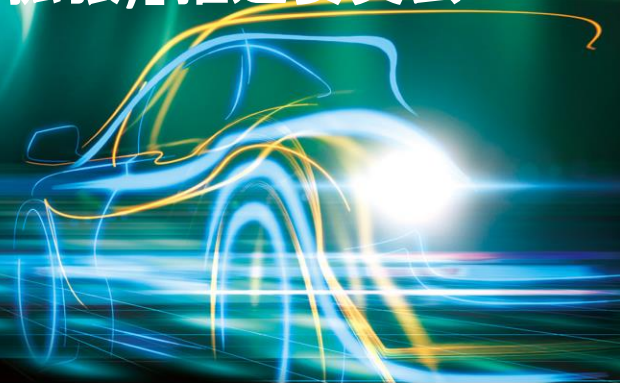


第18回 SIP第2期「自動運転(システムとサービスの拡張)」推進委員会



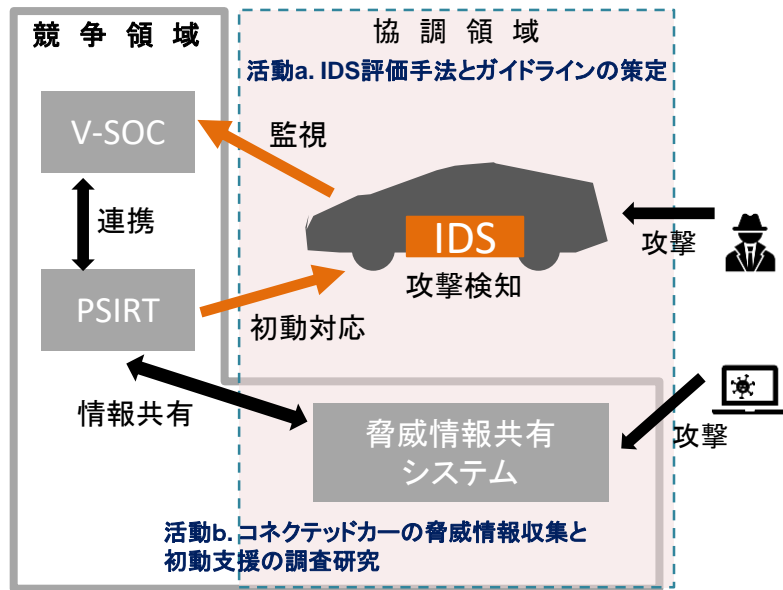
新たなサイバー攻撃手法と対策技術

内閣府 SIP自動運転 Cybersecurityテーマリーダー
平井 康雅

2022年6月10日

テーマ概要

- セキュリティ環境の変化や国連法規の施行に伴い、サイバー攻撃からの継続的な保護が求められている
- 以下2点の実現を目指し活動
 - ✓ 設計時に想定した(顕在化している)脅威の検知 (活動a)
 - ✓ 運用時(出荷後)に新たに顕在化する脅威の迅速な発見・共有 (活動b)



