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」

2021年度分　中間成果報告書

概要版

PwCコンサルティング合同会社

2022年3月

本事業の背景・目的

車両に対するサイバーセキュリティに関して、新たなサイバー攻撃手法がBlackHatを初めとする国際会議等で継続的に報告されている。また、車両販売後の新たなサイバー攻撃手法への対策として、悪意ある第三者からの車両へのサイバー攻撃に対する侵入検知システム（以下、「IDS」という。）が注目されている。

2019 年度の調査研究では、これらを踏まえて新たなサイバー攻撃手法への対策技術として、IDS の動向調査及び基礎評価を行い、車両に対するサイバーセキュリティ技術として、IDS の必要性及び有効性が確認された。さらに、IDS の性能評価にとどまらずIDS の導入や運用面を取り入れた総合的な評価手法のニーズがあることを確認した。

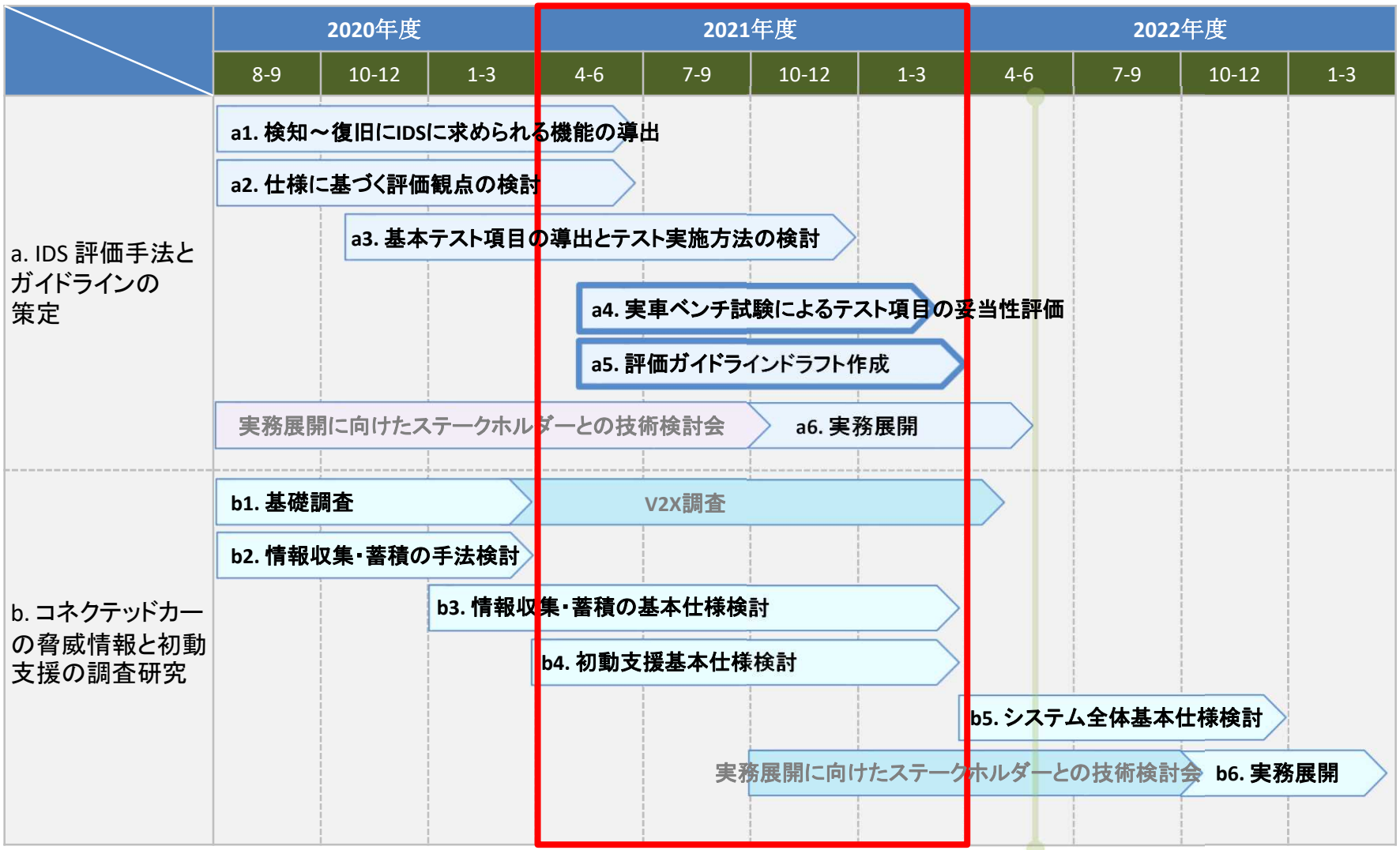
2020 年度以降は調査研究として、
「**a. IDS 評価手法とガイドラインの策定**」 及び、
「**b. コネクテッドカーの脅威情報と初動支援の調査研究**」 を行う。

本調査研究の目的と活動概要(a, b)

#	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」** 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。 • 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。 • 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。 • 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」** 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。 • 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。 • 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。

全体スケジュール

本プロジェクトの全体スケジュールは以下の通り。



本報告書は、2021年度(上図の赤枠期間)に活動した内容を記載しています。
業界団体との今後の調整次第で変更箇所が発生する可能性があります。最終的な内容は、次年度の最終報告書をご覧ください。

a. IDS 評価手法とガイドラインの策定

調査研究の目標 （再掲）

車載IDSの評価方法を判定基準も含めてガイドライン化し、2022年に業界団体に運用移管することを目標とする。

#	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」** 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。 • 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。 • 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。 • 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

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

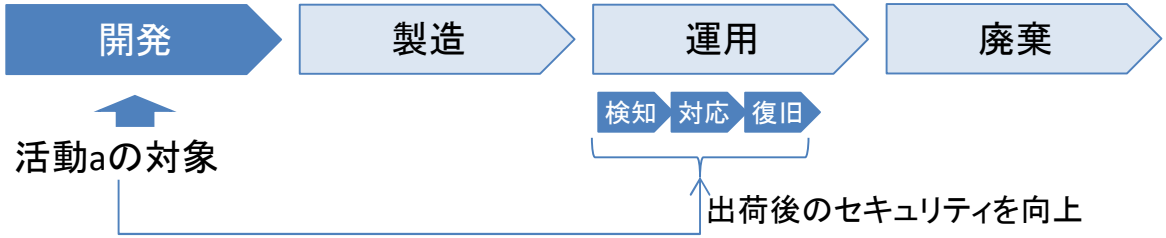
WP29 UN-R155でサイバー攻撃を検知・対処することが求められており、自社車両が検知(detect)・対処(respond)できることを説明する必要がある。

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。



活動方針：IDS評価ガイドラインのスコープ

前提として、ガイドラインの内容は、OEM/サプライヤーが検討するべき要件・評価観点であり、ガイドラインで挙げた要件を必ず満たさなければならない、ガイドラインの方法でテストをしなければならないという主旨のものではない。

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

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する。

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する。

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。

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。

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

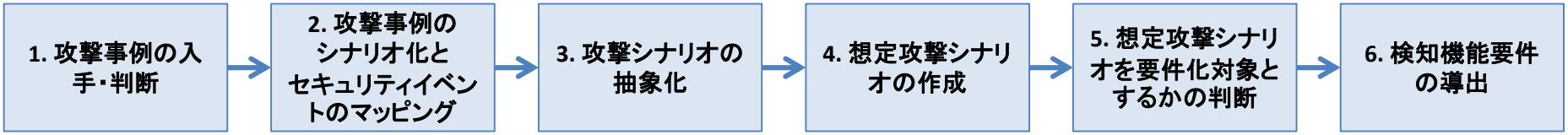
- IDS評価ガイドライン（ドラフト）

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]

