SIP-adus活動報告
～情報セキュリティ～

Cross-Ministerial Strategic Innovation Promotion Program
Innovation of Automated Driving for Universal Services

2017年2月14日

谷口　覚
SIP-adus情報セキュリティSWG主査/㈱トヨタIT開発センター

目次

Ⅰ. 車両へのCyber security攻撃事例

Fiat Chrysler recalls 1.4 million cars after Jeep hack

Ⅰ. 車両へのCyber security攻撃事例

The Washington Post

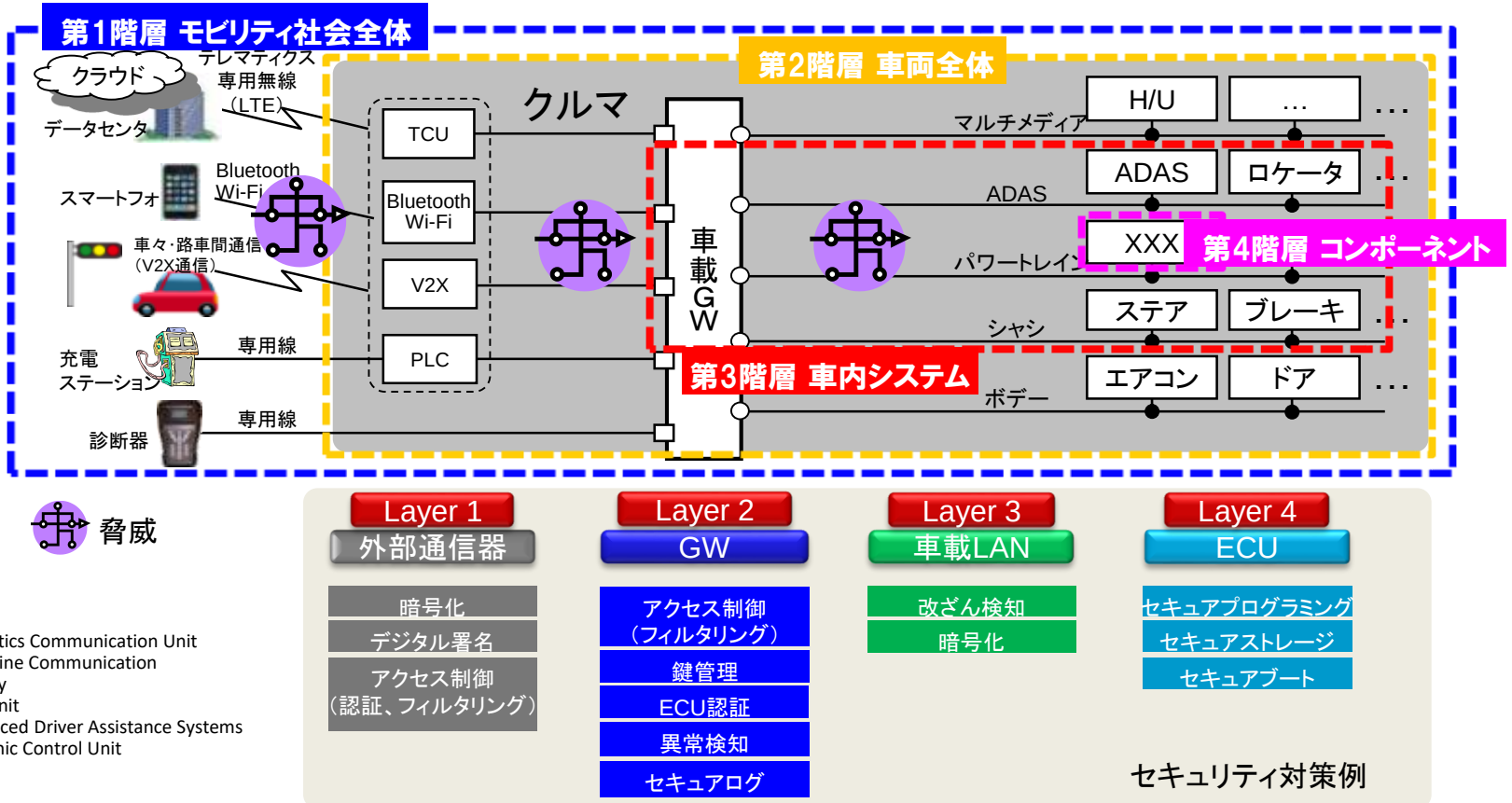
Researchers remotely hack Tesla Model S

