平成２７年度
戦略的イノベーション創造プログラム（自動走行システム）：Ｖ２Ｘ等車外情報の活用にかかるセキュリティ技術の研究・開発プロジェクト

平成 28 年 3 月

一般財団法人　日本自動車研究所

平成 27 年度
戦略的イノベーション創造プログラム（自動走行システム）：
V2X 等車外情報の活用にかかるセキュリティ技術の研究・開発
プロジェクト

― 目 次 ―

第 1 章　はじめに

1.1　事業全体の目標

我が国では、交通事故死者数低減を国家目標として掲げており、2014 年末まで 14 年連続で減少傾向となっているが、交通事故死者数全体に占める 65 歳以上の高齢者の割合は高い水準で推移しており、その対策が急務となっている。さらに、社会問題の一つである交通渋滞は渋滞損失時間を発生させ、経済機会そのものの損失につながっている。これらの課題に対する究極の解決策として期待されるのが自動走行システムであり、欧米各国と ICT 関連企業などの新規参入事業者を巻き込んだ熾烈な競争が繰り広げられている。

自動走行システムでは、様々なセンサによって収集される自動車そのものの動きや人の動きなどのデータが一つの地図基盤上にリアルタイムで統合され、統合されたこれらのデータ等を自動車が認知し、AI 等によって一歩先を読んで判断、動作を制御する自動走行システムの実現により、交通事故や交通渋滞の低減を価値として提供できる。また、技術の適用範囲を拡大することで公共交通機関の定時運行や、誰もがストレスなく移動できる手段等を新たな価値として提供できる。

自動走行システムの基盤となる高度な地図（ダイナミックマップ）のデータや、地図上にマッピングされる自動車、歩行者、インフラ設備等の情報は、主として車外との通信手段を用いて入手することが想定されている。通信手段としては、車車間や路車間の通信を行う V2X の他、スマートフォンの活用や、PHEV/EV の充電スタンドとの通信等、様々な形で行われる。また、車両情報の外部とのやり取りという点では、車に備えられた OBD ポートを経由するものも通信に含まれる。こうした通信の中で、リアルタイム性の高い V2X 通信では、交差点における直交する交通や、前前方車両の急停止等、直接見えていない他の車両の情報や、効率的でスムースな交通の流れを実現する信号との協調情報等のやり取りが想定されている。

自動走行システムでは、こうした情報を活用するために、車外から通信によって伝えられる情報を、車内の情報系や制御系に、例えばゲートウェイ等を介して繋がるようになるため、従来の自動車にはなかったサイバーセキュリティへの対応を検討する必要がある。これまでにも、車内のネットワークに直接接続することで、車両の制御を乗っ取る実験が行われた例があり、本年、車両の外部から自動車メーカが提供する通信サービスを経由して、車両の制御をハッキングした事例が報告されている。自動車を安全に運行させるためには、こうしたサイバー攻撃への対策が重要な課題となっている。

自動走行システムの技術開発にあたって、各国および企業間の競争がその技術レベルの向上に大きく貢献していることは論を待たないが、そのセキュリティの確保にあたっては多くのユースケースを見据えた対策が必要であり、多方面の知見に基づく共通基盤技術として共通評価技術等の開発、およびそこから得られた知見等の共有化を進めることが望ましい。

しかし、各国および企業により研究・開発されているセキュリティ技術は、個々の自動車が持つ機能･特性および必要性に応じて取捨選択され､適用されることが想定されるが、セキュリティ技術の効果・評価について数値化などで比較することは非常に困難である。結果として、個々の自動車に対するセキュリティ対策の妥当性を客観的に証明することは難しい。

このため共通的な基本システムに対して対策すべきポイントや、そのポイントに対する対策の評価指針・基準・指標などは、企業間の競争によるものではなく、それらを共通課題として知見等を共有化できるようにするためには、共通モデルを構築していくことが必要となる。

なお、競争分野である対策技術開発においても、時間経過と共にある程度一般化されていく（業界として常識化していく）技術もある。一方で、一般化機能との差異化部分で新たな競争領域として進化する技術もある。

本事業では、自動走行システムに向けた自動車のシステムアーキテクチャの共通モデルを構築し、そのモデルに基づく脅威分析の実施、テストベッドの構築に向けた検討・技術開発、V2X 通信における署名検証の簡略化の研究を行うとともに、V2X 通信に関連する海外の技術・動向等の調査を実施した。

1.2　全体スキーム

本事業の全体実施体制を図 1-1 に示す。

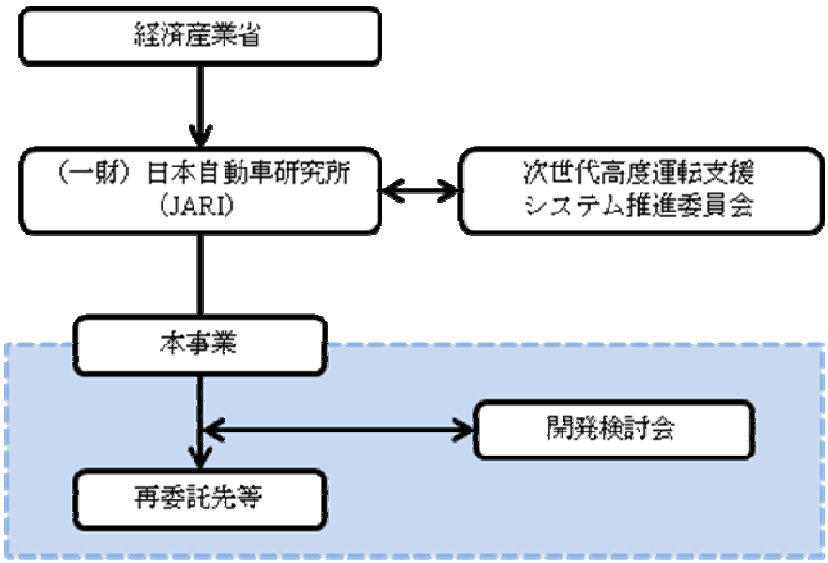


図 1-1　事業の全体実施体制図

事業実施にあたっては、成果の最大化、活用促進を図るため、セキュリティ関連の研究等を行っている外部有識者等を含む開発検討会を設置した。また、自動走行に関するプロ

ジェクトの全体推進に関して別途設置されている外部有識者や自動車メーカ等からなる次世代高度運転支援システム推進委員会を活用し、助言をいただきながら推進した。

また、研究・開発を効率的に進めるため、民間の組織である情報セキュリティ研究開発シナリオ検討 SWG（以下、情報セキュリティ SWG と称す）とも意見交換を行うなど、関係組織との連携体制も構築した。

1.3 委員名簿

本事業の研究・開発方針の策定や、事業の推進における課題等を議論する場として、セキュリティ関係の研究を行う機関や、自動車関連団体のメンバーから構成される開発検討会を平成 27 年度に 3 回開催した。委員名簿を表 1-1 に示す。

・第 1 回（平成 27 年 12 月 21 日）:「V2X セキュリティ」プロジェクト概要、計画の説明
・第 2 回（平成 28 年 1 月 29 日）: 研究・開発の進捗報告、課題の議論
・第 3 回（平成 28 年 2 月 17 日）: 研究・開発成果の見通し報告、課題の議論

表 1-1　V2X セキュリティ開発検討会　委員名簿

	氏名	組織名　所属／役職
座長	松本　勉	国立大学法人 横浜国立大学大学院 環境情報研究院教授
委員	水間　毅	独立行政法人 交通安全環境研究所 理事
委員	桑名　利幸	独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ技術ラボラトリー次長
委員	盛合　志帆	国立研究開発法人 情報通信研究機構 ネットワークセキュリティ研究所 セキュリティ基盤研究室 室長
委員	川久保　淳史	一般社団法人 日本自動車工業会 情報セキュリティ WG 副主査
委員	橋本　寛	一般社団法人 JASPAR 情報セキュリティ技術 WG 主査
オブザーバー	経済産業省 製造産業局 自動車課	
オブザーバー	経済産業省 商務情報政策局 情報セキュリティ政策室	
オブザーバー	JPCERT コーディネーションセンター	
事務局	日本自動車研究所	

また、本事業を推進するに当たり、自動走行に関する有識者メンバーで構成される次世代高度運転支援システム推進委員会に対して、研究・開発の進捗状況等の報告を実施した。本委員会は平成 27 年度に 5 回開催され、本事業からは、そのうちの第 3 回、第 5 回にて報告を行い、質疑応答および意見交換を実施した。上記推進委員会の委員名簿を表 1-2 に示す。

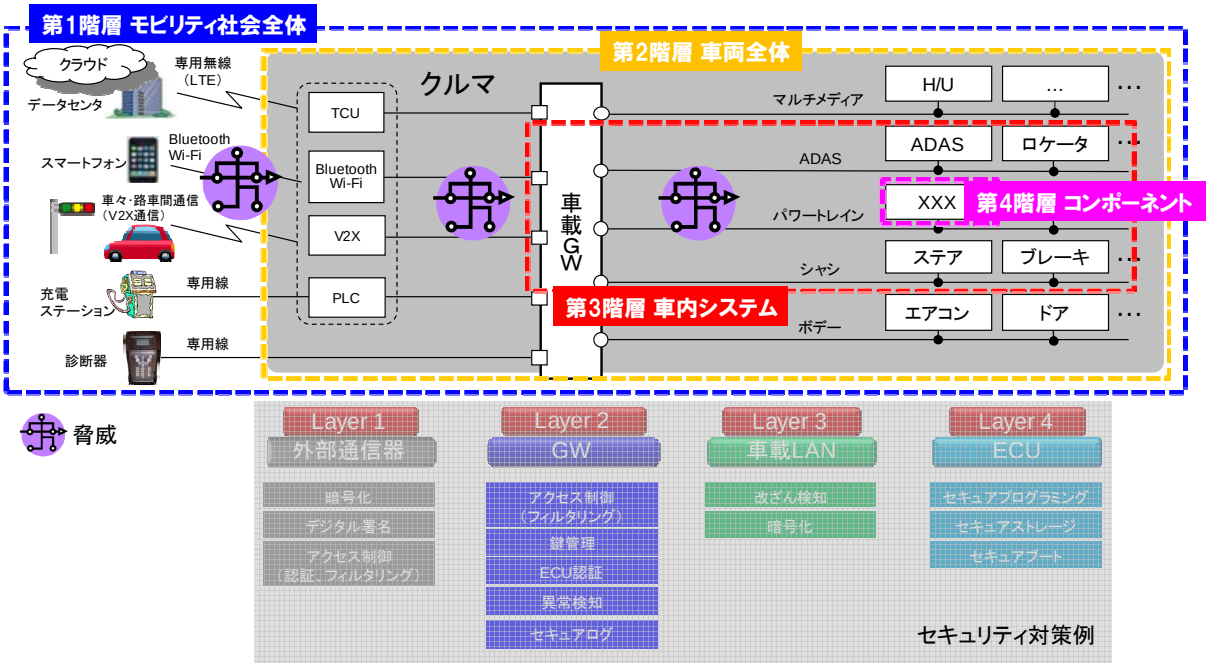
・第 3 回（平成 27 年 12 月 8 日）：プロジェクト概要、計画の説明
・第 5 回（平成 28 年 2 月 29 日）：研究・開発成果の見通し報告

表 1-2　次世代高度運転支援システム推進委員会　委員名簿

	氏名	組織名　所属／役職
委員長	石　太郎	早稲田大学 環境総合研究センター 参事
委員	伊藤　誠	筑波大学 システム情報系 教授
委員	大前　学	慶應義塾大学大学院 政策・メディア研究科 教授
委員	北崎　智之	国立研究開発法人 産業技術総合研究所 自動車ヒューマンファクター研究センター 研究センター長
委員	葛巻　清吾	トヨタ自動車 CSTO 補佐（SIP システム実用化 WG 副主査）
委員	菅沼　直樹	金沢大学 新学術創成研究機構 准教授
委員	須田　義大	東京大学 生産技術研究所 教授 次世代モビリティ研究センター長
委員	横山　利夫	本田技術研究所 上席研究員 （日本自動車工業会自動運転検討会主査）
オブザーバー	経済産業省 製造産業局 自動車課	
事務局	日本自動車研究所	

第 2 章　技術開発項目

本事業において、セキュリティを検討していく上で、自動車として検討すべき対象の階層を図 2-1 の様に分類することとした。第 1 の階層としては、今後繋がる車を含む「モビリティ社会全体」であり、クラウド等を含んでいる。第 2 の階層は、車両外部との通信端末を含む「車両全体」、第 3 の階層は、外部からの情報がゲートウェイを経由して接続される車内のネットワークであり、ここでは「車内システム」と呼ぶ。第 4 の階層は、ECU 等の個別の「コンポーネント」である。



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

図 2-1　本事業の対象の定義

本事業では、主として第 2 階層以下を対象とする。但し、第 1 階層において発生したセキュリティ上の脅威は、外部通信（V2X、WiFi、スマートフォン等）を経由して、第 2 階層以下への入力となるため、どういった脅威があるかについて検討を行う。

特に、V2X 通信については、車両間の通信（V2V）もあり、自動車向けのセキュリティ技術として検討されているため、本事業の対象に含んでいる。また、V2X 通信に関しては、国内と海外とではセキュリティ仕様が異なっているため、海外のセキュリティ技術やプロジェクト等の動向について調査を行い、海外の V2X 通信に関する情報共有の仕組みを構築する。

4 年の実施期間を想定している本事業における 4 つのテーマにおける具体的な実施内容については以下の通りである。

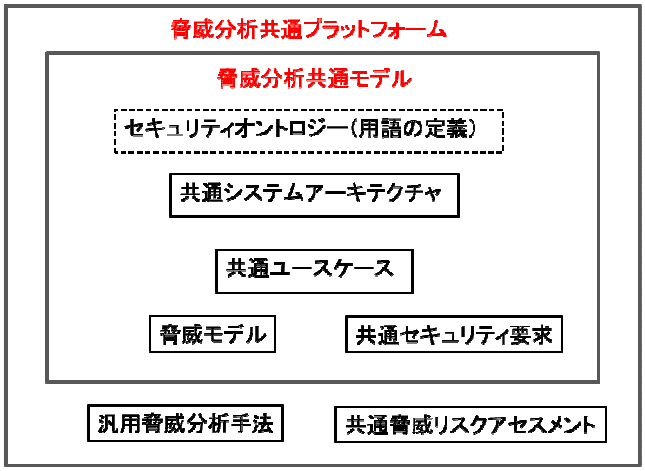
2.1　自動運転の共通モデルの構築と、それに基づく脅威分析、セキュリティ要件及び対策の検討（テーマ①）

セキュリティ対策の重要な要素技術の一つが脅威分析である。セキュリティの対策を立案するためには、どのような脅威が存在し、その脅威に対する対抗策（セキュリティ要求）として何が適切であるかを考え、その予想されるリスクを十分低減しているかを明確にするために実施されるのが脅威分析である。

脅威分析は、以下の要素を基に実施するのが一般的である。

・システムアーキテクチャ
・（対象システムの利用方法に関する）ユースケース（想定利用例）
・脅威分析手法
・リスクアセスメントのための基準
・対抗策（セキュリティ要求）の作成

これらの技術の開発は自動車メーカの各社が個別に対応するのではなく、自動車産業全体で共有されることで、効率的に、より安全で、セキュアな自動車の開発が可能になる。個社別のアーキテクチャや、ユースケース、脅威分析手法、アセスメントのための基準ではなく、自動車業界で共通に利用できるものとするためには、共通に議論するためのモデルの構築が必要になる。本事業においては、これを「脅威分析共通モデル」と呼び、その構築、それに基づく汎用脅威分析手法、共通脅威リスクアセスメント、共通セキュリティ要求の導出と、これらを支援するためのツール「脅威分析共通プラットフォーム」に関する研究開発を実施する（図 2.1-1）。



注：セキュリティオントロジーとは、本事業において開発される全てのセキュリティ関連の用語の統一のために作成される用語体系を意味する。

注：脅威モデルは、脅威分析の結果得られる攻撃の情報を意味する（例えば、アタックツリーで記述された攻撃ベクター）

図 2.1-1　脅威分析共通モデルと脅威分析共通プラットフォーム

2.1.1　共通システムアーキテクチャ

システムアーキテクチャとしては、セキュリティ機能を集中的に管理するセントラル・ゲートウェイ方式や、各 ECU に暗号処理機能を持たせるものなど、様々なセキュアなアーキテクチャが考えられるが、これらの共通部分を抽出した上で、複数の共通アーキテクチャを策定し、それに基づく脅威分析を実施する。

2.1.2　共通ユースケース

平成 26 年度において実施した調査（JARI :「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 26 年度戦略的イノベーション創造プログラム）においては、欧州を中心に実施されている V2X 関連の研究プロジェクト、我が国における ITS 関連のユースケースを精査したが、全てのユースケースが自動走行を想定したものではなかった。本事業では、昨年度の調査の結果を利用しつつ、自動走行に特化したユースケースを収集し、最終的に開発される脅威分析を支援する「脅威分析共通プラットフォーム」において利用できるようにユースケースを策定する。

2.1.3　汎用脅威分析手法

脅威分析手法の選択肢としては、広く利用可能な手法の選択が望ましい。欧州 FP7 プロジェクトの中で自動車のセキュリティの検討を行った EVITA においては、アタックツリー（Attack Trees）が利用されている。さらに、アタックツリー自身は、様々な産業におけるセキュリティ脅威分析の手法として利用されている。表 2.1.3-1 に、アタックツリーの利点と欠点を示す。

表 2.1.3-1　アタックツリーの特徴

- アタックツリーの利点：
  - ・攻撃の経路や対象（保護資産）の記述（個々の攻撃木の手法に依存)、メトリックス計算が可能。
  - ・安全分析（故障木（Fault Trees)）との親和性が高く、統合した手法がいくつか提案されている。
- アタックツリーの欠点：
  - ・現代的な多段攻撃やトラストレベル等の分析は出来ないので、改良もしくは、他の手法との併用が必要。
  - ・分析手法の学習に時間がかかり、分析にかかる工数が大きい。

現在のセキュリティを取り巻く状況では、高度な多段攻撃、複数のパーティにおける信頼度を判定するトラストレベル（C2C-CC における TAL : Trust Assurance Level）などの新しい傾向や枠組みが提案されており、それに対応したセキュリティ上の脅威を分析する方法論が生まれつつある。例えば、航空機のセキュリティ規格である DO-326A （RTCA,

Airworthiness Security Process Specification (2014)） においては、以下のような攻撃の分析方法（多段攻撃やトラストレベルを用いた分析）が示されている（図 2.1.3-1）。

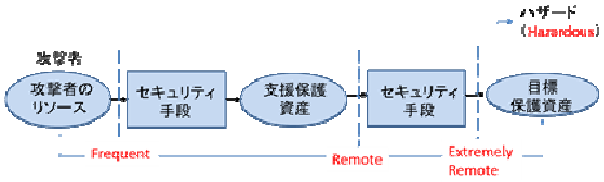


図 2.1.3-1　攻撃の分析例

これらの新しいセキュリティの分析手法を調査し、業界全体で汎用的に利用できる手法について研究する。

2.1.4　共通脅威リスクアセスメント

自動車に対する脅威のアセスメントにおいては、自動車用の機能安全規格である ISO 26262 の ASIL (Automotive Safety Integrity Level) のようなセキュリティのアセスメント基準（例えば、 Automotive Security Integrity Level (ASecIL)と呼ばれるようなもの）がない状況である。しかし、V2X 関連においては、EVITA が IT 関連のセキュリティ規格である IEC/ISO 15408 (CC（Common Criteria）の CEM（Common Criteria for Information Technology Security Evaluation (2012)）を基にしているように、CC との調和を考慮したアセスメント基準を採用している例もある。

このことから、自動車のセキュリティのアセスメントには、様々なアセスメント基準が混在して利用されることが予想される。このような状況を鑑みつつ、複数の基準を利用する場合、個社別の基準を利用する場合などを考慮した、アセスメント方式を研究開発する。さらに、安全との相互の影響を考え、ASIL と ASecIL との併用方式などについても考慮する（図 2.1.4-1）。

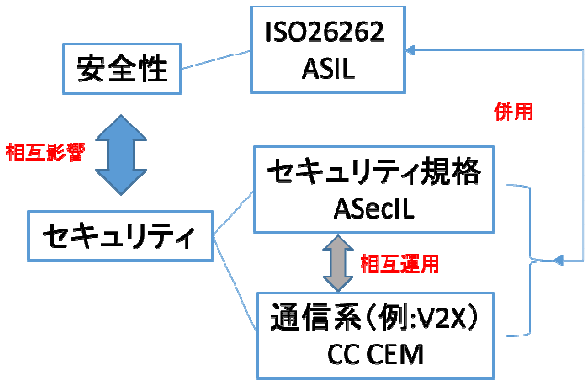


図 2.1.4-1　想定される脅威のアセスメント基準

2.1.5　共通セキュリティ要求

前述の脅威分析手法で同定された脅威に対して、対抗策としてのセキュリティ要求を導出する。さらに、セキュリティ要求が安全要求に対して影響を与えていないかどうかのトレードオフ分析の方法、安全分析プロセスとの相互影響を加味した要求導出方法の確立を目指す。例えば、安全分析と脅威分析のプロセスは以下の図 2.1.5-1 のように定義することも可能であり、このような脅威分析プロセスと安全側のプロセスは融合することが容易である。

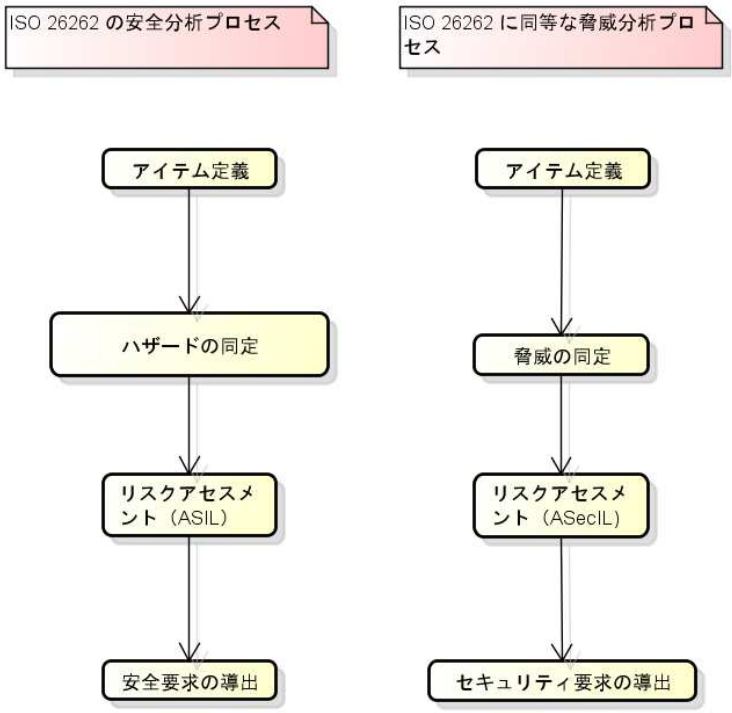


図 2.1.5-1　安全分析プロセス（ISO 26262）と同等なセキュリティ分析プロセス

さらに、アタックツリーの拡張であるアタックカウンターメジャーツリー（Attack Countermeasure Trees）を利用すると、攻撃に対する、検知機能と対抗策（セキュリティ要求）が同時に分析出来るという特徴があり、攻撃と対抗策（セキュリティ要求）の両方を同時に分析することが可能となる。（図 2.1.5-2）

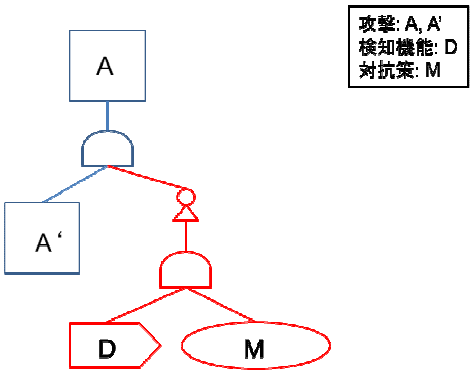


図 2.1.5-2　アタックカウンターメジャーツリーによる分析

このような手法を調査研究し、産業界で共通に利用可能な手法を開発する。

2.1.6 脅威分析共通プラットフォーム

「脅威分析共通モデル」に基づき、汎用脅威分析手法、共通脅威リスクアセスメントの方式を提供するツール「脅威分析共通プラットフォーム」を開発する。

本テーマでは、自動走行のシステムアーキテクチャ、ユースケースや脅威分析の技術、及び､自動車のセキュリティに関連する様々な研究プロジェクトについて調査を実施する。また、既にセキュリティ分野における研究で先行している IT 関連、制御機器関連のセキュリティ技術に関しても、自動走行への応用を考慮した場合に有益な情報となるかについて調査を行う。さらに、現在、公表されている自動車に対する攻撃方法についても調査する。

これらの調査結果を基に､「脅威分析共通モデル」のためのシステムアーキテクチャ、脅威分析手法の開発を行い、それを基に脅威分析を実施し、同定された脅威に対するセキュリティ要求を導出する。

さらに､「脅威分析共通モデル」を利用するためのツール「脅威分析共通プラットフォーム」の開発を行う。本プラットフォームを利用したケーススタディ､利用手引書を作成し、産業界において利用できるものとして準備する。最終的には、開発した「脅威分析共通プラットフォーム」で利用するのに適した脅威モデルを作成し、脅威モデルの評価と同時にツールの評価を実施する。

本年度は、まず、脅威分析を実施するために必要となるシステムアーキテクチャやユースケース、脅威分析手法等に関して、先行する事例の調査を実施する。

2.2　車両への攻撃に対する対策の評価手法・認証の調査・研究（テーマ②）

本テーマの目的は、自動走行時代のセキュリティ評価技術を確立し、セキュリティ対策の妥当性を評価することである。一般に、セキュリティ評価には、「評価対象」に対する評価技術の蓄積により「評価方法・評価基準」を策定しつつ、実評価のための「評価環境」の構築が必要となる（図 2.2-1）。テーマ②の「評価対象」を自動走行時代のセキュリティの重要性を鑑みて、車外連携システム、車内システム、コンポーネントとする。

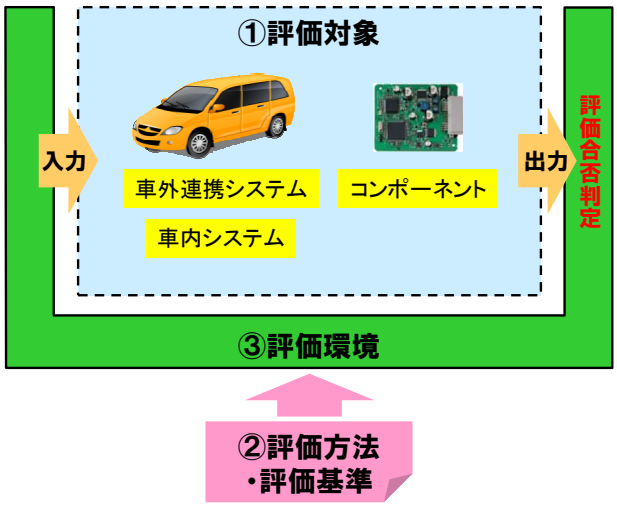


図 2.2-1　セキュリティ評価技術の 3 要素

2.2a　コンポーネント・車内システムにおける評価技術の検討（テーマ②a）

一般に評価基準は、提供サービス・システム構成・攻撃レベルの進化を踏まえた継続的な更新が必要である。自動走行時代の標準的なコンポーネントから車内システムにおいても同様であるため、評価技術の体系化が必要である。

これらの活動には以下の 3 点が重要である。

・自動走行時代の標準的なコンポーネントと車内システムの評価対象
・既存の評価知見と評価対象の実評価結果に基づく評価方法・評価基準
・前記評価基準を効率的に確認可能な評価環境

本テーマではセキュリティ評価の一般解を導き出すために、具体的なユースケースに基づいたセキュリティ対策ではなく、自動車の機能を一般化して検討する（図 2.2a-1）。

一般に、自動車にはお客様にご提供する主機能と、品質保証や機能確証に必要な特権機能が存在する。主機能は「走る・曲がる・止まる」などが代表例であり、アプリケーション依存のセキュリティ対策が求められる。一方、特権機能はソフトウェア更新（リプログラミング）やデバッグなどアプリケーション非依存となる。

従って、本テーマにおける車内システムは主機能が中心となり、コンポーネントは特権機能が主となる。

項目	定義	例	分類
主機能	自動車オーナが活用する機能	走曲止、高度運転支援	アプリ依存
特権機能	品質保証や機能確証に必要な機能	デバッグ、リプロ	アプリ非依存

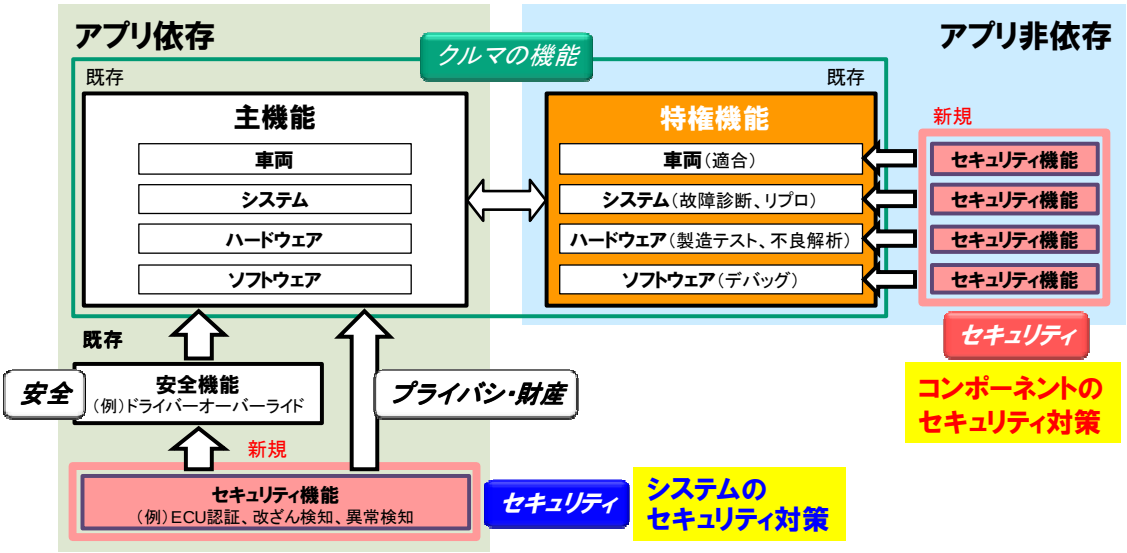


図 2.2a-1　自動車の機能とセキュリティ対策との関係

2.2a.1　評価対象の開発

標準コンポーネント（ECU）の機能は、特権機能の中でセキュリティ上、特に重要な「リプログラミング、デバッグ」を選択する。一方、ECU 内の部品仕様については、主要部品のマイコンはチップベンダに標準搭載されつつあるセキュリティ IP（SHE: Secure Hardware Extension）付きとする。またソフトウェアは AUTOSAR で検討中の BSW のセキュリティモジュールを搭載する。

標準システムの機能は、自律型自動走行システムを想定して、複数の ECU が車載 LAN 経由での連携制御とする。標準システムを実現する ECU は、平成 27 年度に開発する標準コンポーネントをベースに、平成 28 年度にセキュリティ機能を拡張する。

2.2a.2　評価方法・評価基準の開発

コンポーネントの評価方法・評価基準は、他業界のコンポーネントの評価技術動向と ECU との差分を踏まえて仮説を立てる。またこれまでの動向と将来予測も踏まえて、評価技術のロードマップを仮決めする。

一方、前記標準 ECU を用いた実評価の結果を考慮して、前記ドラフトを更新する。車内システムの評価基準も同様に、動向調査を元に仮説を立て、実評価結果を踏まえて更新する。

2.2a.3　評価環境の開発

評価対象に対する評価方法・評価基準を入力に、評価環境の仕様を開発する。本仕様は自動車業界において汎用性の確保と効率化が重要となる。特に主機能を守るシステムのセキュリティについては、自動車メーカや対象システム・ユースケースによって対策および評価が変わる可能性がある。有識者会議や WG で合意形成しながら仕様を確定する。

一方、評価環境の開発は、前記評価基準ドラフトより、評価インタフェースの CAN と JTAG に対するテストベクタを生成・入力し、その処理結果を出力・期待値と合否判定をする評価環境を開発する。

本テーマにおける 2.2a.1～2.2a.3 の開発目標を整理したものが以下の表 2.2a.3-1 である。

表 2.2a.3-1　コンポーネント・システムの開発目標

技術	内訳	開発目標	
2.2a.1 評価対象	自動走行時代の標準コンポーネント（ECU）と標準システム（車内システム）の開発	ECU	・機能：リプログラミング、デバッグ ・マイコン：セキュリティ IP（SHE）搭載 ・ソフト：AUTOSAR BSW
		車内 システム	・機能：複数 ECU が車載 LAN（CAN）経由で連携制御 ・ソフト：BSW のセキュリティ機能拡張、連携制御用サンプルアプリケーション
2.2a.2 評価方法・ 評価基準	評価技術動向調査と評価対象への実評価	ECU	・評価技術ロードマップ ・自動走行時代の評価方法・評価基準
		車内 システム	
2.2a.3 評価環境	効率的な評価環境の開発	ECU	・評価先：CAN、JTAG ・評価基準：ECU
		車内 システム	・評価先：CAN ・評価基準：車内システム

ECU: Electronic Control Unit, IP: Intellectual Property, SHE: Secure Hardware Extension,
BSW: Basic Software, LAN: Local Area Network, CAN: Controller Area Network,
JTAG: Joint Test Action Group

2.2a.4　テストベッドの開発

2.2a.1～2.2a.3 の活動および欧米の動向および国内自動車メーカーのニーズを踏まえて、車業界として恒久的なテストベッドの必要性を検討する。テストベッドが必要な場合は、恒久組織における評価の試行をする。なお、テストベッドの開発目標は、3 年目に 2.2a.1～2.2a.3 の開発状況と車業界のニーズを踏まえて設定する。

2.2b　車外連携システム・車両レベルにおける評価技術の検討（テーマ②b）

本テーマは、以下の手順で実施する。

①自動走行を行うシステムを仮定し、そのシステムに想定されるサイバー攻撃の事例をICT分野での事例を収集することで推定する。
②対策すべきセキュリティポイントおよび対策技術の評価指針・指標について研究・開発・検証を行う。
③検証結果から対策技術の評価指針・指標について見直しを行い、フィードバックを踏まえた上でガイドラインの作成を行う。

なお、サイバー攻撃については日々変化・高度化していることから、進め方や評価指標等については状況に応じて随時検証・見直しを実施する。

2.2b.1　他業界におけるセキュリティ情報の共有状況・管理方法の調査

サイバー攻撃の事例は機微な情報であるため単純に収集・共有することは難しい。このため、他業界でどのように扱われているかの事例について聞き取り調査を実施し、共有化の可能な範囲（収集対象）、維持・管理方法の現状についてまとめる。

2.2b.2　自動走行を行うシステムの選定

自動走行の共通モデルの構築について別途検討が行われるが、ひとまず仮定として「平成26年度次世代高度運転支援システム研究開発・実証プロジェクト」において用いられている自動走行システムのアーキテクチャを採用して進め、テーマ①の共通モデルの検討が進み次第、そちらのシステムモデルに合わせる。

2.2b.3　想定されるサイバー攻撃の事例収集

中立的な研究機関などと協力し、ICT での攻撃事例を元に 2.2b.2 のシステムに想定されるサイバー攻撃の事例を収集する。このとき ICT での対策事例についても合わせて収集する。この活動についてはひとまず初年度時点で一旦まとめ作業を実施するが、事例収集の活動は継続的に実施する。

この収集する情報の取り扱いについて、2.2b.1 の調査結果を基に管理方法などにおける要件・課題を検討し，恒久的な維持組織のあり方などを検討課題としてまとめる。

2.2b.4　対策すべきポイントとその評価指針の仮定

2.2b.3 で得られる ICT 分野での知見に基づいて、自動車としての各部分の重要性や機能安全との関係性を意識しながら各ポイント（系やユニットなどを想定）での評価基準（応答速度、検知率などを想定）を仮定する。

2.2b.5　対策技術の評価指針・指標についての実証実験

別途進められる自動走行の共通モデルとの整合性を図りながら、実機での実証実験として以下を実施する。

①2.2b.2の模擬装置を構築する。

②2.2b.3の事例に相当するサイバー攻撃を、2.2b.1で構築した装置に対して実施する。

2.2b.6　仮説検証と実証結果のフィードバック

2.2b.5 の結果を分析し、2.2b.4 で仮定した指針の見直しを実施する。2.2b.4 と 2.2b.5 を 2 回実施することで精度の向上を目指す。

2.2b.7　ガイドラインの作成

2.2b.4～2.2b.6 の結果を踏まえて、共通モデルにおける各評価ポイントでの評価基準のガイドラインをまとめる。

2.2c　車内通信プロトコルの仕様に基づく評価方法の検討（テーマ②c）

自動走行に向けて運転支援システム等が高度化することに伴い、これまで以上に車両内の ECU やセンサ等のコンポーネントが協調動作することの重要性が増してくる。この協調動作には車内のネットワークが欠かすことができず、当該ネットワーク上の通信プロトコルがより重要な役割を担い、車内で多く利用されると考えられる。そのため、自動車に対するサイバー攻撃により、車内ネットワークの通信プロトコルがどのような影響を受けるかを明らかにすることは、自動走行時代の車両のセキュリティ対策に必要である。

本テーマでは、自動走行のための制御に関わる車内ネットワークの通信プロトコルを中心に、通信プロトコル仕様及びアプリケーションにおける処理方法の観点から、攻撃方法の調査及び評価方法・評価基準の検討を実施する。また、攻撃方法の調査及び評価方法・評価基準の検討結果を基に、通信プロトコルに対するセキュリティ対策が攻撃の耐性を有しているかを調べるための評価方法を用いた評価環境をシミュレータにより開発する。

2.2c.1　車内通信プロトコル、アプリケーションにおける処理方法及び既存の攻撃方法の調査

以下の項目に関して、公開情報を基に調査を実施する。

・各通信プロトコル仕様の調査

・各通信プロトコルのアプリケーションにおける処理方法の調査

・各通信プロトコルのセキュリティの観点からの脆弱性及び攻撃方法の調査

2.2c.2　評価方法・評価基準の検討の実施

以下の観点から、評価方法・評価基準の検討を実施する。また、検討結果を基に、シミ

ュレータでの評価が有効であるかを整理する。
・通信プロトコルの仕様の特徴を利用する。
・通信プロトコルのアプリケーションにおける処理方法の特徴を利用する。
・通信プロトコルのネットワーク構成やネットワークアクセス方式の特徴を利用する。

2.2c.3　シミュレータによる評価方法を用いた評価環境の開発

上述の 2.2c.1 及び 2.2c.2 における攻撃方法の調査及び評価方法・評価基準の検討を行った結果、シミュレータでの評価が有効であると判断した評価方法に関して、セキュリティ対策の攻撃に対する耐性の有無を調べるための評価方法を用いた評価環境をシミュレータにより開発する。

2.2d　実機を用いた評価の実施（テーマ②d）

コンポーネント、システム、車両、およびモビリティ社会の各要素に対して攻撃を行う際には、車載システムに対する既知の攻撃を中心に、一般的な組み込む機器に対する攻撃なども含める必要がある。

本テーマでは､自動車オーナ主導による車両運行など平常時のサービスである主機能と、メーカ主導による車両点検など特殊用途向けのサービスである特権機能に着目し、それぞれのケースにおける攻撃方法を検討する。また評価技術開発への成果展開を意識し、実施のための難易度や影響などを、攻撃毎に導き出す。

2.2d.1　コンポーネントを対象とした攻撃方法の調査

以下の項目に関して、テーマ②a および関係各所と連携しながら調査を実施する。
・コンポーネントの仕様と想定される攻撃の調査
・コンポーネントに対する攻撃側のプロファイル調査
・コンポーネントを対象とした攻撃の実施
・コンポーネントに対する攻撃結果の考察と展開

2.2d.2　システムを対象とした攻撃方法の調査

以下の項目に関して、テーマ②a および関係各所と連携しながら調査を実施する。
・システムの仕様と想定される攻撃の調査
・システムに対する攻撃側のプロファイル調査
・システムを対象とした攻撃の実施
・システムに対する攻撃結果の考察と展開

2.2d.3　車両を対象とした攻撃方法の調査

以下の項目に関して、テーマ②a、②b および関係各所と連携しながら調査を実施する。
・車両の仕様と想定される攻撃の調査

・車両に対する攻撃側のプロファイル調査
・車両を対象とした攻撃の実施
・車両に対する攻撃結果の考察と展開

2.2d.4　モビリティ社会を対象とした攻撃方法の調査

以下の項目に関して、テーマ②a、②b および関係各所と連携しながら調査を実施する。
・モビリティ社会の仕様と想定される攻撃の調査
・モビリティ社会に対する攻撃側のプロファイル調査
・モビリティ社会を対象とした攻撃の実施
・モビリティ社会に対する攻撃結果の考察と展開

2.2e　第三者認証に関する調査（テーマ②e）

IT 業界等においては、情報セキュリティに関する第三者認証として、CC（Common Criteria）認証が知られている。CC は情報セキュリティに関する評価基準の規格であり、国際的に用いられている。また、CC 認証以外にも、それぞれの機器の相互接続性を確認するなどの認証が行われているケースもある。

本テーマでは、他業界における第三者認証制度について調査を行うとともに、認証に関する海外の動向についても調査を行い、自動車のセキュリティにおける認証のあり方について検討を行う。第三者認証が必要と考えられる場合には、認証を行うための機関についても検討を行う。

2.2e.1　他業界における第三者認証の現状調査

・他業界における第三者認証機関へのヒアリング調査

2.2e.2　自動車のセキュリティへの適用の検討

・他業界における認証対象と自動車における対比
・自動車セキュリティへの第三者認証の妥当性検討

2.2e.3　第三者認証機関の検討

・認証すべき対象の検討
・認証を実施するために認証機関に求められる要件の整理

2.3　V2X 通信における署名検証の簡略化の研究（テーマ③）

本テーマでは、V2X 通信の実用化を図る上での課題解決のひとつとして署名検証の簡略化（図 2.3-1）を挙げている。

本年度、簡略化方式開発に係る机上評価を実施、方向性を明らかにすることとし、この成果を受け来年度以降、通信評価や実装評価等を行いながら自動走行セキュリティ共通モデルの進捗状況を踏まえ、実際の運用システムに近い形でのモデル検討を重ねていくこととする。

また、国内外での署名検証に係る標準化動向をウォッチし、国際協調を図りながら標準化検討も推進することとする。

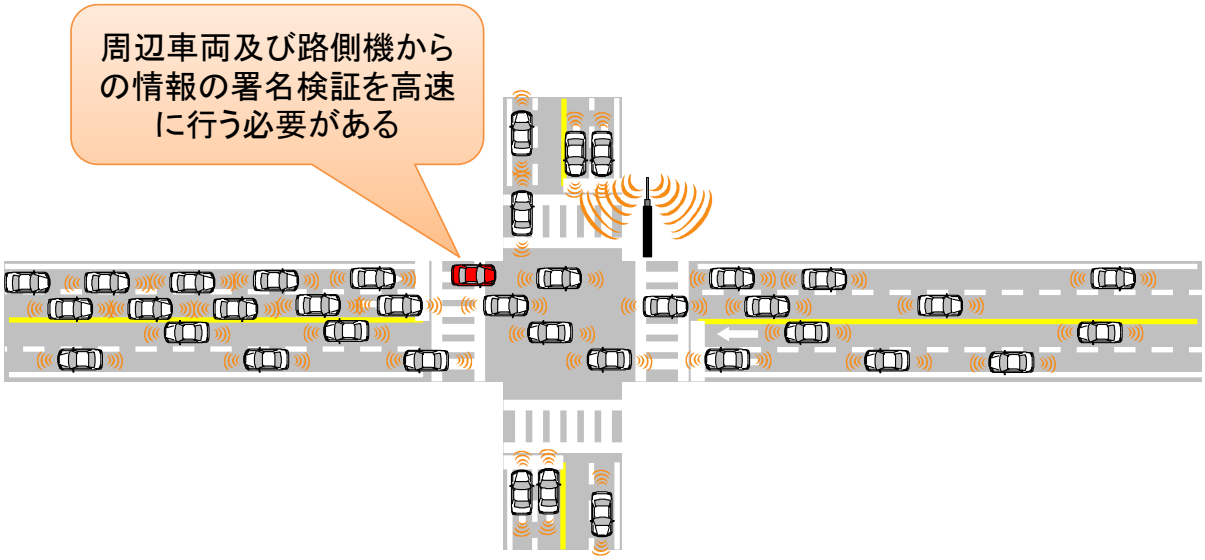


図 2.3-1　V2X 通信における署名検証簡略化概念図

4 年間の事業概要について以下に示す。なお、検討にあたっては、国内外の動きや他テーマの検討状況に十分留意することとし、進め方等について必要に応じ見直し等を加えるものとする。

2.3.1　簡略化方式開発

① 机上評価

以下の実施内容ポイントに基づき机上検討を行う。

・V2X通信の処理時間の調査
・V2X通信における署名検証の簡略化方式の調査
・署名検証簡略化方式の評価と分析
・調査結果まとめ

② 通信評価

簡略化方式検討での評価に基づいた「署名検証簡略化方式」に対し、車車間および路車間での通信評価を実施する。

③ 実装試験

セキュリティ処理部を実装した機器にて、必要な性能試験等を行うこととする。

④ 総合検証試験

実運用システムに近い模擬環境下での検証試験を行うこととする。

2.3.2 標準化活動

署名検証簡略化検討の検討成果を踏まえ、国内外における動向を調査の上、国際協調活動等を推進し、必要な事項の標準仕様化策定を図るものとする。

2.3.3 V2X 運用検討

① 運用方式検討

自動走行の共通モデル検討やセキュリティ運用全般の検討進捗との整合性を図りながら署名検証の運用方式について検討する。

② 運用システム試作試験

上記、運用方式検討に基づいた模擬運用システムモデルを構築し、署名検証性能試験を行う。

2.4　V2X セキュリティに関する海外の仕様や技術動向に関する情報共有（テーマ④）

2.4.1　海外の動向調査

V2X セキュリティ技術に関する海外の動向調査として、V2X 関連の海外のプロジェクトの最新状況を WEB 等で確認するとともに、フォーラム等が開催されている場合には参加しての調査を検討する。また、技術動向の調査としては、V2X を含む自動車セキュリティに関する国際会議等をリスト化し、公表されている情報から参加要否等を検討し、必要であり、参加可能な場合は参加して調査を実施する。

2.4.2　情報共有の仕組み構築

2.4.1 で調査した結果については、海外向け V2X 通信システムに関する製品を製造する事業者や、自動車セキュリティを扱うコンサルタント等をメンバーとする情報共有の会議体を立ち上げる。海外の情報収集に当っては、これらのメンバーによる国際会議の参加も検討する。

以上、4 年の事業実施期間を想定した研究・開発の内容について説明した。自動車業界にとって、セキュリティは本格的な取組みが始まったところであり、セキュリティ技術や考え方で先行する他業界の知見を有効活用することが重要である。平成 27 年度は、主に、自動車業界においてこれまでに実施されたプロジェクトや、他業界での事例等の調査などを実施した。第 3 章に平成 27 年度に実施した事業内容について説明する。

第 3 章　事業内容

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

自動運転システムでは、従来は考える必要が無かったサイバーセキュリティへの対応が不可欠となっている。サイバーセキュリティへの対策を行うためには、対象システムにどのような脅威があり、どの程度のリスクがあるかを見積もる必要がある。その具体的方法として、図 3.1-1 で表されるプロセスを利用するのが一般的である。このプロセスでは、まず、セキュリティの対策がなされていない対象システムのユースケース、アーキテクチャなどの前提条件を明確化することから始める。これらの明確化された前提条件により、対象システムのアタックサーフェイス、保護資産を洗い出し、脅威を同定していく。さらに、これらの情報は同定された脅威のリスク評価に利用する。このような分析結果を基に、どのようなセキュリティ対策が、どこに必要かを検討することで、セキュアなシステムアーキテクチャの設計が可能となる。

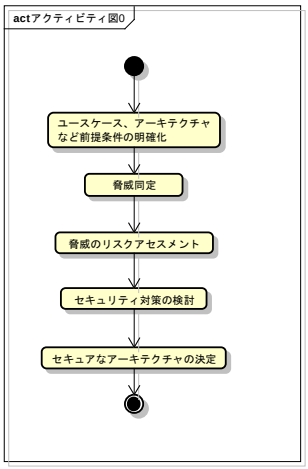


図 3.1-1　脅威分析プロセス

自動運転システムは、様々な国、企業において研究開発されており、多種多様な前提条件や分析手法によりセキュリティ対策が実現されている。しかし、自動運転システムの基本システム部分は共通していると考えられる。

本事業では、この自動運転の共通部分について、その前提条件、分析手法、リスク評価方法、対抗策として、自動車業界が共通して使うことのできる自動運転のシステムアーキテクチャ、ユースケースを構築し、これと合わせて検討を進める汎用脅威分析手法、共通脅威リスクアセスメントを用いて、自動運転システム全体のセキュリティ対策の要件を導出することを目的としており、平成 27 年度は、そのための先行事例調査を実施した。

3.1.1　セキュリティオントロジー（セキュリティの概念体系）

セキュリティの概念は様々な用語により表現されているが、用語の理解にズレが生じていると分析や評価が正しく行えない可能性が高くなる。本節では調査を通じて得られた脅威分析の用語を整理し、その関係のモデル化を実施した。モデル化によって、用語間の関係が明確になり共通理解を得やすくなると考えられる。

(1) 脅威分析の用語一覧

今回の調査対象で用いられている用語について検討した。各用語は調査対象で明確に定義されていなかったり、定義がずれていたりする。そのため、NIST SP 800-30 (Guide for Conducting Risk Assessments) [1]に対応する用語がある場合は、NIST SP 800-30 の定義を採用する。その場合でも、定義が本報告の中で使用する意味と異なる定義である場合は採用せず、以下の方法で定義した。本報告の意味と異なる場合や NIST SP 800-30 に対応する用語がない場合は、調査対象の定義を採用する。ただし、明確に定義がされている場合に限ることとした（ここでは「保護資産」、「アタックサーフェイス」、「攻撃者」が対象となる）。それ以外の用語は、その用語が使用されている調査対象の文脈より定義した（ここでは「格納場所」と「影響」が対象となる）。用語とその説明の一覧を表 3.1.1-1 に示す。

表 3.1.1-1　用語一覧

用語	説明
保護資産	脅威により脅かされる対象。
格納場所	保護資産の存在する場所。
アタック サーフェイス	攻撃者が攻撃を加える場所。 トラストバウンダリ、攻撃の入口とも表現される。
脅威	システムに対し、望まない結果をもたらす、あらゆる状況または事象。
攻撃者	攻撃を実施する可能性のある人、モノ。
攻撃	情報システム資源または情報自体の収集、混乱、否認、機能低下、または破壊を試みる、あらゆる種類の悪意のある活動。
動機	攻撃者（人）が攻撃をする理由。 攻撃によって得られる利益などが対応する。
脆弱性	システムなどに存在する、攻撃者に使用される可能性がある弱点。
影響	脅威によって引き起こされる望まない結果。 安全性、プライバシー、運用、財務、生産性、法律遵守などがある。
対象システム	脅威分析を実施する対象。
対抗策	脅威へ対抗する方法。脅威のリスクを低減する。
リスク	脅威の影響の大きさのレベル。 複数のパラメータにより決定されるのが一般的。

(2) 用語の関係のモデル化

前節で列挙した用語間の関係を、主にオブジェクト指向分析や設計のために用いられるUML（Unified Modeling Language）のクラス図を用いて表現したものが図 3.1.1-1 である。

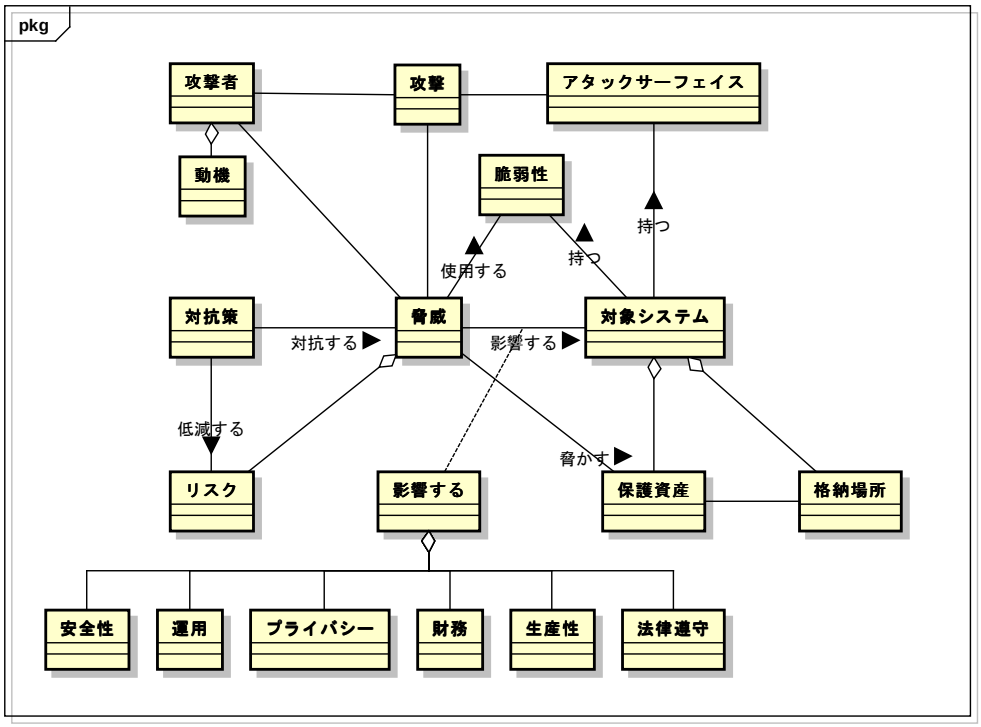


図 3.1.1.-1　脅威分析で使用される用語の関係

本モデルは「脅威」を中心として作成されている。「脅威」が脅かす対象である「保護資産」は「対象システム」の部分として存在しており、「対象システム」のもう一つの部分である「格納場所」と関係している。また、「脅威」は「対象システム」に対し「影響する」。ここでは、影響の種類として、調査した分析手法で取り上げられている「安全性」、「運用」、「プライバシー」、「財務」、「生産性」、「法律遵守」を記述している。その他の種類も今後、取り上げる必要があると考えられる。

次に「脅威」を引き起こすのは「攻撃者」であり、その活動である「攻撃」も「脅威」と関連している。また、「攻撃」を加える場所である「アタックサーフェイス」もモデル化されている。最後に「脅威」は「リスク」を持ち、その「リスク」を低減し、「脅威」へ対抗するものが「対抗策」である。

3.1.2　自動運転の共通システムアーキテクチャ

脅威分析を実施する際には、例えば攻撃者がどこから攻撃するか、何を攻撃するかを検討しなくてはならない。そのため、対象システムにおいてどのようなコンポーネントが、どのように接続されているかを明確にする必要がある。共通モデルにおいても、脅威分析の対象となるシステムアーキテクチャの明確化が必要である。このシステムアーキテクチ

ャの案として、本事業において検討中のものを共通システムアーキテクチャとして仮定し、その内容の評価を他のシステムアーキテクチャとの比較により行う（以下、検討中の案を共通システムアーキテクチャ案と呼ぶ）。

本節では、共通システムアーキテクチャ案が、脅威分析の前提条件として十分利用可能であるかを評価した結果を説明する。評価は、現在提案されている様々な自動運転システム（またはそれに準じたシステム）のシステムアーキテクチャを調査し、それらとの対応関係を明確にし、その過不足を検討した。調査対象は以下の 3 件である。

・EVITA[2]
・IPA 自動車の情報セキュリティへの 取組みガイド[3]
・本事業の着手時に仮定したアーキテクチャ

一方で、セキュリティ機能として様々なものが提案されており、それに伴いセキュリティ機能を実装したアーキテクチャも、いくつかのものが提案されている。現在提案されているセキュリティ機能の実現方法をアーキテクチャの観点から調査・分類を行った。

(1) 自動運転のために検討されているアーキテクチャ

自動運転に関しては様々な機関で研究が行われており、アーキテクチャに関してもそれぞれの研究によって差異がある。本節では公開されている自動運転（またはそれに準ずる）システムのアーキテクチャを調査し、それぞれの概要を示す。

① EVITA

EVITA[2]では以下の図 3.1.2-1 に示すアーキテクチャが提案されている。

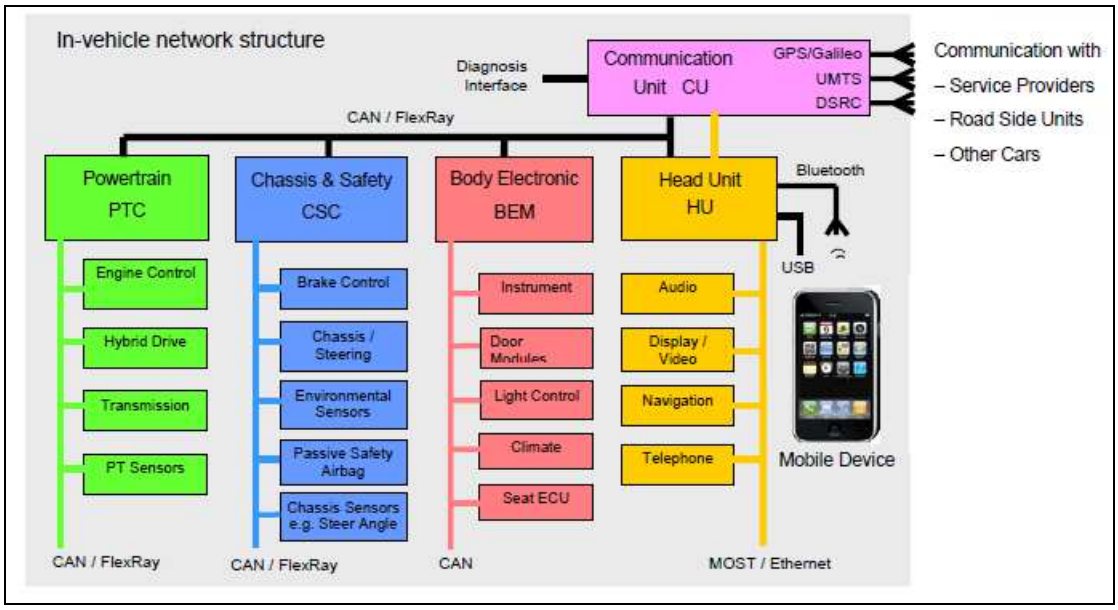


図 3.1.2-1　EVITA のアーキテクチャ（[2] Figure 6 より）

各機能はパワートレイン系（PTC (Powertrain Controller)の系統）、シャシ系（CSC (Chassis System Controller)の系統）、ボディ系（BEM (Body Electronic Module) の系統）、ヘッドユニット（HU (Head Unit)の系統）とコミュニケーションユニット（CU (Communication Unit)）に分類され、それぞれの系統ごとにネットワークが分割されている。また、各系統は domain control unit（PTC、CSC、BEM、HU）を介して、一つのバックボーンバスでつながり相互に通信が可能となっている。外部接続は CU と HU のみに限られている。

EVITA で提案されているアーキテクチャは、コンポーネントがどのような通信経路（Controller Area Network (CAN) や FlexRay など）でどのように接続されているか、どのような外部通信経路があるか、といった内容が明確になっており、脅威分析に必要となる情報が十分明確化されている。さらに、外部通信の相手先も明確になっており、詳細な脅威分析の実施が可能となっている。

② IPA

IPA 自動車の情報セキュリティへの 取組みガイド[3]においては図 3.1.2-2 に示すアーキテクチャが提案されている。

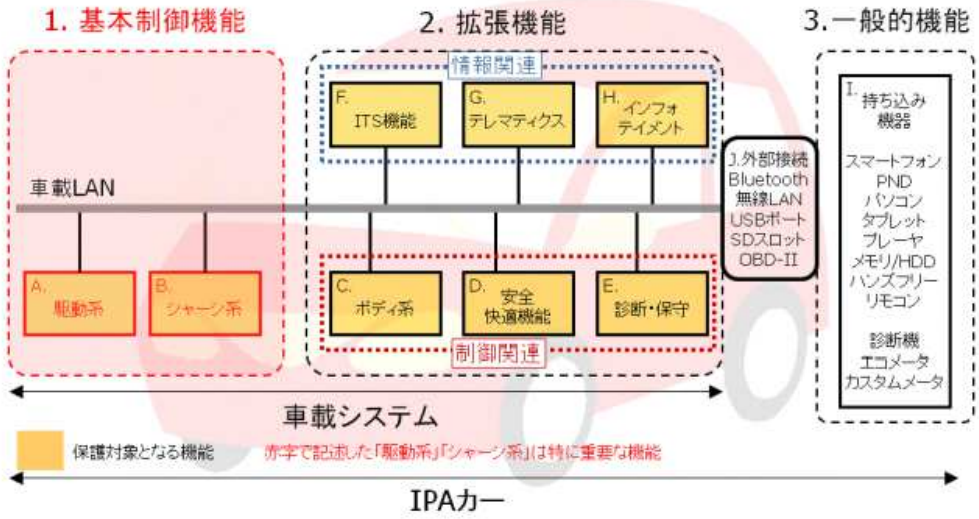


図 3.1.2-2　IPA で提案されているシステムアーキテクチャ（[3] 図 2-2 より）

EVITA のアーキテクチャ（図 3.1.2-1）と同様に系統ごとに機能が分類されており、それらが車載 LAN で接続されている。各系統間で直接通信が可能となるアーキテクチャと考えられる。外部との通信は「J. 外部接続」で Bluetooth、無線 LAN、USB、SD スロット、OBD-II (On-Board Diagnostics)で通信される。さらに、図 3.1.2-2 のアーキテクチャ図には明記されていないが、「G. テレマティクス」には携帯電話回線やスマートキーとの無線通信、「F. ITS 機能」には DSRC (Dedicated Short Range Communications)による通信接続、「H. インフォテイメント」には携帯電話回線といった外部接続があると説明されている。明確に通信を行わないのは、駆動系、シャシ系、安全快適機能、診断・保守の 4 つの系統である。

本アーキテクチャ図では、ITS 機能の DSRC のように、外部通信経路の中に明確になっていないものが存在している。さらに、外部通信経路と通信相手先の関係も明確にされていないため、アタックサーフェイスを特定することが難しい。そのため脅威分析に用いるには不十分であると考えられる。

③ 本事業の着手時に仮定したアーキテクチャ

本事業では、図 2-1 に示す階層構造を仮定して、評価技術の検討等に取り組んでいるが、このうち、脅威分析に関連するアーキテクチャ部分を図 3.1.2-3 に抽出した。

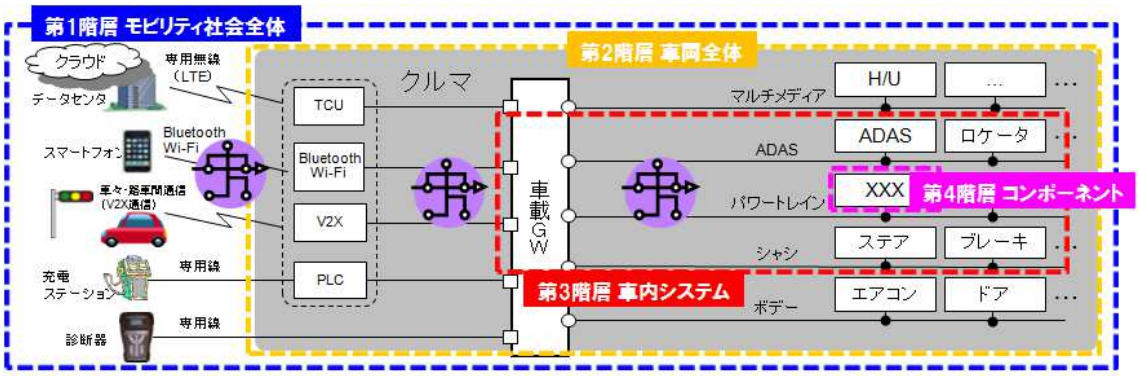


図 3.1.2-3　本事業で仮定したアーキテクチャ（図 2-1）からの抜粋

本アーキテクチャは車載 GW（通信用ゲートウェイ（Gateway））を介して各系統が通信を行えるようになっている。外部通信経路は全て車載 GW を介して行われている。また、各外部通信の相手先も明確になっており、アタックサーフェイスの同定に十分な情報が明確化されている。

一方で、パワートレイン系など機能が詳細に記載されていない部分もあり、そのため十分な脅威が同定できない可能性がある。

(2) 共通システムアーキテクチャ案との比較

本節では、現在検討中の共通システムアーキテクチャ案（図 3.1.2-4）と、調査したアーキテクチャの対応関係について説明する。

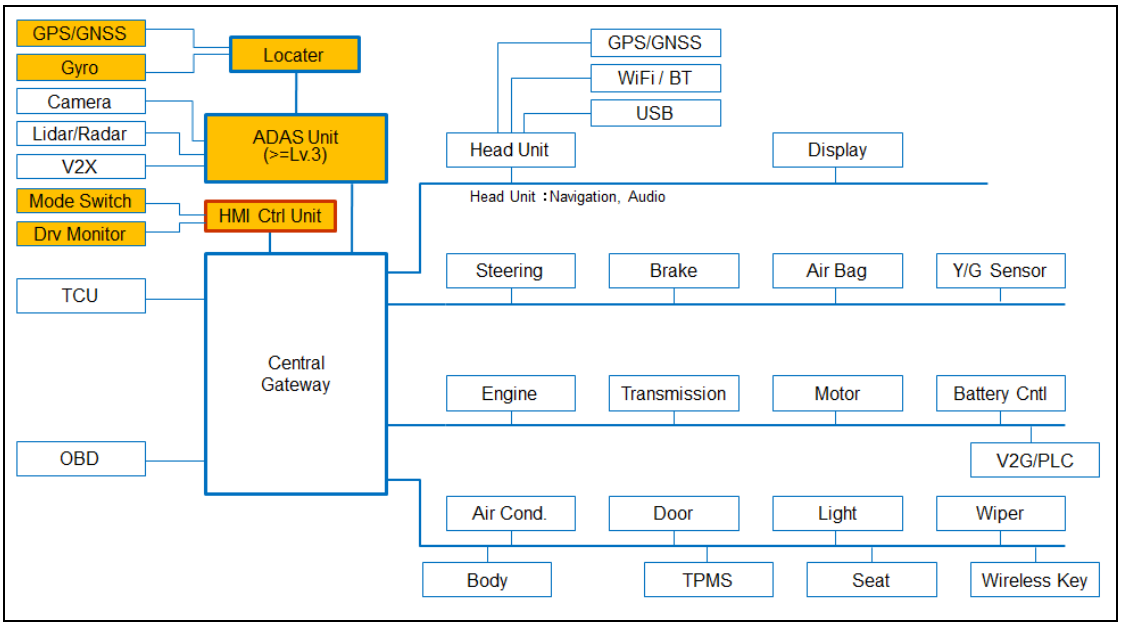


図 3.1.2-4　共通システムアーキテクチャ案

上記共通システムアーキテクチャ案と調査したシステムアーキテクチャの対応を、ECU の機能の分類、外部通信経路、ECU のつながり方という観点から明確にする。

【ECU 機能の分類】

共通システムアーキテクチャ案では以下の分類となる ECU が明確化されている。

・ADAS (Advanced Driver Assistant System)
・HMI (Human Machine Interface) control unit
・Head Unit 系（インフォテイメント）
・シャシ系
・パワートレイン系
・ボディ系
・セントラルゲートウェイ（各系統の接続を集約）

これらと調査したアーキテクチャの ECU の分類間の対応関係を表 3.1.2-1 で示す（表中の〇は対応するものがあることを意味する）。

表 3.1.2-1　ECU 分類の比較表

共通システム アーキテクチャ案	EVITA	IPA	本事業での仮定 （図 3.1.2-3）
ADAS	なし（ただし、シャシ系に Passive safety がある）	なし（ただし、安全快適機能が一部を担う可能性がある）	○
HMI control unit	なし	なし	なし
Head Unit 系（インフォテイメント）	○	○（インフォテイメントとして存在）	○
シャシ系	○（ただし Air bag はない）	○（詳細は無し）	○
パワートレイン系	○（ただし V2G (Vehicle to Grid)、PLC (Power Line Communication)はない）	○駆動系として存在（詳細は無し）	○（PLC はセントラルゲートウェイへ入力されている）
ボディ系	○（TPMS (Tire Pressure Monitoring System)、Air Conditioner はない）	○（詳細は無し）	○
セントラルゲートウェイ	なし（ただし、Communication Unit と各系統へのゲートウェイが相当すると考えられる）	なし	○

【外部通信経路】

共通システムアーキテクチャ案で確認できる外部通信経路は以下のとおりである。

・GPS/GNSS: ADAS Unit の Locater で接続
・V2X: ADAS Unit で接続
・TCU (Telecommunication control unit): セントラルゲートウェイで接続
・OBD (On-board diagnostics): セントラルゲートウェイで接続
・WiFi/BT (Bluetooth): Head Unit で接続
・USB: Head Unit で接続
・V2G/PLC: パワートレイン系のバスに接続
・Wireless Key: ボディ系のバスに接続
・Mode Switch 及び Drv Monitor: ドライバからの入力

これらと調査したアーキテクチャの外部通信経路との対応関係を表 3.1.2-2 に示す。

表 3.1.2-2　外部通信経路の比較表

共通システム アーキテクチャ	EVITA	IPA	本事業での仮定 （図 3.1.2-3）
GPS/GNSS	Communication Unit に接続している。	明確に記載はないが、ITS 系で接続していると考えられる。	なし。
V2X	Communication Unit に接続している。	図では明確に記載されてないが、ITS 系で接続している。	セントラルゲートウェイに通信モジュールを介して接続（通信相手先も記載されている）。
TCU	Communication Unit に接続している。	図では明確に記載されてないが、テレマティクスで接続している。	セントラルゲートウェイに通信モジュールを介して接続（通信相手先も記載されている）。
OBD	Communication Unit に接続している。	車載 LAN に直接つながっている外部接続に、接続されている。	セントラルゲートウェイに接続（通信相手先も記載されている）。他の通信と異なり、直接セントラルゲートウェイに接続されている。
WiFi/BT	Head Unit に接続している。	車載 LAN に直接つながっている外部接続に、接続されている。	セントラルゲートウェイに通信モジュールを介して接続（通信相手先も記載されている）。
USB	Head Unit に接続している。	車載 LAN に直接つながっている外部接続に、接続されている。同様の外部接続として SD スロットも定義されている。	なし。
V2G/PLC	なし。	なし。	セントラルゲートウェイに通信モジュールを介して接続（通信相手先も記載されている）。
Wireless Key	なし。	図では明確に記載されてないが、ボディ系で接続している。	なし。
Mode Switch 及び Driver Monitor	なし。	なし。	なし。

【ECU のつながり方】

詳細度に差があるものの、共通システムアーキテクチャ案、調査したアーキテクチャ共に、機能によって分類され、分類された系統ごとに接続されている。共通システムアーキテクチャ案にはセントラルゲートウェイが存在しており、本事業提案書のアーキテクチャ（図 3-3）に最も近い。EVITA（図 3.1.2-1）でも Communication Unit および各 Bus の domain control unit を合わせてセントラルゲートウェイとみなすことにより、同様の接続と考えることができる。一方で IPA（図 3.1.2-2）は持込み機器などに関しては外部通信がセントラルゲートウェイと同様の役割を持つと考えられるものの、その他の図に明記されていない外部通信経路において、ゲートウェイに対応するものが存在しているかは不明確となっている。

(3) 共通システムアーキテクチャ案についてまとめ

以上の調査結果と対応関係の明確化から、共通システムアーキテクチャ案についての考察を述べる。

共通システムアーキテクチャ案には、調査したアーキテクチャで明確化されている情報とほぼ同様の情報が明確化されている。具体的には、どのような ECU がどのように接続されているか、センサも含めた外部通信がどこで行われているかが明確になっている。また、ドライバとのインターフェイス、Wireless key の通信経路、いくつかのセンサや ECU は、他のアーキテクチャでは不明確（または存在していないもの）であるが、共通システムアーキテクチャ案では明確なため、より詳細な脅威分析が実施可能になると考えられる。

一方で、EVITA（図 3.1.2-1）で明確になっている CAN や FlexRay といった通信経路の種類、EVITA および本事業での仮定（図 3.1.2-3）で明確になっている外部通信の相手先、これら二つの情報は共通システムアーキテクチャ案では明確になっていない。これらの情報を明確化することで、より詳細な脅威分析の実施が可能になると考えられる。

さらに、共通システムアーキテクチャ案ではドライバとのインターフェイスが考慮されている。これは、自動運転のレベル 3 (SAE)で必要とされるドライバのモニタリングや自動運転の切り替えスイッチである。この考え方をさらに進め、ドライバからの制御のインプットもアーキテクチャ図に導入することを推奨する。これは ISO 26262[4]、MISRA[5]で提案されている自動車の制御モデルである Driver in the Loop の考え方を導入するものである。完全自動運転以外では何らかの形でドライバが制御に関与するため、この制御モデルを使用することとなる。脅威分析を実施する際においてもドライバがシステムに対しどのように関与するかを明確することで、より詳細な脅威分析が実施可能になると考えらえる。

(4) 現在検討されているセキュリティ機能を実装したアーキテクチャ

現在、様々な方法による自動車への攻撃が報告されており、そのような攻撃から自動車を守るために様々なセキュリティ機能が提案されている。本節では、現在提案されているセキュリティ機能を調査し、どのようなアーキテクチャで実現されているか、その分類を行う。

① TCG TPM 2.0 Automotive Thin Profile

Trusted Computing Group（TCG: コンピュータの信頼性、安全性を向上させるための技術の標準化を行っている業界団体）では各車載 ECU にセキュリティのモジュールを追加するアーキテクチャ[6]が提案されている。これは、すでに一般のコンピュータなどに対して普及している、Trusted Platform Module（TPM）を各 ECU で利用するものである。ただし、以下の図 3.1.2-5 で示す通り、全ての ECU に一様に同じモジュールを利用するのではなく、外部との通信の入り口となる Head Unit や車載 GW 部分にはより高機能なもの（Auto-Rich TPM）を、それ以外の各 ECU にはより簡易なもの（Auto-Thin TPM）を利用することを提案している（ただし、すべての ECU で Auto-Thin TPM を利用することも想定されている）。

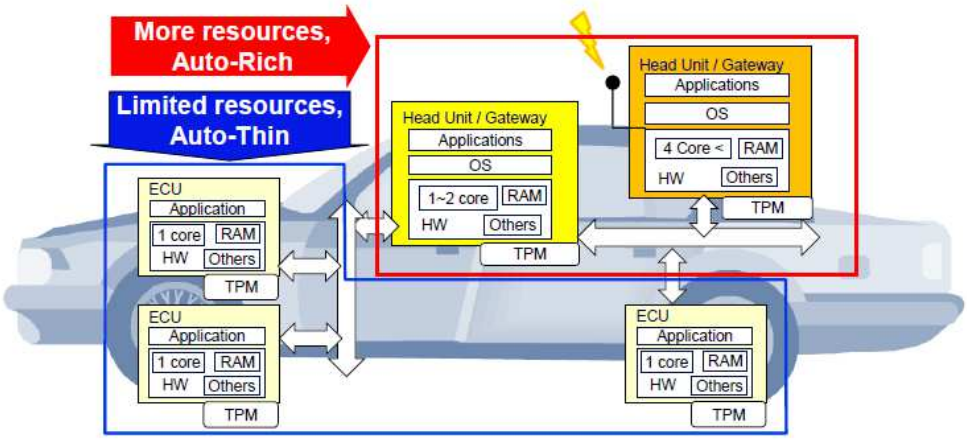


図 3.1.2-5　TPM Auto-Rich および Auto-Thin を利用した例（[6]の Figure 2 より抜粋）

Auto-Rich と Auto-Thin を併用し、Head Unit/車載 GW が自動車内の ECU の署名を検証することにより、通信の相手先では Head Unit/車載 GW の署名のみを検証すればよくなる。また、自動車内の ECU に不正なものがある場合は、Head Unit/車載 GW の Auto-Rich TPM で検出し、Remote Center などへ報告される。

この方式を利用することで、通信相手先の負荷は減るが、Head Unit/車載 GW の Auto-Rich TPM にリソースが必要となる。

② 論文発表されているセキュリティ機能

(ⅰ) 車載制御システムを保護するセキュリティ技術（escar Asia 2015）[7]

車載ネットワークのセキュリティ対策における、短期から長期にかけての取り組みとして、パナソニックにおけるアプローチを紹介している。短期的には外部通信経路となるECU で検知率の高いフィルタリング機能を実装する方法を提案しており、長期的にはECU ごとにメッセージ認証機能を付加することを提案している。その間の中期的なアプローチとしては、不正メッセージを検知・阻止するセキュリティ ECU を導入する方法を提案している。

不正メッセージは複数のフィルタリングにより検知され、エラーフレームを送信することにより阻止を行う。これは、短期的なアプローチであるフィルタリング機能より高度なセキュリティ機能が実装されており、長期的なアプローチであるメッセージ認証方式より低コストで導入可能な方法である。

(ⅱ) 車載ネットワークのセキュリティ監視システム（SEI テクニカルレビュー第 187 号）[8]

CAN のなりすまし攻撃に対する脆弱性に対処するために、メッセージ認証コードを用いたセキュリティ対策が提案されている。提案されている手法では、各 ECU でメッセージ認証コードを付加し、監視 ECU でその検証を行い、なりすましが発見された場合にはエラーフレームにより不正メッセージを上書きが実施される。

この手法では、セキュリティ ECU の追加と各 ECU へのセキュリティ機能の実装が必要となる。

(ⅲ) Symposium on Cryptography and Information Security（SCIS 2016）

SCIS 2016 は暗号と情報セキュリティの国内学会である。自動車に関するセキュリティの論文も多数投稿されており、本年は66あるセッションのうち5つが自動車セキュリティというテーマで行われている。本件では、自動車セキュリティ機能の実現について提案している論文の概要とどのようなアーキテクチャを想定しているかについて調査した。調査結果は Appendix A にまとめた。

③ セキュリティ機能を実装したアーキテクチャの分類

ここまで調査したセキュリティ機能は大きく以下の 3 つのアーキテクチャへ分類することができる。

(ⅰ) セントラルゲートウェイへのセキュリティ機能実装

本分類は、外部からの通信、機能ごとに分割された ECU の集合（系統）からの通信をセントラルゲートウェイで集約し、そこでメッセージのフィルタリングなどのセキュリティ機能を実装する方式である。

本分類は、セキュリティの機能はセントラルゲートウェイ部分に集約されるため、各系統で ECU などは既存のものを利用できる可能性が高いと考えられる。ただし、すでにセントラルゲートウェイ方式のアーキテクチャを採用している場合は問題ないが、そうでな

いアーキテクチャを採用している場合はアーキテクチャの大きな変更が必要となると考えられる。また、系統内での通信のようにセントラルゲートウェイを通過しないメッセージについては、不正メッセージが流れても対処できないという問題点もある。

(ⅱ) 各 ECU へのセキュリティ機能の実装

本分類は、すべての ECU においてセキュリティ機能を実装する方法である。各 ECU にセキュリティ機能の実装が必要となるため、ECU の変更が必要となる。さらに、現状よりも ECU の負荷が大きくなるという問題点もある。しかし、アーキテクチャによらないという利点があり、全体のアーキテクチャは現状から大きく変更する必要が無いと考えられる。

(ⅲ) セキュリティ機能を実装した ECU 等を追加

本分類は不正メッセージの検知阻止などを行うセキュリティ機能を実装した ECU 等を追加する方法である。新しくセキュリティ機能を持つ ECU 等を追加するため、従来のアーキテクチャを大きく変更する必要が無く、各 ECU にセキュリティ機能を実装する場合に比べて、コストを抑えることができると考えられる。

3.1.3 自動運転の共通ユースケース

脅威分析を実施するためには、対象システムがどのように利用されるか、そのユースケースの明確化が必要である。特に共通モデルにおいては、脅威分析の対象となる自動運転システムの共通部分について、そのユースケース（共通ユースケースと呼ぶ）を明確にする必要がある。

共通ユースケースを作成するために、現在検討されている自動運転に関係するユースケースの調査を実施した。調査は、主に自動運転のユースケースを対象に実施したが、自動運転は現在研究中の技術であるため、入手できる事例はそれほど多くない。自動運転は現在の ADAS や隊列走行の発展形である（以後、自動運転に準ずるシステムと呼ぶ）ため、ADAS および隊列走行のユースケースも調査対象とした。調査はウェブや論文など一般に広く公開されている資料により実施し、訪問しての聞き取り調査などによる方法は、時間的な制約から実施していない。調査対象の候補としたのは以下のプロジェクトである。

・国内
  - 内閣府 自動運転システム推進委員会
  - 平成 26 年度 次世代高度運転支援システム研究開発・実証プロジェクト[9]
  - 平成 26 年度 グリーン自動車技術調査研究事業[10]
・海外
  - interactIVe: accident avoidance by active intervention for Intelligent Vehicles
  - US AdaptIVE
  - SARTRE: Safe Road Trains for the Environment[11]
  - HAVEit: Highly automate vehicles for intelligent transport[12]

- Intel Advanced Driver Assistant System[13]

この内、「内閣府 自動運転システム推進委員会」、「interactIVe」、「US AdaptIVE」の三件は資料が非公開となっており、今回は調査が実施できなかった。「US AdaptIVE」の前身プロジェクトが「HAVEit」、「SARTRE」である。

また、自動運転は車両単独で達成されるものではなく、車車間、路車間など V2X 通信が必要となる。V2X に関しては、平成 26 年度 海外技術動向調査[14]の中で、ユースケースの調査も行っており、V2X のユースケースについてはこの結果を利用した。

調査結果はユースケースごとに対応関係を明確化し、比較表（Appendix B）としてまとめている。この比較表を基に、調査したユースケースを統合し、共通ユースケースの第一次案として作成した。（Appendix C）

(1) 現在考えられている自動運転のユースケース

本節では調査した自動運転システム（または自動運転に準ずるシステム）のユースケースの概要について説明する。

① 平成 26 年度次世代高度運転支援システム研究開発・実証プロジェクト

プロジェクトの目標は次世代型の高度運転支援システムの開発である。この中のサブテーマとして、自動運転システム レベル 3 (SAE)を想定し、将来の自動運転システムとしてクラウド連携、V2X 通信を考慮したセキュリティとフェールセーフ技術開発を目的としている。このサブテーマの目的を達成するためには、将来の自動運転システムの姿を一致させることが必要であり、自動運転のユースケース、アーキテクチャの明確化が行われている。

ここでの自動運転は、通常時はシステムが周辺監視を含む走行の制御を行うが、緊急時にはドライバへ権限が渡され、ドライバよって制御するものである。対象システムでは自動運転実施、自動運転時にドライバによる操作のオーバーライド、自動運転解除、緊急時（単一故障、性能限界、セキュリティ侵害、ドライバの不調）の自動運転解除などの機能が仮定されている。特に緊急時の自動運転解除については、自動運転を解除することをドライバへ通知し、「(1) ドライバからの（正しい）オーバーライド」、「(2) 安全な場所へ自動運転による停車」のどちらかが満たされるまで、自動運転を継続するようになっている。

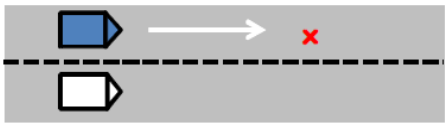
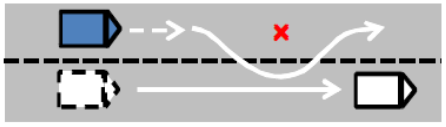
ここでは高速道路での走行（SA/PA を除く、ETC 料金所に進入し、離脱するまで）に対し、表 3.1.3-1 の条件を付加してシナリオ（ユースケース）導出、ユースケースから必要となる機能、アーキテクチャを策定している。

表 3.1.3-1　平成 26 年度次世代高度運転支援システムの前提条件

走行道路	高速道路（SA/PA は対象外）。
環境条件	雪、霧は対象外。
運転技量	熟練のドライバを想定。
道路交通法	遵守する。
走行車線	最も左側を基本とし、障害物回避時のみ追い越し車線を走行。3 車線以上で最も左側以外の走行は対象外。
車線有無	本線は有り。 合流/分流路は無し。 ETC ゲート前後は無し。
運転マナー	自社進路に入る他車へ針路を譲るなど、模範的なものを想定。

各ユースケースは自車、周辺の他車、障害物、交通法規を含む状況を明確にし、その際に実施する制御を操舵系（車線変更など）とブレーキ系/エンジン系（加減速など）の二つに分けて記述している。表 3.1.3-2 に「自車線に落下物（障害物）があり、隣車線（ここでは 2 車線を想定）に併走車または自車より速い後続車（1 台）」という状況で併走車/後続車を通過させた後、落下物を避けるシナリオを表として再構成したものを例として示す。

表 3.1.3-2　次世代高度運転支援システムユースケース例（[9]のデータを基に再構成）

No				
前提初期シーン		基本走行		本線定速走行（100km/h）
		付随事象 1		自車線に落下物
		付随事象 2		隣り車線に併走車 or 自車より速い後続車（1 台）
		初期設定イメージ ※灰：自車、白：他車、×：落下物		
		事象 1 対象物	最大相対速度 [km/h]	100
			TTC [s]	5
			初期距離 [m]	139
		事象 2 対象物	最大相対速度 [km/h]	40
			TTC [s]	5
			初期距離 [m]	56
平常時動作（（（（前提初期シーン以外の障害物は無し）））	認知	前方		○
		側方	前	○
			横	○
			後ろ	○
		後方		
	判断	基本方針		側方車通過後の操舵回避を選択
	操作	操舵系	動作	併走車通過後 車線変更⇒ 落下物追抜後 車線復帰
			横 G	
		ブレーキ系 エンジン系	動作	減速⇒ 併走車通過後 車速維持⇒ 車線復帰後 車速復帰
			減速 G	
		平常時動作イメージ ※点線は減速		

プロジェクトで導出されているユースケースは、通常時の基本的な動作、車線減少による合流動作、車線増加による分流動作、ETC ゲート進入動作、ETC ゲート離脱動作、前方交通情報を得た場合の動作の 6 つの動作に分類されている（合計 59 個）。これらのユースケースに加え「自動運転の解除時に、ドライバへ主権を譲渡できない場合」（緊急時）のシナリオの導出が行われている。この緊急時のシナリオ導出は試行として実施されているため、本件では対象とせず、通常時のみをユースケースとして使用している。

② 平成 26 年度 グリーン自動車技術調査研究事業

この事業は、自動車から得られる情報をどのように利活用できるかを検討し、将来の事業化の可能性の検討、社会的課題の解決を目指したプロジェクトである。その中で自動運転の実現により実現可能となるサービスを ITS 利用者のニーズから抽出し、そのニーズを基にユースケースを導出している。利用者としては、ドライバ、道路管理者、地域住民、公共交通、新ビジネス、運行管理者があげられており、それぞれから抽出されたニーズを実現可能性などから絞り込み、自動運転の形態ごとに以下の 6 つの分野に分類している。

1. 路車協調型自動運転システム
2. センター監視型自動運転システム
3. 隊列・追従走行型自動運転システム
4. 車載システム完結型自動運転システム
5. 無人型自動運転システム
6. 緊急時対応型自動運転システム

これらのグループ化の方針は図 3.1.3-1 により示されている。

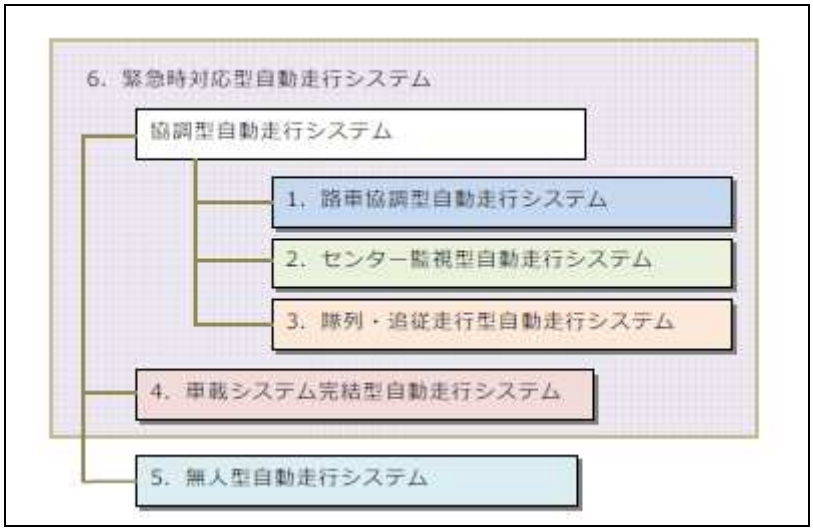


図 3.1.3-1　自動運転システムの走行形態別のグループ化方針（[10]より引用）

導出されたユースケースはこの走行形態ごとに運転状況が設定されており、ユースケースごとに協調しなくてはならない外部の対象も明確化されている（ユースケースにおける関連するアクタに相当）。また、各ユースケースは自動運転レベルを限定せず、対応可能となるレベル（自動運転レベル 2～4 (NHTSA)及び無人走行で分類）を記載している。本プロジェクトで導出されているユースケースの例として「路車協調により高速道路で安全スムーズに合流したい」の内容を表 3.1.3-3 に再構成して示す。

表 3.1.3-3　再構成したユースケース例（[10]を再構成）

走行形態		1. 路車協調型自動走行システムのユースケース(インフラや他車との通信が不可欠となる自動走行システム)
状況		1.1 高速道路での安全・快適な走行
ユースケース		1. 1. 1 高速道路で安全にスムーズに合流したい
自動化レベル	情報提供　＋レベル2 以下	○
	情報提供　＋レベル 3	○
	自動走行システムレベル4 以上	
	ドライバレス	
協調の有無	路側	○ （協調があるとサービスが向上する）
	他車	○ （協調が必須）
	歩行者	
利用シーン	高速道	○
	一般道	
	限定エリア	
ニーズ所有者		ドライバ
ニーズを実現する自動走行システム		高速道路の本線部やランプ部において、車載センサや V2V，I 2V 通信情報を用いて周囲の車両を認識し、安全に走行・合流できる自動車

③ SARTRE (Safe Road Trains for the Environment)

一般的なハイウェイなど幹線道路でのトラック、乗用車が混在した隊列走行を実現するためのプロジェクトであり、実際に公道での試験走行が実施されている。

ユースケースは Platoon Use Case（PUC）と Back Office Use Case（BUC）に分けられる。PUC は隊列走行の構造や基本的なオペレーションに関係したユースケースで、BUC は隊列への車両追加などのようにインフラに関係するユースケースである。SARTRE では最も上位（抽象度が高い）のユースケース（L1 ユースケースと呼ぶ）が定義されている。L1 ユースケースを基に、より詳細なユースケース(L2、L3 ユースケースと呼ばれ詳細になっていく）を適宜作成している。L2、L3 などの詳細化したユースケースは公開されていない。

SARTRE では以下の車両（および車両のドライバ）と Back Office Administrator（BOA: 隊列の形成について車両へ支持を出す役割）がユースケースのアクタとして現れる。

・FV (Following Vehicle) : 隊列走行中の追従車両

・LV (Lead Vehicle) : 隊列走行中のリーダ（先頭）車両

・OV (Other Vehicle) : 隊列走行に関係しない車両

・PFV (Potential Following Vehicle) : 隊列に加わる（追従する）車両になる可能性のある車両
・PLV (Potential Lead Vehicle): 隊列のリーダ（先頭）車両になる可能性のある車両
・PPV (Potential Platoon Vehicle): 隊列走行する可能性のある車両
・PV (Platoon Vehicle): 隊列走行している車両

L1 ユースケースのうち PUC に関しては図 3.1.3-2 のユースケース図が示されている。例えば、隊列を形成するユースケースである Create platoon では、隊列を形成しようとする PLV と PFV、隊列形成を支持する BOA、隊列形成の障害となりえる OV がユースケースのアクタとなっている。

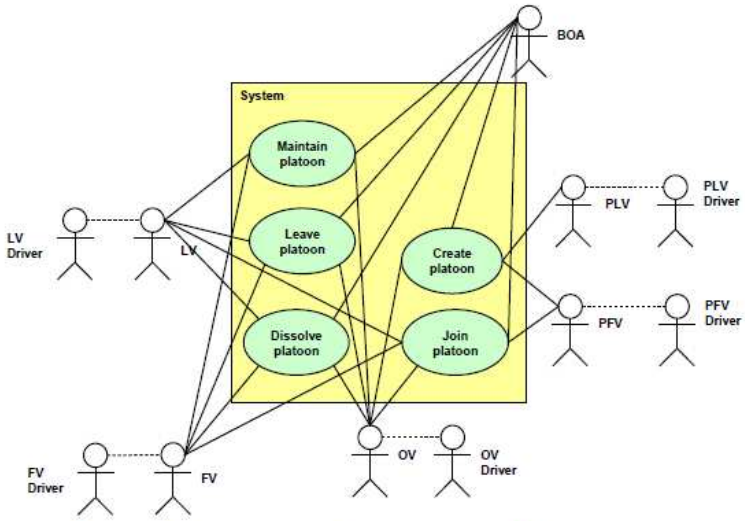


Figure 1. Overview of system, actors and L1 Use Cases

図 3.1.3-2　PUC のユースケース図

それぞれのユースケースは表 3.1.3-4 に示すテンプレートで作成されている。表 3.1.3-4 のテンプレートに記載されている内容はユースケース図でも取り上げた Create Platoon のシナリオであり、PLV、PFV 各一台が新しく隊列を形成するというユースケースである。隊列形成は、BOA が PLV を LV として選び、さらに PFV を FV として隊列に加わるように指示するという手順で行われる。ユースケースではその際に危険となる可能性についても Risk という項目で明確化している（ここでは隊列走行に関係しない OV が妨害してしまうことが想定されている）。

表 3.1.3-4. SARTRE のユースケースシナリオのテンプレート記述例（[11]より引用）

Name	One PLV and one PFV create a platoon via Back Office.	
ID	PUC.L1.Create_Platoon.1	
Super-ordinates	Not applicable	
Sub-ordinates	None	
Description	This UC is invoked when one PLV and one PFV wish to initiate a new platoon. The PLV is a Truck/Bus and will be selected as LV since the driver of the PLV has been properly trained. Back Office services are used for identifying the PLV, guidance to it and charging. One PLV and one PFV are involved.	
Environment	Road and conditions are suitable for platooning.	
Goal	Creation of a platoon with one PLV and one PFV.	
Priority level	This UC shall be further elaborated	
Trigger	A PPV that would like to be included in a platoon.	
Risk	Emergency situation Interfering OV(s) PFV not reaching PLV in time	
Involved actors	One PLV, one PLV driver One PFV, one PFV driver Zero or more OVs, zero or more OV drivers BOA	
Start state	There is no suitable platoon for the PLV/PFV to join.	
Main scenario sequence	Step	Action: Main scenario
Main	1	PLV driver/PFV driver contacts Back Office to find a PFV/PLV respectively and registers to Back Office,
	2	Back Office finds a suitable PLV-PFV match. Back Office gets acceptance from PLV driver for including PFV.
	3	The PFV driver accepts offer from Back Office.
	4	Back Office gives guidance information to PFV driver to find PLV.
	5	PFV driver requests PLV for inclusion in a platoon. The distance is still such that safe manual driving is possible.
	6	PLV driver/PLV checks if PFV has activated ACC/CC and in that case turns it off. PFV driver is informed by PLV driver/PLV.
	7	PLV driver acknowledge inclusion. PLV becomes an LV and PFV becomes an FV and is thus driven autonomously. Distance between vehicles is optimized
	8	LV driver/LV informs Back Office that platoon is created
Main End state		A new platoon is created with one LV and one FV. Back Office is informed.
Exception M2.E		No PLV-PFV match is found
	1	PLV driver/PFV driver is informed by Back Office that no match is found.
M2.E End state		A new platoon is not created.
Comments	If not a successful creation of platoon no charging is made for guidance information. Back Office checks if driver of truck/bus has proper platoon training. If not, he/she is not registered as PLV. An emergency situation could occur: when PLV and PFV are far from each other (M2). This situation is the same as separate vehicles (under full manual control). That the platoon may pass toll booth(s) on its way has been included in the agreement for creating the platoon.	

④ HAVEit (Highly automated vehicles for intelligent transport)

乗用車だけでなくバスやトラックを含め、安全性と効率を高める自動運転（追従走行や高度運転支援）の実現を目指したプロジェクトである。ドライバと自動運転車との最適なタスクの分割がなされた次世代 ADAS の開発、ドライバと自動運転システム（自動運転車のドライバに相当する部分）の統合、スケーラブルかつ安全なアーキテクチャの開発が行われている。自動運転を達成するために複数のアプリケーションに分割してユースケースを記述している。検討されたアプリケーションは以下のとおりである。

A) Joint system: ドライバと自動運転システムの権限の受け渡しについてのユースケース
B) Electrically controlled wheel brake truck for safety architecture validation: スケーラブルかつ安全なプラットフォーム
C) Automated assistance in roadworks and congestion (ARC): 高速道路での道路工事や渋滞時を考慮した自動運転機能
D) Automated queue assistance (AQuA): 高速道路での低速でのトラックの運転や混雑した交通状況でドライバをサポートする機能
E) Temporary autopilot (TAP): 限定された状況下における完全自動運転機能
F) Active green driving (AGD): 燃費向上などのためのドライバ補助機能

上記のうち B) はスケーラブルかつ安全なプラットフォームの開発、F) Active green driving は燃費向上のためのドライバ補助機能であり、自動車の制御そのものではない。そのため、本件の調査対象からは除外している。

HAVEit では複数の自動運転レベルを想定しており、A) Joint system では状況により手動または自動で他の自動運転レベルへ遷移することが想定されている。自動運転レベル、その間の遷移および自動運転が実施不可能となった場合の付随する状態は図 3.1.3-3（Automation spectrum with different automation levels, sublevels and additional states と呼ばれる図[12] Figure 3 より引用）で示されている。

図 3.1.3-3 の中央は 5 つのレベルが、自動運転レベルの高さの順に並んでいる。最も左はドライバがすべてを判断し制御する状態で、最も右が完全自動運転である。中間の 3 つのレベルは、順に自動運転レベルが上がり、内部に 2 つのサブレベルを持っている。これらの自動運転レベルに加え、上下左にそれぞれ各一つ状態が追加されている。状態 Off は自動運転が切られた状態で Joint system がバイパスされている。Minimum risk state は自動運転が継続できずドライバへ制御が渡されないといけないにも関わらず、ドライバが受け取れない際に遷移する状態である。具体的な状態としては、路肩への安全な停止などが考えられる。

Failure はハードウェアおよびソフトウェアの故障により自動運転が正しく動かない状態であり、この状態への遷移は本来望まれないものである。図に記入されているのは、この状態への遷移の最小化を検討するためである。

自動運転レベル間の可能な遷移は図 3.1.3-3 の矢印で示されている。この中からユースケースごとにどのような遷移を許すか（Off、Minimum risk state、Failure への遷移も含め

て）検討している。

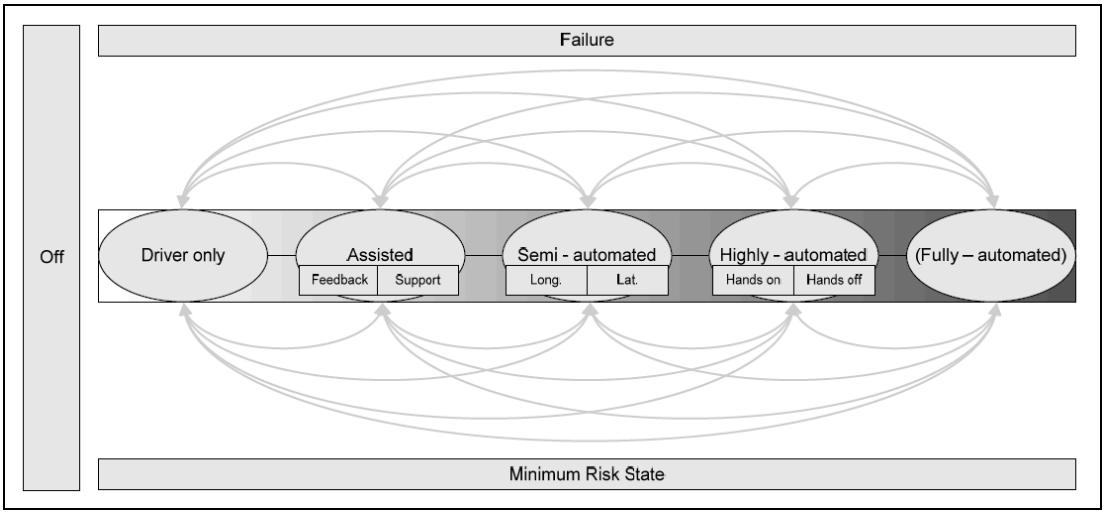


図 3.1.3-3　自動運転レベルとその間の遷移

⑤ Intel Advanced Driver Assistant System

将来の自動運転へとつながる ADAS システムに対し、セキュリティ対策の実装方法を提案したプロジェクトである。ADAS のアーキテクチャ、ユースケースの決定から始まり、その情報を基にした脅威分析を実施、脅威分析の結果を基にセキュリティ要求事項の導出がなされている。セキュリティ要求事項として、セキュアなプラットフォーム、センシング、アクチュエータ、内部処理、コミュニケーションに関して全部で 25 が導出されている。ADAS の最も重要なユースケースとして Lane Departure Warning と Adaptive Cruise Control の二つに関して脅威分析の詳細な過程が公開されている（図 3.1.3-4）。

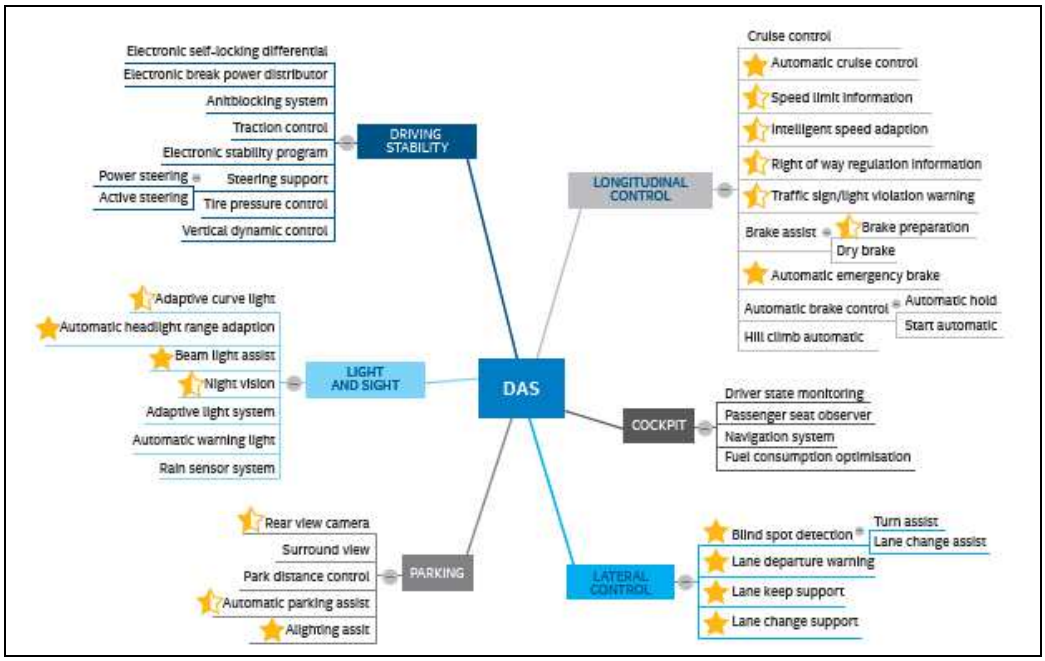


図 3.1.3-4　DAS（ADAS）の機能スペクトラム（[13]より引用）

(2) 自動運転共通ユースケース

今回調査したユースケースを比較し、以下の手順により、自動運転の共通ユースケース案を作成した。

A) 調査対象のユースケースを運転状況により分類する。
B) 各分類内でユースケース詳細を比較し、関係のあるユースケースをまとめる。
C) まとめられたユースケースを適宜、命名し共通ユースケース案とする（ユースケースの内容は関連する調査対象のユースケースより作成。

B で使用している「関係のある」という意味は、ユースケースが同一である、もしくは自動運転レベルが異なるが同一の機能であることを言う。例えば「走行車線変更時に周囲の他車両を検知し運転者へ警告を出す（平成 26 年度調査の UC-19)」と、「走行車線変更時に周囲の他車両を検知し運転者へ警告を出し、走行車線を保持する（HAVEit-AQuA3)」の二つがその関係になる。両者は車線変更時の危険を回避することが目的となっており、同一の機能の実現を目指している。自動運転レベルについては、後者が前者に車両の制御を加えて実施しており、より高いレベルとなっている。

A の分類は以下の観点から行った。まず、大きな分類として自動車の走行状態を用いた。自動車の走行状態としては以下のように分類している（その他にはシステムの起動、終了といった走行状況で分類できないユースケースも含まれている）。

・通常走行
・駐車
・緊急車両通行時
・停車時
・その他

次に通常走行に関しては、さらに詳細な状況の分割を行った。分割は交差点以外の車線のある道路、交差点以外の車線のない道路、交差点（信号有)、交差点（信号なし)、その他の 5 種類である。また、交通法規や道路環境への対応は、状況によらず通常走行時に対応が必要である。そのため、詳細な状況と同等のレベルの分類として作成した。この比較結果はユースケース比較表（Appendix B の「ユースケース比較表と共通ユースケース導出）シート左側の表）としてまとめられている。

作成された比較表とユースケースの関係より、共通ユースケース案を作成した。まず、各状況に分類されたユースケースの内容を基に、さらに詳細な分類を実施した。その分類は、各運転状況は運転状況の詳細化および運転状況における制御により分割している。各分類に関係するユースケースを 1 つのユースケースとしてまとめ、共通ユースケース案とした。この分類をユースケース比較表の右方向へ記載している。ユースケースの関係の検討結果は、比較表の横方向に並べることで表現されている。共通ユースケースと、その基となった調査対象ユースケースの関係は、Appendix B にまとめられている。

(3) 共通ユースケースまとめ

本節では ADAS、隊列走行など自動運転システムの基礎となるシステムおよび、自動運転システムのユースケースの調査を実施し、それらの比較を行い自動運転システムの共通ユースケース案を提案した。今回、提案したユースケースが自動運転を実現するのに十分であることを示す根拠は存在していない。このユースケースの十分性の評価は Connected Vehicle Reference Implementation Architecture (CVRIA) [15]にあげられている Application との対応関係や、ISO/TR 20545（Report on standardization for vehicle automated driving systems (RoVAS)）との対応関係などによって評価できると考えられる。今後は上記のような文献を指標としてユースケースの十分性の評価を実施し、共通ユースケースの充実を図るべきと考える。

3.1.4　脅威分析

セキュリティ上の脅威について分析する手法（脅威分析手法）は、これまでいくつかの方法が提案されてきた。現在、高度な多段攻撃や、通信相手の信頼度を表すレベルの導入など、これまでとは異なる新しい考え方が提案されている。今後、自動車がより高い情報セキュリティを確保するために、自動車分野全体で汎用的に利用可能であり、上記のような新しい考え方に対応した手法が必要とされる。

平成 27 年度は、共通脅威分析手法を開発するための準備として、現在提案されている分析手法の調査を実施した。また調査した分析手法による試行を行い、自動車分野の脅威分析に必要とされる要件の洗い出しを行った。

(1) 脅威分析手法の調査

調査対象は自動車分野で使用された手法のみでなく、広く IT 分野で使用されている手法も含めた。調査対象の各手法については、その特徴を明確にしている。調査は時間的な制約から、ウェブや論文など一般に広く公開されている資料により実施し、実際に脅威分析の実施者への聞き取りなどは行っていない。具体的には以下の手法に対し調査した。

・Attack Trees （EVITA プロジェクト）
・Misuse Cases
・Security Development Lifecycle (SDL)
・OCTAVE Allegro
・JASO 自動車-情報セキュリティガイド

本件では自動車分野で使用されたことがある手法はもちろん、IT 系において使用された手法についても調査を行うべきと考え、上記の手法を対象とした。Attack Trees は自動車の車車間、路車間通信を対象として脅威分析を実施した EVITA プロジェクトで使用された手法[16]である。OCTAVE は文献調査の結果では、自動車分野での明確な使用実績は確認できていないが、自動車のセキュリティに関するガイドラインである SAE J 3061 で取り上げられている手法である。JASO は自動車の情報セキュリティのガイドラインであり、自動車のセキュリティを確保するために必要となる脅威分析手法を提案している。このように EVITA、OCTAVE、JASO の手法は自動車（自動運転システム）のセキュリティに十分使用可能であると考え調査対象とした。Misuse cases、SDL は自動車分野で使用された実績は確認できていないが、IT 系のセキュリティ脅威分析で広く使用されており、IT 系で使用される手法がどれだけ自動車分野において有効であるかを調査するために対象とした。

① Attack Trees

Attack Trees は B. Schneier[17] により発案されたと言われている手法である。安全分析におけるトップダウンの分析手法である Fault Tree Analysis (FTA) [18]と類似した木構造の分析手法であるが、FTA のように国際規格などで標準化されておらず、様々なバリエーションが存在している（セキュリティ要求との組み合わせ（Attack Defense Trees [19] や Attack Countermeasure Trees [20] ）や、新しいゲート（順序、並列など）の追加、木以外の表現形式（グラフ表現）など）。一般的には、攻撃の手段を抽象度の高い方から、より詳細な手段へと分解することで脅威を分析し、リスクの評価を行う。これにより、攻撃の組み合わせに何があるかを分析することが出来る手法である。Attack Trees は Fault Trees とほぼ同様の構文規則を持ち、アタックイベント、ゲート記号（AND、OR ゲートなど）、基本アタックイベントなどから構成される（図 3.1.4-1 及び表 3.1.4-1）。

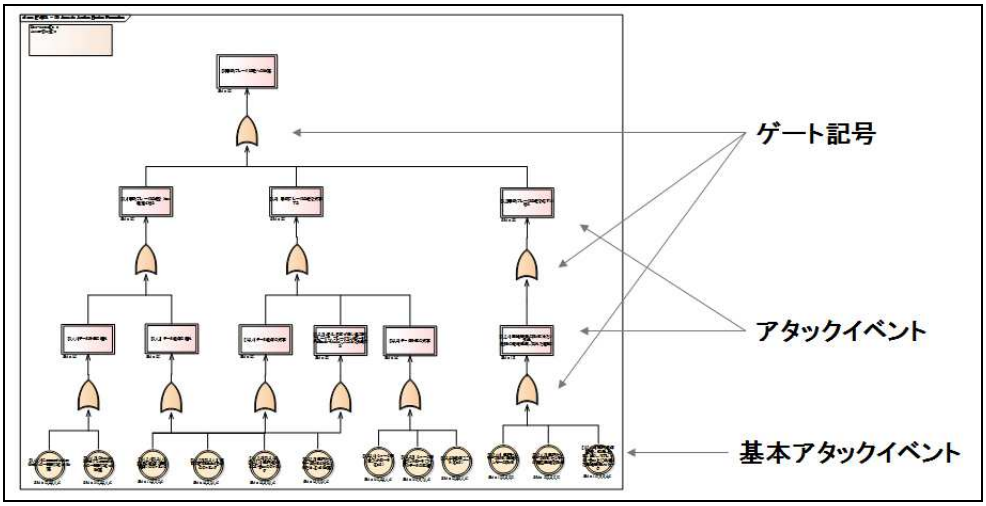


図 3.1.4-1　Attack Trees の例

表 3.1.4-1　Attack Trees と Fault Trees の構文比較

解釈	FT	AT
トップのノード	望ましくない事象。	攻撃者の目標、攻撃の結果得られる事象。
ゲート	ゲートの下位の事象が発生すると、ゲートの上位の事象が発生。	ゲートの下位の事象が発生すると、ゲートの上位の事象が発生。
AND ゲート	ゲートの下位の事象の全てが発生すると、ゲートの上位の事象が発生。	ゲートの下位の事象の全てが発生すると、ゲートの上位の事象が発生。
OR ゲート	ゲートの下位の事象の少なくとも一つが発生すると、ゲートの上位の事象が発生。	ゲートの下位の事象の少なくとも一つが発生すると、ゲートの上位の事象が発生。
ゲートの解釈	AND ゲートは、下位事象の確率の積、OR ゲートは、下位事象の確率の和。	EVITA においては、AND ゲートは、下位事象の攻撃確率の最小値、OR ゲートは、下位事象の確攻撃率の最大値をとる。

以下では特に EVITA で用いられた Attack Trees の手法について説明する。

EVITA において Attack Trees は攻撃者を仮定し、その攻撃者がどのようにシステムに対し攻撃をするかを分析する。Attack Trees は以下の 4 つのレベルに分けて分析が進められる（図 3.1.4-2）。

・Attack Goal
・Attack Objective
・Attack Method
・Asset (Attack)

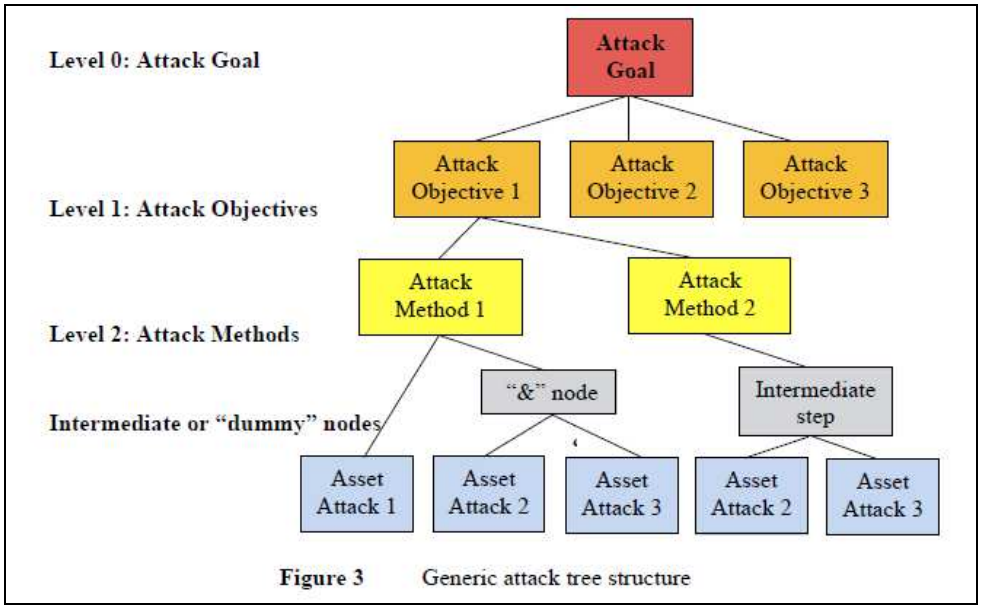


図 3.1.4-2　EVITA の Attack Trees 概略（[16]より引用）

これらの各レベルについて以下で説明する。

・Attack Goal

攻撃者の利益を同定し Attack Trees のトップイベントとする。

・Attack Objective

Attack Goal に対し、それを達成するために必要となる攻撃（それによる対象システムの状態など）を配置する。Attack Objective には攻撃によって引き起こされる影響も含まれる。そのため、Attack Objective はリスクを決定するパラメータである深刻度を見積もる対象となる。

・Attack Method

Attack Objective を分解し、具体的に対象システムのどの部分にどのような攻撃するかが記述される。例えば、Attack Objective が「機能 X を妨害する」（機能 X はセンサからの情報をトリガーとして実行されるとする）であった場合、Attack Method としては「機能 X を破壊する」、「センサからの情報を遮断する」、「センサへ攻撃する」となる。また、リスクはこの Attack Method に対し見積もられることとなる。

・Asset (Attack)

Attack Method は一つ以上の Asset への攻撃の論理的な組み合わせ（AND/OR）へと分解される。この Asset への攻撃は Asset Attack とよばれ、Attack Trees の末端のノードになる。Asset Attack は具体的な保護資産に対する操作を記述し、リスクを決定するパラメータである Attack Probability を見積もる対象となる。

Attack Trees では、作成された木構造によって、同定された攻撃のリスク計算が行われる。リスクは攻撃による結果の深刻度と、攻撃の容易さ（安全性を考える場合はさらにコントローラビリティを加える）から決定される。各パラメータおよび、その見積もり方法

については 6 章で説明するため省略し、本節では Attack Trees によってどのようにリスク計算が実施されるかについて説明する。

リスクは Attack Trees における Attack Method ごとに決定されるレベルである。このリスクを決定するためには、リスクを決定する深刻度、攻撃の容易さが見積もられる。深刻度は結果に対して見積もる必要があるため、Attack Trees の Attack Objective に対して見積もられる。これは、どのような攻撃によっても結果が一つとなるため、下位の Attack Method へと値が継承される。

一方で、攻撃の容易さは詳細な攻撃方法が明確になっている必要があるため、Asset（Attack）に対して見積もられる。Attack Method は一つ以上の Asset（Attack）の（AND/OR による）組み合わせであるため、見積もられた値は上位の Attack Method へと統合される。ただし、統合はその組み合わせ方により計算方法が異なる。AND ゲートによる組み合わせは、下位のすべての攻撃が達成され必要があるため最も困難な攻撃が選択され、その値が上位の Attack Method の攻撃の容易さとなる（EVITA では値が大きいものが困難としているため最大値となる）。OR ゲートによる組み合わせは、下位の攻撃のどれか一つが達成されればよいため、最も容易な攻撃が選択され、その値が上位の Attack Method の攻撃の容易さとなる（EVITA では値が小さいものが容易としているため最小値となる）。

このようにして Attack Method の深刻さと攻撃の容易さが見積もられ、リスクが決定される（図 3.1.4-3）。図 3.1.4-3 の「AP =5」は攻撃の容易さを表すレベル Attack Probability が 5 であることを意味している。

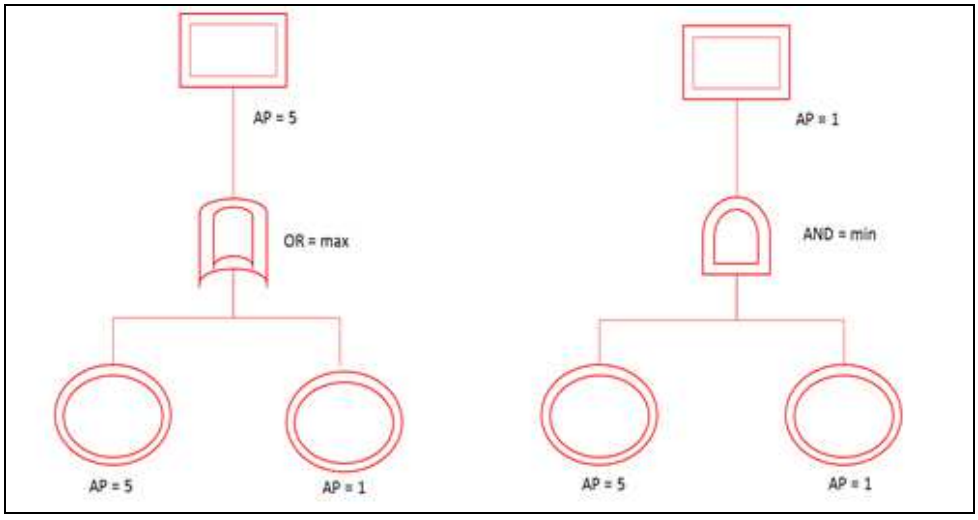


図 3.1.4-3　EVITA によるリスク決定

② Misuse cases

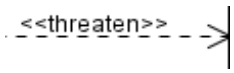
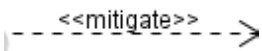
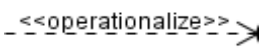
Misuse cases は Guttorm Sindre と Andreas L. Opdahl により提案された脅威分析の手法[21, 22]で、システム開発で用いられるユースケース図を拡張した分析手法である。Misuse cases には様々なバリエーションが存在している。例えば、John P. McDermott と Chris Fox によって提案されている Abuse Case[23]、Donald Firesmith によって提案されている Security

use case[24]などがある。ここでは、Misuse cases に保護資産、セキュリティゴールの概念を付加した拡張 Misuse cases[25, 26]について取り上げる。この拡張を選択したのは、本件で調査している手法と同等のセキュリティの概念が考慮されており、本件の脅威分析を実施するのに適していると考えられるためである。

すでに述べたとおり、Misuse cases はユースケース図を基に拡張を行った図である。これには表 3.1.4-2 に示すエレメントが用いられる。

表 3.1.4-2　Misuse cases のエレメント

（エレメントはチェンジビジョン社 Astah professional [27]で作成）

エレメント	名前	説明
	アクター	ユースケースに関連する人、組織、外部システム等。
	攻撃者	意図的にシステムへ危害を加えようとするアクター。
	ユースケース	少なくとも一つのアクターがシステムを使用して行うアクション。
	保護資産	ユースケースに関する、保護すべき価値のあるもの。ユースケースで使用するデータとユースケースそのものが保護資産となる。
	ミスユース	攻撃者により行われる保護資産への脅威。
	ゴール	セキュリティ要求事項。
	対抗手段	脅威に対して対抗するための手段。
		ミスユースから脅威を与える保護資産への関連。
		対抗手段から、対抗するミスユースへの関連。
		対抗手段から、それによって実現されているゴールへの関連。

Misuse cases による脅威の同定は以下の手順で実施される。

(1)ユースケースの作成

(2)保護資産の同定

(3)セキュリティゴールの同定:

(4)保護資産とセキュリティゴールの評価

(5)ミスユースの同定と評価

(6)対抗手段の同定

以上の手順により図 3.1.4-4 の様な Misuse cases 図が作成される。

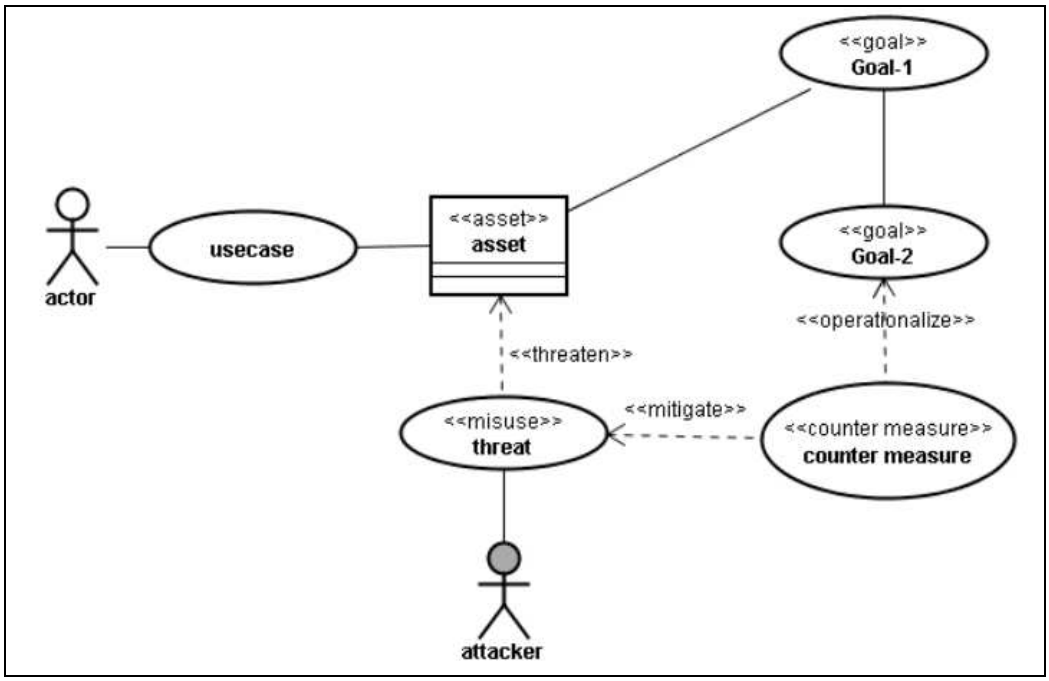


図 3.1.4-4　Misuse cases 図の例

③ Security Development Lifecycle (SDL)

2004 年にマイクロソフト社が提唱した、安全なソフトウェア製品開発のための開発プロセスで、製品リリース後のサポートまでがライフサイクルに含まれている[28]。SDL では設計フェイズで Threat Modeling により脅威の同定、対抗策の検討が行われる。その際に使用する Threat Modeling Tool[29]はマイクロソフト社から無償で提供されている。Threat Modeling は図 3.1.4-5 の様なプロセスにより実施される。

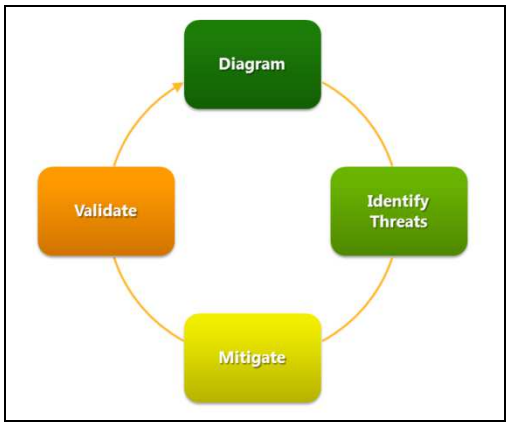


図 3.1.4-5　Threat Modeling のプロセス（[28]より引用）

各フェイズの概要は以下のとおりである。

・Diagram: 対象となるシステムをモデル化する。モデル化には Data Flow Diagram (DFD) を用い、攻撃の入り口（システム、権限などの境界）となる部分を表すトラストバウンダリーを付け加える。

・Identify Threat: 作成された Diagram を用いて脅威を同定する。DFD の各エレメントに対し脅威分類 STRIDE を用いて同定していく（STRIDE の詳細な説明は後述）。

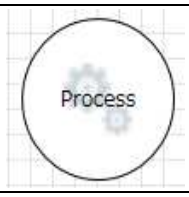
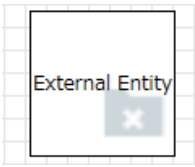
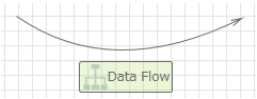
・Mitigate: 同定された脅威にごとに基本的な対抗策が挙げられている。これを用いて対象システムへの対抗策の検討を行う。

・Validate: 上記のフェイズで作成されたモデル、同定された脅威、対抗策が妥当であるかを確認する。

ここでは、上記のうち Diagram と Identify Threat フェイズで行われる DFD による対象システムのモデル化と、STRIDE を用いた脅威の同定について説明する。

DFD はデータのフローを表現した図で、どこからデータが発生し、どのような処理が加えられ、どこに格納されるかなどが表現されている。DFD で使用されるエレメントとその説明を表 3.1.4-3 に示す。

表 3.1.4-3　DFD のエレメントとトラストバウンダリー（エレメントの絵は[29]のものを使用）

エレメント	名前	説明
	プロセス	入力されたデータに対し、何らかの処理を加え出力データとするもの。
	外部エンティティ	モデル化しているシステムの外部に存在するものを表す。データの出元や出力先となる。
	データストア	データベースなどデータの保管場所。
	データフロー	他のエレメント間のデータの流れ。
	トラストバウンダリー	プロセス境界やファイルシステムなど、攻撃の口（機械、権限などの境界）となる部分。

DFD はコンセプト段階の抽象的なレベル、シナリオごとのレベル、サブコンポーネントまで詳細化されたレベルなどが作成される。DFD で作成されたモデルを図 3.1.4-6 に示す。

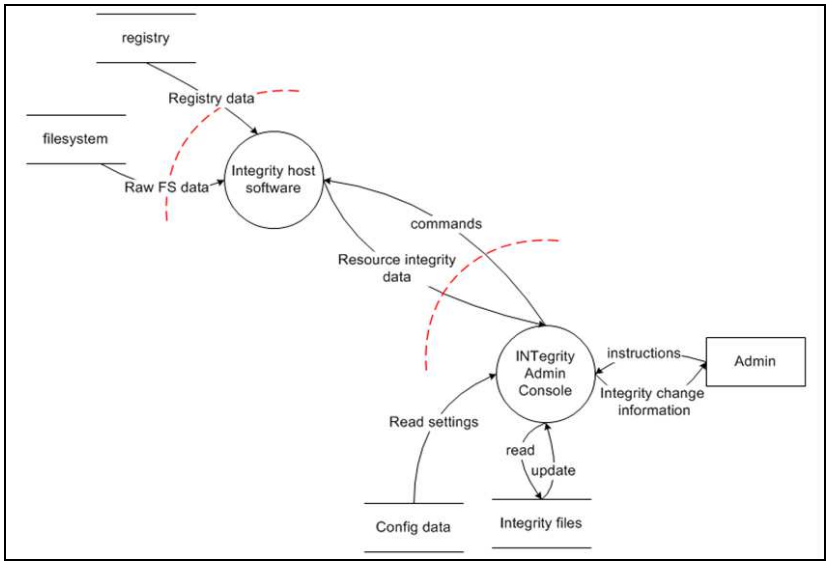


図 3.1.4-6　DFD の例（[28]より引用）

作成された DFD の各エレメントに STRIDE によって脅威を同定する。STRIDE は表 3.1.4-4 に列挙されている脅威の分類の頭文字をとったものである。

表 3.1.4-4　STRIDE の説明

脅威	説明	対応する性質
Spoofing	人や物へのなりすまし	Authentication
Tampering	データやコードの改竄	Integrity
Repudiation	アクションの否認	Non-repudiation
Information Disclosure	権限のないものへの情報の漏洩	Confidentiality
Denial of Service	サービスの妨害	Availability
Elevation of Privilege	権限の昇格	Authentication

DFD のエレメントの種類により STRIDE のどの脅威が影響するかが与えられている。その対応を示したのが表 3.1.4-5 である。影響するものには○をつけている。ただし、Data Store と Repudiation は基本的には影響しないが、Data Store に保存されるデータがログの場合には影響するため、△としている。また、Data Flow がプロセス内部である場合（トラストバウンダリー内）には、これらの脅威を考慮しなくてよい。

表 3.1.4-.5　エレメントに影響する脅威

	S	T	R	I	D	E
Process	○	○	○	○	○	○
External Entity	○		○			
Data store		○	△	○	○	
Data Flow		○		○	○	

以上のように SDL の Threat Modeling では対象システムをモデル化し、脅威の同定が行われる。

④ OCTAVE Allegro

OCTAVE は Software Engineering Institute (SEI)が Department of Defense (DoD)の Telemedicine and Advanced Technology Research Center (TATRC)と連携して作成した、プロセス・ドリブンな脅威・リスクアセスメントの手法である。また、Health Insurance Portability and Accountability Act (HIPAA)のセキュリティルールに適合した手法である。また、OCTAVE には基本的なもの以外に、100 名以下の製造組織への適用を考慮した簡易版である OCTAVE-S、これらをより合理化し、情報資産に焦点を絞った OCTAVE Allegro がある。本件では OCTAVE Allegro について調査を行っている。

OCTAVE Allegro[30]のプロセスは 8 つのステップで構成されている（図 3.1.4-7）。

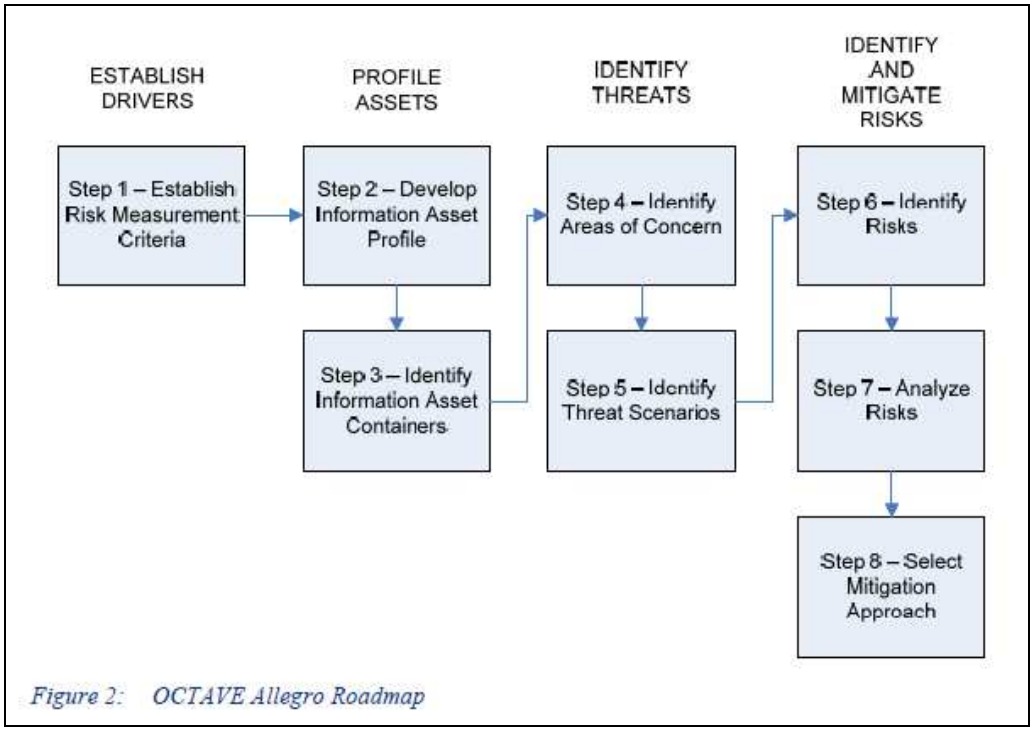


図 3.1.4-7　OCTAVE Allegro のステップ（[30]より引用）

ここでは本節の目的である脅威が同定される Step 5 までについて詳細を説明する。また、OCTAVE Allegro では様々な側面から脅威の同定・分析、リスク評価が行われるが、本節の説明では安全に関する側面を例として取り上げて説明する。

Step1 Establish Risk Measurement Criteria: 組織のミッションや目的への影響を評価するための評価軸を確立する段階。

最低限の評価軸として顧客の信用、財務、生産性、安全性、法的罰則が提供されており、これに適宜評価軸の修正・追加を行い、評価軸を作成する（安全性に関する評価軸のワークシートを表 3.1.4-6 に示す）。さらに、作成された評価軸の優先順位を明確にすることも必要である。

表 3.1.4-6　安全性の評価軸

Impact Area	Low	Moderate	High
Life	No loss or significant threat to customers' or staff members' lives	Customers' or staff members' lives are threatened, but they will recover after receiving medical treatment.	Loss of customers' or staff members' lives
Health	Minimal, immediately treatable degradation in customers' or staff members' health with recovery within four days Minimal, immediately treatable degradation in customers'' or staff members' health with recovery within four days	Temporary or recoverable impairment of customers' or staff members' health	Permanent impairment of significant aspects of customers' or staff members' health
Safety	Safety questioned	Safety affected	Safety violated

Step2 Develop an Information Asset Profile ではシステムの情報資産を列挙し、その特徴、価値などを記述する。

そのために、以下の手順を実施する。

(ⅰ) 全ての情報資産を収集する。

(ⅱ) 収集した情報資産から、漏洩、改竄、破壊、アクセス妨害が起きた際にシステムや組織に影響があるものを選択する。

(ⅲ) 表 3.1.4-7 のワークシートの情報資産のプロファイルを作成する。

表 3.1.4-7　CRITICAL INFORMATION ASSET PROFILE ワークシート

(1) Critical Asset What is the critical information asset?	(2) Rationale for Selection Why is this information asset important to the organization?	(3) Description What is the agreed-upon description of this information asset?
4) Owner(s) Who owns this information asset?		
(5) Security Requirements What are the security requirements for this information asset?		
Confidentiality	Only authorized personnel can view this information asset, as follows:	
Integrity	Only authorized personnel can modify this information asset, as follows:	
Availability	This asset must be available for these personnel to do their jobs, as follows:	
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	
Other	This asset has special regulatory compliance protection requirements, as follows:	
(6) Most Important Security Requirement What is the most important security requirement for this information asset?		
Confidentiality, Integrity, Availability, Other		

Step3 Identify Information Asset Containers: Step2 において列挙された情報資産が格納、通信、処理される場所を明確にする。

明確化は技術的、物理的（技術的ではない部分で）、人の側面から検討を行う（各側面に対し検討のためのワークシートが用意されている([30]の Appendix B 9a, 9b, 9c を参照)）。

上記 Step2 及び 3 により対象システムの情報資産が何であるか、それらがどこに格納、通信、処理されるかが明確になる。この結果を基に Step4 および 5 で脅威の同定が進行われる。

Step4 Identify Areas of Concern : 情報資産に脅威を与えるための、状態や状況（Areas of Concern）を同定する。

状態や状況の同定は網羅的に同定されることが目的ではなく、分析チームが思いつくものをブレインストーミングにより収集する。同定すべき項目は以下のとおりである（[30]の Appendix B Worksheet 10 より抜粋）。

(1)Actor: 攻撃を行うことができる人。
(2)Means: Actorがどのように、何ができるか。
(3)Motive: Actorの動機（故意か、過失かなど）。
(4)Outcome: 上記の結果Disclosure, Modification, Destruction, Interruptionのどれに影響するか。

Step5 Identify Threat Scenarios: Step4 で得られた Areas of Concern を脅威シナリオとして拡張し、シナリオの分析を実施することで広範囲の脅威シナリオを考慮する。

脅威シナリオの範囲は Threat Trees により表現されている（Threat Trees は OCTAVE で使用されているものであり、脅威の分類を木構造で表現したものであり Attack Trees とは異なるものである）。また、必要に応じて脅威の可能性を見積もる。脅威の可能性は後の対抗策の検討で優先度を考慮する際に有用である。表 3.1.4-8 に Threat Trees の説明を示す。

表 3.1.4-8　Threat Trees の説明

Threat Tree	Definition
Human actors using technical means	The threats in this category represent threats to the information asset via the organization's technical infrastructure or by direct access to a container (technical asset) that hosts an information asset. They require direct action by a person and can be deliberate or accidental in nature.
Human actors using physical access	The threats in this category represent threats to the information asset that result from physical access to the asset or a container that hosts an information asset. They require direct action by a person and can be deliberate or accidental in nature.
Technical problems	The threats in this category are problems with an organization's information technology and systems. Examples include hardware defects, software defects, malicious code (e.g., viruses), and other system-related problems.
Other problems	The threats in this category are problems or situations that are outside the control of an organization. This category of threats includes natural disasters (e.g., floods, earthquakes) and interdependency risks. Interdependency risks include the unavailability of critical infrastructures (e.g., power supply).

