東京工業大学
Tokyo Institute of Technology

NTT

# IoTセキュリティ－セキュアコンポーネントの潮流

第10回　ASISTシンポジウム
2022年4月27日

東京工業大学/日本電信電話（株）

庭野 栄一

# 本日の内容※

IoT環境に対するインシデントが顕在化しつある今日、ソリューションの一つとして期待される「セキュアコンポーネント技術」の新たな流れについて、国際標準化組織GlobalPlatformの動向を中心に概説する

- **IoTセキュリティ～トラスト基盤とセキュアコンポーネント**
- **標準化の牽引～GlobalPlatform**
- **IoTを背景とするセキュアコンポーネント技術の進展**
  - SE（ICカード、SIM/eSIM/iSIM）
  - TEE（Trusted Execution Environment）
- **TPS（Trusted Platform Service）**
- **セキュアデバイス認証～世界的動き、そしてsBOM**
- **セキュアデバイス応用～セキュアオンボーディング**
- **IoT分野への展開**
  - IoTガイドライン
  - スマートシティ
- **ダイナミックケーパビリティ**
- **今後の課題**

  **～セキュアコンポーネント上のIDコンポーネント管理**

**※ 次の講演内容をベースに改編・追加・構成**

庭野: 「デジタル社会におけるトラスト基盤 – セキュアコンポーネント技術 」
電子情報通信学会 デジタルサービス・プラットフォーム技術 特別研究専門委員会
第 8 回DPF研究会、2021.9

# IoTセキュリティ～トラスト基盤

東京工業大学 Tokyo Institute of Technology　NTT

## IoT環境の進展・エコシステム化によりデータ集約化・構成の分散化が進展し、動的に拡大する多様なオブジェクトの**真正性・信用・信頼性保証**の重要性増大

- 「ひと」だけではなく、「もの」、「こと」、これらの複合としての「システム」、これらが提供する「サービス」、など多様化するオブジェクトに対するトラスト保証～特に、信頼の基点と連鎖
- 実世界・仮想世界の融合による接合と摂動～データドリブン、アクチュエータ、デジタルツイン環境
- ゼロトラストネットワークにおけるデバイス・ID単位の認証、信頼の基点保証
- エコシステム化、 SoS（System of Systems）など複雑化するインターネット環境におけるサプライチェーン、ダイナミックデバイスオンボーディング・コンフィギュレーションの問題～多層化・複合化が進行する構成要素の信頼性
- 公共系APの本格搭載などモバイルデバイスの信頼性強化へのニーズ拡大～モバイルID

「ひと」の認証から、「もの」の認証、「ひと」に紐づけられた「もの」の認証、「ひと」・「もの」に紐づけられた「こと」の認証へ

－ **多様なオブジェクトの信頼の基点・基盤**としての ”**新たなセキュアコンポーネント技術**” の登場 －

# セキュアコンポーネントとは？

東京工業大学 Tokyo Institute of Technology　NTT

- ICカード、SIMカードに代表される「セキュアコンポーネント」は外部からの攻撃に対する強い耐タンパ性を有する独立した一種のコンピュータ
  - 多様なステークホルダの、強固なセキュリティが要求されるAPを、独立したセキュア環境で管理・実行可能
- 2000年代から、決済系における磁気カードのセキュリティ問題等より「ひと」のセキュアな認証が可能なICカードが普及進展
- 同時に世界的な電子行政の流れで、国民IDカードのICカード化、マルチAP化の議論が活発化し、併せて携帯電話の加入者認証のためのSIMカード普及
  - 発行後に、**リモートでセキュアにAPを管理する仕組み**の開発と標準化が進展
  - 国際標準化組織**GlobalPlatform**がマルチアプリケーション管理の標準化を牽引
- 現在、IoT・コネクテッド環境などデジタル社会の基盤進展とそれに伴うセキュリティに関わる脅威の拡大に伴い、**「トラスト」を鍵とした新たな展開**へと進展中

# GlobalPlatform（GP）

セキュアコンポーネントの「運用管理」に関して、世界最有力の国際標準化団体（フォーラム標準）

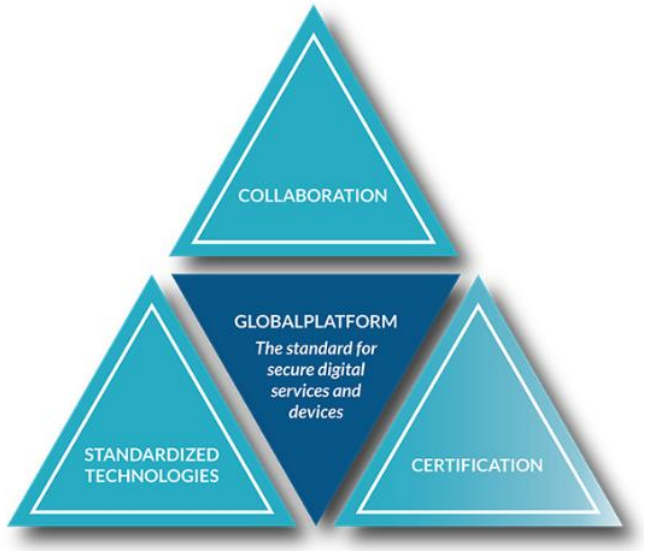
## 1999年設立、IoT向けセキュアデジタルサービス・デバイスに関わる団体へと発展

- 耐タンパ環境を提供する「セキュアコンポーネント」の管理および共通サービスの規定がベース
- 決済・通信市場におけるユーザ認証から、IoT市場におけるデバイス認証向けの標準化を推進中
- 仕様のみならず、機能・セキュリティ認定も提供（現在約30のプログラム）

## 多様な企業で構成、多くの関連団体とアライアンス形成

- 企業数約90団体、連携パートナ30団体以上（2022.4現在）
- 多様な業種から11人の理事（庭野は理事の一人、現在アジア唯一）

## 国内からはPKIベースの管理方式や非接触通信方式などで貢献




出典：GlobalPlatform

# GPの最近の動向

東京工業大学 Tokyo Institute of Technology　NTT

セキュアコンポーネント技術の進展、デバイスプラットフォームIF規定、デバイス評価認証・応用

- **SIM多様化**、SIM管理のモバイルID対応、**TEE※1の多様なSecure MCU対応**
  - 発行者書き換え可能なSIM(eSIM）の普及【GSMA連携、自動車業界】, SoC※2統合型SIM（iSIM）の出現、SAMによるモバイル系の再燃
  - SIM内の**ハイパーバイザ（VPP: Virtual Primary Platform）化**と**ファームダウンロード**の標準化進展、OSへの適用検討予定【ETSI連携】
  - TEEの**RISC-V対応**【RISC-V Foundation連携】、ハイパーバイザー化・マルチTEE対応【CCC※1連携（今後）】
- デバイスの**トラストサービスIF（TPS: Trusted Platform Service）の標準化**着手
  - RoT/構成証明【TCG連携、IETF関連】の規定、外部汎用IoTデバイスアーキテクチャへの組込【OCF※2 連携：予定】
- IoT向けセキュアデバイス**評価認証**、セキュアデバイス**応用**へと対象拡大
  - 欧州ニーズ(Cybersecurity ACT-EUCC）を契機とした**デバイスPF評価認証**【ENISA/NIST連携】、**sBOM※3**議論【米国関連】
  - デバイスプロファイルに基づく、**セキュアオンボーディング**の推進【NIST連携】
- 耐量子暗号、軽量暗号の推奨暗号リスト及びセキュアチャネルプロトコル追加の検討中
- セキュアチップ系から、ローエンドデバイス系、そしてNW・デバイス制御系へとキープレイヤ拡大
  - 【セキュアチップ】Tales/G&D/STMicro/NXP→【モバイル】ARM/Qualcomm+モバイル端末ベンダ→【PC/NW系】Cisco
  - インテルが加入し、高機能デバイス関連の検討加速か？（GSA※4との連携検討中）

