

第3部 広がるサイバー空間に対応するPKIの新しい応用領域

PKIの新しい活躍の場＝繋がる車。

そこで生まれる恩恵と脅威、それらへの方策

-PC/サーバでの10年のセキュリティ経験を踏まえた提案、
標準化活動-

2015年4月10日

株式会社富士通研究所

R&D戦略本部 IPR戦略室

TCG常任理事、組込系WG共同議長

小谷誠剛



自己紹介



- 1956年、九州は熊本、その天草の島でおぎゃ〜と...
- 1980年、東北大理学部物理学学科卒
- 1982年、筑波大学理工系大学院修士課程物質工学科修了
- 同年、富士通入社、研究所配属、超伝導コンピュータ研究
- 1991年、名古屋大学論文博士(工学、超伝導コンピュータ研究)
- 1994年、超高速計算機の応用としてセキュリティ研究開始
- 1999年、トラステッドコンピューティング(TC)研究開始
- 2002年、TC応用ビジネス開拓および標準化活動開始
- 2006年、TCG非常任理事当選*、富士通米国研究所へ移籍、渡米
*富士通、TCG理事会メンバーに選出 <http://pr.fujitsu.com/jp/news/2006/12/5-2.html>
- 2008年、TCG常任理事へ昇格
- 2011年、帰国、TCG組込系WG設立/共同議長就任、自動車を含むセキュリティ標準化/ビジネス開拓に従事、現在に至る

- NPO団体TCG(Trusted Computing Group)が策定し、ISO化したセキュリティチップ(TPM, Trusted Platform Module)は、当然ながらPKIに基づく仕様であり、2004年から多くのPC/サーバ、近年はスマホ等に広く搭載され、セキュリティ強化に役立っている。
- このTPMを自動車に適用する検討をTCGが2011年から進めている。即ち、PKIが自動車で活躍する！
- 自動車でのリコールは近年、数百万台/件に及び大きな課題である。種々の原因の内、現時点で約3割がソフトウェアに拠るものと言われ、この割合は将来増大する事が確実視される。これを回収する事なく、リモートで改修する事が可能になれば、メーカーのみならずユーザも恩恵を手にする。
- 現状では実施困難な自動車ソフトの遠隔保守/アップデートを、TCG/PKI技術で実現する活動について状況、将来見通しをTCG理事である講師が紹介する。

- 自動車と車外と繋がる事で生まれる恩恵、優位性
 - 情報配信、自動運転、リモートリプロ、ドラレコ、スマホ連携...
 - 経済効果
- そして生まれる脅威、それらへの方策
 - 車両状況把握
 - 証拠保全
- 脅威への対抗策、将来性
- まとめ

- 情報配信、自動運転、リモートリプロ、ドラレコ、スマホ連携...
- 経済効果

■ 現状

- リコール発生時、行政指導により全車回収、部品交換/対処後返却。
- ハードウェア/部品の不具合に拠る事象が大部分であるが、今後はソフトウェアのバグ/セキュリティホール具現化に拠って起きる割合の増大が必然。
 - ✓ 2013年度のリコールとサービスキャンペーンの総数の内、現時点で28%程度が車内ソフトウェアのトラブルに起因するものであることがわかっている。

日経Automotive Technology: PHEV不具合に学ぶ

<http://techon.nikkeibp.co.jp/article/HONSHI/20130920/304646/>

- だとしても、現状では些細なソフトウェアアップデートでも、対象全車両回収必須。

■ 恩恵

- ソフトウェアアップデートのみで対処可能なリコールは回収不要、リモートリプロで出来、運転者/自動車メーカー双方に有益。ディーラーも作業量平準化、上得意客向け集中営業で、手間賃減少を補って余りある効果。

■ 経済効果

- 運転者の自車搬送/回収手間、ディーラー工賃、自動車メーカーの告知/管理費用等、リコール一件当たり数十億円の経費のかなりの部分を削減可能。

■ 現状

- 米運輸省(DoT)・米運輸省高速道路交通安全局(NHTSA)・米航空宇宙局の最終報告(2011/2/8)で、対象となった自動車に器械的な不具合はあったものの、電子制御装置に欠陥はなく、急発進事故のほとんどが運転手のミスとして発表された。
<http://www.nhtsa.gov/PR/DOT-16-11>
- イベントデータレコーダー、ドライブレコーダー等市販機器が、業務用車両に搭載されるようになって来ている。しかし、乗用車ではほとんど搭載されていない。
- 「ドライブレコーダーは事故の検証に役立つことも目的の一つとした製品ですが、裁判における証拠としての効力を保証するものではありません。」
<http://www.jafmate.co.jp/dr/support/f-a-q.html#q2>

■ 恩恵

- 航空機のフライトレコーダー同様に事故原因分析が出来、運転者/自動車メーカー双方に有益。不毛な訴訟、調査費用、弁護士費用等の低減可能。

■ 経済効果

- フライトレコーダーと同等装置の自動車内設置は价格的/構造的に不適合。車両が車外と通信する事に拠って安価に達成出来れば、負の経済効果を減殺。

- 米運輸省(DoT)は2011年8月、電子制御システムを持った自動車に於けるサイバーセキュリティと安全性について意見を公募。

Cyber security and Safety of Motor Vehicles Equipped with Electronic Control Systems

https://www.fbo.gov/?s=opportunity&mode=form&tab=core&id=40c0c2730b334df090dba322a61e956f&_cview=0

- TCG、その他各種機関/団体が意見書提出

前頁の報告の半年後！

Secure update mechanisms including the three processes;

- Check current situation remotely,
- Confirm installation completion,
- and Store certifiable log for indemnity.

**三つのプロセスを含む、セキュアな更新機構
これらが担保されないから、リモメン実施不可！**

- ・ その時点での車両状態を正確にリモートで把握
- ・ インストール作業の完了確認
- ・ 保障/免責のために、検証可能なログを保存

- 米国運輸省道路交通安全局(NHTSA)が2014年12月、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について意見公募。

Automotive Electronic Control Systems Safety and Security

<http://www.regulations.gov/#!documentDetail;D=NHTSA-2014-0108-0001>

- TCGを含め、44機関が意見書提出、公開中

- ✓ 本提案は、先日(2015/3/16)発行した自動車用TPM仕様に基づくものである！

ご参考: 各種機関の意見募集へのTCG対応実績

募集元	内容	TCGから意見提出
DoT (米国運輸省) (2011/8)	Cyber security and Safety of Motor Vehicles Equipped with Electronic Control Systems 「サイバー化 (繋がる: コンピュータネットワーク化) された車に於ける安全安心の実現方法/方式を問う」	組込系WGを中心に意見書作成/提出、その後、DoTと意見交換実施
OMG (オブジェクト指向技術標準化団体) (2012/5)	Assuring Dependability of Consumer Devices: Automobiles, Service Robots, Smart Houses, Avionics, etc. 「自動車、自動機器、スマートハウス、航空機等の民生機器に於ける信頼性確保の実現方法/方式を問う」	組込系WGを中心に意見書作成/提出
DoE (米エネルギー省) (2012/7)	Cyber security for the electric delivery system 「サイバー化された電力供給システムに於ける信頼性確保の実現方法/方式を問う」	組込系WGを中心に意見書作成/提出
NIST (米標準技術研) (2013/4)	Cybersecurity Framework for Critical Infrastructure 「サイバー化された重要な経済/社会基盤に於ける安全安心確保の枠組み/方式を問う」	TNC WGを中心に意見書作成/提出
FTC (米連邦取引委員会) (2013/5)	Seeks Input on Privacy and Security Implications of the Internet of Things, Cars, appliances, and medical devices,... 「車を含むあらゆる機器が繋がる世界に於けるプライバシー/セキュリティの在り方を問う」	組込系WGを中心に意見書作成/提出
NHTSA (米国運輸省道路交通安全局) (2014/12)	Automotive Electronic Control Systems Safety and Security 「自動車電子制御システムの安全性とセキュリティ」	組込系WGを中心に意見書作成/提出

