２０２１年度
「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研究」

# 中間成果報告書

２０２２年３月

PwC コンサルティング合同会社

本報告書は、国立研究開発法人新エネルギー・産業技術総合開発機構(NEDO)が管理法人を務め、内閣府が実施した「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）」(NEDO管理番号：JPNP18012)の成果をまとめたものです。

# 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。また、UNECE WP29 における UN-R155/R156 の合意に伴って、法規の観点からもサイバー攻撃への対策が必要となっている。

このような問題を解決するために、「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研究」では、出荷後における新たなサイバー攻撃への対策技術として、侵入検知システム（IDS）に着目し、IDS 導入時における評価・テストのベースラインとなる IDS 評価ガイドラインを策定した。また、実際にインシデントが発生した際の初動対応を支援するための仕組みづくりとして、コネクテッドカーの脅威情報の収集・蓄積方法の検討およびハニーポット等による収集実験が計画されている。本事業は、２０２２年度までの計画となっており、本年度は、基礎調査や検討に加え、実機を用いた検証も行い、活動成果としてまとめた。

「IDS 評価ガイドラインの策定」については２０２１年度末までの活動計画となっており、２０２０年に引き続き業界団体との技術検討会の他、検知機能を中心とした IDS の性能評価項目の妥当性検証として、実機による検証を行い、ガイドラインとして文書化を行った。

「コネクテッドカーの脅威情報と初動支援の調査研究」については、２０２０年に実施した IT 業界の脅威情報共有活動調査結果を踏まえ、自動車業界における脅威情報収集・蓄積方法の検討ならびにインシデントの初動対応基本仕様の検討を行った。また、脅威情報収集実験として、アフターマーケット製品（例：OBD を介して接続される外部機器）を模したハニーポットの観測実験に加え、コネクテッドシステムに対する攻撃技術・手法調査のため、プレイグラウンド実施にむけた検討を開始した。

# 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 with the conventional non-connected cars. Also, with the adoption of UN-R155 and R156 by the UNECE WP29, it is necessary to take measures against cyber-attacks from the aspect of legal and regulatory compliance as well.

″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 ″ focuses on Intrusion Detection System as an effective measure against vehicle cyber-attacks. The program includes development of IDS evaluation guideline as basis of evaluation and testing of the IDS upon vehicle implementation and study on method to collect vulnerability information of connected vehicles as well as experimenting using honey pod etc. as part of developing a system to support initial response against vehicle cyber-attacks.

In the first year of a three-year program until the end of FY2022, basic research and verifications using actual machines were conducted, and the results are summarized as follows.

Development of IDS evaluation guideline:

- Conducted a research on the cyber-attacks newly reported in 2020 to be used as the inputs for evaluation items for IDS’s detection performance.
- Conducted a research on IDS specifications by surveying three IDS vendors using questionnaires.
- Examined IDS evaluation items for NIDS detection performance using testbed/vehicle test-bench.

Research on connected car threat intelligence and initial response support:

- Conducted a research on method for collection and accumulation

of threat information as well as basic specifications for initial response to automotive incidents.

- Commenced experiments on threat monitoring using honey pods disguised as after-market product (e.g. External device connected via OBD).
- Conducted planning playgrounds to investigate attack techniques and methods for connected systems.

# 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研究」として、２０２０年度から２０２２年度まで計画されている、IDS の評価ガイドラインの策定および、コネクテッドカーの脅威情報の収集・蓄積方法とこれらを活用した初動支援の調査研究の２０２１年度分の中間成果報告書である。

# 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。また、UNECE WP29 における UN-R155/R156 の合意に伴って、法規の観点からもサイバー攻撃への対策が必要となっている。

このような問題を解決するために、「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研究」では、出荷後における新たなサイバー攻撃への対策技術として、侵入検知システム（IDS）に着目し、IDS 導入時における評価・テストのベースラインとなる IDS 評価ガイドラインを策定した。また、実際にインシデントが発生した際の初動対応を支援するための仕組みづくりとして、コネクテッドカーの脅威情報の収集・蓄積方法の検討およびハニーポット等による収集実験が計画されている。本事業は、２０２２年度までの計画となっており、本年度は、基礎調査や検討に加え、実機を用いた検証も行い、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研究」における研究開発計画および目的、目標に合致する形で、下記２つの活動を２０２０年８月～２０２３年２月まで実施する予定となっている。

| # | 公募要領／仕様書に記載の目的概要 | 目標 |
|---|---|---|
| a | **「IDS評価手法とガイドラインの策定」**<br><br>評価項目、評価手法、評価手順、評価環境を車載IDS 評価法としてまとめ、それぞれの評価項目に対し判定基準を検討、導出し、ガイドライン化を行い、関連業界団体にハンドオーバーし、連携して本ガイドラインの自動車業界への実務展開、実務運用につなげる。 | • 2021年度末に業界団体へIDS評価手法ガイドラインの運用移管をすることを最終目標とする。<br>• 2021年末までに各種IDSの基本機能の要素調査およびテストベッドおよび実車、あるいは実車ベンチを用いた実機による実験を行い、その結果をインプットとしてガイド化する。<br>• そのために2020年度中に最新の攻撃事例やIDSの調査といった、実験に必要な情報収集および実験内容の検討を行い、ガイドの骨子を完成させる。<br>• 2019年度の活動を踏まえ、適宜業界ステークホルダーへのヒアリングおよび調整を行うことで、実務展開および業界団体へのスムーズな運用移管を可能とする。 |
| b | **「コネクテッドカーの脅威情報と初動支援の調査研究」**<br><br>脅威インテリジェンスの収集・蓄積手法の検討と、ハニーポットによる攻撃観測の実証実験、ならびに初動支援のためのシステムの基本仕様の策定、関連業界団体にハンドオーバーし、自動車業界として共同開発が進むよう連携支援を行う。 | • 2023年に業界団体へインシデント対応初動支援を行うためのシステム基本仕様の運用移管をすることを最終目標とする。<br>• インシデント対応初動支援においては、「情報共有システム」による業界内での脅威情報の共有が有用であると仮定し、脅威情報の収集および蓄積方法、ならびにこれらを用いた初動支援の基本仕様を2021年度末までに策定する。<br>• これらの要素をシステムとして運用する際のシステム全体の基本仕様検討を行い、実務展開および最終目標である、業界団体への運用移管を2023年に完了させる。 |

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. IDS 評価手法とガイドラインの策定」、第４章にて、「b. コネクテッドカーの脅威情報と初動支援の調査研究」について、２０２１年度までの取り組みについてまとめる。

なお、本報告書は、2021 年度に活動した内容を記載したものである。業界団体との今後の調整次第で変更箇所が発生する可能性があり、最終的な内容は、次年度の最終報告書に記載予定である。

# 3. a.IDS 評価ガイドラインの策定

本章では、「a.IDS 評価ガイドラインの策定」に関する内容についてまとめる。本テーマでは、図 3-1 に示すとおり、「出荷後のセキュリティ対策」に貢献することを目的とし、各 OEM において、IDS を選定・検証・運用する際のベースラインとして活用いただくための、「IDS 評価ガイドライン」の策定および業界団体へのハンドオーバーを目標としている。また、車両の出荷後セキュリティ品質の底上げを目的とし、車載 IDS 導入の検討を始めたばかりの OEM を主な想定読者としている。

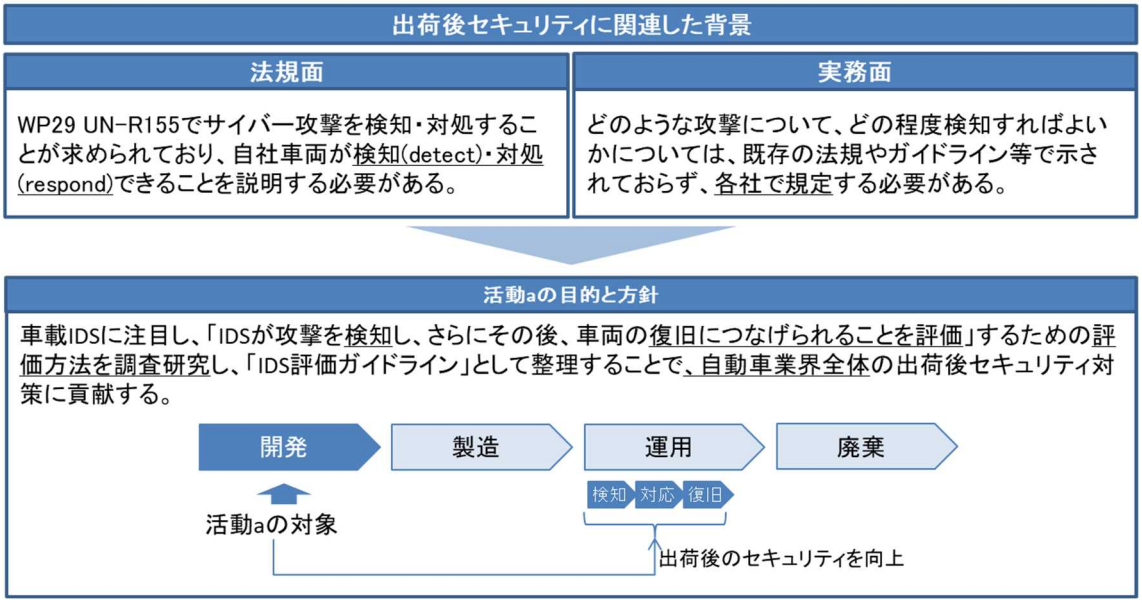



図 3-1 「a.IDS 評価ガイドラインの策定」の目的と方針

## 3.1. 活動方針

### 3.1.1. IDS 評価ガイドラインのスコープ

ガイドラインでは、下記の方針に沿って IDS 選定時の IDS 評価を行うこととした。なお、ガイドライン全体における前提として、ガイドラインの内容は、OEM/サプライヤーが検討するべき要件・評価観点であり、ガイドラインで挙げた要件を必ず満たさなければならない、ガイドラインの方法でテストをしなければならないという主旨のものではない。車両の機能や OEM のセキュリティ方針等に従い、必要に応じて OEM/サプライヤーで追加・削除することを想定している。

また、ガイドラインで示す基本テストケースのテスト方法の例において、一部、信号値の閾値やバス負荷の閾値を示しているが、これらも参考値であり、実際に評価をする際は、OEM/サプライヤーで独自に定義することを想定

している。

【ガイドラインの IDS 評価の方針】

**方針 1: 網羅的かつ IDS を比較することができる詳細レベルで概要を評価する**

**方針 2: 過去の攻撃事例と同等の想定攻撃の検知・解析可否を評価する**

**方針 3: 容易に構築可能なテスト環境で IDS 実機テストをする**

以下、各方針の背景と内容について解説をする。

### 【方針 1】網羅的かつ IDS を比較することができる詳細レベルで概要を評価する

2019 年の「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」で実施した IDS の机上評価では、多くの IDS ベンダーは特定のセキュリティイベント（SEv）[1]の検知可否や検知に関連する特定の情報のロギング可否について、「OEM からの要求に基づき対応する」と回答しており、これら観点について、机上評価により IDS の差異を理解して比較するための情報を得ることは難しいことが分かっている。

さらに、上記 2019 年の調査以降の IDS ベンダーへの追加ヒアリングにより、V-SOC[2]との連携機能、ソフトウェアアップデートに対する方針等、検知以外の重要な特性が IDS により異なること、OEM へのヒアリングにより、IDS 選定時は、全ての要求が明確に定義されているという訳ではなく、IDS の既存の優れた機能を比較して取り込みながら IDS を選定し、仕様を決定したいというニーズがあることも分かっている。

このため、使用性や拡張性等、検知可否やロギング対象の情報以外についても、網羅的、かつ、IDS の違いが理解できる詳細度で机上評価することを目指した。

一方、SEv の検知可否や検知に関連する特定の情報のロギング可否については、机上評価は難しいため、IDS 実機を使って評価をすることとした。

### 【方針 2】過去の攻撃事例と同等の想定攻撃の検知・解析可否を評価する

[1] Security Event の略。攻撃あるいは攻撃の可能性を示す事象。
[2] Vehicle - Security Operation Center の略。車両を監視し、インシデント等が検知された場合は対応を行う。

ガイドラインでは、既知の攻撃（＝過去に起きた車両への攻撃）と同等の攻撃は基本的に全て、検知・解析する必要があるという方針をたてた。

そして、この方針に従って導出した「IDS の基本要件」を満たすか否かを評価することとした。また、机上評価ではこれらの評価は不十分と考え、IDS 実機を利用して評価することとした。

【IDS の基本要件の方針】

■ 検知機能の基本要件の方針

過去の攻撃事例と同等の想定攻撃により発生した SEv を検知できる

■ ロギング・通知機能の基本要件の方針

上記検知内容を V-SOC 等で解析するために必要な機能を提供できる

**【方針 3】容易に構築可能なテスト環境で IDS 実機テストをする**

IDS 選定時点では、IDS 搭載車両や車両に搭載する部品（ECU、センサー、アクチュエーター等）は開発中であるため存在しない（一部の部品が完成形で存在する場合はあるものの、全ての部品が完成していることはない）。このため、ガイドラインでは、OEM/サプライヤーが容易に調達でき、かつ、テストに最低限必要な機材・データのみを利用し、IDS の基本要件の充足可否を IDS 実機でテストすることを目指すこととした。

3.1.2. IDS 評価ガイドライン策定に向けたアプローチ

前節で検討したガイドラインのスコープ・活動に対して図 3-2～図 3-5 で示すアプローチ、および技術検討会を通じた、業界団体からのフィードバックを得ながら、本テーマの調査・研究を進めた。