これ以降のステップでは同定された脅威を基にそのリスクの同定・分析、対抗策の検討が行われるが、ここでは説明を省略する。

上記説明でもワークシートを[30]より引用しているが、OCTAVE Allegro はステップごとの詳細なアクティビティや用いるワークシートが定義されている。

⑤ JASO 自動車-情報セキュリティガイド手法

車載ネットワークシステムの脅威の抽出および対策の立案手順を示したガイドで、評価対象定義（本報告書の前提条件の明確化に相当）、脅威分析、リスク評価、対策の策定、さらに対策に対応する CC の要件選択方法までが記載されている。ここでは、評価対象定義、及び脅威分析について説明する。

評価対象定義は次に実施される脅威分析の入力となる情報を明確化する段階である。具体的にはシステム概要を入力として以下の三つの資料を作成する。

A) 評価対象モデル図（図 3.1.4-8）: DFD（Data Flow Diagram）によりシステムの構成要素間の情報のやり取りを表現する。これにより脅威分析での攻撃の入口（攻撃経路）が洗い出される。

B) モジュール機能一覧表（図 3.1.4-9）: 評価対象モデルにより明確になったモジュールごとに機能、保護資産、CIA（機密性 : Confidentiality、完全性 : Integrity、可用性 : Availability）への影響の有無を記載。これにより攻撃対象となる保護資産および、脅威分析での具体的な脅威が洗い出される。

C) ライフサイクル一覧表（図 3.1.4-10）: 対象システムのライフサイクルを明確にし、そこでの関与者とその役割を明確に記載する。これは脅威分析での攻撃実施フェイズ、攻撃者の洗い出しに使用される。

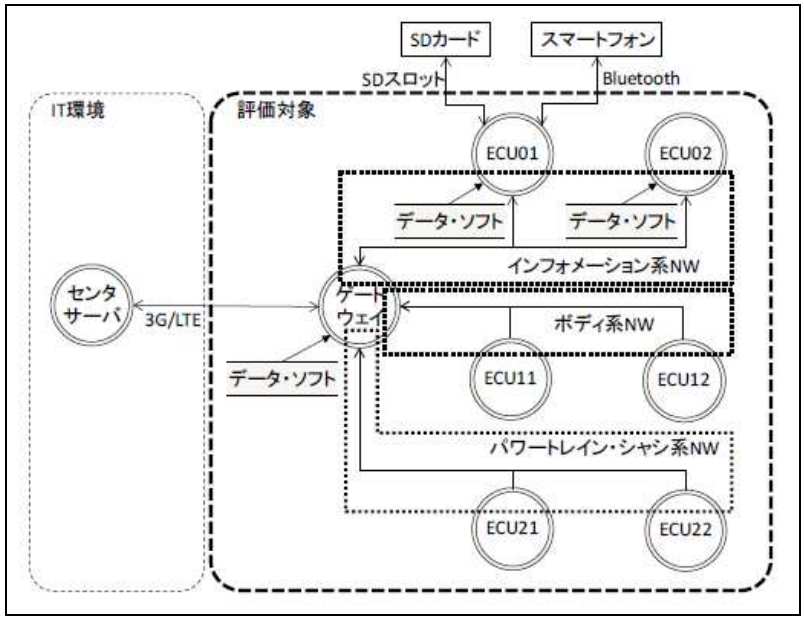


図 3.1.4-8　評価対象モデル図の例（[31] 図 B.1 を引用）

#	モジュール名	機能	保護資産	C	I	A
1	ゲートウェイ	・認証機能 センタサーバの識別と認証を行う	認証機能		○	○
			認証鍵	○	○	
		・情報転送機能 ECU 生成情報をセンタサーバに転送する センタサーバ生成情報を ECU に転送する	情報転送機能		○	○
2	インフォメーション ECU （ECU01，02）	・インフォメーション機能 ゲートウェイを介してセンタサーバから受信した情報を表示デバイスに表示する	インフォメーション機能		○	○
		・センタサーバ問合せ機能 ゲートウェイを介して車両識別情報と問合せコマンドをセンタサーバに送信し，センタサーバが生成した情報を搭乗者に提供する	センタサーバ問合せ機能		○	○
			車両識別情報	○	○	
		・スマートフォン通信機能 Bluetooth インタフェースを介してスマートフォンとの間でデ	スマートフォン通信機能		○	○

図 3.1.4-9　モジュール機能一覧表の例（[31] 表 B.1 を引用）

フェーズ	サブフェーズ	概要	関与者
企画	―	OEM において車両の製品企画を行い，車両の機能・非機能要件を定義する。	OEM 職員 第三者
開発	製品設計	OEM，もしくはサプライヤにおいて，要件に従い，システム，ハードウェア，ソフトウェアの仕様書・設計書を作成する。	OEM 職員 サプライヤ職員 第三者
	製造	OEM，もしくはサプライヤにおいて，仕様書・設計書に基づき，部品，システム，車両を製造する。	OEM 職員 サプライヤ職員 第三者
運用	運送	運送業者は，製造した部品，システム，車両を運送する。	OEM 職員 運送業者 ディーラ職員 第三者
	個人化 （初期設定）	ディーラ職員は，車両を所有者・利用者に受け渡す前の初期設定を実施する。（ETC やマルチメディア系 ECU など）	ディーラ職員 所有者/利用者 第三者
	定常運用・利用	所有者や利用者が自動車を日常的に使用する。	所有者/利用者 サービス事業者 第三者
	メンテナンス	ディーラ職員，もしくは整備工場職員は，車両の修理や車検を実施する	ディーラ職員 整備工場職員

図 3.1.4-10　基本的なライフサイクル一覧表（[31] 表 B.2 を引用）

上記の資料を基に脅威の同定が実施される。まず保護資産（B によって列挙されている）ごとに以下の観点について A、B、C の資料より情報を列挙する（図 3.1.4-11）。

a) Where：攻撃の入口。A によって洗い出される。
b) Who：攻撃者（攻撃を行うことができる人）。C によって洗い出される。
c) When：攻撃実施フェイズ。C によって洗い出される。
d) Why：攻撃の動機。故意と過失の二つを検討対象とする。ただし、故意に攻撃を行わないとした関与者以外は、必ず両方を検討する。
e) What：脅威を CIA の観点に基づいて具体的な内容を記載する。B により洗い出される。

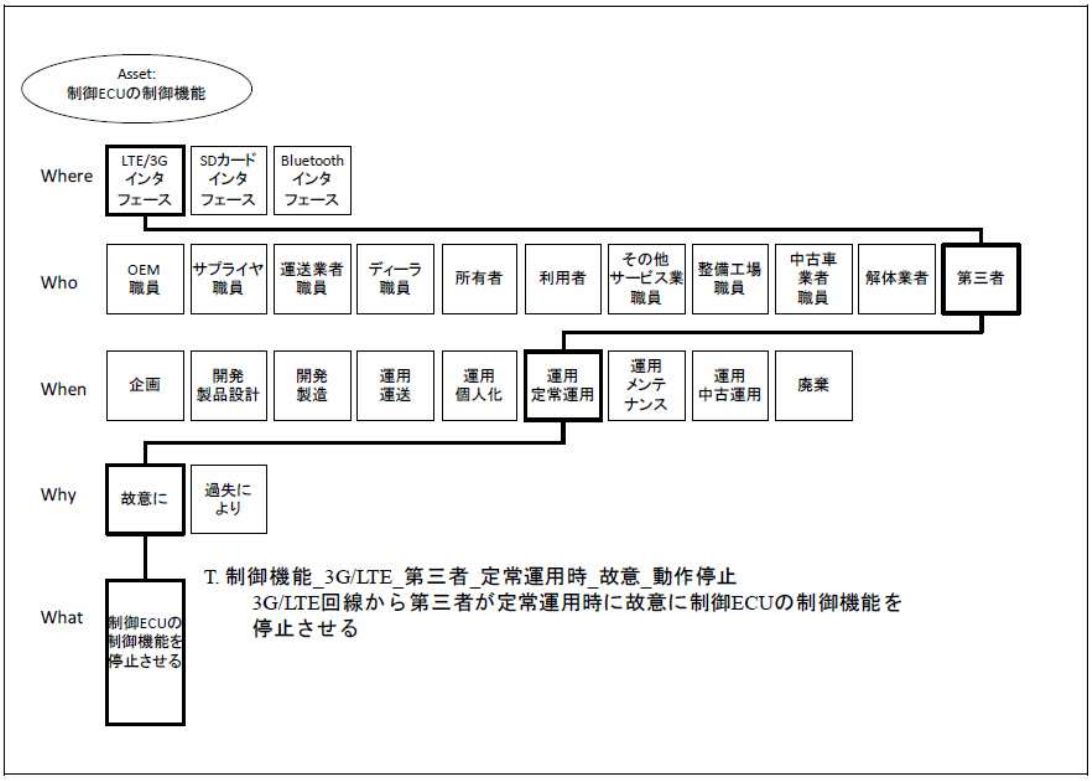


図 3.1.4-11　脅威の同定例（[31]より引用）

列挙された情報のありえるすべての組み合わせが脅威となる。脅威は脅威名がつけられ、その内容と共に一覧としてまとめられる。例えば図 3.1.4-11 で同定されている脅威の脅威名と内容は以下のようになる。

・脅威名「T.制御機能_3G/LTE_第三者_定常運用時_故意_動作停止」
・内容「3G/LTE 回線から第三者が定常運用時に故意に制御 ECU の制御機能を停止させる」

(2) 調査対象分析手法による試行

ここで調査した分析手法が自動車分野における脅威分析でどの程度利用可能であるか、その特徴を明確にするために、既存の分析結果を各手法によって再分析を行い、その結果を比較した。分析は EVITA プロジェクト[2]のアーキテクチャ図（図 3.1.2-1）とユースケース「Use Case 1 – (Car 2 My Car) Safety reaction: Active brake」、「Use Case 2 – (Car 2 My Car) Local Danger Warning from other Car」、「Use Case 18 – (Diagnosis) Flashing per OBD」（[16]を参照）を前提条件として使用した。これらは EVITA プロジェクト[16]で分析された結果のうち、以下の三つの Attack Trees に相当するものである。

A) Attack Active Brake Function
B) Simulate traffic jam
C) OBD flashing

ただし、試行に利用した前提条件が EVITA のものであるため、EVITA で使用されている Attack Trees に関しては試行を実施していない。Attack Trees の試行の代替として EVITA で実施された分析結果のレビューを行い、その問題点と成り得る部分を洗い出した。

以下では Misuse cases、SDL、OCTAVE Allegro、JASO により実施された再分析の結果得られた、Attack Trees での分析との差異、各手法の特徴を説明し、最後に Attack Trees のレビュー結果を説明する。

① Misuse cases による試行結果

EVITA で同定されている脅威のうち、一部の脅威を同定するには保護資産の記述に工夫が必要であることが分かった。また、EVITA で同定されていない脅威が一部同定されている。

一般的には保護資産は情報資産であり、コンポーネントや通信経路は扱わないと考えられる。そのためジャミングや DoS 攻撃といった脅威は同定しにくいと考えられる。本分析ではシステムのコンポーネント、通信経路を明示的に保護資産として記述することにより、それらに対するジャミングや DoS 攻撃が脅威として同定がなされている。

「車両になりすまし、偽の緊急ブレーキ情報を送信する」という脅威が同定されている。これは EVITA では同定されていない脅威である。本分析では、対象システムの保護資産である緊急ブレーキ情報から同定されたものである。EVITA の分析では、緊急ブレーキを妨害するという目的で実施される脅威を同定しているため、意図しない緊急ブレーキをかけさせるという結果を引き起こす脅威は対象外としているものと考えられる。

以上のように、情報資産に関しての脅威については Attack Trees と同程度の脅威が同定可能であるが、ジャミングや DoS 攻撃などを同定するためには、保護資産の記述に工夫が必要であった。

② SDL による試行結果

分析の結果、EVITA で同定されている脅威に対し、一部の脅威が同定されていない。一方で、EVITA の対応する Attack Trees では同定されていない脅威が同定されている。

同定されていない EVITA の脅威は、Simulate Traffic Jam で同定されている「RSU への攻撃」がその例である。本件での評価の範囲は車両であり、RSU、診断機器、車内持込み機器は外部の要素とされている。そのため、前提条件として、それらの機能やアーキテクチャなどは明確化されていないことが原因である。

EVITA で同定されていない脅威としては、Active Brake Function への攻撃で「他車両へのなりすまし」（図 3.1.4-12）、「コンポーネントのコード改竄」がある。他車両へのなりすましは、結果として意図しないブレーキをかけさせることとなる。EVITA はトップダウンの分析で、そのトップ事象としてブレーキをかけさせないことを分析し脅威の同定を

行っている。そのため、逆のことを結果として引き起こす「他車両への成りすまし」は脅威として同定されていない。これは Attack Trees が意図しない結果から分析するトップダウンの分析手法であるのに対し、SDL は各コンポーネントや通信でどのような攻撃が実施されるかというから分析するボトムアップの分析であるためであると考えられる。

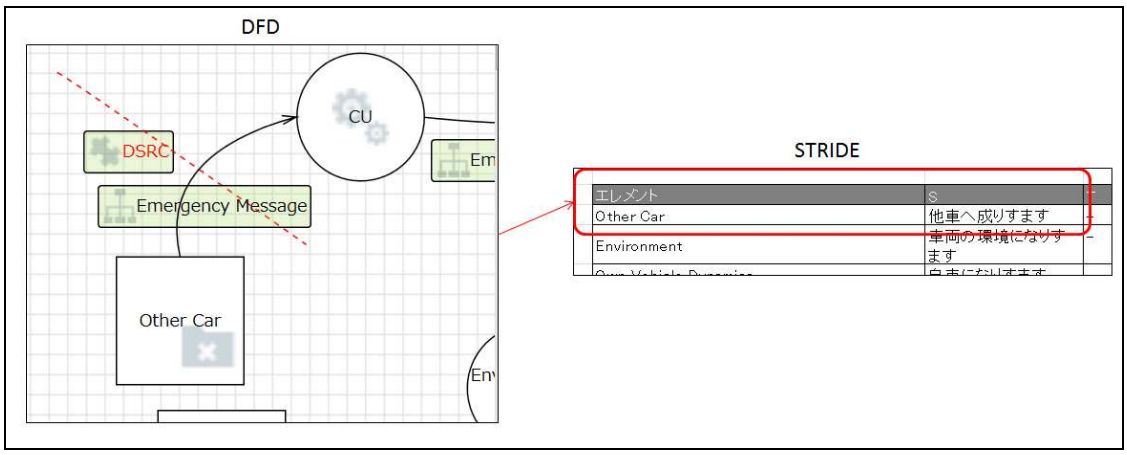


図 3.1.4-12　Active Brake Function の分析における脅威の同定（[28]より引用）

「コンポーネントのコード改竄」は意図しない動作を引き起こし、様々な結果を招くことが可能とされている。EVITA の Simulate Traffic Jam や Active Brake Function は通常の運用時（通常走行中）を前提として分析を実施していると考えられる。通常の運用時にファームウェアのアップデートやコード改竄といったことは不可能であり、脅威としては同定されていないと考えられる。一方で、ファームウェアのアップデートやコードの改竄はメンテナンス時に実施することが想定されているため、Flashing per OBD などの Attack Trees で脅威が同定されている。

以上のように、SDL は Attack Trees と同等の脅威を同定可能であるが、その分析の観点の違いから、Attack Trees では同定されない脅威が同定可能であること、各脅威がどのような結果を導くかの検討が必要になる。

③ OCTAVE Allegro による試行結果

分析の結果、他の手法と異なり、EVITA で同定されている脅威が全て同定されている。また、EVITA の対応する Attack Trees で同定されていない脅威も同定されており、特に、他の手法では同定できなかった、本件で対象範囲外とされている機器への攻撃が同定されている。本手法で分析時に使用する前提条件は、まず情報資産に絞られる。情報資産が明確化された後は、その情報資産へアクセス可能な人や物など、関連情報を対象システム内外に関わらず列挙する。他の手法のようにアーキテクチャ図等、対象範囲を明確化する情報は明示的には使用されない。そのため、対象範囲外とした機器の脅威も同定される。

対象範囲を明確にしないことは、対象範囲外の脅威を同定する場合もあるが、対象範囲内の脅威の同定漏れが起こる可能性も高い、そのため避けるべきであると考える。

EVITA で同定されていない脅威としては、Active Brake Function における前方車両へのなりすましがある。本手法では、情報資産「緊急メッセージ」に対する脅威として同定されている。「緊急メッセージ」が誰によって作成・送信され、だれが受け取り、どのように処理するかのプロファイルでの記載、information container として他の車両が挙げられていることから、脅威が同定されている。

以上のように Attack Trees と同様の脅威を同定することが可能であると考えられる。一方で、情報資産に注目して脅威の同定を実施するため、プロファイルや information container に記載する情報を詳細に記述しなくては、機器への攻撃やソフトウェアコードの改竄などが同定しにくくなると考えられるため注意が必要である。

④ JASO 自動車-情報セキュリティガイド手法による試行結果

分析の結果、EVITA で同定されている脅威に対し、同定できたものとできなかったものが存在していた。その一方で、EVITA の対応する Attack Trees で同定されていない脅威が、JASO では同定されている。

EVITA で同定されているが JASO で同定できなかった脅威は、二つに分類される。一つ目の分類は、評価範囲内の通信経路に対する攻撃である。例えば、Attack Trees では Active Brake Function において、データ通信の妨害・遅延のため、車内の Backbone-Bus や Chassis System-Bus へのジャミングが同定されている。JASO では車内通信は評価対象内であり、外部からの直接の通信経路を持たない。そのため、脅威の同定がされにくいと考えられる。このような攻撃は実際に存在しており、タイヤ空気圧モニタリングシステムへの攻撃[32]などが報告されている。今後、車内の通信の無線化も進む可能性があるため、この点をどのように解決するかは重要であると考えられる。

二つ目の分類は対象範囲外の機器への攻撃である。Simulate Traffic Jam で同定されている「RSU（Road Side Unit）への攻撃」がその例である。本件での評価の範囲は車両であり、RSU、診断機器、車内持込み機器は外部の要素とされている。そのため、前提条件として、それらの機能やアーキテクチャなどは明確化されていないことが原因である。

次に JASO で同定されているが、EVITA で同定されていない脅威としては、「前方車両になりすます」脅威が同定されている。これは、成りすますことにより、意図しないブレーキを行わせるという結果につながる攻撃である。対応する Attack Trees では Active Brake を妨害・遅延する脅威を同定しているため、この様な脅威が同定されていない。

EVITA は意図しない結果から脅威を同定しているトップダウン手法であるのに対し、JASO はモジュールでどのような脅威があり得るかを考慮し、それがどのような結果を招くかを分析するボトムアップ手法であることがこのような 差異を生んだ理由である（EVITA では Active Brake が意図せずかかることは問題ないと考え、分析していないと考えられる）。図 3.1.4-13 に JASO 脅威分析結果を示す。

図 3.1.4-13　JASO 脅威分析結果（[31]より抽出）

また、JASO の手法を用いる際にはモジュール機能概要一覧表を作成する際に、モジュールの分け方に注意が必要と考えられる。モジュール機能概要一覧表は評価対象モデル図を基に、いくつかのモジュールを統合して一つのモジュールとして扱い、その機能を列挙している。どのモジュールを統合して扱うかは、観点により様々な方法があると考えられる。JASO テクニカルペーパー[31]の図 B.1 および表 B.1 のように系統ごとに ECU をモジュールとして扱うと、Chassis System-Bus 内の Chassis System Control (CSC)と Brake Control Unit (BCU)間の通信は失われ、CSC へ DoS 攻撃を行い、ブレーキコマンドを遅らせるという脅威が漏れる可能性がある。

⑤ Attack Trees による分析結果（EVITA）のレビュー

本節では EVITA で実施された Attack Trees による脅威分析結果について、レビューを実施した。レビューの結果を表 3.1.4-9 に示す。

表 3.1.4-9　EVITA の Attack Tree レビュー結果

ID	Attack Tree	ノード ID	ノードの説明	コメント
1	Attack Tree 1	[1.1]	「緊急車両になりすます」	分析の前提となるユースケースに緊急車両に関するものが無いため、このような分析を行うことは困難だと考えられる。
2		[1.1.1.1.2.2.1.1.]	「実際の鍵の入手または、偽造鍵の生成」	「実際の鍵の入手」と「偽の鍵の生成」を一つの攻撃として扱うのは問題があると考える。その理由は、両者の Attack Probability（6.1.3 節を参照）が異なる可能性があると考えたからである。そのため、Attack Tree としては何らかの中間事象を加え、「実際の鍵の入手」OR「偽の鍵の生成」という構造になる必要があるではないだろうか。
3	Attack Tree 2	[2.2.2.1]	「RSU から Authority への通信に対し攻撃する」	上位の攻撃と逆の方向の通信に対し攻撃しており、上位の攻撃を達成できないのではないか。
4	Attack Tree 3	[3.1.1.2.2.1]	「無線通信経路で盗聴、搾取、変更、挿入、リプレイで攻撃する」	盗聴、搾取、変更、挿入リプレイを組み合わせた攻撃であるならば、そのように Attack Tree を構成すべきではないだろうか。
5	Attack Tree 4	[4.2]	「インフラへの攻撃」	インフラへ攻撃することで上位の攻撃を達成可能となると考えられるが、RSU などインフラは対象の通信相手先であり、分析の範囲外ではないだろうか。もし、分析対象である場合は前提条件として必要な条件が不足していると考えられる。 どちらの場合においても、現在の前提条件では、このような攻撃を分析するのは困難であると思われる。
6	Attack Tree 5	[5.3.2.1]	「無線通信へ攻撃し、backbone bus の警告メッセージを盗聴、搾取、改竄、挿入、リプレイする 」	盗聴、搾取、改竄、挿入、リプレイを組み合わせた攻撃であるならば、そのように Attack Tree を構成すべきではないだろうか。
7		[5.3.1.1]	「無線通信へ攻撃し、backbone bus の警告メッセージを盗聴、搾取、改竄、挿入する」	盗聴、搾取、改竄、挿入を組み合わせた攻撃であるならば、そのように Attack Tree を構成すべきではないだろうか。
8	Attack Tree 6	[6.1.2.1][6.2.1.1]	「無線通信から連絡先電話番号の変更」	ユースケースによると連絡先電話番号は E-Call が行われた後に使用される保護資産であり、上位の攻撃である「事故を起こしていないのに E-Call を起こす」を達成できない攻撃ではないか。
9		[6.1.2.2][6.2.1.2]	「無線通信から変更された位置情報	ユースケースによると位置情報は E-Call が行われた後に使用される保護

			を送信」	資産であり、上位の攻撃である「事故を起こしていないのに E-Call を起こす」を達成できない攻撃ではないか。
10	Attack Tree 7	[7.1.1.2]	「バスパラメータの改竄 」	この次にバスパラメータと思われるものが列挙されている。これらがどのようなことを意味しているのかの記述が無い。
11		[7.2.1], [7.2.2.1]	「PTC バス上のペリフェラルからの警告送信」、「同じドメインからの送信」	攻撃間に依存関係の様な線が引かれているが、何を意味しているか記述が無い。
12	Attack Tree 8	[8.1.1.1.1], [8.1.1.2.1], [8.2.1]	「バックボーンで盗聴、搾取、改竄、挿入によりメッセージの生成する」、「バックボーンバスへ周囲の車両からブレーキ情報を流す」	攻撃間に依存関係の様な線が引かれているが、何を意味しているか記述が無い
13		[8.2.1.2.1]	「In-Vehicle 通信での盗聴､搾取､改竄、挿入」	盗聴、搾取、改竄、挿入を組み合わせた攻撃であるならば、そのように Attack Tree を構成すべきではないだろうか。
14	Attack Tree 9	[9.2.1.3]	「In-Vehicle 通信の CS-Bus に偽造した環境情報メッセージを送信する（盗聴、搾取,改竄、挿入、リプレイ)」	盗聴、搾取,改竄、挿入、リプレイを組み合わせた攻撃であるならば、そのように Attack Tree を構成すべきではないだろうか。
15		[9.3.2]	「ブレーキコントローラにフォールバックモードに入るよう強制する」	ブレーキコントローラにフォールバックモードあることが明示されていない。実際の分析時には漏れる可能性があると考えられる。
16	Attack Tree 14	関連ノードなし	関連ノードなし	修理工場において､Diagnosis Tool と修理工場端末間での中間者攻撃が可能である[33]。
17		[14]	「OBD からのフラッシング攻撃 」	他の Attack Tree 10 Prevent driver from passing toll gate で「OBD から ECU にマルウェアをフラッシングする」という攻撃の下位に本 Attack Tree が配置されている。本 Attack Tree では、正当なフラッシングを妨害するという攻撃も含まれており、正確な分析がなされていないのではないだろうか。

表 3.1.4-9 のレビュー結果より、以下の Attack Trees の問題点が得られている。レビュー結果の一部（ID2、5、10、11、12、16、17）は Attack Trees の問題点ではなく、分析結果の問題点であるため、ここでは個別に詳細な説明は行わない。

・分析の詳細度が不明確

・保護資産が同定されていない

・アタックサーフェイスが同定されていない
・ユースケース（または攻撃者の動機）と Attack Tree の関係が不明確

上記に加え、レビュー結果に関連しないものとして、以下の問題点もあげられている。
・多段攻撃の同定が困難

以下に、各問題点についての説明と関連するレビュー結果を示す。

(ⅰ) 分析の詳細度が不明確

Attack Trees は攻撃の目的から詳細な攻撃手法へと分解するトップダウンの手法である。この詳細化が、どこまで実施されていれば十分であるか、手法では規定されていない。そのため、詳細化レベルの規定は分析実施前に明確化すべきと考える。詳細化レベルの規定を行わない場合、分析結果の粒度にばらつきが生じ、リスクアセスメントが困難になる可能性がある。また、リスクアセスメントの結果が不正確になる可能性もあると考えらえる。

本レビューでは ID4、6、7、13、14 の結果が関連している。EVITA プロジェクトでは、これらの詳細化レベルでリスクアセスメントが可能であると判断したと考えられる。しかし、その説明がなされていないため判断が適切であるか評価できず、より詳細化が必要でないかというレビュー結果に至っている。

(ⅱ) 保護資産が同定されていない

Attack Tree のリーフノードは保護資産が記載される。しかし、Attack Trees では保護資産の同定がされていない。そのため、分析時に保護資産の検討漏れが生じ、必要な脅威が漏れる可能性がある。

本レビューでは ID8、9 の結果が関連している。それぞれのリーフノードで使用されている保護資産は E-Call が行われた後に使用されるものとユースケースから読み取れる。しかし、分析結果では E-Call を起こすために使用されている。ユースケースにおいて、これらの保護資産がどこで格納され、使用されるかを明確にされていないことが、この原因と考えられる。また、本レビューの ID15 からもリーフノードではないが、保護資産が同定されていないという問題点が得られる。ただし、ID15 のレビュー結果は「ユースケースから読み取れない保護資産（フォールバックモード）が分析に使用されている」というもので、考察と逆の指摘となっている。

(ⅲ) アタックサーフェイスが同定されていない

Attack Trees で分析を実施する際に、アタックサーフェイスが同定されていない。そのため、アタックサーフェイスが全て網羅されているか不明確であり、脅威が漏れる可能性がある。

本レビューでは ID3 が関連している。アタックサーフェイスが明確になっていないため、上位の攻撃で使用しているアタックサーフェイスと、下位の攻撃で使用しているものが異なってしまっていると考えられる。

(ⅳ) ユースケース（または攻撃者の動機）と Attack Tree の関係が不明確

Attack Tree のルートノードはユースケースと攻撃者の動機の組み合わせにより導出されている。しかし、各 Attack Tree がどのユースケースと動機を組み合わせたかは明確に記載されていない。どのような組み合わせがあり、どのような取捨選択が行われたか明確でないと、ルートノードの同定漏れが起きる可能性がある。

本レビューでは ID1 が関連している。ID1 は考察とは逆に組み合わせとして存在していないものが、Attack Tree に現れている。

(ⅴ) 多段攻撃の同定が困難

Attack Trees では保護資産はリーフノードとして現れる。そのため、ある保護資産を攻撃し、それを踏み台として別の保護資産を攻撃する、というものを表現することは難しいと考えられる。保護資産を Attack Trees でどのように扱うと、そのような攻撃を同定可能になるか検討が必要であると考える。

一方で Attack Trees の利点として以下の様な点があると考えられる。

a. 分析範囲が明確

Attack Trees ではユースケースごとにシステムアーキテクチャの関連する部分が明確になっている。そのため、分析の範囲を限定でき、効率的に分析が可能になっていると考えられる。

b. 脅威の影響が明確

ユースケースと動機から Attack Tree のルートノードが導出されているために、脅威の影響が明確である。また、リスクアセスメントも Attack Tree 上で実施可能になっている。

c. 安全分析との親和性が高い

安全分析で広く使用されてきた Fault Trees と似た構造であることから、FTA を実施した経験がある場合に、容易に習得ができると考えられる。また、安全分析とセキュリティの分析の調和・統合を行う際に、まったく異なる構造のものを扱うよりも容易であると考えられる。

(3) 脅威分析に必要な要件

本節では、調査した各分析手法について、その特徴や長所、短所をまとめる。また、自動車への脅威を同定するためにどのような点が不足しているかについて、論文等で報告されている脅威を基に考察を行う。

調査を実施した各分析手法の特徴などを以下の表 3.1.4-10 にまとめる。

表 3.1.4-10　分析手法の特徴

			Attack Trees	Misuse cases	SDL	OCTAVE	JASO
分析手法の特徴			木構造を用いたトップダウンの分析手法。安全分析の Fault Trees と似た手法。	ユースケースを拡張して作成される。保護資産やセキュリティの要求事項まで記載可能。	データの流れに注目した記法 DFD をベースに分析を実施する。脅威の分類である STRIDE を用いて脅威を導出する。	対象システムの情報資産を基にそれに対する脅威を同定する。脅威の同定、リスク評価は詳細なステップごとにワークシートを埋める形で実施される。	保護資産ごとに Where、Who、When、Why, What について情報をリストアップし、脅威を同定する。
分析に使用する情報	保護資産に関する情報	保護資産	情報資産のみでなく、通信経路、システムのコンポーネントも保護資産としている。	基本的には情報資産を保護資産としている。	情報資産を保護資産としている。	情報資産を保護資産としている。	情報資産だけでなく、システムのコンポーネントも保護資産としている。
		影響する性質	Safety、Financial、Privacy、Operational を結果から分類する。	特に明確化していない。	保護資産に対する脅威として STRIDE を使用する。	CIA を使用し順位付けを行う。	CIA を使用する。
		格納場所			DFD により表現する。	明確化する	モジュール機能一覧表で記載する。
	アタックサーフェイス				DFD で明確化する。どこをアタックサーフェイスとするかは、分析者による。		DFD に外部との通信経路を記載し、攻撃の入口として同定する。
	攻撃者			考慮する。		考慮する。	攻撃が実施されるライフサイクルに関係する人を特定する。
	動機			攻撃者の得る利益として同定。			

脅威分析を実施するために必要となる要件について以下にまとめる。

【保護資産】

保護資産はどのような脅威分析手法においても明確される重要な情報である。ただし、何を保護資産として明確にするか、保護資産に関連する情報として何を明確化するかは、各手法で異なる。システムのコンポーネントへの攻撃（不正なファームウェアへのアップデートなど）により安全性などへ影響を及ぼす。そのため、一般的な情報資産に加え、システムのコンポーネント、通信経路などを明確にする必要がある。

次に、保護資産そのものではなく、それに関連する情報も明確化する必要がある。関連する情報としては、保護資産が影響する性質、保護資産の格納場所がある。保護資産の影響する性質は従来の情報セキュリティで提案されているCIAのほかに、安全性、財務、プライバシー、運用といったものもある。CIAなどの性質を利用することで、保護資産（特に情報資産）に対する脅威の同定漏れを防ぐことが期待できる。脅威のリスクを決定する際には、安全性のリスクと同様に、脅威がもたらす結果の深刻度も見積もるのが一般的になってきている。結果の深刻度を見積もる対象は、脅威がもたらす結果である。

保護資産の格納場所とは、情報資産であれば、どのコンポーネントで処理、通信、記録されるかを表している。システムのコンポーネントの場合はどのような場所に設置されているかということを表す。脅威分析を実施する際には、各保護資産へアクセス可能となる場所の特定が重要であり、これが明確でない場合には同定されるべき脅威が漏れてしまう可能性がある。これは次に説明するアタックサーフェイスと非常に深くかかわる事項である。

【アタックサーフェイス】

アタックサーフェイスは攻撃の経路であり、保護資産へつながる通信経路として同定される。アタックサーフェイスはシステムの脆弱性を分析し、どこから攻撃可能であるかを検討するための情報である。いくつかの手法で利用されている情報であるが、SDLではトラストバウンダリー、JASOでは攻撃の入口と用語が異なっている。一般的なアーキテクチャ図等で通信経路は明確になっているが、通信経路と保護資産の関係は明確ではなく、アタックサーフェイスとして同定することが必要となる。

アタックサーフェイスの記載がないと、ある通信経路からの攻撃が同定されない可能性がある。また、アタックサーフェイスは外部との通信経路のみでなく、システム内部の通信経路にも同定されなくてはならない。例えば、Tire Pressure Monitoring Systemのように、センサから無線通信でデータを送信するなど、内部通信経路であっても攻撃可能な場合があるためである[32]。

【攻撃者】

脅威はそれを引き起こす人（攻撃者）によりその可能性が異なる。そのため、攻撃者を明確にして脅威を同定することは、後のリスクを決定する際の攻撃の容易さの見積もりの指標となる。攻撃者はシステムの利用状況により異なる。例えば自動車の通常

利用時であればドライバ、サービス業者などが考えられるが、メンテナンス時にはサービス業者の代わりにディーラ職員、整備工場職員が加わる。そのため、利用状況と共に明確にするために、ユースケースを基に明確化が行われる。

【攻撃の動機】

攻撃者がなぜ攻撃を実施したかを明確にする。これは、Attack Trees のようにトップダウンの分析を実施する際に特に必要なる情報である。また、攻撃の動機はリスクを決定する際のパラメータである深刻度を見積もる際に、どの性質（安全性やプライバシーなど）の深刻度を見積もるかを明確にすることとなるため、分析手法によらず明確にすることは重要である。以上のことから攻撃の動機としては、より具体的にどのような利益を攻撃者が得ようとしているかまで明確にすべきと考える。

以上のように分析手法の調査・試行から自動車の脅威分析に必要となる情報がその役割と共に明確になった。さらに、調査・分析以外に、共通システムアーキテクチャ案の検討などからも分析の要件が導出されている。導出された要件は保護資産間の関係、脅威とセキュリティ要求の関係、Trustworthiness Level の分析への使用、アーキテクチャ図へのドライバの導入、複数の脅威分析手法の組み合わせである。これらの要件について説明する。

【保護資産間の関係】

保護資産間の関係を明確にすることで、さらに高度な脅威の同定分析が可能になると考えられる。例えば、現状すでに多段攻撃は可能であることが報告されており、分析手法で、それが同定できる必要がある。ある保護資産への攻撃が成功することで、それを踏み台としてより重要な別の保護資産への攻撃が可能となる場合、後者の重要な保護資産が前者の保護資産に何らかの依存関係があると考えられる。そのため、保護資産間の関係を明確にすることで多段攻撃の同定が可能になると考えられる。

【脅威とセキュリティ要求の関係】

通常のセキュリティの開発プロセスは、脅威を同定し、そのリスクを見積もり、リスクを低減するセキュリティ要求を導出するという流れになる。そのため脅威同定とセキュリティ要求導出は異なるフェイズであるというのが一般的である。しかし、脅威とセキュリティ要求には密接な関係があり、その関係を明確にしつつ双方の分析を進める方法も考えられる。例えば既存の研究成果としては Attack Trees にセキュリティ要求を追加する Attack Defense Trees の研究があり、その他に Attack Trees とセキュリティの要求木の対応関係を考慮するというアイデアもある。

さらに、セキュリティ要求は脅威のリスクを低減することを目的としている。しかし、導出されたセキュリティ要求で脅威のリスクがどの程度低減しているか、十分であるかの計算方法は確立していない。以上のように脅威とセキュリティ要求の関係を明確にする分析方法、セキュリティ要求によるリスク低減の計算方法も必要になると考えられる。

【Trustworthiness Level の分析への使用】

Trustworthiness Level とは通信先がどれだけ信頼できるかを表すレベルで、航空機のセキュリティ規格である DO-356 [34]で提案されているものである。この Trustworthiness Level を分析に使用し、Level の高低でセキュリティ対策を変更するという考え方もある。今後、路車間、車車間通信が重要な役割を担う自動運転では、非常に重要な要素になると考える。

【複数の脅威分析手法の組み合わせ】

本件では様々な分析手法を調査した結果、手法毎に長所・短所があり、ある一つの分析手法ですべてをカバーすることは困難である。そのため、複数の脅威分析手法をその長所を基に組み合わせて使用するべきであると考える。複数の手法を組み合わせることで、脅威の同定漏れを防ぐ効果も期待される。脅威分析をどのようなプロセスで実施し、その各段階でどの手法を用いるとより良い脅威分析が実施できるかが、今後検討が必要な課題として導出された。

3.1.5 共通脅威リスクアセスメント

現在、車載の機能安全に関連するリスクアセスメントの基準としては、ISO 26262 の Automotive Safety Integrity Level (ASIL) があるが、セキュリティに関するリスクアセスメントのための ASIL と同等なメトリクス、例えば Automotive Security Integrity Level (ASecIL) と呼べるようなものはまだ確立されておらず、一般的に利用されていないのが現状である。一方で、EVITA のように、CC（Common Criteria）の CEM（Common Evaluation Methodology）を基にし、CC との調和を考慮したメトリクスを採用した例もある。

ここでは、車載のセキュリティに関するリスクアセスメントのメトリクスを検討するために、規格や研究レベルで提案されている脅威リスクアセスメントのメトリクスについて調査を行った。調査結果はリスク決定のパラメータおよび、その見積もり方法の比較を行い、車載のセキュリティに関するリスクアセスメントのメトリクスに推奨される事項を考察した。

(1) リスクアセスメントのメトリクス

① Security Level

Security Level (SecL)は、安全性やプライバシーなどの性質についてセキュリティからの影響を考慮する手法 Security-Aware Hazard Analysis and Risk Assessment (SAHARA) [35]で使用されている脅威のリスクアセスメントのメトリクスである。

同定された脅威の SecL は以下の三つの観点により決定される。

・Threat Criticality (T): 脅威の重大さ。影響する性質より決定される。

・Know-how (K): 脅威を引き起こすために必要とされる知識のレベル。

・Resources (R): 脅威を引き起こすために必要とされるツールの種類。

上記の観点は 0 から 3（K については 2 まで）のレベルで評価される。K と R は脅威の引き起こしやすさに関するもので、レベルが大きいほど引き起こすのが難しいと定義されている。一方で T は脅威ではなく、その結果に関するものである。EVITA でも脅威の結果に対しその深刻度 severity が見積もられているが、これとは大きく異なる。EVITA でのメトリクスが性質（安全性、プライバシー、財務、運用）での被害の大きさで見積もるのに対し（安全性の場合は人の負う怪我の大きさ（死亡を含む））、SecL では影響する性質によってレベルが変化する。これら各観点の各レベルの説明を図 3.1.5-1 に示す。

Level	Knowledge example	Resources example	Threat criticality example
0	Average driver, unknown internals	No tools required	No impact
1	Basic understanding of internals	Standard tools, screwdriver	Annoying, partial reduced service
2	Internals disclose, focused interests	Non-standard tools, sniffer, oscilloscope	Damage of goods, invoice manipulation, privacy
3		Advanced tools, simulator, flasher	Life-threatening possible

図 3.1.5-1　セキュリティの脅威に対する T、K、R の分類例（[36]より引用）

見積もられた各観点のレベルを用い、以下の図 3.1.5-2 で示すマトリクスに従い SecL を決定する。SecL は 3 を最大（最も危険なもの）とし 0 を最小（影響がないまたは無視できるもの）としている。

Required Resources 'R'	Required Know-How 'K'	Threat Level 'T'			
		0	1	2	3
0	0	0	3	4	4
	1	0	2	3	4
	2	0	1	2	3
1	0	0	2	3	4
	1	0	1	2	3
	2	0	0	1	2
2	0	0	1	2	3
	1	0	0	1	2
	2	0	0	0	1
3	0	0	0	1	2
	1	0	0	0	1
	2	0	0	0	1

図 3.1.5-2　SecL 決定マトリクス（[36]より引用）

さらに本アセスメントのメトリクスは安全性および Serviceability（サービサビリティ）のアセスメントのメトリクスとの統合について提案がなされている（[36]）。安全性については、ISO 26262[4]の ASIL を用いている。サービサビリティは信頼性と保守性を合わせた概念である。サービサビリティでは Deterioration Resistance Level (DRL)というメトリクスが使用されている。DRL は Service Deterioration Analysis (SDA) [37]という手法で使用されている信頼性とアベイラビリティのメトリクスである。これらのメトリクスにより評価された結果を基にそれぞれの性質間のトレードオフを検討する方法について提案されている。例えば、サービサビリティと安全性の場合、「DRL が 3 以上の場合は safe state（安全状態）をレビューし、縮退運転のコンセプトが必要となる」などである。

② OCTAVE Allegro

OCTAE Allegro においても、脅威が導く望まれない結果と脅威の起こされる可能性により評価を行っている。ただし、OCTAVE Allegro において、リスクと呼ばれているのは、脅威が導く望まれない結果がおこる可能性である。用語の定義による混乱を防ぎ、他の節との比較を容易にするために、本資料においては OCTAVE Allegro の説明を行う際でも、リスクという言葉を OCTAVE Allegro で用いられている意味ではなく、そのほかの資料で用いられている「脅威の深刻さのレベル」の意味で使用する。

すでに述べたようにリスクは脅威が導く結果と脅威の起こる可能性により決定される。

まず、脅威が導く結果に対しては点数がつけられる。結果には様々な種類のものが存在し、一つの脅威で複数の結果を導く可能性もある。例えば、ある脅威によって、個人情報が漏えいし、財務的な被害をこうむることは容易に想像できる。OCTAVE Allegro では、脅威分析の最初の手順として影響の評価軸を決定する。最低限の評価軸としては、顧客の信用、財務、生産性、安全性、法的罰則の 5 つで、必要に応じて定義可能である。さらに、評価軸ごとにそのレベルを High、Moderate、Low の三つに分類する。各レベルに対し High が 3 点、Moderate が 2 点、Low が 1 点とレベルごとに点数が与えられている。そして最後に、評価軸の優先順位を検討し、評価軸ごとに Impact value を与える。Impact value は最下位を 1 点とし、一つ順位が上がるごとに 1 点加点する。

同定された脅威に対し、それが導く結果を分析する。分析により得られた情報を基に、評価軸ごとのレベルが決定されることで、脅威が導く望まれない結果の点数が求められる。評価軸ごとのレベルの点数と Impact value の積を求め、その総和が点数となる。図 3.1.5-3 に、計算の例を示す。例では、Financial が最も重要であり、以下 Reputation、Productivity、Fines/Legal と続き、Safety and Health が最も重要でないという優先度になっている。

Impact Area	Ranking	Impact Value	Score
Reputation	4	Moderate (2)	8
Financial	5	Low (1)	5
Productivity	3	Low (1)	3
Safety and Health	1	Low (1)	1
Fines/Legal	2	High (3)	6
		Total Score	**23**

図 3.1.5-3　望まれない結果の点数計算例（[30]より引用）

一方で脅威が起こる可能性は、定性的に見積もられる。こちらに関しても High、Medium、Low の三つのレベルとなる。具体的に各レベルの詳細は記述されていないが、High は可能性が高いと考えられるもの、Low はありえないような可能性のもの、Medium は、その間である。

上記の点数と可能性のレベルより、図 3.1.5-4 のマトリクスを用いてリスクを決定する。リスクは POOL1 から POOL4 に分類され、POOL1 が最もリスクが高いものである。POOL1 は必ず対抗策を必要とするレベル、POOL2 は対抗策を与えるか先送りするか検討するレベル、POOL3 は先送りするか受容するか検討するレベル、POOL4 は受容するレベルである。

RELATIVE RISK MATRIX			
PROBABILITY	RISK SCORE		
	30 TO 45	16 TO 29	0 TO 15
HIGH	POOL 1	POOL 2	POOL 2
MEDIUM	POOL 2	POOL 2	POOL 3
LOW	POOL 3	POOL 3	POOL 4

図 3.1.5-4　リスクマトリクス（[30]より引用）

(2) リスクアセスメントのメトリクスの比較

調査した各メトリクスにおいてリスクは同定された脅威に対し決定されている。決定のために使用されるパラメータは脅威に関するものと、それ以外に分類できる。

脅威に関するパラメータは脅威の起こりやすさであり、この観点はすべてのアセスメント手法で採用されている。ただし、起こりやすさを見積もる詳細なパラメータはそれぞれ若干異なっていた。EVITA はCC CEM をベースとしたパラメータで経過時間、経験的知識、システムの知識、期間の時間枠、装置を使用している。Security Level では Know-how と Resources の二つのパラメータが使用されている。Know-how は CC CEM の専門性に、Resources は装置に対応する。OCTAVE Allegro では、詳細なパラメータは存在せず、定性的に見積もるのみである。

それ以外のパラメータは脅威による結果の深刻度と、脅威による影響の（人の操作による）コントローラビリティの二つである。影響の深刻度については、各メトリクスで見積もられているがその見積もり方がそれぞれ異なる。各メトリクスとも複数の観点での危害を想定しているが、観点に若干の差異がある。Security Level では影響の種類によってレベルが決定する。そのため、影響の種類についての優先順位が決定されているとみることができる。一方で EVITA と OCTAVE Allegro では影響の種類ごとに被害の大きさを見積もる。OCTAVE Allegro では各観点の優先順位を決定し、優先順に基づいて統合される。EVITA では影響の種類に優先順位はなく、それぞれの影響の種類ごとにリスクが決定される。

複数の性質へ影響が考えられる場合、影響の種類ごとのリスク評価は非常に重要である。また、複数の影響が考えられる場合は、複数の対抗策がトレードオフ関係となる可能性もあり得る。対抗策のトレードオフ関係の検討を行うためには、対抗する脅威が影響する性質と、性質ごとの脅威のリスクをについて考慮する必要があると考えられる。そのため、リスクを評価する際には、性質ごとにリスク評価を行うこと、性質の優先順位の決定が必要になると考える。

コントローラビリティは EVITA のみで使用されている観点である。自動運転においてドライバが全く不要となるのは level 5 以上である。そのため、ドライバに関するパラメータであるコントローラビリティはリスクのアセスメントに重要である。また、今後コントローラビリティを低下させるといった脅威の可能性もあり、その点でも重要なパラメータである。

CC CEM をベースとしたアセスメントのメトリクスは平成 26 年度に調査を実施した。ここでは、平成 26 年度の結果[14]について、この後実施するアセスメントのメトリクスの比較で必要となる情報を説明する。CC CEM ベースのメトリクスは、脅威を起こす容易さを見積もるのが一般的である。ここでは脅威を起こす容易さに加え、脅威の導く結果を考慮している EVITA を比較対象として取り上げる。

EVITA におけるメトリクスの特徴は、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)と組み合わせリスクを見積もることである(ただし、安全性に関するメトリクスは、運転者による回避可能性であるコントローラビリティも加える)。深刻度の 4 つの観点は、安全性、プライバシー、財務、運用であり、以下の図 3.1.5-5 のようになっている。

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	プライバシー : Sp	財務 : Sf	運用 : So
0	ケガなし	プライバシーの侵害なし	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)

図 3.1.5-5　EVITA の深刻度(EVITA Deliverable D2.3 より)

もう一つのパラメータである攻撃の容易さは経過時間、経験的知識、システムの知識、期間の時間枠、装置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[16]を参照)。点数から導かれる攻撃の容易さは図 3.1.5-6 のように分類される。

点数	Attack potential required to identify and exploitattack 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
≧25	高を超えている	1

図 3.1.5-6　EVITA の攻撃の容易さ

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図 3.1.5-7 に示す通りである。

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.

図 3.1.5-7　EVITA のコントローラビリティ（[16]より）

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 に関するものを図 3.1.5-8 にそれ以外を図 3.1.5-9 に示す。

Controllability	Safety Severity	Attack Probalitiy				
		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+

図 3.1.5-8　EVITA の Safety に関するリスク決定マトリクス（[16]より）

Ri (i ∈ {p,f,o})		Attack provability				
		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

図 3.1.5-9　EVITA の Safety 以外に関するリスク決定マトリクス（[16]より作成）

上記の調査の結果として、以下のような要素を考慮したメトリクスを一部に利用することが推奨される

・脅威の起こりやすさについては CC CEM をベースとして、パラメータの値を適宜調整する。
・脅威の影響する性質の優先順位を決定し、性質ごとにその深刻度の評価を行う。
・コントローラビリティをリスクのパラメータに使用する。

リスクアセスメントのメトリクスを比較した結果をまとめたのが表 3.1.5-1 のパラメータの比較表である。表中で横方向に対応するパラメータを配置しており、「-」は対応するものがないことを表している。

表 3.1.5-1　パラメータの比較表

	EVITA		Security Level		OCTAVE Allegro	
脅威により生じる結果	安全性、プライバシー、財務、運用に関して危害の大きさをそれぞれ見積もる。安全性に対するリスクが独立してあるため、安全性とそれ以外のリスクの比較が可能である。	安全性	結果の種類によって見積もる。安全性に対するリスクが他のリスクと統合されているため、安全分析で得られるリスクと調和する際には工夫が必要と考えられる。	安全性	顧客の信頼・評判、財務、生産性、安全性、法制度に関して危害の大きさをそれぞれ見積もる。安全性に対するリスクが独立してあるため、安全性とそれ以外のリスクの比較が可能である。	安全性
		プライバシー		プライバシー		-
		財務		財産		財務
		運用		サービス		-
		-		-		生産性
		-		-		法制度
		-		-		顧客の信頼・評判
脅威に対する評価	脅威の起こりやすさについて見積もる。	経過時間	Know-how と Resources について見積もる。	-	脅威の起こりやすさについて見積もる。詳細な見積もり方法はなし。	-
		専門性		Know-how		-
		システムの知識		-		-
		攻撃の機会		-		-
		装置		Resources		-
その他	コントローラビリティ		-		-	

3.1.6 まとめ

本案件は自動運転の基本システム部分および、その脅威への対抗策の効率的な開発を可能とするための、脅威分析共通プラットフォームの開発を目的としている。ここでは、脅威分析共通プラットフォームの要素を作成する準備として、共通プラットフォームの要素であるシステムアーキテクチャ、ユースケース、脅威分析手法、脅威リスクアセスメントの現状の調査・考察を実施した。また、共通プラットフォームで使用される脅威分析の概念をセキュリティオントロジーとして明確にした。以下では、各要素について結果の概要を説明する。

セキュリティオントロジーとして、脅威分析を実施する際に使用される用語の定義、用語間の関係を明確にした。セキュリティオントロジーでは、今回の調査・考察で抽出された概念を採用している。用語の定義は基本的に NIST SP 800-30 の定義を使用した。ただし、NIST SP 800-30 に定義がない用語は調査対象での定義を使用している。さらに、両者に定義がない用語は調査対象で使用されている文脈より定義を作成した（表 3.1.1-1）。また、用語間の関係は UML のクラス図により、図 3.1.1-1 に示したモデルとして明確化した。

調査結果との対応関係を明確にすることで、この共通システムアーキテクチャ案に、脅威分析で使用するのに十分な情報が含まれているかを評価した。その結果、共通システムアーキテクチャ案は脅威分析に十分使用可能なレベルであるという評価が得られた。一方で、さらに詳細な脅威分析を実施するためには、通信経路と通信相手先の明確化を行うことが推奨されるという結論も得ている。また、共通システムアーキテクチャ案においてすでに考慮されているドライバからの入力について、ドライバからの車両操作の入力先を明確化することにより、さらに詳細な脅威分析の実施が可能になると考えられる。

共通ユースケースでは、現在検討されている自動運転（または自動運転に準ずるシステム）のユースケースを比較し、共通ユースケース案（Appendix C）を作成した。今回の案は CVRIA、ISO/TR 20545 などを用いて作成したが、自動運転の共通ユースケースとしての十分性の評価は別途必要である。また、共通ユースケースは、今後実施されるプロジェクトなどを継続して調査しつつ、定期的なメンテナンスが必要になると考えられる。

汎用脅威分析手法では、自動車分野のみでなく、IT 分野など広く脅威分析手法の調査を行った。また、調査した分析手法による分析試行および、分析結果のレビューを実施することで、各手法の特徴を洗い出し、その比較を行った。結果として、自動車の脅威分析手法に求められる要件が抽出できた。

共通脅威リスクアセスメントでは、広く用いられている CC CEM とは異なるメトリクスの調査を行った。さらに、調査結果を CC CEM の例の一つである EVITA と比較し、リスクアセスメントメトリクスにいくつかの推奨項目を挙げた。

これまでの調査・考察は、プラットフォーム作成のための準備として、共通プラットフォームの要素ごとに、作成のための要件や推奨事項を明確化した。これらの結果は、脅威分析共通プラットフォームの開発に用いることができると考えられる。

参考文献

[1] NIST SP 800-30 Revision 1, Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology, 2012.

[2] EVITA deliverable D2.1: Specification and evaluation of e-security relevant use cases, 2009.

[3] 自動車の情報セキュリティへの 取組みガイド, Information-technology Promotion Agency Japan, 2013.

[4] ISO 26262, “Road vehicles. Functional safety”, 2011 (10 parts).

[5] MISRA: Guidelines for Safety Analysis of Vehicle Based Programmable System, November 2007.

[6] TCG TPM 2.0 Automotive Thin Profile, Trusted Computing Group (TCG), 2015.

[7] 松島 秀樹, 車載制御システムを保護するセキュリティ技術, escar Asia, 2015.

[8] 上田 浩史, 倉地 亮, 高田 広章, 水谷 友洋, 井上 雅之, 堀端 啓史, 車載ネットワークのセキュリティ監視システム, SEI テクニカルレビュー第 187 号, 2015.

[9] 平成 26 年度 次世代高度運転支援システム研究開発・実証プロジェクト 成果報告書, 2015 年 3 月.

[10] 平成 26 年度 グリーン自動車技術調査研究事業 報告書, 2015 年 3 月.

[11] SARTRE Project Final Report, www.sartre-project.eu, 2013.

[12] HAVEit Deliverable D11.1 Function description and requirements, 2008.

[13] Intel Technical White Paper, Advanced Driver Assistant System: Threats, Requirements, Security Solutions, 2015.

[14]（一財）日本自動車研究所：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 26 年度戦略的イノベーション創造プログラム、 2014

[15] Connected Vehicle Reference Implementation Architecture, http://www.iteris.com/cvria/index.html.

[16] EVITA deliverable D2.3: Security requirements for Automotive on-board networks based on dark-side scenarios, 2008.

[17] B. Schneier: Attack Trees: modeling security threats, Dr. Dobb’s J 24 (1999) pp21-9.

[18] IEC 61025: 2006: Fault Trees Analysis.

[19] B. Kordy, S. Mauw, S. Radomirovic, P. Schweitzer: Foundation of Attack-Defense Trees, FAST 2010, LNCS 6561, pp. 80-95, 2011, Springer.

[20] A. Roy, D. S. Kim, and K. S. Trivedi: ACT: Towards unifying the constructs of attack and defense Trees, Security and Communication Networks, 2011:3:1-15.

[21] Guttorm Sindre and Andreas L. Opdahl, Eliciting security requirements by misuse cases, In TOOLS (37), pages 120–131. IEEE Computer Society, 2000.

[22] Guttorm Sindre and Andreas L. Opdahl, Eliciting security requirements with misuse cases, Requirements Engineering Journal, 10(1):34–44, 2005.

[23] John P. McDermott and Chris Fox. Using abuse case models for security requirements analysis. In ACSAC, pages 55–64. IEEE Computer Society, 1999.

[24] Donald Firesmith. Security use cases. Journal of Object Technology, 2(1):53–64, 2003.

[25] T. Okubo, K. Taguchi, and N. Yoshioka. Misuse cases + assets + security goals, In 2009 International Conference on Computational Science and Engineering, pages 424–429, 2009.
[26] T. Okubo, K. Taguchi, Haruhiko Kaiya, and N. Yoshioka, MASG: Advanced Misuse Case Analysis Model with Assets and Security Goals. Journal of Information Processing Vol. 22 No.3, pp536-546, 2014.
[27] Astah Professional, http://astah.change-vision.com/ja/.
[28] Introduction to Microsoft Security Development Lifecycle (SDL) Threat Modeling, https://www.microsoft.com/en-us/sdl/default.aspx.
[29] Security Development Lifecycle Threat Modeling Tool, https://www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx.
[30] Caralli, Richard, James Stevens, Lisa Young and William Wilson, Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Software Engineering Institute, May 2007.
[31] JASO TP15002 自動車―情報セキュリティ分析ガイド, 公益社団法人自動車技術会, 2015.
[32] Ishtiaq Rouf, Rob Miller, Hossen Mustafa, Travis Taylor, Sangho Oh, Wenyuan Xu, Marco Gruteser, Wade Trappe and Ivan Seskar, Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study, USENIX Security Symposium, 2010.
[33] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage, Comprehensive Experimental Analyses of Automotive Attack Surfaces, 20th USENIX Security Symposium, 2011.
[34] RTCA DO 356, Airworthiness Security Methods And Considerations, 2014.
[35] Macher, G., Sporer, H., Berlach, R., Armengaud, E. and Kreiner, C.: SAHARA: a security-aware hazard and risk analysis method. In: 2015 Design, Automation Test in Europe Conference Exhibition (DATE), pp. 621‑624, March 2015.
[36] Georg Macher, Andrea Holler, Harald Sporer, Eric Armengaud and Christian Kreiner, A Comprehensive Safety, Security, and Serviceability Assessment Method, SAFECOMP 2015, LNCS 9337, pp. 410–424, 2015.
[37] Macher, G., Hoeller, A., Sporer, H., Armengaud, E. and Kreiner, C.: Service deterioration analysis (SDA): an early development phase reliability analysis method. In: Review at 45th Annual International Conference on Dependable Systems and Networks (DSN) - RADIANCE Workshop (2015).

3.2a　コンポーネント・車内システムにおける評価技術の検討

3.2a.1　評価方法・評価基準の調査

(1) はじめに

コンポーネントの評価方法・評価基準を調査研究するにあたり、セキュリティで先行する他業界、特に、ICT 業界におけるスマートカード分野を中心に、IC と組込みソフトウェアから構成される電子機器の先行事例と評価技術動向の調査を主体とした。

この他業界の先行事例・評価技術動向の中から、自動車業界のコンポーネント（平成 27 年度は標準 ECU が対象）との類似点等整理した上で、流用可能な部分を活用しながら、自動車業界のコンポーネント評価の既存知見を踏まえた評価方法・評価基準ドラフトを策定するのが、本調査研究の目的である。

(2) 他業界のコンポーネント評価技術動向調査

① 概要

本章では、他業界におけるコンポーネントに実装されているセキュリティ機能を評価する方法や基準をまとめる。コンポーネントは、IC と組込みソフトウェアから構成される電子機器ととらえ、セキュリティ機能の評価技術が成熟している ICT 業界、なかでも、最新のセキュリティ機能の評価技術が進んでいるスマートカード業界や金融端末業界を中心にその技術動向調査を行った。

② 調査対象

他業界のコンポーネント評価技術動向に関連する調査対象としては、ICT 業界で国際評価基準として、広く実際のセキュリティ製品の評価認証に使用されている以下を対象とした。

・ISO15408/18045（CC/CEM）
・ISO19790/24759（CMVP/FIPS）

後者は、ソフトウェア/ファームウェア/ハードウェア形態の暗号モジュールに特化したものであり、調査対象となる自動車業界のコンポーネントに、暗号モジュール相当のセキュリティ機能が実装され評価対象となる場合は、適用性の高い国際基準である。

一方、前者は、特定の製品分野・セキュリティ機能に特化したものではなく、各種コンポーネントから製品・システムをカバーする極めて汎用的な国際基準である。従って、そのままでは自動車業界のコンポーネントとの比較検討対象として広過ぎるので、今回は、自動車業界のコンポーネント（標準 ECU）の製品形態と類似性の多い「ハードウェア/ファームウェア/ソフトウェア」を含めた製品形態を持つ以下のような製品分野のセキュリテ

ィ評価に絞り込んだ調査を行った。

・スマートカード（Smart card）分野

・デジタルタコグラフ（Digital tachograph）分野

・決済端末（POI：Point-of-Interaction）分野

これらの製品分野のセキュリティ機能について、後者（ISO19790/24759－FIPS）レベル相当の評価基準・評価方法を比較検討するには、さらに当該分野の具体的なセキュリティ要件まで詳細化して定義したプロテクションプロファイル（Protection Profile、以降、PP と略記）レベルの要件定義書（セキュリティ機能仕様の定義）が必要となるため、これらの製品分野の調査においては、各分野の主要な PP を調査対象とした。

下表（表 3.2a.1-1）に調査対象の技術文書[1]を示す。

表 3.2a.1-1　調査対象

#	略号	分野	技術文書名
1	[SC]	スマートカードの攻撃	Application of Attack Potential to Smartcards Version 2.9
2	[BSI-PP-0084]	スマートカードの PP	Security IC Platform PP Version 1.0
3	[SB]	セキュリティボックス付ハードウェアの攻撃	Application of Attack Potential to Hardware Devices with Security Boxes Version 2.0
4	[BSI-PP-0057]	デジタルタコグラフの PP	Digital Tachograph - Vehicle Unit Version 1.0
5	[POI]	決済端末の攻撃	Application of Attack Potential to POIs Version 1.0
6	[POIPP]	決済端末の PP	Point of Interaction Protection Profile Version 4.0
7	[FIPS]	暗号モジュール評価基準、試験基準	・FIPS PUB 140-2, Security Requirements for Cryptographic Modules ・Derived Test Requirements [DTR] for FIPS PUB 140-2, Security Requirements for Cryptographic Modules ・Implementation Guidance [IG] for FIPS PUB 140-2 and the Cryptographic Module Validation Program

③ 他業界のコンポーネントの評価技術

(ｉ) ICT 業界におけるコンポーネント評価

他業界のコンポーネント評価技術動向に関連する調査対象とした 2 つのセキュリティ評価技術の概略的な特徴と差異は、以下にまとめることができる（表 3.2a.1-2）。

[1] 文書 1～5 はすべて SOG-IS ホームページからダウンロードできる。http://sogis.org/index_en.html
文書 6 はフランス認証機関 ANSSI のホームページからダウンロードできる。
http://www.ssi.gouv.fr/administration/produits-certifies/cc/profils-de-protection/
文書 7 は NIST のホームページからダウンロードできる。http://csrc.nist.gov/groups/STM/cmvp/standards.html
http://csrc.nist.gov/groups/STM/cmvp/announcements.html

表 3.2a.1-2　CC/CEM と CMVP/FIPS の特徴と差異

	CC/CEM（ISO15408/18045）	**CMVP/FIPS（ISO19790/24759）**
適用範囲	ICT 製品全般に適用可能な評価基準･評価方法	暗号モジュールに特化した試験基準・試験方法
評価要件	評価すべきセキュリティ機能自体を「何を（保護資産）、何から（脅威）、どのような対策方針（セキュリティ対策方針）に基づいて、どう守るのか（機能要件・保証要件）」の視点から開発者自身が（定められた形式に従って）定義する必要がある	定義済み
評価の実施方法	評価は、開発者が定めたセキュリティ機能が、想定した脅威に過不足なく確実に対抗し、正しく実装・テストされ、悪用される脆弱性が残っていないかどうか、定義済みの評価基準・評価方法に基づいて実施される	評価（試験）は、定義・承認済みの標準暗号アルゴリズムの中から開発者が選択した暗号アルゴリズムを対象に、その暗号アルゴリズムを実装した暗号モジュールに対し、定義済みのセキュリティ機能要件・保証要件に対する定義済みの試験基準・試験方法に基づいて実施される
評価のレベル	評価保証レベルは EAL1～EAL7 の 7 段階（民生用は EAL4 まで）	レベル 1～レベル 4 の 4 段階（ソフトウェアの場合は、レベル 2～レベル 4 の動作環境は、EAL2～EAL4 以上相当の CC 評価済み OS 環境が要求される）
ハードウェアを含む製品のセキュリティ評価に関わる主要な要件		
改ざん耐性の要件	FPT_PHP（物理的保護） FDP_ITT（ユーザデータ内部転送） FPT_ITT（TSF データ内部転送）	4.5（物理セキュリティ）
不完全動作回避の要件	FPT_PHP（物理的保護） FPT_FLS（フェールセキュア） FRU_FLT（耐障害性）	4.5.5（環境故障保護）
無許可アクセス防止の要件	FDP_AC*（アクセス制御） FIA_*（利用者識別・認証） FMT_*（セキュリティ管理）	4.3.3（オペレータ認証）
暗号鍵の管理要件	FCS_CKM （暗号鍵管理）	4.7 （暗号鍵管理）
内部状態･内部処理情報漏えい防止の要件	FDP_ITT（ユーザデータ内部転送） FPT_ITT（TSF データ内部転送） FDP_IF*（情報フロー制御） FPT_PHP（物理的保護） FPT_FLS（フェールセキュア） FRU_FLT（耐障害性）	4.11（その他の攻撃の対処） ［最新の ISO19790 では「7.8 非侵襲セキュリティ」も関係する］
製品完全性の保証要件	Part3 保証要件： ADV_*、AGD_*、 ALC *、ATE_*、 AVA_VAN	4.10（設計保証） APPENDIX A 文書要求事項

CC/CEM（ISO15408/18045）が、広範な ICT 製品を対象としているのに対し、CMVP/FIPS（ISO19790/24759）が暗号モジュール製品に特化している点が大きな特徴であり、その対象範囲の違いによって、前者はその評価要件(機能要件・保証要件)が汎用的・抽象的で、しかも予め定められた要件カタログから選択・抽出する形式になっているため、理解しにくく実適用に困難性が伴う（しかし、適用範囲が広い）ものになっているのに対し、後者は暗号モジュールに特化した具体的な要件が規格内に定義済みの要件と明示されているため、理解しやすく実適用が容易（しかし、適用範囲が狭い）という差があることに注意が必要である。

次節以降に各々のコンポーネント評価の考え方を説明する。

(ⅱ) ISO15408/18045 におけるコンポーネント評価の考え方

ISO15408/18045 または[CC]・[CEM]における評価の考え方は、対象となるセキュリティ製品分野それぞれで、消費者団体や政府機関などの調達者が購入したい製品のセキュリティ要件を PP に定義することから始まる。製品ベンダはその PP に適合する製品を開発し、第三者によって評価・認証を受ける。認証を取得した製品は、PP に定義されているセキュリティ要件を適切に実装し、第三者によってその機能がテストされ、評価当時に公知となっている脆弱性を持っていない、ということが自動的に明らかになる。

セキュリティ要件の定義は、セキュリティ対策方針から導かれ、セキュリティ対策方針は想定する運用環境における脅威から導かれる。すなわち、PP 作者である調達側は、製品が設置されたり搭載されたりする運用環境において、製品が扱う資産が棄損されるような脅威を考えることから始まる。次に脅威に対抗するために、運用環境を厳しくするのか、それとも製品のセキュリティ機能で対抗するのか、方針を決める必要がある。前者は運用環境のセキュリティ対策方針として PP に設定され、後者はセキュリティ対策方針[2]として PP に設定される。セキュリティ対策方針を導くことができたら、その方針を実現するためのセキュリティ機能の要件を、要件集である[CC]パート 2 から選択すればよい。要件集に所望の機能の要件がないとか、うまく当てはまらない場合は、執筆者がセキュリティ機能要件を新たに定義することも許されている。

ISO15408/18045 に則った場合、製品のセキュリティ機能の評価は、おおよそ以下のような手順で行われる。

・対象となるセキュリティ機能の決定

CC ではセキュリティターゲット（ST）と呼ばれる文書に評価対象となるセキュリティ機能が記載されている。PP が存在する場合は、ST の大部分は PP の複写であるが、セキュリティ機能要件の実現方法は製品の実装に依存する。ST の最後には要約仕様という章が設けられており、そこにセキュリティ機能要件の実現方法を記載する。

[2] 正しくは TOE のセキュリティ対策方針という。TOE とは Target of Evaluation、評価対象と言う。

・ドキュメント検査
セキュリティ機能が正しく呼び出すことができるか、適切に設計され実装されているか、インターフェース仕様書や内部設計書を検査する。またセキュリティ機能が迂回されたり無効化されたりしないような保護機能が設計されていることも検査する。

・ソースコードレビュー
仕様や設計が正確かつ完全に実装されているか、保護機能が適切か、ソースコードを検査する。

・脆弱性分析
上記までの過程において、セキュリティ機能が攻撃可能か検討し、弱点となりうる実装を潜在的脆弱性として記録しておく。またセキュリティ機能や保護機能が適切であり、攻撃方法が適用できない場合もその根拠を記録する。

・侵入テスト計画
潜在的脆弱性を攻撃する方法を、弱点を持つソースコード、ソースコードが含まれるソフトウェアを動作させるためのスクリプトやプログラム、弱点を悪用できたときとできないときのソフトウェアの応答、弱点を攻撃するツール等を侵入テスト計画書に記載して具体化する。

・侵入テスト実施
侵入テスト計画に従い、侵入テストを実施する。

・脆弱性評定
侵入テストによって潜在的脆弱性を攻撃した結果を評定する。攻撃が成功した弱点（悪用可能脆弱性）なのか、侵入テストを実施した時点において攻撃は成功しなかったが、将来機器の向上や攻撃手法の発見などにより攻撃が成功する可能性を持つ弱点（残存脆弱性）なのか分類する。

CC を用いた評価では、上記のセキュリティ機能の検査だけではなく、ベンダが開発過程で実施した機能テストをテスト手法の妥当性、テストの深さやカバー範囲の観点からの妥当性検査や、開発・製造環境のセキュリティを ISMS や ISO/IEC 27002 のような手法で検査する過程がある。

(ⅲ) ISO19790/24759 におけるコンポーネント評価の考え方

ISO19790/24759 または［CMVP］・［FIPS］における評価の考え方は単純である。米国政府が暗号モジュール製品を調達する際の基準として作成された経緯からセキュリティ要件（FIPS）に加え試験要件（Derived Test Requirements [DTR] for FIPS PUB 140-2）が規定されている。以下に FIPS の要求事項の概要をまとめる（表 3.2a.1-2）。

表 3.2a.1-2　FIPS 140-2 のセキュリティ要求事項一覧

	セキュリティレベル 1	セキュリティレベル 2	セキュリティレベル 3	セキュリティレベル 4
暗号モジュールの仕様	暗号モジュール、暗号境界、承認されたアルゴリズム、承認された動作モードの仕様。全てのハードウェア、ソフトウェア、ファームウェアのコンポーネントを含む暗号モジュールの記述。暗号モジュールのセキュリティポリシの宣言.			
暗号モジュールのポート及びインターフェース	必須のインターフェース及び選択可能なインターフェース。全てのインターフェースの仕様及び全ての入出力データパスの仕様。		他のデータポートから論理的又は物理的に分離された、保護されていない CSP のためのデータポート。	
役割,サービス,及び認証	必須の役割及びサービスと選択可能な役割及びサービスとの論理的な分離	役割ベースのオペレータ認証又は ID ベースのオペレータ認証	ID ベースのオペレータ認証.	
有限状態モデル	有限状態モデルの仕様。必須の状態及び選択可能な状態。状態遷移図及び状態遷移の仕様。			
物理的セキュリティ	製品レベルの装置。	錠又はタンパ証跡。	カバー及びドアに対するタンパ検出及びタンパ応答。	囲いのタンパ検出及びタンパ応答。EFP 又は EFT。
動作環境	単一のオペレータ。実行可能なコード。承認された完全性技術。	参照 PP に適合し、EAL2 の条件で評価を受けた環境。EAL2 の条件で評価を受け、任意アクセス制御機構及び監査機構をもつ環境。	参照 PP に加え、高信頼パスに適合し、EAL3 に加え、セキュリティポリシのモデル化の条件で評価を受けた環境。	参照 PP に加え､高信頼パスに適合し、EAL4 の条件で評価を受けた環境。
暗号鍵管理	鍵管理機構：乱数生成及び鍵生成、鍵確立、鍵配送、鍵入出力、鍵の保管、並びに鍵のゼロ化。			
	手動の方法を用いて確立された秘密鍵及びプライベート鍵は、平文の形式で入力又は出力してもよい。		手動の方法を用いて確立された秘密鍵及びプライベート鍵は、暗号化又は知識分散処理を用いて、入力又は出力されなければならない。	
EMI/EMC	47 CFR FCC Part 15。Subpart B, Class A(ビジネス向け)。適切な FCC 要件(無線向け)。		47 CFR FCC Part 15。Subpart B, Class B(家庭向け)。	
自己テスト	パワーアップ自己テスト：暗号アルゴリズムテスト、ソフトウェア/ファームウェア完全性テスト、重要機能テスト、条件自己テスト。			
設計保証	構成管理(CM)。セキュアな設置及び生成。設計とポリシとの対応。ガイダンス文書。	構成管理システム。セキュアな配送。機能仕様。	高級言語による実装。	形式的モデル。詳細な説明(非形式的証明)。事前条件と事後条件。
その他の攻撃への対処	攻撃への対処の仕様。現在は、試験可能な要求事項は用意されていない。			

DTR は、図 3.2a.1-1 の通り、FIPS で要求される各セキュリティ要件をアサーション（AS：ASsertion）としてシーケンス番号を付与して一意に識別し、各々に対して暗号モジュールの開発者が準備すべきドキュメントなどを VE（Vender Evidence）として記述している。加えて、暗号モジュールの評価者が試験すべき内容も各々の要件に対比する形で TE（Tester Evidence）として記述されている。

評価者は、DTR に基づき暗号モジュール製品の試験を実施する過程の中で、暗号アルゴリズムが正しく実装されているかどうかも NIST から試験機関に貸与されるツールを用いて確認することが求められている。

調達者にとって、要求するセキュリティ要件と評価者が試験をする要件が一対一で確認でき、試験合格した製品が間違い無く要求通りの暗号モジュール製品であることを確信できるという意味で非常に分かり易い仕組みである。

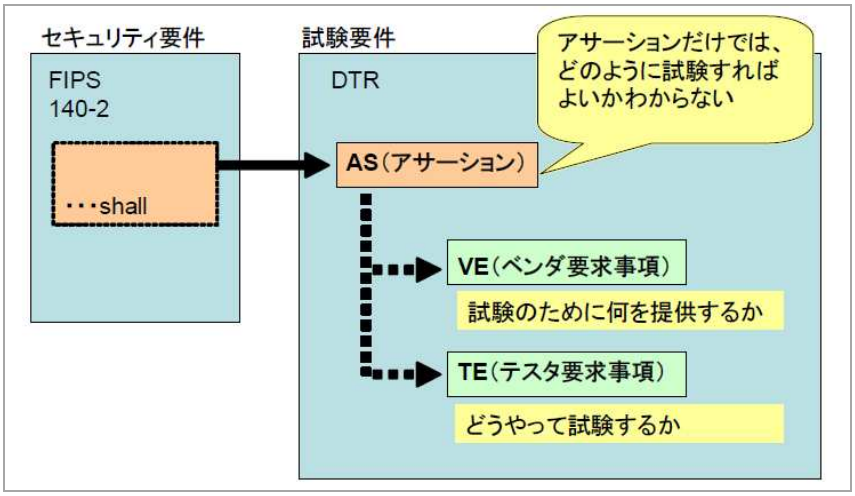


図 3.2a.1-1　セキュリティ要件（FIPS）と試験要件（DTR）との関係

また、CMVP/FIPS では、規格（FIPS・DTR）の統一的な適用・解釈を補うために、実際の試験段階で直面する判断事例・解説等を事例集としてまとめ、定期的に[IG]として発行することで、一つの規格（FIPS・DTR） で、多様な暗号モジュール製品に対応できるようにしている。

(ⅳ) スマートカード分野に求められるセキュリティ機能と評価技術

a. 基本 PP の概要

スマートカード用 IC はほとんどの場合 ISO15408/18045 に則って評価される。従って PP に従いセキュリティ機能が定義されている。この業界の PP のデファクトスタンダードは Security IC Platform Protection Profile with Augmentation Packages Version 1.0（[BSI-PP-0084]）である。本 PP の脅威・セキュリティ対策方針とセキュリティ機能要件の対応関係をまとめる。

b．想定脅威と対策方針

スマートカード用 IC の業界が想定する脅威と、それに対抗する IC の方針は次の通りである（表 3.2a.1-3）。

表 3.2a.1-3　スマートカード用 IC の脅威と対抗の方針

脅威	セキュリティ対策方針
T.Leak-Inherent 攻撃者は、資産の一部である秘密ユーザデータを暴露するために、セキュリティ IC の使用中にリークする情報を利用するかも知れない。	O.Leak-Inherent 評価対象は、セキュリティ IC に保存され、処理される秘密のユーザデータの暴露に対抗する保護を提供しなければならない。 （例えば、電源、クロック、I/O ラインの）波形の測定と分析、信号の増幅によるユーザデータの暴露。 （例えば、電源、クロック、I/O ラインの）信号の測定によって見つかったイベント間隔の測定と分析によるユーザデータの暴露。
T.Phys-Probing 攻撃者は、以下の目的のために評価対象を物理的にプロービングするかも知れない。 (i)　ユーザデータの暴露。 (ii)　組込みソフトウェアの暴露または改ざん。 (iii)　ユーザデータや組込みソフトウェアの暴露や改ざんを可能にする評価対象の動作に関する重要なデータの暴露。	O.Phys-Probing 評価対象は、ユーザデータの暴露に対抗する保護、組込みソフトウェアの暴露／改ざんに対抗する保護、評価対象の動作に関するその他の重要なデータの暴露に対抗する保護を提供しなければならない。これは、下記に対抗する保護を含む： - ボンディングされたパッドを除いたチップ表面への直接的な物理的フロービングの電気的接触を介した（標準的な電圧・電流測定ツールを使った）測定。 - 電気的接触を使わない他のタイプの（固体物理研究や IC 不良解析にツールを使った）電荷間の相互作用の測定。 これらに先立ち、 - 設計と、その属性や機能を理解するためのリバースエンジニアリング。
T.Malfunction 攻撃者は、下記の目的のために、環境ストレスを与えてセキュリティ機能または組込みソフトウェアの誤動作を起こさせるかも知れない。 (i)　評価対象のセキュリティサービスの改変、または (ii)　組込みソフトウェアのセキュリティサービスの改変 (iii)　ユーザデータや組込みソフトウェアの暴露やマニピュレーションを可能にする評価対象のセキュリティメカニズムの停止または悪影響。これは、セキュリティ IC の通常の使用条件外で達成されるかも知れない。	O.Malfunction 評価対象は、正しい動作を保証しなければならない。 評価対象は、信頼性やセキュリティ動作が証明されていない、または、テストされていない通常動作条件外での動作を知らせるか、防がなければならない。これは、誤動作を防止するためである。環境の例としては、電圧、クロック周波数、温度、外部のエネルギー場がある。

脅威	セキュリティ対策方針
T.Phys-Manipulation 攻撃者は、下記の目的のために、セキュリティ IC を物理的に改変するかも知れない。 (i) ユーザデータの改変。 (ii) 組込みソフトウェアの改変。 (iii) 評価対象のセキュリティサービスの改変または停止。 (iv) ユーザデータや組込みソフトウェアの暴露やマニピュレーションを可能にする評価対象のセキュリティメカニズムの改変。	O.Phys-Manipulation 評価対象は、自分自身（ソフトウェアやデータを含む）、組込みソフトウェア、ユーザデータの改ざんに対抗する保護を提供しなければなりません。これは、下記に対抗する保護を含む： - （設計と、その属性や機能を理解する）リバースエンジニアリング。 - ハードウェアと全てのデータの改ざん。 - のみならず、メモリ内容（アプリケーションデータ）の制御された改ざん。
T.Leak-Forced 攻撃者は、資産の一部である秘密ユーザデータを暴露するために、情報リークが固有のものではなく攻撃者に起因するものであっても、セキュリティ IC の使用中に評価対象からリークする情報を利用するかも知れない。	O.Leak-Forced セキュリティ IC は、情報リークが固有のものではなく攻撃者に起因するとしても、セキュリティ IC の中で処理されている秘密データの暴露に対抗する保護を提供しなければならない。 - 強制的な誤動作（“環境ストレスによる誤動作に対する保護（O.Malfunctio）”参照）によるもの。 - 物理的改ざん（“物理的改ざん（O.Phys-Manipulation）”参照）によるもの。 これ以外のケースでは、通常は秘密に関する重要な情報を含まない信号が、リーク攻撃の情報チャネルになる場合がある。
T.RND 攻撃者は、例えば提供される乱数の乱雑さが不足している為に、評価対象セキュリティサービスが生成する乱数を予測したり、見つけたりするかも知れない。	O.RND 評価対象は、乱数生成の暗号品質を保証する。例えば、乱数は、予測不能で十分な乱雑さを持っているべきである。乱数は、例えば暗号鍵の生成に使われるので、評価対象は、生成された乱数についての情報を攻撃者が使えない事を保証する。

c. 求められるセキュリティ機能

b. のように設定されたセキュリティの対策方針から導かれるセキュリティ機能の要件は次の通りである（表 3.2a.1-4）。

表 3.2a.1-4　対策方針と対応する機能の要件

セキュリティ対策方針	セキュリティ機能要件
O.Leak-Inherent	FDP_ITT.1 基本内部転送保護 FPT_ITT.1 基本 TSF 内データ転送保護 FDP_IFC.1 サブセット情報フロー制御
O.Phys-Probing	FDP_SDC.1 保存データの機密性 FPT_PHP.3 物理的攻撃への抵抗
O.Malfunction	FRU_FLT.2 制限付き障害耐性 FPT_FLS.1 セキュアな状態を維持する障害
O.Phys-Manipulation	FDP_SDI.2 保存データの完全性の監視とアクション FPT_PHP.3 物理的攻撃への抵抗
O.Leak-Forced	FDP_ITT.1 基本内部転送保護 FPT_ITT.1 基本 TSF 内データ転送保護 FDP_IFC.1 サブセット情報フロー制御 FRU_FLT.2 制限付き障害耐性 FPT_FLS.1 セキュアな状態を維持する障害 FPT_PHP.3 物理的攻撃への抵抗
O.Abuse-Func	FMT_LIM.1 制限付き能力 FMT_LIM.2 制限付き利用可能性 FDP_ITT.1 基本内部転送保護 FPT_ITT.1 基本 TSF 内データ転送保護 FDP_IFC.1 サブセット情報フロー制御 FRU_FLT.2 制限付き耐障害性 FPT_FLS.1 セキュアな状態を維持する障害 FPT_PHP.3 物理的攻撃への抵抗
O.RND	FDP_ITT.1 基本内部転送保護 FPT_ITT.1 基本 TSF 内データ転送保護 FDP_IFC.1 サブセット情報フロー制御 FRU_FLT.2 制限付き耐障害性 FPT_FLS.1 セキュアな状態を維持する障害 FCS_RNG.1 乱数生成

d. 評価基準・評価方法

スマートカード業界は、現在最も進んでいる評価技術を持つ業界のひとつである。

評価技術は SOG-IS という団体で定期的に議論されており、最新の攻撃技術が非公開文書である Application of Attack Method for Smartcards（以下[AAMS]）にまとめられ、原則 2 年に一度更新されている。[AAMS]から攻撃技術を悪用されないよう具体的方法を消去し、概要だけをまとめた文書が[SC]である。

スマートカードを実装するベンダは、[SC]に例示されている多様な攻撃概要に対して、何らかの対抗策を実装しなければならない。最近では、CHES[3]や FDTC[4]のような攻撃方法を論じる学会やワークショップも多数開催されており、攻撃方法も年々進化している。このような洗練された攻撃方法に対してひとつの対抗策だけでは十分ではなく、さまざまな対抗策が実装されているスマートカードが一般的である。評価機関は、対抗策が攻撃に耐え得る性能を持つかどうか、実際の攻撃を通じて評価し、点数づけをすることによって総合的に合否判定を下す。具体的な評価方法や攻撃方法の概要、攻撃対抗策の評価技術を以降にまとめる。

スマートカードの評価方法は、一般的に[CC]、[CEM]と CC サポート文書に基づく。CC サポート文書には[SC]が含まれており、その他に Application of CC to Integrated Circuits、Security Architecture requirements (ADV_ARC) for smart cards and similar devices、Guidance for smartcard evaluation といったスマートカード関連分野の評価をするために必要な情報が提供されている。

スマートカードは、IC とカード OS と呼ばれる組込みソフトウェアから構成される。カード OS 上にアプリケーション（Java カードではアプレットと呼ばれることもある）を搭載することができるスマートカードもある。スマートカードのセキュリティ機能は、IC によって実現される機能、IC のセキュリティ機能だけでは攻撃に対抗できない場合に、IC を補完するためにカード OS が実装するセキュリティ機能に分けられる。IC ベンダは CC に基づいて IC のセキュリティ機能の評価、認証を依頼し、認証書を CC ポータルサイトや各国の認証機関のホームページに公開する。カードベンダはその認証済みの IC をプラットフォームとしてカード OS を開発する場合が多い。CC に基づく評価では、IC 単体で対抗できない攻撃の対抗策をハードウェアマニュアルに明記することが求められる。IC のセキュリティ機能を正しく利用し、IC が求める対抗策をカード OS 側が正しく対処し、スマートカードとして総合的に十分なセキュリティ機能を実装しているか、という評価観点を提供するのが、CC サポート文書の一つである Composite product evaluation for Smartcards and similar devices である。

[SC]では、次表で示す点数づけされた攻撃能力を持つ攻撃者を定義している。この攻撃者に対抗できるかどうかで脆弱性を評定する（表 3.2a.1-5）。

[3] CHES : Conference on Cryptographic Hardware and Embedded Systems。International Association for Cryptologic Research (IACR)が毎年開催する暗号モジュールへの攻撃や対抗策に関するワークショップ。

[4] FDTC : Fault Diagnosis and Tolerance in Cryptography。おもに暗号モジュールへの故障利用解析を扱うワークショップ。例年 CHES と同じ場所で引き続き開催される。

表 3.2a.1-5　評価対象のレート付け

点数の範囲	次の攻撃能力を持つ攻撃者に対抗する評価対象の抵抗力
0～15	レート：なし。評価対象は基本的な攻撃能力を持つ攻撃者にも対抗できない。
16～20	レート：基本。評価対象は基本的な攻撃能力を持つ攻撃者に対抗できる。
21～24	レート：強化基本。評価対象は基本的な攻撃能力よりやや高い攻撃能力を持つ攻撃者に対抗できる。
25～30	レート：中。評価対象は中程度の攻撃能力を持つ攻撃者に対抗できる。
31 以上	レート：高。評価対象は高い攻撃能力を持つ攻撃者に対抗できる。

攻撃の計算は大きく「識別」と「悪用」に分けて計算する。これは攻撃する方法を開発する過程である「識別フェーズ」と、実際に攻撃対象に攻撃方法を適用する「悪用フェーズ」の二つがあると考えているからである。

攻撃の識別では、使用する機器を選択してセットアップしたり、攻撃に使用するプログラムやスクリプトを開発したり、評価対象を分解して回路を露出させたり、スマートカードを動作させて消費電力を計測したりといった、一連の攻撃方法を開発する。開発攻撃の識別フェーズで評価対象への攻撃を完全に成功させる必要はなく、成功の見込みがたてばよい。

攻撃の悪用は、開発した攻撃方法を評価対象に適用するフェーズである。開発された攻撃手法を適用するだけであるから、開発よりも少ない時間で攻撃できるだろうし、専門知識も必要ないかもしれない。

攻撃方法の開発過程で使用した機器、専門知識、攻撃対象の数量、また開発にかかった時間などの攻撃の要素を重みづけして点数化しており、それを攻撃の計算に使う（表 3.2a.1-6）。

表 3.2a.1-6　攻撃要素の点数

攻撃要素		攻撃の識別	攻撃の悪用
所要時間	１時間未満	0	0
	１日未満	1	3
	１週間未満	2	4
	１カ月未満	3	6
	１カ月を超える	5	8
	非現実的	*	*
専門知識	素人	0	0
	熟練者	2	2
	エキスパート	5	4
	複数のエキスパート	7	6
評価対象の知識	公開	0	0
	制限	2	2
	秘密	4	3
	危機的	6	5
	非常に重要なハードウェア設計	9	該当なし
評価対象へのアクセス	１０サンプル未満	0	0
	３０サンプル未満	1	2
	１００サンプル未満	2	4
	１００サンプルを超える	3	6
	非現実的	*	*
機器	なし	0	0
	標準	1	2
	特殊	3	4
	特別注文	5	6
	複数の特別注文	7	8
オープンサンプル	公開	0	該当なし
	制限	2	該当なし
	秘密	4	該当なし
	危機的	6	該当なし

以下に攻撃の要素それぞれを説明する。

・所要時間

攻撃を開発する所要時間、悪用して成功させるまでの所要時間を定義している。攻撃者と違い、評価者は 3 カ月を越えて成功するまで攻撃をすることはない。所要時間を決定するとき、攻撃の推定時間となる場合もある。

所要時間のなかで、「非現実的」という箇所がある。非現実的かどうかは評価対象によって異なる。所有者がカードの紛失に気付き、速やかに会社に報告すれば、紛失した当日中にでもカードが使用不能になるような場合、たとえ攻撃者が 1 週間で攻撃成功する攻撃方法を開発しても非現実的な所要時間となる。このようなセキュアな利用環境が整っていない場合、おおよその目安は評価対象であるカードのライフサイクルに従う。例えば、クレジットカードは有効期限が切れる 5 年、IC 旅券は有効期限である 10 年といった期間を越えた時間が非現実的な所要時間となる。

・専門知識

攻撃するために必要な専門知識を次のように定義している。

－素人：特に専門知識を持たない。

－熟練者：セキュリティのふるまいや評価対象を熟知している。

－エキスパート：アルゴリズム、プロトコル、ハードウェア構造といった開発者の知識と攻撃を開発するための技術やツールに精通している。攻撃技術は、暗号、電力差分解析（DPA）、故障差分解析（DFA）、電磁波解析（EMA）、リバースエンジニアリング手法、といった専門知識が必要である。また攻撃ツールであるオシロスコープ、研磨装置、走査型電子顕微鏡、レーザー機器、収束イオンビーム装置などを操作する知識が必要である。複数のエキスパートとは、装置に習熟しているエキスパートと暗号学のエキスパートというような異なる分野のエキスパートを想定している。

・評価対象の知識

－公開：公知になっている情報である。

－制限：スマートカード開発の様々なフェーズ中に使用するドキュメントに対応する。例えば、機能仕様書、マニュアル、カード発行者やユーザー用に通常用意される文書がある。

－秘密：上位（システム）設計書及び下位（モジュール）設計書の情報。

－危機的：実装表現（設計及びソースコード)。

－非常に重要なハードウェア設計：開発関係者から得た特別な情報。

・評価対象へのアクセス

攻撃方法を開発する過程において、多数のデバイスを破壊して試行錯誤する必要があったり、スマートカードが攻撃を検知すると自身を動作不能にする保護機能を持っていたりする場合、多数の評価対象が必要になる。「非現実的」は、識別の場合は 2000 サンプル、悪用の場合は 500 サンプルが目安である。

・機器

機器のカテゴリは価格と可用性によって分けられている。可用性とは、公的に入手可能かどうかや、大学や研究機関から借用できるかどうかなども考慮する必要がある。[SC] ではおおよそ以下のようにグループ化されている。

－標準：フラッシュライト、低性能の光学顕微鏡、電圧源、アナログオシロスコープ、チップカードリーダ、PC またはワークステーション、信号解析ソフトウェア、信号生成ソフトウェア。

－特殊：高性能の光学顕微鏡及びカメラ[5]（図 3.2a.1-2)、紫外線顕微鏡及びカメラ、マイクロプローブステーション[6]（図 3.2a.1-3)、レーザー機器[7]（図 3.2a.1-4)、高性能デジ

[5] 写真はオリンパス社の工業用光学顕微鏡「BX53M」
http://www.olympus-ims.com/ja/microscope/bx53m/

[6] 写真は Cascade Microtech 社の解析用マニュアル・プローバ「MPS150」
https://www.cascademicrotech.com/jp/products/probe-systems/150mm-wafer/150mm-wafer

[7] 写真は Riscure 社のダイオードレーザーステーション「Inspector FI」
https://www.riscure.com/security-tools/inspector-fi/

タルオシロスコープ[8]（図 3.2a.1-5）、信号アナライザ、ケミカルエッチング、プラズマエッチング、研削用ツール。

図 3.2a.1-2　工業用光学顕微鏡

図 3.2a.1-3　マイクロプローブステーション

図 3.2a.1-4　レーザー機器

図 3.2a.1-5　デジタルオシロスコープと DPA ワークステーション

－特殊機器：走査型電子顕微鏡[9]（SEM、Scanning Electron Microscope）（図 3.2a.1-6）、電子ビームテスタ、原子間力顕微鏡（AFM、Atomic Force Microscope）、集束イオンビーム[10]（FIB、Focused Ion Beam）（図 3.2a.1-7）、新技術による設計検証及び故障解析ツール。

[8] 写真は Rambus 社の消費電力解析装置「DPA Workstation」
http://www.rambus.com/security/dpa-countermeasures/dpa-workstation-platform/

[9] 写真は日立ハイテクノロジーズ社の SEM「S-3700N」
http://www.hitachi-hightech.com/jp/product_detail/?pn=em-s3700n

[10] 写真は日本電子社の収束イオンビーム加工観察装置「JIB-4000」
http://www.jeol.co.jp/products/detail/JIB-4000.html

図 3.2a.1-6　SEM

図 3.2a.1-7　FIB

・オープンサンプル

オープンサンプルとは、IC のマニュアルでソフトウェアが実装するよう指示されているセキュリティ機能を持たないソフトウェアや、IC のセキュリティ機能を無効化できる設定ができるソフトウェアを、評価者が自由にインストールできるようなサンプルを言う。このようなソフトウェアを用いて攻撃方法が正しいかどうかを確かめながら開発できる。あるいは、暗号鍵や暗証番号を知っているサンプルも含まれる。このサンプルを用いて電力差分解析や故障差分解析の攻撃場所やタイミングが正しいか確かめることができる。

ただし、オープンサンプルの目的はカード OS の攻撃手法の開発であり、IC の評価を繰り返すことではない。またオープンサンプルを用いた場合の所要時間の見積もりは、オープンサンプルを利用しない場合の見積もりをした後に、利用したオープンサンプルに対応する点数を加算する。

オープンサンプルは次のように分類する。

－公開：サンプルが保護されておらず、管理なしで配付されている（NDA なし、顧客の確認なし）。または、その IC がセキュリティの推奨事項を実装している保証がないアプリケーションや、ネイティブコードによって自由にプログラムできるバージョンで使用されている。あるいは容易に推定できる秘密しかないサンプルを言う

－制限：カードの仕様や IC のデータシートと同等の典型的な保護がされている。あるいは、例えば、ウェブサイト経由の匿名アクセスでは利用できることはないような、情報を取得するためにアクションが必要になる。

－秘密：設計書と同等の保護がされている。あるいは限られた数の人々またはデバイスでしか共有されず、強力なアクセス制御がある秘密データが含まれたもの。秘密データの取り扱いは、データを保護するため書面での手順によって管理し、秘密データを特定する明確な方法がある。

－危機的：ソースコード、VHDL、レイアウトと同等の保護がなされている。オープンサンプルをほとんど作成させないこと、配付を厳重に管理すること、受領側の組織が同じレベルの管理をセットアップできることが保証される必要がある。あるいは、サンプル内で生成されてそのサンプルのみに所有される秘密データを持つサンプルである。したがって秘密データは、通常の条件下においてカード外で利用可能ではない。例えば、秘密データにアクセスする特定のコマンドを評価者に提供するような例外的

な条件下でのみ、これらの秘密データが既知になる可能性がある。

e. 脆弱性評価（攻撃能力算出と攻撃耐性評価）に必要とされる評価技術

脆弱性評価とは、攻撃が成功するか、あるいは成功する見込みがあるかを、攻撃方法を評価対象に実際に適用することである。以下に攻撃概要、使用機器、攻撃方法をまとめる。

・物理攻撃

スマートカードへの物理攻撃は、スマートカードから IC を取り出し、IC に化学的・物理的な加工を施して配線層やシリコン層を露出させた上で物理的攻撃を実施するものである。後述するテスト機能の悪用やかく乱攻撃の準備のために物理攻撃する場合もある。

・センサやフィルタの制圧

IC は、おかれる環境や供給電源を監視し、異常な動作を起こさせないよう、光センサ、温度センサ、電圧センサ、周波数フィルタといった保護機能を実装している。この攻撃は、IC の異常動作を起こすことができるよう、これらの保護機能を無効化する。

・かく乱攻撃

評価対象の動作中に悪用可能な誤動作を起こさせる攻撃である。IC の動作仕様範囲外の温度に置いたり、仕様範囲外のスパイク状の電圧や周波数を入力したりする方法がある。最近ではレーザー光を対物レンズで絞って照射する方法や、高いエネルギーの電磁波を印加する方法がポピュラーである。

かく乱攻撃は IC 単体に適用してかく乱攻撃への耐性を評価する場合と、カード OS が実装する対抗策を評価する場合がある。前者のケースでは、メモリ周辺回路にレーザーを照射したり、メモリ読み出し／書き込みタイミングで周波数グリッチを印加したりしてデータを改ざんする攻撃がある。また CPU やコプロセッサにレーザーを照射し、プログラムカウンタの改ざん、フラグの反転、レジスタ値の改ざんを図る。

メモリ周辺回路に対する攻撃によって、メモリに格納されている値は変わらないが途中の回路でデータ改ざんされ CPU やコプロセッサへの入力値が変わる。また CPU のプログラムカウンタやコプロセッサの内部レジスタが改ざんされる。このような IC 単体に対する攻撃がある。

攻撃によってデータが改ざん可能なら、カード OS がデータ改ざんに対処するよう、IC のマニュアルに指示が記載される。カードベンダは、メモリに書き込んだデータを読み出して書き込みデータと突合し、書き込みデータの完全性を検証したり、2 回読み出ししたりして読み出しデータの改ざん検知を行う対抗策や、条件判定文を 2 重化するような対策をカード OS に実装する。この対抗策が有効かどうかを評価するケースがある。

・DFA（Differential Fault Analysis, 差分故障解析）による鍵の取得

DFA とは、誤りなしの計算結果と誤りがある計算結果を比較することにより、秘密情報の取得を試みる攻撃である。この攻撃を用いて RSA の秘密鍵や AES の鍵を取得できる

方法[11]が知られている。この攻撃は電源への周波数グリッチを印加するような非侵襲的な方法でも、IC を研磨して暗号演算回路にレーザー光線を照射するような侵襲的な方法でも実施することができる。

・サイドチャネル攻撃

この攻撃はアルゴリズム実装の意図的ではないチャネルを通じて漏えいした秘密情報を標的にする。意図的ではないチャネルは、処理時間、消費電力、放射電磁波などの物理的現象を対象とする。処理時間を測定して比較する攻撃はタイミング攻撃と呼ばれる。消費電力を測定して秘密情報を取得しようとする攻撃は PA（Power Analysis）と呼び、数個から数百個の測定電力波形を用いて解析する攻撃を単純電力解析（Simple Power Analysis、SPA）、数千から数百万の波形を用いて統計処理をして差分をとり、所望の秘密を分析する攻撃を差分電力解析（Differential Power Analysis、DPA）と呼ぶ。放射電磁波を測定する攻撃は電磁波解析（Electro-Magnetic Analysis、EMA）と呼ばれ、これも利用する解析方法により単純電磁波解析（Simple EMA、SEMA）と差分電磁波解析（Differential EMA、DEMA）と呼ばれる。

・テスト機能の悪用

この攻撃は IC や IC カードのテストモードを悪用するものである。例えばテストモードに遷移すると不揮発メモリ内容の読み出しが無制限にできたり、センサ機能を無効化することができたりすることがある。テストモードに遷移できないようにする認証機能をかく乱機能でバイパスしたり、テスト回路のヒューズ配線を収束イオンビーム装置で再接続したりするような攻撃がある。

・乱数生成器への攻撃

この攻撃は乱数生成器を侵襲的な方法で物理的に破壊したり、非侵襲的な方法でかく乱したりして、出力を固定化したりエントロピーを低下させたりする攻撃である。乱数生成器の乱数性に依存するセキュリティ機能、例えば鍵生成機能などが信頼できなくなる。

・ソフトウェア攻撃

この攻撃はソフトウェアの脆弱性を悪用した攻撃である。中間者攻撃、リプレイ攻撃、オーバーフロー攻撃がよく知られている。

・不正な形式の Java アプリケーション

不正な形式の Java Card アプリケーションは、不正なバイトコード命令シーケンスで構成されていたり、バイトコードのパラメータを不正に書き変えていたりするものである。例えばバイト配列を読み出す命令を、ワード配列を読み出す命令に書き換えた不正アプリケーションを作成して Java Card にインストールし、メモリをダンプする攻撃がある。

---

[11] D. Boneh, R. A. DeMillo, R. J. Lipton, "A New Breed of Crypto Attack on "Tamperproof" Tokens Cracks Even the Strongest RSA Code", 25 Sep 1996.
P. Dusart, G. Letourneux, O. Vivolo, "Differential Fault Analysis on A.E.S.", 01/10/2002

スマートカードから見て、アプリケーションは悪意を持って作成されている可能性があるため、カード OS の動作がアプリケーションから干渉されないようなセキュリティ機能を持つことをカード OS に求められる。

・アプリケーション分離

マルチアプリケーションプラットフォームと呼ばれる、複数のアプリケーションをカード OS 上に搭載できるスマートカードが持つ、アプリケーション分離機能への攻撃である。攻撃対象は、隣接するアプリケーションやカード OS が保持する機密データ、アプリケーションとカード OS そのものとなる。上記「不正な形式の Java アプリケーション」で述べたように、攻撃者が不正な形式の Java カードアプリケーションを作成してそれを搭載しようとする。カード管理者が Java カードアプリケーションをオフカード検証器で検証したあとに搭載するか、スマートカードが検証器を実装（オンカード検証器）し、アプリケーション搭載時に検証する方法がある。後者をすり抜けるよう、トランザクション機能を攻撃する方法がある。

Java カード OS がバイトコードを実行するまえにオペランドをチェックする防御的仮想マシンを実装しているが、この防御的仮想マシンのチェック機能の抜けを見つけ出し悪用する攻撃がある。

f. 自動車業界のコンポーネント評価への適用性

自動車業界のコンポーネントにおいて、コンポーネントが具備すべきセキュリティ機能を導出する手法の一つとして、脅威の設定から対策する方針の決定、方針を満足するために必要で十分な機能要件の定義という流れは応用することができる。機能要件そのものは、ISO15408 から選択することも可能であるし、あるいは業界で必要な機能要件を決定してもよい。

