戦略的イノベーション創造プログラム

「戦略的イノベーション創造プログラム（SIP）／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

概要版

PwCコンサルティング合同会社

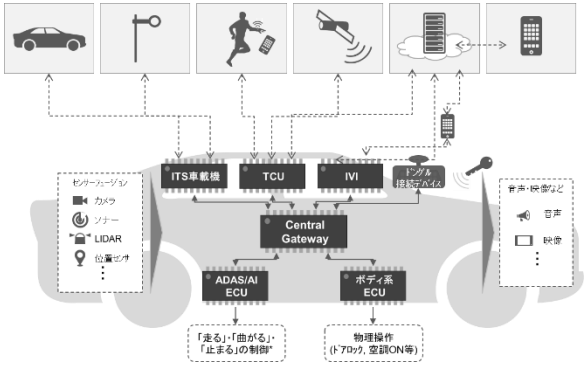
2023年2月

プロジェクトの背景と研究内容・実施体制

自動走行システムの普及によるセキュリティ環境の変化や国際的な法規の整備より、本事業では、「IDS評価手法と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と初動支援の調査研究」の2つの活動を行った。

セキュリティ環境の変化

車両のコネクテッド化に伴うセキュリティリスクの増大



国際的な法規の整備

UNECE WP29におけるUN-R155/R156の合意

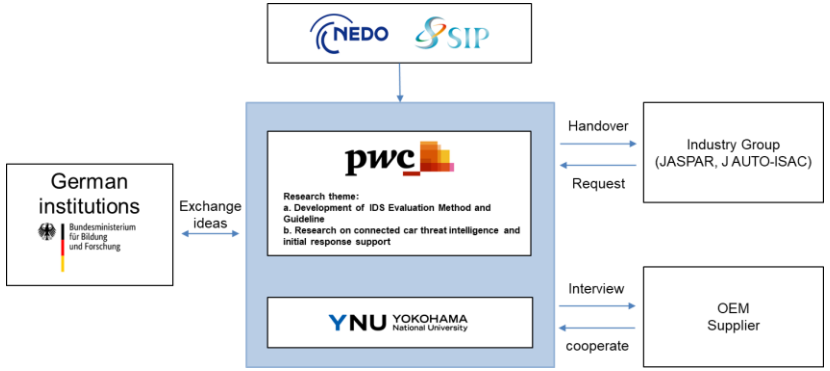
国連自動車基準調和世界フォーラム(WP29)

IDS評価手法とガイドラインの策定（活動a）

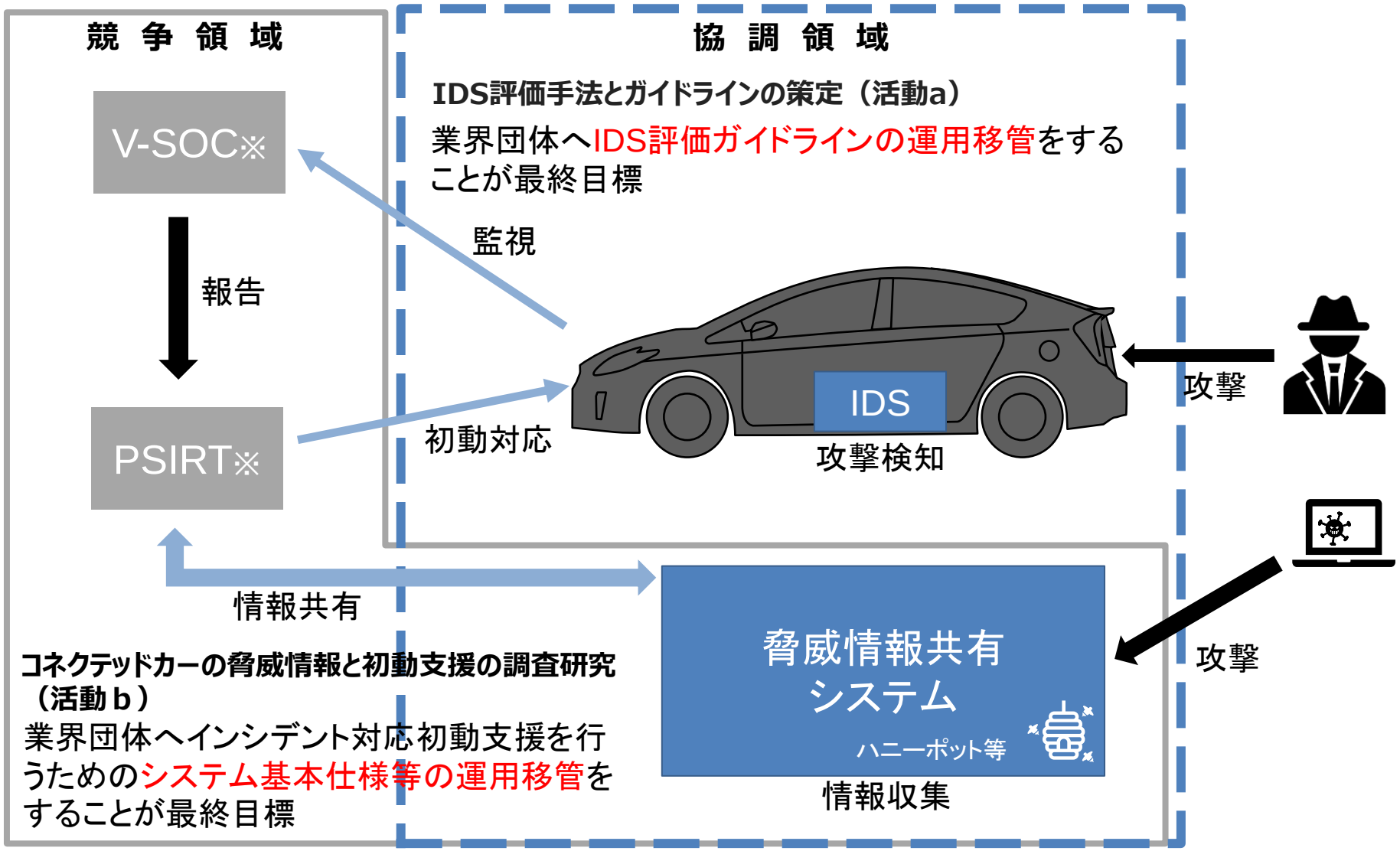
車両の侵入検知システム（IDS）に着目し、IDS評価ガイドラインを策定した。

コネクテッドカーの脅威情報と初動支援の調査研究（活動b）

自動車に対する脅威情報の収集方法の手引きと情報共有システムの基本仕様書を策定した。



活動スコープと目標



※V-SOC : Vehicle-Security Operation Center.　車両を監視し、インシデント等が検知された場合は、PSIRTと連携し、対応を行う。
※PSIRT : Product Security Incident Response Team. V-SOCや第三者からのインシデント通報を受け、対応を行う。

a. IDS 評価手法とガイドラインの策定

IDS評価ガイドライン策定の目的

活動aでは、攻撃の検知技術である車載IDSの評価方法について調査研究し、開発時に活用できる「IDS評価ガイドライン」として整理することで、自動車業界全体の「出荷後のセキュリティ対策」に貢献する。

出荷後セキュリティに関連した背景

法規面

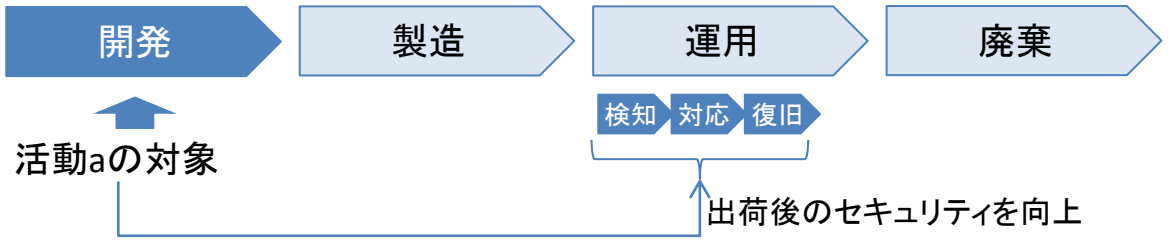
WP29 UN-R155でサイバー攻撃を検知・対処することが求められており、自社車両が検知(detect)・対処(respond)できることを説明する必要がある。

実務面

どのような攻撃について、どの程度検知すればよいかについては、既存の法規やガイドライン等で示されておらず、各社で規定する必要がある。

活動aの目的と方針

車載IDSに注目し、「IDSが攻撃を検知し、さらにその後、車両の復旧につなげられることを評価」するための評価方法を調査研究し、「IDS評価ガイドライン」として整理することで、自動車業界全体の出荷後セキュリティ対策に貢献する。

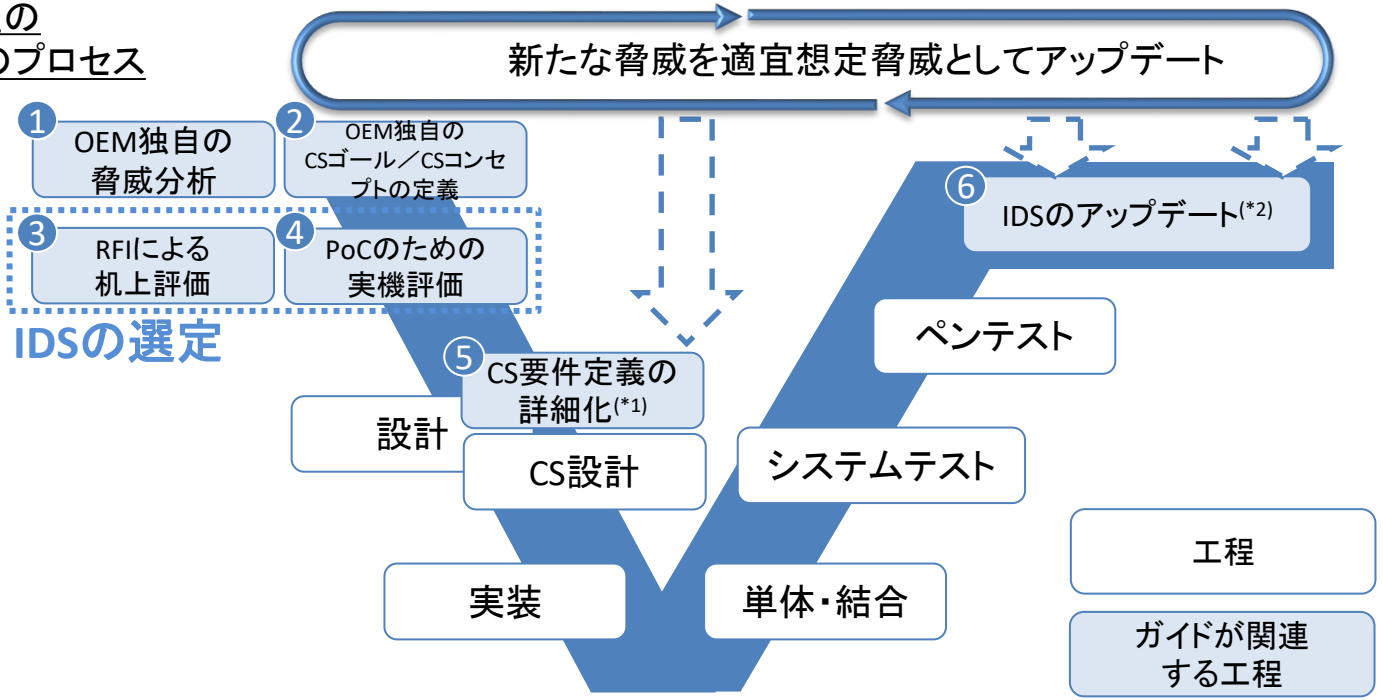


IDS評価ガイドラインの目標

基本的な機能を実装済のOff-the-Shelf型の開発スタイルを前提とし、IDSの選定とIDSの要求定義・追加要求定義の工程において、OEM/サプライヤーに参照いただける情報を提供することを目標とした。

