第12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

SIP-adus活動及び、業界団体連携

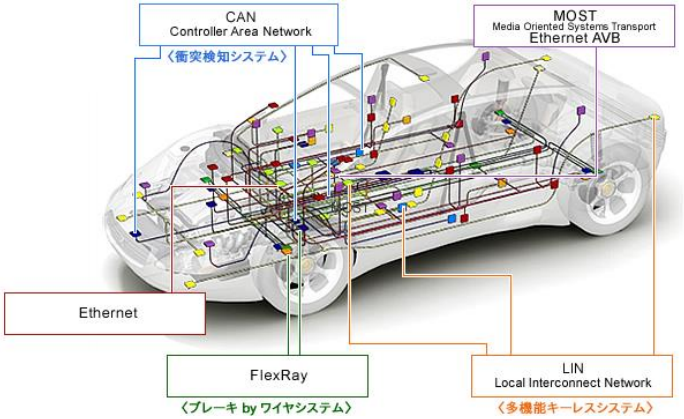
1. 自動車のセキュリティ動向
2. 自動車業界団体の取組み
3. Auto ISAC
4. 情報セキュリティ研究開発シナリオ検討

自動車の構成

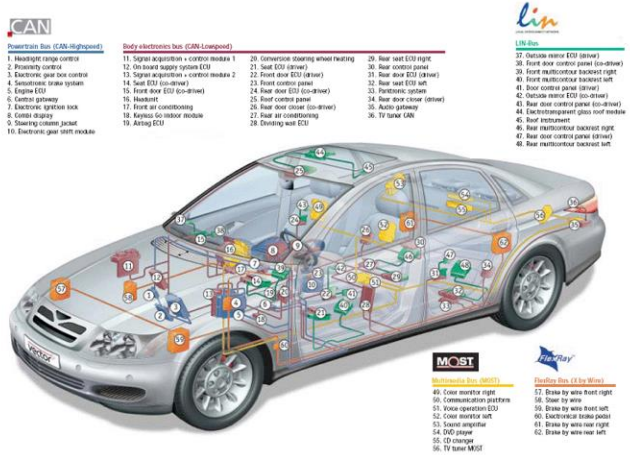
◆自動車内は複数のECU (Electronic Control Units: 電気制御ユニット)で構成

◆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

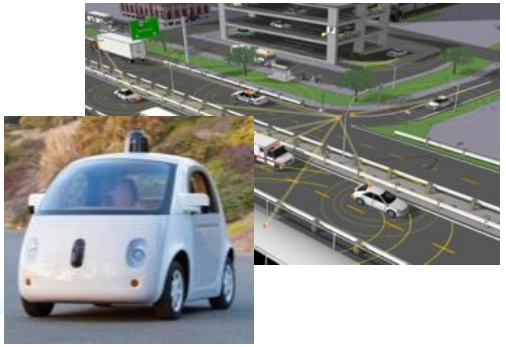
◆「走る・曲がる・止まる」といった基本機能をサポートしつつ「安全で快適なモビリティ」を提供する自動車へ

◆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

・全てドライバが操作

・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)



・『自動運転』と『つながるクルマ』の時代

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

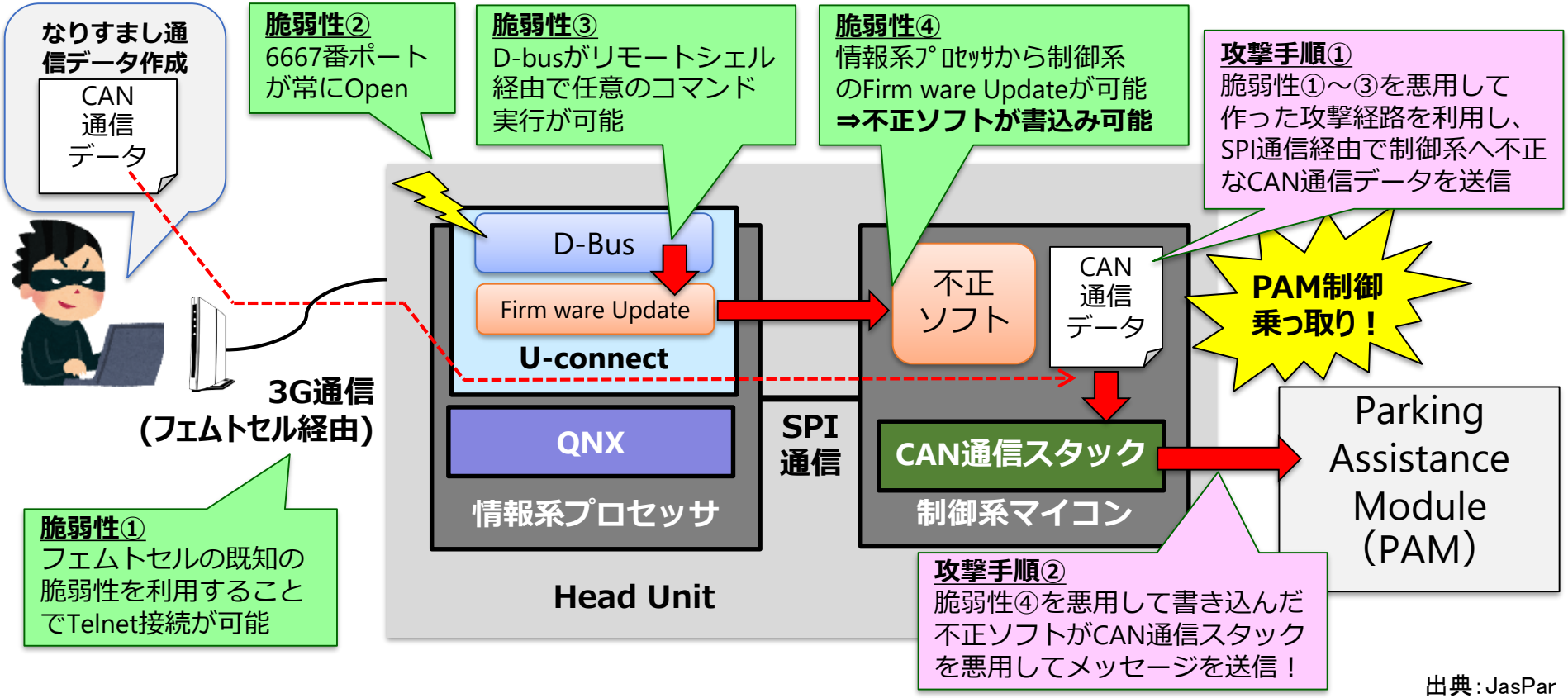
＜対象車両＞
Tesla model X
＜攻撃内容＞
model S同様
（新たな脆弱性を攻撃）

