Rev. March 19, 2015

**Trusted Computing Group (TCG)と自動車セキュリティ**
**2015 年 3 月**

**Q. Trusted Computing Group (TCG)の自動車セキュリティにおける取り組みについて教えてください。**
A. TCG と自動車市場の SoC (System-on-a-Chip)技術とその他の自動車部品のサプライヤである TCG 会員は、いくつかの TCG 仕様と技術は、今日の「つながるサービス」を目指す自動車市場において根本的なセキュリティ課題に対処するには最適な技術であると確信しています。

**Q. これまでパソコンやコンピュータ機器などに使われていたセキュリティ技術が、なぜ自動車に必要なのでしょうか？**
A. つまり、今日の自動車は、車輪が付いているコンピュータと同じです。ほとんどの自動車には 100 以上のプロセッサが搭載されており、それぞれの OS、ファームウェア、アプリケーションで動いています。これらのほとんどは組織内の閉じたネットワークで繋がっていますが、これらは無線のモデムや Wi-Fi 経由で更に広い世界へと接続されるようになってきています。何種類ものシステムとネットワークが、複雑な小規模のコンピュータの集まりによって作られます。そしてそれらは、遠隔やネッ直接接続で、システムへの不正侵入やマルウェア等での攻撃を受けやすい環境になっています。

**Q. 自動車の中のコンピュータシステムをセキュアにするための TCG の役割とは何ですか？**
A. TCG は、数年前に組み込みシステム部会 (EmSys) を設立しました。当部会は、自動車セキュリティにおいて重要な以下 2 点の脆弱性に注力し取り組むことを決意しました。
(a) 製造側/第三者と自動車間のデータ通信
(b) 自動車を制御する車載機器、電子制御装置(ECUs)の完全性。つまり、メモリを積んでいる小さなパソコンが、ファームウェアとアプリケーションソフトで動作するのと似たようなことです。

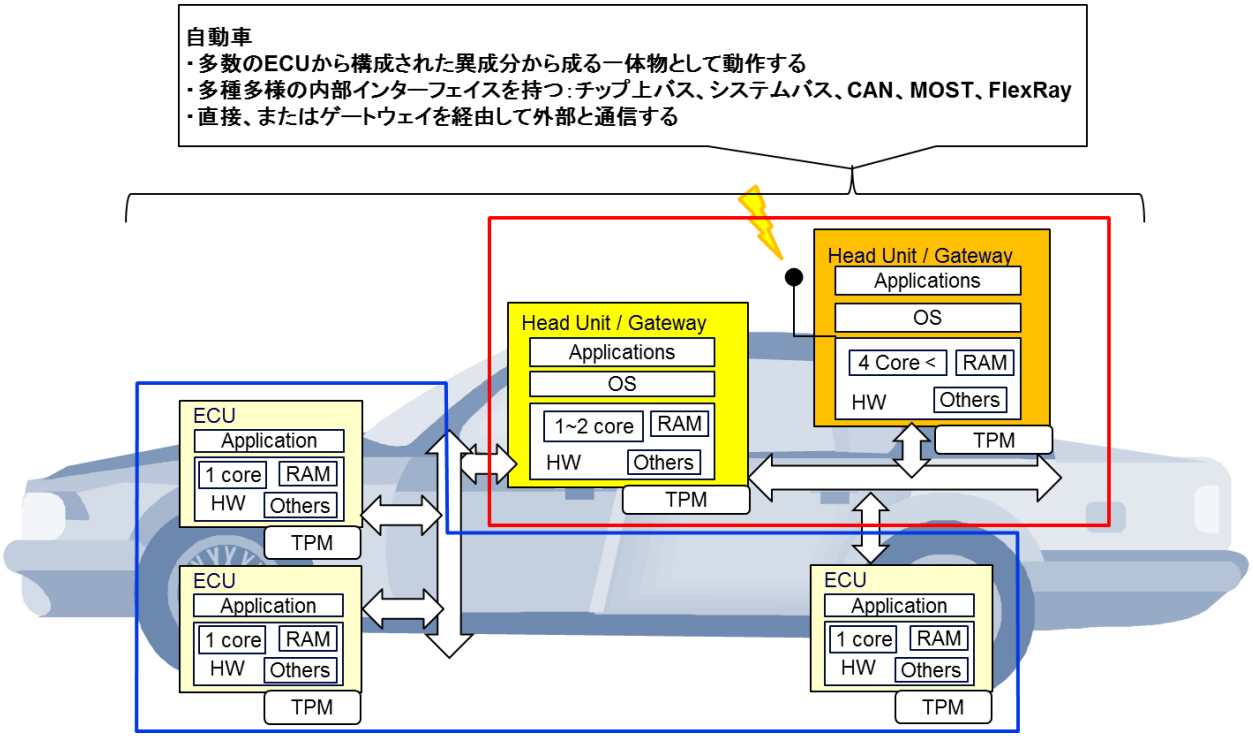
**Q. 具体的にはどの TCG 技術を ECUs に応用することができますか？**
A. TPM (Trusted Platform Module) と TNC (Trusted Network Connect) のプロトコルは、パソコン、タブレット、携帯電話にも幅広く導入されているように、ECUs にも応用することができます。TPM と TNC プロトコルは、以下のことを可能にします。

1. ECU で用いられているファームウェア/ソフトウェアの完全性検査を行い、報告する。
2. ECU で用いられる暗号鍵を生成、収納、管理する。
3. ECU の完全性の認証と保証を行う。
4. ECU に用いられるファームウェア/ソフトウェアのセキュアな更新を行う。
5. ECU 内情報の書き戻しを防ぎ、記憶装置を安全に管理する。