The company said the vulnerabilities that Keen Security Lab uncovered would only be accessible under a very specific circumstance: when the vehicle's Web browser was in use and the car was connected to a malicious WiFi hotspot.

SIP

Ⅱ. 車両の構造及び、Cyber security対応例

第1階層のテレマティクス、WiFiを攻撃の入口として、
第2階層以下の車載システムをコントロールして動かす事例の報告が増加。

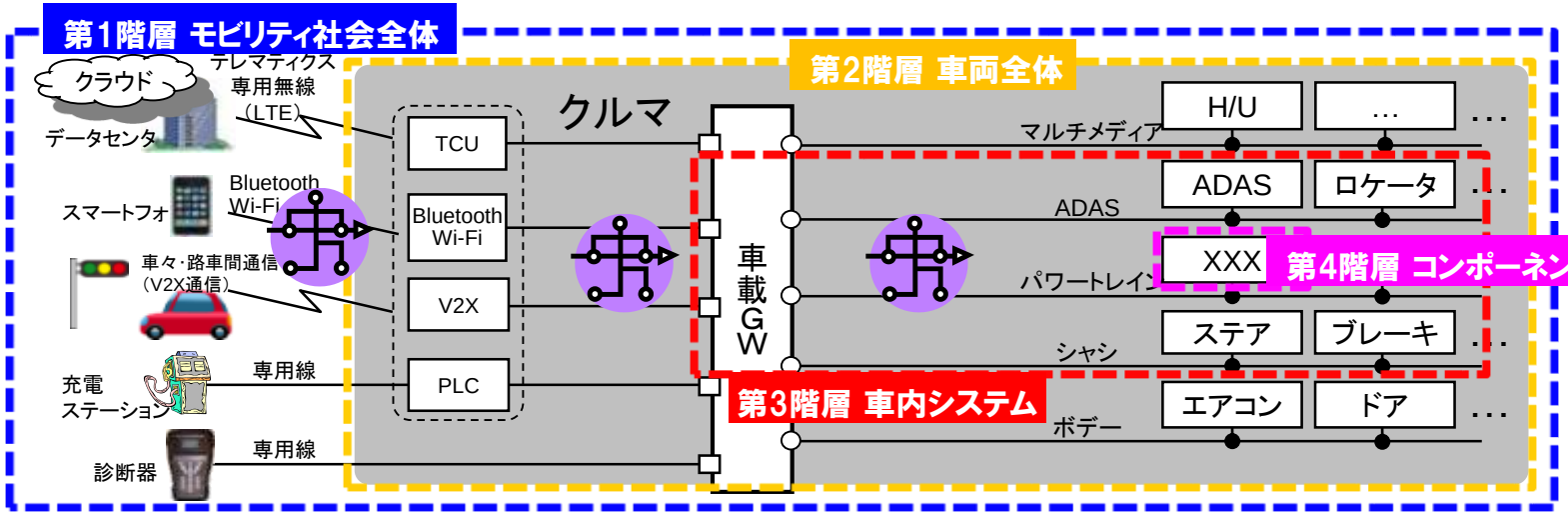


TCU: Telematics Communication Unit
PLC: Power Line Communication
GW: Gateway
H/U: Head Unit
ADAS: Advanced Driver Assistance Systems
ECU: Electronic Control Unit

