SIP-adus Workshop 2022

Session 6
Cyber Security

自動車領域における脅威情報の共有と収集に関する研究

韓 欣一 (PwCコンサルティング合同会社)

12, October, 2022

SIP

Cabinet Office

INDEX

1

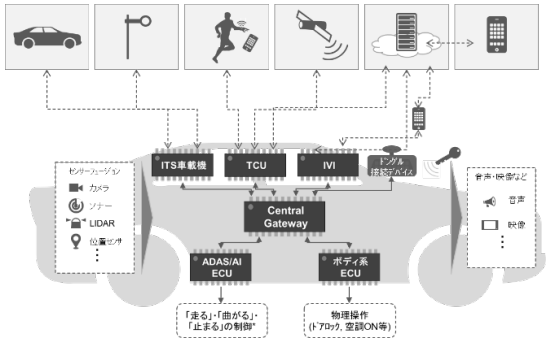
導入

プロジェクトの背景と研究テーマ

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と国際的な法規の整備に伴い、本プロジェクトでは、「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つの活動を行っている。

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

国際自動車基準調和世界フォーラム
(WP29)

活動a. IDS評価手法とガイドラインの策定

車載 IDS を評価するためには、どのような手法、手順および環境が必要か

活動b. コネクテッドカーの脅威情報と初動支援の調査研究

自動車に関する脅威情報を収集・共有するための方法にはどのようなものがあるか

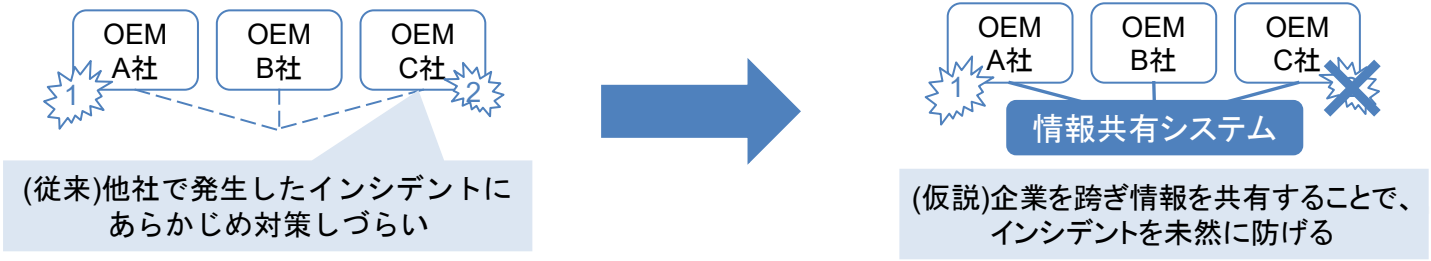
2

脅威情報共有システム

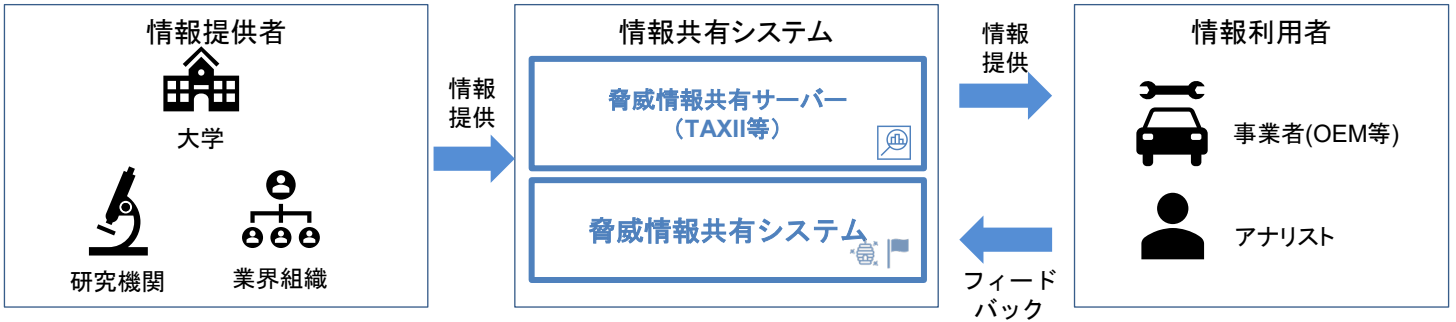
脅威情報共有システム

自動車業界における出荷後セキュリティの向上に寄与するため、情報共有システムの基本仕様を研究している。

✓ 情報共有システムの利点

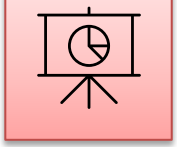
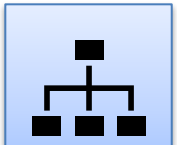


