平成 26 年度
戦略的イノベーション創造プログラム
V2X（Vehicle to X）システムに係るセキュリティ技術の
海外動向等の調査

平成 27 年 3 月

（委託先）

一般財団法人 日本自動車研究所

目 次

調査事業の内容および成果等（要約）.....1

はじめに.....3

第 1 章　欧米等、海外における V2X システムに係るセキュリティ技術動向等の調査.5

1.1 セキュリティの技術動向調査.....5
1.1.1 米国における V2X セキュリティ関連調査.....6
(1) UMTRI による Safety Pilot.....6
(2) V2X セキュリティについて.....7
(3) 米国プロジェクトの進捗.....10
(4) 将来の展望.....11
1.1.2 欧州における V2X セキュリティ関連調査.....13
(1) PRESERVE.....13
(2) PRESERVE の進捗.....14
(3) TAL.....15
(4) TAL の進捗.....17
(5) 欧州プロジェクトの進捗.....17
1.1.3 米国と欧州の方式の比較.....18
1.1.4 まとめ.....19

1.2 セキュリティ方式調査.....20
1.2.1 C2C-CC Organization.....20
1.2.2 Protection Profile Finalization Task Force.....21
(1) 受信側の自動車におけるセキュリティ要件.....21
(2) HSM のセキュリティレベル.....21
1.2.3 Security Requirements and Qualification Task Force.....21
1.2.4 C2C-CC 参加者状況.....22
1.2.5 まとめ.....23

1.3 米国 V2X 開発状況調査.....23
1.3.1 北米 PlugFest 参加.....23
(1) 日程.....23
(2) 評価ユニット.....24
1.3.2 試験環境および試験内容.....25
1.3.3 セキュリティ仕様について.....27
1.3.4 米国 TestBed 参加者状況.....27
1.3.5 まとめ.....29

1.4 調査結果の分析、まとめ.....30
1.4.1 欧米のプロジェクトの進捗状況.....30
1.4.2 現状の課題としてのプライバシ保護とインフラ構築.....30
1.4.3 V2X システムの車両への搭載は欧米とも 2017 年頃.....31
1.4.4 性能とコストの考え方.....31
1.4.5 次世代高度運転支援でのリスクを想定した脅威分析に必要な要件の検討.....32

第 2 章　海外展開可能な V2X システムに係るセキュリティ技術のあり方の検討.....33

2.1 欧州のセキュリティ仕様の前提条件調査.....33
2.1.1 前提条件の分類.....33
2.1.2 調査対象と調査結果.....34
2.1.3 想定するアーキテクチャの提案（調査項目(1)）.....35
2.1.4 基礎となるユースケースの作成について（調査項目(2)）.....36
2.1.5 リスク見積もり方法の比較（調査項目(3)）.....37
(1) EVITA.....37
(2) ETSI.....39
(3) ITS-Forum.....41
(4) リスク見積もり方法の考察.....42
2.1.6 まとめと今後の課題について.....43

2.2 セキュリティ技術のあり方の検討.....44
2.2.1 現状で性能未達になっているハードウェアの技術開発.....44
2.2.2 欧米で継続議論中のインフラ等の技術課題に関する研究.....44
2.2.3 情報提供レベルから、自動運転に応用する際に追加で検討すべき事項.....45
2.2.4 標準化に対する取組み.....45
2.2.5 V2X システムの製品化における認証のあり方.....46

2.3 まとめと今後の課題.....47

おわりに.....48

参考資料.....49
1）先行プロジェクトの調査結果.....50
1-1 保護すべき情報資産.....50
1-2 リスク見積もり方法.....50
2）ユースケース一覧.....52
3）ユースケースの比較表.....54
4）ユースケースの統合結果.....56
5）ユースケース詳細.....58
6）自動化レベルとユースケースの紐付けについて.....76

調査事業の内容および成果等（要約）

現在、各国で開発が進められている自動運転では、通信による外部情報との連携が重要であり、中でも V2X システムが注目されている。V2X システムを用いて安全に通信を行うためには、特に、セキュリティ技術が重要である。この分野において、我が国のサプライヤの技術を海外にも展開出来る様にするためには、海外の技術動向および実施上の課題を把握した上で、セキュリティ技術のあり方を検討することが必要である。

本事業では、欧米において進められているセキュリティ関連のプロジェクトの現状や進捗状況、今後の計画等を把握することを目的に、主要なプロジェクトの関係者へのヒアリング等により調査を実施した。次にこれを受けて今後取り組むべき内容を提案した。

欧米のプロジェクト調査結果により、インフラ側でのセキュリティ技術に関連する運用の部分で未定となっているものがあるが、V2X システムの機器開発に関わるところは、ほぼ計画通りに進捗していることが分かった。注目していた欧州 PRESERVE プロジェクトの遅れは、技術的な面ではなく、半導体デバイス製造上のスケジュール調整であった。また、欧米ともに、活動の活発化がみられ、これまで行ってきた実証実験の参加台数を増やしたり、路側機の設置範囲を広げるなど、規模を拡大することが計画されている。

一方、欧米の V2X システムのセキュリティ技術に関するインフラ側やセキュリティ運用上の課題とされているのは次の 3 つである。

①端末側の署名検証処理能力不足の対策としての署名検証の簡略化。
②プライバシ保護に関連して、V2X のメッセージに付加する証明書の運用の詳細が未定。
③誤った情報を発信する端末や、なりすまし端末を認識する Misbehavior Authority における Misbehavior の検出方法。

さらに、実用化する時点で必要となる、通信機器としてセキュリティ処理を含む相互接続性を保証するための、認証の仕組みが未だ確立されていないことも課題であると考える。

現在の V2X システムは、ドライバへの情報提供を前提にして構築されている。今後、検討が進むと思われる自動運転や車両制御へ応用する場合には、要求されるセキュリティレベルは現在の想定より高いものになると考えられる。この点に関して、欧米の主要なプロジェクトで、V2X システムを自動運転に応用する場合を想定した取組みが行われているかは、プロジェクトの関係者へのヒアリングでも明確な答えは得られなかった。

これらの調査結果を踏まえ、セキュリティ技術の有識者、海外向け V2X システムを開発する事業者の代表による V2X セキュリティ検討 WG を設置し、議論した結果、V2X システムに係るセキュリティ技術のあり方として、以下の様な取組みを行うことを提案する。

まず、現状で課題になっている V2X システムのセキュリティ技術に関するインフラ側の運用に関する研究を進める。次に、自動運転への応用を行うために必要となるセキュリティレベルを見極めるために、脅威分析を実施する。その際、制御応用となるため、機能安

全とも組合せて分析を行う。また、日本と海外で異なる仕様を適用している技術について、海外との協調の視点で、どの様に標準化に取り組んでいくのかを検討するとともに、海外の技術動向に関する情報を共有する仕組みを構築する。認証については、適正なレベルの認証について検討するとともに、国内でも認証を行える様にしていく。これらの取組みが、我が国のサプライヤの技術を海外にも展開出来る様にするために重要であると考える。

はじめに

自動車の普及に伴う交通事故や交通渋滞は、世界中で甚大な社会的損失をもたらしており、今後の世界的な人口増大に伴う自動車保有の増加や高齢化、都市の過密化の進展により、こうした問題も深刻さを増すものと考えられる。これら課題の先進国である我が国において、自動車乗車中の交通死亡事故件数は、ここ数年減少幅が逓減し、引き続き厳しい状況が続いており、高齢者の自動車乗車中の交通死亡事故件数については、近年増加に転じている。また、交通渋滞による燃料消費量や NOx 排出量の増大も問題であり、省エネルギー・環境対策の観点から、渋滞対策も喫緊の課題である。

これら課題の抜本的な解決に貢献するものとして、緊急対応にとどまらない、定常的な自動運転を可能とするシステムの実現が期待されており、その実現に向け、自動車の走行機能の 3 要素（検知・判断・操作）の高度化が求められている。このうち、検知技術については、車載センサーを通じて走行環境を認識するもののほか、通信を用いて外部（周辺車両、インフラ、クラウド等）から情報を入手する V2X システムがあり、車載センサーでは検知出来ない範囲の走行環境の認識を補完する技術として期待されている。

V2X システムの実現に向けては、それを安全に行うためのセキュリティ技術が欠かせない。V2X システムに対する脅威としては、緊急車両等へのなりすまし、偽情報（渋滞情報、信号情報、車両停止情報、等）の受信、自車の位置情報などを改ざんするケースと、車両システム内に入り込んで、車両の制御を乗っ取るものや、車両の持つ情報、例えば、走行距離データを改ざんするなどのケースが想定される。

現在実用化が進められているシステムは、V2X システムで得られる情報をドライバに伝達する用途を想定しており、もし誤った情報が伝えられたとしても、ドライバが判断する余地があるため、現状でのセキュリティに対する要求はそれ程厳しいものではないが、自動運転への適用を進めるためには、情報を受け取った自動車が誤った動きをしない様、通信で得られる情報には、より高いレベルの完全性と信頼性が求められる。

こうした中、日本、および欧米では、それぞれ、V2X システムに係るセキュリティ技術の開発や実証が進められている。また、米国では、周辺車両からの情報をドライバーへの情報提供・注意喚起に活用する車車間通信用車載器について、数年内の搭載義務化を検討する旨の発表がなされている。

ただし、日本と欧米の V2X システムではその仕様が異なっている。通信周波数については日本は 760MHz 帯、欧米は 5.9GHz 帯、セキュリティ仕様では日本は秘密鍵方式、欧米は公開鍵方式となっている。そのため、国内仕様の V2X システムをそのままでは欧米向けに展開することは出来ない。また、セキュリティ仕様の策定に関しては、日米欧がそれぞれ独自に進めてきていたが、2012 年以降、欧米の間では仕様のすり合わせを行う EU/US Harmonization が始まっている。

欧米では情報提供を対象としたセキュリティ仕様の一部は既に標準化され、WEB 等で公開されている。また、自動運転応用に対応したセキュリティ仕様については、議論が進められているものと想定されるが、未だ公開情報はない。標準規格は、一旦定まってしまうと、規格を満たすために他社の技術を使用せざるを得ないケースも想定され、その場合にはライセンスの問題が発生することが懸念される。また、実際の V2X システムの出荷が始まると、相互接続性などの認証取得が必要となることも想定される。欧米向けの V2X システムに対して、国内で認証取得が出来ない場合には、海外の認証機関に頼らざるを得ず、国内で行う場合に比べて認定取得までに時間が掛かる可能性もある。

我が国のサプライヤ等が開発する V2X システムに係るセキュリティ技術を、海外にも展開可能なものとするためには、欧米をはじめとする海外動向を詳細に調査し、それを踏まえ、海外に展開が可能な V2X システムに係るセキュリティ技術のあり方を検討することが必要である。特に、V2X システムを、情報提供の次の段階としての制御応用に移行することで、セキュリティ仕様が見直される可能性のある現時点において、欧米の現状を正しく理解することが必要である。

本事業の目的は、欧米における V2X システムのセキュリティ技術に関わるプロジェクトがどこまで進んでいるのか、どういったところに課題があるのかについて調査を行うものである。調査の方法としては、欧米の主たるプロジェクトの関係者にヒアリングするとともに、V2X システムの実証実験に参加する等により行う。合わせて、それぞれのプロジェクトにおける標準化に対する取組みについてもヒアリングした。これらの調査結果から、セキュリティ技術としてどういった部分に注力していくべきか、標準化も視野に入れて、セキュリティ技術のあり方の検討を行うものである。

第 1 章　欧米等、海外における V2X システムに係るセキュリティ技術動向等の調査

V2X システムについては、ドライバへの情報提供を前提に、日米欧のそれぞれで実証実験や実用化に向けた取組みが行われている。日本では、ITS 情報通信システム推進会議(ITS-Forum)から運転支援通信システムに関するセキュリティガイドラインとして RC-009 が、運用管理ガイドラインとして RC-008 が発行され、ITS-Connect 推進協議会を中心に実用化に向けた取組みが進められている。米国では USDOT (U.S. Department of Transportation：米国運輸省)が主導して Safety Pilot と呼ばれる実証実験が行われており、PlugFest と呼ばれる相互接続性の実験も行なわれている。欧州では、車載機器全般のセキュリティについて、EVITA (E-safety Vehicle Intrusion proTected Applications)で検討が行われ、続く PRESERVE (Preparing Secure Vehicle-to-X Communication Systems)においては、V2X システムに適用する VSS (V2X Security Subsystem)を開発し、実証するとともに、欧州で行われる FOT (Field Operational Test)に提供することが目的の一つとして挙げられている。また、V2X システムの実証実験は、C2C-CC (CAR 2 CAR Communication Consortium)等で実施されている。

欧米における V2X システムの車両への搭載は、2017 年頃から始まると見られており、2014 年 9 月にデトロイトで開催された ITS 世界会議では、GM から 2016 年に発売するキャデラック 2017 年型車への搭載が発表されている。

特に米国では、オバマ大統領が車両事故と交通渋滞を減らすためのハイテク・ソリューション、および雇用創出の機会として、V2V (Vehicle to Vehicle)、V2I (Vehicle to Infrastructure)の導入に積極的な姿勢を示している。また、TRB (Transportation Research Board)において、ITS-JPO (ITS Joint Program Office)から「USDOT の投資の最優先事項は NHTSA (National Highway Traffic Safety Administration：米運輸省高速道路交通安全局)の V2V の規則作りに必要な標準をサポートすること」との説明もあり、米国政府は V2X システムの実用化を強力に進めようとしていることが分かる。

1.1　セキュリティの技術動向調査

本調査は米国・欧州における V2X セキュリティプロジェクトにおいて、その進捗度合いの確認、スケジュールの遅延がある場合にはその理由の確認が主な目的である。

現在米国 5 都市で行われている Safety Pilot では、それぞれが独自の技術に基づいて車車間通信サービスを検証している。この中でミシガン州とカリフォルニア州は USDOT の関係者が見学に訪れるなど注目されているが、本調査では 5 都市の中でも注目を集めているミシガン州の Safety Pilot を中心に調査を行う。

また、欧州では Framework Programme と呼ばれる枠組みで実施されるプロジェクトとして、FP7 (第 7 期) の中で EVITA や OVERSEE (Open Vehicular Secure Platform)など車載システムセキュリティに関連するプロジェクトが実施された。今回は EVITA 等のプロジェクト

の後継として現在進行中であり、V2X システムに係るセキュリティ技術に関する開発・検証を実施するプロジェクトである PRESERVE を中心に調査を行う。

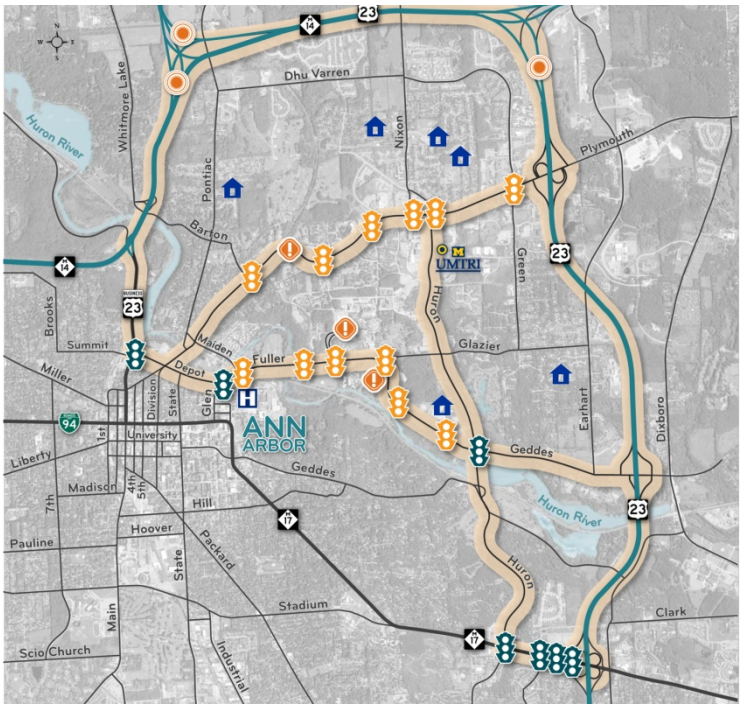
1.1.1　米国における V2X セキュリティ関連調査

ミシガン州の Safety Pilot は、技術基盤の面のみならず、天候変化の大きさなどの環境面からも実証実験に適していること、実施されている実証実験の規模が一番大きいことから、5 都市の中で最も注目されている。今回の調査では、プロジェクトを統括する UMTRI (University of Michigan Transportation Research Institute：ミシガン大学の交通研究所) を訪問してヒアリングを実施した。

(1) UMTRI による Safety Pilot

第 1 期 Safety Pilot は、2012 年 8 月 21 日から 2014 年 2 月 17 日にかけて図 1.1-1 に示す Ann Arbor エリア（ミシガン州）で実施された。合計で 2836 台の車載器を利用した実証実験であり、車載器は一般車のみならず、公共のバスやトラック、バイク、自転車などにも搭載された。図 1.1-1 上の交差点には図 1.1-2 の様な RSU (Road Side Unit：路側機)が導入され、路側機と車載器の間は DSRC (Dedicated Short Range Communication：狭域無線)、インフラ側との間は IPv6 により接続されている。

このインフラを利用した想定サービスは図 1.1-3 の様になっており、ドライバへの情報提供・警告を行うものである。

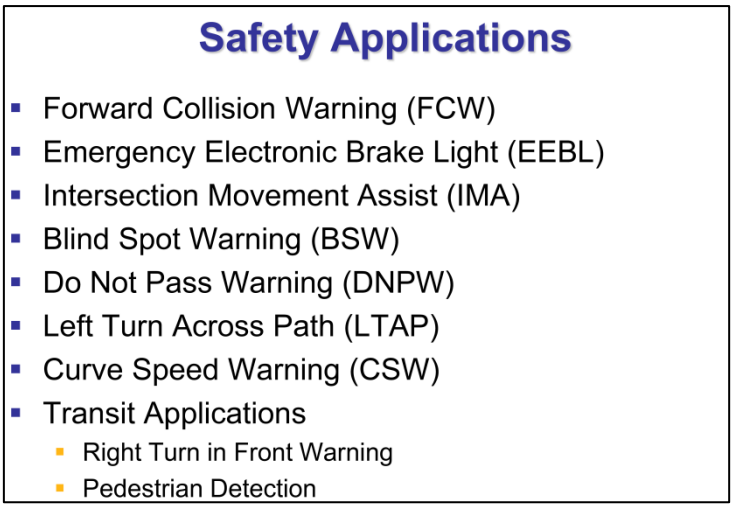


（出典：André Weimerskirch, "V2V Communication Security: A Privacy Preserving Design for 300 Million Vehicles", CHES 2014, September 25th, 2014、以下 CHES 2014 と略す）

図 1.1-1　Ann Arbor における Safety Pilot 実施エリア

（出典：CHES 2014）

図 1.1-2　信号に取り付けられた RSU



（出典：UMTRI よりヒアリング時に入手）

図 1.1-3　想定サービス一覧

(2) V2X セキュリティについて

Safety Pilot などで利用する V2X セキュリティ技術に関しては、米国 CAMP (Crush Avoidance Metrics Partnership) が、UMTRI を中心に VSC (Vehicle Safety Communications) プロジェクトの中で検討している。

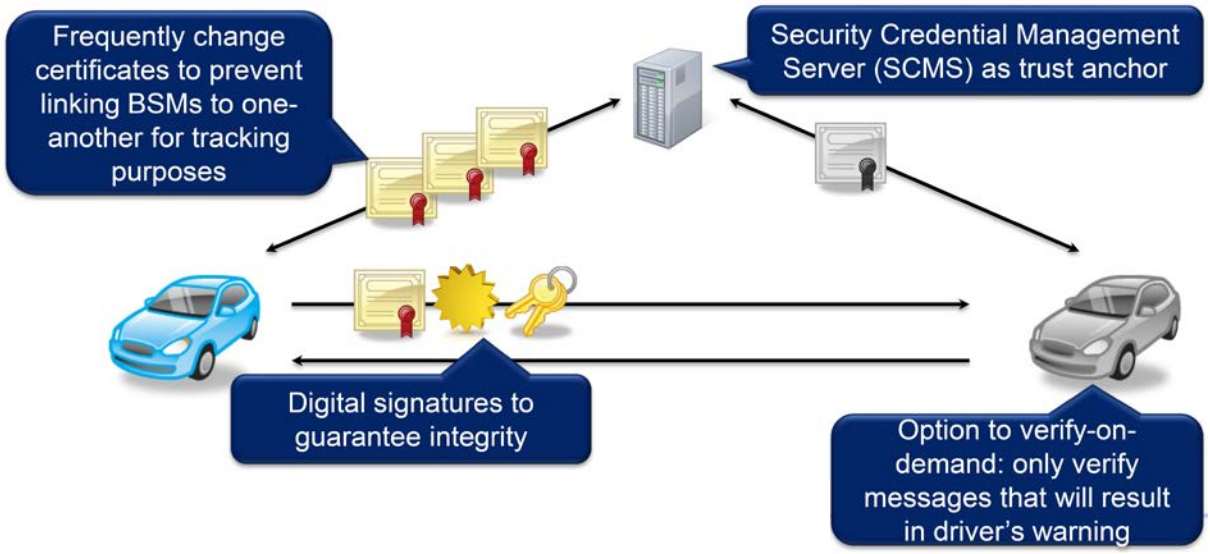
図 1.1-4 に CAMP における V2X セキュリティメッセージ送信の概要を示す。メッセージは PKI (Public Key Infrastructure：公開鍵)ベースであり、電子署名付与によるメッセージの完全性と電子証明書付与による送信者の妥当性を担保している。受信者は電子証明書に含まれる公開鍵を利用してメッセージの完全性を確認する。送信者は同報通信により、毎秒 10 メッセージを送信する。V2X の中でも車車間通信には即時応答性が求められるため、CAMP では以下の様な工夫を行っている。

