第13回 日本ITS推進フォーラム

自動走行システム

Cyber Security

今井 孝志

SIP-adus国際連携WG／株式会社トヨタIT開発センター

SIP

Cabinet Office

業界動向およびSIP-adus活動

1. 自動車のセキュリティ動向
2. 自動車業界団体の取組み
3. SIP-adusの取組み

1

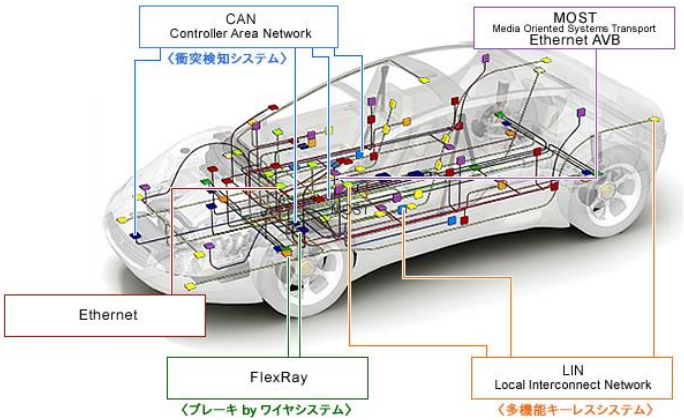
自動車のセキュリティ動向

自動車の構成

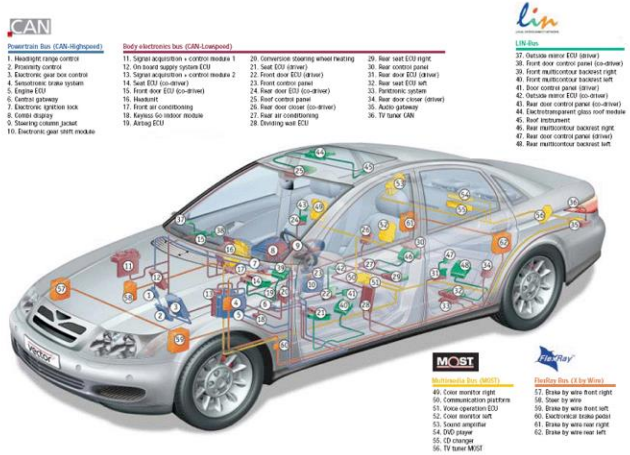
◆自動車内は複数のECU (Electronic Control Units: 電気制御ユニット)で構成

◆用途ごとの特徴や特性に応じて複数の車載LANで繋がっている

◆中でもCAN (Controller Area Network)プロトコルは車載LANの事実上の標準。
「走る・曲がる・止まる」といった自動車の諸機能のサポートに使われている



https://www.renesas.com/ja-jp/solutions/automotive/technology/networking.html

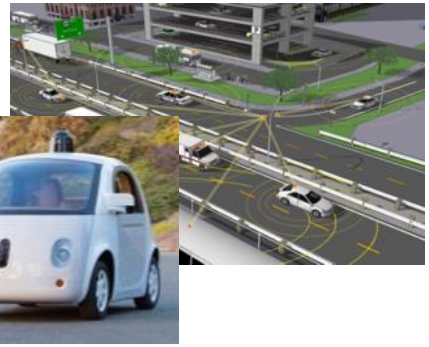


http://monoist.atmarkit.co.jp/mn/articles/0805/09/news152_2.html

自動車の進歩

◆「走る・曲がる・止まる」といった基本機能をサポートしつつ
「安全で快適なモビリティ」を提供する自動車へ

◆自動車内部にあるECU(コンピュータ)が相互に情報を
やり取りして実現する



・『自動運転』と『つながるクルマ』の時代

センサ情報に基づいて
ECUが各種操作を行う

・各種センサで車両周辺
の障害物等検知

・CANによるサポート
・パワステ等
・OBD-IIの義務化

・ADAS(Advanced Diver Assistance System)で
ドライバをサポート(例:衝突防止)

・全てドライバが操作

自動車のセキュリティ動向

クルマのシナリオ	高度運転支援・自動運転：レベル３ → レベル４ つながる：V2V / V2G　ビッグデータ活用　V2X
車両を取巻く環境の変化	車両外通信の増大、自律制御から協調制御 持込み機器の普及、車両との連携機能の増大 標準技術(例:AUTOSAR, Linux,Ethernet等)の活用増大
情報セキュリティ	クラッキングのリスク増大

Security 対策　　つながるクルマ

出典：JasPar

自動車のセキュリティ動向

◆クルマへのハッキングレベルは年々向上

FCA　リコール 140万台

＜対象車両＞
Uconnect（ネット接続サービス）搭載車

＜攻撃内容*＞
PCによる遠隔操作で、
ディスプレイの表示、操舵制動、変速装置を制御
※遠隔攻撃による事故は発生していない

’13
クルマに乗り込んで実施
（通信注入）
※事前に通信内容を解析して攻撃

’15
遠隔からのハッキングに成功
（低速走行時）

＜対象車両＞
Tesla model S
＜攻撃内容＞
PCによる遠隔操作で、
走行中車両のブレーキ作動等を制御

’16
整備モードを利用し、車両を制御（走行時）
※診断用コネクタ経由で通信注入

＜対象車両＞
FCA　Jeep
＜攻撃内容＞
・診断コネクタから整備コマンドを注入
・正規ECUになりすまし、に操舵を制御

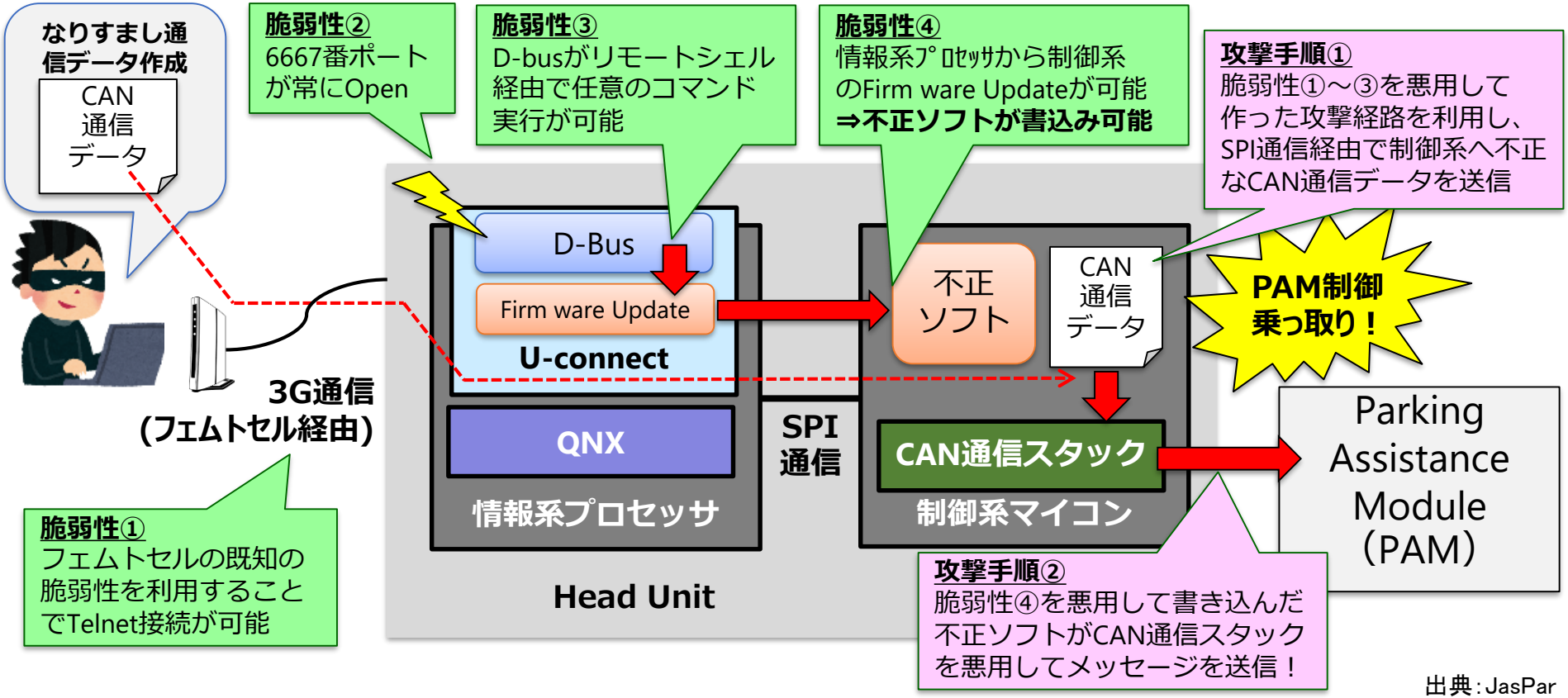
＜対象車両＞
Tesla model X
＜攻撃内容＞
model S同様
（新たな脆弱性を攻撃）

