平成２８年度
戦略的基盤技術高度化・連携支援事業
戦略的基盤技術高度化支援事業

「高度 IT 融合社会の安全・安心を支える次世代自動車用セキュリティ・ゲートウェイ・ECU の開発」

研究開発成果等報告書

平成２９年 3 月

担当局　　中部経済産業局
補助事業者　株式会社ヴィッツ
　　学校法人立命館

留意点

「この報告書には，補助事業の成果として，産業財産権等の対象となる技術情報（未出願又は未公開の産業財産権等又は未公開論文），ノウハウ等の秘匿情報が含まれているので，通例の取扱いにおいて非公開とする．ただし，行政機関の保有する情報の公開に関する法律（平成１１年法律第４２号）に基づく情報開示請求の対象の文書となります.」

目次

第１章 研究開発の概要 ……4
１－１ 研究開発の背景・研究目的及び目標 ……4
１－１－１ 研究開発の背景……4
１－１－２ 研究目標……6
１－２ 研究体制……7
１－３ 成果概要……10
１－４ 当該研究開発の連絡窓口 ……11
第２章 セキュリティ・ゲートウェイ・ECU の開発12
２－１ セキュリティ・ゲートウェイ・ECU 仕様開発……12
２－１－１ 遠隔リプログラミングシステムの基本仕様策定 ……12
２－１－２ 脅威分析およびリスク分析の実施 ……15
２－１－３ 脅威に対抗するためのセキュリティ機能仕様の導出 ……17
２－１－４ セキュリティ・ゲートウェイ・ECU のアーキテクチャ設計……18
２－１－５ 自動車業界向け研究成果の活用検討……20
２－２ セキュリティ・ゲートウェイ・ECU ハードウェア開発 ……22
２－２－１ ベーシックシステムの開発……22
２－２－２ FPGA 向け PUF 技術の設計／評価……23
２－２－３ セキュアな統合回路の開発……25
２－２－４ PUF 技術を活用した鍵交換プロトコルの設計／評価 ……27
２－３ セキュリティ・ゲートウェイ・ECU ソフトウェア開発 ……28
２－３－１ ベーシックシステムの開発……28
２－３－２ 遠隔リプログラミング用アプリケーションの開発……29
２－３－３ 自動車業界向け研究成果の活用検討……31
第３章 IEC 62443 準拠の開発 …… 33
３－１－１ セキュリティコンセプト文書の開発……33
３－１－２ 国際認証機関によるコンサルティング／アセスメント……35
第４章 全体総括 …… 37

第 1 章 研究開発の概要

1－1 研究開発の背景･研究目的及び目標

1－1－1 研究開発の背景

【背景】

わが国の自動車産業は，世界に先駆けた事故防止機能による優れた安全・安心性能，故障が極めてまれな高い信頼性，高級感がありながらも比較的低価格な車両作りを強みとして，世界市場の大部分を獲得する産業に成長し，自動車大国としてのわが国の経済を牽引している．わが国の自動車のものづくりは，製品本来の性能や品質を高める設計と，機能欠陥が生じたとしても事故に至らない安全設計との摺合せ開発を基盤としており，わが国の自動車製品に対する信頼は高い（2010 年の米国における日本車アクセル問題も最終的には安全性が確認されている）．

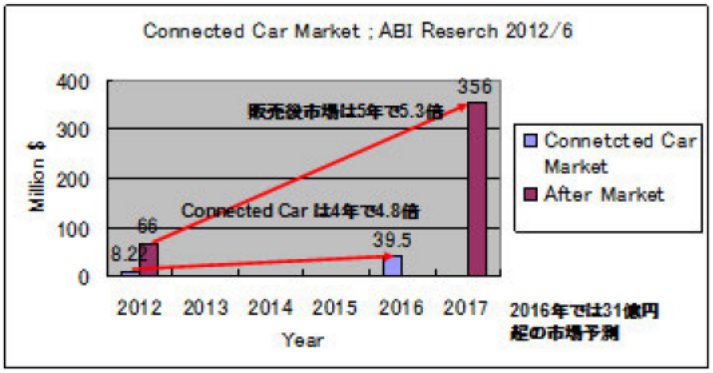


図1-1「繋がる車」の市場予測

一方，地球温暖化防止に向けた省エネルギー化を図るため，エネルギー利用の効率化や再生可能エネルギーの活用が，今日の人類に課せられた大きな課題となっている．その解決策の 1 つが，情報技術を応用してあらゆる機器を相互接続することによりエネルギーの需要供給管理を最適化する高度 IT 融合システム社会であり，早期の実現が求められている．とりわけ次世代自動車は，外部ネットワークを介して様々な機器と連携することにより（Connected Car），省エネルギーへの貢献と利便性の向上が期待され，市場規模も大きいと予想されている（図 1）．例えば，EV/PHV の内蔵バッテリを有効活用した電力消費の平準化，走行連携による渋滞緩和，エアコンやドアロック等の遠隔制御による快適性や防犯性，メンテナンス性の向上などが実現しつつある．

しかしながら，2010 年に米国ワシントン大学の研究者らが自動車の IT 化部位へのサイバー攻撃が可能であることを実証した研究論文を発表し，自動車のセキュリティ脆弱性が露呈した．それ以降，ハッキング技術のワークショップとして有名な DEFCON では自動車へのサイバー攻撃がデモされるなどした結果，現在では一般利用者でさえ攻撃方法が入手できる状況になっている．これにより，犯罪者は従来の情報機器のみならず自動車も攻撃対象とすることが可能となり，恐喝等を目的とするハッキングの発生が国内自動車メーカの大きな脅威になっている．

こうした状況に対し，欧州では自動車への脅威が顕在化する以前の 2008 年より，自動車セキュリティに関する研究(EVITA プロジェクト)を開始し，路車間等の通信を前提とした場合のセキュリティ脅威への対策が進められた．一方，わが国の自動車セキュリティ対策は，まだ議論が始められた段階であり，欧米諸国と比較して 5 年～10 年の遅れがある．こうした状況は，来るべき高度 IT 融合社会においてわが国の自動車産業の国際競争力の低下を招きかねない事態である．すなわち，わが国の自動車産業はセキュリティ対策において以下の課題を抱えている．

○課題 1：高度 IT 融合社会の一員としてセキュリティ脅威への対策を短期間で可能とする技術開発が必要

高度 IT 融合社会において自動車は，クラウドとの情報連携，車車間による運転連携，宅内家電ネットワークとの連携など，様々な形態で他の機器と繋がる．しかし，これらのサービスを実現するために必要な外部ネットワークが，直ちにすべての車載システムと接続されることは，コストやセキュリティ強度の観点から考えにくい．6 年後に迫る東京オリンピックまでに実用化すべき技術に焦点を当て，クラウドを経由したサイバー攻撃から車載システムを守る必要がある．

○課題 2：市場優位性確保のため，欧州が主導する技術に対してアドバンテージを有する技術開発が必要

自動車セキュリティを実現するためには，EVITA 成果物である EVITA セキュリティチップをそのまま活用することもできる．しかし，EVITA セキュリティチップは「セキュアメモリに暗号鍵を保管すること」を前提としており，従来の情報機器の開発現場においては，製造工場において「チップに書き込む鍵の管理」に高いコストを支払っているという課題がある．この様な課題への対抗策を世界に先駆けて開発することで，自動車産業の国際競争力を強化する必要がある．

○課題 3：相互接続性確保のため，欧米主導で制定された規格に準拠した技術開発が必要

欧州では制御機器セキュリティの国際規格である IEC 62443 が策定されている．機能安全に関連する国際規格と同様に，自動車に対するサイバー攻撃の事例が増加するに伴い，欧州で自動車を販売するために IEC 62443 に準拠した製品開発が必須となることが予見される．そのような事態に備え，セキュリティ規格への対応知見を蓄積する必要がある．

１－１－２ 研究目標

○セキュリティ・ゲートウェイ・ECU の開発

本事業では，クラウドを経由したサイバー攻撃から車載システムを守ることに焦点を当て，自動車内部の制御機器と外部機器との間のセキュアな通信を確保するための**セキュリティ・ゲートウェイ ・ECU を研究開発(対策 1)**する．次世代自動車は，この ECU を搭載することにより外部機器による自動車内部ネットワークへの不正侵入を阻止することができ，従来の自動車の安全性を保ちつつ高度 IT 融合社会を支えるための信頼性を備えることが可能となる．またセキュリティ対策を施す対象をセキュリティ・ゲートウェイ・ECU に限定することにより，**2020 年東京オリンピックまでという短期間での実用化目標に合致した提供が可能である【課題 1 関連】**.

1. 外部接続ネットワークより車載内部 ECU へのセキュリティ脅威を排除する．
   利用シナリオに基づき，攻撃リスクの 80%以上を低減する．評価は，IPA による共通脆弱性評価システム CVSS, 日立製作所 森田らによる車載システム向けセキュリティ分析支援ツール，Carleton 大学 Laurendeau らによる脅威事象ランク付け手法などを参考として実施する．
2. 一般的な攻撃手法には対処する
   なりすまし，DoS 攻撃，中間者攻撃，バックドア，ポートスキャン，改ざん，サイドチャネルなど一般的な攻撃に対処する．

○PUF 搭載セキュリティチップの開発

本事業では，次世代セキュリティ技術として注目を集めており実用化研究が盛んな **PUF (Physical Unclonable Function) 技術を活用(対策 2)**する．PUF は LSI 製造時に生じる物理特性のわずかなばらつきを利用して，いわばマイコン固有の指紋情報を生成する技術であり，従来技術ではメモリ上に保存する必要のある機器固有の認証情報の代わりとなるものである．つまり，PUF をセキュリティチップに搭載することにより，EVITA 等では必要な「鍵情報のためのセキュア保存領域」が不要となる．これにより，鍵情報の偽造や窃取が不可能となることから耐攻撃性を向上できると同時に，製造時の鍵管理にかかるコストを低く抑えることができる．車載環境における実用化のためには PUF の信頼性・安定性を確保するため技術が必要となるため，従来から研究を進めている立命館大学の知見を活用する．こうした**自動車の IT セキュリティ対策に PUF を利用する試みは他に類がなく，わが国のアドバンテージとすることができる．【課題 2 関連】**.

1. 国内技術を用いた国内セキュリティチップを試作する．
   立命館大学のシーズ技術である PUF 技術と暗号技術を活用し，国内チップベンダーの協力で FPGA 上で稼動する対攻撃性を高めたセキュリティチップを開発する．

○IEC 62443 準拠の開発

対策 1 および対策 2 で開発した技術により，耐攻撃性を向上させることはできる．しかし，これらの技術を国際規格に準拠したプロセスで開発しなければ，万が一攻撃により被害を被った場合の保障側面を有することができず，欧米への輸出への足かせとなる恐れがある．

そのため，対策 1 および対策 2 の技術を**制御機器セキュリティ規格である IEC 62443 に準拠して開発(対策 3)することにより，国内の規格対応知見を蓄積する【課題 3 関連】**.

1. IEC62443 の要求事項に準拠したセキュリティ・ゲートウェイ・ECU のセキュリティコンセプトを開発する．
   国際認証機関より適合性の評価を受けることで，セキュリティコンセプトが規格に準拠できていることを最終年度までに確認する．

1－2 研究体制

本事業の研究開発体制を以下に示す.

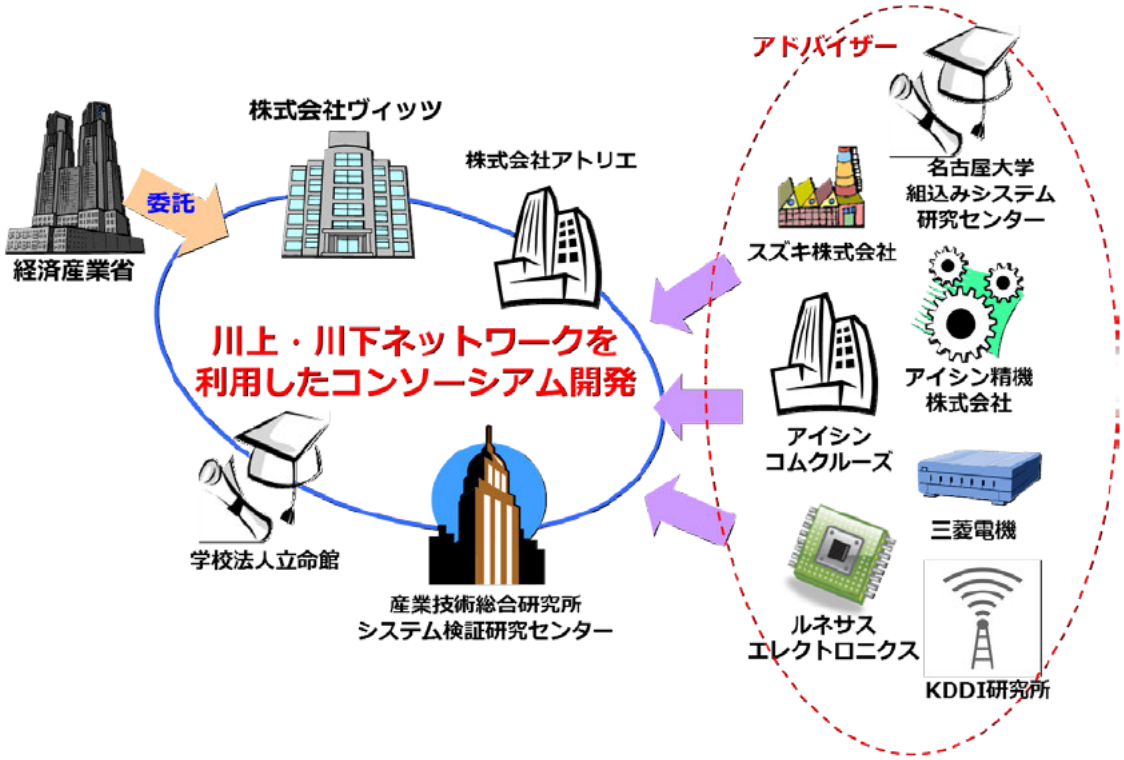
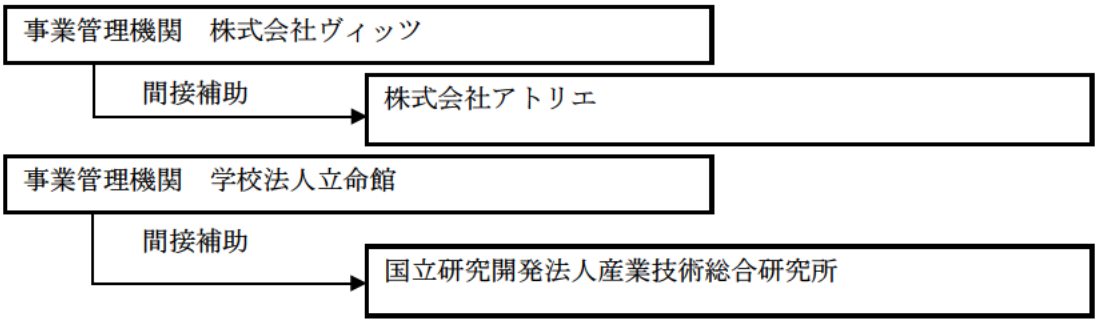