’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

Blackhat 注目技術

ハードウェアハッキング

- 廃車から取り出したテレマユニットを分解
- iphoneと同じチップを搭載しているため、
  既知脆弱性を利用してリモートアタックに成功

SIEM (Security Information Event Management)

- 脅威が発生したことを検知して見える化
- あらかじめ定めたルールにしたがって
  インシデントレスポンスの自動化も可能
- Businessブースで多数展示

Symantec.

Malwarebytes

RSA

LogRhythm
The Security Intelligence Company

CISCO

Fidelis
AUTOMATED DETECTION & RESPONSE

出典：JasPar

自動車に対するハッキング事例一覧（2017年抜粋）

◆ 自動車のコネクテッド化、CAN通信へアクセスするツールの普及により、ハッキングのハードルが低下⇒ 増加するハッキングに対抗するため、セキュリティ対応は必須！

時期	メーカ	概要	ソース
2017年2月	車両メーカ多数	各車両メーカの携帯向けアプリに対する脆弱性調査を実施。複数の車両メーカでドアロックの解除ができることを確認。	Kaspersky Lab
2017年4月	Bosch製ドングル	Bosch製 Driver log connector の脆弱性を利用して、CANバスへメッセージを送信し、エンジンの遠隔停止が可能。	ARGUS
2017年4月	Hyundai	アプリ“Blue Link Mobile”の脆弱性を利用し、車両位置特定、ドアロック解除、エンジン始動が可能。	Rapid7
2017年6月	SUBARU	アプリ“STARLINK”に脆弱性が発見され、車両の使用履歴へのアクセスや、ホーン、ドアロック解除などが可能。	Aaron Guzman（研究者）
2017年6月	ホンダ	ホンダ 狭山工場のPCがWannacryに感染し、生産ラインを一時停止。約1千万台の車両生産に影響を及ぼした。	日経新聞、他
2017年7月	Tesla	Tesla Moel Xへの遠隔ハッキングに成功し、CANバスへの攻撃により、ブレーキ、ドアロック、ミラーなどを制御。	Keen Security Lab（中国）
2017年8月	BMW、Ford、日産	2G回線を利用するTCUに脆弱性が発見され、ベースバンド無線プロセッサで任意のコードが実行される恐れがある。	マカフィ

出典：JasPar

自動車のセキュリティ動向　まとめ

◆クルマと外部をつなげる無線通信を経由した制御系への攻撃事例が多数報告されている

◆携帯通信網やBluetoothと比較して攻撃の歴史が長い、Wi-Fi経由の攻撃が懸念される

◆自動運転車両の時代には外部からのハッキングには注意とコストを払う必要がある

◆充分なセキュリティ評価とセキュアな設計プロセスが必要

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**

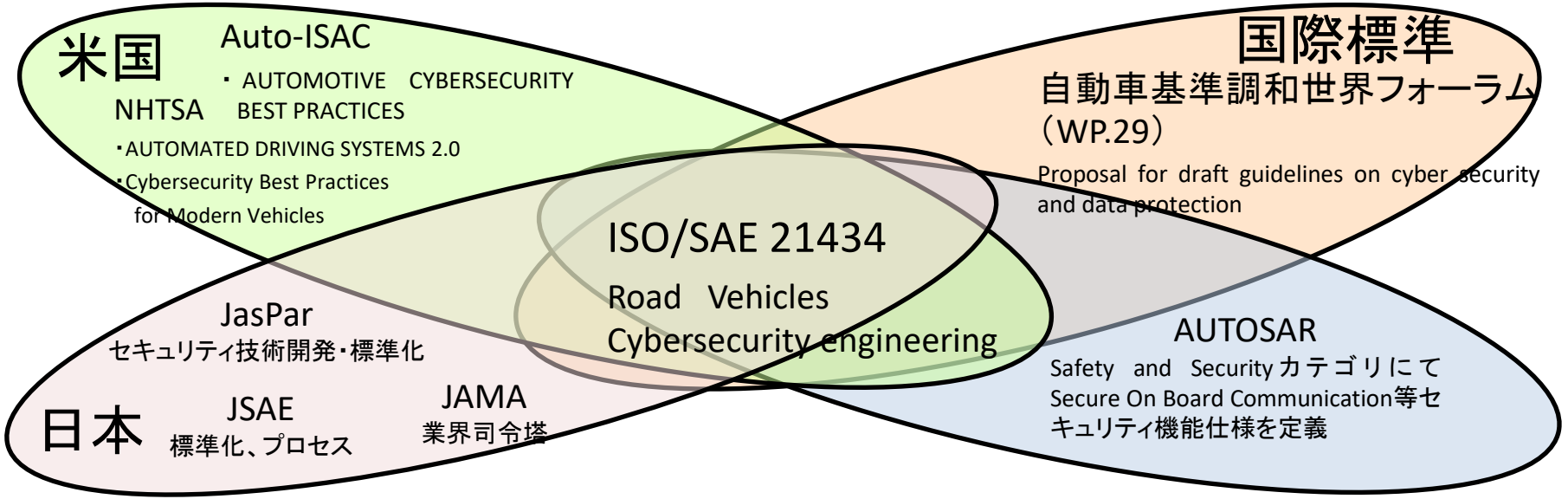
クルマの情報セキュリティ上の課題は、競争領域ではなく協調領域。
OEM間、業界団体間で積極的に連携を進める。

