繋がる車のセキュリティ

押田 大介† 竹森 敬祐†† 川端 秀明†† 磯原 隆将†††

山梨 晃† 塩田 茂雅† 横田 雅勝†

†ルネサスエレクトロニクス（株）
100-0004 東京都千代田区大手町 2-6-2
daisuke.oshida.ux@renesas.com

††KDDI 研究所（株）
356-8502 埼玉県ふじみ野市大原 2-1-15

†††（株）KDDI
102-8462 東京都千代田区飯田橋 3-10-10

あらまし 近年の自動車業界では、自動走行などの観点化から、自動車内部に存在する保護すべき資産が激増しており、高いセキュリティが要求されてきている。大きくは外部からのアクセスセキュリティと車内ネットワークセキュリティに分類される。本論文では、車内ネットワークの脅威の洗い出しを行い、セキュリティのコンセプトを示す。さらには、車内ネットワークを守る最低限のセキュリティ実装として、車内ネットワークの認証とセキュアブート機能を用いてしセキュアな車内ネットワークを検討した結果に関して報告するものである。

Connected Vehicle Security

Daisuke Oshida† Keisuke Takemori†† Hideaki Kawabata†† Takamasa Isohara†††

Akira Yamanashi† Shigemasa Shiota† Masakatsu Yokota†

†Renesas Electronics Corporation
2-6-2, Ote-machi, Chiyoda-ku, Tokyo 100-0004, JAPAN
daisuke.oshida.ux@renesas.com
††KDDI R&D Laboratory
2-1-15 Ohara, Fujimino, Saitama, 356-8502 JAPAN

†††KDDI Corporation
Garden Air Tower, 3-10-10, Iidabashi, Chiyoda-ku, Tokyo 102-8460, JAPAN

Abstract In this paper, we studied about vehicle network security based on actual threat analysis. We report about the consideration about the authentication of the network in the vehicle and a secure boot function as minimum security implementations to protect a vehicle, and realized secure inside of vehicle network.

1　はじめに

近年、自動車分野においては、V2X（Vehicle to X, e.g. Vehicle, Infrastructure, Personal, etc…）と呼ばれる車と車、またはその他との通信や、それらの通信とセンサー情報を加えて自動車がアクセル、ステアリング、ブレーキ等を操作する自動走行などの研究が進んでいる。すでにレーダーやカメラからの情報を元に、自動車が障害物との衝突を回避する技術が実用化されており、運転者のアシストを行う技術は、これからも加速すると考えられる。（Electronic Control Unit）ECU が走る・曲がる・止まるといった基本的な動作のみを制御していた時代から、サラウンドビュー表示や一部の制御を行う部分自動化を経て、統合コックピットとして IT と連携しつつ、高度な制御 / 制御の完全自動化が進むと予想される。その実現のために、クラウド連携も検討されている。すなわち、これからの自動車は IT と制御の融合が進むと予想される。

従来では、高速道路等の通行料の課金に利用されている ETC（Electronic Toll Collection System）が個人情報として保護されていたが、V2X system においては、個人を特定する情報だけではなく、駐車場や電気自動車の充電課金の為のクレジットカード情報なども保護すべき資産となっており、様々なサービスへの適応も検討されている。さらには、ネットワーク経由で自動車の状態監視を行い、ECU のリプログラミングを行うサービス等も検討されている。さらには、近年活発に議論されている自動車の自動走行を実現するためには、自動車そのものの動作の完全性を確保する必要がある。このため、自動車内部に存在する保護すべき資産は、この数年で増加する傾向にあるため、自動車へのセキュリティの実装が急務となっている。

2　自動車セキュリティの課題

自動車においては、多くて１００以上の半導体が搭載されており、各半導体は異なる動作を行う仕様となっている。全ての ECU に高いセキュリティ機能を実装する事が理想であるが、コストや応答性の観点から現実的では無い。保護すべき資産も想定される攻撃手法も異なるため、各 ECU に対して最適なセキュリティを検討すると、システムが複雑化してしまう。

