資料25-2-1-1-3

戦略的イノベーション創造プログラム
（自動走行システム）
「V2X等車外情報の活用にかかる
セキュリティ技術の研究・開発」プロジェクト

2016年9月28日

一般財団法人　日本自動車研究所

1.　前回WGでのご指摘事項・コメント等

報告	ご指摘事項
システム実用化WG （第45回　6/8）	• 脅威分析、セキュリティ要件の検討では、関係各機関、特に、JAMAとかJASPARとの連携が欠かせないが、どれくらい進んでいるか。②の評価手法・基準と、①の脅威分析とのリンクがどうなっているのか。 • シミュレータによる評価方法の有効性検証というところで攻撃が再現可能であるかを確認するとなっているが、「再現可能である」という確証はまだ持てないのか。うまくいかなかったらどうするのか。 • セキュリティはどこまでやっても終わりがないが、ゴールは、これを満足すれば合格という要件を決めるのか、対策の検討指針になるのか。 *→基本的には要件を決めていく、また、どう評価し、その基準がどうかを出すことがゴールと考えている。* • セキュリティの問題というのはグローバルに考える必要があるが、ここで作られていく要件やガイドラインが国際的に通用するものになるかどうかが非常に重要なので、その観点も是非お願いしたい。
開発検討会 （第1回　8/2）	• 事業実施に利用するツール等が業界関係者で利用できるようなものになるように、関係者、特に、JASPAR・JAMAの意見を反映していくことが重要である。また、JASPAR・JAMAで取組んでいることとの整合を図り、今後の事業計画に反映させることも検討する。

2. 本年度の計画

再掲

① 自動運転の共通モデルの解析用モデルデータに基づく脅威分析、セキュリティ要件及び対策の検討

- ✓ 調査結果を元に、脅威分析の試行フェーズへ移行

② 車両への攻撃に対する対策の評価手法・認証の調査・研究

- ✓ 車外連携および車内システムにおける評価環境の構築検討（項目追加）
- ✓ コンポーネントは、セキュリティのレベルを上げて攻撃（評価手法）を実施
- ✓ 車外連携システムは、対策技術の評価指針・指標について研究
- ✓ 車内通信プロトコル仕様に基づく攻撃に関するシミュレーション評価の有効性検証
- ✓ 第三者認証に関する調査・検討

③ V2X通信における署名検証の簡略化の研究

- ✓ 車車間、路車間の通信を模擬した署名検証簡略化の評価の実施

④ V2Xセキュリティに関する海外の仕様や技術動向に関する情報共有

- ✓ 海外動向の調査の継続・調査対象の拡大

3.　進捗状況（概要）

① 自動運転の共通モデルの解析用モデルデータに基づく脅威分析、セキュリティ要件及び対策の検討

- ✓ ツール化にあたり、将来活用を見据えた関係団体との調整を優先

② 車両への攻撃に対する対策の評価手法・認証の調査・研究

- ✓ 車外連携および車内システムにおける評価環境のシステム要件検討中
- ✓ コンポーネントは、セキュリティのレベルを上げたものを開発中
- ✓ 車外連携システムは、対策技術の評価指針・指標について研究
- ✓ 車内通信プロトコル仕様に基づく攻撃に関するシミュレーション評価に着手
- ✓ 第三者認証に関する調査・検討　調査内容等の検討中

③ V2X通信における署名検証の簡略化の研究

- ✓ 車車間、路車間の通信を模擬した署名検証簡略化の評価中

④ V2Xセキュリティに関する海外の仕様や技術動向に関する情報共有

- ✓ 海外動向の調査の対象を選定

3．1　進捗状況（概要）

■ 実質着手は6月からとなったが、1、2N、2e以外はほぼ計画通り

4．1　共通モデル検討・脅威分析（テーマ①）

1．自動走行システムの共通システムアーキテクチャ

調査により明らかになった複数のアーキテクチャについて、汎用的な記述言語（例：SysML (Systems Modeling Language)のブロック図、AADL（Architecture Analysis and Design Language）のセキュリティ拡張、等）を利用して統一的に記述する。

