２０２０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

２０２１年３月

国立研究開発法人新エネルギー・産業技術開発機構

委託先　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）の委託業務として、PwCコンサルティング合同会社が実施した「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）/新たなサイバー攻撃手法と対策技術に関する調査研究」の２０２０年度成果を取りまとめたものです。

従って、本報告書の著作権は、ＮＥＤＯに帰属しており、本報告書の全部または一部の無断複製等の行為は、法律で認められたときを除き、著作権の侵害にあたるので、これらの利用行為を行うときは、ＮＥＤＯの承認手続きが必要です。」

# 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する。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、基礎調査や検討を中心に行い、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、IDS 検知機能の評価項目へのフィードバックを目的として、２０２０年に公表された新たなサイバー攻撃の調査を行った。また、ベンダー３社に対してアンケートおよびヒアリングによる仕様調査のほか、NIDS の検知機能を中心に、テストベッドや車両ベンチといった実機環境による IDS の性能評価項目についても検討した。

「コネクテッドカーの脅威情報と初動支援の調査研究」については、脅威情報を業界で共有することが初動支援に寄与するという仮説のもと、先行する IT 業界での脅威インテリジェンス活動および、脅威情報収集・蓄積方法の検討を行った。また、脅威情報を収集実験として、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検討および観測実験を開始した。

# 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 the three-year-program until the end of FY2022, basic research was 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.

Research on connected car threat intelligence and initial response support:

- Conducted research on method for collection and accumulation of threat intelligence as well as overall threat intelligence activities

in the IT sector.

- Commenced experiments on threat monitoring using honey pods disguised as after-market product (e.g., External device connected via OBD).

# 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２０２３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２０２０年度分の中間成果報告書である。

# 目次


1. 事業概要 ..... 9
2. 本研究調査の目的と活動概要 ..... 10
3. a.IDS 評価ガイドラインの策定 ..... 11
3.1. 「テスト」と「評価」の違い ..... 11
3.2. IDS 評価ガイドラインのスコープ ..... 12
3.3. IDS 評価ガイドライン策定に向けたアプローチ ..... 13
3.4. IDS 基本機能の要素調査・検討 ..... 15
3.4.1. 車両に対する攻撃事例調査 ..... 15
3.4.2. 事例から抽出した検知対象のセキュリティイベント ..... 21
3.5. 仕様に基づく評価観点検討 ..... 22
3.6. 基本テスト項目導出・実施方法検討 ..... 24
3.6.1. 基本テストケースの定義 ..... 24
3.6.2. 基本テストケースの導出方法案 ..... 25
3.6.3. 基本テストケース概要（ドラフト） ..... 26
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 ..... 28
4.1. 調査研究アプローチ ..... 28
4.2. 基礎調査 ..... 30
4.2.1. 脅威インテリジェンスの定義 ..... 31
4.2.2. IT 領域の脅威インテリジェンス ..... 32
4.2.3. （参考）脅威インテリジェンス活動一覧（国・業界団体） ..... 34
4.2.4. （参考）脅威インテリジェンス活動一覧（企業） ..... 37
4.2.5. 脅威情報共有活動の調査 ..... 39
4.2.6. IT 領域の脅威情報収集手法 ..... 39
4.2.7. IT 領域での情報の分析手法 ..... 43
4.2.8. IT 領域での情報の蓄積手法 ..... 44
4.3. 情報収集・蓄積の手法検討 ..... 45
4.3.1. 脅威が観測され得るサービス・機器 ..... 45
4.3.2. 自動車領域の特性を考慮した脅威情報収集方法の検討 ..... 47
4.3.3. 脅威情報の収集実験に対する仮説と期待 ..... 48
4.4. 情報収集・蓄積の基本仕様検討 ..... 49
5. 日独連携 ..... 51
6. まとめ ..... 52
6.1. 本事業の中間成果 ..... 52
6.2. 総括 ..... 53

# 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する。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、基礎調査や検討を中心に行い、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～２０２２年３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、２０２０年度の取り組みについてまとめる。

# 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。

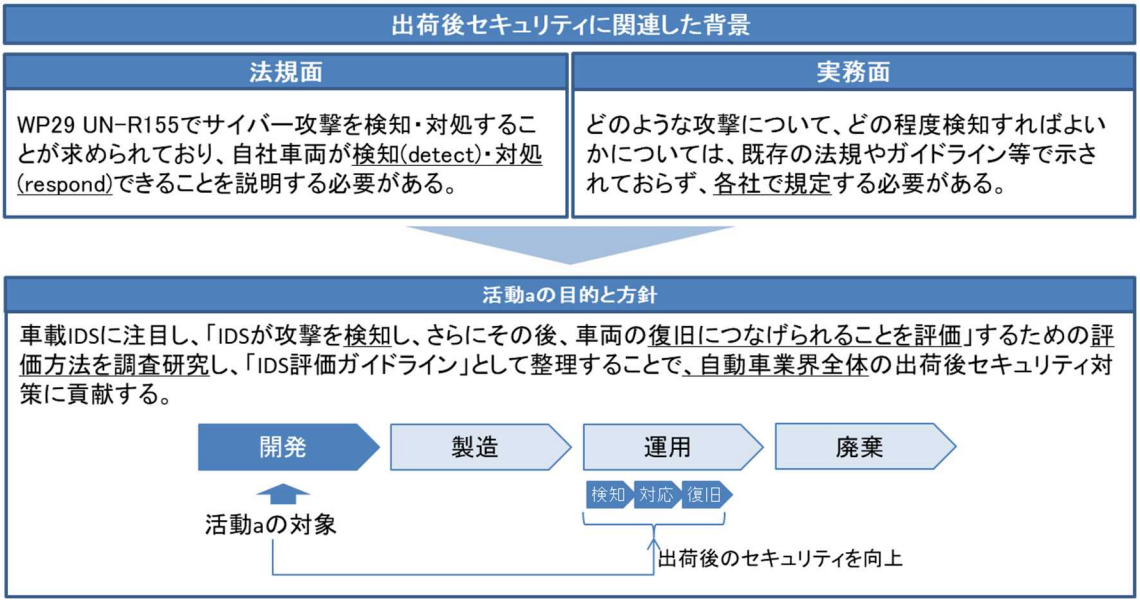



図 3-1 「a. IDS 評価ガイドラインの策定」の目的と方針

## 3.1. 「テスト」と「評価」の違い

本テーマでは、IDS に対する「テスト」と「評価」という 2 つのキーワードが用いられており、以下に定義と違いを示す。

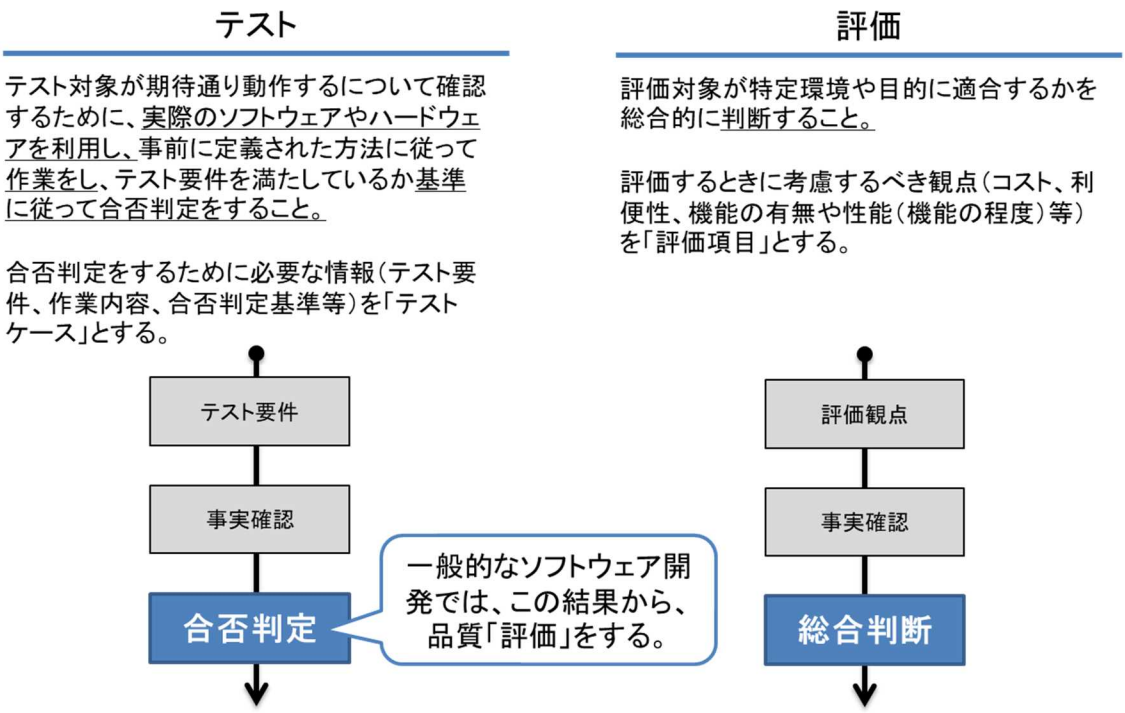



図　3-2　「テスト」と「評価」の違い

## 3.2.　IDS 評価ガイドラインのスコープ

図　3-3 で示すとおり、車のライフサイクルの開発～運用フェーズにおいて、より良い IDS を選定し、実験室で可能な限り IDS の不具合を見つけ、新たな脅威に継続して対応することを論点として導出し、表　3-1 で示す 3 つの活動をすることとした。また、これら活動の想定成果と期待される効果は（仮説）は図　3-4 の通り。

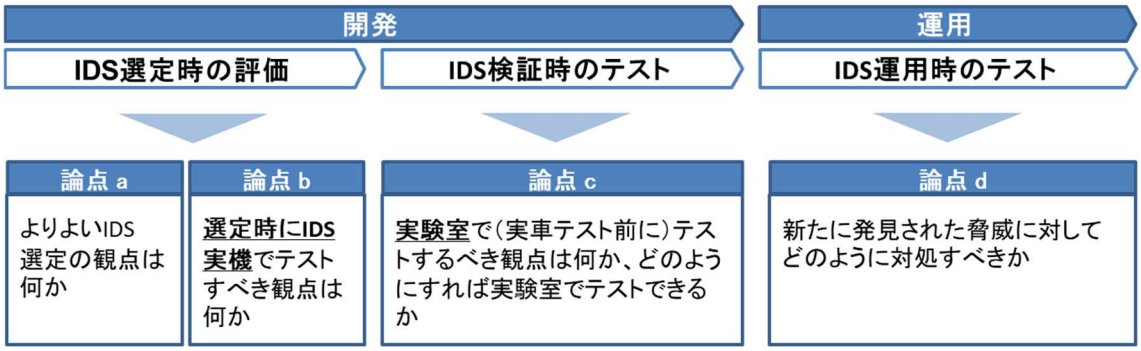



図　3-3　開発～運用フェーズにおける IDS の評価・テストに関する論点

表 3-1 IDS 評価ガイドライン策定に向けた活動スコープ

| # | 活動 | 対応する論点 |
|---|---|---|
| 1 | 仕様に基づく評価観点の検討 | a |
| 2 | 基本テストケース（テスト要件、前提条件、テスト環境、テスト手順等）の検討 | a, b, c |
| 3 | 攻撃事例から IDS に求められる検知機能を導出する手法の検討 | d |

