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」

2020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

2021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。

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）

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
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

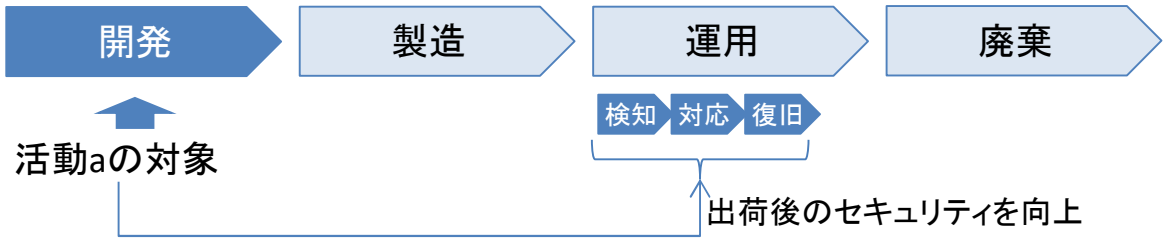
WP29 UN-R155でサイバー攻撃を検知・対処することが求められており、自社車両が検知(detect)・対処(respond)できることを説明する必要がある。

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。



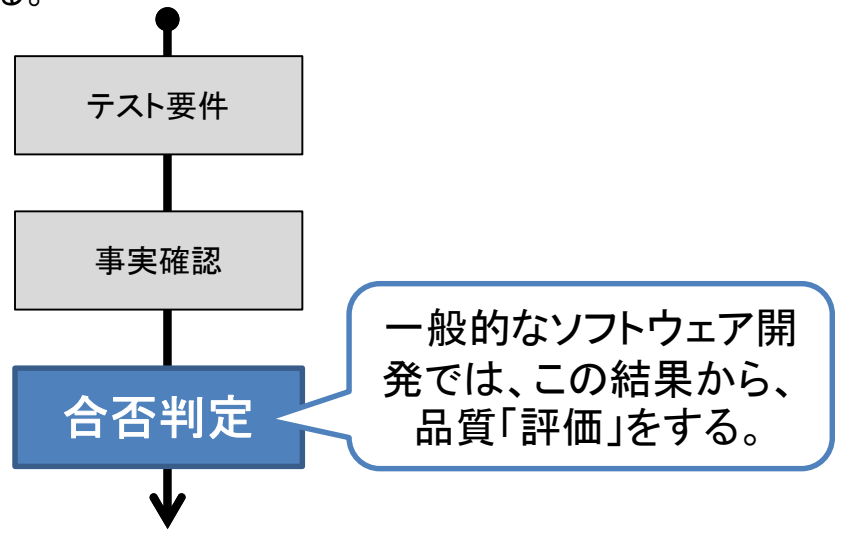
「テスト」と「評価」の定義と違い

IDS評価ガイドラインでは、IDSに対するテストと評価両方のキーワードが用いられているため、以下にこれらの定義と違いを示す。

テスト

テスト対象が期待通り動作するについて確認するために、実際のソフトウェアやハードウェアを利用し、事前に定義された方法に従って作業をし、テスト要件を満たしているか基準に従って合否判定をすること。

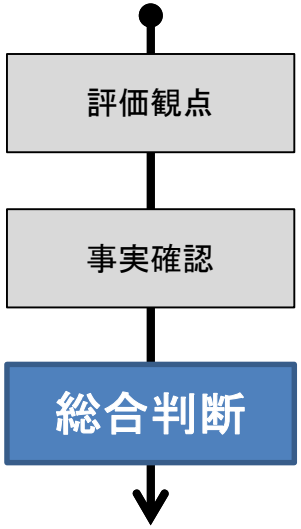
合否判定をするために必要な情報（テスト要件、作業内容、合否判定基準等）を「テストケース」とする。



評価

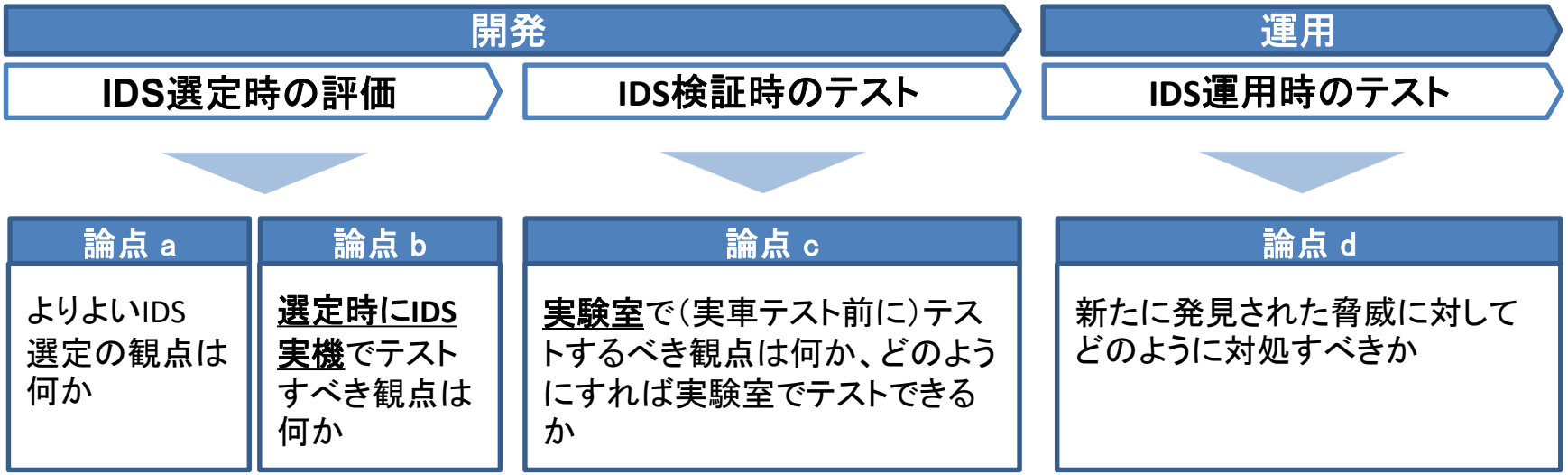
評価対象が特定環境や目的に適合するかを総合的に判断すること。

評価するときに考慮するべき観点（コスト、利便性、機能の有無や性能（機能の程度）等）を「評価項目」とする。



IDS評価ガイドラインのスコープ

よりよいIDSを選定し、実験室で可能な限りIDSの動作を検証して不具合を見つけ、新たな脅威に対応し継続して運用するために、IDSの評価に関わる1～3の活動を行う。