図 1-2 研究開発体制図



研究員

【事業管理機関】株式会社ヴィッツ

氏　名	所属・役職	備考
武田英幸	技術本部　執行役員	PL
杉山歩	組込セキュリティ PF 開発部 組込セキュリティ PF 開発室　室長	
井上博雄	組込セキュリティ PF 開発部 組込セキュリティ PF 開発室　マネージャ	
平井伸幸	組込セキュリティ PF 開発部 組込セキュリティ PF 開発室　チーフエンジニア	

松井康治郎	組込セキュリティ PF 開発部 組込セキュリティ PF 開発室	
紅谷明宏	組込セキュリティ PF 開発部 組込セキュリティ PF 開発室	
谷口賢司	組込セキュリティ PF 開発部 組込セキュリティ PF 開発室	
後藤孝一	高信頼性 PF 開発部 スマートシステム統合 PF 開発室　室長	
宮田亜美	高信頼性 PF 開発部 スマートシステム統合 PF 開発室	
安藤萌	高信頼性 PF 開発部 スマートシステム統合 PF 開発室	
澤田貴裕	高信頼性 PF 開発部 スマートシステム統合 PF 開発室	
山田竜正	高信頼性 PF 開発部 スマートシステム統合 PF 開発室	
荒川まり子	高信頼性 PF 開発部　高信頼性 PF 開発室 グループリーダー	
藤井祥人	高信頼性 PF 開発部　高信頼性 PF 開発室 グループリーダー	
深見修一郎	高信頼性 PF 開発部　高信頼性 PF 開発室	
出口雅也	高信頼性 PF 開発部　高信頼性 PF 開発室	
井上欣也	高信頼性 PF 開発部 オートモーティブ標準 PF 開発室　室長	
森祐也	高信頼性 PF 開発部 オートモーティブ標準 PF 開発室	
原浩晃	機能安全開発部　設計・技術開発室	
堀田有彩	機能安全開発部　設計・技術開発室	
石川義也	機能安全開発部　プロセス支援室	

【間接補助事業者】株式会社アトリエ

氏　名	所属・役職	備考
水口大知	取締役	
高村博紀	エキスパートエンジニア	
山口光樹	チーフ・エンジニア	
石山康介	エキスパートエンジニア	
平井誠	エキスパートエンジニア	

【事業管理機関】 学校法人立命館

氏　名	所属・役職	備考
冨山宏之	理工学部理工学部電子情報工学科　教授	SL
藤野毅	理工学部理工学部電子情報工学科　教授	
熊木武志	理工学部理工学部電子情報工学科　准教授	
汐崎充	総合科学技術研究機構　准教授	
久保田貴也	総合科学技術研究機構・研究員	

【間接補助事業者】国立研究開発法人産業技術総合研究所

氏　名	所属・役職	備考
堀洋平	ナノエレクトロニクス研究部門，主任研究員	
片下敏宏	ナノエレクトロニクス研究部門，主任研究員	
藤原充(研究補助員)	ナノエレクトロニクス研究部門，第 2 号契約職員	
恩田泰則(研究補助員)	ナノエレクトロニクス研究部門，第 2 号契約職員	

1－3 成果概要

○セキュリティ・ゲートウェイ・ECUの開発

本事業では，クラウドを経由したサイバー攻撃から車載システムを守ることに焦点を当て，自動車内部の制御機器と外部機器との間のセキュアな通信を確保するためのセキュリティ・ゲートウェイ・ECU を研究開発した．

リプログラミングシステムをユースケースとして，まず，セキュリティ・ゲートウェイ・ECUの仕様開発から行った．その後，セキュリティアーキテクチャを設計し，ソフトウェア，ハードウェアの機能分担を行った．ハードウェアはFPGAにPUF(Physical Unclonable Function)を活用したセキュア統合回路を開発した．ソフトウェアは，AUTOSARをベースとして，インターネット側も動作させる為に，TLS(Transport Layer Security)/SSL(Secure Socket Layer)，TCP/IP，Etherドライバの実装を行った．車載ネットワーク側(CANバス側)は，AUTOSARのSecOC仕様に準拠したセキュリティ対応モジュールを実装した．

また，同じく自動車業界で標準的に利用されているUnified Diagnosis Services （UDS）仕様におけるSecurity Accessのステップに，PUF技術を活用した暗号鍵管理プロトコルの導入提案を行う事もできた．

初年度からハードウェアの核となるPUFは，その特徴である「ばらつき」に関する性能を改善し，ソフトウェアは，CAN MAC(Message Authentication)の性能改善を行い，最終的には，リプログラミングシステムの中で，HSM(Hardware Security Module)の搭載されたECU，PUFの搭載されたECU，ハードアシストのないソフトウェアでセキュリティ処理を実行するECUの3種類に対して，リプログラミングを比較評価できる環境をくみ上げ，性能差や混在環境での挙動などを実証できるようにした．

これにより今後の車載に必要となるセキュリティ・ゲートウェイ・ECUの原型開発が完了し，短期間でのセキュリティ対策が行える成果をあげる事ができた．

○PUF搭載セキュリティチップの開発

本事業では，次世代セキュリティ技術として注目を集めており実用化研究が盛んなPUF (Physical Unclonable Function) 技術を活用した．PUFはLSI製造時に生じる物理特性のわずかなばらつきを利用して，いわばマイコン固有の指紋情報を生成する技術であり，従来技術ではメモリ上に保存する必要のある機器固有の認証情報の代わりとなるものである．

本事業では，FPGAを用いてPUFとAESの暗号回路を統合し，セキュリティの要となる鍵が漏洩しない統合回路をくみ上げ，セキュリティ・ゲートウェイ・ECUと通信相手となる各ECU間でのCAN MAC(Message Authenticaion Code)への応用事例を示す事ができた．この鍵管理の事例は，国際的なESCARなどの学会でも発表しており，他の類を見ない成果である．

○IEC 62443準拠の開発

セキュリティ・ゲートウェイ・ECUの開発及びPUF搭載セキュリティチップの開発を実施する上で，リプログラミングシステムをユースケースとして，第三者認証機関である独TÜV SÜDにコンサルを受け，その後，制御セキュリティ規格であるIEC62443に準拠する為の要求レベルを把握，セキュリティコンセプトの文書であるセキュリティ管理計画書(SMP)，セキュリティ要求仕様書(SRS)，セキュリティアーキテクチャ設計書(SAD)を作成し，技術レビューを受け、「Principal is OK !」という評価を貰い，妥当である事が確認できた．本活動はH27年度で上記，IEC62443への適合性評価として「Principal is OK !」とのコメントを頂くレベルに到達した為，H28年度は実施せず、セキュリティ・ゲートウェイ・ECUの開発及びPUF搭載セキュリティチップの開発に注力する事とした．

1－4 当該研究開発の連絡窓口

＜事業管理者＞
株式会社ヴィッツ
愛知県名古屋市中区栄2-13-1 名古屋パークプレイス

＜統括研究代表者＞
株式会社ヴィッツ
組込システム事業領域統括
組込セキュリティPF開発部　部長
取締役　　武田 英幸
TEL：052-220-1218　FAX：052-218-5855
E-mail：takeda@witz-inc.co.jp

第２章 セキュリティ・ゲートウェイ・ECUの開発

２－１ セキュリティ･ゲートウェイ･ECU 仕様開発

◆概要

セキュリティ・ゲートウェイ・ECUの要求仕様を定義する．すなわち，自動車メーカもしくは電装部品メーカが求めるセキュリティ･ゲートウェイ･ECUの基本仕様（ハードウェアリソースなど）の検討に加えて，セキュリティ関連特性を決定する．すなわち，セキュリティ・ゲートウェイ・ECUの利用シナリオに基づいて厳格にセキュリティ脅威を分析しリスクを見積もった上で，耐攻撃性目標および方策，PUF特性(生成する識別情報の信頼性目標など)，暗号回路特性(暗号種別，暗号長，処理時間など)を決定し，セキュリティ・ゲートウェイ・ECUの要求仕様を開発する．

２－１－１ 遠隔リプログラミングシステムの基本仕様策定

【目標】

従来のリプログラミング方法は，OBD2ポートからリプログラミング用ツールを接続しなければならないため，車をカーディーラなどへ持ち込み，専任の技術者が実施する必要がある．それに対して，遠隔リプログラミングシステムを利用することで，3GやLTEなどの回線を利用して，自宅の駐車場でリプログラミングを実施可能であることから，ユーザ負担の軽減，および，リコール費用の削減を見込むことができる．

そのため，本研究の開発ターゲットであるセキュリティ・ゲートウェイ・ECUを使用するシステムとして，車載制御システムにおいて遠隔処理でECUの制御プログラムを書き換えるシステム（Reprogramming System）を定義する．

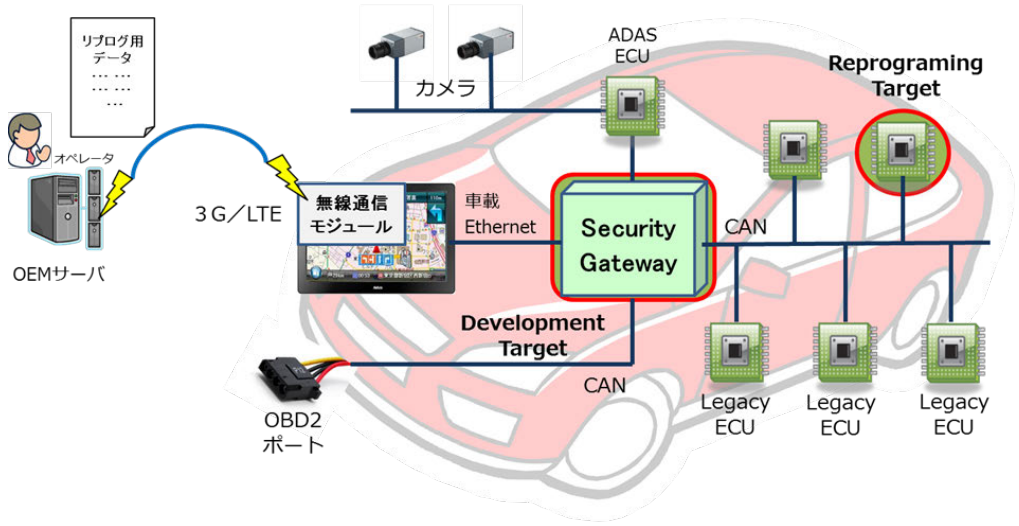


図2-1 遠隔リプログラミングシステムとセキュリティ･ゲートウェイ･ECUの関係

【研究成果】

本研究で開発する遠隔リプログラミングシステムでは，OEM Server からマルチメディアシステム，および，セキュリティ・ゲートウェイ・ECU を経由して，Reprograming Target にリプログラミング用データを送信する．本研究で開発する遠隔リプログラミングシステムの構成図，および，リプログラミングシーケンスを以下に示す．

