SIP-adus Workshop 2020

Session3：安全な自動運転社会の実現に向けて

侵入検知システム（IDS）の有効性検証と対策技術

奥山　謙
PwCコンサルティング合同会社

2020年11月10日

SIP

Cabinet Office

INDEX

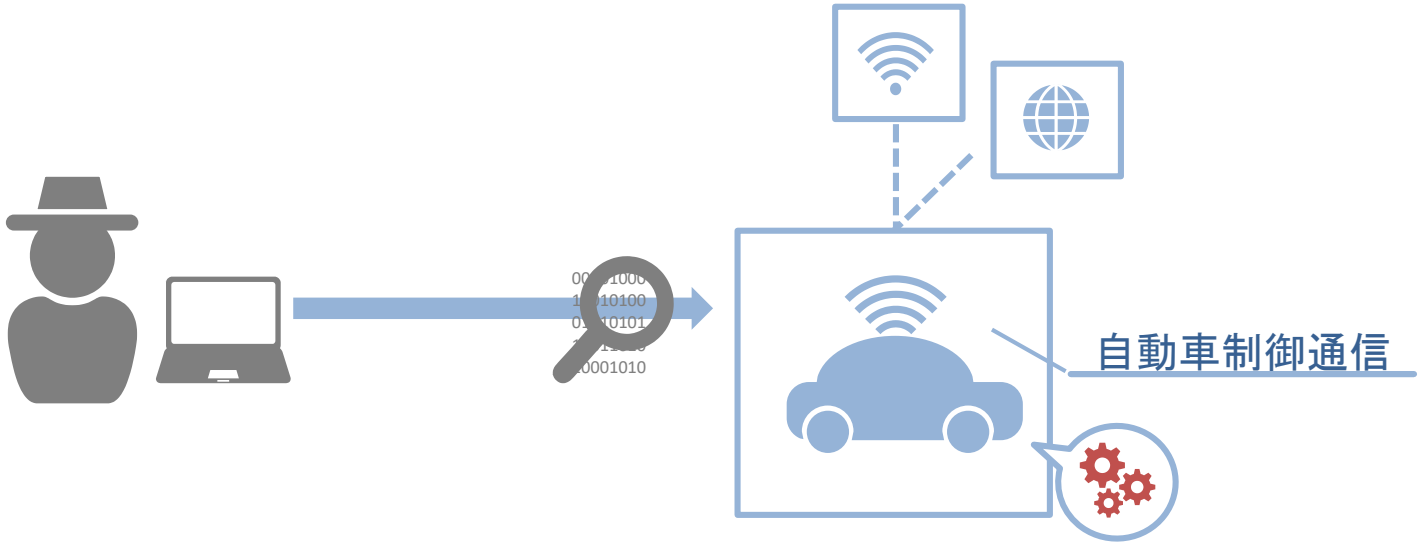
1. 本研究調査の背景と目的
2. 2019年度活動概要
3. 今後の活動計画

1

本研究調査の背景と目的

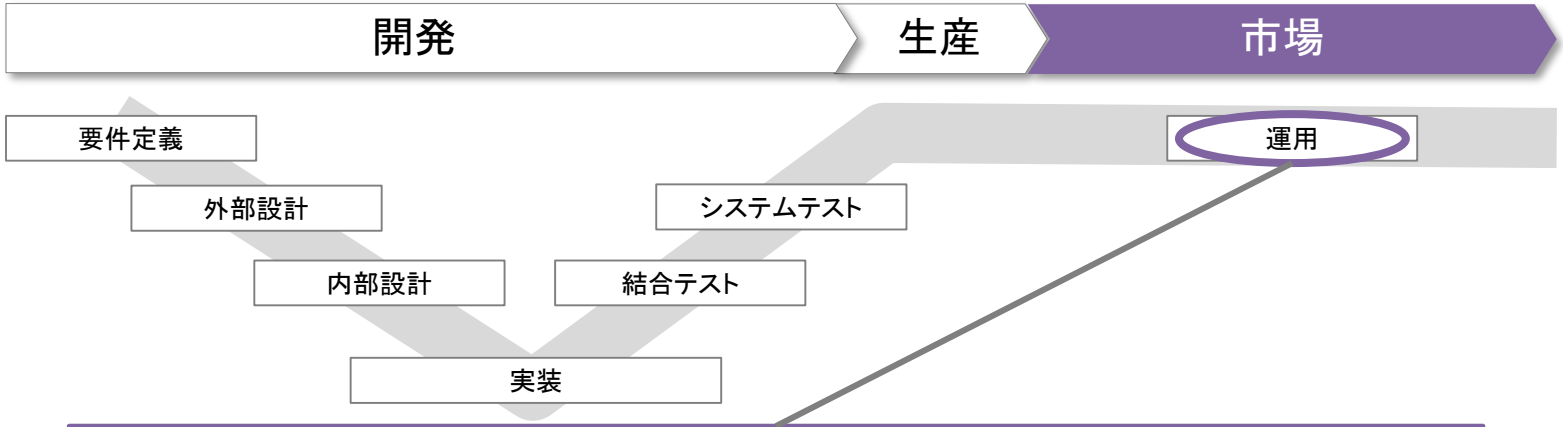
本研究調査の背景

