2019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）第 2 期
／自動運転（システムとサービスの拡張）／
新たなサイバー攻撃手法と対策技術に関する調査

2020年3月

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。

このような問題を解決するため、「戦略的イノベーション創造プログラム（SIP）第２期／自動運転（システムとサービスの拡張）／新たなサイバー攻撃手法と対策技術に関する調査」では、車両に対するサイバー攻撃手法の調査／分析、車両販売後における新たなサイバー攻撃への対策として、侵入検知システム（IDS）に着目して、IDS の動向および評価方法の検討および、テストベッドによる実機検証の実施が計画されている。

本年度の事業においては、「車両への攻撃動向調査」、「IDS 等のサイバーセキュリティ対策動向調査」、「IDS 評価方法の検討と基礎評価による検証」、「技術標準の策定・文書化（JASPAR との連携）」および「情報セキュリティガイドラインの更新方法の検討」を行い、活動成果としてまとめた。

「車両に対するサイバー攻撃動向調査」については、２０１７年から２０１９年に国際会議等で報告された事例のリスク値を算出した。リスク値の算出にあたり、各報告事例は、報告者や組織によって内容や調査範囲が異なることから、同一基準で分析・比較する手法を検討し、各事例に対して車両システムの共通モデルに基づいた攻撃シナリオ化および容易度、影響度の評価並びにリスク値の算出方法を定義した。

「防御技術に関する調査」については、公開情報および各ベンダーへのヒアリングを通じて製品の提供形態や、検知方式、ログ収集、管理方式などの調査を行った。

「IDS 評価方法調査」では、有識者並びにベンダーからのヒアリング結果、公開文書、前述の「車両に対するサイバー攻撃動向調査」に基づき、次の 4 つの観点と評価方法を定義した。

１．基本仕様。目的、要求に適合するかどうかを判断するための観点。２．導入（PoC を含む）。対象となるシステムへの導入のしやすさを判断するための観点。３．運用。定常的なモニタリングや検知後のログの分析のしやすさなどを判断するための観点。４．検知性能。IDS としての基本的な性能を判断するための観点。

上記観点のうち、４．検知性能については、さらに５つの観点で実機による評価方法を定義し、IDS ベンダー１社によるご協力のもと、テストベッドを用いた実機による評価を実施した。

１．定常状態において検知しない。通常の操作、あるいは仕様上除外されたイベントで検知してはいけない。２．予期しないメッセージ／動作の検知。インジェクション攻撃などを検知すること。３．不正な機器の物理的な接続の検知。不正な診断機器や ECU の追加などを検知すること。４．マルウェア活動の検知。マルウェアによる通信や脆弱性攻撃を検知すること。５．プロトコルとしての異常の検知。想定されない診断プロトコルの使用や異常なメッセージのインジェクションなどを検知すること。

「技術標準の策定・文書化」では、JASPAR 情報セキュリティ技術ワーキンググループと連携を行い、ガイドの有効性確保のための更新体制、方法の検討のほか、第１期の成果として策定したペネトレーションテスト手法に基づいて、ECU ペネトレーションテストガイドの文書化を行った。

要約（英文）

The basis of automated driving systems, information such as high definition map data, data of vehicles, pedestrians, road infrastructure etc., are expected to be obtained primarily from external vehicular networks. Such information will be transferred to vehicle control/information devices to be used for vehicle control in the automated driving system. This could lead to cause cybersecurity issues that did not exist before, in the time of conventional non-connected cars.

"Strategic Innovation Promotion Program (SIP) Phase 2/Automated Driving (Expansion of Systems and Services)/Research on New Cyber-attacks and Countermeasures against New Cyber-attacks " aims to solve such issues through research and analysis on cyber-attack methods as well as its countermeasures, especially Intrusion Detection System (IDS) to protect vehicles in the field against new cyber-attacks. The project also covers research and development of evaluation methods for IDS as well as conducting trial evaluation of the actual IDS product using a vehicle test bed.

In this year, following activities were conducted and summarized into this report: "Research on the Trend of Cyber-attack against Vehicles", "Research on Cybersecurity Countermeasures such as IDS", "Research on IDS Evaluation method and Trial Evaluation", "Development and Documentation of Technical Standard (in collaboration with JASPAR)" and "Investigation on Update Framework of Information Security Evaluation Guideline"

For the "Research on the Trend of Cyber-attack against Vehicles", the risk values were calculated for the cases reported during 2017 to 2019 at international conferences and other major events. In calculating risk values, methods for analyzing and comparing each reported case with the same criteria were examined since the contents of the reports were inconsistent in the scope and level of detail described depending on the writer and/or publishing organization. For each case, an attack scenario and attack feasibility using a common model of vehicle systems and impact were defined to calculate the risk values.

As for the "Research on Cybersecurity Countermeasures such as IDS ", the service model of the product, detection method, log collection, management system, etc. were investigated through public information and interview with each vendor.

The "Research on IDS Evaluation Method and Trial Evaluation" defined the following four aspects and methods for the evaluation based on the result of interviews with the experts and vendors, public documents, and the result of aforementioned " Research on the Trend of Cyber-attack against Vehicles".

1. Basic specifications: Determine compliance with the objectives and requirements. 2. Implementation (including PoC): Determine the feasibility of implementation to the target system. 3. Operation. Determine the feasibility of regular monitoring and analysis of logs after detection. 4. Detection performance. Determine the basic performance as an IDS.

For "4. Detection performance", an evaluation method covering five criteria was defined and trial evaluation using the method was conducted to an actual IDS product on a test bed with the cooperation of a IDS vendor.

The five criteria are: 1. No detection during steady state, normal operation or by the events excluded by specification. 2. Detection of unexpected message/activities

including injection attacks, etc. 3. Detection of physical connection of unauthorized devices such as fraudulent diagnostic equipment or the addition of ECUs. 4. Detection of malware activity such as malware communications and vulnerability attacks. 5. Detection of abnormality in the protocol such as unexpected use of diagnostic protocols or the injection of anomalous messages.

In "Development and Documentation of Technical Standards", Vehicle ECU penetration testing guideline using the outcome of the "Information Security Field Operational Test" during SIP phase 1 in collaboration with JASPAR Information Security Technology Working Group Testing Team as well as the update framework and method for ensuring to maintain effectiveness of the guideline.

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（SIP）第2期／自動運転（システムとサービスの拡張）／新たなサイバー攻撃手法と対策技術に関する調査」として、車両に対するサイバー攻撃の調査およびリスク値の評価方法の検討と算出、防御技術の調査、IDS の評価方法の検討とテストベッドによる実機評価結果、および昨年度成果である評価ガイドラインを用いた JASPAR との連携による文書化についてまとめたものである。

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。

このような問題を解決するため、「戦略的イノベーション創造プログラム（SIP）第２期／自動運転（システムとサービスの拡張）／新たなサイバー攻撃手法と対策技術に関する調査」では、車両に対するサイバー攻撃手法の調査／分析、車両販売後における新たなサイバー攻撃への対策として、侵入検知システム（IDS）に着目して、IDS の動向および評価方法の検討および、テストベッドによる実機検証の実施が計画されている。

本年度の事業においては、「車両への攻撃動向調査」、「IDS 等のサイバーセキュリティ対策動向調査」、「IDS 評価方法の検討と基礎評価による検証」、「技術標準の策定・文書化（JASPAR との連携）」および「情報セキュリティガイドラインの更新方法の検討」を行い、活動成果としてまとめた。

2. 本研究調査の目的と活動概要

「戦略的イノベーション創造プログラム（SIP）第 2 期／自動運転（システムとサービスの拡張）／新たなサイバー攻撃手法と対策技術に関する調査」における研究開発計画及び目的、目標に合致する形で、下記 2 つの活動を 2019 年 7 月～2020 年 3 月の期間で実施した。

#	目的	PwCによる活動概要
1	車両に対するサイバーセキュリティに関して、新たなサイバー攻撃手法がBlackHatを初めとする国際会議等で継続的に報告されている。また、車両販売後の新たなサイバー攻撃手法への対策として、悪意ある第三者からの車両へのサイバー攻撃に対する侵入検知システム（IDS）が注目されている。 これらを踏まえ、新たなサイバー攻撃手法の動向と対策技術の調査を行う。	**「a.新たなサイバー攻撃手法及び侵入検知システム（IDS）等の動向及び評価方法調査」** ✓ 過去2年および本年度に報告された新たな攻撃手法・インシデントについて攻撃再現方法を含め調査し、インパクト・リスクを評価する ✓ 攻撃手法に対応する対策手法をまとめ、それら対策の技術的・運用的な有効性を評価する手法を検討し、基礎評価を実施する ✓ 上記作業を将来にわたって効率的に実施するため「車両攻撃のシナリオ化」、「シナリオに基づくリスク分析」、「対策立案」、「対策評価」のフレームワークを構築する
2	さらに車両セキュリティ標準検討組織等と連携し、新たなサイバー攻撃手法に対応するための技術標準（案）を策定する。	**「b. 車両情報セキュリティに関する新たな攻撃手法等への対策方法の調査」** ✓ JASPAR情報セキュリティ技術ワーキンググループ／ペンテストSTMにおいて、車両情報セキュリティに係る対策技術、技術標準化範囲の検討および情報収集を推進する ✓ 上記の場にて、SIP第1期で検討した新たな攻撃方法への対策となるペネトレーションテストの技術標準の策定を進める

図 2-1　研究調査の目的と PwC による活動概要

第 3 章にて「a. 新たなサイバー攻撃手法および侵入検知システム（IDS）等の動向及び評価方法調査」の活動である、「車両に対するサイバー攻撃動向調査」、「防御技術に関する調査」、「IDS 評価方法調査」の取り組み結果をまとめる。第 4 章にて、「b. 車両情報セキュリティに関する新たな攻撃手法等への対策方法の調査」に関して、昨年度成果を活用し、JASPAR と連携して実施した「技術標準の策定・文書化」及び「更新方法の検討」の取り組みについてまとめる。

3. a. 新たなサイバー攻撃手法および侵入検知システム（IDS）等の動向及び評価方法調査

本章では、「a. 新たなサイバー攻撃手法および侵入検知システム(IDS)等の動向及び評価方法調査」に関する内容についてまとめる。本活動は、「攻撃動向の調査」、「防御技術の調査」及び「IDS 評価方法の検討と基礎評価による検証」の項目で構成される。

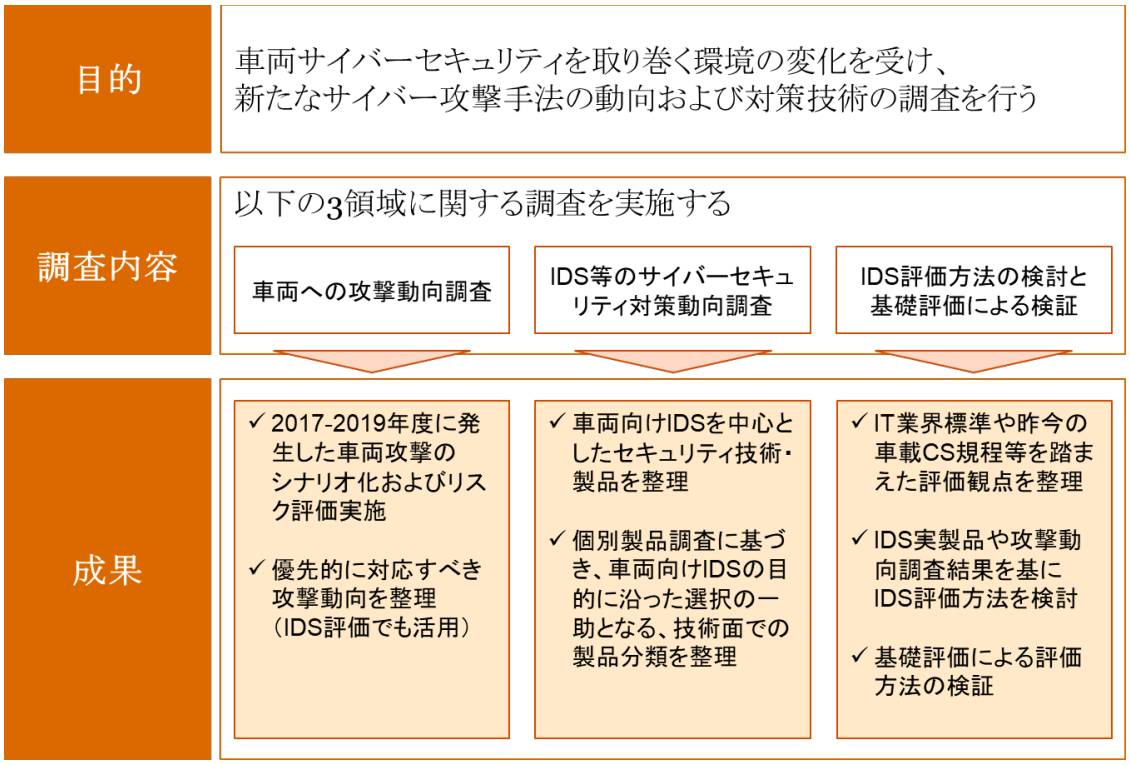

図 3-1 「a. 新たなサイバー攻撃手法および侵入検知システム(IDS)等の動向及び評価方法調査」の活動成果概要

3.1. 攻撃動向の調査

攻撃動向の調査活動では、２０１７年から２０１９年度に発生した車両攻撃をシナリオ化・リスク評価し、攻撃動向を整理した。これは、車両関係各社が、現在の車両セキュリティ環境のサイバーセキュリティリスクを分析し、セキュリティ対策を検討する際の基礎として活用できる。

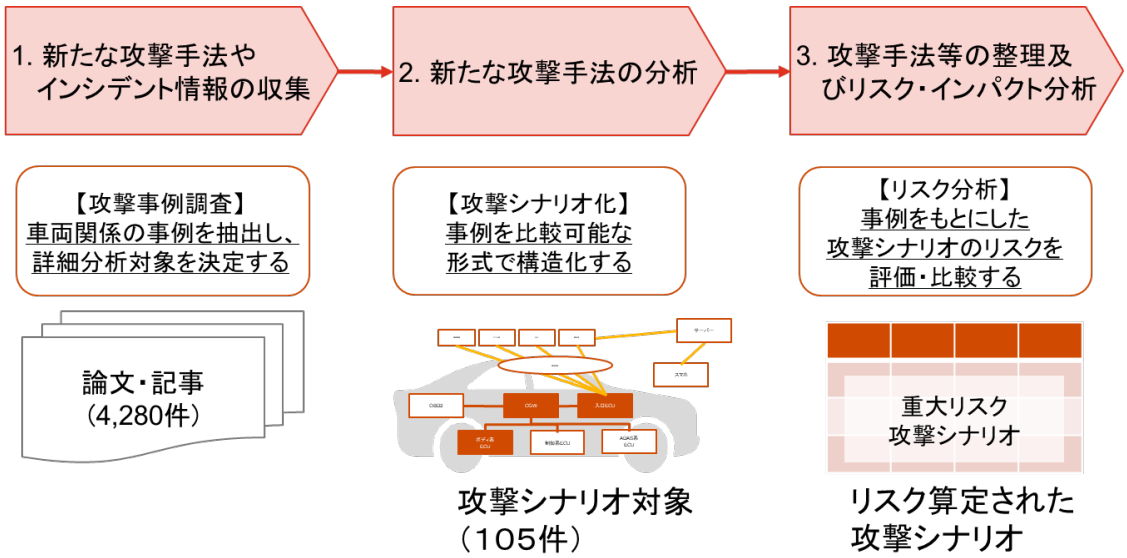

図 3-2　車両に対するサイバーセキュリティ動向の調査方法

3.1.1. 新たな攻撃手法やインシデント情報の収集

本調査では、以下の情報源を調査し、車両セキュリティにかかわる対象を選定基準に沿って選定することで、攻撃シナリオ化の対象を決定した。

カテゴリ	対象
論文	Blackhat, DEFCON, escar, RSA Conference, CHES, CODE BLUE, 電子情報通信学会, USENIX, etc.
脆弱性情報	CVE, NVD, JVN, JPCERT/CC
Web情報	主要セキュリティカンファレンス等で出展/研究発表する有力ベンダーのサイトのうち、指定したキーワードにマッチした記事

図 3-3　調査の情報源

情報源に対する選定基準は以下の通り。

i. 車両または、車両の部品に対する『攻撃事例』
ii. 対象が車両関連ではないが、車両制御に影響する可能性が高い攻撃事例（通信プロトコルの脆弱性を利用した攻撃など）

シナリオ化された事例は、情報源からの収集結果、４２８０件に対して選定基準に基づく一次分類の結果１０５件まで絞り込まれ、さらに情報源の内容を精査することで最終的に５８件となった。

