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
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

平成 30 年　2 月

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　PwC コンサルティング合同会社

要約（和文）

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

このような課題を解決するため、「戦略的イノベーション創造プログラム　自動走行システム／大規模実証実験　情報セキュリティ実証実験」では、自動走行におけるセキュリティ脅威の調査/分析を行い、国際標準化も見据えた車両レベルでのセキュリティ評価手法・プロトコルを策定し、本実証実験を通して募る参加者の実車両システムを用いて対ハッキング性能検証のためのブラックボックステストの実施が計画されている。

本年度の事業においては、平成 30 年度での実証実験の実施に向けた事前調査として、「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」の調査活動を行い、事前調査結果としてまとめた。

「a.脅威分析調査」については、自動走行に係る V2X 等車外からの攻撃を含む脅威の全体像の整理し、自動走行車両セキュリティに関するコンセンサスの醸成を目的として調査分析した。脅威の全体像を整理するにあたり、初めに自動車メーカ、部品サプライヤ、IT 企業などの自動運転・コネクテッドカーに係る取り組みをファクトベースで調査し、整理・類型化することで自動走行システム共通モデルを導出した。続いて、導出した自動走行システム共通モデルをベースに WP29 などの車両関係およびセキュリティ研究者による脅威分析結果をもとにして、V2X 等車外からの攻撃を含む脅威項目を抽出し、脅威項目ごとに車両システムにおける影響度評価を実施した。影響度評価の結果、特に重大な脅威については、対策状況を調査し、必要に応じて別途作成した評価ガイドラインに反映した。

「b.情報セキュリティ評価ガイドラインドラフトの作成」については、車両 OEM 各社等のステークホルダーとの議論の結果を踏まえて、車両開発の V 字モデルにおける総合評価などで活用できるガイドラインとする方針とし、ガイドラインドラフト版として策定した。本ガイドラインの評価手法の特徴として、1. 実際のハッカー（攻撃者）の視点とした車両外部 I/F から侵入テストによる評価 2. 現実の車両インシデント事例を考慮し、HW セキュリティ耐性評価を盛り込んだこと、の 2 点が挙げられる。さらに、評価項目の選定にあたっては、既知の車両セキュリティインシデントにおける攻撃者のプロファイルを分析し、攻撃者が高度な技術レベルや設備を持つ場合もカバーする評価内容として策定した。これにより、本ガイドで策定した評価を実施することにより、既知の車両セキュリティ被害と同種の問題の発生を防止することができる。

「c. 情報セキュリティ評価の試行調査」では、策定した評価ガイドラインドラフトを用いて、実際の車両部品システムに対して評価を行い、評価ガイドラインの妥当性の確認と修正を行った。合わせて、車両部品システム提供者に対して、評価内容、評価実施手順、評価結果、対策提案をまとめて評価レポートとして提出し、対象車両のセキュリティ品質向上にも寄与した。本評価内容は車両部品システム提供者との取り決めにより、評価結果は未公開とするが、システム提供者のご厚意もあり、評価実施内容の一部を公開することができた。

「d. 実証実験の運営準備」では、平成 30 年度の実証実験の実施計画を立案し、実証実験参加プロトコル、実証実験情報管理手法、実証実験環境などを整理した。また、実証実験の円滑な推進のために、実証実験参加者に周知および合意すべき事項を明らかにし、参加者募集要項、参加規約、各種契約文書案などを用意した。実証実験参加者への重要な依頼事項の 1 つに、評価対象車両ないしシステムの提供があるが、これら評価対象の用意については車両 OEM 各社との議論を通じて内容を調整し、実証実験情報セキュリティ評価の実施に必要な要件を満たしつつ、車両 OEM 各社の負担を可能な限り最小限とする実現性を考量した内容にできた。

要約（英文）

High precision map information, mapping information of vehicles, pedestrians and infrastructures as basis of automated driving systems are expected to be obtained mainly from external network. The obtained information will be transmitted to control/information devices of the vehicle to be used for its control in automated driving system. However such situation could cause cybersecurity issues that did not exist for conventional automobiles.

In order to solve such issues, “SIP Large-scale Field Operational Test for Automated Driving Systems / Information Security Field Operational Test” plans to conduct research/analysis on security threats, establish security evaluation method/protocol for vehicles towards international standardization as well as black box testing to verify anti-hacking performances of vehicle systems provided by the project participants.

In this project, as research activities prior to the field operational test in 2018, “a. Threat Analysis”, “b. Development of Information Security Evaluation Guideline Draft”, “c. Information Security Evaluation Trial“, “d. Preparation for Management of Field Operational Test” were conducted and the research results were summarized.

“a.Threat Analysis Research” clarified the whole picture of threat against automated driving system including attacks from outside of the vehicle such as V2X to foster public consensus regarding security of automated driving vehicles. Research and analysis were conducted for the activities related to the automated driving/connected car promoted by automotive manufacturers, suppliers and IT companies etc. to develop common model for the automated driving system. Based on the common model and results of threat analysis by researchers related to vehicle and security such as WP29, threat items including attack from outside of the vehicle such as V2X were extracted and impact evaluation regarding vehicle system was conducted.

Based on impact evaluation results, countermeasures for significant threats were identified, and as necessary, reflected to the evaluation guideline developed separately.

In “b. Development of Information Security Evaluation Guideline”, draft version of the guideline was developed directing towards use in comprehensive evaluation in V model of the vehicle development process based on the results of discussion with stakeholders such as OEM etc. Two characteristics of evaluation method of this guideline are 1. Evaluation by intrusion test from vehicle’s external interface from actual hacker (attacker)’s point of view, 2. Included hardware security evaluation based on actual vehicle security incidents. Furthermore, evaluation items were selected to cover cases when attackers have highly advanced technical capabilities, equipment and/or facilities. Therefore by using this guideline, similar incidents to known vehicle security incidents can be prevented.

In “c. Information Security Evaluation Trial“, Information Security Guideline Draft was verified and checked through evaluation for actual vehicle component system. In addition, an evaluation report summarizing the procedure, contents, results and countermeasures was submitted to provider of the vehicle component system and contributed to security quality improvement of the provided vehicles. Modified version of the evaluation result was disclosed by the courtesy of the provider as the entire evaluation result cannot be disclosed due to the agreement with the vehicle component provider,

In “d. Preparation for Management of Field Operational Test”, an implementation plan for the field operational test in 2018 was developed and participation protocol, information management method and test environment etc. were arranged. Also, in order to conduct the field operational test smoothly, some matters have to be acknowledged and agreed by the participants were clarified and application requirements, terms and conditions for participation and other related contract drafts were documented. Through discussion and arrangements with the OEMs, practical conditions were defined regarding vehicle or system to be provided to require minimum obligations for the participants while meeting necessary requirements for conducting field operational test for information security evaluation.

まえがき

本報告書は、戦略的イノベーション創造プログラム自動走行システム／大規模実証実験　情報セキュリティ実証実験の実施に向けた事前調査として、自動走行におけるセキュリティ脅威の調査/分析および国際標準化も見据えて車両レベルでのセキュリティ評価手法・プロトコル策定の活動結果についてまとめたものである。また、セキュリティ評価手法の検証として実施した評価の試行調査の結果および平成 30 年度の実証実験の計画立案の内容についてもまとめている。

目次

1　事業概要

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

このような課題を解決するため、「戦略的イノベーション創造プログラム　自動走行システム／大規模実証実験　情報セキュリティ実証実験」においては、自動走行におけるセキュリティ脅威の調査/分析を行い、国際標準化も見据えて車両レベルでのセキュリティ評価手法・プロトコルを策定し、本実証実験を通して募る参加者の実車両システムを用いて対ハッキング性能検証のためのブラックボックステストを行うことによる技術調査を行うことが計画されている。

本年度の事業においては、平成 30 年度での実証実験の実施に向けた事前調査として、「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」の調査活動を行い、事前調査結果としてまとめた。

2　本事業の構成

本事業の構成は以下のとおりである。

事業フェーズ	取り組み	主な成果物
実証前調査	*脅威分析調査*	• *将来の自動走行モデルの全体像* • *上記に対する脅威の全体像*
	評価ガイドラインドラフトの作成	• *評価ガイドラインドラフト（初版および第2版）*
	情報セキュリティ評価の試行調査	• *評価ガイドラインを用いた実車両システム評価* • *評価ガイドラインの妥当性評価および見直し*
	実証実験の運営準備	• *実証実験実施計画（スケジュール）* • *実証実験参加プロトコル（フローチャート等）* • *参加者募集要領（要領、規約、申込書、契約書類）* • *参加者募集説明実施要領、説明資料* • *実証実験情報管理手法、体制案*

図 2-1　本事業の構成

第 3 章にて「a. 脅威分析調査」の活動である、自動走行システムの共通モデルおよび脅威の全体像の整理の結果をまとめる。第 4 章にて、「b.情報セキュリティ評価ガイドラインドラフトの作成」に関して評価ガイドラインの位置づけや評価アプローチをまとめる。なお、本報告書には策定したガイドライン自体は含んでいない。第 5 章にて、「c. 情報セキュリティ評価の試行調査」の実施結果のうち、車両部品システムの提供者との協議で公開許可をいただいた内容についてまとめる。第 6 章にて「d. 実証実験の運営準備」として、平成 30 年度実証実験の計画および準備内容についてまとめる。

3　脅威分析調査

3.1.　脅威分析調査の目的とスコープ

目的

自動走行に係る V2X 等車外からの攻撃を含む脅威の全体像の整理し、自動走行車両セキュリティに関するコンセンサスの醸成を支援すること

スコープ

I. 脅威分析調査	**自動走行システム共通モデル調査**	• 自動車メーカ、部品サプライヤ、IT企業などの自動運転・コネクテッドカーに係る取り組みをファクトベースで調査し、整理・類型化することで自動走行システム共通モデルを導出する
	脅威の全体像調査	• 自動走行システム共通モデルに係る、V2X等車外からの攻撃を含む脅威項目を抽出する • 脅威項目ごとに影響度評価を実施し、特に重大な脅威については、対策状況を調査し、必要に応じて別途作成する評価ガイドラインに反映する