- 車両状況(リモメン前後)把握
- 証拠保全

下の三つのプロセスを含む、
セキュアな(更新)機構

- ・ その時点での車両状態を正確にリモートで把握
- ・ インストール作業の完了確認
- ・ 保障/免責のために、検証可能な証拠/ログを保存

安価に、かつ確実に実現
する事は非常に困難
これらが担保されないから、
リモメン実施不可！

パソコン/サーバの業態で
約10年の実績がある技術、
国際標準化/公開済み仕様を
導入する事で実現！

TCG & PKI

Trusted Computingの提案

2011年 100億台
2020年 500億台*

FUJITSU

- ネットワークによって全てがつながる(製品寿命が異なる機器含む)
- リモートでソフトウェアによる機能拡張・修正が一般化
- 相互信頼確認が必須

これから

Who What How

従来



信頼

対面で五感を駆使した
値踏み、目視、握手、会話



全てがつながる

人・機器・環境情報を相互に
交換し、確認し合うことによって
適切な信頼関係を築く
⇒新しい機能・サービスの提供



信頼度判断・判定仕組みで、
「守る」のではなく、「救う」
個人情報扱いへの配慮しつつ

各種リモートメンテナンスの必須要件

重要三項目のクリアが課題

- その時点での相手状況の正確な把握
- 処理完遂(あるいは未完)の確認
- 将来に渡る証拠(ログ)保存(免責)

*「富士通グループ社会・環境報告書2012」2012年8月
<http://jp.fujitsu.com/about/csr/reports/>

Trusted Computing Group (TCG)とは

- 信頼できるプラットフォーム/インフラ構築のため、ハード/ソフトウェアの業界標準、統合的仕様開発、普及を目的とする2003年発足のNPO <http://www.trustedcomputinggroup.org/>, <http://www.trustedcomputinggroup.org/jp> (日本支部)

- HP, IBM, Intel, MSが設立した団体(TCPA, 1999年)を改組
- 理事11社(上記およびAMD, Cisco, Fujitsu, Juniper, Infineon, Lenovo, Wave)

- 世界96社加盟(1/15現在)

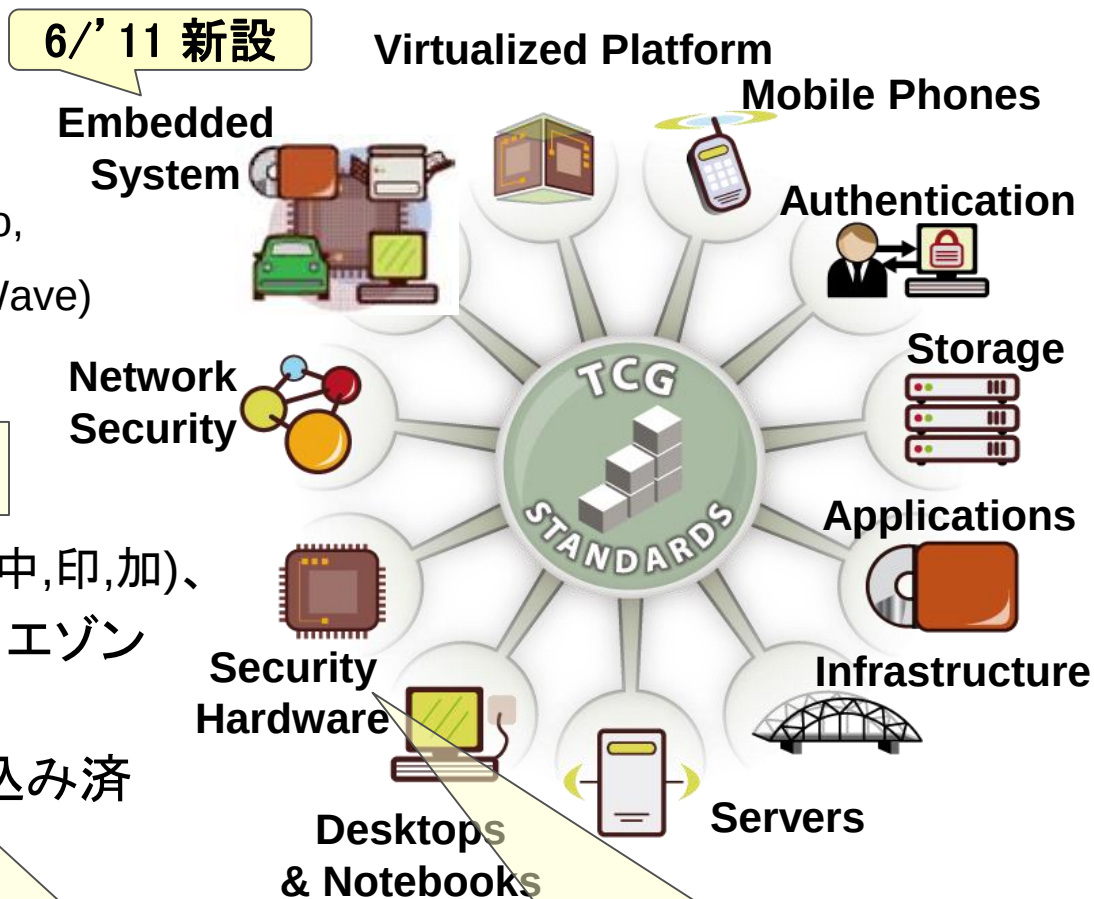
ARM(2/12)、トヨタ(3/12)、Cisco(5/12)、Google(9/13)、Canon(10/13)加盟

- 多数国家機関(日,米,英,独,仏,中,印,加)、大学/研究機関/業界団体がリエゾンとして参画
- 米国/EUの政府調達要件盛り込み済(1/06~)、日本は検討中

IPA(経産省)、NICT(総務省)

ETSI, Global Platform, etc

TPM(Trusted Platform Module)



■ 日本からの参加

- IPA, NICT (リエゾン), Fujitsu (理事), Canon, Hitachi, Insight, Panasonic, Ricoh, Toshiba, Toyota (一般), Hagiwara (賛助) が加盟

■ パソコン/サーバで約10年の実績

- 2004年から各社ノート/デスクトップPC、サーバにTCGが仕様策定したセキュリティチップ(TPM)を搭載、出荷中。2009年からはコピー/複合機へも搭載。TPM出荷総数は数億個と推定。

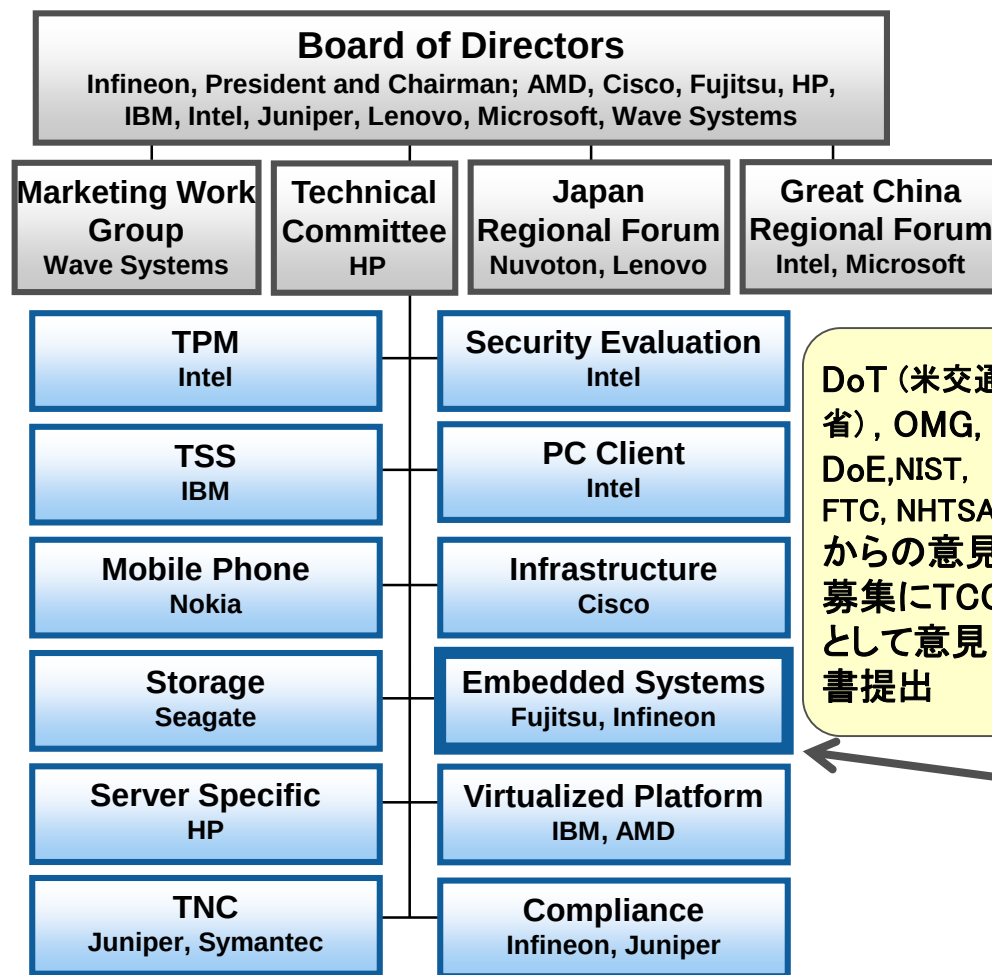
■ 自動車を含む組込み機器向け取り組みを2011年開始

- 2014年3月、TPMを自動車向けに最適化した仕様(TPM-Thin)の公開レビュー開始、会員内外からのコメントに基づく修正を経て
- **2015年3月16日完結、発行！(後述)**