本プロジェクトの活動スコープ

#	活動	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

活動成果で期待される効果の考察

各活動の成果をガイドラインのコンテンツとして記載することで、業界ステークホルダーに対して、業界共通の評価・分析観点を提供するほか、実施の際に活用することでコスト削減に貢献することが期待される。

活動	想定成果 （ガイドラインのコンテンツ）	期待される効果 （仮説）
1. 仕様に基づく評価観点の検討	**仕様評価項目** IDS製品の仕様を机上で評価するときに確認するべき観点をリストアップする。	• IDS選定時における、**重要な評価観点をおさえることができる**。 • 各社のIDSを**同じ観点で比較**できる。 • ガイドラインをベースに活用することで、**仕様評価項目の作成コストを削減**できる
2. 基本テストケースの検討	**基本テストケース** IDS実機の動作を評価するために必要なテスト要件をリストアップするとともに、実車テスト前に実験室でテストをするためのテスト環境、テスト手順などを例示する。	• IDS選定時とIDSの検証初期段階に、IDSの検知機能に**致命的な問題がないことを確認**できる。 • 環境等を含む要件を示すことで、**テストの準備・実施コストを削減**できる。 • ガイドラインをベースに活用することで、**テストケース作成コストを削減**できる。
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	**新たな脅威からのテスト要件導出方法** 出荷後に新たな脅威が見つかった場合、搭載しているIDSで検知できるかを調べるための観点を導出するための方法を示す。	• 出荷後に新たな脅威が発見された場合、IDSが検知できるかを**論理的に説明可能な方法でテスト**できる。

IDS評価ガイドライン策定アプローチ概要

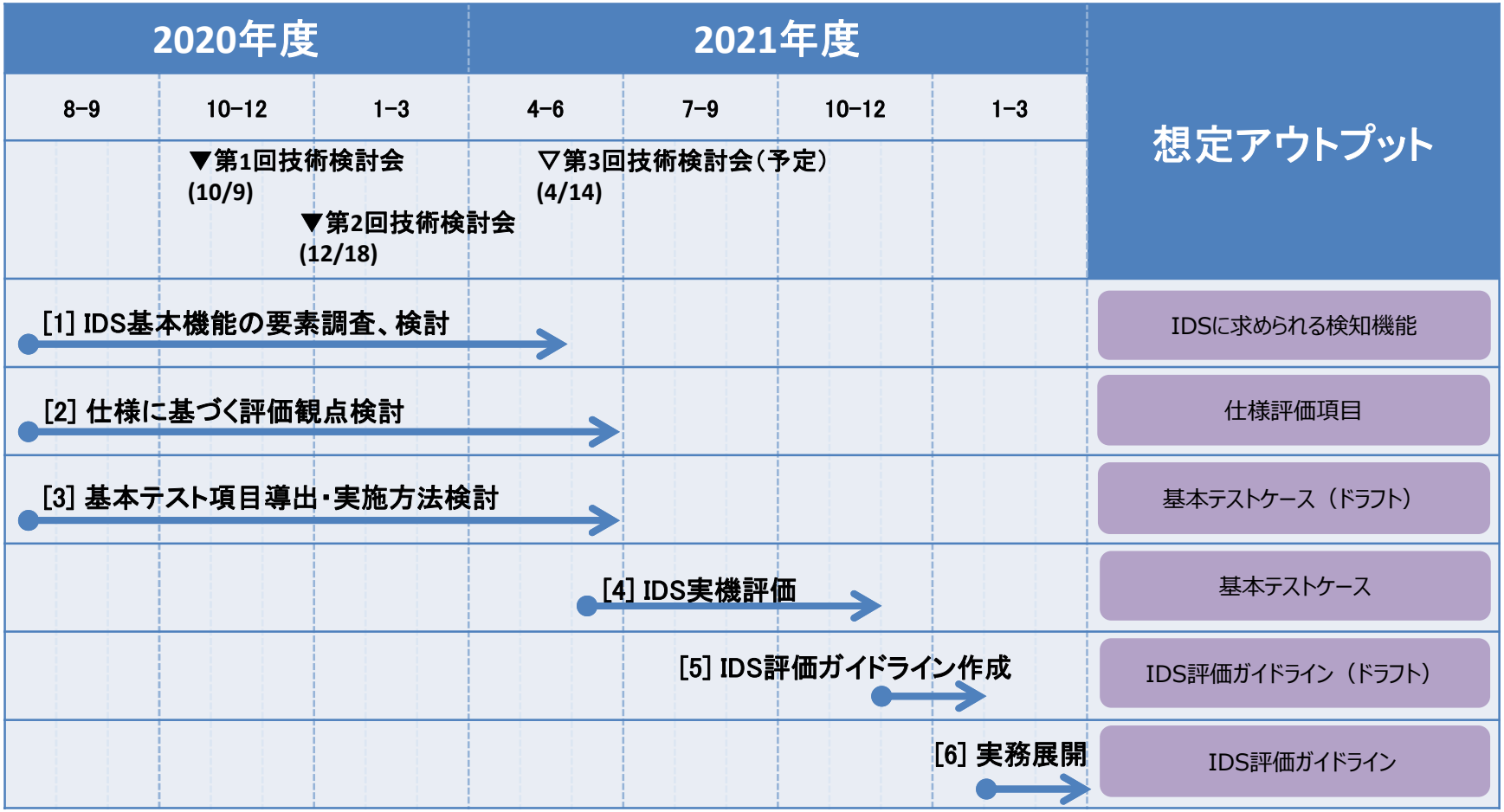
以下のアプローチでIDS評価ガイドラインを作成し、業界団体にハンドオーバーする。

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 全体スケジュール

2022年3月末に、業界団体への成果物の移管を目指すため、各年度で達成する目標を設定する。

●——→ 作業期間　▼：マイルストン（確定）、▽：マイルストン（予定）、　想定OUTPUT



活動a アプローチ (1/2)

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 (1/2)

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 (1/2)

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）

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、12件について、車両に対するサイバー攻撃として詳細に分析した。

	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**

【参考】 分析対象とした攻撃例

- **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。

- **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。

事例から導出した検知対象のセキュリティイベント

分析した攻撃事例ついて、攻撃により車載ネットワークやECUにどのような事象が生じうるのか分析し、セキュリティイベントを導出した。

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

仕様評価項目（ドラフト）

IDS選定時、OEMがIDSベンターに仕様に関する質問をする際のベースとしてご利用することを想定し、仕様評価項目と対応する質問のドラフトを作成した。IDSの比較がしやすいように、回答は出来る限り選択式とした。