3.2.　脅威分析調査の進め方

脅威分析調査は「自動走行システム共通モデル調査」「脅威の全体像調査」の大きく 2 つのフェーズに分けて実施する。

以下、脅威分析調査の各フェーズの進め方の概略を示す。

自動走行システム共通モデル調査

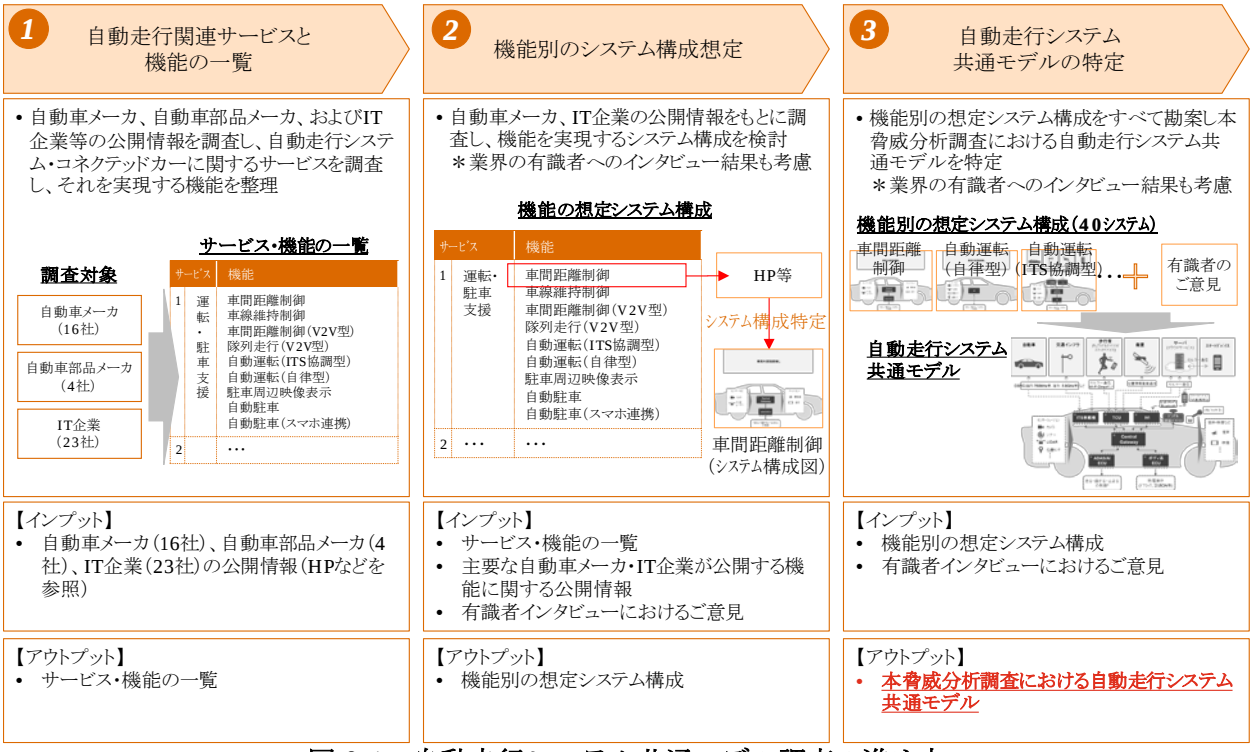


図 3-1　自動走行システム共通モデル調査の進め方

脅威の全体像調査

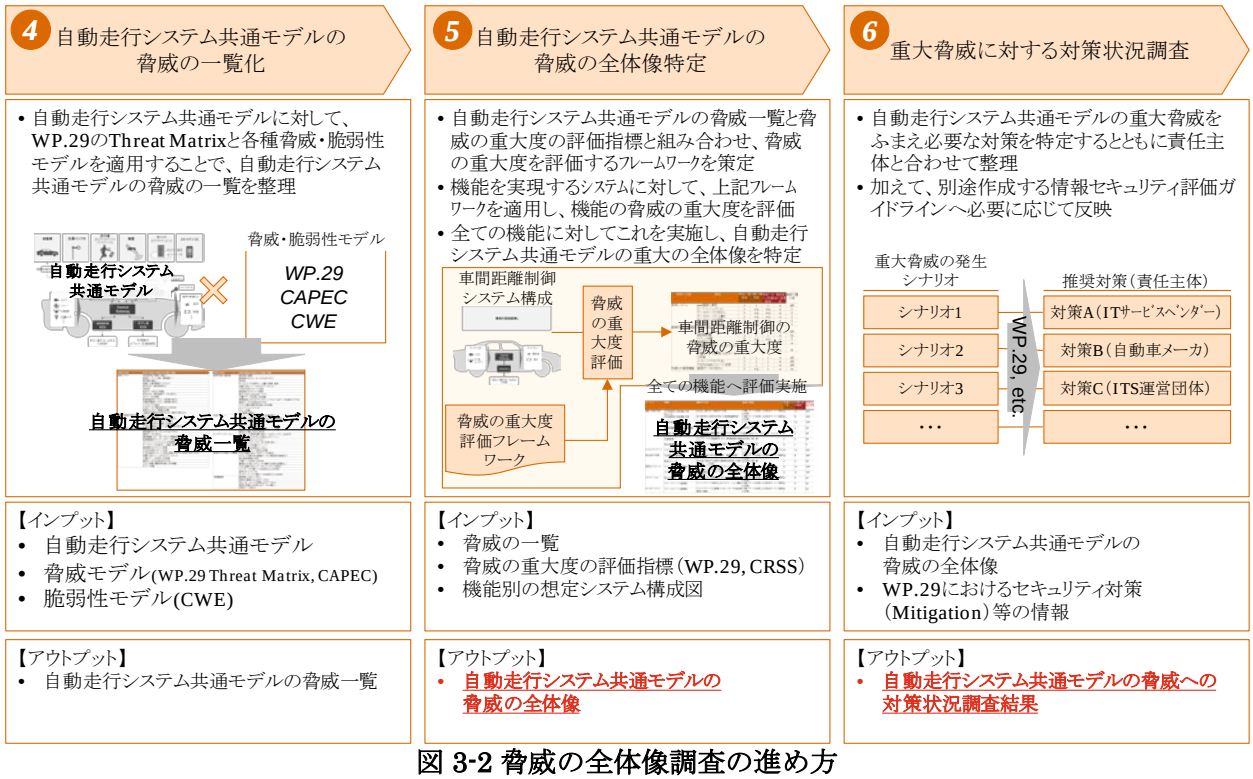


図 3-2 脅威の全体像調査の進め方

3.3. 自動走行システム共通モデル調査

3.3.1. 自動走行関連サービスと機能の一覧化

自動走行システム共通モデル調査の第 1 ステップとして、自動走行関連サービスと機能の一覧化を行う。調査手順は、自動車メーカ、自動車部品メーカ、および自動走行車両を開発する IT 企業を調査し、自動走行システムやコネクテッドカーに係るサービスとそれを実現する機能を整理した。

以下に調査対象会社を一覧に示す。

調査対象会社・団体

- 自動車メーカ
  BMW, Daimler, Fiat Chrysler Automobiles, Ford, Freightliner Trucks, GM, Hyundai, Volkswagen/Audi, Volvo, Tesla,トヨタ, 日産, ホンダ, マツダ, 日野,三菱ふそう
- 自動車部品メーカ
  Continental, DENSO, パイオニア
- 自動走行車両を開発するIT企業
  Alibaba, Baidu, EasyMile, Faraday Future, LeEco Group, Local Motors, NAVYA, Next Future Transportation, Otto, RDM Group, Waymo(Google), ZMP, Lyft, nuTonomy, Uber, DeNA, Aimotive, Delphi.ai, FiveAI, Innoviz Technologies, Intel, Mobileye, NVIDIA

調査の結果整理した、サービスおよびサービスを実現する機能を以下に示す。

サービス			機能		
名称		内容	名称		内容
1	運転・駐車支援	自動車の走行・駐車を支援するサービス	1-1	車間距離制御	ITSと協調せずに先行車両との車間距離を制御する機能
			1-2	車線維持制御	ITSと協調せずに走行車線を維持する機能
			1-3	車間距離制御（ITS協調型）	ITSと協調し先行車両との車間距離を制御する機能
			1-4	隊列走行	先頭車両と通信を行うことで後続車が無人で先頭車両を追従する機能（トラックなど商用車向け）
			1-5	自動運転（ITS協調型）	ITSと協調することで人間に代わりあらゆる運転タスクを実施する機能
			1-6	自動運転（自律型）	ITSと協調することなく、内蔵するセンサーフュージョンを活用することで、人間に代わりあらゆる運転タスクを実施する機能
			1-7	駐車周辺映像表示	車両を駐車する周辺の映像を表示することで人間による車両の駐車を支援する機能
			1-8	自動駐車	内蔵するセンサーフュージョンを活用することで、人間に代わり車両の駐車を実施する機能
			1-9	自動駐車（スマホ連携）	スマートフォンにインストールされたアプリケーション経由で車両の操作指示を行うことで、遠隔からの車両の自動駐車を実施する機能
2	安全走行支援	自動車の安全走行を阻害する状態を検知・警告・回避するサービス	2-1	緊急ブレーキ	歩行者や接近する車両・障害物を検知した際に、音声/表示による運転者に警告、必要に応じた自動でブレーキを実施する機能
			2-2	歩行者検知（V2P型）	歩行者の所有するスマートデバイスと連携し、車両の近くにいる歩行者を検知することで、必要に応じて車両を制御し歩行者との衝突を回避する機能
			2-3	注意喚起（ITS協調型）	協調型ITSを活用した路車間通信システムにより、周辺環境の情報を提供することで、右折時注意・赤信号注意などの各種注意喚起を実施する機能
3	省燃費走行支援	燃費効率の良い走行を支援するために、アクセルワークを制御するサービス	3-1	省燃費走行支援	（左記の内容に同じ）（商用車向け）
4	車両遠隔操作	遠隔地からの操作により自動車に備わる制御システムを制御するサービス	4-1	遠隔からのﾄﾞｱﾛｯｸ・ｱﾝﾛｯｸ	スマートデバイスなどと連携し、遠隔地より車両のドアのロック・アンロックを制御する機能
			4-2	充電制御	スマートデバイスと連携し、遠隔地より充電状況の管理（充電率の把握、充電停止等）を制御する機能
			4-3	充電制御（音声認識AI連携）	音声認識AIエージェントと連携し、遠隔地より充電状況の管理（充電率の把握、充電停止等）を制御する機能
			4-4	エアコン制御	スマートデバイスと連携し、遠隔地よりエアコンのオン・オフを制御する機能
			4-5	エアコン制御（ 音声認識AI連携）	音声認識AIエージェントと連携し、遠隔地よりエアコンのオン・オフを制御する機能
			4-6	エンジン再駆動・ステアリングロック解除禁止	オーナーの要請に基づき、エンジンの再始動・ステアリングロックの解除の禁止を実施する機能
5	故障検知	自動車に備わる自己診断機能を活用し、故障を予知・検知するサービス	5-1	故障検知	（左記の内容に同じ）
6	ナビゲーション	目的地へ到着するための経路情報を提供するサービス	6-1	ルート検索	目的地へのルート検索（最短・最安ルートの検索）などを実施する機能
			6-2	オペレータサービス	オペレーターがドライバーをサポートするコンシェルジュ機能（に口頭で情報検索、検索結果の配信依頼など）
7	エンタテイメント	車内において娯楽などを提供するサービス	7-1	カレンダー・メール同期	ITサービスベンダーのサービスと連携し、カレンダーやメール等の内容のIVIシステムへの表示・読み上げ等を実施する機能
			7-2	SNS連携	ITサービスベンダーのSNSと連携し、その内容をIVIシステムへ表示する機能
			7-3	Wi-Fiスポット	IVIシステムをWi-Fiホットスポットとして活用することで、乗員にインターネットにアクセスを提供する機能
			7-4	各種アプリケーション利用	・・・
8	緊急通報	緊急時に的確な支援を仰ぐために、通報を行うサービス	8-1	自動衝突通知	車両衝突後時に、自動でセンターへの衝突通知発信を実施する機能
			8-2	車両故障時の電話サポート	乗員の体調不良発生や車両の故障時にボタン押下することでセンターへの通知を行い、トラブル対応を支援する機能
9	ｿﾌﾄｳｪｱｱｯﾌﾟﾃﾞｰﾄ	無線通信を利用した電子制御システムのソフトウェア更新サービス	9-1	OTA	（左記の内容に同じ）
10	車両状態監視	車両の状態を監視するサービス	10-1	ドア・トランク・ハザードランプなどの状態監視	ドア、トランク、ハザードランプ、ウィンドウ等の状態をスマートデバイスなどにより遠隔監視する機能
			10-2	車両異常検知・通知	ドアこじ開けなどの異常を検知した際に、メール等により所有者へ通知する機能
			10-3	車両位置追跡	車両の位置情報を取得し現在地の把握・追跡を可能とする機能
11	シェアリングサービス	自動車のシェアリングサービス	11-1	カーシェアリング	（左記の内容に同じ）
12	料金支払いサービス	車両利用中に発生する様々な料金の支払い（高速道路・駐車場・ガソリンスタンドなど）を支援するサービス	12-1	料金支払い	（左記の内容に同じ）

表 3-1 自動走行関連のサービスと機能一覧

3.3.2. 機能別のシステム構成想定

3.3.1 にて調査した自動走行関連サービスと機能の一覧をもとに、機能別の想定システム構成を作成した。作成にあたり、自動走行車種別に自動走行システム開発で先行する企業を選定したうえで、企業が公開する情報を確認し、機能別の想定システム構成を机上調査した。また、作成した想定システム構成をもとに、有識者インタビューを実施し想定システム構成を見直した。

以下に、調査の流れを図示する。

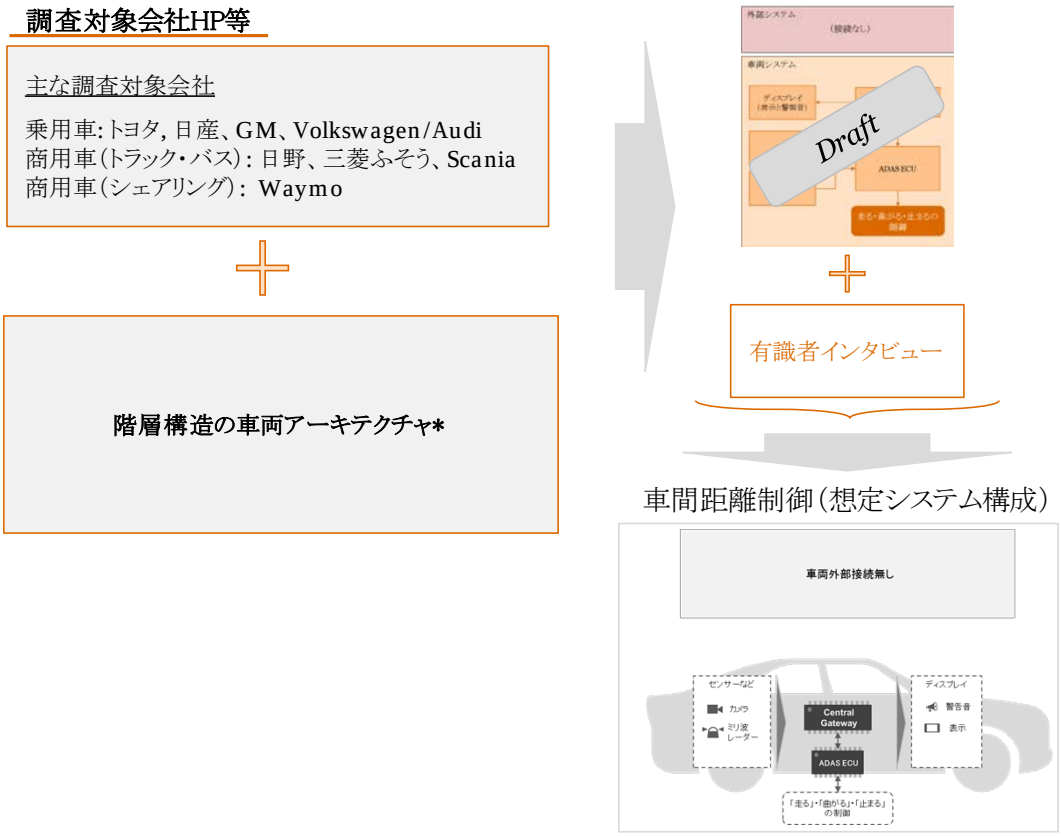


図 3-3 機能別のシステム構成想定の流れ

3.3.3. 自動走行システム共通モデルの特定

機能別の想定システム構成をすべて勘案し、想定システム構成の要素をすべて統合する形で、本脅威分析調査における自動走行システム共通モデルを導出した。この調査についても、有識者インタビューを実施し、モデルを見直した。