機能要件を定義し、PP 通りに機能要件をセキュリティ機能として実装したなら、その実装が適切か検査しなければならない。ISO15408 のように設計書からソースコードまで検査してから機能テストによる実証を行うこともできる。

ISO15408 の主な特徴の一つとして、定義されたセキュリティ機能が迂回されたり、無効化されたり、あるいは初期化の途中で停止させられて、セキュリティ機能が動作していない状態にさせられたり、といったことがないようにセキュリティアーキテクチャ設計が必要である。このセキュリティアーキテクチャ設計は、有る意味当たり前の機能として機能要件に定義されない。機能要件の不具合はバグとして扱われるのに対し、セキュリティアーキテクチャ設計の弱点が脆弱性である。その脆弱性を攻撃することでセキュリティ機能を迂回したり無効化したりできないかテストで実証することが侵入テストである。機能テストとは異なり、テストする方法やツールは、悪用しようとする脆弱性に合わせて試行錯誤して適切なものを選択しなければならない。そのガイドラインを定めるために業界の知識人が定期的に議論している。

一方、米国においてセキュリティ製品の調達には、NIAP が承認した Standard PP（SPP）に基づく必要がある。NIAP が承認した SPP には、上記のセキュリティアーキテクチャ設

計に対応した機能要件を定義しているものがある。たとえば、スタックやヒープのオーバーフロー攻撃に対抗するためにアドレス空間をランダム化する機能要件を設定している。この機能要件は、NIAP が主導して設立したテクニカルコミュニティが設定に携わる。

セキュリティアーキテクチャに相当する機能を機能要件にするか、あるいは脆弱性として攻撃手法を決定するか、いずれにせよ、業界の知識が結集されているのは同じである。

最近の ISO15408 の認証の相互承認は、この SPP を Collaborative PP（cPP）として捉えて CCRA 加盟国で共有しようとする動きが始まっている。SPP と同じように CC ユーザーズフォーラムの中でテクニカルコミュニティを設立し、そこに参加している各社の知識人が PP の作成に携わる。特徴的なのは、サポート文書を別に作成し、機能要件ごとに必要なテストをサポート文書の方へ定義していることである。例えば通信プロトコルを規定した要件は PP の方に記載して通信プロトコルの追加や変更に PP が対処し、テスト方法の変更や更改はサポート文書の方が対処するように、技術の進歩に伴い柔軟な対応を取ることができる。

(ｖ) セキュリティボックス付きハードウェア分野に求められるセキュリティ機能と評価技術

a. 基本 PP の概要

暗号化 USB メモリ、暗号化ハードディスク、ハードウェアセキュリティモジュール（HSM）、ルータ、金融端末、デジタルタコグラフ、タクシーメータといった機器を想定している。これらの機器は、情報資産を物理的攻撃から保護するための特別な筐体を内部に持つものがある。この特別な筐体をセキュリティボックスと呼んでいる。

セキュリティボックスはハードウェアとソフトウェアの物理保護対抗策から構成され、セキュリティ機能として、例えばセンサが攻撃を検知したときのセキュアなデータ消去、警報がある。またコンポーネントの緊急破壊といった電気的な改ざんに対抗するメカニズムと連動した金属シールドや、メッシュ状の配線、エポキシ樹脂による化学保護がある。

このような物理的な攻撃に対する手段を評価するため、JIL（Joint Interpretation Library）では[SB]を制定して公開した。

自動車業界に関連する PP の一つにドイツの認証機関である BSI が発行したデジタルタコグラフユニットの PP－Digital Tachograph – Vehicle Unit (VU PP) Version 1.0（[BSI-CC-PP-0057]）がある。デジタルタコグラフは、機密データを保存するタコグラフカードとセットになって用いられる。

ここでは、スマートカードとデジタルタコグラフユニットとの大きな違いをまとめる。

b. 想定脅威と対策方針

デジタルタコグラフにおいて、想定する脅威と、それに対抗する方針の特徴的なものは次の通りである（表 3.2a.1-7）。

表 3.2a.1-7　デジタルタコグラフの脅威と対抗の方針

脅威	セキュリティ対策方針
T.Card_Data_Exchange デジタルタコグラフユニットとタコグラフカードの間で交換されるユーザデータを改ざんする。	O.Audit：不正試行を監査し、その行為を利用者まで追跡する。 O.Processing：入力から出力まで正しく処理する。 O.Reliability：信頼できるサービスを提供する。 O.Secured_Data_Exchange: タコグラフカードとセキュアなデータ交換をする。
T.Access アクセス権のない利用者が、許可されていない機能に不正アクセスをする。	O.Access：機能やデータへのアクセスをコントロールする。 O.Audit：不正試行を監査しその行為を利用者まで追跡する。 O.Authentication：利用者と接続機器を認証する。
T.Fake_Devicelock 偽のデバイスを接続しようとするかもしれない。	O.Access：機能やデータへのアクセスをコントロールする。 O.Audit：不正試行を監査し、その行為を利用者まで追跡する。 O.Authentication: 利用者と接続機器を認証する。O.Processing：入力から出力まで正しく処理する。 O.Reliability：信頼できるサービスを提供する。 O.Secured_Data_Exchange: タコグラフカードとセキュアなデータ交換をする。
T.Software 組込みソフトウェアを改ざんするかもしれない。	O.Audit：不正試行を監査し、その行為を利用者まで追跡する。 O.Output：格納データを正しく出力データに反映する。 O.Reliability：不正試行を監査し、その行為を利用者まで追跡する。 O.Secured_Data_Exchange: タコグラフカードとセキュアなデータ交換をする。

上記の攻撃のエンティティは人間の攻撃者を想定しているが、T.Fake_Devicelockは偽の機器が接続されることを想定している。この脅威には認証、アクセス制御、セキュアなデータ交換、動作信頼性、監査の方針が設定されている。

c. 求められるセキュリティ機能

b.のように設定されたセキュリティの対策方針から導かれるセキュリティ機能の要件は次の通りにまとめられる（表 3.2a.1-8）。

表 3.2a.1-8　デジタルタコグラフの対策方針と対応する機能の要件

セキュリティ対策方針	セキュリティ機能要件
O.Audit	FAU_GEN.1、FAU_SAR.1、FAU_STG.1、FAU_STG.4：監査データ生成、監査ログ読み出し者限定、監査データの不正削除防止、監査データ満杯のときのアクション FDP_SDI.2：保存データの完全性の保護 FIA_UID.2、FIA_ATD.1、FIA_AFL.1：アクション前の利用者識別、認証が失敗したときのアクション FPT_FLS.1 でフェールセキュア、つまりかく乱などからの保護 FPT_STM.1：正確なクロックを提供 FPT_TST.1：セルフテストを実行
O.Processing	FDP_ACC.1、FDP_ACF.1：アクセス制御

セキュリティ対策方針	セキュリティ機能要件
	FDP_ITC.1、FDP_ITC.2：インポートするデータの制御 FDP_RIP.1：消去データにアクセスできないようにする FMT_MSA.3：静的なセキュリティ属性の初期化 FPR_UNO.1：サイドチャネル攻撃からの保護 FPT_PHP.3：物理攻撃からの保護 FPT_STM.1：正確なクロックを提供 FPT_TDC.1：機能ブロック間でのデータが改ざんされない
O.Reliability	FDP_ACC.1、FDP_ACF.1：アクセス制御 FDP_ITC.1、FDP_ITC.2：インポートするデータの制御 FDP_RIP.1：消去データにアクセスできないようにする FDP_SDI.2：保存データの完全性の保護 FIA_AFL.1：認証が失敗したときのアクション FMT_MSA.3、FMT_MOF.1：静的なセキュリティ属性の初期化、セキュリティ機能の管理 FPR_UNO.1：サイドチャネル攻撃からの保護 FPT_FLS.1 でフェールセキュア、つまりかく乱などからの保護 FPT_PHP.2、FPT_PHP.3：物理攻撃を受けたときの通報と物理攻撃からの保護 FPT_TDC.1：機能ブロック間でのデータが改ざんされない FPT_TST.1：セルフテストを実行 FRU_PRS.1：優先度低のプロセスに干渉されず、機能やセキュリティに関するデータを必要なときに必ず使える
O.Secured_ Data_ Exchange	FCO_NRO.1：発信の証明・否認防止 FCS_CKM.1、FCS_COP.1：鍵生成と暗号 FDP_ACC.1、FDP_ACF.1：アクセス制御 FDP_ETC.2：エキスポートするデータの制御 FDP_ITC.2：インポートするデータの制御 FIA_UID.1、FIA_UAU.2、FIA_UAU.5、FIA_UAU.6：アクション前の利用者識別と認証、再認証、複数の認証メカニズム FMT_MSA.3、FMT_SMF.1、FMT_SMR.1：セキュリティの管理
O.Access	FDP_ACC.1、FDP_ACF.1：アクセス制御 FDP_RIP.1：消去データにアクセスできないようにする FIA_UID.2、FIA_UAU.5：アクション前の利用者識別と複数の認証メカニズム FMT_MSA.1、FMT_MSA.3、FMT_MOF.1、FMT_SMF.1、FMT_SMR.1：セキュリティの管理
O.Authentication	FIA_UID.2、FIA_UAU.2、FIA_UAU.3、FIA_UAU.5、FIA_UAU.6：アクション前の利用者識別と認証、偽造されない認証、再認証、複数の認証メカニズム
O.Output	FCO_NRO.1：発信の証明・否認防止 FDP_ETC.2：エキスポートするデータの制御 FDP_SDI.2：保存データの完全性の保護 FPR_UNO.1：サイドチャネル攻撃からの保護 FPT_PHP.3：物理攻撃からの保護

d. 評価基準・評価方法

デジタルタコグラフは、高い攻撃能力を持つ攻撃に対抗できることが求められている。攻撃能力は、スマートカード分野と同じように次のようにまとめることができる。

セキュリティボックスの場合も、“識別”（攻撃の定義）のコストと、“悪用”（例えば一度スクリプトが公表された）のコストを区別している。従って、セキュリティボックスの攻撃力を計算する時には、攻撃パスを理解し文書化する識別と、完全な攻撃を構築する悪用の 2 つの段階の点数を加算し、最終的な攻撃力の合計を計算する。

スマートカード IC 分野と異なる攻撃の要素を説明する。

－機会：攻撃機会は重要な要素であり、所要時間に大きく影響を与える。

－制限なし：攻撃が検知されるリスクが何もなく無制限に攻撃ができる。

－容易：一時間以内に評価対象にアクセスができる。

－中間：一日以内に評価対象にアクセスできる。

－困難：評価対象にアクセスするのに一週間以上かかる。

－機会なし：攻撃実施するだけの攻撃機会がない。例えば、評価対象に到達するまでに 2 週間かかる攻撃方法にもかかわらず、1 週間ごとに鍵が交換されるケースなど。

e. 脆弱性評価（攻撃能力算出と攻撃耐性評価）に必要とされる評価技術

以下に攻撃概要、使用機器、攻撃方法をまとめる。

・物理的侵襲攻撃

手動で分解する：内部の設計情報や機密データを解析するために、改ざん検知シールの剥離、耐タンパねじのバイパス、接着されたカバーの取り外し、分解といった攻撃で筐体のセキュリティ機能をバイパスする。

これらの攻撃は以下のような方法に分類する。

－機械加工

－ウォータージェット加工

－レーザー機械加工

－サンドブラスト加工

CNC 工作機械、ウォータージェット加工機、レーザ加工機、サンドブラスタを用いて溶接部を剥がしたり、エポキシを剥がしたりする。

・センサの無効化

－改ざん検知センサネットワークへの攻撃

バスモニタなどを用いてセンサ出力を監視し、センサの出力を改ざんする。JTAG 経由でレジスタ値を改ざんし、センサのふるまいを変える。

－エポキシ樹脂の剥離

－改ざん検知メッシュの剥離

配線をショートするように加工して改ざん検知を無効化しドリルで穴開け加工する。

－耐タンパ処理装置への直接攻撃

メモリ回路にスパイク電流を印加して書込みデータや読出しデータをゼロ化する。または絞った高エネルギのビームを照射して処理動作を止めたり、改ざんしたりする。

所望の回路を識別するため、X 線断層撮影などが必要になる。

－付属電源への攻撃

耐タンパ処理装置が付属の電源で駆動している（メイン装置と耐タンパ装置の電源を分けている）なら、その電源を破壊する。

・物理的準侵襲攻撃

－かく乱攻撃

動作仕様範囲外の高い温度や低い温度に置き、RAM からデータを暴露する。あるいは電源にスパイク状の高電圧を印加し装置の挙動を観察する。

・物理的非侵襲攻撃

－リバースエンジニアリング

リバースエンジニアリング対抗策を次のような方法でバイパスして設計情報や機密データを暴露する。目視で観察する、X 線で透視する、断層撮影する、サーモグラフィーで動作中の IC を見つける。

－消費電力分析

暗号処理などを実行している時の消費電力を測定、収集、解析することで鍵を暴露する。

－電磁波測定

IC にアンテナを近接させて放射電磁波を測定収集し、解析することで鍵を暴露する。

－タイミング解析

入力を変化させた暗号アルゴリズム実行時間を収集してふるまいを解析したり、鍵や暗証番号を推測したりする。

f. 自動車業界のコンポーネント評価への適用性

デジタルタコグラフの PP は、複数の機能コンポーネントから構成されるプリント基板とそれを保護する筐体から構成されており、スマートカードや IC よりも自動車業界のコンポーネントに近い構成である。この PP では、スマートカード用 IC の PP に比べ、より多く機能要件を選択し、セキュリティ機能を提供している。PP 作者は、サイドチャネル攻撃への対抗機能や物理攻撃への対抗機能を要件化することでデジタルタコグラフにこれら機能を実装するよう要求している。この要件も ISO15408 の機能要件を用いて定義している。セキュリティボックス付きハードウェアの攻撃方法は主に物理的攻撃に焦点を当てている。[SC]では耐タンパ機能を無効化あるいは迂回する手法の対象が IC の内部の配線層やその下のポリシリコン層であったが、[SB]では、プリント基板や IC を保護するメッシュ配線や樹脂になっている。それに伴い攻撃方法やツールも異なる。このように攻撃するコンポーネントの構成によって手法やツールを考慮する必要があることがわかる。

(vi) 決済端末分野に求められるセキュリティ機能と評価技術

a. 基本 PP の概要

この決済端末の PP は、Point of interaction protection profile Version 4 であり、大きく分けて 3 つの構成がある。ひとつは Pin Entry Device（PED） Only、もうひとつは PED-COMPREHENSIVE、最後に PED-CHIP-ONLY がある。PED-ONLY、PED-CHIP-ONLY は PED-COMPREHENSIVE のサブセットなのでここでは PED-COMPREHENSIVE（以下 PED-COMP）を取り上げる。

PED-COMP には、PIN などを格納している高いセキュリティを必要とするモジュールと、暗号化された PIN を扱う中程度のセキュリティを必要とするモジュール、磁気ストライプカードデータを扱う低いセキュリティを必要とするモジュールが含まれている。従ってセキュリティレベルによって想定する脅威や対策が異なり、また評価手法も異なってくる。

ここでは、スマートカードと決済端末のとの大きな違いをまとめる。

b. 想定脅威と対策方針

金融端末では、利用者の暗証番号と購買情報をいかに守るかが焦点であり、脅威もそのデータの暴露に関するものになっている。その対象は金融端末の機能コンポーネント間で交換されるデータ、金融端末と情報処理センター間のトランザクションデータ、あるいは機能コンポーネントに搭載されているデバイスと多様である。

以下に特徴的な脅威と対策方針をまとめる（表 3.2a.1-9）。

表 3.2a.1-9　金融端末の脅威と対抗の方針

脅威	セキュリティ対策方針
T.CardholderUsurpEPIN PIN 入力値あるいは処理中の PIN を暴露する	O.PINEntry：入力中の PIN の機密性を保護する O.EncPIN：PIN を暗号化している間、耐タンパの機能で保護する O.CoreSWHW：コアソフトウェアとハードウェアの正しい実行と真正性、完全性を保証する
T.Transaction 決済トランザクションへの攻撃	O.PaymentTransaction：決済データと決済端末の真正性と完全性を保証する O.POI_SW：決済端末の管理とトランザクションデータを処理する決済ソフトウェアの正しい実行を保証する O.POIApplicationSeparation：決済アプリケーションと他のアプリケーションを分離する
T.IllegalCodeInstall ダウンロードした決済アプリケーションを改ざんして攻撃	O.PaymentApplicationDownload：決済ソフトウェアのダウンロードやアップデート中の真正性と完全性を保証する O.POI_SW：決済端末の管理とトランザクションデータを処理する決済ソフトウェアの正しい実行を保証する

c. 求められるセキュリティ機能

b. のように設定された特徴的なセキュリティの対策方針から導かれるセキュリティ機能の要件はおおよそ次の通りにまとめられる（表 3.2a.1-10）。

表 3.2a.1-10　決済端末の対策方針と対応する機能の要件

セキュリティ対策方針	セキュリティ機能要件
O.PINEntry	FDP_IFC.1、FDP_ITC.1：情報フロー制御とデータインポート FIA_UID.1、FIA_UAU.2：利用者の識別と認証 FPT_EMSEC.1：サイドチャネル防止 FTA_SSL.3：特定時間後のセッション終了 FPT_PHP.3：物理攻撃からの保護
O.EncPIN	FIA_UID.1、FIA_UAU.2：利用者の識別と認証 FDP_IFC.1、FDP_ITF.1：情報フロー制御 FDP_RIP.1：消去データにアクセスできないようにする FDP_ITT.1：内部転送データの保護 FTP_TRP.1：高信頼パス FCS_RND.1、FCS_COP.1：暗号要件 FDP_ITC.1：データインポート FTP_ITC.1：機能間高信頼チャネル FPT_TDC.1：機能ブロック間でのデータが改ざんされない FPT_EMSEC.1：サイドチャネル防止 FPT_PHP.3：物理攻撃からの保護
O.Core SWHW	FIA_UID.1、FIA_UAU.2：利用者の識別と認証 FPT_TST.1：セルフテストを実行 FPT_FLS.1 でフェールセキュア、つまりかく乱などからの保護 FDP_ACC.1：アクセス制御 FDP_ITC.1：インポートするデータの制御 FPT_PHP.3：物理攻撃からの保護
O.Payment Transaction	FDP_ACC.1、FDP_ACF.1：アクセス制御 FDP_ITT.1：内部転送データの保護 FDP_UIT.1：機能間の利用者データ完全性転送保護 FDP_UCT.1：機能間の利用者データ機密転送保護 FDP_RIP.1：消去データにアクセスできないようにする FTP_ITC.1：機能間高信頼チャネル FPT_PHP.3：物理攻撃からの保護 FPT_EMSEC.1：サイドチャネル防止
O.POI_SW	FDP_ACC.1：アクセス制御 FDP_ITC.1：インポートするデータの制御 FPT_FLS.1 でフェールセキュア、つまりかく乱などからの保護
O.POI Application Separation	FDP_ACC.1、FDP_ACF.1：アクセス制御 FDP_RIP.1：消去データにアクセスできないようにする
O.Payment Application Download	FDP_ACC.1：アクセス制御 FDP_ITC.1：インポートするデータの制御

d. 評価基準・評価方法

決済の端末の評価技術文書である[POI]は[SB]と同様な内容であるが、[POI]に特徴的な内容がいくつかある。

一つは部分的な攻撃成功と完全な攻撃成功を分け、それぞれの計算方法を定義している。完全な攻撃成功とは、キーボード入力音から暗証番号を割り出すような、完全に資産を暴露できる攻撃である。部分的な攻撃成功とは、例えば耐タンパセンサの取り外しの攻撃と、内部スイッチの無効化の二つが成功して完全に攻撃成功する場合をいう。この場合は二つの攻撃にかかるコストをそれぞれ計算し、最後に合算して攻撃コストにする。

次に攻撃要素のひとつが異なる。[SC]では、オープンサンプルという攻撃方法を試行錯誤するためのサンプルが攻撃要素に含まれていたが、[POI]ではその代わりに「部品」という要素になっている。部品とは、攻撃の兆候を隠したり、攻撃の結果壊れた部分の代わりにしたり、ディスプレイやプリンタのようなデータのモニタをしたり、直接的に攻撃に必要だったりするものである。部品は以下のように分けられている。

・標準：容易に購入できるものや、同じようなデバイスから再利用できるもの。
・特殊：大きな労力なしで入手できるもの。店で購入できるが、納品まで長い時間がかかるものや、ある単位のロットでしか購入できないもの。
・特別注文：簡単に購入できず特別に製造するもの。特別注文のスペアパーツを使った攻撃はほとんどない。

e. 脆弱性評価（攻撃能力算出と攻撃耐性評価）に必要とされる評価技術

決済端末業界で想定している攻撃の概要を次にまとめる。

・最小限の侵襲あるいは非侵襲の物理的攻撃

次にあげる攻撃は、PIN そのものやキーパッド入力を暴露するため、タンパ応答メカニズムをバイパスしようとする。

－フレキシブル基板を用いた小さな PIN 盗聴器。スマートカードの端子に接触するようカードリーダーのスロットに装着し PIN を盗聴する。
－カードリーダーの IO ラインに配線して PIN を盗聴する。
－キーパッドのうち使っていないキーに仕掛けをしてキーマトリックスを盗聴する。
－PIN 入力パッドへの電源供給を監視し、キー入力を盗聴する。

・センサ、スイッチ、フィルタの制圧

センサやフィルタは POI の動作環境（電圧、周波数、温度）を監視し、スイッチは改ざんを検知するメカニズムである。これらを無効化、あるいは回避するため、接続を切断したり、ふるまいを改変したり、環境条件の隙間を見つけたりする。タンパ検知スイッチは、ケースやキーパッドのような機械的なスイッチや、コネクタのような取り外しを検知する論理的スイッチがある。

これらの攻撃により、メモリやレジスタの値が改ざんされる、プログラムフローがスキップされる、動作モードやパラメータが変わり管理者モードや特権が使えるようになる、コールドブート攻撃のように RAM からデータを吸い出す、といったことができる。

・物理的攻撃
シールド線で覆われているプリント基板や、樹脂の中に埋め込まれているデバイスを露出させる攻撃である。あるいはプリント基板の BGA のコンタクトを露出させるような加工を施す。物理的攻撃を用いてキーパッドの回路をモニタしたり LSI を露出させメモリ回路に直接アクセスしたりする。

・かく乱攻撃
グリッチのようなかく乱を入力して、POI の振る舞いを変えて悪用可能な動作エラーを引き起こす。一般的には異常な温度、電圧、周波数を印加する。暗号動作の故障注入攻撃や認証ステータスの改ざんを意図してこの攻撃を使う場合もある。
この攻撃により、命令をスキップする、セルフテストを成功状態にする、演算エラーを引き起こす、弱い乱数になる、と言ったふるまいに変更できる。

・フロントサイド攻撃
暗証番号入力装置を直接物理攻撃し、カード所有者に気づかれないよう、キー入力を監視して暗証番号を盗聴する攻撃である。

・EMA や音響攻撃
POI 動作中に放射される電磁波を計測して暗号鍵や PIN を復元する攻撃である。音響攻撃は、キーパッドが押される時の音を解析して入力 PIN を復元する攻撃である。

・乱数生成器への攻撃
乱数生成器への攻撃により、乱数の種のエントロピーを低下させ、予測しやすい乱数にしたり、あるいは乱数値を固定にしたりする。この結果、生成される鍵が固定値であったり、予測可能になったりする。

・ソフトウェア攻撃
ソフトウェアのバグや、プロトコル仕様の脆弱性を見つけ出し、悪用する攻撃である。そのためにコマンドを編集して異常なパラメータを入力したり、プロトコルシーケンスを変えてふるまいを観察したり、バッファオーバーフローを引き起こすような値を入力したりする。その他に中間者攻撃やリプレイ攻撃がポピュラーである。

・PIN や暗号鍵に関するプロトコル攻撃
POI に PIN を入力して処理したり、PIN から生成される暗号鍵をインポートしたり POI 外へエキスポートしたりするプロトコルがあるため、通信経路上の暗号化 PIN から PIN を復号するような攻撃である。

f. 自動車業界のコンポーネント評価への適用性

金融端末の PP は、複数の機能コンポーネントから構成される端末を分割し、それぞれの機能コンポーネントが扱うデータの重要度に応じて必要としている機能要件を設定している。この機能コンポーネントはデジタルタコグラフと同じようにプリント基板とそれを保護する筐体から構成される。PP 作者は、サイドチャネル攻撃への対抗機能や物理攻撃への対抗機能を要件化しているが、デジタルタコグラフ PP では ISO15408 の要件を選択し

ているのに対し、金融端末 PP では PP のなかで要件を新たに定義している。自動車業界においては、このように PP の中で新たに要件を定義する手法を参考にできると考えられる。

(3) 自動車業界のコンポーネントに対する評価方法・評価基準ドラフト

① 概要

本章では、下図（図 3.2a.1-8）に示される平成 27 年度の調査対象の標準コンポーネント（標準 ECU）におけるリプログラミング、デバッグなどの特権機能を含めアプリ非依存の基本機能に関わるセキュリティ機能の評価基準・評価方法の調査検討結果をまとめた。

標準 ECU は各種 ECU の共通プラットフォームの位置づけであり、前章での調査検討した他業界、特に、スマートカード業界における共通のプラットフォームとされるスマートカード PP［BSI-PP-0084］との類似点・相違点を基にしながら、標準 ECU に対する評価基準・評価方法を検討した。

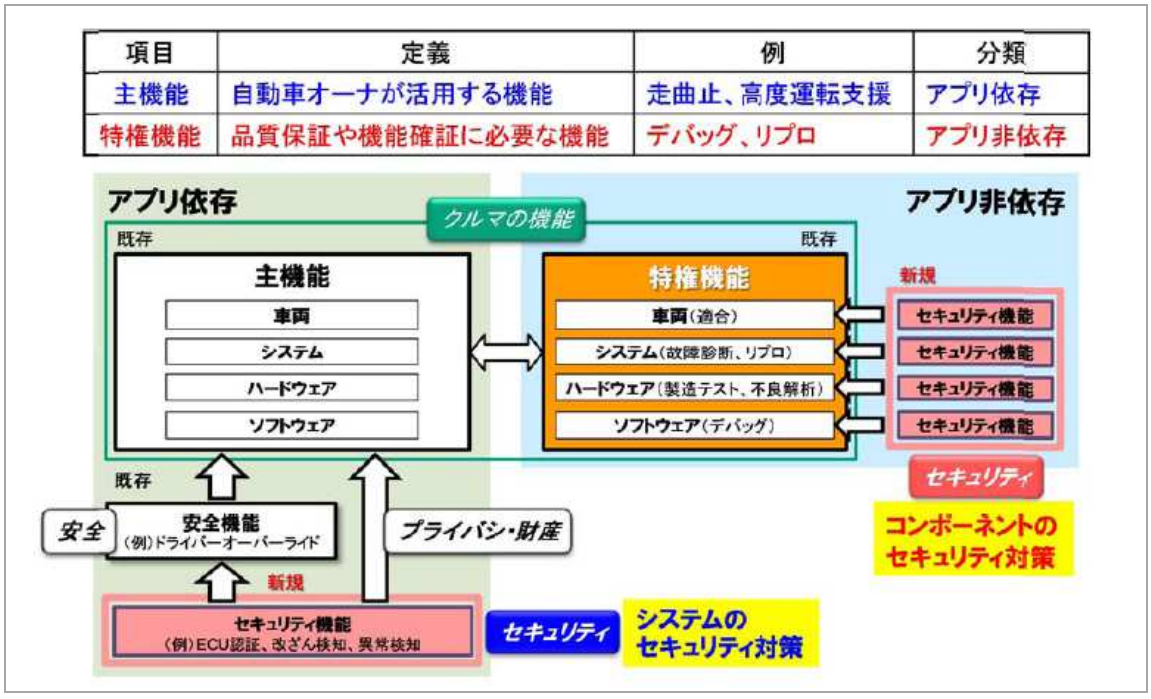


図 3.2a.1-8　自動車の機能とセキュリティ対策との関係　（出典：本テーマ企画提案書）

② 他業界と自動車業界の類似点、相違点

(ｉ) 評価対象の範囲とモデル（標準 ECU）

今回の検討対象とした標準 ECU の評価対象範囲を下図（図 3.2a.1-9）に示す。ECU に求められるセキュリティ要件は、主機能の動作を攻撃から保護するアプリ依存の要件と、特権機能など ECU として共通化が可能なアプリ非依存の要件の 2 種類がある。今回は標準 ECU に対する評価のため、後者のアプリ非依存要件を対象とした。

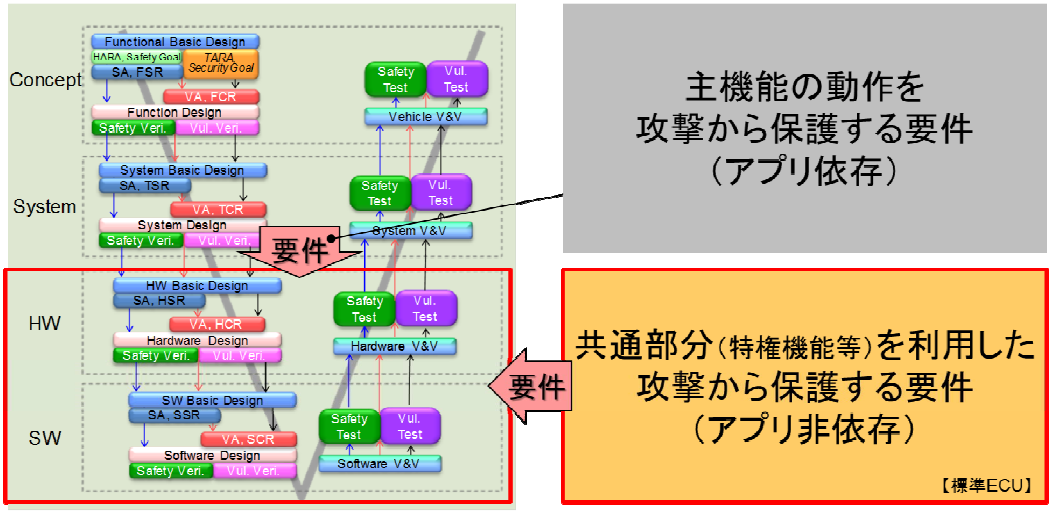


図 3.2a.1-9　標準 ECU の評価対象範囲

この標準 ECU の評価対象範囲は、下図（図 3.2a.1-10）に示すスマートカードの基本 PP［BSI-PP-0084］の評価対象範囲（黄色の「Security IC PP」部分）と極めて類似性が高く、上位に業務依存の各種アプリが搭載されて、個別の製品が開発・評価されることを意識した「共通プラットフォーム」の範囲・評価モデルとして、共通性がある。

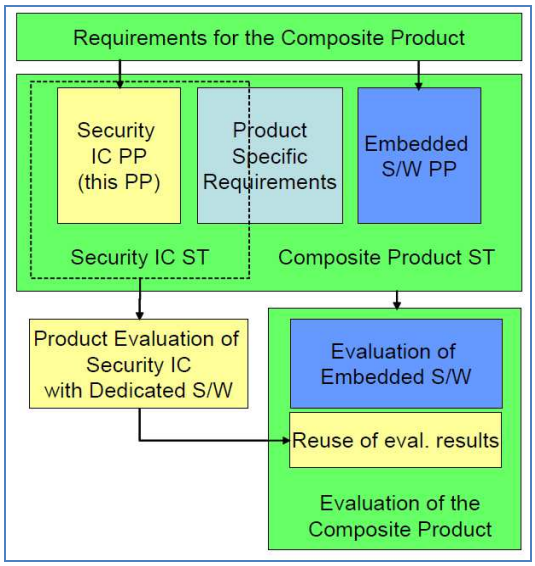


図 3.2a.1-10　スマートカード基本 PP の評価対象範囲（出典：[BSI-PP-0084]）

次に、今回の評価検討対象とした標準 ECU の攻撃モデルを図 3.2a.1-11 に示す。標準 ECU としての保護資産を「プログラム」、「データ」と定義し、それらを脅かす攻撃パターンを整理したものである。

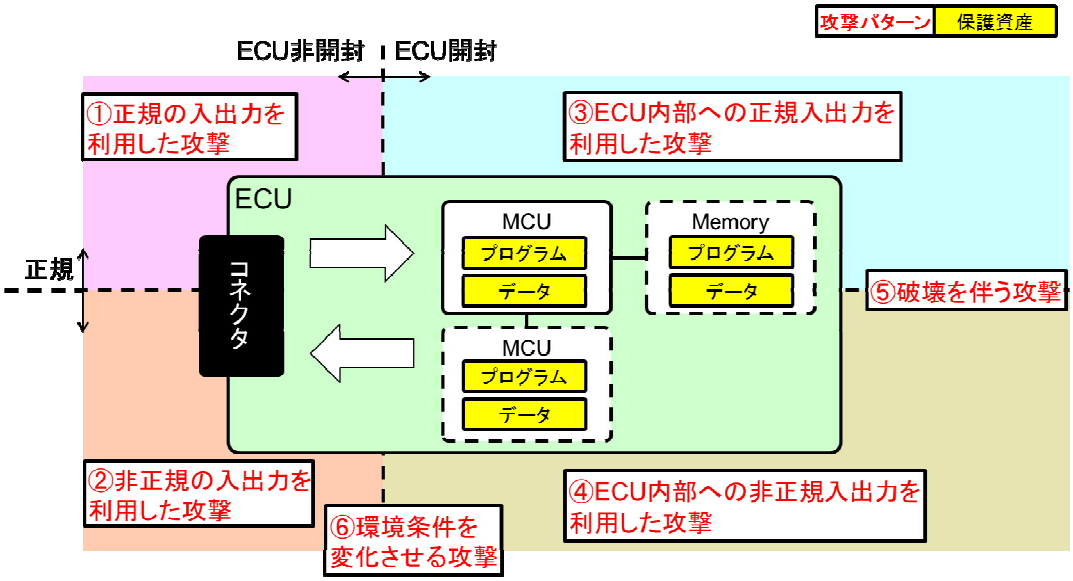


図 3.2a.1-11　標準 ECU の攻撃モデル

この標準 ECU の攻撃モデルは、下図（図 3.2a.1-12）に示すスマートカードの基本 PP［BSI-PP-0084］の物理境界・外部インターフェースとその境界を介した攻撃モデルとも、正規インターフェースの種類は異なるものの、共通点が多い。

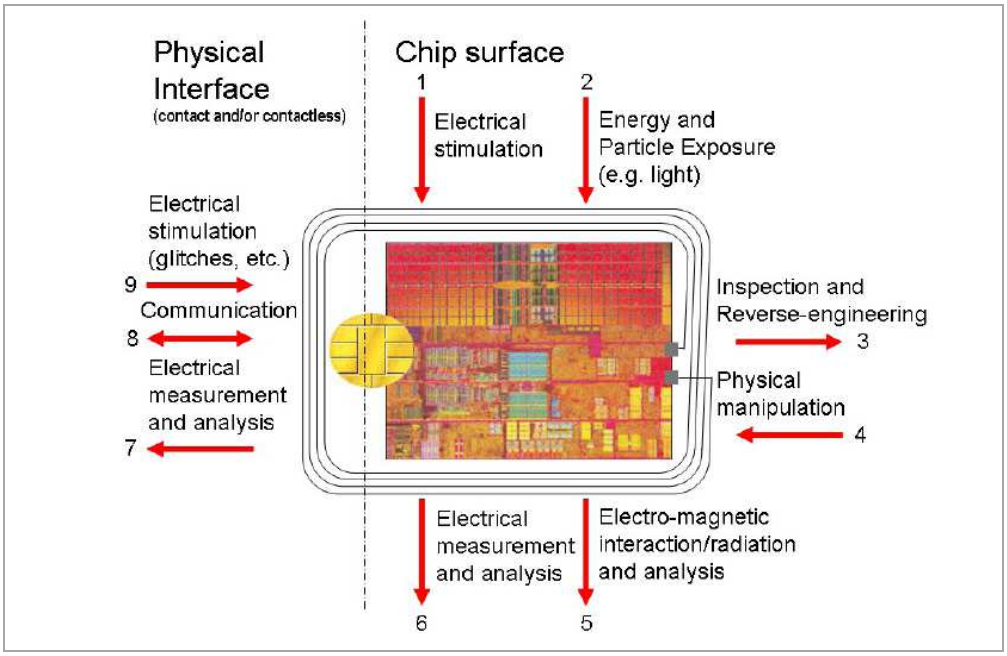


図 3.2a.1-12 スマートカード基本 PP の物理境界・外部インターフェース（出典：［BSI-PP-0084］）

(ⅱ) 想定される脅威・攻撃方法

標準ECUに想定される脅威･攻撃方法について､前掲の標準ECUの攻撃モデル(図3.2a.1-11）を用いて、他業界、特に、スマートカード業界で想定されている脅威・攻撃方法を参考に整理した結果を下表（表3.2a.1-11）に示す。

表3.2a.1-11　標準ECUの攻撃モデルを用いた攻撃方法分類・整理

	ECU非開封	ECU開封	ECU破壊
正規 入出力IF	・ソフトウェア攻撃 ・アプリケーション分離の迂回 ・ファジング（ソフトウェアバグの探索・検出） ・脆弱な暗号の悪用 ・脆弱な乱数の悪用	・JTAGデバッグインターフェースの悪用 ・物理プローブ（MCU/メモリ、PCBなど）	・センサ無効化 ・レーザー故障解析 ・チップ破壊解析 ・乱数攻撃 ・閉塞されたテストインターフェースの悪用
非正規 入出力IF	・ファジング（隠しインターフェースの探索・検出）	・テストインターフェースの悪用 ・隠しインターフェースの悪用 ・物理プローブ（内部バスなど） ・サイドチャネル	
環境条件 操作	・電源グリッチ/クロックグリッチ ・温度操作		・温度操作

これらを攻撃方法（攻撃パターン）として、大きく分類･整理すると以下のようになる。（[]内の記載は、表3.2a.1-11で整理した攻撃方法である）

A1. 正規インターフェース（API、含：リプログラミング用）の悪用
［ソフトウェア攻撃、アプリケーション分離の迂回］

A2. デバッグインターフェースの悪用
［JTAGデバッグインターフェースの悪用、テストインターフェースの悪用］

A3. （デバッグインターフェース以外に存在する可能性のある）隠しインターフェースの悪用
［ファジング（隠しインターフェースの探索・検出）、隠しインターフェースの悪用］

A4. ソフトウェアバグの悪用
［ソフトウェア攻撃、ファジング（ソフトウェアバグの探索・検出)］

A5. 実装暗号の不備（評価されていない独自暗号、実装評価されていない標準暗号）を利用
［脆弱な暗号の悪用、サイドチャネル、レーザー故障解析、電源グリッチ/クロックグリッチ］

A6. 実装乱数の不備（乱数品質が評価されていない独自乱数・標準乱数）を利用
［脆弱な乱数の悪用、乱数攻撃］

A7. 物理的な攻撃

A7.1 物理加工

［センサ無効化、チップ破壊解析、閉塞されたテストインターフェースの悪用］

A7.2 環境条件設定　［電源グリッチ/クロックグリッチ、温度操作］

A7.3 物理プローブ　［物理プローブ（MCU/メモリ、PCB）（内部バスなど)］

A7.4 サイドチャネル　［サイドチャネル］

A7.5 かく乱（パータベーション）・故障利用

［レーザー故障解析、チップ破壊解析、電源グリッチ/クロックグリッチ］

対象となるインターフェースや物理攻撃の対象となる箇所・物理特性が異なるところもあるが、攻撃パターンはスマートカード業界と類似している。

従って、これらの標準 ECU に想定される脅威を、スマートカードの基本 PP［BSI-PP-0084］を参考に分類・整理することが可能であり、以下のようにまとめることができる。

T.ECU1（一般的な情報リークの脅威）

攻撃者は、資産の一部である秘密ユーザデータを暴露するために、標準 ECU の使用中にリークする情報を利用するかも知れない。

T.ECU2（物理プローブによる情報曝露の脅威）

攻撃者は、以下の目的のために標準 ECU を物理的にプロービングするかも知れない。

1) ユーザデータの暴露、2) 組込みソフトウェアの暴露または改ざん、

3) ユーザデータや組込みソフトウェアの暴露や改ざんを可能にする評価対象の動作に関する重要なデータの暴露。

T.ECU3（環境ストレスによる誤動作の脅威）

攻撃者は、下記の目的のために、環境ストレスを与えてセキュリティ機能または組込みソフトウェアの誤動作を起こさせるかも知れない。

1) 評価対象のセキュリティサービスの改変、または、2) 組込みソフトウェアのセキュリティサービスの改変、3) ユーザデータや組込みソフトウェアの暴露やマニピュレーションを可能にする標準 ECU のセキュリティメカニズムの停止または悪影響。

これは、標準 ECU の通常の使用条件外で達成されるかも知れない。

T.ECU4（物理的改変による誤動作の脅威）

攻撃者は、下記の目的のために、標準 ECU を物理的に改変するかも知れない。

1) ユーザデータの改変、2) 組込みソフトウェアの改変、3) 標準 ECU のセキュリティサービスの改変または停止、4) ユーザデータや組込みソフトウェアの暴露やマニピュレーションを可能にする標準 ECU のセキュリティメカニズムの改変。

T.ECU5（強制的な情報リークの脅威）

攻撃者は、資産の一部である秘密ユーザデータを暴露するために、強制的に情報リークを誘引させるような操作を行って、使用中の標準 ECU からリークする情報を利用するか

も知れない。

T.ECU6（閉塞機能の不正使用による脅威）　［塞いだデバッグ/テスト機能等の不正使用を想定］

攻撃者は、標準 ECU の配付後には使われないような機能を使って、1) ユーザデータや組込みソフトウェアの暴露やマニピュレーション、2) 標準 ECU のセキュリティサービスのマニピュレーション（探索、バイパス、非活性化、改変）、3) 組込みソフトウェアの機能のマニピュレーション（探索、バイパス、非活性化、改変）、4) ユーザデータや組込みソフトウェアの暴露やマニピュレーションを可能にする攻撃をするかも知れない。

T.ECU7（特権機能の不正使用による脅威）　［リプログラミング/診断機能等の不正使用を想定］

攻撃者は、標準 ECU の特権機能を不正に使用して、1) ユーザデータや組込みソフトウェアの暴露やマニピュレーション、2) 標準 ECU のセキュリティサービスのマニピュレーション（探索、バイパス、非活性化、改変）、3) 組込みソフトウェアの機能のマニピュレーション（探索、バイパス、非活性化、改変）、4) ユーザデータや組込みソフトウェアの暴露やマニピュレーションを可能にする攻撃をするかも知れない。

T.ECU8（暗号の実装の欠陥による脅威）　［AES/SHA 等を想定］

攻撃者は、暗号の実装の欠陥を利用して、標準 ECU のセキュリティサービスが提供する暗号操作や暗号鍵を解読するかも知れない。

T.ECU9（実装乱数の欠陥による脅威）

攻撃者は、乱数の乱数性の不足を利用して、標準 ECU のセキュリティサービスが生成する乱数を予測したり、見つけたりするかも知れない。

T.ECU10（ソフトウェアバグの悪用）

ファジング攻撃を含め、本脅威は、標準 ECU 自体が対抗すべき脅威（すなわち、機能要件を導き出すための脅威）ではなく、標準 ECU のソフトウェア開発に対する保証要件（ADV、ALC）で対抗する脅威となる。

(ⅲ) 必要なセキュリティ対策の考え方（セキュリティ対策方針）

標準 ECU に想定される脅威に対するセキュリティ対策を考える上でも、前述のスマートカードの基本 PP［BSI-PP-0084］が非常に参考になる。

ます、セキュリティ対策方針を定めるにあたって、その基本的な考え方として、「セキュリティゴール（SG)」を設定している点である。

組込みソフトウェアの共通プラットフォームとしては、標準 ECU も同様で、以下のようなセキュリティゴールを設定するとセキュリティ対策方針が導きやすいと考えられる。

【基本的な考え方：セキュリティゴール（SG)】

SG.ECU1：ユーザデータ・組込みソフトの完全性を維持すること

SG.ECU2：ユーザデータ・組込みソフトの機密性を維持すること

SG.ECU3：標準 ECU が提供するセキュリティサービスの正確な動作を維持すること

SG.ECU4：実装確認された標準暗号サービスを提供すること

SG.ECU5：乱数性が確認された乱数を提供すること

この基本的な考え方の下で、標準 ECU に求められるセキュリティ対策方針は、概ね、以下のようなものにまとめることができる。

【セキュリティ対策方針】

O.ECU1（一般的な情報リークに対する保護）

評価対象は、標準 ECU に保存され、処理される秘密のユーザデータの暴露に対抗する保護を提供しなければならない。

O.ECU2（物理プローブによる情報曝露に対する保護）

評価対象は、ユーザデータの暴露に対抗する保護、組込みソフトウェアの暴露／改ざんに対抗する保護、評価対象の動作に関するその他の重要なデータの暴露に対抗する保護を提供しなければならない。

O.ECU3（環境ストレスによる誤動作に対する保護）

評価対象は、正しい動作を保証しなければならない。

評価対象は、信頼性やセキュリティ動作が証明されていない、または、テストされていない通常動作条件外での動作を知らせるか、防がなければならない。これは、誤動作を防止するためである。環境の例としては、電圧、クロック周波数、温度、外部のエネルギー場がある。

O.ECU4（物理的改変による誤動作に対する保護）

評価対象は、自分自身（ソフトウェア、データを含む)、組込みソフトウェア、ユーザデータの改ざん（下記を含む）に対抗する保護を提供しなければならない。

・(設計と、その属性や機能を理解するための）リバースエンジニアリング

・ハードウェアと全てのデータの改ざん

・メモリ内容（アプリケーションデータ）の改ざん

O.ECU5（強制的な情報リークに対する保護）

評価対象は、強制的に情報リークを誘引させるような操作に対しても、標準 ECU の中で処理されている秘密データの暴露に対抗する保護を提供しなければならない。

・強制的な誤動作によるもの（O.ECU3 環境ストレスによる誤動作保護関連）

・物理的改ざんによるもの（O.ECU4 物理的改変による誤動作保護関連）

・その他の強制的な情報リーク操作

O.ECU6（閉塞機能の不正使用に対する保護）
評価対象は、標準 ECU の配付後には使われないような機能、例えばデバッグ機能、テスト機能、が不正に使用され、1) ユーザデータや組込みソフトウェアの暴露、2) 組込みソフトウェア、および、そのクリティカルデータに対する操作（探索、バイパス、非活性化、改変）、3)標準 ECU のセキュリティサービスに対する操作（探索、バイパス、非活性化、改変）が行われることに対抗する保護を提供しなければならない。

O.ECU7（特権機能の不正使用に対する保護）
評価対象は、標準 ECU の特権機能が不正に使用され、1) ユーザデータや組込みソフトウェアの暴露、2) 組込みソフトウェア、および、そのクリティカルデータに対する操作（探索、バイパス、非活性化、改変）、3) 標準 ECU のセキュリティサービスに対する操作（探索、バイパス、非活性化、改変）が行われることに対抗する保護を提供しなければならない。

O.ECU8（実装確認された標準暗号の提供と保護）
評価対象は、実装確認された標準暗号を使った暗号サービスを提供しなければならない。

O.ECU9（乱数性が確認された乱数の提供と保護）
評価対象は、予測不能で十分な乱雑さを持つ乱数を提供しなければならない。

(ⅳ) 求められるセキュリティ機能

ISO15408（CC）では、策定したセキュリティ対策方針をどのように実現するか、その実現手段を、セキュリティ機能要件の観点では、Part2 の機能要件カタログから、セキュリティ保証要件の観点では、Part3 の保証要件パッケージから、各々適切なものを選択・カスタマイズしながら要件定義として完成させるのが一般的である（この点が、機能要件・保証要件いずれも規格の中に明確に規定されている ISOISO19790/24759/ FIPS140-2 との大きな違いである）。

前節で導出したセキュリティ対策方針を、どのようなセキュリティ機能要件を使って実現すればよいか、すなわち、求められるセキュリティ機能/機能要件は具体的にどのようなものかについて、これも前述のスマートカードの基本 PP［BSI-PP-0084］を参考しながら導き出してみると、求められるセキュリティ機能/機能要件は、以下のようなものにまとめることができる。

ここでは、Part2 の機能要件ひとつひとつの詳細を記述するのは本書の枠を超えるので、機能要件の主な要件クラス名/ファミリ名/コンポーネント名で記述しているが、例示が必要なものについては、いくつか後方に機能要件そのものを記載している。

【セキュリティ対策方針ごとに対応させた機能要件】
O.ECU1（一般的な情報リークに対する保護）の実現
- FDP_ITT.1　基本内部転送保護（Basic internal transfer protection）
- FPT_ITT.1　基本 TSF 内データ転送保護（Basic internal TSF data transfer protection）
- FDP_IFC.1　サブセット情報フロー制御（Subset information flow control）

O.ECU2（物理プローブによる情報曝露に対する保護）の実現

・FDP_SDC.1　保存データ機密性（Stored data confidentiality）

・FPT_PHP.3　物理的攻撃への抵抗（Resistance to physical attack）

O.ECU3（環境ストレスによる誤動作に対する保護）の実現

・FRU_FLT.2　制限付き耐障害性（Limited fault tolerance）

・FPT_FLS.1　セキュアな状態を保持する障害（Failure with preservation of secure state）

O.ECU4（物理的改変による誤動作に対する保護）の実現

・FDP_SDI.2　蓄積データ完全性監視及びアクション（Stored data integrity monitoring and action）

・FPT_PHP.3　物理的攻撃への抵抗（Resistance to physical attack）

O.ECU5（強制的な情報リークに対する保護）の実現

・O.ECU1（一般的な情報リークに対する保護）を実現するものすべて

- FDP_ITT.1　基本内部転送保護
- FPT_ITT.1　基本 TSF 内データ転送保護
- FDP_IFC.1　サブセット情報フロー制御

・O.ECU3（環境ストレスによる誤動作に対する保護）と O.ECU2（物理プローブによる情報曝露に対する保護）を実現する以下のもの

- FRU_FLT.2　制限付き耐障害性
- FPT_FLS.1　セキュアな状態を保持する障害
- FPT_PHP.3　物理的攻撃への抵抗

O.ECU6（閉塞機能の不正使用に対する保護）の実現

・FMT_LIM.1 制限付き能力（Limited capabilities）

・FMT_LIM.2 制限付き利用（Limited availability）

・O.ECU1（一般的な情報リークに対する保護）～O.ECU5（強制的な情報リークに対する保護）を実現するものすべてが、閉塞機能の不正使用保護に寄与する

O.ECU7（特権機能の不正使用に対する保護）の実現

・FIA_*　利用者の識別と認証

・FDP_ACC/ACF　アクセス制御

・FDP_IFC/IFF　情報フロー制御

・FMT_*　セキュリティ管理

・FTP_ITC.1 TSF 間高信頼チャネル

・FTP_TRP.1 高信頼パス

・O.ECU1（一般的な情報リークに対する保護）～O.ECU5（強制的な情報リークに対する保護）を実現するものすべてが、特権機能の不正使用保護に寄与する

O.ECU8（実装確認された標準暗号の提供と保護）の実現

・FCS_COP.1 暗号操作（Cryptographic operation）
・FCS_CKM.1 暗号鍵生成（Cryptographic key generation）
・FCS_CKM.2 暗号鍵配付（Cryptographic key distribution）
・FCS_CKM.3 暗号鍵アクセス（Cryptographic key access）
・FCS_CKM.4 暗号鍵破棄（Cryptographic key destruction）
・FPT_TST.1 TSF 自己テスト （あるいは、開発保証要件 ADV_ARC.1 で対応）
・O.ECU1（一般的な情報リークに対する保護）～O.ECU5（強制的な情報リークに対する保護）を実現するものすべて

O.ECU9（乱数性が確認された乱数の提供と保護）の実現

・FCS_RNG.1 乱数生成（Random number generation）
・FPT_TST.1 TSF テスト（あるいは、開発保証要件 ADV_ARC.1 で対応）
・O.ECU1（一般的な情報リークに対する保護）～O.ECU5（強制的な情報リークに対する保護）を実現するものすべて

これらの中で、FDP_SDC.1、FMT_LIM.1、FMT_LIM.2、FCS_RNG.1 は、標準の Part2 のカタログにはないが、その拡張定義機能を使って、標準 ECU に必要となる機能要件として追加拡張したものである。

また、標準の機能要件カタログに定義されている機能要件は、多様な分野への適用が可能となるように、実現するセキュリティ機能のレベルに応じて、機能要件そのものを選択する、あるいは、テンプレート化されている機能要件の部分を適宜カスタマイズすることができるようになっている。

以下にその例をいくつか示す。イタリックで表記されている部分がカスタマイズ可能な（選択・割付等の操作によって目的とする機能要件を完成させる）部分である。

a. 乱数生成に関するもの

FCS_RNG.1 乱数の生成

FCS_RNG.1.1	TSF は、[割付: *セキュリティ能力のリスト*] を実現する [選択: *物理的*、*非物理的真*、*決定論的*、*ハイブリッド物理的*、*ハイブリッド決定論的*] 乱数生成器を提供しなければならない。
FCS_RNG.1.2	TSF は、[割付: *定義された品質尺度*] を満たす[選択: *ビット*, *オクテットビット*, *数*[割付: *数値の形式*]]の乱数を提供しなければならない。

b. 暗号操作に関するもの

FCS_COP.1 暗号操作

FCS_COP.1.1	TSF は、[割付: *標準のリスト*]に合致する、特定された暗号アルゴリズム[割付: *暗号アルゴリズム*]と暗号鍵長[割付: *暗号鍵長*]に従って、[割付: *暗号操作のリスト*]を実行しなければならない。

FIA_SOS.1 秘密の検証

FIA_SOS.1.1　TSF は、秘密が[割付: *定義された品質尺度*]に合致することを検証するメカニズムを提供しなければならない。

FIA_SOS.2 TSF 秘密生成

FIA_SOS.2.1　TSF は、[割付: *定義された品質尺度*]に合致する秘密を生成するメカニズムを提供しなければならない。

FIA_SOS.2.2　TSF は、[割付: *TSF 機能のリスト*]に対し、TSF 生成の秘密の使用を実施できなければならない。

ここで、FCS_RNG や FIA_SOS にてカスタマイズが必要な「定義された品質尺度」は、リスク値に応じて割付値、つまり基準を決める必要がある。

リスク値は「影響度」と「発生可能性」の 2 点でリスクアセスメントをするが、特に ECU に対する攻撃の「発生可能性」については、定量化の研究事例が存在せず、自動車業界としての検討が必要になる。そこで、平成 27 年度はリプログラミングモジュール認証時の乱数の品質尺度に着目した発生可能性の定量化を行うべく、評価対象の開発を実施した。本内容は 3.2a.2 で詳細を説明する。

③ 自動車業界のコンポーネントに対する評価方法・評価基準案

(ｉ) 自動車業界のコンポーネントに対する評価方法案

自動車業界のコンポーネントに対する評価方法案の検討にあたって、情報セキュリティ評価の国際的な標準となっている ISO15408/18045（CC/CEM）における評価モデルと評価の流れを参考とした。ISO15408/18045（CC/CEM）における評価モデルを以下に示す（図 3.2a.1-13）。

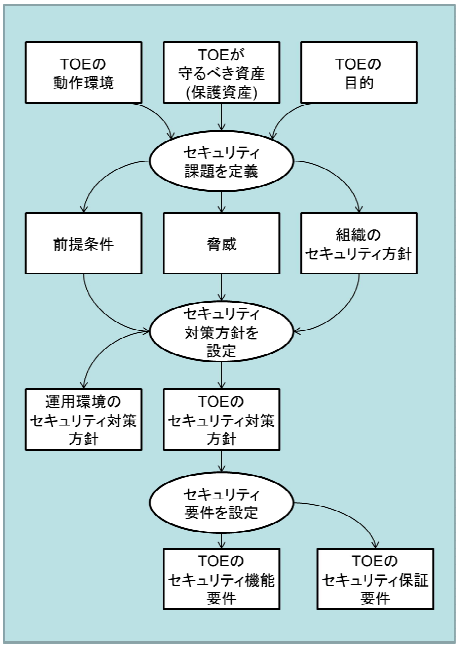


図 3.2a.1-13　CC のセキュリティ評価モデル

この評価モデルにおけるポイントは以下の通りである。

・何（保護資産）を、何（脅威）から
・どのような環境（動作環境）と付帯条件（前提条件、組織方針）の下で
・どのような対策方針（セキュリティ対策方針）に基づいて、守るのか
・その対策方針はどのようなセキュリティ要件（機能要件、保証要件）で実現するのか

標準 ECU に対する保護資産や脅威、機能要件等は既に前節にて定義済みである。これに対し、ISO15408/18045（CC/CEM）では以下の流れで保証要件の評価を実施する。

・要件定義されたセキュリティ機能要件が、対策方針を過不足なく満たし、確実に脅威に対抗できているか評価[APE/ASE 評価]
・評価確認されたセキュリティ機能要件が、実際の製品設計・開発、製造・出荷（含：ガイダンス）、製品テストの各段階で、正確かつ十分なレベルで実現されているか評価[ADV/AGD/ALC/ATE 評価]
・上記の各評価過程を含めて、製品に実装したセキュリティ機能について、悪用される可能性のある脆弱性があるかどうか、製品全体としての脆弱性を評価[AVA 評価]

また、保証要件の一覧を以下に示す（表 3.2a.1-12）。

表 3.2a.1-12　ISO15408/18045（CC/CEM）の保証要件一覧

工程	保証クラス	保証ファミリ	名称
要件定義	プロテクションプロファイル評価（APE）	APE_INT	PP概説
		APE_CCL	適合主張
		APE_SPD	セキュリティ課題定義
		APE_OBJ	セキュリティ対策方針
		APE_ECD	拡張コンポーネント定義
		APE_REQ	セキュリティ要件
	セキュリティターゲット評価（ASE）	ASE_INT	ST概説
		ASE_CCL	適合主張
		ASE_SPD	セキュリティ課題定義
		ASE_OBJ	セキュリティ対策方針
		ASE_ECD	拡張コンポーネント定義
		ASE_REQ	セキュリティ要件
		ASE_TSS	TOE要約仕様
開発設計	開発（ADV）	ADV_FSP	機能仕様
		ADV_TDS	TOE設計
		ADV_IMP	実装表現
		ADV_SPM	セキュリティ方針モデル化
		ADV_ARC	セキュリティアーキテクチャ
		ADV_INT	TSF内部構造
	ガイダンス（AGD）	AGD_PRE	準備手続き
		AGD_OPE	利用者操作ガイダンス
製造出荷	ライフサイクルサポート（ALC）	ALC_LCD	ライフサイクル定義
		ALC_CMC	CM能力
		ALC_CMS	CM範囲
		ALC_DVS	開発セキュリティ
		ALC_TAT	ツールと技法
		ALC_FLR	欠陥修正
		ALC_DEL	配布
テスト	テスト（ATE）	ATE_FUN	機能試験
		ATE_COV	カバレージ
		ATE_DPT	深さ
		ATE_IND	独立テスト
	脆弱性評定（AVA）	AVA_VAN	脆弱性分析

ここで、標準 ECU に適用可能な保証要件を検討する。標準 ECU では、要件定義～開発～テストまでのプロセスを対象としていることから、ガイダンス（AGD）やライフサイクルサポート（ALC）は除外することができる。脆弱性評定（AVA）に関しては、要件定義～設計の早期の段階から、脆弱性を意識した網羅的な検討を行い、（３）-②-（ｉｖ）で示した標準 ECU に対する対策（セキュリティ機能等）を定義しているため、不要と考える。また、プロテクションプロファイル評価（APE）、セキュリティターゲット評価（ASE）の適合主張（APE_CCL/ASE_CCL）とセキュリティ要件（APE_REQ/ASE_REQ）は、ISO15408/18045（CC/CEM）通りに各要件が厳格に定義されているかを評価するものであり、認証を取得しない場合はあまり意味をなさない。

以上より、標準 ECU に適用可能な保証要件は以下のように定義することができる（表 3.2a.1-13）。

表 3.2a.1-13　標準 ECU に適用可能な保証要件一覧

工程	保証クラス	保証ファミリ	名称
要件定義	プロテクションプロファイル評価 (APE)	APE_INT	PP概説
		APE_SPD	セキュリティ課題定義
		APE_OBJ	セキュリティ対策方針
		APE_ECD	拡張コンポーネント定義
	セキュリティターゲット評価 (ASE)	ASE_INT	ST概説
		ASE_SPD	セキュリティ課題定義
		ASE_OBJ	セキュリティ対策方針
		ASE_ECD	拡張コンポーネント定義
		ASE_TSS	TOE要約仕様
開発設計	開発 (ADV)	ADV_FSP	機能仕様
		ADV_TDS	TOE設計
		ADV_IMP	実装表現
		ADV_SPM	セキュリティ方針モデル化
		ADV_ARC	セキュリティアーキテクチャ
		ADV_INT	TSF内部構造
テスト	テスト (ATE)	ATE_FUN	機能試験
		ATE_COV	カバレージ
		ATE_DPT	深さ
		ATE_IND	独立テスト

・プロテクションプロファイル評価（APE。以降、PP 型要件定義評価）

この評価クラスにおいては、プロテクションプロファイル（PP 型要件定義書）が信頼でき内部的に一貫していること、および、所定の内容を満たすものとして、適切に実装非依存型のセキュリティ要件定義を行っているかを評価する。

・セキュリティターゲット評価（ASE。以降、ST 型要件定義評価）

この評価クラスにおいては、セキュリティターゲット（ST 型要件定義書）が信頼でき内部的に一貫していること、および、所定の内容を満たすものとして、適切に実装依存型のセキュリティ要件定義を行っているかを評価する。

・開発評価（ADV）

この評価クラスにおいては、実装依存型の ST 型要件定義書で定義された開発対象に対するセキュリティ機能要件（SFR）が、設計開発・実装段階で、過不足なく正確に詳細化・具体化され、評価対象に実装されていることを評価する。

・テスト評価（ATE）

この評価クラスにおいては、実装依存型の ST 型要件定義書に基づいて設計開発実装された評価対象のセキュリティ機能が、最終製品として設計記述通りに動作することを確認評価する。

これらの評価はいずれも、PP 型/ST 型要件定義で定義したセキュリティ機能要件（SFR）が、その要件定義された通りに、もれなく確実に実装され、テストされたかを評価するもので、すべてのセキュリティ機能要件（SFR）について、追跡し評価するものになっている。

ただし、ISO15408/18045（CC/CEM）では、具体的にどのように評価すべきか規定されていない。(2)-③-(ⅳ)-f.でも紹介したように、最近の米国 NIAP および CCRA では、「cPP（Collaborative Protection Profile）」という考え方の下で、PP に定義されている機能要件ごとに、どの範囲をどのようにテストすべきか、FIPS-DTR に近い形でのテスト要件・評価要件を、各々の cPP に対応する補助文書[12]として定める方法を定着させる方向で活動が進められている。

標準 ECU でもこの考え方は適用できると考え、(3)-②-(ⅳ)で定義した各機能要件に対して、どの範囲をどのようにテストすべきかを定義する、つまり評価の方法論を定義することが、自動車業界のコンポーネントに対する評価方法になり得ると考える。

(ⅱ) 自動車業界のコンポーネントに対する評価基準案

自動車業界のコンポーネントに対する評価基準案の検討にあたって、情報セキュリティ評価の国際的な標準となっている ISO15408/18045（CC/CEM）や関連業界の評価基準を参考とした。まず ISO15408/18045（CC/CEM）における評価基準であるセキュリティ評価保証レベル（EAL）対応要件一覧表を下表（表 3.2a.1-14）に示す。

[12] 例：CCRA Suppoeting Document, Mandatory Technical Document, Evaluation Activities for Network Device cPP, Version 1.0, February 2015, CCDB-2015-01-001
https://www.commoncriteriaportal.org/files/supdocs/CCDB-2015-01-001.pdf

表 3.2a.1-14　セキュリティ評価保証レベル（EAL）対応要件一覧表

工程	保証クラス	保証ファミリ	名称	評価保証レベル別コンポーネント						
				EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
要件定義	プロテクションプロファイル評価（APE）	APE_INT	PP概説	1						
		APE_CCL	適合主張	1						
		APE_SPD	セキュリティ課題定義	1						
		APE_OBJ	セキュリティ対策方針	2						
		APE_ECD	拡張コンポーネント定義	1						
		APE_REQ	セキュリティ要件	2						
	セキュリティターゲット評価（ASE）	ASE_INT	ST概説	1						
		ASE_CCL	適合主張	1						
		ASE_SPD	セキュリティ課題定義		1					
		ASE_OBJ	セキュリティ対策方針	1	2					
		ASE_ECD	拡張コンポーネント定義	1						
		ASE_REQ	セキュリティ要件	1	2					
		ASE_TSS	TOE要約仕様	1						
開発設計	開発（ADV）	ADV_FSP	機能仕様	1	2	3	4	5		6
		ADV_TDS	TOE設計		1	2	3	4	5	6
		ADV_IMP	実装表現				1		2	
		ADV_SPM	セキュリティ方針モデル化						1	
		ADV_ARC	セキュリティアーキテクチャ		1					
		ADV_INT	TSF内部構造					2	3	
	ガイダンス（AGD）	AGD_PRE	準備手続き	1						
		AGD_OPE	利用者操作ガイダンス	1						
製造出荷	ライフサイクルサポート（ALC）	ALC_LCD	ライフサイクル定義			1				2
		ALC_CMC	CM能力	1	2	3	4		5	
		ALC_CMS	CM範囲	1	2	3	4	5		
		ALC_DVS	開発セキュリティ				1		2	
		ALC_TAT	ツールと技法				1	2	3	
		ALC_FLR	欠陥修正							
		ALC_DEL	配布		1					
テスト	テスト（ATE）	ATE_FUN	機能試験			1			2	
		ATE_COV	カバレージ		1		2		3	
		ATE_DPT	深さ			1		3		4
		ATE_IND	独立テスト	1			2			3
	脆弱性評定（AVA）	AVA_VAN	脆弱性分析	1		2	3	4	5	

一方、自動車業界のコンポーネントに対するセキュリティ評価基準・評価方法を考える時、自動車業界のコンポーネントのセキュリティレベル（Security Level：SL）は、FIPS でのレベル分け（4 レベル）、欧州自動車業界で検討されているレベル分け（4 レベル）、制御システムのサイバセキュリティ基準 IEC62443 でのレベル分け（4 レベル）を考慮すると、1～4 の 4 段階を想定するのが自然と考えられることから、求められる 4 段階のセキュリティレベルと ISO15408（CC）セキュリティ評価保証レベル（EAL）との適切な対応関係を定めておくことが必要と考えられる。

今回検討した標準 ECU の攻撃モデル（図 3.2a.1-11）で想定した攻撃パターンは、最高レベルとして、スマートカード業界が標準設定している「EAL4+VAN.5」相当のものも含まれており、想定すべき攻撃者の攻撃能力、従って標準 ECU が持つべき攻撃耐性の最高レベルは「VAN.5」相当であると考えられる。これらのことから、自動車業界のコンポーネントに対するセキュリティレベル SL1～SL4 に対応する ISO15408 のセキュリティ評価保証レベルは以下のように設定するのが妥当と考えられる。

SL1： EAL2～EAL3　［基本的な攻撃能力に対する抵抗力を保証］
SL2： EAL4　［強化基本程度の攻撃能力に対する抵抗力を保証］
SL3： EAL4+VAN.4　［中程度の攻撃能力に対する抵抗力を保証］
SL4： EAL4+VAN5　［高度な攻撃能力に対する抵抗力を保証］

このように基準値となる自動車業界のセキュリティレベルは他業界や欧州自動車業界を参考に設定可能であるが、評価基準を定める上で、各レベルの攻撃能力の定量化が必要となる。

ただし、自動車業界のコンポーネントに対する評価方法でも述べたように、標準 ECU に対しての脆弱性評定は実施せず、要件定義～設計の早期の段階から、脆弱性を意識した網羅的な検討を行い、セキュリティ機能要件（対策）を定義するとした。

そのため機能要件をリスク値に応じてカスタマイズする必要がある。リスク値は「影響度」と「発生可能性」の 2 点でリスクアセスメントするが、「攻撃能力」と「発生可能性」は明確な関連性が存在する。高度な攻撃能力が必要な場合、攻撃に時間がかかったり専門知識が必要であったり、発生可能性は低くなる。

一方、基本的な攻撃能力でも十分な場合、誰でもすぐに攻撃ができる可能性があるため、発生可能性は高くなる。つまり標準 ECU に対する攻撃の発生可能性（攻撃能力）を定量化することが、評価基準の策定につながる。

他業界に目を向けるとスマートカード業界では、（2）-③-（ⅳ）で紹介した「スマートカードに対する攻撃能力の適用」とされる[AAMS]文書において、脅威となる実際の攻撃に対する攻撃能力の定量化基準をまとめたものが存在する。

自動車業界ではそのような研究事例が存在しないため、平成 27 年度は一例として、リプログラミングモジュール認証への攻撃に着目し、発生可能性の定量化に向けた評価対象の開発を実施した。本内容の詳細は 3.2a.2 で説明する。

(4) まとめ

① 他業界のコンポーネント評価技術

今回の調査で、先行する他業界、特にスマートカード分野等、IC と組込みソフトウェアから構成される電子機器の評価技術は、具体的なインターフェース・ハードウェア部品には異なる点もあるものの、極めて共通点が多く、自動車業界のコンポーネント評価に流用・活用可能なものが多々存在することが確認された。

ISO19790/24759（CMVP/FIPS）は、暗号モジュールに特化した試験基準・試験方法であり、自動車業界のコンポーネントが暗号モジュールとして、あるいは、標準暗号アルゴリズムを実装し、その暗号サービスを提供するコンポーネントである場合は、参考になる試験基準・試験方法である。

ISO15408/18045（CC/CEM）は、暗号モジュール・標準暗号アルゴリズム実装以外の広範囲な ICT 製品分野に適用され、多くの実績があるものの、評価基準・評価方法が汎用的・抽象的であるため、実適用に困難性が伴う評価基準・評価方法である。そのため、先行する他業界では、適用する製品分野ごとに、より明確・具体的な補助文書を作成した上で、その困難性を克服し、効果を上げていることが確認された。

② 自動車業界のコンポーネント評価方法・評価基準

自動車業界のコンポーネント評価方法に関して、先行する ICT 業界の事例を参考にしつつ、評価すべき対象、つまり標準 ECU にどのような脅威があり、どのようなセキュリティ要件（対策）を定義すべきかを洗い出すことができた。この中には脆弱性を意識した検討も含まれているため、ISO15408/18045（CC/CEM）で言われているような実際の製品に攻撃を行うような脆弱性評定は不要と考える。そのため、標準 ECU に対する評価方法としては、定義したセキュリティ要件が確実に実装され、テストされたかを評価するものになると考えられる。

また、自動車業界のコンポーネント評価基準に関して、他業界や欧州自動車業界を参考に基準値となるセキュリティレベルを 4 つ定義した。セキュリティレベルに紐付く発生可能性に関しては、継続的な議論が必要な内容であり、平成 27 年度は評価基準の一例を作るべく、リプログラミングモジュール認証への攻撃に着目し、発生可能性の定量化に向けた評価対象の開発を 3.2a.2 にて実施する。

3.2a.2　評価対象（コンポーネント）の開発

(1) はじめに

自動車業界のコンポーネント評価基準策定に向け、ECU に対する攻撃の発生可能性を定量化する必要がある。そこで、リプログラミングモジュール認証への攻撃に着目し、発生可能性の定量化に向けた評価対象を開発した。

(2) 開発対象の概要

① 自動走行時代のコンポーネントとしての標準 ECU の概要

自動走行時代のコンポーネントとしての標準 ECU は、自動走行機能を構成するという性質を鑑み、設計段階から安全面および信頼面について慎重に配慮しなければならない。これを IPA が提唱しているソフトウェア品質 6 特性（機能性、信頼性、使用性、効率性、保守性、移植性）の観点から分析すると、上記 6 特性の中でも機能性に含まれるセキュリティ（Security）に着目する必要がある。その理由を以下に記す。

- 標準 ECU が外部の情報ネットワークに Gateway（Firewall）を介して接続される場合、情報ネットワークを経由した脅威の対象になることが想定されるため。
- 特に ECU プログラム自体を改変するような脅威が発生し攻撃が成功した場合、ECU の不正動作や無効化が想定されるため。

上記理由のいずれも ECU や自動走行機能に対して重大な影響を与えるものである。設計者はこれらの影響を抑止するためにセキュリティ特性に着目し、コンポーネントのセキュリティモデルを構築する必要が有る。

本事業において開発する標準 ECU は、セキュリティ特性に対する評価が有効となるような機能を実装する。

※参照: 組込みソフトウェア開発における品質向上の勧め（コーディング編）
https://www.ipa.go.jp/files/000005106.pdf
※参照: 高信頼化ソフトウェアのための開発手法ガイドブック
https://www.ipa.go.jp/files/000005144.pdf

② リプログラミング環境全体

自動走行時代のコンポーネントとしての標準 ECU は、ECU を構成するプログラムのダウンロード（リプログラミング）を前提条件として設計する。これは標準 ECU における様々な機能上の問題を ECU プログラム更新で解決するために重要な手段である。

リプログラミング手段に関しては、ISO14229-1 Road vehicles – Unified diagnostic service（UDS）によって診断サービスの一機能として規定されている。リプログラミング環境は

この規定を実現するために必要な環境である。構成する要素を以下に記す。（図 3.2a.2-1）

・リプログラミング手順 – 共通規格（ISO14229-1）をベースにし、開発者の独自仕様を加えた診断サービス機能手順。

・リプログラミング手順を実施できる外部機器 – 一連のリプログラミング手順を何らかの手段で実行できる外部機器または PC ソフトウェア。

・リプログラミング可能な ECU – 上記リプログラミング手順を機能として実現するソフトウェアモジュールを実装した ECU。

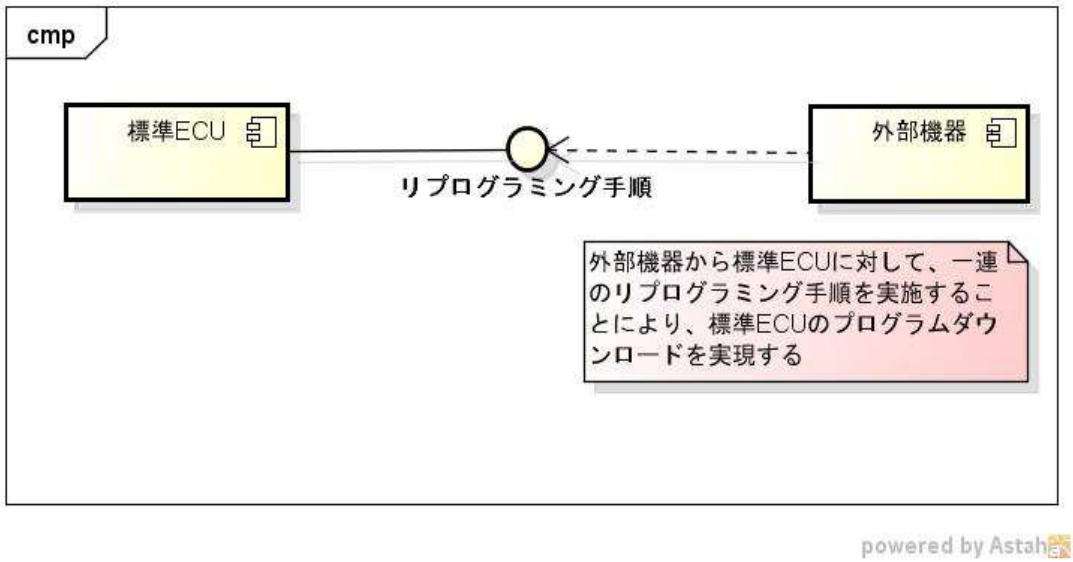


図 3.2a.2-1　リプログラミング環境構成

上記要素で構成するリプログラミング環境では、リプログラミング手順を保護するためのセキュリティ機能の堅牢性が重要となる。これはリプログラミング手順にセキュリティ的脆弱性が存在する場合、不正な外部機器によるリプログラミングが実現する、すなわちセキュリティ攻撃が成功する確率が高まるためである。

本事業では、これらリプログラミング手順の信頼性を評価することが可能となる評価コンポーネントを開発することとしており、まず、基本的な構成のものを開発した。

③ デバッグ環境全体

評価コンポーネントの開発期間および評価期間におけるデバッグ作業では下記の動作環境を使用した。（図 3.2a.2-2）この環境はマイコン評価用およびリプログラミング手順検証用として実績がある環境構成である。

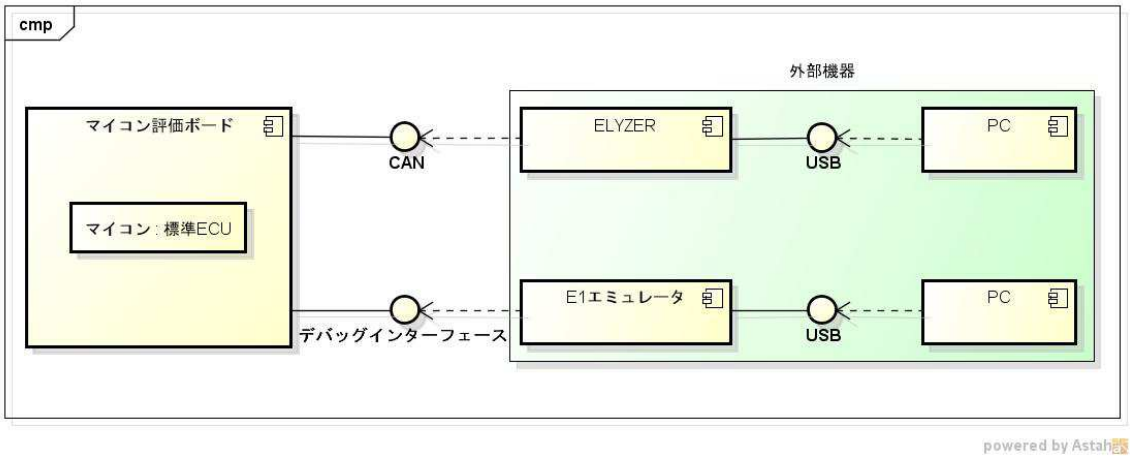


図 3.2a.2-2　デバッグ環境構成図

また両期間中においては、リプログラミング手順を実現する外部機器として ELYZER（イーソル株式会社製）を使用する。これはリプログラミング手順およびセキュリティ手順の動作を確認することを目的としている。更に ELYZER は CAN 通信アナライザ兼ログ取得ツールとしても使用可能である。

(3) 要求仕様

① 評価コンポーネント（標準 ECU）

評価コンポーネント（標準 ECU）に必要な機能を以下に記す。

・セキュリティ評価の対象となるような認証機能
・リプログラミング手順を実現するためのリプログラミング機能
・外部評価者が容易に評価コンポーネントの状態を認識できるような表示機能

上記機能は、実際の ECU に近い形式で実装する。その為、基本的な ECU の機能やインターフェースを実現できる車載マイコン環境を用意する。パソコンおよびエミュレータ環境上での仮想動作による機能実現は行わない。

本評価コンポーネントの要件を表 3.2a.2-1 に記す。

表 3.2a.2-1　評価コンポーネント要件一覧

項目	説明
マイコン	一般的な 32bit 車載マイコン （例: ルネサス エレクトロニクス株式会社製 RH850 シリーズ）。
通信規格	一般的な ECU 間通信、診断、リプログラミング、デバッグ等で用いられる CAN 通信。
評価ボード	使用する車載マイコンに対応した機能評価ボード。 CAN 通信インターフェースおよびデバッグポートを備えること。 動作状態を目視できる表示器（LED、LCD 等）を備えること。

※注: CAN ネットワーク仕様に関しては ISO15765-2 Road vehicles - Diagnostics on Controller Area Networks (CAN) - Part 2: Network layer services に準拠する。

② リプログラミング仕様

本評価コンポーネントで実現するリプログラミング仕様は、ISO14229-1 Road vehicles – Unified diagnostic service (UDS) Second edition 2013-03-15の記述に準拠する。ISO14229-1では一般的な診断サービスおよび各種仕様が規定されている。本評価では必要最小限のリプログラミング仕様をISO14229-1 Chapter 15 Non-volatile server memory programming processより抽出し設計と実装を行うものとする。

また評価コンポーネントには、リプログラミング禁止状態、許可状態を設定する。リプログラミング禁止状態から許可状態への遷移時は、セキュリティアクセス手順の正常完了を必須とする。

リプログラミング仕様要件を以下に記す。

・電源投入またはリセット後は、「リプログラミング禁止状態」に遷移すること。
・DSC 診断サービスを用いてセキュリティアクセス手順を実行できる状態に遷移すること。
・「リプログラミング許可状態」に遷移するには、セキュリティアクセス手順を用いて、認証成功すること。
・セキュリティアクセス手順を用いずに「リプログラミング許可状態」に遷移しないこと。
・リプログラミング許可状態において、プログラムダウンロード手順を用いた FLASH メモリ書き換え機能を実現すること。
・リプログラミング禁止状態において、プログラムダウンロード手順を用いた FLASH メモリ書き換え機能を拒否すること。

リプログラミング仕様における状態遷移を図 3.2a.2-3 に記す。

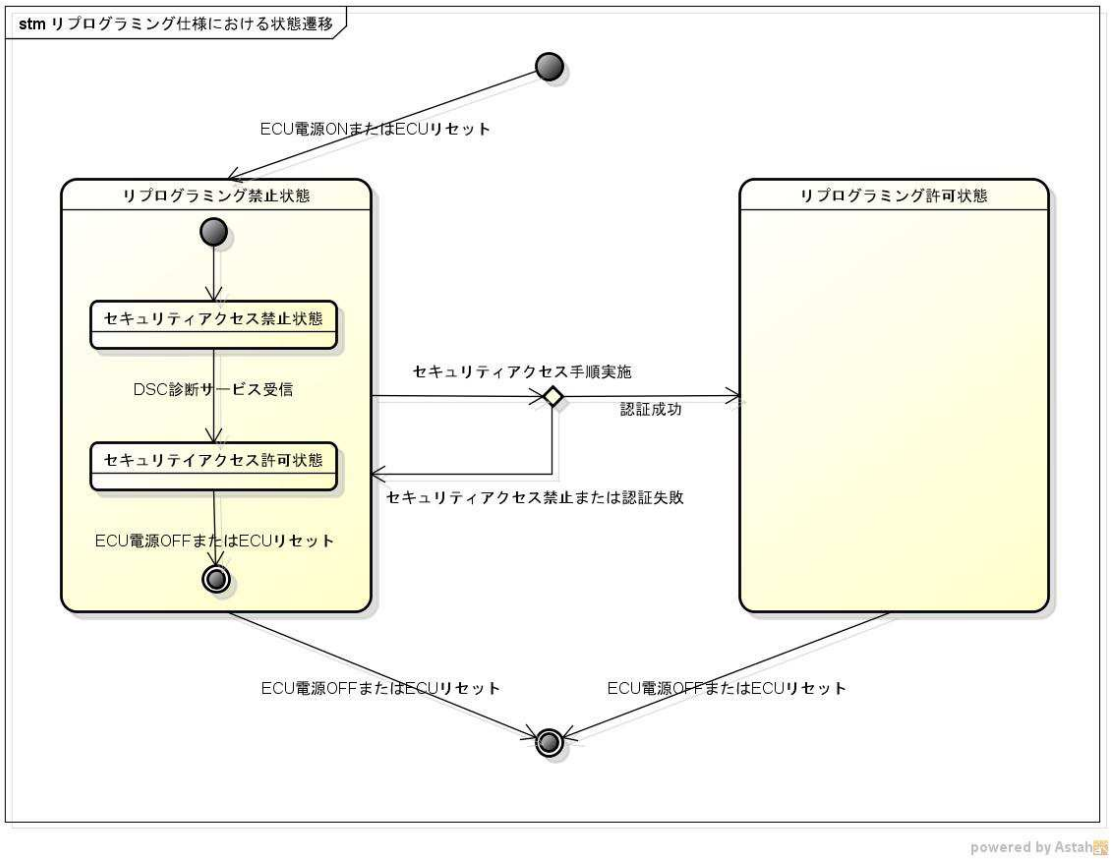


図 3.2a.2-3　リプログラミング仕様における状態遷移

ISO14229-1 準拠のリプログラミング手順をシーケンスとして図 3.2a.2-4 に記す。

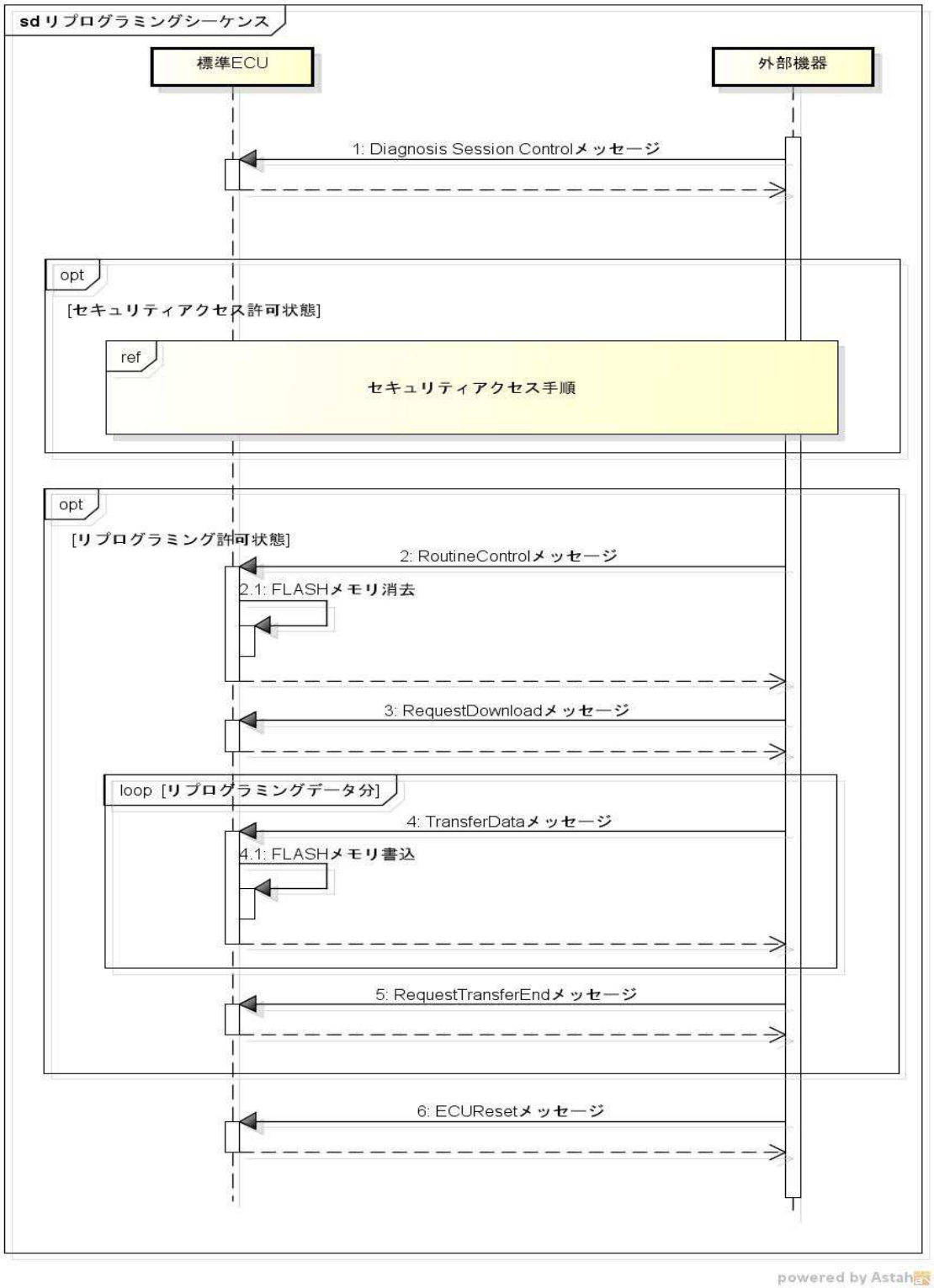


図 3.2a.2-4　リプログラミング手順

※注：シーケンス中の「～メッセージ」は ISO14229-1 にて規定された診断メッセージを示す。
※注：セキュリティアクセスシーケンスの詳細については、③セキュリティアクセス仕様にて規定する。
※注：2.RoutineControl メッセージから 5.RequestTransferEnd メッセージまでの手順がプログラムダウンロード手順となる。

③ セキュリティアクセス仕様

セキュリティアクセス仕様は、ISO14229-1 Road vehicles – Unified diagnostic service (UDS) Second edition 2013-03-15 の 15 Non-volatile server memory programming process および Annex I (normative) Security access state chart にある規定に準拠する。ただしこれらの規定にはツールからの ECU 認証形式のみ規定されており、その他の認証形式や手順詳細は規定されていない。よって本評価向けに認証形式と手順の詳細を定義する必要がある。

セキュリティアクセス仕様の機能要件を以下に記す。

・診断サービスメッセージを使用した相互認証（ECU からツール、ツールから ECU)を実現すること。
・暗号化アルゴリズムは AES128 を使用する。
・暗号化アルゴリズムで使用する鍵は、類推されにくい鍵を選定すること。
（例：「123456…」や「abcdef…」のような、一般的に脆弱とされる定型的な数値や文字列を使用しないこと。）
・疑似乱数生成器アルゴリズムは、標準的な疑似乱数生成を実装すること。
・疑似乱数生成器初期化の有無を切り替えられるようにすること。
・生成される疑似乱数のエントロピーを切り替えられるようにすること。
・今回の評価においては、車載マイコン内蔵のハードウェアセキュリティ機能を用いないこと。
・ECU リセット時には、認証状態を維持しないこと。

本評価においては、上記セキュリティアクセス手順失敗時のペナルティは設定しない。ペナルティの例を以下に記す。

・セキュリティアクセス手順の連続実行における応答の遅延対応
・試行回数による応答変更や拒否対応

セキュリティアクセス手順をシーケンスとして図 3.2a.2-5 に記す。

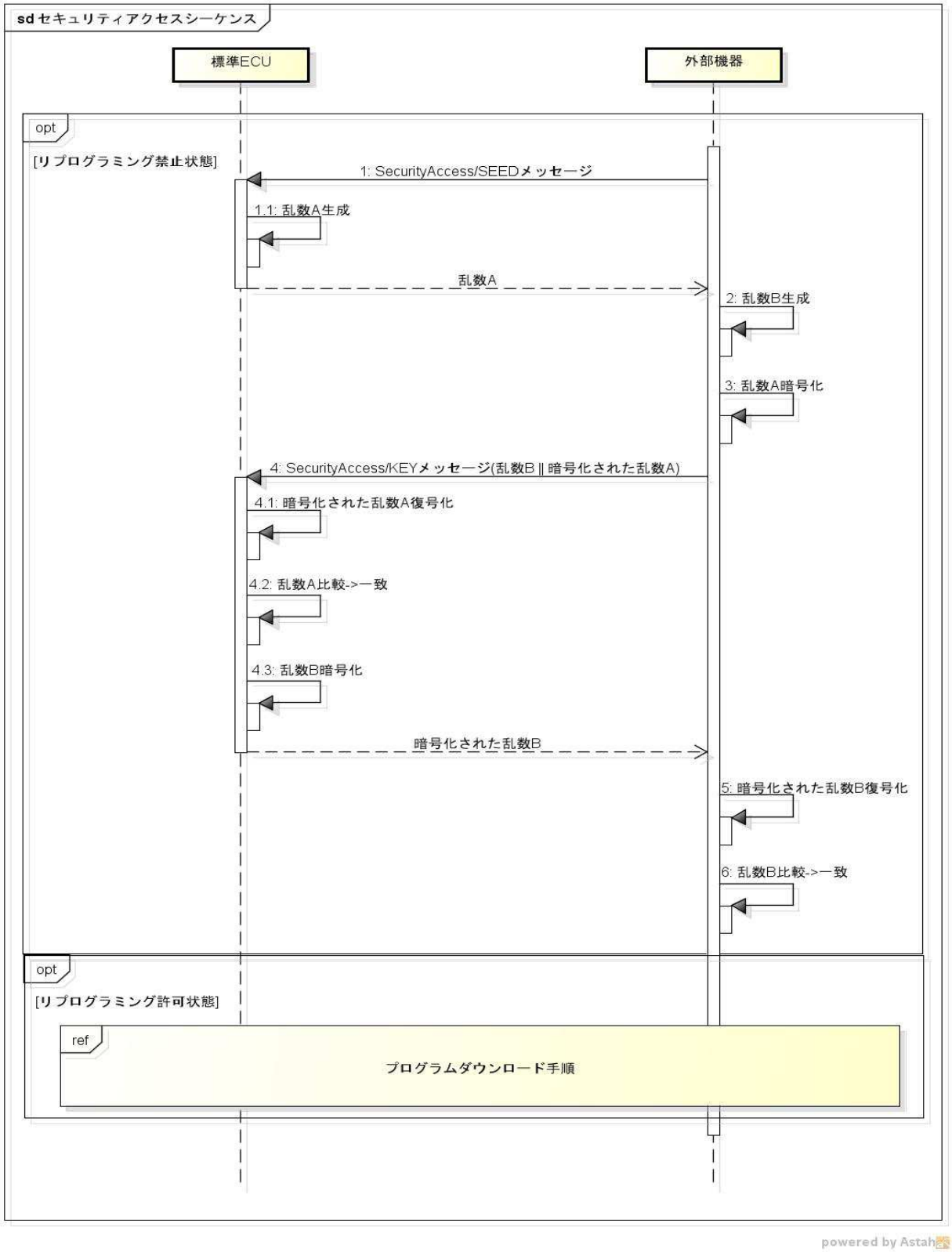


図 3.2a.2-5　セキュリティアクセス手順

④ デバッグインターフェース仕様

評価コンポーネントに対するデバッグインターフェース接続は、評価コンポーネントの開発およびデバッグ時に必須である。だが無条件で接続を許可する場合、評価コンポーネントへの物理的な攻撃（リバースエンジニアリングによる秘匿情報の暴露）が成功する危険性が大きくなる。

この危険性を小さくするために、デバッグインターフェース接続では、正規のプログラミング環境またはデバッグ環境であるかを認証することが必須となる。

デバッグインターフェース仕様に関する要件を以下に記す。

・正規のプログラミング環境またはデバッグ環境であることを認証すること。

・不正なプログラミング環境やデバッグ環境からの接続を拒否すること。

⑤ 脆弱性水準

本評価に対してのセキュリティ評価を行う観点から、評価コンポーネントには異なる脆弱性水準を設定する必要がある。

ここで、3.2a.1-(3)-②-(ⅳ)で定義した標準 ECU に必要な機能要件の一つを下記に示す。

FCS_RNG.1.2　TSF は、[割付: *定義された品質尺度*] を満たす[選択: *ビット*, *オクテットビット*, *数*[割付: *数値の形式*]]の乱数を提供しなければならない。

この機能要件に割り付けられる値が脆弱性水準となり、セキュリティアクセス仕様に対して設定した水準を表 3.2a.2-2 に記す。

表 3.2a.2-2　セキュリティアクセス脆弱性水準一覧

水準	乱数生成器初期化有無	生成乱数空間長(bit 長)
①	有り	128bit
②	有り	4bit (先頭 bit から 124bit までは 0 とする。)
③	無し	128bit
④	無し	4bit (先頭 bit から 124bit までは 0 とする。)

セキュリティ強度の観点から見ると①>②>③≒④の順位となる。

生成される乱数の空間長が十分に長い場合、生成乱数に関するセキュリティ強度は高まる。ただし強度を高める条件として「完全乱数に近い疑似乱数、つまり類推されにくい乱数を生成する」ことが条件となる。これは乱数生成パターン解析からのメッセージデータ構築とメッセージ再送攻撃を抑止もしくは遅延するために必須の事項となる。

上記水準の③と④の場合、生成される乱数は常に固定された値となる。これは乱数生成器の初期化が無いことによるものである。その結果メッセージ再送攻撃に極めて弱くなることが想定される。

デバッグインターフェースに対して設定する脆弱性水準を表 3.2a.2-3 に記す。

表 3.2a.2-3　デバッグインターフェース脆弱性水準一覧

水準	接続用パスワード有無
①	有り
②	無し

(4) ソフトウェア仕様

本事業で実装するセキュリティ評価向けソフトウェアの実装仕様について記述する。

① セキュリティ評価向けソフトウェア

本事業で求められる機能要件を実現するためのセキュリティ評価向けソフトウェアを構成する要素を表 3.2a.2-4 に記す。

表 3.2a.2-4　セキュリティ評価向けソフトウェア構成要素一覧

要素名	説明
Boot/Loader 部	マイコンリセット時に実行を開始するモジュール。マイコンおよび周辺ペリフェラルの初期化、および ISO14229-1 診断サービスモジュール起動またはアプリケーションの起動を行う。
Application 部	リプログラミング対象となるモジュール。本評価向けソフトウェアでは、一定周期で LED 点滅または点灯を行う機能（ON/OFF パターンは複数ある）を実装する。これは評価者（攻撃者）が、リプログラミングに成功したことを目視するための機能である。また CAN インターフェースによる診断メッセージの受信処理およびリプログラミングモジュールの起動処理も実装する。
ISO14229-1 診断サービスモジュール	ISO14229-1 リプログラミング手順を実現するためのモジュール。診断サービスに依存する処理は本モジュール内に実装する。
リプログラミングモジュール	リプログラミング手順のうち、プログラムダウンロードを実現するためのモジュール。FLASH メモリ書き換えに関する処理を行う。
セキュリティアクセスモジュール	セキュリティアクセス手順を実現するためのモジュール。認証処理および認証状態管理を行う。
セキュリティモジュール	セキュリティアクセス手順処理で必要となるアルゴリズムを実装するモジュール。アルゴリズムインターフェースを提供する。

上記構成要素のうち、ISO14229-1 診断サービスモジュール、リプログラミングモジュール、セキュリティアクセスモジュールおよびセキュリティモジュールに関しては、本章以降で仕様詳細を記述する。

セキュリティ評価ソフトウェアおよびApplication、外部機器の構成を図3.2a.2-6に記す。

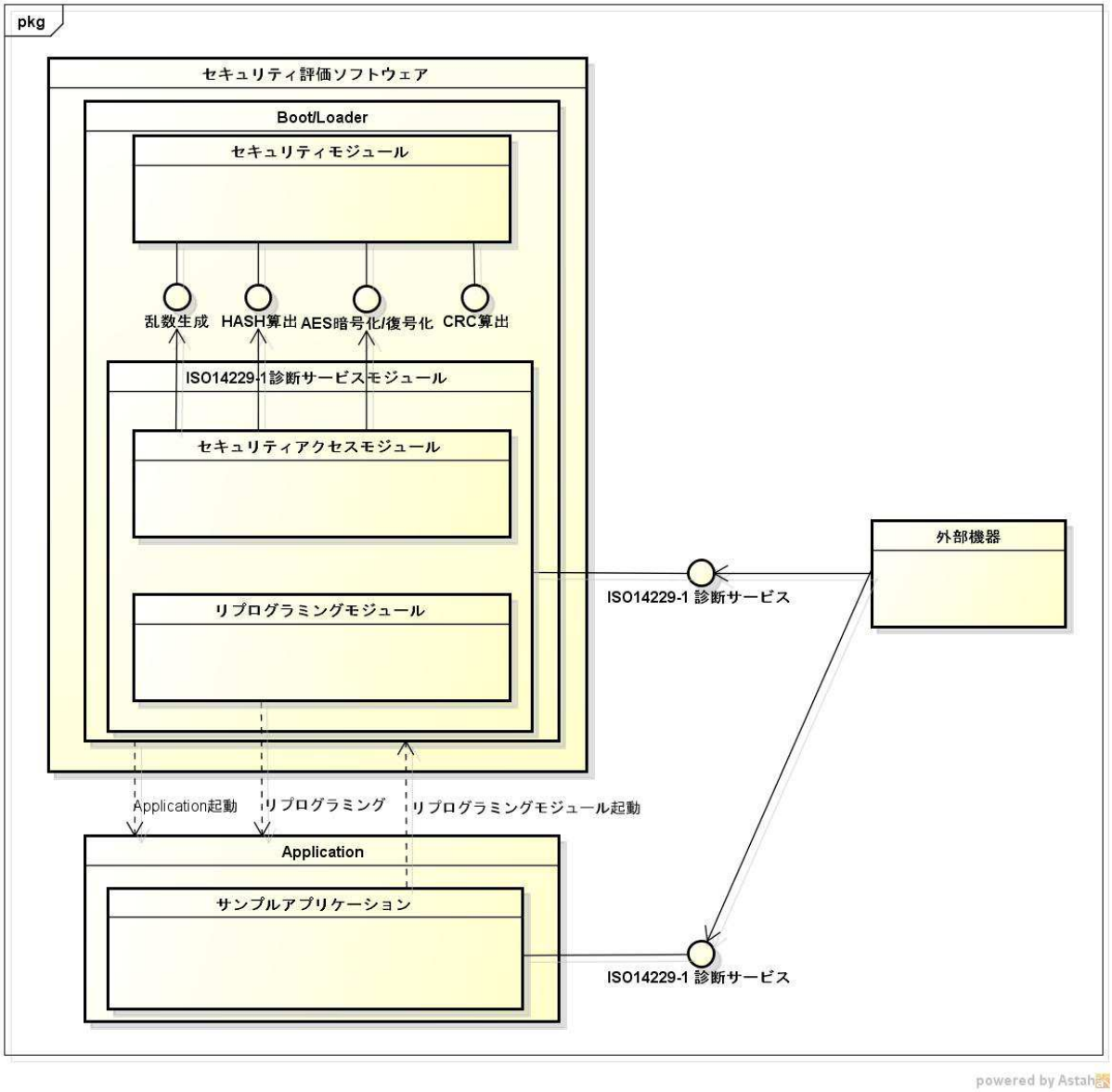


図 3.2a.2-6　セキュリティ評価向けソフトウェア構成

② ISO14229-1 診断サービスモジュール

ISO14229-1診断サービスモジュールは、ISO14229-1に規定されている診断サービスに依存する実装で構成される。実現する機能を以下に記す。

・診断要求メッセージの解析。
・セキュリティアクセスモジュールの実行。
・リプログラミングモジュールの実行。
・診断応答メッセージの構築と送信。
・その他診断サービスに関する実装。

本モジュールは、セキュリティアクセスモジュールとリプログラミングモジュールを内包する。処理する診断サービスに従って、いずれかのモジュールを実行する。

ISO14229-1 診断サービスモジュールを構成する要素を表 3.2a.2-5 に記す。

表 3.2a.2-5　ISO14229-1 診断サービスモジュールを構成要素一覧

要素名	説明
インターフェース部	本評価ソフトウェアの場合 Boot/Loader 部から呼び出されるためのインターフェースを実装する。
フレームワーク部	診断サービス機能を実現するための実装部。周期処理管理やプロセス実行などを実装する。
診断サービス部	ISO14229-1 に規定されたリプログラミング手順を実現するための診断サービス固有実装部。診断要求メッセージの解析と判定、リプログラミング動作として必要なプラットフォームインターフェースの呼び出しとプラットフォーム処理状態確認、診断応答メッセージの構築と送信を行う。
プラットフォーム部	Boot/Loader プラットフォームに実装するデバイスドライバとのインターフェース変換処理群。診断サービスとプラットフォーム間の仕様差分は本実装で解決する。

ISO14229-1 診断サービスモジュール構成を図 3.2a.2-7 に記す。

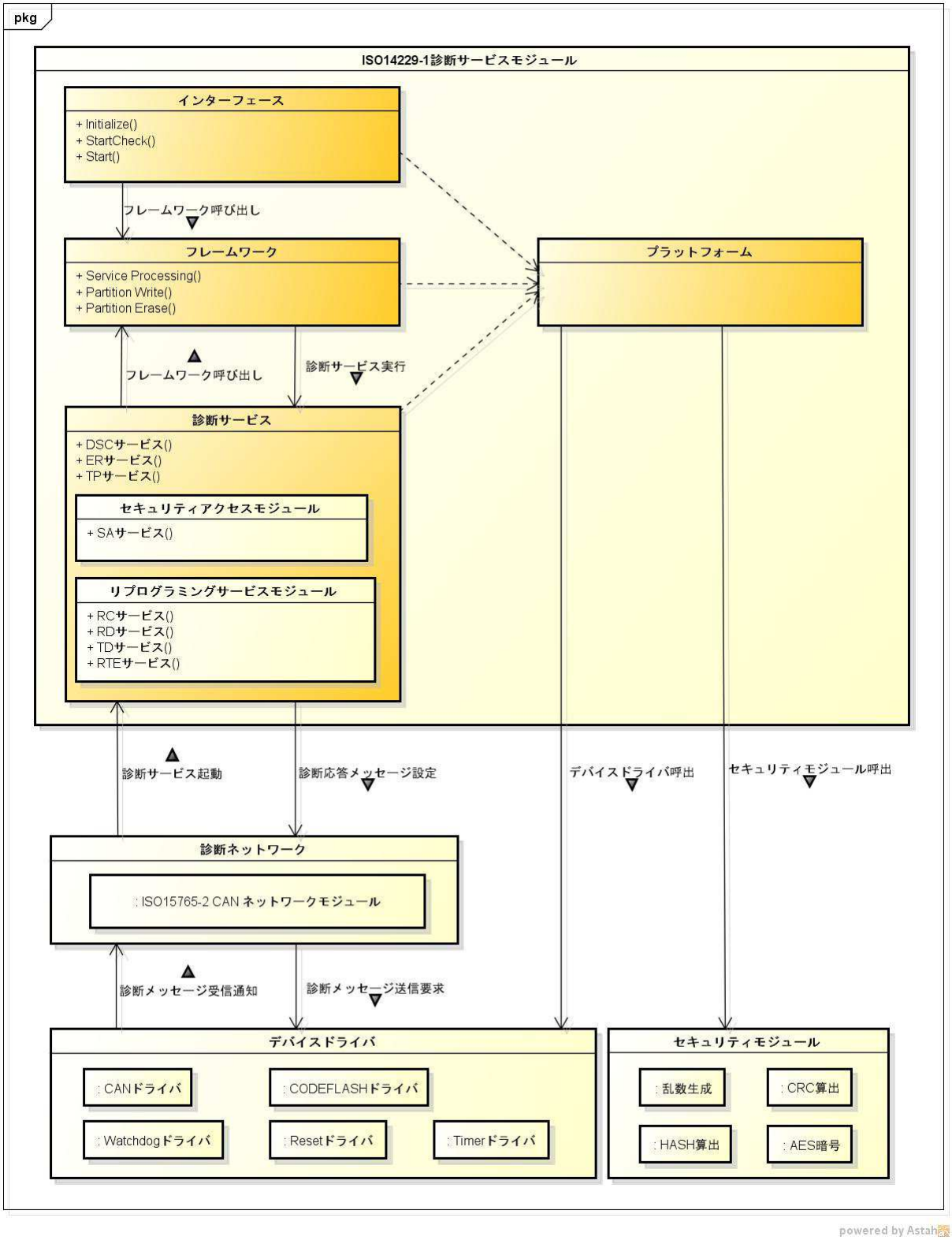


図 3.2a.2-7　ISO14229-1 診断サービスモジュール構成

③ リプログラミングモジュール

プログラムダウンロード機能を実現するリプログラミングモジュールを構成する要素を表 3.2a.2-6 に記す。

表 3.2a.2-6　リプログラミングモジュール構成要素一覧

要素名	説明
RC サービス実装	RoutineControl 診断サービス実装。本評価ソフトウェアの場合、FLASH メモリの消去を実行する。
RD サービス実装	RequestDownload 診断サービス実装。TransferData 診断サービスの実行に必要な手続きを行う。
TD サービス実装	TransferData 診断サービス実装。書き換え対象のデータを受信し、FLASH メモリに書き込む処理を実行する。
RTE サービス実装	RequestTransferData 診断サービス実装。FLASH メモリ書き込みすなわちプログラムダウンロードの終了処理を行う。

④ セキュリティアクセスモジュール

セキュリティアクセス手順を実現するセキュリティアクセスモジュールを構成する要素を表 3.2a.2-7 に記す。

表 3.2a.2-7　セキュリティアクセスモジュール構成要素一覧

要素名	説明
SA サービス実装	SecurityAccess 診断サービス実装。認証手続きに必要な SEED の生成と、外部機器から通知される KEY の認証処理を実行する。

単一の評価向けソフトウェアで複数の脆弱性水準を評価することを可能とするために、上記 SA サービス実装で処理する診断サービス要求メッセージ内のパラメータの Security Level（LEV）を設定する。異なる SecurityLevel を指定することにより、対象の脆弱性水準を切り替えることを可能とする。この実装は単一の物理環境上において、脆弱性水準が異なる ECU としての仮想環境を実現する。

脆弱性水準の切り替えを実現する診断サービス要求メッセージについては、[添付資料] パラメータ一覧に記載する。

※注:Security Level(LEV)は、ISO14229-1 に option 扱いで規定されているパラメータである。

⑤ セキュリティモジュール

セキュリティモジュールは、リプログラミング手順で使用する各種アルゴリズムを実装するモジュールである。このモジュールでは、診断サービスに対する依存実装は行わない。

セキュリティモジュールで実装する機能を表 3.2a.2-8 に記す。

表 3.2a.2-8　セキュリティモジュール実装機能一覧

機能名	説明
乱数生成	C 言語向けの標準乱数生成器実装を採用する。
HASH 算出	オープンソースである mbedTLS から SHA1 実装を抽出し実装する。
AES 暗号処理	オープンソースである mbedTLS から AES128 実装を抽出し実装する。
CRC 算出	CRC に関しては CCITT-16 で実装する。

⑥ デバッグインターフェース

本評価コンポーネントを開発、評価する際に使用するデバッガとマイコン評価ボードを接続するインターフェースは、LPD 接続方式を採用する。採用理由を以下に記す。

・評価用ボードに LPD 接続用コネクタが実装されている
・評価用ボードに JTAG 接続用コネクタが実装されていなかった
・本マイコンの標準状態では JTAG 接続設定が無効となっている

また本評価で使用するマイコンでは、マイコン内に搭載されている OCD（On Chip Debugger）に対してセキュリティパスワードを設定することが可能である。このセキュリティパスワード設定がマイコン（OCD）とデバッガで不一致となる場合、デバッガからの FLASH コード参照を防止することが可能となる。つまりリバースエンジニアリングのようなハードウェア攻撃を抑止できることになる。

セキュリティパスワードは、専用の FLASH メモリプログラマ（外部機器）から任意の値をマイコンに書き込むことで設定する。ただしセキュリティパスワード設定と確認手順、ハードウェア観点としての LPD 接続手順、マイコン内部の OCD へのアクセス方法などは、マイコンメーカが非公開としているデバイス仕様である。

デバッグインターフェースの設定を、以下に記す。

・JTAG 接続設定: 無効（JTAG 接続用専用端子設定=無効）
・LPD 接続設定: 有効（ソフトウェア設定項目は無し）
・セキュリティパスワード: 未設定（default 値: 0xFFFFFFFFFFFFFFFF）

(5) リプログラミング評価

標準 ECU コンポーネント上で動作するセキュリティ評価ソフトウェアが提供するリプログラミング機能に対する評価の観点を以下に記す。

・先に規定するリプログラミング手順を外部機器から実行し、リプログラミング対象で

ある標準 ECU コンポーネント内の Application 部プログラムが正常に更新されること。

・リプログラミング手順内のセキュリティアクセス手順において、設定した脆弱性水準毎に正常終了すなわち認証成功を確認できること。

リプログラミング評価環境構成を以下に記す。（図 3.2a.2-8）

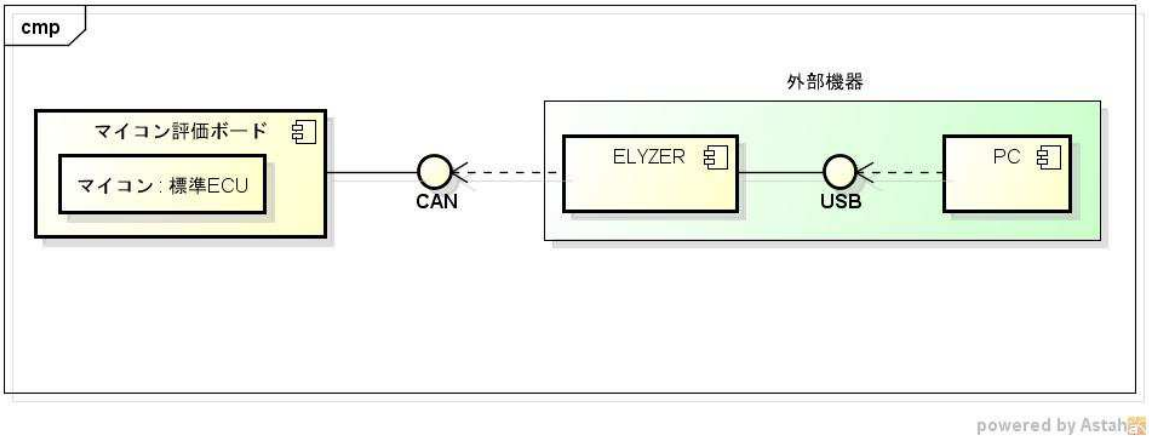


図 3.2a.2-8　リプログラミング評価環境構成

本評価では、外部機器としてイーソル株式会社製 ELYZER を使用する。ELYZER はハードウェアおよび PC 上で動作する専用アプリケーションで構成される。

ELYZER の接続例を以下に記す（図 3.2a.2-9）。

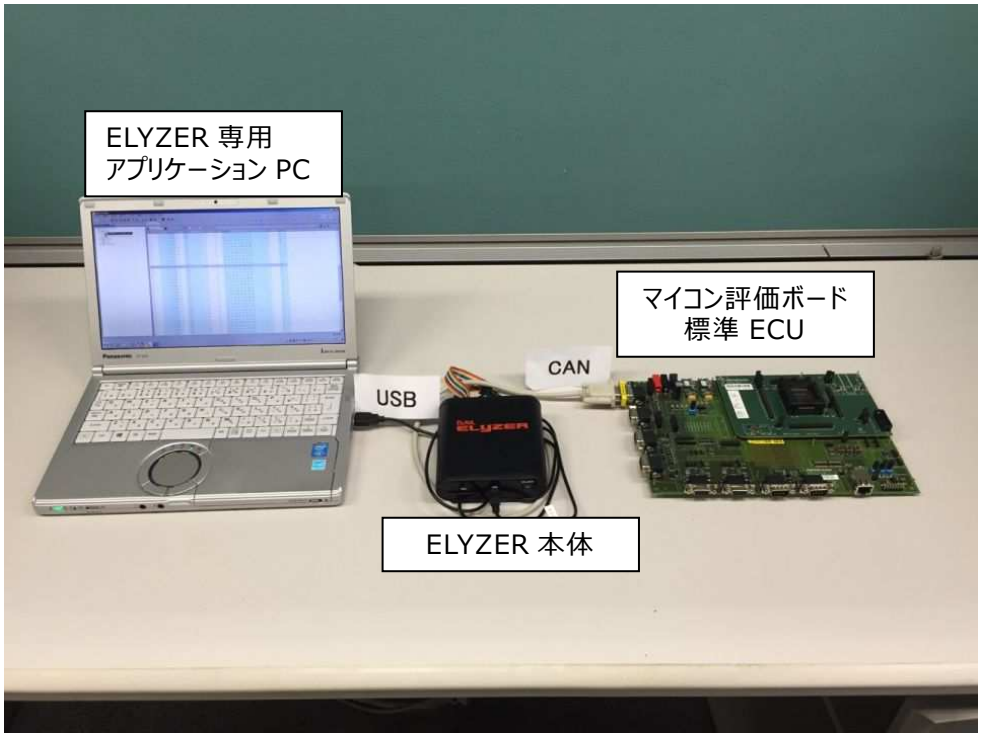


図 3.2a.2-9　ELYZER を用いた評価環境

ELYZER は「モデル」という概念で ECU とのシーケンスを実現する。モデルではリプログラミング手順に必要な診断メッセージの送受信を記述する。この記述中にはセキュリティアクセス時に必要な認証動作も存在する。モデルは生成専用 EXCEL ファイルでの自動生成または手動編集によって、専用のインタープリタ言語として記述する。

ELYZER 専用アプリケーションのスクリーンショットを図 3.2a.2-10 に記す。

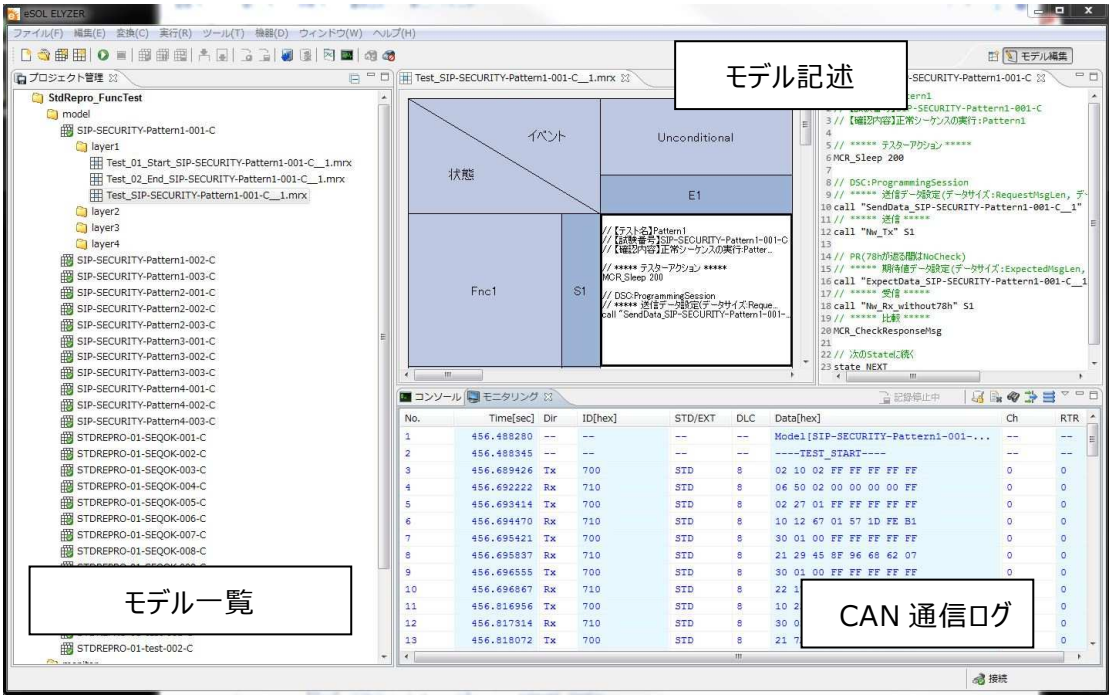


図 3.2a.2-10　ELYZER 専用アプリケーション

また ELYZER は CAN アナライザ（モニタ）としての機能も持つ。セキュリティアクセス手順の確認時には、ELYZER で取得した CAN 通信ログ（csv 形式ファイル）の出力内容を使用する。CAN 通信ログの例を図 3.2a.2-3 に記す。

