信頼される安心を、社会へ。
SECOM

第22回情報セキュリティ・シンポジウム

スマホ時代のリスク管理
- スマホ・プラットフォームをどうトラストするか

セコム IS研究所
磯部 光平
ko-isobe@secom.co.jp

自己紹介

- 磯部 光平
- 略歴
  - 2016年 セコム IS研究所
    コミュニケーションプラットフォームDiv. 暗号・認証基盤G.
  - 2020年 セキュアオープンアーキテクチャ・エッジ基盤技術研究組合(TRASIO) 研究員
    IoT向けエッジセキュリティ研究に従事
- 研究領域
  - 暗号利用システム、デバイス管理システム、PKI

背景

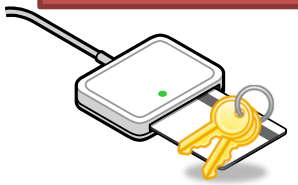
- 金融サービス提供にスマホ対応は不可欠
- サービスのアーキテクチャ・実装は大きく変動
  - ネイティブアプリ、ユーザデバイス機能の活用など
  - スマホ対応と共にリスクの所在も変化
- サービス全体の安全性の維持
  - スマホ・プラットフォームのリスクにも留意が必要
  - サービスの土台として適切か、信頼(=トラスト)できるか

アーキテクチャの比較

例：オンラインバンキング

Webサービス

ICカード認証



OS/ブラウザ

PC

スマホ向けサービス

API

- スマホに搭載されたセンサ/デバイスの活用
- 認証情報（APIトークン、生体データ)の保存先
- ユーザ対話,オフライン決済など機能

アプリ

OS/SDK

スマートフォン

生体認証/カメラ

スマホでのサービス提供の特徴

- ネイティブアプリ開発による参入
  - アプリ開発プラットフォーム(SDK,マーケット)の利用は不可欠
  - 外部API・ライブラリの活用や提供も盛んに
- プラットフォーム化された機能
  - 生体認証やカメラなど多彩な装置が汎用的に利用可能
  - プラットフォームへの依存度は上がったが、
    アプリ提供者による介入は困難に
    - OSやメーカー等が混在、ブラックボックス化

アーキテクチャの比較(リスク)

金融機関の
提供・責任範囲

例：オンラインバンキング

スマホ向けサービス

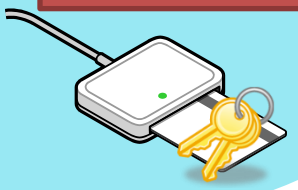
重要な要素を調達・提供

重要な要素がスマホ上に存在

Webサービス

API

ICカード認証



- スマホに搭載されたセンサ/デバイスの活用
- 認証情報（APIトークン、生体データ)の保存先
- ユーザ対話,オフライン決済など機能

OS/ブラウザ

PC

対応に限界

利用者

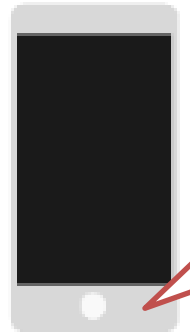
アプリ

OS/SDK

スマートフォン

生体認証/カメラ

変化するリスクのありか

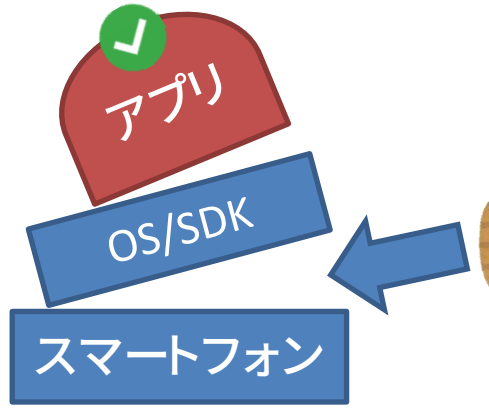


APIトークンが正当
→アクセス許可

生体認証OK→
APIトークンの使用を許可

- ユーザデバイスへの依存が増大
  - PC(Webブラウザ):WebサービスのI/Fが主
  - スマホ(アプリ):
    認証など重要なロジック, データをデバイス側に保存・実行
    生体認証機能等はプラットフォーム・SDKを用いて呼び出し

- デバイスが持つリスク
  - サービス提供者が開発しない(=外部)箇所のリスク
  - プラットフォームに存在するため、
    サービス提供者からは認識・対処しづらい
    - APIを呼び出した先はブラックボックス