以下、本脅威分析調査における自動走行システム共通モデルを図示する。

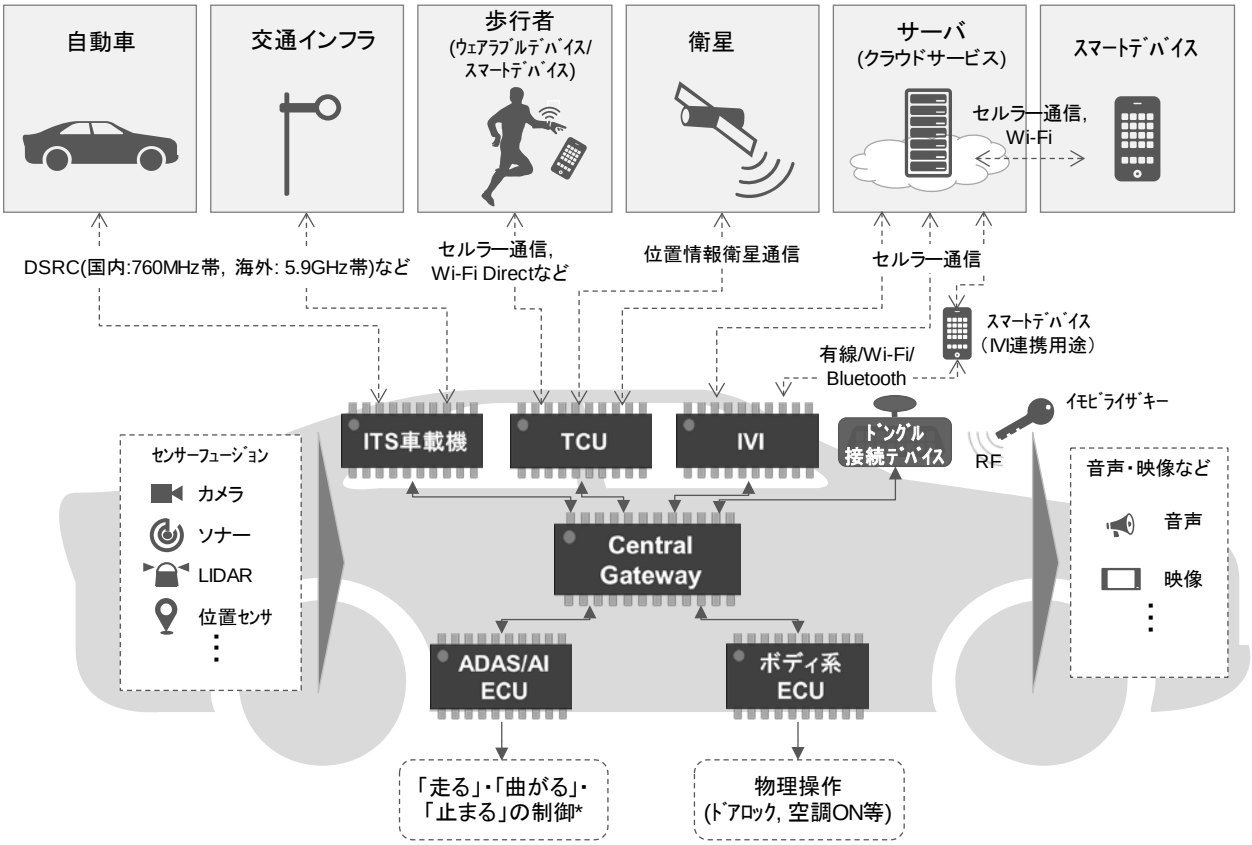


図 3-4　自動走行システム共通モデル

3.4. 脅威の全体像調査

3.4.1. 自動走行システム共通モデルの脅威の一覧化

はじめに、本調査における脅威を、「自動走行システム共通モデルに危害(被害）を与える潜在的原因」と定義する。これは ISO/IEC 27000:2009　の脅威定義を本調査向けに具体化したものである。

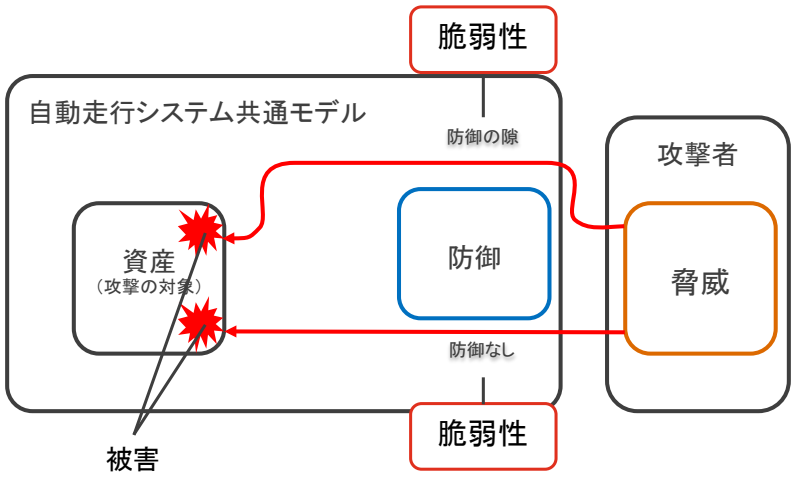


図 3-5　自動走行システム共通モデルにまつわるセキュリティ用語の関連性を示す模式図

上記定義のもと、自動走行システム共通モデルと自動車基準調和世界フォーラム（WP29）で検討されている Threat Matrix と比較し、自動走行共通モデルに関連する「攻撃の対象」、および「脅威」を抽出した。さらに CAPEC(Common Attack Pattern Enumeration and Classification：サイバー攻撃方法の種類を一意に識別するために攻撃方法のタイプを体系化し)での攻撃タイプをもとに分類を整理し、CWE（Common Weakness Enumeration：共通脆弱性タイプ一覧のこと)を使い、分類された結果を欠陥の観点から比較し検算することで、自動走行システム共通モデルにおける脅威の一覧を導出した。

攻撃の対象	脅威（被害の原因となる攻撃・欠陥）
車両システム	OEM資産（情報）の漏えい
	車両オーナーの個人情報漏えい
	暗号鍵の漏えい
	偽装した車両制御ソフトウェア
	許可のない車両ID改ざん
	ID詐称
	走行データなどの偽造
	許可のない車両診断データの改ざん
	ログデータの削除
	制御機能用のパラメータ数値の改ざん
	充電用機能のパラメータ数値の改ざん
	マルウェアの追加
	不正データ大量送信などによるDoS
	車両モニタリング機能の妨害
	（通常は自動走行を許可しない場所で使うとか）
車両の物理外部I/F	センサーの改ざん
	通信データを横流しするように改ざん
	外部メディアからのウイルス感染
	物理外部I/Fからの侵入（USBなど）
	不正な診断用メッセージ送信（ODB-IIなど）
車両（内部）の通信路	通信路の盗聴
	通信路からのデータへの不正アクセス
	通信データの改ざん
	通信機能（リモートキーなど）の機能改ざん
	短距離通信/センサーのデータ改ざん
	コマンドインジェクションによる意図しない機能実行
	データ/コードの改ざん・上書き・削除・追加
	通信路からのウイルス感染
	不正なCANメッセージ送信
	不正な専用メッセージ送信（通常OEMしか送信できないもの）
	信頼できないソースからのデータ入力
	大量のデータ送信による妨害
	通信データの送信元なりすまし
	シビル攻撃（複数ID生成による攻撃）
	リプレイ攻撃

攻撃の対象	脅威（被害の原因となる攻撃・欠陥）
車両外部の通信路	通信路の盗聴
	通信路からのデータへの不正アクセス
	MITM
	データ/コードの改ざん・上書き・削除・追加
	信頼できないソースからのデータ入力
	不正なV2Xメッセージ送信
	通信路からのウイルス感染
	改ざんされた3rd party アプリ
	大量のデータ送信による妨害
	車間通信におけるブラックホールアタック（全データを届かなくする）
	通信データの送信元なりすまし
	シビル攻撃（複数ID生成による攻撃）
	コマンドインジェクション
	リプレイ攻撃
	root権限の奪取
外部サーバー	サーバーへの不正侵入による情報漏えい
	サーバー上のデータ共有（ミス）による情報漏えい
	サーバーへの不正侵入によるサーバー乗っ取り
	同上
	サーバーへのDoS攻撃
	サーバーへの不正侵入によるサーバー破壊
	認証の不備による不正利用
アップデートサービス	アップデート用暗号鍵の漏えい（不正アップデートを許可）
	アップデートの妨害/アップデートプログラムの改ざん（サーバー）
	アップデートの妨害/アップデートプログラム改ざん（ローカル）
	不正なアップデートデータの作成（混入）
	正当なアップデート実行の妨害
車両からの攻撃（2次被害）	不正/信頼できないV2Vデータの転送
	タイミング攻撃（安全機能データの意図的な遅延など）
	偽の緊急情報の送信
	大量データ送信によるDoS
	車両からの他システムへの攻撃（※手法は記載なし）
	不正/信頼できないデータのインフラへの転送
	インフラへの大量データ送信などによるDoS
	車両のボットネット化
	ネットワークへの大量データ送信などによるDoS
（物理要因）	衝突等によるデータロス
	DRMの管理ミスによるデータロス
	ITコンポーネントの故障によるデータロス
	車両の売買による持ち主データの漏えい
	OEMデータ改ざん

表 3-2　自動走行システム共通モデルの脅威一覧

3.4.2.　自動走行システム共通モデルの脅威の全体像特定

導出した脅威に関して、脅威の重大度を測るためのフレームワークを用意した。同フレームワークは WP.29 および JSAE によって策定された脅威の重大度の評価指標を組み合わせ、「脅威の大きさ」、「攻撃の発生確率」を半定量化し、「脅威の重大度」を見積もるフレームワークである。

脅威の重要度

重要度	内容	スコア
Lv 7	車両の安全性へ影響を与える	7
Lv 6	車両機能の動作停止	6
Lv 5	ソフトウェアの改ざん、パフォーマンスの変更	5
Lv 4	ソフトウェアの変更（ただし、操作上の影響なし）	4
Lv 3	データの完全性侵害	3
Lv 2	データの機密性侵害	2
Lv 1	その他	1

攻撃の難易度

難易度	内容	スコア
高	権限昇格や情報収集など攻撃に至るまでに複数の条件が必要となるもの	1
中	難易度がシステムに内在する脆弱性に依存する攻撃	2
低	攻撃が容易（難易度「高」に記載するような条件が不要な攻撃）	3

事象の与える影響範囲

影響範囲	内容	スコア
大	不特定多数の対象に影響を及ぼす	3
中	複数あるが周辺の対象のみに限定される	2
小	1つの対象のみに限定される	1

情報資産の重要度

重要度	内容	スコア
特高	制御情報	4
高	金融資産に関する情報	3
中	プライバシー情報	2
低	上記以外の情報	1

脅威の重大度

脅威のレベル	スコア
レベルIII（重大）	10.0 ~ 7.0
レベルII（警告）	6.9 ~ 4.0
レベルI（注意）	3.9 ~ 0

図 3-6　脅威の重大度評価フレームワーク

策定したフレームワークを使い、自動走行システムの機能を実現するシステムに対して、脅威の重大度評価のためのフレームワークを適用し、機能別の脅威の重大度を算定した。

自動走行システム共通モデルに内在する脅威のうち、脅威の重大度スコアがレベル II 以上のものを抽出し、以下に示す。

サービス		機能			脅威	脅威の大きさ	攻撃の発生確率	脅威の重大度
名称		名称		内容				
1	運転・駐車支援	1-3	車間距離制御（V2V型）	ITSと協調し先行車両との車間距離を制御する機能	信頼できないソースからのデータ入力	2.8	1.6	4.4
					大量のデータ送信による妨害	4.2	1.6	6.7
		1-4	隊列走行（V2V型）	先頭車両と通信を行うことで後続車が無人で先頭車両を追従する機能（トラックなど商用車向け）	信頼できないソースからのデータ入力	2.8	1.6	4.4
					大量のデータ送信による妨害	4.2	1.6	6.7
		1-5	自動運転（ITS協調型）	ITSと協調することで人間に代わりあらゆる運転タスクを実施する機能	信頼できないソースからのデータ入力	2.8	2.4	6.7
					大量のデータ送信による妨害	4.2	2.4	10.0
		1-9	自動駐車（スマホ連携）	スマートフォンにインストールされたアプリケーション経由で車両の操作指示を行うことで、遠隔からの車両の自動駐車を実施する機能	サーバーへの不正侵入によるサーバー乗っ取り	1.8	2.4	4.3
					信頼できないソースからのデータ入力	2.8	2.4	6.7
2	安全走行支援	2-2	歩行者検知（V2P型）	歩行者の所有するスマートデバイスと連携し、車両の近くにいる歩行者を検知することで、必要に応じて車両を制御し歩行者との衝突を回避する機能	信頼できないソースからのデータ入力	2.8	1.6	4.4
					大量のデータ送信による妨害	4.2	1.6	6.7
4	ｿﾌﾄｳｪｱｱｯﾌﾟﾃﾞｰﾄ	4-1	OTA	無線通信を利用した電子制御システムのソフトウェア更新サービス	アップデートの妨害/アップデートプログラムの改ざん（サーバー）	4.2	2.4	10.0
					正当なアップデート実行の妨害	3.6	1.2	4.3
5	故障検知	5-1	故障検知	自動車に備わる自己診断機能を活用し、故障を予知・検知するサービス	サーバーへの不正侵入によるサーバー乗っ取り	1.8	2.4	4.3
8	車両遠隔操作	8-1	遠隔からのﾄﾞｱﾛｯｸ・ｱﾝﾛｯｸ	スマートデバイスなどと連携し、遠隔地より車両のドアのロック・アンロックを制御する機能	サーバーへの不正侵入によるサーバー乗っ取り	1.8	2.4	4.3
		8-3	充電制御	スマートデバイスと連携し、遠隔地より充電状況の管理（充電率の把握、充電停止等）を制御する機能	サーバーへの不正侵入によるサーバー乗っ取り	1.8	2.4	4.3
		8-4	充電制御（音声認識AI連携）	音声認識AIエージェントと連携し、遠隔地より充電状況の管理（充電率の把握、充電停止等）を制御する機能	サーバーへの不正侵入によるサーバー乗っ取り	1.8	2.4	4.3
		8-5	エアコン制御	スマートデバイスと連携し、遠隔地よりエアコンのオン・オフを制御する機能	サーバーへの不正侵入によるサーバー乗っ取り	1.8	2.4	4.3
		8-6	エアコン制御（ 音声認識AI連携）	音声認識AIエージェントと連携し、遠隔地よりエアコンのオン・オフを制御する機能	サーバーへの不正侵入によるサーバー乗っ取り	1.8	2.4	4.3
		8-7	エンジン再駆動・ステアリングロック解除禁止	オーナーの要請に基づき、エンジンの再始動・ステアリングロックの解除の禁止を実施する機能	サーバーへの不正侵入によるサーバー乗っ取り	1.8	2.4	4.3