TCG TPM 2.0 Library Profile for Automotive-Thin

http://www.trustedcomputinggroup.org/resources/tcg_tpm_20_library_profile_for_automotivethin

TCG内での組込み分野/ITSに対する取り組み



DoT (米交通省), OMG, DoE, NIST, FTC, NHTSA からの意見募集にTCGとして意見書提出

検討WG設立、参加のメリット

- ・ 自社の戦略に沿った仕様
⇒ 各国政府調達要件への盛り込み
- ・ タイムリーな製品/サービス投入
⇒ 仕様検討と開発を並行して進め、公開と同時に製品発表(我田引水)

例えば、自動車のセンシング情報保存/保証、リモートメンテナンス分野への展開

Standardization for

- Automotive
- Hardcopy Devices (Printer/Scanner/MFP)
- Mobile communication devices
- Industrial control and machinery
- Financial transaction terminals
- Household applications (TV/Settop box)
- Medical equipment
- Smart Grid/Smart meter
- Sensor network/Monitor cameras
-

Embedded Systems

9/'10構想開始、4/'11理事会承認
6/'11会員会議で公開、BMWが基調講演

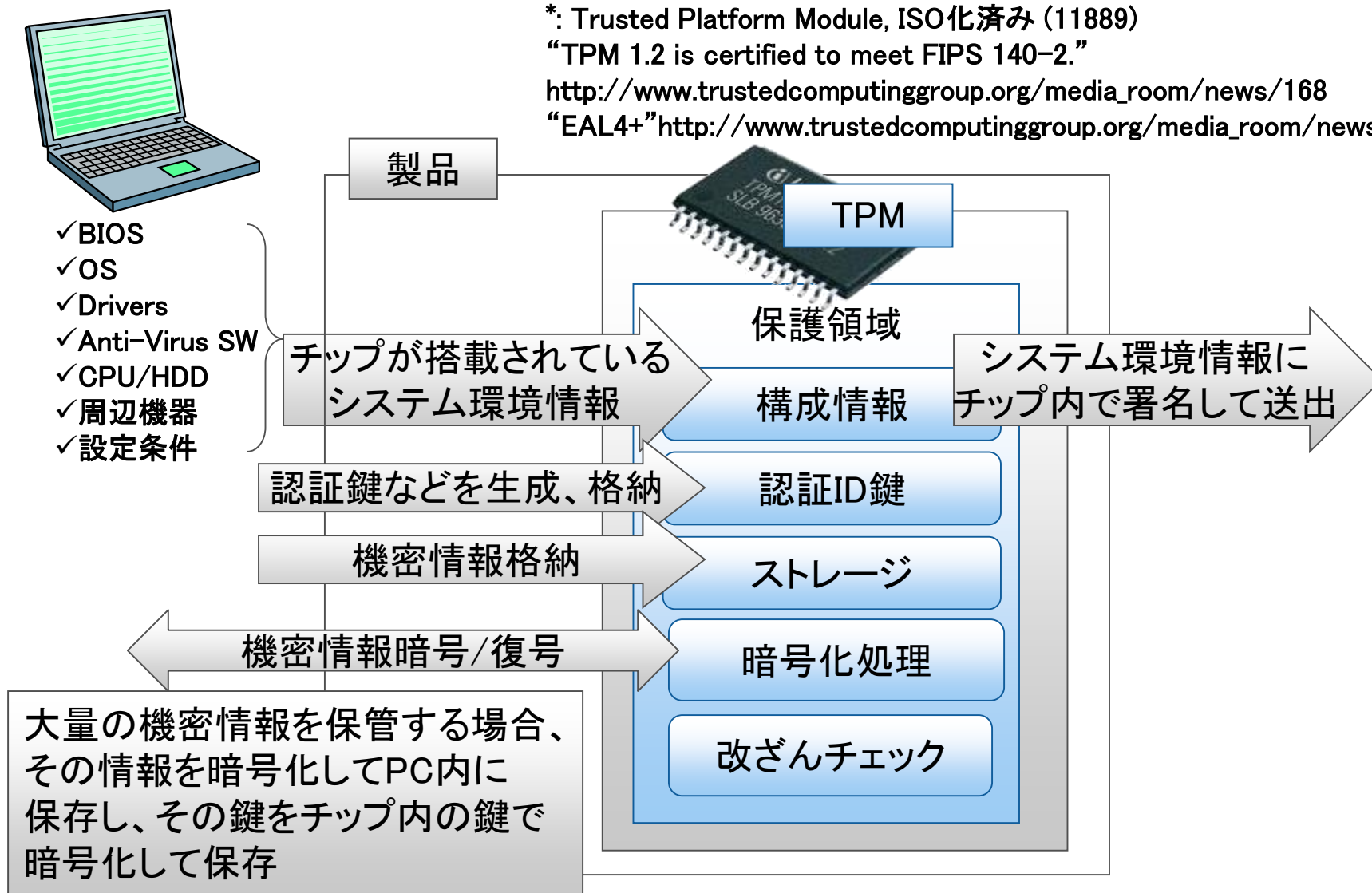
(ご参考)TPM*のしくみ: HW信頼基点

*: Trusted Platform Module, ISO化済み (11889)

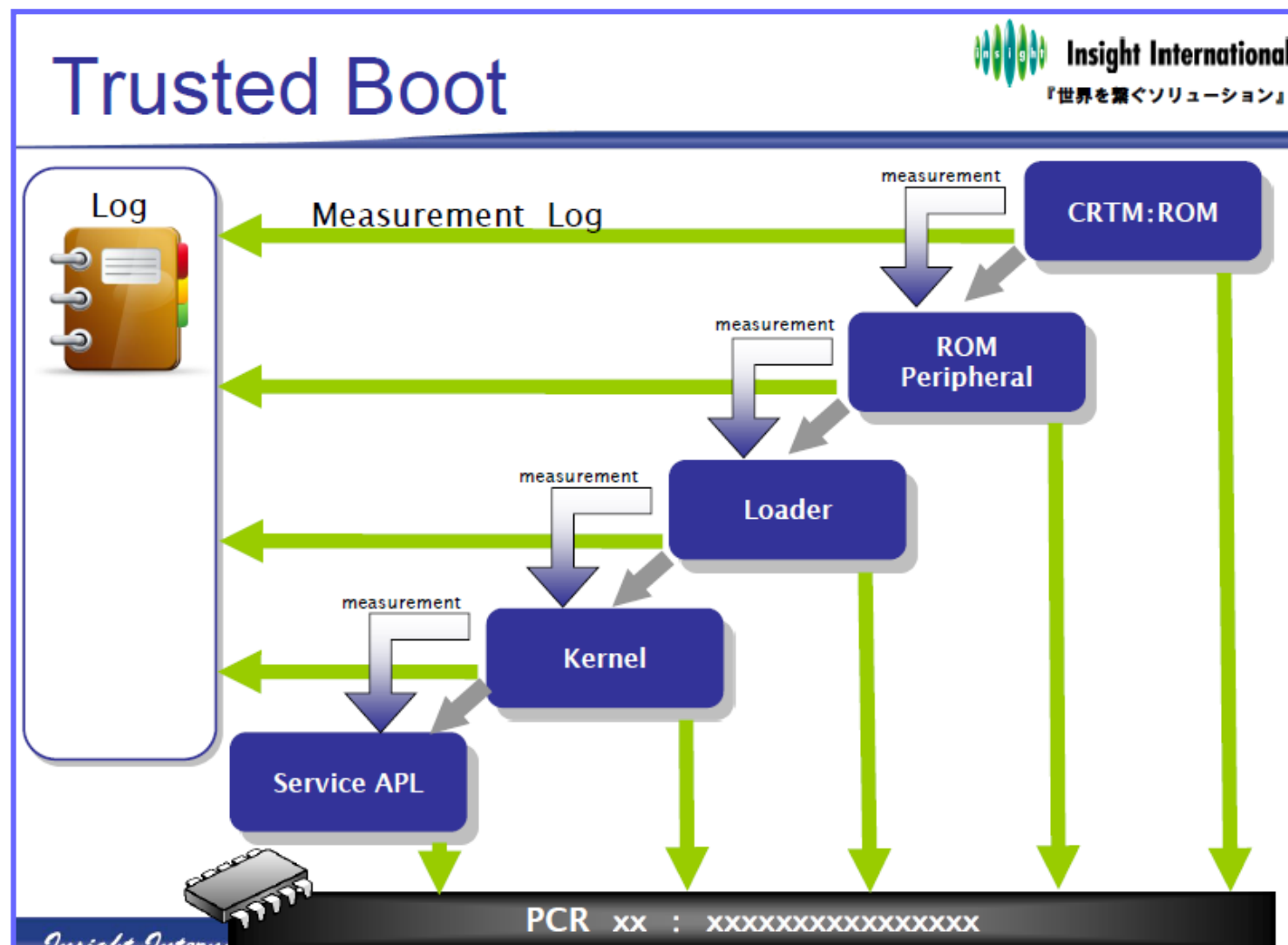
“TPM 1.2 is certified to meet FIPS 140-2.”

