デジタルの日・JNSA標準化部会主催シンポジウム
「DXのためのデジタルトラスト実現に向けて」

トラスト・プラットフォーム視点からのスマートフォン
～スマホ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

©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

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

©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

プロローグ

- デジタルトランスフォーメーション
  - 爆発的に普及したスマートフォンによって
    誰もが高機能な端末を持ち歩く環境が当たり前に
  - デジタル化を可能とする背景の一つ
- DXとスマートフォン(とトラスト)
  - (デジタル)サービスと人の間をとりなすデバイス
    - サービス提供者はスマートフォンへの提供を念頭に
      サービスの設計・開発を行う
  - トラストなDXとスマートフォンの関係

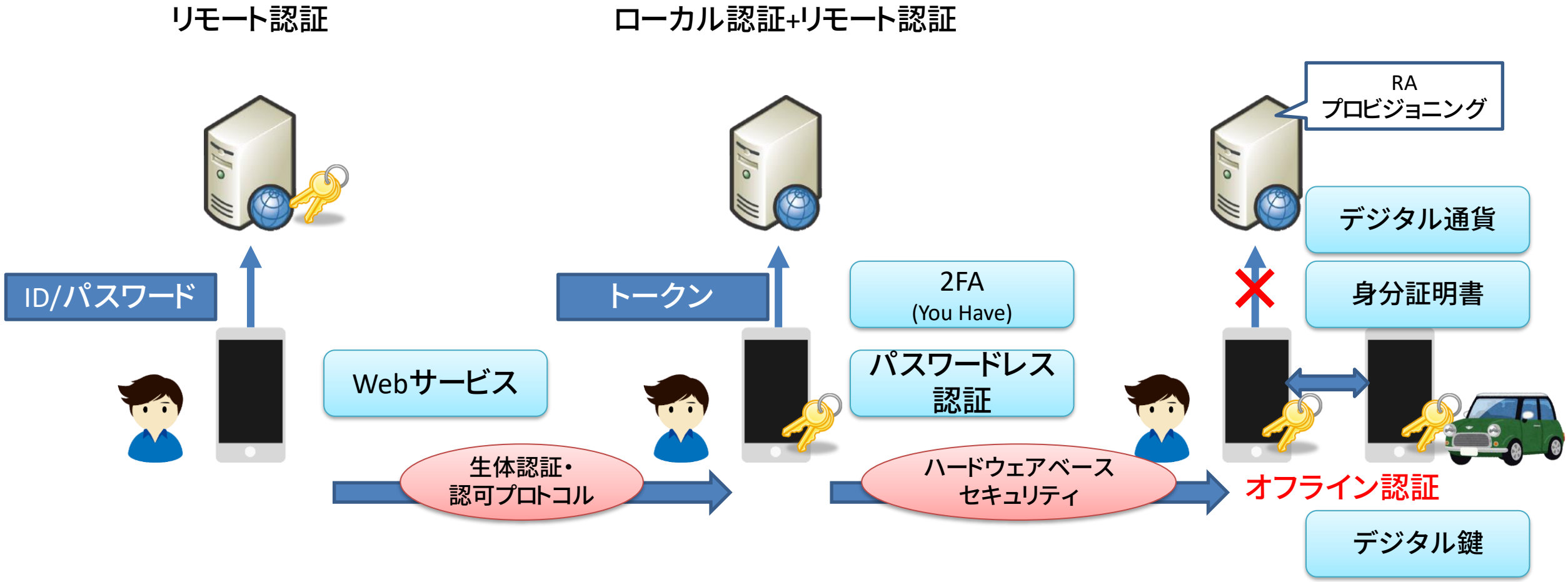
©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

スマートフォンとサービス

- 当初のスマートフォン
  - PCのサイトが見れるケータイ?
  - アプリ・デバイスが爆発的に増加
- スマートフォンの進化
  - ハードウェア・ソフトウェア・エコシステムの変化
    - ネイティブアプリ、生体認証、センサ等デバイスを活用したアプリ
  - あらゆるサービスをスマートフォンに取り込む
    - 会員証、IoT・家電等の操作、決済・・・

©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

スマホにおける認証の変遷



©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

高い安全性を要求するサービスの実装

- CBDC(デジタル通貨)
  - 法定通貨をデジタル化し、スマートフォンで
    取り扱えるようにするもの
    ネットワークに接続が出来ない場合、エンドユーザーがオフライン決済を行えるよう、何らかの能 力を有するべきである。
- デジタルID
  - EU Digital Identity Wallet(EDIW)
    eIDをスマートフォンに取り込み、オンライン/オフラインで利用可能に
    All European Digital Identity Wallets should allow users to electronically identify and authenticate online and offline across borders for accessing a wide range of public and private services.
- デジタル鍵
  - Car Connectivity Consortium
    - 車両と直接無線通信し、開錠・エンジン始動を行う
    - トロンボーンモデル(メーカーのクラウドなどオンラインサービスの仲介を受ける)ではない

©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

サービス提供者から見たスマホ

信頼される安心を、社会へ。
SECOM

- リスク
  - マルウェア・偽アプリ等の存在
  - Root化・脱獄等の改造行為
    - サービス利用者が攻撃者になりうる
- 期待
  - アップデートが容易
    - サービスの変化に追従しやすい
  - 生体認証・カメラ・センサ等が利用可能
    - 個々のデバイスに依存せず、プラットフォームSDK/APIを通じて汎用的に活用できる

©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

トラストの重要性

- これまで:スマートフォンはオンラインサービスのフロント
  - 常時通信可能を前提に、Webサービスなどの展開が進んだ
  - 不正利用やトラブルの際にはオンラインサービス側で停止・失効できた
    - バーコード決済はこのモデルに近い