- 車両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
- 自動車が外部とつながることにより、多くのセキュリティ脅威にさらされる。自動車制御を奪う等の実証実験も公表されている



サイバー攻撃検知（IDS）技術

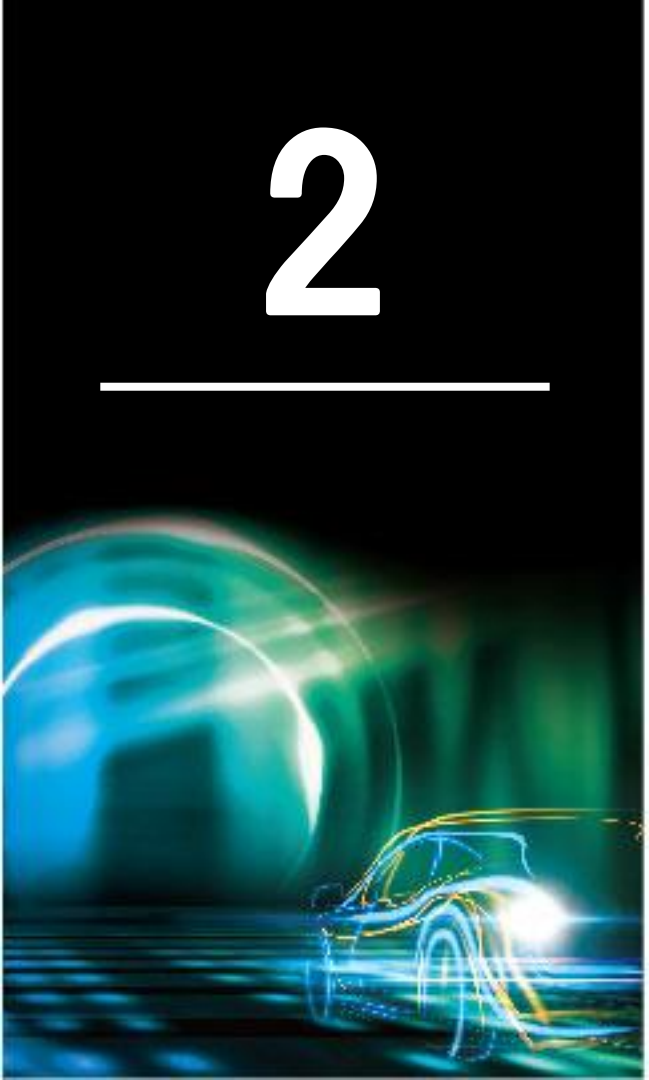
◆ 新たなサイバー攻撃への対策としての攻撃検知（IDS）技術



- 車両運用時には、**サイバー攻撃を検出・監視する仕組み**が必要である
- 車両販売後に見つかる**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（IDS）が注目**されている