’17
遠隔から複数の脆弱性を攻撃し、車両を制御

出典：JasPar

どのようにして車の制御が乗っ取られたのか？

◆ Head Unitにおける複数の脆弱性を悪用して攻撃経路を開き、CANバスに不正メッセージを流し、PAMの制御を乗っ取った。



出典：JasPar

2

自動車業界団体の取組み

業界団体の取組み

◆クルマの情報セキュリティの難しさ

① IT業界と異なり、**お客様の安全**も扱う

② **「機能安全」（偶発故障）**に対して

「情報セキュリティ」（悪意）をどう考えるか

③ クルマは**ライフサイクルが長い**

クルマの情報セキュリティ上の課題は、競争領域ではなく協調領域。
OEM間、業界団体間で積極的に連携を進める。

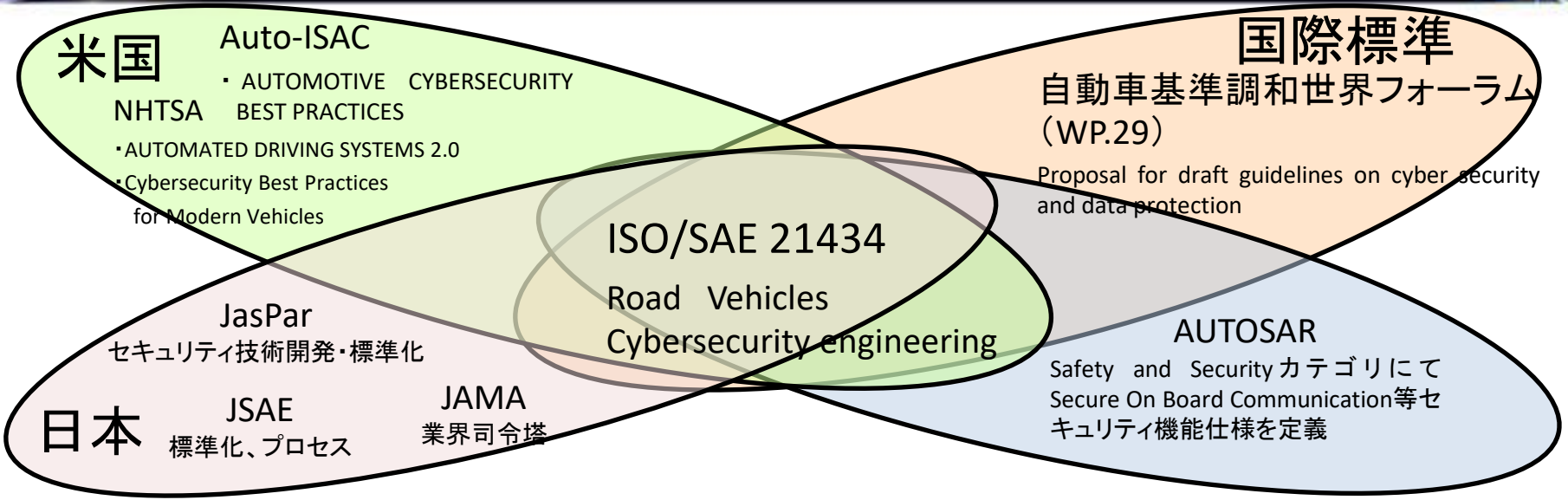
業界団体の取組み

◆ 役割に応じ大まかには、

企画：JAMA　　要件：JSAE　　設計：JasPar　　運用：JAMA

出典：JasPar

セキュリティに関わる標準化／法制化の動き



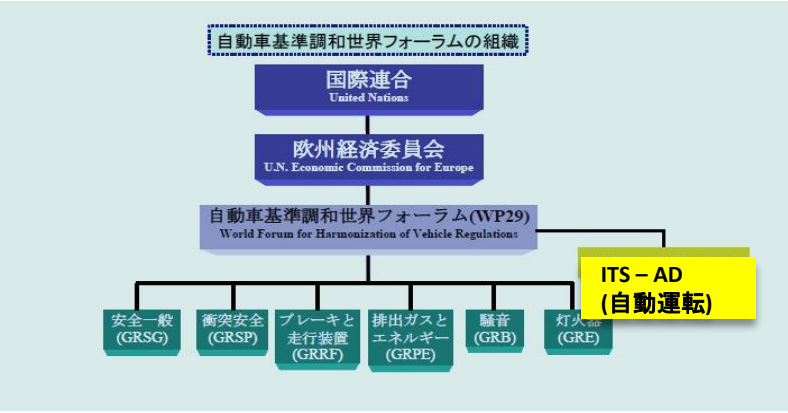
団体名	活動概要
NHTSA	自動運転車両（セキュリティへの要求含む）の規制やガイドを策定。
Auto-ISAC	自動車業界でインシデント／脆弱性情報を共有するための中心組織。
ISO/SAE 21434	ISO(欧)とSAE(米)のJoint workingで、自動車セキュリティ規格を策定。
WP.29	自動運転者・コネクテッドカー向けのセキュリティとデータ保護ガイド。
AUTOSAR	電子プラットフォーム仕様としてセキュリティ機能要求を策定。

出典：JasPar

セキュリティに関わる標準化／法制化の動き

WP29 ～Cyber security and data protection～

- 自動運転車　情報セキュリティガイドライン
- 「外部からのサイバー攻撃」を検知した際に「運転手への警告」と「車両を安全制御すること」を要求
- 「個人データ（Privacy）の漏えいや不正利用からの保護」も要求。



ISO/SAE 21434 ～ Road Vehicles - Cybersecurity engineering ～

- 自動車向けサイバーセキュリティ開発プロセスのISO提案
- ISOとSAE のJoint Working (世界初) で議論されている
- 2020年 発行予定

