Always Verifyの実装となるリモートアテステーション

2023年8月23日

PKI相互運用技術ワーキンググループ　リーダー　松本 泰

PKI相互運用技術ワーキンググループの活動

出典: https://www.jnsa.org/mpki/index_j.html

Challenge PKI Project

The Multidomain PKI Interoperability Framework

Japanese
English

Contents

- ニュース
- はじめに
- プロジェクト
- 発表資料
- 連絡先
- パートナ

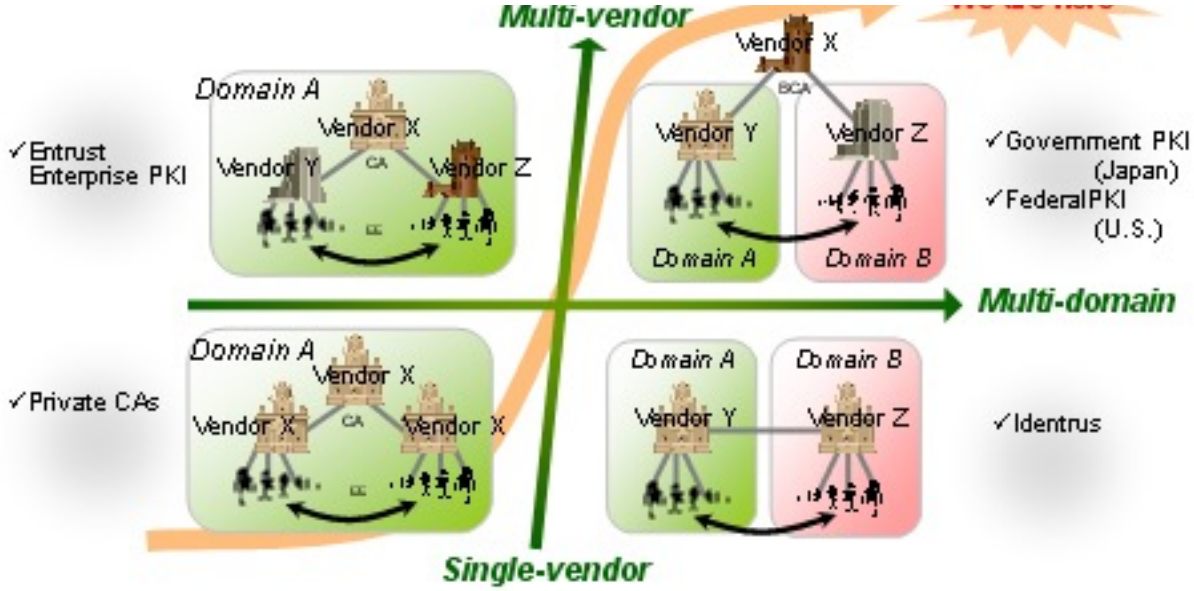
ニュース

- インターネット・ドラフト 「マルチドメインPKIの相互運用性に関するメモ」がRFC 5217として公開されました。 (2008/07) NEW!
- Challenge PKI Test Suite 2.0で利用可能な、タイムスタンプ・プロトコル(TSP)用のテストケースが公開されました。(2004/7)
- Challenge PKI Test Suite 2.0で利用可能な、GPKI、地方公共団体認証基盤(LGPKI)、公的個人認証(JPKI)に対応したテストケースが公開されまし

はじめに

各国の電子政府プロジェクトや電子商取引が活発化するなかで、PKI(Public Key Infrastructure)は 安全で安心できる電子社会を実現するための、重要な要素技術となっています。 初期のPKIは、ごく少数のベンダによって提供され、また単一の管理主体（ドメイン）の下で使われていました。 しかし昨今では、PKIを提供・利用する沢山のプレイヤーが存在し、複数のドメインが相互に接続されています。 政府認証基盤（GPKI）や、米国のFederalPKIが代表例です。 我々は、この複雑なPKIのモデルを、「マルチドメイン・マルチベンダPKI」と呼んでいます。

- 「Challenge PKIプロジェクト」は、NPO JNSAが、2001年に開始したプロジェクト
- マルチドメインPKIのための標準化活動や、テストスイートなどの開発を行なってきた。
- 「Challenge PKIプロジェクト」から20年以上経った2023年現在、マルチドメ イン・マルチステークホルダー間のトラストの 確立、及び、相互運用性の確保は、Society5.0 的課題