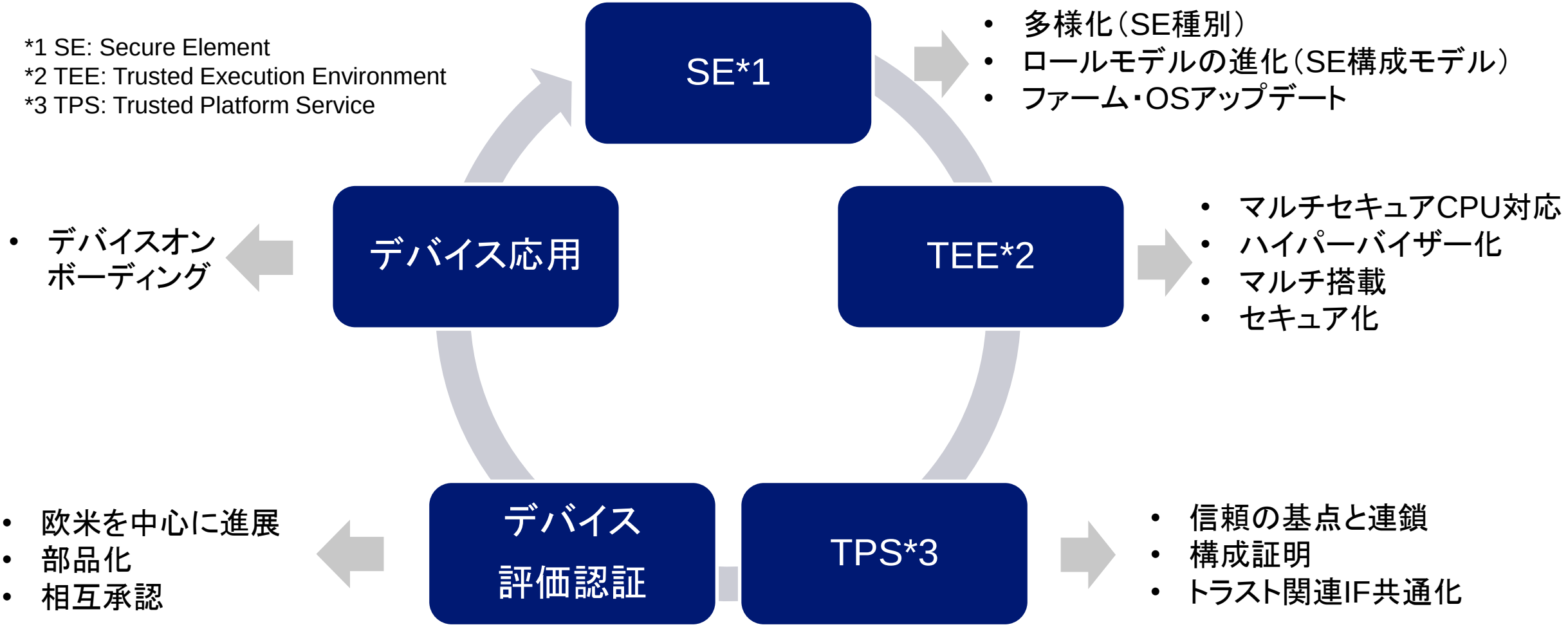
※1. TEE: Trusted Execution Environment, ※2. System on Chip, ※3. Confidential Computing Consortium, ※4. Open Connectivity Foundation,
※5. Software Bill Of Materials（ソフトウェア部品表）※6. Global Semiconductor Association

# セキュアコンポーネントの潮流

東京工業大学 Tokyo Institute of Technology　NTT

## IoTデバイスを対象としたトラスト基盤としての進化～GPを中心に標準化進展

*1 SE: Secure Element
*2 TEE: Trusted Execution Environment
*3 TPS: Trusted Platform Service




