価手法の策定、 (2) 体系的な侵入テスト手法の実現にフォーカスをあてて取り組む。その成果物は、ISO 等の国際標準を参照し、JasPar 関連組織が活用することにより、技術的なスキル向上かつ新たな脅威に対して保守・運用できるものとする。

成果と達成状況

実施契約書で定義された実施内容について達成することが出来た。

a. 脅威分析調査

b. 情報セキュリティ評価ガイドラインドラフトの作成

c. 情報セキュリティ評価の試行調査

d. 実証実験の運営準備

和文要約

a.　脅威分析調査

V2X 等車外からの攻撃を含む自動走行車両及びシステムに関する脅威全体像整理し、自動走行車両のみならず、各車両とシステム構成要素間の連係動作やシステム運用時のエコシステムやユースケースを観点とした脅威を明らかにした。

b.　情報セキュリティ評価ガイドラインドラフトの作成

市場で既知のセキュリティ問題事例（以下「インシデント事例」という。）や脆弱性の情報及び既存のセキュリティ評価手法をもとに、車両向けセキュリティ評価ガイドラインドラフトを作成した。

c.　情報セキュリティ評価の試行調査

上記 b.項で策定する評価ガイドラインドラフトを用いて、車両または車両を構成するシステムに対して実車や部品システムでの評価を行い、評価ガイドラインドラフトの妥当性の検証を行うとともに、必要に応じて評価ガイドラインドラフトの修正を実施した。

d.　実証実験の運営準備

以上の a.～c.項に基づき、平成 30 年度に実施する実証実験の早期開始の実現を目的として、実証実験開始に必要な計画立案、実証実験参加者の募集要領、申請書、規約類、契約書類（秘密保持条件含む）等の策定を行った。

英文要約

a. Threat analysis study

This study is intended to identify the entire picture of the threats relevant to automated driving vehicles and systems including the attacks from outside the vehicle, such as V2X; it is not only intended to reveal threats relevant to the automated driving vehicles, but also the threats relevant to linked operations between each vehicle and system-composing elements as well as the ecosystem and usages when the system is in operation.

b. Preparation of draft guidelines for information security assessment

Based on existing security issues in the market (hereinafter, “incidents”) and vulnerability information as well as existing security assessment techniques, a draft guideline for security assessment for vehicles will be prepared.

c. Trial study on information security assessment

Using the draft assessment guideline developed in the above Item b, we will perform an assessment on actual vehicles and component systems to assess a vehicle or the comprising systems and will also check the validity of the guideline; if necessary, modifications will be made to the draft assessment guideline.

d. Preparation for management of field operation test (FOT)

Based on above a to c items and to realize early launching of the FOT held in the fiscal year 2018, we will propose a necessary plan for launching the FOT and will develop application procedures, forms, terms, contract documents (including provisions for non-disclosure), etc. for participants of the FOT.

報告書、ガイドラインドラフト等

SYNOPSYS®

「戦略的イノベーション創造プログラム(SIP)自動走行システム／大規模実証実験」のうち「情報セキュリティ実証実験」

a脅威分析調査報告書

1　序論

本書は，「戦略的イノベーション創造プログラム（SIP）自動走行システム」の大規模実証実験プログラムの「情報セキュリティ実証実験」に対する調査結果をまとめるものである．

1.1 本書の目的

本書の目的は，近い将来実用化が期待されている自動走行システムの脅威分析を実施することである．
しかしながら，一方で，自動走行技術を搭載するシステムは，開発者のポリシーにより構成が異なり，セキュリティ上の脅威やリスクもシステム構成により大きく異なることが課題となる．このため，本書では，日本及び世界の主要な自動走行システムを調査し，類型化されたシステムで脅威分析を試みた．この類型化された車両システムはいくつかの構成要素で実現されており，それらの構成要素に対する脅威を導出した．そして，導出された脅威に対して，現状対策がされているかどうか整理を行い，脅威の全体像の整理を行った．

尚，本書での脅威分析は，自動車のセキュリティに関するガイドラインである SAE J3061 でも定義されるコンセプトフェーズの脅威分析に近いものを想定している．つまり，類型化された車両システムを用いることにより，脅威を洗い出すことを目的としている．このため，システムレベルでの各構成要素の脆弱性の情報を含まず，脅威のレベル（深刻度や発生可能性）から対策要否を検討するアプローチを採用している．

1.2 脅威分析の範囲

自動運転システムは単に自動走行を実現するだけではなく，社会基盤となりうる様々なサービスと密接に連携することが予想されている．このため，本論で取り扱う範囲は，自動走行システム及び自動走行システムが接続される機器やサービスなどを含むものとする．

1.3 調査手順

本調査は以下の手順で実施した.

① 調査と類型化

現在までに研究開発されている自動走行システムを対象に，車両システムや機能を調査し，類型化を実施した．類型化により導出された車両システムに対して脅威分析を実施した．この結果，車両システムと機能／サービスを分けて，脅威分析する方法を採用した.

②脅威分析

自動走行システムには様々な機能やサービスが搭載され，それらを実現するための構成要素や機器が多岐に渡るため，情報セキュリティの脅威分析手法をそのまま適用することが難しい．このため，本論では，まず最初に，より広く脅威が導出される脅威分析手法を検討した．その上で，類型化された車両システムに対して脅威分析を実施した．次に，類型化された機能あるいはサービスの観点での脅威分析を実施した.

③リスク算定法の検討

洗い出された脅威に対するリスク値の算定方法を検討した．自動走行システムの構成要素は各自動車メーカーにより様々異なる可能性がある．このため，実装されるシステムの脆弱性について言及することは困難である．しかしながら一方で，対策するべき脅威の洗い出しについては自動車メーカーが車両の開発当初に設定する必要がある．このため，本論では脅威の Impact をランク付けする手法により，リスクの算定を行った.

④機能/サービスの脅威分析

前述する③までの結果より，各導出された脅威のリスク値を適用し，脅威の実現可能性を示した.

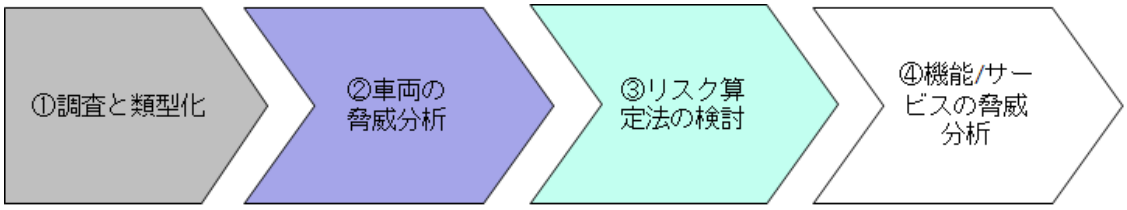


図 1-1 調査のアプローチ

2　略語，用語，定義

2.1 略語，用語

表 2-1 略語，用語

略語	記述
RADAR	電波を対象物に向けて発射し，その反射波を測定することにより対象物までの距離や方向を測る装置を指す.
LIDAR	Light Detection and Ranging の略. 光を用いて測距を行うためのセンサーのこと.
Over the Air (OTA)	Over the Air の略. 一般的に，車両システム内の制御用コンピュータのプログラムの更新機能のこと. 例えば，プログラムの欠陥や改修，機能のアップデートなどを行うために使用される.
LDW(Lane Departure Warning)	車線逸脱防止支援システムのこと. 車線逸脱を行いそうになった場合，警告音などにより運転者に危険を通知するシステムのことである.

3　関連文書

3.1 入力文書など

[1] 官民 ITS 構想・ロードマップ 2017,
https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20170530/roadmap.pdf, 2017.
[2] 平成 26 年度　戦略的イノベーション創造プログラム　V2X(Vehicle to X)システムに係るセキュリティ技術の海外動向等の調査,
http://www.meti.go.jp/meti_lib/report/2015fy/000326.pdf, 2017.
[3] 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）：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 28　年 3　月
[4] 自動運転レベルの定義　を巡る動きと　今後の対応（案），平成 28 年 12 月 7 日，内閣官房 IT 総合戦略室,
https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/detakatsuyokiban/dorokotsu_dai1/siryou3.pdf
[5] 自動運転バス、完全無人化　ソフトバンク系が実験　,
https://www.nikkei.com/article/DGXLASDZ18H7M_Y7A710C1000000/, 2017.
[6] トラック、高速道で隊列組み自動走行　政府が実験へ,
http://www.asahi.com/articles/ASK2J535XK2JULFA013.html, 2017.
[7] EVITA, 2017.
[8] HAVEit, http://www.haveit-eu.org/displayITM1.asp?ITMID=6&LANG=EN, 2017.
[9]
http://www.smbc.co.jp/hojin/report/investigationlecture/resources/pdf/3_00_CRSDReport039.pdf, 2017.
[10]「レベル4」完全自動運転バス、国内4カ所で30年秋にも公道実験　ソフトバンク子会社、「高齢者の足」確保狙う, http://www.sankei.com/west/news/161218/wst1612180019-n1.html, 2017.
[11] 自動走行に関する取組について,
http://www.kantei.go.jp/jp/singi/keizaisaisei/miraitoshikaigi/4th_sangyokakumei_dai3/sankou4.pdf, 2017.
[12] Driverless Car: A Thing of the Future? Terms and technologies you need to know!,
https://techglimpse.com/how-driverless-car-works-technologies/ 2017.
[13] Valeo Park4U Automatic Parking System, http://psipunk.com/valeo-park4u-automatic-parking-system/, 2017.

[14] Self-parking cars hit legal obstacles, http://www.telegraph.co.uk/motoring/news/10404850/Self-parking-cars-hit-legal-obstacles.html, 2017.

4　自動運転システム

自動運転システムとは，自動走行を行うための自動運転車両及び，その車両と連携するインフラや機器などを含めたシステムを指す．自動運転車(Self-driving car)の目的は，自動車自身が道路や周辺環境に合わせて安全に目的地へ走行するシステムを搭載した自動車を指す．この自動運転システムの目指すところは以下の通りである．

1) **経済損失**：交通渋滞により損失する経済効果や膨大であり，交通の流れを効率化することにより，都市や高速道路での渋滞などを緩和することが期待されている．

2) **交通事故低減**：交通事故死亡者数を低減することが期待されている．自動運転車両が多数走行するようになれば，システムが誤動作しない回切りは，車両同士の事故は少なくともゼロにすることができる．自動運転車両が車両と歩行者などの交通弱者との事故も低減できる可能性がある．

3) **都市交通の効率化**：シェアリングエコノミーに代表されるように，公共交通網への自動運転車両の適用が期待される．例えば，都市中心部での交通渋滞緩和が挙げられる．さらに，ラストワンマイルに代表されるように，駅と自宅を結ぶ交通手段としても期待されている．

4) **環境負荷低減**：運転者の熟練度にも依存するが，無駄なアクセルやブレーキなどを低減できることによる環境負荷低減が期待されており，CO2 などの排出量を低減することも期待されている．

5) **交通弱者への救済**：例えば，過疎地域に住む高齢者などは公共交通サービスを十分に受けられない状況にある．これらを救済するために，自動運転バスなどにより，過疎地域でも低いコストで公共交通サービスが受けられるような仕組み作りが必須となっている．

一方，自動運転システムを実現する手段としては様々存在しているものの，少なくとも車両自身にセンシング技術，データ処理，判定アルゴリズム，通信技術などの様々な技術が必要となる．

4.1 自動運転システムの歴史

自動運転自動車の研究としては，1939 年に開催されたニューヨーク万国博覧会に展示された GM の Futuurama(ヒューチュラマ)という模型が人気を博した.

その後，1960 年代には月面調査のために構想された最初のスマートカー「Stanford Cart」が挙げられ，ビデオカメラと遠隔操作のための長いケーブルが取付けられる方法により実現された. その後，さらなる研究開発が進み，障害物回避技術の搭載や画像処理能力の向上が実現した.

実際に通常の道路を走ることを想定して作られた最初の自動運転車は，1960 年台後半から 1970 年台にかけてつくば機械技術研究所の津川定之教授らによって開発された. このとき，信号処理にアナログコンピュータ技術を利用した 2 つのカメラを備え，高架式レールを利用して，時速 30 ㎞まで走行した.

その後，1995 年にカーネギーメロン大学のロボット研究者らにより開発された，小型コンピュータ，フロントガラスのカメラ，GPS 受信機などを搭載し，ピッツバーグからロサンゼルスまでの自動運転での走行を目指した

表 4-1 自動運転システムの歴史と変遷

自動運転システムの世代	年代	主流方式
第 1 期	1950～1960 年代	路車協調型(誘導ケーブルを用いたガイド式)
第 2 期	1970～1980 年代	自律型(マシンビジョン)
第 3 期	1990 年代	IVHS/ITS 関連 各種技術の試用
第 4 期	2001～現在	実用化を目指した技術の検証

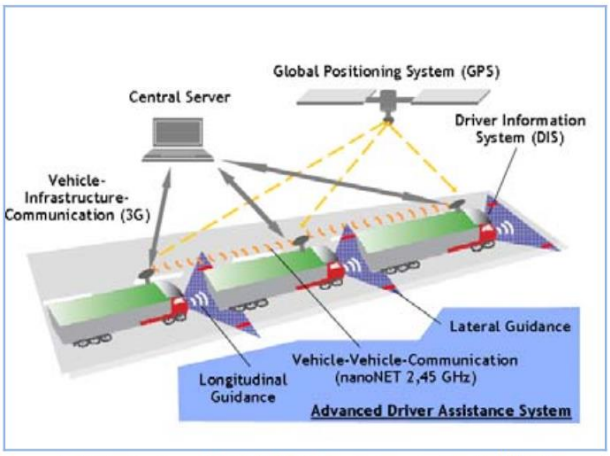
4.2 隊列走行システム

一方，国内においても，2020 年代に自動運転を実用化するべき，国土交通省が 2012 年に検討会を発足し，自動運転隊列走行実験が行われた. 同様の取り組みは海外でも広く行われており，ドイツでは 2005 年から 2009 年にドイツ運輸省およびアーヘン工科大学が中心となり，「KONVOI」

と呼ばれる 4 台の隊列走行システムが開発され，アウトバーンなどの公道での走行実験を行ったとされる．この他にも，米国では UC バークレイの研究所 PATH が米国運輸省 DOT の予算で隊列走行システムを開発した．

図Ⅲ.2-1　隊列走行実現イメージ

図 4-1 隊列走行実現イメージ（http://www.nedo.go.jp/content/100095912.pdf より出典）



図Ⅲ.2-2　KONVOI のシステム構成
（出典：KONVOI 資料）

図Ⅲ.2-3　PATH のシステム構成
（出典：PATH 資料）

図 4-2 ドイツ KONVOI と米国 PATH のシステム構成図
（http://www.nedo.go.jp/content/100095912.pdf より出典）

国交省の研究プロジェクトは 2008 年から 2012 年の 5 年間の間に開発された．この時に開発された実験車両の外観は次の図に示す通りである．このシステムから，GPS，レーザレーダ，ミリ波レーダ，カメラが採用されていることがわかる．

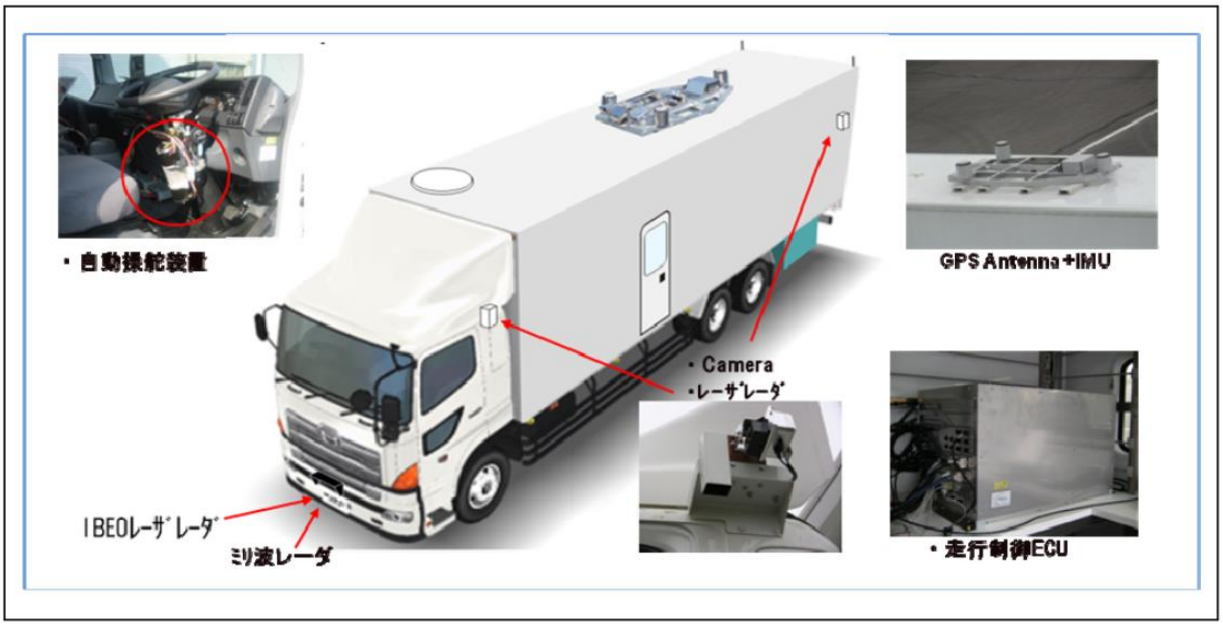


図 4-3 隊列走行に用いた実験車両の外観 http://www.nedo.go.jp/content/100095912.pdf **より出典）**

その他，主要な隊列走行プロジェクトのシステム構成の違いについては以下の表に示すとおりである．主たる違いは，前車追従の仕組みが異なること，車間距離の検出方法が違うこと，車車間通信を用いるかどうかが挙げられる．

表 4-2 各隊列走行プロジェクトの比較

プロジェクト	開発主体	システム構成			
		隊列台数/車間距離	レーンマーカ	車車間通信	車間距離センサ
ショープアー	ベンツ	2 台 10m	マーカ追従型	なし	画像認識
Phoenix Project	PATH	2 台 4m	磁気マーカ	2.48GHz	ミリ波レーダ レーザレーダ
KONVOI	アーヘン大	4 台 10m	白線	2.48GHz	ミリ波レーダ レーザレーダ
IMTS	トヨタ	3 台 20m	磁気マーカ	2.48GHz	車車間通信

4.3 ASV(先進安全自動車)

先進安全自動車（ASV）は，先進技術を利用してドライバーの安全運転を支援するシステムを搭載した自動車を指す．国土交通省は，「ASV 推進計画」として，ASV に関する技術の開発・実用化・普及を促進するプロジェクトを立ち上げており，平成 3 年度から 15 年以上にわたって取り組まれた．

ASV推進計画の概要

第１期	第２期	第３期	第４期	第５期
平成3～7年度	平成8～12年度	平成13～17年度	平成18～22年度	平成23～27年度
・技術的可能性の検討	・実用化のための研究開発	・普及促進のための検討 ・新たな技術開発	・本格的な普及促進 ・通信を利用した安全システムの一部実用化	・飛躍的高度化の実現
・自動車単独（自立検知型）	・自動車単独（自立検知型） ・道路インフラとの連携	・自動車単独（自立検知型） ・道路インフラとの連携	・自動車単独（自立検知型） ・他車両との連携 ・道路インフラとの連携	・実用化されたASV技術の飛躍的高度化 ・次世代通信利用型運転支援システムの開発促進

図 4-4 ASV 推進計画の概要(http://www.mlit.go.jp/jidosha/anzen/01asv/aboutasv.html より出典)

ASV では，当初の計画として，以下の図に示すような技術開発に取り組まれた．これらの機能の一部はすでに実用化されており，エアバッグなどは標準装備することが義務化されるなど実用上の貢献も大きい．さらに，未だ実用化されていない機能についても研究開発が進められている．

図 4-5 ASV 推進計画より
(http://www.mlit.go.jp/jidosha/anzen/01asv/resourse/data/asv1pamphlet.pdf より出典)

また，想定する車両システムとしては，下図に示すシステムである．この図が示すように，自動運転車両では，前述するカメラや各種センサを採用することにより実現が検討されている．

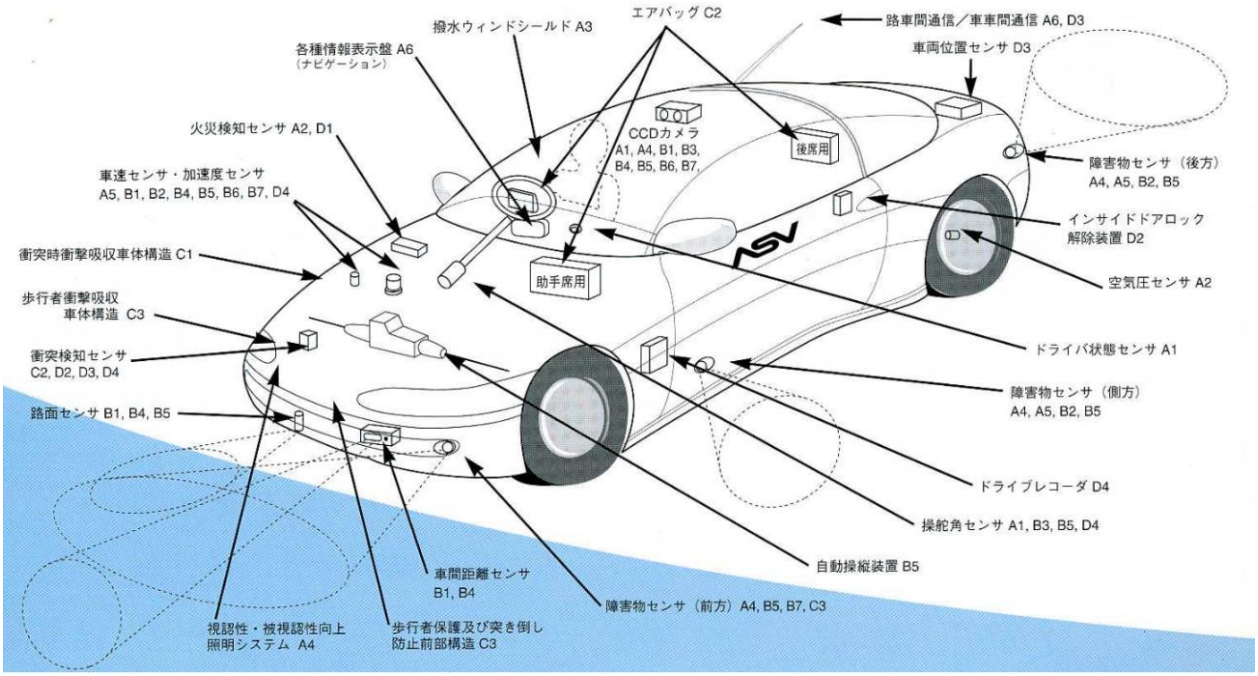


図 4-6 ASV 推進計画にて想定する自動運転システム
（http://www.mlit.go.jp/jidosha/anzen/01asv/resourse/data/asv1pamphlet.pdf より出典）

最後に，実用化された ASV 関連技術は下図に示すとおりであり，ESC, LKAS, ACC, AEBS などが存在している.

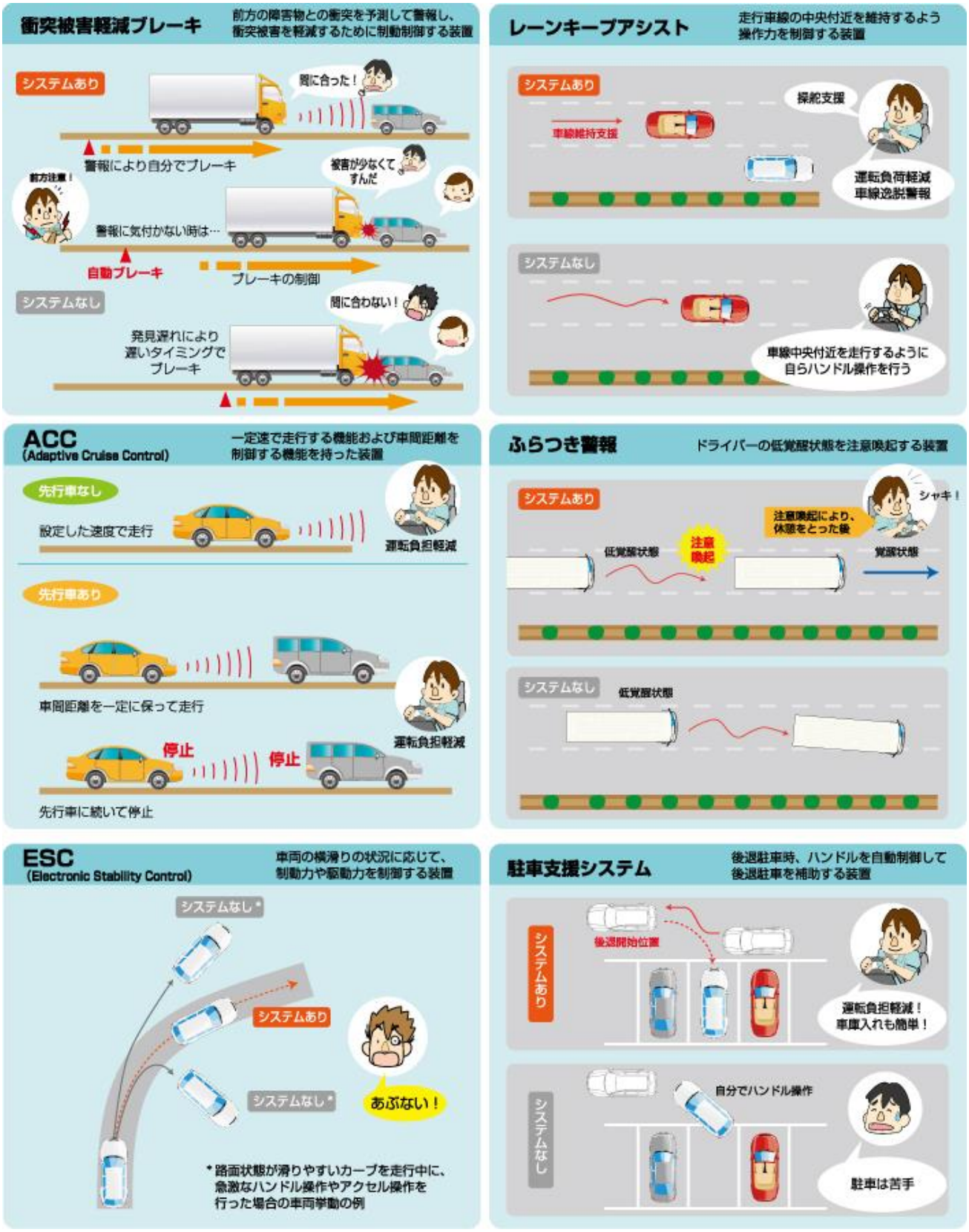


図 4-7 実用化された ASV 関連技術

（http://www.mlit.go.jp/jidosha/anzen/01asv/japanese/practical.html より出典）

4.4 自動運転システムの今後

自動運転システムは，完全自動運転を目指し研究開発が進められている．近年では，特に実用化を目指した自動運転システムの開発が様々な企業において進められている．特に，新規プレイヤーとして IT ベンダなどが自動運転車両の研究開発に参入しており，今後もますます研究開発が活発になると考えられる．

図 4-8 自動走行技術の開発状況(http://www.mlit.go.jp/common/001155023.pdf より出典)

図 4-9 自動運転に関する取り組み状況と分類(http://www.mlit.go.jp/road/ir/ir-council/autopilot/pdf/06/4.pdf より出典)

4.5 SAE J3016

SAE では自動運転技術やサイバーセキュリティに対して様々な規格文書が発行されている. そのうち, J3016 では自動運転レベルは 5 段階に分けて整理されており, 今後はこの指標に応じて自動運転度合いが決定されるものと考えられる. 一口に, 自動運転技術といっても, このような 6 段階(実質 5 段階)の車両が共存し連携することになることが予想される.

Table 4-1 SAE が定める自動運転レベル(参考文献[4]より引用)

レベル		自動運転の内容
0	運転自動化なし(No Driving Automation)	人間の運転者が、全てを行う。
1	運転支援(Driver Assistance)	車両の自動化システムが、人間の運転者をときどき支援し、いくつかの運転タスクを実施することができる。
2	部分的運転自動化(Partial Driving Automation)	車両の自動化システムが、いくつかの運転タスクを事実上実施することができる一方、人間の運転者は、運転環境を監視し、また、残りの部分の運転タスクを実施し続けることになる。

3	条件付運転自動化 (Conditional Driving Automation)	自動化システムは、いくつかの運転タスクを事実上実施するとともに、運転環境をある場合に監視する一方、人間の運転者は、自動化システムが要請した場合に、制御を取り戻す準備をしておかなければならない。
4	高度運転自動化(High Driving Automation)	自動化システムは、運転タスクを実施し、運転環境を監視することができる。人間は、制御を取り戻す必要はないが、自動化システムは、ある環境・条件下のみで運航することができる。
5	完全運転自動化(Full Driving Automation)	自動化システムは、人間の運転者が運転できる全ての条件下において、全ての運転タスクを実施することができる。

特に，このレベルにおいて重要なのは，車両システムと運転者の責任分解点にある．車両システムが運転の責任を負う場合には，車両メーカーが事故の責任を取る必要がある．このため，特に難しいのは，レベル 3 の運転者と車両システムの間で制御主体が行き来する場合であり，事故後にいずれが責任を負うかはドライブレコーダーなどに記録された情報などから解析するしかない可能性がある．

4.6 自動運転とセキュリティ

近年，自動運転システムの開発が進むにつれて，自動運転システムを狙った攻撃事例が報告されている．以降では，これらの脅威について，既存する脅威事例として概説する．

4.6.1 既存する脅威事例

4.6.1.1 BlackHat EU2015, escarUSA2016

自動運転システムに対する脆弱性として，Jonathan Petit がセンサを攻撃することにより，自動運転システムの判断を誤らせることが出来ることを指摘している．対象となるセンサは，自動運転車特有のカメラや LIDAR を想定しており，これらの入力を不作動にしたり，混乱させるような入力を与える攻撃を提案している．特に，カメラは特別な機器を使わなくとも，標識を付け替えるなどするソーシャル攻撃により，容易に混乱させることが可能であることを指摘している．さらに，車両システムが搭載するセンサ類（カメラ，LIDAR，超音波センサ，RADAR）に対する攻撃に対して，表 4-3 に示されるように強化策を導入しなければならないことを指摘している．

図 4-10 カメラに対する脅威(Jonathan Petit, AUTOMATED VEHICLES VULNERABILITIES? escarUSA2016 より出典)

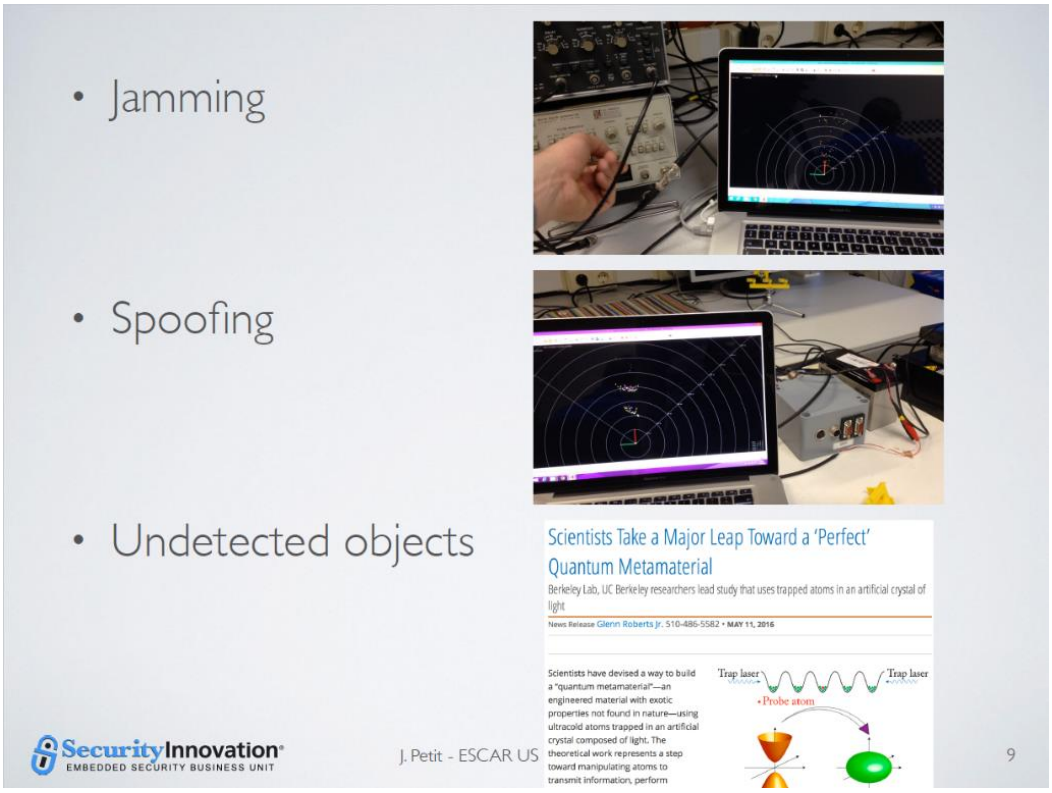


図 4-11 LIDAR に対する脅威(Jonathan Petit, AUTOMATED VEHICLES VULNERABILITIES? escarUSA2016 より出典)

表 4-3 指摘された脅威と強化策の一覧

対象	脅威	影響	強化
LIDAR	なりすまし	偽の物体を通知	冗長化
RADAR	なりすまし	偽の物体を通知	冗長化
超音波センサ	なりすまし	偽の物体を通知	冗長化
カメラ	混乱	間違った物体の検出	ニューラルネットを堅牢にする
センサフュージョン	不確定さの増加	間違った状況の認識	バイアス推定
GPS	なりすまし	間違った運転判断	発信元の認証
地図	毒される	間違った運転判断	否認防止,
ECU	特権獲得	信頼できないシステム	認証, 暗号化
TCU (SOTA)	間違ったソフトウェア更新	システムの乗っ取り	認証, 完全性

4.6.1.2 Tesla Model S

中国の IT 企業であるテンセントらにより, テスラ社の車両に対する様々な脅威が実現されている. 特に, LIDAR などの Time of Flight (TOF)方式においては, 障害物からの反射波が LIDAR までに届く間の遅延時間を早めたり, 遅くしたりすることにより, 障害物までの位置情報を改ざんすることができることを実証した. このように, 車両自体に接触しなくても, 車両の外部(至近距離)から攻撃する手法が多数存在している.

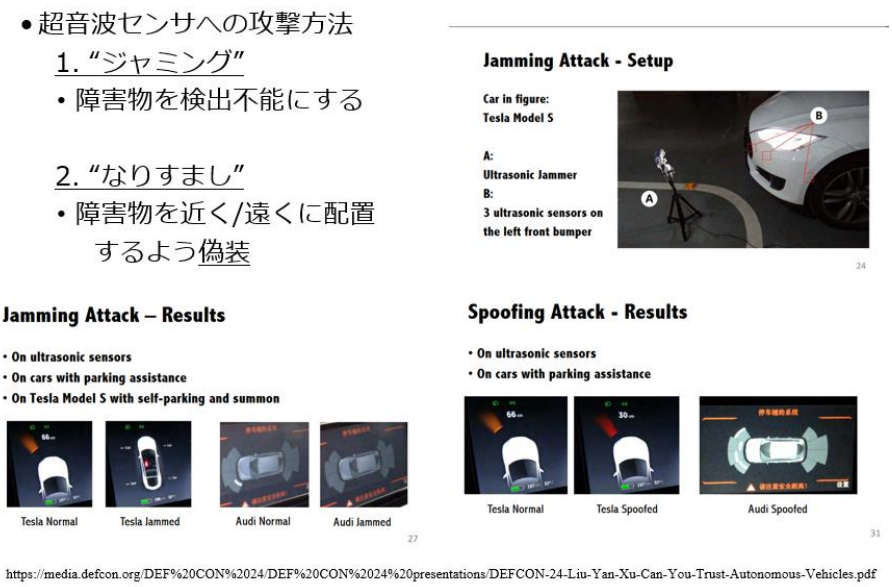


図 4-12 超音波センサのなりすましによる距離の改ざん
(https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Liu-Yan-Xu-Can-You-Trust-Autonomous-Vehicles.pdf より出典)

図 4-13 ミリ波レーダへのなりすましによる物体の位置改ざん
(https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Liu-Yan-Xu-Can-You-Trust-Autonomous-Vehicles.pdf より出典)

5　自動運転システムの類型化

5.1　アプローチ

自動運転システムの構成を網羅的に類型化するため，以下の 2 つの観点で調査を行った．

調査 1．自動運転システムの導入シナリオの調査

自動運転システムの導入シナリオとして，トラック，タクシーなどの商業車両，バス，トラムのような物流や公共交通での導入シナリオも存在する．このような導入シナリオの多くは，新規サービスと紐づいていることが多い．より具体的には，自動運転車両を用いたトラック，バス，タクシーなどが挙げられる．

調査 2．車両システムの構成調査

次に，各自動車メーカーや部品サプライヤ，IT ベンダ，スタートアップ企業などが考える車両構成を調査した．これは，サービスの土台となる車両システムがどのような構成を採るかに依存し，実現する脅威も異なるためである．

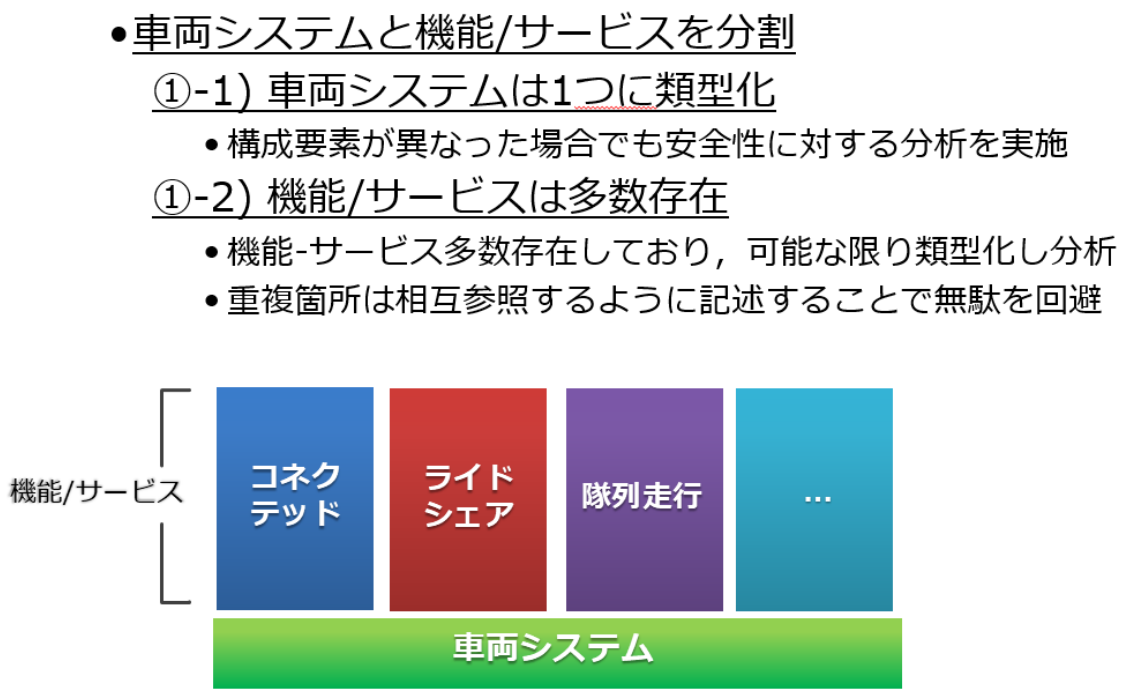


図 5-1　我々のアプローチ

5.2 自動運転の導入シナリオの調査

5.2.1 調査対象

海外の研究開発プロジェクトで検討されている自動運転システムのサービスについて以下の表に示すプロジェクトを調査した．尚，以降では調査された代表的な一部の例のみを説明する．

表 5-1 調査対象一覧

プロジェクト	内容
Transdev	自動運転トラムなどにより，オンデマンド型のシェアリングサービスを計画
自動運転バス	過疎地域での自動運転バスの運行事業の計画
トラック	トラックの電子牽引を用いた隊列走行の計画
自動車シェアリング	自動車をシェアすることにより，個人の費用負担を減らす取り組み

5.2.2 Transdev

19 の国で採用されるバスシステムであり，部品サプライヤの Delphi や日産・ルノーをパートナーにして，自動運転バスを走らせている．そのサービスの例としては，様々なユースケースが考えられており，例えば，以下のようなファーストマイルやラストマイル以外は，自動運転バスが使用されることが検討されている．また，ユーザーが要求するバス停にオンデマンドで予約するサービスなどが検討されている．

図 5-2 自動運転バスによる拠点間移動（http://www.eglobaltravelmedia.com.au/customer-convenience-is-king-with-transdev-to-deliver-on-demand-transport-pilots-in-sydney/より出典）

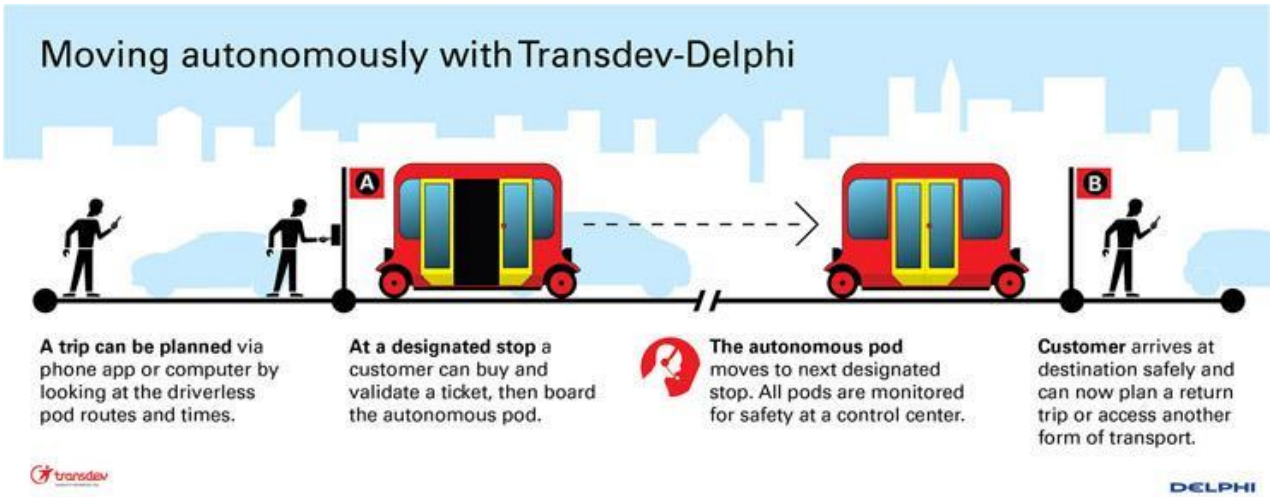


図 5-3 Transdev にて考えられているバスの自動運転システム
（http://www.autonews.com/article/20170607/MOBILITY/170609829/delphi-transdev-plan-self-driving-taxis-in-france より出典）

5.2.3　自動運転バス

過疎地域でのバス運行

文献[5]などから，社会的なニーズとして，過疎地域でのバス運行を行うことが示唆されている．過疎地では，移動手段に困る高齢者などをバスに乗せて走るサービスが社会保障サービスとして必要とされている．一方，バスの運行事業者は，バスを運行するための採算性が取れないような地域ではバスを運行するのが難しいという問題がある．そこで，自動運転車両を用いれば，バス運行のコストである人件費などが低減できるという狙いがある．

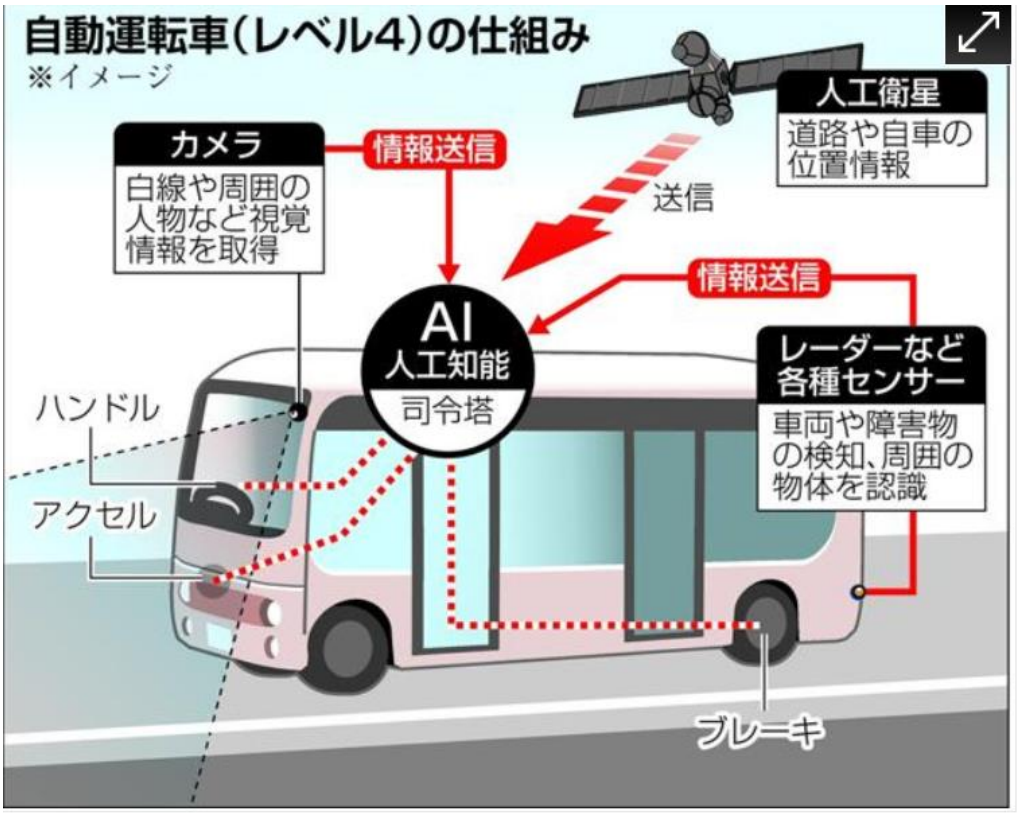


図　5-4　過疎地域でのバス運行システム（文献[10]より出典）

5.2.4　トラックによる隊列走行

高速道路での貨物牽引車両

文献[6]では，高速道路での隊列走行を一部無人で行うことが言及されている．これは，物流の効率化やトラックによる高速道路での事故防止，運転手不足の解消などの狙いがある．一方，隊列走行の技術には車車間通信を用いるなどが検討されており，先頭車両が追突すると甚大な被害を及ぼす可能性も否定できない．

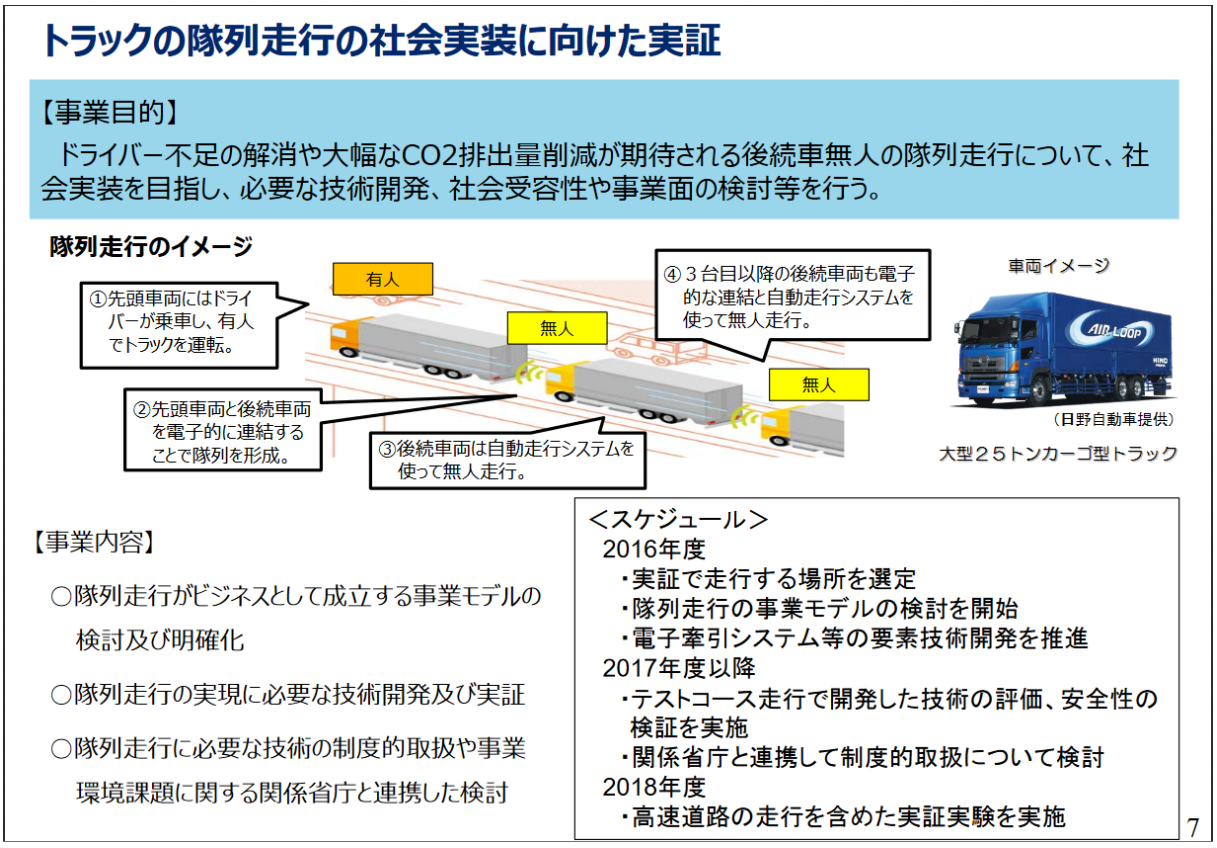


図 5-5 高速道路での自動運転（隊列走行システム，文献[11]より出典）

5.2.5 都市交通と次世代モビリティ

都市交通システムの進化とパーソナルモビリティ

文献[7]より，都市交通システムをより効率的なものにするために，都市交通システムに対して，パーソナルモビリティを提供するサービス事業者が増えることが予想されている．一方で，欧州ではライドシェアと呼ばれるサービスが普及しており，各都市の中心地までの移動はライドシェアし，中心地における移動はパーソナルモビリティで移動する街づくりが計画されている．個人で所有する自動車で中心地へ乗り入れる場合にはバレーパーキングなどにより，郊外の駐車場へと移動することが想定されている．

5.2.6 自動車シェアリング

近年，所有するのではなく，シェアすることにより維持コストを下げるシェアリングエコノミーの取り組みが進められており，自動車も個人で所有するものではなく，必要な時にだけ自動車を使用するようなサービスが数多く実現されている．この場合には，あるユーザーが使用した後で別のユーザーが車両をそのまま使用することが想定されており，悪意のあるユーザーが自動車内のシステムに改造を加えても検出することが難しいなどの課題がある．レンタカーの場合には，レンタカー

の事業者が整備を実施可能であったが，シェアカーではこのようなメンテナンスサービスを実施することが難しいなどの課題がある．

図 5-6 自動車シェアリングの概要（文献[9], https://www.transdevna.com/services-and-modes/autonomous-mobility/より出典）

5.3 車両システムの構成調査

5.3.1 調査対象

以下の表に挙げる自動運転技術を研究開発するメーカーの車両システムを調査した. 調査したメーカーを分類すると, 自動車メーカー, 自動車部品サプライヤ, IT ベンダ, スタートアップの 4 つのカテゴリに分類できる. 以降では構成の違いが分かりやすい代表的な車両システムのみを記載し, 特徴を説明する.

表 5-2 調査対象一覧

業種	会社名	内容
自動車メーカー（10社）	GM	Chevy Bolts をベースとした自動運転車両. Lyft と一緒に 2018 年に公道実験を始める
	Mercedes Benz	2014 年に販売された S クラスの情報から類推する.
	Daimler Truck	ダイムラー社のトラックにおける構成を調査した.
	Audi	A8 に関する構成を調査した.
	BMW	Trendforce による情報から Mobileye と推定する.
	Nissan	Nissan ProPILOT の情報より推定した.
	Ford	自動運転車両を開発中
	Hyundai	EV である IOIQ の自動運転システムを開発している
	SAIC	中国向けには GM とともに開発している
	Changan Motor	GPS+LIDAR+CAMERA による自動運転システムを開発
サプライヤ（5 社）	Bosch	情報なし
	Delphi	Aptiv に関する情報が記載
	Valeo	プライバシーに関する情報が記載
	Continental	ADAS をベースにした自動運転システムを開発中
	Samsung	完全自動運転システムを韓国国内で試験中
IT ベンダー（6 社）	Google	自動運転車両を開発中
	Tesla	Tesla Model S などすでに販売されている車両の一部機能に Auto Cruise 機能などを搭載
	Baidu	米国カリフォルニアなどで走行試験中
	Uber	自動運転タクシーの開発中
	Lyft	自動運転の走行テストを米国内にて実施中
	Waymo	同上

スタートアップ（2 社）	.Commna	一部の車両に後付け可能なユニットにより，完全自動運転を実現するシステムを販売中
	AutoX	LIDAR などの高価なセンサを使用することなく，カメラの画像処理により実現する．

5.3.2 GM(Cruise)

GM が想定する構成は，複数の RADAR と LIDAR とカメラを搭載することにより実現される．その特徴は，Strobe 社の LIDAR を採用することにより，多数の LIDAR を搭載してもなお，価格競争力のあるシステムを構築できる点とされる．

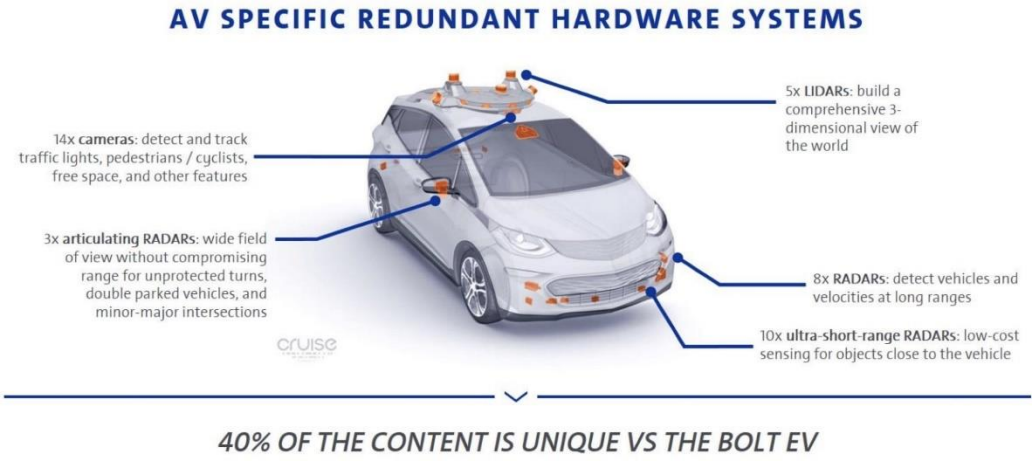


図 5-7 GM(Cruise)が想定する自動運転車両システムの構成
（https://electrek.co/2017/11/30/gm-electric-vehicle-autonomous-driving-tesla/より出典）

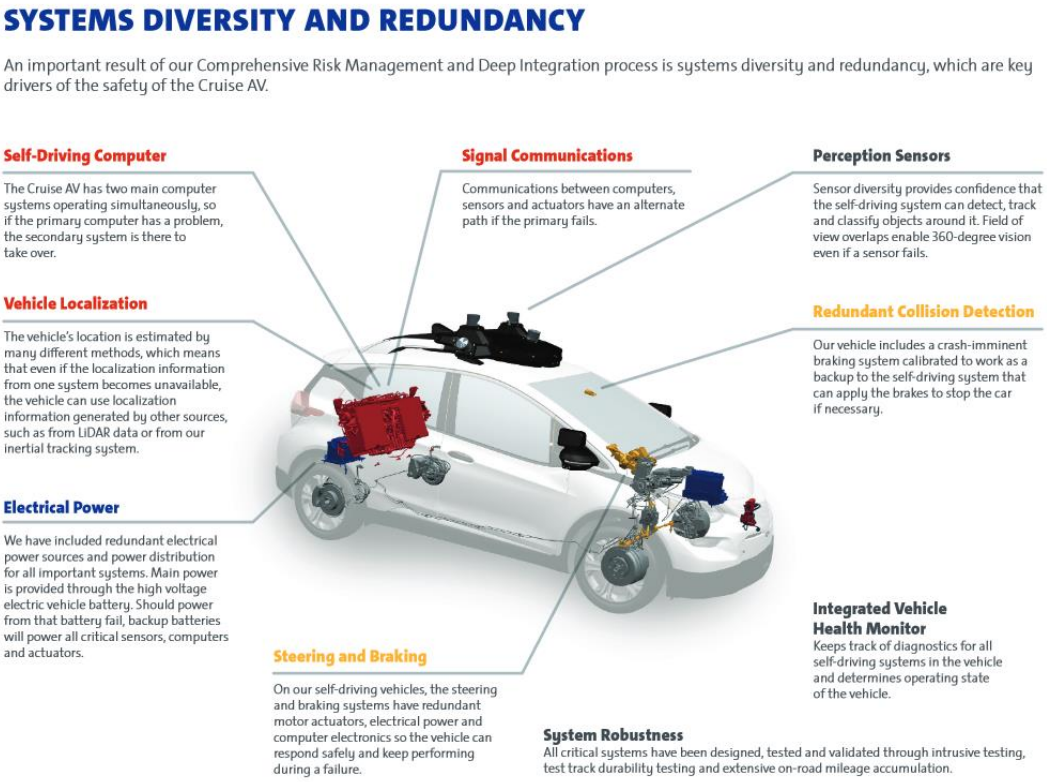


図 5-8 センサの冗長構成

（http://www.gm.com/content/dam/gm/en_us/english/selfdriving/gmsafetyreport.pdf より出典）

図 5-9 Strobe 製の Lidar(https://insideevs.com/wp-content/uploads/2017/12/6.png より出典)

5.3.3 Mercedes Benz

2014 年に発売された S-Class では，下図のような RADAR，ステレオカメラ，超音波センサを要する構成となる．

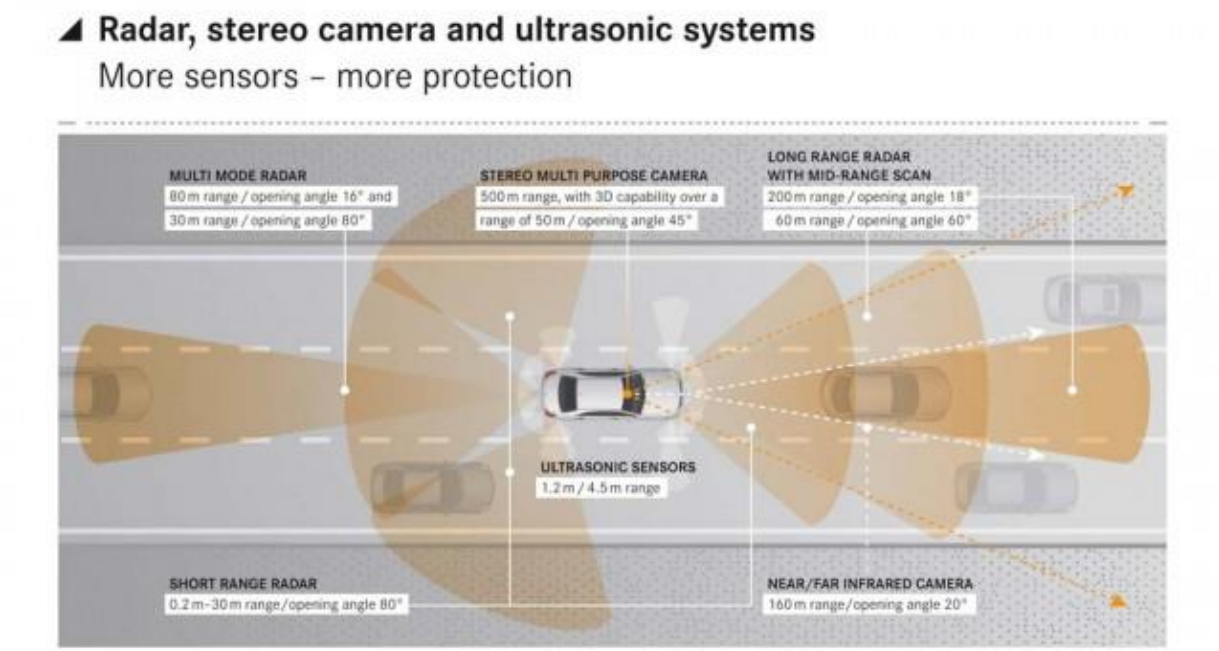


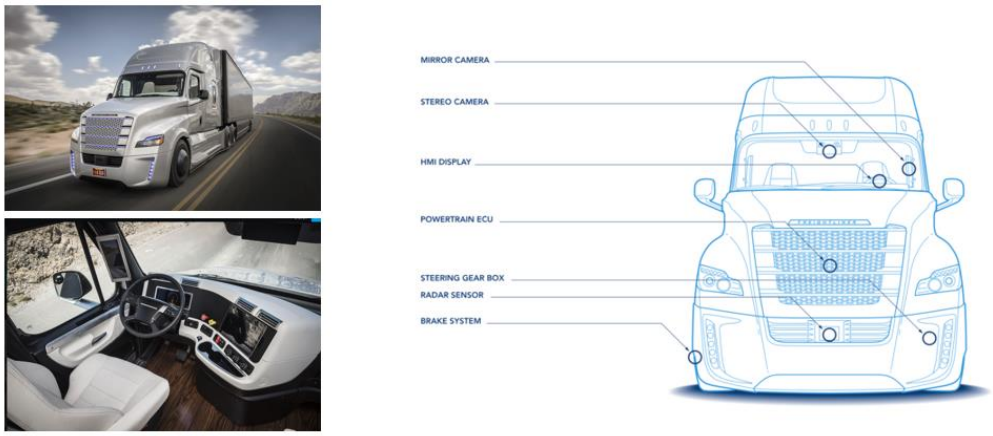
図 5-10 Mercedes Benz のセンサの構成（http://www.extremetech.com/extreme/166598-frankfurt-auto-show-mercedes-shows-off-fully-autonomous-s-class-production-cars-coming-by-2020 より出典）

また，2017 年には，運転席を搭載しない自動運転車のコンセプトを提供することにより，非常に多くの点で驚きがあったが，Lv4 以上の自動運転ではこのような車室空間を提供できる可能性を示した．

図 5-11 運転席のない車両システムのコンセプト（http://cdn.wonderfulengineering.com/wp-content/uploads/2015/01/Mercedes-Benz-F-015-3-610x458.jpg より出典）

5.3.4 Daimler Truck

2015 年，ダイムラーはトラックで，RADAR を搭載した車両にて自動運転の走行テストを実施していることが公表されている．これらの構成から，ステレオカメラや RADAR などを用いていることがわかる．



https://www.computerworld.com/article/2919094/telematics/the-first-self-driving-18-wheeler-hits-the-highways.html

図 5-12 Daimler Truck の構成
(https://www.computerworld.com/article/2919094/telematics/the-first-self-driving-18-wheeler-hits-the-highways.html より出典)

5.3.5 Audi

Audi の場合，LIDAR，RADAR，超音波センサ，カメラの各センサを複数ずつ保持している．これにより，全方位でセンサをカバーすることを実現している．

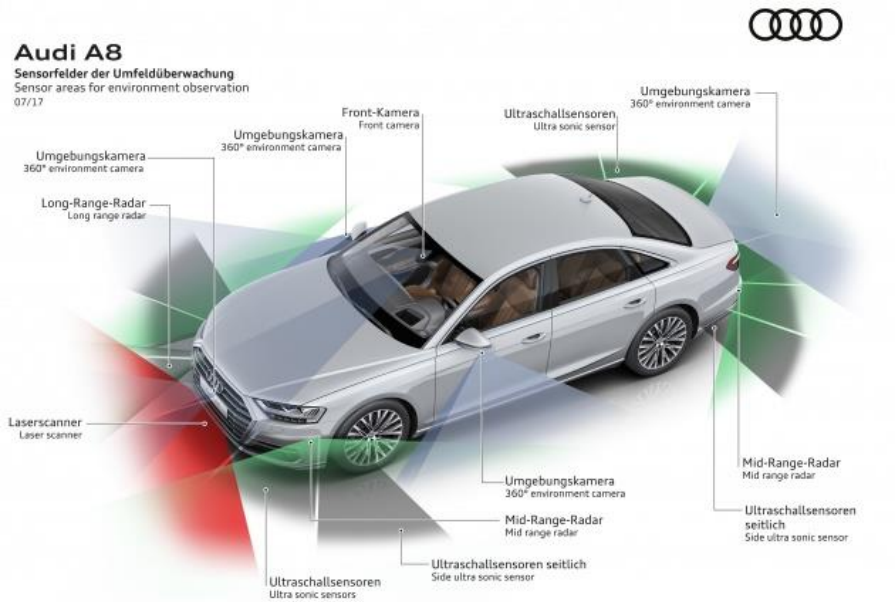
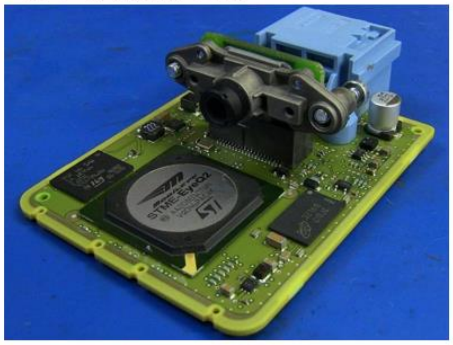


図 5-13 2017 年に発表された Audi A8 の構成(http://www.nydailynews.com/autos/news/self-driving-cars-ready-put-computer-dr-article-1.2320628 より出典)

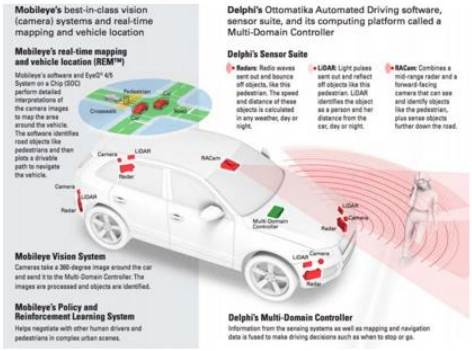
5.3.6 BMW

Trendforce によると，BMW は Mobileye の EyeQ2 を搭載した車両を数多く販売している．今後も，Mobileys と Intel が共同で開発している完全自動運転を目的としたユニットを搭載することが予想される．

- 2017年のTrendforceによると，BMWはMobileyeのEyeQ2を搭載
- 2016年には210万個を超え，テスラの76万個を大きく超える
- Intel-Mobileyeは2021年には完全自動運転を目的としたユニットを発売する予定がある



EyeQ2の写真



Mobileyeが想定するシステム構成

図 5-14 BMW が採用する Mobileye の構成
（https://www.computerworld.com/article/3181332/computer-processors/intel-mobileye-merger-to-boost-bmws-self-driving-car-plans.html より出典）

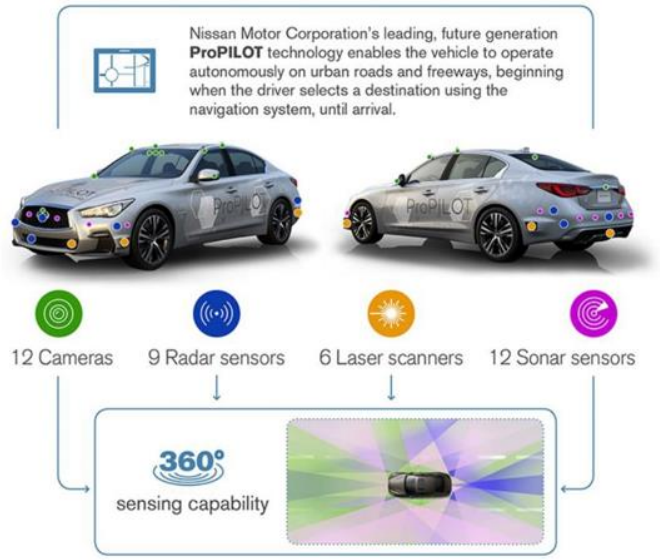
5.3.7 Nissan

日産は自動運転技術を ProPILOT として様々売り出している．現在では，セレナなどに，レーンキープアシスト機能などを搭載しており，2020 年には，下図に示すような構成で完全自動運転を目指すことが公表されている．

●多数のセンサを搭載することにより全方向監視

●構成

- 12個のカメラ
- 9個のLADAR
- 6個のLIDAR
- 12個のソナー



http://autobuzz.my/2017/11/21/nissans-propilot-technology-available-real-world-use-2020/

図 5-15 Nissan PROPILOT の構成（http://autobuzz.my/2017/11/21/nissans-propilot-technology-available-real-world-use-2020/より出典）

5.3.8 Hyundai

Hyundai が，2016 年 11 月に発表した自動運転車両 IONIQ については，RADAR(Long, Middle レンジにより前方を監視するのと同時に，後方の RADAR を搭載している．また，その他カメラを搭載することにより，前方の障害物を検出するカメラや車線逸脱防止(LDW 用)のカメラなどにより進行方向の情報を収集する． 尚，カメラはステレオカメラや，2020～2021 年に実用化することを目論んでおり，研究開発が進められている．

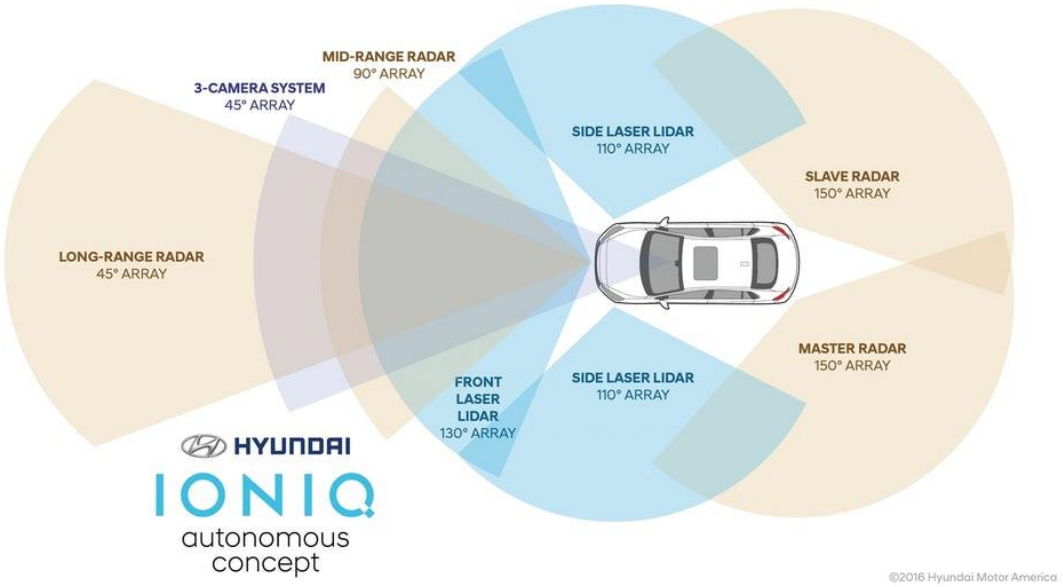


図 5-16 Hyundai IONIQ に搭載されるセンサの認識範囲（https://newatlas.com/hyundai-autonomous-ioniq-concept/46489/#p435975 より出典）

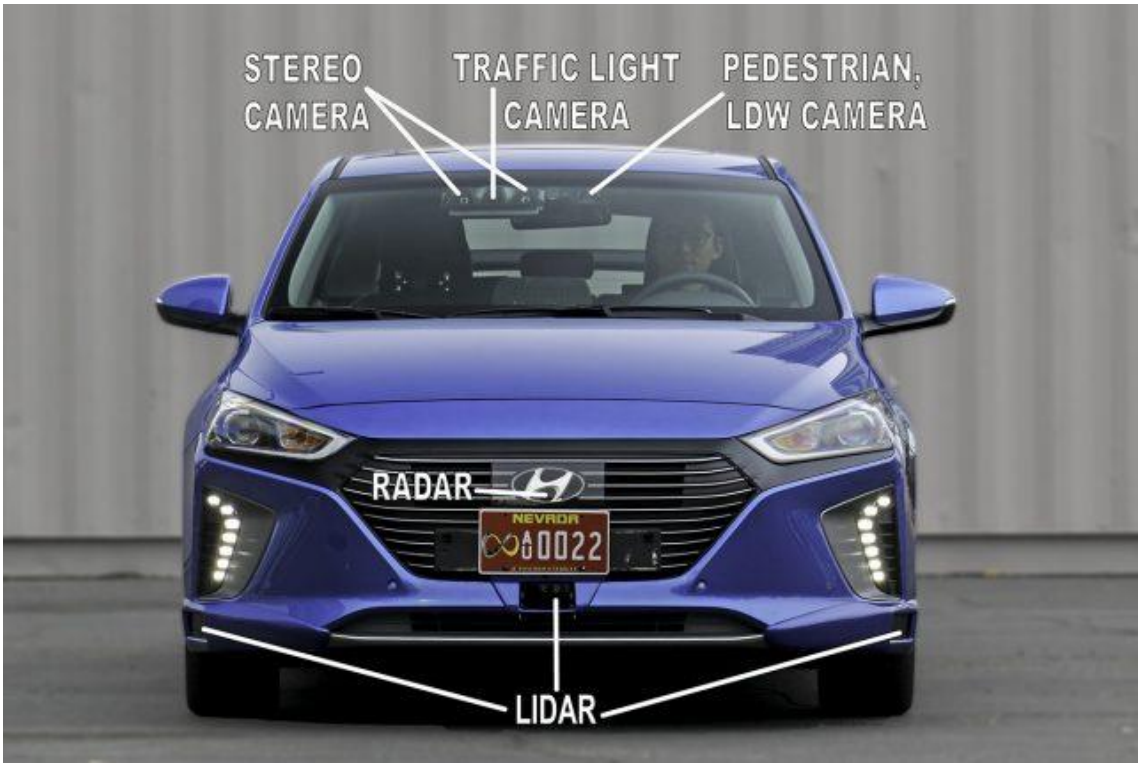


図 5-17 Hyundai IONIQ に搭載されるカメラ（https://www.extremetech.com/extreme/241242-hyundai-ioniq-self-drive-car-flawless-right-turns-no-danger-speeding-tickets より出典）

5.3.9 Delphi(Aptiv)

2017 年 3 月より部品サプライヤ Delphi の自動運転システムは Aptiv というブランドで展開されている. Aptiv は，以下の図 5-18 に示すような構成を想定している. 車両システムに搭載するセンサ類は他社と同様の構成であることが判る.