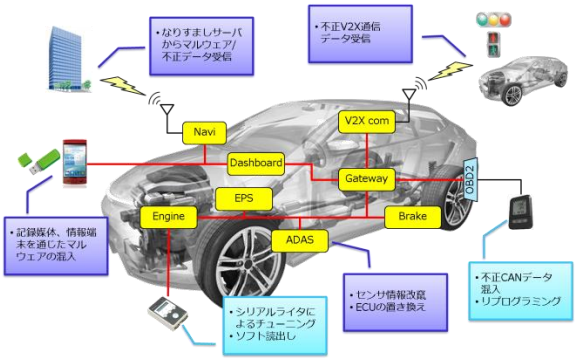

図１．　自動車における脅威の概要

2.1　自動車内部の課題

従来から、自動車の内部においてもセキュリティの観点から見た脅威は存在している。例えば、車内ネットワーク上の不正なデータの混入や、シリアルライタを経由した不正プログラムの書き込みによるチューニング、リプログラミング時におけるマルウェアの混入、不正な ECU への置き換えなどが挙げられる。

自動走行を視野に入れたこれからの自動車においては、カメラやセンサーから入力される情報と、地図情報などを統合的に判断し、自動車の制御を行うため、センサーそのもののなりすましや、センサー情報の改竄などの新しいセキュリティの課題が見えてきている。また、判断するシステムそのものを改竄される事により、自動車そのものを不正に操作する事が可能になるため、ECU 上で動作するソフトウェアに対するセキュリティも必要となってくる。

2.2　外部ネットワークの課題

自動車が外部と繋がるインターフェースは多岐に渡る。すでに実用化されているものとしては、オーディオ機器とスマートフォンなどの Bluetooth 接続による音楽再生や、Dedicated Short Range Communication（DSRC）を利用した

ITS スポットによるインターネット接続サービス、広域道路交通情報提供サービス、安全運転支援サービス、観光サービス、ETC などの決済サービスや、各自動車会社が提供する、テレマティクスを利用した最新の地図情報の提供や、オペレータ接続サービス、e-call などのサービスも提供されている。

これからは、車車間、路車間の通信による衝突防止や、リアルタイムな道路状況提供、緊急車両の接近通知、駐車場の空き情報等のサービスが検討されている。さらには、自動走行との連携として、他の車両から得られた情報を元に、緊急ブレーキの自動化の実用化検討をされている。

2.3 機能安全との融合の課題

セキュリティを実装するに際して、一般的には、評価対象の定義、脅威分析、リスク評価、対策方針策定、セキュリティ要件の選択というステップをとる。自動車における機能安全とセキュリティの融合を考えた場合、このフローそのものから見直しを行う必要が出てくる。

2.3.1 評価対象の定義

ICカードなどでは、評価対象はマイコンのチップそのものを考えてセキュリティを担保してきている歴史がある。しかし、複雑化する自動車のシステムにおいて、様々な階層での定義が可能となる。例えば、従来通りマイコンをTarget of evaluation（TOE）としたり、ECUをTOEにしたり、さらには自動車そのものをTOEとする場合も考えられる。

自動車そのものをTOEとした場合、インターフェースに関しては定義が可能であるため、入出力する情報に関しての対策は比較的容易と考えられるが、物理的な攻撃という観点から考えると、攻撃の範囲が非常に広くなってしまう可能性があり、現実的では無いと考えられる。一方で、マイコン単体と定義した場合、接続される機器が多岐に渡るため、脅威分析時に発散してしまう可能性がある。現状では、EUCをTOEとし、システムを評価対象とするのが現実的であると考えられる。

2.3.2 脅威分析

現在、CANネットワークにパソコンを接続して自動車を制御したり、CANネットワークにBluetoothモジュールを接続しリモートで不正なコマンドを送付する攻撃など、自動車に対して様々な攻撃成功例が報告されているが、まだ研究報告が中心である。一方で、公開されている実被害としてはイモビカッターと呼ばれる自動車のイモビライザーを初期化して電子錠を開錠して自動車を盗難する被害などが報告されている。一方で、公開されていない被害も存在する可能性がある。

このように、公開されている自動車におけるインシデント例が少なく、脅威分析を行う際の脅威の網羅性を確保する事が課題となる。

2.3.3 リスク評価・対策方針策定

自動車における保護すべき資産は、大きくは、金銭情報・個人情報・著作権に代表されるような情報資産と、安全に関わる安全資産の２つに分類できる。この保護資産は対策方針策定に影響を及ぼすため、セキュリティポリシーに関しては、十分に検討を行う必要がある。

情報資産におけるセキュリティの対策では、異常を検知した際に動作を停止する事が一般的である。しかし、自動車において、機能が突然停止すると、自動車の制御ができなくなり、事故を引き起こす可能性がある。このように、ITセキュリティでは、定義した保護資産の価値は平等であり、一律に保護する必要があったが、自動車においては、安全資産と情報資産の重み付けを行う必要がある。