目標1	IDSの選定工程で利用する評価項目やテスト手順書のテンプレートを作成する（③④）
目標2	OEM/サプライヤー独自のIDSの要求定義の工程において、攻撃シナリオを作成してIDSの要求を導出する方法の例を示す（①②⑤⑥）

Off-the-Shelf型の開発スタイルのプロセス



(*1) 車両の機能や想定する脆弱性を踏まえてリスクアセスメントをし、詳細にCS要求を定義すること。ISO/SAE 21434のrefinement of cybersecurity requirementsに該当。
(*2) 新たな脅威からIDSに求められる検知機能を整理し、必要に応じてIDSの検知ルールの定義ファイルやプログラムを更新すること。

IDS評価ガイドラインの評価方針

ガイドラインでは、以下の3つの方針でIDSを評価をすることとした。特に、検知・対応機能について、「過去の攻撃事例と同等の攻撃を検知・解析できること」を評価することがガイドラインの特徴である。

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

検知・対応機能だけではなく、保守性やセキュリティ等を含め、網羅的に評価する。

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

過去に起きた攻撃と同等の攻撃は基本的に全て、車両として防御対策をするか、あるいは、攻撃を検知・解析できることを評価する。

方針3

簡易なテスト環境でIDS実機評価をする

IDS選定時点では、IDS搭載車両や部品は存在しない。このため、OEM/サプライヤーが容易に調達でき、かつ、テストに最低限必要な機材・データのみを利用してIDS実機評価をすることを目指す。

活動方針：IDS評価ガイドライン策定アプローチ

以下のアプローチでIDS評価ガイドラインを作成し、業界団体にハンドオーバーした。

1 IDS基本機能の要素調査、検討	車両に対する最新の攻撃事例についてWeb情報や論文の調査を行い、車載IDSが検知すべき要素を調査、整理する。
2 仕様に基づく評価観点検討	IDS選定時に評価するべき観点を「仕様評価項目」として整理する。さらに、OEMやIDSベンダーへのインタビュー等により成果物の妥当性を検証し、仕様評価項目を再度整理する。
3 基本テスト項目導出・実施方法検討	[1]の調査、OEMへのインタビュー等により、IDS選定・検証段階でIDS実機を利用して評価するべき観点を整理し、「基本テストケース」のドラフトを作成する。
4 IDS実機評価	テストベッドや実車ベンチ等とIDS実機を利用したテストにより、[3]で導出した「基本テストケース」のドラフトの妥当性を検証し課題を明確化する。
5 IDS評価ガイドライン作成	[4]で明確化した課題を踏まえ「基本テストケース」を再度整理するとともに、攻撃事例から「基本テストケース」の観点を導出した手順を元に「新たな脅威からのテスト要件導出方法」を導出する。
6 実務展開	[1]～[5]の成果物を「IDS 評価ガイドライン」として纏めて関連業界団体にハンドオーバーし、自動車業界への実務展開、実務運用につなげる。

活動a アプローチ (1/3)

過去の車両への攻撃情報・論文調査やIDS製品に関する公開情報調査等により「仕様評価項目」と「基本テストケース」のドラフトを作成し、OEMやIDSベンダーへのインタビュー、IDS実機調査を実施して妥当性を検証した。

1 IDS基本機能の要素調査、検討

車両に対する最新の攻撃事例についてWeb情報や論文の調査を行い、車載IDSが検知すべき要素を調査、整理する。

INPUT

- Web攻撃情報、論文
- 2019年度成果（攻撃シナリオ調査・分析結果）

OUTPUT

- IDSに求められる検知機能（セキュリティイベント）

2 仕様に基づく評価観点検討

IDS選定時に評価するべき観点を「仕様評価項目」として整理する。さらに、OEMやIDSベンダーへのインタビュー等により成果物の妥当性を検証し、仕様評価項目を再度整理する。

INPUT

- IDSに求められる検知機能（セキュリティイベント）
- IDSの公開情報（2019年度成果を含む）
- OEM、IDSベンダーインタビュー

OUTPUT

- 仕様評価項目一覧

活動a アプローチ (2/3)

過去の車両への攻撃情報・論文調査やIDS製品に関する公開情報調査等により「仕様評価項目」と「基本テストケース」のドラフトを作成し、OEMやIDSベンダーへのインタビュー、IDS実機調査を実施して妥当性を検証した。

3 基本テスト項目導出・実施方法検討

[1]の調査、OEMへのインタビュー等により、IDS選定・検証段階でIDS実機を利用して評価するべき観点を整理し、「基本テストケース」のドラフトを作成する。

INPUT

- 論文、各種ガイドライン(NIST SP800-94など)
- IDSに求められる検知機能(セキュリティイベント)

OUTPUT

- 基本テストケース(ドラフト)
- テスト実施環境の検討結果

4 IDS実機評価

IDS実機を利用したテストにより、[3]で導出した「基本テストケース」のドラフトの妥当性を検証するとともに、必要に応じてテスト方法を修正する。

INPUT

- 基本テストケース(ドラフト)

OUTPUT

- 基本テストケース

活動a アプローチ (3/3)

過去の車両への攻撃情報・論文調査やIDS製品に関する公開情報調査等により「仕様評価項目」と「基本テストケース」のドラフトを作成し、OEMやIDSベンダーへのインタビュー、IDS実機調査を実施して妥当性を検証した。

5 IDS評価ガイドライン作成

[4]で明確化した課題を踏まえ「基本テストケース」を再度整理するとともに、攻撃事例から「基本テストケース」の観点を導出した手順を元に「新たな脅威からのテスト要件導出方法」を導出する。

INPUT

- 基本テストケース（導出方法を含む）
- 仕様評価項目

OUTPUT

- IDS評価ガイドライン（ドラフト）

6 実務展開

[1]～[5]の成果物を「IDS 評価ガイドライン」として纏めて関連業界団体にハンドオーバーし、自動車業界への実務展開、実務運用につなげる。

INPUT

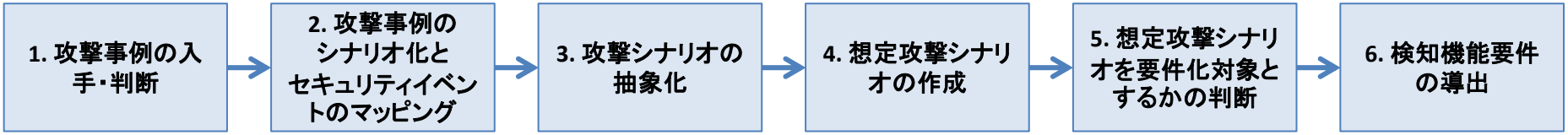
- IDS評価ガイドライン（ドラフト）

OUTPUT

- IDS評価ガイドライン（初版）

検知機能の要件化方法

活動方針で示した、「方針2：過去の攻撃事例と同等の想定攻撃の検知・解析可否を評価する」について、ある過去事例から検知要件を導出する方法を検討した。



#	概要
1	攻撃事例を入手して検知対象とする攻撃事例を選定
2	攻撃事例を各車両コンポーネントへの攻撃手順に分解、攻撃が成立する条件と目的を付加し攻撃シナリオ化し、各攻撃手順で発生する可能性のあるセキュリティイベントをマッピング
3	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
4	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
5	OEM/サプライヤーで定義された想定攻撃シナリオのリスク評価方法や対応方法に従い、具体的な対応方法を検討
6	攻撃により車載ネットワークに発生する可能性があるセキュリティイベントのうち、IDSで検知するべきものを選定し、要件として導出

IDS基本機能の調査検討 （1/3）

2020年までに開催されたセキュリティカンファレンスWeb情報、脆弱性情報を調査し、うち、車両に直接関係のある、12件について分析を行い、セキュリティイベントを導出した。

	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**

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
	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

IDS基本機能の調査検討 （2/3）

対象とした12件の事例は以下の通り。

情報ソース	攻撃事例概要
USENIX Security '20 Technical Sessions	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]
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]
脆弱性情報	トヨタLexus等のDCU(Display Control Unit)のBTモジュールのバッファーオーバーフローの脆弱性を利用して自動的に外部のWiFi APに接続するようにするとともに、CANコントローラーのファームウェアを改ざんしてメッセージフィルタリング機能を無効化し、外部から車両にWiFi接続して診断メッセージをCANバスに送信できた。[Lab, 2020]
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]
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]
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]
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]
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]
Web情報	Viper社のスマートアラームにおいて、サーバのAPIの脆弱性により、正規ユーザーになりすまして車両を追跡したり、エンジンを停止することができた。[PARTNERS, 2019]
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]
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]

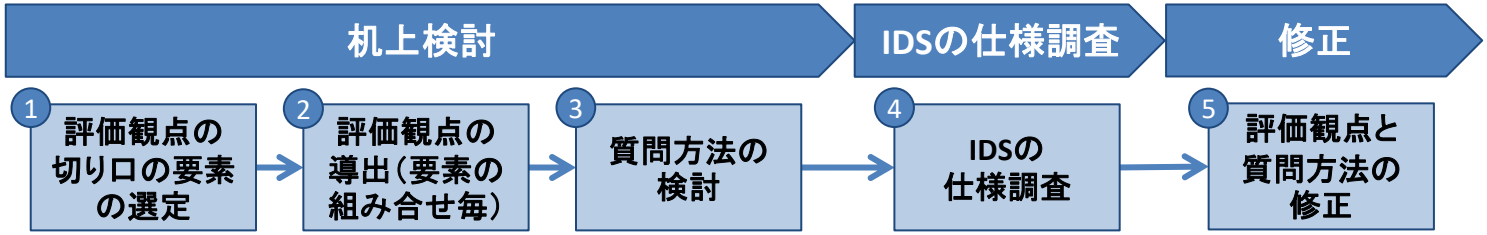
IDS基本機能の調査検討 （3/3）

事例の分析結果から導出した、IDS基本要件は以下の通り。
※具体的な基本要件はガイドラインのみの記載とする。

大分類	小分類	ID
検知機能	誤検知なし	SD-FP-1
		SD-FP-2
	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
	送信周期の異常	SD-TP-2-1
		SD-TP-2-2
	前後のメッセージとの関係の異常	SD-TP-3-1
		SD-TP-3-2
	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
	車載NWの状態の異常	SD-TP-5-1
	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

IDS仕様評価観点の検討 （1/3）

「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」に基づき、下記の流れで仕様評価観点を導出した。



#	概要
1	IDSの製品ライフサイクルと、ソフトウェア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」の品質特性を評価観点の切り口として選定
2	1に対して網羅的に評価できるよう、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検討
3	2の検討した評価観点が、IDSを比較することができる詳細度であるかを評価するためにIDSベンダーへの質問リストを作成
4	作成した質問リストに基づいてIDSベンダー（パナソニック株式会社（日）・イータス株式会社（独）・Arilou Information Security Technologies（以））にヒアリングを行い、仕様評価観点・質問内容の妥当性を検証
5	検証結果及びJASPAR、想定読者のOEMからのフィードバックに基づいて仕様評価観点の最終化

IDS仕様評価観点の検討 （2/3）

IDSベンダーへの質問項目は以下の通り。

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
		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）