仕様評価項目（ドラフト）－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）

仕様評価項目（ドラフト）－質問と選択肢（一部抜粋）

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（　　）

仕様評価項目の妥当性検証結果と考察

IDSベンダー3社（6製品）について、仕様評価項目の質問に回答いただき、ドラフトの妥当性を検証した。

仕様評価項目の回答結果サマリー

- 検知対象のセキュリティイベントについて、基本的な検知機能は概ねサポートしており※1、選択肢として挙げた粒度では仕様のレベルで大きな差異はなかった。
- CAN TP・AVB/TSNのサポート有無、シグネチャベースの検知、外部機器の接続の検知等、一部仕様については差異があった。
- ロギングまたは通知の出力項目については、各社、対応済、または、カスタマイズ対応としていた。
- 検知内容の分析に必要となるSOC（Security Operation Center）については、自社提供／協業による提供／OEMで対応等、サポート状況に差があった。

回答結果に対する考察

- 質問の回答を選択式とすることで、**必要な機能や特性を備えているかを容易に把握したり、複数のIDS製品を比較することができた**。
- **検知対象のセキュリティイベントについて、質問の粒度の仕様レベルで搭載車両への適合可否判断や各製品の差異の識別をすることは難しい。**
- サポートするプロトコル、検知アルゴリズム、外部機器の接続の検知機能の有無、SOCの対応状況等、**いくつかの仕様については容易に差異を識別できた**。
- ロギングまたは通知の出力項目については、基本的にカスタマイズ対応となっているため、**ロギング・通知項目に関する差異を識別することは難しい**。

※1. 未知の外部機器の接続については、一部サポートしていない製品があった。また、Ethernet対応製品はコンテキストレベルのセキュリティイベントの対応状況に差異があった。

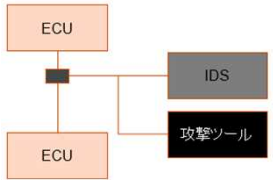
基本テストケースとは

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、テスト要件やテスト方法を下記に示す。

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
	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。

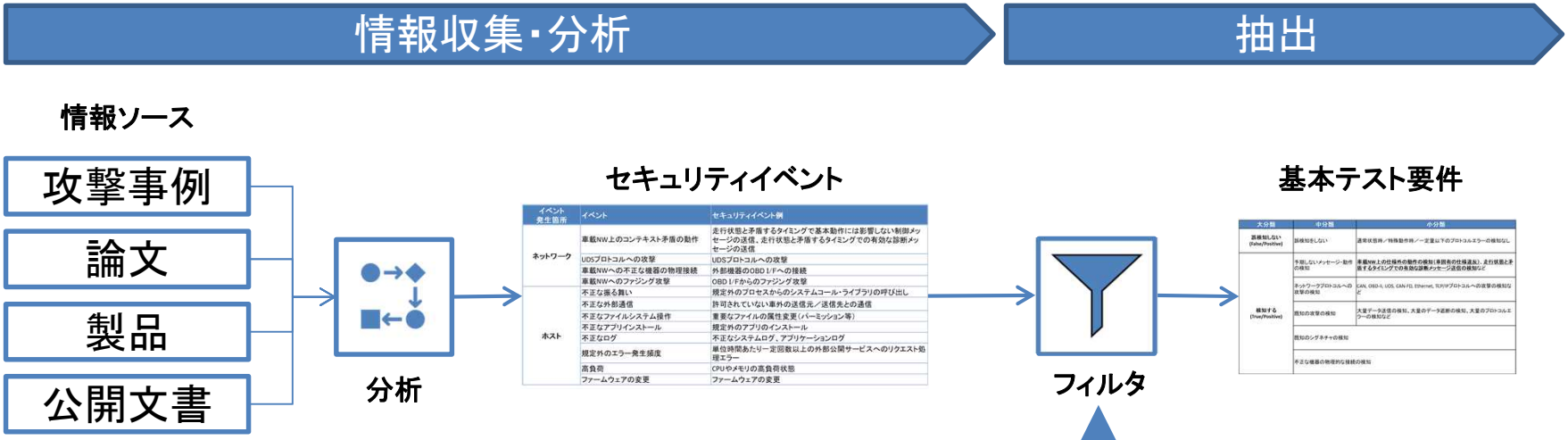
【参考】基本テストケースイメージ

「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」に対するテストケースの例を下記に示す。

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。 • メッセージにはMACは設定されていない。 • 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。 2. 電源を入れる。 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。 4. IDSの検知ログを取り出す。 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。 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： 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。

基本テスト要件の導出方法（仮）

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する。



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テスト要件一覧（ドラフト）

NIDS用のテスト要件のドラフトの概要を下記に示す。論文からは、「車載NW上の仕様外の動作の検知」、事例からは「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」などを追加した。

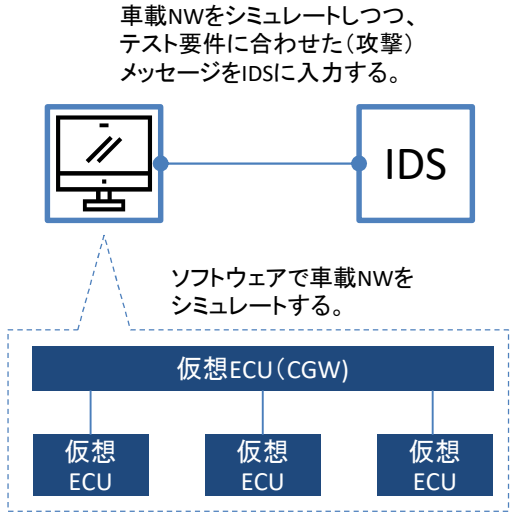
大分類	中分類	小分類
誤検知しない (False/Positive)	誤検知をしない	通常状態時／特殊動作時／一定量以下のプロトコルエラーの検知なし
検知する (True/Positive)	予期しないメッセージ・動作の検知	**車載NW上の仕様外の動作の検知（車固有の仕様違反）、走行状態と矛盾するタイミングでの有効な診断メッセージ送信の検知**など
	ネットワークプロトコルへの攻撃の検知	CAN, OBD-II, UDS, CAN-FD, Ethernet, TCP/IPプロトコルへの攻撃の検知など
	既知の攻撃の検知	大量データ送信の検知、大量のデータ遮断の検知、大量のプロトコルエラーの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

【参考】 IDSテスト環境の種別と考察

ドラフトしたIDS基本テストケースの実行環境として、以下の選択肢が挙げられる。
今後はこれらのいずれか、あるいは組み合わせを踏まえてテストケースの検証を行っていく予定である。

