ドライバーに安心を提供する車載セキュリティシステム

Vehicle Security System to Enhance Driver Safety

川端　健　■KAWABATA Takeshi
駒野　雄一　■KOMANO Yuichi
磯崎　宏　■ISOZAKI Hiroshi

車載システムでは，自動運転の実現につながる高度化や，機能不全によるリスクを低減するための機能安全に対する取組みが進んでいる。近年，高度化が進む車載システムの変化に伴い，機能安全の脆弱（ぜいじゃく）性を狙って，制御をリモート操作するような攻撃が報告されるようになってきた。このような悪意のある攻撃者に対処するためには，車載システムを適切な境界で監視し，セキュアな機能領域を確保することが必要である。

このようななか，東芝は，ドライバーや車載システム開発者に安心を提供する車載セキュリティシステムの構築に向け，車外NW（ネットワーク）との境界となる車両内V2X（Vehicle to X）システムにおける高速な署名認証技術や，車載システムの機能境界の適切な分割と必要なセキュリティコンポーネントの組合せによるセキュリティアーキテクチャなどを開発している。

The development of increasingly sophisticated functional safety features for in-vehicle systems is progressing, aimed at realizing autonomous car systems and reducing the risk of hazards caused by malfunctional operations. However, the expansion of sophisticated in-vehicle systems in recent years has been accompanied by a higher risk of such systems being hijacked by cyberattacks targeting vulnerabilities in their functional safety features. To construct a vehicle security system that provides safety to both developers and drivers, protection from malicious hackers is necessary through supervision at the appropriate boundary and implementation of a secure functional area.

In response to this situation, Toshiba is developing a high-speed signature authentication technology to secure in-vehicle vehicle-to-X (V2X) systems at the boundary between the areas inside and outside the vehicle network and a security architecture to combine the required security components by appropriately dividing in-vehicle functional boundaries.

1　まえがき

先進運転支援システム（ADAS）やインフォテインメントシステムなどの車載システムは，交通事故の削減や渋滞緩和に向けた高度化が進んでいる。このような車載システムの高度化の進展は，自動運転につながると期待されている。一方，車載システムの高度化は，SW（ソフトウェア）の大規模化や，機能連携を実現するNW化，低コスト化を目的としたオープン化（モジュール化）などの変化をもたらしている。

車載システムの変化によって，従来のクローズドシステムと違い，攻撃のきっかけとなる情報の入手や推測がしやすくなってきており，2006年頃から学会で車載システムの脆弱性を指摘する報告がされている。代表的なものとして，タイヤ空気圧監視システムの無線通信や，車両診断を行うための通信・コネクタ規格OBD-Ⅱの検査ポートなどの脆弱性[1), 2)]がある。

これらの報告に共通しているのは，NWを介して攻撃されているという点である。特に無線NWは，車内へ侵入せずに攻撃ができるので，攻撃の事実をドライバーが気づきにくいという特徴がある。また，高価な攻撃ツールは用いずに，組込み機器やパソコンに対して使われている従来の攻撃手法を組み合わせているものが多い。しかし，従来の対策手法をそのまま適用することはできない。他業界と違い，車載システムに求められるセキュリティ特性や，高信頼性，リアルタイム性，各マイコンに対するコスト要件などが大きく異なるからである。

東芝は，車載セキュリティ技術として，ドライバー及び開発者に安心を提供するためのセキュリティシステム及びコンポーネントの開発を行っている。

2　海外の車載セキュリティ技術の動向

車載セキュリティは，欧米などで先行して検討されており[3)–5)]，二つのカテゴリーに分けられる。自車と自車外の間の通信を守るV2Xセキュリティと，自車内セキュリティである。

V2Xシステムは，異なる自動車間やインフラとの通信を行うため，統一仕様である必要があり，セキュリティ検討も先行している。欧州と米国は，共に公開鍵（PKI）をベースとしたセキュアシステムを構成しているが，運用方法に関する提案には差異があり，現在これを調整する検討が進められている。

