Hitachi Solutions Technology

Draft2

HITACHI

From IDPS-TEE Integration to a Security Platform Specification for SDV
IDPSとTEEの統合を起点としたSDV向けセキュリティ・プラットフォーム仕様の提案

2026/5/26

Hitachi Solutions Technology, Ltd. (Hitachi Group)
Security Solution Design 2nd Department

Kimitaka Asaka　kimitaka.asaka.hb@hitachi.com

Speaker Introduction

HITACHI

Draft2

浅香王隆　　Kimitaka Asaka
◆ セキュリティソリューション部門　部長　Manager, Security Solutions Division
◆ 日立ソリューションズ・テクノロジー　　Hitachi Solutions Technology, Ltd. (Hitachi Group)

経歴　Professional Background
◆ 2001年にキャリアスタート、開発業務に従事　　Career started in 2001, with hands-on development experience in:
- データベースエンジン開発とサーバーサイドアプリケーション開発
  Database engine and server-side application implementation
- 無線LAN、TCP/IPファームウェア開発
  WLAN and TCP/IP firmware implementation
- 自動車カメラアプリケーション開発
  Automotive camera application implementation

◆ 2024年からセキュリティソリューションビジネスのリーダー　　Since 2024: leading and launching security solution business

現在の取組　Current Focus
◆ 組み込みおよび自動車サイバーセキュリティ　　Embedded & Automotive Cybersecurity
◆ SDV指向のセキュリティアーキテクチャ　　SDV-oriented security architecture
◆ IDPS、TEE、OTA等を信頼性の高いプラットフォームとして統合　　IDPS, TEE, OTA and trust integration

HITACHI

Contents

Draft2

1. はじめに (Introduction)

HITACHI

Draft2

◆ SDV時代のセキュリティ課題 (Security Challenges in the SDV Era)

- 出荷後のソフト更新 (Software updates after shipment)
- ネットワークへの常時接続 (Constant connection to the network)
- 外部サービスやサードパーティアプリケーションとの連携
  (Integrate with external services and third-party applications)
- ECU種別や準拠規格ごとの要請　ex. IVI,Cockpit,Gateway…, ISO/SAE21434,IEC62443…
  (Requests for each ECU type and compliant standard)

◆ 取組みのポイント　(Key points of this initiative)

- ***個別最適から全体最適へ — SDVのセキュリティは共通基盤として設計できるか？***
  (From individual to holistic – Can SDV security be designed as a common foundation?)

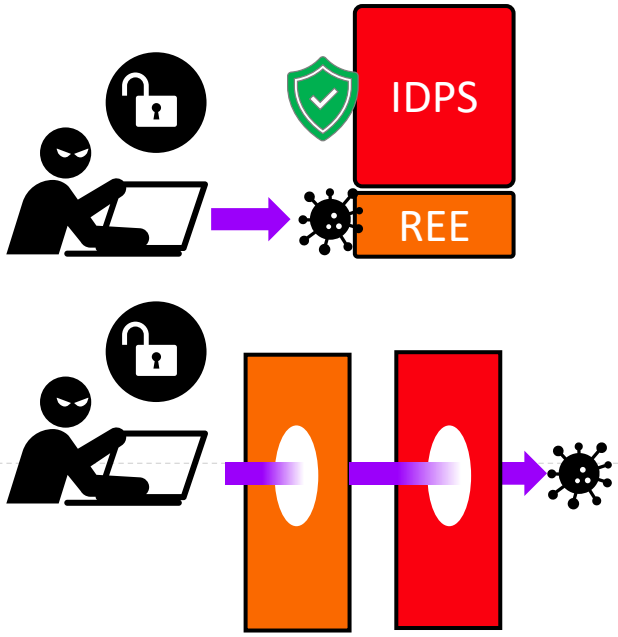
2. 私たちの課題 (Problem Statement)

HITACHI

Draft2

◆ 既存アプローチの限界 — なぜ個別実装の寄せ集めでは不十分か
(Limitations of existing approaches - why a hodgepodge of individual implementations is not enough)

- 想定される構造的な問題 (Expected structural problems)
  - ✓ REE管理下のIDPS防御機構の無効化　防御ルールと証跡が書換え
    (Disabling IDPS Defenses under REE Management: Rewriting Defense Rules and Trails)
  - ✓ 防御機構そのものが 起動前に無効化
    (The defense mechanism itself is disabled before activation)