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）
	その他（　　）

※ 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。

IDS仕様評価観点の検討 （3/3）

IDSベンダー3社（6製品）について、質問リストへの回答に対する考察は以下の通り。

1. 検知対象のセキュリティイベント

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。

2. ロギング・通知方式

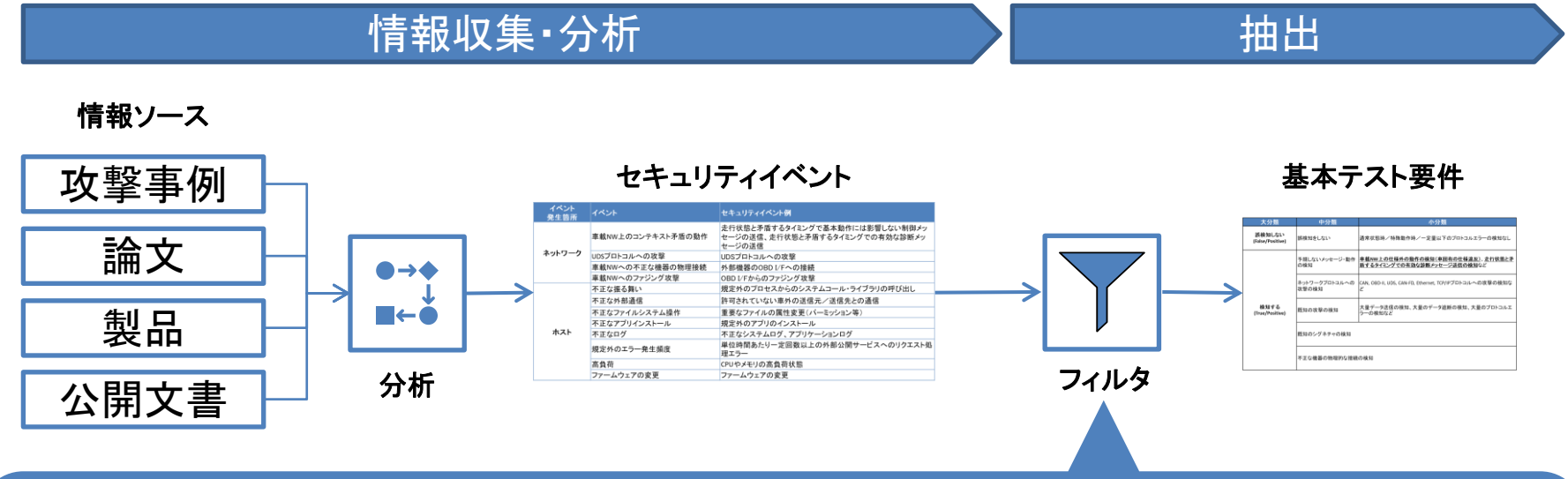
各社対応済み、もしくはカスタマイズ可能であり、基本的にはOEMの要求ベースでカスタマイズする前提である。したがって、OEMとしてIDSに要求する機能とカスタマイズ機能のフレキシビリティのギャップを知ることで、IDSの比較検討がある程度可能ではないかと考える。

3. V-SOC運用サービス

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。

基本テストケースの検討 （1/6）

攻撃事例を分析してセキュリティイベントを導出し、そのうち、一定条件を満たすものをIDSが最低限検知するべきセキュリティイベント（基本セキュリティイベント）として抽出し、それらを検知できることを基本テスト要件とした。



フィルタ条件

1. 過去（2019～2021年）に公開された※1、どのIDSでも対応するべき※2車両への攻撃事例で発生する、および／または；
2. 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

基本テストケースの検討 （2/6）

基本テストケースは、IDS選定時や検証時のソフトウェア単体テストで必要最低限テストするべき観点について、まとめたものであり、記載項目は以下の通り。

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
	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（次スライドを参照） 検知種別: 検知の種別（次スライドを参照） 検知理由: 検知の理由（次スライドを参照） 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

基本テストケースの検討 （3/6）

全スライドに掲載した基本テストケース記載項目の期待値（検知バス・種別・理由）の定義は以下の通り。

検知バス定義

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

検知種別定義

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

検知理由定義

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

基本テストケースの検討 （4/6）

基本テストケースの一例を以下に示す。

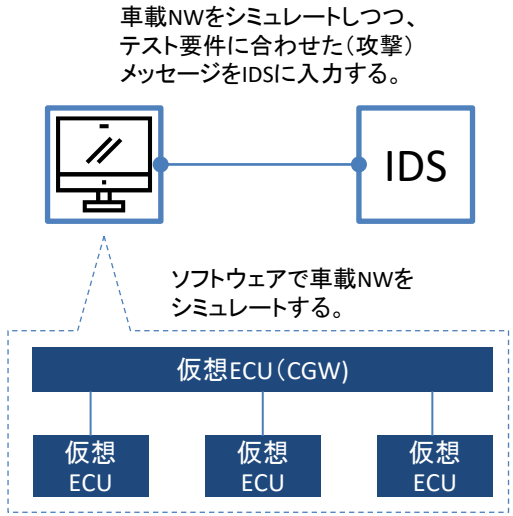
カテゴリ	項目	内容
テスト観点	テストケースID	SD-TP-1-2
	テストケース名	PT／シャシー系msg, ボディ系msgの注入による不正なデータの範囲の検知
	目的	定義された信号値の範囲に違反したメッセージが存在したとき検知することを確認する。
	検知対象SEv	不正なデータの範囲
	注入する攻撃msg種別	PT／シャシー系msg, ボディ系msg
	前提条件	走行状態：等速走行中
	導出源の攻撃事例	OBD2dongle/Wen(USENIX'20)-2 Jeep Cherokee(BH USA 2015)
テスト方法	テスト環境	シミュレーション環境
	前提とする車載NWの仕様	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。
	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		

基本テストケースの検討 （5/6）

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コストが大きいため、後者2つのどちらかで行うことを前提に検討した。

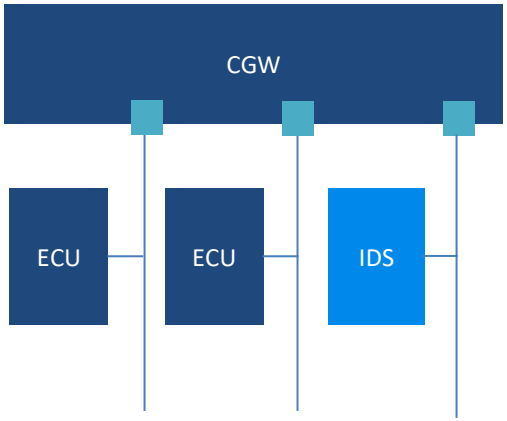
シミュレーション環境

実ECUを使用しないテスト環境。ソフトウェア上で車載ネットワークを再現する。



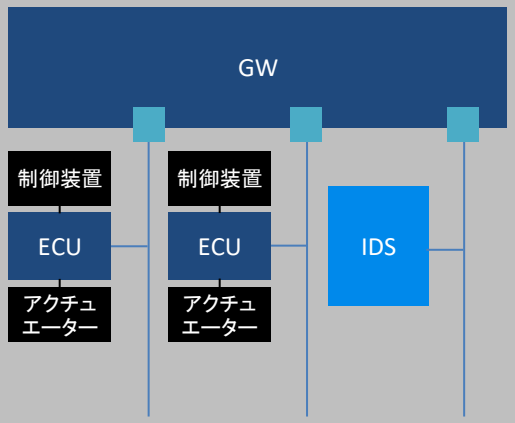
テストベッド環境

テスト要件を満たす、必要最低限のハードウェアで構築した環境。



車両（ベンチ）環境

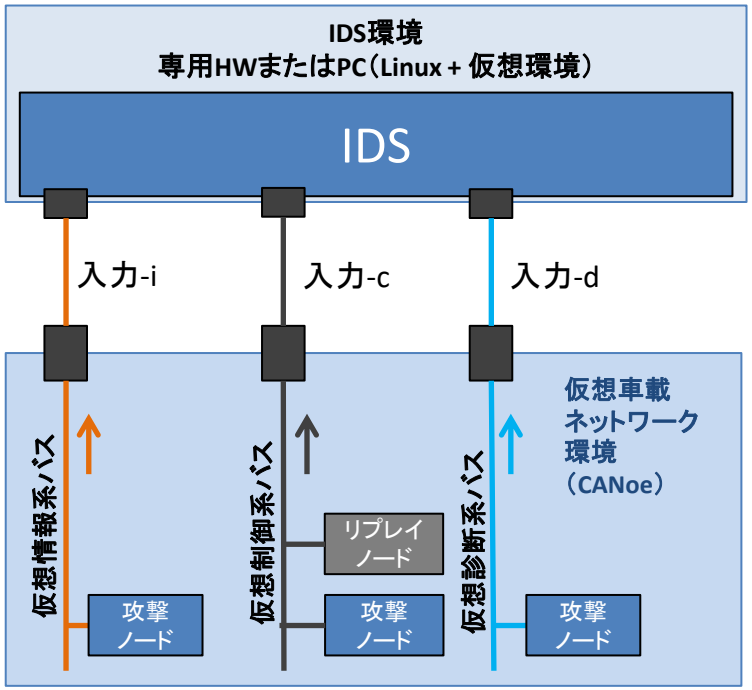
実車相当の入力装置、ECU、アクチュエーターを接続した環境。



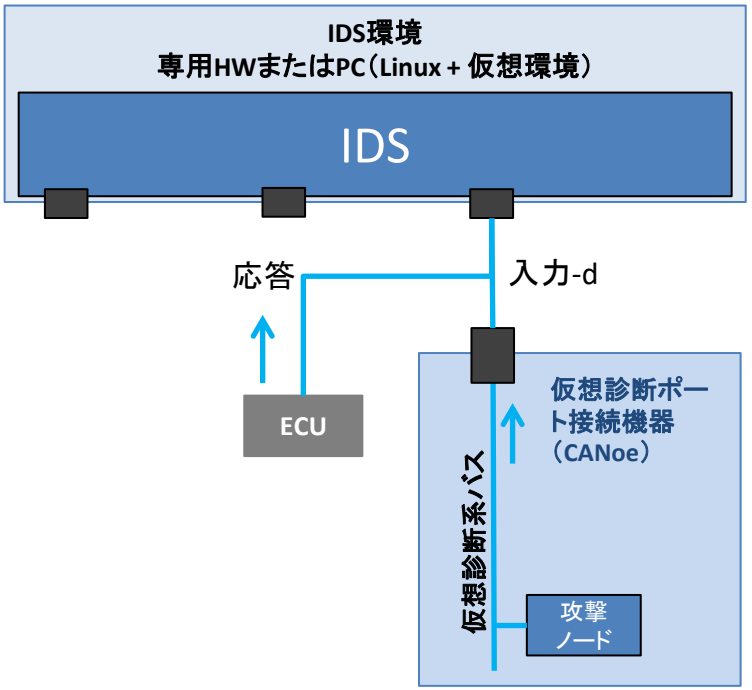
基本テストケースの検討 （6/6）

基本テストケースが前提とする基本構成は以下の通り。

シミュレーション環境

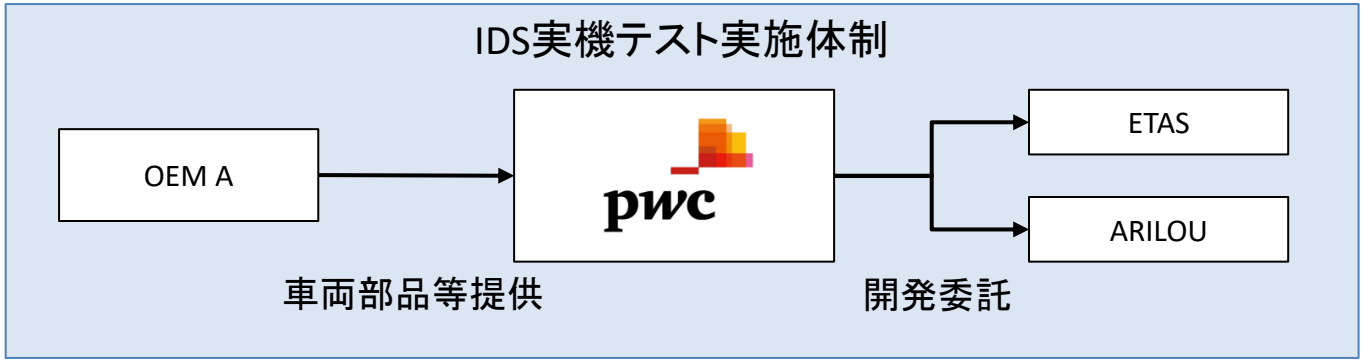


テストベッド環境



IDS実機テストによるテストケースの検証 （1/5）

IDS実機テストは、IDSを評価することが目的ではなく、基本テストケースの妥当性を検証することである。実機テストの実施体制について以下に示す。



IDS実機テストによるテストケースの検証 （2/5）

基本テストケースは、評価観点のベースラインであり、対象となる車両（ECU）やIDSの仕様によって、テスト方法及び期待値の一部を調整する必要がある。実機テストにおいてもECU及びIDSの仕様に基づいてテスト方法及びIDSに対する要求仕様を調整した。