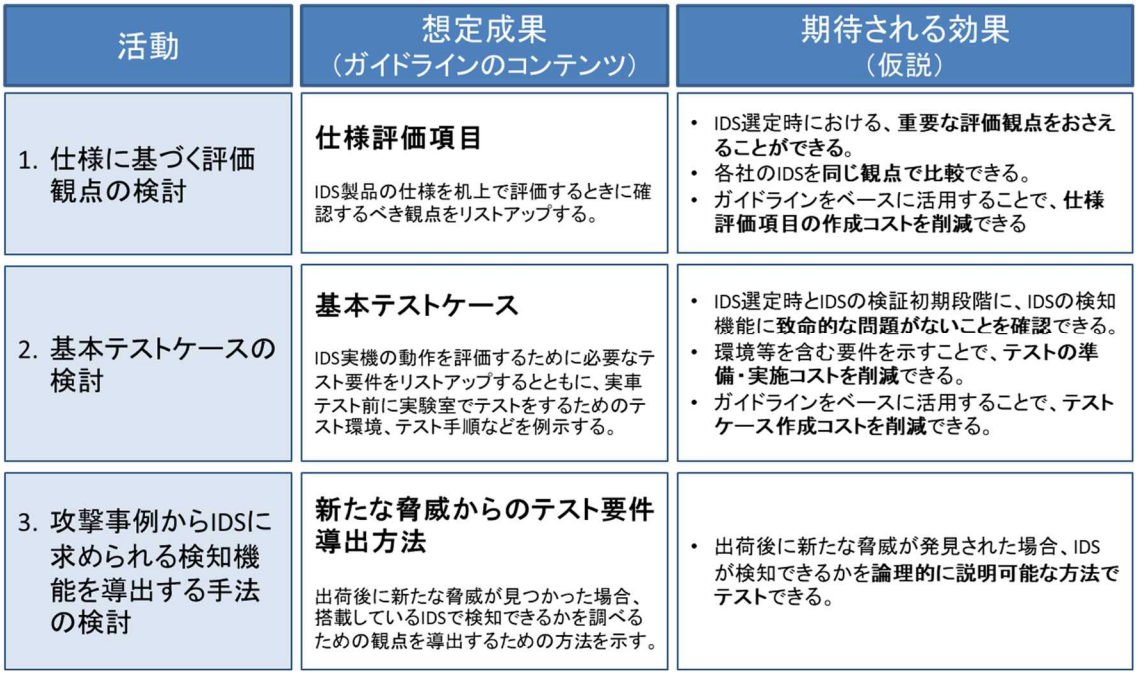



図 3-4 活動成果で期待される効果の考察

## 3.3. 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 3-5～図 3-8 で示すアプローチで調査・研究を進める。このうち、1～3 までが今年度の活動となる。

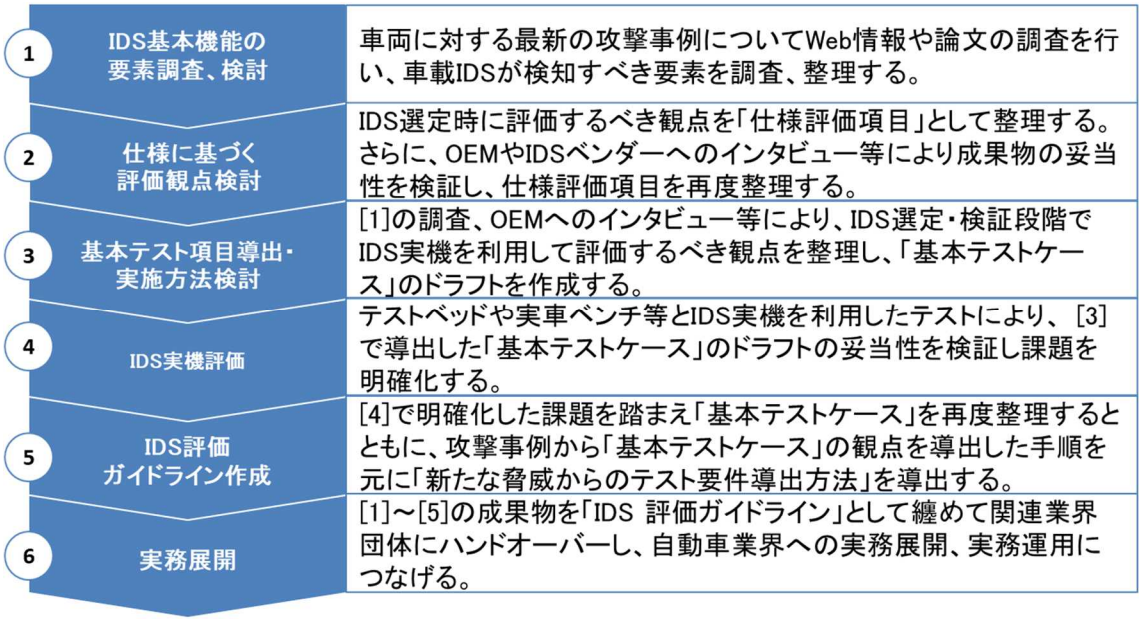



図 3-5 IDS評価ガイドライン策定アプローチ概要

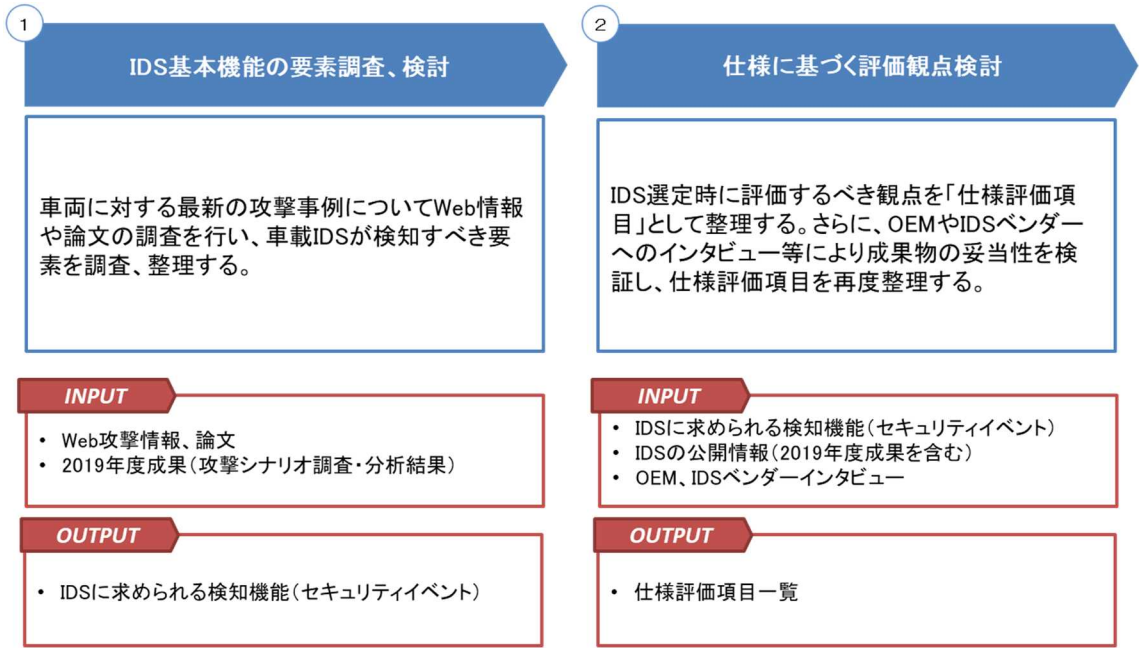



図 3-6 アプローチ詳細（1）

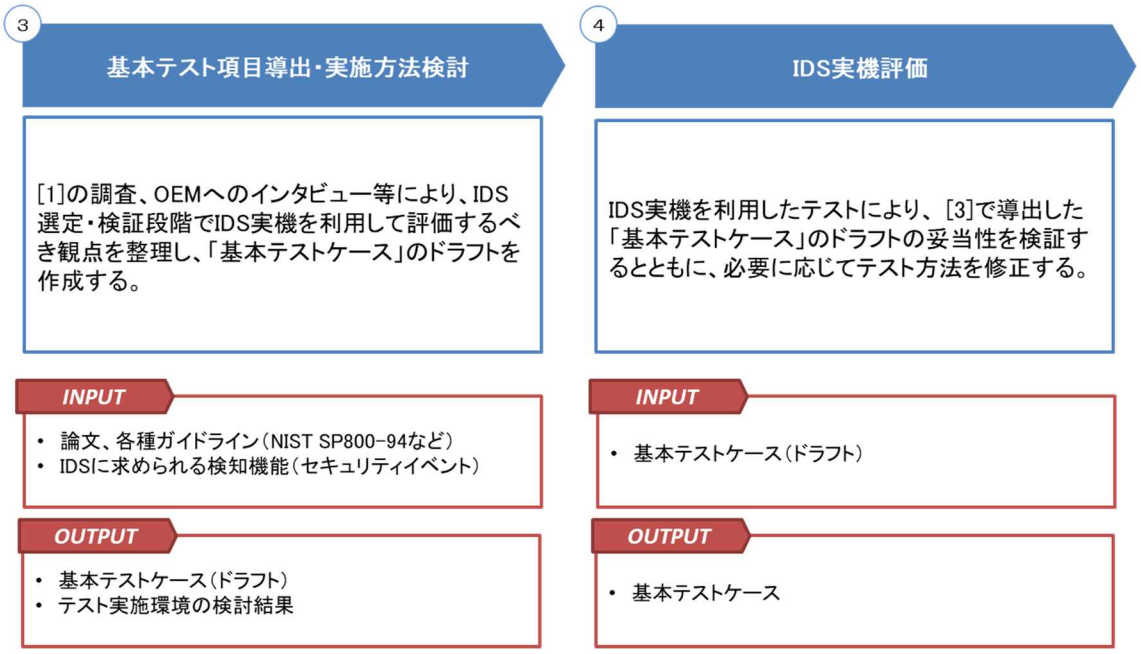



図　3-7　アプローチ詳細（２）

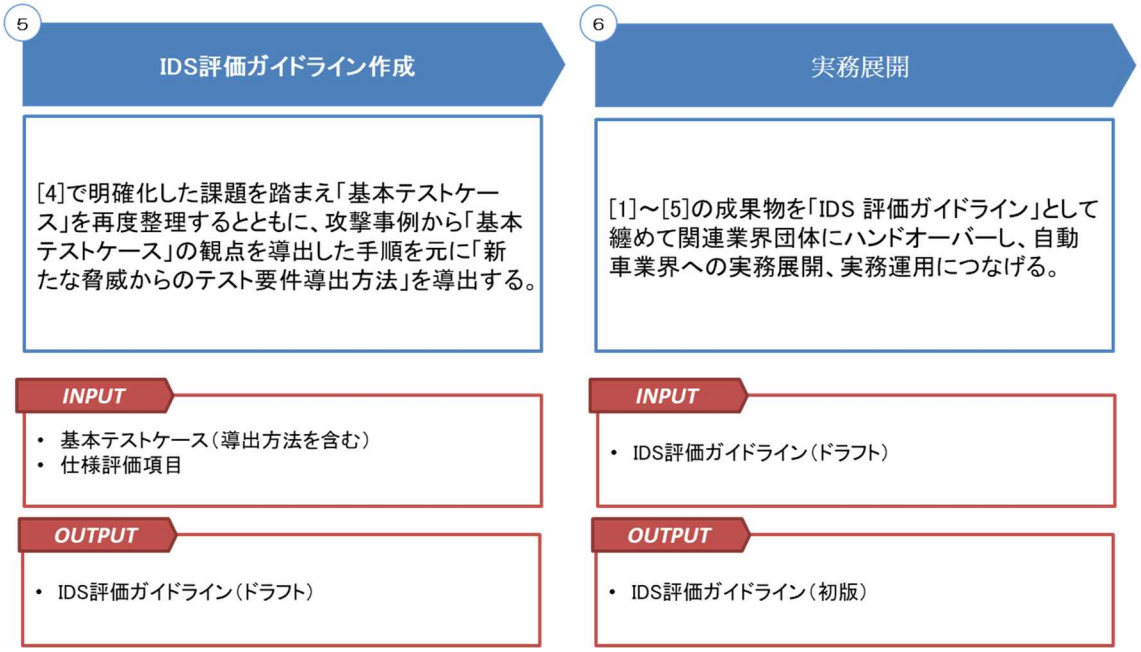



図　3-8　アプローチ詳細（３）

## 3.4.　IDS 基本機能の要素調査・検討

### 3.4.1. 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。

| | 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 3-9 事例調査、分析件数

以下に分析対象とした事例概要および分析内容について示す。

| Tesla Model S/X に対する攻撃事例 |
|---|
| 2018年3月以前に製造された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 Wi-Fi 接続時のバッファーオーバーフローの脆弱性を悪用し、HU を攻撃者の Wi-Fi AP に接続させ、TCP23 番ポートのサービスを利用することができた。<br>https://keenlab.tencent.com/en/2020/01/02/exploiting-wifi-stack-on-tesla-model-s/<br>https://blog.lookout.com/jp/%E3%83%86%E3%82%B9%E3%83%A9-model-s%E3%81%AE%E3%83%8F%E3%83%83%E3%82%AD%E3%83%B3%E3%82%B0-%E3%81%9D%E3%81%93%E3%81%A7%E5%BE%97%E3%81%9F%E7%99%BA%E8%A6%8B%E3%81%A8%E6%95%99%E8%A8%93 |

表 3-2 （参考）Tesla Model S/X に対する攻撃事例の分析

| # | 手順 | 攻撃元 | 攻撃対象 | Tactics (ATT&CK) | Techniques (ATT&CK) | 発生する可能性のあるイベント |
|---|---|---|---|---|---|---|
| 1 | Wi-Fi チップのファームウェアを解析する | 同種の部品 | 同種の部品 | Analyze hardware/software security defensive capabilities | Analyze hardware/software security defensive capabilities | N/A |

| # | 手順 | 攻撃元 | 攻撃対象 | Tactics (ATT&CK) | Techniques (ATT&CK) | 発生する可能性のあるイベント |
|---|---|---|---|---|---|---|
| 2 | Wi-Fi AP－Wi-Fi チップ間の通信を解析する | 同種の部品 | 同種の部品 | Technical Information Gathering | Conduct passive scanning | N/A |
| 3 | 攻撃者の Wi-Fi AP を近くに配置する | 通信経路 | 通信経路 | Network Effects | Rogue Wi-Fi Access Points | N/A |
| 4 | バッファーオーバーフローの脆弱性を利用するペイロードを作成する | N/A | N/A | Build Capabilities | Create custom payloads | N/A |
| 5 | 車両が Wi-Fi 接続している Wi-Fi AP に DEAUTH メッセージを送信する | 攻撃者のデバイス | 通信経路 | Initial Access | Exploit via Radio Interfaces | N/A |
| 6 | （車両が AP に再接続する） | N/A | N/A | N/A | N/A | N/A |

| # | 手順 | 攻撃元 | 攻撃対象 | Tactics (ATT&CK) | Techniques (ATT&CK) | 発生する可能性のあるイベント |
|---|---|---|---|---|---|---|
| 7 | 車両に細工をした Action Frame を送信する | 攻撃者のデバイス | 通信経路 | Initial Access | Exploit via Radio Interfaces | N/A |
| 8 | バッファーオーバーフローの脆弱性を利用して Wi-Fi チップで任意のコードを実行する | 通信経路 | 入口 ECU | Execution | Exploitation for Client Execution | バッファーオーバーフロー |
| 9 | 攻撃者の Wi-Fi AP に接続させる | 通信経路 | 入口 ECU | Network Effects | Rogue Wi-Fi Access Points | 規定外の Wi-Fi AP への接続 |
| 10 | Wi-Fi NW に公開している 23 番ポートにアクセスして公開しているプログラムを不正に実行する | 通信経路 | 入口 ECU | Lateral Movement | Exploit Public-Facing Application | N/A |

| # | 手順 | 攻撃元 | 攻撃対象 | Tactics (ATT&CK) | Techniques (ATT&CK) | 発生する可能性のあるイベント |
|---|---|---|---|---|---|---|
| 11 | 23 番ポートで公開されているサービスを実行する | - | 入口 ECU | Impact | N/A | N/A |

| Mercedes-Bentz E クラスに対する攻撃事例 |
|---|
| 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ーに接続させ、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。<br>https://i.blackhat.com/USA-20/Thursday/us-20-Yan-Security-Research-On-Mercedes-Benz-From-Hardware-To-Car-Control.pdf |