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



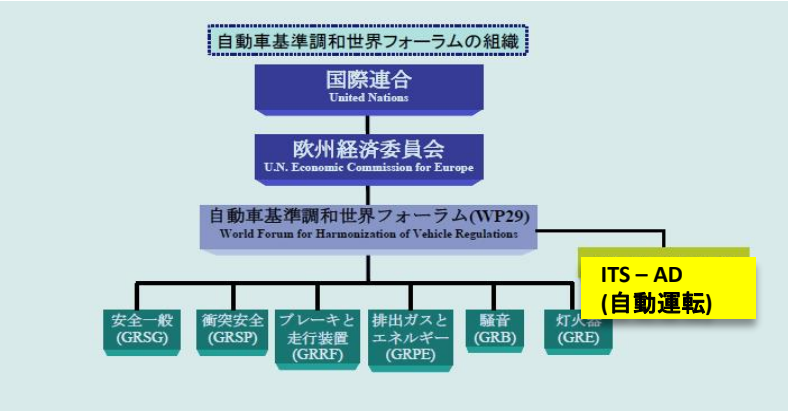
団体名	活動概要
NHTSA	自動運転車両（セキュリティへの要求含む）の規制やガイドを策定。
Auto-ISAC	自動車業界でインシデント／脆弱性情報を共有するための中心組織。
ISO/SAE 21434	ISO(欧)とSAE(米)のJoint workingで、自動車セキュリティ規格を策定。
WP.29	自動運転者・コネクテッドカー向けのセキュリティとデータ保護ガイド。
AUTOSAR	電子プラットフォーム仕様としてセキュリティ機能要求を策定。

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。



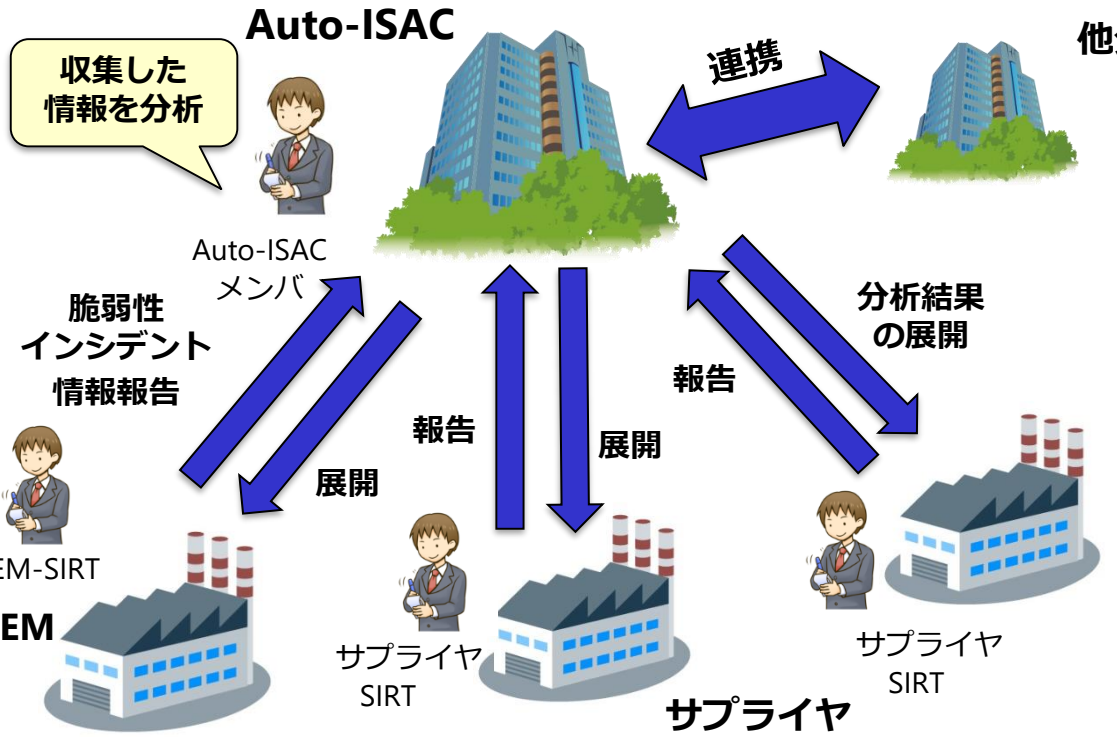
ISO/SAE 21434 ～ Road Vehicles - Cybersecurity engineering ～