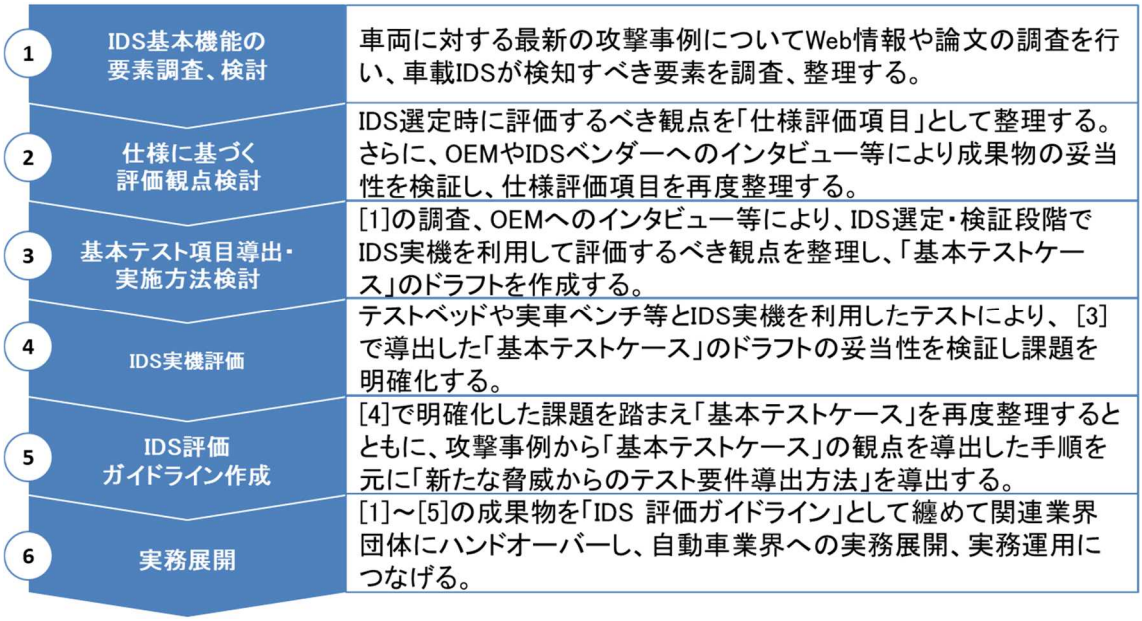



図 3-2 IDS 評価ガイドライン策定アプローチ概要

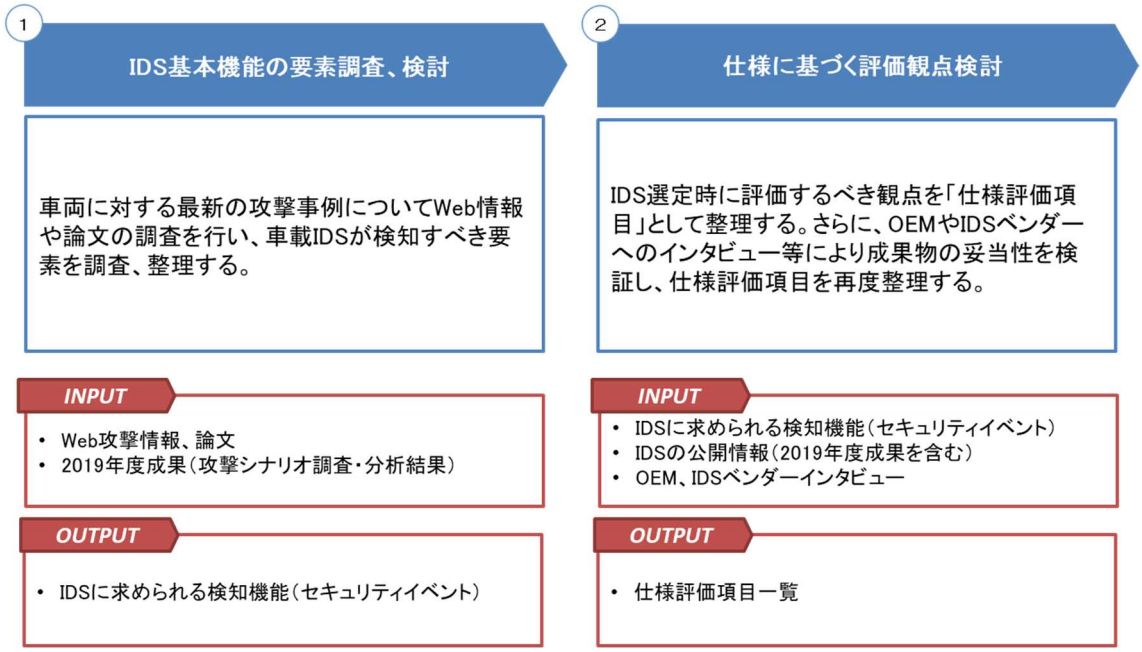



図 3-3 アプローチ詳細（１）

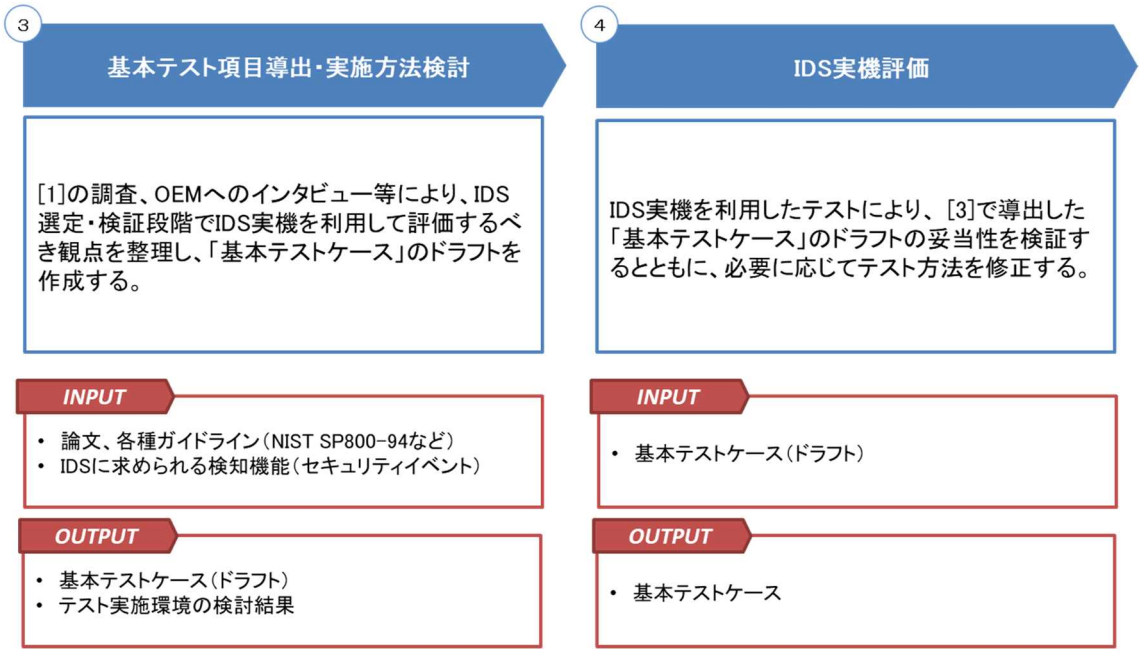



図　3-4　アプローチ詳細（２）

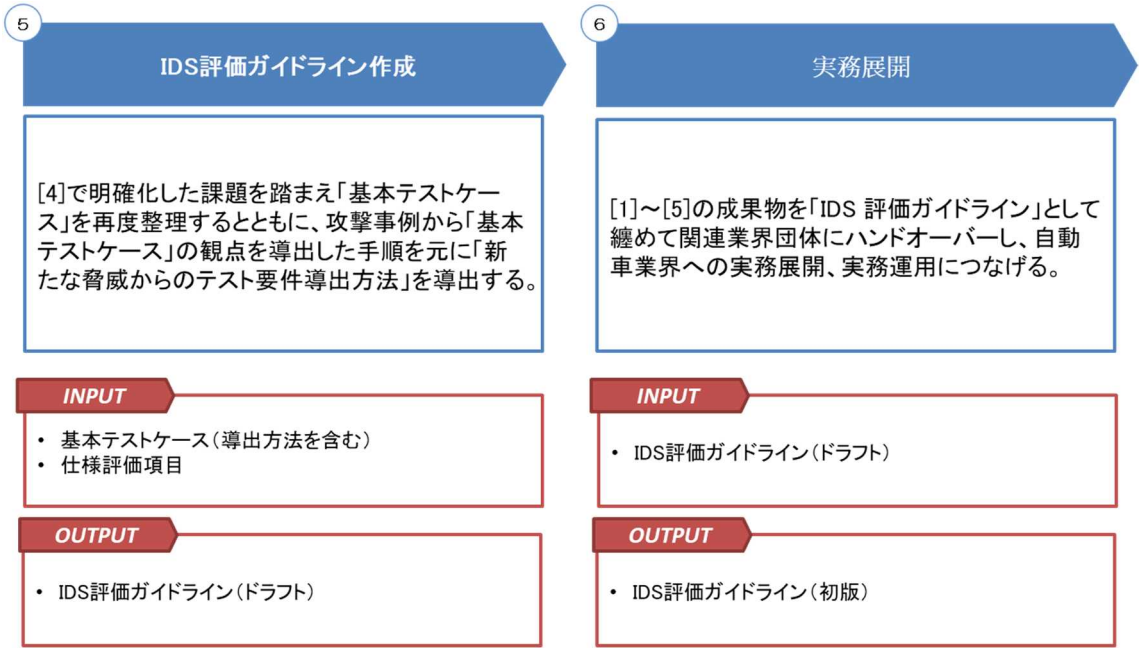



図　3-5　アプローチ詳細（３）

### 3.2. 検知機能の要件化方法の検討

前節で示した方針のうち、「過去の攻撃事例と同等の想定攻撃の検知・解析可否を評価する」に対応するために、ある過去事例から検知要件を導出する方法を検討した。要件化の流れは主に以下の通りである。


図 3-6 検知機能の要件化方法

最初に攻撃事例を入手して検知対象とする攻撃事例を選定し([1])、攻撃事例を各車両コンポーネントへの攻撃手順に分解する。このように、攻撃事例や脅威を各車両コンポーネントへの攻撃手順に分解し、各攻撃手順の攻撃が成立するための条件と達成できた攻撃の目的の情報を付加したものを「攻撃シナリオ」とする。さらに、各攻撃手順で発生した可能性がある SEv をマッピングする[2])。

攻撃事例の攻撃対象車両は、車種固有のコンポーネントを利用していたり、固有のアーキテクチャが採用されていたりするため、ソフトウェアの種類、ソフトウェアの呼び出しシーケンス、車載ネットワークに送信するメッセージのビット列や送信タイミング等、攻撃対象車両と全く同じ攻撃が特定車両で成立する可能性は極めて低い。そこで、攻撃事例と「同等」の攻撃シナリオを導出するために、攻撃シナリオを抽象化([3])する（図 3-7)。抽象化した攻撃シナリオを「抽象化攻撃シナリオ」とする。

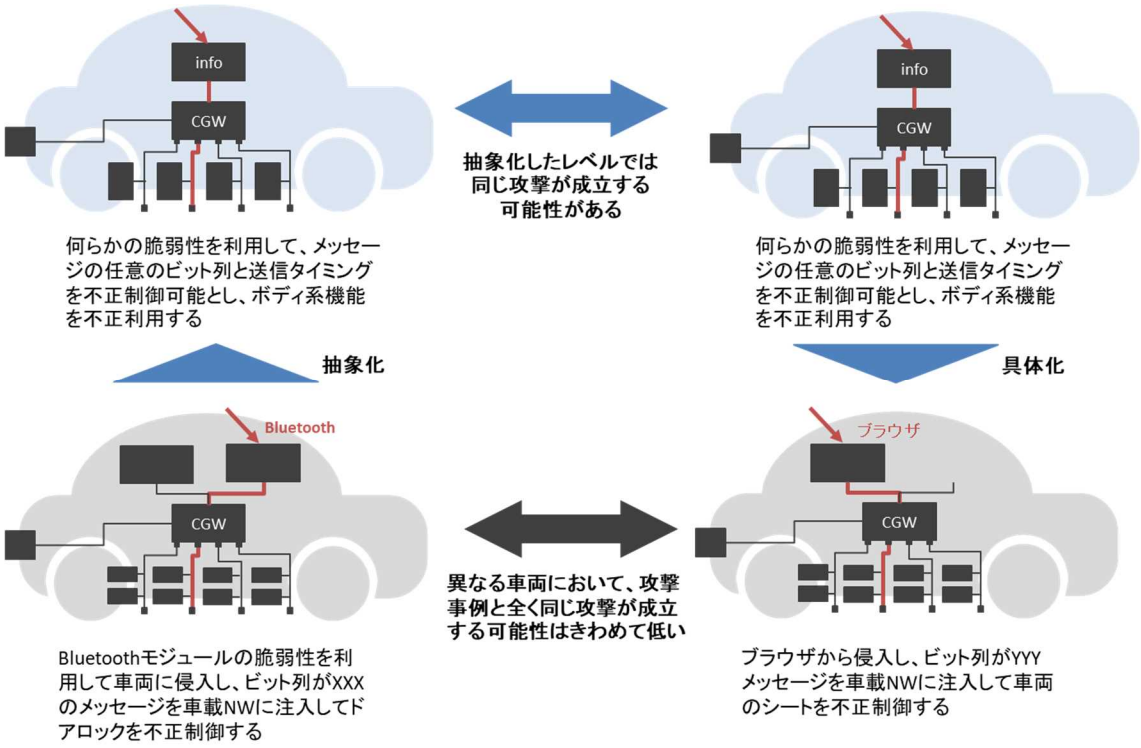



図 3-7　攻撃事例の抽象化と具体化

次に、IDS 搭載車両の仕様や脆弱性の可能性を考慮して抽象化攻撃シナリオが IDS 搭載車両で成立する場合にどのような攻撃手順になるか具体化し、IDS 搭載車両で成立する可能性がある攻撃シナリオを作成する([4]) する（図 3-7)。これを IDS 搭載車両用の「想定攻撃シナリオ」とする。

次に、OEM/サプライヤーで定義された想定攻撃シナリオのリスク評価方法や対応方法に従い、具体的な対応方法を検討する([5])。一般的に、想定攻撃シナリオ導出後の対応として、防御機能を追加する（設計開発時)、脆弱性を修正する（出荷後)、攻撃を検知可能（設計開発時、出荷後）とする、対応しない等が考えられるが、ガイドラインは、攻撃を検知可能とする対応をする場合を前提とする。

最後に、攻撃により車載ネットワークに発生する可能性がある SEv のうち、IDS で検知するべきものを選定し、要件として導出する([6])。

### 3.3. IDS 基本要件の調査検討

あらかじめ選定した攻撃事例に対して前節で検討した IDS 検知機能の要件化方法を利用し、基本要件を導出した。

### 3.3.1. 車両に対する攻撃事例調査

IDS で検知するべきセキュリティイベントを導出するために、2020 年に開催されたカンファレンスや Web 情報、脆弱性情報を調査した。うち、車両に直接関係のある 12 件について、詳細に分析した。

表 3-1　調査対象のカンファレンス一覧（閲覧日：2022.3.31）

| カンファレンス名 | URL |
|---|---|
| Blackhat USA/EU/Asia | https://www.blackhat.com/ |
| Defcon | https://defcon.org |
| ESCAR USA/EU/Asia | https://www.escar.info/ |
| USENIX SOUPS/WOOT/ScAINet/Technical Sessions | https://www.usenix.org/ |
| CodeBlue | https://codeblue.jp/ |
| SCIS | https://www.iwsec.org/scis/2020/index.html<br>https://www.iwsec.org/scis/2019/index.html<br>https://www.iwsec.org/scis/2018/index.html |
| CHES | https://ches.iacr.org/ |
| 電子情報通信学会 | https://www.ieice.org/jpn_r/ |

上記カンファレンスの論文のうち、車両への攻撃事例（車両部品単体への攻撃ではない）を選定して「検知対象の攻撃事例」として詳細に調査をした。

本事業では、以下の攻撃事例や脆弱性情報は検知の対象外とした。

i. 車両部品単体の脆弱性情報等、車両に与えた具体的な影響が不明な攻撃
ii. 車載ネットワークを経由しない攻撃（IVI や TCU から侵入してこれら ECU 内で攻撃の目的を達成する場合は対象外）
iii. センサーへの攻撃（車載ネットワークの仕様違反は発生しないため）
iv. 車載ネットワークや ECU に物理的に接続して攻撃する攻撃（車載ネットワークに直接攻撃メッセージを送信する、ECU に高電圧をかける等）

| | 調査件数 | 詳細分析対象件数 |
|---|---|---|
| Web情報、脆弱性情報 | 1329 | 6 |
| 論文 | 1062 | 6 |
| 合計 | 2391 | 12 |

図 3-8　事例調査、分析件数サマリ

表 3-2　検知対象の攻撃事例一覧

| カンファレンス名 | 攻撃事例概要 | ガイドライン上の略称 |
|---|---|---|
| USENIX Security '20 Technical Sessions | A2.認証機能に不備がある BT/WiFi<->OBD ドングルと接続し、リモートロックを無効にするメッセージを車載ネットワークに注入して車両を盗むことができた。 [Haohuang Wen, 2020] | OBD2dongle/ Wen(USENIX'20)-2 |
| Blackhat USA 2015 | FCA Jeep Cherokee において、Sprint の NW 上の任意の端末から車両にリモートアクセスし、公開されている 6667 に SSH して HU/TCU のホスト（OMAP）にアクセスし、CAN コントローラ(V850)の FW を書き換えて、SPI 経由で任意の CAN メッセージ（ステアリング、ブレーキ操作等）を送信することができた。 [Dr. Charlie Miller, 2015] | Jeep Cherokee(BH USA 2015) |
| 脆弱性情報 | トヨタ Lexus 等の DCU(Display Control Unit)の BT モジュールのバッファーオーバーフローの脆弱性を利用して自動的に外部の WiFi AP に接続するようにするとともに、CAN コントローラーのファームウェアを改ざんしてメッセージフィルタリング機能を無効化し、外部から車両に WiFi 接続して診断メッセージを CAN バスに送信できた。 [Lab, 2020] | Lexus BT 脆弱性利用の診断 msg 送信 |
| Blackhat USA 2019 | BMW の 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、UDS メッセ | BMW/Keen(BH USA2019)-1 |

| カンファレンス名 | 攻撃事例概要 | ガイドライン上の略称 |
|---|---|---|
| | ージ経由で 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。 [Zhiqiang Cai, 2019] | |
| Blackhat USA 2019 | BMW の 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、UDS メッセージ経由で 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。 [Zhiqiang Cai, 2019] | BMW/Keen(BH USA2019)-2 |
| Blackhat USA 2019 | 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 サーバにアクセスさせ、ブラウザの脆弱性等を利用して UDS メッセージ経由で ECU のリセットまたはシートの前後移動ができた。 [Zhiqiang Cai, 2019] | BMW/Keen(BH USA2019)-3 |
| Blackhat USA 2019 | 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できた（ドアのオープン、ホーン、ライトの点灯等）。 [Zhiqiang Cai, 2019] | BMW/Keen(BH USA2019)-4 |
| Blackhat USA 2019 | BMW の車両について、偽の基地局と車両の通信に MITM 攻撃を行い Provisioning データ用の署名を改ざんするとともに TCU のバッファーオーバーフローの脆弱性を利用して、UDS メッセージ経由で ECU のリセット、シートの前後移動ができた。 [Zhiqiang Cai, 2019] | BMW/Keen(BH USA2019)-5 |
| Web 情報 | Viper 社のスマートアラームにおいて、サーバの 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。 [PARTNERS, 2019] | Viper スマートアラーム サーバの脆弱性 |
| 脆弱性情報 | Daimler Mercedes-Benz Me App において、アプリとサーバ間で利用している access token を盗んだあと、本人になりすましてサーバにログイン | Daimler Mercedes-Benz Me App を悪用した不正 |

| カンファレンス名 | 攻撃事例概要 | ガイドライン上の略称 |
|---|---|---|
| | し、車両にアプリ経由でできる機能（ドアのロック／アンロック等）を利用することができた。[NVD, CVE-2018-18071 Detail, 2018] | リモート操作(2019) |
| 脆弱性情報 | 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 Key を計算し、エアバックを膨らませることができた。 [NVD, CVE-2017-14937 Detail, 2017] | エアバッグ SA 不備(2017) |