・受信者でメッセージのペイロードを確認し、処理すべきか否かを判断する。処理すべきメッセージについてはメッセージの完全性を確認、それ以外のメッセージは破棄する。

また電子証明書についても、その更新に関して以下の様な工夫を行っている。

・電子証明書の有効期限を短くして、証明書をトレースすることによるロケーションプライバシの侵害が起きない様にしている。

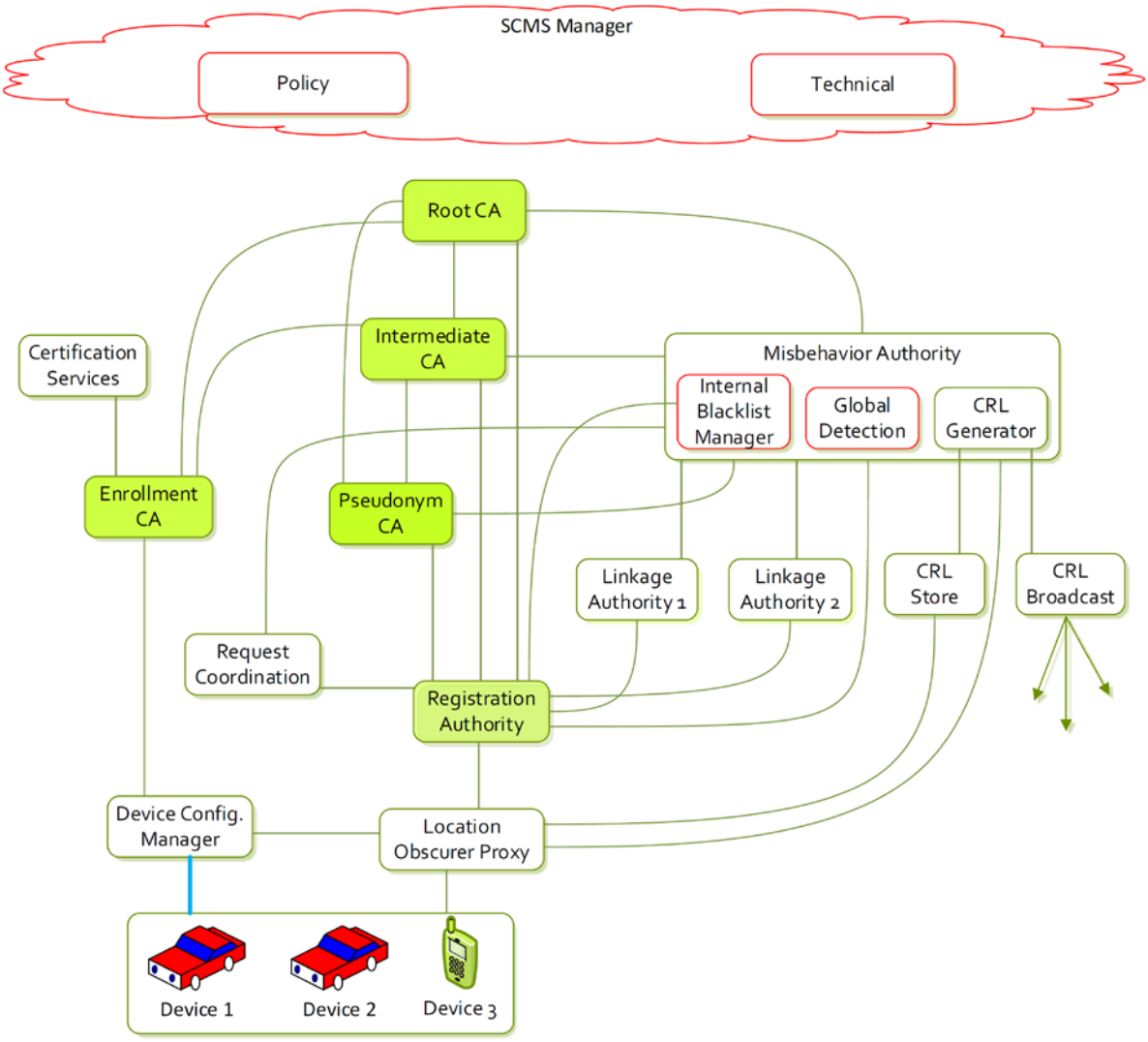
・署名に利用する秘密鍵は定期的な更新が必要であり、電子証明書を作成する認証局にて保管する公開鍵も、秘密鍵とペアで更新する必要がある。一方で認証局と送信者は安定した通信路を確保出来ない可能があるため、送信者と認証局が独立して公開鍵ペアを更新出来る Butterfly Algorithm を提案している。



（出典： CHES 2014）

図 1.1-4　米国におけるセキュアな V2X メッセージ送信概要

SCMS (Security Credential Management System) と呼ばれるインフラ側のアーキテクチャを図 1.1-5 に示す。認証局として Root CA (Certificate Authority)および有効期間が短い電子証明書を作成する Pseudonym CA を中心に、実運用時に必要な要素が複雑に連携している。機能を細かく分割し、結果として複雑な連携をする理由は、インフラ内外からのトレーサビリティを難しくし、プライバシ保証を担保するためである。

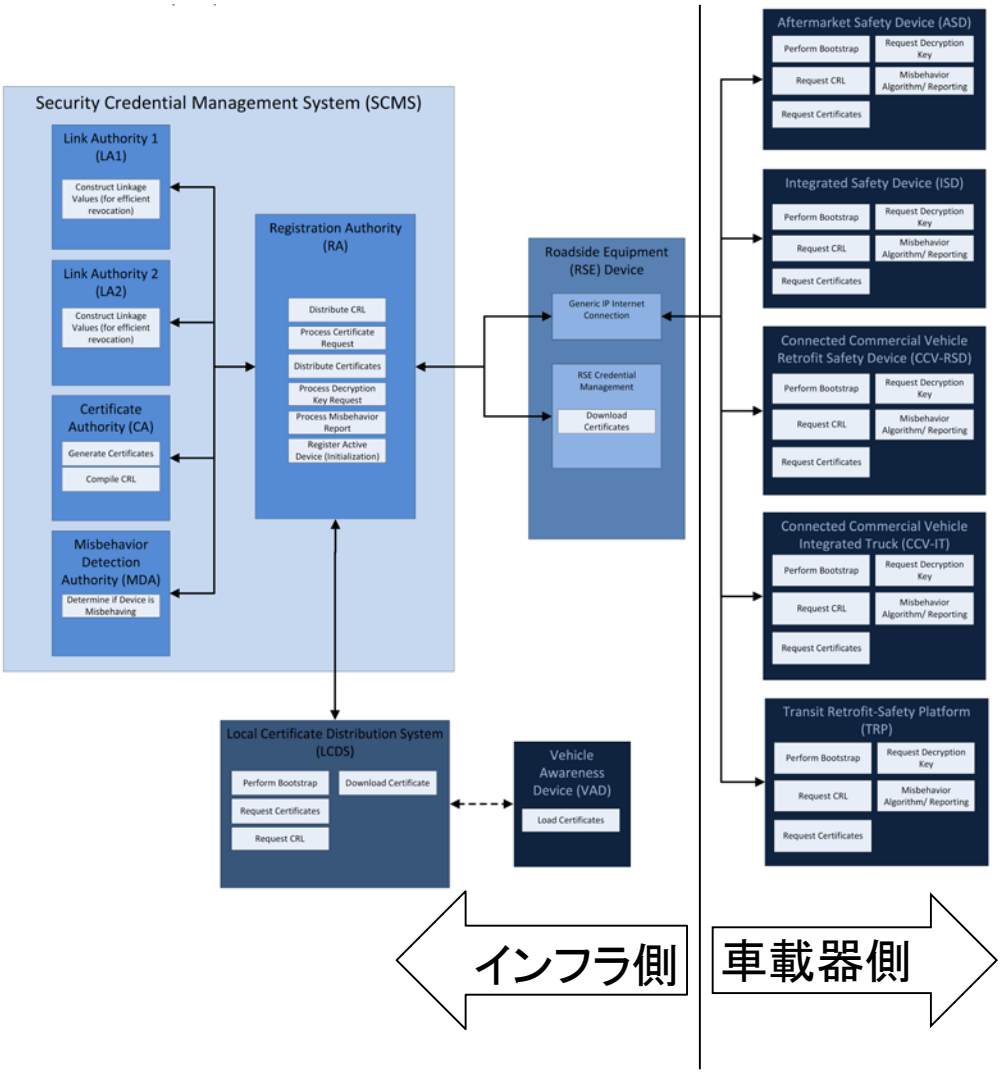


（出典：CHES 2014）

図 1.1-5　SCMS 概要

図 1.1-6 に第 1 期実証実験で実現し、現在も Ann Arbor エリアにて動作しているシステムの機能構成図を示す。2012 年 4 月の時点における機能構成図であるため、図 1.1-5 にて示した SCMS よりも機能が簡略化されている。証明書管理も Butterfly Algorithm による更新ではなく、電子証明書は RSU を経由して CA から 1 週間に 100 個が配布される。RSU から車載器に対しては、DSRC を利用した WSMP (WAVE Short Message Protocol) と呼ばれるプロトコルを利用している。WSMP では RSU と車載器がシングルホップ（他の機器へ受信情報を転送しない通信モード）による通信を実施する。

CAMP の本来の目的は車車間通信によるセーフティアプリケーション実現のための通信技術を研究開発することであったが、最近ではセキュリティの取り組みも強化している。Safety Pilot と平行に進んでいる CAMP では様々な技術について検討しており、セキュリティに対する性能要件もその一つである。性能要件については現在議論中であり、詳細な要件は 2015 年の夏頃に見えてくる予定である。また CAMP の成果物は外部の標準化団体へ展開されるため、CAMP として標準化活動を行うことは無い。



（出典：UMTRI よりヒアリング時に入手）

図 1.1-6　第 1 期実証実験における機能構成図

(3) 米国プロジェクトの進捗

UMTRI 主導によるミシガン州の Safety Pilot の第 1 期は成功裏に終了したが、現在もデータ収集を行っており、最長で 3 年間は継続される見通しである。また実際の商品との融合も計画的に進められている。例えば GM は 2017 年にキャデラックブランドで DSRC による V2X 通信ユニットの搭載を計画している。この通信ユニットは Delphi が製造、通信部位は Cohda Wireless が担当、さらにその通信部位のソフトウェアスタックは Security Innovation が担当している。一方、インフラ側については、現在、RSU の整備が,デトロイトを通過する 96 号線において進められている。

米国における棲み分けとしては

・技術を検討する CAMP

・実証実験を行う DOT の Safety Pilot

となり、UMTRI はそれぞれに技術提供として貢献する一方、自身としても後述する様な独自の実証実験を行っている。

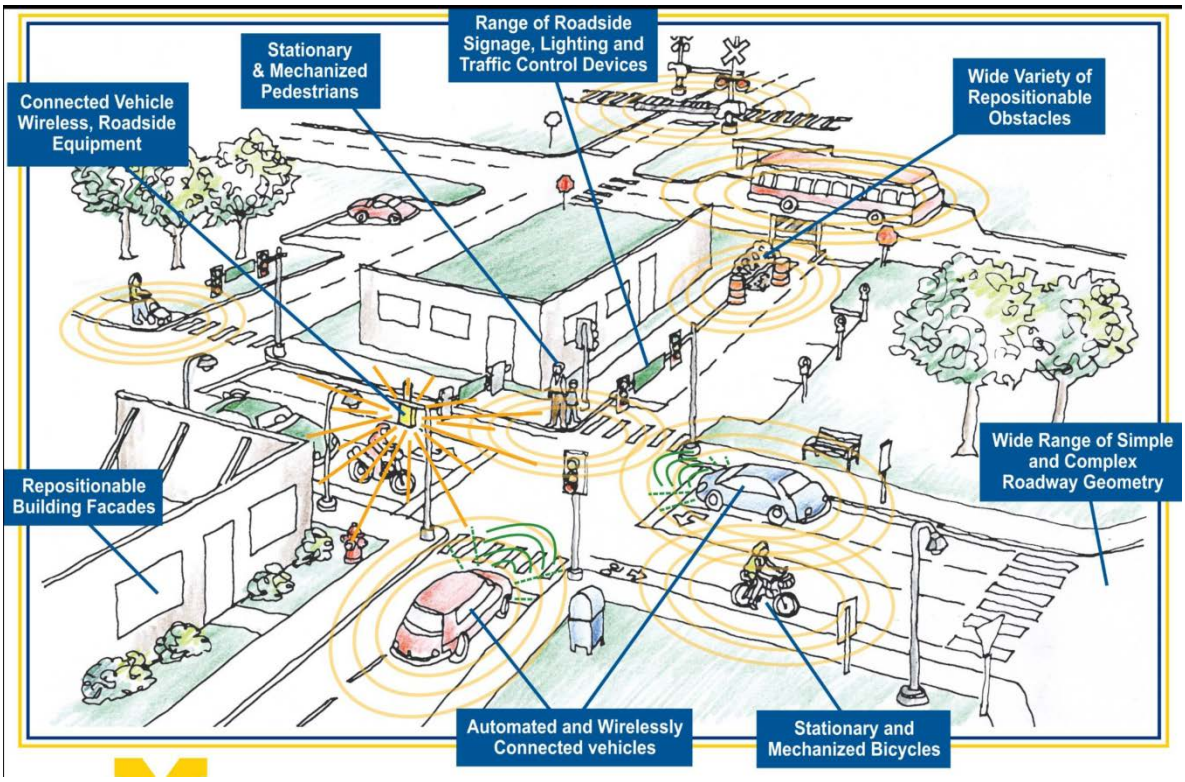
(4) 将来の展望

ミシガン州における Safety Pilot の FOT では Ann Arbor 市街地に 25 台の路側機と、3000 台弱の車両に通信機器の導入を完了し、現在はデータ収集を継続しているところであり、3 年間延長される見込みである。この実施する実証実験では、救急車など通信機能を有さない車両も混在するため、図 1.1-3 に示したサービス全てを実施することは出来ない。

UMTRI では Safety Pilot とは別に、MTC (Mobility Transformation Center)が次のプロジェクトとして立ち上がっている。MTC では 3 つの柱(pillar)がある。第 1 の柱では Safety Pilot を拡張して、2017 年頃に路側機を 60 台まで増やして Ann Arbor 市街地の全域に配備するとともに、通信機器を導入した車両等を 9000 台まで増やす。第 2 の柱では、2019 年頃に車両等を 20000 台まで増やし、ミシガン南東部エリアと繋ぐ。第 3 の柱では、2021 年頃に 2000 台規模の自動運転車を Ann Arbor エリアに導入することを計画している。

また、MTC のプロジェクトの一部として、UMTRI の敷地内に模擬市街地 ("M-City" testing facility)を構築し、自動車や自転車、歩行者に至るまであらゆる移動体に通信機能を導入した実験を行う予定である。"M-City"は 7 月 20 日～24 日に Ann Arbor で開催される Automated Vehicles Symposium 2015 に合わせて公式オープンする予定である（図 1.1-7）。

MTC では、図 1.1-6 で示した SCMS 側も図 1.1-5 により近い機能を含む様になり、Butterfly Algorithm による証明書生成なども行われる予定である。RSU などインフラ側の施設は Delphi、Bosch、デンソーなどが手がける予定となっている。また、Safety Pilot では欧州 OEM の参加は無かったが、現在ドイツの OEM が MTC への参加を予定している。なお、MTC への参加費用は、Founding Member が 3 年間で 1M$であり、Affiliate Member が 150K$となっている。



(http://www.mtc.umich.edu/test-facility)

図 1.1-7　UMTRI 内にて実施される実証実験

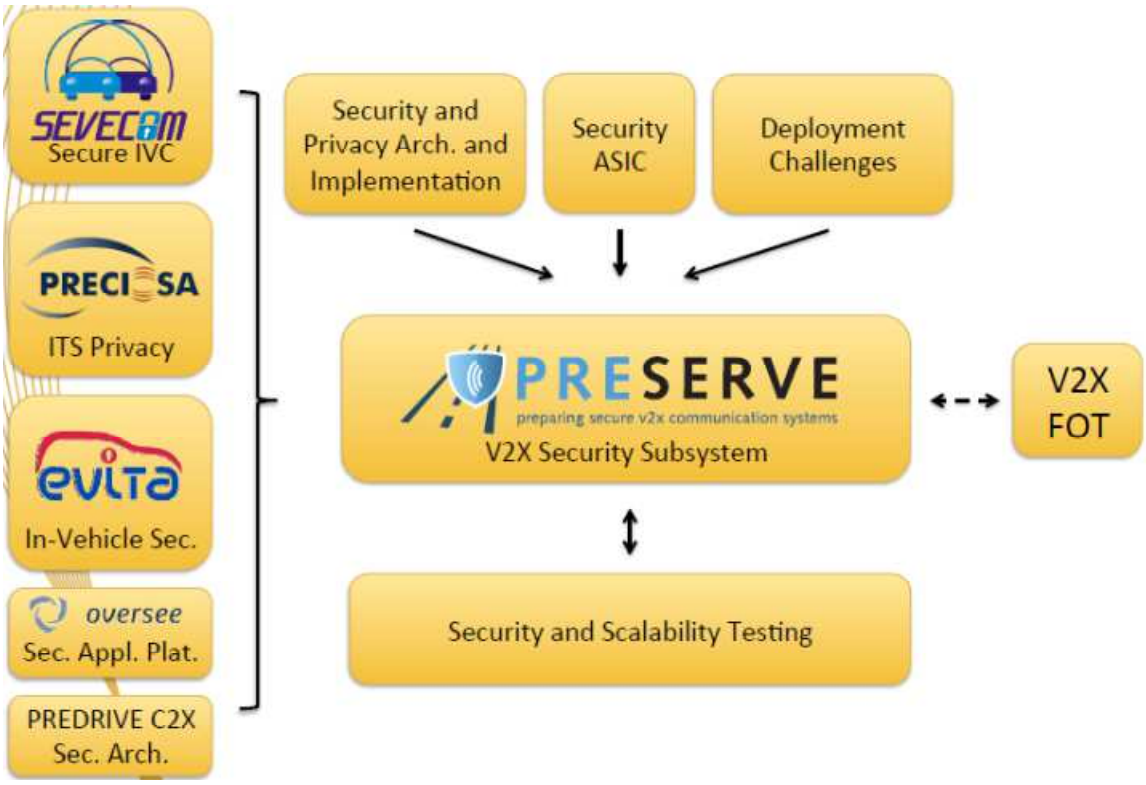
1.1.2 欧州における V2X セキュリティ関連調査

欧州では FP7 の PRESERVE による V2X セキュリティモジュールの ASIC (Application Specific Integrated Circuit：特定用途向け集積回路)化、C2C-CC による PKI ライクなインフラ検討などが実施されている。PRESERVE、および C2C-CC のプロジェクト関係者を訪問してヒアリング調査を実施した。

(1) PRESERVE

欧州第 7 期フレームワークプロジェクトの 1 つである PRESERVE は、4 つの既存プロジェクトの成果を統合し、V2X システムの実用化に向けて、セキュリティに関する技術開発と実証を行った上で、すぐに使える VSS (V2X Security Subsystem)と呼ばれるソフトウェアを他のプロジェクトで行われる FOT (Field Operational Test)に提供することを目的としたプロジェクトである。

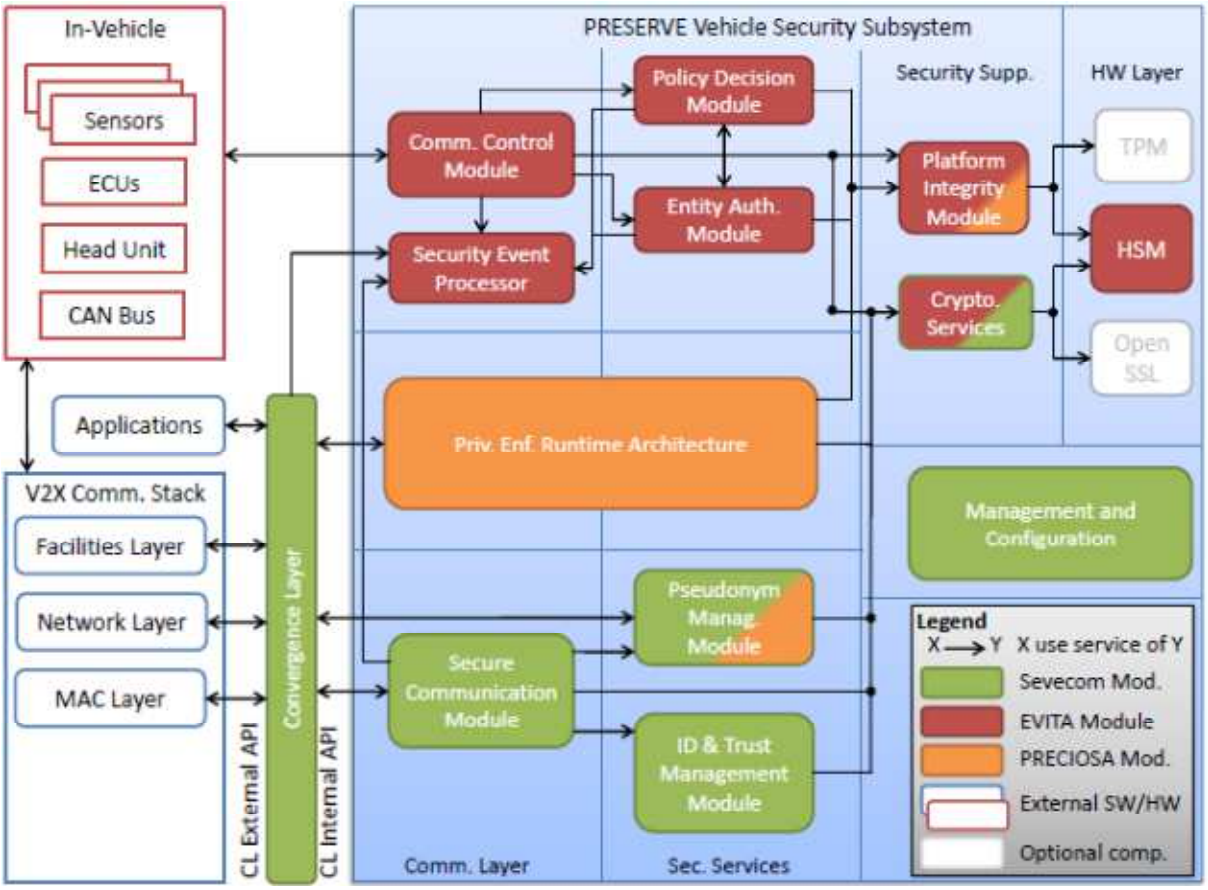
PRESERVE では実証のためのハードウェアの構成要素として ASIC の開発を行っているが、この ASIC は、図 1.1-8 に示すように、先行する 4 つのプロジェクトの成果を統合している。FP6 の SEVECOM(SEcure VEhicle COMmunication)は車車間通信のセキュリティ、FP7 の EVITA は車内システムのセキュリティ、FP7 の OVERSEE は ECU 向け仮想マシンマネージャー、FP7 や eSafety から出資を受ける PRECIOSA は V2X のプライバシをターゲットとしている。