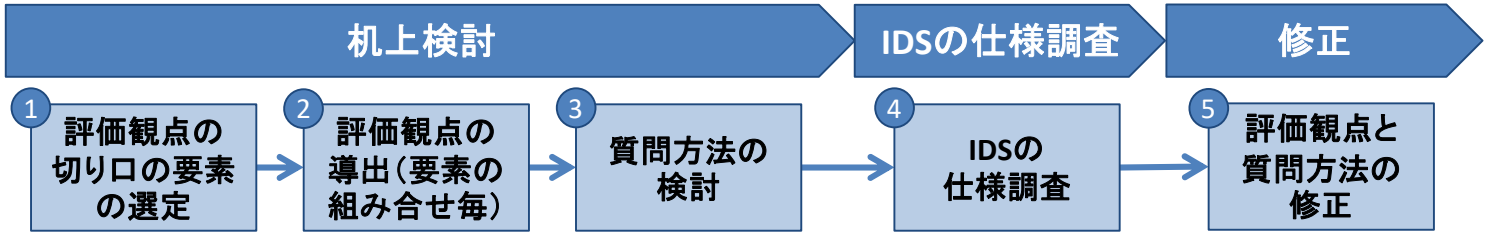
IDS基本機能の調査検討 （3/3）

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 （1/9）

「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 （2/9）

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 （3/9）

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

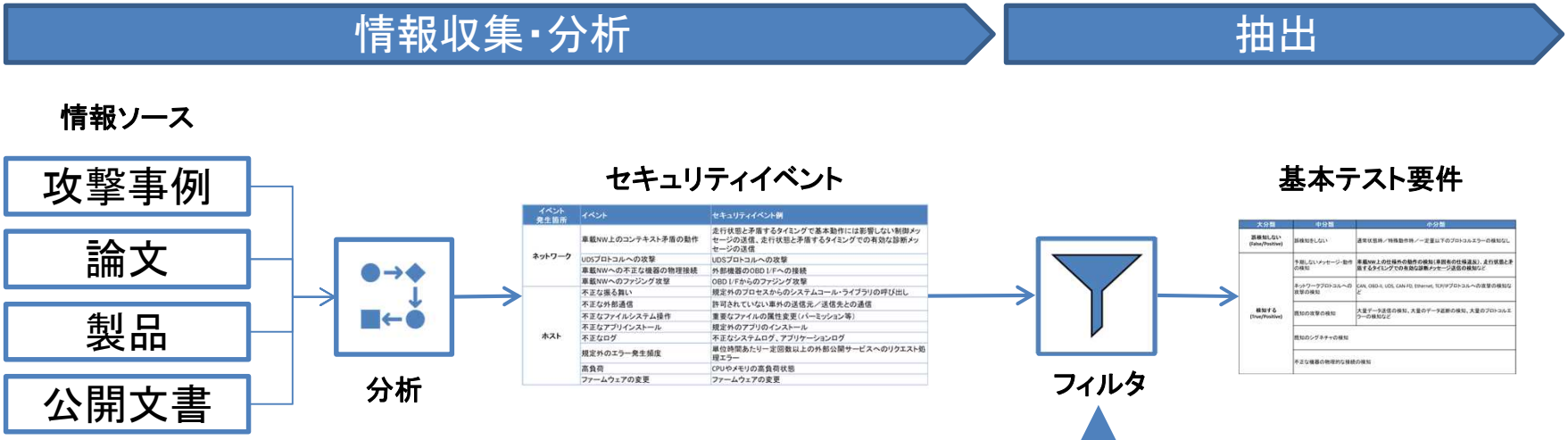
各社対応済み、もしくはカスタマイズ可能であり、基本的にはOEMの要求ベースでカスタマイズする前提である。したがって、OEMとしてIDSに要求する機能とカスタマイズ機能のフレキシビリティのギャップを知ることで、IDSの比較検討がある程度可能ではないかと考える。

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 （4/9）

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 （5/9）

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 （6/9）

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 （7/9）

基本テストケースの一例を以下に示す。

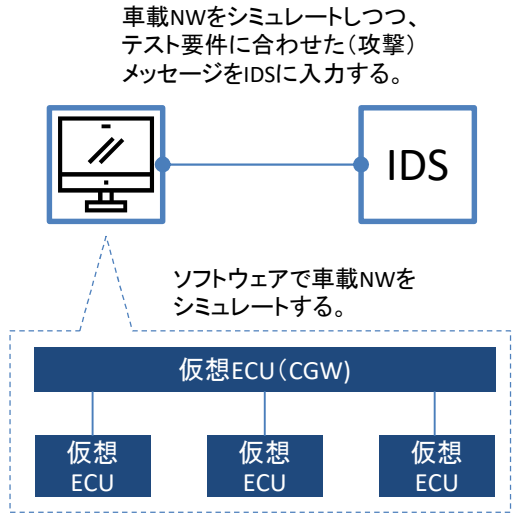
カテゴリ	項目	内容
テスト観点	テストケースID	SD-TP-1-2
	テストケース名	PT／シャシー系msg, ボディ系msgの注入による不正なデータの範囲の検知
	目的	定義された信号値の範囲に違反したメッセージが存在したとき検知することを確認する。
	検知対象SEv	不正なデータの範囲
	注入する攻撃msg種別	PT／シャシー系msg, ボディ系msg
	前提条件	走行状態：等速走行中
	導出源の攻撃事例	OBD2dongle/Wen(USENIX'20)-2 Jeep Cherokee(BH USA 2015)
テスト方法	テスト環境	シミュレーション環境
	前提とする車載NWの仕様	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 （8/9）