- 多様化（SE種別）
- ロールモデルの進化（SE構成モデル）
- ファーム・OSアップデート

- マルチセキュアCPU対応
- ハイパーバイザー化
- マルチ搭載
- セキュア化

- 信頼の基点と連鎖
- 構成証明
- トラスト関連IF共通化

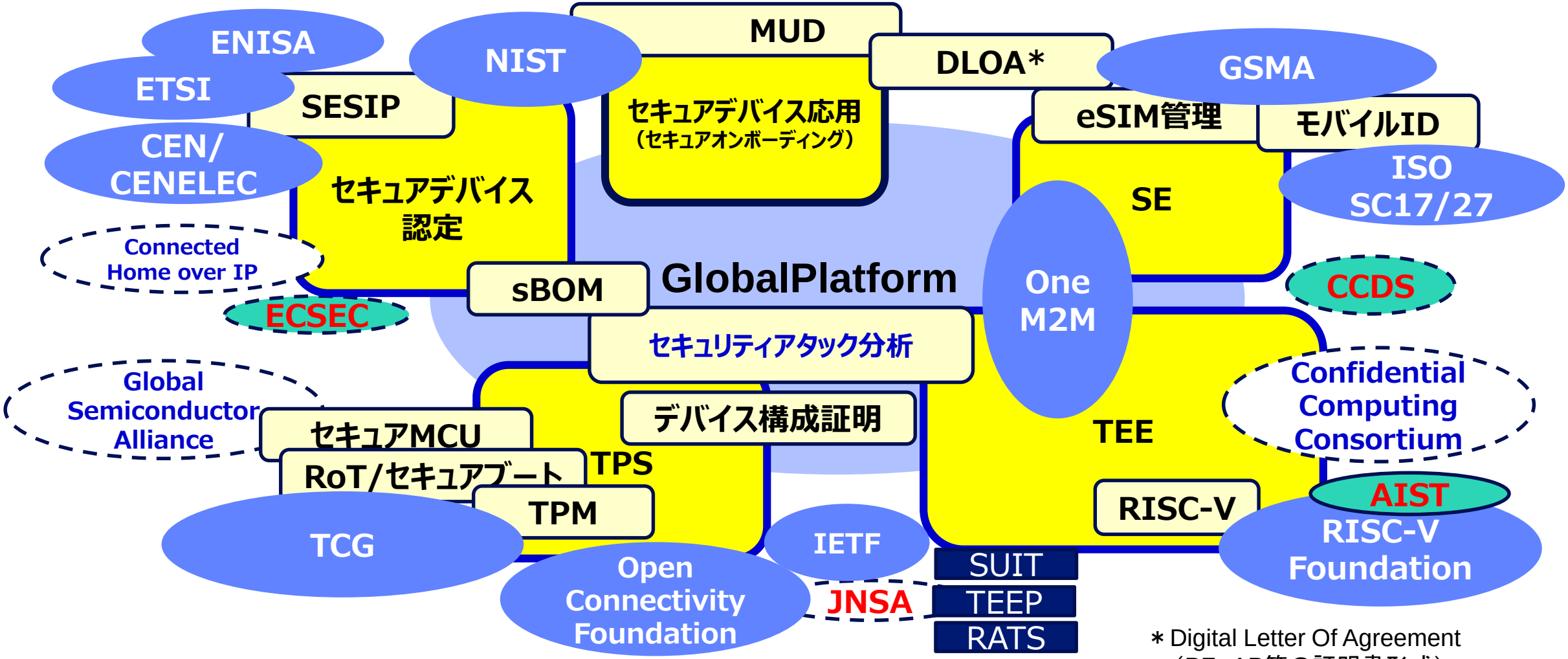
- 欧米を中心に進展
- 部品化
- 相互承認

- デバイスオンボーディング

# IoTに関わるGP連携の拡大

東京工業大学 Tokyo Institute of Technology　NTT

■ トラステッドプラットフォームサービス、セキュリティ認定、TEE関連の連携活発化




＊Digital Letter Of Agreement
（PF、AP等の証明書形式）

# セキュアコンポーネント技術の進展

東京工業大学 Tokyo Institute of Technology　NTT

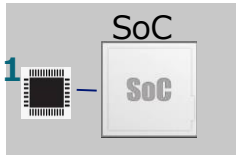
- 埋め込み型のeSIM（発行者可変）、SoC一体型のiSIM、デバイス内の高信頼実行環境TEE登場
- セキュアコンポーネント/セキュアデバイスの国際標準化団体GlobalPlatformを中心に標準化が進展

## HWベース

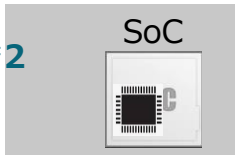
SE: Secure Element
耐タンパHW（コンピュータ）

①リムーバブル型


②埋め込み型 eSIM*1
IoTデバイス等、発行者可変




③統合型
セキュアブート等



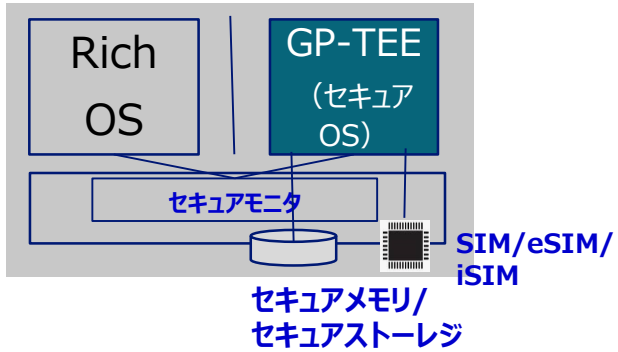

デバイス

## SW＋HWベース

TEE: Trusted Execution Environment
セキュアOS(SW)＋HW*

*①耐タンパHW　または
②セキュアコア（MCU/MPU）

構成例




デバイス

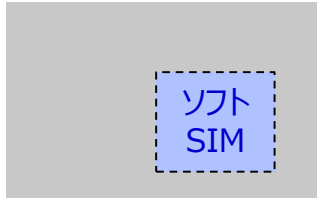
## 参考：その他

難読化等

例1．AMD SEV(TEE)

セキュアメモリ/ストレージを前提とせずVMの実行を秘匿化することによるTEE技術

例2．ドイツテレコム　nuSIM
（通信モジュール向け）




通信モジュール

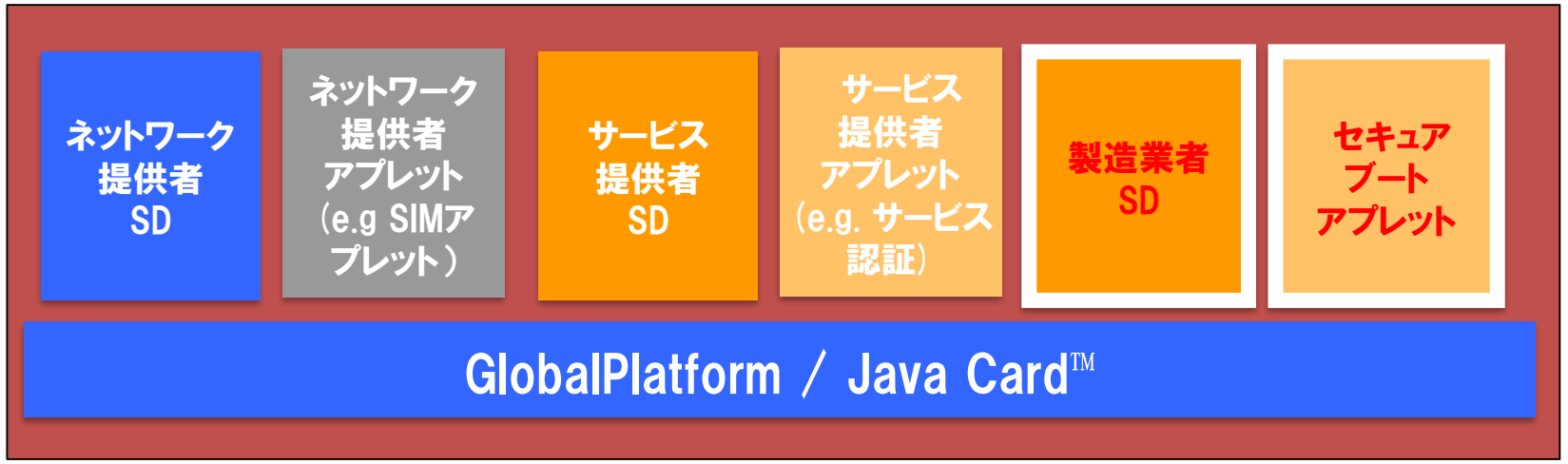
*1 eSIM: embedded SIM　*2 iSIM: integrated SIM

# IoTデバイス向けSE 構成例

東京工業大学 Tokyo Institute of Technology　NTT

## 埋め込みSE（eSIM/eUICC）の遠隔SD/AP管理（GSMA RSP＊）

- SD及びアプレットの搭載、パーソナライズ、クレデンシャルやコンテンツを遠隔で管理可能
- ネットワーク提供者のアプレット (e.g. セルラーネットワークのためのSIMアプレット)やセキュアブート用アプレット