新たなサイバー攻撃の動向調査と、対策技術としての侵入検知システム（IDS）を調査テーマとして選定

2



2019年度活動概要

2019年度調査の活動方針・概要

目的	車両サイバーセキュリティを取り巻く環境の変化を受け、 新たなサイバー攻撃手法の動向および対策技術を調査

調査内容

以下の3領域に関する調査を実施した

車両への攻撃動向調査	IDS等のサイバーセキュリティ対策動向調査	IDS評価方法の検討と基礎評価による検証
✓ 2017-2019年度に発生した車両攻撃の評価 ✓ 優先的に対応すべき攻撃動向を整理	✓ 車両向けIDSを中心としたセキュリティ技術・製品を整理 ✓ 個別製品調査に基づく、特徴を整理	✓ IT業界標準や車載CS規程等を踏まえた評価観点整理 ✓ IDS評価方法を検討・検証

車両への攻撃動向調査（概要）

1. 新たな攻撃手法や
インシデント情報の収集

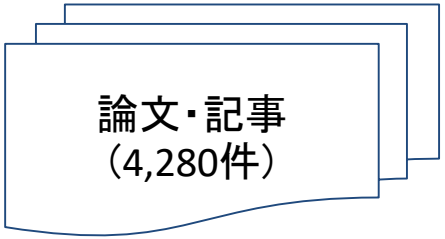