3 車載セキュリティ設計

Denial Of Service（DoS）攻撃等があった場合でも、安全に関わる機能を確保する事が重要である。そのため、走行機能に関わる自動車の内部ネットワークと、情報系機能を有する外部のネットワークを遮断する必要がある。自動車のネットワーク構成を車内ネットワークと車外ネットワークの２つに大きく分類し、それぞれに対して施すセキュリティを検討する。

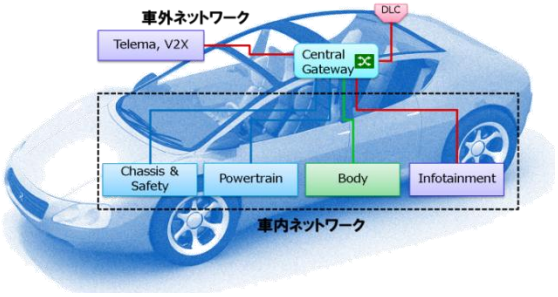

図２． 車内ネットワーク構成

3.1 車内ネットワークセキュリティ

車内ネットワークにおいては、ほぼ全ての資産が安全資産であり、安全な動作が優先される。この傾向は、自動走行など自動車技術が進んでも変わらないと推測される。すなわち、完全性と可用性を確保する事が重要となる。これら車内ネットワークにおける脅威は、ネットワーク上に不正なデータを流す事や、ECU の改竄・不正な置き換え、リプログラミング時におけるマルウェアの混入が挙げられる。

言い換えると、車内ネットワークに流れるデータの正当性を検証する事と、同じ車内ネットワークに接続されている ECU が正しい事を他の ECU が確認する事により、完全性と可用性を確保できると考えられる。

3.2 車外ネットワークセキュリティ

自動車をパソコンに見立てて考察すると、社外ネットワークに関しては、従来の IT で培われた技術が流用できると考えられる。考えられる脅威としては、不正なデータの注入や、サーバのなりすまし、記録媒体や情報端末を通じたマルウェアの混入が考えられる。

車車間通信・路車間通信など、V2X では様々な接続先が存在するが、接続先そのものは IT の世界と比べコントロール可能であるため、接続先の全てを認証する事が可能である。正しく認証を行い、相手を確認した後にセッションを張って通信を行う事により、車外ネットワークからのマルウェアや不正データの注入、サーバのなりすましは防ぐ事が可能であると考えられる。それに加え、正しく起動する事を確認するために、Secure boot 機能も実装する必要がある。一方で、記録媒体や情報端末を介したマルウェアの混入に関しては、これらとは別の対策を検討する必要がある。例えば、記録媒体や情報端末と接続する ECU の車内ネットワークからの遮断や、ECU 内部にスーパーバイザーモードを用意し、秘匿とされる情報を扱う領域に関しては、セキュアな環境下のみで実行するなどの対策が必要であると考えられる。

3.3 開発プロセス

機能安全と融合したセキュリティの開発プロセスを検討するためには、双方の開発プロセスを平行して進めるのではなく、各プロセスにおいて融合させて検討する必要がある。

セキュリティ目標設定時に安全目標を設定し、アプリケーションレベルでの目標レベルを定義する。機能レベルの分析として安全を脅かす事象を脅威と捉えた脅威分析を行う必要がある。また、安全要求を満たした対策方針を策定し、脆弱性分析・安全分析の評価サイクルを行う。実装・製品化後に、機能検証と安全性の妥当性検証・セキュリティの観点から侵入テストを実施する。

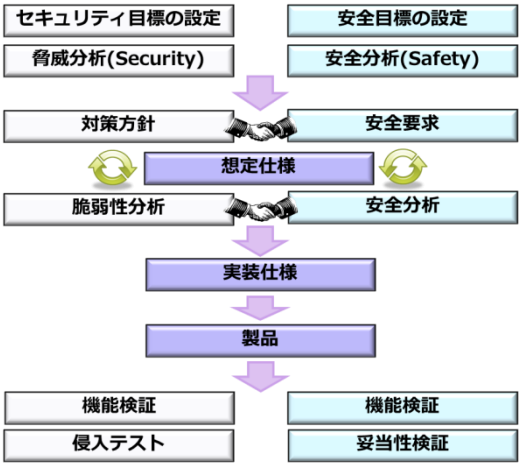

図３． 機能安全と Security を融合した開発プロセス

4 車載セキュリティのコンセプト

4.1 提案

本論文で提案する車の制御システムに対する攻

撃対策の概要を図 4 に示す。(i)ECU のセキュアブート，(ii)ECU の認証，(iii)パケットの認証，(iv)コードの署名検証である。これらを、H/W レベルの堅牢性で実現することを本論文の目標とする。はじめにセキュア IP 搭載の ECU の選定を行い、その上で(i)～(iv)を構築していく。