活動概要

a. IDS評価手法とガイドラインの策定

車載IDS 評価法および各評価項目の判定基準を導出し、ガイドライン化、自動車業界へ実務展開、実務運用につなげる

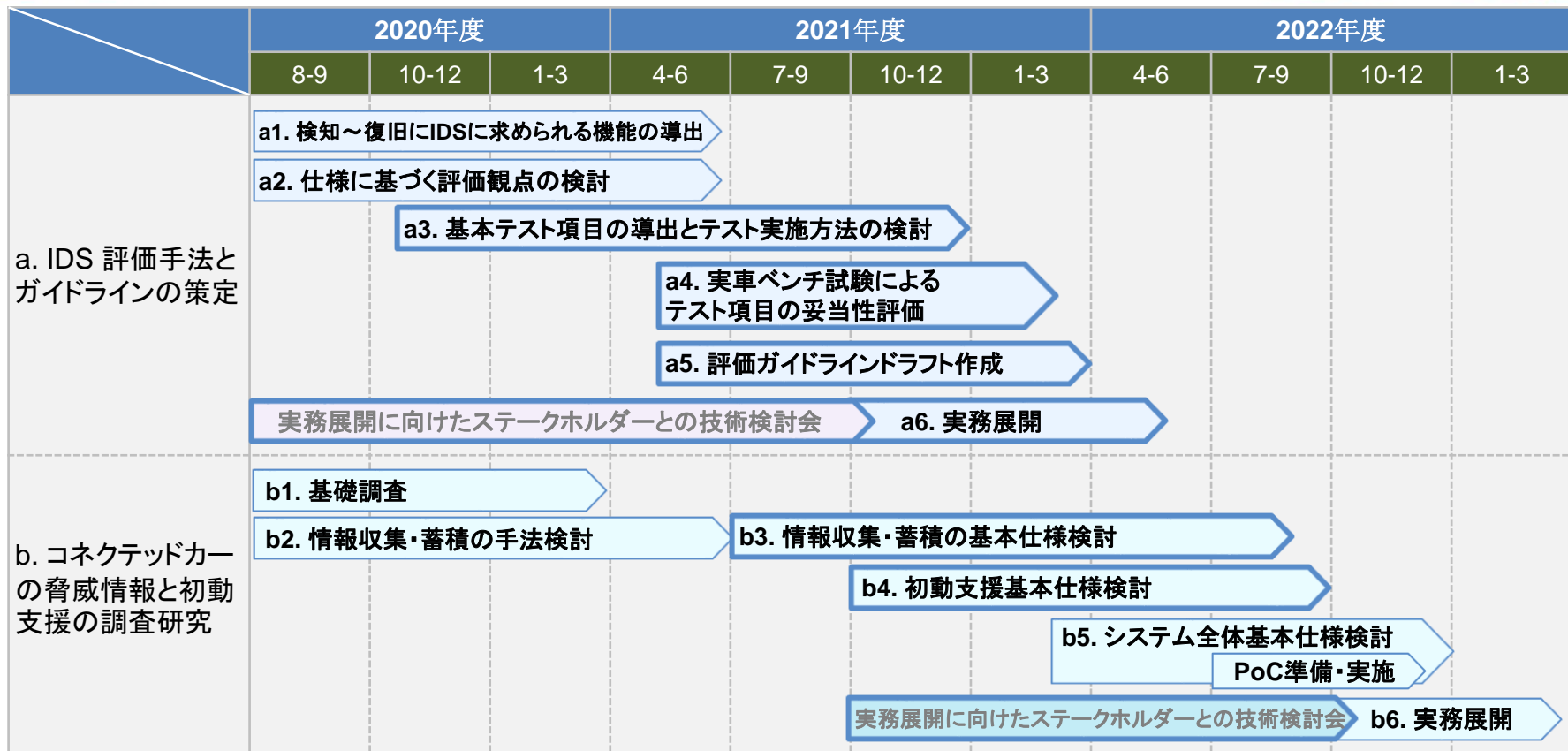
IDS: Intrusion Detection System

b. コネクテッドカーの脅威情報と初動支援の調査研究

脅威情報の収集・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、初動支援のためのシステム基本仕様を策定し、関連業界団体に展開、協調領域における情報共有促進と業界全体のサイバー対応力の底上げを支援する

➡ 成果の社会実装に向け業界団体への移管を目指す

全体スケジュール



2021年度 活動と成果の概要 (活動a)

- Off-the-Shelf型 IDSを対象に以下を実施
 - ✓ IDS評価観点および基本テスト項目・テスト実施方法の検討
 - ✓ 実機ベンチを用いた試験によるテスト項目の妥当性評価
 - ✓ IDS評価ガイドラインの作成
 - ✓ 2022年5月の一般社団法人 JASPAR※への移管に向け、技術検討会の実施

IDSの開発形態

ビスポーク (Bespoke)

- ・検知アルゴリズムやルールを含むすべての機能仕様を発注元のOEM/サプライヤが要件定義、開発
- ・国内大手OEMに多い

オフ・ザ・シェルフ (Off-the-Shelf)

