SIP-adus Workshop 2021

Session 6
Cyber Security

自動車に対する新たなサイバー攻撃手法と検知技術に関する調査研究

韓欣一　(PwCコンサルティング合同会社)

9-10, November, 2021

SIP

Cabinet Office

INDEX

1

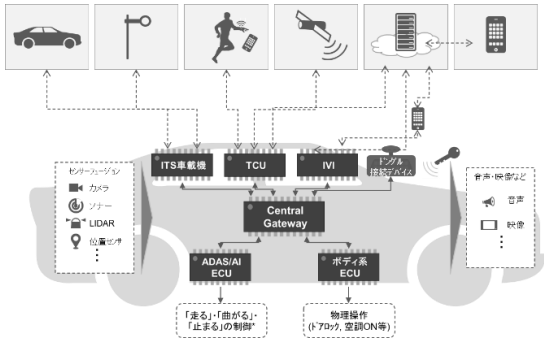
背景と目的

プロジェクト背景と研究目的

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や国際的な法規の整備より、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つの活動を行う。

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

国連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

Research Question : 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

Research Question :自動車に関する脅威情報を収集・蓄積するための方法にはどのようなものがあるか?
:インシデントの初動対応に必要な情報とは何か?

2

車載IDS評価

車載IDS評価の研究目的

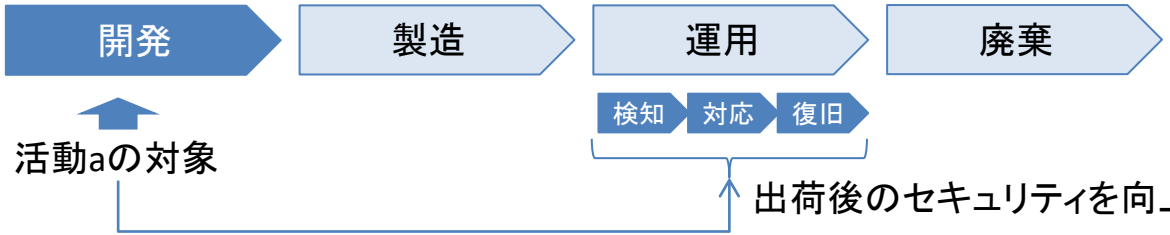
本活動(活動a)では、サイバー攻撃の検知技術である車載IDSの評価方法について調査研究し、開発時に活用できる「IDS評価ガイドライン」として整理することで、自動車業界全体の「出荷後のセキュリティ対策」に貢献します。

出荷後セキュリティに関連した背景

法規面	実務面
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ります。	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ります。

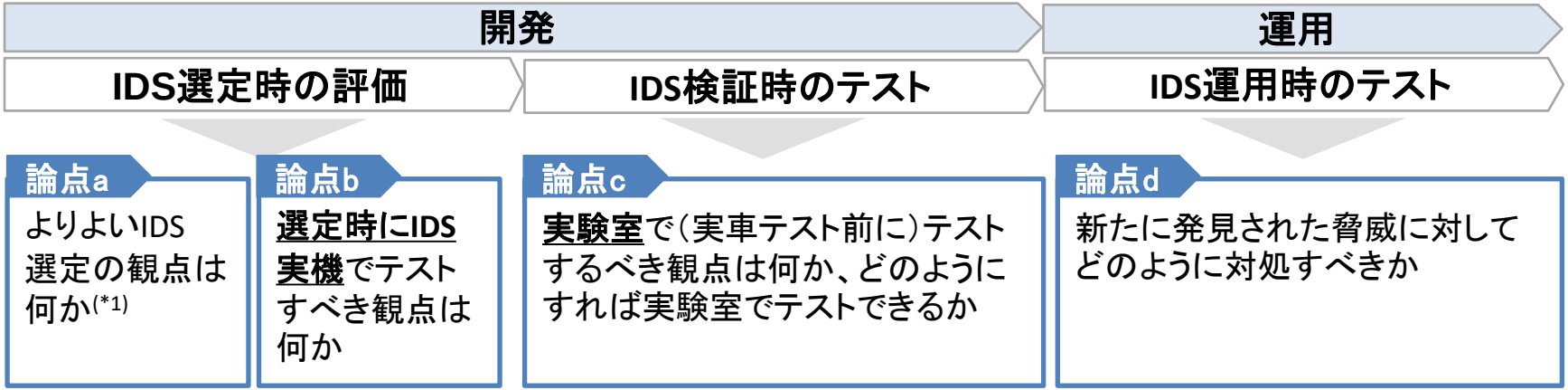
活動aの目的と方針

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します。



フォーカスする論点および研究内容

搭載する車両に必要な機能を備え、より良いIDSを選定し、実験室で可能な限りIDSの動作を検証し、新たな脅威に対応して継続して運用することが重要であると考え、IDSの評価に関わる1～3の研究を行います。