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。

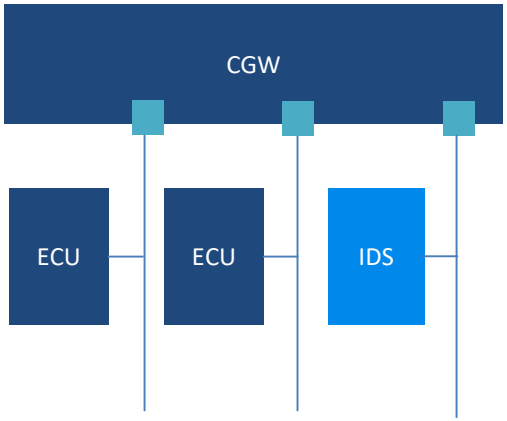
シミュレーション環境

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。



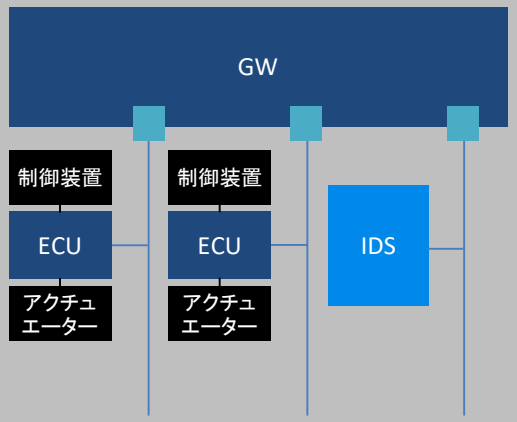
テストベッド環境

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

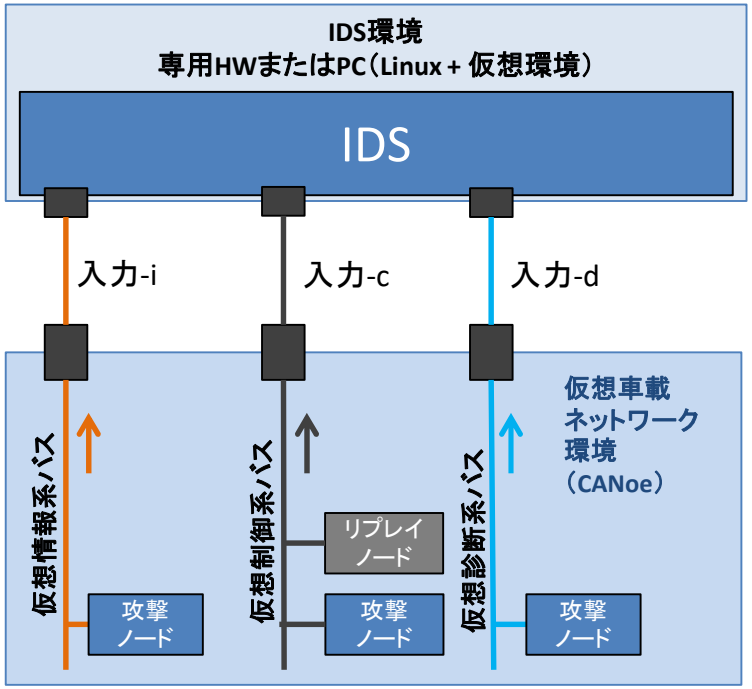
実車相当の入力装置、ECU、アクチュエーターを接続した環境。



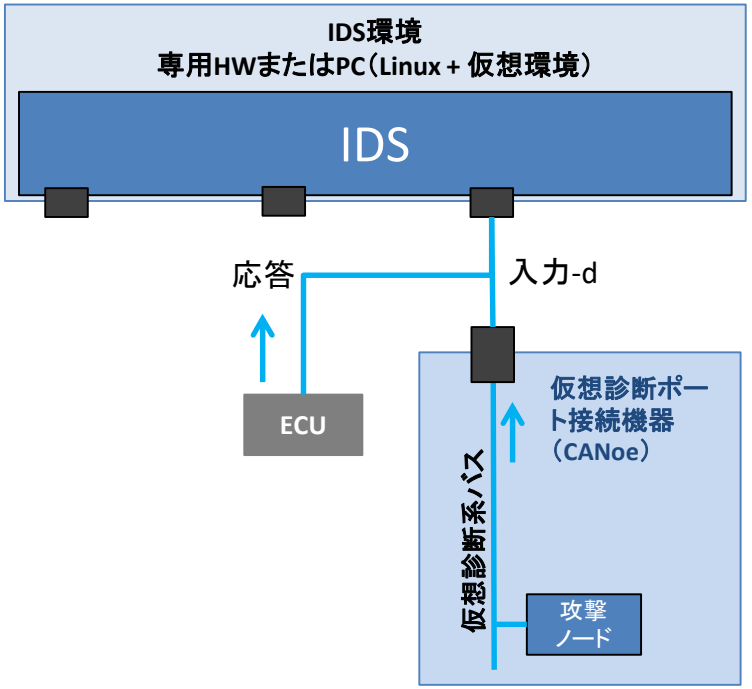
基本テストケースの検討 （9/9）

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

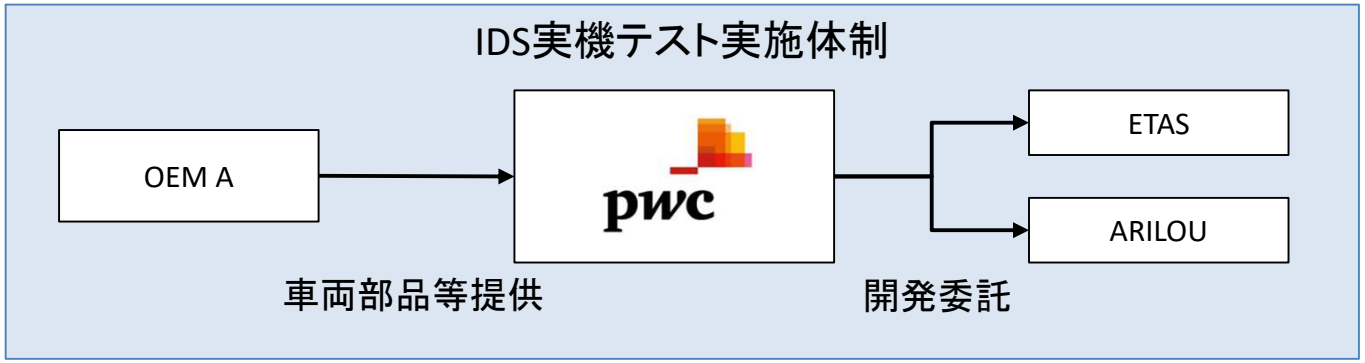


テストベッド環境



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および契約形態について以下に示す。



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

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、貸与された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）

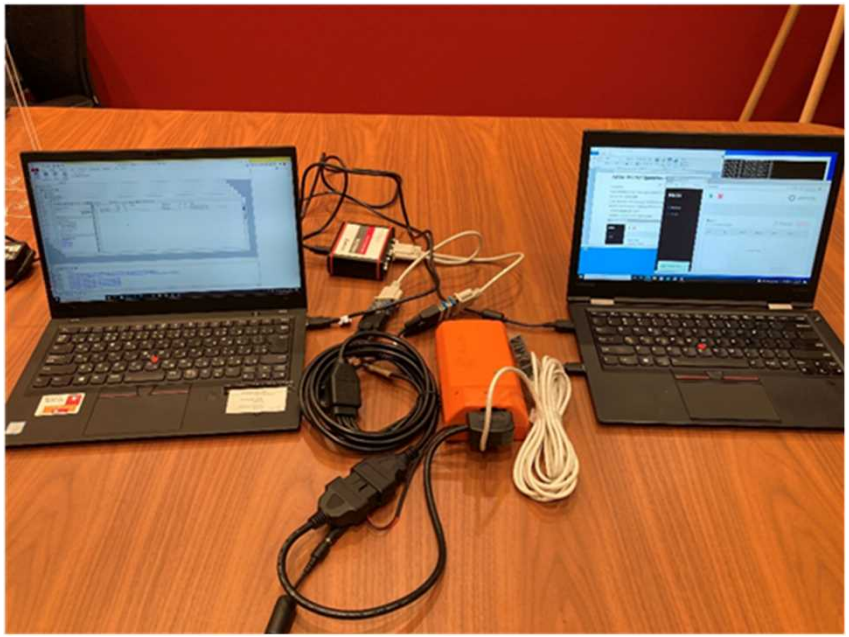
ベースIDSの仕様による対象外とした理由（前スライド*1～3）を以下に示す。

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。

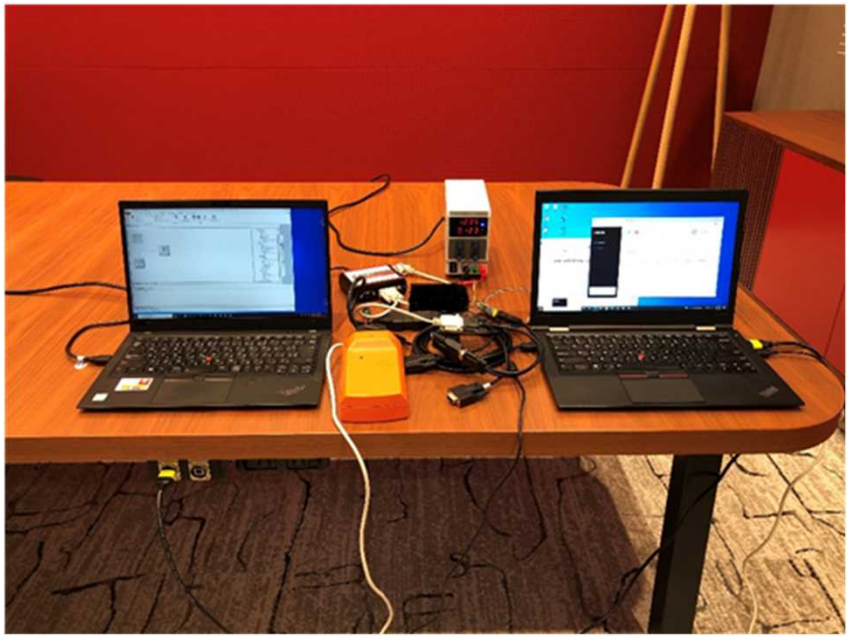
IDS実機テストによるテストケースの検証 （5/5）

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



実務展開に向けた活動

ガイドラインの移管に向けて、技術検討会を合計8回開催し、移管先であるJASPARからガイドラインに関するご意見を伺い、フィードバックを行った。開催実績は以下の通り。