自車内セキュリティは，自車内システムの制御情報が不正に変更されないための対策が，NW視点及び制御SW視点を中心に検討されている。必要になるセキュリティコンポーネントは，様々なプロジェクトから提案されており，代表的なものとして，EVITA（E-Safety Vehicle Intrusion Protected Applications）[6)]や，SHE（Secure Hardware Extension）[7)]，TPM

(Trusted Platform Module)[8]などがある。しかし，自車内システムに対するセキュリティは，システムデザインポリシーに依存し，各社のシステムデザインが統一されていないため，セキュリティデザインも統一することが難しく，検討が十分に行われていない。

3　車載システムに求められるセキュリティデザイン

3.1　攻撃者視点の理解

セキュリティデザインにおいて，攻撃者視点の理解が必要な理由には，ここで述べるような背景がある。

車載システムに対する脅威は，交通事故などの人的被害を与えるリスクを持つ。この場合，脅威は意図的な脅威，つまり攻撃者による脅威のことを指す。また，脅威はあっても起こりえない脅威であれば，それはリスクにならない。つまり，攻撃者による攻撃可能性の高さに応じてリスクが高まることになる。

攻撃者による攻撃可能性の高さを検討する際に，攻撃者の活動ステップをモデル化する。

悪意のある攻撃者による活動は，次の二つのステップで行われる。まず，侵入可能な境界（以下，Attack I/Fと呼ぶ）を探し，車載システムに侵入する。そして，侵入後に目的を果たすための調査及び攻撃活動を行う。

また，悪意のある攻撃者だけが，車載システムを脅かすわけではない。例えば，ドライバーによる車載システムのカスタマイズ行為によって，Attack I/Fを増やしてしまう可能性がある。カスタマイズ行為を許容するかどうかは，適用システムのデザイン設計の一部である。

したがって，攻撃者による攻撃の入口となるAttack I/Fを検討することが攻撃者の視点でのセキュリティデザインとなる。

3.2　車載システムの特徴

車載システムは，次のような特徴を持つため，セキュリティデザインでは，それらを十分に考慮する必要がある。

(1)　セキュリティ特性　　車載システムで優先されるセキュリティ特性は，完全性である。一方，一般の業務システム及び制御システムで優先されるセキュリティ特性は，前者が機密性であり，後者が完全性と可用性である。しかし，車載システムでは，求められる特性に近い制御システムを流用することが簡単にはできない。これは，制御システムと車載システムのデザインポリシーが異なるためである。例えば，制御システムでは一般ユーザーに対するカスタマイズ性などの自由度を必要としない。

(2)　車載システムの進化　　従来の車載システムは，単機能の集合体であった。しかし現在は，機能連携によるシステムの複雑化や高度化が進展し続けており，変化の激しい成長期にある。

また，車載システムの変化は，制御機能に関わる高度化だけではなく，メンテナンス性も高める動きがある。現行の車検時に用いられる，メンテナンス用のOBD-Ⅱの検査ポートは，物理的なアクセスにより車載システム内の状態確認や，ECU（電子制御ユニット）のファームウェア更新が可能である。また，このメンテナンスをリモートで行えるようにすることが望まれている。

(3)　企業連携を要する業界構造　　車載システムのデザイン・製造方法は，従来の垂直統合型から，多企業連携による部分的水平分業型へと変化している。水平分業型への変化は，競争力強化などのメリットがある一方，機能モジュール間の公開情報が増加するため，Attack I/Fの発生や増加の可能性を秘めている。

また，多企業連携におけるセキュリティ運用は，リスクも高まる傾向にあり，十分な検討が必要である。例えば，車載システム内の複数のECUに対し，それぞれのECUが保持する暗号鍵を誰が埋め込むのかなどの課題が発生する。

(4)　厳しい性能・資源制約　　車載システムの制御に対するリアルタイム性の要求は，ドライバーの操作性だけでなく安全性にも影響があるため，厳しいものとなっている。また，そこで用いられる制御ECUなどは，コスト面での資源制約がかなり大きい。そのため，セキュリティデザインに対しても，低コストでの実現が求められる。