	A	B	C	D	E	F	G	H	I	J
1	Date Mon Mar 07 17:13:13 2016									
2	Timestamps absolute									
3	Ch0 Bitrate 500Kbps TSEG1 6 TSEG2 3 SJW 1 BRP 1 BSP 1									
4	Ch1 Bitrate 500Kbps TSEG1 5 TSEG2 2 SJW 1 BRP 4 BSP 1									
5	No.	Time[sec]	Dir	ID[hex]	STD/EXT	DLC	Data[hex]	Ch	RTR	
6	1	28.984263	--	--	--	--	Model[SIP-SECURITY-Pattern1-001-C] start	--	--	
7	2	28.984328	--	--	--	--	----TEST_START----	--	--	
8	3	29.024558	RX	1800ffff	EXT	8	ff 23 a3 aa 88 88 86 ff	0	0	
9	4	29.185407	TX	700	STD	8	02 10 02 ff ff ff ff ff	0	0	
10	5	29.186219	RX	710	STD	8	06 50 02 00 00 00 00 ff	0	0	
11	6	29.187412	TX	700	STD	8	02 27 01 ff ff ff ff ff	0	0	
12	7	29.188464	RX	710	STD	8	10 12 67 01 21 0a c5 28	0	0	
13	8	29.189412	TX	700	STD	8	30 01 00 ff ff ff ff ff	0	0	
14	9	29.189832	RX	710	STD	8	21 7e 98 52 41 6f 31 03	0	0	
15	10	29.190550	TX	700	STD	8	30 01 00 ff ff ff ff ff	0	0	
16	11	29.190860	RX	710	STD	8	22 e6 30 f2 ed 27 ff ff	0	0	
17	12	29.240949	TX	700	STD	8	10 22 27 02 13 15 93 37	0	0	
18	13	29.241395	RX	710	STD	8	30 01 00 ff ff ff ff ff	0	0	
19	14	29.242149	TX	700	STD	8	21 06 94 a0 a4 79 12 8e	0	0	
20	15	29.242421	RX	710	STD	8	30 01 00 ff ff ff ff ff	0	0	
21	16	29.243180	TX	700	STD	8	22 0d 5f 8c a1 c2 6a 6a	0	0	
22	17	29.243495	RX	710	STD	8	30 01 00 ff ff ff ff ff	0	0	
23	18	29.244260					7e fb 30 bd 00 c6	0	0	
24	19	29.244676					00 ff ff ff ff ff	0	0	
25	20	29.245434					cb 56 7f 07 bc 9a	0	0	
26	21	29.249028					67 02 3d 50 67 83	0	0	
27	22	29.249973	TX	700	STD	8	30 01 00 ff ff ff ff ff	0	0	
28	23	29.250389	RX	710	STD	8	21 cc e4 34 0a a2 d0 c3	0	0	
29	24	29.251107	TX	700	STD	8	30 01 00 ff ff ff ff ff	0	0	
30	25	29.251417	RX	710	STD	8	22 a9 e1 4a 6c d9 ff ff	0	0	
31	26		TX	700	STD	8	10 0d 31 01 ff 00 44 00	0	0	
32	27		RX	710	STD	8	30 01 00 ff ff ff ff ff	0	0	
33	28		TX	700	STD	8	21 01 00 00 00 01 00 00	0	0	
34	29	29.413713	RX	710	STD	8	04 71 01 ff 00 ff ff ff	0	0	

図 3.2a.2-11　CAN 通信ログ例

3.2a.3　まとめ

自動走行時代のコンポーネントと車内システムに対して、セキュリティ対策の妥当性を定量的に確認可能な評価技術を開発すべく、平成 27 年度は、コンポーネントにおける評価方法・評価基準案の検討、評価対象となる標準 ECU の開発を行った。

コンポーネントの評価方法・評価基準案の検討では、セキュリティで先行する他業界のうち、主にスマートカード業界を参考に、ECU との類似点、相違点の整理を行い、標準 ECU に対する評価方法・評価基準の方針を示すことができた。

また、評価対象となる標準 ECU として、リプログラミング機能を搭載した ECU の開発を行った。

今後、コンポーネントに対する評価方法・評価基準のブラッシュアップを行うと共に、車内システムへと範囲を広げた評価方法・評価基準案の検討を進めていくことが重要である。

3.2a.4　付録

A. 用語

セキュリティ機能要件（SFR： Security Functional　Requirement）

セキュリティ機能を実現するための技術的な機能要件。ISO15408 では、ISO15408-2（Part2）に定義済みの要件カタログが用意されており、その中から目的とするセキュリティ機能を実現するために必要なセキュリティ要件を選択し、定義されている操作可能な部分をカスタマイズすることで、目的とするセキュリティ機能要件を完成させる。

セキュリティ保証要件（SAR： Security Assurance Requirement）

目的とするセキュリティ機能がどの程度信頼できるレベルで実現・達成できているかを評価・判断する上で必要とされる評価保証要件。

ISO15408 では、ISO15408-3（Part3）に、さまざまな視点からのセキュリティ保証要件が 7 つのクラスに分けて定義されており、目的とする評価保証レベルによって、セキュリティ保証要件の細かな内容が選択できるようになっている。

評価保証レベル（EAL： Evaluation Assurance Level）

セキュリティ保証要件に基づくセキュリティ評価を実施する上で、目的とする評価保証のレベルを定めたもの。ISO15408 では、EAL1（最小の評価保証レベル）から EAL7（最大の評価保証レベル）まで 7 つの評価保証レベルを予め定義している。

評価対象（TOE：Target of Evaluation）

セキュリティ評価の対象となる製品/システム。ISO15408 では、ガイダンスを伴うことがあるソフトウェア、ファームウェア、及び/またはハードウェアのセットとして定義される。

プロテクションプロファイル（PP：Protection Profile）

ある共通の製品種別/システム種別に対するセキュリティニーズについての実装に依存しないステートメント。一般に調達者や開発者グループによって、対象となる製品種別/システム種別に要求されるセキュリティ要件を定義するものとして作成される。

その文書構成・内容は、ISO15408-1（Part1）において定められている。本書では「実装非依存型のセキュリティ要件定義書」の用語を用いて、この概念を説明する場合がある。

セキュリティターゲット（ST：Security Target）

識別された特定の評価対象製品/システム（TOE）に対するセキュリティニーズについての実装に依存するステートメント。一般に評価対象の開発者によって、開発対象に要求されるセキュリティ要件を定義するものとして作成される。

その文書構成・内容は、ISO15408-1（Part1）において定められている。本書では「実装依存型のセキュリティ要件定義書」の用語を用いて、この概念を説明する場合がある。

プロテクションプロファイル評価（APE： Assurance for Protection Profile Evaluation）

ISO15408-3（Part3）で定められている 7 つセキュリティ保証要件の中のひとつ。

プロテクションプロファイル（PP）が信頼でき内部的に一貫していること、および、所定の内容を満たすものとして、適切に実装非依存型のセキュリティ要件定義を行っているかを評価するもの。

セキュリティターゲット評価（ASE： Assurance for Security Target Evaluation）

ISO15408-3（Part3）で定められている 7 つセキュリティ保証要件の中のひとつ。

セキュリティターゲット（ST）が信頼でき内部的に一貫していること、および、所定の内容を満たすものとして、適切に実装依存型のセキュリティ要件定義を行っているかを評価するもの。

開発評価（ADV： Assurance for Development Evaluation）

ISO15408-3（Part3）で定められている 7 つセキュリティ保証要件の中のひとつ。

実装依存型のセキュリティ要件定義（ST）で定義された開発対象に対するセキュリティ機能要件（SFR）が、設計開発・実装段階で、過不足なく正確に詳細化・具体化され、評価対象（TOE）に実装されていることを評価するもの。

テスト評価（ATE： Assurance for Tests Evaluation）

ISO15408-3（Part3）で定められている 7 つセキュリティ保証要件の中のひとつ。

実装依存型のセキュリティ要件定義（ST）に基づいて設計開発実装された評価対象（TOE）のセキュリティ機能が、利用者に配付される最終製品において、設計記述通りに動作することを確認評価するもの。

ガイダンス評価（AGD： Assurance for Guidance Documents Evaluation）

ISO15408-3（Part3）で定められている 7 つセキュリティ保証要件の中のひとつ。

評価対象（TOE）の利用者向けのガイダンスが、製品をセキュアに使用する上で必要なガイダンス情報を、誤解をまねくことなく提供していることを評価するもの。

ライフサイクル評価（ALC： Assurance for Life-Cycle Support Evaluation）

ISO15408-3（Part3）で定められている 7 つセキュリティ保証要件の中のひとつ。

設計開発・製造・出荷・運用の各プロセスにおいて、評価対象（TOE）の意図されたセキュリティ機能が、適切な管理統制の下で、損なわれることなく正確に実現・確保されていることを評価するもの。

脆弱性評価（AVA： Assurance for Vulnerability Assessment）

ISO15408-3（Part3）で定められている 7 つセキュリティ保証要件の中のひとつ。

評価対象（TOE）の設計開発または運用で生じる悪用可能な脆弱性の可能性を評価価するもの。

日本語翻訳版では「脆弱性評定」の訳語があてられているが、厳密に日本語翻訳版に従う場合を除き、本書では「脆弱性評価」の訳語を使用している。

セキュリティ課題定義（SPD：Security Problem Definition）

ISO15408-1（Part1）で定められているセキュリティ要件定義に必須とされる記述項目のひとつ。評価対象（TOE）が対処する必要のあるセキュリティ上の課題を定義するもの。

この課題定義は、1) 環境に関する前提条件、2) 資産に対する脅威、3) 組織のセキュリティ方針の観点から記述することが求められている。

評価対象（TOE）のセキュリティ機能を定義・設計する上での起点となるものであり、セキュリティ要件定義の最も重要な部分である。

セキュリティ対策方針（OBJ： Security Objective）

ISO15408-1（Part1）で定められているセキュリティ要件定義に必須とされる記述項目のひとつ。評価対象（TOE）が対処する必要のあるセキュリティ上の課題として定義された「セキュリティ課題定義（SPD)」に対する対応方法・解決策を「セキュリティ対策方針」として簡潔に記述するもの。

この解決策（対策方針）は、1) 評価対象（TOE）自身に実装される技術的なセキュリティ対策に関する方針、2) 評価対象（TOE）の運用環境に対する技術的・手続き的なセキュリティ対策に関する方針の観点から記述することが求められている。

前者は「評価対象（TOE）のセキュリティ対策方針」と呼ばれ、評価対象（TOE）に実装される「セキュリティ機能要件」の起点となる。即ち、この「評価対象（TOE）のセキュリティ対策方針」を満たす「セキュリティ機能要件」を導出・定義することが、セキュリティ要件定義の中核となる。

後者は、「運用環境のセキュリティ対策方針」と呼ばれ、評価対象（TOE）が設置される運用環境（IT 環境、または、IT 環境以外の人的・手続き的・物理環境的な運用・管理）によって実現されるものとして定義される。

B. 参考資料

【ISO15408/ISO18045】

[1] ISO/IEC 15408-1, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, 3rd edition, 2009-12-15 (corrected 2014-01-15)

[2] ISO/IEC 15408-2, Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components, 3rd edition, 2008-08-15 (corrected 2011-06-01)

[3] ISO/IEC 15408-3, Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components, 3rd edition, 2008-08-15 (corrected 2011-06-01)

[4] ISO/IEC 18045, Information technology — Security techniques — Methodology for IT security evaluation, 2nd edition, 2008-08-15 (corrected 2014-01-15)

【CC/CEM】

[5] Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4, Part 1: Introduction and general model, September 2012, CCMB-2012-09-001

[6] Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4, Part 2: Security functional components, September 2012, CCMB-2012-09-002

[7] Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4, Part 3: Security assurance components, September 2012, CCMB-2012-09-003

[8] Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4, Evaluation methodology, September 2012, CCMB-2012-09-004

【CCRA/SOGIS】

[9] Common Criteria Supporting Document, Mandatory Technical Document, Application of Attack Potential to Smartcards, May 2013, Version 2.9, CCDB-2013-05-002

[10] Joint Interpretation Library, Application of Attack Potential to Hardware Devices with Security Boxes, December 2015, Version 2.0（for trial use）

[11] Joint Interpretation Library, Application of Attack Potential to POIs, June 2011, Version 1.0（for trial use）

【CC/CEM/CCRA 日本語翻訳版】（独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室）

[12] 情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1, 改訂第 4 版, パート 1: 概説と一般モデル, 2012 年 9 月, CCMB-2012-09-001, 翻訳第 1.0 版

[13] 情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1, 改訂第 4 版, パート 2: セキュリティ機能コンポーネント, 2012 年 9 月, CCMB-2012-09-002, 翻訳第 1.0 版
[14] 情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1, 改訂第 4 版, パート 3: セキュリティ保証コンポーネント, 2012 年 9 月, CCMB-2012-09-003, 翻訳第 1.0 版
[15] 情報技術セキュリティ評価のための共通方法 バージョン 3.1, 改訂第 4 版, 評価方法, 2012 年 9 月, CCMB-2012-09-004, 翻訳第 1.0 版
[16] Common Criteria サポート文書, 必須技術文書, スマートカードへの攻撃能力の適用, 2013 年 5 月, バージョン 2.9, CCDB-2013-05-002, 翻訳第 1.0 版

【ISO19790/ISO24759（FIPS140-2）、ISO17825】
[17] ISO/IEC 19790, Information technology — Security techniques — Security requiremnts for cryptographic modules, 2nd edition, 2012-08-15 (corrected 2015-12-15)
[18] ISO/IEC 24759, Information technology — Security techniques — Test requiremnts for cryptographic modules, 2nd edition, 2014-02-01 (corrected 2015-12-15)
[19] ISO/IEC 17825, Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules, 1st edition, 2016-01-15

【CMVP/FIPS140-2 日本語翻訳版】（独立行政法人 情報処理推進機構 、独立行政法人 情報通信研究機構）
[20] 暗号モジュール評価基準第 0.1 版, 平成 17 年 3 月
[21] 暗号モジュール試験基準第 0.1 版, 平成 17 年 3 月

C. 評価対象（コンポーネント）資料

・マイコン評価ボード LED 点灯パターン一覧

評価向け標準 ECU の動作状態は LED の点灯、消灯パターンで目視することが可能である。各標準 ECU の動作状態と対応する LED 点灯、消灯パターンを以下に記す。

表 3.2a.4-1　マイコン評価ボード LED 点灯パターン一覧

状態	LED 点灯パターン
リプログラミングモジュール動作中またはリプログラミング手順開始待ち。	単一の LED のみ、約 500ms 周期で点滅する。
サンプルアプリケーション 1 実行中。	LED1 と 2 が点灯。3 と 4 が消灯。※注
サンプルアプリケーション 2 実行中。	LED1 と 2 が消灯。3 と 4 が点灯。※注

※注: 使用するマイコン評価ボードによって、点灯する LED の組み合わせが異なる場合がある。

・セキュリティアクセス脆弱性水準切り替えパラメータ一覧

評価ソフトウェアのセキュリティアクセス脆弱性水準を切り替えるためのパラメータは要求メッセージ送信側で設定する。本評価の場合、要求メッセージ送信側は外部機器ツールとなる。各脆弱性水準に対応したセキュリティアクセス要求メッセージを以下に記す。

表 3.2a.4-2　セキュリティアクセス脆弱性水準切り替えパラメータ一覧

セキュリティアクセス 脆弱性水準	SecurityAccess/SEED 要求メッセージ （図 3.2a.2-参照/ メッセージ長 2byte: 16 進）	SecurityAccess/KEY 要求メッセージ （図 3.2a.2-参照/ メッセージ長 34byte: 16 進）
生成乱数空間長 128bit / 乱数生成器初期化有り	27 01	27 02 xx xx xx… (xx: 認証データ 32byte)
生成乱数空間長 4bit （先頭から 124bit は 0）/ 乱数生成器初期化有り	27 15	27 16 xx xx xx… (xx: 認証データ 32byte)
生成乱数空間長 128bit / 乱数生成器初期化無し	27 25	27 26 xx xx xx… (xx: 認証データ 32byte)
生成乱数空間長 4bit （先頭から 124bit は 0） / 乱数生成器初期化無し	27 35	27 36 xx xx xx… (xx: 認証データ 32byte)

・セキュリティ評価向け eSOL ELYZER モデル一覧

セキュリティ評価向けに作成した eSOL ELYZER モデルを以下に記す。

表 3.2a.4-3　セキュリティ評価向け eSOL ELYZER モデル一覧

対応する脆弱性水準	モデル名	実行するリプログラミング手順
生成乱数空間長 128bit / 乱数生成器初期化有り	SIP-SECURITY-Pattern1-001-C	リプログラミング正常手順 (DSC→SA SEED→SA KEY → RC → RD → TD → RTE → ER)
	SIP-SECURITY-Pattern1-002-C	セキュリティアクセスループ① (DSC→SA SEED→SA KEY)
	SIP-SECURITY-Pattern1-003-C	セキュリティアクセスループ② (DSC→SA SEED→SA SEED)
生成乱数空間長 4bit (先頭から 124bit は 0) / 乱数生成器初期化有り	SIP-SECURITY-Pattern2-001-C	リプログラミング正常手順 (DSC→SA SEED→SA KEY → RC → RD → TD → RTE → ER)
	SIP-SECURITY-Pattern2-002-C	セキュリティアクセスループ① (DSC→SA SEED→SA KEY)
	SIP-SECURITY-Pattern2-003-C	セキュリティアクセスループ② (DSC→SA SEED→SA SEED)
生成乱数空間長 128bit / 乱数生成器初期化無し	SIP-SECURITY-Pattern3-001-C	リプログラミング正常手順 (DSC→SA SEED→SA KEY → RC → RD → TD → RTE → ER)
	SIP-SECURITY-Pattern3-002-C	セキュリティアクセスループ① (DSC→SA SEED→SA KEY)
	SIP-SECURITY-Pattern3-003-C	セキュリティアクセスループ② (DSC→SA SEED→SA SEED)
生成乱数空間長 4bit (先頭から 124bit は 0) / 乱数生成器初期化無し	SIP-SECURITY-Pattern4-001-C	リプログラミング正常手順 (DSC→SA SEED→SA KEY → RC → RD → TD → RTE → ER)
	SIP-SECURITY-Pattern4-002-C	セキュリティアクセスループ① (DSC→SA SEED→SA KEY)
	SIP-SECURITY-Pattern4-003-C	セキュリティアクセスループ② (DSC→SA SEED→SA SEED)

［開発環境］

・ルネサス エレクトロニクス株式会社製 RH850/F1L マイコン
・ルネサス エレクトロニクス株式会社製 CS+（統合開発環境/R850 コンパイラ等含む）
・ルネサス エレクトロニクス株式会社製 CPU 評価ボード
・テセラ・テクノロジー株式会社製 CPU 評価ボード
・イーソル株式会社製 ELYZER （CAN アナライザ/リプログラミングシーケンス実行環境）
・Microsoft 社製 EXCEL （ELYZER 実行 model 生成用）

3.2b　車外連携システム・車両レベルにおける評価技術の検討

自動走行を想定した車外連携システムと車両全体に対して、ICT におけるサイバー攻撃の事例などを元に、サイバーセキュリティ対策を行うべきポイントを抽出し、そこに適用される対策技術の評価指針・指標について調査・検討を行った。

これに先立ち、サイバーセキュリティ情報の取り扱いについて、先行している組織の事例調査を行い、プロジェクト内でサイバーセキュリティ情報を受け取り、共有する際の課題についても検討を行った。

なお、特に断りが無い限り，本項での“セキュリティ”とはサイバーセキュリティや情報セキュリティを意味する。

3.2b.1　他業界におけるセキュリティ情報の共有状況・管理方法の調査

サイバー攻撃の事例は機微な情報であるため、単純に業界内の関連組織から収集することや、その組織間で共有することは難しい。このため、先行している事例を参考に取り組みを考える必要がある。

本事業において、先行していると思われる他業界でどのように扱われているかの事例調査を実施し、セキュリティ情報の共有を行う上での課題を検討した。

(1) わが国におけるセキュリティ情報の共有・管理の全体概要

まず、わが国におけるセキュリティ情報の共有・管理がどのように行われているかについて調査を行った。

① 重要インフラ毎のセプターの整備

内閣官房情報セキュリティセンター（NISC、2015 年 1 月 9 日に内閣サイバーセキュリティセンターに改組）の IT 戦略本部のもとに設置された情報セキュリティ政策会議において、2005 年 12 月 13 日、「重要インフラの情報セキュリティ対策に係る行動計画」（以下、「第 1 次行動計画」）が策定された。

この中で重要インフラとは、「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活および社会経済活動の基盤であり、その機能が停止、低下または利用不能な状態に陥った場合に、わが国の国民生活または社会経済活動に多大なる影響を及ぼすおそれが生じるもの」と定義されている。

第 1 次行動計画において、官民の緊密な連携のもと、情報システムの障害が国民生活や社会経済活動に重要な影響を及ぼさないように重要インフラに対する情報セキュリティ対策の強化として次の 4 つの柱からなる施策が設定されている。

ア）安全基準等の整備および浸透
イ）情報共有体制の強化

ウ）相互依存性解析
エ）分野別横断的な演習

このうち、「イ）情報共有体制の強化」における施策として、重要インフラ分野毎にセプターを整備することが決定された（表 3.2b.1-1）。セプター（CEPTOAR）は、Capability for Engineering of Protection, Technical Operation, Analysis and Response の頭文字から命名されたもので、重要インフラ事業者等の情報共有・分析機能および当該機能を担う組織を指す呼称である。

表 3.2b.1-1　重要インフラ分野とセプター

重要インフラ分野	事業の範囲	セプターの名称		事務局
情報通信	電気通信	T-CEPTOAR		(一財) 日本データ通信協会テレコム・アイザック推進会議
	放送	ケーブルテレビCEPTOAR		(一社) 日本ケーブルテレビ連盟
		放送CEPTOAR		(一社) 日本民間放送連盟
金融	銀行等	金融CEPTOAR連絡協議会	銀行等CEPTOAR	(一社) 全国銀行協会　事務システム部
	証券		証券CEPTOAR	日本証券業協会　IT統括部
	生命保険		生命保険CEPTOAR	(一社) 生命保険協会　総務部組織法務グループ
	損害保険		損害保険CEPTOAR	(一社) 日本損害保険協会　IT推進部共同システム開発室
航空	航空	航空分野におけるCEPTOAR		国土交通省　航空局　安全企画課
鉄道	鉄道	鉄道CEPTOAR		国土交通省　鉄道局　総務課　危機管理室
電力	電力	電力CEPTOAR		電気事業連合会　情報通信部
ガス	ガス	ガスCEPTOAR		(一社) 日本ガス協会　技術部
政府・行政サービス	政府公共団体	自治体CEPTOAR		地方公共団体情報システム機構　情報化支援戦略部
医療	医療	医療CEPTOAR		厚生労働省　医政局　研究開発振興課　医療技術情報推進室
水道	水道	水道CEPTOAR		(公社) 日本水道協会　総務部総務課
物流	物流	物流CEPTOAR		(一社) 日本物流団体連合会
化学	化学	化学CEPTOAR		石油化学工業協会
クレジット	クレジット	クレジットCEPTOAR		(一社) 日本クレジット協会
石油	石油	石油CEPTOAR		石油連盟

現在、重要インフラ CEPTOAR は、表 3.2b.1-2 に示す 13 分野、18 セプターから構成されている。13 分野、18 セプターを俯瞰した特徴として次の 3 点を挙げることができる。

ア）多くは、事務局が業界団体であるが、省庁が事務局となっているセプターが 3 つ
（航空、鉄道：国土交通省、医療：厚生労働省）
→これらは、セプターを構成する事業者が比較的小規模で、行政との連携が密な分野といえる。
イ）構成員が 1,000 以上のセプターが 3 つ（銀行等、自治体、水道）
→多くの構成員を持つことから、情報共有体制の重要度が高い分野といえる。
ウ）2014 年に新たに加入したセプターが 3 つ（化学、クレジット、石油）
→東日本大震災の経験から重要度が改めて再認識された分野といえる。

表 3.2b.1-2　重要インフラ分野別概要（セプター特性把握マップ）

2015年3月末現在

重要インフラ分野	情報通信			金融				航空	鉄道	電力	ガス	政府・行政サービス	医療	水道	物流	化学	クレジット	石油
事業の範囲	電気通信		放送	銀行等	証券	生命保険	損害保険	航空	鉄道	電力	ガス	政府公共団体	医療	水道	物流	化学	クレジット	石油
名称	T-CEPTOAR	ケーブルテレビCEPTOAR	放送CEPTOAR	金融CEPTOAR連絡協議会 銀行等CEPTOAR	証券CEPTOAR	生命保険CEPTOAR	損害保険CEPTOAR	航空分野におけるCEPTOAR	鉄道CEPTAOR	電力CEPTOAR	GAS CEPTOAR	自治体CEPTOAR	医療CEPTOAR	水道CEPTOAR	物流CEPTOAR	化学CEPTOAR	クレジットCEPTOAR	石油CEPTOAR
事務局	(一財)日本データ通信協会 テレコム・アイザック推進会議	(一社)日本ケーブルテレビ連盟	(一社)日本民間放送連盟	(一社)全国銀行協会 事務システム部	日本証券業協会 ＩＴ統括部	(一社)生命保険協会 総務部組織法務グループ	(一社)日本損害保険協会 ＩＴ推進部共同システム開発室	国土交通省 航空局 安全企画課	国土交通省 鉄道局 総務課 危機管理室	電気事業連合会 情報通信部	(一社)日本ガス協会 技術部	地方公共団体情報システム機構 情報化支援戦略部	厚生労働省 医政局 研究開発振興課 医療技術情報推進室	(公社)日本水道協会 総務部総務課	(一社)日本物流団体連合会	石油化学工業協会	(一社)日本クレジット協会	石油連盟
構成員（内訳）	２６社・団体 （固定系のネットワークインフラを設置する電気通信事業者、アクセス系の電気通信事業者、ISP事業者、携帯電話事業者等）	310社 ((一社)日本ケーブルテレビ連盟の正会員ケーブルテレビ事業者)	１９４社・団体 （日本放送協会、地上系民間基幹放送事業者、(一社)日本民間放送連盟）	1,487社 （銀行、信用金庫、信用組合、労金、商工中金、農協等）	254社７機関 （証券会社、取引所等証券関係機関）	42社 ((一社)生命保険協会の定款に定める社員および特別会員)	29社（オブザーバ３社含む） ((一社)日本損害保険協会 情報システム委員会参加会社)	２グループ３機関 （航空運送事業者、定期航空協会、官庁［航空局、気象庁］）	２２社１団体１機関 （鉄道事業者22社、１団体、官庁［鉄道局］）	１２社２機関 （一般電気事業者、日本原電(株)、電源開発(株)、電気事業連合会、電力中央研究所）	１０社 （主要なガス事業者10社）	４７都道府県1,741市区町村	１グループ６機関 （医療機関、(公社)日本医師会、四病院団体協議会（(一社)日本医療法人協会、(公社)日本精神科病院協会、(一社)日本病院会、(公社)全日本病院協会）、保健医療福祉情報システム工業会）	８水道事業体 （会員水道事業体のうち会長都市並びに地方支部長都市）[補足]障害の内容によって、構成員を選し、全国の日本水道協会の会員水道事業体(1,356事業体)へ情報を提供	６団体１６社 （日本物流団体連合会、日本船主協会、日本内航海運組合総連合会、日本港運協会、日本倉庫協会、全日本トラック協会及び主要な物流事業者16社）	８社 （主要な石油化学事業者）	18社 （主要なクレジットカード会社等）	15社・グループ （主要な石油精製・元売会社）
緊急窓口	2007年4月運用開始	2012年12月運用開始	2007年4月運用開始										2008年4月運用開始			2015年1月運用開始	2014年4月運用開始	2014年12月運用開始
情報の取扱ルール	2007年1月制定	2012年11月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2006年9月制定	2007年3月制定	2007年3月制定	2008年3月制定	2008年3月制定	2008年3月制定	2014年12月制定	2014年４月制定	2014年１２月制定
情報と連絡手段	障害事例 情報等 メール、電話	障害事例 情報等 メール、電話	障害事例 情報等 メール、電話、FAX、WEB	障害事例 情報等 メール、電話、ＷＥＢ	障害事例 情報等 メール、電話、FAX、WEB	障害事例 情報等 メール、電話、携帯	障害事例 情報等 メール、電話	障害事例 情報等 メール、電話	障害事例 情報等 メール、電話	脆弱性に関する情報等 メール、電話、携帯、FAX、電子会議室、TV会議、会議体	障害事例 情報等 メール、電話、携帯、AX	障害事例 情報等 メール、電話、WEB	障害事例 情報等 メール、電話、携帯、衛星電話、FAX	障害事例 情報等 メール、電話、携帯、衛星電話、FAX	障害事例 情報等 メール、電話	障害事例 情報等 メール、電話、携帯電話	障害事例 情報等 メール、電話	障害事例 情報等 メール、電話

（注）　本マップは、各セプターの自主的な整備状況を把握し、マップとして取り纏めたもの。

（出典　NISC　「2014年度セプターの活動状況の把握について」2015年3月）

② NISC と重要インフラ事業者等との情報共有件数と内訳

表 3.2b.1-3 は、第 2 次行動計画および第 3 次行動計画のうちの 2014 年度分に基づき NISC との間で行われた情報共有の件数の推移を示し、表 3.2b.1-4 は事象別の内訳を示す。。

表 3.2b.1-3　NISC と重要インフラ事業者等および関係省庁・関係機関との間で行われた情報共有の件数

年度	2009	2010	2011	2012	2013	2014
重要インフラ事業者等から内閣官房への情報連絡件数	128件	169件	43件	110件	153件	124件
関係省庁・関係機関から内閣官房への情報共有件数	294件	137件	400件	50件	55件	27件
内閣官房からの情報提供件数	13件	48件	34件	38件	49件	38件

（出典　重要インフラ専門調査会 第 2 回会合 参考資料 2
「2014 年度の情報連絡等について」（2015 年 7 月 17 日））

表 3.2b.1-4　NISC と重要インフラ事業者等及び関係省庁・関係機関との間で行われた情報共有の事象別の内訳

事象の類型		事象の例	2014年度
未発生の事象		予兆・ヒヤリハット	9件
発生した事象	機密性を脅かす事象	情報の漏えい	9件
	完全性を脅かす事象	情報の破壊	14件
	可用性を脅かす事象	システム等の利用困難	38件
	上記につながる事象	マルウェア等の感染	27件
		不正コード等の実行	3件
		システム等への侵入	12件
		その他	12件

（出典　重要インフラ専門調査会 第 2 回会合 参考資料 2
「2014 年度の情報連絡等について」（2015 年 7 月 17 日））

これらの数値から業界団体として年間に扱う可能性があるセキュリティ情報のおおよその規模・件数を知ることができる。

(2) 各業界におけるサイバーセキュリティ情報の共有・管理方法

次に各団体においてサイバーセキュリティ情報がどのように扱われているかについて公開されている情報と、一部では協力いただける範囲での事務局へのヒアリングを含む調査を行った。

調査した対象は情報セキュリティの意味合いが、より深いと考えられる「情報通信分野」と「金融分野」，参加団体の件数が多い「政府・行政サービス分野」，そしてこれらのセプター間を横串にする「業界横断の組織」である。

以下に調査結果を報告する。

① 情報通信分野

情報通信分野における重要インフラ事業者には、電気通信事業者、地上基幹放送事業者、ケーブルテレビ事業者があり、それぞれ、T-CEPTOAR、放送 CEPTOAR、ケーブルテレビ CEPTOAR を構成している。

(ｉ) 電気通信業界（T-CEPTOAR）

一般財団法人日本データ通信協会テレコム・アイザック推進会議を事務局とする T-CEPTOAR は、固定系のネットワークインフラを設置する電気通信事業者、アクセス系の電気通信事業者、ISP 事業者、携帯電話事業者等 26 社・団体を構成員とする組織である（2015 年 3 月末現在）。

電気通信分野の情報共有・分析機能として、2007 年 1 月に情報取り扱いルールを制定し、同 4 月より運用を開始している。障害事例情報等をメールや電話により連絡している。

T-CEPTOAR では、T-CEPTOAR 運営委員会が設置され、以下の SG（サブグループ）が設置されている。

ア）固定系ネットワークインフラを設置する電気通信事業者等から構成される：SG1
イ）アクセス系電気通信事業者等から構成される：SG2
ウ）ISP 事業者等から構成される：SG3
エ）携帯電話事業者等から構成される：SG4

T-CEPTOAR には、次の 3 つの役割（機能）がある[1]。

ア）電気通信事業における IT 障害[2]の未然防止、IT 障害の拡大防止・迅速な復旧、IT 障害の要因等の分析・検証による再発防止のための構成員間の情報共有および連携
イ）政府、他のセプター等から提供される情報の構成員への連絡
ウ）政府、他のセプター等から提供される情報に関連する事項の構成員間の情報共有

2013 年度には、以下のような活動を実施している。

ア）SG によっては月に 1 度の頻度で月例会合を開催。SG 内で大規模障害時を想定した携帯電話／携帯メール等による休日情報伝達訓練を実施。
イ）T-CEPTOAR 構成員であるテレコム・アイザック推進会議主催のサイバー攻撃対応演習を他セプター構成員の参加を得て実施。
ウ）分野横断的演習に参加。セプター訓練に参加。
エ）サイバーセキュリティ関連セミナー等の T-CEPTOAR 及び他セプターへ情報展開・共有。
オ）セプターカウンシルにおけるＷＧ活動に参加。
カ）セプターカウンシルの HP レスポンス観測活動について異常検知におけるアラートメールの発出機能等の追加。

T-CEPTOAR の事務局であるテレコム・アイザック推進会議への聞き取り調査を行った。その結果、及び前述の公開情報を踏まえ、情報共有・管理のあり方を検討すると、以下のように考えることができる。

ア）テレコム・アイザック推進会議のメンバーは、基本的に通信事業者である。
サイバーセキュリティ上の問題となり得る脆弱性等を、通信機器のユーザーである通信事業者が見つけるのは必ずしも容易ではない。その観点から、通信機器メーカーなどが、機器提供者として、自社の製品の脆弱性を発見した場合に、それを通信事業者に、情報共有することは重要となる。
イ）その中で、テレコム・アイザック推進会議の役割は、通信事業者間で、こうしたセキュリティ情報を円滑に共有できるようにする仕組みを整えること、その土壌づくりのために、情報共有の重要性を訴えていくところにある。
ウ）セキュリティ情報の共有の実効性を上げるという意味で大切なことは、相互に信頼のおける人的ネットワークである。信頼できる人、関係ができている人にでないと、情報を流すということにはなりにくい。流れてきた情報も、信頼できる人

[1] https://www.telecom-isac.jp/public/t-ceptoar.html
[2] 事業において発生する障害（サービスの停止や機能の低下等）のうち、IT の機能不全が引き起こすもの（「第 1 次行動計画」より）

からのものでないと、受け取り方に迷うことになる。

エ）例えば、各 ISP には通信に関するトラブル全般の処理に対応するセクションがある。各社のトラブル対応のセクションの担当者間にはテレコム・アイザックの下で、ネットワークができており、フェース・トゥ・フェースでオン／オフなど様々な会合を持っている。このような専門家同士の信頼で、普通は話さないことも話すような雰囲気ができている。こうした個人的なつながりが、セキュリティ情報の共有といった、通常は積極化しにくいところを、実効的なものとしている。

オ）自動車も含めてモノのインターネットといった世界になると、必ずしも ICT の知識が深くない人がソフトウェアに携わることになり、そうするとセキュリティホールのあるモジュールを使ってしまう、ということが起こりがちになる。

このため今後、ますます、セキュリティ意識を持つことや教育、情報共有、管理といったことが大切になる。

(ⅱ) 地上基幹放送業界（放送 CEPTOAR）

一般社団法人日本民間放送連盟を事務局とする放送 CEPTOAR は、日本放送協会（NHK）、地上系民間基幹放送事業者（多重単営社及びコミュニティ放送事業者を除く）、一般社団法人日本民間放送連盟の 194 社・団体を構成員とする組織である（2015 年 3 月末現在）。

IT 障害に関し、NISC から提供される情報及びこれを補完する情報を適切に放送事業者に提供し放送事業者間において共有を図っている。2007 年 3 月に情報取り扱いルールを制定し、同 4 月より運用を開始している。障害事例情報等をメールや電話、FAX、Web により連絡している。

2013 年度には、以下のような活動を実施している。

ア）分野横断的演習に参加。セプター訓練を実施。

イ）セプターカウンシルにおけるＷＧ活動に参加。

ウ）セプターカウンシルにおけるＨＰレスポンス観測活動に参加。

エ）セプターカウンシルにおける標的型攻撃に関する情報共有体制に参加。

(ⅲ)ケーブルテレビ業界（ケーブルテレビ CEPTOAR）

一般社団法人日本ケーブルテレビ連盟を事務局とするケーブルテレビ CEPTOAR は、一般社団法人日本ケーブルテレビ連盟の正会員ケーブルテレビ事業者で、310 社を構成員とする組織である。（2015 年 3 月末現在）

IT 障害への予防力と再発防止力を高めることで国民生活や社会活動へ重大な影響を及ぼさないようにすることを目的としてケーブルテレビ事業者内での情報共有を図っている。

また、NISC から提供される情報セキュリティ情報および IT 障害情報、あるいはケーブルテレビ CEPTOAR が把握した情報セキュリティ情報および重要インフラの IT 障害情報の CEPTOAR 内での共有等に取組んでいる。2012 年 11 月に情報取り扱いルールを制定し、同 12 月より運用を開始している。障害事例情報等をメールや電話により連絡している。

2013 年度には、以下のような活動を実施している。

ア）セプターカウンシル総会（2013 年 4 月 9 日）にケーブルテレビ CEPTOAR として正式参加。

イ）第 8 回セプター訓練に参加（2013 年 10 月 8 日）。

ウ）分野横断的演習に参加。

② 金融分野

金融分野における重要インフラ事業者には、銀行、証券、生命保険、損害保険の各事業者があり、それぞれ、銀行等 CEPTOAR、証券 CEPTOAR、生命保険 CEPTOAR、損害保険 CEPTOAR を構成している。さらに、CEPTOAR 間の情報共有等のために、金融 CEPTOAR 連絡協議会がある。

わが国の金融機関によるサイバーセキュリティに関する情報共有および分析を行い、金融システムの安全性の向上を推進することにより、利用者の安心・安全を継続的に確保することを目的とする組織として、一般社団法人金融 ISAC が活動している。表 3.2b.1-5 は、金融 ISAC の主な活動項目である。

表 3.2b.1-5　金融 ISAC の主な活動項目

項目/内容	正会員	準会員
メーリングリスト（ML) インシデントや脆弱性情報等についてMLを通じ情報共有を行う。 MLはTLP（Traffic Light Protocol)を用い情報共有範囲を限定することにより、情報提供者の不利益を避ける。また、匿名による情報提供も可能な仕組みを用意。	対象	特定の情報のみ事務局より配信されます。準会員は投稿できない。
ワーキンググループ（WG) 特定の重要課題の分析、対策検討等を行います。 成果はWSやアニューアルカンファレンス等で発表。	参加可能	WG座長が指名した場合のみ参加可能。
レポート配信 MLで共有されている情報の傾向、FS-ISAC等の連携機関からの情報を金融機関向けの目線で配信。	対象	一部のみ配信。
ワークショップ（WS) 2ヶ月に1回程度　会員内の研究会を開催。 連携機関やアフィリエイト会員等からのトピック発表あり。会員同士の顔合わせの場。	対象	対象外。
アニュアルカンファレンス 年1回の社員総会。WG・連携機関・アフィリエイト会員等からのトピック発表。	対象	対象 但し、社員総会は対象外。

（出典　金融 ISAC のホームページ　http://www.f-isac.jp/institute/activities.html）

金融 ISAC では会員間でのメーリングリストを通し、日々のインシデントや脆弱性情報等をリアルタイムに共有している。また、特定の重要課題については、テーマごとのワーキンググループ（WG）を設け、会員共同で対策検討等を行いながら、知見と対応力を高めていく活動を行っている。これらの成果は、ワークショップやアニュアルカンファレンス等の場において共有している。

わが国の金融 ISAC は、1999 年に設立され、5,000 を超える会員組織により活発な情報共有が行われている米国の FS-ISAC をモデルとしている。

また、金融情報システムに関連する諸問題（技術、利活用、管理態勢、脅威と防衛策等）の国内外における現状、課題、将来への発展性とそのための方策等についての調査研究を行う機関として、公益財団法人金融情報システムセンター（FISC：The Center for Financial Industry Information Systems）がある。

調査研究活動は、会員企業からの派遣者を中心とするスタッフによって支えられており、内容の充実を図るため、国内外の金融機関、メーカー、決済機関、研究機関、学者、専門家等と活発に交流している。

調査研究から得られた知見は、整理・分析・評価のプロセスを経て、「金融機関等コンピュータシステムの安全対策基準」を始めとする各種ガイドライン等や、調査レポートとして各種刊行物やセミナーを通じて還元されている。例えば、サイバーセキュリティに関する「FISC 安全対策基準」の解釈運用について、FISC への問合せ状況を踏まえ、「FISC 安全対策基準」の適切な解釈運用のために有用な留意点及び参考情報を「FISC サイバーセキュリティ参考情報」として公表している。

図 3.2b.1-1 は、金融分野における情報共有体制を図示したものである。上記の金融 ISAC や FISC とも連携しながら実効性の高い情報共有を図っている。

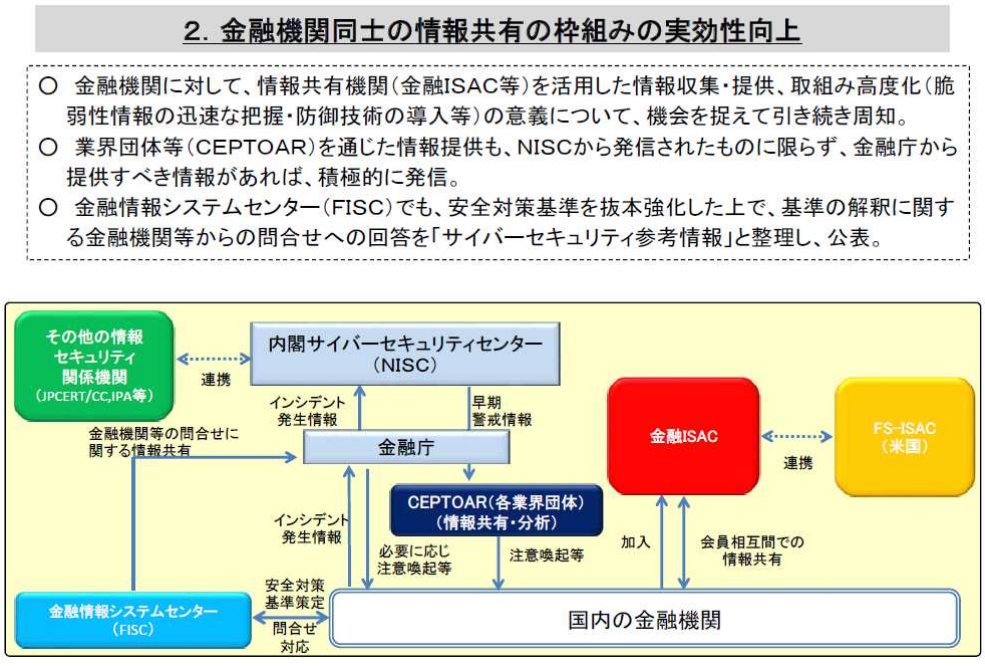


図 3.2b.1-1　金融分野における情報共有体制

（出典　金融庁、重重要インフラ専門調査会第 3 回会合 資料 2-2　「金融分野におけるサイバーセキュリティ強化に向けた取組方針（概要）」（2015 年 10 月 27 日）

【銀行業界（銀行等 CEPTOAR）】

一般社団法人全国銀行協会事務システム部を事務局とする銀行等 CEPTOAR は、銀行、信用金庫、労働金庫、商工中金、農協等 1,487 社を構成員とする組織である（2015 年 3 月末現在）。銀行等 CEPTOAR は、預金取扱金融機関の各業態全体を構成員としたほか、決済システム等の運営者も構成員に加えて組織している。

預金取扱金融機関は決済システム等を通じて相互に関連しており、1 金融機関に発生した IT 障害に起因する決済不全が他の金融機関にシステミックに拡大する可能性がある。このため IT 障害情報の共有を進めるとともに、その分析を行い、対応策を検討する機能を銀行等 CEPTOAR に設けている。預金取扱金融機関だけでなく、各種決済システム等の運営者を含めて情報展開を行うことにより、決済インフラ全体で情報共有を行っている点が特徴的である。

共有する情報には、各金融機関が金融庁に報告する IT 障害に関する情報に加え、IT を利用した金融犯罪に関する情報を含めている。このほか、脆弱性情報、ウイルス情報、その他 IT 障害の未然防止、発生時の被害拡大防止・迅速な復旧および再発防止に資する情報を共有対象としている。

分析は、構成員の各業界を代表する IT 担当者で構成する情報セキュリティ対策委員会が行う。同委員会には、金融業界の安全基準等である「金融機関等コンピュータシステムの安全対策基準」の設定主体である公益財団法人金融情報システムセンター（FISC）が参加し、FISC の協力を得て、IT 障害情報を分析し、対応策を検討している。

2007 年 3 月に情報取り扱いルールを制定、同 4 月より運用を開始し、障害事例情報等をメールや電話、Web により連絡している。

2013 年度には、以下のような活動を実施している。

ア）NISC から所管省庁を通じて提供される情報や重要インフラニュースレターを構成員と共有。
イ）JPCERT コーディネーションセンターから提供された情報を構成員と共有。
ウ）分野横断的演習に参加。セプター訓練に参加。
エ）セプターカウンシルにおけるＷＧ活動に参加。
オ）セプターカウンシルにおける標的型攻撃に関する情報共有体制に参加。

③ 政府・行政サービス分野

政府・行政サービス分野は、自治体 CEPTOAR として構成される。

【自治体の組織（自治体 CEPTOAR）】

地方公共団体情報システム機構（J-LIS）情報化支援戦略部を事務局とする自治体 CEPTOAR は、47 都道府県の 1,741 市区町村を構成員とする組織である（2015 年 3 月末現

在）。

地方公共団体間で利用する行政専用ネットワーク（LGWAN）を活用し、地方公共団体の情報セキュリティ対策の実施に必要な情報やツール等を地方公共団体で共有することで、適切な予防及び復旧に役立てる。NISC 等から提供される情報を、LGWAN メールにより地方公共団体へ提供する。また、地方公共団体の情報セキュリティレベルの向上を支援するための事業を実施するとともに、LGWAN を活用して、情報セキュリティに関する各種情報をメール及びポータルサイトにより提供する。

2007 年 3 月に情報取り扱いルールを制定、同 4 月より運用を開始し、障害事例情報等をメールや電話、Web により連絡している。

2013 年度には、以下のような活動を実施している。

ア）インターネットを通じて診断ポータルサイトから自動的にシステムによる診断を行う脆弱性診断（セキュリティ健康診断）を約 700 団体に対して実施した。WEB アプリケーションの脆弱性診断数は 2011 年の事業開始以降累計で約 4,200 サイト。また、インターネットに公開している Web サーバやネットワーク機器等の脆弱性診断数は 2011 年の事業開始以降累計で約 5,500IP。

イ）WEB 感染型マルウェア検知（ガンブラー等マルウェアが地方公共団体のサイトにあるかどうかを巡回検知）を約 800 団体に対して実施した。検知対象は約 18,600 サイト。

ウ）標的型攻撃（いわゆるマルウェアによる攻撃）の検知支援を約 220 団体に対して実施。

エ）内閣官房情報セキュリティセンターやセキュリティ関係機関から提供されるＩＴ障害等の情報を地方公共団体と共有。

・内閣官房情報セキュリティセンターからの情報の共有：13 件
・セキュリティ関係機関からの情報の共有：20 件

オ）WEB アプリケーションやネットワーク機器等の脆弱性について理解を深めるためのセミナーを全国 5 か所、実技講習会を全国 2 か所で開催。

カ）WEB 感染型マルウェアのトレンドについて月次報告するとともに、セミナーを全国 5 か所で開催。

キ）なりすましメール対策として送信ドメイン認証技術の導入に関するセミナーを全国 5 か所で開催。

ク）分野横断的演習に参加。

ケ）セプターカウンシルにおけるＷＧ活動に参加。

コ）セプターカウンシルの HP レスポンス観測活動について地方公共団体に参加を斡旋。

サ）（独）情報通信研究機構が提供する対サイバー攻撃アラートシステム「DAEDALUS」の利用を地方公共団体に斡旋。

上記のような自治体 CEPTOAR のセキュリティ情報共有の仕組みを踏まえ、情報共有・管理のあり方を検討すると、以下のように考えることができる。

A) ルール関係では、サイバーセキュリティ基本法、および、地方公共団体における情報セキュリティポリシーに関するガイドラインに伴い、セキュリティインシデント発生時の対応等をマニュアル化した情報セキュリティインシデント対応ハンドブックを整備している。こうした、インシデント発生時に、対応窓口が、迅速かつ的確な対応ができるように、必要な手順や関連情報をまとめることが重要である。
B) 他の自治体や他の重要インフラに影響を及ぼすセキュリティ情報・IT 障害については、自治体 CEPTOAR 経由で、LGWAN を通じて、すべての都道府県及び市区町村に対して、その情報を配信する
C) 他の自治体や他の重要インフラに影響を及ぼさない、個別自治体のセキュリティ情報については、総務省から都道府県を通じて市区町村へと連絡する。
D) その際のセプター（つまり業界ごとの組織）の役割とは、例えば自治体 CEPTOAR の場合であれば、自治体だけでも 1800 程度あるので、情報の内容は同じだとしても、直接 NISC から、各業界に属するメンバーにその情報を配信するのは現実的でなく、業界ごとに配信ルートを整備し、必要なメンバーに情報を着実に配信する役割を担う、という位置づけといえる。

④ 業界横断の組織

【サイバー情報共有イニシアティブ（J-CSIP）（重要インフラ機器製造業界、電力業界、ガス業界、化学業界、石油業界、資源開発業界）】

図 3.2b.1-2 は、独立行政法人情報処理推進機構（IPA）が情報ハブとなり民間組織とともに運営しているサイバー情報共有イニシアティブ（J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan）の体制を図示したものである。

図 3.2b.1-2　サイバー情報共有イニシアティブ（J-CSIP）
（出典　サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））
https://www.ipa.go.jp/security/J-CSIP/）

J-CSIP の設立は、2010 年より経済産業省が開催した「サイバーセキュリティと経済研究会」における提言の一つとして、「サイバー攻撃に対する官民での情報共有の必要性」が挙げられ、同省にてその準備を進めていた中、2011 年 9 月に国内重工業等複数社に対するサイバー攻撃事案の報道をうけて、経済産業省の呼びかけのもと、同年 10 月 25 日に国内の重工・重電等、重要インフラで利用される機器の製造業者 9 社を中心に、情報共有と早期対応の場として、IPA を情報ハブとする情報共有体制サイバー情報共有イニシアティブ J-CSIP が発足した。

2012 年 4 月、IPA と参加 9 社との間の NDA 契約（Non-Disclosure Agreement、秘密保持契約）を締結し、情報共有ルール策定が完了したことから正式運用が開始されている。その後、全体で 6 つの SIG（Special Interest Group、類似の産業分野同士が集まったグループ）、61 の参加組織による情報共有体制を確立し、サイバー攻撃に関する情報共有の実運用を行っている。

【J-CSIP の情報共有の仕組み】

ア）IPA と各参加組織が NDA 契約を締結し、情報の授受は、IPA を中継して実施。

イ）IPA は参加企業から情報提供を受け、必要な分析や加工を行った上で、参加組織へ情報共有を行う。

ウ）参加組織で検知された攻撃メール等のデータは、安全な方法で IPA へ情報提供される。攻撃を検知する手段は各組織に任せられており、IPA への情報提供を行うか否かについても各組織のベストエフォートとしている。

エ）IPA は、提供データを分析し、必要に応じてメールに添付されたウイルスの解析情報を付加する。また、情報提供元に関する情報など機微情報の匿名化を行う。

オ）情報提供元の最終確認を経て、他の参加組織に対して情報提供（共有）を行う。

カ）各組織は、共有された情報をもとに分かったことについては、可能な限り報告を上げることとし、同様な攻撃が発見された場合等にそれらの情報を再共有する仕組みとなっている。

キ）J-CSIP の運用状況を四半期ごとに、年次で活動レポートをホームページに掲載している。

J-CSIP では、この他に、標的型サイバー攻撃特別相談窓口を設置し、標的型攻撃を受けた際の駆け込み寺として専門知識を有する相談員による窓口対応を行っている。

また、IPA が特に重大な攻撃が発生していると判断する場合には、対象参加組織（企業）の協力のもと、検出された不審ファイルの分析や現地調査など標的型サイバー攻撃の実態調査を行っている。

業界横断のセキュリティ情報共有の仕組みである J-CSIP の事務局である IPA への聞き取り調査を行った。その結果、及び、上の公開情報を踏まえ、情報共有・管理のあり方を検討した結果、以下のように整理した。

A) J-CSIP では、現状標的型攻撃メールを中心に、業界内、業界間の情報共有を行っている。秘密保持契約（NDA）を IPA と各組織との間で締結している。

B) 基本的には標的型メール攻撃に対象を絞り、情報提供は宛て先情報をカットしたメール情報を共有するというものである。このため情報提供者の匿名化が行われ、自己の不具合など情報提供者にデメリットのある情報でも無いため、情報提供の敷居が低く参加し易い一因である。

C) 情報提供は、行うかどうか任意であるが、契約企業の本社が検知したものだけでなく、関連会社で見つかったものについても共有の対象としている。逆に、IPA からの情報を、本社だけでなく、関連会社に広げて提供してもよいことになっている。受け取った情報をどのように活用するかは、メンバーの自由である。

D) ただし、情報共有は契約者間で閉じて行う。情報が漏洩した場合は、どの攻撃については検知／対処できていて、どの攻撃についてはできていないかを、攻撃側に知らせてしまうことになる。

E) 情報提供や活用に任意性を持たせているのは、義務化すると参加しにくくなるからである。一方で、脆弱性等の情報を外に漏らしてはならない、受け取った情報を使って、こういうことをすることは許可しないなどの規定がある。

F) 情報共有の仕組みを作っても、普段からの訓練や慣れが重要である。例えば、攻撃メールの情報を受け取ったとして、それに該当するメールが過去にどれだけ来ているかをすぐに検索できるようになっていないと、速やかな対策ができない。

G) 怪しいメールがあった場合、その情報を報告してよいのかの判断を、組織階層に従って上の人に判断を仰いでいては、時間ばかりかかってしまい、適時性のある対応ができない。対策についても同じである。担当者が判断して、情報提供したり、対策をとったりできるように、予め、受け取り側の組織としてルールを整備しておく必要がある。

H) 攻撃を受けた場合、その痕跡、証拠を残しておくことが重要である。報告や情報提供に必要であり、分析や対策のためにも必要である。

I) 実際に危険が発生していなくても、怪しいメールが来ているかどうか、という情報は重要である。実際の危険に至っていなくても、攻撃メールが来ているということは、狙われているということであり、対策の必要がある。

J) パソコンやサーバの不自然な挙動など、人間の感覚による気づきも、対策上、非常に重要になるケースもある。

K) 情報共有の仕組みを作る上でのポイントとしては、スモールスタートで、開始当初から、着実に授受する情報がある状態を作ること。開始してから数ヶ月も音沙汰のない状態を作ってしまうと実効性のある情報共有基盤として立ち上がらない可能性がある。些細な情報でも授受することが重要であり、他のメンバーはそれを受け取って、自分たちも情報を出してみようという気になれる。

L) これから情報共有をはじめる場合、そうした、開始当初における呼び水の設定が重要になる。

M) 脆弱性の情報を流すということは、製品等の不具合をさらすということであり、情報を出すのに消極的になってしまう可能性もある。しかし、脆弱性が残ったままで製

品を世の中に供給し続けるのは問題であり、責任ある対応が求められる。逆に、受け取る側には、脆弱性というのは初めからゼロにはできなくて、見つけて塞いでいくしかない、という理解を得ることも重要である。

N) 脆弱性の検知方法について、従来の品質検査は物理的な耐久試験等である。それに対し、サイバーセキュリティの脆弱性は、例えば、ファジングなどで、ハングアップしないかなどを調べたりするため、コストがかかる。

O) サプライチェーンの階層の上下など、ビジネス上の関係が、情報共有に影響を与える可能性はある。発注者側からすると、情報を出せ、ということになりがちだが、義務化すると提供側は参加しづらくなる。一方で、組み込みソフトのソースが流出したとか、設計図が流出したということになると、脆弱性を攻撃されるリスクが非常に高まるので、情報公開してもらうことは非常に重要である。こういう情報は、現場よりも事務系から漏れるケースもあるので、特に注意が必要である。

P) 共有体制の課題として、中小企業までカバーできていないことがある。中小企業では、知識や専門家も不足しており、対応が難しい。例えば、問題となる攻撃メールを確保して送ってもらおうとしても、既に消してしまった、といったことになることが多い。

(3) 考察

以上の調査結果からセキュリティ情報を共有する場合の組織作り、組織運営について以下のような示唆が得られる。

A) 組織化後に情報流通を有効に行うための運営努力（スモールスタート、日頃から呼び水となるような情報共有など）が重要である

B) 情報の内容／レベルに合わせた複数の連絡網構築が必要である

C) 受け取った情報を厳格に管理するため、個社内での情報管理／流通／対応体制の構築が必要である

D) 組織内のメンバー間の人的ネットワーク構築による信頼関係の構築が重要である。

E) ホワイトハッカーなど組織外の関係者との信頼感構築も重要である。このためには既に構築され情報が集まる既存の組織（IPA、JPCERT/CC など）との組織間の良好な関係構築が近道と考えられる

F) 脆弱性に対する理解（供給側、利用者側）の教育・浸透をサポートする必要がある

3.2b.2　自動走行を行うシステムの選定

セキュリティの検討を行う上では対象とするモデルを明確にする必要がある。

本事業では自動走行の共通モデルの構築についてテーマ①で検討が行われるが、検討を並行して進めるため、仮定として一財）日本自動車研究所が公開している自動走行システムのアーキテクチャを採用して、検討対象とする自動走行システムのベースモデルを検討する。

(1) 想定する自動走行モデル

以下の図 3.2b.2-1 は、本プログラムの V2X セキュリティ第 2 回 WG で検討した自動走行システムアーキテクチャ案である。

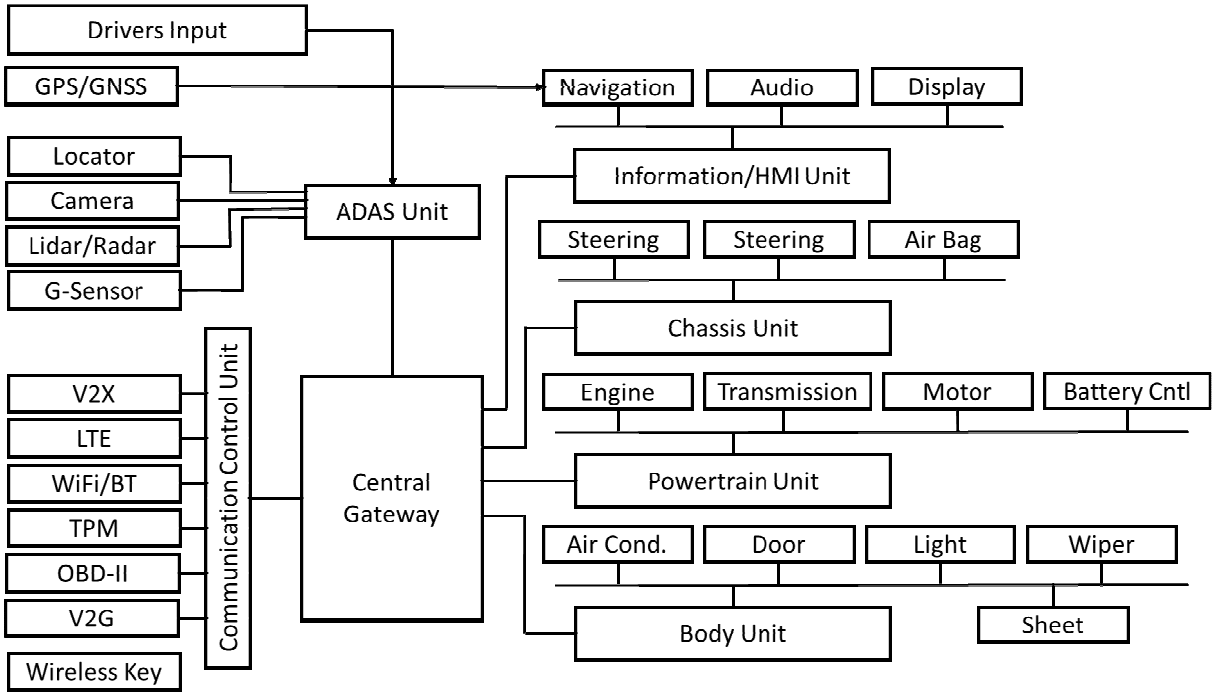


図 3.2b.2-1　自動走行システムアーキテクチャ案(V2X セキュリティ WG)

図 3.2b.2-2 は、図 3.2b.2-1 を基に今回の脅威分析用に整理した自動走行システムアーキテクチャである。セントラルゲートウェイを中心に、シャシー、パワートレイン、ボディーなど、それぞれ目的によって異なるユニット（システム）で構成されている。各ハードウェアの機能概要は、表 3.2b.2-1 に示す。

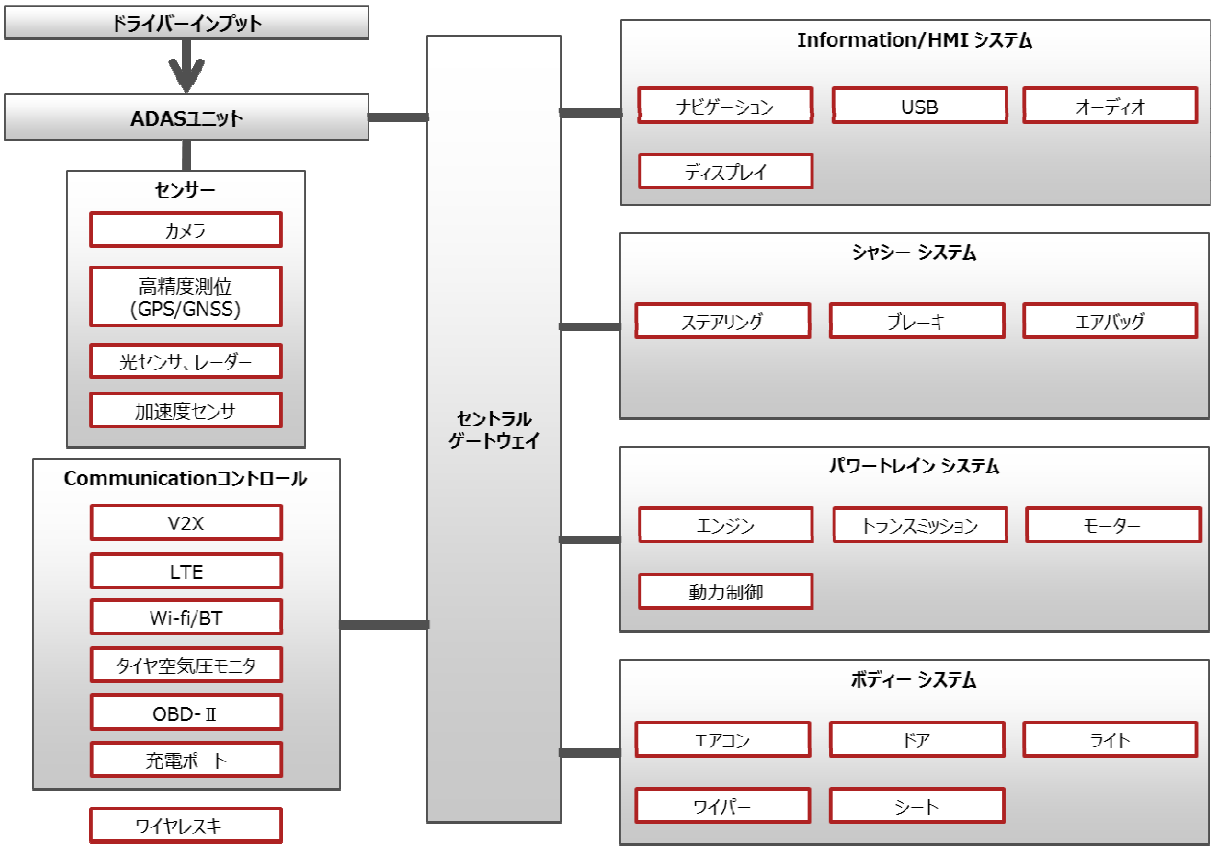


図 3.2b.2-2　自動走行システムアーキテクチャ

表 3.2b.2-1　自動走行システムアーキテクチャの各機能の概要

ユニット名	ハードウェア名	機能概要
ドライバ インプット	-	ドライバの操作情報（機械的・電気的信号）
ADAS ユニット	-	自動走行のための認知・判断・制御を行う機能
セントラル ゲートウェイ	-	各システム間をルーティングする装置（セキュリティ機能を持つ）
センサ	カメラ	外部の状況を撮影する
	高精度測位(GPS/GNSS)	衛星通信を用いて車の位置情報を高精度に測位する
	Lidar、 レーダー	周辺環境の距離・方向を検知する（検知対象は車だけではなく、歩行者や建物等も含まれる）
	加速度センサ	車の加速度を計測する
Communication コントロール	V2X	自車と周辺（他車、路側機、歩行者等）との通信
	LTE	携帯電話網を利用する通信技術
	Wi-Fi/BT	近距離無線通信デバイス
	タイヤ空気圧モニタ	タイヤの空気圧情報を受信する
	OBD-Ⅱ	診断ポート
	充電ポート（V2G)	車電源系統への電力を供給するポート
Information/HMI システム	ナビゲーション	目的地までの道案内サポート
	USB	USB ポート
	オーディオ	音声・音響を再生する装置
	ディスプレイ	表示装置
シャシー システム	ステアリング	舵取り装置
	ブレーキ	車輪の回転を調節したり止めたりする装置
	エアバッグ	衝突時乗員保護装置
パワートレイン システム	エンジン	動力機関
	トランスミッション	変速機、動力伝達装置
	モータ	電動機
	充放電制御	バッテリーの充放電管理
ボディー システム	エアコン	空調管理
	ドア	ドアの開閉、施錠開錠の制御
	ライト	ライト類の制御
	ワイパー	ワイパーの制御
	シート	シート位置、傾斜の制御
その他	ワイヤレスキー	ドアを施錠開錠するリモコン信号の受信

以上の図 3.2b.2-2 を基に図 3.2b.2-3 の自動走行モデル図を作成した。ここでは、ECU 単位の物理的アーキテクチャから、機能単位へモデル化を行っている。ECU イコール機能とは必ずしも限らず、ひとつの ECU で複数の機能を有するものもあれば、複数の ECU でひとつの機能を有するものがあると考える。

モデル図では、各機能を、走行に関する機能、外部接続、センサ系統、その他の機能で色分けして表現している。

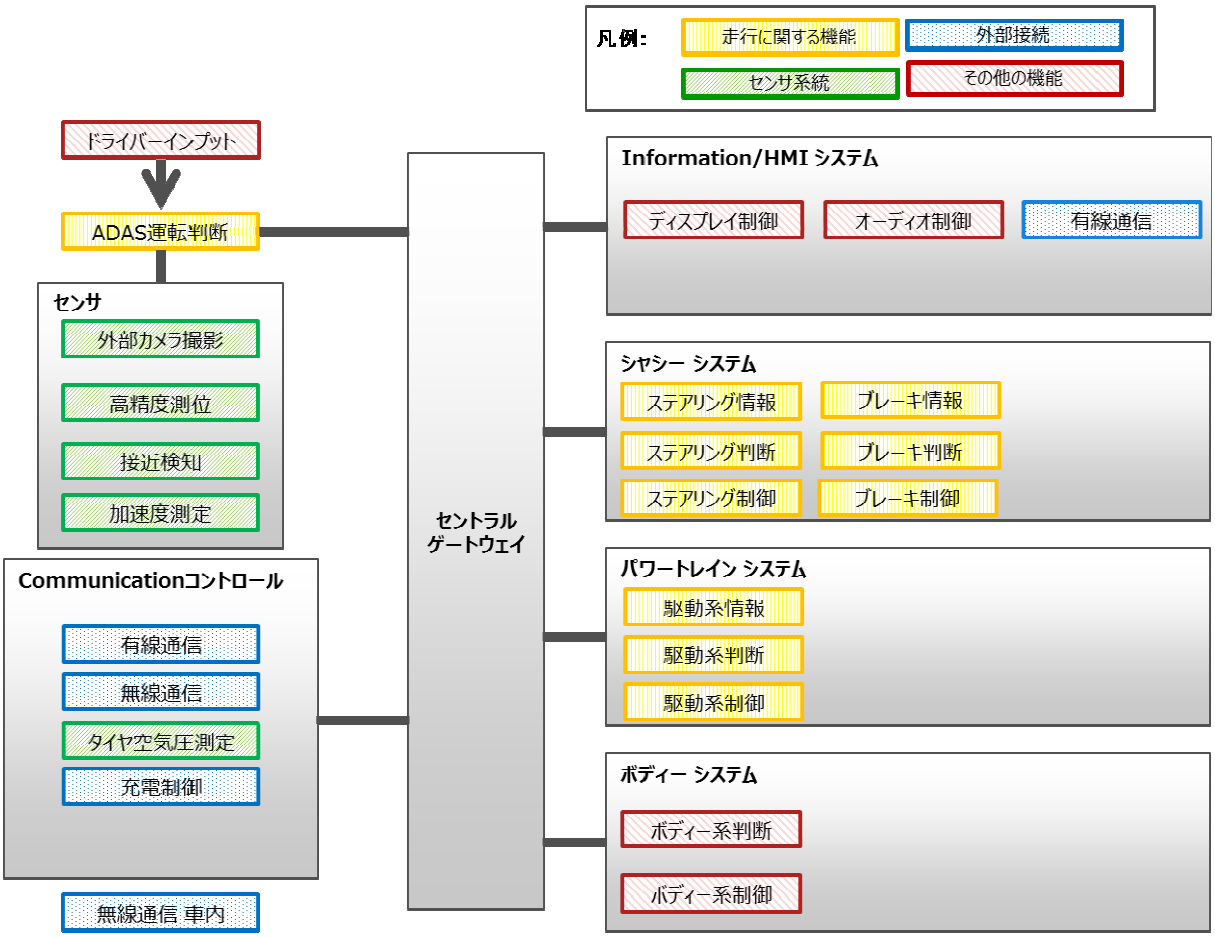


図 3.2b.2-3　自動走行モデル図

本自動走行モデルは、セントラルゲートウェイを中心に、各システムがつながる構成である。

ドライバーインプットは、ドライバの意思をデータ情報に変換する機能である。タッチパネルディスプレイが例としてあげられる。ADAS 運転判断は、ドライバのインプット情報やセンサ情報をもとに、車の ADAS 機能の動作方針を決定する機能である。車の走行ルートの軌跡生成などが例としてあげられる。センサは、車が外部情報や自車状態をセンシングするための機能の集合である。Communication コントロールは、有線無線を問わず、自動走行車が装置や他車と情報の送受を行うための出入り口となる機能の集合である。データだけでなく、電力のやりとりをおこなう充電制御もここに分類している。Information/HMI システムは、ドライバと車が情報をやり取りするための手段や、そのための装置やソフトウェアなどの機能の集合である。カーナビ装置が例としてあげられる。

シャシーシステムは、車の足回り機構に関する機能の集合である。パワートレインシステムは、エンジンやモータで作られた回転力を駆動輪へと伝える機能の集合である。ボディーシステムは、エアコン、ドアなど内装品に関する機能の集合である。

なお、ハードウェア名とモデル図上の機能名との対応をまとめたものが、表 3.2b.2-2 である。

表 3.2b.2-2　自動走行システムアーキテクチャ

ハードウェア名	機能名大項目	機能名小項目
ドライバーインプット	ドライバーインプット	—
ADAS ユニット	ADAS 運転判断	—
カメラ	外部カメラ撮影	—
高精度測位(GPS/GNSS)	高精度測位	—
光センサ、 レーダー	接近検知	—
加速度センサ	加速度検知	—
V2X	無線通信	—
LTE		—
Wi-Fi/BT		—
ワイヤレスキー		—
OBD-Ⅱ	有線通信	—
充電ポート		—
USB		—
ナビゲーション	ディスプレイ制御	—
タイヤ空気圧モニタ	タイヤ空気圧測定	—
オーディオ	オーディオ制御	—
ディスプレイ	ディスプレイ制御	—
ステアリング	ステアリング系	ステアリング情報
		ステアリング判断
		ステアリング制御
ブレーキ	ブレーキ系	ブレーキ情報
		ブレーキ判断
		ブレーキ制御
エンジン	駆動系	駆動系情報
トランスミッション		駆動系判断
モータ		駆動系制御
動力制御		—
モータ		—
エアコン	ボディー系	ボディー系判断
ドア		ボディー系制御
ライト		—
ワイパー		—
シート		—
エアバッグ		—

(2) 車両レベルでのセキュリティ分析

① 機能モデル図（センシング、判断、操作）について

図 3.2b.2-4 は、図 3.2b.2-3 の自動走行モデル図の機能を「検知・認知」「判断」「操作」の 3 項目に分類しマッピングした機能モデル図である。

なお、モデル化を行うにあたり、以下の定義を用いて機能のマッピングを行っている。

「検知・認知」とは、外部及び車内の情報を受信する機能と定義している。

「判断」とは、得た情報を基に操作を行うための命令を生成する機能と定義している。

「操作」とは、命令に基づいて実行する機能と定義している。

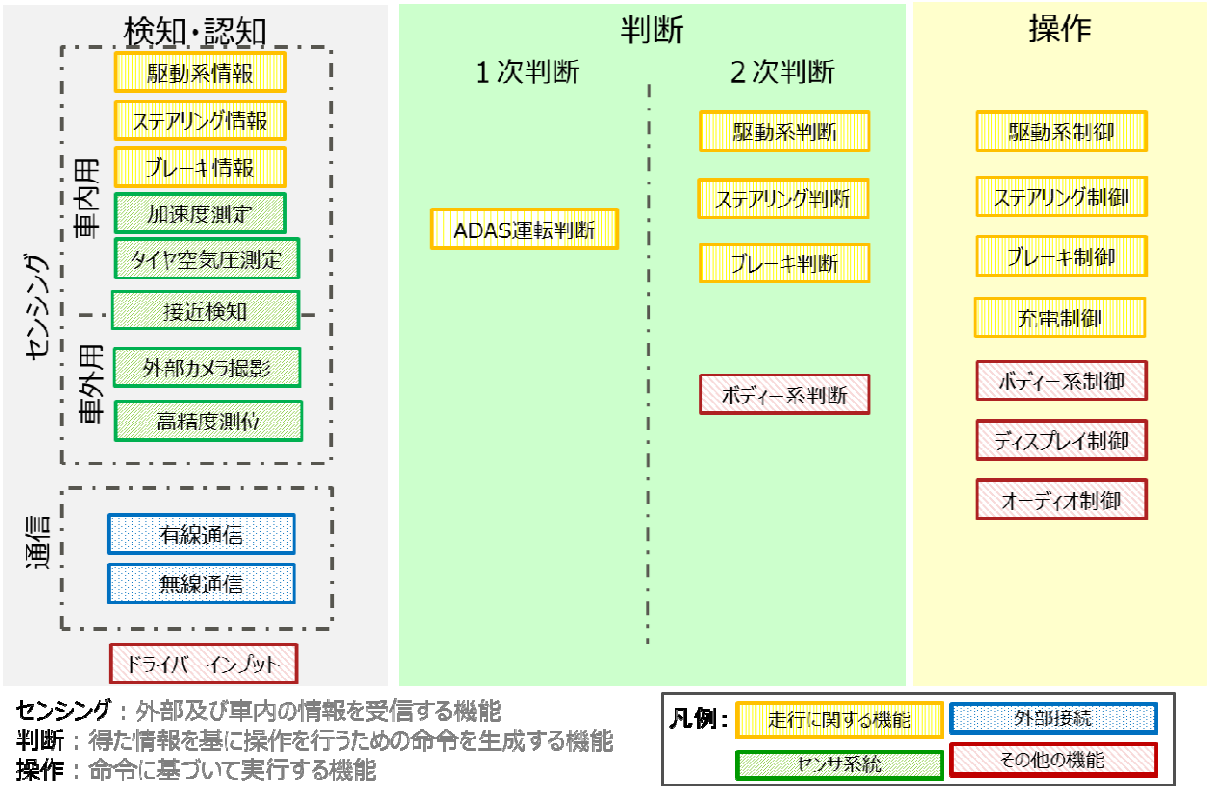


図 3.2b.2-4　自動走行の機能モデル図

図 3.2b.2-4 の機能モデル図において、「判断」の分類を 1 次判断と 2 次判断にさらに分けて表現している。1 次判断は ADAS 運転を行う際の軌道の生成や周辺の障害物の有無、走行時の白線認識など、自動走行を実現するための情報を受け取り判断する機能を一次判断とし、2 次判断は実際にブレーキや駆動、ステアリングなどの走行制御に関わる機能に対して、具体的な命令を生成する機能を 2 次判断としている。認知機能群から 1 次判断を介さずに直接 2 次判断にデータが送られる場合もあると考える。

② 侵入経路の洗い出し

システムへの攻撃の侵入経路となるのは一般的にシステムとの境界であり、外部から情報を送受信するロが侵入経路となると考えられる。そのため、モデル図内でセンシングに分類された機能から、攻撃の侵入経路となりうるものを抽出した。

本来は全ての個所が侵入経路になりえるため、対処する必要があるが、以下の理由で対象外とした

しかし、センシングに分類された機能のうち、駆動系情報、ステアリング情報、ブレーキ情報、加速度測定と、ドライバー入力は侵入経路の対象でないと判断した。その理由を以下に示す。

・駆動系情報、ステアリング情報、ブレーキ情報などの走行制御系
走行制御に対してのフィードバックに用いられる情報は、それぞれ駆動系判断、ステアリング判断、ブレーキ判断の走行制御に関する判断機能に送られる。分析した車載 LAN アーキテクチャ上ではそれらの機能は同一の HW にひとまとめになっており、途中でデータ改ざんを行ったり不正なデータ注入が困難なため侵入経路にされる可能性は低いと判断した。

・加速度測定
加速度測定については、センサ内部の加速度検知用の物質が加速度によって起こる、何らかの変化を取得して加速度を数値的に測定しているため、誤った測定をさせることは難しい。よって、センサを用いて他の ECU へのメッセージの完全性を損なわせることは難しいと考える。また、外部から測定周期を変更させることはできないので侵入経路にはなりにくいと判断した。

・ドライバ入力
外部から多車へのサイバー攻撃を分析の対象としているためドライバ入力は対象外とした。

そのほかに、侵入経路を選ばない攻撃としてハーネスクリッピングなど、バスに直接改造を加える攻撃も想定されるため CAN 内のバス全ても攻撃の侵入口となりうる。

これらの理由から抽出した侵入経路を以下の図 3.2b.2-5 の上に丸で囲んだ番号を割り当てた。表 3.2b.2-3 に侵入経路をまとめる。

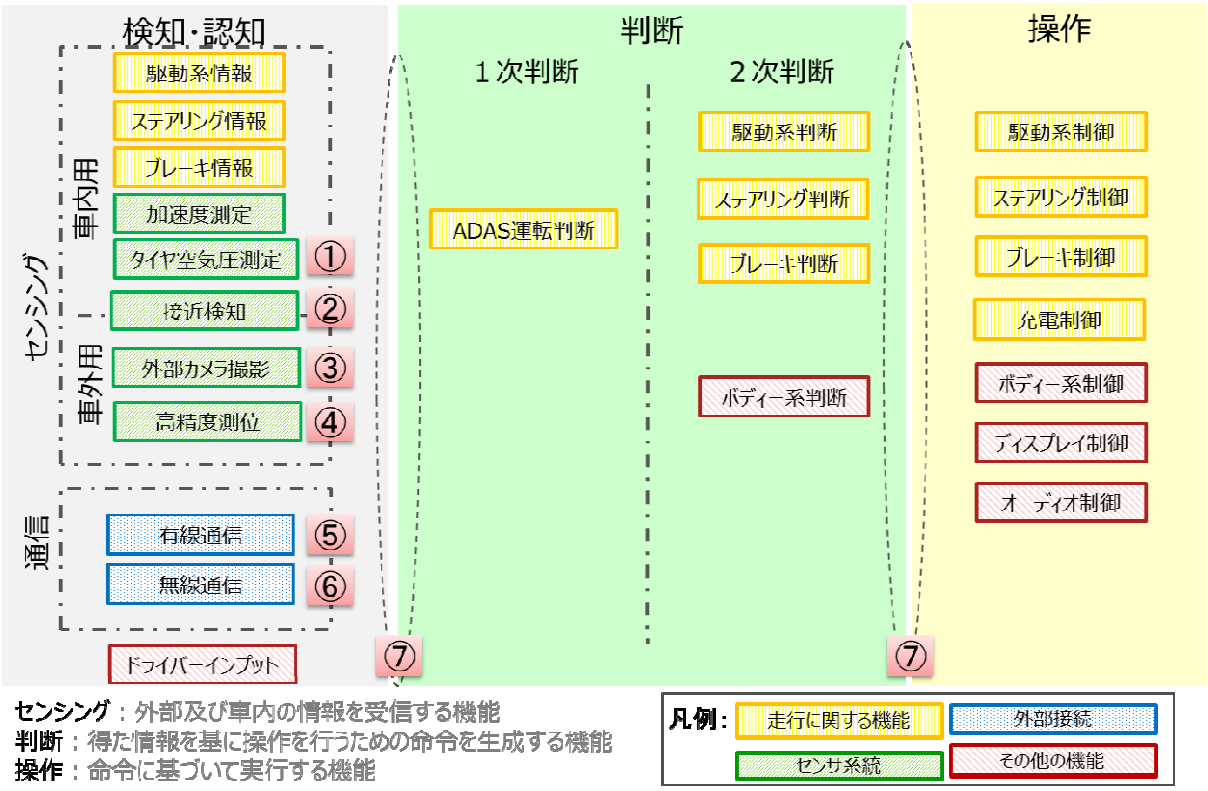


図 3.2b.2-5　自動走行モデルの想定侵入経路

表 3.2b.2-3　自動走行モデルの想定侵入経路一覧

No.	分類	侵入箇所
①	車内情報センシング	タイヤ空気圧測定
②	車外情報センシング	接近検知
③	車外情報センシング	外部カメラ撮影
④	車外情報センシング	高精度測位
⑤	外部接続口	有線通信
⑥	無線通信機器	無線通信
⑦	その他	全ての CAN バス

【①～④車内/外センシング】

センサは車両周辺の外界情報や、自車の制御情報をセンシングする装置のため、攻撃者が悪意をもって外界から不正な情報（光や電波など）をセンサから入力することができる状態である。攻撃される可能性は低いと考えるが、車載 LAN と攻撃者の境界点になる可能性がある。よって、侵入箇所となりうる。

攻撃としては「センサ装置に不正な情報を入力する攻撃」が想定される。レーダーに対して不正な電波を入力する攻撃、カメラへ大量の光を入力して不正なアナログデータを送信する攻撃などがあげられる。

【⑤外部接続口について】

外部接続口は、攻撃者が不正機器を有線で接続できる状態となっている。また、電気的、プロトコル的にも仕様が一般公開されており、車載 LAN と攻撃者の境界点になる可能性がある。よって、侵入箇所となりうる。

攻撃としては「不正機器を接続してネットワークに侵入する攻撃」が想定される。CAN につながる ECU に予期しない動作をさせる ECU への攻撃、CAN のネットワーク帯域占有などのネットワーク妨害、メッセージ盗聴、全データ無効化などがあげられる。

【⑥無線通信機器について】

無線通信機器は攻撃者が無線で接続できる状態である。また、電気的、プロトコル的にも仕様が一般公開されており、車載 LAN と攻撃者の境界点になる可能性がある。よって、侵入箇所となりうる。

攻撃としてまず一つ目に、「無線経由でネットワークに侵入する攻撃」が想定される。無線通信機器に不正接続して攻撃する。CAN につながる ECU に予期しない動作をさせる ECU への攻撃、CAN のネットワーク帯域占有などのネットワーク妨害、メッセージ盗聴、全データ無効化などがあげられる。

二つ目に、「外部との無線通信への攻撃」が想定される。妨害電波による通信妨害、不正な無線通信機器によるメッセージ盗聴、無線経由で通知される情報の破壊などがあげられる。

【⑦その他】

CAN 内でのメッセージ送信はブロードキャスト方式であり、MAC や認証などの対応をとっていない ECU は CAN 内を流れるすべてのメッセージを受信する。そのため CAN ケーブルを改造して直接不正端末を取り付けることで不正なメッセージを CAN 内に送信たり、盗聴することが可能となる。

③ 想定脅威

ISO/IEC 27005 では、情報セキュリティのリスクマネジメントについて規格を策定している。ISO/IEC 27005 内のセキュリティ脅威とセキュリティ対策方針事例において、脅威の対象となる情報資産ごとに求められる脅威一覧を挙げている。情報資産の分類はデータ、プログラムコード、プログラム実行（サービス）、監査・監視、利用主体（行為を含む）、情報処理システム（利用と運用）、情報機器が挙げられている。

車載 LAN において検討するべき保護資産は、システム（記憶媒体）、ネットワーク上のデータ、プログラムコード、プログラム実行（サービス）であり、それらが 2013 年に IPA が発行した「自動車セキュリティへの取組みガイド」(https://www.ipa.go.jp/files/000027273.pdf)内の 2.2.2 章 「攻撃者による干渉に起因する脅威」に記載されている攻撃手法の対象になっているため脅威の抽出として十分であると判断した。IPA では、自動車システム（車載システム、車載ネットワーク、周辺システム）を対象として、そのシステム上にある情報を狙う攻撃、設備そのものやサービスを維持するためのシステムや機器が攻撃されることを脅威と述べている。

IPA 想定脅威と説明を表 3.2b.2-4 にまとめる。

表 3.2b.2-4　想定脅威一覧

（IPA 発行 2003 年 「自動車セキュリティへの取り組み」2.2.2 章 表 2.6 参照）

IPA 想定脅威	説明
不正利用	なりすましや機器の脆弱性の攻撃によって、正当な権限を持たない者に自動車システムの機能を利用される脅威
不正設定	なりすましや機器の脆弱性の攻撃によって、正当な権限を持たない者に自動車システムの設定値を不正に変更される脅威
情報漏えい	自動車システムにおいて保護すべき情報が、許可のされていない者に入手される脅威
盗聴	自動車内の車載機同士の通信や、自動車と周辺システムとの通信が盗み見られたり奪取されたりする脅威
DoS 攻撃	不正もしくは過剰な接続要求によって、システムダウンやサービスの阻害をひきおこす脅威
偽メッセージ	攻撃者がなりすましのメッセージを送信することにより、自動車システムに不正な動作や表示を行わせる脅威
ログ喪失	操作履歴等を消去または改ざんし、後から確認できなくする脅威
不正中継	通信経路を操作し、正規の通信を乗っ取ったり、不正な通信を混入させる脅威

④ 自動走行モデル図での脅威分析(C,I,A 分析)

図 3.2b.2-5 に示す自動走行モデルの各想定侵入経路（①～⑦）に対して、脅威分析（C,I,A 分析）を行い、各想定侵入経路における具体的なセキュリティの脅威について以下に整理した。

以降、この整理に基づき、具体的な対策を検討する必要がある。

(ｉ) タイヤ空気圧測定

表 3.2b.2-5　タイヤ空気圧測定に各攻撃を行った場合の影響

攻撃	影響	CIA への影響		
		可用性	完全性	機密性
不正利用	完全性を失ったタイヤ圧情報がステアリング/ブレーキ判断に伝えられ、精確な走行制御ができなくなる可能性がある	なし	あり	なし
不正設定	完全性を失ったタイヤ圧情報がステアリング/ブレーキ判断に伝えられ、精確な走行制御ができなくなる可能性がある	なし	あり	なし
情報漏えい	機密性が担保できなくなるが走行制御上問題なし	なし	なし	あり
盗聴	機密性が担保できなくなるが走行制御上問題なし	なし	なし	あり
DoS 攻撃	ステアリング/ブレーキ制御時にタイヤ圧情報の可用性が担保できず、精確な走行制御ができなくなる可能性がある	あり	なし	なし
偽メッセージ	完全性を失ったタイヤ圧情報がステアリング/ブレーキ判断に伝えられ、精確な走行制御ができなくなる可能性がある	なし	あり	なし
ログ喪失	ログ喪失により総当たり攻撃や DoS 攻撃対策が無効化され、ステアリング/ブレーキ制御時にタイヤ圧情報の完全性/可用性が担保できず、精確な走行制御ができなくなる可能性がある	あり	あり	なし
不正中継	完全性を失ったタイヤ圧情報がステアリング/ブレーキ判断に伝えられ、精確な走行制御ができなくなる可能性がある	なし	あり	なし

(ⅱ) 接近検知

表 3.2b.2-6　接近検知に各攻撃を行った場合の影響

攻撃	影響	CIA への影響		
		可用性	完全性	機密性
不正利用	完全性を失った情報が伝えられ、不正にパワードアが開けられたり、正しい利用者が接近してもあかない可能性がある	なし	あり	なし
不正設定	完全性を失った情報が伝えられ、不正にパワードアが開けられたり、正しい利用者が接近してもあかない可能性がある	なし	あり	なし
情報漏えい	機密性が担保できなくなるが走行制御上問題なし	なし	なし	あり
盗聴	機密性が担保できなくなるが走行制御上問題なし	なし	なし	あり
DoS 攻撃	接近検知情報の可用性を担保できない場合、接近検知ができず、正しい利用者が接近してもあかない可能性がある	あり	なし	なし
偽メッセージ	完全性を失った情報が伝えられ、不正にパワードアが開けられたり、正しい利用者が接近してもあかない可能性がある	なし	あり	なし
ログ喪失	ログ喪失により総当たり攻撃や DoS 攻撃対策が無効化され、情報の完全性/可用性が担保できず、不正にパワードアが開けられたり、正しい利用者が接近してもあかない可能性がある	あり	あり	なし
不正中継	完全性を失った情報が伝えられ、不正にパワードアが開けられたり、正しい利用者が接近してもあかない可能性がある	なし	あり	なし

(iii) 外部カメラ撮影

表 3.2b.2-7　外部カメラ撮影に各攻撃を行った場合の影響

攻撃	影響	CIA への影響		
		可用性	完全性	機密性
不正利用	完全性を失った情報が伝えられ、周辺の障害物が検知できず事故につながる可能性がある	なし	あり	なし
不正設定	完全性を失った情報が伝えられ、周辺の障害物が検知できず事故につながる可能性がある	なし	あり	なし
情報漏えい	機密性が担保できなくなるが走行制御上問題なし	なし	なし	あり
盗聴	機密性が担保できなくなるが走行制御上問題なし	なし	なし	あり
DoS 攻撃	カメラ利用時に情報取得できず、周辺の障害物が検知できず事故につながる可能性がある	あり	なし	なし
偽メッセージ	完全性を失った情報が伝えられ、周辺の障害物が検知できず事故につながる可能性がある	なし	あり	なし
ログ喪失	カメラから来る情報には影響なし	なし	なし	なし
不正中継	カメラから来る情報には影響なし	なし	なし	なし

(ⅳ) 高精度測位

表 3.2b.2-8　高精度測位に各攻撃を行った場合の影響

攻撃	影響	CIA への影響		
		可用性	完全性	機密性
不正利用	完全性を失った情報が伝えられ、正しい地図情報が取得できず自動運転時に事故が発生する可能性がある	なし	あり	なし
不正設定	完全性を失った情報が伝えられ、正しい地図情報が取得できず自動運転時に事故が発生する可能性がある	なし	あり	なし
情報漏えい	機密性が担保できなくなるが走行制御上問題なし	なし	なし	あり
盗聴	機密性が担保できなくなるが走行制御上問題なし	なし	なし	あり
DoS 攻撃	地図情報が取得できず自動運転ができない可能性がある	あり	なし	なし
偽メッセージ	完全性を失った情報が伝えられ、正しい地図情報が取得できず自動運転時に事故が発生する可能性がある	なし	あり	なし
ログ喪失	総当たり攻撃や DoS 攻撃対策が無効化され、情報の完全性/可用性が担保できず、自動運転時に事故が発生する可能性がある	あり	あり	なし
不正中継	完全性を失った情報が伝えられ、正しい地図情報が取得できず自動運転時に事故が発生する可能性がある	なし	あり	なし

(ｖ) 有線通信

表 3.2b.2-9　有線通信に各攻撃を行った場合の影響

攻撃	影響	CIA への影響		
		可用性	完全性	機密性
不正利用	完全性を失った情報が伝えられ、自動運転時に事故が発生する可能性がある	なし	あり	なし
不正設定	完全性を失った情報が伝えられ、自動運転時に事故が発生する可能性がある	なし	あり	なし
情報漏えい	機密性が担保できなくなるが走行制御上問題なし	なし	なし	あり
盗聴	機密性が担保できなくなるが走行制御上問題なし	なし	なし	あり
DoS 攻撃	情報の可用性が担保できず、自動運転ができない可能性がある	あり	なし	なし
偽メッセージ	完全性を失った情報が伝えられ、自動運転時に事故が発生する可能性がある	なし	あり	なし
ログ喪失	総当たり攻撃や DoS 攻撃対策が無効化され、情報の完全性/可用性が担保できず、自動運転時に事故が発生する可能性がある	あり	あり	なし
不正中継	有線通信の場合影響なし	なし	なし	なし

(vi) 無線通信

表 3.2b.2-10　無線通信に各攻撃を行った場合の影響

攻撃	影響	CIA への影響		
		可用性	完全性	機密性
不正利用	完全性を失った情報が伝えられ、自動運転時に事故が発生する可能性がある	なし	あり	なし
不正設定	完全性を失った情報が伝えられ、自動運転時に事故が発生する可能性がある	なし	あり	なし
情報漏えい	機密性が担保できなくなるが走行制御上問題なし	なし	なし	あり
盗聴	機密性が担保できなくなるが走行制御上問題なし	なし	なし	あり
DoS 攻撃	情報の可用性が担保できず、自動運転ができない可能性がある	あり	なし	なし
偽メッセージ	完全性を失った情報が伝えられ、自動運転時に事故が発生する可能性がある	なし	あり	なし
ログ喪失	総当たり攻撃や DoS 攻撃対策が無効化され、情報の完全性/可用性が担保できず、自動運転時に事故が発生する可能性がある	あり	あり	なし
不正中継	完全性を失った情報が伝えられ、自動運転時に事故が発生する可能性がある	なし	あり	なし

(vii) すべての CAN バス

表 3.2b.2-11　CAN バスに各攻撃を行った場合の影響

攻撃	影響	CIA への影響		
		可用性	完全性	機密性
不正利用	完全性を失った情報が伝えられ、自動運転時に事故が発生する可能性がある	なし	あり	なし
不正設定	完全性を失った情報が伝えられ、自動運転時に事故が発生する可能性がある	なし	あり	なし
情報漏えい	機密性が担保できなくなるが走行制御上問題なし	なし	なし	あり
盗聴	機密性が担保できなくなるが走行制御上問題なし	なし	なし	あり
DoS 攻撃	情報の可用性が担保できず、自動運転ができない可能性がある	あり	なし	なし
偽メッセージ	完全性を失った情報が伝えられ、自動運転時に事故が発生する可能性がある	なし	あり	なし
ログ喪失	総当たり攻撃や DoS 攻撃対策が無効化され、情報の完全性/可用性が担保できず、自動運転時に事故が発生する可能性がある	あり	あり	なし
不正中継	CAN バスへの攻撃の場合影響なし	なし	なし	なし

3.2b.3　想定されるサイバー攻撃の事例収集

前項までで、想定したモデルに対してセキュリティ対策を行うべきポイントについて整理をした。一方で、現時点では車両に対するサイバー攻撃事例として、実質の被害などの事例は報告されておらず、研究・実験レベルでの報告に留まっている。

報告内容によれば、その攻撃の原理は、脆弱性を見つけて改竄し、バックドア相当の機能を送り込んで制御を奪う、など ICT 機器に対する攻撃と同じであり、今後現実の被害になる可能性がある。

本節では、ICT での攻撃事例を元に図 3.2b.2-2 の車載システムに想定されるサイバー攻撃の事例を考察し、車両での対策のヒントになるであろう ICT での対策事例を元に、どのような対策をすべきかについても合わせて考察する。

(1) 事例

① サービス妨害の攻撃事例

サービス妨害は、文字通りインターネットを用いた各種サービスに対する妨害であるが、その攻撃手段はさまざまな手段が存在し、車両に対する攻撃としては別の目的でこれらの手段が使われる可能性はある。

“2000 年 2 月に米国の大手の Web サービス(Yahoo、eBay 等)に対してサービス妨害が行われ、実質的なサービス不能に陥ったことがきっかけである。

大手 Web サービスは大量のユーザからの接続に対応するために非常に高い処理能力を備えており、簡単にサービス不能になることはないと考えられていたが、インターネット上の多くのコンピュータから一斉に攻撃対象に大量のデータを送る「分散型サービス妨害(Distributed Denial of Service、DDoS)」という手法が攻撃に使われるようになったことで、実際に被害が生じるに至った。

これ以降、金銭目的や組織に対する恐喝・抗議・嫌がらせ、社会的・政治的意図等を動機としてさまざまなサービス妨害攻撃が発生し、今ではインターネットを用いた各種サービスの安定的な提供に対する主要な脅威の 1 つとなっている。”

【IPA「サービス妨害攻撃の対策等調査-報告書-」2010 年 12 月から引用】

② 外部からの動作制御（誤動作）の攻撃事例

車両も含めて、これまでの組込みシステムはスタンドアロンで動作、機械的な制御であったのに対し、これからの組込みシステムではインターネットを含めた様々なネットワークと接続して動作、クラウドの活用、ソフトウェア制御、個人情報や操作情報のような機微な情報を含めた様々な情報を扱う傾向にある。

組込みシステムが繋がっていく中では、情報だけでなく「機器の操作」も行われ、機器同士が連携するようになってくる。そのため、これまでの情報漏えいや改ざん等への対策

だけでは無く、攻撃者によって機器が利用者の意図しない動作を防ぐ対策も必要となる。

以下に、ICT での攻撃事例を記載する。

【Webカメラの画像を意図しない相手が見ることが可能な事例（2015年3月）】

・IPアドレス等から2,163台のWebカメラを検出、内769台でパスワードが未設定
・非公開の試作品や店舗や工場の様子が確認できた
・カメラによっては場所を特定できるケースもあり
・カメラの向き等を第三者が操作できた可能性も指摘される

パスワードが設定されていたとしても
・デフォルトパスワードの利用
・Webカメラ自体に脆弱性がある可能性もあり

【スマートハウスのセキュリティ事例（2015年5月）】

・次世代省エネ住宅「スマートハウス」の情報を一元管理する「HEMS: Home Energy Management System」をルータを介せずネットワークに繋げた場合、第三者に情報を見られたり、家庭内機器を遠隔操作されたりする可能性があった。

ルータ自体の脆弱性も従来から数多く報告されている。
・脆弱性情報対策データベース（JVN iPedia）でルータの脆弱性を検索すると283件の情報がヒットする（2015年9月現在）。
・最近のものでは2015年8月31日にも、ハードコートされたパスワードや、バッファオーバーフローの脆弱性など、複数の脆弱性を含む機器が報告されている。
（上記 2 件は、IPA「IoT におけるセキュリティの脅威と対策」2015 年 11 月 20 日（https://www.ipa.go.jp/files/000049819.pdf）から引用）

車両の動作制御に対する攻撃事例を以下に記載する。それまでの車両に対する攻撃は車両に乗り込むのが前提の直接的な攻撃で、難度が極めて高いものであったのに対し、以下の事例では無線通信を介して攻撃できたことから、自動車業界を揺るがす“事件”であり、自動車メーカーに“実害”（リコール）が生じている。

【車両へのハッキングのセキュリティ事例（2015年8月）】

Black Hat及びDEF CONにおいて、クライスラー社のJeep Cherokeeの脆弱性を攻撃し、遠隔操作を成功させた事例の発表があった。
・Jeep Cherokeeに搭載されている車載器Uconnectに認証回避の脆弱性があり、悪意あるファームウェアに書き換えることが可能
・UconnectにはIPアドレスが割り振られており、遠隔で特定の車に対して通信が可能
・ファームウェアを改ざんした車に対して攻撃コードを送りこむことで、ブレーキ、スアリング、エアコン等への干渉が可能

・影響がある140万台に対してリコール
　修正ソフトはオーナ及び整備工場にUSBメモリで配られた

上記 DEF CON では、テスラモーターズ社の Model S において、6 つの脆弱性があったことも報告されている。

・遠隔操作ではなく、車載ネットワークに直接PCを繋ぐことで攻撃が可能となる脆弱性
・二つの脆弱性ではインフォテイメントのルート権限を奪取できるもの
・これらの脆弱性を利用することでエンジンスタートや扉の開閉等が可能
・テスラモーターズ社は自動アップデートで対応
（上記事例は、IPA「IoT におけるセキュリティの脅威と対策」2015 年 11 月 20 日
（https://www.ipa.go.jp/files/000049819.pdf）から引用）

【広域ネットワークを利用した車載ネットワークへの攻撃事例(2011年)】

これまでの車両に接触もしくは近距離からの攻撃に加え、携帯電話に繋がっている車両に対して、遠隔地から攻撃を行う手法についての論文「Comprehensive Experimental Analyses of Automotive Attack Surfaces.」が発表された。この中ではこの攻撃に依る様々な影響について検討されているが、遠隔地からのドア解錠や、悪意ある攻撃者による車両の監視については、被害が大きくなるものと考えられる。（図 3.2b.3-1）

・始めにテレマティクス車載器に関して不正アクセスを行い、脆弱性を利用して遠隔操作用のクライアントを立ち上げる
・立ち上がった遠隔操作用クライアントに対して、車両の制御に関する任意のメッセージを送る事によって、遠隔地からのドアロック解除やエンジンスタートを実施する
・攻撃の難易度としては高いものであるが、大手テレマティクスサービスの攻撃コードが開発され、それが流布された場合、被害が広範囲にわたることが考えられる
・攻撃に対する対策として、「外部からの不必要な通信を遮断する」「不要な通信サービスについては機能として削除する」「車載システム開発時にセキュアプログラミングの概念を持つ」「ソフトウェアアップデート手法を持つ」「複数の機能が連携した場合のセキュリティを検討する」ことなどが挙げられており、情報システムと同様の情報セキュリティ対策を実装することで被害を防ぐことが可能である。

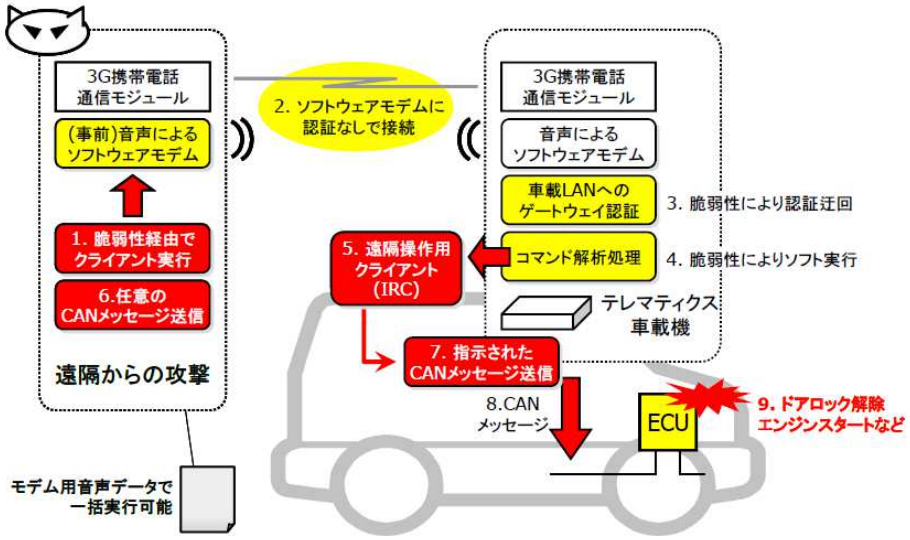


図 3.2b.3-1　遠隔地から車両への攻撃例

（引用・出典　IPA　「自動車の情報セキュリティ」に関するレポート　2012年5月31日）

③ 各種情報搾取（情報取得）の攻撃事例

以下に、ICT での攻撃事例を記載する。情報システムという性質上からも事例が多いため、代表的な報道を一覧で記載する（表 3.2b.3-1）。

表 3.2b.3-1　サイバー攻撃事例

時期	報道
2011/3	仏財務省にサイバー攻撃、G20情報盗まれる　（読売新聞等）
2011/6	米グーグル：中国からサイバー攻撃 米韓政府関係者ら被害（毎日新聞等）
2011/9	三菱重にサイバー攻撃、80台感染…防衛関連も　（読売新聞等）
2011/9	IHIにもサイバー攻撃 日本の防衛・原発産業に狙いか　（産経新聞等）
2011/10	衆院にサイバー攻撃 議員のパスワード盗まれる　（朝日新聞等）
2011/11	サイバー攻撃：参院会館のPC、ウイルス感染は数十台に　（毎日新聞等）
2012/1	JAXA：職員のパソコン感染、無人補給機情報など流出か　（毎日新聞等）
2012/2	農水省に標的型メール攻撃、情報流出狙う？　（読売新聞等）
2012/2	特許庁、トロイの木馬型感染…メール情報流出か　（読売新聞等）
2012/3	国際協力銀行の顧客220社とのメール流出　（毎日新聞等）
2012/6	パソコン5台、ウイルス感染か＝外部サイトと通信－原子力安全基盤機構（時事通信等）
2012/7	財務省PC数か月情報流出か…トロイの木馬型　（読売新聞等）

（出典　IPA　「サイバー攻撃と組込みセキュリティ自動車の情報セキュリティ」2012年11月15日）

最近の代表事例では、2015年6月の「日本年金機構から125万件の個人情報流出」がある。

(2) 考察

① 車両における侵入経路の想定

ICT での攻撃事例を、車両システムで想定するため、図 3.2b.2-2 の自動走行システムアーキテクチャで想定した侵入経路を以下に記載する。

①はサービス妨害の攻撃の侵入経路、②は外部からの動作制御の侵入経路、③は各種情報搾取の攻撃に侵入経路と想定する。

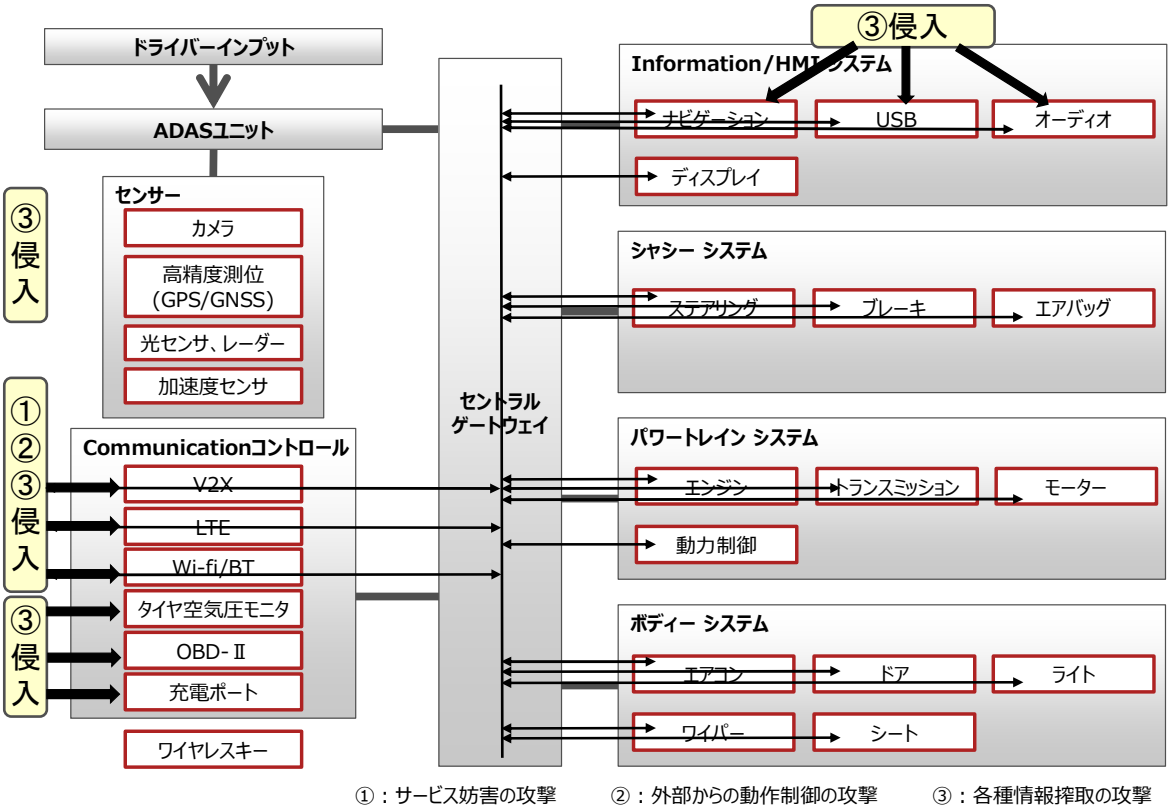


図 3.2b.3-2　システムアーキテクチャで想定する侵入経路

② 攻撃種別毎の考察

(ⅰ) サービス妨害の攻撃

企業でのインターネットへの依存度の高まりにより、大規模なサービス妨害攻撃の発生は企業の事業継続に重大な影響を及ぼす状況となっている。

ICT での対策として、近年クラウド化が注目されている。これまで企業側のサーバで行っていた処理やサービスをクラウド側で効率的に行おうとするものであり、サービス妨害攻撃の耐性が向上し、影響を受けにくくなる効果が期待出来る。一方で、クラウドを使うことでインターネットを情報が流通する機会が増える為、サービス妨害等の影響を受けてネットワーク上の障害が発生すると、外部との接続で成り立っているシステムである為、

接続が切断され、業務やサービスに重大な影響が生じる可能性がある。

昨今、インターネット上の多くのコンピュータに加え、自動車、監視カメラ、ATM、録画機、ゲーム機、自動販売機、スマートフォン等のさまざまな機器がインターネットに接続されている。それらの機器が攻撃者に乗っ取られ、攻撃者の実行指示によりボット[3]と化して攻撃者の一部になっている事例がある。攻撃者の踏み台にされた機器が、その善意の所有者・利用者の意図に反して攻撃者になってしまう点が脅威である。

ICT での Dos 攻撃に対する防御手法の一つがクラウド化であるが、車両レベルでの防御策を考える場合、車両に搭載する機能でクラウドを利用することで対応できる機能・サービスについては可能な限りクラウドで実装することも対策の一つになる。

DoS 攻撃は、インターネットで一般的に使われているプロトコルの仕組みを悪用することが多く、車両への DoS 攻撃は図 3.2b.2-2 の自動走行システムアーキテクチャで想定した場合、外部ネットワークを利用する V2X・LTE・Wi-Fi 等の Communication コントロール部を利用した攻撃が想定される。

攻撃の主な動機がインターネットを用いた各種サービスの提供に対して、金銭目的での恐喝・抗議・嫌がらせである事から、車両そのものに対する攻撃よりも、車両が利用する外部ネットワーク側のサービスが妨害され、それにより車両側でサービスの利用ができなくなる事例が発生すると推測される。

また、Information/HMI システム部に搭載される機能（Navigation や Audio 等）に依存して、車両でのインターネット利用が普及していく現状から、車両そのものに対する DoS 攻撃の可能性もあり、さらに車両を踏み台にした攻撃も考えられるため（乗っ取られた車両が攻撃者になり得る）、車両そのものにも防御策が必要である。

車両に対する攻撃内容が ICT での事例と同様の攻撃の場合、ICT での対策事例と同等の対策が有効となるが、実際の車両での対策としては以下の考慮が必要と考える。

ア）「走る・曲がる・止まる」に影響する制御機能を最優先で防御する為、攻撃を検出した時点でインターネットを用いた各種サービス自体を遮断する

イ）制御機能に影響しない場合、ICTでの事例と同様の脆弱性に対する対策、攻撃元IPアドレスの遮断措置などを実施する。対策実施後の効果の確認も検討が必要（ファジングの活用等）

ウ）車両外部での対策もICTでの事例と同様に、インターネットサービスプロバイダ側での対策、通信キャリアへの協力依頼、車両へのサービス提供側においてクラウド化を検討する

[3] 「ロボット」の略称。人間がコンピュータを操作して行っていた処理を、人間に代わって自動的に実行するプログラムのこと

(ⅱ) 外部からの動作制御の攻撃

外部からの動作制御（誤動作）を車両で考えた場合、車載システムや車載 LAN 等におけるオープン化・汎用プロトコル等の利用促進に伴い、車両の「走る・曲がる・止まる」という基本制御機能に与える影響が増加している。自動車メーカーが提供するサービスとして、リモートドアロック制御、ソフトウェア更新サービスなどの機能があるが、これらの車載システムに Linux のような汎用 OS が利用されつつある。

また、車載 LAN に対する Ethernet や TCP/IP の利用についても研究開発が行われている。これまでの車載ネットワークの通信方式は、要求命令や応答内容などの意味が自動車メーカーごとに異なることが多かったが、統一化の検討も始まりつつあり、今後車載ネットワークへの接続は容易になっていくと考えられる。

様々な車内外の機器や情報システムが繋がり、多種多様なサービスの利用が可能になっていく一方で、汎用技術の採用で通信内容の解析や攻撃の難易度が下がると考えられ、車両としてのセキュリティ対策の検討が必要である。

車両の動作制御に対する攻撃や情報破壊は、運転中に攻撃を受けると車両事故に直結し、影響が重大かつ広範囲の被害が発生する可能性があり、身体や生命への重大な被害、社会的混乱を招く可能性がある。従って、制御用車載ネットワークへのセキュリティ検討は最も重要であり、他の機能を遮断してでも守る必要がある。

車両に対して情報システムと同様のセキュリティ対策を実装する場合、以下の様な課題への取り組みが必要である。

ア）車両システムと情報システムの差分調査
　車両に依存したシステム仕様と実装部分の洗い出し

イ）外部からの不必要な通信の遮断、不要通信サービスの機能削除
　追加評価試験内容（ポートスキャン試験等）の検討、および評価試験環境整備

ウ）車載システム開発時にセキュアプログラミングの概念を持つ
　車両システム実装作業者に対するセキュアプログラミング教育の実施等

エ）ソフトウェアアップデート手法
　機能実現にあたっての安全性検討（リモートリプロ等）

オ）複数の機能が連携した場合のセキュリティ
　ICT で適用されている多重防御の考え方を車両システムに適用することの検討

カ）その他（性能）
　車両の動作制御に関わる部分へセキュリティ対策を搭載する場合、セキュリティ対策機能が動作する事による性能劣化を考慮する必要がある。
　「走る・曲がる・止まる」の制御に影響を与えるような性能劣化は重大な事故に繋がるため、セキュリティ対策搭載前後での性能を検証し、車両の動作制御の阻害にならないレベルまでチューニング（リソース割り当て、CPU 選定、割り込み処理・排他制御時間見直し等による高速化など）を実施した上で搭載する必要がある。

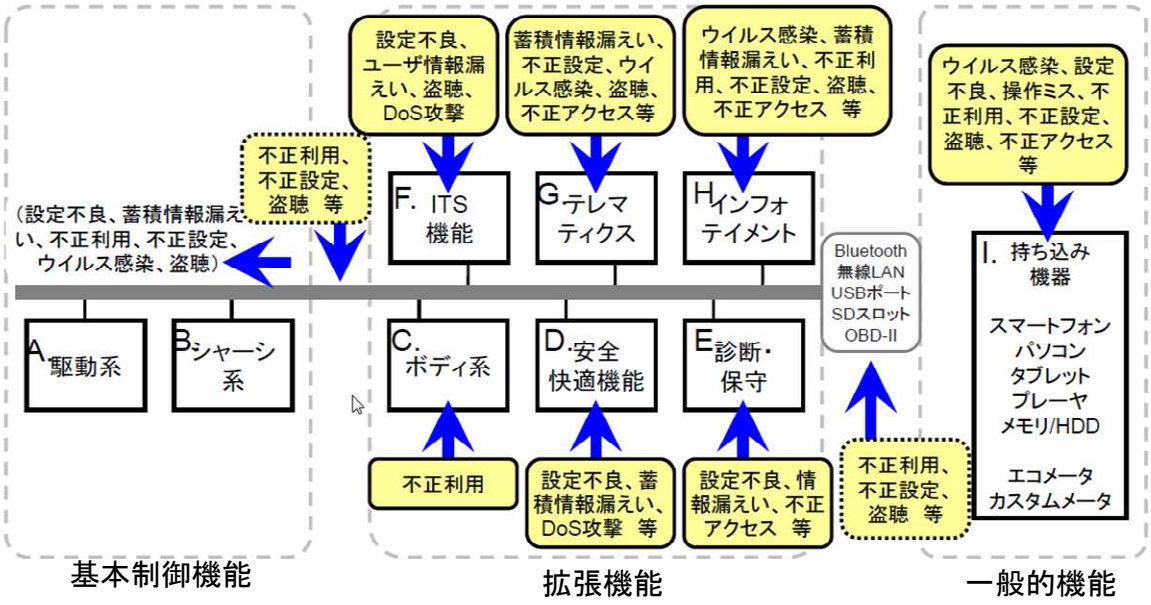
(ⅲ) 各種情報搾取の攻撃

ICT での情報搾取のセキュリティインシデントの 1 つが「コンピュータウイルス」であり、侵入経路はネットワークやコンピュータに直接接続するデバイスが主な要因となっている。

ウイルス感染による情報の破壊や漏えい（情報搾取）、業務の停滞、ウイルスメール発信（拡散）の被害が多く、主な侵入経路は電子メール、インターネット接続（ホームページ閲覧など）、USB メモリ等の外部記憶媒体、ファイルのダウンロードなどとなっている。

車両においては、拡張機能や一般的機能（図 3.2b.3-3 参照）で扱う様々な情報について外部から情報搾取の被害にあう可能性がある。
スマートフォンの普及により、信頼性の低いアプリケーションの脆弱性によりスマートフォンが踏み台となり、車両の車載機やカーナビに損害を与えたり、車内情報の漏えいによる運転者のプライバシ侵害などが想定される。また、移動中の車両に対して外部からネットワークを介した攻撃も実施可能になると想定される。

ETC（Electronic Toll Collection System）、スマートキーのように無線による接続や、充電ポートを経由した車載ネットワークとの接続に対しても同様のリスクが想定される。



車両制御に直接攻撃を仕掛けるのではなく、脆弱なシステムを踏み台にして、
車両制御に影響を与える危険性もある

図 3.2b.3-3 車両セキュリティ分析例

（出典　IPA　IoTにおけるセキュリティの脅威と対策　2015年6月11日）

車両における侵入経路を図3.2b.2-2の自動走行システムアーキテクチャで想定した場合、外部ネットワークを利用する V2X・LTE・Wi-Fi等のCommunicationコントロール部を利用した情報搾取が想定され、車両本体側でスマートフォン等の持込機器を踏み台にして攻撃を受けた場合の防御策が必要となる。

また、USB メモリ等のリムーバブルメディア経由でマルウェアに感染し、情報搾取の可能性がある。（タイヤ空気圧モニタ、OBD-Ⅱ、充電ポート等も物理的な外部接続という観点では USB 機能と類似している）

図 3.2b.3-3 に記載のように、「走る・曲がる・止まる」を制御する基本制御機能以外に、車両には快適な運転や、運転のサポートを担う拡張機能と、持ち込み機器も含めた一般的機能がある。

【拡張機能】

ア）車両の快適な運転や、運転のサポートを担う機能

イ）外部との通信機能を持つ事も多く、また車内での連携機能も多い

ウ）今後も機能向上が見込まれ、それに伴ったセキュリティ対策が必要

【一般的機能】

エ）スマートフォンやPCに代表されるユーザが外から持ち込んで使う機器

オ）サービスが多様で、様々な情報を扱う為攻撃者に最も狙われやすい

カ）既存のセキュリティ技術の適用が可能だが、対策実施にはユーザの協力が必要

これらの拡張機能や一般機能で扱う様々な情報について、外部から情報の入出力が出来る通信ポートを持つ機能については PC と同様の脅威があり、外部から情報搾取の被害にあう可能性がある。よって、車両においても PC と同様の対策検討が必要である。

但し、PC と車両システムではシステムを構成するハードウェア構成や通信ポートの接続構成、ソフトウェアの OS や構成が同一ではない為、PC と同様の対策適用にあたってはシステム差分の調査、実装方法の検討、評価試験の環境構築、対策適用による効果の確認方法について事前検討が必要である。

ICT サイバー攻撃の事例では、USB メモリ等のリムーバブルメディア経由でのマルウェア感染がある。マルウェアの感染手法として利用している機能は「自動実行機能」と「自動再生機能」であり、USB メモリの接続や CD-ROM の挿入などに応答してシステムが動作することを目的として実装された機能を利用して、特定のプログラム実行や、音楽再生を実行する、などの動作を行う手法である。

不正プログラムの実行により、レジストリ書き換えや、不正ファイルが作成された結果、アカウント情報等詐取、脆弱性攻撃、パスワードクラック等の情報漏えい事件、Web サイトアクセス妨害、ハードディスクドライブ暗号化によるアクセス制限等、情報破壊事件が発生している。

ICT での対策事例としては大きく 2 種類あり、1 つは「自動実行機能」「自動再生機能」を無効化する方法であるが、前提として、OS メーカーより提供されている最新のサービスパック及びセキュリティパッチを適用する対策となる。

もう 1 つは書き込み防止機能を持つリムーバブルメディアの利用、ウイルス対策機能を持つリムーバブルメディアを利用等、利用するメディアで対策する方法である。

現時点ではリムーバルメディア経由で車両がマルウェアに感染した事例は報告されていないが、車両がマルウェアに感染した場合、走行不能や車載ネットワークを経由して外部（インフラや他の車両）への感染が考えられ、脅威となる。