### 3.3.2. IDS 基本要件一覧

事例の分析結果から導出した、IDS の基本要件の一覧を以下に示す。

表 3-3 IDS の基本要件一覧

| 大分類 | 小分類 | ID | 基本要件 |
|---|---|---|---|
| 検知機能 | 誤検知なし | SD-FP-1 | 具体的な基本要件はガイドラインのみに記載 |
| | | SD-FP-2 | |
| | 1. 単一メッセージのデータの異常 | SD-TP-1-1 | |
| | | SD- TP -1-2 | |
| | | SD- TP -1-3 | |
| | 2. 送信周期の異常 | SD-TP-2-1 | |
| | | SD-TP-2-2 | |
| | 3. 前後のメッセージとの関係の異常 | SD-TP-3-1 | |
| | | SD-TP-3-2 | |
| | 4. コンテキストの異常 | SD-TP-4-1 | |
| | | SD-TP-4-2 | |
| | | SD-TP-4-3 | |
| | | SD-TP-4-4 | |
| | 5. 車載 NW の状態の異常 | SD-TP-5-1 | |
| | 6. 診断プロトコルへの攻撃 | SD-TP-6-1 | |
| | | SD-TP-6-2 | |
| | | SD-TP-6-3 | |
| | | SD-TP-6-4 | |

| 大分類 | 小分類 | ID | 基本要件 |
|---|---|---|---|
| | | SD-TP-6-5 | |
| | | SD-TP-6-6 | |
| | | SD-TP-6-7 | |
| | | SD-TP-6-8 | |
| ロギング機能 | | SL-1-1 | |
| | | SL-1-2 | |
| | | SL-1-3 | |
| 通知機能 | | SN-1-1 | |

### 3.4. IDS 仕様評価観点の検討

「方針 1: 網羅的かつ IDS を比較することができる詳細レベルで概要を評価する」ことを方針として仕様評価観点を導出した。図 3-9 に導出方法の概要を示す。

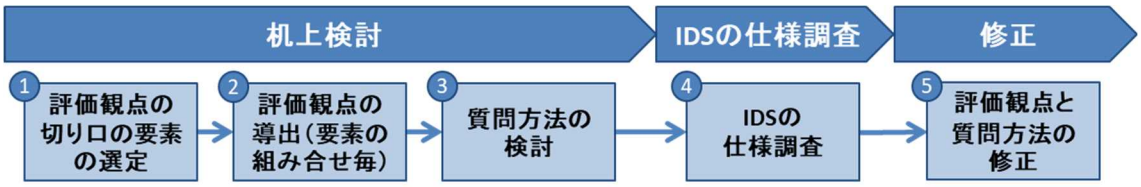



図 3-9 仕様評価観点の導出方法概要

時間軸を示す IDS の製品ライフサイクル（図 3-10）と、ソフトウェアの品質を体系的に整理した「ISO/IEC 25010 システム・ソフトウェアの製品品質モデル」の品質特性（表 3-4）を評価観点の切り口として選定し（①）、この 2 つの切り口に対して網羅的に評価できるように、製品ライフサイクルの各フェーズで参照／利用する特性に関する評価観点を表 3-5 のとおりに挙げた（②）。

さらに、①で導出した仕様評価観点が IDS を比較することができる詳細レベルかを評価するために、IDS ベンダーへの質問・回答選択肢を作成した（③）。その後、これらの質問に対して実際に IDS ベンダーに回答いただき（④）、その回答結果から、導出した仕様評価観点と質問の妥当性を検証するとともに、ガイドライン移管先である JASPAR とガイドラインの想定読者の OEM からご意見いただき、仕様評価観点・質問・回答選択肢を修正して仕様評価観点を最終化した（⑤）。

④については、質問は IDS のソフトウェアを開発している 3 社（パナソニック株式会社、イータス株式会社、Arilou Information Security Technologies Ltd.）に送付し、3 社より回答をいただいた。回答結果は、機密情報に該当するため、非公開とする。

①～⑤のステップを経て作成した仕様評価観点については、ガイドラインを参照すること。

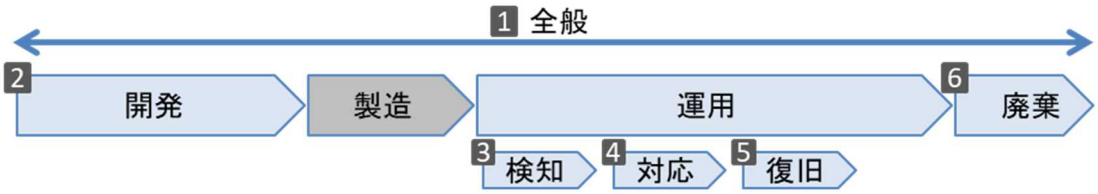



図 3-10　製品ライフサイクル

表 3-4　「ISO/IEC 25010 システム・ソフトウェアの製品品質モデル」の製品品質特性

| 品質特性 | 説明、副品質特性 |
|---|---|
| 機能適合性 | ある状況において、ニーズを満たせる機能を提供する度合い。機能完全性、機能正確性、機能適切性。 |
| 性能効率性 | ある条件で使用する資源の量に関係する性能の度合い。時間効率性、資源効率性、容量満足性。 |
| 互換性 | 同じ環境を共有する間、他の製品やシステムなどと情報交換できる度合い、機能を実行できる度合い。共存性、相互運用性。 |
| 使用性 | 効率的に、高い満足度で利用者が製品・システムを利用できる度合い。習得性、運用操作性、ユーザーエラー防止性等。 |
| 信頼性 | 明示された条件でシステムや製品などが機能を実行できる度合い。可用性、障害許容性（耐故障性）、回復性。 |
| 保守性 | 製品やシステムを修正することができる有効性や効率性の度合い。再利用性、解析性、修正性。 |
| 移植性 | ある運用環境または利用環境からその他の 環境に、システム・製品などを移すことができる度合い。適応性、設置性、置換性。 |
| セキュリティ | 認められた権限に応じたデータアクセスができ、情報及びデータを保護する度合い。機密性、責任追跡性、インテグリティ等。 |

表 3-5　IDS 製品ライフサイクルと品質特性の切り口からの仕様評価観点の導出

品質特性

| IDS製品ライフサイクル | | 機能適合性 | 性能効率性 | 互換性 | 使用性 | 保守性 | 移植性 | セキュリティ |
|---|---|---|---|---|---|---|---|---|
| 1. 全般 | | （該当する観点なし） | • 利用メモリ容量 | • CANの上位プロトコル<br>• 車載NWのプロトコル<br>• 上位Ethernetプロトコル | （該当する観点なし） | | • 提供形態対応プラットフォーム<br>• 最大入力可能バス数 | （該当する観点なし） |
| 2. 開発 | | • 設定ツールの提供有無<br>• ロギング／通知設定方法 | （該当する観点なし） | （該当する観点なし） | • DBCファイルの要否<br>• DBCファイル以外に必要な情報 | | （該当する観点なし） | （該当する観点なし） |
| 運用 | 3. 運用全般 | … | … | … | … | … | … | … |
| | 4. 検知 | … | … | … | … | … | … | … |
| | 5. 対応 | … | … | … | … | … | … | … |
| | 復旧 | … | … | … | … | … | … | … |
| 6. 廃棄 | | … | … | … | … | … | … | … |

### 3.4.1. IDS ベンダーへの質問の作成

仕様評価項目として、２０１９年度に実施したアンケート内容をベースに、IDS ベンダー３社、６製品について、検知アルゴリズム等の基本仕様、検知機能の種類、ロギング項目等、２４項目についてアンケート調査を行うことで、評価項目（アンケート項目）から得られる情報に関して考察を行った。なお、アンケート内容については、可能な限り比較が容易になるよう、選択式となるように設計した。

表 3-6　仕様評価項目（アンケート項目）概要

| セキュリティ機能分類 | 機能 | 項目 |
|---|---|---|
| 基本仕様 | 提供形態 | 製品版の提供形態 |
| | | PoC（※1）のための IDS 提供形態 |
| | | 対応プラットフォーム（SW 提供の場合） |
| | | 製品種別 |
| | プロトコル | サポートする車載ネットワークのプロトコル |
| | | サポートする上位 CAN プロトコル |
| | | サポートする上位 Ethernet プロトコル |

| セキュリティ機能分類 | 機能 | 項目 |
|---|---|---|
| | その他 | 検知方法 |
| | | 使用メモリ容量 |
| | | SOC 連携 |
| | | 車外との通信機能 |
| 検知 | 検知設定 | DBC ファイルの要否 |
| | | DBC ファイル以外に必要な情報 |
| | | 設定ツール提供の有無 |
| | | 閾値の指定パラメーター |
| | 検知 | 検知対象のセキュリティイベント |
| | | IDS ベンダー側での検知パラメーターの調整方法 |
| 対応 | ロギング／通知設定方法 | ロギング／通知設定方法 |
| | ロギング | 定常時のロギング項目 |
| | | 検知時のロギング項目 |
| | 通知 | 検知時の通知項目 |
| | 詳細分析 | ログ分析支援ツール提供の有無 |
| 復旧 | アップデート | アップデート対象（物理ポート利用） |
| | | アップデート対象（OTA 利用） |

※1 Proof of Concept の略。概念実証。新たなアイデアやコンセプトの実現可能性やそれによって得られる効果などについて検証すること。

表 3-7 「検知対象のセキュリティイベント」項目に対する質問と選択肢

| 質問 | 選択肢 |
|---|---|
| 検知対象のセキュリティイベントを選択してください。 | 車載ネットワークの負荷状態の異常 |
| | 未知の外部機器の接続またはメッセージ送出 |
| | 通信プロトコル異常 |
| | 車両の仕様外の動作（送信周期、データの閾値） |

| 質問 | 選択肢 |
|---|---|
| | ルールで定義した車両の通常状態と異なる動作（値の変化の閾値等の異常等） |
| | 車両状態としてありえない動作（高速走行中のドアオープン等） |
| | センサーで認識した走行環境としてあり得ない動作（右カーブでの左折ステアリング操作等） |
| | 送信元、送信先に関するルールからの逸脱（IP、ポートベース） |
| | その他（　　） |

### 3.4.2. 仕様評価観点の妥当性の検証

全質問項目 30 件のうち、12 件については、回答内容に差があり、IDS 製品の差異を理解できることを確認した。

以下に、回答内容に差があった内容の一部を示す。

表 3-8　回答に差があった内容（一部抜粋版）

| 評価観点 | 質問 | 回答の差異の内容 |
|---|---|---|
| 検知方法 | 検知方法を選択してください。 | シグネチャーベースの検知方法のサポートの有無に差異があった。 |
| V-SOC 連携 | 自社または他社と連携してクラウド等で検知内容を分析するサービスを提供していますか。 | 自社またはグループ会社により提供するケース、業務提携により提携するケース、その他等、差異があった。 |
| 防御機能 | 検知後、攻撃の影響を低減／防御をする機能はありますか。ある場合、具体的にどのような機能かご記入ください。 | 標準機能としてサポートするケースと、追加要求としてサポートするケースがあった。 |

また、上記を及びその他の回答を踏まえた仕様をベースとした机上評価における総括と考察を以下に示す。

- 検知対象のセキュリティイベントについて、これは、表 3-7 で示す選択肢の結果が各社概ね共通であったことから、基本的な検知機能は各社と

もにサポートしており、公称仕様における大きな違いは出にくく、この項目のみで各社の比較検討を行うことはできない。その一方で、サポートするプロトコルの種類や外部機器接続の検知機能等、一部の機能仕様について、ベンダーの独自性が出る部分もある。

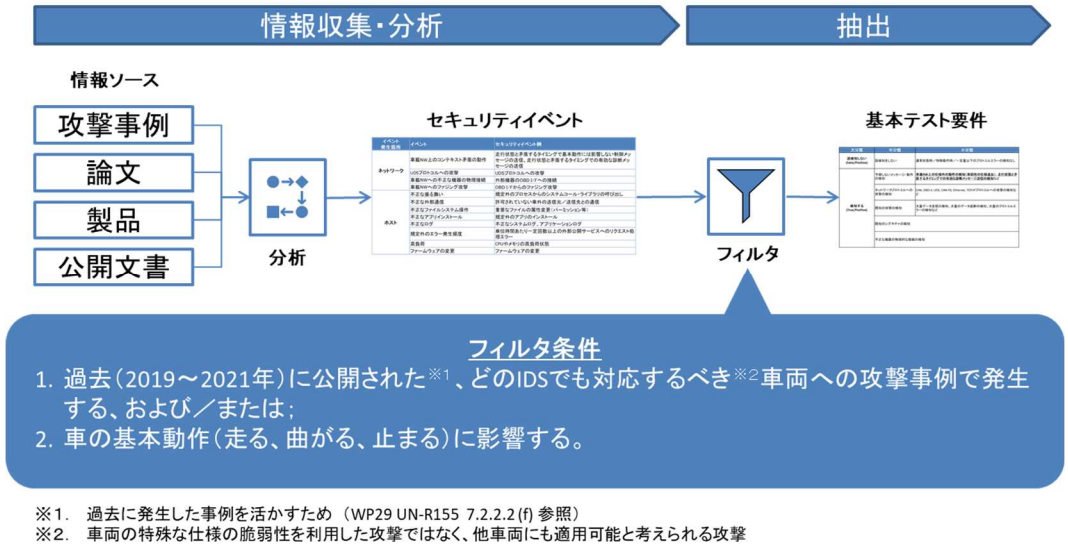
- ロギングや通知方式などについては、各社対応済み、もしくはカスタマイズ可能であり、基本的には OEM の要求ベースでカスタマイズする前提である。したがって、OEM として IDS に要求する機能とカスタマイズ機能のフレキシビリティのギャップを知ることで、IDS の比較検討がある程度可能ではないかと考える。
- 検知内容の分析を行う、SOC（Security Operation Center）に関する運用面でのサービスについては、サービスメニューとして存在しているベンダーとそうでないベンダーで差が出ていることから、IDS によるモニタリングや検知以降の分析や必要に応じた対応・復旧の支援を含めて検討する際に、この項目は比較検討する上で有用と考える。

## 3.5. IDS 基本テストケースの検討

### 3.5.1. 基本テストケースの導出方法

基本テストケースのテスト要件となり得るセキュリティイベント抽出の流れを下記に示す。なお抽出する際のフィルタ条件は以下の通りである。

1. 過去（２０１９年～２０２１年）に公開された、どの IDS でも対応するべき車両への攻撃事例で、発生する、および／または；
2. 自動車の基本動作（走る・曲がる・止まる）に影響する。




※1. 過去に発生した事例を活かすため（WP29 UN-R155 7.2.2.2 (f) 参照）
※2. 車両の特殊な仕様の脆弱性を利用した攻撃ではなく、他車両にも適用可能と考えられる攻撃

図 3-11 基本テストケースの導出方法

### 3.5.2. 基本テストケース記載項目

各基本テストケースの記載項目を表 3-9 に示す。

「テスト方法」の各項目は、そのテスト観点についてテストをするための方法の 1 例であり、基本的には 1 つのテスト観点に対して、メッセージ ID や信号値等が異なる複数のテスト方法が紐づくことを想定している。