(5)　長寿命性　　自動車は，15～20年間の利用を可能にする必要があるため，その間に進化する攻撃の高度化にも対応できるセキュリティシステムが求められる。

3.3　車載システムのセキュリティデザイン検討

セキュリティデザインは，攻撃者の視点と車載システムデザインによって決まる。ここでは，**図1**のような車載システムの構成をベースに検討を行う。

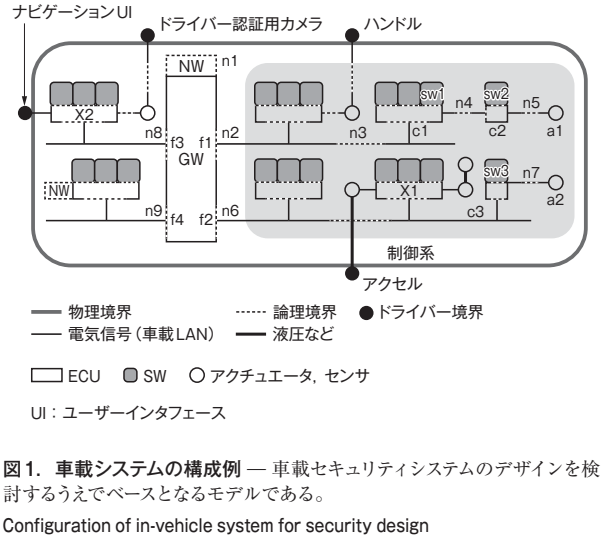

図1．車載システムの構成例 ― 車載セキュリティシステムのデザインを検討するうえでベースとなるモデルである。

Configuration of in-vehicle system for security design

(1) 物理境界と論理境界　　物理境界は，物理攻撃を防ぐだけでなく，物理攻撃かサイバー攻撃かを判別するうえでも重要である。現在，車載システムの物理境界は，スマートキーを用いた所有者認証であることが多い。メンテナンス者や車載機器を守るには，物理境界での個人認証が必要である一方で，認証機器に必要なエネルギー供給源は限られているため，セキュリティ確保を物理境界だけに頼ることは難しい。また，アクチュエータとECUが，専用工具などを要する物理パッケージになっている場合がある（図1のX1近傍）。このような場合でも，正規のメンテナンス者以外が専用工具を入手できれば，攻撃を防ぐための物理境界にはなりえない。

論理的境界のAttack I/Fは，車載NWとなる場合が多い。車載システムで用いられるNWには，無線及びCAN（Controller Area Network）などの有線がある。無線は，物理境界がないことが使用上のメリットだが，反面もっとも大きな脅威になることは言うまでもない。

(2) 守るべき論理エリアの明確化（局所化）　　セキュリティデザインは，攻撃者による攻撃目的・対象が何であるかによって変わる。車載システムの守るべきエリアは，制御系である。これは，攻撃者によって制御が奪われ，制御不能になるリスクがあるからであり，図1では，守るべきエリアをグレーで示してある。

守るべきエリアである制御系の持つ機能を，その境界で他の機能と分離することで，論理エリアを局所化できるが，将来的な機能拡張も予測したデザインが必要になる。

(3) 論理境界と意味境界　　図1では，論理境界をゲートウェイ（GW）で分離し，各部品境界を小文字の英字と数字から成る記号で示してある。既に，車載システムでの攻撃例として報告されているのは，nと数字から成る記号で表されるNWの論理境界を経由しているものである。また，部品のベースとなるECUとの境界及びセンサやアクチュエータとの境界が，cと数字から成る記号及びaと数字から成る記号で示してあり，部品の機能を実現するために必要なSWの境界がswと数字から成る記号で示してある。