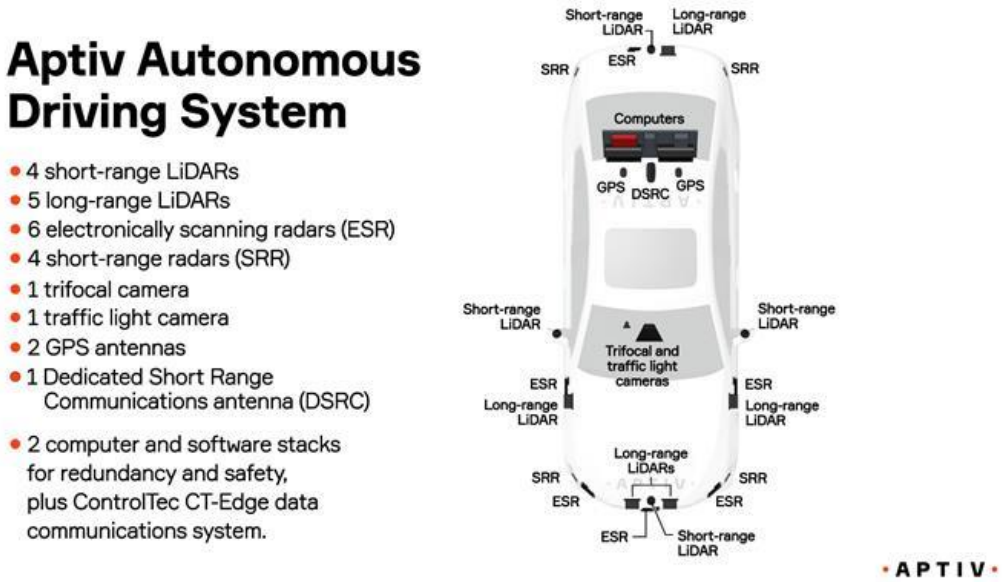


図 5-18 Aptiv の自動運転車両の構成（http://safecarnews.com/aptiv-reveals-details-of-its-autonomous-driving-sensor-fusion/より出典）

5.3.10 Tesla Model S

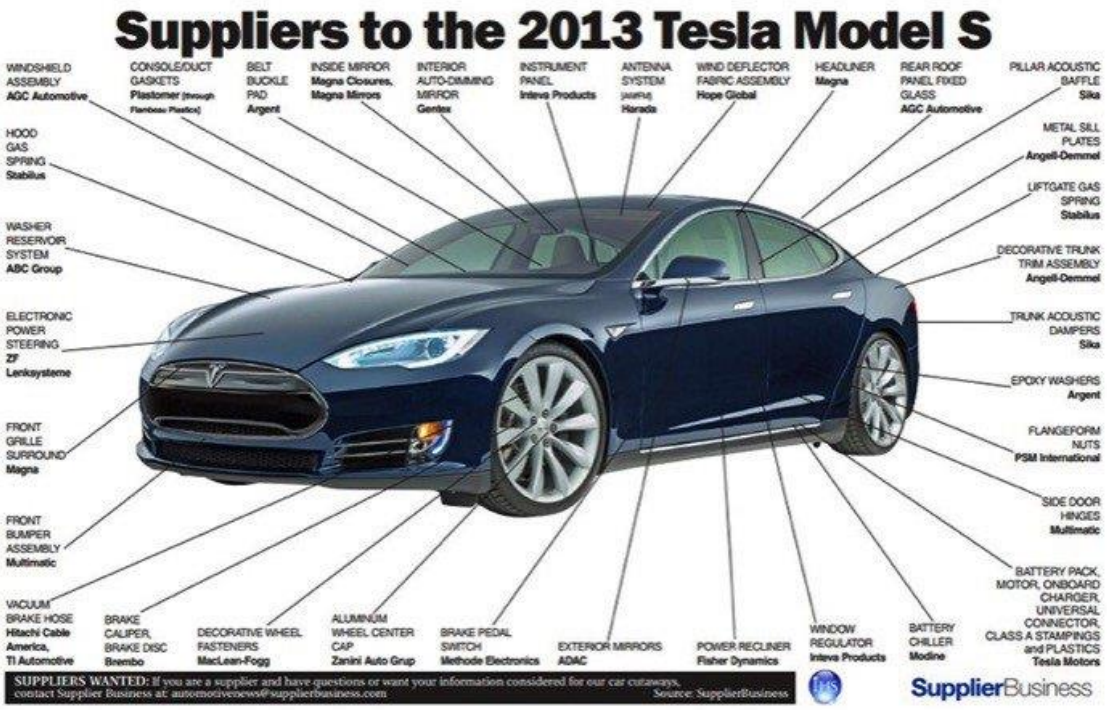


図 5-19 2013 年に発売された Tesla Model S の構成
（https://www.enterpriseirregulars.com/101595/innovation-driven-disruption-automotive-value-chain-part-3/より出典）

5.3.11 Uber

サンフランシスコでの実験車両の構成から車両システムがわかる．基本的な構成は他の車両メーカーと同様であり，とてもシンプルな構成を採る．

- 2016年，Uberの実験車両@サンフランシスコ
- 構成
  - Volvo XC90を使用
  - 前方に360度RADAR
  - 360度の3D LIDAR
  - 前方カメラ
  - GPS
  - ワイヤレス通信

https://techcrunch.com/2016/12/14/ubers-self-driving-cars-start-picking-up-passengers-in-san-francisco/

図 5-20 Uber の構成（https://techcrunch.com/2016/12/14/ubers-self-driving-cars-start-picking-up-passengers-in-san-francisco/より出典）

5.3.12 後付け可能なシステム

5.3.12.1 Comma Openpilot

既存する自動車に対して，約 800 ドルのハードウェアコストのみで，自動運転車両に改造することが出来るシステムを開発した．このシステムは，単眼カメラとオープンソースを用いて開発されるものであるが，そのプラットフォームは，Commma が開発した Openpilot を使用している．これは，自動車メーカーが設計するとても高価な自動運転システムとは対極にあり，低価格に自動運転システムを実現できる可能性を示した．

Figure 1 Comma one(https://commaai.blogspot.jp/より出典)

5.4 自動運転車両の制御対象と機能

自動運転システムの多くは，以下のような認知(Sense)，判断(Understand)，操作(Act)に分類される．認知においては，自律走行を実現するために，GPS，カメラ，RADER，LiDAR，超音波センサなどを搭載することが想定されている．この他にも，V2X 通信などを行う場合には，通信モジュールが搭載されることが予想される．

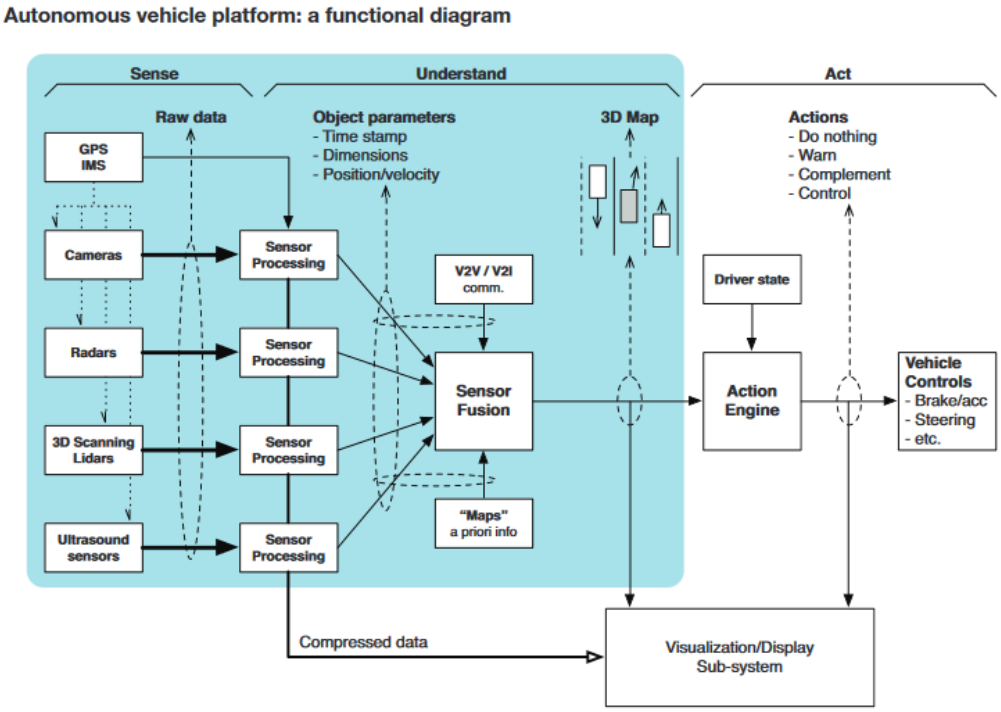


Figure 1. A functional view of the data flow in an autonomous car's sensing and control system.

図 5-21 自動運転システムの構成概要(http://www.ti.com/lit/wp/sszy010a/sszy010a.pdf より出典)

5.4.1 自動運転車両システムの機能

自動運転車両システムが搭載する機能としては，以下のような機能で構成されることが予想される．各機能の詳細については，以降で説明する．

表 5-3 自動運転車両システムの機能

レベル	機能	内容
全共通	無線通信によるプログラムアップデート	無線通信を介したソフトウェアアップデート機能．この機能を通じて，プログラム上の問題点の修正や機能アップデートを行うことを想定している．一般的に Over The Air の頭文字をとり，OTA と呼ばれる．
レベル 2	レーンキープアシスト	カメラなどの一部のセンサを用いて，レーンを読み取り，車線の逸脱などを検知する機能のこと．尚，車線を逸脱した場合の動作については各社異なる．
〃	自動ブレーキアシスト	カメラや超音波センサなどを用いて，車両前方の障害物を認識し，自車両がぶつからないようにブレーキを作動させる機能を指す．
〃	駐車支援	駐車支援としては，カメラなどの情報を用いて，運転者に代わり，ハンドル操作などを行うことが
レベル 3 以上	環境認識	搭載されるセンサ情報から自動運転車慮の位置推定を行う．位置推定を行うためには，自動運転車両周辺の位置推定を行うことが重要となる．
〃	自車位置推定	センサから読み取った環境情報から自車両の位置の状態を推定する機能を指す．
〃	パスプランニング	推定された自車位置や環境情報から，走行するべき動作軌道を決定し操作する手法である．
〃	バレーパーキング	決められた位置に対して，
〃	V2X 通信機能	他の車両との調停を行い，それらの機能を実現することになる．
〃	電子牽引機能	トラックを物理的ではなく，論理的に連結することにより，先頭車両以外の後続車両については無人で牽引することが可能なトラックの機能を指す．
〃	運転者の状態推定	レベル3では，運転者と制御システムが連携を行い，制御主体を切り替えることが想定されている．この位置推定に対して，これまでの自動車からの

5.4.2 Over the Air (OTA)

近年，自動車業界でも無線通信による制御用コンピュータのプログラムアップデート手段として Over The Air(OTA)の導入が検討されている．OTA を用いることにより，出荷後に発見された脆弱性に対する更新プログラムの配送が可能になる．今後，自動運転車両においては必ず導入される機能の一つになると考えられている．
以下の図では，様々な脅威に対抗する手段として OTA の有効性が言及されている．この記事では，2025 年には OTA が 990 億ドル規模の市場になることが予想されている．

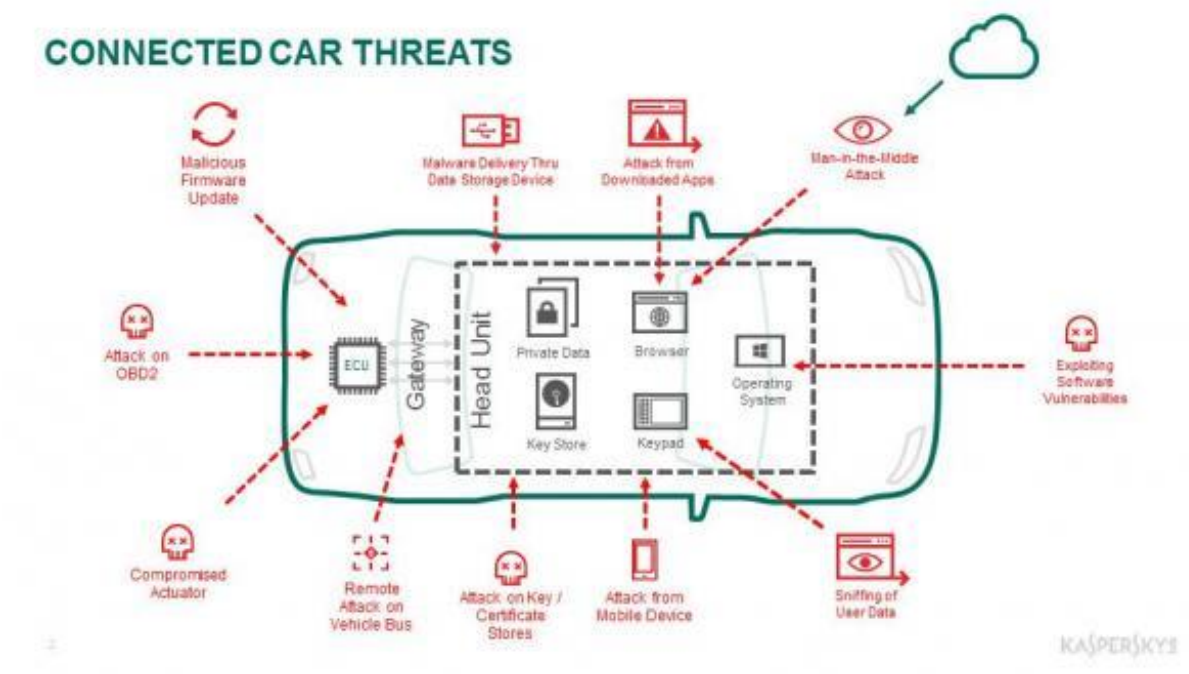


図 5-22（http://www.eenewsautomotive.com/news/airbiquity-introduces-platform-secure-over-air-ota-software-updates-ces より出典）

5.4.3　レーンキープアシスト機能

レーンアシスト機能は，車の車線維持支援システムのことであり，車体の前方に備え付けられた単眼カメラで車線を検知し，車が車線の中央から離れようにドライバーを支援する．また、車線から外れそうになると，ドライバーに対しステアリングの振動，ブザー音や画面表示などで警告を行う機能のことである．

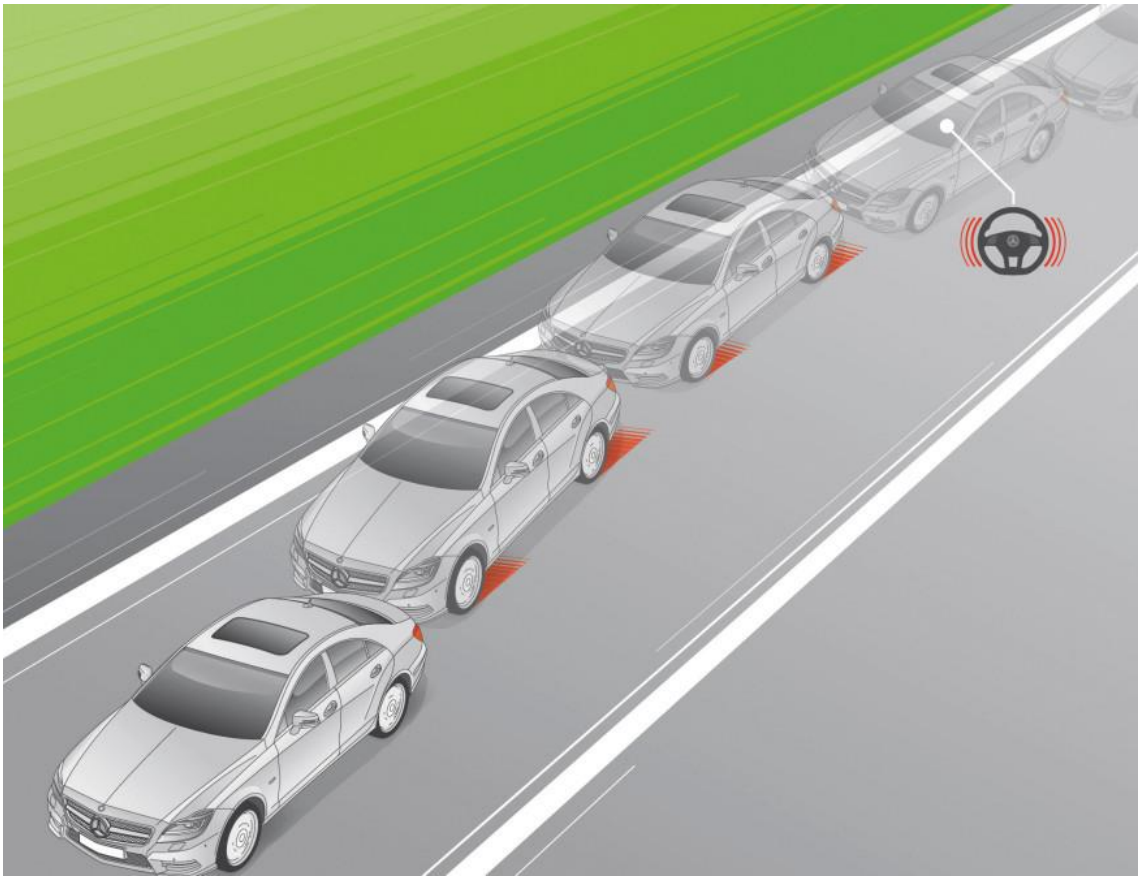


図　5-23 Lane Keep Assist 機能（文献 12 より出典）

5.4.4　自動ブレーキアシスト機能

自動ブレーキアシスト機能は，高度運転支援機能の一つであり，カメラや超音波センサなどを用いて，車両前方の障害物に追突しないよう，運転者への注意喚起やブレーキの作動などを行う機能を指す．

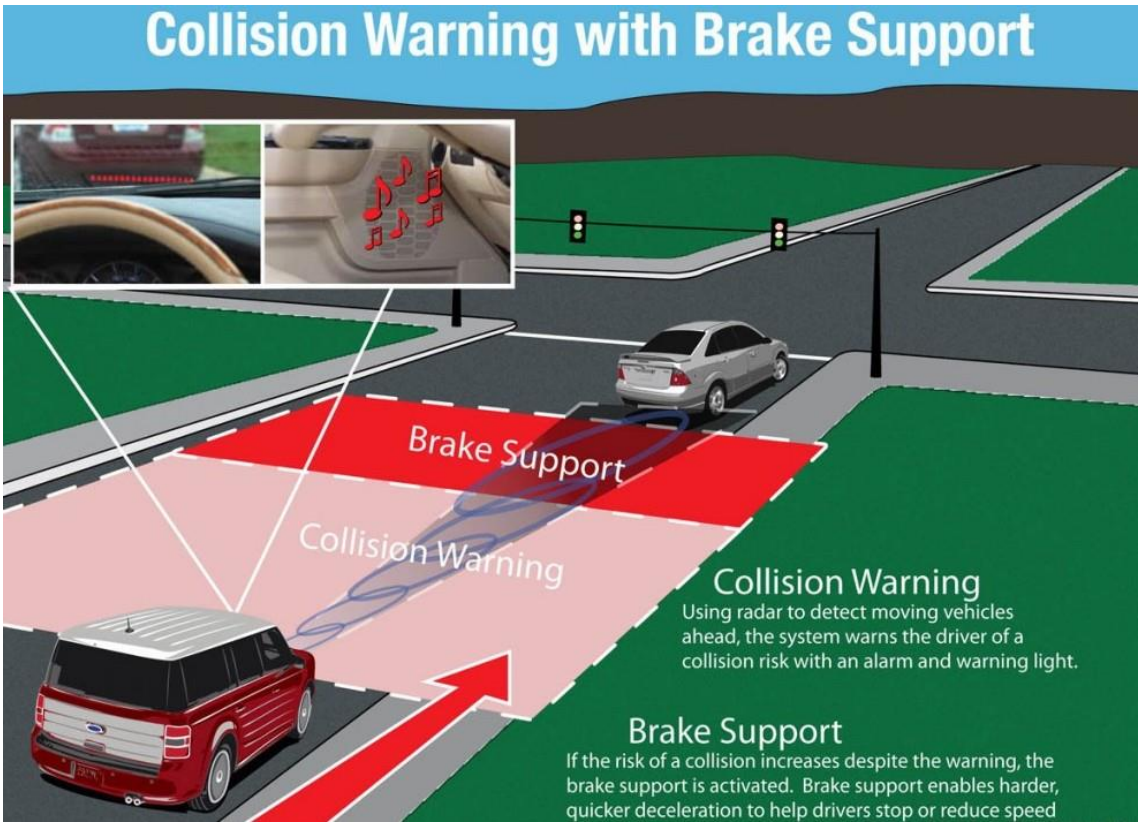


図 5-24 自動ブレーキアシスト機能の例（文献 12 より出典）

5.4.5 自動駐車機能

自動駐車機能は，運転者が駐車位置付近に車両を動かした後に車両の駐車位置を決める．その後，車両に搭載されるカメラや超音波センサなどを用いて，車両システムが目的の駐車位置に駐車できるよう制御を行う．これらの駐車支援機能のことを自動駐車機能と呼ぶ．

図 5-25 自動駐車システムの概要（文献 13 より出典）

5.4.6 パスプランニング機能

パスプランニングには，グローバルパスプランイングとローカルパスプランニングの 2 つ存在する．グローバルパスプランイングとは，いわゆるカーナビ上の経路探索と同様で，自車位置から目的地までの経路探索を表す．ローカルパスプランイングとは，センシングした環境情報から自車位置を推定した後で，自身が走行すべき経路を決定する手法のことである．このため，ローカルパスプランイング機能では自車両の周辺環境を認識し，障害物や他車両の位置などを把握しながら，自身が道路上のどのようなパスを走行するかを決定する機能を指す．いずれの機能も，Lv5 の完全自動運転を実現する場合には，必ず搭載される機能の一つとなる．

5.4.7 バレーパーキング機能

現在のバレーパーキング(バレットパーキング)は，高級ホテルなどによくあるサービスで，宿泊者がホテルに乗りつけた自家用車を自分で駐車場に駐車するのではなく，ホテルのドアマンなどに依頼することにより実現される．今後は，所有者のスマホから指示を行うと，自動運転車両が自動でホテルや郊外の駐車場に移動し駐車することが期待されている．また，現在の自動駐車機能との違いは，運転者がいなくても実現できる点であり，都市交通の観点でも都市部に多くの駐車場を配置せずとも，車両を郊外の駐車場へと自動で移動できるなど，渋滞緩和のメリットがある．

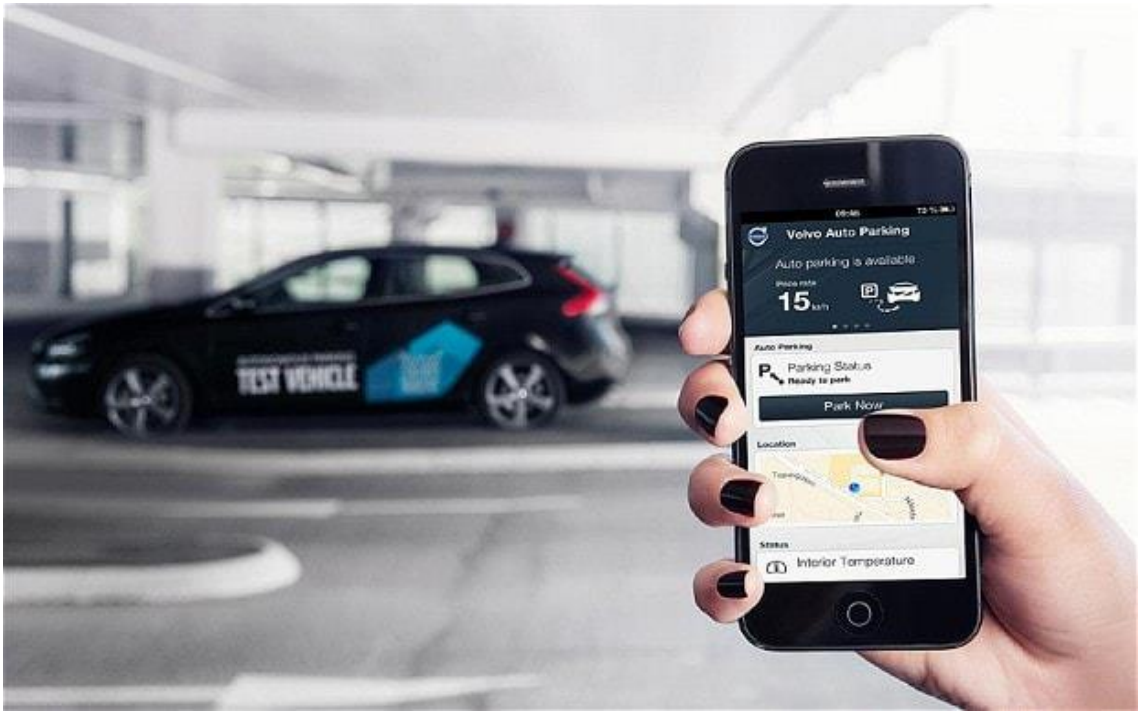


図 5-26 バレーパーキング機能のイメージ(文献 14 より出典)

5.4.8 隊列走行機能(V2X 通信機能)

隊列走行機能は，V2V 通信などを介して，他車両と調停しながら，最適な経路を走ることを可能にする．特に，V2X 通信機能は，自動運転システムのいくつかのサービスを実現するために必要となる機能である．例えば，効率的に高速道路へ合流したり，車線変更したりするには，他車両と V2V 通信を介して調停する必要がある．

5.4.9 運転者の状態推定機能

Lv3 では，運転者と制御システムの間で車両制御の主体を行き来することにより実現される．このとき，運転者が居眠りしているなどの場合に，制御主体を運転車に移してしまうと，事故につながる可能性がある．このため，Lv5 の完全自動運転ではなく，Lv3 のような車両システムの場合には，運転者の状態を把握した上で，制御主体を決定する必要がある．

5.4.10 機能のまとめ

これらの機能が搭載されるサービスをまとめると，以下の表のとおりになる．これらの表が示すように，特定の自動運転サービスのみに必要となる機能やレベル 3 以上の機能に包含される一部の機能については分析対象から除外した．これは，冗長的な分析を避けるためである．

表 5-4 共通機能まとめ(分析対象は〇とし，分析対象外は×とする)

レベル	機能	自動運転バス	貨物牽引車両	カーシェア	備考
全共通	無線通信によるプログラムアップデート	〇	〇	〇	
レベル 2	レーンキープアシスト	×	×	×	パスプランニングに含まれる
〃	自動ブレーキアシスト	×	×	×	パスプランニングに含まれる
〃	駐車支援	×	×	×	バレーパーキングに含まれる
レベル 3 以上	パスプランニング	〇	〇	〇	※隊列走行に含まれる
〃	バレーパーキング	〇	〇	〇	
〃	隊列走行 (V2X 通信機能)	〇	〇	〇	
〃	電子牽引機能	✖	〇	〇	
〃	運転者の状態推定	〇	〇	〇	※今回の分析では対象外とする．

5.5 車両システムの類型化

前述するように主要な自動運転システムの構成調査の結果より，車両システムを類型化する．まず，前述の調査の結果，スタートアップ企業が開発している車両システムについてはコスト効率化を図るために試作されているものが多く，自律走行は行うが，車車間連携などを対象とはしていないため，自動車メーカーや部品サプライヤ，IT ベンダが開発している自動運転車両で機能としては包含されることから，類型化の対象から除外した．

我々の類型化のアプローチは，車両システムとサービス/機能の 2 つに分類し類型化する．まず，車両システムについては前述の調査の結果より， 1 台の車両システムを仮定する．

我々が想定するシステムでは，下図のような構成をとる．この車両システムでは，GPS，カメラ，RADAR，LIDAR，超音波センサを搭載し自律走行を実行する．その上で，V2X 通信により，他車両の状況や路側機からの情報を得ることにより，他車両と強調して，事故の少ない効率的な協調制御を実現する．また，このシステム内には地図データベース（DB）を保持し，OEM が有するサーバーと連携して，ソフトウェアを更新し，スマホからバレーパーキングの制御や制御システムの起動を行えるなどの機能を備えるものである．このように自動運転システムに入力される情報を資産として置き換えることにより，類型化されたシステムにて脅威分析を行う．より詳細なシステム構成図については図 5-28 に示す通りである．この図は，車両自身が，運転手の状態を把握した上で，自動運転のモードを切り替えるなど行える機能も搭載しているが，Lv4 以降ではこれらの機能は不要になると想定される．

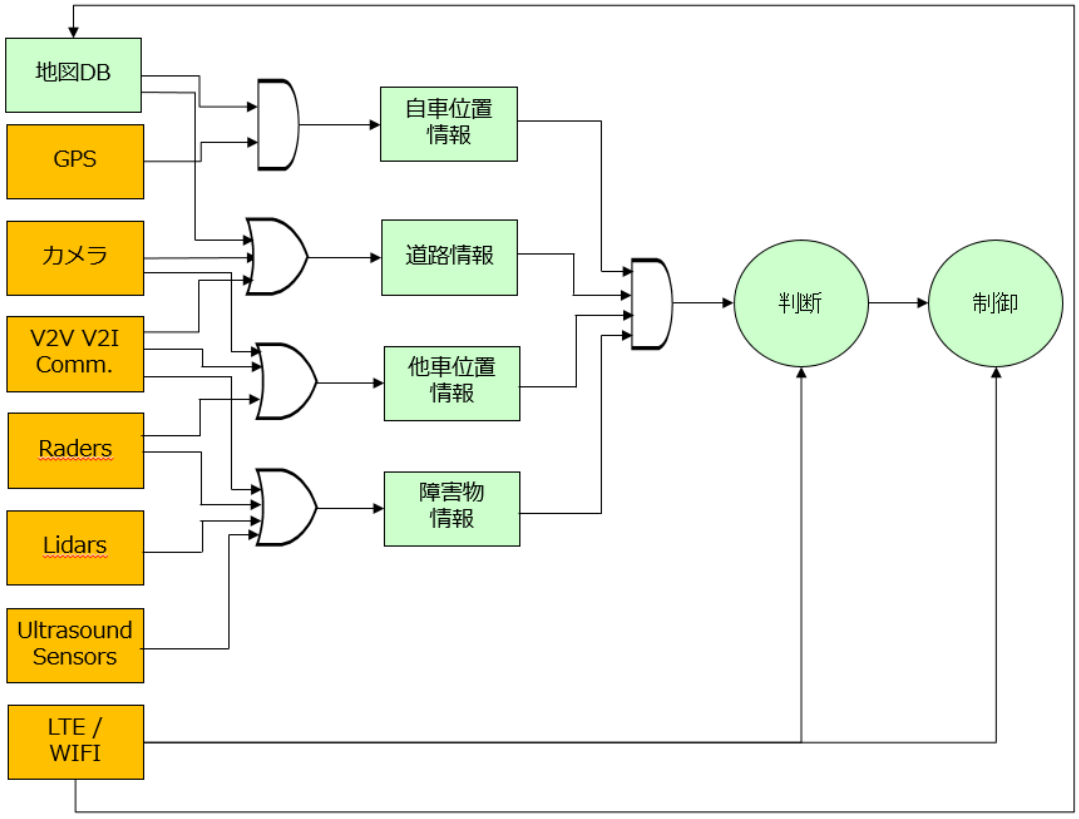


図 5-27 類型化された自動運転システムのシステム構成図

次に，資産となりうる各情報について説明する．

5.5.1 自車位置情報

自車位置情報は，地図 DB と GPS による自車位置情報のマッチングにより決定されるものである．このため，地図 DB が誤り，GPS からの情報を受信できないと自車位置を把握することはできない．その一方で，自動走行システムは外界環境を認識することにより自律走行する機能が搭載されている．例えば，トンネルの中などの GPS などの電波を受信できないような場合にでも自律的に走行できなければならない．このため，自車位置情報が把握できなくても安全に走行することが出来るものと想定する．さらに，南極や北極圏などでは自車両の位置が正確に把握できないなども考えられることより，GPS の情報を信頼して走行する車両についてはありとあらゆる情報を考慮して走行することが難しいと考えられる．

5.5.2 道路情報

自動運転システムは，自車両の周辺の道路情報を利用して，走行すべきルートを決定する．これらの自車両周辺の道路情報は，地図 DB，カメラ，V2I を使用して環境認識をしつつ走行すべきパスプランニングを決定する．これらの情報が突如として喪失してしまう場合には，車両走行に支障をきたす．つまり，自動運転システムとしては，これらの情報は必ず必須であり，完全性が要求される．

5.5.3 他車位置情報

V2V 通信を用いて他車位置情報を獲得することになる．フォールトオペラブルの観点からも，V2V 通信だけを信じることは非常に難しい．例えば，DoS 攻撃などにより V2V 通信が邪魔される場合でも，他車両との位置関係を認識し走行する能力が必要になる．この場合，他車両との位置関係を把握するには，LIDAR，超音波センサあるいはカメラなどを用いて，位置関係を把握する．このため，これらの情報が成り済まされると，意図しない挙動をすることになる．

5.5.4 障害物情報

自立が必要となる自動運転システムでは，カメラや LIDAR，超音波センサ，RADAR などを駆使して，障害物の情報を獲得し，パスプランニングを決定するための障害物情報である．車両システムごとにどのセンサを用いるかは異なるが，各センサが取得した障害物情報を利用して，自動走行システムは走行するべきパスを決定する．つまり，これらの情報が改ざんされたり，成り済まされたりする脅威が発生すると，自車両及び周辺の車両や人の安全性を侵害する可能性がある．

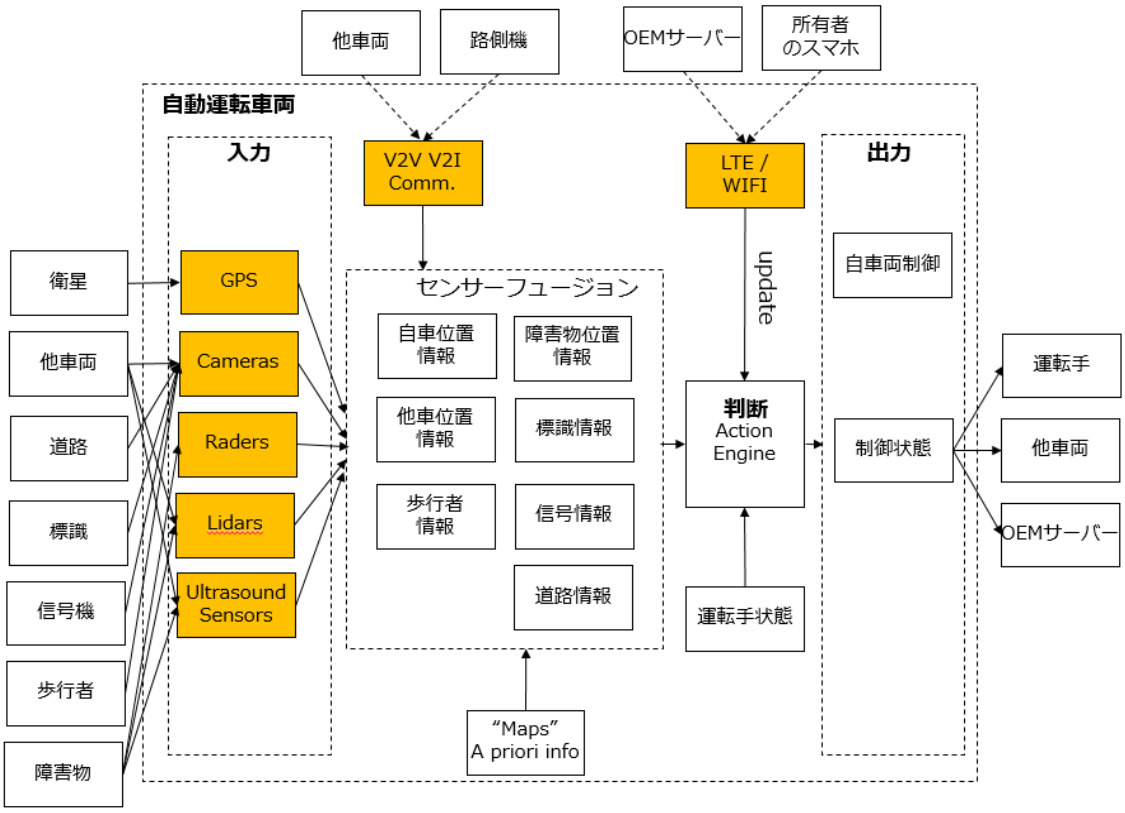


図 5-28 分析対象となる自動運転車両

この車両システムにおいては，以下の表のような情報を各センサや通信を通じて入力することにより，自動運転の制御を実現するものである．尚，電子車両牽引に用いるマーカについては，LIDAR かカメラ，V2V の通信のいずれかにより実現されるものであり，この点はトラックであろうが，一般車であろうが変わらないものとして扱った．また， LTE 通信により，OEM サーバーとやり取りする情報（例えば，使用履歴）については，自動運転車両が適用されるサービスに応じて，やり取りする情報が異なる．例えば，一般車両の場合はよくとおる道や走行時のドライバの癖や各自動車の診断情報などを送ることになるが，乗り合いバスなどでは，それ以外にも乗客の情報などの個人情報(PII)をサービスプロバイダーに提供するなどが考えられる．

表 5-5 自動運転車両が入力するデータ

		静的	センサ				車外通信	
		地図 DB	GPS	カメラ	RADAR	LIDAR	V2V	LTE (WiFi)
制御	自車位置	✔	✔					
	他車位置		✔	✔	✔	✔	✔	
	標識	✔		✔				
	信号			✔			✔	
	障害物			✔	✔	✔	✔	

	道路		✔	✔		✔		
前方追従	マーカ			✔		✔	✔	
プライバシー	使用履歴							✔

✔:使用する可能性のあるデータ

5.6 サービスの類型化

次に，自動運転システムの主要な導入シナリオより，サービスに対して類型化を実施する．類型化されたサービスは，大きく 2 つに分類される．
まず，1 つ目に自動走行車両の基本機能である．これらは，サービスによらず共通の機能としてすべての自動運転車両に共通するサービスと考える．例えば，電子牽引などが挙げられる．電子牽引は，トラックなどで最初に導入される予定があるものの，一般車両にも導入されることが考えられるなど，共通的な基本機能として定義できる．

表 5-6 共通サービス

共通サービス名	説明
OTA(Over The Air)	OTA による無線通信のリプログラミング機能のこと
電子牽引	高速道路や専用道路における車両間の電子連結を用いた自動走行機能のこと
バレーパーキング	自動駐車機能のこと
隊列走行（V2X 通信機能）	V2V などを用いて，車群を形成して走行する機能のこと

次に 2 つ目として， バスなどの公共的な乗り物を想定する．これは個人所有の自動運転車両ではなく，サービスを運営する事業者が所有する車両にユーザーとして乗員が乗り込むことを想定する．これらのサービスでは課金情報がやり取りされるほか，誰が乗り込んだかの乗員のプライバシーなどに関連する．

6　脅威分析

6.1 脅威分析のフレームワーク

本節では，類型化された自動運転車両に対する脅威分析を行う．尚本調査で扱う範囲は，SAE が定めた J3061 では，システムアーキテクチャの脅威分析と同様である．特に，今回の脅威分析については，我々が定義した自動運転車両とサービスに対する脅威を洗い出すことを目的としている．

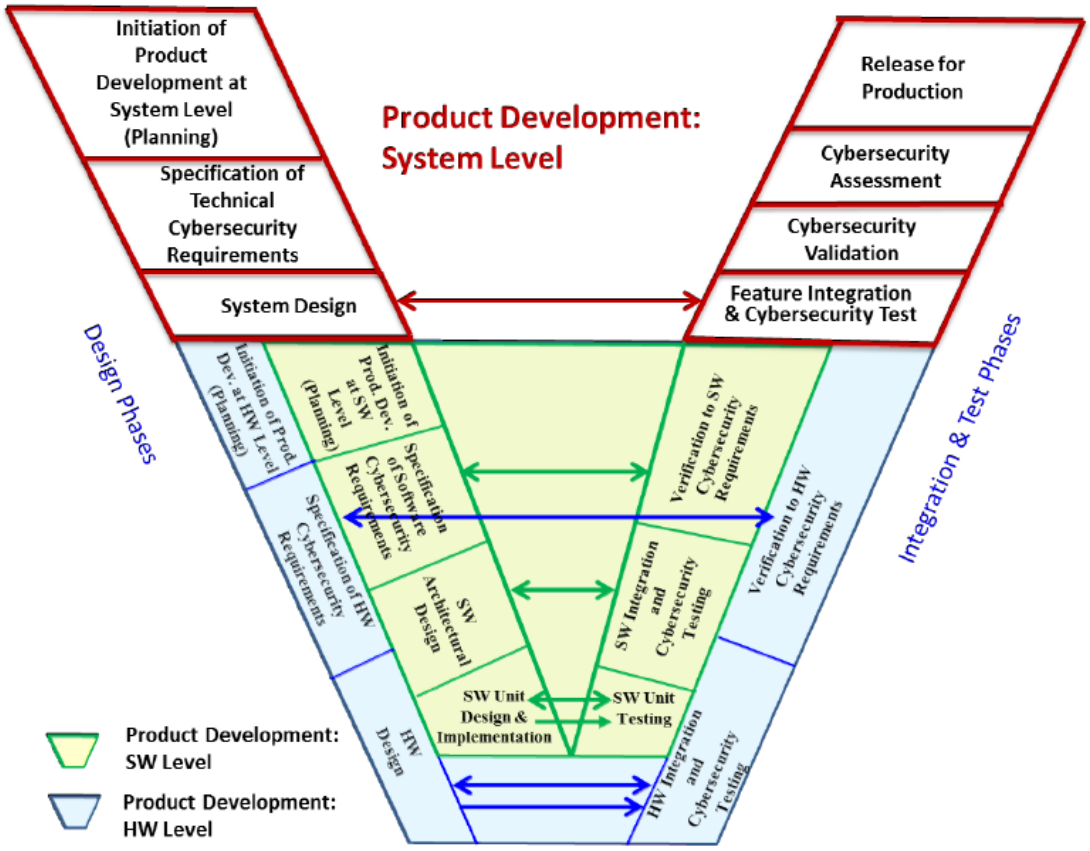


Figure 5 - Relationships between product development at the system, hardware, and software levels

図 6-1　J3061 にて定められる製品開発時の開発プロセス（SAE J3061 より出典）

6.2 脅威分析のアプローチ

本分析では，類型化された自動運転システム及びサービスに対して，脅威分析を実施する．この脅威分析では，脅威の網羅性を上げるために，マイクロソフト社にて提案された STRIDE を適用した．STRIDE では，以下のガイドワードを用いて，資産に対する脅威を洗い出すことを目的とする．尚，資産については類型化する段階で導出されているため，容易に当てはめることが可能である．また，STRIDE で使用するガイドワードについては，以下のとおりである．

表 6-1 STRIDE のガイドワード一覧

ガイドワード	説明
Spoofing（なりすまし）	各機器や人になりすます脅威
Tampering（改ざん）	機器を改造や改ざんすることにより実現する脅威（機器の設置や機器の除去などを含む）
Repudiation(否認)	サービスや機器の利用を否認する脅威
Information disclosure（情報漏洩）	秘密情報が暴露される脅威
Denial of service(妨害)	サービスを妨害する脅威
Elevation of privilege(権限昇格)	権限が昇格し，本来は利用できないサービスや機器を使用することが可能になる脅威

また，STRIDE は資産を起点に脅威分析を実行するため，網羅性が確保できない可能性がある．このため，今回はシステム構成図を用いて，脅威エージェントとなりうるコンポーネントを洗い出すことにより，脅威の網羅性を上げるよう試みた．尚，以下の表に示す各ガイドワードはシステム構成図より導出されたデータフロー図のデータフロー，データ保持，処理，相互作用者/機器，内部機器に対して適用した．

表 6-2 STRIDE のガイドワードの適用箇所

ガイドワード	データフロー	データ保持	処理	相互作用者/機器	内部機器
Spoofing（なりすまし）			X	X	
Tampering（改ざん）	X	X	X		X
Repudiation(否認)		X	X	X	
Information disclosure（情報漏洩）	X	X	X		X
Denial of service(妨害)	X	X	X	X	X
Elevation of privilege(権限昇格)			X		

洗い出された脅威の重要度については，NIST800-30 の脆弱性マトリクスを用いた．これは，今回使用した脅威分析がシステムアーキテクチャレベルの脅威分析であり，脅威の発生確率や影響度についてはシステムの詳細が固まってから行うことが多いためである．

6.3 想定する攻撃

本分析では，まずは攻撃者を想定するために，想定する攻撃者及びその攻撃者の能力について以下の通りとした．

6.3.1 想定する攻撃者

自動運転システムに対する脅威を洗い出すために，まず，攻撃者のモデルを定義する．本脅威分析にて想定する攻撃者は，以下の表に示すとおりである．これらの攻撃者は，専門知識に対して精通しているものとする．特に，自動運転車両だけではなく，情報セキュリティなどの技術にも精通しているものとする．

表 6-3 攻撃者のモデル

攻撃者の分類	モチベーション	ゴール
政府	金銭，影響力	情報収集，
犯罪者	金銭	金銭情報をせしめる，ゆする
コンペティタ	金銭	競合の経済活動の妨害，企業の評判を落としめる
内部犯行	興味，スパイ活動	経済的な利益，組織へのダメージや報復
ユーザー	意図しない行動	何が起こるかわからないために，問題を引き起こす行動をとる
ハクティビスト	能力の誇示	能力を誇示した結果，攻撃された企業の評判を貶める

6.3.1 攻撃のゴール

自動運転システムに対する攻撃のゴールは主に 2 つが考えられる．1 つは，車両システムの安全性や信頼性に対する脅威であり，攻撃者は車両に乗車する人間や攻撃対象となる車両周辺の人間の健康や安全性を侵害する攻撃を目的とする．もう 1 つは，複数の攻撃者が連携する大きな組織になると，金銭的にも潤沢であり，大規模に物理的な攻撃を仕掛けることも可能になる．このような場合には，企業価値を損ねるようなコンペティタやハクティビストによる大規模な攻撃を引き起こすことが可能になる．

6.3.2 想定する攻撃者の能力

本脅威分析では攻撃の機会については限定しないものとした. 自動車の多くが自動運転車両になったとしても, 公共の駐車場に止めたりすることが想定される. このため, 攻撃者が攻撃するチャンスは従来と変わらず存在するものと仮定した.

その上で, 攻撃者が備える能力は, 攻撃対象となる車両, あるいはインフラなどに対して常に自由に接触できる可能性がある. 例えば, 夜間の交通量の少ないときに, 路側機になりすました脅威エージェントを設置することが出来ることを想定している. また車両に対しても同様とし, 駐車場に停車された場合には誰でも容易にその車両に物理的にアクセスする可能性があるものとして扱う.

本脅威分析にて想定する脅威は, 以下の 3 つの攻撃に分類される. 1 つ目は, 遠隔攻撃であり, 主に, Wi-Fi や LTE などの物理的に遠い距離から車両に対して影響を及ぼすことが出来る無線通信に対する攻撃である. これらの無線通信規格は, IP ベースで構成される通信プロトコルであり, 通信事業者の設定ミスなどにより, 攻撃が地球の裏側からも実行することが可能となる. 2 つ目に, 近接攻撃は, 車両には直接物理的に接触はしていないが, 車両が行き来する道路や駐車場の上から, ターゲットとなる車両システムに対して, 任意の攻撃を行う攻撃である. この攻撃の対象は, 車両に備えられる無線通信モジュールや自動運転で使用するセンサを対象としている.

表 6-4 攻撃者の能力 1 (ターゲットへのアクセス)

攻撃者の分類	説明	ターゲット
遠隔攻撃	攻撃対象に対して, 物理的に遠い距離から攻撃する.	無線通信(Wi-Fi, LTE など)
近接攻撃	攻撃対象に対して, 物理的に近い距離から攻撃する.	無線通信及びすべてのセンサ(Wi-Fi, Bluetooth, LTE, カメラ, LIDAR, RADAR)
物理的攻撃	攻撃対象に対して, 物理的に接触した上で攻撃を行うことになる.	無線通信, すべてのセンサ及び車両や装置など

本分析では, 車両への攻撃は, いくつかのステップで行われることを仮定する. 一般的に, サイバー攻撃の多くは, 下図に示す手順により実現されていることが知られている. ここで注意すべきは, 自動車のような制御システムの場合, Step3 の制御を乗っ取る所までが重要であり, 以降の情報の漏洩やトレーサビリティについては自動運転車両では必要ない可能性があるものの, 将来的にセキュアロギングなどの機能が自動車内に搭載されたりする場合には必要になる.

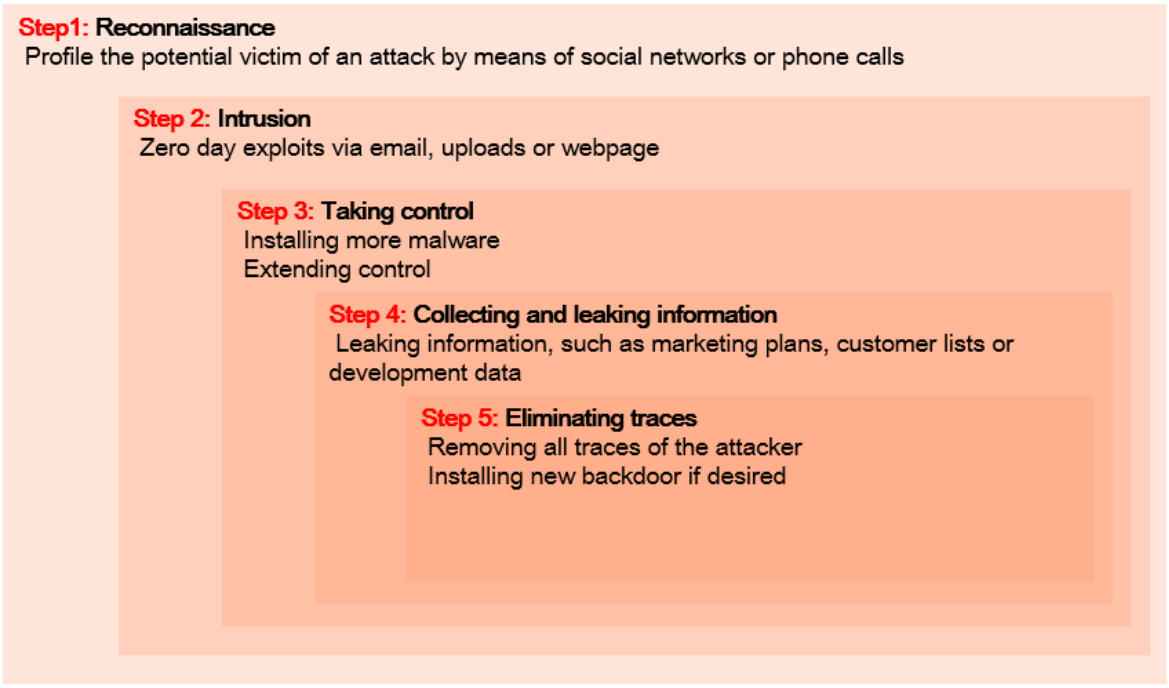


図 6-2 Cybersecurity の攻撃の段階

また，Step1 の情報の漏洩については，様々な漏洩が考えられる．自動車の場合，様々なステイクホルダーが存在する．例えば，車両システムの設計開発者が漏洩する場合も存在するし，販売店の整備士が情報を漏洩する場合も存在する．このため，製品のライフサイクルに係るすべてのステイクホルダーからの情報漏洩を阻止する手立てが必要となる．

6.3.3 偵察(Reconnaissance)とライフサイクル

特に，システムの構成や情報などが洩れるのは，実際の車両システムから設計情報が洩れる場合と，製品のライフサイクル上のステイクホルダーから漏洩する場合の 2 つが存在する．前者については，攻撃者がターゲットとなる車両システムをリバースエンジニアリングすることにより情報を収集することを指す．一方，後者については，悪意のある場合や悪意がなくても結果的に製品上のライフサイクルからクリティカルな製品の設計情報やパスワードが漏洩することがある．これは，例えば鍵を紛失した場合の鍵再発行のプロセスなどにおいて，所有者になりすました偽の所有者(攻撃者)にパスワードを漏洩するなどの例として挙げられる．このため，本調査では，ステイクホルダーからの情報漏洩に配慮して，各ライフサイクルとステイクホルダーを定義する．

表 6-5 自動車のステイクホルダーと製品ライフサイクル

ライフサイクル	ステイクホルダー	説明

開発時	企画者，開発者	設計情報を知りえる(例えば，暗号アルゴリズム，暗号鍵生成方法など)
製造時	製造者，	製造時に各車両に書き込んだ鍵情報を知りえる
販売時	整備士	所有者の個人情報やユーザーが使用する車両情報，ユーザー認証鍵などを知りえる． 整備時に使用するツールを使用して，車両情報を盗み見たり，書き換えたりすることが出来る．
廃棄時	中古車販売事業者	中古車販売業者が前所有者の情報を取得できる可能性がある．

攻撃者は様々な手段を利用して設計情報を取得した上で，実際のターゲットとなる車両への侵入を試みる．攻撃者からの取得する情報から最も必要な情報を調べるために，攻撃対象となるシステムの情報を収集することにより，侵入を試みる．

6.4 リスクの考え方

J3061 ではコンセプトフェーズにおいて，脅威分析とリスク評価することが明記されている．本論での脅威分析もこれと同じレベルの分析とした．尚，脅威の考え方としては以下の通りとして扱う．

Risk ＝ Impact(Severity × Controllability) × Likelihood(Vulnerability × Threat × Exposure)

上記のリスクの考え方は，ISO26262 の安全分析から来ている．自動運転システムについては，人命や健康を資産とする場合には，上記の考え方が成り立つと考える．一方，プライバシーや知的財産のような資産については，この限りではない．
より簡単に説明すると，Impact は，Severity と Controllability の 2 つに分解できる．これは，脅威が実現したときの深刻度と外部方策などにより，危険事象を回避することが出来るかどうかを示すものとする．これらの定義は ISO26262 などで扱われるものと同じとみなすことができる．次に，Likelihood は，Vulnerability と Threat と Exposure の 3 つに分解される．これは，脅威がいかに強力だとしても，脆弱性や脅威を発生させる機会がなければ，脅威は実現しないことを表す．しかしながら，脆弱性はシステム構成が決まらないと想定することは難しい．つまり，脆弱であるかどうかは実際に設計された ECU や車両ごとに異なるため，脆弱であるかどうかを本脅威分析にて取り扱うことはできない．さらに，Exposure についても攻撃者が攻撃しなければ発生しないため，攻撃者のモチベーションなどと関連する．例えば，ハッカーと敵対する自動車メーカーが仮に存在する場合には，とても狙われる可能性が高いし，ハッカーと仲良く付き合う自動車メーカーが存在する場合には，狙われにくいと定義できる．

以上より，Vulnerability と Exposure を評価することは難しいため，本論では，Severity と Controllability と Threat のみでリスクを評価するものとした．各項目のレベルについては，以下の通り定義した．

Table 6-1　Severity のクラス分類

クラス	S0	S1	S2	S3
Lv.	Informational	Low	Medium	High
例	悪用が困難 障害なし	車両システムへの影響はない． 一部のサービスに対してのみ影響 軽度及び中度の障害	一部の車両・サービスに対して影響 重度および生命を脅かす可能性あり	すべての車両・サービスに影響 生命を脅かす

Table 6-2　Controllability のクラス分類

クラス	C0	C1	C2	C3
Lv.	Informational	Low	Medium	High
例	一般的に回避可能	容易に回避可能	通常は回避可能	回避困難または不可

Table 6-3　Threat のクラス分類

クラス	T0	T1	T2	T3
Medium	Informational	Low	Medium	High
	発生可能性はあるが，注意喚起レベル	**発生可能性が少ない** ・攻撃するために複雑な条件を必要とする脅威 ・その他、レベル II に該当するが再現性が低いもの	**発生可能性がある** ・一部の情報が漏えいするような脅威 ・一部の情報が改ざんされるような脅威 ・一部のサービス停止に繋がるような脅威	**発生可能性が高い** ・システムの制御が乗っ取られる脅威 ・システムの情報が改ざんされる脅威 ・すべてのシステムのサービス停止につながるような脅威

尚，Controllability については， 外部方策などが適用される可能性があるため，自動運転システムでは車両レベルではなくサービスレベルで考える必要がある．つまり，脆弱な車両が存在したとしても，LTE 網で悪意のある攻撃がブロックされる場合には，車両への攻撃は実現できない．このような外部方策についても今回の脅威分析では期待できないものとした．つまり，Jeep の脆弱性事例で挙げられるように，自動車は世界中に販売されるため，どのような通信事業者の通信網に接続されるかはわからない．このため，実際には Controllability により実現性が低減される攻撃も存在することが想定できるが，本論で Controllability は期待できないもの，つまり参考値として扱うこととした．

6.4.1 想定する資産

前述するように，本分析で想定する資産は，類型化されたシステムにて行うものとする．このため，類型化されたシステムや機能サービスから導出される粒度での資産を想定する．より具体駅には，自車位置情報などの粒度とする．

6.4.2 想定する被害と攻撃経路

想定する被害としては，自動運転システムに対しては，安全性が重要となる．このため，代表的な攻撃シナリオとしては，前述する脆弱性事例などでも取り上げられた攻撃手法などが挙げられる．

Table 6-4 攻撃者と車両の距離の想定

攻撃者の距離	遠隔	近接	物理的接触
GPS	×（不可能）	○	—（対象外）
WiFI／LTE	○	○	—（対象外）
V2X 通信	○	○	—（対象外）
Bluetooth	×（不可能）	—（対象外）	—（対象外）
センサ類（LIDAR/RADAR/超音波）	×（不可能）	—（対象外）	—（対象外）

まず，ここでいう攻撃者とは，攻撃を行う人及び機器を含むものとする．このため，ハッカーは攻撃を実行するために，各道路などに特殊な機器を取り付けて攻撃を行うことがあることを仮定する．そのうえで，遠隔とは，自動運転システムとの距離は問わない攻撃であり，具体的にはインターネット網や IP 電話網などにつながる場合を指す．これらの脅威にさらされるのは，WiFi/LTE/V2X 通

信を想定する. 次に, 近接とは, 自動運転車両の見える範囲に攻撃者がいることを想定しており, より具体的には, 車両が搭載するセンサ類の有効範囲に依存する. このため, 各種センサ類や Bluetooth, GPS などを対象とすることを想定した. 尚, 今回は分析対象の範囲から排除したが, 各車両に物理的に攻撃できる場合を想定する必要がある. これは無線通信や各種センサへの攻撃の他に, シェアカーなどの場合には不正機器を車内に容易に設置したり, 車両システムを改造できるためである. ただし, 物理攻撃を想定する場合には, 脅威の可能性は広がるが, その Impact(Severity)は低いため, セキュリティ強化からは排除される場合がある.
本脅威分析では, 既存する脆弱性事例でも言及されるように, 遠隔から車両システムに侵入した上で, 車両内部の制御用コンピュータのプログラムを改ざんしたり, マルウェアを注入する攻撃は想定している. つまり, 攻撃者は車両には直接的に触れないものの, 無線通信路経由で車両内に侵入して攻撃する場合については取り上げるものとする.

6.5 脅威分析の前提

各機能の実現方法は車両システムに応じて異なる可能性がある. 例えば, 前方の障害物を認識するために用いるセンサはカメラだけ用いる場合も存在するし, 一方で LiDAR などの測距センサを用いる場合もある. このようにシステム構成の違いについて存在するものの, 攻撃方法が異なるだけで脅威の大きさ(つまり, 発生確率と深刻度の掛け合わせ)は同じとみなせる. ただし, 例えば LIDAR とカメラの 2 つを付けて冗長化する場合には, 同時に 2 つのセンサを同時に騙す攻撃方法が必要であり, 攻撃の難易度が上がる. このように攻撃の難易度を上げるような方策がなされている場合は, Controllability で扱うことを想定している.

6.6 分析の手順

本論で採用する脅威分析のアプローチは, 資産に対して, ガイドワードを適用することにより, 脅威を導出する手法を採用した. その一つとして STRIDE を上げているが, STRIDE はマイクロソフト社が考案した情報資産に対する脅威分析手法として広く知られている. しかしながら, 一方で, 自動運転システムのような情報資産以外の物理的な資産や健康, 安全などに影響するシステムには, ガイドワードが必ずしも適切に適用できるとは限らない. このため, 本節では, 分析対象となる車両システムおよび機能, サービスに対する資産を最初に洗い出す方法と採用した. 尚, ガイドワードについては, 一部独自に拡張や改良した上で分析を実施した.

6.7 車両システムの資産

前述の類型化された車両システムでは，以下のような資産が存在する．まず，類型化されたシステムより情報資産やソフトウェア資産が導出される．その上で，物理的資産，サービス，人，無形資産などに分類した．

表 6-6 車両システムの資産

資産分類	資産	説明
情報	自車位置情報	自車位置の情報
	道路情報	自車が認識する道路情報
	他車位置情報	他車位置の情報
	障害物情報	障害物の情報
ソフトウェア資産	地図 DB	自車に組み込まれた地図情報
	自動運転システムにおける判断処理部	自動運転を実現するための判断処理部．前述の情報資産を使用し判断を実施する．
	システムソフトウェア	自動走行のソフトウェアプラットフォーム．各種デバイスドライバや通信機能などを備える．
物理的資産	自動運転車両自体	車両自体
サービス	自動走行機能	自動運転車両が搭載する共通機能
人	乗員	自動運転車両に乗員する人の健康，安全．
	周辺の人	自動運転車両の周辺に居る人
無形資産	企業イメージ	自動運転車両を販売する OEM の企業ブランド，企業イメージなど

6.8 機能，サービスの資産

各機能やサービスにより資産が異なるため，車両システムと同様，分析対象となる機能やサービスを類型化し資産を洗い出し，その上で脅威分析を実施した．尚，サービスレベルでは，前述する車両システムレベルでの資産よりも抽象度の高い資産を想定するものとする．

6.8.1 Over The Air (OTA)

OTAサービスは自動運転システムが導入する以前にすべての車両に導入される可能性がある．このため，自動運転システムにおいてはすべての車両に共通するサービスになると想定した．OTAは特に，攻撃者により悪用されると重大な事故になりかねないため，この機能を分析対象とした．以下の表に示す通り，OTAでは，情報資産，ソフトウェア資産，物理的資産，サービス，無形資産など多岐に渡り，様々な資産が定義できる．

表 6-7 OTA の資産

資産分類	資産	説明
情報	バージョン情報	現在のシステムソフトウェアのバージョン情報のこと
	OTA認証鍵	OTAサービスを実行するための認証鍵情報のこと
ソフトウェア資産	システムソフトウェア	自動走行のソフトウェアプラットフォーム．各種デバイスドライバや通信機能などを備えるシステムソフトウェアのこと
	ファームウェア	更新用のファームウェアのこと
物理的資産	自動運転車両自体	車両自体のこと
	OTAサーバー	OTAの必要有無を検証し，新しいソフトウェアを配送するためのサーバーのこと
サービス	OTAサービス	OTAの通信路などを含めたサービスのこと
無形資産	企業イメージ	OTAサービスプロバイダーの企業ブランド，企業イメージなど

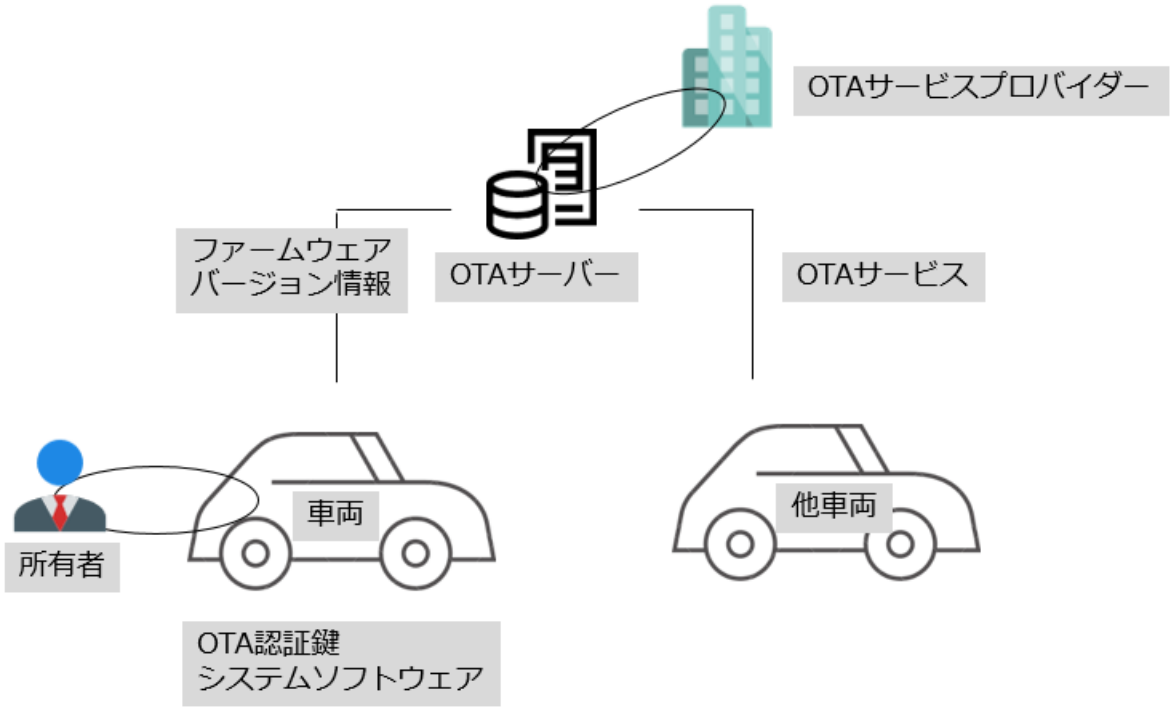


図 6-3 OTA サービスと資産

6.8.2 電子牽引

電子牽引では，電子牽引システムを実現するための情報資産，ソフトウェア資産，物理的資産に追加が必要となる．追加された情報資産は電子牽引プロトコル及び電子牽引における認証情報であり，前者は電子牽引に用いられるプロトコルや通信情報を指し，後者はその上で使用する通信相手を認証するための情報を指す．次に，ソフトウェア資産として定義した電子牽引処理部は，電子牽引プロトコルや認証を実現するためのシステムソフトウェアを指す．最後に，物理的資産として追加した電子牽引機器は，電子牽引プロトコルを通信するための通信用トランシーバやレシーバを指す．

表 6-8 電子牽引の資産

資産分類	資産	説明
情報	電子牽引プロトコル	電子牽引プロトコルのこと
	電子牽引における認証情報	電子牽引における認証情報のこと
ソフトウェア資産	電子牽引処理	電子牽引の処理を行う処理部の事

物理的資産	電子牽引通信機器	電子牽引の通信を行うための制御機器
サービス	電子牽引サービス	電子牽引を利用したサービス

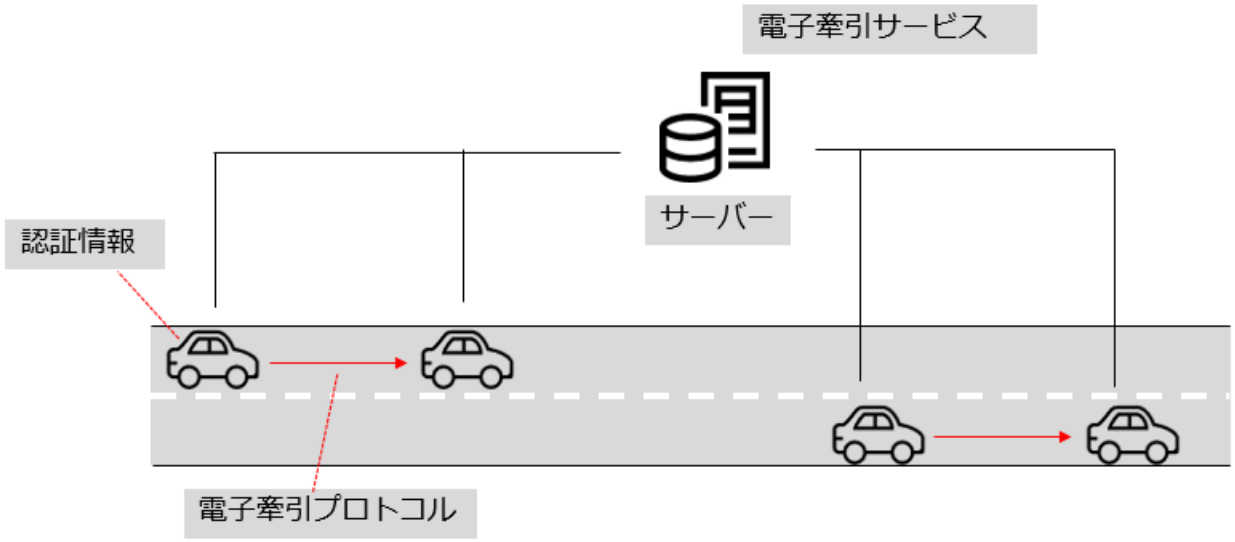


図 6-4 電子牽引サービスと資産

6.8.3 バレーパーキング

バレーパーキングでは，バレーパーキングを実現するための機器構成が自動運転車両システムだけではなく，所有者のスマートフォンやバレーパーキング用の管理サーバーが存在するものと仮定している．このため，これらのシステムにおける資産の追加は，以下の通りを想定する．
まず，情報資産として，バレーパーキング用プロトコル，所有者の認証情報，課金情報を追加する．それぞれ，バレーパーキングのためのプロトコル，対象車両の所有者を認証するための情報，バレーパーキング利用時の課金情報である．ソフトウェア資産として，サービスの可用性などが必要となるため，バレーパーキング処理部などが含まれる．さらに物理的資産として，他の車両や駐車場なども挙げられる．さらに，サービスとしてバレーパーキングサービス，車両周辺の人などが挙げられる．無形資産としては，運行事業者によるサービスプロバイダーの評判など挙げられる．

表 6-9 バレーパーキングの資産

資産分類	資産	説明
情報	バレーパーキング	バレーパーキング用の通信プロトコルのこと

	用通信プロトコル	
	所有者の認証情報	車両の所有者の認証情報
	課金情報	車両の所有者の課金情報
ソフトウェア資産	バレーパーキング処理部	バレーパーキングを実行する制御ソフトウェアのこと
物理的資産	他車両	バレーパーキングを実行したい他車両のこと
	駐車場	バレーパーキングの駐車場のこと
サービス	バレーパーキングサービス	バレーパーキングのサービスのこと．例えば，移動する駐車場を指定し，そこまで自動運転で移動するなどのサービスを指す．バレーパーキングのサービス運行事業者が存在し，駐車場の空き情報や他車両が予約した駐車場の位置などを共有するための使用される．
無形資産	企業イメージ	バレーパーキングのサービスプロバイダーの評判，ブランド，企業イメージなど