3.1.2. 新たな攻撃手法分析

3.1.2.1. 前提条件

日々報告されている車両攻撃・脆弱性に関する事例は、報告者や組織によって報告内容や調査範囲が異なる。こうした事例を同一基準で分析・比較し、リスク評価のベースとする手法を検討した。

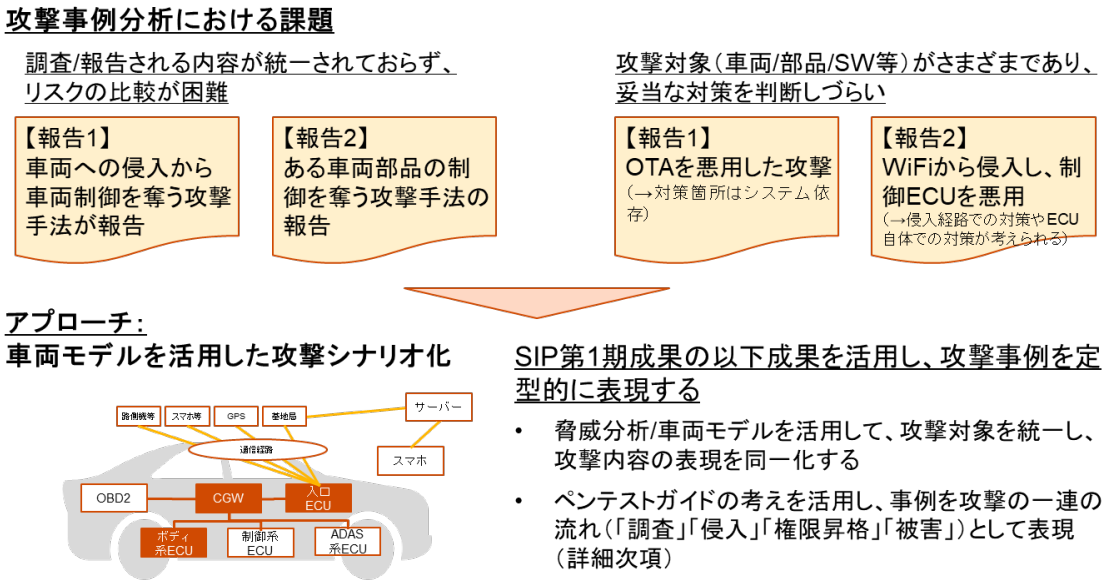

図 3-4 攻撃事例分析における課題と本活動におけるアプローチ

3.1.2.2. シナリオの表記方針

調査した攻撃事例は、攻撃シナリオとして以下のように表現する。

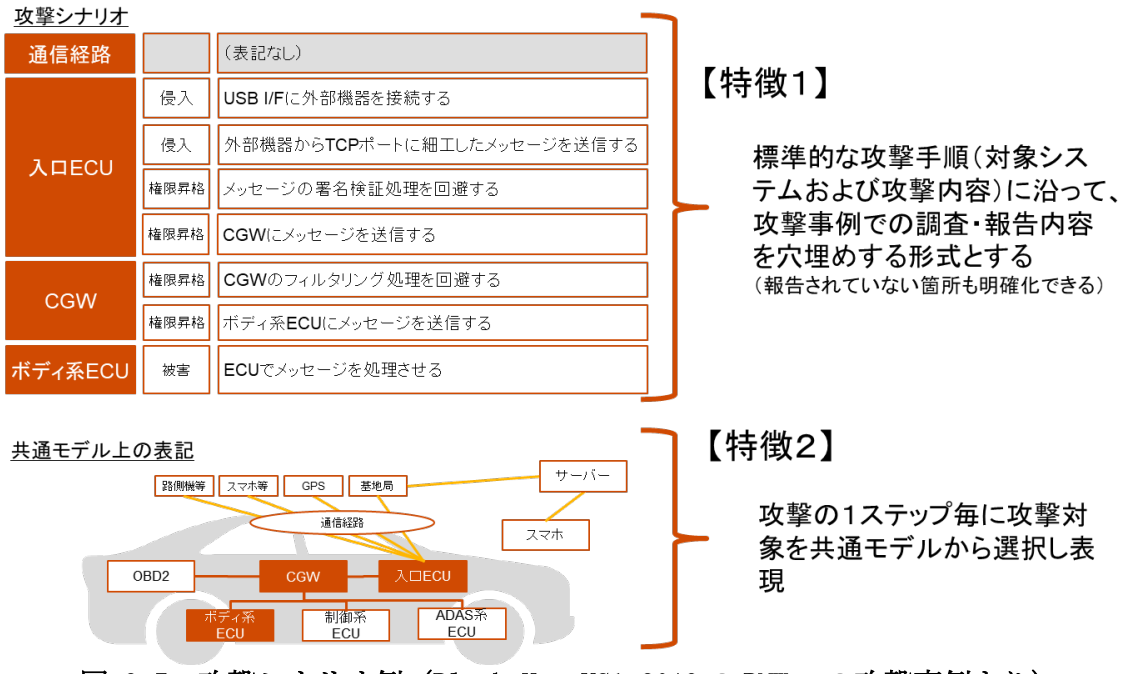

図 3-5 攻撃シナリオ例 (Black Hat USA 2019 の BMW への攻撃事例より)

3.1.3. 攻撃手法の整理及びリスク・インパクト分析

3.1.3.1. リスク・インパクト分析手法

自動車業界においてリ結おうされている脅威／リスク評価手法を参考に、前節で策定した車両共通モデルを活用した、攻撃シナリオのリスク・インパクト分析・評価手法を策定した。

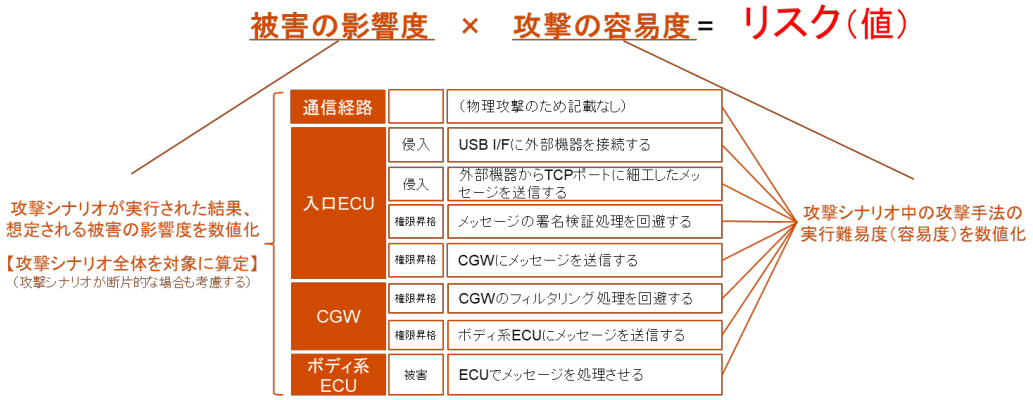

図 3-6 リスク・インパクト分析手法

3.1.3.2. 容易度の評価

攻撃手法に対して「専門スキル」、「攻撃の機会」及び「ツールの特殊性」の３つの要素について、それぞれ０～３のスコアを付与する。各要素については、RSMA（Risk Scoring Methodology for Automotive system）手法を基本とし、PwC により改定した。

表 3-1 専門スキル

Value	スコア	説明
Unknown	3	事例での記載なし、あるいは該当のシナリオ項目は攻撃を示すものではない
Layman	3	セキュリティ知識はないが、単純なドキュメントに従ってツールを利用することはできる
Proficient	2	セキュリティ分野の一般的な知識を有する
Expert	1	保護技術のアルゴリズム、プロトコル、OS やセキュリティの原理、新しい攻撃技術やツールに詳しいエキスパート
Multiple Expert	0	複数のエキスパート

表 3-2 攻撃の機会

Value	スコア	説明
Unknown	3	事例での記載なし、あるいは該当のシナリオ項目は攻撃を示すものではない
Critical	3	論理的に（遠隔から）いつでもアクセス可能 （例：GPS やセルラー網経由での攻撃など）
High	2	回数は限定的だが、論理アクセスが可能 （例：Wi-Fi や Bluetooth 経由の攻撃など）
Medium	1	車両への物理アクセスが必要であるが、特殊なツールを利用せずにアクセス可能 （例：USB や OBD I/F への接続）
Low	0	攻撃に車両の解体が必要

表 3-3 ツールの特殊性

Value	スコア	説明
Unknown	3	事例での記載なし、あるいは該当のシナリオ項目は攻撃を示すものではない
Standard	3	標準的なツール（簡単な OBD 診断機、ラップトップ PC、公開されている解析ツールなど）
Specialized	2	簡単には入手できない特殊なツール（車載ネットワークに直接接続する機器など） ※攻撃者が用意、利用できるのはここまでと想定する
Bespoke	1	取り扱いが制限された特注品か、非常に高価なツール
Multiple Bespoke	0	複数の特注品

各要素のスコアのうち、容易度が最も低い値（難易度が高い項目）を採用し、それらを合計することで「攻撃シナリオの容易度」を算出する。

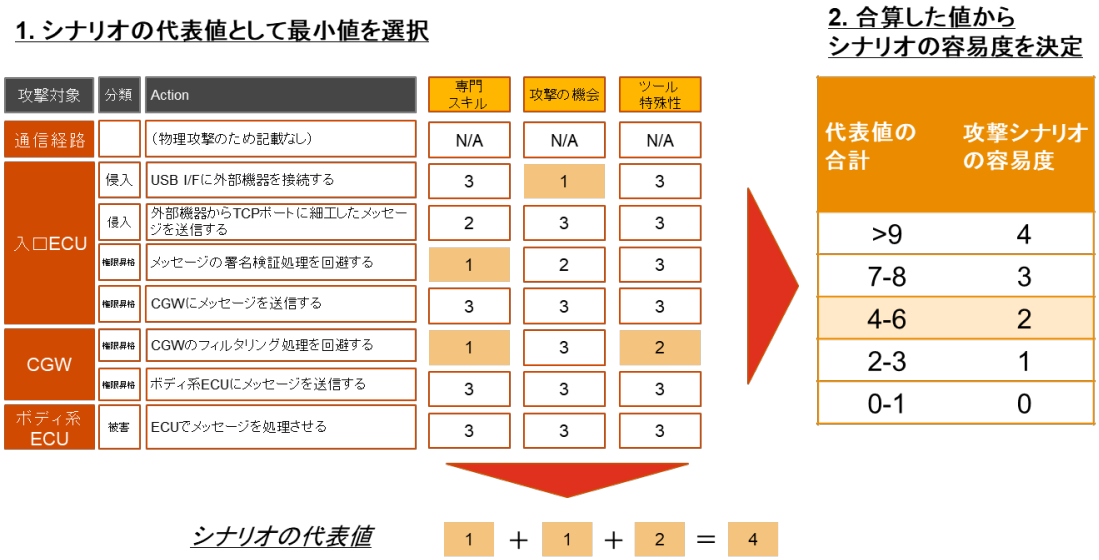

図 3-7　容易度の算出方法

3.1.3.3.　影響度の評価

攻撃シナリオの実行結果に関する想定被害に対して、「Safety」、「Financial」、「Operational」および「Privacy」への影響についてスコアを付与し、さらに各スコアの合計値から影響度の値を算出する。

表 3-4　Safety スコア

Value	スコア	説明
Critical	1000	生命を脅かす
High	100	重症
Moderate	10	軽い障害
No Injury	0	障害なし

表 3-5　Financial スコア

Value	スコア	説明
High	1000	組織にとって金銭的なインパクトがあり、組織の存続に影響する
Medium	100	組織にとって金銭的なインパクトがあるが、組織の存続には影響しない
Low	10	組織にとって金銭的なインパクトはあるが、対応可能
No Impact	0	組織にとって金銭的なインパクトはほぼなし

表 3-6　Operational スコア

Value	スコア	説明
High	1000	基本操作（走る、曲がる、止まる）に影響がある
Medium	100	自動運転に必要な機能（地図、センサー、自動駐車機能など）に影響がある
Low	10	車両操作に直接関連しない機能（音楽の再生、ライトの点灯など）に影響がある
No Impact	0	影響なし

表 3-7　Privacy スコア

Value	スコア	説明
High	1000	複数のステークホルダーのプライバシーに影響があり、且つ、金銭の侵害が可能
Medium	100	特定のステークホルダーのプライバシーに影響があり、且つ、金銭の侵害が可能
Low	10	特定のステークホルダーのプライバシーに影響があるが、金銭の侵害にはつながらない。
No Impact	0	プライバシーに影響なし

表 3-8　影響度のスコア

各スコアの合計値	影響度のスコア
1000 以上	4
100～999	3
20～99	2
1～19	1
0	0

3.1.3.4.　　リスク値の評価

下記のリスク評価マトリクスを用いて、「容易度のスコア」と「影響度のスコア」を合算し、５段階でリスクを評価する。

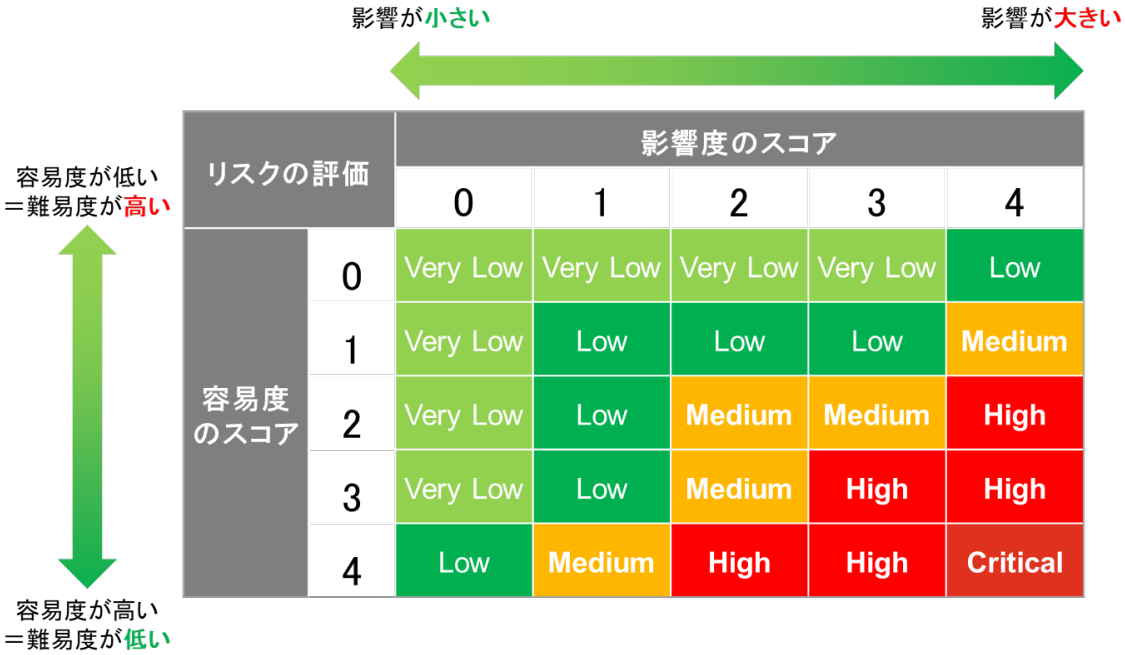

図 3-8　リスク・インパクト分析マトリクス

3.1.3.5. 策定したリスク・インパクト分析手法の特長

本調査のために策定したリスク・インパクト分析手法の特長は以下の通り。

I. 断片的な攻撃事例でも、統一手法でモデル化・リスク算定

侵入から被害発生まで一気通貫した攻撃から、部品単体レベルの攻撃の事例報告もある。この現況を踏まえ、情報が完全にそろっていないものも攻撃シナリオ化できる手法とし、その状態を踏まえたリスク算定ができる手法とした

- ✓ 攻撃成功できる情報量があるものが高リスクと判断し、情報欠落があるものはリスク値が下がる算定となっている

II. 攻撃手法にも注目したモデル化・リスク算定

攻撃シナリオでは、ATT&CKを利用し攻撃手法単位で表現した。また、攻撃難易度については攻撃手法単位で算定する手法とした。これにより、攻撃事例（＝シナリオ）全体でのリスク算定以外に、攻撃手法毎の傾向分析も可能としている