（出典： EVITA D1.2.5.2, Final EVITA Workshop）

図 1.1-8　PRESERVE の構成要素

PRESERVE で開発された VSS（図 1.1-9）は Score@F 等の FOT や RSU の初期展開を実施する Amsterdam Group 等に展開される。FOT の結果は PRESERVE へフィードバックされる。PRESERVE 自体は技術開発と実証に注力するため、C2C-CC や ETSI (European Telecommunications Standards Institute)といった業界団体・標準化団体へ意見をするなどの活動は実施しない。Strong Advisory Board として登録する企業 (具体的には Audi、BMW、Daimler、Volks Wagen、デンソー、Infineon) が PRESERVE プロジェクトの意図を組んで、上述した業界団体へ意見することとなる。



（出典：PRESERVE D1.3 V2X Security Architecture V2）

図 1.1-9　PRESERVE のアーキテクチャ

(2) PRESERVE の進捗

2014 年 12 月末終了の予定は、現在当初計画から 6 ヶ月延長され 2015 年 6 月末までとなっている。遅延の原因は ASIC 開発の遅れであることが、PRESERVE の WEB ページ上の情報からも確認出来る。

PRESERVE では VSS の開発を行っているが、Kit-1、Kit-2 という 2 段階で進めており、Kit-1 では FPGA (Field-Programmable Gate Array)を用いたハードウェアモジュールの試作を完了している。Kit-2 と呼ばれるモジュールを構成するために用いられるのが、この ASIC である。また、Kit-1 ではセキュリティプロセッサは 1 つであったものが、Kit-2 では 2 つになり並列処理が行える様になっている。VSS のソフトウェアも Kit-2 では並列処理を扱

える様に変更されており、VSS Kit-2 の実証を行うために、PRESERVE では ASIC を製造することとしていた。

ヒアリングの結果、ASIC 開発に関連する遅延は、ASIC 製造に伴う外的要因であることが判明した。具体的には、ASIC の製造に IMEC (Interuniversity Microelectronics Centre) が提供するシャトルサービス*を利用しており、シャトルサービスに相乗りする他のプロジェクトの影響により、当初予定していたプロセス技術での製造がキャンセルされ、設計変更を余儀なくされた、というのが理由である。この結果、ASIC 製造に適用されるプロセスは、180nm、90nm、55nm と順次変更され、その都度再設計などを行っている。現在、55nm プロセスルールによる ASIC 製造が進んでおり、評価用チップのウェハプロセスは 2015 年 3 月頃に完了する予定である。

また、この ASIC は、実証評価用のデバイスであり、量産品ではないため、自動車レベルのテストや高温テストなどは行わず、耐タンパ性も考慮されていない。セキュリティの内部処理は並列動作を行う様に作られており、ASIC 上で動作する VSS Kit-2 も並列処理が可能な様に作られている。VSS Kit-2 はオープンソース方式で Twente 大学や Trialog 等が参加して開発された。

プロジェクトの完了は ASIC による検証完了に合わせて延長されているが、開発完了した VSS Kit-2 は既に WEB からダウンロード可能となっている。

＊ シャトルサービス：半導体ウェハを製造する際に使用するマスクに、複数のデバイスを搭載することで、マスク費用、ウェハプロセス費用を複数のプロジェクト等で分担し、コストを削減するもの。

(3) TAL（Trust Assurance Level：信用保証レベル）

TAL は、車載システムの信用保証レベルとして、C2C-CC で提案されたものである(図 1.1-10)。V2X システムでは、証明書を用いて送信されたメッセージの正当性の検証を行うが、これが実現出来たとしても、元々のデータが信頼出来るかどうかは別問題である。そこで、発信者の情報をどれだけ信用して良いかを示す指標として TAL を定義し、自動車がどのレベルのセキュリティ基準を満たしているかを、その開発時に認証しておく、という考え方である。

TAL では 0-4 のレベルが設定されており、その信頼性レベルを認証局に保証してもらうことで、特に車車間通信における送信元の保証に活用する。

C2C-CC にて議論している内容も Amsterdam Group による初期展開への適用が検討されている。C2C-CC の議論に基づき実施される FOT は「Day1 Use Case」と呼ばれる第 1 段階から実施され、以降議論が成熟するに従って Day2 Use Case という様に段階を踏みながら実施される。現在予定されている Day1 Use Case では TAL2 以上の高い信頼性を要求することとなっている。

TAL	Minimum Requirements			Security Implications		
	Evaluation Scope (TOE)	Evaluation Assurance Level (EAL)	Hardware Security Functions (HWSFR)	Prevented CC Attack Potential	Potential Security Implications	C2X Use Case Examples
0	None or unknown	None or unknown	None or unknown	None or unknown	Not reliable against security attacks in general	Some limited, e.g. using trusted C2I infrastructures
1	+ V2X box software	EAL 3	Mostly SW security functions w/ min hardware security like	Basic	Not reliable against simple hardware attacks (e.g., offline ulation)	Non-safety, but most privacy relevant use cases
2	+ V2X box hardware	EAL 4	+ dedicated HW security (i.e., secure processing & flash) + tamper evidence	Enhanced basic	Not reliable against more sophisticated hardware attacks (e.g., side-channel attacks)	C2C-CC day one use cases (e.g., passive warnings and helpers)
3	+ private ECU and private network	EAL 4+ with AVA_VAN.4 vulnerability resistance	+ basic tamper resistance	Moderate	C2X box secure as stand alone device, but without trustworthy in-vehicle inputs	Safety relevant relying not only on V2X inputs
4	+ all V2X relevant in-vehicle sensors and ECUs	EAL 4+ with AVA_VAN.5 vulnerability resistance	+ moderate to high tamper resistance	Moderate to high	C2X box is trustworthy also regarding all relevant in-vehicle inputs	All

Minimum Level for Day One Use Cases 2015

（出典：S. Goetz and H. Seudié: “Operational Security”, C2C-CC 2012）

図 1.1-10　C2C-CC にて議論中の Trusted Assurance Level

1.1.1(2)節で述べた米国方式同様に、欧州も車車間通信に電子証明書をメッセージに付与することで、メッセージ送信元の真正性担保を目指している。各 OEM は適切な TAL を選択して自動車を製造する。TAL ではレベルに相当する PP (Protection Profile) が配布されるため、OEM は PP を参照することで、選択した TAL に応じた製品を製造することが出来る。

製造した自動車は認証局に登録する際にどの PP を利用したかについて TOE (Target of Evaluation) を利用してデータベースに登録、またそのデータベースを参照する Long Term CA に対して電子証明書の発行を依頼する。実際に車車間メッセージ送信時に付与する証明書は、Long Term CA を参照する Pseudonym CA が有効期限の短い証明書を作成する。Pseudonym は、仮名、或いは偽名と訳され、ID を顕わに含まない。このため、Pseudonym Certificate は匿名証明書とも呼ばれる。有効期限の短い証明書を使う理由は、トレーサビリティ不可によるプライバシ確保が目的である。図 1.1-10 に示す TAL のコンセプトや実用時に必要なアイテムについては独 Escrypt を中心に議論が行われている。

Day1 Use Case では証明書の有効期限などは未定であり、証明書の CRL (Common Revocation List) 登録などと共に Day2 Use Case から導入される予定である。

(4) TAL の進捗

図 1.1-10 の認証方式に基づく FOT は、Day1 ユースケースおよび Day2 ユースケースを Amsterdam Group と連携して行うとしていた。当初は 2015 年末に実施予定であった Day1 ユースケースは、現在 2017 年開始に変更されている。C2C-CC における議論では、OEM およびサプライヤなど参加者の合意形成がとれていないため、昨年中旬から議論が停滞している。この影響は特にインフラ整備の遅延を招いている。このため 2017 年開始予定の FOT では、TAL の情報も含めた証明書配信に OEM センタから携帯電話網を利用するなどの代替案も検討されている。

参加者の合意形成がとれていない理由は企業間のみならず、企業内でもとれていないことも要因として考えられる。例えば Bosch グループでは FP7 プロジェクトである EVITA の成果物を Bosch HSM として実現している。この Bosch HSM (Hardware Security Module) では導入コストを意識し、耐タンパ性を犠牲にしている。しかしながら Escrypt 社（Bosch の孫会社）を中心に議論している TAL では、Day1 アプリに求められる最低レベルを TAL-2 としており、EAL4 相当（耐タンパ性を前提）を求めている。この様に企業またはグループ内で耐タンパ性に対する考え方が一致していない。

さらに欧州は複数の国で方式を共有するため、特にプライバシに関する各国の考え方の違いもプロジェクト進捗の遅延に影響している。

(5) 欧州プロジェクトの進捗

ETSI では、セキュリティ仕様などの規格化・標準化の部分がほぼ固まってきたので、PlugTest を Organize している段階にある。次の PlugTest はこの春に行われる予定であり、Preserve も PlugTest に参加を予定している。なお、C2C-CC はこの PlugTest に参加していない。ETSI としては、次の段階の Test を行い、ETSI で制定した標準が運用可能であることを検証することを目的としている。実用化の段階でのインフラ側の運営者が誰になるかは未定だが、実証実験に用いられる Pilot PKI は escrypt と FraunhoferSIT により運営される。

また、PRESERVE では、署名検証の要求レベルが 1000 メッセージ/s であるのに対して、コスト・消費電力等を考慮した現実的なハードウェアの性能はおよそ 400 メッセージ/s と、要求レベルを下回っている。そのため、署名検証の簡略化によって、ハードウェアの性能不足をカバーすることが検討されている。

この他、実用化に向けては V2X 通信の過密状態が起こるケースが予想されるため、例えば、渋滞などの混雑時に車からの発信周期を 10Hz から下げることによる対応が検討されている。

1.1.3 米国と欧州の方式の比較

V2X セキュリティは米国・欧州が同意したハーモナイゼーションにより統合化の議論が行われている。米国と欧州は 5.9GHz や IEEE1609.2 ベースのフォーマットを使うなど、通信メディアに関する項目のみならず、暗号アルゴリズムとして ECDSA（Elliptic Curve Digital Signature Algorithm：楕円曲線 DSA)を用いるなどの点で共通点を持っている。しかしながら表 1.1-1 の様に、細かい点までの相互互換は実現されていない。

表 1.1-1　V2X 通信に関する米国と欧州の比較

	米国	欧州
電子証明書	Butterfly Algorithm により Pseudonym Certification 間に関連性を残す	Pseudonym CA が独立して都度作成するため、Pseudonym Certification のトレースによるプライバシ漏洩は無い
電子署名	全てのメッセージの完全性担保のために付与	最初のメッセージのみ付与し、連続メッセージについてはハッシュなどのダイジェスト値のみ付与
車車間メッセージの送信頻度	10 メッセージ/秒	10 メッセージ/秒、速度が遅いときに発信周期を下げることを検討中
受信者によるメッセージ検証方式	ペイロードを確認して必要なメッセージのみ電子証明書・電子署名の検証を実施	全てのメッセージに対する検証を実施
成り済まし車載器への対策	Misbehavior Authority に履歴が蓄積され、成り済まし車載器からのメッセージ拒絶が同報通信される ただし、V2V のみでは迅速な検出／検証は不可能	電子証明書などが漏洩しない様、EAL4 レベルの車載器に電子証明書および電子署名を作成する秘密鍵を保管する
メッセージ伝送方式	シングルホップのみ、インフラの情報伝達にはマルチホップ	マルチホップに対応、中継する車載器はそのままメッセージをリレーする
Pseudonym Certification 配布方法	WiFi や携帯網等を利用して OEM から配布、RSU から配布なども検討中	ドイツは 2 年ごとの車検での補充を検討、国ごとに変わる可能性もあり、米国方式も検討中

これ以外にも認証方式や鍵管理インフラについて互換性を持たない項目が残っている。認証方式など表 1.1-1 に記載しなかった項目は米国・欧州ともにいくつかのプランを提案した未決定状態であるため、単純に比較出来ず記載していない。

1.1.4 まとめ

米国および欧州の V2X セキュリティプロジェクトについて、ヒアリングを中心にした調査結果を述べた。特に注目したプロジェクトの進捗度合いについて、米国は順調に推移し、欧州は技術以外の要因による遅れであることが確認出来た。欧州は 2006 年から開始された FP6 の SEVECOM を起点として、公的機関による V2X セキュリティ検討が開始された。米国は 2003 年から実施されていた VII (Vehicle Infrastructure Integration) が 2009 年に IntelliDrive と名称を変えて計画および推進体制の見直しをした時点から、キーワードレベルのセキュリティが含まれる様になった。V2X のセキュリティ方式は IEEE 1609.2 として規定され、欧州もこれを取り入れ、ETSI の規定としている。

また、具体的な動きとしては 2012 年に NHTSA (National Highway Traffic Safety Administration) からサイバーセキュリティに関する研究プランがリリースされた。この様な背景および表 1.1-1 の比較結果から、下記の様にまとめることが出来る。

・欧州は標準化ビジネスが得意なこともあり、Framework Programme 実施などプロジェクト開始が早かった。しかしながら具体的なアイテムの検討フェーズに移行するに従って、メッセージ送信頻度などシステムの挙動を決定するパラメータが複雑となってしまった。
・米国は欧州に遅れて開始した一方、車車間および路車間との通信はシングルホップのみにするなど、システムの挙動を決定するパラメータが単純であり、性能要件などの決定が容易である。
・ヒアリングに基づくこれらの現状から V2X におけるセキュリティ機能について、米国の方がより早くシステム導入されると予想される。

今後は V2X セキュリティ機能の標準化および通信ユニットの認証などが注目される。認証については米国・欧州ともにいくつかの実現方法が検討され、そのレベルも「公的機関による認証」「公的機関に委託された第 3 者による認証」「公的機関が OEM に認証作業を委託」と様々である。また「公的機関によるリファレンスモデルを参照した OEM による独自認証」なども候補としてあがり、この議論はしばらく継続すると考えられる。

通信規格は IEEE1609.x など既に標準化されている。一方通信ユニットについては、V2X システムのうち、車車間通信および路車間通信等は、自動車業界に閉じ、インターオペラビリティなど他業界との連携を考慮する必要が無いことから、C2C-CC からの仕様公開などによる実質的な業界標準が使われると予測される。

また、インフラ側の応用等として議論されているものであっても、署名検証の簡略化や、渋滞時の送信周期を下げるといった動作は、車載機等の端末側で行うべき処理と考えられる。この場合、ハードウェアは同一であっても、ソフトウェア等の変更が必要になる可能性がある。そのため、セキュリティ技術としては、インフラ側をどの様に構築し、どの様に運営するのかについても理解しておくことが重要である。

1.2　セキュリティ方式調査

現在車車間/路車間通信（以下 V2X）は日米欧にて実用化に向けた開発が進んでおり、日本では 2015 年中にはサービス開始が予定されている。欧米でも同様に実用化に向けた開発及び実証実験が行われており、2016～2017 年にかけてサービス開始が予定されている。

各地域とも V2X 実用化に向けたシステム開発が最終段階を迎えており、OEM 及び Tier1 が実証用のプロトタイプを製作しているが、それぞれの地域の規格に準拠した機能を実装しており互換性のない通信ユニットとなっている。特にセキュリティに関しては規格作成の遅れや地域間でのポリシーの違いなどもあり、最終的な機能がどうなるか不透明な点が多い状況である。

今回、欧州において PP (Protection Profile）や、Standard Profile を策定している C2C-CC (CAR 2 CAR Communication Consortium）の Security WG のキーパーソンと面会し、欧州における V2X セキュリティの標準化動向に関し調査を行った。本レポートでは現在の C2C-CC 内で議論されている内容と、欧州における V2X システムセキュリティの検討状況を報告する。

また、米国の PlugFest においては、今年度中に実施されると見込まれていた相互接続性試験に用いられるセキュリティ仕様のアップデートが、テストサイト等での評価項目にはなく、仕様説明も行われなかったため、ここでは欧州の動向のみについて報告する。

1.2.1　C2C-CC Organization

C2C-CC は図 1.2-1 の様に、Steering committee の下にいくつかの Technical committee があり、その中に Working Group が存在している。V2X に関するセキュリティを検討しているのは、Security Working group で、現在は、この Working group 内に以下に示す 3 つの Task force group が設けられ、集中的に課題検討を行っている。

- Protection Profile finalization Task Force
- Security Requirements and qualification Task Force
- PKI Task Force

（https://www.car-2-car.org/index.php?id=22）

図 1.2-1　C2C-CC Organization

1.2.2 Protection Profile Finalization Task Force

2014 年 7 月に Protection Profile Version 1.01 が発行されている。

(1) 受信側の自動車におけるセキュリティ要件

ETSI で想定されている V2X システムのユースケースでは、自動車 OEM、Tier 1 によってパフォーマンスの要求に開きがあるが、概ね 1 秒間に 400～1000 回の証明書の署名検証を要求されている。

また、Brainpool のサポートを BSI (Bundesamt für Sicherheit in der Informationstechnik)が提案している。Brainpool を使う背景として、欧州のインフラストラクチャー側で Brainpool が使われているからである。従来、C2C-CC では、署名生成・検証に使う楕円暗号アルゴリズムを NIST (National Institute of Standards and Technology:アメリカ国立標準技術研究所) P256 としているが、この提案を採用すると、この二つのアルゴリズムの平行使用となる。

署名検証のパフォーマンスを達成する事と、2 つの暗号アルゴリズムの平行使用実現が容易ではない。

(2) HSM のセキュリティレベル

現状の PP では、ISO 15408 で定義される Common Criteria の EAL (Evaluation Assurance Level)における EAL 4 相当を TAL 2 と定義し、V2X モジュールへの要求としている。

1.2.3 Security Requirements and Qualification Task Force

自動車内部ネットワークセキュリティ等の検討を行っている。V2X モジュールについては、車車間ないし路車間通信を行った後に、衝突の危険などを察知して運転者に警告を表示するシステムとなっている。V2X モジュールは、Control Area Network（以下 CAN）などを介してインフォテインメントデバイス等に接続される。V2X モジュールは外部との通信を行うため、V2X モジュールを踏み台にして攻撃者が自動車内部ネットワークに攻撃を行う事が可能となる。そのため、内部ネットワーク接続を行う際のセキュリティが必要となる。

1.2.4　C2C-CC 参加者状況

欧州 C2C-CC 参加者情報については、最近までは詳細が分からなかったが、WEB 上で公開される様になった。（https://www.car-2-car.org/index.php?id=members）

<Partners>

- AUDI
- BMW
- DAIMLER
- FORD
- HONDA
- HYUNDAI
- MAN
- OPEL
- PSA Peugeot Citroën
- RENAULT
- VOLKSWAGEN
- VOLVO
- YAMAHA

< Associate Members>

- Atmel
- Autotalks
- Bosch
- CETECOM
- Cohda Wireless
- commsignia
- Continental
- DELPHI
- DENSO
- dSPACE
- ejct
- escrypt
- HESSEN Mobil
- HITACHI
- iav
- KOSTAL
- lesswire
- LG
- MARBEN
- NEC
- nordsys
- NXP
- Renesas
- ROHDE&SCHWARZ
- Security Innovation
- SIEMENS
- SPRINT Communication
- swarco
- TASS International
- TE connectivity
- ublox
- Vector
- Visteon electronics

<Development Members>

- bast
- CSIC
- DLR (Deutsches Zentrum für Luft- und Raumfahrt：ドイツ航空宇宙センター)
- EUROCOM
- HTW
- Fraunhofer（グループ 5 社：AISEC, ESK, FOKUS, Heinrich Hertz Institute, SIT）
- ifak (Institut für Automation und Kommunikation)
- ihp (http://www.ihp-microelectronics.com/en/start.html)
- ika (RWTH Aachen Unversity)
- iMdea networks
- IMST GmbH
- INRIA
- ISMB (Istituto Superiore Mario Boella)
- KIT (Karlsruhe Institute of Technology)
- KTH Electrical Engineering
- Technische Hochschule Ingolstadt
- TNO (https://www.tno.nl/en/)
- Technische Universitat Braunschweig
- Technische Universitat Chemnitz
- technische universitat dortmund
- TUM (Technische Universität München)
- Leibniz Universitat Hannover
- University of Twente
- Ulm University

1.2.5 まとめ

今回 C2C-CC の仕様検討の状況に関して調査を行った。欧州における仕様策定は実装検討フェーズに入りつつあり、認証の枠組みなども具体的に検討がスタートしている。また、自動車内部ネットワークセキュリティの検討もスタートしており、セキュリティ実装要求は高まる傾向であると考えられる。