2. 新たな攻撃手法の分析

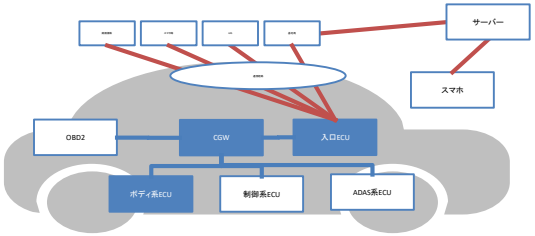
3. 攻撃手法等の整理及び
リスク・インパクト分析

【攻撃事例調査】
車両関係の事例を抽出し、
詳細分析対象を決定する

【攻撃シナリオ化】
事例を比較可能な
形式で構造化する

【リスク分析】
事例をもとにした
攻撃シナリオのリスクを
評価・比較する





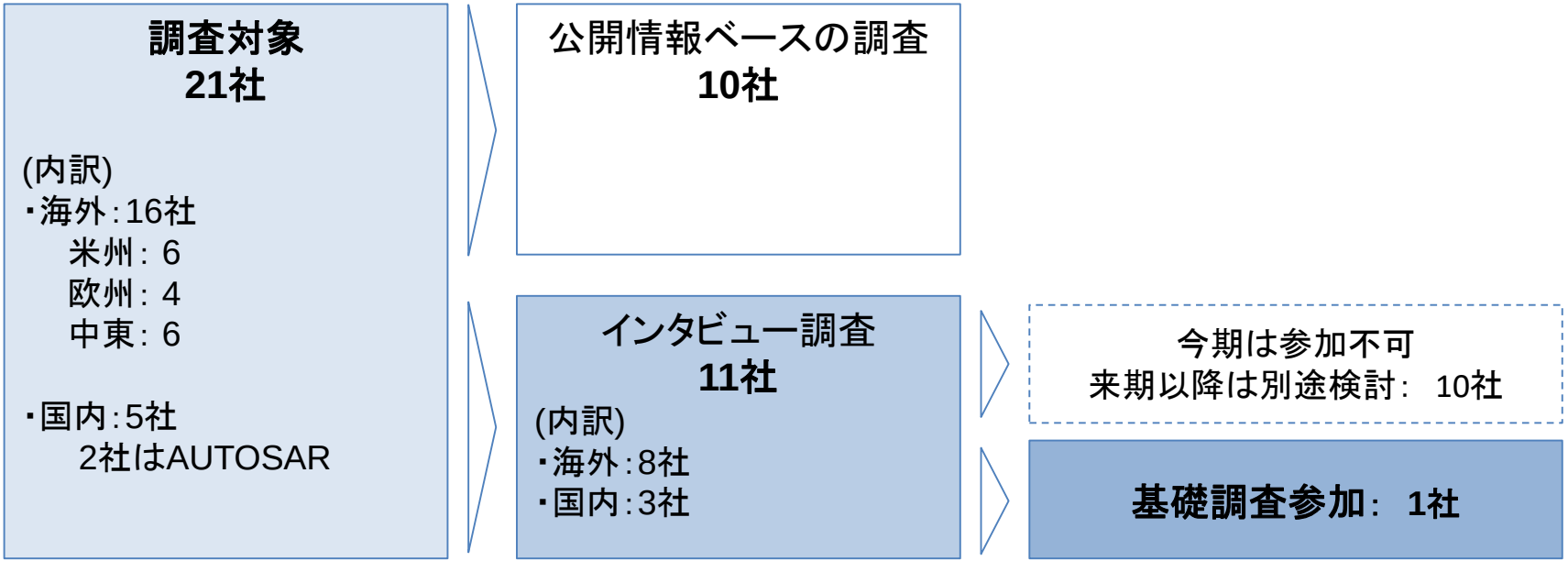
攻撃シナリオ対象
（105件）

リスク算定された
攻撃シナリオ

IDS動向調査

◆IDSベンダーを中心にインタビューによる調査を実施

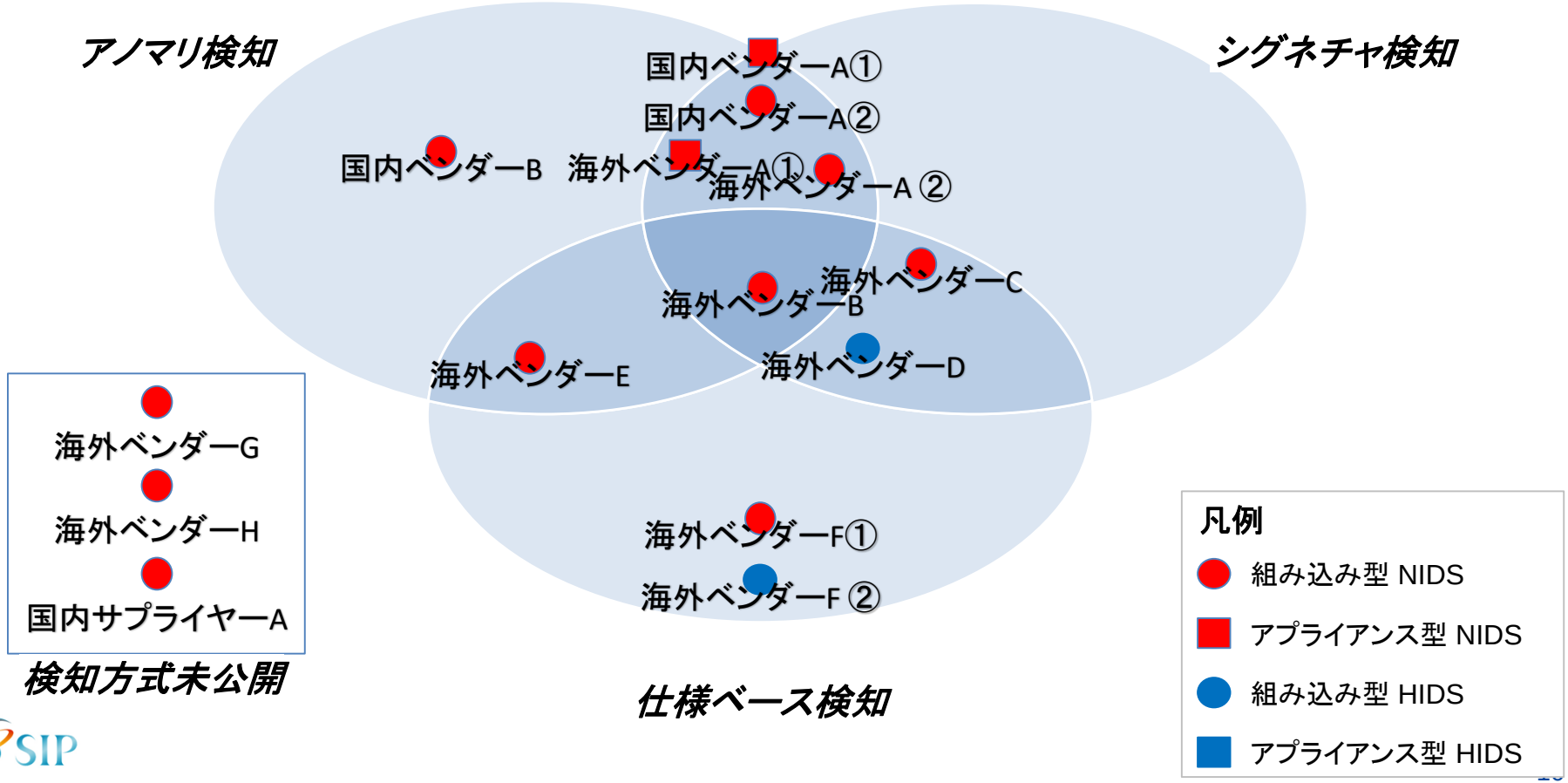
セキュリティベンダ・サプライヤ（書面・インタビュー調査）



IDS製品の特徴