- ✓ 例として、攻撃手法の登場頻度を算出しており、登場頻度を重要視した対策優先度検討などが可能となっている

III. 従来手法との親和性を考慮したリスク算定

既存の脅威/リスク算定手法を可能な限り採用したことで、過去のリスク算定結果を一定範囲活用することが可能とした

図 3-9 リスク・インパクト分析手法の特長

3.1.4. 分析結果

各シナリオのリスク評価結果は下記を参照。なお、各事例のシナリオ分析結果は別紙を参照。

シナリオ ID	概要	重大度	攻撃者の専門性	攻撃の機会	必要なツール	容易度	容易度レベル	安全性への影響	事業への影響	車両操作への影響	プライバシーへの影響	影響度	影響度レベル
1	HU の OBD I/F または USB I/F 経由で TCP ポートで待ち受けているサービスにコマンドを送信し、TOCTOU の脆弱性を利用して K-CAN に CAN メッセージを送信し、ECU のリセットまたはシートの前後移動をさせることができた(3.1.2)	Medium	0	2	2	4	2	10	100	100	0	210	3
2	HU の USB I/F から細工したナビのアップデート管理ファイルを挿入し、アップデート管理ファイルを解析するプロセスの脆弱性を利用して ECU のリセットまたはシートの前後移動をする(3.2 Stack Overflow)	Medium	0	1	3	4	2	10	100	100	0	210	3

シナリオ ID	概要	重大度	攻撃者の専門性	攻撃の機会	必要なツール	容易度	容易度レベル	安全性への影響	事業への影響	車両操作への影響	プライバシーへの影響	影響度	影響度レベル
3	偽の基地局を設置して、BMW ConnectedDrive service のレスポンスを書き換えて攻撃者の Web サーバーにアクセスさせ、ブラウザの脆弱性等を利用して ECU のリセットまたはシートの前後移動をする(3.3)	Medium	0	2	2	4	2	10	100	100	0	210	3
4	偽の基地局から SMS 経由で ConnectedDrive の用の NGTP(BMW のリモートサービス)メッセージを送信し、リモートサービス用の機能を不正に利用する（ドアのオープン、ホーン、ライトの点灯等）(4.1.2)	High	1	2	2	5	3	0	100	10	0	110	3
5	偽の基地局と車両の通信に MITM 攻撃を行い Provisioning 用コンテンツの署名を改ざんして、TCU のバッファーオーバーフローの脆弱性を利用して、ECU のリセット、シートの前後移動をする(4.2, 4.3)	High	1	2	2	5	3	10	100	100	0	210	3
6	5G の仕様の不備により、セルラー網端末の device capability を改ざんし、通信速度を極度に低下させることができた。	Medium	0	2	2	4	2	0	10	10	0	20	2
7	5G の仕様の不備により、セルラー網端末が基地局に送る UE の capability の内容を改ざんし、セルラー端末のバッテリーの消費を 3 倍にすることができた。	Low	0	2	2	4	2	0	0	10	0	10	1
8	ECU の物理 I/F に機器を接続し、UDS コマンド実行時の認証処理中に瞬間的に高電圧をかけることにより特定の命令の実行をスキップさせ、security access をバイパスして ECU のファームウェアを抽出する	Medium	1	0	2	3	2	0	100	0	0	100	3
9	デバッグポートからのコマンド実行時の認証処理中に瞬間的に高電圧をかけることにより命令の実行をスキップさせ、ECU のファームウェアを抽出した	Low	1	0	2	3	2	0	10	0	1	11	1
10	回線交換フォールバックの脆弱性を利用して、基地局になりすますことができた	Very Low	0	0	2	2	1	0	0	0	0	0	0
11	セキュアブート中に瞬間的に高電圧をかけることにより命令の実行をスキップさせ、改ざんしたブートローダーをロードさせた	Medium	1	0	2	3	2	0	100	0	0	100	3
12	Adversarial Attack により、誤認識させる道路標識を作成し、70Km 速度制限を 30Km の速度制限と誤認識させた	Very Low	1	2	3	6	3	0	0	0	0	0	0

シナリオ ID	概要	重大度	攻撃者の専門性	攻撃の機会	必要なツール	容易度	容易度レベル	安全性への影響	事業への影響	車両操作への影響	プライバシーへの影響	影響度	影響度レベル
13	何らかの方法で、リモートからテレマティクスユニット経由で VIDS を侵害し、CANH/CANL に接続されたピンのモードを変更することで、マイクロコントローラーに最大電流以上の電流を流し、VIDS が搭載されたマイクロコントローラーを破壊する [前提条件] ECU に VIDS が搭載されている	Low	1	1	2	4	2	0	10	0	0	10	1
14	何らかの方法で、リモートからテレマティクスユニット経由で VIDS を侵害し、CANH/CANL に接続されたピンのモードを変更することで、ドミナントビット送信中にレセッシブビットを検知できなくなり、CAN バスにビット列を送信不可となる [前提条件] ECU に VIDS が搭載されている	High	1	0	2	3	2	10	100	1000	0	1110	4
15	何らかの方法で、リモートからテレマティクスユニット経由で VIDS を侵害し、CANH/CANL に接続されたピンのモードを変更することで、任意の ECU に CAN フレームの再送を強制する [前提条件] ECU に VIDS が搭載されている	High	1	0	2	3	2	10	100	1000	0	1110	4
16	Vipar 社のスマートアラームにおいて、サーバーの API の脆弱性により、正規ユーザーになりすまして車両を追跡したりエンジンを停止することができた。	Critical	2	3	3	8	4	10	100	1000	0	1110	4
17	車両に搭載されたネットワークサービス Subaru Starlink 用の Harman 製 IVI において、USB I/F から細工したアップデートプログラムをインストールすることができた	Low	1	1	3	5	3	0	10	0	0	10	1
18	Daimler Mercedes-Benz COMMAND のサービス運用妨害に関する脆弱性 [前提条件] 車両はサーバーからナビゲーションデータを受信して地図情報システムに利用している	Medium	1	3	2	6	3	0	10	10	0	20	2

シナリオ ID	概要	重大度	攻撃者の専門性	攻撃の機会	必要なツール	容易度	容易度レベル	安全性への影響	事業への影響	車両操作への影響	プライバシーへの影響	影響度	影響度レベル
19	Daimler Mercedes-Benz Me App において、アプリとサーバー間で利用している access token を盗んだあと、本人になりすましてサーバーにログインし、車両にアプリに公開されている機能を利用することができた。 同じ手法で複数種類の被害が発生するが、最も被害が大きい「ドアのロック／アンロック」のシナリオとした [前提条件] 正規ユーザーがサーバー経由で車両に対してリモートパーキング、ドアのアンロック、車両データ（位置情報、走行データ）の入手をリクエストすることができる。	Medium	1	1	2	4	2	0	10	10	0	20	2
20	車両遠隔操作用の StarLink サービスにおいて、Web アプリの認証に利用されるトークンを奪われた場合、正規ユーザーになりすましてドアのアンロックやホーンの操作、位置データの取得ができた	Medium	1	1	2	4	2	0	100	10	1	111	3
21	Continental 社が提供する TCU におけるリモートからのバッファメモリ制御の脆弱性	Very Low	1	2	2	5	3	0	0	0	0	0	0
22	SecurityAccess のための組み合わせが 256 通りしかなかったため、攻撃者が CAN バスへのアクセスができた場合、エアバックを膨らませることができた。	Medium	1	1	2	4	2	0	10	10	0	20	2
23	攻撃者によって正規ユーザーの「StarLink」アカウントのトークン情報が窃取されることで、車両をリモート操作（ドアロック、アンロック、ホーンを鳴らす、ライトの点灯）される可能性がある	Medium	1	2	3	6	3	0	10	10	0	20	2
24	APE の root 権限を取得したあと、攻撃者のサーバーから定期的にステアリングを制御するメッセージを取得し、さらに、タイムスタンプとカウンダーによるメッセージの正当性検証処理をバイパスしてステアリングをリモートから操作することができた	High	1	1	2	4	2	10	100	1000	0	1110	4
25	細工をした画像を投影することで、ワイパーを動かすことができた	High	2	3	3	8	4	0	10	10	0	20	2
26	ステッカーを道路上に配置することでレーンを誤認識させ、車を対向車線に誘導することができた	Critical	2	3	3	8	4	10	100	1000	0	1110	4
27	シトロエン DS5 1955 Limited Edition の IVI と同じ WiFi AP に接続してポートスキャンを行い、telnet サービスが公開されていること、	Medium	1	2	3	6	3	0	10	10	1	21	2

シナリオ ID	概要	重大度	攻撃者の専門性	攻撃の機会	必要なツール	容易度	容易度レベル	安全性への影響	事業への影響	車両操作への影響	プライバシーへの影響	影響度	影響度レベル
28	攻撃対象の ECU が CAN バスにドミナントビットを送出したタイミングで攻撃ノード等からドミナントビットを送出し、ビットエラーの閾値を超えて攻撃対象ノードでビットエラーを検出させ続け、攻撃対象 ECU をバスオフとする	Very Low	1	1	2	4	2	0	0	0	0	0	0
29	Subaru のキーレスエントリーシステムのキーフォブでリプレイ対策として利用されているローリングコードがランダムでなかったため、簡単に正規のキーフォブになりすますことができた。	Very Low	1	1	2	4	2	0	0	0	0	0	0
30	Tesla 車両のスマートキーにおいて、弱い認証方式が利用されていたため、攻撃者が正規のキーフォブになりすますことができた	Very Low	1	1	2	4	2	0	0	0	0	0	0
31	攻撃者の WiFi AP に接続させてブラウザと OS の脆弱性を利用して IVI 上で root 権限で任意のコードを実行可能としたあと、APE(Autopilot ECU)の install コマンドを実行し、攻撃者のサーバーから細工した FW を DL してインストールさせることができた。	Medium	1	0	2	3	2	10	100	100	0	210	3
32	PCI express カードに実装された HSM モジュールの署名検証処理にバッファーオーバーフローの脆弱性があり、細工をしたファームウェアを書き込むことができた	Low	0	0	2	2	1	0	100	0	0	100	3
33	LTE には、CS (Circuit Switched:回線交換) フォールバック機能があるが、CS フォールバック利用時は、認証処理が行われない。この場合、攻撃者が端末と基地局の通信に対して MITM 攻撃を実施することができる。	Very Low	1	3	2	6	3	0	0	0	0	0	0
34	「検出」と「識別」を同時に行う画像認識の 1 手法である YOLO(You Only Look Once)手法に対して、ノイズを加えることで画像をご認識させた（いわゆる Adversarial 攻撃)	Very Low	1	2	3	6	3	0	0	0	0	0	0
35	Linux kernel の L2CAP スタックのバッファーオーバーフローの脆弱性により、近接するデバイスに対して root 権限で任意のコードを実行することができた	Medium	1	2	3	6	3	0	10	10	0	20	2
36	WiFi 機器を接続するための WPA2 認証プロトコルの 4-way handshake 処理において、プロトコルの仕様に脆弱性があり、通信内容の傍受／改ざん／再送が可能であった	Medium	1	2	3	6	3	0	10	10	1	21	2

シナリオ ID	概要	重大度	攻撃者の専門性	攻撃の機会	必要なツール	容易度	容易度レベル	安全性への影響	事業への影響	車両操作への影響	プライバシーへの影響	影響度	影響度レベル
37	rowhammer と呼ばれる DRAM で発生するメモリセル間で電気的な相互作用を原因とした問題を、サイバー攻撃に流用した手法。rowhammer への従来緩和策を潜り抜ける新たな手法により、root 権限/kernel 権限を奪うことができた（現象自体は過去事例と同様）	Low	1	1	3	5	3	0	10	0	0	10	1
38	Linux kernel v3.17 以降で使える USB/IP の処理は高権限で実行されるため、悪意のある者が範囲外のメモリアクセスをトリガーし、カーネルメモリに任意のデータを書き込むことができる可能性がある。リモートからの攻撃が可能となる可能性が高い。	Low	1	1	3	5	3	0	10	0	0	10	1
39	主要ブランド 4G モジュール（15 種類以上）を調査したところ、脆弱なパスワードを使用したリモートアクセス、AT コマンド/リスニングサービスのコマンドインジェクション、などいろいろな脆弱性が見つかった。攻撃は、偽の基地局からの通信・オペレーターのイントラからの攻撃・Private APN 経由の攻撃がありえ、Private APN 経由の攻撃で車両乗っ取りができた	High	1	3	3	7	3	0	100	10	0	110	3
40	マルウェアで BPF_PROG_TYPE_SOCKET_FILTER タイプの eBPF プログラムをシステムコールにアタッチすることで、kernel または任意のユーザープログラムのメモリを読み込んだり、任意のコード(ROP:Return Oriented Program)を実行することができた。	Low	1	3	3	7	3	0	10	0	0	10	1
41	マルウェアで BPF_PROG_TYPE_SOCKET_FILTER タイプの eBPF プログラムをシステムコールにアタッチすることで、kernel または任意のユーザープログラムのメモリを読み込んだり、任意のコード(ROP:Return Oriented Program)を実行することができた。	Low	1	3	3	7	3	0	10	0	0	10	1
42	AES 等のブロック暗号の秘密鍵を見つけるための計算速度最適化方法とそのツールを提示。	Medium	0	3	3	6	3	0	10	0	10	20	2
43	BTLE 5 のチャンネルセレクションアルゴリズム(CSA #2)で利用されている PRNG について、生成方法に問題があったため（公開情報である各機器の Access Address とカウンターから生成されていた）、通信内容を傍受することができた。	Medium	1	2	2	5	3	0	10	10	0	20	2

シナリオ ID	概要	重大度	攻撃者の専門性	攻撃の機会	必要なツール	容易度	容易度レベル	安全性への影響	事業への影響	車両操作への影響	プライバシーへの影響	影響度	影響度レベル
44	GSM で利用されている暗号方式 A5/1 と A5/3 の仕様の不備により、暗号化された GSM 通信内容と利用されているチャンネルから、平文の通信内容を入手することができた	Medium	1	2	2	5	3	0	10	0	10	20	2
45	TLS 1.3 の 0-RTT 方式を利用する通信において、通信に MITM し、パケットを再送することができた（リプレイ攻撃） ※そもそも、通信速度を重視した 0-RTT の仕様では、リプレイされても問題ない場合のみ、0-RTT を利用可とあり、0-RTT 禁止としているブラウザも多い。多くのサーバーで 0-RTT 禁止としている。	Medium	1	3	3	7	3	0	10	10	0	20	2
46	ARM Cortex M が搭載された NXP 社の SOCs において、JTAG や MCU から FPB(Flash Patch and Brake Unit)のファームウェアアップデート機能を呼び出して、SoC の識別子を変更してチップのファームウェアを書き換えることができた。	Very Low	1	1	2	4	2	0	0	0	0	0	0
47	PIE (position-independent executable)な実行ファイルにおいて、heap overflow がない状態でも任意のコードを実行することができた。	Very Low	1	1	2	4	2	0	0	0	0	0	0
48	GPS シミュレーターを利用して、GPS レシーバーを接続した NTP サーバーの時刻を改ざんした	High	1	2	2	5	3	10	100	100	0	210	3
49	Continental 社の TCU において、既存の脆弱性(*1)を利用してリモートから細工した AT コマンドを送信し、任意のコードを実行されることができた。 (*1) AT コマンドにおいて、TMSI の処理にバッファーオーバーフローの脆弱性があった	Medium	1	1	2	4	2	0	100	10	0	110	3
50	Honda Civic の EPS（電動パワーステアリングシステム）において、ファームウェアを取り出すためのパスワードが容易かつファームウェアの改ざんのチェック機能がなかったため、ファームウェアを改ざんして低速時の自動運転を可能とすることができた（仕様では低速走行時は自動運転不可）	Medium	1	1	2	4	2	10	10	100	0	120	3
51	キーレスエントリー用イモビライザー等で利用されている車両用のブロック暗号 AUT64 において、仕様や実装に複数の脆弱性があったため、現実的な時間（8round の場合は数 msec）で暗号を破ることができた。	Low	0	2	2	4	2	0	10	0	0	10	1

