# TCG最新動向のご紹介

TCG常任理事
TCG組込系WG共同議長
TCG自動車サービスサブG共同議長
小谷　誠剛　富士通株式会社

15周年

# TCG – 改めてのまとめ

## 2003年設立NPO: HP, IBM, Intel, MSが設立した団体(TCPA, 1999年)を改組

### 会員企業 (2018/11/18 現在、日々募集中！)

https://trustedcomputinggroup.org/membership/member-companies/

- Promoter(理事会員)
  AMD, Cisco, Dell, Fujitsu, HPE, HPi, Huawei, IBM, Infineon, Intel, Juniper, Lenovo, MS
- Contributor(一般会員)
  Canon, Hitachi, Insight, Panasonic, Ricoh, Toshiba, Toshiba Memory, Toyotaを含む52社
- Adapter(賛助会員)
  CS Services, Hagiwara Solutions, Ubiquitous を含む16社(公開情報のみに基づく)

### 連携組織

https://trustedcomputinggroup.org/membership/industry-participation/

- 各国政府関係機関Liaison
  IPA, NICTを含む米、英、仏、独等多数
- 各種国際標準化団体
  ETSI, GP, IIC, ISO, OMA, FIDO等多数
- 各国大学/学術機関
  Beijing University of Technology等多数

### 支部

- JRF: 日本支部 — 10周年
- GCRF: 中国支部 — Greater, 8周年

# TCG – 最近の動向ご紹介

## 新設作業部会(WG)

- Cyber Resilient Technologies (CyRes)

https://trustedcomputinggroup.org/work-groups/cyber-resilient-technologies/

Chaired by MS, HP and Huawei

- Device Identifier Composition Engine (DICE) Architectures

https://trustedcomputinggroup.org/work-groups/dice-architectures/

Chaired by MS

## 組込作業部会(EmSys WG)

- Embedded Systems

https://trustedcomputinggroup.org/work-groups/embedded-systems/

Chaired by Fujitsu and Infineon

- IoT SG in EmSys

https://trustedcomputinggroup.org/work-groups/internet-of-things/

Chaired by Infineon and Intel

- Industrial SG in EmSys

https://trustedcomputinggroup.org/work-groups/industrial/

Chaired by GE and Infineon

# TCG – Cyber Resilient Technologies

- 2018/6 設立

https://trustedcomputinggroup.org/work-groups/cyber-resilient-technologies/

- 回復のための主要な以下三方式支援に特化する
  - Protecting updatable persistent code and configuration data
  - Detecting when vulnerabilities are not patched or when corruption has occurred
  - Recovering reliably to a known good state even if the platform is compromised

- このWGの成果物は、回復に関する公開された他の文書(以下等)を補完するものとなる
  - NIST SP800-193 (米国国立標準技術研究所発行のコンピュータセキュリティ関係レポートの一つ)

  Platform Firmware Resiliency Guidelines (2018/5 確定、公開)

  https://csrc.nist.gov/publications/detail/sp/800-193/final

# TCG – Device Identifier Composition Engine

- 2016/10 設立

https://trustedcomputinggroup.org/work-groups/dice-architectures/

- 必要最小限のチップでのセキュア確立、プライバシー保護を目指す

The DICE Architectures Work Group is exploring new security and privacy technologies applicable to systems and components with or without a TPM.  The goal is to develop new approaches to enhancing security and privacy with minimal silicon requirements.

- TPMを用いるシステム、TPMを用いないシステム両方を扱う

The DICE Architectures Work Group approach holds promise to enhance security and privacy on systems with a TPM and provide viable security and privacy foundations for systems without a TPM.

# TCG – Vehicle Services SG in EmSys WG

- 2011/6 EmSys WG設立、2012/9 自動車サブG設立

(トヨタ自動車の2012/3 TCG加盟を契機とする活動活性化の一環)

https://www.trustedcomputinggroup.org/wp-content/uploads/Toyota-TCG-release-JP-Mar-14-final_Toyota_approved.pdf

Chaired by Fujitsu and Toyota

**2016/2 RSA Conf. SF,**
**2016/4 SAE World Cong. Detroit**

- 自動車用TPM仕様(TPM2.0 Auto-Thin)改版確定、公開(2018/5)

https://trustedcomputinggroup.org/wp-content/uploads/TCG_TPM_2.0_Automotive_Thin_Profile_v1.1-r15.pdf

➢ 説明責任担保を強調(Accountability): 4.9章

TCG supports "audit and accountability" from vehicles to third parties based on a total ecosystem including a chip as Hardware Root of Trust (HRoT=TPM), a security network attestation protocol (TNC: Trusted Network Communications), and central key management (PKI-Public Key Infrastructure) with Remote Center.