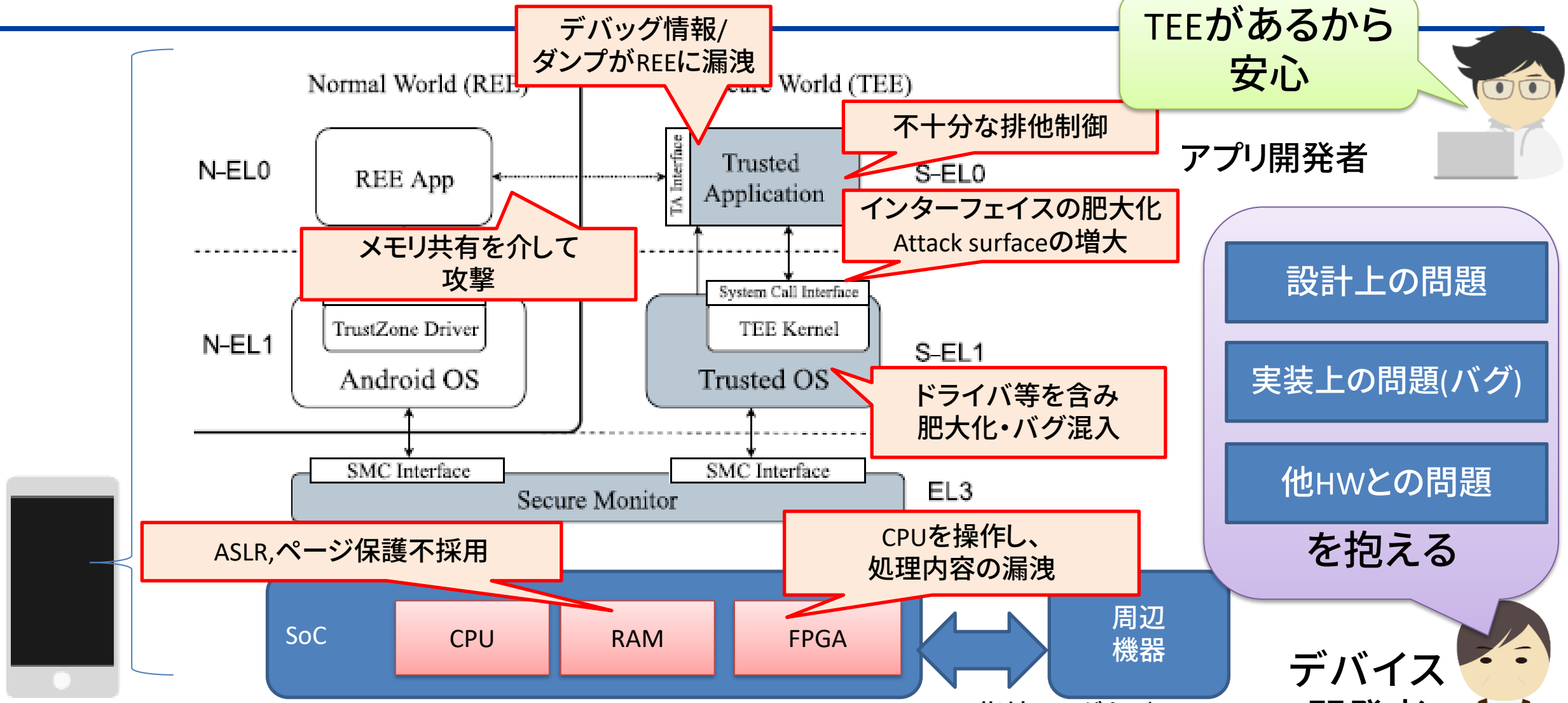
外部リスク管理のハードル

- 対象となる範囲・コンポーネントの増大
  - ハードウェア・ソフトウェア両面にまたがる
    - OS、ハードウェア、各種センサ・デバイス・・・
  - メーカー、プラットフォームも多数市場に存在・流通
  - セキュリティ機能も複数の実装形態が存在
- 必ずしも低減できるリスクとは限らない
  - 例：TEEの脆弱性（次スライド）
  - メーカーが対応できない場合、リスクは残存する

スマートフォン等のスマート・デバイスにおけるセキュリティ：プラットフォーム化によるリスクの現状と展望
https://www.imes.boj.or.jp/research/abstracts/japanese/20-J-17.html

TEE: Trusted Execution Environment

TEEに関する脆弱性



参考および出典：
SoK: Understanding the Prevailing Security Vulnerabilities in TrustZone-assisted TEE Systems
https://www.cs.purdue.edu/homes/pfonseca/papers/sp2020-tees.pdf