GP資料を修正

＊RSP: Remote SIM Provisioning

# モバイルID関連の動き～ポストICカード

東京工業大学 Tokyo Institute of Technology　NTT

- モバイル環境におけるセキュアな公共サービス利用ニーズの拡大に伴い、モバイルデバイス関連の動き再加速中

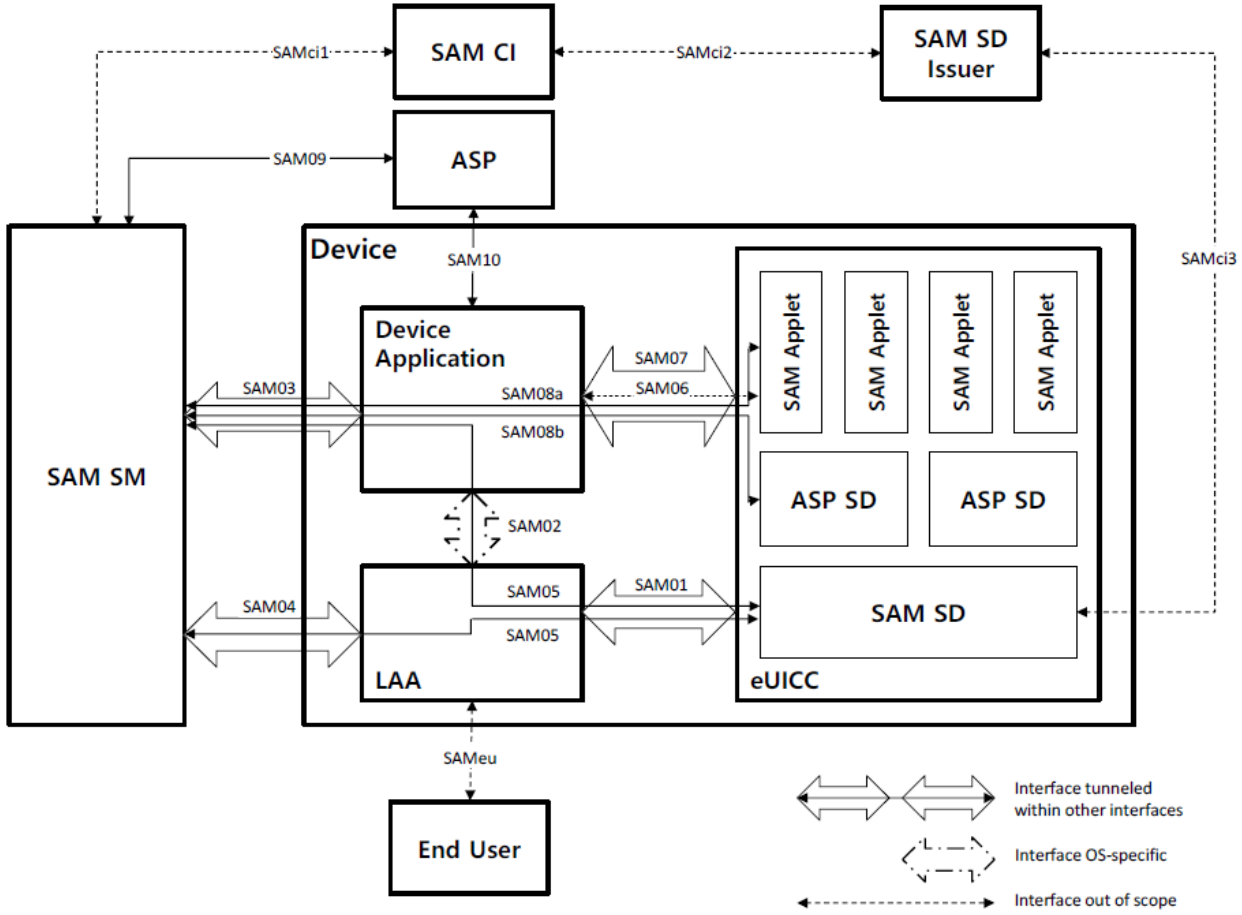
| いD項目 | 内容 | 種別 |
|---|---|---|
| マイナンバーカード機能のモバイル搭載 | 公的個人認証機能のモバイル搭載 | 政策（国内） |
| 欧州デジタルIDウォレット | EU全域にわたるモバイルID利用 | 政策（欧州） |
| GSMA SAM(Secured Applications for Mobile) | オペレータとは独立にeSIM等にデバイスAPと抱き合わせでセキュアアプレットを管理する仕組み | 標準化 |
| Android Ready SE | 公共サービス搭載を意識した、モバイルデバイスセキュリティ強化 | 技術/標準化 |
| ISO/IEC 23220（個人IDのためのICカードおよびセキュリティデバイス） | トラストに基づくセキュリティデバイス上のモバイルID管理 | 標準化 |
| 参考.<br>GSMA IoT SAFE【関連する動き】<br>（IoTデバイス向け） | RoTとしてのSIMを活用したIoTデバイス/クラウド間高信頼E2E通信の実現 | 標準化 |