2．共通ユースケース

共通ユースケースの調査結果をデータベース化するための、データフォーマットの設計を行い、共通脅威分析プラットフォームにおいて利用可能な形にする。

3．脅威分析手法・試行

調査の結果を基に、新たな脅威分析手法を開発し、脅威分析の試行を行い、手法としての実効性の評価を行う。

4．共通脅威リスクアセスメント

セキュリティのアセスメント基準（セキュリティメトリックス）の基本原則を明らかにし、アセスメントの基準を策定し、（3）の脅威分析手法の試行に用いて、その評価を行う。

5．セキュリティ要求の導出

セキュリティ要求の導出を行うとともに、セキュリティ要求がどれだけセキュリティ上のリスクを低減しているかの評価を行う。

⇒　ツール化に関して、関係団体（JasPar、JAMA）との調整を優先（詳細は次頁）

4．1　共通モデル検討・脅威分析（テーマ①）

⇒ 情報セキュリティSWGから、他団体との連携や進め方についてのコメントを頂戴し、それに基づいて、JasPar 等の団体との連携を進めている。

⇒ JasPar が昨年度実施した、セキュリティ脅威分析結果利用して、方法論の評価を行うように計画を変更した。

– 現在、ツールの実際の開発前に、分析方法等の評価の実施を行うように計画を変更

関連団体	概要
情報セキュリティSWG	• 進め方、方法論についてのコメント
JasPar	• 脅威分析事例の開示について基本合意 • NDA等の手続きに着手 • 事例の解析 • 事例を基に、方法論の評価
日本自動車工業会	• 自動運転ユースケース情報の開示 • 共通ユースケースへの統合

注：進捗のある箇所を赤字で表記

【参考】 脅威分析・共通モデル分析ツール：目標

- 脅威分析・共通モデル分析ツールは、脅威分析を実施するための統合支援ツールの開発を目指している。
  - 様々な手法、方法論を統合可能なツール環境の提供
  - セキュア開発プロセスにおける開発工程の支援
    - 機能セキュリティコンセプト（Functional Security Concept）開発支援

- 今後、3～5年後において必要になる技術の提供。
  - 多層防御（Defense in depth）戦略
    - 多層防御戦略のモデル化、それに基づく脅威分析と対抗策の同定とリスクアセスメント
  - 外部環境を含んだ脅威分析
    - V2V、V2I において侵入経路として考えられる、他システム（路側機、他自動車、他）等を含んだアーキテクチャモデルに基づいた脅威分析
  - 外部脅威データベースのデータの参照
    - 既に存在する脅威DB（例：NVD、CWE）、Auto ISAC、等の脆弱性、脅威情報を参照できる外部 I/F の提供
  - セキュリティ上の複数のリスクアセスメント方式の支援
    - 複数のアセスメント方式（例：CVSS、CC-CEM）が混在する環境でのアセスメント方式の提供

- 関連団体との密接な連携。
  - セキュリティ分析やセキュリティのリスク評価、自動運転のユースケースを開発している各組織（情報セキュリティSWG, JasPar, 自工会）との連携を進めることで、自動車業界全体が利用しやすい共通プラットフォームの開発を目指す。

4. 2N 車外連携および車内システム評価環境 （テーマ②N）

本プロジェクトで策定する自律型自動走行システムの共通システムアーキテクチャを踏まえて、評価対象のシステム仕様として、本来機能とセキュリティ機能とを検討する。

実機評価には、安全性の確保や再現性の保証に課題があるため、HILS（Hardware-in-the-Loop Simulator）等を用いたシミュレータベースで行うことを検討し、車両挙動等を模擬してシミュレーションを行うことが可能な環境を用いることを検討する。

⇒ WG-Aにおいて、評価対象としてのシステム要件について議論中、まず本来機能、評価環境の位置付け定義を進めている。

4. 2a コンポーネントレベルの評価 （テーマ②a）

1. 評価対象

ECU評価では、さらにセキュリティレベルを上げて評価、定量化する。

⇒ 評価対象の仕様検討に着手、マイコンハードウェアIPを活用し、乱数生成のセキュリティ強度を上げたリプロ仕様を検討中。

ECU連携制御における車載LANに対する脅威への評価、および、車載LANのセキュリティ対策として、ECUのなりすましやメッセージの改ざんを防御する機能を検討する。

⇒ 車両内鍵管理について検討を進めることとした。

2. 評価方法・評価基準

コンポーネントの評価方法・評価基準ドラフトに対して、実機評価の結果を反映した更新を行う。車内システムの評価方法・評価基準は、コンポーネントと同様に、他業界の事例を調査し、ドラフト版を策定する。