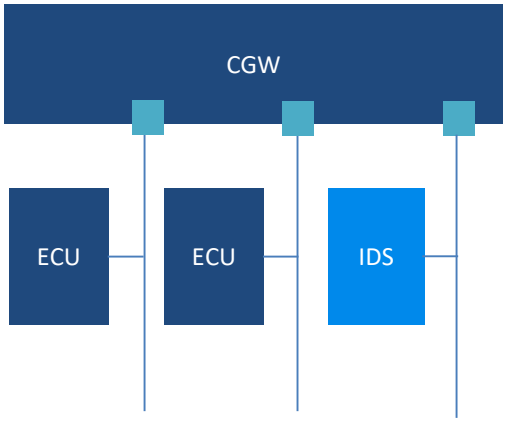
シミュレーション環境

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。



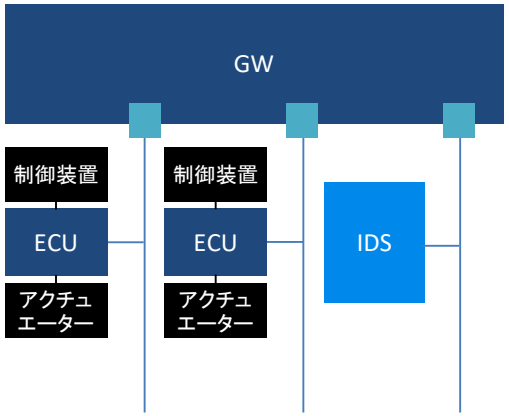
テストベッド環境

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。



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。

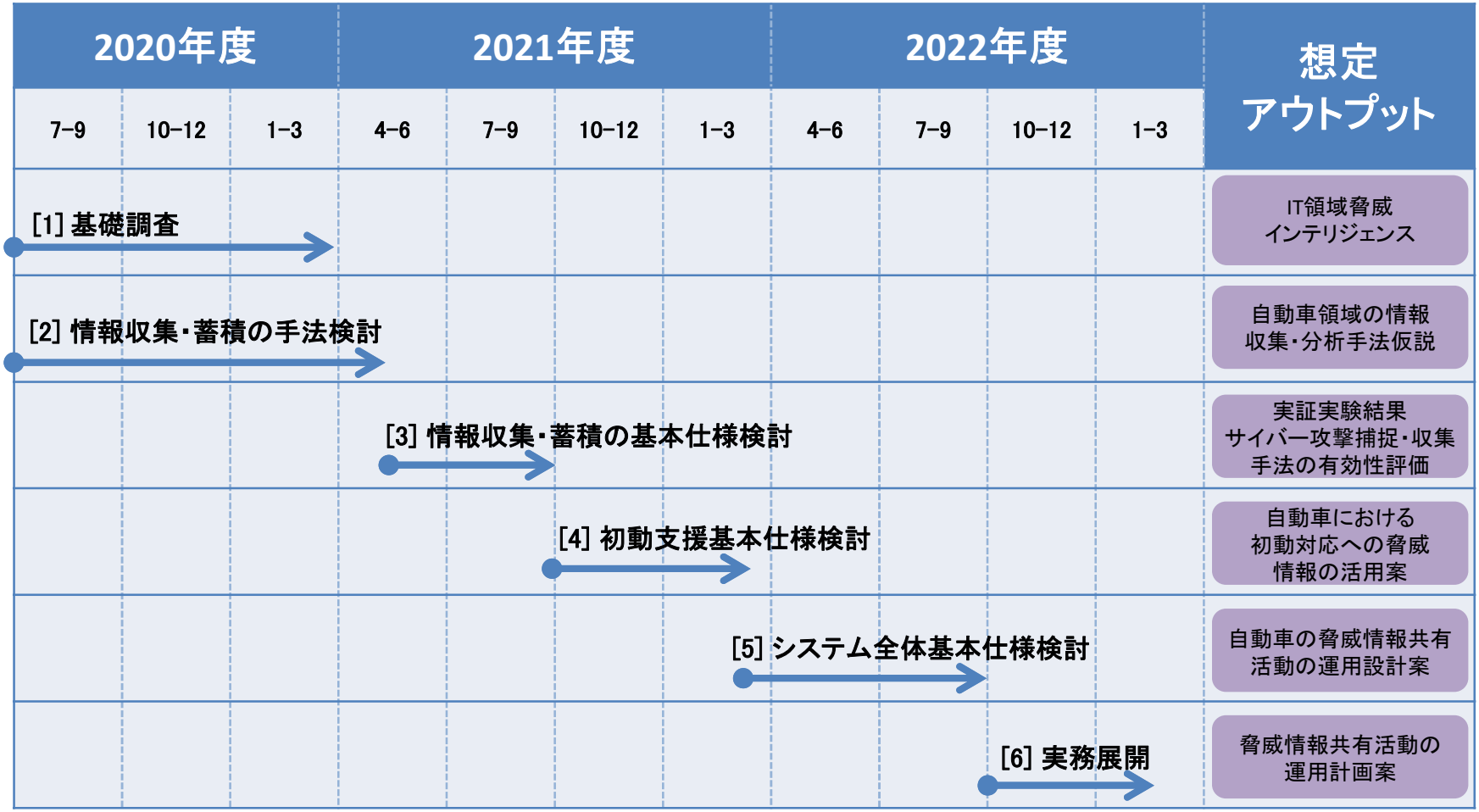
6. 実務展開

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。

活動b 全体スケジュールと各年度の目標

2023年3月末に、業界団体への成果物の移管を目指すため、各年度で達成する目標を設定する。

●——→ 作業期間　▼：マイルストン（確定）、▽：マイルストン（予定）、　想定OUTPUT



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

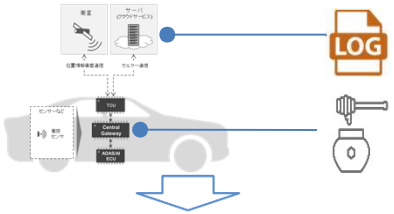
- **(2-1)自動車領域の情報収集・分析手法仮説**

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、実証実験を行う。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する。