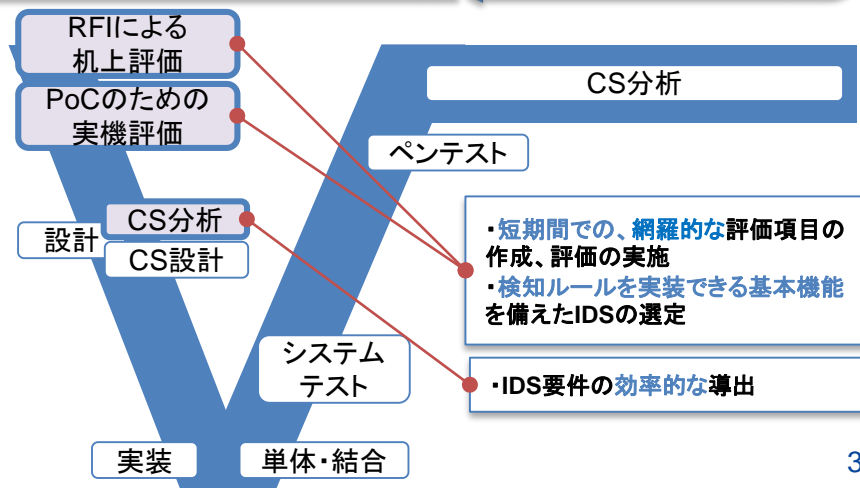
- ・検知アルゴリズムやルールのコンフィグレーション機能等、基本機能が実装済みのIDSを選定、ベースに開発
- ・短期間で実装ができる可能性
- ・海外のOEMに多い



※ 車載ネットワーク、ソフトウェア、情報セキュリティにおける標準化を推進

評価ガイドラインが対象とする工程と狙い

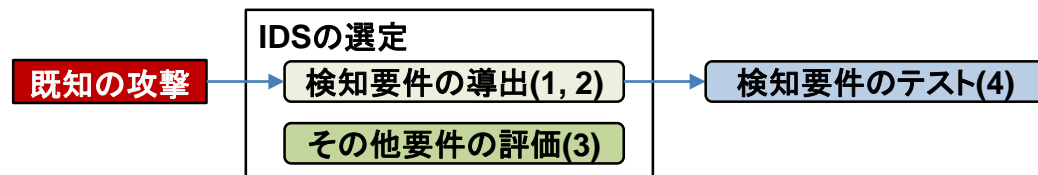
新たな脅威を適宜想定脅威としてアップデート



2021年度 活動と成果の概要 (活動a)

■ 成果物:IDS評価ガイドライン

既製品を活用して開発(Off-the-Shelf型)する際の評価方法を示し、IDS開発の選択肢を広げるとともに、特に立ち上がりに時間を要しているOEM/サプライヤーを想定読者として、IDS開発の加速に寄与することを目的としたガイド