各Layerでの対策、検知技術を組み合わせることで、システム耐性を確保するため、
構成は各社毎に異なる。

Ⅲ. SIP-adus情報セキュリティでのターゲット

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

Ⅲ-1. 脅威分析

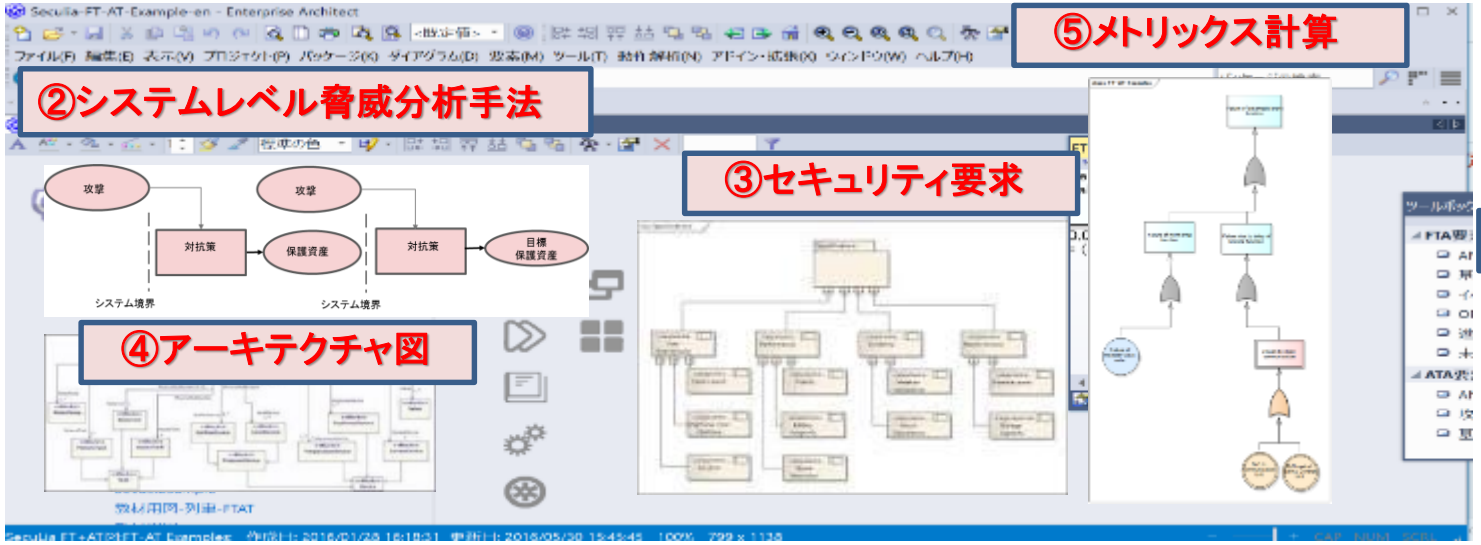
(1)Cyber攻撃に対する脅威分析手法検討【H28年度】

- 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

(2)統合的分析ツール開発【H29年度～】

- 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

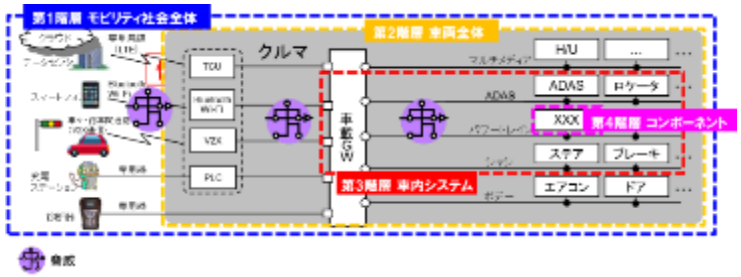
【ツール全体の概要（完成予想図）】



Ⅲ-2. 評価手法

第2階層　車両全体

(1)車両ブラックボックス評価手法開発