# GSMA SAM Architecture

東京工業大学 Tokyo Institute of Technology

NTT

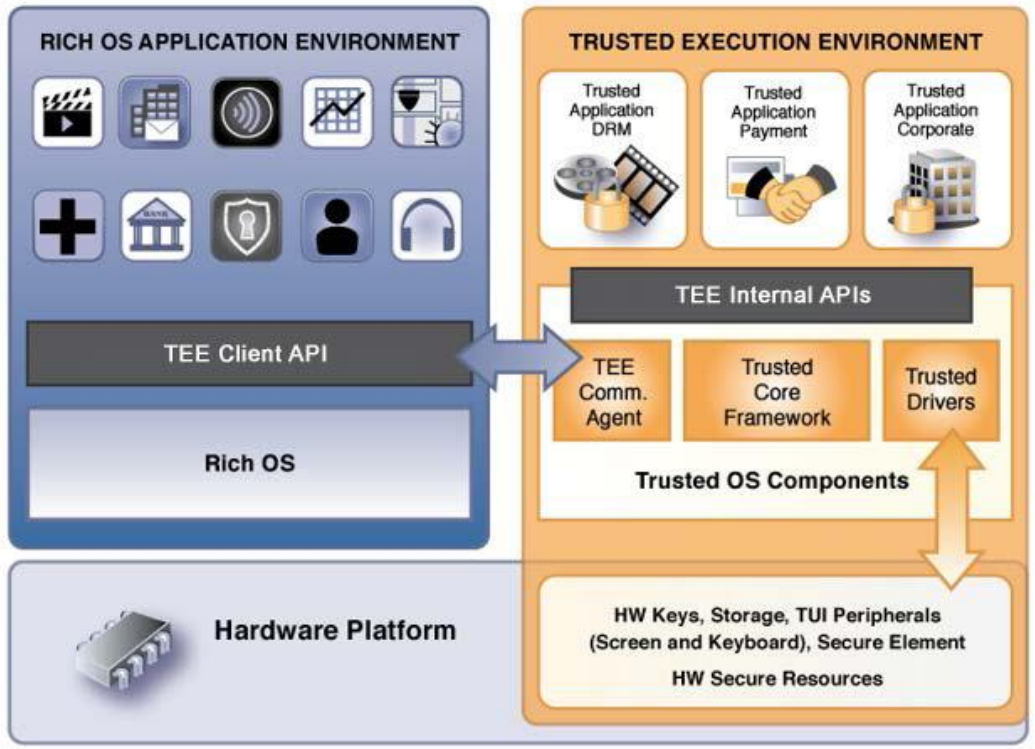
- カード発行とは独立にサービスAPを管理する仕組み



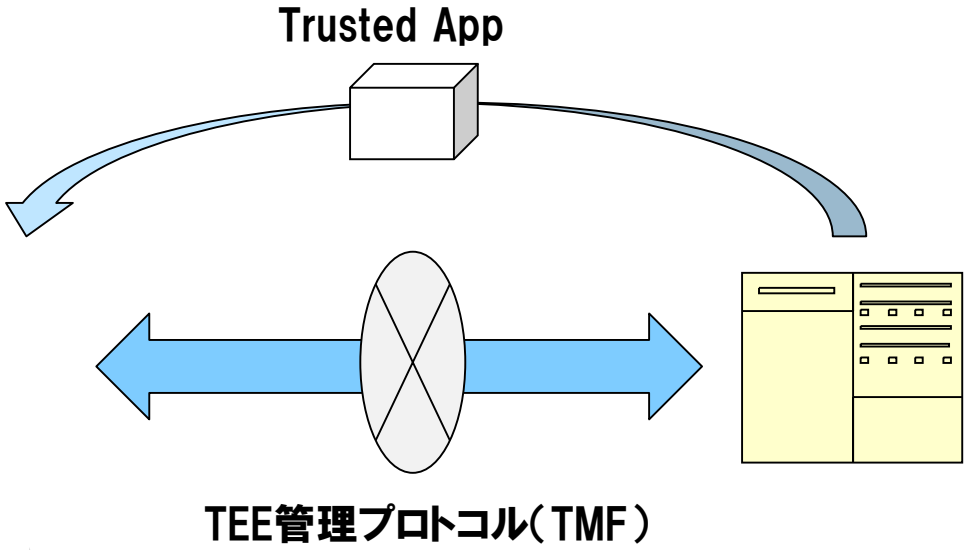

GSMA「Secured Applications for Mobile - Requirements Version 1.0 08 June 2021」より再掲

# TEE～ハイパーバイザー・マルチ化

- GP-TEE※としてはARM Trust-zoneベースの実装に加え、RISC-V上の実装検討進行中
- 現在、GP-TEEの他に多様なTEEが存在*1し、今後共通化／相互運用が鍵
- 産総研がRISC-V上でGPベースのクライアントAPIを検討*2




GP資料より再掲




- セキュアMCU: ARM Trust-zone, RISC-V
- ハイパーバイザー化・マルチ搭載

*1 他のTEE： Intel SGX, AMD SEV, RISV-Keystone など

*1, 2
須崎、「TEE(Trusted Execution Environment)とそれに関する研究開発動向」
電子情報通信学会 デジタルサービス・プラットフォーム技術 特別研究専門委員会
第８回DPF研究会、2021.9

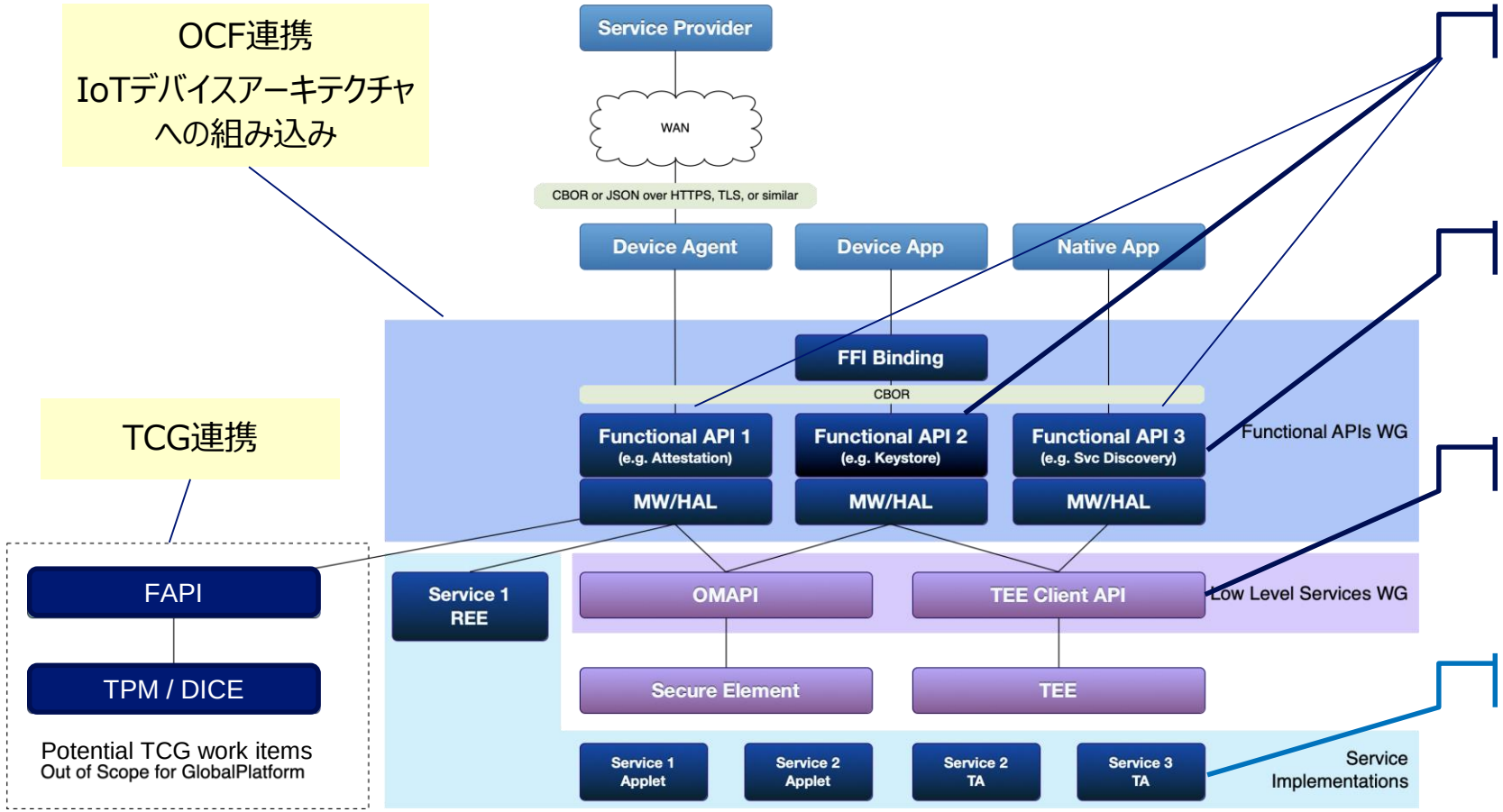
# TPS APIs～ロードマップ

東京工業大学 Tokyo Institute of Technology　NTT

■ セキュアコンポーネントを抽象化、セキュアデバイスサービスIFを規定

OCF連携
IoTデバイスアーキテクチャへの組み込み

TCG連携




## Common Client API design

Common approach to API design makes Learning and using new APIs easier

## Functional Descriptions

Each TPS Service has a separate Functional specification with (if needed) multiple configurations

## Low-Level Services

Design re-uses existing GlobalPlatform Specifications for communication with Secure Components

## TEE/SE/TPM implementations

Service implementations in TEE or SE
Co-operation with TCG MPWG on FAPI + TPM configurations/bindings.