**Q. これまで TPM は、物理的なスペース、製品構成、消費電力が比較的大きいパソコン、タブレット、携帯電話などに組み込まれてきました。これらの 3 つ全ての設計要因にかなりの制約がある自動車電子市場においてどうしたら TPM が活用されるのでしょうか？**
A. TCG と TCG 会員は、自動車機器、自動車構成部品の市場は別の物と認識しています。従って、EmSys 部会は、新しいプロファイルを使った仕様を策定しました。この仕様は、ECU に有効な TPM 機能のサブセットで、不必要な機能がなく ECU に負担を与えず、自動車の安全性に不可欠で大変重要な機能を取り入れています。

**Q. この新しい TPM のプロファイルとはどういったものですか？**
A. 新しい仕様は、「TCG TPM 2.0 Automotive Thin Profile」と言い、自動車環境におけるユニークな動作条件（温度、振動、加速、他を含む）である、限定的な記憶容量、使用電力量制限、ファームウェアに制限を与えるかもしれないユニークなソフトウェア条件に対応します。

この仕様は、20 年を超える長い製品寿命を持つ可能性の高い自動車を、意識して策定されたものでもあります。




**Q. この新しい仕様の Automotive-Thin TPM は自動車の中でどのように機能しますか？**
A. 各 ECU は、それぞれ自身の TPM を持ちます。重要な機能は以下 4 つが含まれます。

1. 資源制約がある ECU を支援し、ECU の完全性を報告し、ECU 内構成情報の監査/書き込み/認証を行い、信頼性のあるリモート管理を行なう。

2. ECU ファームウェア監査情報収納、完全性ダイジェストと電子署名を作成する。

3. 電子署名検証を行った上でのファームウェア更新、リモートサービスセンターへの更新完了報告の確認をする。

4. 暗号鍵の生成、収納、削除、エクスポート、インポートなどの作業をセキュアに管理する。

**Q. 遠隔操作での車載電子機器のメンテナンス工程の安全性をどのように保証することができますか？**
A. 次のステップを用いてファームウェア/ソフトウェアの更新をセキュアにします。

1. その時点での自動車ソフトウェアとハードウェア内の構成、状態を遠隔で正確に把握する。（TPM に基づく測定、測定値の TPM 自身、および第三者による検証可能性保証、TNC プロトコルを用いての通信）

2. 意図されたソフトウェア更新が完了したことを検証し、証拠保存する。（TPM に基づく測定、測定値の TPM 自身、および第三者による検証可能性保証、TNC プロトコルを用いての通信）

3. 更新動作と TPM 測定動作の(TPM によって生成された)監査ログを長期間セキュアに収納する。TNC プロトコルを用いた転送、ネットワークアクセスが可能な自己暗号化記憶装置や他の高信頼性の収納等を行う。

**Q. Automotive-Thin TPM の他に自動車向けの TPM プロファイルはありますか？もし存在する場合は、どのアプリケーション/システムの種類に対応していますか？**
A. 将来 TCG は、また他のプロファイルを開発するかもしれません。次のプロファイルでは、自動車の中の複数の ECU 個々に搭載されている TPM の管理と調整に使われるヘッドユニットやゲートウェイシステムのセキュリティを強化し、リモートサービスセンターや第三者と自動車間の無線やインターネット通信のセキュリティを強化することも可能です。

**Q.自動車業界からどういった意見がありましたか？**
A. TCG 会員は、世界をリードするいくつかの自動車電子機器サプライヤーに加え世界をリードする自動車メーカーを含み、仕様開発に取り組んでいます。TCG は、SAE 自動車電子システムセキュリティ委員会と SAE 自動車電子ハードウェアセキュリティ調査特別委員会の会議にも参加しています。また米国運輸省道路交通安全局の「自動車に於ける電子制御システムの安全とセキュリティ」と題した意見募集に対し、意見を提出しました。さらに、自動車の遠隔ソフトウェア更新を検討している国際組織 ITU-T の SG-17 委員会とも連携して活動しています。

**Q.この新しい TPM プロファイルについてどこで詳細を知ることができますか？**
A. TCG は、4 月 22 日に米国デトロイトで開催される SAE 2015 World Congress & Exhibition (世界最大級の自動車関連団体主催の総会/展示会)で、講演とデモンストレーションを実施します。詳細については、以下 URL をご覧ください。
http://www.trustedcomputinggroup.org/media_room/events/189

**Q. SAE 2015 World Congress & Exhibition でのデモンストレーションについて詳しく教えてください。**
A. TCG 会員である富士通株式会社と株式会社トヨタ IT 開発センターが、TPM (Trusted Platform Module)をハードウェア信頼基点として使い、自動車の中の ECU で用いられているファームウェアのセキュアなリモート更新のデモンストレーションをします。

Rev. March 19, 2015

デモンストレーションは、以下 3 点に基づいて実施されます。

1. その時点での自動車ソフトウェアとハードウェア内の構成、状態を遠隔で正確に把握する。（TPM に基づく測定、測定値の TPM 自身、および第三者による検証可能性保証、TNC プロトコルを用いての通信）

2. 意図されたソフトウェア更新が完了したことを検証し、証拠保存する。（TPM に基づく測定、測定値の TPM 自身、および第三者による検証可能性保証、TNC プロトコルを用いての通信）

3. 更新動作と TPM 測定動作の(TPM によって生成された)監査ログを長期間セキュアに収納する。TNC プロトコルを用いた転送、ネットワークアクセスが可能な自己暗号化記憶装置や他の高信頼性の収納等を行う。

【お問い合わせ先】
Trusted Computing Group　広報担当　PR Works Inc.
アン・プライス（Anne Price）
電話：1-602-840-6495(US)
E メール：anne@prworksonline.com
Twitter: @TrustedComputin
https://www.trustedcomputinggroup.org