http://www.trustedcomputinggroup.org/media_room/news/168

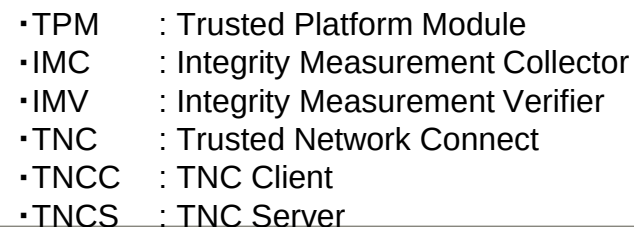
“EAL4+” http://www.trustedcomputinggroup.org/media_room/news/95



(ご参考) TPM活用例:



TCG日本支部主催、第1回公開ワークショップ講演「TPM技術の概要とソリューション」から引用
<http://www.trustedcomputinggroup.org/jp/jrfworkshop/pastworkshop1>



Copyright 2015 FUJITSU LIMITED. Slide #16

(ご参考)TCGと他方式との比較

項目	TCG	特定会社方式/一般暗号通信方式
信頼性	◎ ・信頼基点として、ハードウェア(TPM)を利用し、ソフトと組み合わせる ・規格が公開され、専門家による継続的、自発的な検証を受けることができ、バグや抜け道の存在確率が低い ・作成されたレポートの正確性が高く、これを用いて判定した信頼度が高い	○ ・独自(秘密)方式のソフトを端末にインストール ・秘密であるので中程度の信頼性はある ・但し、内部犯罪やバグに対する対応は不完全
検証性/ オープン性	◎ ・規格が公開されているため、運用・監査ログ等の記録(機密情報自体では無い)について、第三者による自律的な検証作業が将来に渡って可能	× ・秘密方式であるため、ログの解析にはその会社から供給、あるいは指定Black boxを使わざるを得ず、よって真の意味での第三者検証は不可能
コスト	○(△) ・TPMチップ(1ドル程度)、実装コスト、チップ回りソフト類費用が発生、但しPC実装が大量になるに従い低下 ・現状、ライセンス費用はなし	○ ・端末側費用はソフトインストールのみのため安価 ・但し、内部犯罪やバグに対する保険費用等が高コスト

「俺を信じろ！」の世界観の終焉。第三者による検証性確保が必要条件。
自らの免責性を確保する上でも必須要件。

■ 自動車の情報セキュリティへの取組みガイド: -「繋がる」自動車に情報セキュリティを - (IPA自動車研究会, 2013/4)

[報告書2ページ下段抜粋] 米国の研究者等により、自動車内外からの通信によって自動車内のソフトウェアのぜい弱性を攻撃することで、自動車の制御等に影響を与えることが可能であることが明らかとなっている[1]。

- [1]. "Comprehensive Experimental Analyses of Automotive Attack Surfaces", CAESS, Stefan Savage, Tadayoshi Kohno, 2011/6/3, <http://www.autosec.org/publications.html>

[補足] 同じ研究者らによる1年前の論文は大きな衝撃を与えた。一方でアタッカーが車載ネットワークに物理的に接続する事を前提としており、非現実的であると多くの批判を浴びた。それに対し現実的な方法でアタックを試みた論文。

ここでは、OBD-IIからのCANへの侵入、Bluetooth/リモートキーエントリー、携帯電話などからの攻撃を記載。現在のPCで起こっていることが、外の世界と繋がる自動車に於いて起こり得る事を実証した。提案として、バスを完全に切り離れた利用制限、セキュアなソフトウェアアップデート、コンピュータのセキュリティ関係者と連携した取り組みの必要性、等に言及。

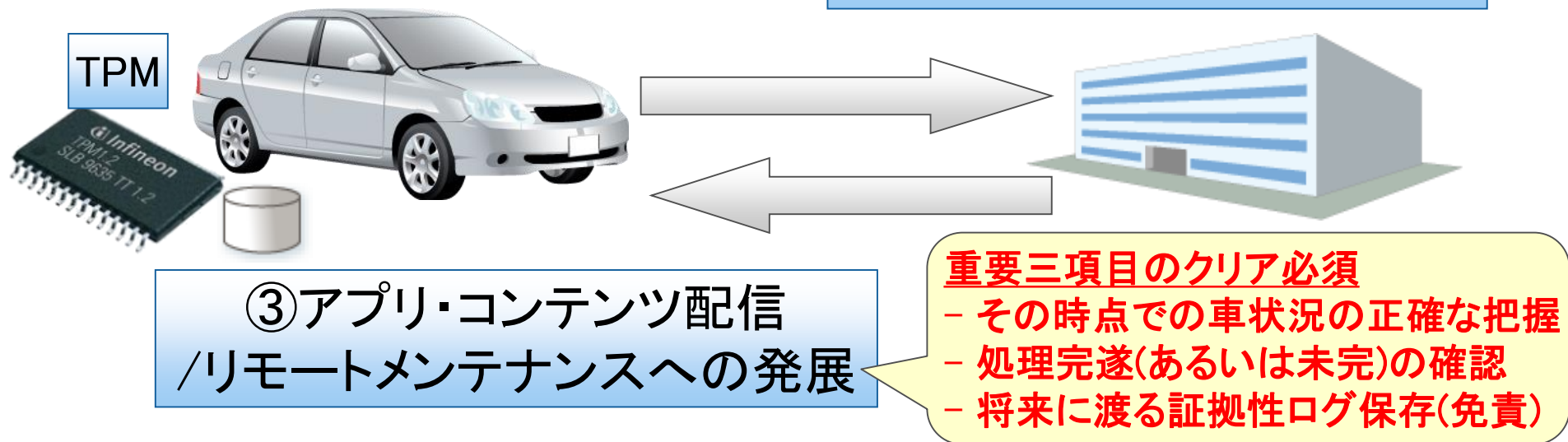
IPA自動車研究会では、調査活動の一環として、著者であるKohno教授にインタビューを行っている。概要は2011年度報告書に記載。