リスク管理に求められる視点

信頼される安心を、社会へ。
SECOM

- 「このデバイス・プラットフォームにサービス提供してよいか」
  - サービスの展開先として信頼(トラスト)できるかどうか
  - コントロール不能な外部リスクだからこそ判断が求められる
  - 特に認証などセキュリティ上重要な機能では不可欠

- 自動化された検証・リスク評価が求められる
  - 膨大・多様なデバイスでは継続的な監視が必要な反面、
    手動でのリスク管理は難しい
  - Never Trust, Always Verify (ゼロトラストアーキテクチャ)
    暗黙的な信頼を置かず、常時必要な検証・評価を行うしくみ
  - 自動化された検証・リスク管理の下では提供するサービスの制御も可能

外部リスク管理の自動化に資する取り組み

信頼される安心を、社会へ。SECOM

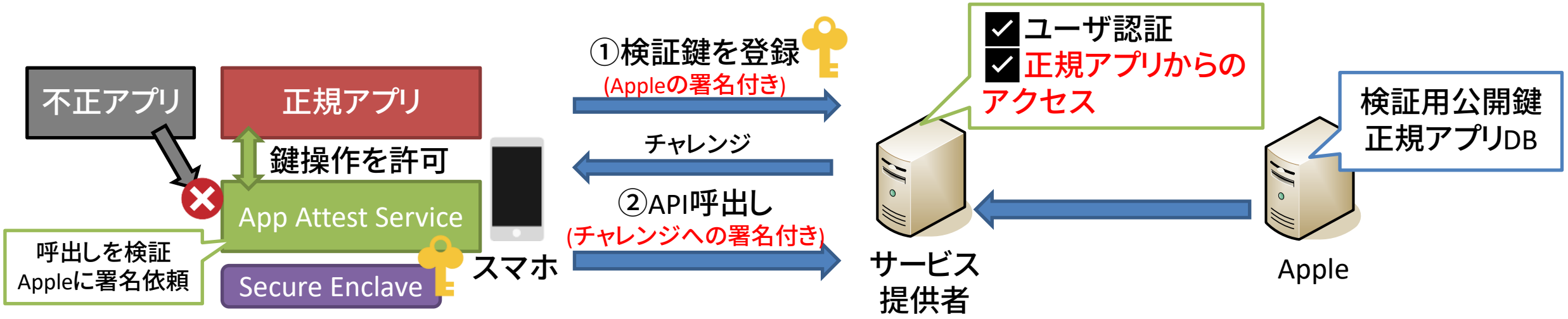
- 1. アテステーション
  - デバイス/アプリが信頼できる状況か検証する
  - Apple App Attest
- 2. オープン化
  - 仕様/実装を検証可能にし信頼の判断材料を提供する
  - TRASIO
- 3. オープン標準＋アテステーション
  - IETF RATS

1. アテステーション Attestation

- システムやデバイス構成が意図した状態であるか検証する
  - セキュアブート等で安全な状態をあらかじめ構築しておく
  - システムが生成した電子署名の検証等から正常な状態であるか確認
- リモートアテステーション
  - アテステーションを遠隔で実施する
  - サービス提供時にデバイスの信頼可否を判断できる