出典：JasPar

3

SIP-adusの取組み

SIP-adusセキュリティ施策の目的と概要

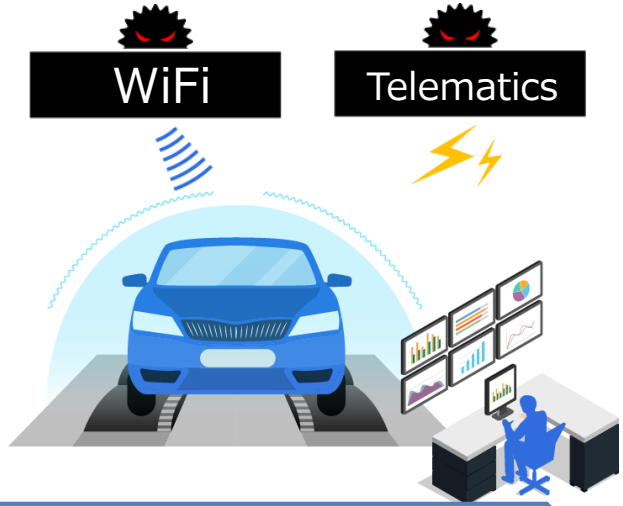
目的　車両のサイバーセキュリティ防御性能評価ガイドライン確立

①脅威分析

◆世界の自動運転実証等の
　システム構成を調査
◆既知の脆弱性や
　インシデントを調査
◆リスク/インパクト分析

②セキュリティ評価ガイドライン策定

③国内OEMとの実証実験による検証



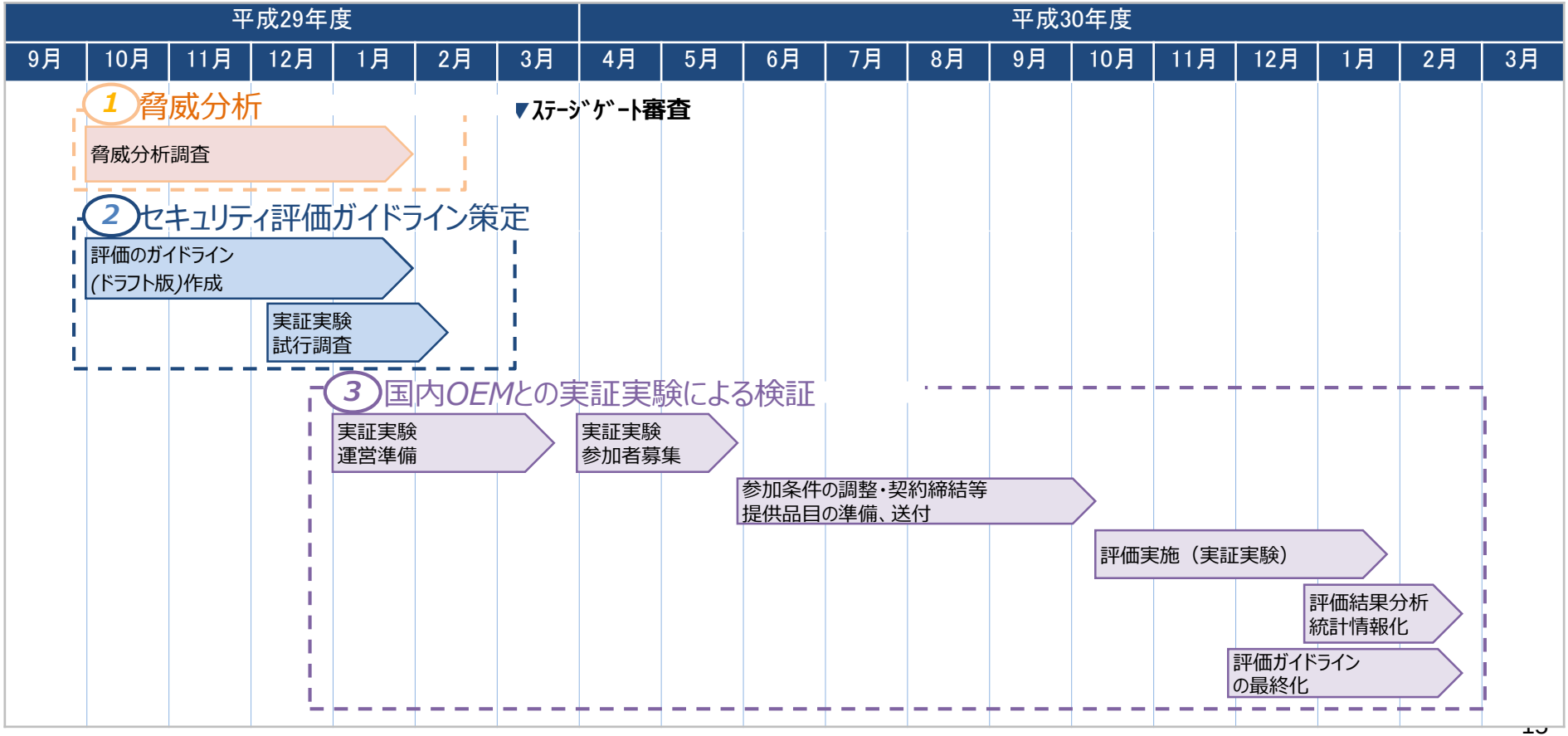
有力セキュリティベンダ3社で競争的にガイドライン策定

①デロイトトーマツリスクサービス　②日本シノプシス、
③PwCコンサルティング＆サイバーディフェンス研究所

最も優れた
ガイドライン選定して実証

PwCコンサルティング＆サイバーディフェンス研究所

全体スケジュール


平成29年度
平成30年度
9月
10月
11月
12月
1月
2月
3月
4月
5月
6月
7月
8月
9月
10月
11月
12月
1月
2月
3月
1 脅威分析
脅威分析調査
▼ステージゲート審査
2 セキュリティ評価ガイドライン策定
評価のガイドライン
(ドラフト版)作成
実証実験
試行調査
3 国内OEMとの実証実験による検証
実証実験
運営準備
実証実験
参加者募集
参加条件の調整・契約締結等
提供品目の準備、送付
評価実施（実証実験）
評価結果分析
統計情報化
評価ガイドライン
の最終化

3
①

SIP-adusの取組み

脅威分析調査

脅威分析の目的と実施アプローチ

目的　自動走行に係るV2X 等車外からの攻撃を含む脅威の全体像の整理する

1 自動走行関連サービスと機能の一覧

- 自動車メーカ、自動車部品メーカ、およびIT企業等の公開情報を調査し、自動走行システム・コネクテッドカーに関するサービスを調査し、それを実現する機能を整理

調査対象

- 自動車メーカ（16社）
- 自動車部品メーカ（4社）
- IT企業（23社）

サービス・機能の一覧

	サービス	機能
1	運転・駐車支援	車間距離制御 車線維持制御 車間距離制御（ITS協調型） 隊列走行 自動運転（ITS協調型） 自動運転（自律型） 駐車周辺映像表示 自動駐車 自動駐車（スマホ連携）
2		…

【インプット】
- 自動車メーカ（16社）、自動車部品メーカ（3社）、IT企業（23社）の公開情報（HPなどを参照）

【アウトプット】
- サービス・機能の一覧

2 機能別のシステム構成想定

- 自動車メーカ、IT企業の公開情報をもとに調査し、機能を実現するシステム構成を検討
  ＊業界の有識者へのインタビュー結果も考慮

機能の想定システム構成

	サービス	機能
1	運転・駐車支援	車間距離制御 車線維持制御 車間距離制御（ITS協調型） 隊列走行 自動運転（ITS協調型） 自動運転（自律型） 駐車周辺映像表示 自動駐車 自動駐車（スマホ連携）
2	…	…

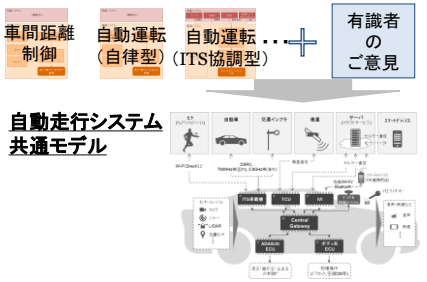
【インプット】
- サービス・機能の一覧
- 主要な自動車メーカ・IT企業が公開する機能に関する公開情報
- 有識者インタビューにおけるご意見