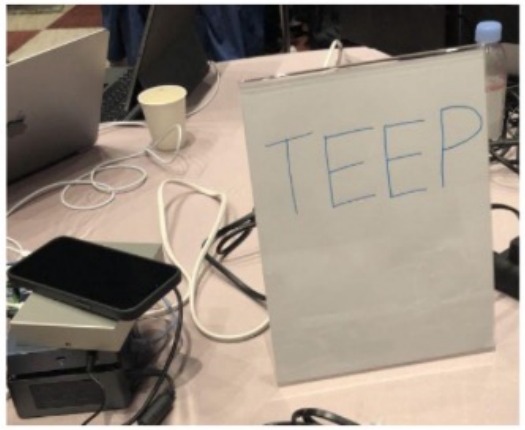


Transition of PKI models

最近の活動　2023年3月開催　IETF 116 横浜
TEEP（Trusted Execution Environment Provisioning） Hackathon

JNSA

Pictures




近年のPKIの使われ方の特徴
→　ここに関して情報共有を行っている

マシンが署名
マシンが署名検証
（人の関与が最小限）

ドキュメント以外の署名
（マシンの状態、構成への署名とか）

3

出典：https://github.com/IETF-Hackathon/ietf116-project-presentations/blob/main/ietf116-hackathon-TEEP-2023-03-26-2.pdf

最近の活動
サイバーフィジカルシステム（IoTシステム）におけるゼロトラストアーキテクチャ(*1)
そのためのプロトコルの標準化（IETF　TEEP, SUIT, RATS）

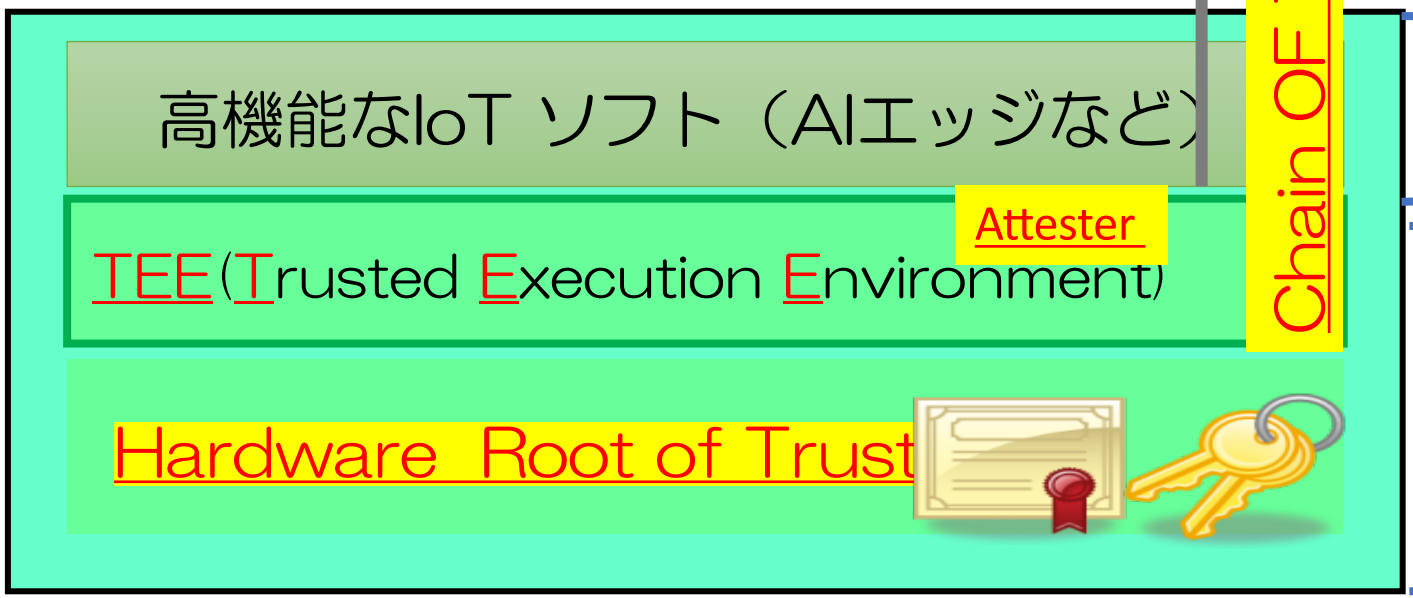
膨大な数のデバイスのリモート管理・トラスト管理

ゼロトラスト環境に置かれた膨大な数の
IoTデバイス
（サブジェクト）

Remote Attestation
（Allway verify）

Chain OF Trust

traceability
accountability
transparency



アプリケーション
セキュリティ

プラットフォーム
セキュリティ

ハードウェア
セキュリティ

不正改造

サイバー攻撃

プライバシ侵害

＊1　欧州にHorizon2020, Horizon Europeにおいては、サイバーフィジカルシステムにおけるゼロトラストアーキテクチャの適用を目指したプロジェクトが多数存在する。
参考　システムのデジタルトラスト　https://www.jst.go.jp/crds/pdf/2022/FR/CRDS-FY2022-FR-04/CRDS-FY2022-FR-04_20405.pdf

