JNSA PKI相互運用技術WG・電子署名WG主催セミナー資料
PKI Day 2018「超スマート社会（Society 5.0）におけるトラストの在り方」

FUJITSU
shaping tomorrow with you

PKIが熱望される場＝繋がるクルマ。そこで生まれる恩恵と脅威、それらへの方策

- TCG*: PC/サーバでの10年のセキュリティ経験を踏まえた提案
- 車載ソフトの遠隔(OHA*)保守/アップデート/地図配信/EDR*/TPMS*
- SDGs*, GDPR*対策

2018年4月17日

富士通(株) Mobility IoT事業本部 Mobility プラットフォーム事業部
TCG常任理事、組込系WG共同議長、自動車サブG共同議長
小谷誠剛

*個々の用語説明は後程行いますので、ご心配無きようお願いします。

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
- 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
- 2015年4月のPKI Dayで講演させて頂きました～3年振りです～

本日のキーワード

- OTA: Over The Air、無線で遠隔からいろいろ作業する総称
- EDR: Event Data Recorder、第三者検証性担保での法制化間近？

「国土交通省、自動運転車の損害賠償責任対応まとめ」2018/3/20
https://www.aba-j.or.jp/info/industry/2874/

- TPMS: Tire Pressure Monitoring System、同上?

各国で義務化(米国: 2007年、欧州:2012年、韓国: 2013年、中国: 2019年)

- FIDO: Fast IDentity Online、世界250社以上加盟NPOで策定する公開仕様

装置(スマホ/クルマ等)内で、利用者の生体情報と秘密鍵を紐づけ、PKIで通信、個人認証
プライバシー上取り扱いで慎重になる生体情報の管理をPKIと連携して解決、今後の主流？

- SDGs: Sustainable Development Goals、国連主導2030年の世界目標

長いPW記憶等のややこしい所作を個々に強いるのは愚問。FIDO活用が一つの解法。

- GDPR: General Data Protection Regulation、EU2018/5施行個人情報保全法

すべてに効く薬は存在しないが、FIDO/PKI/TPMで、そこそこの準備/対応は可能と思われる

- TCG: Trusted Computing Group、世界100社/機関以上加盟のNPO

TPM: Trusted Platform Module、TCGが仕様策定、ISO11889化したセキュリティチップ

→まず、ここまででご質問ある方、どうぞ！

本日の概要(開催案内から引用、若干加筆)

- NPO団体TCGが策定し、ISO化したセキュリティチップ(TPM)は、PKIに基づく仕様であり、2004年から多くのPC/サーバ、スマホ等に搭載され、セキュリティ強化に役立っています。
- このTPMをクルマに適用する検討をTCGが2012年からトヨタ様、弊社議長で作業部会 (Vehicle Services SubG) を立ち上げ進めています。即ち、PKIがクルマで活躍します！ 2018年内にクルマ用ISO15408Protection Profileを確立します！
- クルマでのリコールは近年、数百万台/件に及び大きな課題です。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です。クルマ自体を回収せず、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、社会全体も恩恵を手にします。更に自動運転用ダイナミック地図配信、EDR、TPMSのセキュア化についても対策が急務です。加えてPKI活用前提でスマホ等で広がっている FIDOを、自動車へ応用する検討も進められています。これはSDGs, GDPRの観点からも重要と考えられます（FIDOとTCGはリエゾン関係)。
- これら現状では実施困難な車載ソフトの遠隔保守/アップデート/地図配信/EDR/TPMSセキュア化/FIDO応用に関し、TCG/PKI技術で実現する活動についての状況、世界的流れ「SDGs, GDPR」につながる将来見通しを、国連活動を含む世界視野でTCG常任理事である講師が紹介します。

→次に、ここまででご質問ある方、どうぞ！

本日の内容

- 自動車が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、EDR(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

自動車が車外と繋がる事で生まれる恩恵

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

例1) リモートリプロ/メインテナンス

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。

(こういう制約を考慮しない動きがある事は、いろいろ報道されていますが…)