- これから:オフラインでも使える高機能なエッジデバイス
  - オフラインで使うサービスの取り込み
    - 身分証明、決済、鍵
    - スマートフォンがオフライン環境下でも認証や決済が実行できる
  - スマートフォンに搭載されたハードウェアの活用
  - スマートフォンが重要な処理・データの受け皿
    →スマートフォンそのものが信用できるプラットフォームである必要性

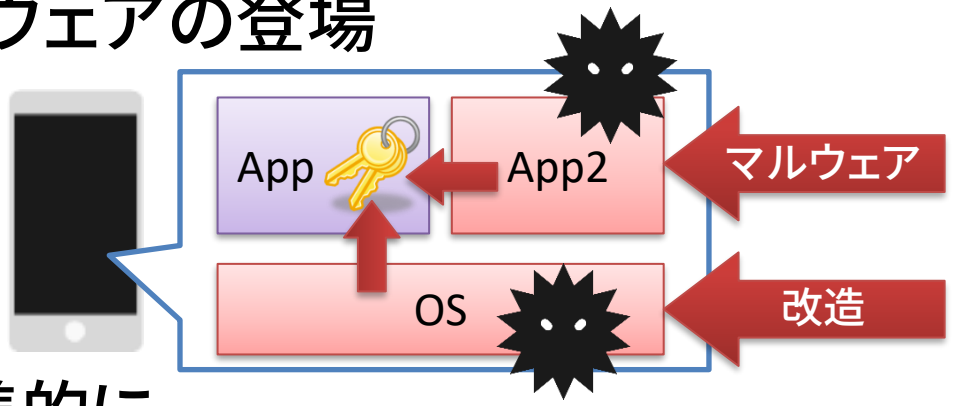
©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

信頼されるプラットフォームへの取組

©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

スマートフォンのセキュリティ対応

- 当初からスマートフォン(OS)はセキュリティ機能を具備
  - OSが提供するAPIに対するアクセス制御・ユーザへの認可要求
  - アプリ間のサンドボックス機構
  - ユーザ・アプリに対するRoot権限の無効化
- ソフトウェアでの対策の限界
  - 対応されない脆弱性などを悪用したマルウェアの登場
  - ソフトウェアへの改造行為(例:脱獄)
    改造に伴うセキュリティ機構の無効化



→ハードウェアを利用した対策の採用が標準的に

©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

ハードウェアベースのセキュリティ機能

- SE (Secure Element)
  - 従来のICカードに相当。
  - 暗号鍵などを耐タンパ性を持った領域に保護
- TEE (Trusted Execution Environment)
  - ハードウェアを利用した実行環境分離機構
  - 認証・署名などの重要なロジック・データを通常OSから分離して実行

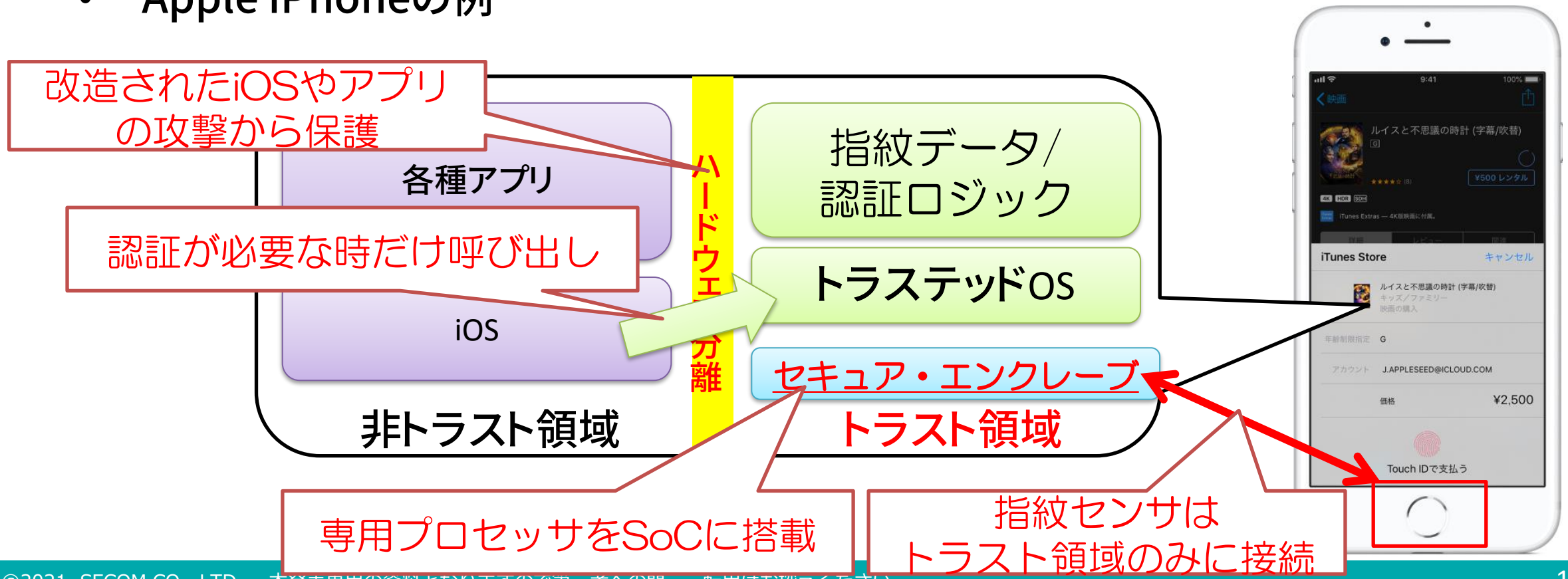
©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