アテステーションの実装

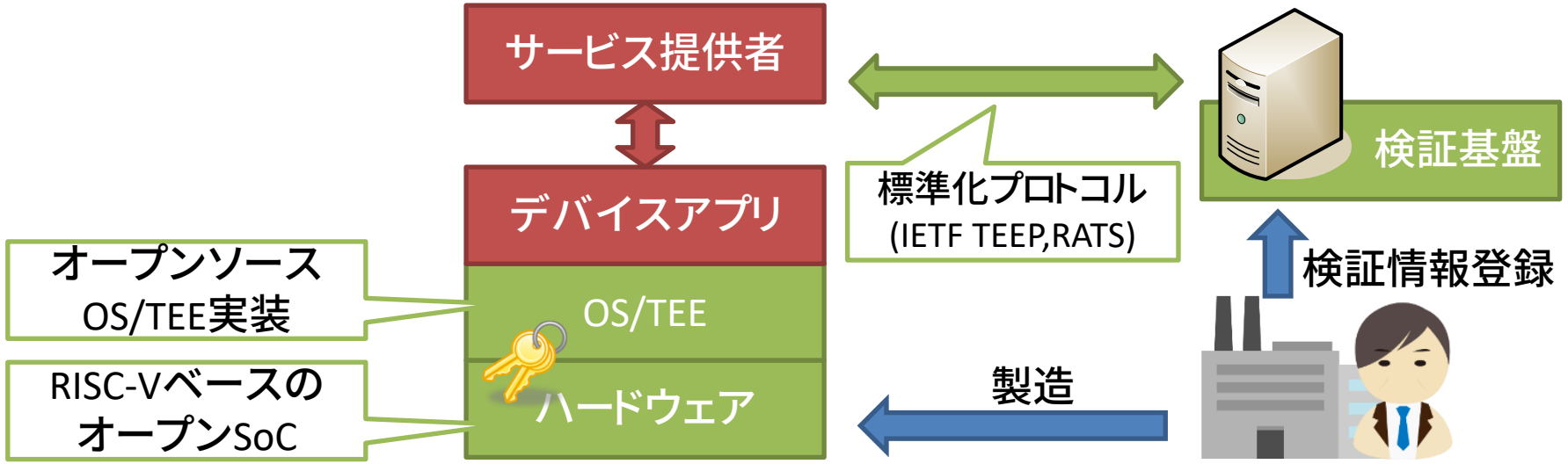
- Apple App Attest
  - 正規のアプリからのAPIリクエストであることを検証



- 他プラットフォームでも同様の取り組み
  - Android SafetyNet Attestation
    デバイスの改造の有無(セキュアブート等の状況)を検証
  - FIDO Metadata Service
    FIDO認証器の正当性検証に必要な情報を配信

2. オープン化

- TRASIO(セキュアオープンアーキテクチャ基盤技術研究組合)
  - IoTを主対象にオープン技術で構成された、セキュリティスタックの研究開発を推進
  - 第三者から検証可能な構成
    - 設計・実装のブラックボックスを低減し、検証可能箇所を増やす
    - アテステーションにより機器やサプライチェーンの検証を可能に



3. オープン+アテステーション

- IETF RATS(Remote Attestation procedureS) WG
  - アテステーションプロトコルやフォーマットの標準化
  - 複数のプラットフォームでの統一プロトコルを企図