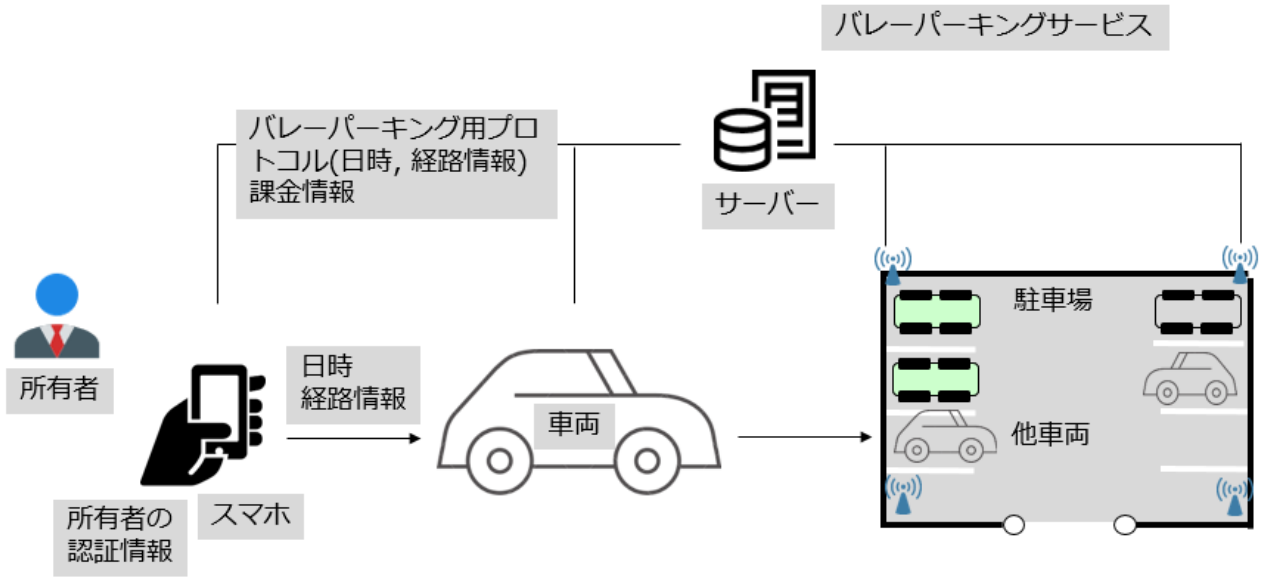


図 6-5 バレーパーキングサービスと資産

6.8.4 隊列走行（V2X 通信機能）

隊列走行については，自車両の周辺位置から情報を取得するだけではなく，他車両に情報を通知するなど，自車両だけではなく，他車両に影響を与えることになる．このため，他車両を攻撃する踏み台として使われてしまう可能性も存在する．さらに，路側機（RSU: Road Side Unit)から電子証明書を受け取り，RSU から信号制御などへも影響を及ぼす可能性がある．このため，電子牽引と比較し，物理的資産を増やしている．この理由は，V2X 通信を介して，他車両の公道や路側機から交通管制に影響を及ぼす可能性があるためである．

表 6-10 隊列走行機能の資産

資産分類	資産	説明
情報	V2X 通信プロトコル	V2X 通信プロトコルのこと
	V2X 通信における認証情報	V2X 通信における認証情報のこと
ソフトウェア資産	V2X 処理	V2X 処理部のこと
物理的資産	（自車両の）V2X 通信機器	V2X 通信を行うための制御機器のこと
	他車両	隊列走行に参加している周辺車両の事
	路側機（RSU）	道路の側壁に設置された路側機のこと．この機器から電子証明書の情報などを受け取る．一方，悪用される可能性もある．
サービス	V2X 通信サービス	V2X 通信を介した様々な機能を想定する

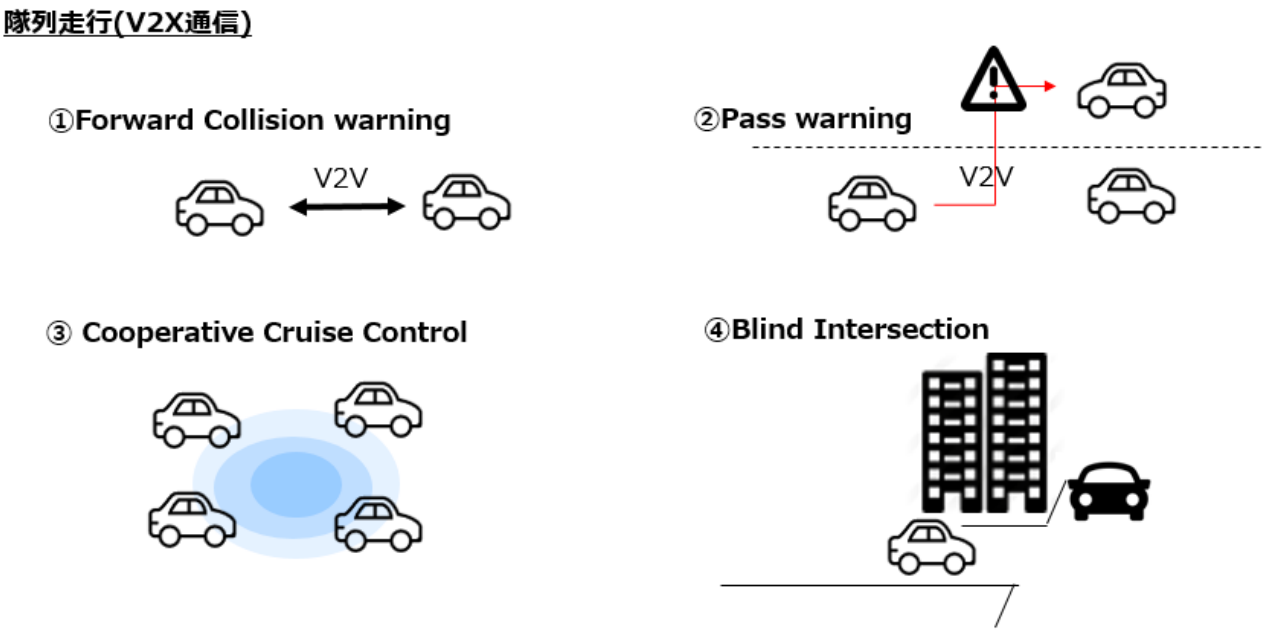


図 6-6 隊列走行

6.8.5 シェアカー（バス，タクシー）

下表の通り，自動運転バスやサービスに対する資産を洗い出した．このように，公共サービスとなると，課金情報などのプライバシーに関連する情報資産がサービス内で適用されることが明確になる．また，予約情報などを悪用し妨害するなどの脅威が容易に想定できるようになる．

表 6-11 シェアカー（バス，タクシー）の資産

資産分類	資産	資産の例
情報	課金情報	ユーザーへの課金情報
	個人情報	ユーザーの利用履歴
	予約情報	ユーザーからの予約情報
ソフトウェア資産	地図 DB	地図情報（※ただし，車両にも含まれている）
	アプリ	サービス用のアプリ
物理的資産	スマホ	ユーザーの所有するスマホのこと
	シェアカー	予約したシェアカーのこと
サービス	バス，タクシーサービス	バスなどの待ち受けサービスのこと

人	乗員	シェアカーに乗車している乗員のこと
	予約者	アプリを通じて配車サービスを予約した人
無形資産	企業イメージ	運行事業車の企業ブランド，企業イメージなど

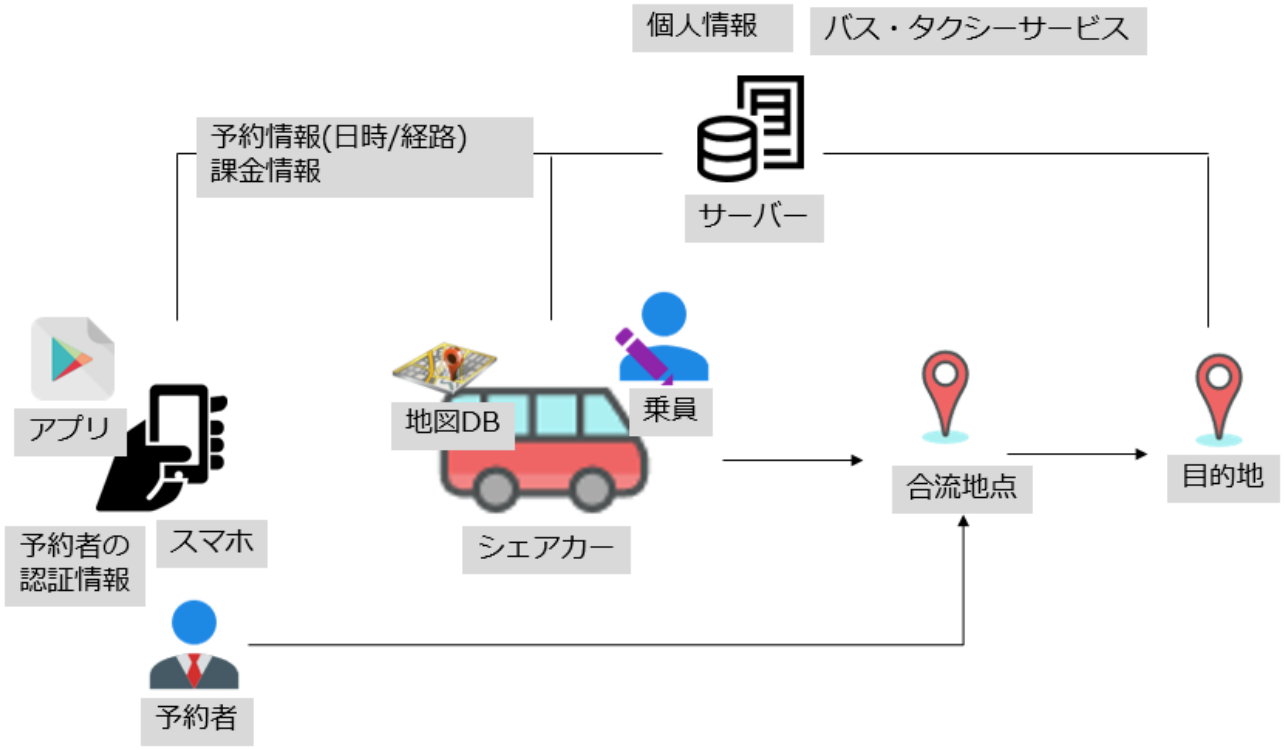


図 6-7 シェアカーサービスと資産

7　脅威分析の結果

7.1 自動運転車両システム

自動運転車両に対する脅威分析については，類型化したシステムに対して実施する．このシステムの資産は，安全性に関連する自動走行関連する各情報資産とソフトウェア資産に対してのみ分析する．

7.1.1 自車位置情報

自車位置情報に対する脅威分析結果を以下の通り記載する．自車位置を判定する上で特に重要なデータは，GPS による位置座標と，地図データベースが重要になる．この 2 つのデータのいずれか一方を妨害すれば，自車位置情報を確定することはできなくなるし，いずれか一方のデータの改ざんが実現できれば，自車位置を容易に意図しない位置へと変更することができる．ただし，これらの攻撃は衛星を乗っ取らない回切り，車両 1 台ずつに対して攻撃しなければならないため，攻撃可能性が低いと考えられる．

表 7-1 自車位置情報に対する脅威

Asset	脅威エージェント	ガイドワード	脅威シナリオ	T	C	S
自車位置情報	衛星*	なりすまし	**・衛星のなりすまし**	**T3**	**C3**	**S3**
		否認	該当なし(衛星からの信号はグローバルのため)	**T1**	**C3**	**S3**
		権限昇格	**・衛星の乗っ取り**	**T3**	**C3**	**S3**
	衛星—GPS 間	改ざん	**・衛星からの信号の改ざん**	**T3**	**C0**	**S3**
		情報漏洩	該当なし(衛星からの信号はグローバルのため)	—	—	—
		妨害	**・衛星からの信号を妨害**	T0	C0	S2
	GPS	改ざん	・GPS の取り換え（不正改造）	**T3**	**C0**	**S3**
		情報漏洩	該当なし(漏洩しても問題ないと判断)	—	—	—
		妨害	**・GPS 機能停止**	T0	C0	S2
	地図 DB	改ざん	・地図データの改ざん	**T3**	**C0**	**S3**
		否認	・利用したデータの不正利用	—	—	—
		情報漏洩	該当なし(漏洩しても問題ないと判断)	T0	C0	S2
		妨害	**・地図データの利用停止**	**T3**	**C3**	**S3**

	自車位置判定処理	なりすまし	・プログラムの不正実行	T0	—	S0
		改ざん	**・処理/プログラムの改ざん**	**T2**	**—**	**S0**
		否認	・不正な処理の起動	T0	—	S0
		情報漏洩	・自車位置判定アルゴリズムの漏洩	T0	—	S0
		妨害	**・自車位置判定処理の妨害**	**T2**	**—**	**S2**
		権限昇格	**・マルウェアなどによる権限昇格**	**T3**	—	**S2**

7.1.2 他車位置情報

他車位置の情報に対する分析結果を以下の通り記載する. 他車位置情報は, V2V 通信, カメラ, Rader や Lidar などのセンサから取得する. これらのセンサから通信をただし, 複数センサが付与されている場合には Controllability が向上する. 例えば, V2V 通信の他にカメラを付与することにより, 同時に 2 つの改ざんなどを実現しないと攻撃が成功しないため, 攻撃の難易度が低下する.

Asset	脅威エージェント	ガイドワード	脅威シナリオ	T	C	S
他車位置情報	他車両*	なりすまし	**・他車両のなりすまし**	**T3**	**C3**	**S3**
		否認	**・他車両のデータの否認**	**T1**	**C3**	**S3**
		権限昇格	**・他車両の乗っ取り**	**T3**	**C3**	**S3**
	他車—V2V Com 間	改ざん	**・V2V 通信の信号の改ざん**	**T3**	**C0**	**S3**
		漏洩	※漏洩しても問題ないため対象外	—	—	—
		妨害	・V2V 通信を妨害	T0	C0	S2
	カメラ	改ざん	**・カメラ画像の改ざん**	**T3**	**C0**	**S3**
		漏洩	※漏洩しても問題ないため対象外	—	—	—
		妨害	・カメラ機能停止	T0	C0	S2
	Rader	改ざん	**・Radar の改ざん(距離情報の改ざん)**	**T3**	**C0**	**S3**
		漏洩	※漏洩しても問題ないため対象外	—	—	—
		妨害	・Radar の機能停止	T0	C0	S2
	Lidar	改ざん	**・Lidar の改ざん(距離情報の改ざん)**	**T3**	**C0**	**S3**
		漏洩	※漏洩しても問題ないため対象外	—	—	—
		妨害	・Lidar の機能停止	T0	C0	S2
	超音波	改ざん	**・信号の改ざん(距離情報の改ざん)**	**T3**	**C0**	**S3**
		漏洩	・※漏洩しても問題ないため対象外	—	—	—
		妨害	・超音波センサの機能停止	T0	C0	S2

7.1.3 道路情報

道路情報に対する脅威を以下の表のとおり記載する. 道路情報は, 車両が保持する地図 DB とカメラから取得した標識などの情報により構成される. このため, いずれも改ざんされたデータなどが入力される場合には, 道路情報を正しく認識することは難しくなる. 尚, 地図については妨害され, 可用性がなくなるだけでも同様に致命的となる.

表 7-2 道路情報に対する脅威

Asset	脅威エージェント	ガイドワード	脅威シナリオ	T	C	S
道路情報	カメラ	改ざん	**・カメラ画像の改ざん, 誤認識**	**T3**	**C0**	**S3**
		漏洩	※漏洩しても問題ないため対象外	—	—	—
		妨害	・カメラ機能停止	T0	C0	S2
	地図 DB	改ざん	**・地図 DB の改ざん**	**T3**	**C2**	**S3**
		漏洩	・知的財産は侵害されるが安全性は影響なし	—	—	—
		妨害	**・地図の機能停止**	**T3**	**C3**	**S2**

7.1.4 障害物情報

障害物情報は, 自車両が走行しようとするパス上に存在する障害物であり, 本来は避けて走行するようパスプランニングされるものである. しかしながら一方で, 認識でない障害物が存在したり, 本来は存在しないはずの障害物を攻撃者が偽装するなどにより, 走行を妨害することが可能になる. しかしながら, これらの障害物情報は, いずれか 1 つのセンサで検出することができれば, 回避行動がとれるため, 致命傷とはなりにくいものと考えられる. このため, 要求されるシステムの可用性と各センサの能力に応じて, 適切な組み合わせで実装される必要がある.

表 7-3 障害物情報に対する脅威

Asset	脅威エージェント	ガイドワード	脅威シナリオ	T	C	S
障害物情報	障害物*	なりすまし	**・障害物ののなりすまし**	**T3**	**C3**	**S3**
		否認	※障害物に認証機能はないため対象外	**—**	**—**	**—**
		権限昇格	**・衛星の乗っ取り**	**T3**	**C3**	**S3**
	カメラ	改ざん	**・カメラ画像の改ざん**	**T3**	**C0**	**S3**
		漏洩	※漏洩しても問題ないため対象外	—	—	—
		妨害	・カメラ機能停止	T0	C0	S2

	Rader	改ざん	**・Radar の改ざん(距離情報の改ざん)**	**T3**	**C0**	**S3**
		漏洩	※漏洩しても問題ないため対象外	—	—	—
		妨害	・Radar の機能停止	T0	C0	S2
	Lidar	改ざん	**・Lidar の改ざん(距離情報の改ざん)**	**T3**	**C0**	**S3**
		漏洩	※漏洩しても問題ないため対象外	—	—	—
		妨害	・Lidar の機能停止	T0	C0	S2
	超音波	改ざん	**・信号の改ざん(距離情報の改ざん)**	**T3**	**C0**	**S3**
		漏洩	・※漏洩しても問題ないため対象外	—	—	—
		妨害	・超音波センサの機能停止	T0	C0	S2

7.2 OTA

OTA サービスにおける脅威分析の結果として， OTA サーバー側の攻撃が特に深刻になる．車両単位で攻撃することは容易ではあるものの，世界中から接続される OTA サーバーが世界中から攻撃される可能性も考えうる．車両単位での攻撃よりも，OTA サーバー側のプログラムを改ざんできれば，より広範囲に同時に攻撃ができるなどの利点がある．

,

表 7-4 OTA に対する脅威

Asset	脅威エージェント	ガイドワード	脅威シナリオ	T	C	S
車両	所有者*	なりすまし	**・所有者のなりすまし**	**T3**	**C2**	**S3**
		否認	※該当なし	**—**	**—**	**—**
		妨害	**・意図しない不正操作，妨害行為** **・OTA サービスの起動**	**T3**	**C2**	**S2**
	OTA サーバー*	なりすまし	**・OTA サーバーのなりすまし**	**T3**	**C2**	**S2**
		否認	・OTA サーバーからのバージョンアップ否認	T2	C2	S2
		妨害	**・OTA のアップデートを繰り返す**	**T3**	**C2**	**S2**
ファームウェア	OTA サーバー	漏洩	・ファームウェアの漏洩	T3	C1	S2
		改ざん	・OTA サーバー上でのファームウェアの改ざん	T3	C1	S2
		妨害	・OTA サーバー上でのファームウェアの破壊	T3	C1	S2
	OTA サーバーと車両間通信	漏洩	・ファームウェアの漏洩	T3	C1	S2
		改ざん	・通信路上でのファームウェアの改ざん	T3	C1	S2
		妨害	・通信路上での妨害	T3	C1	S2
		漏洩	・ファームウェアの漏洩	T3	C1	S2

バージョン情報	OTA サーバー	改ざん	**・OTA サーバー上でのバージョン情報の改ざん**	T3	C1	S2
		妨害	**・OTA サーバー上でのバージョン情報の破壊**	T3	C1	S2
	OTA サーバーと車両間通信	漏洩	・バージョン情報の漏洩	T3	C1	S2
		改ざん	・通信路上でのバージョン情報の改ざん	T3	C1	S2
		妨害	・通信路上での妨害	T3	C1	S2
OTA 認証鍵	車両内の攻撃者	漏洩	・鍵漏洩による自車両のなりすまし	T3	C0	S1
		改ざん	・OTA 認証鍵の改ざん	T3	C0	S1
		妨害	・OTA 認証鍵の妨害	T3	C1	S2
システムソフトウェア	車両内の攻撃者	漏洩	・システムソフトウェアの漏洩	T2	C0	S1
		改ざん	**・システムソフトウェアの改ざん**	**T3**	**C0**	**S2**
		妨害	・システムソフトウェアの妨害	T1	C0	S1
OTA サーバ	攻撃者	漏洩	・攻撃者によるサーバーの情報漏洩	T3	C0	S3
		改ざん	**・攻撃者によるサーバーの情報改ざん**	**T3**	**C0**	**S3**
		妨害	・攻撃者によるサーバーの妨害	T3	C0	S3
OTA サービス	サービスプロバイダー	なりすまし	・OTA サービスプロバイダーによるなりすまし	T1	C0	S3
		否認	・OTA サービスプロバイダーによる否認	T1	C0	S3
		妨害	・OTA サービスプロバイダーによる妨害	T1	C0	S3

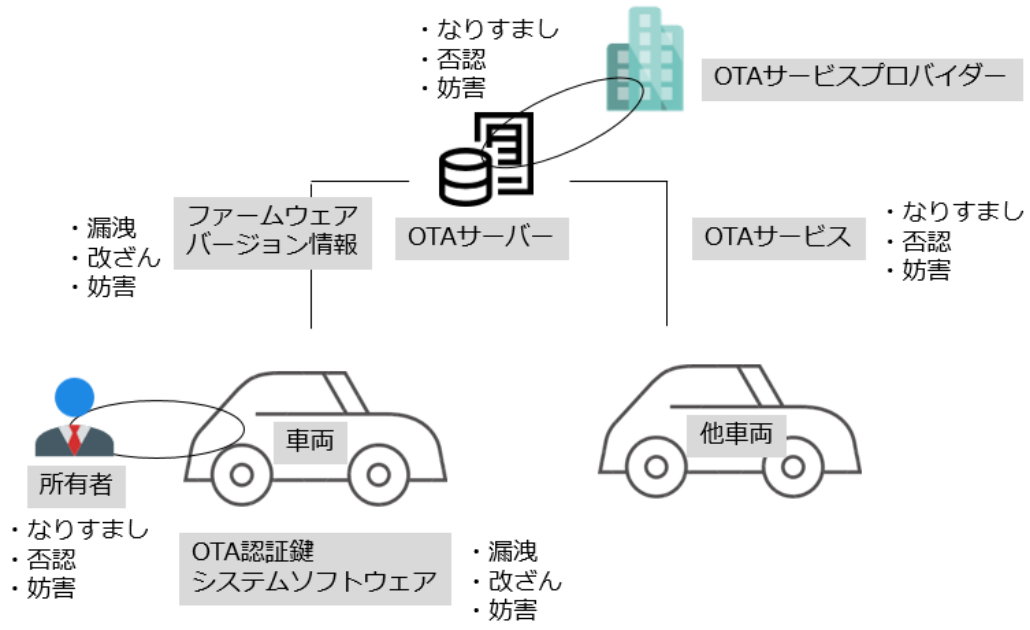


図 7-1 OTA の脅威分析（資産とガイドワード）

7.3 電子牽引

電子牽引に関しては，車両に対する攻撃として，他車両（先頭/追従車両）になりすまされる場合，電子牽引サービス中に強制停止される場合などが深刻な事態となる．さらに，よく発生する可能性があるのは電子牽引通信の妨害であり，ひどく深刻なのが，サーバーに対する妨害攻撃などにより，すべての電子牽引サービスが停止する場合といえる．

表 7-5　電子牽引に対する脅威

Asset	脅威エージェント	ガイドワード	脅威シナリオ	T	C	S
車両	他車両*	なりすまし	**・他車両（先頭/追従車両）のなりすまし**	**T3**	**C3**	**S2**
		否認	・他車両による否認	T1	C0	S2
		妨害	・他車両による妨害 **・電子牽引サービスの強制停止**	**T3**	**C3**	**S2**
	牽引サーバー*	なりすまし	・牽引サーバーのなりすまし	T1	C0	S3
		否認	・牽引サーバーによる否認	T1	C0	S3
		妨害	・牽引サーバーによる車両への妨害	T1	C0	S3
認証情報	攻撃者	漏洩	・認証情報の漏洩によるなりすまし （不正課金や不正請求）	T3	C0	S2
		改ざん	・認証情報の改ざん	T3	C0	S2
		妨害	・認証情報の破壊	T3	C0	S2
電子牽引プロトコル	攻撃者	漏洩	・通信の漏洩	T3	C1	S2
		改ざん	・通信の改ざん	T3	C1	S2
		妨害	**・通信の妨害**	**T3**	**C3**	**S3**
サーバー	攻撃者	漏洩	・攻撃者によるサーバーの情報漏洩	T3	C0	S3
		改ざん	・攻撃者によるサーバーの情報改ざん	T3	C0	S3
		妨害	**・攻撃者によるサーバーの妨害 （サービス停止）**	**T3**	**C3**	**S3**

7.4 バレーパーキング

バレーパーキングサービスにおいては，車両の通信相手になるサーバー，スマホ，駐車場などにより騙される可能性がある．また，実装されるプロトコルに依存するものの，課金情報などの金銭情報がやり取りされ，本来は使用した所有者が料金を踏み倒すために否認したり，知識のないユーザーがサービスを妨害するなどの可能性もある．さらに，市街地を自動運転車両が無人で走行する場合には攻撃者による車両盗難などへのリスクが高くなるといえる．

表 7-6 バレーパーキングに対する脅威

Asset	脅威エージェント	ガイドワード	脅威シナリオ	T	C	S
車両	所有者	なりすまし	**・所有者のなりすまし**	**T3**	**C3**	**S2**
		否認	※該当なし	—	—	—
		妨害	**・意図しない車両操作** **・意図しないサービスの起動** **・意図しない駐車位置の変更**	**T3**	**C3**	**S2**
	スマホ	なりすまし	・スマホのなりすまし	T1	C1	S2
		否認	・マルウェアによる否認	T1	C3	S2
		妨害	**・マルウェアによるサービス妨害**	**T3**	**C3**	**S2**
	サーバー	なりすまし	・なりすましサーバーによる不正アクセス	T1	C1	S2
		否認	・サーバーによる否認	T1	C3	S2
		妨害	・マルウェアによるサービス停止	T1	C1	S2
	駐車場	なりすまし	**・駐車場のなりすまし**	**T2**	**C3**	**S2**
		否認	**・駐車場の否認（来てないと嘘をつく）**	**T2**	**C3**	**S2**
		妨害	**・駐車場の妨害（意図した車を駐車できないようにする）**	**T2**	**C3**	**S2**
バレーパーキングプロトコル	攻撃者	漏洩	・プロトコルの漏洩	T3	C1	S2
		改ざん	・プロトコルの改ざん	T3	C1	S2
		妨害	・プロトコルの妨害	T3	C1	S2
	攻撃者	漏洩	・サーバー上の個人情報漏洩	T3	C1	S3

サーバー		改ざん	・サーバー上の課金情報の改ざん	T3	C1	S3
		妨害	・サーバー上のサービス妨害	T3	C1	S3
スマホ	攻撃者	漏洩	・スマホのデータの窃盗，盗み見，・マルウェア感染による漏洩	T3	C1	S2
		改ざん	・スマホの改ざん，認証情報や課金情報の改ざん	T2	C1	S2
		妨害	・スマホの窃盗，破壊	T3	C1	S2
駐車場	攻撃者	漏洩	※物理的なもののため，該当なし	—	—	—
		改ざん	・駐車場の不正改造（駐車場の位置情報を改ざん）	T3	C1	S3
		妨害	**・駐車場の妨害（駐車できないようにする）**	**T3**	**C1**	**S3**

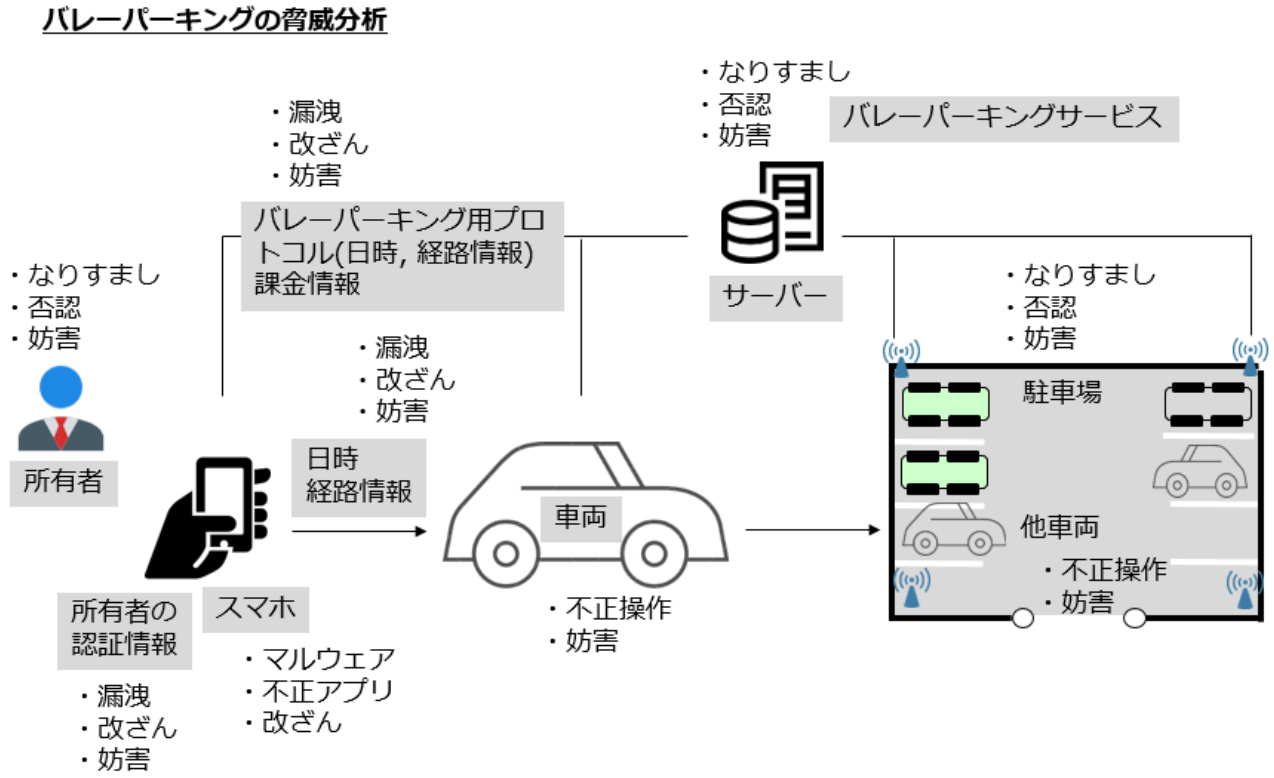


図 7-2　バレーパーキングの脅威分析（資産とガイドワード）

7.5 隊列走行

隊列走行においては，電子牽引サービスと同様ではあるが，2 点違いがある．まず，1 点目は，V2X 通信を用いて RSU などと通信するため，攻撃経路や攻撃手法が増加する．次に 2 つ目として，車群を形成するため，インシデントが発生した場合の深刻度が酷くなることが挙げられる．さらに，妨害攻撃に対して弱い側面があるため，コントローラビリティが低くなる可能性がある．

表 7-7　隊列走行に対する脅威

Asset	脅威エージェント	ガイドワード	脅威シナリオ	T	C	S
車両	他車両	なりすまし	・他車両（先頭/追従車両）のなりすまし	T3	C3	S2
		否認	・他車両による否認	T1	C0	S2
		妨害	・他車両による妨害 ・電子牽引サービスの強制停止	T3	C3	S2
	V2X サーバー	なりすまし	・V2X サーバーのなりすまし	T1	C0	S3
		否認	・V2X サーバーによる否認 （V2X 機能）	T1	C0	S3
		妨害	・牽引サーバーによる車両への妨害	T1	C0	S3
	RSU	**なりすまし**	**・RSU のなりすまし**	**T3**	**C1**	**S3**
		否認	**・RSU による否認**	**T3**	**C0**	**S3**
		妨害	**・RSU による妨害**	**T3**	**C3**	**S3**
認証情報	攻撃者	漏洩	・認証情報の漏洩によるなりすまし （不正課金や不正請求）	T3	C0	S2
		改ざん	・認証情報の改ざん	T3	C0	S2
		妨害	・認証情報の破壊	T3	C0	S2
隊列走行プロトコル	攻撃者	漏洩	・通信の漏洩	T3	C1	S2
		改ざん	・通信の改ざん	T3	C1	S2
		妨害	・通信の妨害	T3	C3	S3
サーバー	攻撃者	漏洩	・攻撃者によるサーバーの情報漏洩	T3	C0	S3
		改ざん	・攻撃者によるサーバーの情報改ざん	T3	C0	S3
		妨害	・攻撃者によるサーバーの妨害 （サービス停止）	T3	C3	S3

7.6 シェアカー

シェアカーについては，サーバーサイドあるいはサービスを妨害することにより，事業の継続が困難になりそうな攻撃を深刻度で表した．この結果，予約者のなりすまし，サーバーへの攻撃などが深刻となる．

表 7-8 シェアカーに対する脅威

Asset	脅威エージェント	ガイドワード	脅威シナリオ	T	C	S
シェアカー	予約者	なりすまし	**・予約者のなりすまし**	**T3**	**C3**	**S3**
		否認	・サービスの不正利用	T3	C0	S2
		妨害	**・意図しないサービスの使用**	**T3**	**C3**	**S3**
	スマホ	なりすまし	・スマホのなりすまし	T1	C1	S2
		否認	・マルウェアによる否認	T1	C3	S2
		妨害	・マルウェアによるサービス妨害	T3	C3	S2
	サーバー	なりすまし	**・なりすましサーバーによる不正アクセス**	T1	C1	S2
		否認	**・サーバーによる否認**	T1	C3	S2
		妨害	**・サーバーによるサービス停止**	T1	C1	S2
	合流地点	なりすまし	・合流地点のなりすまし	T2	C3	S2
		否認	※該当なし	—	—	—
		妨害	・合流地点の破壊，妨害	T2	C3	S2
	目的地店	なりすまし	・合流地点のなりすまし	T2	C3	S2
		否認	※該当なし	**—**	**—**	**—**
		妨害	・合流地点の破壊，妨害	T2	C3	S2
プロトコル	攻撃者	漏洩	・プロトコルの漏洩	T3	C1	S2
		改ざん	・プロトコルの改ざん	T3	C1	S2
		妨害	・プロトコルの妨害	T3	C1	S2
サーバー	攻撃者	漏洩	**・サーバー上の個人情報漏洩**	**T3**	**C1**	**S3**
		改ざん	**・サーバー上の課金情報の改ざん**	**T3**	**C1**	**S3**
		妨害	**・サーバー上のサービス妨害**	**T3**	**C1**	**S3**
スマホ	攻撃者	漏洩	・スマホのデータの窃盗，盗み見，・マルウェア感染による漏洩	T3	C1	S2
		改ざん	・スマホの改ざん，認証情報や課金情報の改ざん	T2	C1	S2

		妨害	・スマホの窃盗，破壊	T3	C1	S2
合流地点	攻撃者	漏洩	※物理的なもののため，該当なし	—	—	—
		改ざん	・駐車場の不正改造（駐車場の位置情報を改ざん）	T3	C1	S3
		妨害	・破壊や妨害行為により到達できないなど	T3	C1	S3
目的地点	攻撃者	漏洩	※物理的なもののため，該当なし	—	—	—
		改ざん	・駐車場の不正改造（駐車場の位置情報を改ざん）	T3	C1	S3
		妨害	・破壊や妨害行為により到達できないなど	T3	C1	S3

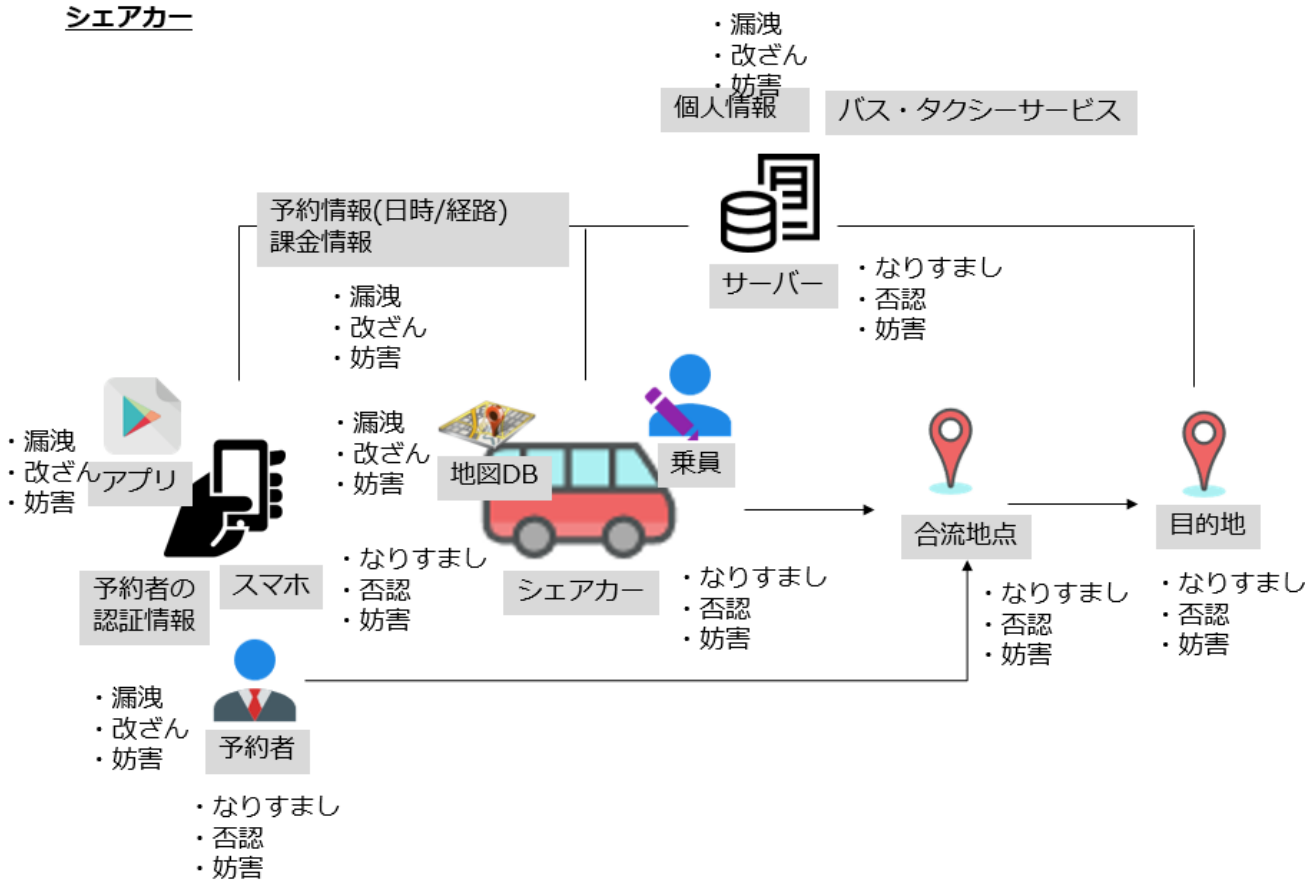


図 7-3 シェアカーの脅威分析（資産とガイドワード）

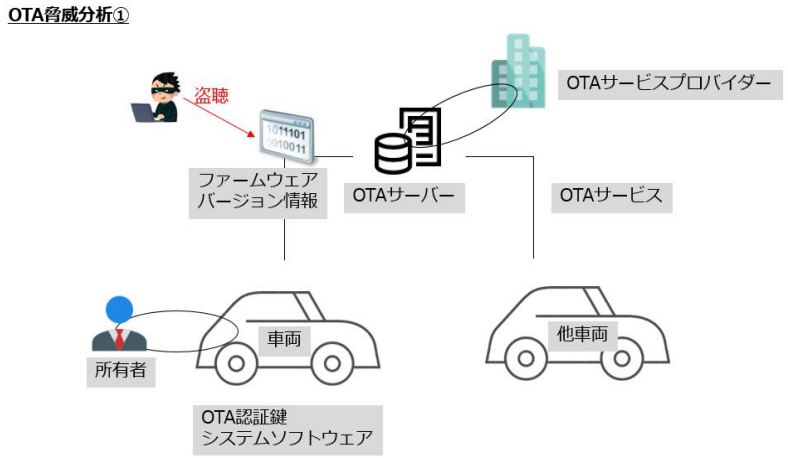
8　脅威シナリオ

脅威分析された結果をシナリオベースで特に重要度の高いものについて，分析結果をまとめなおす．以降では，前述の分析結果より，典型的な攻撃シナリオを示すためのものである．

8.1 OTA

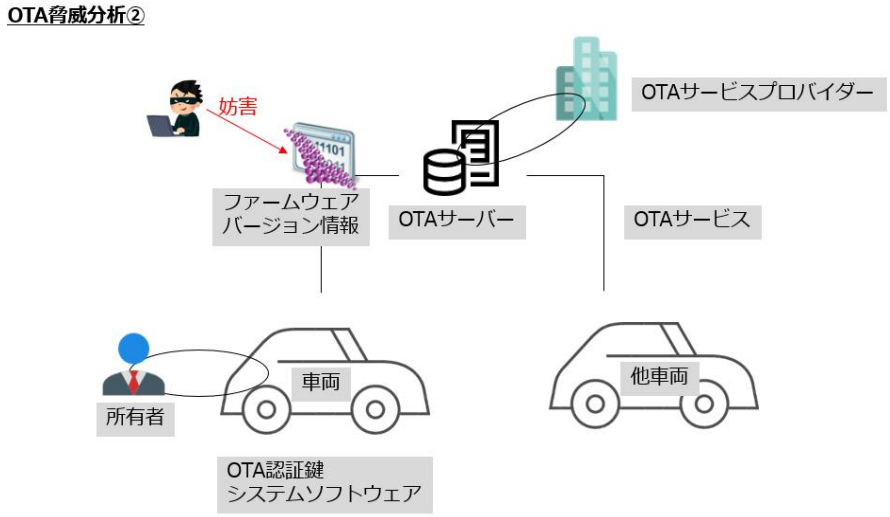
8.1.1 OTA の盗聴

OTA 中の無線通信プロトコルを盗聴することにより，ファームウェアを取得したり，通信プロトコルをリバースエンジニアリングしようと試みる攻撃のことである．

シナリオ番号		1
ユースケース名		OTA の盗聴
資産		ファームウェア
攻撃ゴール/攻撃目標		ファームウェアの奪取
攻撃方法の例		OTA を実行している車両の近くで，Wi-Fi/LTE 通信を盗聴する
攻撃説明		攻撃者が OTA サーバーから車両に送信されたファームウェアを通信プロトコルを盗聴することでファームウェアを取得しようと試みる攻撃を指す．例えば，暗号化されていないファームウェアなどが転送される場合には，ファームウェア自体が流出してしまう．
攻撃説明図		
リスク算定結果	T	T3
	C	C1
	S	S2
関連ユースケース番号		なし

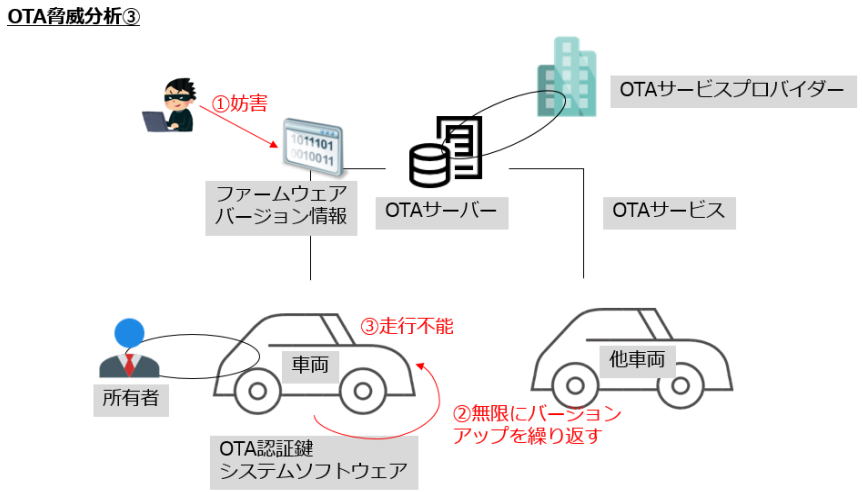
8.1.2 OTA の妨害 1

OTA で流れてくる通信を妨害することにより，バージョンアップを妨害する.

シナリオ番号		2
ユースケース名		OTA の妨害 1
資産		OTA サービス
攻撃ゴール/攻撃目標		OTA サービスの妨害
攻撃方法の例		車両外のネットワークトラフィックを妨害（ジャミングなど）し，ECU が特定のファームウェアを受信するのを妨害する.
攻撃説明		攻撃者が OTA を実行しようとしている車両の近くで，妨害電波を発生させるなどの装置を用いて妨害攻撃を行うことにより実現する. これは車を電波が遮蔽された空間に配置することでも実現できる.
攻撃説明図		
リスク算定結果	T	T3
	C	C1
	S	S2
関連ユースケース番号		OTA の妨害 2 OTA の妨害 3

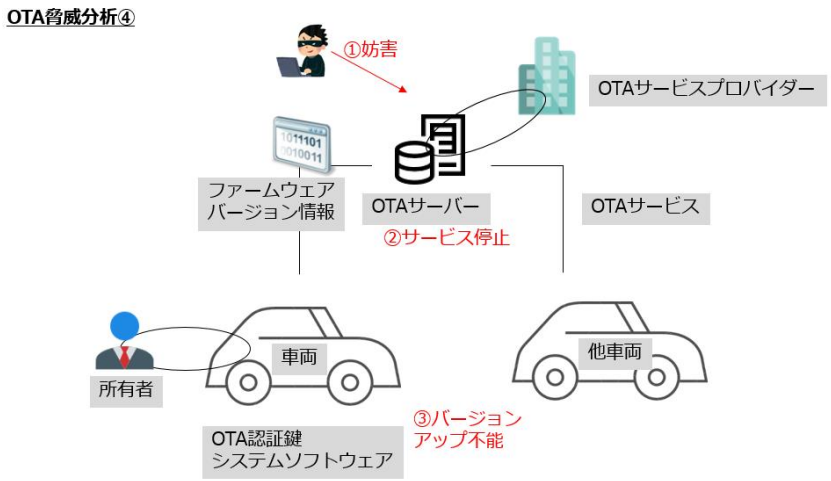
8.1.3 OTA の妨害 2

OTA で流れてくるファームウェアの更新完了を実行させなくすることで，永久にバージョンアップ動作を繰り返させる.

シナリオ番号		3
ユースケース名		OTA の妨害 2
資産		OTA サービス，車両
攻撃ゴール/攻撃目標		OTA サービスの妨害，車両走行の妨害
攻撃方法の例		OTA サービスを無限に繰り返すような妨害攻撃を実行する.
攻撃説明		OTA サービスで使用するプロトコルが漏洩すると，車両からバージョンアップ完了したという通知を妨害することにより，無限にバージョンアップを引き起こさせるような攻撃が可能になる.
攻撃説明図		
リスク算定結果	T	T3
	C	C2
	S	S2
関連ユースケース番号		OTA の妨害 1 OTA の妨害 3

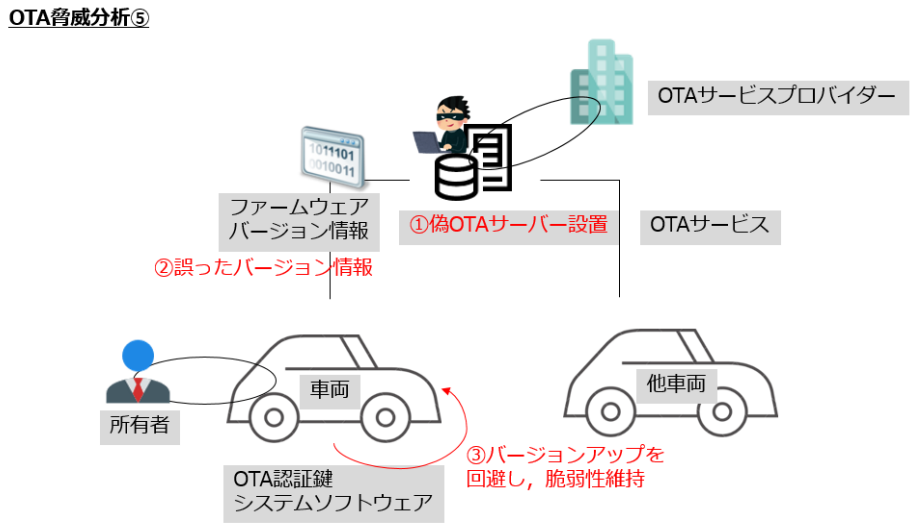
8.1.4 OTA の妨害 3

OTA サーバー自体に妨害攻撃を実施することにより，OTA サービスを停止させる攻撃を指す．

シナリオ番号		4
ユースケース名		OTA の妨害 3
資産		OTA サービス，OTA サーバー
攻撃ゴール/攻撃目標		OTA サービス，あるいは OTA サーバーの妨害
攻撃方法の例		OTA サービスを実行したいときに実行できない．
攻撃説明		OTA サービスを実行したいにもかかわらず，OTA を実行しようとしても OTA サーバーが反応しない．OTA サービスを実行できなくなる攻撃を指す．
攻撃説明図		
リスク算定結果	T	T3
	C	C0
	S	S3
関連ユースケース番号		OTA の妨害 1 OTA の妨害 2

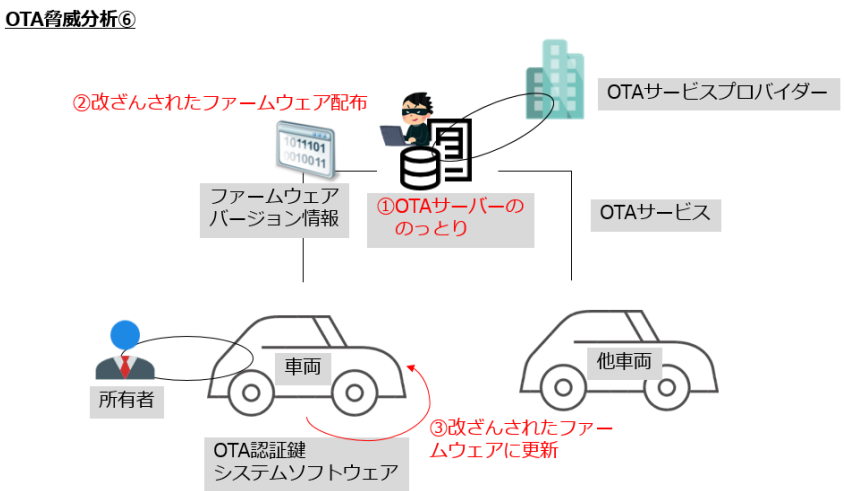
8.1.5 OTA サーバーのなりすましによる妨害 1

OTA サーバーになりすますことにより，新しいバージョンのファームウェアが存在しないようにふるまい，車両のソフトウェアの更新を妨害する.

シナリオ番号		5
ユースケース名		OTA サーバーのなりすましによる妨害 1
資産		車両，システムソフトウェア
攻撃ゴール/攻撃目標		任意の車両のバージョンアップを妨害する
攻撃方法の例		OTA サーバーのふりをして，新しいファームウェアのバージョンが存在しないようにふるまうことにより，任意の車両のバージョンアップを妨害する.
攻撃説明		車載機側の DNS を書き換えるなどして，偽の OTA サーバーに接続させる. その上で偽の OTA サーバーから新しいバージョンは存在しないようにふるまわせることにより，バージョンアップをさせないように妨害する.
攻撃説明図		
リスク算定結果	T	T3
	C	C2
	S	S2
関連ユースケース番号		なし

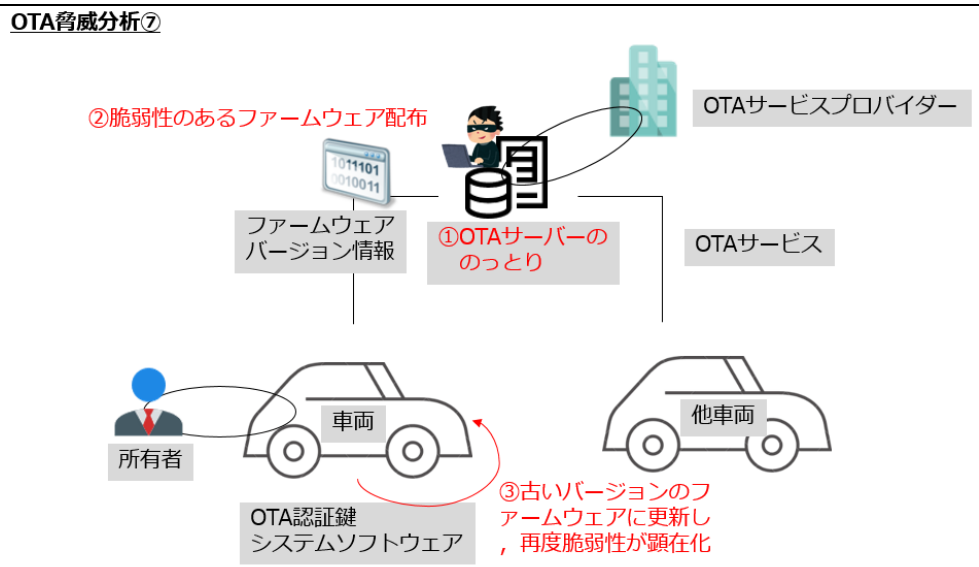
8.1.6 OTA サーバーののっとり 1

OTA サーバーをのっとることにより，悪意のあるファームウェアをダウンロードし更新させる攻撃を指す．

シナリオ番号		6
ユースケース名		OTA サーバーののっとり 1
資産		車両，システムソフトウェア
攻撃ゴール/攻撃目標		OTA サーバーをのっとることにより，OTA を実施する車両すべてに悪意のあるソフトウェアを配布
攻撃方法の例		OTA サービスを悪用して，悪意のあるファームウェアをダウンロードさせる
攻撃説明		OTA サーバーがのっとられると，悪意のあるファームウェアがすべての車両に配布される可能性がある．この場合，任意の脆弱性を仕込んだファームウェアに更新される可能性がある．
攻撃説明図		
リスク算定結果	T	T3
	C	C0
	S	S3
関連ユースケース番号		OTA サーバーののっとり 2　OTA サーバーの改ざん

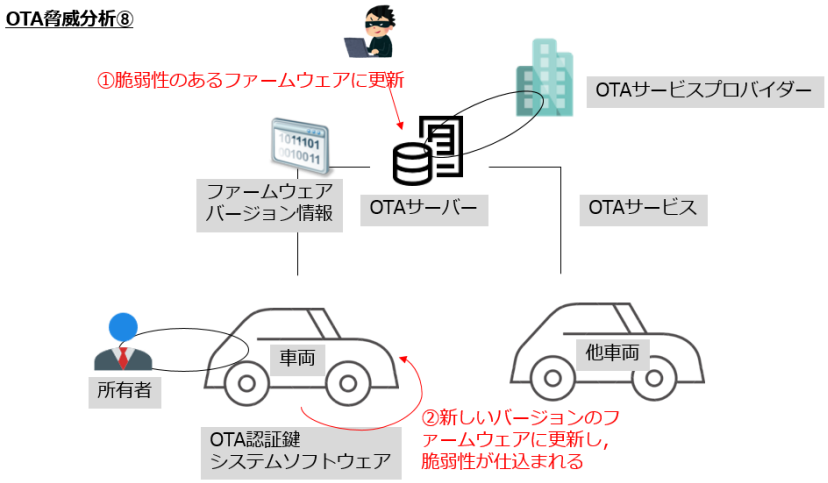
8.1.7 OTA サーバーののっとり 2

OTA サーバーをのっとることにより，古いバージョンのソフトウェアにロールバックさせる.

シナリオ番号		7
ユースケース名		OTA サーバーのなりすまし
資産		車両，システムソフトウェア
攻撃ゴール/攻撃目標		OTA サーバーになりすますことにより，OTA を実施する車両すべてに悪意のあるソフトウェアを
攻撃方法の例		OTA サービスを無限に繰り返すような妨害攻撃を実行する.
攻撃説明		OTA サービスで使用するプロトコルが漏洩すると，車両からバージョンアップ完了したという通知を妨害することにより，無限にバージョンアップを引き起こさせるような攻撃が可能になる.
攻撃説明図		
リスク算定結果	T	T3
	C	C0
	S	S3
関連ユースケース番号		OTA サーバーののっとり 1　OTA サーバーの改ざん

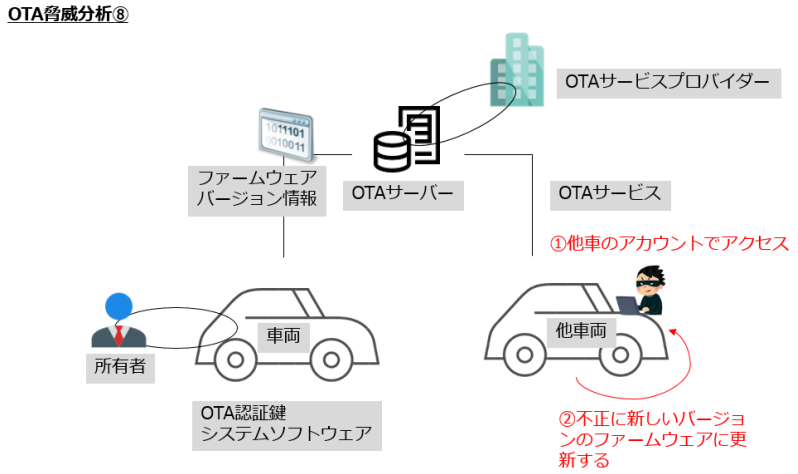
8.1.8 OTA サーバーの改ざん

OTA サーバー上のファームウェアを改ざんすることにより，悪意のあるファームウェアをダウンロードさせる.

シナリオ番号		8
ユースケース名		OTA サーバーの改ざん
資産		OTA サーバー，ファームウェア
攻撃ゴール/攻撃目標		OTA サーバー上にあるファームウェアを改ざんすることにより，誤ったファーウェアを配布させる.
攻撃方法の例		OTA 上の特権ユーザー情報を用いて，ファームウェアを不正に書き換える.
攻撃説明		OTA サーバーに用意されたバージョンアップ用のファームウェアを攻撃者が書き換えることにより実現する. この書き換え攻撃に対しては，本来秘密鍵で署名しておくことにより対策は可能であるが，車両側でその署名を検証できる能力を有しているかに依存する.
攻撃説明図		
リスク算定結果	T	T3
	C	C0
	S	S3
関連ユースケース番号		OTA サーバーののっとり 1　OTA サーバーののっとり 2

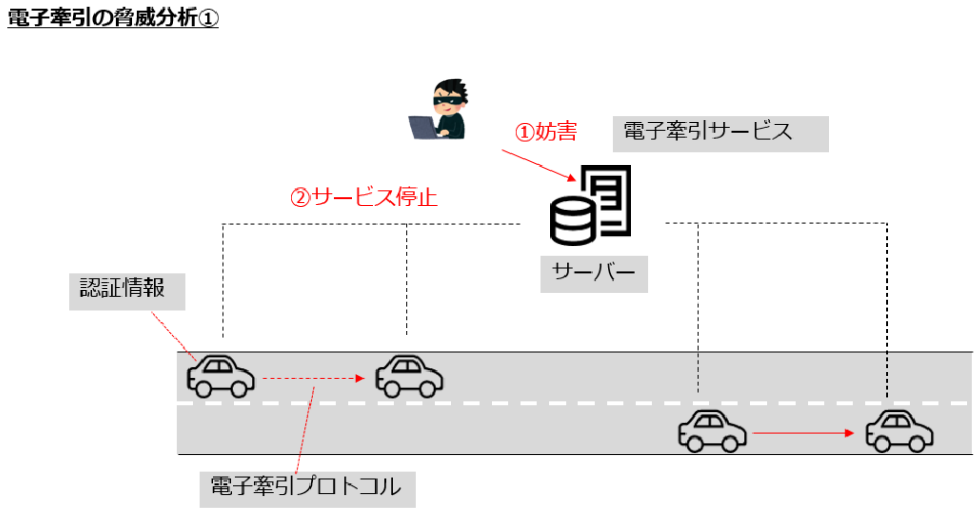
8.1.9 OTA サーバーの不正利用

OTA サービスの更新期限が切れているにもかかわらず，別のユーザーアカウントを使って不正利用する.

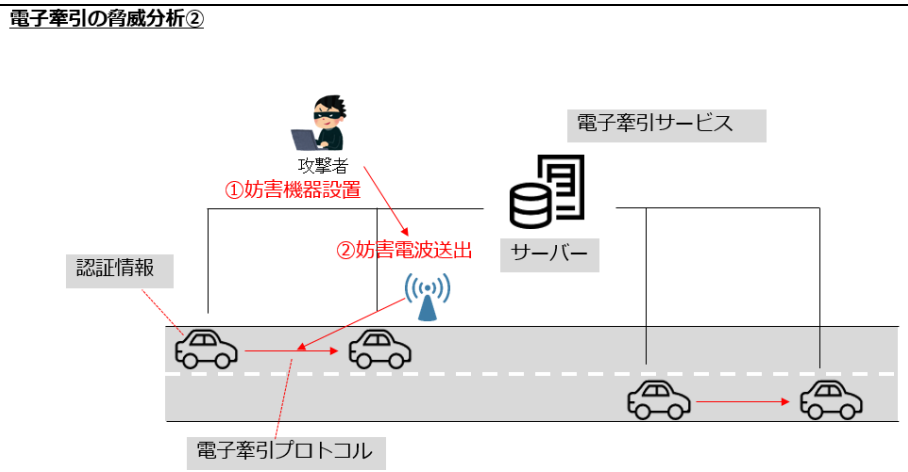
シナリオ番号		9
ユースケース名		OTA サーバーの不正利用
資産		OTA 認証情報
攻撃ゴール/攻撃目標		正規のユーザーのふりをして，フリーランチする.
攻撃方法の例		OTA サーバーへのアクセスするため，正規の所有者情報を利用する.
攻撃説明		所有者情報を用いて，サービスを使用できないユーザーや車両がファームウェアをアップデートしようとする攻撃を指す. これは，例えば機能制限されている車両の機能制限を解除したり，新しいアプリケーションなどをタダで利用しようとするユーザーの悪事により実行される場合がある. もしくは，所有者情報を不正に利用とする攻撃者などの場合もある.
攻撃説明図		
リスク算定結果	T	T3
	C	C2
	S	S3
関連ユースケース番号		なし

8.2 電子牽引

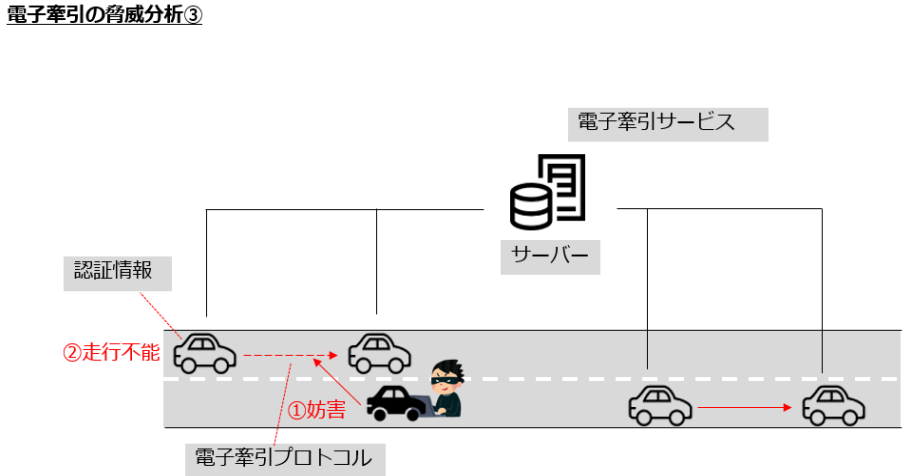
8.2.1 電子牽引サーバーの妨害

シナリオ番号		1
ユースケース名		電子牽引サーバーの妨害
資産		電子牽引システムの可用性
攻撃ゴール/攻撃目標		電子牽引サービスの妨害
攻撃方法の例		電子牽引サーバーに DoS 攻撃を仕掛けるなどしてサービスを妨害
攻撃説明		電子牽引サービスを実行するための認証サーバーなどを妨害することにより，電子牽引サービスそのものを妨害する攻撃のことである．攻撃者は，電子牽引サーバーの IP アドレスなどからサーバーへの攻撃を実施する．攻撃が成功すると，すべての電子牽引処理が停止する．さらに，悪い場合には電子牽引サービスが実行できずに，物流が停止するなど事業継続が難しくなる．
攻撃説明図		
リスク算定結果	T	T3
	C	C3
	S	S3
関連ユースケース番号		なし

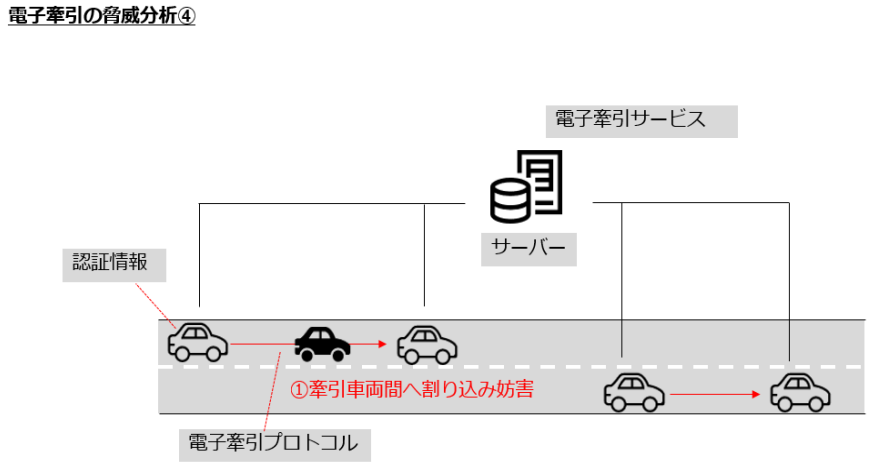
8.2.2 追従中の妨害

シナリオ番号		2
ユースケース名		先頭車両への妨害
資産		電子牽引プロトコルの可用性
攻撃ゴール/攻撃目標		電子牽引プロトコルの妨害
攻撃方法の例		電子牽引プロトコルに妨害電波を注入
攻撃説明		電子牽引中に，攻撃者が設置した妨害機器から妨害電波により電子牽引プロトコルのセッションが終了．電子牽引中の後続車両自体は自走することにより安全に停止するなどの対策が必要になる． 攻撃者の能力としては，電子牽引でプロトコルの内容を知らなくても，妨害電波を送出することにより，電子牽引を解除できるため，容易に実行することが可能である．
攻撃説明図		
リスク算定結果	T	T3
	C	C3
	S	S3
関連ユースケース番号		なし

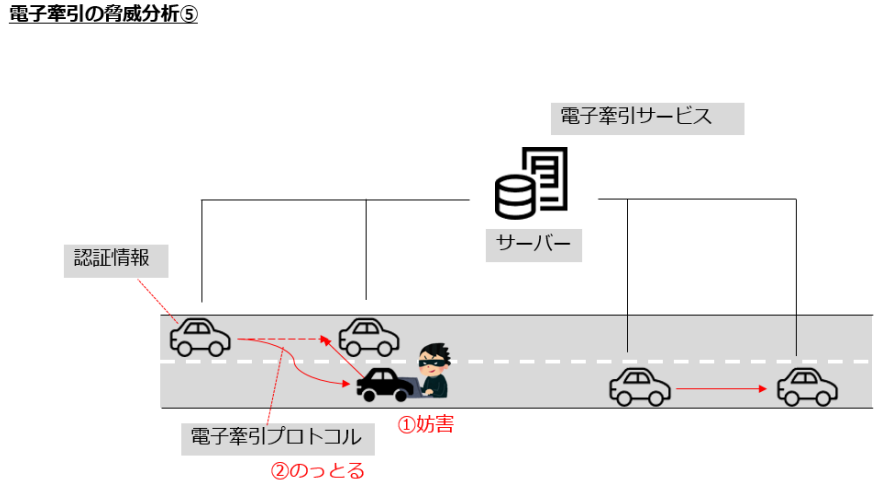
8.2.3 電子牽引プロトコルの妨害 1

シナリオ番号		3
ユースケース名		電子牽引プロトコルの妨害 1
資産		電子牽引プロトコルの可用性
攻撃ゴール/攻撃目標		電子牽引プロトコルの妨害
攻撃方法の例		電子牽引プロトコルのセッション確立時や電子牽引中に妨害するなど.
攻撃説明		電子牽引を開始しようとしても，電子牽引が開始できない．この場合，後続車両の無人化は難しいため，自走する必要がある．自走することが難しい車両の場合はサービスが実行できなくなる．さらに悪い場合には，電子牽引中に妨害電波を受けて，電子牽引が強制解除する．有人で自走する場合は，フェールセーフにより被害が低減する可能性があるものの，Lv5 の場合には，後続車が自立して走行することが求められる．
攻撃説明図		
リスク算定結果	T	T3
	C	C3
	S	S2
関連ユースケース番号		電子牽引プロトコルの妨害 2

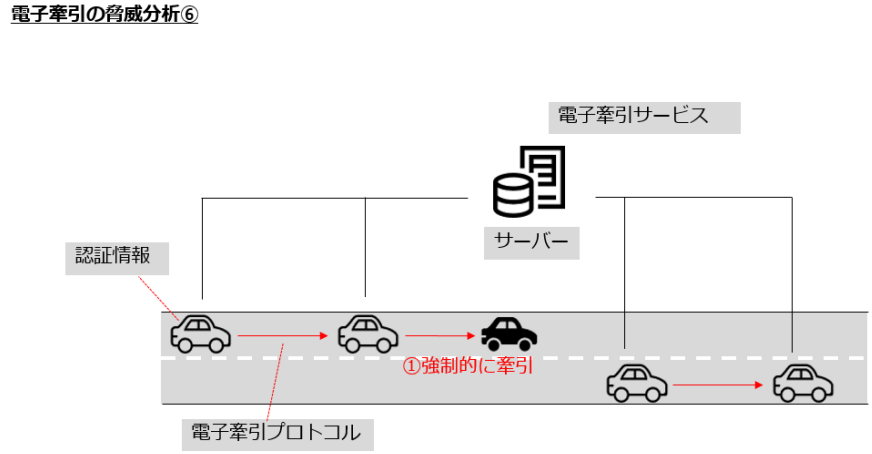
8.2.4 電子牽引プロトコルの妨害 2

シナリオ番号		4
ユースケース名		電子牽引プロトコルの妨害 2
資産		電子牽引プロトコルの可用性
攻撃ゴール/攻撃目標		電子牽引プロトコルの妨害
攻撃方法の例		電子牽引プロトコルのセッション確立後，電子牽引中に妨害するなど.
攻撃説明		電子牽引を開始後，走行中に電子牽引車両間の間に，攻撃者の車が割り込むなどにより妨害する. 攻撃車両ではない通常の車両が 1 台程度の割り込みでは特に問題ない場合でも，攻撃者はジャミングするツールなどを用いて，故意に妨害することができる.
攻撃説明図		
リスク算定結果	T	T3
	C	C3
	S	S2
関連ユースケース番号		隊列走行の妨害 1

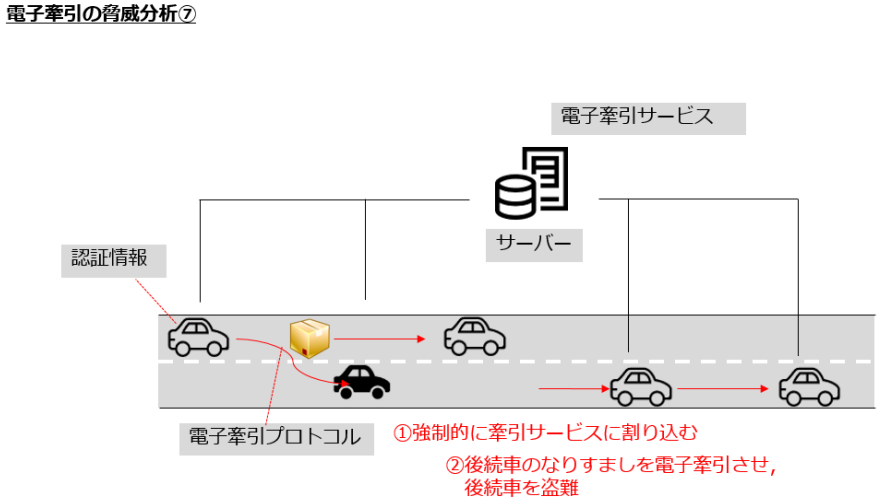
8.2.5　追従を悪用したのっとり 1

シナリオ番号		5
ユースケース名		追従を悪用したのっとり 1
資産		自車両(車両自体)あるいは他車両を含む
攻撃ゴール/攻撃目標		車両の盗難
攻撃方法の例		電子牽引プロトコルのリカバリ処理を悪用
攻撃説明		電子牽引プロトコルで，ノイズなどにより再接続する場合には，再接続先になりすまし，追従車両の牽引を乗っ取る．このような攻撃は発生する可能性があるものの，先頭車両側に居る運転手が犯行に気付く可能性は高い．しかしながら，牽引されている追従者を盗難することが可能になる．
攻撃説明図		
リスク算定結果	T	T3
	C	C3
	S	S2
関連ユースケース番号		追従を悪用したのっとり 2　後続車車両のなりすまし

8.2.6　追従を悪用したのっとり 2

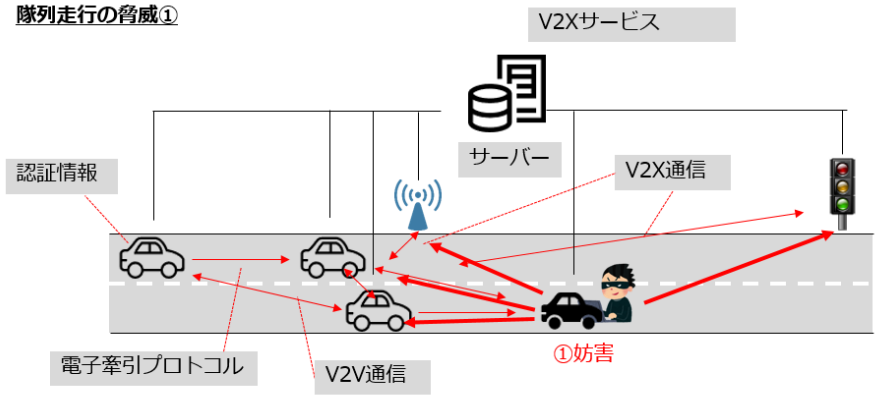
シナリオ番号		6
ユースケース名		追従を悪用したのっとり 2
資産		自車両(車両自体)あるいは他車両を含む
攻撃ゴール/攻撃目標		車両の盗難
攻撃方法の例		電子牽引プロトコルの脆弱性を利用
攻撃説明		電子牽引プロトコルの再接続や強制接続を悪用し，攻撃者が電子牽引している車両ごと制御を乗っ取る．この場合には，先頭車両に乗車している運転手により，強制的に電子牽引処理を中断させることにより，制御を取り戻すことが可能になる．一方，電子牽引システム上，このような強制解除が存在しない場合には，乗っ取りが成功する．
攻撃説明図		
リスク算定結果	T	T3
	C	C3
	S	S2
関連ユースケース番号		追従を悪用したのっとり 1　後続車車両のなりすまし