表 3-3　自動走行システム共通モデルの脅威の全体像

また、上記重大度を算定した脅威のうち、脅威度（スコア）が 6.0 以上のものを、自動走行システム共通モデル上に図示したものを以下に示す。

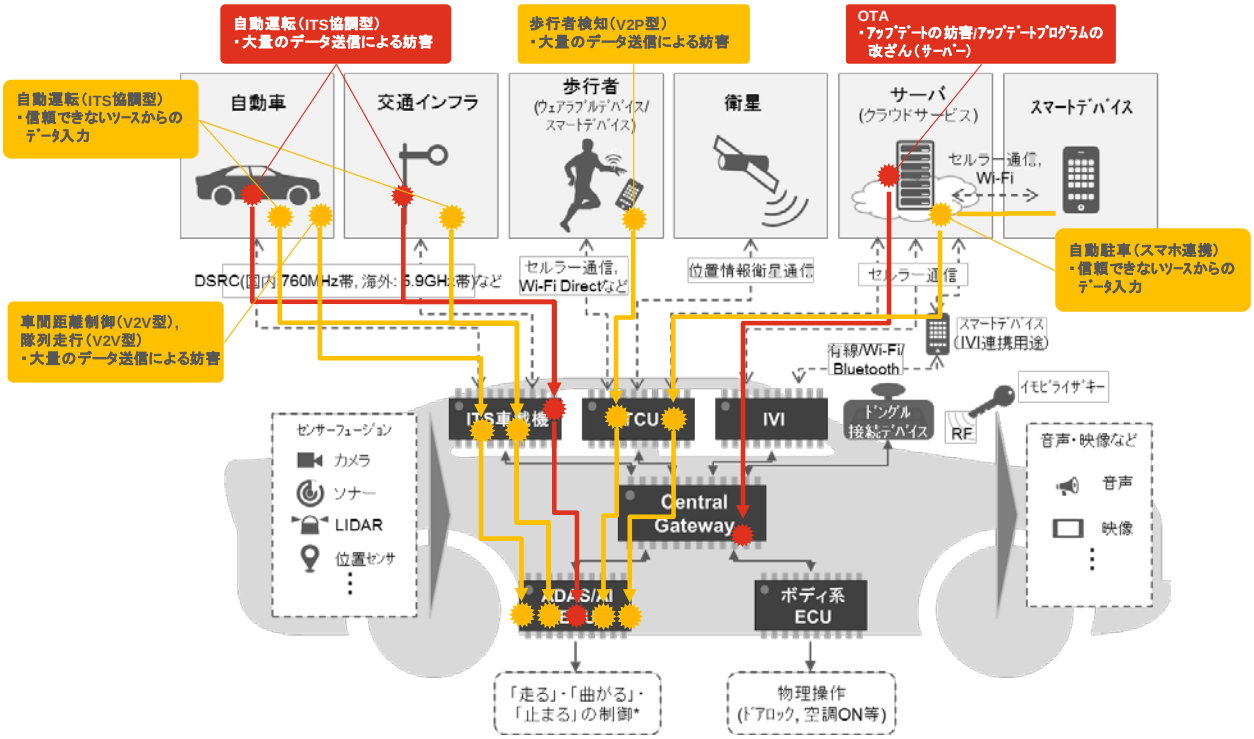


図 3-7　自動走行システム共通モデルの脅威の全体像図

3.4.3.　重大脅威に対する対策状況調査

抽出した重大脅威への対策・及び責任主体を WP.29 等の推奨セキュリティ対策を踏まえ整理した。

脅威のレベル	レベルI（注意）	レベルII（警告）	レベルIII（重大）
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

サービス		機能		脅威	脅威の重大度	責任主体				評価ｶﾞｲﾄﾞにおける対応状況	本事業外で必要な対応
名称		名称				自動車メーカ	ITｻｰﾋﾞｽ事業者	ﾃﾞﾊﾞｲｽ提供事業者	政府等		
1	運転・駐車支援	1-3	車間距離制御（V2V型）	信頼できないソースからのデータ入力	4.4	✔				項目追加	-
				大量のデータ送信による妨害	6.7	✔				項目追加	-
		1-4	隊列走行（V2V型）	信頼できないソースからのデータ入力	4.4	✔				項目追加	-
				大量のデータ送信による妨害	6.7	✔				項目追加	-
		1-5	自動運転（ITS協調型）	*信頼できないソースからのデータ入力*	6.7	✔	✔		✔	項目追加	*ITサービス事業者およびインフラ整備責任主体（政府等）においても、評価ガイドとは別に対策の検討が必要*
				大量のデータ送信による妨害	10.0	✔	✔		✔	項目追加	
		1-9	自動駐車（スマホ連携）	*ｻｰﾊﾞｰへの不正侵入によるｻｰﾊﾞｰ乗っ取り*	4.3		✔			（ｽｺｰﾌﾟ外）	*SIP「重要インフラ等」におけるサイバーセキュリティの確保」にて検討*
				信頼できないソースからのデータ入力	6.7	✔	✔			項目追加	
2	安全走行支援	2-2	歩行者検知（V2P型）	*信頼できないソースからのデータ入力*	4.4	✔		✔		項目追加	*ヒトが利用するﾃﾞﾊﾞｲｽへの対策については、デバイス提供事業者において、評価ｶﾞｲﾄﾞとは別に、対策の検討が必要*
				大量のデータ送信による妨害	6.7	✔		✔			
4	ｿﾌﾄｳｪｱｱｯﾌﾟﾃﾞｰﾄ	4-1	OTA	*アップデートの妨害/アップデートプログラムの改ざん（サーバー）*	10.0	✔	✔			項目追加	*SIP「重要インフラ等」におけるサイバーセキュリティの確保」にて検討*
				正当なアップデート実行の妨害	4.3	✔	✔				
5	故障検知	5-1	故障検知	*ｻｰﾊﾞｰへの不正侵入によるｻｰﾊﾞｰ乗っ取り*	4.3		✔			（ｽｺｰﾌﾟ外）	*SIP「重要インフラ等」におけるサイバーセキュリティの確保」にて検討*
8	車両遠隔操作	8-1	遠隔からのﾄﾞｱﾛｯｸ・ｱﾝﾛｯｸ	*ｻｰﾊﾞｰへの不正侵入によるｻｰﾊﾞｰ乗っ取り*	4.3		✔			（ｽｺｰﾌﾟ外）	*SIP「重要インフラ等」におけるサイバーセキュリティの確保」にて検討*
		8-3	充電制御		4.3		✔				
		8-4	充電制御（音声認識AI連携）		4.3		✔				
		8-5	エアコン制御		4.3		✔				
		8-6	ｴｱｺﾝ制御（音声認識AI連携）		4.3		✔				
		8-7	エンジン再駆動・ステアリングロック解除禁止		4.3		✔				

表 3-4　対策状況調査結果

レベル II 以上の脅威について、車両側で必要となる対策は、本事業で策定した情報セキュリティ評価ガイドラインへ項目を追加済である。一方で、赤字で記載した脅威への対策は、車両側だけでは不十分であり、責任主体に記載の該当者が、別に対策の検討が必要である。IT サービス事業者による対策については、SIP「重要インフラ等」におけるサイバーセキュリティの確保」にて検討が進められており、参照のこと。

3.4.4.　脅威の全体像調査のアプローチまとめ

本調査では、自動走行システムに係るすべてのシステム構成を踏まえ顕在化しうる脅威を抽出し、重大度評価フレームワークを適用することで優先して対応すべき脅威を特定した。さらに、特定した脅威に対して、対策の責任主体を明確化するとともに、車両側での対策が必要な脅威は、評価ガイドへ反映した。以下に本調査の分析アプローチを図示する。

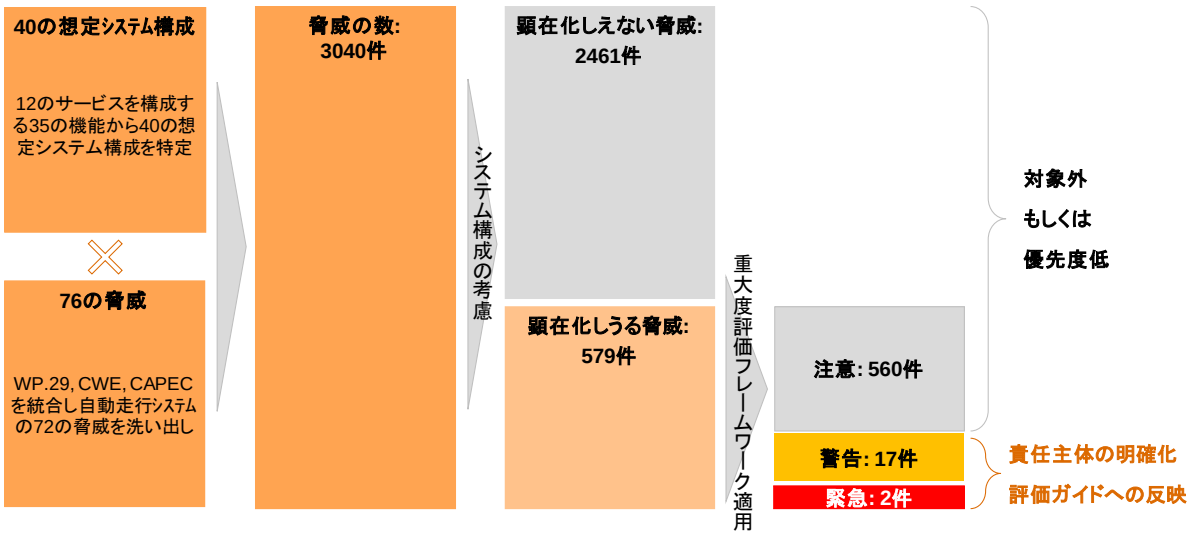


図 3-8　*脅威の全体像調査のアプローチ（まとめ）*

最後に、本調査結果を踏まえたステークホルダーへの提言をまとめる。各ステークホルダーが危惧すべき脅威と対策を提言するものである。

4　情報セキュリティ評価ガイドラインドラフトの作成

4.1.　評価ガイドラインのスコープ

本ガイドラインにて確立する評価手法に関して、車両開発の V 字プロセスにおける位置づけと役割を以下に示す。

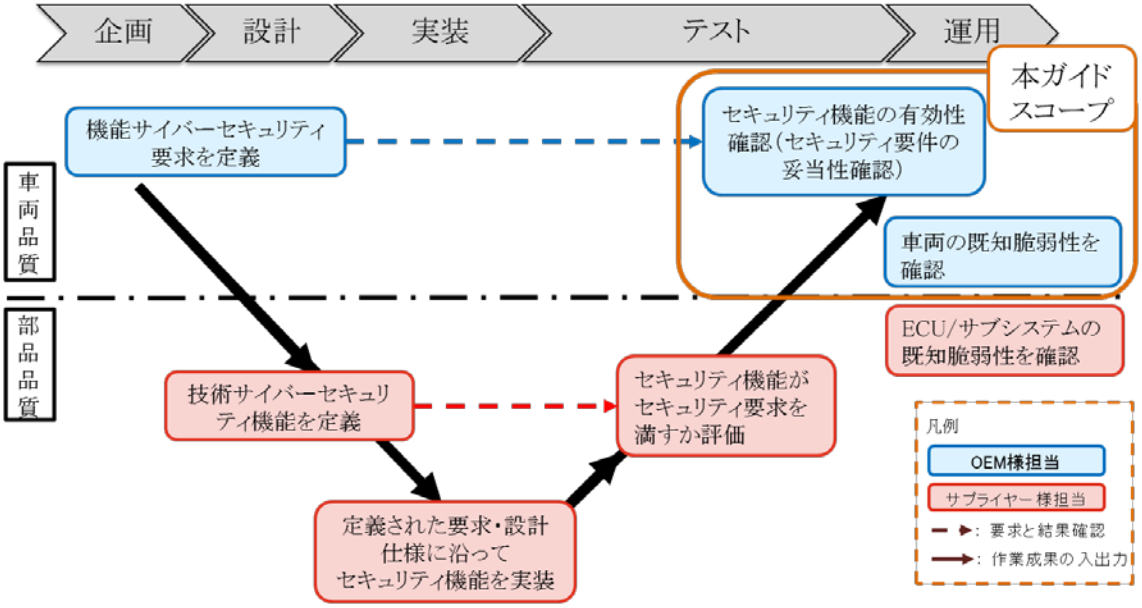
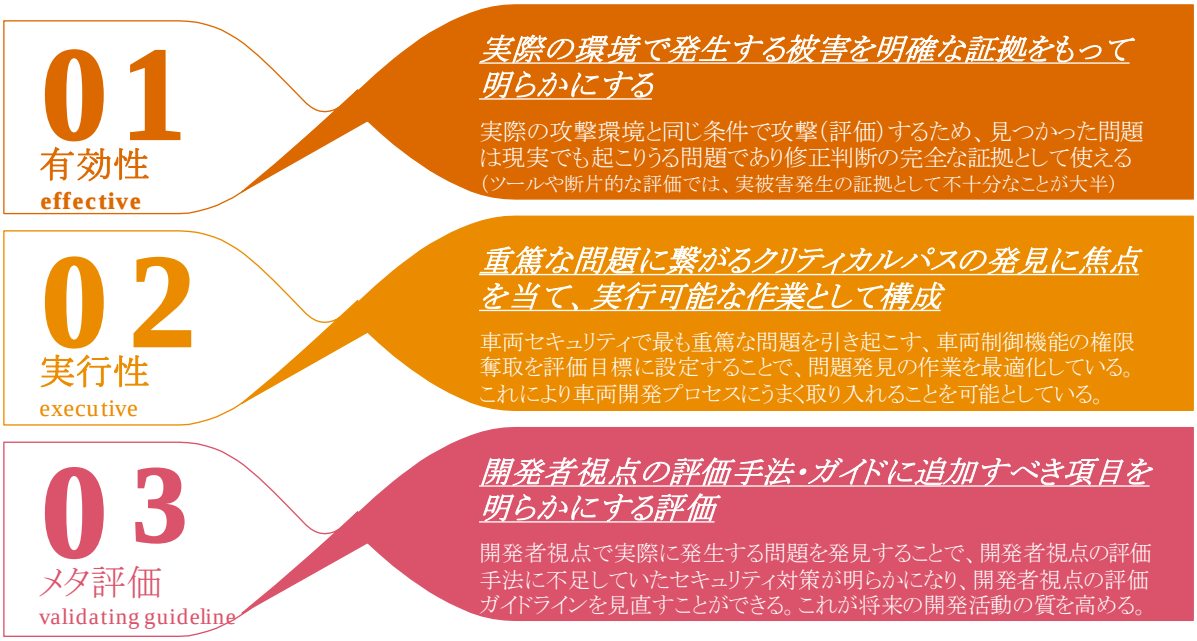