Trusted Execution Environments（TEE、信頼できる実行環境）

- ハードウェアにより通常アプリと隔離されたトラスト領域
- トラスト領域：通常アプリやOSが改ざん等の侵害されても影響を受けない

決済や認証、暗号化処理等の重要な処理・データを配置し、通常アプリと連携

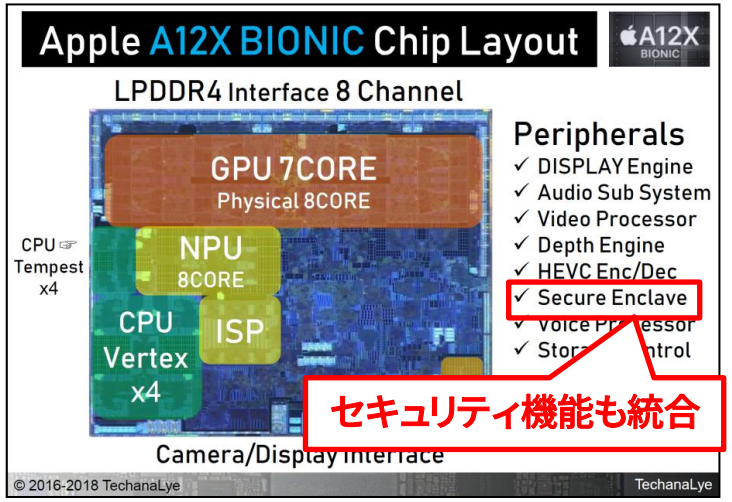
- Apple iPhoneの例

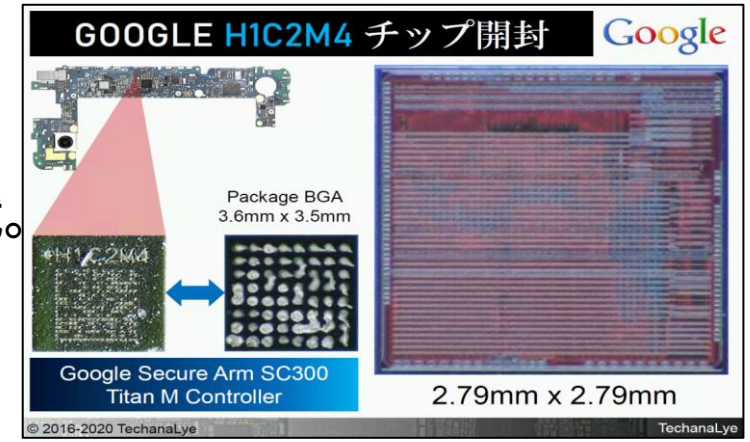


©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

実装のバリエーション

- Apple
  - Secure Enclave + sepOS
  - Touch ID等はEnclaveのみに接続して隔離
- Android
  - ARM TrustZone + Trusted OS
    - Trusted OSはベンダごとに複数の実装が存在
  - Google Titan M
    - Google自社設計のセキュリティチップ。自社開発スマホに搭載。
  - Qualcomm Secure Processing Unit
- 対応したいリスクや提供する機能は様々
  - 各社の工夫の現れ





出典：テカナリエレポート

©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

セキュリティ機能の統合例

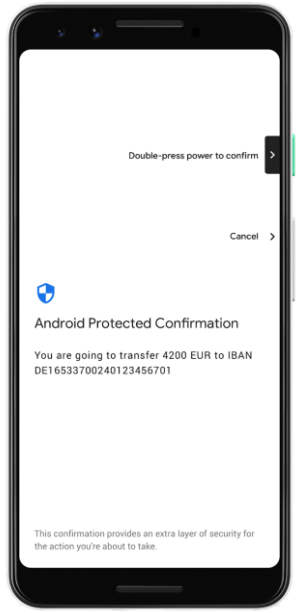
信頼される安心を、社会へ。
SECOM

- Android Keystore API
  - アプリケーションから利用可能な暗号鍵の管理機能
  - Ver.6 (2016) TEEでの鍵管理に対応
  - Ver.7 (2017) TEE対応が必須化
- Apple iOS
  - iPhone 5s(2013) Touch IDと同時にSecure Enclaveを実装
    - 生体認証の保護が当初のユースケース
  - Keychain API
    - アプリケーションから利用可能な暗号鍵管理機能
    - Secure Enclaveでの保護対象。端末のロック状態と連動可能

©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

高度なセキュリティ機能

- Android Protected Confirmation
  - TEE等によるGPU制御(Trusted UI)により、ユーザ同意をOSではなくTEE側で実行させる
  - 同意を署名付きトランザクションとして出力



- Apple Pay, Wallet
  - Secure Enclaveを中心とした隔離機構がコア
    - 生体認証やカメラ、画面制御を独立
  - 決済、鍵、身分証明書(運転免許)の取り込みなど拡張多数
    - Secure Enclaveで動作するアプリケーションをアップデートすることで拡充

©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

サービス提供者のハードル

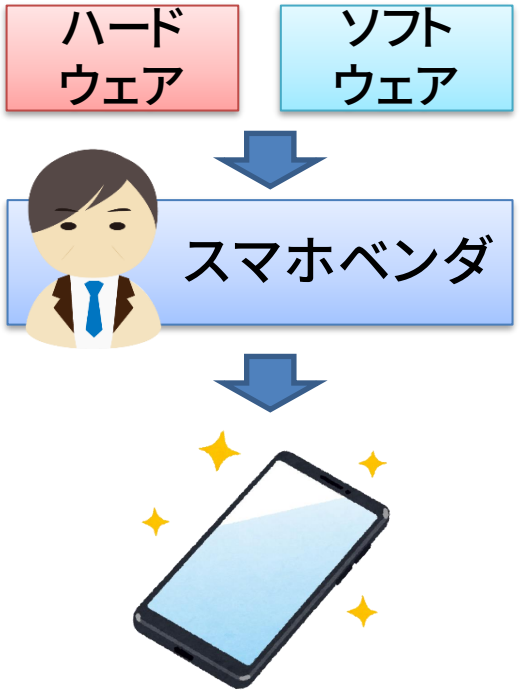
- プラットフォームのセキュリティ機能の活用
  - (前提)単一のアプリが多数のスマホで動作するのが利点
  - スマートフォンのデバイスを活用したセキュリティ機能もOSからAPIとして提供される
    →アプリの改修によって活用可能?
- サービス提供者(アプリ開発者)のハードル
  - 多様なベンダ・デバイスの存在
  - セキュリティ機能に関わる脆弱性
  - APIを中心としたプラットフォーム・エコシステム