表 3-3 （参考）Mercedes-Bentz E クラスに対する攻撃事例の分析

| # | 手順 | 攻撃元 | 攻撃対象 | Tactics (ATT&CK) | Techniques (ATT&CK) | 発生する可能性のあるイベント |
|---|---|---|---|---|---|---|
| 1 | TCU のファームウェアの内容を解析する | N/A | 同種の部品 | Technical Weakness Identification | Analyze hardware/software security defensive capabilities | N/A |
| 2 | ECU から APN の情報とクライアント証明書を入手する | 物理接続 | 入口 ECU | Technical Information Gathering | Discover target logon/email address format | N/A |

| # | 手順 | 攻撃元 | 攻撃対象 | Tactics (ATT&CK) | Techniques (ATT&CK) | 発生する可能性のあるイベント |
|---|---|---|---|---|---|---|
| 3 | クライアント証明書を復号化する | | | Technical Information Gathering | 秘密情報を復号する | N/A |
| 4 | 車両の eSIM を取り出す[new] | 物理接続 | 入口 ECU | Initial Access | 車両の部品を取り出す | N/A |
| 5 | （eSIM 経由で）OEM のバックエンドサーバーにアクセスする | eSIM | バックエンドサーバー | Network Effects | Rogue Cellular Base Station | N/A |
| 6 | バックエンドサーバーから（eSIM に対応した車両ではなく）他の車に対して“remote services”コマンドを送信する | バックエンドサーバー | 入口 ECU | Lateral Movement | Remote Services | （認証エラー）※そもそもこの事例では認証していなかったとの記載があるため、認証エラーは発生しなかったはず |
| 7 | MCU 経由で CAN メッセージを送信する | 入口 EU | ボディ系 ECU | Lateral Movement | CAN メッセージを送信する（CAN コントローラの制御不可） | 走行状態と矛盾するタイミングでの基本動作には影響しない制御メッセージの送信 |

| # | 手順 | 攻撃元 | 攻撃対象 | Tactics (ATT&CK) | Techniques (ATT&CK) | 発生する可能性のあるイベント |
|---|---|---|---|---|---|---|
| 8 | 他人の車のドアのロック／アンロック、エンジンのスタート／停止をする | | ボディ系 ECU | Impact | 車両のリモートサービスを不正に利用する | N/A |

3.4.2. 事例から抽出した検知対象のセキュリティイベント

分析結果より、最終的にネットワークで検知すべきイベントとホストで検知すべきイベントそれぞれで計１２件のイベントを抽出した。

表 3-4　調査した事例から抽出したセキュリティイベント

| イベント発生箇所 | イベント | セキュリティイベント例 |
|---|---|---|
| ネットワーク | 車載 NW 上のコンテキスト矛盾の動作 | 走行状態と矛盾するタイミングで基本動作には影響しない制御メッセージの送信、走行状態と矛盾するタイミングでの有効な診断メッセージの送信 |
| | UDS プロトコルへの攻撃 | UDS プロトコルへの攻撃 |
| | 車載 NW への不正な機器の物理接続 | 外部機器の OBD I/F への接続 |
| | 車載 NW へのファジング攻撃 | OBD I/F からのファジング攻撃 |
| ホスト | 不正な振る舞い | 規定外のプロセスからのシステムコール・ライブラリの呼び出し |
| | 不正な外部通信 | 許可されていない車外の送信元／送信先との通信 |
| | 不正なファイルシステム操作 | 重要なファイルの属性変更（パーミッション等） |
| | 不正なアプリインストール | 規定外のアプリのインストール |

| イベント発生箇所 | イベント | セキュリティイベント例 |
|---|---|---|
| | 不正なログ | 不正なシステムログ、アプリケーションログ |
| | 規定外のエラー発生頻度 | 単位時間あたり一定回数以上の外部公開サービスへのリクエスト処理エラー |
| | 高負荷 | CPU やメモリの高負荷状態 |
| | ファームウェアの変更 | ファームウェアの変更 |

### 3.5. 仕様に基づく評価観点検討

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 3-5 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 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 |
| | 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 |

| セキュリティ機能分類 | 機能 | 項目 |
|---|---|---|
| | | 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） |

表 3-6 「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） |
| | 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） |

| 質問 | 選択肢 |
| --- | --- |
| | その他（　　） |

IDS ベンダーからの回答の総括と考察は以下の通りである。

- 検知対象のセキュリティイベントについて、これは、表 3-6 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。

## 3.6. 基本テスト項目導出・実施方法検討

### 3.6.1. 基本テストケースの定義

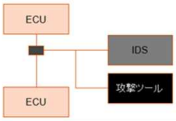
本活動では、テストの最小単位を基本テスト項目ではなく、テストケースと呼び、テストケースは複数の要件や条件などの情報が 1 セットになったものである。

表 3-7　テストケースの構成

| 項目 | | 説明 |
| --- | --- | --- |
| **テスト要件** | | 当該テストで確認したい観点が分かるようにテストの期待値を端的に記載したもの |
| **テスト方法** | **前提条件** | 当該テスト実施前に満たしておくべき条件や前提知識 |
| | **テスト環境** | 当該テストに利用する機材とそれらの接続方法 |
| | | |

| 項目 | | 説明 |
|---|---|---|
| | テスト手順 | 当該テストをするときの手順 |
| | 合否判定方法例 | 当該テスト項目に関する合否を判定するための方法。指標を基準に照らし合わせて判定する。 |

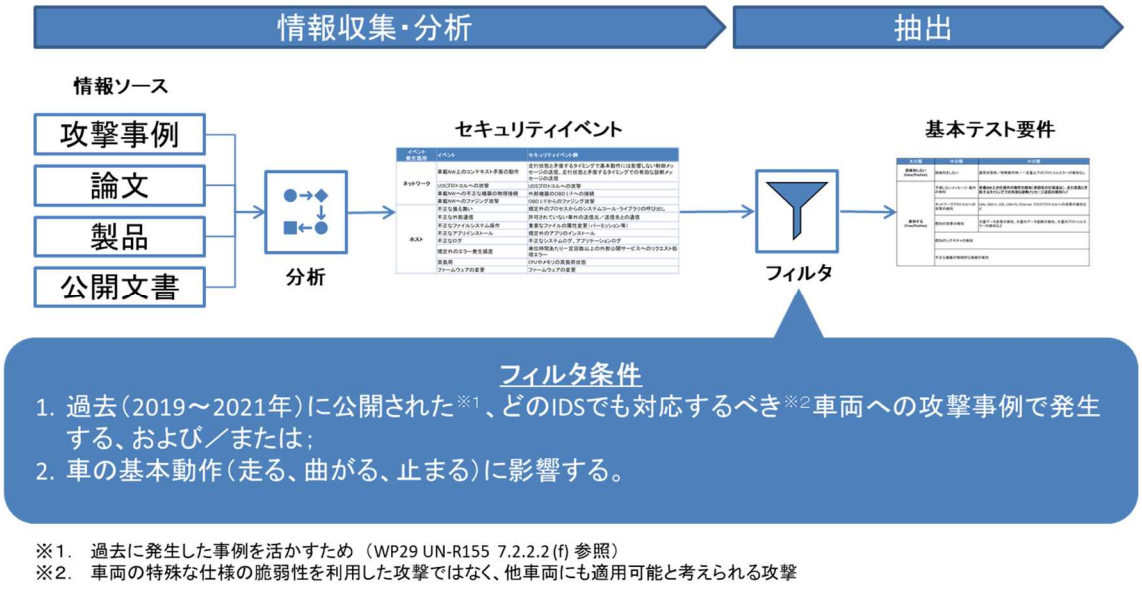
表 3-8　テストケースの記載イメージ

| 項目 | | 内容 |
|---|---|---|
| テスト要件 | | 定期的に送信されているメッセージについて、仕様外の送信周期を検知する。 |
| テスト方法 | 前提条件 | • CAN ID=xxのメッセージは100msec周期でECU Xから車速を送信する。<br>• メッセージにはMACは設定されていない。<br>• メッセージは暗号化されていない。 |
| | テスト環境 |  |
| | テスト手順 | 1. テスト環境の図のように機器を接続する。<br>2. 電源を入れる。<br>3. 攻撃ツールから正規のCAN ID=xxのメッセージを受信した10msec後に同じCANバス上に同じ内容のメッセージを1秒に1回、10メッセージ送信する。<br>4. IDSの検知ログを取り出す。<br>5. IDSのログを参照し、攻撃ツールから送信したメッセージが全て入力されていることを確認する。<br>6. IDSのログを参照し、セキュリティイベント検知状況を確認する。 |
| | 合否判定方法例 | 合格条件:<br>攻撃ツールから送信した10コのメッセージ中、10コについて、周期異常として検知されている。 |

### 3.6.2. 基本テストケースの導出方法案

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は、下記XXXの流れで抽出した。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 3-10 基本テストケースの導出方法

### 3.6.3. 基本テストケース概要（ドラフト）

NIDS 向けの基本テストケースの要件一覧を下記に示す。下記のうち、攻撃事例等から抽出、追加した要件は「車載ネットワーク上の仕様外の動作の検知」および「走行状態と矛盾するタイミングでの有効な制御・診断メッセージの検知」となる。

表 3-9 基本テストケース概要

| 大分類 | 中分類 | 小分類 |
|---|---|---|
| **誤検知しない (False/Positive)** | 誤検知をしない | 通常状態時／特殊動作時／一定量以下のプロトコルエラーの検知なし |
| **検知する (True/Positive)** | 予期しないメッセージ・動作の検知 | 車載 NW 上の仕様外の動作の検知（車固有の仕様違反）、走行状態と矛盾するタイミングでの有効な診断メッセージ送信の検知など |
| | ネットワークプロトコルへの攻撃の検知 | CAN, OBD-II, UDS, CAN-FD, Ethernet, TCP/IP プロトコルへの攻撃の検知など |
| | 既知の攻撃の検知 | 大量データ送信の検知、大量のデータ遮断の検知、大量のプロトコルエラーの検知など |

| 大分類 | 中分類 | 小分類 |
|---|---|---|
| | 既知のシグネチャの検知 | |
| | 不正な機器の物理的な接続の検知 | |

今後は、テストケースの詳細化を行い、実機検証による妥当性検証を行っていく予定である。なお、実機検証を行うための環境としては、以下の選択肢およびこれらの組み合わせ（例：シミュレーション環境＋テストベッド環境など）が考えられる。

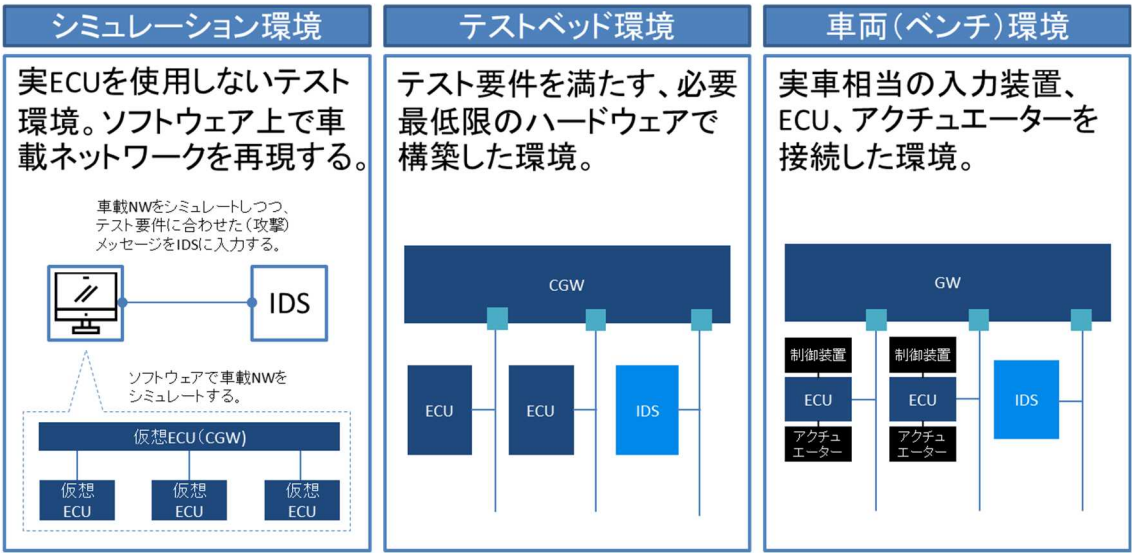



図 3-11 IDS テスト環境の種別

## 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. 4. 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、共有されているのは IT 領域の脅威インテリジェンスが中心となっている。

