特集論文

自動車機器での製品セキュリティへの取組み

松井俊憲* 高塚雄也***
山口晃由** 井上知之†
跡部悠太***

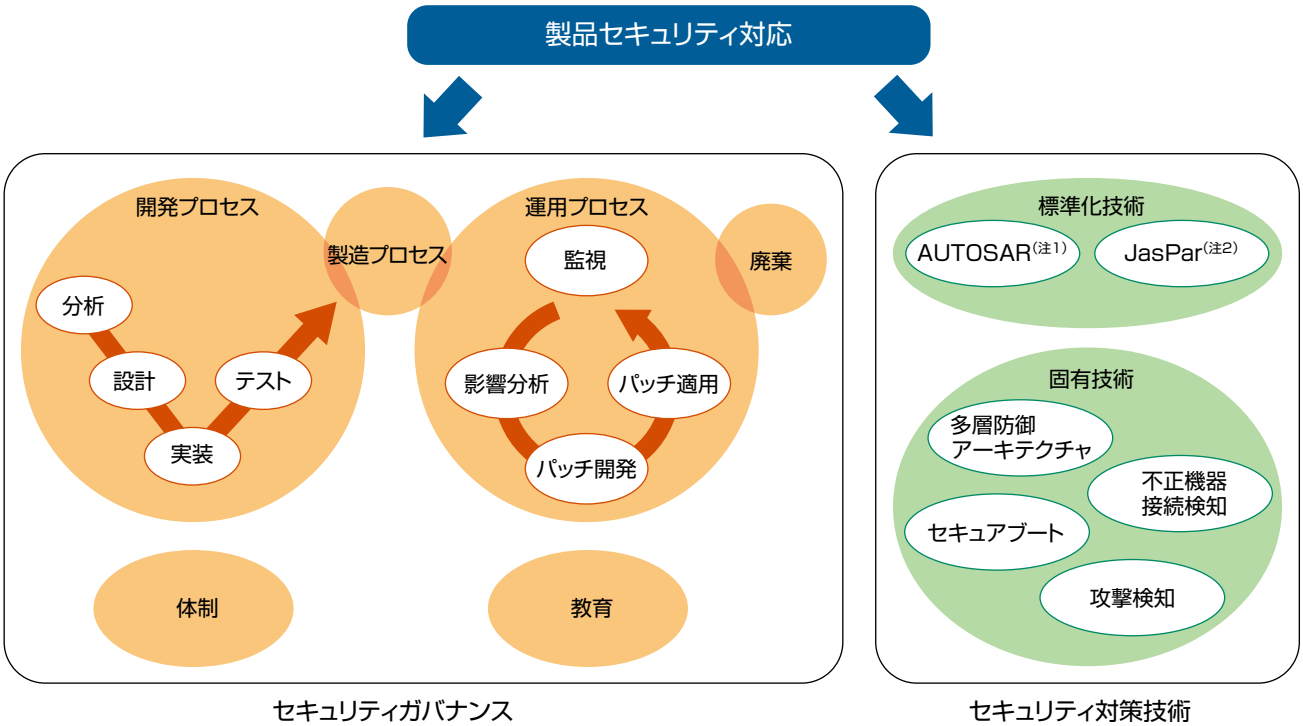
Approach to Product Security in Automotive Equipments

Toshinori Matsui, Teruyoshi Yamaguchi, Yuta Atobe, Yuya Takatsuka, Noriyuki Inoue

要　旨

車外から情報を入手するコネクテッドカーでは，新たな機能を提供できる反面，サイバー攻撃の対象にもなり得る。そのため自動車機器でもセキュリティ対応が必要となる。セキュリティ対応では，セキュリティポリシーに基づくライフサイクル全体のプロセス定義と体制整備，教育といったセキュリティガバナンス，及びサイバー攻撃から自動車機器を守るセキュリティ対策技術を準備する必要がある。

三菱電機では，自動車機器の製品ライフサイクル全体のプロセスとして開発・製造・運用・廃棄でのプロセス定義を進めている。開発プロセスでは，構築済みの品質と機能安全の要件に対応した開発プロセスにセキュリティの要件を融合させ，“Safety & Security開発プロセス”として定義した。運用プロセスでは，出荷後の脆弱(ぜいじゃく)性情報を監視し，脆弱性情報の検出をトリガーに関係者が連携して対応するプロセスを定義した。さらにこれらプロセスを円滑に回すための体制として，PSIRT(Product Security Incident Response Team)を各拠点に設け，研究所等の社内連携も明確にした。またセキュリティ対策技術では，AUTOSAR，JasPar等が規定する標準化技術を準備するだけでなく，固有技術も準備している。固有技術では，多層防御アーキテクチャ，起動時に正当なプログラムであることをチェックするセキュアブート，発生順序の特徴を見つけ出すことで巧妙化する攻撃を検知できる攻撃検知技術，車載ネットワークへの不正機器接続検知技術等を開発している。