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

©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

多様なベンダ・デバイスの存在

- プラットフォームのセキュリティ機能対応はベンダに依存
  - ハードウェアを活用する機能：ソフトウェア・ハードウェアの連携はスマートフォンベンダの役割に
  - プラットフォーム側ではベンダへ対応を要求

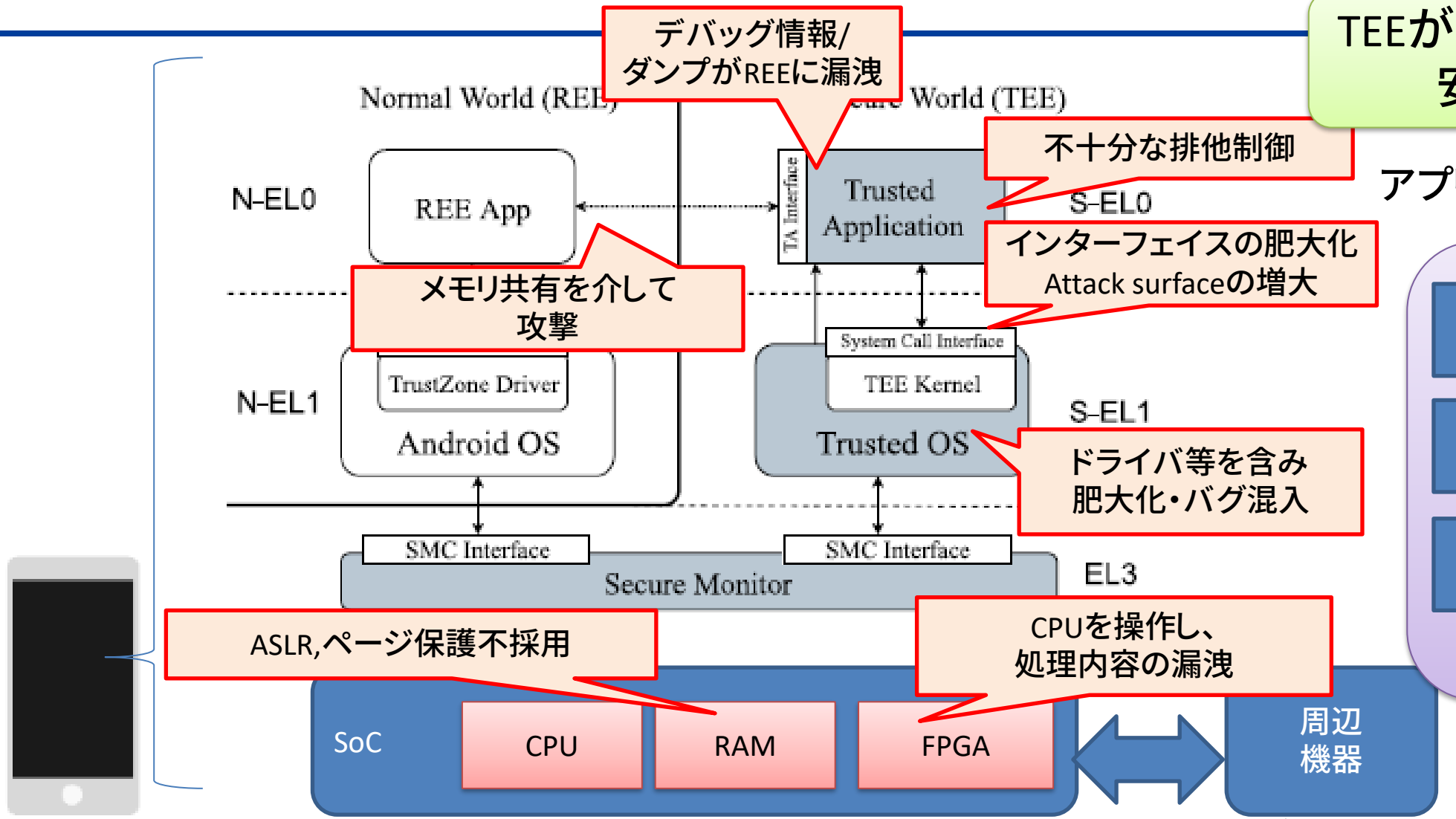


- セキュリティ機能への対応状況にバラツキ
  - 暗号化鍵管理機能に関する調査*
  - サービス開発者は事前にデバイスの内部構成まで確認することは困難

* 磯部光平, 坂本,一仁 , 葛野弘樹, "ハードウェアベース暗号鍵管理に関する日本向けAndroidプラットフォームの調査", コンピュータセキュリティシンポジウム2019論文集, pp. 1140-1147

©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

TEEに関する脆弱性



TEEがあるから
安心

アプリ開発者

設計上の問題

実装上の問題(バグ)