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。

自動車リプロ関連技術報告書

TTC技術レポート
Technical Report

TR-1068
自動車の遠隔更新技術の
標準化動向と実用化課題
第 1 版
2017年12月11日制定
一般社団法人
情報通信技術委員会

- 世界の17の機関/組織での活動を調査

特に、以下は注目すべきと思われる

- 国連WP29 TFCS
- 米国NHTSA
- 欧州ACEA
- TCG

次ページ以降に各概要を説明する

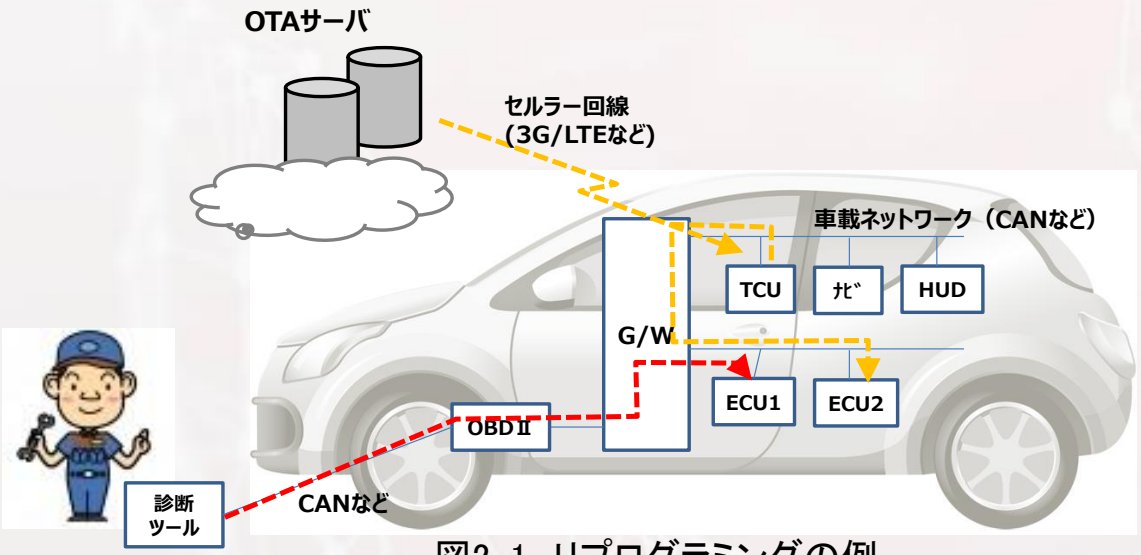


図2-1 リプログラミングの例
（赤色：従来の有線リプログラミング、黄色：OTAリプログラミング） http://www.ttc.or.jp/j/info/topics/20171214/

引用: 国連 WP29 TFCS

World Forum for Harmonization of Vehicle Regulations (WP.29)

- 国際連合配下の活動の一つである自動車基準調和世界フォーラム（WP29）は、協定に基づく規則の制定・改正作業及び協定の管理・運営を行っている。協定には1958年協定（国連の車両等の型式認定相互承認協定）、1998年協定（国連の車両等の世界技術規則協定）がある。
- WP29傘下に設置された自動運転分科会（ITS/AD）にて、2016年末に自動運転車のサイバーセキュリティとOTAに関して検討を行うタスクフォース（TFCS）が発足し、日本とイギリスが共同議長となり活動を進めている。
- Recommendation of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 IWG ITS/AD on Software Updates
- 上記のドラフト（草案）が準備されており、この中で「ソフトウェアアップデートに関する型式認定プロセス」が協議されている。
- 2017年末～2018年には成果物の取りまとめが行われる予定であり、成果物の内容は、各国における車両の基準策定に反映されていく見込みである。

引用: 米国NHTSA

- U.S.DOTはアメリカ合衆国運輸省、NHTSAはその傘下にある国家道路交通安全局の略称である。NHTSAは車のSafetyの推進を使命の一つとしており、Safetyの観点からV2Xや自動運転を推進し、ガイドラインやポリシーの発行を行なっている。
- 本レポートでは、NHTSA発行のAutomated Driving Systems2.0(2017/09発行)、Cybersecurity Best Practices for Modern Vehicles (2016/10発行)、Federal Motor Vehicle Safety Standards(2016/12発行)についてOTAに関する内容を中心に調査・報告している。
- Automated Driving Policy 2.0

2016年発行のFederal Automated Vehicles Policyの更新版。
Level3以上の自動運転システムを開発・運用する際のVoluntary Guidanceである。V2.0では、V1.0に比べてスリム化されており、V1.0ではOTAに際してSafety Assessmentを提出すべきとの言及があったがV2.0では省かれている。但し、Privacy等今後の議論が必要とされる項目も省かれており、将来的なバージョンアップにより再度記載される可能性がある。「テストは"独立した"第三者機関によって行なわれてもよい」など、Assessmentへの意識が垣間見られる記載は残されている。

引用: 欧州ACEA

- ACEA（欧州自動車工業会）は、ベルギーのブリュッセルに本部を置く、欧州自動車メーカの業界団体である。現在の加入企業は以下のとおり。

  BMWグループ, DAF, Daimler, FCA, Fordヨーロッパ, Hyundaiヨーロッパ, Iveco, Jaguar & Land Rover, PSAグループ、Renaultグループ, トヨタ自動車ヨーロッパ, VWグループ, Volvoグループ