車両（ECU）仕様に基づいて調整したテスト方法の内容

1. テストで利用する信号値の閾値
2. 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）
3. 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%）
4. 各バスの最大バス負荷（95%）

IDS仕様に基づくテスト方法の調整・実施方針

a. 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。
b. 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。
c. 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。
d. 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）

IDS実機テストによるテストケースの検証 （3/5）

対象外とした項目のうち*a～cについては、前スライドで事前に定義したIDS仕様に基づくテスト方法の調整・実施方針に基づいて対象外としたテストケースである。
*1～3については、ベースIDSの仕様及びベンダーとの協議に基づいて対象外としたテストケースであり、その理由については次スライドに記載する。

大分類	小分類	テストケースID	ETAS	ARILOU
検知機能	誤検知なし	SD-FP-1	○	○
		SD-FP-2	対象外(*a)	対象外(*a)
	1. 単一メッセージのデータの異常	SD-TP-1-1	○	○
		SD- TP -1-2	調整（msgの仕様）	対象外(*1)
		SD- TP -1-3	調整（前提条件）	調整（検知対象のmsgはペイロードのみ出力）
	2. 送信周期の異常	SD-TP-2-1	○	調整（検知回数）
		SD-TP-2-2	○	調整（検知回数）
	3. 前後のメッセージとの関係の異常	SD-TP-3-1	調整（msgの仕様）	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)

IDS実機テストによるテストケースの検証 （4/5）

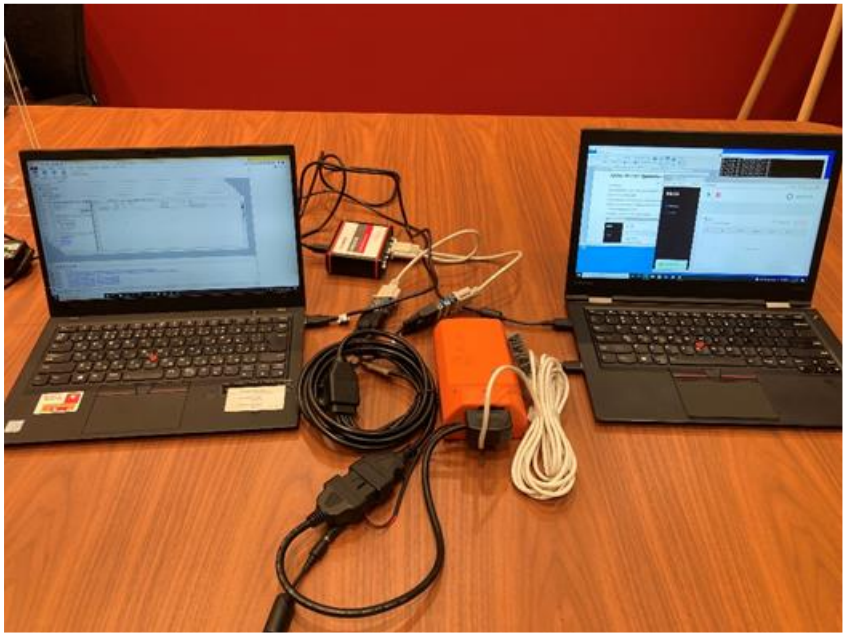
ベースIDSの仕様による対象外とした理由（前スライド*1～3）を以下に示す。

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、対象外としたり、検知ルールの設定において、注入する攻撃メッセージを「定期送信でない」とする等の調整をしたりした。
(*2)	ETAS社のベースのIDSは、シーケンス、ステートフルな検知ルールは対応していないため、一部テストケースは対象外とした。
(*3)	ARILOU社のIDSは、例えばAUTOSARのIdsRモジュールに対し他のCANバスに出力は可能であるが、今回、開発工数短縮の為、車載ネットワークへのメッセージ送信機能は省いた。このため通知機能に関するテストケースは対象外とした。

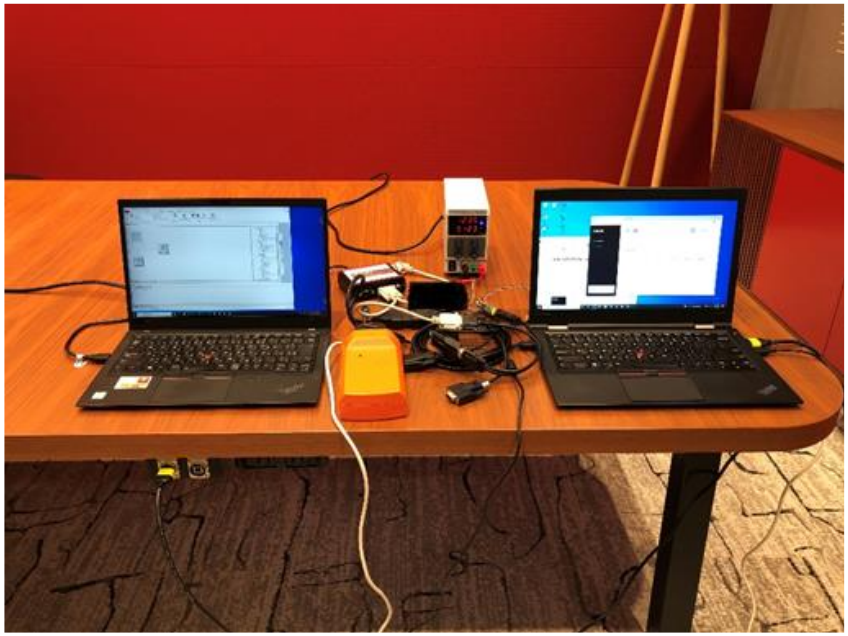
IDS実機テストによるテストケースの検証 （5/5）

IDS実機テスト環境は、基本テストケースの検討時に前提とした基本構成に基づいて構築し、テスト対象としたすべてのテストケースで示す手順が期待通りに実施できることを確認した。Arilou Information Security Technologies社のIDSで検証した際の実機構成を以下に示す。

シミュレーション環境



テストベッド環境



社会実装に向けた活動

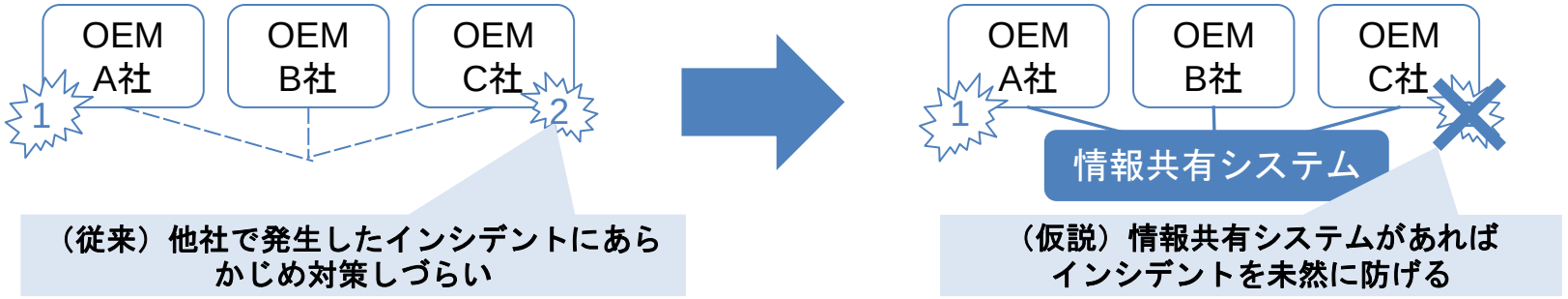
移管先であるJASPARと技術検討会を合計8回開催し、フィードバックをいただいた。成果物は2022年にJASPARに移管。

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

b. コネクテッドカーの脅威情報と初動支援の調査研究

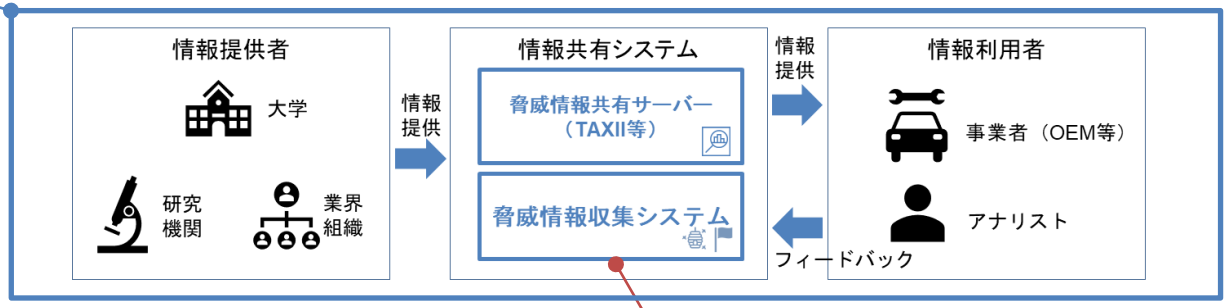
調査研究の目的

情報共有システムの基本仕様および情報収集方法を調査し、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する。



【成果物（１）】情報共有システムの基本仕様書

自動車領域における脅威情報を蓄積し、セキュリティインシデントの初動対応支援に活きる共有システム全体に関する基本仕様書を取り纏めます。



【成果物（２）】情報収集の手引き

ハニーポットおよびプレイグラウンドの実証実験で得られた車両コネクテッドシステムに対する攻撃手法・技術に関する知見や、各種実証実験のノウハウを取り纏めます。

活動b成果一覧

活動bでは、「情報共有システムの基本仕様書」と「情報収集の手引き」の2つの成果物を作成した。
成果物は自動車業界において利活用されることを想定し、J-Auto-ISACへ展開する。

情報共有システムの基本仕様書の目的	想定読者
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

情報収集の手引きの目的	想定読者
自動車領域における業界団体、各OEMおよびサプライヤーが、車両システムにおける脅威情報をプロアクティブに収集する際に参考となる収集方法やノウハウを提示することを目的とした。	• 車両システムへの攻撃に関する情報をプロアクティブに収集したい業界団体、OEMおよびサプライヤー

活動方針：活動b 調査研究アプローチ

以下のアプローチで「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、業界団体にハンドオーバーする。

「情報共有システムの基本仕様書」の作成

1. 基礎調査	2. 情報収集・蓄積の手法検討	3. システム仕様の検討	4. システム仕様の導出	5. 基本仕様書の作成	6. 実務展開
IT領域の脅威インテリジェンス活動はどのようなものがあり、どのように対策に活用されているか調査する。	自動車領域での初動対応支援をするため、IT領域の脅威情報の蓄積手法を、応用する手法を検討し仮説を立てる。	共有システムの目指すべき姿を導出し、目指すべき姿達成のための仕様を検討する。	目指すべき姿達成のための仕様を導出し、あわせて、PoCを実施し要素技術の自動車領域への適用性を検証する。	[2]～[4]をもとに基本仕様書としてまとめる。	[5]で作成した成果物を関連業界団体にハンドオーバーし、自動車業界への実務展開につなげる。

「情報収集の手引き」の作成

1. 基礎調査	2. 情報収集・蓄積の手法検討	3. 実証実験の実施	4. 実証実験の拡大	5. 手引きの作成	6. 実務展開
IT領域において、脅威インテリジェンスを形成するために、どのようにして情報を収集・分析しているか調査する。	IT領域の脅威情報の収集手法を、応用する手法を検討し仮説を立てる。	[2]の仮説をもとに実験計画を立案し、実証実験を通して、自動車業界における情報収集手法の有効性を評価する。	[3]の実験の拡張手法や他の手法について、自動車業界における情報収集手法の有効性を評価する。	[4]の実証実験は継続しつつ、当該実験と[2]～[4]をもとに手引きとしてまとめる。	[5]で作成した成果物を関連業界団体にハンドオーバーし、自動車業界への実務展開につなげる。

b. コネクテッドカーの脅威情報と初動支援の調査研究

【情報共有システムの基本仕様書】

「情報共有システムの基本仕様」の適用範囲

基本仕様書の適用範囲は、初動支援を行うための情報共有システムとした。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である。