【アウトプット】
- 機能別の想定システム構成

3 自動走行システム共通モデルの特定

- 機能別の想定システム構成をすべて勘案し本脅威分析調査における自動走行システム共通モデルを特定
  ＊業界の有識者へのインタビュー結果も考慮

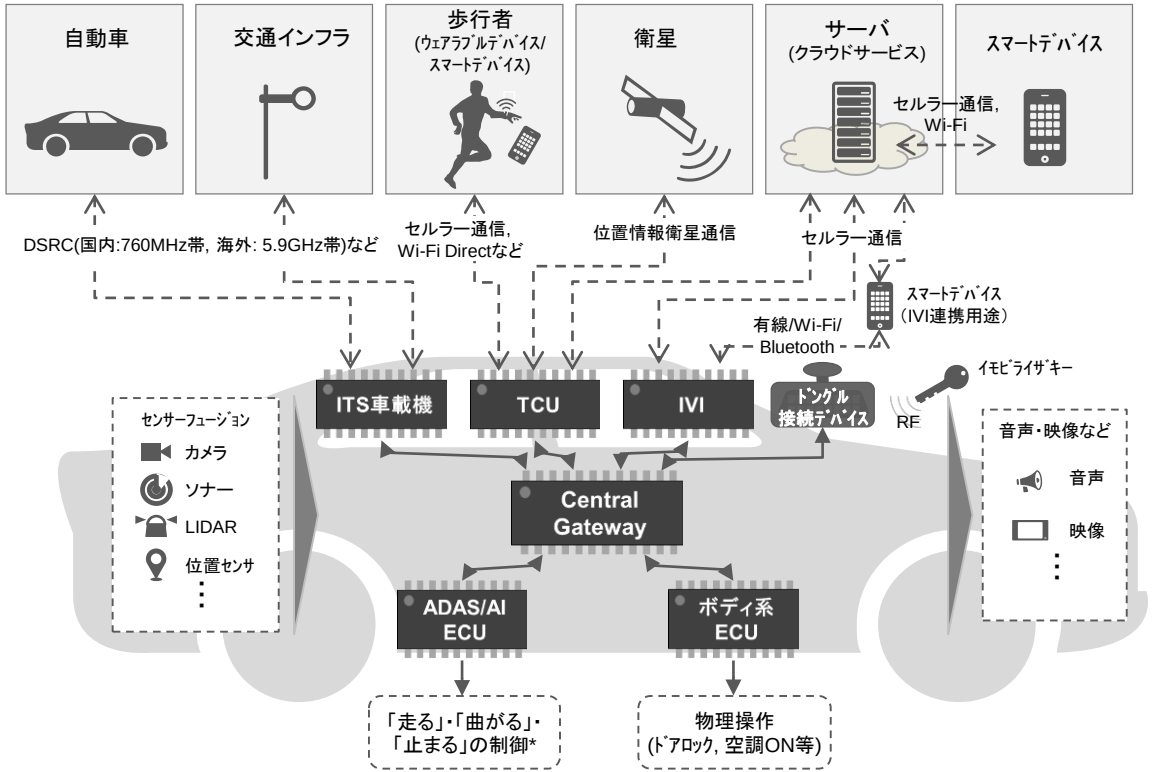
機能別の想定システム構成



【インプット】
- 機能別の想定システム構成
- 有識者インタビューにおけるご意見

【アウトプット】
- **本脅威分析調査における自動走行システム共通モデル**

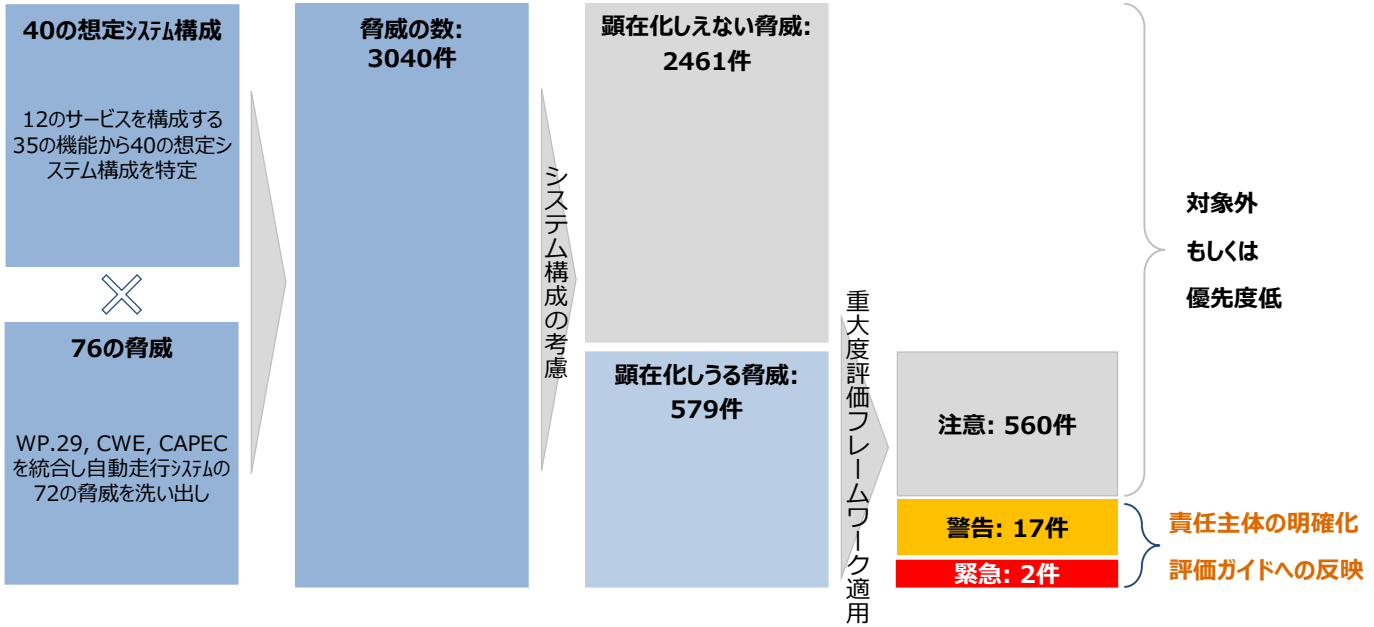
自動走行システム共通モデル（2020年代前半の想定）



*ステアリング・ブレーキ・エンジン等に係る制御機能のトポロジーは本脅威分析結果に直接影響しないため抽象化

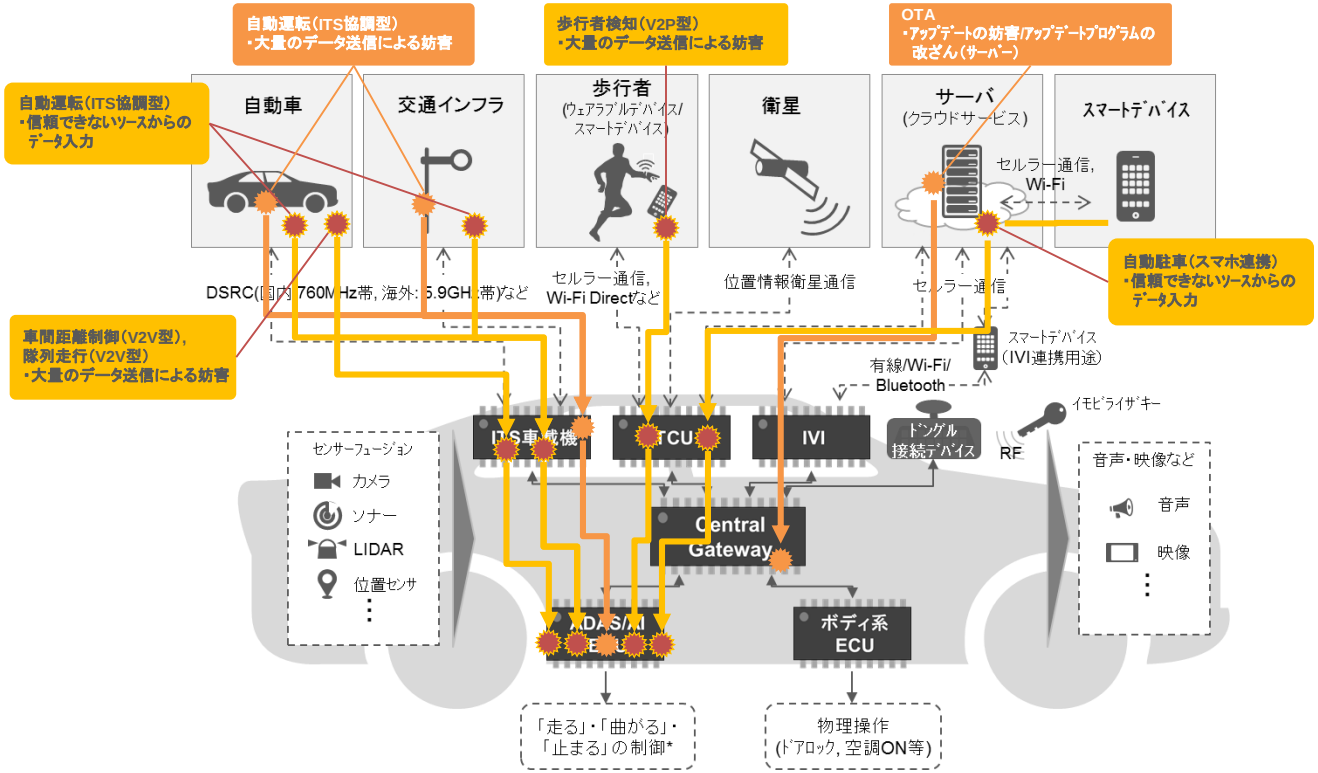
脅威分析の分析結果概要①

- 自動走行システムに係るすべてのシステム構成を踏まえ顕在化しうる脅威を抽出し、重大度評価フレームワークを適用することで優先して対応すべき脅威を特定
- 特定した脅威に対して、対策の責任主体を明確化するとともに、車両側での対策が必要な脅威は、評価ガイドへ反映



脅威分析の分析結果概要②

重大な脅威について共通モデルに図示



SIP-adusの取組み

セキュリティ評価
ガイドライン策定

ガイドライン概要

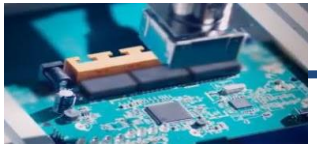
多様なサイバー攻撃を行い、車両侵入の足掛かりになるセキュリティ設計情報等を奪われない事や、攻撃により不正動作が発生しない事を評価

評価項目

大項目	中項目
1. 偵察	1.1 HW調査 1.2 SW調査
2. 侵入	2.1 ユーザー介在型の受動的攻撃 2.2 ユーザー非介在型の受動的攻撃 2.3 脆弱性を利用した能動的攻撃 2.4 通信傍受した情報を用いた能動的攻撃
3. 権限昇格	3.1 保護機能の解除 3.2 高権限の奪取
4. 目的の実行	4.1 情報漏えい 4.2 サービス停止 4.3 不正操作（制御系） 4.4 不正操作（制御系以外）

評価内容例

①ECUからのチップはがし



eMMC

EEPROM

②ファームウェア抽出

③ファームウェア(バイナリファイル)解析

リバースエンジニアリング

④ソースコード復元によるセキュリティ設計等把握

評価者(攻撃者)