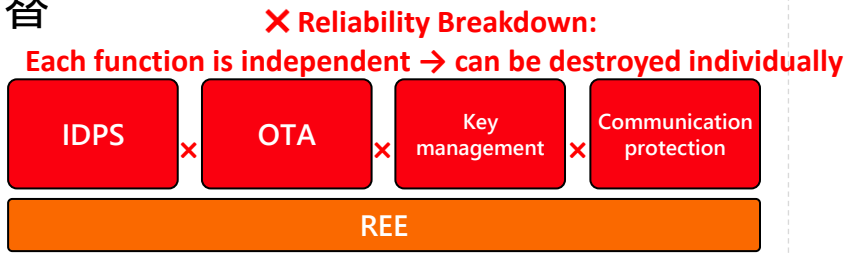


Example）攻撃シナリオ (Attack Scenario)

① 攻撃者がREEの権限を取得
(Attacker gains REE privileges)

② 防御ルール改ざん／ログ削除／IDPSプロセス停止／フック差替
(Defense Rule Tampering/Log Deletion/IDPS Process Stop/Hook Replacement)

- 結果として「重なっているだけ」(As a result, "it's just overlapping")
  - ✓ 各層が決定的に他の層と違うことをする必要がある
    (Each layer needs to do something decisively different from the others)



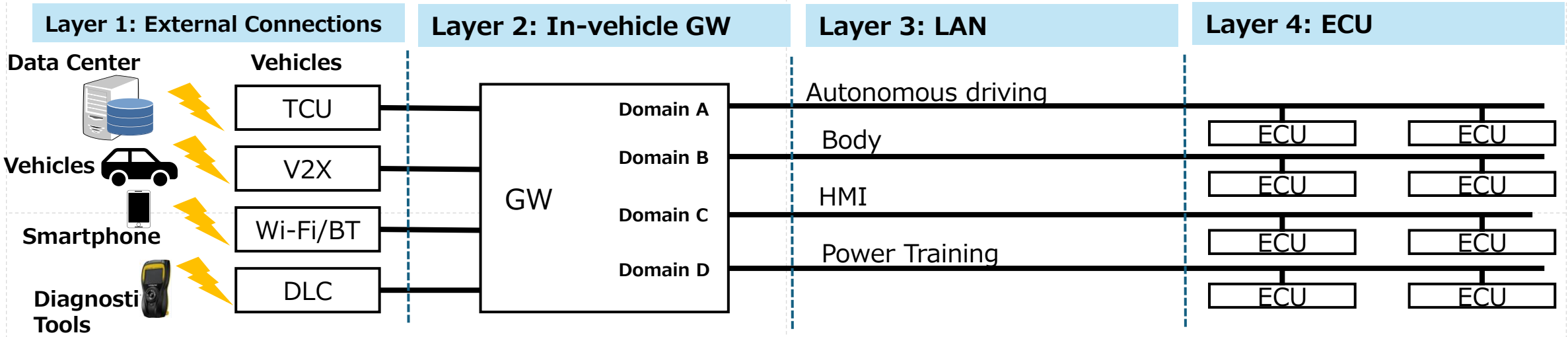
3. 防御の戦略(1) (Defense Strategy(1))

HITACHI

Draft2

◆ 多層防御を検討 (Consider defense-in-depth)

● 一般的なアーキテクチャ (General architecture)



→それぞれの階層でバラバラに設計していると信頼性の断絶が発生する

(If you design separately at each level, there will be a disconnect in reliability)

→ では、各層にどの要素技術を配置し、どこから統合を始めるべきか？

(Which elemental technologies should be placed in each layer and where should the integration begin?)

3. 防御の戦略(2) (Defense Strategy(2))

HITACHI

Draft2

- **「信頼性の断絶」を埋めるための要素技術マッピング**
  (Elemental technology mapping to fill the “trust gap”)
  - ✓ 最初はECUにフォーカスを当て、他の層との連携を模索
    (Initially, the focus was on ECUs and the search for collaboration with other layers)
  - ✓ １つの層内で複数の技術を組み合わせセキュリティを強化
    (Combine multiple technologies within one layer to enhance security)