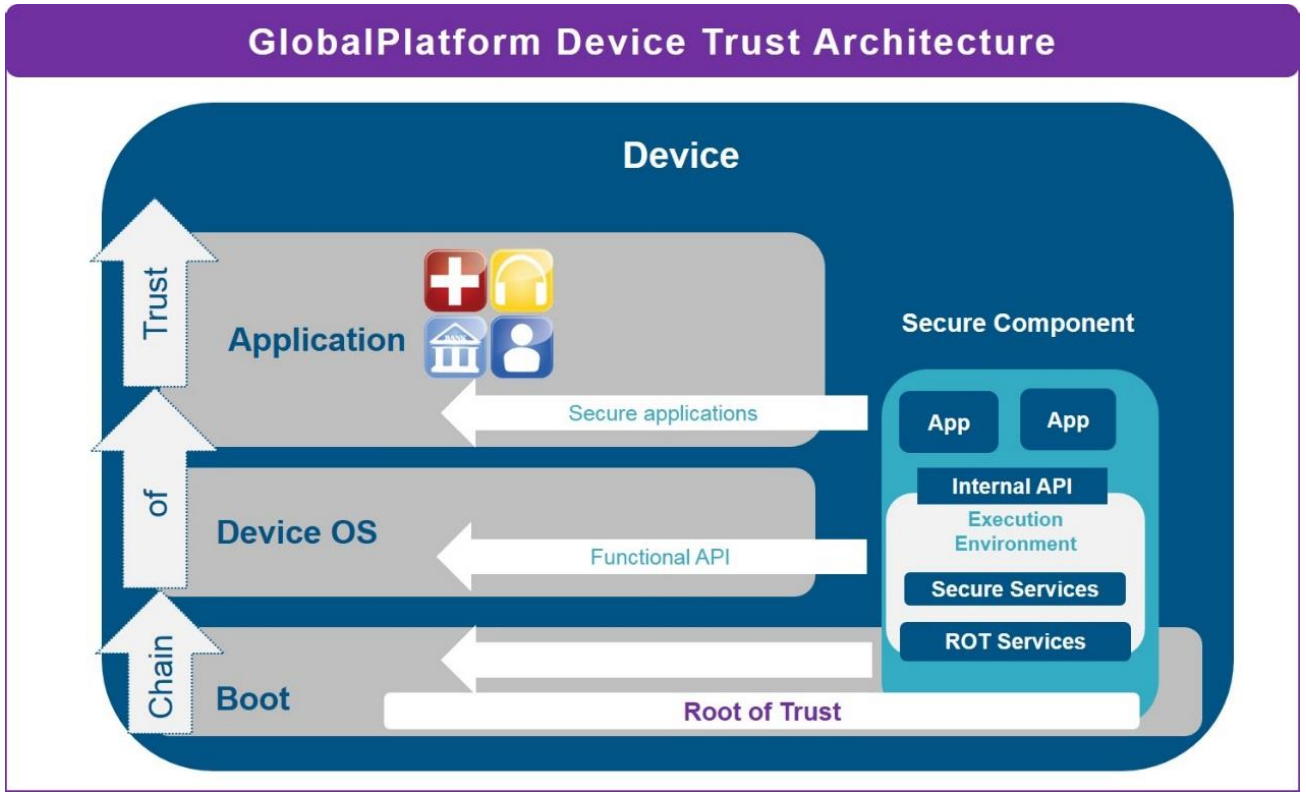
GP資料に加筆

# TPS～デバイストラストアーキテクチャ「DTA」

東京工業大学 Tokyo Institute of Technology

NTT

- 信頼の基点（Root of Trust）や連鎖（Chain of Trust）によるデバイスの信頼性提供
- 現在、TPSクライアントAPI、鍵管理API、構成証明プロトコルの検討作業中




GP資料より再掲

| 提供API | 内容 | 状況 |
|---|---|---|
| TPSクライアントAPI | TPSサービスを利用するためのAPI | 作業中 |
| キーストアAPI | 鍵管理用API | 作業中 |
| 構成証明API | 構成証明用プロトコルIF | 作業中 |
| デジタル認定書 | 機能認定、セキュリティ認定などのステークホルダで共有する認定のための認定書フォーマット | 公開済 |
| その他 | Open Mobile API等 | 公開済 |

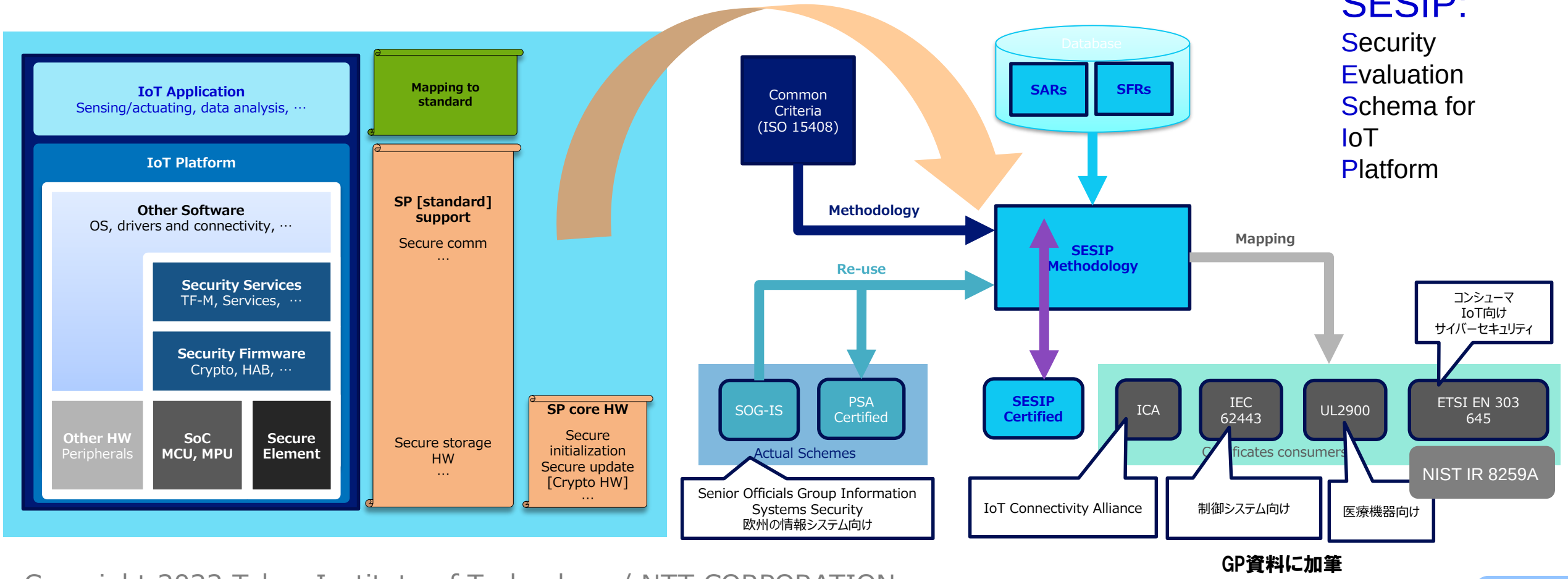
# デバイス評価認証(PF)～「SESIP」

東京工業大学 Tokyo Institute of Technology　NTT

- ISO15408をベースに規定
- 欧米（ENISA、NIST等）を中心に提案中、CEN/CENELEC/JTC13のNWIPとして採択 、米国「sBOM（ソフト部品表）」への対応検討開始
- GPでは認証機関の審査認定スキームを整備し、最初の認証機関として「TrustCB」を認定
  - TrustCB配下に、Brightsight等の評価機関【NXP/**Renesus**認証取得】、国内からは**ECSEC Lab**も申請中