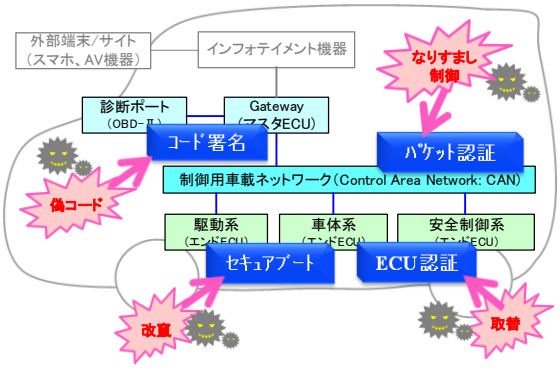

図４．　車の制御システムに対する攻撃対策

4.2　Secure IP 搭載マイコンの特徴

Secure boot 機能と、車内ネットワークのパケット認証を行った Chip では、内部に耐タンパ性のある、独立したシーケンサーとセキュア RAM、セキュア ROM（フラッシュメモリ）を内蔵した構成となっており、この独立した領域内で暗復号や乱数生成、ハッシュ生成や検証を行う機能を持つ。ROM は非セキュリティモジュール領域と、セキュリティモジュール領域に分離する事が可能であり、セキュリティモジュール領域のみ、セキュリティモジュールでリード/ライト/消去が可能である。CPU は、この内部で独立している RAM、ROM へ直接アクセスする事が物理的に出来ない構成となっている。

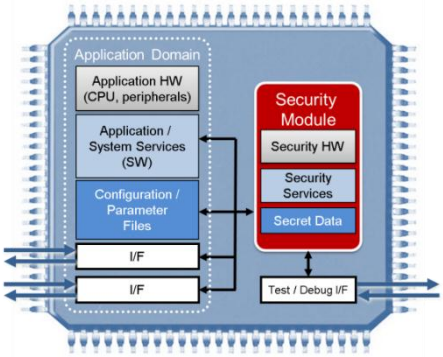

図５．セキュア IP 搭載マイコンの構成図

4.3　ECU のセキュアブート

ECU の Application Domain の一部に、Write Protection を施した Root of Trust を作り込み、不変な Boot Loader とセキュアエレメントとのインタフェース(IF)を、Write Once で書き込む。ここを基点としたセキュアブートを以下の手順で実施する(図 6)。前提として、Security Service には、対称鍵暗号である AES、ファイル測定のための Cipher-based MAC (CMAC)、乱数生成の機能が H/W 実装されており、制御コードの測定には、BOOT_MAC_KEY と呼ばれる鍵を用いた CMAC 演算が行われる。また、起動後に ECU 間で共有される秘密の情報を管理する機能を設ける。Secret Data には、複数の暗号鍵と、制御コードの期待値を管理する領域(BOOT_MAC)に、CMAC の期待値が予めセットされている。

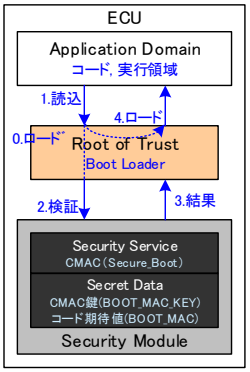

図６．　エンド ECU (RH850F1L) のセキュアブート

Step 0) Boot Loader とセキュアエレメント IF をロードする.

Step 1) 可変の制御コードが Application Domain から、Root of Trust の Boot Loader を通じて Security Module の CMAC 処理に渡される.

Step 2) Secret Data の CMAC 鍵(BOOT_MAC_KEY)を用いて制御コードの CMAC(Secure_Boot)演算が行われる. この値と, Secret Data で管理される CMAC の期待値(BOOT_MAC)を比較する.

Step 3) 一致/不一致の結果を Root of Trust に返す.