✓ 情報共有システムの概略図



情報を効率的に共有するためには

業界全体で効率的に情報を共有するためには、「情報の蓄積・共有」、「情報の分析・活用」、「情報の収集」の三つの要素が必要である。

1		効率的に脅威情報を蓄積し共有する	• 構造化された脅威情報 • 情報処理の方法の共通化
2		OEMおよびサプライヤーの現状を把握する	• 企業の製品およびシステムに存在するソフトウェアの一覧表
3		有益な情報を収集する	• プロアクティブな情報収集の方法

STIX TAXII

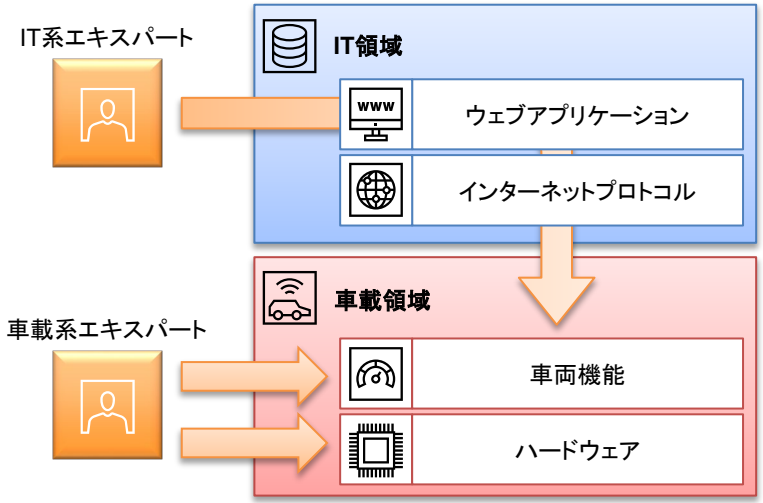
SBOM

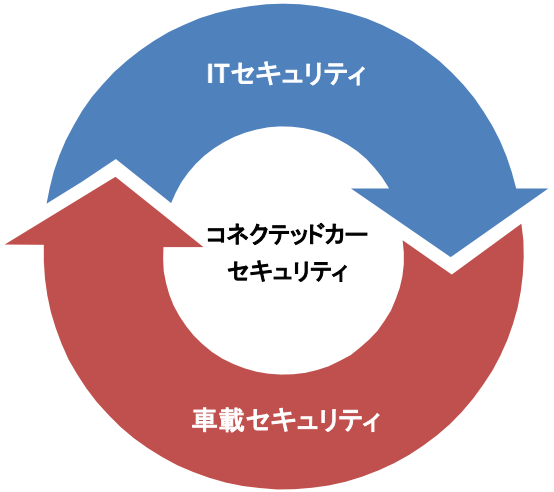
ハニーポット
CTF

脅威情報の記述・共有方法の検討

記述できる情報の豊富さとIT領域における活用実績から、脅威情報を記述するフォーマットとして、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。