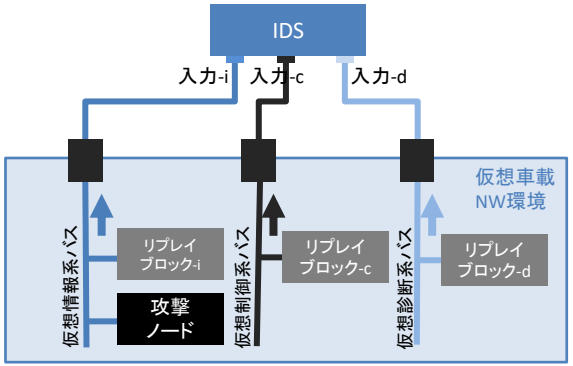


#	活動	対応する論点
活動内容1	仕様に基づく評価観点の検討	a
活動内容2	基本テストケース（テスト観点、前提条件、テスト環境、テスト手順等）の検討	a, b, c
活動内容3	攻撃事例からIDSに求められる検知機能を導出する手法の検討	d

テスト環境例

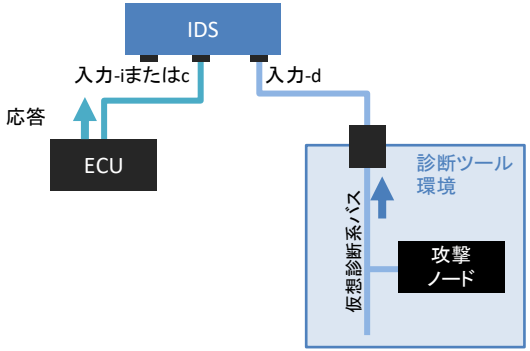
基本テストケースで例として提示するテスト環境は、以下の通りです。基本テストケースのうち、車の状態（停車中、等速直線走行中等）を表すメッセージの入力が必要なものはシミュレーション環境、ECUからの応答の入力が必要なものはテストベッド環境を用いました。