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

実務展開に向けた活動

ガイドラインの移管について内諾は得ているが、具体的な事務手続きは2022年5月末を予定している。また、実機テストや内容検討などの実質的な調査研究は3月末で終了しているが、JASPARからのフィードバック対応は移管直前まで実施する。

#	作業・手続き	実施主体	ステータス
1	SIP版ガイドラインの最終化	対応：PwC レビュー：JASPAR、IDS評価ガイドライン想定読者	5月末までに修正予定することでJASPAR、SIPと合意。
2	移管に関する契約内容の決定	NEDO、JASPAR	調整中
3	移管	PwC、NEDO、JASPAR	5月末予定

b. コネクテッドカーの脅威情報と初動支援の調査研究

調査研究の目標 （再掲）

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対応支援の基本仕様を策定し、2023年に業界団体に運用移管することを目標とする。

#	公募要領／仕様書に記載の目的概要	目標
b	**「コネクテッドカーの脅威情報と初動支援の調査研究」** 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。 • 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。 • 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。

活動b 調査研究アプローチ

脅威インテリジェンスを活用したインシデント対応で先行するIT領域の脅威インテリジェンス活動を基礎として、自動車領域への応用を検討する。

IT領域の脅威インテリジェンス調査

1. 基礎調査

自動車領域に応用するために、IT領域の脅威インテリジェンス活動を以下の観点から調査する。

(1-1)脅威インテリジェンス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？

(1-2)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？

自動車領域の脅威インテリジェンスへの応用検討

2. 情報収集・蓄積の手法検討

自動車領域で、IT領域の脅威情報の収集・分析手法や初動対応支援を、応用する手法を検討し仮説を立てる。
その際に、脅威インテリジェンスの形成に影響する可能性がある、ITと自動車の違いに着目する。