8.2.7 後続車車両のなりすまし

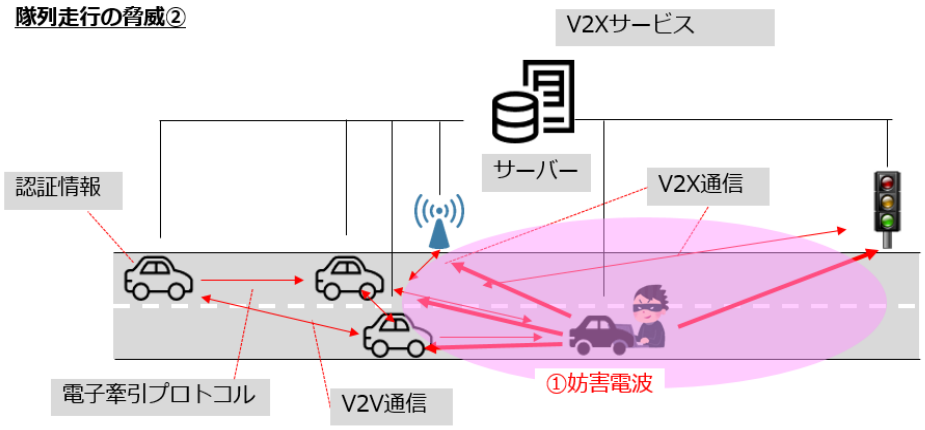
シナリオ番号		7
ユースケース名		後続車両のなりすまし
資産		後続車両
攻撃ゴール/攻撃目標		後続車両になりすます機器を電子牽引させることにより，正規の後続車を盗難する
攻撃方法の例		電子牽引中の車両間への割り込みと後続車両のなりすまし
攻撃説明		電子牽引中に先頭車両と後続車両の間に攻撃車両が割り込むことにより，電子牽引プロトコルの強制解除を発動．強制解除された後続車両に対して，先頭車両のふりをして，攻撃者の車両に後続車両の牽引を実行する． 後続車両のシステムの構成に依存するが，少なくとも，強制解除による実行時の状態変化に対して，認証サービスが必要になる．もし仮に，認証が実行されない場合は，互いに共有された地図情報などから自律走行するなども有効と考えられる．
攻撃説明図		
リスク算定結果	T	T3
	C	C3
	S	S2
関連ユースケース番号		追従を悪用したのっとり 1　追従を悪用したのっとり 2

8.3 隊列走行

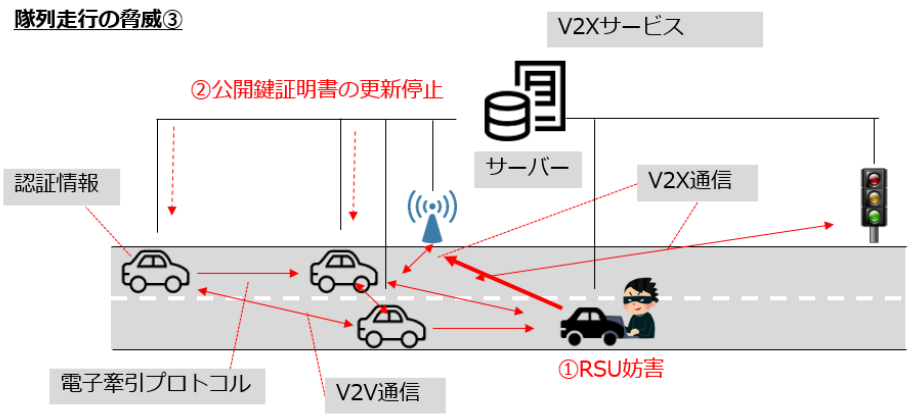
8.3.1 隊列走行の妨害 1

シナリオ番号		1
ユースケース名		隊列走行の妨害 1
資産		V2X 通信の可用性
攻撃ゴール/攻撃目標		V2X 通信の機能停止と隊列走行の強制解除
攻撃方法の例		隊列走行中に，隊列走行を妨害する車両が侵入する．隊列走行中の車両群に対して，妨害電波やなりすましメッセージを大量に浴びせるなどにより，正しい判断をさせることを難しくする可能性がある．
攻撃説明		隊列走行中に，攻撃者が設置した妨害機器あるいは妨害車両から妨害電波により V2X 通信に対して，妨害電波や妨害メッセージを大量に送信することにより実現する．多くの V2V 通信を用いて隊列走行する車両では，車両内で受信したメッセージの優先度（自車位置から近い位置に居る他車両からのメッセージを優先的に処理する）ことより，攻撃者がこれらの優先度の高いメッセージを多量受信した結果，発生する．
攻撃説明図		
リスク算定結果	T	T3
	C	C3
	S	S2
関連ユースケース番号		隊列走行の妨害 2 RSU の妨害

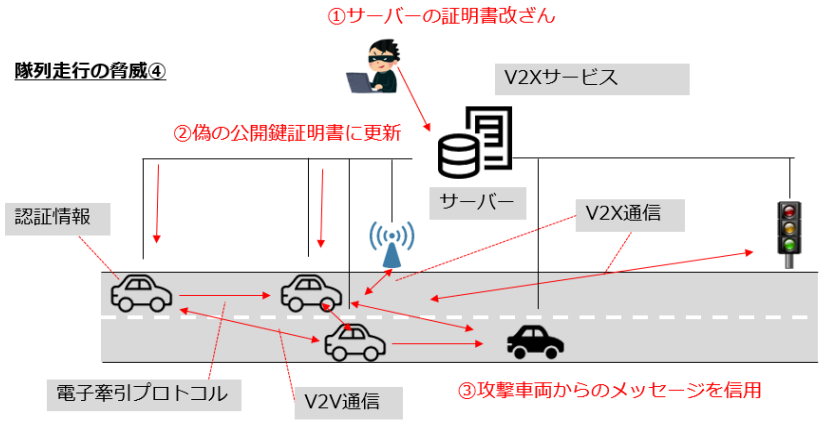
8.3.2 隊列走行の妨害 2

シナリオ番号		2
ユースケース名		隊列走行の妨害 2
資産		自車両および他車両の乗員の安全や健康
攻撃ゴール/攻撃目標		V2X 通信の機能停止と隊列走行の強制解除
攻撃方法の例		V2X 通信をジャミングする
攻撃説明		V2X 通信をエラーにするような電波を送信することにより，V2X 通信を不能にする．これにより，車群としては動作せず，各自の保持するセンサを用いて自律走行する必要がある．
攻撃説明図		
リスク算定結果	T	T3
	C	C3
	S	S2
関連ユースケース番号		隊列走行の妨害 1 RSU の妨害

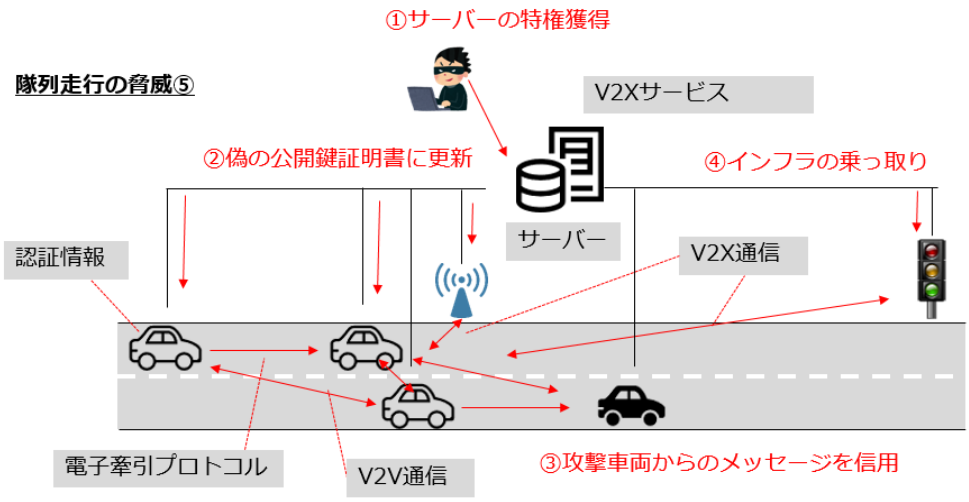
8.3.3 RSU の妨害

シナリオ番号		3
ユースケース名		RSU の妨害
資産		RSU の可用性
攻撃ゴール/攻撃目標		RSU の機能停止
攻撃方法の例		V2X 通信の証明書検証を不能
攻撃説明		V2X 通信の隊列中の他車両から V2X 通信にめ CAM を受け取るが，証明書が更新されないため，付与される証明の検証ができなくなる．この場合，V2X 通信の信頼性がなくなるため，各車両は車群を解除し，各自の保持するセンサを用いて自律走行する必要がある．
攻撃説明図		
リスク算定結果	T	T2
	C	C3
	S	S2
関連ユースケース番号		隊列走行の妨害 1 隊列走行の妨害 2

8.3.4 サーバー上の証明書改ざん

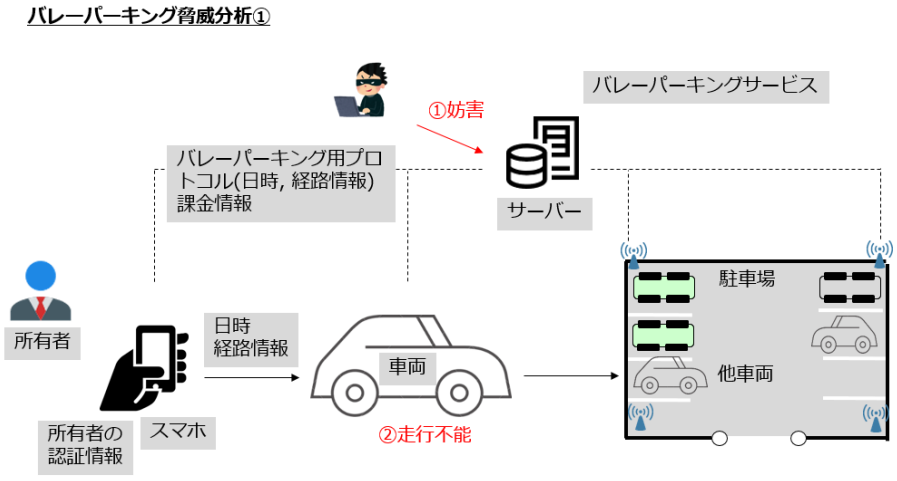
シナリオ番号		4
ユースケース名		サーバー上の証明書改ざん
資産		証明書の改ざん
攻撃ゴール/攻撃目標		証明書を改ざんすることで，攻撃車両のメッセージの注入
攻撃方法の例		V2X 通信におけるなりすましを実行するために，証明書を改ざん
攻撃説明		V2X 通信の隊列中の他車両から V2X 通信にめ CAM を受け取るが，攻撃車両からの CAM は署名検証が正しく行われないため，無視される．しかしながら，改ざんされた証明書がインストールされてしまう場合には，攻撃車両からの V2V 通信を信じてしまう．この場合，V2X 通信の信頼性がなくなるが，騙されてしまう．
攻撃説明図		
リスク算定結果	T	T3
	C	C3
	S	S2
関連ユースケース番号		管制サーバーののっとり

8.3.5 管制サーバーののっとり

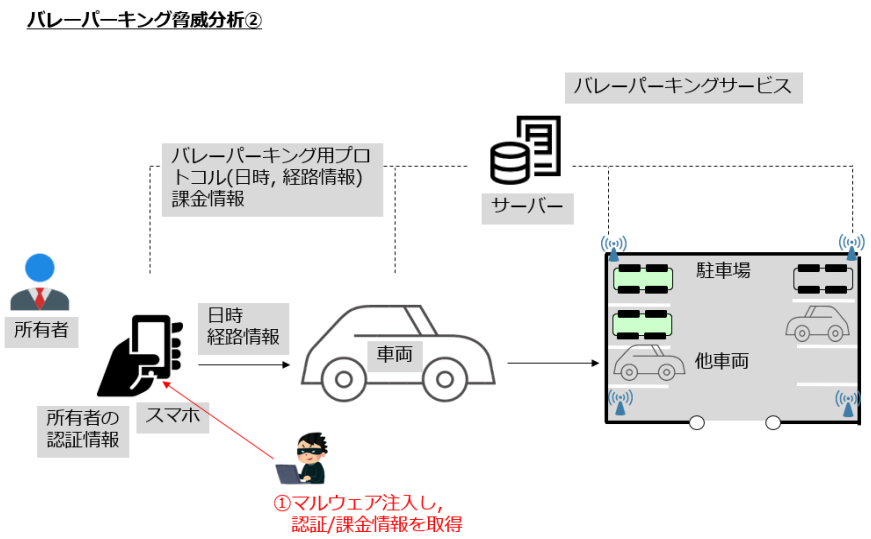
シナリオ番号		5
ユースケース名		管制サーバーののっとり
資産		V2X 通信の信頼性，可用性
攻撃ゴール/攻撃目標		V2X 通信ののっとり
攻撃方法の例		V2X 通信におけるなりすましと交通管制の乗っ取り
攻撃説明		V2X 通信の隊列中の他車両から V2X 通信にめ CAM を受け取るが，攻撃車両からの CAM は署名検証が正しく行われないため，無視される．しかしながら，改ざんされた証明書がインストールされてしまう場合には，攻撃車両からの V2V 通信を信じてしまう．この場合，V2X 通信の信頼性がなくなるが，騙されてしまう．また，交通管制を攻撃者が制御可能となり，交通システムへの混乱を引き起こすことが可能になる．
攻撃説明図		
リスク算定結果	T	T3
	C	C3
	S	S3
関連ユースケース番号		サーバー上の証明書改ざん

8.4 バレーパーキング

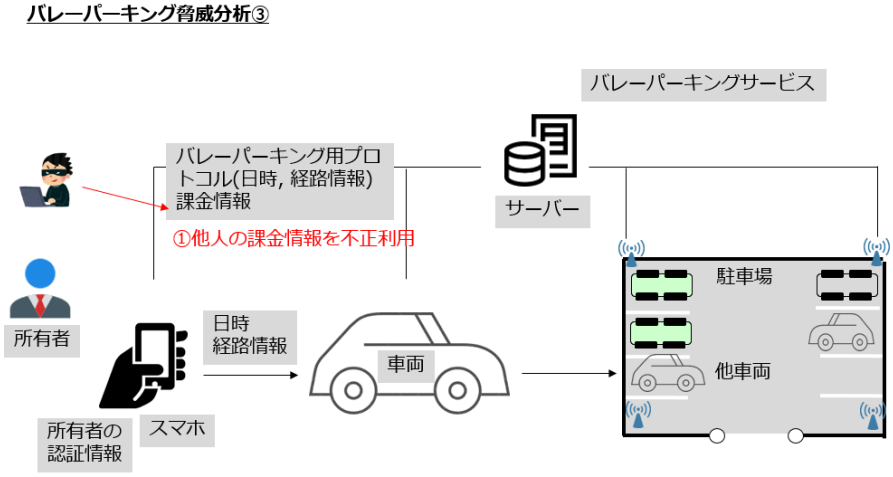
8.4.1 バレーパーキングの妨害

シナリオ番号		1
ユースケース名		バレーパーキングの妨害
資産		バレーパーキング中の車両
攻撃ゴール/攻撃目標		バレーパーキングシステムを停止させる.
攻撃方法の例		バレーパーキングサーバーを攻撃することにより，バレーパーキングを停止させる.
攻撃説明		バレーパーキングサーバーに DoS 攻撃などを仕掛けることにより，バレーパーキングシステムを動作できないようにする. このような場合に，バレーパーキング中に車が入庫できないとか，駐車場から出庫できないなどのトラブルを引き起こすことが可能になる. バレーパーキングのサービス事業者は金銭的な補償を含め，多大な損害を被る.
攻撃説明図		
リスク算定結果	T	T1
	C	C1
	S	S2
関連ユースケース番号		なし

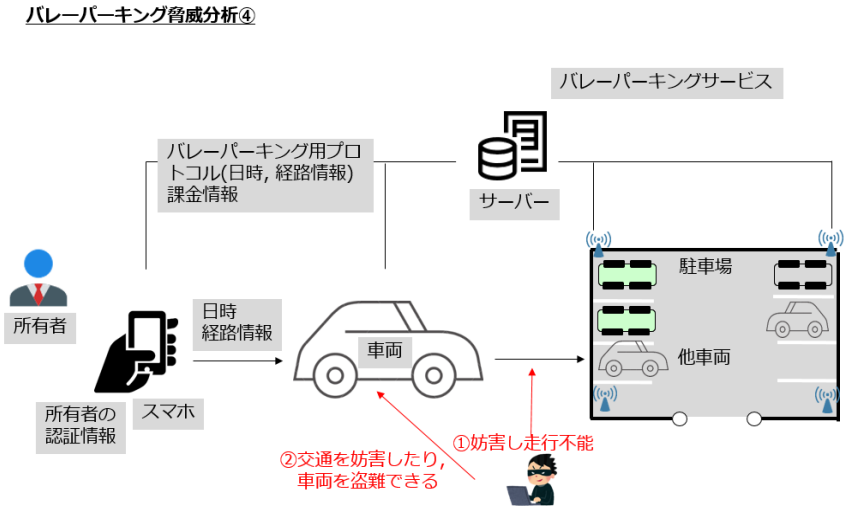
8.4.2 バレーパーキング用プロトコルの漏洩

シナリオ番号		2
ユースケース名		バレーパーキング用プロトコルの漏洩
資産		バレーパーキング上の課金情報や経路情報，所有者の認証情報など
攻撃ゴール/攻撃目標		所有者の認証情報などを盗む
攻撃方法の例		バレーパーキング車両と紐づけられたスマホから認証情報などを盗む．
攻撃説明		バレーパーキングに使用するスマホなどにマルウェアを注入し，そのマルウェアから課金情報などを盗み出す．また，バレーパーキングを利用している人のスマホを盗難したり，ショルダーハックするなどして情報を盗むことでも攻撃可能となる．ただし，より多くの情報を盗むには，マルウェアなどにより収集する方がシビアといえる．また，サーバーを攻撃することにより，情報を入手することも可能となる．
攻撃説明図		
リスク算定結果	T	T1
	C	C1
	S	S2
関連ユースケース番号		バレーパーキングの不正利用　バレーパーキング中の車両盗難

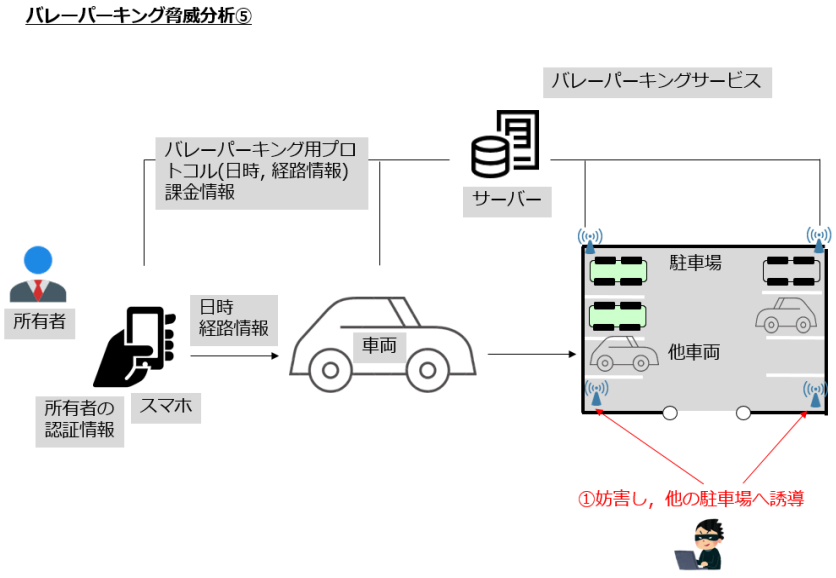
8.4.3 バレーパーキングの不正利用

シナリオ番号		3
ユースケース名		バレーパーキングの不正利用
資産		バレーパーキングに用いられる認証情報や課金情報
攻撃ゴール/攻撃目標		他人の情報を利用して，不正にバレーパーキングを利用する．また，他人の車両を呼びつけることにより，車両盗難する場合もある．
攻撃方法の例		不正に入手したバレーパーキングの認証情報を用いて，サービスを不正利用する．
攻撃説明		他人の決済情報などを用いて，バレーパーキングサービスを利用する．これにより，請求はなりすまされたユーザーに課金される．
攻撃説明図		
リスク算定結果	T	T3
	C	C3
	S	S2
関連ユースケース番号		バレーパーキング用プロトコルの漏洩

8.4.4 バレーパーキング中の車両盗難

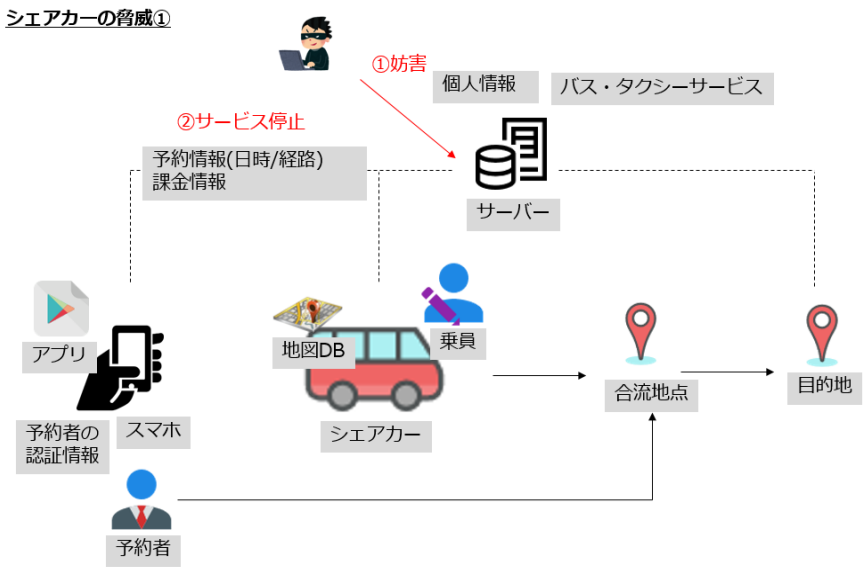
シナリオ番号		4
ユースケース名		バレーパーキング中の車両盗難
資産		車両自体
攻撃ゴール/攻撃目標		車両の盗難
攻撃方法の例		バレーパーキング中の車両に対する妨害などによりバレーパーキングの強制解除
攻撃説明		バレーパーキング中に，車両を停止あるいは妨害などにより，強制的に意図しない場所へと誘導する．あるいは，バレーパーキング中に意図しないような車両システムへの妨害を行うことにより，走行不能にする．これにより，車両盗難を実行する．または，特定の車両を不正に誘導するなどを行う．
攻撃説明図		
リスク算定結果	T	T3
	C	C3
	S	S2
関連ユースケース番号		バレーパーキング用プロトコルの漏洩

8.4.5 意図しない駐車場への誘導

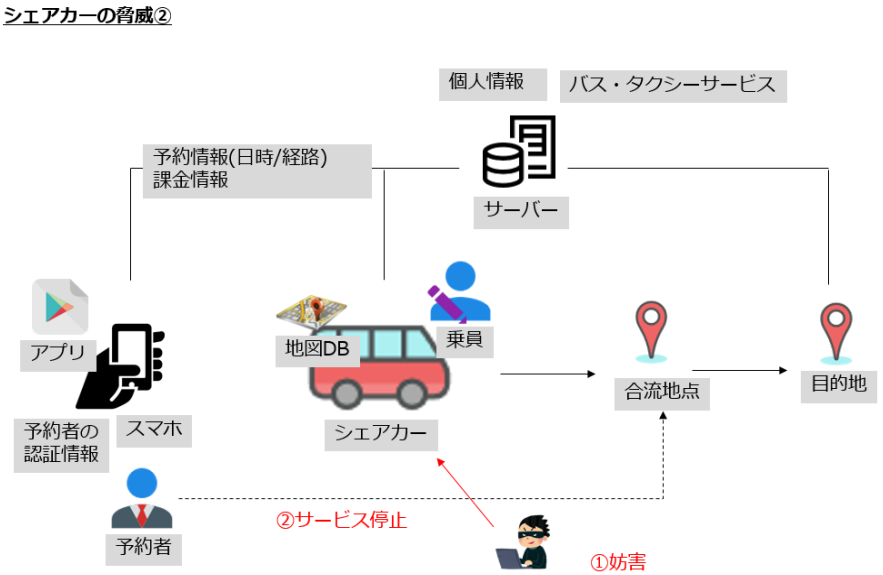
シナリオ番号		5
ユースケース名		意図しない駐車場への誘導
資産		車両自体
攻撃ゴール/攻撃目標		車両盗難
攻撃方法の例		ユーザーが目的地として設定した駐車場の位置情報を改ざんするような攻撃を実施する．例えば，自動運転車両の位置情報を改ざんするような攻撃を実施する．例えば，衛星からの位置情報を妨害する．あるいは，地図上のバレーパーキングの位置情報を改ざんする．あるいは，目的地となっているバレーパーキングを満車と認識させるような妨害電波を発生させ，別の意図しない駐車場へ駐車させる．
攻撃説明		幾つかの方法で意図しない駐車場へ誘導する方法がある．1 つ目は，目的となる駐車場の情報を妨害するなどして利用不能にしてしまい，他の駐車情報へ誘導させる．2 つ目に，スマホなどから指定する駐車場をプロトコルを改ざんするなどして，改ざんされた別の駐車場へと誘導するなどである．
攻撃説明図		
リスク算定結果	T	T3
	C	C3
	S	S2
関連ユースケース番号		なし

8.5 シェアカー(バス，タクシー)

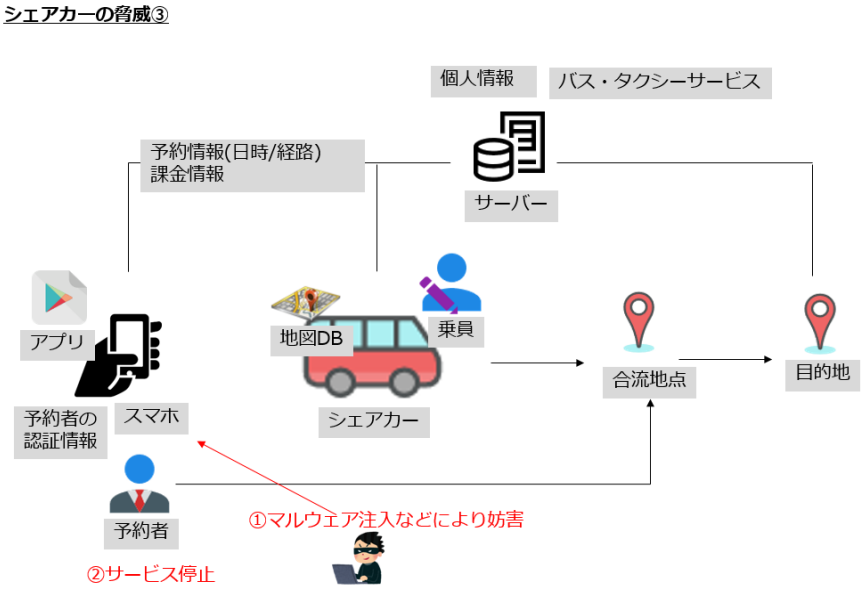
8.5.1 シェアカーサービスへの妨害

シナリオ番号		1
ユースケース名		シェアカーサービスへの妨害
資産		シェアカーのシステム／サーバー
攻撃ゴール/攻撃目標		シェアカーサーバーの不作動
攻撃方法の例		不特定多数が同時にシェアカーを呼び出すなどにより，サービスを妨害する攻撃
攻撃説明		シェアカーを呼び出すことにより，シェアカーシステムの妨害を実現する．このほかにも，様々な手順により妨害攻撃を実現することが可能となる．例えば，シェアカーを運営する事業者のサーバーに DoS 攻撃を仕掛ける．
攻撃説明図		
リスク算定結果	T	T3
	C	C1
	S	S3
関連ユースケース番号		なし

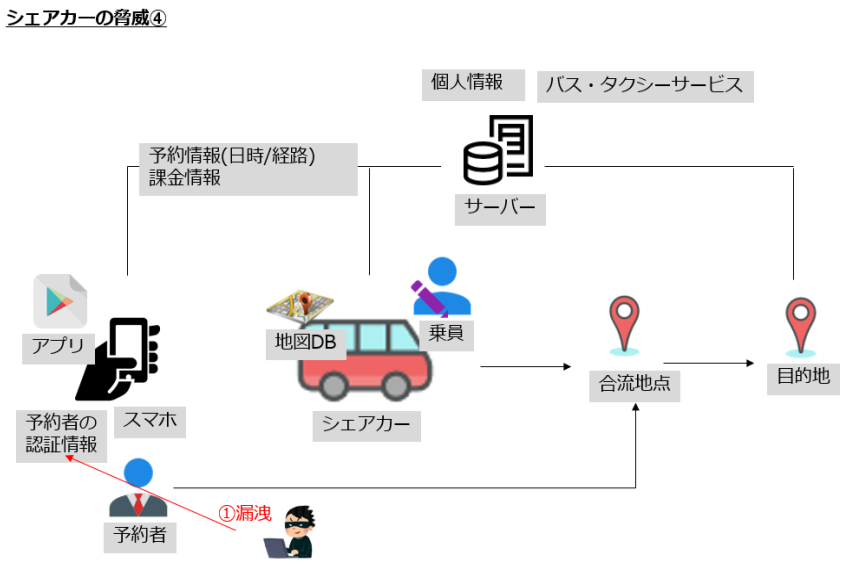
8.5.2 シェアカーへの妨害 1

シナリオ番号		2
ユースケース名		シェアカーへの妨害 1
資産		シェアカー(車両)
攻撃ゴール/攻撃目標		シェアカーの動作を停止させる
攻撃方法の例		シェアカーを移動できないようにする.(例えば,シェアカーをサークル内に閉じ込めるなど)
攻撃説明		特定のシェアカーをある場所から移動させないようにすることにより,シェアカーを不作動にさせる.個別の車両で起きた場合には,それほど影響はないことが想定されるが,サービスやメンテナンスの負荷を上げる.
攻撃説明図		
リスク算定結果	T	T3
	C	C3
	S	S3
関連ユースケース番号		シェアカーへの妨害 2

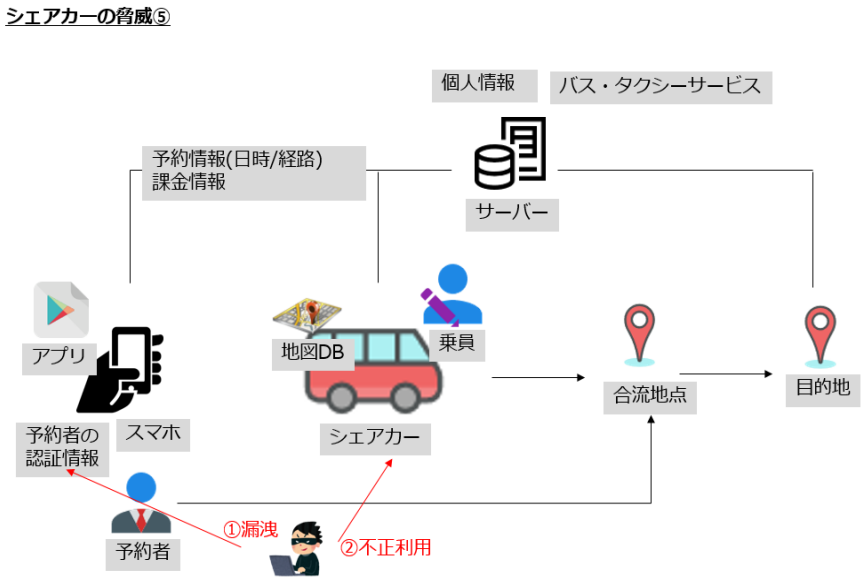
8.5.3 シェアカーへの妨害 2

シナリオ番号		3
ユースケース名		シェアカーへの妨害 2
資産		ユーザーのスマホ
攻撃ゴール/攻撃目標		ユーザーのスマホアプリの動作を停止する
攻撃方法の例		・マルウェアを用いたスマホアプリへの感染 ・シェアカーへの不正送信を繰り返す
攻撃説明		シェアカーサービスに登録したユーザーのスマホがマルウェアに感染し，異常な頻度でシェアカーサービスに対してサービスへの要求を発行する．あるいは，マルウェアがシェアカーを占有するよう予約を取り続けるなどの攻撃を実行する．
攻撃説明図		
リスク算定結果	T	T3
	C	C3
	S	S3
関連ユースケース番号		シェアカーへの妨害 1

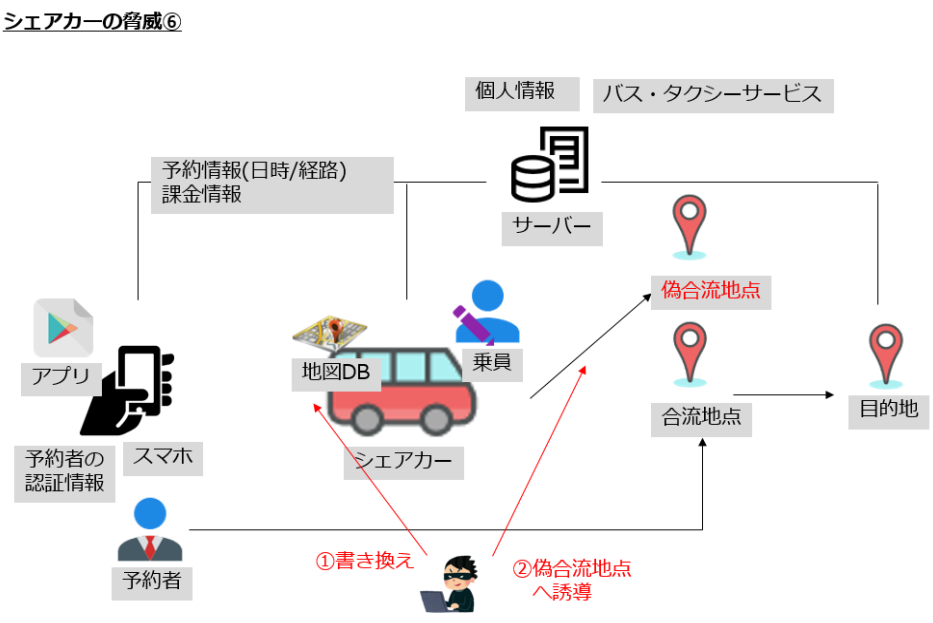
8.5.4 アカウント情報の漏洩

シナリオ番号		3
ユースケース名		アカウント情報の漏洩
資産		ユーザーのアカウント情報
攻撃ゴール/攻撃目標		ユーザーのアカウント情報を搾取する
攻撃方法の例		ユーザーのアカウント情報を搾取するため，通信を盗聴する．（そのほか，サーバー側に保存される情報を搾取）
攻撃説明		ユーザーのアカウント情報を搾取するために，ユーザーのスマホの通信を盗聴する．これにより，盗聴時の暗号などに不備がある場合には，暗号通信により保護されたデータの盗聴が可能となる．暗号化されていない場合には，当然のことながら情報が容易に漏洩する．そのほか，わかりやすいパスワードを設定するなどにより，通信路を暗号化しているかどうかにかかわらず，通信内容が漏洩することが懸念される．
攻撃説明図		
リスク算定結果	T	T3
	C	C1
	S	S2
関連ユースケース番号		ユーザーのなりすまし

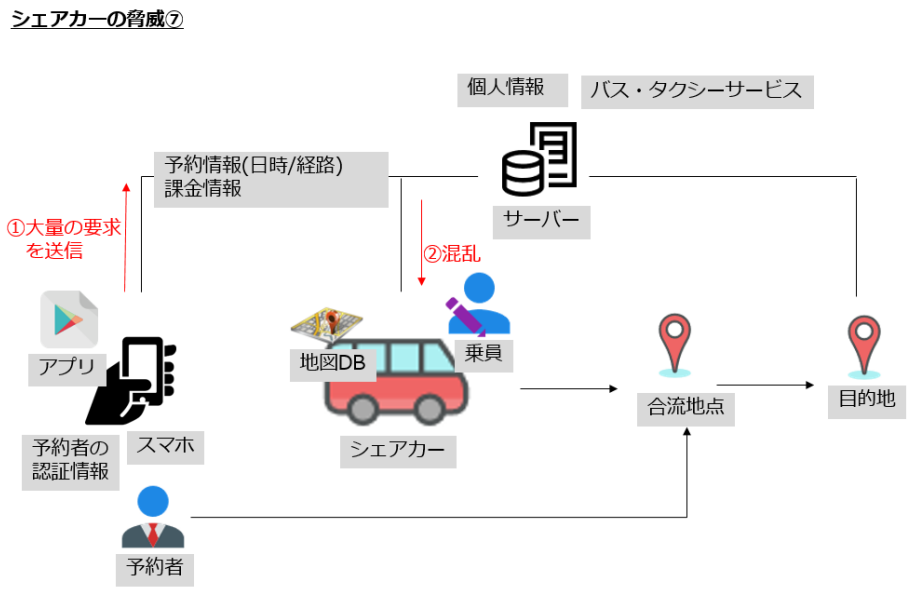
8.5.5 ユーザーのなりすまし

シナリオ番号		5
ユースケース名		ユーザーのなりすまし
資産		ユーザーのアカウント情報
攻撃ゴール/攻撃目標		ユーザーのアカウント情報を不正利用する
攻撃方法の例		ユーザーのアカウント情報を搾取し，スマホアプリに登録する，ユーザーのスマホを不セリ利用する
攻撃説明		ユーザーが要求しないにも関わらず，ユーザーのアカウント情報を不正に利用して，ユーザーのなりすましを実施する．これにより，ユーザーの意図しない利用料の請求が発生する．
攻撃説明図		
リスク算定結果	T	T3
	C	C3
	S	S3
関連ユースケース番号		アカウント情報の漏洩

8.5.6 偽地点へ誘導

シナリオ番号		6
ユースケース名		偽地点へ誘導
資産		合流地点
攻撃ゴール/攻撃目標		偽の合流地点へ呼び出す
攻撃方法の例		地図 DB や地点情報を書き換えることにより，偽の合流地点へ呼び出す.
攻撃説明		攻撃者が，シェアカーや通信プロトコル上の合流地点の情報を書き換えることにより，偽の合流地点に呼び出す．これにより，本来予約者が待っている(正しい)合流地点にはシェアカーは現れず，サービスが利用できなくなる.
攻撃説明図		
リスク算定結果	T	T3
	C	C1
	S	S3
関連ユースケース番号		なし

8.5.7 シェアカーサービスへの大量送信

シナリオ番号		7
ユースケース名		シェアカーサービスへの大量送信
資産		シェアカーサービスの可用性
攻撃ゴール/攻撃目標		ユーザーが早くシェアカーを呼びたいために大量のトラフィックを送信
攻撃方法の例		ユーザーが急いでシェアカーを呼びたいために，大量に予約情報及びキャンセル情報を送信
攻撃説明		ユーザーが急いでおり，シェアカーをすぐに呼びたいために，ある地点への呼び出しリクエストを大量に送信する．これにより，複数のシェアカーが合流地点に呼び出されるなどの混乱を引き起こす．また，最初のシェアカーが合流地点に到着した後で，大量のキャンセルリクエストを発行するなどの場合もある．
攻撃説明図		
リスク算定結果	T	T3
	C	C1
	S	S3
関連ユースケース番号		なし

9　自動運転システムのセキュリティ強化技術の状況と今後の課題

前述するように自動運転技術の導入により，様々な脅威が発生することを分析した．この章では，世の中で広くセキュリティ強化が検討されているかどうかを議論する．

9.1 自動運転車両システム

現時点では，自動運転車両システムという観点でのセキュリティ強化については十分議論されていない．特に，以下の点が課題となる．

9.1.1　センサの開発(性能限界と信頼性)

各種センサへの攻撃の内，妨害攻撃はセンサの信頼性に依存している．例えば，カメラの場合には，どの程度の照度でも画像が飛ぶことなく，物体を正しく検出可能であるかはレンズの性能に依存する．これと同様に，LIDAR や RADAR などの様々なセンサが使用されるのも，各センサによって検出可能なものと不可能なものが存在するためである．一方，軍事利用されるようなセンサを搭載する場合には，センサの信頼性は高くなるものの，値段も高くなり，一般車両に適用することは難しくなる．このため，各種センサフュージョンなどにより，信頼性を上げる手法が自動運転では様々語られているものの，セキュリティ攻撃においてセンサフュージョンが有効であるかどうか明確には語られていない．このため，どのようなセンサの組み合わせがセキュリティ上有効であるかを議論する必要がある．

9.1.2　認知の妥当性

各種センサからの入力が正しい場合にでも，自動運転車両の認知処理が正しく判定できるわけではない．つまり，100%正しく認識できるわけではなく，ある誤検知率で誤検知が発生すると考えるべきである．例えば，下図に示すように，本来はトラックが横切っているのを，鳥が飛んでいると誤検出する場合には，自動運転車両は止まることなく，トラックに突っ込んでいくことが考えられる．このように，本来人間が運転手である場合には，誤らないような状況をコンピュータでは見誤る可能性がある．これらを防ぐための手法について，様々研究されているものの，100%無くなるとは言えない状況である．これらは今後研究を進めていくことにより，解決されることが期待される．同様に，自動運転システムをどのように評価すべきか重要な研究課題となっている．

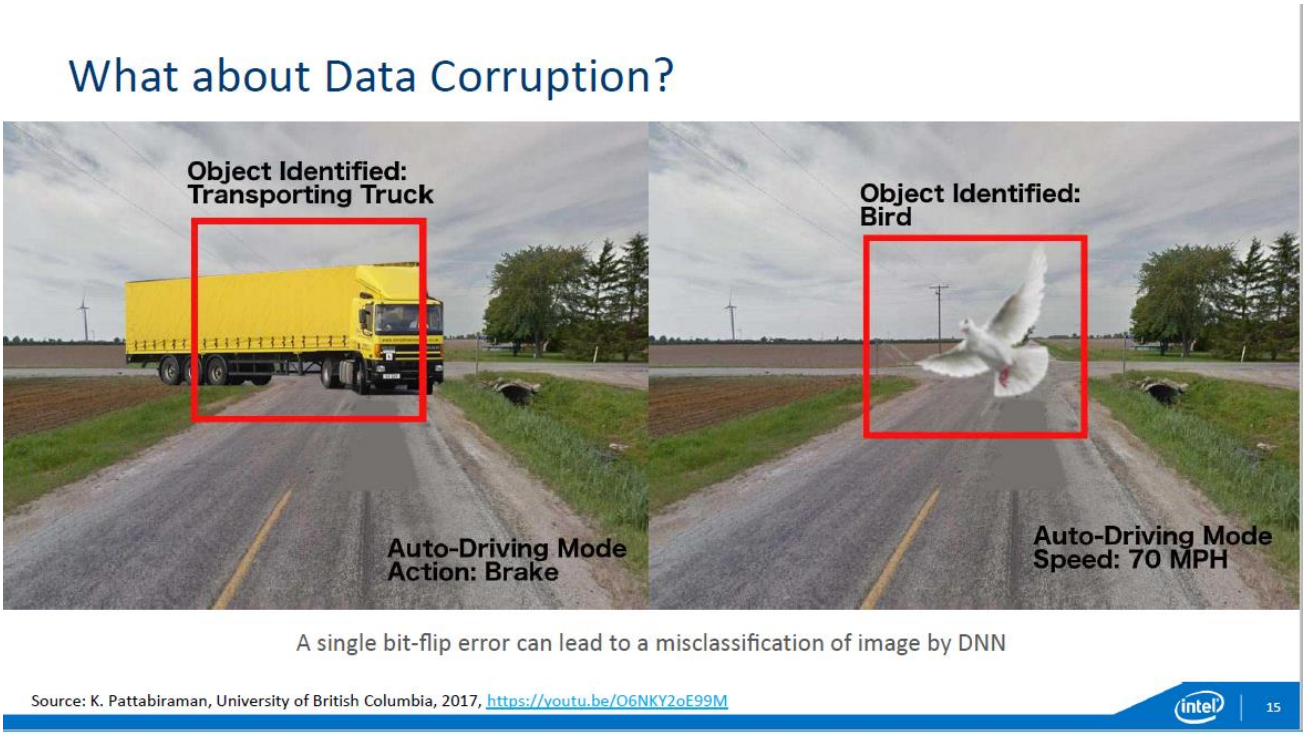


図 9-1 自動運転の認知に関する誤検出の一例 (Matthias Schunter, Vehicle to Cloud – Emerging Security Research Challenges for Intelligent Vehicles, escarEU2017 より)

9.1.3 ソフトウェアプラットフォームの信頼性

自動運転システムに適用されるソフトウェアプラットフォームの構成に応じて，顕在化する脆弱性も変化することが考えられる．例えば，Robot Operating System (ROS)をベースとする自動運転のソフトウェアプラットフォームが多数開発されているが，ROS 本体とセキュリティパッチは別で管理されており，各社が ROS で実装する場合でも，正しくセキュリティ実装がなされているかは異なる可能性がある．一方，自動運転のためのソフトウェアプラットフォームを目指す AUTOSAR Adaptive についても，様々な規約などが存在するものの，各社が提供するベース OS が QNX や Automotive Grade Linux(AGL)など様々異なることが予想される．このため，どのようなテストをした結果，ソフトウェアが正しく実装されているとするのか，あるいは正しくセキュリティが実装されていることを検証できたとするかの基準がない．このため，今後はセキュリティプロセスを含めて，どのような評価が必要かを明確にする活動が必要となる．

9.2 サービスの観点

9.2.1 OTA

一部，研究レベルでは OTA に関する脅威分析が進められているものの，これまで多くはソフトウェアプラットフォーマ(例えば，Windows の場合は Microsoft，Android の場合 Google)が管理していた．しかしながら，自動車のような組込みシステムでは，どのようにバージョン管理するかは自動車メーカーや部品サプライヤの各社で実装するソフトウェアに依存しており，ブラックボックスで扱うことは難しい．このため，様々なベンダから携帯電話などで使われるソフトウェアが提供されているが，より自動車に最適な OTA 手法については，オープンに議論されるべきである．

9.2.2 電子牽引と隊列走行

通信プロトコルは，ある自動車メーカー独自とすることはなく，標準化されたプロトコルを用いて実装されることになる．このため，これらのプロトコルについては各種標準化活動の中で，具体的なセキュリティ強化が検討されている．しかしながら一方で，プロトコルスタックを実装したソフトウェアの脆弱性についても検討されるべきである．

9.2.3 バレーパーキング，シェアカー(バス，タクシー)

バレーパーキングサービスについては，各社自動車メーカーやサービスプロバイダーに依存している．このため，各社で検討されるプロトコルや実装方法が妥当か，セキュリティ上の観点で評価する必要がある．これはシェアカーなどのサービスでも同様と言える．

10 まとめ

本論では，自動運転システムを取り巻く現状と様々な導入シナリオの観点から脅威分析を実施した．この結果，今後導入されると思われる車両システムとサービスを類型化し，その脅威を導出する方法を提示し分析を行い，様々な脅威があることを指摘した．

今後の課題として，以下の点が挙げられる． まず，脅威分析の観点として，攻撃手法の明確化を行う必要がある．これには，自動運転車両に搭載されるソフトウェアプラットフォームなどを明確化し，でどのような脅威が発生するかを検証する必要がある．また，各センサに対しても，具体的なセンサを決定した上で，その中で検出できない攻撃が存在しないかを評価する必要がある．これらの分析は，J3061 におけるシステムレベルでの設計と脅威分析の範囲となるため，本論では分析の対象外となっているが，どの程度の脆弱性が許容されるかを見積もる上では，より具体的なシステム(ハードウェアとソフトウェア)を想定した上で，もう一段具体化された脅威分析を実施する必要がある．

SYNOPSYS®

「戦略的イノベーション創造プログラム(SIP)自動走行システム／大規模実証実験」のうち「情報セキュリティ実証実験」

bセキュリティガイドラインドラフト

図表

1. フレームワークの紹介

1.1. 目的

本書の目的（しばしば「フレームワーク」とも呼ばれます）は、生産開始後に悪意ある攻撃の対象となる可能性のある自動車コンポーネントのセキュリティ OEM テスト手順を説明することです。したがって、先進部分的自律型車両用のワイヤレス（Wi-Fi）、Bluetooth、モバイル、Web サーバー、およびセルラー（LTE）コンポーネントが次の目的で主題として選択されます。

- Bluetooth 接続は、車両を公衆インターネットに接続する最も一般的な方法です。これは、通常、車両トラストゾーン外のエンドユーザーの携帯電話で行われます。
- 通常、車両内の「ホットスポット」を通じた無線ネットワーク接続は、攻撃者が車から遠く離れた距離にあり、使い易いため、悪用する最も簡単なアタックサーフェスの代表です。消費者および企業クラスの無線ネットワークで動作するのと同じツールが、車載グレードのネットワーク上で動作します。
- LTE または類似のセルラー技術は、ナビゲーションまたは無線（OTA）更新の転送など、車両内のさまざまなコンポーネントを更新するためによく使用されます。さらに、この共通技術は V2X の機能にますます使用されるようになるでしょう。この接続技術を攻撃するこのような能力は、攻撃ツールがより能力が高くなり普及していくにつれ、ますます広く使用されるようになります。
- API とも呼ばれるモバイル側とサーバー側のインターフェイスは、車両のユーザーレベル機能の共通手段となります。これらは、スマートフォンや IoT 業界で使用されているのと同じ技術であり、今日消費者によく知られているアプリケーションの大部分を構成する要素となっています。大規模なインフラストラクチャコンポーネントは、モバイルと Web サーバーテクノロジーの組み合わせで構築されているため、1 つのエクスプロイトが、車両サブシステム全体に複雑な侵害に通じる可能性があります。

1.2. 範囲

これらのセキュリティガイドラインには、ワイヤレス（Wi-Fi）、V2X、Bluetooth、モバイル、Web サーバー、セルラー（LTE）、その他の RF ベースの車両エコシステムコンポーネントが含まれていて、それらは典型的なインフォテインメントシステムに見られるインターフェイスです。これらのインターフェイスの選択の背後にある理論的根拠は、これらが攻撃者によって悪用される現代の車両で最も一般的な接続オプションであるという事実によって定義されます。これは、ジープ「uConnect」攻撃、BMW「コネクテッド・ドライブ」攻撃、テスラ ModelS「ワイヤレス LAN」攻撃、および三菱アウトランダー「ワイヤレス攻撃」を含む大きくメディア報道された脆弱性の最近の例によって証明されます。これらのすべてはセクション 2.1 でより詳細に言及します。

1.3. 補足資料

この自動車セキュリティフレームワークは、独立して動作するように、または Synopsys、Inc.によって作成された自動車 BSM や自動車全体の脅威面分析などの追加文書に沿って設計されています。これらの追加文書への言及は、本書全体にわたってありますが、このフレームワークの機能または使用にとって重要ではない補足的なものです。

このフレームワークと使用できる、より直接的な補足的文書は、『Tooling and OEM Matrices』です。これはセキュリティ関連ツールに馴染みのない OEM QA エンジニアがそのテストと理解に役立てるように作成された資料です。これらの資料は本文書の機能には重要ではありませんが、フレームワークテスト項目ごとのテストの効率と OEM の理解を高めることを目的に作成されているため、その理解を深める上では大きく役立ちます。

1.4. 規格準拠

1.4.1. 品質、安全性、セキュリティ

このフレームワークをセキュリティガイドラインとして使用することに関連して、本書は、主に「サイバーフィジカル自動車システムのサイバーセキュリティガイドブック」（SAE J3061）および ISO 26262 の自動車セキュリティサブセクション 6 の補足文書となります。本書は、2 つのガイドラインに関する機能試験と技術試験の違いを理解するための橋渡しとなることを目的としています。さらに、JasPar、SAE J2980 および ISO 21434 をテストケースおよび修正ガイドラインを作成する際に考慮します。本書で言及している各規格は、車両試験全体の 3 つの基本的な領域に焦点を当てています。品質、安全性、セキュリティ本書では、セキュリティの重要性と、品質テストと機能安全性テストのニーズとのバランスを取るセキュリティの必要性に焦点を当てています。また、テストエンジニアは、障害状態が安全クリティカルシステムにいつ、どのように影響するか、どのような安全状態が失敗する可能性があるか、またどのように引き起こされるべきかを判断できる必要があります。そのようなエンジニアは、適切な関係者に全体的な見解を提示するためのセキュリティテストの意味を理解しながら、結果を解釈して提示することができなければなりません。

1.4.2. JasPar

日本の自動車ソフトウェアプラットフォームおよびアーキテクチャ（JasPar）規格に従って、この文書では、テストごとに成功基準不合格という合理的かつ修正ガイドラインでまとめた、成功基準、再現手順、および各コンポーネントに対する既知の攻撃と技法を利用するためのコマンド例を含むテスト基準項目を構成します。これは、道路を走行している車両のコンポーネントをテストする際に、セキュリティの失敗の意味とその車両安全性への影響にさらなる洞察を提供することを目的としています。JasPar がどのようにアプローチしたかについてのより明快な説明は、この文書のセクション 5.2 に見られます。

1.4.3. SAE J3061

自動車サイバーセキュリティテストの基本的要件の基礎として、2015 年に「サイバーフィジカル自動車システムに対するサイバーセキュリティのガイドブック（Cybersecurity Guidebook for Cyber-Physical Vehicle Systems）」（SAE J3061）と題される規格が米国自動車技術会（SAE）によって発行され、このフレームワーク文書がこのような一連のサイバーセキュリティテスト要件を開発するための出発点です。SAE J3061 は、以来、道路車両に焦点を当てたサイバーセキュリティ関連活動の ISO 規格開発の基礎として使用されてきました。この ISO 規格は ISO 21434 として参照されており、SAE J3061 とそれに続く資料を補完します。

1.4.4. ISO 26262

ISO 26262 は自動車向けの機能安全規格 IEC 61508 に適合しています。ISO 26262 は、すべての車載電子および電気安全関連の重要システムのライフサイクルに亘って適用可能な自動車機器の機能安全を定義しています。ISO 26262 の自動車安

全サブセクション 6 の機能安全基準の遵守を維持するために、必須のテスト項目の分類を含む、すべてのテストシナリオと推奨改善策が、セキュリティ違反が発生した場合に安全重要システムへの影響を最小限に抑えるために選択されています。テスト項目の車両セキュリティおよび分類への適用範囲に関する詳細は、セクション **5.3**で参照されます。

1.4.5. SAE J2980

SAE J2980 に準拠したこの文書推奨の試験および修正ガイドラインを確実にするためのさらなる措置が講じられています。この文書には、車載用電気・電子（E/E）システムの自動車安全性レベル（ASIL）を決定するテスト項目が含まれています。この文書の技術的な焦点は車両無線周波数（RF）制御システムおよびアプリケーションにあり、重量 3.5 トン以上の乗用車のテストケースに限定されているため、衝突の危険性から、テストの失敗の結果起こる可能性のある他の関連する機能や事故にまで広がっています。

2. 自動車セキュリティの背景

このセクションでは、この文書の必要性を生じさせている自動車エクスプロイトとその内容を網羅して、自動車の現在のセキュリティ状態を探ることになります。この文書のユーザーがこれらのエクスプロイトを車両セキュリティのベースラインとして目標に設定してテストを実行できるよう、明示的なフレームワークテスト項目を参照項目として記述しています。これらのテスト項目は、「関連するフレームワークテスト項目」という見出しの下でセクションごとに参照できます。

2.1. 以前に知られていたエクスプロイト

2.1.1. BMW コネクテッド・ドライブ

2015 年にドイツ自動車協会（ADAC）は BMW コネクテッド・ドライブシステムのセキュリティ評価を委託しました。この評価の結果は最終的に 220 万台のリコールにつながりました。コネクテッド・ドライブシステムは、車両のドアロック解除や HVAC システムの管理を含む、セルラーネットワークを介して車両の遠隔管理が可能です。これは所有者のスマートフォンのモバイルアプリケーションを通じて行われます。

BMW システムは、適切な通信暗号化や不正改ざん防止が実装されていないなど、複数の基本的セキュリティ対策の欠如が発見されてしまったことによって、侵害可能であるという評価となりました。そのような事実認定を発見するために利用された方法論は、セルラーモデム用のファームウェアを抽出するために基礎となるコンポーネントを分解して、リバースエンジニアリングされることから始まりました。これによって、ソフトウェアが NGTP（次世代テレマティクスプロトコル）を使用して、同じハードウェア構成を持つすべての BMW 車両で同じ主要部品が使用されていたことを発見することにつながりました。さらに、コネクテッド・ドライブシステムでは、より旧式でより堅牢性の低い暗号化システムである DES（データ暗号化規格）が使用されていることも判明しました。

さらに、コネクテッド・ドライブがモバイルアプリケーションからリモートアンロック機能を有効にしたことが発見されました。これにより、ドライバーはドアを遠隔地からロック解除できるようになりました。この機能を有効にするには、所有者は BMW 管理サーバーにアカウントを作成し、リモートサービスを有効にする必要がありました。残念ながら、このリモートサービス機能は、遠隔の攻撃者が車両と BMW サーバー間の車両データ伝送を記録して監視することによって、そのような機能を遠隔から起動する脆弱性があることが判明しました。この攻撃は、通信チャネル上に SSL または TLS 暗号化が実装されておらず、すべての通信が HTTP 経由であったため、極めて単純な手法でした。

そのため、一般的に、同一のデバイス間で単一の暗号鍵を共有することは絶対にお勧めしません。また、このようなシステムの違反が最大限の被害につながり、侵害された場合の安全性とセキュリティへの影響をもたらすため、旧式の貧弱な暗号化も使用しないでください。さらに、サーバーから送信されたデータに暗号化、コード署名、または改ざん防止制御

がないため、攻撃者はデータを簡単に監視し、リモートサービスを有効にして変更し、それを正当なユーザーであると偽装して BMW サーバーに送り返すことができました。これが車両のロックを解除するための最初のステップでしたが、これが一度達成されると、車両のドアのロックを解除し、車両エコシステム全体の安全性とセキュリティを損なうという、正規のリクエストのリプレイを送信することは簡単なことでした。

概して、BMW がこの攻撃を防止できるいくつかの方法があります。車両とバックエンドサービス間の通信に SSL または TLS を使用すること、ランダムまたはローリングノンスまたはタイムスタンプ付き期限切れ署名の実装など、以前に送信されたコマンドのリプレイを防止するメカニズムを提供すること、エラーメッセージに個人情報（VIN）を送信しないこと、より強力な暗号化アルゴリズムを使用し、関連性のないすべての車両でプライベート暗号化キーを共有しないことなどです。

2.1.1.1. 関連フレームワークテスト項目

コンポーネントテクノロジー	フレームワークカテゴリー	セクション	テスト項目名
Wi-Fi	推奨	6.2.2.4	ソフトウェア（ソース）の特定
Wi-Fi	アドバンスド	6.2.3.1	チャンネルベースの MITM
Wi-Fi	アドバンスド	6.2.3.6	ネットワークプロトコルで送られるデータのファジング
Wi-Fi	アドバンスド	6.2.3.7	脆弱な設定の特定
Wi-Fi	アドバンスド	6.2.3.8	旧式の無線サービスの ID
Wi-Fi	アドバンスド	6.2.3.9	ソフトウェアの特定（ファームウェア）
Wi-Fi	アドバンスド	6.2.3.12	認証されていないネットワークアクセスのチェック
Wi-Fi	アドバンスド	6.2.3.13	承認されていないデータ
モバイル	アドバンスド	6.5.2.3	アプリケーション通信チャンネルのセキュリティテスト
Web サービス	必須	6.6.1.20	脆弱な X.509 証明書署名ハッシングアルゴリズム

Web サービス	必須	6.6.1.24	脆弱な SSL/TLS を使った暗号化スイート
Web サービス	必須	6.6.1.26	クライアントが開始する SSL/TLS 再ネゴシエーションを有効にする
Web サービス	推奨	6.6.2.1	エントロピーが小さいセッション ID

2.1.2. マツダ Get_Info 乗っ取り

2017 年、セキュリティテスターがコードダンプを発行し、USB デバイスを介して、マツダ車のインフォテイメントシステムのデータエクスフィルトレーション（攻撃者が標的システムの機密データを見つからないように持ち出す行為）と制御を可能にしました。このコードは、2014 年から 2017 年までマツダが使用していたインフォテインメントコンソールでの有名なエクスプロイトに基づいています。このエクスプロイトは、ファームウェアのアップデートと情報取得の仕組みにありました。偵察によって、ファームウェアアップデートメカニズムが、車両に接続されたドライブ上の特定ファイル名の存在をチェックしていたことが発見されました。このファイルが存在する場合、システムはあらかじめ保存された構成スクリプトで指定されたアクションの実行を開始します。エクスプロイトは、マツダのファイルシステムを改ざんしてサードパーティのアプリケーションをターゲットユニットにアップロードし、マツダのディスプレイをカスタマイズすることを可能にしました。さらに、USB によって読み込まれた構成ファイルを変更して、USB をメディアデバイスとしてマウントし、選択したファイルを USB にコピーする bash スクリプトをトリガーとすることで、ファイルシステムデータのデータ探索が可能であることが判明しました。デモンストレーションでは、この方法を使用してインフォテイメントシステムから「/etc/passwords」ファイルを抽出し、パスワードが回復したら Wi-Fi または直接接続によってシステムに直接アクセスすることができました。このような脆弱性は、通信デバイス上で実行されるソフトウェアの基本的なコードの健全性管理によって防止された可能性があります。

2.1.2.1. 関連フレームワークテスト項目

コンポーネントテクノロジー	フレームワークカテゴリー	セクション	テスト項目名
Wi-Fi	アドバンスド	6.2.3.9	ソフトウェアの特定（ファームウェア）
Wi-Fi	アドバンスド	6.2.3.6	ネットワークプロトコルで送られるデータのファジング
Wi-Fi	推奨	6.2.2.4	ソフトウェア（ソース）の特定
Wi-Fi	必須	6.2.1.5	セキュアなプロトコルの実装の評価
Web サービス	アドバンスド	6.6.3.7	認証バイパス

Wi-Fi	アドバンスド	6.2.3.13	承認されていないデータ

2.1.3. テスラ ModelS

2016 年、セキュリティ研究者は、車両が使用されて人間のユーザーが運転している最中にテスラ ModelS を遠隔ハッキングすることができることを実証しました。攻撃はテスラのドライバーを巧みに工作して悪意のある Web サイトに接続して、不正な Wi-Fi アクセスポイント（テスラゲストなど）に接続し、テスラのアップデートのふりをして不正なソフトウェアをインストールし、最終的にバックドアアクセスを車の一部の機能にインストールすることを実証しました。

このような脆弱性を発見するためのアプローチである技法には、研究者チームがテスラ S 独自の Web ブラウザに影響を与えた脆弱性を最初に発見することが含まれていました。ブラウザが、脆弱性が知られていたサードパーティ製のオープンソースフレームワーク（WebKit）をベースにしていたため、これにより、研究者チームは、研究者が設計した悪意のある Web サイトを訪問したテスラブラウザをターゲットにした、自動車車両に特化したエクスプロイトを設計することができました。その結果、ウェブサイトからダウンロードされたマルウェアでハッキングされたテスラは、バックグラウンドで常にブラウザを自動的に実行するようになり、ドライバーの介入なしに研究者チームとターゲット車両との間の継続的な遠隔アクセスを可能にしました。

また、エクスプロイトがテスラのインフォテイメントシステムに存在する特権の低いアカウントへのアクセスを可能にして、公開されているいくつかのセキュリティ上の欠陥がある古いバージョンの Linux がシステムで使用されていたことが判明しました。これらの欠陥はピボットポイントとして使用され、低特権アカウントのアクセス特権をインフォテイメントシステム上で root 権限で実行できるようにしました。

リモートルートシステムの特権を使用して、CAN バスメッセージングシステムに存在する重要な車両機能（ブレーキ、ステアリング、アクセルなど）と残りの車両の送信ラインとの間の車両のアーキテクチャフレームワークにテスラが試行で実装していたセキュリティゲートウェイに研究者が遭遇したのはこのケースでした。実装されたセキュリティゲートウェイは PowerPC RTOS（リアルタイムオペレーティングシステム）で、その SD ストレージシステムは OTA（無線）ファームウェアアップデートを利用していました。この OTA ファームウェアアップデートシステムは、通常同様の技術に対してテストされているいくつかの些細なエクスプロイトに対して脆弱であったため、その結果、研究者は悪意あるコードをインストールして OTA のセキュリティをリバースエンジニアリングしてハッキングすることができ、元の OTA ファームウェアアップデートメカニズムを完全に置き換えることができました。

カスタムファームウェアアップデート OTA を導入したことで、実装されたセキュリティゲートウェイは、インフォテイメントシステム上のルート権限アカウントへのリモートアクセスに対する対策として完全にハッキングされ、役に立ちま

せんでした。研究者チームはユーザー制御のインフォテインメントトラストゾーンから重要な CAN バスにアクセスできるようになりました。チームは、正確に細工された CAN メッセージを送信することで、ブレーキ、加速ドア、窓、およびライトを簡単に制御できることを実証しました。さらに、ECU は誤った情報を読み取ってユーザーに反映させることがあります。そのような危険な方法には、120km/h ではなく 60km/h と速度を表示することが含まれます。

自動車におけるセキュリティ制御の欠如は、制御システムの一部にアクセスする攻撃者が極端に少ない可能性が想定されるため、車両サブシステムが保護を必要としないという共通の仮定に起因することがよくあります。そのような仮定は、一般的に見落とされた事実のために、誤ってしまうことがあります。なぜなら、最終的に車両全体のテールコントロールを行うためには、制御された環境に 1 つの特異な侵入工作を取るしかありません。

このエクスプロイトが明らかになった後、テスラは責任あるセキュリティ対策を講じて、そのような重大な侵入工作を修正するために、以下のようないくつかの基本的なセキュリティコントロールを適切に実装することで解決できることを証明しました。旧式の Linux OS をアップデートし、レガシーWeb ブラウザコンポーネントをアップデートします。

2.1.3.1. 関連フレームワークテスト項目

コンポーネントテクノロジー	フレームワークカテゴリー	セクション	テスト項目名
Wi-Fi	必須	6.2.1.2	暗号化されていない通信およびデータコンテンツ
Wi-Fi	必須	6.2.1.5	セキュアなプロトコルの実装の評価
Wi-Fi	アドバンスド	6.2.3.1	チャンネルベースの MITM
Wi-Fi	アドバンスド	6.2.3.8	旧式の無線サービスの ID
Wi-Fi	アドバンスド	6.2.3.9	ソフトウェアの特定（ファームウェア）
Wi-Fi	アドバンスド	6.2.3.12	認証されていないネットワークアクセスのチェック
Wi-Fi	アドバンスド	6.2.3.13	承認されていないデータ
モバイル	必須	6.5.1.2	コンパイラの設定チェック - 開発
モバイル	必須	6.5.1.3	コンパイラの設定チェック - プロダクション
モバイル	必須	6.5.1.4	アプリエンタイトルメント/権限チェック
モバイル	必須	6.5.1.5	ハードコードされた機密情報
モバイル	必須	6.5.1.12	証明書の検証

モバイル	必須	6.5.1.13	証明書のピンニング
モバイル	必須	6.5.1.14	バイナリ難読化 - 展開
モバイル	推奨	6.5.2.2	暗号化チェック
モバイル	推奨	6.5.2.3	アプリケーション通信チャンネルのセキュリティテスト
モバイル	アドバンスド	6.5.3.7	バイナリ難読化 -
Web サービス	必須	6.6.1.1	認証スキームの存在を検証
Web サービス	必須	6.6.1.8	HTTPS の有効化/強制化
Web サービス	必須	6.6.1.20	脆弱な X.509 証明書署名ハッシングアルゴリズム
Web サービス	必須	6.6.1.24	脆弱な SSL/TLS を使った暗号化スイート
Web サービス	必須	6.6.1.25	SSL/TLS インセキュア認識オン
Web サービス	必須	6.6.1.26	クライアントが開始する SSL/TLS 再ネゴシエーションを有効にする
Web サービス	アドバンスド	6.6.3.7	認証バイパス

2.1.4. ジープの「UConnect」

2015 年に FCA は 140 万台の車両をリコールし、ジープ UConnect システムに対して攻撃者が重要な車両機能にリモートアクセスすることにより、ユーザーの安全性と車両のセキュリティをハッキングできるようにするセキュリティエクスプロイトを修正しました。

2015 年のジープチェロキーには車内 Wi-Fi のオプションがありました。このホットスポットは、ウェブ上または UConnect システムを通じてサービスを支払った後にのみアクセス可能なホットスポットです。この機能に脆弱性が発見され、システムに脆弱性があることが証明されました。UConnect プロトコルに対して偵察を行うことで、システムが無線ネットワークおよびセルラーLTE のポート 6667 で DBUS サービスを公開していることが発見され、それを利用することでこの脆弱性は発見されました。これは単純な車輌へのポートスキャンによって簡単に発見され、短距離通信と長距離通信の両方から容易にアクセスできました。

研究とリバースエンジニアリングにより、DBUS サービスがコマンドインジェクションに対して脆弱であることが発見されました。つまり、認証されていないシステムコマンドをリモートでサービスに送信し、デバイス上ですぐに実行されてしまいます。これにより、攻撃者はブートプロセスおよびファイルシステム上のさまざまな保護された場所にあらゆるセキュリティシステムによって妨げられない形で書き込むことができ、最終的には車両の変更されていないユニットへの

ルート特権アクセスを取得することで、元の車両サブシステムのファームウェアは、インフォテイメントユニットからクリティカル CAN バスへの直接アクセスを可能にするように変更されてしまいます。

リモートによるルート権限でのシステムアクセスが一度得られたら、HVAC 設定、無線設定や値、表示設定の変更、マニュアル制御の無効化がすべて完全にアクセス可能になり、車両サブシステム全体すなわちジープと乗客の安全性とセキュリティが完全にハッキングされます。

非常に基本的なセキュリティ制御を実装することにより、この攻撃を簡単に回避することができました。そのような制御には次のものがあります。正当性と妥当性についてすべての着信メッセージをチェックするコード署名。DBUS サービスに対する UConnect 認証と、保護されたシステムファイルとユーザーレベル制御ファイルへの基本的なファイルアクセスの分離。

2.1.4.1. 関連フレームワークテスト項目

コンポーネントテクノロジー	フレームワークカテゴリー	セクション	テスト項目名
Wi-Fi	必須	6.2.1.1	ワイヤレス通信のデフォルトの特定
Wi-Fi	推奨	6.2.2.4	ソフトウェア（ソース）の特定
Wi-Fi	アドバンスド	6.2.3.2	実装されたウェブサービスのファジング
Wi-Fi	アドバンスド	6.2.3.9	ソフトウェアの特定（ファームウェア）
Wi-Fi	アドバンスド	6.2.3.11	WIDS/WIPS 検出
Wi-Fi	アドバンスド	6.2.3.12	認証されていないネットワークアクセスのチェック
モバイル	必須	6.5.1.5	ハードコードされた機密情報
Web サービス	必須	6.6.1.8	HTTPS の有効化/強制化
Web サービス	必須	6.6.1.14	永続的 Cookie に機密情報が含まれる
Web サービス	推奨	6.6.2.1	エントロピーが小さいセッション ID

2.1.5. 三菱アウトランダーワイヤレス LAN

2016 年、セキュリティ研究者は、ラップトップから盗難防止アラームを無効にできることを含むいくつかの脆弱性を、三菱アウトランダーハイブリッド SUV に発見しました。

三菱アウトランダープラグインハイブリッドには、この攻撃の対象となった車両の高度な機能の一部を制御するために、モバイルアプリで車両に接続するオプションがあります。セルラーネットワーク上で動作するほとんどの自動車プラットフォームとは異なり、アウトランダーは車載 Wi-Fi ホットスポットに直接接続するだけで動作します。これは、指定された狭い範囲内のモバイルデバイスのみが車両に接続できるというセキュリティ実装であることを意味していましたが、三菱は一般的な基本セキュリティ制御対策を行わずにこの機能を実装していたため、長距離からの攻撃を削減するという意図を無効にし、結果としてこの脆弱性の発見につながりました。

基本的な偵察によって、重要な機能へのアクセスを備えた車両通信ネットワークへの共有キーがオーナーズマニュアルに書かれていることが判明しました。これは、ネットワークにアクセスできるユーザーすべてがマニュアルを参照可能という意味で大きな脆弱性です。さらに、認証キーが短すぎて予測可能であることが判明したため、そのようなキーを解読するための基本的なハードウェアを持つ攻撃者が短時間で解読することは当たり前のことでした。

さらに厳密に調査すると、モバイルデバイスと車両との間のハンドシェイクが捕捉され、修正され、攻撃者が盗難警報をオフにするなどの行動を実行するように車両に命令するメッセージをデコード、修正、および再生することが可能になることが発見されました。これは、モバイルデバイスとアクセスポイント（AP）接続が干渉され、モバイルアプリケーションがコントロールされた時間に AP に再接続するように強制する「認証解除」と呼ばれる基本的な技術によって実現されていました。