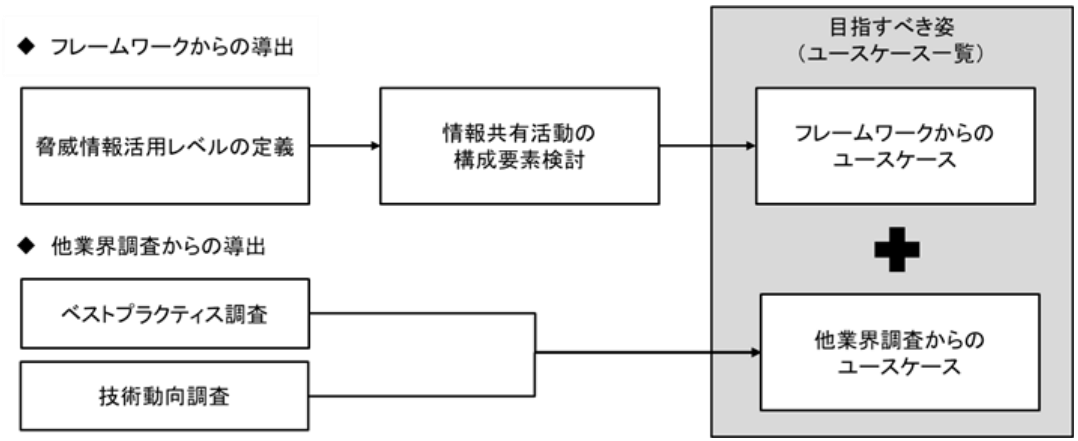
	フェーズ	説明
予防対策	特定	情報収集を通じて、保有する車両・システムに関する脅威・脆弱性を特定する
予防対策	防御	特定された脅威・脆弱性に対して適切なセキュリティ対策を行う
発生時対策	検知	車両・システムをモニタリングし、イベントを検知する
発生時対策	対応	発生したインシデントに対応する
発生時対策	復旧	発生したインシデントの復旧および恒久的対策を行う

本プロジェクトにおける「初動」のスコープ

情報共有システムの目指すべき姿の導出方法

目指すべき姿は、2つの方法で導出したユースケースの集まりで表現した。1つ目はフレームワークを参考に情報の活用レベルを定義し当該定義が実現された際のユースケース、2つ目は他業界調査から導出したユースケースである。

目指すべき姿の作成方針



情報の活用レベル定義（Lv.Adaptive）

Lv.	説明
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、脅威情報をタイムリーに収集している。 脅威情報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。

参考：NIST 関連文書：https://www.ipa.go.jp/security/publications/nist/index.html
サイバーセキュリティ成熟度モデル：https://www.acq.osd.mil/cmmc/about-us.html

目指すべき姿を実現する情報共有システムの概要

前頁で示した、フレームワークから導出したユースケースと他業界調査から導出したユースケースは以下のとおり。

フレームワークから導出したユースケース例

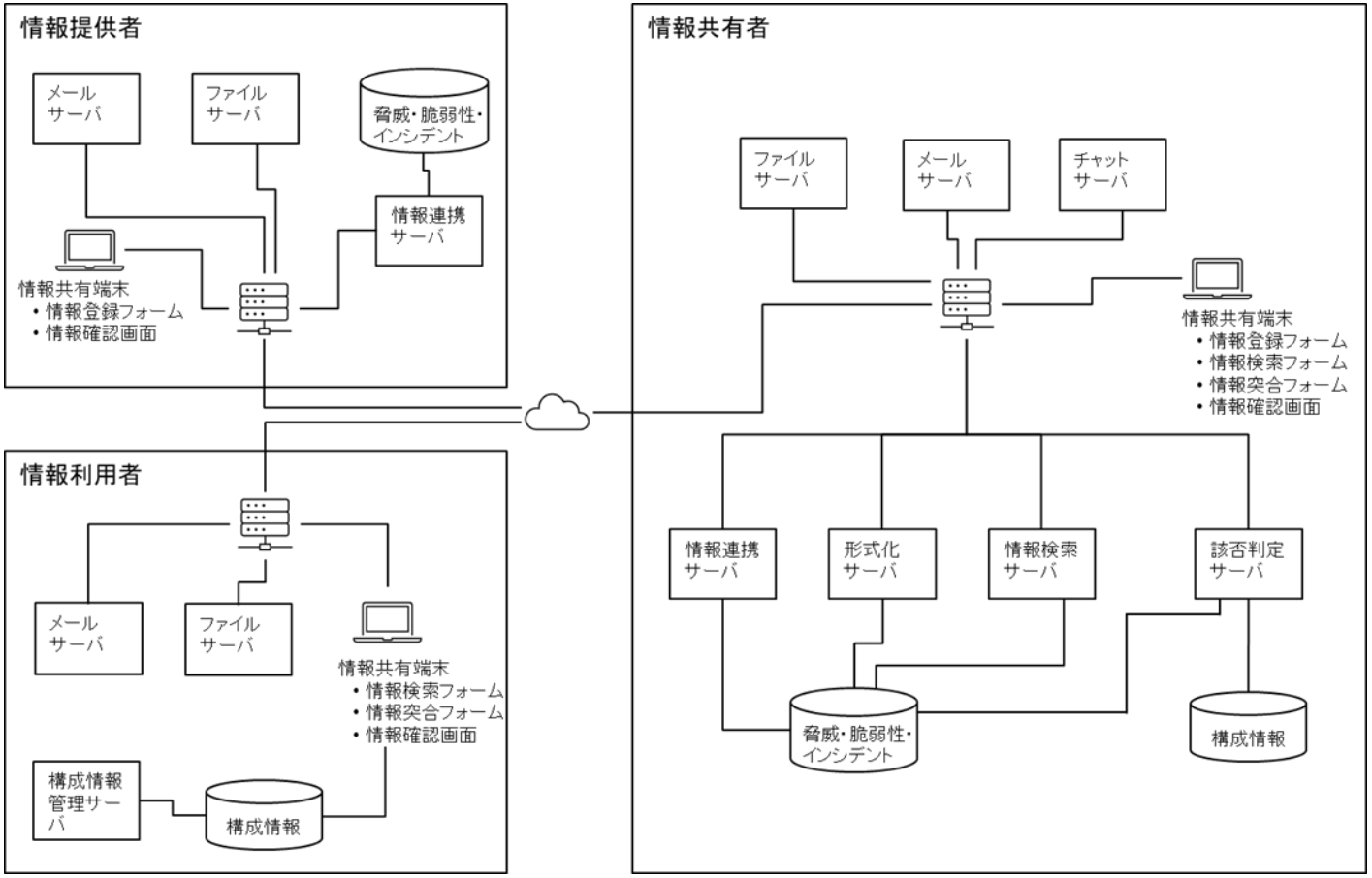
ユースケースID	活動目標(分類)	ユースケース
U-1	情報共有	情報提供者が形式化されていない情報群（脅威情報、脆弱性情報、インシデント情報）を情報共有者に提供、情報共有者が情報を保管・情報利用者に展開し、情報利用者が内容を分析したうえで、自身に関係する情報からリスクを把握する
U-2		情報提供者が形式化されていないインシデント情報を情報共有者に提供、情報共有者が情報を保管・分析し、脅威情報や脆弱性情報として整理し形式化したうえで情報利用者に展開し、情報利用者が自身に関係する情報からリスクを把握する
U-6	情報活用	情報提供者が形式化された情報群（脅威情報、脆弱性情報）を情報共有者に提供、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-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

他業界調査から導出したユースケース例

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

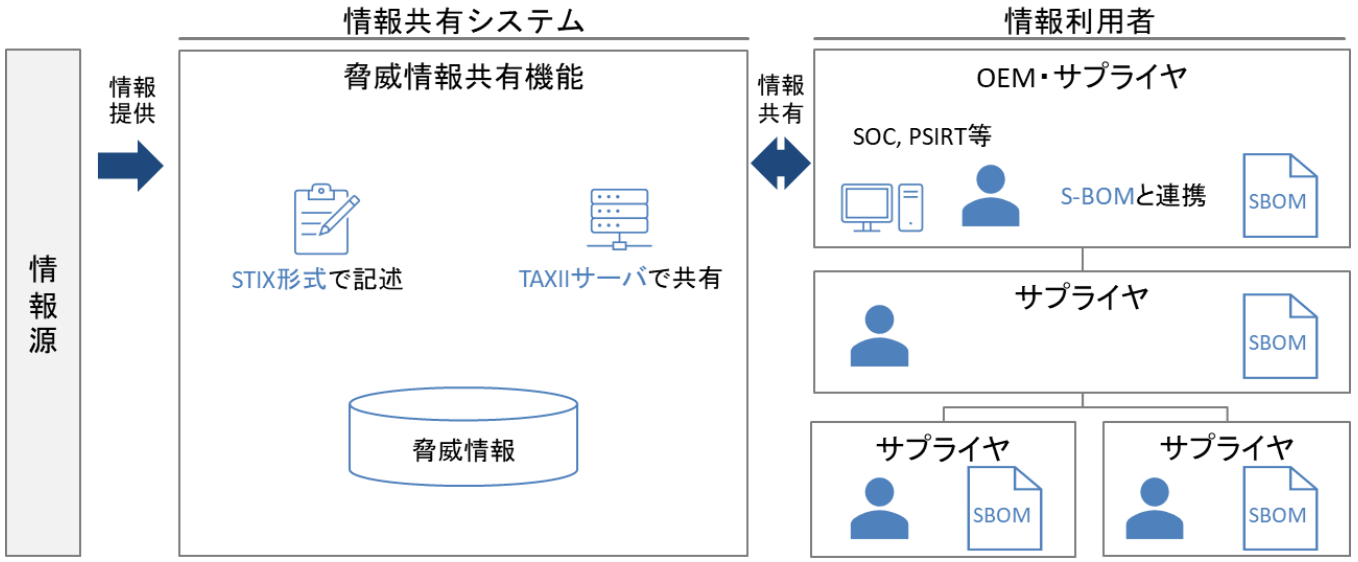
情報共有システムの全体概要図

目指すべき姿であるユースケースの集まりを実現するための情報共有システムの仕様を、「情報提供者」、「情報共有者」および「情報利用者」それぞれについて導出した。当該仕様から整理した情報共有システムの概要図は、以下のとおり。

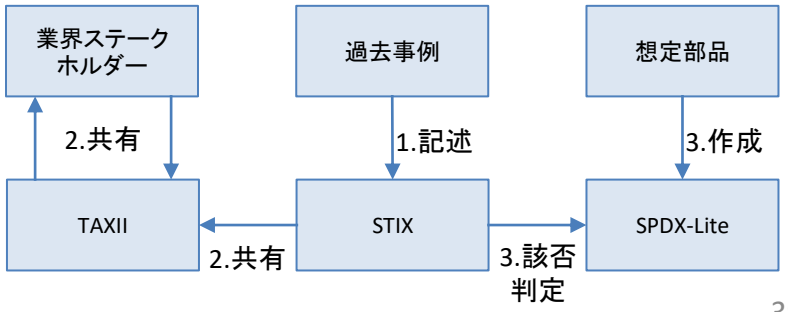


情報共有システムに関するPoC

実装に最新技術の適用をすることで目指すべき姿の達成につながると考えられるSTIX、TAXII、S-BOMについて、自動車業界の特性を考慮した適用性を検証することを目的にPoC（Proof Of Concept）を実施した。実験内容は、以下のとおり。



1. **脅威情報の記述（STIX）**
   - 過去事例がSTIXで記述可能か検証
2. **業界の企業構造を考慮した情報共有（TAXII）**
   - TAXIIがもつ標準的機能が
     基本仕様で定義した仕様を満たすか検証
3. **業界の企業構造を考慮した対応判断（SPDX-Lite）**
   - STIXで記述された過去事例の脅威情報に対して、
     SPDX-Liteで記述されたSBOMを使用して
     該否判定することが可能かどうか検証