⇒ 抽出した”対策方針”、”セキュリティ機能”に対する評価基準の具体化検討着手。

3. 評価環境

コンポーネントの評価環境として、前年度の調査結果である評価方法・評価基準（ドラフト）に対応した評価環境を開発する。

⇒ コンポーネント評価環境については、JasParや各OEMでも対応の動きがあり、本事業における取組み内容について見直しの予定。関係団体との議論を予定。

4．2b　車両レベル・車外連携システムの評価（テーマ②b）

■ 車両レベルの評価技術検討

1．対策すべきポイントとその評価指針の見直し

15年度のアウトプットを、共通モデルの最新状況に合わせて、見直しを実施

⇒　現時点では、共通モデルの修正はない

2．対策技術の評価指針・指標についての評価環境の構築

1.の検討内容を検証するための実験システムを構築し、指標の妥当性を検証する。具体的には，自動運転の簡易モデル車両を使用して、1.で設定したモデルの車内ネットワークを構築 し、必要と考えられる標準的なセキュリティ対策技術を搭載する。

並行してICT機器における侵入検知の評価基準について調査を行う。（追記）

⇒　簡易モデル車両の構造について調査を行い、改造ポイントと改造内容について検討を実施した。引き続き，具体的な改造部品の手配と加工を行い、メッセージ認証など標準的なセキュリティ対策技術の搭載を行う。

⇒　ICT機器における侵入検知の評価基準について調査中。

4．2b　車両レベル・車外連携システムの評価（テーマ②b）

■ 車両レベルの評価技術検討

3．実証結果の検証と指標ガイドラインの作成

2.の環境において1.の評価指標を検証（攻撃データの作成を含む）し、指標の妥当性や課題について検討を行う。その結果に基づき車両レベルでセキュリティを考える上で必要なセキュリティ**指標ガイドラインの作成**を行う。