- ISO15408準拠 PM2.0 Auto-Thin Protection Profile 公開レビュー(2018/9-11)

https://trustedcomputinggroup.org/wp-content/uploads/TCG_PP_AT_Specific_TPM_SecV2_v1.0_-v0p25_PUBLIC_REVIEW.pdf

➢ このPP確立に拠って、チップベンダーがAuto-Thin製品化推進 (EAL4+以上取得)

ご参考：2018/10/16のTCG年次総会での組込WG入門講座での説明資料の一部

# Comments to NHTSA RFC were accepted

- The NHTSA second version was released on Sep. 2017
  - The Automated Driving Systems (ADS) 2.0 was the simplified version of v1.0, Sep. 2016
  - Due date of RFC was Nov. 2017.
  - VSSG discussed with BoD.
  - We submitted our comments with “Accountability.”
  - It was accepted and is shown on NHTSA public site as below;


Detailed Commentary:
TCG standards, among other mechanisms, can support "Audit and Accountability" analyzed by third parties. Hardware Root of Trust (HRoT=TPM), related attestation, and Trusted Network Connect (TNC) support different aspects of vehicle and data integrity. TPM is an international standard (ISO/IEC 11889), and TNC is also available via IETF. These standards, together with other building blocks can facilitate consistent testing via self-testing or third party testing or evaluation. TCG provides guidelines for third party security evaluation, while other technical consortia focus on self-certification in this space.

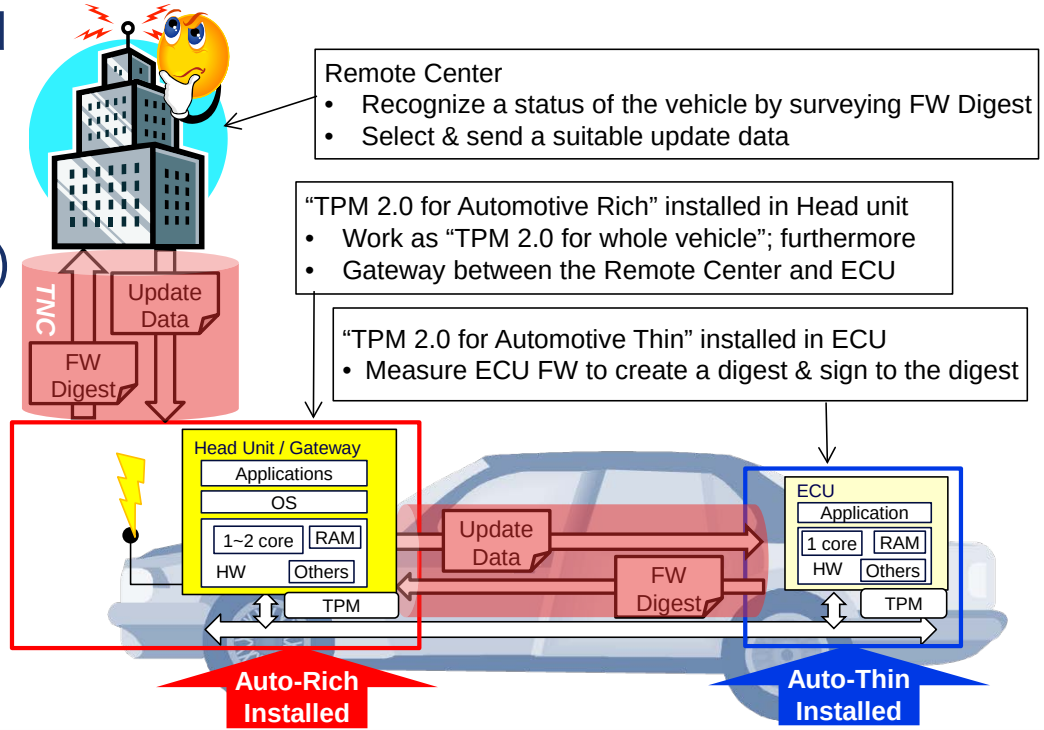
# TCG TPM 2.0 Library Profile for Automotive-Rich

- Draft is started
- Use cases need to be extended

(Dynamic map delivering,
Event Data Recorder,
Tire-Pressure Monitoring System..)

- GDPR must be considered
- TPM resources and

capabilities sizing



# ありがとうございました。

小谷誠剛
skotani@jp.fujitsu.com