表 3-9　基本テストケースの項目一覧

| カテゴリ | 項目 | 記載内容 |
|---|---|---|
| テスト観点 | テストケース ID | ID を記載 |
| | テストケース名 | テストケースの名称を記載する |
| | 目的 | テストケースの目的を記載する |
| | 検知対象 SEv | 検知対象の SEv を記載する |
| | 注入する攻撃 msg 種別 | テストのために注入する攻撃 msg の種別 |
| | 前提条件 | 車両の走行状態を記載する |
| | 導出源の攻撃事例 | テストケースの導出源となった攻撃事例 |
| テスト方法 | テスト環境 | シミュレーション環境／テストベッド環境のいずれかを記載する |
| | 前提とする車載 NW の仕様 | IDS 搭載車両（IDS 搭載車両）の仕様を記載する。 |
| | テスト手順 | テスト環境構築後のテストの手順を具体的に記述する<br>各観点に連番（1.、2.、・・・）をつける |
| | 期待値 | テスト結果の期待値を記載する<br>＜検知に関するテストケース（SD-FT-*, SD-TP-*）の期待値に関する説明＞<br>ガイドラインでは、IDS の検知ログにこれらの情報が出力される仕様とした。<br><br>検知件数：検知した数<br>検知バス：IDS が SEv として検知したバス（表 3-10 参照）<br>検知種別：検知の種別（表 3-11 参照）<br>検知理由：検知の理由（表 3-12 参照）<br>検知対象メッセージ |

| カテゴリ | 項目 | 記載内容 |
|---|---|---|
| 備考 | | 評価を実施する上での注意点等を記載する |

表 3-10　検知バスとして指定可能な値

| 指定可能な値 | 説明 |
|---|---|
| I | 情報系バス |
| C | 制御系バス |
| D | 診断系バス |

表 3-11　検知種別として指定可能な値

| 検知種別 | 説明 |
|---|---|
| Specific | 特定のメッセージを検知 |
| Range | 特定の時間間隔を検知 |

表 3-12　検知理由として指定可能な値

| 検知理由 | 説明 |
|---|---|
| Incorrect ID | 不正な ID |
| Range | 不正なデータの範囲 |
| Cycle | 不正な送信周期 |
| Variation | 不正なデータの変化量 |
| Order | 不正な送信順序 |
| Amount | 不正なメッセージ量 |
| Diag UDS | UDS プロトコル違反 |
| Diag OBD | OBD プロトコル違反 |
| Diag DoCAN | DoCAN プロトコル違反 |
| Diag Err | エラーレスポンス（ネガティブレスポンス含む）の受信 |

以下に、基本要件 ID　SD-TP-1-2 に対応する基本テストケースの例を示す。

車速の取り得る値は、0km/h 以上、140km/h 以下として、この範囲を逸脱した車速メッセージが指定された場合、IDS で検知することを想定したテストケースとなる。

表 3-13　基本テストケース SD-TP-1-2

| カテゴリ | 項目 | 内容 |
|---|---|---|
| テスト観点 | テストケース ID | SD-TP-1-2 |
| | テストケース名 | PT／シャシー系 msg，ボディ系 msg の注入による不正なデータの範囲の検知 |
| | 目的 | 定義された信号値の範囲に違反したメッセージが存在したとき検知することを確認する。 |
| | 検知対象 SEv | 不正なデータの範囲 |
| | 注入する攻撃 msg 種別 | PT／シャシー系 msg，ボディ系 msg |
| | 前提条件 | 走行状態：等速走行中 |
| | 導出源の攻撃事例 | • OBD2dongle/Wen(USENIX'20)-2<br>• Jeep Cherokee(BH USA 2015) |
| テスト方法 | テスト環境 | シミュレーション環境 |
| | 前提とする車載 NW の仕様 | 車速の取り得る範囲は 0 Km/h 以上、140 Km/h 以下。 |
| | テスト手順 | 1. CANoe の制御系バスに、実車の制御系バスのロギングデータを[Replay Block]から注入する。<br>2. CANoe の制御系バスに、任意のタイミングで、＜車速＞の値が 141，142，143 Km/h のメッセージを[i-Generator]から 1 件ずつ、合計 3 件注入する（注入の契機に設定したキーを押下）。<br>3. IDS の検知ログで期待値通りのログが出力されていることを確認する。 |
| | 期待値 | 検知件数：3 件<br>検知バス：C<br>検知種別：Specific<br>検知理由：Range<br>検知対象メッセージ：｛攻撃 msg｝ |
| 備考 | | |

### 3.5.3. 基本テストケース実施環境

想定されるテスト環境は大きく下記の３種類に分けることができる。そのうち、車両（ベンチ）環境はテスト環境構築において、シミュレーション環境やテストベッド環境よりも準備コストが大きいため、基本テストケースは、シミュレーション環境もしくは、テストベッド環境のいずれかで行うことを前提としたテスト手順を検討した。

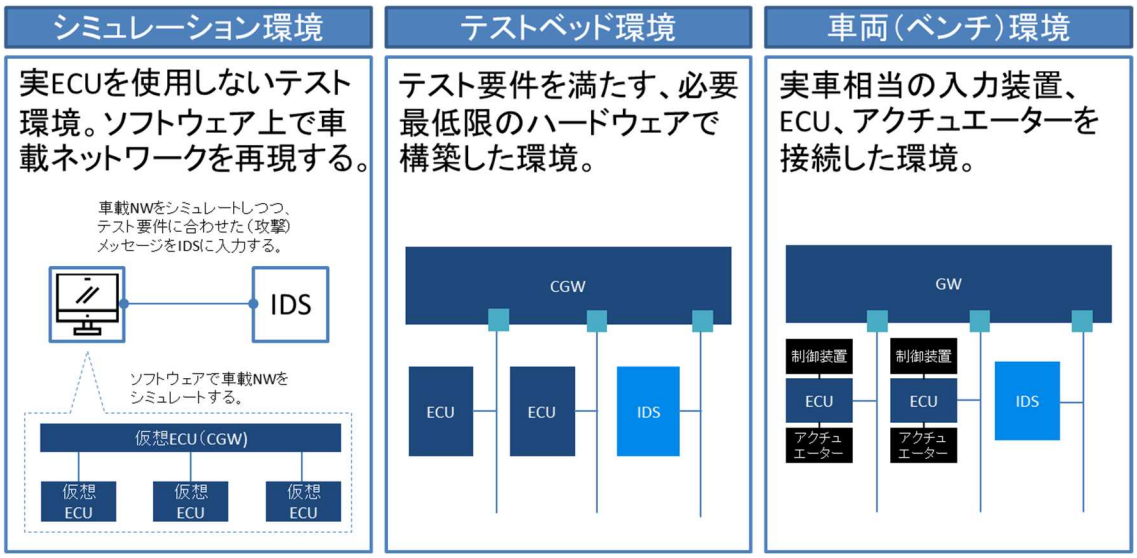



図　3-12　IDS テスト環境の種別

シミュレーション環境およびテストベッド環境で想定する基本構成は以下の通りである。

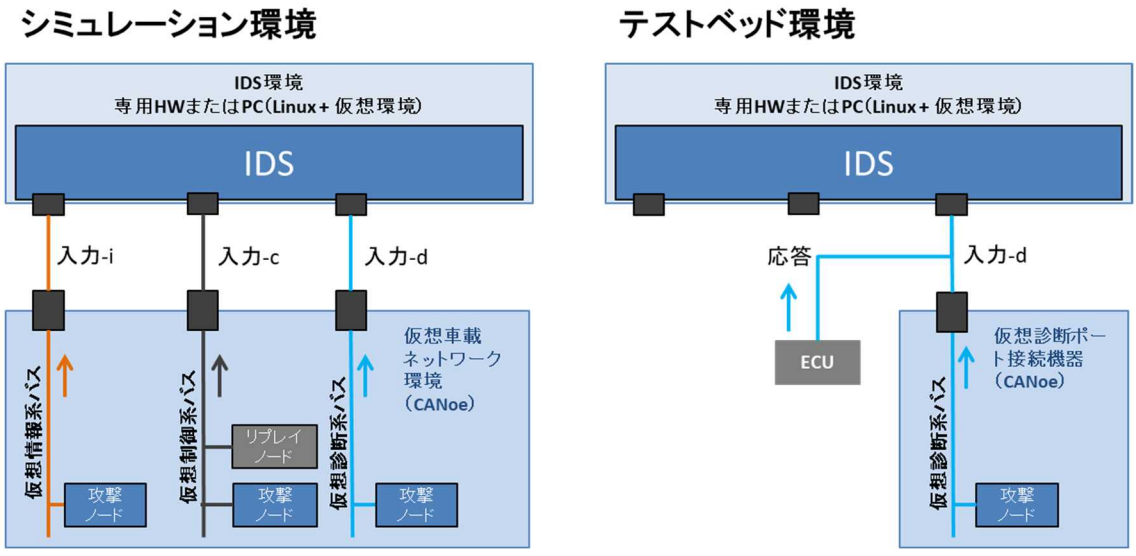



図　3-13　テスト環境概要

### 3.6. IDS 実機テストによるテストケースの検証

IDS 実機テストの目的は、基本テストケースのテスト方法の妥当性（記載したテスト方法でテストができるか）を検証することである。

このため、OEM 1 社（以降、OEM A と記載する）より、基本テストケースのテストの実施に必要な車両部品や車載ネットワークの通信データや通信仕様を提供いただいた。提供いただいた品目は全て同一車両のものである。さらに、イータス株式会社（以下、ETAS 社とする）と Arilou Information Security Technologies Ltd.（以下、ARILOU 社とする）に、各社の IDS を OEM A の特定車種用にコンフィグレーションしていただき、基本テストケースのテスト手順に従ってテストを実施し、テスト結果が期待値と一致するかを確認した。

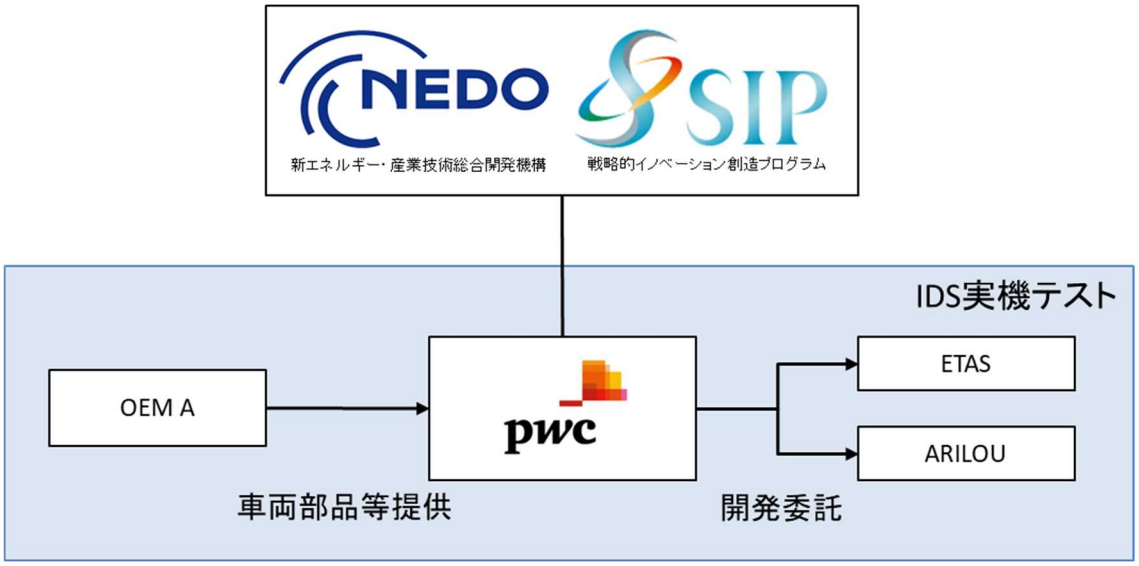



図 3-14 IDS 実機テストの体制

#### 3.6.1. 契約形態

IDS 実機テストのために締結した契約を以下に示す。IDS ベンダーごとに締結した参加基本合意書をベースに、OEM A と動産使用貸借契約を、各 IDS ベンダーと業務委託契約を締結した。

| # | 契約書名 | 主な合意項目 | 契約主体 |
|---|---|---|---|
| 1 | IDS実機テスト参加基本合意書 | • 基本事項： IDS実機テストの目的、実施における参加者、PwCの相互協力　等<br>• 機材の使用貸借： 別立ての「本件動産使用貸借契約」の締結<br>• 契約の有効期限： 活動に伴う契約の有効期限<br>• IDS実機テストの中止： 実証実験が中止となる条件<br>• 知財の帰属： 知的財産権を留保する　等<br>• 秘密保持： 以下の情報の定義、取り扱い、開示範囲　等 | OEM、IDSベンダー、PwC |
| 2 | 動産使用貸借契約書 | • 使用方法・目的： 目的、提供者による使用方法の説明、本活動以外の利用不可<br>• 引き渡し・返還： 引き渡し・返還場所、設置方法、返還期限等<br>• 費用負担区分： 参加者・PwCの施行区分、費用負担区分<br>• 提供品目（リスト）： IDS実機テストに提供するシステム、部品等の種類、数量提供に関連して支援頂く作業等の詳細 | OEM、PwC |
| 3 | 業務委託契約 | • 委託内容： 開発物、技術サポート<br>• 費用： 委託費用<br>• 納期： 納期、検収日、支払い期限 | PwC、IDSベンダー |

図　3-15　契約書一覧

### 3.6.2. 実施スケジュール

IDS 実機テストの準備から実施までの作業内容とスケジュールを以下に示す。

ETAS 社の IDS のコンフィグレーションと実機テストの期間が長くなっているのは、ETAS 社の IDS に関するこれら作業を先行して開始し、要求仕様の確認・調整や、PwC が作成した攻撃メッセージの動作確認に時間を要したためである。


図　3-16　IDS 実機テストのスケジュール

IDS 実機テストの準備として、車載ネットワークの通信仕様や OEM A へのヒアリングを元に攻撃メッセージの ID やペイロード等を仮決定したのち、IDS ベンダーと IDS 要求の調整や各基本テストケースをテスト対象とするか否かの判断をした。

### 3.6.3. 利用品目一覧

IDS 実機テストで利用した品目の一覧を以下に示す。

表 3-14　利用品目一覧

| 利用目的 | 提供元 | 品目 | 品目種別 | 詳細 |
|---|---|---|---|---|
| IDS コンフィグレーション用 | OEM | 車載ネットワーク通信データ | 電子データ | 以下を条件とした。<br>【走行データ】<br>• 車速 70Km/h 以上、100Km/h 以下で等速走行をしている状態が 2 分以上含まれる。<br>• テストで利用する ID のメッセージが全て含まれる。<br>【診断データ】<br>• テスト対象の UDS SID を含む一連の診断シーケンスが含まれる |
| | OEM | 車載ネットワーク通信仕様 | 電子データ | 以下を条件とした。<br>【走行データ】<br>• 車速、ステアリングアングルと、注入するメッセージに関して、DBC ファイルに記載されている情報が含まれる。<br>• SD-TP-6-*のテストケースで注入するメッセージの送信が許容される条件に関する情報が含まれる。<br>【診断データ】<br>• テスト対象の UDS SID の診断メッセージについて、OEM 独自に定義 |

| 利用目的 | 提供元 | 品目 | 品目種別 | 詳細 |
|---|---|---|---|---|
| | | | | した情報が含まれる。 |
| テスト準備 | OEM | 対象車両の一部の車両部品群（ECU、ハーネス等） | HW | 下記2セット<br>• CGW ECU<br>• CGW ECU用電源ケーブル<br>ハーネス（CGW ECUをIDS搭載機器と接続するため） |
| | PwC | CANoe搭載用PC ＋CANoe 12.0.101 | SW+HW | |
| | PwC | USB-CAN変換機（Vector VN-1630A） | HW | CANoe搭載PCに接続 |
| | PwC | CAN Cable 2Y | HW | VN-1630Aに接続 |
| | PwC | ETAS社IDS ＋IDS搭載用PC(Virtual Box搭載) | SW+HW | |
| | ETAS | USB-CAN変換機（ETAS ES582.1） | HW | IDS搭載用PCに接続 |
| | ARILOU | ARILOU社IDS＋IDS搭載用専用HW | SW+HW | |
| | ARILOU | ARILOU社IDSのログ出力用PC | SW+HW | IDS搭載用専用HWとイーサネットケーブルで接続 |
| | ARILOU | CAN分岐ケーブル | HW | |
| | ETAS | D-Sub 9ピン（メスメスコネクタ） | HW | |
| | ETAS | 120Ω抵抗 | HW | |
| | OEM | ECUの使い方マニュアル | 電子データ | |
| | ETAS/ ARILOU | 各社IDSの使い方マニュアル | 電子データ | Sを搭載したハードウェアの接続方法、Sの利用方法 |

### 3.6.4. IDSベンダーとの調整事項

各テスト観点に関する具体的なテスト方法の例を示すために、車両の仕様に関する以下の内容について整理・定義した。車両の仕様は、基本的にはOEMの仕様をそのまま利用したが、OEMで明確に定義されていない場合は、開示いただいた車両の仕様を元に本事業で独自に定義した。