WiFi、テレマティクスを攻撃口として
耐性及び、機能安全を確認



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

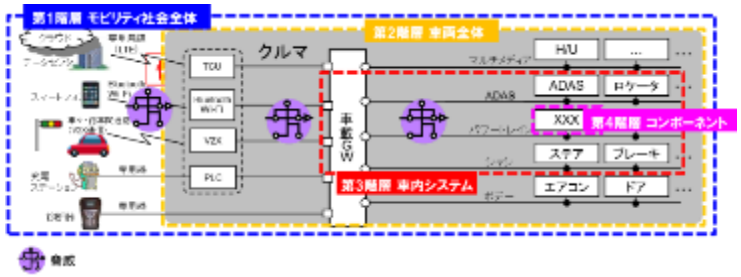
H29以降の大規模実証実験
業界の標準的評価法への反映
Auto-ISAC連携

Ⅲ-2. 評価手法

第3階層　車内システム

(2)車内通信（CAN bus)に対する評価手法開発

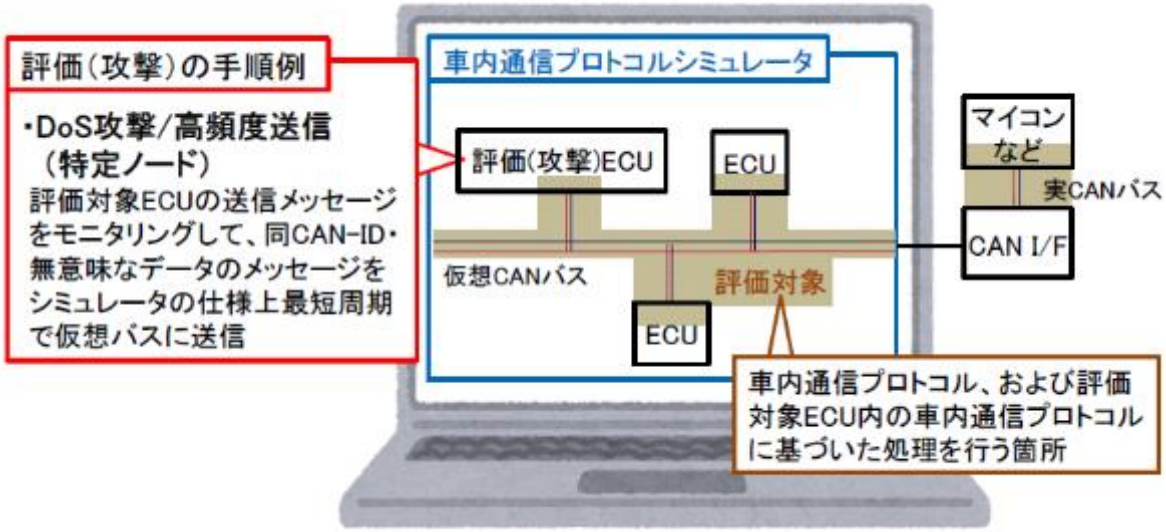
①車内通信シミュレータを用いて、
- ・想定される攻撃手法
- ・その場合の通信挙動を確認



《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

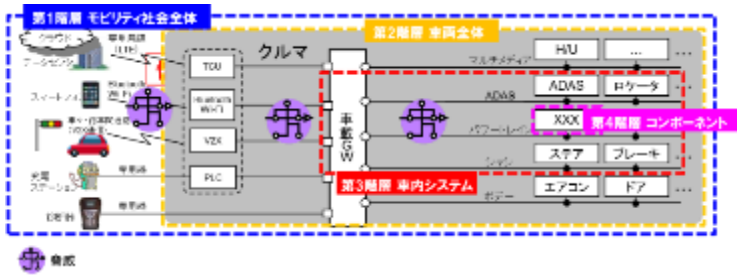
b) なりすまし攻撃
- 1)メッセージリプレイ
- 2)メッセージ改竄
- 3)送信頻度改竄