C2C-CC で 4 月に発行される予定の Protection Profile 及び、Standard Profile に関しては、大幅に変更される可能性もあるため、今後も C2C-CC の動向を注意深く見守る必要がある。

1.3 米国 V2X 開発状況調査

現在、V2X システムは日米欧にて実用化に向けた開発が進んでおり、日本では 2015 年中にはサービス開始が予定されている。欧米でも同様に実用化に向けた開発及び実証実験が行われており、2016～2017 年にかけてサービス開始が予定されている。

各地域とも V2X 実用化に向けたシステム開発が最終段階を迎えており、OEM 及び Tier1 が実証用のプロトタイプを制作しているが、それぞれの地域の規格に準拠した機能を実装しており互換性のない通信ユニットとなっている。特にセキュリティに関しては規格作成の遅れや地域間でのポリシーの違いなどもあり、最終的な機能がどうなるか不透明な点が多い状況である。

今回、北米 USDOT が運営する Test Lab で相互接続性試験（以下 PlugFest）において、通信プロトコル及びセキュリティの機能確認を行った。ここでは、相互接続性試験として実施された内容について報告する。

1.3.1 北米 PlugFest 参加

(1) 日程

PlugFest は USDOT が主催しており、2014 年は 5 回行った実績がある相互接続性試験 (http://www.its.dot.gov/testbed/plugFests.htm) である。

当初 2015 年は 2 回開催が予定されていたが、毎週水曜日に Lab を解放し接続性を確認する様に対応が変更されたことから、下記に日程にて USDOT の Lab を訪問し、その接続性を検証した。

日程：1 回目　2014 年 12 月 15 日～12 月 17 日
　　2 回目　2015 年 2 月 3 日～2 月 5 日
場所：39555 Orchard Hill Pl, Novi, MI 48375, Southeast Michigan Test Bed 内 Lab

図 1.3-1　USDOT テストラボ

(2) 評価ユニット

今回 PlugFest に参加して相互接続性試験を実施した評価ユニットは図 1.3-2 のシステム構成となっている。

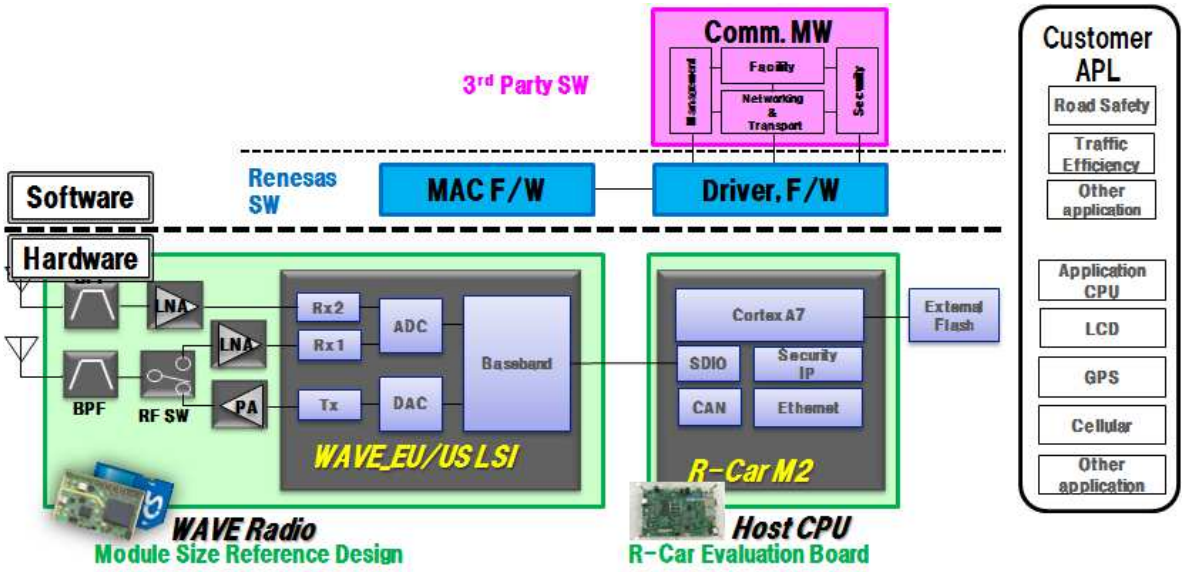


図 1.3-2　評価デバイス構成

またシステムの構成要素は下記に示す。

・ハードウェア 1：ルネサス社製無線デバイス評価ボード（図 1.3-3）

－IEEE802.11p/ITS-G5 用無線デバイスを実装

－外付け部品として、送信アンプ、フィルタ等を実装

－I/F：SMA(高周波)、SDIO、UART

・ハードウェア 2：ルネサス社製プロセッサ評価ボード（図 1.3-4）
　－ルネサス社製 R-CAR-M2 デバイス
　－セキュリティ対応：R-CAR-M2 内蔵のセキュリティアクセラレータ使用
　－BSP：Linux ベース BSP (Board Support Package)
・通信用ミドルウェア：パートナー製 WSMP、SAE J2735 対応ソフトウェア
・セキュリティーミドルウェア:パートナー製 IEEE1609.2［北米セキュリティ規格追加］
　応ソフトウェア

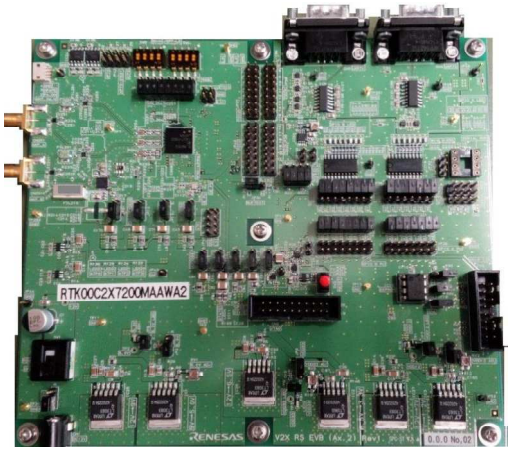


図 1.3-3　無線ボード

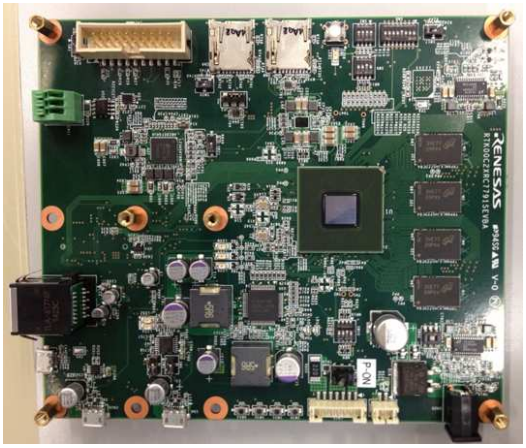


図 1.3-4　ホストボード

今回ハードウェアはルネサス社製であるが、ソフトウェアは海外製である。通信用ミドルウェアを供給可能な国内メーカーが 2 社程あるが、欧州・米国向けのセキュリティソフトウェアに関しては国内メーカーにて製品化の予定なく、海外メーカーに差別化される要因となる可能性がある。

1.3.2　試験環境および試験内容

今回相互接続性試験に使用した Lab は Southeast Michigan Test Bed の一部であるため、USDOT が考案した CVRIA (Connected Vehicle Reference Implementation Architecture)に準拠している。CVRIA はシステムやアプリケーションを決めており、 さらに各種インターフェースも決めている。

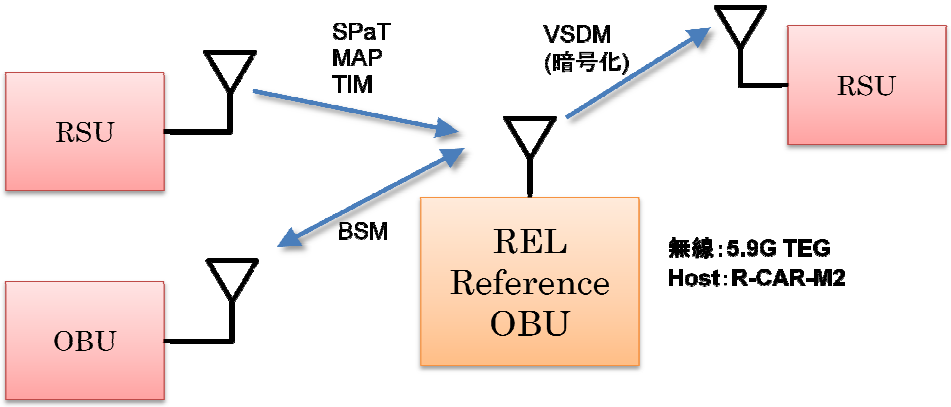


図 1.3-5　PlugFest 試験環境

今回のテストでは相互接続性の確認と、V2X デバイスの機能を確認する目的のため、テストシナリオについては以下の内容での試験を実施した。

表 1.3-1　テスト項目

No.	Type	Title	Description	RF Channel (Ch.No.)	Mode	Item
1	**Basic**	Channel Switch	CCH / SCH channel switching	CCH (178), SCH (174)	Alternate	
2	**IPv6 (VSDM)**	Access to warehouse	Transmit VSDM on SCH(174)	CCH (178), SCH (174)	Alternate	Awareness
3			(with BSM Tx on SCH(172))	(SCH (172))		Trust Establishment
4						Data Exchange
5	**V2V, V2I, VSDM**	2 Radios (Alternate)	Radio1(Rx, RxTx):	Radio1:	Radio1:	WSA Verification
6	**Combination**		TIM, WSA on CCH (178),	CCH (178), SCH (174)	Alternate	WSA Decoding
7			VSDM on SCH (174)			TIM Verification
8			Radio2(Rx, Tx):	Radio2:	Radio2:	TIM Decoding
9			SPaT, MAP, BSM(Rx) on SCH (172),	SCH (172)	Continuous	SPaT Verification
10			BSM(Tx) on SCH(172)			SPaT Decoding
11						MAP Verification
12						MAP Decoding
13						BSM (Rx) Verification
14						BSM (Rx) Decoding
15						BSM (Tx) Encoding
16						BSM (Tx) Signning
17						VSDM Awareness
18						VSDM Trust Establishment
19						VSDM Data Exchange

Test Bed では 2 種類の通信、Broadcast 及び Transactional、がサポートされており、その上にアプリケーションが実装されている。 Broadcast は BSM (Basic Safety Message)、SPaT (Signal Phase and Timing)、MAP(intersection geometry and topology)に用いられている。また Transactional は 10kbytes 程度のデータ交換に用いられている。その際複数の RSU にまたがる様な通信は前提にしていない。各通信に対し Test Bed としてテストシナリオが決定していないため、参加者がテストシナリオを持ち込みテスト行うことが前提となっている。これは過去の PlugFest でも同様の方針で対応していた様である。

また、Lab には RSU (Roadside Unit)、 VAD (Vehicle Awareness Devices)、ASD (Aftermarket Safety Devices) が設置されており、今回は RSU と VAD との接続性確認を行った。

1.3.3　セキュリティ仕様について

セキュリティソフトは、Safety Pilot と SouthEast Michigan TestBed で異なるバージョンを利用している。また、Test Bed で使用される 2 種類の通信に対しては、それぞれ異なるセキュリティが適用される。

Broadcast：　署名付きだが非暗号化したメッセージを使用。また署名もサーバーでは行わず RSU で署名される。そのため北米で議論されている SCMS（図 1.1-5 参照）に準拠した署名対応は Southeast Michigan Test Bed では行われていない。

Transactional：　Unicast 通信が前提であり Pier to Pier データ交換に用いられ署名付き暗号化メッセージを使用。セッション鍵の配信は SCMS が構築されていないため、PC ベースで行われている。

1.3.4　米国 TestBed 参加者状況

USDOT の HP では、TestBed に参加している企業・団体等が公開されており、2015 年 1 月時点で 62 団体の参加が確認出来た。62 団体のうち、企業は 47 であり、アプリケーションコンテンツ：9 社、OEM：5 社、デバイスメーカー：13 社、エンジニアリングサービス：9 社、セキュリティサービス：4 社、テスティングサービス：3 社、事業者団体：4 団体となっている。(http://www.its.dot.gov/testbed/testbed_affiliated.htm)

- Arada Systems
- CETECOM
- Cohda Wireless America LLC
- DENSO Corporation
- Dering & Estrada
- Detroit Department of Public Works
- Industrial Technology Research Institute (ITRI)
- La Trobe University (Melbourne)
- Marben Products
- 7Layers Inc.
- NextEnergy
- OminiAir
- Pioneer Advanced Solutions
- Security Innovation
- Siemens Industry Inc.
- Southwest Research Institute
- Tampa Hillsborough Expressway Authority
- TIEMAC CORPORATION
- University of Arizona
- University of Michigan/UMTRI
- Autotalks LTD
- Connected Vehicle Trade Assc.
- Battelle Memorial Institute
- Rohde & Schwarz USA, Inc.
- Contra Costa Transportation Authority
- Virginia Tech Transportation Institute
- Traffic Technology Solutions
- University of Wisconsin Madison
- Commsignia LTD
- Global Mobile Alert
- Ericsson
- Savari Inc.
- Renesas Electronics America, Inc.
- The Road Commission for Oakland County
- The Regents of the University of California, Berkeley

・Unex Technology Corporation
・Go-Light
・Case Western Reserve University
・Vehicle Data Science Corporation
・Green Driver Inc.
・Commsignia Danlaw, Inc.
・Azimuth Systems
・Peiker Acustic UL, LLC
・Carnegie Mellon University
・Sirius XM Radio Inc.
・Pravala Networks
・Illinois Tollway
・MET Laboratories
・On Time Systems Aldis, Inc.
・eTrans 2020
・Paxgrid Telemetric Systems, Inc.
・AutoTech Technology Development, Inc.

なお、現状で USDOT の仕様に適合するポテンシャルがあるメーカーの製品が、Safety Pilot Qualified Products List (QPL)として、USDOT の HP 上に掲載されている。
(http://www.its.dot.gov/safety_pilot/spmd.htm)

Roadside Equipment
- Arada Systems
- Kapsch TrafficCom, Inc.
- Industrial Technology Research Institute
- Cohda Wireless and Cisco Systems Inc.
- Savari Networks

Vehicle Awareness Devices
- AutoTalks Ltd
- Cohda Wireless
- Denso International America, Inc.
- DGE Inc.
- Industrial Technology Research Institute
- Savari Networks
- Arada Systems

Aftermarket Safety Devices
- Cohda Wireless (with Delphi as a subcontractor)
- Cohda Wireless (with Visteon as a subcontractor)
- Denso International of America, Inc.
- Kapsch TrafficCom, Inc.

Device Certifier
- Booz Allen Hamilton
- OmniAir

また、UMTRI の一角には、V2X 関連機器の試作品と思われるものが展示してあり、機器に記載されている名前は、ARADA、SAVARI、Cohda Wireless、工業技術研究院（ITRI）の 4 つであった。

図 1.3-6　UMTRI 内の一角に設けられた RSU 等の機器の展示

1.3.5　まとめ

今回 USDOT の PlugFest に参加し、相互接続性の検証を行った。　結果として当初予定していたテストシナリオで動作することが確認出来た。相互接続試験の相手方となったデバイスもまた、北米向け V2X の仕様を少なくとも同等以上のレベルで実現していると見られる。

セキュリティについては Southeast Michigan Test Bed が提供する機能に対応することが確認出来た。ただし、今回はテスト用のシステムであり、商用化で適用される SCMS への対応は確認出来ておらず、いつ SCMS 対応の評価が行われる様になるか状況を注視していく必要がある。

1.4　調査結果の分析、まとめ

欧米における V2X システムに係るセキュリティ技術に関するプロジェクトの状況や、実際にプロジェクトで行われている実証実験に参加する等により集めた情報の整理とまとめを行った。また、調査の過程で得られた追加の情報や、事業活動の中で把握している情報とも整合させた結果、以下の様に整理した。

1.4.1　欧米のプロジェクトの進捗状況

欧米のプロジェクトに関しては、一部の工程に遅れはあるものの、全体としては大きな問題なく進展しており、特に米国では V2X システムの実用化に向けて NHTSA などがさらに積極的に推進しようとしている。一部の工程の遅れとして確認出来たものは、欧州 PRESERVE での ASIC 開発に関するものであるが、技術的な遅れというより、ASIC 製造上の理由によるものと判明した。従って、車載機等の V2X モジュールのハードウェアレベルの仕様はこれまでに公開されているものからの変更の可能性は低いと言える。

ただし、C2C-CC において使用している署名生成・検証に使う暗号アルゴリズムである NIST P256 に加えて、Brainpool を平行して使用する様 BSI から勧告があり、ハードウェアレベルでの仕様が見直され、追加される可能性がある。

欧米ともに、欧州の ITS Corridor の様に実証実験の規模を拡大したり、米国の MTC の様に模擬市街路を作って全ての車が V2V システムを搭載した状態での実験を行う、といったことが計画されている。

V2X システムのインフラ側におけるセキュリティ仕様に関しては、仕組みは欧米のそれぞれで決まっているが、その仕組みを使った実証実験が、近々行われる可能性があり、引き続き動向に注意しておく必要がある。

1.4.2　現状の課題としてのプライバシ保護とインフラ構築

V2X システムのセキュリティに関する課題は、主としてプライバシ保護とインフラ構築である。プライバシ保護に関しては、米国と欧州で証明書の呼び名がそれぞれ Short Term Certificate と Pseudonym Certificate と異なり、証明書の有効期間も異なる。欧米での違いに加え、さらに欧州では国ごとに適用される法律も異なるため、プライバシ保護に対して求めるレベルが異なり、欧州の内部でも扱いが決まっていない部分である。

もう一つの主要な課題は、インフラ側に関連する部分であり、インフラを構築する枠組みは欧米ともほぼ固まっているが、枠組みの中では Misbehavior Authority における Misbehavior と判断する方式が決まっておらず議論が継続している。また、インフラ側では個人情報を扱う様になることと、ビジネスモデルが見えていないため、インフラ側を運営する事業者がどうなるか決まっていない。

これらの課題をセキュリティ技術の面から見ると、欧州でセキュリティ技術の 3 つの柱と表現されていた、セキュアな ID 管理方法、プライバシ保護、データの正当性、となっており、欧州で研究に力を入れている分野でもある。なお、3 つの柱に関して、それぞれ

の項目に対し、セキュアな ID 管理方法（Secure Identity Management）では、Message Signature, Secure Storage, PKI, Security Credential Management, Certificate, etc 等、プライバシ保護（Privacy Protection）では Pseudonym、データの正当性（Data Consistency）は Misbehavior Detection が関連項目としてある。

1.4.3 V2X システムの車両への搭載は欧米とも 2017 年頃

V2X システムの実際の車両への搭載は欧米とも 2017 年頃から始まると見られる。米国では GM が 2017 年型キャデラックへの搭載を表明している。欧州では、C2C-CC の中で一部の OEM は 2017 年に First Product を出すという話をしている。ただし、First Product イコール市販車を意味しないため、V2X システム搭載車の市販時期は米国より遅くなる可能性もある。

車両側の実用化時期については上記の通りであり、V2V 通信は可能になるが、V2I 通信を含めた V2X システム全体の実用化時期については現状見えていない。そのため、V2X 車載機に格納している暗号鍵のアップデートについては、スマートフォンを経由して行う方式などが検討されている。

また、V2X システムが実用化される際には、車載機や路側機の相互接続性を保障する仕組みとして、車載機等の V2X モジュール認証の取得が必須となる可能性が高い。現状では認証に関する議論に関する情報は入手出来ていないが、実用化時期が 2017 年とすれば、認証のあり方も近々議論が開始されるものと考えられる。認証のあり方は、今後、V2X モジュールの製品化スケジュールに影響を及ぼす可能性があるため、セキュリティ技術に関連する項目として、認証のあり方についても早急に議論を開始する必要がある。

1.4.4 性能とコストの考え方

今回調査を行ったプロジェクトの一つである PRESERVE では、セキュリティに対する要求として、V2X システムの車載機における署名検証の能力が 1000 メッセージ/s という項目（周辺に 100 台の車両が存在し、それぞれの車両が 100ms 毎にメッセージを送信する状況を想定）があった。この数値自体は、署名検証処理を行う半導体の動作クロックを上げたり、並列処理数を増やしたりすることにより達成は可能であるが、車載機のコストが上がる。

V2X システムの車載機が普及するためには、半導体のコストも現実的なレベルであることが必要である。現時点で妥当なコストで実現出来る性能レベルである 400-500 メッセージ/s でも、セキュリティを担保出来る仕組みとして署名検証簡略化等の適用が検討されている。一方で、署名検証を行う部分は、公開鍵を使うため、秘密鍵を格納する不揮発性メモリ等が不要であり、耐タンパ性も要求されない。このため、この部分の半導体を別チップとして作る半導体メーカーもいる。

欧米のプロジェクトでは、そこに参画する大学教授等も現実的なコストで実現出来るシステムであることが重要と発言されており、現実的なコストで性能が実現出来ない場合に、どういった対策が出来るか、ということも研究の一分野になっている。

1.4.5　次世代高度運転支援でのリスクを想定した脅威分析に必要な要件の検討

高度運転支援システムの最終の目標は、自動運転の実現であり、その実現のためには、どういった要件を満たす必要があるのかを論理的に導出する必要がある。論理的な分析手法としては脅威分析が用いられているが、脅威分析の実施にあたっては、自動運転の各レベルごとのユースケースの明確化が必須である。

そこで、まず、現状使われているユースケースが、どのレベルまでをカバー出来ているのかをまとめる。さらに、その結果から類推される自動運転の各レベルに対応したユースケースの抽出とカテゴリの明確化を行うべきである。

これらを検討するにあたり、まず、現状検討されている高度運転支援システムのユースケースを調査し、必須となると考えられるものを基礎となるユースケースとしてまとめる。また、このユースケースを現在 SIP で考えられている自動走行のレベルと紐付けることで、現状どの程度カバー出来ているか明確にする。さらに、カバーされていないのがどのようなカテゴリのユースケースになるかを検討してまとめる。