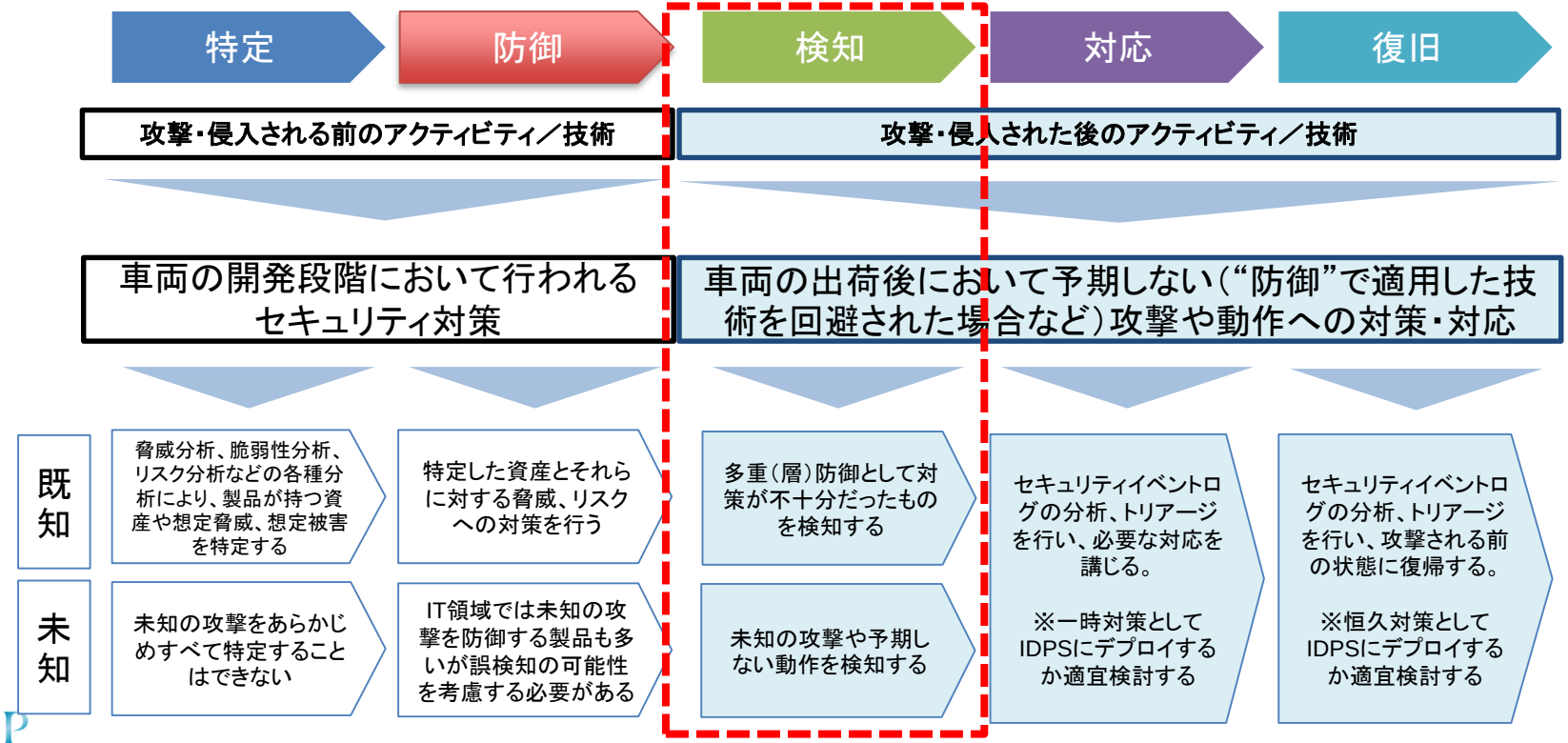
実装方法	組み込み型	ソフトウェアとして提供され、(既存の)ECUにインテグレーションされるタイプ
	アプライアンス型	ECUや後付けのドングルとして提供されるタイプ
検知対象	ネットワーク(NIDS)	CANバスなどのネットワークおよび通信(ペイロードなど)を監視するタイプ
	ホスト(HIDS)	ホスト内のアプリケーション(バイナリやプロセス)を監視するタイプ
検知方式	アノマリー	頻度(タイミング)	メッセージ周期などのタイミングを観測して検知
		ML(機械学習)	機械学習アルゴリズムによる異常検知
		統計(ビヘイビア)	統計アルゴリズムによる異常検知
	シグネチャ	既知の攻撃パターン(シグネチャ)を用いて検知
	仕様ベース	仕様や運用ルール(状態遷移や操作順序等)を用いて検知
	ハイブリッド	複数の検知方式の組み合わせによる検知 ※多くの商用製品はハイブリッド方式を採用している。