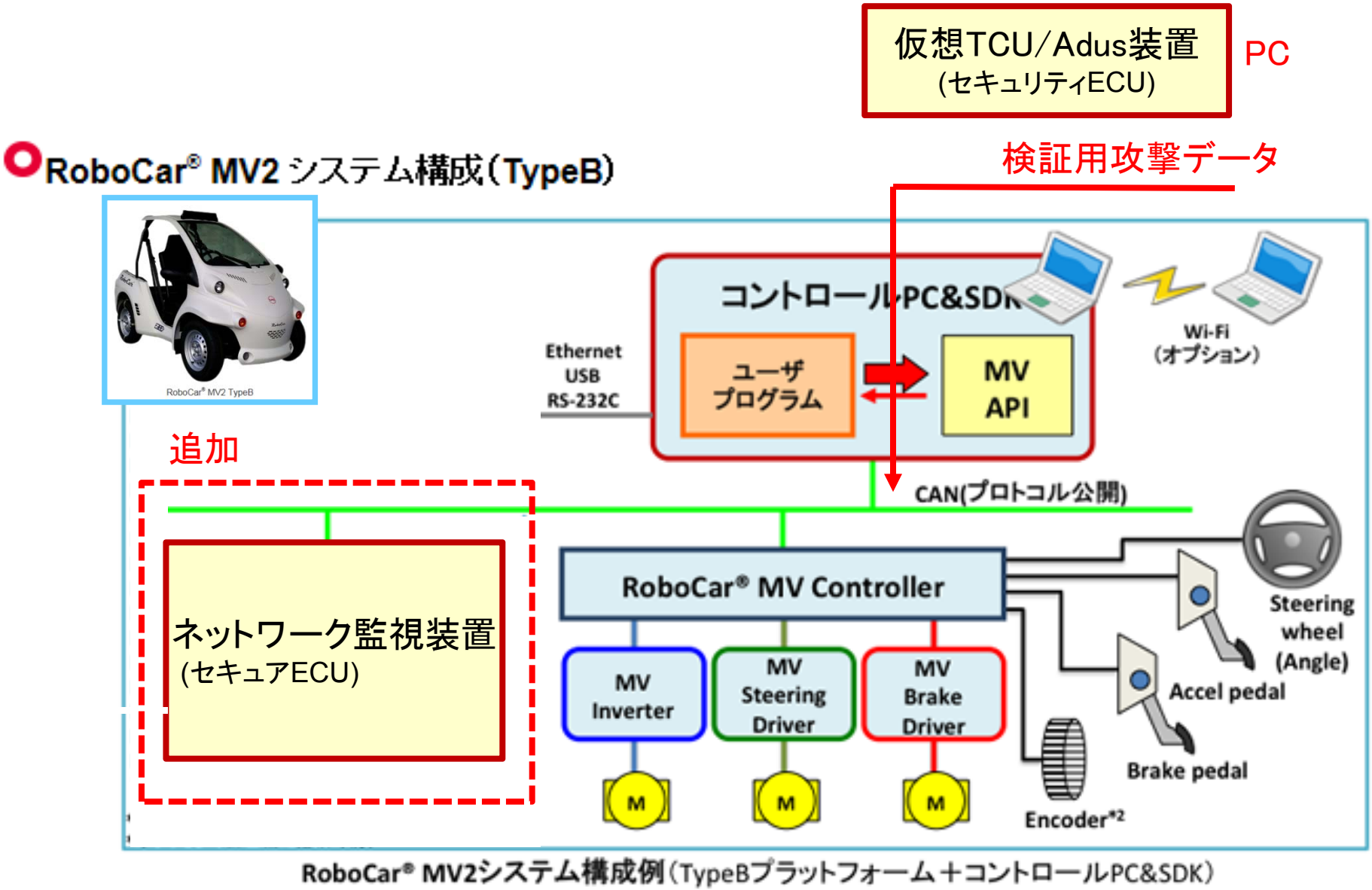
⇒　検証用の攻撃データ作成のため(2)のシステムの調査を開始した。

■ セキュリティインシデントの扱いの調査・検討

1. サイバー攻撃情報としてJPCERT/CCなどに提供される善意の情報をどのように扱うか，15年度の調査結果に基づいて、組織に跨がる情報共有の際に必要となる調査・検討を実施する。
2. また、本プロジェクト内での情報共有の枠組みを検討し、情報共有について試行する。

⇒　JPCERT/CCと、PJメンバー間での情報交換の場を設定することで合意、まずは、NDA不要の範囲での議論を実施する。（10月後半で調整中）

【参考】 評価環境イメージ



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)

4．2c　車内通信プロトコルの仕様に基づく評価（テーマ②c）

1.　評価方法の検討

– 調査で実施した内容を基に、攻撃方法を選定し、シミュレータ上で攻撃を行うための詳細な手順を検討する。
攻撃方法の選定においては、車内通信プロトコル（CAN、CAN-FD、LIN）とそれらに対しての攻撃手法の組み合わせの中から、攻撃の実現可能性が高そうなものを選定する。

⇒ 昨年度の調査で抽出した論文について、遠隔攻撃の実現性の観点で絞り込み（22件 → 18件）、更に攻撃の類似性の観点から整理・分類して攻撃シナリオ6種類にまとめた（DoS攻撃3種類、なりすまし攻撃3種類）。通信プロトコルは上記論文（18件）すべてが対象としていたCANを選定。