Ⅲ-2. 評価手法

第3階層　車内システム

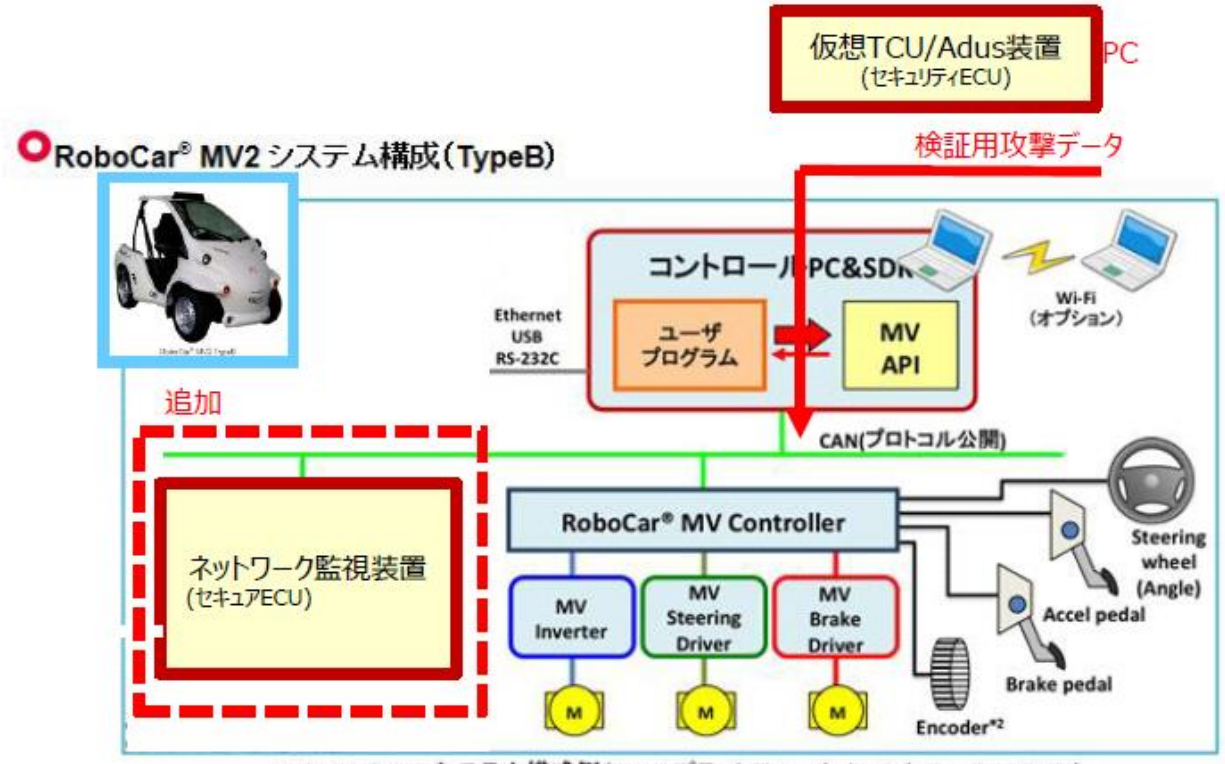
(2)車内通信（CAN bus)に対する評価手法開発



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.

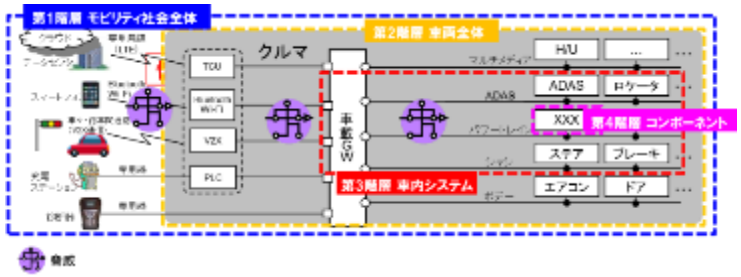


RoboCar® MV2システム構成例(TypeBプラットフォーム＋コントロールPC&SDK)