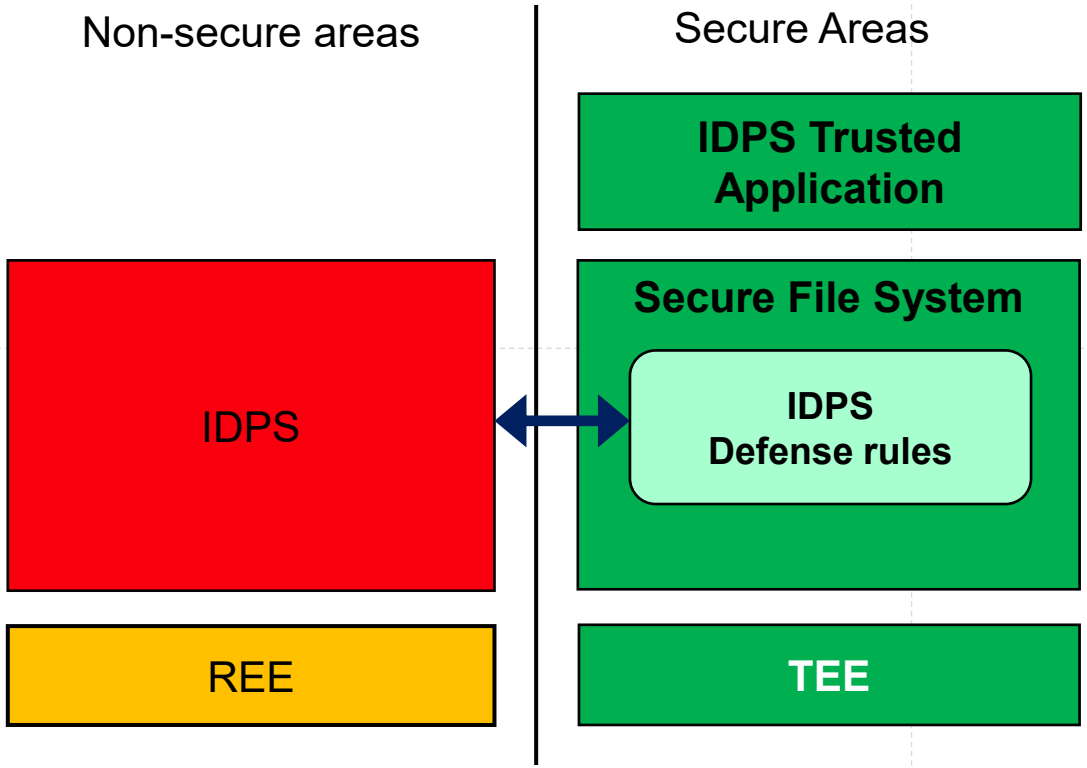
Layer 1: External Connections	Layer 2: In-vehicle GW	Layer 3: LAN	Layer 4: ECU
☐ PKI / Certificate Foundation ☐ TLS / DTLS / IPsec ☐ Secure OTA ☐ API Security ☐ Network IDS / IPS ☐ Host IDS ☐ TEE/HSM	☐ Secure Gateway ☐ Automotive Firewall ☐ Network Segmentation ☐ Network IDS / IPS ☐ Key Management ☐ Rate Limiting / DoS ☐ Same as Layer 4	☐ SecOC（AUTOSAR） ☐ Message Authentication Code（MAC） ☐ Network IDS / IPS ☐ Replay Protection ☐ Secure SOME/IP ☐ VLAN / TSN Security	☐ Secure Boot ☐ HSM ☐ TEE ☐ microTEE ☐ Host IDS / IPS ☐ Firmware Authentication ☐ Memory Protection（MPU / MMU） ☐ Secure Debug ☐ Runtime Protection

4. 進捗状況(1) (Current Status(1))

Draft2

◆ IDPSとTEEの統合 (Integrating IDPS with TEE)

- IDPS防御ルールのTEE内保護試作 (Prototype of In-TEE Protection of IDPS Defense Rules)



■ Our Evaluation Environment

Evaluation board
R-CarH3 StarterKit（Renesas）
CPU
ARM CA57 1.5 GHz quad core
ARM CA53 1.2 GHz quad core
Memory
RAM：4GB LPDDR4
OS
Linux Yocto
TEE
Kinibi (Trustonic)
IDPS
xCarbon (VicOne)

[References] https://cdn.vicone.com/archives/vicone/solution-brief/vicone-trustonic-idps-tee.pdf

4. 進捗状況(2) (Current Status(2))

Draft2

- 要素技術の配置の進捗とターゲット（Progress and targets of elemental technology placement)