Step 4) 結果が一致していれば, 制御コードが完全であると判断され, Application Domain に制御コードがロードされる. 不一致であれば, 起動を停止するなど, エラー処理に進む.

4.4 ECU の認証

セキュアブートが完了し、個々の ECU が完全な状態で起動すると、制御システムに偽の ECU が混入してしないか、マスタ ECU からエンド ECU に向けてチャレンジ・レスポンス認証を行い、構成検証を進める（図 7）。

尚，認証に用いる暗号方式として、処理速度や H/W サポートの面から、対称鍵(K)を用いることとする。

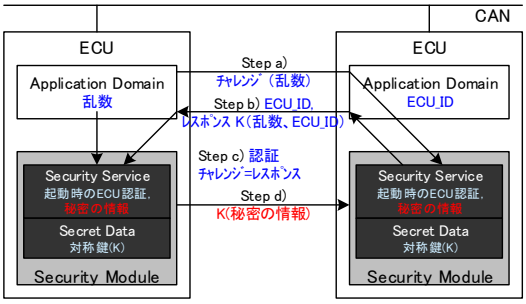

図7．ECU 認証と秘密の情報の共有

Step a) マスタ ECU の Application Domain で乱数を生成し，エンド ECU へチャレンジとして送付する．

Step b) エンド ECU は，受け取った乱数と ECU_ID を Security Service に渡し，Secret Data で管理される対称鍵 K で暗号化 K(乱数，ECU_ID)する．これをレスポンスとしてマスタ ECU へ返信する．このとき CAN パケットには，送信元を示す ECU_ID が付される．

Step c) マスタ ECU は，受け取った K(乱数,ECU_ID)と ECU_ID を Security Service に渡し，Secret Data で管理される対称鍵 K で K(乱数,ECU_ID)を復号する．そして送信した乱数と復号した乱数，ECU_ID が一致することを確認し，エンド ECU を認証する．

$$乱数=K^{-1}(K(乱数),\ ECU\_ID=K^{-1}(K(ECU\_ID)$$

Step d) 認証に成功するとマスタ ECU の Security Service で，新たな乱数である秘密の情報を生成し，Secret Data で管理される対称鍵 K で暗号化して，エンド ECU へ送付する．

エンド ECU は受け取った K(秘密の情報)を，Secret Data で管理される対称鍵 K で復号し，Security Service で管理する．

Step a)～d)により、制御システムを構成する ECU 群の認証が完了し、マスタ ECU が生成した秘密の情報を正規の ECU のみが安全に共有することになる。この秘密の情報は、エンジン始動毎にマスタ ECU が生成し、1 つの車両を構成する全ての ECU で共通の値とする。

4.5 CAN パケットの認証

ECU は，送信する全ての CAN パケットに Media Authentication Code(MAC)を挿入する（図 8）。MAC には、データの完全性と送信元認証を担保するために、CAN フレームのデータ部と事前に共有した秘密の情報を含める。また、リプレイ攻撃を阻止するために、ECU の Application Domain で、自身が送信したパケット数”s”をカウントし、これも MAC に含める。各 ECU から受信したパケット数”r”もカウントしておき、MAC 検証に利用する。

MAC＝Hash（データ，秘密の情報，カウンタ）

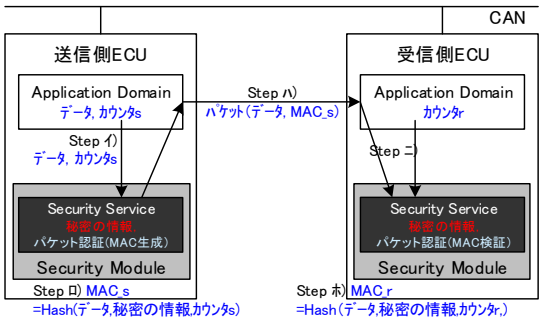

図8．MAC による CAN パケット認証

Step イ）送信側 ECU は，Application Domain からデータ，パケットカウンタ”s”を Security Service に渡す．

Step ロ） Security Service は，起動時に共有しておいた秘密の情報を加えて，MAC を算出する．

$$MAC\_s=Hash\ （データ，秘密の情報，カウンタ”s”）$$

Step ハ）Security Service は，算出した MAC を Application Domain に渡し，CAN にブロードキャストする．受信側 ECU は，所望の C パケットを取り込む．