上記、リムーバブルメディアに対する対策の事例では Windows OS での対策を挙げているが、車両システムでもリムーバブルメディアからの感染対策が必要である（サンドボックス機能の搭載、音楽データ等のデータチェック機能搭載、接続機器の認証機能搭載などが考えられる）。

(ⅳ) 複数の攻撃に対して

年々進化する ICT においては、各侵入経路を単体で防御しても防御をすり抜けるような複数の攻撃が多発しており、「多層防御」(複数の対策を多層で行うこと)を考慮したセキュリティ対策と運用管理の実施が重視されている。

車両においてもコネクテッド機能の進化に伴い攻撃の拡大が想定される。このため、制御用 ECU や車載ネットワークを単体で守るだけでなく、未知の攻撃対策も含めた多層防御の考え方を導入する必要がある。

3.2b.4　対策すべきポイントとその評価指針の仮定

セキュリティ要素として ISO TR13335 では以下のように定義されている。

真正性（Authenticity）	：	相手が本物であること
完全性（Integrity）	：	情報が改ざん、破壊、削除されないこと
可用性（Availability）	：	要求された機能が確実に動作すること
信頼性（Reliability）	：	意図した動作、結果が得られること
機密性（Confidentiality）	：	情報が外部から解読できないこと
追跡性（Accountability）	：	事象の発生を追跡できること

これらは保護対象物の性質や価値により、要素の必要性や優先度、その対策方法は異なる。

3.2b.3 のような攻撃事例を意識した上で、3.2b.2「自動走行を行うシステムの選定」で想定した脅威分析結果について、対策すべきポイントとその評価指針について仮定を行った。

(1) 自動走行モデル図にセキュリティ対策技術をマッピング

表 3.2b.4-1 に、攻撃手法、想定侵入経路を基に行うべき対策手法を抽出し、整理した。また、各セキュリティ対策を施すことで得られる効果について述べる。

表 3.2b.4-1　想定脅威に対するセキュリティ技術一覧

攻撃の種類	セキュリティ対策技術
不正利用	(ⅰ) メッセージ間の MAC 生成/検証 (ⅱ) 侵入検知
不正設定	(ⅰ) メッセージ間の MAC 生成/検証 (ⅱ) 侵入検知 (ⅲ) API のアクセス制限 (ⅳ) HW で対策
情報漏えい	(ⅴ) 通信メッセージの暗号化 (ⅵ) サーバ認証 (ⅸ) セキュアファイルシステム
盗聴	(ⅴ) 通信メッセージの暗号化 (ⅵ) サーバ認証
DoS 攻撃	(ⅶ) ドメイン分離 (ⅷ) パケットフィルタリング
偽メッセージ	(ⅴ) 通信メッセージの暗号化 (ⅵ) サーバ認証
ログ喪失	(ⅳ) HW で対策 (ⅲ) API のアクセス制限
不正中継	(ⅴ) 通信メッセージの暗号化 (ⅵ) サーバ認証

【(ⅰ)メッセージ間の MAC 生成/検証】

偽メッセージへの対策はメッセージ認証コード（MAC: Message Authentication Code）の生成/検証が有効である。MAC は、通信データの改ざんの有無を検知するために通信データから生成する符号のことを指す。あらかじめ検証鍵（共通鍵）を共有しなければ生成/検証ができずメッセージの完全性を検証することができないため、偽メッセージを送信するなどのなりすまし行為に対して有効である。

【(ⅱ)侵入検知】

不正書き換えが行われた装置の存在を確認することに対して侵入検知は有効である。ネットワークを監視して正常でない通信を検知する技術である。不正書き換えが行われた装置は偽メッセージを送信するため、それを検出することが可能となる。

【(ⅲ) API のアクセス制限】

装置のパラメータを不正に書き換えたり、ログを改ざんする攻撃に対してアクセス制限は有効である。API へのアクセス制限とは、正当な権限を持たないアクセスを制限(禁止)する機能である。例として GNU/Linux システムに対して、LSM (Linux Security Module）と呼ばれるアクセス制御フレームワークなどがある。

【(ⅳ)HW で対策】

HW で対策については、セキュリティ技術が汎用的ではなく、一般的に導入できる技術が少ないため検討の対象外とする。

【(ⅴ)通信メッセージの暗号化】

情報の盗聴/漏えいを防ぐために暗号化は有効な手法である。暗号化鍵を用いて通信メッセージの暗号化を行い、暗号化されたメッセージは復号鍵を持つ者のみが復号し、読むことができる。復号鍵を持たない第三者が不正にメッセージを入手してもメッセージの中身を知ることができず、機密性が守られる。

【(ⅵ)サーバ/端末認証】

不正書き換えが行われた装置の有無を確認することに対して機器認証は有効である。相手から送られた情報を自己の持つ情報を用いて認証する技術である。システム内に有効な認証情報を持たなければ認証されない。不正書き換えが行われた装置は認証情報を持たないため、不正書き換えを検出することが可能となる。

【(ⅶ)ドメイン分離】

車両システム系と自動運転システム系など、機能を実現する上で密接に関わる ECU をひとつのドメインとしてまとめ、それぞれのドメインを物理的に分離させる（ゲートウェイ等を用いる）。そうすることで侵入箇所から攻撃があった場合にも、守るべき ECU が属するドメインの可用性、完全性に影響が及ばないようにできる。

【(ⅷ)フィルタリング】

フィルタリングには 3 種類の方法があり、一つはパケットの ID 情報を用いた ID フィルタリング、もう一つは TCP/IP プロトコルにおいて IP アドレスを利用して行う IP フィルタリング、最後にパケットの通過量を監視するパケットフィルタリングである。

ドメインを論理的に分離させる対策として、ID フィルタリングは有効である。ホワイト/ブラックリストフィルタリングとは、信頼できるメッセージのみを他のドメインに転送するあるいは、ある ID を完全に信頼しないものとして、それ以外を他のドメインに転送する機能であり、ゲートウェイに搭載することで他のドメインの可用性、完全性に影響が及ばないようにできる。

また、パケット通過量フィルタリングは単位時間当たりのパケットの通過量を監視し、閾値を超えた場合 DoS 攻撃として検知する手法である。

【(ix)セキュアファイルシステム】

セキュアファイルシステムは、暗号通信に用いられる秘密鍵や、デジタル署名に用いる署名情報など、第三者からの書き換えを防ぐのに有効である。セキュアファイルシステムは、情報への不正なアクセスを制限したり、改竄された場合に検知する機能を持つファイルシステムである。

これらの対策技術を、図 3.2b.2-5 に示す想定侵入経路（①～⑦）毎に、図 3.2b.2-4 自動走行の機能モデル図上のどの箇所に施すべきなのかを検討した。

それが、図 3.2b.2-2 自動走行システムアーキテクチャでどの箇所にあたるのかを整理し、対策概要を表としてまとめた。

【①タイヤ空気圧監視への対策】

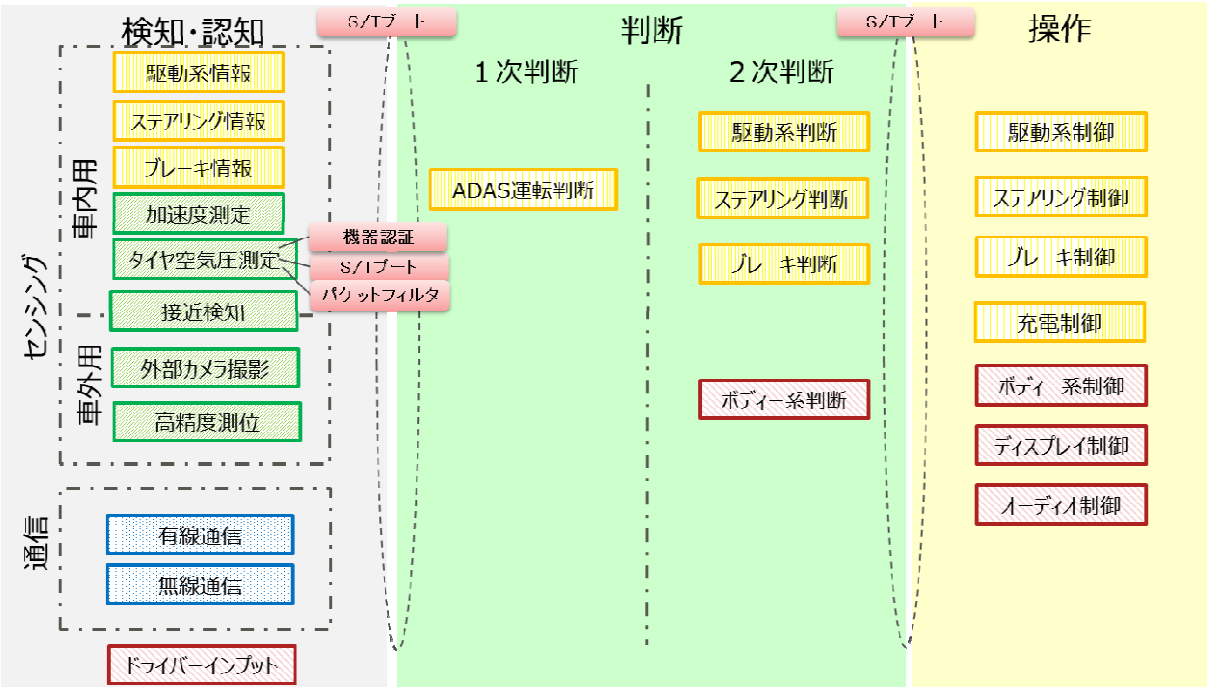


図 3.2b.4-1　タイヤ空気圧監視への対策概要

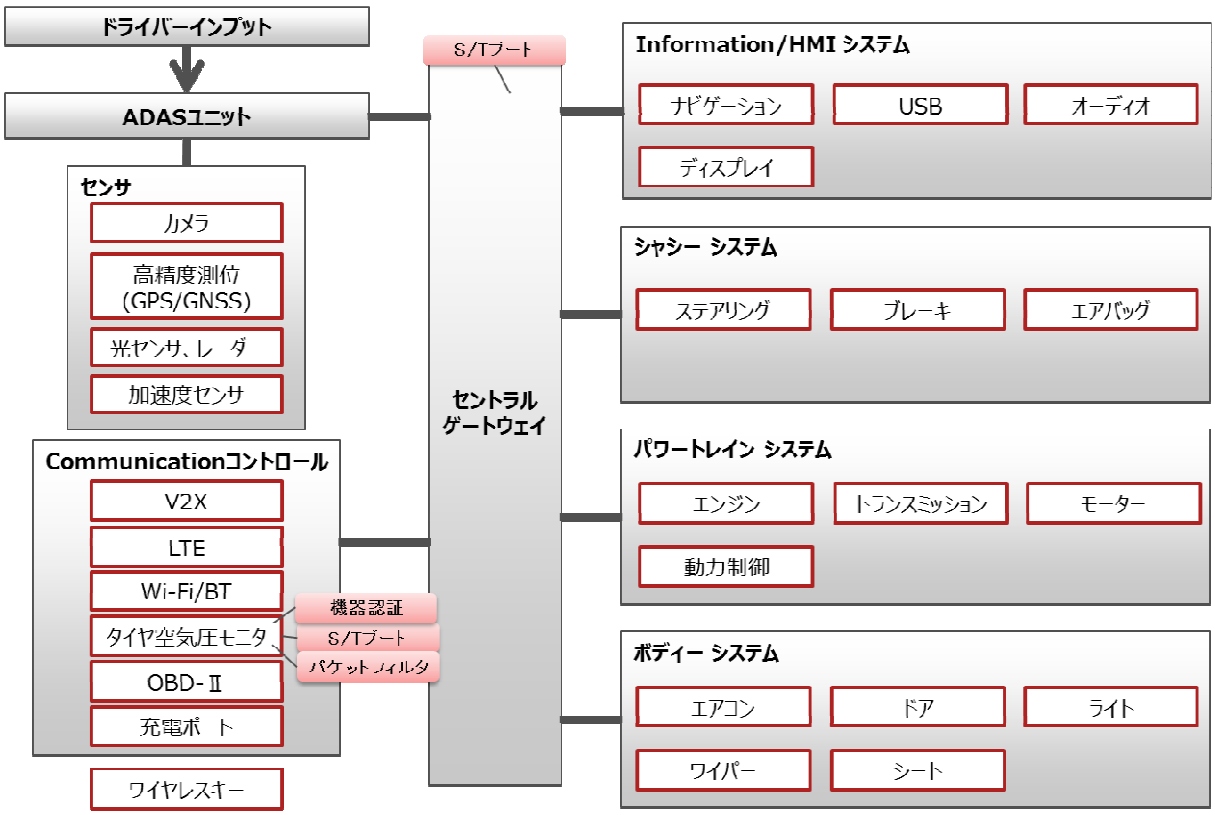


図 3.2b.4-2　タイヤ空気圧監視への対策概要（HW）

表 3.2b.4-2　タイヤ空気圧監視への対策概要（HW）

対策手法	対象	対象によって得られる効果
機器認証	タイヤ空気圧測定	正しいタイヤ空気圧監視用機器が接続されたか認証する
セキュアブート トラステッドブート	タイヤ空気圧測定	タイヤ空気圧監視用機器のプログラムの正当性を検証する
セキュアブート トラステッドブート	セントラルゲートウェイ	セントラルゲートウェイのプログラムの正当性を検証する
パケットフィルタ	タイヤ空気圧測定	急激なパケット増加を監視する

【②接近検知への対策】

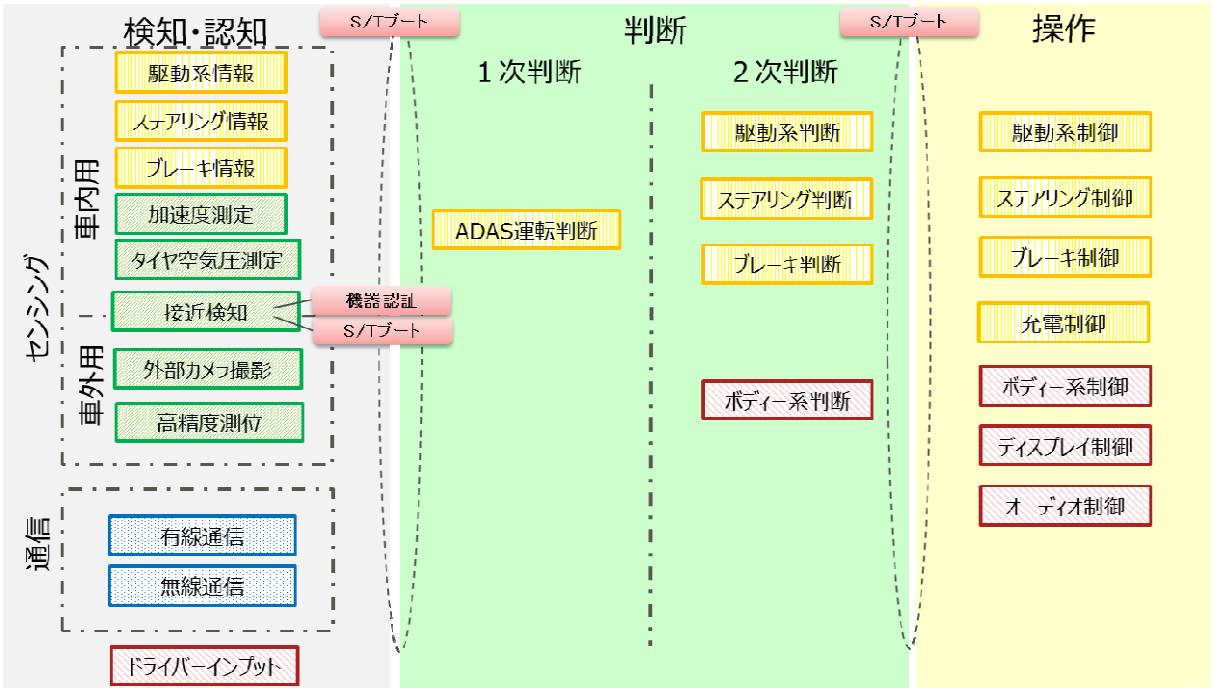


図 3.2b.4-3　接近検知への対策概要

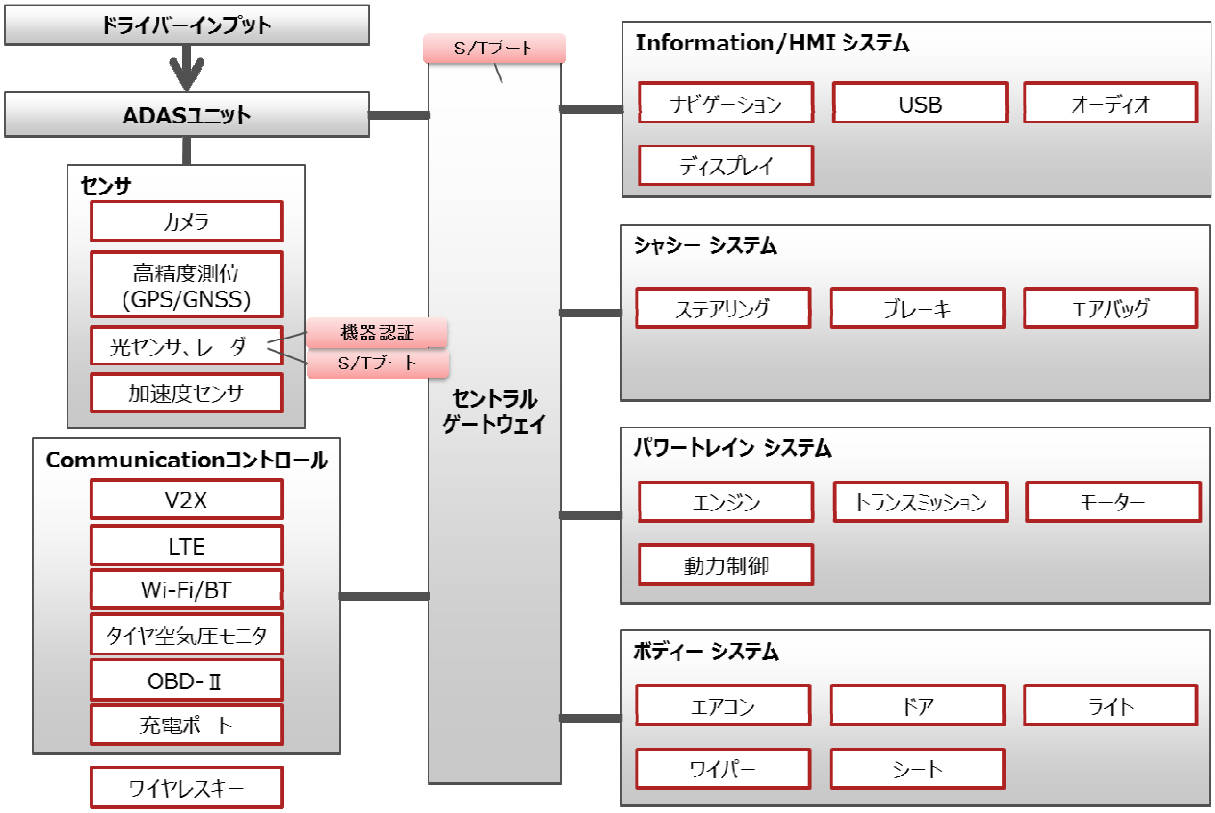


図 3.2b.4-4　接近検知への対策概要（HW）

表 3.2b.4-3　接近検知への対策概要（HW）

対策手法	対象	対象によって得られる効果
機器認証	接近検知	正しいドライバ所持端末が接続されたか認証する
セキュアブート トラステッドブート	接近検知	接近検知用機器のプログラムの正当性を検証する
セキュアブート トラステッドブート	セントラルゲートウェイ	セントラルゲートウェイのプログラムの正当性を検証する
パケットフィルタ	接近検知	急激なパケット増加を監視する

【④高精度測位への対策】

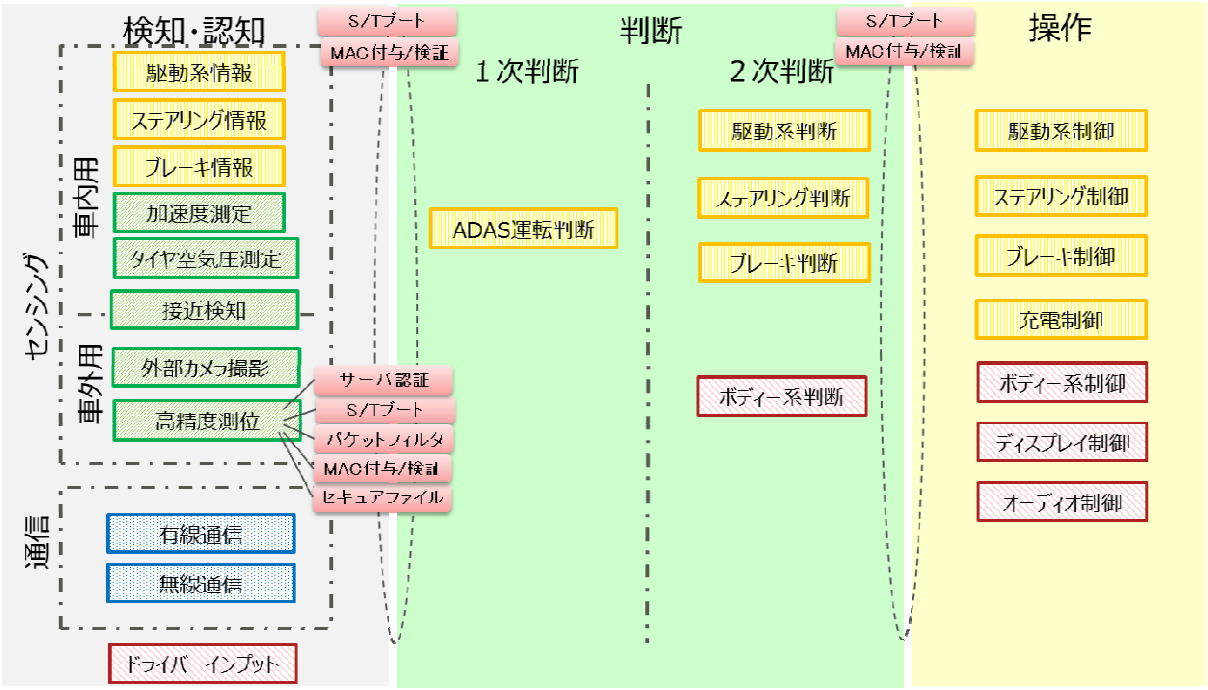


図 3.2b.4-5　高精度測位への対策概要

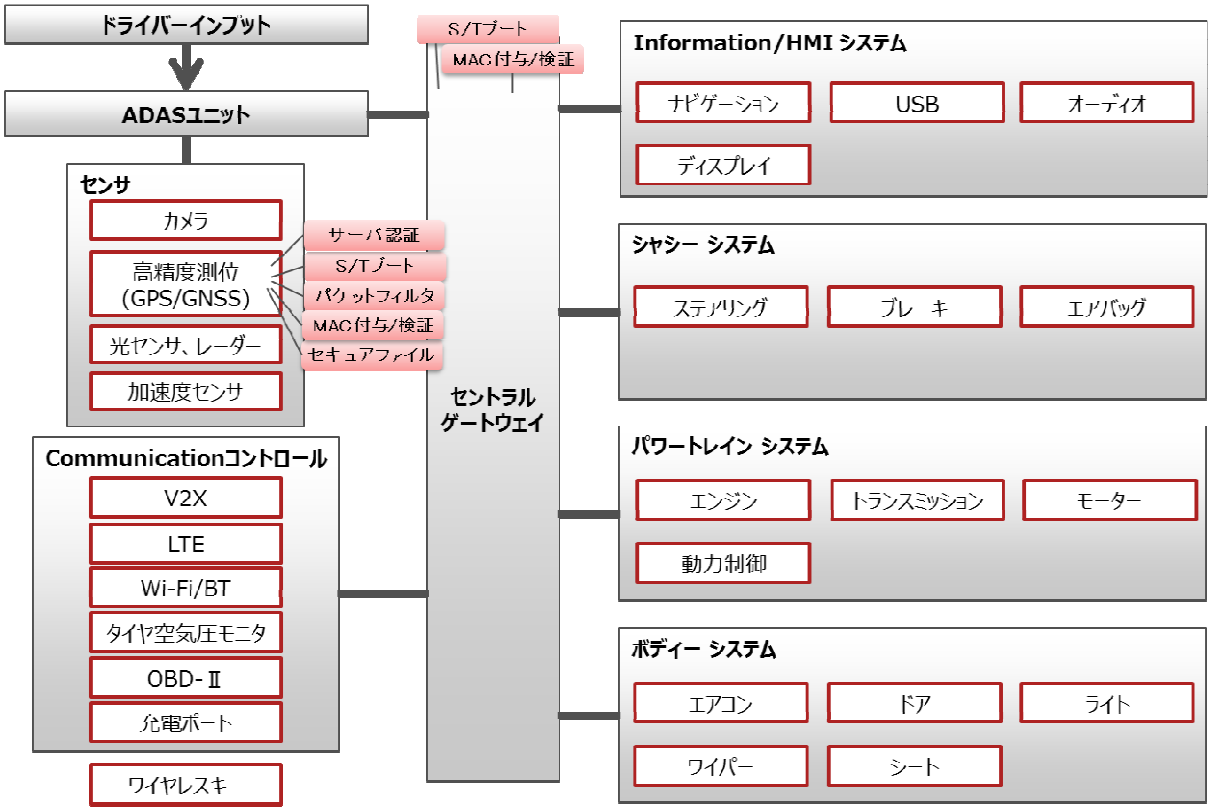


図 3.2b.4-6　高精度測位への対策概要（HW）

表 3.2b4-4　高精度測位への対策概要（HW）

対策手法	対象	対象によって得られる効果
サーバ認証	高精度測位に接続されるサーバ	中間者攻撃等による偽サーバからの接続を防ぐ
セキュアブート トラステッドブート	高精度測位	高精度測位のプログラムの正当性を検証する
セキュアファイルシステム	高精度測位	高精度測位の所持するルート証明書の改ざんを防ぐ
MAC 付与/検証	高精度測位とセントラルゲートウェイ間	メッセージの完全性を検証する
セキュアブート トラステッドブート	セントラルゲートウェイ	セントラルゲートウェイのプログラムの正当性を検証する
パケットフィルタ	高精度測位	急激なパケット増加を監視する

【⑤有線通信への対策】

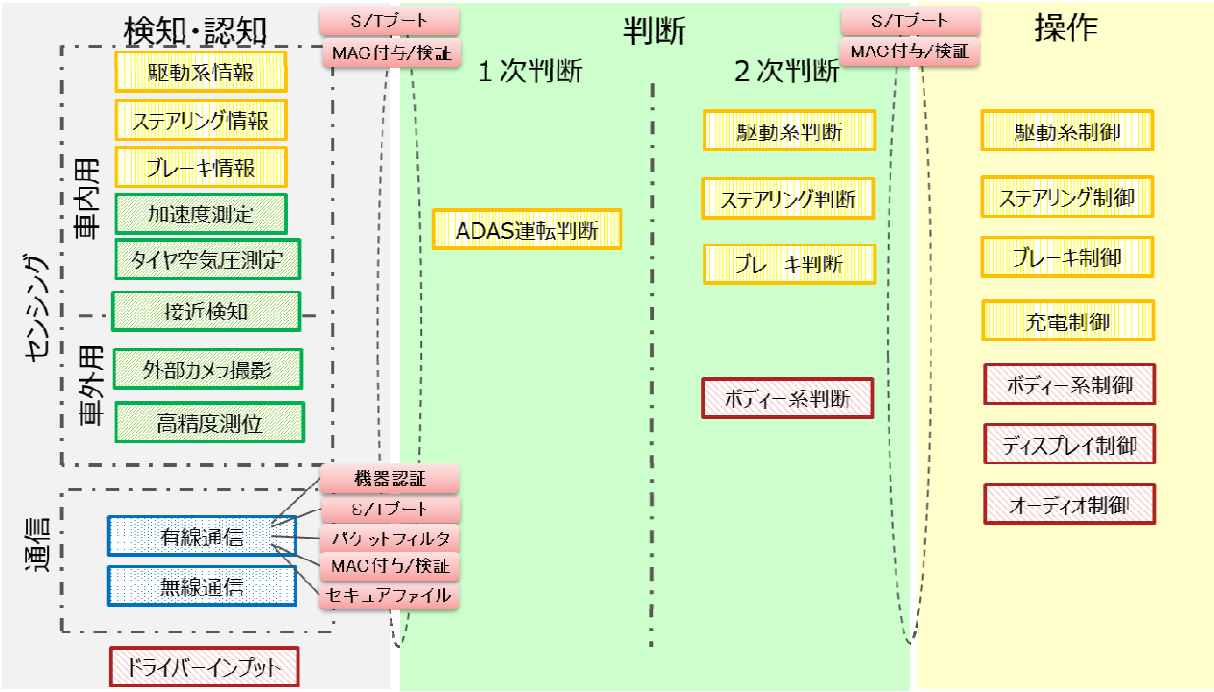


図 3.2b.4-7　有線通信への対策概要

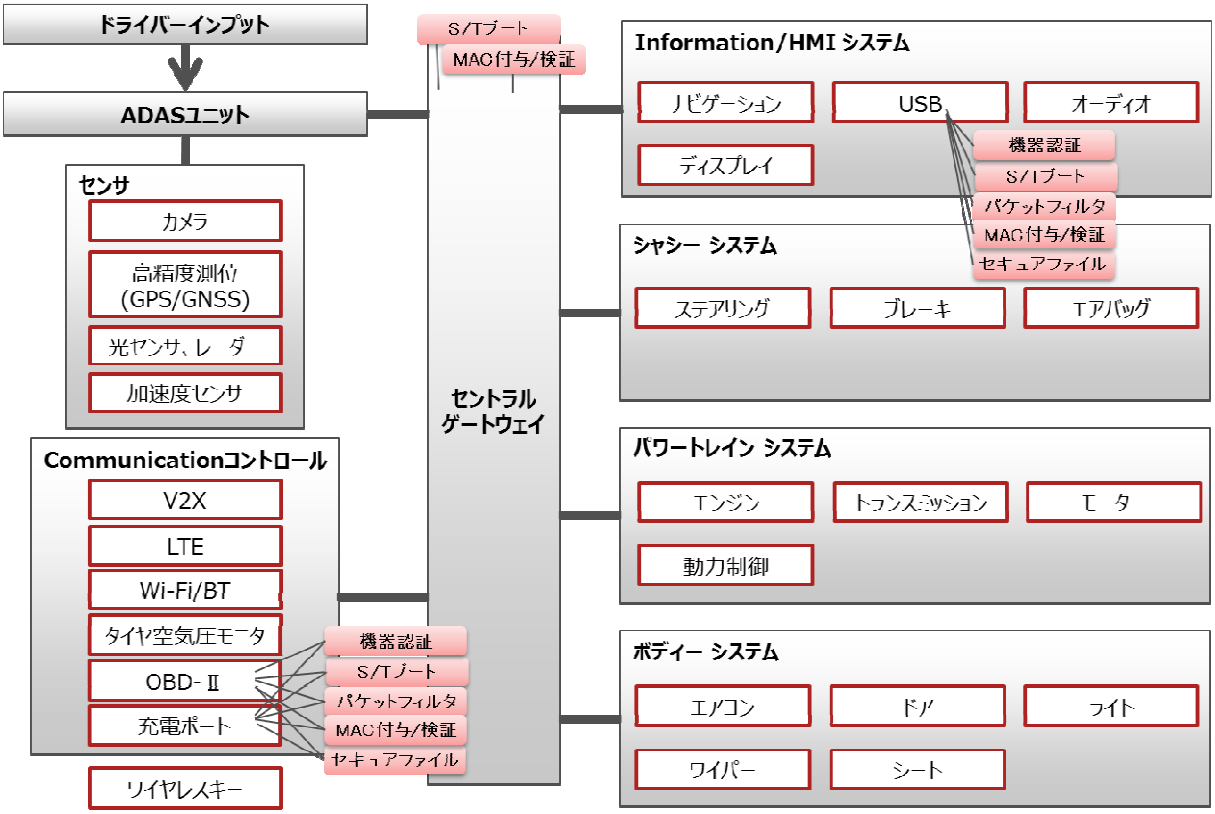


図 3.2b.4-8　有線通信への対策概要（HW）

表 3.2b.4-5　有線通信への対策概要（HW）

対策手法	対象	対象によって得られる効果
機器認証	有線通信	偽端末が接続されたかを検知する
セキュアブート トラステッドブート	有線通信	有線通信のプログラムの正当性を検証する
セキュアファイルシステム	有線通信	接続端末との認証データの不正改ざんを防ぐ
MAC 付与/検証	有線通信とセントラルゲートウェイ間	メッセージの完全性を検証する
セキュアブート トラステッドブート	セントラルゲートウェイ	セントラルゲートウェイのプログラムの正当性を検証する
パケットフィルタ	高精度測位	急激なパケット増加を監視する

【⑥無線通信への対策】

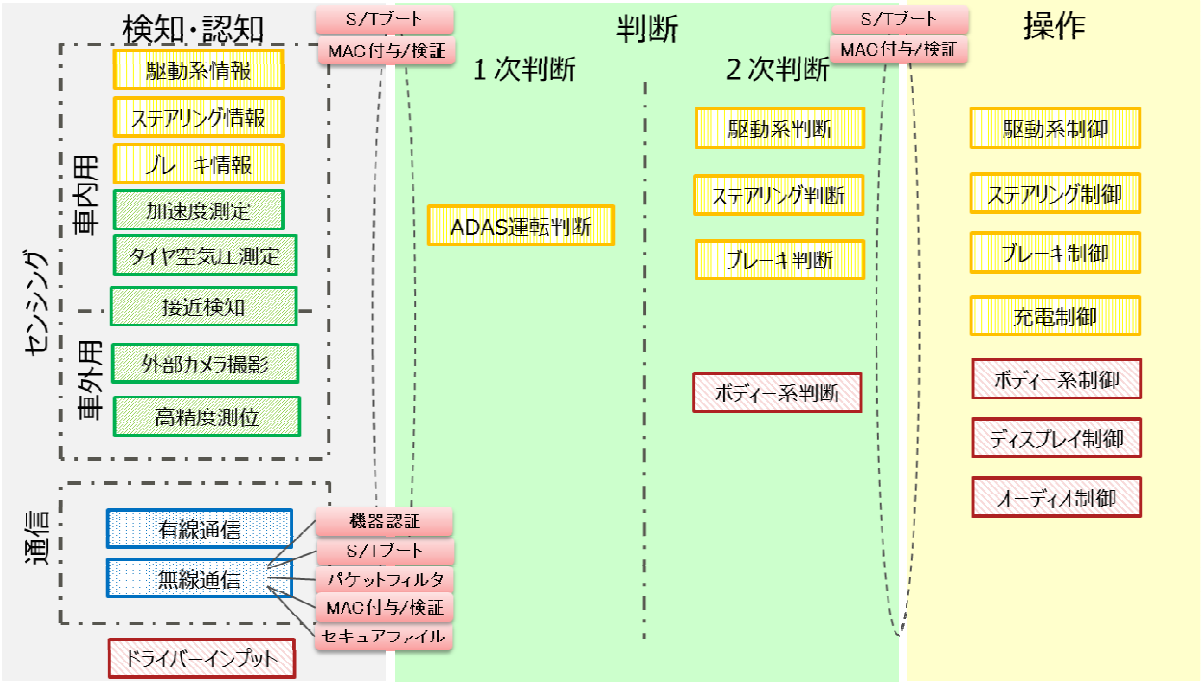


図 3.2b.4-9　無線通信への対策概要

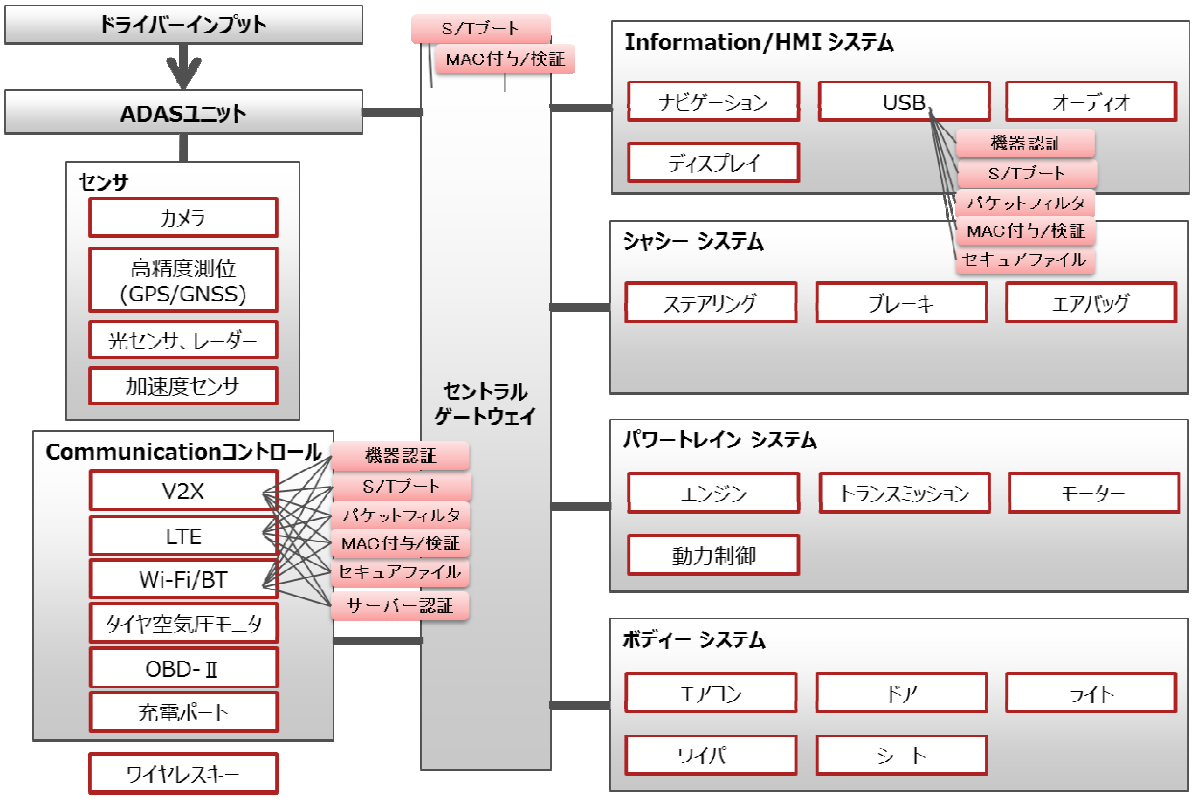


図 3.2b.4-10　無線通信への対策概要（HW）

表 3.2b.4-6　無線通信への対策概要（HW）

対策手法	対象	対象によって得られる効果
サーバ認証	無線通信に接続されるサーバ	中間者攻撃等によって偽サーバに接続されるのを防ぐ
セキュアブート トラステッドブート	無線通信	無線通信のプログラムの正当性を検証する
セキュアファイルシステム	無線通信	ルート証明書の不正改ざんを防ぐ
MAC 付与/検証	無線通信とセントラルゲートウェイ間	メッセージの完全性を検証する
セキュアブート トラステッドブート	セントラルゲートウェイ	セントラルゲートウェイのプログラムの正当性を検証する
パケットフィルタ	無線通信	急激なパケット増加を監視する

【⑦全ての CAN バスへの対策】

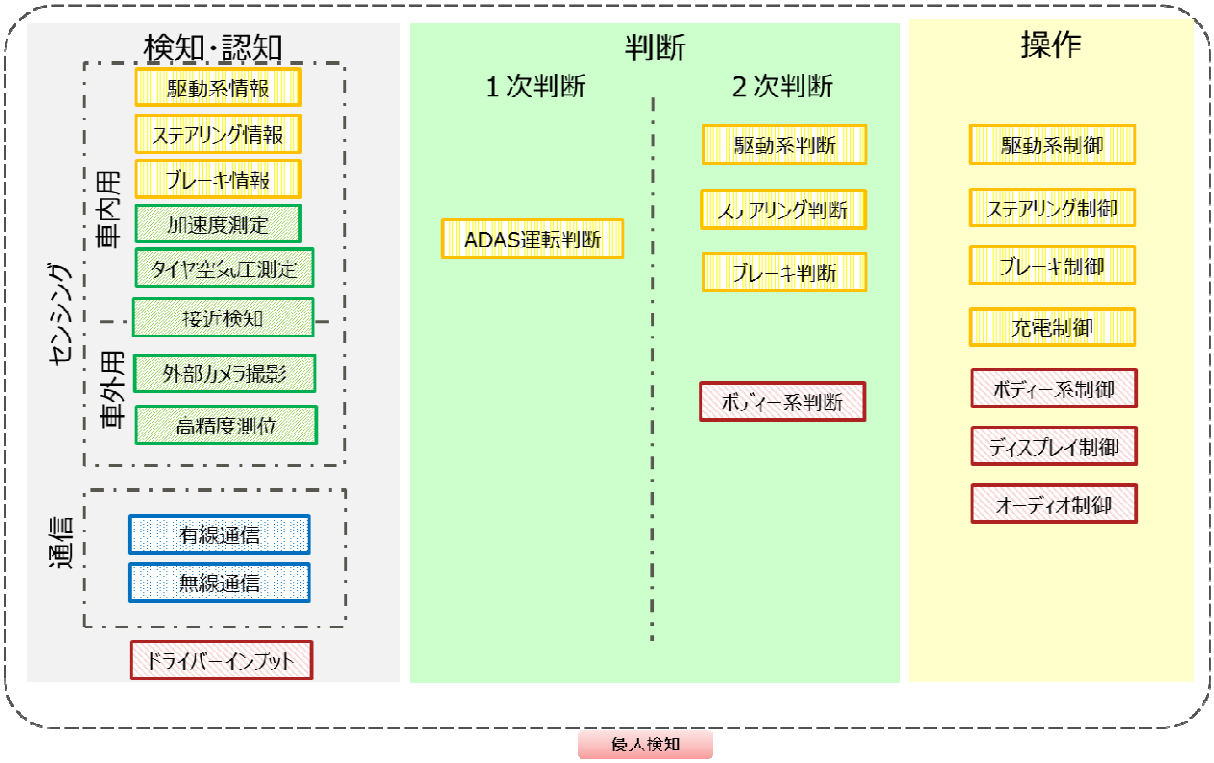


図 3.2b.4-11　全ての CAN バスへの対策概要

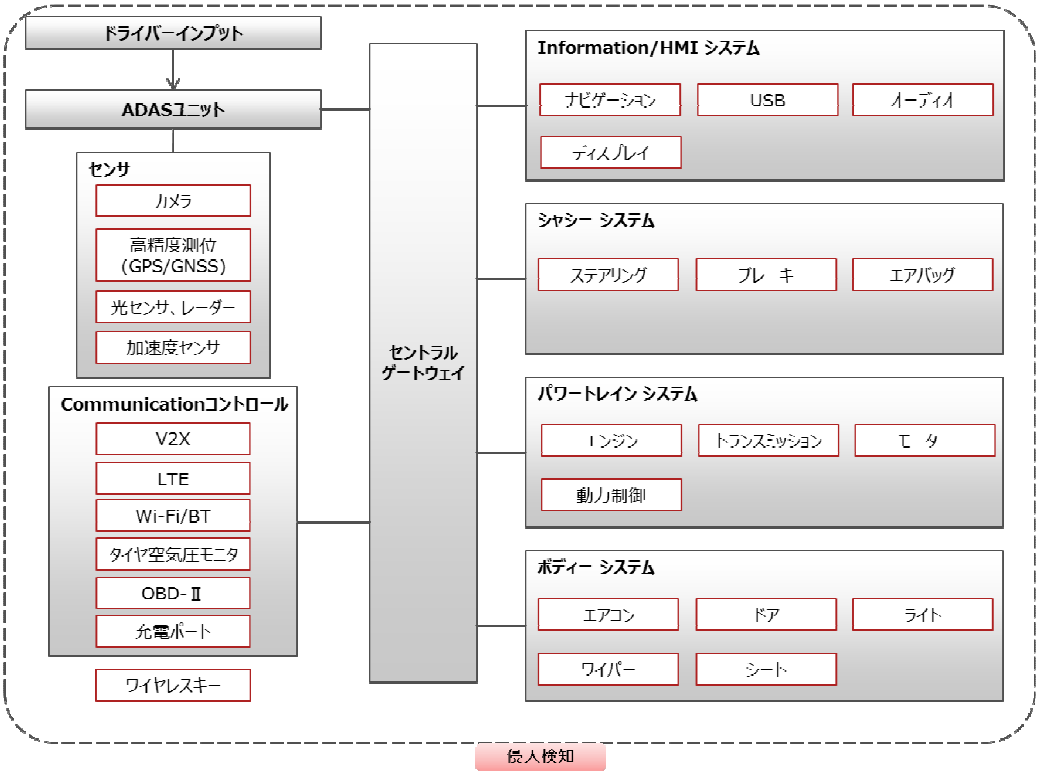


図 3.2b.4-12　全ての CAN バスへの対策概要（HW）

表 3.2b.4-7　全ての CAN バスへの対策概要（HW）

対策手法	対象	対象によって得られる効果
侵入検知	各バス	不正端末がバスに直接取り付けられたかを検知する

各侵入口に対する対策手法の検討結果を踏まえ、想定される車載 LAN アーキテクチャ全域に対する対策は以下の通りと判断した。

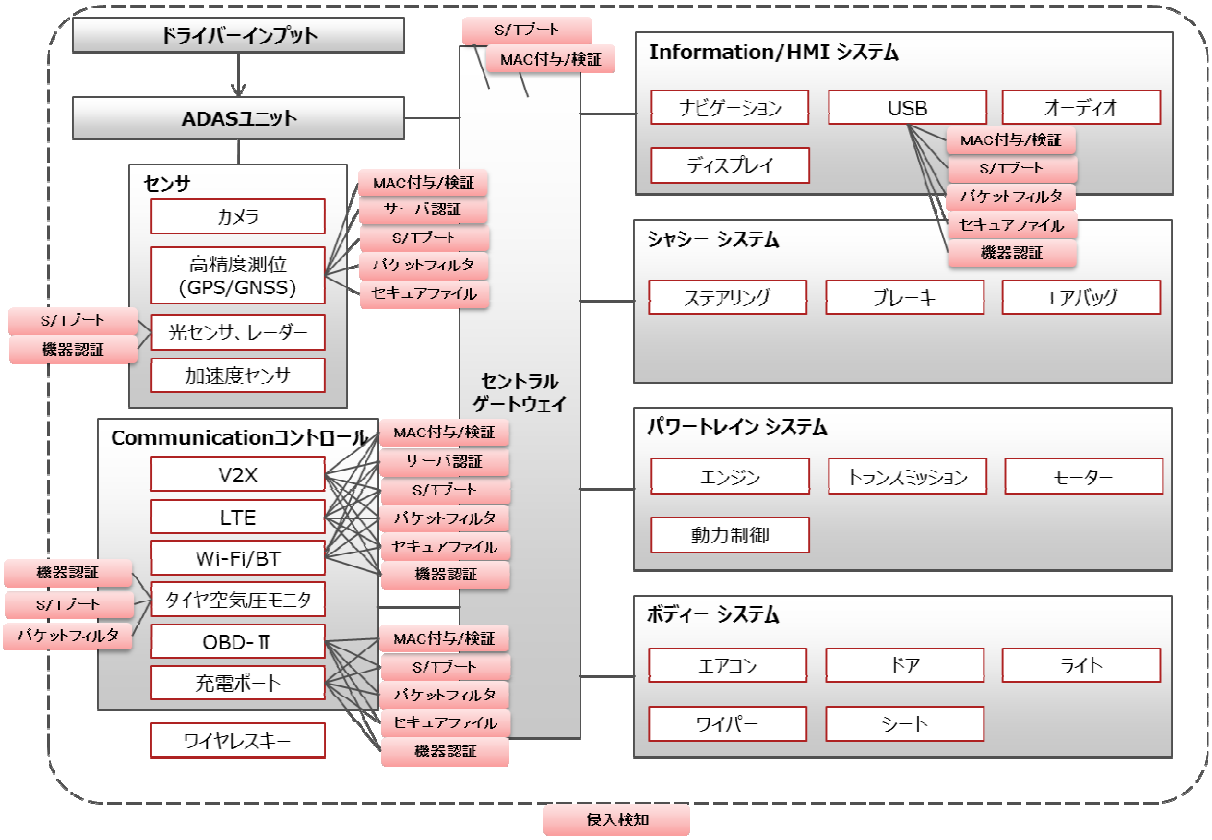


図 3.2b.4-13　車載 LAN アーキテクチャ全域に対する対策

(2) まとめ

本節では、評価指針の確立を目的に、モデル図と分析を行った脅威を利用して、対策すべきポイントと、対策要件の策定を行った。まず、対象となるシステムを機能単位で構成したモデル図を利用して分析を行った。実際の車両では機能を実現するブロックが複数の装置で構成されるケースもあるため、機能間の全ての情報の装置機能について脅威分析、対策検討を行うことで網羅的にセキュリティ分析を行うことができる。

これらの分析結果より導き出された対策は、車両システムを安全に保つために必要となる。しかし一方で、ICT の世界では各侵入経路を単体で対策する、いわゆる水際防御では防ぐことができない攻撃も多発しており、システムに侵入されたときに被害を最小限にと

どめるために内部でも階層的に対策を施すのが一般的となっている。

このようなセキュリティ対策概念は多層防御と呼ばれ、IPA の「ウイルス感染を想定したセキュリティ対策と運用管理を」という注意喚起においても推奨されている。近年のシステムの複雑化により、車両システムに対してもこの多層防御の概念が必要となってくると言える。

ICT の多層防御は、非常に広い範囲で多層化が行われており、システムの重要度（保護資産の重要度）に応じて、どこまで、どのような対策を行うのか（どれだけコストをかけるのか）が決まってくる。

例えば、図 3.2b.4-14 のようにシステムの入口、内部、出口の各層で複数の対策が行われており、さらにシステムのモニタリング、ログの採取、従事者の教育や訓練、装置が設置されている場所の入出室管理など物理的な対策までも含めて、広範囲な多層階層に渡って行われている。

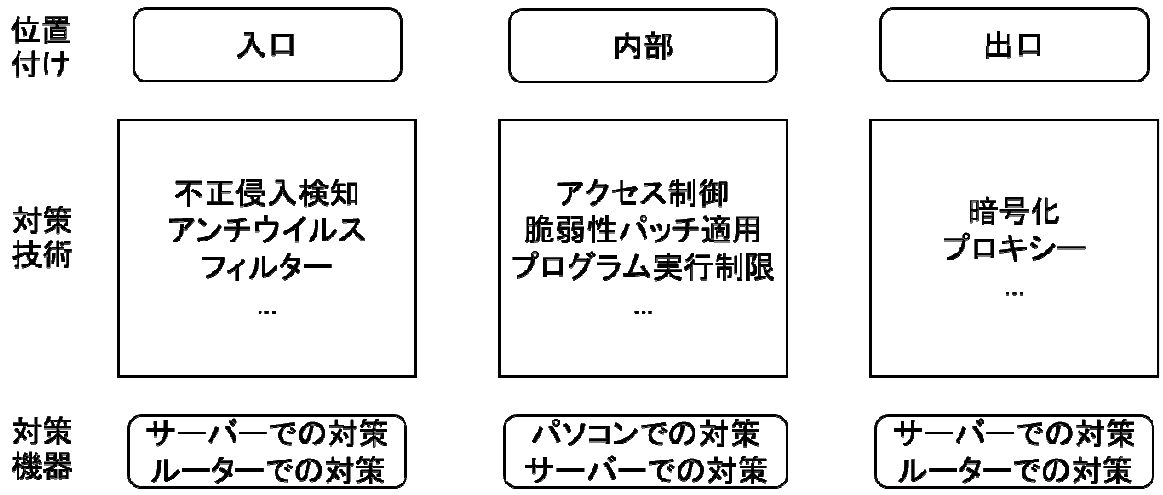


図 3.2b.4-14　ICT での多層防御の例

この多重防御の考え方を車両レベルのセキュリティに適用すると、以下のように考えることができる。

セキュリティ対策は破られる可能性があることを前提に考えると、まずは ECU での対策や外部接続機器のセキュリティ対策が破られ、システム内に侵入されたことを検知することが必要になる。

未知の攻撃に対してはふるまい検知を行うことが有効とされているが、侵入検知に用いるシステムの挙動や情報は多岐にわたり、車両の実装アーキテクチャにも依存する。

よって、今後は攻撃を効率的に検知する技術開発と、それを評価する指標が求められると考える。

3.2c　車内通信プロトコルの仕様に基づく評価方法の検討

自動走行に向けて運転支援システム等が高度化することに伴い、これまで以上に車両内の ECU やセンサ等のコンポーネントが協調動作することの重要性が増してくる。この協調動作には車内のネットワークとコンポーネント間の通信を欠かすことができず、当該ネットワーク上の通信プロトコルがより重要な役割を担い、車内で多く利用されると考えられる。従来の車内ネットワークの通信プロトコルを対象とした研究では、特定の通信プロトコルの攻撃方法のみが検討の対象となっており、自動走行時代に利用されることが予測される通信プロトコルの評価方法・評価基準の調査および検討はほとんど行われておらず、脆弱性の有無および評価方法・評価基準は明らかになっていなかった。また、既知の脆弱性や攻撃方法を評価することが可能な評価環境は確立されていなかった。そのため、自動車に対するサイバー攻撃により、車内ネットワークの通信プロトコルがどのような影響を受けるかを明らかにすることは、自動走行時代の車両のセキュリティ対策を考える上で必要である。そこで、自動走行時代に主流になることが予測される車内ネットワークの通信プロトコルを主な対象とし、通信プロトコルのセキュリティ対策を評価することが可能な評価環境の開発に必要となる要件を検討するために、公開情報を基に下記の調査を実施した。

・通信プロトコル仕様の調査（3.2c.1）
イーサネット等の IT 分野で利用されている通信プロトコルと、車内ネットワークの通信プロトコルとの相違点や類似点を確認し、評価方法を検討する際の材料とするために、6 種類の車内ネットワーク（CAN、CAN-FD、LIN、CXPI、SENT、PSI-5）の通信プロトコルの仕様の調査・整理を実施した。

・通信プロトコルのアプリケーションにおける処理方法の調査（3.2c.2）
上記通信プロトコルの仕様には規定しておらず、車載マイコン独自の実装方法を整理し、評価方法を検討する際の材料とするために、各通信プロトコルを処理できる市販の車載マイコンを数種類ずつ調査した。

・通信プロトコルにおける既存の脆弱性および攻撃方法の調査（3.2c.3）
情報セキュリティに関連する国際会議・学会のうち、自動車セキュリティ関連技術の発表が多いと予測される 7 会議に関して調査を実施し、攻撃方法の傾向を分析した。

3.2c.1　通信プロトコルの仕様の調査

車内ネットワークの通信のために、目的や特徴に応じて様々な通信プロトコルが考案され標準化されている。今回は、自動走行時代に利用されると思われる通信プロトコルの中から、自動車の制御系に用いられる可能性があり、万が一攻撃を受けた場合に自動走行やその安全性に支障をきたす恐れが考えられる通信プロトコルを中心にプロトコル仕様の調査を実施した。
調査対象として選定した 6 種類の通信プロトコルは以下の通りである。

・主に制御系で用いられ、自動車の各機能を電子制御する ECU 間の通信に主に用いられる CAN、およびそれを高速化した CAN-FD
・制御系のサブバスで用いられ、自動車内部のセンサと ECU 等の制御ユニット間におけるセンサ信号をデジタル化して伝達する SENT、およびそれらがより高い信頼性が必要となる場合に利用される PSI5
・ボディ系のサブバスと一部制御系にも用いられ、パワーウィンドウ、ミラー調整、ドアロックなどのボディ制御に利用されている LIN、及びそれよりも応答性や信頼性を高めた CXPI

これらの通信プロトコルについて、メッセージ送受信方法の概要やメッセージの構造等をまとめる。

(1) CAN 通信プロトコルの仕様

① CAN プロトコルの概要

ここでは CAN の概要を述べる。CAN は自動車の各機能を電子制御する装置 ECU 間の通信に採用されている通信プロトコルである。1980 年代に Bosch 社によって提唱され、1994 年に ISO 化された。2016 年 3 月現在 ISO の規格は全 6 章から構成されており、CAN は OSI 参照モデルのうち、レイヤ 1：物理層、レイヤ 2：データリンク層を規定している（図 3.2c.1-1）[1] [2] [3] [4] [5] [6]。物理層の構成によって最大 125K～1Mbps 程度の速度で通信できる。主にデータリンク層に関わる CAN の特徴について報告する。

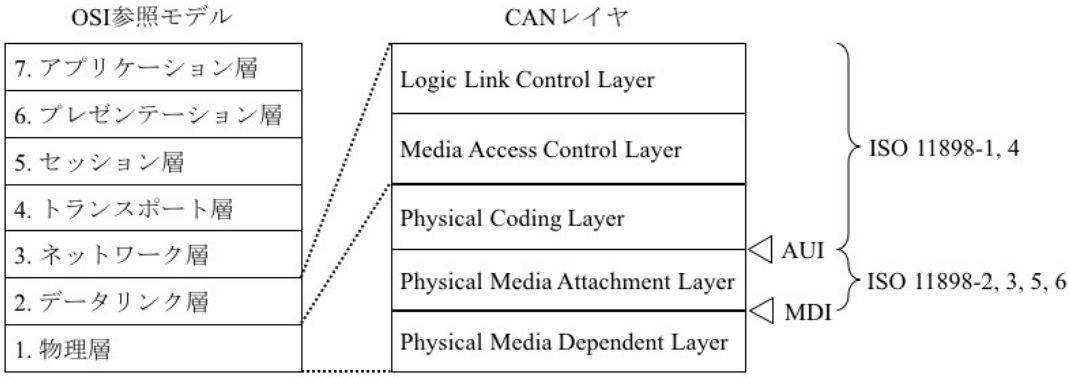


図 3.2c.1-1　CAN プロトコルが規定するレイヤ

② CAN プロトコルの特徴

CAN プロトコルには以下の 6 つの特徴が挙げられる。以降、それぞれの特徴について個別に説明する。なお一般的にネットワークに接続する通信機器をノードと呼び、CAN の場合は主として ECU がノードを意味する。

(ⅰ) ライン型構造

図 3.2c.1-2 に CAN が採用するライン型のネットワークを示す。CAN はレイヤ 1 にツイストペアケーブル式を採用しており、高い電位を示す物理線を CAN_H、低い電位を示す物理線を CAN_L と呼ぶ。CAN_H と CAN_L とを合わせて 1 本のラインと見做す。このラインを CAN バスと呼ぶ。CAN バスに各ノードを接続するだけでネットワークが構成できる。ライン型の特長はネットワークがシンプルな構造を取ることで設計が容易に行える点である。CAN バス 1 本当たりに接続可能なノード数はレイヤ 1 で規定されている。

CAN では配線設計が完了したネットワークに対しても、規定された接続数の範囲内であれば後からノードを容易に追加することができる。

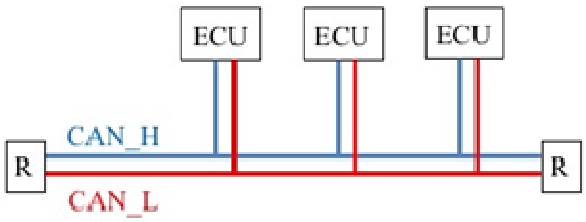


図 3.2c.1-2　CAN ライン型のネットワークトポロジ（R は終端抵抗を表す）

(ⅱ) マルチマスタ方式

CAN では接続するノードに優先順位を設けない。CAN バスにメッセージが流れていない場合は、各ノードが自由にメッセージを送信することができる。これをマルチマスタ方式と呼ぶ。ノードに優先順位を設けない代わりに各ノードが流すメッセージに優先順位を設ける（特徴（v）を参照）。マルチマスタ方式の特長は以下の 3 点が挙げられる。

・各ノードを均一な仕様で設計できる
・各ノードに優劣がないため、イベント指向通信に向いている
・ノードの追加が容易である

(ⅲ) ブロードキャスト方式

CAN が採用するブロードキャスト方式とは、ある 1 つメッセージがあるネットワークに送信された場合、同一ネットワークに接続する全てのノードがそのメッセージを受信し、そのメッセージに対して各ノードが個別に反応することを言う。

(ⅳ) 拡張 CSMA/MD

マルチマスタ方式、マルチキャスト方式を採用する CAN では、異なるノードが同一タイミングで同一 CAN バスにメッセージを送信することが起こりえる。その時複数のメッセージの電気的データが衝突して正しくメッセージが送信できなくなってしまう。そのため、あるメッセージが CAN バスを使用している場合は他のメッセージが送信できないようにする仕組みが CAN では規定されている。CAN では CSMA/CD を採用し、メッセージ

毎に優先順位を規定できるようになっている。具体的には、各ノードはメッセージを送信する前に、そのメッセージよりも高い優先順位のメッセージが他のノードによって CAN バスに流されているかどうかを確認する。そして優先順位が高いメッセージが流れている場合は CAN バスが空くまでメッセージの送信を保留し、その後、再度送信できるか確認してメッセージの送信を実施する仕組みである。

(ｖ) 優先順位付きメッセージ（ID を使用したメッセージアドレッシング）

CAN では 1 つのメッセージをフレームという単位で表現する。前述の優先順位を実現するために、フレームのヘッダには ID が規定されている。CAN プロトコルではメッセージのビット値が 0（ゼロ）を表す電気信号をドミナント信号（dominant：支配的な）と呼称し、1 を表す電気信号をレセシブ信号（recessive：劣性の）と呼称する（図 3.2c.1-3）。その名のとおり、あるノードがドミナント信号を CAN バスに送信した場合、同時に他のノードがレセシブ信号を送信したとしても CAN バスに流れる電気信号はドミナントになるように物理的に設計されている。そのためドミナントが連続する ID の優先順位が最も高く、レセシブが連続する ID の優先度が最も低い。メッセージの優先順位の定め方は CAN では規定されていない。例えば、ブレーキの制御に関わるメッセージの CAN ID とステアリングに関わるメッセージの CAN ID とでどちらの優先順位を高く設定するかはその製品の設計思想により規定される。

各ノードは CAN バス全体の電気信号がドミナントかレセシブかを常に観測しており、自身が 1 ビットの電気信号を送信した際に CAN バスの電気信号がドミナントかレセシブかを確認する。確認した結果、例えばあるノードがレセシブの電気信号を CAN バスに送信したにも関わらず CAN バスの電気信号がドミナントであると観測した場合は、他ノードが自ノードのメッセージ ID よりも優先順位の高いメッセージ ID を送信していると判断して自ノードの 2 ビット目以降のメッセージ送信を中止する。優先順位のための一連の処理を調停と呼ぶ。またブロードキャストで送られてきたメッセージが、自ノードが受信するメッセージかどうかを識別する情報としても ID を用いる。

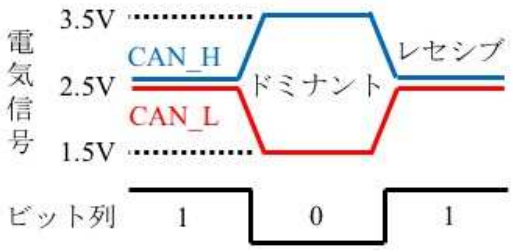


図 3.2c.1-3　CAN の電気信号とビット列

(vi) 不具合抑制

全メッセージがブロードキャストされるネットワークでは、仮にノードがバスにメッセージを流し続けて占有するとネットワーク全体が機能不全を陥ってしまう可能性がある。そのため CAN に接続する各ノードには、

・自身の短時間の不具合（エラー）と長時間のエラーとを識別する機能（I）
・自身が長時間のエラーを発生させるノードであると判断した場合は自ら CAN ネットワークから離脱（メッセージの送受信を停止）する機能（II）
・エラーを検出したことを他ノードに通知する機能（III）

が搭載されている。

まず前述の不具合抑制機能（I）ならびに機能（II）に関して説明する。CAN では各ノードが以下のメッセージエラーを検出する。

・ビットエラー：送信ノードが送信したビット値と違う値が CAN バスに流れている状態
・スタッフエラー：受信ノードが 6 ビット以上連続して同じビット値を受信した状態
・CRC エラー：受信ノードが受信メッセージの CRC フィールドのビット値と受信メッセージの CRC を算出したビット値とが異なる状態
・フォームエラー：受信ノードが規定に従っていない値を含むメッセージを受信した状態
・アクノレッジエラー：送信ノードが受信ノードからアクノレッジ（受信を完了したことを意味するドミナント 1 ビットの返信）を受信できなかった状態

図 3.2c.1-4 について、各メッセージエラーを検出する範囲を後述するデータフレームを例として図示する。各ノードは REC と TEC という 2 つのエラーカウンタを内蔵している。上記のエラーを検出すると、その内容によってエラーカウンタの値を増減させる。自ノードのエラーカウンタ数によって CAN ネットワークから離脱するかどうかを自己判断する。エラーカウンタ値に合わせて各ノードは以下の 4 状態を遷移する。

・初期状態：ノードが CAN バスに接続するための初期化が行われる前の状態
・エラーアクティブ：CAN バスに接続している通常のノード状態
・エラーパッシブ：REC または TEC がある程度蓄積した状態。メッセージの送受信は継続して行うことができる。エラーが検出されなければ各カウンタの値は減少し、ある値を下回ればエラーアクティブ状態に遷移する
・バスオフ：TEC が一定以上蓄積した状態。メッセージの送受信を停止する

図 3.2c.1-5 にノードの状態遷移を示す。前述の短時間の障害とはエラーパッシブを指し、長時間の不具合はバスオフを指す。

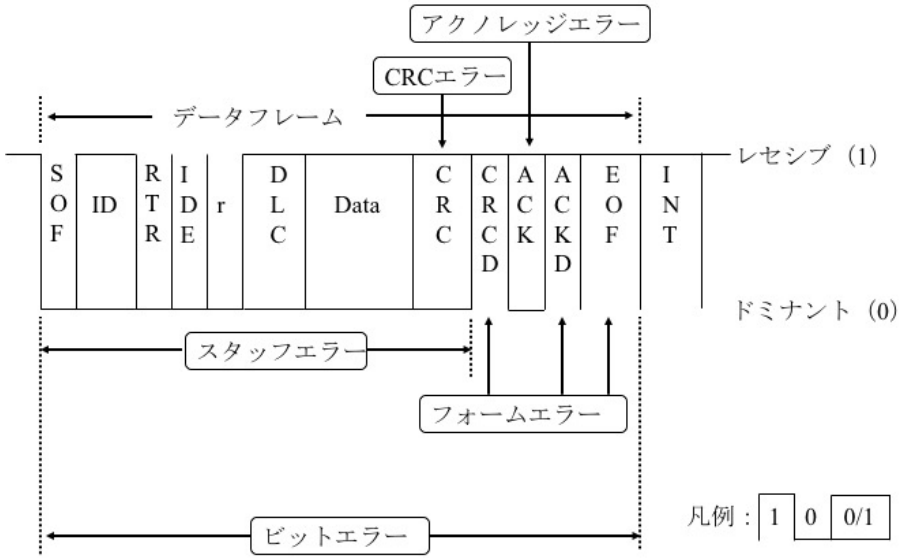


図 3.2c.1-4　CAN メッセージに対するエラー検証範囲

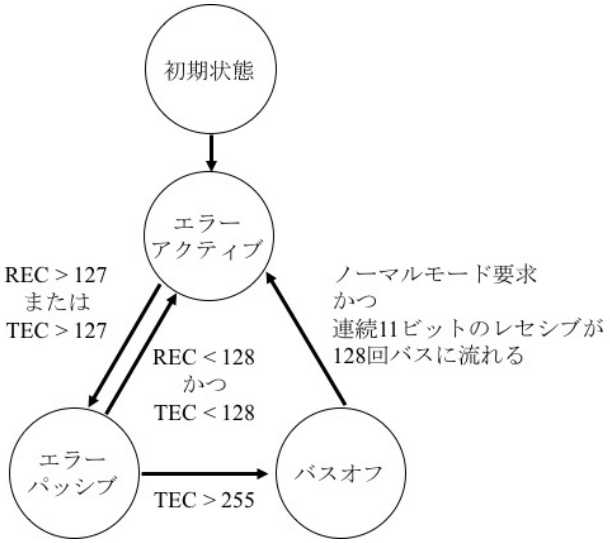


図 3.2c.1-5　エラーカウンタによるノードの状態遷移

つぎに不具合抑制の機能（III）の実現方法について述べる。はじめに、あるノードが自ノードの不具合または CAN バス上のメッセージエラーを観測すると特定のビット列を CAN バスに送信する。特定のビット列が流されると同時に他のノードによってメッセージが送信されている場合、特定のビット列を受け取った送信ノードは直ちにメッセージの送信を中止して、代わりに送信を中止した旨を表すビット列を送信する。送信の中止を表す特定のビット列を受信した全てのノードは中途半端に受信したメッセージを処理することなく破棄する。一定時間が経過した後にメッセージは再送される。

以上の手順によりバスオフ状態以外の全ノードが同じメッセージを同じ順番、タイミングで受信することができる。そのため CAN ではネットワーク全体において受信メッセージが統一される。

(vii) レイヤ毎のプロトコル規定とメッセージフレーム

ここでは前述の特徴を実現するために CAN のレイヤ毎に規定されている事項とメッセージフレームについて述べる。まず CAN レイヤは 5 層に分かれており、前述の特徴を実現しているレイヤは主にデータリンク層に相当する以下のレイヤである（図 3.2c.1-1）。

(viii) LLC レイヤ

ここでは LLC レイヤで規定される機能の概要について述べる。LLC レイヤでは以下 3 つの機能が規定されている。

・フレーム受容選択：ブロードキャスト方式である CAN プロトコルにおいて、フレームを受信したノードはそのフレームが自ノード宛かどうか判断する必要がある。フレームに規定される ID フィールドの値を用いて前述の判断を実施する。
・オーバロード通知：あるノードが受信したフレームの処理に時間を要する場合、そのノードは次のフレームの送信開始を遅延させるために他のノードにオーバロード通知を行う。後述する MAC レイヤのオーバロードフレームを送信することでオーバロード通知とする。CAN プロトコルが策定された時代はノードの処理性能が低かったためオーバロード機能が実際に通信時に用いられていたが、現代のノードは処理性能が向上したためオーバロードフレームを送信することはまれである（1）。
・リカバリ管理：前述のとおり CAN プロトコルは優先順位付きメッセージを採用している。そのため優先順位が低いメッセージは調停に負けてメッセージが最後まで送信されない場合がある。その場合、最後まで送信できなかったメッセージは自動的に再送するというリカバリ機能が規定されている。ただし送信メッセージが調停に負けたら再送しないという設定も可能である。メッセージを再送するかどうかの判断が LLC レイヤで行われる。

(ix) MAC レイヤ

ここでは MAC レイヤで規定される機能の概要、そしてその機能を実現するためのメッセージのフレーム形式について述べる。CAN の MAC レイヤは LLC レイヤの中間に位置し、OSI 標準モデルの MAC レイヤと同様に、

・送受信フレームのカプセル化、脱カプセル化
・信号の誤り検出
・物理層に対する送受信の方法やフレーム形式の規定

といった機能を実現している。これらの機能は OSI 参照モデルを準拠する一般的な通信プロトコルの MAC レイヤにおいて規定されている機能と同一であるため、CAN プロトコルの MAC レイヤにおける各機能の詳細は報告を省略する。つぎに、CAN の MAC レイヤでは以下 5 種類のメッセージフレームが規定されている。なお、フレーム内の各フィールドの説明は省略する。

・（通常）データフレーム：0～64 ビットのデータを送信するために用いる、CAN における基本フレームである（図 3.2c.1-6）。

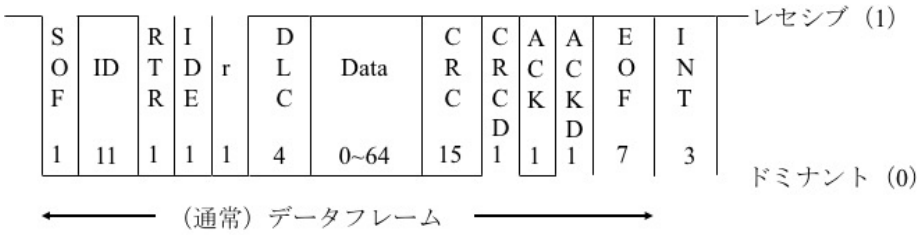


図 3.2c.1-6　（通常）データフレーム

・拡張データフレーム：（通常）データフレームと同様に 0～64 ビットのデータを送信するために用いるフレームである（図 3.2c.1-7）。（通常）データフレームの CAN ID は 11 ビットであり、拡張データフレームの CAN ID は ID と ID Ex を合わせて 29 ビットである。

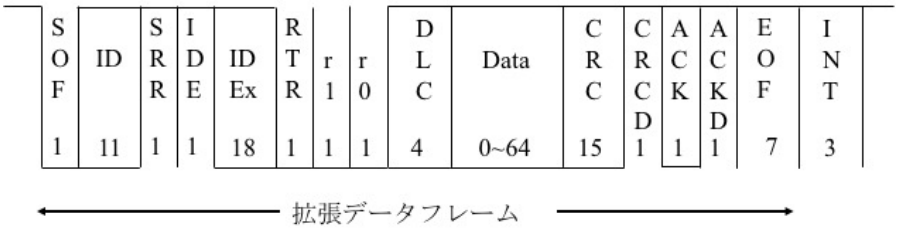


図 3.2c.1-7　拡張データフレーム

・リモートフレーム：データフレームの送信を他のノードに要求するために用いるフレームである（図 3.2c.1-8）。ただしリモートフレームは CAN を用いる現代のシステムではほとんど使われていない。それは、リモートフレームを用いずとも CAN によるノード間の通信は円滑に行えることに加えて、リモートフレームを用いない分だけバスの占有率を下げられるからである。リモートフレームを通信の基点とするとデータをやりとりするためにリモートフレームとデータフレームの 2 フレームが必要になる。しかしデータフレームを適切なタイミングで定期的に送信するようノードを設計すれば、リモートフレームは必ずしも必要ではない。

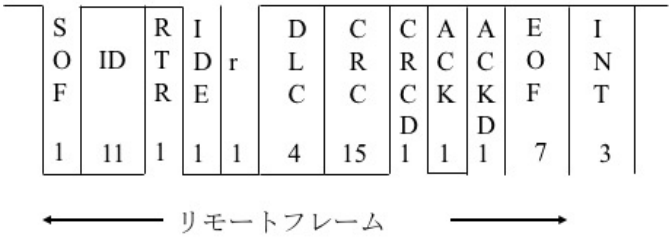


図 3.2c.1-8　リモートフレーム

・オーバロードフレーム：ノードが前回受信したフレームの処理を終えていない場合、次に送られてくるフレームの送信開始を遅延させるために用いるフレームである（図 3.2c.1-9）。ただしオーバロードフレームは現代の CAN を用いる現代のシステムではほとんど使われない。それは、CAN プロトコルが提唱された当時と比較してノードの処理性能が飛躍的に向上したため、次のフレームを受信する前にフレームを処理し終えることができるようになったからである。

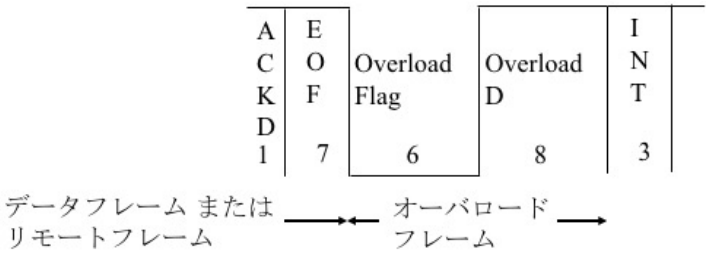


図 3.2c.1-9　オーバロードフレーム

・エラーフレーム：通信中に各種のエラーが発生した場合に用いるフレームである（図 3.2c.1-10）。図 3.2c.1-4 のとおり各種のエラーをノードが検出したとき、エラーフレームが送信される。

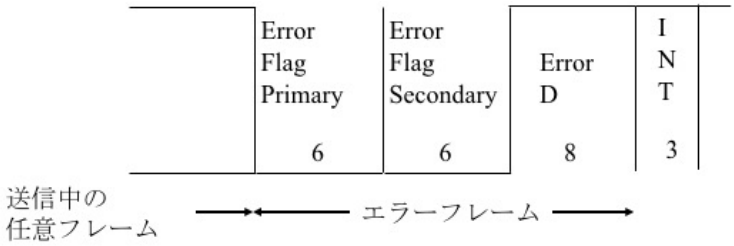


図 3.2c.1-10　エラーフレーム

(2) CAN-FD 通信プロトコルの仕様

ここでは車内通信プロトコル CAN-FD の仕様について述べる [1] [7]。CAN-FD は CAN プロトコルと多くの部分が同一の仕様である。CAN プロトコルで規定されている語句については、ここでは説明を省略する。

① CAN-FD プロトコルの概要

ここでは CAN-FD について車内通信プロトコル CAN と比較してその概要を述べる。2012 年 3 月に Bosch によって CAN-FD が発表されて仕様が公開された。そして CAN のデータリンク層に関する標準 ISO 11898-1:2003 に加筆される形で、CAN-FD は 2015 年 12 月に ISO 11898-1:2015 として標準仕様が公開された。

CAN-FD が策定された経緯は以下の通りである。自動車の高機能化に伴い車内ネットワ

ークに流れるデータ量は増加し続けていた。そのため CAN の最大通信速度では今後製品の要件を満たすことができない可能性が指摘されるようになった。2000 年頃規定された車内通信プロトコル FlexRay は CAN の最大通信速度を遙かに上回るものの製造コストが高いため CAN の代替にはなっていない。また FlexRay のタイミングトリガ形式の通信方式は車内通信プロトコルとして万能ではない。そのため Bosch は、CAN と代替可能な製造コストかつ CAN の特徴を活かしつつ CAN の最大通信速度を上回る車内通信プロトコルを検討し CAN-FD として策定するに至った。

② CAN-FD プロトコルのフレーム形式

CAN-FD の MAC サブレイヤにおいて独自のフレームとして以下の 2 通りが規定されている。

・データフレーム（標準フォーマット）
・データフレーム（拡張フォーマット）

一方 CAN プロトコルではフレームが 5 通り規定されている。そのうち CAN のデータフレーム（標準フォーマット）および CAN のデータフレーム（拡張フォーマット）の 2 通りについて、CAN-FD のデータフレームが対応関係にある。CAN で規定されている、リモートフレーム、オーバロードフレーム、エラーフレームの 3 通りは CAN-FD で新たに規定していない。CAN-FD ではリモートフレームはサポートしておらず、オーバロードフレームとエラーフレームは CAN と同一である。以下に CAN-FD で規定されるデータフレームについて述べる。

(ｉ) データフレーム（標準フォーマット）（図 3.2c.1-11）

CAN の特徴を活かしつつ CAN の最大通信速度を上回るために、1 フレームあたりの Data フィールドのサイズ上限を拡張し、CAN メッセージと調停が可能であり、CAN よりも高速に通信可能な可変ビットレートを採用した。そのために CAN と CAN-FD とでは、SOF 以降から CRC までのフィールド構造が異なる。

まず Data フィールドより前つまり調停に用いられる領域について、CAN では SOF(1)、ID(11)、RTR(1)、IDE(1)、r(1)、DLC(4)と規定されている。(　)内の数字はビット長を表し、合計 19 ビットである。一方 CAN-FD は図 3.2c.1-11 の通りであり合計 22 ビットで EDL、BRS、ESI の 3 ビットが追加されている。EDL は CAN メッセージと CAN-FD メッセージを識別するビットである。CAN では予約ビット r が EDL と同位置でドミナントとして規定されており、CAN-FD では EDL がレセシブとして規定されている。BRS は当該フレームが可変ビットレートかどうかの識別に用いる。BRS がレセシブであれば可変ビットレートで送信されることを意味する。ESI は CAN FD を用いるノードのエラー状態を識別する際に利用するビットとして規定されている。

次に Data フィールド以降について、CAN は 0～64 ビットと規定され CRC フィールドは 15 ビットで固定値と規定されているのに対して、CAN-FD は Data フィールドが 0～512 ビ

ットと規定され、Data フィールドの長さに合わせて CRC は 17～21 ビットと規定されている。

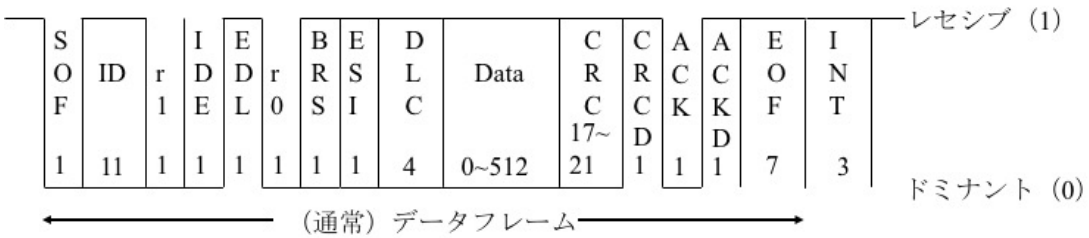


図 3.2c.1-11　CAN-FD データフレーム（標準フォーマット）の各フィールド

(ⅱ) データフレーム（拡張フォーマット）（図 3.2c.1-12）

CAN のデータフレームについて ID のビット長を拡張したデータフレーム（拡張フォーマット）が存在することと同様に、CAN-FD においても ID のビット長を拡張したデータフレームが規定されている。

図 3.2c.1-12　CAN-FD データフレーム（拡張フォーマット）の各フィールド

③ CAN-FD プロトコルの特徴

前述のとおり CAN-FD は CAN の仕様である ISO 11898-1:2015 に内包される形式で規定されており、仕様の大部分は CAN と同一である。具体的には物理層は CAN と同一で良い。そのためここでは OSI 参照モデルのデータリンク層における CAN-FD に固有の特徴について述べる。CAN-FD の特徴は大別して以下の 3 点が挙げられる。各特徴について以下に詳細を述べる。

・可変ビットレート

CAN は固定ビットレートの通信プロトコルである。一方 CAN-FD は可変ビットレートの通信プロトコルである（図 3.2c.1-13）。調停に用いられるフィールドは CAN と同じビットレートである。一方 BRS から CRCD までは CAN プロトコルよりも速いビットレートで通信可能である。CAN のビットレートは最速 1Mbps であるのに対して CAN-FD の Data フィールドのビットレートは 1Mbps 以上、最速 8Mbps である。例えば CAN-FD プロトコルにおいて CAN-FD ID が 11 ビットかつ Data フィールド 512 ビットを 8Mbps

の速度で送信した場合、CAN-FDデータフレーム全体のビットレートはおよそ6.05Mbpsであり512ビットのデータを約89マイクロ秒で伝送する。これに対して、CANプロトコルにおいてCAN IDが11ビットかつDataフィールド64ビットを1Mbpsの速度で送信した場合、CANデータフレーム全体のビットレートは1Mbpsのままであり64ビットのデータを約103マイクロ秒で伝達する。可変ビットレート速度を適切に実装すれば、CAN-FDではCANと比較して1メッセージあたりのデータ量が8倍であるにもかかわらず、CANよりも高速な通信が可能である。

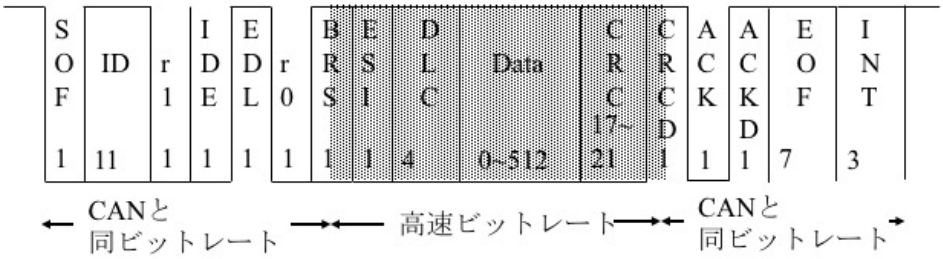


図 3.2c.1-13　CAN-FD の高速ビットレート範囲

・Data フィールド長の拡張

前述の通りCAN-FDのフレーム形式について述べたとおり、Dataフィールド長の上限が64ビットであったCANに対して、CAN-FDは上限が512ビットに拡張されている。なおCANでは8ビットずつData長を指定できたが、CAN-FDでは64ビット以上のDataフィールドについては32ビットずつ、64ビット未満の場合は8ビットずつData長を指定できる。

・拡張されたDataフィールドに伴う新しいCRC多項式

CANでは0〜8バイトのデータに対して15ビット固定長のCRCが規定されている。一方CAN-FDではデータ長に合わせて2通りのCRCが規定されている（表3.2c.1-1）。

表 3.2c.1-1　CAN と CAN-FD における CRC の比較

Data フィールド長	CRC フィールド長	CRC 多項式
0〜8 バイト（CAN）	15 ビット	$x^{15}+x^{14}+x^{10}+x^{8}+x^{7}+x^{4}+x^{3}+1$
0〜16 バイト（CAN-FD）	17 ビット	$x^{17}+x^{16}+x^{14}+x^{13}+x^{11}+x^{6}+x^{4}+x^{3}+x+1$
20〜64 バイト（CAN-FD）	21 ビット	$x^{21}+x^{20}+x^{13}+x^{11}+x^{7}+x^{4}+x^{3}+1$

(3) SENT 通信プロトコルの仕様

ここでは、SENT 通信プロトコル仕様に関して記載する。

① 概要

SENT 通信は、自動車内部のセンサと ECU 間においてセンサ信号をデジタル化して伝達する通信手法である。SENT は高精度のセンサ信号を、センサから ECU への単一方向で伝達するために利用されている。単一の信号線で 1 メッセージ当たり 2 つの信号を伝達することが可能であり、CRC により誤り検出を行うことも可能である。図 3.2c -14 に SENT の ECU とセンサの接続構造例を示す。

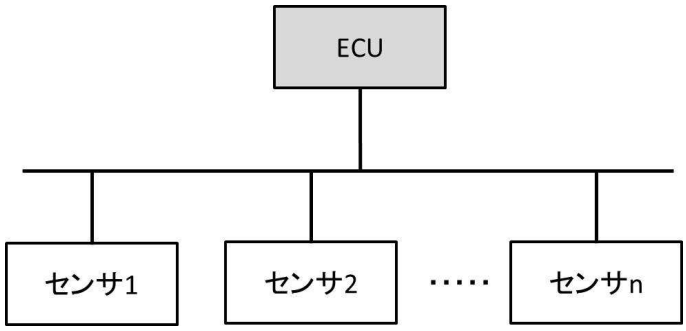


図 3.2c.1-14　SENT の接続構造例

センサ信号は、後述の立ち下がりエッジ間の時間に基づいてエンコード/デコードされる。通信プロトコルのタイミングはあらかじめ決められた Tick と呼ばれる時間単位に基づいており（Tick は 3~90 マイクロ秒の範囲で設定可能）、送信側（センサ）と受信側（ECU）であらかじめ Tick を同値に設定する必要がある。ここでは、SENT の評価手法に関係する、メッセージフォーマットおよび通信手法に関して記載する[8]。

② 通常のメッセージフォーマット

図 3.2c.1 - 15 に SENT のメッセージフォーマットの例を示す。図 3.2c.1-15 では典型的な 6 ニブルのデータフレームを持つフォーマットを示す。図に示す通り、メッセージは以下の情報を含む。

・Synchronization/Calibration パルス： 56 Ticks
・Status & Communication ニブルパルス：12～27 Ticks
・1～6 個のデータニブルパルス：12～27 Ticks
・チェックサム（CRC）ニブルパルス：12～27 Ticks
・オプションポーズパルス：12～768 Ticks

SENT のメッセージフレームは、Synchronization/Calibration パルスの開始から CRC ニブルの終了までとなる。メッセージフレームは Synchronization/Calibration パルスで始まり、

この期間で送信者と受信者間で Tick の値を同期する。Synchronization/Calibration パルスの次に Status & Communication ニブルパルスが続く。データニブルパルスは Data1 から最大 Data6 までをとり、これらは 4 ビット長であり、（データ値＋12）Tick としてエンコードされる。データの次に 4 ビットのチェックサムニブルが続き、データニブル専用の CRC 値が計算される。CRC 値の後にポーズパルスが続くがこれはオプションであり、SENT の実装によっては、メッセージの受信間隔が常に一定になるようにポーズパルスを利用してメッセージフレームの長さを調整する。

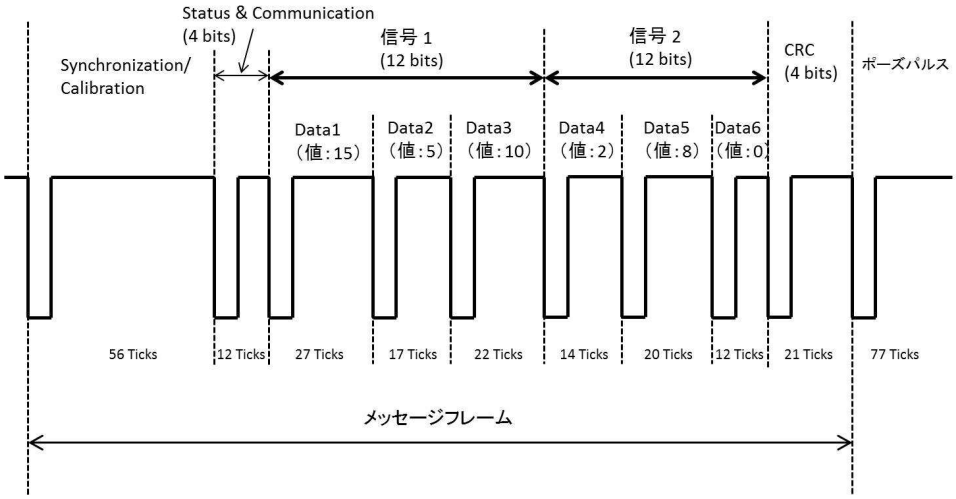


図 3.2c.1-15　SENT のメッセージフォーマット（6 ニブルデータフレーム）

③ 短縮および拡張シリアルメッセージフォーマット

SENT では、オプションとして 2 種類のメッセージフォーマット（短縮シリアルメッセージフォーマットおよび拡張シリアルメッセージフォーマット）が定義されている。ここでは例として、拡張シリアルメッセージフォーマットの概要を記載する。拡張シリアルメッセージフォーマットは、ビット長の長いデータをエンコードする時に利用される。

図 3.2c.1-16 に拡張シリアルメッセージのフォーマットを示す。拡張シリアルメッセージフォーマットでは、(ⅰ)12 ビットのデータ、8 ビットのメッセージ ID、(ⅱ)16 ビットのデータ、4 ビットのメッセージ ID の 2 種類があるが、ここでは例として(ⅰ)12 ビットのデータ、8 ビットのメッセージ ID の場合を示す。図の Serial Communication Nibble Receiver No. 8 はコンフィグレーション値を示し、(ⅰ)の場合は 0、(ⅱ)の場合は 1 を設定する。

拡張シリアルメッセージフォーマットは、8 ビットのメッセージ ID、12 ビットのデータフィールド、6 ビットの CRC 値から構成される。メッセージ ID はデータフィールドのデータタイプを特定するために利用される。CRC 値は、Serial Data #2 と#3 の 7 ビット目から 18 ビット目を利用して計算される [8]。

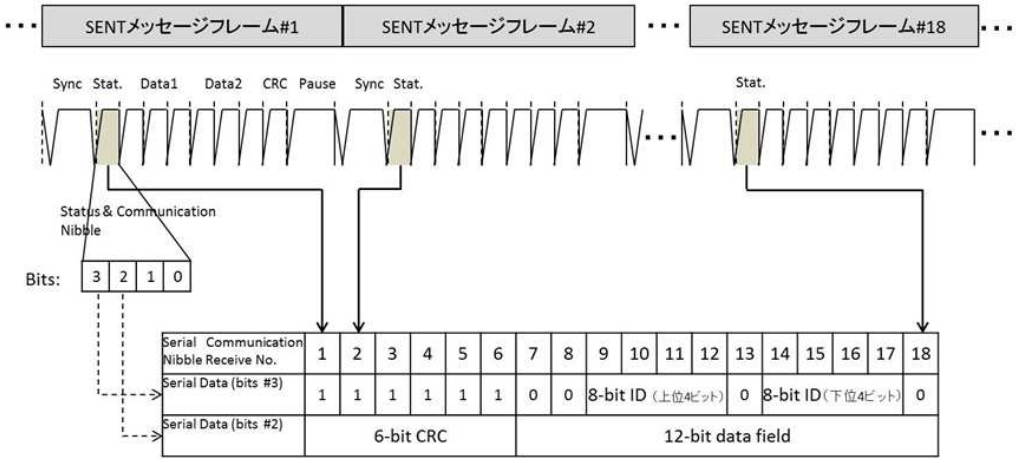


図 3.2c.1-16　拡張シリアルメッセージフォーマット

④ メッセージ送受信

送信者（センサ）は Synchronization/Calibration パルスに後にあらかじめ決まった数のニブルに対応したパルスおよびポーズパルスを連続して送信する。図 3.2c.1-17 に例として、拡張シリアルメッセージフォーマット（8 ビットのメッセージ ID および 12 ビットのデータフィールド）において、10 個のメッセージ ID を持つメッセージを周期的に送信する場合を示す。受信者（ECU）は信号の立下りエッジ間を監視し、メッセージを受信する。

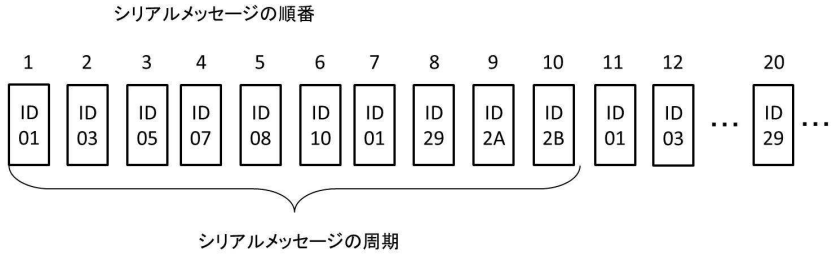


図 3.2c.1-17　メッセージ送信例

(4) PSI5 通信プロトコルの仕様

ここでは、PSI5 通信プロトコル仕様に関して記載する。[9]

① 概要

PSI5 通信は、自動車内部のセンサと ECU 間においての信号を伝達する通信手法であり、ECU からセンサに信号を伝達する通信と、センサから ECU に信号を伝達する通信を行う 2 つの方法が用意されている。パリティビット、または CRC により誤り検出を行うことも可能である。図 3.2c.1-18 に PSI5 の ECU とセンサの接続構造例を示す。

ECU からセンサに伝達される信号は、マンチェスタコードによってエンコード／デコ

ードされる。また、センサから ECU に伝達される信号は Tooth Gap 方式、または Pulse Width 方式によってエンコード／デコードされる。ここでは、PSI5 の評価手法に関係する、データフレームのフォーマットおよび通信手法に関して記載する。

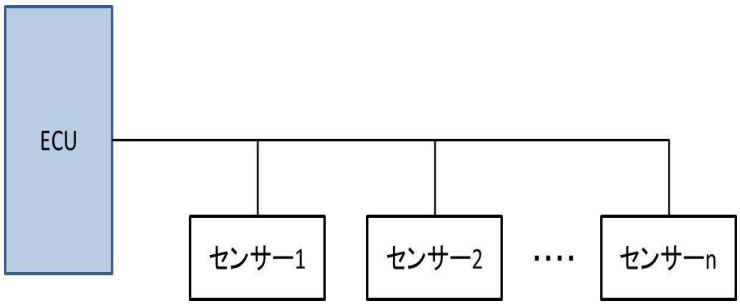


図 3.2c.1-18　PSI5 の接続構造例

② ECU からセンサへ送信されるデータフレームフォーマット

ECU からセンサへの通信は Tooth Gap 方式と Pulse Width 方式の 2 つの処理方式がある。図 3.2c.1-19 に Tooth Gap 方式のデータフレームの例を示す。図 3.2c.1-20 では 3 種類のデータフレームのうち典型的なロング型のデータフレーム（4 ビットデータニブル）のフォーマットを示す。図 3.2.c-20 に示す通り、データフレームは以下の情報を含む。

・Start bits:3bit
・SAdr（Sensor アドレス）:3bit
・FC（Function　Code）：3bit
・RAdr（アドレス）：6bit
・Data：4bit
・チェックサム（CRC）：3bit

Start Condition は少なくとも 5 つの連続した 0 か、あるいは少なくとも連続した 1 から成り立つ。ECU からセンサへ送信されるデータフレームは、Start bits の開始から CRC の終了までとなる。その後に続く 3 回の同期信号内に、センサからのレスポンスが送られる。

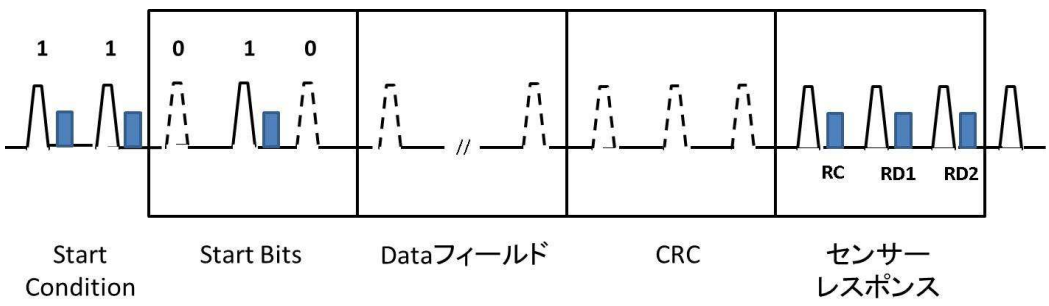


図 3.2c.1-19　ECU からセンサに送信されるデータフレーム（Tooth Gap 方式）

Start				SAdr				FC				RAdr								Data					CRC			
0	1	0	S	A0	A1	A2	S	F0	F1	F2	S	X0	X1	X2	S	X3	X4	X5	S	D0	D1	D2	S	D3	C2	C1	S	C0

Resp		
0	1	0

図 3.2c.1-20　ECU からセンサに送信されるデータフレームのフォーマット
（frame2　LONG（4-bit Data Nibbles））

③ センサから ECU へ送信されるデータフレームフォーマット

図 3.2c.1-21 に PSI5 のセンサから ECU へのデータフレームの例を示す。

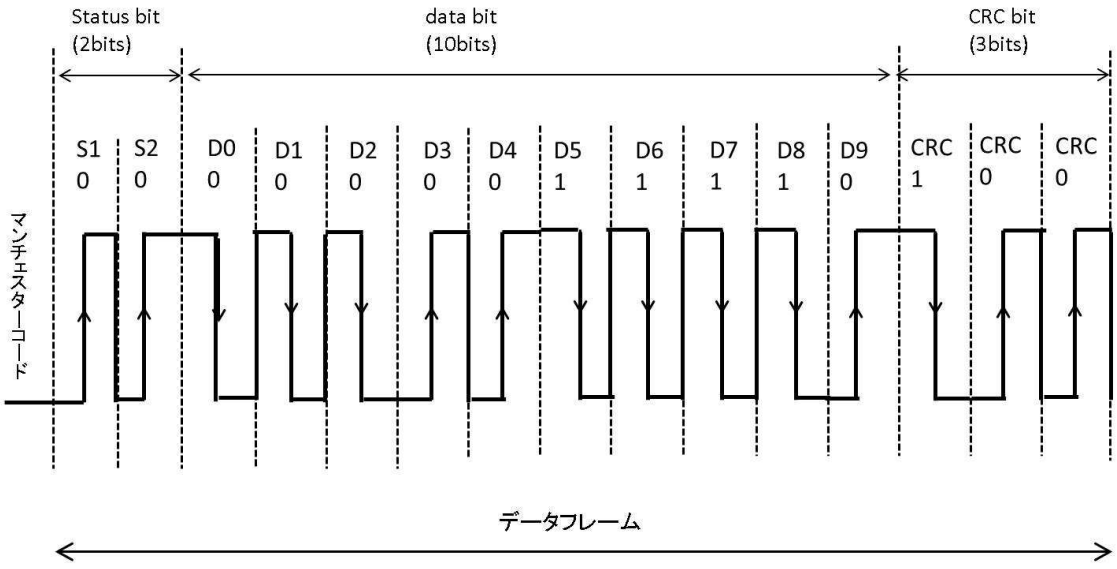


図 3.2c.1-21　センサから ECU に送信されるデータフレーム

図 3.2c.1-22 では、CRC が 3bit のデータフレームを持つフォーマットを示す。図 3.2c.1-22 に示す通り、データフレームは以下の情報を含む。

・Start bits：2bit
・Payload Data Region：10～28bit
・チェックサム（CRC）：3bit

また、図 3.2c.1-22 に Payload Data Region 内のフォーマットを示す。図 3.2c.1-22 に示す通り、Payload Data Region は以下の情報を含む。

・messaging（Serial messaging channel）：0,2bits オプション
・frame control：0,1,2,3,4bits オプション
・status（Sensor status(error flag)）：0,1,2,3bits オプション
・Data Region B（追加データ領域）：0,1,2,…,12bits オプション

・Data Region A：10,…,24bits マンダトリ

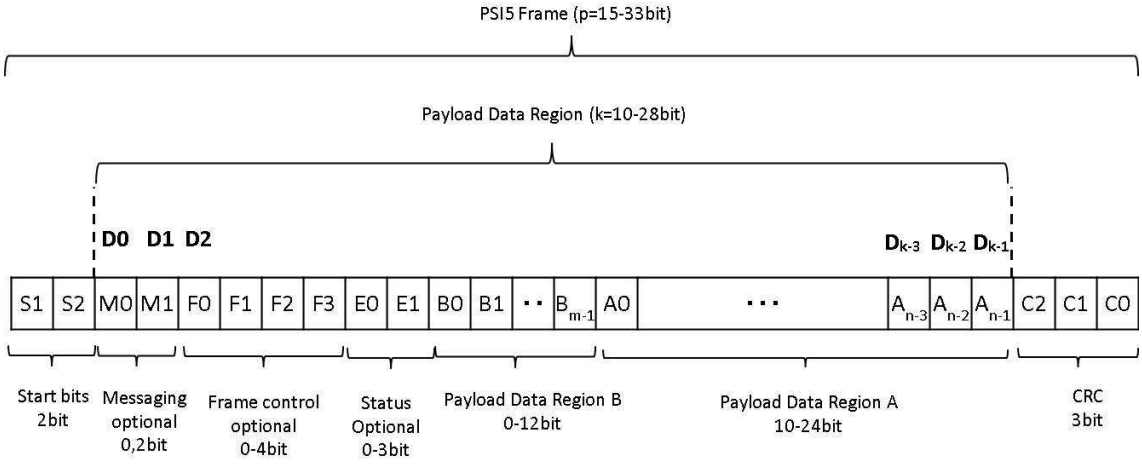


図 3.2c.1-22　センサから ECU に送信されるデータフレームのフォーマット

④ シリアルチャネル

PSI5 では、18 の連続したデータフレームを実現するシリアルデータフレームのフォーマットが定義されている。ここでは、その概要を記載する。シリアルデータフレームのフォーマットは、ビット長の長いデータをエンコードする時に利用される。

図 3.2c.1-23 にシリアルデータフレームのフォーマットを示す。シリアルデータフレームのフォーマットでは、(ⅰ) 8 ビットのシリアル ID を含む 12 ビットのデータ、(ⅱ) 4 ビットのシリアル ID を含む 16 ビットのデータの 2 種類があるが、ここでは例として(ⅰ) 8 ビットのシリアル ID を含む 12 ビットのデータ場合を示す。図 3.2c.1 - 23 の Sensor Frame Frame No.8 はコンフィグレーション値を示し、(ⅰ)の場合は 0、(ⅱ)の場合は 1 を設定する。

シリアルデータフレームのフォーマットは、8 ビットのシリアル ID を含む 12 ビットのデータフィールド、6 ビットの CRC 値から構成される。シリアル ID はデータフィールドのデータタイプを特定するために利用される。CRC 値は、Sensor frame#7 の Serial Data（bit M0）から Sensor frame#18 の Serial Data（bit M1）を利用して計算される。

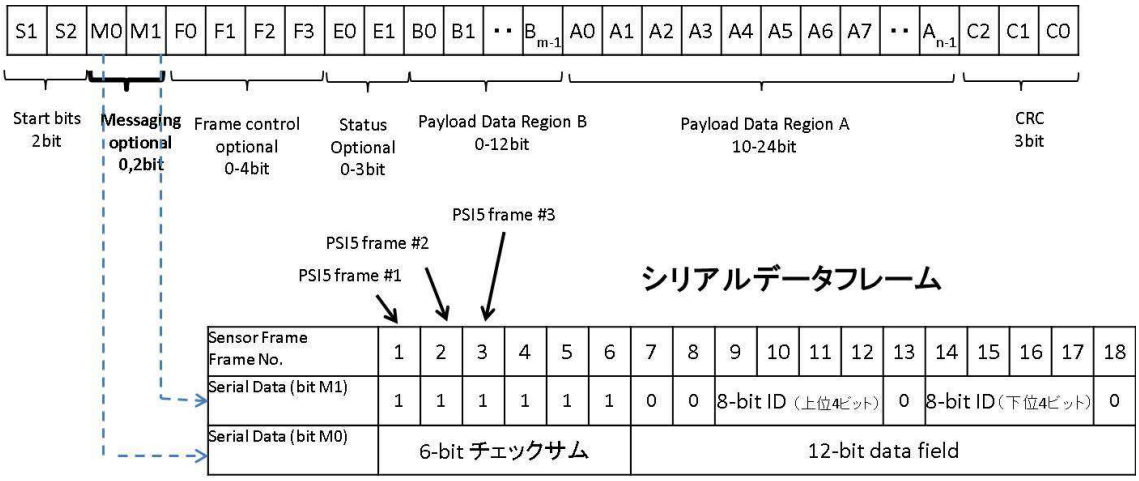


図 3.2c.1-23　センサから ECU に送信されるシリアルデータフレームのフォーマット

(5) LIN 通信プロトコルの仕様

ここでは、LIN 通信プロトコル仕様に関して記載する。

① 概要

LIN は主に自動車のパワーウィンドウ、ミラー調整、ドアロックなどのボディ制御に利用されており、シンプルで安価な車載向けサブネットワークの構築を行うために利用されている。LIN は OSI 参照モデルのうち、物理層、データリンク層、トランスポート層、アプリケーション層の 4 階層が規定されている。また、LIN 仕様のバージョン 2.0 以降では、診断機構も規定されている。ここでは、LIN の攻撃方法に関係するデータリンク層で規定されているメッセージフレームの構造、種類及び通信手順に関して述べる [10] [11] [12]。図 3.2c.1-24 に LIN の構造を示す。

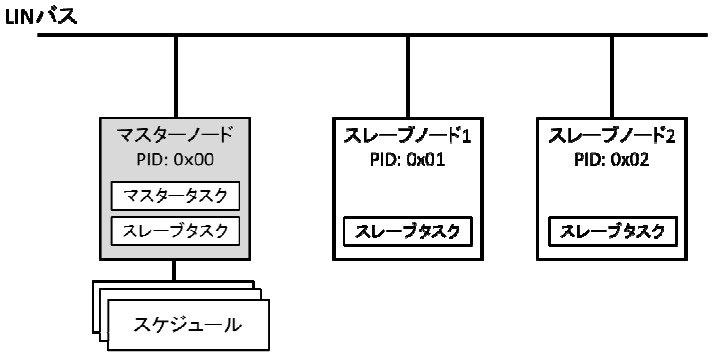


図 3.2c.1-24　LIN の構造

② フレーム構造およびメッセージフォーマット

図 3.2c.1-24 に LIN の構造の例を示す。図に示す通り、単一の LIN バス上に単一つのマスターノードと単一または複数のスレーブノードが接続される。LIN の各ノードの機能はマスタータスクとスレーブタスクがある。マスタータスクはマスターノードのみが有する機能であり、ヘッダの送信順番や送信タイミング等を管理するスケジュールに基づき、ヘッダの送信を行う。スレーブタスクはマスターノード及びスレーブノードが有する機能であり、ヘッダに応じてレスポンスの送受信を行う。ここで、マスタータスクからのヘッダの送信が伴わないレスポンスは破棄される。

LIN のメッセージフレームは図 3.2c.1-25 に示す通り、マスタータスクから送信されるヘッダとスレーブタスクから送信されるレスポンスから構成される。ヘッダは、下記の情報を含む。

・Break フィールド：意図的にフレーミングエラーを起こすことにより、各スレーブノードに LIN の通信開始を通知する。ここでフレーミングエラーとは、スタートビット（ドミナント)から数えて 10 ビット目にストップビットが検出されない場合に発生するエラーである。Break フィールドは、13 ビット以上のドミナントを表す Break と、1 ビット以上のリセッシブを表す Break-delimiter から成る。

・Synch フィールド：Synch フィールドは同期信号を示し、各ノード間のクロック誤差の補正に利用され、0x55 の値を送信する。

・PID フィールド：PID フィールドは LIN のフレームの識別情報を示す 6 ビットと 2 ビットのパリティの合計 8 ビットから成る。スレーブタスクは本 ID を解釈し、自身に割り当てられている PID であればレスポンスを送信する。

レスポンスは下記の情報を含む。

・データフィールド：データフィールドは最大 8 バイトのデータが格納される。

・チェックサム：チェックサムはデータを正確の受信できたかの確認に利用され、各データ値の総和を反転した値を格納する。

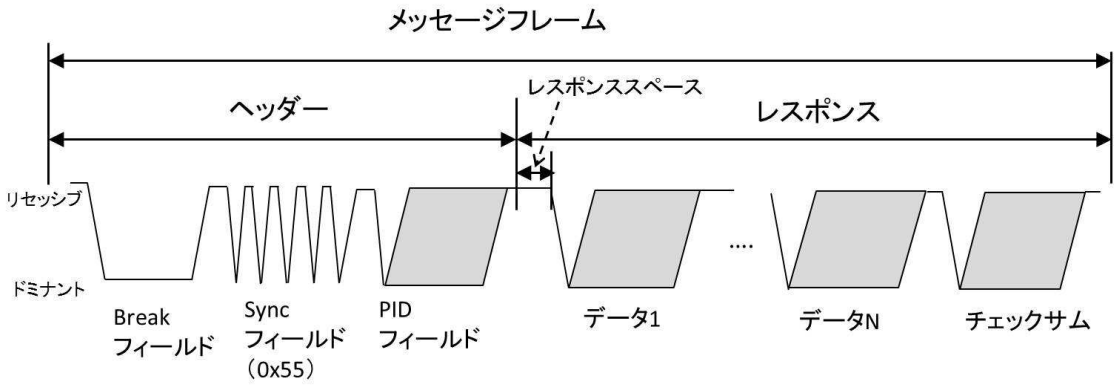


図 3.2c.1-25　メッセージフレームの構造

③ メッセージ送受信

LIN の仕様では、4 種類のメッセージフレームタイプが規定されている。ここでは、一般的に利用されている Unconditional フレームによる 3 種類の通信手順を記載する。

ここでは例として、マスターノードと 2 つのスレーブノードがバス上に接続されているとする。

・スレーブノード 1 から送信されたレスポンスをスレーブノード 2 が受信する場合は、図 3.2c.1-26 に示す通り、マスターノード内のマスタータスクはあらかじめ決められたスケジュールに基づき、ヘッダをバス上に送信する（図 3.2c.1-26①）。この時、ヘッダはバス上にブロードキャストされる。スレーブタスクはヘッダ内の PID を解釈し、自身に割り当てられた PID であれば、レスポンスをバス上に送信する。この場合は、スレーブノード 1 がレスポンスを送信する（図 3.2c.1-26②）。その後、該当するスレーブノード 2 がレスポンスを受信し、処理を行う（図 3.2c.1-26）。

・スレーブノード 1 から送信されたレスポンスをマスターノードが受信する場合は、マスターノード内のマスタータスクはあらかじめ決められたスケジュールに基づき、ヘッダをバス上に送信する。スレーブタスク 1 はヘッダの PID を解釈し、レスポンスを送信する。その後、マスターノードがレスポンスを受信し、処理を行う。

・マスターノードから送信されたレスポンスをスレーブノード 1 と 2 が受信する場合：マスターノード内のマスタータスクはあらかじめ決められたスケジュールに基づき、ヘッダをバス上に送信する。マスターノード内のスレーブタスクはヘッダに応じてレスポンスを送信する。その後、スレーブノード 1 と 2 がレスポンスを受信し、処理を行う。

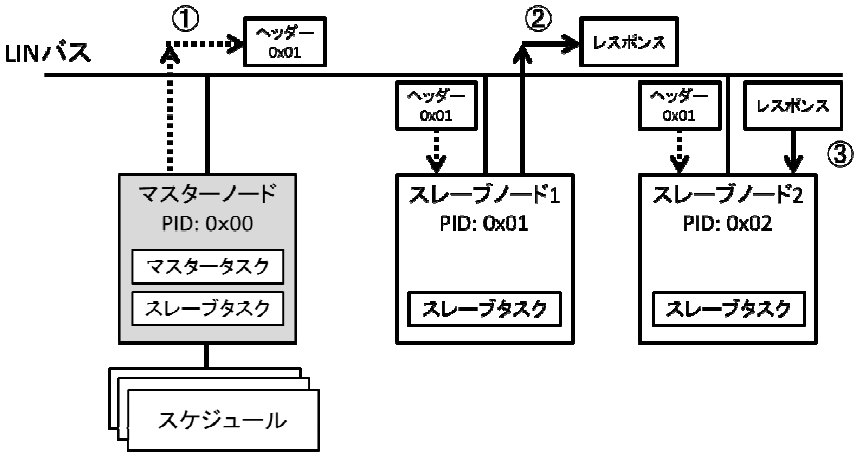


図 3.2c.1-26　LIN の通信手順

④ go-to-sleep モード／wakeup モード

LIN は主にボディ制御に利用されているため、車両の状況によっては LIN 通信が不要な時がある。このように通信が不要の状態となった時に省電力モード（go-to-sleep モード／wake up モード）に切り替え、LIN の各ノードの消費電力を抑えることが可能となる。ここでは、go-to-sleep モードおよび wake up モードに関して述べる[10]。

・go-to-sleep モード

go-to-sleep モードとは、マスタータスクによって送信された go-to-sleep コマンドにより、スレーブノードが通信を停止する状態に移行することを意味する。go-to-sleep コマンドはマスターノードのみが送信可能であり、図 3.2c.1-27 に示す通り、PID は 0x3C であり、データバイトの 1 バイト目に 0x00、2 から 8 バイト目に 0xFF を格納する。

・wake up モード

wake up モードとは、マスターノードまたはスレーブノードのスレーブタスクが各ノードに wake up シグナルを送信することにより、初期化および動作中へ移行することを意味する。wake up シグナルは 250 マイクロ秒から 5 ミリ秒のドミナント状態で開始される。

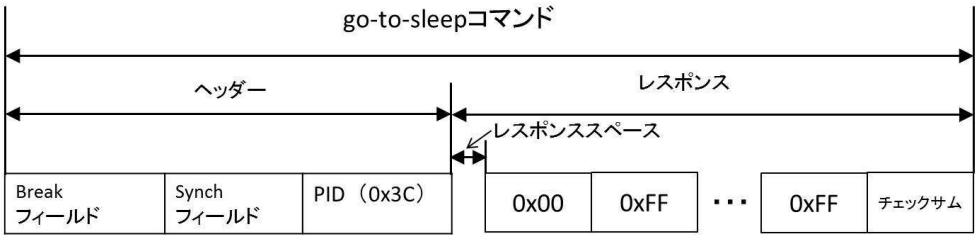


図 3.2c.1-27　go-to-sleep コマンド

(6) CXPI 通信プロトコルの仕様

ここでは、CXPI 通信プロトコル仕様に関して記載する。

① 概要

CXPI は自動車のステアリングスイッチシステム、インパネシステムなどのボディ制御用に開発された通信プロトコルである。主に、ワイパーやライトなどの瞬時に応答が必要な領域での利用が期待されている。本通信プロトコルは OSI 参照モデルのうち、物理層、データリンク層、アプリケーション層の 3 階層で構成される [13] [14]。ここでは、主に CXPI の攻撃手法に関連すると考えられる、データリンク層で規定されているフレームの構造、送受信処理およびエラー機構、アプリケーション層で規定されているフレーム送信管理および Wake/Sleep 機能に関して述べる [13] [14]。

② 通信方式

図 3.2c.1-28 に CXPI の構造例を示す。図に示す通り、単一の CXPI バスに単一のマスターノードと単一または複数のスレーブノードが接続される。マスターノードは、内部でクロックを生成してバス上に常に送信する役割を持つ。各スレーブノードは、通信バスからクロックを受信し、通信処理に利用することにより、システム内の通信クロックを同期する。また、マスターノードは通信の順番が記載されたスケジュールを持つ。

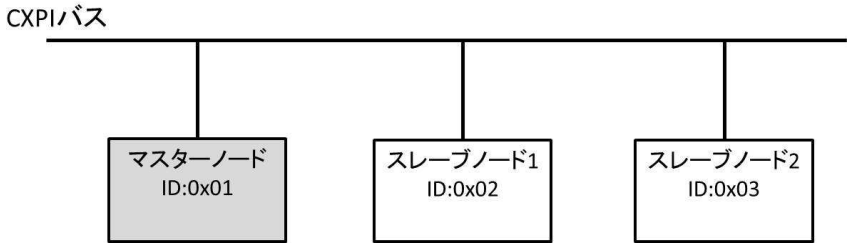


図 3.2c.1-28　CXPI の構造例

CXPI の通信プロトコルには、イベントトリガ方式（1 種類）とポーリング方式（2 種類）の合計 3 種類のアクセス方式がある。イベントトリガ方式は、各ノードがバスのアイドル状態を見つけて自由にリクエストの送信が可能である。（ただし、マスターノードはリクエストを定期送信する。）イベントトリガ方式のリクエストは PID 領域と呼ばれる。一方、ポーリング方式は、マスターノードから送信されたリクエストに対してのみ、スレーブノードがレスポンスを送信することができる。ポーリング方式の場合は、リクエストとして PID 領域のみを送信する場合と、PTYPE 領域と PID 領域を送信する場合の 2 種類がある。イベントトリガ方式は主にイベントに対する応答性を重視する場合に用い、ポーリング方式は通信の定期性を重視する場合に用いる。以下に各方式に関して述べる。

(ｉ) イベントトリガ方式

イベントトリガ方式は、各ノードがバスのアイドル状態を検知したら、PID 領域を送信することができる。複数のノードが同時に PID 領域を送信し、それらが衝突した場合には、論理値 1 に対して論理値 0 が優先されるという形で調停を行い、優先度の高い PID 領域がバス上に送信される（優先順位は文献[13]に記載）。この時、マスターノードが定期的に送信している PID 領域と各ノードが送信した PID 領域が衝突した場合も PID 領域の優先度に従い同様の調停が行われる。リクエストがバスに送信された後、該当する PID 領域をもつノードがレスポンスを送信する。

ここで例として、マスターノードと 2 つのスレーブノードが接続されている場合のイベントトリガ方式の通信手順の例を下記に示す。

・スレーブノード 1 から送信されたレスポンスをマスターノードとスレーブノード 2 が受信する場合：マスターノードはバスがアイドル状態であることを検知した上で、スケジュールに基づき、リクエスト（ID：0x02）を送信する（図 3.2c.1-29（ア））。こ

の時、リクエストはバス上にブロードキャストされる。次にリクエスト（ID：0x02）に相当するスレーブノード 1 がレスポンスを送信し（図 3.2c.1-29（イ））、マスターノードとスレーブノード 2 がレスポンスを受信する（図 3.2c.1-29（ウ））。

・スレーブノード 2 から送信されたレスポンスをマスターノードとスレーブノード 1 が受信する場合：スレーブノード 2 はバスがアイドル状態であることを検知した上で、リクエスト（ID：0x03）を送信する。次にリクエスト（ID：0x03）に相当するスレーブノード 2 がレスポンスを送信し、マスターノードとスレーブノード 1 が受信する。