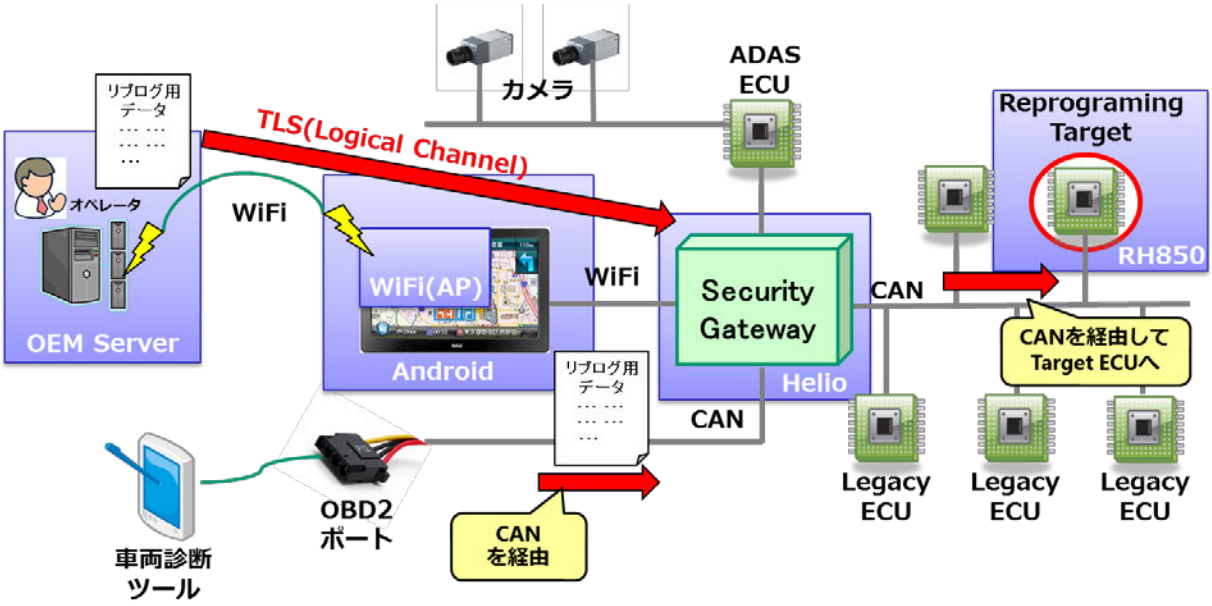


図2-2　遠隔リプログラミングシステムの構成図

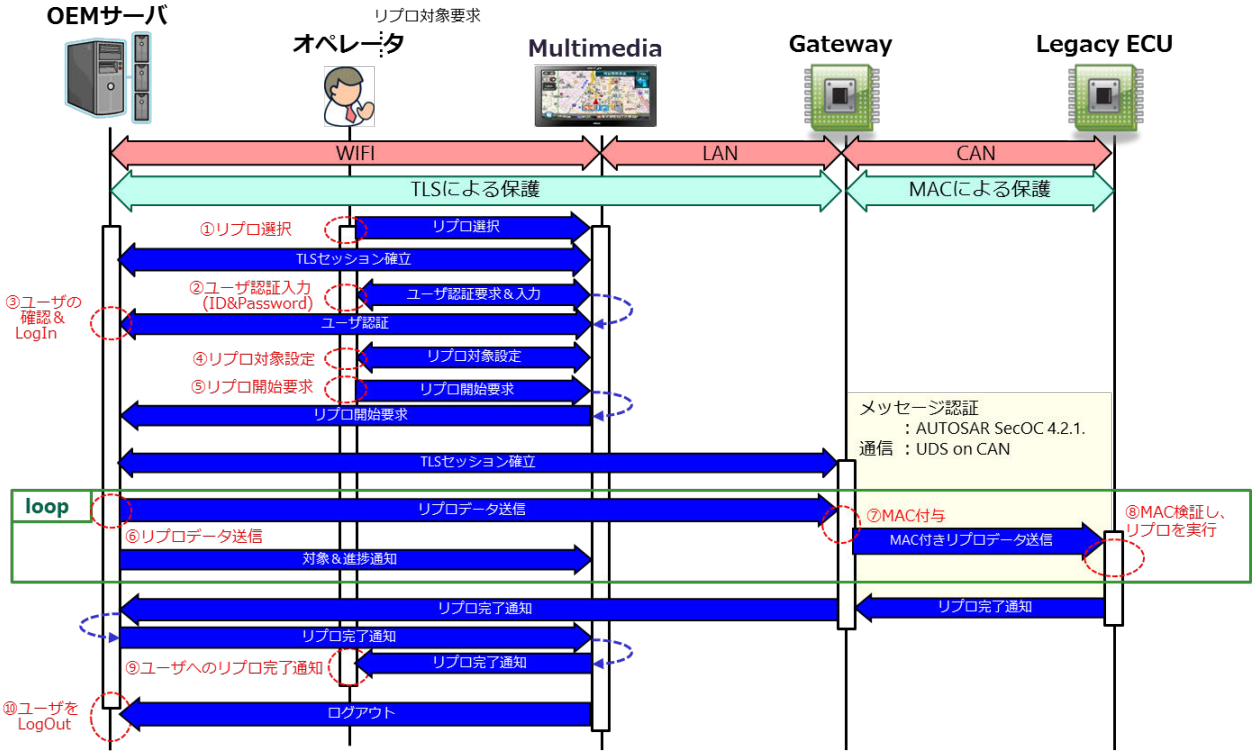


図2-3　遠隔リプログラミングシステムのシーケンス図

【課題】

実際の自動車システムでは，以下の一覧に示す通信プロトコルが利用されている．本研究では，これら全てを対象とすることはできない．そのため，本研究では，以下に示す通信プロトコルのうち，制御系通信プロトコルの代表であるCANと，無線通信プロトコルの代表としてWi-Fiをターゲットとした．

表2-1　車載システムで利用される通信プロトコルの一覧

No.	通信プロトコル	概要
1	CAN	Controller Area Network (CAN) は，耐ノイズ性の強化を考慮して設計され，相互接続された機器間のデータ転送に使われる規格.
2	LIN	車両のバックボーン・ネットワーク以外の用途で，CANほど高いデータ伝送速度が求められない低コストのサブネットワークに向けて開発された.
3	FlexRay	FlexRayは，車載向け通信バスシステムの標準規格．確定性が高い上に，フォールトトレラント機能があり，データ伝送速度が高いことが特徴.，
4	車載Ethernet	オフィス内など一般的に利用されるEthernetはリアルタイム通信を保証していないので，例えば動画を転送して再生する際などに，どうしてもタイムラグが発生する恐れがある．これを解決してリアルタイム動作，大容量データ伝送を実現したのがEthernet AVBである.
5	MOST	Media Oriented Systems Transport（MOST）は，自動車などの輸送機械で，マルチメディア装置間を接続するために策定されたコンピュータネットワーク規格である.
6	USB	ユニバーサル・シリアル・バス（英語: Universal Serial Bus，略称 USB，ユーエスビー）は，コンピュータ等の情報機器に周辺機器を接続するためのシリアルバス規格の1つである.
7	Wi-Fi	Wi-Fi（ワイファイ，英: Wireless Fidelity）は，無線LANの規格のひとつ. Wi-Fi Alliance (米国に本拠を置く業界団体) によって，国際標準規格であるIEEE 802.11規格を使用したデバイス間の相互接続が認められたことを示す名称.
8	Bluetooth	Bluetooth（ブルートゥース，ブルーツース）は，デジタル機器用の近距離無線通信規格の1つである．数mから数十m程度の距離の情報機器間で，電波を使い簡易な情報のやりとりを行うのに使用される.
9	DSRC	DSRC（Dedicated Short Range Communications）は，車両との無線通信に特化して設計された5.8GHz帯のISMバンドを用いた一方向，または双方向の無線通信技術.
10	3G/4G(LTE)	LTE（Long Term Evolution）は，新たな携帯電話の通信規格である．仕様は標準化団体である3GPPにて3GPP Release.8内で2009年3月に凍結された.

本研究成果を実際の車両システムに対して適用するためには，本研究で対象とできなかった通信プロトコルを利用したユースケースを拡張する必要がある．

2－1－2 脅威分析およびリスク分析の実施

【目標】

本研究では，セキュリティ・ゲートウェイ・ECU を利用する想定システムとして定義した遠隔リプログラミングシステムにおいて考えらえる「セキュリティ上の脅威」へ対抗するためのセキュリティ要件を導出するために，Attack Tree を利用する．Attack Tree で脅威を実現する具体的な攻撃手法を導出し，その攻撃を防ぐためのセキュリティ要求を導出する．

【研究成果】

本研究では，遠隔リプログラミングシステムが攻撃されることで重篤度が高い脅威へと繋がるアセット（保護資産）の一覧を洗い出し，それに対して考えられる攻撃手法を導出した．本研究では，ここで導出した攻撃手法への対抗策をセキュリティ要件として定義した．

表 2-2 脅威を実現するための攻撃手法を導出するためノード一覧

No.	Asset	Root Node
1	Software Image	Software Image に攻撃を加え，Legacy ECU の制御に不調を発生させる．
2	Update Finish Information	Update Finish Information に攻撃を加え，Reprogramming system に不調を発生させる．
3	Car-ID	Car-ID に攻撃を加え，Reprogramming system に不調を発生させる．
4	Software Version List	Software Version List に攻撃を加え，Legacy ECU の制御に不調を発生させる．
5	Repeat Request	Repeat Request に攻撃を加え，Reprogramming system に不調を発生させる．

◆攻撃手法の導出

本研究では，上記 5 つのアセットに対してそれぞれ Attack Tree を作成した．ここでは，そのうちの 1 つを事例として示す．

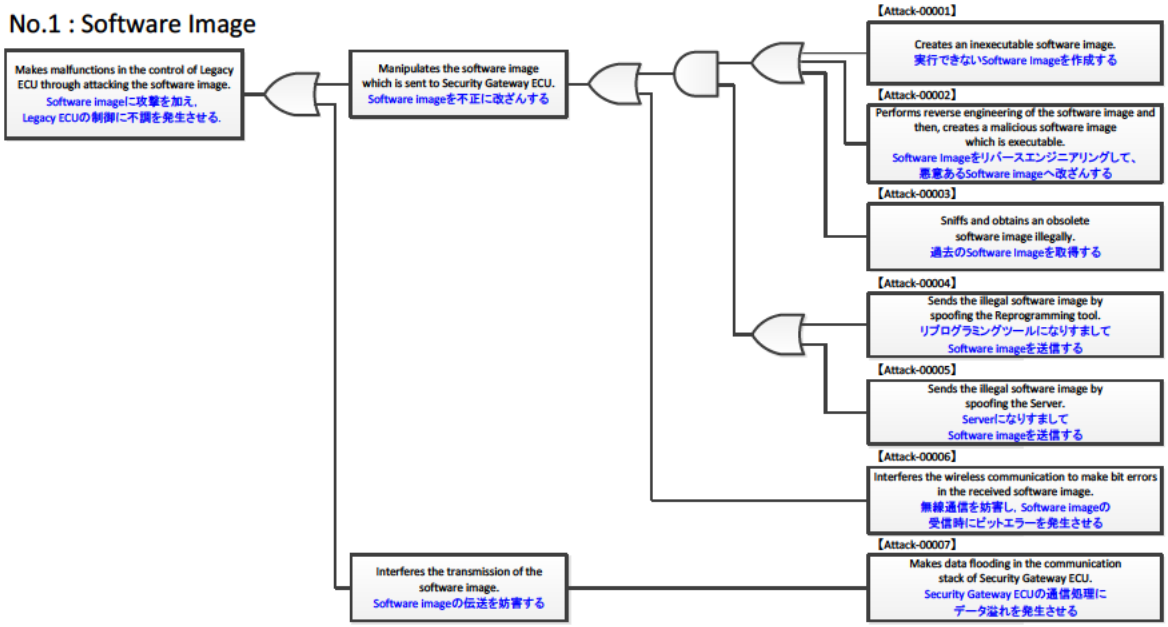


図2-4 Attack Treeを利用した攻撃手法の導出事例

【課題】

本研究で定義した Attack Tree は，国際認証機関である TÜV SÜD による第三者レビューを受け，その妥当性を確認したため，残課題はない.

２－１－３　脅威に対抗するためのセキュリティ機能仕様の導出

【目標】

本研究では，脅威分析の結果から，セキュリティ・ゲートウェイ・ECU に搭載すべきセキュリティ機能仕様を導出する．なお，セキュリティ機能仕様を実現する際には，PUF 技術を利用することで，その実用化検討を行う．

【研究成果】

脅威分析の結果から，導出したセキュリティ機能仕様を以下に示す．

1. Session keyを利用したリプログラミング用ソフトウェアイメージの保護仕様
2. Pre-shared symmetric keyを利用してSession keyをセキュアに生成するための保護仕様
3. Pre-shared symmetric keyをセキュアに交換するための保護仕様
4. Audit Log keyを利用してリプログラミングログを保護するための仕様
5. Boot keyを利用してセキュリティ・ゲートウェイ・ECU自身の完全性を検証する仕様