他HWとの問題

を抱える

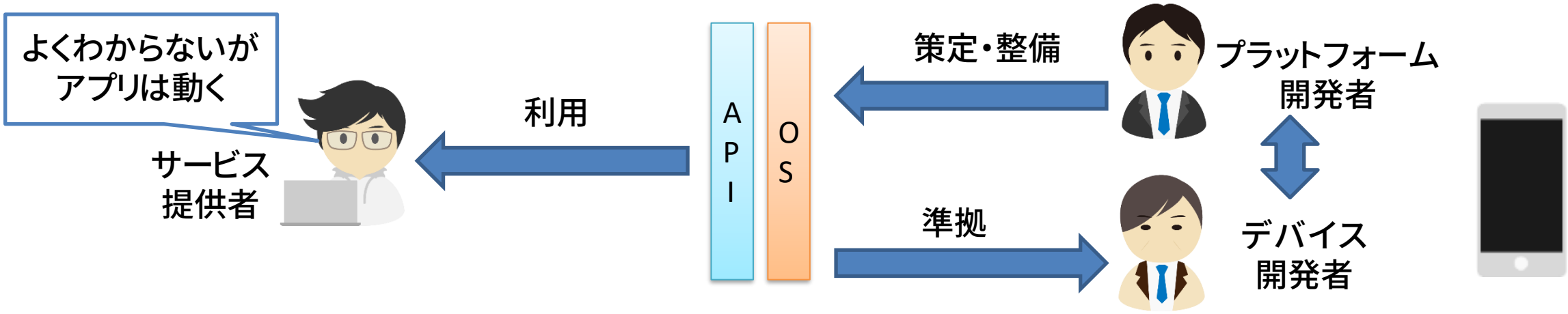
デバイス
開発者

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

©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

APIを中心とするプラットフォーム・エコシステム

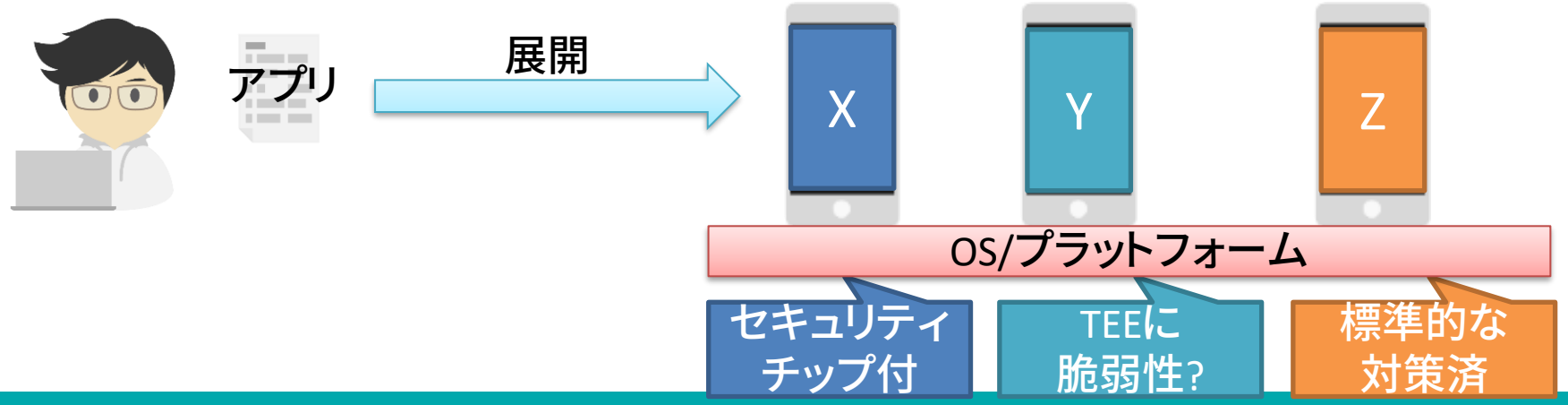
- サービス提供者の界面：OSが提供するAPI
  - 各種セキュリティ機能もAPIコールによって利用可能
  - APIコール後はOSがハードウェア機能も含め、処理を担当する
  - デバイス個別の実装に立ち入る必要がない
- サービス提供者とプラットフォーム側のコミュニケーション方法
  - 規定されたAPIを用いる/プラットフォーム側の安全策を採用することが基本
  - 提供者による独自の対策や特定のベンダ・機種に関わる問題への対処は難しい
    場合によっては、問題の発生個所すら認識できない場合もある



©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

サービス提供者から見たスマホのトラスト

- 信頼できるプラットフォームとしてスマートフォンの改良は連綿と行われている
  - ハードウェア・ソフトウェアを融合したセキュアなプラットフォームの形成
  - ベンダ・プラットフォーム提供者によってアプローチや対応状況はさまざま
- スマートフォンをトラストできるか
  - 画一的なアプリ開発が可能な反面、画一的な信頼は難しい
  - サービス提供者の立場からはブラックボックスとなっている箇所が少なくない



©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

スマホのトラストに向けた取り組み

- トラストの粒度
  - プラットフォーム全体, デバイス型式, 個別デバイス…
- 1. アテステーション
  - Never Trust, Always Verify (ゼロトラストアーキテクチャ)
  - 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
  - ブラックボックスの低減
  - 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

©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

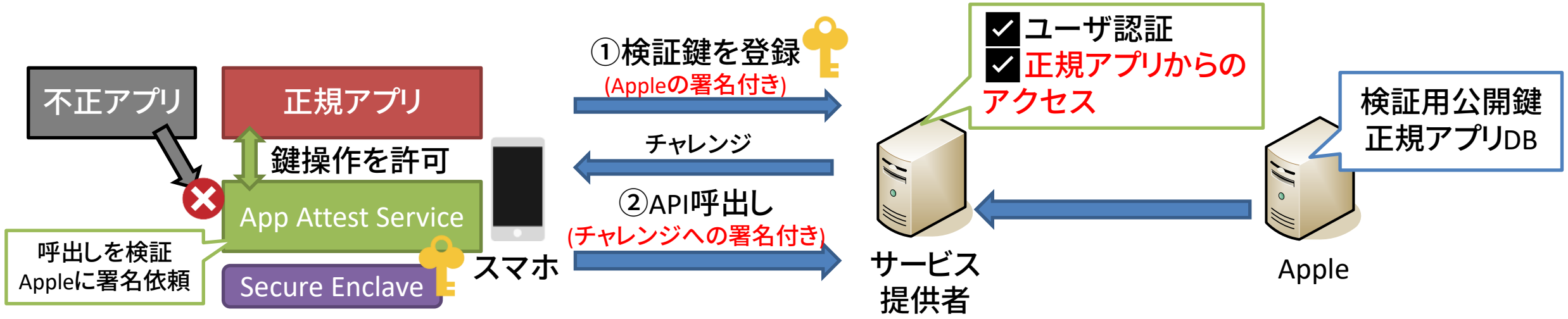
1. アテステーション Attestation

- 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
  - サービス提供時に個々のデバイスの信頼可否を判断できる