3. 情報収集・蓄積の基本仕様検討

実証実験を行い、自動車業界における、情報収集・蓄積手法を検討する。

4. 初動対応基本仕様検討

自動車業界で、3で実証した手法で得られたインテリジェンスを活用し、初動対応支援する手法を検討する。

業界への実務展開

5. システム全体仕様検討

自動車業界として、3の手法で脅威情報を収集・分析し、その情報を共有し、4の手法で初動対応支援する仕組みを運用するための、課題と解決策を検討する。

6. 実務展開

5で検討した仕組みを業界団体に実務移管するための計画を作成する。

2020年度目標へのアプローチ概要

2020年度は、IT領域の脅威インテリジェンス活動を調査し、自動車領域へ応用を検討した。自動車の脅威情報収集手法の仮説を作成した。

1 基礎調査

- IT領域の脅威インテリジェンス活動を情報収集・分析手法の観点、初動対応支援の観点から調査する。

(1-1)IT領域の脅威インテリジェンス
・脅威インテリジェンス活動
・提供される脅威情報の例
・初動対応への活用

(1-2)脅威情報収集・分析手法
(1-1)の情報をどのように収集するか ？
・情報収集手法
・分析の観点

INPUT

- IT領域の脅威インテリジェンス活動

OUTPUT

- **(1-1)IT領域脅威インテリジェンスの例、脅威インテリジェンス用いた初動対応支援**
- **(1-2)IT領域の脅威情報収集手法・分析手法**

2 情報収集・蓄積の手法検討

- IT領域の情報収集・分析手法を自動車領域に応用するための課題を挙げ、課題を解決するための仮説を立てる。

(1-2)IT領域の情報収集・分析手法

↓

自動車領域とIT領域の相違点の考慮

(2-1)自動車領域の情報収集・分析手法（仮説）

INTPUT

- (1-2)IT領域の情報収集・分析手法
- ITと自動車領域違いに関する考察

OUTPUT

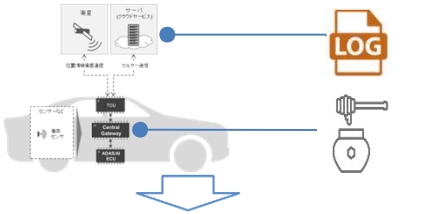
- **(2-1)自動車領域の情報収集・分析手法仮説**

2021年度目標へのアプローチ概要

2021年度は前年に作成した仮説に基づき、実証実験を行った。収集した脅威情報を活用した初動対応支援の仕様を検討した。

3 情報収集・蓄積の基本仕様検討

- ②で作成した計画を基に実証実験を実施し、捕捉方法の有効性を評価する。



INPUT

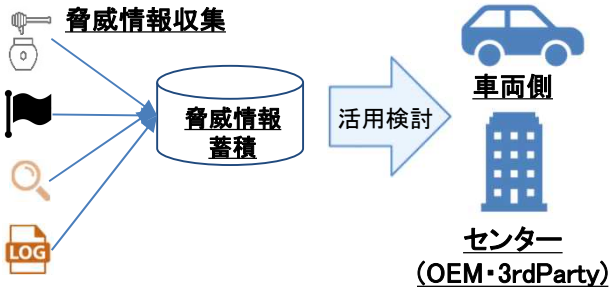
- サイバー攻撃捕捉・収集手法実験計画

OUTPUT

- **実証実験結果**
- **サイバー攻撃捕捉・収集手法の有効性評価**

4 初動支援基本仕様検討

- ③で検討した方法で収集・蓄積した脅威情報を初動対応に活用する方法を検討する。



INTPUT

- サイバー攻撃捕捉・収集手法の有効性評価
- IT領域における脅威情報活用事例

OUTPUT

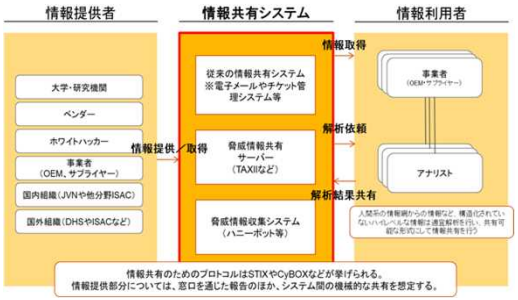
- **自動車における初動対応への脅威情報の活用案**

2022年度目標へのアプローチ概要

2022年度は、脅威情報を業界として脅威情報を収集、分析、共有する仕組みを検討し、業界団体への実務移管計画を検討する。

5 システム全体基本仕様検討

- 自動車業界における脅威情報収集・共有活動を円滑に運用するために、IT業界の事例を参考に活動を設計する。



INPUT

- IT領域の脅威情報共有活動の運用事例
- ステークホルダーとの意見交換

OUTPUT

- **自動車の脅威情報共有活動の運用設計案**

6 実務展開

- 実務展開に向けて、運用移管先と意見交換を踏まえて、運用計画案を作成する。

INTPUT

- 自動車の脅威情報共有活動の運用設計案
- 運用移管先との意見交換

OUTPUT

- **脅威情報共有活動の運用計画案**

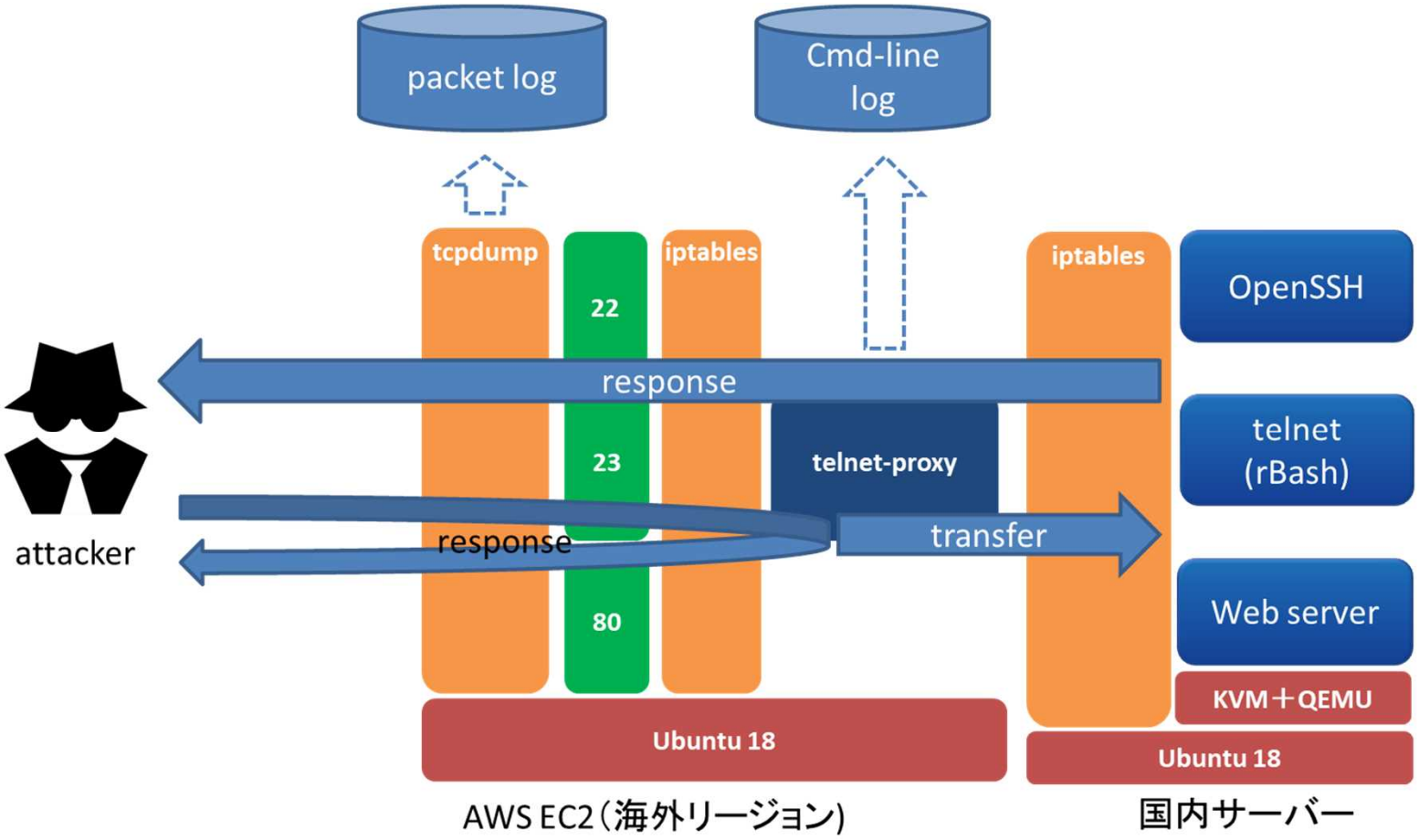
脅威情報収集手法

自動車領域における脅威情報の収集・蓄積手法を確立するため、IT領域での実施事例を参考に、脅威情報観測実験を行う。
本活動では、ハニーポットおよびCTFに着目し、調査研究を行う。

目的	• 自動車領域における脅威情報の収集・蓄積手法を確立する。
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 / CTF / 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	• コネクテッドシステムへの攻撃パターンを整理し、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、実際の観測実験を通して評価する。

ハニーポット実証実験

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。



インターネットから発見可能な機器

車載ルータやゲートウェイなど12機器がインターネット広域スキャンにより発見された。

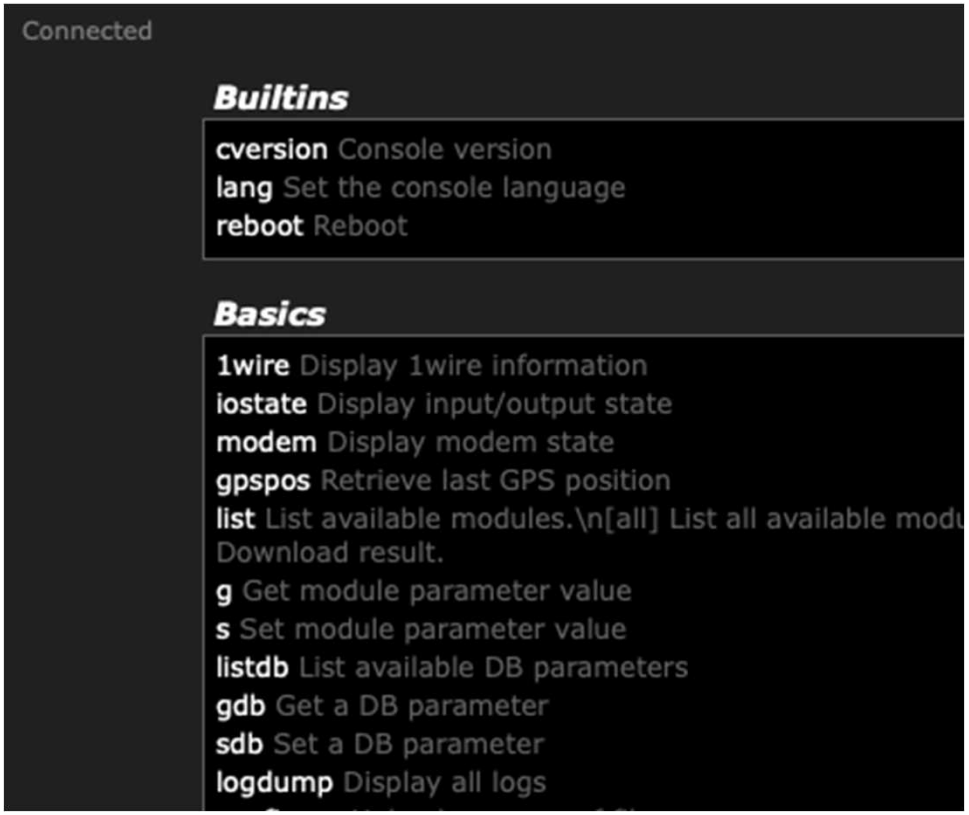
device name	Web-base/Cluster-base	#devices	Discovered countries	Open ports
製品A	Cluster-based	278	NL 26.0% SE 18.9% US 16.3%	22/tcp 80/tcp 8080/tcp
製品B	Cluster-based	391	ES 59% MA 20.3% DE 11.9%	22/tcp 23/tcp 80/tcp
製品C	Web-search-engine-based	821	US 96.5% BR 2.2%	8443/tcp 22/tcp 8080/tcp 80/tcp 443/tcp
製品D	Web-search-engine-based	186	IT 59.1% DE 40.0%	80/tcp or 81/tcp 21/tcp 22/tcp
製品E	Web-search-engine-based	88	DE 95.6%	80/tcp 22/tcp 23/tcp
製品F	Both	104	US 60.0% ES 11.8% AU 10.0%	2332/tcp 9191/tcp 9443/tcp
製品G	Web-search-engine-based	5	TW 100.0%	161/tcp
製品H	Web-search-engine-based	360	ES99.4%	80/tcp
製品I	Web-search-engine-based	3	DE 100%	21/tcp 80/tcp 443/tcp
製品J	Web-search-engine-based	67	US 51.5% FR 19.6% CN9.6%	2332/tcp 9191/tcp 9443/tcp
製品K	Web-search-engine-based	144	ES 99.9%	21/tcp 22/tcp 80/tcp 123/tcp
製品L	Web-search-engine-based	85	us 84.3%	8443/tcp 22/tcp 8080/tcp 80/tcp 443/tcp