本報告書では，上記の 5 つのうち，1 の“Session key を利用したリプログラミング用ソフトウェアイメージの保護仕様”を一例として以下に示す．

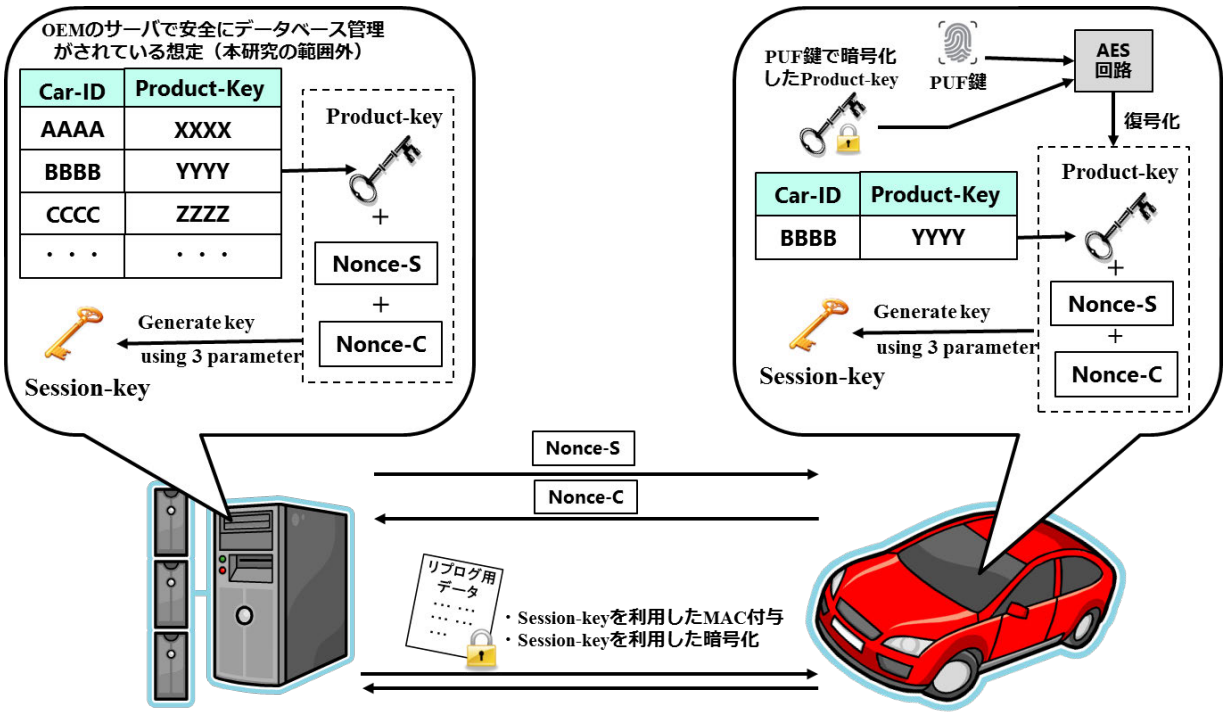


図2-5　セキュリティ・ゲートウェイ・ECUに搭載するセキュリティ機能

【課題】

本研究で策定したセキュリティ・ゲートウェイ・ECU のセキュリティ機能仕様は，国際認証機関である TÜV SÜD による第三者レビューを受け，その妥当性を確認したため，残課題はない．

2－1－4　セキュリティ･ゲートウェイ･ECUのアーキテクチャ設計

【目標】

セキュリティ・ゲートウェイ・ECU に搭載するセキュリティ機能仕様を実現するためのセキュリティアーキテクチャ設計を行い，セキュリティ・ゲートウェイ・ECU のハードウェア開発，および，ソフトウェア開発を行うための仕様を導出する．

【研究成果】

本研究で作成したシステムレベルのセキュリティアーキテクチャ設計の構成，および，構成要素（Product）に割り付けたセキュリティ機能要求を以下に示す．

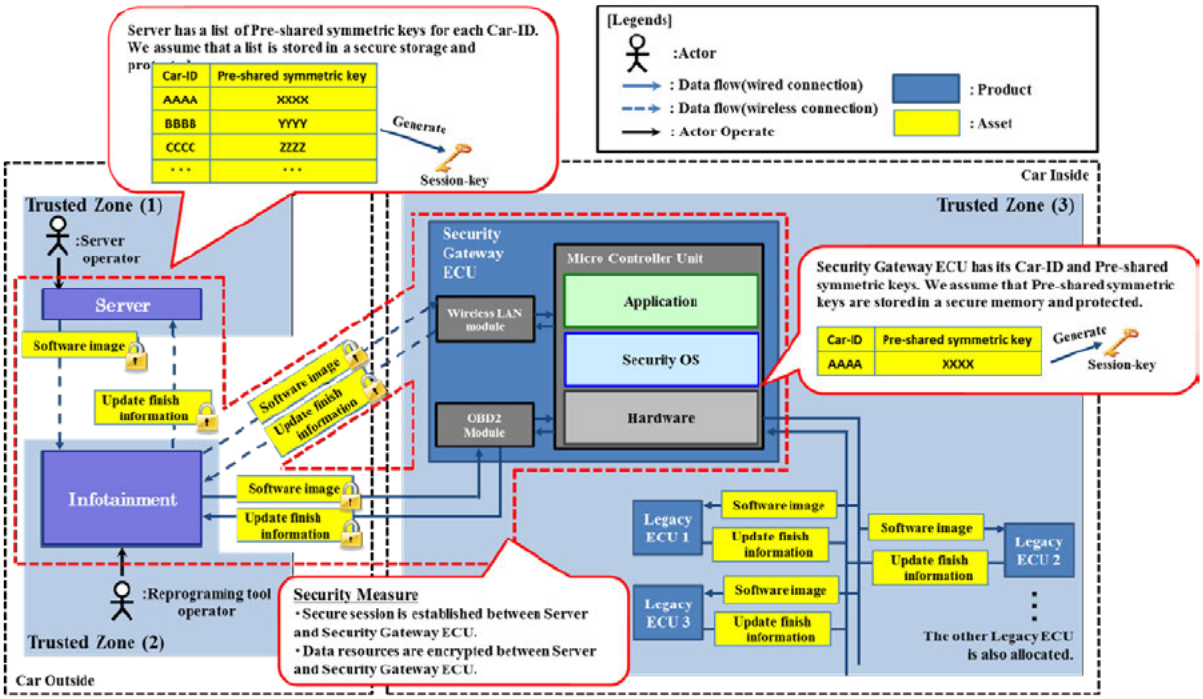


図2-6　想定システムに対するセキュリティアーキテクチャ設計（一部）

表2-3　想定システムのアーキテクチャから導出したセキュリティ機能要求

Product	Description of Security Requirement (Product Level)
Server	Server は，Car-ID と Pre-shared symmetric key の対応リストを保管すること．Car-ID と Pre-shared symmetric key は 1 対 N (N=2)に対応する【SecOS-SW-01-SRS-10001】. Server は, Car-ID それぞれの Pre-shared symmetric key リストの中で，Pre-shared symmetric key に付随するいくつかの情報を保持する． ・キーを識別するための ID 値 ・キーが危殆化しているかを示すフラグ ・キーが過去何回使用されたかの回数 Note：対応リストは，OEM の情報セキュリティ管理により保護されセキュアストレージへ格納される想定である．
	Server は，Pre-shared symmetric key を利用して，Security Gateway ECU と Session key の合意をするための機能を持つこと．Server および Security Gateway ECU は，Session key を利用して Data Asset のセキュリティ特性を保証する．これは，Pre-shared symmetric key の利用頻度を下げることで，鍵が危殆化するリスクを低減するためである．

Product	Description of Security Requirement (Product Level)
Infortainment	Infortainment は，無線 LAN 通信の制御ソフトウェアと他のソフトウェア間で独立性を保ち，リプログラミング処理を維持するための機能を持つこと【SecOS-SW-01-SRS-10002】. Note：Infortainment には汎用 OS が採用され，MMU などを利用した一般的なパーティショニング機能が搭載されている想定である.
Security Gateway ECU	Security Gateway ECU は，Car-ID と車に対応する Pre-shared symmetric key を保管すること．Pre-shared symmetric key は，製造時にセキュアストレージへ格納される想定である【SecOS-SW-01-SRS-10003】. Note：セキュアストレージは，アクセス権限を持たないアプリケーションからの不正な読出しから格納されたデータを保護する機能を持つ.
	Security Gateway ECU は，Pre-shared symmetric key を利用して Server と Session key を合意するための機能を持つこと.
	Security Gateway ECU は，Audit Log の真正性，および，完全性を保つために，MAC の生成／検証機能をもつこと．Security Gateway ECU は, Audit Log 管理に利用する Audit Log key を製造時に Secure Storage へ保管すること【SecOS-SW-01-SRS-10096】.
	Security Gateway ECU は，無線 LAN 通信の制御ソフトウェアと他のソフトウェア間で独立性を保ち，リプログラミング処理を維持するための機能を持つこと【SecOS-SW-01-SRS-10004】.
	Security Gateway ECU は, 自身の完全性を保証するための Secure Boot 機能を持つこと【SecOS-SW-01-SRS-10078】．Security Gateway ECU は，Secure Boot 機能に利用する Boot key と Boot MAC を製造時に Secure Storage へ保管すること【SecOS-SW-01-SRS-10097】. なお，Security Gateway ECU における Software image がリプログラミングする際には，新しい Software image に対応する Boot MAC が Server によって演算され，Software image と合わせてリプログラミングされる【SecOS-SW-01-SRS-10098】.

【課題】

本研究で定義したセキュリティ・ゲートウェイ・ECU のアーキテクチャ設計は，国際認証機関である TÜV SÜD による第三者レビューを受け，その妥当性を確認したため，残課題はない.

２－１－５　自動車業界向け研究成果の活用検討

【目標】

国際標準規格で策定されているリプログラミングシーケンスでは，リプログラミングデータの完全性，および，真正性を保証するための仕組みが明記されていない．そのため，本研究活動にて，UDS on CAN に対してセキュリティ機能としてメッセージ認証の仕組みを追加する．

【研究成果】

本研究では，国際標準規格で策定されているリプログラミングシーケンスにおいて，セッション鍵の生成&配布を行う機能を追加する．該当箇所を記した図を以下に示す．

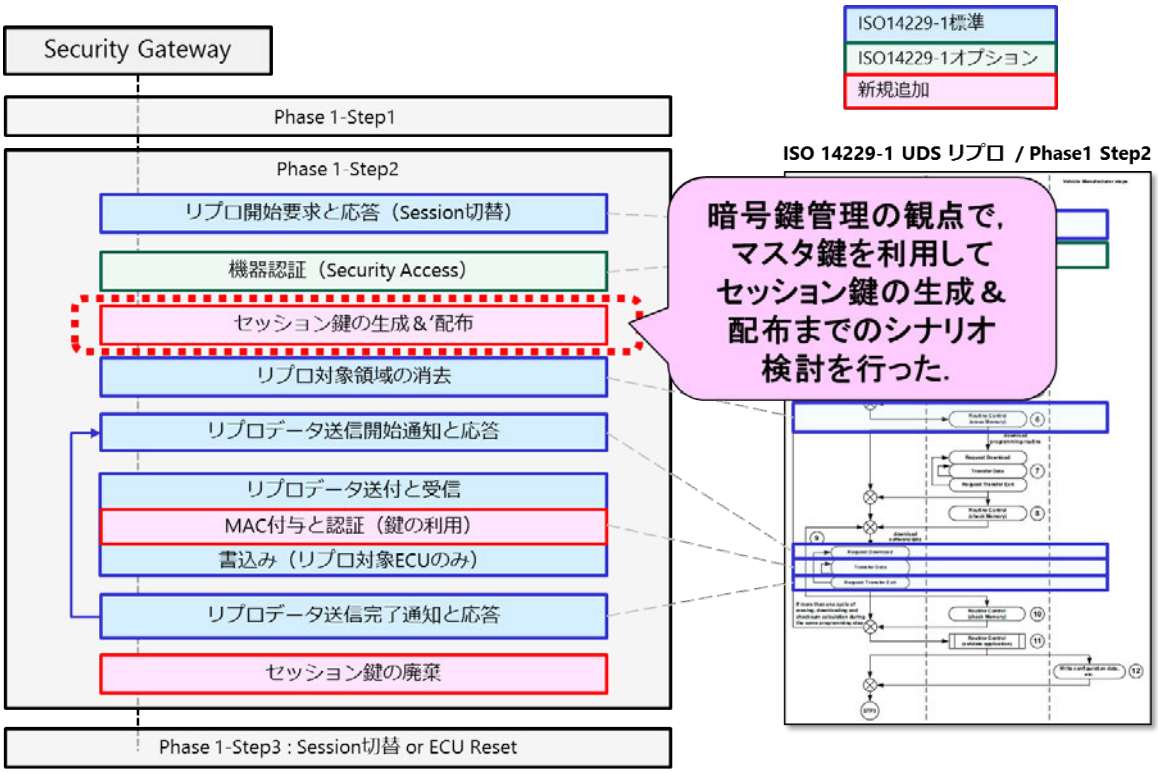


図2-7　セッション鍵の生成と配布を行うタイミング

上記に示すリプログラミングシーケンスにおいて，セッション鍵を交換するシナリオとして，セキュリティ・ゲートウェイ・ECU で生成したセッション鍵を制御 ECU に対して配布する手段として，HSM に格納されたマスタ鍵を利用する場合と，PUF を利用する場合とでは，実行すべき処理シーケンスが異なる．

その両方のケースの特徴と，それぞれを実現するための比較検討を行った結果を以下に示す．

要素 / 方式	生成	配布時に扱うデータ	利用済み鍵の扱い	事前共有鍵（Master鍵）
HSM（SHE）	乱数より生成	暗号化	破棄	必要（SHEの鍵更新で利用）
PUF	事前に対象ECUで生成	平文	再利用	不要

図2-8　HSM／PUF利用時のセッション鍵の生成と配布に必要な情報の違い

【課題】

PUF を利用する場合には，事前に使用する鍵と対象となる PUF を搭載した ECU を用いて，PUF 情報（ECU に保存された Challenge＆Helpler データに対応する Cipher 鍵）を生成し，GW はそれらを保持するメモリが必要となる．メモリのサイズには上限があるため，使用できる鍵が事前に生成＆管理している本数となり，一般的なセッション鍵の様に鍵を使い捨てるような使い方は実現できない．

但し，車両システムでの鍵の本数に上限がある事は，適応するシステムにおける鍵のライフサイクルに依存するため，一概に課題となるとは言えない．

2－2 セキュリティ･ゲートウェイ･ECU ハードウェア開発

◆概要

セキュリティ・ゲートウェイ・ECU 仕様開発の成果である，PUF 仕様および暗号回路仕様からセキュリティ・ゲートウェイ・ECU のハードウェア開発を行う．カスタム設計されたマイコンチップの開発には億単位の金額を要するため，本研究では FPGA 上にセキュリティチップを実現する．そのため，FPGA にて実現可能なマイコンコアのうち，国内半導体メーカで製品化が可能な ARM コアを採用する．このコア周辺の FPGA 上に PUF 回路および暗号回路を HDL にて回路設計を行う．