©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

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

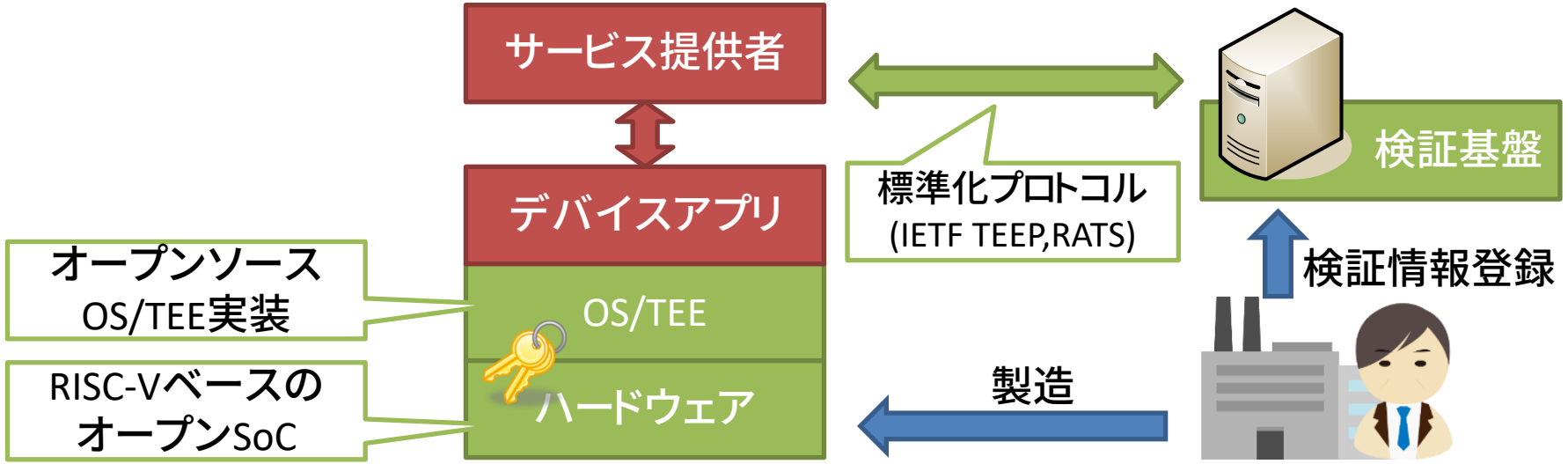


- 他プラットフォームでも同様の取り組み
  - Android SafetyNet Attestation
    デバイスの改造の有無(セキュアブート等の状況)を検証
  - FIDO Metadata Service
    FIDO認証器の正当性検証に必要な情報を配信