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、補足方法の有効性を評価する。



INPUT

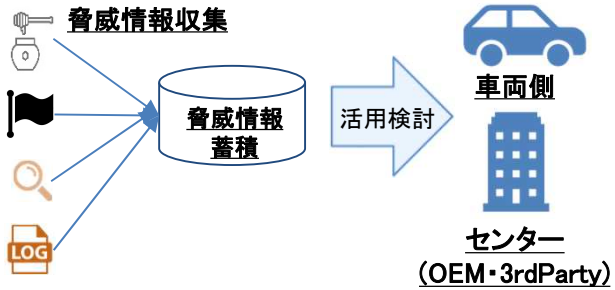
- サイバー攻撃捕捉・収集手法実験計画

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

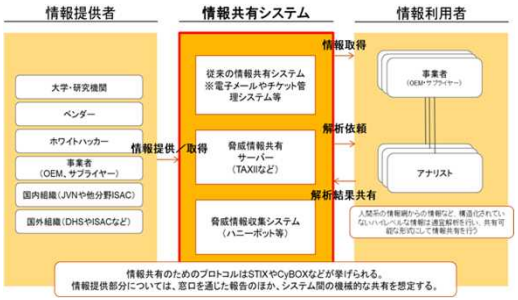
- **自動車における初動対応への脅威情報の活用案**

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

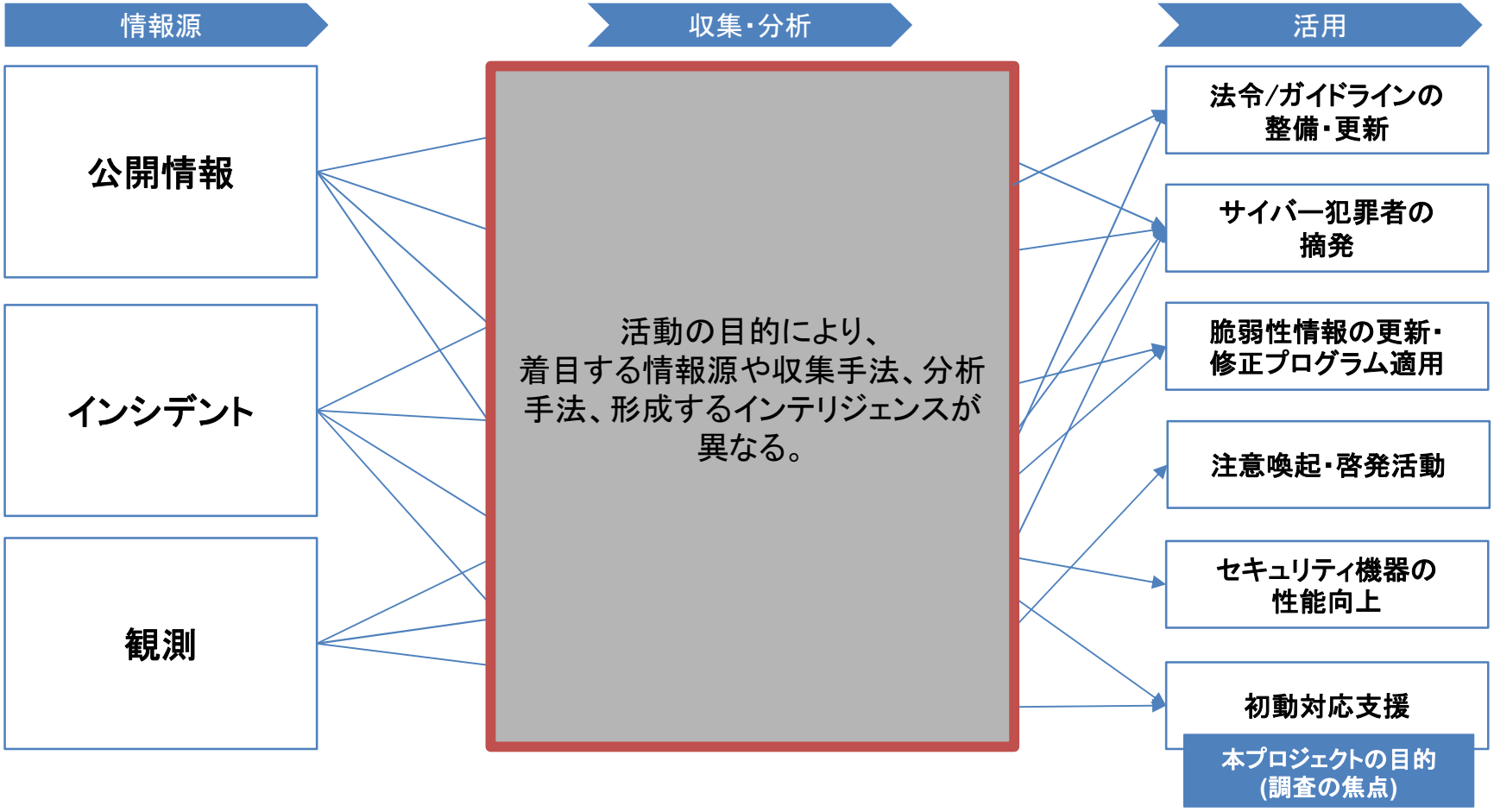
- 自動車の脅威情報共有活動の運用設計案
- 運用移管先との意見交換

OUTPUT

- **脅威情報共有活動の運用計画案**

脅威インテリジェンスの調査方針

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。



脅威インテリジェンスを活用したインシデント対応

先述の脅威インテリジェンスがどのようにインシデント対応に活用されているか、NIST CSFの各フェーズでの活用例を以下に示す。

	特定	防御	検知	対応・復旧
①インジケーター サイバー攻撃によって観測された具体的な事象		サイバー攻撃で、利用された、IPアドレス、URL、ドメインをブラックリストに入れてブロックする。	サイバー攻撃で観測されたイベントから、セキュリティイベントを定義し検知する。	IPアドレス、ハッシュ値など攻撃の痕跡を照合し、サイバー攻撃か判断し、対応・復旧を策定する。
②TTP(戦術、戦略、手順) 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	標的になりうる情報資産やシステムを特定し、サイバー攻撃を受けた場合の影響度を評価する。	攻撃シナリオを作成し、対応訓練を行う。	TTPに特有のふるまいを定義し、不審な動作を検知する。	
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の情報	脆弱性のあるシステムや、悪用された場合の影響度を評価する。	脆弱性のあるシステムに、修正プログラムを適用する。		
④インテリジェンスレポート 組織の状況認識を高める脅威関連情報を記述したドキュメント	自組織に関連する脅威を特定し、ビジネスへの影響度を評価する。			
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ツールの設定		攻撃を防御・検知・復旧するために、①～④から得られた情報から、セキュリティツールの設定を定義し、ポリシーとして配信する。		