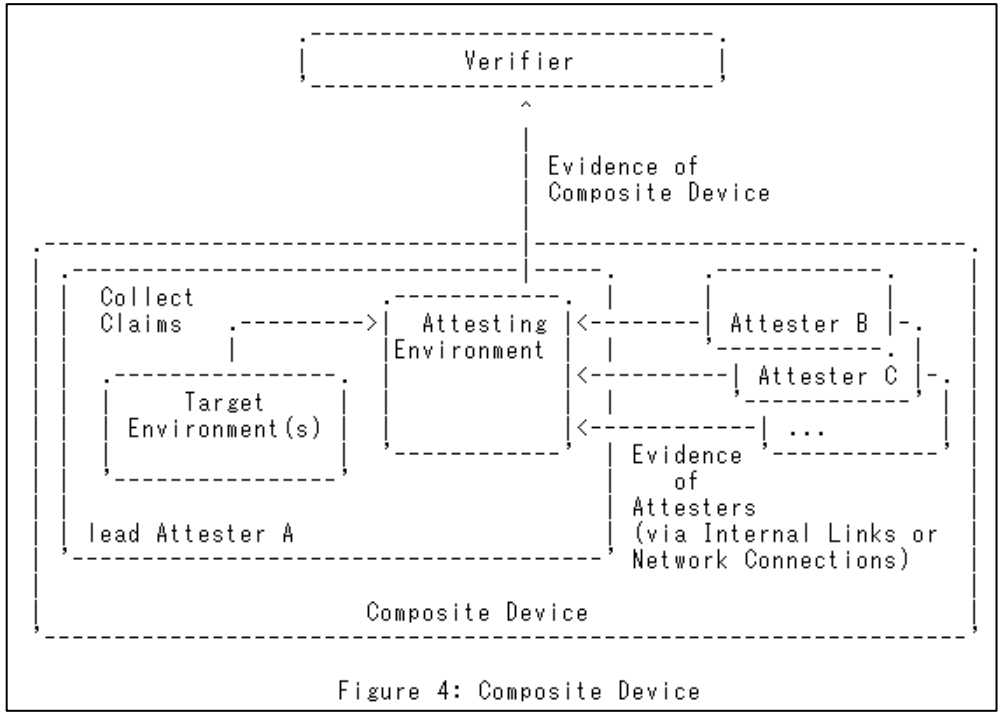
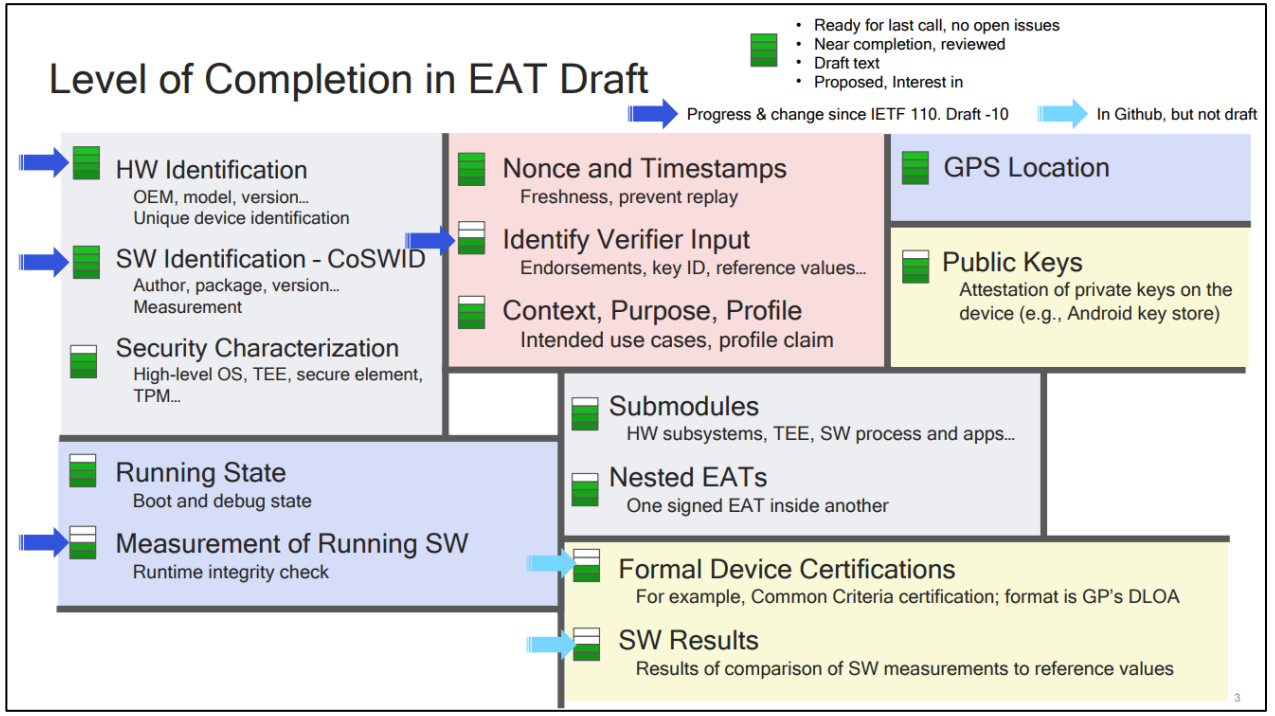
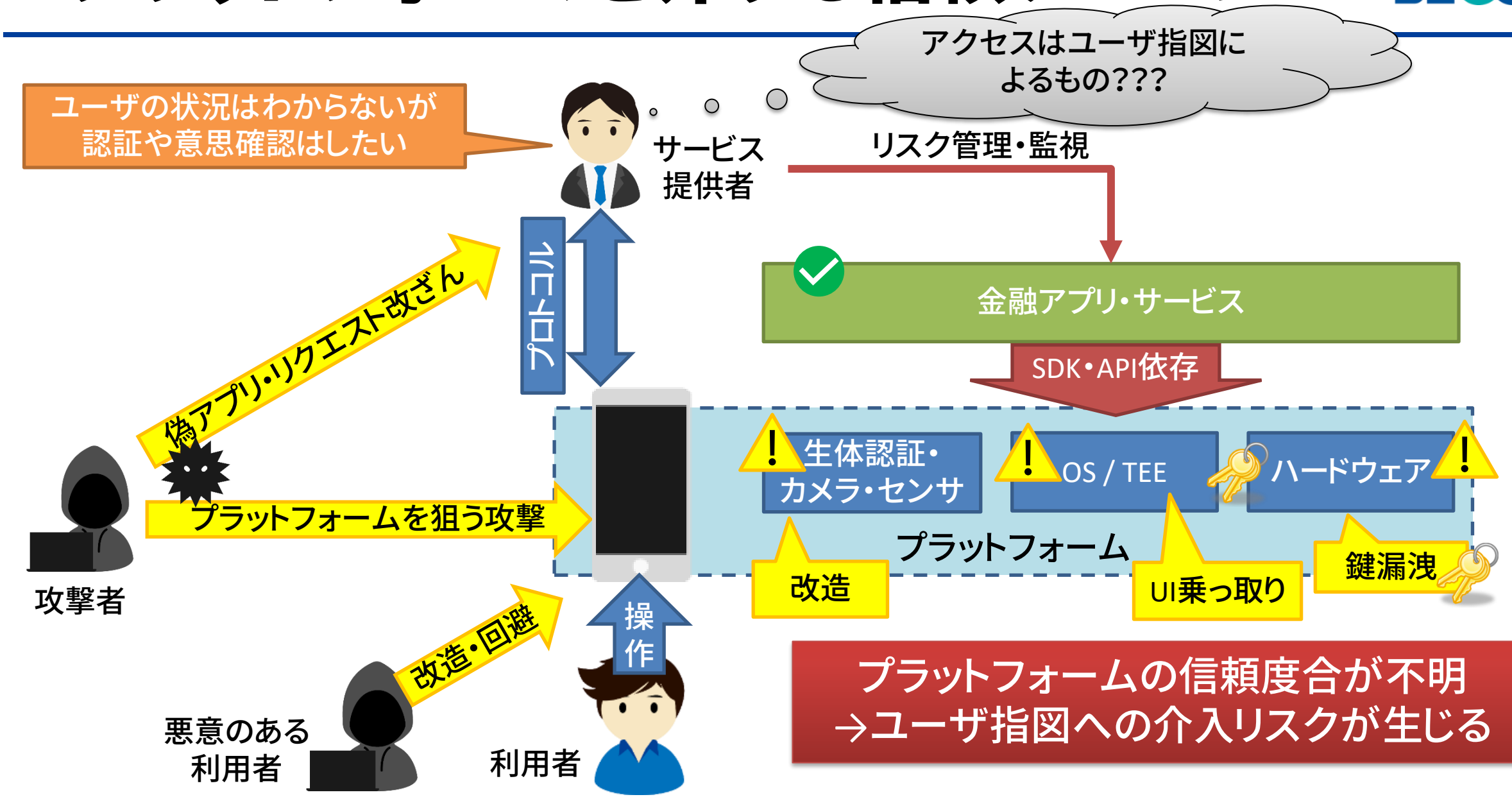