（注１） AUTOSARは，AUTOSAR GbRの登録商標である。
（注２） JasParは，㈱ネクスティエレクトロニクスの登録商標である。

製品セキュリティ対応に必要な要素

自動車機器での製品セキュリティ対応は，セキュリティガバナンスとセキュリティ対策技術の側面がある。セキュリティガバナンスは，セキュリティポリシーをベースとした製品ライフサイクルの各プロセスの実施内容の規程，プロセスを円滑に回すための体制，教育が含まれる。セキュリティ対策技術は，標準化技術と固有技術に分類される。標準化技術はAUTOSARやJasPar等が規定する非競争領域となる対策技術であり，固有技術は競争領域として当社が力を入れている対策技術となる。

*自動車機器開発センター　**情報技術総合研究所(工博)　***同研究所
†自動車機器業務部

1. まえがき

自動車産業を取り巻く環境の大きな変化の一つとして，乗員にとってより便利な機能を提供するために，自動車に搭載される機器は，自身が持つセンサや車内の別の機器から情報を入手するだけではなく，コネクテッドカーとして車外とつながって様々な情報を入手するようになってきている。車外とつながることで，より多くの情報を入手することができるが，一方で，パソコン，IoT(Internet of Things)機器等と同様にセキュリティ上の脅威にさらされ，サイバー攻撃の対象となり得る。車載システムやシステムを構成する個々の機器をサイバー攻撃から防御するための製品セキュリティ対応は，出荷の段階で全てが完了するわけではなく，出荷後に出現する新たな脅威への対応も求められる。これらの対応が不十分であると，カーナビゲーションシステム等に保存されている電話帳などの個人情報が盗まれたり，自動車を車外から操作されて安全が脅かされたりすることになり得る[1]。今後，通信インフラの整備に伴ってコネクテッドカーが増加することが予想されることからも，製品セキュリティ対応が急務になっている。

製品セキュリティ対応には，自動車業界としても取組みを進めている。この一つの動きとして，ライフサイクル全体でのセキュリティ要件をまとめた国際標準(ISO21434)が2020年に発行される予定である。当社は，公益社団法人 自動車技術会を介して，国際標準の策定活動にも力を入れている。

2. セキュリティガバナンス

製品セキュリティ対応では，**図1**に示す製品ライフサイクル全体をカバーする開発・製造・運用・廃棄プロセスとそれを円滑に回すために関連部門と連携する体制が必要となる。これらのプロセスと体制は，企業が定めるセキュリティポリシーに基づくセキュリティガバナンスとなる。プロセスと体制は規則化し，定期的に見直していくことが重要となる。

当社での自動車機器の開発でも，自動車機器サプライヤーとして，安全性の高い製品と顧客・ユーザーへ安心安全を提供するため，セキュリティに関する取組みの継続的な推進・改善を進めることを目的としたセキュリティポリシーを策定し，それに基づく体制とプロセスの整備を進めている。

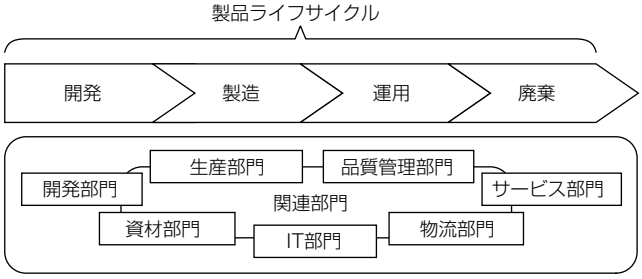


図1．製品ライフサイクル全体

2.1 製品ライフサイクルでのプロセス

自動車機器での製品ライフサイクルは，開発プロセス，製造プロセス，運用プロセス，廃棄プロセスの流れになる。それぞれのプロセスで，製品セキュリティ対応として実施すべきことを明確にしている。