シナリオ ID	概要	重大度	攻撃者の専門性	攻撃の機会	必要なツール	容易度	容易度レベル	安全性への影響	事業への影響	車両操作への影響	プライバシーへの影響	影響度	影響度レベル
52	Velodynes 社の Lider に対して、同じ波長の光を特定の距離／角度から照射することで、センサーに無数の dot を誤認識させ、さらに実際の物体を認識不可とさせることができた	Very Low	0	2	2	4	2	0	0	0	0	0	0
53	Velodynes 社の Lider が出力した光波を受信し、遅延させて、特定の距離／角度から再度攻撃対象の Lidar に照射することで、センサーに無数の dot を誤認識させることができた	Very Low	0	2	2	4	2	0	0	0	0	0	0
54	攻撃対象の CIDS が接続された CAN ネットワーク上の既存の CAN ノードを乗っ取り、そのノードの CID と細工をしたタイムスタンプを指定してパケットを送信することで、CAN パケットの周期性を利用する CIDS(Clock-based IDS)の防御機能を無効にすることができた。	Very Low	1	0	2	3	2	0	0	0	0	0	0
55	市販の機器(SLD: Speed Limit Defender)を C 車載ネットワークに接続し、VSS が送信したスピードを通知するメッセージを破棄または偽のメッセージを送信し、最高速度（180Km/h）以上での走行を可能とした ※VSS(Vehicle Speed Sensor)：車輪の回転数から車両速度を検知する機器	Medium	1	0	2	3	2	0	10	10	0	20	2
56	Tesla Model S のパッシブキーレスエントリー＆スタートシステム(PKES)において、古い暗号アルゴリズムである DST40 を利用していたため、40bit の Challenge に対するありうるレスポンスのリストを事前に計算しておくことでレスポンスの探索空間を小さくして時間内にレスポンスを返すことができた	Medium	1	1	2	4	2	0	10	10	0	20	2
57	NW 上のノードを物理特性を利用して、車載 NW 上の特定のノード間で秘密鍵を共有するためのプロトコルである PnS(Plug-and-Secure) CAN において、サイドチャネル攻撃により秘密鍵を計算することができた	Low	1	1	2	4	2	0	10	0	0	10	1
58	ISO 15118 を実装した車両－充電ステーション間の通信において、電磁放射(EMR)を傍受する（サイドチャネル攻撃）オープンソースツールの HomePlug GreenPHY (HPGP)を利用して PLC の通信内容を入手した。 ※ISO/IEC 15118：EV の充電規格のうち、車両－グリッド間の通信規格	Low	1	1	2	4	2	0	10	0	1	11	1

3.2. 防御技術の調査

3.2.1. 調査概要

主要OEM、サプライヤー、セキュリティベンダーに対して調査を実施する。なお、主要OEMについては、JASPARを通じて調査を行った。

調査は、公開情報調査に加えて、IDS ベンダーを中心にインタビューによる調査を実施し、併せて基礎評価への参加についても調整を行った。

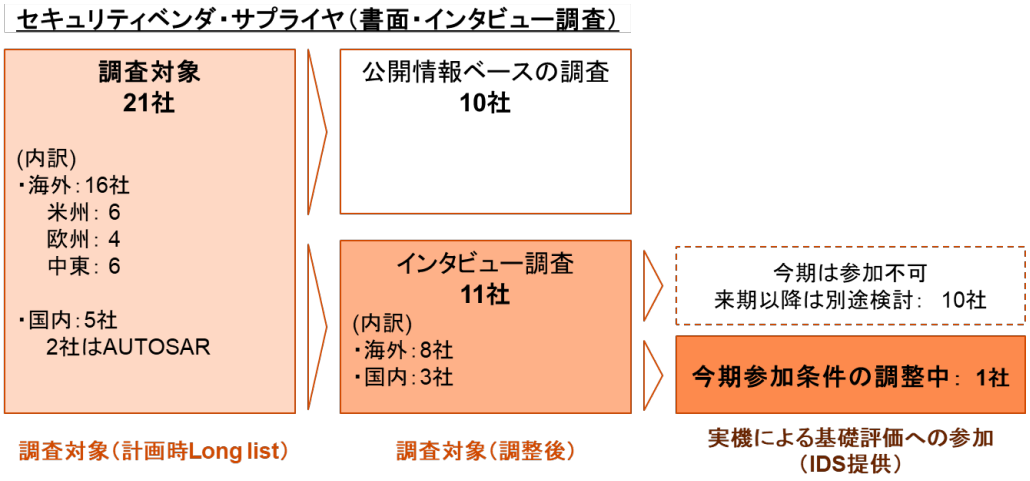

図 3-10

3.2.2. 情報公開範囲の調整

インタビューを行った企業から提供を受ける情報、および提供を受けた IDS 製品を用いた評価結果などについては、以下の範囲での開示を検討した。なお、最終的な対象情報および開示範囲については各企業と事前に協議、合意の上対応する。

分類	情報名	開示対象			
		PwC	NEDO(SIP-adus関係者含む) NDAあり	OEM等関係者	一般公開
技術調査（インタビュー）結果	インタビュー協力企業名	○	○	○	○
	技術動向、評価手法に関するご意見(*1)（匿名）	○	○	○	○
	製品仕様(*1)	○	協議	協議	協議
IDS評価フレームワーク	技術評価結果を基に策定したIDS評価フレームワーク	○	○	○	○
IDS基礎評価結果	会社・製品名	○	○	協議	協議
	評価結果（作業で判明した製品仕様を含む）（匿名）	○	○	協議	協議

図 3-11　情報公開範囲

3.2.3. ヒアリング項目

技術動向調査の一環として、車両セキュリティ技術全般の動向について以下の質問項目で調査を行った。

ID	質問
1-1	車載IDSについて、注目している製品はありますか？
1-2	車載IDS以外に、車載システム（単体ECUを含む）に対するセキュリティ対策技術として注目している技術はありますか？
1-3	車載システム（単体ECUを含む）に対するセキュリティ対策技術に関して、注目しているコミュニティや研究機関はありますか？
1-4	IDS/IPS製品を評価する際にどのような観点が重要と思いますか？ 以下1～5から選択ください。また、選択した理由について簡単に記載ください。（複数回答可） 1. 検知性能 2. 運用時の使いやすさ 3. 車両への導入のしやすさ 4. コスト 5. その他

図 3-12　車載セキュリティ対策技術の動向

また、各ベンダーについては製品やソリューションに関して以下の質問項目で調査を行った。

ID	カテゴリ	質問概要	NIST*のカテゴリ
2-1	製品の提供形態	ソフトウェア／ハードウェア構成および動作要件	概要
2-2		ライセンスモデル	概要
2-3		完成品の提供に必要な情報や作業	概要
2-4	ログの管理、分析方式	ログの保存範囲	セキュリティ機能
2-5		ログの保存および転送先と方式	セキュリティ機能
2-6		ログの分析タイミング	セキュリティ機能
2-7		セキュリティイベント検出方式／アルゴリズム	セキュリティ機能
2-8		セキュリティイベント検出方式／アルゴリズムのカスタマイズ可否	セキュリティ機能
2-9		ログの保全（完全性）	セキュリティ機能
2-10		ログの保全（機密性）	セキュリティ機能
2-11		ログの保全（可用性）	セキュリティ機能
2-12	運用	ログの分析基盤との連携	ライフサイクルコスト
2-13		検知方式／アルゴリズムの更新可否／頻度	その他
2-14		製品のEOLポリシー	その他
2-15		他車種への移植可能性	その他
2-16	その他	導入実績	その他
2-17		上記以外の他社製品との違い	その他

図 3-13　IDS 製品仕様

IDS の評価方法策定に向けたインプットとして、既存の評価方法や課題について以下の項目で調査を行った

ID	質問
3-1	これまでにIDSの第三者評価（競合調査）を実施、あるいは受けたことがありますか？ある場合、どのような機関あるいは評価を行いましたか？
3-2	IDSのテストは実際の攻撃（カンファレンス発表されたものなど）を模したシナリオを使用していますか？
3-3	IDSのテストでは、共通的な攻撃パターンのデータセットなどを用いていますか？
3-4	ITシステム向けのIDSではマルウェアが行う通信をはじめ、一般的なネットワーク経由での攻撃が利用する通信をパターン化（シグネチャ）することで検知するタイプがありますが、車両の場合も同様でしょうか？
3-5	ITシステム向けのIDS、SIEMでは攻撃や検知の状況を観測しながら、運用中に各種パラメータを調整することも少なくありませんが、車載IDSの場合は、どのような情報を用いてパラメータ調整を行いますか？
3-6	IDS開発およびOEMに提供する際の課題（.dbcファイルやキャリブレーション・トレーニングに必要な情報が提供されないケースがある等）はありますか？ また、この課題に対して国や地域毎の違いはありますか？

図 3-14　IDS の評価方法

3.2.4. 調査結果（計画時の long list）

主に公開情報ベースで調査を行った、計画時の調査対象リストは以下の通りである。下記のうち、１１社については、ヒアリング及び実機評価への協力調整を実施した。

表 3-9　調査対象企業一覧

No	組織・会社名	地域・国	製品分類	製品名	概要
1	ARGUS CYBER SECURITY	イスラエル	IDPS	ARGUS CONNECTED ECU PROTECTION など	ネットワーク型、ホスト型の IDPS 製品を展開。 ホスト型には CFI（Control Flow Integrity）が用いられている。 検知ロジックは機械学習によるモデルデータではなく、別途サービス提供しているペンテスト結果に基づいた Deterministic なロジックを適用しているとのこと。
2	Karamba Security	イスラエル	IDPS	Carwall など	多くの CFI 製品が関数呼び出しの正当性のみチェックしている中、関数呼び出しだけでなく関数の復帰（リターンアドレス）の正当性もチェックすることができ、これによりインメモリ攻撃から防御する。 上述の通り、あらかじめ組み込まれた制御フローの完全性検証によって実現されていることから、Deterministic なロジックによるホスト型 IDS であるといえる。 別サービスである Threat Hive は AUTO ISAC での採用実績あり。

No	組織・会社名	地域・国	製品分類	製品名	概要
3	AuroraLabs	イスラエル	OTA	SELF-HEALING SOFTWARE	以下 HP より。(HP閲覧日:2020.3.1) コネクテッドカー向けの自己修復ソフトウェアとのこと。 大きく以下の機能を謳っている。 ・検知：ソフトウェアの動作の障害を検出しダウンタイムイベントを予測 ・修正：シームレスなユーザーエクスペリエンスのためのセーフティネットを提供 ・更新：ゼロダウンタイムでクライアントレスのホットアップデート ・検証：ランタイムソフトウェアの変更のエビデンス 上記以外の具体的な技術情報は公開情報より確認できていない。技術領域としては OTA プラットフォームを提供していると考えられる。 https://www.auroralabs.com/
4	Arilou Technologies	イスラエル	IDPS	In-Vehicle Intrusion Detection and Prevention System など	今回実機評価にご協力頂いたベンダー。ネットワーク型、ホスト型の IDPS 製品を展開（実機評価ではネットワーク型の評価ボックスを使用） 以下 HP より。(HP閲覧日:2020.3.1) IDPS は高度なソフトウェア（SW）ソリューションで、コントロールエリアネットワーク（CAN）バスを監視し、電子制御ユニット（ECU）の通信パターンの異常を検出します。100%の検出率、ゼロ誤検知、ゼロ遅延を備えた、市場で唯一の実績のあるソリューション。 PIPS は、ハイジャックされた ECU から発信される悪意のある通信を積極的に傍受することにより、車両ネットワーク全体を単一のポイントから保護します。 https://ariloutech.com/
5	SafeRide Technologies	イスラエル	IDPS	vSentry	2018 年より AGL のメンバー企業であり、CES 2020 の AGL ブースにて出展したとのこと。 上記より、主に IVI などの情報系 ECU を対象とした IDPS 製品であると考えられる。 ファイアーウォールや、アクセス制御などによる保護機能のほか、ディープラーニングを用いたアノマリ検知技術も組み合わせているとこのこと。

No	組織・会社名	地域・国	製品分類	製品名	概要
6	GuardKnox	イスラエル	IDPS	Communication Lockdown	以下 HP より。(HP閲覧日:2020.3.1) 車両のサイバーセキュリティに対する当社のアプローチは、すべての内部ネットワーク通信をロックダウンする集中化されたソリューションを提供することです。また、単一の ECU を保護するローカルソリューションも含まれています。単一の ECU 保護は、外部接続のある ECU に接続する単純な「プラグイン」デバイスによって提供されます。これにより、すべての外部ネットワーク通信が「ロックダウン」されます。このような実装により、統合、複雑さの軽減、認証の簡素化、全体的なコスト削減が実現します。 GuardKnox テクノロジーとソフトウェアスタックは、さまざまなハードウェアアーキテクチャに実装できるため、既存の自動車用コンピューターへの統合プロセスが容易になります。 https://www.guardknox.com/
7	ST マイクロエレクトロニクス	スイス	HSM	Telemaco3P	ARM Cortex-A7 デュアルコアプロセッサを搭載したマイコン。 HSM や独立した ARM Cortex-M3 サブシステムが搭載されており、主に通信系 ECU 用途を対象としている。 また、試作開発用のオープン開発環境として、Modular Telematics Platform(MTP)を発表、販売している。
8	ESCRYPT(via ETAS K.K.)	ドイツ	IDPS	CycurIDS など	ネットワーク対応車両のための埋め込み型攻撃検知と持続的な保護。 以下、HP より。(HP閲覧日:2020.3.1) CycurIDS は埋め込み型のセキュリティコンポーネントとして、周期的なメッセージや診断リクエストの乱用などを典型的な「シグネチャ型」と「アノマリ型」で検知します。 CycurIDS のキャリブレーションは、車両の CAN ネットワーク用のメーカー独自の設定データ（DBC/ARXML）をもとに行われます。この設定は、記録されたネットワークトラフィックに基づいたシミュレーション、そして検知率とエラー検出率の自動解析を通じて検証・最適化されます。これにより、高い検知率と低いエラーアラーム発生率を実現しています。 https://www.escrypt.com/ja
9	Infenion Technologies	ドイツ	HSM	AURIX	HSM に対応した 32 ビットマイコンで、ハードウェアアクセラレータによる AES-128 暗号化や SHE と SW による非対称暗号にも対応。 HSM セキュリティレベルは EVITA Medium

No	組織・会社名	地域・国	製品分類	製品名	概要
10	APTJ	日本	AUTOSAR	Julinar	AUTOSAR CP Release Number/Revision：R4.2.2 ※一部モジュールは R4.3.x に準拠 → Security モジュール（Csm/SecOC/CryIf/Crypto）が該当 **AOBA(JARI)のECUに採用されている。**
11	AUBASS	日本	AUTOSAR	AUBIST など	AUBIST Sec として認証、リプロ、AES ライブラリなどの複数パッケージが提供される。 またセキュリティ関連技術として、仮想化やコンテナ技術への対応ソリューションも提供予定となっている。
12	Panasonic	日本	IDPS	N/A	以下 HP より **(HP閲覧日:2020.3.1)** 本開発システムは以下の特長を有しています。 1. 攻撃の初期段階であるインターネットからの侵入、さらに第二段階である車載ネットワークへの侵入を検知できます。 2. 車載ネットワークとして、広く普及している CAN※1 に加えて、今後の普及が見込まれる Ethernet※2 にも対応しており、車両全体の侵入を網羅的に検知することが可能です。 3. 複数の車載機からの情報をクラウドに集約することで、攻撃がセキュリティの脅威として顕在化する前に検知が可能です。 https://news.panasonic.com/jp/press/data/2017/10/jn171010-2/jn171010-2.html
13	住友電工	日本	IDPS	N/A	セントラルゲートウェイに搭載されることを想定している（CAN、CAN-FD に対応、Ethernet は開発中）。 検知対象は、予期しないメッセージ・動作の検知のほか、不正な機器の物理接続の検知、プロトコルとしての異常の検知となる。 基本的には、メーカーの要件に基づいて開発が行われるため、製品単体としての提供や販売は行われない。 不正機器の接続検知については、SCIS2020 において、関連技術に関する論文（CAN 信号を用いたフレーム攻撃前の接続検知）が発表されている。
14	富士通	日本	IDPS	N/A	CAN メッセージの受信時間などに基づいて、リアルタイムに検知を行う技術を使用（累積和検知技術）。 導入容易性を考慮し、設計情報に基づくアノマリ検知方式を採用している。