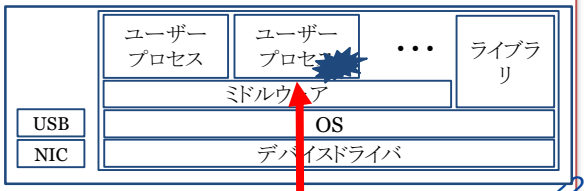
「1. 偵察」で得た車両セキュリティ情報

攻撃ツール（コード）

0101011011101010010
1101010101101111011

攻撃実施

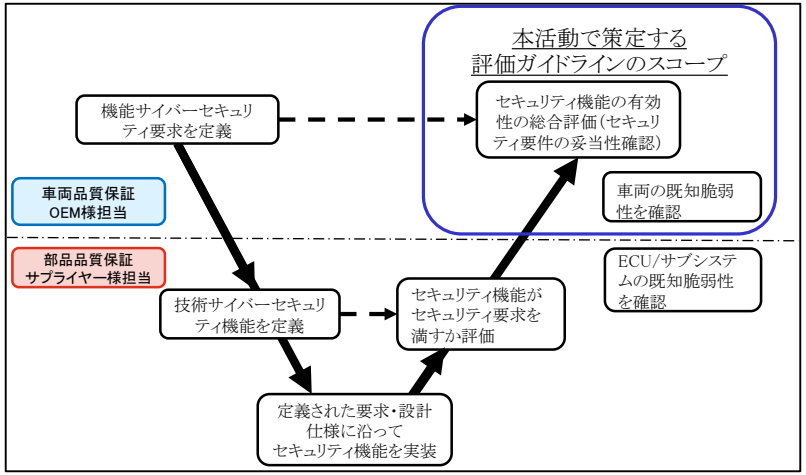
車両システム



ガイドラインのスコープと特徴

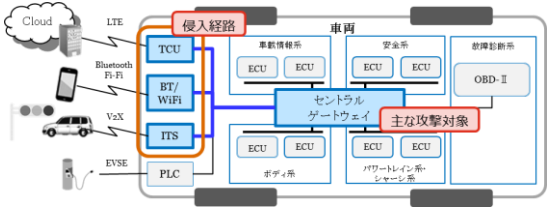
スコープ

- 車両OEM各社、JasPar等のステークホルダとの議論および脅威分析の結果を踏まえ、車両開発のV字モデルにおける総合評価などで活用できるガイドラインにする方針とした

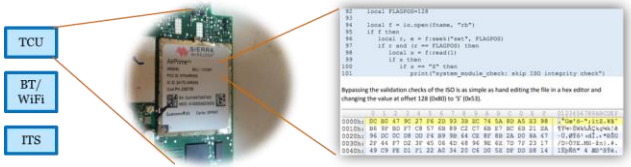


特徴

1. 実際のハッカー（攻撃者）の視点で車両外部I/Fから侵入テストによる評価



2. 現実の車両攻撃内容を考慮したHWセキュリティ対策も評価対象とする

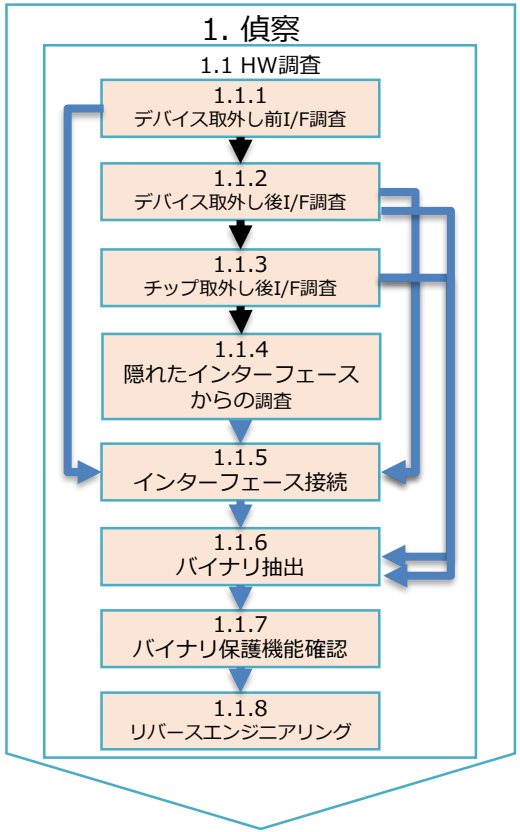


ガイドライン情報源（車両インシデント）

本ガイドラインは実際の過去車両インシデントをプロファイルし、再現する手法を取り込んでいるため同種の車両インシデントの再発を防止します。

インシデント事例	インシデント概要
Jeep CherokeeのuConnect脆弱性	第３者により車両位置の特定やリモートで車両を操作される脆弱性。Cellular Network上の開放ポートから車載器に侵入し、CANコントローラのファームウェア改ざんすることで車両をリモート操作することが可能
BMWのConnectedDrive脆弱性	第３者により車両をリモート操作される可能性のある脆弱性。研究者の用意したテレマティクスサーバーから車両に対しドア解錠のコマンドを送ることでドアを解錠することが可能
Tesla ModelSの無線LAN脆弱性	第３者により車両をリモート操作される脆弱性。研究者は偽WiFiスポットを利用して攻撃サイトに誘導する方法を提示したが、Cellular Networkを介した攻撃も可能である。その場合、おとりメール等を用いて、ユーザーを攻撃サイトに誘導する。
三菱アウトランダーのモバイルアプリ脆弱性	第３者により空調設定等の環境設置をリモート操作される脆弱性。車内に設置されたWiFiスポットにアクセスすることで防犯装置の設定や空調操作をリモート操作することが可能
日産Nissan Connect EVの脆弱性	一般ユーザーが利用しない開発設定が残存しており、これを利用することでユーザーID,パスワード等の機密情報が外部に漏えいさせることが可能
日産リーフの脆弱性	認証方式に不備があり、スマートフォン⇔サーバーAPIに認証の仕組みが実装されておらず、VIN下5桁が判明すれば他の車両を制御することが可能 ※スマートフォンアプリの脆弱性であるが、車両⇔サーバー、あるいは車両⇔スマートフォンで同様の事象が発生しないか確認する
スバルStarLinkの脆弱性	スマートフォンのデバイス認証に使用されるセキュリティトークンには有効期限がなく、窃取された場合、第３者によりドアを解錠させることが可能 ※スマートフォンアプリの脆弱性であるが、車両⇔サーバー、あるいは車両⇔スマートフォンで同様の事象が発生しないか確認する
Continental AGのTCUの脆弱性	第３者によりTCUがリモート操作される可能性のある脆弱性
マツダのMazda Connectの脆弱性	車内のUSBポートから任意のコードを実行される脆弱性。AVNのカスタマイズに利用された ※ローカル攻撃であるが、リバースエンジニアリング耐性を図る評価ポイントとして採用
本田技研工業のHonda Connectの脆弱性	車内のUSBポートから任意のコードが実行される脆弱性。AVNのカスタマイズに利用された ※ローカル攻撃であるが、リバースエンジニアリング耐性を図る評価ポイントとして採用

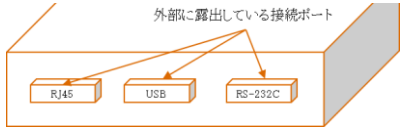
1.偵察/1.1 HW調査



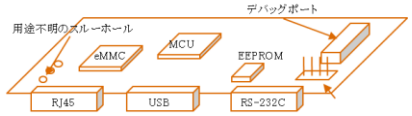
【評価方針】

- 搭載HW（車両,デバイス,チップ）が*データ入出力に使うすべてのI/F*からのデータ抽出を試行し、成功した段階でバイナリファイルをリバースし、システムを解析する

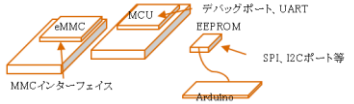
【1.1.1 対象I/F】
RJ45, USB, RS-232C等



【1.1.2 対象I/F】
デバッグポート(JTAG等),
UART, 不明なスルーホール



【1.1.3 対象I/F】
デバッグポート,UART（ピン),
MMC I/F, SPI, I2Cポート等



【インシデント以外で取り込んだ評価項目】

- バイナリ抽出にあたり、データ入出力I/F以外からデータ抽出を行う手法を項目化した
  ex.レーザー照射を用いたレジスタビット反転による抽出
  顕微鏡を用いた半導体回路の撮影による抽出
  セキュアエレメントからのデータ抽出、解析

1.偵察/1.2 SW調査

1. 偵察

1.2 SW調査

1.2.1 アプリケーションの通信経路の調査

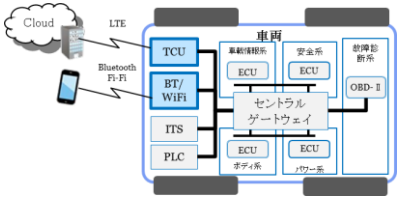
1.2.2 WiFi(外部設置）の通信傍受	1.2.3 WiFi(内部設置）の通信傍受
1.2.4 BlueTooth の通信傍受	1.2.5 BluetoothLEの通信傍受
1.2.6 TCUの通信傍受	1.2.7 CANメッセージの通信傍受
1.2.8 ブラウザ、HTMLエンジンの調査	1.2.9 アプリケーションの通信傍受