図 4-1 開発 V 字モデルと評価の位置づけ

4.2.　評価ガイドライン策定方針

4.1.1.　ガイドライン策定の基本アプローチ

本ガイドラインは以下の３つの方針に従って評価項目を策定した。



4.1.2. 本書の評価項目がカバーする範囲

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

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

インシデント事例	インシデント概要
Jeep Cherokee の uConnect 脆弱性	第３者により車両位置の特定やリモートで車両を操作される脆弱性。CellularNetwork 上の開放ポートから車載器に侵入し、CAN コントローラのファームウェア改ざんすることで車両をリモート操作することが可能
BMW の ConnectedDrive 脆弱性	第３者により車両をリモート操作される可能性のある脆弱性。研究者の用意したテレマティクスサーバーから車両に対しドア解錠のコマンドを送ることでドアを解錠することが可能
Tesla ModelS の無線 LAN 脆弱性	第３者により車両をリモート操作される脆弱性。研究者は偽 WiFi スポットを利用して攻撃サイトに誘導する方法を提示したが、Cellular Network を介した攻撃も可能である。その場合、おとりメール等を用いて、ユーザーを攻撃サイトに誘導する。
三菱アウトランダーのモバイルアプリ脆弱性	第３者により空調設定等の環境設置をリモート操作される脆弱性。車内に設置された WiFi ス

	ポットにアクセスすることで防犯装置の設定や空調操作をリモート操作することが可能
日産 Nissan Connect EV の脆弱性	一般ユーザーが利用しない開発設定が残存しており、これを利用することでユーザーID,パスワード等の機密情報が外部に漏えいさせることが可能
日産リーフの脆弱性	認証方式に不備があり、スマートフォン⇔サーバーAPI に認証の仕組みが実装されておらず、VIN 下 5 桁が判明すれば他の車両を制御することが可能 ※スマートフォンアプリの脆弱性であるが、車両⇔サーバー、あるいは車両⇔スマートフォンで同様の事象が発生しないか確認する
スバル StarLink の脆弱性	スマートフォンのデバイス認証に使用されるセキュリティトークンには有効期限がなく、窃取された場合、第３者によりドアを解錠させることが可能 ※スマートフォンアプリの脆弱性であるが、車両⇔サーバー、あるいは車両⇔スマートフォンで同様の事象が発生しないか確認する
Continental AG の TCU の脆弱性	第３者により TCU がリモート操作される可能性のある脆弱性
マツダの Mazda Connect の脆弱性	車内の USB ポートから任意のコードを実行される脆弱性。AVN のカスタマイズに利用された ※ローカル攻撃であるが、リバースエンジニアリング耐性を図る評価ポイントとして採用
本田技研工業の Honda Connect の脆弱性	車内の USB ポートから任意のコードが実行される脆弱性。AVN のカスタマイズに利用された ※ローカル攻撃であるが、リバースエンジニアリング耐性を図る評価ポイントとして採用

表 4-1　対象とする車両インシデント事例一覧

また具体的なインシデント事例に加え、「3.脅威分析調査」で明らかにした自動走行システムに係る脅威のうち、早急な対策が求められる重大脅威を踏まえ、車両セキュリティ評価に必要な項目は、本ガイドに反映した。

4.1.3.　ガイドラインで想定する評価レベル

4.1.1 のアプローチに従い、有効性・実効性を確保するため、攻撃者のプロファイルを分析し、高度な技術レベルや設備を持つ場合をカバーする評価内容を策定した。以下に、本ガイドラインで想定する評価レベルを図示する。

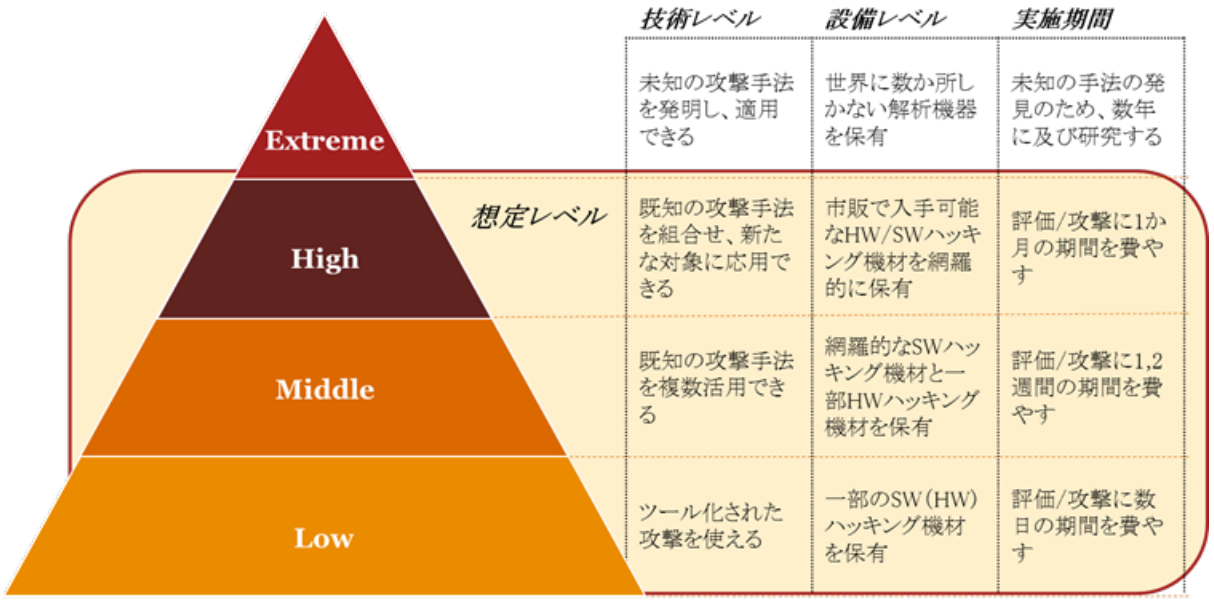


図 4-2　想定する情報セキュリティ評価レベル

4.3. 評価ガイドライン項目

4.3.1. 評価項目概要

本ガイドラインの評価手順と評価項目毎の評価内容の概略を示す。

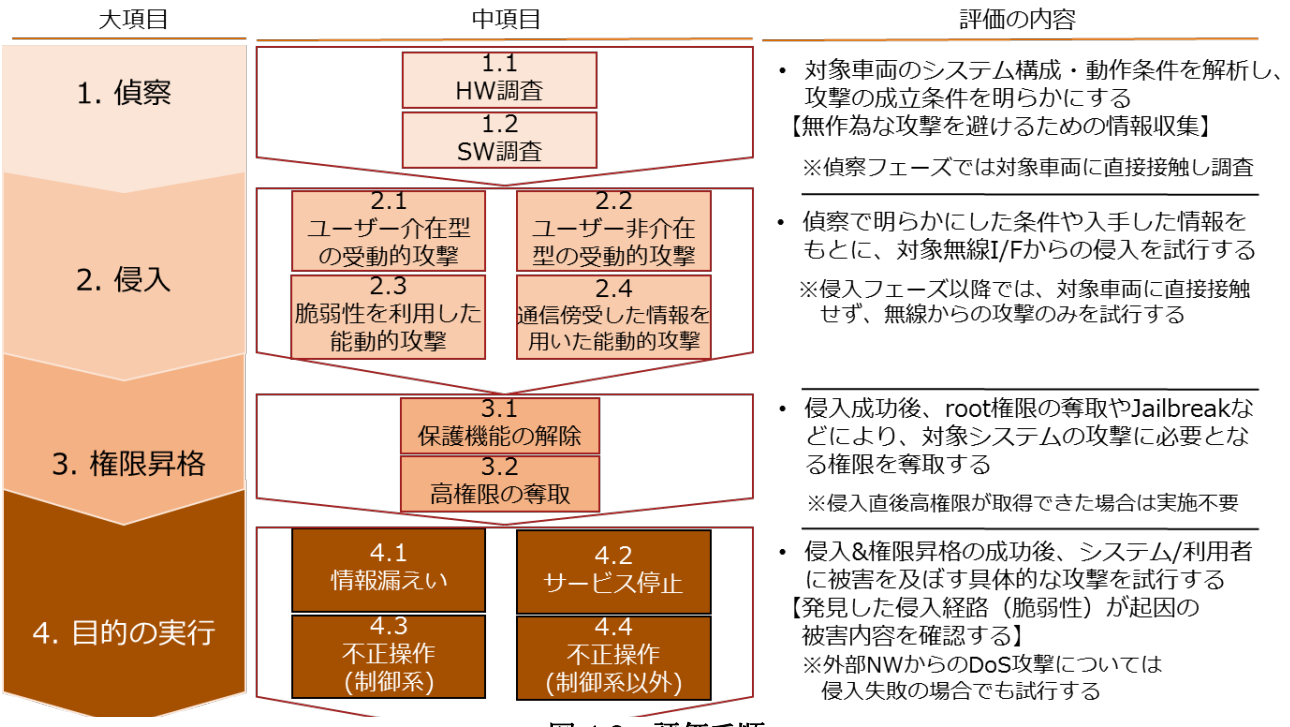


図 4-3　評価手順

4.3.2.　評価項目の策定方針

各評価項目の策定方針を以下に記載する

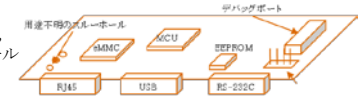
- 1.偵察　－ 1.1 HW 調査

【評価方針】

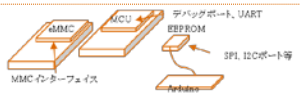
- 搭載HW（車両,デバイス,チップ）が*データ入出力に使うすべてのI/F*からのデータ抽出を試行し、成功した段階でバイナリファイルをリバースし、システムを解析する

【1.1.1 対象I/F】
RJ45, USB, RS-232C等

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

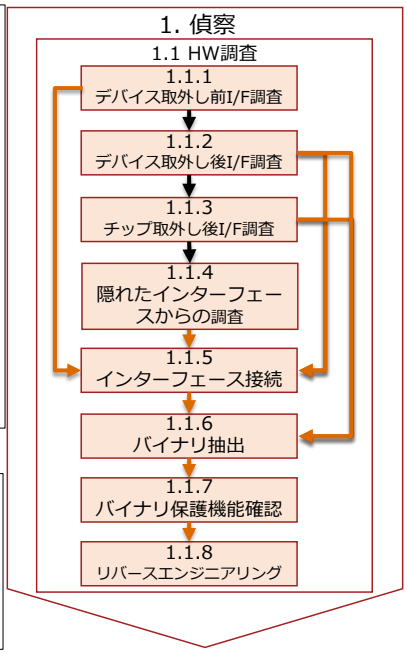


【1.1.3 対象I/F】
デバッグポート,UART（ピン),
MMC I/F, SPI, I2Cポート等



【インシデント以外で取り込んだ評価項目】

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

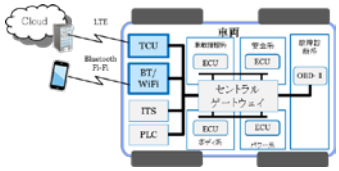


➢ 1.偵察 － 1.2 SW 調査

【評価方針】

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

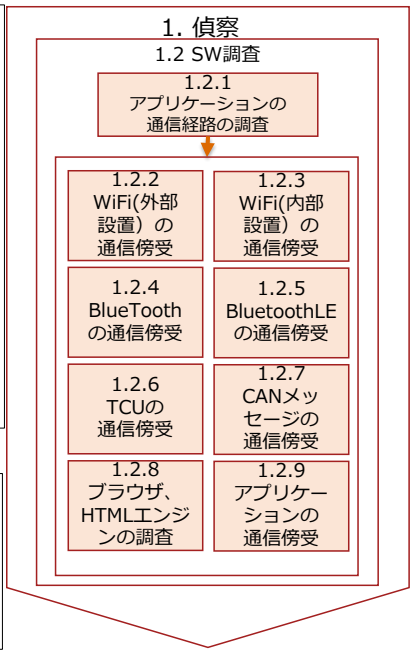
【対象通信】
- TCU(3G/4G)
- WiFi
- Bluetooth



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

【インシデント以外で取り込んだ評価項目】

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

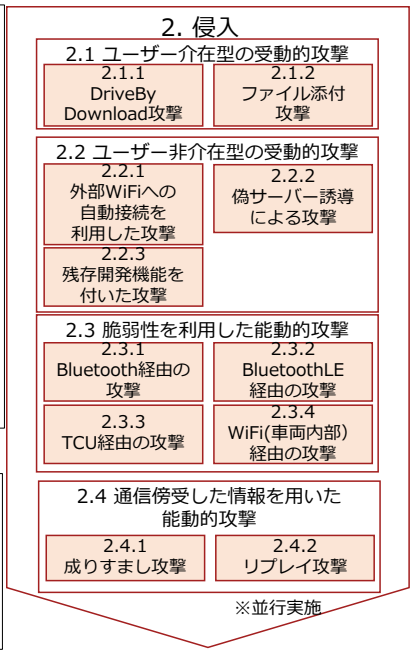


➢ 2.侵入

【評価方針】

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

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



【インシデント以外で取り込んだ評価項目】

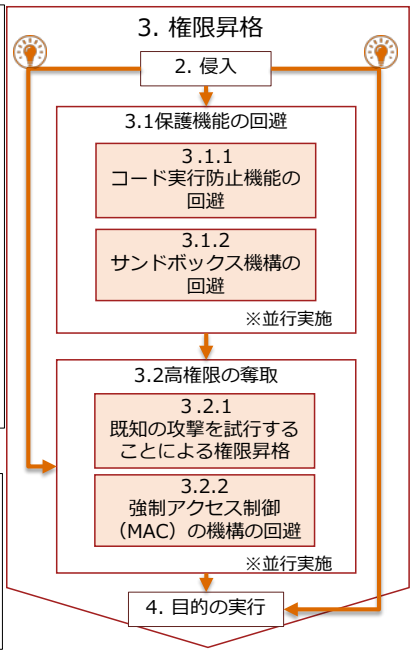
- Bluetooth関連について、Bosch社のBluetoothドングル等の車両部品システムにインシデント事例があり、それら内容を項目化した
- ITセキュリティで攻撃事例および被害の多い標的型攻撃を考慮するものと判断し、「ファイル添付攻撃」「偽サーバー誘導による攻撃」を項目化した