- 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

Auto ISAC

◆ 米国ではハッキング事例報告の増加を受け，米国自動車工業会と国際自動車工業協会が連携して，Auto-ISAC（Automotive Information Sharing and Analysis Center）を創設



- Auto-ISACは，自動車の電子部品や車載ネットワーク，
その他様々なサイバー脅威の情報を業界内全体でリアルタイムに共有するための中心的組織.
- Auto-ISACに対する報告や情報展開を受け取る役割は各社のSIRT（Security Incident Response Team）が担う.

出典：JasPar

Auto ISAC

Auto ISAC (Information Share & Analysis Center)設立（'16/01）

AUTO-ISAC
Automotive Information Sharing and Analysis Center

✓ **政府主導により主要なインフラ系、産業系でISACを設立**

・クリントン大統領令PDD63＝主要インフラ18分野に情報共有体設立を指示(1998)
（銀行・金融、電力、上下水道、交通、通信、原子炉、軍事産業・・・）

・主要なOEM、サプライヤその他による大規模なAuto-ISACを設立(2016/01～　OEM,サプライヤ38社)

・米下院がNHTSAに対し、車両へセキュリティ対応を義務付ける法案策定に向け検討指示(2017)

Auto ISAC 設立（'17/01）

・経産省 サイバーセキュリティ経営ガイドライン ＝ 産業界へ10項目の対応強化を要請（2015）

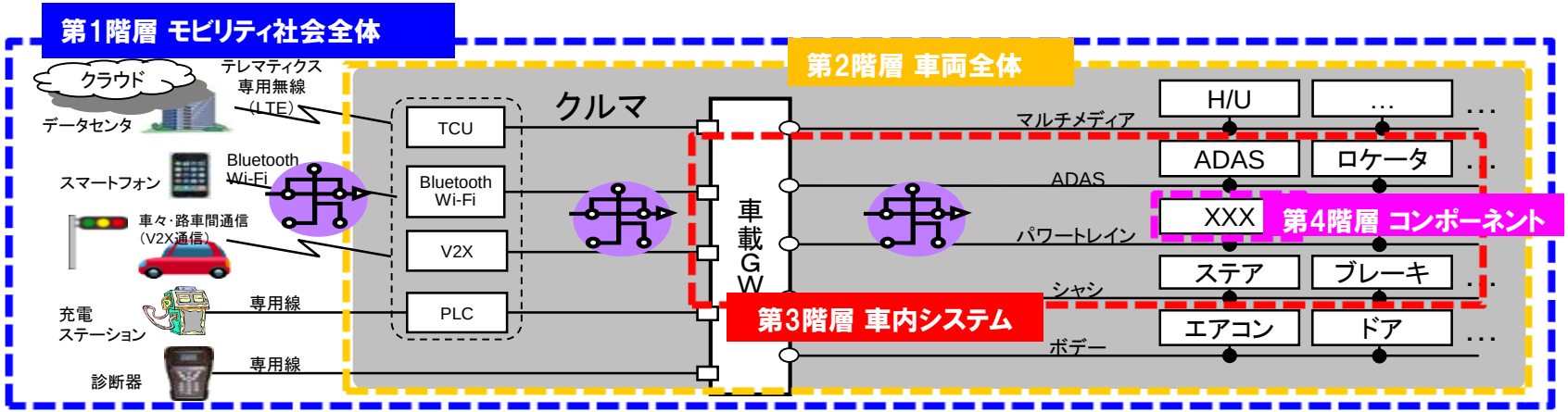
・当面 国内でのサイバー事案発生頻度は低いと予測し　まず　小さく、早く設立を目指した。

・上記経産省要請 第8項 **“情報共有活動への参加と有効活用”** に沿った形で
自工会 安全環境技術委員会の下にWGとして設立（国内OEM 11社）4月より本格活動開始

出典：JasPar

SIP-adus情報セキュリティ研究開発シナリオSWG活動

◆ 日本の自動車業界として、検討する標準的な車載システム構造を合意。
車両【第2階層以下】を対象として、業界標準、国際標準を視野に研究。



TCU: Telematics Communication Unit
PLC: Power Line Communication
GW: Gateway
H/U: Head Unit
ADAS: Advanced Driver Assistance Systems
ECU: Electronic Control Unit

データセンターのセキュリティに関しては、
『SIP重要インフラ等おけるサーバーセキュリティ』 にて検討

当SWG 4年間の計画

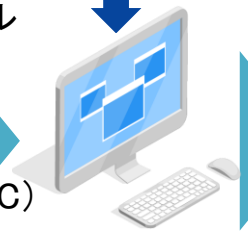
- 自動走行システムの共通モデルを構築し、脅威分析によりセキュリティ要件を策定するとともに、評価環境（テストベッド）構築、評価法標準化を目指す。
- V2X通信では、署名検証の簡略化について研究し、標準化を目指す。