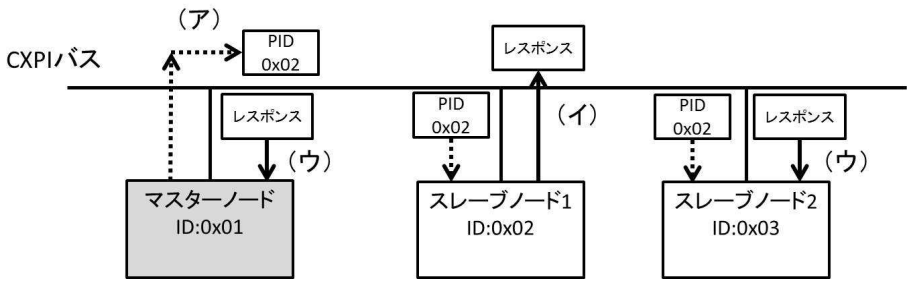


図 3.2c.1-29　イベントトリガ方式の通信手順の例

(ⅱ)　ポーリング方式

マスターノードがバス上に PID 領域のみを送信した場合、その PID に該当するノードはレスポンスを送信することができる。マスターノードがバス上に PTYPE 領域と PID 領域を送信した場合、任意のノードは任意の PID 領域を送信することができる。この時、複数のスレーブノードが同時に PID 領域を送信した場合や、マスターノードが送信した PID とスレーブノードが送信した PID が衝突した場合は通信調停を行い、優先度の高い PID 領域がバス上に送信される。その後、PID 領域に相当するノードがレスポンスを送信する。このように、スレーブノードは、マスターノードからリクエストを受信した場合のみレスポンスを送信するこが可能となる。ここで例として、マスターノードと 2 つのスレーブノードが接続されている場合のポーリング方式の通信手順の例を下記に示す。

・マスターノードが PTYPE 領域と PID 領域を送信する場合：マスターノードはバスがアイドル状態であることを検知した上で、PTYPE 領域を送信する（図 3.2c.1-30（ア））。PTYPE 領域に基づきスレーブノード 2 がリクエスト（PID：0x03）を送信する（図 3.2c.1-30（イ））。この時、同時にマスターノードも PID 領域（PID：0x53）を送信するが、通信調停により、バス上にはリクエスト（PID：0x03）が送信される。次にリクエスト（ID：0x03）に相当するスレーブノード 2 がレスポンスを送信し（図 3.2c.1-30（ウ））、マスターノードとスレーブノード 1 が受信する（図 3.2c.1-30（エ））。

・マスターノードが PID 領域を送信する場合：この場合はイベントトリガ方式のマスターノードがリクエストを送信する場合と同等である。

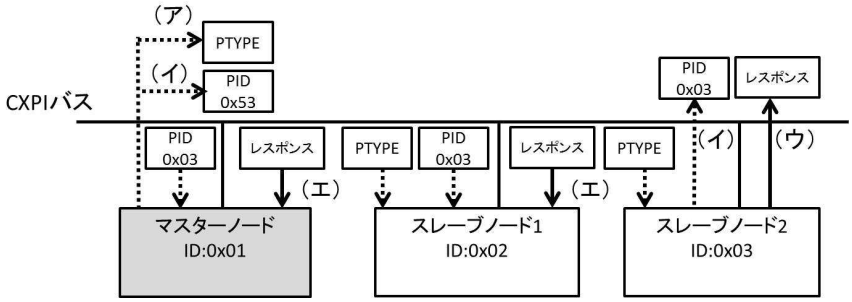


図 3.2c.1-30　ポーリング方式の通信手順の例

③ フレーム構造

CXPI のフレームには、通常フレーム、Sleep フレーム、バーストフレームの 3 種類があるが[13]、ここでは通常フレームを例に示す。図 3.2c.1-31 にイベントトリガ方式の場合とポーリング方式の場合の通常フレームの構造を示す。通常フレームは、リクエスト（PID 領域）およびレスポンス（フレーム情報、データ、CRC）から成る。ポーリング方式の場合は、通常フレームに PTYPE 領域が追加される。以下に各々の領域に関して述べる。

(ⅰ) PTYPE 領域

ポーリング方式の場合にマスターノードがスレーブノードに対して自由に PID 領域を送信しても良い場合だけ利用される。PTYPE 領域は、1 ビットのパリティビット（値は 1）と 7 ビットのフレーム TYPE（値は 0）から成る。

(ⅱ) PID 領域

1 ビットのパリティビットと 7 ビットのフレーム ID から成る。

(ⅲ) フレーム情報

4 ビットの DLC、2 ビットの NM、2 ビットのカウンタから成る。DLC はフレーム内のデータのデータ長をバイト単位で表す。NM は Wakeup/Sleep 処理に基づいた値である。CT はフレームの連続性を示すために用いる。CT はシステムごとに利用するか選択可能なオプションである。

(ⅳ) データ

データ長はフレーム情報の DLC で指定したバイト数とし、0～12 バイトのデータを格納する。

(ⅴ) CRC

CRC はデータを正確に受信できたかの確認に利用する。CRC の演算対象は、PID 領域、フレーム情報、データである。

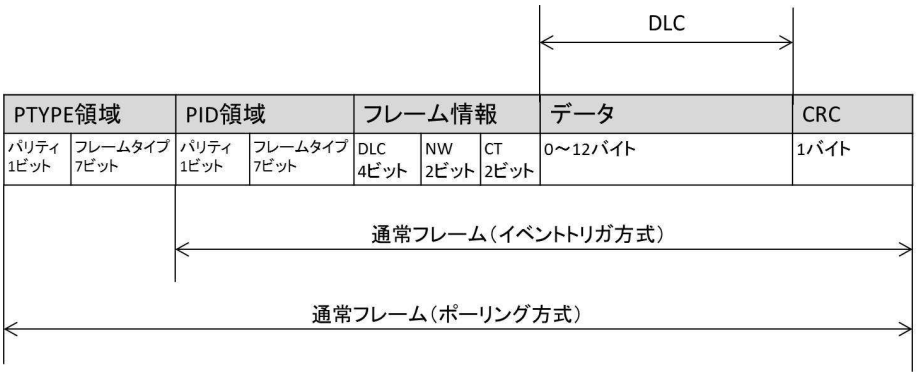


図 3.2c.1-31　通常フレームの構造

④ エラー機構

CXPI のデータリンク層では表 3.2c.1-2　エラーの種類に示す 8 種類のエラーを検出する機能をもつ。

表 3.2c.1-2　エラーの種類

エラーの種類	概要
ビットエラー	各ノードは送信しているビット値とバス上のビット値を比較し、不一致の場合に検出する。
CRC エラー	受信ノードが CRC 演算結果と受信した CRC が異なる時に検出する。
パリティエラー	受信ノードが受信した PTYPE 領域および PID 領域の論理値 1 の数が偶数個であった場合に検出する。
フィジカルバスエラー	Standby モードまたは Normal モードの際にフィジカルバスエラーの判定時間以上、何らかのフレームを受信しない場合にエラーを検出する。
データレングスエラー	受信ノードはフレーム情報の DLC と受信したフレームのデータ長を比較し、異なる場合にエラーを検出する。
カウンターエラー	受信ノードは任意のフレームのフレーム情報の CT を確認し、前に受信した同じ ID のフレームに含まれる CT の値と比較して連続していなかった場合にエラーを検出する。
オーバーランエラー	受信ノードのコントローラがバスから受信した UART データをバッファレジスタから読みだす前に、次の UART データが転送され、読みだすべきデータが新しいデータに上書きされた場合にエラーを検出する。
フレーミングエラー	受信ノードが、受信した UART フレームの最後のストップビットの論理値が 0 であった場合にエラーを検出する。

⑤ Wakeup/Sleep 機能

システムの消費電力低減のため、各ノードのデータ送受信を停止または開始させることが可能である。データの送受信の停止（Sleep）はマスターノードが各スレーブノードのSleep禁止状態を確認した上で指定する。データ送受信開始(Wakeup)は各ノードがWakeup要因を受け取ることで実現される。Wakeup 要因は、スイッチが押されたことを検知するなどの内部要因とバスから Wakeup パルスを受信する外部要因がある。各ノードのWakeup/Sleep の状態を管理するために、Sleep モード、Standby モード、Normal モードの 3種類がある。

(ⅰ) Sleep モード

Sleep モードとは、各ノードがデータの送受信を停止した省電力の状態を示す。Sleep モードに移行させるための Sleep フレームの PID は 0x1F であり、データの 1 バイト目に 0x00を、2～8 バイト目には 0xFF を格納する。

(ⅱ) Standby モード

Standbyモードとは、Normalモードへの遷移を待機する状態を示す。Standbyモードへは Sleep モードからのみ遷移する。

(ⅲ) Normal モード

Normalモードとは、通信が可能な状態を示す。Normalモードへは Standbyモードからのみ遷移する。

3.2c.2　通信プロトコルのアプリケーションにおける処理方法の調査

様々な種類の車内の通信プロトコルが標準化されているが、それらの通信プロトコルを実装した市販の車載マイコンには、標準で定義されている処理手順を実行する機能だけではなく、独自に実装されている機能が存在することがある。この独自に実装されている機能も、通信プロトコルの処理の一部を担うため、自動車に対する攻撃に利用される恐れがある。このため、ここでは、一般的な市販マイコンに実装されている標準では定義されていない機能を調査する。

調査対象は、仕様調査を実施した通信プロトコルを 6 種類選定し、各通信プロトコルについて市販マイコンの仕様書から機能調査を実施した。これらの機能の中から、標準で定義されていない機能について概要をまとめる。

(1) CAN 通信プロトコルが実装されたマイコンのアプリケーションの処理方法

ここでは、車内通信プロトコル CAN が実装されたマイコンのアプリケーションの処理方法を調査した結果を報告する。特にアプリケーションの処理方法のうち、CAN では定義されておらず、アプリケーション独自の処理について述べる。

① ノードのモード追加

前述のとおり、CANにおいてノードは初期状態1通りと、エラーアクティブ状態、エラーパッシブ状態、バスオフ状態の通信エラー回数による3通りの合計4通りの状態が規定されている。ここでは上記4状態をまとめて通常モードと呼称する。ISO11898-1: 2015では通常モード以外のモードを実装することを許可している。例えばバスモニタリング（Bus Monitoring）モードや限定作動（Restricted Operation）モードを実装してもよいとしている。バスモニタリングモードのマイコンは、有効なデータフレームと有効なリモートフレームを受信することができるが、レセシブ信号のみ送信できる。限定作動モードのマイコンは、データフレームとリモートフレームを受信して ACK を返送できるが、エラーフレームとオーバロードフレームは送信できないなど CAN で規定された処理のうち部分的に処理できる。これら追加モードの具体的な実現方法は ISO11898-1: 2015 では規定されていない。以下にアプリケーションで実装されている追加モードについて整理した。

Microchip 社製 SPI インタフェーススタンドアロン CAN コントローラ MCP2515 [15]では、3 種類の追加モードが実装されている。これら追加モードの切り換えはノードの制御レジスタ CANCTRL の値を書き換えることによって実現する。

・スリープ（sleep）モード：CAN コントローラの電流消費を最小にするモードである。CAN メッセージによるウェイクアップ（wake up）を受信すると通常モードに移行する。
・リッスンオンリ（listen only）モード：CAN コントローラは全てのメッセージを受信できるが一切送信できないモードである。CAN バスのモニタリングやボーレート検出に用いることができる。前述のバスモニタリングモードに類する状態である。
・ループバック（loop back）モード：CAN コントローラは CAN バスにメッセージ送信を実施せずに、自 CAN コントローラ内部で送信メッセージのバッファから受信メッセージのバッファにメッセージを転送するモードである。CAN バスにメッセージを送信していないため、正しく受信できたことを意味するドミナント 1 ビットの信号 ACK が他ノードから届かないが、本モードでは ACK エラーにならない。CAN コントローラのシステム開発やテストに用いることができる。

Renesas 社製マイコン RX ファミリ [16]では、以下の追加モードが実装されている。これらの追加モードの切り替えはマイコンの制御レジスタの値を書き換えることによって実現する。

・スリープモード：MCP2515 と同様の機能である。
・リッスンオンリモード：MCP2515 と同等の機能である。
・セルフテストモード（外部ループバック）：MCP2515 のループバックモードに類する機能であり、マイコン内の CAN トランシーバのテストに用いるためのモードである。マイコンによる送信メッセージはデータリンク層を司る CAN コントローラを通過して物理層を司る CAN トランシーバまで届く。その後 CAN バスには送信されずに CAN トランシーバ内で送り返されて自マイコンに受信メッセージとして到達する。
・セルフテストモード（内部ループバック）：MCP2515 のループバックモードに類する

機能であり、マイコン内の CAN コントローラのテストに用いるためのモードである。マイコンによる送信メッセージは CAN コントローラで送り返されて自マイコンに受信メッセージとして到達する。

NXP 社製 SJA1000 スタンドアロン CAN コントローラ [17]では、以下の追加モードが実装されている。

・リッスンオンリモード：MCP2515 と同様の機能である。
・グローバルセルフテストモード：MCP2515 のループバックモードに類する機能であり、CAN コントローラのシステム開発やテストに用いることができる。自 CAN コントローラ内で ACK を生成する必要がある。
・ローカルセルフテストモード：MCP2515 と同様の機能である。グローバルセルフテストモードと比較すると、MCP2515 と同様に ACK を必要としない。

② バスオフ状態からの復帰機能

前述のとおり、CAN の通常モードにはバスオフ状態が規定されている。ISO11898-1:2015 の規定では、ノードがバスオフ状態からエラーアクティブ状態に復帰するためには、CAN の MAC レイヤに対して上位レイヤがノーマルモード要求を実施し、かつ 11 ビット連続するレセシブ信号を 128 回受信する必要がある。しかし、バスオフ状態であっても緊急にメッセージを送信したい場合を想定して、上記以外の手順によりエラーアクティブ状態に復帰する機能が実装されている場合が存在する。

MCP2515 では、11 ビット連続するレセシブ信号を 128 回受信すればバスオフ状態からエラーアクティブ状態に遷移する。このとき MAC レイヤに対するリセット要求は不要である。また、11 ビット連続するレセシブ信号を 128 回受信しても、上位レイヤがエラー割り込み処理を実施することでバスオフ状態を維持できる。

RX ファミリでは、通常モードを拡張して即座にエラーアクティブ状態に復帰するなど、任意のタイミングで復帰できるように実装している。具体的には、通常モードの 4 状態に加え、新たに CAN Halt 状態を規定している（図 3.2c.2-1）。CAN Halt 状態からエラーアクティブ状態への遷移は初期状態の際に設定した制御レジスタの値によって、バスオフ状態からの遷移が以下の 5 通り存在する。

・ノーマル遷移（ISO 11898-1:2015 の規定通り）（図 3.2c.2-1(ⅰ)）
・バスオフ状態が開始したら自動的にエラーアクティブ状態へ遷移（図 3.2c.2-1(ⅱ)）
・バスオフ状態が開始したら自動的に CAN Halt 状態へ遷移（図 3.2c.2-1(ⅲ)）
・バスオフ状態が終了したら自動的に CAN Halt 状態へ遷移（図 3.2c.2-1(ⅳ)）
・バスオフ状態中の制御レジスタの値変更により CAN Halt 状態へ遷移（図 3.2c.2-1(ⅴ)）

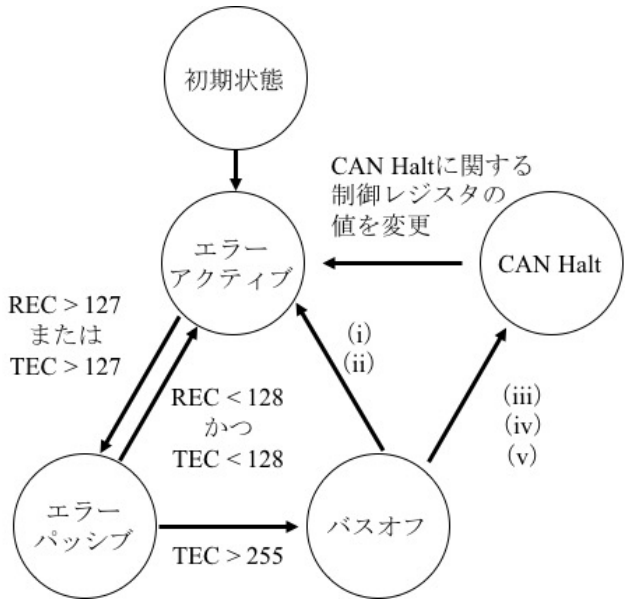


図 3.2c.2-1　RX ファミリのバスオフ状態からの復帰機能

(2) CAN-FD 車内通信プロトコルが実装されたマイコンのアプリケーションの処理方法

ここでは、車内通信プロトコル CAN-FD が実装されたマイコンのアプリケーションの処理方法を調査した結果を述べる。特にアプリケーションの処理方法のうち、CAN-FD のプロトコルでは規定されておらず、アプリケーション独自の処理について調査した。

前述のとおり CAN プロトコルと CAN-FD プロトコルの仕様は大部分が同一である。そのため、CAN プロトコルでは定義されておらず CAN のマイコンのアプリケーションにおいて独自に実装された処理について、CAN-FD においても同様な独自の処理がマイコンのアプリケーションに実装されている場合があった。CAN のマイコンと CAN-FD のマイコンとで重複する独自の処理については報告を省略する。

① メッセージ送信の一時停止機能

Cypress Semiconductor 社製マイコン FM4 ファミリ [18]では、メッセージが高頻度で流れるバスにおいて低優先順位の CAN-FD ID を持つメッセージが調停に負け続けて遅延し続けるという事態の発生を低減するために、メッセージ送信の一時停止機能を規定している。一時停止機能を有効にしたノードは、メッセージ送信完了後に次のメッセージを送信するまでに、他ノードがメッセージ調停を数回行える分の時間を空ける。高優先順位の CAN-FD ID のメッセージを送信するノードに対して本機能を有効にすると、高優先順位のメッセージが連続して流れることによってバスが占有されることがなくなるため、低優先順位のメッセージの送信が遅延し続ける頻度が減少する。

② CAN-FD プロトコルの例外イベントに対する機能

FM4 ファミリでは CAN-FD プロトコルを満たさないメッセージの受信をプロトコル例外

イベント（PEE）と見做して以下の処理を規定している。具体的には受信データフレームの特定フィールドに関するエラー処理であり、以下のとおりに実施する。

CAN-FD の規定により CAN-FD のデータフレームにおいて r0 フィールドはドミナント 1 ビットで固定値である。r0 がレセシブのメッセージを受信した場合を PEE と見做して、通常のエラー処理とは異なるエラー処理を行う。CAN-FD では通常のエラーカウンタとして REC と TEC を規定しているが、PEE では REC と TEC をエラーカウンタとして用いない。そのため PEE 中は REC と TEC は増減しない。受信メッセージを PEE と見做したノードはレセシブを送信し続ける状態に移行する。そして内蔵ビットカウンタを用いてバスのレセシブビット数を数える。レセシブが連続して 11 ビット受信できた場合は PEE が終了したと見做して通常の送受信状態に戻る。11 ビット数える前にドミナントを受信した場合はビットカウンタの値をゼロクリアして、改めてレセシブを送信し続けながらレセシブビット数を数える。

③ その他

なお NXP 社製マイコン MPC5777M に対しても CAN-FD に関するアプリケーション独自の処理について調査したが、MPC5777M には独自の処理に関する記述は見当たらなかった [19]。

(3) SENT 通信プロトコルが実装されたマイコンのアプリケーションの処理方法

ここでは、SENT 通信プロトコルが実装されたマイコンのアプリケーションの処理方法に関して記載する。マイコンのアプリケーションの処理方法のうち、通信プロトコルでは定義されておらず、アプリケーション独自の処理に関して記載する。

① エラー処理

SENT モジュール [20]には、フレーミングエラーと CRC 不一致を自動的に検出して、エラーフラグを立てる機能が実装されている。

フレーミングエラーは、Status & Communication ニブルパルスまたはデータニブルパルスが 12~27 Ticks の範囲内ではない場合に検出されるエラーである。本エラーが検出されると、レジスタに格納されるフレーミングエラーステータスビットを 1 と設定し、受信エラー割り込みが生成される。その後、後続のメッセージの Synchronization / Calibration パルスが送付されるまで受信側は待機をする。フレーミングエラーステータスビットは、受信側が後続の Synchronization / Calibration パルスを正常に受信するまで 1 に設定した状態である。この時、アプリケーションの実装によってフレーミングエラーステータスビットを 0 と設定することも可能である。

CRC 不一致は受信側で CRC の照合に失敗した時に検出されるエラーである。本エラーが検出されると、レジスタに格納される CRC ステータスビットを 1 と設定し、受信エラー

割り込みが生成される。その後、後続のメッセージの Synchronization / Calibration パルスが送付されるまで、CRC ステータスビットを 1 と設定した状態で、受信側は待機をする。この時、アプリケーションの実装によってCRCステータスビットを0と設定することも可能である。

② 省電力モード中の処理

SENT モジュールにおいて、アプリケーション側で二種類の省電力モードが設定可能である [20]。

(ⅰ) スリープモード

SENT モジュール内のレジスタに格納されたモジュールの有効を示すビットを 0 と設定することにより、SENT モジュールの動作を停止させて、モジュールが搭載されたデバイスをスリープモードに移行させることが可能である。モジュールが送信側として動作している場合、メッセージの送信が完了するまで待機してからデバイスをスリープモードに移行させることが可能である。

(ⅱ) アイドルモード

デバイスがアイドルモードに移行した時の SENT モジュールの動作は以下の 2 通りがある。

- レジスタに格納されたアイドル中の動作を表すビットが 1 の時、デバイスがアイドル状態に移行するとモジュールの動作は停止する。この時の動作は上記に記載したスリープモードと同等である。
- レジスタに格納されたアイドル中の動作を表すビットが 0 の時、デバイスがアイドル状態に移行した後も SENT モジュールは送受信の処理を継続する。モジュールが送信側として動作している場合、デバイスがアイドル状態から復帰してレジスタ内のデータを書き換えない限り、SENT モジュールはレジスタにすでに格納されているデータを送信し続ける。モジュールが受信側として動作している場合、デバイスがアイドル状態から復帰してデータを読み出さない限り、レジスタに格納された古いデータは失われる。

③ その他

その他、文献 [21]の SENT が実装されたモジュールに関する調査を実施したが、アプリケーション独自の処理に関する記述は見当たらなかった。

(4) PSI5 通信プロトコルが実装されたマイコンのアプリケーションの処理方法

ここでは、PSI5 通信プロトコルが実装されたマイコンのアプリケーションの処理方法に関して記載する。マイコンのアプリケーションの処理方法のうち、通信プロトコルでは定義されておらず、アプリケーションに依存する処理に関して記載する。調査対象としたマイコンについては、機能安全性の要求に関して下記の実装が行われている。[22]

① バッファチェック処理

データの損失を避けるために、本マイコンにはデータバッファが用意されている。データバッファ内のデータは送信機能によって読み込まれた後に、センサデータ送信開始の時点でデータレジスタはクリアされ、新しいデータフレームを受け取ることができる。

本マイコンが初期化を行うにあたって、安全性の機能として下記のような機能を有している。安全性の機能として、本マイコンは常にデータバッファの状態をチェックしている。正しいデータの読み込みの後に、エラーコード 1FO（data buffer empty を意味する）がデータバッファに書き込まれる。このチェックが失敗すれば、バッファーエンプティ失敗がラッチされ、SR2 レジスタに BEx ビットが記憶される。そして、送信モジュールの読み込みの後にクリアされる。本マイコンは、バッファエンプティチェックのテストを行う機能が実装されている。

本マイコンがこの機能をスタートさせる時、または通常操作時にこの機能をテストすることを許可するために、バッファエンプティチェックのテストは STSR レジスタに与えられる。この STSR レジスタにビットが設定されると、読み込み操作の後に古いデータがバッファに残される。このようにして、バッファエンプティフォールトの状態が設定されるため、本マイコンはバッファチェック処理をテストすることができる。

② センサ初期化データの自動保存処理

センサがデータレンジ初期化処理を利用し、PSI5 のペイロードが 3 ビットのフレームコントローラを持った 20bit のデータである場合に、デバイスは設定されることができる。その結果、初期化データは本マイコンのトランシーバ IC 内に保持される、そして送信機能を実行する際に読み込むことができる。

・初期化データの登録
・初期データの自動的検知
・送信機能を実行する際の読み込み

インタフェースの活性化の後に、トランシーバ IC はインタフェース上で入力されるセンサ初期化データをチェックする。そしてその後の処理のためにデータを保存する。この振る舞いは、Configuration bit READ_INIT_DATA によって引き起こされる。もし、この bit がセットされれば、内部 FSM はインタフェース上に入力されるペイロードデータ内の IDn とデータブロック Dn をチェックし、そしてデータをデータフォーマット内の対応す

るフレーム id の init buffer id 内に保存する。

初期化データの自動保存が活性化されている時に、フレームコントロール bit は 8 init data buffer まで使用することを許可している。そして両方のインタフェース（READ_INIT_DATA1 = READ_INIT_DATA2 = 1）が用いられる。1 つのインタフェースのみが活性化されている場合において、トランシーバ IC はインタフェース上で 6 init data まで保存することができる。

PSI5 で仕様化されているように、データニブル　D2 と D3 はそれぞれの特定フレーム ID に対して全ての初期化処理に期待されるデータブロック数を含む。

全ての初期化データが従事しているセンサに対して両方のインタフェース上で受け取る際に。すなわち、少なくとも一つの正しいデータブロックを送ってくるセンサに対して。

初期化データ rdy がセットされ、そしてマイコンは全ての初期化データを送信機能に読み込むことができる。リセットの間、入力データバッファはクリアされ、そしてそれぞれの初期化データブロックのカウンタは 00 にセットされる。

インタフェースは、非同期モードと同期モードの両方に設定される。受け入れられる初期化データの設定は以下のようにトータル 20bit に基づいている。

・16 data bit
・1 status
・3 frame control

③ その他

なお Freescale Semiconductor 社製マイコン MC33789 のドキュメント[19]に対しても PSI5 に関するアプリケーションに依存する処理について調査したが、MC33789 にはアプリケーションに依存する処理に関する記述は見当たらなかった。

(5) LIN 通信プロトコルが実装されたマイコンのアプリケーションの処理方法

ここでは、LIN 通信プロトコルが実装されたマイコンのアプリケーションの処理方法に関して述べる。マイコンのアプリケーションの処理方法のうち、通信プロトコルでは定義されておらず、アプリケーション独自の処理に関して記載する。

① エラーハンドリング機構：LIN のエラーの検出方法やエラー検出後の処理はプロトコルで規定されておらず、各アプリケーション独自で実装する必要がある [23]。LIN では、送受信が正常に行われたかどうかの情報を基に通信エラーを検出する。表 3.2c.2-1 に LIN 通信で規定されているエラーの種類の例を示す。ここで、例えば LIN バス上でビットエラーが発生した場合の処理として、単に次のヘッダ送信を待つといったシンプルなエラー処理が実装されている場合もある [24]。

② スリープコマンド送信後の処理：LIN の通信プロトコルにおいて定義されているスリープコマンドを送信した後の処理は、アプリケーションに依存している。スリープコマンドとは、LIN の通信プロトコル仕様で記載した通り、マスターノードが送信するフレームであり、PID が 0x3C、レスポンスのデータフィールドの 1 バイト目が 0x00 で構成されているフレームである。例えば、スリープコマンド送信後に、フラグの反映やマイコン動作モードの遷移といった特別な動作に移行しない場合もある [23]。

表 3.2c.2-1　LIN のエラー種類例

エラーの種類	エラーを検出する条件
ビットエラー	送信スレーブノードがビット単位またはバイト単位でレスポンスを監視し、それとバス上のデータレベルが一致していない場合
チェックサムエラー	レスポンスのデータとチェックサムを加えた値が 0xFF でない時
シンクフィールドエラー	受信したシンクフィールドデータが 0x55 でなかった場合
スレーブノットレスポンディングエラー	メッセージフレーム送受信中、一定時間内にスレーブノードからのレスポンスが受信完了されなかった場合
ノーバスアクティブエラー	一定時間に LIN バス動作がない場合

(6) CXPI 通信プロトコルが実装されたマイコンのアプリケーションの処理方法

ここでは、CXPI 通信プロトコルが実装されたマイコンのアプリケーションの処理方法に関して記載する。

CXPI が搭載されたマイコンに関する文献の調査を実施したところ、公開されているアプリケーションノートは発見されなかった。そのため、CXPI 搭載のマイコンである車載向け CXPI トランシーバ（BD41000FJ-C） [25] [26]および車載 MCU シリーズ（S6BT11x CXPI トランシーバ） [27] [28]に関する公開資料の調査を実施した。これらの資料には CXPI 仕様に記載されていないマイコンのアプリケーションに関する記載はされていなかった。

3.2c.3　通信プロトコルにおける既存の脆弱性及び攻撃方法の調査

自動車のセキュリティに関して、脆弱性や攻撃方法、およびそれらに対する対策の検討等、様々な研究が行われている。例えば、車車間・路車通信の無線通信に関する研究、車内ネットワークの電気的な信号の改ざんによる不正な操作の研究、ECU の LSI における耐タンパ性に関する研究など、その対象も攻撃方法も様々である。

車内通信プロトコルの仕様についても、各々の目的、機能、特性などに応じて、十分な内容となっている反面、セキュリティ面での脆弱性が存在している恐れがある。そこで、既存の研究の中から、車内通信プロトコルの脆弱性や、その脆弱性を利用した攻撃方法について調査を行った。

調査対象は自動車セキュリティ関連技術の発表が多いと予測される、情報セキュリティ

に関連する国際会議・学会等（表 3.2c.3-1）における発表の中から、論文、プレゼンテーション資料などが公開されている発表である。

表 3.2c.3-1　脆弱性及び攻撃方法の調査対象会議等

会議等名称	調査対象年	調査対象発表件数
Embedded Security in Cars (escar)　Europe	2013-2015	47（*）
Embedded Security in Cars (escar)　USA	2013-2015	33（**）
Embedded Security in Cars (escar)　Asia	2014-2015	25
Vehicular Technology Conference (VTC) Spring, Fall	2013-2015	2621
暗号と情報セキュリティシンポジウム (SCIS)	2013-2015	983
コンピュータセキュリティシンポジウム (CSS)	2013-2015	500
Black Hat USA	2015	93（***）

（*）：escar Europe は総発表件数 53 件の内、論文または資料が入手した発表のみ調査
（**）：escar USA は総発表件数 51 件の内、論文または資料が入手した発表のみ調査
（***）：Black Hat USA 2015 は総発表件数 117 件の内、論文または資料が入手した発表のみ調査

(1) escar Europe

ここでは、2013 年から 2015 年の escar Europe で発表された論文のうち、通信プロトコルの脆弱性および攻撃方法に関する発表内容を記載する。また、追加で他の年に開催された escar Europe の調査を行った結果、escar Europe 2004 において CAN および LIN に対する攻撃方法が見つかったため、これに関して述べる。

① escar Europe 2013

下記発表論文に、SENT 通信プロトコル等のセンサとの通信方法に対する攻撃方法が記載されている。

(ⅰ) 論文名：Approaches to Economics Secure Automotive Sensor Communication in Constrained Environments

・著者：B. Glas and M. Lewis
・所属：Robert Bosch GmbH

センサ（送信側）と ECU（受信側）との間で SENT 等の通信プロトコルを利用してメッセージの一方向通信を行っている際の、リプレイ攻撃の可能性が挙げられる。図 3.2c.3-1 にセンサ信号が 1 つのセンサと ECU 間で送受信されている際の攻撃例を示す。ここで、以下に攻撃の前提を示す。

・攻撃者はデジタル通信上にアクセス可能であるとする。
・攻撃者はセンサデータを盗聴、遮断が可能であるとする。また、不正な信号を通信上に挿入可能であるとする。
・通信上の信号は暗号化されていないとする。

上記前提の時、攻撃者は SENT 通信上のセンサ信号を盗聴し、同信号を繰り返し再送す

ることによってリプレイ攻撃を実行することが可能である。

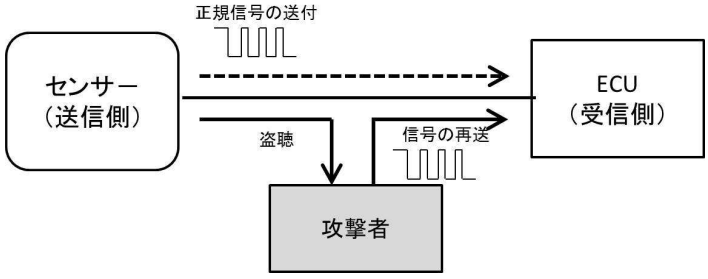


図 3.2c.3-1　リプレイ攻撃の例

② escar Europe 2014

下記発表論文に、CAN 通信プロトコルの通信方法に対する攻撃方法が記載されている。

(ｉ) 論文名：CaCAN – Centralized Authentication System in CAN (Controller Area Network)

・著者：R. Kurachi*, Y. Matsubara*, H. Takada*, N. Adachi †, Y. Miyashita † and S. Horihata †
・所属：*名古屋大学、†株式会社オートネットワーク技術研究所

以下の 2 つの攻撃シナリオにより、悪意のある攻撃ノードが CAN バス上にアクセスし、正規ノードになりまして偽のメッセージを送信する攻撃やリプレイ攻撃を実施することが可能である。

・シナリオ 1：正規ノードが、プログラムコード書き換えツール等の利用により、悪意のあるプログラムに書き換えられて、CAN バス上になりすましメッセージを送信する（図 3.2c.3-2）。
・シナリオ 2：CAN バス上に攻撃ノードが接続され、それがなりすましメッセージを送信する（図 3.2c.3-3）。

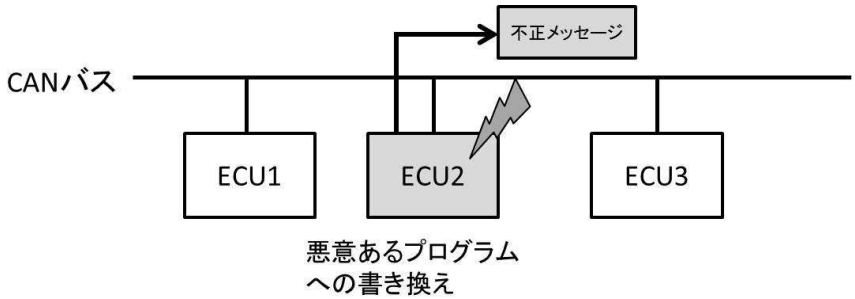


図 3.2c.3-2　正規ノードの悪意あるコードへの書き換え

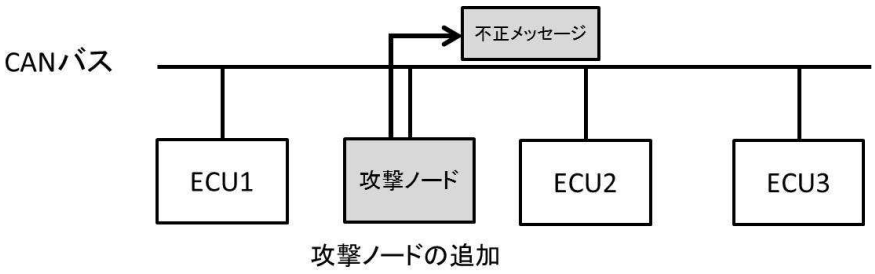


図 3.2c.3-3　攻撃ノードの追加

③ escar Europe 2015

下記発表論文に、CAN 通信プロトコルの通信方法に対する攻撃方法が記載されている。

(ⅰ) SecGW - Secure Gateway for in-vehicle networks

・著者：*R. Kurachi, *H. Takada, †T. Mizutani, †H. Ueda and †S. Horihata
・所属：*名古屋大学、†株式会社オートネットワーク技術研究所

CAN への攻撃の例として、escar Europe 2014 の報告に記載した 2 種類の攻撃シナリオが再掲されている。その 2 種類の攻撃シナリオに追加して、別の攻撃事例として、攻撃ノードがエラーフレームを利用して正規送信ノードをバスオフ状態にすることによりなりすまし攻撃を行う手法が記載されている。本攻撃手法は、攻撃者は CAN バス上に攻撃ノードを追加できるという前提が置かれている。下記に具体的な攻撃手順を記載する。

・攻撃ノードは、攻撃対象の送信ノードがメッセージを送信した後、何らかの方法で故意に通信エラーを起こして送信ノードの送信エラーカウンタ値（TEC）を増加させる（図 3.2c.3-4（ア））。攻撃者はこれを繰り返すことによって、送信エラーカウンタ値を最大値まで引き上げることにより、攻撃対象の送信ノードを故意にバスから切り離す。
・攻撃対象の送信ノードはバスオフ状態になるため、メッセージの送受信を停止する。よって、攻撃ノードは送信ノードになりすまして、不正メッセージをバス上に送信することが可能となる（図 3.2c.3-5（イ））。受信ノードは不正メッセージを正規の送信ノードが送信したものを誤認識し、受信する（図 3.2c.3-5（ウ））。

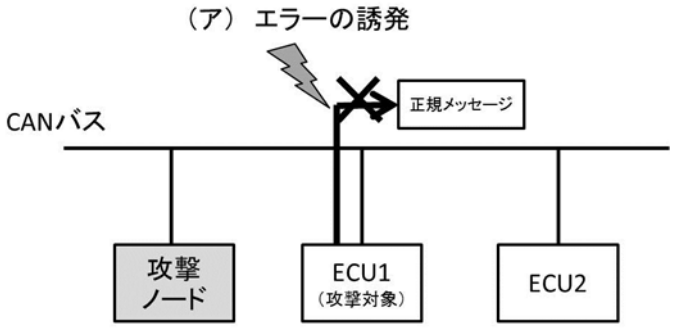


図 3.2c.3-4　エラーの誘発

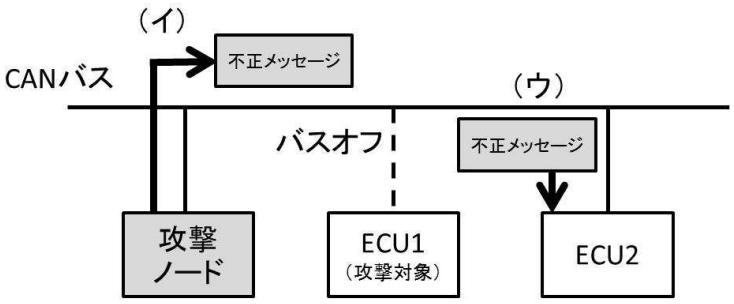


図 3.2c.3-5　不正メッセージの送受信

(ⅱ) 論文名：A Method for Disabling Malicious CAN Messages by Using a Centralized Monitoring and Interceptor ECU

・著者：Y. Ujiie, T. Kishikawa, T. Haga, H. Matsushima, T. Wakabayashi, M. Tanabe, Y. Kitamura and J. Anzai
・所属：パナソニック株式会社

セキュリティの観点における、下記の CAN の脆弱性に関して記載されている。
・CAN のメッセージはバス上に接続された全ての ECU にブロードキャストされる。
・CAN の ID には送信者の情報は含まれない。

よって、上記特性より、攻撃者が正規 ECU になりすまして不正メッセージをバス上に送信する攻撃であるなりすまし攻撃により、他の ECU を不正に制御することが可能であることが記載されている。

更に、なりすまし攻撃の他に、CAN 通信プロトコルにおけるセキュリティの脅威として下記が挙げられている。
・通信傍受：CAN メッセージを不正に入手・解析する。
・DoS 攻撃：優先度の高い CAN メッセージでバスを占有する。

④ escar Europe 2004

下記発表論文に、CAN 通信プロトコルの通信方法に対する攻撃方法が記載されている。

(ⅰ) 論文名：Security in Automotive Bus Systems

・著者：M. Wolf, A. Weimerskirch and C. Paar
・所属：escrypt GmbH

CAN 通信を妨害するためには下記の 2 つの攻撃方法がある。
・バスの占有：CAN では通信調停が行われるため、優先順位の高い ID を含むメッセージが優先してバス上に送信される。このことを利用して、攻撃者が妨害対象のメッセージよりも優先順位の高い ID を含む不正なメッセージをバス上に定期的に送信することにより、不正なメッセージでバスを占有し、正規メッセージの送信を妨害するこ

とが可能である。
・バスの接続妨害：攻撃者が故意に CAN 通信エラーを引き起こし、CAN バス上のノードのエラーカウンタを上限に達するまで加算する。カウンタ値が上限に達するとノードが CAN バスから切り離されるため、バスに接続されたノードの接続妨害を引き起こすことが可能である。

LIN 通信を妨害するためには下記の 2 つの攻撃方法がある。
・バスに接続されたノードの動作妨害：攻撃者が、強制スリープを任意のタイミングで不正に LIN バス上に送信することにより、LIN バス上に接続される全てのスレーブノードを休止状態にすることが可能である。このことにより、全てのスレーブノードを動作不能にすることでバスに接続されたノードの動作妨害を引き起こすことが可能となる。
・LIN 通信妨害：攻撃者が，マスターノードになりすまして，偽の同期バイト（SYNC_FIELD）を含む偽のヘッダを LIN バス上に送信する．このことにより，スレーブノードとマスターノードが同期をとって通信を行うことが不可能となり、予期しない挙動が誘発されるため、LIN 通信妨害を引き起こすことが可能である。

(2) escar USA

ここでは、escar USA 2013 から 2015 に発表された論文の調査結果を報告する。

escar USA 2013 から 2015 において発表された 51 件のうち、論文または発表資料が入手できた 33 件に関して調査を実施した。このうち、通信プロトコルの脆弱性や攻撃方法に該当する発表は見当たらなかった。

(3) escar ASIA

国際シンポジウム escar ASIA の開催概要は以下の通りである。escar ASIA は 2014 年が第 1 回目の開催である。なお escar ASIA では主催団体所属の記者による講演レポートが公開される。講演で用いられたプレゼンテーション資料は一部の発表分が参加者にのみ配布された。論文等の文書資料は参加者に配布されず、必ずしも論文形式の資料が作成されたとは言えない。本報告書では前述の講演レポートならびに入手できたプレゼンテーション資料を調査した結果を報告する。

① escar ASIA 2014

・主催：日経 Automotive Technology
・開催期間：2014 年 4 月 17 日（木）～ 2014 年 4 月 18 日（金）
・講演数：12
・調査数：12

escar ASIA 2014 では報告対象が 0 件である。ECU に搭載するハードウェアに関する調査

や車車間、路車間通信に関する調査が主たる演目であり、具体的な車内通信プロトコルに関する演目は存在しなかった。

② escar ASIA 2015

・主催：日経 Automotive Technology
・開催期間：2015 年 9 月 7 日（月）～ 2015 年 9 月 8 日（火）
・講演数：13
・調査数：13

escar ASIA 2015 では報告対象が 1 件存在する。以下にその詳細を述べる。

（ｉ）論文名：車載制御システムを保護するセキュリティ技術
・発表者：松島 秀樹
・所属：パナソニック株式会社

上記報告では、パナソニック社における CAN に対するセキュリティの取り組みを解説しCANのセキュリティを高めるための同社の提案方式を紹介している。特にCAN IDの詐称による CAN メッセージのなりすまし攻撃を脅威として掲げ、CAN のセキュリティを高めるためのフィルタリング方式、ネットワーク監視方式、認証付メッセージ方式の合計 3 方式による脅威の無効化を主張している。なお上記報告が紹介した同社の車内通信ネットワークに対するセキュリティ技術の提案方式は国内シンポジウム SCIS 2015 にて詳細が報告されているため、ここでは報告内容の詳細は省く（SCIS の項を参照）。

(4) VTC

VTC では発表論文が冊子として編纂されて公開され、また IEEE Xplore Digital Library を通じて公開される。本報告書では IEEE Xplore Digital Library から入手可能な論文資料を調査した結果を報告する。

① 2013 IEEE 77th Vehicular Technology Conference (VTC2013 Spring)

・開催期間：2013 年 6 月 2 日（日） ～ 2013 年 6 月 5 日（水）
・公開論文件数：436

公開論文全 436 件に対して、自動車のセキュリティに関する発表が 8 件存在する。その 8 件全てが車車間、路車間通信といった無線通信に関する研究である。その他に、車内通信プロトコルに関する発表が 2 件存在する。1 件は FlexRay プロトコルの故障検出に関する検証実験の報告であり、もう 1 件は CAN プロトコルを拡張した高速多重化 CAN プロトコルの提案である。前述の 10 件には車内通信プロトコルの脆弱性や攻撃手法に関する言及はなかった。以上から VTC2013 Spring において報告対象は 0 件である。

② 2013 IEEE 78th Vehicular Technology Conference (VTC2013 Fall)

・開催期間：2013 年 9 月 2 日（月） ～ 2013 年 9 月 5 日（木）
・公開論文数：434

会議全体 434 件に対して、自動車のセキュリティに関する発表が 7 件存在する。うち 6 件が車車間、路車間通信といった無線通信に関する研究であり、残り 1 件はキーレスエントリシステムにおける無線通信に関する研究である。その他に、車内通信プロトコルに関する発表が 1 件存在するものの、CAN プロトコルにおける通信速度の評価方法に関する研究である。前述の 8 件には車内通信プロトコルの脆弱性や攻撃手法に関する言及はなかった。以上から VTC2013 Fall において報告対象は 0 件である。

③ 2014 IEEE 79th Vehicular Technology Conference (VTC2014 Spring)

・開催期間：2014 年 5 月 18 日（日） ～ 2014 年 5 月 21 日（水）
・公開論文件数：408

公開論文全 408 件に対して、自動車のセキュリティに関する発表が 11 件存在する。その全てが車車間、路車間通信といった無線通信に関する研究であり、車内通信プロトコルの脆弱性や攻撃手法に関する言及はなかった。以上から VT2014 Spring において報告対象は 0 件である。

④ 2014 IEEE 80th Vehicular Technology Conference (VTC2014 Fall)

・開催期間：2014 年 9 月 14 日（日） ～ 2014 年 9 月 17 日（水）
・公開論文数：433

会議全体 433 件に対して、自動車のセキュリティに関する発表は 12 件存在する。その 12 件全てが車車間、路車間通信といった無線通信に関する研究である。その他に、車内通信プロトコルに関わる発表は 1 件存在するものの、CAN プロトコルにおける通信速度上限を 1Mbps から 100Mbps に向上させる手法に関する研究である。前述の 13 件には車内通信プロトコルの脆弱性や攻撃手法に関する言及はなかった。以上から VT2014 Fall において報告対象は 0 件である。

⑤ 2015 IEEE 81st Vehicular Technology Conference (VTC2015 Spring)

・開催期間：2015 年 5 月 11 日（月） ～ 2015 年 5 月 14 日（木）
・公開論文件数：499

公開論文全 499 件に対して、自動車のセキュリティに関する発表が 14 件存在する。その全てが車車間、路車間通信といった無線通信に関する研究であり、車内通信プロトコルの脆弱性や攻撃手法に関する言及はなかった。なお会議目録には、車内通信プロトコル FlexRay のセキュリティに関して言及されていることが題目から推測できる発表が 1 件存在するものの、該当論文は IEEE Xplore Digital Library に公開されていなかった。以上から、

VT2015 Spring において報告対象は 0 件である。

⑥ 2015 IEEE 82nd Vehicular Technology Conference (VTC2015 Fall)

・開催期間：2015 年 9 月 6 日（日） ～ 2015 年 9 月 9 日（水）
・公開論文数：411

会議全体 411 件に対して、自動車のセキュリティに関する発表が 13 件存在する。うち 12 件が車車間、路車間通信といった無線通信に関する研究であり、残りの 1 件は ECU の LSI における耐タンパ性に関する研究である。その他に、車内通信プロトコルに関する発表は1件存在するものの、CANプロトコルにおけるリアルタイム応答の観点を考慮したネットワークトポロジの設計手法に関する研究である。前述の 14 件には車内通信プロトコルの脆弱性や攻撃手法に関する言及はなかった。以上から VT2015 Fall において報告対象は 0 件である。

(5) SCIS

国内シンポジウム「SCIS　暗号と情報セキュリティシンポジウム」の開催概要は以下の通りである。各回とも主催は電子情報通信学会　情報セキュリティ研究専門委員会（ISEC 研）である。SCIS では発表論文が電子媒体（PDF 形式）として編纂されて参加者に配布される。本報告書では各回の参加者から入手した発表論文を調査した結果を報告する。

① The 30th Symposium on Cryptography and Information Security（SCIS 2013）

・開催期間：2013 年 1 月 22 日（火） ～ 2013 年 1 月 25 日（金）
・公開論文数：308

会議全体 308 件に対して、自動車のセキュリティに関する発表が 1 件存在する。車車間、路車間通信といった無線通信に関する研究であり、本報告書の対象外である。

② The 31st Symposium on Cryptography and Information Security（SCIS 2014）

・開催期間：2014 年 1 月 21 日（火） ～ 2014 年 1 月 24 日（金）
・公開論文数：343

会議全体 343 件に対して、自動車のセキュリティに関する発表が 4 件存在する。うち 3 件は車車間、路車通信といった無線通信に関する研究であり、本報告書の対象外である。残り 1 件は車内通信プロトコル CAN に対する脆弱性を指摘しているため、以下にその詳細を報告する。

(ｉ) 論文名：不正 CAN データ送信を抑制するホワイトリスト・ハブ

・著者：関口 大樹*、向達 泰希*、吉岡 克成*、松本 勉*

・所属：*横浜国立大学

上記論文に、CAN プロトコルに対する攻撃経路と攻撃の種別が記載されている。

a. CAN に対する攻撃経路

CAN 通信に対して攻撃するためには下記 3 通りの攻撃経路がある。

・外部接続用ポートを用いる：故障診断用ポート OBD-II に攻撃者の端末（PC 等）を接続して、不正な CAN 通信を行う手法である。

・CAN バスや ECU などのハードウェアを用いる：不正 ECU を CAN バスに新たに接続したり、既存の正規 ECU と不正 ECU を取り換えて CAN バスに接続したり、電磁波を照射して正規 ECU に故障を起こしたりすることで、不正な CAN 通信を行う手法である。

・CAN バスに接続する端末のソフトウェアを用いる：Telematics 通信、Bluetooth 通信、音楽ファイルなどメディア通信からの CAN バスに接続する ECU のファームウェアアップデート機能を悪用して ECU のソフトウェアを不正に改竄して、不正な CAN 通信を行う手法である。

b. CAN に対する攻撃の種別

CAN 通信に対する攻撃は下記 2 通りに大別できる。

・盗聴：CAN プロトコルには守秘性がなく、ネットワークがバス型で全メッセージがブロードキャスト配信されるため、上記攻撃経路 2 または 3 により車載ネットワーク内に攻撃者が用意した不正な ECU が存在する場合、不正な ECU は CAN 通信を容易に盗聴できる。OBD-II ポートから受信できる CAN 通信に適切なフィルタリングを行っていない場合は、攻撃経路 3 に接続した攻撃者の端末からも容易に CAN 通信を盗聴できる。攻撃者は盗聴した CAN 通信の内容を分析して、下記の不正なデータ送信攻撃につなげられる可能性がある。

・不正なデータ送信：メッセージの送信元情報や宛先情報、認証機能を付与するといった各経路からの攻撃をフィルタリングする対策が送信されるメッセージに講じられていない場合は、CAN バスに対して、OBD-II ポートや不正 ECU の接続、正規 ECU のソフトウェア改ざんにより、CAN バスに任意の不正なメッセージを挿入することが可能である。不正なメッセージはさらに以下に分類できる。

・DoS 攻撃となるメッセージ：

・CAN の通信規格とは異なる電気信号通信を CAN バスに挿入する。

・正規 ECU が送信することがない CAN ID のメッセージを挿入する。

・高頻度で何らかのメッセージを挿入する。

・誤動作に繋がるメッセージ：

・攻撃者による端末・ECU が他の ECU になりすまして不正なメッセージを挿入する。例えばあるメッセージが本来流れえないタイミングでメッセージを不正挿入する。

・メッセージ内のデータ値を不正な値に偽造して、受信 ECU の誤動作を誘発させる。

③ The 32nd Symposium on Cryptography and Information Security（SCIS 2015）

・開催期間：2015 年 1 月 20 日（火）～ 2015 年 1 月 23 日（金）

・公開論文数：322

会議全体 322 件に対して、自動車のセキュリティに関する発表が 14 件存在する。うち 3 件は車車間、路車通信といった無線通信に関する研究であり、本報告書の範囲外である。残り 11 件は車内通信プロトコル CAN に対する脆弱性を指摘しているため、以下にその詳細を報告する。

(ⅰ) 論文名：CAN における再同期を利用した電気的データ改ざん

・著者：松本 勉*、中山 淑文*、向達 泰希*、土屋 遊*、吉岡 克成*

・所属：*横浜国立大学大学院環境情報研究院

上記論文に、CAN プロトコルで規定されているノードの再同期機構の脆弱性を利用したメッセージの改ざん攻撃手法の理論と、CAN バスの実験環境における攻撃の実証結果が記載されている。

a. CAN プロトコルの再同期機構

ここでは上記論文で利用されている再同期機構の脆弱性に関わる機構について説明する。CAN プロトコルにおいて 1 ビットの電気信号は以下の 4 つのセグメントから構成される。

・シンクロナイゼーションセグメント（SS）

・プロパゲーションタイムセグメント（PTS）

・フェーズバッファセグメント 1（PBS1）

・フェーズバッファセグメント 2（PBS2）

各セグメントは Tq という最小単位で構成される。1 ビットを Tq にまで分割する構成を「ビットタイミング」と呼ぶ。SS は 1Tq、PTS は 1～8Tq、PBS1 は 1～8Tq、PBS2 は 1～8Tq の範囲で実装される。図 3.2c.3-6 は 1 ビット内のビットタイミングを表している。PBS1 の終端をサンプルポイント（SP）と呼ぶ。ノードは SP 時点の電位によって受信した信号がドミナント(0)かレセシブ(1)かを判断する。また、PTS と PBS1 を合わせて TSEG1、PBS2 を TSEG2 と呼ぶ。

TSEG1 と TSEG2 は下記のハード同期機構、再同期機構のために Tq 長がリシンクロナイゼーションジャンプ幅（SJW）の範囲で増減する。

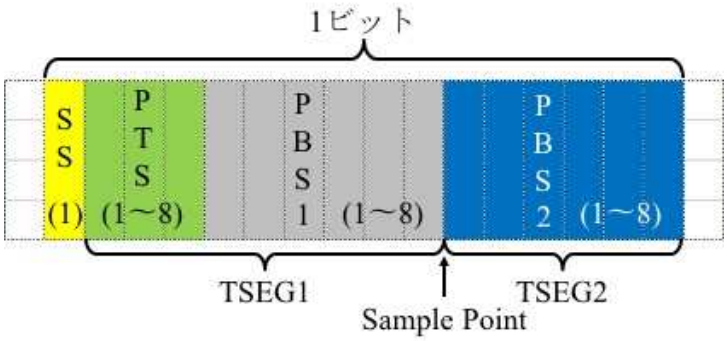


図 3.2c.3-6　1 ビット内のビットタイミング
（例として PTS = 3Tq、PBS1 = 6Tq、PBS2 = 6Tq の場合を示す）

同期機構：
CAN バスに接続するそれぞれのノードは内部に水晶振動子（クロック）を有し、プログラム処理などを行うための基準時間を生成している。各ノードが自身のクロックを利用して、CAN バス上に流れる電位がドミナントあるいはレセシブ何ビット分の長さかを判断している。各ノードは外気温や振動など外的要因の影響によりクロックにずれが生じる場合がある。くわえて CAN バスを流れる電気信号が遅延を生じる場合もあるため、各ノードの 1 ビットの長さに違いが生じて正常なデータのやりとりが困難になる場合がある。そのため各ノード間のクロックのずれを補正するための「同期」と呼ばれるルールが各ノードに規定されている。CAN バスを流れる電位がレセシブからドミナントへ変化する際に同期が行われる。

再同期機構：
送信ノードによる CAN バス上の電位変化を基準にして、受信ノードが行う同期合わせの機構である。具体的には、バス上の信号がレセシブ(1)からドミナント(0)に変化するエッジと呼ばれるタイミングを受信ノードが検出するたびに、あらかじめ定められた SJW を Tq 数の増減の限度として、自身の PBS1 の Tq 数を増加させたり PBS2 の Tq 数を減少させたりして同期を行う。図 3.2c.3-7 にエッジが TSEG1 にある場合の受信ノードの再同期手順を示す。図 3.2c.3-7 では送信ノードに対して受信ノードのクロックが早いため、受信ノードが PBS1 の Tq 数を SJW の範囲内で増加させて同期している。図 3.2c.3-8 にエッジが TSEG2 にある場合の受信ノードの再同期手順を示す。図 3.2c.3-8 では送信ノードに対して受信ノードのクロックが遅いため、受信ノードが PBS2 の Tq 数を SJW の範囲内で減少させて同期している。

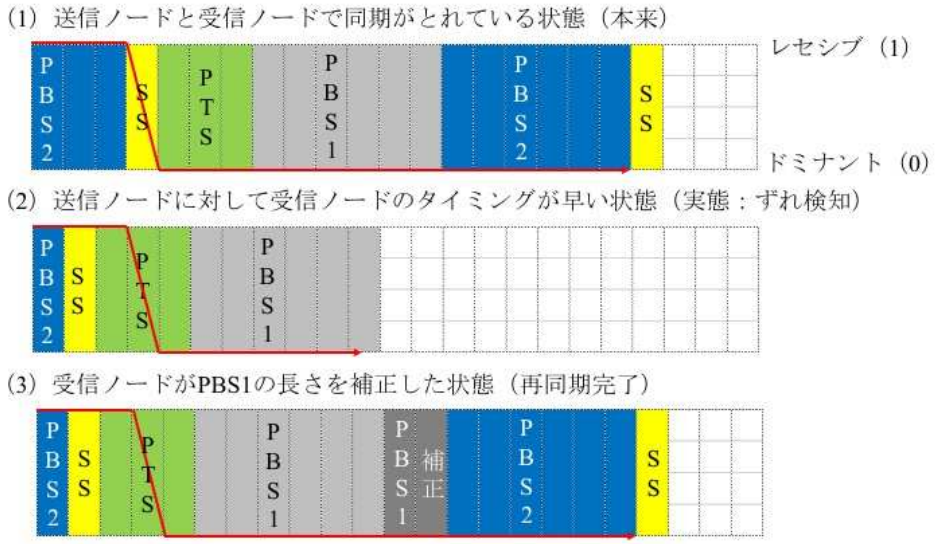


図 3.2c.3-7　受信ノードの再同期手順：受信ノードのエッジが TSEG1 にある場合
（赤実線は CAN バスに流れた電気信号を表す）

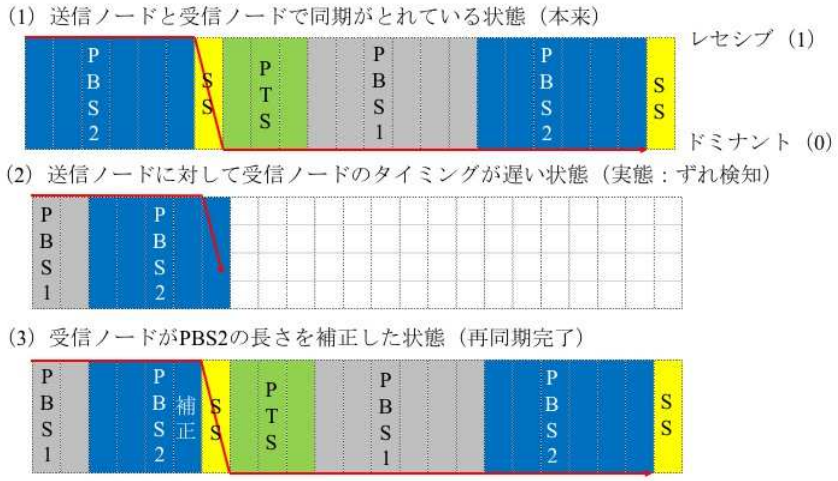


図 3.2c.3-8　受信ノードの再同期手順：受信ノードのエッジが TSEG2 にある場合
（赤実線：CAN バスに流れた電気信号を表す）

b. メッセージの改ざん攻撃手法

著者らは再同期機構の脆弱性を利用した以下の手順によって、CAN バス上に送信されたメッセージをリアルタイムで改ざんして、送信ノードには改ざんを検出させずに受信ノードに改ざんデータを受信させることが可能であると主張している（図 3.2c.3-9）。攻撃者は送受信ノードのバス間に物理的に存在して、送受信ノード間に流れる CAN バスの電位を変更可能だと仮定する。加えて、電位操作前の時点では送受信ノードは同期できているものとする。なお、電位操作前の時点で送受信ノードが同期ずれを起こしている場合における電位操作攻撃は同著者らによって報告されている（後述の CSS 項「題：電気的データ改ざんに対する CAN のインテグリティ強化策」を参照のこと）。攻撃者は以下の 2 つの電位操作を行うことで改ざんしたデータを受信させる。

電位操作 I：
まず、攻撃者は受信ノードの SP のタイミングを送信ノードの SP のタイミングより遅くなるようにずらしたい。改ざん対象のビットもしくはその直前のビットがバスに流れているタイミングかつ、バス上の電位レベルがレセシブ（1）からドミナント（0）へと変化するビットに対して電位操作を行う。具体的には SJW の範囲内で数 Tq の時間分レセシブからドミナントに変化するのを遅らせるように電位操作する。図 3.2c.3- 9 では 2Tq だけ変化を遅らせている攻撃を例示している。本操作によって受信ノードは図 3.2c.3-7 の状態に陥る。受信ノードは同期ずれを検知して再同期を行うため、PBS1 を増加して補正する。そのため受信ノードの SP のタイミングが送信ノードの SP のタイミングより遅くなる。

電位操作 II：
攻撃者は送信ノードにビットエラーを検出させることなく受信ノードには改ざんしたビットを受信させたい。電位操作 I で送受信ノードの SP のタイミングをずらしたことにより、送信ノードの SP と受信ノードの SP の間に時間差が発生する。本時間差において行う電位操作を電位操作 II と呼ぶ。具体的には送信ノードの SP のタイミングより後かつ、受信ノードの SP のタイミングに合わせて電位操作 II を行う。送信ノードは自身の SP より後の電位の変化に対してはビットエラーを検出することができない。そのため電位操作 II に対して送信ノードはエラーフレームを流すことはない。かつ受信ノードは改ざんされた電位を受信する。

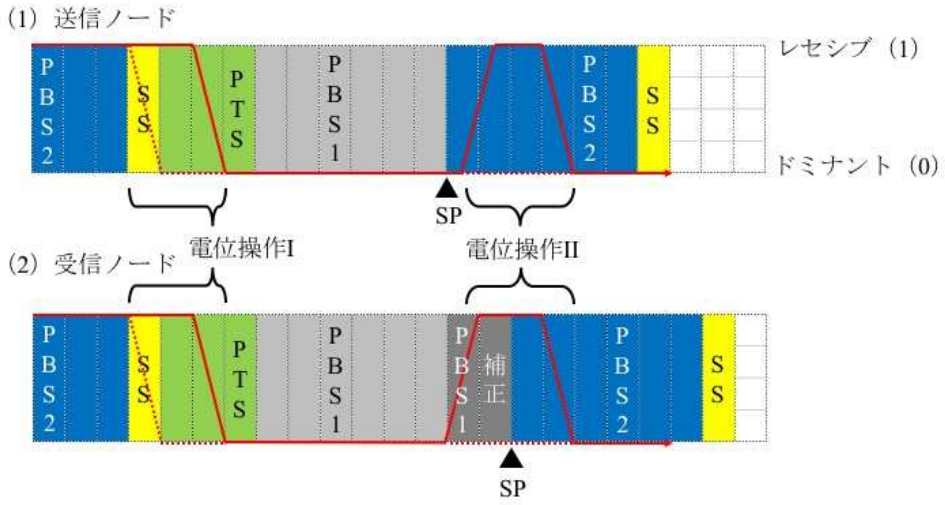


図 3.2c.3-9　電位操作のタイミング。
赤実線：電位操作され CAN バスに実際に流れた信号、
赤点線：送信ノードが流した信号、を表す。

一方、CSS の論文で報告されている攻撃手法について詳細を述べる。前述のとおり、本攻撃では前提として攻撃者による電位操作前の時点で、何らかの要因によって送受信ノードが同期ずれを起こしており、さらに再同期が実施される前のタイミングであることを仮定する。そのため攻撃者にとって送信ノードにはエラーフレームを送信させずに受信ノードに改ざんメッセージを受信させるためには、電位操作 I を実行することなく、電位操作

II を実施するだけでよい。

c. 実証実験環境と結果

著者らは図 3.2c.3-10 の構成で CAN バスを模擬して前述のメッセージ改ざんが可能であることを検証し報告している。送信ノードにエラーフレームを送信させることなく、Data フィールドと CRC シーケンスの値を変更することができたと報告している。また同様に②CSS 2014 の報告では、図 3.2c.3-11 の構成で前述のメッセージ改ざんが可能であることを検証し報告している。

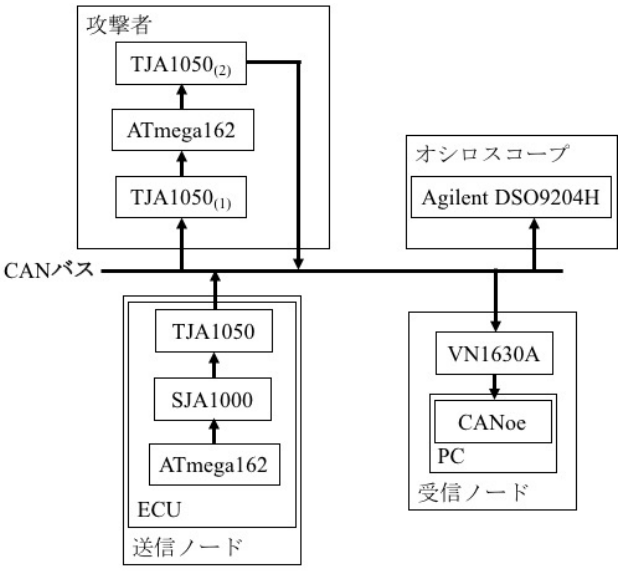


図 3.2c.3-10　提案手法における実験機器構成

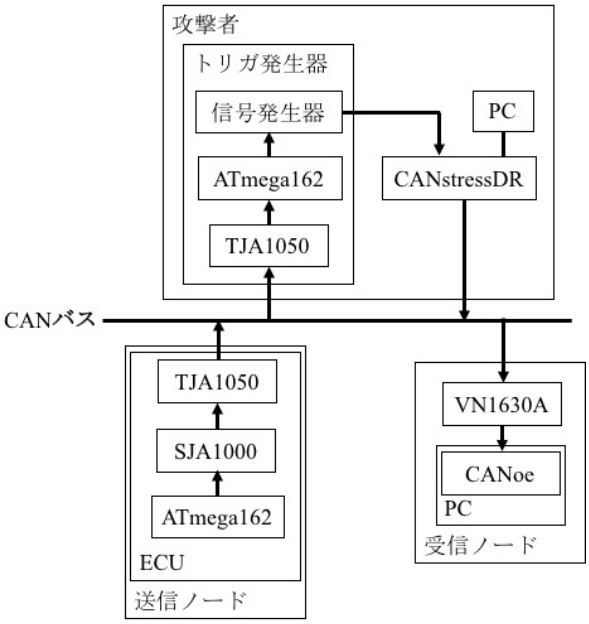


図 3.2c.3-11　CSS 2014 攻撃における実験機器構成

(ⅱ) 論文名：車載 ECU に対する CAN 経由のファジング手法

・著者：松本 勉*、小林 優希*、土屋 遊*、吉田 直樹*、森田 信義†、萱島 信†
・所属：*横浜国立大学大学院環境情報研究院、†株式会社日立製作所

上記論文は CAN に接続する車載 ECU に対するファジングの実施方法を提案している。ファジングとはソフトウェア製品の脆弱性を検証する手法の一つである。具体的にはファズと呼ばれる検査対象のソフトウェアが問題を引き起こしそうなメッセージを送信して、そのメッセージに対するソフトウェアの応答に着目することでソフトウェアの不具合を見つける手法である。上記論文は CAN プロトコルに対する脆弱性や攻撃手法を指摘するものではない。ただし上記論文ではファジングを行う際に CAN メッセージをどのように加工できるかが検討されている。ファジングにいて加工可能な CAN メッセージの項目とは、CAN メッセージを用いる攻撃者にとっても悪用できる項目と読み換えることができる。そのため以下に上記論文が指摘する CAN メッセージの加工可能な項目について述べる。

a. CAN 経由で送信可能なファジングメッセージ

CAN バスに接続するノードに対してファジングにおいて CAN 経由では以下のパラメータを変更することができる。

・CAN 経由で送信可能なメッセージフレーム：CAN の仕様で定められたメッセージフレームは以下の通りに分けられる。なお各メッセージフレームの詳細は CAN プロトコルの仕様を参照のこと。

－データフレーム
－リモートフレーム
－エラーフレーム
－オーバロードフレーム
－インターフレームスペース

CAN の仕様で定められていないメッセージフレームは以下の通りである。

・各フレームの一部を改変したビット列
・メッセージ送信のタイミング：メッセージの送信タイミングについて以下の通りに分けられる。
・定期送信：送信周期を設定し、周期的なメッセージ送信を行う。
・イベント送信：特定のイベントが発生したときだけメッセージの送信を行う。
・他ノードと同タイミングの送信：他の ECU と同タイミングで送信を行う。CAN プロトコルで定められているメッセージの優先度を判断する調停が起きる。
・高頻度送信：通常の送信周期よりも短い送信周期でメッセージを送信する。

攻撃者は攻撃を行うために CAN バスに流す何らかのメッセージについて、以上で挙げた項目を加工することになる。例えば、1）データフレームに対してメッセージ ID を当該 CAN ネットワーク内では用いられない ID に変換してメッセージを送信する、2）通常想定されない高頻度でデータフレームメッセージを送信する、などといった CAN メッセージ

が自動車に何らかの不正動作を引き起こす可能性が考えられる。上記論文では以下の実験環境に対して、比較的簡単に加工できる 3 通りのファズを用いて CAN 経由のファジングを実験している。実験環境は図 3.2c.3-12 のとおりである。

・評価対象：IndirectNM パッケージ（サニー技研製評価ボード S810-CLG3-85 に搭載された、ルネサス社製マイコン M30853 FJGP 上に実装された TOPPERS NonOS 対応 CAN 通信ミドルウェア）
・評価対象の通信相手：Vector 社製 CANoe8.2.64.2（VN1630A を CAN インタフェースとする PC にインストールされたソフトウェア）
・CAN バスに電気的障害を発生させる機器：Vector 社製 CANstressDR

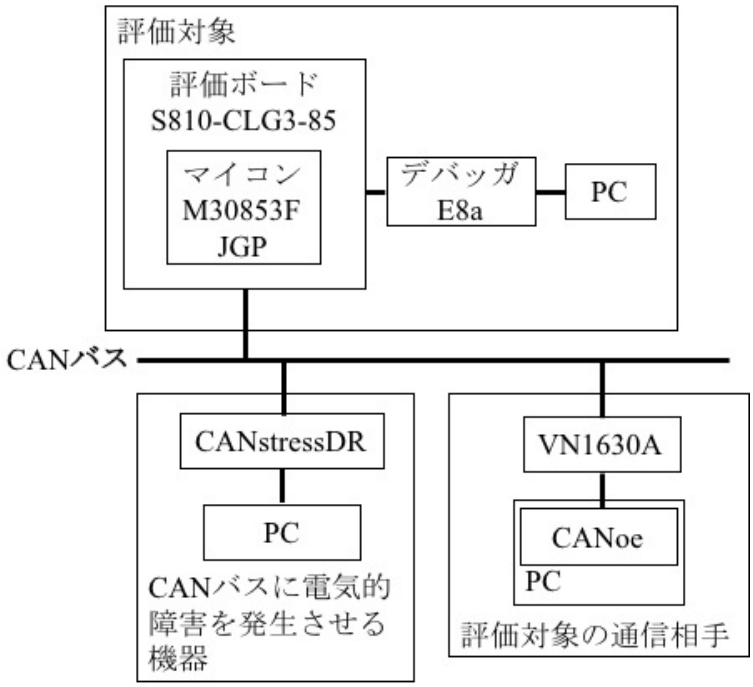


図 3.2c.3-12　実験環境と実験機器の構成

ファズ項目 1：

ID フィルタリング検証／不使用 ID 送受信実験：評価対象が受信側の場合について CAN ID フィルタリング機能が適切に動作しているかどうかを検証している。評価対象が受信しないはずの CAN ID が指定されたメッセージを送信者 CANoe から評価対象に送信周期 100 ミリ秒で 10 セット、送信周期 10 ミリ秒で 1000 セット送信する。次に各送信メッセージに対する評価対象の挙動を検証する。本実験では評価対象は想定外の挙動を示すことはなかった。そのため適切に評価対象は CAN ID をフィルタリングできていると言える。

ファズ項目 2：

高負荷時動作検証／高頻度送信実験：評価対象が受信側の場合について高頻度にメッセージを受信して高負荷がかかった場合の動作について検証している。評価対象が受信して処理を行う CAN ID が指定されたメッセージを CANoe から評価対象に通常想定されるよりも高頻度（送信周期 1 ミリ秒）で送信し続ける。評価対象について受信メッセージを処理す

る挙動について検証する。本実験では評価対象が処理するよりも早く受信キューにメッセージが貯まっていったものの、メッセージの受信周期ではなく評価対象自体の周期で処理が行われた。高頻度送信によって評価対象自体の処理遅延（DoS）は観測されなかった。

ファズ項目 3：
エラー処理検証／エラー誘発メッセージ送信実験：評価対象が送信側、受信側双方の場合についてエラーカウンタの値に応じたノードの状態遷移が適切に行われているか検証している。まず CANstressDR は評価対象と CANoe が通信するメッセージのペイロード 1 ビット目の値を改変する。評価対象はエラーフレームを CAN バスに送信しエラー内容に合わせて自身のエラーカウンタを上昇させる。CANstressDR による改変を繰り返し実施し、エラーカウンタの値に合わせて評価対象の状態が遷移するかを検証する。本実験では評価対象が送信側の場合における状態遷移が CAN の仕様とは異なることを発見している。さらにミドルウェアのソースコードに該当する箇所を特定することまで行っている。

(ⅲ) 論文名：攻撃メッセージの無効化機能を備えたホワイトリスト CAN ハブ

・著者：矢嶋 純*、武仲 正彦*、長谷部 高行*
・所属：*富士通研究所

上記論文は、何らかの手段によってマルウェアに感染したノードが存在する CAN ネットワークにおいて、感染ノードによる攻撃メッセージの送信を防ぐために、CAN ネットワークにおけるホワイトリスト方式の CAN ハブ（中継機器）を提案している。提案手法が対策できると主張している攻撃 CAN メッセージは以下のとおりである（図 3.2c.3-13）。

まず本来 ID が Y のメッセージだけを送信する ECU1 がマルウェアに感染するなどして ID X のメッセージを送信するように改ざんされる。すなわち ECU1 は CAN ID のなりすましメッセージを送信するように改ざんされる。次に ECU1 から送信される ID X の不正メッセージは CAN ハブを通じて ECU2、ECU3 に到達する。ID X のメッセージを受信すると何らかの処理を行う ECU2 は不正なメッセージに対して誤作動を起こす可能性がある。つまり攻撃が成功する。一方 ID Y のメッセージを受信すると何らかの処理を行う ECU3 は ID X の不正メッセージに対して処理を行わないため、ECU3 は誤作動を起こさない。

前述の攻撃は CAN プロトコルにおける 2 つの特徴から実現可能だと言える。

特徴 1：
CAN メッセージには ID が存在するものの、TCP/IP のような送信先、送信元に関する情報がない。

特徴 2：
CAN はブロードキャスト通信であるから CAN バスに接続する ECU1 が送信したメッセージを同一バスに接続された全ての ECU が受信する。

上記論文ではCANハブの通信調停ユニットと各CANトランシーバ間に改造を施すことで前述の攻撃をフィルタリングできる方式を提案している。

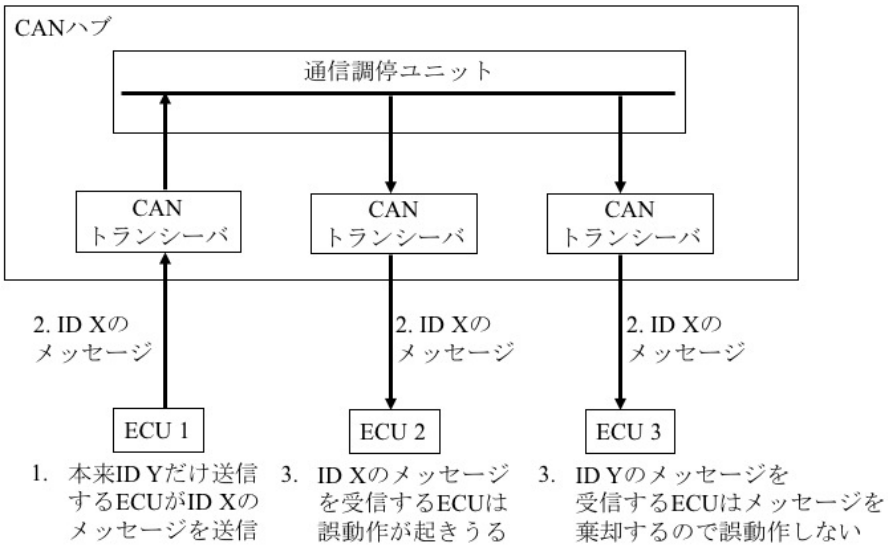


図 3.2c.3-13　CANの通信調停ユニット

(ⅳ) 論文名 車載CAN通信暗号化デモシステムの構築とサイドチャネル攻撃評価

・著者：久保田 貴也*、中野 将志**、倉地 亮†、本田 晋也†、汐崎 充*、藤野毅‡

・所属：*立命館大学総合科学技術研究機構、**立命館大学理工学研究科、†名古屋大学大学院情報科学研究科、‡立命館大学理工学部

上記論文は、CANメッセージの暗号化手法の提案と、暗号化CAN通信のセキュリティ評価を目的としたデモシステムの構築と提案手法の動作確認、同デモシステム内のマイコンに対するサイドチャネル攻撃評価を実施している。

デモシステムの構成は以下のとおりである（図3.2c.3-14）。株式会社ヴィッツ製の「車載 CAN 通信学習キット（1)」を複数用いて、コントローラからの入力に対してラジコンカーの制御を模擬している。通常のCANネットワークと提案方式が実装されたCAN通信を行うAES CANネットワークとに対して、下述するなりすましECUによる攻撃を検証できる。なお、AES CANでは各ECUとCANバスとの間に共通鍵暗号AESの暗号回路を実装したFPGAボードTerasic社製Altera DE2-115を接続することで提案手法による暗号化通信を実現している。

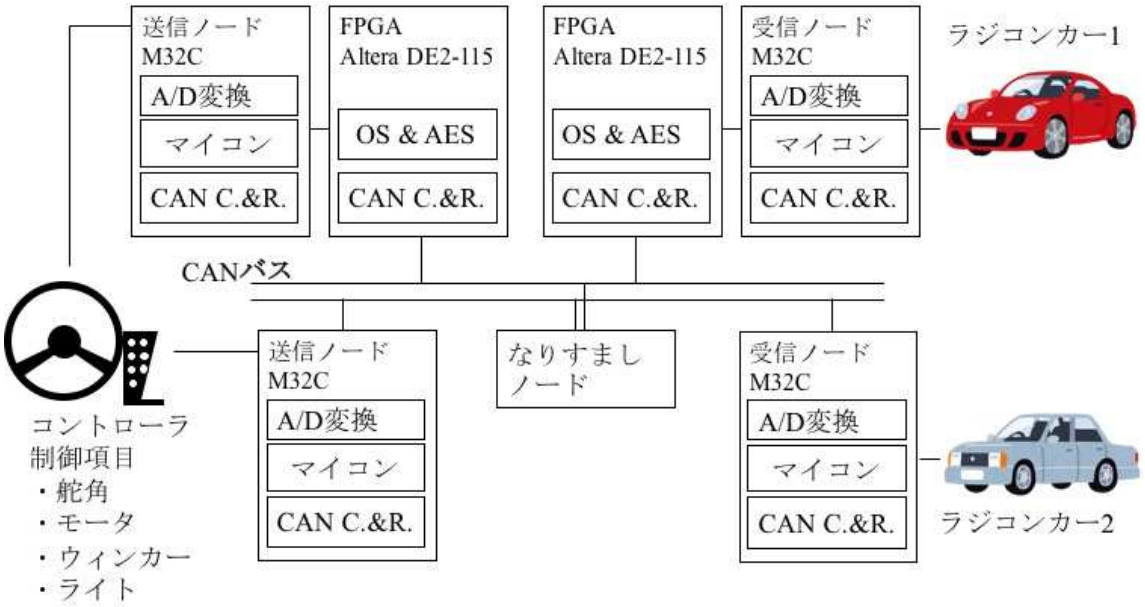


図 3.2c.3-14　車載 CAN 暗号通信デモシステム

上記のデモシステムでは以下の攻撃シナリオを想定する。

- 送信 ECU：コントローラから読み取ったステアリングの舵角、アクセルの踏量、ブレーキの踏量を受信 ECU に定期的に送信する。そしてウィンカ、ライトの点灯というイベントもその都度送信する。
- 受信 ECU：送信 ECU からの CAN メッセージを受信してタイヤの角度やモータの回転数を制御する。加えてウィンカ、ライトの点灯も実施する。
- なりすまし ECU：送信 ECU になりすまして CAN メッセージを送信し、ステアリングやモータ、ウィンカ、ライトの制御の乗っ取りを試みる。

提案手法の前提として、正規の送信 ECU と受信 ECU が AES の秘密鍵を事前に共有しているとする。送信 ECU はコントローラから読み取った信号と固定値を AES で暗号化してから送信し、受信 ECU は復号を行うとともに、復号した文に固定値が含まれているかどうかを確認してメッセージを棄却するか容認するか判断する。暗号化が施されていない通常の CAN ネットワークでは、なりすまし ECU は CAN バスを盗聴して送信メッセージの形式を解析することで、容易に自動車の制御を乗っ取ることができる。

一方、提案手法が施された CAN ネットワークでは、なりすまし ECU は CAN バスを盗聴してもメッセージの意味を読み取ることができない。なりすまし ECU は暗号化に用いる秘密鍵の値を知らないため、暗号文に偽装された不正メッセージを受信 ECU が復号すると前述の固定値が含まれている可能性はきわめて低い。受信 ECU は不正メッセージをほぼ確実に棄却できるため、なりすまし ECU による乗っ取りは失敗する。ただしなりすまし ECU は、盗聴した暗号化メッセージをそのまま不正なタイミングで送信することで受信 ECU に不正なタイミングでメッセージを容認させるリプレイ攻撃が可能である。

上記論文では、CAN プロトコルにはリプレイ攻撃の対策が規定されていないため提案手法のような暗号化による対策だけではすべてのなりすましを防ぐことはできない、と指摘している。

提案方式は AES の秘密鍵が秘匿されている事が安全性の基点となっているため、秘密鍵の値が漏洩すると提案方式の安全性は保証できない。そのため上記論文では ECU が AES を演算している際に発生する電磁波や消費電力、処理時間といったサイドチャネル情報から秘密鍵を窃取するためにはどの程度の解析が必要か実験している。ECU 自体に関する評価は本調査の範囲外のため解析結果の詳細は省略する。

(ｖ) 論文名：車載システムにおける低電圧時のマルウェア挙動

・著者：田中 卓*、大久保 隆夫†
・所属：*兵庫県立大学院、†情報セキュリティ大学院大学

上記論文は、CAN を代表とする車載ネットワークプロトコルに対するセキュリティ対策の提案技術の限界について、ECU に供給される電力の観点から指摘している。特に電源オフ時の暗電流や縮退運転時といった電源が十分に確保できない状態における ECU の挙動について、そして供給される電力の値を偽装することによる不正な制御について議論されている。ここでは後者の電力値の偽装に関する議論について整理した。

上記論文では車載ネットワークを 2 種類に大別している。まず CAN や LIN を代表とする通信系ラインと呼称するノード間の情報通信のためのネットワークである。次に電力供給系ラインと呼称するノードに電力供給を行うネットワークである。上記論文では想定される脅威についてパワーウィンドウの制御を例として挙げている。上昇するパワーウィンドウに異物が挟まった場合、ウィンドウを下降させる機能が存在する。そして異物の検出方法として 1）ウィンドウの上昇速度を通信系ラインから監視して上昇速度が落ちた場合に異物が挟まったと判断する、2)ウィンドウを作動させるモータの消費電力を電力供給系ラインから監視して異物が挟まった場合の消費電力の変化から判断する、という 2 方式を挙げている。

パワーウィンドウが電力供給系ラインの情報を基に制御する方式である場合は、たとえ通信系ラインに対して不正メッセージ阻止などのセキュリティ対策を行ったとしても、電力供給系ラインの消費電力情報が偽装されて不正な制御が行われうる。車内の全 ECU に対する電源供給は特定の ECU によって制御されているため、通信系ラインのセキュリティ強化とともに電源供給系ラインもまた何らかのセキュリティ対策を講じる必要があると上記論文は指摘している。

(vi) 論文名：車載ネットワークにおける CAN フィルタの提案

・著者：氏家 良浩*、岸川 剛*、芳賀 智之*、松島 秀樹*、田邉 正人†、北村 嘉彦†、
安齋 潤†
・所属：*パナソニック株式会社先端研究本部、†パナソニック株式会社 AIS 社

上記論文は、CAN のセキュリティ上の脅威を列挙して、その対策として CAN メッセージのフィルタリング技術を提案している。以下の脅威が指摘されている。

・盗聴：CAN メッセージの内容が不正に取得、解析されること
・なりすまし：特定の ECU に対して誤動作を起こすために正規の ECU になりすましたメッセージを送信する。
・DoS 攻撃：優先度が高い CAN ID のメッセージを高頻度で送信することでバスを通信不能にする。

これらの脅威が想定できる理由として、CAN プロトコルの以下の特徴を挙げている。

・バス型のネットワークのため、全メッセージがブロードキャストされる。
・CAN ID だけで受信して処理すべきメッセージかどうか判断する。
・CAN ID だけによってメッセージの送信優先度が決まる。

上記論文は、攻撃が成功した場合自動車が危険な状態に陥る可能性が高いという観点からなりすましが CAN プロトコルでは特に問題であると指摘している。そして、なりすましを行う攻撃者をその能力によって 2 段階に分けている。

第 1 段階：
不正なメッセージを CAN バスに送信可能だが、攻撃対象の CAN メッセージの仕様は知らない。
第 2 段階：
不正なメッセージを CAN バスに送信可能かつ CAN メッセージの仕様を知っている。

上記論文では第 1 段階の攻撃者に対するフィルタリング手法を提案している。第 1 段階の攻撃者が送信する不正なメッセージを具体的に述べると、

・盗聴により得られた正規メッセージに基づき、CAN ID やペイロードをそれらしく設定した不正メッセージを送信する。
・盗聴により得られた正規メッセージを不正なタイミングで再送信する。
・大量のメッセージを高頻度で送信する。

の 3 通りである。第一段階の攻撃者は攻撃対象の CAN 仕様を精確に把握していないため、ID などの値や送信タイミング、送信頻度を当て推量で変化させることになる。そのため第 1 段階の攻撃者が送信する不正メッセージは結果的にランダムな攻撃と見做すことができると捉え、ランダムなメッセージと正規のメッセージとを識別するフィルタリング技術を提案して提案手法の検知率／誤検知率を試算している。

(vii) 論文名：車載ネットワーク向けメッセージ認証方式の提案

・著者：森田 信義*、伯田 恵輔*、大和田 徹*、萱島 信*
・所属：*株式会社日立製作所

上記論文は、ECU のなりすましについて、対策として CAN メッセージ認証方式を提案している。特に提案方式は電気的ノイズによって値が一部変化した正規メッセージと、なりすましのために改ざんされたメッセージとを判別できると謳っている点が他のメッセージ認証方式の提案と比べて特徴的である。まず上記論文では以下の攻撃者を仮定する。

・インタフェース：攻撃者が CAN に接続するには自動車に予め装備されている OBD−II ポートを利用する。
・能力 1：インタフェースを通じて ECU 間の CAN 通信を傍受できる
・能力 2：インタフェースを通じて各 ECU にメッセージを送信できる
・能力 3：インタフェースを通じて送信するメッセージは任意の値に変更できる

そして攻撃者は以下のいずれかの攻撃を実施する。

・リプレイ攻撃：傍受したメッセージを任意のタイミングで OBD-II ポートから送信する。
・ノイズへのなりすまし：傍受したメッセージを任意の値に改ざんして任意のタイミングで OBD-II ポートから送信する。特に対象の CAN において誤り訂正可能な符号誤り率（BER）の範囲内のビット反転による値の改ざんをノイズへのなりすましと定義する。
・パケット改ざん：傍受したメッセージを任意の値に改ざんして任意のタイミングで OBD-II ポートから送信する。特に BER の範囲を超えるビット反転による値の改ざんをパケット改ざんと定義する。

提案手法ではメッセージ認証子 MAC の再利用によるリプレイ攻撃を防ぐために、メッセージと送信の都度更新されるカウンタとを基に MAC を更新する。MAC の検証が正しく行われるためには送信 ECU と受信 ECU のカウンタが一致していなければならない。受信 ECU が MAC の検証に失敗した場合、その理由が 1）ノイズによる値変化であるならば、送信 ECU のカウンタは上昇しているので、受信 ECU のカウンタも上昇しなければ次回以降のメッセージ全てで MAC の検証に失敗してしまう。理由が 2) メッセージの改ざんであるならば、送信 ECU のカウンタは上昇していないため、受信 ECU はカウンタを上昇してはいけない。そのため提案方式では電気的ノイズによって値が一部変化した正規メッセージと、なりすましのために改ざんされたメッセージとを判別できるように誤り検出訂正技術を導入している。

すなわち上記論文では、CAN メッセージのフレームには CRC シーケンスが規定されているため単純な誤り検出は可能であるが、より高度な検証を行うためには CRC は不十分であると指摘している。

(viii) 論文名：車載制御ネットワークにおける送信周期監視システムの提案

・著者：倉知 亮*、高田 広章*、上田浩史†、堀端 啓史†
・所属：*名古屋大学大学院情報科学研究科付属組込みシステム研究センター†、株式会社オートネットワーク技術研究所

上記論文は、CAN プロトコルについて、周期的に送信されるメッセージに対するなりすまし攻撃を紹介し、なりすましを阻止する手法を提案している。また実車両から取得した CAN バスのログを用いて提案手法のなりすまし阻止の性能を評価している。提案手法の概略は次の通りである。CAN バスに監視ノードという振る舞い検知を行う端末を新たに追加することで、監視ノードがなりすましメッセージを検知した際にはエラーフレームを用いてなりすましメッセージを棄却する。監視ノードの検知ルールの詳細については本報告書の範囲外であるため省略する。

以下の手順でなりすまし攻撃を模擬し、そして提案手法の性能を評価している。なお、評価環境が明示されていないものの、FPGA 上に実装する前の予備実験であることが明示されているため、本評価環境は汎用 PC 上で模擬したものと推測される。

手順 1：
走行中の実車両から CAN バスに流れるメッセージのログを取得する。
手順 2：
メッセージログになりすましメッセージを追記し、改ざんメッセージログを作成する。具体的にはメッセージログに周期的な送信が観測される CAN ID を割り出して、なりすましメッセージを周期的な CAN ID のメッセージの直後に追加する。
手順 3：
改ざんしたメッセージログに対して提案手法の振る舞い検知ルールを適用し、正規メッセージとなりすましメッセージそれぞれに対して監視ノードがエラーフレームを送信するかどうか評価する。

手順 1 について、メッセージログの取得方法は明示されていない。おそらく OBD-II ポートに専用機器を接続して CAN バスに流れるメッセージを吸い出したと想定される。手順 2 について、追記されたなりすましのメッセージの具体的な内容は明示されていない。なりすましによる攻撃者の目的は、受信ノードがなんらかの誤動作を引き起こすことだと考えられる。正規のメッセージ周期に同期してなりすましメッセージを流す攻撃パターンを上記論文ではコバンザメ攻撃と称している。手順 3 および評価結果について、提案手法によるコバンザメ攻撃の誤検出、見過ごし共に 0%であったと主張している。

(ix) 論文名：車載ネットワークにおける監視・検証モード切換えの提案

・著者：田邊 正人*、北村 嘉彦*、安齋 潤*、岸川 剛†、氏家 良浩†、芳賀 智之†、松島 秀樹†
・所属：*パナソニック株式会社 AIS 社、†パナソニック株式会社先端研究本部

上記論文は、CAN プロトコルを用いるネットワークのセキュリティを向上させるために、各ノードが CAN バスの監視と検証とを切換えながら通信する手法を提案している。

上記論文では CAN における脅威として 2 つの攻撃が想定されると指摘している。

なりすまし攻撃：
ECU は CAN バスを流れるメッセージの CAN ID のみを確認して自 ECU が受信すべきメッセージかどうかを判断する。そのため、何らかの手段により CAN バスにメッセージを流すことができる攻撃者ならば正規の ECU が送信するメッセージと同じ CAN ID のメッセージを送信するだけでなりすますことができる。

DoS 攻撃：
何らかの手段により CAN バスにメッセージを流すことができる攻撃者ならば、CAN ID の調停機能の性質を悪用して、優先順位が高い CAN ID のメッセージを送信し続ける事で CAN バスを麻痺させることができる。

(ｘ) 論文名：車載ネットワークを保護するセキュリティ ECU の提案：HW/SW 協調による更新可能な CAN の保護手法とその評価

・著者：岸川剛†、氏家良浩†、芳賀智之†、松島秀樹†、田邊正人*、北村嘉彦*、安齋潤*
・所属：*パナソニック株式会社 AIS 社、†パナソニック株式会社先端研究本部

上記論文は、CAN プロトコルを用いるネットワークのセキュリティを向上させるために、CAN バスにセキュリティ ECU と呼称される監視機器を新たに追加することによって既存の ECU が不正なメッセージを誤って受信してしまうことを防ぐ方式を提案している。また提案方式の実装評価している。

まず上記論文が指摘する CAN のセキュリティ上の問題点について述べる。CAN ではなりすまし攻撃が容易であることを指摘している。具体的には CAN ID のみに依存してメッセージの受信と破棄を規定する CAN プロトコルでは、送信元が保証されない。そのため攻撃者はなりすまし対象の ECU が送信する CAN ID と同じ CAN ID のメッセージを送信すれば容易になりすましメッセージを送信できる。

次に上記論文の実装評価について述べる。実装評価環境は図 3.2c.3-15 および表 3.2c.3-2 のとおりである。セキュリティ ECU は CAN コントローラ SX-card6 上で受信メッセージの CAN ID が事前登録されたホワイトリストに存在するかどうか確認する。加えて、マイコン ATmega162 上においても受信メッセージの CAN ID が事前登録されたホワイトリストに存在するかどうか確認ならびに受信メッセージが事前登録された送信周期を満たすかどうか確認する。本実装評価はセキュリティ ECU の性能を検証するためのものであるため、不正なメッセージを送信できる送信ノードと監視ノードだけが存在すれば十分であり、受信専用のノードは実装されていない。送信ノードが CAN バスに送信したメッセージについて、CAN ID の値など具体的な記載はないものの、正規の送信ノードとしてメッセージ

を送信したり、攻撃者の送信ノードとしてホワイトリストに登録されていない CAN ID のメッセージを送信したり、そして送信周期を短くして送信を繰り返したりしたと報告している。

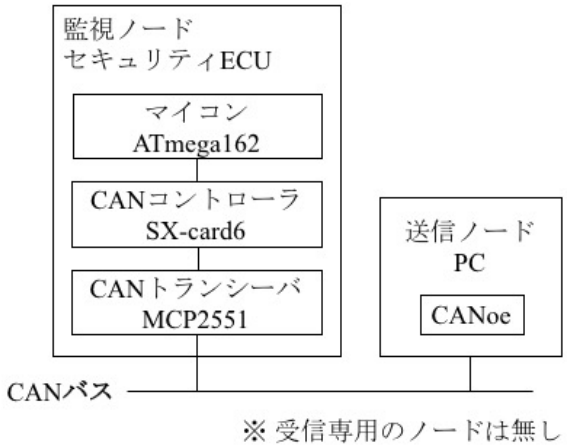


図 3.2c.3-15　実装環境概略図

表 3.2c.3-2　実装評価環境

FPGA ボード	SX-Card6
FPGA 拡張ボード	Card-UNIV3
マイコン	Atmega 162
CAN トランシーバ	MCP2551
FPGA 開発環境	Xilinx ISE 14.7
マイコン開発環境	Atmel Studio 6.1
動作クロック	16MHz
CAN 通信ビットレート	500kbps
CAN シミュレーションツール	CANoe

(xi) 論文名：車載ネットワークを保護するセキュリティ ECU の提案：導入インパクトを抑えた CAN 保護手法のコンセプトとその評価

・著者：芳賀智之†、氏家良浩†、岸川剛†、松島秀樹†、田邊正人*、北村嘉彦*、安齋潤*

・所属：*パナソニック株式会社 AIS 社、†パナソニック株式会社先端研究本部

上記論文は、CAN プロトコルに用いるネットワークのセキュリティを向上させるために、セキュリティ ECU と呼称される監視機器を CAN バスに追加することによって既存の ECU が不正なメッセージを誤って受信してしまうことを防ぐ方式を提案している。上記報告のセキュリティ ECU とは（ix）で報告したセキュリティ ECU と同一の著者による提案である。セキュリティ ECU の監視項目が（ix）の方式とは異なる。そのため、上記報告で指摘される CAN の脆弱性、および実装評価環境は（ix）と同一である。

(6) CSS

① 論文名：CAN における不正送信阻止が可能となる条件

・著者：小林優希*、中山淑文*、松本勉*
・所属：*横浜国立大学大学院環境情報研究院

上記発表論文では、CAN 通信に対する攻撃手法が不正送信阻止方式によって阻止可能となる前提や条件が整理されている。また、不正送信阻止方式に対する新たな脅威となる攻撃手法について考察されている。

(ⅰ) 不正送信阻止方式

論文 [29] [30]にて提案されている CAN プロトコルの保護手法である。本来自ノードが送信するはずのメッセージが他のノードから送信されたことを検知し、エラーフレームを用いて不正メッセージの送信を中断させる。その結果、再度不正メッセージが送信される際には、不正メッセージとエラーフレームの送信が繰り返されるため、不正メッセージの送信を行うノードはエラーカウンタの値が上がり、ノードの状態がバスオフに遷移し、バスに対するすべての操作が禁止される。

以下に、論文発表者が調査を行った CAN プロトコルに対する攻撃手法に関して、想定する攻撃者の保持する能力、攻撃概要および調査した攻撃手法によって不正送信阻止方式を実装されたノード（以下、不正送信阻止ノード）に攻撃を行った際の影響を整理した。

これらの攻撃手法に共通する方法として CAN プロトコルのエラー検出と検出した場合の対応に関する仕様を利用している。
その仕様は具体的には、CAN プロトコルは ECU の故障等によって正常でないメッセージが繰り返し送信された場合に、そのエラーを CAN バスの電気信号から検知し、正常でないメッセージを送信している ECU 自身が送信制限を行うものである。不正送信阻止方式を実装したノードに対する攻撃手法は、この仕様を利用することで不正送信阻止を実装したノードを CAN バスから切り離し、保護を無効化することで、最終的に意図したなりすましメッセージを送信する。

(ⅱ) なりすましメッセージ送信

a. 攻撃概要
OBD-Ⅱポートや不正 ECU の接続、正規 ECU の改ざんによりバス上に任意のメッセージを挿入することが可能であるため、他の ECU になりすまして不正メッセージを送信する攻撃である。

b. 想定する攻撃者の保持する能力
・CAN の本来の仕様に準拠した CAN コントローラを使用可能。
・攻撃者ノードはエラー状態へ遷移する。（エラーパッシブ、バスオフの状態へ遷移す

る）
・CAN のメッセージ形式でのみバス電圧変更が可能。

c. 不正送信阻止手法を実装されたノード（被攻撃者）に対する攻撃手法の影響

・被攻撃者は攻撃者が不正メッセージを送信したことを検知することが可能。被攻撃者が CAN メッセージにより他のノードに対して、被攻撃者の送信メッセージがエラーメッセージであることをアクティブエラーメッセージにより通知することができる。
・攻撃者のメッセージ送信を妨害するアクティブエラーメッセージの送信によって、被攻撃者のエラーカウンタは増加せずエラー状態遷移は起こらない。

CAN では全てのメッセージを観測できるため、受信した正規メッセージを再度バス上になりすましメッセージとして送信することや、送信にあたっては一般的な CAN コントローラでなりすましメッセージを送信することが出来るため、通常の ECU を乗っ取る、もしくは追加で通常 ECU を接続することで簡単になりすまし送信を実行することが出来る。

攻撃実施の難易度は低い。このため、不正送信阻止ノードに対する影響も低く、不正送信阻止手法によって攻撃を保護することが出来る。

(ⅲ) サンプリングポイントのずれ

a. 攻撃概要

不正送信阻止手法を回避する攻撃手法として論文 [31] [32]にて提案されたものである。バスに接続されたノードのサンプリングポイントが送信ノードと受信ノードで異なっていることに注目した攻撃手法である。CAN では送信ノードが自ら送信したビットとバス上に現れた実際の信号をサンプリングした結果のビットとが一致しているかを確認し、不一致を検知した場合にはビットエラーとして扱う仕組みがある。

また、受信ノードは自らが計算した CRC 値と、受信したメッセージに含まれる CRC 値を比較することにより、誤りを検出する仕組みがある。

しかし、送信ノードと受信ノードにおいてバス上を流れるビットをサンプリングする時点が異なっている場合には、受信ノードのサンプリングポイントの付近に電気的改ざんを行うことで、送信ノードに検知されることなく、受信ノードに不正メッセージを受信させることが可能である。

また、送信ノードと受信ノードのサンプリングポイントがずれていない場合でも、CAN の機能である再同期を電位差操作により誘発することで、サンプリングポイントのずれを作り出すことができる。

b. 想定する攻撃者の保持する能力

・CAN の仕様に準拠しない CAN コントローラを使用可能。
・攻撃者ノードはエラー状態へ遷移しない。（エラーパッシブ、バスオフの状態へ遷移

しない）
・任意の手段によってバス電圧変更を行うことが可能。

c. 不正送信阻止手法を実装されたノード（被攻撃者）に対する攻撃手法の影響

・被攻撃者が送信するデータフレームを改変する。
・被攻撃者は攻撃者が不正メッセージを送信したことを検知することが不可能。
・被攻撃者による他ノードへの CAN でのエラー通知が不可能。
・不正送信阻止ノードのエラー状態遷移は起こらない。
・攻撃に求められる電圧改変精度は高い。

被攻撃者が攻撃されていることを検知することや、他ノードへ攻撃されていることを伝えることが出来ない攻撃手法であるが、攻撃の難易度が高い。これは、サンプリングポイントのずれを利用した電気的改ざんは、サンプリングポイント付近のみを改ざんする必要があり、電圧改変精度が高くなければならず、バスのビットレートが高い場合には攻撃の難易度が高くなることや、サンプリングポイントの位置やずれ幅などを攻撃前に調べる必要があるためである。

(ⅳ) 強いリセッシブ

a. 攻撃概要

不正送信阻止手法を回避する攻撃手法として論文 [33]にて提案されたものである。不正送信阻止手法では、エラーフレームを用いてなりすましメッセージの送信阻止を行うが、これはエラーフレームを構成する論理 0 の信号が論理 1 の信号と衝突した際に、論理 0 が優先されるという性質に由来する。そのため、物理的な細工により、論理 1 の優先度を引き上げることでエラーフレームに上書きされない強い不正フレームを作る攻撃手法である。

b. 想定する攻撃者の保持する能力

・CAN の仕様に準拠しない CAN コントローラを使用可能。
・攻撃者ノードはエラー状態へ遷移しない（エラーパッシブ、バスオフの状態へ遷移しない）。
・任意の手段によってバス電圧変更を行うことが可能。

c. 不正送信阻止手法を実装されたノード（被攻撃者）に対する攻撃手法の影響

・被攻撃者が送信しるエラーフレームを改変する。
・被攻撃者は攻撃者が不正メッセージを送信したことを検知することが可能
・被攻撃者による他ノードへの CAN でのエラー通知は被攻撃者のエラー状態に依存する
・不正送信阻止ノードのエラー状態遷移は発生する。具体的には受信エラーカウンタである REC 増加によって、エラーパッシブの状態に遷移する。

・攻撃に求められる電圧改変精度は低い

この攻撃では、不正送信阻止ノードの REC が増加することになるため、不正送信ノードをバスオフの状態にまで遷移させることは出来ない。このため、正規のメッセージは CAN バス上に存在することになる。攻撃者の意図する攻撃は完全には実現されない可能性がある。

(ｖ) エラーカウンタ値増加攻撃

a. 攻撃概要

不正送信阻止手法に対する新たな攻撃手法として本論文中にて提案されたものである。攻撃者は、被攻撃者である不正送信阻止ノードが送信するデータフレーム、およびエラーフレームに改変を行うことによって不正送信阻止ノードのエラー状態をエラーパッシブに遷移させることで、不正送信阻止が行えないようにすることを意図した攻撃である。

b. 想定する攻撃者の保持する能力

・CAN の仕様に準拠しない CAN コントローラを使用可能。
・攻撃者ノードはエラー状態へ遷移しない。（エラーパッシブ、バスオフの状態へ遷移しない）
・任意の手段によってバス電圧変更を行うことが可能。

c. 不正送信阻止手法を実装されたノード（被攻撃者）に対する攻撃手法の影響

・被攻撃者が送信するデータフレームおよびエラーフレームを改変する。
・被攻撃者は攻撃者が不正メッセージを送信したことを検知することが可能。
・被攻撃者による他ノードへの CAN でのエラー通知は被攻撃者のエラー状態に依存する。
・不正送信阻止ノードのエラー状態遷移は発生する。具体的には送信エラーカウンタである Transmit Error Counter （以下、TEC）の増加によって、エラーパッシブの状態、およびバスオフの状態にまで遷移する。
・攻撃に求められる電圧改変精度は低い。

この攻撃では、被攻撃者である不正送信阻止ノードの TEC が増加することになるため、不正送信阻止ノードをバスオフの状態にまで遷移させることが可能である。このため、正規のメッセージは CAN バス上に存在しなくなるため、攻撃者の意図する攻撃を完全に実施することが出来る。

エラーカウンタ値増加攻撃の手順について下記に示す。

d. エラーカウンタ値増加攻撃の攻撃手順

ア）攻撃者は、非攻撃者が送信するデータフレームのデータフィールドに 1bit の改変を行う。
イ）被攻撃者はビットエラーを検知し、TEC が増加するとともに、直後のビットからアク

ティブエラーフレームを送信する。

ウ）攻撃者は（ア）の改変以降もデータフレームの形を保つように ACK スロットまで改変する。この時、ACK スロットの改変を終えるまでに被攻撃者の TEC が 128 以上になるように改変する必要がある。

エ）攻撃者が改変を終えた後に被攻撃者はエラーフレームの再送とメッセージの再送を行う。この時、被攻撃者は TEC＞127 のため、送信するエラーフレームはパッシブエラーフレームとなる。

オ）（ア）から（エ）を繰り返し行うことで被攻撃者の不正送信阻止機構を働かせることなく、攻撃者はなりすまし攻撃を行うことが可能。

（ア）から（オ）までを同じバス上である第三者ノードから見ると、不正送信阻止ノードが使っている ID のデータフレームが短い間隔で 2 個送信されたように見え、エラーは検出できない。これは不正送信阻止ノードが最後に送信したパッシブエラーフレームが、1 個目のデータフレームの ACK デリミタからバスアイドルの 1 ビット目に重なってしまうからである。

② 論文名：CAN におけるエラーフレーム監視機構の提案

・著者：倉知亮*、高田広章*、上田浩史†、堀端啓史†
・所属：*名古屋大学大学院情報科学研究科、†株式会社オートネットワーク研究所／住友電気工業株式会社

上記発表論文では、CAN のエラーフレーム監視機構による異常検出手法について提案されている。また、提案手法でも防ぐことが困難なセキュリティ攻撃について分析されている。本提案方式は、CAN バス上に CAN メッセージを監視するノードを設置し、該当の監視ノード上で MAC エラーフレームを検出し、収集した情報をもとに攻撃等により異常が発生していると考える CAN-ID を正しく識別し、攻撃対象となっている CAN メッセージを排除する等の機能を有している。

この提案された方式でも防ぐことが困難なセキュリティ攻撃として下記 2 つの攻撃について考察されている。

・エラーフレームを故意に送信することにより、ある CAN メッセージの通信を途絶することができ、それにより特定の機能を縮退させる。
・攻撃者が物理的に不正なノードを設置することにより、監視ノードを監視対象バスから隔離することができ、監視ノードが観測するべきエラーフレームを不正に設置されたノードによって監視不可能にする。

③ 論文名：電気的データ改ざんに対する CAN のインテグリティ強化策

・著者：松本勉*、向達泰希*、土屋遊*、中山淑文*、吉岡克成*
・所属：*横浜国立大学大学院環境情報研究院

上記論文の内容については、SCIS の①題：CAN における再同期を利用した電気的デー

タ改ざん　b. メッセージの改ざん攻撃手法を参照のこと。

(7) Black Hat USA

本章では、Black Hat で発表された通信プロトコルの脆弱性および攻撃手法に関して記載する。

① Black Hat USA 2015

下記発表論文に、CAN 通信プロトコルの通信方法に対する攻撃手法が記載されている。

(ｉ) 論文名：Remote Exploitation of an Unaltered Passenger Vehicle

・著者：C. Valasek* and C. Miller†
・所属：*IO Active 社、†Twitter 社

クライスラー・ジープに対して、Wi-Fi または携帯電話網から車載テレマティクスシステム（U-Connect）を経由して、CAN 通信を行うルネサス製のマイコン（V850）のファームウェアを改ざんして不正な CAN メッセージを送信するなりすまし攻撃手法に関して記載されている。

攻撃者が送信する不正メッセージとして、通常に動作する際に流れるメッセージである通常メッセージと、ECU の故障等を診断する際に利用する故障診断用のメッセージの 2 種類が挙げられている。
通常メッセージの送信により、下記の不正操作が可能であることが挙げられる。
・ウィンカの点灯
・ドアロック/アンロック操作
・タコメータ表示の改ざん

診断メッセージの送信により、下記の不正操作が可能であることが挙げられる。なお、診断メッセージ送信時は、低速での走行時のみ有効である。
・エンジン停止
・ブレーキの無効化
・ステアリング操作（パークアシスト機能を利用）

但し、ステアリングの操作に関して、単純に攻撃者が不正メッセージを送信すると、パークアシストモジュールから送信される正規のメッセージと不正メッセージが衝突し、ステアリングの操作を担うパワーステアリング ECU は異常が起きたと判断する。そのため、パークアシスト機能は作動状態とならずに、不正メッセージを送信してもステアリングの不正操作を誘発することが難しい。
よって、ステアリングの不正操作を行う場合は、まず診断メッセージを送信し、パーク

アシストの機能を診断モードに移行し、パークアシストモジュールから正規メッセージを送信することを停止する。次に、パワーステアリング ECU を制御する不正メッセージを送信することにより、ステアリングの不正操作を行うことが可能となる。

(8) 脆弱性・攻撃評価の調査のまとめ

ここまでに記載してきた今回の調査対象の論文等では、脆弱性及び攻撃方法について、参考文献が参照／引用されている。そこで、調査対象の論文等において、脆弱性及び攻撃方法に関するどのような参考文献を参照／引用しているのかについて調査し表 3.2c.3-3 および表 3.2c.3-4 にまとめた。これらの表からわかるように、同一の参考文献が、複数の論文から参照／引用されている。この傾向を分析するために、参照関係を図 3.2c.3-16 にまとめた。図 3.2c.3-16 では、調査対象の論文を□、それらの論文から参照されている論文を○、参照元から参照先に→で表している。また、○の太さは参照されている件数が多いほど、太く描画してある。

表 3.2c.3-3　調査対象論文が引用する脆弱性及び攻撃方法に関する文献一覧（1）

会議		著者	論文タイトル	文献（タイトル、会議）
Escar Europe	2013	B. Glas and M. Lewis	[EE2013]Approaches to Economics Secure Automotive Sensor Communication in Constrained Environments	発表資料のため記載なし
	2014	R. Kurachi, Y. Matsubara, H. Takada, N. Adachi. Y. Miyashita and S. Horihata	[EE2014]CaCAN - Centralized Authentication System in CAN (Controller Area Network)	発表資料のため記載なし
	2015	R. Kurachi, H. Takada, T. Mizutani, H. Ueda and S. Horihata	[EE2015]SecGW: Secure Gateway for in-vehicle networks	[A] Security Threats to Automotive CAN Networks - Practical Examples and Selected Short-Term Countermeasures, SAFECOMP 2008.
				[B] Adventures in Automotive Networks and Control Units, technical white paper, 2014.
				[C] Yet Another Electrical Forgery Attack on CAN using Strong Recessive, IEICE Technical Report, Mar. 2015 (in Japanese).
				[D] Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, 2010.
Escar USA	2013	なし	なし	なし
	2014	なし	なし	なし
	2015	なし	なし	なし
Escar Asia	2014	なし	なし	なし
	2015	松島秀樹（パナソニック株式会社）	[EA2015]車載制御システムを保護するセキュリティ技術	[D] Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, 2010.
				[E] Comprehensive Experimental Analyses of Automotive Attack Surfaces、USENIX Security 2011
				[F] Remote Exploitation of an Unaltered Passenger Vehicle、DefCon 23 2015
VTC Spring	2013	なし	なし	なし
	2014	なし	なし	なし
	2015	なし	なし	なし
VTC Fall	2013	なし	なし	なし
	2014	なし	なし	なし
	2015	なし	なし	なし
SCIS	2013	なし	なし	なし
	2014	関口太樹、向達泰希、吉岡克成、松本勉（横浜国立大学）	[SCIS2014]不正 CAN データ送信を抑制するホワイトリスト・ハブ	[D] Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, 2010.
				[E] Comprehensive Experimental Analyses of Automotive Attack Surfaces、USENIX Security 2011
	2015	倉知亮、高田広章、上田浩史、堀端啓史（名古屋大学）	[SCIS2015-1]車載制御ネットワークにおける送信周期監視システムの提案	[D] Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, 2010.
				[G] CAN Security: Cost-Effective Intrusion Detection for Real-Time Control Systems、SAE Technical Paper 2014
		氏家良浩、岸川剛、芳賀智之、松島秀樹、田邉正人、北村嘉彦、安齋潤（パナソニック株式会社）	[SCIS2015-2]車載ネットワークにおける CAN フィルタの提案	[H] 自動車の情報セキュリティ　ECU・車載 LAN・車外ネットワークの脅威と対策、書籍 2013
				[D] Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, 2010.
				[I] Adventures in Automotive Networks and Control Units、DefCon 21 2013
		田中 卓(兵庫県立大学院)、大久保 隆夫(情報セキュリティ大学院大学)	[SCIS2015-3]車載システムにおける低電圧時のマルウェア挙動	[D] Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, 2010.
				[J] CAN における不正送信阻止防止方式実装と評価、ISEC2012-74 2012

表 3.2c.3-4　調査対象論文が引用する脆弱性及び攻撃方法に関する文献一覧（2）

SCIS	2015	氏家良浩、岸川剛、芳賀智之、松島秀樹、田邉正人、北村嘉彦、安齋潤（パナソニック株式会社）	[SCIS2015-4]車載ネットワークにおける監視・検証モード切換えの提案	[D] Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, 2010.
				[E] Comprehensive Experimental Analyses of Automotive Attack Surfaces、USENIX Security 2011
		氏家良浩、岸川剛、芳賀智之、松島秀樹、田邉正人、北村嘉彦、安齋潤（パナソニック株式会社）	[SCIS2015-5]車載ネットワークを保護するセキュリティ EC の提案:HW/SW 協調による更新可能な CAN の保護手法とその評価	[D] Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, 2010.
				[E] Comprehensive Experimental Analyses of Automotive Attack Surfaces、USENIX Security 2011
		松本勉、中山淑文、向達泰希、土屋遊、吉岡克成（横浜国立大学大学）	[SCIS2015-6]CAN における再同期を利用した電気的改ざん	[H] 自動車の情報セキュリティ　ECU・車載 LAN・車外ネットワークの脅威と対策、書籍 2013
				[CSS2014] 電気的データ改ざんに対する CAN のインテグリティ強化策、CSS 2014
		松本勉、中山淑文、向達泰希、土屋遊、吉岡克成（横浜国立大学大学)、森田信義、萱島信（株式会社日立製作所）	[SCIS2015-7]車載 ECU に対する CAN 経由のファジング手法	[D] Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, 2010.
				[E] Comprehensive Experimental Analyses of Automotive Attack Surfaces、USENIX Security 2011
				[H] 自動車の情報セキュリティ　ECU・車載 LAN・車外ネットワークの脅威と対策、書籍 2013
		矢嶋純、武仲正彦、長谷部高行（富士通研究所）	[SCIS2015-8]攻撃メッセージの無効化機能を備えたホワイトリスト CAN ハブ	[K] A Survey of Remote Automotive Attack Surfaces、BLACK HAT 2014
		久保田貴也、中野将志、倉知亮、本田晋也、汐崎充、藤野毅（立命館大学、*名古屋大学）	[SCIS2015-9]車載 CAN 通信暗号化デモシステムの構築とサイドチャネル攻撃評価	[D] Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, 2010.
				[L] Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study、USENIX Security Symposium 2010
		森田信義、伯田恵輔、大和田徹（日立製作所）	[SCIS2015-10]車載ネットワーク向けメッセージ認証方式の提案	[M] 自動車の情報セキュリティへの取組みガイド、ウェブページ（http://www.ipa.go.jp/files/000027273.pdf）
		氏家良浩、岸川剛、芳賀智之、松島秀樹、田邉正人、北村嘉彦、安齋潤（パナソニック株式会社）	[SCIS2015-11]車載ネットワークを保護するセキュリティ ECU の提案: 導入インパクトを抑えた CAN 保護手法のコンセプトとその評価	[D] Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, 2010.
				[E] Comprehensive Experimental Analyses of Automotive Attack Surfaces、USENIX Security 2011
CSS	2013	なし	なし	なし
	2014	松本勉、向達泰希、土屋遊、中山淑文、吉岡克成	[CSS2014]電気的データ改ざんに対する CAN のインテグリティ強化策	[D] Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, 2010.
				[E] Comprehensive Experimental Analyses of Automotive Attack Surfaces、USENIX Security 2011
				[N]Security Threats to Automotive CAN Networks-Practical Examples and Selected Short-Term Countermeasures、27th international conference on Computer Safety, Reliability, and Security, SAFECOMP 08,2009
	2015	倉知亮、高田広章、上田浩史、堀端啓史（名古屋大学）	[CSS2015-1]CAN におけるエラーフレーム監視機構の提案	[D] Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, 2010.
				[E] Comprehensive Experimental Analyses of Automotive Attack Surfaces、USENIX Security 2011
				[I]Adventures in Automotive Networks and Control Units、DEFCON 21、2013
		小林優希、中山淑文、松本勉、	[CSS2015-2]CAN における不正送信阻止が可能となる条件	[D] Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, 2010.
				[E] Comprehensive Experimental Analyses of Automotive Attack Surfaces、USENIX Security 2011
Black Hat USA	2015	Chris Valasek (IOActive), Charlie Miller (Twitter)	[BH2015]Remote Exploitation of an Unaltered Passenger Vehicle	[D] Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, 2010.
				[E] Comprehensive Experimental Analyses of Automotive Attack Surfaces、USENIX Security 2011

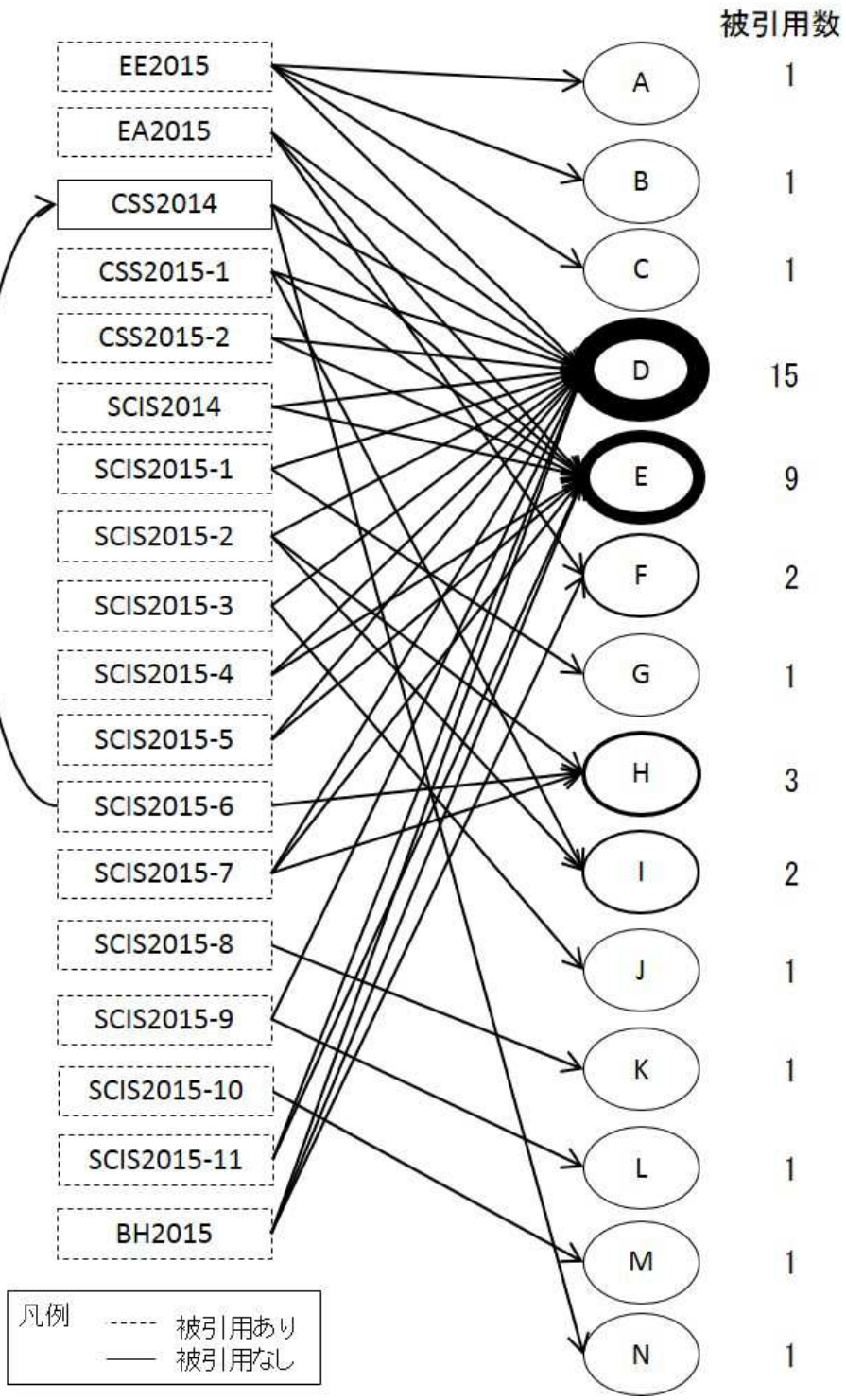


図 3.2c.3-16　調査対象と引用文献の参照関係

これらの結果から、複数の論文から参照されている参考文献は、以下の 5 論文（引用数順で記載）であることがわかった。

・[D] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage: Experimental Security Analysis of a Modern Automobile. In Proceedings of the 2010 IEEE Symposium on Security and Privacy (SP '10). IEEE Computer Society, Washington, DC, USA, 447-462. DOI=http://dx.doi.org/10.1109/SP.2010.34.