- OTAリプロに関連する文書として、2017/9に以下を発行した。

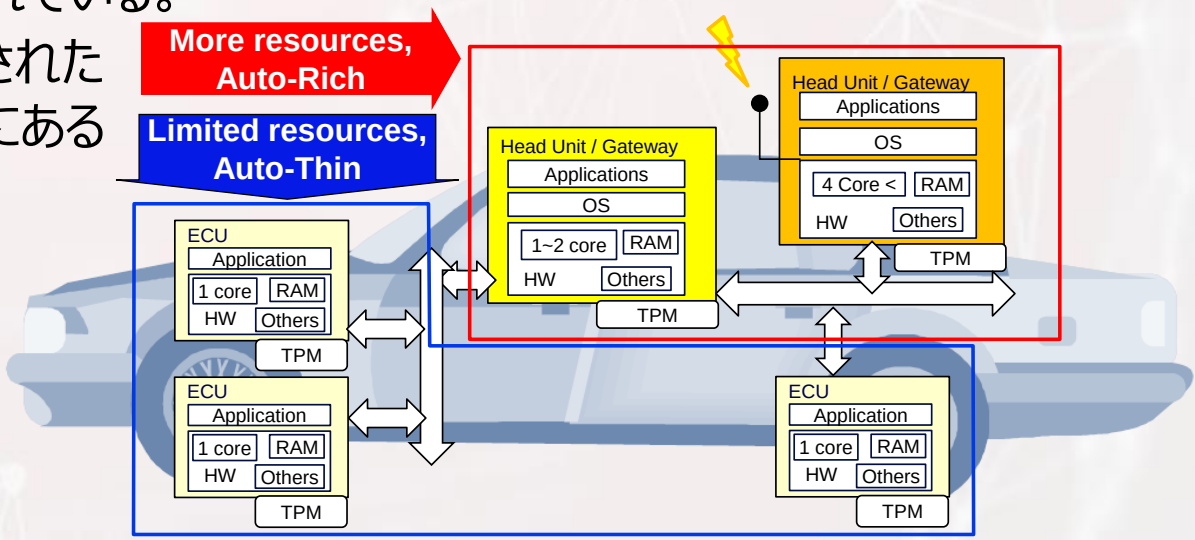
- ACEA Principles of Automobile Cybersecurity
  本書の中で、Secure over-the-air software updatesについて論じている。
  本発行物自体は法的拘束力を持たないが、ACEAがENISA, UNECE/WP29, Auto-ISACなどへの勧告に利用されることが記載されている。また、ACEA会員企業がISO/SAE21434における議論を進める上でのリファレンスとすることも言及されている。
- この中で、PKIに関し、以下の記述がある。

“Control keys and access: Keys are managed securely, and the use of a trusted infrastructure (Public Key Infrastructure) is encouraged.”

引用: TCG

- TCG (Trusted Computing Group) は、信頼できるプラットフォーム/インフラ構築のため、必要になる種々ハードウェア、ソフトウェアの業界標準、統合的公開仕様の開発、普及を目的とする2003年発足の非営利団体である。組織は世界各地の約90社の会員企業、約30の国家機関/大学/業界団体のリエゾンで構成されている。
- 主な活動として、プラットフォーム/インフラを構成する種々のハードウェア、ソフトウェアについて、各々を専門とする作業部会 (Working Group) で仕様を策定、上部組織である技術委員会で技術的面から他の規格/標準との関係を調整し、理事会では上記リエゾン関係にある各国政府機関の動静/意見を踏まえ評価、確定、公開している。
- さらに、それらの仕様を、標準化団体として実績あるISO, IETF等に提案、その結果、国際公開標準として認定されている。

右図は2015/3に公開/出版された自動車用セキュリティチップ仕様にある自動車への実装例である。



例2) EDR

■ 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
- EDR(日本では「ドライブレコーダー」とも呼ばれる)等市販機器が、業務用車両に搭載されるようになって居り、乗用車への搭載も徐々に進みつつある。
- 「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 ←3年前には記述が在ったのですが…

■ 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価格的/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。

ご参考：日経記事2018/3/31

https://www.nikkei.com/news/print-article/?R_FLG=0&bf=0&ng=DGXMZO28805990Q8A330C1MM8000

■ 自動運転中の事故、車の所有者に賠償責任、政府方針

- 2019年にも、国会に関連法案提出
- 事故原因の解明のため、運転記録装置（小谷注：EDRも、その類の一つ）の設置を義務付け、位置情報はハンドル操作、自動運転システムの稼働状況などを記録させる。
- ハッキングによる事故の賠償は、盗難車による事故被害と同様に政府の救済制度を使う。所有者がシステム更新など、セキュリティ対策をしていることが条件。

そして生まれる脅威/それらへの方策、各種機関の意見募集

TCG対応実績: TPM/PKIに基づくAudit & Accountability訴求

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中心に意見書提出、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**
NHTSA (2016/11)	**Agency Information Collection Activities; Proposals, Submissions, and Approvals: Federal Automated Vehicles Policy**	**組込系WGを中心に意見書作成/提出**
NHTSA (2017/11)	**Automated Driving Systems - A Vision for Safety 「自動車電子制御システムの安全性とセキュリティ」** https://www.regulations.gov/document?D=NHTSA-2017-0082-2907	**NHTSAとのF2F会合に基づいて意見書作成/提出**