		平成27年度	平成28年度	平成29年度	平成30年度
① 共通モデル検討・脅威分析		調査	開発・決定・導出	プロト開発	構築・評価・改善
②評価技術・評価環境	a) コンポーネント・車内システム	ｺﾝﾎﾟ評価対象の開発、基準調査	ｺﾝﾎﾟ評価環境とｼｽﾃﾑ評価対象の開発	ｺﾝﾎﾟ評価技術完、ｼｽﾃﾑ評価環境開発	ｼｽﾃﾑ評価技術完、ﾃｽﾄﾍﾞｯﾄﾞ試行
	b) 車外連携ｼｽﾃﾑ・車両レベル	ICT攻撃事例調査、AV対策箇所調査	対策技術の評価指針・指標の研究開発	評価指針・指標の検証	検証結果フィードバックとガイドライン化
	c) 通信プロトコルに基づく評価	調査（プロトコル仕様・攻撃方法）	評価方法・評価基準検討	シミュレータによる評価環境 開発・改善	
	d) 実機を用いた評価	コンポに対する攻撃方法の調査	車両に対する攻撃方法の調査		
			システムに対する攻撃方法の調査	モビリティ社会に対する攻撃方法の調査	
	e) 第三者認証の調査	他業界の認証の現状調査		第三者認証機関の検討	
			自動車応用検討		
③ V2X署名検証の簡略化		机上検討	通信評価	実装試験	総合検証試験
			標準化活動		
				V2X運用検討	
④ V2X海外調査・情報共有		海外動向調査			
		情報共有の仕組検討	情報共有の仕組運用		

SIP-adus情報セキュリティ研究開発シナリオSWG活動

利用し易さ（自工会）

◆共通アーキテクチャモデル
◆自動運転
ユースケース（自工会）
◆脅威情報
（JPCERT/CC、Auto-ISAC）
◆評価（攻撃）情報
（Auto-ISAC）