整理・定義後のテスト方法については、ガイドラインを参照すること。ただし、車両に関する機密情報が含まれるため、一部、非公開とする。

【整理・定義したテスト方法の内容】

- テストで利用する信号値の閾値
- テストで利用する信号値のうち、特定の値が許容される前提条件（特定の信号値が許容されるコンテキストの定義）
- テストで利用するメッセージの周期乱れの最大許容値（10%）
- 各バスの最大バス負荷（95%）

さらに、各 IDS について、上記の車両の仕様や「ベースの IDS」の仕様を元に、以下の方針でテスト対象の IDS に対する要求を調整し、一部の基本テストケースについて、対象外としたり、テストの期待値等を変更したりした。表 3-15 に IDS に対する要求の調整結果の概要を示す。詳細な調整結果は、車両や IDS の機密情報が含まれるため、非公開とする。

【IDS に対する要求調整の方針】

i. 他のテストケースを参照してテストができるテストケースは対象外とする(*a)
ii. 実機テストで利用する車両にない機能（リモート機能等）に関連するテストケースは対象外とする(*b)
iii. 検知の累積発生回数の出力等、実装が難しくない（高すぎないコストで要求通りに開発可能）と考えられる機能は、対象外とする(*c)
iv. ベースの IDS が、SEv の検知はできているものの、テストケースの期待値と異なる検知（検知回数、検知理由）をし、かつ、期待値通りに検知するように開発するのに一定以上のコストがかかる場合は、対象外とするか、IDS の要求等を調整する（実際に OEM と PoC をする場合や、量産車両に搭載する場合に期待値通りに動作するかは、IDS ベンダーとの調整次第）

上記 i～iv の方針に従い、テストの対象外としたり、期待値を調整したりしたテストケースを表 3-15 に、対象外／調整した理由を表 3-16 に示す。

表 3-15 テスト対象とするかの判断と IDS 要求等の調整結果

| 大分類 | 小分類 | テストケース ID | ETAS | ARILOU |
|---|---|---|---|---|
| 検知機能 | 誤検知なし | SD-FP-1 | ○ | ○ |
| | | SD-FP-2 | 対象外(*a) | 対象外(*a) |
| | 1. 単一メッセージのデータの異常 | SD-TP-1-1 | ○ | ○ |
| | | SD- TP -1-2 | 調整(msg の仕様)(*1) | 対象外(*1) |
| | | SD- TP -1-3 | 調整（前提条件） | 調整（検知対象の msg はペイロードのみ出力） |
| | 2. 送信周期の異常 | SD-TP-2-1 | ○ | 調整（検知回数） |
| | | SD-TP-2-2 | ○ | 調整（検知回数） |
| | 3. 前後のメッセージとの関係の異常 | SD-TP-3-1 | 調整(msg の仕様)(*1) | 対象外(*1) |
| | | SD-TP-3-2 | 対象外(*a) | 対象外(*a) |
| | 4. コンテキストの異常 | SD-TP-4-1 | 調整(検知対象の msg) | ○ |
| | | SD-TP-4-2 | ○ | 調整(検知対象の msg) |
| | | SD-TP-4-3 | 対象外(*b) | 対象外(*b) |
| | | SD-TP-4-4 | 調整（前提条件） | ○ |
| | 5. 車載 NW の状態の異常 | SD-TP-5-1 | ○ | ○ |
| | 6. 診断プロトコルへの攻撃 | SD-TP-6-1 | 調整（前提条件） | ○ |
| | | SD-TP-6-2 | 調整（前提条件） | 調整（検知理由） |
| | | SD-TP-6-3 | 対象外(*2) | 調整（検知理由） |
| | | SD-TP-6-4 | ○ | ○ |
| | | SD-TP-6-5 | 対象外(*a) | 対象外(*a) |
| | | SD-TP-6-6 | ○ | ○ |
| | | SD-TP-6-7 | ○ | ○ |
| | | SD-TP-6-8 | ○ | ○ |
| ロギング機能 | | SL-1-1 | ○ | ○ |
| | | SL-1-2 | 対象外(*c) | 対象外(*c) |
| | | SL-1-3 | 対象外(*c) | 対象外(*c) |
| 通知機能 | | SN-1-1 | ○ | 対象外(*3) |

表 3-16　ベースの IDS の仕様により対象外とした理由

| 注釈番号 | 対象外とした理由 |
|---|---|
| (*1) | ETAS/ARILOU 社の IDS は、通常 OEM 様向けカスタマイズを行うが、本 IDS 実機テストでは、開発期間短縮の為、定期送信のメッセージを注入した場合は優先度の高い検知理由（「不正な送信周期」等）を 1 つだけ出力する最小限の仕様とすることとした。一方、元々の期待値は、攻撃メッセージについて、該当する全ての検知理由を出力することとしていた（例：(「不正な送信周期」と「不正なデータの範囲」を検知理由として出力する)。<br><br>今回、上記の影響があるテストケースについては、対象外としたり、検知ルールの設定において、注入する攻撃メッセージを「定期送信でない」とする等の調整をしたりした。 |
| (*2) | ETAS 社のベースの IDS は、シーケンス、ステートフルな検知ルールは対応していないため、一部テストケースは対象外とした。 |
| (*3) | ARILOU 社の IDS は、例えば AUTOSAR の IdsR モジュールに対し他の CAN バスに出力は可能であるが、今回、開発工数短縮の為、車載ネットワークへのメッセージ送信機能は省いた。このため通知機能に関するテストケースは対象外とした。 |

### 3.6.5. 実機テスト環境構築

3.5.3 で示した 2 種類のテスト環境（シミュレーション環境、テストベッド環境）でテストを実施し、意図した通りにメッセージを IDS に入力できることを確認した。

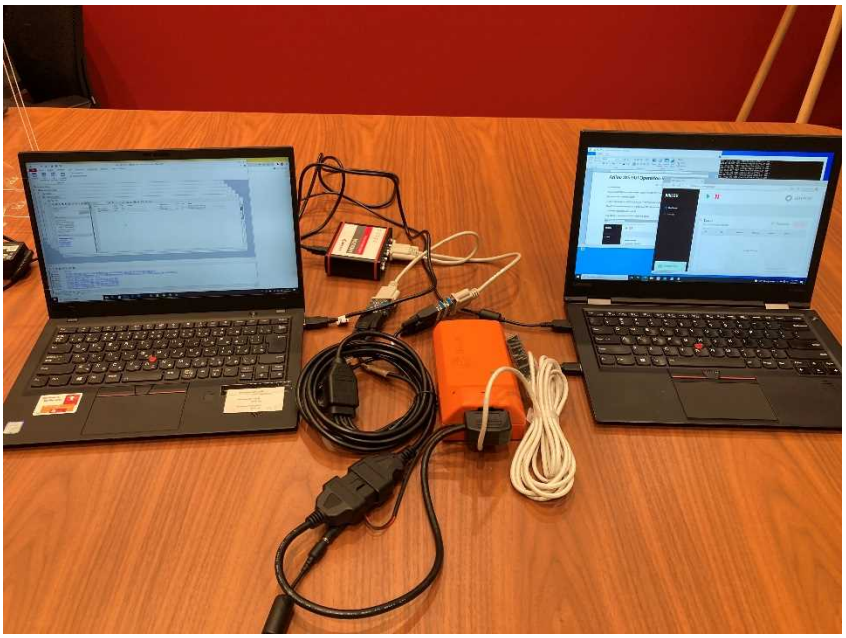


図 3-17　シミュレーション環境（ARILOU IDS 利用時）

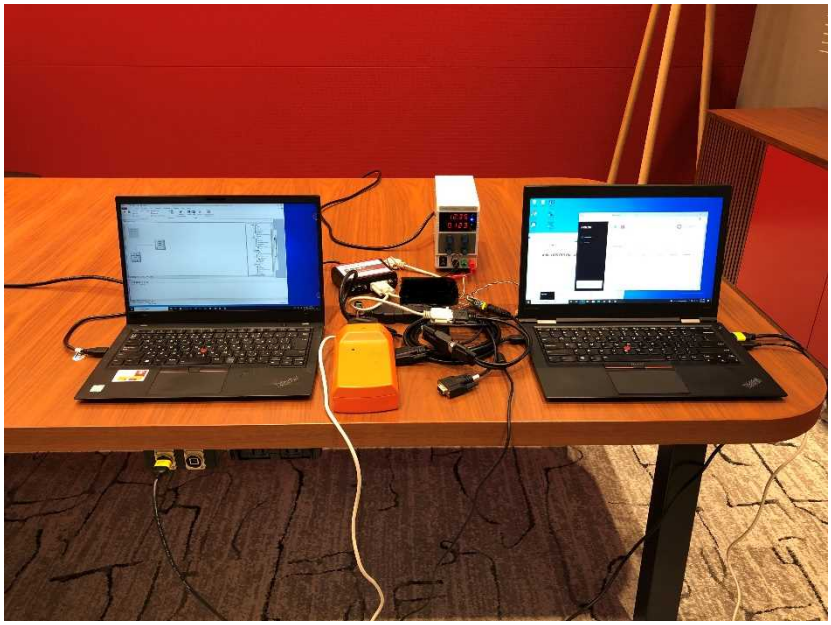


図 3-18　テストベッド環境（ARILOU IDS 利用時）

### 3.6.6. 実機テストによる検証結果

2 社の IDS について、基本テストケースで挙げたテスト観点のうち、テスト対象とした全てのテスト観点のテスト方法で示す手順を実施し、手順に誤りがないこと、期待値通りに動作することを確認することができた。

## 3.7. 実務展開に向けた活動

### 3.7.1. 業界団体との技術検討会実施履歴

ガイドラインの移管に向け、技術検討会を合計 8 回開催し、JASPAR からガイドラインに関するご意見を伺った。技術検討会の一覧を以下に示す。

表 3-17 技術検討会一覧

| 会議名称 | 日付 | アジェンダ |
|---|---|---|
| 第 1 回技術検討会 | 2020 年 10 月 9 日 | ・ 活動 a の説明 |
| 第 2 回技術検討会 | 2020 年 12 月 18 日 | ・ 活動の有効性<br>・ 機材提供のご相談 |
| 第 3 回技術検討会 | 2021 年 4 月 14 日 | ・ IDS 開発プロセスの確認と想定する基本テストケースの利用シーン<br>・ 基本テストケースのスコープ |
| 第 4 回技術検討会 | 2021 年 6 月 28 日 | ・ 基本テストケース テスト観点 |
| 第 5 回技術検討会 | 2021 年 7 月 29 日 | ・ 基本テストケース テスト方法 |
| 第 6 回技術検討会 | 2021 年 10 月 5 日 | ・ 仕様評価観点 |
| 第 7 回技術検討会 | 2021 年 11 月 18 日 | ・ 活動目的の説明（再度） |
| 第 8 回技術検討会 | 2022 年 2 月 10 日 | ・ IDS 開発の立ち上げに課題のある OEM からのコメントの説明<br>・ 移管までのスケジュールの確認 |

### 3.7.2. 業界団体への移管の準備

移管に向けた準備状況を以下に示す。

ガイドラインの移管について内諾は得ているが、具体的な事務手続きは２０２２年５月末を予定している。また、実機テストや内容検討などの実質的な調査研究は３月末で終了しているが、移管予定のガイドラインについては、移管直前まで移管先（JASPAR）からのフィードバック対応を行い、最終化を行う予定である。

表 3-18 移管に向けた準備の状況

| # | 作業・手続き | 実施主体 | ステータス |
|---|---|---|---|
| 1 | SIP 版ガイドラインの最終化 | 作成：PwC<br>レビュー：JASPAR、IDS 開発の立ち上げに課題のある OEM | 5 月末までに修正予定することで JASPAR、SIP と合意。 |
| 2 | 移管に関する契約 | NEDO、JASPAR | 調整中 |

| # | 作業・手続き | 実施主体 | ステータス |
|---|---|---|---|
| | 内容の決定 | | |
| 3 | 移管 | PwC、NEDO、JASPAR | 5月末予定 |

## 4. b.コネクテッドカーの脅威情報と初動支援の調査研究

本章では、「b.コネクテッドカーの脅威情報と初動支援の調査研究」についてまとめる。本テーマでは、コネクテッドカーの脅威情報の収集・蓄積手法、脅威インテリジェンスを活用した初動支援の基本仕様を策定し、２０２３年に業界団体への運用移管することを目標とする。

脅威インテリジェンスとは、サイバー攻撃などの脅威への対応を支援するために、収集・分析・蓄積された情報のことで、一部の産業では、企業横断的に脅威情報ならびに脅威インテリジェンスを共有する活動が行われている。脅威インテリジェンスを共有することで、類似のサイバー攻撃による連鎖的な被害を防ぐなどの効果が期待できるが、現状これらの活動はIT領域を中心に行われている。

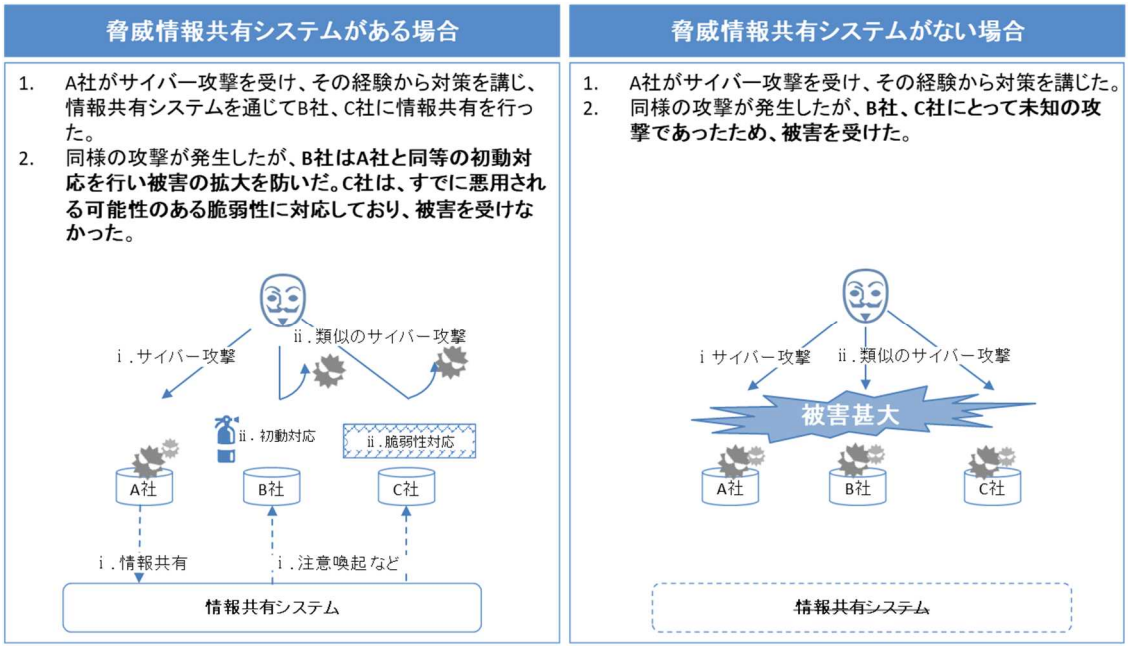



図 4-1 脅威情報共有システムのインシデント対応への効果

### 4.1. 調査研究アプローチ

脅威インテリジェンスを活用した初動対応支援の基本仕様を策定するために、以下のアプローチに基づいて計画を策定した。図 4-2～図 4-5 に全体の活動アプローチおよび２０２０年度～２０２２年度それぞれについて示す。