・[E] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno: Comprehensive experimental analyses of automotive attack surfaces. In Proceedings of the 20th USENIX conference on Security (SEC'11). USENIX Association, Berkeley, CA, USA, 6-6.

・[H] 中野学, 松本勉, Camille Vuillaume, and 小谷誠剛: 自動車の情報セキュリティ -ECU・車載 LAN・車外ネットワークの脅威と対策 -,日経 Automotive Technology 編, 日経 BP 社, ISBN 978-4-8222-7515-0, 2013. 12. 27.

・[F] C. Miller, Chris Valasek: Remote Exploitation of an Unaltered Passenger Vehicle, DEFCON 23, 2015. Available at: http://illmatics.com/Remote%20Car%20Hacking.pdf

・[I] C. Miller, Chris Valasek: Adventures in Automotive Networks and Control Units, DEFCON 21, 2013. Available Online: http://illmatics.com/car_hacking.pdf

上記論文の中で最も引用が多かった 2 件の論文（D と E）の概要を以下に述べる。

・文献[D]に関して：自動車内の OBD-II ポートに PC を接続し、PC から不正な CAN メッセージを送信することにより、なりすまし攻撃法や DoS 攻撃により自動車の不正操作が可能であることを実証した。実際には、CAN バス上のメッセージの取得・解析の実施や ECU のリバースエンジニアリング・内容を実施して、CAN メッセージや ECU の各機能を明らかにした上で、上記の実証を実施している。

・文献[E]に関して：自動車への侵入の口（OBD-II ポート、メディアプレイヤー、Bluetooth、携帯電話接続）を挙げ、各々の脆弱性の指摘や攻撃コストに関する評価を行い、実験的に攻撃の有効性を確かめた。攻撃の例として、遠隔から携帯電話の通信モジュールが搭載された車載機にアクセスし、CAN バス上に不正に CAN メッセージを送信し、自動車の不正操作が可能であることを示している。

3.2c.4　車内通信プロトコルの仕様に基づく評価方法の検討　調査結果のまとめ

以上調査のまとめとして、各々の車内ネットワークの通信プロトコルの特徴に基づき、IT 分野における攻撃方法の事例を応用した攻撃が自動車分野でも可能であるかを検討するための考察を行った。

IT 分野（特にネットワークセキュリティ分野）では、OSI 参照モデル：データリンク層の通信プロトコル（イーサネット、ATM 等）における脆弱性を利用した有名な攻撃の例として下記が挙げられる。

① 盗聴

通信上のパケットが暗号化されていないため、容易に盗聴を行うことが可能である。

② なりすまし攻撃

イーサネットアドレス解決（ARP）プロトコルには、通信上のパケットの真正性を保証する仕組みがないため、ARP スプーフィングといったなりすまし攻撃（中間者攻撃）が可能である。

③ DoS 攻撃

ブロードキャストの仕組みを持ち、通信バスの帯域が有限かつネットワークが終端を持たずに循環するような構造の場合、攻撃者がブロードキャストを用いてバス上に大量のパケットを送信することにより、通信を行うことが不可能になる攻撃（ブロードキャストストーム）が可能である。また、大量のパケットを送信して通信上のスイッチ等の機器の処理機能を麻痺させることにより装置を不能にする攻撃も可能である。

通常は、データリンク層より上位層で上記の攻撃に対する対策が行われている。

ここで、ネットワークセキュリティ分野の攻撃方法が CAN や LIN といった車内ネットワークの通信プロトコルへ応用が可能であるかに関して調査結果を基に述べる。

・盗聴

イーサネットと同様、CAN や LIN バス等に流れるメッセージは暗号化されていないため、攻撃者は自動車に搭載された様々なインタフェース（情報系端末接続ポート、診断用ポート等）を介して、メッセージを盗聴・取得することが可能である。このようにして取得したメッセージを解析することにより、以下に示すなりすまし攻撃を実施することが可能となる。

・なりすまし攻撃（リプレイ攻撃を含む）

イーサネットと同様、CAN や LIN バス等の通信上のメッセージ送信者の認証は行われていないため、バスに接続された正規メッセージを送信するノードになりすまして、攻撃者が不正な挙動を誘発する不正メッセージを送信し、受信ノードに正しいものとして誤認識させることが可能である。

・DoS 攻撃

イーサネットと同様、攻撃者がバス上に不正メッセージを大量に送信し、帯域を占有するなどして、ノードが正規メッセージを受信できなくなる攻撃や、意図的に通信エラーを発生させ、攻撃対象のノードをバスから論理的に切り離すといった攻撃が可能である。一方で、自動車分野において、イーサネットで行われているような、大量のメッセージを送信してノードの処理能力を超えた負荷をかけることによりノードを不能にする攻撃は、本調査では見つからなかった

更に、自動車分野では他の攻撃方法として、スリープコマンド等のノードの動作を止めることができる命令を攻撃者が不正に利用することにより、バス上に接続されたノー

ドの動作を妨害する攻撃が可能である。

上記の通り、イーサネットにおける攻撃方法は車内通信プロトコルにおいて適用することは可能であり、これらの攻撃を各通信プロトコルにおいて適用することにより自動車の正規動作の妨害や、不正操作が可能であると考えられる。更に、車内通信において新たな攻撃の方法として、正規の送信ノードが送信したメッセージに対して、攻撃者が電気信号を与えることにより、メッセージの値を改ざんする攻撃（メッセージの電気的改ざん）が可能であることが近年示されている。

ここで、既存研究の傾向を述べると、2013 年から 2015 年において、CAN や LIN におけるなりすまし攻撃の発表件数は 2013 年、2014 年共に 2 件であったのに対して、2015 年には 15 件と増加している。また、DoS 攻撃の発表件数は、2013 年は 0 件、2014 年は 1 件であったのに対し、2015 年は 7 件と増加している。メッセージの電気的改ざんは 2014 年、2015 年に 1 件ずつ発表があった。

図 3.2c.4-1 に 2013 年から 2015 年における、なりすまし攻撃、DoS 攻撃、電気的改ざんの発表論文件数を示す。本結果から、なりすまし攻撃や DoS 攻撃といった、ネットワークセキュリティの分野でも有名な攻撃方法の研究発表が 2015 年に急増していることがわかる。また、攻撃方法もバスに大量にメッセージを送信するといった単純なりすまし攻撃から、対策が実装されていても可能な攻撃方法といった複雑な攻撃へと進化している。攻撃対象は CAN が最も多いが、近年、SENT といった通信プロトコルも攻撃の対象となってきている。

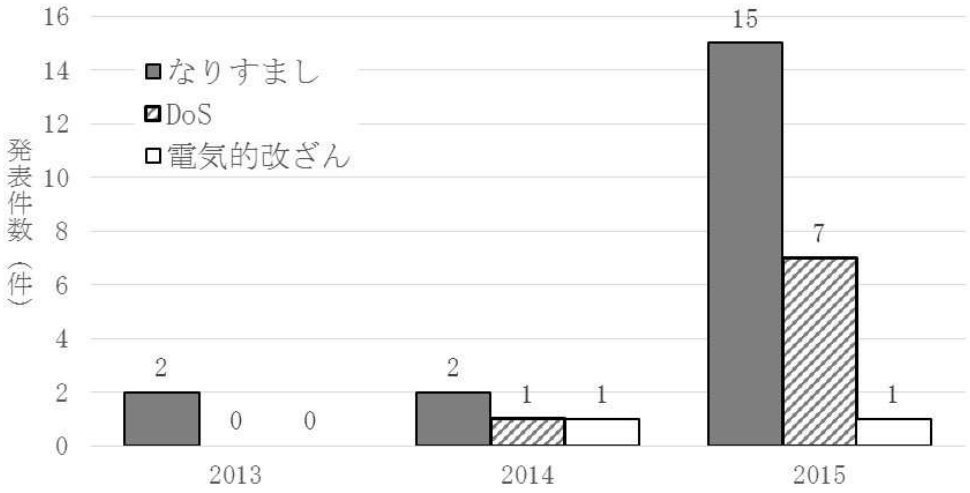


図 3.2c.4-1　各攻撃の発表件数

参考文献

[1] ISO, “ISO 11898-1:2015 Road vehicles -- Controller area network (CAN) -- Part 1: Data link layer and physical signalling,” 2015.

[2] ISO, “ISO 11898-2:2003 Road vehicles -- Controller area network (CAN) -- Part 2: High-speed medium access unit,” 2003.

[3] ISO, “ISO 11898-3:2006 Road vehicles -- Controller area network (CAN) -- Part 3: Low-speed, fault-tolerant, medium-dependent interface,” 2006.

[4] ISO, “ISO 11898-4:2004 Road vehicles -- Controller area network (CAN) -- Part 4: Time-triggered communication,” 2004.

[5] ISO, “ISO 11898-5:2007 Road vehicles -- Controller area network (CAN) -- Part 5: High-speed medium access unit with low-power mode,” 2007.

[6] ISO, “ISO 11898-6:2013 Road vehicles -- Controller area network (CAN) -- Part 6: High-speed medium access unit with selective wake-up functionality,” 2013.

[7] Robert Bosch GmbH, “CAN with Flexible Data-Rate Specification Version 1.0,” 2012.

[8] “SAE International (R) SENT-Single Edge Nibble Transmission for Automotive Applications J2716,” 2010-01.

[9] “Peripheral Sensor Interface for Automotive Applications V2.1,” The PSI5 organization, 2012.

[10] “DRAFT INTERNATIONAL STANDARD ISO/DIS 17987-3.2 Road vehicles - Local Interconnect Network (LIN) Part 3: Protocol specification,” 2015-12-05.

[11] “LIN Specification Package Revision 2.2A,” 2010-12-31.

[12] 株式会社ベクター, “はじめての LIN”.

[13] 公益社団法人自動車技術会, “JASO　D 015-3 自動車－クロックエクステンションペリフェラルインターフェース（CXPI）－第 3 部：プロトコル仕様,” 2015.

[14] SAE International, “J3076 Clock Extension Peripheral Interface (CXPI),” 2015.

[15] Microchip Technology Inc., “SPI インタフェーススタンドアロン CAN コントローラ MCP2515,” 2005.

[16] Renesas Electronics, “アプリケーションノート RX ファミリ CAN の使い方 R01AN1448JJ0100 Rev.1.00,” 2013.

[17] Philips Semiconductors, “APPLICATION NOTE SJA1000 Stand-alone CAN controller AN97076,” 1997.

[18] Cypress Semiconductor Corp., “FM4 32 ビット・マイクロコントローラ FM4 ファミリ 通信マクロ編 PERIPHERAL MANUAL,” 2015.

[19] Freescale Semiconductor, “Application Note Using the MPC5777M MCAN Module to Exchange CAN FD Messages,” 2014.

[20] Microchip, “SENT (Single-Edge Nibble Transmission) モジュール　dsPIC33/PIC24 ファミリ　リファレンスマニュアル”.

[21] “KMA215 Programmable angle sensor with SAE J2716 SENT Product data sheet Rev. 1-24 February 2014,” NXP, 2014.

[22] ST マイクロ, “PSI5 Transceiver IC　Datasheet-production data”.

[23] ルネサステクノロジー, “H8/300H Tiny シリーズ　H8/3664F/3694F/36014F LIN (Local Interconect Network) マスタ編”.

[24] 富士通, “16-BIT Microcontroller F2MC-16FX Family MB96600 sereies　LIN の使用方法”.

[25] ローム株式会社, “車載向け CXPI トランシーバ　BD41000FJ-C,” 2015.

[26] ローム株式会社, “業界初、次世代車載通信「CXPI」を実現する汎用トランシーバ IC を開発,” 24 9 2015. [オンライン]. Available: http://www.rohm.co.jp/web/japan/news-detail?news-title=2015-09-24_news_cxpi&defaultGroupId=false.

[27] サイプレス, “Traveo TM ファミリ車載 MCU シリーズの新製品も発表,” 2016.

[28] サイプレス, “サイプレスが車載マイコンに 40nm プロセスを初採用、低価格メータークラスタ向け,” 13 1 2016. [オンライン]. Available: http://monoist.atmarkit.co.jp/mn/articles/1601/13/news046.html.

[29] 畑正人、田邉正人、吉岡克成、大石和臣、松本勉, “不正送信阻止 : CAN ではそれが可能である,” *CSS*, pp. 624-629, 2011.

[30] 畑正人、田邉正人、吉岡克成、松本勉, “CAN における不正送信阻止方式の実装と評価,” *ISEC2012-72*, 第 巻 342, 第 112, pp. 15-22, 2012.

[31] 松本勉、向達泰希、土屋遊、中山淑文、吉岡克成, “電気的データ改ざんに対する CAN のインテグリティ強化策,” *CSS*, pp. 635-642, 2014.

[32] 松本勉、中山淑文、向達泰希、土屋遊、吉岡克成, “CAN における再同期を利用した電気的データ改ざん,” *SCIS2015*, 2015.

[33] 菅原健、佐伯稔、三澤学, “強いリセッシブを用いた CAN の電気的データ改ざん,” *ICSS2014-74*, 第 巻 74, pp. 67-72, 2014.

付録 A　用語集

ACK: Acknowledgement
ACKD: ACK Delimiter
ARP: Address Resolution Protocol
ATM: Asynchronous Transfer Mode
BER: Bit Error Rate
BRS: Bit Rate Switch
Bosch: Robert Bosch GmbH
CAN: Controller Area Network
CRC: Cycle Redundancy Check
CRCD: CRC Delimiter
CT: Counter
CSMA/CD: Carrier Sense Multiple Access with Collision Detection
CXPI: Clock Extension Peripheral Interface
DoS: Denial of Service
DLC: Data Length Code
ECU: Engine Control Unit
EDL: Extended Data Length
EOF: End Of Frame
Error D: Error Delimiter
escar: Embedded Security in Car
ESI: Error State Indicator
FSM: Finite State Machine
FD: Flexible Data Rate
ID: Identifier
IDE: ID Extension
ID Ex: Extended ID
INT: Interframe space
LIN: Local Interconnect Network
LLC: Logical Link Control
LSI: Large Scale Integration
MAC: Medium Access Control
MCU: Micro Controller Unit
NM: Network Management
OBD: On-Board Diagnostics
Overload D: Overload Delimiter
PBS: Phase Buffer Segment
PCS: Physical Coding Sub-layer
PID: Protected Identifier

PMA: Physical Media Attachment
PMD: Physical Media Attachment
PTS: Propagation Time Segment
PTYPE: Protected TYPE
REC: Receive Error Counter
RTR: Remote Transmission Request
SENT: Single Edge Nibble Transmission
SJW: reSynchronization Jump Width
SOF: Start Of Frame
SP: Sample Point
SRR: Substitute RTR
SS: Synchronization Segment
TEC: Transmit Error Counter
TSEG: Time Segment
Tq: Time Quantum

3.2d　実機を用いた評価の実施

自動車を構成する実機に対して、サイバー攻撃を行うための技術を開発する。攻撃対象として現在、標準的なコンポーネント(ECU)、複数のコンポーネントから構成されるシステム、システムの組み合わせにより構成される車両本体、および車両本体とそれを取り巻くモビリティ社会を想定している。これらはインタフェースを含めた機能および計算機資源が異なるため、画一的な攻撃手法を確立することはできない。

本事業では一般的な組み込み機器に対する攻撃などを参照し、コンポーネントからシステムまでと範囲を広げながら、様々な攻撃を試みていくこととしているが、平成 27 年度は、コンポーネントレベルへの攻撃を試みた。またその成果は評価技術開発へ展開し、評価基準作成および評価環境作成へ活用することを想定している。

3.2d.1　コンポーネントの仕様と想定される攻撃の調査

テーマ②a において開発予定の標準コンポーネントは、リプログラミングとデバッグの機能、その機能を制御するマイコンに搭載されたセキュリティ IP、マイコン上のソフトウェアとして AUTOSAR にて検討している BSW のセキュリティモジュール、さらに、自身以外のコンポーネントと連携するなどを目的とした車載 LAN のインタフェースをそれぞれ搭載している。まず、それら搭載機能の仕様や特徴から、定性的にどのような攻撃が想定可能かを把握する。

実際の現場においてリプログラミングおよびデバッグは、ハードウェアとしての標準コンポーネントが具備する JTAG などのデバッグ用インタフェース、および車載 LAN を利用して実施される。このうちデバッグ用インタフェースは開発時のみならず、製品として出荷した後に問題が発覚した際に、以降の新規開発時へのフィードバックを目的とした情報収集のためにそのまま残されるケースがある。他方車載 LAN は車両として組み立てた後に、主にリプログラミングを目的に利用される。これにより単一のインタフェースから任意の ECU へのアクセスが可能となり、特に CAN を利用する方法は CAN リプロと呼ばれている。車両のライフサイクルにおいて、双方のインタフェースは有効であり続けるため、攻撃のインタフェースとして検討することは現実的である。

JTAG については以降で述べる標準コンポーネントとして利用する評価ボード、および、評価ボードと接続するデバッガの機能をそのまま利用し、車載 LAN については ISO14229、および、ISO15765 にて定義されたプロトコルを利用することになる。例えば[1]では JTAG を用いた自動車の ECU への攻撃について指摘されている。またこれまでにも組込みシステムに対して、以下の様な攻撃事例が報告されている。

- JTAG からメモリの内容を直接読み書きできるデバイスがあり、セキュリティ対策が施されていない、あるいは迂回できることがあり、ファームウェアの改ざんが可能となるといった攻撃
- JTAG を経由してメモリ上のデータを読み出すことで、暗号ハードウェアの秘密鍵の抽出に成功

これらの攻撃は攻撃対象車両に対する物理的接触を伴う直接侵入型の攻撃であり、攻撃者にとってコストがかかる一方、多数のハードウェアチップで同じ鍵が用いられているような場合には、そのコストに見合うだけの効果がある可能性があり、評価の必要がある。また、今回の調査結果も踏まえ、攻撃の具体的方法を検討し、以下で説明する攻撃を実施した。

3.2d.2　コンポーネントに対する攻撃側のプロファイル調査

攻撃側のプロファイル調査は、主に本テーマ作業従事者の属性をリストアップすることにより行う。リストアップ項目例を列挙する。

・計算機科学教育を受けた年数や学位、およびその時期と年齢
・IT 産業において作業に従事した年数
・ソフトウェア開発経験がある場合、1 日にコーディングできるライン数
・上記で述べた攻撃調査に要した時間
・下記で述べる攻撃実施に要する時間

本事業においては、攻撃を実施する役割を担う被験者として、2 つのグループにおいて、それぞれ 3 チーム、2 名をアサインした。それぞれにおける被験者のプロファイルを以下に記載する。

＜グループ A＞

・チーム B　情報工学を専門として教育を受けている学部 4 年生 2 名からなるチーム
・チーム M　情報・物理セキュリティを専門として修士論文研究を実施中の大学院生 3 名のチーム
・チーム D　情報・物理セキュリティを専門として博士論文研究を実施中の大学院生 1 名および博士号を有するポスドク研究者 1 名からなるチーム

＜グループ B＞

・被験者 A: 20 代、学部卒相当のコンピュータサイエンスに関するリテラシあり
・被験者 B: 20 代、機械工学系の大学卒業後、自動車業界に 5 年間従事

3.2d.3　コンポーネントを対象とした攻撃の実施

攻撃作業は、作業コンソールとしての PC と標準コンポーネントを模擬した評価ボードを利用した UDS に対して行う。UDS を利用したディーラリプロでは CAN を通信メディアとして利用している。現在想定している機器は以下の通りである（図 3.2d.3-1）。

・正規ツール: コンソールとして Windows PC を利用し、CAN アダプタを具備する
・RH850 評価ボード: UDS をサポートしたソフトウェアをインストール
・盗聴およびリプレイ攻撃ツール: コンソールとして Windows PC を利用し、CAN をクリッピングして接続

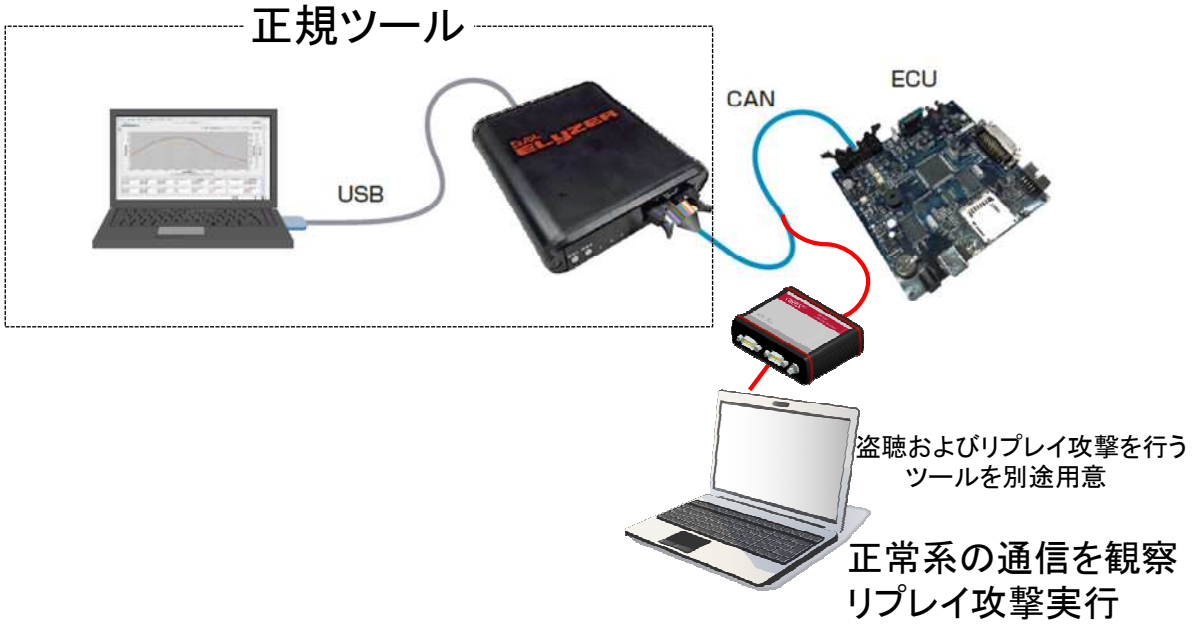


図 3.2d.3-1　攻撃環境

これらを利用して、攻撃調査にて定性的に得た結果に対する攻撃を実施する。攻撃実施時において得られる成果物として、以下の項目を想定している。

・各攻撃実施における具体的な手順
・各攻撃実施における所要時間

グループ A に対して与えられた条件としては、攻撃者端末は正規のリプログラミングツールと同じ CAN バス上に接続され CAN メッセージの観測・再送を行うことができる。ただし、今回は観測・再送を ELYZER ソフトからも行ってよいとした。図 3.2d.3-2 に攻撃環境の全体図を示す。

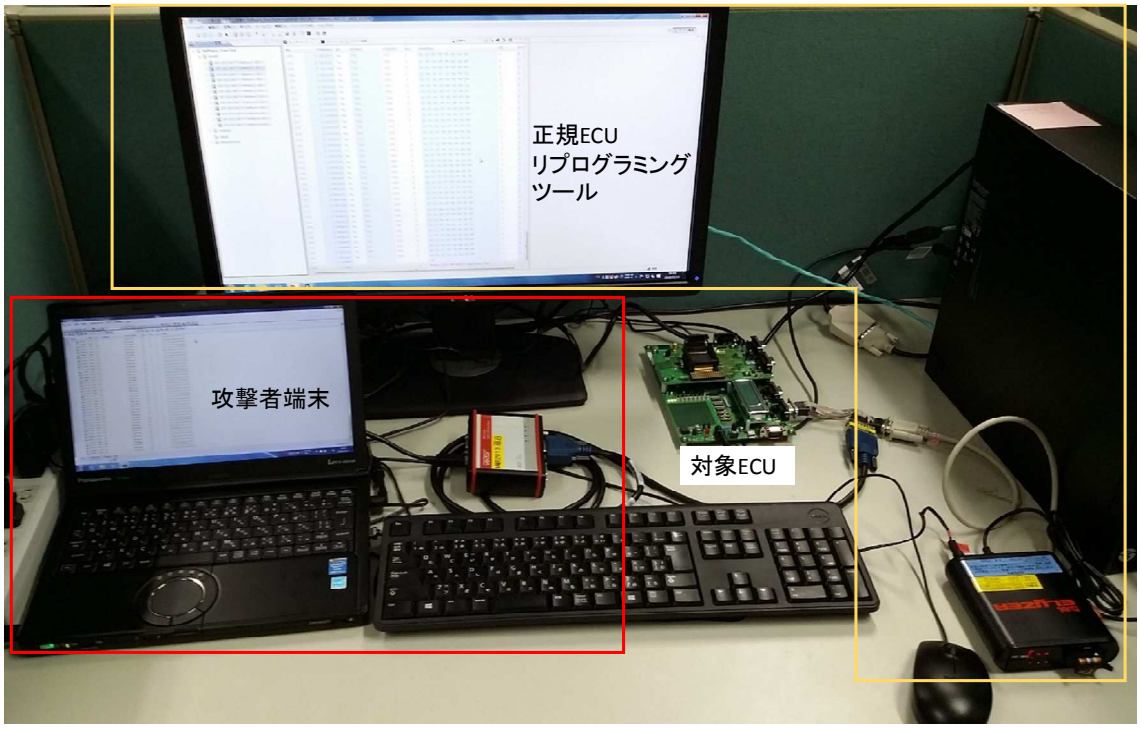


図 3.2d.3-2　攻撃環境の全体図

攻撃者は ELYZER ソフト上に用意された 1 つの動作モデル（水準 1～4 とする）に対して実行のみを行うことが可能である。ただし、水準の中身（エントロピーや乱数初期化）とは対応付けられていない。

実行すると ELYZER ハードウェアから CAN メッセージが送受信され ECU への認証とリプログラミングが行われる。ELYZER ソフトは CAN バスの観測を行いメッセージのログをとることができる。

ELYZER ソフトの UI を図 3.2d.3-3 に示す。左のタブ内の model と記述されているところの Pattern 1～4 が水準 1～4 に対応している。ロードして実行を行うことで各水準に対応した動作がなされる。右側のタブにあるように CAN バスのメッセージが表示されログがとられている。

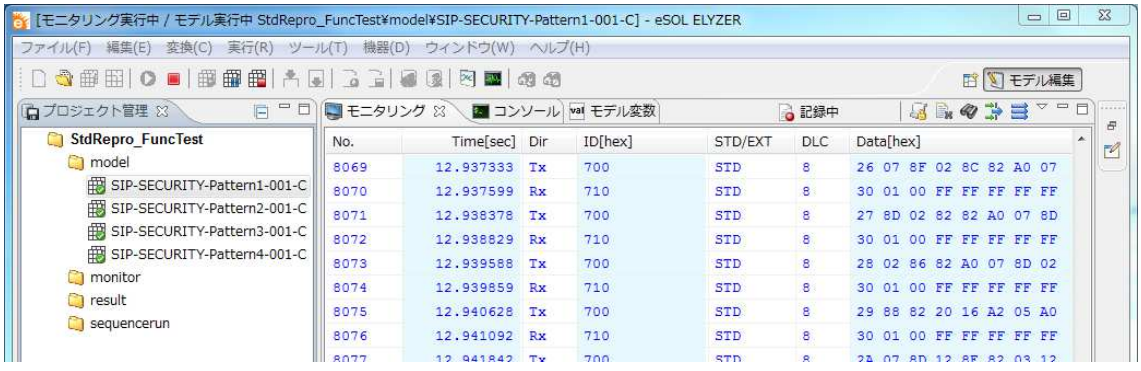


図 3.2d.3-3　ELYZER の UI

(1) 攻撃者に公開とした情報

以下の 4 種類の実装水準（順不同）があることが知らされている。

・乱数エントロピー小、乱数初期化あり
・乱数エントロピー小、乱数初期化なし
・乱数エントロピー大、乱数初期化あり
・乱数エントロピー大、乱数初期化なし

ここで乱数エントロピーは乱数のとりうる空間のサイズである。乱数初期化なしは乱数生成器のシードとして固定値が与えられ、初期化ありは乱数生成器のシードを ECU 上の何らかの乱数で初期化したものである。

(2) 攻撃実験結果

攻撃は、ツールに「なりすまし」、ECU を騙すことを目標とした。「なりすまし」とは、ECU をアンロック状態（リプログラム可能状態）にすることをいう。各対象に対して各チームが実施した攻撃実験の結果を表 3.2d.3-1 にまとめる。

表 3.2d.3-1　ECU リプログラミング攻撃実験

	水準 1	水準 2	水準 3	水準 4	付録
チーム B	なりすまし断念	なりすまし成功	なりすまし成功	なりすまし成功	A1
チーム M	なりすまし成功（1 日）	なりすまし成功	なりすまし成功	なりすまし成功	A2
チーム D	なりすまし方法考案	なりすまし成功	なりすまし成功	なりすまし成功	A3

ここで特筆すべき点は、水準 1（今回の評価対象の中では最高難度）の対象に対してもチーム M がなりすましに成功したことである。ECU－ツール間の通信の観測に加え、ECU／ツールプログラム実装者の立場で考察して、実装上の脆弱性を発見しつつ試行錯誤を行うという方法が有効に作用したと思われる。

グループ B の 2 名の被験者に対しては、攻撃調査としてある程度の情報を与えた。与えた情報は以下のシナリオの手順により知見を得たという前提を実現するに十分な量である。

・攻撃者は自身が保有する自動車を対象として、ディーラで行われる CAN リプロをモニタし、正規ツールと対象 ECU 間のメッセージシーケンスを得た。
・UDS（Unified Diagnostic Services）と呼ばれる国際規格 ISO14229 にて定義されるセキュリティアクセス（ツールとコンポーネント間の認証など）の外部仕様は、インターネットなどへの流出情報を活用した。

3.2d.4　コンポーネントに対する攻撃結果の考察と展開

ここまでの調査結果、攻撃実施結果およびそれらに対する考察を行う。図 3.2d.4-1 に UDS に関する調査から得られたメッセージフローを示す。UDS として定義されているセキュリティ機能は、ECU・ツール間の認証フェーズと、実際にリプログラミングを行うフェーズに分割される。前者は互いに正しい機器同士であるかの確認、後者はイメージの完全性確認などを目的としている。今回は認証フェーズに関するセキュリティ機能への攻撃を行うこととする。また図 3.2d.4-2 に UDS で定義されているリプログラミングに関する仕様を示す。図 3.2d.4-2 において、「xx」は認証に関わるデータを表す。

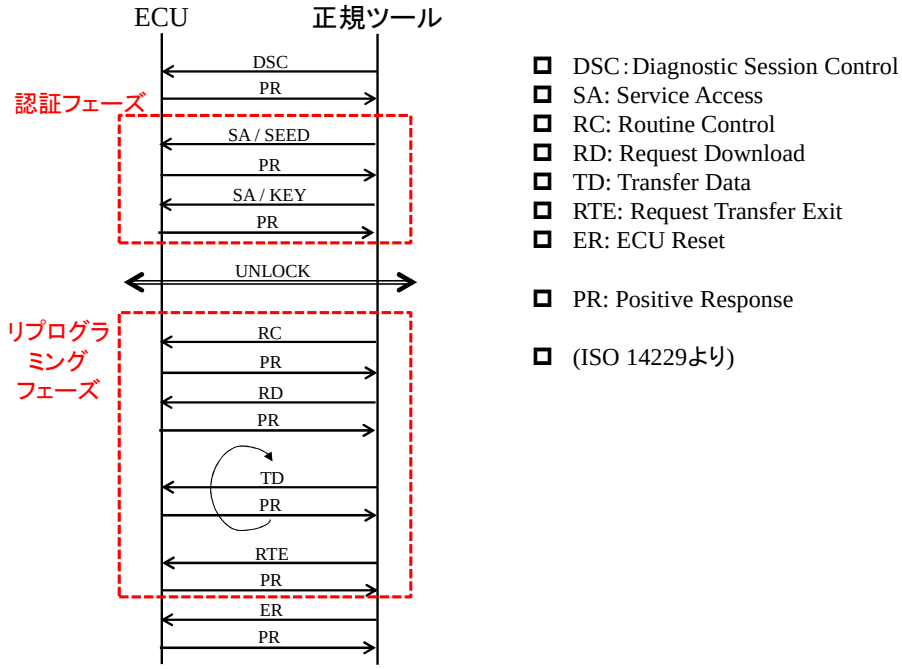


図 3.2d.4-1　UDS における ECU とツール間のメッセージフロー

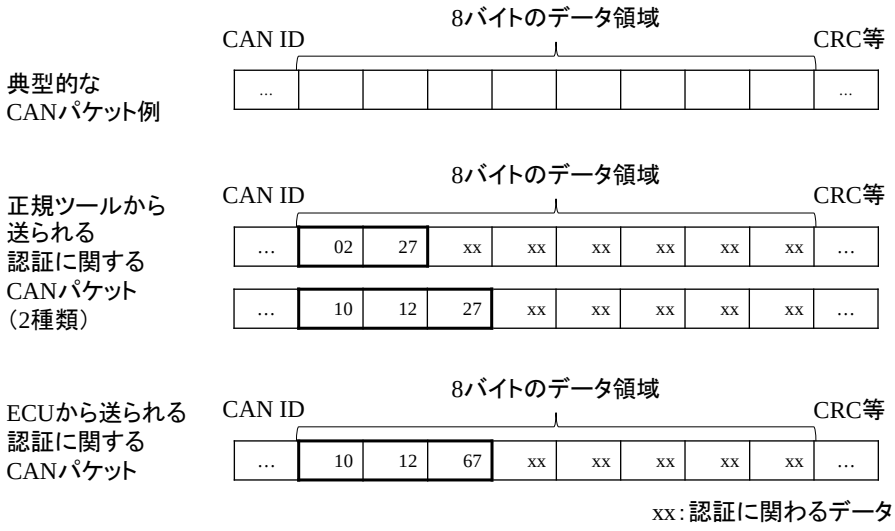


図 3.2d.4-2　UDS で定義されているリプログラミングに関する仕様

UDS の認証フェーズにおいて、始めに正規ツールから送信される乱数の生成方法は、再送攻撃を防ぐためにも重要な決定事項である。乱数の生成ビットの大きさは、セキュリティレベルと応答時間とのトレードオフである。初期化の有無も同様にセキュリティレベルとシステム構造の複雑さのトレードオフとなる。今回は、認証フェーズにおけるセキュリティレベルを以下のように設定した。

・乱数のエントロピー大 / 初期化あり
・乱数のエントロピー大 / 初期化なし
・乱数のエントロピー小 / 初期化あり
・乱数のエントロピー小 / 初期化なし

今回の攻撃作業時において、被験者に対しては 4 つの各モデルと上記セキュリティレベルとのマッチングは明らかにしていない。被験者には、攻撃作業を通じて、そのマッチングを明らかにすることが求められた。

ここでは、グループ B の被験者 2 名が行った実験をベースとして、考察を進めていく。

4 つのモデルに対し、被験者両名が行った実際の作業内容を図 3.2d.4-3 に示す。この中で、両名が分担した作業は攻撃ツールを利用するための環境整備時のみであり、その他の作業は共同で行っている。最初の 2 時間で、上記セキュリティレベルとモデルとのマッチングが明らかとなった。さらに正規ツールと ECU 間のインタラクションを盗聴し解析することにより、被験者両名は有効な攻撃手段を導出し、具体的な攻撃の実施段階に移行している。

グループ A、B の両方の結果を総合すると、乱数のエントロピーが大きく、初期化を行っている場合では、攻撃の難易度が高く、1 チームしか攻撃に成功していない。一方、それ以外の乱数生成方式では、全てのチームが、認証フェーズに対する攻撃、具体的には正規ツールへの成りすましに成功している。

一般に「セキュリティに絶対はあり得ない」と言われているように、全ての攻撃を防ぐことは困難である。よって、実際の製品では開発コストに見合ったセキュリティ技術を導入することとなる。この尺度は非常に曖昧であり、セキュリティ機能を含むシステム設計者により決定されることが想定される。この尺度の決定には ISO15408 における Protection Profile 生成時と同様に、想定脅威とその脅威に対する分析を行い、実際に適用可能なセキュリティ技術と先述した開発コストを照らし合わせるやり方が考えられる。

そのため、上述した脅威の想定作業、脅威分析作業および尺度の決定の怠りは、致命的な脆弱性となる。今回の認証フェーズにおけるセキュリティレベルでは、上述した通り乱数のエントロピーが大きく、また初期化がある場合には強固な設定となっていた。しかしながら 1 工程に過ぎない初期化を省いただけで、認証フェーズは数時間で突破可能となった。この結果は、セキュリティ機能実現時において、単純な作業であっても確実に遂行することが重要である事を実証することとなった。

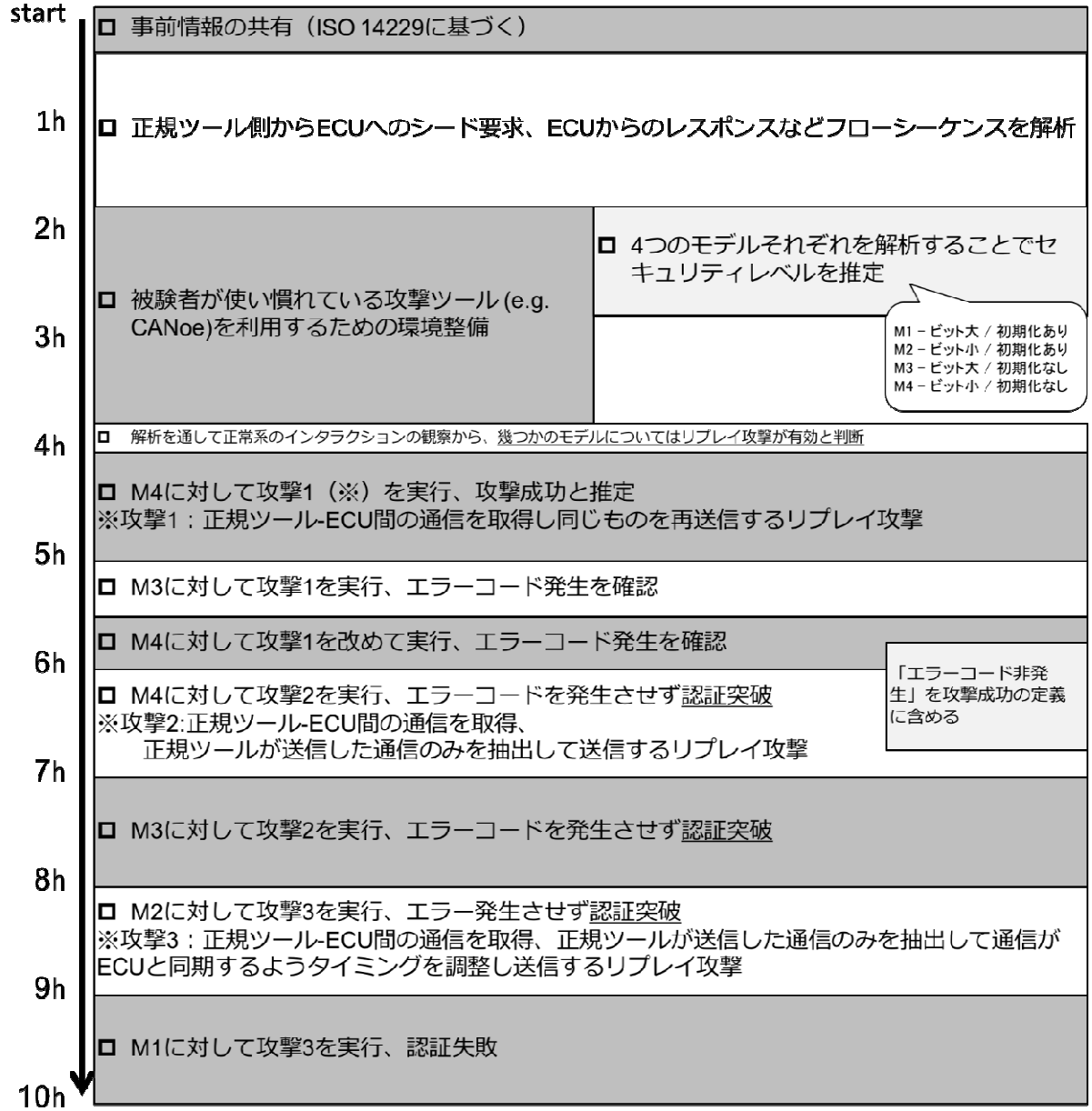


図 3.2d.4-3　攻撃者側の作業内容

3.2d.5　システムを対象とした攻撃方法の調査

車内システムに対する調査については、標準コンポーネントに対する攻撃調査と同様の手順で実施する。具体的には複数のコンポーネントが接続される車内ネットワークにおける連携機能、および連携制御用アプリケーションを対象に、定性的にどのような攻撃が想定可能かを把握し、以下の様な整理を行った。

・CAN バスに対して不正なメッセージを送信する攻撃の例は多く存在する。2010 年の Koscher らによる報告[2]では、OBD-II ポートを経由して、対象車両の CAN メッセージの解析を行った上で、正規のメッセージになりすました CAN メッセージを送ることで自

動車を不正に操作したことが報告されている。その後 2013 年には BlackHat USA において、車両や送信したメッセージの内容まで公表され大きな話題となった。また 2015 年の BlackHat USA においては、特定の車両において外部から侵入し、ファームウェアを改ざんすることで遠隔で操作が可能であることが発表された。

・日本でも自動車のセキュリティについて活発に研究が行われており、2016 年の 1 月に開催された電子情報通信学会主催の情報セキュリティに関する研究会 SCIS2016 でも、不正な CAN メッセージの送信に対する対策やシステムを対象とした新たな攻撃方法や対策について多くの発表があった。

・2015 年、Usenix Security と共に行われたワークショップ、WOOT では、車外から遠隔で運転を診断し、保険料を割り引くなどのサービスを行うための OBD-II に接続する Metromile 社のドングルの脆弱性を突くことで遠隔で自動車を操作するための不正な CAN メッセージを送信する攻撃が報告された。名古屋大学の倉地らは外部ネットワークと接続する ECU のプログラムが改変され、他の ECU に攻撃を行う「踏み台 ECU」となった場合の対策として、3 つの保護機能を提案している[3]。1 つ目には、踏み台 ECU における CAN メッセージを送受信するためのレジスタ群であるメールボックスについて、本来送信のために使用するメールボックス以外の使用を禁止すること、2 つ目には踏み台 ECU が本来送信するべき CAN メッセージ以外のメッセージ送信を禁止すること、3 つ目には踏み台 ECU が本来送信するメッセージの送信頻度を超えてメッセージを送信することを防ぐことを挙げ、これら 3 つの具体的な実現方法についても検討している。

・立命館大学の中野らの報告では、特定の車両おける衝突回避システムである自動ブレーキは悪天候時の誤動作を防止するために、ワイパーが作動中の場合には正常に作動しないことに注目した攻撃を提案している[4]。実験において、ワイパーを作動させる偽メッセージを送信することで自動ブレーキが正常に動作しないことを示している。このようなシステムに対する攻撃の対策手法として、CAN メッセージ中に挿入されているチェックサム 1byte 分を MAC に変更することで、CAN メッセージのペイロードの負荷を軽減しつつなりすましのメッセージを検出する手法が提案されている。

・攻撃の対象として、CAN だけでなく、LIN バスを対象とした攻撃方法も提案されている。NTT セキュアプラットフォーム研究所の高橋らの報告では LIN の特性を考慮し、幾つかの攻撃手法とその対策について提案している[5]。攻撃の例を以降に挙げる。LIN のマスターノードに対するレスポンスを正規のスレーブノードが行う場合、攻撃者が用意した攻撃用の ECU が異常なメッセージを流す。この時、ビットエラーが起きたと判断し、正規のスレーブノードはメッセージの送信を停止する。正規のスレーブノードがメッセージの送信を停止した後は、攻撃用の ECU は送信者になりすまし、任意のメッセージを送信することができる。対策としては、LIN にも CAN のメッセージと同様に MAC をつける方式や、データフィールドの 1 バイト目に重要なデータをおく方式により、そのあとのメッセージが衝突により改ざんされてもマスターノードが誤認識しにくくなる方式などが提案されている。

また、複数の ECU からなるシステムの脆弱性を調べる方法の一つとしてファジング(Fuzzing)という技術があることが知られている。そこで、ファジングに関連する主な論文等の調査を行った。

組込み機器に対するファジングの規定として、ISA Secure 認証仕様[6]では、EDSA (Embedded Device Security Assurance) 認証の CRT (Communication Robustness Testing) におけるファジング項目や手順等について規定している。この中では誤りのあるメッセージに対するシステムの応答や、システムに高負荷をかけた状態での応答を調査するとしている。IP ベース、Ethernet、UDP、TCP 等のプロトコルに対して CRT 仕様が規定されているが、CAN プロトコルに対しては規定されていない。

車載ネットワークを経由したファジングの関連研究として、国際会議 CHES 2014 におけるポスター発表[7]では、Stephanie Bayer らが DoCAN（Diagnostic communication over CAN）プロトコルを介して接続する PC 上の ECU シミュレーションに対して、ファジングを行った事例が紹介されている。ファズの生成には汎用のファジングツールである Peach Fuzzer [8]を用いており、効率的なファズの生成や集中的なモニタリングが可能であると主張している。テスト対象のデバイスの現在の状態の評価は、ファザーからの確認要求に対してデバイスの反応が正確に行えるかどうかで行っており、特定のデータを送った時には予測に反した反応を示す例がファジング実験により確認されている。

また、同じく Stephanie Bayer らは 2015 年 11 月に開催された escar Europe において、CAN の診断機能である UDS（Unified Diagnostic Services）に対するファジング事例を示している[9]。この論文中では、自動車の開発初期段階からセキュリティ評価を行う必要性を述べている。システムの仕様書を基に評価を行う Theoretical Security Analysis では、インプリメンテーションの欠陥や、仕様書の記述が十分でない仕様、外部からのコンポーネントの脆弱性が見つけられないため、Fuzzing を含む Practical Security Testing が重要であると主張している。実験では PC 上の ECU シミュレーションに対して、UDS のサービスリクエストである Communication Control、RadDataByIdentifier、ReadDTCInformation、RequestUpload の 4 つをファズとして送信し、ターゲットモニターでフォールトを観測している。ECU シミュレーションに相当するサーバの評価は以下の図 3.2d.5-1 の構成で行われる。これにより、攻撃に利用できるフォールトが 8 つ見つかり、そのうち 6 つは不正な値の応答で 2 つはサーバの停止であった。また、不正な値の応答は再現可能なフォールトだったとされている。

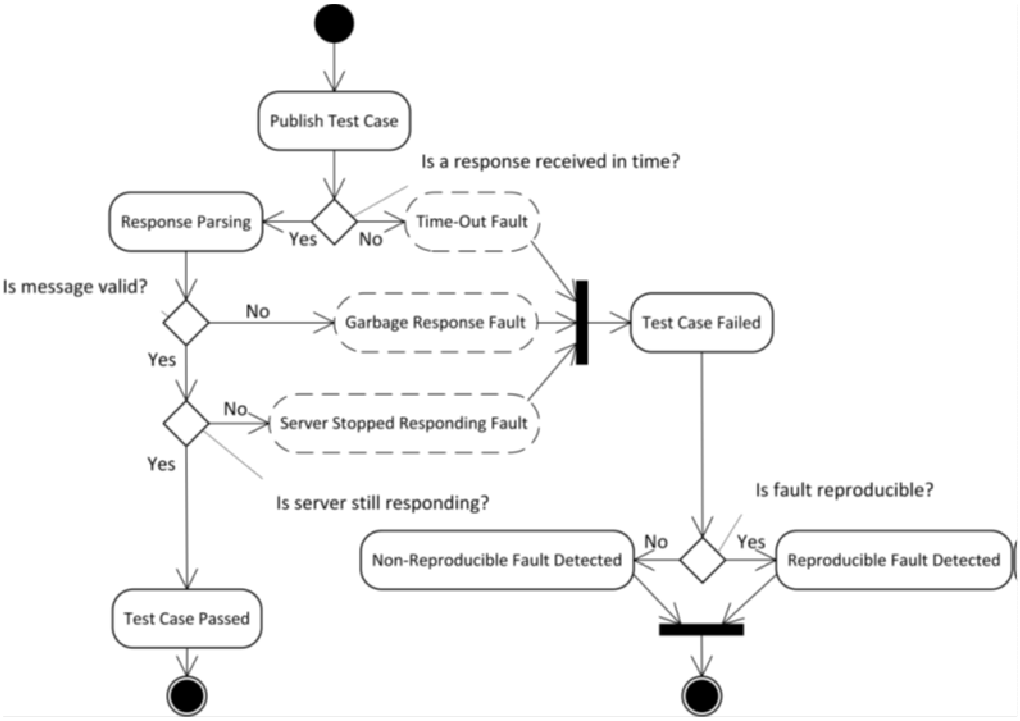


図 3.2d.5-1　Validation of the server's response [4]

これらのファジング事例では、車載ネットワークとして用いられるプロトコルを対象とはしているが CAN の診断機能に限定されおり、また、ネットワークに接続されている ECU のファームウェアやミドルウェアの問題点までは言及していない。

参考文献

[1] 中野学, 松本勉, Camille Vuileaume, 古谷誠剛, “自動車の情報セキュリティ,” 日経 BP 社, 2013.

[2] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," 2010 IEEE Symposium on Security and Privacy, pp.447-462, 2010.

[3] 倉地 亮,本田 晋也, 高田 広章, 上田 浩史, 堀端 啓史 "Controller Area Network (CAN) の不正送信防止機構の提案," SCIS2016 予稿集, SCIS2016, 2016.

[4] 中野 将志, 中澤 祐希, 久保田 貴也, 汐崎 充, 藤野 毅, "ADAS ECU の動作条件を悪用した自動車の衝突回避システムに対する攻撃手法と軽量 MAC 認証手法の提案," SCIS2016 予稿集, SCIS2016, 2016.

[5] 高橋 順子, 荒金 陽助, 宮澤 俊之, 冨士 仁, 山下 普史, 早川 桂太, 鵜飼 慎太郎, 早川 浩史, "自動車の不正な挙動を誘発する LIN 通信上での攻撃及び対策," SCIS2016 予稿集, SCIS2016, 2016.

[6] ISA Secure, Japanese-ISASecure Program, http://isasecure.org/en-US/Certification/IEC-62443-4-2-EDSA-Certification-(In-Japanese)

[7] Stephanie Bayer, Petr Vyleta, “Fuzzing in vehicular networks: Finding vulnerabilities before the predator”, CHES2014 Poster Presentation, Sept. 2014.

[8] Deja vu Security, PEACH FuzzerTM platform, 2013, http://peachfuzzer.com/

[9] Stephanie Bayer, Alexander Ptok, “Don’t Fuss about Fuzzing: Fuzzing Controller in Vehicular Networks,” escar Europe Conference 2015, 2015.

3.2e　第三者認証に関する調査

自動車では、近年になって車内の電子化が進み、また、V2X 通信やスマホ等による車外との接続が始まったところであり、セキュリティへの取組みは行われているが、まだ、第三者認証に関しては、その要否も含めて検討が進んでいない。

IT 業界等においては、情報セキュリティに関する第三者認証として、CC (Common Criteria) 認証が知られている。CC は情報セキュリティに関する評価基準の規格であり、国際的に用いられている。また、CC 認証以外にも、それぞれの機器の相互接続性を確認するなどの認証が行われているケースもある。

本事業では、自動車のセキュリティにおける第三者認証制度の必要性や、必要な場合にはどういったことが対象となるかを検討するための前段階として、他業界における状況について、第三者評価や認証などを行っている機関である、株式会社 ECSEC Laboratory（以下、ECSEC と称す)、技術研究組合　制御システムセキュリティセンター（以下、CSSC と称す）にヒアリング調査を実施した。

3.2e.1　ECSEC ヒアリング調査

第三者認証を検討する上で、まずは、どういった仕組みで認証が行われているかを理解する必要がある。そこで、IT 製品/システムとスマートカード（IC カード）関連デバイスの分野にて認定を受けた評価機関でもある ECSEC にヒアリングを行った。

図 3.2e.1-1 は、一般的な第三者認証における関係者とその関係を示したものである。

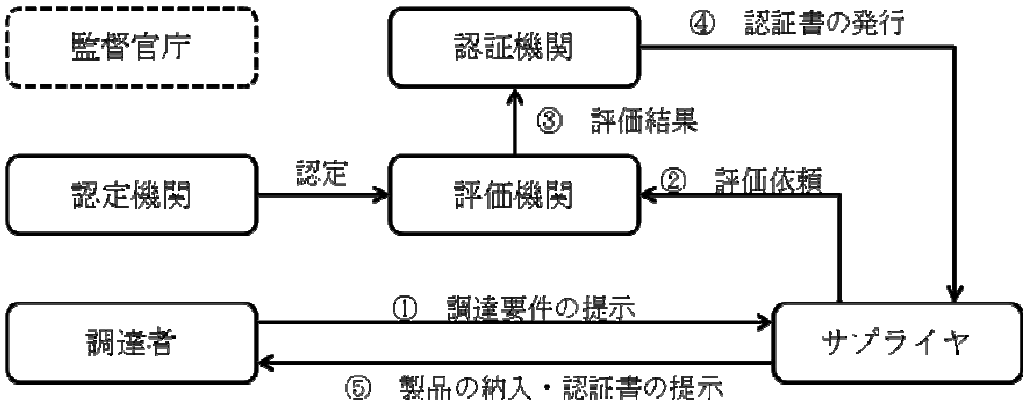


図 3.2e.1-1　第三者認証における関係者

ここでは、調達者があるサプライヤから製品の供給を受ける場合に、第三者認証を調達要件としている場合の流れを示している。調達者は、その調達要件の中で、サプライヤに対して納入する製品に対して受けるべき第三者認証を提示する。サプライヤは、該当する製品の評価を評価機関に依頼する。評価機関は、その製品を評価しその結果を認証機関に報告する。認証機関では、その評価報告を受けて、その内容を審査して合格の場合、評価対象となった製品に対する認証書をサプライヤに発行し、サプライヤは、その認証書を、調達要件を満たしていることの証明として調達者に示す、というのが第三者認証の流れで

ある。また、認定機関の役割は、評価機関において評価の手順や評価に用いられる基準が正しいものであるかを確認し、認定するものである。その評価手順や評価基準は、IC カードや、クレジットカード、制御システム、医療機器などのセクタごとに設けられている。

図 3.2e.1-2 に一例として、IPA により運営されている「IT セキュリティ評価及び認証制度 (JISEC:Japan Information Technology Security Evaluation and Certification Scheme)」の仕組みを示す。

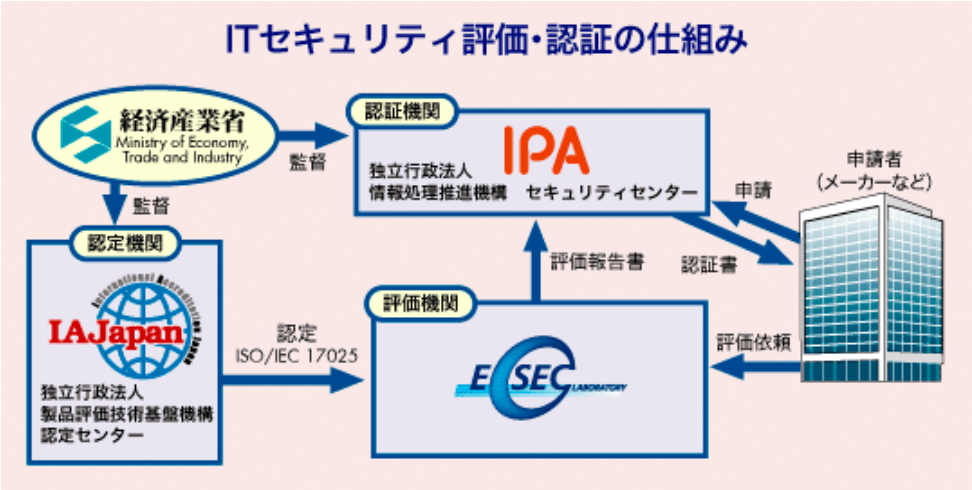


図 3.2e.1-2　IT セキュリティ評価・認証の仕組み（http://www.ecsec.jp/CC1.html）

上記の JISEC の枠組みによって認証された製品等は、IPA および CCRA のサイトに掲載されており、各製品等に対応する認証書と認証報告書（評価機関における評価の結果）が公開されている。(https://www.ipa.go.jp/security/jisec/certified_products/cert_list.html）この認証書には、例えば、「IT セキュリティ評価及び認証制度に基づき、下記のとおり認証する」と記載されている。この記載からも分かるとおり、認証が成立するためには、どういった制度に基づいて評価が行われるのかが確立されている必要がある。

図 3.2e.1-1 や図 3.2e.1-2 に示すように、認定機関、評価機関、認証機関は、それぞれ独立した機関で構成されることが一般的ではあるが、セクタによっては、認証機関が認定機関を兼ねている場合もある。これに該当する例の 1 つが、図 3.2e.1-3 に示す EMV 仕様（Europay International、MasterCard International、Visa International の共同制定による金融取引用 IC カード関連仕様）に基づく認定の仕組みである。また、調達者が認定機関を兼ねる例もあるが、この場合でも評価機関は第三者である。なお、評価機関は複数でも良いが、認定機関、認証機関は、判断が同じになる必要があるため、セクタで 1 つだけとなっている。

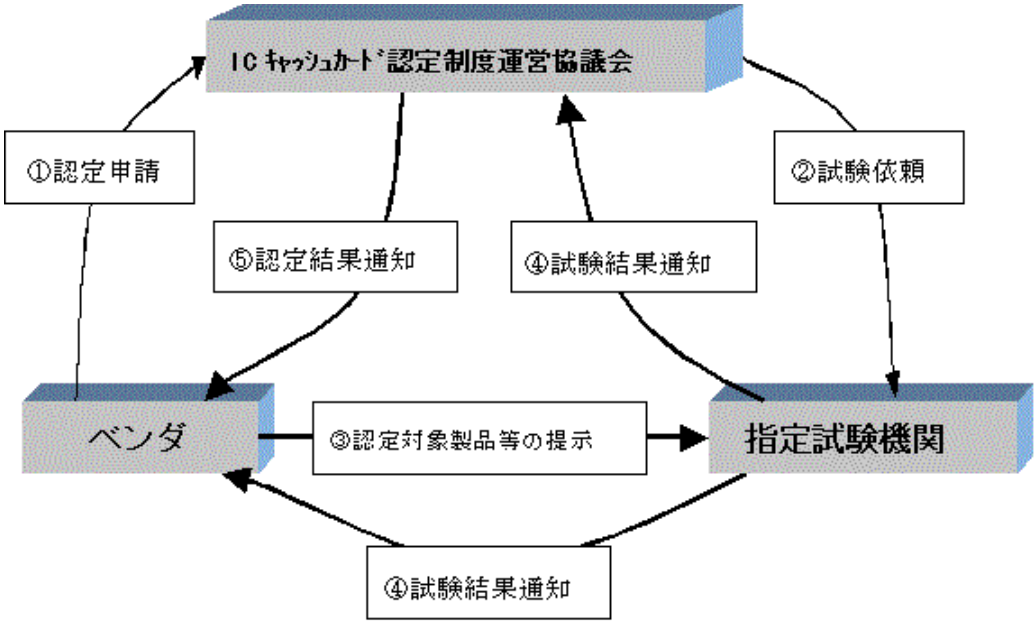


図 3.2e.1-3　IC キャッシュカード認定の仕組み（http://www.ictac.jp/kaisetsu3.htm）

JISEC の仕組みで発行された認証書は、国内に限らず CCRA（Common Criteria Recognition Arrangement）加盟 26 か国で有効となり、日本の制度で認証取得した製品は海外でも同様に認証を取得した製品と認められる仕組みが構築されている。

自動車に関する認証の仕組みは、海外を含めまだ出来ていないが、欧州では、EVITA、C2C-CC 等のプロジェクトの中で議論されていると推測される。また、米国では NIST（National Institute of Standards and Technology）や、NHTSA（National Highway Traffic Safety Administration）、SAE（Society of Automotive Engineers）で検討されているものと推測される。

3.2e.2　CSSC ヒアリング調査

制御システムにおけるセキュリティ認証については、IEC62443 で規定されており、CSSC は、そのスキームである ISASecure®認証の、日本における認証機関の位置付けである（図 3.2e.2-1）。

現在、CSSC で実際に行っている ISASecure®認証としては「制御機器認証（EDSA）」、「セキュリティ開発ライフサイクルのプロセス認証（SDLA）」、「制御システム認証（SSA）」がある。EDSA は、さらに「通信ロバストネス試験（CRT）」「セキュリティ機能評価（FSA）」「セキュリティ開発ライフサイクル評価（SDSA）」という階層に分かれている（図 3.2e.2-2）。

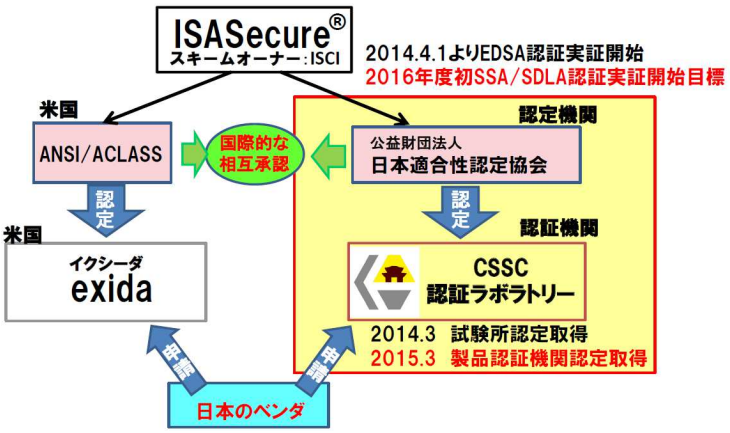


図 3.2e.2-1　ISASecure®認証スキームの日本での展開（CSSC 公開資料より）

http://www.css-center.or.jp/sympo/2015/documents/20150514-22_03kobayashi.pdf

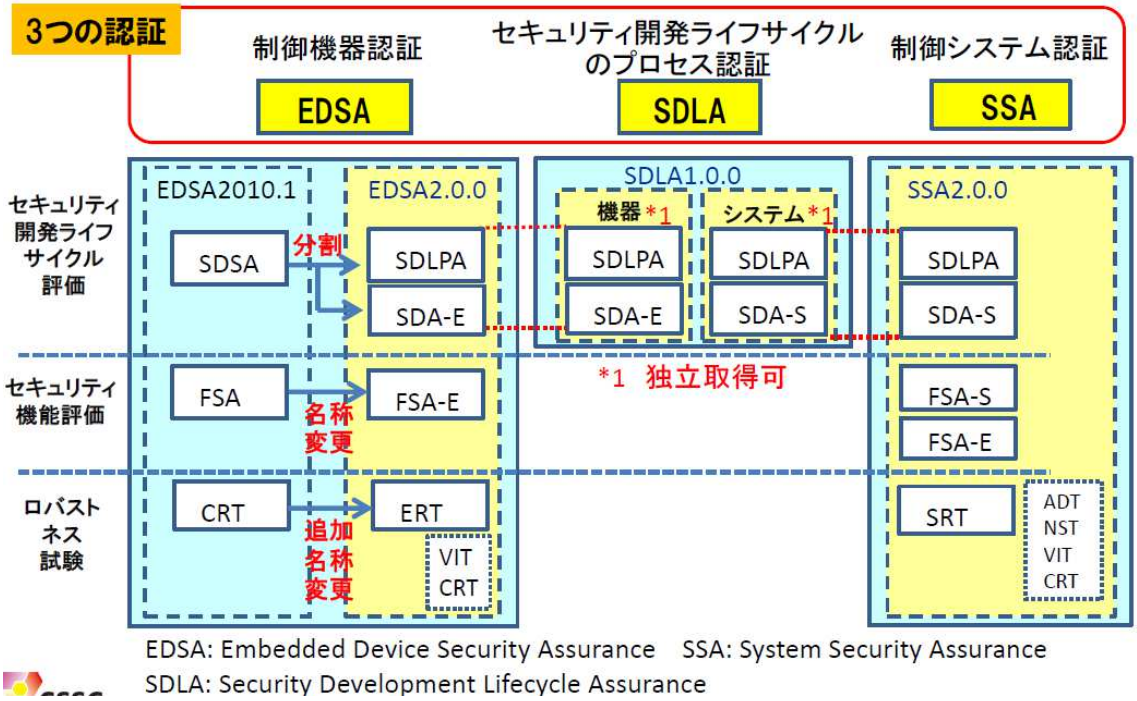


図 3.2e.2-2　ISASecure®における認証（CSSC 公開資料より）

このうち、通信ロバストネス試験は、例えば、通信のポートから攻撃を加えるといった評価を実施するものである。セキュリティ機能評価では、データの秘匿性や完全性が担保されているか、あるいは、セキュリティ機能が実装出来ているかを確認する。実装の確認方法としては、セキュリティガイドを提示して、それが実装されているということをドキュメントにしている場合は、ドキュメントを中心とした確認となる。

また、セキュリティ開発ライフサイクル評価では、製品がセキュアなものになるように開発されているかどうかを製品開発プロセスに沿って評価を行うものである。

EDSA 認証は、PLC、SIS コントローラ、DCS コントローラ等の組込み機器を対象とした認証であり、スキームオーナーである ISCI（ISA Security Compliance Institute）が運営している。また、組込み機器を対象としているが、製品開発プロセス全体に責任を持てるベンダーの製品であることが前提となっている。

EDSA 認証を含む ISASecure®の特徴は、制御システムを対象としていることから、CC 認証と比べて、認証にかかる期間や費用が少なく済むことである（目安としては、3 ヶ月、1 千万円程度）。また、制御システムでは、多様な機器が接続され、かつ、それらの機器のバリエーションも多数あることから、制御システムを構成する全ての機器に対しての認証を行うことは現実的ではないと考えられる。

なお、CSSC は、EDSA の製品認証機関としての認定を受けているが、今後、制御システム認証（SSA）の認定を受けるための準備を進めている段階である。図 3.2e.2-3 に SSA の評価項目を示す。

項目		内容
SRT	ADT: Asset Discovery Testing	ポートスキャンによるパッシブな探索
	CRT: Communication Robustness Testing	ツールによるファジングテスト
	NST: Network Stress Testing	ツールによるネットワーク負荷テスト
	VIT: Vulnerability Identification Testing	Nessusによる既知脆弱性探索
FSA-S: Functional Security Assessment for System		システムのセキュリティ機能アセスメント
SDA-S: Security Development Artifacts for System		システムのセキュリティ開発記録評価
SDLPA: Security Development Lifecycle Process Assessment		組織のセキュリティ開発プロセス保証
(FSA-E): Functional Security Assessment for Embedded Device Components		EDSA認証を受けていない機器については、レベル1相当のセキュリティ機能をもつことを確認

SRT: System Robustness Testing

図 3.2e.2-3　SSA における評価項目（CSSC 公開資料より）

認証そのものが必要となるかどうかは、最終需要者が必要と考えるかどうかに大きく依存している。現在、ISCI の設立メンバーに、Chevron、Exxon Mobile が名を連ねており、石油業界がこの活動をリードしていることが伺える。

車のシステムを考えたときに、どうやれば安全になるのか、システム全体をカバーして、ようやくセキュリティをカバーできるとも考えられるため、大きな枠組みが必要になる可能性がある。

また、個別のコンポーネントである ECU を評価する際にも、Firewall や Gateway をおくことがあるが、基本的には Firewall の外から試験をすることになる。ここでは、通信パケット（プロトコル）として、異常なものが来ても、リアクションしないことの確認を行う。

IEC62443 は制御システム全般のセキュリティをカバーしているので、その考え方は、自動車セキュリティにも応用できる可能性がある。また、IEC62443-3-2 では、Zone と Conduit という考え方を導入している。これは、Zone ごとに必要なものを高いセキュリティにしようという考え方である。脅威分析を行う際に、Zone-Conduit に分けて分析する手法は、自動車セキュリティでも参考に出来る可能性がある。なお、IEC62443-3-2 に脅威分析のやり方が記載されており、現状は ISA の HP でドラフトが公開されている。
（http://isa99.isa.org/ISA99 Wiki/WP_List.aspx）

3.2e.3　考察

自動車セキュリティにおける第三者認証については、制度としての必要性は言われているものの、認証を行うとした場合の対象、評価手法・評価基準など、まだ決まっていない。欧米においても同様に検討段階にあるものと考えられるが、自動車やその部品は輸出入されるものが多く、今後、相互認証制度や評価基準の整合など、国際協調が重要な分野である。その際、認定機関や評価機関のあり方についても検討が必要ではあるが、国際協調の議論にあたっては、まず、日本としての評価手法や評価基準に対する考え方を固めておくことが重要と考えられる。

3.3　V2X 通信における署名検証の簡略化の研究（テーマ③）

「平成 26 年度戦略的イノベーション創造プログラム V2X システムに係るセキュリティ技術の海外動向等の調査」にて、署名検証の簡略化・最適化は、海外の V2X システムにおける課題の一つであり、V2X 通信が普及していった際に重要となる技術であることが挙げられた。

本節では、メッセージ検証を構成する内部処理の処理時間を効率的に調査し、欧米の論文等で検討中の簡略化方式を評価・分析した。

署名検証の簡略化検討にあたっては、V2X 通信への適用により、セキュリティを担保しつつ、その処理能力を高めリアルタイム性を確保可能な署名検証簡略化のモデル案を立案した。

3.3.1　V2X 通信の処理時間の調査

本項では、テーマ③の研究対象と、V2X 通信のセキュリティ規格である IEEE1609.2[1] の概要を説明した後、V2X 通信メッセージ検証を構成する内部処理の分析と、各内部処理の処理時間の調査・計測を行った結果を報告する。

(1) テーマ③の研究対象

テーマ③の研究対象は、V2X システムを構成する V2X 車載器のメッセージ検証である（図 3.3.1-1 参照）。V2X システムは、V2X 通信を利用して V2X 車載器と路側機が互いにメッセージを送受信しながら、例えば運転支援等のサービスをドライバに提供する。V2X 車載器や路側機は自車位置や周辺情報等を V2X 通信のメッセージとして周期的にブロードキャストする。そのため、一つの V2X 車載器の通信範囲に N 台の V2X 車載器や路側機がある場合、伝送効率を無視すれば、毎周期 N 個のメッセージを受信する。欧州の研究事例[2]では一つの V2X 車載器が 1 秒あたりに受信するメッセージ数を最大で 1,000 程度と予測しており、メッセージ検証のリアルタイム性の確保が重要な課題となっている。そこでテーマ③の研究対象をメッセージ検証（図 3.3.1-1 中の破線内）とした。

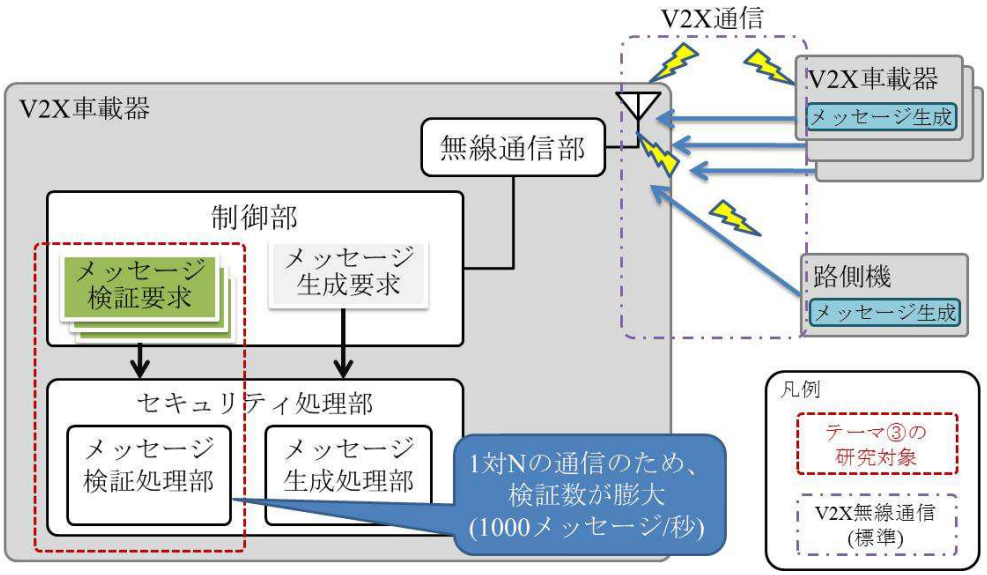


図 3.3.1-1　V2X システム構成図

テーマ③の研究対象であるメッセージ検証はキューを用いることを想定しており、次の様に動作する（図 3.3.1-2 参照）。制御部は、(1) 他の V2X 車載器から受信したメッセージを検証するための検証要求を生成しセキュリティ処理部に送信する。セキュリティ処理部は(2) 受信した検証要求をキューに入れる一方で、(3) キューから検証要求を取り出し、メッセージ検証処理を行う。メッセージ検証が終了した際には、(4) その結果を制御部に送信する。(5) 制御部は受信した検証結果を検証結果キューに入れる一方で、(6) 検証結果キューから検証結果を取り出してアプリケーション処理を行う。

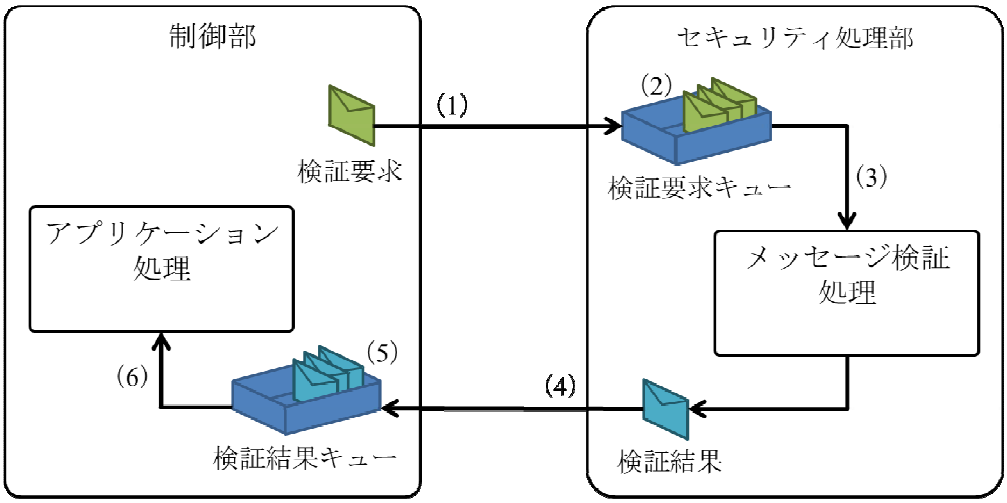


図 3.3.1-2　メッセージ受信時の V2X 車載器の動作

(2) V2X 通信のセキュリティ規格（IEEE1609.2）の概要

IEEE1609.2[1]は、V2X 通信のアーキテクチャやインタフェース等の標準を定める IEEE 1609 ファミリの一つであり、セキュリティに関するプロトコルやフォーマット、サービス等を規定する規格である。IEEE1609.2 の特徴は、不特定多数の車両と通信することから PKI（Public Key Infrastructure）を使用することや、V2X 通信は比較的帯域の少ない通信であることから独自フォーマットの証明書等を用いることである。

IEEE1609.2 が規定するメッセージフォーマットは 1609Dot2Data という型の構造体として定義されている。1609Dot2Data で定義されるメッセージのタイプとして、署名付きメッセージ、暗号化メッセージ、証明書失効リスト（CRL：Certificate Revocation List）等が存在する。

本項では、V2X 通信で主に使用されると予想される署名付きメッセージについて、そのメッセージの検証処理時間を調査した。

(3) 署名付きメッセージの構造

IEEE1609.2 の署名付きメッセージのフォーマット（概略）を図 3.3.1-3 に示す。

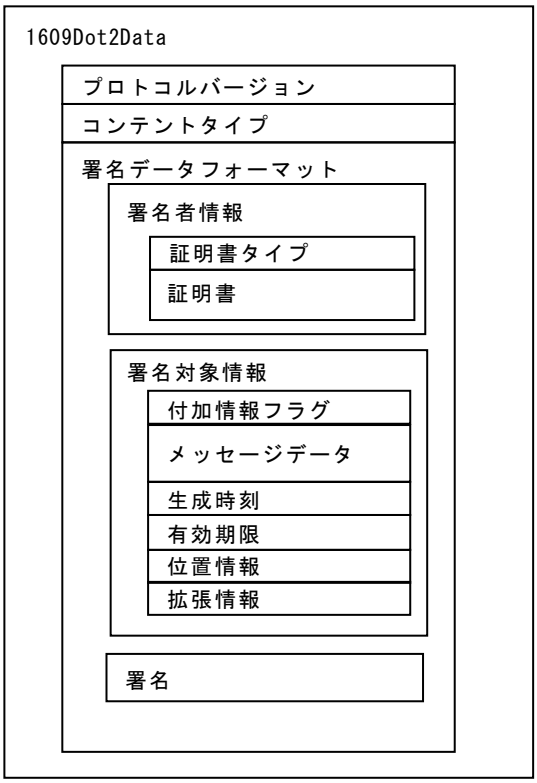


図 3.3.1-3　IEEE1609.2 の署名付きメッセージのフォーマット（概略）

プロトコルバージョンには、バージョン情報を示す値が格納される。

コンテントタイプにはメッセージのタイプ（署名付きメッセージ、暗号化メッセージ等）を示す値が格納され、そのタイプに応じて後続のデータ構造が定まる。コンテントタイプが署名付きメッセージを示す場合、後続のデータ構造は署名データフォーマットになる。

署名データフォーマットは、署名者情報、署名対象情報、署名の 3 つから構成される。署名者情報は証明書タイプと証明書から構成され、証明書タイプには後続のデータが証明書、証明書チェインもしくは証明書の ID のいずれであるのかを示す値が格納される。署名対象情報は付加情報フラグ、メッセージデータ、生成時刻、有効期限、位置情報、拡張情報等から構成される。付加情報フラグは本メッセージ中に生成時刻、有効期限、位置情報、拡張情報等の各情報が存在するかどうかをフラグで示している。生成時刻は本メッセージが生成された時刻を、有効期限は本メッセージの有効期限を、位置情報は本メッセージが生成された位置を、それぞれ示している。署名は署名対象情報に対する署名値が格納されている。

(4) 署名付きメッセージの検証処理

前節で述べた署名付きメッセージを検証する際の処理について、その処理時間を調査するため、便宜上、内部処理を計 9 つの Step に細分化した（図 3.3.1-4）。

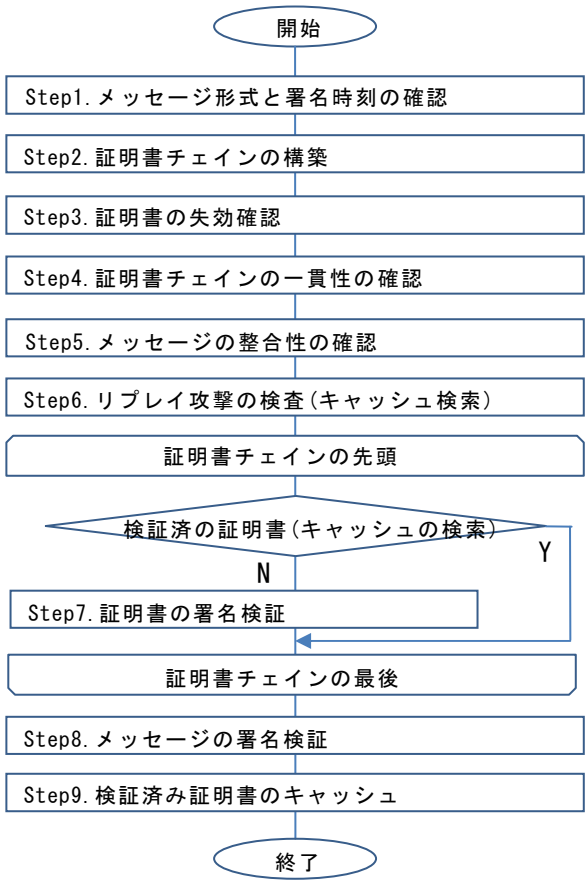


図 3.3.1-4　IEEE1609.2 の署名付きメッセージの検証処理フロー

各 Step の処理内容の詳細について表 3.3.1-1 に示す。

表 3.3.1-1　各 Step の処理内容の詳細

Step	処理の詳細
Step1 （形式と時刻の確認）	メッセージのコンテントタイプが署名付きメッセージを示す値であるかを確認する。また、メッセージの有効期限が過ぎていないか、生成時刻と有効期限の時系列が不正でないか等を確認する。
Step2 （チェイン構築）	メッセージ内および機器内に格納されている証明書を用いて、送信者の証明書から Root 証明書までのパスを構築する。
Step3 （失効確認）	Step2（チェイン構築）でパスを構築した証明書が失効していないかを検証する。
Step4 （チェインの一貫性確認）	パスを構築した証明書チェインの証明書に記載されている有効期限や有効範囲等について証明書間の一貫性を確認する。
Step5 （メッセージの整合性確認）	メッセージ中に格納された生成時刻、有効期限、位置情報等と証明書の有効期限や有効範囲等からその整合性を確認する。
Step6 （リプレイ攻撃検査）	リプレイ攻撃への対処のため、過去に受信したメッセージ情報のキャッシュを検索し、同じメッセージを受信済みでないかを確認する。未受信の場合は検索終了後に当該メッセージの情報をキャッシュへ登録する。
Step7 （証明書の署名検証）	検証済みの証明書情報のキャッシュを検索し、存在しない場合は証明書の署名検証を行う。
Step8 （メッセージの署名検証）	メッセージの署名検証を行う。
Step9 （証明書のキャッシュ）	検証の済んだ証明書情報を機器内のキャッシュに保持する。

(5) 検証処理の時間に影響するパラメータ

署名付きメッセージの検証処理時間に影響するパラメータを抽出するため、図 3.3.1-4 で示した各 Step について、処理時間に影響を及ぼし得る要素を洗い出した。その結果を表 3.3.1-2 に示す。

表 3.3.1-2　各 Step に影響を及ぼし得る要素

Step	影響を 及ぼし得る要素	理由
Step1 （形式と時刻の確認）	なし	－
Step2 （チェイン構築）	証明書のチェイン数	チェイン数が増えるほど構築のための処理時間も増える。
	検証済み証明書のキャッシュ数	検証済み証明書のキャッシュ数が増えると、検索時間も増える。ただし、キャッシュにヒットした場合には処理時間の短縮が見込める。
Step3 （失効確認）	証明書のチェイン数	チェインを構成する証明書毎に失効確認を行う必要がある。
	CRL のエントリ数	CRL のエントリ数が増えると 1 回の失効確認に要する時間も増える。
Step4 （チェインの一貫性確認）	証明書のチェイン数	上位と下位の証明書間の一貫性の確認を行うため、チェイン数が増えれば確認する回数も増える。
Step5 （メッセージの整合性確認）	なし	－
Step6 （リプレイ攻撃検査）	検証済みメッセージのキャッシュ数	検証済みメッセージのキャッシュ数が増えると、検索時間も増える。
Step7 （証明書の署名検証）	証明書のチェイン数	チェイン数が増えると、署名検証の回数も増える。
	検証済み証明書のキャッシュ数	検証済み証明書のキャッシュ数が増えると、検索時間も増える。ただし、キャッシュにヒットした場合には検証処理が不要となり、処理時間の短縮が見込める。
Step8 （メッセージの署名検証）	なし	－
Step9 （証明書のキャッシュ）	証明書のチェイン数	チェインを構成する証明書毎にキャッシュ処理を行うため。
	検証済み証明書のキャッシュ数	検証済み証明書のキャッシュ数が増えると、キャッシュ追加処理が遅くなる。

表 3.3.1-2 で洗い出した要素を整理すると、表 3.3.1-3 に示す 5 項目が署名付きメッセージの検証処理時間に影響を及ぼすパラメータとなる。なお、検証済の証明書の数については、EndEntity（EE）の証明書のキャッシュと Sub Certification Authority（Sub CA）の証明書のキャッシュは別管理となるため、それぞれ別のパラメータとしている。

表 3.3.1-3　処理時間に影響を及ぼすパラメータ

処理時間に影響を及ぼすパラメータ		説明
（a）	チェイン数	証明書のチェイン数
（b）	EE 証明書数	内部で保持する検証済 EE 証明書の数
（c）	Sub CA 証明書数	内部で保持する検証済 Sub CA 証明書の数
（d）	CRL 数	CRL のエントリ数
（e）	メッセージ数	内部で保持する検証済メッセージの数

次に、表 3.3.1-3 に示す 5 つのパラメータそれぞれについて、規格、各地域仕様、先行研究事例等からその取り得る値を選定した。選定結果を表 3.3.1-4 に示す。

表 3.3.1-4　パラメータ毎の取り得る値

処理時間に影響を及ぼすパラメータ		値	値の選定理由
（a）	チェイン数	2、3、8	2: 米国仕様[3]による。 3: 欧州プロジェクトの報告[4]による。 8: V2X 通信のセキュリティ規格[1]の最大値。
（b）	EE 証明書数	1,700	1 台の車載器の通信範囲に存在する車両の台数、日本の研究事例[5]を流用。
（c）	Sub CA 証明書-数	30	米国仕様[3]では Sub CA なし。 欧州仕様では記述は無いが EU 各国（28 か国）に一つの Sub CA が存在すると仮定。
（d）	CRL 数	500 万 1,600 万	販売台数＝廃車台数と仮定し、ある年の販売台数を流用[6] 。 日本： 500 万台（2013 年） 米国：1,600 万台（2013 年） （欧州は CRL を使用しない）
（e）	メッセージ数	1,700	1 台の車載器の通信範囲に存在する車両の台数、日本の研究事例[5]を流用。

(6) 測定環境

測定装置、測定方法および測定条件を以下に示す。

今回の測定では、実際の車載システムは用いず、汎用 PC 上で署名付きメッセージの検証処理を実行し、その時間を測定した。

① 測定装置

・プロセッサ：Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz

・メモリ：4GB　　OS：Windows 7 SP1, 64bit　　暗号 SW：OpenSSL (1.0.2d)

② 測定方法

署名付きメッセージの検証処理を図 3.3.1-4 の各 Step に細分化し、各 Step の開始と終了でシステム時間を測定した。表 3.3.1-3 に示した 5 つのパラメータの値を変化させながら、測定条件毎に計 10 回の測定を行った。その後、処理時間が長い上位 2 個の結果と処理時間が短い下位 2 個の結果を除いた中間の 6 回分のデータについて、その平均値を求めた。

③ 測定条件

測定条件として表 3.3.1-5 に示す計 27 項目を定めた。

表 3.3.1-5　測定条件

No	パラメータ					備考
	(a)	(b)	(c)	(d)	(e)	
1	2	0	0	0	0	最少構成
2	3	0	0	0	0	(a)チェイン数の影響検証
3	8	0	0	0	0	
4	2	10	0	0	0	(b)EE 証明書数の影響検証
5	2	100	0	0	0	
6	2	200	0	0	0	
7	2	1,000	0	0	0	
8	2	1,700	0	0	0	
9	2	10,000	0	0	0	
10	3	0	10	0	0	(c)Sub CA 証明書数の影響検証
11	3	0	30	0	0	
12	3	0	100	0	0	
13	3	0	200	0	0	
14	3	0	1,000	0	0	
15	3	0	10,000	0	0	
16	2	0	0	100	0	(d)CRL 数の影響検証
17	2	0	0	1,000	0	
18	2	0	0	10,000	0	
19	2	0	0	100,000	0	
20	2	0	0	420,000	0	
21	2	0	0	5,000,000	0	
*22	2	0	0	16,000,000	0	*測定不可
23	2	0	0	0	100	(e)メッセージ数の影響検証
24	2	0	0	0	1,000	
25	2	0	0	0	1,700	
26	2	0	0	0	10,000	
27	2	0	0	0	100,000	

No.1 は今回の測定結果の基準となる最少構成の測定条件である。最少構成は、(a)チェイン数を 2 段に、その他の(b)EE 証明書数～(e)メッセージ数の各パラメータ数を全て 0 とした。No.2 以降は、それぞれのパラメータの影響を調べるため、注目パラメータ以外は最小構成と同じになる様に設定した。また、No.22 では、(d)CRL 数の値として米国では 1600 万までが想定されているが、今回用いた測定環境の処理性能上、測定不能であるため、No.21 の結果から予測値を求めている。No.21 は日本国内の想定値、No.20 は日本国内の年間廃車台数が 500 万台として、毎月の廃車対象台数（500 万/12）が更新される場合の CRL の値である。

なお、(c)Sub CA 証明書数については Sub CA が存在することが前提のパラメータであるため、証明書のチェイン数が 3 以上の測定条件でなければその影響度を検証することが出来ない。そのため、No.10～15 については(a)チェイン数を 3 段に設定している。従って、No.10～15 については No.1（チェイン=2）ではなく No.2（チェイン=3）の結果を基準値とし、No.2 との差異から(c)Sub CA 証明書数の影響度を検証することとした。

以後の説明の中で各測定条件の詳細を示す場合には、“No.1（チェイン=2、EE=0、SubCA=0、CRL=0、Msg=0）”のような表記とする。括弧内の表示は順に、(a)チェイン数、(b)EE 証明書数、(c)Sub CA 証明書数、(d)CRL 数、(e)メッセージ数を意味しており、上記例では、テスト番号 No.1 における各パラメータの値が、(a)チェイン数は 2 段、(b)EE 証明書数は 0、(c)Sub CA 証明書数は 0、(d)CRL 数は 0、(e)メッセージ数は 0 であることを表している。

(7) 測定結果

各測定条件で測定を行った結果を以下に説明する。

① 最少構成での結果

まず、基準値となる No.1 の測定結果を以下に示す（図 3.3.1-5）。

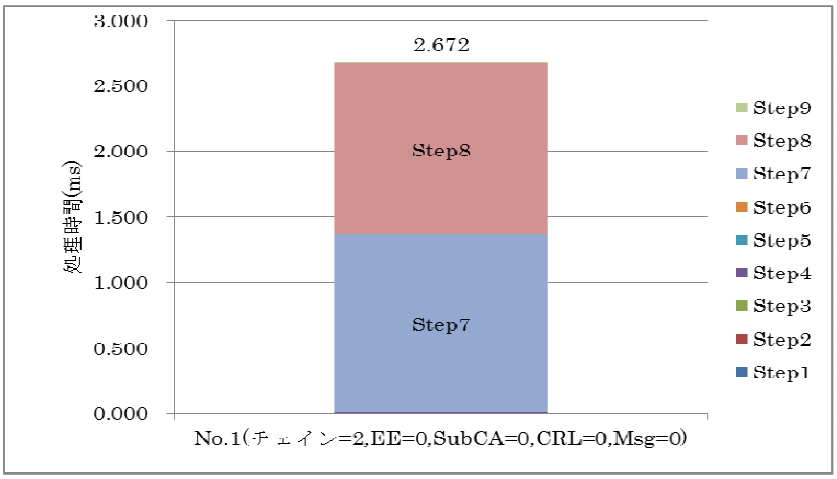


図 3.3.1-5　No.1 の測定結果

署名付きメッセージの検証処理全体では約 2.67ms かかっており、そのうちの 98%超は Step7（証明書の署名検証）と Step8（メッセージの署名検証）の処理で占められていることが分かった。Step7（証明書の署名検証）と Step8（メッセージの署名検証）はどちらも約 1.3ms の処理時間であった。

本結果から、署名付きメッセージの検証処理において Step7(証明書の署名検証)と Step8（メッセージの署名検証）の割合が支配的であり、処理時間短縮を実現するためにはこれら署名検証を如何に短縮するかが重要となることが分かった。

② チェイン数の検証結果

(a)チェイン数の影響を検証した No.2～3 の結果を以下に示す（図 3.3.1-6）。

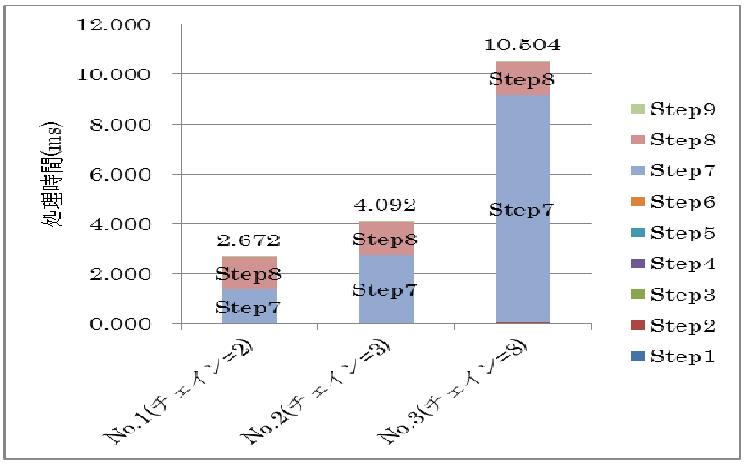


図 3.3.1-6　No.2～3 の測定結果

基準の No.1 に対し、チェインを増やすと Step7（証明書の署名検証）の処理時間が増加していくことが分かった。これは、チェインを構成する証明書毎に Step7（証明書の署名検証）の処理を行っているためである。

図 3.3.1-7 は、図 3.3.1-6 の結果から Step7（証明書の署名検証）の処理のみを抜き出したものである。

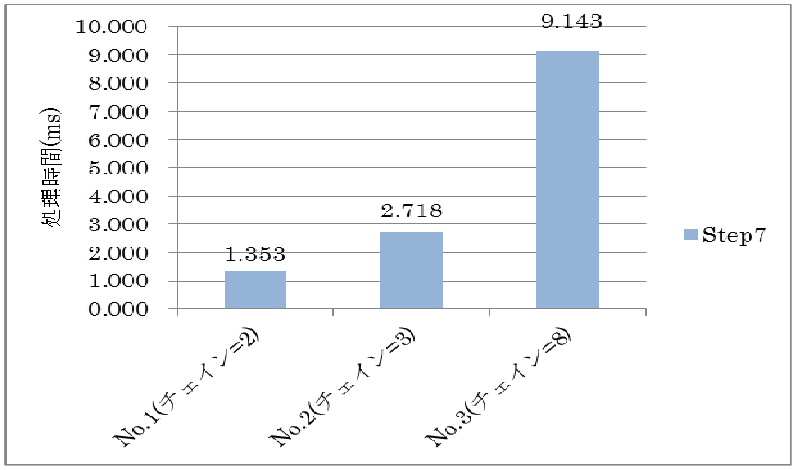


図 3.3.1-7　No.2～3 の結果から抜き出した Step7 の処理時間

これを見ると、No.1 では Step7(証明書の署名検証)は約 1.35ms の時間がかかっており、チェインを 1 段増やす毎に凡そ 1.3ms で比例して Step7（証明書の署名検証）の処理時間が増加していくことが分かった。

本結果から、検証済みの証明書のキャッシュが存在しない場合には、証明書のチェイン数が増えると全体の検証処理時間も大幅に増えるため、可能な限り少ないチェイン数で構成することが重要であることが分かった。ただし、検証済みの証明書のキャッシュを行うことでこの検証処理時間の増加は低減させることも可能と考えられる。

③ EE 証明書数の検証結果

(b)EE 証明書数の影響を検証した No.4～9 の結果を以下に示す（図 3.3.1-8）。

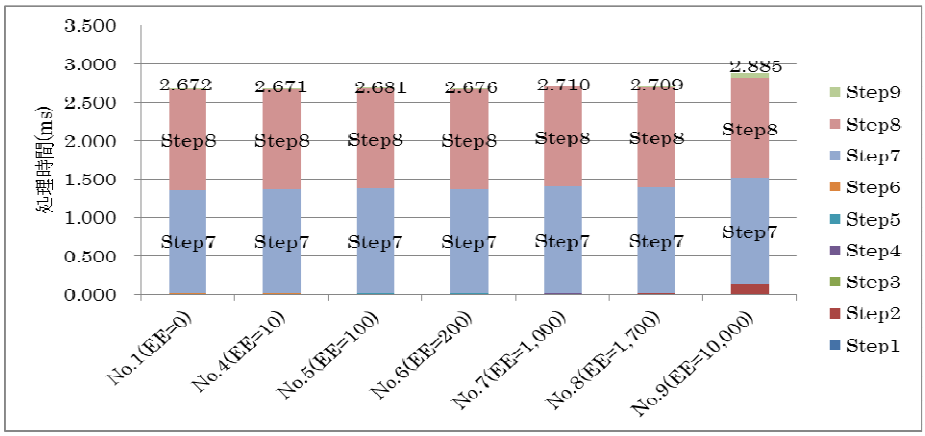


図 3.3.1-8　No.4～9 の測定結果

(b) EE 証明書数を最小 0 から最大 1 万の幅で変化させても、全体の検証処理時間に大きな影響は及ぼさないことが分かった。

ただし、(b) EE 証明書数の値を増加させると Step2（チェイン構築）と Step9（証明書のキャッシュ）の処理時間が増加していく。

図 3.3.1-9, 図 3.3.1-10 は、図 3.3.1-8 の結果から Step2(チェイン構築)の処理と Step9(証明書のキャッシュ）の処理をそれぞれ抜き出したものである。

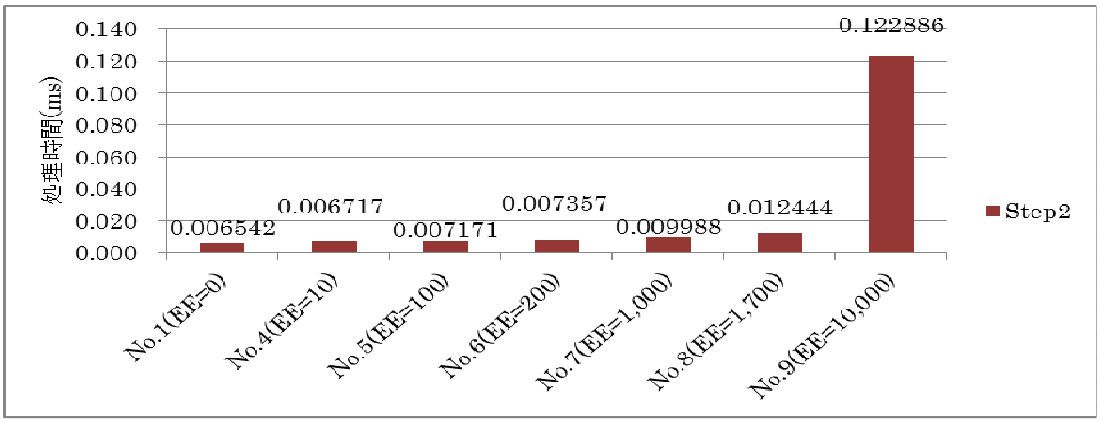


図 3.3.1-9　No.4～9 の結果から抜き出した Step2 の処理時間

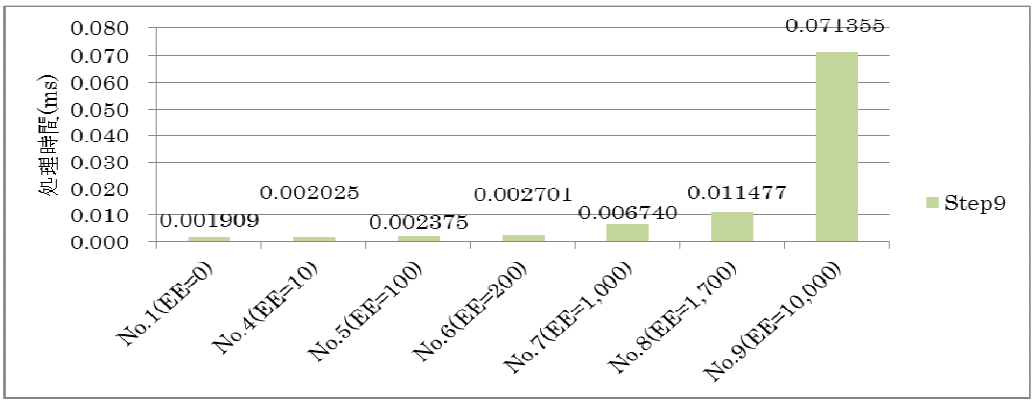


図 3.3.1-10　No.4～9 の結果から抜き出した Step9 の処理時間

(b) EE 証明書数を増やすと Step2（チェイン構築）と Step9（証明書のキャッシュ）もそれぞれ増加していき、1 万まで増やすと（No.9）、0 の時(No.1)と比べて Step2（チェイン構築）が約 0.116ms、Step9（証明書のキャッシュ）が約 0.069ms、併せて約 0.185ms ほどの増加となっている。

また、(b) EE 証明書数の取り得る値として想定している 1,700（No.8）の場合は、0 の時（No.1）と比べると Step2（チェイン構築）と Step9（証明書のキャッシュ）を併せて約 0.015ms の増加となっている。

これらの数字は全体の検証処理時間に及ぼす影響としては小さく見えるものの、今回の測定で使用した PC と実際の車載システムとでは CPU 性能に差があるため、車載システム上での処理時間を考えた場合にはやや影響が大きくなってくる可能性が懸念される。

④ Sub CA 証明書数の検証結果

(c) Sub CA 証明書数の影響を検証した No.10～15 の結果を以下に示す（図 3.3.1-11）。

なお、既述のとおり、(c) Sub CA 証明書数の検証には証明書のチェイン数が 3 以上である必要があるため、ここでは No.1 ではなく No.2 の結果を基準値としている。

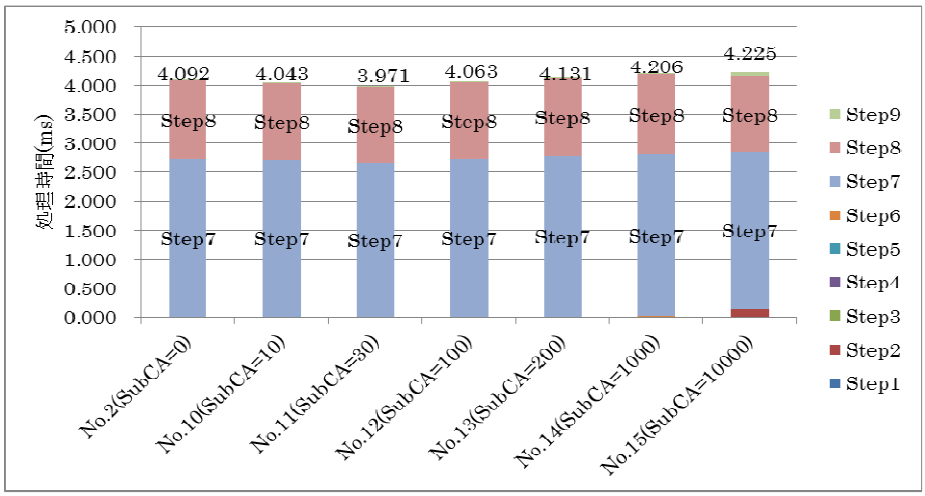


図 3.3.1-11　No.10～15 の測定結果

(b) EE 証明書数の結果と同様、(c) Sub CA 証明書数についても、最小 0 から最大 1 万の幅で変化させてもトータルの検証処理時間には特に大きな影響を及ぼさないことが分かった。

ただし、(c) Sub CA 証明書数の値を増加させると Step2（チェイン構築）と Step9（証明書のキャッシュ）の処理時間が増加していく。

図 3.3.1-12、図 3.3.1-13 は、図 3.3.1-11 の結果から Step2（チェイン構築）の処理と Step9（証明書のキャッシュ）の処理をそれぞれ抜き出したものである。

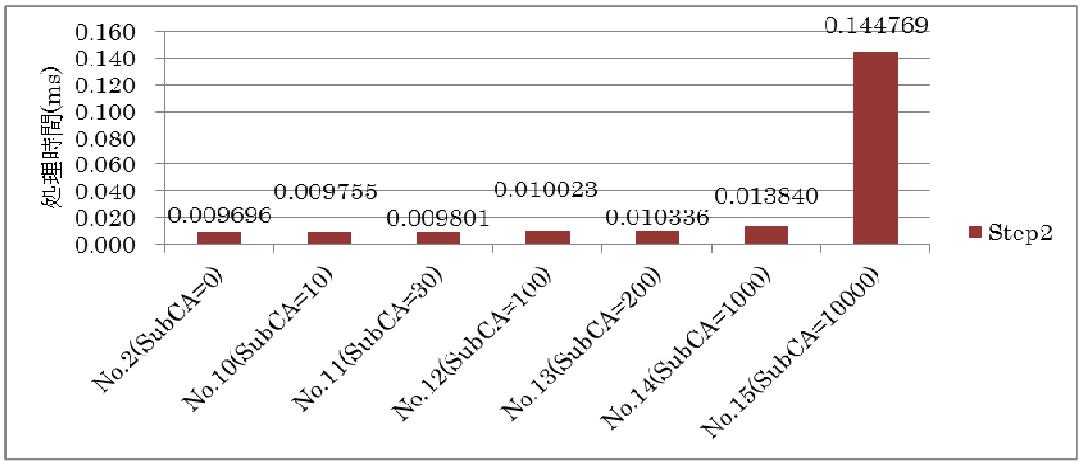


図 3.3.1-12　No.10～15 の結果から抜き出した Step2 の処理時間

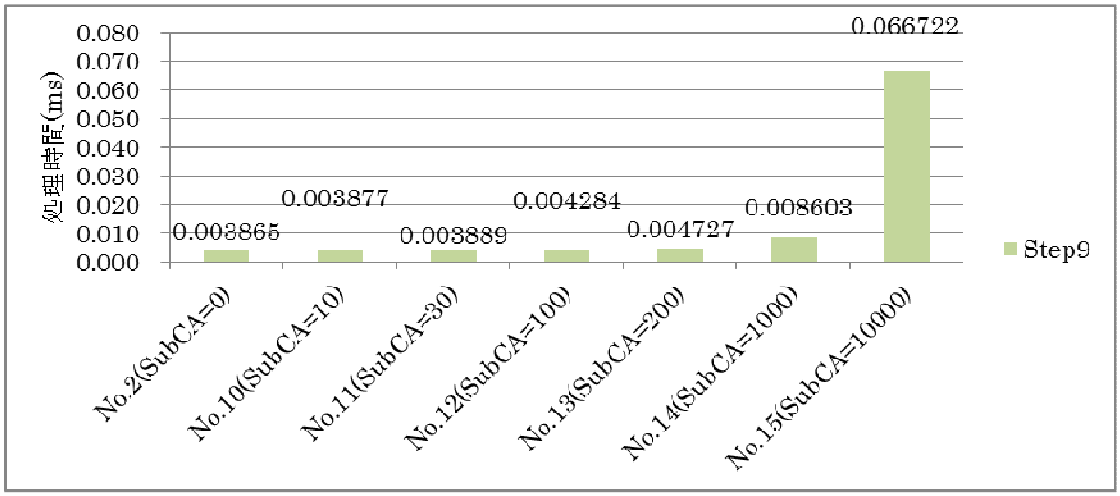


図 3.3.1-13　No.10～15 の結果から抜き出した Step9 の処理時間

(c) Sub CA 証明書数についても、(b) EE 証明書数と同じく、数を増やせば Step2（チェイン構築）と Step9（証明書のキャッシュ）がそれぞれ増加していく。1 万まで増やすと（No.15）、0 の時（No.2）と比べて Step2（チェイン構築）と Step9（証明書のキャッシュ）併せて 0.21ms 程度の差となってくるが、1,000 程度（No.14）までであれば 0.01ms 以下の処理時間に収まっており全体の検証処理時間に特に大きな影響は及ぼさないことが分かった。

表 3.3.1-4 に記載のとおり、(c) Sub CA 証明書数の取り得る値としては 30 を想定しており、その想定によれば、No.11 の結果からも(c) Sub CA 証明書数は署名付きメッセージの検証処理においてボトルネックとはならないことが分かった。

⑤ CRL 数の検証結果

(d)CRL 数の影響を検証した No.16～21 の結果を以下に示す（図 3.3.1-14）。

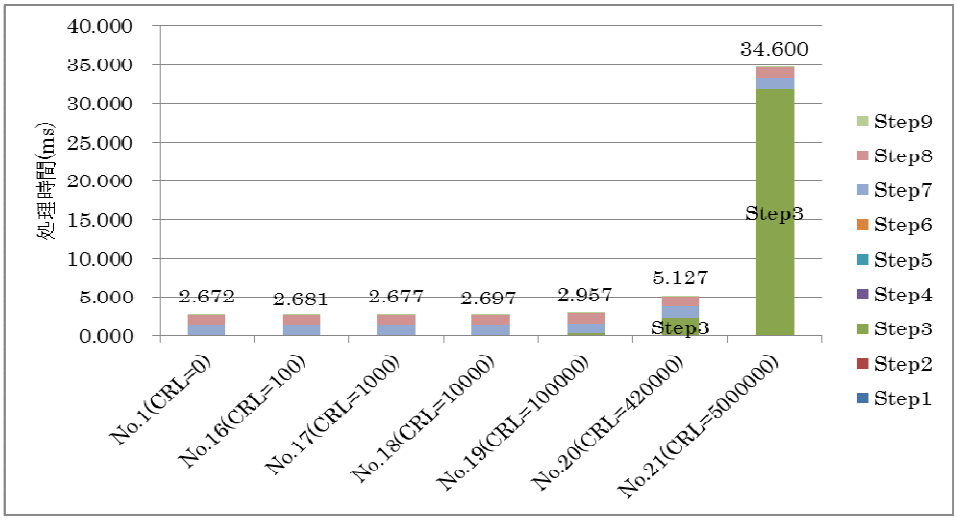


図 3.3.1-14　No.16～21 の測定結果

(d) CRL 数が 1 万以下まで（No.1, No.16～18）であれば全体の検証処理時間はほぼ変化がないことが分かった。しかしながら、10 万まで増やすと（No.19）、0.28ms 程度増加しており、影響が徐々に表れることが分かった。さらに 42 万まで増やすと（No.20）、全体の検証処理時間も 5ms を超えて、そのうち Step3（失効確認）が占める割合は約 47%まで増加し、500 万のケース（No.21）では全体の検証処理時間は 34.6ms、そのうち Step3（失効確認）が占める割合も約 92%まで増加した。また、この結果から、今回測定を行えなかった 1,600 万のケース（No.22）での全体の検証処理時間は、No.21 の 3 倍以上で約 110.7ms となるものと予想される。

図 3.3.1-15 は、図 3.3.1-14 の結果から値の大きい No.20 と No.21 を除外し、No.16～19 に関して Step3（失効確認）の処理を抜き出して処理時間を比較したものである。

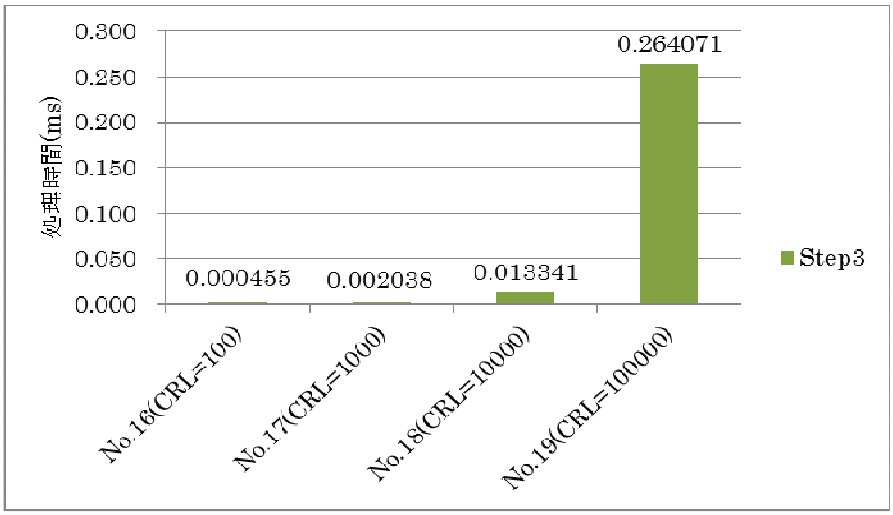


図 3.3.1-15　No.16～19 の結果から抜き出した Step3 の処理時間

図 3.3.1-14 では確認できなかったが、やはり(d) CRL 数を増やすと Step3（失効確認）の処理時間も増えて行っていることが図 3.3.1-15 から見て取れる。

表 3.3.1-4 に記載のとおり、(d) CRL 数の取り得る値として日本国内において 500 万に上ると想定すると、(d) CRL 数は署名付きメッセージの検証処理において極めて大きなボトルネックとなる。さらに、米国における年間の CRL 数を 1,600 万件と想定すると、米国では(d) CRL 数がさらに大きな問題となってくることが予想される。

⑥ メッセージ数の検証結果

(e) メッセージ数の影響を検証した No.23～27 の結果を以下に示す（図 3.3.1-16）。

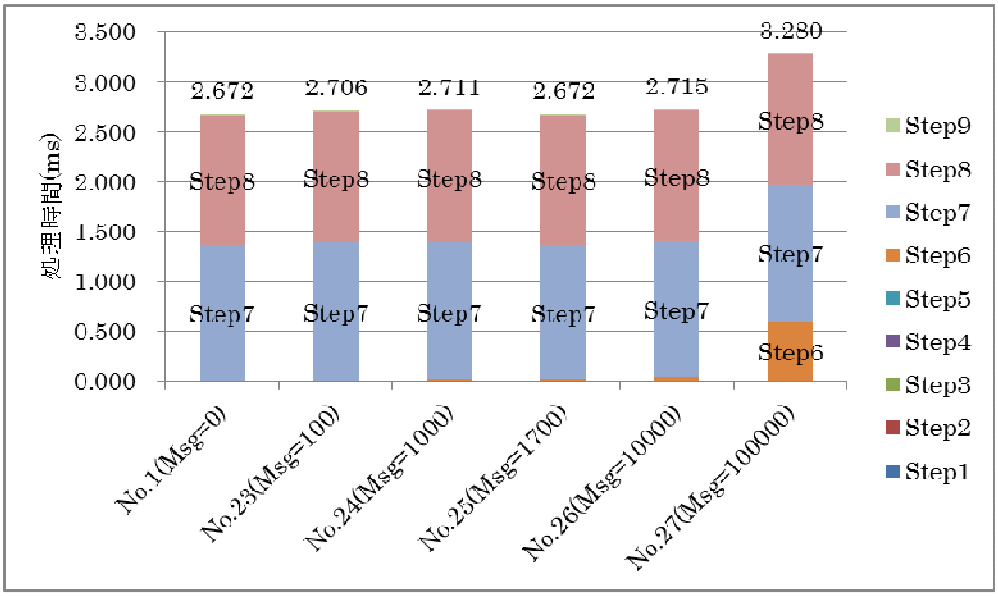


図 3.3.1-16　No.23～27 の測定結果

検証済みメッセージの数が 1 万以下まで（No.1, No.23～26）であれば全体の検証処理時間はほぼ変化がないことが分かった。ただし、10 万まで増やす（No.27）と、Step6（リプレイ攻撃検査）の処理時間が長くなり、全体の検証処理時間も 3.28ms まで伸びることが分かった。

図 3.3.1-17 は、図 3.3.1-16 の結果から Step6（リプレイ攻撃検査）の処理を抜き出したものである。

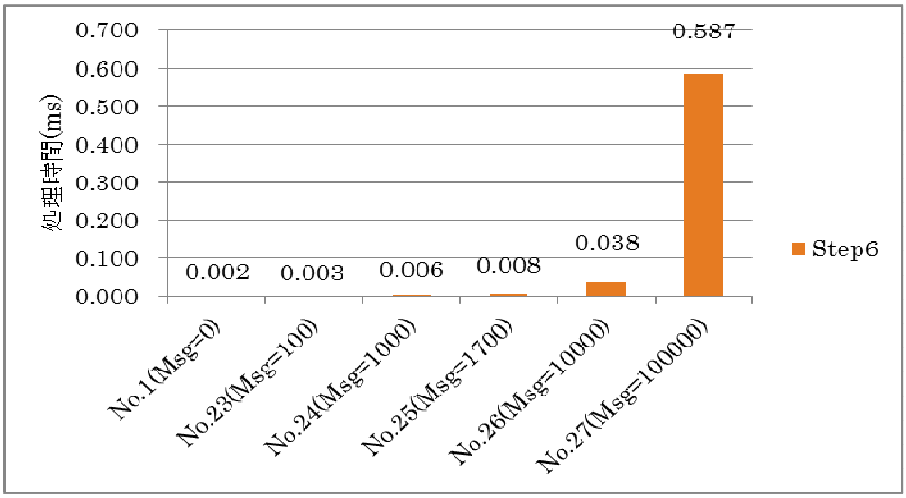


図 3.3.1-17　No.23～27 の結果から抜き出した Step6 の処理時間

(e)メッセージ数の数を増やせば Step6（リプレイ攻撃検査）の処理時間も増加していき、10 万まで増やすと（No.27）、0 の時（No.1）と比べて 0.58ms 以上の差となって影響が大きいが、取り得る値として想定している 1,700 まで（No.23～25）であれば全体の検証処理に大きな影響は及ぼさないことが分かった。

しかしながら、(b) EE 証明書数と同様に、車載システム上での処理時間を考えた場合にはその影響がやや大きくなってくる可能性が懸念される。

⑦ メッセージの検証処理時間が最短となる条件での検証結果

これまでの測定では、前提として内部で保持した検証済みの EE 証明書や Sub CA 証明書とは合致しない署名付きメッセージを受信したケースの検証処理時間を測定した。そのため、常に Step7（証明書の署名検証）で証明書の署名検証が発生している。しかしながら、実環境においては、検証済みの EE 証明書や Sub CA 証明書を内部で保持しておくことで Step7（証明書の署名検証）の処理を省略できるケースも存在する。

これまで見てきたとおり、Step7（証明書の署名検証）は少なくとも約 1.3ms ほどの処理時間がかかるため、この処理が省略できた場合にはメッセージの検証処理時間は大幅に短縮が見込める。