脅威情報共有活動の考察

一部の産業では、インシデントの発生防止や適切な初動対応など、共通の目的を持ち、企業横断的に脅威情報共有活動が行われていた。

産業横断的な情報共有

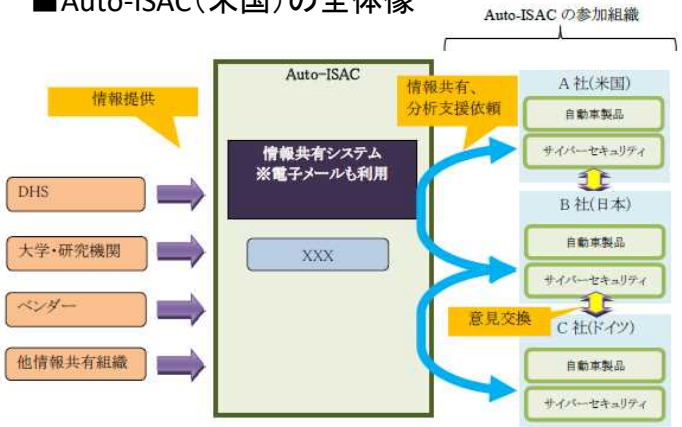
■CiSP（英国）の全体像

■DHS（米国）の全体像

産業内の情報共有

■Healthcare Ready（米国）の全体像

■Auto-ISAC（米国）の全体像



本プロジェクトでは、複数の企業や組織が横断的に脅威情報を共有する活動を支える仕組みを「情報共有システム」と呼ぶ。

（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

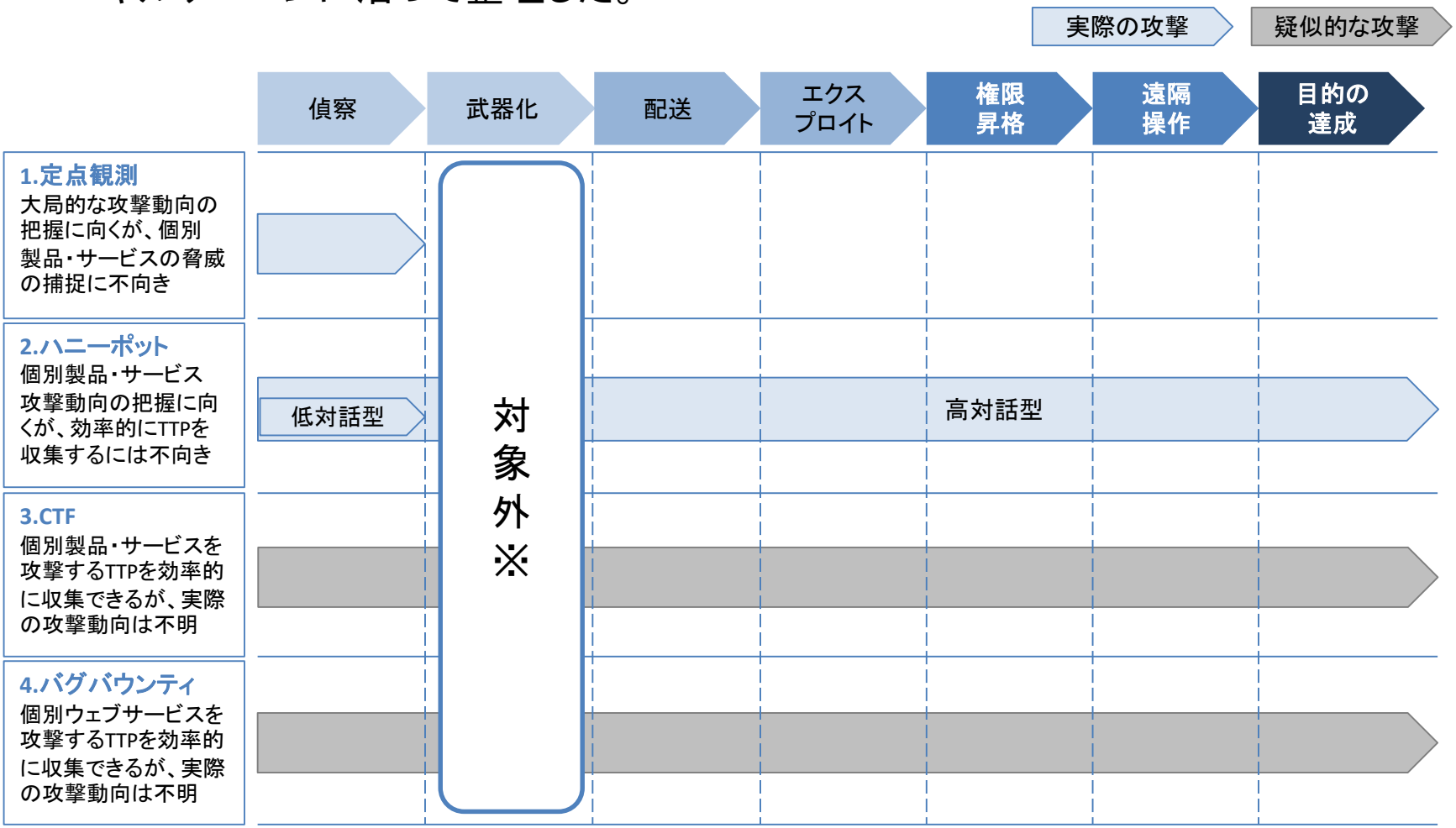
IT領域の脅威情報収集手法

IT領域の脅威情報は、主に公開情報、インシデント、観測・実験を情報源にしている。
ここでは、その収集手法の概要と、収集されるデータ、分析の観点を整理した。

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） • 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。 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） • A IoT Malware Story（Kaspersky社） • 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。 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 • 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 • 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。 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）。

脅威情報収集手法の考察

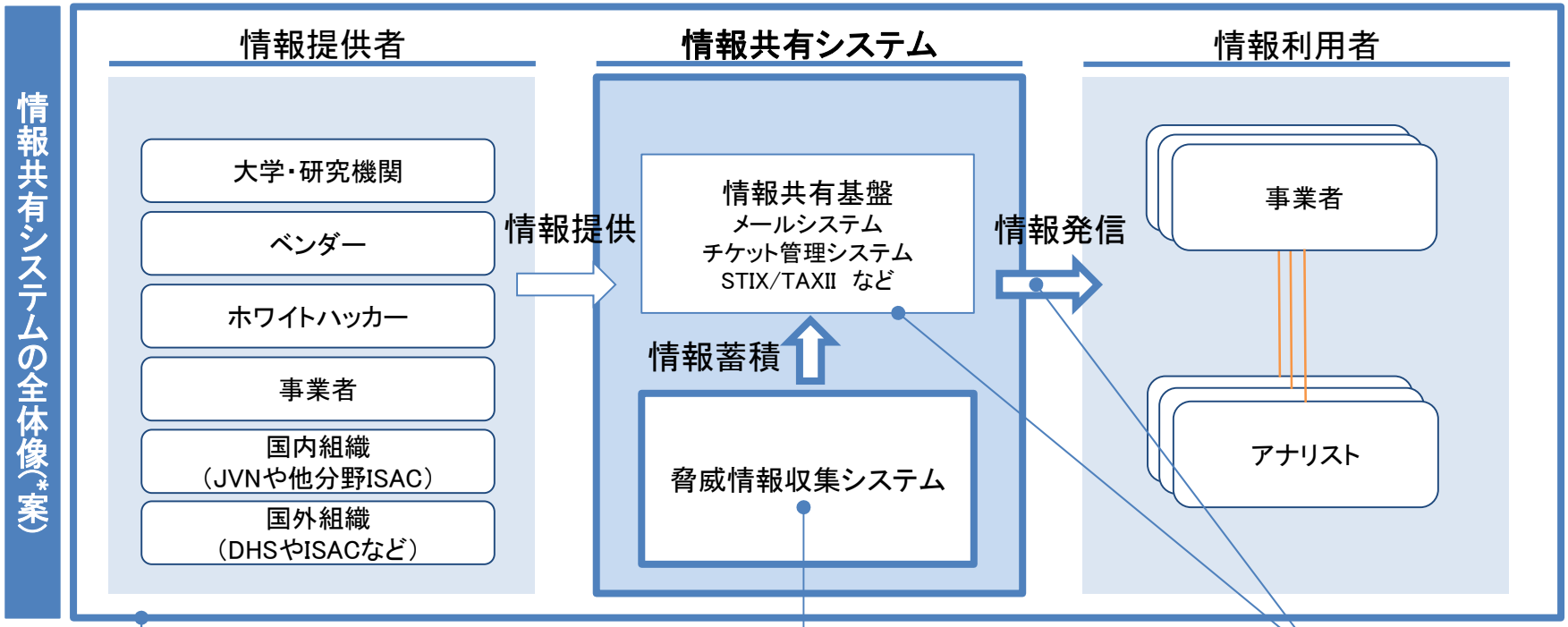
前述の手法で収集した情報から、攻撃者の手口をどの程度まで捕捉できるかをサイバーキルチェーンに沿って整理した。