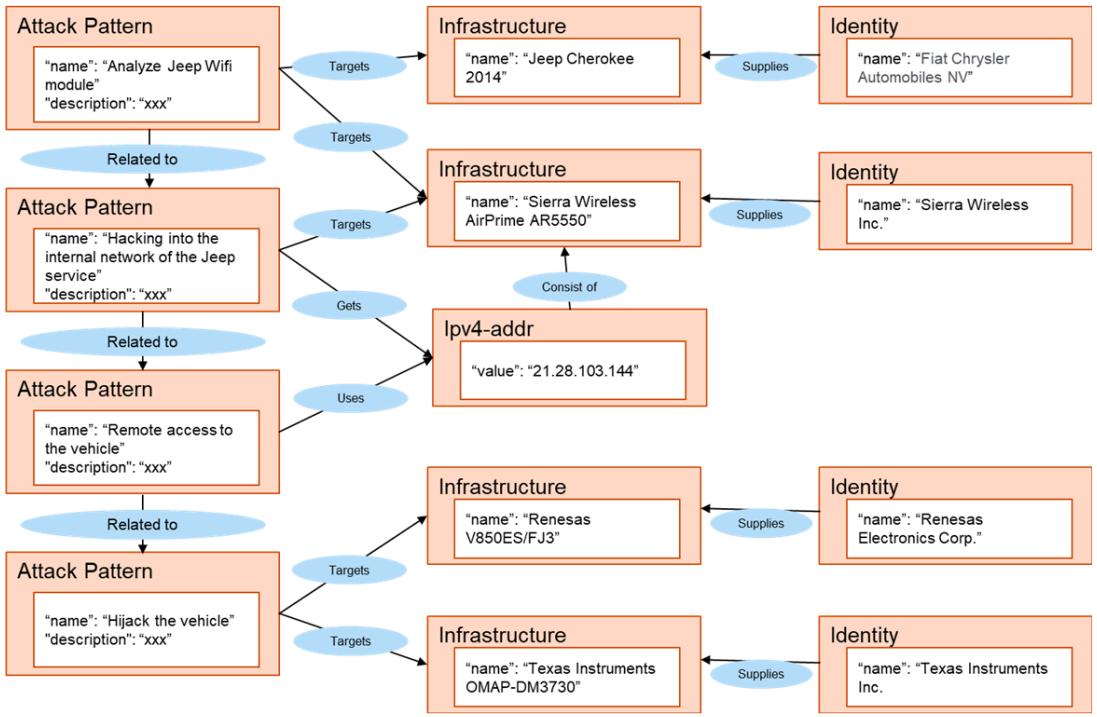
STIXに関するPoC

実事例から得られた脅威情報のSTIX形式での記述を試みた。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。

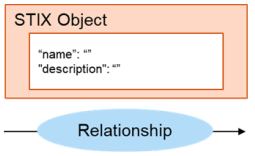
対象事例

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）

STIXオブジェクトとその関係性の整理



凡例



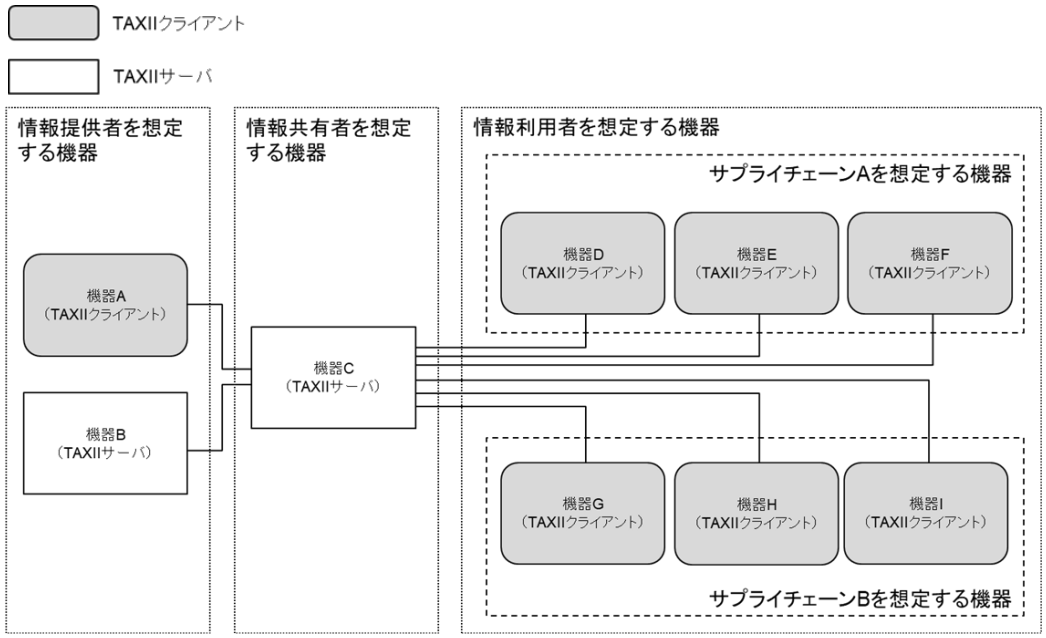
脅威情報のSTIX化のプロセス

1. 研究報告された自動車への攻撃事例を攻撃手順毎に整理
2. 攻撃手順から脅威情報を抽出
3. 抽出した脅威情報をSTIXオブジェクトとして記述
4. 各STIXオブジェクト間の関係性を”Relationship”タグで記述

TAXIIに関するPoC

以下の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。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システムで利用されている技術と組み合わせる必要があることを確認した。

PoC環境



確認内容

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

S-BOM（SPDX-Lite）に関するPoC

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。

架空の構成情報

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

突合（抜粋）

No		1	2	3	4	5	6	7	8	9	10	11	12
STIX	項目	identity	attack-pattern			ipv4-addr	infrastructure			-	-	-	-
	内容	Jeep Cherokee（車種）	Air Prime AR5550（部品名）	V850 controller（部品名）	OMAP chip（部品名）	21.28.103.144（IPアドレス）	Sierra Wireless AirPrime AR5550（組織名・部品名）	Renesas V850 processor（組織名・部品名）	Texas Instruments OMAP-DM3730 system（組織名・部品名）	-	-	-	-
S-BOM	項目	-	-	-	-	-	Creator- Organization(組織名)			DocumentName（SWパッケージ名）			
	内容	-	-	-	-	-	Supplier-B	Supplier-C	Supplier-D	Software_A-1	Software_B-1	Software_C-1	Software_D-1

今後の展望

将来を見据え、本基本仕様の全部または一部を参考にすることで、自動車業界のサイバーセキュリティ対策が進むことを期待している。なお、今後の方針や、更なる研究や注力する分野としては、以下等が考えられる。

- 本基本仕様を元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
- 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/サプライヤーが独自に調査・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

b. コネクテッドカーの脅威情報と初動支援の調査研究

【情報収集の手引き】

「情報収集の手引き」の策定方針

IT領域で脅威情報を収集するために利用されているプレイグラウンドとハニーポットに着目し、自動車領域における脅威情報の収集可能性を、実証実験を踏まえて検討する。

目的	• 自動車領域における業界団体、各OEMおよびサプライヤーが、車両システムにおける脅威情報をプロアクティブに収集する際に参考となる収集方法やノウハウを提示すること。
仮説	• IT領域において、能動的にサイバー攻撃者の動向や攻撃手法等に関する脅威情報を収集する方法として様々な手法が実験・運用されており、サイバーインテリジェンスの構築に役立っている。 • コネクテッドシステムにおいても、同様の手法により脅威情報を収集し、サイバーインテリジェンスの構築が可能である。 (例) 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
収集情報（想定）	• サイバー攻撃者の属性（IPアドレス、URL等のインジケータ） • 攻撃手口（試行された攻撃コード、マルウェア等のTTPs）
アプローチ	• IT領域の脅威情報収集手法を用いて、コネクテッドシステムにおける脅威情報の収集可能性を、実際の観測実験を踏まえて検討する。

実証実験への期待

本研究で行う実証実験は、自動車の脅威情報を得ることが目的ではなく、プレイグラウンドやハニーポットが自動車領域に適用可能かを検討し、実用化に備えて方法論を整理することを目的とする。

背景:

- 現時点で、自動車を標的とした実際のサイバー攻撃は稀
- さらに、自動車を標的とした大規模なサイバー攻撃（いわゆるキャンペーン）は、これまでに行われていない

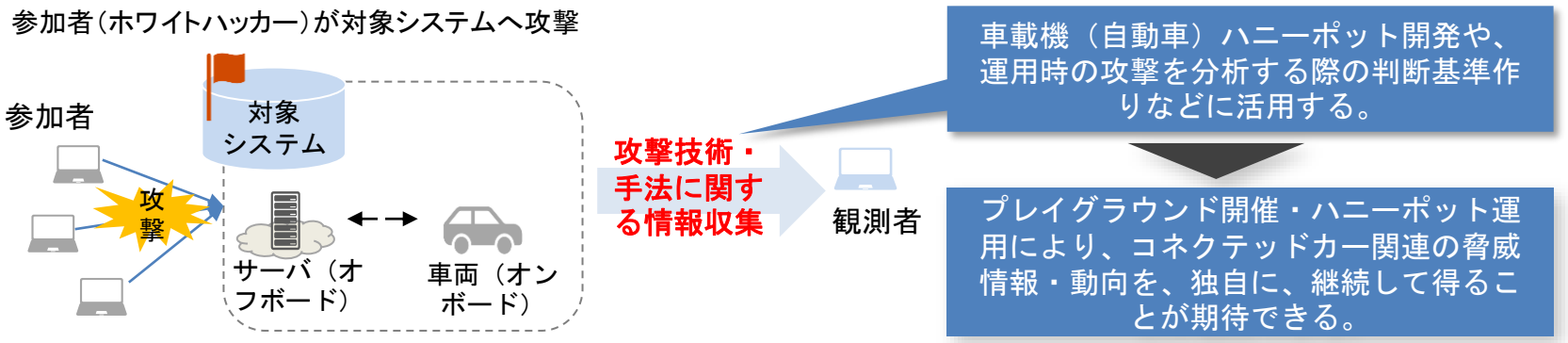
脅威情報観測実験に期待すること:

- インターネットからアクセスできる、自動車や車載機器はそもそも存在するか
- 意図せずインターネットにさらされているような自動車や車載機器はあるか
- 疑似的な攻撃者 (CFT参加者)は、どのような手法を用いて、自動車を攻撃するか
- 攻撃者は、どのような動機で自動車を攻撃するか