  ✅ has been realized 🎯 is the next target 🗓️ is being planned

Layer 1: External Connections	Layer 2: In-vehicle GW	Layer 3: LAN	Layer 4: ECU
☐ PKI / Certificate Foundation ☐ TLS / DTLS / IPsec 🎯 **Secure OTA** ☐ API Security ☐ Network IDS / IPS ☐ Host IDS ☐ TEE/HSM	☐ Secure Gateway ☐ Automotive Firewall ☐ Network Segmentation 🎯 **Network IDS / IPS** ☐ Key Management ☐ Rate Limiting / DoS ☐ Same as Layer 4	☐ SecOC（AUTOSAR） ☐ Message Authentication Code（MAC） 🎯 **Network IDS / IPS** ☐ Replay Protection ☐ Secure SOME/IP ☐ VLAN / TSN Security	🗓️ **Secure Boot** 🎯 **HSM** ✅ **TEE** 🎯 **microTEE** ✅ **Host IDS / IPS** ☐ **Firmware Authentication** ☐ **Memory Protection（MPU / MMU）** ☐ **Secure Debug** ☐ **Runtime Protection**

4. 進捗状況(3) (Current Status(3))

HITACHI

Draft2

- 今後の課題 (Future challenges)
  - ✓ セキュアなOTAアップデート機能追加のための検討
    (Consideration for adding a secure OTA update function)
  - ✓ 他の技術(microTEE/HSM等)との役割分担 (Division of roles with other technologies (microTEE/HSM, etc.))
  - ✓ 性能ベンチマーク
    (Performance Benchmarks)

→***これらの検討から、単なる機能追加ではなく、設計思想そのものを創出したい***
(From these considerations, we would like to create the design concept itself, not just adding functions)

5. 取り組みから得られた考え(1) (What This Suggests(1))

HITACHI

◆ IDPS × TEE 統合で示す**3つの設計転換** (Three Design Shifts Demonstrated by IDPS × TEE Integration)

転換(1)　「守る側」こそ「守られるべき対象」
(Conversion (1) "The guardian" is the "object to be protected)

- IDPSは防御機構だが、REE上にある限り攻撃対象になり得る
  (IDPS is a defensive mechanism, but as long as it is on the REE, it can be a target of attack)

- TEEで防御ルール・ログを隔離 → 防御機構自体の耐性を確立
  (Isolate defense rule logs with TEEs → Establish the resistance of the defense mechanism itself)

5. 取り組みから得られた考え(2) (What This Suggests(2))

HITACHI

転換(2)　TEEは「鍵の金庫」ではなく「信頼の基盤」
(Conversion (2) TEE is not a "key safe" but a "foundation of trust")

- 従来：TEE ＝ 鍵・証明書の安全な保管場所
  (Traditional: TEE = Secure storage for keys and certificates)

- 転換：TEE ＝ 防御層全体を支える信頼のアンカー（ルール保護・ログ保全・真正性検証）
  (Transformation: TEE = Anchor of trust that supports the entire defense layer (rule protection, log maintenance, authenticity verification))

5. 取り組みから得られた考え(3) (What This Suggests(3))

HITACHI

転換(3)　単機能統合から「プラットフォーム化」へ
(Transformation (3) From single-function integration to "platformization“)

- IDPS×TEE統合の経験 → 他のセキュリティ機能も同じ構造で統合可能
  (Experience with IDPS × TEE integration → Other security functions can be integrated in the same structure)

- OTA・鍵管理・セキュア通信 → TEEを中核にした共通アーキテクチャの可能性
  (OTA, Key Management & Secure Communications → The Potential of a Common Architecture with TEE at Its Core)

→ ***この転換(3)を具体化したものが、次の Platform Vision***
(This transformation (3) is embodied in the next Platform Vision)