これらの脅威ベクトルは、強力な事前共有キーの実装、機密性の高い認証データの適切な保管と基本暗号化、通信回線上のローリングノンスのような基本的なセキュリティ対策によって容易に修復できます。

2.1.5.1. 関連フレームワークテスト項目

コンポーネントテクノロジー	フレームワークカテゴリー	セクション	テスト項目名
Wi-Fi	必須	6.2.1.1	ワイヤレス通信のデフォルトの特定
Wi-Fi	必須	6.2.1.3	盗聴（スニッフィング）
Wi-Fi	必須	6.2.1.6	露呈されているネットワークおよびサービスの発見
Wi-Fi	推奨	6.2.2.1	暗号化ダウングレード攻撃
Wi-Fi	推奨	6.2.2.2	グループ暗号キーの予測可能性の決定
Wi-Fi	アドバンスド	6.2.3.2	実装されたウェブサービスのファジング

Wi-Fi	アドバンスド	6.2.3.6	ネットワークプロトコルで送られるデータのファジング
モバイル	必須	6.5.1.10	機密データ
モバイル	必須	6.5.1.15	情報漏洩
Web サービス	必須	6.6.1.1	認証スキームの存在を検証
Web サービス	必須	6.6.1.8	HTTPS の有効化/強制化

2.1.6. アウディ TT エアバッグ

2015 年、研究者はサードパーティのソフトウェアに含まれるゼロデイ脆弱性を利用して、アウディ TT（および他のさまざまなモデル）やその他の機能でエアバッグを無効にする方法を実証しました。多くの自動車のようにアウディ TT には診断機能が備わっており、メカニックが車両に接続して ECU の問題を診断し解決することができます。この攻撃では、テスターはサードパーティの診断ツールを脅威ベクトルとして使用して車両サブシステムをハッキングしました。テスターが使用した方式は、診断システムが使用するプロトコルをリバースエンジニアリングすることでした。侵入テストと偵察の両方を使用して、攻撃者は、診断ツールを制御するターゲット PC を感染させるための特殊なマルウェアを準備しました。このマルウェアは悪意あるソフトウェアであり、診断において車両通信を行う DLL を置き換えました。これにより、診断ツールが車に接続されてメカニックが使用したとき、MITM 攻撃が可能となりました。このスタクスネット形式の攻撃（事前認証された/信用できる車両サブシステムと通信する、ハッキングされてはいるが正当な第三者のツールからの攻撃ベクトルのため）の間、攻撃者がこのツールを使用することで、保護された CAN バスシステムに対して悪意あるペイロードを含む形に修正されたパケットを送信し、エアバッグを強制的に膨張させて、最終的に車両の安全性とセキュリティがハッキングするという興味深い事例です。

いくつかのセキュリティ手順を実装することで、車両の保護された制御システムにアクセスするサードパーティコンポーネントを取り扱う際に実装されると予想されるこの攻撃を防ぐことが可能です。車両から接続ポイントまでの正当性チェック（ハッシュチェック）、保護されたファイルシステムアクセスの必要性および重要な機能のメンテナンスアクセスによるユーザー制御機能への内部分離の評価などがこの例にあたります。

2.1.6.1. 関連フレームワークテスト項目

コンポーネントテクノロジー	フレームワークカテゴリー	セクション	テスト項目名
Wi-Fi	アドバンスド	6.2.3.9	ソフトウェアの特定（ファームウェア）
Wi-Fi	アドバンスド	6.2.3.6	ネットワークプロトコルで送られるデータのファジング

Wi-Fi	推奨	6.2.2.4	ソフトウェア（ソース）の特定
Wi-Fi	必須	6.2.1.5	セキュアなプロトコルの実装の評価
モバイル	推奨	6.5.2.2	暗号化チェック
Web サービス	アドバンスド	6.6.3.7	認証バイパス

2.2. 現在の自動車セキュリティの状態

通信経路および ECU の増加によって、複雑なタスクとスケジューリングを必要とする車輌が持つリスクは、自動車業界全体に対するこのようなエクスプロイトにより認識されることになりました。これらの処理ユニットおよび通信経路は、バックエンドシステムおよび将来の V2x 通信に有用なデータを提供する常時接続を可能にし、乗客および歩行者の安全性だけでなく、道路渋滞を軽減することを目的としていますが、セキュリティは車両の安全性に直接関係するため、セキュリティは安全性と同等の優先度に上昇していることが分かります。

特に、インターネットベースのハッキングの試みが一般化した際に、セキュリティ対策を実施していた他の業界に追いつくためのさまざまな対策を行わなければならない状況にも関わらず、重要な安全システムに意図した（またはそれなりの）リモートアクセスを追加するために、近代的な車両には短距離および長距離 RF 技術が導入されたことにより、セキュリティの欠陥はますます憂慮されつつあります。その中でこのフレームワークは、そのような欠陥をテストして、そのようなエクスプロイトが最初に起こることを防ぐセキュリティフレームワークを自動車産業が持つことを支援するために、セクション 1.4 で参照されている規格と連携することを目的としています。したがって、セキュア NEDO BSM モデルで実証されているように、自動車セキュリティをより実用的なレベルに打ち出す必要があります。自動車のインタラクティブ性を高めることは、自動車の内部に存在するいくつかの潜在的な攻撃経路をさらすことになりますが、このフレームワークのようなセキュリティ文書は、現代の走行車両に関連する様々な無線デバイスの安全を確保するために必要なプロセスと手順を説明し、これらの攻撃ベクトルの懸念に対応します。

3. フレームワーク方法論

このセクションでは、このフレームワークで公開されているテスト項目が、自動車エコシステムにおける一般的なサイバーセキュリティテストのどの段階で実施され、脆弱性、エクスプロイト、関連するインスタンスを発見するために必要な方法論を詳述することを目的としています。以下の図は、自動車製品ライフサイクル（SDLC）と、方法論とフレームワークがシステムライフサイクルの各段階にどのように適用されるかを表しています。

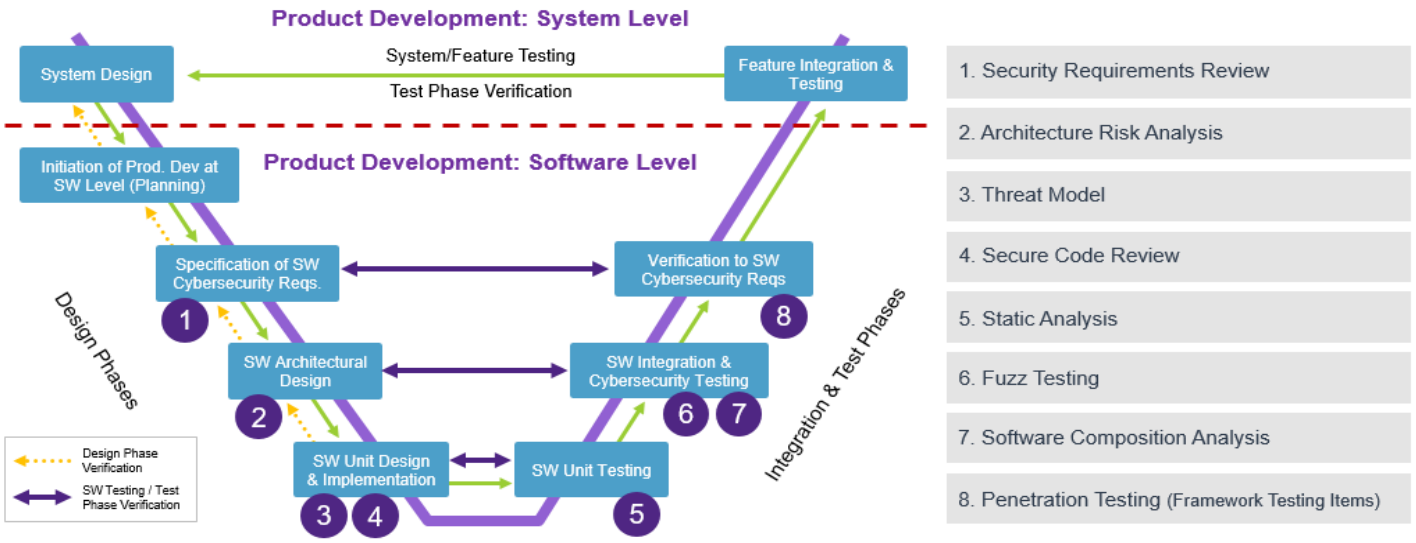


図 1：セキュリティステップを組み込んだ製品開発ライフサイクル

3.1. 偵察

3.1.1. 説明

偵察は攻撃における情報収集段階です。ターゲットのセキュリティ状態を理解するだけでなく、ターゲットに関する多くの情報を捜索することもあります。偵察は SDLC のどの段階でも実行されますが、車両の安全に関する問題が表面化すると直ちに捕捉できるシステム設計または要件レビューが最も効果的です。

3.1.2. アプローチ

このようなタスクに頻繁にアプローチするには、システムの機能をより深く理解するために、提供された成果物を読み、レビューすることが重要です。これらの成果物には、アーキテクチャ説明、ソフトウェア設計文書、API 仕様、およびエンドユーザー文書が含まれますが、これらに限定されません。このフェーズは、システムに精通したエンジニアとの会話を含む場合があります。この短期間であるが重要な分析は、システム内の高リスクエリアを特定し、開示されたテストの

方法論に含まれる将来のすべての活動の基礎を形成することになります。運用プロセス（関連する場合）とすべてのシステム入力（ネットワーク、IPC、ファイルシステムなど）の分析、およびいくつかのリバースエンジニアリングがこの段階で実行されることに注意してください。

3.1.3. ツール

使用される主なツールは検索エンジンで、特にターゲットに大きな操作基盤がある場合、可能な限り多くの情報を自由に見つけるために使用します。いくつかの追加のネットワーク接続ツールは、次のものを含む関連するさまざまなワイヤレスインターフェイスを検出するのに役立ちます。最も基本的なものであるワイヤレススキャンツール、これはそのエリアの利用可能なネットワークに接続するスマートフォンのもう少し堅牢なバージョンです。

3.2. 脅威モデリング

3.2.1. 説明

脅威モデリング（侵入テスト計画またはアーキテクチャリスク分析とも呼ばれます）には、個々の攻撃努力を作成および実行する前にテスト計画を作成することが含まれます。説明するアプローチには、ビジネスリスク、資産、攻撃者、潜在的な攻撃ベクトルを特定し、優先順位を付ける侵入テスト計画を作成することが含まれます。信頼ゾーン、潜在的な脅威、保護される資産、およびサブシステムに適用されている現在の防御を分類します。

3.2.2. アプローチ

脅威モデリングに対するさまざまなアプローチを記述するために特別に書かれたいくつかのリソースが見つかります。しかしながら、基本的にすべてのアプローチでには範囲内および範囲外のターゲットシステムの概要、発見を視覚化するための図、信頼ゾーン、セキュリティ制御、保護する資産、および潜在的な脅威エージェント（およびその後の脅威ベクトル）の強調表示を作成することになります。作成された資料は、多くの聴衆が脆弱なコンポーネントの確定し、その脆弱な通信経路の発見を容易にします。

3.2.3. ツール

脅威モデリングの結果には、通常、相当量の情報が含まれています。この情報は車両の全体的な安全保障状態を包含し、そのために明確に規定された手順を、結果出力が適切な関係者と共有されるように提供しなければなりません。したがって、組織は NIST 800-30 脅威マトリックスなどのフレームワークを利用して、どのように結果を扱うべきか、どの程度まで扱うべきかを導くことができます。クリティカルインパクトおよびクリティカル可能性項目は、生産を即時停止して Auto-ISAC などの外部団体に通知する必要があります。

		影響レベル				
		非常に低い	低い	中間	高い	非常に高い
可能性	非常に高い	非常に低い	低い	中間	高い	非常に高い
	高い	非常に低い	低い	中間	高い	非常に高い
	中間	非常に低い	低い	中間	中間	高い
	低い	非常に低い	低い	低い	低い	中間
	非常に低い	非常に低い	非常に低い	非常に低い	低い	低い

表 1：NIST 800-30 脆弱性マトリクス

マトリクスの各辺は、脅威のモデリング中に見つかった問題の可能性と影響のレベルに影響する一連のパラメータによって計算されます。NIST の詳細については、 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf のオンライン脅威計算ツールを参照してください。そのような脅威モデリング方法論を実行する組織ごとに個別にプロセスを作成して、要件チーム、開発、購買、セキュリティ組織などの主要なステークホルダーにフィードバックを提供して、結果の影響を最小限に抑えることが一般的に推奨されます。

3.3. ファジング

3.3.1. 説明

ファジングは、ソフトウェアの未知の脆弱性を突き止めるための業界標準技術です。それはシスコシステムズやマイクロソフトなどの組織を含む多くの現代のセキュアソフトウェア開発ライフサイクル（SSDLC）の必須部分です。ファジングは、ネットワークプロトコルファジングとファイルフォーマットファジングがこの方法論でカバーされる主要な分野であり、それぞれのファジング分野では、実行、注入モード、および故障モードにわずかなばらつきがある複数の分野に大別することができます。しかし、基本的な原則は、ターゲットシステムによる入力のクラッシュまたは処理によって脆弱性を明らかにするために、悪意ある入力をターゲットソフトウェアに配信するという点で同じです。

3.3.2. アプローチ

具体的には、ファジングの目的は脆弱性を突き止めることです。失敗しなければ、製品はファズテストに合格します。ファジングは無限の空間問題であるため、製品のリリース準備が整ったとみなされる前に*どれだけ*のファジングが行われなければならないかを決定することが課題です。製品のセキュリティは、その最弱リンクほどしか強くありません。ファ

ジングに関しては、すべての攻撃ベクトルが等しくファズ化されなければならないことを意味します。ファジングを計画する最初のステップは、ターゲットソフトウェアのアタックサーフェスをマッピングすることです。アタックサーフェスは、ターゲットソフトウェアが入力を取り込むすべての場所のリストになります。そのようなテストの実行者による決定を支援する努力の中でさらに詳細に記載されているファズテスト成熟モデルが公開されています。

それにもかかわらず、ファジングは*ネガティブテスト*の領域に陥ります。ほとんどのソフトウェアテストはポジティブテストであり、有効な入力がソフトウェアに提供されます。ソフトウェアが正しい出力を生成する場合、テストは合格になります。これらは、機能テストまたは適合テストとも呼ばれます。ファジングは、予期しないまたは不正な形式の入力があった場合にターゲットソフトウェアが失敗しないことを保証することを目的としているため、他のタイプのテストに対して補完的となります。

- ポジティブテストは、ターゲットソフトウェアが正しく動作するかどうかを評価します。
- ネガティブテストは、ターゲットソフトウェアが失敗しないかどうかを評価します。

ファジングは、グレーまたはホワイトボックス技法として実行されるのが望ましいですが、テスターがターゲットソフトウェアについては何も知らないブラックボックス技法としても利用できます。ただし、ターゲット内部の知識があれば、障害検出が向上します。

3.3.3. ツール

ファジングの結果は、ターゲットソフトウェアの場合のように無限空間問題であり、悪く形成された入力（テストケース）が無限に生成される可能性があります。優れたファジング実行者は、ターゲットソフトウェアで最も障害が発生する可能性が高いテストケースを作成する方法を理解しています。プレフォームファジングに関して考慮すべき追加のポイントは次のとおりです。

- ランダムなファジングはめったに効果がありません。テストケースは実際のプロトコルメッセージのようには見えません。ターゲットソフトウェアはほとんどのテストケースを完全に無視します。
- 突然変異ファジングは、有効なメッセージに異常を導入してテストケースを作成します。これは、いくつかのシナリオで有効です。ただし、セッション番号、シーケンス番号、長さフィールド、チェックサムフィールドなどの標準プロトコル機能は処理されません。
- 世代ファジングは、テストするプロトコルまたはファイル形式の基本的な理解に基づいています。これは、可能なすべての構造とメッセージの種類、すべてのメッセージのすべてのフィールド、メッセージ交換に関するルールを認識していることを意味します。世代ファジングではすべてのルールを知っているので、すべてのルールを体系的に破ることができます。世代ファジングは、ターゲットに正当に見える高品質のテスト材料を作成します。複数メッセージの交換が行われるプロトコルでは、世代ファジン

グは、ターゲットと複数の有効なメッセージを交換し、それを特定の状態にした上で異常なテストケースを配信することができます。

作成者が意図したり予期していなかったように動作すると、ソフトウェアは失敗します。伝統的に適用されているファジングでは、故障モードは 4 つのカテゴリに分類されます。

- クラッシュ
- 無限ループ
- リソースのリークまたは不足
- 予期しない動作

これらの障害モードは、テスト対象のシステムまたはソフトウェアの種類、基盤となるオペレーティングシステムなどによって異なります。クラッシュは単なるクラッシュであるか、または、ターゲットのサービス拒否、パフォーマンスの低下、情報漏えい、セキュリティ破壊の招来などにつながる可能性があります。その結果は、ソフトウェアの目的と機能、アプリケーションがいつどこで実施されるかによって異なり、ファジング性能は要求されるテスト時間が短い単純なものか、より長い時間を必要とする非常に複雑なタスクであるか、が変わってきます。

3.4. ソフトウェアコンポジション解析（SCA）

3.4.1. 概要

ソフトウェアは、物理的製品が部品から組み立てられるのとほぼ同じ方法でコンポーネントから組み立てられます。ソフトウェアエコシステムでは、ビルダー（または開発者）がソフトウェア製品を作成し、バイヤー（または消費者）がそれらを使用します。製品がモバイルアプリケーション、ECU、インフォテイメントシステム、テレマティクスユニットのいずれであっても、ビルダーは複数のコンポーネントを組み立ててソフトウェアを作成します。

自社製コンポーネントは、ビルダー組織によって直接開発されます。通常、このコードはサードパーティ製コンポーネントを組み合わせて、ソフトウェア固有の追加機能を提供します。
サードパーティ製コンポーネントは、ソフトウェア製品チームの外部で作成されます。それらの多くはオープンソースのコンポーネントですが、業務用であったりまたはビルダー組織とは別の部分で開発されていることもあります。たとえば、ソフトウェア製品チームはネットワーク通信を保護するために OpenSSL を使用します。彼らはバイナリのみのコンポーネントとして提供される、購入済みの商用ネットワーク通信スタックを使用することができます。また、データの暗号化と復号化のために、同じ組織内の別のチームによって維持管理されている内部開発されたコンポーネントを使用することもあります。

完成したソフトウェアは、サードパーティのコンポーネントと自社製コードの組み合わせとなります。正確な比率はプロジェクトや業界によって異なりますが、すべての業界のほぼすべてのソフトウェアがこのように組み立てられています。このようなサードパーティのコンポーネントの統合は、従来の製造におけるサプライチェーンのすべての課題が内在し、悪意のあるソフトウェアや脆弱なオープンソースソフトウェアを導入するリスクを含むソフトウェアサプライチェーンとなります。ソフトウェアコンポジション解析（SCA）ソリューションを使用してソフトウェアサプライチェーンを管理することで、リスクを最小限に抑えることができます。

3.4.2. アプローチ

製品受入要件を定義することは、SCA の結果を解釈する上で重要です。最低限の確認として、製品に含まれるコンポーネントに既知の脆弱性がないことを確認します。より実践的なポリシーは以下のことを考慮します。

- 製品に古いコンポーネントが含まれていますか？すべてのコンポーネントを最新にする必要がありますか？古いバージョンのコンポーネントでは最大エージタイムを適用する必要がありますか？
- 既知の脆弱性を持つコンポーネントは許可されていますか？個々の脆弱性が製品に適用されない場合は、検査して効果を減じることができますか？
- コンポーネントライセンスには制限がありますか？ビルダーは、製品のライセンスと互換性のあるライセンスのみが使用されるようにする必要があります。

3.4.3. ツール

ソース解析に基づく SCA ソリューションは、製品のソースコードを参照し、既知のサードパーティのオープンソースプロジェクトのデータベースと比較し、製品、ライセンス、および関連する既知の脆弱性で使用されるソフトウェアコンポーネントの一覧を作成します。SCA ソリューションは、ソフトウェアインベントリを把握し、新しいコンポーネントの製品を含む管理方法を構築することもできます。SCA ソリューションは、２つの方法があり１つはソース解析、もう一つはバイナリ解析です。ソース解析 SCA ソリューションは、ソフトウェアサプライチェーンを管理しなければならないビルダー組織に最適です。対照的に、バイナリ解析 SCA ソリューションは、ソフトウェアの実行可能ファイルを直接分析します。ソースコードは必要ありません。これはソフトウェアを分析する強力なツールになります。

3.5. 侵入テスト

3.5.1. 説明

侵入テストは、潜在的な脆弱性に関してシステムを分析する手法です。タスクを実行するには、自動テストとマニュアルの 2 つの方法があります。自動テストでは、スキャナーを使用してテストを効率的に実行します。スキャナーは、ブルートフォース等によって脆弱性を探すのに有効です。対照的に、マニュアルによる侵入テストは、自動化プロセスでは解析できない領域のテストに向いています。ビジネスロジックとデータのやりとりのシナリオを解析したり、特定の仮説をテストするために、コーパスを視覚的にレビューしたり、データを処理するためのカスタムスクリプトやアプリケーションを開発することによって分析されるデータを低レベルのツールを使用して取得することが含まれます。

3.5.2. アプローチ

チェックツールは、攻撃を効率化したり、複数のターゲットを検査するために使用されます。脆弱性スキャナー、ファジングツール、データキャプチャアプリケーションは、攻撃の効率化に役立つツールにはいくつかの種類があります。

攻撃者は、脆弱性チェックツールの結果を使用して、その他手動によるの侵入を試みます。侵入テストは、知識とスキルが要求され、侵入可能なデータが得られない可能性があるため、攻撃の中で難しいものです。ここでは、ターゲットシステムや懸念される攻撃に大きく依存し、メモリダンプの実行、特権の昇格を許可する可能性のある IPC チャネルのテスト、ファジングファンクションの入力、詳細なリバースエンジニアリングなどのアクティビティが含まれます。

3.5.3. ツール

セキュリティテスターには、多くの侵入テストツールがあり、次の 3 つに分類されます。

脆弱性スキャナーは、ターゲットシステムの弱点を特定するために、シグニチャーベースによりターゲットの脆弱性を検出します。これらは、Web ベースアプリケーション（IBM Web Inspect）ネットワークホスト（Qualys）およびデータベースサーバー（SQLMap）があます。
ファジングツールは、悪意あるデータを入力としてアプリケーションへの送信を自動化します。ツールは、さまざまな選択基準でデータを並べ替えながら、毎秒 1000 回送信できます。これは、ターゲットシステム内の新らたな脆弱性を見つける方法の 1 つです。低レベルプロトコル用 Defensics など、システムの特定の側面に焦点を当てたツールがあります。
Wireshark や BurpSuite/Fiddler のようなデータキャプチャツールは、後で分析または再生するために、攻撃のセッションの通常のトランザクションデータを捕捉できます。これらのツールは、トラフィックデータとネットワークノード間の通信を理解するために不可欠です。

4. 用語の定義

このセクションには、ガイドラインで使用されている用語と、定義されていない技術用語および使用中の略語を解説します。

4.1. 攻撃者モデル

本書で概説している攻撃の種類は、「実世界」技術とアプローチのモデリングに基づきます。さらに、攻撃者は、オートメーションツールやプロキシツール、カスタムファジング、プロトコル傍受アプリケーションなど、さまざまなソフトウェアを使用しています。適用できる場合は、これらについて詳しく説明します。

現代の攻撃者は、主に攻撃面を特定し、成功への最適な経路を可能にする計画を策定するために、偵察から始めます。「攻撃モデル」または「攻撃計画」を開発することには、アプローチを導くために使用される攻撃ツリーを開発するためのターゲットとアプローチの分析が含まれます。

偵察の側面は、OSINT（オープンソースインテリジェンス）を含む多くの形態の情報収集を頻繁に使用します。これは通常、公的または容易に利用可能なリソースを用いた研究です。自動車の場合、サービスマニュアル、配線図、インターネットフォーラム、特許、さらにはメーカーの Web サイトや以前のハードウェアモデルがあります。

ほとんどの場合、攻撃者はさまざまなツールを使用して各種ハードウェアコンポーネントからファームウェアを抽出し、それをシステム情報を収集するための出発点として使用します。これに続いて、ネットワークトラフィックを観察し、サーバーへの接続と収集される可能性のあるデータの送信を探します。

4.2. 資産とセキュリティ目的

本書で関心のある資産の種類には、PII（個人識別情報）データ、および車両に関する技術データまたは設定データが含まれます。いくつかの例として、システムパスワード、電話帳連絡先データベース、所有者と車両識別情報、詳細なナビゲーション履歴、電話通話記録とテキストメッセージ（SMS）データがあります。

主なセキュリティ目的は、将来のハッキングを可能にするインフォテイメントユニットに関する技術情報を抽出することです。この目的には、接続番号やテレマティクスサーバー情報などのデータの収集があります。内部クレデンシャルと暗号化キーは、非常に貴重なターゲット/資産です。

最後に、ワイヤレスインターフェイスやインフォテイメントシステムを乗り超えて攻撃を拡大する能力は、本書の重要な特徴です。この攻撃には、コントローラネットワークに接続して有害な影響を与える方法で車両の機能にアクセスする能

力が必要です。潜在的な悪意のある行為のために、インフォテイメントユニット自体のアプリケーションを攻撃することも含まれます。

許可されたユーザーがインフォテイメントシステムを使用することを妨げる、システムへの接続の促進が適切な目的である場合もあります。

4.3. 略語

以下の表は、この文書全体で使用されている頭字語と用語を示しています。セキュリティに関して自動車分野でよく使用されているものとそうでないものが含まれます。これらの表の目的は、このフレームワークの全体的な理解度を高めるために技術用語の理解を深めることにあります。

略語	詳細語	説明
MITM	Man in the Middle	MITM は、攻撃者が秘密裏に中継し、おそらくは互いが直接通信していると信じている 2 人の間の通信を変更する攻撃です。
V2X	Vehicle to Everything（車両からあらゆるものへ）	V2X は、車両からその車両に影響を与える可能性のあるエンティティへのすべての情報の通信プロトコルであり、その逆もあります。
BT/BTLE	Bluetooth/Bluetooth low energy（Bluetooth/低エネルギーBluetooth）	Bluetooth は、携帯電話、コンピュータ、およびその他の電子デバイスの近距離無線接続規格です。
WLAN	Wireless Local Area Network（ワイヤレスローカルエリアネットワーク）	WLAN は、限定されたエリア内のコンピュータを相互接続するコンピュータワイヤレスネットワークです。
OEM	Original Equipment Manufacturer（相手先商標製造会社）	OEM は、別のメーカーによって販売される可能性のある部品およびデバイスを生産する会社です。
QA	Quality Assurance（品質保証）	QA は、製造された製品の間違いや欠陥を防止し、顧客にソリューションやサービスを提供する際の問題を回避する方法です。
DOS	Denial of Service	DoS とは、提供するサービスを妨害したり、停止させるものを指します。
DDOS	Distributed Denial of Service	DoS 攻撃は単体では行われなくなってきました。DoS に代わって行われ、強力な威力を持っている手法が DDoS です。

表 2：本書で使用する略語

用語	フルスペル	定義
SAE	Society of Automotive Engineers（米国自動車技術者協会）	SAE は、米国に拠点を置く世界的に活躍する専門家団体であり、さまざまな業界のエンジニア向けの標準化開発機構です。
USB	Universal Serial Bus（ユニバーサルシリアルバス）	USB は、コンピュータとデバイス間の接続、通信、および電源供給のためのケーブル、コネクタおよび通信プロトコルを定義する業界規格です。
OSS	Open Source Software（オープンソースソフトウェア）	OSS は、著作権者がソフトウェアの研究、変更、および配布を誰にでも、またいかなる目的でも提供するライセンスをソースコードとともに提供するコンピュータソフトウェアです。
GPL	Gnu General Public License（GNU 一般公有使用許諾）	GPL は広く使用されているフリーソフトウェアライセンスであり、エンドユーザーにソフトウェアの実行、調査、共有、変更の自由を保証します。

表 3：本書で使用されている頭字語を説明する頭字語表 2

5. セキュリティ評価フレームワーク

5.1. フレームワークの可視化

このセクションの目的は、本書で提案されるテストフレームワークの包括的な理解を助けるために開設します。車両エコシステムは、セクション 5.1.1 に引用されています。このセクションは、本書の扱う範囲が何であるか、この範囲で間接的に何が扱われているか、さらにフレームワークのテストカテゴリ毎の説明に分割されています。ここでは、車両全体のセイフティに関するセキュリティテストの直接的な効果が何であるかを説明します。

5.1.1. 車両全体のエコシステム

次の図は、「車両エコシステム」として定義されているシステムの全体図です。紫色にハイライトされている部分は直接的にテストされる項目であり、これはさらに、このフレームワークのサブカテゴリ（Wi-Fi、Bluetooth など）に区分されます。オレンジ色にハイライトされている部分は保護するアセットです。青くハイライトされている部分は、テスト結果として間接的に影響を受ける項目、またはテストに合格しなかった結果として直接的な影響を受ける項目です。

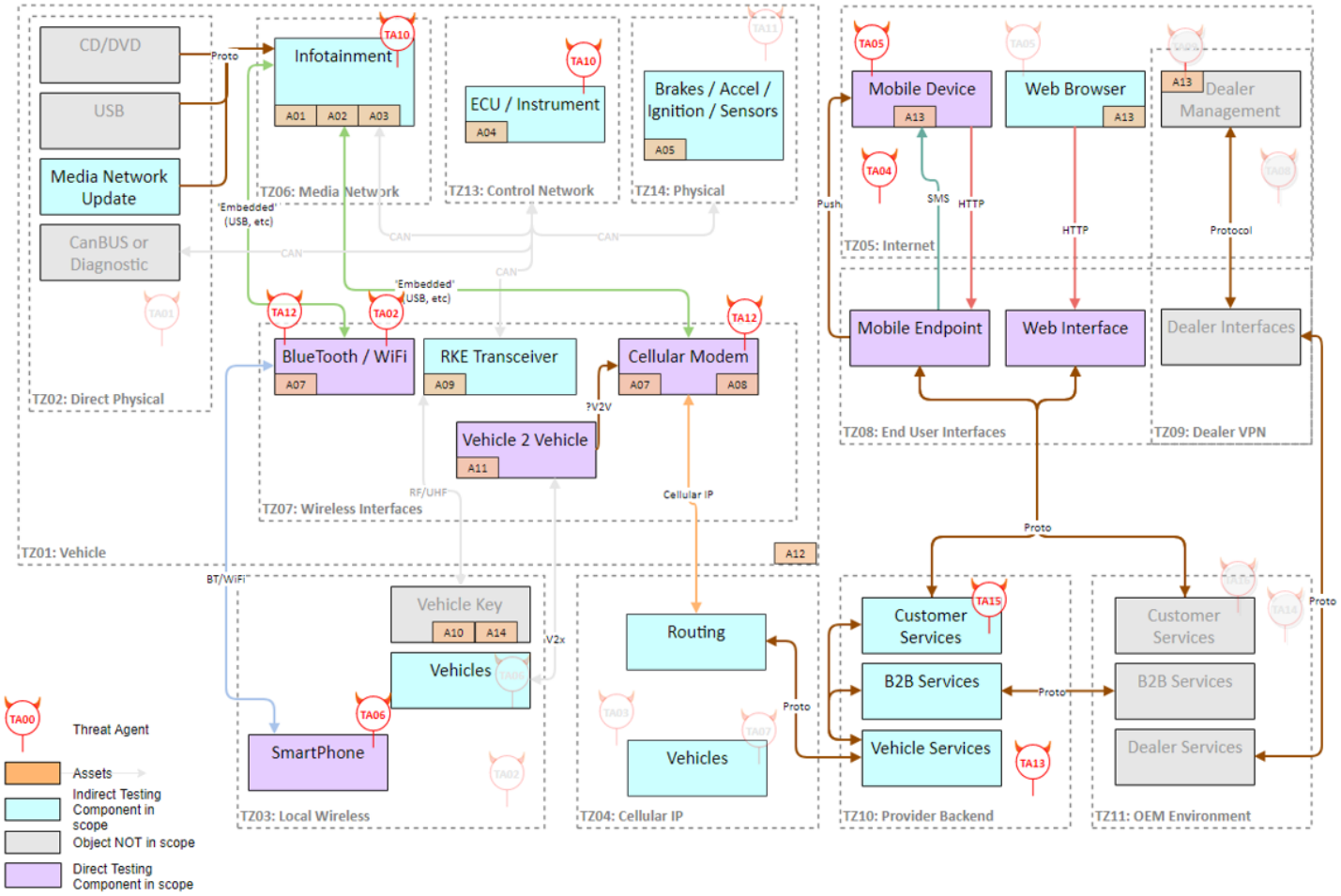


図 2：車両全体のエコシステム - システムの要素（サブコンポーネント）は、フレームワーク内で直接テストされることを示すため、および当該コンポーネントのテスト結果の間接的な影響を示すために、ハイライト

このフレームワークでは、対象とする影響テストが全車両のサブシステムに、したがって車両のセキュリティに及ぼす影響をハイライトするために、個々のテストカテゴリ内で、この図の個別のセクションが黄色にハイライトされています。

5.1.2. 対象となる車両エコシステム

分かりやすくするために、本書の範囲での車両エコシステムを可視化すると次の図になります。このテストフレームワーク内の各カテゴリは、この図の中では個別の項目です。車両エコシステムがフレームワークの中心であり、本書で焦点をあてるカテゴリです。

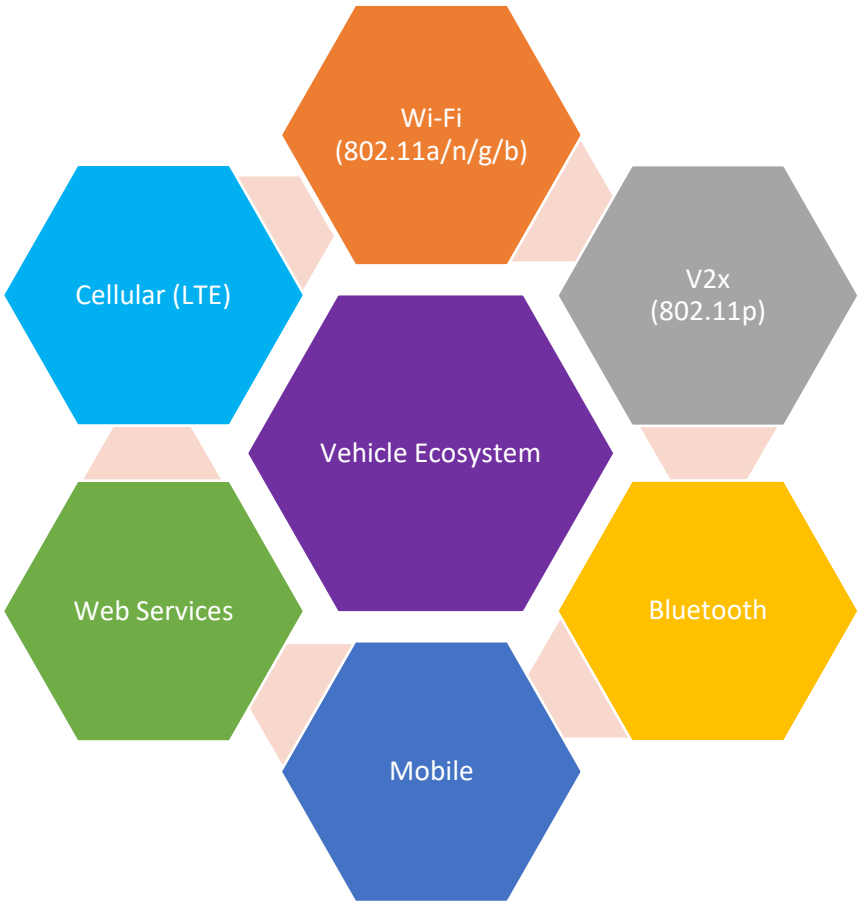


図 3：このテストフレームワークの範囲内の全車両エコシステム

この図の目的は、本書のユーザーに対象となるビューを提供し、前節では図で示されている車両全体のエコシステムと併せて、このイメージ図を使用して貰うことです。

5.2. テストケースの書式

5.2.1. テストケースの詳細

以下のセクションでは、フレームワークセキュリティテストのシナリオを詳しく調べます。このシナリオでは、テクノロジーを基準に配列されたテストケース毎にテスト合格基準が説明されています。このテスト合格基準は、各テクノロジーが紹介され、テストの全体サマリが強調され、さらにテスト項目の各々が示されています。テスト項目には、例示されるシナリオで必要となる具体的なテストケースが入っています。

この書式は、どのように構成されていたか、各セクションの中に何が含まれるべきか、フレームワーク全体の価値を高めるためにどのセクションが追加されたか、および各セクションが何を伝えようしているかまたは各セクションに何を含めようとしているかが、次の表で十分に説明されています。

名称	記述内容
フレームワークのセクション名	完了すべきテストの見出し番号および名称
項目番号	完了すべきテストに割り当てられる固有の ID 現在、これは **NEDO_分類コード_番号**で構成しています。
項目名	テスト項目の略称
目的	テストの目的および何をテストすべきかの簡単な説明
想定実施工数	テスト項目を実施するための想定工数
前提テスト事項	見出し ID で引用されている前提テスト項目であり、現在のテスト項目の前に完了している必要がある。引用されているテストからのテスト結果無しまたは資料、材料無しでは、このテストは実施できない。
入力情報	テスト項目を完了させるために必要な資料、材料
実施条件	テストを実施するために、車両エコシステムに要求される環境的なテスト条件
確認事項	テスト合格要求を正確に項目にして、それをアルファベット書式にした確認事項。これは本書を使いテスト項目に PASS と記入するために必要な合格要求である。確認事項の 1 つのみが不合格でも、テスト全体が不合格であるとされ修正/調査が要求される。

実施例	テストに関して、受講対象者にガイダンスを与えるように特化されたワークフローの系統的な実施例であり、使用可能な個々のツールの例が、この実施例で明示的に引用されている。テスト項目を進めるために使用されると思われるコマンドセットも引用されている。
備考	表で示されるこのセクションは本書のユーザーに以下の情報をあたえる。 「**ツール**」：テスト項目を完了させるために使用できるツールイクスプリットスクリプティングまたはツールのカスタム化が含まれる場合、その旨が注記される。 「**車両#**」：本書のセクション 2 で示され、本書の事例に関連するこれまでの車両攻撃にリンクしているテスト項目を引用している見出しこのセクションに挙げられている攻撃は、テスト項目内のある確認事項が確認できなかったことの直接的結果を表しています。 「**BSM #**」：ベースシステムモデル文書を直接的に引用しているスレッドモデル ID（TMID）であり、このベースシステムモデル文書はフレームワーク文書と同時進行的に作成された。 「**関連する攻撃**」： テスト項目と関連して発見された車両へのその他の攻撃このセクションに挙げられている攻撃は、テスト項目内のある確認事項が確認できなかったことの直接的結果を表しています。
故障の影響および修正	確認項目を満足できないこと（故障）が車両エコシステムの安全性および他からの攻撃に対する安全性（セイフティおよびセキュリティ）に与える影響の追加説明品質保証を改善するために考えられる修正をテスターが文書化する助けとして、修正のためのガイダンスに少し触れています。

表 4：セクションおよびフレームワークに含まれるべき内容

5.2.2. テスト項目の区分

フレームワークテストシナリオは、次の 3 つの優先度を示すカテゴリに区分されます。「必須、推奨およびアドバンスト」。これは、どの車両エコシステムに関しても実施されるすべてのテストの効率を図るものです。次の表は、カテゴリ毎に、どんなセキュリティに関する経験がテスターに要求されているか、当該のカテゴリのテスト項目が完全に完了した結果として車両エコシステムのセキュリティに現れる影響を詳細に説明しています。

テスト項目は、NIST SP800-30 のアセスメントスケールを参照し、影響をもたらす可能性と脅威が発生する可能性をベースに整理しました。一般的に、脅威事象を発生させるために専門性が要求される場合には、発生する可能性が減少します。それらを鑑みて、テストケースを次のように分類します。

		影響度			
専門性	発生確度	**低い**	**中間**	**高い**	**非常に高い**
低い	**非常に高い**	-	低い **推奨**	高い **推奨**	非常に高い **必須**
中間	**高い**	-	低い **推奨**	高い **推奨**	非常に高い **必須**
高い	**中間**	-	低い **アドバンスド**	低い **アドバンスド**	高い **アドバンスド**
非常に高い	**低い**	-	-	-	低い **アドバンスド**

表 5：リスクとテスト項目の区分

必須：　脅威事象が開始されたまたは発生した場合、負の影響がもたらされるのはほぼ確実であり、エラーまたはインシデントが発生するのはほぼ確実であるもの。

推奨：　脅威事象が開始されたまたは発生した場合、負の影響がもたらされる可能性は高く、エラーまたはインシデントが発生するの可能性は高いもの。

アドバンスド：脅威事象が開始されたまたは発生した場合、負の影響がもたらされる可能性はある程度あり、エラーまたはインシデントが発生する可能性はある程度あるまたは低いもの。

5.3.　テスト項目の網羅性

本テストケースは、リスク分析の手法（NIST SP800 等）をベースにしてベースシステムモデルを作成して、資産の洗い出しを行いました。今回の攻撃対象の入り口には、無線通信を対象にしています。その侵入口から資産に対する脅威とその時のインパクトと発生確率から、重要度を分類しました。セキュリティリスク分析の枠組みに従い分析することで、テスト項目の網羅性をはかりました。次にテストケース抽出方法を示します。

・攻撃対象（侵入口）は、車載システムの無線通信を対象とする

・ISO2626 を利用した BSM と脅威分析から攻撃者モデルを作成

・テストケースの作成は、十分なペネトレーションテスト経験を持つコンサルタントが策定

・自動車のセキュリティナレッジを有するものの知見の活用

・既知の自動車に関するセキュリティインシデントを分析し、テストケースと突合

これらから、車両システムと BSM の類似点と既知の車両システムのインシデントの活用をすることで、既知の自動車セキュリティ評価として有効であると判断します。ただし、ハードウェアの進化や新たな診断ツールが公開されることにより対象のテストケースの更新は必要になる可能性があります。

ここに示されているように、必須項目のテストは車両セキュリティへの基本的なベースラインを提供しています。推奨に加えて、車両のセイフティとセキュリティは一般的な攻撃に対してかなり改善されています。セクション 2 で引用されているように、これは有効であると証明されています。しかし、専門家向けテストが含む追加範囲がエコシステムの全体的なセイフティ、セキュリティおよびロバストネスを含むことを考えると、このフレームワークを適用する際に車両テストに 3 つのカテゴリのすべてのテストを実施できれば、車両エコシステム全体がセイフティとセキュリティの両面で、車両の脆弱性攻略の最新の研究レベルを考慮しても完全に保護されていることになります。

6. フレームワークテスト項目

6.1. 構造の概要

このフレームワーク内の主なスイート（パッケージソフト）に焦点をあてたテストケースと、該当する見出し番号、ページ番号およびカテゴリを項目にして、以下に示します。

6.2. Wi-Fi（802.11a/n/g/b）

このセクションでは、対象となる車両内の Wi-Fi のセキュリティを評価するための方法論を示します。インフォテインメントシステム、気象情報システムおよび電気システムを制御するためにユーザーが自分のスマートフォンを車両の Wi-Fi モジュールのようなエントリポイントへ接続できるため、これは車両のセキュリティ（およびセイフティ）の重要な側面です。Wi-Fi モジュールのような装置は、インフォテインメントシステムに内蔵される 1 つ以上のインターフェイスに接続されます。

インフォテインメントシステムは、診断情報を得るための車両の CAN バス、インターネットおよび/またはインフォテインメントプロバイダーサーバーのバックエンド、V2X または車両製造者のバックエンドサポートまたはモニタリングシステムにアクセスするためのセルラーモデムモジュールを含む、他のネットワークに接続される可能性があります。

車両の乗客は、ほとんどの場合、携帯電話のような別のネットワークを介してインターネットの機能を利用するために Wi-Fi に接続します。これにより、複数の乗客が同時にインターネットに接続できる便利さが得られます。さらに、車両によっては、スマートデバイスへの Wi-Fi コネクションを使いソフトウェアの更新が受信できるものもあります。

攻撃者が Wi-Fi アクセスポイントにアクセスした場合、その攻撃者は、インフォテインメントシステムで動作しているサービス、CAN バス上のハードウェア、または Wi-Fi アクセスポイントから接続可能バックエンドシステムやネットワークのどれかに、アクセスと試みることが可能です。ネットワークサービスやセキュリティシステムのルールはこのようなアクセスを制限するように構築されているでしょうが、このようなルールを特定することおよびルールをバイパスすることがセキュリティテストの次のステップです。したがって、これらは評価の一部としてレビューされます。

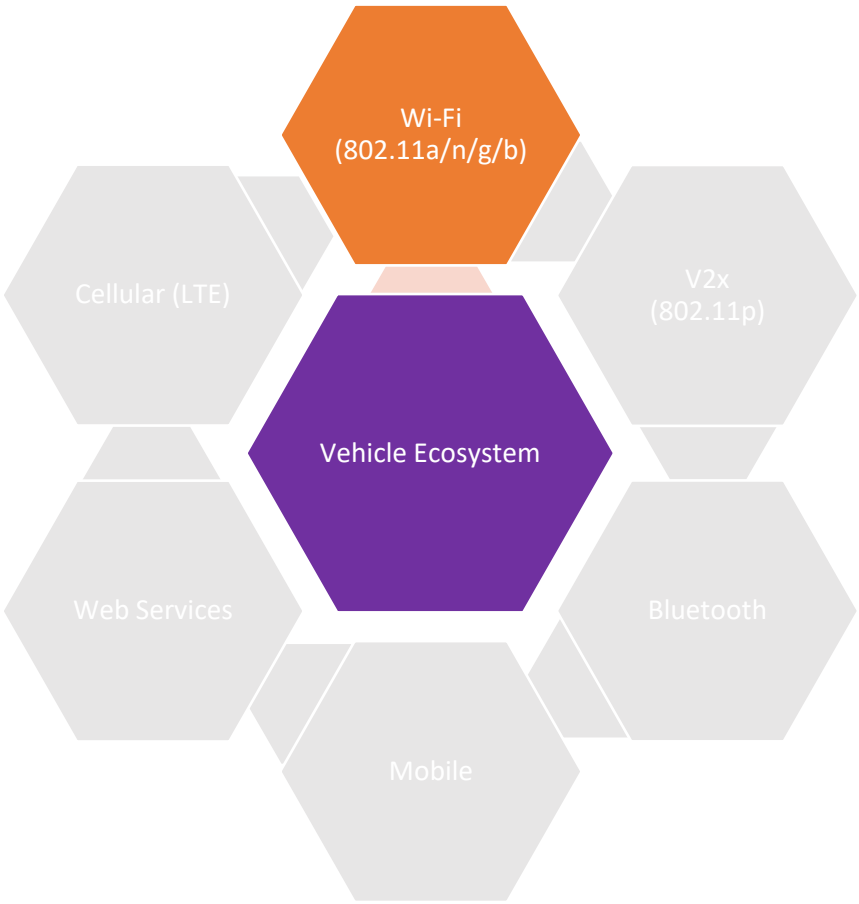


図 4：サブコンポーネントである Wi-Fi がハイライトされている

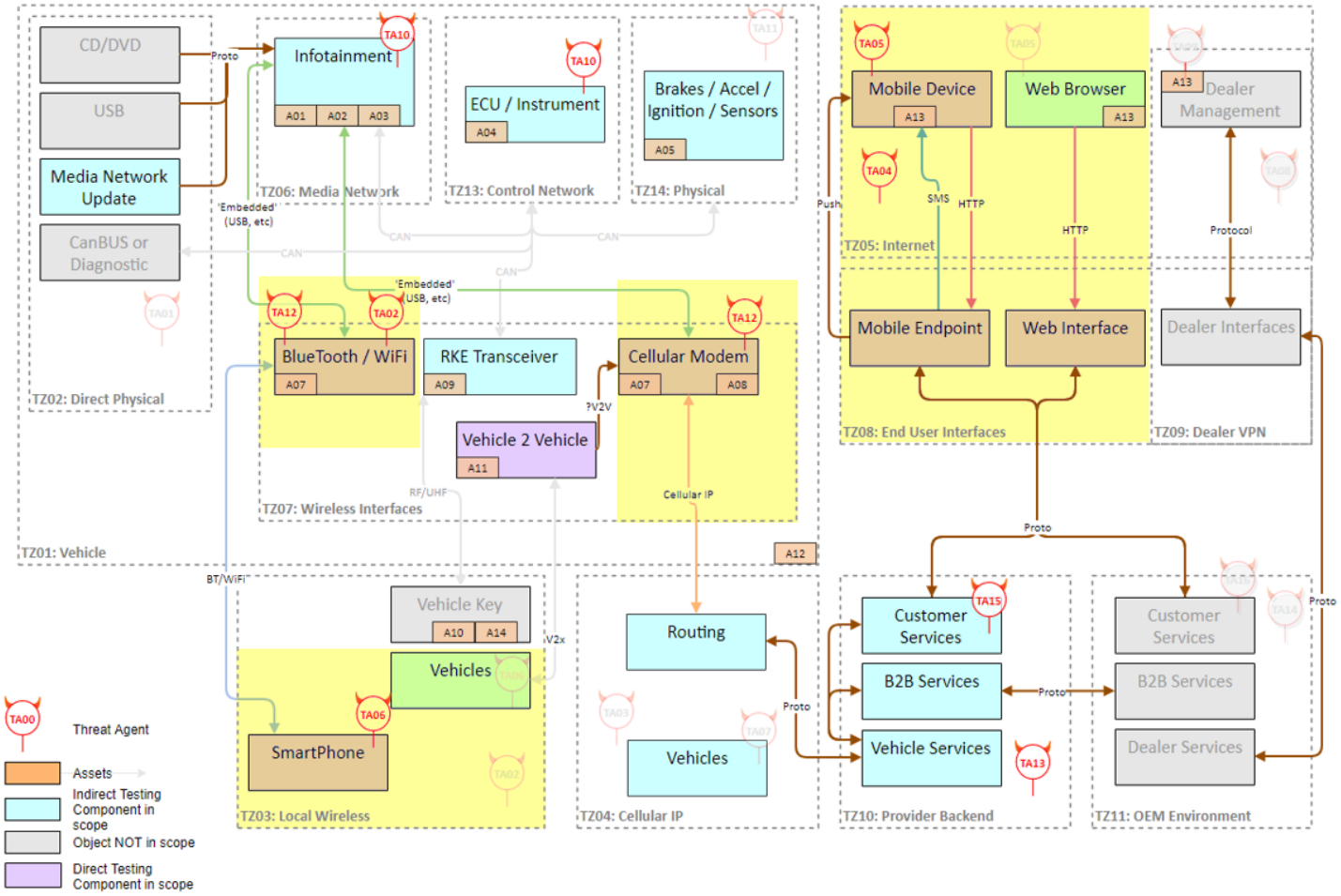


図 5：Wi-Fi の範囲内の項目への直接的なテストの影響

=

6.2.1. 必須

6.2.1.1. ワイヤレス通信のデフォルトの特定

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WIFI_1</td></tr>
<tr><td>項目名</td><td>Wi-Fi のデフォルト設定の特定</td></tr>
<tr><td>目的</td><td>デフォルト SSID とそれの個々のプロトコルを特定する。
このテストは、他のテストが競合するこのテスト項目に依存するので、このテストは必須としてランク付けされる。
車両コンポーネントを公開しているオープンなネットワークがないことを保証する。
車両の無線プロファイルの概要が簡単な攻撃のために開いていないことを保証する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>0.5 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>車両仕様マニュアル</td></tr>
<tr><td>実施条件</td><td>1. システムコンポーネントの Wi-Fi をオンする。
2. 車両は、ワイヤレスアクセスポイントモードに対応している。
3. コンソールまたは製造者が提供している Wi-Fi ネットワーク対応表</td></tr>
<tr><td>確認事項</td><td>車両がオフである場合、SSID が見つからない（ブロードキャストまた隠されている）。
Open Network も WEP もない。
SSID モードおよび暗号化モードがすべて特定されている。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>公開用資料のため、記載内容を削除</td><td>TMID-01</td><td>セクション 2.1.4、2.1.5</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>車両が OFF の時に SSID が見つかった場合、その車両が攻撃者から攻撃を受ける可能性が常時あります。「Open Network」または「WEP」が見つかった場合、攻撃者はその車両へのコネクションを容易に確立できる可能性があります（テストシナリオ 2 および 3）。このようなセキュリティが弱い</td></tr>
</table>

	プロトコルは、さらに車両/デバイス通信の保護に適したプロトコルへアップグレードすべきです。

6.2.1.2. 暗号化されていない通信およびデータコンテンツ

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WIFI_2</td></tr>
<tr><td>項目名</td><td>Wi-Fi を使って送信されるデータが暗号化されていないかどうかの特定</td></tr>
<tr><td>目的</td><td>プレーンテキストプロトコルがトラフィックに使用されていることを特定する。
このテストは、他のテストが競合するこのテスト項目に依存し、アクセスポイントで暗号化されていないプロトコルの仕様はクリティカルな脆弱性となるため、このテストは必須としてランク付けされる。
センシティブな情報をセキュアとするために通信が暗号化されていることを保証する。
このテストは、Wifi が正しく暗号化され、顧客や OEM のデータが適切に保護されていることを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>0.5 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.2.1.1</td></tr>
<tr><td>入力情報</td><td>1. 車両マニュアル
2. 車両とデバイス間のアクティブなデータコネクション</td></tr>
<tr><td>実施条件</td><td>コンテンツがセンシティブなものであれ、そうでないものであれ、テスト中、車両はアクティブなデータコネクションを行っている</td></tr>
<tr><td>確認事項</td><td>プレーンテキストプロトコルは使用されていない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>公開用資料のため、記載内容を削除</td><td>TMID-01</td><td>セクション 2.1.3</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>ネットワークを使い送信される機密データは、暗号化されているべきです。ワイヤレスプロトコルが提供しているセキュリティは、このデータを盗聴者となり得る者から保護するには十分ではない。ネットワークを介して送信されるデータは、なんらかの暗号化スイートで暗号化して、センシ</td></tr>
</table>

	ティブな情報のすべてが TLS 1.1 以上で提供されるセキュリティと同等なセキュリティを持つようにする。さらに、ネットワーク通信を介した機密データのやりとりは、最小限に抑え、攻撃者がデータをキャプチャして、後日メカニズムに欠陥が見つかった場合に暗号解読する機会を最小限にとどめるべきである。

6.2.1.3. 盗聴（スニッフィング）

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WIFI_3</td></tr>
<tr><td>項目名</td><td>Wi-Fi 盗聴</td></tr>
<tr><td>目的</td><td>パッシブな盗聴を試みる外部コンポーネントに対する車両の反応を実証する。
暗号化可能なプロトコル上で暗号化されていない通信を行っている場合、深刻な脆弱性となるため、このテストは必須としてランク付けされる。
センシティブな情報が暗号化されていること。
センシティブな情報が保護されていること。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>3 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.2.1.1</td></tr>
<tr><td>入力情報</td><td>車両マニュアル</td></tr>
<tr><td>実施条件</td><td>Wi-Fi エクスプロテーション（攻略）が成功した場合、アクセス可能なトラフィックを模擬するために、車両はその内部のサブコンポーネントとアクティブに通信している。</td></tr>
<tr><td>確認事項</td><td>車両は、機密データをプレーンテキストで露出していない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>公開用資料のため、記載内容を削除</td><td>TMID-01</td><td>セクション 2.1.5</td><td>Wi-Fite</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>ネットワークを使い送信される機密データは、暗号化されているべきです。ワイヤレスプロトコルが提供しているセキュリティは、このデータを盗聴者となり得る者から保護するには十分ではない。ネットワークを介して送信されるデータは、なんらかの暗号化スイートで暗号化して、センシティブな情報のすべてが TLS 1.1 以上で提供されるセキュリティと同等なセキュリティを持つようにする。さらに、ネットワーク通信を介した機密データのやりとりは、最小限に抑え、攻撃者がデー</td></tr>
</table>

	タをキャプチャして、後日メカニズムに欠陥が見つかった場合に暗号解読する機会を最小限にとどめるべきです。

6.2.1.4. 入力処理の評価ファジング

項目	記載内容
項目番号	NEDO_WIFI_4
項目名	Wi-Fi のファジング
目的	クライアントとアクセスポイント間の通信を無効にできることを実証する。 このテストは、ファジングが比較的簡単に実行できること、また深刻な脆弱性を発見可能なことから必須としてランク付けされる。 実装における深刻なフローを発見する。 クリティカルなシステムにおける安全性とセキュリティを保護すること。
実施タイミング	
想定実施工数	24 時間
前提テスト項目	項目 6.2.1.1 でワイヤレスプロトコルが使用されていることが特定されていることが必要である。
入力情報	1. 車両の通信仕様書（通信モジュールがすべて搭載されている） 2. 車両モジュールが対応している Wi-Fi スペクトラムブロードキャスト周波数範囲
実施条件	1. ステータスが ON および HIBERNATE である車両でテストする。 2. 車両は、検査対象であるトラフィック向けのワイヤレスを使い、アクティブに通信を行っている。
確認事項	A. メッセージをドロップする。 B. 変更したメッセージをインジェクトする。 C. 無効な暗号化スイート D. 無効な EAPOL-Key ディスクリプタイプ E. 無効な EAPOL-Key 情報フラッグ F. 予想外の EAPOL-K 暗号化スイート、たとえば SHA1 付きの AES が MD5 付きの RC4 で置き換えられている。 G. 無効な EAPOL-Key リプレイカウンター（予想よりも少ないかまたは多い）。 H. 無効な EAPOL-Key ノンス I. 無効な EAPOL-Key MIC： セットされている/セットされていない。 J. クラッシュ K. 無限ループ L. リソースのリークまたは不足 M. 予期しない動作
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除

<table>
<tr><td></td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>公開用資料のため、記載内容を削除</td><td>TMID-08</td><td>N/A</td><td>WPA2 KRACK</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>ファジングテストは、書式が間違ったプロトコルや情報に対するシステムの回復力（レジリエンスィ）を検査している。システムが、これらのテストの 1 つ以上に合格せずに予想外の反応をした場合、またはこれらのテストに反応しなくなった場合、物理的な実装または Wi-Fi ドライバーに欠陥があると考えられる。ハードウェアおよびドライバーとインタラクションしているファームウェアをモニタおよび解析して、ファジングプロセスに見つかった弱点を検出、補修、または除去するべきです。</td></tr>
</table>

6.2.1.5. セキュアなプロトコルの実装の評価

項目	記載内容
項目番号	NEDO_WIFI_5
項目名	セキュアなエンドポイントに共通な欠陥は、推奨されているよりも脆弱なバージョンの TLS を利用しているために生じている。 このテストは、比較的簡単に実行され、深刻な脆弱性を露出するため、必須としてランク付けされる。 すべてのプロトコルが正しくセキュアになっていること。 プロトコルすべてが保護されていることを証明すること。
目的	車両エコシステムの存在する TLS 実装の脆弱さを、系統的に調べて特定する。
実施タイミング	
想定実施工数	0.5 時間
前提テスト項目	項目 6.2.1.1
入力情報	1. 車両マニュアル（公的に入手できる場合） 2. 認められている暗号化プロトコルのリスト
実施条件	1. 車両は、6.2.1.5.5 で発見された各ステータスでテストされる。 2. TLS を使用する暗号化された Wi-Fi 通信標準 3. 車両は、それが通信中のデバイスとアクティブに通信している。
確認事項	A. サービスが、CBC、MD5、RC4、Des およびその他の陳腐化した方法のような脆弱なセキュリティプロトコルを使っていないことを確認する。 B. TLS 1.1 以上が使用されていることを確認する。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除
備考	ツール / BSM # / 車両#： / 関連する攻撃

	公開用資料のため、 記載内容を削除	TMID-01	セクション 2.1.2、 **2.1.3**、2.1.6	KCI 攻撃
故障の影響および修正	セキュリティが弱いプロトコルは、攻撃者がデータストリームに不正侵入し、その中の情報へのアクセスすることを許してしまう。セキュリティプロトコルは、データを確実に保護するためにさらにセキュアな暗号化スイートを使用すべきです。TLS1.1 以上の暗号化スイートを使うべきであり、RC4 のような弱い暗号化スイートを採用すべきではない。			

6.2.1.6. 露呈されているネットワークおよびサービスの発見

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WIFI_6</td></tr>
<tr><td>項目名</td><td>車両のネットワークが脆弱であるために、どのサービスが露呈されているか判断する。
どのサービスが動作しているか、インフォテインメントシステム上のどのサービスが予期せず動作しているか露呈することから、このテストは必須としてランク付けされる。

必要なサービスだけが動作していることを保証する。

システム上で予期せぬプロトコルが使用されていないことを保証する。</td></tr>
<tr><td>目的</td><td>どのネットワークサービスが露呈されているか判断する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>6 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>1. 車両仕様マニュアル
2. 車両により露呈されているはずのすべてのウェブサービスのリスト</td></tr>
<tr><td>実施条件</td><td>システムコンポーネントの Wi-Fi をオン。</td></tr>
<tr><td>確認事項</td><td>サービスが予想どおりであることを確認する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>公開用資料のため、
記載内容を削除</td><td>TMID-01</td><td>セクション 2.1.2</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>車両により露呈されるウェブサービスは、ユーザーが必要とするサービスに限定されるべきである。入力リストに存在しない、およびユーザーが直接的に通信しないウェブサービスはすべて、除外するかまたはファイアウォールで防護されるべきである。</td></tr>
</table>

6.2.2. 推奨

6.2.2.1. 暗号化ダウングレード攻撃

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WIFI_7</td></tr>
<tr><td>項目名</td><td>使用されている暗号化を不正侵入され得るものにダウングレードすることを試みる。</td></tr>
<tr><td>目的</td><td>エントリポイントへの非認証アクセスを取得する。暗号化の脆弱化を利用する。
このテストは、WPA/WPA2 暗号と無線での侵入攻撃手法の知識が必要となるため、Recommended としてランク付けされる。
システムが暗号化ダウングレード攻撃に対する保護を有していることを保証する。
車輌が KRACK のような攻撃から安全であることを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>4 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>車両マニュアル（公的に入手できる場合）</td></tr>
<tr><td>実施条件</td><td>A.ステータスが ON および HIBERNATE である車両でテストする。
B.WPA/WPA2 および TKIPWi-Fi に対する通信標準
C.車両は、Wi-Fi デバイスとアクティブに通信している。</td></tr>
<tr><td>確認事項</td><td>TKIP ダウングレードを行おうとする試みにシステムが抵抗する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>公開用資料のため、記載内容を削除</td><td>TMID-08</td><td>セクション 2.1.2</td><td>WPA2 KRACK</td></tr>
</table>
</td></tr>
</table>

故障の影響および修正	ダウングレード攻撃により、攻撃者はデータパケットの観察ができ、データパケットの改ざんもできる可能性がある。ダウングレード攻撃に対する主なソリューションは、ダウングレードの可能性に対する防護を確実に行うために、システムのファームウェアを更新する。さらに、TKIP 脆弱性がありそうな場合、TLS 暗号化を使いデータ侵害があった際にデータを保護するべきです。

6.2.2.2. グループ暗号キーの予測可能性の決定

項目	記載内容
項目番号	NEDO_WIFI_8
項目名	ワイヤレスネットワークのセキュリティは、暗号キーの強度に依存しています。しかし、攻撃者がこの暗号キーを予測できれば、この強度は劣化する。
目的	暗号キーを予測できる方法があるかを判断する。 このテストは、攻撃に時間がかかること、およびファームウエアのリバースエンジニアリングか静的解析を行う特別なスキルを必要とするため、 Recommended としてランク付けされる。 システムが予測可能な暗号キーを生成しないことを確認する。
実施タイミング	
想定実施工数	6 時間
前提テスト項目	項目 6.2.1.1
入力情報	車両マニュアル（公的に入手できる場合）
実施条件	ステータスが ON および HIBERNATE である車両でテストする。
確認事項	実用的に攻撃に利用できる時間内に、キーを予測できる方法がない。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除
備考	<table><tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr><tr><td>公開用資料のため、記載内容を削除</td><td>TMID-02</td><td>セクション 2.1.2</td><td>N/A</td></tr></table>
故障の影響および修正	予測可能なグループキーは、攻撃者が車両の防衛されたネットワークを観察し、参加することを許してしまう。グループキーが使用される可能性がある時間枠内で、グループキー作成の予測または計算ができないように、キー生成プロセスは再設計されるべきである。

6.2.2.3. 車両とエコシステム間の車内通信の評価

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WIFI_9</td></tr>
<tr><td>項目名</td><td>車両が提供するネットワーク上の 2 つのデバイス間の通信量には、限界がある。</td></tr>
<tr><td>目的</td><td>車両の自動車ワイヤレスの 2 つのデバイスが相互にやりとりできる通信量を確定する。
このテストは、無線通信とモデムとトラフィックの直接通信に対する特別な知識を要求されるため、 Recommended としてランク付けされる。
システム間の通信に割り込む方法がないことを証明する。
通信システムが隔離されていることを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>2 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.2.1.1</td></tr>
<tr><td>入力情報</td><td>車両マニュアル（公的に入手できる場合）</td></tr>
<tr><td>実施条件</td><td>1. ステータスが ON および HIBERNATE である車両でテストする。
2. 車両が、2 つのモバイルデバイスとアクティブに通信している。</td></tr>
<tr><td>確認事項</td><td>明示的に許可されたデバイス以外との直接の相互作用がないこと。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>公開用資料のため、
記載内容を削除</td><td>TMID-09</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>車両ワイヤレスネットワーク上のデバイス同士は、直接的なコンタクトを持つべきではない。このテストに合格しない場合、車両ネットワークに関連付けられたデバイスは、それ自体がアクセスすべきよりも多いアクセスを他のデバイスにアクセスをすべきです。これにより、あるデバイスがネットワーク上の別のデバイスへ攻撃を試みることができる。</td></tr>
</table>

6.2.2.4. ソフトウェア（ソース）の特定

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WIFI_10</td></tr>
<tr><td>項目名</td><td>オープンワークソフトウェアに基づいて、車載のどのソフトウェアサービスが期限切れのソフトウェアサービスであるか特定する。</td></tr>
<tr><td>目的</td><td>GPL を調べ、期限切れの車載ソフトウェアを特定する。
このテストは、特別なツールとその検出結果から誤検知を特定する能力が必要とされるため、Recommended としてランク付けされる。
すべてのソフトウェアが最新であること保証する。
コードベースに既知の CVE がないことを保証する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>2 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>1.車両仕様マニュアル
2.オープンソースソフトウェア宣言のリリース</td></tr>
<tr><td>実施条件</td><td>研究のために、オープンソースソフトウェアがダウンロードされている。</td></tr>
<tr><td>確認事項</td><td>A.予想されるバージョンより前のバージョンのソフトウェアはない。
B.公開されているシビアな CVE をもつソフトウェアはない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>公開用資料のため、
記載内容を削除</td><td>TMID-09</td><td>セクション
2.1.1、2.1.2、2.1.4、
2.1.6</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>オープンソースソフトウェア（OSS）は多くの利点を持つが、そのコード内のセキュリティ上の脆弱性を見つけるために、継続的にテストされている。ソースが最新版に更新され続けられていない場合、攻撃者が悪用できる既知の脆弱性がシステムに含まれる可能性がある。ファームウェアを作成するために使用されたソースのどれかに既知の CVE があった場合、それらの項目は、当該の CVE を無くしたバージョンに更新する必要がある。</td></tr>
</table>

6.2.3. アドバンスド

6.2.3.1. チャンネルベースの MITM

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WIFI_11</td></tr>
<tr><td>項目名</td><td>ワイヤレストラフィックへ MITM 攻撃を行おうと試みる。</td></tr>
<tr><td>目的</td><td>このテストは、ジャミング攻撃および基本的な MITM 攻撃に対する車両の耐性を判断するために、ワイヤレスプロトコルを解析しようとするテストです。このテストには、車両を承認されていないチャンネルおよび承認されていないアクセスポイントに強制的に参加させる試み、ならびにシステムが提供している防衛手段を無効にしようとする試みが入っているべきです。
このテストは、無線信号と WPA 仕様について特別な知識が必要とされるため、Advanced としてランク付けされる。
システムが外部からの MITM 攻撃から保護されていることを保証する。
システム間通信が保護されていることを保証する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>2 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.2.1.1</td></tr>
<tr><td>入力情報</td><td>車両マニュアル（公的に入手できる場合）</td></tr>
<tr><td>実施条件</td><td>1.ステータスが ON および HIBERNATE である車両でテストする。
2.車両は、検査対象であるトラフィック向けのラインを使い、アクティブに通信を行う必要がある。</td></tr>
<tr><td>確認事項</td><td>MITM 攻撃に対してシステムが回復機能を持つことを確認する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>公開用資料のため、
記載内容を削除</td><td>TMID-09</td><td>セクション 2.1.1、
2.1.3
2.1.2</td><td>WPA2 KRACK</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>MitM を許す脆弱性がデバイスに存在すると、それはセキュリティ上、重大な懸念である。正しい Wi-Fi チャンネルおよびアクセスポイントのみが関連付けられるように、システムを調整すべきで</td></tr>
</table>

	ある。また、不正なアクセスポイントが検知された場合、その問題を防衛手段が他にアラートできるように、システムを調整すべきである。

6.2.3.2. 実装されたウェブサービスのファジング

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WIFI_12</td></tr>
<tr><td>項目名</td><td>車両で使用されるウェブサービスをファジングする</td></tr>
<tr><td>目的</td><td>このテストは、デバイスが提供するウェブサービスをすべてリスト化し、様々なファジング技法を採用すべきです。ウェブサービスのリストには、まず、アクティブな捜査（ネットワークスキャン）とパッシブな捜査（スニッフィング）の両方が含まれるべきです。このようにして発見された各プロトコルは、カスタム化されたファジングテストの対象とされ、当該のプロトコル実装時の欠陥を明らかにする。
このテストは、複数の Web サービスについて、発見されたフローの深刻性を判断するための知識が要求されるため、Advanced としてランク付けされる。
クリティカルなサービスの実装においてフローが存在するか確認する。
システムに明らかなフローが存在しないことを保証する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>25 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.2.1.1</td></tr>
<tr><td>入力情報</td><td>車両マニュアル（公的に入手できる場合）</td></tr>
<tr><td>実施条件</td><td>1.システムコンポーネント上の Wi-Fi システムをオンする（該当する場合）。
2.ワイヤレスデバイスを車両に関連付ける。
3.テストツールを車両に関連付ける。</td></tr>
<tr><td>確認事項</td><td>テスト時には、サービス停止、クラッシュ、予期しない動作がないことを確認する</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-02</td><td>セクション 2.1.5、2.1.4</td><td>ハートブリード
Vault7 テレネット</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>車載のウェブサービスのほとんどは、標準的なプロトコルに基づいている。このサービスのどれかがウェブへの一般的な攻撃に脆弱である場合、そのコンフィギュレーションにミスがないか確認すべきです。ミスが見つからない場合、問題が解決されている最新のバージョンにサービスを更新すべきです。ファジングにより脆弱性が発見されたら、そのサービスの脆弱性を簡単に直すことはできないと考えられる。その脆弱性を無くするために、なぜその脆弱性が存在するか、どんなきっかけでその脆弱性が分かったかを調べるべきです。</td></tr>
</table>

6.2.3.3. ファジングテレネット

項目	記載内容
項目番号	NEDO_WIFI_13
項目名	テレネット実装のテスト
目的	このテストは、テレネットプロトコルに焦点を絞り、そのプロトコルを実装した際に欠陥がないか徹底的にテストする。テレネットはシステムへの主要なエントランスの一つであるので、このテストが可能な限り完璧なものであるように注意を払うべきです。テレネットのバージョンには、パスワード無しに改ざんされたコネクションリクエストを介してシステムレベルでのアクセスを許すようにできることが、最近のエクスプロイトで分かったので、完璧なテストをおこなうことが強調されている。 このテストは、テレネットプロトコルとテスト結果にフローが存在するかを判断するスキルが必要とされるため、Advanced としてランク付けされる。 テレネット実装にフローが存在するかを確認する。 システムに対してのアクセスが承認されていないプロトコルにおいてフローが存在しないことを確認する。
実施タイミング	
想定実施工数	2 時間
前提テスト項目	項目 6.2.1.6
入力情報	車両マニュアル（公的に入手できる場合）
実施条件	1.システムコンポーネント上の Wi-Fi システムをオンする（該当する場合）。 2.ワイヤレスデバイスを車両に関連付ける。 3.telnet が実行されていることを検証する。
確認事項	データのファジングでクラッシュや予期しないステータスが生じないことを確認する。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除
備考	ツール: BSM # TMID-01 / 車両#： N/A / 関連する攻撃 Vault7 テレネット
故障の影響および修正	ファジング telnet により発見された脆弱性を調査して、その問題の深刻さおよび脆弱性がどこで生じているかを判断する必要がある。一般的には、telnet 実行コードとそのライブラリのコードのレビューまたは静的解析を行い、問題を解決するための最善の方法を決める必要がある。