No	組織・会社名	地域・国	製品分類	製品名	概要
15	Elektrobit	フィンランド	AUTOSAR	EB zentur など	AUTOSAR 発足当初からのプレミアムメンバー。HSM ファームウェアへの統合や、暗号化ライブラリ、JASPAR エクステンションに対応する。その他、暗号鍵の管理を行う Key Management やアクティベーション管理用の Function Enabling、物理的なセキュリティとして、ECU の再利用を防ぐための Anti-Theft 機能などがラインナップとして存在する。
16	Harman International	米国	IDPS	ECUSHIELD など	CGW などの車載 NW 向けでは非常に小さなソフトウェア容量を実現しており、検知アルゴリズムには機械学習を採用している。 TCU 向けには、Wi-Fi やセルラーの通信解析を行うことで高精度な検知が行えるとのことである。
17	Dellfer	米国	IDPS	ZeroDayGuard	ZeroDayGuard は署名なしで動作し、安全で安全な動作を保証します。 正しい動作を逸脱する試みが行われると、Dellfer は悪意のあるアクションを防ぎます。 上記より、ARGUS や Karamba 同様に CFI あるいは類似したソフトウェアのビヘイビアをモニタリング、検知する技術と考えられる。
18	Synopsys	米国	HSM	Designware tRoot	事前に構築された定義済みのセキュリティを提供する Vx HSM のほか、要件に併せてコンフィグレーション可能な Fx HSM、iSIM 用の HSM などがラインナップとして存在する。
19	Trillium	米国	IDPS	vSEC	以下 HP より **(HP閲覧日:2020.3.1)** Trillium の業界をリードする認証暗号化機能により、すべての安全な IVN ノードとミッションクリティカルな IVN ノード間で有効かつ機密の IVN メッセージを保証します。 リソースに制約のある IVN よりも最適なパフォーマンスを発揮するように設計されており、すべての車両ハードウェア、オペレーティングシステム、ネットワークトポロジで動作します。 独自の特許取得済みのアプローチを使用して、基本的なデータの信頼性と車両のセキュリティを、ルールなしで確定的な機能とともに提供します。 これは、偽陽性や偽陰性の心配のないフェイルセーフ IDPS ソリューションに変換されます。 https://trilliumsecure.com/

No	組織・会社名	地域・国	製品分類	製品名	概要
20	WindRiver	米国	OTA	Wind River Edge Sync	自動車専用の OTA プラットフォームを提供。モジュール形式の OTA アーキテクチャにより、コンポーネント個別に、あるいは E2E ソリューションとして一括して実装することができる。 アップデートプロセスを通して完全性、気密性、真正性を確保している。また、差分アップデート用の差分ツールや OS やハードウェアに依存しない移植性の高い車載クライアントがコア機能の一部として提供される。
21	Mentor Graphics	米国	IDPS	なし（SOW ベースのため）	公式 HP では非公開だが、SOC 上の組み込み Linux 向けの HIDS を顧客の要求するセキュリティポリシーに合わせてサービスベース（SOW、Statement of Work）で開発、提供している。当該 IDS は前述の通りプロジェクト単位で提供されることから、実現方式や検知方式には多様性がある（オフ・ザ・シェルフではなく、顧客の要求ベースのため、事実上固有の機能が存在しているわけではない）。 なお展示会（CES 2019）での展示品はアクセス制御ログに基づくルールベースの検知方式を採用していたとのことである。

3.2.5. IDS の調査

調査対象企業のうち、下記サプライヤー及び IDS ベンダーをヒアリング調査対象とした。そのうち、インタビュー調査にご協力頂いたサプライヤー、ベンダーは以下の通り（順不同）。なお、下記以外の海外ベンダー３社については期限内に回答を得られなかった、または公開情報のみで調査を行ったベンダーとなる。

- パナソニック株式会社（オートモーティブ社）
- 住友電工株式会社
- 富士通株式会社
- ESCRYPT GmbH（イータス株式会社）
- Karamba Security Ltd.（株式会社アズジェント）
- Arilou Technologies Ltd.（NNG Navigations 株式会社）
- Mentor Graphics Japan Co.,Ltd.
- Harman International Industries, Inc

3.2.5.1. 調査結果まとめ

調査の結果、現在の車載向け IDS は大きく分けて、「実装方法」、「検知対象」、「検知方式」の３つの観点で分類することができる。

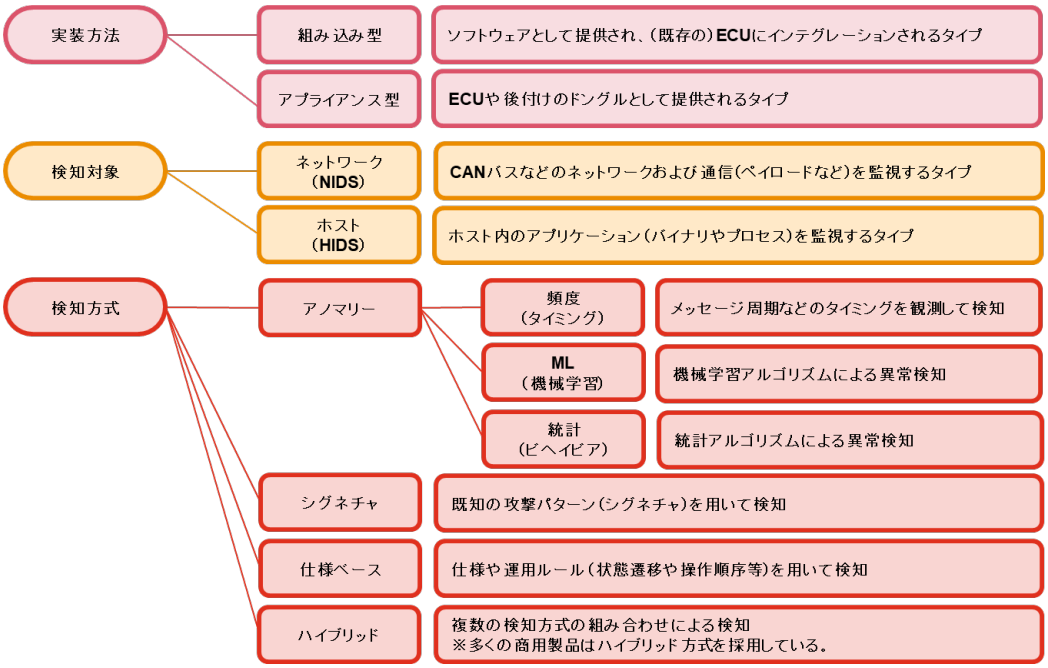

図 3-15　車載 IDS 製品技術分類

上記分類のうち、検知方式を基に各製品を分類した場合、以下のようになる。

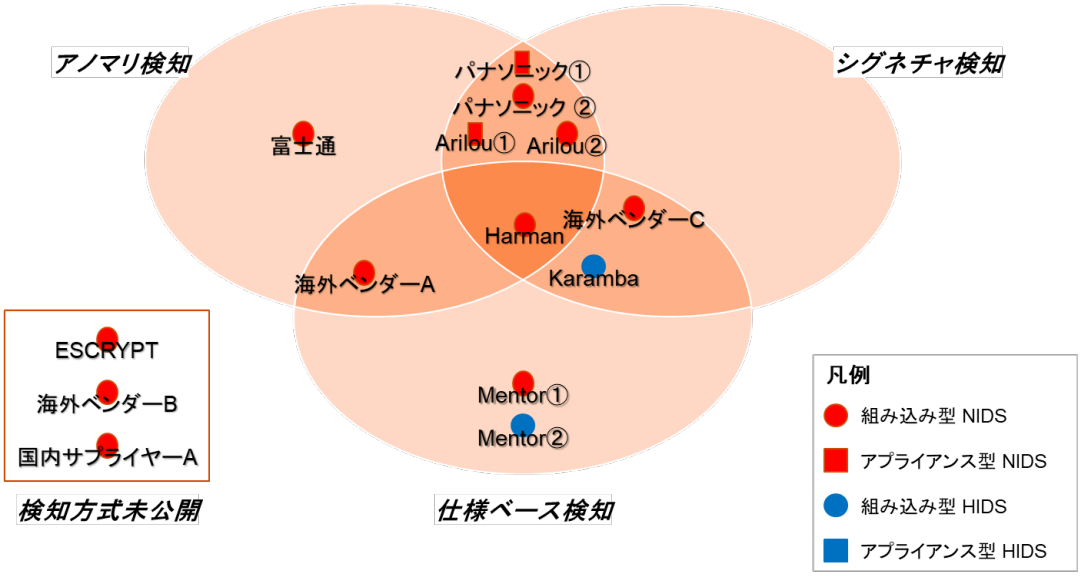

図 3-16　検知方式マップ

3.2.5.2.　調査結果詳細

表 3-10　調査を行った IDS ベンダー一覧

No.	ベンダー名	製品名	国
1	Arilou	IN-VEHICLE INTRUSION DETECTION AND PREVENTION SYSTEM(IDPS)	イスラエル

No.	ベンダー名	製品名	国
2	Escrypt	Cycur IDS	ドイツ
3	Harman International	HARMAN CAN IDS (HARMAN SHIELD Solution)	米国
4	Karamba Security	XGuard Carwall (Karamba XGuard)	イスラエル
5	Mentor Graphics Japan	N/A	米国
6	パナソニック	N/A	日本
7	住友電工	N/A	日本
8	富士通	N/A	日本
9	海外ベンダーA	N/A	イスラエル
10	海外ベンダーB	N/A	イスラエル
11	海外ベンダーC	N/A	米国

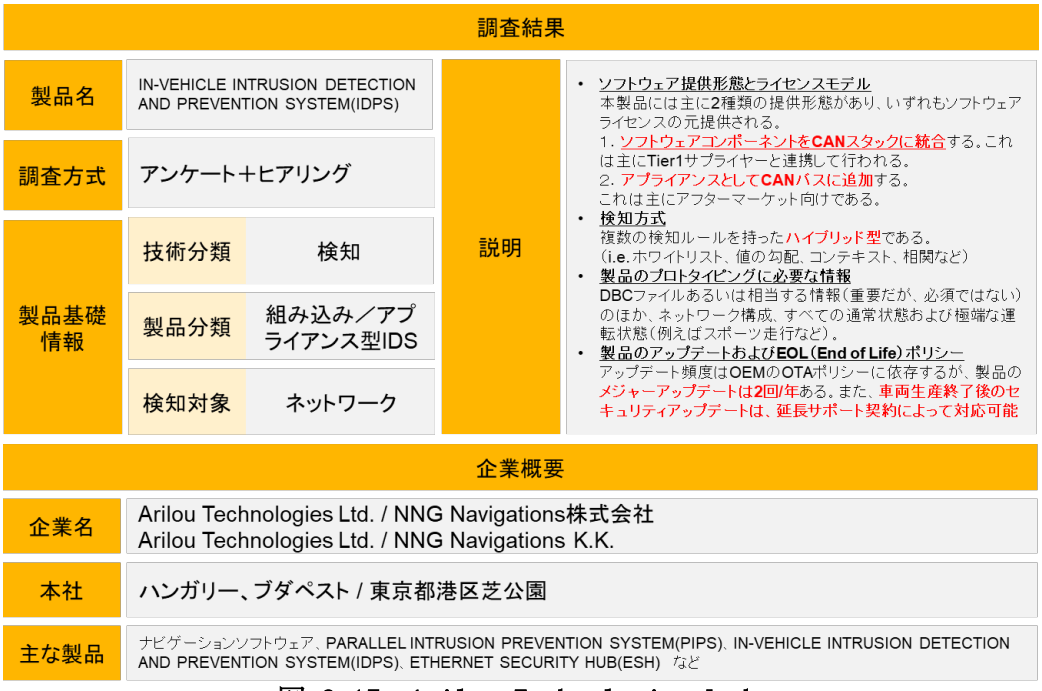

図 3-17 Arilou Technologies Ltd.

図 3-18　ESCRYPT GmbH

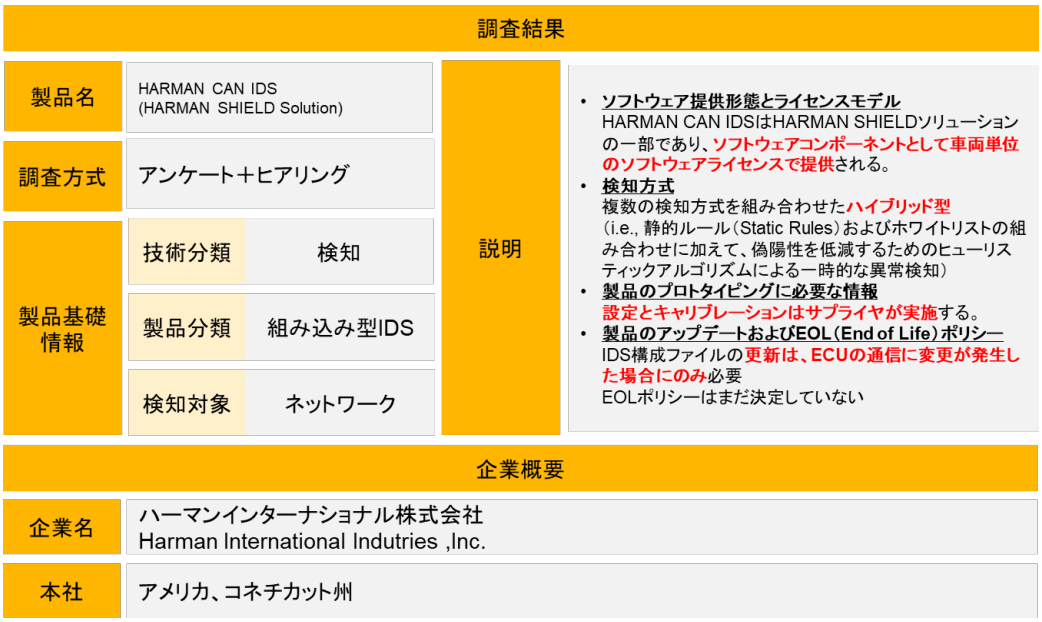

図 3-19　Harman International Industries, Inc.

調査結果			
製品名	XGuard Carwall (Karamba XGuard)	説明	• ソフトウェア提供形態とライセンスモデル 開発プロジェクト毎のロイヤリティ方式で開発環境の一部として提供される 上記提供方式により他の製品とは異なり、本製品はビルド時にECUのソフトウェアに組み込まれる • 検知方式 複数の検知方式を組み合わせたハイブリッド型 (i.e., ホワイトリスト、メモリ操作、システムの完全性、ルール等) • 製品のプロトタイピングに必要な情報 特になし • 製品のアップデートおよびEOL(End of Life)ポリシー ECUのEOLポリシーに準拠
調査方式	アンケート＋ヒアリング		
製品基礎情報	技術分類: 検知		
	製品分類: 組み込み型IDS		
	備考: ホスト		
企業概要			
企業名	カランバセキュリティ Karamba Security Ltd.		
本社	イスラエル、ホッドハシャロン		
主な製品	Karamba Carwll(Karamba XGuard)、Karamba VCode など		

図 3-20 Karamba Security Ltd.

調査結果			
製品名	N/A	説明	メンター・グラフィックス・ジャパンでは、同社が提供するSOC上の組み込みLinux向けのIDSを顧客の要求するセキュリティポリシーに基づき、サービス(プロジェクト)毎に開発、提供している。 顧客、プロジェクト毎に開発、提供されることから、実現方式や検知方式は、通常のオフ・ザ・シェルフ製品とは異なり、多様性がある(顧客要求・実装方式によってはネットワークを監視、検知するNIDSにも、ホスト内のアクティビティを監視、検知するHIDSのどちらにもなり得る)。 同社がCES 2019で展示したデモでは、アクセス制御ログなどをデータベースと照合し、あらかじめ定義されたセキュリティポリシーに違反するアクティビティを検知する方式を採用していたとのことである。
調査方式	アンケート＋ヒアリング		
製品基礎情報	技術分類: 検知		
	製品分類: 組み込み型IDS		
	検知対象: クライアント要求による		
企業概要			
企業名	メンター・グラフィックス・ジャパン株式会社 Mentor Graphics Japan Co.,Ltd.		
本社	東京都品川区北品川		
主な製品	ESL設計製品(Vista)、AUTOSAR製品(Volcano Family)、Mentor Embedded Linux,、Nucleus、XSe Automotive、etc		

図 3-21 Mentor Graphics Japan Co., Ltd.