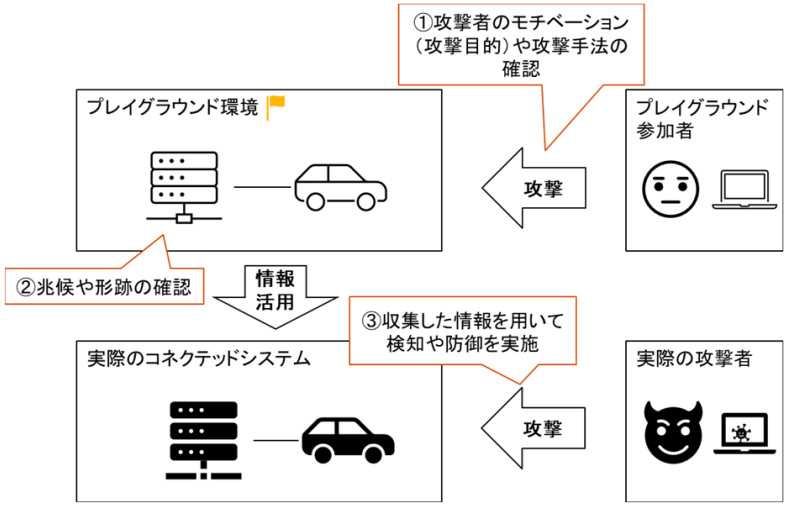
プレイグラウンドの目的

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。

実施イメージ



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ポイント

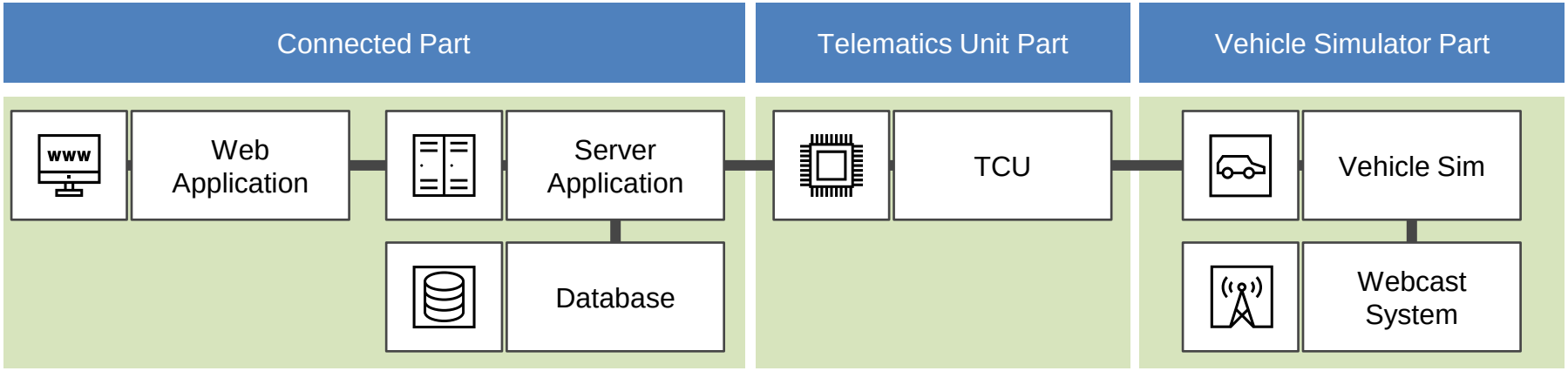


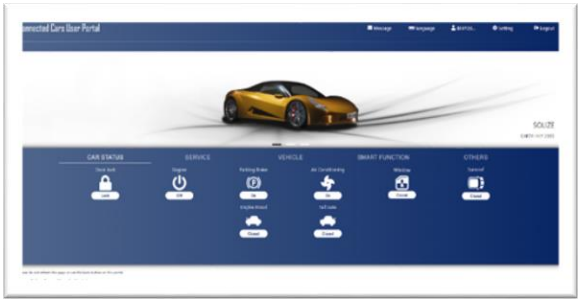
プレイグラウンドを適用すると…

1. コネクテッドシステムに対する攻撃者のモチベーションや攻撃手法が確認できる
2. 攻撃の兆候や形跡が（ログ等で）確認できる
3. 得られた情報を元に、実際のコネクテッドシステムの防御を強化できる。

プレイグラウンド環境

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。





ユーザーポータルサイト
ユーザーがアプリにログインした際に見える画面

TCU機材
コネクテッドサービス部と車両部をつなぐ構成要素

シミュレーション画面
インパネや車両の外観を表示し、ユーザーからの操作結果を反映させる

実装したコネクテッド機能一覧

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

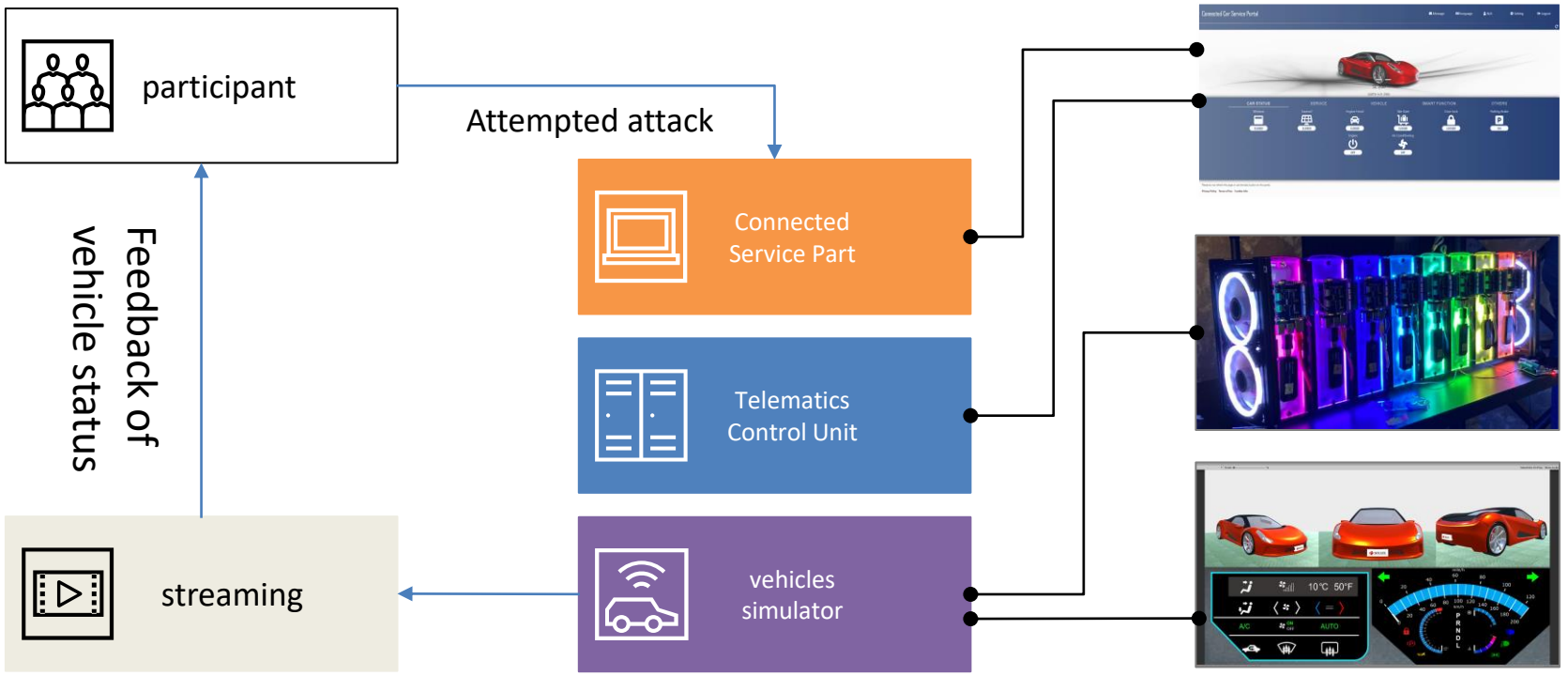
Connected Service Part			Telematics Unit Part	Vehicle Simulator Part
For vehicle owners Function	Functions for Dealers	Communication Functions		Simulation
Owner Portal Screen	Management Portal Screen	Send and receive SMS		CG Model of Vehicle
Door lock/unlock	Vehicle Management	TCU communication protocol (SMS+HTTP)		Body ECU
turning on the light	active test			Chassis ECU
horned pipistrelle				Powertrain ECU
Air conditioner operation				Air conditioning and active testing
Vehicle Information Display				
Engine start				

ドア開閉やアクティブテスト等の、ユーザー向け機能と管理者（ディーラー）向け機能を実装

SMSを用いたサーバからのリクエスト送出方法や、車両シミュレーション部へのリクエストのリレー方法を検討し、実装

（参考）プレイグラウンド実施の様子

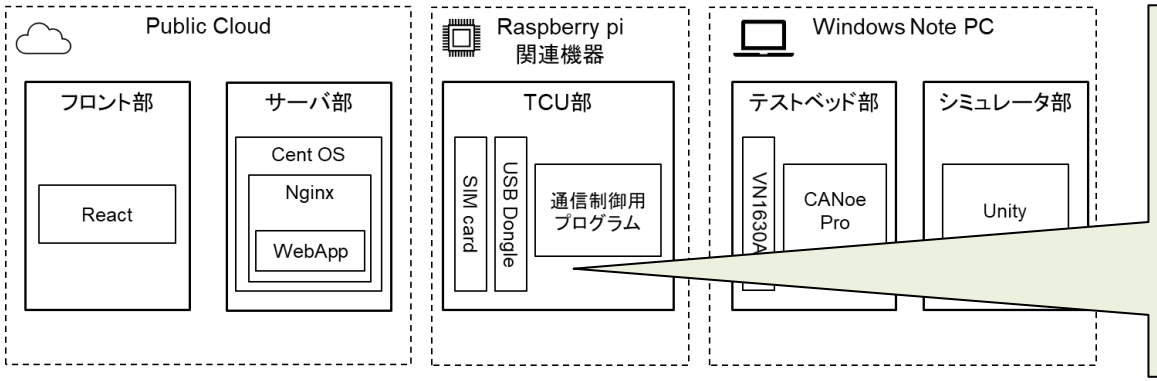
プレイグラウンド参加者は、まずユーザーポータルサイトを介した車両への攻撃を試みる。車両シミュレータ部の映像は配信サービスを通して参加者に配信され、攻撃や車両操作の結果が確認できる。



プレイグラウンド実証実験結果

本実証実験では「Webアプリケーション」「サーバ」「TCU」を車両へのアタックサーフェースとして定め、各構成要素を攻撃する際のモチベーションや攻撃手法を調査した。

プレイグラウンド環境詳細



プレイグラウンド環境のうち、
- Webアプリケーション
- サーバ
- TCU

をアタックサーフェースとした

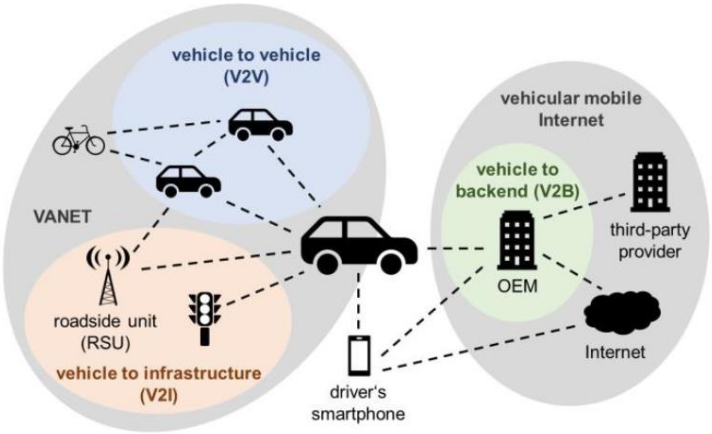
実験結果（抜粋）

構成要素	モチベーション	試行された攻撃
Webアプリケーション	• 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	• 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
サーバー	• Webアプリケーションの全体構造やAPI使用法の把握	• Webアプリケーションのソースコードの抽出・解析
TCU	• 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	• 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

ハニーポットの目的

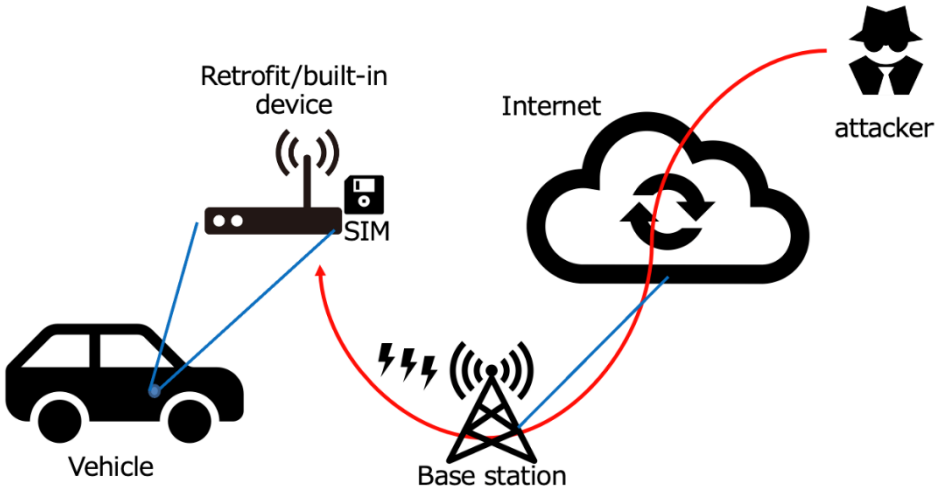
本ハニーポットは、インターネット上に公開された車載ルータやゲートウェイ等の車載機器に対して、インターネットからどのようなサイバー攻撃が行われるかを観測することを目的とした。