※　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すことから、上記1～4の手法では補足できない。

自動車領域の脅威インテリジェンスへの応用検討

以降②～⑤のフェーズで、情報を収集・分析・蓄積し、ステークホルダーに共有することで、初動対応支援の仕組みを検討する。各フェーズで検討する課題を設定した。



課題

脅威情報を収集し、初動対応支援につなげる仕組みを、自動車業界としてどのように構築するか？ **（⑤で検討）**	自動車の脅威情報をどのように収集するか？ **（1-2の調査結果を基礎に②③で検討）**	初動対応支援するために、どのように収集した情報を蓄積し発信するか？ **（1-1の調査結果を基礎に④で検討）**

（※）UA Auto- ISACの全体像を参考に案を作成。日本の自動車業界として、どのような全体像を構成するかについては、⑤のフェーズで検討する。

情報収集・蓄積の手法検討

本プロジェクトでは、前述で調査したような収集手法で、自動車の脅威情報が収集できるか、実証実験を行う。このフェーズでは、その準備として、脅威が観測されうる車載機器を調査し、それぞれにどのような収集手法が適用可能か検討した。

仮説

ITおよびそれ以外の他業界（IoTやICSなど）においても、ハニーポットなど、**能動的に情報を収集する手法はすでに実験・実践されており、コネクテッドカーにおいても同様に収集が可能**である。

検討

IT領域の脅威情報の収集手法（1-2で実施）

脅威が観測されうる車載機器・サービス
(2-1で調査)

自動車領域の特性を考慮し、脅威情報の収集方法を検討（2-2で検討）

実験

コネクテッドカー関連の脅威情報を収集することができるかどうか実験を行う。（3で実施）

評価

得られた脅威情報として構造化した際に、各ステークホルダーに対して価値のある情報であるかをヒアリングなどを通じて評価する。

脅威情報収集実証実験への期待

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、自動車の脅威情報を収集するために適用可能か評価し、実用化に備えて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

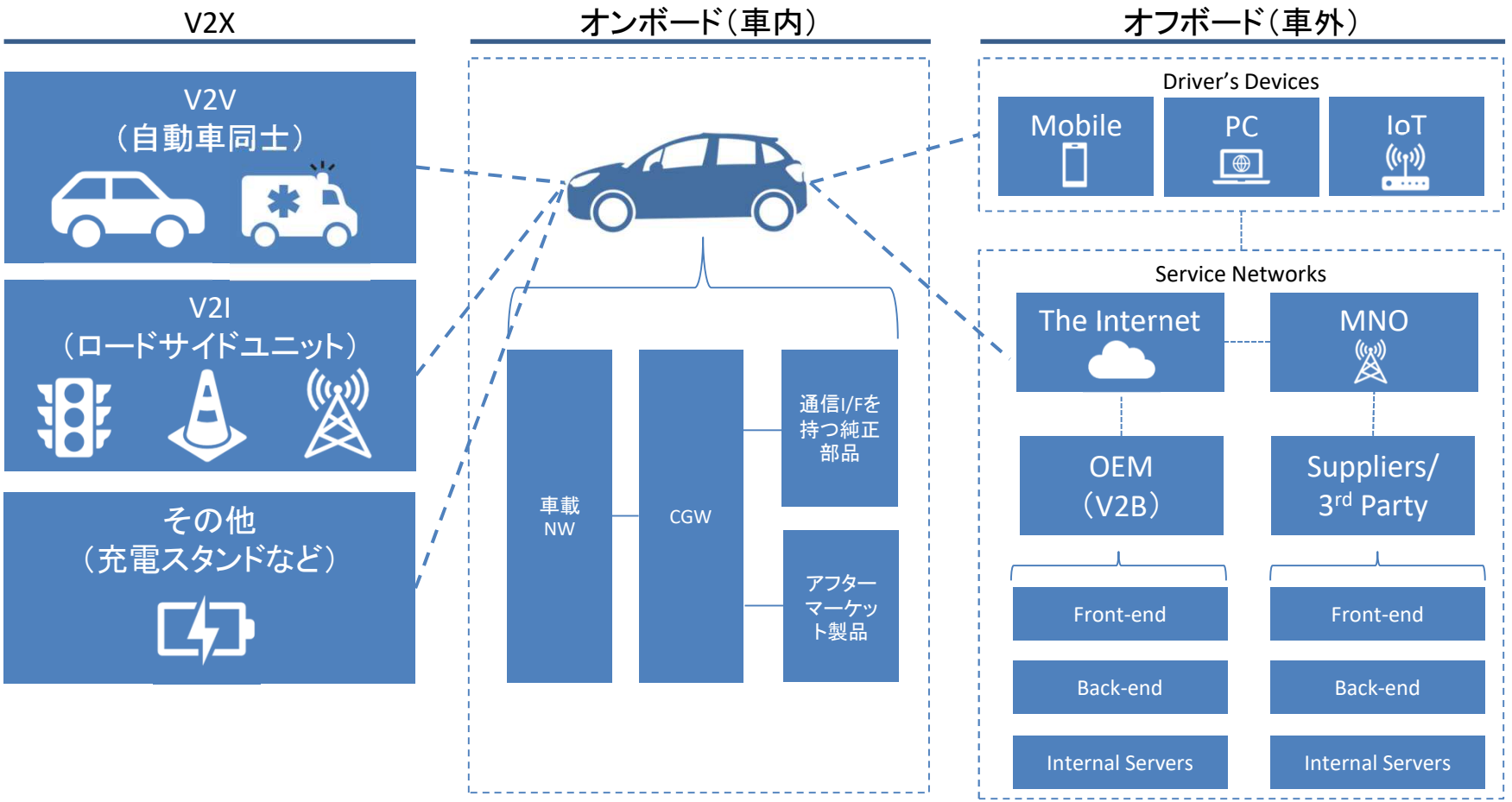
脅威情報観測実験に期待すること:

- 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

脅威が観測されうるサービス・機器の調査

市場において現実的な脅威が予想される車載機器やこれらの機器の市場流通数量を調査し、基礎調査の結果も踏まえて、車両の脅威情報収集・蓄積手法を検討した。

調査対象のイメージ



自動車領域の特性－攻撃の手法の特殊さ

前述で検討したカテゴリには、攻撃手法の特殊さ、攻撃検知の容易さ、攻撃の頻度観点で違いがあり、それぞれに適した情報収集方法を検討した。

検討カテゴリ	V2X	オンボード領域	オフボード領域
通信プロトコル	RF/CAN等	BLE/Wi-Fi/ZigBee/HTTPS/CAN等様々	主にHTTPS
攻撃手法	DSSSや充電スタンドのように一部社会実装が進んでいるものもあるが、実証段階の技術も多く、具体的な脅威が顕在化していない。	個別の要素については、IoT領域で、ある程度の情報がある一方で、車特有の情報は多くはない	一般のWebシステムに対する攻撃のナレッジは既に収集されている
攻撃検知の容易さ	攻撃を検知する仕組みの検討が必要	攻撃を検知する仕組みの検討が必要	一般的な製品で攻撃の検知が可能
攻撃の頻度	攻撃者が対象に到達できるように工夫する必要がある	攻撃者が対象に到達できるよう工夫する必要がある	インターネットからアクセス可能なため、攻撃頻度は高いと考えられる また、公開されているOEMのサービスはDNS等で識別可能なため、攻撃対象となりやすい
主なチャレンジ	• 社会インフラの一部であるため、OEMやサプライヤーだけではなく、インフラ事業者の協力が必要になる	• 特殊なプロトコルを用いた現時点で情報の少ない攻撃手法であるため、検知が難しい • どのように攻撃者を環境に誘導するか	• 一般的なWebシステムに対する攻撃の中から、特にテレマティクスサービスを狙った攻撃をどのように識別するか • 環境はOEMが保持しているため、実在するサービスへの攻撃を観測するためにはOEMの協力が不可欠

自動車領域での脅威情報共有における仮説と評価方針

自動車は、ITと違いアーキテクチャがOEM毎に共通ではないため、ある車両に対する事例が、他の車両に対しては脅威とならない可能性が高い。一方で、事例を分析することで、部分的に他の車両でも成立する脅威を得られる可能性がある。

仮説

車両制御は車種によりHW/SW、通信プロトコルの違いがITに比べて大きく、車両制御の乗っ取り事例のみに注目した場合、**他の車両でも共通の脅威にはならない場合があるのでは**ないか。

一般的に、**車両制御に関する攻撃事例、報告は複数の攻撃が組み合わせられ成立していることが多い**（2019年度および2020年度活動aにおける事例調査より）。

そのため、ある車両に対して発生した事例は必ずしもその事例すべてが**他の車両に対して対象外になるとは限らない**。

調査／分析

ある車両に対する攻撃事例のイメージ（手法）

攻撃の流れ（Tactics）別に分解、手法（Techniques）を分析可能

偵察	侵入	目的の達成
• ネットワーク・脆弱性スキャンによる既知の脆弱性調査 • ファジングによる未知の脆弱性調査 • ファームウェアの抽出（ハードウェアハック等）	• 開発者向けのI/Fからのログイン • 強度が不十分なパスワード設定 • 既知もしくはゼロデイ脆弱性によるシェルの取得や権限昇格	• ECUのリプロ／アップデート時の認証処理の回避 • 任意のCANメッセージの入力による車両の任意制御

評価

分解、分析後の脅威情報について、車両に依存せず、OEMをはじめとした自動車領域のステークホルダー間で活用することができるかどうか評価する（窓口としてJ-AUTO-ISACを想定）。

情報収集・蓄積の基本仕様検討

横浜国立大学と協力し、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ます。アフターマーケット製品を模したハニーポット開発し、2021年1月下旬よりサイバー攻撃の観測実験を開始した。

検討状況	• 広域スキャンで発見可能な車載製品を調査し、当該製品に特長的な挙動を模したソフトを開発（調査の結果、国内製品に該当する製品がなく、EU圏で販売されている製品にて開発） • クラウドを契約しEU圏のIPアドレスを取得。EU圏で受けたメッセージをYNUで受け応答する仕組みで、稼働後、製品に特有のコマンドの送信は観測されていない。IoTを無差別に狙う攻撃のみ
課題	• 製品は通常、SIMを使って通信しているが、EUのキャリアと契約ができないため、やむを得ずクラウドで稼働している（実際の製品群とは異なるIPアドレスレンジで運用していることによって攻撃の収集能力に懸念がある）
今後の展望	• 現状は製品の挙動をソフトウェアで再現しているが、実製品に置き換える予定。実製品を使ったハニーポットでは、ホスト側のイベントは観測しにくいため、主にネットワーク側のイベントを観測予定 • 車載機器狙ったサイバー攻撃は、現状それほど多くないことが予想され、かつ多様な車載製品があり、あらゆる車載製品で、ハニーポットを運用するのは困難なため今後、車載機器でハニーポットを運用するためのフレームワークとしてまとめることを検討

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kick off　(結果・今後の展望)

日本側の研究概要を紹介したところ、以下3点で連携の可能性の提案を受けた。
2021年4月にワークショップのテーマや役割などについてミーティングを実施し、同年6月にワークショップの開催するなど、連携を進めていく。

#	連携候補名	内容
1	Vehicler attack database (カールスルーエ工科大学)	• カールスルーエ大学は、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）を提案している。 • 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、taxonomyの考え方が参考になる。
2	IDS management system（Autosar）	• 販売済みの車両に搭載されたIDSが脅威情報を交換し、ソフトウェアを更新する仕組みを提唱している。 • 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。
3	IDSベンダーESCRYPT	• #2に参加しており、「a. IDS 評価手法とガイドラインの策定」についても連携ができる可能性がある。