TCG応用による解決策提案

- TCGが仕様策定したセキュリティチップ(TPM)を自動車に搭載し、それを信頼基点としてセンターと通信することで、以下を安心安全、合理的コストで実現

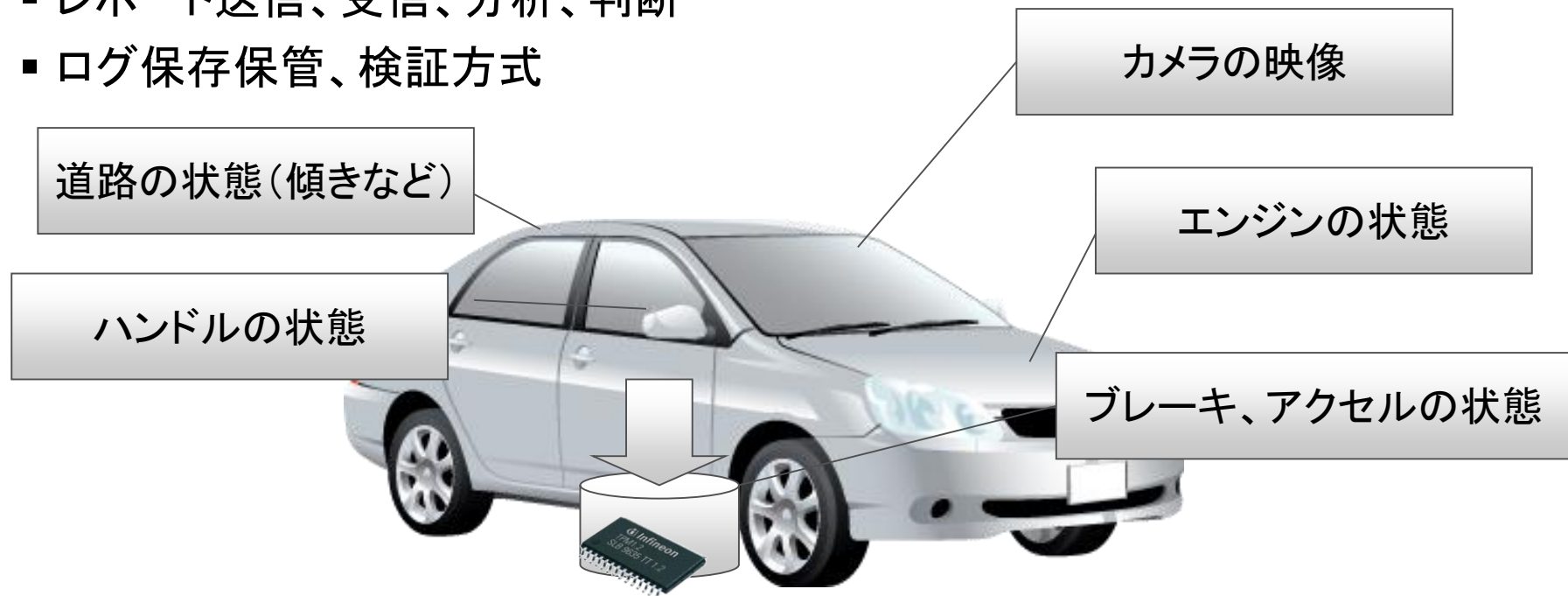
①センシング情報真正性検証

②ネットワークを介したセンシング情報の収集/保管



■ TCGではログ記録仕様などが規定/公開されており、それによりセンシングデータが改竄されていないことを第三者が検証できる。

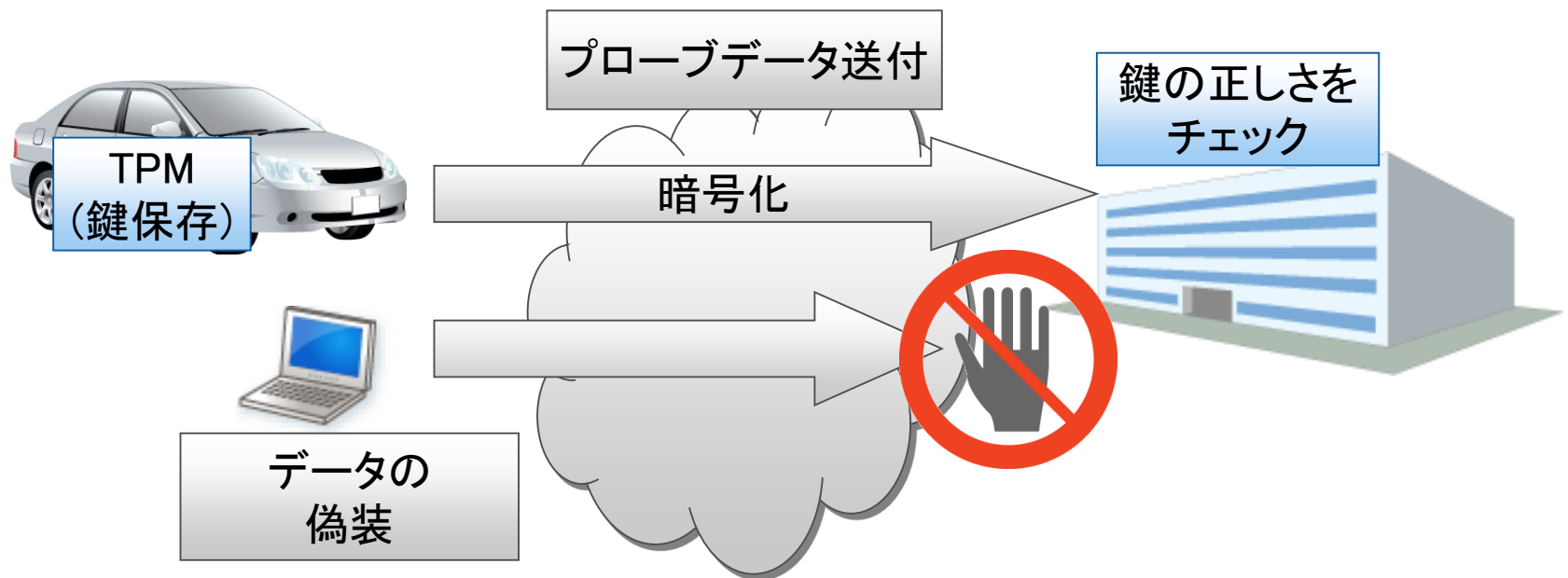
- TPMに基づく、センシングデータを含む車内情報の収集、レポート作成
- レポート送信、受信、分析、判断
- ログ保存保管、検証方式



センシングデータを安全に保存でき、改竄されていないことを証明

■ TCGによる安全な情報収集/ネットワークの提供

- 確実なエラー訂正機能を有する
- 通信経路中、なりすまし配受信、盗聴、改竄を抑制、検知する策を施してある
- たとえ盗聴等が行われたとしても、内容の解析を事実上不可能とする



クルマからのデータだけを確実に集めることができる

適用③アプリ・コンテンツ配信/リモートメンテ

■ センターから安全にクルマに配信

- アプリ・地図データ更新
- リモートメンテナンス

重要三項目のクリア必須

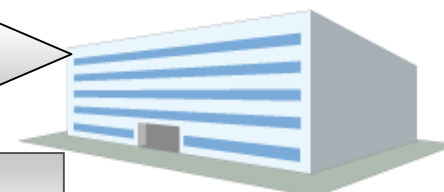
- その時点での車状況の正確な把握
- 処理完遂(あるいは未完)の確認
- 将来に渡る証拠性(第三者検証性)ログ保存(免責)



センター信頼性
確認

① 相互認証

② 自動車への報告書要求



TPMベースで自動車構成情報
収集/報告書作成、署名付与

③ 当該時点構成情報送信

ホワイトリストに基づき
自動車信頼性確認
報告書分析

ソフトインストール

④ 適合ソフト(パッチ)送信

リコール情報等により
最適なソフト選択

完了後、再度情報
収集/報告書作成、署名付与

⑤ 完了後構成情報送信

完了確認、一連ログ
その他を証拠保管

■ TCGへの自動車関係会社の参加状況

- 現時点でトヨタ、Google(自動車)、パナソニック、富士通テン(部品)、Infineon、Freescale、Qualcomm等(チップ)が加盟
- 多数が関心を表明(自動車(独B、日H、米G)、部品(独B、日D)、チップ(日R))

■ TCGでのITS関係の作業スケジュール、目標

- 自動車用セキュリティチップ(TPM-Thin)仕様確定、発行: 2015年3月16日。
他仕様、PP、ユースケース等: 2015年内 ← **2019年自動運転実用化に必須**
- リコール時リモートメンテでの運用指針案(法案)提示/提案: 2015年内

■ ISOやITU-Tなどへの仕様提案計画/実績

- TPMv1.2: ISO提案、認定済(2009年、ISO11889)
- TPMv2.0: 同じ番号でのISO認定を目指し、2015年内確定目標
- 自動車向けTPMv2.0 for Automotive-Thinについては、TPMv2.0の番号をそのまま引き継ぐか、新規に認定を受けるか検討中
- 通信規格TNC: IETFに提案し、RFC認定済(2010年、RFC 5792/5793)
- その他、ITU-T(SG-16/17), oneM2M等への提案を検討、一部提案中