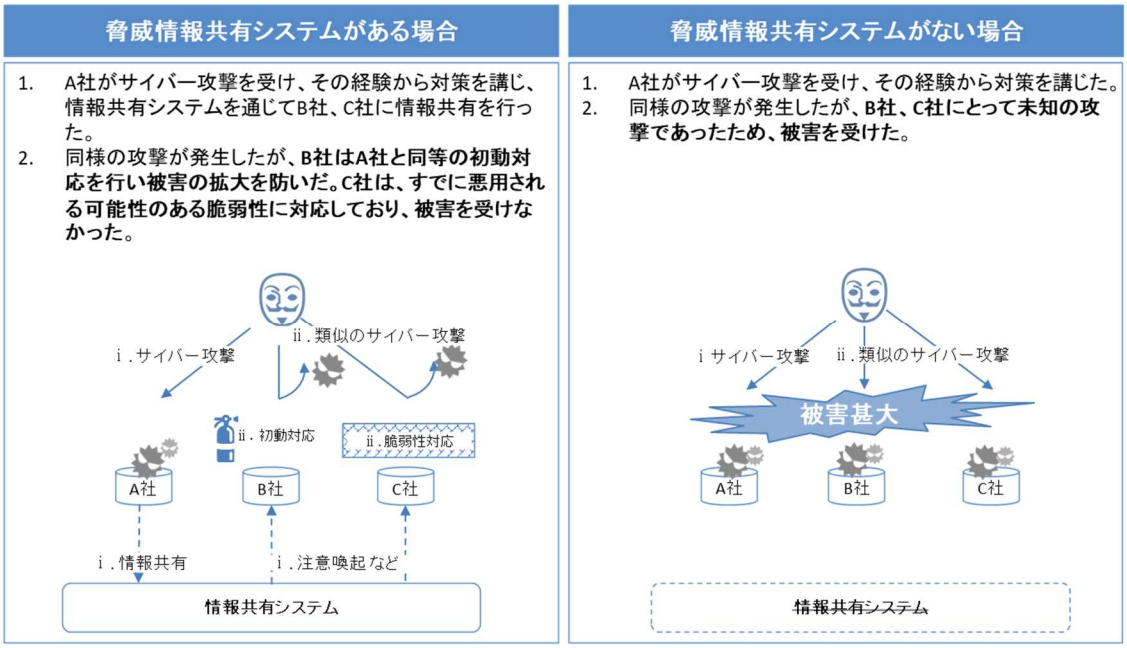



図　4-1　脅威情報共有システムのインシデント対応への効果

### 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。下記 XXX 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。

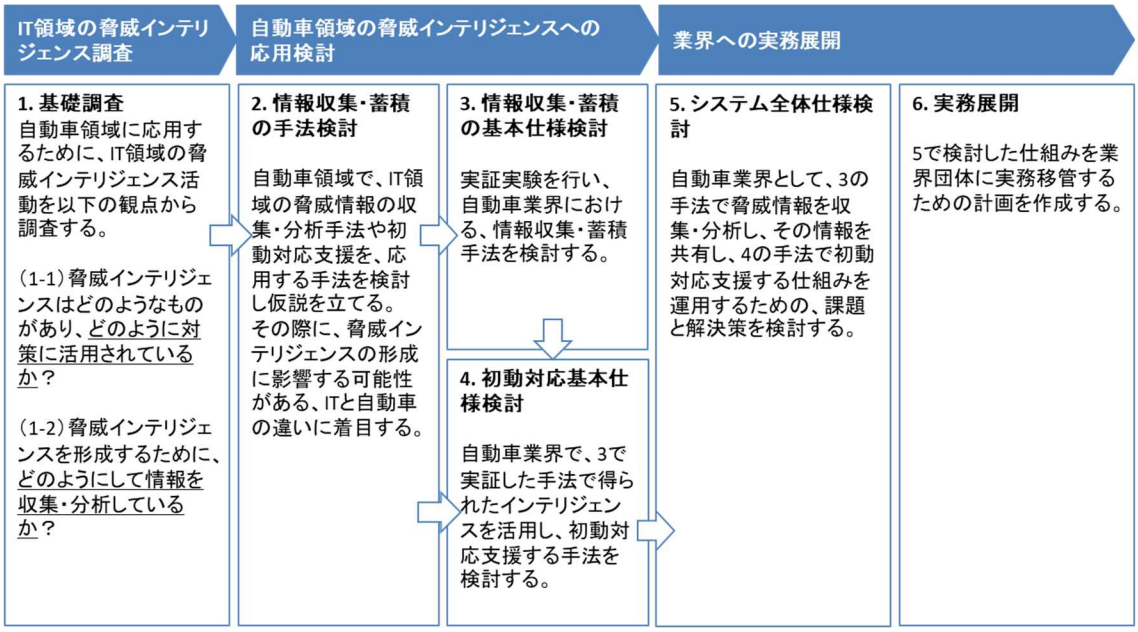



図　4-2　調査研究アプローチ概要

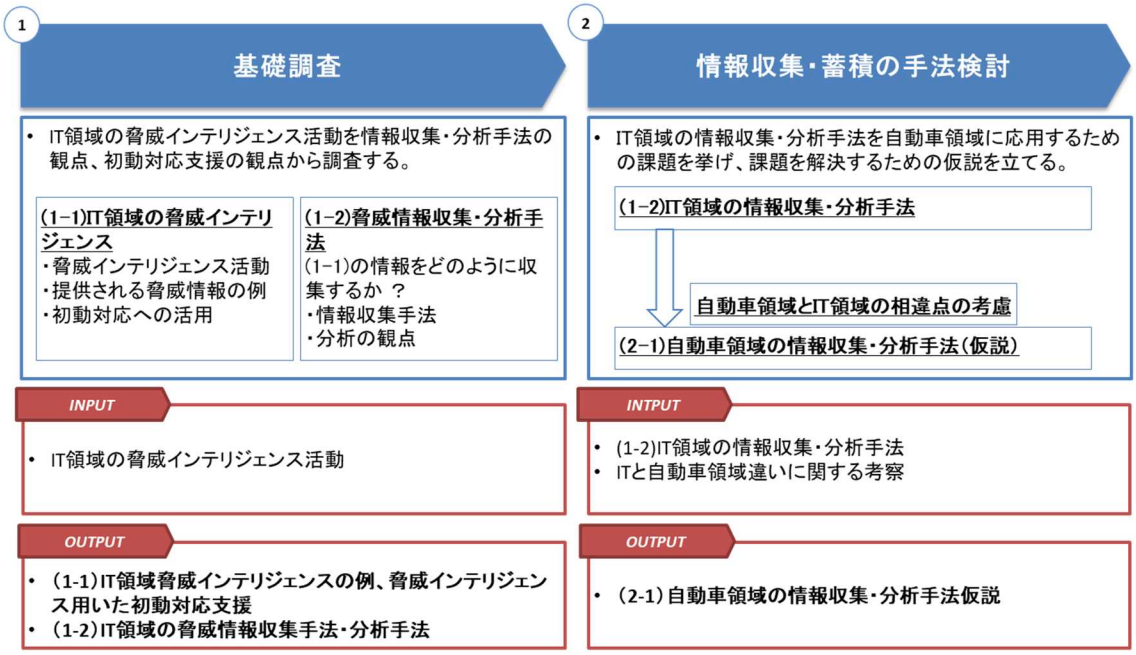



図　4-3　２０２０年度の活動アプローチ

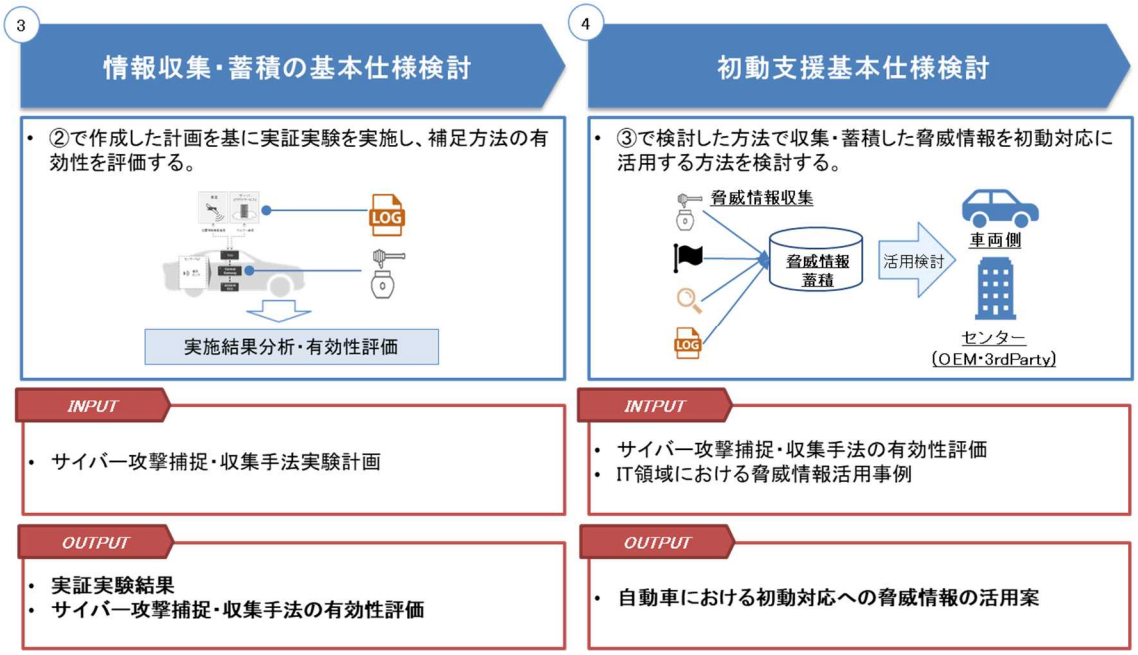



図　4-4　２０２１年度の活動アプローチ

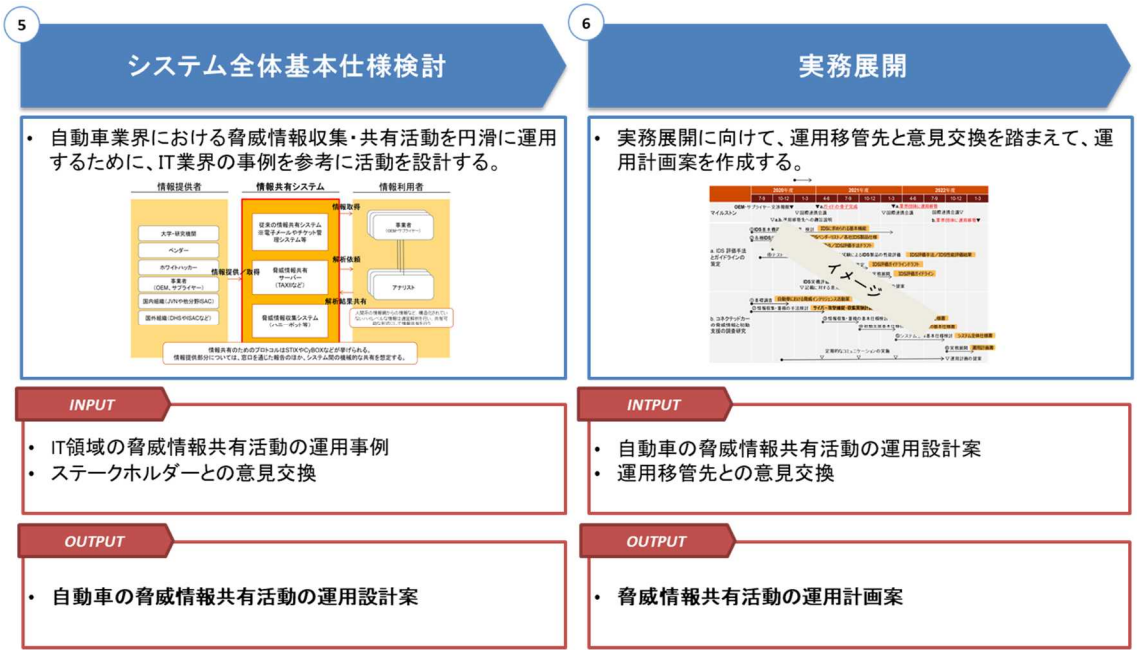



図　4-5　２０２２年度の活動アプローチ

## 4.2.　基礎調査

自動車の脅威インテリジェンスの基礎とするため、先行するIT領域の脅威インテリジェンス活動事例から、どのような脅威インテリジェンスが提供されているか、どのようにして脅威情報を収集・分析しているかを調査した。

4.2.1. 脅威インテリジェンスの定義

脅威インテリジェンスとは、脅威への対応を支援するために、収集分析された情報の事を指す。以下に各組織・機関における脅威インテリジェンスの定義を示す。

| # | 機関 | 脅威インテリジェンスの定義 | 出典 |
|---|---|---|---|
| 1 | **米国情報コミュニティ** | 情報コミュニティ※を構成する機関が保有する、以下に関わるようなインテリジェンスのこと<br>(i) 政府または民間企業の**システムまたはネットワークの脆弱性**。<br>(ii) 政府または民間企業のシステムまたはネットワークの完全性、機密性、可用性に対する脅威、またはそのようなシステムまたはネットワーク上に保存され、処理され、または通過する**情報に対する脅威**。<br>(iii) 政府機関または民間企業のシステムまたはネットワークへの**アクセスを拒否したり、劣化させたり、混乱させたり、破壊したりしようとする試み**。<br>(iv) 政府または民間事業体のシステムまたはネットワークに保存されている、処理されている、または政府または 民間事業体のシステムまたはネットワークを通過する情報を流出させる目的での**不正アクセスを含む、政府または民間事業体のシステムまたはネットワークへの不正アクセスする試み**。 | 米国サイバーセキュリティ法[*1] |
| | **（補足）** | 情報コミュニティによるインテリジェンスの定義<br>**指導者が国を守るうえで健全な意思決定を行うために**、収集、分析された情報のこと。 | 情報コミュニティ/mission[*2] |

| # | 機関 | 脅威インテリジェンスの定義 | 出典 |
|---|---|---|---|
| 2 | 米国標準技術研究所（NIST） | **意思決定プロセスに必要なコンテキストを提供するため**に収集、変換、分析、解釈、または強化された脅威情報。 | NIST SP 800-150 Guidance threat information sharing |
| 3 | UK-CERT、CPNI | 「未知の未知」を「既知の未知」に変え（脅威が存在することを知り）、「既知の未知」を「既知の既知」（脅威の性質を知る）一連のプロセス。または、そのプロセスによって生成された、**攻撃を防ぐための意思決定を支援する情報。** | 脅威インテリジェンスに関するホワイトペーパー*3 |
| 4 | MITRE 社 | サイバー攻撃者の行動を理解し予測し、**対応するためのアクションをとるために活用される情報。**<br>サイバー犯罪者の用いるマルウェア、コマンド、特定の攻撃グループが用いる技術など、様々な形態をとる。 | MITER 社脅威インテリジェンス*4 |
| 5 | ガートナー社 | IT または情報資産に対する既存または新たな脅威または危険性に関する、コンテキスト、メカニズム、指標、影響、および実用的なアドバイスを含む、証拠に基づく情報。情報は、**脅威または危険性に対して、情報を受け取る者がどう対応するか意思決定するために活用される。** | ガートナー社、脅威インテリジェンスサービス調査*5 |