第 2 章　海外展開可能な V2X システムに係るセキュリティ技術のあり方の検討

日本国内のサプライヤ等が開発する V2X システムのセキュリティ技術が海外へ展開可能とするためには、開発する製品を海外で適用される標準や規格に適合させることが必要である。これに加えて、自らが持つ技術をベースにした標準化・規格化への提案を行っていくことが重要である。

V2X システムのセキュリティ技術については、既に定まっているものもあるため、追加提案を行うことが想定される。追加提案を行うためには、どの様な考え方を基に規格策定を進めてきたか、現状の技術やプロジェクトがどこまで進んでいるのか、を理解した上で技術開発や研究を進めていくことが重要である。

そこで、現在の技術やプロジェクトの状況の調査を行い、第 1 章としてまとめている。ここでは、セキュリティ技術に関する規格策定を進める上で必須となる脅威分析が、これまでの主なプロジェクトでどの様に進められたか、特に脅威分析がどの様な前提条件のもとに実施されたかの調査を行った。

これらの調査結果を踏まえ、V2X セキュリティ検討 WG において、V2X システムに係るセキュリティ技術のあり方について検討を行った。

2.1　欧州のセキュリティ仕様の前提条件調査

2.1.1　前提条件の分類

脅威分析を実施するにあたり用いられる前提条件は、以下の 3 つ、① 前提条件、② セキュリティを使用するときの条件、③ 脅威分析を実施したときのリスク条件である。これらを具体化して、以下の調査項目に分け、調査を実施した。

① 対象システムの想定アーキテクチャ

車車間、路車間通信を用いたシステムのセキュリティに関する、欧州を中心としたプロジェクトを対象に、各プロジェクトの対象としたシステムで想定されるアーキテクチャおよび、そこで扱われる情報がどの様な側面から保護されるか(保護すべき情報資産)を調査する。ただし、プロジェクトによってはこれらが明記されていない場合もある。この場合は、対応情報なしとなる。

② 対象システムのユースケース

各プロジェクトの対象としたシステムで、どの様なユースケースが前提とされているかを調査する。さらに、調査結果を統合し、現状の基礎となるユースケースのリストを作成する。

③ リスク見積もり方法

各プロジェクトにおいて実施された脅威分析で用いられたリスクの見積もり方法について調査する。ただし、調査対象の中には明確にリスクを見積もっていないものもある。これについては、対応情報なしとなる。また、調査結果を基に今後どの様なリスク見積もり方法を用いるべきか、考察を行う。

2.1.2 調査対象と調査結果

ここでは、欧州で実施されたプロジェクトを中心に、国内でのプロジェクトも調査対象とし、10 のプロジェクトを抽出した。このうち、⑥sim^{TD}、⑦PRE-DRIVE、⑨C2C-CC の三つに関しては調査を実施出来ていない。⑥は詳細な成果報告書等としてはドイツ語のドキュメントしか存在しない、⑦は一般への公開がなされていない、⑨は詳細な資料が入手出来ないというのが、その理由である。

また、①PRESERVE で前提としたユースケースは、ここで挙げているその他のプロジェクトのユースケースを基に作成されており、プロジェクト固有のものが存在していない。そこで、これについては個別でまとめず、2.1.3 節記載の基礎となるユースケース作成時に行った調査結果比較で対応を明確化するのみにとどめた。また、調査が実施出来なかった⑥、⑦、⑨のプロジェクトのみに依存するものも存在しない。結果として、調査対象は②、③、④、⑤、⑧、⑩の 6 つのプロジェクトとした。

① PRESERVE
- Deliverable 1.1 Security Requirements of Vehicle Security Architecture

② EVITA
- D2.1 - Specification and evaluation of e-security relevant use cases
- D2.3 - Security requirements for automotive on-board networks based," 2009.

③ ETSI
- TS 102 165-1, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis
- TR 102 638, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions
- TR 102 893, Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)

④ OVERSEE
- D1.1 - Use Case Identification
- D1.4 - Functional Requirements Analysis

⑤ PRECIOSA
- D1 V2X Privacy Issue Analysis

⑥ sim^{TD}
- simTD D11.2 - Ausgewählte Funktionen

⑦ PRE-DRIVE：一般公開なし

⑧ SEVECOM

- D1.1 - VANETS Security Requirements

⑨ C2C-CC：詳細な公開資料無し

⑩ ITS-Forum

- 運転支援通信システムに関するセキュリティガイドライン ITS FORUM RC-009 1.0 版

2.1.3 想定するアーキテクチャの提案（調査項目①）

ここでは調査結果を基に想定するアーキテクチャを作成した。想定するアーキテクチャは Vehicle 内部のアーキテクチャと外部のアーキテクチャに分けられる。Vehicle 内部のアーキテクチャは特定の用途を想定せず、抽象的な特徴を表すことを目的として作成した。V2X Box は V2X の通信を行う装置である。その他の Vehicle 内部の装置は V2X Box との関係を基に分類している。Private ECU は V2X と他の ECU と排他的に V2X Box とつながったもので、V2X の GPS センサなどが例として挙げられる。Non-private ECU は V2X Box とつながっているが、その他の ECU ともつながっている様なものを表している。例えば、Non-private ECU には Sensor や OBD ポートなどが繋がっている。

外部のアーキテクチャを作成するために、各調査対象で考慮されている構成要素を列挙した。構成要素としては、Vehicle、RSU、ITS Service Center (Traffic management center)、Internet、Sensor、Nomadic device、Diagnosis device である。この内、Vehicle、RSU、ITS Service Center、Internet はどの調査対象においても考慮されている要素である。また、Nomadic device、Diagnosis device は基礎となるユースケースで現れる要素である。Sensor は歩行者や二輪車、V2X システム非搭載車を検知するための要素であるが、基礎となるユースケースに現れない装置である。以上より、基礎となるユースケースに必要となるもののみを Vehicle 外部のアーキテクチャとして採用した。

以上の様にして作成した想定アーキテクチャを図 2.1-1 に示す。

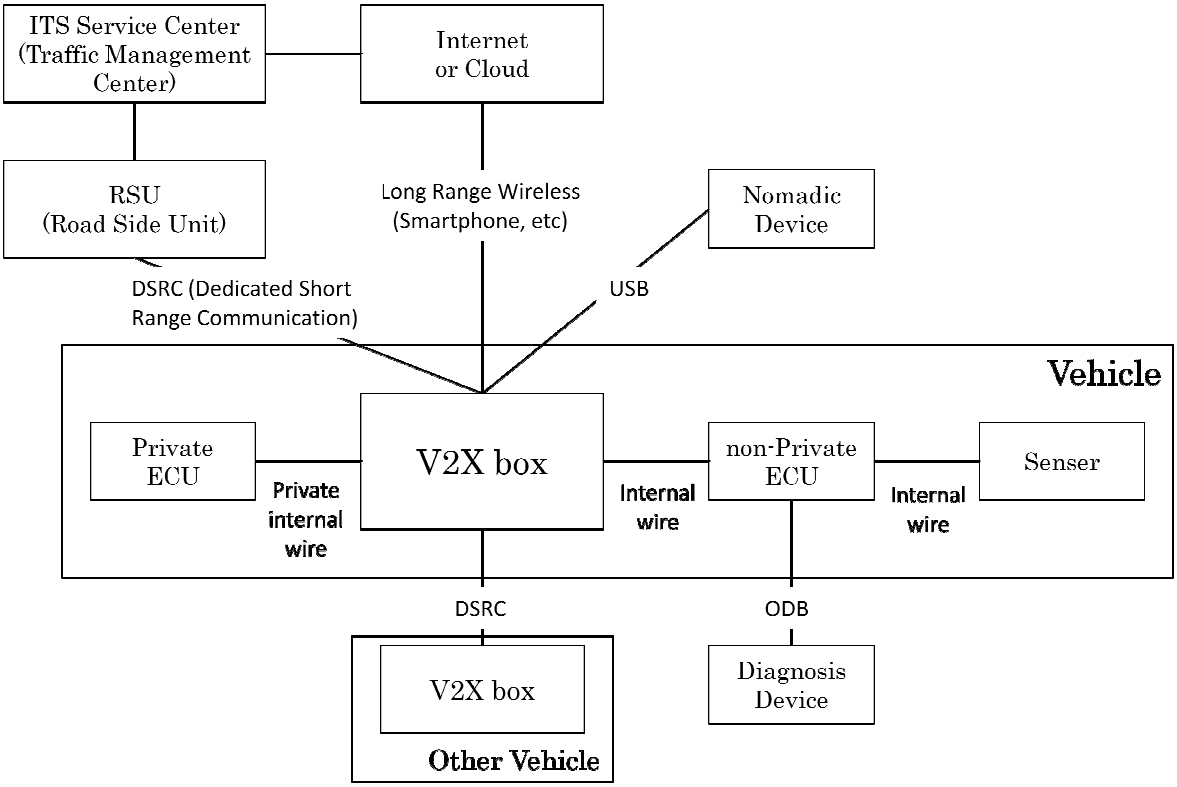


図 2.1-1　想定したアーキテクチャ

2.1.4　基礎となるユースケースの作成について（調査項目②）

本節では調査結果に基づいて統合された、基礎となるユースケースについて、その作成手順および統合結果を説明する。
基礎となるユースケースの作成手順は以下のとおりである。

手順1.　各プロジェクトの調査結果の比較。
手順2.　手順 1 の結果を基にすべてのユースケースを統合。
手順3.　統合結果より基礎となるユースケースを選定。

各手順について以下で説明する。

手順 1 では調査結果の比較表を作成した。比較表は、以下の理由から EVITA および ETSI を軸として作成した。EVITA に加え ETSI も軸の一つとしたのは、その機関の性質上、様々な他のプロジェクトでも参照されており、さらに広範囲を対象としており、ユースケースのカテゴリ分けもなされていることが理由である。

OVERSEE のユースケースには ETSI のユースケースとの対応関係が明記されているため、そのまま使用した。そのほかの関係は ETSI を参照しているなどの記述があるものの、明確にどのユースケースと対応するかの記載はなかった。そのため、ユースケースの詳細な内容にも踏み込んで対応関係を作成した。例えば、OVERSEE の「Safety Reaction: Active Brake」は ETSI の「Emergency electronic brake lights」および「Safety function out of normal condition warning」に対応していると記載されているが、その内容は OVERSEE ではブレー

キをかけるのに対し、ETSI では警告するにとどまっている。そのため、これらは別のユースケースとした(EVITA の「Safety Reaction: Active Brake」も同様)。このほかにも ETSI の「Across traffic turn collision risk warning」、ITS-Forum の「右折時衝突防止(V2I)」はともに対向車線を横切って曲がる際に対向車との衝突を警告するというものであるが、異なるユースケースとして扱っている。これは、ETSI では V2V 通信で行うのに対し、ITS-Forum では路側機からセンサで対向車を検知して行うためである。

この様にして作成されたユースケース比較表を参考資料 3）に示す。各プロジェクトのユースケースが縦に列挙され、プロジェクト間で関係するユースケースが横に並んでいる。もっとも左の列は統合されたユースケースである。

手順 2 では手順 1 で作成された比較表を基にユースケースを統合し統合ユースケース一覧を作成した。統合ユースケースは参考資料 4）の統合結果に記載されている。各ユースケース名は ETSI に関連するものは ETSI のものを使用し、EVITA にも対応する場合は EVITA での名前を[ ]内に付け加えている。また、ETSI に対応しないもので EVITA に対応する場合は EVITA の名前を採用している。そのほかのユースケースは全て唯一のユースケースからなるため、各プロジェクトでの名前を採用している。

ユースケースは ETSI で用いられているカテゴリに分類して記述している、カテゴリは Vehicle status warnings (自車の状態を他車へ警告)、Vehicle type warnings (緊急車両や二輪車など異なる種類の車両や歩行者に関する警告)、Traffic hazard warnings (渋滞など交通状況に関する警告)、Dynamic vehicle warnings (自車の動きに関する警告)、Collision risk warnings (交差点や右左折等の危険の警告)、Traffic efficiency (スピード制限などの様な交通法規に関する警告)、Others (その他、情報提供など)となっている。ただし、Active Brake を Others に関しては適切なカテゴリが ETSI に無かったため Vehicle control というカテゴリを作成した。また、統合結果には PRESERVE との対応関係、ETSI の BSA (Basic Set of Application) に対応するか否かも明記されている。

最後に手順 3 では統合ユースケースから基礎となるユースケースの選定を行った。選定は「ETSI の BSA に対応するユースケースである」または「EVITA に対応するユースケースである」という基準で行った。選定されたユースケースに関してはそれぞれの詳細を参考資料５）のユースケース詳細に記載している。また、統合されたユースケースのうち、運転者(同乗者など)への警告にとどまらず、何らかの制御(自動車そのものに限らず、ドア開閉なども含める)を行うものは、参考資料 2）のユースケース一覧で制御対象を記載している。

2.1.5 リスク見積もり方法の比較（調査項目③）

(1) EVITA

EVITA におけるリスクの特徴は、攻撃の結果の深刻度(severity)を 4 つの観点で見積もり、観点ごとに攻撃の容易さ(attack provability)と組み合わせ(ただし、安全性に関しては運転者による深刻度の低減可能性であるコントローラビリティ(controllability)も加える)リスクを

見積もることである。深刻度の 4 つの観点は、safety、privacy、financial、operational であり、以下の表 2.1-1 の様になっている。

表 2.1-1　EVITA の深刻度

脅威による結果の深刻度クラス	セキュリティ脅威のアスペクト			
	安全性 ：Ss	プライバシ: Sp	財務 ：Sf	運用 ：So
0	ケガなし	プライバシの侵害なし	財務的な被害なし	支障なし
1	軽傷	匿名情報のみ	低い損失	運行継続可能
2	重症	個人の特定	中程度の損失	短時間の運行停止
3	生命にかかわる	個人の追跡可能	多額の損失	長時間の運行停止
4	複数の生命にかかわる	複数の個人を追跡可能		運行不可能（長期間の）

(出典：EVITA Deliverable D2.3)

もう一つのパラメータである攻撃の容易さは elapsed time、expertise、knowledge of system、window of opportunity、equipment の要素で点数をつけその合計点から決定される(各要素の点数のつけ方は参考資料 1-a を参照)。点数から導かれる攻撃の容易さは表 2-1-2 の様に分類される。

表 2.1-2　EVITA の攻撃の容易さ

点数	Attack potential required to identify and exploit attack scenario	Attack probability　(reflecting relative likelihood of attack)
0-9	基本	5
10-13	基本の拡張	4
14-19	適度	3
20-24	高	2
≧0-	高を超えている	1

(出典：EVITA Deliverable D2.3)

また、Safety に関するリスクを見積もる際に使用されるコントローラビリティは表 2.1-3 に示す通りである。

表 2.1-3　EVITA のコントローラビリティ

分類	説明
C1	Despite operational limitations, avoidance of an accident is normally possible with a normal human response.
C2	Avoidance of an accident is difficult, but usually possible with a sensible human response.
C3	Avoidance of an accident is very difficult, but under favourable circumstances some control can be maintained with an experienced human response.
C4	Situation cannot be influenced by a human response.

(出典：EVITA Deliverable D2.3)

以上のパラメータを組み合わせリスクが決定される。リスク決定のマトリクスは Safety に関するものを表 2.1-4 にそれ以外を表 2.1-5 に示す。

表 2.1-4　EVITA の Safety に関するリスク決定マトリクス

Controllability	Safety Severity	Attack Probability				
		1	2	3	4	5
1	1	R0	R0	R1	R2	R3
	2	R0	R1	R2	R3	R4
	3	R1	R2	R3	R4	R5
	4	R2	R3	R4	R5	R6
2	1	R0	R1	R2	R3	R4
	2	R1	R2	R3	R4	R5
	3	R2	R3	R4	R5	R6
	4	R3	R4	R5	R6	R7
3	1	R1	R2	R3	R4	R5
	2	R2	R3	R4	R5	R6
	3	R3	R4	R5	R6	R7
	4	R4	R5	R6	R7	R7+
4	1	R2	R3	R4	R5	R6
	2	R3	R4	R5	R6	R7
	3	R4	R5	R6	R7	R7+
	4	R5	R6	R7	R7+	R7+

(出典：EVITA Deliverable D2.3)

表 2.1-5　EVITA の Safety 以外に関するリスク決定マトリクス

Ri		Attack probability				
(i ∈ {p,f,o})		1	2	3	4	5
深刻度	0	R0	R0	R0	R0	R0
	1	R0	R0	R1	R2	R3
	2	R0	R1	R2	R3	R4
	3	R1	R2	R3	R4	R5
	4	R2	R3	R4	R5	R6

(出典：EVITA Deliverable D2.3)

(2) ETSI

ETSI ではリスクを決定する際に攻撃の頻度（likelihood）と影響（impact）を用いる。頻度に関しては EVITA と同じ elapsed time、expertise、knowledge of system、window of opportunity、equipment の要素で点数をつけその合計点から決定される。ただし、EVITA の場合と点数のつけ方が若干異なるため注意が必要である(各要素の点数のつけ方は参考資料 1-b を参照)。点数から導かれる頻度は表 2.1-6 の様に分類される。

表 2.1-6　ETSI の頻度

点数	Vulnerability rating	Likelihood	
		Name	Value
0-2	No rating	Likely	3
3-6	Basic		
7-14	Moderate	Possible	2
15-26	High	Unlikely	1
＞26	Beyond high		

（出典：ETSI TS 102 165-1）

一方で影響は保護資産への影響(asset impact)と攻撃の強度(attack intensity)から決定される。各パラメータに割り振られた値(value)の和が影響の値(value)となる（ただし 3 を最大値とし、3 を超えるものは全て 3 にする）。以下に保護資産への影響と攻撃の強度の分類を表 2.1-7、表 2.1-8 にそれぞれ示す。

表 2.1-7　ETSI の保護資産への影響

Asset Impact	説明	Value
Low	The concerned party is not harmed very strongly; the possible damage is low.	1
Medium	The threat addresses the interests of providers/subscribers and cannot be neglected.	2
High	A basis of business is threatened and severe damage might occur in this context.	3

（出典：ETSI TS 102 165-1）

表 2.1-8　ETSI の攻撃の強度

Attack Intensity	Value
Single instance of attack	0
Moderate level of multiple instance	1
Heavy level of multiple instance	2

（出典：ETSI TS 102 165-1）

以上の様に与えられた頻度と影響の値(value)の積を取り、その結果が 9 または 6 の場合は Critical、4 または 3 の場合は Major、2 または 1 の場合は Minor というリスクになる。各リスクの説明は表 2-1-9 に示す。

表 2.1-9　ETSI のリスク

Risk	説明
Critical	The primary interests of the providers and/or subscribers are threatened and the effort required from a potential attacker's to implement the threat(s) is not high. Critical risks should be minimized with highest priority.
Major	Threats on relevant assets are likely to occur although their impact is unlikely to be fatal. Major risks should be handled seriously and should be minimized by the appropriate use of countermeasures.
Minor	No essential assets are concerned, or the attack is unlikely. Threats causing minor riskshave no primary need for counter measures.