攻撃者のターゲットは，攻撃の効果を見いだしやすい，意味のある境界（以下，意味境界と呼ぶ）への侵入である。

一般に，意味境界はアクチュエータへの境界になる。アクチュエータは車両の制御に直接関わるので，攻撃者にとって効果が得やすいためである。つまり，攻撃者は車載NWから侵入しアクチュエータを操作することを目的としている。センサは，車両内外のシステムの状況を把握するためにあるので，攻撃により状況把握を狂わせ二次的に影響を及ぼすことが可能である。つまり，センサ及びアクチュエータ自身であるa1及びa2や，その情報を扱うsw2及びsw3が，もっとも脅威を受ける対象となる。

ここで注意すべきことは，意味境界は技術進化に伴い変化することである。例えば，あるセンサに関連した脅威分析をした時点では意味境界でないと分析されたものが，異なる役割に利用されることで攻撃脅威にさらされる可能性がある。

車載システムの技術進化が著しいことを考えると，攻撃可能になりうる境界は広範囲に及ぶと予想される。

車載システムをシンプルな構成にし，各境界が脅威にさらされにくいルール作りが必要になる。ルール作りには，いつ（When），誰が（Who），どこから（Where）及びどこに（Where），どのように（How），どのぐらいのコストで（How much又はHow many）といった4W2Hが重要となる。また，ルール作りの基盤としては，暗号機能が使いやすく，一般化しやすい。

3.4 開発・運用プロセスのデザイン検討

システムそのもののデザイン以外に，車載システムの長期ライフサイクルや人とモノの境界を十分に考慮する必要がある。

ライフサイクルは，開発ライフサイクルと運用ライフサイクルに分かれる。セキュリティコンポーネントの一つとなる暗号機能の鍵管理は，両ライフサイクルに大きな影響を及ぼす。開発時の鍵の管理者の局所化や運用中のメンテナンス時に用いられる鍵の扱いには，技術サポートが不可欠である。また，SWアップデートは，運用ライフサイクルにおいて重要な役割を担い，4W2Hの管理が必須となる。

人とモノの境界には，開発者と技術仕様の問題や組立て者と部品仕様の問題がある。SW開発者のSW・HW（ハードウェア）仕様に対する理解が不十分なために引き起こされる不具合が，リスクにつながるケースが多い。また，組立て者が部品調達時にセキュリティ要件を満たしているかを判断することは難しい。前者は技術サポートが，後者は評価認定などの仕組みが重要になる。

4 車載セキュリティに対する取組み

当社の車載セキュリティに対する取組みの中で，代表的な例として，車載システムのAttack I/Fに配置される暗号コア及び車載NWの中継を担うGWへの取組みについて述べる。

4.1 暗号コア

V2Xシステムに対しては，デジタル署名ベースの高速署名認証が要求されるため，低レイテンシで実行可能な公開鍵暗号の開発を行っている。

また，V2Xシステムだけでなく自車内システムでは，改ざん検出や秘匿を目的とした共通鍵暗号が要求されている。これらの暗号コアは，NW上の改ざんやなりすましを抑止するだけでなく，許可されたプロセスでしかECU内のSWを起動できなくするセキュアブートとしても用いられる。

暗号コアの秘密鍵の漏えいは，システムデザインの安全性を

脅かす。当社は，物理攻撃が比較的容易な環境で使われるICカードに対し，内部構造などの解析をしにくくして攻撃を防御する耐タンパ実装技術を保有している。これをベースに，車載システムでは，鍵の更新頻度に合わせて耐タンパ性を確保する暗号実装技術を開発している。

4.2 車載GW

開発中の車載GWは，多くの主要なECUコアや車外NWチップと接続することを想定しており，機能境界になる。これが管理する機能とそのセキュリティ要件を次に示す。

(1) ECUのSW管理　SW更新では，車両外からSWが入力されるため,4W2Hで管理する仕組みが必要である。すなわち，正規更新者（Who）の更新要求だけを受け付け，改ざんされたら検知可能な仕組み（How）で，更新対象のECU（Where）に対して，更新可能なタイミング（When）で，適切な領域（How many area）に送信する必要がある。これらの管理機能は，正規の車載システム設計者だけが，自由に選択可能にする必要がある。