※並行実施

【評価方針】

- 車両システムが持つ下記の無線通信（当該機能を有するコンポーネント）を対象として通信傍受を試行し、侵入・なりすましに必要な情報を入手する

【対象通信】
- TCU(3G/4G)
- WiFi
- Bluetooth

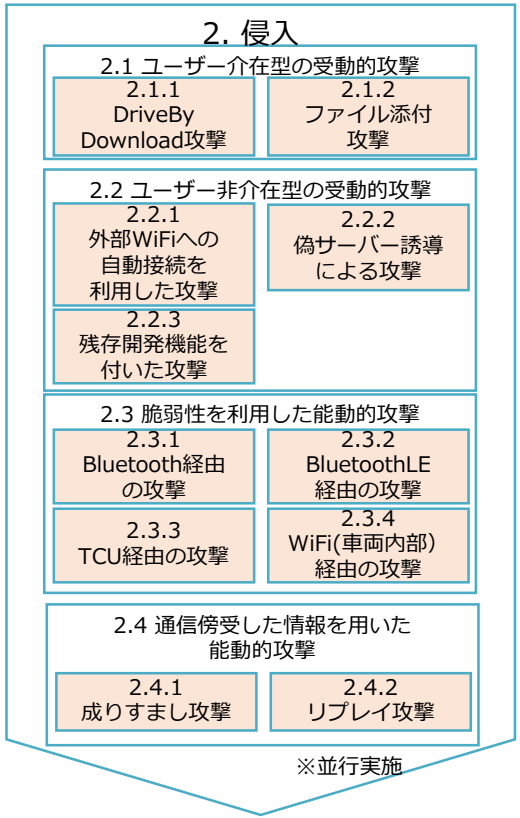


- 上記無線I/Fを利用するすべてのアプリケーションに対して、送受信データの傍受を試行し、侵入・なりすましに必要な情報を入手する

【インシデント以外で取り込んだ評価項目】

- Bluetooth関連について、Bosch社のBluetoothドングル等の車両部品システムにインシデント事例があり、それら内容を項目化した

2.侵入



【評価方針】

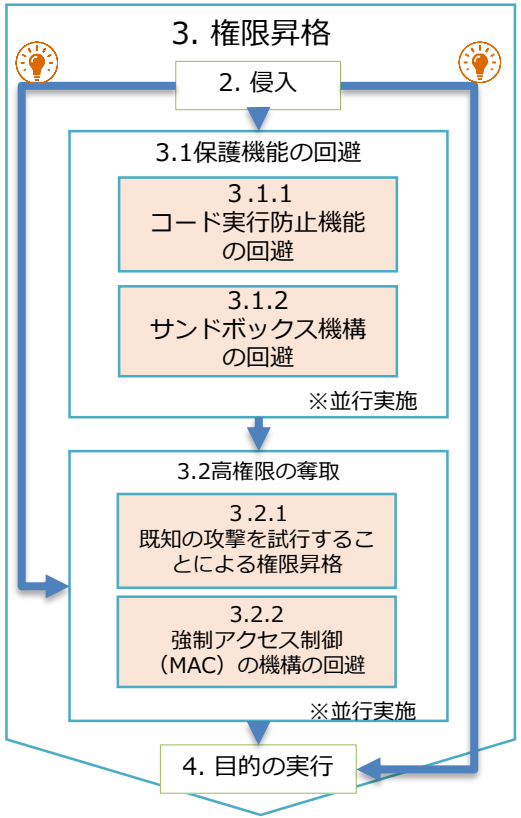
- 無線I/Fを経由した攻撃を試行し、システムのコンソールが利用できる段階までの攻撃（侵入）を行う
- 攻撃方法に影響を与える「車両NWアクセス条件」、「搭乗者関与」を軸に攻撃パターンを分類

搭乗者関与 / NWアクセス	搭乗者の介在を必要とする攻撃（人を罠に嵌める）	搭乗者が不要な自動化された攻撃（機械を罠に嵌める）
外部NWから車両への直接接続しない（外部からのレスポンスのみ）	攻撃プログラムの実行開始を人の操作に頼る攻撃 評価項目 2.1	システムが自動アクセスする対象を攻撃者の意図で誘導する 評価項目 2.2
外部NWから車両への直接アクセスが可能	(N/A)	各種I/Fの脆弱性をつく攻撃(評価項目 2.3) 通信傍受した情報を使う攻撃(評価項目2.4)

【インシデント以外で取り込んだ評価項目】

- Bluetooth関連について、Bosch社のBluetoothドングル等の車両部品システムにインシデント事例があり、それら内容を項目化した
- ITセキュリティで攻撃事例および被害の多い標的型攻撃を考慮するものと判断し、「ファイル添付攻撃」「偽サーバー誘導による攻撃」を項目化した

3.権限昇格



【評価方針】

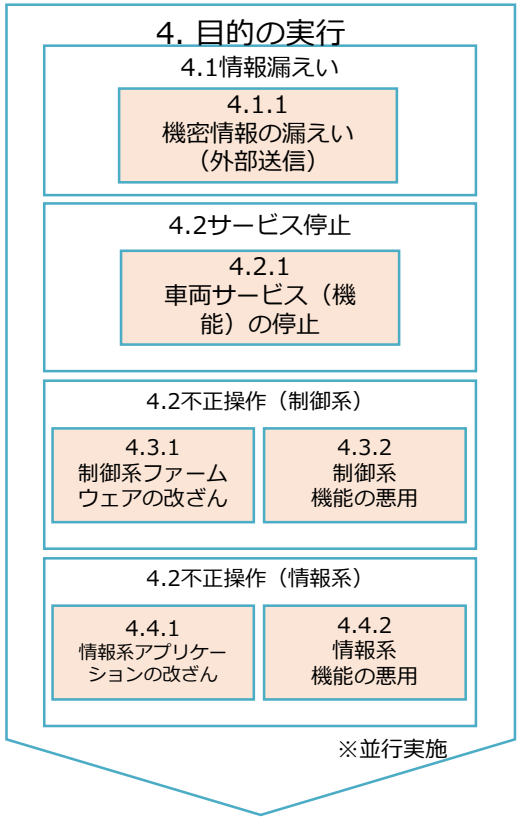
- 任意コード実行が失敗した際のエラー状態に応じて、当該原因の回避策を試行する
- 任意コード実行の失敗の状態と原因は以下のとおり

失敗の状態	評価項目	失敗の原因	防御機構例
実行できない	3.1.1.	意図した位置にコードが存在しない	ASLR
		コード実行禁止のセグメントに配置	DEP、Nxbit
攻撃対象にアクセスできない	3.1.2.	コード実行が管理された領域に配置された	サンドボックス
実行が途中で停止する	3.2.1.	実行権限の不足	一般アクセス管理
	3.2.2.	強制アクセス制御による停止	SELinux

【インシデント以外で取り込んだ評価項目】

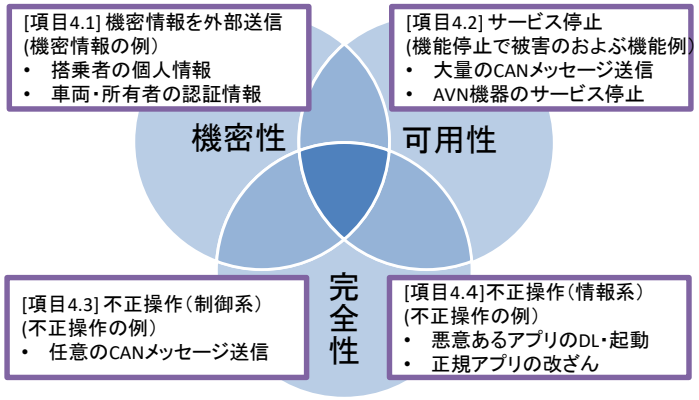
- IoT製品（特にスマートデバイス）でのJailBreak事例を踏まえ、今後車両セキュリティで同種の問題が発生することを考慮し、各項目化した

4.目的の実行



【評価方針】

- セキュリティ特性（CIA：機密性、完全性、可用性）の各観点で、システムに被害を及ぼす攻撃を実行する



【インシデント以外で取り込んだ評価項目】

- 特になし
  （既知の車両インシデントでは攻撃後に機密性、完全性、可用性それぞれの観点で攻撃が実行されている）

3
③

SIP-adusの取組み

国内OEMとの
実証実験によるガイドライン検証

国内OEMとの実証実験によるガイドライン検証

目的　策定したガイドランを実システムに適用することで検証し改善する

実証実験により実システムにて評価を行うことの重要性を確認

参加数

平成29年度に、国内の**OEM1社参加**での実証実験（試行）実施

平成30年度に、**OEM4社参加**での実証実験実施

成果項目

実証実験を通じた検証・改善により情報セキュリティ評価ガイドライン最終化

実証実験成果報告項目

① 参加者からの実施内容・項目に対する評価
② 実証実験実施を通した評価プロセス整理
③ 実証実験実施を通した評価ガイドライン改善

成果①:参加社からの実施内容評価

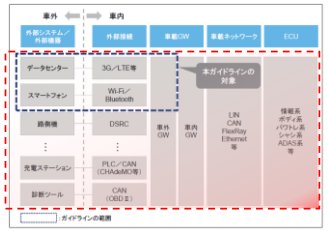
評価項目	評価内容
評価手法の確立 (評価ガイド策定)	• 一定レベルのセキュリティ品質確保に寄与する手法 • 属人性の高いペネトレーションテストの均質性向上に寄与する手法
車両システムを 用いた実証実験	• 評価ガイドの妥当性検証に寄与する活動 • 複数車両を用いた検証が良い取り組み
今後の取り組み	• 発見された問題への対策検討などは依然、評価者依存である点は改善の余地ある • V字後期の総合評価だけでなく、設計等前工程でも活用できるガイド化を望む