©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

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



http://trasio.org/home/

©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

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

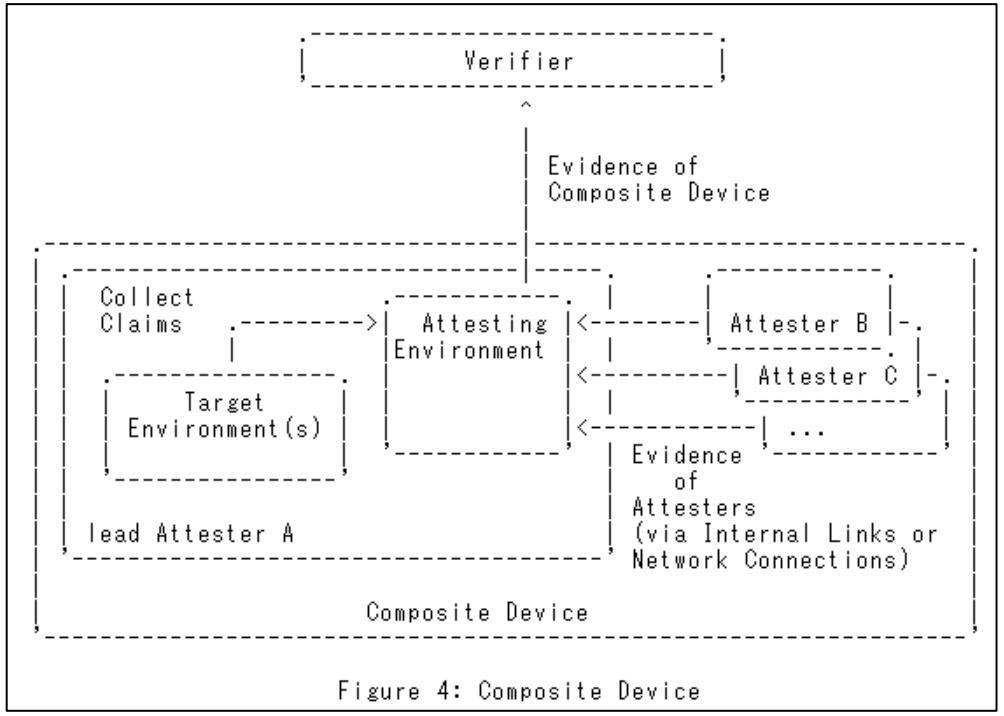
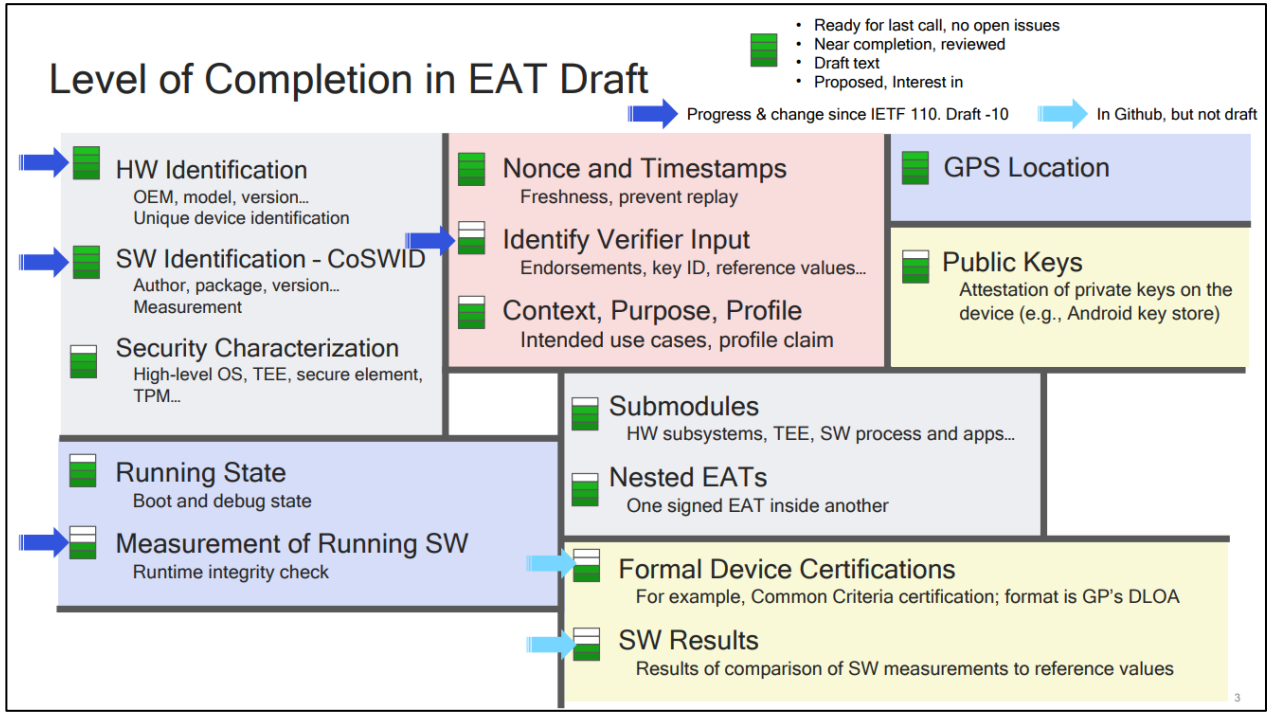