調査対象IDS製品における分類



IDS評価方法の検討と基礎評価による検証

◆ 既知・未知攻撃の観点で、IDSの評価方法を検討した



実機評価構成

◆ 実機による評価は、Arilou Technologies社（以下、Arilouと記載）に協力頂くことで行った。また、実機による評価にはテストベッドを利用し実施した

Fig1. Arilou提供のIDSをPASTAに接続、動作させているところ。
今回、両者には評価用IDS（Fig3）の他、モニタリング用の環境もご提供頂いた。

Fig2. Vector VN1630A + CANPiggy×2
上記はCANoeで制御

Fig3. Arilou提供 評価用IDS

IDS評価

◆ 評価内容概要

■ 攻撃動向調査結果を使い攻撃メッセージを入力（あるいは中継停止）し、IDS側の検知ログとの突合を行うことで誤検知や見逃しを確認

観点ID	項目名	攻撃メッセージと検知ログの突合結果	CANoeから入力した攻撃数	IDSが検知したメッセージ数	攻撃数に対する正解率
4-1	定常状態での計測	OK	0	0	0%（誤検知なし）
4-2	メッセージインジェクション（IDゼロ）	OK	1000	1000	100%
	メッセージインジェクション（ビットフリップ）	OK	1000	1000	100%
	メッセージインジェクション（ランダムメッセージ）	OK	1000	1000	100%
	メッセージインジェクション（UDSによるECUリセット／software reset）	OK	2	2	100%
	メッセージインジェクション（UDSによるECUリセット／Key off on reset）	OK	2	2	100%
	メッセージインジェクション（UDSによるECUリセット／hardware reset）	OK	2	2	100%
	中間者によるメッセージ置換	OK	1000	1000	100%
	中間者によるメッセージ置換（ビットフリップ）	OK	1000	1000	100%
	中間者によるメッセージ中継停止	OK	400	389	97%
4-3	中間者ECUの設置	対象外	---	---	---
4-4	メッセージインジェクション（脆弱性攻撃）	OK	1	1	100%
	中間者によるメッセージベースの脆弱性攻撃（ブロードキャスト）	OK	1	1	100%
4-5	メッセージインジェクション（エラーフレーム）	OK	1000	0	100%

評価（攻撃）パターン

◆ 結果および考察（概要）

- 中間者によるメッセージ停止を除いて、攻撃メッセージを検知可能
- メッセージの周期に関する検知は、誤検知の可能性
  - 回避するために設定変更可能な閾値がある