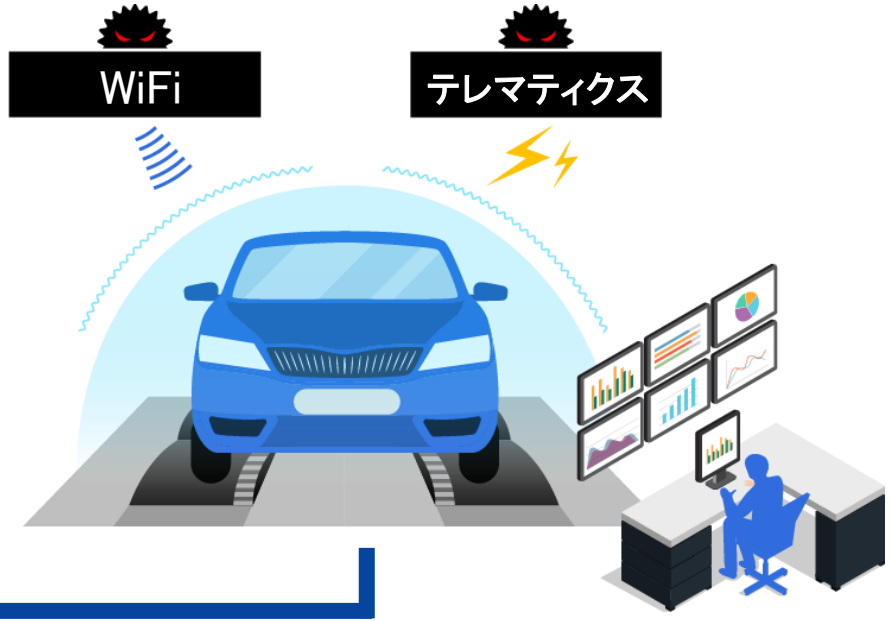


脅威分析ツール

◆対策
◆対策レベル

現状の脅威分析との比較
（JasPar）

脆弱性評価



情報セキュリティ評価ガイドライン

SIP-adus情報セキュリティ研究開発シナリオSWG活動

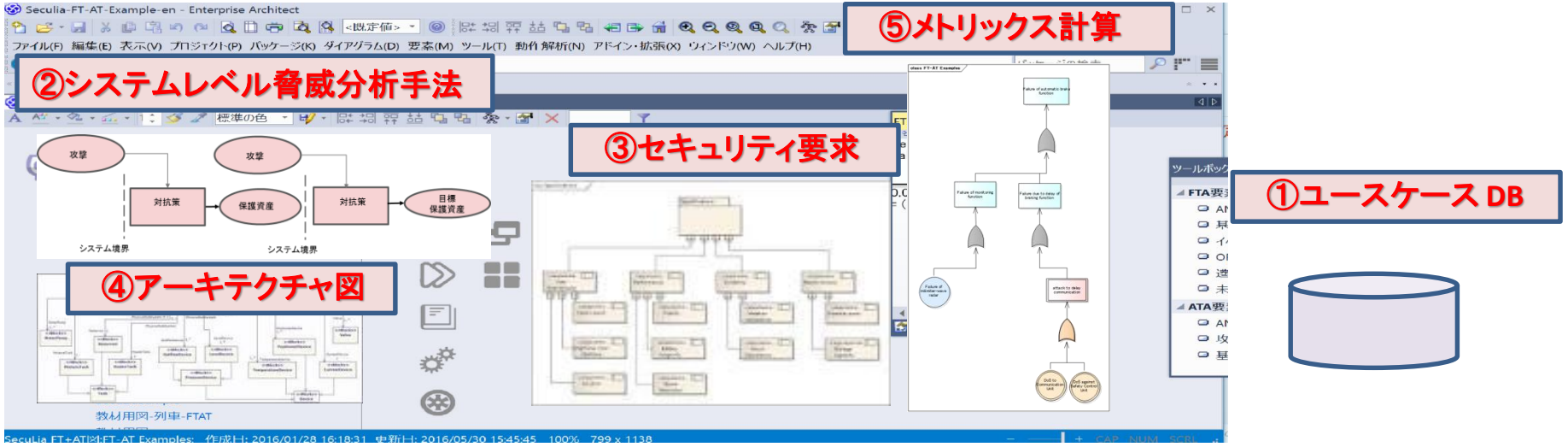
◆ Cyber攻撃に対する脅威分析手法検討

- ・多層防御、多段攻撃戦略の織込み
- ・脅威データベースの参照（Auto-ISAC、NVD等)
- ・JasPar分析仕様との連携

◆ 統合的分析ツール開発

- ・機能安全と統合した分析ツール化
- ・JAMA、JasParと連携した業界標準的ツールの開発

【ツール全体の概要（完成予想図）】



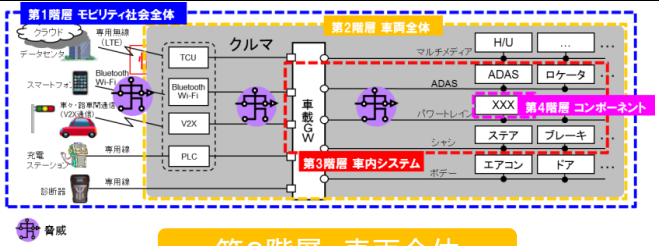
SIP-adus情報セキュリティ研究開発シナリオSWG活動

◆ 車両評価ガイドライン開発

SIP　　：**実装上不備視点**の評価ガイドライン
JasPar：**設計視点**のガイドライン

実機評価知見・経験の集約が必要

⇒　上記統合し、国際標準化を狙う。



第2階層　車両全体

a) 通信盗聴
b) ポートスキャン
c) ファジング
d) ペネトレーション
e) ジャミング

Ⅰ.脅威分析調査
Ⅱ.評価ガイドライン作成
Ⅲ.大規模実証実験

H29/1-4月	5-8月	9-12月	H30/1-4月	5-8月	9-12月	H31/1-3月
実験公募（3社選定）		Ⅰ.脅威分析調査　3社競争的に実施	ステージゲート審査（H30年度受託者決定）Ⅱ. ガイドライン作成			
				実験参加者募集	実験準備	Ⅱ. ガイドライン更新
					Ⅲ. 大規模実証実験	

情報セキュリティ評価法・ガイドラインの確立

◆ 車両評価ガイドライン開発(つづき)

【現状の成果】

- ◆ 評価ガイドライン策定のため、 **３社競争**による研究開発を導入
- ◆ ガイドライン及び実機評価能力を元に、有識者による技術委員会にて **ステージゲート審査**（３月）の上、評価ベンダー**１社を選定**

⇒ 受託会社毎に**アプローチが異なり、ガイドライン策定のポイント**が明確化

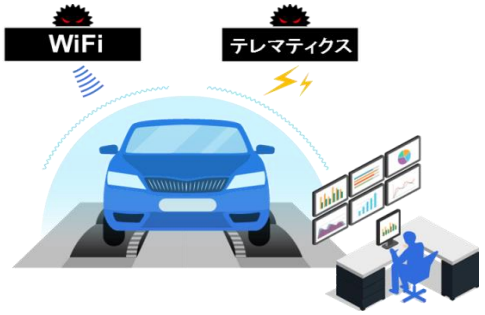
【日本シノプシス社】
国際標準化でも存在感を持つ世界的なセキュリティ診断ツール開発事業者

【PwCコンサルティング社】
ソフトウェアに加えてハードウェア側の脆弱性診断もできるハードウェアハッキングラボを保有

【デロイトトーマツリスクサービス社】
世界有数の総合コンサルティング企業であるデロイトグループのセキュリティ専門企業

【次年度】

- ◆ 選定した評価ベンダーによる**車両へのアタック評価**を実施し評価ガイドラインの妥当性、有効性の確認
- ◆ **情報セキュリティ評価体制の構築**と**国際標準化**(JasPar連携)