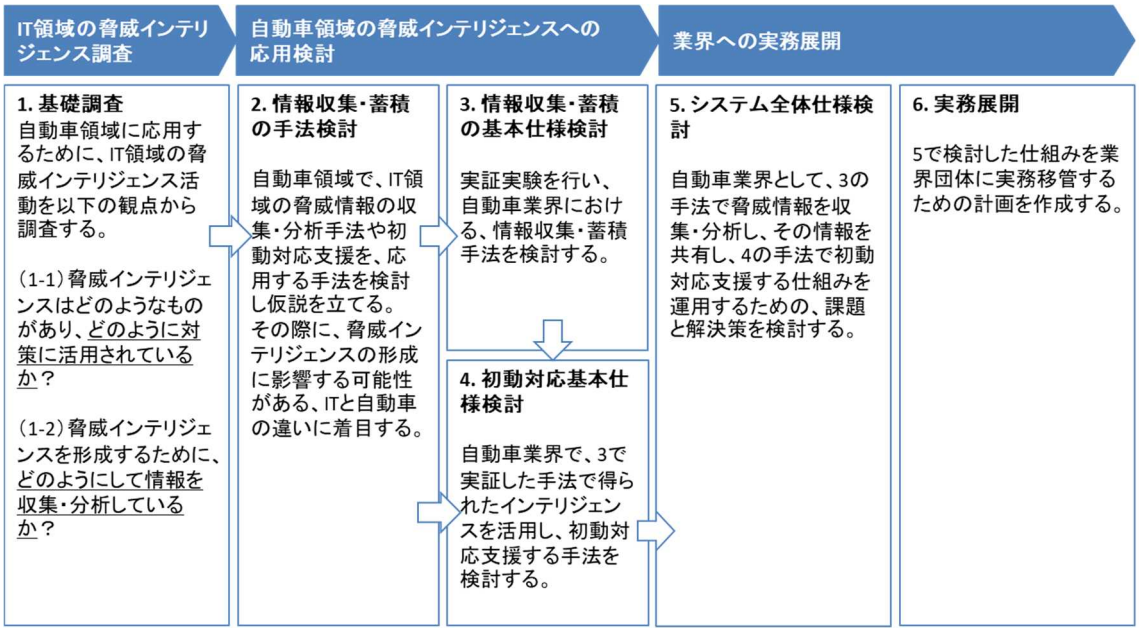



図　4-2　調査研究アプローチ概要

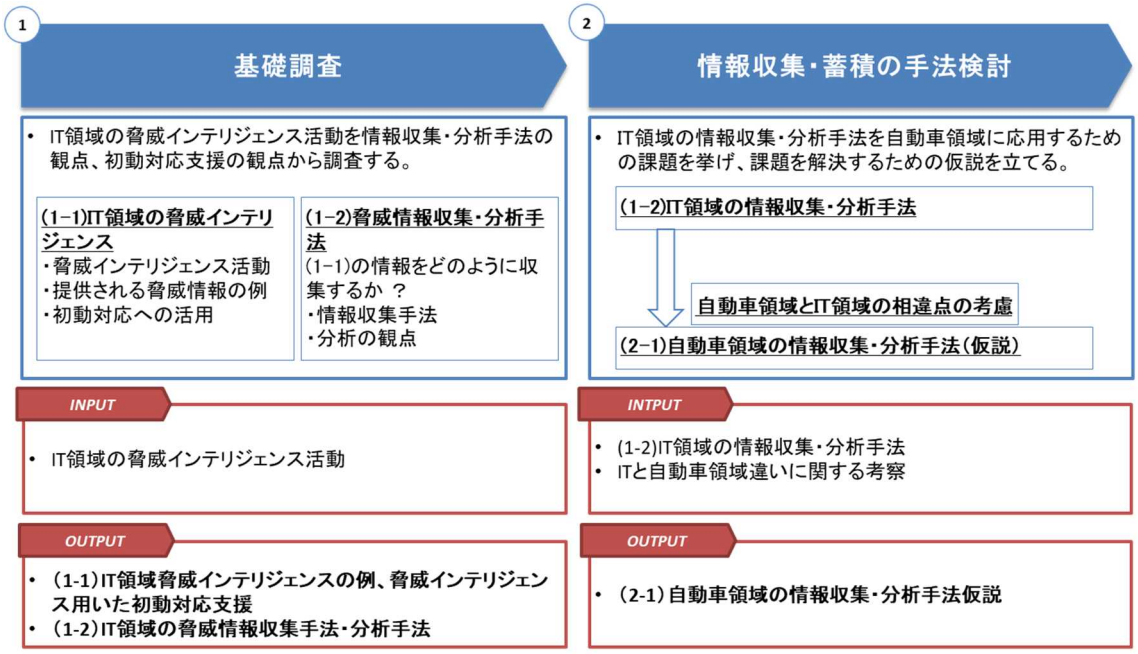



図　4-3　２０２０年度の活動アプローチ

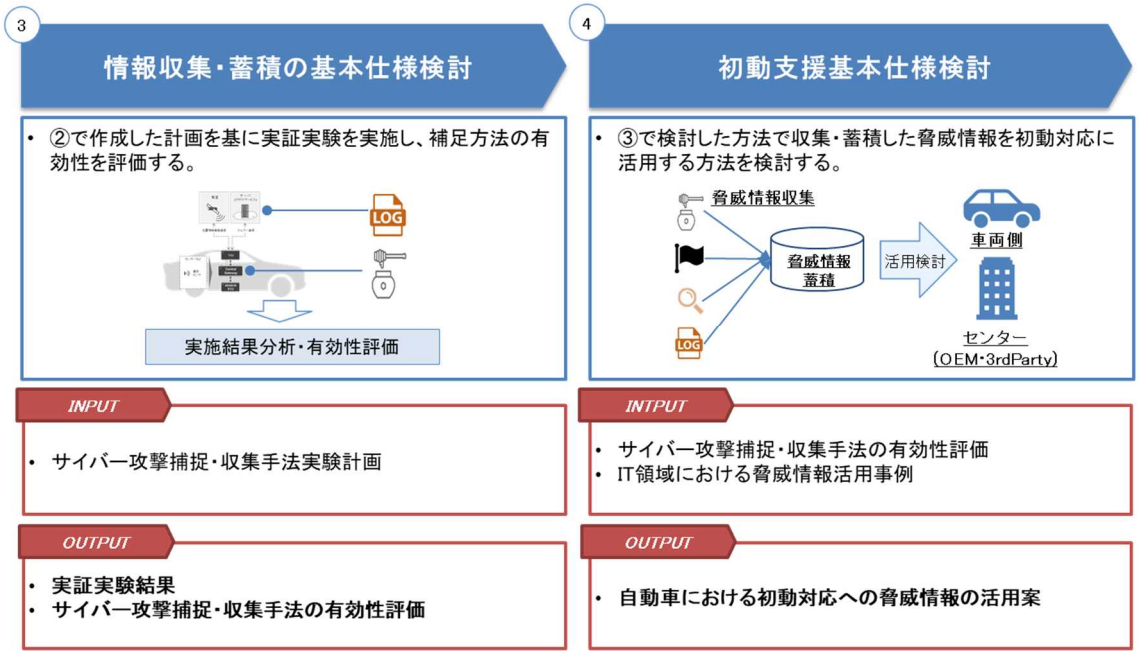



図　4-4　２０２１年度の活動アプローチ

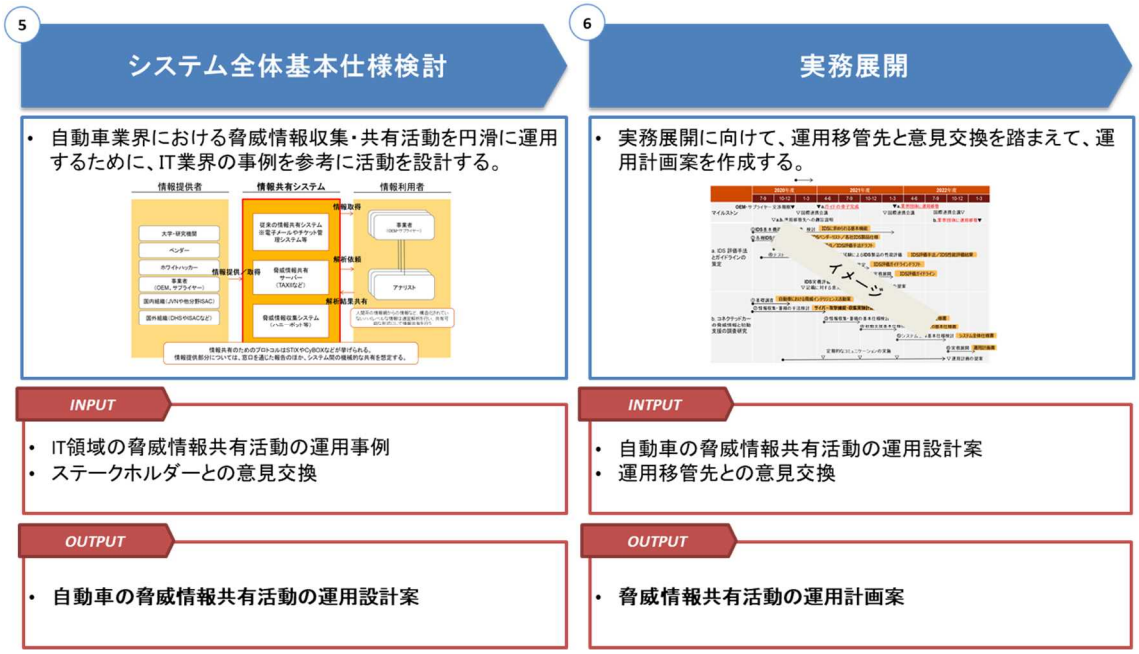



図　4-5　２０２２年度の活動アプローチ

## 4.2. 情報収集・蓄積の基本仕様検討

情報共有の価値を上げる、あるいは自動車業界の各ステークホルダーがより効率的に脅威情報を得るために、公開情報の収集以外の収集方法についてIT領域での実施事例を参考に実証実験を行う。本活動では、ハニーポットおよびプレイグラウンド(CTF)に着目し、これらの手法が自動車領域にも応用可

能か検討する。


図 4-6 情報収集・蓄積手法の検討アプローチ

4.2.1. ハニーポット実証実験

IT領域で用いられているハニーポットの自動車版を作成し、実証実験を行った。具体的には、広域スキャンで発見可能なアフターマーケット製品を調査し、該当する製品でハニーポットのプロトタイプを開発し、２０２１年１月下旬よりサイバー攻撃の観測実験を開始した。

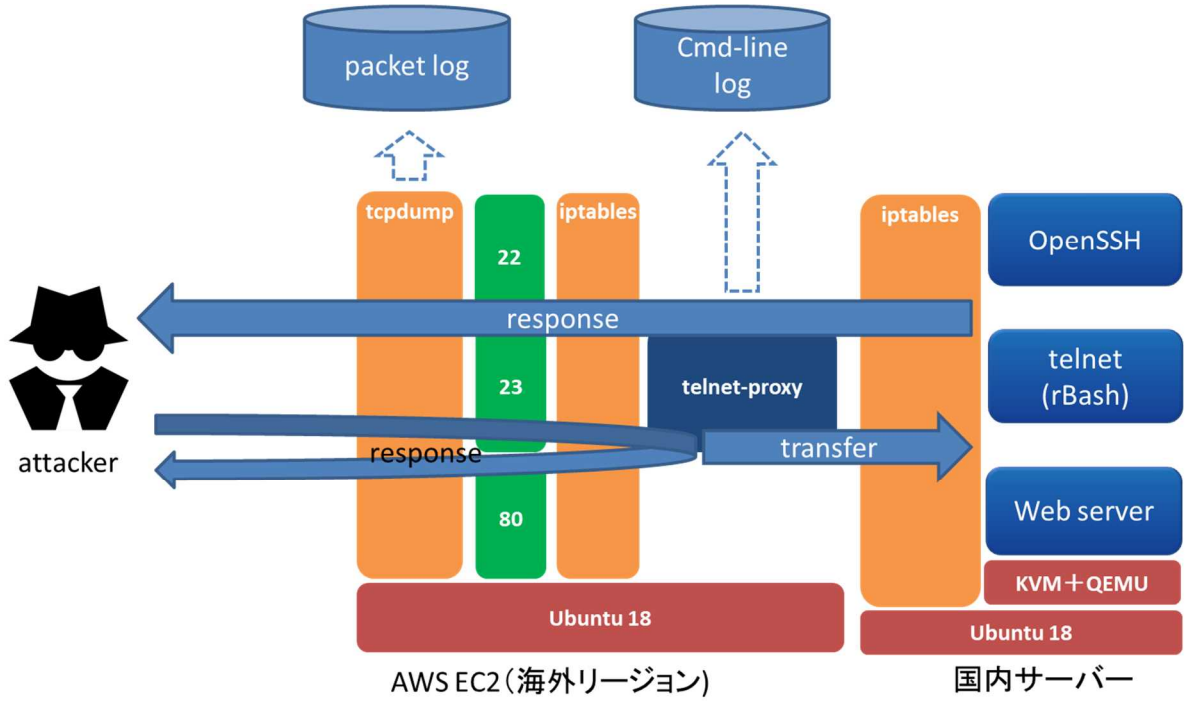



図 4-7 ハニーポット構成図

ハニーポット作成の過程で、車載ルーターやゲートウェイ等１２製品がインターネット広域スキャンにより発見された。

表 4-1 インターネット広域スキャンにより発見された製品一覧

| device name | Web-base/Cluster-base | #devices | Discovered countries | Open ports |
|---|---|---|---|---|
| 製品 A | Cluster-based | 278 | NL 26.0%<br>SE 18.9%<br>US 16.3% | 22/tcp<br>80/tcp<br>8080/tcp |
| 製品 B | Cluster-based | 391 | ES 59%<br>MA 20.3%<br>DE 11.9% | 22/tcp<br>23/tcp<br>80/tcp |
| 製品 C | Web-search-engine-based | 821 | US 96.5%<br>BR 2.2% | 8443/tcp<br>22/tcp<br>8080/tcp<br>80/tcp<br>443/tcp |
| 製品 D | Web-search-engine-based | 186 | IT 59.1%<br>DE 40.0% | 80/tcp or 81/tcp |

| | | | | |
|---|---|---|---|---|
| | | | | 21/tcp<br>22/tcp |
| 製品 E | Web-search-engine-based | 88 | DE 95.6% | 80/tcp<br>22/tcp<br>23/tcp |
| 製品 F | Both | 104 | US 60.0%<br>ES 11.8%<br>AU 10.0% | 2332/tcp<br>9191/tcp<br>9443/tcp |
| 製品 G | Web-search-engine-based | 5 | TW 100.0% | 161/tcp |
| 製品 H | Web-search-engine-based | 360 | ES99.4% | 80/tcp |
| 製品 I | Web-search-engine-based | 3 | DE 100% | 21/tcp<br>80/tcp<br>443/tcp |
| 製品 J | Web-search-engine-based | 67 | US 51.5%<br>FR 19.6%<br>CN9.6% | 2332/tcp<br>9191/tcp<br>9443/tcp |
| 製品 K | Web-search-engine-based | 144 | ES 99.9% | 21/tcp<br>22/tcp<br>80/tcp<br>123/tcp |
| 製品 L | Web-search-engine-based | 85 | us 84.3% | 8443/tcp<br>22/tcp<br>8080/tcp<br>80/tcp<br>443/tcp |

発見された一部の機器については、認証無しの Telnet を含むいくつかのサービスがインターネット上に公開されている状態であった。

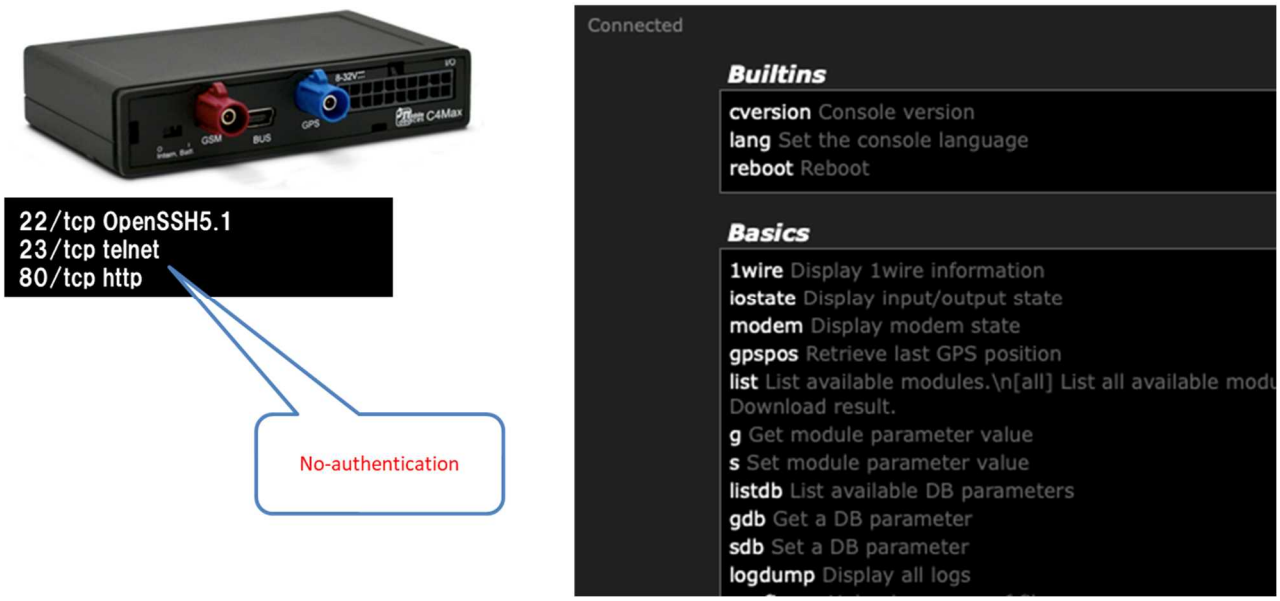



図 4-8 インターネットから発見可能な機器例

また、効率的な機器探索の方法論についても並行して検討を進めており、Web 検索エンジンを用いてキーワード検索を行い、車載器製品の Web サイトを検索するアプローチと、車載器関連のキーワードを直接 Censys で検索するアプローチの 2 つを提唱した。