など

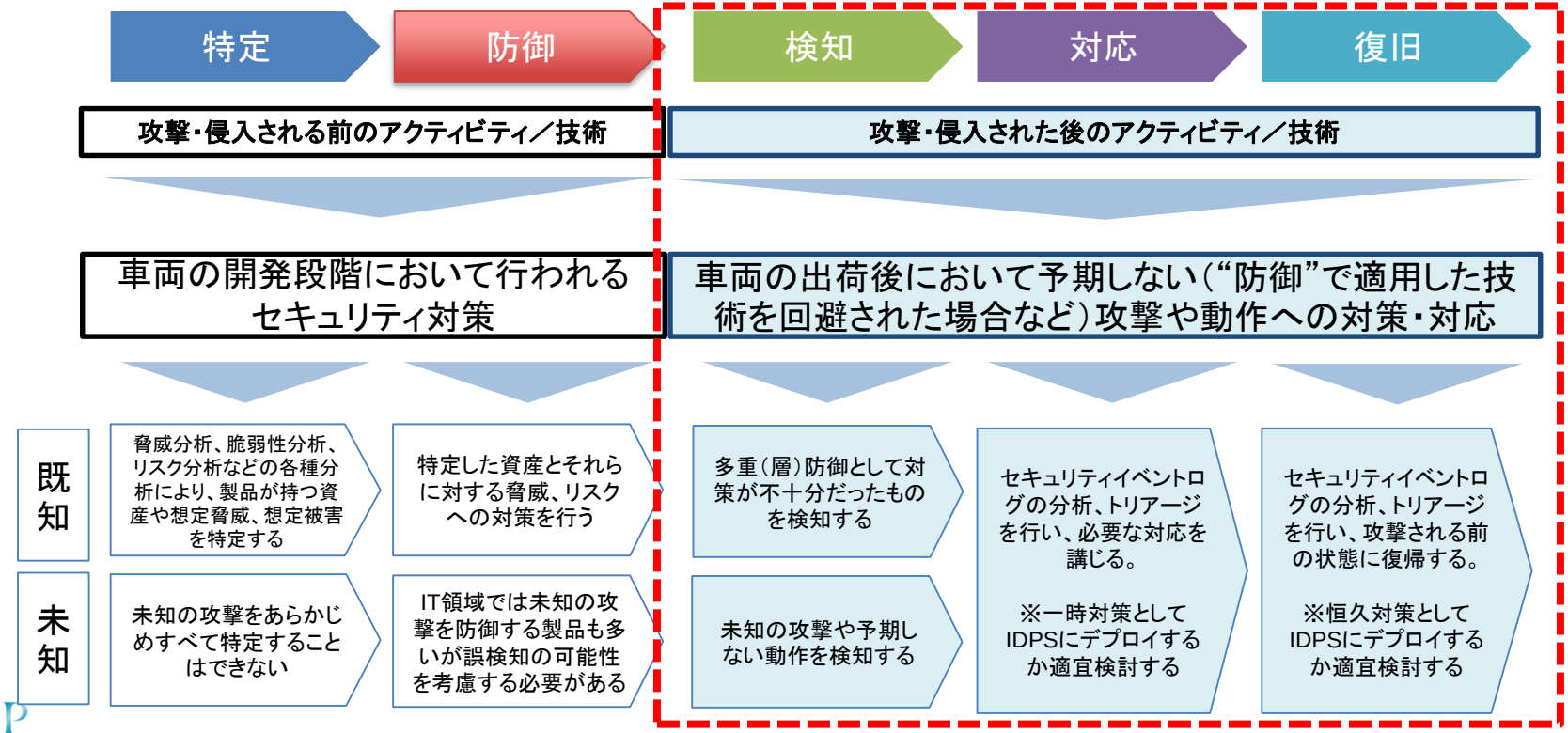
- セキュリティイベントをどのように検知するか、柔軟に対応が可能
- 一方、検知する、しないを判断するためのメーカーのセキュリティポリシーに基づく判断や、車両モデル固有の項目も必要

3

今後の活動計画

IDSを活用した対応・復旧に関する調査

◆ 検知のみならず、対応・復旧までを調査対象に拡大



IDS評価ガイドライン初版の作成・検証

◆ 検知のみならず、対応・復旧までをスコープとして、IDSおよび関連システムの評価手法を検討し、実機による検証により、手法の妥当性を検証し、ガイドライン作成を目指します