インターネットから発見可能な機器例

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

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

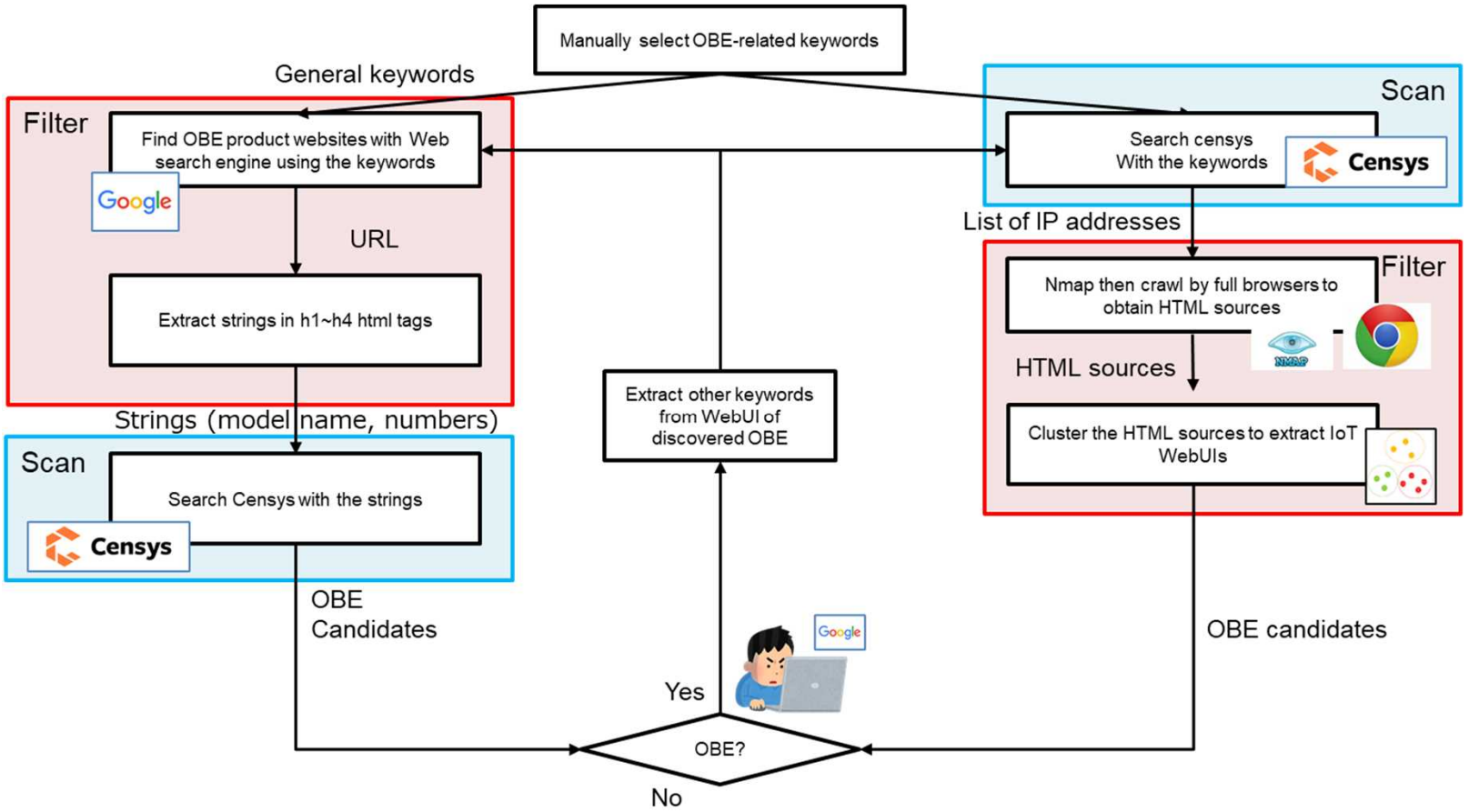
No-authentication



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

機器探索の方法論について

車載機器の探索を効率的に行うため、Web検索エンジンを用いてキーワード検索を行い、車載器製品のWebサイトを検索するアプローチと、車載器関連のキーワードを直接Censysで検索するアプローチの2つを実施した。

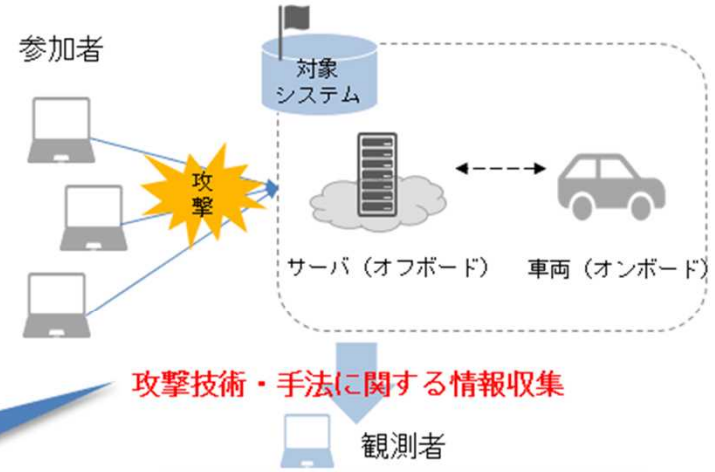


プレイグラウンド(CTF)の実施について

コネクテッドシステムにおいて、どのような攻撃を受ける可能性があるかを知るため、プレイグラウンドを実施し、参加者の挙動・攻撃手法からコネクテッドシステムに対する攻撃の知見を得る。

目的	• 自動車のコネクテッドシステムに対して、どのような攻撃が成立し得るかを調査する。 • どのようなアクティビティが「車両を狙った攻撃」に該当するのか、判断基準を検討する。
実施方針	• 車両の制御や車両情報の取得等をターゲットとし、参加者は対象システムに対して攻撃を試行する。 • 攻撃者の攻撃技術・手法等の観測結果から、攻撃を素早く検知するための知見を得る。