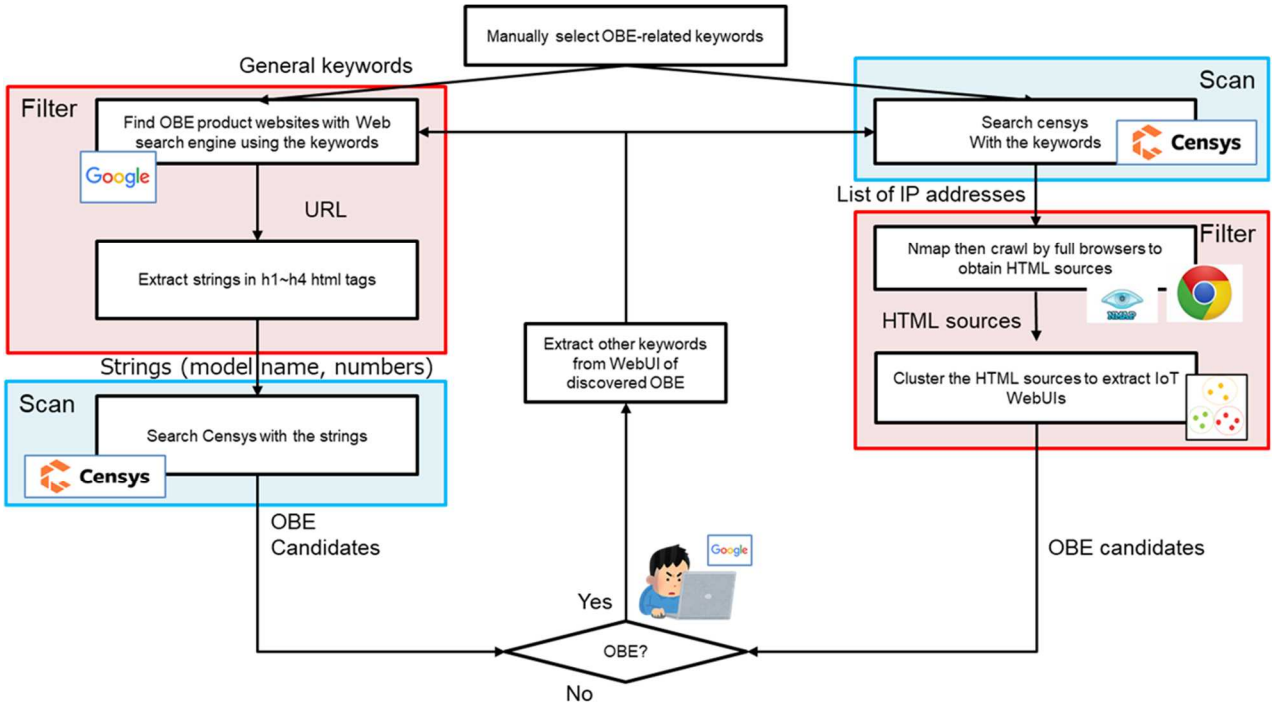



図 4-9 機器探索のアプローチ

4.2.2. プレイグラウンド(CTF)の実施検討

コネクテッドシステムにおいて、どのような攻撃を受ける可能性があるかを知るため、プレイグラウンドの実施を検討している。プレイグラウンドでは、参加者の挙動および攻撃手法から、コネクテッドシステムに対する攻撃方法・技術に関する知見を得ることを計画中である。

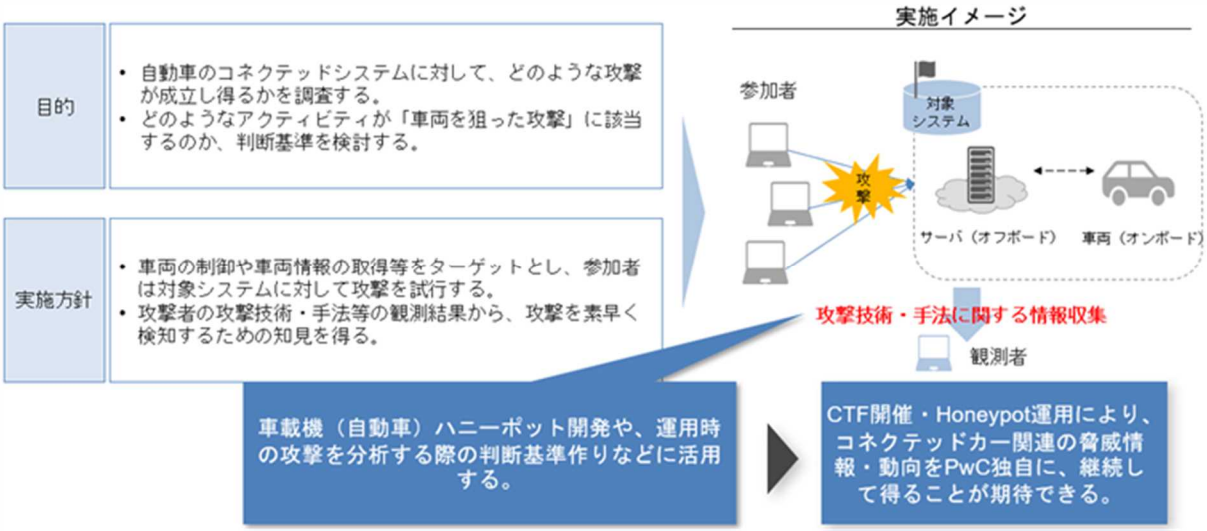



図 4-10 プレイグラウンド(CTF)の実施イメージ

4.2.3. 脅威情報記述・共有方法

効率的な脅威情報の収集および共有を行うためには、取り扱う脅威情報が一定のレベルで構造化され、共有方法が定式化されている必要がある。また、車両のコネクテッド化および自動化に伴い、既存の Web/IT 技術と連携する場面が増えており、車両と IT システムが融合したコネクテッドシステムにおいて効率的に脅威情報を活用する仕組みとして、 IT 領域で最も普及しており、記載できる情報の種類が多い STIX/TAXII に焦点を当てて調査研究を行う。

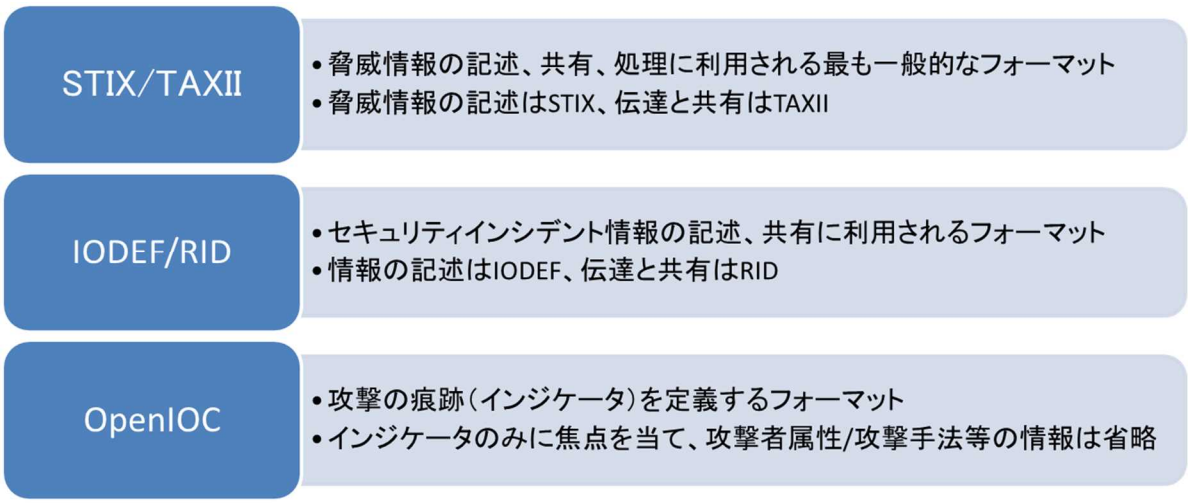



図 4-11 IT 領域で利用されている構造化プロトコル

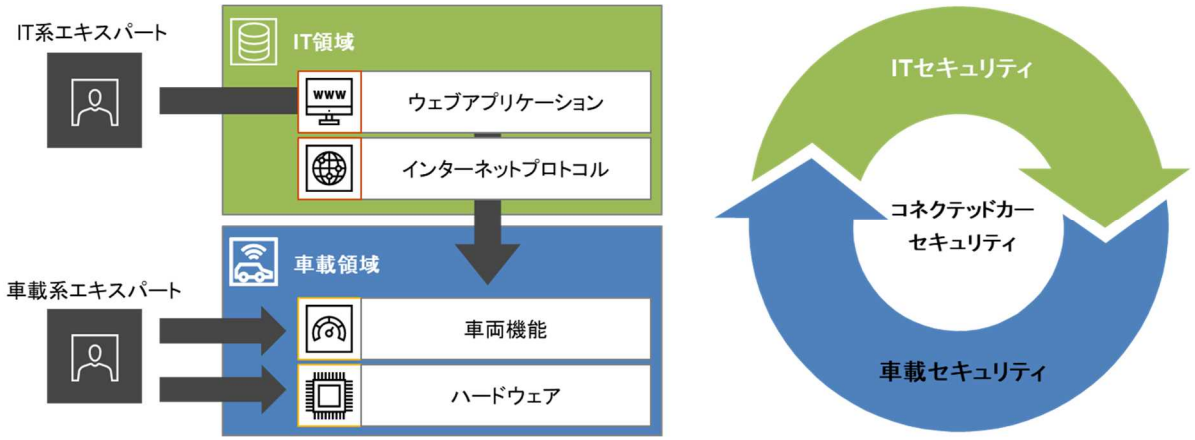



図 4-12 自動車と IT 領域の融合が進んでいる

表 4-2 STIX で記述可能な脅威情報

| # | 分類※1 | STIX 情報※2 | 説明 |
|---|---|---|---|
| 1 | IOC（侵害指標） | アイデンティティ/識別子 | 攻撃のターゲットとなった、または、なり得る実際の個人、組織、グループ、システム、業界等を表す情報。 |
| 2 | | インジケータ | 攻撃の発生または疑義があることを示す技術的なログまたはイベントに関する情報。ハッシュ値、IP アドレス、ドメイン名、証明書等。 |
| 3 | | 位置情報 | サイバー攻撃者、攻撃基盤、ターゲット等の攻撃に関する位置情報。 |
| 4 | | 観測データ | ファイル、システム、ネットワーク IP アド |

| | | | |
|---|---|---|---|
| | | | レス等のサイバー攻撃に関する情報。<br>インジケータ、位置情報と異なり、実際に1度以上観測された（単なる）情報を指す。 |
| 5 | TTPs（戦術/戦略/手順） | 攻撃パターン | サイバー攻撃者がターゲットへの攻撃に用いる方法（スピアフィッシング等）を説明する情報。 |
| 6 | | 攻撃基盤（インフラ） | 攻撃支援を目的としたシステム、ソフトウェア、物理/仮想リソース等に関する情報。<br>攻撃時に使用されるC2サーバやターゲットシステムの一部であるモバイルデバイス、サーバ等を記述する。 |
| 7 | | 攻撃セット | 単一のサイバー攻撃者によって作成・調整・実行されていると考えられる、共通のプロパティを持つ攻撃パターンと攻撃基盤群のグループ（セット）に関する情報。 |
| 8 | | マルウェア | ターゲットシステムに対して差し込まれる攻撃用のプログラム（マルウェア）がどのように機能し、何を行うかについての詳細情報。 |
| 9 | | マルウェア分析 | マルウェアの疑義のあるプログラムに対して特定の分析を行い、結果を示す。 |
| 10 | | ツール | サイバー攻撃者が使用できる正当なソフトウェアに関する情報。<br>マルウェアと異なり、システム上に存在する正当なソフトウェアであり、サイバー攻撃者に使用される可能性のあるソフトウェアを指す。 |
| 11 | セキュリティアラート | ノート | 既存のSTIXオブジェクトに対して情報（ノート）を追加することで、さらなるコンテキストを提供する。 |
| 12 | | オピニオン | 既存のSTIXオブジェクトの情報の正確性について第三者が評価したものを意見（オピニオン）という。<br>強く同意～強く反対までの5段階評価。 |

| | | | |
|---|---|---|---|
| 13 | | 脆弱性 | ソフトウェアおよびハードウェアの要件、設計または実装の弱点・蹴感に関する情報。 |
| 14 | インテリジェンスレポート | サイバー攻撃活動 | サイバー攻撃活動（キャンペーン）に関する情報。<br>特定のターゲットに対して一定期間に発生する一連の悪意のあるアクティビティまたは攻撃を説明する。<br>キャンペーンは、その目的と発生するインシデント、ターゲットとする人またはリソース、および使用するリソース（インフラストラクチャ、インテリジェンス、マルウェア、ツールなど）によって特徴付けることが可能。 |
| 15 | | レポート | サイバー攻撃者、マルウェア、攻撃手法の説明等､1つ以上のテーマに焦点を当てたサイバーインテリジェンスを纏めた情報。 |
| 16 | | サイバー攻撃者 | 悪意を持って活動していると考えられる個人、グループまたは組織に関する情報。<br>その動機、能力、目標、熟練度、過去の活動等によって特徴付けられる。 |
| 17 | ツールコンフィギュレーション | 行動（設定）の方針 | サイバー攻撃の予防または対応のために実行すべきアクションに関する情報。<br>パッチの適用、ファイアウォールの再構成、従業員のトレーニングやポリシー変更等に関する情報。 |

※1 NIST SP800-150における脅威情報の分類を参照

※2 STIX(v2.1)で定義されたDomain Objects

STIX形式で自動車領域の脅威情報が記述可能かを評価するため、２０１５年から２０２０年の間に報告された4件の自動車セキュリティに関する研究事例に着目し、以下のアプローチに従い、実際に脅威情報のSTIX形式での記述を試みた。

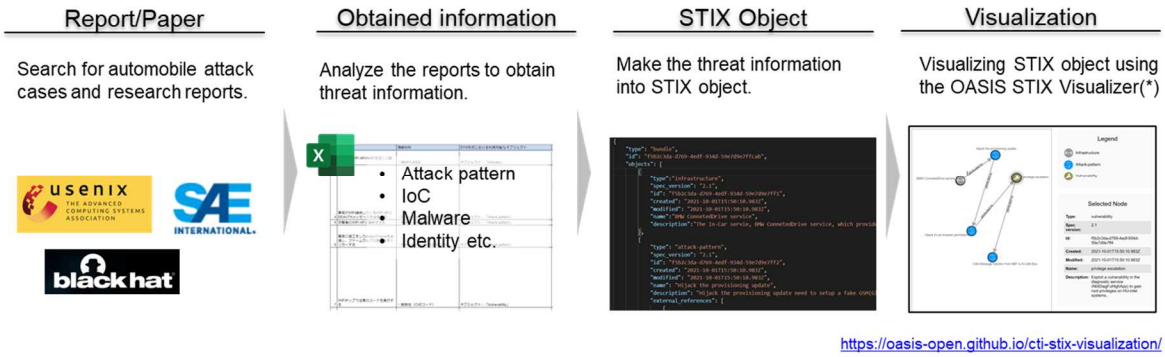



図 4-13 STIX 評価アプローチ

表 4-3 着目した研究事例 4 件

| # | 対象車種 | 概要 |
|---|---|---|
| 1 | Connected Drive 搭載 BMW 車両（BMW） | 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行った。（2020 年） |
| 2 | Model S/X（Tesla） | Tesla Model S / X に組み込まれている Marvell 製 Wi-fi モジュール（88W8688）に存在する WiFi 接続時のバッファーオーバーフローの脆弱性を悪用し、TCP23 番ポートのサービスを利用することができた。（2018 年） |
| 3 | E-Class（Mercedes-Bentz） | TCU（HERMES/Linux/ARM）の eSIM を攻撃者の 4G ルーター経由でバックエンドサーバに接続させ、他人の車両に対して Mercedes ME の機能（ドアのロック／アンロック等）を利用することができた。（2020 年） |
| 4 | Cherokee（Jeep） | 走行中の車両に対して、携帯電話網を通じて、ECU ファームウェアを書き換え、車両の操舵およびエアコン、ステレオ等の BCM を不正に操作可能と報告された。（2015 年） |