背景



自動車のコネクテッド化に伴い、攻撃インターフェースが多様化し、コネクテッドカーに対する攻撃が増加している。

本ハニーポットの目的

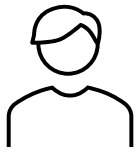


本ハニーポットは、インターネットから車載機へ直接攻撃される場合を想定し、どのような攻撃を受けるか観測することを目的とする。

（参考）車載ハニーポットの考え方

インターネットからアクセス可能な車載器などを模したシステムを構築し、インターネットに公開することで、攻撃者を誘引し、攻撃動向や攻撃手法等の示唆・知見を得る。

1 実際の車載製品に模倣したシステムを外部に露出させる



The Internet

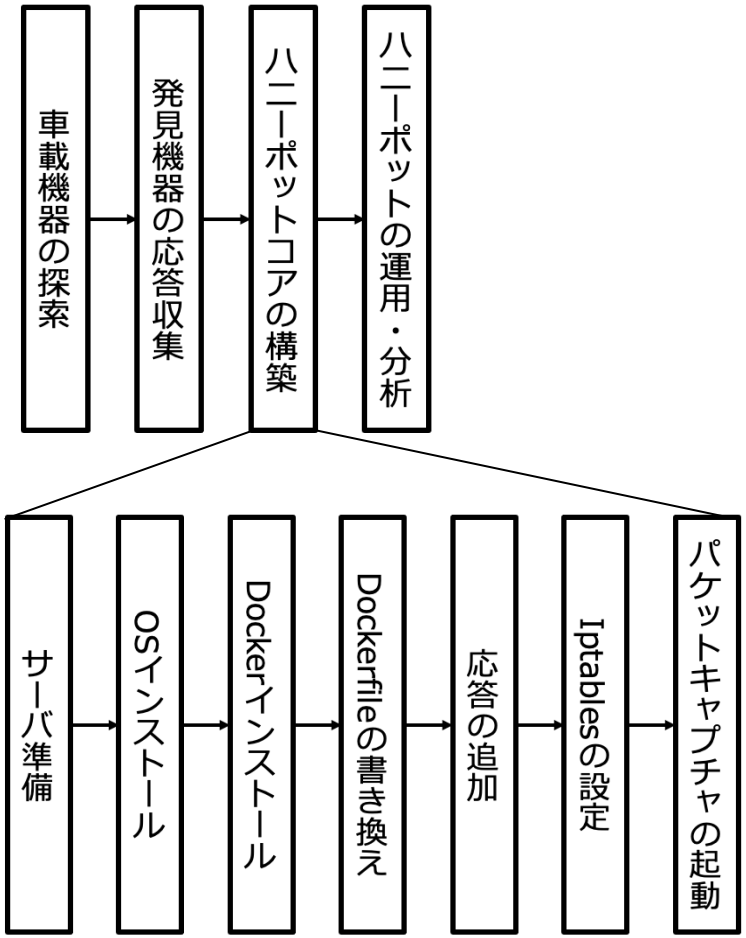
2 攻撃者やシステムによるスキャンや既知脆弱性攻撃試行などの他、IoTマルウェアによる攻撃など、多様な攻撃が機器に対して行われる

3 ハニーポットで受けた攻撃（ログ）を観測・分析することで、攻撃動向や新たな攻撃手法等の示唆・知見を得る。

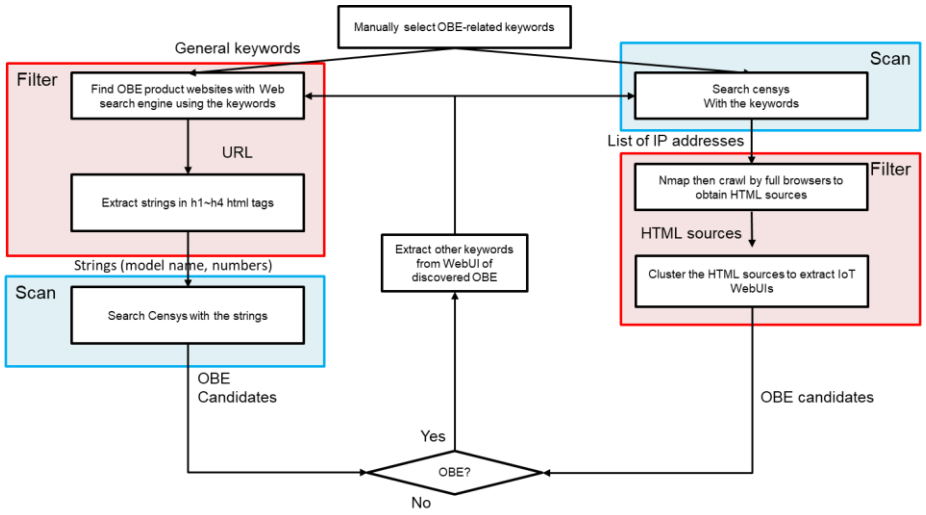
ハニーポットの構築プロセス

本ハニーポットは、以下の4ステップで構築した。そのうち、車載器の探索は2つのアプローチ方法で実施した。また、ハニーポットコアは、さらに7つのプロセスで構築した。

ハニーポット構築プロセス



車載器探索アプローチの概要



2種類の車載器探索アプローチ

- 始めに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で検索し、機器の型番・名前・モデル等を収集する。収集した情報を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。
- 始めにCensysで車載器関連のキーワードを検索する。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。その後、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。

発見された車載器例

インターネットから車載機が発見可能かを探索した結果、複数の機器がインターネット上に脆弱な状態で公開されていることが分かった。

発見された車載機の例


```
22/tcp OpenSSH5.1
23/tcp telnet
80/tcp http
```

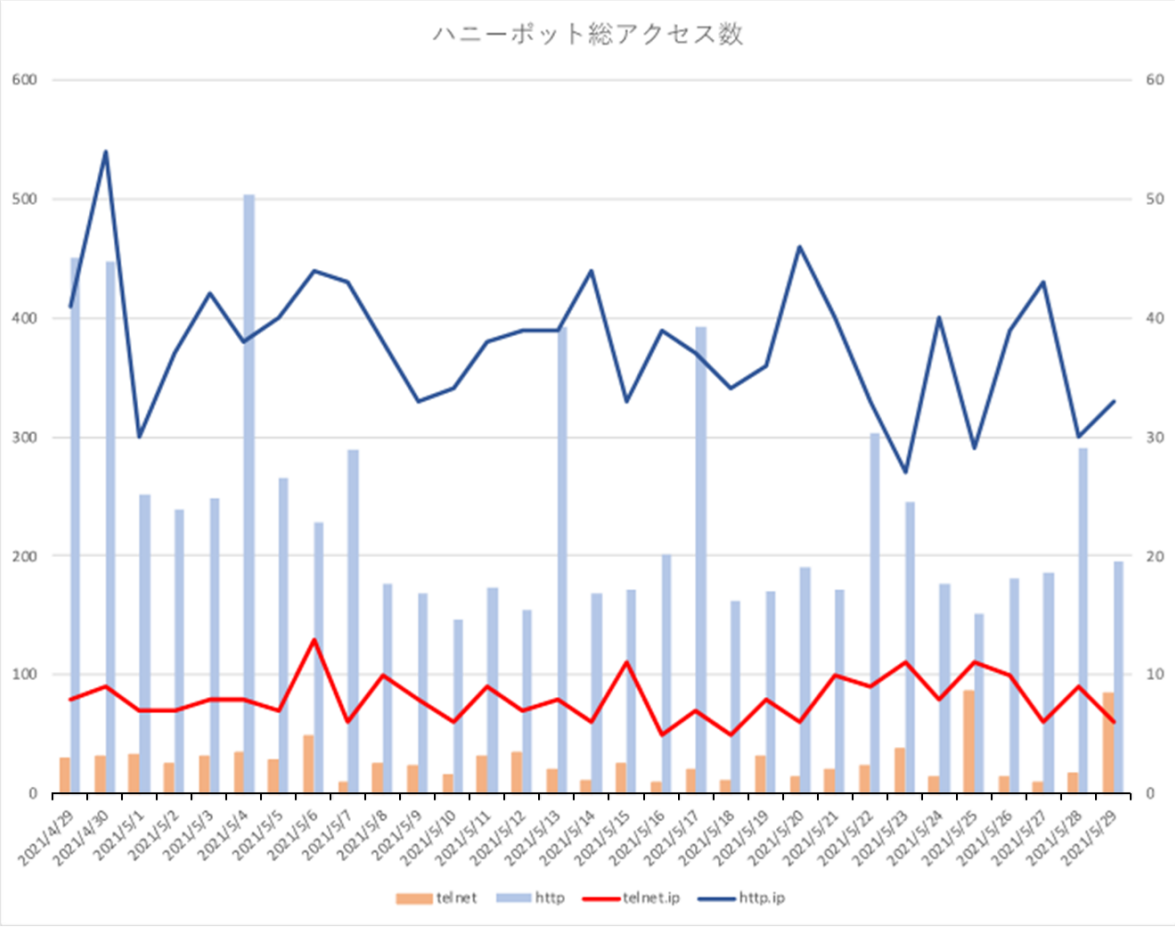
No-authentication

```
Connected

Builtins
cversion Console version
lang Set the console language
reboot Reboot

Basics
1wire Display 1wire information
iostate Display input/output state
modem Display modem state
gpspos Retrieve last GPS position
list List available modules.\n[all] List all available modu
Download result.
g Get module parameter value
s Set module parameter value
listdb List available DB parameters
gdb Get a DB parameter
sdb Set a DB parameter
logdump Display all logs
```

Jose Carlos Norte. Hacking industrial vehicles from the internet: http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html（参照 2023.02.22）

ハニーポットの観測結果

今回は、車載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、結果的に車載機の動作に影響する攻撃を受けるおそれがあることが確認できた。



今後の展望

本手引きを参考にすることで、能動的な自動車業界の脅威情報収集が進むことを期待している。なお、今後の方針や、更なる研究や注力する分野としては、以下等が考えられる。

- 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
- 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

社会実装に向けた活動

展開先であるJ-Auto-ISACと技術検討会を5回、また、「情報共有システムの基本仕様書」と「情報収集の手引き」それぞれの引受担当者と意見交換会を開催し、フィードバックをいただいた。成果物は2023年にJ-Auto-ISACに利用許諾契約にて展開。

成果物	展開先	今後の展望
情報共有システムの基本仕様書	J-Auto-ISAC	• J-Auto-ISACにて、現状の情報共有活動と、「仕様書」に記載のあるべき姿を照らし合わせ、情報共有活動の改善点について検討する。 • US-Auto-ISAC等の国内外の組織との連携を見据え、脅威情報の構造化について検討を進める。 • 引き続き、US-Auto-ISACや他組織との意見交換会を行い、最新技術動向に関する情報を収集する。
情報収集手引き	J-Auto-ISAC	• 今後、J-Auto-ISACが自動車に関する脅威情報をプロアクティブに収集し、会員に発信する際の参考情報として「手引き」を活用する。 • J-Auto-ISACの会員に対して「手引き」を公開することで、OEMやサプライヤーが自社製品に関する脅威情報を収集する際の参考情報として提供する。

日独連携

ドイツの自動運転セキュリティ開発支援動向

ドイツでは、連邦教育・研究省(BMBF)が主導で、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。本プロジェクトは、「SecForCARs」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。
- 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）

https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/it-sicherheit-und-autonomes-fahren

日独連携ワークショップ

計5回の日独連携ワークショップ開催し、日独双方の研究内容の共有や各国の自動車業界の状況等の情報交換を行った。

時期, 場所	会議名	アジェンダ
2021/7 オンライン	WS1	• Threat intelligence and Vehicular honeypots • Concept and demonstration for integrated OTA software update • IDS management concept for distributed IDS
2021/12 オンライン	WS2	• Threat intelligence and Vehicular honeypots • Security Composition for Automotive System of Systems • Platform and Hardware Security
2022/4 オンライン	WS3	• Threat information sharing system • Discovery of exposed automotive devices • Crypto Hardware security
2022/10 対面・オンライン	WS4	• Incorporating Threat Intelligence into Automotive Trust Models • Model-based Security-Testing: Yet another Pentest? • Threat information sharing and vehicular honeypot
2023/1 対面・オンライン	WS5	• Threat information sharing and proactive information collecting for connected cars • Enhancing Automotive Security with Hardware Trust Anchors • Automotive Security Future challenges and approaches

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。