*1. https://www.govinfo.gov/content/pkg/BILLS-112hr3523rfs/pdf/BILLS-112hr3523rfs.pdf

*2. https://www.intelligence.gov/mission

*3. https://www.foo.be/docs/informations-sharing/Threat-Intelligence-Whitepaper.pdf

*4. https://www.mitre.org/capabilities/cybersecurity/cyber-threat-intelligence

*5. https://www.gartner.com/reviews/market/security-threat-intelligence-services

### 4.2.2. IT 領域の脅威インテリジェンス

IT 領域の脅威インテリジェンス活動は、国・業界団体、民間企業などの組織により、様々な目的をもって行われている。本研究の「初動対応支援」に類似する目的を持つ脅威活動に焦点を当て、提供される情報を調査した。

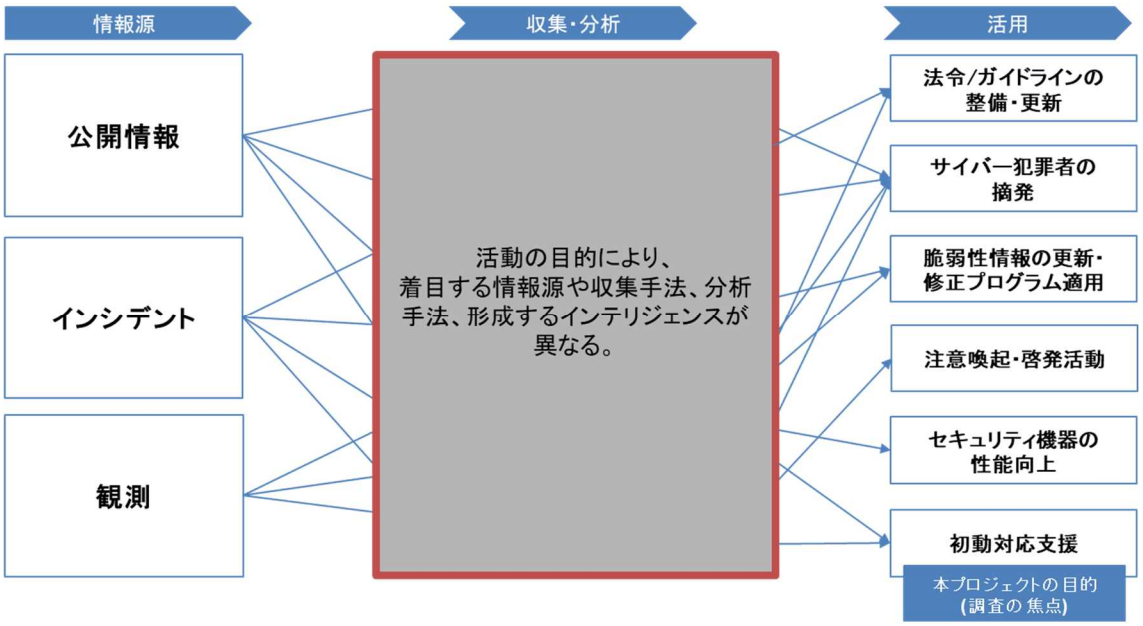



図 4-6 脅威インテリジェンスの調査方針

脅威インテリジェンスを構成する主な情報として、５つの情報を上げることができる。

| # | 情報 | 定義・概要 |
|---|---|---|
| 1 | インジケーター | サイバー攻撃によって安息された具体的な事象(マルウェアハッシュや IP アドレス、URL、ドメイン情報など) |
| 2 | TTPs (戦術／Techniques、戦略／Tactics、手順／Procedures) | 攻撃者の意図、ふるまいや手口を使用するリソース。攻撃対象などの観点から説明したもの。 |
| 3 | セキュリティアラート | システムの脆弱性情報やエクスプロイト情報 |
| 4 | インテリジェンスレポート | 組織の状況認識を高めるための、脅威関連情報を記述したドキュメント |
| 5 | ツールコンフィギュレーション | １～４で得られた情報の活用を支援するためのツール設定 |

続いて、上記の脅威インテリジェンスがどのように活用されているか、NIST の CSF (Cyber Security Framework) で定義される「特定」、「防御」、「検知」、

および「対応」と「復旧」それぞれのフェーズでの活用例を整理した。

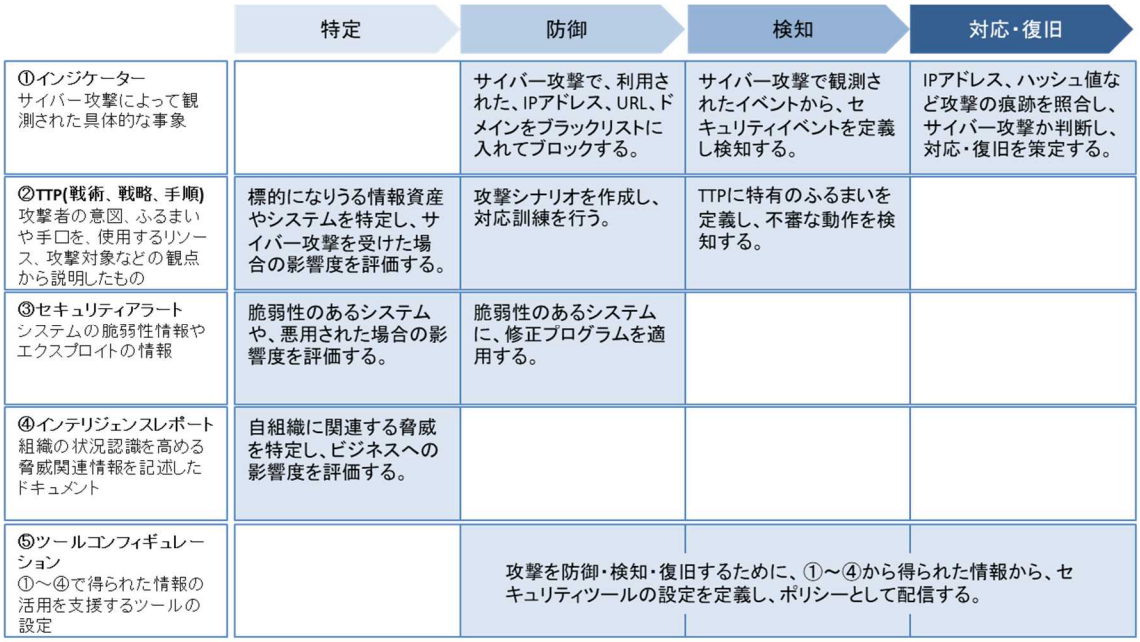



図 4-7 CSF ベースの脅威インテリジェンス活用例

### 4.2.3. （参考）脅威インテリジェンス活動一覧（国・業界団体）

| # | 国 | 活動 | 活動概要 |
|---|---|---|---|
| 1 | 日本 | CEPTOAR<br>-内閣サーバーセキュリティセンター(NISC) | 重要インフラサービス障害の未然防止、発生時の被害拡大防止・迅速な復旧および再発防止のため、NISC 等から提供される情報を重要インフラ事業者等に提供し関係者間で共有。 |
| 2 | 日本 | J-CSIP<br>-情報処理推進機構(IPA) | サイバー攻撃による被害拡大防止のため、重工、重電等、重要インフラで利用される機器の製造業者を中心に情報共有し早期に対応。 |
| 3 | 日本 | ICT-ISAC | 多様な事業者が情報収集・分析および対応について情報共有し、業界の枠を超えて連携・協調する組織として脅威に対処。脅威情報の収集・調査・分析・共有のほか人材育成活動、サイバー演習を提供。 |

| # | 国 | 活動 | 活動概要 |
|---|---|---|---|
| 4 | 日本 | 金融 ISAC | 日本の金融機関によるサイバーセキュリティに関する情報共有、分析、演習を実施。会員専用ポータルにて脆弱性情報を提供。米国 FS-ISAC と情報共有。複数の WG が存在。 |
| 5 | 日本 | 電力 ISAC | 電気の安定供給に重要な役割を担う事業者間のサイバーセキュリティに関する脅威情報等を共有と、迅速に対応を目的として設立。 |
| 6 | 日本 | J-AUTO-ISAC<br>-日本自動車工業会 | サイバーセキュリティインシデントに関する情報を共有するため、日本自動車工業会(JAMA)の WG として発足。2021 年度に、JAMA から独立予定。 |
| 7 | 英国 | Cyber security Information Sharing Partnership (CiSP)-National Cyber Security Centre | 英国内でのサイバー攻撃の影響を軽減するために、脅威情報をリアルタイムで交換する仕組み。情報共有システムは将来的には STIX/TAXII を採用する見込み。 |
| 8 | 米国 | Automated Indicator Sharing (AIS)<br>-米国国土安全保障省(DHC) | 脅威情報のリアルタイム共有システム。侵入検知後すぐにすべてのパートナーとリアルタイムで共有。情報は STIX 形式で表現し、TAXII プロトコルで共有。※CISCP の一環として提供。 |
| 9 | 米国 | Cyber Information Sharing and Collaboration Program(CISCP) -米国国土安全保障省(DHC) | 米国とその重要インフラ事業者のサイバーレジリエンスと防御力を強化することを目的とした活動。 |
| 10 | 米国 | Enhanced Cybersecurity Services (ECS)<br>-米国国土安全保障省(DHC) | 米国拠点法人や自治体を保護する侵入防止システム。DHS が検知した脅威を即時に展開しネットワークを保護。 |

| # | 国 | 活動 | 活動概要 |
|---|---|---|---|
| 11 | 米国 | Information Sharing and Analysis Centers -National Council of ISACs | サイバーおよび物理的な脅威やその緩和策を、ISAC 間、政府、民間セクターのパートナーと共有するためのフォーラムを提供。情報共有は様々な頻度で行われ、演習の場も提供。 |
| 12 | 米国 | Information Sharing and Analysis Organization -ISAO Standards Organization | サイバーセキュリティリスク、インシデント、ベストプラクティスの情報共有や分析にガイドラインと標準を作成する機関。脅威インテリジェンス標準「ISAO 300-2: AUTOMATING CYBER THREAT INTELLIGENCE SHARING」を策定。 |
| 13 | 米国 | Global Resilience Federation (GRF) | FS-ISAC が他の産業セクターにレポートを共有したことから始まり、産業部門横断的な情報共有組織として独立。脅威情報共有ツール（eXchange）を加盟組織に提供。 |
| 14 | 欧州 | European Network for Cyber Security | 欧州の送電網と電力インフラのセキュリティを保護するため、メンバーとパートナーと専門家で、セキュリティ要件の定義やテストを実施。自動車に関しては、EV や充電設備のセキュリティ要件を定義。 |
| 15 | 欧州 | EE-ISAC | 欧州のエネルギーインフラのレジリエンスとセキュリティを強化するために情報共有し、脅威・脆弱性・インシデント・オペレーション・オポチュニティについて協力し分析するためのフォーラムを提供。 |
| 16 | 欧州 | European FI-ISAC | EU の機関の情報共有・分析を目的に組織された。EU 各国の金融部門、CERT（国家レベルの）、法務・執行機関の代表のほか、ENISA、Europol、欧州中央銀行、EPC、欧州理事会が参加。 |
| 17 | 欧州 | Cyber Information and Intelligence Sharing Initiative - European Central Bank | 欧州連合市民の金融資産を保護するため、サイバー脅威情報を交換する仕組み。 |

| # | 国 | 活動 | 活動概要 |
|---|---|---|---|
| 18 | 独国 | UP KRITIS | ドイツ国内の重要インフラをサイバー攻撃から保護するための、重要インフラ事業者と通信事業者の間のイニシアティブ。 |
| 19 | 独国 | Alliance for Cyber Security | ドイツ国内でのサイバー攻撃に対する防御力を高めるために、情報交換する仕組み。 |
| 20 | 独国 | Cyber Security Sharing and Analytics | メンバー企業で発生したインシデントや脅威、脆弱性に関する専門家による発信。 |
| 21 | 仏国 | French Information Security Club | 情報セキュリティに関するベストプラクティスの収集と伝達、コンファレンスを実施。 |

### 4.2.4. （参考）脅威インテリジェンス活動一覧（企業）

| # | 事業者名 | サービス名 |
|---|---|---|
| 1 | Anomali | ● Anomali ThreatStream<br>● Match<br>● Lens+ |
| 2 | Blueliv | ● Threat Intelligence Services |
| 3 | Cofense | ● Cofense Intelligence |
| 4 | CrowdStrike | ● Falcon X |
| 5 | Cyberint | ● Cyberint Cyber Intelligence Suite |
| 6 | Cyware Labs | ● Cyber Fusion Suite, Cyware Threat Intelligence eXchange (CTIX) |
| 7 | DarkOwl | ● DarkOwl |
| 8 | DigitalShadows | ● SearchLight |
| 9 | Domain Tools | ● Iris Investigation Platform<br>● DomainRisk Score |
| 10 | ElectricIQ | ● ElectricIQ Platform<br>● ElectricIQ Fision Center |
| 11 | FireEye | ● Threat Intelligence Subscriptions<br>● Intelligence Capability<br>● Development<br>● Digital Threat Monitoring |
| 12 | Flashpoint | ● Flashpoint Intelligence Platform<br>● Flashpoint Alerting |

| # | 事業者名 | サービス名 |
|---|---|---|
| 13 | VirusTotal (Google) | ● VirusTotal |
| 14 | Group-IB Threat Intelligence | ● Group-IB |
| 15 | IBM Security | ● IBM QRadar Vulnerability Manager<br>● IBM XForce Incident Response and Intelligence Services (IRIS)<br>● IBM X-Force Exchange |
| 16 | Intel 471 | ● Adversary Intelligence<br>● Malware Intelligence |
| 17 | IntSights | ● Threat Command<br>● Threat Intelligence Platform<br>● Vulnerability Risk Analyzer<br>● Threat Third Party |
| 18 | Kaspersky | ● Kaspersky Threat Intelligence |
| 19 | KELA | ● RADARK<br>● DARKBEAST<br>● Intelligence SOC |
| 20 | LookingGlass Cyber Solutions | ● scoutPRIME<br>● scoutSHIELD<br>● scoutTHREAT<br>● Managed Threat Intelligence |
| 22 | Palo Alto Networks | ● Cortex XSOAR (formerly Demisto)<br>● AutoFocus<br>Unit 42 |
| 23 | PhishLabs | ● Phishing Threat Indicator Feed<br>● Digital Risk Protection |
| 24 | Proofpoint | ● Emerging Threats Intelligence |
| 25 | RecordedFuture | ● Recorded Future for Threat Intelligence<br>● Threat Intelligence Platform |
| 26 | ReversingLabs | ● Explainable Threat Intelligence |

| # | 事業者名 | サービス名 |
|---|---|---|
| 27 | RiskIQ | ● Illuminate<br>● RiskIQ Security Intelligence Services |
| 28 | Secureworks | ● Attacker Database<br>● Countermeasures<br>● Enterprise Brand Surveillance<br>● Global Threat Intelligence<br>● Threat Intelligence Support |