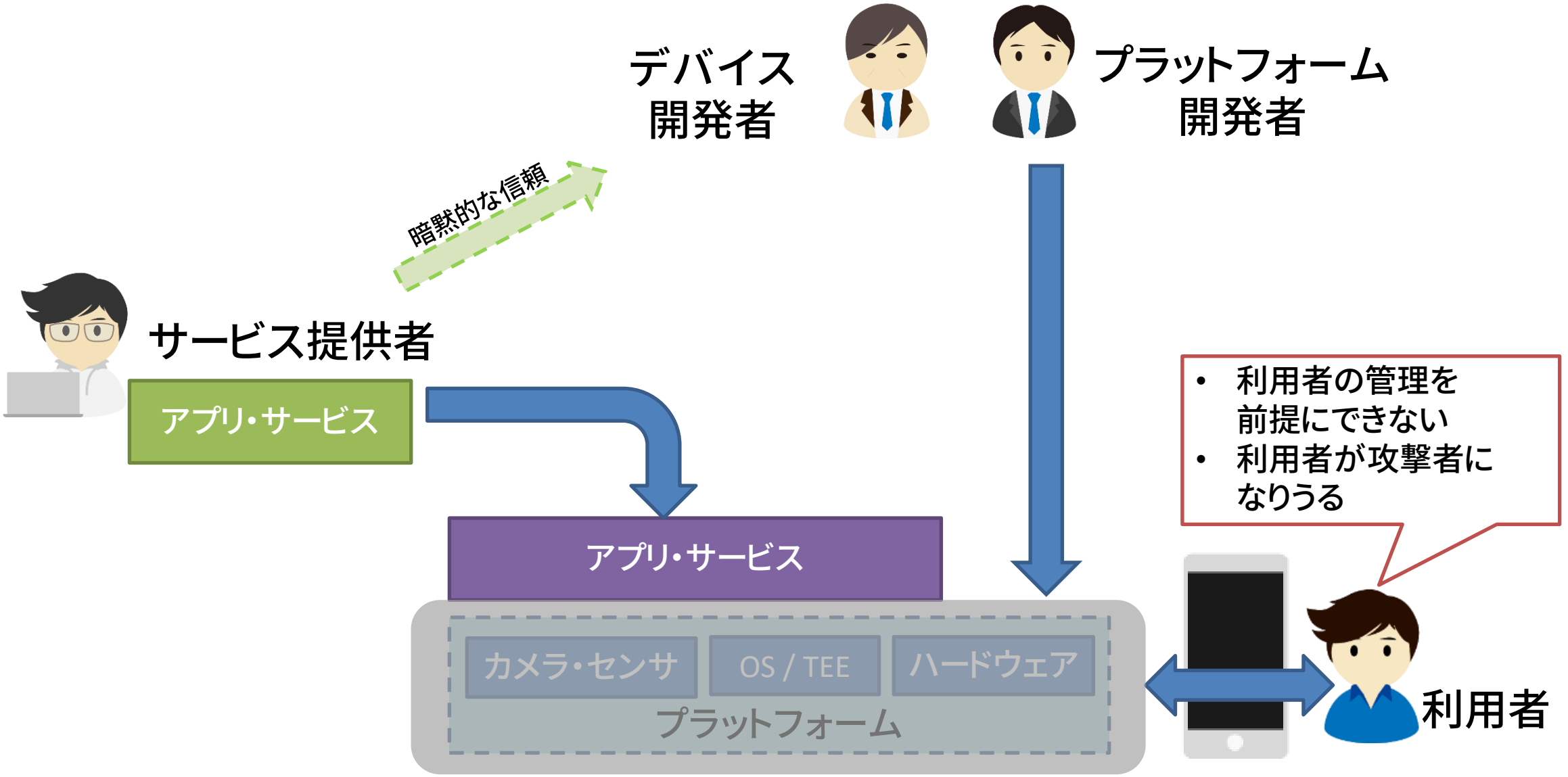
Figure 4: Composite Device



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

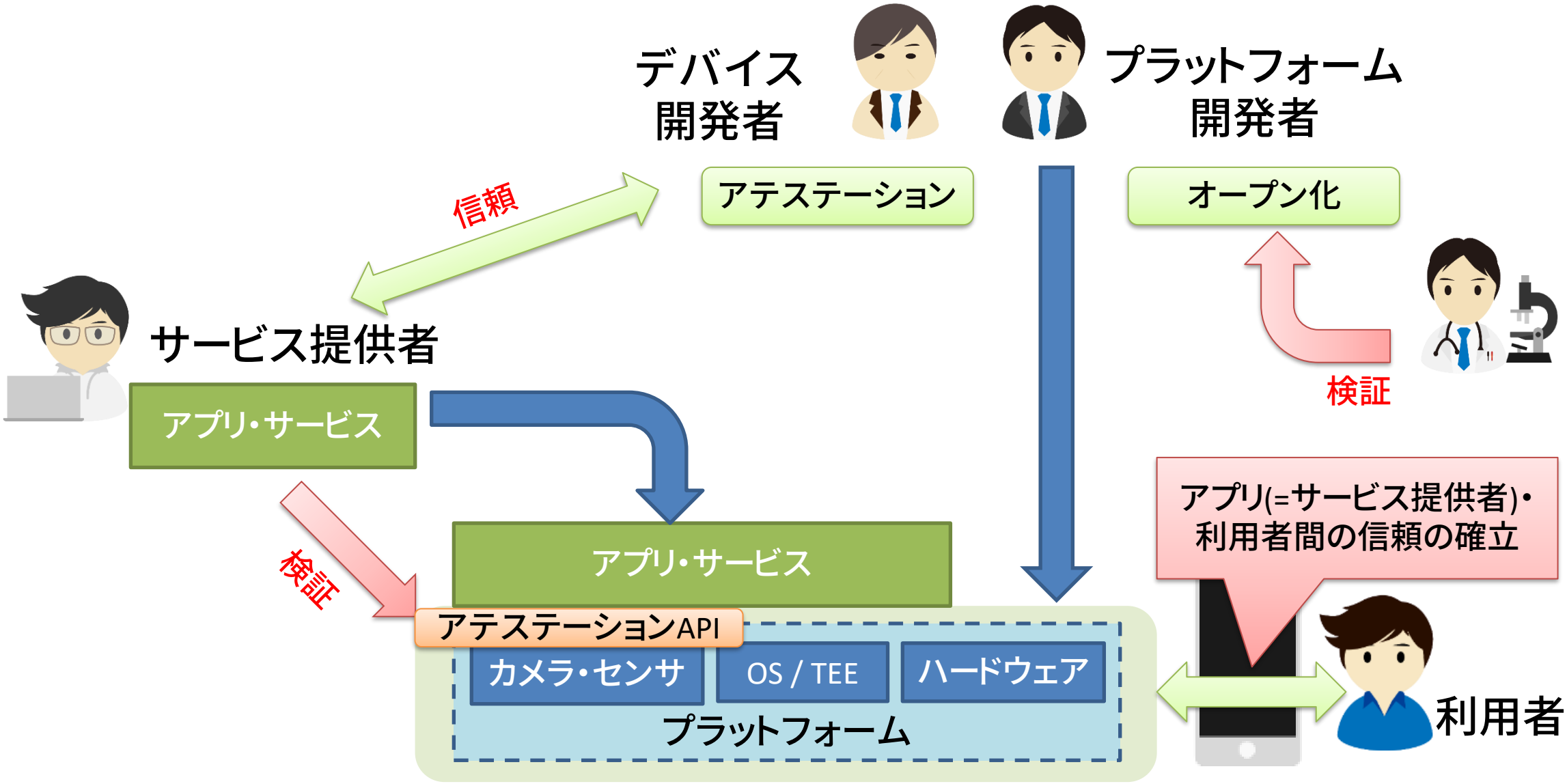
©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

スマートフォンとトラスト



©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

スマートフォンとトラスト



©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。

まとめ

- スマートフォンへのサービス提供
  - DXの推進には不可欠なプラットフォーム
  - オフライン認証・決済などスマホ自体が安全・信頼できる必要がある
- プラットフォームセキュリティ技術と活用
  - ハードウェアを活用した分離機構
    - TEE, セキュアエレメントなど。それらを活用したAPIもアプリ開発者向けに提供
  - サービス提供者の活用にはハードルがある
    - 実装・対応状況のバラツキ、ライフサイクルの長期化、セキュリティ機能の脆弱性対応等
    - ブラックボックスをどうトラストするか
- スマートフォンをトラストするための試み
  - 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
    - トラストの粒度、アテステーション、オープン化
  - サービス提供者：どうトラストするか判断が求められる

©2021 SECOM CO., LTD. 本発表専用の資料となりますので第三者への開示・転用はお控えください。