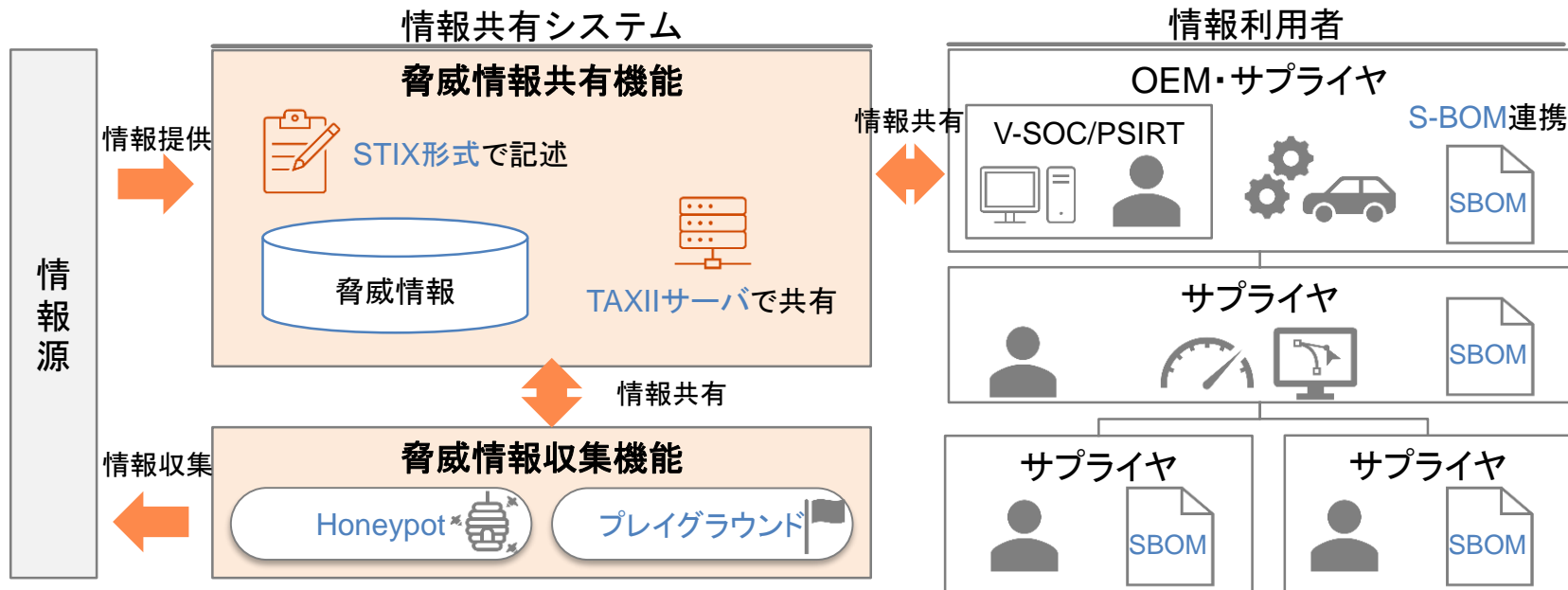


本ガイドラインの概要

#	内容	概要
1	検知機能の要件化方法	既知の具体的な攻撃事例から類似した攻撃を検知するための、 攻撃事例のシナリオ化方法と検知機能要件の導出方法
2	IDSの基本要件	2017～2020年の攻撃事例を#1に適用した結果を基とした IDS基本要件の導出手順と導出結果
3	仕様評価観点	通知機能やアップデート機能等の対応に係る機能の具備や使用性、性能効率性等、 IDS, IDSベンダーを網羅的に机上評価するための評価観点リスト
4	基本テストケース	実機評価結果に基づく、 IDS基本要件のテスト観点と、各テスト観点の実機テスト方法の例

2021年度 活動と成果の概要 (活動b)

- 情報共有システムにおける情報収集・共有の仕組みを調査、机上評価
- 一般社団法人 Japan Automotive ISAC(J-Auto-ISAC)※との協議、技術検討会を開始



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, プレイグラウンド)
- 利用者の機能：S-BOM(Software Bill of Materials)との連携

2022年度の活動概要

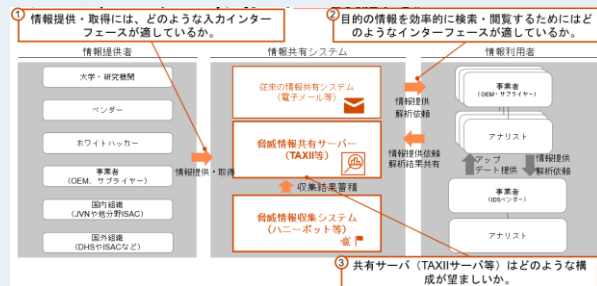
- 活動bについて、2022年12月の成果移管を目指して活動を実施

システム全体基本仕様検討

- 2021年度までの各種調査結果を踏まえて、脅威情報の活用について検討

A PoC実施

脅威情報の記述・表現方法および共有形式に関するPoC(実証)を実施

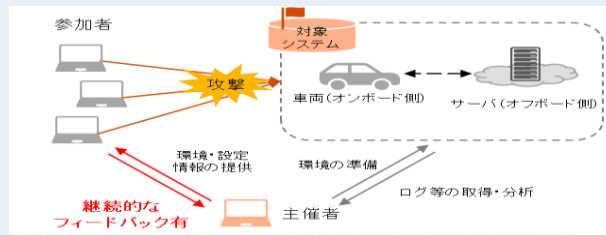


脅威情報観測実験

- ハニーポットで観測された攻撃を分析し、プロアクティブな脅威情報収集方法としての有効性評価、知見・ノウハウの取りまとめ

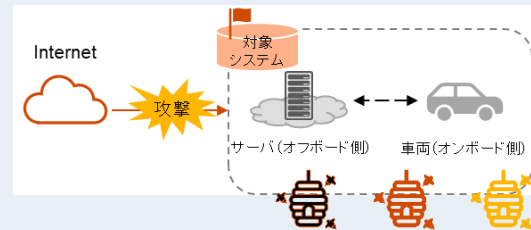
B プレイグラウンドの実施 (9月)

攻撃者のモチベーションや攻撃技術・手法等の調査



C ハニーポット拡充 (~10月)

ハニーポットの種類、設置する国・地域を拡充し、より広く脅威情報を収集



社会実装に向けた取組

- 技術検討会を通じて移管に向けた議論を実施し、実運用との親和性が高い成果を構築
- 成果の検証のためのPoC等、技術検討会にて新たに発生する活動の実施