6.2.3.4. SSH のファジング

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WIFI_14</td></tr>
<tr><td>項目名</td><td>SSH サービスの実装テスト</td></tr>
<tr><td>目的</td><td>このテストは、SSH プロトコルに焦点を絞り、そのプロトコルを実装した際の欠陥がないか徹底的にテストします。このプロトコルは、システムへの主要なエントランスの一つであるので、このテストが可能な限り完璧なものであるように注意を払います。車両に予想外のステータスおよび膨大な情報漏洩をもたらすことになるパケットは存在しないことを、このテストで確認します。
このテストは、SSH プロトコルとテスト結果にフローが存在するかを判断するスキルが必要とされるため、Advanced としてランク付けされる。
SSH 実装にフローが存在するかを確認する。
システムに対してのアクセスが承認されていないプロトコルにおいてフローが存在しないことを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>2 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.2.1.6</td></tr>
<tr><td>入力情報</td><td>車両マニュアル（公的に入手できる場合）</td></tr>
<tr><td>実施条件</td><td>1. システムコンポーネント上の Wi-Fi システムをオンする（該当する場合）。
2. ワイヤレスデバイスを車両に関連付ける。
3. SSH が実行中かを確認する。</td></tr>
<tr><td>確認事項</td><td>SSH サービスのファジングによってクラッシュや意図しない状態を引き起こさないかを確認する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-01</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>テストが上手くいかない場合、SSH が適切に実行されていない。ファジングによって発見された脆弱性については、問題の深刻度と発生場所を特定するための調査を行う必要がある一般的に、コードレビューまたは静的解析は、SSH 実行ファイルとそのライブラリについて行い、問題解決の最善策を特定する必要がある。</td></tr>
</table>

6.2.3.5. HTTP のファジング

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WIFI_15</td></tr>
<tr><td>項目名</td><td>HTTP サービスの実装テスト</td></tr>
<tr><td>目的</td><td>このテストは、HTTP プロトコル、また、インフォテイメントシステム内の対応する Web サーバーについて重点的に行う必要がある。これらのシステムは複数のファイルやメッセージタイプをパースできるため、ファジングには時間がかかる可能性がある。テスト担当者は、ファジングで確認される一般的なクラッシュやフリーズの影響だけでなく、機密データの読み込みや書き込みが行われる領域にも注意する必要がある。
このテストは、HTTP プロトコルとテスト結果にフローが存在するかを判断するスキルが必要とされるため、Advanced としてランク付けされる。
HTTP 実装にフローが存在するかを確認する。
システムに対してのアクセスが承認されていないプロトコルにおいてフローが存在しないことを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>3 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.2.1.6</td></tr>
<tr><td>入力情報</td><td>車両マニュアル（公的に入手できる場合）</td></tr>
<tr><td>実施条件</td><td>1.システムコンポーネント上の Wi-Fi システムをオンする（該当する場合）。
2.ワイヤレスデバイスを車両に関連付ける。
3.列挙された HTTP サービスが実行されているかを確認する。</td></tr>
<tr><td>確認事項</td><td>データのファジングでクラッシュや予期しないステータスが生じないことを確認する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-01</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>HTTP のファジングによって発見された脆弱性については、問題の深刻度と発生場所を特定するための調査を行う必要がある。一般的に、コードレビューまたは静的解析は、サーバーの実行ファイルとクライアントの実行ファイル、それらのライブラリについて行い、問題解決の最善策を特定する必要がある。</td></tr>
</table>

6.2.3.6. ネットワークプロトコルで送られるデータのファジング

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WIFI_16</td></tr>
<tr><td>項目名</td><td>車両が使用するサービスの実装テスト</td></tr>
<tr><td>目的</td><td>プロトコルそれ自体とは別に、Web サービスプロトコルで送られるデータのファジングも行う必要がある。このテストには、プロトコルが使用するデータの観察、また、Web サービスをコントロールするエンドポイントを徹底的に破壊するのに特化したファジングテンプレートの作成が含まれる。
Web サービスがあるか確認する。
このテストは、何らかのプロトコルとテスト結果にフローが存在するかを判断するスキルが必要とされるため、Advanced としてランク付けされる。
様々なプロトコルよって使用されるデータにフローが存在するかを確認する。
システムに対してのアクセスが承認されていないプロトコルにおいてフローが存在しないことを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>1.デバイス上のワイヤレスを特定する。
2.プロダクトツールを隔離する。</td></tr>
<tr><td>入力情報</td><td>車両マニュアル（公的に入手できる場合）</td></tr>
<tr><td>実施条件</td><td>1.システムコンポーネント上の Wi-Fi システムをオンする（該当する場合）。
2.ワイヤレスデバイスを車両に関連付ける。</td></tr>
<tr><td>確認事項</td><td>データのファジングでクラッシュや予期しないステータスが生じないことを確認する</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-01</td><td>セクション 2.1.1、2.1.2、2.1.5、2.1.6</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>特定のプロトコルファジングによって発見された脆弱性については、問題の深刻度と発生場所を特定するための調査を行う必要がある。一般的に、コードレビューまたは静的解析は、実行ファイルとそのライブラリについて行い、問題解決の最善策を特定する必要がある。</td></tr>
</table>

6.2.3.7. 脆弱な設定の特定

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WIFI_17</td></tr>
<tr><td>項目名</td><td>安全性の低いシステムを適切に再設定できる場合には、システムのセキュリティを確保できる。</td></tr>
<tr><td>目的</td><td>このテストによって、情報システムで実施される Web サービスが使用するさまざまな設定を特定する必要がある。各サービスを確認し、デバイスの全体的なセキュリティの向上が可能かを検証し、安全性と説得力の観点から妥協点を探りだす。

このテストは、様々なサービスがどのように構成されるべきか、という知識が要求されるため、Advanced にランク付けされる。

システムが正しく構成されていることを保証する。

構成に起因する脆弱性がシステム上に存在しないことを保証する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>車両仕様マニュアル</td></tr>
<tr><td>実施条件</td><td>車両へのファームウェアレベルのアクセスを実行する。</td></tr>
<tr><td>確認事項</td><td>すべてのサービス設定が正しいこと</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-09</td><td>セクション 2.1.1</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>テストが上手くいかない場合には、車両で実行中の Web サービスについて、然るべき安全性が確保されていない。このテストが実行できないサービスそれぞれについて、最も安全な設定になっているかどうか確認する必要がある。</td></tr>
</table>

6.2.3.8. 旧式の無線サービスの ID

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WIFI_18</td></tr>
<tr><td>項目名</td><td>Web サービスの調査によって、車両で無効となっているソフトウェアサービスを特定する。</td></tr>
<tr><td>目的</td><td>このテストは、各 Web サービスのバージョンの特定に加え、既知のセキュリティ上の弱点にシステムがさらされていないことを確認するためにコンポーネントが使われていることを確認する。
このテストは、無線サービスのバージョンを評価するためにエキスパートなスキルが要求されるため、Advanced にランク付けされる。
すべての Web サービスが最新であることを保証する。
古いソフトウェアに含まれる既知の脆弱性が存在しないことを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.2.1.6</td></tr>
<tr><td>入力情報</td><td>車両仕様マニュアル</td></tr>
<tr><td>実施条件</td><td>システムコンポーネントの Wi-Fi をオンする。</td></tr>
<tr><td>確認事項</td><td>A.予想されるバージョンより前のバージョンのソフトウェアはない。
B,既知の共通脆弱性識別子（CVE）を持つソフトウェアがない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-01</td><td>セクション 2.1.1、2.1.3</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>ワイヤレスサービスは、車両への入り口となる。既知の脆弱性があるサービスがデバイスで使われている場合には、失敗した各コンポーネントを確認し、それぞれの脆弱性がセキュリティに及ぼす影響の大きさを検証する。さらに、より安全性の高いバージョンにサービスを更新する必要もある。</td></tr>
</table>

6.2.3.9. ソフトウェアの特定（ファームウェア）

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WIFI_19</td></tr>
<tr><td>項目名</td><td>車両で無効となっているソフトウェアサービスの特定。</td></tr>
<tr><td>目的</td><td>このテストは、ソフトウェアを構築するために提供されるファームウェアイメージの解析に加え、車両が使用するカーネルが最新であり、イメージに既知の脆弱性がないかを解析する。
このテストは、無線サービスのバージョンを評価するためにエキスパートなスキルが要求されるため、Advanced にランク付けされる。
すべての Web サービスが最新であることを保証する。
古いソフトウェアに含まれる既知の脆弱性が存在しないことを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.2.1.6</td></tr>
<tr><td>入力情報</td><td>車両仕様マニュアル</td></tr>
<tr><td>実施条件</td><td>車両で使われるファームウェアイメージを取得する。</td></tr>
<tr><td>確認事項</td><td>A.予想されるバージョンより前のバージョンのソフトウェアはない。
B.公開されているシビアな CVE をもつソフトウェアはない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-09</td><td>セクション 2.1.1、2.1.2、2.1.4、2.1.6
2.1.3</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>車両のファームウェアは、次々と発見される新たな脆弱性を修正するため、常に最新の状態にしておく必要がある。このテストが上手くいかない場合、ファームウェアが依存する 1 つまたは複数のコンポーネントに、システムのセキュリティ回復のために解消の必要のある既知の不具合があることを示す。</td></tr>
</table>

6.2.3.10. ソフトウェア（ソース）の特定

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WIFI_20</td></tr>
<tr><td>項目名</td><td>オープンソースソフトウェアに依存する車両で無効となっているソフトウェアサービスの特定</td></tr>
<tr><td>目的</td><td>GPL を調べ、期限切れの車載ソフトウェアを特定する。
このテストは、提供されたソフトウェアのバージョンを評価するエキスパートなスキルが要求されるため、Advanced にランク付けされる。
すべてのソースコードが最新であり、予期しない脆弱性が存在しないことを保証する。
古いソフトウェアに含まれる既知の脆弱性が存在しないことを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>1.車両仕様マニュアル
2.オープンソースソフトウェア公開の布告</td></tr>
<tr><td>実施条件</td><td>研究のために、オープンソースソフトウェアがダウンロードされている。</td></tr>
<tr><td>確認事項</td><td>A.予想されるバージョンより前のバージョンのソフトウェアはない。
B.公開されているシビアな CVE をもつソフトウェアはない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-02</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>オープンソースソフトウェア（OSS）は多くの利点を持つが、そのコード内のセキュリティ上の脆弱性を見つけるために、継続的にテストされている。ソースが最新版に更新され続けられていない場合、攻撃者が悪用できる既知の脆弱性がシステムに含まれる可能性がある。既知の脆弱性があるパッケージはすべて、より安全なバージョンに更新する必要がある。</td></tr>
</table>

6.2.3.11. WIDS/WIPS 検出

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WIFI_21</td></tr>
<tr><td>項目名</td><td>システムが不正アクセスポイントに接続できてしまうかの検証</td></tr>
<tr><td>目的</td><td>このテストは、WIDS/WIPS のセキュリティ状況の有効性を検証するためのテストとなる。テスト担当者は、WIPS のセキュリティの回避を試み、不正アクセスポイントを検出した場合の対策の有効性を検査する。また、WIDS が使用するチャンネルを妨害し、別のチャンネルに接続しようとする場合や正しいプロトコルを実行する場合、チャンネル調整が試みられる場合を記録するなど、システムがそれをどう埋め合わせようとするかを見極める必要もある。

このテストは、WIDS/WIPS および不正アクセスポイントに関するエキスパートなスキルが必要とされるため、Advanced としてランク付けされる。

WIDS/WIPS バイパスからシステムが保護されていることを保証する。

WIDS/WIPS バイパスからシステムが保護されていることを保証する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>3 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.2.1.1</td></tr>
<tr><td>入力情報</td><td>車両仕様マニュアル</td></tr>
<tr><td>実施条件</td><td>車両の Wil-Fi を有効にする。</td></tr>
<tr><td>確認事項</td><td>不正アクセスポイントが検出されても、デバイスがそのアクセスポイントにアクセスできない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-01</td><td>セクション 2.1.4</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>WIDS/WIPS は、ホワイトリストに登録されているシステムで、不正アクセスポイントをスキャンし、その対策を試みる。車両が不正アクセスポイントに接続しない場合、WIDS/WIPS の設定を確認し、さらにシステムを攻撃から守るために変更すべきことがないか見極める必要がある。</td></tr>
</table>

6.2.3.12. 認証されていないネットワークアクセスのチェック

項目	記載内容
項目番号	NEDO_WIFI_22
項目名	ワイヤレスインターフェイス経由で V2X、CAN-bus またはバックエンドに影響を及ぼすパスがないかの検証
目的	攻撃者がワイヤレスサービスのコントロールを回避して攻撃する可能性のあるアクセスレベルと車両のセキュリティの上位レベルを特定する。テスト担当者は、ワイヤレスネットワークを他の通信システムへの突破ポイントとして使用した場合の突破の難易度を評価するとともに、そのような攻撃を防ぐ対策すべての有効性を評価する。 このテストは、長い時間をかけ、あるシステムから他のシステムへ許容されていないアクセスを試みるようなエキスパートなネットワークと組込みシステムのスキルを要求するため、必須としてランク付けされる。 通信システムそれぞれが隔離されていることを確認する。 それぞれのインタフェースが異なるインタフェースの攻撃から保護されることを保証する。
実施タイミング	
想定実施工数	1 時間
前提テスト項目	なし
入力情報	なし
実施条件	車両へのシステムレベルのアクセス権がある。
確認事項	その他の外部ネットワークと内部ネットワークがともにワイヤレスネットワーク経由で直接行われる。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除
備考	<table><tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr><tr><td></td><td>TMID-10</td><td>セクション 2.1.1、2.1.3、2.1.4</td><td>N/A</td></tr></table>
故障の影響および修正	CAN-bus および V2X などの通信システムへの突破ポイントとして Wi-Fi アクセスポイントが利用できるとすれば問題となる。ネットワークデバイスは、アクセスポイント同士が直接つながらないようにするなど、互いに切り離す必要がある。

6.2.3.13. 承認されていないデータ探索

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WIFI_23</td></tr>
<tr><td>項目名</td><td>ネットワーク経由で車両からデータを盗み出す方法がないかを検証</td></tr>
<tr><td>目的</td><td>テスト担当者は、攻撃者を装って、インフォテイメントシステムの実行レベルにアクセスする必要がある。アクセスしたら、システムのデータ探索対策として取られている対策を見つけ出し、データの引き出しを試みる。システムへのアクセスは、HTTP または攻撃者が行いそうな荒っぽい方法を発見できるようなやり方で、Web サービスへの不正アクセスの形で行う必要がある。テストのスピードを加速する必要がある場合には、ファームウェアイメージまたはソースコードが提供される場合もある。
このテストは、ネットワークと組込みシステムのエキスパートなスキルを持ち、長期間の作業を要求されることから、必須としてランク付けされる。
システムが侵害されているかどうかを確認し、攻撃者が情報をシステムから漏洩させることは困難であることを確認する。

攻撃者が検出されずに情報を漏洩させることができないことを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>40 時間</td></tr>
<tr><td>前提テスト項目</td><td>車両へのファームウェアレベルのアクセス権がある。</td></tr>
<tr><td>入力情報</td><td>車両仕様マニュアル</td></tr>
<tr><td>実施条件</td><td>1.システムコンポーネントの Wi-Fi をオンする。
2.車両のシェルコマンドを実行するためにアクセスする。</td></tr>
<tr><td>確認事項</td><td>最新のファームウェアを搭載したデバイスから容易にデータを引き出すことができない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-09</td><td>セクション 2.1.1、2.1.2、2.1.3</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>攻撃者が機密データを盗み出せる方法がネットワーク上にあれば、それは深刻な脆弱性となる。システムがデータの取り出しに気づかないままデバイスからデータを引き出せる方法を攻撃者に使わ</td></tr>
</table>

	れないようにするため、車両の保護環境からのデータの取り出しを許可する方法は限定する必要がある。

6.3. V2X （802.11p）

現代の自動車は、専用狭域通信（DSRC）としても知られている Vehicle to Every（V2X）というプロトコルを採用し始めています。経済的な観点から、V2X 技術の潜在需要は巨大です。2016 年、業界ではほとんど利用されていませんが、生産は今後数年で急激に増加すると予想されています。

V2X は、車両とその乗客の安全性を向上させるために設計されており、車両が周辺をより認識し、危険を回避するのに役立つはずのデータを伝達する車両間のメッシュネットワーク通信を可能にすることによって、この優れた技術が達成されます。V2X には、巧みに操って潜在的な危険から車両を遠ざけ、車両の位置を追跡し、事故への反応時間を加速する機能があります。残念ながら、このプロトコルは現在、車両とその乗客の安全性を高めるサービスに悪影響を及ぼす可能性のあるいくつかのセキュリティ上の欠陥があります。これは、適切なツールを使用した攻撃者がエアバッグを「事前展開」し、架空の歩行者を回避して潜在的な危険状況に陥る可能性があることを意味します。

世界各国で適用される規制が異なり、国ごとに異なる車両インフラストラクチャ要件があるため、以下はヨーロッパ（EU）、アメリカ合衆国（USA）、日本の相違点を示している注意事項です。

- **日本**
  日本の V2X は、ARIB と TTA によって参照および管理されています。V2V（車両から車輌）は 700 MHz で動作し、V2E（車両からなんでも、道路など）は 700 Mhz と 5.8 GHz の両方を使用します。日本の DSRC を規制する規格は、ARIB STD-T75、ARIB STD-T88、ITU-R M.1453-2 です。
- USA（802.11p）
  USA の V2X は WAVE と命名され、IEEE-SA から提供されます。NHTSA の要求に対応し、US-V2X に関連する規格は、IEEE 1609.X などの IEEE 規格内で参照されます。USA に関連する SAE 基準は SAE J2735 です。
- EU
  EU の V2X は ITS-GS と呼ばれ、ETSI から提供されます。GeoNework、基本的なトランスポートプロトコル、IPv4 と IPv6 テクノロジを多用しています。USA 規格と EU 標準化文書は同じです。
- **今後の展開**
  VTx はコミュニティ内で、5G とも呼ばれる C-V2X に向かう動きが激しいです。LTE インフラストラクチャとテクノロジーに大きく依存しており、LTE のセキュリティ対策の多くを継承しています。

このセクションの焦点は、全体として V2X の潜在的な弱点を取り上げ、自動車メーカーがこれらの潜在的な問題を保護するために十分な注意を払っているかどうかを判断することです。このフレームワークの目的のために、IEEE 802.11p がこ

れらのテストケースのターゲット環境として選択されました。ただし、802.11 は USA、EU、日本の間で共有されているため、ARIB と TTA（日本）内でのテストは全体的に適用可能でなければなりません。これらのテスト項目の将来の使用に関して、C-V2X は LTE ネットワークインフラストラクチャに大きく依存しているため、本書および V2X（802.11p）のセルラー（LTE）セクションと組み合わせての中で、全体的な車両のカバレッジは同じになります。

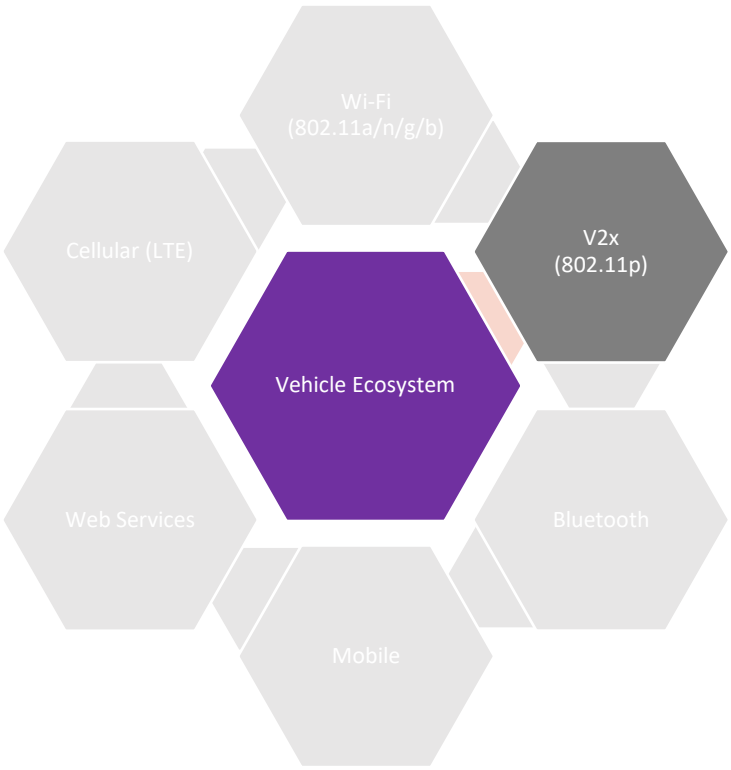


図 6：V2x サブコンポーネントカテゴリーをハイライト

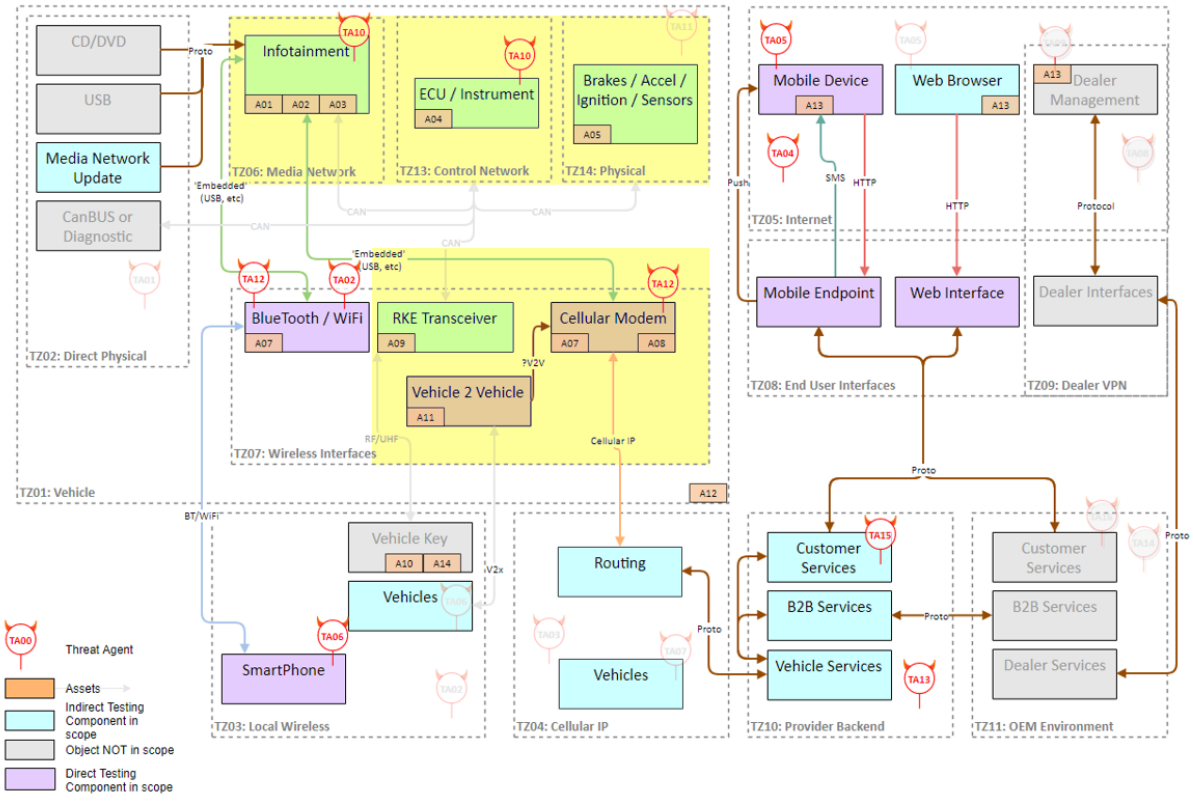


図 7：V2X 範囲内の項目に対する直接的なテストの影響

6.3.1. 必須

6.3.1.1. V2X の存在を特定

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_V2X_1</td></tr>
<tr><td>項目名</td><td>V2X が車両によって使用されているかどうかの確認</td></tr>
<tr><td>目的</td><td>V2X が車両によって使用されているかどうかを確認する。
このテストでは、V2X が正しく動作していることを確認するために必須と評価されている。
V2X が既知で予測可能な状態で動作していることを保証する。
OEM は、脅威サーフェスの完全なカバレッジを保証するためすべての V2X 機能を認識する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>車両仕様マニュアル</td></tr>
<tr><td>実施条件</td><td>なし</td></tr>
<tr><td>確認事項</td><td>メーカーが有効にすると、V2X が検出される。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-11</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>このテストが失敗した場合、メーカーによって報告されたインスタンスがあるとき V2X プロトコルが検出されないことを意味する。</td></tr>
</table>

6.3.1.2. 入力の V2X 順序

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_V2X_2</td></tr>
<tr><td>項目名</td><td>自動車への入力の適切な順序の確認</td></tr>
<tr><td>目的</td><td>車両の安全性に基づいて判断を下す際に、どの入力が優先されるかを確認する。
このテストは、情報に関連する優先順位が自動車によって行われた重要な安全性の決定に影響を及ぼす可能性があるため、必須であると評価されている。
誤った情報によって車両の安全が損なわれないことを確認する。
ハッカーがメッセージだけを変更して AI をクラッシュさせることはできないことを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>5 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.3.1.1</td></tr>
<tr><td>入力情報</td><td>1.車両仕様マニュアル
2.シミュレートされた環境</td></tr>
<tr><td>実施条件</td><td>1.シミュレートされた攻撃者は車両に虚偽の情報を送ることができる。
2.車両センサーは、情報が偽であると判断することができる。</td></tr>
<tr><td>確認事項</td><td>車両は、V2X から得られた情報が環境と一致せず、反応しないことを認識する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-11</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>このテストが失敗した場合、車両が自動車のセンサーからの V2X メッセージを信頼し、ハッキングされる可能性があることを意味する。</td></tr>
</table>

6.3.1.3. V2X 事前展開安全対策

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_V2X_3</td></tr>
<tr><td>項目名</td><td>セーフティ機能の事前展開を制限するセキュリティ対策があるかどうかの特定</td></tr>
<tr><td>目的</td><td>V2X がリモートで引き起こす可能性のある安全上の危険を特定する。
このテストは車両のオペレータの安全に直接影響を及ぼすため、必須であると評価されている。
攻撃者が自由に安全機能を発動できないようにする。
攻撃者が安全機能を使用してユーザーに危害を加えないことを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.3.1.1, 6.3.1.2</td></tr>
<tr><td>入力情報</td><td>1.車両仕様マニュアル
2.シミュレートされた環境</td></tr>
<tr><td>実施条件</td><td>1.シミュレートされた攻撃者は車両に虚偽の情報を送ることができる。
2.車両センサーは、情報が偽であると判断することができる。</td></tr>
<tr><td>確認事項</td><td>車両は、得られた情報が環境と一致せず、安全対策を講じないことを認識する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-14</td><td>セクション 2.1.1</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>このテストが失敗した場合、攻撃者は必要がないときに自動車のエアバッグとシートベルトを開けることができる。</td></tr>
</table>

6.3.1.4. V2X 信号改ざん

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_V2X_4</td></tr>
<tr><td>項目名</td><td>V2X データが制限され、誤ったデータが受信された場合の反応の観察</td></tr>
<tr><td>目的</td><td>誤ったメッセージが受信された後に、V2X が詰まっていることが自動車事故を発生する可能性があるかどうかを確認する。
このテストは、高度な SDR スキルを必要とする一方で、重大な安全関連システムに深刻な影響を与える可能性があるため、必須と評価されている。
メッセージが変更された際に車両がそれを理解できることを確認する。
車両が簡単なメッセージ操作から守られていることを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.3.1.1, 6.3.1.2</td></tr>
<tr><td>入力情報</td><td>1.車両仕様マニュアル
2.シミュレートされた環境</td></tr>
<tr><td>実施条件</td><td>1.シミュレートされた攻撃者は車両に虚偽の情報を送ることができる。
2.車両センサーは、情報が偽であると判断することができる。</td></tr>
<tr><td>確認事項</td><td>車両は、得られた情報がその環境と一致せず、安全対策を展開しないことを認識する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-13</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>このテストが失敗した場合、攻撃者は必要がないときに自動車のエアバッグを開くことができる。</td></tr>
</table>

6.3.1.5. V2X ファイアウォール

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_V2X_5</td></tr>
<tr><td>項目名</td><td>ある自動車が開いているポートを別の自動車でスキャンできるかどうかの確認</td></tr>
<tr><td>目的</td><td>このテストの目的は、1 台の自動車のオープンポートが同じネットワーク上の別の車両にさらされているかどうか、またはセキュリティシステムが正しく動作しているかどうかを判断することである。
このテストは、高度な SDR スキルが必要な一方で、攻撃者によって利用される単純なベクターを暴き出す可能性があるため、必須と評価されている。
システムファイアウォールが正しく配置されていることを確認する。
システムファイアウォールが適切に配置されていることを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.3.1.1, 6.3.1.2</td></tr>
<tr><td>入力情報</td><td>車両仕様マニュアル</td></tr>
<tr><td>実施条件</td><td>1.シミュレートされた攻撃者は車両に虚偽の情報を送ることができる。
2.車両センサーは、情報が偽であると判断することができる。</td></tr>
<tr><td>確認事項</td><td>車両は、他の車両から直接ポートを検出する攻撃をブロックする</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>N/A</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>このテストが失敗した場合は、攻撃者が自動車のセキュリティに弱点を見つける可能性が高く、試行錯誤している可能性が高いことを意味する。</td></tr>
</table>

6.3.1.6. V2X スプーフィング

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_V2X_6</td></tr>
<tr><td>項目名</td><td>V2X は認証を使用せず、これにより、攻撃者は他の車両やデバイスの ID にスプーフィングすることができる。</td></tr>
<tr><td>目的</td><td>スプーフィングした ID を車両が検出するために使用する保護レベルを決定する。
このテストは、SDR スキルが必要とされる一方で、システムによってなされた決定に影響を与え、また車両のセキュリティにも悪影響を与えるため、必須であると評価されている。
偽装されたされたメッセージを受信しているかどうかをシステムが判断できるかを確認する。
偽装された攻撃に対して、システムが耐性があることを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.3.1.1, 6.3.1.2</td></tr>
<tr><td>入力情報</td><td>車両仕様マニュアル</td></tr>
<tr><td>実施条件</td><td>シミュレートされた攻撃者は車両に虚偽の情報を送ることができる。</td></tr>
<tr><td>確認事項</td><td>車両は、送信者が識別された送信者ではないことを認識する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-11</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>このテストが失敗した場合、プロトコルのこの弱点を保護するために、車両にさらに多くの保護機能を組み込む必要があることを意味する。</td></tr>
</table>

6.3.1.7. V2X リプレイ

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_V2X_7</td></tr>
<tr><td>項目名</td><td>V2X プロトコルでは、リプレイに対する適切なセキュリティ制限は適用されない。</td></tr>
<tr><td>目的</td><td>車両によって受信されたリプレイメッセージを得るための努力レベルを決定する。
このテストは、古いデータに基づいてシステムが安全性の判断を下す可能性があるため、必須と評価されている。
再生されたメッセージを受信していることを、システムが判断できるかを確認する。
偽装された攻撃に対して、システムが耐性があることを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.3.1.1, 6.3.1.2</td></tr>
<tr><td>入力情報</td><td>車両仕様マニュアル</td></tr>
<tr><td>実施条件</td><td>シミュレートされた攻撃者は車両に虚偽の情報を送ることができる。</td></tr>
<tr><td>確認事項</td><td>車両は、メッセージが以前にあったことを認識し、無視する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-12</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>このテストが失敗した場合、システムは潜在的に危険な状況につながる可能性のあるリプレイ攻撃に対して脆弱になる可能性がある。</td></tr>
</table>

6.3.1.8. V2X メッセージ操作

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_V2X_8</td></tr>
<tr><td>項目名</td><td>V2X は、アドホック無線メッシュの概念に基づいて設計されたプロトコルです。無線メッセージは一時的に変更される可能性がある。</td></tr>
<tr><td>目的</td><td>メッセージを転送中に変更しても受信されるレベルを特定する。
このテストは、メッセージがアドホックなネットワークを介して偽の情報を伝達し、安全に悪影響を与える可能性があるため、必須であると評価されている。
システムが、注入されたメッセージを受信していることを判断できるかを確認する。
システムが、注入されたメッセージに対して耐性あることを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.3.1.1, 6.3.1.2</td></tr>
<tr><td>入力情報</td><td>車両仕様マニュアル</td></tr>
<tr><td>実施条件</td><td>シミュレートされた攻撃者は車両に虚偽の情報を送ることができる。</td></tr>
<tr><td>確認事項</td><td>車両は、到着する前にメッセージが変更されたことを認識し、無視する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-14</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>このテストが失敗した場合、システムは潜在的に危険な状況につながる恐れのある不正メッセージを受信することに対して脆弱になる可能性がある。</td></tr>
</table>

6.3.1.9. V2X Brute Force

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_V2X_9</td></tr>
<tr><td>項目名</td><td>1 つのデバイスをスプーフィングする能力がある場合、複数のデバイスをスプーフィングする可能性がある。</td></tr>
<tr><td>目的</td><td>偽の渋滞を作り出し、車両に応答させるのに十分なデバイスにスプーフィングすることが可能かどうかを特定する。
このテストは、車両が環境に適切に適用できない状況を作り出す可能性があるため、必須であると評価されている。
システムが、複数の偽装されたシステムに対して耐性があるかを確認する。
システムが、複数の偽装されたシステムに対して耐性があることを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>V2X サービスを使用する必要がある。</td></tr>
<tr><td>入力情報</td><td>車両仕様マニュアル</td></tr>
<tr><td>実施条件</td><td>シミュレートされた攻撃者は車両に虚偽の情報を送ることができる。</td></tr>
<tr><td>確認事項</td><td>車両は、到着する前にメッセージが変更されたことを認識し、無視する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-14</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>このテストが失敗した場合、システムはブルートフォースインスタンス生成攻撃による大量のスプーフィングに対して脆弱になる可能性がある。</td></tr>
</table>

6.3.2. アドバンスド

6.3.2.1. V2X MITM

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_V2X_10</td></tr>
<tr><td>項目名</td><td>メッセージの改ざんや ID のスプーフィングが可能であるため、攻撃者がこのシステムで MITM を作成する可能性がある。</td></tr>
<tr><td>目的</td><td>V2X で ID をスプーフィングするために必要な努力のレベルを判断する。
このテストは、双方向のスプーフィングと、メッセージを操作システムを作成するための知識とツールが必要なため、上級と評価されている。
システムが中間者攻撃に対して安全であることを確認する。
システムが中間者攻撃に対して安全であることを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.3.1.1,6.3.1.6, 6.3.1.8</td></tr>
<tr><td>入力情報</td><td>なし</td></tr>
<tr><td>実施条件</td><td>システムコンポーネントで V2X を有効にする。</td></tr>
<tr><td>確認事項</td><td>V2X ネットワーク上のトラフィックは中間にならない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-14</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>このテストが失敗した場合、システムは潜在的に危険な状況や情報漏えいにつながる可能性のあるリプレイ攻撃に対して脆弱になる可能性がある。</td></tr>
</table>

6.3.2.2. V2X センサー操作

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_V2X_11</td></tr>
<tr><td>項目名</td><td>V2X システムの特徴の 1 つは、長距離運転者が V2X も採用している車両の後ろの位置を自動で追うようにして燃料を節約できるようにすることである。</td></tr>
<tr><td>目的</td><td>攻撃者が車両の位置を変更する可能性のある方法を特定する。
このテストは、センサーに誤った情報を信じるさせるために、車両が使用するセンサーについての詳細な知識をテスターが必要とするため、高度であると評価されている。
システムがセンサーのデータの操作に対して安全かを確認する。
車両の安全性は、センサーのデータを変更しようとする攻撃者の影響を受けないことを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>V2X サービスを使用する必要がある。</td></tr>
<tr><td>入力情報</td><td>車両仕様マニュアル</td></tr>
<tr><td>実施条件</td><td>シミュレートされた攻撃者は車両に虚偽の情報を送ることができる。</td></tr>
<tr><td>確認事項</td><td>車両は、到着する前にメッセージが変更されたことを認識し、無視する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-11</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>このテストが失敗した場合、システムは速度と位置を維持するために車両が使用する値を操作する脆弱性がある。</td></tr>
</table>

6.4. Bluetooth

Bluetooth は、2.4〜2.485 GHz 帯でおよそ 78 チャンネルを使ってスペクトラム拡散を行う、低出力の近距離無線通信用ユニバーサルプロトコルです。最新の車両に装備され、スマートフォンやインフォテイメントシステムとつながるデバイスへの接続に使われています。車両のオーディオシステムに接続し、ハンドル制御とつなげることで、スマートフォンの「ハンズフリー」操作が可能になります。主としてドライバーの利便性を向上させる一方、スマートフォンユーザーであれば誰でも Bluetooth 経由でインフォテイメントシステムに接続できてしまいます。

Bluetooth 技術は、他のワイヤレスプロトコルに比べ、比較的新しいワイヤレス技術です。ますます普及する一方で、初期のいくつかのバージョンには深刻な脆弱性がいくつか見つかっています。Bluetooth LE 4.2 は、現時点で最も安全なバージョンですが、安全性の低いバージョンを使用しているデバイスも依然多くあります。このため、Bluetooth のセキュリティを確認し、他の 2.4GHz デバイスを最新の状態にして然るべきセキュリティを確保する必要があります。Bluetooth セキュリティを評価することで、複数の目的を達成できます。

現在利用可能な Bluetooth のバージョンはいくつもあるため、それぞれの短所を把握しておく必要があります。各バージョンの短所を以下のようにまとめました。

- Bluetooth 4.2 LE
  現在最も安全なプロトコルバージョンです。適切な暗号化が行われているものの、キーストレージやピンジェネレーションなど、実装に不具合がある可能性もあります。
- Bluetooth v4.0〜4.2 LE
  このバージョンにはペアリング盗聴保護機能がなく、MTTM 攻撃に対する保護機能もありません。
  セキュリティモード 1 のレベル 1 の場合には、暗号化などのセキュリティ対策は不要です。
- Bluetooth v2.1〜v3.0
  このバージョンには、スタティックキーを使用するための明らかな問題である、ペアリング盗聴や MTTM 攻撃に対する保護機能がありません。また、セキュリティモード 4 では、接続に問題がある場合、より低いセキュリティ設定にフォールバックする可能性があります。
- Bluetooth v1
  このバージョンのキーは常にスタティックで、再利用されます。セキュリティモード 1 では、セキュリティ対策はありません。また、生成されるピンも非常に短く、適切にランダム化されません。

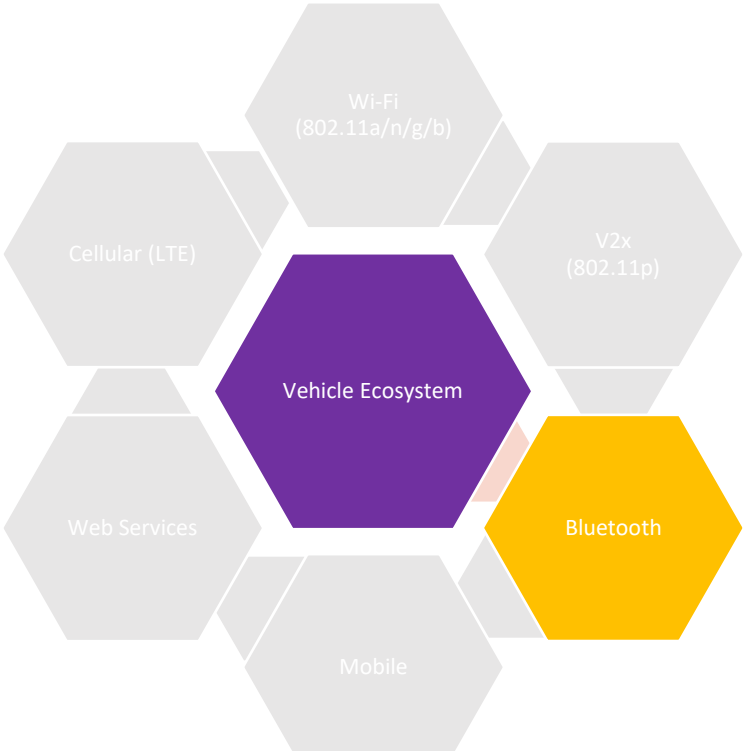


図 8：Bluetooth のサブコンポーネントカテゴリー（黄色ハイライト部）

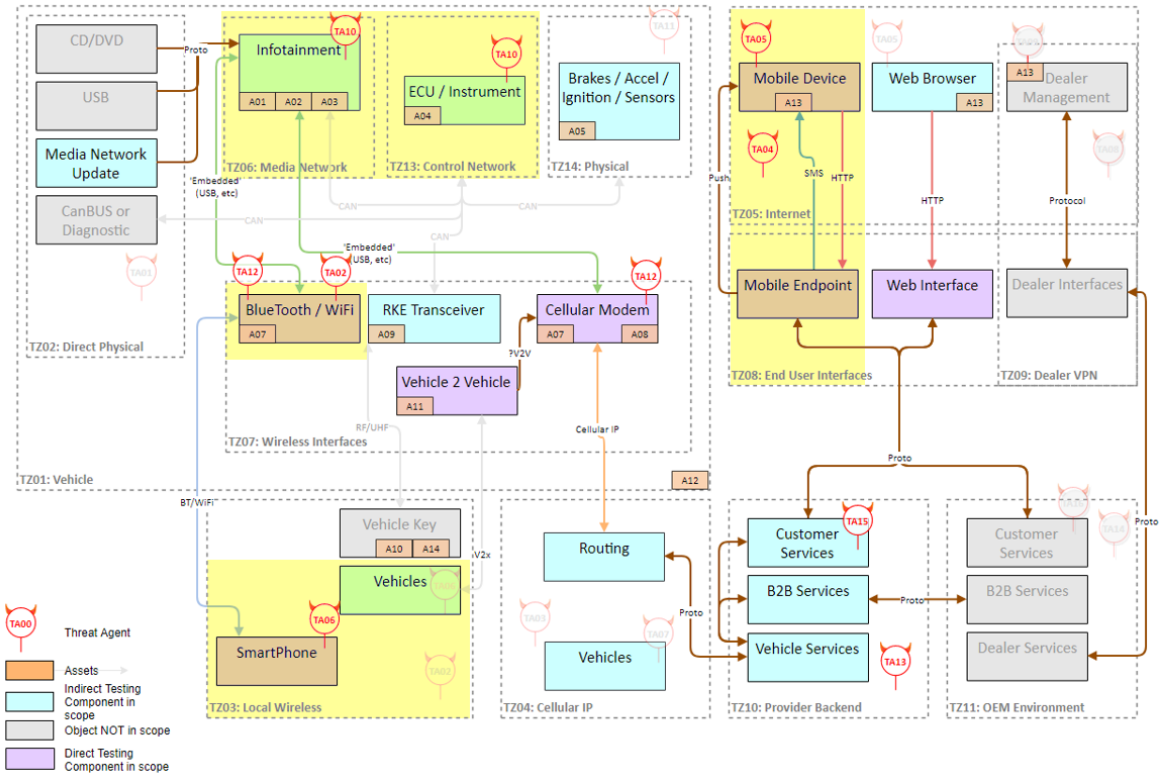


図 9：Bluetooth の対象項目へのテストによる影響

6.4.1. 必須

6.4.1.1. Bluetooth デバイスの特定

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_Bluetooth_1</td></tr>
<tr><td>項目名</td><td>広告 Bluetooth デバイスの特定</td></tr>
<tr><td>目的</td><td>広告 Bluetooth デバイスを特定する。

このテストは、複数のテストに必要な入力であり、Bluetooth が正常に動作しているかどうかを確認するため、必須であると評価される。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>1.車両マニュアル（公的に入手できる場合）
2.Bluetooth デバイスの Mac アドレスおよびブロードキャスト ID</td></tr>
<tr><td>実施条件</td><td>システムコンポーネントが使われている場合には、そのコンポーネントで Bluetooth を有効にする。</td></tr>
<tr><td>確認事項</td><td>Bluetooth がエラーなく各プロファイルに接続される。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-03</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>車両がマニュアルでそのための詳細を表示しない場合、ユニットは正常に機能していない。正しい識別子とプロファイルで応じるよう車両を設定する必要がある。</td></tr>
</table>

6.4.1.2. Bluetooth プロファイルの特定

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_Bluetooth_2</td></tr>
<tr><td>項目名</td><td>広告 Bluetooth のプロファイルの特定</td></tr>
<tr><td>目的</td><td>広告 Bluetooth プロファイルおよびデータタイプを特定する。
このテストは、アドバタイズされたプロファイルが、製造元がアクティブであると信じるプロファイルと一致するかどうかを確認するため、必須であると評価される。
承認されたプロファイルのみがデバイスでサポートされていることを確認する
検証されていない未テストの Bluetooth プロファイルがシステムによってアドバタイズされていないことを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.4.1.1</td></tr>
<tr><td>入力情報</td><td>車両マニュアル（公的に入手できる場合）</td></tr>
<tr><td>実施条件</td><td>システムコンポーネントで Bluetooth を有効にする。</td></tr>
<tr><td>確認事項</td><td>Bluetooth がエラーなく各プロファイルに接続される。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-03</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>このテストが上手くいかない場合、デバイスに必要な機能が欠けているか、追加の機能が有効になっているかのいずれかである。機能の欠如の深刻度によって、デバイスのやり取りが不安定になる可能性がある。追加の機能はたまたま有効になってしまった可能性もあり、セキュリティが適切にテストされていない可能性もある。デバイスは、マニュアルで規定されているプロファイルだけで構成されるよう設定する必要がある。</td></tr>
</table>

6.4.1.3. Bluetooth 実装の脆弱性の特定

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_Bluetooth_3</td></tr>
<tr><td>項目名</td><td>実装の脆弱性の特定</td></tr>
<tr><td>目的</td><td>一覧で示されたプロファイルに脆弱性があるか特定する。
このテストは、実装されたプロファイルに、システムクラッシュやコード実行を引き起こす重大な脆弱性があることを検出するため、必須と評価される。
Bluetooth ドライバの実装に大きな欠陥がないことを確認する
リモートから悪意を持って実行されるような欠陥が Bluetooth のドライバにはないことを証明する</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>2 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.4.1.1, 6.4.1.2</td></tr>
<tr><td>入力情報</td><td>車両マニュアル（公的に入手できる場合）</td></tr>
<tr><td>実施条件</td><td>1.システムコンポーネントが使われている場合には、そのコンポーネントで Bluetooth を有効にする。
2.デバイスへの Defensics のペアリング</td></tr>
<tr><td>確認事項</td><td>A.テスト中、Bluetooth がクラッシュしない。
B.テスト中、Bluetooth がフリーズしない。
C.Defensics テストが失敗しない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-03</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>Defensics は有効な機能やプロトコルが正しく実装されていない領域を確認できる。障害の重大度によって、システムはクラッシュするか、潜在的なバッファオーバーフロー攻撃を受ける可能性がある。ファジングが予期しない動作を引き起こさない場合、ドライバーを検査して動作の原因を特定する必要がある。この検査ではプロファイルに未完成のライブラリ実装がないかを確認したり、他</td></tr>
</table>

	の反応の原因を調べるために、ソースコードの監査や静的解析が必要な場合がある。攻撃者がシステムを攻撃する際に利用する可能性のある脆弱性を防ぐため、すべての予期しない動作は調査し、解決する必要がある。

6.4.1.4. リストにない Bluetooth のプロファイルの特定

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_Bluetooth_4</td></tr>
<tr><td>項目名</td><td>隠れている Bluetooth の機能性を特定する</td></tr>
<tr><td>目的</td><td>Bluetooth デバイスが、完全に実装されておらず、攻撃者が利用する可能性のある脆弱性を持つ可能性がある、リストにない Bluetooth のプロファイルの機能性を保持しているかを確認する。
アドバタイズされていないプロファイルにおいて意図しない活動を検出する可能性があるため、このテストは必須と評価される。これらのプロファイルは、部分的にのみ実装されている可能性があり、システムへの意図しないアクセスを可能にする可能性がある。
アドバタイズされていないプロトコルへの接続がシステムによってサポートされておらず、接続できないことを確認する
未承認の Bluetooth プロファイルがシステムに存在しないことを証明する</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>5 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.4.1.1, 6.4.1.2</td></tr>
<tr><td>入力情報</td><td>車両マニュアル（公的に入手できる場合）</td></tr>
<tr><td>実施条件</td><td>1.システムコンポーネントが使われている場合には、そのコンポーネントで Bluetooth を有効にする。
2.デバイスへの Defensics のペアリング</td></tr>
<tr><td>確認事項</td><td>A.テスト中、Bluetooth がクラッシュしない。
B.テスト中、Bluetooth がフリーズしない。
C.広告プロファイルがまったく通過していない証拠がない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-03</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>Defensics が公表されていないプロファイルに対しテストが合格となる場合、未知のプロトコルに対し少なくとも幾つかの機能が存在すると想定する事が妥当である。これは、ライブラリの再利用、</td></tr>
</table>

	または部分的に移植された機能が原因である可能性がある。ライブラリの実装が完了されない場合は、デバイスは動作または予想不可能な動きをする結果になる可能性がある。

6.4.1.5. 暗号化されてない Bluetooth 通信

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_Bluetooth_5</td></tr>
<tr><td>項目名</td><td>プレーンテキスト通信の使用を識別</td></tr>
<tr><td>目的</td><td>暗号化が Bluetooth 通信を保護するために使用されるかの確認。
このテストでは、Bluetooth 接続によって送信される情報が暗号化されていないことを確認するため、必須と評価される。適切なツールを備えた攻撃者は、Bluetooth 通信の間で、連絡先やその他の情報のような機密情報を車両から復元することができる。
Bluetooth 接続を介して送信された機密データが適切に暗号化されていることを確認する
機密データが媒体に関係なく常に保護されていることを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>2 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.4.1.1, 6.4.1.2</td></tr>
<tr><td>入力情報</td><td>車両マニュアル（公的に入手できる場合）</td></tr>
<tr><td>実施条件</td><td>システムコンポーネントで Bluetooth を有効にする。</td></tr>
<tr><td>確認事項</td><td>Bluetooth がプレーンテキストデータに送信されない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-03</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>暗号化していないプロトコルはリプレイ攻撃につながり、攻撃者はプロトコルをリバースエンジニアリングしその実装における脆弱性を容易に見つけることができる。Bluetooth デバイスは、デバイスで利用可能な最も安全なバージョンを使用する必要がある。可能であれば、車両はデフォルトで暗号化された Bluetooth 5.0 を使用する事を選択する必要がある。Bluetooth 5.0 はセキュアである一</td></tr>
</table>

	方、より古い暗号化されないプロトコルと完全な互換性が維持できない可能性がある。より安全な通信に向けたオプションの選択がある場合は、其れを確認する注意が必要とされる。

6.4.1.6. Bluetooth ペアリングにおける簡単な Pin セキュリティ

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_Bluetooth_6</td></tr>
<tr><td>項目名</td><td>車両とのペアリングに用いる Pin ナンバーの安全性を確認する</td></tr>
<tr><td>目的</td><td>Bluetooth の Pin 成形における脆弱性の特定
予測可能な Pin 番号は Bluetooth セキュリティの重大な脆弱性であるため、このテストは必須と評価されている。 シンプルなピン番号の場合は、攻撃者に接続を許し社内のやり取りを盗聴される可能性がある。
単純なピン攻撃がデバイス上で成功しないことを確認する。
攻撃者が一般的に使用されているピンを推測することによって、匿名でシステムに接続できないことを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>2 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.4.1.1, 6.4.1.2</td></tr>
<tr><td>入力情報</td><td>1. 車両マニュアル（公的に入手できる場合）
2. 最も一般的なピンのリスト</td></tr>
<tr><td>実施条件</td><td>システムコンポーネントで Bluetooth を有効にする。</td></tr>
<tr><td>確認事項</td><td>Pin が予測不可能かつ見地されにくい。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMD-06</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>Pin ナンバーの危殆化は、攻撃者が、一般ユーザーを装って全ての情報と機能にアクセスを行う。
Pin ナンバーは、容易に推測、予見されない保証のために安全にランダムかつ予測不可能なものにする必要がある。</td></tr>
</table>

6.4.2. 推奨

6.4.2.1. Bluetooth における DOS の効果テスト

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_Bluetooth_7</td></tr>
<tr><td>項目名</td><td>車両の DOS 攻撃を処理する能力の確定</td></tr>
<tr><td>目的</td><td>DOS 攻撃による悪影響を特定。
このテストは、高度な Bluetooth テストスキルが必要であり、SDR や gnu ラジオなどの複雑なツールを使用する必要があるため、推奨と評価されている。
Bluetooth 実装が DOS 攻撃に対して安全であることを確認する。
システムが DOS 攻撃に対して耐性があることを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>2 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.4.1.1</td></tr>
<tr><td>入力情報</td><td>車両マニュアル（公的に入手できる場合）</td></tr>
<tr><td>実施条件</td><td>システムコンポーネントで Bluetooth を有効にする。</td></tr>
<tr><td>確認事項</td><td>車両は、一旦 DOS 条件が取り除かれてしまうと悪影響が明確にならない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-05</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>DOS 攻撃は、容易に影響を与えるため一般的とされる。攻撃範囲から車両を単に除く事により攻撃を停止させる事が可能であるため最も脅威のある攻撃とはされない。しかしながら、DOS の十分な保護がなされてない場合、システムに悪影響を与える可能性がある。DOS 攻撃がなされた場合、攻撃が終った後でもシステムが適切に機能するようシステムの強化が必要とされる。</td></tr>
</table>

6.4.2.2. Bluetooth デバイスのスプーフィング

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_Bluetooth_8</td></tr>
<tr><td>項目名</td><td>車両とペアリングする既知のデバイスをスプーフィングしそこから個人情報を抽出</td></tr>
<tr><td>目的</td><td>スプーフィングされた既知のデバイスを介し車両から情報を抽出。
このテストは、高度な Bluetooth テスト技術を必要とし、Bluetooth 中間者攻撃の可能性を実証するため、推奨と評価されている。
Bluetooth の実装がスプーフィング攻撃に対して安全であることを確認する。
システムがスプーフィングの試みに対して耐性があることを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>10 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.4.1.1, 6.4.1.2</td></tr>
<tr><td>入力情報</td><td>車両マニュアル（公的に入手できる場合）</td></tr>
<tr><td>実施条件</td><td>1.システムコンポーネントで Bluetooth を有効にする。
2.セカンダリデバイスを車両とペアリングする。</td></tr>
<tr><td>確認事項</td><td>A.車両は、スプーフィングデバイスと通信しなくなる。
B.車両は、スプーフィングデバイスに機密データを提供しない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-03</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>攻撃者が既知のデバイスにスプーフィングした場合、車両ユーザーに関わる機密情報の抽出同様に車両の通常操作の運転に影響を及ぼすといった可能性がある。車両は、接続、ペアリング時に安全なプロトコルを使用する必要がある。車両はデフォルトで暗号化された Bluetooth 4.2 を使用する事を選択する必要があるが、不可能な場合、Bluetooth が最も安全なバージョンと設定が可能であるかを確認する。一部の旧バージョンの Bluetooth は、デフォルトでは安全ではないが、セキュリティを強化する設定を備えている。</td></tr>
</table>

6.4.2.3. Blueborne

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_Bluetooth_9</td></tr>
<tr><td>項目名</td><td>多くの Bluetooth デバイスが、攻撃者による Bluetooth デバイスのファームウェアイメージを遠隔操作で変更可能とするスタックバッファオーバーフローに対して脆弱性をとる事が確認される。</td></tr>
<tr><td>目的</td><td>Bluetooth の実装の Blueborne 不具合の割合を特定する。

このテストは、スキャナが提供する警告が正確であるかどうかを評価するためのセキュリティ知識と、Bluetooth ファームウェアの操作するための知識を必要とするため、推奨と評価されている。

Bluetooth の実装が BlueBorne の脆弱性から保護されていることを確認する。

システムが BlueBorne の脆弱性の影響を受けていないことを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>0.5 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.4.1.1</td></tr>
<tr><td>入力情報</td><td>1.車両接続の侵入地点（エントリーポイント）方法（前提条件より）
2.車両の Bluetooth 実装を（前提条件より）認識</td></tr>
<tr><td>実施条件</td><td>1.車両は、Bluetooth デバイスとペアリングできる。
2.車両は、Bluetooth デバイスとペアリングしない。</td></tr>
<tr><td>確認事項</td><td>Bluetooth デバイスが Blueborne に対し脆弱性があるかの確認</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-04</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>Blueborne は、一部の Bluetooth チップの脆弱性であり、それにより攻撃者に標的にされた Bluetooth デバイスを知らぬ間に乗っ取られる可能性がある。この脆弱性は、車両のファームウェアではなく Bluetooth チップに存在するためこの問題を解決する前に更新過程にてチップを再プログラムする必要がある。一部の車両においては、システムレベルよりなされ、その他の車両では、チップ自体が直接再プログラムされる必要がある。</td></tr>
</table>

6.4.3. アドバンスド

6.4.3.1. Bluetooth MITM（Man-In-The-Middle attack 中間者攻撃）

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_Bluetooth_10</td></tr>
<tr><td>項目名</td><td>ペアリングメカニズムを標的とする Bluetooth の中間者攻撃</td></tr>
<tr><td>目的</td><td>シミュレートされた攻撃者としてアクティブな高度な侵入テストを実行
このテストは、暗号化の安全性を解除し、Bluetooth 上での中間者攻撃を実行するための、
Bluetooth の専門知識と特別なソフトウェアを必要とするため、高度と評価されている。
Bluetooth 実装が中間者攻撃から保護されていることを確認する。
システムが中間者攻撃攻撃の影響を受けていないことを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>20 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.4.1.1, 6.4.1.2</td></tr>
<tr><td>入力情報</td><td>車両マニュアル（公的に入手できる場合）</td></tr>
<tr><td>実施条件</td><td>1.システムコンポーネントで Bluetooth を有効にする。
2.セカンダリデバイスを車両とペアリングする。</td></tr>
<tr><td>確認事項</td><td>中間者攻撃を作成する方法がない事を確認する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-06</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>Bluetooth 中間者攻撃は、車載にて使用されているデータを考察し変更する機会を与える。中間者攻撃の攻撃は暗号化と Pin ペアリング要求をすり抜ける事が可能である。Bluetooth 中間者攻撃は、適切な Pin 生成によりデバイスが適切に暗号化、保護、ガードされてない場合において可能となる。これら両方の領域は、問題を解決するのに改良されるべきである。</td></tr>
</table>

6.4.3.2. Bluetooth ペアリングにおける高次 Pin セキュリティ

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_Bluetooth_11</td></tr>
<tr><td>項目名</td><td>車両とのペアリングに用いる Pin ナンバーの安全性を確認する</td></tr>
<tr><td>目的</td><td>シュミレーションした攻撃者による行為による Bluetooth の Pin 生成における脆弱性の特定
このテストは、ファームウェアのリバースエンジニアリングや暗号技術の専門家のスキル、ピン番号の生成に関連するエントロピーを決定するための統計的分析を必要とするため、高度と評価されている。
Bluetooth の実装がより高度なペアリング攻撃に対して安全であることを確認する。
より高度なペアリング攻撃に対する耐性があることを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>2 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.4.1.1</td></tr>
<tr><td>入力情報</td><td>車両マニュアル（公的に入手できる場合）</td></tr>
<tr><td>実施条件</td><td>システムコンポーネントで Bluetooth を有効にする。</td></tr>
<tr><td>確認事項</td><td>Pin は、予測不可能で使用可能領域で攻撃者が予測する事が不可能とする。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-05</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>Pin 生成は、予測不可能でなければならない。Pin ナンバーが攻撃者により推測または予測される場合、Bluetooth 通信は攻撃者に容易に狙われる可能性がある。この問題を解決するために Pin ナンバーの生成は可能な限りランダムに近い状態である必要がある。</td></tr>
</table>

6.4.3.3. 車載デバイスへの認証されないアクセス

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_Bluetooth_12</td></tr>
<tr><td>項目名</td><td>Bluetooth デバイスは、車内の多数のデバイスに接続する可能性がある</td></tr>
<tr><td>目的</td><td>車内でのシステムへの無線誘導ポイントとして Bluetooth デバイスの使用が可能かを確認。
このテストは、Bluetooth とそれを実行するシステムを攻撃し、他のサブシステムと他の重要な通信手段にアクセスするために長時間にわたって複数の分野で専門的なスキルを必要とするため、高度と評価されている。
Bluetooth の実装が他の通信システムから分離されていることを確認する。
システムがサンドボックス化され、他の車両システムに直接影響を与えることができないことを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>5 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.4.1.1</td></tr>
<tr><td>入力情報</td><td>車両マニュアル（公的に入手できる場合）</td></tr>
<tr><td>実施条件</td><td>システムコンポーネントで Bluetooth を有効にする。</td></tr>
<tr><td>確認事項</td><td>Bluetooth プロファイルの攻撃で、シミュレートされる攻撃者にデバイスで用いる他のネットワークへのアクセスを許容させない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-04</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>Bluetooth を車両の侵入地点として用いて CAN-bus や V2X を含む車載用システムの全てにアクセスする可能性がある。AT コマンドより車載モデムへアクセスする等メインシステムへの侵入地点が、攻撃者が Bluetooth コントローラから別のシステムに渡る方法がないことを確認する必要がある。</td></tr>
</table>

6.4.3.4. Bluetooth ファームウェア実装のエラー特定

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_Bluetooth_13</td></tr>
<tr><td>項目名</td><td>ドライバーは、実装自体に不具合が存在する可能性がありそれにより攻撃者が Bluetooth の予期しない動作にアクセスする事が可能となる。</td></tr>
<tr><td>目的</td><td>Bluetooth ドライバーがその実装自体に不具合があるかを確認する場合、分析は、広域のファジングまたはドライバーのリバースエンジニアリングが含まれる必要がある。
このテストは、ファジングのテストで発見された脆弱性がなぜ失敗したのか、そしてセキュリティがどの程度影響を受けるのかを発見するための組み込みエンジニアリングとリバースエンジニアリングの専門知識を必要とするため、高度と評価されている。
6.4.1.3 で発見された脆弱性の重大度を判断する。
実装で発見された欠陥を使用して高度な攻撃からシステムを保護することを証明する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>5 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.4.1.1, 6.4.1.2, 6.4.1.3</td></tr>
<tr><td>入力情報</td><td>車両マニュアル（公的に入手できる場合）</td></tr>
<tr><td>実施条件</td><td>システムコンポーネントで Bluetooth を有効にする。</td></tr>
<tr><td>確認事項</td><td>Bluetooth ドライバーは、機能停止または予想不可能な方向に反応してはならない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-07</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>攻撃者が、インフォテインメントシステムのシステムレベルにアクセスする事が可能になるインフォテインメントのクラッシュより何でもする事が可能となる脆弱性へアクセスする可能性がある。全てのファームウェアは、システムがクラッシュしたり異常なパケットにより脆弱性を露呈がされる事がないように検査する必要がある。</td></tr>
</table>

6.5. モバイル

モバイルアプリケーションおよびデバイスが、車両に関するデータまたは機能へのアクセスを提供するために使用されることが増えています。これには、デバイス自身の公開または配置されているデータや機能、または車両やメーカーに関連するバックエンドコンポーネントや Web サービスとの通信が含まれます。これらのアプリケーションは、Bluetooth、Wifi、セルラーネットワークなどのモバイルデバイスによって提供される多数のインターフェイスを活用することも、さらにさまざまな形態のネットワーク接続を使用して、車両データへのアクセスや機能を活用することもできます。この強力な組み合わせにより、開発者と消費者にアプリケーションを展開して使用できる多種多様なフォームを提供します。この柔軟性の向上により、悪意のあるエージェントがアプリケーション機能を中断して干渉する可能性のある新しい攻撃ベクトルのセットが導入されます。

アプリケーションデータの公開やその操作による改ざんは、機密データの盗難から車両の重要な機能障害に至るまで、車両と乗客の両方に大きな影響を及ぼします。したがって、これらのアプリケーションが意図したとおりに機能して、可能な限り攻撃ベクトルを減少することが不可欠です。

このセクションでは、車両または組み込みアプリケーションが利用する Web サービスのセキュリティ状態を評価する方法を示します。このプロセスでは、一般的な攻撃パターンに対するサービスの耐性を含むサービスの全体的なセキュリティの姿勢を評価し、悪意のあるユーザーによって悪用される可能性のある内部または外部インターフェイスの脆弱な領域を特定します。これらの領域には、以下の試験が含まれます。

1. バイナリレベルの保護
2. クライアント側のコントロール
3. デバイスの誤設定
4. 暗号機能
5. 通信/ネットワークレイヤの問題
6. 情報開示/漏洩
7. ビジネス/アプリケーションロジックの欠陥

モバイルデバイスやアプリケーションのテストでは、目的とする操作を実行する能力を改ざんするか、さもなければ混乱させることを意図する装置やアプリケーションの目的とする機能に関する知識を活用するために、デバッガやコード解析ツールからトラフィックプロキシへのさまざまなツールを利用する必要があります。本書には、車両システムで使用されるすべてのモバイルアプリケーションに対して実行する必要があるセキュリティチェックリストと、デバイスとアプリケーションのセキュリティをさらに向上させる高度な技術が含まれています。

追加の Web サービスチェックは、デバイスまたはアプリケーションが通信する Web サービスコンポーネントの性質上、モバイルデバイスおよびアプリケーションのテストと連携して行う必要もあることに注意する必要があります。

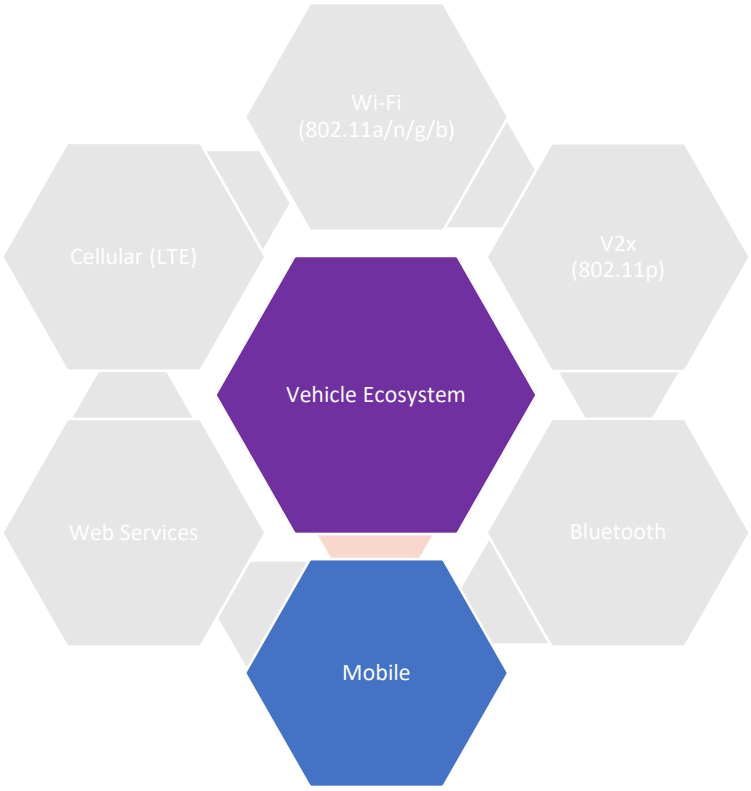


図 10：モバイルサブコンポーネントカテゴリーをハイライト

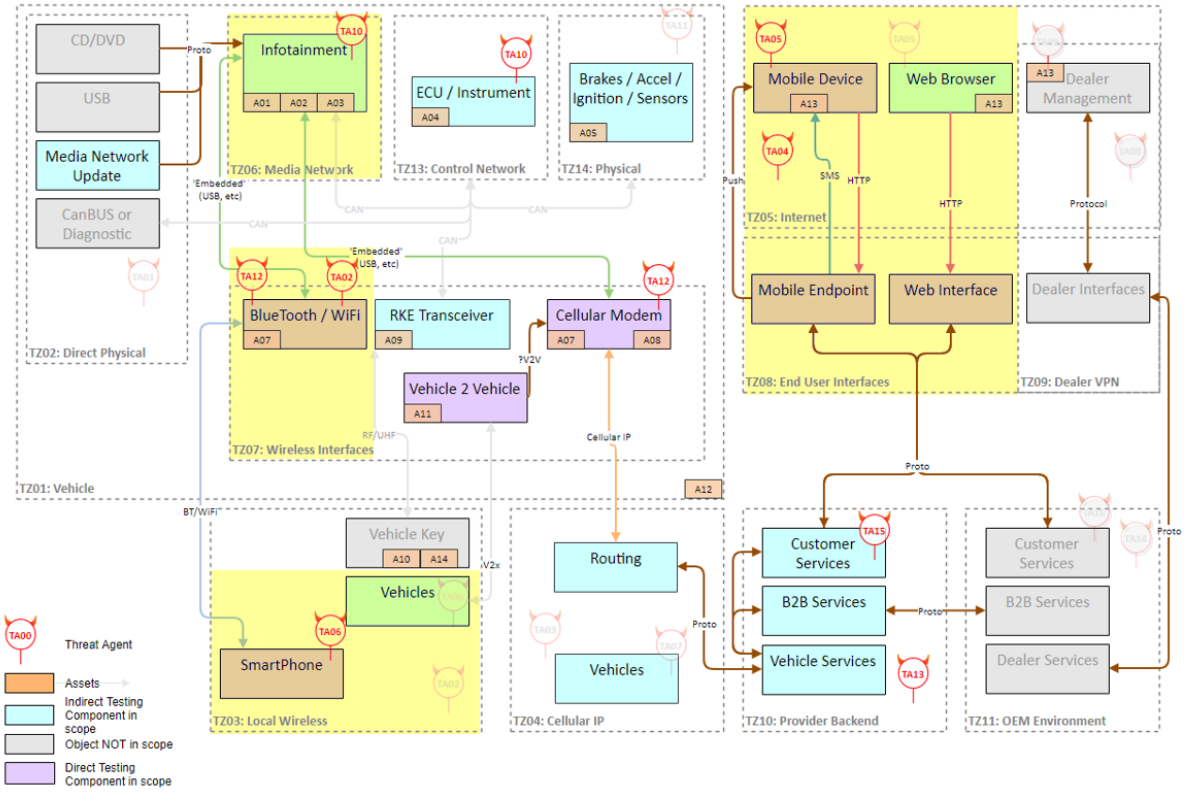


図 11：モバイル範囲内の項目に対する直接的なテストの影響

6.5.1. 必須

6.5.1.1. 機密フィールドのコピー＆ペースト

項目	記載内容
項目番号	NEDO_MOBILE_1
項目名	機密データフィールドのコピー＆ペーストをチェック
目的	許可されていないユーザーまたはアプリケーションがこの情報を入手できる可能性があるため、一般的なクリップボードに機密情報を平文で記載しない。
実施タイミング	
想定実施工数	0.5 時間
前提テスト項目	なし
入力情報	有効なアプリケーションの認証情報
実施条件	アプリケーションに機密フィールドが含まれている。
確認事項	アプリケーションは他のアプリケーションにコピー＆ペースト機能を許可しない。 または、アプリケーションに機密データフィールドがない。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除
備考	ツール: モバイルデバイス / BSM #: TMID-16 / 車両#：: N/A / 関連する攻撃: N/A
故障の影響および修正	アプリケーションが機密データのコピー＆ペーストを許可している場合、ユーザーがコピーしてはならないバッファに情報を間違ってコピーしてしまう可能性がある。コピー＆ペーストは、アプリケーションのすべての機密エリアから無効にする必要がある。

6.5.1.2. コンパイラの設定チェック - 開発

項目	記載内容
項目番号	NEDO_MOBILE_2
項目名	アプリケーションのコンパイル時に適切なセキュリティフラグが設定されていることの確認
目的	コンパイル時にセキュリティフラグを設定しないと、バッファオーバーフローなどの脆弱性をもたらす可能性がある。これらの設定のほとんどはデフォルトでオンになっており、開発者が明示的に無効にする必要がある。
実施タイミング	
想定実施工数	1 時間
前提テスト項目	なし
入力情報	アプリケーション構築プロセスへのアクセス、またはアプリケーションコンパイラ設定へのアクセス。 モバイルアプリケーションの安全なコンパイラ設定のリスト
実施条件	なし
確認事項	アプリケーションが適切なコンパイラ設定でコンパイルされている。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除

	公開用資料のため、記載内容を削除
備考	<table><tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr><tr><td></td><td>TMID-16</td><td>セクション 2.1.3</td><td>N/A</td></tr></table>
故障の影響および修正	適切なコンパイラ設定が有効になっていないと、攻撃者が悪用できる弱点が存在する可能性がある。以下は、アプリケーションを構築するときに設定する必要がある基本的なコンパイラ設定である。 公開用資料のため、記載内容を削除

6.5.1.3. コンパイラの設定チェック - プロダクション

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_3</td></tr>
<tr><td>項目名</td><td>コンパイル時にセキュリティフラグを設定しないと、バッファオーバーフローなどの脆弱性が導入される可能性がある。</td></tr>
<tr><td>目的</td><td>アプリケーションのコンパイル時に適切なセキュリティフラグが設定されていることを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>0.5 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>アプリケーションバイナリ</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>アプリケーションが適切なコンパイラ設定でコンパイルされている。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>その他のモバイル静的解析ツール</td><td>TMID-16</td><td>セクション 2.1.3</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>適切なコンパイラ設定が有効になっていないと、攻撃者が悪用できる弱点が存在する可能性がある。以下は、アプリケーションを構築するときに設定する必要がある基本的なコンパイラ設定である。

公開用資料のため、記載内容を削除</td></tr>
</table>

	公開用資料のため、記載内容を削除

6.5.1.4. アプリエンタイトルメント/権限チェック

項目	記載内容
項目番号	NEDO_MOBILE_4
項目名	アプリケーションが不要な権限または安全でない権限を要求しているかどうかを確認する。
目的	アプリケーションが要求するすべての権限がビジネス機能に必要であり、危険な権限が回避されていることを確認する。
実施タイミング	
想定実施工数	1 時間
前提テスト項目	なし
入力情報	Android マニフェストファイル
実施条件	なし
確認事項	アプリケーションが悪いものを拒否する。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除