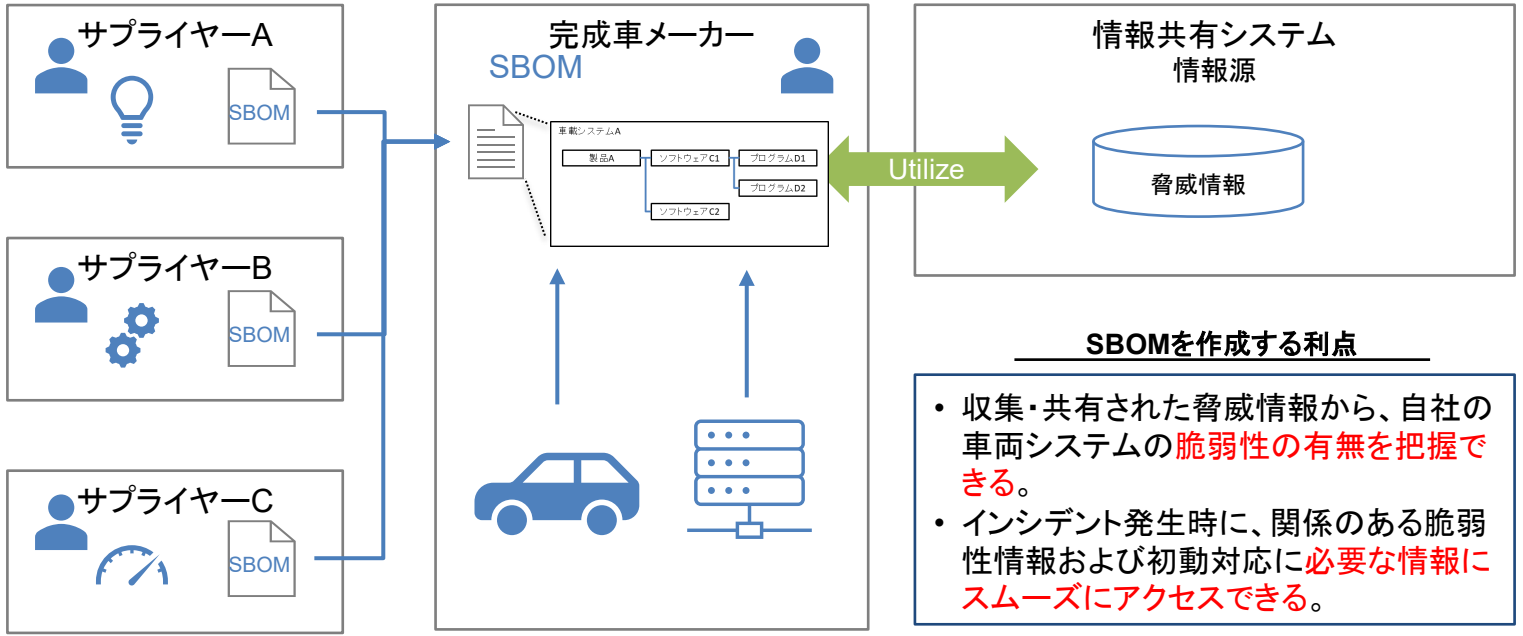




車両とITシステムが融合したコネクテッドシステムにおいて効率的に脅威情報を活用する仕組みとして、IT領域で最も普及しており、記載できる情報の種類が多いSTIX/TAXIIに焦点を当てて調査研究を行っている。
STIX/TAXIIを用いて脅威情報を記述した場合、IT領域で顕在化した脅威を類似の車載向けプロトコルや機能等に素早く展開できることで、車載領域では脅威が顕在化する前に対処できるメリットもある。

脅威情報の活用方法

製品やシステムに存在するソフトウェアの一覧表を作成することで、OEMやサプライヤーは、情報収集システムに蓄積されている脅威情報を効率的に分析、活用できる。



SBOMを作成する利点

- 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できる。
- 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できる。

プロアクティブな脅威情報の収集法

IT領域で脅威情報を収集するために運用・実施される、ハニーポットやCTFを、コネクテッドカーシステムに適用し、自動車特有の脅威情報を収集する。

目的	• 自動車領域における脅威情報を収集・蓄積するための方法の確立
仮説	• IT領域では、脅威情報を収集する様々な方法が開発されている。開発された脅威情報の収集法は、攻撃手法を明らかにするために運用されており、サイバーインテリジェンスの構築する際に、役立つ。 • IT領域で開発された脅威情報の収集法は、自動車領域でも有用であり、コネクテッドシステムに対する脅威情報を収集できる。 (例) ハニーポット / CTF / OSINT / Bug bounty / 監視
脅威情報	• 攻撃者の属性/TTPs
アプローチ	• IT領域で活用されている脅威情報の収集法を用いて、実際に攻撃を観測する。収集した脅威情報の分析を行うことで、コネクテッドシステムに対する攻撃パターンを考察する。

3

プロアクティブな脅威情報の収集法

ハニーポットの運用とCTF開催の目的

本プロジェクトでハニーポットとCTFを検討する目的は、特定の脅威を明らかにすることではなく、自動車に関連した脅威を明らかするための有効な方法を調査し、将来にそれらの手法を用いるために整理することである。

背景:

- 現時点では、コネクテッドカーを狙った攻撃が稀である。
- 現在のところ、アタックキャンペーンと呼ばれる、車両を狙った大規模な標的攻撃は、確認されていない。

ハニーポットとCTFは、以下の事柄を明らかにするために用いられる:

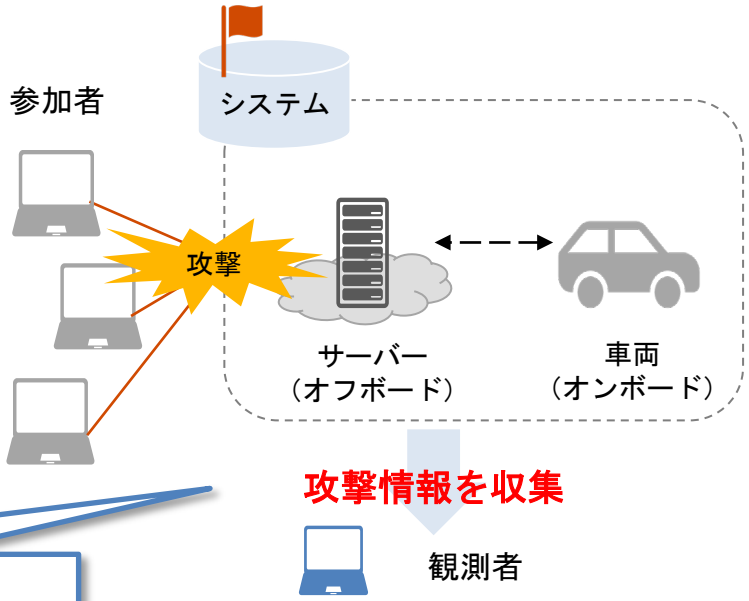
- インターネットからアクセス可能なコネクテッドカーは存在するか。
- インターネットに公開されているデバイスは存在するか。

- 攻撃者(CTFの参加者)はどのようにして車両を攻撃するか。
- 攻撃者が車両を攻撃する動機は何か。

CTFの概要

コネクテッドカーやシステムにとって、サーバーに対するどのような振る舞いが悪意を持つかを分析する。攻撃のターゲットを設置し、CTFの参加者に実際に攻撃してもらうことで、攻撃を検知するための知見を得る。

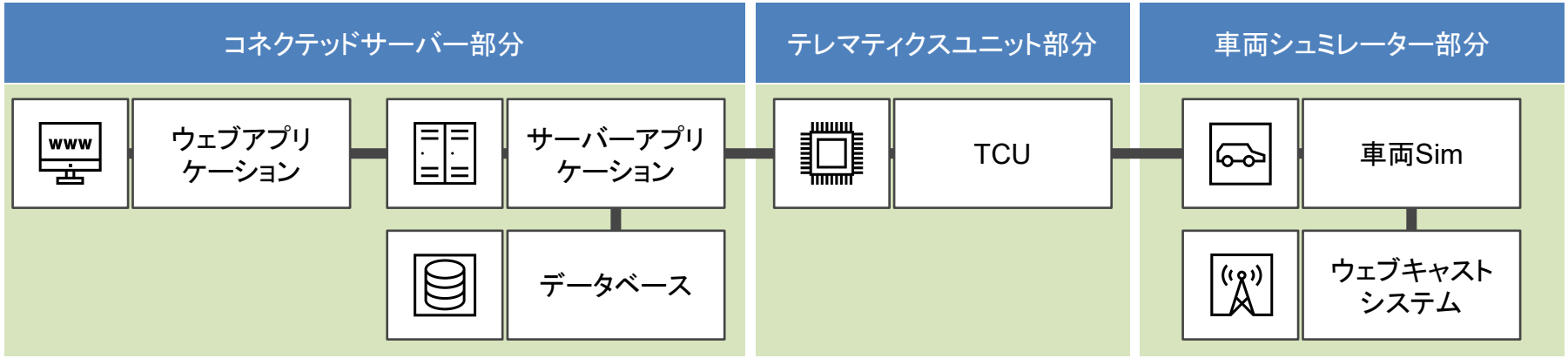
目的	• コネクテッドシステムに対し、どのような種類の攻撃が有効か。 • 車両を対象とした攻撃のために、攻撃者はどのような振る舞いをするか。
計画	• 参加者は、車両の制御や車両の情報を取得などを目的に、対象システムへの攻撃を試みる。 • 攻撃者の攻撃手法や攻撃技術を観察することで、攻撃を一早く検知するための知見を得る。

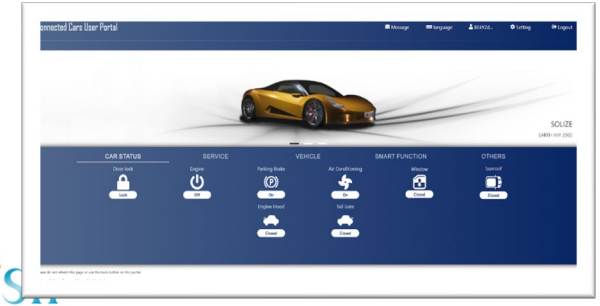


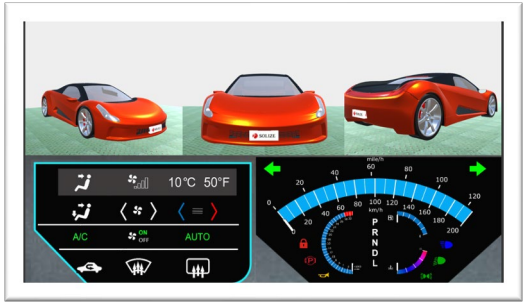
CTFで得られた知見は、ハニーポットの開発や、
攻撃を分析するための基準を作成するために使用される