Ⅲ-2. 評価手法

第4階層　コンポーネント

(3)鍵配布、リプログラム認証評価手法開発

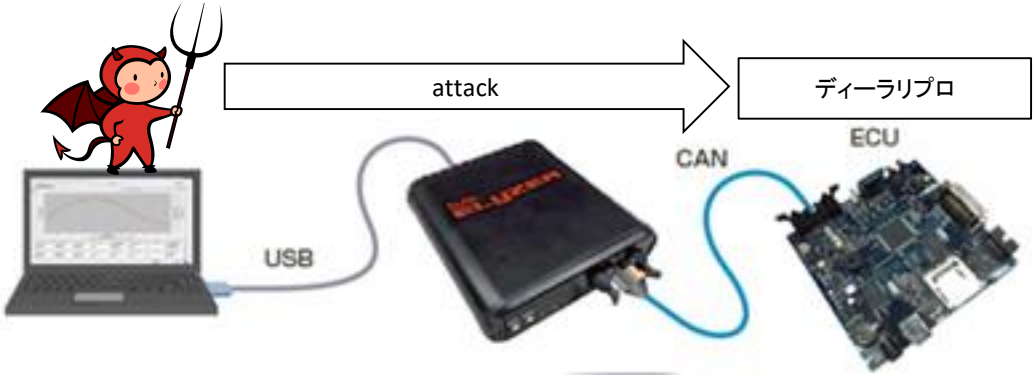


車載コンピュータ（ECU）のセキュリティリスクレベルに応じて、リプログラム時に必要な標準的目標レベルを検討

・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



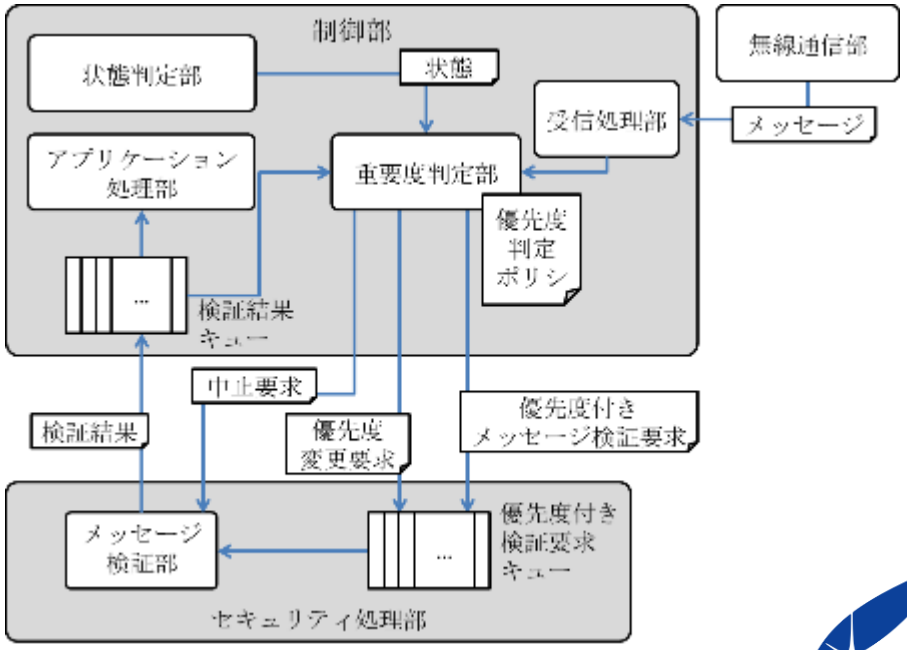
Ⅲ-3. V2X署名検証

【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



Ⅳ. 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
テーマA	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		
テーマB	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		

END

ご清聴ありがとうございました。