<table>
<tr><td></td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>テキストエディタ</td><td>TMID-16</td><td>セクション 2.1.3</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>アプリケーションが実際に要求する危険な権限を実際に使用していなくても、攻撃者が（1）コードを注入するか、（2）被害者アプリケーションを特権のある権限を使って騙すことができれば、攻撃者コードは被害者アプリケーションをプロキシとして悪用することにより、基本特権機能に効果的にアクセスする。後者の場合は、権限再昇格攻撃と呼ばれることもある。アプリケーションで本当に識別された権限が必要かどうかを判断する。そうでない場合は、アプリケーションの[AndroidManifest.xml]ファイルからそれらを削除する。</td></tr>
</table>

6.5.1.5. ハードコードされた機密情報

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_5</td></tr>
<tr><td>項目名</td><td>車両エコシステムのソースファイルでハードコードされた機密を確認します。</td></tr>
<tr><td>目的</td><td>機密情報がアプリケーションソースコードの検査によって公開されていないことの確認。アプリケーションバイナリは、ハードコードされた文字列の形式で、アクセス認証情報または暗号化キーを含む機密情報を頻繁に公開する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>１時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>1. アプリケーションソースコード
2. 関連する機密リスト</td></tr>
<tr><td>実施条件</td><td>なし</td></tr>
<tr><td>確認事項</td><td>アプリケーションバイナリが、ハードコードされた文字列によって機密情報を公開しない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>アプリケーションソースコード</td><td>TMID-16</td><td>セクション 2.1.3</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>この影響は、公開されるデータによって異なりますが、まだテスト中の可能性のあるリソースやエンドユーザー向けではない機能への本番用またはリソース用ではない情報へのアクセスや、認証情報や暗号化キー/プロセスへのアクセスが含まれる。機密データの暴露を避けるために有効なバイナリハード技術が適用されていることを確認する。</td></tr>
</table>

6.5.1.6. カスタムキーボード無効

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_6</td></tr>
<tr><td>項目名</td><td>車両エコシステムのカスタムキーボードが無効になっていることの確認</td></tr>
<tr><td>目的</td><td>カスタムキーボードを使用しないようにアプリケーションが設定されていることの確認。カスタムキーボードがユーザーのキーストローク/データを攻撃者に公開する可能性がある。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>0.5 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>iOS デバイス/アプリケーション</td></tr>
<tr><td>確認事項</td><td>アプリケーションが、機密入力にカスタムキーボードを使用することを防止する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>カスタムキーボード</td><td>TMID-16</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>カスタムキーボードは、リモートシステムへのネットワークアクセスによって被害者のキー入力情報を送信できる可能性がある。アプリケーションは、カスタムキーボード拡張の使用を明示的に防止するように構成する必要がある。これは、適切な Application Delegate API メソッドから[No]を返すことによって実行する。</td></tr>
</table>

6.5.1.7. デバッグ防止 - 開発

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_7</td></tr>
<tr><td>項目名</td><td>開発中のアプリケーション構成のデフォルトにデバッグ防止メカニズムがあるかの確認</td></tr>
<tr><td>目的</td><td>アプリケーションが適切なデバッグ防止メカニズムで構成されていることを確認する。デバッグ防止の欠如は、攻撃者がセキュリティコントロールをバイパスしたり、機密データをメモリから読み取ったりできる可能性を高める。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>0.5 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>1. アプリケーションマニフェスト（Android）
2. アプリケーションソースコードまたはアプリケーションビルドプロセスへのアクセス（iOS）</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>アプリケーションがデバッグを困難にする適切な設定を使用している。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>テキストエディタ</td><td>TMID-16</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>デバイスに物理的にアクセスする攻撃者やデバイス上で実行されている他のアプリケーションは、デバッグ可能なアプリケーションを完全に制御できる。これにより、いくつかの攻撃が可能となる。クロスプラットフォーム開発フレームワークを使用してアプリケーションを構築する場合は、フレームワークのドキュメントを参照して、デバッグ可能属性を無効にする方法を決定する。</td></tr>
</table>

6.5.1.8. ローカル認証ブルートフォース攻撃

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_8</td></tr>
<tr><td>項目名</td><td>アプリケーションが繰り返しログイン試行を遅くしたり停止したりするのを確認する。</td></tr>
<tr><td>目的</td><td>クライアント側の認証 PIN またはパスワードがブルートフォース攻撃されないことを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>0.5 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>アプリケーションがローカル認証をサポートしている。</td></tr>
<tr><td>確認事項</td><td>アプリケーションがタイムアウト期間を開始する、ロックアウトする、またはクライアント側のログイン試行が繰り返し失敗した後に別の認証方法が必要になる。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-16</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>ブルートフォース攻撃パスワードの推測により、攻撃者は有効なユーザーアカウントにアクセスできる。有効なユーザーアカウントの認証情報が見つかると、攻撃者は機密情報とすべての機能を含め、これらのアカウントに完全にアクセスする。アプリケーションは、攻撃の速度を低下させ、失敗を記録するという組み合わせによって、推測の繰り返しを抑止する必要がある。</td></tr>
</table>

6.5.1.9. バックグラウンドアプリケーション再開後の再認証

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_9</td></tr>
<tr><td>項目名</td><td>バックグラウンドのモバイルアプリケーションが再開された後、車両エコシステムに認証が必要であることの確認</td></tr>
<tr><td>目的</td><td>機密データや機能を含むアプリケーションは、フォアグラウンドを終了するときにユーザーのセッションを無効にする必要がある。バックグラウンドアプリケーションが再開された後再認証が欠けていると、デバイスに物理的にアクセスしている攻撃者が、非アクティブなアプリケーションを再開することによって、認証および許可の制御を迂回することを可能にする。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>0.5 時間</td></tr>
<tr><td>前提テスト項目</td><td>NEDO_MOBILE_ADVANCED_7 – 証明書のピンニングバイパス（または証明書のピンニングが無効なアプリケーションバイナリ）</td></tr>
<tr><td>入力情報</td><td>1.アプリケーションバイナリ
2.有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>アプリケーションがローカル認証をサポートしている。</td></tr>
<tr><td>確認事項</td><td>A.アプリケーションがバックグラウンドからアクティブ状態に移行するときに再認証が必要。
B.アプリケーションは、バックグラウンドに送信されたときに現在のセッションを無効にする（セッションもサーバー側を無効にする必要がある）</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-16</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>デバイスへの物理アクセスを持つ攻撃者は、バックグラウンド再開後にアプリケーションへの認証アクセスを取得できる。これにより、被害者のセッションに対する完全な認証バイパスが行われ、</td></tr>
</table>

	クライアントアプリケーションに格納されている機密情報をハッキングしたり、被害者の代わりに不正な操作を実行したりすることができる。アプリケーションは、フォアグラウンドに入るたびにユーザーに認証を強制する必要があります。バックグラウンドに入ると、アプリケーションはクライアントとサーバーの両方でセッションを無効にする必要がある。

6.5.1.10. 機密データのログ書き込みの禁止

項目	記載内容
項目番号	NEDO_MOBILE_10
項目名	アプリケーションは、機密データをシステムログに書き込んで、システムログを攻撃者に公開する可能性がある。
目的	アプリケーションは、機密情報、アプリケーションロジック、およびユーザーの個人識別情報（PII）などのシステムログに書き込まれたデータを公開する可能性がある。
実施タイミング	
想定実施工数	1 時間
前提テスト項目	なし
入力情報	1.有効なアプリケーションの認証情報 2.アプリケーションソースコード
実施条件	なし
確認事項	機密情報（アプリケーションの内部プロセスおよびエンドユーザーデータに関連するデータを含む）は、システムログに記録してはならない。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除

	公開用資料のため、記載内容を削除
備考	<table><tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr><tr><td></td><td>TMID-16</td><td>セクション 2.1.5, 2.1.6</td><td>N/A</td></tr></table>
故障の影響および修正	機密情報のログ記録により、デバイスにアクセスするすべてのユーザーは、機密情報を修復することができる。リリースビルド版のアプリケーションでは、いかなるタイプの機密情報もシステムログに保存してはならない。アプリケーションのログにはアプリケーションに関する限定的な情報だけを含み、常に同様の構成を保つようにする。エンドユーザーが直接使用できないシステムログには情報を保存しないようにする。

6.5.1.11. ジェイルブレイク/ルート化検出

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_11</td></tr>
<tr><td>項目名</td><td>ジェイルブレイク/ルート化検出のチェック</td></tr>
<tr><td>目的</td><td>アプリケーションが適切なメカニズムを採用してデバイスの状態をチェックし、ジェイルブレイクやルート化が検出された環境にデプロイされていないかを判断できるかどうかを検証する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>0.5 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>1.アプリケーションバイナリ
2.ルート化またはジェイルブレイクされたモバイルデバイス</td></tr>
<tr><td>実施条件</td><td>アプリケーションにジェイルブレイク/ルート化検出機能を採用する必要がある場合、またはそれを試みる場合、こういったメカニズムがその効果を確保できるか確認する必要がある。</td></tr>
<tr><td>確認事項</td><td>アプリケーションが、ジェイルブレイク/ルート化されたデバイス内部へのデプロイの試みを検出すること。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>ジェイルブレイク/ルート化されたモバイルデバイス</td><td>TMID-16</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>ジェイルブレイクされたデバイスは、攻撃者がアプリケーションによって完全な制御権を得ることができる。そうして数種類の攻撃が可能となる。ジェイルブレイク検出を採用して、ジェイルブレイクされたシステムでの実行を防がなければならない。</td></tr>
</table>

6.5.1.12. 証明書の検証

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_12</td></tr>
<tr><td>項目名</td><td>アプリケーションが証明書の検証を無効化するかどうかの決定</td></tr>
<tr><td>目的</td><td>証明書の検証をデバイスがデフォルトで行う。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>1.アクティブなインターネット接続
2.このアプリケーションが HTTPS 接続で機密データを通信すること。</td></tr>
<tr><td>確認事項</td><td>このアプリケーションが x509 証明書を正確に検証すること。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-16</td><td>セクション 2.1.3</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>証明書の検証が無効化されている場合、アプリケーションは接続しているサーバーを認証しない。よって、攻撃者はネットワーク層を使って攻撃し、対象とするデバイスのアプリケーションを使って自分のサーバーに接続し、ユーザーの認証情報を盗み出し、アプリケーションに有害なデータを供給し、さらに関連する攻撃を仕掛ける。プラットフォームが提供するデフォルトの証明書検証機能をバイパスしてはならない。デフォルトでは提供されていないチェックの追加（例えば証明書のピンニングの実行など）は許容されるが、デフォルトチェックをバイパスしてはならない。デフォルトの証明書検証ロジックを変更する場合は、セキュリティ評価の一部として全面的にレビューし、意図しない副次的影響を及ぼさないことを確認しなければならない。</td></tr>
</table>

6.5.1.13. 証明書のピンニング

項目	記載内容
項目番号	NEDO_MOBILE_13
項目名	アプリケーションが証明書のピンニングを使用するかどうかの判断。証明書のピンニングとは、第三者の認証局に頼らず、ホストを想定される x509 証明書または公開鍵に関連付けるプロセスである。
目的	証明書のピンニングを行わない場合、アプリケーションはデバイスが信用する証明書をすべて受け入れてしまい、攻撃者がユーザーの認証情報やその他の機密情報を使って、暗号化した信号を傍受したり改ざんしたりできる場合があり、それについて検証を行う。
実施タイミング	
想定実施工数	1 時間
前提テスト項目	なし
入力情報	有効なアプリケーションの認証情報
実施条件	1.アクティブなインターネット接続 2.このアプリケーションが HTTPS 接続で機密データを通信すること。
確認事項	アプリケーションが証明書のピンニングを採用していて、攻撃者が機密の通信を傍受することを防いでいること。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除
備考	ツール / BSM # / 車両#： / 関連する攻撃

		TMID-16	セクション 2.1.3	N/A
故障の影響および修正	証明書のピンニングを行わない場合、攻撃者が自身が管理する公開鍵を導入することができる。攻撃者が信頼される証明書によって署名された公開鍵/秘密鍵のペアを取得できる場合、または新しい証明書を許容するようにユーザーをだませる場合、攻撃者はこの脆弱性を利用してユーザーに対して中間者攻撃（MITM）をかけ、平文でのパスワードやその他の機密情報を含む全ネットワークトラフィックを傍受したり改ざんしたりできるようになる。証明書ピンニングを採用してチャンネルを保護しなければならない。さらにコード難読化も併用して一層保護を強化するべきである。			

6.5.1.14. バイナリ難読化 - 展開

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_14</td></tr>
<tr><td>項目名</td><td>アプリケーションが難読化されているかのチェック</td></tr>
<tr><td>目的</td><td>攻撃者がアプリケーションをリバースエンジニアリングしにくいようにする。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>0.5 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>アプリケーションソースコードまたはビルドプロセスへのアクセス</td></tr>
<tr><td>実施条件</td><td>アプリケーションバイナリに機密のビジネスロジック、極秘事項、知的財産が含まれている。</td></tr>
<tr><td>確認事項</td><td>アプリケーションバイナリが簡単に判読可能なコードに変換できない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>IDE または
テキストエディタ</td><td>TMID-16</td><td>セクション 2.1.2</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>バイナリ難読化を行わないと、攻撃者にとって、アプリケーションのリバースエンジニアリングが比較的容易となる。コードの機密部分についてはアプリケーションに難読化を施して、攻撃者がリバースエンジニアリングをしにくいようにするべきである。Android 用には、簡単にネイティブコードを難読化する多くのオープンソースおよび商用製品がある。暗号作成、ルート化検出、証明書ピンニングのような非常に機密度の高い操作部分に関しては、NDK で C. C obfuscator を使って書き直すと、逆コンパイルしやすい Java よりもより安全である。</td></tr>
</table>

6.5.1.15. 情報漏洩

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_15</td></tr>
<tr><td>項目名</td><td>URL クエリ文字列でのリクエストや安全ではない HTTP メソッドの使用によって、機密情報が漏洩しないことの検証</td></tr>
<tr><td>目的</td><td>安全に使用できる HTTPS を含むバックエンド通信において、デバイスの通信により機密データが漏洩する可能性がある。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.5.1.13</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>A.機密データが URL クエリ文字列で送信されていない。
B.機密データが GET HTTP メソッドを使って送信されていない（機密データは安全なチャンネルで、POST メソッドを使って通信されなければならない。）</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-16</td><td>セクション 2.1.5</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>アプリケーションが送信する機密データには、個人を特定できる情報（PII）が含まれる場合がある。機密データは適度に安全な SSL/TLS チャンネルで、HTTP POST メソッドを使って、リクエストのボディ部分でのみ通信しなければならず、URL クエリ文字列や GET HTTP メソッドに含まれてはならない。</td></tr>
</table>

6.5.1.16. アプリケーションのバックアップ許可

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_16</td></tr>
<tr><td>項目名</td><td>アプリケーションがデータをバックアップし、他のデバイスで修復することが許可されるよう構成されているかのチェック</td></tr>
<tr><td>目的</td><td>バックアップが許可されている場合、攻撃者はアプリケーションがローカル環境に保存しているデータを、デバイスの「ルート」にアクセスせずに閲覧したり改変したりできる可能性がある。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>0.5 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>アプリケーションマニフェスト</td></tr>
<tr><td>実施条件</td><td>1.Android 上でアプリケーションが実行する。
2.アプリケーションがアプリケーションディレクトリに機密情報を収容できる。</td></tr>
<tr><td>確認事項</td><td>アプリケーションがアプリケーションディレクトリに機密情報を持たない、またはアプリケーションがバックアップを許可しない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>テキストエディタ</td><td>TMID-16</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>アプリケーションが保存したデータはローカル PC や SD カード、クラウドサービスにバックアップでき、かつ他のデバイスに修復できる。攻撃者はユーザーのデバイスにバックアップを開始でき、また幾つかの方法でユーザーの既存のバックアップにアクセスできる。アプリケーションのバックアップを無効化するには、アプリケーションの AndroidManifest.xml ファイル内で、<application>エレメントの"android:allowBackup"属性を"false"に設定しする。属性を省略すると、Android はデフォルトでバックアップを許可します。詳細は、
http://developer.android.com/guide/topics/manifest/application-element.html を参照。</td></tr>
</table>

6.5.2. 推奨

6.5.2.1. サードパーティのライブラリチェック

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_17</td></tr>
<tr><td>項目名</td><td>アプリケーションが使用するサードパーティのライブラリが、既知の脆弱性をもたらさないことの検証</td></tr>
<tr><td>目的</td><td>アプリケーションが使用するサードパーティのライブラリをチェックして、そのライブラリが公表されている既知の脆弱性を持っていたり誘発しないことを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>2 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>アプリケーションソースコードまたはアプリケーションバイナリ</td></tr>
<tr><td>実施条件</td><td>アプリケーションがサードパーティのライブラリまたはフレームワークを使用する。</td></tr>
<tr><td>確認事項</td><td>アプリケーションが使用するサードパーティのライブラリが、公表されている既知の脆弱性を持っていない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>静的解析ツール</td><td>TMID-16</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>このテストに合格できない場合、サードパーティのライブラリに既知の弱点がある。アプリケーションは、使用するサードパーティのライブラリに存在する脆弱性を受け継ぐ。アプリケーションが使用するサードパーティのライブラリを最新版に更新して、入手可能な最新のパッチを適用するか、または被害を軽減する方法を見つける。</td></tr>
</table>

6.5.2.2. 暗号化チェック

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_18</td></tr>
<tr><td>項目名</td><td>アプリケーションが使用する暗号化の実装が目的にかない、適切に実装されていることの検証</td></tr>
<tr><td>目的</td><td>安全ではない暗号化の実装、機能、アルゴリズムは既知の攻撃に対して脆弱だったり、また弱点を継承して使用に適さない可能性があるのでその点を検証する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>アプリケーションバイナリを逆コンパイルしたコードまたはアプリケーションのソースコード</td></tr>
<tr><td>実施条件</td><td>アプリケーションが暗号化操作を行う。</td></tr>
<tr><td>確認事項</td><td>アプリケーションが最新の暗号化アルゴリズム/機能を安全に実装している。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>IDE またはテキストエディタ</td><td>TMID-16</td><td>セクション
2.1.3、2.1.6、2.1.2</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>暗号化のチェックに問題があれば、攻撃者のチェックへの侵入が容易となる。暗号化機能を更新して、AES や SHA-2+ファミリーのハッシュ関数のような 128 ビット以上のブロック長を持つ安全なアルゴリズムによる最新の実装を使用する。</td></tr>
</table>

6.5.2.3. アプリケーション通信チャンネルのセキュリティテスト

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_19</td></tr>
<tr><td>項目名</td><td>デバイスの通信が安全なチャンネルで行われて、機密データの漏洩が起こらないことの検証</td></tr>
<tr><td>目的</td><td>デバイスとサーバーの通信は、暗号化された HTTPS 接続のような、適切に構成された安全な伝達手段で行われていなければならず、かつ、必要に応じて例えば FTP より SFTP を使うといった、それ以外の暗号化された適切なバージョンを使用しなければならない。その点を検証する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>1.アプリケーションソースコード
2.有効なアプリケーションの認証情報
3.証明書のピンニングの無効化</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>A.デバイスが、通信の発生の特質に合った、適切に安全な通信手段を使用している。例えば、HTTPS と SFTP など。
B.アプリケーションが最新の安全なプロトコル標準を使用して通信を開始している。
C.サーバー側のエンドポイントが安全な SSL/TLS 接続を実行するよう構成されている。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>IDE またはテキストエディタ</td><td>TMID-16</td><td>セクション 2.1.1、2.1.3</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>安全ではない/暗号化していないチャンネルでの通信の発生は、攻撃者によって盗聴され改ざんされる。アプリケーションコードを監査して、確立している接続/通信で使用されているメソッドが、最新で安全なプロトコル標準を使用していることを確認しなければならない。サーバー上で一度 HTTPS が有効化されると、HTTPS 接続だけが許容されることを確認することが最初のタスクとなる。ユーザーが HTTP でアプリケーションのいずれかの部分にナビゲートしようと試みる場合、アプリケーションはそのユーザーをアプリケーションの HTTPS ポートにリダイレクトする必要がある。次のタスクは、セッション ID の設定時に常に安全な Cookie の属性を設定することです。安全な属</td></tr>
</table>

	性はユーザーのブラウザに、Cookie が暗号化したチャンネルにだけ供給されなければならないことを通知する。アプリケーションが Cookie の属性の設定に失敗し、ユーザーが誤って HTTP 版のアプリケーションにナビゲートした場合、ネットワークを盗聴している攻撃者はやはりユーザーのセッション ID を得ることができる。

6.5.3. アドバンスド

6.5.3.1. コマンドインジェクション

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_20</td></tr>
<tr><td>項目名</td><td>潜在的な危険性をはらむ機能/コマンドインジェクションの可能性のあるインスタンスを識別</td></tr>
<tr><td>目的</td><td>コマンドインジェクションは、ユーザーがどのように特定の OS コマンドを実行するのかを変更させたり、サーバーが実行する完全に新しいコマンドを挿入できるようにして、ユーザーにターゲットとするシステムのある程度のレベルの制御権を与える。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>0.5 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>アプリケーションソースコード</td></tr>
<tr><td>実施条件</td><td>なし</td></tr>
<tr><td>確認事項</td><td>アプリケーションが exec()、popen()、system()といった関数を持たない、またはコマンドがパラメータを定義したユーザー入力を持たない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>IDE 検索ツールまたは grep</td><td>TMID-16</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>攻撃者はコマンドインジェクションを利用して、どのように脆弱なコマンドが実行されるかを変更させたり、または新しいコマンドを完全に彼らの制御下で実行させたりする可能性がある。ユーザーが提供するデータを、OS が実行するコマンドに挿入することはいかなる場合でも避け、もし避けられない場合には、ホワイトリストで入力の検証を厳重に行い、OS がコマンドセパレーターと解釈する制御文字を拒否またはフィルターする。</td></tr>
</table>

6.5.3.2. デバイスに保存される機密データ

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_21</td></tr>
<tr><td>項目名</td><td>機密データのローカルデバイスへの格納チェック</td></tr>
<tr><td>目的</td><td>攻撃者が PII、認証情報/トークン、アカウントデータの機密データの修復を行うことを防止する</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>2 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>ジェイルブレイク/ルート化されたモバイルデバイス</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>アプリケーションが機密情報をローカル環境に保存しないこと、またはアプリケーションが安全に機密情報を暗号化している。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-16</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>暗号化していない機密データをローカルの記憶装置に保存すると、攻撃者にデータが漏洩する可能性がある。機密データをローカルのデバイスに保存することはできるだけ避けなければならない。</td></tr>
</table>

	デバイスのファイルシステムに保存する機密情報はすべてアプリケーションが暗号化しなければならず、また NSFileProtectionNone 属性を使用してはならない。

6.5.3.3. アプリケーションファイルパーミッション

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_22</td></tr>
<tr><td>項目名</td><td>アプリケーションが使用/作成するファイルに適用するファイルパーミッションの状態の決定</td></tr>
<tr><td>目的</td><td>ファイルの記憶領域にある機密データは、安全ではない API の使用により漏洩したり、また安全な API でも安全ではない使用方法により漏洩する危険がある。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>ルート化/ジェイルブレイクされたモバイルデバイス</td></tr>
<tr><td>確認事項</td><td>機密データがデバイスに保存されていない。またはデバイスに保存されている機密データに、適切な保護がなされている。（外部記憶装置に保存するデータは、デバイス上のすべてのアプリケーションからアクセスでき、また固有のファイル保護機能を持たない点に注意すること）</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-16</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>暗号化していない機密データをローカルの記憶装置に保存すると、攻撃者にデータが漏洩する可能性がある。機密データをローカルのデバイスに保存することはできるだけ避けなければならない。デバイスのファイルシステムに保存しなければならない機密情報は、すべてアプリケーションが暗号化しなければならない。</td></tr>
</table>

6.5.3.4. GUI のバイパス

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_23</td></tr>
<tr><td>項目名</td><td>ローカル環境での認証やクライアント側の GUI 制御をバイパスする試み</td></tr>
<tr><td>目的</td><td>クライアント側の認証や制御は、ルート化/ジェイルブレイクされたデバイスでデバッグツールを使用すればほぼ常にバイパスできる。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>8 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>1.有効なアプリケーションの認証情報
2.ルート化またはジェイルブレイクされたデバイス</td></tr>
<tr><td>実施条件</td><td>アプリケーションがクライアント側の認証、またはクライアント側の機密のビジネスロジックを実装している。</td></tr>
<tr><td>確認事項</td><td>アプリケーションが GUI 制御より優先して安全な制御を実行する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-16</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>クライアント側の認証スキームまたはセキュリティ制御を使用する場合、攻撃者にとっては時間をかけ専門知識を駆使すればほぼ常にそれをバイパスすることが可能となる。認証スキームは可能であればサーバー側に移管すべきである。</td></tr>
</table>

6.5.3.5. ジェイルブレイク/ルート化検出のバイパス

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_24</td></tr>
<tr><td>項目名</td><td>デバイスの状態を検証し、ジェイルブレイク/ルート化された環境に展開されていることをチェックするかどうかの判断</td></tr>
<tr><td>目的</td><td>ジェイルブレイク/ルート化されたデバイスは、攻撃者がアプリケーションを通じて完全な制御権を得ることができ、その結果セキュリティ制御をバイパスして機密データが漏洩する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>2〜24 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.5.1.11</td></tr>
<tr><td>入力情報</td><td>アプリケーションバイナリ</td></tr>
<tr><td>実施条件</td><td>アプリケーションにジェイルブレイク/ルート化検出機能を採用する必要がある場合、またはそれを試みる場合、こういったメカニズムがその効果を確保できるか確認する必要がある。</td></tr>
<tr><td>確認事項</td><td>A.アプリケーションが、ジェイルブレイク/ルート化されたデバイス内部への配置の試みを検出すること。
B.アプリケーションがバイナリ強化技術の追加を含む、複数レベルの制御セットを採用すれば、攻撃者にとっては実装した保護機能のバイパスが実現困難となる。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-16</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
</table>

故障の影響および修正	ジェイルブレイクされたデバイスは、攻撃者がアプリケーションによって完全な制御権を得ることができる。その場合、攻撃者からの攻撃回数が増える。モバイルアプリケーションはその環境をテストして、ジェイルブレイクされた、またはエミュレートされたデバイス上で実行されていないかを判断する必要がある。

6.5.3.6. Android IPC チェック

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_25</td></tr>
<tr><td>項目名</td><td>Android の InterProcess Communications（IPC）の脆弱性または構成上のミスをテスト</td></tr>
<tr><td>目的</td><td>InterProcess Communications が悪意のあるユーザーまたはデバイス上のアプリケーションから適切に保護されているかを検証する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>8 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>1.アプリケーションバイナリ
2.ルート化された Android デバイス</td></tr>
<tr><td>実施条件</td><td>アプリケーションが、他のアプリケーションとの通信に IPC を使用する。</td></tr>
<tr><td>確認事項</td><td>被害を防ぐために強化したアプリケーションが使用するあらゆるアクティビティ、コンテンツプロバイダー、サービス、ブロードキャスト受信者を見つける。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td>モバイル静的解析ツール</td><td>TMID-16</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>このテストに合格できない場合、IPC が開始したインスタンスが所有する全データが流出する可能性がある。すべての InterProcess 通信は、アクセス権と扱っているデータに合った、適切な許可と保護の下でエクスポートされなければならない。IPC はホワイトリストによって入力を検証するように安全にコード化して、悪意のあるアプリケーションからのインジェクション攻撃を防がなければならない。</td></tr>
</table>

6.5.3.7. バイナリ難読化 - プロダクション

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_26</td></tr>
<tr><td>項目名</td><td>アプリケーションが難読化されているかのチェック</td></tr>
<tr><td>目的</td><td>アプリケーションのプロダクションビルドにコード難読化が使用されていることを検証する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>0.5 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.5.1.14</td></tr>
<tr><td>入力情報</td><td>アプリケーションバイナリ</td></tr>
<tr><td>実施条件</td><td>アプリケーションバイナリに機密のビジネスロジック、極秘事項、知的財産が含まれている。</td></tr>
<tr><td>確認事項</td><td>アプリケーションバイナリが簡単に判読可能なコードに変換できない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-16</td><td>セクション 2.1.3</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>コードの機密部分についてはアプリケーションに難読化を施して、攻撃者がリバースエンジニアリングをしにくいようにするべきである。Android 用には、簡単にネイティブコードを難読化する多くのオープンソースおよび商用製品がある。暗号作成、ルート化検出、証明書ピンニングのような非常に機密度の高い操作部分に関しては、NDK で C. C obfuscator を使って書き直すと、逆コンパイルしやすい Java よりもより安全である。</td></tr>
</table>

6.5.3.8. 証明書のピンニングのバイパス

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_27</td></tr>
<tr><td>項目名</td><td>さらに高度なテストを有効化するために必要なテスト活動</td></tr>
<tr><td>目的</td><td>証明書のピンニングを有効化した際にバイパスして、ピンニングし暗号化したサーバーへの通信を傍受し精査する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>4 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.5.1.13</td></tr>
<tr><td>入力情報</td><td>ルート化/ジェイルブレイクされたモバイルデバイス</td></tr>
<tr><td>実施条件</td><td>1.アクティブなインターネット接続
2.このアプリケーションが HTTPS 接続で機密データを通信すること。
3.アプリケーションが証明書のピンニングを実装していること。</td></tr>
<tr><td>確認事項</td><td>アプリケーションが強力な証明書ピンニングの実装を採用していて、これをバイパスできない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-16</td><td>セクション 2.1.3.</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>証明書のピンニングは、特定の暗号化したチャンネルで、クライアントとホスト間の通信を保護するために必要である。証明書ピンニングが簡単にバイパスできると、攻撃者が容易にチャンネルに侵入できる。このバイパスの作成を困難にするには、難読化とカスタムの X09 証明書ストアの実装を考慮する。</td></tr>
</table>

6.5.3.9. デバッグ防止 - プロダクション

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_MOBILE_28</td></tr>
<tr><td>項目名</td><td>アプリケーションが適切なデバッグ防止機能を備えているかの検証</td></tr>
<tr><td>目的</td><td>デバッグ防止機能の欠如により、攻撃者がセキュリティ制御をバイパスしたり、メモリから機密データを読み出す可能性が増す。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>0.5 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>ルート化/ジェイルブレイクされたモバイルデバイス</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>アプリケーションがデバッグを困難にする適切な設定を使用している。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#：</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-16</td><td>セクション 2.1.3</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>デバイスに物理的にアクセスする攻撃者やデバイス上で実行されている他のアプリケーションは、デバッグ可能なアプリケーションを完全に制御できる。これにより、いくつかの攻撃が可能になる。それに対処するには、アプリケーションでのデバッグを無効化する。</td></tr>
</table>

6.6. Web サービス

ウェブサービスには、HTTP または安全な HTTPS を使って、インターネットやローカルのイントラネット経由で、車両内で実行されているコンピュータシステムからアクセスします。こういったサービスは車両部内でのローカルサービスとして、または外部からインターネット経由でアクセスされるものとして設置されている場合があります。こうしたサービスは車両の距離測定データの追跡や中継から、車両へのメディア配信まで、様々な機能を提供できます。可能なアプリケーションの数はますます多くなり、車両の機能にとって一層重要になっています。このようなウェブサービスは車両の利用者も車両システムそれ自身も使用するので、様々な利用方法を生み出すだけでなく、新しく悪用の機会をもたらします。

車両やその利用者が信頼するウェブサービスを混乱させたり傍受したりすることで、機密データの流出や重要な車両機能の障害といった、広範囲に及ぶ影響が発生します。したがって、これらのアプリケーションが意図したとおりに機能して、可能な限り攻撃ベクトルを減少することが不可欠です。

このセクションでは、車両または組み込みアプリケーションが利用する Web サービスのセキュリティ状態を評価する方法を示します。このプロセスでは、一般的な攻撃パターンに対するサービスの耐性を含むサービスの全体的なセキュリティの姿勢を評価し、悪意のあるユーザーによって悪用される可能性のある内部または外部インターフェイスの脆弱な領域を特定します。これらの領域には、以下の試験が含まれます。

認証管理
承認管理
ネットワーク層（SSL/TLS 構成）
情報開示/漏洩
ビジネス/アプリケーションロジックの欠陥
入力/データ検証
サーバー構成
セッション管理

サービスのテストでは、しばしば HTTP/HTTPS プロキシから SSL/TLS スキャニングライブラリまで様々なツールを活用し、サービスが意図する機能の知識を利用して、想定されるビジネス機能の遂行能力を変更またはかく乱する必要があります。この文書には、車両システムが使用するすべてのウェブアプリケーションが実行するはずのセキュリティチェックのリストと、アプリケーションのセキュリティを改良するより高度な技術のリストが含まれています。

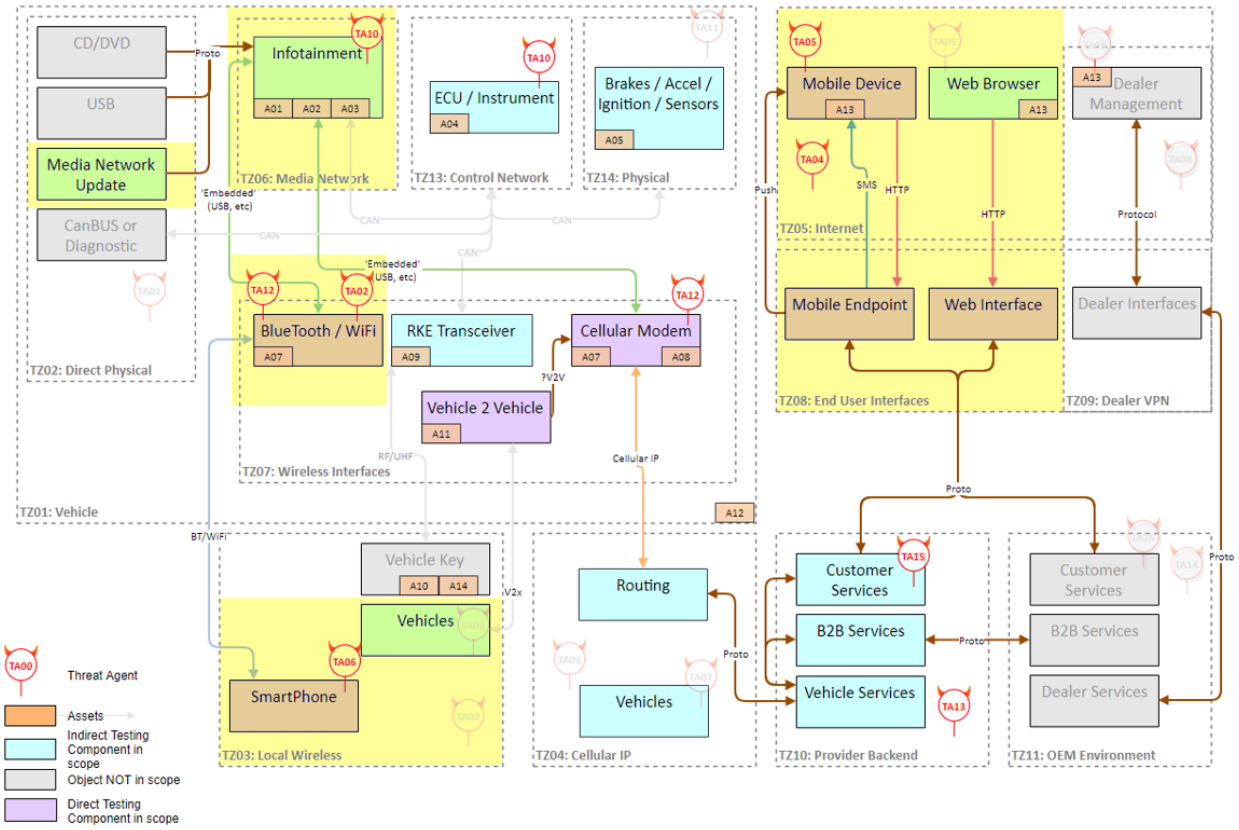


図 12：ウェブサービス範囲内の項目に対する直接的なテストの影響

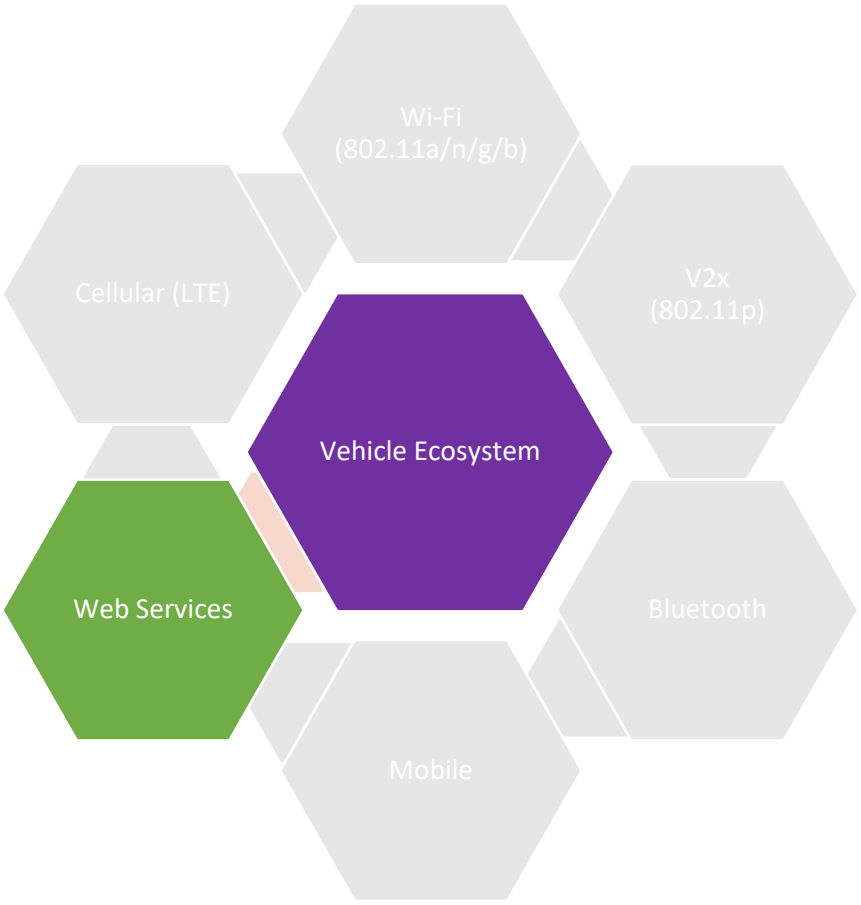


図 13：ウェブサービスのサブコンポーネントカテゴリーをハイライト

6.6.1. 必須

6.6.1.1. 認証スキームの存在を検証

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_1</td></tr>
<tr><td>項目名</td><td>サービスに認証機能が実装されていることの確認</td></tr>
<tr><td>目的</td><td>認証/アクセス制御が機能に実装されていることを検証する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>適切な検証なしにアクセスできてはいけない URL のリスト</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>A.認証スキームが実装されている。
B.認証されていない機能へのアクセス要求が拒否される。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>セクション 2.1.1、2.1.3、2.1.5</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>安全でなければならないページへのユーザーの閲覧を許可すると、保護するべき機密情報が漏洩する恐れがある。機密データを含むあらゆるリソースの承認機能を強化する必要がある。</td></tr>
</table>

6.6.1.2. パスワードリセットの危険性

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_2</td></tr>
<tr><td>項目名</td><td>パスワードリセット機能の検査を実施</td></tr>
<tr><td>目的</td><td>パスワードのリセットに非公開情報が必要かどうかを特定する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.1.1.</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>1.アクティブなインターネット接続
2.パスワードのリセット機能がユーザーから見える。</td></tr>
<tr><td>確認事項</td><td>A.パスワードのリセットには非公開情報が必要であり、悪意のあるユーザーや未承認のユーザーが、正規のアカウントに対してサービスのリセットやサービス妨害を行うことを防いでいる。
B.アプリケーションが、入力したユーザー名が有効なアカウントに関連付いていてもいなくても、同じ応答を返す。
C.このメッセージが、サーバー側でパスワードリセットのロジックが実行される前に返されて、ユーザーがサーバーの応答時間を基に有効なユーザー名を推測できないようにしている。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>パスワードリセットの適切なメカニズムを実装していない場合、ユーザーのアカウントやサービス妨害、有効なユーザーアカウントの列挙型データに侵入される場合がある。パスワードリセットのメカニズムは、何らかの追加の検証を経由してユーザーの ID を確かめる必要がある。
さらにテストでは、ユーザー名やアカウントの詳細情報が有効なものでも無効なものでも、パスワードリセット機能に入力した時に、受信に対する応答が同じであって、パスワードリセット機能によってユーザー名やアカウントの詳細情報を列挙する可能性を回避していることを検証しなければならない。</td></tr>
</table>

6.6.1.3. ユーザー名の列挙型データ

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_3</td></tr>
<tr><td>項目名</td><td>情報の開示を求めるログインの試みへの応答の精査</td></tr>
<tr><td>目的</td><td>有効なユーザー名やアカウントの詳細情報を特定できるかを検証する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>2 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.1.1</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>認証中に入力されるユーザー名が有効か無効かに関わりなく、応答が同じである。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-16</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>ユーザー名の列挙型データにより、攻撃者はブルートフォースアタックを使って有効なアカウント ID を発見できるようになる。アプリケーションは、入力されるユーザー名が有効なアカウントに関連するものであるかどうかに関わらず、同じ応答を返すように変更されなければならない。</td></tr>
</table>

6.6.1.4. パスワード変更機能

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_4</td></tr>
<tr><td>項目名</td><td>パスワード変更機能が提供されている場合、現在のパスワードの検証が行われる必要がある。</td></tr>
<tr><td>目的</td><td>ユーザーが、現在の認証情報に関する知識を持たずにアカウントに関連するパスワードを変更できるかどうかを判断する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>1.アクティブなインターネット接続
2.パスワードの変更機能がユーザーから見える。</td></tr>
<tr><td>確認事項</td><td>ユーザーはパスワード変更プロセス中に、変更したいパスワードに加えて現在の認証情報の再入力を求められる。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>現在のパスワードの入力を要求せずに認証し、その間にパスワードの変更を許可すると、攻撃者に攻撃対象者のパスワードの変更を許可し、そのアカウントへの継続的なアクセス権を与えてしまい、ユーザーが混乱する。アプリケーションはユーザーの現在の認証情報、例えば現在のパスワードなどを要求して、パスワードの変更プロセス中にその ID を検証する必要がある。</td></tr>
</table>

6.6.1.5. パスワードポリシーの監査

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_5</td></tr>
<tr><td>項目名</td><td>内包する弱点に対処する車両ウェブサービスのパスワードポリシーのチェック</td></tr>
<tr><td>目的</td><td>実施されているパスワードポリシーが、アカウント登録やパスワード変更/リセット機能において、適度に強力なパスワードの使用を義務付けているかを検証する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>1.有効なアプリケーションの認証情報
2.実施されているパスワードポリシー</td></tr>
<tr><td>実施条件</td><td>パスワード生成プロセス</td></tr>
<tr><td>確認事項</td><td>アプリケーション/サービスが強力なパスワードポリシーを実施している。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>虚弱なパスワードは簡単に推測される恐れがある。その場合、攻撃者がユーザーのアカウントに侵入する可能性が増える。複数の規則を組み合わせた強力なパスワード複雑性ポリシーを実装して、</td></tr>
</table>

	簡単に推測できるパスワードが使用されるのを防ぎ、同時にパスワードが確実に充分なエントロピーを持つようにする。ほとんどのセキュリティ推奨では、最小 8 文字で、大文字、小文字、数字および少なくともひとつの特殊文字を含むパスワードを提案している。

6.6.1.6. アカウントロックアウトポリシーの実施

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_6</td></tr>
<tr><td>項目名</td><td>適切なアカウントロックアウトポリシーの実施の検証</td></tr>
<tr><td>目的</td><td>ブルートフォースアタックの成功によるパスワード推測の可能性を減らす。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.1.1</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>適度な回数、認証に失敗した後には、ユーザーのアカウントとリソースへのアセスを停止するロックアウトポリシーを、アプリケーションが実施している。このロックアウトはサーバー側で行う必要がある。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>ロックアウトポリシーが実施されていない、あるいは不充分なアプリケーションは、ブルートフォースアタックによるパスワード推測に対して脆弱であり、攻撃者は既知のユーザー名と考えられるパスワードのリストを使って、適切な組み合わせを見つけるまでログインを試みる。何回かログインを試みて失敗した場合には、設定した期間アカウントをロックするアカウントロックアウトポリシーを実装する。ロックアウトまでに許容するログインを試みる回数は、6 回が標準的である。</td></tr>
</table>

6.6.1.7. 冗長サーバーバナー

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_7</td></tr>
<tr><td>項目名</td><td>冗長サーバー情報が HTTP レスポンスで送信される。</td></tr>
<tr><td>目的</td><td>サーバー応答で使用情報が潜在的な攻撃者に公開されていないことを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>タイプやバージョンなどの冗長サーバー情報がレスポンスヘッダーに表示されない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>冗長サーバーバナーには、アプリケーションや基本インフラストラクチャで使用されている特定のテクノロジースタックに対して攻撃者が攻撃できるようになる追加情報が表示される。冗長サーバー情報は、すべての HTTP レスポンスから削除する必要がある。これを行うには、サーバーの構成ファイルを変更するか、Web アプリケーションファイアウォールを使用する。</td></tr>
</table>

6.6.1.8. HTTPS の有効化/強制化

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_8</td></tr>
<tr><td>項目名</td><td>HTTPS を有効化および強制化する。</td></tr>
<tr><td>目的</td><td>通信が暗号化されたチャンネルを介してのみ行われるようにする。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>HTTPS URL のリスト</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>A.HTTPS がサーバー上で有効になっている。
B.リソースおよび機能へのアクセスは、TLS 暗号化接続を介してのみ行う必要がある。応答は HTTPS 接続を介してのみ受け取る必要がある。プレーンテキストの HTTP 接続を介した通信は処理されず、ユーザーを適切なリソースの HTTPS バージョンにリダイレクトする必要がある。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>セクション 2.1.1
2.1.3、2.1.4、2.1.5</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>アプリケーションサーバーで HTTPS が有効化/強制化されていない場合、アプリケーショントラフィックはプレーンテキストで通信されるか、プレーンテキスト接続経由で取得することができる。被害者とアプリケーションサーバー間のネットワークで listen している攻撃者は、アプリケー</td></tr>
</table>

	ショントラフィックを表示し、変更することができる。最善のセキュリティを導入するために、HTTPS を有効化し、TLS v1.1 または 1.2 を採用する必要がある。また、HTTP トラフィックの HTTPS への転送を強制化する。

6.6.1.9. WebDAV MKCOL HTTP メソッドの有効化

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_9</td></tr>
<tr><td>項目名</td><td>Web-based Distributed Authoring and Versioning（WebDAV）HTTP/1.1 拡張が有効化されている IIS サーバーは、リモート Web サーバー上にある文書を編集できる危険な HTTP メソッド（MKCOL など）を潜在的にサポートしている。</td></tr>
<tr><td>目的</td><td>Web サーバー上にディレクトリとリソースを作成する WebDAV サポートを攻撃者が悪用できないことを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>1.アクティブなインターネット接続
2.サーバーが IIS を実行中である。</td></tr>
<tr><td>確認事項</td><td>IIS サーバーが HTTP MKCOL メソッドをサポートしていないか、WebDAV を無効化している。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>MKCOL は WebDAV が使用できる HTTP メソッドであり、Web サーバー上に「コレクション」（ディレクトリ）を作成する際に使用できるため、特に危険と見なされる。こうしたディレクトリは、リクエスト URI（Uniform Resource Identifier）で指定した場所に作成できる。IIS サーバー上で WebDAV を無効にするか、HTTP メソッド MKCOL を不許可にすべきである。</td></tr>
</table>

6.6.1.10. 脆弱なサーバーバージョン

項目	記載内容
項目番号	NEDO_WEB_10
項目名	Web サーバーが脆弱性を公開している。
目的	サーバー、またはアプリケーションが使用中の追加機能について、公開されている既知の脆弱性が存在しないことを確認する。
実施タイミング	
想定実施工数	1 時間
前提テスト項目	冗長性の詳細がないことはバージョンの安全性を示すものではないが、テストは NEDO_WEB_20（冗長サーバーバナー）によって通知される。
入力情報	有効なアプリケーションの認証情報
実施条件	アクティブなインターネット接続
確認事項	サーバーバージョンと使用中の追加テクノロジーに既知の脆弱性がない。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除
備考	ツール: BSM # TMID-18; 車両#: 2.1.5; 関連する攻撃: N/A
故障の影響および修正	既知の脆弱性を持つ Web サーバーまたはアプリケーションサーバーのプラットフォームを使用すると、サーバーに保存されているデータまたはホストされているアプリケーションがすべて搾取にさらされる。Web サーバーまたはアプリケーションサーバーを、現時点で既知の脆弱性を持たないバージョンにアップグレードするか、パッチを当てる必要がある。

6.6.1.11. 制限されない HTML5 クロスドメインリソースシェアリング

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_11</td></tr>
<tr><td>項目名</td><td>アプリケーションが過度に寛容な CORS ポリシーを設定していて、信頼できない発信元にリソースを公開していないかどうかを判別する。</td></tr>
<tr><td>目的</td><td>過度に寛容なクロスドメイン/クロスオリジンリソースシェアリング（CORS）では、攻撃者が同一オリジンポリシーベースのセキュリティコントロールを上書きすることにより、外部リソースから悪意あるコンテンツをロードできる。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>アプリケーションが過度に寛容な CORS ポリシーで構成されていない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>攻撃者は、過度に寛容な CORS ポリシーを利用して、CORS ポリシーが認証情報付きリクエストを許可する場合にターゲットサーバー上の機密データにアクセスしたり、ユーザーの知識がなくても機密の操作を実行したりできる悪意ある JavaScript を自身のオリジンに置くことができる。HTTP レスポンスの Access-Control-Allow-Origin ヘッダーは、ワイルドカードマッチを設定したり、入力値検証をせずに HTTP リクエストの Origin ヘッダーに基づいて動的に入力したりしないようにする必要がある。ほとんどの場合、このヘッダーは安全に削除できる。ただし、アプリケーションに同一オリ</td></tr>
</table>

	ジンポリシーの緩和が必要な場合、このサーバーが信頼できるオリジンをホワイトリストに登録する必要がある。

6.6.1.12. 認証前のセッション ID の設定

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_12</td></tr>
<tr><td>項目名</td><td>アプリケーションが認証の前にユーザーのセッションを確立し、ユーザー認証時にはセッション ID を更新しない。</td></tr>
<tr><td>目的</td><td>認証後にセッション ID が正しく更新されていることを確認して、乗っ取り攻撃にユーザーセッションがさらされないようにする。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.1.1</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>認証時にアプリケーションが新しい安全なランダムセッション ID を発行している。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>ログイン時にセッション ID の更新に失敗すると、その ID は必要以上に長い期間にわたって公開されたままになるため、攻撃者にセッションを盗む時間と機会を与えることになる。ユーザーがアプリケーションへの認証に成功したら、新しいセッションと ID を確立し、認証前のすべてのセッションとトークンを無効にする必要がある。セッション ID の再利用は許可しないでください（例えば、ASP.NET で Cookie なしのセッション状態は無効にする必要がある）。</td></tr>
</table>

6.6.1.13. セッション固定

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_13</td></tr>
<tr><td>項目名</td><td>ユーザーがアプリケーションに認証された後、セッション ID が変更されない場合、攻撃者が別のユーザーに使用しているセッション ID を制御できる脆弱性がある。</td></tr>
<tr><td>目的</td><td>アプリケーションに認証されたユーザーが使用しているセッション ID を攻撃者が制御して、そのユーザーにスプーフィングすることができないことを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.1.1, 6.6.1.8</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報
セッション ID の変数名
セッション ID の形式</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>A.アプリケーションがクライアントによって設定されたセッション ID を拒否する。
B.アプリケーションが受け入れる ID がサーバーから特定のクライアントに発行されたもののみである。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>セッション固定の脆弱性は、攻撃者と被害者を同じセッション ID でアプリケーションに接続する。攻撃者と被害者は同じセッション ID をアプリケーションに提供するため、セッションがアクティ</td></tr>
</table>

	ブであるかぎり、アプリケーションは攻撃者からのトランザクションを被害者からのものであるように処理する。ユーザーの認証時に、アプリケーションは既存のセッション ID を無効にし、既存のセッションデータをクリアして、新しいセッション ID と新しいセッションデータを作成する必要がある。

6.6.1.14. 永続的 Cookie に機密情報が含まれる

項目	記載内容
項目番号	NEDO_WEB_14
項目名	永続的 Cookie ストレージによって機密情報が無許可ユーザーに公開されていないことを確認する。
目的	ユーザー、アプリケーション、またはセッションに関する機密情報が、クライアント/ユーザーのコンピュータ上にある永続的 Cookie に保管されている可能性がある。
実施タイミング	
想定実施工数	0.5 時間
前提テスト項目	なし
入力情報	有効なアプリケーションの認証情報
実施条件	アクティブなインターネット接続
確認事項	アプリケーションは機密情報を永続的 Cookie に保管しておらず、Cookie に有効期限が設定されている。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除
備考	ツール: (空) / BSM #: TMID-18 / 車両#: セクション 2.1.4 / 関連する攻撃: N/A
故障の影響および修正	永続的 Cookie に保管されている機密情報は無許可ユーザーに漏れる可能性がある。機密情報は永続的 Cookie に保管しない。セッショントラッキング情報は、セッションが終了すると有効期限が切れるセッション Cookie に保管する必要がある。

6.6.1.15. 長すぎるセッションタイムアウト期間

項目	記載内容
項目番号	NEDO_WEB_15
項目名	アプリケーションは、適正な非アクティブ期間後に現在のセッションユーザーをログアウトする必要がある。
目的	アプリケーションが非アクティブセッションを終了することを確認する。非アクティブタイムアウト期間は、データの機密度とアプリケーションに含まれる機能によって異なるが、通常 15〜30 分より長いアイドルセッションは脆弱であると見なされる。
実施タイミング	
想定実施工数	0.5 時間
前提テスト項目	なし
入力情報	有効なアプリケーションの認証情報
実施条件	アクティブなインターネット接続
確認事項	適正な非アクティブ期間後にセッションが終了する。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除
備考	ツール: (空) / BSM #: TMID-18 / 車両#: セクション 2.1.4 / 関連する攻撃: N/A
故障の影響および修正	セッションタイムアウトが長くなれば、攻撃者が被害者のセッションを乗っ取る可能性が高くなる。攻撃者が有効なセッション ID を取得すると、アプリケーション内で被害者にスプーフィングすることができる。長いセッションタイムアウトはサーバーメモリの開放を妨げることにもなり、潜在的なサービス運用妨害状態になる。十分に短いアイドル期間後にサーバーサイドのユーザー

	セッションを終了してください。ユーザーが終了したセッションを使用してリクエストを作成すると、スプラッシュページまたはログインページにリダイレクトされる。

6.6.1.16. Cookie の誤った構成：Secure 属性が設定されていない

項目	記載内容
項目番号	NEDO_WEB_16
項目名	この属性が設定されていない場合、Cookie は脆弱なサイトへのすべての HTTP リクエストとともにそのサイトに送信されるため、被害者とサーバー間のトラフィックを盗聴可能な攻撃者は Cookie を盗むことができる。
目的	'Secure'属性が明示的に設定されていないかどうかを判別する。
実施タイミング	
想定実施工数	1 時間
前提テスト項目	なし
入力情報	有効なアプリケーションの認証情報
実施条件	アクティブなインターネット接続
確認事項	すべての Cookie に Secure 属性が構成されている。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除
備考	ツール / BSM # / 車両# / 関連する攻撃 TMID-18 / N/A / N/A
故障の影響および修正	被害者の Cookie に'Secure'属性が設定されていない場合、被害者と同じネットワーク上にいる攻撃者にその Cookie を盗まれる恐れがある。Cookie に被害者のセッション ID が含まれる場合、攻撃者は被害者のセッションを盗むことができる。HTTPS を常に使用することを考慮すれば、すべての場合において Secure 属性を明示的に true に設定する必要がある。

6.6.1.17. Cookie の誤った構成：HttpOnly 属性が設定されていない

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_17</td></tr>
<tr><td>項目名</td><td>‘HttpOnly’属性が明示的に設定されていない。</td></tr>
<tr><td>目的</td><td>HttpOnly 属性がない場合、Cookie の値には JavaScript などのクライアントサイドのスクリプトからアクセスできる。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>A.スクリプトで使用されていない Cookie に HttpOnly 属性が設定されている。
B.すべてのセッション Cookie に HttpOnly 属性が構成されている。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>‘HttpOnly‘フラグは Set-Cookie ヘッダーの一部として設定されるフラグであり、最新ブラウザのクライアントサイド JavaScript に Cookie の値が読み取られたり設定されたりするのを防ぎます。重要な Cookie に HttpOnly フラグが設定されていないと、クロスサイトスクリプティングなどの攻撃の実行を招く恐れがある。Cookie の値がスクリプトからのアクセスを求めないすべてのケースで、HttpOnly 属性を明示的に true に設定する必要がある。</td></tr>
</table>

6.6.1.18. Cookie の誤った構成：広範なセッション Cookie ドメイン

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_18</td></tr>
<tr><td>項目名</td><td>Cookie に広く定義されたドメインがある。</td></tr>
<tr><td>目的</td><td>アプリケーションに設定されている Cookie の適用範囲が広すぎるかどうかを判別する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>アプリケーションが適用範囲の広い Cookie ドメインを拒否する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>過度に範囲の広いドメインが設定された Cookie は、そのドメインおよびすべてのサブドメインでホストされているすべてのアプリケーションに送信される。こうしたアプリケーションには、Cookie 経由で渡されたセッション情報を公開する脆弱性が含まれる場合がある（クロスサイトスクリプティングなど）。"domain"属性は、すべてのセッション Cookie のほか、セッション Cookie 値を要求するサブドメインに設定する必要がある。</td></tr>
</table>

6.6.1.19. Cookie の誤った構成：広範なセッション Cookie パス

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_19</td></tr>
<tr><td>項目名</td><td>Cookie に広く定義されたパスがある。</td></tr>
<tr><td>目的</td><td>Cookie 構成のパスが過度に広範に設定されているかどうかを判別する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>アプリケーションに適用範囲の広いセッション Cookie パスが設定されていない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>過度に範囲の広いパスが設定された Cookie は、そのドメインおよびパスでホストされているすべてのアプリケーションに送信される。こうしたアプリケーションには、Cookie 経由で渡されたセッション情報を公開する脆弱性が含まれる場合がある（クロスサイトスクリプティングなど）。"path"属性は、すべてのセッション Cookie のほか、アプリケーションの特定のパスに設定する必要がある。"path"属性の値は、アプリケーションが存在するディレクトリを明示的に示す必要があるほか、属性がルートディレクトリに設定されていないことも確認する必要がある。</td></tr>
</table>

6.6.1.20. 脆弱な X.509 証明書署名ハッシングアルゴリズム

項目	記載内容
項目番号	NEDO_WEB_20
項目名	X.509 証明書署名ハッシングアルゴリズムは脆弱である
目的	車両エコシステムのハッシングアルゴリズムが脆弱でないことを確認する。
実施タイミング	
想定実施工数	1 時間
前提テスト項目	項目 6.6.1.8
入力情報	有効なアプリケーションの認証情報
実施条件	アクティブなインターネット接続
確認事項	強力な証明書署名アルゴリズムであることが知られている（少なくとも RSA を使った SHA-256）。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除
備考	<table><tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr><tr><td></td><td>TMID-18</td><td>セクション 2.1.1 2.1.3</td><td>N/A</td></tr></table>
故障の影響および修正	攻撃者は、システムからみて有効に見える証明書を偽造して、システムのその偽造証明書を承認させようとすることがある。識別の証明としてこの証明書を提示するパーティにスプーフィングすることで、中間者攻撃（MITM）を行い易くするために、これが利用されることがある。このスプーフィングを防止するために、強度の高い、証明書ハッシングアルゴリズム、最低でも sha244 を使うべきである。

6.6.1.21. 自己署名 X.509 証明書

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_21</td></tr>
<tr><td>項目名</td><td>サーバーが自己署名 X.509 証明書を発行する。</td></tr>
<tr><td>目的</td><td>サーバーは、クライアントとの暗号化コネクションを確立するときに、自己署名 X.509 証明書を発行する。自己署名 X.509 証明書は、信頼できる内部または第三者の認証局により作成されたものではない。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.1.8</td></tr>
<tr><td>入力情報</td><td>なし</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>X.509 証明書は、信頼できる認証局が発行したものである。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>最新のウェブブラウザは、自己署名 X.509 証明書が信頼できる内部または第三者の認証局により作成されたものではない場合、それを受け付けず、エラーを生成してユーザーに表示する。信頼できる内部または第三者の認証局により作成されたものでない自己署名 X.509 証明書は、ユーザーにエラー対応はできていると過信させ、結果として中間者攻撃の餌食となる機会が増加する。自己署名 X.509 証明書を使用してインターネットにアクセスできるすべてのサービスは、信頼できる認証局から信頼できる新しい証明書を取得すべきである。</td></tr>
</table>

6.6.1.22. 間違ったホスト名をもつ X.509 証明書

項目	記載内容
項目番号	NEDO_WEB_22
項目名	不正確または操作可能なデータの Web 証明書をテストする
目的	サーバーが示している X.509 証明書のコモンネーム（CN）セットが、要求しているサイトのドメインと一致しません。コモンネームは、X.509 証明書に関連付けられ、完全に認定された 1 つ以上ドメインを指定している。コモンネームは、証明書のタイプ次第で、同一のドメイン（たとえば、"site.com"や"www.site.com"）、ワイルドカード名（たとえば、"*.site.com"）またはドメインリストに属する 1 つ以上のホストであることがある。証明書は、リクエストホスト名が証明書のコモンネームフィードに挙げられているドメインの 1 つに合致した場合にのみ、有効であるとみなされる。
実施タイミング	
想定実施工数	1 時間
前提テスト項目	項目 6.6.1.8
入力情報	なし
実施条件	アクティブなインターネット接続
確認事項	X.509 証明書の CN が、リクエストされたサイトと合致している。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除
備考	ツール / BSM # / 車両# / 関連する攻撃 TMID-18 / N/A / N/A
故障の影響および修正	証明書のコモンネームが証明書を発行しているサーバーに合致しない X.509 証明書を使用すると、機密データが失われることになるかもしれない。自己署名 X.509 証明書を使用したすべてのサービスは、信頼できる認証局から信頼できる新しい証明書を取得すべきである。

6.6.1.23. X.509 証明書チェーンに、2048 ビット未満の RSA キーが含まれている。

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_23</td></tr>
<tr><td>項目名</td><td>X.509 証明書は、その暗号化およびデジタル署名アルゴリズムに 2048 ビット未満の長さのキーをもつ RSA を使っている。2048 ビット未満のキーを使用するとそのアルゴリズムの強度が著しく劣化し、既知の暗号攻撃に対して当該のアルゴリズムが脆弱になる。シマンテック社の「SSL Cert Checker」のような自動化されたツールは、ターゲットアプリケーションで使用されている X.509 証明書のキーのサイズが 2048 ビット以下であるかを迅速に検知するために利用できる。</td></tr>
<tr><td>目的</td><td>X.509 証明書チェーンに、2048 ビット未満の RSA キーが含まれていないことの確認</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.1.8</td></tr>
<tr><td>入力情報</td><td>なし</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>RSA を使用した証明書はすべて、少なくとも 2048 ビットのキーを使用している。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>攻撃者は、2048 ビット未満の長さのキーをもつ RSA を使った証明書を複製できる可能性はある。RSA を使ったすべての証明書は、少なくとも 2048 ビットの長さのキーを使用すべきであり、この長さ以下のキーを使った証明書はすべて使用しないようにすべきである。</td></tr>
</table>

6.6.1.24. 脆弱な SSL/TLS を使った暗号化スイート

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_24</td></tr>
<tr><td>項目名</td><td>サーバーが対応している SSL/TLS 暗号化スイートには脆弱性がある。</td></tr>
<tr><td>目的</td><td>サーバーサイド SSL/TLS のエンドポイントは、脆弱な SSL/TLS 暗号化スイートを許すようなコンフィギュレーションを持っている。これらの暗号化スイートには、攻撃者がトラフィックを解読、または改ざんすることを許す欠陥があることが分かっている。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.1.8</td></tr>
<tr><td>入力情報</td><td>なし</td></tr>
<tr><td>実施条件</td><td>1.アクティブなインターネット接続
2.承認済みであり対応可能な暗号化のリスト</td></tr>
<tr><td>確認事項</td><td>アプリケーションは、十分な強度で暗号化された TLSv1.2 コネクションのみに対応すべきである。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>攻撃者は、2048 ビット未満の長さのキーをもつ RSA を使った証明書を複製できる可能性はある。RSA を使ったすべての証明書は、少なくとも 2048 ビットの長さのキーを使用すべきであり、この長さ以下のキーを使った証明書はすべて使用しないようにすべきである。</td></tr>
</table>

6.6.1.25. SSL/TLS インセキュア認識オン

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_25</td></tr>
<tr><td>項目名</td><td>サーバーのコンフィギュレーションは、クライアントが開始するインセキュアな再ネゴシエーションに対応するように設定されている。</td></tr>
<tr><td>目的</td><td>サーバーのコンフィギュレーションは、TLS/SSL コネクションを行うためにクライアントが開始するインセキュアな再ネゴシエーションを許すように設定されている。SSL/TLS のハンドシェイクプロセスの設計の欠陥のために、その中間者攻撃中にクライアントがサーバーと通信を開始する時に、攻撃者は任意のデータをインジェクトできる。クライアントが開始する再ネゴシエーション機能の目的は、クライアントが TLS/SSL コネクションを行うために新しい暗号化パラメータを再ネゴシエーションできるようすることであるが、RFC 5746 にプロトコルレベルの変更が導入される前は、このハンドシェイクは既存のコネクションとの関連付けが不適切であったために、この再ネゴシエーションハンドシェイクはセキュアではなかった。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.1.8</td></tr>
<tr><td>入力情報</td><td>なし</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>サーバーは、（RFC 5746 に準拠して）クライアントが開始するインセキュアな再ネゴシエーションに対応していない。または、サーバーはクライアントが開始する再ネゴシエーションに対応している。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>セクション 2.1.3</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>クライアントが開始する SSL/TLS 再ネゴシエーションがインセキュアであると、クライアントがサーバーと通信を開始する時に攻撃者は任意のデータをインジェクトできる。RFC 5746 に導入されたクライアントが開始する再ネゴシエーションがセキュアである SSL/TLS のバージョンに、サー</td></tr>
</table>

	バーを更新すべきである。サーバーを更新できない場合、クライアントが開始する再ネゴシエーションは無効にすべきである。

6.6.1.26. クライアントが開始する SSL/TLS 再ネゴシエーションを有効にする

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_26</td></tr>
<tr><td>項目名</td><td>クライアントが開始する SSL/TLS 再ネゴシエーションは、攻撃者が悪用できるシングル TCP コネクション内に SSL/TLS コネクション向けの新しい暗号化パラメータを、クライアントが再ネゴシエーションできるようにする機能である。</td></tr>
<tr><td>目的</td><td>クライアントが開始する再ネゴシエーションに、サーバーが対応しているか判断する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.1.8</td></tr>
<tr><td>入力情報</td><td>なし</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>サーバーは、クライアントが開始する再ネゴシエーションに対応していない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>セクション 2.1.1
2.1.3</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>クライアントが開始する SSL/TLS 再ネゴシエーションを可能にすることで、サーバーに対して攻撃者がサービス妨害（DoS）攻撃を行われるようになる。クライアントが開始する SSL/TLS 再ネゴシエーションに、アプリケーションが対応する必要が無い場合、サーバーは再ネゴシエーションを無効にするべきである。再ネゴシエーションに対応する必要がある場合、シングル TCP コネクションを使用して短期間、多数回の再ネゴシエーションを開始する可能性のあるクライアントをブロックするために、サーバーは転送速度制限を使用すべきである。</td></tr>
</table>

6.6.1.27. OpenSSL メモリバッファー盗み読み（ハートブリード）

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_27</td></tr>
<tr><td>項目名</td><td>あるバージョンの OpenSSL は、ハートブリードと呼ばれるエクスプロイトに対して脆弱である。このエクスプロイトにより攻撃者はサーバーメモリの一部を抽出できる。</td></tr>
<tr><td>目的</td><td>サーバーが、ハートブリードエクスプロイトに対して脆弱であるかを判断する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.1.8</td></tr>
<tr><td>入力情報</td><td>なし</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>サーバーは、脆弱性の無いバージョンの OpenSSL を使用している。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>サーバーのメモリへアクセスすることで、攻撃者は機密データを取得できる。ハートビートにより機密データが漏洩することを防止するために、OpenSSL を最新の安定したバージョンに更新する。ハートブリードに対して耐性がある最新のバージョンは 1.0.1g である。バージョンを更新したら、影響を受けているすべての X.509 証明書を無効にしてから、再発行し、すべてのユーザーにパスワードのリセットを強制する。</td></tr>
</table>

6.6.1.28. X.509 証明期限切れ

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_28</td></tr>
<tr><td>項目名</td><td>サーバーが使用している X.509 証明書の有効期限が経過している。</td></tr>
<tr><td>目的</td><td>X.509 証明書の有効期限日が現在日よりも前である場合、その証明書は失効にされる。証明書管理のやり方が悪いと、この問題が生じることがある。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.1.8</td></tr>
<tr><td>入力情報</td><td>なし</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>サーバーは、現在有効な証明書のみを使用している。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>失効した X.509 証明書を使うとセンシティブな情報が失われることになる可能性がある。現在有効である X.509 証明書を使うべきであり、証明書はその失効前に更新すべきである。</td></tr>
</table>

6.6.1.29. 有効期限が迫った X.509 証明書

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_29</td></tr>
<tr><td>項目名</td><td>サーバーが使用している X.509 証明書の有効期限がすぐに切れるように設定する。</td></tr>
<tr><td>目的</td><td>現在日が、X.509 証明書の有効期限に近づくと、「有効期限が迫っている」と見なされる。有効期限の 90 日前になると、証明書の発行者（つまり、認証局）が証明書の所有者にその証明書の更新を促すのが一般的である。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.1.8</td></tr>
<tr><td>入力情報</td><td>なし</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>サーバーは、残りの有効期限がテスト時から 90 日以上に設定されている証明書のみを使用する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>有効期限が迫っている X.509 証明書が失効前までに更新されない場合、その証明書はエンドユーザーとの通信のセキュリティを保証でないとみなされる。現在有効である X.509 証明書を使うべきであり、証明書はその失効前に更新すべきである。</td></tr>
</table>

6.6.1.30. まだ有効でない X.509 証明書

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_30</td></tr>
<tr><td>項目名</td><td>サーバーが使用する X.509 証明書がまだ有効でない。</td></tr>
<tr><td>目的</td><td>メッセージ、[X.509 certificate Not Yet Valid]は、証明書の承認はこれからなされることを意味している。証明書管理のやり方（たとえば、コンフィギュレーションが間違っている）が悪いと、この問題が生じることがある。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.1.8</td></tr>
<tr><td>入力情報</td><td>なし</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>サーバーは、現在有効である証明書を使用する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>確認開始日を基準にしたときにまだ有効ではない X.509 証明書を使うと、機密データを失うことがある。現在有効である X.509 証明書を使うべきであり、証明書はその失効前に更新すべきである。</td></tr>
</table>

6.6.2. 推奨

6.6.2.1. エントロピーが小さいセッション ID

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_31</td></tr>
<tr><td>項目名</td><td>エントロピーが小さいアプリケーションセッション ID を使用すると、ID が予測されやすくなる。</td></tr>
<tr><td>目的</td><td>適切な暗号論的擬似乱数生成器（CSPRNG=Cryptographically Secure Pseudo-Random Number Generator）を使いセッション ID が生成されていることを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.1.1</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>1.アクティブなインターネット接続
2.アプリケーションは、セッション ID を使用する。</td></tr>
<tr><td>確認事項</td><td>セッション ID のエントロピーが、少なくとも 64 ビットである。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>セクション 2.1.1
2.1.4</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>エントロピーが小さいセッション ID を使用すると、攻撃者が有効なセッショントークンを推定したり、または総当たりで見つけたりすることを許可し、認証を得ないままアプリケーションにアク</td></tr>
</table>

	セスすることを許可する。セッション ID を生成するメカニズムを、少なくとも 64 ビット長/128 ビットのエントロピーであるセッション ID を作成する暗号論的擬似乱数生成器（CSPRNG）を使うようなメカニズムに変更する。

6.6.2.2. HTTP レスポンス分割

項目	記載内容
項目番号	NEDO_WEB_32
項目名	キャリッジリターン文字およびラインフィード文字（CR+LF、ASCII 0x0D + 0x0A）がこのようにインジェクトできる場合、アプリケーションは信頼できない無いデータを受け付け、HTTP レスポンスヘッダーの作成に使う。攻撃者は、正当なレスポンスデータとして解釈される新しいコンテンツラインを作成できる。
目的	キャリッジリターン/ラインフィード文字のインジェクションでは、任意の HTTP レスポンスデータを動的に作成できないことを確認する。
実施タイミング	
想定実施工数	2 時間
前提テスト項目	なし
入力情報	有効なアプリケーションの認証情報
実施条件	アクティブなインターネット接続
確認事項	A.アプリケーションは、信頼できないデータを使い動的にレスポンスヘッダーを生成しない。 B.信頼できない入力をサニタイズして、予想される値のみを許容し、キャリッジリターン文字およびラインフィード文字とそのエンコードされたコードを明確にブラックリストに入れる。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除
備考	ツール: （空） BSM #: TMID-18 車両#: N/A 関連する攻撃: N/A

故障の影響および修正	攻撃者は、HTTP レスポンス分割をエクスプロイトし、データラインが追加された CR+LF シーケンスをインジェクションすることにより、任意のヘッダーを設定したり、HTTP レスポンスボディーをコントロールしたり、レスポンスを別々の 2 つ以上のレスポンスに分割できる。アプリケーションは、レスポンスヘッダーを動的に生成するために信頼できないデータを使うべきではありません。レスポンスヘッダーを作成するためにアプリケーションが信頼できないデータを使う必要がある場合、信頼できない入力をサニタイズして、そのアプリケーションが、CR+LF とそのエンコードされたコードを明確にブラックリストにすることに加えて予想される値のみを許すようにする。たとえば、信頼できないデータが URL 内をパスした場合、CR+LF の URL エンコード値、つまり%0D%0A はブラックリストにする。

6.6.2.3. XML 外部エンティティ解決（XXE）

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_33</td></tr>
<tr><td>項目名</td><td>外部のどんなリソースからでも XML ドキュメントがドキュメントを作成できるようにすると、システムファイルやユーザーの認証情報のような通常はアプリケーションからアクセスできない機密データを露出することになる。</td></tr>
<tr><td>目的</td><td>XML 文書型定義（XML DTD）を変更することにより、XML パーサが外部 URI からデータ抽出できるかを判断する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>XML 機能を利用するために必要な場合に有効なアプリケーション認証情報</td></tr>
<tr><td>実施条件</td><td>1.アクティブなインターネット接続
2.アプリケーションは、XML ドキュメントに対応している。</td></tr>
<tr><td>確認事項</td><td>アプリケーションは、ユーザーから提供された DTD を受け付けない。
または、アプリケーションのコンフィギュレーションは、SYSTEM エンティティの解決を行わないコンフィギュレーション。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
</table>

故障の影響および修正	XXE が脆弱であると、攻撃者はローカルマシンまたはサーバーのローカルネットワーク内のアクセス可能なマシンからデータを密かに盗み出せる。可能であれば、DTD 解決を完全に無効にする。DTD が受け入れられた場合、外部（システム）エンティティの解決は、確実に無効にされるべきである。

6.6.2.4. XML エンティティ拡張

項目	記載内容
項目番号	NEDO_WEB_34
項目名	コンテンツの再帰的拡張を許す XML エンティティリファレンスがアプリケーションにある場合、それによりサービス妨害の状態になることがある。
目的	解析されたどの XML も、再帰的エンティティエクスパンションを許さず、パーサがエクスパンドできる対象に妥当な制限を課すことを保証する。
実施タイミング	
想定実施工数	1 時間
前提テスト項目	なし
入力情報	有効なアプリケーションの認証情報
実施条件	1.アクティブなインターネット接続 2.アプリケーションは、リクエストで送られた XML ドキュメントを受け入れる。
確認事項	アプリケーションは、ユーザーから支給された DTD を受け付けない。 または、アプリケーションは、エンティティリファレンスのエクスパンションを制限するか、または無効にする。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除
備考	ツール: (空) BSM #: TMID-18 車両#: N/A 関連する攻撃: N/A

故障の影響および修正	XML エンティティ拡張攻撃は強力なサービス妨害攻撃であり、この攻撃はサーバーCPU およびメモリを多量に消費する。これは、ビジネス機能に深刻な影響を及ぼす。エンティティエクスパンションを無効にするか、シングルレベルの再帰に制限する（つまり、エンティティが定義されていない）と、別のエンティティが含まれるかもしれません。DTD を完全に無効にすると、XXE 攻撃に加えてこのタイプの攻撃も防止する。

6.6.2.5. ディレクトリトラバーサル

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_35</td></tr>
<tr><td>項目名</td><td>攻撃者が、サーバーがそのリソースへのパスをどのように動的に生成しているかをエクスプロイトして、サーバー上のディレクトリまたはファイルのコンテンツに非承認のアクセスを得たときに、ディレクトリトラバーサルが生じる。</td></tr>
<tr><td>目的</td><td>アプリケーションがアクセスするリソースのファイル名やパスの構造に信頼できない入力を含ませることによるファイルシステムへの認証されていないアクセスに対抗する保護</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>2 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>1.有効なアプリケーションの認証情報
2.サーバー上のテストファイルの場所</td></tr>
<tr><td>実施条件</td><td>アクティブなインターネット接続</td></tr>
<tr><td>確認事項</td><td>アプリケーションは厳密なアクセスコントロールを強化し、ファイルアクセスのためのリファレンスのパス名を作成するために使用される入力を検証する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>ディレクトリトラバーサルは、パス名を作成するためにアプリケーションが使用する入力を操作することにより、ファイルシステムへ不正なアクセスを攻撃者に与えることになる。ディレクトリトラバーサルから防護するために、アプリケーションは厳密なアクセスコントロールを強化し、ファイルアクセスのためのインダイレクトオブジェクトリファレンスまたはパス名を作成するために使用されるユーザー入力を検証すべきである。</td></tr>
</table>

6.6.2.6. XML インジェクション

項目	記載内容
項目番号	NEDO_WEB_36
項目名	アプリケーションがユーザー提供の信頼できないデータを、XML シンタックスが入力の一部となるように XML ドキュメントの構造に挿入すると、XML インジェクションは XML ドキュメントを修正できる。
目的	ユーザーデータは、XML ドキュメントの一部として解釈されず、テキスト/データノードまたは属性値の何れかとして使用される適切に使用されることを保証する。
実施タイミング	
想定実施工数	2 時間
前提テスト項目	なし
入力情報	有効なアプリケーションの認証情報
実施条件	アクティブなインターネット接続
確認事項	1.アクティブなインターネット接続 2.アプリケーションは、ドキュメント内部のデータを使い XML ドキュメントを作成する。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除

	公開用資料のため、記載内容を削除
備考	<table><tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr><tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr></table>
故障の影響および修正	XML インジェクションにより、攻撃者は、XML ドキュメントのコンテンツを劇的に変えてしまう可能性がある XML ドキュメントの構造を変更できる。この変更で、当該ドキュメントの処理方法、解釈方法を変える可能性がある。これにより、認証バイパスやコードインジェクションを含むその他の様々な攻撃が導入され得ます。XML ストリングに信頼できない入力を挿入する前に、XML 制御/メタ文字は適切にコード化されているべきである。XML のすべての定義は、アプリケーションサーバー上で行われ、ユーザー提供のコンテンツは、XML ドキュメントの有効なタグや属性の定義には決して使用すべきではない。

6.6.2.7. SQL インジェクション

項目	記載内容
項目番号	NEDO_WEB_37
項目名	ユーザーが提供したデータを静的な SQL クエリストリングへ動的に連結することにより生成された SQL クエリをアプリケーションが実行する。この実装では、データベースは、開発者が意図した SQL シンタックスとユーザーが提供した入力に含まれるすべての SQL シンタックスを区別していない。結果として、静的クエリに挿入された SQL シンタックスを含むすべてのユーザー提供のデータが、解釈され実行される。この結果、攻撃者がターゲットのクエリの構造および意味を意図的に改変する SQL クエリシンタックスをインジェクトできるので、アプリケーションは SQL インジェクションに対して脆弱のままである。
目的	SQL クエリを変更するために SQL インジェクション攻撃を試みる。
実施タイミング	
想定実施工数	2 時間
前提テスト項目	なし
入力情報	有効なアプリケーションの認証情報
実施条件	1.アクティブなインターネット接続 2.アプリケーションは、ユーザーデータを使い SQL クエリを作成する。
確認事項	アプリケーションはユーザーデータをサニタイズし、SQL クエリ内のデータを使用する前にメタ文字を適切にエスケープする。 または、アプリケーションは用意されたステートメントを使用し、ユーザーデータを用意されたステートメントへのパラメータとしてのみ利用する（パラメータ化されたクエリ）。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除

<table>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>SQL インジェクション攻撃により、認証バイパス、永続データの操作、リモートセルのオープニングなどが生じる。パラメータ化されたクエリを持つ予め用意されたステートメントのようなインジェクション対策済みのクエリメカニズムを使用するために、動的結合を使い作成されたすべてのSQL クエリを書き換えます。</td></tr>
</table>

6.6.3. アドバンスド

6.6.3.1. F5 BIG-IP Cookie 情報ディスクロージャ

項目	記載内容
項目番号	NEDO_WEB_38
項目名	アプリケーションは、F5 BIG-IP Cookie を使用している。
目的	悪意のあるユーザーは、BIG-IP Cookie の値をデコードし内部およびリモートサーバーのホスト名の双方が明らかになるようにする。これにより、Web サーバーおよび組織の内部ネットワークに関連する情報が露出される。
実施タイミング	
想定実施工数	0.5 時間
前提テスト項目	なし
入力情報	有効なアプリケーションの認証情報
実施条件	1.アクティブなインターネット接続 2.アプリケーションは、F5 ロードバランサーの後ろにあり、BIG-IP Cookie を含む/露出する。
確認事項	アプリケーションは、BIG-IP Cookie はフィーチャーしない/F5 ロードバランサーの後ろに存在しない。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除
備考	ツール: (空) / BSM #: TMID-18 / 車両#: N/A / 関連する攻撃: N/A

故障の影響および修正	悪意のあるユーザーは、BIG-IP Cookie の値をデコードし内部およびリモートサーバーのホスト名の双方が明らかになるようにする。これにより、Web サーバーならびに組織の内部ネットワークに関連する情報が露出される。HTTP Cookie をクライアントシステムへ送信する前に、HTTP Cookie を暗号化するように BIG-IP LTM システムのコンフィギュレーションを設定する。

1.