（出典：ETSI TS 102 165-1）

(3) ITS-Forum

ITS-Forum におけるリスク見積もりは、ETSI の見積もり手法をベースに改良されたもので、攻撃者の動機を明確にパラメータとして採用しているのが特徴である。攻撃者の動機と攻撃の技術的困難さから発生可能性を決定する。動機、技術的困難さは表 2.1-10、表 2.1-11 それぞれに示すとおりであり、これらの値から表 2.1-12 のマトリクスに従い発生可能性を決定する。

表 2.1-10　ITS-Forum の動機

ランク	定義
High	攻撃する人や組織にとって多くの利益がある
Moderate	サービスの混乱(愉快犯等)
Low	あまり利益は得られない

（出典：ITS-Forum RC-009）

表 2.1-11　ITS-Forum の技術的困難さ

ランク	定義
None	技術的、経済的に容易に攻撃が可能(前例あり)
Solvable	理論的には攻撃が可能
Strong	理論的、技術的、経済的にも攻撃が大変困難

（出典：ITS-Forum RC-009）

表 2.1-12　ITS-Forum の発生可能性決定マトリクス

		動機		
		High	Moderate	Low
技術的困難さ	None	Likely	Likely	Unlikely
	Solvable	Likely	Possible	Unlikely
	Strong	Unlikely	Unlikely	Unlikely

（出典：ITS-Forum RC-009）

また、発生可能性の各レベルには、表 2.1-13 で示す様に値(value)が与えられる。

表 2.1-13　発生可能性と値

ランク	定義	値
Likely	全ての要素が存在する	3
Possible	いくつかの要素が存在する	2
Unlikely	重要な要素が抜けている	1

（出典：ITS-Forum RC-009）

一方で、攻撃の結果の影響も見積もる。攻撃の影響はサービスに対する影響として考慮され、三つのレベルに分類される（表 2.1-14）。

表 2.1-14　ITS-Forum の影響

ランク	定義	値
High	利用者やサービスに深刻な影響を与える	3
Medium	短期間のサービス停止に陥る	2
Low	利用者やサービスに影響を与える	1

（出典：ITS-Forum RC-009）

影響と発生可能性の値（value）の積を取り、その結果が 6 以上の場合は Critical （対策が必須）、4 の場合は Major（要注意）、3 以下の場合は Minor（早急な対策は不要）というリスクに分類される。

(4) リスク見積もり方法の考察

本節では調査したリスク見積もり手法を比較し、どの様な手法を検討すべきかについての考察を述べる。

リスク見積もりは攻撃（脅威）に対し、その深刻度と攻撃の可能性を見積もることで行われている。ただし、各手法、それぞれを決定するための要素が異なっている。
攻撃の可能性に関しては、どの手法も IEC 15408（Common Criteria）を基にしている様に思われる（ITS-Forum については非常に簡略化されている）。これに、ITS-Forum では攻撃者の動機という面を明確に付け加えている。
一方で深刻度は各手法で異なる。もっとも大きな違いは EVITA では 4 つの観点について考慮され、その中に safety があることである。それぞれの観点はトレードオフの関係になる可能性があると考えられるため、その様な場合の考慮に有用であると思われる。
また、EVITA においては ISO 26262 や MISRA Safety Analysis Guidelines に現れるコントローラビリティという概念を取り入れている点も大きな違いである。これは、機能安全との関係を考える際に重要な要素となりうる可能性がある。

以上のことから、現状では EVITA を基に ETSI で考えられている Attack Intensity や ITS-Forum の攻撃者の動機といった概念を加えていくことを検討するのが良いのではないかと考えられる。

ただし、EVITA において分析されている Safety は、Security に原因があるものしか考慮されていない。そのため自動運転システムなどの分析を実施するためには、広範囲に Safety と Security の関係を考慮する必要があると考えられ、そのための分析手法やメトリクスの検討が必要になる。

2.1.6 まとめと今後の課題について

本案件では、欧州を中心に V2X システムのセキュリティに関するプロジェクトの前提条件を調査・統合し、今後セキュリティの分析を実施する際の基礎となる前提条件の提案を行った。また、セキュリティのメトリクスとしてどの様な手法を用いているか調査し、その比較を行った。

前提条件は現状では十分なものとなっていると考えられるが、そのほとんどが運転者や同乗者への警告を行うというものであり、自動車の制御例は多くない。しかし、今後、V2X システムは自動運転を実現する方向へ進むと考えられる。そのため、制御に関与するユースケースの検討が必要になってくる。また、V2X システムを搭載していない車、二輪車、歩行者などの対処も検討事項である。一つの方法としては、すでに ITS-Forum ではユースケースとして、センサによる検知と、I2V 通信で車両に送信を考慮している。また、ETSI においても、検討が始まっているとのことである。以上の様に今後の V2X システムのセキュリティを考慮するためには、前提条件のレベルにおいても再検討が必要である。

本案件で調査したものはこれまでに実施されてきた V2X システムのセキュリティに関するプロジェクトである。そこでは、TVRA (Threat Vulnerability, and Risk Analysis)や Attack Tree などの手法が用いられセキュリティの分析が行われていた。しかし、現状では安全分析における FTA、FMEA、HAZOP といった分析手法の様に、セキュリティ分析のデファクトとなる手法が存在していない。

また、現在の対象システムは V2X 通信を用いて運転者に対し危険を警告するということが主とした目的であり、制御に関与する物は非常に少ない。しかし、今後のシステムは自動運転へと進んでいくため、これまで以上に安全性との関連の考慮が重要になってくる。様々な分野で試みられている、安全性とセキュリティの双方を分析する際のアプローチとしては、

・各々を別のものとして分析し、結果を基にトレードオフを考慮する
・攻撃も故障の一部として取扱う
・安全性を脅かす要因として攻撃を考慮する

といったものがある。自動運転システムの分析を実施する際にどの様なアプローチが適切であるかの検討は非常に重要になると考えられる。

今後、以上の様な課題を解決し安全性とセキュリティの相互影響を考慮した分析が可能となる手法を開発と普及が必要となる。そのために、現状の分析プロセス、手法の調査を

行い、自動運転システムの安全性との関連を考慮した脅威分析を実施する際の問題点を洗い出し、その調査を基に安全性との関係を考慮した自動運転システムの脅威分析を行うためのプロセス並びに手法を確立し、ツール化を行う必要があると考えられる。

2.2 セキュリティ技術のあり方の検討

V2X セキュリティ技術のあり方について、V2X セキュリティ検討 WG に報告し、議論を行った。現状は V2X システムをドライバへの情報提供に使うことを前提に、日米欧で実用化に向けた取組みが進められているところであり、V2X システムを次世代高度運転支援で考えられている車両制御に用いるための検討については、欧米での活動はまだ本格化していないと見られる。

そこで本検討 WG では、今後の V2X システムに係るセキュリティ技術の開発・研究・実用化に向けて、以下の通り 5 つの面から検討を行った。

・現状で性能未達になっているハードウェアの技術開発
・欧米で継続議論中のインフラ等の技術課題に関する研究
・情報提供レベルから、自動運転に応用する際に追加で検討すべき事項
・標準化に対する取組み
・V2X システムの製品化における認証のあり方

2.2.1 現状で性能未達になっているハードウェアの技術開発

自動運転に対応したセキュリティレベルは、現状の情報提供で求められるレベルに比べて、より高いレベルが求められると推測される。一方、現在の現実的なコストで実現出来るハードウェアでは PRESERVE の要求仕様を満たすことは難しい状況である。

また、既に暗号長の 256bit から 384bit への拡張や、Brainpool との並行使用の提案があるなど、ハードウェアの高機能化への要求も高くなっていくと考えられる。ただし、ハードウェア、特に半導体の部分は微細化することにより、性能の向上や、並列処理数の増加などが可能とも考えられる。まずは、2.2.3 で後述するセキュリティに求められる要件により、どういったレベルの技術が必要になるかを見極めることが重要と考える。

2.2.2 欧米で継続議論中のインフラ等の技術課題に関する研究

本事業による調査では、ドライバへの情報提供レベルであって、主にインフラ側に関わる実際の運用については決まっていない項目がいくつかある。そのうちのセキュリティ技術に関連する主な項目は、プライバシ保護のあり方に関連して、一時証明書や偽名証明書などの証明書をどう運用するかという点と、ハードウェアの性能未達をカバーするための署名検証の簡略化技術、Misbehavior の検出方法の 3 点である。

これらの仕組みは一旦出来上がると、V2X システムを自動運転に応用する際にも、検出感度の向上等はあるものの、基本的な枠組みはそのまま使われるものと想定される。これ

らの枠組みは現在の日本の V2X システムのインフラ側のものとは異なるため、国内では議論されていなかった分野と考えられる。

将来的に、日本で自動運転を実用化する際に、こういった仕組みの導入が必要となるかどうかの検討も含めて、技術的には検討する価値のあるテーマと考えられる。また、Misbehavior の検出に関しては欧米共通の課題であり、この部分で日本が技術的に貢献出来る可能性があると考えられる。

2.2.3 情報提供レベルから、自動運転に応用する際に追加で検討すべき事項

ドライバへの情報提供に用いられるレベルのセキュリティに求められる要件等については、既に日米欧のプロジェクトで検討された結果が、全てではないが WEB 上等に公開されている。これらの事例調査から、ユースケースとして使用されているものには、車両制御に関連するものはほとんど含まれていないこと、また、アーキテクチャについても自動運転に対応したものではないという結果が得られている。

そこで、自動運転を想定した場合に追加すべきユースケース、および自動運転に対応したアーキテクチャの検討を行い、これらのインプットを整理した上で脅威分析を実施することで、自動運転に対応したセキュリティに求められる要件を導き出すことが出来る。ただし、V2X システムの自動運転応用では、V2X システムから車両の制御系に何らかの入力が行われることと、無線通信の利用では通信の品質劣化や途絶なども起こりえることから、制御系で用いられている機能安全の考え方を入れることが必須と考えられる。

また、セキュリティの分析手法には様々なものが存在しており、デファクトとなるものも存在していない。V2X 通信に関するプロジェクトでは、これまで TVRA や Attack Tree を用いた脅威の同定・分析が行われてきている。しかし、自動運転を想定した場合、現状の分析手法では不十分となる可能性がある。

そこで、まず現状の分析プロセス、手法の調査を行い、自動運転システムの機能安全との関連を考慮した脅威分析を実施する際の問題点の洗い出しを行うべきである。さらに、その調査を基に機能安全とセキュリティの関係を考慮した自動運転システムの脅威分析を行うためのプロセス・手法を確立し、ツール化を行い、これらを用いた脅威分析を実施することで、V2X システムに係るセキュリティに求められる要件を明確化することが必要である。

2.2.4 標準化に対する取組み

上記の様な研究・開発を行った場合、その成果を標準や規格に反映させていくことが重要である。V2X システムに係るセキュリティ技術の標準化における課題の一つは、日本と欧米とで V2X システムに適用される技術が異なっているため、国内において欧米で適用される技術に関して議論する場がないことである。

そのため、標準化への対応については、現状個別企業の努力に任されており、実際に一部企業は欧米で行われているプロジェクトに個別に参画している。とはいえ、個別企業で

対応する場合には、それぞれが手掛ける事業が路側機や車載機、半導体であったりと事業範囲が限られているため、欧米で議論されている様なインフラ側のシステムや運用といった部分まで含めた全体の議論に十分に対応出来ているか、という点で課題があると考えている。

もし、国内で標準や規格に関する議論を行ったとしても、どの様な形で提案するかという課題が残る。V2X システムに関しては、EU/US Harmonization が行われ、日本もオブザーバとして参加しているが、日本で使わない技術の部分であれば、日本の標準・規格として制定されるものでなく、これを日本案として海外向けに提案することは難しいと考えられる。現状では、こうしたケースに対応する方法は明確ではなく、我が国のサプライヤが保有する技術を、どうやって標準化・規格化に結び付けるかは今後の課題と考えられる。

また、我が国のサプライヤの技術を海外にも展開出来る様にするためには、セキュリティ技術に関する議論・提案が行える体制の構築に加え、欧米におけるセキュリティ仕様等の情報を早期に入手することが必要である。議論・提案が行える体制はまた、欧米のプロジェクトの動向を把握し、情報共有する仕組みとして構築することが有効であると考えられる。

2.2.5 V2X システムの製品化における認証のあり方

標準化・規格化に近い部分でのもう一つの課題が認証である。V2X システムで適用が考えられる認証は 2 通りあり、CC (Common Criteria)認証とモジュール認証である。CC 認証では、セキュリティ機能の耐タンパ性を試験しており、モジュール認証では、ある機器が他の機器との相互接続性を試験するものである。現在、V2X システムはドライバへの情報提供を前提としているため、CC 認証は不要と考えられているが、V2X システムを自動運転へ応用する場合には、CC 認証あるいは代替するものが必要になることが推測される。

これらの認証で適用されるレベルが過剰に厳しい場合は、コスト増の要因になるため、適正なレベル設定が重要であり、また、どこで認証試験を行うことが出来るかという点も今後の事業展開に影響を及ぼす可能性のある項目である。

CC 認証については、適用されるレベルと、実際に認証を取得する必要のあるデバイスに関し、欧米でもまだ議論は進んでいないため、適正なレベルに関しては提案の余地がある部分でもある。また、セキュリティ仕様の違いはあるものの、日本の V2X システムとで同じ考え方を適用出来る可能性もあり、早期に検討を進めることが重要である。

また、これらの認証試験を国内で行える様にするために、どの様に進めるかについても合わせて検討する必要がある。

2.3　まとめと今後の課題

V2X システムのセキュリティに関して、欧州のプロジェクト等で実施された脅威分析関連のドキュメントから、脅威分析の前提として用いられた条件について調査した。調査対象となったプロジェクトでは、いずれもドライバへの情報提供・警告の用途を想定した前提条件が設定され、脅威分析が行われていた。また、リスク見積り方法も異なるケースもあり、デファクトが確立していない状況である。また、一部では機能安全と組合せているケースもあった。

今後、V2X システムを自動運転、あるいは制御応用に活用する場合には、システムのアーキテクチャも変わる可能性と､ユースケースも追加すべき事項があることが想定される。また、自動運転の場合には、制御に応用することから、機能安全と組合せての脅威分析が必須となる。また、リスク見積り方法も、これまでのプロジェクトで使われたものが最適かどうか、検討することが必要である。

V2X システムに係るセキュリティ技術のあり方として、現状の課題、自動運転の実現に向けた次の課題、V2X システムの実用化における周辺の課題を解決することが重要と考えた。V2X セキュリティ検討 WG では、海外のプロジェクトの結果や進捗状況の調査結果から、これらを 5 つ（ハードウェアの技術開発、インフラ等の技術課題、自動運転に対応するための追加検討事項、標準化、製品化における認証のあり方）に分けて、それぞれについて、どういったことを進めていくべきかの検討を行った。

現状の課題としては、ハードウェア等でのセキュリティ処理の性能向上、インフラ等のセキュリティ技術の運用に関する部分の研究、の 2 つがあり、後者については、欧米の動向等にも注視しつつ、研究を進めるべき分野とした。自動運転の実現に向けた次の課題としては、自動運転への適用を行うためにセキュリティ技術に求められる要件とは何か、アーキテクチャやユースケースの見直しを行い、脅威分析による要件の明確化を行うべきとした。V2X システムの実用化における周辺の課題として、標準化に対する取組み、認証の仕組み作り、について検討した。

標準化に取組む体制をどの様に構築するかは大きな課題であるが、まずは、標準化に向けた認識を共有した上で、海外でのプロジェクトに関する情報を効率的に収集し、共有することが出来る仕組みを作りが非常に重要である。

おわりに

本調査事業は、日本自動車研究所が有しているサプライヤ等とのネットワークにより、欧米の V2X システムにかかるセキュリティを扱うプロジェクトの責任者等へのヒアリング調査を実施出来、また、セキュリティ仕様を策定する際に用いられた脅威分析の前提条件や手法がどういうものであるかを整理した。

これらの調査により得られた知見を元に、V2X システムにかかるセキュリティ技術を開発するためのあり方として提案をまとめた。

今回の調査事業は、同じ様な製品でありながら、日本と海外とで仕様が全く異なる場合に、海外での規格化・標準化に対して、個別の企業や団体等が議論に参加するだけで良いのか、あるいは日本として何らかの意見を取り纏めて対応すべきであるのか、といったことを議論する必要があると考えられる。

参考資料

1）先行プロジェクトの調査結果

1-1 保護すべき情報資産

1-2 リスク見積り方法

2）ユースケース一覧

3）ユースケースの比較表

4）ユースケースの統合結果

5）ユースケース詳細

6）自動化レベルとユースケースの紐付けについて

1）先行プロジェクトの調査結果

1-1　保護すべき情報資産

＜EVITA＞

Privacy、Safety、Financial、Operational という側面からセキュリティが考慮されている。Safety に関してはその多くが運転者、同乗者への警告にとどまっている。

＜ETSI＞

Privacy と情報の Confidentiality, Integrity, Availability を対象としている。非常に広範囲を対象としている。

＜OVERSEE＞

複数の独立した V2X アプリケーションの情報の Confidentiality, Integrity, Availability を対象としている。

＜PRECIOSA＞

Privacy と情報の Confidentiality, Integrity, Availability を対象としているが、特に Privacy に重点が置かれている。

＜SEVECOM＞

Privacy、Safety と情報の Confidentiality, Integrity, Availability を対象としている。Safety に関しては明記してはいない。

＜ITS-Forum＞

Safety に関しての情報を対象としている。センサによる歩行者検知などセンサ情報も考慮されている。詳細な通信情報が定義されている。通信経路で路側機と車載機の通信はその送受信の方向も考慮し、路側機から車載機へ送信する場合は路車間通信、車載機から路側機へ送信する場合は車路間通信と記載している。

1-2　リスク見積もり方法

＜EVITA＞

リスクはSafety、Privacy、Financial、Operationalの4つの側面に対し見積もられる。Privacy、Financial、Operational に関してはAttack potentialとSeverity、から決定され、Safetyに関してはこれにControllabilityを加えて決定される(参照：Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios)。

SeverityはSafety、Privacy、Financial、Operationalそれぞれについて算出される。Attack PotentialはElapsed time、Expertise、Knowledge of system、Window of Opportunity、

Equipmentという観点から点数付され、その合計点で決定される。これはISO/IEC 15408 (Common Criteria)を基にして作成されている。

＜ETSI＞

リスクは likelihood と impact から決定される。Elapsed time、Expertise、Knowledge of system、Window of Opportunity、Equipment に対し点数付され、その合計点で Vulnerability rating が決定される。この Vulnerability rating から likelihood が決定される。Impact は Asset impact と Attack intensity から決定される。

＜OVERSEE＞

ETSI を参照しているが、明確には記載されていない。

＜PRECIOSA＞

不明

＜SEVECOM＞

ユースケースに対し脅威の Motivation、Target、Attacker の Skill、Technical effort、Risk が見積もられているが、その間の関係については明確にされていない。一方で、各 Use Case ごとに複数の Attack Use Case が検討されており、これに対しては攻撃対象や攻撃方法が詳細化され、その Severity が見積もられている。

＜ITS-Forum＞

以下の文献にある方法（ETSI の手法を改良したもの）を使用。

C. Laurendeau and M. Barbeau, “Threats to Security in DSRC/WAVE,” ADHOC-NOW Lecture Notes in Computer Science, Volume 4104, 2006, page 266-279.

リスクは発生可能性と影響で見積もる。発生可能性は動機と技術的困難さから見積もる。

2）ユースケース一覧

ユースケース ID	ユースケース名	基礎となるユースケース	制御対象
UC-1	Safety reaction: Active brake	✓	ブレーキ
UC-2	Emergency electronic brake lights [Messages lead to safety reaction]	✓	なし
UC-3	Safety function out of normal condition warning [Messages lead to safety reaction]	✓	なし
UC-4	Emergency vehicle warning	✓	なし
UC-5	Slow vehicle warning	✓	なし
UC-6	Motorcycle warning	✓	なし
UC-7	Vulnerable road user Warning		なし
UC-8	左折時衝突防止(V2V)		なし
UC-9	左折時衝突防止(V2I)		なし
UC-10	追突防止(V2I)		なし
UC-11	Wrong way driving warning	✓	なし
UC-12	Stationary vehicle warning	✓	なし
UC-13	Traffic condition warning	✓	なし
UC-14	Signal violation warning	✓	なし
UC-15	Roadwork warning	✓	なし
UC-16	Decentralized floating car data	✓	なし
UC-17	一時停止規制見落とし防止(V2I)		なし
UC-18	Overtaking vehicle warning		なし
UC-19	Lane change assistance		なし
UC-20	Pre-crash sensing warning		なし
UC-21	Co-operative glare reduction		✓(ヘッドライト)
UC-22	Across traffic turn collision risk warning		なし
UC-23	Merging Traffic Turn Collision Risk Warning		なし
UC-24	Co-operative merging assistance		なし
UC-25	Hazardous location notification		なし
UC-26	Intersection Collision Warning [Local Danger Warning from other Cars and to other Car]	✓	なし
UC-27	Co-operative forward collision warning		なし
UC-28	Collision Risk Warning from RSU		なし
UC-29	右折時衝突防止(V2I)		なし
UC-30	出会い頭衝突防止(V2I)		なし
UC-31	Regulatory/contextual speed limits	✓	なし
UC-32	Traffic light optimal speed advisory	✓	なし
UC-33	Traffic information and recommended itinerary [Traffic Information from other Entities and to other Entities]	✓	なし
UC-34	Enhanced route guidance and navigation	✓	なし
UC-35	Intersection management		なし
UC-36	Co-operative flexible lane change		なし

UC-37	Limited access warning, detour notification	✓	なし
UC-38	In-vehicle signage	✓	なし
UC-39	Electronic toll collect　[eTolling]		なし
UC-40	Co-operative adaptative cruise control		ブレーキ、アクセル
UC-41	Co-operative vehicle-highway automation system (Platoon)		ブレーキ、アクセル、ハンドル
UC-42	Point of interest notification　[Point of Interest]	✓	なし
UC-43	Automatic access control/parking access	✓	なし
UC-44	Local electronic commerce	✓	なし
UC-45	Car rental/sharing assignment/reporting		なし
UC-46	Media downloading	✓	なし
UC-47	Map download and update		なし
UC-48	Ecological/economical drive		なし
UC-49	Instant messaging		なし
UC-50	Personal data synchronization		なし
UC-51	SOS service　[eCall]	✓	なし
UC-52	Stolen vehicle alert		なし
UC-53	Remote diagnosis and just in time repair notification　[Remote Diagnosis]	✓	なし
UC-54	Vehicle relation management		なし
UC-55	Vehicle data collect for product life cycle management		なし
UC-56	Insurance and financial Services	✓	なし
UC-57	Fleet management	✓	なし
UC-58	Vehicle software/data provisioning and update　[Remote Flashing and Flashing per OBD]	✓	なし
UC-59	Loading zone management	✓	なし
UC-60	Vehicle and RSU data calibration	✓	なし
UC-61	Personalize the car	✓	シート位置など
UC-62	Car Finder (e.g., via mobile phone)		なし
UC-63	Electronic License Plate		なし
UC-64	Remote Car Control (e.g. door opener)	✓	ドアなど
UC-65	Pay as You Drive (Road Safety & Eco)		なし
UC-66	Install applications	✓	なし
UC-67	Parking Sensor System		なし
UC-68	Electronic Driver Logbook		なし
UC-69	Secure Integration	✓	なし
UC-70	Replacement of Engine ECU	✓	なし
UC-71	Installation Car2x Unit	✓	なし
UC-72	Booking a Hotel on the Road		なし
UC-73	Combination of the "Calculating Route from Current Position to Home" and "Booking a Hotel on the Road"		なし
UC-74	Road Surface Conditions to TOC		なし