➢ 3.権限昇格

【評価方針】

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

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

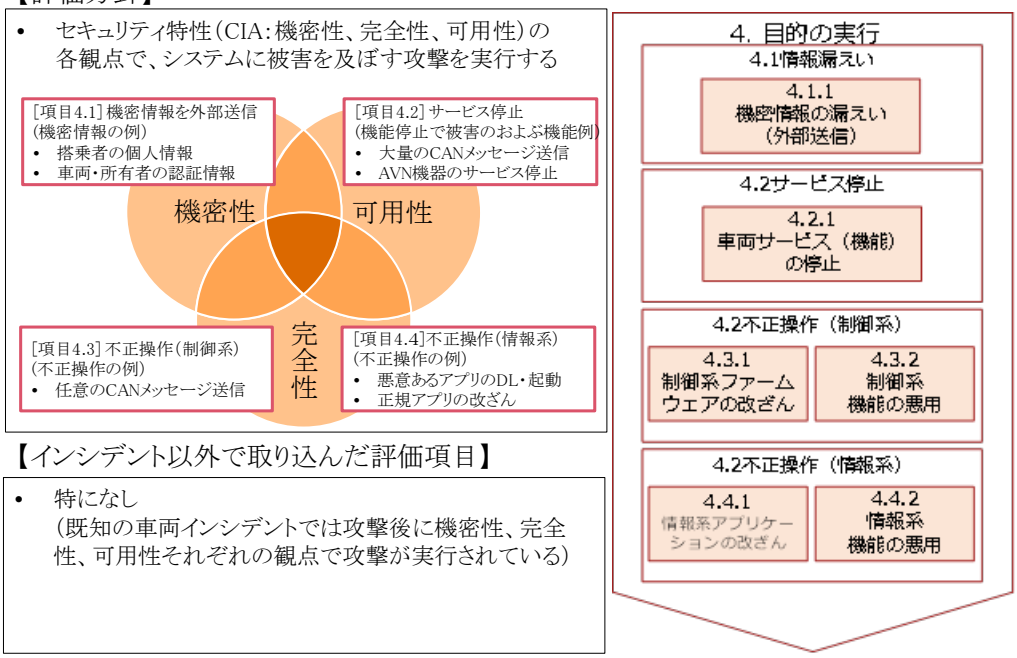


【インシデント以外で取り込んだ評価項目】

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

➢ 4.目的の実行

【評価方針】



【インシデント以外で取り込んだ評価項目】

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

4.3.3. 評価項目一覧

本ガイドラインの評価項目の一覧を示す。

カテゴリ（大項目）	*カテゴリ（中項目）*	*評価項目*	*確認項目*
1.偵察	1.1 HW 調査	1.1.1 デバイス取り出し前 I/F 調査	1.1.1.1 USB ポート接続確認
			1.1.1.2 RJ45 ポート接続確認
			1.1.1.3 RS-232C ポート接続確認
		1.1.2 デバイス取り出し後 I/F 調査	1.1.2.1 目視による確認
			1.1.2.2 マルチメータによる確認
			1.1.2.3 ポートファジングツールを用いた確認
		1.1.3 チップ取り外し後 I/F 調査	1.1.3.1 MCU のチップ調査
			1.1.3.2 EEPROM のチップ調査
			1.1.3.3 NAND フラッシュ、eMMC のチップ調査
		1.1.4 隠れたインターフェースからの調査	1.1.4.1 公開情報からのスペック調査
			1.1.4.2 専門業者への解析依頼
		1.1.5 インターフェース接続	1.1.5.1 イーサネットからのパスワード認証の確認
			1.1.5.2 イーサネットから脆弱性診断スキャン
			1.1.5.3 シリアルからのパスワード認証の確認
			1.1.5.4 シリアルからの BootLoader の確認
			1.1.5.5 NAND フラッシュ、eMMC からのコンソール取得
			1.1.5.6 root 権限の取得
		1.1.6 バイナリ抽出	1.1.6.1 root 取得後のバイナリ抽出
			1.1.6.2 ADB からのバイナリ抽出
			1.1.6.3 BootLoader からのバイナリ抽出
			1.1.6.4 デバッグポートからのバイナリ抽出
			1.1.6.5 EEPROM からのバイナリ抽出

			1.1.6.6 NAND フラッシュ、eMMC からのバイナリ抽出
		1.1.7 バイナリ保護機能確認	1.1.7.1 マニュアルによる調査
			1.1.7.2 目視によるバイナリファイルの調査
			1.1.7.3 EEPROM からの鍵の入手
			1.1.7.4 RAM からの鍵の抽出
			1.1.7.5 暗号処理モジュールからの鍵の抽出
			1.1.7.6 暗号化方式の確認
			1.1.7.7 別の車載器からの鍵の抽出
		1.1.8 リバースエンジニアリング	1.1.8.1 ファイルシステムの調査
			1.1.8.2 逆アセンブラの実行
			1.1.8.3 逆コンパイラの実行
	1.2 SW 調査	1.2.1 アプリケーションの通信経路の調査	1.2.1.1 通信経路の調査
		1.2.2 WiFi（車両外部）の通信傍受	1.2.2.2 外部へのアクセス先の確認
			1.2.2.2 待ち受けポートの確認
			1.2.2.3 SSL 暗号化の確認
			1.2.2.4 認証情報の確認
			1.2.2.5 リプレイ、成りすまし防止情報の解析
		1.2.3 WiFi（車両内部）の通信傍受	1.2.3.1 アクセス先ポート確認
			1.2.3.2 SSL 暗号化の確認
			1.2.3.3 認証情報の解析
			1.2.3.4 リプレイ防止情報の解析
			1.2.3.5 認証方式の確認
			1.2.3.6 パスワード規則性の推測
			1.2.3.7 WiFi パスワードの解析
		1.2.4 Bluetooth の通信傍受	1.2.4.1 BluetoothMAC アドレスが検出可能なタイミングの確認
			1.2.4.2 ペアリング方式の確認
			1.2.4.3 Bluetooth プロファイルの調査
		1.2.5 BluetoothLE の通信傍受	1.2.5.1 スマートフォン⇔車載間の BLE 通信傍受
			1.2.5.2 キーフォブ⇔車載間の BLE 通信傍受
		1.2.6 TCU の通信傍受	1.2.6.1 公開 IP アドレススキャン
			1.2.6.2 AT コマンドを利用したオーバーフロー攻撃
			1.2.6.3 AT コマンドを利用した DDoS 攻撃
		1.2.7 ブラウザ、HTML エンジンの調査	1.2.7.1 ブラウザアプリの選別
			1.2.7.2 バージョンの取得
		1.2.8 CAN メッセージ通信傍受	1.2.8.1 CAN メッセージキャプチャツールの設置
			1.2.8.2 CAN メッセージの送受信
		1.2.9 アプリケーションの通信傍受	1.2.9.1 プロキシ用端末の証明書のインストール
			1.2.9.2 キャプチャ内容の確認
2.侵入	2.1 ユーザー介在型の受動的攻撃	2.1.1 DrivebyDownload 攻撃	2.1.1.1 ブラウザの脆弱性確認
			2.1.1.2 攻撃用 Web サイトへのアクセス
			2.1.1.3 Web サイトから攻撃の反応確認
		2.1.2 ファイル添付攻撃	2.1.2.1 リバースシェルの配布
			2.1.2.2 リバースシェルのダウンロード
			2.1.2.3 リバースシェルの実行

	2.2 ユーザー非介在型の受動的攻撃	2.2.1 外部 WiFi への自動接続を利用した攻撃	2.2.1.1 マニュアルベースの確認
			2.2.1.2 バイナリファイルの確認
			2.2.1.3 接続確認
		2.2.2 偽サーバー誘導による攻撃	2.2.2.1 アプリケーションの脆弱性調査
			2.2.2.2 アプリケーションの実行
			2.2.2.3 攻撃の確認
		2.2.3 残存開発環境を用いた攻撃	2.2.3.1 用途不明の通信経路の調査
			2.2.3.2 WiFi への接続
			2.2.3.3 通信ログ確認
	2.3 脆弱性を利用した能動的攻撃	2.3.1 Bluetooth 経由の攻撃	2.3.1.1 MAC アドレスの入手
			2.3.1.2 API の脆弱性を利用した攻撃
			2.3.1.3 プロトコルの脆弱性を利用した攻撃
		2.3.2 BluetoothLE 経由の攻撃	2.3.2.1 MAC アドレスの入手
			2.3.2.2 API の脆弱性を利用した攻撃
			2.3.2.3 プロトコルの脆弱性を利用した攻撃
		2.3.3.TCU 経由の攻撃	2.3.3.1 TCU 側サービス API の脆弱性を利用した攻撃
			2.3.3.2 機器の脆弱性を利用した攻撃
		2.3.4 WiFi（車両内部）経由の攻撃	2.3.4.1 公開ポートからのログイン
			2.3.4.2 スマートフォンの解析
			2.3.4.3 API ソースコードの解析
	2.4 通信傍受した情報を用いた能動的攻撃	2.4.1 成りすまし攻撃	2.4.1.1 サーバーを経由した成りすまし攻撃
			2.4.1.2 BluetoothLE からの成りすまし攻撃
			2.4.1.3 WiFi（内部設置）からの成りすまし攻撃
			2.4.1.4 成りすまし攻撃の対策確認
		2.4.2 リプレイ攻撃	2.4.2.1 サーバー⇒TCU パケットをリプレイ
			2.4.2.2 BluetoothLE デバイス⇒車両パケットをリプレイ
			2.4.2.3 WiFi デバイス⇒車両（WiFi 内部設置）パケットをリプレイ
			2.4.2.4 リプレイ攻撃への対策確認
3. 権限昇格	3.1 保護機能の回避	3.1.1 コード実行防止機能の回避	3.1.1.1 NX ビットの確認
			3.1.1.2 ASLR の確認
			3.1.1.3 SSP の確認
			3.1.1.4 PIE の確認
			3.1.1.5 RELRO-FULL の確認
			3.1.1.6 既知の脆弱性を利用したデータ実行保護機能の確認
		3.1.2 サンドボックス機構の回避	3.1.2.1 ファイルシステムの制限の確認
			3.1.2.2 システムコールの制限の確認
			3.1.2.3 既知の脆弱性を利用したサンドボックスの回避
	3.2 高権限の奪取	3.2.1 既知の攻撃を試行することによる権限昇格	3.2.1.1 root 権限の昇格
		3.2.2 強制アクセス制御（MAC）の機構の回避	3.2.2.1 強制アクセス制御の確認
			3.2.2.2 強制アクセス制御の回避
4.目的の実行	4.1 情報漏えい	4.1.1 機密情報の漏えい（外部送信）	4.1.1.1 機密情報の調査
			4.1.1.2 外部へのデータ送信
	4.2 サービスの停止	4.2.1 車両のサービス（機能）の停止	4.2.1.1 プロセス強制終了による車両サービスの停止
			4.2.1.2 CPU 負荷上昇による車両サービスの停

			止
			4.2.1.3 ネットワーク負荷上昇による車両サービスの停止
			4.2.1.4 ディスク負荷上昇による車両サービスの停止
	4.3 不正操作（制御系）	4.3.1 制御系ファームウェアの改ざん	4.3.1.1 チェックサムによるアップデート保護の回避
			4.3.1.2 デジタル署名によるアップデート保護の回避
			4.3.1.3 ファームウェアのダウングレード
		4.3.2 制御系機能の悪用	4.3.2.1 CAN メッセージを実行する API の調査
			4.3.2.2 API を利用した制御系の操作
	4.4 不正操作（情報系）	4.4.1 情報系アプリケーションの改ざん	4.4.1.1 監視項目の確認
			4.4.1.2 セーフティシステムの無効化
			4.4.1.3 暗号化方式の確認
			4.4.1.4 デジタル署名を改ざんした状態でのアプリケーション起動
			4.4.1.5 異なるユーザーのデジタル署名を付与した状態でのアプリケーション起動
		4.4.2 情報系機能の悪用	4.4.2.1 アプリケーションを実行する API の調査
			4.4.2.2 API を利用した情報系の操作

表 4-2　評価項目一覧

4.3.4. 評価項目と車両インシデントとの関係

本ガイドの評価項目の一覧と本ガイドで想定する既知の車両インシデント（脆弱性）との関連を示す。

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

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

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

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

5　情報セキュリティ評価の試行調査

5.1.　試行調査の目的

情報セキュリティ評価試行調査では、ベンチシステム（検証機）を対象に、策定した情報セキュリティ評価ガイドラインドラフト版の評価手順に従い評価を実施した。

策定した評価ガイドラインに従い評価を試行することで、情報セキュリティ評価ガイドラインの実行可能性および内容の妥当性を評価すると共に、攻撃者の立場から検証機に関わるセキュリティ脅威の顕在要因となりうる脆弱性を調査し、改善が必要とみられる事項を検出した場合は、改善の方向性について助言を行うことを目的とする。

5.2.　評価期間とスケジュール

ベンチシステム搬入から評価レポートの提出まで、約 8 週間の期間で評価を実施した。そのうち 7 週間を偵察フェーズにおけるファームウェア入手の作業に充てた。一方、時間的な制約の都合で権限昇格や目的の実行に関する作業は一部のみ実施した。

期間
2017 年 12 月 15 日　～　2018 年 2 月 9 日（36 日間）

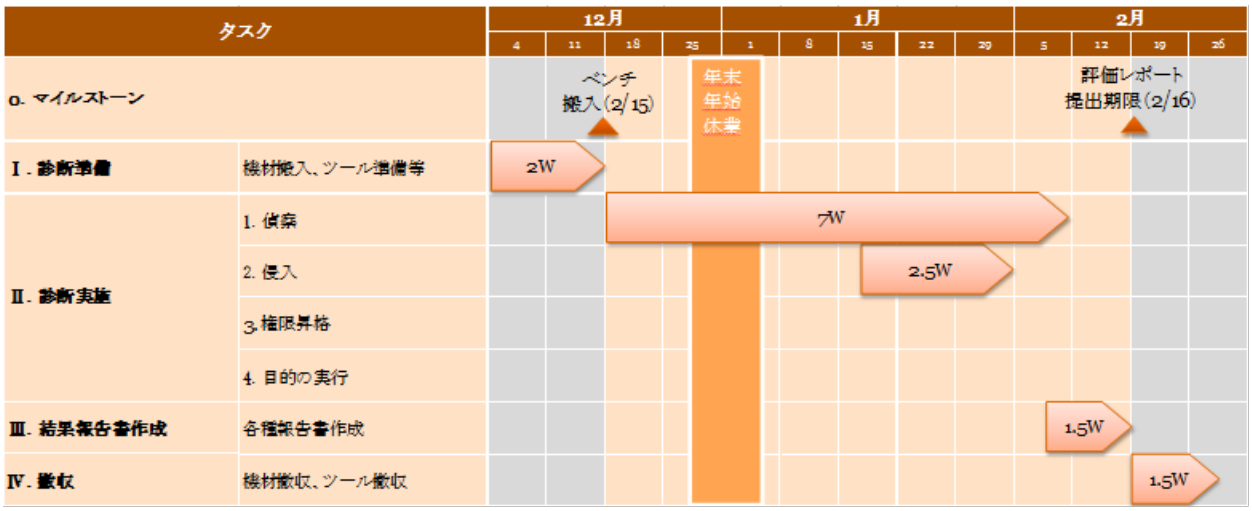


図 5-1　評価実施スケジュール

5.3.　評価実施内容

5.3.1.　評価実施項目

本評価において実施した、具体的な評価項目は下表のとおり。

評価を実施した項目を（〇）、評価のための前提条件が揃わず未実施となった項目を（✖）、評価対象システムが対象となる機能やアプリを実装していないため未実施となった項目を（-）と記す。