調査結果			
製品名	N/A	説明	• ソフトウェア提供形態とライセンスモデル ソフトウェアモジュールによるゲートウェイやセントラルECUに実装を想定。ハードウェア（セキュリティECU）としても実装、提供可能。ライセンスは提供形態による。 • 検知方式 複数の検知方式の組み合わせによるハイブリッド方式。 複数のコンテキストを組み合わせた攻撃を検知する機能が特徴 • 製品のプロトタイピングに必要な情報 DBCファイルおよびCANサンプルデータの他、ADASなどの制御仕様があれば、仕様に基づくルール作成により、より高度な攻撃検知対応ができる • 製品のアップデートおよびEOL（End of Life）ポリシー アルゴリズムとルール更新を定期的に更新する。 • その他 SIEMと一体開発加えて、自社SOCでの運用実績があるため、検知以降の対応も可能な体制がある 共通部分と車両固有部分が分離されているため、短期間で適用できる。
調査方式	アンケート＋ヒアリング		
製品基礎情報	技術分類：検知		
	製品分類：組み込み／アプライアンス型IDS		
	検知対象：ネットワーク		

企業概要	
企業名	パナソニック株式会社 オートモーティブ社
本社	横浜市都筑区池辺町
主な製品	カーナビゲーション、次世代コックピット、ECU、車載充電システムなど

図 3-22　パナソニック株式会社　オートモーティブ社

調査結果			
製品名	N/A	説明	• ソフトウェア提供形態とライセンスモデル Tier1サプライヤーとして、メーカーの要求に基づいて開発を行っており、固有のIDS製品は存在しない。 • 検知方式 非公開 • 製品のプロトタイピングに必要な情報 非公開 • 製品のアップデートおよびEOL（End of Life）ポリシー メーカーの要求に基づく。 • その他 SCIS2020にて、検知技術に関する発表あり。 「CAN信号を用いたフレーム攻撃前の接続検知」
調査方式	アンケート＋ヒアリング		
製品基礎情報	技術分類：検知		
	製品分類：組み込みIDS		
	検知対象：ネットワーク		

企業概要	
企業名	住友電工株式会社
本社	大阪市中央区北浜
主な製品	自動車用ワイヤーハーネス、EV/HEV/PHEV用製品、エレクトロニクス製品など

図 3-23　住友電工株式会社

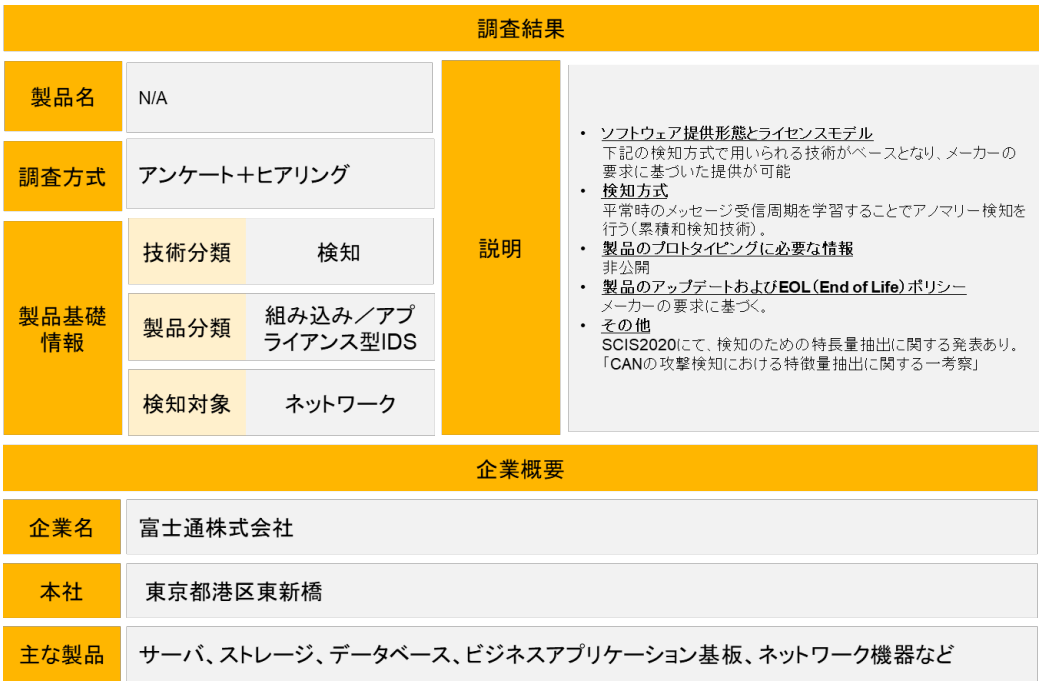

図 3-24　富士通株式会社

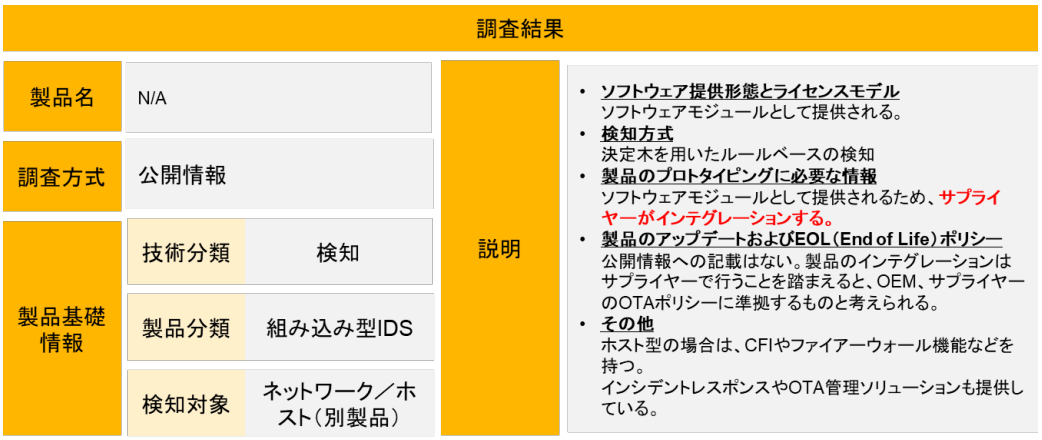

図 3-25　海外ベンダーA（イスラエル）

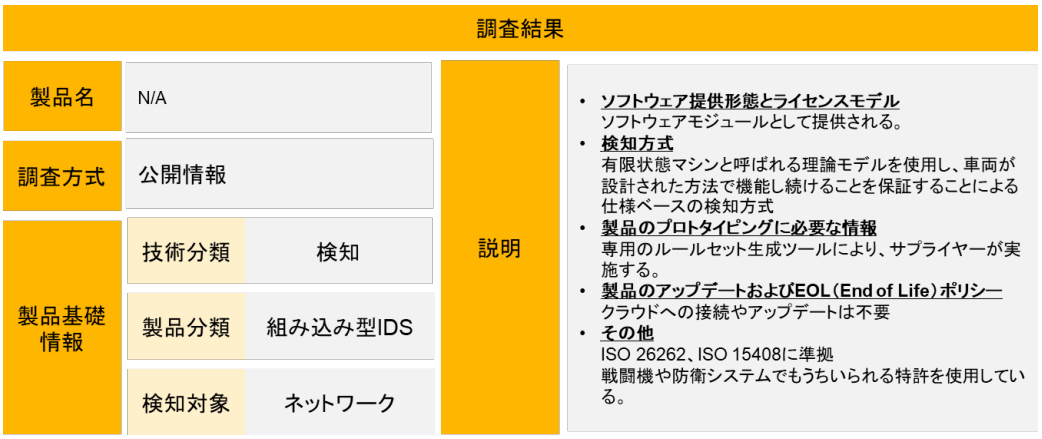

図 3-26　海外ベンダーB（イスラエル）

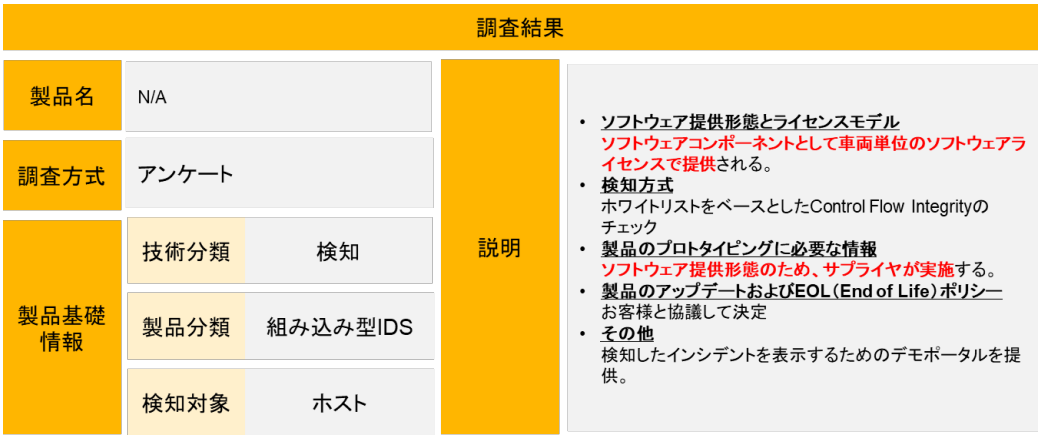

図 3-27　海外ベンダーC（米国）

3.2.6. IT 領域における IDS 製品の調査

IT 領域の IDS 製品の有識者にインタビューを実施し、IT 領域の IDS 製品の実態を調査した。この情報を基に車載向け IDS との差分把握や、評価方法へ反映を行った。

表 3-11　IT 領域の製品調査結果

項目	IT領域の製品の状況
記録項目	どの製品もほぼ同じ項目を記録している（下記参照） 記録項目 • イベントまたは警報の種類 • 評価（優先度、重大度、影響の程度、確実性など） • ネットワーク層、トランスポート層、アプリケーション層のプロトコル • 送信元および宛先 IP アドレス • 送信元および宛先の TCP または UDP ポート、あるいは ICMP タイプおよびコード • 当該接続を介して伝送されたバイト数 • 復号したペイロードデータ(アプリケーションの要求／応答など) • 状態に関する情報（認証されたユーザ名など） • 実行された防止措置（該当する場合）
記録場所	• ローカル環境またはリモート環境に保存する • 保存場所は、製品の構成（センサー＋管理サーバー／アプライアンス製品／ソフトウェア製品）に依存
ログの増加に対する対応	• 6ヵ月～永年等、事前に保存期間を決め、古いログを削除する • ログの多くは誤検知であるため、導入後、検知状況をみてパラメーターを調整して、誤検知の量が多くなりすぎないようにする
ログ管理に関する重要なポイント	ログだけを見て誤検知かどうかを判断できない場合があるため、サーバーのログや、通信のペイロード等、他のデータも参照して判断する場合がある

3.3. IDS 評価方法の検討と基礎評価による検証

将来起こり得る攻撃（既知・未知）という観点において、検知には大きく２つの目的があると仮定した。本活動では、この目的を達成するための技術の１つとして IDS の評価方法の検討と検証を行った。

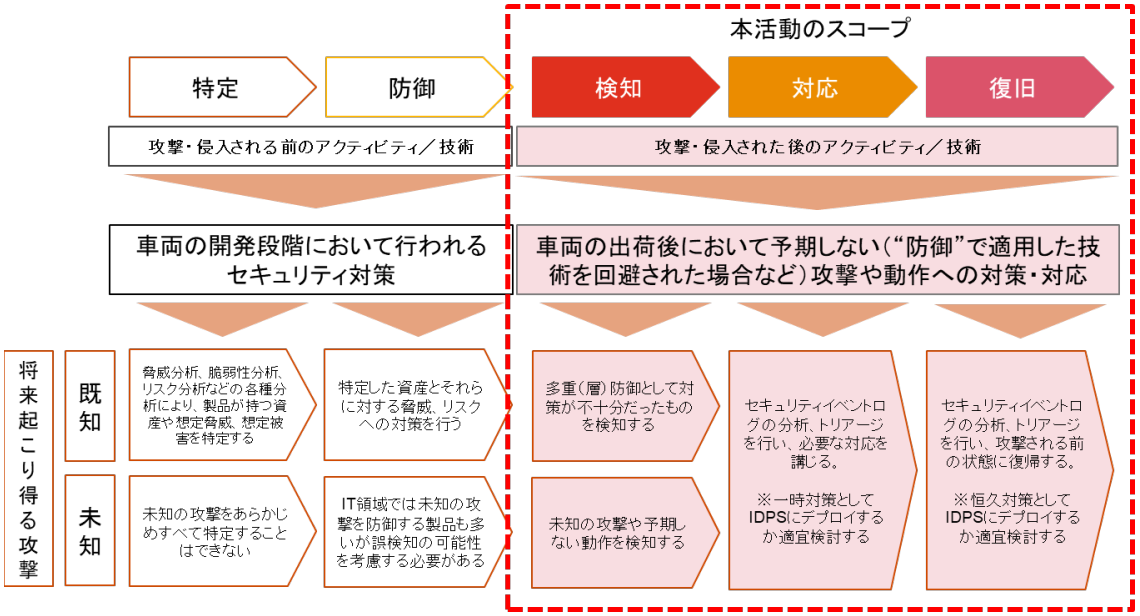

図 3-28　IDS 評価の目的／スコープ

3.3.1. 評価観点の検討

防御技術の調査結果や、各種文書（NIST SP800-94、WP.29、NHTSA DOT HS 812 708 など）を基に「基本仕様」、「導入（PoC を含む）」、「運用」、「検知性能」の４つの観点を定義した。IDS の主たる機能である、「検知性能」においては、さらに５つの観点に細分化した。

これらの観点に基づいて、ヒアリングによる机上ベースでの評価と IDS ベンダー1 社の協力によるテストベッドを用いた実機での検知性能評価を行った。なお、前提として各観点は、ベンダー側が想定する脅威やメーカー側が IDS に求める要件が、車載システムや ECU 毎に異なることから、必ずしもすべてを満たす必要はなく、また、各観点における判断基準はメーカー毎に決定すべき要素である。

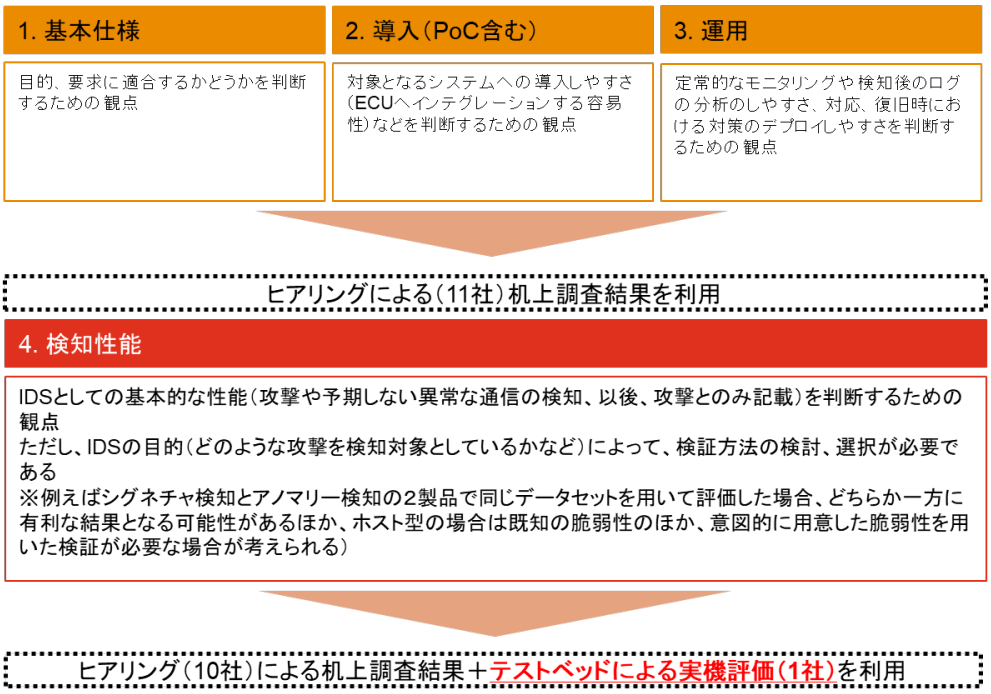

図 3-29　評価観点の検討結果（全体）

評価観点		評価内容
1.基本	目的、要求に適合するかどうかを判断するための観点	1-1. IDSの種別
		1-2. テストベッド上のCANネットワークの異常を検知可否
		1-3. ECUへの組み込み、アプライアンスの選択可否
		1-4. ライセンス（ロイヤリティ発生）形態
2.導入	対象となるシステムへの導入しやすさ（ECUへインテグレーションする容易性）などを判断するための観点	2-1. DBCファイルの要否
		2-2. ドライビングデータの要否
		2-3. 今回のPJ工数（IDS受領までの期間）
3.運用	定常的なモニタリングや検知後のログの分析のしやすさ、対応、復旧時における対策のデプロイしやすさを判断するための観点	3-1. 検知イベントの分類可否
		3-2. ログ分析支援ツール（あるいはサービス）の有無
		3-3. ソフトウェアアップデート有無
		3-4. OEM/サプライヤーによるコンフィグレーション調整の可否

図 3-30　評価観点の検討結果（基本仕様、導入、運用）

4. 検知性能	
4-1. 定常状態で検知しない	想定する攻撃例：なし／通常の操作で検知してはいけない。
4-2. 予期しないメッセージ／動作の検知	想定する攻撃例：メッセージインジェクション攻撃等
4-3. 不正な機器の物理的な接続の検知	想定する攻撃例：不正なOBDドングルの接続やクリッピング等
4-4. マルウェアの活動の検知	想定する攻撃例：MiraiやWannaCryのようなネットワーク感染型のマルウェアの活動やマルウェアによる脆弱性攻撃、（C2サーバなどへの）外部通信等
4-5. プロトコルとしての異常の検知	想定する攻撃例：OBDやUDS、あるいは独自のプロトコル仕様外のメッセージや異常なフレーム（CRCエラー等）のインジェクション等