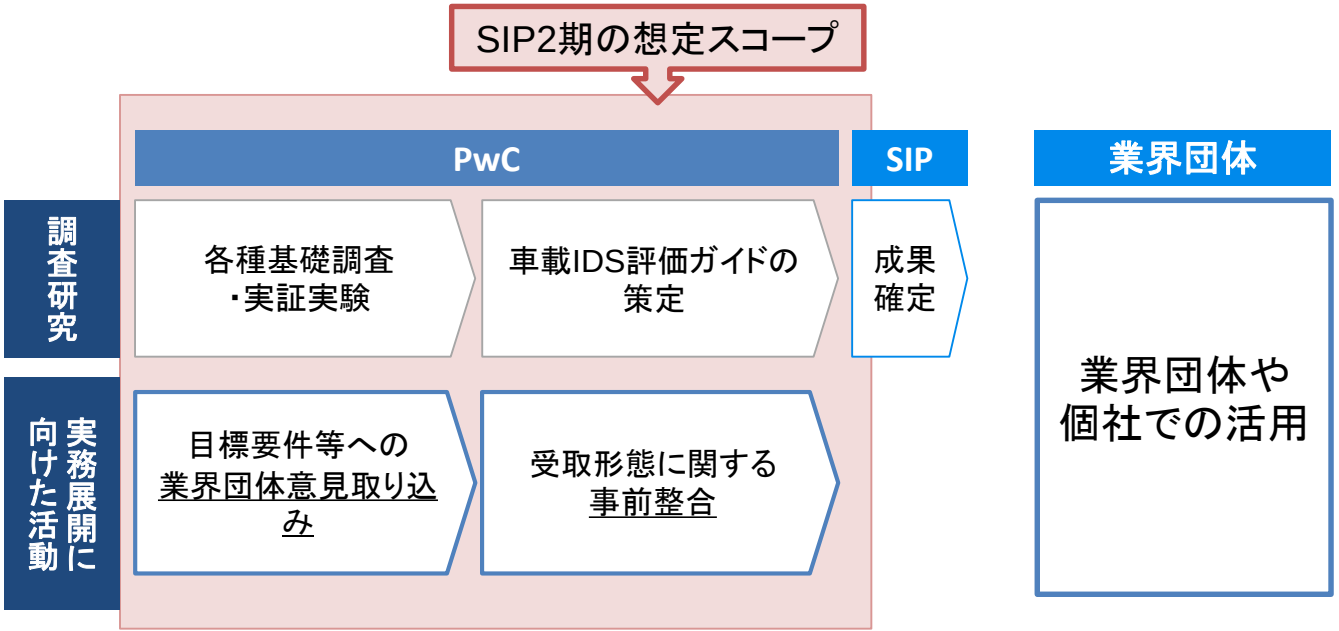
対策フェーズ	開発フェーズ	機能	評価項目	製品品質分類
基本			IDS種別（NIDS/HIDS）	N/A
			サポートする車載ネットワークのプロトコル（CAN／CAN-FD／Ethernet／FlexRay／Lin）	N/A
			検知方法（仕様／アノマリ／シグネチャ）	N/A
検知	導入	キャリブレーション	DBCファイルの要否	使用性
			ドライビングデータの要否	使用性
			既存モデル用キャリブレーション情報の流用可否	移植性
	運用	セキュリティイベントの検知	検知の正確さ(*1)	機能適合性
			検知理由の説明の有無と粒度	使用性
対応	導入	対応条件の設定	導入時にOEMが指定可能な通知条件	使用性
	運用	セキュリティイベントの通知	定常時／検知時のセキュリティイベントの通知内容	機能適合性
			セキュリティイベントの通知先	使用性
		セキュリティイベントのロギング	ロギング内容（検知コード／メッセージの内容／車両の状態／危険度等）	機能適合性
復旧	運用	アップデート	プログラムのアップデートの方法（物理ポート経由／OTA／その他）	保守性
			シグネチャや設定のアップデートの方法（物理ポート経由／OTA／その他）	保守性
			アップデート時のアップデートサーバー／アップデート管理モジュール／IDS等の役割分担	保守性

評価項目（イメージ）

実機による評価と結果のフィードバック

実務展開に向けた業界との共通認識の形成

◆ 出口戦略として最終目標である実務への活用に向けて、アウトプットであるIDS評価ガイドの目標要件や記載されるIDS評価方法についてステークホルダーと事前整合する



Thank you