■ 経産省/総務省を中心に様々な動きが活発化(小谷が把握する範囲に於いて)

No	所管元/部会	内容/主メンバー	当社の関与
1	IPA(経産省): 自動車情報セキュリティ研究会	2008年から自動車セキュリティ動向調査/研究を行い、年度単位で報告書作成/公開。2011年11月にドイツで開催の自動車セキュリティ国際会議(escar)に参加、Kohno教授にインタビュー。2014年度は休止。名大/三菱/トヨタITC/ルネサス/日産/MS。2015年度復活可能性有。	2011/9から委員として参加、報告書にTCG関連記載
2	IPA: 消費者機械安全標準化WG	消費者が使う機械の機能安全をOMG (国際標準化団体、オブジェクト指向技術標準化を目指す) に提案、OMGからRFI発行。高い機能安全を求められる物の一つとして自動車を対象。トヨタ/産総研。	2010から参加、提案書策定に関与
3	TTC(総務省): スマートカーWP(Working Party)	欧州中心で個人利用携帯型端末までを含む広義なITSの標準化が進展。これら動向を踏まえ、広義で高度な自動車交通関連通信の標準化課題を検討する場として設置。沖、KDDI、NTT、クアルコム、NEC、トヨタITC、ルネサス、JARI。仕様策定のWGを新設、活動拡大。	2011/8から参加、提案書策定に関与、セキュリティサブ部会の議長拝命
4	TTC: oneM2M専門委員会	oneM2Mの発足に伴い、その標準化活動に参加する体制として発足。M2Mサービスの、交通(自動車)、環境・エネルギー、防災、医療、農業、建築等、様々な分野におけるさらなる展開を視野。KDDI、NTT、NEC。	2012/3から参加、一つのユースケースとして入れ込む事に成功

技術的に出来る事を示すだけでは不足、これを、ガイドライン/法的に是認、裏付けして頂く事が、実ビジネス展開には必須
→ 国際標準/公開仕様に則った技術 = TCG/PKIを基礎とする事で、短手番、低コストで、法制化達成を目指す(欧米に伍して行く)。

Vehicle

- Works as a heterogeneous cluster with ECUs
- Internal communication: on-chip bus, system bus, Controller Area Network (CAN), Media Oriented Systems Transport (MOST), FlexRay.
- External communication directly or via Gateway