2.1.1 開発プロセス

開発プロセスでは，まず，機能安全とセキュリティの開発プロセスを共通化して効率的に開発できるように，機能安全に対応した開発プロセスに，セキュリティ対応として求められる要件を融合させたSafety & Security開発プロセス(S&S開発プロセス)を策定した。さらに，**図2**に示すようにS&S開発プロセスでの分析・設計・実装・テストの各フェーズの実施を支援するガイドを作成している。各ガイドの特徴を次に示す。

(1) 分析ガイド：機能安全の分析結果に対して，当社が持つセキュリティ分析技術に自動車業界で検討されているセキュリティ分析技術の要素を加えた自動車機器向けのセキュリティ分析技術を用いて，網羅的に分析するための手順を明確化している。

(2) 設計ガイド：分析結果から導出されたセキュリティ対策のコンセプトを，システム・ハードウェア・ソフトウェア設計で作り上げる具体的な対策とするための手順を明確化している。さらに，当社の情報システム，重要インフラ向けのセキュリティ対策実績を元に，分析結果と対策が紐(ひも)付いたリストを作成することによって，自動車分野でも対策を導き出すことを効率化している。

(3) 実装ガイド：セキュリティ対策を盛り込んだコードを作成するために守るべきセキュアコーディングルールを明確にするとともに，AUTOSARやJasParをベースとしたセキュリティ対策での標準化技術(メッセージ認証，Hardware Security Module等)の実装と適用方法を明確にしている。作成したコードに脆弱性が含まれていないか，コーディングルールが守られているかを解析するツールの導入も併せて実施している。

(4) 評価ガイド：セキュリティに特化したテストとして，テスト対象の動作状態と連動させたファズテストを実施する評価環境と評価手順を明確にしている。さらに，侵入テストを軸にしたより実践的なセキュリティテストを実施する体制を整えている。

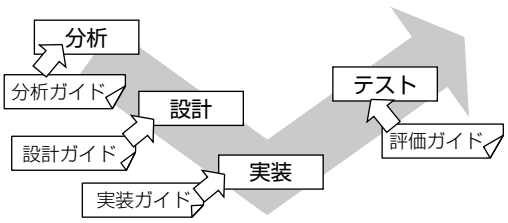


図2．開発プロセスを支援するガイド

2.1.2 製造プロセス

製造プロセスでは，セキュリティ対策を行う上でベースとなる暗号化に必要な鍵情報や，機器に実装するプログラムやデータといった秘密情報を製造ラインでどのように管理し，取り扱うかについて明確にしている。

2.1.3 運用プロセス

運用プロセスで，PSIRTは，開発・販売する製品について脆弱性情報の収集と分析を行い，対策の実施を支援する役割を担う。

脆弱性情報については，まず自動車関係のサイバーセキュリティに関する情報を共有し，連携して対策に当たる組織である米国Auto-ISAC(Automotive Information Sharing and Analysis Center)に加入して自動車業界固有の情報収集を行っている。またIT(Information Technology)分野を源流として，今後車載適用が増えてくるOS(Operating System)や通信等の技術についての脆弱性情報も監視するためにJPCERT/CC(Japan Computer Emergency Response Team Coordination Center)等からの情報収集も行っている。さらにOSS(Open Source Software)などの脆弱性情報を検出するツールも導入している。なお，製品に関する脆弱性情報は収集するだけでなく，外部から直接報告される場合に備えて，情報収集の窓口を設けて対応している。

脆弱性を悪用され被害が発生した場合や被害が発生する可能性が高い場合はインシデント対応を実施する。対応では，PSIRTが影響度，緊急度を基にインシデントのレベルを算出し，レベルに応じてPSIRTと製作所が連携するだけでなく，自動車メーカーや関係するサプライヤーチェーンと連携して対応する。

2.1.4 廃棄プロセス

廃棄プロセスでは，個人情報や鍵情報，プログラムそのものが流出しない仕組みを組み込んでいくことが必要になる。そのために，ソフトウェアでの対策だけではなく，ハードウェアを連携させた対策を進めている。

2.2 体　　制

体制として，実際に自動車機器を開発する当社製作所には，脆弱性の影響分析と教育を行う組織を立ち上げるとともに，製作所を統括する事業本部に脆弱性情報の監視と製作所のプロセスの改善を支援する組織をそれぞれ2018年度に立ち上げた。これらの組織は，**2.1.3項**で述べた製品セキュリティインシデント対応チーム(PSIRT)となる。