CTFのプラットフォームのシステム構成

車両とコネクテッドサービス(サーバー、ユーザーポータル、アプリ)を模擬するプラットフォームを構築し、車両をハイジャックすることをゴールとするCTFを開催する。CTFのプラットフォームは、コネクテッドサーバー、テレマティクスユニット、車両シュミレーターで構成される、サイバー攻撃検証システムである。







CTFのプラットフォームの特徴

CTFのプラットフォームは、以下のようなコネクテッド機能を、主要な特徴としており、ユーザーはコネクテッドサービスを通して、車両(のシュミレーター)を作動できる。

コネクテッドサービス部分			テレマティクスユニット部分	車両シュミレーター部分
車両オーナー向け機能	ディーラー向け機能	通信機能		シュミレーション
オーナー向けポータル画面	管理ポータル画面	SMSの送受信		車両のCGモデル
ドアの施錠/開錠	車両管理	TCU通信プロトコル(SMS+HTTP)		ボディ系ECU
照明の点灯/消灯	動的テスト			シャーシ系ECU
クラクション				パワートレーン系ECU
エアコン				空調及び動的テスト
車両情報の表示				
エンジン作動				

4

まとめ

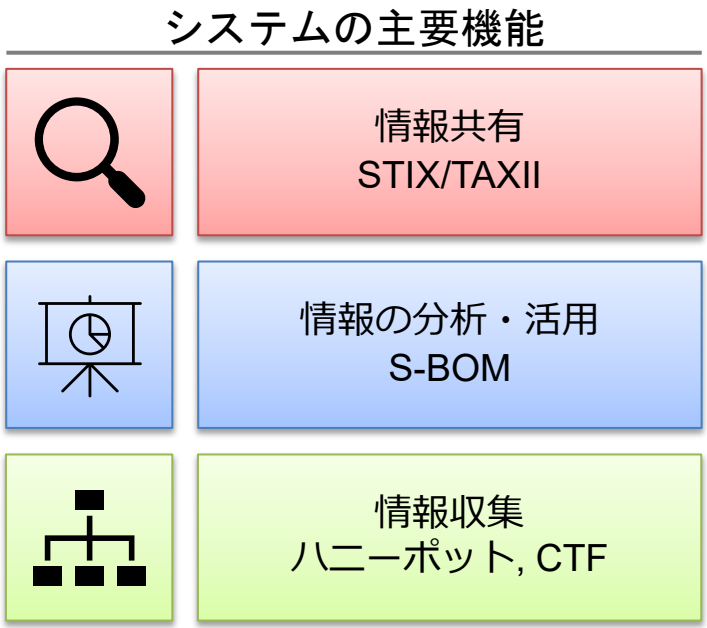
まとめ

<情報共有システム>

- 業界団体、完成車メーカー、サプライヤー間で、脅威情報を効率的に共有・活用・収集する方法を検討している。
- 業界団体への成果物の移管するために、議論を行っている。

<プロアクティブな脅威情報の収集>

- 既に存在する脅威情報を収集・蓄積する方法に加え、自動車領域における新しい攻撃手法に関する知見を収集する方法として、ハニーポットとCTFを提案した。
- コネクテッドシステム全体を模擬する、CTF環境のハニーポット化を検討している。



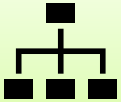
Thank you

A

付録

情報共有システムの機能

業界団体、完成車メーカー、サプライヤー間で、情報の共有・活用・収集を効率的に行う方法を検討している。

	システムの主要機能	利点
	情報共有機能 STIX/TAXII	• 認識の齟齬なく円滑に情報共有ができる。 • 情報処理を機械化、自動化できる。
	情報の分析・活用機能 S-BOM	• 特定の車両、機器、ソフトウェア等に関する脅威情報を迅速に検索できる。 • 自組織だけでなく、関連するサプライヤーへの情報提供と注意喚起ができる。
	情報収集機能 ハニーポット, CTF	• 日々出現する新たな脅威情報をプロアクティブに収集し、有益な情報を発信できる