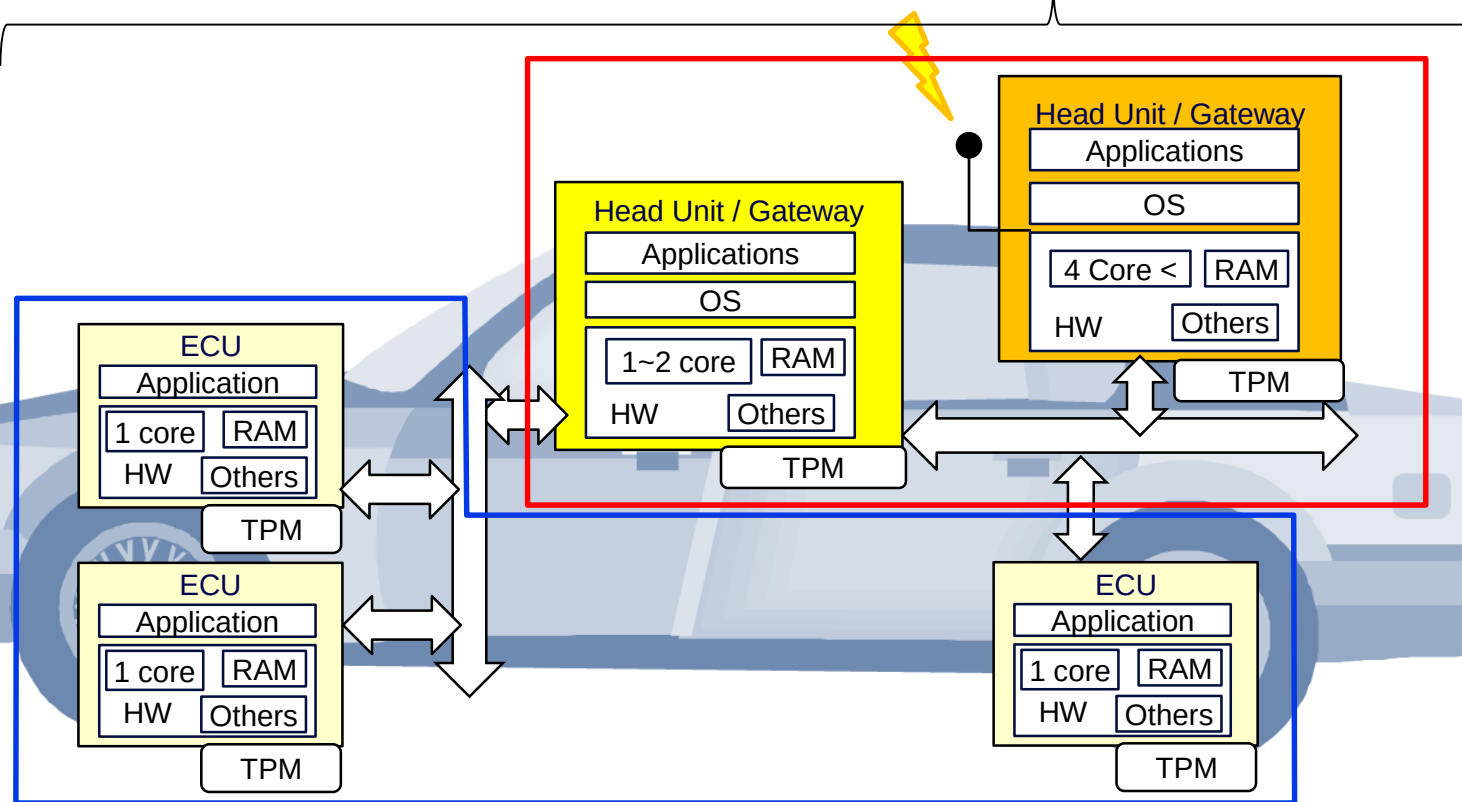


Figure 1: Overview of an automotive vehicle

補足: 最近の自動車は多数のECU(マイコン)を実装している。その総数は100個/台を超える

ご参考:自動車向けTPM仕様書内説明図

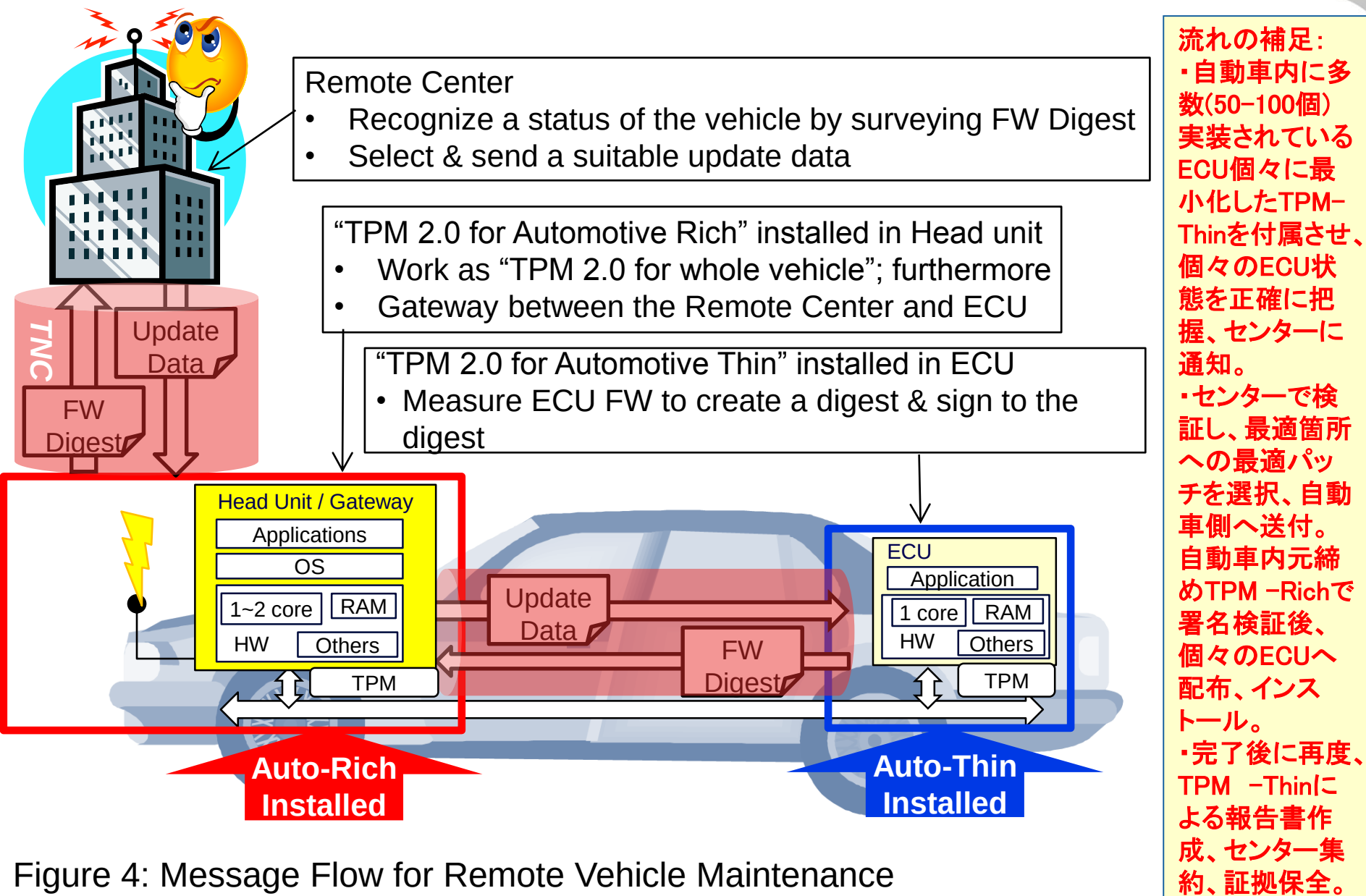


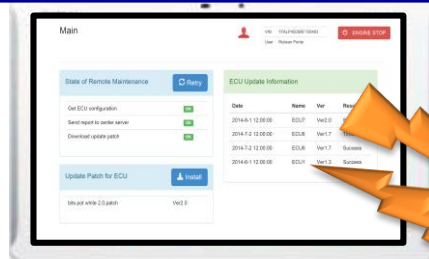
Figure 4: Message Flow for Remote Vehicle Maintenance

ご参考：自動車向けTPM仕様を実装するデモ

Connecting Center, In-vehicle Server and ECUs, files downloaded from Center enable "ECUs update" with TCG's TPM authentication capabilities.

Vehicle

In-Vehicle HMI on Tablet PC



Wi-Fi

TCG published TPM 2.0
Automotive Thin Profile v1.0

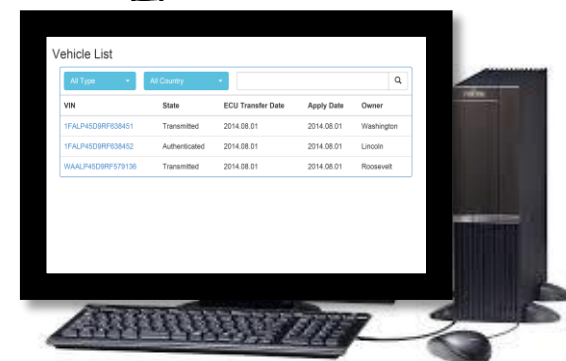
3G LTE
or other

Cloud

In-Vehicle
Server



Remote Maintenance
Center



CAN or other

Motor



ECU1: Actuator



ECU2: LED



自動車を模したプラモデル、リモートセンターを模したノートPC、その間を繋ぐ機器で構成
2015/4/20 RSA展示会(サンフランシスコ)、4/22 SAE年次総会(デトロイト)でデモ紹介予定

TCG応用による解決策提案(続)

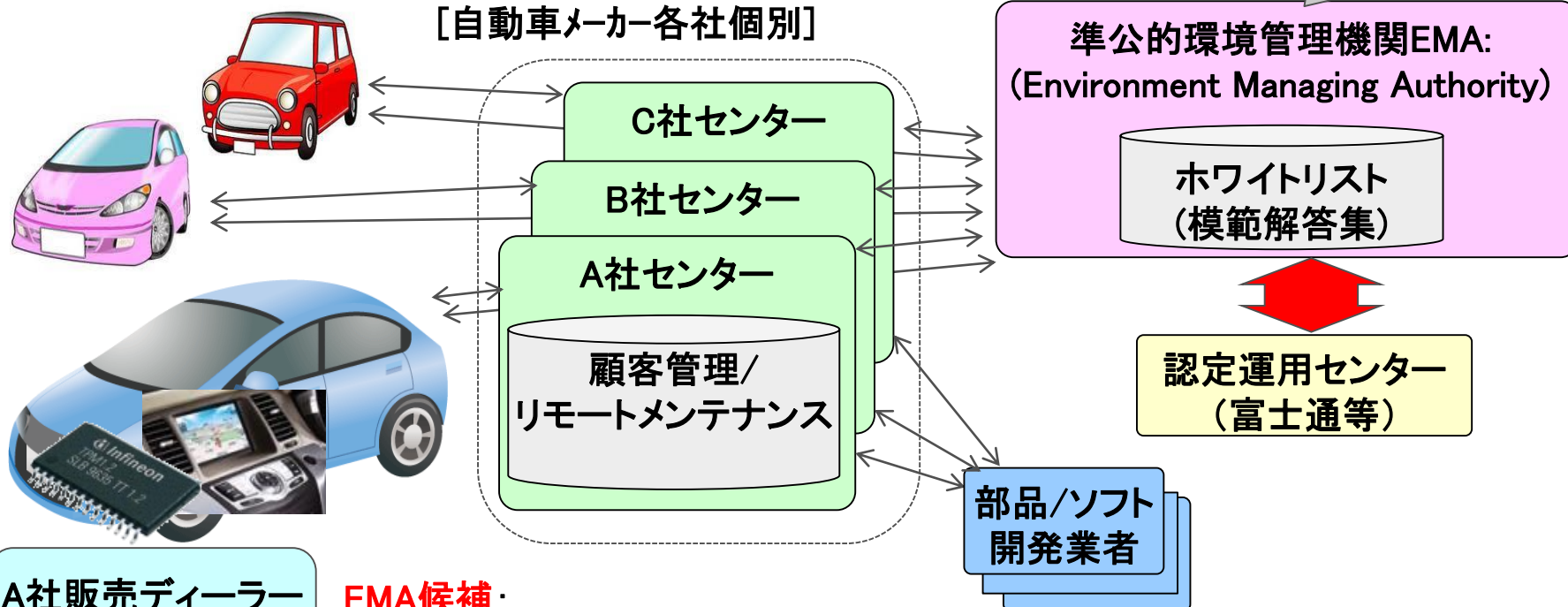
将来形態 センター側を分割、ジョブ分担させ、トータルコスト圧縮／順法性を確保

- ・汎用的/業界共通部分 : 準公的機関
- ・各社固有/顧客情報に関わる部分 : 各社個別
(種々情報を分散して保持するため、攻撃を受けた場合の被害拡大抑止のメリットも在り)

準公的機関が必要と想定される理由:

- ・リコール時などの行政指導対応
- ・業界統一適用等管理運用面で最適

[自動車メーカー各社個別]



A社販売ディーラー
/車載システム

EMA候補:

IPA (経産省管轄)、TTC (総務省管轄)、
自動車工業会(JAMA)、自動車技術会(JSAE)、JASPAR(標準化団体)、他

最後の付言:20年前の状況から進歩したか？



1993年7月5日に米国の雑誌に掲載された漫画。
「インターネット上では、あなたが犬だとは誰も知らない」

The above cartoon by Peter Steiner has been reproduced from page 61 of July 5, 1993 issue of The New Yorker, (Vol.69 (LXIX) no. 20) only for academic discussion, evaluation, research and complies with the copyright law of the United States as defined and stipulated under Title 17 U. S. Code.