NHTSA文書公開、それへのTCG意見提出: 2017/11

概要：2017/9発行v2は、2016/9v1のダイジェスト版(文章量は前版の約1/10)
- Privacy, Accountability等を削除
- v1.0で明示したチェックすべき15項目個々ガイダンス等が細か過ぎるとの批判に対処
- 「独立した第三者機関による検証可能性確保重要性」は削除されず明記
- コメントを2017/11/14まで受け付け、それらに基づき、その後改版する予定

TCGとしての対応:
- NHTSA幹部と2回会合 (2017/9/14理事会会合招待, 10/27小谷が代表でDoT訪問、F2F会議)
- v1.0コメント募集に提出したAccountability確保策(TPM/TNC/PKI)が、v2.0に反映されていないと苦言、ダイジェスト故であり、理論立ててコメント提出があれば検討可能との返答
- 国際公開仕様に基づくエコシステム(車載チップ、通信、鍵管理含む)でOTAリプロ実現可能、故に独立した第三者でも検証可能と主張、同意を得、その主旨のコメント提出を要請された
- TCG所定プロセスを経て理事会承認、2017/11/17提出、受理され、DoT公開サイトに掲示
  https://www.regulations.gov/document?D=NHTSA-2017-0082-2907
- v3.0で採用して貰えるよう3点に絞り込み(前回2016年は12点)、具体的修正文案提示
- ”Audit & Accountability” を強調/改版作業支援/採用働き掛け継続、ACEA(欧州自動車工業会)の宣告(PKI運用推奨明言)を最大限活用(日米追従必至)

  Validation Methods, Suggested Change:

  “Testing may be performed by the entities themselves, but could also be performed by an independent third party.
  Whichever entity performs the testing, audit and accountability should be considered.”(この最後一行追加を提言)

参考: FIDO: ユニバーサルで秘匿性の高い個人認証

■ EDR信頼性向上(自動運転も)のキーの一つはPersonalization

今現在、誰が運転席に座っているか”Audit & Accountability”