Step ニ）受信側 ECU は，CAN パケットのデータ，MAC_s，送信元 ECU ID に該当する受信パケットカウンタ”r”を，Security Service に渡す．

Step ホ） Security Service は，データ，起動時に共有しておいた秘密の情報，パケットカウンタ”r”から

MAC を算出する．そして，MAC_s＝MAC_r を検証することで，データの完全性，送信元認証，リプレイ攻撃阻止を担保する．

MAC_r＝Hash（データ，秘密の情報，カウンタ"r"）

4.7 信頼の輪

署名検証処理が改竄されると、検証の信頼性が担保されない。そこで ECU のセキュアブートにおける測定対象として、署名検証処理も含めることにする。尚、ECU 認証、CAN パケット認証に関わる処理についても、セキュアブートの測定範囲に含める。この信頼の輪を図 10 に示す。セキュアブートと認証によって、エンジン始動時、走行時、メンテナンス時をトータルに、Safety を担保できるようになる。

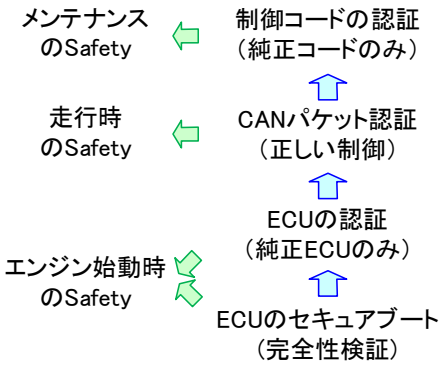

図 9 始動・走行・メンテナンスの安全性

4.8 センタ局によるリモート管理

車メーカなどが運営するセンタ局では、出荷した車の状態を統合管理できるよう、図 10 に示すような状態監視システムを構築する。ここでは、個々の車の状態として、CAN 通信、ECU の正常/異常を一覧表示している。これにより、異常な車の検知、車検やリコールの進捗確認、事故が発生したときの責任分解が行えるようになる。

図 10 車のリモート管理局

5 終わりに

自動車分野において、利便性・安全性向上させる動きは、すでに始まっており、今後も加速すると考えられる。利便性・安全性を向上させる事に伴う自動車における新たなる脅威が見えてきており、今後はセキュリティを抜きに考える事が出来ない。本論文で紹介したセキュアブートは ECU における改竄に対して確実な検知を行い、自身の正当性を証明する事が可能になる。また、チャレンジ・レスポンスを用いた MCU 間認証を確実に行い、コード認証とパケット認証を行う事により、純正コードが適用され、正しい制御を保証するための有効な手段になると期待される。

今後の課題として、本技術では MCU が起動した後のプログラムの改竄にたいしての対策を検討する必要がある。この方法として、Chip 全体への耐タンパ機能実装もあるが、コスト面を考えると現実的では無い。ECU の開封時の対応など、他の手法を検討する必要があると考える。

謝辞

本研究を進めるにあたり、セキュアブートプログラム及び、パケット認証システム、リモート管理システムを開発いただいた、KDDI 研究所の藤池氏、北原氏に感謝いたします。