(2) ECUの鍵管理　ECUは，複数のチップベンダーによって開発されるため，チップごとに秘密鍵を管理する必要がある。このため，各ベンダーからの提案は，開発者や開発体制などで鍵を厳格に管理する運営を前提としているものが多い。そこで，鍵管理主体をGWに集約して各ECUベンダーでの鍵の管理運営を緩和する方式,NW非依存な論理的グルーピング方式，及び鍵の値に対する物理解析耐性のあるPUF（Physically Unclonable Function）ベース方式の三つの特徴を持った鍵管理方式の開発を行っている。更に，車載システムのライフサイクルを見通した鍵管理についても検討を行っている。

5 あとがき

車載システムにおけるセキュリティの検討で重要となるAttack I/F，及び車載セキュリティシステム開発における当社の取組みについて述べた。

自動運転の車載システムでは，攻撃者によって攻撃されたとしても影響がドライバーなどの命に及んではならない。既知攻撃に対するAttack I/Fでの“防御”や“検知”などの対応策は，他業界でも検討されているが，これを適用するには車載システム要件に合わせたカスタマイズが必要になる。特に，各部品境界は，セキュリティレベルの統一や標準化が必要である。

また，車載システムの長期ライフサイクルに伴う未知攻撃への対応や，SW更新，多企業連携を含めた人とモノの間のリスクを軽減する技術など，業界独自のセキュリティも必要になってくる。

自動運転時代に向け，今後も，サイバー攻撃などの悪意のある攻撃者からドライバーを守り，安心を提供する車載セキュリティシステムの研究開発を行っていく。

文　献

(1) Rouf, I. et al. "Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tier Pressure Monitoring System Case Study". Proceedings of the 19th USENIX Security Symposium. Washington DC, USA, 2010-08, USENIX Association. 2010, p.323－338.

(2) Koscher, K. et al. "Experimental security analysis of a modern automobile". 2010 IEEE Symposium on Security and Privacy. Berkeley, CA. USA, 2010-05, IEEE. 2010, p.447－462.

(3) Fraunhofer SIT. "EVITA E-safety Vehicle Intrusion protected Applications". EVITA. <http://www.evita-project.org/>, (accessed 2016-01-08).

(4) Oversee. "open vehicular secure platform". Oversee. <https://www.oversee-project.com>, (accessed 2016-01-08).

(5) OST-R. "Safety Connected Vehicle Safety Pilot". ITS JPO. <http://www.its.dot.gov/safety_pilot/safety_pilot_plan.htm>, (accessed 2016-01-08).

(6) Weli, B. et al. Secure On-board Architecture Specification. EVITA. 2010, Deliverable D3.2, 299p.

(7) Daimler. "HIS - Hersteller Initiative Software". HIS. <http://portal.automotive-his.de/>, (accessed 2016-01-08).

(8) Trusted Computing Group. "TCG TPM2.0 Library Profile for Automotive-Thin". Trusted Computing Group. <https://www.trustedcomputinggroup.org/resources/tcg_tpm_20_library_profile_for_automotivethin>, (accessed 2016-01-08).

川端　健　KAWABATA Takeshi
研究開発統括部 研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー研究主務。暗号技術及び暗号応用システムの研究・開発に従事。
Computer Architecture & Security Systems Lab.

駒野　雄一　KOMANO Yuichi, D.Sci.
研究開発統括部 研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー研究主務，博士（理学）。暗号技術及び暗号応用システムの研究・開発に従事。電子情報通信学会，IEEE，IACR会員。
Computer Architecture & Security Systems Lab.

磯崎　宏　ISOZAKI Hiroshi, D.Med. and Gov.
研究開発統括部 研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー主任研究員，博士（政策・メディア）。組込みセキュリティ技術及びIoTセキュリティ技術に関する研究・開発に従事。
Computer Architecture & Security Systems Lab.