図 3-31　評価観点の検討結果（検知性能）

3.3.2. 机上による評価結果

机上による評価は、ヒアリング結果（回答ありの場合）および公開情報に基づいて行った。なお、各製品の優劣を評価するものではなく、要件に合うかの参考指標のため、数値化ではなく項目に対する要否（可否）や有無で表現している。

表 3-12　机上評価結果（1）

評価観点	評価内容	Arilou	Karamba	ESCRYPT	Mentor	Harman
1. 基本	1-1. IDS 種別	NIDS	HIDS	NIDS	SOW 依存	NIDS
	1-2. テストベッド上の CAN ネットワークの異常を検知可否	可	不可	可	SOW 依存	可
	1-3. ECU への組み込み、アプライアンスの選択可否（PoC／デモを	選択可	組込のみ	組込のみ	組込のみ	組込のみ

	除く）					
	1-4. ライセンス（ロイヤリティ発生）形態	ソフトウェア（PJ 毎）	ソフトウェア（PJ 毎）	ソフトウェア（ボリューム）	ソフトウェア（PJ 毎）	ソフトウェア（車両モデル）
2. 導入	2-1. DBC ファイルの要否	必須ではない	不要	必須ではない	要件依存	必須ではない
	2-2. ドライビングデータの要否	要	不要	要	要件依存	要
	2-3. 今回の PJ 工数（IDS 受領までの期間）	2 週間	-	-	-	-
3. 運用	3-1. 検知イベントの分類可否	可	可	可	要件依存	可
	3-2. ログ分析支援ツール（あるいはサービス）の有無	有	有	有	要件依存	有
	3-3. ソフトウェアアップデート有無	有	有	有	要件依存	有
	3-4. OEM/サプライヤーによるコンフィグレーション調整の可否	可	可	可	要件依存	可

表 3-13　机上評価結果（２）

評価観点	評価内容	海外ベンダーA	海外ベンダーB	海外ベンダーC	パナソニック	住友電工	富士通
1. 基本	1-1. IDS 種別	NIDS/HIDS	NIDS	HIDS	NIDS	NIDS	NIDS
	1-2. テストベッド上の CAN ネットワークの異常を検知可否	可	可	可	可	可	可
	1-3. ECU への組み込み、アプライアンスの選択可否（PoC／デモを除く）	組込のみ	組込のみ	組込のみ	選択可	組込のみ	選択可
	1-4. ライセンス（ロイヤリティ発生）形態	不明	不明	ソフトウェア（PJ 毎）	要件による	不明	要件依存
2. 導入	2-1. DBC ファイルの要否	不明	不明	不要	要	不明	不明
	2-2. ドライビングデータの要否	不明	要	不要	要	不明	不明
	2-3. 今回の PJ 工数（IDS 受領までの期間）	-	-	-	-	-	-
3. 運用	3-1. 検知イベントの分類可否	可	可	可	可	要件依存	可
	3-2. ログ分析支援ツール（あるいはサービス）の有無	有	有	有	有	要件依存	不明
	3-3. ソフトウェアアップデート有無	有	有	有	有	要件依存	不明
	3-4. OEM/サプライヤーによるコンフィ	可	可	可	可	要件依存	可

評価観点	評価内容	海外ベンダーA	海外ベンダーB	海外ベンダーC	パナソニック	住友電工	富士通
	グレーション調整の可否						

3.3.3. 実機による評価結果

実機による評価は、Arilou Technologies 社（以下、Arilou と記載）に協力頂くことで行った。同社の紹介については、3.2 節を参照。

3.3.3.1. テストベッドの選定

実機による評価にはテストベッドを利用した。今回、テストベッドとして、以下の通り PASTA および AOBA を利用することを検討した。結果、今回は機器の接続、各種操作の容易性やベンダーへの貸し出しなど際に持ち運びがしやすい PASTA を利用することで決定した。

	PASTA （トヨタ自動車開発）	AOBA （JARI）
ライセンス状況	オープン（MIT、GitHubで公開）	2019年10月現在未公開
販売形態	一般販売	N/A（研究目的での借用のみ）
プロトコル	CAN	CAN-FD Ethernet CAN（HILSに接続するためのインターフェイスとして）
ポータビリティ	持ち運び可能 （小型[3辺計97.5㎝]・軽量[8kg]）	持ち運びには注意が必要 （組み立て状態での移動不可）
機能・その他	➢ シミュレータとの接続が可能 ➢ テストベッドBに比べると、シンプルな構成であり、高度な検証を行うためにはある程度の工数をかける必要がある。 ➢ 各ECUのソースコードはGitHubに公開されていることからカスタマイズしやすい印象を受ける。	➢ シミュレータとの接続が可能 ➢ テストベッドAと比較して基本構成としての複雑性が高く、より高度な検証が行える印象を受ける（i.e. 標準構成としてOTAサーバーを備えており、メッセージ認証が実装されているなど） ➢ 各ECUの基本ソフトウェアとしてAUTOSAR（商用）を使用している。

図 3-32　テストベッドの検討・選定

3.3.3.2. ベンダーとの調整

ベンダーとの調整は以下の計画に基づいて実施した。

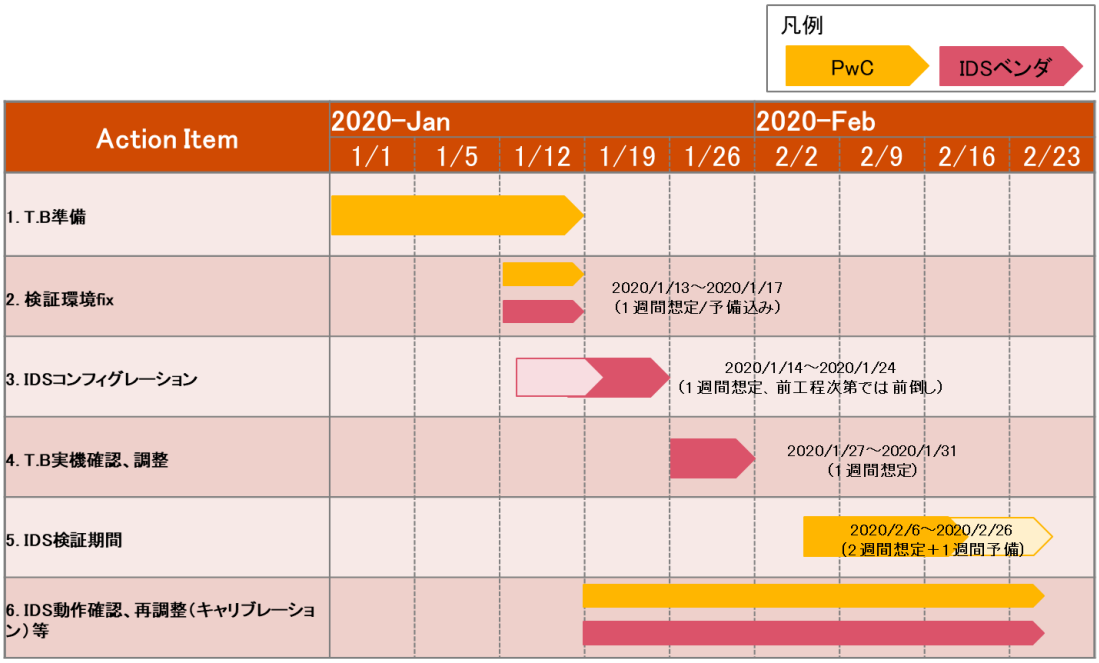

図 3-33 基礎評価計画

3.3.3.3. 検証構成

PASTA は CGW、Powertrain、Body、Chassis の計４つの ECU と、それらの動作状態を示すシミュレーターで構成される、各制御系 ECU は物理的には個別のバスに接続されているが、CGW は、デフォルト状態ではすべてのメッセージを各バスに転送する全転送モードで動作しているため、見かけ上は１つのバスで通信しているように見える。

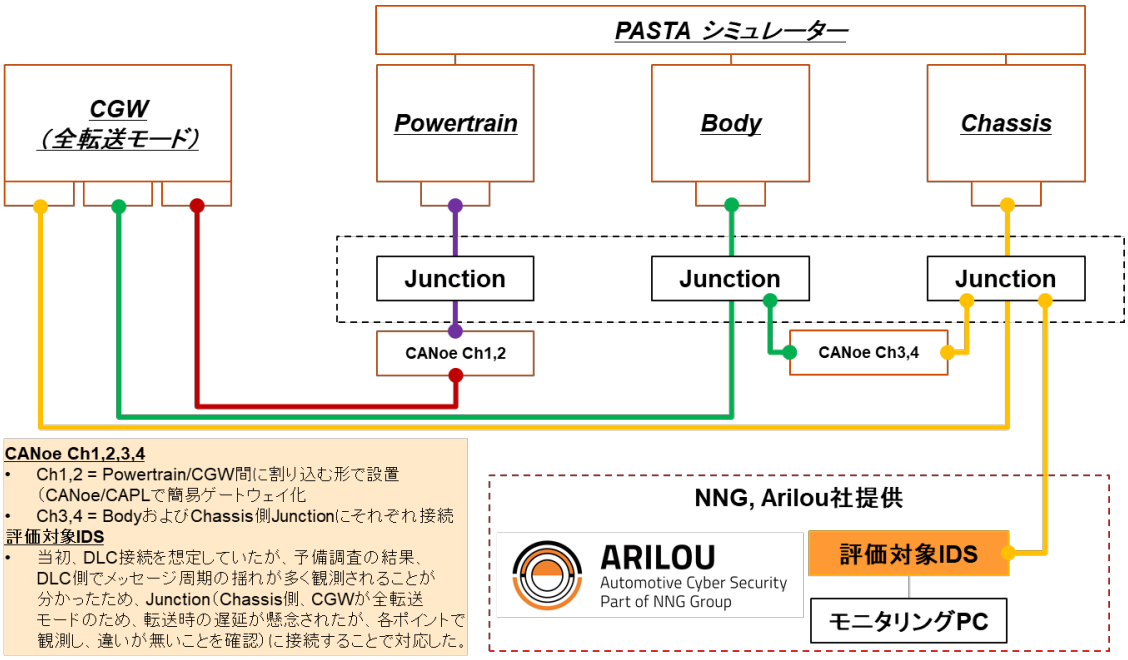

図 3-34　実機評価構成（PASTA+Arilou IDS）

3.3.3.4.　　使用した機材

本検証において、PASTA 以外に使用した機材は以下の通り。

- Arilou 提供の評価用 IDS およびモニタリングツール
- VN1630A+CANPiggy（Vector）
- CANoe Professional SP12.0

図 3-35　Arilou 提供の評価用 IDS

図 3-36　VN1630A + CANPiggy (CANoe で制御)

図 3-37 PASTA に機器を接続、動作させているところ

3.3.3.5. 実機での評価方法概要

各評価観点に対応する検証方法を定義、それぞれ CANoe/CAPL で用意した。

表 3-14 評価方法概要

ID	評価観点	検証方法	期待する結果	概要
4-1	定常状態で検知しない	通常環境の再現	検知しない	IG-ON 状態で通常の操作を行う。モニタリングのみで攻撃はしない。
4-2	予期しないメッセージ／動作の検知	メッセージインジェクション攻撃	検知する	仕様上存在する、あるいはしないメッセージを異なる ECU から入力する。
		メッセージ置き換え攻撃	検知する	MITM ECU を設置し、ECU 間のメッセージの置き換えを行う。
		メッセージ中継停止攻撃	検知する	MITM ECU を設置し、ECU 間のメッセージの中継を停止する。 なお、止まったメッセージすべてを検知する必要はない。
4-3	不正な機器の物理的な接続の検知	MITM ECU の設置	検知する	MITM ECU を設置する。
4-4	マルウェア活動の検知	メッセージベースの脆弱性攻撃	検知する	想定脆弱性を定義し、その脆弱性を突くメッセージを入力する。
4-5	プロトコルとしての異常の検知			
		エラーフレームの入力	検知しない	エラーフレームを入力する。

なおメッセージ中継停止攻撃については、止められたメッセージすべてを検出する必要はなく、製品の動作仕様に基づいて、メッセージが止められていることが検知できれば良いものとした。エラーフレームについては、CAN プロトコルとして検知することができ、コントローラーなどに実装されていることが通常であることから、期待する結果は「検知しない」こととした。

3.3.3.6. 実機での評価項目

今回意図的に IDS ベンダーに仕様として依頼した、脆弱性攻撃部分については、診断メッセージが対象となっている。そのため、追加で IG-ON 中における UDS による ECU リセットコマンド送信の検証も行っている。

表 3-15 評価項目一覧

観点 ID	項目	テスト内容
4-1	定常状態での計測	IG-ON 状態で 10 分間モニタリング
4-2	メッセージインジェクション（ランダムメッセージ）	0x700～0x7FF までのメッセージを 1000 件ランダム送信
	メッセージインジェクション（ID ゼロ）	0x000 のメッセージを 1000 件ランダム送信

観点 ID	項目	テスト内容
	メッセージインジェクション（ビットフリップ）	方向指示器（0x8D）のメッセージに対して1000 件送信
	メッセージインジェクション（UDS による ECU リセット／software reset）	セッションコントロール及びキー、ECU リセットコマンド（0x1）送信
	メッセージインジェクション（UDS による ECU リセット／Key off on reset）	セッションコントロール及びキー、ECU リセットコマンド（0x2）送信
	メッセージインジェクション（UDS による ECU リセット／hardware reset）	セッションコントロール及びキー、ECU リセットコマンド（0x3）送信
	中間者によるメッセージ置換	シフトポジション（0x77）のメッセージに対して 1000 件置換
	中間者によるメッセージ置換（ビットフリップ）	シフトポジション（0x77）のメッセージに対して 1000 件置換
	中間者によるメッセージ中継停止	スロットルポジション（0x39）のメッセージに対して 1000 件停止
4-3	中間者 ECU の設置	構成上、中間者 ECU が存在する場合にその存在を検知できるか確認する。
4-4	メッセージインジェクション（脆弱性攻撃）	CAN-TP マルチフレームを送信
	中間者によるメッセージベースの脆弱性攻撃（ブロードキャスト）	CAN-TP マルチフレームをブロードキャスト（0x7DF）で送信
4-5	メッセージインジェクション（エラーフレーム）	エラーフレーム（スタッフエラー）を 1000 件送信

3.3.3.7. 評価結果

各攻撃メッセージは、1000 件を入力（あるいは中継停止）し、IDS 側の検知ログとの突合を行うことで誤検知や見逃しの確認を行った。

なお、中間者 ECU の検知については、今回検証を行った IDS は本来、検知対象外だが、以下の製品は検知することが可能※であるとのことである。

※不正な ECU 接続後、メッセージを 1 件以上受信する必要がある。

- CANtication（ソフトウェア製品）
- PIPS（ハードウェア製品）

中間者によるメッセージ停止を除いて、すべての項目で１０００件の攻撃メッセージを検知できている。中間者によるメッセージ停止については、前述の通り停止したメッセージすべてを検知する必要はないと定義していたため、結果としては参考値扱いとした。なお、メッセージの周期に関する検知は、誤検知の可能性があり、それを回避するために設定変更可能な閾値が設けられている。それに基づいた場合、理想値は４００件となり、９７％が検知できていることになる。

追加仕様である想定脆弱性に対する検知は、特定の条件を満たした CAN-TP によるマルチフレームに対して検知する。また、同様に UDS による ECU リセットコマンドについても、特定の条件に対して検知し、それ以外のコマンドについては検知しないことを確認している。

エラーフレームについては、現時点においては検知しないことが正しい動作として定義しているが、要求によっては検知させることも可能であるとのことである。このように、各セキュ

リティイベントをどのような条件で検知するかは、メーカーの要求によって柔軟に対応が可能である。このことから検証項目は、今回実施した一般的な項目以外に、仕様に基づいて検知する、しないを判断するためのメーカーのセキュリティポリシーに基づく判断や、車両モデル固有の項目も必要となる。