参考文献

1) Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, and Tadayoshi Kohno, "Experimental Security Analysis of a Modern Automobile", IEEE Symposium on Security and Privacy, May, 2010.
2) Stephen Checkoway, Damon McCoy, Brian Kantor,Danny Anderson, Hovav Shacham, and Stefan Savage "Comprehensive Experimental Analyses of Automotive Attack Surfaces", USENIX Security, August, 2011.
3) Charlie Mille and e Mille, "Adventures in Automotive Networks and Control Units", DEF CON 21, August, 2013.
4) 高田広章，松本勉，"載組込みシステムの情報セキュリティ強化に関する提言"，IPA，2013 年 9 月．
https://www.ipa.go.jp/files/000034668.pdf
5) 吉岡顕，小熊寿，西川真，繁富利恵，大塚玲，今井秀樹，"構成証明機能を持つ車内通信プロトコルの提案"，情報処理学会，DICOMO2008，pp.1270-1275，2008 年 7 月．
6) 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”，情報処理学会，CSS2011，pp.624-629，2011 年 10 月．
7) 特許：小熊寿，松本勉，畑正人，田邉正人，吉岡克成，大石和臣，"通信システムにおけるメッセージ認証方法および通信システム"，
https://www.google.com/patents/WO2013065689A1?cl=ja&dq=CAN+message+authentication+ECU&hl=ja&sa=X&ei=0VEhU5OZMcmulAWp4YG4Ag&ved=0CDgQ6AEwA
8) EVITA Project, Hardware Security Module,
http://www.evita-project.org/
http://www.evita-project.org/EVITA_factsheet.pdf
9) HerstellerInitiative Software (HIS), Secure Hardware Extension (SHE),
http://portal.automotive-his.de/index.php?option=com_content&task=view&id=31&Itemid=41&lang=english
10) ルネサスエレクトロニクス，"Security in Automotive Applications" and "ICU", DevCon 2013,
http://www.renesasinteractive.com/file.php/1/CoursePDFs/DevCon_2012/Security/BC05I_FabricePoulard_SecuritySolutionsfortheAutomotiveIndustry_0920_final.pdf
11) ルネサスエレクトロニクス, RH850F1L,
http://japan.renesas.com/products/mpumcu/rh850/rh850f1x/rh850f1l/index.jsp
12) ARM，http://www.arm.com/ja/
13) TCG (Trusted Computing Group),
http://www.trustedcomputinggroup.org/
14) 竹森敬祐，川端秀明，磯原隆将，窪田歩，"Android(ARM)+TMP によるセキュアブート"，電子情報通信学会，SCIS2013，4C1-4，2013 年 1 月．
15) 竹森敬祐，川端秀明，窪田歩，"ARM＋SIM/UIM によるセキュアブート"，電子情報通信学会，SCIS2013，1Ba-2，2014 年 1 月．
16) eMMC，東芝 セミコンダクター&ストレージ社，
http://www.semicon.toshiba.co.jp/product/memory/selection/nand/mlc/emmc/index.html
17) TCG TPM 2.0 Automotive Thin Profile, June, 2014,
http://www.trustedcomputinggroup.org/files/static_page_files/BAA6C75F-1A4B-B294-D0DBC6E5EBDCDD85/TPM%202%200%20Library%20Profile%20for%20Automotive-Thin_v0.91.pdf
18) 中野将志，鵜飼慎太郎，柴谷恵，久保田貴也，汐崎充，藤野毅，"サイドチャネル攻撃対策 AES 暗号と PUF 技術を用いた車載向け耐タンパ認証システムの設計と実装"，信学技報, vol. 113, no. 498, DC2013-93, pp. 139-144, 2014 年 3 月．
19) テセラ，FL-850/F1L-176-S,
http://www.tessera.co.jp/fl/f1l-176.html
20) ルネサスエレクトロニクス，CubeSuite+ for V850
http://www.digikey.jp/product-search/ja?vendor=0&keywords=CUBESUITE+for+V850
21) TOPPERS ATK2,
https://www.toppers.jp/atk2-download.html
22) freescale i.MX6 SABRE-SD,
http://www.freescale.com/ja/webapp/sps/site/prod_summary.jsp?code=i.MX6Q
23) KDDI, KYM11,
http://www.kddi.com/business/mobile/m2m-solution/domestic-m2m/product/kym11/
24) CAN-FD, bosch, “CAN with Flexible Data Rate”, April, 2012.
http://www.bosch-semiconductors.de/media/pdf_1/canliteratur/can_fd_spec.pdf
25) Ethernet AVB, IEEE 802 Audio Video Bridging Task Group,
http://www.ieee802.org/1/pages/avbridges.html
26) TSN，IEEE 802 Time-Sensitive Networking Task Group,
http://www.ieee802.org/1/pages/tsn.html
27) IPA,”2011 年度自動車の情報セキュリティ動向に関する調査”，http://www.ipa.go.jp/files/000024413.pdf
IPA,”自動車の情報セキュリティへの取組みガイド”
http://www.ipa.go.jp/files/000027273.pdf
28) “Hackers release tools, code used to control Ford and Toyota test cars.”
http://www.scmagazine.com/hackers-release-tools-code-used-to-control-ford-and-toyota-test-cars/article/305048/#
29) Forbes “This iPhone-Sized Device Can Hack A Car, Researchers Plan To Demonstrate”
http://www.forbes.com/sites/andygreenberg/2014/02/05/this-iphone-sized-device-can-hack-a-car-researchers-plan-to-demonstrate/
30) インターネット利用者数及び人口普及率の動向
（総務省「平成 19 年通信利用動向調査」より引用）
31) ウイルス届出件数の推移
（出独立行政法人 情報処理推進機構 セキュリティセンター）