◆ 車内通信（CAN）に対する評価手法開発

①車内通信シミュレータを用いて、
- ・想定される攻撃手法
- ・その場合の通信挙動を確認

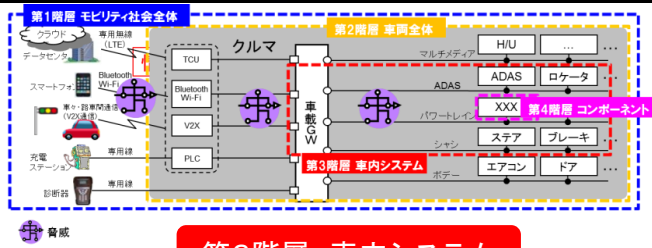
⇒実機に加えて仮想環境を構築し攻撃をシミュレーション

⇒評価データベースとして活用予定

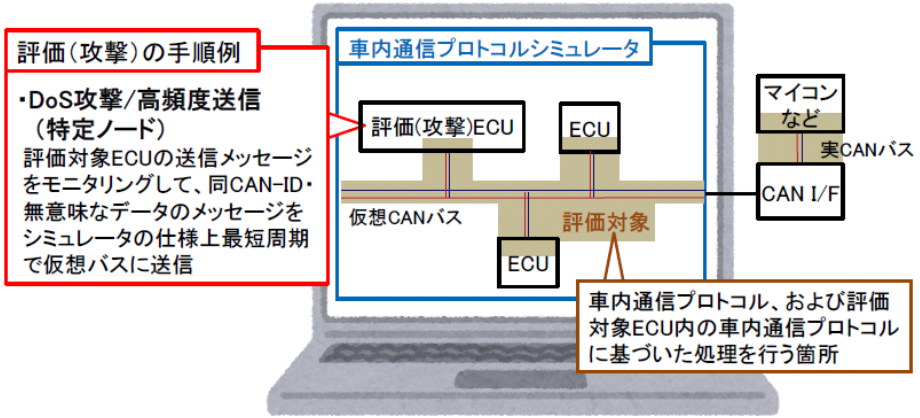
a) DoS攻撃
- 1)高頻度送信
- 2)メッセージ衝突
- 3)異常メッセージ送信

b) なりすまし攻撃
- 1)メッセージリプレイ
- 2)メッセージ改竄
- 3)送信頻度改竄

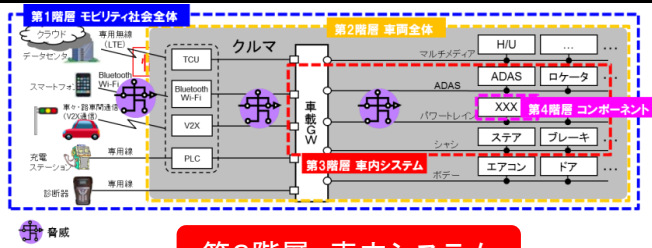
⇒シミュレータ・ベンチを用いた
人材育成への活用



第3階層　車内システム



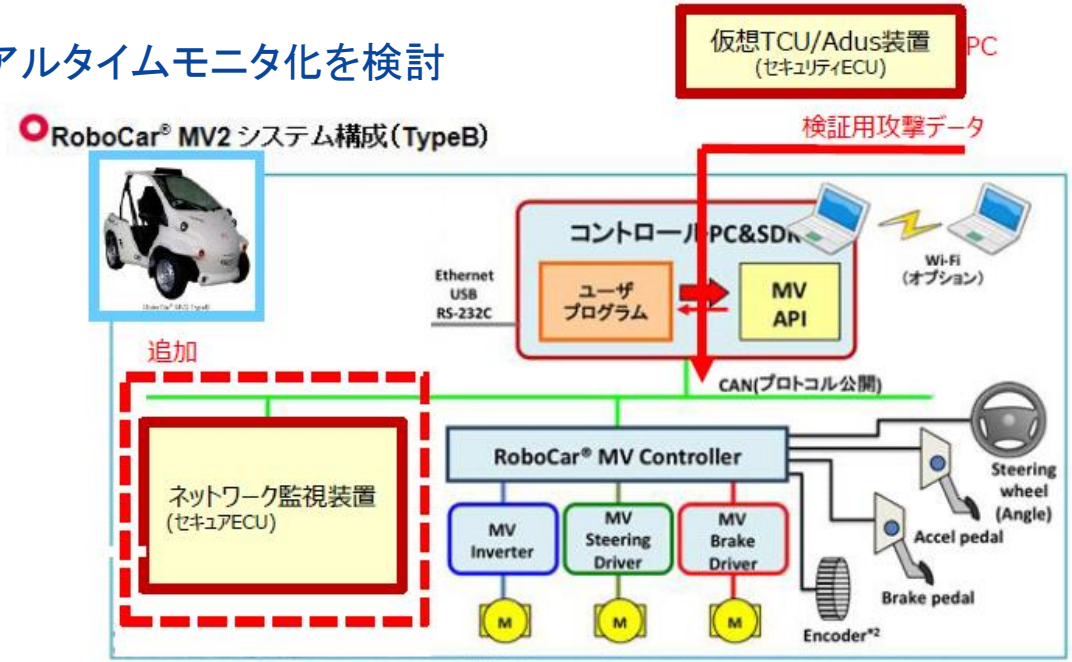
◆ 車内通信（CAN）に対する評価手法開発（つづき）



第3階層　車内システム

②侵入検知ガイドライン
- ・CANメッセージの周期乱れ
- ・CANメッセージの抜け etc.