4.2.5. 脅威情報共有活動の調査

脅威情報を共有するための活動・仕組みは、一部産業においては、インシデントの発生防止や適切な初動対応など、共通の目的を持つことで企業横断的に行われている。本活動では、複数の企業や組織が業界横断的に脅威情報を共通する活動を支える仕組みを「情報共有システム」と呼ぶ。

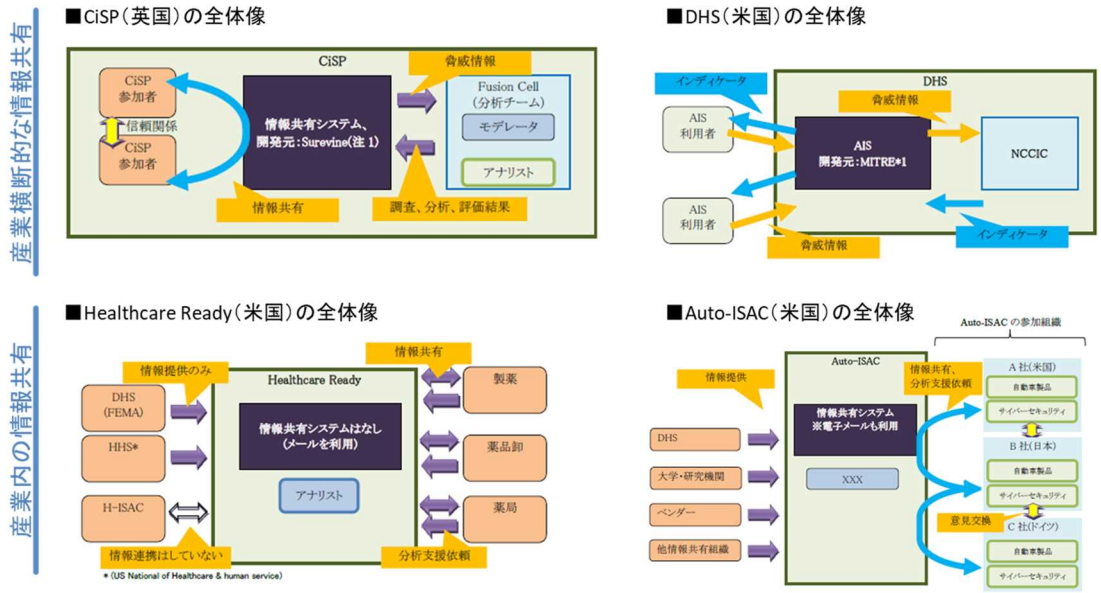



図 4-8 脅威情報共有システムの例

（出典）戦略的イノベーション創造プログラム（ＳＩＰ）重要インフラ等におけるサイバーセキュリティの確保(b2)情報共有プラットフォーム技術「情報共有デザインガイド構築編」2020 年 1 月

4.2.6. IT 領域の脅威情報収集手法

IT 領域における脅威情報は、主に公開情報のサーベイ、インシデントレポー

ト、対象となるネットワークやシステムの観測・実験を情報源としている。これらの代表的な収集例を以下に示す。

表 4-1 脅威情報の収集手法例

| 方法 | 概要 | 実施事例 |
|---|---|---|
| インターネット定点観測 | インターネット上の通信を定点観測することで、サイバー攻撃の大局的な傾向を把握する方法。 | • NICTER（NICT）<br>• TSUBAME（JP-CERT/CC） |
| ハニーポット | 攻撃を受けることを意図したシステムをインターネットに公開し、攻撃者のアクセス情報を収集する方法。<br>本物のシステムを守るために代わり攻撃を受ける、おとりとして活用される場合もある。 | • MITF（IIJ社）<br>• A IoT Malware Story（Kaspersky社）<br>• コネクテッドホーム実験室（横浜国立大学） |
| CTF | システムを模した環境に、ホワイトハッカーに意図的に攻撃を仕掛けてもらい、情報を収集する方法。<br>攻撃の目標（Flag）を設定し、得点を争う（CTF）方式のほか、疑似的な攻撃を試す遊び場（プレイグラウンド）を提供する方式もある。 | • DEFCON CTF<br>• SECCON |
| バグバウンティプログラム | バグの発見者に、報奨金を与える制度を設け、実際のシステムの脆弱性情報を収集する方法。 | • LINE社のBug Bounty Program<br>• HackerOne 、Sproutなどのサービス |
| OSINT収集 | 人手またはウェブクローラー、製品・サービスなどの機械的な手段で、インターネットから情報を収集する方法。<br>事例やレポートのほか、自社の偽サイトや偽アプリ等、すでに起こっている脅威が発見される場合がある。 | • （多数の製品・サービスが展開されている）。 |

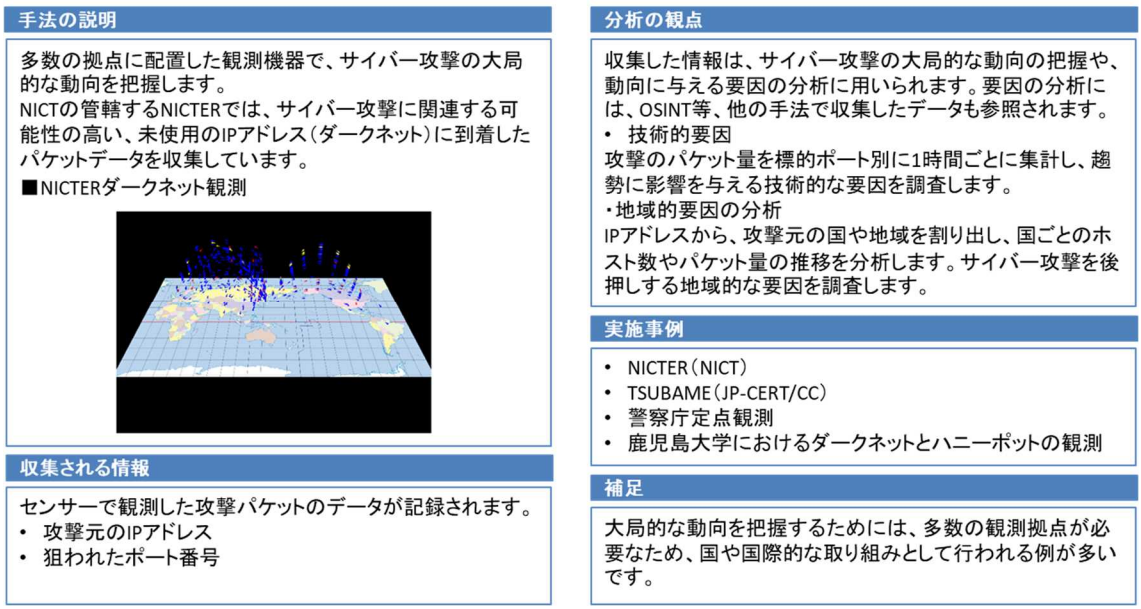



図 4-9 インターネット定点観測概要・事例

（出典） https://www.nicter.jp/

**手法の説明**

ハニーポットはどの程度、システム挙動をするかによって、低対話型と高対話型の2種類に分類されます。

■低対話型ハニーポット
サービス・製品を模した動きをするソフトウェアを用いて、攻撃者のアクセス情報を収集します。詳細まで捕捉できない場合がありますが、安価に導入できます。

■高対話型ハニーポット
実際のサービスや製品をインターネットに公開し、攻撃者のアクセス情報を収集します。

**分析の観点**

特定のシステムを狙うサイバー攻撃の動向の把握に役立てられます。
また、囮のシステムで、サイバーキルチェーンの後半に到達するまで攻撃者を泳がせることができ、攻撃者の目的や、攻撃に利用するツール、悪用される脆弱性、など、TTPを明らかにすることができます。

**実施事例**

- MITF（IIJ社）
- A IoT Malware Story（Kaspersky社）
- コネクテッドホーム実験室（横浜国立大学）
- 鹿児島大学におけるダークネットとハニーポットの観測

**得られる情報**

ハニーポットが攻撃を受けた際に発生するイベントを記録します。記録するイベントは以下のような例があります。
・ホスト上のイベント（ファイルシステムへのアクセス、レジストリへのアクセス、プロセスの制御、ネットワークアクセス）
・ネットワーク上のイベント（攻撃コード・ペイロードの送信、マルウェアのダウンロード）

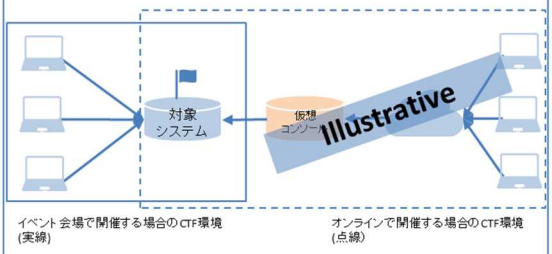
**補足**

すべてのイベントを記録すると、ログが膨大になり、分析が困難になります。あらかじめ攻撃に関係のないイベントは記録から除外する必要があります。
低対話型ハニーポットのソフトウェアの中には、ロギング機能も備わっているものがあり、攻撃に関連するイベントのみが記録されるようにあらかじめ設定されています。

図　4-10　ハニーポット概要・事例

**手法の説明**

CTF（Capture the flag）は、システムを模した環境に、課題の答えとなるFlagを見つけ出し、得点を競う競技のことです。




**得られる情報**

情報収集目的のCTFでは、ハニーポットと同様に攻撃を受けた際に発生するイベントを記録します。
また、参加したホワイトハッカーやセキュリティベンダーから、識別された脅威についてレポートを受けます。

**分析の観点**

ホワイトハッカーが識別した脅威について分析したレポートが受けられます。
また、CTF参加者が、設定されたFlagに到達するまでに用いた、攻撃ツールや悪用された脆弱性など、TTPを明らかにすることができます。

**実施事例**

- DEFCON CTF
- SECCON

**補足**

攻撃者を募集し、攻撃の目標を設定することで、効率よくTTPに関する情報を収集することができます。
CTFはセキュリティ人材育成や採用目的で開催される場合もあります。
特定の目標を設けず、疑似的な攻撃を試す場（プレイグラウンド）を提供する方式もあります。

図　4-11　CTF 概要・事例

**手法の説明**

ウェブサイトの脆弱性を発見し報告した者に、報奨金を与える制度を設け、情報を収集する手法です。

■バグバウンティプログラムの例

**得られる情報**

また、参加したホワイトハッカーが発見した脆弱性についてレポートを受けます。

**分析の観点**

参加したホワイトハッカーが発見した脆弱性や悪用の可能性について分析したレポートを受けます。

**実施事例**

企業が単独で制度を公開し報告者を募る例と、マッチングサービスを活用する例があります。
【自社で募集する例】 LINE社、サイボウズ社 など
【マッチングサービスの例】HackerOne、Sprout など

**補足**

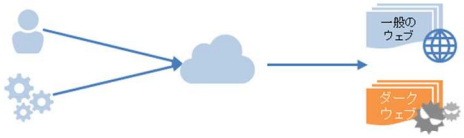
CTFと類似していますが、発見したバグに対する成功報酬である点と、稼働中のシステムで外部に公開されているものが対象である点が異なります。
不特定のホワイトハッカーが稼働中のシステムで調査を行うため、過度な負荷がかかる調査を禁止する、対象のドメイン、アプリを限定するなど、事前の条件設定が必要になります。
開発者が意図的に脆弱性を残して、報奨金を受け取るなど、不正を防止するため、プログラムへの参加条件設定が必要になります。

図 4-12 バグバウンティプログラム概要・事例

（出典）https://bugbounty.linecorp.com/ja/

**手法の説明**

ニュース、ソーシャルメディア、商用データベース、機密指定されていない情報を、人手、クローラーなどで収集します。
公開レポートやホワイトペーパーなどのほか、whoisクエリで入手できるドメインの登録情報や、一般的なブラウザでアクセスできない、ダークウェブも情報源になりえます。




**得られる情報**

インシデント事例やカンファレンス情報や等の一般的な情報のほか、組織がすでに直面している脅威が分かります。
- インシデント事例
- カンファレンス情報
- 脆弱性情報
- 偽サイトや偽アプリ
- 漏えいした情報
- 漏洩したID・パスワード
- マルウェア作成ツール

**分析の観点**

インジケーター、TPP、セキュリティアラート、インテリジェンスレポートなど、対策に活用できる情報が手に入ります。
また、ハニーポットなど、他の手法で収集したデータと組み合わせることで、攻撃者の目的やTTPの分析に役立てられます。