カテゴリ（大項目）	*カテゴリ（中項目）*	*評価項目*	*実施*
1. 偵察	1.1 HW 調査	1.1.1 デバイス取り出し前 I/F 調査	〇
		1.1.2 デバイス取り出し後 I/F 調査	〇

		1.1.3 チップ取り外し後 I/F 調査	○
		1.1.4 隠れたインターフェースからの調査	✖
		1.1.5 インターフェース接続	○
		1.1.6 バイナリ抽出	○
		1.1.7 バイナリ保護機能確認	○
		1.1.8 リバースエンジニアリング	○
	1.2 SW 調査	1.2.1 アプリケーションの通信経路の調査	○
		1.2.2 WiFi（車両外部）の通信傍受	○
		1.2.3 WiFi（車両内部）の通信傍受	–
		1.2.4 Bluetooth の通信傍受	○
		1.2.5 Bluetooth LE の通信傍受	–
		1.2.6 TCU の通信傍受	–
		1.2.7 ブラウザ、HTML エンジンの調査	–
		1.2.8 CAN メッセージ通信傍受	–
		1.2.9 アプリケーションの通信傍受	○
2. 侵入	2.1 ユーザー介在型の受動的攻撃	2.1.1 DrivebyDownload 攻撃	–
		2.1.2 ファイル添付攻撃	–
	2.2 ユーザー非介在型の受動的攻撃	2.2.1 外部 WiFi への自動接続を利用した攻撃	○
		2.2.2 偽サーバー誘導による攻撃	○
		2.2.3 残存開発環境を用いた攻撃	○
	2.3 脆弱性を利用した能動的攻撃	2.3.1 Bluetooth 経由の攻撃	○
		2.3.2 Bluetooth LE 経由の攻撃	–
		2.3.3. TCU 経由の攻撃	–
		2.3.4 WiFi（車両内部）経由の攻撃	–
	2.4 通信傍受した情報を用いた能動的攻撃	2.4.1 成りすまし攻撃	✖
		2.4.2 リプレイ攻撃	–
3. 権限昇格	3.1 保護機能の回避	3.1.1 コード実行防止機能の回避	✖
		3.1.2 サンドボックス機構の回避	✖
	3.2 高権限の奪取	3.2.1 既知の攻撃を試行することによる権限昇格	✖
		3.2.2 強制アクセス制御（MAC）の機構の回避	○
4. 目的の実行	4.1 情報漏えい	4.1.1 機密情報の漏えい（外部送信）	✖
	4.2 サービスの停止	4.2.1 車両のサービス（機能）の停止	✖
	4.3 不正操作（制御系）	4.3.1 制御系ファームウェアの改ざん	✖
		4.3.2 制御系機能の悪用	✖
	4.4 不正操作（情報系）	4.4.1 情報系アプリケーションの改ざん	○
		4.4.2 情報系機能の悪用	✖

表 5-1　実施した評価項目

5.3.2.　評価結果レポートの様式

本試行調査の結果は下記の様式を用いて結果を報告した。

評価ガイドライン項番	（評価項目の対応する項番を記載）
評価結果	評価結果の内容を記載
危険度	下記の判定基準に項目の危険度を記載
評価内容	評価により確認する内容を記載
評価手順	具体的な評価実施手順を記載
想定されるリスク	問題が見つかった場合、想定されるリスク（被害）の内容を記載

攻撃成立条件	問題が見つかった場合、攻撃が成功するための前提条件を記載
改善案	問題が見つかった場合、攻撃を防ぐための改善案を記載

重要度	判定基準の定義
High	対象システムにおいて発見された脆弱性を修正対応しないことにより、高度な技術や高いコストをかけずに緊急性の高いセキュリティ侵害が発生し、事業運営に甚大な悪影響を及ぼす（リコールや業務停止等の）可能性がある。直ちに脆弱性の修正対応等の実施に着手すべきである。
Medium	対象システムにおいて発見された脆弱性を修正対応しないことにより、一定の技術やコストをかけた攻撃により緊急性のあるセキュリティ侵害が発生し、事業運営に多大な悪影響を及ぼす（業務パフォーマンスの著しい悪化等の）可能性がある。必要に応じて脆弱性の修正対応等の実施を推奨する。
Low	対象システムにおいて発見された事項において、直ちにセキュリティ上の影響があるわけではないが、対策を実施することにより一定のセキュリティの向上が見込まれる項目である。将来的に事項の対応等の実施を推奨する。
Info	対象システムにおいて発見された事項において、何らかの影響を及ぼす可能性がある項目である。対策の是非について検討を推奨する。