⇒ 上記のシナリオ6種類について攻撃手順の詳細化を実施中。現時点までにDoS攻撃全3種類が完了。

2.　シミュレータによる評価方法の有効性検証

– 市販の車内プロトコルシミュレータソフトウェア上に攻撃を模擬するテスト環境を実現する方法を検討し、攻撃が再現可能であるかを確認する。

⇒ 攻撃手順の詳細化が完了したシナリオから順に検証・評価に着手。現時点までにDoS攻撃全3種類のうち2種類まで完了。

4. 2d 実機を用いた評価 （テーマ②d）

1. 評価環境調査

BlackHat、SCISなどの周辺情報調査：主に参加者へのヒアリングを予定。
これらの周辺情報は、攻撃手法検討などにフィードバックする。

2. 標準ECUに対する攻撃

昨年度「汎用マイコン」を利用して行った攻撃評価から、「セキュアマイコン」を対象とし、攻撃対象の「ハードル」を上げる。

⇒ 「セキュアマイコン」を第71研究室及びデバイス販売店と議論・選定中。
「セキュアマイコン」利用に伴うNDA締結など事務手続きを並行して進めている。

3. システムに対する攻撃の検討

他研究室を含む関係各所から提供される「システム」を対象として、攻撃手法等について検討する。

⇒ 攻撃対象となりえる実機が具備する通信メディア及びサービスに関する調査を実施、継続中。調査結果は、既存の攻撃方法へとマッピング中。

4．2e　第三者認証に関する調査（テーマ②e）

平成27年度に実施した調査の結果を踏まえ、自動車セキュリティへの第三者認証の妥当性の検討を行う。

妥当性検討を行うための第三者認証研究会を立上げ、この研究会における議論を元に、調査・検討の範囲を明確にし、必要な調査を実施する。

⇒　調査・検討の範囲の素案を作成、メンバー候補との調整中

4．3　V2X通信における署名検証の簡略化（テーマ③）

1．　評価項目、評価条件の検討

・平成27年度「V2X等車外情報の活用にかかるセキュリティ技術の研究・開発」の成果を基に簡略化方式の効果に関する通信評価を行うための評価項目を検討する。

⇒　評価項目を選定中

評価シナリオにおける処理性能（メッセージ/秒）、

メッセージ毎の処理時間（全体や署名検証の割合）、…

・簡略化方式を評価するための評価条件を検討する。

⇒　公開されているユースケースを基に評価シナリオ検討中

（障害物による車線変更）

2．　通信評価機能の開発及び構築

・各項目による評価を行うための通信評価機能の要件を整理する。

⇒　評価で想定するHWの性能を決定

（CPU動作周波数1GHz、暗号HW有）

・要件に従い通信評価機能を開発する。

・評価条件に従って通信評価機能の入力となる評価用データを生成する評価用プログラムを開発する。

4．3　V2X通信における署名検証の簡略化（テーマ③）

3.　評価用データの生成
- 評価条件に従い、評価用プログラムを用いて評価用データを生成する。

4.　簡略化方式の通信評価
- 評価用データを用いて、仮想環境上での通信評価機能により、簡略化方式の通信評価を行う。

5.　評価結果の整理及び分析
- 評価結果を基に、簡略化方式の効果について考察する。

4．4　V2Xセキュリティの海外動向調査（テーマ④）

1．平成27年度の活動を継続

調査対象範囲の拡大を検討する。

⇒　WG-Bにおいて、今年度調査対象の抽出、調査分担を検討

- ITS世界会議（JARI）
- C2C-CC Forum（外注での対応を検討）
- Escar Europe（CAV）
- IEEE VNC（75研で調整中）
- (TRB, SAE GOvernment/Industry Meetingの情報を別途入手）
- ISO TC204/WG16 Technical Meeting（75研で調整中）