**実施事例**

個々の組織で実施するほか、様々なツールやサービスが提供されている。

**補足**

OSINTは、だれでも収集できますが、情報源が多岐にわたり、見逃しやノイズが発生します。
そのため、OSINTを効率よく検索できるツールや、自社に関連性の高い情報を選び配信するサービスが、様々なベンダーから提供されています。

図 4-13 OSINT 概要・事例

表 4-1 で示した情報から、攻撃者の手口をどの程度まで補足できるかをサイバーキルチェーンに従って整理した図を以下に示す。なお、サイバーキルチェーンにおける武器化（Weaponization）は、マルウェアやエクスプロイトキットを開発する段階を指していることから、表 4-1 で示した手法では補足できない（使用されたマルウェア（亜種）やエクスプロイトキットを識別するという観点においては、この限りではない）。

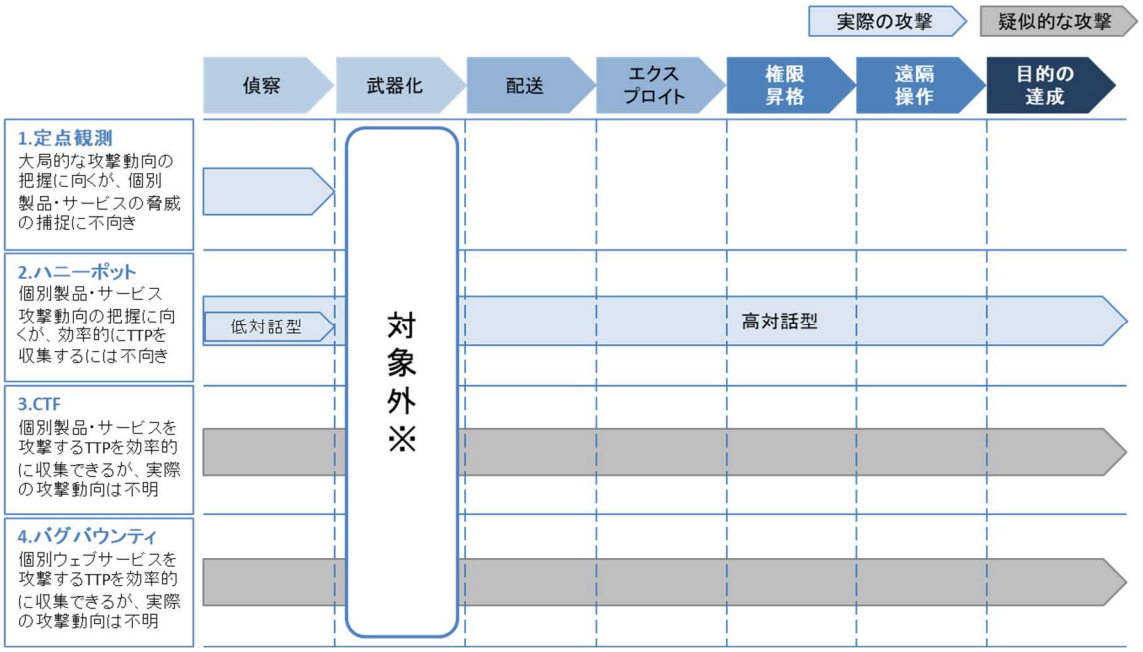



図 4-14 脅威情報収集手法と、サイバーキルチェーンにおける対応関係の考察

### 4.2.7. IT 領域での情報の分析手法

識別したサイバー攻撃や脆弱性を評価・分析するためにフレームワークが用いられる。ここでは、IT 領域で用いられる脅威分析フレームワークと評価基準を調査し概要を整理した。

また、攻撃者の手口について考察を得るために、特定した攻撃者の資源（マルウェア、ドメインなど）について考察を加える手法を調査し、概要と得られるデータ、分析の観点について整理した。

表 4-2 脅威分析のフレームワーク

| 手法 | 概要 |
|---|---|
| Cyber kill chain | 攻撃者が標的を決定し、実際に攻撃し目的を達成するまでの一連の行動を順に、「偵察」、「武器化」、「デリバリー」、「エクスプロイト」、「インストール」、「C&C」、「目的の実行」の 7 フェーズに分類、サイバー攻撃の構造を把握し、切断することで防衛力を高める考え方。 |
| STRIDE | サイバー攻撃を 6 種類（なりすまし、改ざん、否認、情報漏えい、サービス拒否、権限昇格に分類し、システムの開発段階で適切な防御策を講じるための分析手法 |

| 手法 | 概要 |
| --- | --- |
| TRIKE | リスクマネジメントの観点からのセキュリティ監査のために用いられる脅威モデルのフレームワーク。技術者とその他の関係者が共通の観念を持つことを目的としている。 |
| PASTA | Process for Attack Simulation and Threat analysis の頭文字。情報資産ベースの脅威モデリングを実施するためのフレームワーク。 |

表 4-3 脆弱性の評価・分類手法

| 手法 | 概要 |
| --- | --- |
| CVSS | 共通脆弱性評価システム。情報システムの脆弱性に対するオープンで汎用的な評価手法であり、ベンダーに依存しない共通の評価方法。基本評価基準、現状評価基準、環境評価基準 3 つの基準がある。 |
| CWE | 共通脆弱性タイプ一覧（Common Weakness Enumeration）ソフトウェアのセキュリティ上の弱点を識別するための共通の基準。 |

4.2.8. IT 領域での情報の蓄積手法

識別した脅威を体系的に記述するための標準記述様式が提案されている。様式化された脅威情報は、組織でも蓄積されるが、国や非営利組織が、誰でもアクセスできるデータベースに蓄積される例もある。ここでは、IT 領域で用いられる、標準記述様式と公的に利用可能なデータベースの概要を調査した。

表 4-4 脅威情報の記述方式例

| 手法 | 概要 |
| --- | --- |
| STIX | サイバー空間における脅威やサイバー攻撃の分析、サイバー攻撃に関する情報を共有することなどを目的に、関連する情報を標準化された方法で記述するために開発された表記方法。 |
| CybOx | サイバー攻撃によって観測される事象を記述するための仕様。 |

表 4-5 サイバー攻撃 TTPs の分類方式例

| 手法 | 概要 |
| --- | --- |
| CAPEC | 既知の脆弱性を悪用するために攻撃者が採用した既知の攻撃パターンを網羅的に分類・体系化したもの。CWE と紐づけられている。 |
| ATT&CK | CVE をもとに、脆弱性を悪用した実際の攻撃を戦術と技術または手法の観点で分類したナレッジベース。 |

表 4-6 （脅威情報の一部として）脆弱性情報のデータベース例

| データベース | 概要 |
|---|---|
| NVD | NIST が運営する脆弱性のデータベース。CVE で識別された脆弱性の詳細情報を提供する。 |
| JNV | Japan Vulnerability Notes の略。日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイト。<br>CVE で識別された脆弱性に加えて、日本国内に流通している製品の脆弱性が追加されている。 |
| JVN iPedia | 国内外で公開された脆弱性を提供するポータルサイト。日々発見される脆弱性対策情報を適宜収集・蓄積することに焦点がある。 |

## 4.3. 情報収集・蓄積の手法検討

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も実証実験を行う。その準備として、コネクテッドカーの車載機器やサービスを調査し、前節で調査した情報収集の手法を自動車にも応用可能か検討する。

### 4.3.1. 脅威が観測され得るサービス・機器

#### 4.3.1.1. インターネット接続を伴うサービス・機器

表 4-7 OEM が提供するコネクテッドサービスの国内提供状況

| # | OEM | サービス名 | 国内向け提供状況 | 備考 |
|---|---|---|---|---|
| 1 | いすゞ自動車工業株式会社 | MIMAMORI | 提供済 | |
| 2 | 川崎重工業株式会社 | （なし） | 未提供 | 自動車は 2 輪のみ |
| 3 | スズキ株式会社 | スズキコネクト | 未提供 | インド市場で先行 |
| 4 | 株式会社 SUBARU | SUBARU STARLINK | 提供済 | |
| 5 | ダイハツ工業株式会社 | ダイハツコネクト | 提供済 | |

| # | OEM | サービス名 | 国内向け提供状況 | 備考 |
|---|---|---|---|---|
| 6 | トヨタ自動車株式会社 | T-Connect | 提供済 | |
| 7 | 日産自動車株式会社 | Nissan Connect | 提供済 | |
| 8 | 日野自動車株式会社 | ひのこんぱす | 提供済 | |
| 9 | 本田技研工業株式会社 | Honda CONNECT | 提供済 | |
| 10 | マツダ株式会社 | MAZDA CONNECT | 提供済 | |
| 11 | 三菱自動車工業株式会社 | Mitsubishi Connect | 提供済 | 国内は車載オーディオ向け<br>米国市場で先行するサービスあり |
| 12 | 三菱ふそうトラック・バス株式会社 | トラックコネクト | 提供済 | |
| 13 | ヤマハ発動機株式会社 | My TMAX Connect | 未提供 | 2輪向け、欧州のみ |
| 14 | UD トラックス株式会社 | UD Telematics Services | 提供済 | |

4.3.1.2. V2X その他の通信を伴うサービス・機器

インターネット以外の通信（V2V／車車間、V2I／路車間、V2P／歩車間）を伴うコネクテッドサービスの現時点で実装状況を調査した。現状は開発中あるいは実装されていても試験的な運用の段階にあり、観測による脅威収集は困難であることが予想される。これらについては来年度以降も実証実験などの事例調査を含め調査を進める予定である。

表 4-8 V2X 関連コネクテッドサービスの実装状況、事例

| # | 分類 | 通信先 | 関連するコネクテッドサービス | 実装済/開発中 | 備考（実装状況、シェアなど） |
|---|---|---|---|---|---|
| 1 | V2V（車車間通信） | 自動車 | 車間距離制御，隊列走行 | 実装済 | 車間距離制御は、国内では一部の OEM 特定車種で試験的に運用中。 |

| # | 分類 | 通信先 | 関連するコネクテッドサービス | 実装済/開発中 | 備考(実装状況、シェアなど) |
|---|---|---|---|---|---|
| | | | | | 隊列走行は、国内では米国にて商用利用で試験的運用中。 |
| 2 | V2I（路車間通信） | 交通インフラ | ITS 協調型自動運転 | 実装済 | 国内では一部の OEM の特定の車種と特定地域の信号機で試験的に運用中。<br>海外では、ドイツで Audi の一部の車種と信号機で試験的に運用中。 |
| 3 | V2P（歩車間通信） | 歩行者のデバイス | （歩行者検知） | 開発中 | 米国の一部の OEM が開発中 |

表 4-9 その他のコネクテッドサービスの実装状況、事例

| # | 分類 | 通信先 | 関連するコネクテッドサービス | 実装済/開発中 | 備考(実装状況、シェアなど) |
|---|---|---|---|---|---|
| 4 | 人工衛星 | 人工衛星 | ITS 協調型自動運転 | 開発中 | 国内では「みちびき」を用いた自動走行運転の実証実験中 |
| 5 | 充電スタンド | 充電スタンド | （EV、PHEV） | 実装済 | 国内では、EV、PHEV 新車販売に占めるシェアは 2%未満(2019 年実績)<br>一般的に、最適な電流を選択するため、車両の ECU と充電スタンドが CAN で通信する。 |

### 4.3.2. 自動車領域の特性を考慮した脅威情報収集方法の検討

IT システムは、OS などのプラットフォームが利用組織やユーザー間で概ね共通しているが、自動車は車種ごとにアーキテクチャが異なっている。そのため、IT 領域で共有されるような脅威インテリジェンスの形式では対策に活用できない恐れがある。

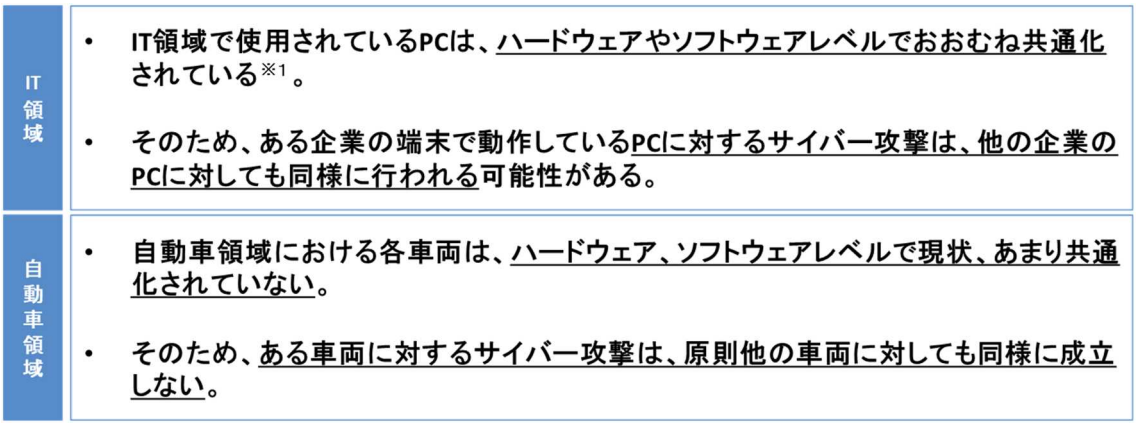



図 4-15 IT 領域と自動車領域におけるアーキテクチャと脅威の共通性

これは、自動車は、「車両制御」という観点において HW/SW や通信プロトコルが OEM に依存しているためで、IT との大きな違いがある。一方で、「車両制御」に至るまでの攻撃の流れを分析することで、最終的な目的の達成に至るまでに、OEM に依存しない手法が用いられていることが明らかになり、共通の脅威として、共有する価値のある情報となる可能性が期待できる。