そこで、メッセージの検証処理時間が最短となると推測されるテスト条件での測定を実施した。測定条件を表 3.3.1-6 に示す。

表 3.3.1-6　最短となる測定条件

No	パラメータ					備考
	(a)	(b)	(c)	(d)	(e)	
28	2	1	0	0	0	キャッシュした EE 証明書に合致するメッセージを受信

(b) EE 証明書数を 1 とし、かつ、その EE 証明書と合致する署名付きメッセージを受信したというテスト条件である。

その結果を図 3.3.1-18 に示す。

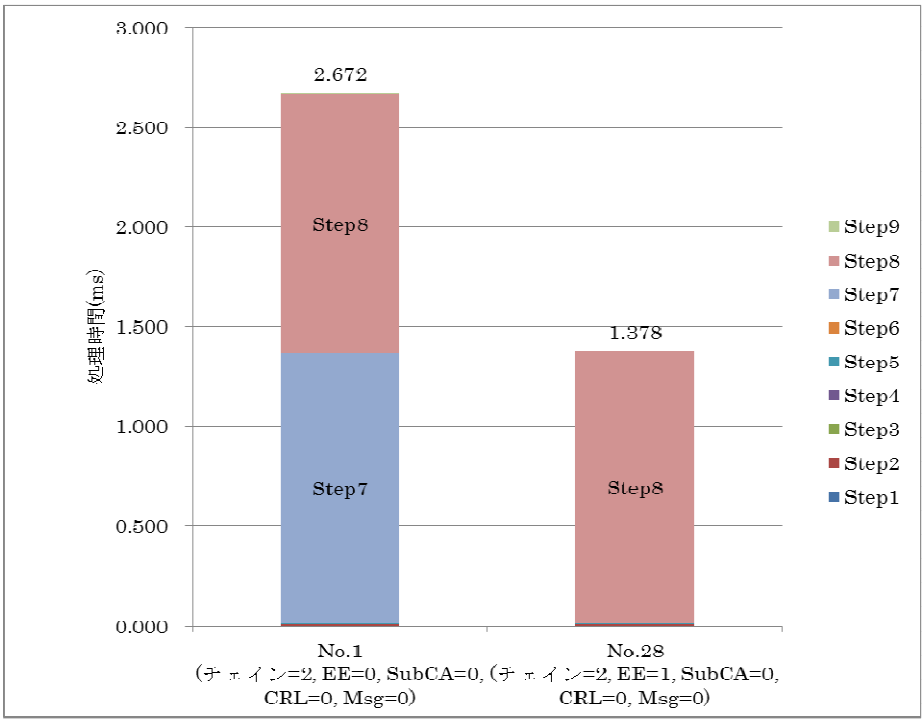


図 3.3.1-18　No.28 の測定結果

No.28 では、Step7（証明書の署名検証）の処理時間がほぼ無くなった結果、No.1 と比べて全体の検証処理時間は約 1.3ms 短縮され、1.378ms となった。

(8) 考察

① 目標とする処理性能

実世界の車載システムで想定される 1 秒間あたりのメッセージ受信数を、欧州の研究事例[2]から 1,000 メッセージ/秒と仮定すると、すべてのメッセージを処理するためには 1 メッセージあたり 1ms 以内に処理する必要がある。

② V2X 通信のメッセージ検証の処理性能予測

今回の測定は 3.6GHz の PC 上で行ったが、実際の車載システムには PC ほどの高性能な CPU は搭載されていないことが一般的である。

ここでは、CPU のクロック数から車載システム上での検証処理時間の概算を行うこととした。

車載システムで使用する CPU を仮に 160MHz とすると、今回の測定で使用した PC の CPU とは約 22.5 倍の性能差があることになる。

PC 上での No.1（チェイン=2、EE=0、SubCA=0、CRL=0、Msg=0）の測定結果は 2.672ms であった。また、最短条件の No.28（チェイン=2、EE=1、SubCA=0、CRL=0、Msg=0 で、EE 証明書のキャッシュにヒット）でも 1.378ms であった。

これらを 22.5 倍して実際の車載システム上に換算すると、No.1 は 60.12ms、No.28 は約 31.01ms かかることがそれぞれ予想され、目標とする 1 メッセージあたり 1ms には大幅に届かないことが分かった。

③ 暗号 HW を利用した場合の処理性能予想

IEEE1609.2 の署名検証ではアルゴリズムに ECDSA（楕円曲線 DSA：Elliptic Curve Digital Signature Algorithm[7]）を使用している。Step7（証明書の署名検証）および Step8（メッセージの署名検証）の処理時間が長くなるのは、この ECDSA の処理時間が影響している。そこで、署名付きメッセージの検証処理時間を短縮させる方法の一つとして、暗号 HW を使用する方法が考えられる。

ここでは、署名検証暗号 HW で行った場合に全体の検証処理時間がどれほど短縮できるかについて、研究事例[8]を参考に試算を行う。この研究事例では、楕円曲線におけるスカラー倍算（楕円スカラー倍算）に関し、動作周波数が 291MHz の HW を用いて 0.38ms で処理できることが報告されている。便宜上、ECDSA の署名検証の処理時間を、支配的な処理である楕円スカラー倍算のみに着目して試算した。ECDSA の署名検証では楕円スカラー倍算が 2 回行われるので、

0.38ms×2×(291MHz/160MHz)=約 1.38ms（式 1）

となる。なお、ここでは、暗号 HW の動作周波数はマイコンの動作周波数と同じ、かつ、その処理時間は動作周波数に比例するものとしている。

また、3.3.1(7) 測定結果”で見たとおり、Step7（証明書の署名検証）と Step8（メッセージの署名検証）で合わせて約 2.65ms の処理時間がかかっている。これは署名検証を暗号 SW（OpenSSL ECDSA NIST p256）を用いて実施した結果である。この結果を基に車載システム上での処理時間の予想値を計算すると、Step7（証明書の署名検証）と Step8（メッセージの署名検証）で合わせて 59.63ms となる。

署名検証は Step7（証明書の署名検証）と Step8（メッセージの署名検証）の 2 回あるた

め、暗号 HW を利用した場合、車載システム上での全体の署名付きメッセージ検証処理時間は、基準の No.1（チェイン=2、EE=0、SubCA=0、CRL=0、Msg=0）で考えると、

60.12ms – 59.63ms + 1.38ms×2 = 3.25 ms（式 2）

まで短縮することが期待できる。従って、1 秒間に処理可能なメッセージは約 307 メッセージであり、1 秒間に 1,000 メッセージを処理するという目標性能に対しては約 30%の達成度となる。

次に、最短条件の No.28（チェイン=2、EE=1、SubCA=0、CRL=0、Msg=0 で、EE 証明書のキャッシュにヒット）については、PC 上での測定値が 1.378ms であり、うち、Step8（メッセージの署名検証）が 1.362ms であったため、車載システム上で暗号 HW を利用した場合を考えると 1.74ms となる。1 秒間に処理可能なメッセージは約 574 メッセージであり、1 秒間に 1,000 メッセージを処理するという目標性能に対しては約 57%の達成度となる。

以上の内容を表 3.3.1-7 にまとめた。

表 3.3.1-7　IEEE1609.2 仕様のメッセージ検証処理時間のまとめ

No	測定条件	（Ⅰ） PC 上で実測した処理時間	（Ⅱ） 車載システムに換算した処理時間（暗号 SW 使用時）	（Ⅲ） 車載システムに換算した処理時間（暗号 HW 使用時）	（Ⅳ） （Ⅲ）における目標性能に対する達成度
1	チェイン=2、EE=0、SubCA=0、CRL=0、Msg=0	2.672ms	60.12ms	3.25 ms	約 30%
28	チェイン=2、EE=1、SubCA=0、CRL=0、Msg=0 で、EE 証明書のキャッシュにヒット	1.378ms	31.01ms	1.74ms	約 57%

車載システム上であっても、暗号 HW を使用することで PC での実測値に近い処理時間の実現が見込める。

しかしながら、それでも No.1、No.28 共に目標性能に対して未達となる。

また、暗号 HW を搭載した場合はその分コストが増加することとなるため、如何に高性能で安価な暗号 HW を採用できるかという新たな課題も発生することが分かった。

④ V2X 通信のセキュリティ処理におけるボトルネック

これまでの測定結果および考察を踏まえると、署名付きメッセージの検証処理時間のオーバヘッドとなり得る内部処理、パラメータは以下の 5 点である。

・署名検証(Step7（証明書の署名検証）および Step8（メッセージの署名検証）の処理)

・(a)チェイン数
・(b)EE 証明書数
・(d)CRL 数
・(e)メッセージ数

まず、Step7（証明書の署名検証）および Step8（メッセージの署名検証）の署名検証を併せた処理時間を見ると、車載システム上での処理時間予測では、暗号 HW を使用せずソフト暗号で計算を行った場合には 59.63ms となる。暗号 HW を使用した場合は 2.76ms まで短縮が見込め、大きな効果を得られる。しかしながら、それでも Step7（証明書の署名検証）および Step8（メッセージの署名検証）の署名検証処理だけで目標とする 1 メッセージあたり 1ms を超えてしまうことが分かった。一度検証済みとなった EE 証明書や Sub CA 証明書をキャッシュとして保持することで、その EE 証明書や Sub CA 証明書の次回以降の Step7（証明書の署名検証）を省略することができるが、その場合でも Step8（メッセージの署名検証）は省略できず、Step8（メッセージの署名検証）のみでも 1.38ms かかるため、やはり目標に対して未達となる。

(a) チェイン数については、チェインを増やすとその分 Step7（証明書の署名検証）の証明書の署名検証が増えるため、チェインが 1 段増えるごとに PC の測定環境上で約 1.4ms、車載システムに換算すると約 31.5ms の増加となる。ただし、これはチェインに含まれた Sub CA 証明書を全て検証した場合の処理時間である。Sub CA 証明書を予め車載システム内部に保存、あるいは一度検証済みとなった Sub CA 証明書をキャッシュとして保持することで、その Sub CA 証明書の署名検証を省略することができる。その場合、(a)チェイン数は署名付きメッセージの検証処理時間における大きなオーバヘッドでは無くなる。

(d) CRL 数については、1 エントリあたりの処理時間は軽微であり、エントリ数を少なく抑えることができればボトルネックとはならないことが確認された。しかしながら、取り得る値としては日本国内においても年間の廃車台数から 500 万件と想定しており、その場合には、全体の検証処理時間は PC 上でも約 12ms、車載システムに換算すると約 270ms になることが分かった。米国における年間の廃車台数（販売台数と同等と仮定）は 1,600 万件であり単純計算でもさらに 3 倍以上の処理時間となると考えられる。いずれにしても、CRL 数は署名付きメッセージの検証処理において大きなオーバヘッドとなることが予想される。

(b) EE 証明書数と(e) メッセージ数については、取り得る値として想定した 1,700 の場合、PC 上での処理時間としてはそれぞれ約 0.015ms、約 0.006ms ほどの増加であり、その影響は軽微に見えた。しかしながら、車載システム上に換算するとそれぞれ約 0.338ms、約 0.135ms となり、併せると約 0.473ms の増加となる。依然として署名検証や(d) CRL 数と比べると小さな値ではあるものの、目標とする 1 メッセージあたり 1ms に対しての影響は大きいことが分かった。

3.3.2　V2X 通信における署名検証の簡略化方式の調査

V2X 通信については米国、欧州でもそれぞれに検討が進められている。そこで、V2X 通信における署名検証の簡略化方式を検討するにあたり、米国、欧州で検討されている簡略化方式についての調査を行った。

(1) 米国仕様における簡略化

① 米国仕様における簡略化の概要

米国の V2X 通信仕様は USDOT Security Credential Management System Design[3]に規定されている。通信メッセージや管理仕様は IEEE1609.2 をベースにしているが、トラッキング防止のため証明書を 5 分毎に切り替える点が特徴的である。そのため 1 台の車両に対して大量の証明書を発行することとなり、そのままでは CRL のエントリ数も膨大な数が必要となってしまう。これを防ぐため、米国仕様では CRL の取り扱い方法が工夫されている。具体的には、CRL のエントリは車両に対して 1 つのみとし、失効した証明書の ID はその 1 つのエントリから算出する。それにより、CRL のエントリ数が膨れ上がって証明書の失効確認処理に長時間を要してしまう事態を回避している。

また、米国仕様では Sub CA を設けず、証明書チェインは EE と Root CA の 2 段である。それにより、証明書チェインの構築処理や証明書の署名検証の処理時間を短く抑えることができる。

まとめると、米国仕様における署名検証の簡略化ポイントとしては以下の 2 点が挙げられる。

・CRL のエントリは車両に対して 1 つのみ。
・証明書チェインが 2 段。

② 米国仕様固有の内部処理

米国仕様での署名付きメッセージ検証処理を細分化したフロー図を図 3.3.2-1 に示す。

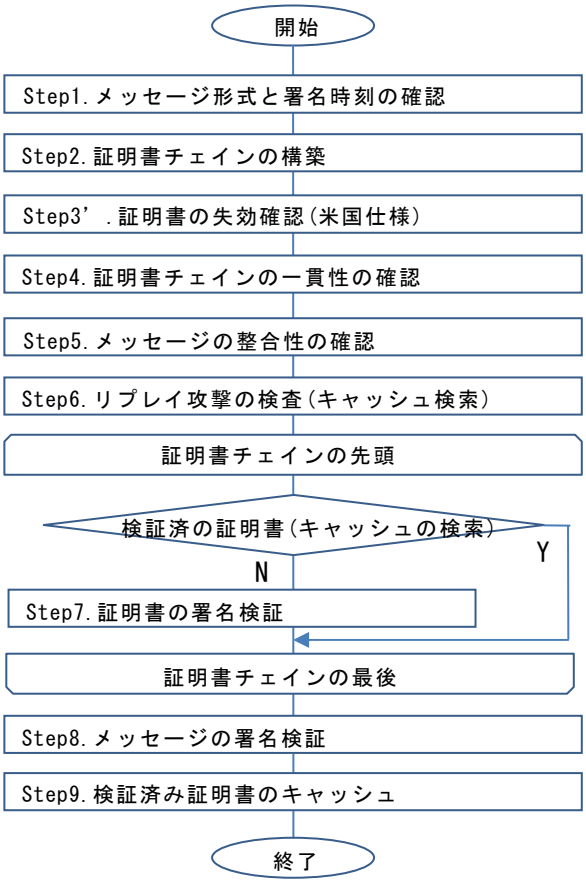


図 3.3.2-1　米国仕様の署名付きメッセージの検証処理フロー

各 Step の処理内容の詳細について表 3.3.2-1 に示す。

米国仕様固有の内部処理としては、図 3.3.1-4 の Step3(失効確認)に代わる処理として、Step3’（米国仕様の失効確認）が存在する。その他の Step については図 3.3.1-4 に示した IEEE1609.2 における検証処理と同一である。

表 3.3.2-1　各 Step の処理内容の詳細

Step	処理の詳細
Step1 （形式と時刻の確認）	メッセージのコンテントタイプが署名付きメッセージを示す値であるかを確認する。また、メッセージの有効期限が過ぎていないか、生成時刻と有効期限の時系列が不正でないかを確認する。
Step2 （チェイン構築）	メッセージ内および機器内に格納されている証明書を用いて、メッセージ内の最初の証明書から Root 証明書までのパスを構築する。
Step3’ （米国仕様の失効確認）	CRL のエントリから失効した一連の証明書の ID を算出し、その値を基に失効確認を行う。より具体的には、CRL のエントリを例えば 1 日単位等で定期的に再計算し、その再計算結果を用いてその定期期間内に使用される一連の証明書の ID を 1 つ 1 つ算出する。ID の算出には SHA-256 と AES が用いられる。
Step4 （チェインの一貫性確認）	パスを構築した証明書チェインの証明書に記載されている有効期限や有効範囲等について証明書間の一貫性を確認する。
Step5 （メッセージの整合性確認）	メッセージについて、メッセージ中に格納された生成時刻、有効期限、位置情報等と証明書の有効期限や有効範囲等からその整合性を確認する。
Step6 （リプレイ攻撃検査）	リプレイ攻撃への対処のため、過去に受信したメッセージ情報のキャッシュを検索し、同じメッセージを既に受信済みでないかを確認する。受信済みでない場合は検索終了後に当該メッセージ情報をキャッシュへ登録する。
Step7 （証明書の署名検証）	検証済みの証明書情報のキャッシュを検索し、存在しない場合は証明書の署名検証を行う。
Step8 （メッセージの署名検証）	メッセージの署名検証を行う。
Step9 （証明書のキャッシュ）	検証の済んだ証明書情報を機器内のキャッシュに保持する。

③ 米国仕様固有の内部処理に影響を及ぼすパラメータ

米国仕様固有の内部処理である Step3’（米国仕様の失効確認）に影響を及ぼすパラメータとしては、

・CRL 数

が挙げられる。

CRL のエントリ毎にその値から証明書の ID を再計算する必要があるためである。

また、その証明書の ID の再計算タイミングによっても処理時間は影響を受ける。署名付きメッセージの検証処理時間を短くするためには、事前に 1 日分等のまとまった単位の ID を全て計算しておくことが効果的であるが、その分、結果を保持する不揮発等の記憶領域が必要となる。米国方式では証明書を 5 分で切り替えるため、1 日単位で行う場合には 1 エントリにつき 288 個の ID の計算が必要となり、計算結果も膨大なサイズとなる。一方、署名付きメッセージの検証処理の中で都度計算を行う場合、不揮発等の記憶領域は

不要になるが、一方で、全体の検証処理時間の増加につながることが分かった。

④ Verify-on-Demand

IEEE1609.2 や米国仕様の署名付きメッセージ検証処理では、図 3.3.2-2 に示すとおり、受信した全てのメッセージについて、まずそのメッセージ署名検証を行う。そして、検証できたメッセージに対してのみ、重要度の判定等、メッセージの内容を解析する。

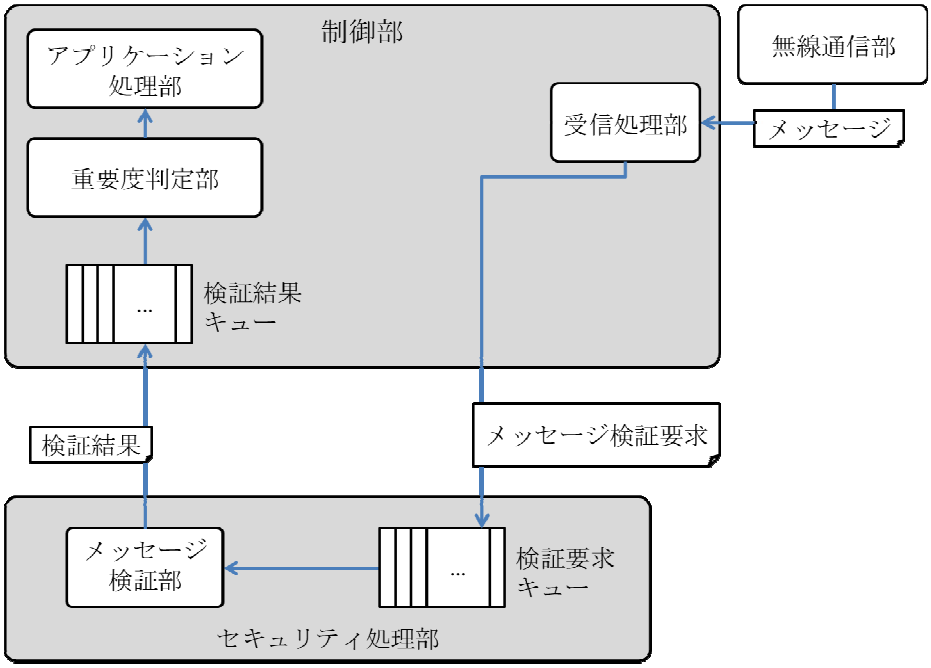


図 3.3.2-2　従来の処理フロー

しかしながら、このメッセージ検証処理には多くの処理時間を要する。そこで、米国において Verify-on-Demand[9]という方式も提案されている。

Verify-on-Demand では、図 3.3.2-3 に示すとおり、まず先にメッセージの内容を見て重要度を判定し、重要度の高いメッセージについてのみメッセージ検証処理を行う。重要度の判定では、例えばユーザーに警告通知を行ったり安全運転制御を動作させたりする必要のあるメッセージかどうかを判断基準とする。これにより、大量のメッセージを受信する環境であっても、重要なメッセージを迅速に処理することが可能となる。

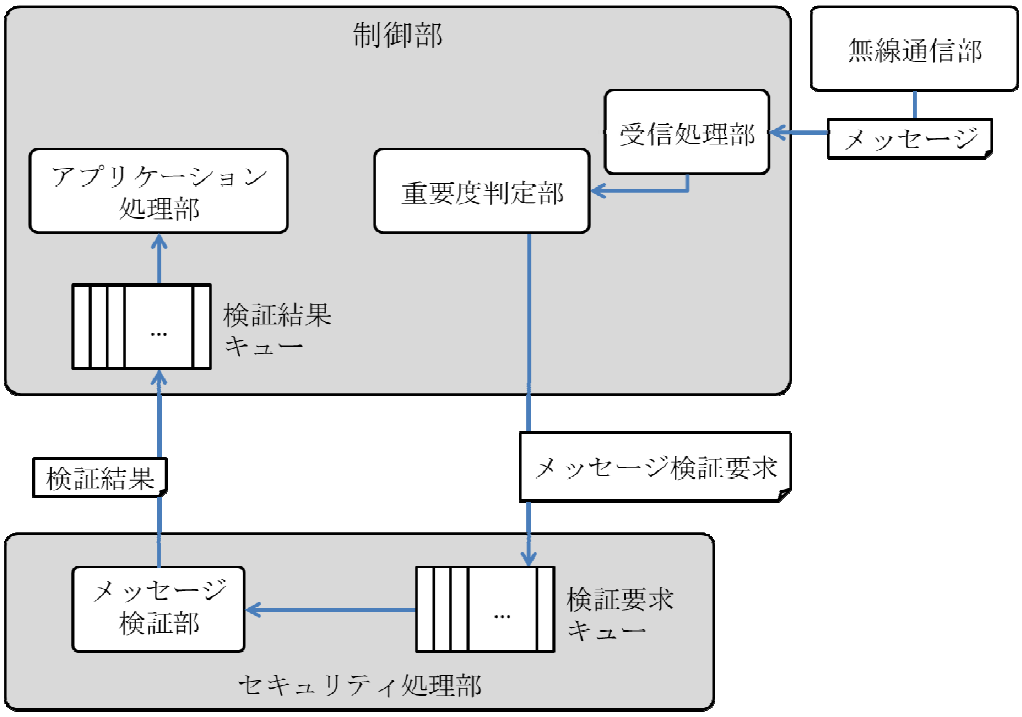


図 3.3.2-3　Verify-on-Demand の処理フロー

(2) 欧州仕様における簡略化

① 欧州仕様における簡略化の概要

欧州の V2X 通信仕様は ETSI（European Telecommunications Standards Institute）にて検討されており、そのメッセージフォーマットは ETSI TS 103 097[10]で規定されている。このフォーマットは IEEE1609.2 の 1609Dot2Data を元に作成されているが，内部の構造は 1609Dot2Data とは大きく異なっている。

欧州のプロジェクト[4]によると、CRL の大規模な配布は困難と予想されることから CRL を使用しない。また、証明書チェインは EE と Root CA、そして Sub CA に相当する Pseudonym CA の 3 段である。

その外、欧州仕様[11]ではリプレイ攻撃検査を行わない。

まとめると、欧州仕様（欧州プロジェクトを含む）における署名検証の簡略化ポイントとしては以下の 3 点が挙げられる。

・CRL を使用しない
・証明書チェインが 3 段
・リプレイ攻撃検査を行わない

② 欧州仕様固有の内部処理

欧州仕様での署名付きメッセージ検証処理を細分化したフロー図を図 3.3.2-4 に示す。

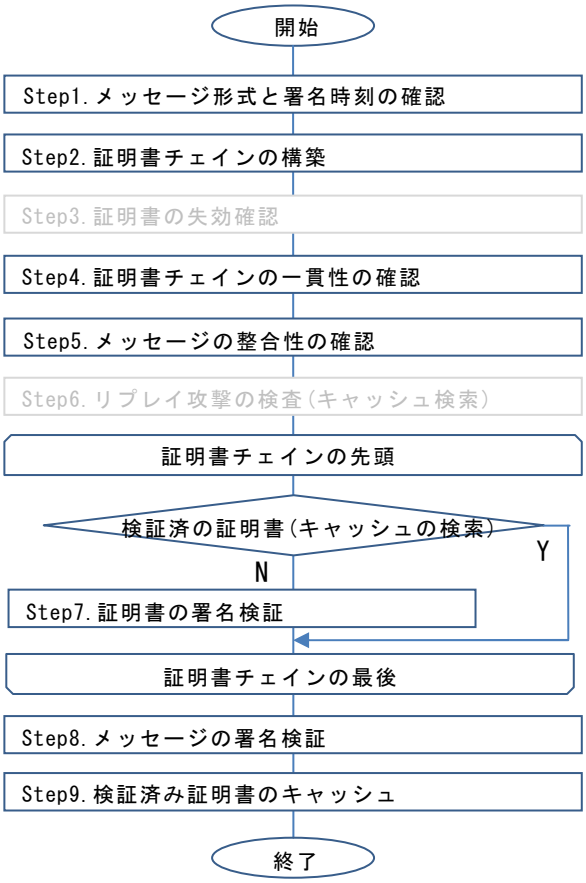


図 3.3.2-4　欧州仕様の署名付きメッセージの検証処理フロー

欧州仕様については固有の内部処理は存在しない。CRL 検証とリプレイ攻撃検査を行わないため、Step3（失効確認）および Step6（リプレイ攻撃検査）が存在しない点が特徴である。その他の Step については図 3.3.1-4 に示した IEEE1609.2 の検証処理と同一である。

③ 欧州仕様固有の内部処理に影響を及ぼすパラメータ

欧州仕様については固有の内部処理は存在しないため、固有の内部処理に影響を及ぼすパラメータも存在しない。(d) CRL 数および(e)メッセージ数が 0 固定となる点が特徴である。

3.3.3 署名検証の簡略化方式の評価と分析

(1) 各簡略化方式のリアルタイム性の評価

① 米国の失効確認仕様における V2X 通信のメッセージ検証の処理性能予測

米国仕様における証明書の失効確認仕様に基づいて実装されたプログラム用いて、署名付きメッセージの検証処理時間の測定を行った。

測定環境および測定方法は 3.3.1(6)測定環境と同一である。測定条件としては、Step3’（米国仕様の失効確認）に対する（d）CRL 数の影響を検証するため、表 3.3.3-1 に示す測定条件を設定した。各パラメータの値は 3.3.1(6)測定環境における No.16～22 と同一である。

今回も、米国における CRL 数として想定している 1,600 万（No.35）については測定環境の処理性能上、測定を行うことができないため、日本国内の想定値である 500 万を測定条件とする No.34 の結果から予想値を算出することとした。

表 3.3.3-1　米国仕様の測定条件

No	パラメータ					備考
	（a）	（b）	（c）	（d）	（e）	
29	2	0	0	100	0	（d）CRL 数の影響検証
30	2	0	0	1,000	0	
31	2	0	0	10,000	0	
32	2	0	0	100,000	0	
33	2	0	0	420,000	0	
34	2	0	0	5,000,000	0	
*35	2	0	0	16,000,000	0	*測定不可

なお、今回の測定では、CRL のエントリの再計算は事前に実施しておき、その値を基に個々の証明書の ID を算出する処理を Step3’（米国仕様の失効確認）の中で都度実施した。

(d) CRL 数の影響を検証した No.29～34 の結果を以下に示す（図 3.3.3-1）。

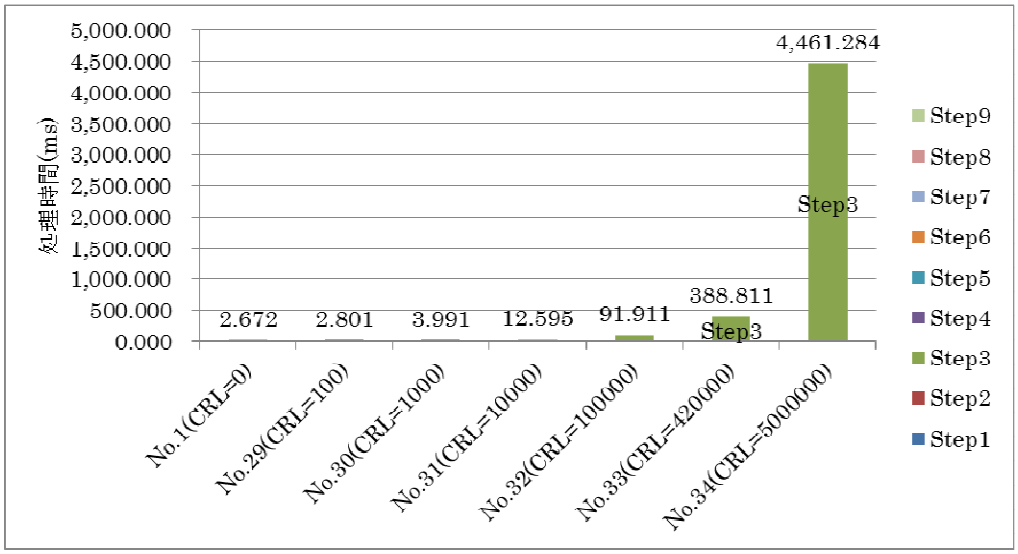


図 3.3.3-1　No.29～34 の測定結果

CRL のエントリ数（CRL 数）を増やすとその分 Step3’（米国仕様の失効確認）の処理時間が大幅に増加し、全体の検証処理時間も膨大となることが分かった。42 万（No.33）で約 388ms、500 万（No.34）では約 4,461ms という結果であった。今回測定を行えなかった 1,600 万のケース（No.35）での全体の検証処理時間は、No.34 の 3 倍以上で約 14,275ms となるものと予想される。

CRL 数の比較的少ないテスト条件である No.29（100）～No.31（1 万）までに絞ってグラフ化した結果も以下に示す。（図 3.3.3-2）

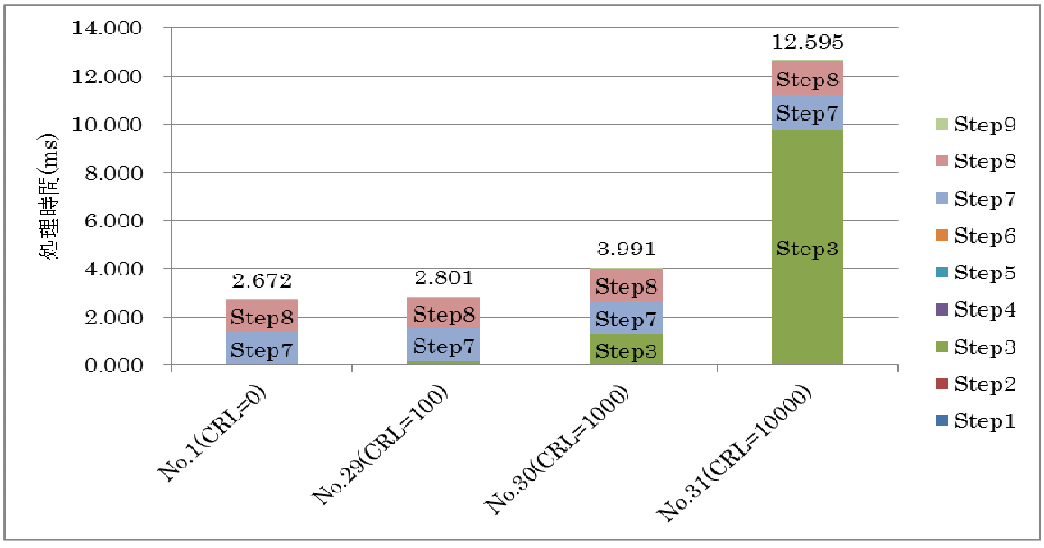


図 3.3.3-2　No.29～31 の測定結果のみを抽出

図 3.3.3-2 からもやはり、CRL 数を増やすと Step3’（米国仕様の失効確認）の処理時間が増加していくことが確認できた。

No.29～No.31 の各結果から 1CRL あたりの Step3’（米国仕様の失効確認）の処理時間を

算出すると、凡そ 0.0009ms（=900ns）であった。一方、3.3.1(6)測定環境の No.16～21 の結果から 1 エントリあたりの Step3（失効確認）の処理時間を算出すると、凡そ 0.000006ms（=6ns）であった。つまり、Step3’（米国仕様の失効確認）は、証明書の ID の計算なしで検索する Step3（失効確認）と比べて 150 倍長くかかることが分かった。しかしながら、米国仕様は 5 分毎に証明書を切り替えるため車両 1 台につき 1 日だけでも 288 個の証明書を必要とする。従って、Step3（失効確認）の方式で単純に 288 個の証明書それぞれに対応した CRL を持つよりも、Step3’（米国仕様の失効確認）は確かに処理時間の簡略化を見込めることが分かった。

結論として、Step3’（米国仕様の失効確認）は、あくまでもトラッキング防止のための米国独自仕様に伴う負荷を軽減することを目的としたものであり、元々のメッセージ検証処理を軽減するものではなかった。

米国仕様の署名付きメッセージの検証処理時間は CRL 数に大きく依存するが、仮に CRL 数を少なく抑えることができて 1,000 のみであったとしても、図 3.3.3-1 の No.30（チェイン=2、EE=0、SubCA=0、CRL=1,000、Msg=0）の結果から測定 PC 上の数値として 3.991ms、車載システム上では約 89.80ms という長い時間を要することが分かった。署名検証を暗号 HW で実施したとしても、約 31.02ms ほどかかる見込みである。1 秒間に処理可能なメッセージは約 32 メッセージであり、1 秒間に 1,000 メッセージを処理するという目標性能に対しては約 3%の達成度となる。

以上の内容を表 3.3.3-2 にまとめた。

表 3.3.3-2　米国仕様のメッセージ検証処理時間のまとめ

No	測定条件	（Ⅰ）PC 上で実測した処理時間	（Ⅱ）車載システムに換算した処理時間（暗号 SW 使用時）	（Ⅲ）車載システムに換算した処理時間（暗号 HW 使用時）	（Ⅳ）（Ⅲ）における目標性能に対する達成度
30	チェイン=2、EE=0、SubCA=0、CRL=1,000、Msg=0	3.991ms	89.80ms	**31.02ms**	**約 3%**

CRL 数を取り得る値として想定した 500 万や 1,600 万から大幅に削減して 1,000 程度に抑える運用が行えたとして、それでも目標性能に対する達成度としては 3%程度となることが分かった。

米国仕様においては Step3’（米国仕様の失効確認）の処理負荷が極めて大きく、ここを如何に短縮するかが重要となってくる。

例えば、今回の測定では CRL のエントリの再計算は事前に実施しているが、その値を基に個々の証明書の ID を算出する処理は Step3’（米国仕様の失効確認）の中で都度実施した。個々の証明書の ID の算出も事前に実施しておくことで、Step3’（米国仕様の失効確認）の処理時間を短縮することができる。

あるいは、個々の証明書の ID の算出には AES が用いられており、今回の測定ではこの

処理を暗号 SW（OpenSSL）で実施したが、ここを暗号 HW に置き換えることでも Step3’（米国仕様の失効確認）の処理時間の短縮が見込めることが分かった。

② 欧州仕様における V2X 通信のメッセージ検証の処理性能予測

欧州仕様における署名付きメッセージの検証処理時間は、証明書チェインが 3 段、かつ、CRL とメッセージのキャッシュが無いという特徴から、図 3.3.1-6 に示した No.2（(a) チェイン数=3 段、(b)EE 証明書数～(e)メッセージ数=0）の結果とほぼ同等になると考えられる。No.2 の全体の検証処理時間は PC 上の測定で 4.092ms であり、うち、Step7（証明書の署名検証）と Step8（メッセージの署名検証）を合わせた処理時間は、約 4.070ms であった。従って、実際の車載システム上で暗号 HW を使用した場合に換算すると、

(4.092ms - 4.070ms) ×22.5 + 1.38ms×3 = 約 4.16ms（式 3）

となる。1 秒間に処理可能なメッセージは約 240 メッセージであり、1 秒間に 1,000 メッセージを処理するという目標性能に対しては約 24%の達成度となる。

欧州仕様では Step3（失効確認）および Step6（リプレイ攻撃検査）が不要なため処理が簡略化されるが、一方で、(a) チェイン数が 3 段であるため、その分、Step7（証明書の署名検証）に処理時間を要する結果となる。

やはり欧州仕様でも目標性能に対して未達となることが分かった。

なお、欧州仕様に関しても、一度検証済みとなった EE 証明書や Sub CA 証明書をキャッシュとして保持することで、その EE 証明書や Sub CA 証明書の次回以降の Step7（証明書の署名検証）を省略することが可能である。

そこで、欧州仕様においてメッセージの検証処理時間が最短になるテスト条件での測定を行った。測定条件を表 3.3.3-3 に示す。

表 3.3.3-3　欧州仕様で最短となる測定条件

No	パラメータ					備考
	(a)	(b)	(c)	(d)	(e)	
36	3	1	1	0	0	キャッシュした EE 証明書および Sub CA 証明書に合致するメッセージを受信

これは(b) EE 証明書数および(c) Sub CA 証明書数を 1 とし、かつ、その EE 証明書および Sub CA 証明書と合致する署名付きメッセージを受信したというテスト条件である。

測定環境および測定方法は 3.3.1(6)測定環境と同一であり、結果を図 3.3.3-3 に示す。

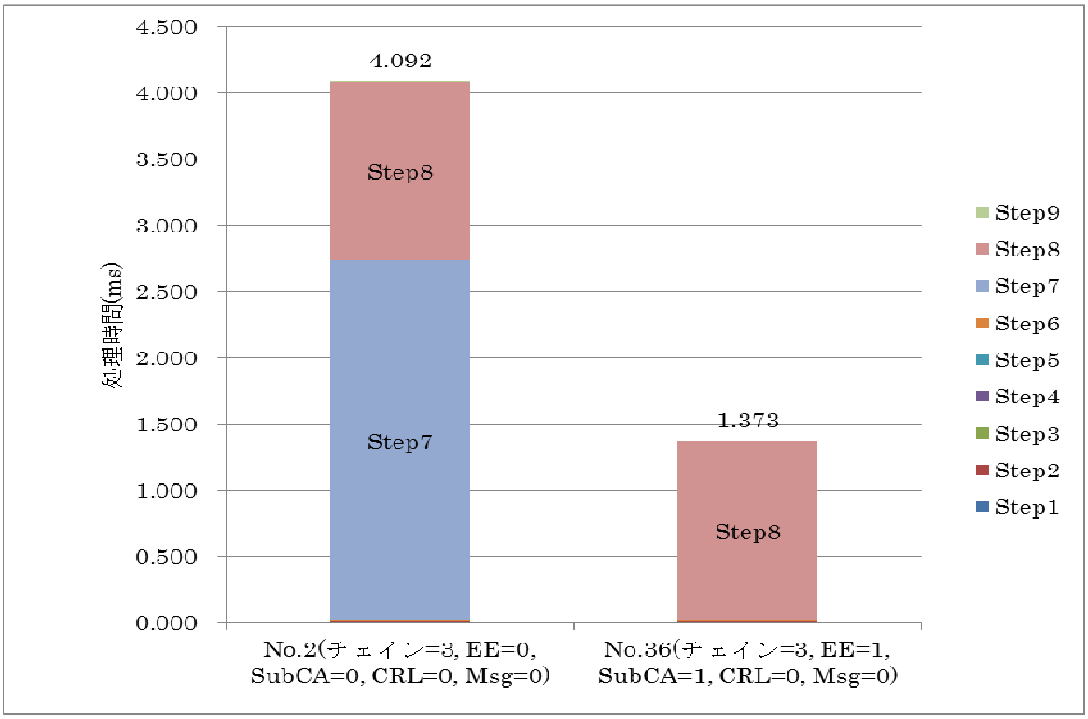


図 3.3.3-3　No.36 の測定結果

No.36 では、Step7（証明書の署名検証）の処理時間がほぼ無くなったため、No.2 と比べて全体の検証処理時間が約 2.7ms 短縮された。

No.36 の全体の検証処理時間は 1.373ms であり、うち、Step8（メッセージの署名検証）の処理時間は 1.355ms であった。この結果を車載システムで暗号 HW を使用した場合に換算すると、

(1.373ms - 1.355ms) ×22.5 + 1.38ms = 約 1.78ms（式 4）

となる見込みである。この場合、1 秒間に処理可能なメッセージは約 561 メッセージであり、1 秒間に 1,000 メッセージを処理するという目標性能に対しては約 56%の達成度となった。

以上の内容を表 3.3.3-4 にまとめた。

表 3.3.3-4　欧州仕様のメッセージ検証処理時間のまとめ

No	測定条件	（Ⅰ） PC 上で実測した処理時間	（Ⅱ） 車載システムに換算した処理時間（暗号 SW 使用時）	（Ⅲ） 車載システムに換算した処理時間（暗号 HW 使用時）	（Ⅳ） （Ⅲ）における目標性能に対する達成度
2	チェイン=3、EE=0、SubCA=0、CRL=0、Msg=0	4.092ms	92.07ms	**4.16ms**	**約 24%**
36	チェイン=3、EE=1、SubCA=1、CRL=0、Msg=0 で、EE 証明書と SubCA 証明書のキャッシュにヒット	1.373ms	30.89ms	**1.78 ms**	**約 56%**

車載システム上で暗号 HW を使用した場合であっても、欧州仕様では目標性能に対して未達となる。

また、全てのメッセージで Step7（証明書の署名検証）をスキップできるものではなく、受信したメッセージごとに No.2 の処理時間となるケースや No.36 の処理時間となるケースが混在すると考えられる。

③ Verify-on-Demand における V2X 通信のメッセージ検証の処理性能予測

Verify-on-Demand は米国で提案された方法であるが、米国仕様のメッセージ検証処理のみではなく、IEEE1609.2 や欧州仕様に対しても適用可能である。

ここでは、欧州研究事例[2]の想定する環境を用いて Verify-on-Demand によるメッセージ検証の削減効果を考察した。本節で想定する環境と Verify-on-Demand による検証要否の判定方法は次のとおりである。

・想定する環境

- ✧ 高速道路片側 3 車線
- ✧ 通信範囲に存在する車両：150 台
- ✧ 100km/時間
- ✧ 車両密度：2600 台/レーン・時間
- ✧ 送信周期：10Hz（メッセージの位置情報を Verify-on-Demand で利用可能）

・Verify-on-Demand による検証要否の判定方法

a. 半径 300m 以内に存在する車両のメッセージのみを検証する[12]

b. 同一方向の車線に存在する車両のメッセージのみを検証する
（反対車線の車両のメッセージは検証しない）

Verify-on-Demand による削減後の 1 秒あたりのメッセージ検証数は a. では 940[*1]、b. では 750[*2] となる。つまり、a. では 1 秒間に受信した 1,000 メッセージ中、940 メッセージを検証すればよく、残りの 60 メッセージは破棄できる。同様に b.では 1,000 メッセージ中 250 メッセージを破棄できる。

また、同一方向の車両には変化は無いと仮定すると、a. では新たに通信範囲に入る（証明書が未検証の）反対車線の車両を考慮しなければならない。その台数は 1 秒間あたり約 5 台[*3] である。つまり a. では 940 メッセージ中 935 メッセージはメッセージの署名検証のみで済み、残りの 5 メッセージは証明書の署名検証も行うことを意味する。

一方、同一方向の車両には変化は無いと仮定すると、b. では 750 メッセージの全てがメッセージの署名検証のみで済む。

ここで、IEEE1609.2 における処理時間である表 3.3.1-7 の値を用いて処理性能を試算した。メッセージの署名検証のみで済む場合のメッセージ検証処理時間を No.28（チェイン=2、EE=1、SubCA=0、CRL=0、Msg=0 で、EE 証明書のキャッシュにヒット）の結果である 1.74ms、証明書の署名検証も行う場合のメッセージ検証処理時間を No.1（チェイン=2、EE=0、SubCA=0、CRL=0、Msg=0）の結果から 3.25ms とする。その場合、a.は 1 秒間に処理できるメッセージ数は約 570 メッセージ[*4] となり、目標性能に対して約 63%[*5] の達成度となる。また、b. は 1 秒間に処理できるメッセージ数は約 574 メッセージであり、目標性能に対して約 82%の達成度となる。

＊1：半径（高速道路上では前後）300m 以内に存在する車両数は、

(2600[台/レーン・h]/ 100[km/h])×((0.3[km] + 0.3[km])×6[レーン]) ≒ 94[台]（式 5）

であり、1 秒あたりのメッセージ検証数は、

94[台]×10[メッセージ/台・秒] = 940[メッセージ/秒]（式 6）

である。

＊2：車両密度が均一とすると、反対車線の車両数は通信する車両の全体の半数であるため半数の車両を無視できる。よって 1 秒あたりのメッセージ検証数は、

(150/2[台])×10[メッセージ/台・秒] =750[メッセージ/秒]（式 7）

である。

＊3：自車両と反対車線の車両は互いに同じ速度で近づいているので、相対的に倍の車両密度となる。つまり 1 秒間に通信範囲に入る車両は

(2600[台/レーン・時間])×(2/3600[時間]×3[レーン]) ≒ 5[台]（式 8）

である。

＊4：仮に 1 秒間に通信範囲に入ってきた 5 台からのメッセージを先に処理し、残りの時間でその他の車両からのメッセージを処理するものとすると、

5[メッセージ] + (1000[ms] – 3.25[ms]×5[メッセージ]) / 1.74[ms] ≒ 570[メッセージ]（式 9）

である。

＊5：Verify-on-Demand により削減できた 60 メッセージ分も合わせると、a.では 1 秒間に 630 メッセージを処理していることになり、1 秒間に 1,000 メッセージを処理するとい

う目標に対する達成度は 63%である。以上の内容を表 3.3.3-5 にまとめた。

表 3.3.3-5　Verify-on-Demand におけるメッセージ検証の処理性能予測

判定方法	1 秒あたりのメッセージ検証数	メッセージの削減率	目標性能に対する達成度
a. 300m 以内の車両のメッセージのみ検証	940 メッセージ	6%	**約 63%**
b. 同一方向の車両のメッセージのみを検証	750 メッセージ	25%	**約 82%**

ただし、これらの試算は高速道路における一例である。メッセージの削減率は状況に応じて変わると予想される（例えば支線から本線に合流する場合は、多数の証明書未検証の車両と通信することが予想される）ため、様々な状況を想定した検討が必要である。

④ 各簡略化方式のリアルタイム性の評価に関するまとめ

米国、欧州で検討されている簡略化方式のリアルタイム性に関する評価結果を以下にまとめた。

・米国の CRL 検証簡略化は米国独自仕様の負荷を軽減することを目的としたものであり、そもそものメッセージ検証処理を簡略化するものではない。CRL 数を 1,000 に抑えた場合であっても、目標性能に対しては 3%程度の達成度となる。米国仕様においては、証明書の ID 計算を事前に済ませる、暗号 HW を用いる、等の方法で CRL 検証処理時間を短縮することが重要となる。

・欧州仕様では CRL 検証とリプレイ攻撃検査を仕様から削除しており、その点でメッセージ検証処理の簡略化が見込める。しかしながらそれでも目標性能に対しては約 24%の達成度となる。

・欧州仕様において、EE 証明書と Sub CA 証明書のキャッシュにヒットして Step7（証明書の署名検証）を行わない場合には、目標性能に対して約 56%の達成度となる。ただし、1,000 メッセージ全てが EE 証明書と Sub CA 証明書のキャッシュにヒットする状況というのは考えにくく、実際には受信したメッセージごとに Step7（証明書の署名検証）が必要なケースと不要なケースが混在すると考えられる。

・欧州仕様では、メッセージの検証処理の中でリプレイ攻撃検査を行わないため、アプリケーションでリプレイ攻撃の考慮が必須となり、アプリケーションの処理負荷が増すと考えられる。また、CRL 検証を行わないため、例えば頻繁に証明書を更新する等の何らかの代替策が必要となり、運用面での負荷も増加すると考えられる。

・Verify-on-Demand により簡略化が見込める。高速道路における対向車のメッセージの破

棄を想定した例では、表 3.3.3-5 で示したとおり、25%程度のメッセージを削減することが可能である。

以上、これまで検証してきた簡略化方式では、いずれの方式を用いても目標性能に対して未達となることが分かった。

目標達成するためには、Verify-on-Demand によるメッセージの削減率を、今回の試算結果よりもさらに向上させる必要がある。仮にメッセージの検証処理時間が最短となる No.28（チェイン=2、EE=1、SubCA=0、CRL=0、Msg=0 で、EE 証明書のキャッシュにヒット）で考えると、車載システム上で暗号 HW を利用した場合のメッセージ検証処理時間は 1.74ms であった。このとき 1 秒間に処理可能なメッセージは約 574 メッセージであるため、残りの約 426 メッセージを削減できれば目標性能が達成できることになる。すわなち、今回の試算では Verify-on-Demand によるメッセージの削減率を 25%程度と見積もったが、これを少なくとも 43%程度まで向上させる必要がある。

これを実現するためには、メッセージ検証処理のみではなくアプリケーションも含めたシステム全体としての検討が必須である。

なお、No.28（チェイン=2、EE=1、SubCA=0、CRL=0、Msg=0 で、EE 証明書のキャッシュにヒット）は常に EE 証明書のキャッシュにヒットして Step7（証明書の署名検証）が不要となり、かつ、CRL 検証もリプレイ攻撃検査も行わないテスト条件であるため、実際の環境を考えた場合には、上記値よりもさらに大きな削減率が必要となると考えられる。

(2) 簡略化によるセキュリティへの影響の分析

V2X 通信のメッセージ検証の簡略化によるセキュリティ上の影響を分析した結果を示す。セキュリティへの影響を分析するシステムは、図 3.3.1-1 で示した V2X システムである。本分析では、米国仕様および欧州仕様の簡略化を考慮した場合に、参考文献[13]の車車間、路車間通信の脅威分析の結果に影響が及ぶかを検討することで、簡略化よるセキュリティへの影響を洗い出した。さらに、リアルタイム性の評価で必要性が示された Verify-on-Demand を利用した場合において、脅威の洗い出しとその発生原因を分析した結果も示す。

なお、Verify-on-Demand は米国の仕様に含めるように提案されているが、欧州仕様でも適用可能な仕組みであることから、それら仕様には依存しない部分を分析した。

① 米国仕様における V2X 通信のメッセージ検証のセキュリティへの影響

米国仕様でのメッセージ検証簡略化の特徴は以下のとおりである（Verify-on-Demand を除く）。

・証明書チェインが 2 段
　－5 分毎に証明書を切り替えることでトラッキングを防止
・CRL による失効確認は米国独自方式を採用

－CRL のエントリから失効確認する証明書の ID を算出し、短期間での証明書切替えに伴う 1 台に必要な CRL のエントリ数の増加を抑止
－証明書の ID を算出するための特殊な処理があるため、CRL のエントリ数が多ければ、メッセージ検証全体の処理時間が増加

また、セキュリティに関わると予想される特徴として次のものが挙げられる。
・送信メッセージに有効期限を設定する機能が無効化されている

表 3.3.3-6 に米国仕様での簡略化によるセキュリティへの影響の分析結果を示す（表中の「対策」は簡略化を含めた米国仕様で脅威への対策ができるかを示す。「影響」は米国仕様の簡略化によって、参考文献[13]の結果に対して影響があったかを示す）。

米国仕様では証明書チェインを 2 段に抑えることが可能であり、DoS 攻撃の影響を軽減できる。しかし、失効確認すべき CRL のエントリ数が多い場合には、メッセージ検証に必要な処理時間が長くなり、DoS 攻撃への耐性が低下する。つまり、リアルタイム性の評価と同様に、CRL のエントリ数を増加させないような運用方法や配信方法を検討し、採用することが重要である。

また、署名検証自体の演算時間が長い上に、署名検証前のチェックを通過したメッセージの署名検証は必ず行われる。つまり、正しい形式のメッセージが大量に送信された場合には、署名検証の処理時間の長さが悪影響し、DoS 攻撃が成立する。このため、Verify-on-Demand 等のメッセージの内容を確認して、不要なメッセージの署名検証を実施しない機構を取り入れる必要がある。

さらに、検証済みメッセージに対するリプレイ対策は有効であるが、メッセージの有効期限を設定する機能が無効である。このため古いメッセージでも証明書の有効期限内であればメッセージ検証で異常を検出できず、過去に受信したメッセージ等を単純に再送する DoS 攻撃による影響を防げない。従ってリプレイ攻撃検査を署名検証前に行う必要がある。また、V2X 通信を利用するアプリケーションは個々に発行した時間を確認する等を行い、リプレイ攻撃の影響を低減するように考慮して開発する必要がある。

表 3.3.3-6　米国仕様での簡略化によるセキュリティへの影響

情報資産	脅威		対策	影響	理由
路情報 走行情報 汎用情報	DoS		軽減可	あり	メッセージ検証の仕組みでは根本的な DoS 対策はできない。 証明書チェインを 2 段にしていることで、DoS 軽減には好影響。ただし、CRL 数が多いと処理負荷になり、悪影響がある。
	Jamming		不可	なし	メッセージ検証の仕組みでは Jamming 対策は困難。
	偽 GPS 信号		不可	なし	メッセージ検証の仕組みでは偽 GPS 信号対策は困難。
	マルウェア		不可	なし	メッセージ検証の仕組みではマルウェアの混入は検知不可。
	装置外情報の改ざん		軽減可	なし	問題発覚後の CRL 更新で事後対策は可。対策の効果は CRL を迅速に更新できるかの運用に依存する。
	装置改ざん		軽減可	なし	
	盗聴		—	—	想定システムではメッセージをブロードキャストされるため、盗聴は脅威ではない。
路情報 （直）	路側機なりすまし	偽情報送信	可	なし	メッセージ検証で可。簡略化による影響はない。
		リプレイ攻撃	軽減可	あり	米国仕様では署名検証前に受信済みリプレイが有効。ただし、メッセージの有効期限を確認したいため、リプレイ攻撃への耐性に悪影響がある。
走行情報 汎用情報	車両なりすまし	偽走行情報送信	可	なし	メッセージ検証で可。簡略化による影響はない。
		偽汎用情報送信	可	なし	
		リプレイ攻撃	軽減可	あり	米国仕様では署名検証前に受信済みのメッセージへのリプレイ対策が有効である。ただし、メッセージの有効期限を確認しないため、リプレイ攻撃の耐性に悪影響がある。
	ロケーショントラッキング		可	なし	米国仕様は証明書の 5 分毎切替えすることで脅威を防ぐ。ただし、運用によって短時間で証明書を発行可能にする必要がある。
路情報 （間）	中継車両による改ざん		—	—	想定システムではメッセージ中継はなく脅威がない。
	偽情報（間）送信		—	—	

・対策：「—」…本検討で脅威として扱わないもの。「不可」… 簡略化を含む米国の V2X 通信仕様で対策できない脅威。「可」…対策できる脅威。「軽減可」…根本対策はできないが緩和できる脅威。
・影響：「—」…本検討で脅威として扱わないもの。「あり」… 米国の簡略化仕様が以前の分析に影響(悪影響、好影響)するもの。「なし」…影響しないもの。

② 欧州仕様における V2X 通信のメッセージ検証のセキュリティへの影響

欧州仕様のメッセージの簡略化は以下のとおりである。

・証明書チェインが 3 段
　－プライバシ情報を含まない匿名の証明書を発行し、トラッキング防止
・CRL による失効確認がない
　－有効期限の短い証明書を発行し、問題が発覚した場合には、新たな証明書を発行しないことで、CRL による失効確認がない影響を低減
・リプレイ対策が無効化

また、セキュリティに関わると予想される特徴として次のものが挙げられる。

・送信メッセージに有効期限を設定する機能が無効化

表 3.3.3-7 に欧州仕様での簡略化のセキュリティへの影響の分析結果を示す。(表中の「対策」は簡略化を含めた欧州仕様で脅威への対策ができるかを示し、「影響」は欧州仕様の簡略化によって、参考文献[13]の結果に対して影響があったかを示す。)

欧州仕様では、証明書チェインを3段と少なくできる上にCRL検証がないことから、簡略化により検証処理の負荷が下がり、結果として DoS 攻撃による影響を軽減はできる。しかし、リプレイ対策が無効になっていることおよび送信メッセージに有効期限を設定する機能も無効になっているため、リプレイ攻撃により DoS 攻撃が成立する恐れが高い。このため、V2X メッセージを利用するアプリケーションは個々にリプレイ攻撃の影響を低減するように考慮して開発する必要がある。

なお、CRL による失効確認が存在しないため、正当な証明書が発行された装置の故障や悪意のある正当な利用者から送られたメッセージを排除する仕組みがない。このため、証明書の有効期限を可能な限り短くし、問題発覚を即時にシステムに伝え、故障や悪意のある装置からのメッセージを迅速に排除できるように運用を工夫する必要がある。

なお、Verify-on-Demand を利用しない場合の米国仕様と同様に受信したメッセージは問題がなければ署名検証を必ず行う。このため、Verify-on-Demand 等のメッセージの内容を確認して不要なメッセージの検証を実施しない機構を取り入れる必要がある。

表 3.3.3-7　欧州仕様での簡略化のセキュリティへの影響

情報資産	脅威		対策	影響	理由
路情報 走行情報 汎用情報	DoS		軽減可	あり	メッセージ検証の仕組みでは根本的な DoS 対策はできないが、証明書チェインを 3 段にしていることや CRL 検証自体がないため DoS 軽減に好影響あり。
	Jamming		不可	なし	メッセージ検証の仕組みでは Jamming 対策は困難。
	偽 GPS 信号		不可	なし	メッセージ検証の仕組みでは偽 GPS 信号対策は困難。
	マルウェア		不可	なし	メッセージ検証の仕組みではマルウェアの混入は検知不可。
	装置外情報の改ざん		軽減可	あり	CRL がないが、証明書の有効期限を短くすることで軽減は可能。ただし、証明書の有効期限が長くなれば失効確認に悪影響する可能性がある。運用に影響がでないように証明書の有効期限を可能な限り短くするために、問題発覚を即時にシステムに伝える仕組みが必要である。
	装置改ざん		軽減可	あり	
	盗聴		—	—	想定システムではメッセージをブロードキャストされるため、盗聴は脅威ではない。
路情報 （直）	路側機なりすまし	偽情報送信	可	なし	メッセージ検証で可。簡略化に対す脅威ではない。
		リプレイ攻撃	不可	あり	欧州仕様ではリプレイ対策が無効である。さらに、メッセージの有効期限を確認しないため、リプレイ攻撃の耐性に悪影響がある。
走行情報 汎用情報	車両なりすまし	偽走行情報送信	可	なし	メッセージ検証で可。簡略化に対す脅威ではない。
		偽汎用情報送信	可	なし	
		リプレイ攻撃	不可	あり	欧州仕様ではリプレイ対策が無効である。さらに、メッセージの有効期限を確認しないため、リプレイ攻撃の耐性に悪影響がある。
	ロケーショントラッキング		可	なし	欧州仕様はプライバシ情報を含まない匿名の証明書を発行する仕様で防ぐことができる。ただし、運用により短時間で証明書が発行可能にする必要がある。
路情報 （間）	中継車両による改ざん		なし	—	想定システムではメッセージ中継はなく脅威がない。
	偽情報(間)送信		なし	—	

・対策：「—」…本検討で脅威として扱わないもの。「不可」… 簡略化を含む欧州の V2X 通信仕様で対策できない脅威。「可」…対策できる脅威。「軽減可」…根本対策はできないが緩和できる脅威。

・影響：「—」…本検討で脅威として扱わないもの。「あり」…欧州の簡略化仕様が以前の分析に影響(悪影響、好影響)するもの。「なし」…影響しないもの。

③ Verify-on-Demand に対する脅威

Verify-on-Demand は、メッセージの内容に基づいて判定した重要度が高いメッセージのみを検証する簡略化の仕組みである。このため、受信するメッセージ数が多い場合には、重要なメッセージを優先して処理することができる。一方、攻撃と判断したメッセージの検証を省くことにも活用でき、単純な DoS 攻撃の対策にも活用できると思われる。ただし、重要度が高いと判定される偽メッセージを大量に送る等の攻撃手法も考えられ、Verify-on-Demand に関係する脅威の把握が必要である。

そこで、悪意のある攻撃が行われた場合にどのような脅威が発生しうるかを分析した。今回の分析では、参考文献[14]に示される脅威分析手法を使用し、脅威の洗い出しとその脅威の発生原因の分析を実施した。なお、脅威の発生原因の分析では、V2X 通信のプロトコルの形式等の詳細な情報を使った分析はしていない。

この脅威分析手法を用いて分析した結果、アプリケーションの誤動作（重要な情報を通知させない、不要／誤った情報を通知させる）、遅延または停止につながる脅威のリスクが高いことが判明した。さらに、これら高リスクの脅威に対して、図 3.3.3-4 に示す。Verify-on-Demand のデータや処理の流れを考慮して原因分析した。

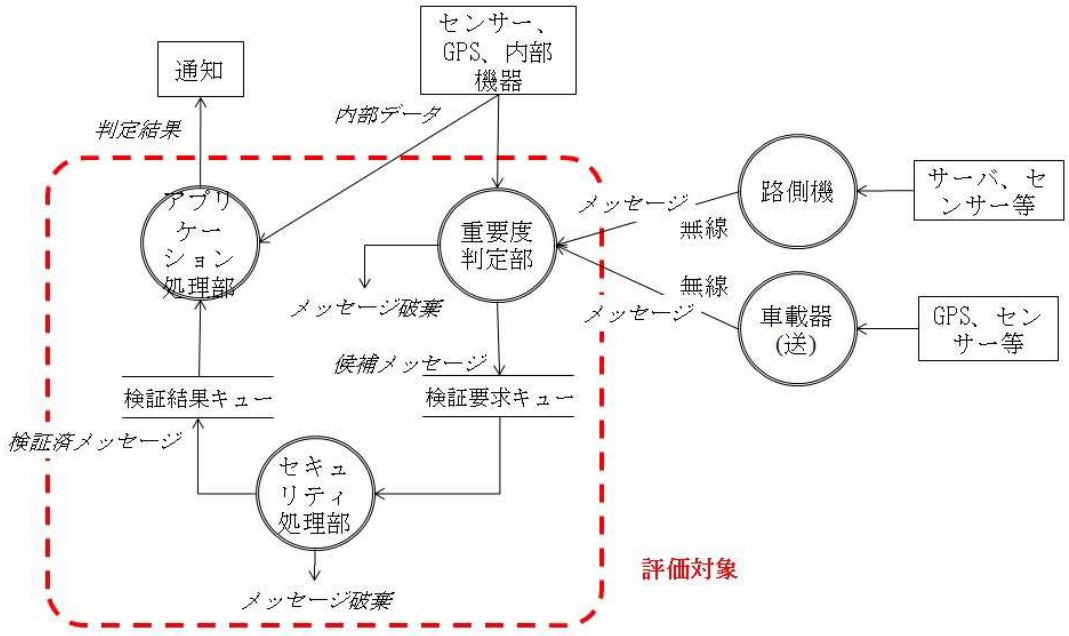


図 3.3.3-4　Verify-on-Demand に関連するデータと処理の流れ

分析の結果、Verify-on-Demand で検証が必要と判定されるように操作し、メッセージを大量送信するような高度な DoS 攻撃を行えば、幾つかの脅威に繋がることが分かった。例えば、要検証と判断される大量のメッセージが送信されれば、先に格納された検証要求の処理が完了するまで、次の検証要求を処理できない。これにより、後から受信した、ドライバへの通知を必要とするような重要なメッセージの検証が遅れてしまう恐れがある。また、検証要求キューを溢れる程の大量のメッセージが送信されれば、重要な情報を含む他車のメッセージが破棄される恐れがある。これは、メッセージ検証自体の処理時間が長く、検証要求を格納した順に処理することが原因である。Verify-on-Demand では、このよ

うな要検証と判定されるメッセージを送信する、より高度な DoS 攻撃へ対応できない。

このため、高度な DoS による影響を軽減するために、Verify-on-Demand の処理を改良すべきであると考える。

3.3.4 調査結果まとめ

前項までの調査結果を基に各簡略化方式を比較した。また、その結果を基に V2X 通信において署名検証を簡略化したとしても、セキュリティの担保が可能となるモデル案について考察した。

(1) 簡略化方式のリアルタイム性とセキュリティへの影響に関する比較調査

簡略化方式のリアルタイム性の評価結果とセキュリティへの影響の分析結果のまとめを表 3.3.4-1 に示す。

表 3.3.4-1 簡略化方式のリアルタイム性とセキュリティへの影響に関する比較（まとめ）

	米国仕様	欧州仕様・プロジェクト
リアルタイム性	・目標*1 に対する達成度：約 3% （3.3.3(1)①参照）	・目標*1 に対する達成度：約 24% （3.3.3(1)②参照）
	証明書の失効確認の負荷高	証明書の失効確認を行わない＊2
	リプレイ攻撃検査のエントリ数が処理性能に影響	リプレイ攻撃検査を行わない （アプリケーションの負荷増）
	検証済証明書の検索に用いるキャッシュのエントリ数が処理性能に影響	同左
セキュリティ	・メッセージ検証の速度不足を悪用した DoS 攻撃の恐れ	・同左
		・リプレイ攻撃の恐れ（リプレイによる DoS 攻撃を含む）
その他	・高頻度の CRL の更新が必要 e.g. 1 回/日以上	・高頻度の証明書更新が必要＊2 e.g. 1 回/日以上

＊1：1,000 メッセージ/秒の検証処理ができること
＊2：証明書の失効確認の代わりに高頻度の証明書更新が必要

リアルタイム性に関して、欧州仕様、米国仕様ともに暗号 HW を利用したとしても、1,000 メッセージ/秒の検証には至っていない。また、証明書の失効確認時の CRL のエントリ数や、リプレイ攻撃検査時のキャッシュ数、検証済証明書の検索に用いるキャッシュ数も、リアルタイム性に影響する。特に、各国の自動車の保有台数を考慮すると V2X 通信の普及時には CRL のエントリ数は膨大になる可能性がある。そのため、リアルタイム性に関して証明書の失効確認が不要となる運用が望ましい。

セキュリティに関して、欧州仕様、米国仕様ともにメッセージ検証の速度不足を悪用した DoS 攻撃の恐れがある。特に、欧州仕様ではリプレイ攻撃検査を行わないため、リプレイ攻撃だけでなく、メッセージの再送による DoS 攻撃の恐れもある。そのため、セキュリティに関してリプレイ攻撃検査を（署名検証前に）行うことが望ましい。

また、Verify-on-Demand は米国仕様、欧州仕様にも適用可能な仕組みであり、メッセージ検証数の削減による負荷軽減が見込めることが分かったが、要検証と判定されるメッセージを送信するような、高度な DoS 攻撃へ対応が必要である。

(2) V2X 通信のリアルタイム性とセキュリティを担保する簡略化のモデル案

これまでの調査・分析結果を基に、V2X 通信のリアルタイム性とセキュリティを担保する簡略化モデルについて考察した。

3.3.4(1)の比較により、メッセージ検証処理では

・CRL を使用しないこと

・リプレイ攻撃検査を行うこと

が望ましいことが分かった。ただし、証明書の失効確認の代わりに高頻度の証明書更新が必要になることに注意が必要である。これを実現した簡略化モデルにおけるメッセージ検証の処理フローを図 3.3.4-1 に示す。

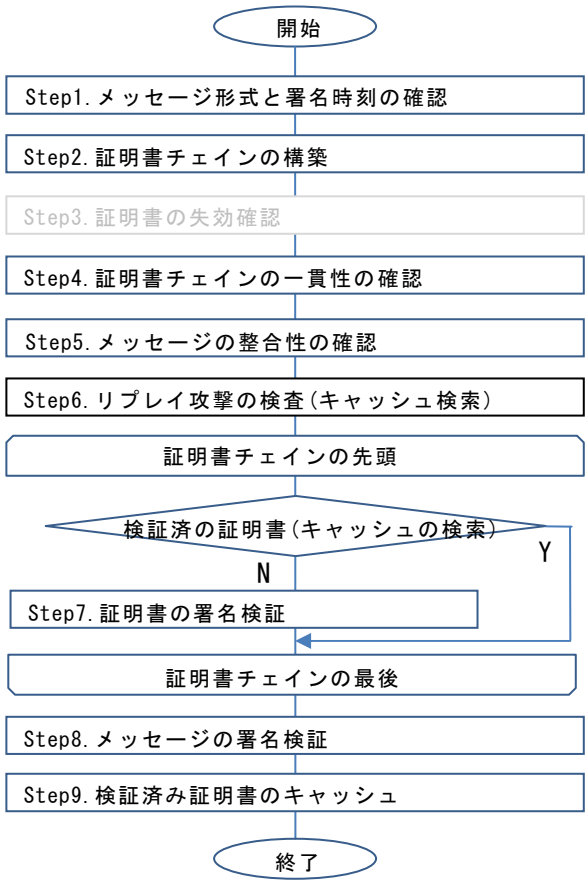


図 3.3.4-1　簡略化モデルにおけるメッセージ検証の処理フロー

次に Verify-on-Demand（従来モデル）関して、要検証と判定されるメッセージを送信するような、高度な DoS 攻撃への対応を検討した。

従来のモデル（図 3.3.4-2 参照）では、検証要求を格納した順に処理するため、先に格納した検証要求の処理が完了するまで、次の検証要求を処理できないことが問題であった。例えば、要検証と判定されるメッセージが大量に送信された場合にも、先に格納された検証要求の処理が完了するまで、次の検証要求を処理できない。これにより、後から受信したドライバへの通知を必要とするような重要なメッセージの検証が遅れてしまう恐れがある。また、検証要求キューが溢れる程の大量のメッセージが送信されれば、重要な情報を含む他車からのメッセージが破棄される恐れがある。これらは、メッセージ検証自体の処理時間が長く、検証要求を格納した順に処理することが原因であることが分かった。

そこで簡略化モデルに、従来モデルと同様の不要なメッセージの検証を実施しない機能に加えて、優先度に応じて検証の順番を変更する機能と格納した検証要求の優先順位の変更する機能、現在進行中の検証処理を中断する機能を追加する。これらの機能を実現する、簡略化モデルを図 3.3.4-3 に示す。

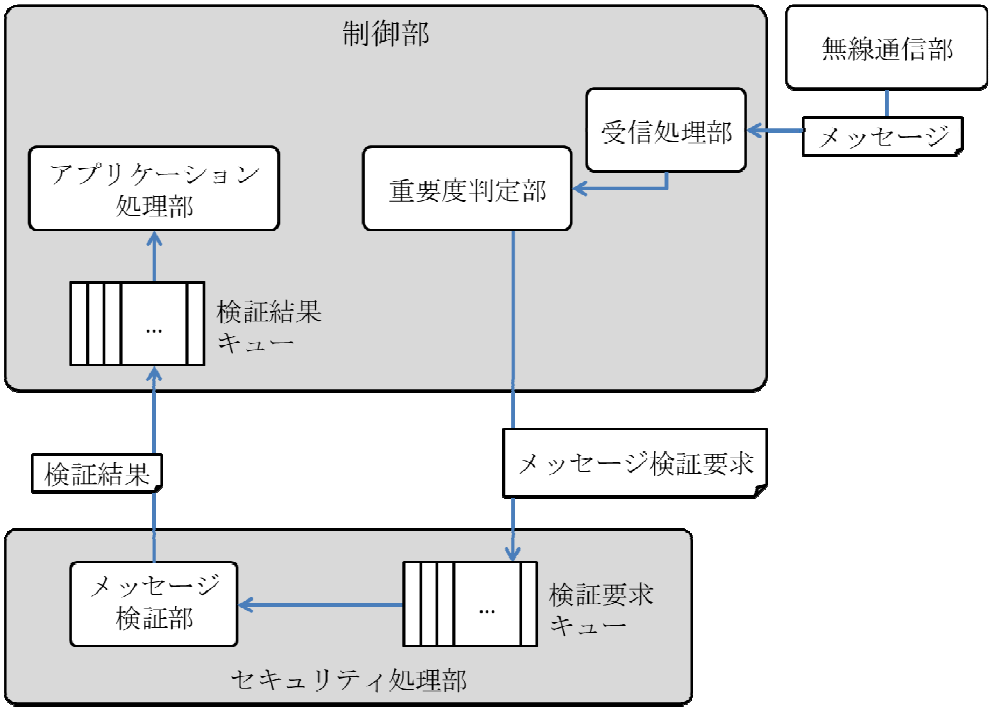


図 3.3.4-2　従来のモデル

図 3.3.4-3 に示す簡略化モデル（優先度付きメッセージ検証モデル）では、従来モデルと比較して、「状態判定部」が追加され、検証要求発行順に従って検証を行っていた「検証要求キュー」が優先度に従って検証を行う「優先度付き検証要求キュー」に換わる。また、従来モデルでは検証要否のみを判定していた「重要度判定部」は、「優先度判定ポリシ」と「状態判定部」から得た「状態」や「検証結果キュー」の検証結果を用いて、受信したメッセージの優先度を判定し、優先度付きメッセージ検証要求を発行する。「重要度判定

部」は、「優先度付き検証要求キュー」に対して「優先度変更要求」を用いて、発行済の優先度付き検証要求の優先度の変更や削除も行える。また、「重要度判定部」は中止要求により「メッセージ検証部」に対して実施中のメッセージ検証の中止を要求できる。

このようにすることで車両の状態や負荷に応じて検証する順番を動的に変更できる。また、図 3.3.4-3 からも分かるとおり、優先度付きメッセージ検証モデルは、メッセージフォーマットの変更を必要としないため、既存のプロトコルとの親和性も高い。

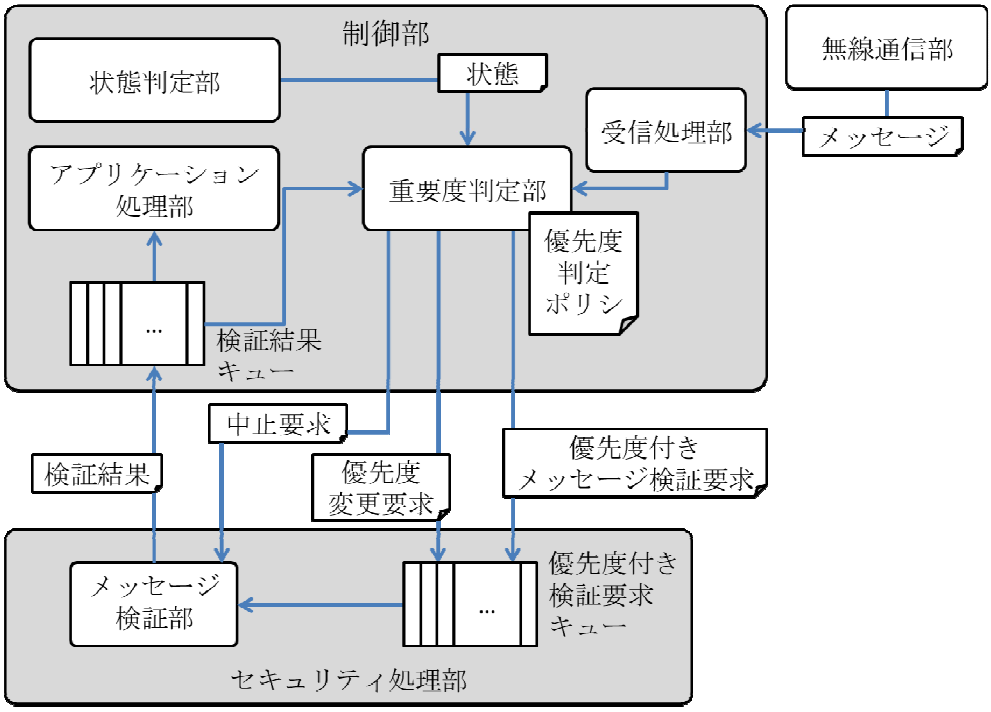


図 3.3.4-3　簡略化モデル（優先度付きメッセージ検証）

(3) その他

ここでは実用化に向けて解決が必要な課題である、①証明書の更新、②CRL のエントリ数と更新、③正当な装置の悪用による不正メッセージの送信、について考察した。

① 証明書の更新に関する考察

欧州仕様では CRL を用いないため、その代わりに証明書の有効期限を短くして頻繁に証明書更新を行う必要がある。次に挙げる条件で一日あたりの証明書発行枚数を試算した。

・証明書の更新頻度は 1 回/日（CA の多くは CRL を 1 回/日で更新）
・1 車両あたりに必要な 1 日の証明書は 288 枚（米国仕様[3]を参考）

この時、システム全体の一日あたりの証明書発行枚数は、

V2X システム全体の一日あたりの証明書発行枚数
=1 車両あたりに必要な 1 日の証明書の枚数×V2X 車載器を搭載した車両の台数（式 10）

である。例えばドイツの四輪車全てが V2X 車載器を搭載した場合、2013 年度末時点のドイツの四輪保有台数(約 4700 万台[15])で試算すると約 135 億枚になる。日本の場合は 7700 万台(15)であるためドイツの約 1.6 倍である約 222 億枚にもなる。これは証明書発行者の負荷だけでなく、証明書を発行する際に必要な通信等への負荷となる。また V2X 車載器が多数の証明書を保持することは車載器のコスト増にもつながる。そのため実用化に向けてインフラや車載器の負荷を軽減することが運用上の課題になる。

さらに、V2X システム全体のセキュリティを維持するためには、セキュアな（e.g. 脆弱でない、乗っ取られていない）V2X 車載器、車両に対してのみ証明書を更新しなければならない。そのため実用化に向けて、セキュアな V2X 車載器や車両であることを認証するフレームワークが必要である。

② CRL のエントリ数と更新に関する考察

本節では CRL を必要としないモデルを推奨している。一方で米国仕様[6]では、不正車両を検出するために CRL を用いる。調査結果のとおり、リアルタイム性に関して、証明書の失効確認の処理負荷を無視できない。失効確認の処理負荷を軽減するには検索対象となる CRL のエントリ数を減らす必要がある。検索対象のエントリ数を減らす方法として CRL の分割が挙げられる。IEEE1609.2[1]の証明書には CRL の ID があり、この ID を用いることで失効確認すべきエントリ数を少なくできる。

また、3.3.4(3)①の証明書の発行と同様に全ての車載器に CRL を配信する場合、CRL の配信に必要な通信等インフラの負荷が高くなることも想定される。実用化に向けて、差分 CRL（デルタ CRL）の活用や CRL の総エントリ数を増やさないような運用方法等のインフラへの負荷を低減することが課題である。

また脆弱な V2X 車載器や車両システムが増えると CRL のエントリ数の増大に繋がる。そのような事態に陥らないようにするためには、3.3.4(3)①と同様にセキュアな V2X 車載器や車両であることを認証するフレームワークが必要である。

③ 正当な装置の悪用による不正メッセージの送信（置装外情報の改ざん、装置改ざん）

3.3.3(2)の分析結果のとおり、正当な装置を悪用してメッセージに含まれる情報を故意に操作した場合には検証する方法がない。例えば、正当な証明書を発行された V2X 車載器の所有者が故意に V2X 車載器に対して不正な情報を送信し、V2X 車載器がこの不正な情報に基づいて、不正な V2X 通信のメッセージを送信した場合、この悪意の検出は V2X 通信の範疇では難しい。これに対応するためには、3.3.4(3)①と同様にセキュアな V2X 車載器、車両であることを認証するフレームワークが必要である。

(4) まとめ

本節では、メッセージ検証を構成する内部処理の処理時間を調査し、欧米等で検討中の簡略化方式を評価・分析し、処理能力を高めリアルタイム性を確保可能な署名検証簡略化のモデル案である優先度付きメッセージ検証を提案した。

平成 27 年度研究・開発では、V2X 通信において負荷の高いと予想される署名検証の簡略化に着目して取り組んだ。今後セキュリティ機能だけでなく、セキュリティ機能以外のプロトコルスタックやアプリケーションを含めた簡略化モデルの効果に関する詳細な検討とともに、効果を評価する環境の構築が必要である。

また本研究を通じて、鍵・証明書等の管理や V2X 車載器や車両の認証フレームワークの構築等、運用上の課題が判明した。これらの運用上の課題も実用化に向けて解決しなければならない。

参考文献（テーマ③）

[1] IEEE 1609.2: 2013. IEEE Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages.

[2] ”PRESERVE Deliverable 1.1 Security Requirements of Vehicle Security Architecture”, PRESERVE, June 2011. https://www.preserve-project.eu/sites/preserve-project.eu/files/PRESERVE-D1.1-Security%20Requirements%20of%20Vehicle%20Security%20Architecture.pdf

[3] USDOT, ”Security Credential Management System Design”, January 24, 2012. http://www.its.dot.gov/meetings/pdf/Security_Design20120413.pdf

[4] “PRESERVE Deliverable 1.3 V2X Security Architecture v2”, PRESERVE D1.3, June 2011. https://www.preserve-project.eu/sites/preserve-project.eu/files/PRESERVE-D1.3-V2X_Security_Architecture_V2.pdf

[5] 情報量と事故の減少効果との関係, 情報通信審議会 情報通信技術分科会 電波有効利用方策委員会, VHF／UHF 帯電波有効利用作業班, ITS グループ（第 1 回） http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/joho_tsusin/denpa_riyou/pdf/070320_1_s2.pdf

[6] 表 1：世界各国の四輪車販売台数, JAMA http://www.jama.or.jp/world/world/world_1t2.html

[7] IEEE Std 1363(tm)-2000, IEEE Standard Specifications for Public Key Cryptography.

[8] A High-Speed Elliptic Curve Cryptographic Processor for Generic Curves over GF(*p*) SAC 2013.

[9] Krishnan, H. et al., ""Verify-on-Demand” - A Practical and Scalable Approach for Broadcast Authentication in Vehicle-to-Vehicle Communication”, SAE Int. J. Passeng. Cars – Mech. Syst. 4(1):536-546, 2011.

[10] ETSI TS 103 097 V1.1.1: 2013. Intelligent Transport System; Security; Security header and certificate formats. https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.01.01_60/ts_103097v010101p.pdf

[11] ETSI TS 102 867 V1.1.1: 2012. Intelligent Transport Systems (ITS); Security; Stage 3 mapping for IEEE 1609.2.
https://www.etsi.org/deliver/etsi_ts/102800_102899/102867/01.01.01_60/ts_102867v010101p.pdf

[12] André Weimerskirch, “V2V Communication Security: A Privacy Preserving Design for 300 Million Vehicles”, CHES 2014, Sep. 2014.
http://www.chesworkshop.org/ches2014/presentations/CHES_2014_Invited.pdf

[13] ITS Forum RC-009 1.2 版: 2013. 運転支援システムに関するセキュリティガイドライン, ITS 情報通信システム推進会議.
http://www.itsforum.gr.jp/Public/J7Database/p41/ITS_FORUM_RC009V1_2.pdf

[14] 公益社団法人自動車技術会 規格審議会, “自動車ー情報セキュリティ分析ガイド” (JASO TP15002:2015), 2015 年 3 月 20 日

[15] 表 1：世界各国の四輪車保有台数（2013 年末現在）, JAMA
http://www.jama.or.jp/world/world/world_2t1.html

3.4　V2X セキュリティに関する海外の仕様や技術動向に関する情報共有（テーマ④）

自動車産業はグローバル産業であり、我が国のサプライヤ等の技術を海外にも展開できるようにすることは重要である。自動車における通信システムとして利用される V2X 通信は、今後、安全運転支援や自動運転での活用が見込まれる分野であるが、そこに適用されるセキュリティ技術は、国内と海外で異なっている。そのため、海外のセキュリティ仕様や、技術・プロジェクトの動向を常に把握しておくことが重要である。

本事業では、V2X セキュリティ技術に関する海外動向の調査として、以下の 3 つのアプローチにより調査を実施した。まず、V2X 関連の海外のプロジェクトの最新状況や、フォーラム、国際会議等の開催状況を WEB 等で確認した。また、国際会議等に参加して、V2X 通信におけるセキュリティ技術の動向や、自動車全般におけるセキュリティ技術動向の調査を実施した。

また、こうした調査から得られた情報の共有を行う仕組みについて検討した。

3.4.1　海外の動向調査（WEB による情報調査）

(1)　調査の背景

近年様々な国際会議で、セキュリティや V2X をテーマとした議論が行われている。しかし、いつ、どこで、どのような会議が開催されているのか、という全体像が掴めていないという実態があり、今後、様々な情報収集活動を行うにあたって、どの会議に出席すべきかといった、会議の重要度を検討するための材料が欠落している。

調査すべき会議、出席すべき会議、注視しておくべき会議を抽出するためには、それぞれの会議で、どういったテーマで誰が発表を行っているか、などといった情報を把握しておくことが重要である。また、効率的に調査するためには、年間のスケジュールや、開催場所についても整理しておくことが欠かせない。

(2)　調査の概要

上記のような背景から、本調査では、自動車セキュリティ等 V2X 通信に関連する議論が行われる国際会議および展示会の情報として、開催時期や開催場所、参加費等の情報を整理し、アジェンダや発表資料の公表有無、入手可否などについて調査を行った。今回ピックアップした国際会議は 65 である。但し、年間開催数を知るという意味で、ESCAR Europe、ESCAR USA、ESCAR Asia のように同じ年の内に開催地を分けて行っているものは、それぞれをカウントしている。調査結果をスケジュール表に整理した（Appendix D, E）。

また、合わせて、欧州で実施されているさまざまな協同プロジェクトのうち、V2X 通信に関連する研究開発を行っているものを抽出し、その概要を調べた。抽出されたプロジェクト数は 32 であるが、ここでは、特に CONVERGE、SCOOP@F について、その概要を記載する。

① CONVERGE

ドイツで行われた CONVERGE は下記特性を持つ通信アーキテクチャの構築を目標として始められた。

・最新の通信技術・セキュリティ技術を反映し、インターネット市場の変化を反映する
・さまざまな通信システムにオープンな、
・インターネットとは真逆の、信頼できる情報のみを配信可能な通信アーキテクチャ

図 3.4.1-1 に CONVERGE システムの概要を示す。

具体的な技術開発内容としては、以下の 2 点を含むネットワークを構築し実証を行っている。

・ハイブリッド通信（ITS-G5 と Cellular の融合）
・対応するセキィリティーシステム（インフラ含む）

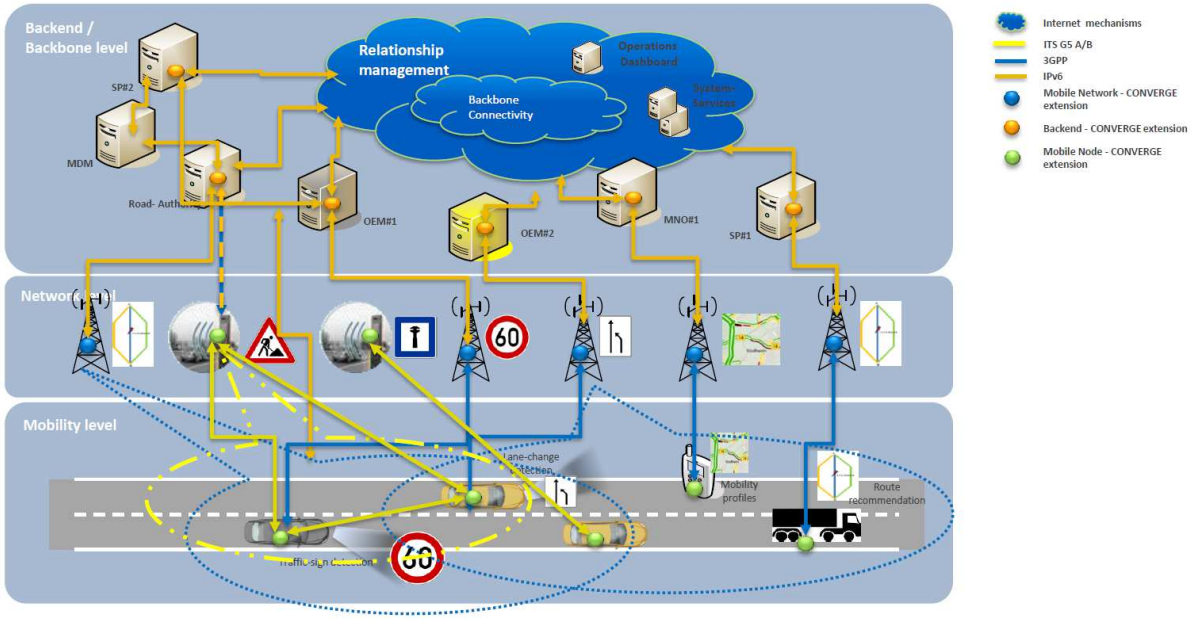


図 3.4.1-1　CONVERGE システム

CONVERGE は 2014 年 10 月から C2C-CC（CAR 2 CAR Communication Consortium）がサポートするプロジェクトの 1 つに位置づけられ、その成果が C2C-CC に報告されている。現在 C2C-CC の Security WG では、CONVERGE の結果をもとに議論している、また結果は C-ITS corridor に反映される予定である。以上のことから CONVERGE は欧州 V2X では技術的に重要なプロジェクトとして位置づけられている（図 3.4.1-2）。

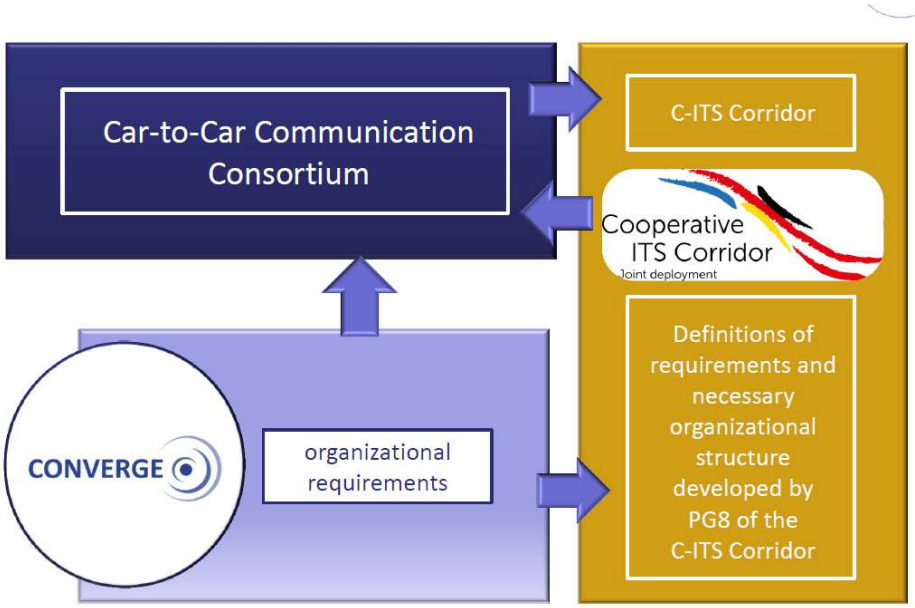


図 3.4.1-2　CONVERGE の展開

C2C-CC が参照している CONVERGE の結果に CIB（Car2X Initialization Body Organizational）がある。これは C2C-CC では Legal entity として定義され、V2X ネットワークの信頼性、完全性を保証する母体となっている（図 3.4.1-3）。

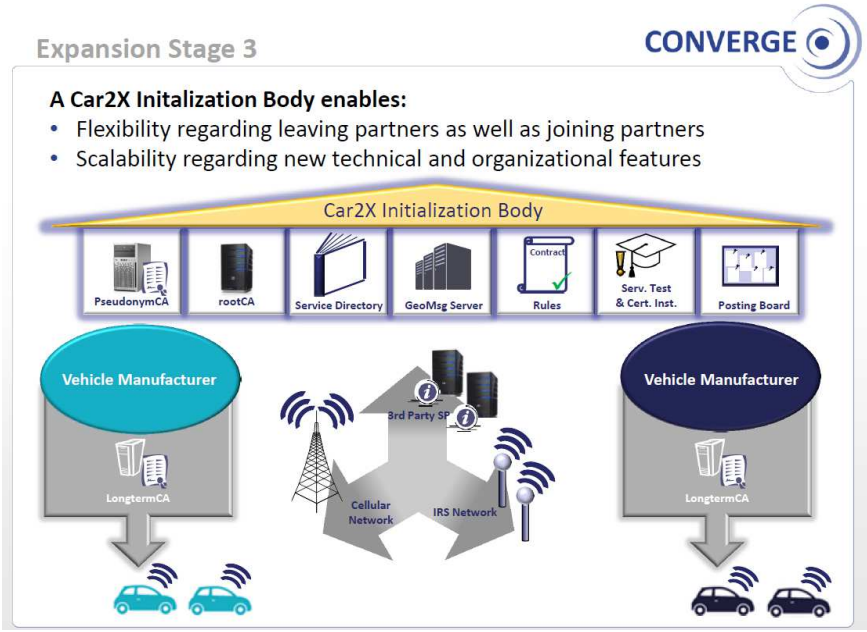


図 3.4.1-3　CIB の役割

② SCOOP@F

SCOOP@F は 2014 年 2 月にフランスの国家プロジェクトとしてスタートしたが、その年の 7 月には EC プロジェクトとして承認された。

SCOOP@F には下記に示すように開発フェーズが 2 期ある。

・1st wave：2014-2017

Priority services、ITS-G5communications

フランス国内での実証実験（図 3.4.1-4）

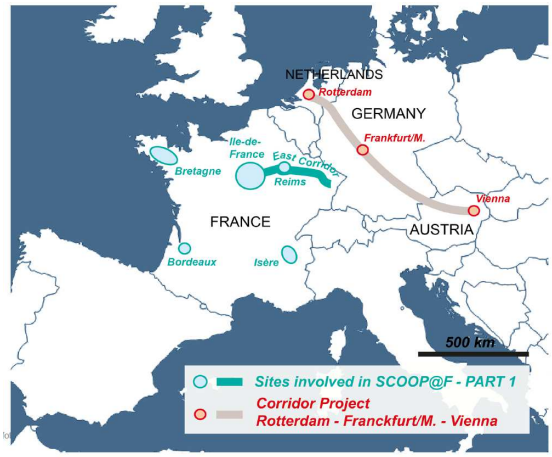


図 3.4.1-4　SCOOP@F FOT [Phase 1]

・2nd wave：2016-2018

New services、Hybrid cellular / ITS-G5communications

SCOOP@F 結果の拡散（フランス⇒スペイン、ポルトガル、オーストリア）（図 3.4.1-5）

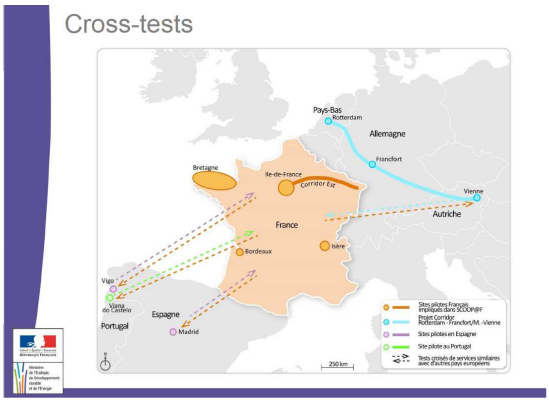


図 3.4.1-5　SCOOP@F FOT [Phase 2]

SCOOP@F では PKI システムにフランスの SystemX の ISE（Its SEcurity）プロジェクトで検討されたシステムを導入した。開発元は IDNOMIC 社（旧 OPENTRUST 社）[1]である。図 3.4.1-6 に SCOOP@F のセキュリティシステムの概要を示す。

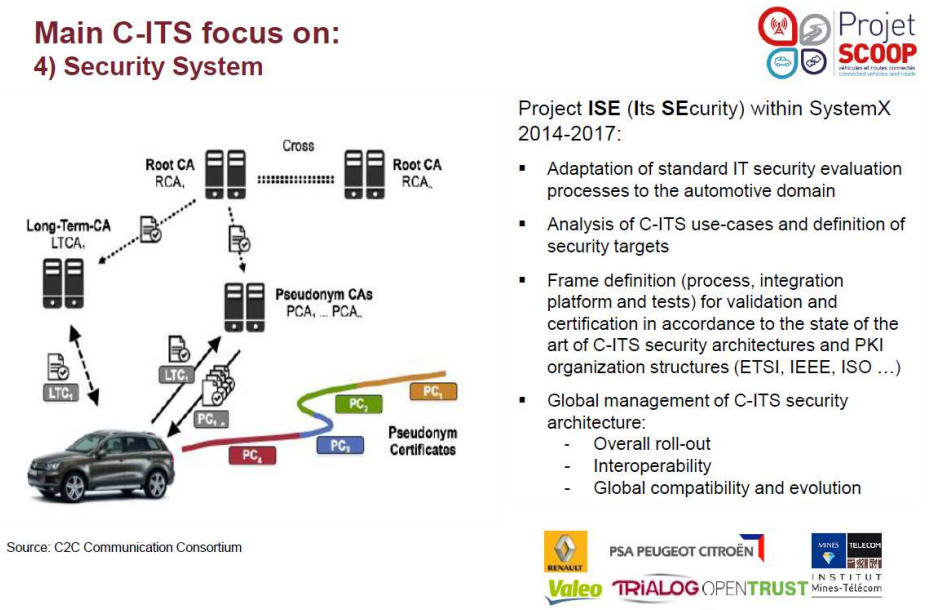


図 3.4.1-6　SCOOP@F　セキュリティシステム

(3) まとめ

今回調査した V2X 技術に関連する国際会議には以下のような特徴が見受けられた。

まず、NHSTA のような政府系の団体、あるいは IEEE など公的と言える組織が主催する会議と、IPQC や TU-Automotive の様なイベントの企画・運営をビジネスとする企業が主催しているものがある。前者は比較的概要やテーマの定まった会議・イベントを年次的に安定して開催するのに対し、後者はその時分に市場で盛り上がりを見せているトピックを次々に拾い上げ､それを冠したイベントを矢継ぎ早に開催するような傾向が見受けられる。

また、一般的に、政府系や公的な団体が主催する会議の参加費は、10 万円程度のレンジにあるのに対して、プライベート企業の主催するものは 30 万円から 50 万円とかなり高く設定されている。

さらに、公的・プライベートの違いに関わらず、一部の会議については、講演で使用されたプレゼンテーション資料がオンラインで入手可能となっているものがある。「AESIN Conference [2]」 のように、参加者以外にも資料をすべて無料で公開しているものもあれば、「Automotive Cyber Security Summit West [3]」のように販売という形で資料を一般に提供しているものもある。これらの資料は、参加することのできなかった会議でどのような議論が行われたかを窺い知るうえで大変有用であり、会議によっては資料の購入を検討するに

[1] https://www.idnomic.com/?lang=en
[2] http://aesin.org.uk/conference-2015/#9f60ee436ce5ed300
[3] http://www.b2biq.com/event.cfm?eventID=431#purchase-all

値するものもあると思われる。

また、現時点では、自動車のセキュリティに関する直接的な議論がされているかどうかは明確ではないが、これから適用が始まろうとしている DSRC による V2X 通信の次の段階として、或いは、V2X 通信との共存の形で、既存の携帯電話網や、5G といわれる次世代の携帯電話網を使うという案が議論されている。今回のリストには含んでいないが、こうした議論は、例えば、Mobile World Congress（MWC）や、World Wide Web Consortium（W3C）等で行われており、今後、自動車セキュリティをテーマとする議論の中でも取上げられる様になっていくのか、注目しておくべきと考えられる。

合わせて調査した欧州の V2X 関連のプロジェクトに関しては、特に EU の提供する枠組みの中で、国境を超えて協調する研究開発の取り組みが数多く実施されている。また EU の枠組みだけでなく、ドイツ、フランス、イギリスやスウェーデンなどでは、国家の支援する形でのプロジェクトも活発に行われている。今後の標準化や規制の動向を把握するためにも、EU のプロジェクトはもちろん、各国の動きについても注意深く観察していくことが重要であると思われる。

3.4.2 海外の動向調査（国際会議等での動向調査）

自動車のセキュリティ、特に V2X 通信に関連するセッションが設定された国際会議等として、以下の 4 つにおいてセキュリティ動向の調査を実施した。

(1) IEEE Vehicular Networking Conference 2015（VNC 2015）

VNC は、開催地が EU/ASIA/US を順番に回る形となっており、2015 年は 12 月 16 日から 18 日に京都で開催された。VNC はその名称の通り、自動車における通信関連の国際会議であり、可視光通信や、車両内部のネットワークや、通信シミュレーション等のセッションがある。セキュリティに関しては、「The future of vehicular networks: in-vehicle, V2V, and V2I」というタイトルのパネルセッションと、「Security and Privacy」のセッションがあった。

パネルセッションにおいては、次の様な話題があった。
セキュリティに対する関心が高まっており、ハッキングの実験報告などが新聞の一面に載ったりしている。このように、自動車のセキュリティは、①簡単にニュースになる、②車の中に繋げれば色々な情報を得ることが出来る、③無線他色々なところから狙われるが、主として CAN バスがアタックされる、という状況にある。自動車業界がもっと速く動かなければ、もっとアタックされることになる。一部の車では既にセキュリティ対策を実装しており、こういった車にはほとんどのアタックが（現在は）効かないことが分かっている。

セキュリティに対する考え方としては、①ID 認証や証明書、プライバシ保護のための Pseudonym の仕組みや、Misbehavior Detection などを活用した ID マネージメント、②他国

など、証明書の管理局が異なる域外へ移動したときにも安全に使うことが出来る File System Protection、③将来アタックされないとは保証できないことから必要となる Security Evolution、といったことに取り組んでいくことが重要とした。
また、セキュリティは複雑で、C2C-CC でも Certificate プロセスに関する議論を継続している。特に、Misbehavior Detection については、データの Consistency などをチェックするか、Detection はシステム内に必要かなどを議論している、という説明があった。

Security and Privacy のセッションでは、メッセージ認証を省略した場合の信頼度を計算し、その結果、累積の信頼度が低下した場合に検証を行うという方式の提案、認証した結果を他の車とシェアする方式、交通流制御に活用するための位置情報取得におけるプライバシ保護を実現する特定鍵を利用する方式、Misbehavior Detection における個々の車に対する信頼度の考え方、の 4 件の発表があった。

その他の情報としては、Misbehavior Detection に関する研究は EU レベルのプロジェクトでは行われておらず、ドイツの国家プロジェクトとして継続して研究中であること、また、Trust Model については、C2C-CC の中で議論されていることが分かった。

(2) Consumer Electronics Show 2016（CES 2016）

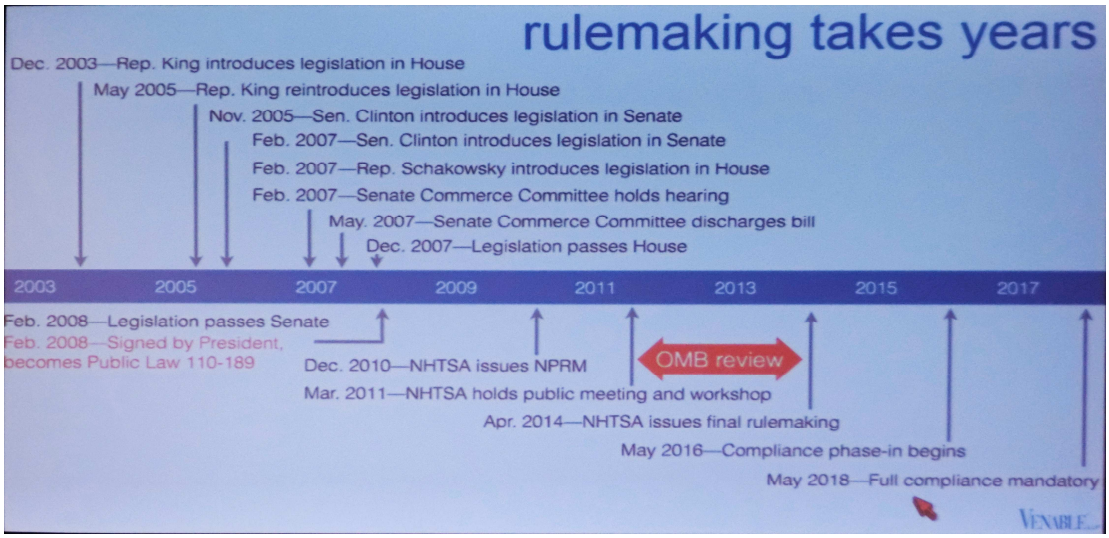
CES は毎年 1 月にラスベガスで開催される元々は、TV や携帯電話など家電の見本市的なショーであったが、近年、自動車関係の展示や発表が多く行われる様になってきた。特に 2015 年にメルセデス・ベンツ社がコンセプトカー「F015」を発表してからは、自動運転に関するアナウンスが自動車メーカから行われることが増えた。

CES では様々な展示が行われるのと並行して Conference が開催されており、その中でセキュリティをテーマとしたセッションにおいて、セキュリティ動向について調査を行った。
セキュリティ全般での話として、クレジットカードでは約 60 年の長い歴史があり、チップカードの導入など、色々な対策が講じられているが、情報を盗んで悪用するというのは無くなっていない。こういったことからも分かるように、セキュリティの対策は難しく、パッチワークを続けているというのが実情である。また、セキュリティを防御する側よりは、攻撃する側の方が多く、セキュリティ対策にどの位のコストを掛けるべきか、非常に難しい問題という認識である。

自動車のセキュリティに特化したセッションとしては「SAE Connected Vehicle Standards」があり、SAE がとりまとめている V2X に関連する標準に関する説明が行われた。今回、紹介されたのは、J2945/1、J2735、J3016、J2831、J3061 であり、特にセキュリティに関するものである J3061 は、ISO26262 のプロセスフレームワークに基づいて構成されており、講演の中で紹介されたとおり、アップデート版が 1 月中旬に公開され、1 月末には On-demand Webcast が開催された。

また、同じセッションにおける発表の中で、Legal Aspect からのルールメイキング活動も行われているが、一般的にルールメイキングには時間が掛るとして、以下の図 3.4.2-1

が示された。ルールメイキングとは別のアプローチとして 5 つ星評価のやり方もあり、ルールを作るより遥かに早く変化に対応することが出来るため、こちらのアプローチの方が現実的とも考えられるとの説明があった。



（出典：CES でのプレゼン，Dr. David L. Strickland，SAE Connected Vehicle Standards より）

図 3.4.2-1　ルールメイキングに要した期間

同じセッションにおける Q&A では、以下の議論があった。

- SAE では米国をベースとした規格・標準を策定しているが、ETSI、ISO とは Agreement があり協力関係にある。但し、ISO との関係は複雑であり、他に日米欧の枠組みもある。
- 規則としては、テクニカルな面とポリティカルな面があるが、セキュリティの場合、数字を規則にするのは合わないと考えられる。
- OBD ドングルのアフターマーケットの標準化については、EDA（Electricity Distributors Association）からのリクエストはあるが、現在、標準はない。ドキュメントがあると、カスタマーが OEM を訴えるということも想定される。

CES においても、Connected Cars という観点から、セキュリティとプライバシが注目されていたが、技術的な議論ではなく、どう扱うかを考える必要があるという面から語られることが多かった。この先、自動車会社はデータ会社に変わっていくという可能性もあり、そうなるにはセキュリティが重要な課題となる。例えば、インフォテインメントシステムやエアコンシステムなどのデータを集めることで、開発を速くすることが出来るが、セキュリティ機能を持たせるために、ゲートウェイを入れることで実現しているとする OEM もあった。

Connected Cars では、OEM が作るもの以外のものが車の中に入ってくる可能性があり、Ford はそういったものを調べるためのリサーチチームを複数持っており、欧州にも拠点を持っている。GM は 4G-LTE を使い、リモート診断などを今後サポートする予定があると説明していた。

(3) Transportation Research Board 2016（TRB 2016）

TRB は毎年 1 月に米国ワシントン DC で開催されており、2016 年は 95 回目である。TRB で取り扱われる内容としては、道路などの交通インフラから、航空、海上輸送なども含まれる非常に幅広いものとなっている。注目していた V2X 通信関連では、通信及び通信に使われるセキュリティの技術的な話題はなく、V2X を利用するプロジェクトに関する報告と、V2X 通信を活用したアプリケーションに関する報告が行われていた。セキュリティ関連では、サイバーセキュリティに関連する話題は、「Cyber Security: We've been Framed!」「Cyber Security Sub-Committee Meeting」「NHTSA Vehicle and Behavioral Safety Research」の 3 つのセッション等で取り上げられた。

「Cyber Security: We've been Framed!」では、サイバーセキュリティのリスクに対して、どの程度のリソースを充てるべきかの考え方の議論があった。サイバーセキュリティの対策に充てる予算は、コストベネフィットで決めることが考えられるが、セキュリティ侵害は会社にとってコストになることは間違いないが、どの位セキュリティ対策に投資するか、どうリスク対策をするかは難しい。最適な投資額を決めるキーとなる要素は、Potential Loss (Cost Saving)、Vulnerabilities / Threats、Productivity of Investments の 3 つがあり、Potential Loss の評価、脆弱性／脅威に対する攻撃の検証、可能な組み合わせから Grid を作り、最大のベネフィットを得られるポイントを選ぶことが出来る。ただ、計算することは出来るが、それだけでは経営判断は難しい。この点では、V2X のセキュリティというポイントに絞っても同様と考えられる。

次いで、SAE J3061 の概要紹介が行われた。サイバーセキュリティのスコープは、セーフティよりも範囲が広く、セーフティでは故障した時の対策を考えれば良いが、セキュリティではアタックの目的をも考慮する必要がある点が異なる。また、インシデントがあった場合に、それを最後はどうマネージメントに報告するか、といったことも考える必要がある。J3061 では、テスト方法やテストツール等の具体的な項目が Appendix に記載されていると紹介があった。また、Q&A の中で、セキュリティとセーフティの人がお互いに話をするという点で、自動車が最初のケースになるのでは、という議論があった。

「Cyber Security Sub-Committee Meeting」では、Jeep の例などから OTA の有効性の議論、組み込み機器によるリスク、ISAC などの情報共有や CISA などの対応組織の考え方、状況等の報告があった。また、CES でも同様の報告があったが、スマートフォンや USB などのユーザー持ち込み機器に関するセキュリティ上の懸念が示された。特に、最近になって自動車に USB ポートが設けられるようになったこと、および、2014 年 8 月に USB の深刻な脆弱性が見付かったこともあり、USB 経由での攻撃に対しても対策が必要ということが報告された。

「NHTSA Vehicle and Behavioral Safety Research」では、V2X セーフティメッセージは、信頼できるソース・認証があること、メッセージが改ざんされたり、変更されないことや、プライバシ保護が必要で、そのためには、システムにはセキュリティが必要で、PKI（Public Key Infrastructure）システムが重要とした。また、Misbehavior Detection とセキュリティの

関連する通信、自動車レベルにおけるセキュリティ認証手順については、改善が必要であり、V2V 特有のサイバーセキュリティの評価も重要とした。NHTSA はサイバーセキュリティに関しても、パートナーシップによる研究への関与のみではなく、in-house Cybersecurity Lab を持っており研究を進めている。NHTSA での研究分野としては、設計プロセスと標準の研究・評価、メッセージ認証、ゲートウェイ／ファイヤウォール、侵入検知技術などがある。

また、TRB の後に 3 極会議が開催された。3 極会議は基本的に各地域 6 名づつのメンバーで構成され、関連するオブザーバー等も参加、今回は、日本からのオブザーバーとして、SIP-adus の各テーマの窓口となる人の他、数名が参加。韓国からも 1 名参加していた。会議では、テーマごとの状況報告が行われ、その後、新しいテーマとして、CyberSecurity と Connected Vehicle を設置するかどうかが議論された。CyberSecurity は、それだけでは対象とする範囲が不明確であるため、CyberSecurity for Automated and Connected Vehicle とすることで合意。Connected Vehicle は継続して議論することとなった。

(4) C2C-CC Forum

C2C-CC Forum は 2015 年 11 月にマインツで開催された。今回の C2C-CC Forum では Day1（欧州 V2X サービスイン）の技術的な検討はほぼ終了しているため、下記 3 点を考慮して発表が行われた。

・今までの開発内容のまとめ
・今後の C-ITS 普及に関する準備/対応
・自動運転を念頭にした Day2 に向けての対応

特に、欧州の V2X システム用の PKI については、RootCA 間の通信や信頼度の考え方など、まだ固まっていない部分があり、CONVERGE の結果を反映されるものと見られる。

3.4.3 情報共有の仕組み構築

3.4.1 で調査した結果については、海外向け V2X 通信システムに関する製品を製造する事業者や、自動車セキュリティを扱うコンサルタント等をメンバーとする情報共有の場として、平成 26 年度に実施された SIP（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）のメンバーによるワーキンググループ B を開催した。

ここで扱う情報は基本的に、Web 上で公開されていたり、国際会議等で議論されている内容を対象として考えているが、参加している企業からは、個社では全ての情報を集めることは難しく、こういった情報共有、及び、海外向け V2X に関する議論の場があることは有意義であるとの意見があった。また、最近の V2X セキュリティ技術の海外動向としては、部品レベルの規格よりは、Misbehavior Detection などのシステムレベルのオペレーションに関する部分の議論が中心となっていることから、システム系のメンバを加えていくことが提案された。

今回は、調査した結果がまとまった後に、ワーキンググループのメンバで情報共有するという形で行ったが、こういった情報は、リアルタイム性が重要であり、調査結果や、今後の国際会議の予定がいつでも見ることの出来る環境を構築することが将来的には必要になると考えられる。また、データを整理してファイルにまとめようとすると、そのサイズが大きくなりすぎて、逆に情報が探しにくいことや、都度ファイルをやり取りする必要があることなどの課題もある。こうしたことを解決するためには、例えば、WEB 上での情報公開といった形態も考えられるが、情報の逐次メンテナンスを継続的に運用していくための仕組み、ビジネス化などを含めた出口戦略の検討を進めていくべきとの意見があった。

3.4.4 まとめ

V2X 通信にかかるセキュリティ技術の海外動向について、どういった会議やフォーラムでその情報が得られるか、実際の会議等の場でどういったことが発表・議論されているかという両面から調査を行った。自動車セキュリティに関連すると思われる国際会議として、今回抽出したものを合計すると、年間 62 回も開催されている。これらの会議全てに参加して調査を行うのは難しいため、プログラムから参加すべき会議の選択、複数企業・団体による調査活動の分担、会議に参加した企業等から情報を集める仕組み作りなど、効率的な情報収集の方法について検討していく必要がある。

国際会議等における V2X 通信分野における発表・議論は、すでに実際の通信機器を用いた実証実験等が進められていることもあり、Misbehavior Detection や署名検証簡略化、プライバシ保護など、インフラやシステム寄りの話題が中心となっている。また、調査した結果としての情報共有については、議論の内容がシステム寄りに移ってきている状況から、現在のメンバから、新たにシステム開発に携わる企業等を加えるなど、メンバの見直しを行うべきとの意見が出た。

今回調査したものは、基本的に公開されていたり、公の場での発言を基本としているが、情報の活用ということを考えた場合、リアルタイム性や検索性がより求められるものもあり、情報の種類ごとに展開や有効活用の仕方を検討していく必要がある。本事業において整理した国際会議の開催情報などは、継続的なサービスとして提供されることが望ましいと考えられる。

3.5　研究開発全体企画・管理

3.5.1　全体工程表の策定

テーマ①（自動運転の共通モデルの構築と、それに基づく脅威分析、セキュリティ要件及び対策の検討）、テーマ②（車両への攻撃に対する対策の評価手法・認証の調査・研究）、テーマ③（V2X 通信における署名検証の簡略化の研究）、およびテーマ④（V2X セキュリティに関する海外の仕様や技術動向に関する情報共有）の各テーマの間の連携を図りつつ、全体工程表を策定するとともに、研究管理を実施した。

実施にあたっては、開発における課題を整理するとともに、国内外での技術開発動向や標準化動向も参考に、実施内容や開発費等についての開発全体企画を策定した。

なお、開発計画や実施内容について審議するとともに、研究開発を効率化するための助言をいただくため、外部有識者を含む開発検討会を設置した。

3.5.2　開発検討会の運営

テーマ①～テーマ④に共通する事項や、各テーマにおける重要な課題などを議論・検討する開発検討会を設置し、平成 27 年度は、12 月 21 日、1 月 29 日、2 月 17 日の 3 回開催した。開発検討会では、本事業の趣旨、実施内容について理解いただき、事業を進めていく上での課題について議論を行った。

開発検討会における最も重要な議論は、情報管理のあり方という点であった。特に、今回の事業においては、セキュリティというセンシティブな内容を扱っているために、研究・開発の成果についてもどこまでの内容を開示することが出来るのか、という課題が明確になった。また、逆に研究・開発に活用するための情報、例えば、IPA や JPCERT/CC といった外部機関からの非公開の情報を受け取るためには、どういった体制や仕組みが必要かを検討しなければならない、ということも課題である。

(1) 第 1 回開発検討会の開催：平成 27 年 12 月 21 日

・本事業の概要、及び、各研究室で取組む研究内容について説明を実施し、以下のコメントをいただいた。
・自動運転のセキュリティは重要であり、全体としてどういうものがあって選定したのか、マッピングが欲しい。他業界との比較についても見える化が出来ると良い。
・セキュリティ認証については、自動車の認証（IWVTA）とのつながりについても、調査・関係整理が必要。部品については基本的に相互認証となっているが、セキュリティも同様かどうか、また、海外における規格化の動向や進め方についても調査すべきである。

・脅威分析については、多様な階層、対象（システム-部品）、重要度を考慮して検討することが重要である。

(2) 第 2 回開発検討会の開催：平成 28 年 1 月 29 日

・脅威分析に用いるシステムアーキテクチャに関するもの、脅威分析の手法など、具体的な内容や位置付けに関する議論を行った。
・脆弱性情報の共有のあり方に関する議論を行い、情報共有のための体制構築が必要だが、まず、共有する情報の内容、目的、共有の範囲等を明確化することが重要との認識を共有した。

(3) 第 3 回開発検討会の開催：平成 28 年 2 月 17 日

・コンポーネントレベルでの評価の結果概要が報告された。初級レベルの対策に対するものとはいえ、短い時間で攻撃することが出来たという結果は重要である。
・これらの結果については、中身の有効活用ということも考慮しつつ、情報の共有を如何に進めていくかといった課題も見えてきた。また、こういった情報に触れた人が他に出て行った場合のリスクへの対応をどうするのか、という課題も確認した。
・未公開早期警戒情報等を受けて、情報共有を行うための体制については、今後、関係団体とも意見交換させていただきながら検討する予定。

3.5.3 その他の会議

また、テーマ①と②、テーマ③と④は、それぞれ関連が深いことから、これらを合わせた、ワーキンググループ A（テーマ①、②）とワーキンググループ B（テーマ③、④）を JARI が主催者となって開催した。ワーキンググループ A は、12 月 21 日と 1 月 19 日の 2 回開催し、今回の研究における最重要課題である共通モデルの考え方について議論を行った。ワーキンググループ B は、3 月 8 日に開催し、海外で開催されている国際会議のリスト（3.4.1 の調査結果）の共有を行うとともに、公開されている情報を整理したものの扱いについて議論した。

また、有識者などが参加する別途設定するに開催された次世代高度運転支援システム推進委員会の第 3 回（12 月 8 日）、第 5 回（2 月 29 日）において研究開発報告を行い、開発計画や実施内容等に関するアドバイスやコメントを頂いた。

第 4 章　まとめ

今後ますます重要となっていくことが予想される自動車セキュリティに関して、4 年間の事業として、以下のテーマを設定して研究・開発への取組みを開始した。

具体的には、①自動運転の共通システムアーキテクチャの構築とそれに基づく脅威分析の実施、②コンポーネントレベル～車両レベルにおけるセキュリティ評価技術・基準の検討、③V2X 通信における署名検証簡略化の技術検討 3 項目と、④V2X 関連セキュリティ技術の海外動向調査である。

平成 27 年度は、その 1 年目として、①では、これまでに行われたプロジェクト等におけるシステムアーキテクチャ、ユースケース、脅威分析手法、リスクアセスメントの調査を行い、比較・分析を行った。これにより、現在構築中の自動運転システムの共通アーキテクチャを用いた脅威分析を行う準備が整った。

②では、コンポーネントレベル～車両レベルにおけるセキュリティ評価技術に関する調査を行い、今後、どのような評価手法を用いて評価基準の検討を行うのかの指針を得ることが出来た。また、コンポーネントレベルの初期評価を実施し、セキュリティ機能を実装していても、乱数発生器の初期化といった処理が適切に行われない場合は、攻撃に対する防御としては不十分になるという結果を得た。

③では、欧米等で提案されている署名検証簡略化方式について机上での評価を行い、これらの方式では DDoS 攻撃等に対して、脆弱性の懸念があることが示された。

④では、V2X 通信に関するセキュリティ技術の海外動向調査を実施した結果、V2X 通信は欧米において実証実験の規模拡大の方向にあり、通信機器そのもののセキュリティ技術の話題は減り、代わって実運用に向けたシステム的な課題の方に論点が移っていることが確認できた。

自動運転においては、V2X 通信をはじめとする通信による情報の入手が欠かせないものという認識とともに、通信で繋がることによりこれまで考える必要がなかったセキュリティ上の脅威が発生するため、その対策が非常に重要となっている。セキュリティ対策には、絶対に安全と言えるものはなく、コスト面も考慮した上で、どこに、どのような対策を実施すべきかを検討していく必要がある。本事業により得られた結果は、今後、セキュリティ対策の評価手法・評価基準を考えていく上で、非常に有効なものになると考えている。

経済産業省委託

平成 27 年度
戦略的イノベーション創造プログラム（自動走行システム）：
V2X 等車外情報の活用にかかるセキュリティ技術の
研究・開発プロジェクト

報　告　書

平成 28 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