Figure 4: Composite Device



https://datatracker.ietf.org/doc/html/draft-ietf-rats-architecture-12
https://datatracker.ietf.org/meeting/111/materials/slides-111-rats-sessb-rats-session-1-slide-bundle-00

プラットフォームを介する信頼チェーン



プラットフォームを介する信頼チェーン

信頼される安心を、社会へ。
SECOM

プラットフォームが信頼できる
→プラットフォーム上でなされる操作も信頼できる

ユーザの状況はわからないが
認証や意思確認はしたい

サービス
提供者

検証機能・情報提供

リスク管理・監視

検証不可・失敗を拒否

プロトコル

検証プロトコル

金融アプリ・サービス

SDK・API依存

信頼

偽アプリ・リクエスト改ざん

攻撃者

プラットフォームを狙う攻撃

プラットフォーム改ざんを検出

生体認証・
カメラ・センサ

OS / TEE

ハードウェア

プラットフォーム

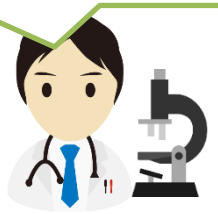
操作

改造・回避

悪意のある
利用者

利用者

第三者評価可能な
オープンプラットフォーム



アテステーション機能・
情報提供

検証鍵
脆弱性情報

まとめ

- スマホ時代は、リスクのありかが変化
  - サービスの展開先となるデバイスの影響度が増大
  - 外部リスクであり、コントロールには難しい面も
  - サービス提供先のデバイスやプラットフォームが信頼できるか
- 外部リスクの管理
  - 自動化された仕組みによるリスク管理・サービス制御
    - アテステーション、オープン化
    - 信頼の維持・検証コストの効率化
  - サービス開発・展開時に限らず、プラットフォーム動向の注視、リスク判断の見直しが必要
- 最適解は現状ない
  - 複数の取組がプラットフォーム提供者や標準化団体から提案
  - サービス提供者がすべてのコンポーネントの信頼・リスク管理する最適解は模索が続く