表 3-16　評価結果一覧

観点 ID	項目名	攻撃メッセージと検知ログの突合結果	CANoe から入力した攻撃数	IDS が検知したメッセージ数	攻撃数に対する正解率
4-1	定常状態での計測	OK	0	0	0%（誤検知なし）
4-2	メッセージインジェクション（ID ゼロ）	OK	1000	1000	100%
	メッセージインジェクション（ビットフリップ）	OK	1000	1000	100%
	メッセージインジェクション（ランダムメッセージ）	OK	1000	1000	100%
	メッセージインジェクション（UDS による ECU リセット／software reset）	OK	2	2	100%
	メッセージインジェクション（UDS による ECU リセット／Key off on reset）	OK	2	2	100%
	メッセージインジェクション（UDS による ECU リセット／hardware reset）	OK	2	2	100%
	中間者によるメッセージ置換	OK	1000	1000	100%
	中間者によるメッセージ置換（ビットフリップ）	OK※1	1000	1000	100%
	中間者によるメッセージ中継停止	OK	400※2	389	97%
4-3	中間者 ECU の設置	対象外	---	---	---
4-4	メッセージインジェクション（脆弱性攻撃）	OK	1	1	100%
	中間者によるメッセージベースの脆弱性攻撃（ブロードキャスト）	OK	1	1	100%
4-5	メッセージインジェクション（エラーフレーム）	OK	1000	0	100%

※１．攻撃メッセージを受信した ECU がフィードバックしたメッセージについても検知することを確認しているが、これは受信した不正な値を返しているため仕様動作として判断。
※２．事前検証の結果、テストベッドのメッセージ送信周期バラつきによる誤検知を回避するために、サンプリングレートを 2.5 倍に広げた設定としている関係上、IDS が検知する期待値は、1000 件の入力に対して 2.5 倍の、400 件となる。

4. b. 車両情報セキュリティに関する新たな攻撃手法等への対策方法の調査

本章では、「b. 車両情報セキュリティに関する新たな攻撃手法等への対策方法の調査」に関する内容についてまとめる。本活動は、「技術標準の策定・文書化」および「更新方法の検討」の項目で構成される。なお技術標準の策定・文書化については下記の通り、JASPAR と連携して行った。

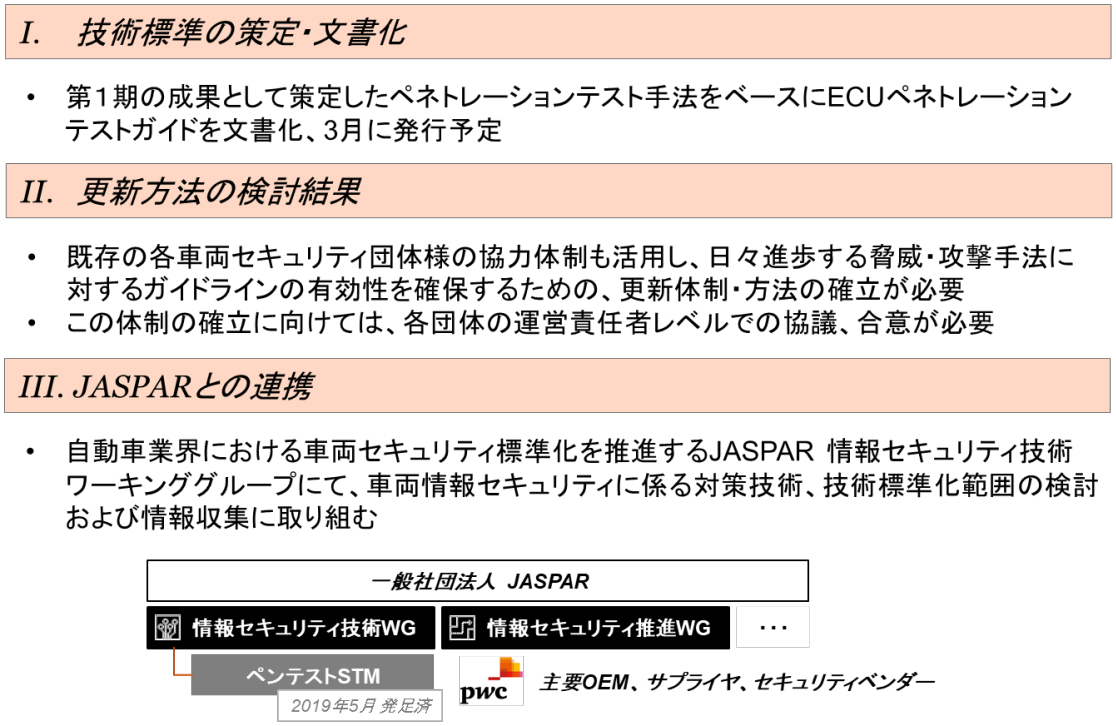

図 4-1 「b. 車両情報セキュリティに関する新たな攻撃手法等への対策方法の調査」の活動成果概要

4.1. 技術標準の策定・文書化

２０１９年５月に発足した、「情報セキュリティ技術ワーキンググループ／評価技術チーム／ペネトレーションテストサブチーム」を通じて、活動を推進した。サブチームに参加する車両メーカー、サプライヤー、セキュリティベンダー各社の意見を取り入れ、SIP 第１期ガイドラインを活用し、標準化に向けた目標要件等を２０１９年１２月に合意、文書化。３月中に ECU ペネトレーションテストガイドとして発行される予定である。

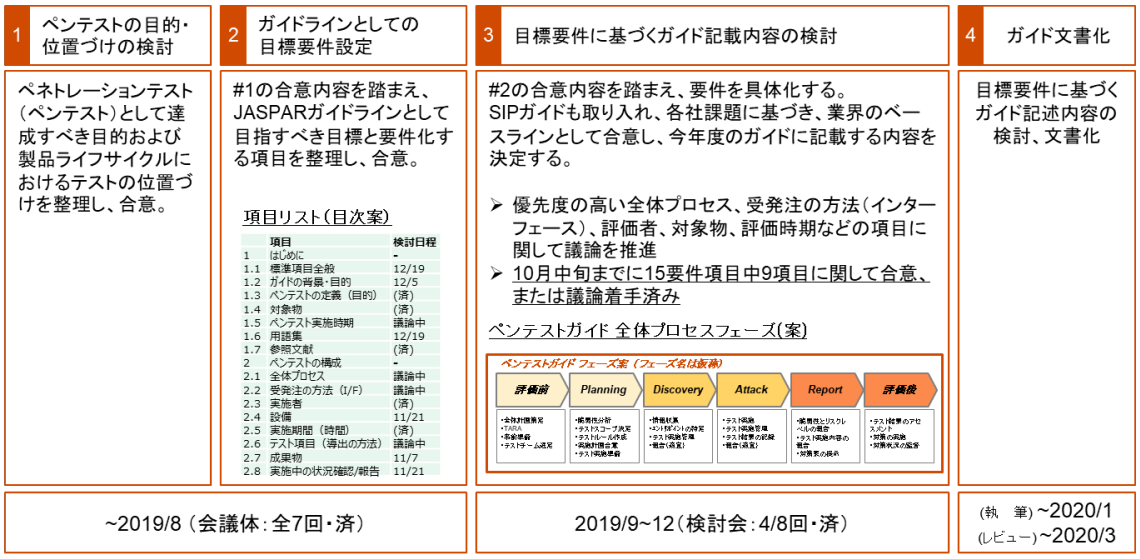

図 4-2　主な検討事項・スケジュール

4.2. 更新方法の検討

ガイドラインの更新方法に関して、ヒアリング等を実施した結果、既存の各車両セキュリティ団体の協力体制を活用し、日々進歩する脅威・攻撃手法に対してガイドラインの有効性を確保するためには、各団体の運営責任者レベルでの協議及び合意が必要であることが分かった。

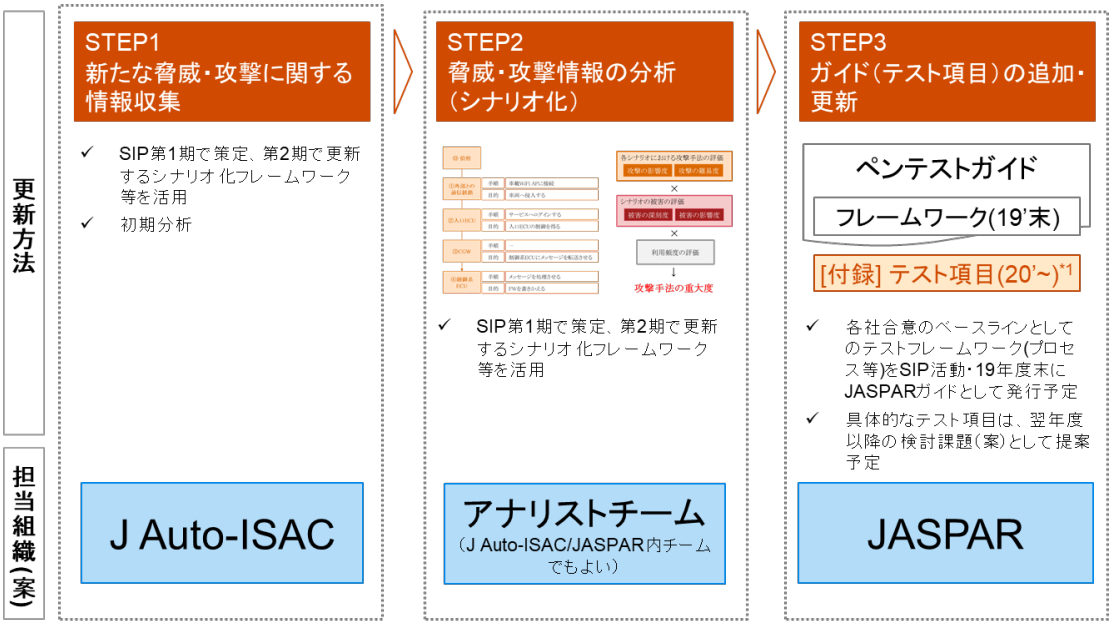

図 4-3　ガイドラインの検討体制イメージ
(*1テスト項目のガイド化については、PwC 想定)

5. 来期以降の活動テーマ案

本章では、主に「a.新たなサイバー攻撃手法および侵入検知システム（IDS）等の動向及び評価方法調査」を通して得られた活動成果に対する課題と、それを踏まえた活動テーマ案についてまとめる。

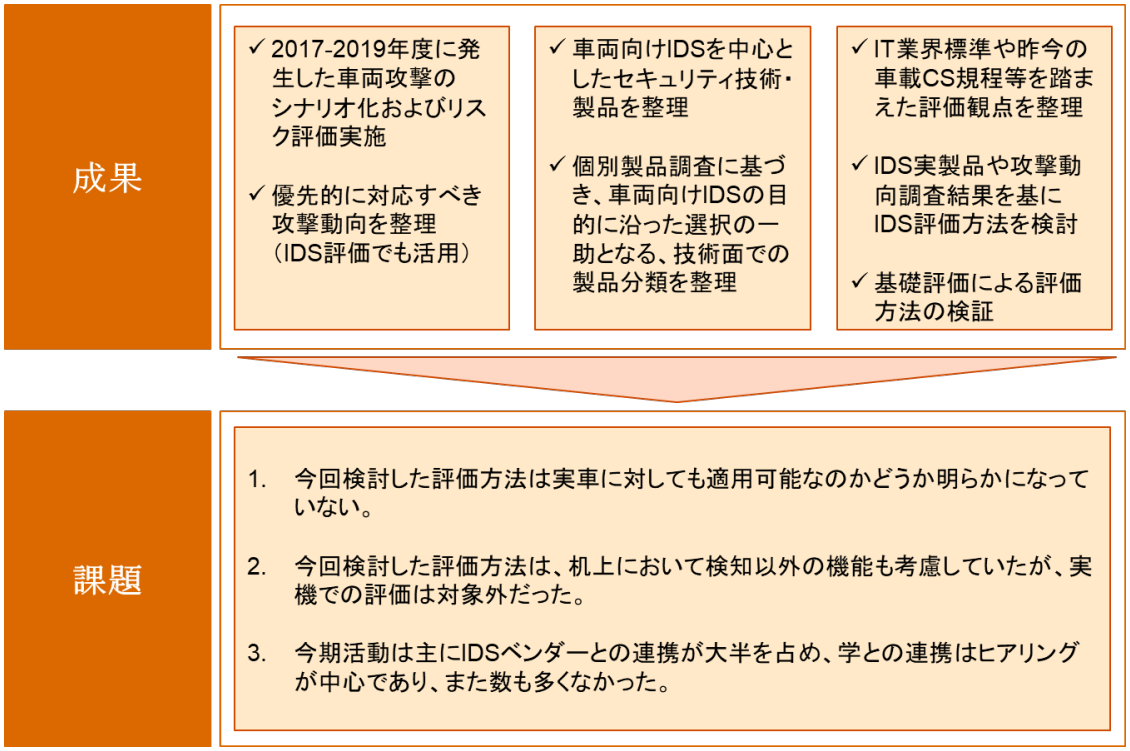

図 5-1　活動成果に対する課題

上記活動成果に対する課題を踏まえて、来期以降の活動テーマとして以下を提案する。

I.　IDS基本情報調査（FY19活動の拡張）

- FY19活動では、IDSの評価方法を検討し、IDSベンダー1社（Arilou社／イスラエル）にご協力頂き、テストベッドを用いて実験を行った。
- 来期以降は、検証環境・対象を拡張し、且つテストベッド以外に実車、実験対象IDSとして複数社に対して検証を行うことで、評価方法の妥当性の精緻化や車両向けIDS製品の有用性を確認する。

II.　IDS検知機能以外の調査

- FY19はIDSの検知機能にフォーカスして実機による実験を行った。
- 来期以降は、IDS検知機能の更新を中心に、検知機能以外（ソフトウェアアップデート機能など）に対する調査（NIST CSFにおける検知以降の対策、復旧の実装に対する各ベンダーの理解や考え方の調査と整理）と実験を行う。

III. 学連携

- FY19は横浜国立大学の松本 教授のほか、ヒアリング先として名古屋大学 倉地 特任准教授、広島市立大学 井上 准教授 にご協力頂いた。
- 引き続き、新たな攻撃手法・技術、検知技術、評価方法に関する意見交換を実施していく。

図 5-2　来期以降の活動テーマ案

6. まとめ

6.1. 本事業の成果

本年度の事業においては、「車両への攻撃動向調査」、「IDS 等のサイバーセキュリティ対策動向調査」、「IDS 評価方法の検討と基礎評価による検証」、「技術標準の策定・文書化（JASPAR との連携）」および「情報セキュリティガイドラインの更新方法の検討」を行い、活動成果としてまとめた。

「車両への攻撃動向調査」
２０１７年から２０１９年度のサイバー攻撃や脆弱性事例をまとめ、シナリオ化した。また、シナリオに対して同一基準でのリスク評価手法を策定し、評価を行った。

「IDS 等のサイバーセキュリティ対策動向調査」
IDS を中心に公開情報に基づいて調査を行い、そのうち１１社に対してはアンケートやヒアリング方式による聞き取り調査を行った。それら結果に基づき、車両向け IDS における製品分類の整理及び後述の評価方法の検討に利用した。

「IDS 評価方法の検討と基礎評価による検証」
公開文献や各社からのアンケートやヒアリング結果に基づいて、評価観点と対応する評価項目の策定を行った。基礎評価については、Arilou および NNG 協力のもと、性能評価を行った。今回の評価項目は、ネットワーク型だけではなく、ホスト型を対象とした観点（マルウェア活動の検知）も存在していたが、テスト項目として、「ネットワーク経由での脆弱性攻撃が行われた場合」を想定することでカバーした。

「技術標準の策定・文書化（JASPAR との連携）」
JASPAR 情報セキュリティワーキンググループの、ペネトレーションテストサブチーム内にて活動を推進し、ECU ペネトレーションテストガイドとして文書化を行った。本文書は、２０２０年３月に公開される予定である。

6.2. 総括

本事業では、昨今の車両に関連するサイバー攻撃事例のリスク評価のほか、対策技術として各 IDS ベンダーの特長の整理、評価観点及び対応する評価方法とテストベッドを用いた実機評価ができた。一方で、車載向け IDS 製品は、IT 領域とは異なり、車両アーキテクチャが、メーカーや車両モデル毎に異なることから個別に開発を行うスタイルであることに起因して、評価であっても一定の開発コストがかかることや、事前に検知すべき、あるいはしてはいけないイベント等について仕様を定義しておく必要があることも分かった。今回は検知における実装評価が主な活動テーマであったが、自動車のセキュリティライフサイクルを踏まえ、IDS 製品のソフトウェア更新機能などを含む、対応や復旧といった、検知後の工程を想定した評価も重要である。
また JASPAR の情報セキュリティワーキンググループ内の活動を通じて ECU ペネトレーションテストガイドの策定を行い、今後発行される予定である。この活動で策定されたガイドを用いて、自動車業界でペネトレーションテストを実施する際に、より効果的、効率的にテストが進

められるように、実際に活用され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、昨今の自動車セキュリティ開発における国際標準・標準規格に提言するなどで、日本企業の強みとして活用できるよう、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、業界のセキュリティ活動の発展に寄与することを期待するものである。

以上