3. セキュリティ対策技術

この章では，車載システムや機器に搭載するセキュリティ対策技術について述べる。

3.1 車載システム向け多層防御アーキテクチャ

従来の車載システムでは，各機器は単独でセキュリティを担保している。しかし，搭載されたセキュリティ対策は各々守るべきところが異なるため，車載システム全体のセキュリティとしては不十分になるおそれがあった。この課題を解決するため，各機器に搭載する複数のセキュリティ対策で補完させることで，従来よりも強固なセキュリティを実現する多層防御アーキテクチャを開発した。この多層防御では，一つのセキュリティ対策では守れない攻撃に対し，別の一つ又は複数の対策を組み合わせて補完することでセキュリティを強化する。例えば，ソフトウェア改ざんを目的とした攻撃に対し，起動時には，**3.2節**で述べるセキュアブートで対応し，起動後の攻撃については攻撃検知で対応する，といった補完関係を持たせた。また，車載システムにはカーナビゲーションシステムを代表としたインフォテイメント系から，ハンドルを操作したり，運転支援をしたりする走行安全系の機器があり，それぞれリアルタイム性や接続性などの特性が異なる。そのため，各機器の特性に適したセキュリティ対策を選定することによって，車載システム全体のセキュリティを確保することを可能にした。

3.2 自動車機器向けセキュアブート

近年，組み込み制御機器で，不正プログラムを実行させないために，実行するプログラムの電子署名を検証することで，正当なプログラムであることをチェックするセキュアブートの採用が増えている。自動車機器でも同様にセキュアブートの採用が増えることが予想される。しかし，従来のセキュアブート方式の場合，ソフトウェア本体とその電子署名を丸ごと古いバージョンに戻すダウングレードを機器単体で検証できない[(2)]。そこで，この課題を解決するセキュアブート方式を開発した[(3)]。

この方式では，機器単体でダウングレードの検証を行うため，初回起動時の署名検証の過程で生成されたハッシュ値をセキュアな領域に格納し，２回目以降のセキュアブートに活用することで，ダウングレードが発生しても，セキュアな領域内のハッシュ値との比較によって検証可能になる。

セキュアブートには，秘密情報の秘匿や改ざん防止のため，ハードウェアで保護されたセキュアな領域が必要になる。よって，SoC(System on a Chip)内に通常の非セキュアな演算を行う主演算部と，鍵などの秘密情報の安全な格納とそれを用いた演算を内部で行えるセキュリティ演算部を搭載するプラットフォームを前提とする。

今回開発したセキュアブート方式を**図３**に示す。ブートローダに含まれるTEE(Trusted Execution Environment)などの既存のセキュアブート機能との併用を可能にするため，ブート時に各ソフトウェアの完全性検証を署名検証ベースで行い，各ソフトウェアのハッシュ値を収集し，あらかじめ計算しておいたMAC(Message Authentication