実施イメージ



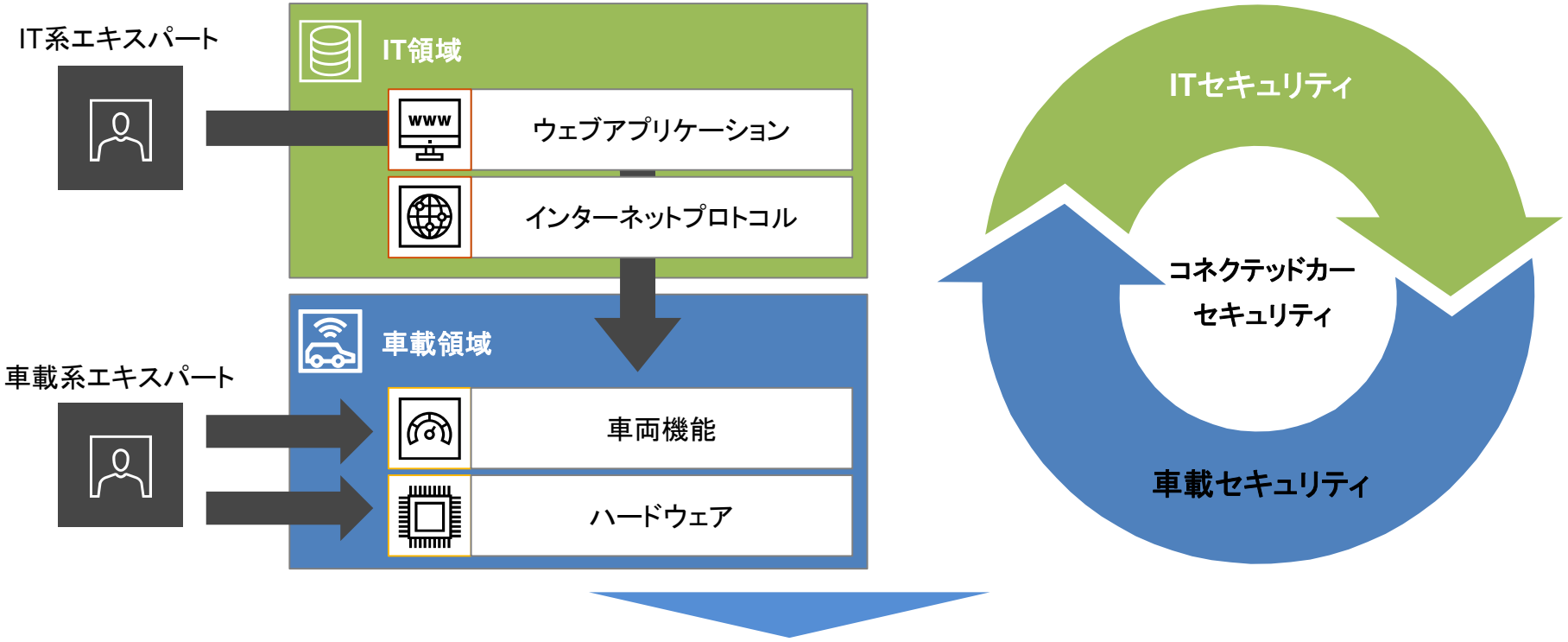
車載機（自動車）ハニーポット開発や、運用時の攻撃を分析する際の判断基準作りなどに活用する。

CTF開催・Honeypot運用により、コネクテッドカー関連の脅威情報・動向をPwC独自に、継続して得ることが期待できる。

脅威情報記述・共有方法

効率的な脅威情報の収集および共有を行うためには、取り扱う脅威情報が一定のレベルで構造化され、共有方法が定式化されている必要がある。本活動では記述できる情報の豊富さとIT領域での活用状況を踏まえ、STIX/TAXIIに着目した。

背景：車両のコネクテッド化および自動化に伴い、既存のWeb・IT技術と連携する場面が増えている。



車両とITシステムが融合したコネクテッドシステムにおいて効率的に脅威情報を活用する仕組みとして、IT領域で最も普及しており、記載できる情報の種類が多いSTIX/TAXIIに焦点を当てて調査研究を行う。

(参考)STIXで記述可能な情報

#	分類※1	STIX情報※2	説明
1	IOC(侵害指標)	アイデンティティ/識別子	攻撃のターゲットとなった、または、なり得る実際の個人、組織、グループ、システム、業界等を表す情報。
2		インジケータ	攻撃の発生または疑義があることを示す技術的なログまたはイベントに関する情報。 ハッシュ値、IPアドレス、ドメイン名、証明書等。
3		位置情報	サイバー攻撃者、攻撃基盤、ターゲット等の攻撃に関する位置情報。
4		観測データ	ファイル、システム、ネットワークIPアドレス等のサイバー攻撃に関する情報。 インジケータ、位置情報と異なり、実際に1度以上観測された(単なる)情報を指す。
5	TTPs(戦術/戦略/手順)	攻撃パターン	サイバー攻撃者がターゲットへの攻撃に用いる方法(スピアフィッシング等)を説明する情報。
6		攻撃基盤(インフラ)	攻撃支援を目的としたシステム、ソフトウェア、物理/仮想リソース等に関する情報。 攻撃時に使用されるC2サーバやターゲットシステムの一部であるモバイルデバイス、サーバ等を記述する。
7		攻撃セット	単一のサイバー攻撃者によって作成・調整・実行されていると考えられる、共通のプロパティを持つ攻撃パターンと攻撃基盤群のグループ(セット)に関する情報。
8		マルウェア	ターゲットシステムに対して差し込まれる攻撃用のプログラム(マルウェア)がどのように機能し、何を行うかについての詳細情報。
9		マルウェア分析	マルウェアの疑義のあるプログラムに対して特定の分析を行い、結果を示す。
10		ツール	サイバー攻撃者が使用できる正当なソフトウェアに関する情報。 マルウェアと異なり、システム上に存在する正当なソフトウェアであり、サイバー攻撃者に使用される可能性のあるソフトウェアを指す。
11	セキュリティアラート	ノート	既存のSTIXオブジェクトに対して情報(ノート)を追加することで、さらなるコンテキストを提供する。
12		オピニオン	既存のSTIXオブジェクトの情報の正確性について第三者が評価したものを意見(オピニオン)という。 強く同意～強く反対までの5段階評価。
13		脆弱性	ソフトウェアおよびハードウェアの要件、設計または実装の弱点・蹴感に関する情報。
14	インテリジェンスレポート	サイバー攻撃活動	サイバー攻撃活動(キャンペーン)に関する情報。 特定のターゲットに対して一定期間に発生する一連の悪意のあるアクティビティまたは攻撃を説明する。 キャンペーンは、その目的と発生するインシデント、ターゲットとする人またはリソース、および使用するリソース(インフラストラクチャ、インテリジェンス、マルウェア、ツールなど)によって特徴付けることが可能。
15		レポート	サイバー攻撃者、マルウェア、攻撃手法の説明等、1つ以上のテーマに焦点を当てたサイバーインテリジェンスを纏めた情報。
16		サイバー攻撃者	悪意を持って活動していると考えられる個人、グループまたは組織に関する情報。 その動機、能力、目標、熟練度、過去の活動等によって特徴付けられる。
17	ツールコンフィギュレーション	行動(設定)の方針	サイバー攻撃の予防または対応のために実行すべきアクションに関する情報。 パッチの適用、ファイアウォールの再構成、従業員のトレーニングやポリシー変更等に関する情報。

STIXによる自動車脅威情報の記述

以下のアプローチに従い、4件の研究事例から得られた脅威情報をSTIX形式での記述を試みた。結果として、SITXを用いることで着目した4件の脅威情報自体は記載可能と判断した。

Report/Paper	Obtained information	STIX Object	Visualization
Search for automobile attack cases and research reports.	Analyze the reports to obtain threat information.	Make the threat information into STIX object.	Visualizing STIX object using the OASIS STIX Visualizer(*)