シミュレーション環境



車の状態を表すメッセージ（車速、ステアリングアングル等）の入力が必要、かつ、ECUからの応答を入力する必要がないテストケース用に使用

テストベッド環境



ECUからの応答をIDSに入力する必要があるテストケースに利用。セッションを利用する診断系メッセージへの攻撃の検知に関するテストケースに使用

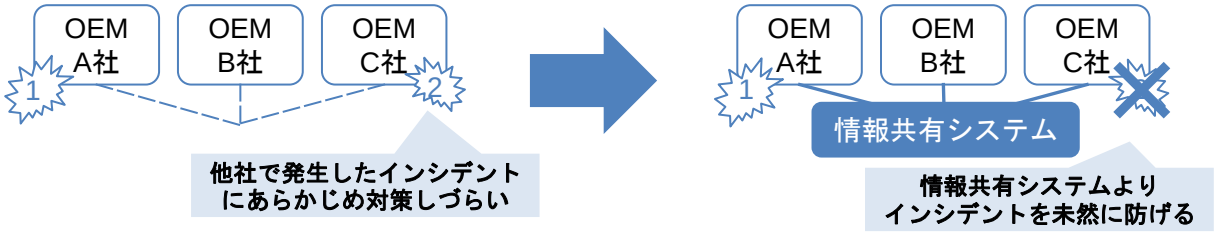
3

脅威情報共有システム

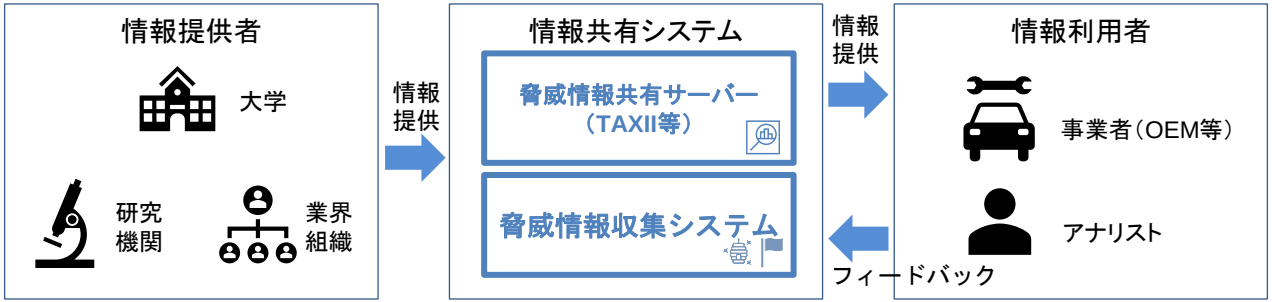
脅威情報共有システムの研究目的

業界全体にわたる情報共有システムの基本仕様を検討し、自動車業界の出荷後セキュリティ対策に貢献します。

✓ 情報共有システムの利点



✓ 情報共有システムの概要



自動車領域での脅威情報共有における仮説と評価方法

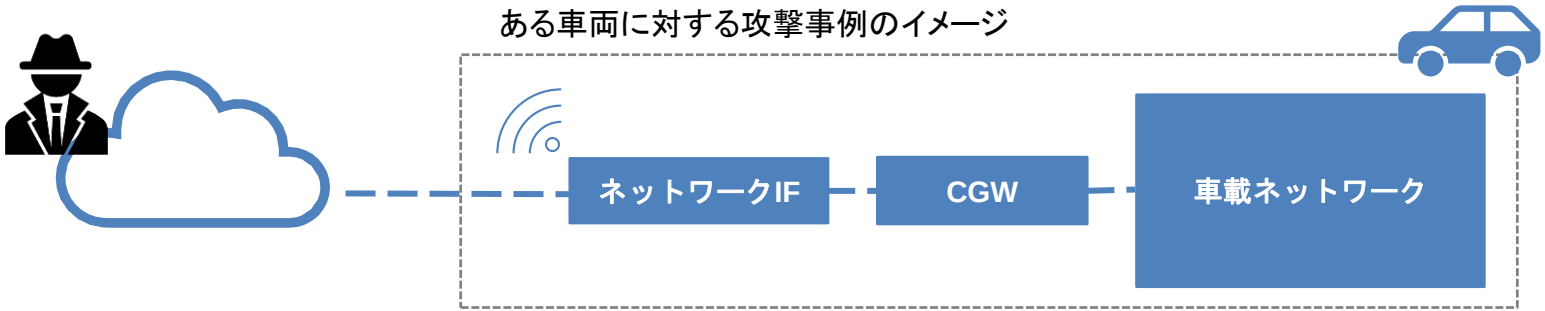
自動車は、ITと違いアーキテクチャがOEM毎に共通ではないため、ある車両に対する事例が、他の車両に対しては脅威とならない可能性が高い。一方で、事例を分析することで、部分的に他の車両でも成立する脅威を得られる可能性があります。

仮説

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



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

評価方法

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します
（窓口としてJ-AUTO-ISACを想定）

脅威情報の収集・蓄積方法について

脅威情報の収集・蓄積の方法として、IT領域で広く使われているSTIX / TAXIIが自動車領域における脅威情報の記述に適しているかを調査します。まずは、過去の報告事例から得られた自動車に係る脅威情報をSTIX形式で記述できるかを検討しました。

目的	• 自動車領域において脅威情報の記述に適している方法を選定する。
仮説	• 将来的にはIT領域で蓄積された脅威情報を自動車領域においても活用することを踏まえると、IT領域で使用されている規格等を採用する利点が多い。 • IT領域で広く用いられている脅威情報共有のための規格は以下の通り。 • STIX / TAXII　• IODEF / RID　• OpenIOC
アプローチ	• 本研究では、IT領域における使用頻度や記述可能な情報の多様性を考慮した結果、STIX/TAXIIを対象としました。 • 自動車分野の脅威情報を収集・蓄積する手法として、STIX/TAXIIが適切かどうか調査開始した。

4

脅威情報観測実験

脅威情報観測実験の目的

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います。

目的	• 自動車領域における脅威情報の収集・蓄積手法を確立したい。
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ます。 • 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だと考えられる。 (例) Honeypot / CTF / OSINT / Bug bounty / Monitoring
収集する脅威情報	• 攻撃者の属性/ TTPs(攻撃手口)
アプローチ	• コネクテッドシステムに対する攻撃パターンを考察し、IT領域の脅威情報収集方法を用いた実験により、自動車領域における脅威情報収集の可能性を評価します。

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します。

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:

- 実際に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？
- 意図せずインターネットにさらされている

- 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？
- コネクテッドカーに対する攻撃のモチベーションは何か?

5

今後の展望

今後の展望

IT領域における基礎調査を経て、情報共有システムに関してはSTIX/TAXII利用検討を進め、脅威情報収集方法として実製品を模したハニーポット実験、プレイグラウンドによる観測実験を計画中です。

2020年

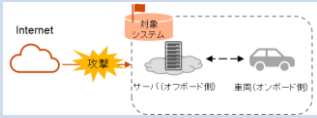
IT領域の基礎調査

- 脅威情報共有活動
- 脅威情報収集手法

2021年

情報共有システム検討

ハニーポット観測実験



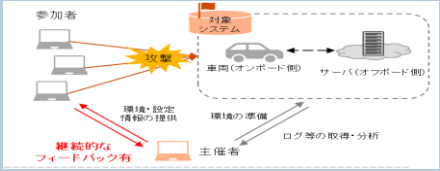
2022年

情報共有システム検討

ハニーポット観測実験

ハニーポット設置数
およびタイプの拡充

プレイグラウンドによる観測実験



Thank you