2－2－1 ベーシックシステムの開発

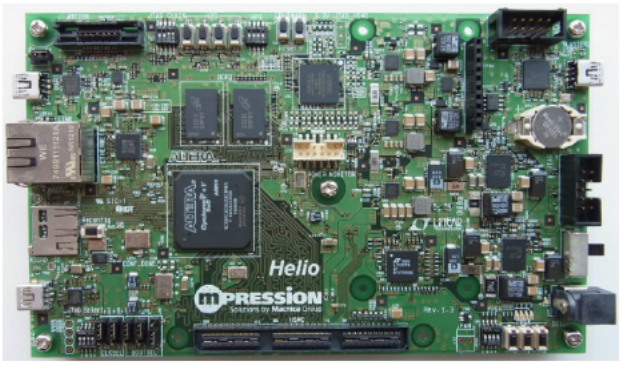
【目標】

本研究におけるコア技術である PUF 技術の確立，および，その評価を行うためのベーシックシステムとして，ターゲットハードウェア上で CAN ネットワークを実現するための HW 開発を実施した．

【研究成果】

本研究事業ではハードウェア開発のプラットフォームとして，AUTOSAR 仕様の車載リアルタイム OS の開発・動作実績のある Altera 社の FPGA ボードを使用した．図 2-9 に本 FPGA ボードの概観と仕様を示す．

CPU としては，組み込み用としてもっとも普及している ARM コアが 2 個と 1GB のダイナミックメモリも搭載されており，Linux などの汎用 OS も起動するため，汎用的な開発ツールが使用できる．前述の AES-128 ハードウェアモジュールおよび PUF のほかに，車載 ECU の通信機能の実現のために必須である，CAN コントローラの開発を行った．



FPGA	5CSXFC5C6U23C7N (デュアルコア ARM® Cortex(TM)-A9 プロセッサ搭載)
コンフィギュレーション	USB 経由 (オンボード USB Blaster II)
	コンフィギュレーションデバイス
	JTAG
電源デバイス	LTC2978 (PSM), LTC3605 x 3, LTC3613 x3 , LTC3026, LT3509
インタフェース	HSMC, Gigabit Ethernet, UART, USB 2.0 OTG, SD card, GPIO, LCD
メモリ	Micron DDR3 1GB @ 32bit @ 400MHz
型番	ALTHELIOSOC-C5
その他	Real Time CLK, Buttons, LEDs, Switches, Linear technology Power monitor

図2-9 本事業で使用するAltera製FPGAボード

【課題】

ここで開発した成果を，以降に記すPUF技術，および，セキュアな統合回路を実装するためのベースシステムとして利用した実績があり，残課題はない．

２－２－２ FPGA向けPUF技術の設計／評価

【目標】

同ターゲットボードは FPGA を搭載しているため，FPGA の特性を考慮したPUF を開発した．ベースとなる PUF は，必要に応じて研究実施者が保有する基礎研究成果を応用し，Altera FPGA上で動作するPUF を評価・設計した．PUF はその期待される機能から，以下の 2 つの指標が重要であるがこの観点ついて重点的に評価を実施した：

1. **再現性**　　同じ個体から安定的に同じ ID が出力される特性
2. **ユニーク性**　　異なる個体からは差異がある（似ていない）ID が出力される特性

【研究成果】

データのサンプルを収集し統計的に分析・評価を実施した．その評価結果を反映させ FPGA に適した PUF 回路の構築を実施した．

今後，上記の特性結果を踏まえてPUF出力の誤り訂正符号回路の仕様に反映させる．

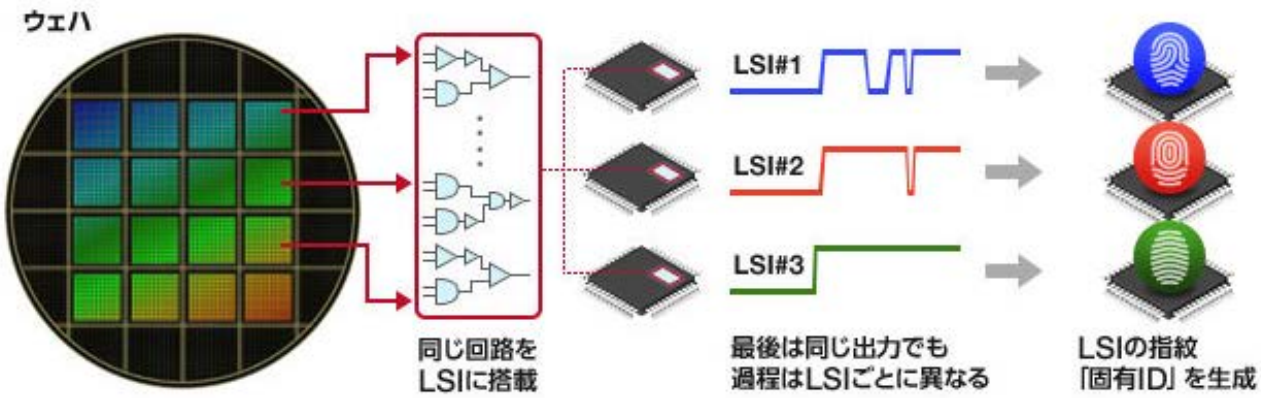


図2-10　同じ回路から固有IDが生成される仕組み

http://mitsubishielectric.co.jp/corporate/randd/spotlight/a26/index.html **より引用**

◆Pseudo-LFSR PUF のユニーク性の評価，および，性能改善

前年度に引き続き，Altera FPGA 上で動作する PUF の開発とその評価を進めた．先行検討により，Xilinx 社製 FPGA 上で動作する PL-PUF を Altera 社製 FPGA CycloneV SoC 上に移植し PUF-ID を取得できるようになった．しかし，生成される PUF-ID を確認したところ，異なる個体の間で生成される PUF-ID がほぼ同一となり，期待するような「個体間の差異」を確認することができなかった．これらの結果を受けて，FPGA の回路を構成する論理素子の構造を確認し，より良好な ID 生成が可能となるように検証・改善を進めた．要因を分析したところ，以下に示す2つに原因があることがわかった．

1）通常の実装方法では論理合成時に回路が最適化されてしまい PUF 回路の構造が維持できない（また最適化を OFF にするオプションがない）
2）LUT（Look-Up Table）や MUX（Multiplexer)といった基本構成要素（プリミティブ）を直接記述することができない

それらを解決するために，以下の3段階のアプローチを取った．

1）PL-PUFを構成するブロックをユーザIP (Intellectual Property) として固定し，デザインを維持する
2）固定したブロックを等間隔に配置し，またデータ取得クロックの高速化する
3）ブロック内のリソース位置を固定（ブロック内での LUT・フリップフロップの位置を固定する

その結果として，**図 2-11**に示すように理想値（=64bit）に近いユニーク性を実現することができた．

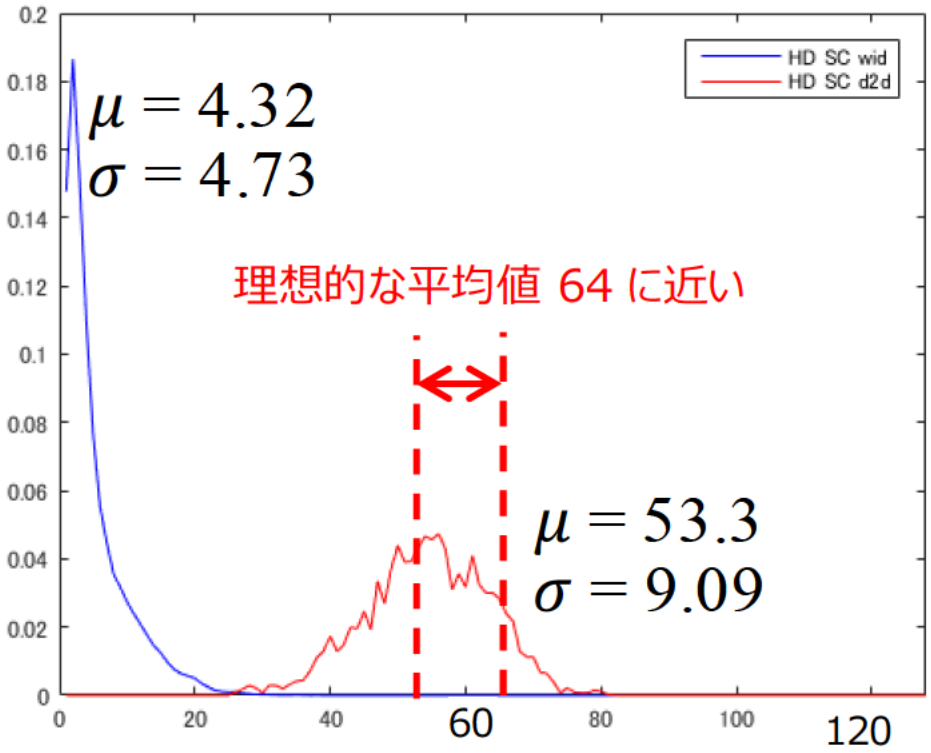


図 2-11 改善した PL-PUF の PUF-ID 出力（128bit）

【課題】

FPGAの各論理セルのレイアウトを適切に変更することで，PL-PUF から得られるレスポンス (PUF-ID) の大幅なユニーク性向上に成功した．しかし，実験で得られたInter-HD SC (Inter Hamming Distance Same Challenge) の値は53.3 であり，理想値からはまだ 10bit 程度の開きがある．今後は，さらなるレイアウト変更・コンフィグレーション変更等により Inter-HD を理想値に近づけることが一点目の課題である．加えて，電圧変動・温度変化によりどのように PUF-ID が変化するかといった対環境性能を評価することが二点目の課題である．

2－2－3 セキュアな統合回路の開発

【目標】

本研究にて開発したFPGA向けのPL-PUF回路とAES回路の協調動作を実現する「統合セキュリティ回路」の基本仕様を策定し，FPGA上にプロトタイプシステムの開発することを目標とする．

【研究成果】

本研究では，Altera FPGA SoC 上に AES, PUF, 誤り訂正回路を含む Fuzzy Extractor 回路を構築，それらを内包するコア回路を構築する．重要な秘密情報はコア回路内部で閉包させ，漏えいを防止する．

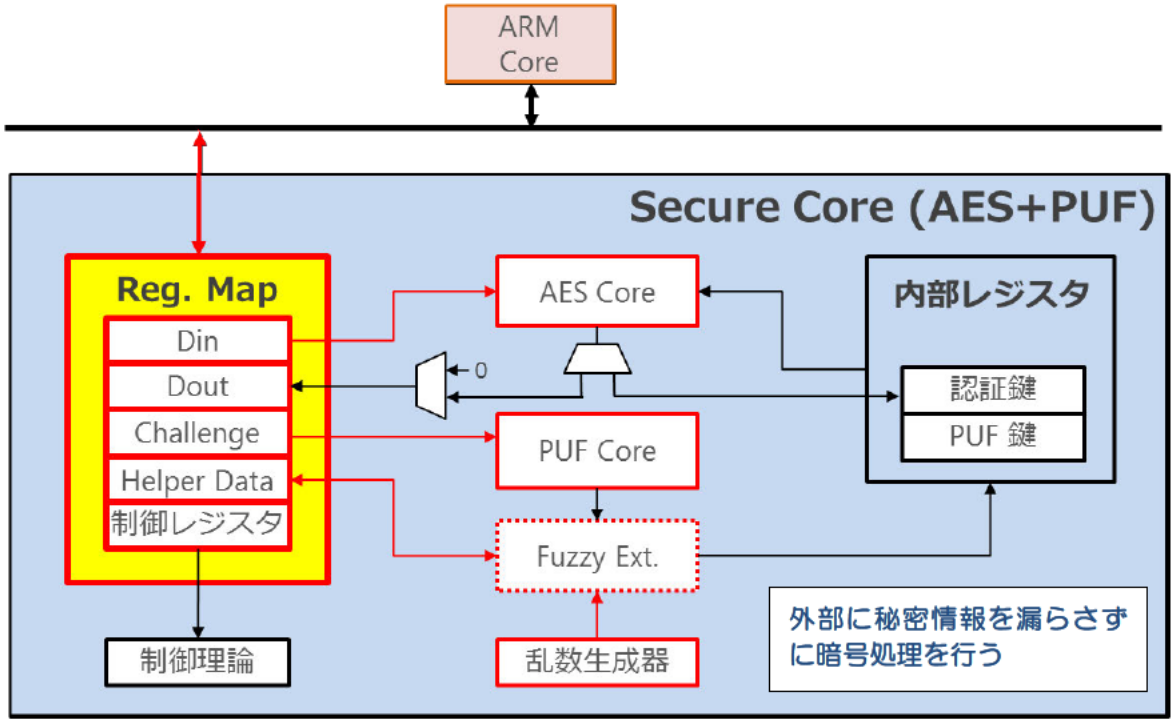


図2-12 統合セキュリティ回路構成案

◆鍵情報漏えいのリスクを排除した統合セキュア回路の仕様検討

暗号を行う AES 回路や，製造ばらつきから ID を生成する PUF 回路といった技術は単体で使用する場合は十分セキュアであるが，CPU やその周辺回路から利用されるときにその実装のまずさから外部に出してはいけない秘密情報を漏えいしてしまうことがある．これを防止するため，秘密情報を漏えいさせずに PUF 回路から得られた ID を AES 暗号に使用する秘密鍵を生成するための情報ソースとして使用するということを行う必要がある．これらを実現するため，PUF 回路を AES 回路と一体化し，鍵となる PUF 回路の出力を隠ぺいできる統合セキュア回路を構築する．初年度は，統合セキュア回路が最低限具備すべき機能とその動作を基本仕様として検討・設計した．またその回路の一部をプロトタイプとして開発に着手した．