TRUSTCB TRUST AND VERIFY

SESIP:
Security
Evaluation
Schema for
IoT
Platform



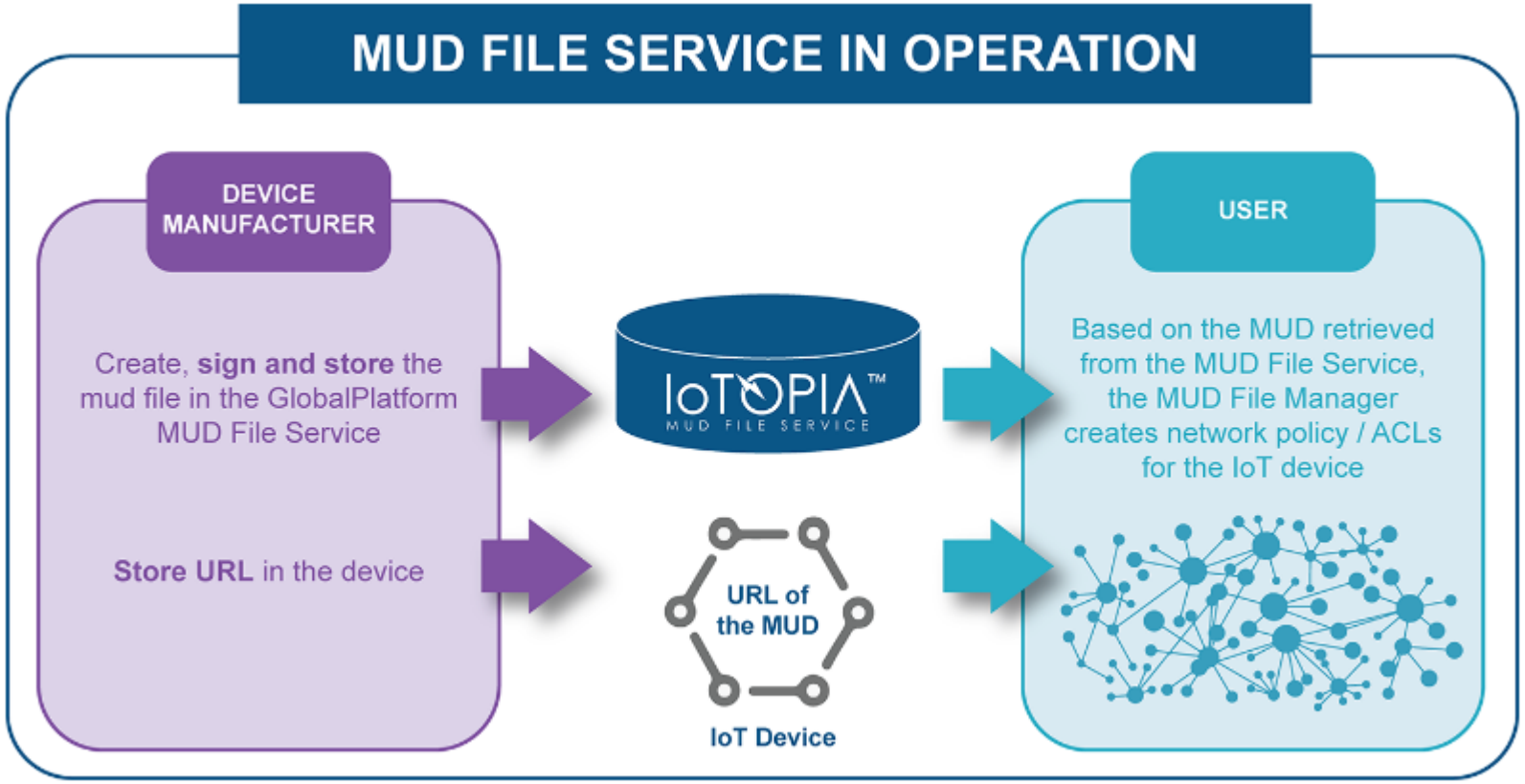

GP資料に加筆

# セキュアデバイス応用～「MUDファイルサービス」

東京工業大学 Tokyo Institute of Technology

NTT

- デバイスアクセス制御のためのMUD(Manufacture Usage Description）ファイルによるセキュアオンボーディング
- MUDの仕組みはIETFが規定




GP資料より再掲

# GP関連の展開状況 - IoT関連 -

東京工業大学 Tokyo Institute of Technology　NTT

IoTセキュリティ関連のガイドラインにおける参照、eSIMの導入が加速中

## 欧米・日本各種ガイドライン/標準

- ENISA-EUCC（SESIP）
- **CEN/CENELEC (SESIP)**
- **ETSI（TEE, eUICC, SESIP）**
- **GSMA（eUICC RSP、SAM、IoT SAFE）**
- NIST (SESIP)
- **OneM2M（SE, TEE参照）**
- CSA（Cloud Security Alliance, SE/TEE参照）
- IPA（GP TEE PP - 日本語版WEB掲載）
- CCDS（SE, TEE参照）

## 導入・展開

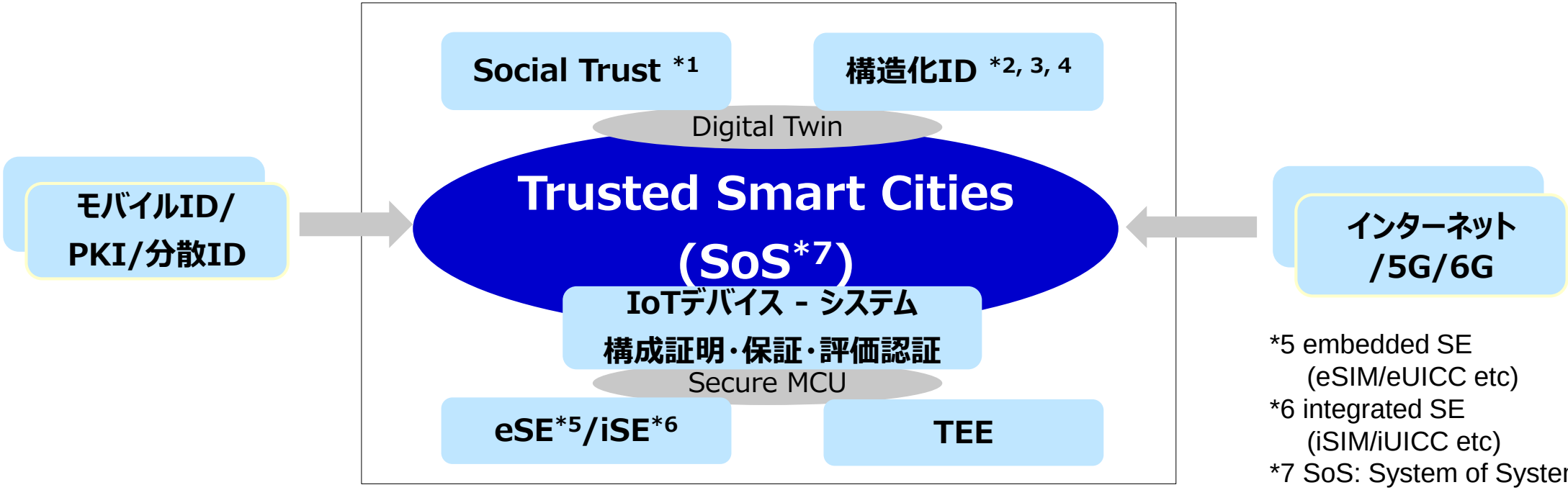
- eSIM
  - 自動車、電力メータ、HGW
  - 国内通信系企業等
- TEE
  - 携帯、ゲーム機、IPTV
- SESIP
  - TrustCB（GP認定最初の認証機関, Netherlands）
    - Certified Labs: Applus+ (Spain)、Riscure B.V. (Netherlands), SGS Brightsight (Netherlands, Spain -> **Renesas**)
    - Candidates: **ECSEC Labs (Japan)** etc.