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

初動対応基本仕様検討

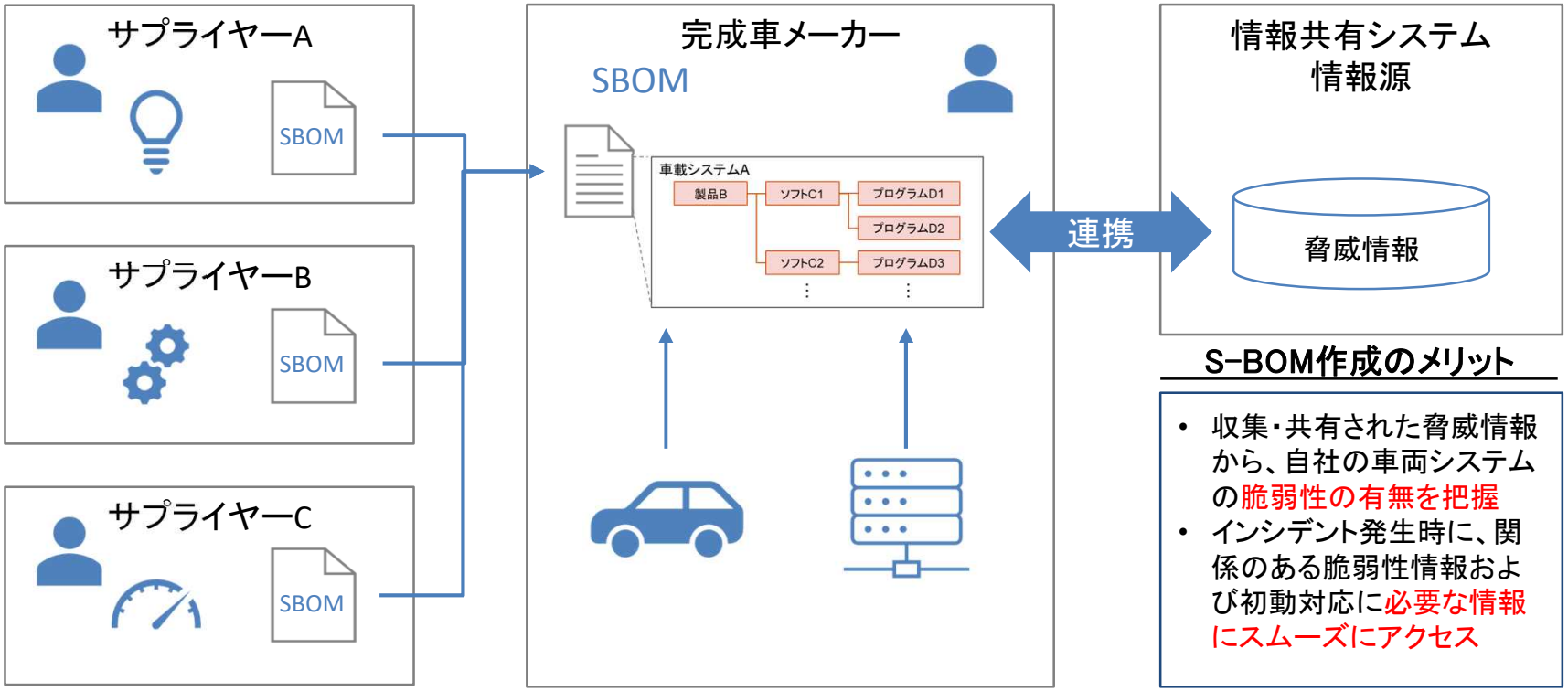
本活動における「初動」とは、平時の情報収集を通してインシデントを未然に防ぐ活動およびインシデント発生後の対応活動を指す。

	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

脅威情報の初動対応への活用

収集すべき脅威情報の選別や収集した脅威情報の該否判定を円滑に行うため、自社の製品およびシステム内のソフトウェア一覧(S-BOM)を作成する必要がある。



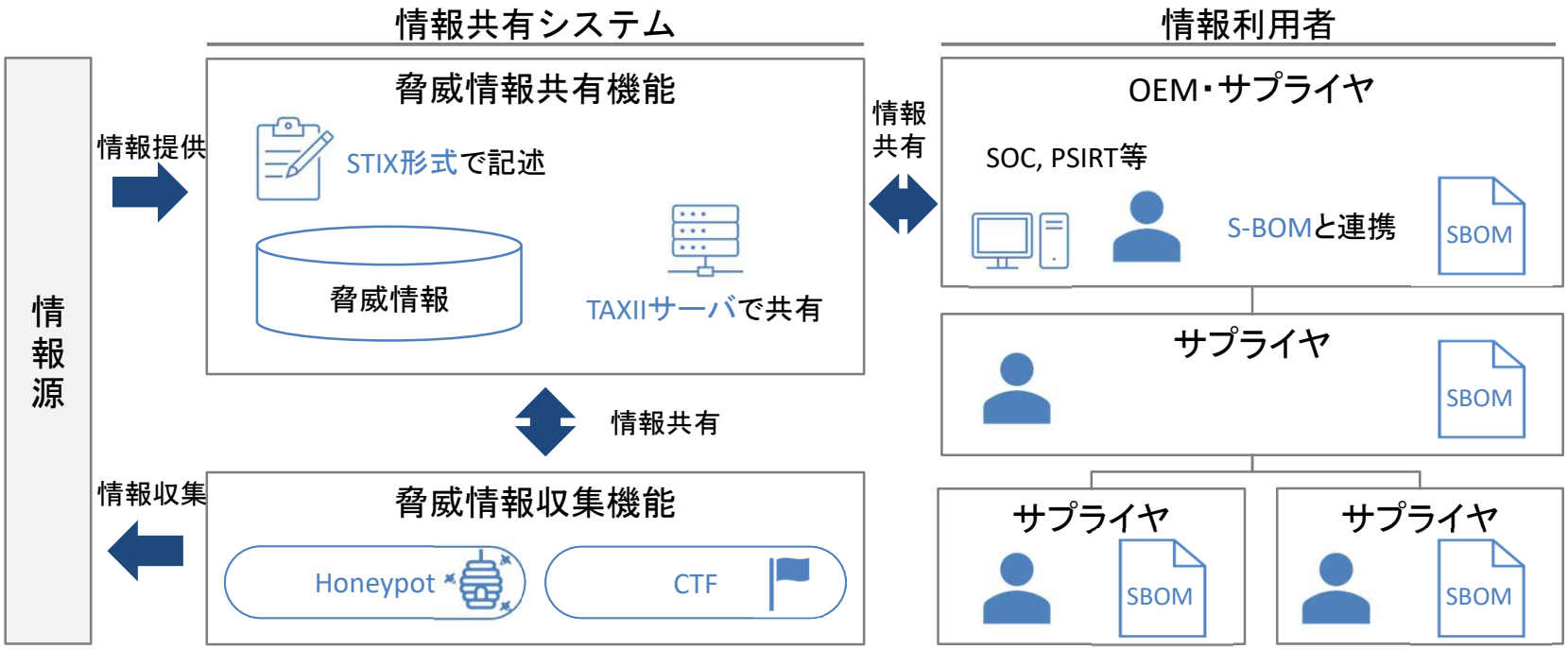
S-BOM作成のメリット

- 収集・共有された脅威情報から、自社の車両システムの脆弱性の有無を把握
- インシデント発生時に、関係のある脆弱性情報および初動対応に必要な情報にスムーズにアクセス

システム全体仕様検討

情報共有システムのあるべき像は以下の通りである。
情報の収集・蓄積・共有において各要素技術を用いることで、脅威情報を円滑に初動支援に活かすことが出来る。

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



日独連携の状況

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、現在少なくとも4つのプロジェクトが進行している。
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を計画しており、2022年4月時点で第3回までの開催が完了している。

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/秋 TBD	WS4	TBD
2023/秋 TBD	WS5	TBD

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。