2．情報共有の仕組み（公開情報の有効活用）

情報発信の仕組みを検討する。

WG-B：事業実施者に限定せず海外仕様のV2Xに関連する事業者により構成
（平成26年度調査事業のメンバーが主体）

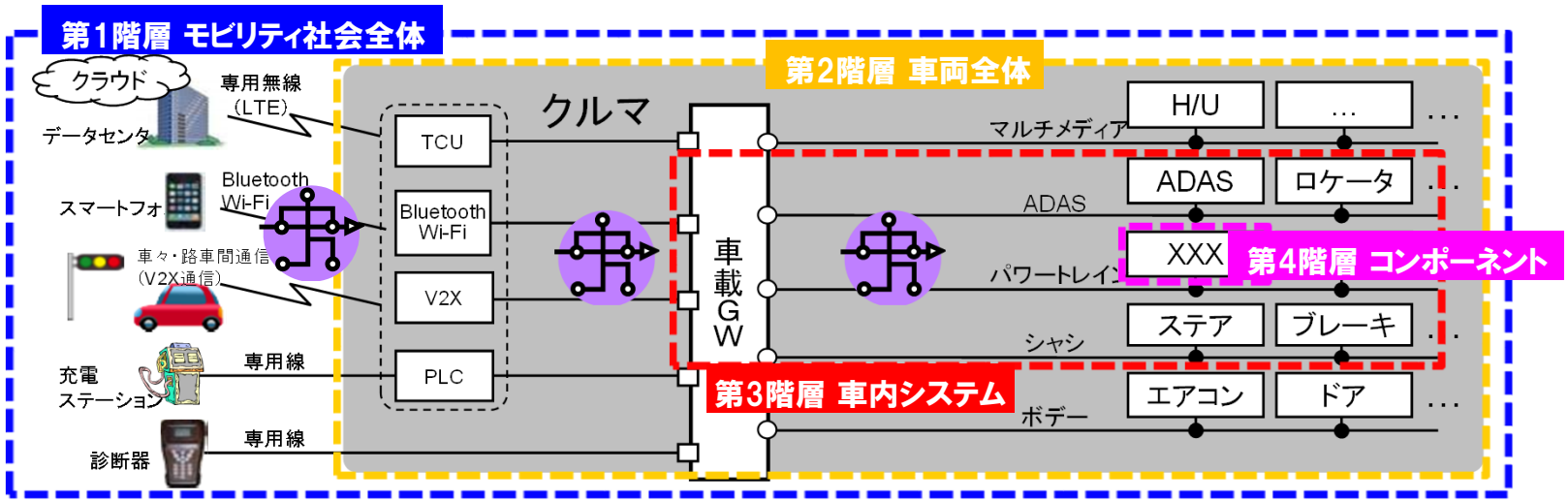
5．1　研究開発実施体制（開発検討会）

座長	国立大学法人　横浜国立大学　大学院 環境情報研究院　教授	松本　勉
委員	独立行政法人　情報処理推進機構セキュリティセンター 情報セキュリティ技術ラボラトリー　次長	桑名　利幸
	国立研究開発法人　情報通信研究機構 ネットワークセキュリティ研究所 セキュリティ基盤研究室　室長	盛合　志帆
	独立行政法人　自動車技術総合機構 交通安全環境研究所　主席研究員	新国　哲也
	一般社団法人　日本自動車工業会 情報セキュリティWG　副主査	川久保　淳史
	一般社団法人　JASPAR 情報セキュリティ技術WG　主査	橋本　寛
	情報セキュリティ研究開発シナリオ検討SWG	谷口　覚
オブザーバ	一般社団法人　JPCERT コーディネーションセンター 経済産業省　製造産業局　自動車課 経済産業省　商務情報政策局　サイバーセキュリティ課 総務省　総合通信基盤局 電波部 移動通信課（第2回より）	
事務局	一般財団法人　日本自動車研究所	

【参考】 事業を進める上での基本的考え方

再掲

- 自動車セキュリティを検討するための対象を、4つの階層に分けて考える
- 自動車に加えられる攻撃はどういったものか、どう対策するのか、その対策をどう評価するのかを研究（第1階層から来る脅威もあるが、第2階層以下での対策に関するもの＝自動車側で出来ること、を対象とする）



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

Layer 1	Layer 2	Layer 3	Layer 4
外部通信器	GW	車載LAN	ECU
暗号化	アクセス制御（フィルタリング）	改ざん検知	セキュアプログラミング
デジタル署名	鍵管理	暗号化	セキュアストレージ
アクセス制御（認証、フィルタリング）	ECU認証		セキュアブート
	異常検知		
	セキュアログ		

セキュリティ対策例

【参考】 事業の目標(４年間)

再掲

■ 本事業では、４つのテーマがあり、それぞれの目標は；

① 自動運転の共通モデルの構築と、それに基づく脅威分析、セキュリティ要件及び対策の検討

✓ セキュリティに対するガイドライン策定のために、共通で使うことが出来るモデルの構築と、セキュリティ要件の策定 （共通認識の醸成）

② 車両への攻撃に対する対策の評価手法・認証の調査・研究

✓ 業界が共通して利用できる評価環境 （テストベッド） の構築の基礎となる評価技術の開発、第三者認証の必要性等の検証

③ V2X通信における署名検証の簡略化の研究

✓ セキュリティを担保しつつ、処理能力を高めることが出来るモデルを立案（H/Wへの性能要求を緩和、コストアップを避ける）

④ V2Xセキュリティに関する海外の仕様や技術動向に関する情報共有

✓ 海外動向の調査を行い、その結果を共有する場を構築

【参考】 事業の実施概要（4年間）

再掲

- 4年間で、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、共通モデルを参考にしつつ評価環境（テストベッド）を構築する。
- V2X通信では、署名検証の簡略化について研究し、標準化を検討する。

			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		

2016年9月28日

一般財団法人　日本自動車研究所