**SoS対応**の進展
～Smart Cityなど

# 「Trusted Smart Cities」の実現に向けて

東京工業大学 Tokyo Institute of Technology　NTT

- 都市・社会を構成する構造化されたIDに関わるトラスト管理が重要
- ID構造、IDコンポーネントとセキュアコンポーネントの構成管理と評価認証が鍵




*5 embedded SE
(eSIM/eUICC etc)
*6 integrated SE
(iSIM/iUICC etc)
*7 SoS: System of Systems

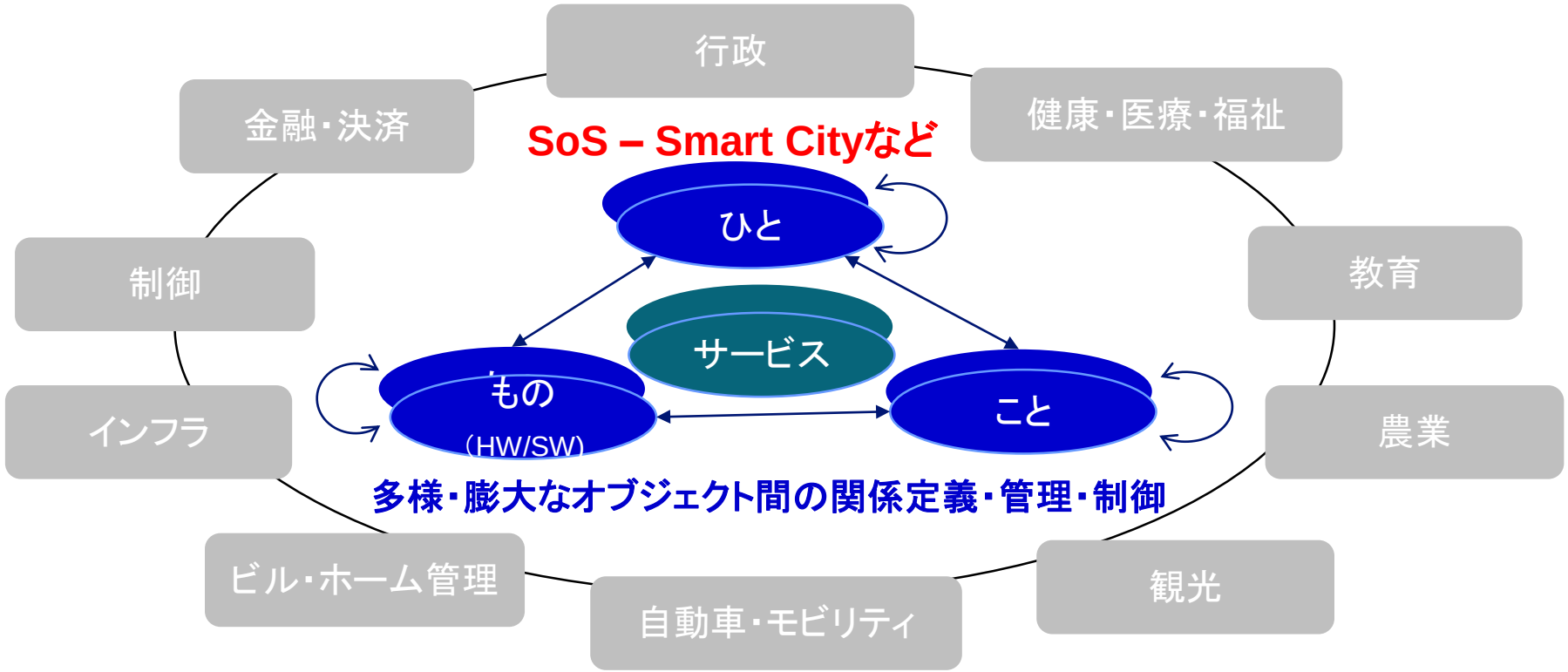
*1 E.Niwano, “From Secure to Trusted Smart Cities”, Global Forum 2015, 2015.9
*2 庭野、「GlobalPlatformの最新標準化動向 —IoT時代のセキュアコンポーネント」、NTT技術ジャーナル 2018. 12
*3 庭野、「IoT・エコシステム時代におけるセキュアコンポーネント～トラステッドなスマート社会を目指して」、ITUジャーナル2019年9月号
*4 E.Niwano, “Structured ID Components over Secure Environments”, Global Forum 2019, 2019.10

# ダイナミックケーパビリティ

東京工業大学 Tokyo Institute of Technology　NTT

## DX分野で使われる用語であるが、システム・サービスに対する対応がビジネス創出の鍵

- IoT・多分野連携により動的に生成される新たな関係・シナリオによる付加価値の創出と連鎖
- 最新技術による動的制御とセキュアコンポーネントを活用したSoSのトラスト保証



# 今後の課題

東京工業大学 Tokyo Institute of Technology

NTT

## セキュアデバイス関連の標準化および展開の加速

- TEE関連の標準化（GP-TEE, Intel SGX、AMD SEV、IETF TEEP等）
- デバイスソフトウェアアップデート標準への組み込み（OMA, BBF, OSGi）
- IoTセキュアデバイス認証の相互承認（欧州、米国、アジア）
- インターネット（IETF）、5G/6G、Smart City（ITU-T SC20等）等システム分野への展開

## セキュアコンポーネント上の構造化IDコンポーネントの管理・保証・評価認証技術の開発

- 構造化されたIDの関係性に基づくトラストの検討
- 上記のデバイス特性・責任モデル・保証レベルに応じたセキュアコンポーネント/デバイスの最適構成方式
- 上記に基づく、多様なNW/システムリソース（端末・エッジサーバ・サーバ、システム、SoS）の構成証明、トラスト保証・評価認証
- 部品化の進展と構成の多様化・複雑化に対応したトラストベースの動的制御