3）ユースケースの比較表

統合した ユースケース	ETSI	OVERSEE	EVITA	PRECIOSA	SEVECOM	ITS-Forum	備考
UC-1		OVERSEE-9	EVITA-1				←EVITA：Active Brake は ETSI とはずれている様に思われる。しかし、OVERSEE での Active Brake が ETSI1,2 と対応していると明記されているため、この様にしている。
UC-2	ETSI-1	OVERSEE-9	EVITA-1?				同上
UC-3	ETSI-2	OVERSEE-9	EVITA-4				
UC-4	ETSI-3	OVERSEE-6			SEVECOM-9	ITS-F-6	
UC-5	ETSI-4	OVERSEE-6				ITS-F-5	←ITS : ETSI は見通しが悪いところに限らないが一致しているとして良いか？
UC-6	ETSI-5	OVERSEE-6					
UC-7	ETSI-6	OVERSEE-6			SEVECOM-4	ITS-F-11	
UC-8						ITS-F-1	
UC-9						ITS-F-9	
UC-10						ITS-F-10	
UC-11	ETSI-7						
UC-12	ETSI-8					ITS-F-5	
UC-13	ETSI-9					ITS-F-5	←ITS：交通情報は明記されていないが、含まれると考えられる。また、ETSI は見通しが悪いところに限らないが一致しているとして良いか？
UC-14	ETSI-10					ITS-F-12	
UC-15	ETSI-11				SEVECOM-10		
UC-16	ETSI-12			PRECIOSA-1			
UC-17						ITS-F-13	
UC-18	ETSI-13	OVERSEE-5					
UC-19	ETSI-14	OVERSEE-6					
UC-20	ETSI-15	OVERSEE-7					
UC-21	ETSI-16	OVERSEE-8					
UC-22	ETSI-17					ITS-F-2	
UC-23	ETSI-18						
UC-24	ETSI-19						
UC-25	ETSI-20				SEVECOM-5		
UC-26	ETSI-21		EVITA-2, EVITA-5	PRECIOSA-2	SEVECOM-4	ITS-F-3, ITS-F-4	
UC-27	ETSI-22						
UC-28	ETSI-23						
UC-29						ITS-F-8	
UC-30						ITS-F-7	
UC-31	ETSI-24						
UC-32	ETSI-25						
UC-33	ETSI-26	OVERSEE-8	EVITA-3, EVITA-6				
UC-34	ETSI-27	OVERSEE-13		PRECIOSA-3			
UC-35	ETSI-28						
UC-36	ETSI-29						
UC-37	ETSI-30				SEVECOM-10		
UC-38	ETSI-31						

UC-39	ETSI-32	OVERSEE-1	EVITA-7				
UC-40	ETSI-33						
UC-41	ETSI-34						
UC-42	ETSI-35		EVITA-10				
UC-43	ETSI-36	OVERSEE-3					
UC-44	ETSI-37						
UC-45	ETSI-38	OVERSEE-18					
UC-46	ETSI-39						
UC-47	ETSI-40				SEVECOM-3		
UC-48	ETSI-41						
UC-49	ETSI-42	OVERSEE-21					
UC-50	ETSI-43	OVERSEE-4					
UC-51	ETSI-44	OVERSEE-2	EVITA-8		SEVECOM-1		
UC-52	ETSI-45	OVERSEE-7			SEVECOM-2		
UC-53	ETSI-46	OVERSEE-14	EVITA-16				
UC-54	ETSI-47						
UC-55	ETSI-48						
UC-56	ETSI-49						
UC-57	ETSI-50						
UC-58	ETSI-51		EVITA-17, EVITA-18		SEVECOM-8		
UC-59	ETSI-52						
UC-60	ETSI-53						
UC-61		OVERSEE-10	EVITA-13				
UC-62		OVERSEE-11					
UC-63		OVERSEE-12			SEVECOM-6		
UC-64		OVERSEE-15	EVITA-9				
UC-65		OVERSEE-16					
UC-66		OVERSEE-17	EVITA-11				
UC-67		OVERSEE-19					
UC-68		OVERSEE-20					
UC-69			EVITA-12				
UC-70			EVITA-14				
UC-71			EVITA-15				
UC-72				PRECIOSA-4			
UC-73				PRECIOSA-5			
UC-74					SEVECOM-7		

4）ユースケースの統合結果

ユースケースID	ユースケースカテゴリ	ユースケース名	他プロジェクトのとの対応							
			EVITA	ETSI		PRESERVE	OVERSEE	PRECIOSA	SEVECOM	ITS-Forum
				BSA	BSA 以外					
UC-1	Vehicle controll	Safety reaction: Active brake	✓				✓			
UC-2	Vehicle status warnings	Emergency electronic brake lights [Messages lead to safety reaction]	✓	✓		✓	✓			
UC-3		Safety function out of normal condition warning [Messages lead to safety reaction]	✓		✓		✓			
UC-4	Vehicle type warnings	Emergency vehicle warning		✓			✓		✓	
UC-5		Slow vehicle warning		✓		✓	✓			✓
UC-6		Motorcycle warning		✓		✓	✓			
UC-7		Vulnerable road user Warning			✓		✓		✓	✓
UC-8		左折時衝突防止(V2V)								✓
UC-9		左折時衝突防止(V2I)								✓
UC-10		追突防止(V2I)								✓
UC-11	Traffic hazard warnings	Wrong way driving warning		✓		✓				
UC-12		Stationary vehicle warning		✓		✓				✓
UC-13		Traffic condition warning		✓		✓				✓
UC-14		Signal violation warning		✓		✓				✓
UC-15		Roadwork warning		✓		✓			✓	
UC-16		Decentralized floating car data		✓		✓		✓		
UC-17		一時停止規制見落とし防止(V2I)								✓
UC-18	Dynamic vehicle warnings	Overtaking vehicle warning			✓		✓			
UC-19		Lane change assistance			✓		✓			
UC-20		Pre-crash sensing warning			✓		✓			
UC-21		Co-operative glare reduction			✓		✓			
UC-22	Collision Risk Warning	Across traffic turn collision risk warning			✓					✓
UC-23		Merging Traffic Turn Collision Risk Warning			✓					
UC-24		Co-operative merging assistance			✓					
UC-25		Hazardous location notification			✓	✓			✓	
UC-26		Intersection Collision Warning [Local Danger Warning from other Cars and to other Car]	✓	✓		✓		✓	✓	✓
UC-27		Co-operative forward collision warning			✓					
UC-28		Collision Risk Warning from RSU			✓	✓				
UC-29		右折時衝突防止(V2I)								✓
UC-30		出会い頭衝突防止(V2I)								✓
UC-31	Traffic Efficiency	Regulatory/contextual speed limits		✓		✓				
UC-32		Traffic light optimal speed advisory		✓		✓				
UC-33		Traffic information and recommended itinerary [Traffic Information from other Entities and to other Entities]	✓	✓		✓	✓			
UC-34		Enhanced route guidance and navigation		✓		✓	✓	✓		

UC-35		Intersection management			✓					
UC-36		Co-operative flexible lane change			✓					
UC-37		Limited access warning, detour notification		✓		✓			✓	
UC-38		In-vehicle signage		✓		✓				
UC-39		Electronic toll collect [eTolling]	✓		✓	✓	✓			
UC-40		Co-operative adaptative cruise control			✓					
UC-41		Co-operative vehicle-highway automation system (Platoon)			✓					
UC-42	Others	Point of interest notification [Point of Interest]	✓	✓		✓				
UC-43		Automatic access control/parking access		✓		✓	✓			
UC-44		Local electronic commerce		✓		✓				
UC-45		Car rental/sharing assignment/reporting			✓		✓			
UC-46		Media downloading		✓		✓				
UC-47		Map download and update			✓				✓	
UC-48		Ecological/economical drive			✓					
UC-49		Instant messaging			✓		✓			
UC-50		Personal data synchronization			✓		✓			
UC-51		SOS service [eCall]	✓		✓	✓	✓		✓	
UC-52		Stolen vehicle alert			✓		✓		✓	
UC-53		Remote diagnosis and just in time repair notification [Remote Diagnosis]	✓		✓		✓			
UC-54		Vehicle relation management			✓					
UC-55		Vehicle data collect for product life cycle management			✓					
UC-56		Insurance and financial Services		✓		✓				
UC-57		Fleet management		✓		✓				
UC-58		Vehicle software/data provisioning and update [Remote Flashing and Flashing per OBD]	✓	✓		✓			✓	
UC-59		Loading zone management		✓		✓				
UC-60		Vehicle and RSU data calibration		✓		✓				
UC-61	—	Personalize the car	✓				✓			
UC-62		Car Finder (e.g., via mobile phone)					✓			
UC-63		Electronic License Plate				✓	✓		✓	
UC-64		Remote Car Control (e.g. door opener)	✓			✓	✓			
UC-65		Pay as You Drive (Road Safety & Eco)					✓			
UC-66		Install applications	✓				✓			
UC-67		Parking Sensor System					✓			
UC-68		Electronic Driver Logbook					✓			
UC-69		Secure Integration	✓							
UC-70		Replacement of Engine ECU	✓							
UC-71		Installation Car2x Unit	✓							
UC-72		Booking a Hotel on the Road						✓		
UC-73		COMBINATION OF THE “CALCULATING ROUTE FROM CURRENT POSITION TO HOME” AND “BOOKING A HOTEL ON THE ROAD”						✓		
UC-74		ROAD SURFACE CONDITIONS TO TOC							✓	

5）ユースケース詳細

UC-1	
Name	Safety reaction: Active brake
Communication Parties	Vehicle
Use Case Scenario	The car receives a message that indicates that the car is in immediate danger of collision with an object. The only way to avoid the collision is an instant brake manoeuvre. Remark: The source of the message is described in detail in Section 3.6. The emergency message contains longitude, latitude and altitude of the dangerous object, the time of message generation, the expiry time of the message, an indicator for the reliability of the information, a code that is classifying the object, an Id that is identifying the sender of the message and an event code that is classifying the emergency situation. All this information is packed in a message frame that adds checksum, information for protocol processing and if necessary security information. The receiving communication unit (CU) will check the message for correctness and then pass the information together with additional relevant information to the chassis safety controller (CSC). The additional information consists of data about the position, speed, heading, type and size of communicating objects nearby; further attributes may also be added. The additional information was collected from older received messages and stored in the neighbourhood table. The neighbourhood table is a list of communication nodes from which the CU received messages in the past. The list contains the nodes Id, position, type and other available attributes. Nodes that are more than 1 km distant will be deleted from the list. The information is provided in regular intervals (ca. 2/s). In parallel to the following action, the CU will assess whether it has to send the information out to other nodes. The assessment depends on the position of nearby CUs, the received RF power of the message and the type of the message. Only event messages will be rebroadcast. If it is obvious that all affected units that are even further away from the sender have received the same message, the message will not be rebroadcast, otherwise it is sent out again. The GPS unit of the CU is used to determine the position; this position is used internally and for car2X communication. The CSC will use further information that is available to perform a plausibility check. This information may be object lists from radar, lidar or video sensors together with data from digital maps, driver status information and status data of the car like position, speed, heading, steering angle etc. Except for the car status all these data sources are optional. If the plausibility check confirms the danger for the car, the CSC decides on appropriate action, which mainly depends on the possibilities that the vehicle dynamics and the neighbourhood conditions permit. If the CSC decides that a

	braking manoeuvre is the best solution, it will send a braking command and information concerning the best deceleration to the brake control unit. In addition, information about the emergency-braking manoeuvre will be sent to the CU. The CU will then broadcast an emergency braking message to warn following cars. The brake control unit (BCU) will adjust the braking mechanics to get a deceleration as close as possible to the desired value, while keeping the car in a controllable state by executing ABS/TCS/ESC algorithms. When starting the braking, the BCU will send a message to the powertrain domain to reduce the driving power. This message is forwarded by the CSC and the Powertrain controller (PTC). The PTC will decide how best to comply with this request and will send the necessary commands to the units of the powertrain domain. The CSC will update the plausibility check and the concluding braking commands in regular intervals (ca. 10/s). The braking commands will be adapted to the situation assessment. When the CSC gets information from environmental sensors (radar, lidar, video) and/or car internal sensors (digital map, speed, yaw rate, etc.) that show that the dangerous situation is no longer existent or that the driver is fully able and ready to cope with the danger, it returns control to the driver by adapting the deceleration to the braking pedal pressure.

UC-2	
Name	Emergency electronic brake lights [Messages lead to safety reaction]
Communication Parties	Vehicle
Use Case Scenario	In order to avoid critical driving situations, car2X communication helps to virtually extend the view of the driver. The driver can be warned in critical situations, where an obstacle may be overseen, e.g. intersection warnings based on communication. This kind of application will reduce the number of fatalities. The communication of local danger warning messages is based on “Cooperative Awareness Messages” CAM and “Decentralized Environmental Notifications” (DEN) specified by the C2C-CC. Within Cooperative Awareness Messages, data is periodically broadcast, e.g. in order to prevent accidents at an intersection. Decentralized environmental notifications provide more specific information about an occurrence, e.g. to indicate a potential danger to other vehicles such as a car with warning lights on. The car that receives the messages processes the information and provides the driver a corresponding warning.

UC-3	
Name	Safety function out of normal condition warning [Messages lead to safety reaction]
Communication Parties	Vehicle
Use Case Scenario	When a dangerous situation occurs that forces the driver, or the car itself, to perform a manoeuvre, this can endanger other vehicles. In order to warn other vehicles, the car sends out a warning message. Nearby cars that are in danger can then react according to the information provided within the message. Remark: The processing of the message in other cars is described in detail in Use Case “Safety reaction: Active brake”. An ECU of the chassis & safety domain detects a danger; this may be the trigger of an airbag, an obstacle in direction of travel seen by an environmental sensor, or an emergency braking performed by the driver or an automatic system. The Chassis Safety Controller (CSC) gets information about the dangerous situation via the Chassis Domain Bus. The CSC will assess the situation and will take measures to mitigate the danger for the car. The measures will result in commands to actuator ECUs in the chassis & safety domain and additionally commands to the powertrain domain to get a helpful driving power adjustment. In parallel it will also send information to the Communication Unit (CU). This information will contain data about the current vehicle dynamic status and detailed information about the planned actions (deceleration or acceleration, steering, etc.). The CU will send out a warning message that contains this information via the DSRC interface to nearby vehicles. The emergency message contains longitude, latitude, altitude, speed, acceleration and heading of the car, the time of message generation, the expiry time of the message, an indicator for the reliability of the information, a code that is classifying the car, an id that is identifying the sender of the message, an event code that is classifying the emergency situation and the planed acceleration and heading. All this information is packed in a message frame that adds checksum, information for protocol processing and if necessary security information.

UC-4	
Name	Emergency vehicle warning
Communication Parties	Vehicle (and emergency Vehicle), RSU
Use Case Scenario	This use case allows an active emergency vehicle to indicate its presence. In many countries the presence of an emergency vehicle imposes an obligation for vehicles in the path of the emergency vehicle to give way and to free an emergency corridor. NOTE: The legal status of vehicles giving way to emergency vehicles is determined by local law although in general national law will take precedence over any social or moral obligation to give way to the emergency vehicle.

UC-5	
Name	Slow vehicle warning
Communication Parties	Vehicle
Use Case Scenario	This use case consists from any slow vehicle to signal its presence (vehicle type) to other vehicles.

UC-6	
Name	Motorcycle warning
Communication Parties	Vehicle, RSU, Motorcycle
Use Case Scenario	Warn driver for arriving motorcycle. This is especially useful in case of reduced visibility.

UC-11	
Name	Wrong way driving warning
Communication Parties	Vehicle, Infrastructure
Use Case Scenario	This use case indicates to vehicles in the affected area that a vehicle is driving against the planned direction of traffic. The affected area is primarily the road in which the vehicle is driving in the wrong direction and the affected vehicles are those vehicles approaching the violating vehicle. NOTE: This form of driver behaviour may be a violation of local laws and require identification of the vehicle and driver by the appropriate authority.

UC-12	
Name	Stationary vehicle warning
Communication Parties	Vehicle
Use Case Scenario	This use case consists for any vehicle being dangerously immobilized on the road (consecutive to an accident, a breakdown or any other reason) to alert other approaching vehicles of the risk for them associated to this dangerous situation.

UC-13	
Name	Traffic condition warning
Communication Parties	Vehicle, Infrastructure (RSU, ITS-center)
Use Case Scenario	This use case allows any vehicle or roadside station to signal to other vehicles the current traffic condition at the point of sensor. Such data may be propagated by the ITS network as authoritative traffic management messages in order to mitigate the impact of the traffic condition on traffic flow.

UC-14	
Name	Signal violation warning
Communication Parties	Vehicle, Infrastructure (RSU, ITS-center)
Use Case Scenario	This use case allows a detecting ITS station (most likely a road side unit) to signal to affected users that a vehicle has violated a road signal and increased the risk of an accident. NOTE: This form of driver behaviour may be a violation of local laws and require identification of the vehicle and driver by the appropriate authority.

UC-15	
Name	Roadwork warning
Communication Parties	Vehicle, Infrastructure
Use Case Scenario	Via road infrastructure to vehicle communication, provides information on current valid roadwork and associated constraints.

UC-16	
Name	Decentralized floating car data
Communication Parties	Vehicle, Infrastructure (RSU, Traffic management-center)
Use Case Scenario	This use case consists for any vehicle to detect and signal to other vehicles some local danger or some traffic flow evolutions. Such information can be propagated until a certain distance (e.g. 20 km) by crossing vehicles (e.g. in local danger opposite direction) using geocasting capabilities. This information can also be received by road side units and forwarded to traffic management centres or nearby road side units for relay to vehicles in greater upstream distance.

UC-26	
Name	Intersection Collision Warning [Local Danger Warning from other Cars and to other Car]
Communication Parties	Vehicle
Use Case Scenario	**From other Vehicle** In order to avoid critical driving situations, car2X communication helps to virtually extend the view of the driver. The driver can be warned in critical situations, where an obstacle may be overseen, e.g. intersection warnings based on communication. This kind of application will reduce the number of fatalities. The communication of local danger warning messages is based on "Cooperative Awareness Messages" CAM and "Decentralized Environmental Notifications" (DEN) specified by the C2C-CC. Within Cooperative Awareness Messages, data is periodically broadcast, e.g. in order to prevent accidents at an intersection. Decentralized environmental notifications provide more specific information about an occurrence, e.g. to indicate a potential danger to other vehicles such as a car with warning lights on. The car that receives the messages processes the information and provides the driver a corresponding warning. **To other Vehicle** In order to avoid critical driving situations, car2X communication helps to virtually extend the view of the driver. The driver can be warned in critical situations, where an obstacle may have been overseen, e.g. intersection warnings based on communication. This use cases describes the detection of a local danger via internal sensors and ECUs of the in-vehicular system, which is used in order to generate a local danger warning message. The local danger warning message is then broadcast to other vehicles. The use case complements the description of the use case in Section 3.3 where the reception of the information is explained.

UC-31	
Name	Regulatory/contextual speed limits
Communication Parties	Vehicle, RSU
Use Case Scenario	This use case consists for a capable Road Side Unit to broadcast at a given frequency the current local speed limits (regulatory and contextual).

UC-32	
Name	Traffic light optimal speed advisory
Communication Parties	Vehicle, RSU
Use Case Scenario	This use case allows a traffic light to broadcast timing data associated to its current state (e.g. time remaining before switching between green, amber, red). NOTE: Traffic light sequences may vary.

UC-33	
Name	Traffic information and recommended itinerary [Traffic Information from other Entities and to other Entities]
Communication Parties	Vehicle
Use Case Scenario	From other Entity Classic traffic information is limited by high levels of latency and partly by inaccurate information. Enhancing this technology with car2X information from other cars, road-side units and backend service infrastructure will allow more efficient restructuring of traffic flows. To other Entity Classic traffic information is limited by high levels of latency and partly by inaccurate information. Enhancing this technology with car2X information from other cars, road-side unit and backend service infrastructure will permit more efficient restructuring of traffic flows.

UC-34	
Name	Enhanced route guidance and navigation
Communication Parties	Vehicle, RSU, Internet
Use Case Scenario	A road side unit which has the capability to access to internet and enable any passing by vehicle or parked vehicle to access to an internet server to request the downloading of an optimized itinerary (new waypoints) according to some personalized requirements. This interaction between a vehicle and an internet server may include a content purchasing transaction and the transfer of Digital Rights. Such access can be the result of received traffic information.

UC-37	
Name	Limited access warning, detour notification
Communication Parties	Vehicle, RSU
Use Case Scenario	Warn the approaching vehicles of some road limited access, provides the restriction data and may ask for access control. May provide some advice/itinerary elements (waypoints) to avoid the restricted area for vehicle being not authorized.

UC-38	
Name	In-vehicle signage
Communication Parties	Vehicle, RSU
Use Case Scenario	Via road infrastructure to vehicle communication, information on current valid traffic signs is given to the driver. NOTE: Depending on the law that applies at the time and place of transmission of such messages the demanded behaviour of the driver may be mandatory (e.g. speed limits) and failure to act on such messages may be considered as a traffic violation and require the identity of vehicle and driver to be made available.

UC-39	
Name	eTolling
Communication Parties	Vehicle
Use Case Scenario	Car tolling is already in use in different countries using different techniques. Most are based on the same principle: The use of an extra On-Board Unit (OBU). In Germany, for example, the service called “Toll Collect” is used to account trucks. The use case will be described based on the German system. According to the EVITA use cases reference architecture the OBU can be seen as an enhanced CU. The Toll Collect system [5] provides two types of accounting: the manual accounting and the automatic one. Just the automatic one will be considered within the description of this use case. To be able to automatically account the trucks, Toll Collect system used the combination of two positioning systems: the Global System for Mobile Communication GSM and the Global Positioning System GPS. Those two technologies are implemented in the Road Side Units (RSU) of the toll provider. In the vehicle, the OBU is equipped with a GPS antenna and GSM antenna in order to communicate with the RSU and to send the relevant information. With the position technologies, the OBU is then able to determine the driven distance in order to calculate the bill based on the driver contract information and in order to send it per mobile phone technology (GSM) to the data processing center of the toll provider. Considering the fact that for car2X communication a communication unit will be introduced in the car, the logical consequence will be the use of this unit for toll purposes. Therefore, in the description it is assumed that the OBU as part of the Communication Unit will handle the communication with the RSU. In this use case, the RSUs of the toll system provider are continually broadcasting a kind of wake-up signal. Depending on its position an OBU recognises a toll road and automatically saves the necessary data for the accounting. Passing the toll provider RSU, the vehicle receives the control signal and the OBU automatically calculates the toll fee. Before sending the needed data for toll accounting the CU checks the origin of the message (authentication of the RSU). If the RSU cannot be identified, the CU does not send any message after the check. Otherwise, it sends the data needed for accounting the driver: the type of the car, toll contract identification, pay method, and the signed bill of the last paid toll. All the data sent by the CU are signed and encrypted in order to ensure that the driver will be correctly accounted and that only an allowed control center can process the data.