統合セキュア回路の仕様を検討するなかで，併せて PUF の性能評価の結果を反映した誤り訂正回路(Fuzzy Extractor) の訂正能力の検討も行った．

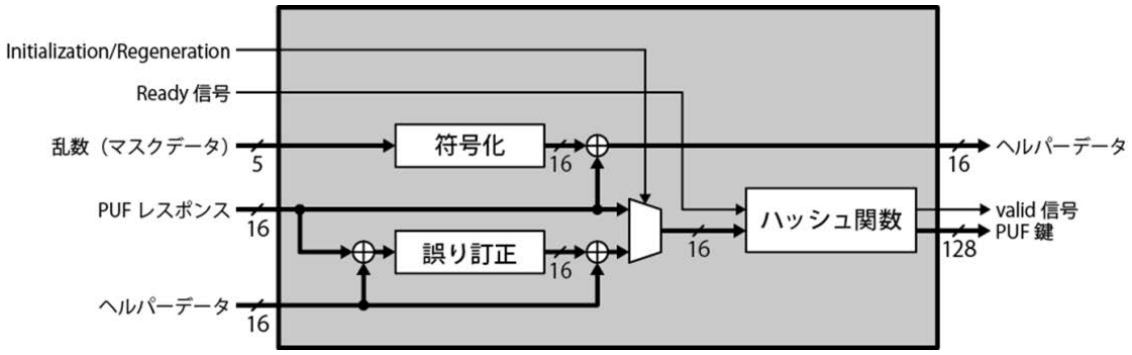


図2-13 誤り訂正回路（Fuzzy Extractor）の設計

【課題】

今回開発した誤り訂正回路（Fuzzy Extractor）は RM(16, 5) 符号という方式を採用しており，得られる情報語のビット長が 5bit，符号長は 16bit の符号方式である．つまり一回の動作で得られる情報は 5 bit であり，鍵として 128bit の情報量を持つデータを作成するにはこの符号化回路を 26 回動作させる必要がある．今後は，この訂正回路を基盤とし，AES 暗号鍵となる 128bit の鍵を生成する鍵生成回路を構築することが課題となる．

2－2－4 PUF技術を活用した鍵交換プロトコルの設計／評価

【目標】

PUF を中心としたハードウェア開発の成果を活用して，車載ネットワークに適した ECU 間における共通鍵暗号の鍵交換プロトコル（通信規約）を提案し，その実証システムを開発する．

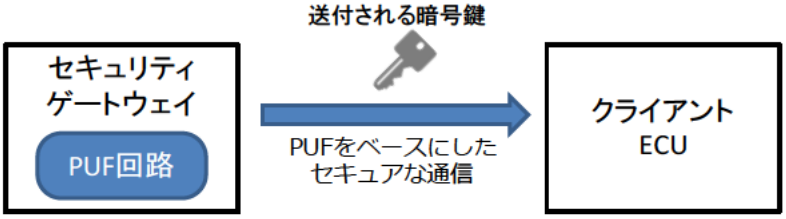


図 2-14 PUFを用いたセキュアな鍵交換システムイメージ

【研究成果】

セキュリティ対応したゲートウェア ECU からクライアント ECU に対して，安全に暗号鍵を配布するシステムを検討する．このとき配布される暗号鍵は PUF ID に基づいて暗号化されセキュアな状態でクライアント EUC へ送信される．

セキュリティ・ゲートウェイ ECU が管理する暗号鍵は PUF の特徴を生かし，鍵自体を PUF-ID で暗号化し保管・管理する「PUF による鍵ストレージ・システム」とする（図 2-15 参照）．

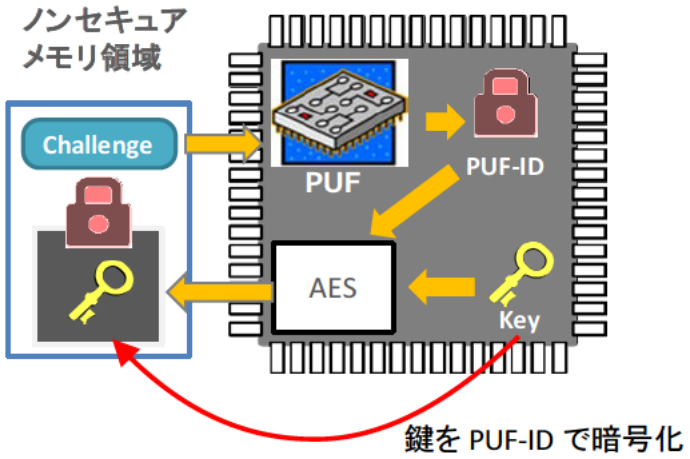


図 2-15 PUF-ID で暗号鍵を暗号化し保管する

以上は，検証を行いながらその結果を実装に反映させていく，いわゆるスパイラルフローでの開発スタイルをとる．検証を通して，識別機能や暗号鍵生成ソースとしてのPUFの特性評価と修正を繰り返し，セキュリティ・ゲートウェイ・ECUに適したPUFを開発した．

【課題】

今回，本活動で開発したPUF そして共通鍵暗号という2つのセキュリティ技術を活用した車載向けシステムの一例として，鍵交換プロトコルを設計し実装した．本プロトコルは，ICTで利用されいている公開鍵暗号系の鍵交換プロトコルや，先行研究で報告されている KDF（Key Distribution Function）を用いた鍵交換プロトコルと比較し，計算量・応答性においていずれも軽量・高速といった良好な結果を得ている．ただし，本活動での検証は，セキュリティ・ゲートウェイ1台に対して ECU が1台という限定された環境での検証であったため，今後は，レガシー

な（既存の）ECU を含めた混載ネットワークのなかで性能測定を行い，より実車に近い環境における本プロトコルの優位性・有用性を検証する必要がある．

2－3 セキュリティ･ゲートウェイ･ECU ソフトウェア開発

◆概要

セキュリティ・ゲートウェイ・ECU仕様開発の成果である，セキュリティ・ゲートウェイ・ECU基本仕様からセキュリティ・ゲートウェイ・ECUのソフトウェア開発を行う．ECUソフトウェアは，セキュリティOS，セキュリティライブラリ，PUFおよび暗号回路ドライバ，セキュリティ通信スタック(提案時はCAN通信を想定)，アクセスログ記録用メモリ管理モジュール，ゲートウェイ処理アプリケーションなどから構成される．

開発はISO 26262およびIEC 62443に準拠したプロセスに従って実施する．国内では提案代表であるヴィッツが，両方の開発プロセスを他社にさきがけて整備しており，セーフティおよびセキュリティの同時開発を効率的に実現できる体制を構築済みである．

2－3－1 ベーシックシステムの開発

【目標】

本研究におけるセキュリティ・ゲートウェイ・ECUの仕様開発で定義した遠隔リプログラミングシステムを開発するために必要な「ベーシックシステム」の開発を実施した．

【研究成果】

本研究では，Altera 社の Helio 上に，AUTOSAR 仕様の車載リアルタイム OS，CAN 通信，および，Ethernet を利用した TCP/IP 通信スタック（SSL/TLS 対応済み）を開発した．

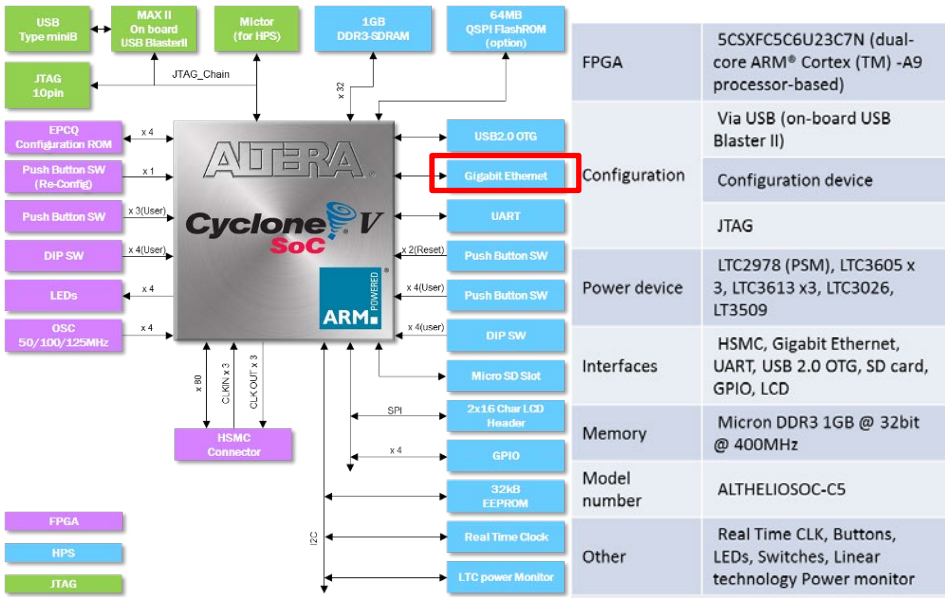


図2-16 Altera社 Helioのスペック

【研究成果】

ここで開発した成果を，以降に記す遠隔リプログラミングシステムを実装するためのベースシステムとして利用した実績があり，残課題はない．

２－３－２　遠隔リプログラミング用アプリケーションの開発

【目標】

セキュリティ・ゲートウェイ・ECUの仕様開発で策定した遠隔リプログラミングシステムの試作開発を行い，その実現性を評価する．

【研究成果】

遠隔リプログラミングシステムの試作，および，評価を実施するために，構築したシステムの構成図を以下に示す．

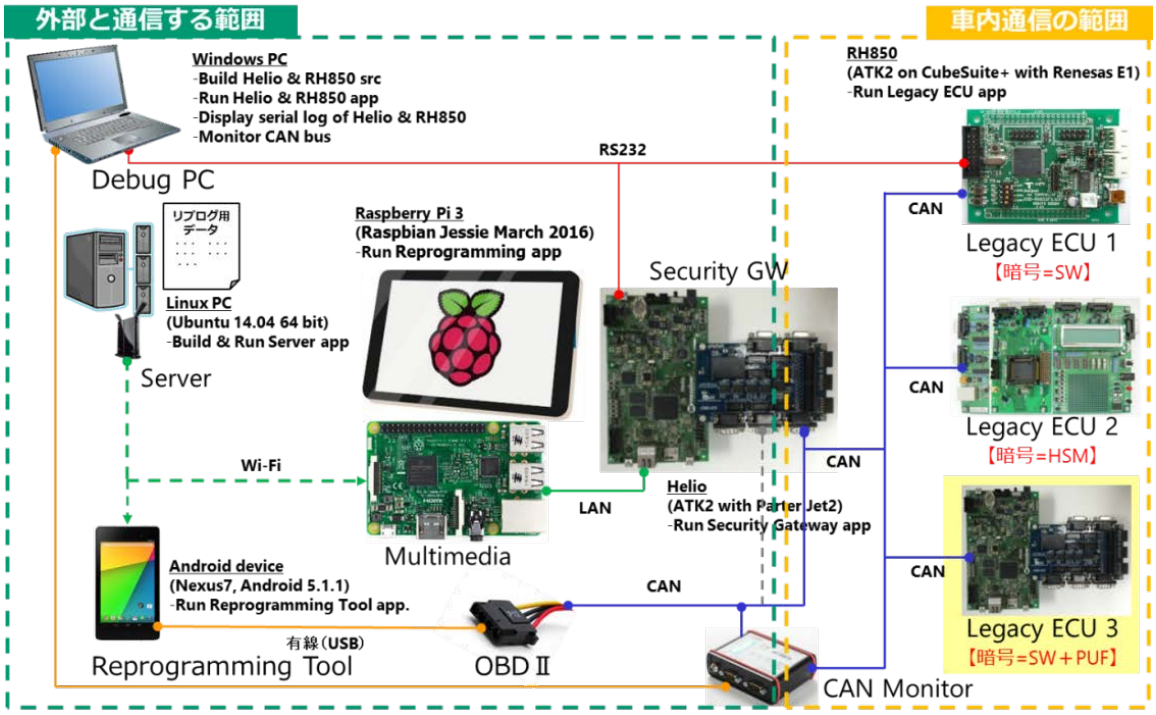


図2-17　PUF適応版の遠隔リプログラミングシステム構成

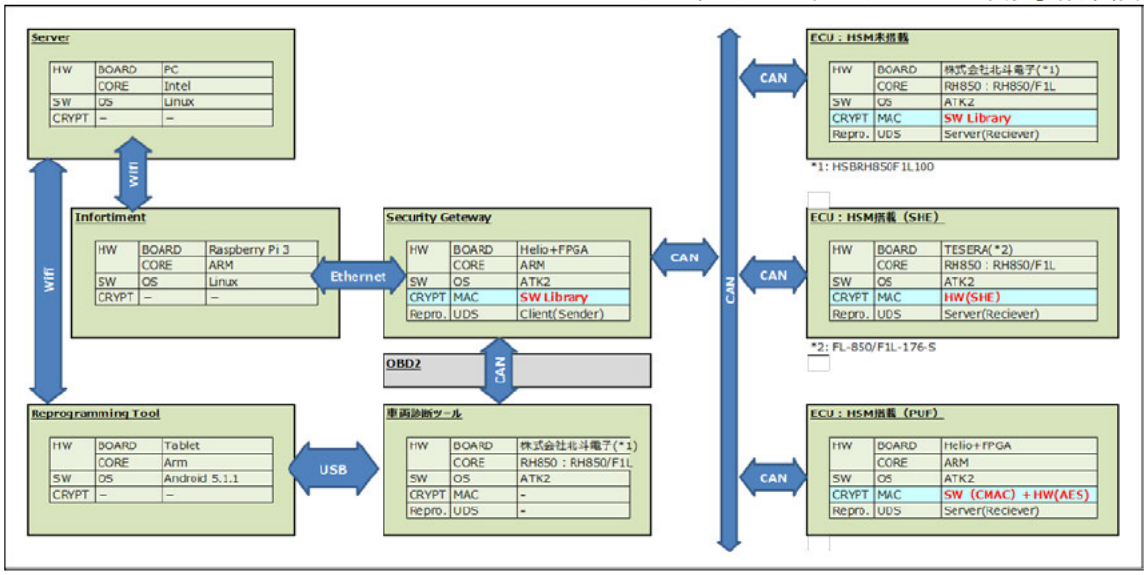


図2-18 遠隔リプログラミングシステム簡略図

◆機能評価

機能評価を実施するために，評価側のECUの種類として以下3つのECUを構築した．各ECUにの評価環境を以下に示す．

表2-4 評価環境

No.	名称	ボード名	プロセッサ	暗号処理モジュール
①	HSM未搭載のECU	HSB-RH850	RH850/F1L	SW
②	HSM搭載(SHE)のECU	FL-850/F1L-176-S	RH850/F1L	SW+HSM(SHE)
③	HSM搭載(PUF)のECU	Helio	ARM Coretex-A9	SW+HSM(PUF)