■ ID/PW入力を強いるのは困難、かつ信頼性に疑問

■ 生体情報に拠る簡便な認証が最適

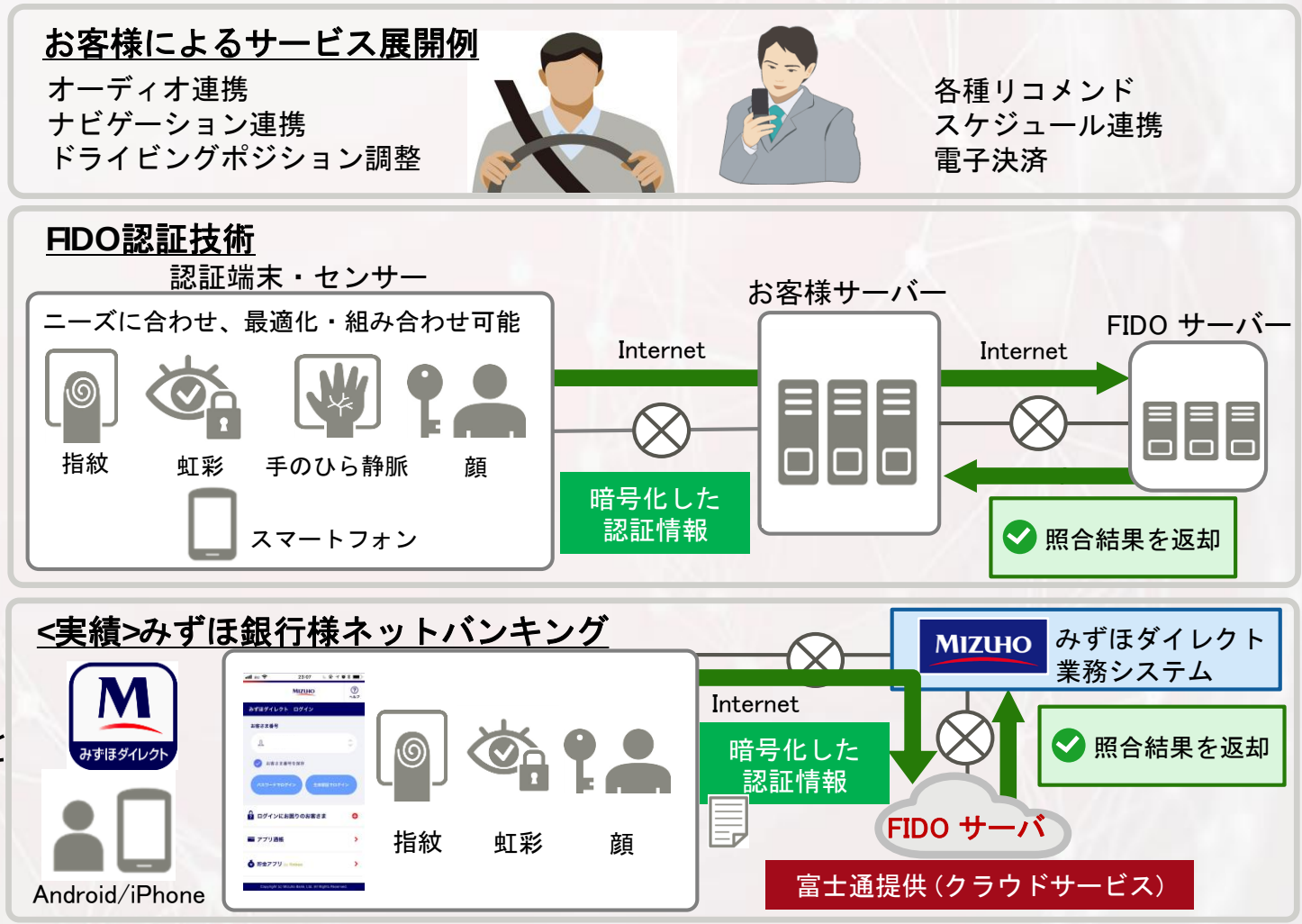
→SDGsに貢献

■ ここでの課題はプライバシー

■ それをPKIベースのFIDOで解決

■ スマホでの実績をクルマに展開

→GDPRに貢献



Trusted Computingの提案

2011年　100億台
2020年　500億台*

- 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

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13社(上記およびAMD, Cisco, Dell, Fujitsu, Huawei, HPH, Infineon, Juniper, Lenovo)
- 世界98社加盟(4/'18現在)

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

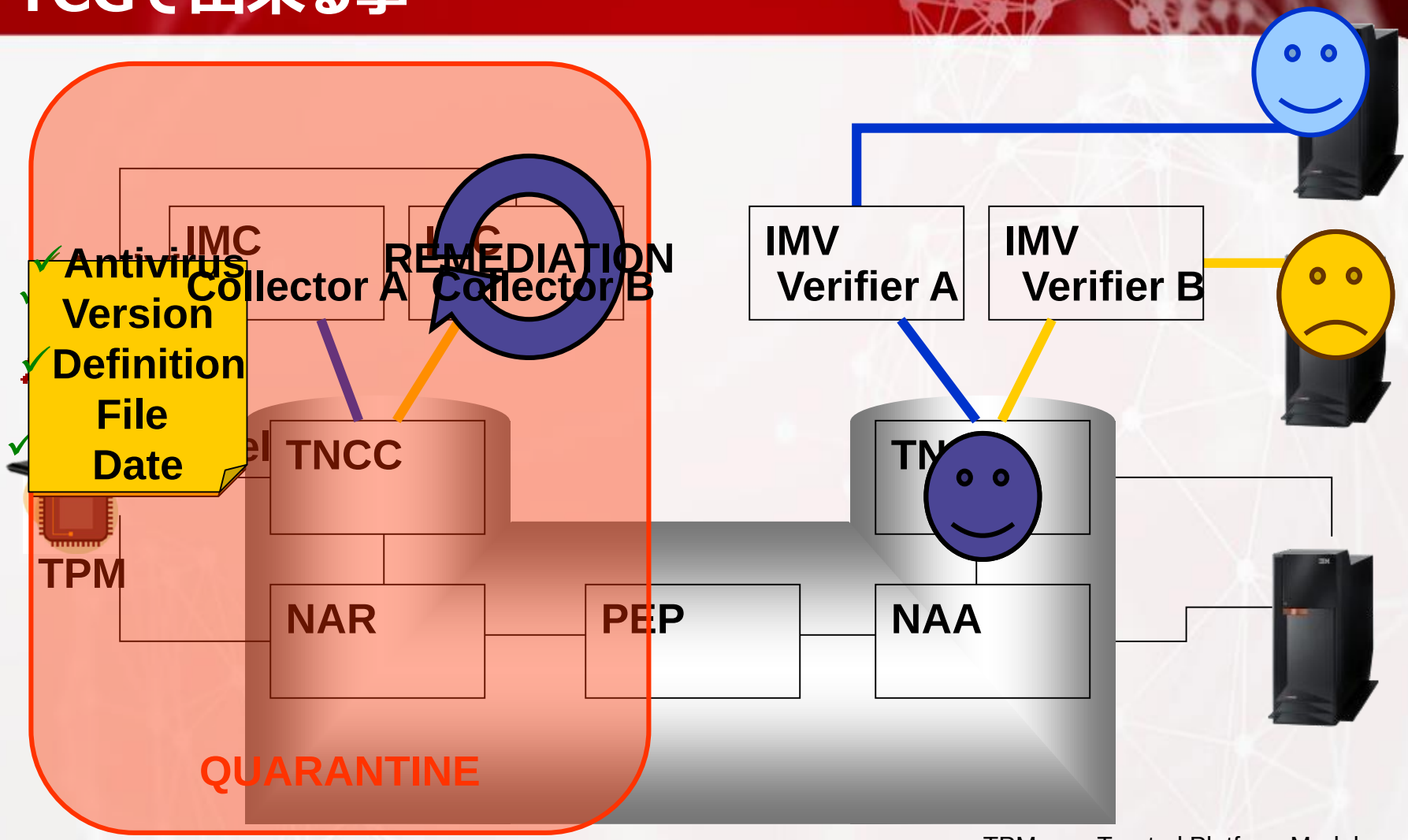
  - 多数国家機関(日,米,英,独,仏,中,印,加)、大学/研究機関/業界団体がリエゾンとして参画
  - 米国/EUの政府調達要件盛込み済(1/'06~)、日本は検討中