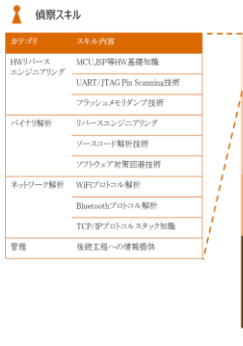
成果②：評価プロセスの整理

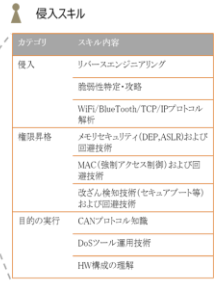
実証実験を通じて車両システムセキュリティ評価（ペネトレーションテスト）の標準的な評価プロセスを定め、アセスメントとして活用できる手法として確立

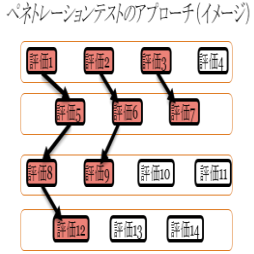
規定した評価プロセス

1. 評価対象定義
2. 評価条件定義
3. 評価項目定義
4. 評価実施



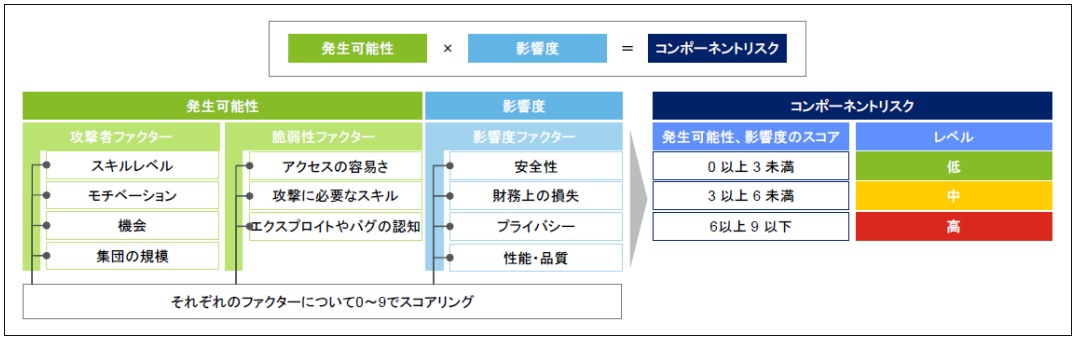


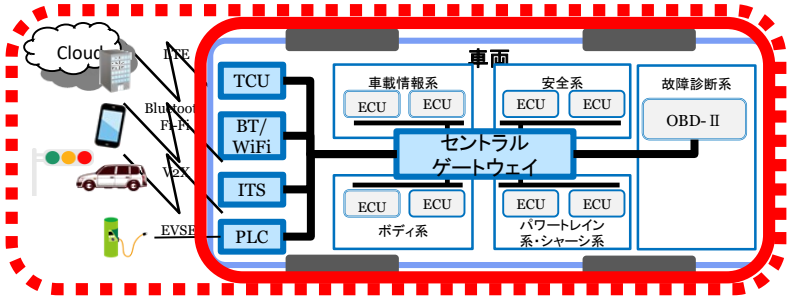




プロセス1. 評価対象選定

車両システム全体および周辺システムを対象にリスク分析を実施し、リスクの高い攻撃I/Fおよびコンポーネントを選別し、本手法による評価対象として選定・定義する





プロセス2. 評価条件定義

評価条件	具体的な条件内容
評価者のスキル	• 評価に必要となるスキルを明確化し、事前に評価者・管理者によるチェックを実施
評価工数	• （本実証実験では） 標準評価期間を計2ヵ月(40営業日）×2名とし、当該工数による評価を実施
評価環境（車両）	• 実際に用意できた機材を踏まえた、可能な評価環境を確認

評価結果	
評価の判定基準	【偵察フェーズ】 上記スキル・期間を充足する評価を実施した結果、偵察が成功せず、対象の安全性をその理由とともに確認することができた 【侵入フェーズ】 上記スキル・期間を充足する評価を実施した結果、いずれのI/F経由でも侵入を成功することができなかった

【参考】「評価者のスキル」の概要

偵察スキル

カテゴリ	スキル内容	概要
H/W解析	表面解析	ハードウェアの知識に基づいてプリント基板構成を分析しデバックポートや外部通信ポートを探索、特定する
	加工処理	プリント基板上にはんだ付けされたフラッシュメモリ等の剥離、再度はんだ付けを行う他、必要に応じてプリント基板に加工処理を施す
	データ入出力ポートからのバイナリ抽出	各種ツール等を用いてプリント基板から剥離したフラッシュメモリ、外部通信ポートからデータの抽出および書込みを行う
	デバッグポートからのバイナリ抽出	上記特定したデバッグポートからデータを抽出する
バイナリ解析	ファイルシステム解析	フラッシュメモリから抽出されたデータを解析し、ファイルシステム等のデータ構造を分析、把握する
	ソフトウェアアーキテクチャ解析	ファイルシステム上から抽出されたファイル群を解析し、OS、ライブラリ等のソフトウェアアーキテクチャを分析、把握する
	バイナリコード解析	特定されたプログラムファイル等の各ファイルを分析し、その設計・実装を分析、把握する
	ソースコード解析	各種ツールによりバイナリコードの逆コンパイルを行い、ソースコードレベルでの設計・実装を分析、把握する
	保護機能の回避	データの暗号化、難読化、エンコード等のソフトウエア的に実装された保護機能を分析、回避する
ネットワーク解析	WiFi通信解析	WiFi通信の傍受、解析を行う
	BlueTooth／BlueTooth LE通信解析	BlueToothおよびBlueTooth LE通信の傍受、解析を行う
	セルラー通信解析	セルラー通信の傍受、解析を行う
	TCP/IP通信解析	TCP/IP通信の傍受、解析を行う
管理	後続工程への情報提供	上記の偵察工程で分析・把握した情報を管理し、後続のフェーズへ提供、連携する

【参考】「評価者のスキル」の概要

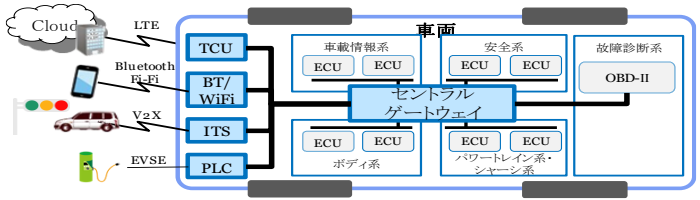
侵入スキル

カテゴリ	スキル内容	概要
侵入	脅威分析	偵察フェーズの結果を踏まえて侵入の起点になると考えられるアタックサーフェイスを分析、特定する
	バイナリコード解析	脅威分析の結果に基づきアタックサーフェイスとなるプログラムファイル等の各ファイルを分析し、その設計・実装を分析、把握する
	脆弱性特定・攻略	バイナリコード解析と並行またはその結果を踏まえて侵入に利用可能な脆弱性を特定し、攻撃コード等を作成することで攻略する
権限昇格	脆弱性緩和技術の回避	データ実行防止、アドレス空間ランダム化等の脆弱性緩和技術を分析、回避する
	安全機構の回避	製品特有の安全機構（動作条件の制限、性能制限等）を分析、回避する
	強制アクセス制御機構の回避	SELinuxに代表される強制アクセス制御機構を分析、回避する
	改竄検知機構の回避	セキュアブートに代表される改ざん検知、完全性検証機構を分析、回避する
目的の実行	車載ネットワーク分析	車載ネットワーク全体の構成（セントラルゲートウェイおよび各種EUCの配置等）を分析、把握する
	CAN通信解析	ネットワーク分析の結果を踏まえたCAN通信の傍受、分析、再送等を実施する
	攻撃検証・再現	上記の偵察および侵入工程の結果を踏まえて脆弱性を悪用した攻撃を検証・再現する