遠隔リプログラミングシステムにおける各ECUの性能を評価する為，以下の区間を計測対象と定義し，ECU毎に10回計測しそれらの平均値を算出した．なお，評価結果には機密情報が含まれるため，本書には記載しない．

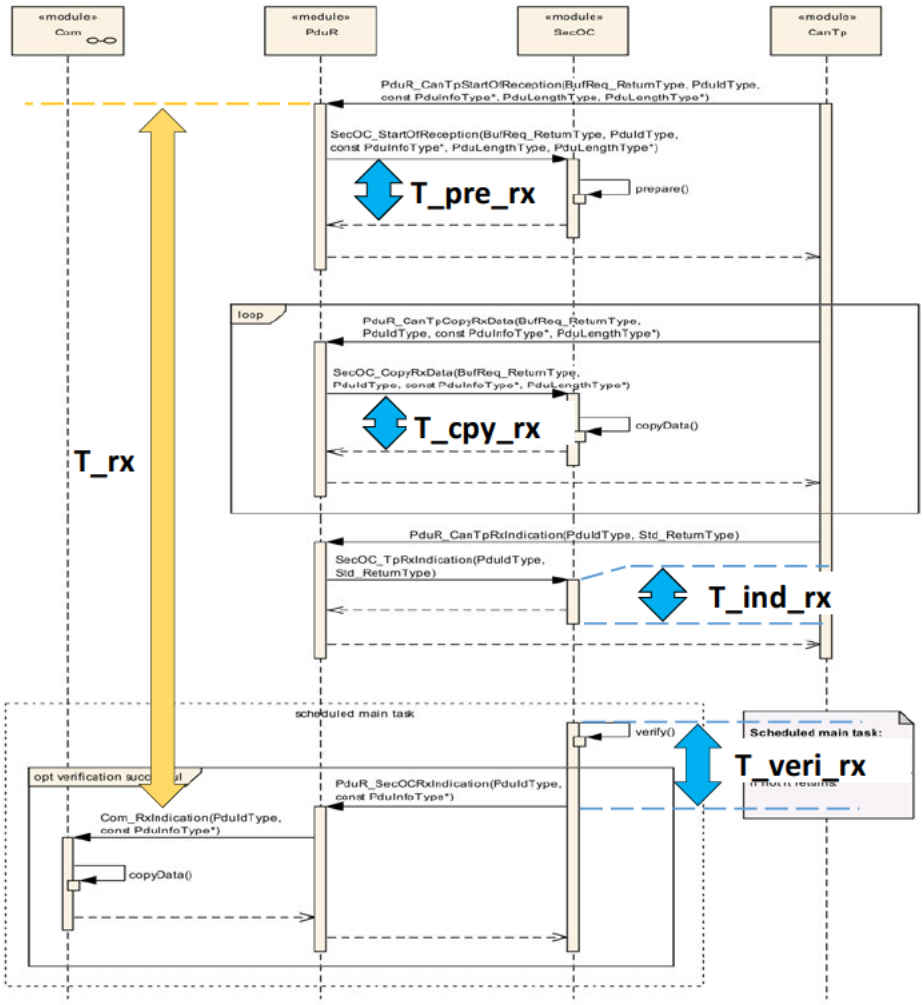


図2-19 計測性能測定の定義

【課題】

PUF適応環境における処理性能が，処理速度が最適化されたSWに比べ低速になる結果である．しかし，PUF向けAESドライバの処理速度最適化や，HSM（SHE）と同様にCMACを含めたHSM(PUF)対応により，大幅な改善が見込まれる．

2－3－3 自動車業界向け研究成果の活用検討

【目標】

自動車業界では，ECU に搭載する制御ソフトウェアのプラットフォームとして，AUTOSAR 仕様が広く一般的に利用されている．AUTOSAR 仕様の中には，自動車の制御に利用されている CAN 通信メッセージに対してメッセージ認証子（MAC）を付与し，改ざんやなりすましの様な攻撃から重要なデータ（制御データ／リプログラミングデータ）を保護するための機能仕様として“Secure On-board Communication 仕様”が公開されている．

そのため，本研究で開発する UDS on CAN に対して適用するメッセージ認証機能も，自動車業界の標準に合わせて AUTOSAR 仕様に従って仕様策定を行う．

【研究成果】

コンセプトにて「AUTOSAR “Secure On-board Communication”を利用したメッセージ認証機能の実現検討」及び「AUTOSAR “Secure On-board Communication” 仕様に対するPUF技術の適用」が定義されたため，それに伴いAUTOSAR SecOCの開発を実施した．

PUF技術を適応したモジュール構成図を以下に示す．PUF技術の適応は，ソフトウェアで実現しているCMAC処理のAES処理を，PUF向けAESドライバを開発し実装することでで実現した．

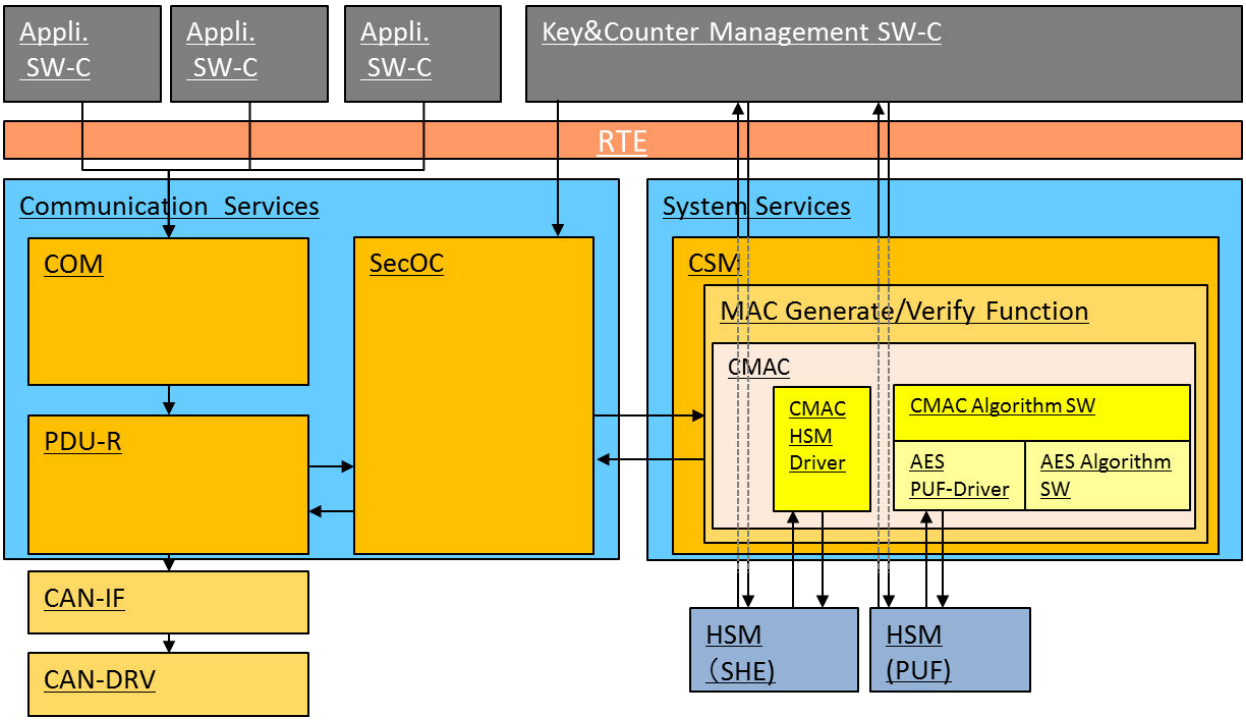


図2-20　PUFを含めたAUTOSARモジュール構成図

【課題】

PUF向けAESドライバを開発し，AUTOSAR SecOCへの適応した結果，AUTOSAR SecOCを仕様変更なく機能が動作することを確認できたため，PUF技術の適応に対する残課題はない．

第３章 IEC 62443準拠の開発

◆概要

セキュリティ・ゲートウェイ・ECUの基本仕様，セキュリティ・ゲートウェイ脅威および分析結果，耐攻撃性目標を条件として，IEC 62443に適合可能なセキュリティコンセプト文書を開発する．国際認証機関による第三者検証をうけることで，規格への適合性の客観的な裏付けを得る．

３－１－１ セキュリティコンセプト文書の開発

【目標】

本研究では，開発するセキュリティ・ゲートウェイがどのような脅威に対してどのような方策によりセキュリティを維持できるのかを説明するセキュリティコンセプト文書として，以下3つの文書を作成する

- セキュリティ管理計画　：SMP（Security Management Plan）
- セキュリティ要求仕様書　：SecRS（Security Requirement Specification）
- セキュリティアーキテクチャ設計書　：SAD（Security Architecture Design）

【研究成果】

セキュリティコンセプトとして開発する文書のうち，SecRS，および，SADの具体的な内容は，セキュリティ・ゲートウェイ・ECUの仕様開発の研究成果として記載済みである．そのため，ここではセキュリティ管理計画であるSMPの内容のみを記載する．SMPは，IEC 62443 に準拠した「セキュリティ開発プロセス」で製品を開発する際，作成が求められている開発計画書である．

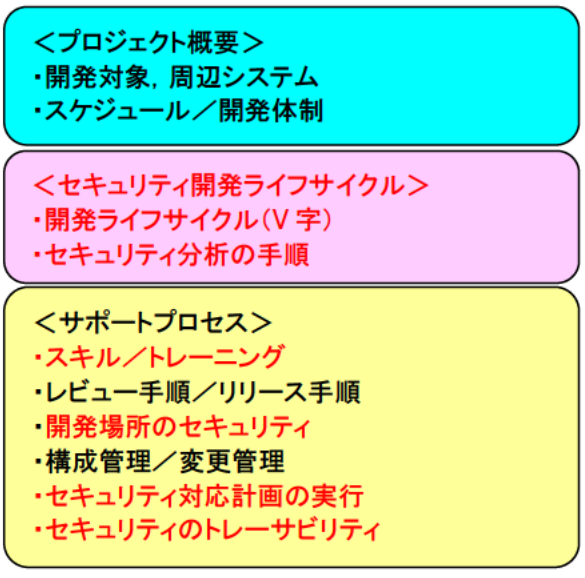


図3-1 SMPの構成

SMP で策定したセキュリティ開発ライフサイクルのフレームワークを以下に示す.

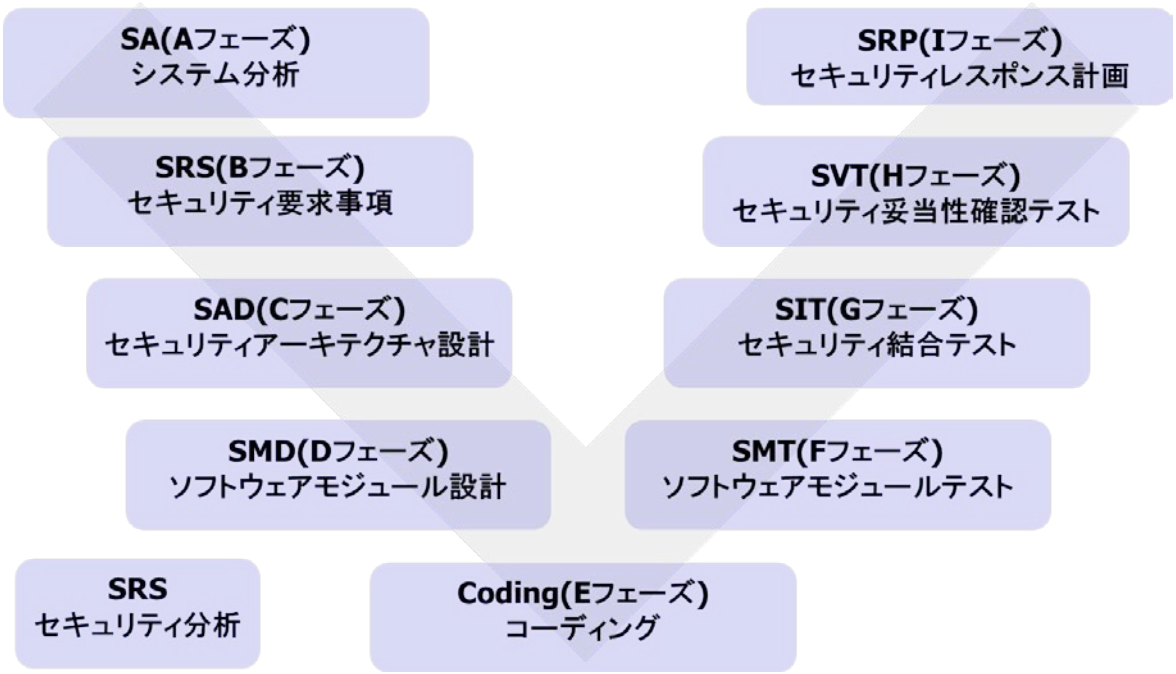


図3-2 セキュリティ・ゲートウェイ・ECU セキュリティ開発ライフサイクル

【課題】

第三者検証を受ける事が可能なレベルのセキュリティコンセプト文書（SMP，SecRS，SAD）を開発できたため，残課題はない.