まとめ：今、そこに有る脅威：誰もが加害者に！

被害者→容疑者*→加害者

IMC
Collector A

IMC
Collector B

TNCC

TPM

IMV
Verifier A

IMV
Verifier B

TNCS

無辜なのに加害者=DDoS**の踏み台

- ・「踏み台」にさせられる仕掛けを取り外す際、チップが信頼基点として機能する
- ・機器の環境を確実に把握できているからこそ、この作業がリモートで可能となる
- ・DDoS攻撃防止は不可能、しかしこの作業を多くの機器に事前に施す事ができれば、DDoS実行時点で大部分の機器が解放済みで、攻撃実効性を低減できる

* 日経記事「ネットなりすまし事件の怖さ、誰もが「容疑者」に」2012/11/17 <http://www.nikkei.com/article/DGXZZO48415000U2A111C1000000/?dg=1>

** Distributed Denial of Services: 悪意者が多数の機器を乗っ取り、集中攻撃を仕掛けさせ、目標をダウンする
日経記事「プリンターを踏み台として使用したDOS攻撃」2013/11/22 http://www.nikkei.com/article/DGXNASFK1302W_T11C13A1000000/?dg=1

ユナイテッド93便の乗客の志 "Let's Roll!"

アメリカン11便、ユナイテッド175便、アメリカン77便の全ての乗客の魂を受け継いで...

悪事の犠牲になることは悲惨である。

しかし、悪事の手先になること、これはもっと悲惨である。(小谷、2001年)

- Dr. Seigo Kotani, Fujitsu labs. America presented at Third Annual US-Japan Critical Infrastructure Protection Forum, Nov. 27-29th, 2006 Washington DC;

“It is overwhelmingly more tragic to become an accomplice to an evil deed than it is to become a victim.”

- Dr. Markus Durig, German Federal Ministry of the Interior, presented at Keynote speech of TCG annual members meeting, Oct. 9th, 2007 Los Angeles, California;

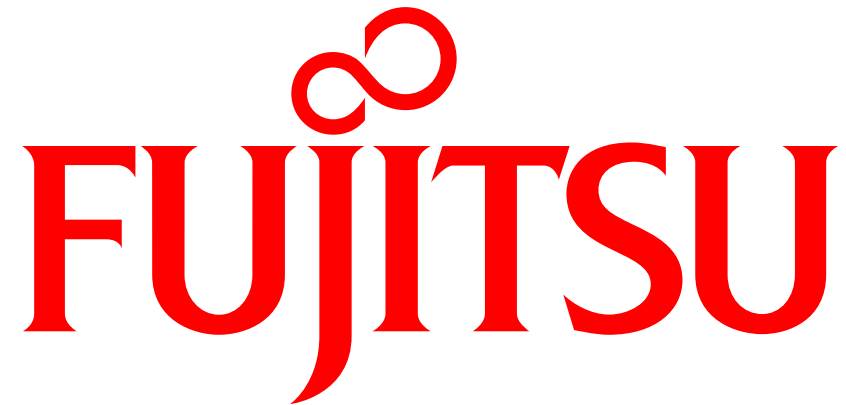
“Threats affecting information technology, New types of crime, Victim

トラステッドコンピューティングを発展させ、信頼できるインフラとして世界規模で確立し、これを運用する事で、無辜の民が悪事の片棒を担がされる（DDoSの踏み台にされる）ことなく、安心してインターネットの利便性を享受できる、世界平和の実現を目指したい。

ありがとうございました。



株式会社 富士通研究所
R&D戦略本部 IPR戦略室
シニアエキスパート、TCG常任理事 小谷誠剛
skotani@jp.fujitsu.com



shaping tomorrow with you

■ センシング情報真正性保証、長期保管、証拠性保持

- 航空機トラブル時のフライトレコーダに匹敵する証拠性確保
→ 第三者による検証可能性保証、免責性獲得
- プライバシー問題先鋭化 → 技術的理論的武装必須
- 電気自動車内電池の充電/寿命管理
→ ドライブ情報重要性増大

事故原因の切り分け：運転者か車か？
これは医療機器等でも同等のニーズ有り！
各国政府機関でのガイドライン制定進行中。
経産/総務省関連機関内で委員会設立済

■ リモートメンテナンス実施

- 部品共通化進展、リコール時影響範囲拡大
→ 一社対応に収まらない可能性増大、回収費用膨大、
ディーラー網が手薄な地域/国への販売促進で課題増大
- 自動車 ← パソコン同様にネット悪用悪意者の攻撃対象に！
従来のリコール時のみメンテナンス → 頻繁なケア実行必須

(ご参考)TCGと関連する他団体、その関係

■ リエゾン(メンバー名等はTCG内機密情報扱い)

■ 国家機関:

- 8国:日(IPA(経産省)、NICT(総務省))、米、英、独、仏、中、印、加

■ 大学/非営利団体:

- 15大学/2団体

■ 共通の権利:各WG参加(議決権無し)、義務:NDAおよびRANDへの署名

■ 非公式連携(メンバー名等はTCG内機密情報扱い)

- 各WGが、関連が有って互いにメリットを受ける団体について、個々の連携の方式について起案し、理事会承認を得て関係を結ぶ

■ 権利/義務/契約内容は個々の連携で異なる

- 例:ネットワークプリンタ/スキャナを検討するHardcopy WGは、以下の各団体と緩い連携(契約書無し、基本的に公開ベースの情報交換)を結んでいる
 - IEEE P2600 WG, IEEE-ISTO PWG Imaging Device Security WG
 - Linux Foundation Open Printing WG
 - JBMIA(社団法人ビジネス機械・情報システム産業協会)

ソフトウェアのみでは改竄や偽造の恐れがあり、実現される信頼性が低く、かつ遠隔からの状況の確認が困難

ハードウェアを信頼基点とし高信頼化、仕様を公開してコンプライアンス保証、見える化でプライバシー対策

Trusted Platform Module
(TPM) セキュリティチップ

ISOとして標準化(2009/10～)

■ ネットワークの安全性

- 確実なエラー訂正機能、なりすまし、盗聴、改竄を抑制、検知

■ プログラムの安全性

- プログラムの完全性、真正性を確認、担保できる

■ システムの安全性、免責性

- アップデートプログラムの検出、配信、適用確認及びその証跡



Trusted Network Connect
(TNC) 高信頼ネットワーク

IETF RFCとして標準化(2010/3～)

(ご参考)TCGの実績:PC/PC以外への展開

<http://cweb.canon.jp/office-mfp/lineup/color/features/management.html>

導入企業	内容
キヤノンリコー (2009/6~)	製品に記録されているパスワード、SSL通信用公開鍵ペア、ユーザー証明書などの機密情報を暗号化する暗号鍵(TPM鍵)をTPMチップ内に安全に保管。重要な情報の漏えいを抑止。
アメリカ大手銀行 (2010/4Q~)	ATMにTPMを実装、PKI鍵運用、ユーザ認証、サービス保守員認証を高信頼化、最適化
国内の某公共交通機関 (2009/12~) ※弊社対応実績	プラットフォーム、踏み切りなど多数のモニターカメラにTPMを実装し、映像の真実性(録画でなく、加工されていない)を保証、将来のトラブルに備えた免責情報として保存
海外の某公共交通機関 (2009/12~) ※弊社対応実績	TPM機能を実装したクラサバシステムで、相互の機器が正しい環境にあることを相互に監査、保証
某社 (2009/10~) ※弊社対応実績	検疫ミドルウェアをTNC準拠にすることによって、監査結果のコンプライアンスを保証

for DoT: 米交通省への意見提案(2011/8)

TCG組込WGからの提案

Trusted Computing Group (TCG)
Embedded Systems Work Group Response
US Department of Transportation Request for Information
Cyber security and Safety of Motor Vehicles Equipped with Electronic Control Systems



3.1.1.d Risk management including risk/vulnerability assessment and approaches/strategies to risk mitigation that can be applicable

Secure Software Architecture requirements.

Key capabilities:

- **Flexible integration** of new security mechanisms and protocols into overall security architecture
- **Flexible deployment** within the on-board network, e.g. centered or multi-centered approach, depending on the system environment and applications
- **Static and dynamic Configuration** of security mechanisms, policies and credentials
- **Secure update** mechanisms including the three processes; Check current situation remotely, Confirm installation completion, and Store certifiable log for indemnity
- **Security API** for application developers

TCG技術によるリモメン重要三項目の実現

- その時点での車状況の正確な把握
- 処理完遂(あるいは未完)の確認
- 将来に渡る証拠性ログ保存(免責)

M2M活動との連携模索

oneM2M-REQ-2013-0188-
UseCase_RemoteMaintenance