UC-42	
Name	Point of interest notification [Point of Interest]
Communication Parties	Vehicle, Infrastructure
Use Case Scenario	In this use case a service provider offers advertising information through Road Side Units (RSUs). Drivers can receive information about shops, service stations, restaurants, drugstores, etc. Although this kind of information is available through most navigation systems; this could be more suitable for clients, because the information will be up-to-date and not software version dependant as with the navigation software. We assume in this use case that the RSU just broadcasts the advertising information. We will not consider a distinction of advertising information type. Drivers preconfigure whether they want to receive advertising information. Entering an area covered by a particular Road Side Unit, the vehicle receives a signed message from the Road Side Unit. The RSU identity is verified. The CU then sends the information to the Head Unit, which then displays it.

UC-43	
Name	Automatic access control/parking access
Communication Parties	Vehicle, RSU
Use Case Scenario	Upon signalization of an access controlled area (e.g. a private or public parking), a concerned vehicle entitled to access this area will supply its identity to the road side unit to obtain the right to access the area.

UC-44	
Name	Local electronic commerce
Communication Parties	Vehicle, RSU
Use Case Scenario	A road side unit signalling some POI/LBS may have the capability to process a local payment (using some electronic purse/wallet) for service reservation or/and some good purchasing.

UC-46	
Name	Media downloading
Communication Parties	Vehicle, RSU, Internet
Use Case Scenario	A road side unit which has the capability to provide multimedia for passenger entertainment using or not an Internet network. The downloading of multimedia can be conditioned by a commercial transaction resulting in the supply of digital rights to be used for the downloading action.

UC-51	
Name	SOS service [eCall]
Communication Parties	Vehicle, Infrastructure
Use Case Scenario	In case of an accident, e.g. detected by the trigger of the airbag, an emergency call is automatically generated. The last positions of the vehicle (position chain) based on GPS/ Galileo signals are also transferred to enable the location of the vehicle. With these measures the delay from the occurrence of the accident to the arrival of the emergency vehicle is minimized. Today only few vehicles are equipped with this facility and a Service Provider (e.g. OnSTAR) aggregates the position data and then transfers the call to the next PSAP (Public Service Access Point). The vehicle owner has to pay a monthly or annual fee for this service, usually combined with other services. The emergency call is transferred via the Service Provider to the next PSAP. No changes in the infrastructure of the PSAPs are necessary. The use case eCall is based on this approach. The public European emergency call system currently under development will use the GSM 112 emergency call number (‘112 eCall’) that is automatically linked to the next PSAP today, so a Service Provider is no longer necessary. In addition to the direct communication with the driver, the PSAPs have to be able to deal with the crash data – thus changes to the PSAP infrastructure are necessary. The European commission has pointed out that with a fully deployed and mandatory eCall system 2500 lives could be saved per year in Europe [6]. The adoption of this approach is therefore being strongly encouraged.

UC-53	
Name	Remote diagnosis and just in time repair notification [Remote Diagnosis]
Communication Parties	Diagnosis, Vehicle
Use Case Scenario	Diagnosis of cars is not a new goal in the automotive industry. It has existed since cars were first designed. During the last 20 years car diagnosis gained more importance because of the increasing use of electronics in cars. Standards were defined not just to allow different manufacturer's ECUs to communicate with each other in an in-vehicle network system, but also to allow different diagnosis tools to have access to diagnosis data; e.g., failure log entries. Those entries are composed of failure codes, their states, and the context in which the failures occurred. We distinguish between two different types of diagnosis: On-Board Diagnosis and Off Board Diagnosis. The difference is that an Off-Board diagnosis is done with an off-vehicle system (e.g. diagnosis tool). It is important to mention that an Off-Board Diagnosis can be done by connecting the diagnosis tool to the On-Board Diagnosis system. For better understanding, a few words about failure log entries. Each ECU has a diagnosis routine, which records failure events (e.g. sensor failure) in the failure log. Since the failure events can be sensitive for different ECUs, different failure records are made. A diagnosis tool will try to know where the real cause comes from, based on two points: the different entries made in different timeframes and the algorithms implemented. Nowadays car diagnosis in Europe is hardwired. A wireless car diagnosis will be described in our case with focus on the communication characteristics of the data transmission. In this use case, a car owner wants his car to be inspected by a service station. After receiving the request of the car owner, a service station using a diagnosis tool will try to assess the state of a vehicle located in their area without making any physical connection to the vehicle. The diagnosis of the vehicle should even be possible if the vehicle is not in the area of the service station, by using an internet connection. This is necessary since real time data when a vehicle is moving can help to discover malfunctions, which are not detectable when the car is in the service area. The service station has to first connect via Internet and Wireless LAN to the in-vehicle network. An employee of the station using the diagnosis tool sends a connection request to the vehicle. The authorization for the connection is checked in the Communication Unit (CU). The message is checked for integrity and the service station is authenticated. A connection answer is sent back to the diagnosis tool. Once the connection is established, the diagnosis tool sends, depending on the option chosen by the employee of the service station, requests to read out diagnosis information (State/Log information) from the Electronic Control Unit (ECU) it wants to check. A motor diagnosis will be considered in this case; therefore, information from the engine control unit shall be read. After receiving the connection request, the CU forwards it

	to the ECU. A secure session is negotiated between the ECU and the diagnosis tool using a challenge response process.

UC-56	
Name	Insurance and financial Services
Communication Parties	Vehicle, RSU, Internet
Use Case Scenario	On-demand and real time interaction (e.g. pay as you drive service) with financial and insurance coverage service provider enabled by I2V and V2I communications.

UC-57	
Name	Fleet management
Communication Parties	Vehicle, RSU, Internet
Use Case Scenario	A road side unit which has internet access capabilities can provide to and collect from vehicles, some fleet management data through exchanges between vehicles (passing by or parked) and a local RSU.

UC-58	
Name	Vehicle software/data provisioning and update [Remote Flashing and Flashing per OBD]
Communication Parties	Vehicle, RSU, Internet
Use Case Scenario	Remote In the use case “Remote Diagnosis”, the process to connect remotely from a service station to the in-vehicle system of a car has been described. Diagnosis is used to assess the state of the vehicle. A possible consequence of diagnosis would be the update of the software version of the Electronic Control Unit ECU to remove bugs or to improve the functionality. Nowadays this is done over cables, flashing per OBD. In this use case flashing an ECU wirelessly will be addressed. On one hand this brings advantages such as faster updates, comfort and money savings for the driver, and more clients per day served for the service station since the driver does not have to use the area of the service station to let his car be repaired. On the other hand, this brings a lot of security issues. We assume that the driver and the service station have an arrangement about the remote flashing of the driver’s vehicle. The service station using a Diagnosis/Flashing Tool establishes a connection via Internet and Wireless LAN to the in-vehicle network. It sends a connection request to the ECU in the Powertrain domain via the Communication Unit (CU). The request is checked for integrity and the service station is authenticated. A connection answer is then sent and session keys are shared to allow a secure communication channel. To know which version will be installed, a diagnosis of the vehicle is done to have all necessary information such as ECU type, Firmware Version, and date of the last update. If the type is the expected one, then the flashing session is started. The flashing tool sends a request to open a programming session at the ECU level. Once the programming session is open, the flashing tool sends the encrypted new software version to the RAM of the ECU. The communication still goes through the CU. Every message is checked for integrity, authenticity, and freshness at the ECU level. The software is flashed in the ROM, and the date is saved. At the end the flashing tool closes the programming session at the ECU level and the connection with the vehicle. OBD In use cases “Remote flashing” and “Remote Diagnosis”, the connection for diagnosis purpose is done wirelessly. Nowadays in Europe, car diagnosis is done hardwired. It’s interesting to take a closer look at the use case, to identify the security issues service stations and vehicles owner are already confronted with. The description is based on the Standard Unified Diagnostics Services UDS, which is specified in [7]. In this use case an ECU firmware of a vehicle will be updated hardwired from a service station. A car owner takes his car to the area of a service station. To start the diagnosis

	session the car has to be activated. The ECU initializes its software and starts the diagnosis function, called diagnosis server. In this state, the diagnosis server is in the default mode (this is defined as a session in [7]). The service station employee connects his diagnosis tool to the on-board diagnosis interface in the vehicle. This is done by plugging a cable to the diagnosis connector, which is different from car to car. A diagnosis request is then sent via the Communication Unit CU (on-board diagnosis interface) to the ECU. The ECU authenticates the diagnosis tool and checks the data integrity. If the request is successful, the ECU opens a programming session. The service station employee begins his diagnosis by checking the ECU type and firmware version. Assuming the ECU type is known, a comparison is also made to figure out the need of an update of the version. The diagnosis tool then sends the encrypted packets of the new firmware to the ECU, which stores it in the RAM. The new firmware is decrypted at ECU level and flashed in the ROM packet wise. The date of the update is written in the ECU and the programming session is closed by sending an EcuReset request to the ECU.

UC-59	
Name	Loading zone management
Communication Parties	Vehicle, RSU
Use Case Scenario	The goal with this Use Case is to support the driver, fleet manager and road operator (including parking zone operator) in the booking, monitoring and management of the urban parking zones for freight driver activities. These activities can be loading/unloading of both heavy vehicles and for parcel operators' smaller vehicles. It describes from the driver or/and fleet operator side the possibility to book in advance an urban loading bay specifying the delivery mission, the planned delivery time, the loading/unloading time required, the vehicle type, any flexibility (e.g. ±15 mins) in the delivery time and the estimated time to reach the parking zone (interaction with traffic management). For the road operator, it describes the possibility to optimize the management of loading zones through better knowledge of the delivery time period and duration. For the fleet operator, it describes the possibility to optimize the delivery time to its customer, reduce driver stress and anticipate congestions problem. NOTE: An important point is to define what a loading zone is. It can be a physical on/off street space or it can be a pedestrian street/area for instance. The layout here is a section of road which is available for freight vehicles to stop, for a limited time, for loading/unloading purposes. It may be part of the main carriageway or an additional lane.

UC-60	
Name	Vehicle and RSU data calibration
Communication Parties	Vehicle, RSU, Internet
Use Case Scenario	An RSU compares its sensor data or calculated traffic status to the respective data delivered by passing vehicles utilizing V2I communication. Also vehicles passing each other compare sensor data utilizing V2V communication. In case of major and recurring discrepancies the respective RSU or vehicle flags malfunctioning sensor data or information pieces so they are not used in further processes until the sensor devices are recalibrated online or offline (maintenance). The RSU or vehicle is, if online calibration fails, transmitting a notification to a dedicated maintenance management server for maintenance scheduling or stores it for information of maintenance staff during next regular maintenance run.

UC-61	
Name	Personalize the car
Communication Parties	Nomadic Device, Vehicle
Use Case Scenario	Enable a driver to personalize a car, i.e. to adjust seat position, mirrors, and preferred settings for multimedia devices, without physical action. Because of this a “User Profile”, which was created once before, will be activated from a mobile device. Here we will exemplify how the seat position becomes adjusted.

UC-64	
Name	Remote Car Control (e.g. door opener)
Communication Parties	Vehicle, Infrastructure
Use Case Scenario	Enable a remote control of car functions from both outside and inside the vehicle via mobile devices. Possible application examples are closing and opening of windows, doors or similar units with a smart phone. In this use case we describe unlocking and opening of the convertible top from outside of the car with a smart phone.

UC-66	
Name	Install applications
Communication Parties	Nomadic Device, Vehicle
Use Case Scenario	The purpose of this use case is to describe the possibility of installing and running applications in the car from an external device. These can be used through modules by the driver or occupants. Here we exemplify the use case for installing a city application, i.e. visitor guidance for a city, which shows interesting routes and points of interests in the city.

UC-69	
Name	Secure Integration
Communication Parties	Nomadic Device, Vehicle
Use Case Scenario	The use case demonstrates the integration of an application installed on mobile device, e.g. a media player on a notebook, within the multi media function of the car. This use case demonstrates how a notebook could access the Internet via the connections of the car, download multimedia content, and use the audio and video devices of the car to display these data.

UC-70	
Name	Replacement of Engine ECU
Communication Parties	Diagnosis device, Vehicle
Use Case Scenario	Due to a malfunction the engine control ECU of a vehicle has to be replaced. Normally this is done by an authorized garage, when the diagnosis shows that the reason for the malfunction is the ECU. If the ECU is capable of being flashed, then the garage has to install exactly the right version of the hardware of the ECU and then download the right software version as described in the “Remote Flashing” and “Flashing per OBD” use cases. If the software cannot be downloaded, e.g. for older cars with ROM (Read-Only Memory), the garage has to install the right ECU hardware with the correct software version. Remark: The processing of the software download and the related communication scenarios are described in the “Remote Flashing” and “Flashing per OBD” use cases.

UC-71	
Name	Installation Car2x Unit
Communication Parties	Diagnosis device, Vehicle
Use Case Scenario	. In a garage a Car2X Communication Unit (CU) is installed into a car. The car was not equipped with a CU before. The installation will include mechanical installation, connection to power supply, connection to the backbone bus of the car and mounting of antennas and antenna cabling. All configuration work that is needed to associate the CU with the car, to allow payment function etc., is done in the garage. The functionality of the car will be only changed in that new information from the CU can be accepted and integrated in the procedures of the installed car systems. The information that is broadcast from the CU will be taken from the backbone bus. To accept and use the data from the CU, the Chassis Safety Controller (CSC) and the Head Unit (HU) will need software updates that have to be installed during the installation. Remark: The processing of messages from and to the CU is described in detail in use case “Safety reaction: Active brake” and use case “Message leads to safety reaction”.

6）自動化レベルとユースケースの紐付けについて

自動化レベルとしては内閣府の SIP で定義されたものと、米国の NHTSA で定義されたもの、米国の SAE (Society of Automotive Engineers)、ドイツ自動車工業会 VDA、OICA(国際自動車工業連合会)で定義されたものがある。SIP は level 1 から level 4 までの 4 段階、NHTSA は level 0 から level 4 までの 5 段階であるが、NHTSA の level 0 は自動化されていないレベルであり、自動化のレベルは双方とも 1-4 となっている。SAE、VDA、OICA の定義はレベル 0 から 5 の 6 段階になっているが、SIP／NHTSA との違いは、Level4 をさらに 2 段階に細分化するか否かである。ここは、今回の検討では優先度が低いと考え、レベル数の少ない SIP/NHTSA の定義を検討した。その比較を以下の表 1 で示す。NHTSA の level 1 の定義では、複数の制御機能が許されており、SIP のものと異なる様に見えるが、それら複数の制御機能は独立しているという制限があるため、SIP と同等のものと考えられる。

表 1　自動化レベルの比較

自動化レベル	SIP 概要	NHTSA 概要
level 0	定義なし	自動化無し。すべて人が操作する。ただし運転支援のための警告やワイパーやヘッドライトなどの制御は行える。
level 1	加速・操舵。制御のいずれかを自動車が行う状態	一つもしくは複数の制御機能が自動で行われる。ただし、複数の制御が行われる場合、それらは独立していなければならず、協調した制御は行わない。 運転は人が行わないといけない。
level 2	加速・操舵。制御の複数の操作を自動車が行う状態	複数の制御機能が協調し、自動で行われる。ただし、人は常に状況を把握し、自動制御が出来なくなった際に直ちに運転出来なくてはならない。
level 3	加速・操舵、制御を全て自動車が行い、緊急時のみ運転者が対応する状態	全ての制御が自動で行われる。建設中のエリアの様に自動制御が出来ないところでは人による運転が必要であるが、直ちに運転出来る状態である必要はなく、ある程度の余裕時間がある。そのため、人が常に状況を把握している必要はない。
level 4	加速・操舵・制御を全て運転者以外が行い、運転者が全く関与しないシステム	完全自動運転。人は目的地などを設定する程度で、運転することは考えていない。また、有人、無人を問わない。

表 2 では各ユースケースが上記 level 0 － 4 のどの自動化レベルで用いられるかを記載している。「level 0」のうち、今後ユースケースが再考され制御も行う場合に、より高いレベルになると考えられるものについては「level 0 *」と表記している。

以上の様に、これまでの脅威分析で用いている前提条件では自動運転を実現するには不十分である。今後はこの調査結果を基に自動運転を実現するためのユースケースの考慮と、

それに適した脅威分析手法の開発、さらにそれらを用いた脅威分析を実施し世界的に標準となる結果を出すことが必要であると考える。

表 2　基礎となるユースケースと自動化レベルの紐付け

ユースケースカテゴリ	ユースケース ID	ユースケース名	自動化レベル
Vehicle control	**UC-1**	**Safety reaction: Active brake**	**level 1**
Vehicle status warnings	UC-2	Emergency electronic brake lights [Messages lead to safety reaction]	level 0 *
	UC-3	Safety function out of normal condition warning [Messages lead to safety reaction]	level 0 *
Vehicle type warnings	UC-4	Emergency vehicle warning	level 0
	UC-5	Slow vehicle warning	level 0 *
	UC-6	Motorcycle warning	level 0 *
	UC-7	Vulnerable road user Warning	level 0 *
	UC-8	**左折時衝突防止**(V2V)	level 0 *
	UC-9	**左折時衝突防止**(V2I)	level 0 *
	UC-10	**追突防止**(V2I)	level 0 *
Traffic hazard warnings	UC-11	Wrong way driving warning	level 0 *
	UC-12	Stationary vehicle warning	level 0 *
	UC-13	Traffic condition warning	level 0 *
	UC-14	Signal violation warning	level 0 *
	UC-15	Roadwork warning	level 0 *
	UC-16	Decentralized floating car data	level 0 *
	UC-17	**一時停止規制見落とし防止**(V2I)	level 0 *
Dynamic vehicle warnings	UC-18	Overtaking vehicle warning	level 0 *
	UC-19	Lane change assistance	level 0 *
	UC-20	Pre-crash sensing warning	level 0 *
	UC-21	Co-operative glare reduction	level 0
Collision Risk Warning	UC-22	Across traffic turn collision risk warning	level 0 *
	UC-23	Merging Traffic Turn Collision Risk Warning	level 0 *
	UC-24	Co-operative merging assistance	level 0 *
	UC-25	Hazardous location notification	level 0 *
	UC-26	Intersection Collision Warning [Local Danger Warning from other Cars and to other Car]	level 0 *
	UC-27	Co-operative forward collision warning	level 0 *
	UC-28	Collision Risk Warning from RSU	level 0 *
	UC-29	**右折時衝突防止**(V2I)	level 0 *
	UC-30	**出会い頭衝突防止**(V2I)	level 0 *
Traffic Efficiency	UC-31	Regulatory/contextual speed limits	level 0 *
	UC-32	Traffic light optimal speed advisory	level 0 *
	UC-33	Traffic information and recommended itinerary [Traffic Information from other Entities and to other Entities]	level 0 *
	UC-34	Enhanced route guidance and navigation	level 0

	UC-35	Intersection management	level 0
	UC-36	Co-operative flexible lane change	level 0 *
	UC-37	Limited access warning, detour notification	level 0
	UC-38	In-vehicle signage	level 0
	UC-39	Electronic toll collect [eTolling]	level 0
	UC-40	**Co-operative adaptative cruise control**	**level 1**
	UC-41	**Co-operative vehicle-highway automation system (Platoon)**	**level 3**
Others	UC-42	Point of interest notification [Point of Interest]	level 0
	UC-43	Automatic access control/parking access	level 0
	UC-44	Local electronic commerce	level 0
	UC-45	Car rental/sharing assignment/reporting	level 0
	UC-46	Media downloading	level 0
	UC-47	Map download and update	level 0
	UC-48	Ecological/economical drive	level 0
	UC-49	Instant messaging	level 0
	UC-50	Personal data synchronization	level 0
	UC-51	SOS service [eCall]	level 0
	UC-52	Stolen vehicle alert	level 0
	UC-53	Remote diagnosis and just in time repair notification [Remote Diagnosis]	level 0
	UC-54	Vehicle relation management	level 0
	UC-55	Vehicle data collect for product life cycle management	level 0
	UC-56	Insurance and financial Services	level 0
	UC-57	Fleet management	level 0
	UC-58	Vehicle software/data provisioning and update [Remote Flashing and Flashing per OBD]	level 0
	UC-59	Loading zone management	level 0
	UC-60	Vehicle and RSU data calibration	level 0
	UC-61	Personalize the car	level 0
	UC-62	Car Finder (e.g., via mobile phone)	level 0
	UC-63	Electronic License Plate	level 0
	UC-64	Remote Car Control (e.g. door opener)	level 0
	UC-65	Pay as You Drive (Road Safety & Eco)	level 0
	UC-66	Install applications	level 0
	UC-67	Parking Sensor System	level 0 *
	UC-68	Electronic Driver Logbook	level 0
	UC-69	Secure Integration	level 0
	UC-70	Replacement of Engine ECU	level 0
	UC-71	Installation Car2x Unit	level 0
	UC-72	Booking a Hotel on the Road	level 0
	UC-73	COMBINATION OF THE “CALCULATING ROUTE FROM CURRENT POSITION TO HOME” AND “BOOKING A HOTEL ON THE ROAD”	level 0
	UC-74	ROAD SURFACE CONDITIONS TO TOC	level 0

経済産業省委託

平成26年度戦略的イノベーション創造プログラム
V2X（Vehicle to X）システムに係る
セキュリティ技術の海外動向等の調査

報告書

平成27年3月

発行　一般財団法人 日本自動車研究所
東京都港区芝大門1－1－30
日本自動車会館 12階
TEL 03（5733）7925