３－１－２　国際認証機関によるコンサルティング／アセスメント

【目標】

本研究はで，開発したセキュリティコンセプト文書に対して，国際認証機関による第三者検証をうけ，規格への適合性の客観的な裏付けを得ることを目標とする．評価の流れを以下に示す．

- セキュリティ・ゲートウェイ・ECUの仕様開発の成果（Security Management Plan，Security Requirements Specification，Security Arhitecture Design）を説明し，IEC62443-4-1のプロセスに準拠した開発が出来ているか否かの評価をして頂く．
- セキュリティ・ゲートウェイ・ECUの仕様開発でまとめたセキュリティ機能要求の内容が技術的に問題ないか，また，脆弱性が残った設計となっていないかを評価して頂く．

【研究成果】

国際認証機関による第三者評価の流れを以下に示す．

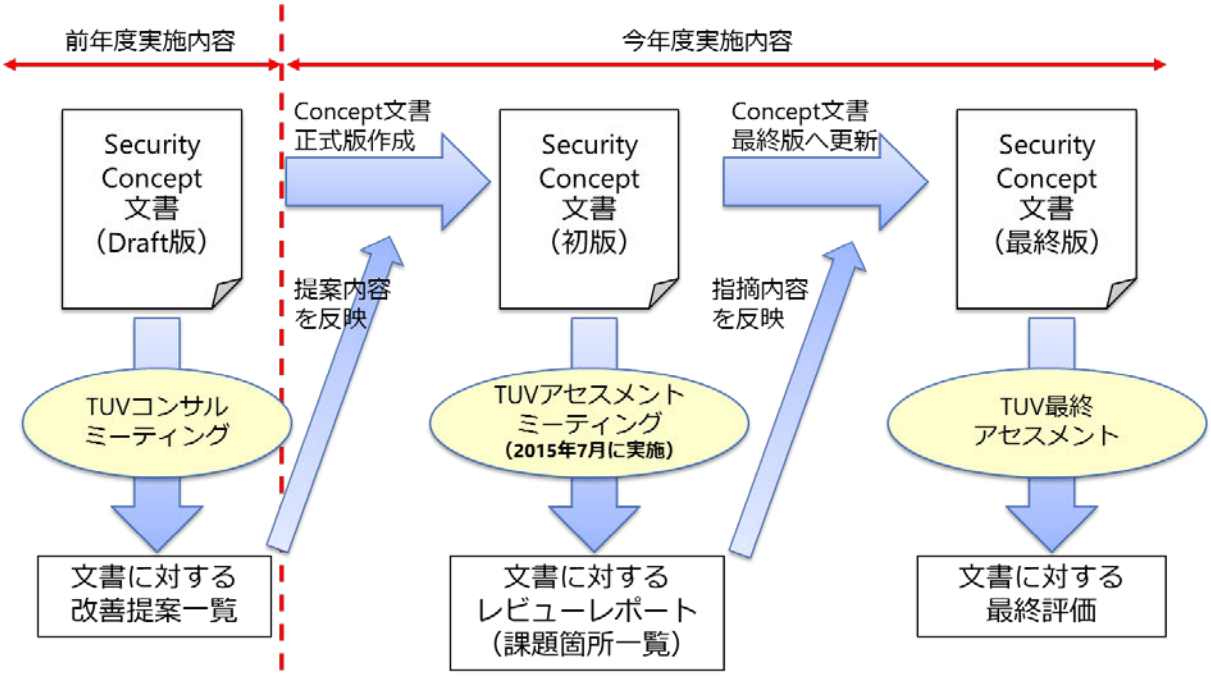
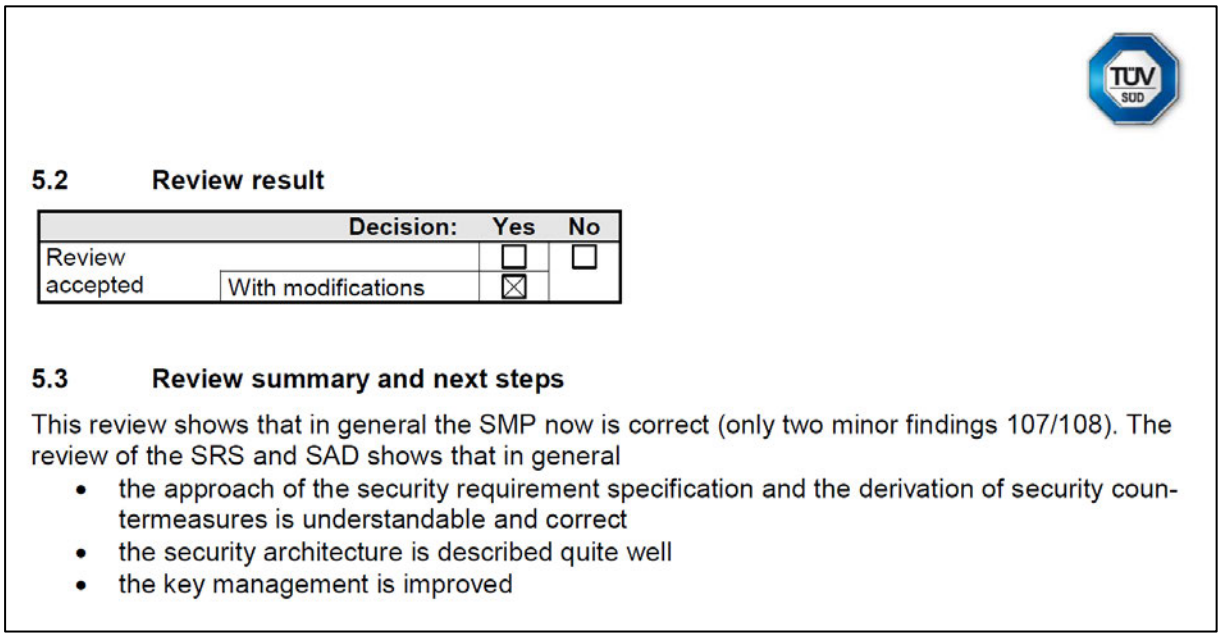


図　3-3　国際認証機関とのレビューの流れ

平成27年度までの活動成果にて，IEC 62443準拠でセキュリティ・ゲートウェイ・ECUのセキュリティコンセプト文書の開発が完了し，国際認証機関であるTÜV SÜDへ提出して第三者評価として以下の評価を得ることができた．



5.2 Review result

		Decision:	Yes	No
Review accepted			☐	☐
	With modifications		☒	

5.3 Review summary and next steps

This review shows that in general the SMP now is correct (only two minor findings 107/108). The review of the SRS and SAD shows that in general

- the approach of the security requirement specification and the derivation of security countermeasures is understandable and correct
- the security architecture is described quite well
- the key management is improved

図3-4 国際認証機関（TÜV SÜD）から受領した技術レビュー結果（抜粋）

上記の通り，SMP（Security Management Plan）についてはCorrectという評価をもらうことができた．また，SRS（Security Requirements Specification）とSAD（Security Arhitecture Design）については，以下の評価を貰うことができた．

- セキュリティ対策やセキュリティ要求仕様の導出アプローチは明確で正しい．
- セキュリティアーキテクチャの記述は非常によくできている．
- 鍵管理の課題についても，改善されている．

このことから，本研究事業で取り組んでいるIEC62443準拠の開発プロセス，および，開発技術について，第三者評価にて十分な評価を得ることができたと考える．

【課題】

開発したIEC62443に適合可能なセキュリティ文書は，国際認証機関であるTÜV SÜDによる第三者レビューを受け，十分な評価を得ることができたため，残課題はない．

第４章 全体総括

本研究は，平成 26 年度より以下 3 点の課題に対して，課題を解決するべく研究をスタートした．

・**課題１：**
高度 IT 融合社会の一員としてセキュリティ脅威への対策を短期間で可能とする技術開発が必要

・**課題２：**
市場優位性確保のため，欧州が主導する技術に対してアドバンテージを有する技術開発が必要

・**課題３：**
相互接続性確保のため，欧米主導で制定された規格に準拠した技術開発が必要

課題 3 ついては，昨年度，「IEC62443 準拠のコンセプトドキュメントの開発」を実施し，その成果物に対して国際認証機関である TÜV SÜD のレビューを受け，「Principal is OK !」という評価を貰い，妥当である事が確認できた．
課題 1，2 については，昨年度からの継続として，セキュリティ・ゲートウェイ・ECU」に対し，「(1)セキュリティ・ゲートウェイ・ECU 仕様の開発」，「(2)セキュリティ・ゲートウェイ・ECU HW / SW の開発」を行った．
「(1)セキュリティ・ゲートウェイ・ECU 仕様の開発」については，

1. 遠隔リプログラミングシステムにおけるユースケースの拡張
2. 自動車向け標準仕様への PUF 技術の適用

をテーマとして行い，その仕様に基づき「(2)セキュリティ・ゲートウェイ・ECU HW / SW の開発」を行った．双方とも本年度で研究を完了し，システムとしても組み上げを完了させたことで，今後の事業化に繋げられる状況となった．
研究初期に事業化に向けた基本方針として 2020 年東京オリンピックでの技術発信などに対応するため急速に IT 融合化が進み，すべてのデバイスが繋がり，相互連携をする高度 IT 融合社会が現実となった際に，それぞれのデバイスが個別に攻撃から自己を脅威から守る必要があり，自動車など制御装置も例外ではなく，近未来に現実化する全デバイスへの対応が迫られるセキュリティ脅威への対策を享受できる事業を展開することが基本方針であった．
IT 融合化が進むことにより，組込み制御製品の社会インフラ連携が確実に進む．この高度 IT 融合社会において，個々のデバイスがセキュリティ脅威に対応する組込みセキュリティ技術は重要な技術要素となる．また，その技術を集積したセキュリティ・ゲートウェイは即時に利用できる基幹部品となる．この技術および製品を利用する分野は，自動車ばかりでなく，サービスロボット・産業機械・航空宇宙など多くの国内牽引産業が利用すると考えられ，他業界への波及効果は大きい．
そして，高度 IT 融合社会にて社会インフラと連携した結果，“セキュリティ脅威によりセーフティを脅かす”危険があるすべての製品に適用可能である．すなわち，自動車，産業ロボット，産業機械，航空宇宙，エレベータ，エスカレータ，自動二輪車などありとあらゆる装置が対象となる．これらの装置へのセキュリティ対策に本製品を利用し，かつ，装置に搭載される制御システム開発に本研究の成果技術を利用することにより，高度 IT 融合社会における利用者安全を担保かつ容易に提供できるセキュリティ基盤として利用されること

が想定されるため，これらの分野に本研究成果の実用化に向けて，アプローチができる状況になった．

また，本研究で実施した IEC 62443 への準拠は，今後，国内外の制御機器・組込み制御機器開発で必要となる準拠規格であり，この対応成果の活用も大いに期待できるため，今後必要となる規格の準拠に対しても事業化に向けて動ける状態になっている．

尚，本研究は，高度 IT 融合社会の構成要素となる「自動車」に搭載する「セキュリティ・ゲートウェイ・ECU」に関するものであり，今後，ますますグローバルネットワークと常時接続され，ADAS 等，ユーザの利便性は高まる一方で，車載制御に対する”Security”脆弱性の克服は大きな課題であり，その克服において，グローバルネットワークと車載の内部ネットワークを分離する「セキュリティ・ゲートウェイ・ECU」は大きな役割を果たし，PUF（Physical Unclonable Function)を車載制御に適用する研究は他に例がないものである．

今後の事業展開であるが、当初の目論見通り

1. セキュリティ開発技術支援
2. セキュリティ・ゲートウェイ
3. セキュリティチップ　IP 販売

の観点で事業化を推進していく．特に 1. については，既に事業化を開始しており，組込みセキュリティが今後必要となる各社への支援を行っている．2，3 については，アドバイザー企業への共同研究を提案し，実用化へ向けての活動を行う．尚，3 は，PUF を用いたセキュリティチップの IP 販売を狙っているが，今回の研究スコープは PUF の応用に力点をおいたので，PUF が一般的に弱いとされる高温時の挙動については対象外とした為，他のプロジェクトの動きも注視しながら，活動を行っていく．

以上より，本研究の進捗および成果は適正であることを報告する．