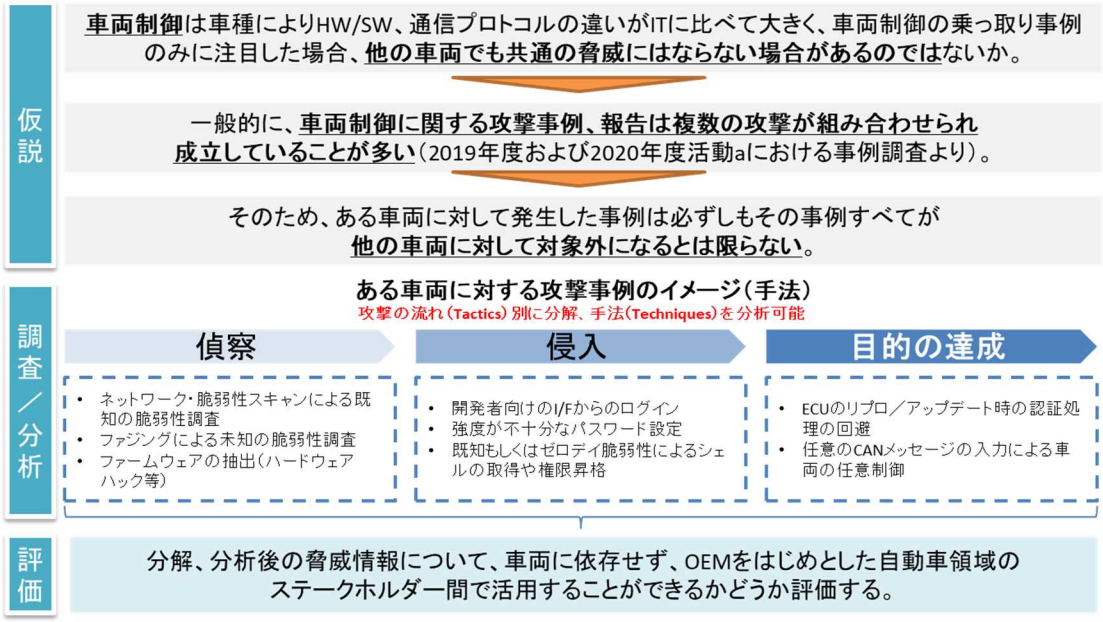



図 4-16 自動車領域での脅威情報共有に関する仮説

### 4.3.3. 脅威情報の収集実験に対する仮説と期待

本活動では、4.2.6 で調査した情報収集手法の一部について、実験を予定している。特にハニーポットについては、IoT や ICS などの他領域において既に実践されている点から、コネクテッドカーにおいても何らかの示唆が得られる

可能性がある。また、現時点において明らかに自動車を狙う攻撃が観測できなかったとしても、ハニーポットの構築方法などのノウハウについては、今後実際の攻撃が観測され始めた際に活用することができる。

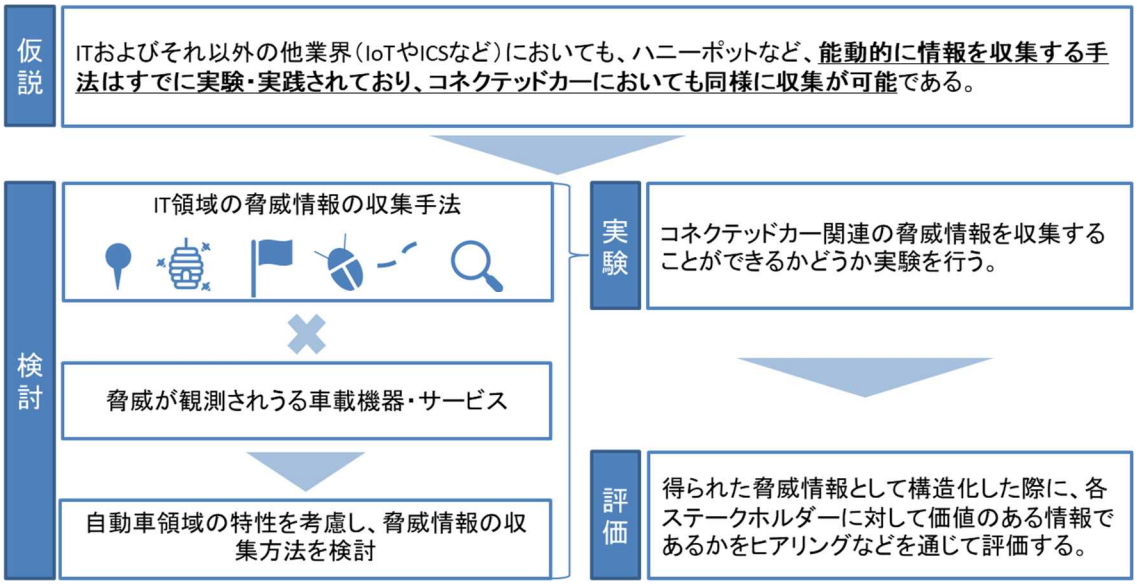



図　4-17　情報収集の手法検討・実験における仮説

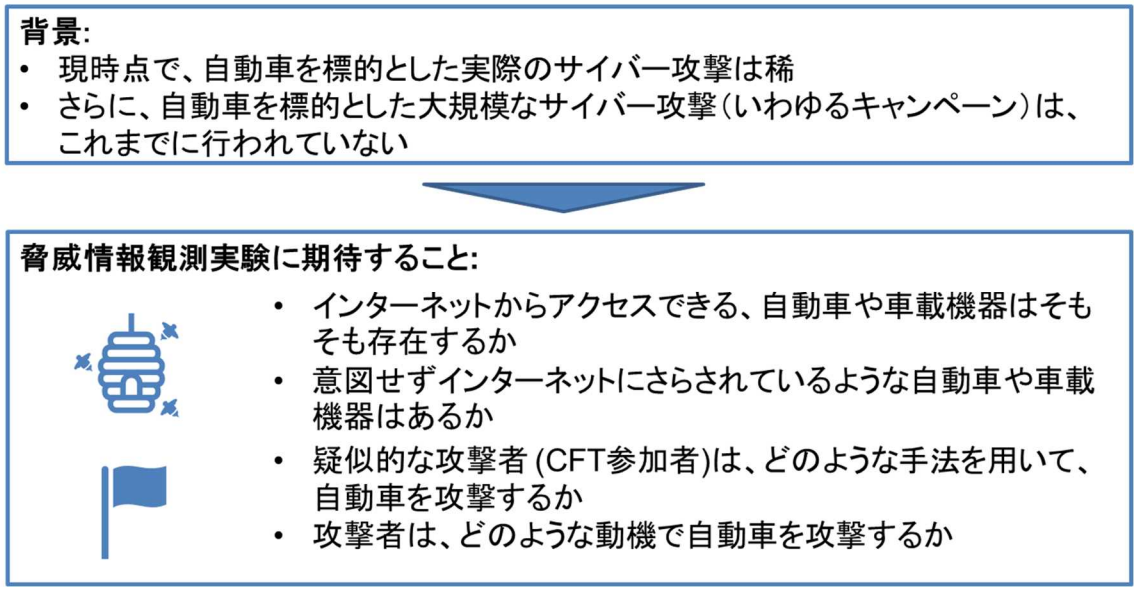



図　4-18　情報収集の実験に対する期待

## 4.4.　情報収集・蓄積の基本仕様検討

アフターマーケット製品のハニーポットによる、脅威情報収集実験に先行して着手している。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。

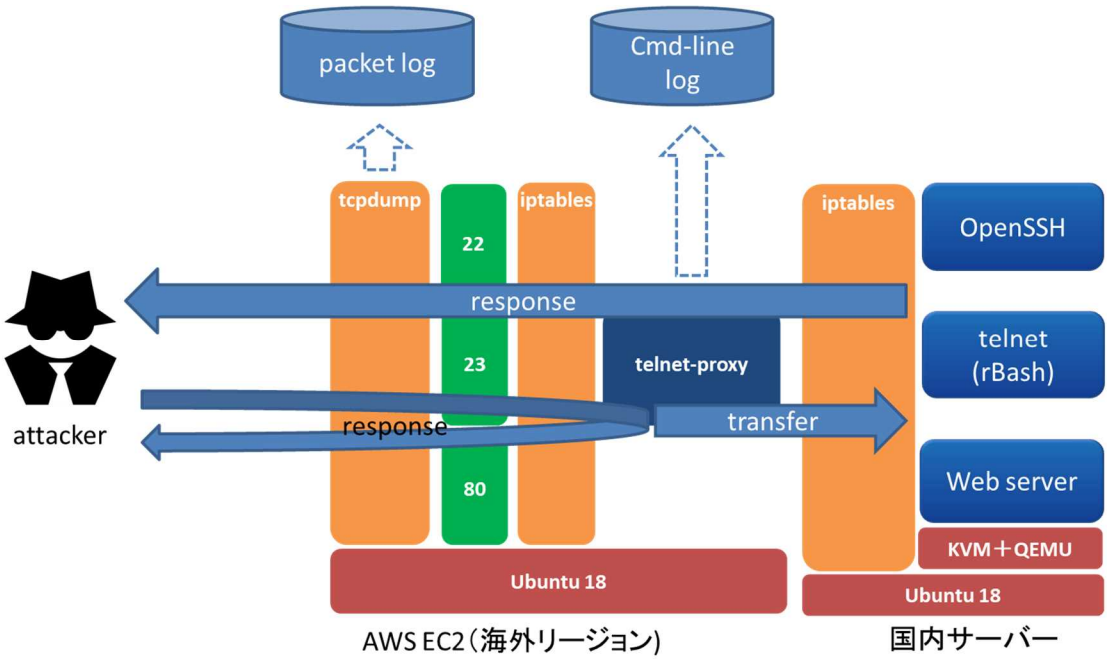



図 4-19 アフターマーケット製品を模したハニーポットのプロトタイプ構成

現状の観測結果としては、IoT 製品同様に telnet に対して ID と弱いパスワードを送り付ける、Mirai（マルウェア）の特徴と一致するアクティビティを多数観測しており、これは、Mirai に感染した機器からの自動化攻撃を受けており、当該ハニーポットを車載機器として認識したうえでの攻撃ではないものと考えられる。

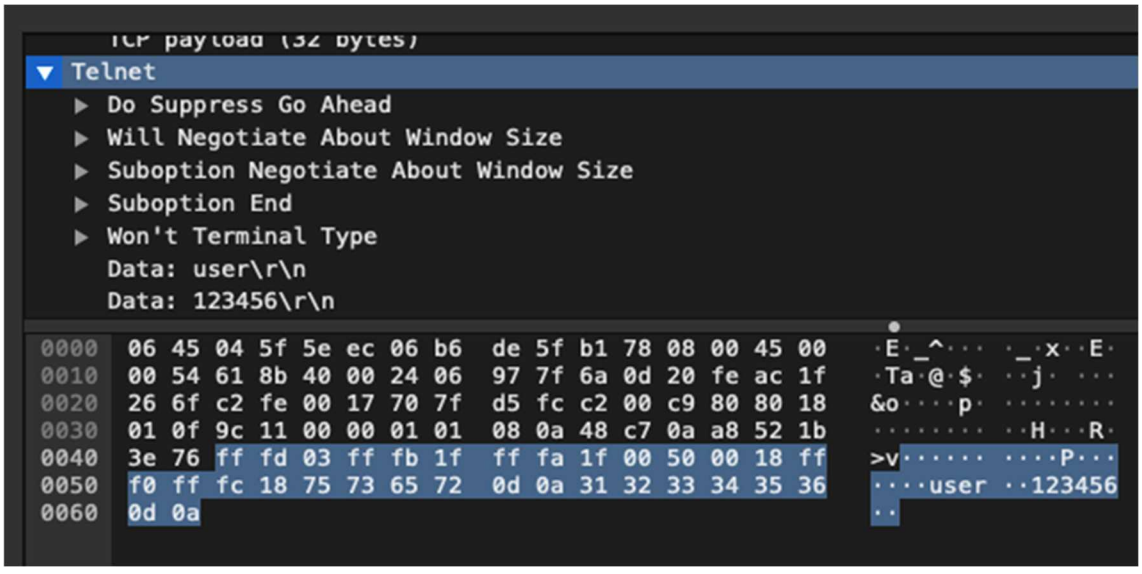



図 4-20 観測したパケットの例（ハイライト部分が ID とパスワード）

## 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

日独連携のキックオフは計２回に分けて、双方の活動概要および主要なメンバーの紹介が行われた。日本側の研究に対して、ドイツ側より以下の３点の研究について連携可能性についてコメントを頂いている。今後、引き続き定期的なコミュニケーションを行い、お互いの研究状況や成果について意見交換を進めていく。

表 5-1 連携可能性が示唆されたドイツ側の研究テーマ一覧

| # | 連携候補名 | 内容 |
|---|---|---|
| 1 | Vehicular attack database<br>（カールスルーエ工科大学） | ● 自動車の脆弱性データベースを構築するための、分類法（taxonomy）の提案 |

| # | 連携候補名 | 内容 |
|---|---|---|
| 2 | IDS management system（Autosar） | ● 複数の IDS が連携して情報の集約、レポーティング、およびソフトウェアを更新する仕組みを提唱している。 |

１は、ハニーポットや CTF で観測・収集した脅威情報を分析する　際に、分類法の考え方取り込める可能性がある。２は、日本側のハニーポットからの脅威情報収集とドイツ側の IDS からの脅威収集で連携できる可能性がある。また、２の活動に参画している ESCRYPT 社は、「a. IDS 評価手法ガイドラインの策定」において、連携の可能性がある。

# 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」

本年度は、２０１９年度の活動成果を活用し、さらに２０１９年～２０２０末までの事例の分析結果より、基本テスト要件を新たに２件追加した。また、仕様評価項目についても、昨年ヒアリングにご協力していただいたベンダーのうち、３社６製品を対象に再度ヒアリングを実施し、項目の整理を行った。

今後は、本年度のアウトプットである基本テストケースに基づいた実機検証や、仕様評価項目のヒアリング先ベンダーについても拡充を行うことで、仕様評価項目および基本テストケースの妥当性評価と精緻化を進めていき、IDS 評価ガイドラインとして文書化する予定である。

「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 サーバー側）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。

以上

契約管理番号：20001599-