IPA(経産省)、NICT(総務省)

FIDO、ETSI、GP、ISO、etc

TPM(Trusted Platform Module)

TCGで出来る事



"Integrity Check of PC" sequence
Solution in TNC* Action

- TPM : Trusted Platform Module
- IMC : Integrity Measurement Collector
- IMV : Integrity Measurement Verifier
- TNC : Trusted Network Connect
- TNCC : TNC Client
- TNCS : TNC Server

(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。

日本政府関連活動まとめ

■ 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): コネクテッドカー専門委員会	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、報告書作成作業部会リーダ
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)。

ご参考：自動車向けTPM仕様書内説明図

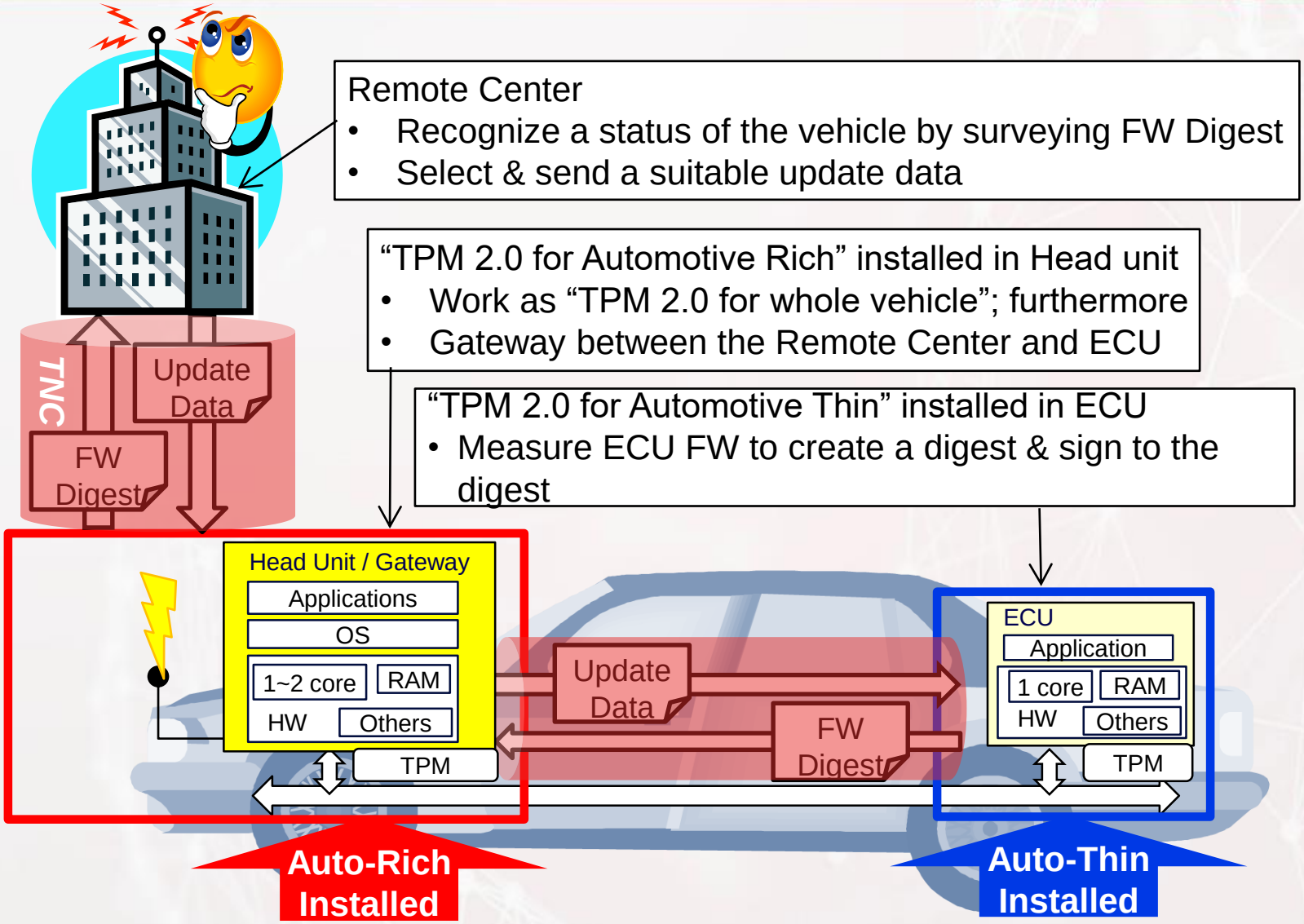
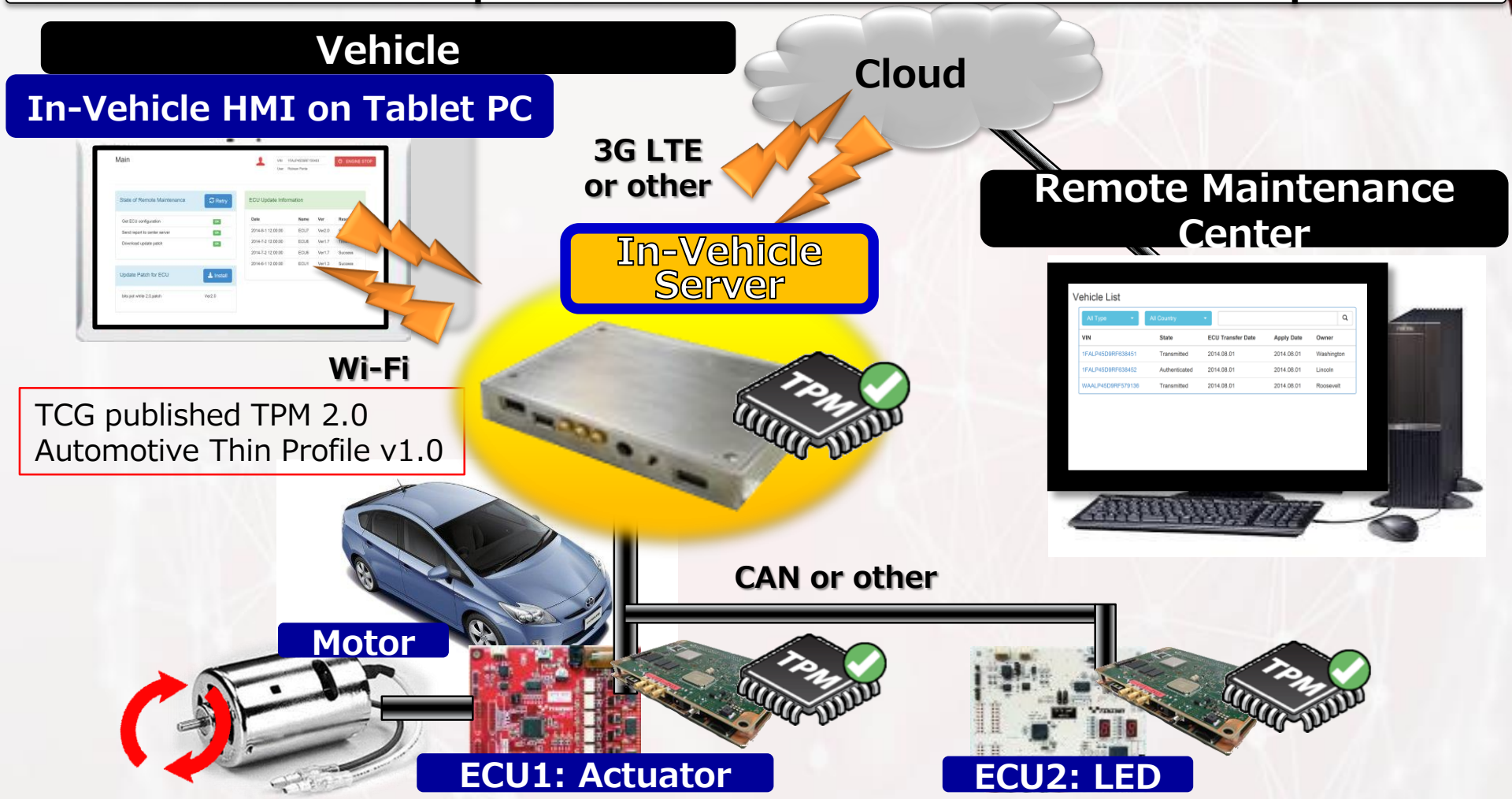


Figure 4: Message Flow for Remote Vehicle Maintenance

流れの補足：
・自動車内に多数(50-100個)実装されているECU個々に最小化したTPM-Thinを付属させ、個々のECU状態を正確に把握、センターに通知。
・センターで検証し、最適箇所への最適パッチを選択、自動車側へ送付。
自動車内元締めTPM –Richで署名検証後、個々のECUへ配布、インストール。
・完了後に再度、TPM -Thinによる報告書作成、センター集約、証拠保全。

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.