プロセス3. 評価項目定義

リスク評価、条件確認の結果を踏まえ、（既存の）セキュリティ評価項目から
実際に実施すべき評価項目および実施順序を決定する

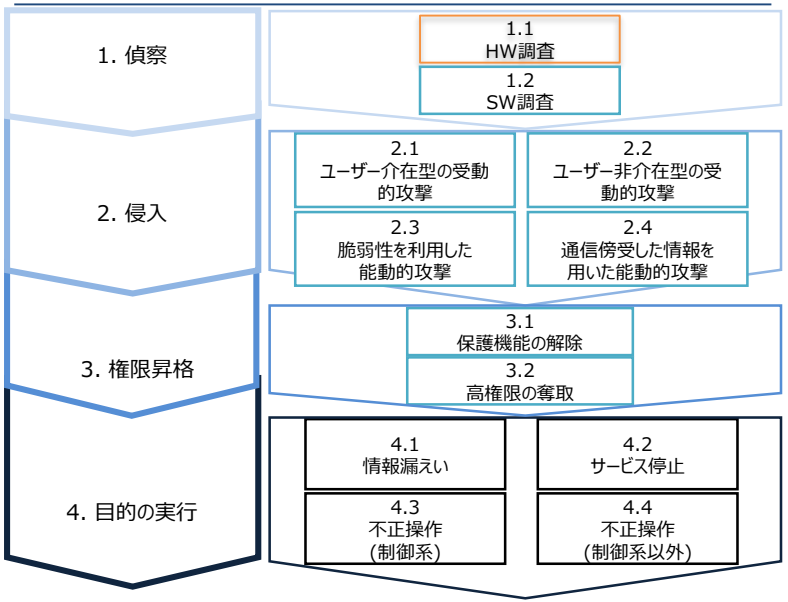
評価対象



評価条件

- **評価者のスキル**
- **評価工数**
- **評価環境（車両）**

評価ガイドライン項目



プロセス4. 評価実施

定義した評価項目に沿って、評価を実施する。ペネトレーションテストの特性を踏まえた評価運営と評価結果に記載すべき項目を規定

ペネトレーションテストの実施フロー

事前準備

- 対象機材に加え、実施する評価項目に合わせて、必要なセキュリティツールを十全に準備する
- 具体的な評価体制・メンバーを確定する

評価実施

- 評価体制役割を明確かし、実施
- 評価リーダー
  評価の状況を踏まえて、侵入の戦略を立案・決定
- 評価者
  リーダーの方針に沿って評価を実施

結果報告

- 結果報告では、以下の内容を報告する
- 評価における試行作業の全体（侵入失敗フローを含む）
- 評価の実施手順・ツール利用・プログラム（依頼者が再現確認ができること）
- 対策提案（見つかった問題を修正する方法）

成果③：実証実験実施を通じたガイドライン改善

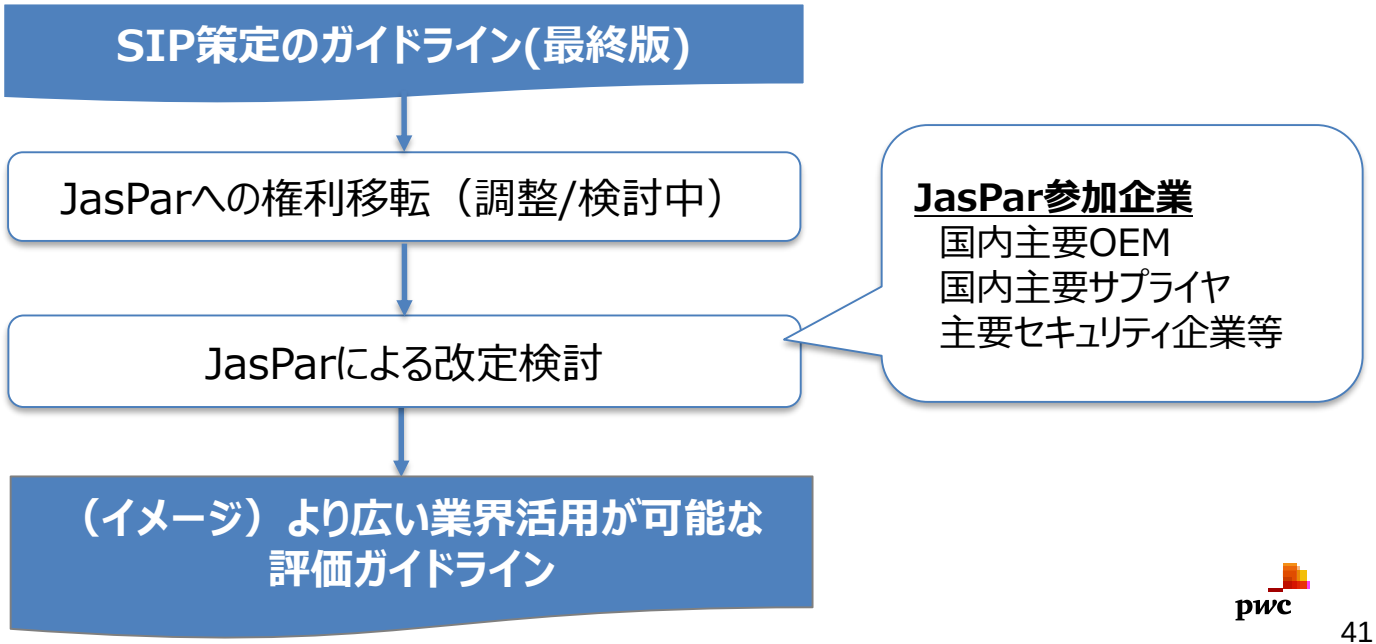
本年度実証実験により、現時点で評価項目19件に関して改善予定

※太枠内は評価内容として特に重要な項目

ガイド項番	内容	理由
1.1.1 デバイス取り出し前I/F調査	評価項目更新「1.1.1.1 USBポート接続確認」	実施結果を受けた評価者による内容見直し
	評価項目追加「1.1.1.4 SDカードの確認」	実施結果を受けた評価者による内容見直し
1.1.3 チップ取り外し後I/F調査	評価内容更新「1.1.3.2 フラッシュメモリのチップ調査」	評価実施者による記述更新
1.1.5 インターフェース接続	評価内容更新「1.1.5.5 バイナリ改ざんによるコンソールの取得」	評価実施者による記述更新
1.1.6 バイナリ抽出	評価内容更新「1.1.6.1 UART(OS起動状態)からのバイナリ抽出」	評価実施者による記述更新
	評価内容更新「1.1.6.3 UART(BootLoader起動状態)からのバイナリ抽出」	評価実施者による記述更新
	評価内容更新「1.1.6.5　フラッシュメモリからのバイナリ抽出」	評価実施者による記述更新
1.1.7 バイナリ保護機能確認	**評価項目追加「1.1.7.8 難読化の調査」**	**実証実験のフィードバック反映**
1.1.8 リバースエンジニアリング	**評価項目追加「1.1.8.2 ターゲットの選定」**	**実証実験のフィードバック反映**
1.2.6 TCUの通信傍受	評価項目更新「1.2.6.1 モデムの調査」	実施結果を受けた評価者による内容見直し
	評価項目追加「1.2.6.2 TCU－IVI間の通信傍受」	実施結果を受けた評価者による内容見直し
1.2.8 CANメッセージ通信傍受	評価手法更新「1.2.8.1 CANメッセージキャプチャツールの設置」	評価実施者による記述更新
2.3.4 WiFi（車両内部）経由の攻撃	評価手法更新「2.3.4.1 公開ポートからのログイン」	評価実施者による記述更新
	評価手法更新「2.3.4.3 APIソースコードの解析」	評価実施者による記述更新
3.1.2 任意アクセス制御(DAC)の回避	評価手法更新「3.1.2.2 任意アクセス制御の確認の回避」	実施結果を受けた評価者による内容見直し
3.1.3 安全機能の回避	評価中項目追加	実施結果を受けた評価者による内容見直し
3.2.1 権限昇格防止機能の回避	評価手法更新「3.2.1.1 権限昇格防止機能の確認」	実施結果を受けた評価者による内容見直し
	評価手法更新「3.2.2.2 強制アクセス制御の回避」	実施結果を受けた評価者による内容見直し
3.3.1 SecureBootの回避	**評価中項目追加**	**実施結果を受けた評価者による内容見直し**

今後のガイドライン活用に向けた取り組み

SIP自動走行（第１期）の終了にあたり、本ガイドラインの自動車業界での活用と今後の管理を見据え、車両セキュリティに関する技術規格を策定するJasParへガイドライン権利移転を行ったうえで、より広い活用に向けた協議を進めている




Thank you