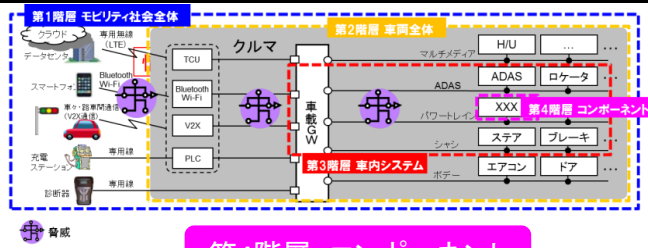
⇒侵入検知のリアルタイムモニタ化を検討



RoboCar® MV2システム構成例（TypeBプラットフォーム＋コントロールPC&SDK）

SIP-adus情報セキュリティ研究開発シナリオSWG活動

◆ 鍵配布、リプログラム認証評価手法開発



第4階層　コンポーネント

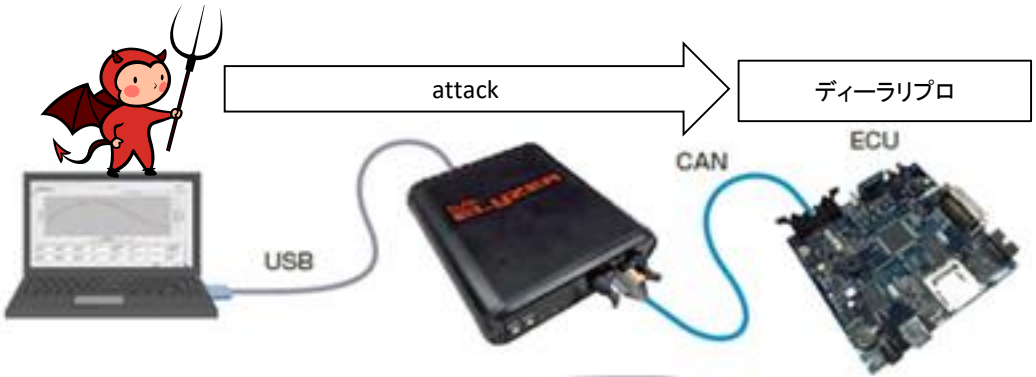
車載コンピュータ（ECU）のセキュリティリスクレベルに応じて、
リプログラム時に必要な標準的目標レベルを検討

- ・暗号アルゴリズム
- ・乱数Bit数、エントロピー

【評価方法】

①評価ボードによる実機攻撃評価
②他業界(※)の鍵管理調査　　(※)銀行ATM、カード決済端末、スマートメータ

⇒秘匿情報の抽出（暴露）にかかるコストの導出し、クライテリア化

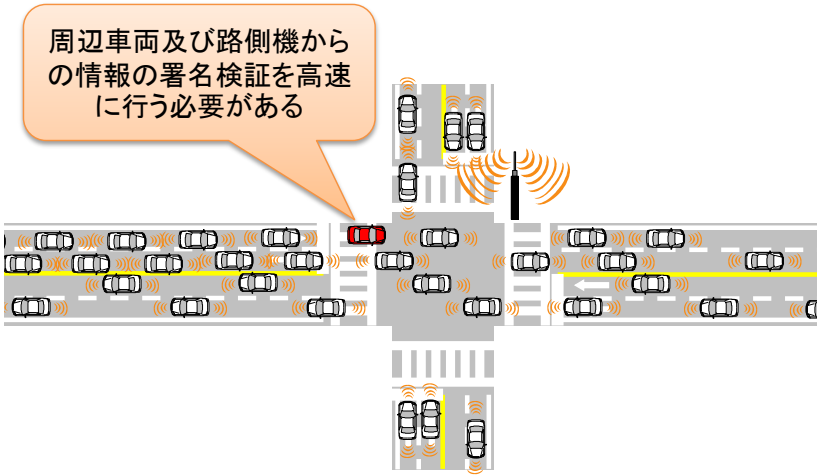


◆ V2X電子署名による通信遅延の改善

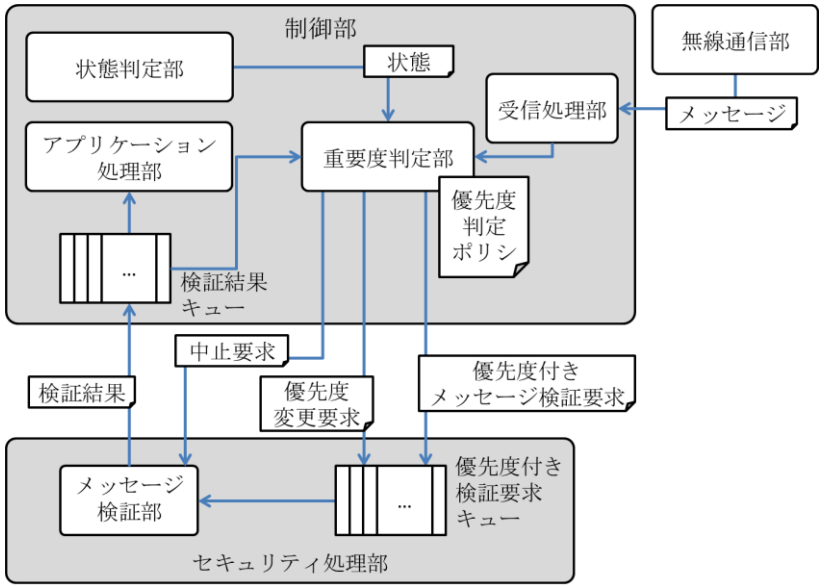
【背景】 V2X通信普及時のリアルタイム性確保
【研究】 V2X通信におけるメッセージ署名検証処理の簡略化
【目標】 1，000メッセージ/秒

⇒『優先度付きメッセージ検証方式』にて、性能目処付け完了。

- 実機での評価確認
- ISO TC204 WG16への標準化提案等を進める予定



優先度付きメッセージ検証方式



SIP-adus情報セキュリティ研究開発シナリオSWG活動

成果

1. OEM間、省庁間理解醸成
   - 競争領域・協調領域の理解醸成
   - 法制化に対する意見交換の促進
2. 業界としての技術底上げ/人材育成
3. 日本からの標準化提案への貢献

課題

1. 関係機関との連携強化
   ⇒ JAMA、JasParをメンバーに組入れ改善中
2. SIP事業成果の継続性
   - 脅威分析ツールの販売、使用性向上
   - 評価ガイドラインのアップデイト

   ⇒ 業界としての標準的評価機関・事業者の育成


Thank you