## 4.3. 初動対応基本仕様検討

本活動における「初動」とは、平時の情報収集を通してインシデントを未

然に防ぐ活動およびインシデント発生後の対応活動を指す。

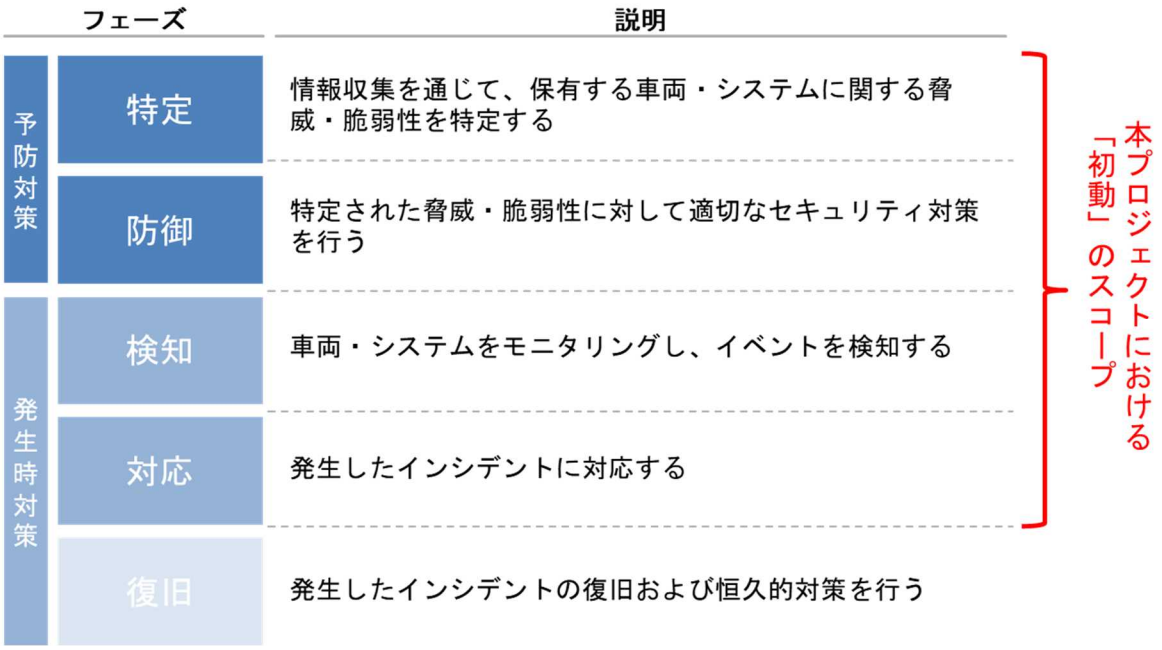



図 4-14 本活動における「初動」の定義

4.3.1. 脅威情報の初動対応への活用

脆弱性等の脅威情報を管理し、初動対応に活かすためには、日々発見・報告される脆弱性情報を収集し、それらが管理対象の車両またはシステムに関連するかの該否判断をすることが求められる。特に、オープンソースソフトウェア(以下、OSS)を活用している場合、大量の脆弱性情報が報告されたり、頻繁にアップデートされることで影響を受けるバージョンを把握する必要があったりと、該否判断を難しくする要因が増える。これらの課題への対応策としてソフトウェアに含まれるコンポーネントを管理するソフトウェア部品(S-BOM)が注目されている。S-BOMは、各社内で作成し脆弱性管理に用いることもできますが、サプライチェーン全体で活用することで、より網羅的で効率的な初動対応を行うことが出来る。S-BOMを作成し、情報共有システム等の情報源と連携することで、自社の車両やシステムの脆弱性の有無を把握できるだけでなく、インシデント発生時に関連する脆弱性および初動対応に必要な情報にスムーズにアクセスできる。

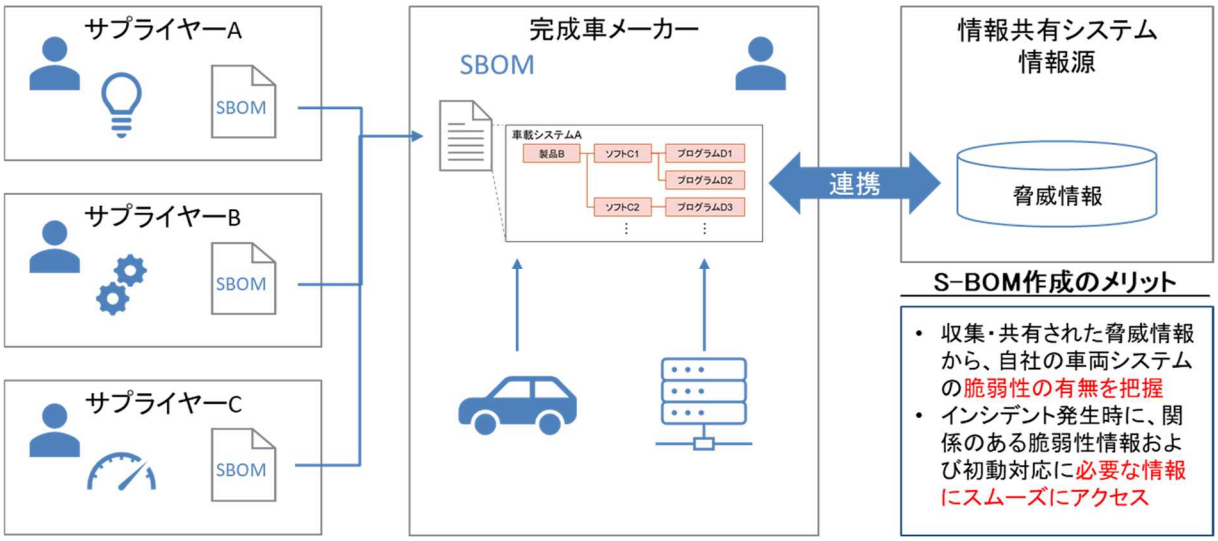



図 4-15 初動対応のための S-BOM の利用

## 4.4. システム全体仕様検討

前節までの検討内容を踏まえ、情報共有システムの情報収集・蓄積・共有を担う要素技術であるハニーポット/プレイグラウンド、STIX/TAXII および S-BOM を活用した情報共有システムのあるべき像を検討した。

| | |
|---|---|
| 情報共有システムのポイント | • 共有システムの機能：脅威情報記述（STIX）/ 共有（TAXII）/ 収集（Honeypot, CTF）<br>• 利用者の機能：S-BOMとの連携 |

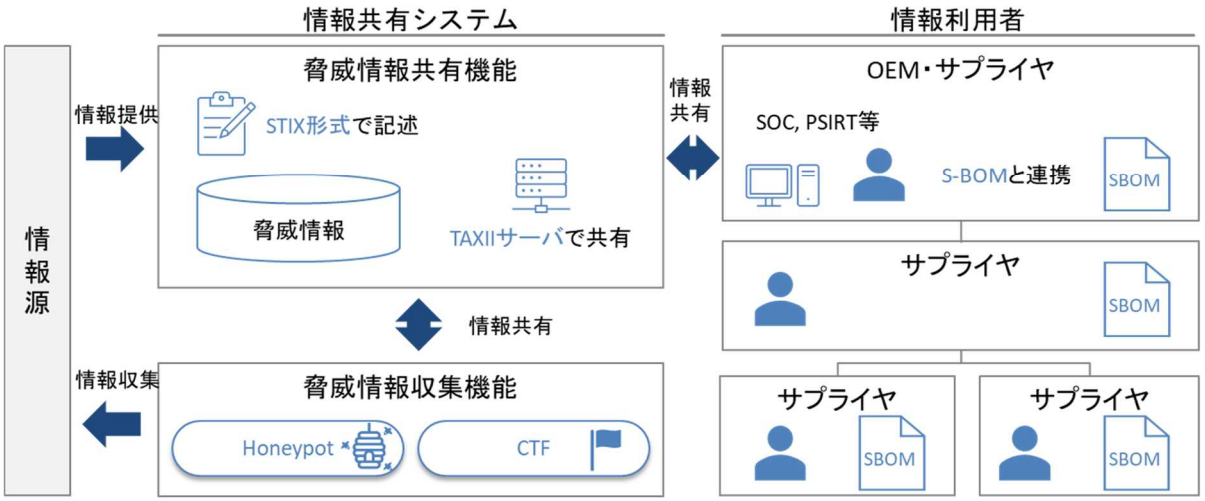



図 4-16 情報共有システムのあるべき像

成果物の移管先である業界団体との議論を推進するため、また本研究におけるスコープを明確にするため、情報共有システムを利用し、各 OEM/サプラ

イヤーが脅威情報をどの程度初動対応に活用できているかを、NIST CSF ならびにサイバーセキュリティ成熟度モデルを参考に、以下の 5 段階で定義した。

表 4-4　脅威情報活用レベルの定義

| Lv. | 説明 |
|---|---|
| 4<br>Adaptive | 自社の製品または保有するシステムに加え、サプライチェーンに関するサイバーセキュリティリスクを把握し、脅威情報をタイムリーに収集している。<br>脅威情報は自社およびステークホルダーにおけるインシデントの予防対策および発生後対策へ活用され、活用方法は定式化（自動化）され、定期的に見直されている。 |
| 3<br>Repeatable | 自社の製品または保有するシステムのサイバーセキュリティリスクを把握し、脅威情報を収集している。<br>脅威情報はインシデントの予防対策および発生後対策へ活用され、活用方法が定式化（自動化）されている。 |
| 2<br>Risk Informed | 自社の製品または保有するシステムのサイバーセキュリティリスクを把握し、脅威情報を収集している。<br>脅威情報は専門部署/チームによって分析され、インシデントの予防対策および発生後対策に活用されている。 |
| 1<br>Partial | 脅威情報を収集しているが、分析していない。<br>脅威情報をインシデントの予防対策および発生後対策に活用できていない。 |
| 0<br>Absent | 脅威情報を収集していない。 |

自動車業界として将来的にサイバーセキュリティ対策において「レベル４」を目指す想定であり、先進的かつ革新的な研究テーマとして成熟度レベル４をスコープとして引き続き業界団体とコミュニケーションし、フィードバックを得ながら調査研究を進める。

## 5. 日独連携

ドイツでは、連邦教育・研究省（BMBF）主導のもと、コネクテッドカー（自動運転）のセキュリティ研究開発支援を行っており、現在、少なくとも４つのプロジェクトが進行している。ＳＩＰは、これらのうち「SecForCARs」プロジェクトと連携している。

| ドイツの研究開発支援要件 | | |
|---|---|---|
| 少なくとも以下の成果を含む必要がある。<br>• サイバー攻撃から車両やインフラを守るための手法<br>• 車両のセキュリティを検証するための手法 | | |
| # | プロジェクト名 | 活動テーマ |
| 1 | SATiSFy<br>（自動運転車両への安全機能の実装） | 自動運転に関わる個々のコンポーネント(センサー等)と、それらの相互影響の評価 |
| 2 | SecForCARs<br>（接続された自動運転車両のセキュリティ） | 車両に対する通信を保護するための手法とツールの研究および評価 |
| 3 | SecVI<br>（車両向け通信ネットワークのセキュリティアーキテクチャ） | 車両向けの、堅牢で複雑性の低いネットワークアーキテクチャの開発 |
| 4 | VITAF | 自動運転システムの信頼性確保<br>サイバー攻撃を検知し迅速に対応する仕組み<br>サイバー攻撃を受けた場合でも安全運転への影響を回避する仕組みの開発<br>車両データの保護（マスキングなど） |

図 5-1 ドイツの政府機関主導による研究開発プロジェクト一覧

具体的には、計５回の日独連携ワークショップを開催し、２０２２年４月時点で第３回までの開催が完了している。これまでのワークショップで、自動車領域における脅威情報の分類方法、情報共有方法、ハニーポット、ハードウェアセキュリティおよび暗号技術等、双方の研究活動に関する意見交換を行った。今後、本ＳＩＰ活動終了までに、２回のワークショップを開催し双方の研究状況や成果について意見交換を進めていく。

## 6. まとめ

### 6.1. 本事業の中間成果

本年度の事業においては、「IDS 評価ガイドライン策定」、「コネクテッドカーの脅威情報と初動支援の調査研究」２つのテーマについて、調査・検討を行った。

「IDS 評価ガイドライン策定」

本テーマでは、主に IDS 開発の立ち上げに課題がある OEM/サプライヤーの車載 IDS 開発の立ち上げの加速に寄与することを目的として「IDS 評価ガイドラインライン」（ガイドライン）を作成した。

本年度は、昨年度の検討結果を踏まえてガイドラインの具体的な内容の検討を進めた。また、「基本テストケース」においては、OEM 及び IDS ベンダー２社の協力のもと、実機テストを行うことによるテストケースの手順や期待値の確認を行い、その妥当性を評価した。今後は、作成したガイドラインの最終化を行うとともに、JASPAR への移管手続きを進めていく。

「コネクテッドカーの脅威情報と初動支援の調査研究」

本年度は、先行する IT 業界を中心に要素技術や事例、フレームワークなどの考え方について情報収集、考察を行った。また、情報収集については、先行してアフターマーケット製品のハニーポットのプロトタイプを作成、実験を開始している。

今後は、オフボード側（サービスを提供する OEM サーバ側）などのハニーポットや CTF などの可能性について検討、実験を行う予定である。また、これらの活動によって集まった脅威情報の自動車領域での活用方法およびその仕組みについても併せて検討を進めていく。

## 6.2. 総括

本事業では、昨今、車両への導入検討が進んでいる IDS に対する評価手法のガイドライン化、および自動車に関する脅威情報の収集・蓄積方法と、インシデント発生時における初動支援の基本仕様について調査研究を進めている。

車載機器向けの IDS は、今後、新たなサイバー攻撃に対応する上で、検知機能を提供する代表的な技術、製品となるが、自動車業界全体としてこの技術が同じレベルで検討が進んでいるわけではないことが一部 OEM 個社へのヒアリングを通じて分かった。また、本事業では IDS の主機能である検知機能を中心としたテスト、評価手法を主なコンテンツとしているが、実際には、システムとして、IDS だけではなく、検知結果の分析（SOC や SIEM など）やその結果に基づいた対応（サプライチェーン管理など）、復旧（修正パッチのデプロイ、配信など）を行うエンティティを含めた設計することが通常であり、こうした検知～復旧までのサイクルおよびシステムを考慮することが、より適切な IDS を選定することに繋がる。

IT業界で先行している脅威情報の収集、蓄積および共有における、重要な前提として、プラットフォームが共通であるという点から、脅威も共通であるという点が挙げられる、一方で自動車の場合はOEM各社によってハードウェアレベルでアーキテクチャが異なることにより、ある脅威は特定のOEMのみの脅威にしかならない可能性が高い。しかし、IVIをはじめ、自動車領域外の既存技術の応用やそれに伴うプラットフォームの共通化が進むにつれて、共通する脅威も増加すると考えられる。加えて、攻撃事例などの実際のインシデントを分析することで、部分的に共通するコンポーネントの脆弱性が利用されている可能性があるなど、現状においても必ずしも各社固有の脅威情報だけであるとは限らない。

情報収集においては、現時点の観測結果から、明確に自動車を狙った攻撃は確認できていない。一般に、ハニーポットは、攻撃キャンペーンなど実際に攻撃が行われていることが明らかな場合に、最も効果が高く、有効に働く。そのため、意図的に自動車を狙った実際の攻撃が観測されていない現状においては、Miraiなどのマルウェアや単純なスキャン行為など、自動車であることを認知したうえで侵入、攻撃を試みるようなアクティビティは観測できない可能性がある。ただし、将来的に現状のIT領域やIoT機器同様に車両も定常的に狙われることになった場合、今回の調査研究成果である自動車向けハニーポットに関するノウハウが情報収集やそこで得られた新たな脅威への対策に寄与することになると考える。

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や業界共通の脅威については日本の業界全体の協調領域とする、あるいは積極的に共有することが適切であり、これによりコネクテッドサービスの開発や運用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や情報共有のための仕組みは、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。

**謝辞**

IDS 実機テストでは、OEM A 様より車載ネットワークの通信データと ECU をご提供いただくとともに、イータス株式会社と Arilou Information Security Technologies Ltd.より、各社 IDS を上記 OEM 様の特定車両用にコンフィグレーションしてご提供いただいた。本事業にご協力いただいた上記 3 社に感謝の意を表す。

以上