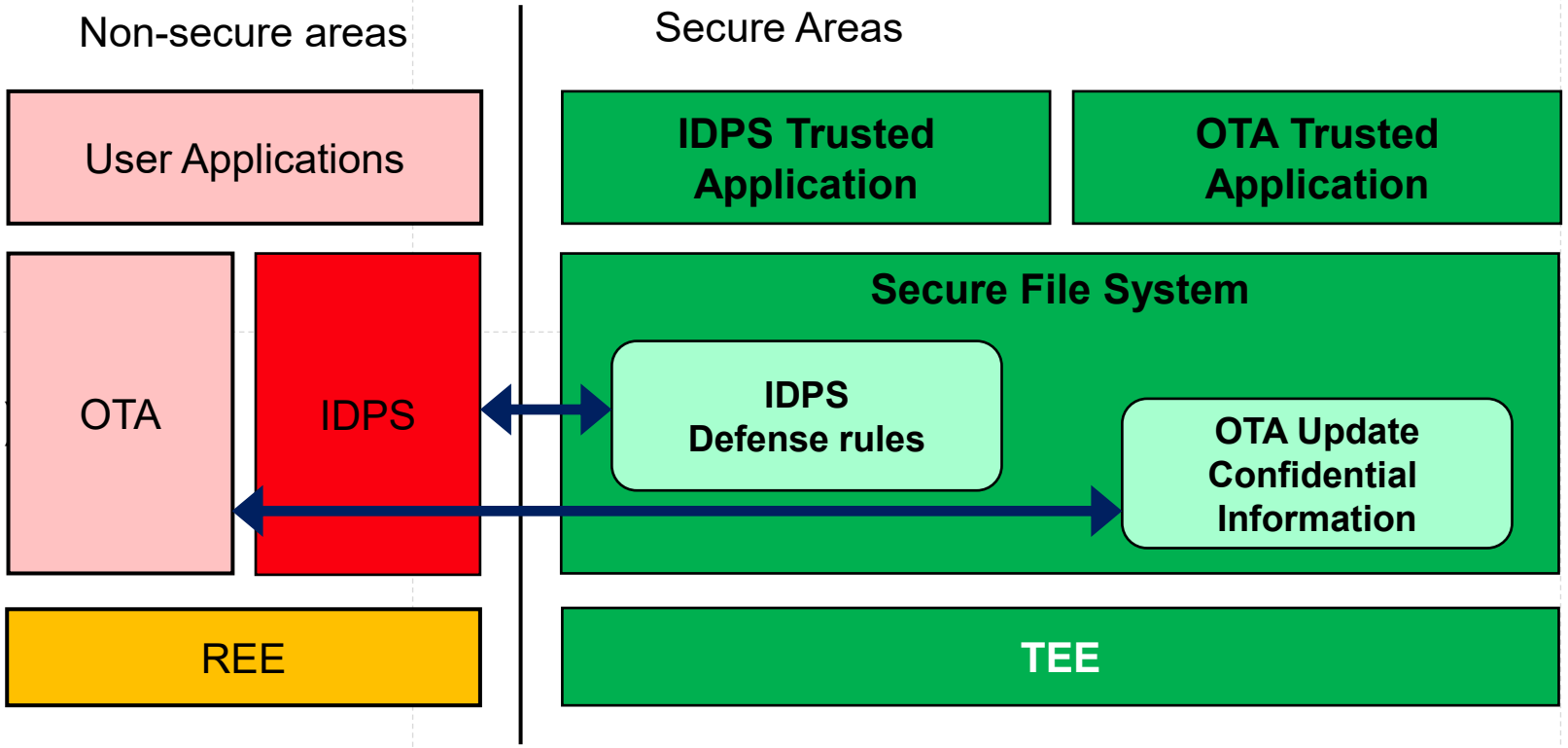
6. プラットフォーム化のビジョン (Platform Vision)

HITACHI

Draft2

◆ 転換(3)「プラットフォーム化」の具体像 — TEEを中核にした統合アーキテクチャ
(Transformation (3) Concrete image of "platformization“ - Integrated architecture with TEE at its core)

- さらなる要素技術を統合
(Integrate more elemental technologies)
  - ✓ OTA
  - ✓ セキュア通信
(Secure communication)
  - ✓ 運用（ログ・鍵管理）
(Operation (Log & Key Management))



7. まとめ (Conclusion)

HITACHI

Draft2

◆ ***問い：個別最適から全体最適へ — SDVのセキュリティは共通基盤として設計できるか？***
(Question: From individual to holistic – Can SDV security be designed as a common foundation?)

①実績：IDPS × TEE 統合を実装済　(Achievements: Implemented IDPS × TEE integration)

- ✓ 「守る側を守る」設計転換を実証し、TEEが信頼の基盤となり得ることを確認
  (Demonstrating a "Protecting the Defender" design shift and confirming that TEE can be a foundation of trust)

②答えの方向性：共通基盤として設計できる可能性がある　(Answer direction: Possibility to design as a common ground)

- ✓ TEEを中核にすれば、OTA・鍵管理・セキュア通信も同じ構造で統合できる
  (With TEE at its core, OTA, key management, and secure communication can be integrated in the same structure)
- ✓ ECU種別やクラウドを超えたEnd-to-Endの共通アーキテクチャへの展望
  (Prospects for an end-to-end common architecture that transcends ECU types and clouds)

③仕様化・標準化：効果の見極めが必要
(Specification and standardization: Determine the effect)

- ✓ 何を・どこまで統合すべきか、仕様としてどう記述すべきか
  (What and to what extent should be integrated, and how should it be described as a specification?)
- ✓ R155 / ISO/SAE 21434 への対応付けと今後のPoC検証
  (Compliance with R155 / ISO/SAE 21434 and Future PoC Verification)


HITACHI