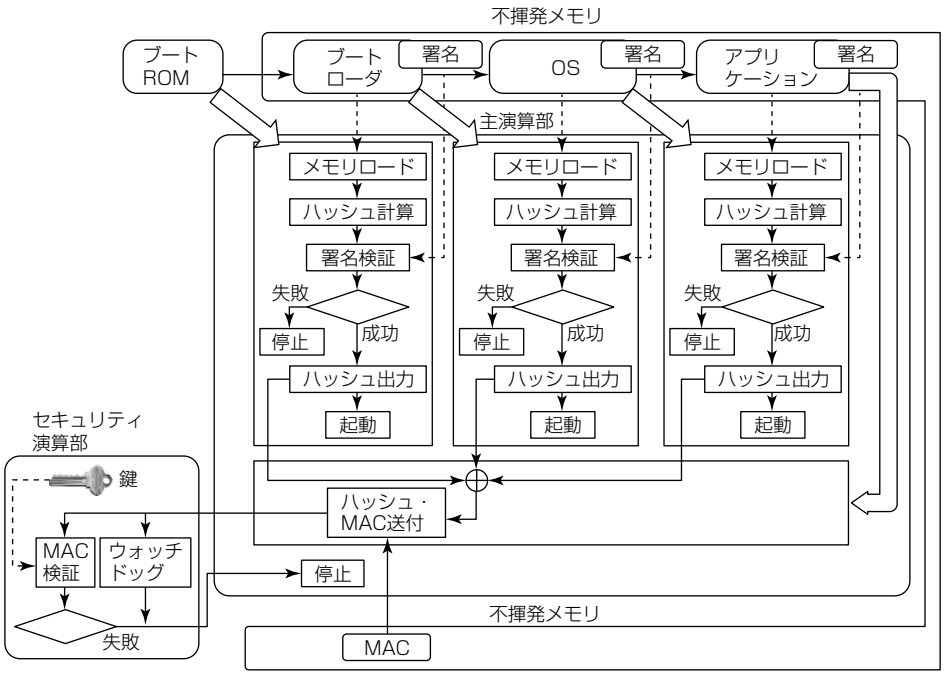


図3．開発したセキュアブート方式の動作

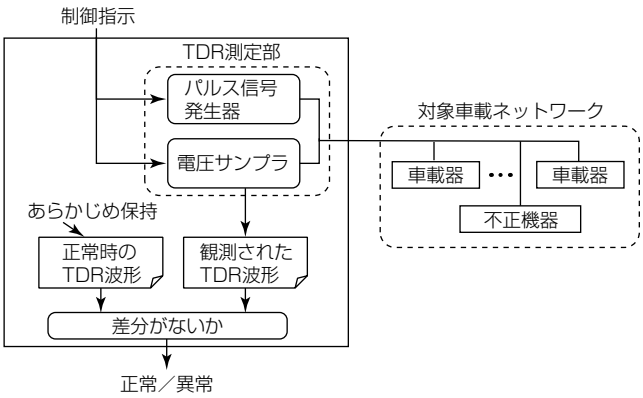


図4．不正機器接続検知方式

Code)とともにセキュリティ演算部に送り，セキュリティ演算部内にある鍵でMACの検証を行う。これによって，ダウングレードを検知する。

3.3　車載システム向けサイバー攻撃検知

従来，外部からのサイバー攻撃に対しては，通信パケットを監視し，攻撃指示が仕込まれているかを検査していたが，攻撃指示の複雑化・巧妙化につれ，対応が困難となっている。しかし，攻撃対象システムに焦点を置き，過去のサイバー攻撃の事例を調査すると，攻撃者が目的を達成するために必ず実施せざるを得ない攻撃の手口があること，複数の攻撃手口は発生順序に特徴があることが分かった。これらに基づき，車載システム向けサイバー攻撃検知では，攻撃者が必ず実施せざるを得ない攻撃手口による痕跡を捉え，攻撃目的に基づく発生順序の特徴を見つけ出すことで，攻撃指示が複雑化・巧妙化したサイバー攻撃を高精度に検知することを可能にした。

3.4　不正機器接続検知

カーシェアでは，遠隔からのサイバー攻撃だけでなく，車両へ物理的に機器を取り付ける攻撃についても考慮する必要がある。攻撃者は，不正機器を車載ネットワークへ物理的に後付けすることで，自動車の走行制御を乗っ取ることができる。この課題に対し，不正機器が車載ネットワークへ後付けされていることを検知する不正機器接続検知技術を開発している。

この技術では，ネットワークの電気的特性を観測するTDR(Time Domain Reflectometry)技術[4]を応用する。TDR技術は，高周波ステップ信号を印加し，それに対する反射応答を時間波形として観測する。**図4**に開発した不正機器接続検知方式を示す。この方式では，不正機器が接続されていない状態の正常時のTDR波形をあらかじめ保持しておき，不正機器の後付けを検査する際にTDR波形を観測し，正常時のTDR波形と比較する。ネットワークの電気的特性は機器の接続構成によって一意に定まるため，観測されたTDR波形と正常時の波形に差分があれば，不正機器の後付けがあったと検知できる[5]。

4. むすび

自動車機器の開発から市場での運用，廃棄までの製品ライフサイクルを通じたセキュリティ対応プロセスと体制構築，及びセキュリティ対策技術を述べた。

今後も自動車機器のセキュリティを向上させるため，継続的な推進・改善や技術開発を行っていく。

参考文献

(1) Charlie Miller，et al.：Remote Exploitation of an Unaltered Passenger Vehicle (2015) http://illmatics.com/Remote%20Car%20Hacking.pdf
(2) Matteo Carlini：Secure Boot on Arm system，Linaro connect San Francisco 2017 (2017)
(3) 山口晃由，ほか：組み込み制御機器におけるセキュアブート方式の検討，SCIS 2019 3D2-3 (2019)
(4) Dascher，D. J.：Measuring Parasitic Capacitance and Inductance Using TDR，Hewlett-Packard Journal，**47**，No.2，83～96 (1996)
(5) 跡部悠太，ほか：TDRを用いた不正機器の車載ネットワーク接続検知に関する一検討，SCIS 2019 1E2-2 (2019)