6.6.3.2. XPath インジェクション

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_39</td></tr>
<tr><td>項目名</td><td>アプリケーションは、ユーザーデータを使い XPath クエリを作成する。</td></tr>
<tr><td>目的</td><td>XML によりアクセスされる基本的なデータから任意のコンテンツを露出する XPath インジェクション攻撃が防止されているかを判断する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>1.アクティブなインターネット接続
2.アプリケーションは、XPath 表現を使用して XML 構造をクエリする。</td></tr>
<tr><td>確認事項</td><td>A.アプリケーションはユーザーデータをサニタイズし、クエリストリングで使用されていた XPath メタ文字を適切にエスケープする。
B.アプリケーションは、提供されたパラメータに存在するメタ文字を評価しないパラメータ化されたクエリを使用する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>攻撃者は、XPath インジェクションにより XPath クエリを操作できる。この結果として、認証バイパス、センシティブな情報の露出、またはアプリケーションの振る舞いのその他の予想外の変化になる。パラメータ化されたクエリを使用する。および/または入力の厳密な検証を実施する。</td></tr>
</table>

6.6.3.3. 特権の昇格

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_40</td></tr>
<tr><td>項目名</td><td>現在認証されているユーザーアカウントと異なるユーザーアカウントおよびロールレベルに許可されているリソース/機能に、ユーザーがアクセスできる。</td></tr>
<tr><td>目的</td><td>他のサービスユーザーに関連付けられたアカウントに関連する情報を露出またはハイジャックしようとする。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>4 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.1.1</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>1.アクティブなインターネット接続
2.認証メカニズムは、アカウントの機密データを保護する。</td></tr>
<tr><td>確認事項</td><td>データをビューしようとしているリクエストを、またはそのアクションが承認されているアクションの実施を、必ずサーバーサイドで確実に確認して承認する。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>ハッカーは、BMW の VIN を認めます。</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>特権が上がると、攻撃者は、侵入したアカウントへのアクセスレベル次第で様々なアクションを仕掛けてくる。修正には、システムの認定は必ず伴う。データを見ようとしてる、またはアクションを行おうとリクエストをしているユーザーを、必ずサーバーサイドで確実に確認する。</td></tr>
</table>

6.6.3.4. ブラインド SQL インジェクション

項目	記載内容
項目番号	NEDO_WEB_41
項目名	アプリケーションがデータベースエラーまたはデータを直接ユーザーへ反映しないので、この問題は標準的な SQL インジェクションとはわずかに異なっている。これにより、攻撃者はパッシブプロービンブ手法を使い、意図した効果をもつべき SQL シンタックスに対してアプリケーションがどんなレスポンスをするかに基づいて、アプリケーションが脆弱であるかを判断することになる。
目的	元の目的のテキストをここに入れる
実施タイミング	
想定実施工数	2 時間
前提テスト項目	なし
入力情報	有効なアプリケーションの認証情報
実施条件	1.アクティブなインターネット接続 2.アプリケーションは、ユーザーから支給されたデータを使い SQL クエリを作成する。
確認事項	アプリケーションはユーザーデータをサニタイズし、SQL クエリ内のデータを使用する前にメタ文字を適切にエスケープする。または、アプリケーションは用意されたステートメントを使用し、ユーザーデータを用意されたステートメントへのパラメータとしてのみ利用する（パラメータ化されたクエリ）。
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除
備考	ツール: （空）／BSM #: TMID-18／車両#: N/A／関連する攻撃: N/A

	SQLMap				
故障の影響および修正	SQL インジェクションを使い、攻撃者はアプリケーションが実行した SQL クエリの構造を変更できる。パラメータ化されたクエリを持つ予め用意されたステートメントのようなインジェクション対策済みのクエリメカニズムを使用するために、動的結合を使い作成されたすべての SQL クエリを書き換える。				

6.6.3.5. セカンドオーダーSQL インジェクション

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_42</td></tr>
<tr><td>項目名</td><td>信頼できない保管されたデータを静的な SQL クエリストリングへ動的に連結することにより生成された SQL クエリをアプリケーションが実行するとき、セカンドオーダーSQL インジェクションが起こります。この設計では、アプリケーションはクエリに挿入された有効なデータから SQL シンタックスを区分できず、挿入された SQL シンタックスはすべて解釈され実行される。静的なクエリに連結されたデータがローカルなデータソースからリトリーブされるので、これはセカンドオーダー SQL インジェクションの脆弱性を示している。このソースのデータは、クライアントのリクエストから直接的に引き出されたデータではなく、アプリケーションが以前に保存したデータである。</td></tr>
<tr><td>目的</td><td>セカンドオーダーSQL インジェクションの脆弱性が存在するかの確認。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.1.10</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>1.アクティブなインターネット接続
2.アプリケーションは、ユーザーから支給されたデータを使い SQL クエリを作成する。</td></tr>
<tr><td>確認事項</td><td>アプリケーションは用意されたステートメントを使用し、ユーザーデータを用意されたステートメントへのパラメータとしてのみ利用する（パラメータ化されたクエリ）。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>セカンドオーダーSQL インジェクションを使い、攻撃者はアプリケーションが実行した SQL クエリの構造を変更できる。厳密な型が指定されたパラメータ化されたクエリを持つ予め用意されたステートメントのようなインジェクション対策済みクエリメカニズムを使うために、動的結合を使い作成されたすべての SQL クエリおよび保存されているプロシージャーをコールしているすべての SQL クエリを書き換える。</td></tr>
</table>

6.6.3.6. アウトオブバンド XML 攻撃

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_43</td></tr>
<tr><td>項目名</td><td>XXE 攻撃がありファイルをリトリーブできない場合、リモートリソースを利用した攻撃がさらに行われる可能性がある。</td></tr>
<tr><td>目的</td><td>OOB XML 攻撃を使い、サーバーサイドリクエストフォージェリ[SSRF]が実行できるか確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>3 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.2.4</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>1.アクティブなインターネット接続
2.アプリケーションは、XML ドキュメントに対応している。</td></tr>
<tr><td>確認事項</td><td>アプリケーションは、ユーザーから提供された DTD を受け付けない。
または、アプリケーションは SYSTEM エンティティを変更しない。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>N/A</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>アウトオブバンド XML 攻撃の結果、機密データが露出されたり、内部ネットワークへの攻撃を受けやすくなったりする。この両者は、通常の XXE 攻撃と同等の攻撃である。DTD 解決は無効にされているべきである。SYSTEM エンティティ解決も、無効にすることもできる。</td></tr>
</table>

6.6.3.7. 認証バイパス

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_44</td></tr>
<tr><td>項目名</td><td>予想される認証プロセスがバイパス可能であるかを判断する。</td></tr>
<tr><td>目的</td><td>潜在的な攻撃者が、必要なアカウントデータの詳細を提示せずにアプリケーションの認証を得られるかを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>2 時間</td></tr>
<tr><td>前提テスト項目</td><td>項目 6.6.1.1</td></tr>
<tr><td>入力情報</td><td>なし</td></tr>
<tr><td>実施条件</td><td>1.アクティブなインターネット接続
2.機密データに該当する URL のリスト</td></tr>
<tr><td>確認事項</td><td>A.匿名ログインは拒否される。
B.アカウントに関連したパスワードなしでのログインは拒否される。
C.無効なログインエントリーおよび SQL インジェクションペイロードは、拒否される。
D.ログインは何度も繰り返されたら、そのアカウントはロックされる。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>セクション. 2.1.6
2.1.2、2.1.3、2.1.6</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>ウェブサービスの認証は、そのアンダーラインコードの範囲でのみ有効とされる。攻撃者は、認証によりサイトに設けられている制約をバイパスするために一般的なタイプの攻撃を使用とする。認証が正しく実装されていることを保証するために、強い強度のセキュリティフレームワークが必要である。SQL インジェクションに対向するために、認証フレームワークは保存してある手順を使うべきであり、ロジックに潜在する欠陥を緩和する助けとなる方法を持っているべきである。</td></tr>
</table>

6.6.3.8. アドバンストパスワード変更バイパス

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_45</td></tr>
<tr><td>項目名</td><td>パスワード変更機能が提供されている場合、現在のパスワードの検証が行われる必要がある。</td></tr>
<tr><td>目的</td><td>ユーザーが、現在の認証情報に関する知識を持たずにアカウントに関連するパスワードを変更できるかどうかを判断する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>1.アクティブなインターネット接続
2.パスワードの変更機能がユーザーから見える。</td></tr>
<tr><td>確認事項</td><td>ユーザーはパスワード変更プロセス中に、変更したいパスワードに加えて現在の認証情報の再入力を求められる。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>NA</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>認証中に現在のパスワードを要求せずに、ユーザーにパスワード変更を許すと、攻撃者は、犠牲者のパスワードを変更できるようになり、犠牲者のアカウントへ継続的にアクセスできるようになる。アプリケーションはユーザーの現在の認証情報、例えば現在のパスワードなどを要求して、パスワードの変更プロセス中にその ID を検証する必要がある。</td></tr>
</table>

6.6.3.9. Open URL リダイレクト

<table>
<tr><th>項目</th><th>記載内容</th></tr>
<tr><td>項目番号</td><td>NEDO_WEB_46</td></tr>
<tr><td>項目名</td><td>アプリケーションは、ユーザーのブラウザを信頼できないデータを使い作成された URL へリダイレクトする。</td></tr>
<tr><td>目的</td><td>攻撃者がコントロールしている場所に、ユーザーがリダイレクトされないことを確認する。</td></tr>
<tr><td>実施タイミング</td><td></td></tr>
<tr><td>想定実施工数</td><td>1 時間</td></tr>
<tr><td>前提テスト項目</td><td>なし</td></tr>
<tr><td>入力情報</td><td>有効なアプリケーションの認証情報</td></tr>
<tr><td>実施条件</td><td>1.アクティブなインターネット接続
2.アプリケーションは、HTTP リダイレクションレスポンスを返す。</td></tr>
<tr><td>確認事項</td><td>A.ユーザー入力データは、リクエスト先のリソースを定義していない。
B.リダイレクトを行う前に、ホワイトリストを使い作成された URL が正当なものであると確認されている。</td></tr>
<tr><td>評価レポートのフォーマット</td><td></td></tr>
<tr><td>実施例</td><td>公開用資料のため、記載内容を削除</td></tr>
<tr><td>備考</td><td>
<table>
<tr><th>ツール</th><th>BSM #</th><th>車両#</th><th>関連する攻撃</th></tr>
<tr><td></td><td>TMID-18</td><td>NA</td><td>N/A</td></tr>
</table>
</td></tr>
<tr><td>故障の影響および修正</td><td>Open URL リダイレクションにより、攻撃者は犠牲者を自分のコントロールしているサイトにリダイレクトできる。攻撃者がこのサイトを完全にコントロールしているので、攻撃者はこのサイトを使い悪意のあるアクションを何回でも実行できる。信頼できないデータを使い作成された URL は、リダイレクトする前にドメインホワイトリストを使い正当なものであると確認されているべきである。ビジネス上から正当性が未確認である先にリダイレクトが必要である場合は、アプリケーションは、リダイレクトを行う前にユーザーに承認を求めるべきである。</td></tr>
</table>

6.7. セルラー（LTE）（プレースホルダ）

本書の作成とは、別にこのセクションに入るべき内容を準備しています。このセクションに入るべき内容は、バージョン 4.0 で挿入されます。

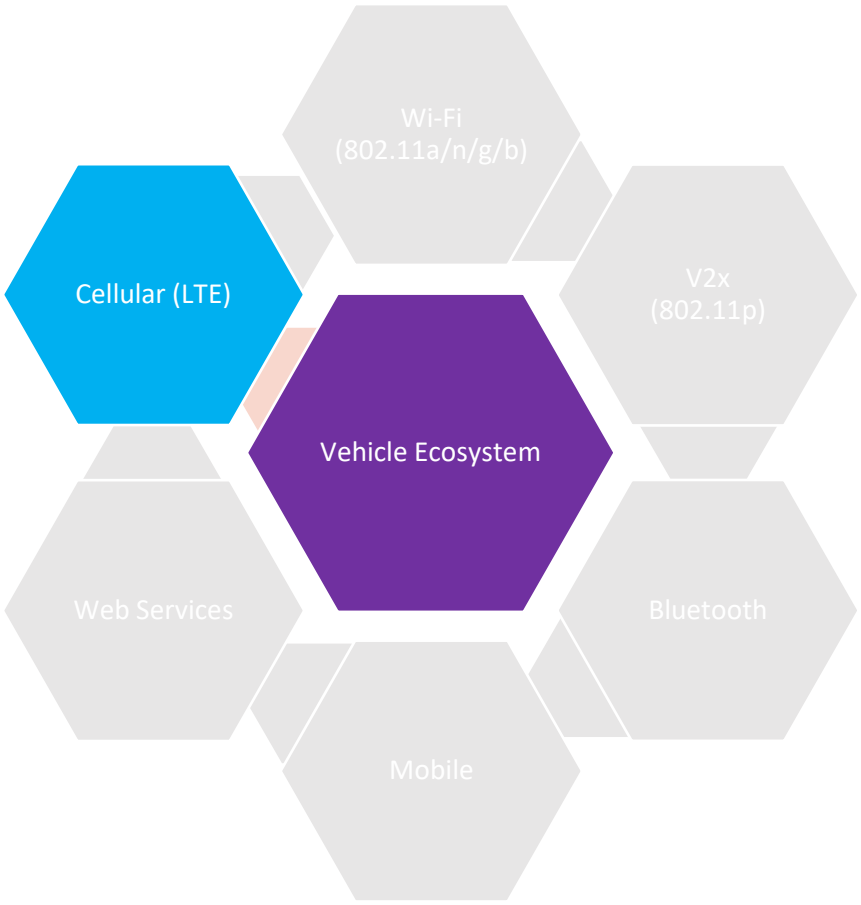


図 14：セルラー（LTE）のサブコンポーネントカテゴリーをハイライト

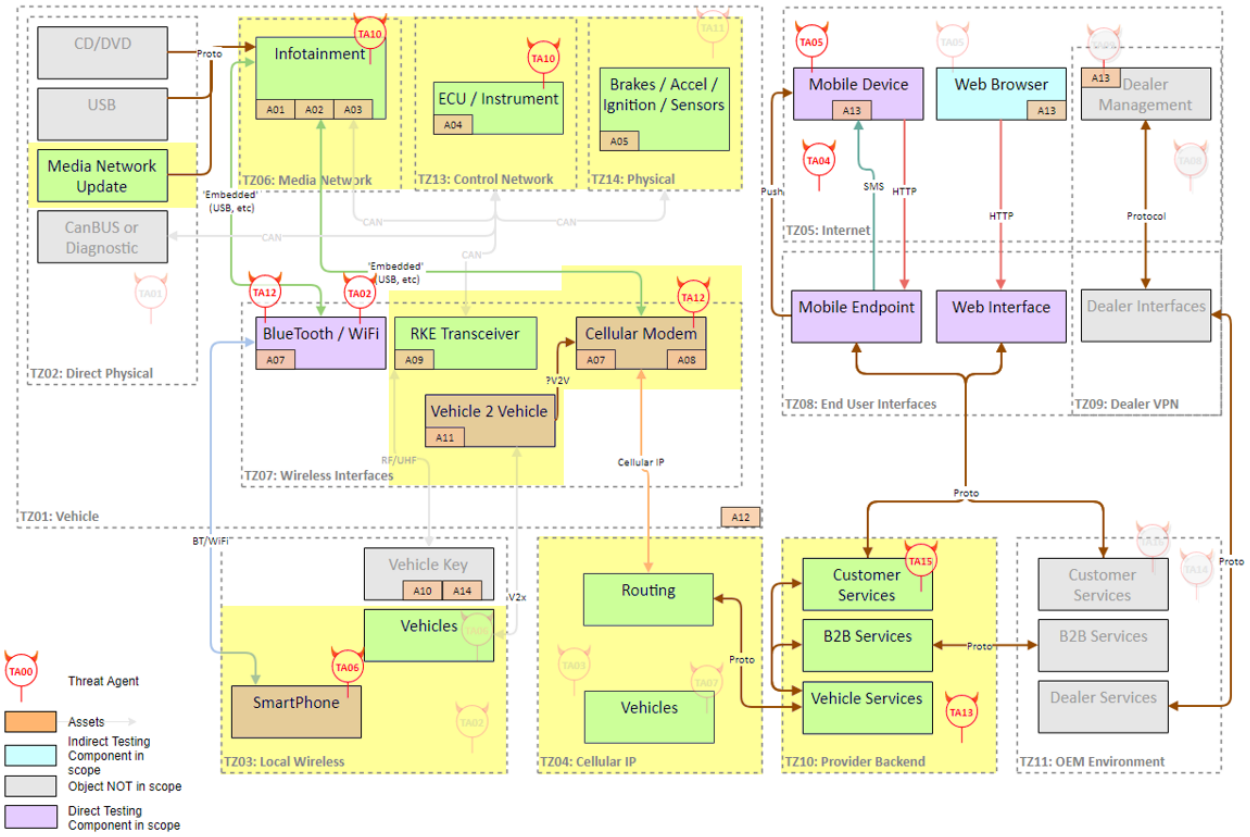


図 15：セルラー（LTE）の範囲内の項目に対する直接的なテストの影響

6.7.1. 必須

6.7.1.1. ネットワーク機能の確認：対応プロトコルとサービス

項目	記載内容
項目番号	NEDO_LTE_01
項目名	ネットワーク機能の確認：対応プロトコルとサービス
目的	ターゲット車両のセルラ通信インターフェース上のオープンポート上で動作しているサービスを検出する
実施タイミング	
想定実施工数	数時間
前提テスト項目	
入力情報	・　②-13：オープンポートのリスト　（別紙：セルラ通信機能セキュリティ評価ガイドライン参照のこと）
実施条件	シミュレータ接続環境
確認事項	・　セルラ通信インターフェース上のオープンポートで稼動しているサービスのリスト
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除

	公開用資料のため、記載内容を削除
備考	

6.7.1.2. ネットワーク機能の確認：TCP/IP 通信データ

項目	記載内容
項目番号	NEDO_LTE_02
項目名	ネットワーク機能の確認：TCP/IP 通信データ
目的	
実施タイミング	
想定実施工数	1 日以内
前提テスト項目	
入力情報	
実施条件	シミュレータ接続環境
確認事項	・ セルラ通信を用いる機能（サーバ機能、クライアント機能）の一覧 ・ 平文で通信される認証情報・秘匿情報 ・ 認証機能が施されているサーバ機能 ・ クライアント機能のアクセス先、等
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除

	公開用資料のため、記載内容を削除
備考	

6.7.1.3. ネットワーク機能の確認：SMS 通信/音声通信によるアクセス確認

項目	記載内容
項目番号	NEDO_LTE_03
項目名	ネットワーク機能の確認： SMS 通信/音声通信によるアクセス確認
目的	
実施タイミング	
想定実施工数	1 日以内
前提テスト項目	
入力情報	②-09：ターゲットに割り当てられた電話番号　（別紙：セルラ通信機能セキュリティ評価ガイドライン参照のこと）
実施条件	実網接続環境
確認事項	・ターゲットに対する SMS 及び音声通話によるアクセス可否
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除

備考	

6.7.1.4. 認証機能：脆弱な認証方式

項目	記載内容
項目番号	NEDO_LTE_04
項目名	認証機能：脆弱な認証方式
目的	
実施タイミング	
想定実施工数	数時間
前提テスト項目	
入力情報	・　②-15：サーバ機能に実装されている認証機能のリスト ・　②-15：平文で送受信されている認証情報のリスト （別紙：セルラ通信機能セキュリティ評価ガイドライン参照のこと）
実施条件	シミュレータ接続環境
確認事項	・　平文若しくは容易に解読可能なエンコードにより認証情報を送受信している認証機能が存在しないかを確認する ・　チャレンジレスポンス方式を用いている認証機能に脆弱性が存在しないかを確認する ・　その他の認証方式を用いている認証機能に脆弱性が存在しないかを確認する
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除

	公開用資料のため、記載内容を削除
備考	

6.7.1.5. 認証機能：認証バイパス

項目	記載内容
項目番号	NEDO_LTE_05
項目名	認証機能：認証バイパス
目的	
実施タイミング	
想定実施工数	1 日以内
前提テスト項目	
入力情報	・　②-15：認証機能のリスト ・　②-15：認証後にアクセス可能なリソース （別紙：セルラ通信機能セキュリティ評価ガイドライン参照のこと）
実施条件	シミュレータ接続環境
確認事項	・　認証をバイパスし、アクセス可能なサーバ機能のリソースが存在しないかを確認する
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除

	公開用資料のため、記載内容を削除
備考	

6.7.1.6. 認証機能：認証情報の解析

項目	記載内容
項目番号	NEDO_LTE_06
項目名	認証機能：認証情報の解析
目的	
実施タイミング	
想定実施工数	数日以上（ハッシュに対するブルートフォースを実施する場合）
前提テスト項目	
入力情報	・　②-15：認証機能のリスト ・　②-10 等：認証情報ファイル（パスワードハッシュ） （別紙：セルラ通信機能セキュリティ評価ガイドライン参照のこと）
実施条件	シミュレータ接続環境
確認事項	・　パスワードハッシュより解析可能な認証情報（パスワード）が存在しないかを確認する
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除

	公開用資料のため、記載内容を削除
備考	

6.7.1.7. セキュア通信：脆弱なセキュア通信方式の検出

項目	記載内容
項目番号	NEDO_LTE_07
項目名	セキュア通信：脆弱なセキュア通信方式の検出
目的	
実施タイミング	
想定実施工数	数時間
前提テスト項目	
入力情報	・　②-15：セキュア通信箇所 （別紙：セルラ通信機能セキュリティ評価ガイドライン参照のこと）
実施条件	
確認事項	・　TLS/SSL 機能において、脆弱なプロトコルバージョンをサポートしていないか、及び脆弱な暗号スイートをサポートしていないかを確認する
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除

	公開用資料のため、記載内容を削除
備考	公開用資料のため、記載内容を削除 ・　IPA「SSL 3.0 の脆弱性対策について(CVE-2014-3566)」

	https://www.ipa.go.jp/security/announce/20141017-ssl.html ・ JVN iPedia「JVNDB-2011-002305 SSL と TLS の CBC モードに選択平文攻撃の脆弱性」 http://jvndb.jvn.jp/ja/contents/2011/JVNDB-2011-002305.html

6.7.1.8. セキュア通信：証明書検証の不備

項目	記載内容
項目番号	NEDO_LTE_08
項目名	セキュア通信：証明書検証の不備
目的	
実施タイミング	
想定実施工数	数時間
前提テスト項目	
入力情報	・　②-15 で検出されたセキュア通信箇所 （別紙：セルラ通信機能セキュリティ評価ガイドライン参照のこと）
実施条件	
確認事項	・　証明書検証の不備がある TLS/SSL クライアント機能が存在しないかを確認する
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除

	公開用資料のため、記載内容を削除
備考	公開用資料のため、記載内容を削除

6.7.1.9. セキュア通信：再送攻撃耐性

項目	記載内容
項目番号	NEDO_LTE_09
項目名	セキュア通信：再送攻撃耐性
目的	
実施タイミング	
想定実施工数	数時間
前提テスト項目	
入力情報	・ ②-15：セキュア通信箇所 ・ ②-16：通信キャプチャ （別紙：セルラ通信機能セキュリティ評価ガイドライン参照のこと）
実施条件	
確認事項	・ ターゲット車両のセルラ通信インターフェース上で動作しているサーバ機能のうち、TLS/SSL 以外の方式により暗号化された通信を受け付けるものについて、再送攻撃に対する脆弱性が存在しないかを確認する
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除
備考	・ 前提として、暗号化されていない通信については基本的に再送攻撃が可能であるため、ここでの確認対象から除外している

6.7.1.10. 既知脆弱性：動的スキャンによる検出

項目	記載内容
項目番号	NEDO_LTE_10
項目名	既知脆弱性：動的スキャンによる検出
目的	
実施タイミング	
想定実施工数	数時間
前提テスト項目	
入力情報	・　②-13：オープンポートのリスト （別紙：セルラ通信機能セキュリティ評価ガイドライン参照のこと）
実施条件	
確認事項	・　脆弱性スキャナにより、ターゲット車両のセルラ通信機能の既知脆弱性を検出する
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除

	公開用資料のため、記載内容を削除
備考	・ Web アプリケーションに限定した脆弱性スキャナについては、以下のサイト等を参照のこと OWASP: Vulnerability Scanning Tools https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools

6.7.1.11. 既知脆弱性：静的情報による検出

項目	記載内容
項目番号	NEDO_LTE_11
項目名	既知脆弱性：静的情報による検出
目的	ターゲット車両のセルラ通信機能に関連するソフトウェア情報から、既知脆弱性を検出する
実施タイミング	
想定実施工数	1 日以内
前提テスト項目	
入力情報	・　②-02：OS やソフトウェア種別及びバージョン番号のリスト ・　②-14：セルラインターフェース上で稼動しているサービスのリスト （別紙：セルラ通信機能セキュリティ評価ガイドライン参照のこと）
実施条件	
確認事項	・　ソフトウェアのバージョン情報などから、攻撃可能な脆弱性情報及び攻撃コードを探索する ・　発見された攻撃コードが実際に有効であるかを確認する
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除

	公開用資料のため、記載内容を削除
備考	・ CVE 情報検索サイトの例 ➢ NVD：National Vulnerability Database https://nvd.nist.gov/vuln/search ➢ CVE details https://www.cvedetails.com/ ・ 攻撃コード検索サイト セキュリティスキャナによりウィルスと判定されるデータも登録されているため、アクセスや検索の際は注意が必要 ➢ Exploit-DB https://www.exploit-db.com/

	➢ Packet Storm https://packetstormsecurity.com/ ➢ Vulnerability LAB https://www.vulnerability-lab.com/search.php · metasploit https://www.metasploit.com/

6.7.1.12. 入力値処理不備：インジェクション脆弱性の検出

項目	記載内容
項目番号	NEDO_LTE_12
項目名	入力値処理不備：インジェクション脆弱性の検出
目的	セルラ通信を用いるサービスにおいて、各種インジェクション脆弱性を検出する
実施タイミング	
想定実施工数	数時間～（確認実施箇所の数に依る）
前提テスト項目	
入力情報	
実施条件	
確認事項	・　セルラ通信側で起動しているサービスについて、各種インジェクションの脆弱性の確認をする
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除

	公開用資料のため、記載内容を削除

	公開用資料のため、記載内容を削除
備考	・ OWASP Testing for SQL Injection (OTG-INPVAL-005) https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OTG-INPVAL-005) ・ OWASP Testing for HTTP Splitting/Smuggling (OTG-INPVAL-016) https://www.owasp.org/index.php/Testing_for_HTTP_Splitting/Smuggling_(OTG-INPVAL-016) ・ OWASP Testing for IMAP/SMTP Injection (OTG-INPVAL-011) https://www.owasp.org/index.php/Testing_for_IMAP/SMTP_Injection_(OTG-INPVAL-011) ・ OWASP Testing for Command Injection (OTG-INPVAL-013) https://www.owasp.org/index.php/Testing_for_Command_Injection_(OTG-INPVAL-013)

6.7.1.13. 入力値処理不備：Fuzzing

項目	記載内容
項目番号	NEDO_LTE_13
項目名	入力値処理不備：Fuzzing
目的	
実施タイミング	
想定実施工数	数時間～（テスト実施箇所の数及び実施件数に依る）
前提テスト項目	
入力情報	・　②-15：セルラ通信を用いる機能（サーバ機能、クライアント機能）の一覧 （別紙：セルラ通信機能セキュリティ評価ガイドライン参照のこと）
実施条件	
確認事項	・　入力データ処理における脆弱性を検出する
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除

	公開用資料のため、記載内容を削除
備考	

6.7.1.14. SMS：偽装 SMS メッセージによる不正制御

項目	記載内容
項目番号	NEDO_LTE_14
項目名	SMS：偽装 SMS メッセージによる不正制御
目的	
実施タイミング	
想定実施工数	1 日以内
前提テスト項目	
入力情報	・　②-09：ターゲット車両のセルラ通信機能に割り当てられた電話番号 ・　②-09：ターゲット車両が受信する SMS メッセージデータ （別紙：セルラ通信機能セキュリティ評価ガイドライン参照のこと）
実施条件	
確認事項	・　SMS メッセージの偽装により、ターゲット車両/モジュールを不正に制御できないかを確認する
評価レポートのフォーマット	
実施例	公開用資料のため、記載内容を削除
備考	

7. 付録

7.1. 参考文書および標準/規格

このセクションは、本書が最終バージョンに成り次第、最終的なものとなります。バージョン 2 によれば、以下の外部文書が本書内で引用されています。

Blommendaal, C. (2015). *Information Security Risks for Car Manufacturers based on the In-Vehicle network.* University of Twente.

Byman, G. (2017). *CONNECTED DEVICES: SECURITY THREATS VS IMPLEMENTED SECURITY.* University of Oulu.

DANIEL FALLSTRAND, V. L. (2015). *Applicability analysis of intrusion detection and prevention in automotive systems.* Sweden: University of Technology Goteborg.

(2001). *DEDICATED SHORT-RANGE COMMUNICATION SYSTEM.* ARIB STANDARD.

Greenberg, A. (2015, October 09). GM Took 5 Years to Fix a Full-Takeover Hack in Millions of OnStar Cars. *Wired*.

Karl Koscher, A. C. (2010). *Comprehensive Experimental Analyses of Automotive Attack Surfaces.* Oakland: IEEE Symposium on Security and Privacy.

Ludovic Apvrille, R. E. (2010). Secure automotive on-board electronics network architecture. *World Automotive Congress* (p. 49). Budapest: FISITA.

Olovsson, P. K. (2013). Protecting Vehicles Against Unauthorised Diagnostics Sessions Using Trusted Third Parties. *In Computer Safety, Reliability, and Security*, 70-81.

peter Schwabe, S. v. (2016). *Secure updates in automotive systems.* Rabound University 2016.

Roderick Currie, M. S. (2015). *Developments in Car Hacking.* 2015: GIAC (GSEC) Gold Certification.

Schweppe, H. (2012). *Security and privacy in automotive on-board networks.* Paris: Networking and Internet Architecture.

sintsov, A. (2016). *yacht - yet Another Car Hacking tool.* London: BlackHat.

Weinmann, R.-P. (2012). *Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks.* Luxembourg: University of Luxembourg.

Winsen, S. v. (2017). *Threat Modelling for Future Vehicles, On Identifying and Analysing Threats for Future Autonomous and Connected Vehicles.* Enschede: University of Twente.

1. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Spec
2. S. K. Miller. “Facing the challenge of wireless security”
3. S. Fluhrer, I. Mantin, and A. Shamir. “Weaknesses in the key scheduling algorithm of RC4
4. Bittau, M. Handley, and J. Lackey. “The Final Nail in WEP’s Coffin”
5. Amendment 6: Medium Access Control (MAC) Security Enhancements. IEEE Std 802.11i.
6. Practical attacks against WEP and WPA
7. https://lirias.kuleuven.be/bitstream/123456789/401042/1/wpatkip.pdf
8. S. Checkoway, D. McCoy, .et .al, “Comprehensive Experimental Analyses of Automotive Attack Surfaces”
9. http://papers.mathyvanhoef.com/blackhat2017.pdf
10. https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_vanhoef.pdf
11. https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013
12. https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

SYNOPSYS®

「戦略的イノベーション創造プログラム(SIP)自動走行システム／大規模実証実験」のうち「情報セキュリティ実証実験」

c 情報セキュリティ評価試行調査報告書

SYNOPSYS®

エグゼクティブサマリ

SYNOPSYS®

1　はじめに

日本シノプシス合同会社 ソフトウェア・インテグリティ・グループは、国立研究開発法人 新エネルギー・産業総合開発機構（以下、「NEDO」と記載）「情報セキュリティ実証実験」プロジェクト（以下、「プロジェクト」と記載）の一環

公開用資料のため、記載内容を削除

1.1　目的

プロジェクトにおいて作成した評価ガイドライン 1st ドラフト（以下、「評価ガイドライン」と記載）を使用して、実際の車両コンポーネントシステムについて評価を行うことで、ガイドラインの有効性確認に加え、車両または車両システムのセキュリティ評価を実施します。また、評価結果を踏まえ、評価ガイドラインの修正も行います。

公開用資料のため、記載内容を削除

1.2　スコープ

セキュリティ評価は日本シノプシス合同会社内にて実施しました：

日本シノプシス合同会社
東京都世田谷区玉川 2-21-1
二子玉川ライズオフィス

策定された評価ガイドラインの評価内容、手順、環境を利用して、対象となる車両システムの検証を実施します。評価対象は下記の通りです：

公開用資料のため、記載内容を削除

下記行為や対象は、スコープ外とします。

- ハードウェア改竄
- USB
- 物理アクセスによる攻略行為
- サーバー関連の脆弱性評価

SYNOPSYS®

2　メソドロジー

2.1　評価アプローチ

公開用資料のため、記載内容を削除

2.2　リスク・レベル

個々の技術的リスクを特定した後、悪用の可能性とビジネス目標およびリスクへの影響により決定される深刻度に基づいて優先度付けを行います。

リスク値は、技術リスクがネットワーク・インフラストラクチャに及ぶ危険性を表し、以下の表に基づき算定します。

表 1: NIST SP800-30 脆弱性マトリクスを参考にしたリスク

		影響レベル (Impact)				
		非常に低い	低い	中間	高い	非常に高い
可能性(Likelihood)	非常に高い	非常に低い	低い	中間	高い	非常に高い
	高い	非常に低い	低い	中間	高い	非常に高い
	中間	非常に低い	低い	中間	高い	高い
	低い	非常に低い	低い	低い	中間	中間
	非常に低い	非常に低い	非常に低い	非常に低い	低い	低い

2.2.1 可能性 (Likelihood)

脆弱性悪用の難易度は、スキルレベルと脆弱性の存在を疑われる要素への必要なアクセス回数に依存します。難易度は、下記レベルにレイティングします：

- **非常に高い**: 攻撃者が脅威イベントを開始することはほぼ確実。
- **高い**: 高スキルではない脅威アクターが悪用できる可能性がある、または、脆弱性の存在が明白で容易にアクセス可能。
- **中間**: 脆弱性悪用には一定以上のハッキング知識が要求される、または、何らかの方法でアクセスが制限されている。
- **低い**: 脆弱性を悪用するには、アプリケーションへのアクセス、重要な時間、リソース、または特別なスキルセットが必要である。
- **非常に低い**: この脆弱性を悪用される可能性はほとんどない。

2.2.2 影響レベル (Impact)

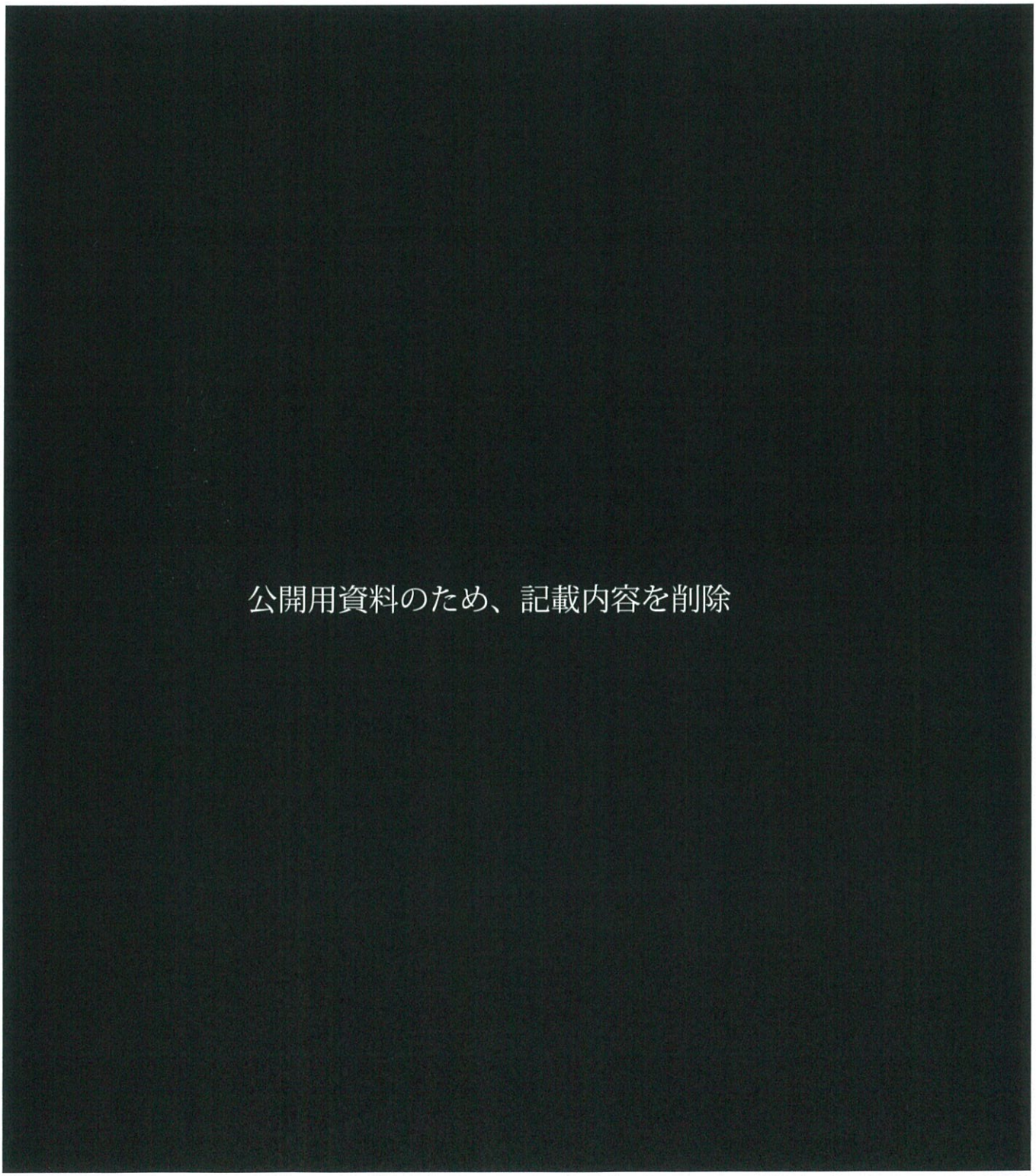
脆弱性が悪用された場合の組織に対する影響レベルを、下記レベルにレイティングします：

- **非常に高い**: 組織の業務、組織の資産、または他の組織に対して複数の重大または致命的な影響を与える。
- **高い**: 組織が主要な機能を遂行できないレベル、組織資産に損害を与えるレベルまでのミッション遂行能力の著しい低下をもたらす。
- **中間**: 主要機能の遂行は可能な程度までミッション遂行能力の低下を引き起こすが、有効性が低下することで組織資産に損害が生じる可能性がある。
- **低い**: ミッション遂行能力の限定的な低下をもたらす。すなわち、組織はその主要機能を実行することができるが、有効性の低下により、組織資産に軽微な損害をもたらす可能性がある。
- **非常に低い**: 組織の業務や組織の資産に対して無視できる悪影響を与える可能性がある。

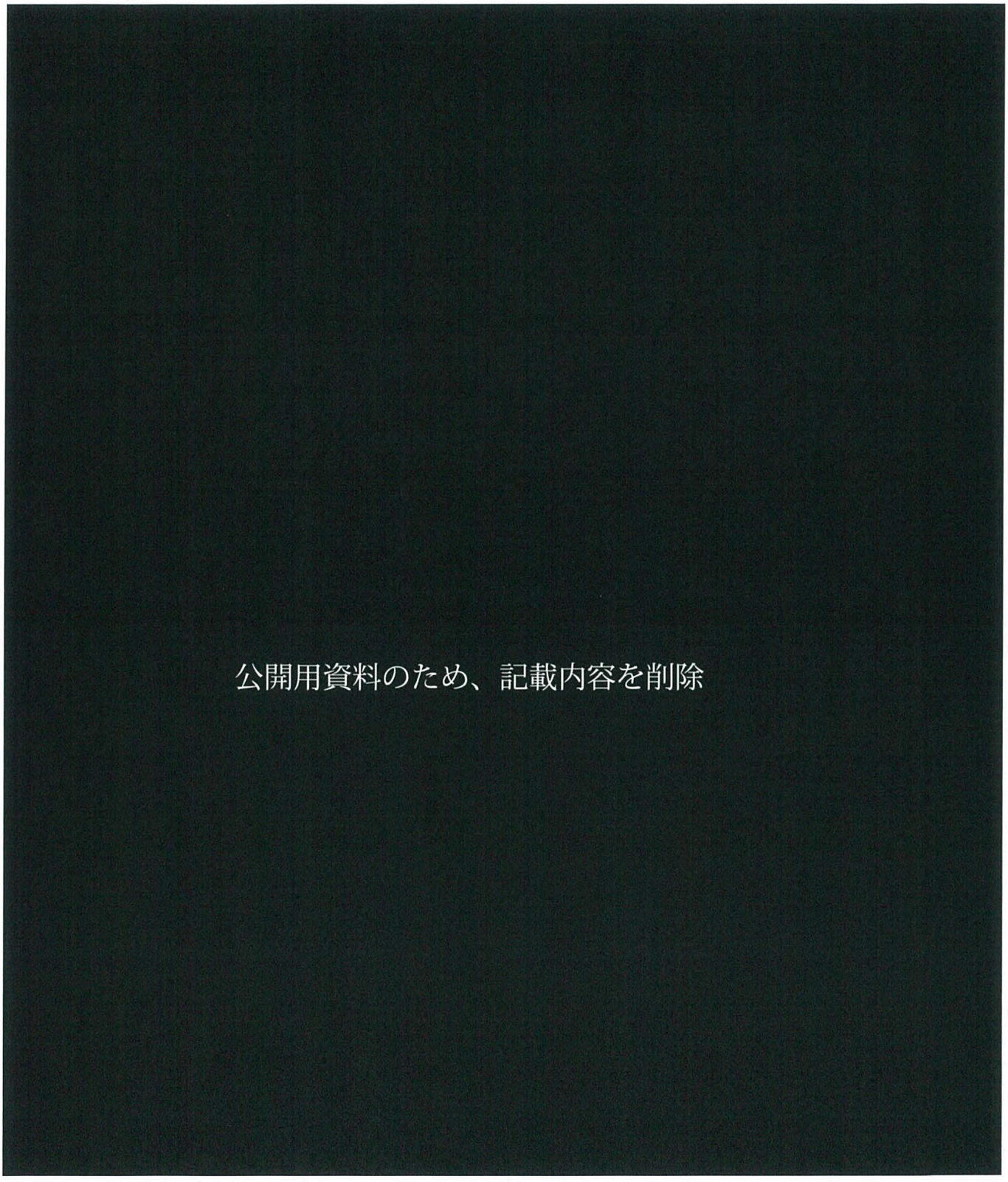
SYNOPSYS®

3 調査結果

3.1 サマリ



3.2 調査結果詳細



SYNOPSYS®

4 Appendix

4.1 Test Items Applicable

公開用資料のため、記載内容を削除

- **Type** = Testing Technology Type
- **Test Case Name** = Name of the Test Case in NEDO Security Guidelines v4
- **NEDO Framework ID** = ID of test name as under "Test Item ID" field in v4
- **Section** = Section number of Test Case in NEDO Security Guideline v4
- **M/R/A** = Mandatory, Recommended or Advanced Type Categorisation of Test Item

公開用資料のため、記載内容を削除

Type	Test Case Name	NEDO Framework ID	Section	M/R/A
WI-FI	Identification of Wireless Communication Defaults	NEDO_WIFI_1	6.2.1.1	M
WI-FI	Unencrypted Communications & Data Content	NEDO_WIFI_2	6.2.1.2	M
WI-FI	Eavesdropping (Sniffing)	NEDO_WIFI_3	6.2.1.3	M
WI-FI	Evaluation of Implementation of Secure Protocols	NEDO_WIFI_5	6.2.1.5	M
WI-FI	Discovery of Exposed Network and Services	NEDO_WIFI_6	6.2.1.6	M
WI-FI	Encryption Downgrade Attack	NEDO_WIFI_7	6.2.2.1	R
WI-FI	Determine Predictability of Group Encryption Keys	NEDO_WIFI_8	6.2.2.2	R
WI-FI	Identification of software (source)	NEDO_WIFI_10	6.2.2.4	R
WI-FI	Channel-Based MITM	NEDO_WIFI_11	6.2.3.1	A
WI-FI	Fuzzing Enumerated Web Services	NEDO_WIFI_12	6.2.3.2	A
WI-FI	Fuzzing Telnet	NEDO_WIFI_13	6.2.3.3	A
WI-FI	Fuzzing SSH	NEDO_WIFI_14	6.2.3.4	A
WI-FI	Fuzzing HTTP	NEDO_WIFI_15	6.2.3.5	A
WI-FI	Fuzzing Data over Network Protocols	NEDO_WIFI_16	6.2.3.6	A
WI-FI	Identification of Weak Configurations	NEDO_WIFI_17	6.2.3.7	A
WI-FI	Identification of out of date wireless services	NEDO_WIFI_18	6.2.3.8	A
WI-FI	Identification of software (source)	NEDO_WIFI_20	6.2.3.10	A
WI-FI	WIDS/WIPS Detection	NEDO_WIFI_21	6.2.3.11	A
WI-FI	Unauthenticated Network Access Check	NEDO_WIFI_22	6.2.3.12	A
WI-FI	Unauthenticated Data Exfiltration	NEDO_WIFI_23	6.2.3.13	A
Bluetooth	Identification of Bluetooth Devices	NEDO_Bluetooth_1	6.4.1.1	M
Bluetooth	Identification of Bluetooth Profiles	NEDO_Bluetooth_2	6.4.1.2	M
Bluetooth	Identification of Bluetooth implementation Vulnerabilities	NEDO_Bluetooth_3	6.4.1.3	M
Bluetooth	Identifying Unlisted Bluetooth Profiles	NEDO_Bluetooth_4	6.4.1.4	M
Bluetooth	Unencrypted Bluetooth Communication	NEDO_Bluetooth_5	6.4.1.5	M
Bluetooth	Simple Pin security on Bluetooth pairing	NEDO_Bluetooth_6	6.4.1.6	M
Bluetooth	Testing the effects of DOS on Bluetooth	NEDO_Bluetooth_7	6.4.2.1	R
Bluetooth	Spoofing Bluetooth device	NEDO_Bluetooth_8	6.4.2.2	R
Bluetooth	Blueborne	NEDO_Bluetooth_9	6.4.2.3	R
Bluetooth	Bluetooth MITM	NEDO_Bluetooth_10	6.4.3.1	A
Bluetooth	Advanced Pin security on Bluetooth pairing	NEDO_Bluetooth_11	6.4.3.2	A

公開用資料のため、記載内容を削除

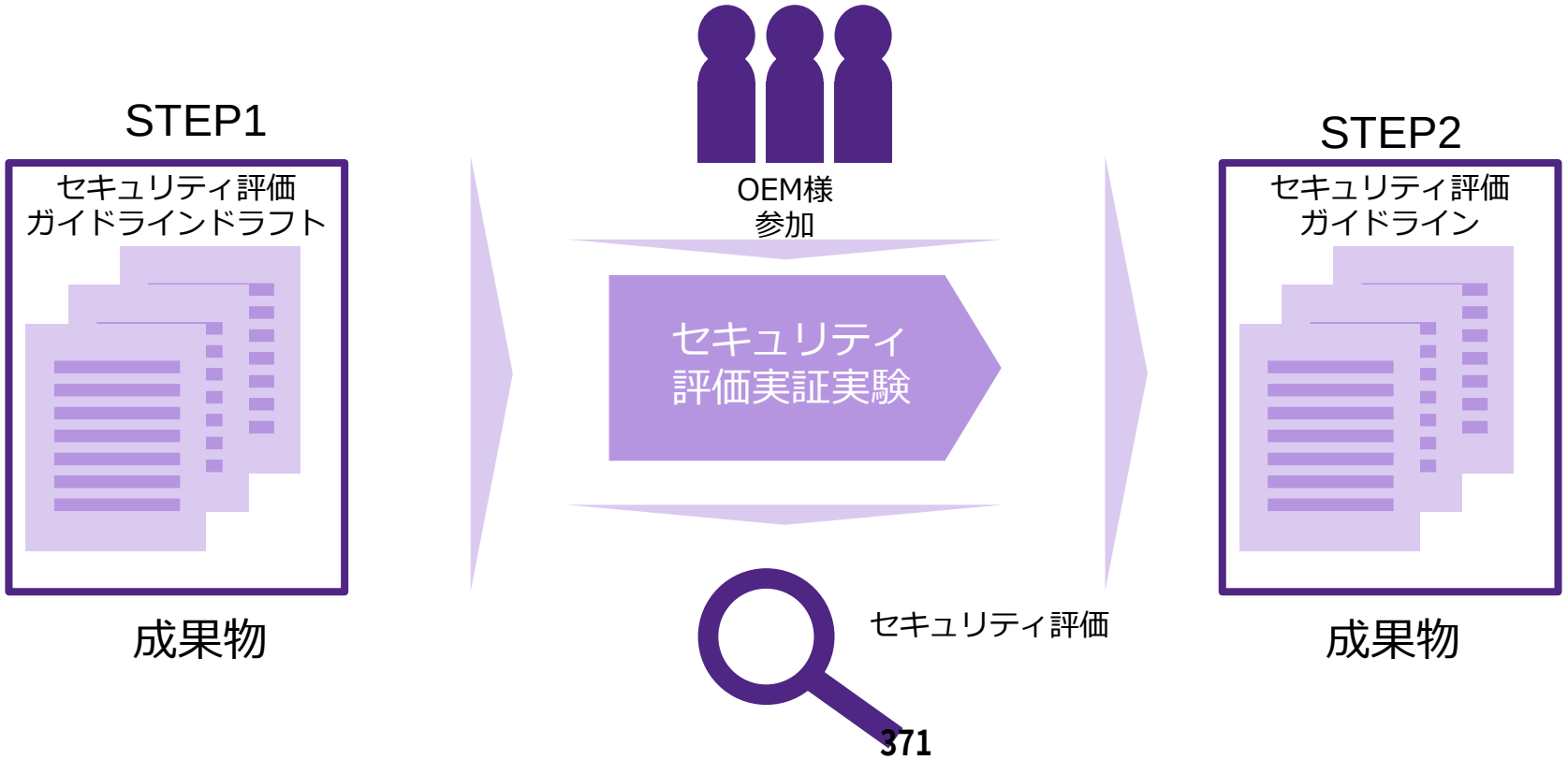
Bluetooth	Unauthorized Access Vehicle Devices	NEDO_Bluetooth_12	6.4.3.3	A
Bluetooth	Identify Bluetooth firmware implementation errors	NEDO_Bluetooth_13	6.4.3.4	A
Mobile	Copy/Paste of Sensitive Fields	NEDO_Mobile_1	6.5.1.1	M
Mobile	Compiler Settings Checks - Development	NEDO_Mobile_2	6.5.1.2	M
Mobile	Compiler Settings Checks - Production	NEDO_Mobile_3	6.5.1.3	M
Mobile	App Entitlements/Permissions Check	NEDO_Mobile_4	6.5.1.4	M
Mobile	Hardcoded Sensitive Information	NEDO_Mobile_5	6.5.1.5	M
Mobile	Custom Keyboards Disabled	NEDO_Mobile_6	6.5.1.6	M
Mobile	Debug Prevention - Development	NEDO_Mobile_7	6.5.1.7	M
Mobile	Local Authentication Brute Force Attacks	NEDO_Mobile_8	6.5.1.8	M
Mobile	No Authentication Required After Background Resume	NEDO_Mobile_9	6.5.1.9	M
Mobile	Application Logs Sensitive Data	NEDO_Mobile_10	6.5.1.10	M
Mobile	Certificate Validation	NEDO_Mobile_12	6.5.1.12	M
Mobile	Certificate Pinning	NEDO_Mobile_13	6.5.1.13	M
Mobile	Binary Obfuscation - Development	NEDO_Mobile_14	6.5.1.14	M
Mobile	Information Leakage	NEDO_Mobile_15	6.5.1.15	M
Mobile	Application Allows Backups	NEDO_Mobile_16	6.5.1.16	M
Mobile	Third Party Library Checks	NEDO_Mobile_17	6.5.2.1	R
Mobile	Cryptography Checks	NEDO_Mobile_18	6.5.2.2	R
Mobile	Application Communications Channel Security Testing	NEDO_Mobile_19	6.5.2.3	R
Mobile	Command Injection	NEDO_Mobile_20	6.5.3.1	A
Mobile	Sensitive Data stored on device	NEDO_Mobile_21	6.5.3.2	A
Mobile	Application File Permissions	NEDO_Mobile_22	6.5.3.3	A
Mobile	GUI Bypass	NEDO_Mobile_23	6.5.3.4	A
Mobile	Android IPC Checks	NEDO_Mobile_25	6.5.3.6	A
Mobile	Binary Obfuscation - Production	NEDO_Mobile_26	6.5.3.7	A
Mobile	Certificate Pinning Bypass	NEDO_Mobile_27	6.5.3.8	A
Mobile	Debug Prevention - Production	NEDO_Mobile_28	6.5.3.9	A
Web	Verify Authentication Scheme Exists	NEDO_WEB_1	6.6.1.1	M
Web	Verbose Server Banner	NEDO_WEB_7	6.6.1.7	M
Web	HTTPS Enabled/Enforced	NEDO_WEB_8	6.6.1.8	M

「戦略的イノベーション創造プログラム(SIP)自動走行システム／大規模実証実験」のうち「情報セキュリティ実証実験」

d.来期実証実験の運営準備

実証実験概要

自動走行システムの社会実装に向けて、攻撃者視点で車両レベルでのセキュリティ評価ガイドラインを策定しました（STEP1）。そして、実証実験として複数車両等を用いてSTEP1で作成したガイドラインを検証し、セキュリティ評価ガイドラインを確立します。（STEP２）



実証実験の進め方

A.実証実験への参加募集と選定	B.提供車両および業務契約等の締結	C.セキュリティ評価（約2か月間/車両を想定）	D.クロージング
・国内OEMを対象として、車両システムのセキュリティ評価実証実験参加者の募集を行います。 ・実証実験の実施概要を参照いただきます。 ・希望者は、参加要領にご記入いただき応募いただきます。	・提供車両に係る諸条件について2社間での合意形成を調整します。 ・提供車両の実装状況と準備等から業務契約書を作成します。 ①無線通信実装状況 ②車両準備状況 ③評価範囲の定義 ④体制と運営方法 ⑤スケジュール	次の順に作業を実施します。 ①開始時ミーティング ②環境構築 ③車両システム分析 ④評価開始 ⑤評価結果情報整理 ⑥レポート作成 ⑦報告会開催 ⑧評価終了	契約内容に基づきて、検収を行います。 また、2社間で、次の内容を確認します。 ・借用物の返却 ・取得情報の破棄 サインオフをして終了します。

A.実証実験への参加募集と選定

4月上旬（募集開始）	4月末（エントリ締切）	5月以降（諸条件調整）
参加エントリの依頼 参加エントリー数により、対応ができない可能性があります。	セキュリティ評価実施について、NEDO殿との選定実施	対象、非対象の無線通信インタフェースの確認
実証実験参加応募に関する説明会の開催。 ・応募要領 ・契約関連 ・実施項目の説明 ・実施環境の説明	車両システムの無線通信インタフェースの実装状況により、セキュリティ評価工数の積算 （評価可能な項目を整理）	・契約書（セキュリティ評価実施） ・借用物等の取り扱いに関する事項 ・セルラー通信等による関連するサービスの利用に係る事項
期間中の質問対応		

参加者へのお願い事項

	C-① 開始ミーティング	C-② 環境構築	C-③ 車両システム分析	C-④評価実施 C-⑤評価結果情報整理 C-⑥レポート作成	C-⑦報告会開催 C-⑧評価終了
物資的お願い事項	・車両システム 無線通信（WiFi, Bluetooth, LTEのいずれかを有する車） ・運搬に係る費用 ・車両故障等の対応体制	・車両操作に関する事前説明 ・車両に係るマニュアル等の情報提供	・車両故障時等の車両または交換部品の提供	・車両故障時等の車両または交換部品の提供	・車両等の搬出 ・運搬に係る費用 ・借用物の返却手続き対応
支援のお願い事項	評価に係る支援体制 ・窓口担当者 ・車両システム不具合にかかる対応体制 ・手続き等の対応	環境構築に係る支援体制	・車両に係る問い合わせ対応 ・車両故障等に関する修復作業 ・車両システムに関する問い合わせ対応	・車両に係る問い合わせ対応 ・車両故障等に関する修復作業 ・車両システムに関する問い合わせ対応	報告会へ参画 ・車両システム関係者 ・終了手続き

B.提供車両および業務契約等の支援スケジュール

		お願い事項	開始前	開始	+1週間	+2週間	+3週間	+4週間	+5週間	+6週間	+7週間	+8週間	+9週間
i.ご提供いただきたいもの	i-①	車両のご提供		▲									
	i-②	車両関連マニュアル一式		▲									
	i-③	セルラーを利用するサービス等		▲									
	i-④	インフォティメイント利用のモバイルアプリケーションのバイナリ		▲									
ii.セキュリティ評価時の支援	ii-①	車両操作方法の説明（必要な事前設定等）	→										
	ii-②	契約交渉（作業範囲、車両利用条件、NDA等）	→										
	ii-③	車両利用時の問い合わせ対応（HW/SW）			平日9:30-17:30の電話またはメールでの問い合わせ対応のお願い →								
	ii-④	車両システム故障時の復旧対応			平日9:30-17:30の故障時の復旧対応。問い合わせから〇日以内の復旧 ⇢								

想定：1.5時間

想定：2か月間

想定：３時間/週

事象に依存

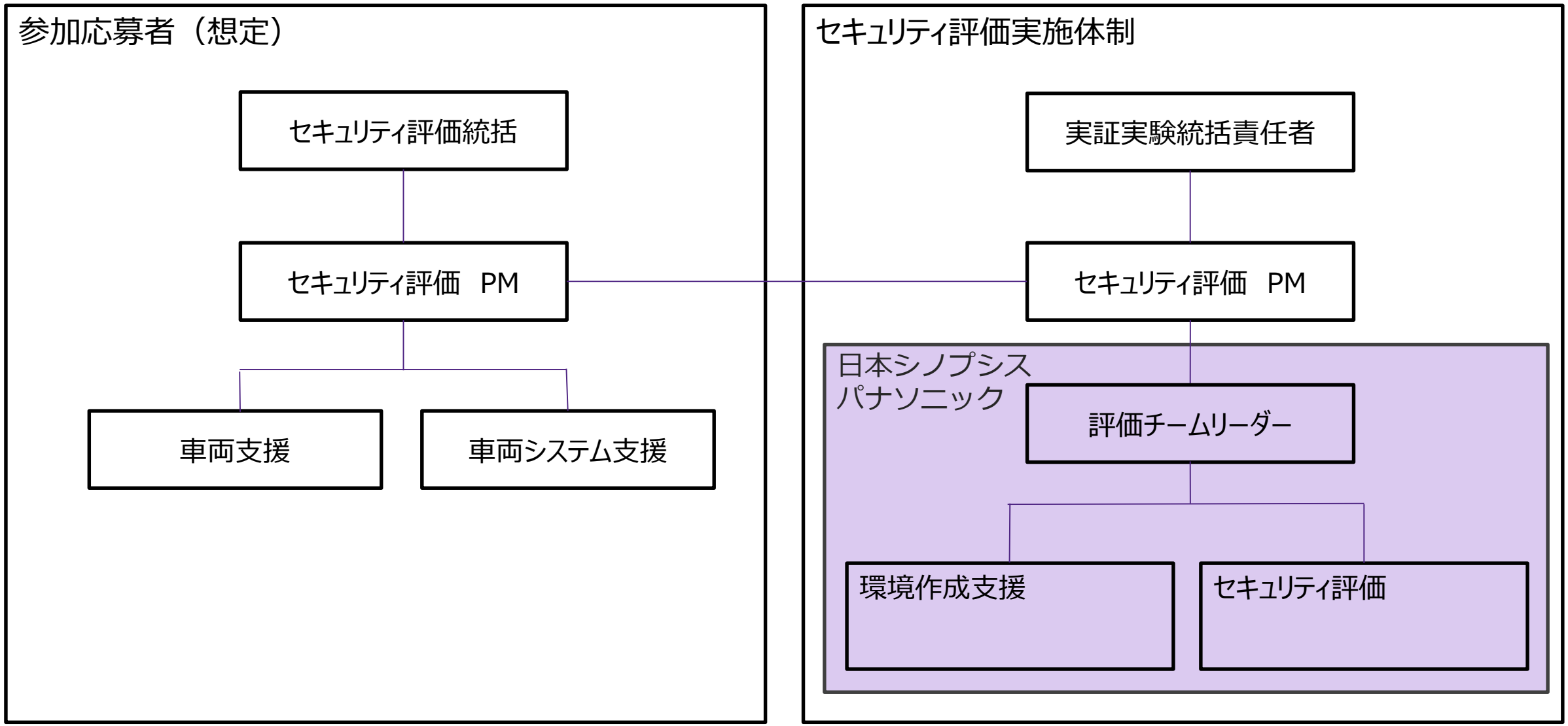
C.セキュリティ評価

①開始ミーティング	②環境構築	③車両システム分析	④評価実施 ⑤評価結果情報整理 ⑥レポート作成	⑦報告会開催 ⑧評価終了
実証実験の進め方について合意を図ります。 ・作業項目の説明 ・役割分担 ・支援依頼内容の合意 ・情報提供依頼 ・借用物の確認 ・スケジュール	車両格納先の準備 ・借用車両の搬入計画 ・実験環境確認 - 電源、ネットワーク利用 - 安全確認 - セキュリティ - セルラー利用方法 ・車両操作方法	セキュリティ実証実験開始に伴い ・車両システムに関する情報収集 - ヘッドユニット - サービス利用 - WiFi、BT、LTE	評価ガイドラインに従いセキュリティ評価を実施 ・WiFi ・BT ・LTE ・その他	報告会の開催 ・セキュリティ評価結果について報告 検出した脆弱性またはその可能性のあるものについて説明します。考えられる対策方法の解説を含めてします。

D.クロージング

- 評価実施時のオペレーションにおいて、セキュリティ評価ガイドラインへの反映
- NEDO委員会への実験結果サマリ報告（NEDO殿と調整要）
- 実証実験終了時の情報の破棄

実証実験　実施体制



情報セキュリティ管理

- セキュリティ管理体制・方法の確立
  - シノプシス　倫理・業務規定　（ Code of Ethics ）
    - 3.6 プライバシーおよび個人情報
    - 4.6 シノプシスの資産および機密情報の使用および保護
    - 4.7 効果的な記録管理および書類保持

参考）https://www.synopsys.com/content/dam/synopsys/company/corporate-governance/code-ethics-business-conduct-2017-japanese.pdf

  - グローバルのセキュリティポリシー、スタンダード、プロシージャをもって運用を実施

  - 情報の取り扱いに関するセキュリティ
    - 全ての社員は、機密情報の取り扱いについてオンライントレーニングを受講。完了状況を監視。
    - 社員は、情報漏洩対策済みのパソコンを利用。
      - ハードディスクの暗号化、クラウドストレージ・メールアクセス不可等。

結び（総括および結論）

実施契約書で定義された、a)脅威分析調査、b)情報セキュリティ評価ガイドラインドラフトの作成、c)情報セキュリティ評価の試行調査、d)実証実験の運営準備の４つの項目について十分な調査ができた。特に、b)情報セキュリティ評価ガイドラインドラフトの作成に関しては、実際の使用を想定し、使用し易い工夫を施すことが出来た。また、a)脅威分析調査に関しても、全体像の把握、具体的な公知の自動車メーカ等の事例情報に基づく脅威の類型化をすることが出来た。

２．研究発表・講演、文献、特許等の状況

(1)研究発表・講演

特になし

(2)文献

特になし

(3)特許等

特になし

(4)その他の公表（プレス発表等）

特になし

契約管理番号	17101426-0