なお、本成果報告書では具体的な評価結果については記載を省略する。

6　実証実験の運営準備

6.1.　平成 30 年度実証実験スケジュール案

平成 30 年度の実証実験のスケジュール案を以下に示す。

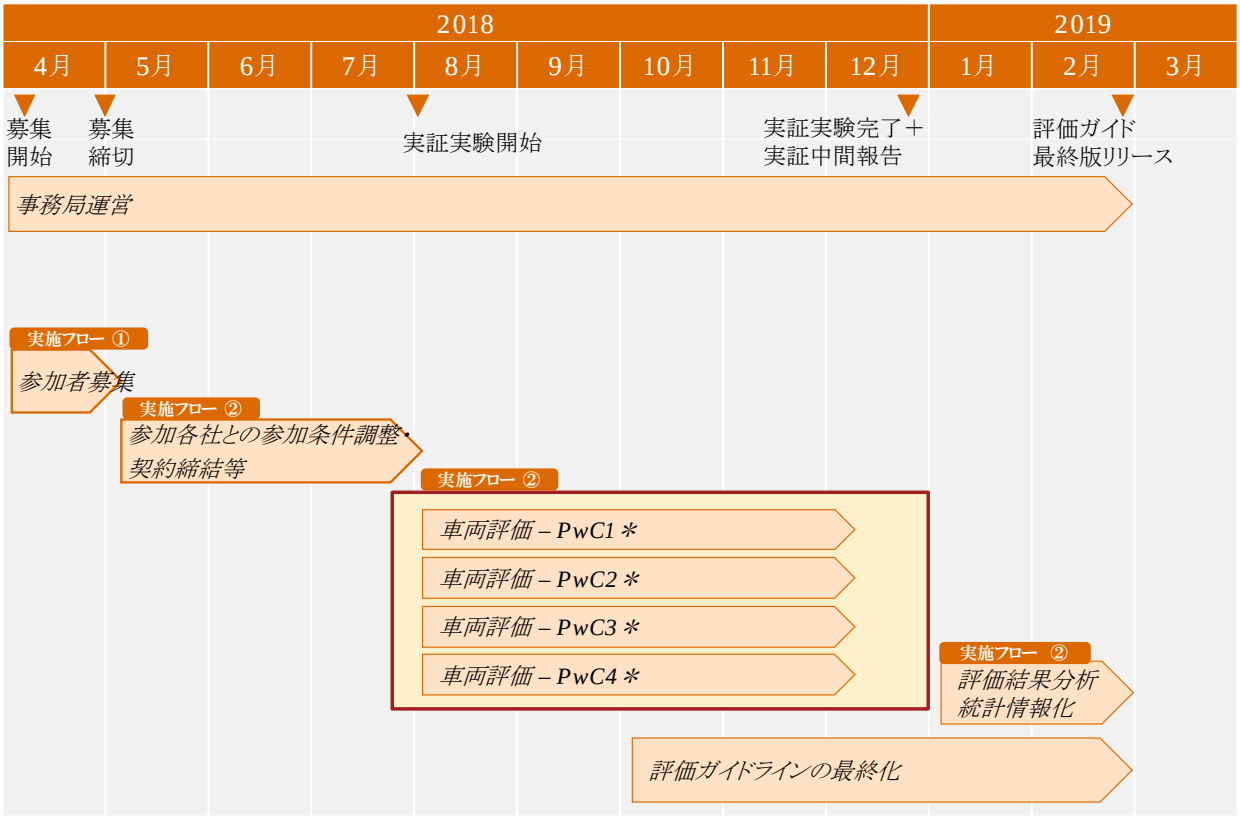


図 6-1　実証実験のスケジュール案

なお、実際の車両評価は、上記車両評価の期間内で各 OEM の実証実験を 2 か月間実施する計画である。

6.1.1.　実施フロー①：　参加者募集

参加者募集及び諸条件の事前調整等に関するフローは以下を想定している。

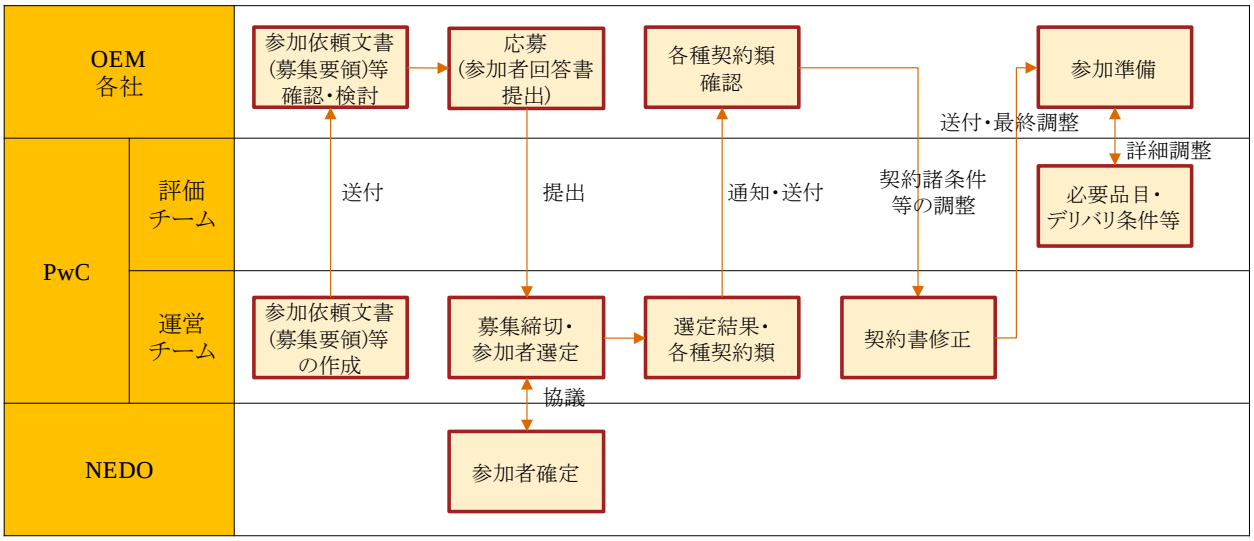


図 6-2　参加者募集フロー

6.1.2.　実施フロー②：　評価準備・実施及び評価結果まとめ

参加者確定後の実証実験準備から実施に関するフローは以下を想定している。

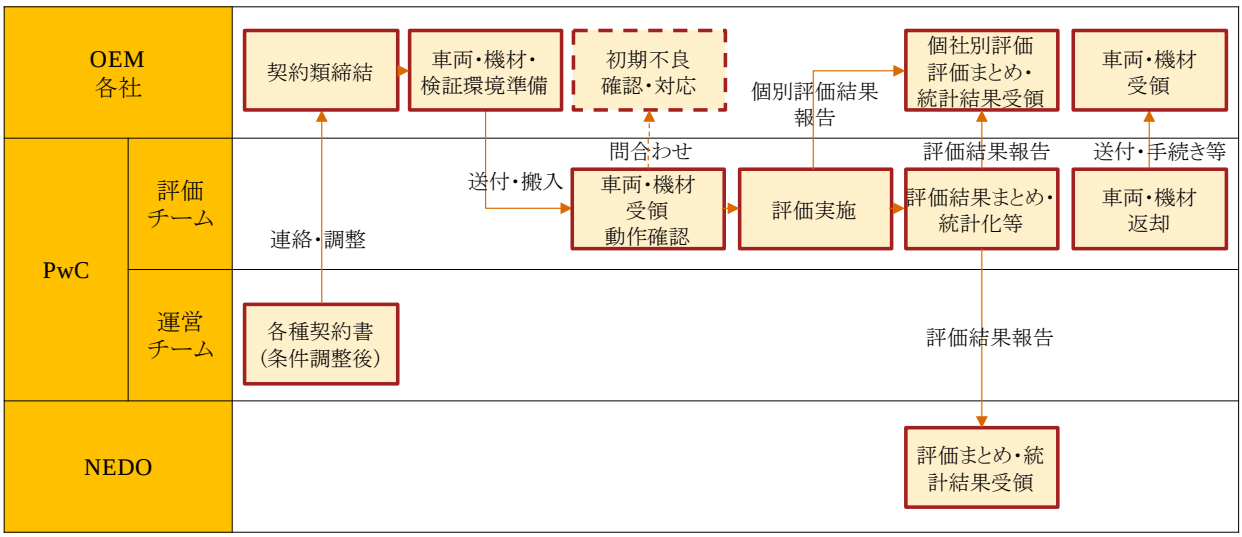


図 6-3　評価準備・実施及び評価結果まとめ

6.2.　実証実験実施概要

6.2.1.　参加 OEM 各社にご支援頂く内容・タイムライン

実証実験に係る契約類締結後（18 年 8 月頃～）より、実証実験のタイムラインに沿って、参加各社に必要なご支援・ご協力を頂く。

実証実験中のタイムラインと作業内容は以下のとおり。

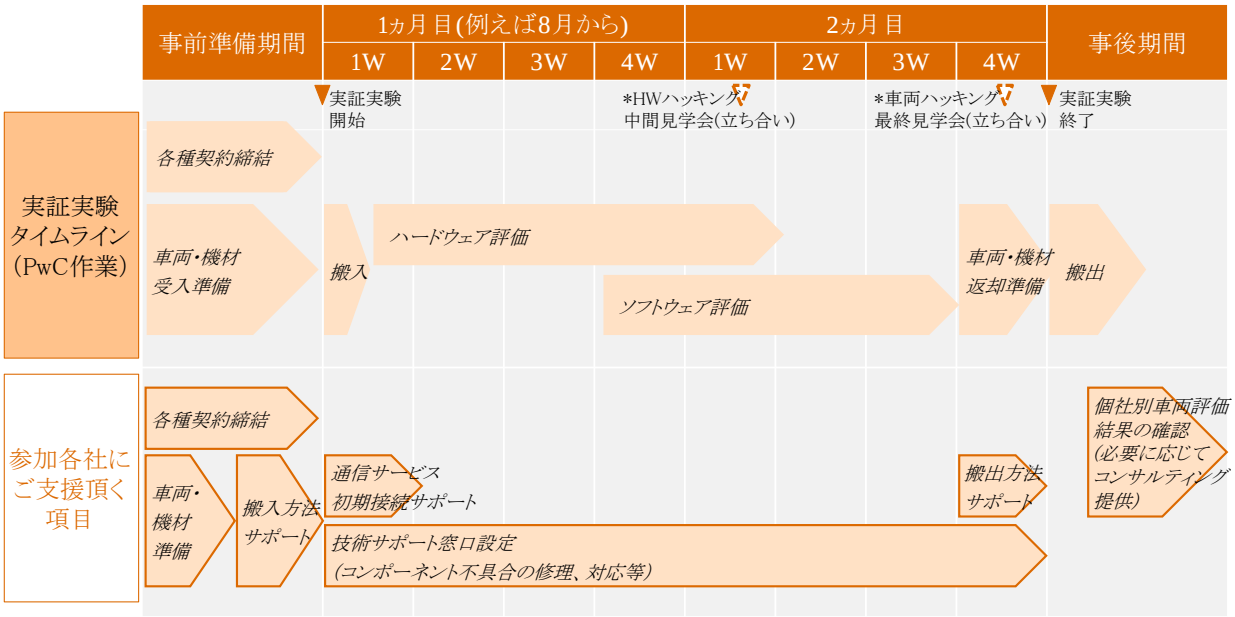


図 6-4　参加各社にご支援頂く内容・タイムライン

6.2.2.　各 OEM にご準備いただく品目

実証実験期間(4 カ月間を予定)において、以下の品目の提供を依頼する。

No.	品名	個数	必要条件・詳細	必須
1	実験車両* (商用車、開発車両も可)	1台	・実験車両からテレマティクスサービスに接続可能な状態であること (検証用のテレマティクスサービスでも可) 【備考】車両は通信コンポーネントを使用した実証実験評価結果の中で、特に重要な内容に関する実車テストに使用します。	○
2	情報系ECU	3セット	・テレマティクスサービスに接続可能なもの (検証用のテレマティクスサービスでも可) ・TCU、AVN等通信コンポーネントを含む ・携帯電話回線、Wi-Fi、BT等の機能を持つ通信コンポーネント含む	○
3	GatewayECU		・情報系ECUと直接接続されるもの	○
4	通信アンテナ	1セット	・GPS、携帯電話回線等	○
5	車内インターフェース		・一般ユーザが車内で利用するインターフェイス ・(ディスプレイ、マイク、USBポート、タッチパッド等)	○
6	情報系ワイヤーハーネス		・各終端にコネクタが付属したもの。加工していない状態でも可	○
7	各ECU毎の コネクタPIN構成	1セット	・どのPINが電源で何V必要なのか判別できるもの	○
8	配線図	1セット	・各情報系ECUおよびGateWayECUを含むもの	○
9	テレマティクス サービスアカウント	4個 (車両+部品合計セット数分)	・一般ユーザが利用可能なテレマティクスサービスが全て利用可能であること (検証用のテレマティクスサービスのアカウントでも可)	○
10	テレマティクス サービスサーバ	―	・上記アカウントで、ご提供いただいた実験車両または通信コンポーネントから接続可能なサーバをご用意いただき、実証実験期間中に稼働していただく 【備考】 ・当該サーバは検証環境/本番環境を問いませんが、以下を実施します: 1.一般ユーザが利用可能なサービスの利用 2.外部から参照可能なサーバ情報の調査 (ホスト名、証明書、利用ポート番号等) ・その他、テレマティクスサービスに影響を与える可能性のある行為は実施しない	○
11	各種マニュアル	各1部	・車両マニュアル、サービスマニュアル等の一般入手可能なマニュアル類一式	

表 6-1　参加者にご準備いただく品目一覧

6.2.3.　契約書案（規約、借用契約書、NDA 等）

実証実験参加各社と協議の上、必要に応じて参加規約類を策定する。また、ご参加いただく際には、実証実験に係る契約条件の合意・契約締結等を依頼する。

以下、実証実験に向けて用意した契約書・規約書類を記載する。

契約等	主な内容	雛型
参加規約	必要に応じて、参加申し込みをしていただく時点で了承いただきたい事項をご提示予定。 〈含む内容(想定)〉 実証実験の費用負担区分、実証実験の内容、実験車両(車両条件等)、安全管理、事前提出物・締結予定の契約に含む内容、実証実験の期間、協力要請事項、等	必要に応じPwCで準備
実証実験に係る契約	参加各社からの実証実験向けの動産(車両・機材等)の授受及び実証実験に必要な使用方法等に関して、以下の事項等を定める個別契約締結を想定。 • 賃料:無償借用等を想定 • 納品/返却条件:実証環境(場所)での納品/返却、輸送費は貸主負担を想定 • 使用方法:ハッキングの実施了承、機材の分解・改造等の現状変更実施の了承 • サポート:納品時動作説明、初期不良対応、実験中問い合わせ窓口の設定等 • 修繕費:実証実験(分解等)に起因しない故障、不具合等への貸主対応 • その他一般的な契約締結に係る内容(善管義務、解除条件・協議条項等)	PwCで準備*
秘密保持契約 (NDA)	• 提供車両・機材に係る機密情報、実証実験の評価内容・結果等の情報の秘密保持、情報取り扱いに関する契約締結を想定。	PwCで準備*
通信サービス利用に係る契約類	• OEM各社、各社指定の通信サービス事業者様等との通信に係る条件等協議し、必要に応じて契約締結を想定。	通信社の雛型等を活用

表 6-2　契約書案一覧

6.3. 評価体制および環境

6.3.1. 機密情報の取り扱いフローおよび体制

実証実験プロジェクト内における機密情報の取り扱い範囲を以下に示す。実証実験プロジェクト内であっても業務遂行に必要最小限で機密情報を取り扱うものとし、情報セキュリティ確保する。

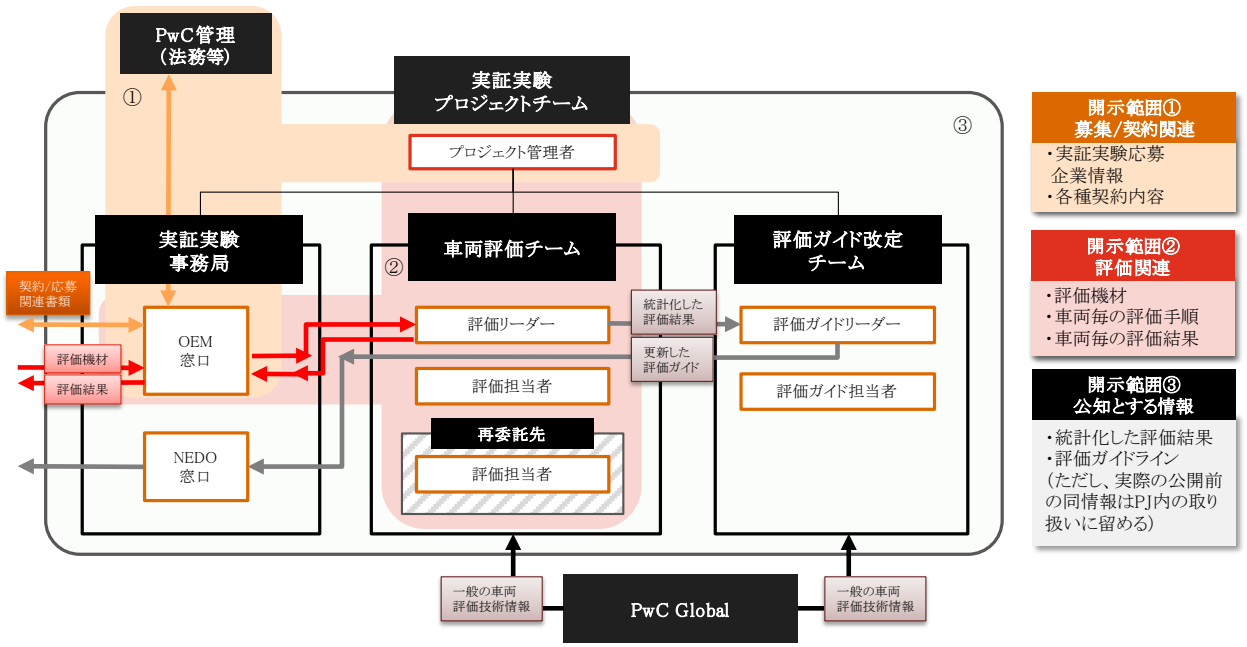


図 6-5　機密情報取り扱いフローおよび体制

6.3.2. 評価実施環境

実証実験における通信コンポーネントの実証環境（場所）は、十分な評価環境とセキュリティ対策が整備された PwC ハードウェアハッキングラボにて実施することを想定している。

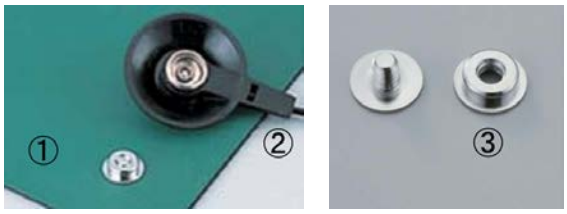
分類	概要
ハードウェア評価環境	静電気防止処理が施された床・机を整備。イメージと共に一部抜粋し記載する。 ①静電テーブルマット ②静電テーブルマット用グランドコード ③スクリュースナップキット 
セキュリティ対策	■ 実証実験は以下セキュリティ設備を有する施設で実施する ✓ カードリーダーと指透過認証による二要素認証を導入した、ラボ入退室管理システム ✓ 監視カメラによるラボ内の常時監視 ※直近3カ月の映像データは、ビデオレコーダにて録画し保存。 ■ PwCのメンバー含め、本案件における実証実験専用の機材やPCのみを使用することとし、外部からの他プロジェクトでも使用しているPC、機材等持ち込み禁止。

表 6-3　車両コンポーネントの評価設備

7 まとめ

7.1. 本事業の成果

本年度の事業においては、平成 30 年度での実証実験の実施に向けた事前調査として、「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」の調査活動を行った。

「a. 脅威分析調査」
自動車メーカ、部品サプライヤ、IT 企業などの自動運転・コネクテッドカーに係る取り組みをファクトベースで調査し、整理・類型化することで自動走行システム共通モデルを導出した。また、導出した自動走行システム共通モデルをベースに V2X 等車外からの攻撃を含む脅威項目を抽出し、脅威項目ごとに車両システムにおける影響度評価を実施した。影響度評価の結果、特に重大な脅威については、対策状況を調査し、必要に応じて別途作成した評価ガイドラインに反映した。

「b.情報セキュリティ評価ガイドラインドラフトの作成」
車両 OEM 各社等のステークホルダーとの議論の結果を踏まえて、車両開発の V 字モデルにおける総合評価などで活用できるガイドラインとする方針とし、ガイドラインドラフト版として策定した。評価項目の選定にあたっては、既知の車両セキュリティインシデントにおける攻撃者のプロファイルを分析し、攻撃者が高度な技術レベルや設備を持つ場合もカバーする評価内容として策定した。

「c. 情報セキュリティ評価の試行調査」
策定した評価ガイドラインドラフトを用いて、実際の車両部品システムに対して評価を行い、評価ガイドラインの妥当性の確認と修正を行った

「d. 実証実験の運営準備」
平成 30 年度の実証実験の実施計画を立案し、実証実験参加プロトコル、実証実験情報管理手法、実証実験環境などを整理した。また、実証実験の円滑な推進のために、実証実験参加者に周知および合意すべき事項を明らかにし、参加者募集要項、参加規約、各種契約文書案などを用意した。

7.2. 総括

本調査を通じて、自動走行システムの共通モデルを導出し、自動走行システムに係る脅威の全体像を明らかとした。また、明らかにした脅威のうち特に重要な脅威については策定した情報セキュリティ評価ガイドラインドラフトに評価項目として取り入れ、将来の自動走行システム開発で求められるセキュリティ評価を形作ることができた。
本事業で策定した平成 30 年度実証実験の計画をもとに、車両 OEM 各社に対して実証実験の参加を募り、参加者の車両を対象に策定した情報セキュリティガイドラインドラフト用いてを対象車両の対ハッキング性能を評価することで汎用的に利用可能な評価ガイドラインを策定、最終化し、将来の自動走行システムに開発での標準とすることが求められる。

自動車のサイバーセキュリティの確保は、自動車の安全（セーフティ）にも影響を与えることも考えられるため、最低限満たすべきセキュリティ水準については日本の業界全体の協調領域とすることが適切であり、これにより開発効率の改善を図ることも可能となり、日本企業の国際的な競争力維持にもつながる。また、定められたセキュリティ対策は、国内の業界における共有にとどめるのではなく、国際標準・標準規格に取り込むことで、不利な技術の普及により競争力を失うことが

ないよう、戦略的に標準化団体に働きかけることも重要である。
　以上を踏まえ、自動走行システムに係る情報セキュリティ活動は、重要な役割を持つものであり、次年度以降も 事業継続および発展に資する活動を期待するものである。

以上

契約管理番号：17101427-0