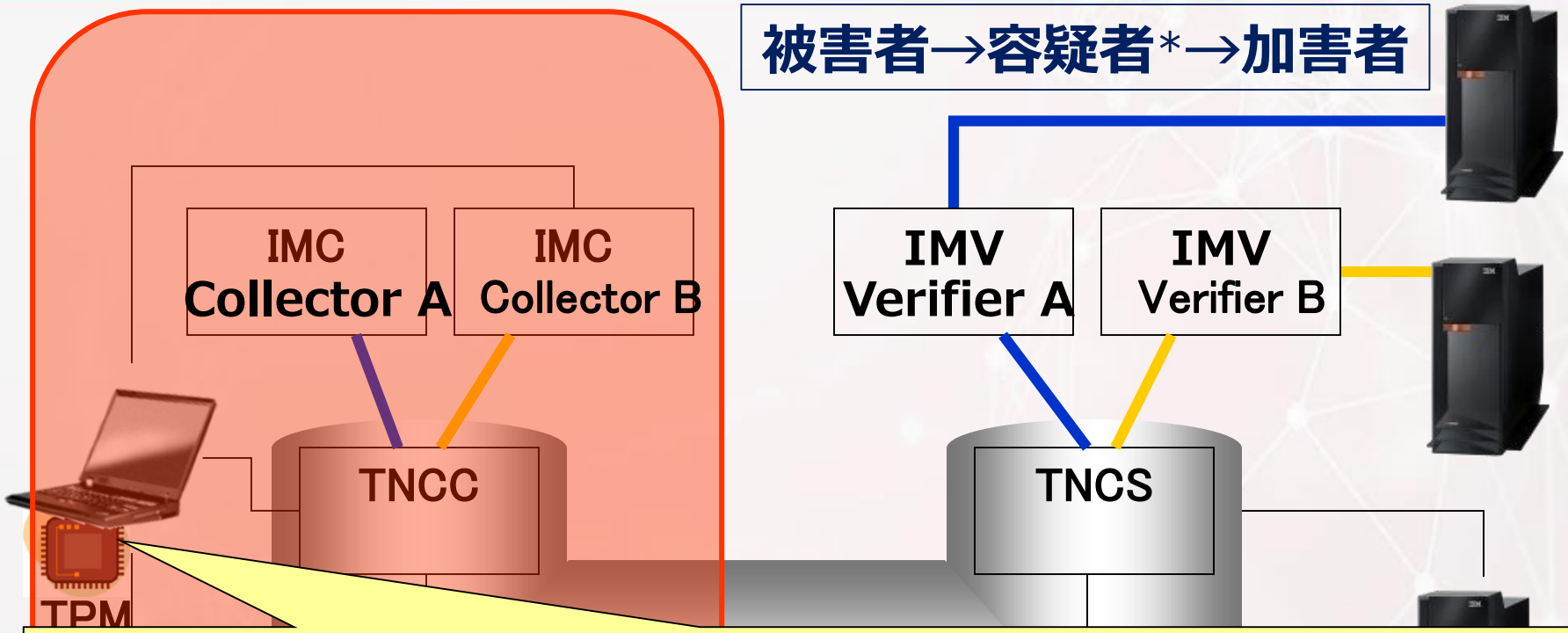


自動車を模したプラモデル、リモートセンターを模したノートPC、その間を繋ぐ機器で構成
2015/4/20 RSA展示会(サンフランシスコ)、4/22 SAE年次総会(デトロイト)でデモ紹介

最後の付言: 25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」

まとめ：今、そこに有る脅威：誰もが加害者に！



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 ttp://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、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

Trusted Computing 基盤：私の熱意

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.”

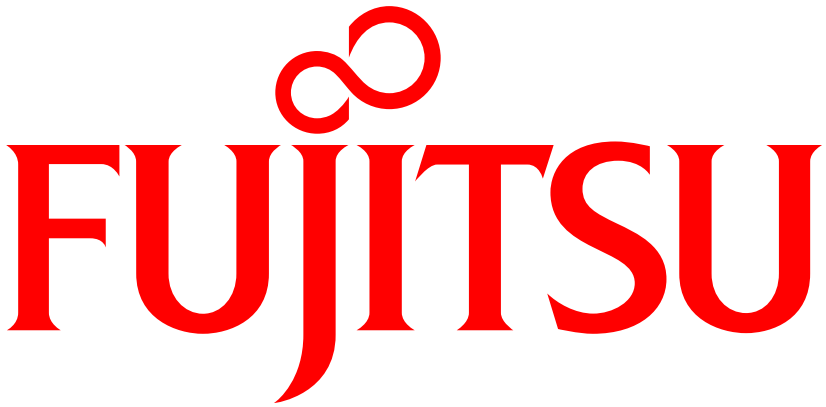
- Dr. Markus Durig, German Federal Ministry of the Interior, presented at Keynote speech of TCG annual members meeting, Oct. 9th, 2007 Los Angeles, California;

“Threats affecting information technology, New types of crime, Victim as *accomplice* (e.g. through botnets)”

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） こと無く、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。

富士通(株) Mobility IoT事業本部
Mobility プラットフォーム事業部
TCG常任理事 小谷誠剛
skotani@jp.fujitsu.com



shaping tomorrow with you