Always Verifyの実装となるリモートアテステーション

リモートアテステーションの用語の理解のために
サブジェクトのtrustworthinessという用語を導入する

JNSA

ソフトウェア
更新
新機能追加

不正改造

サイバー攻撃

プライバシ侵害

ゼロデイ
攻撃

サブジェクトの
trustworthiness

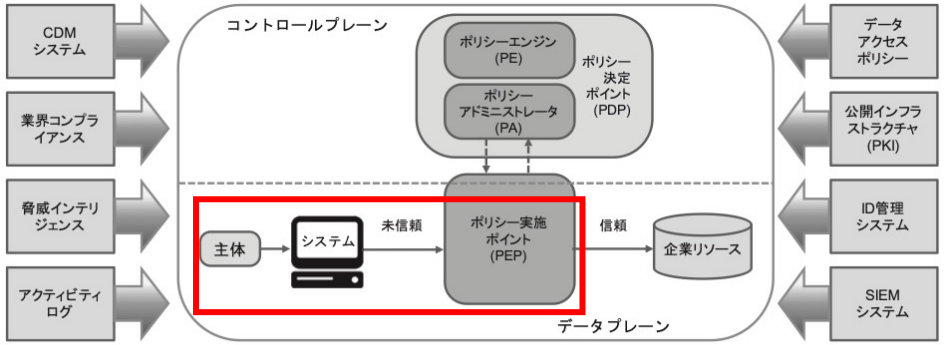
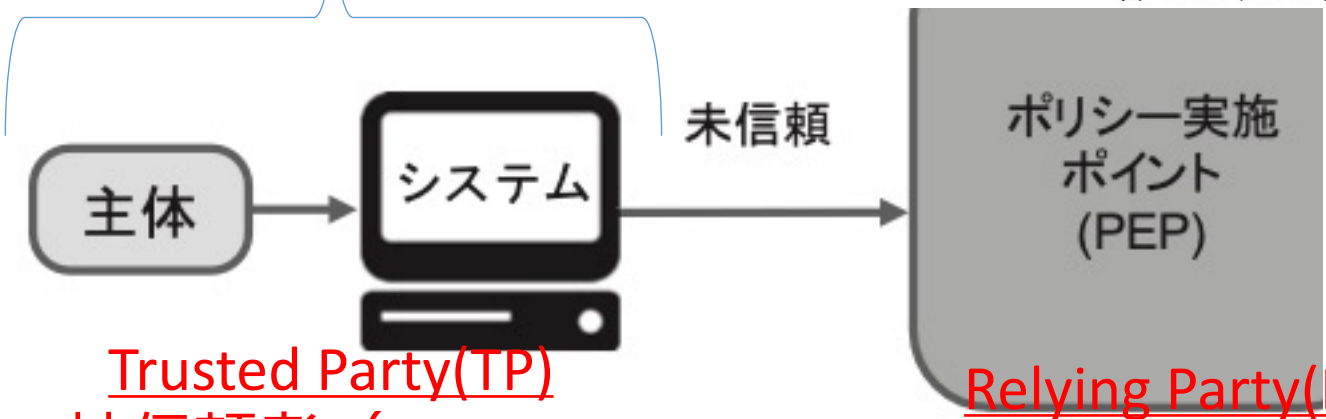


図 2: ゼロトラストの中核となる論理コンポーネント



Trusted Party(TP)
被信頼者（Trustee)

Relying Party(RP)
信頼者(Trustor)

出典：
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

サブジェクトのtrustworthinessは、変化する！！！
そのためにAlways Verifyが重要

トラストモデル　Trusted Party(TP)、Relying Party(RP)
サブジェクトの信頼性(Trustworthiness)

Trusted Party(TP)
被信頼者 Trustee

UnTrusted Network
(ZeroTrust Network)

Relying Party(RP)
信頼者 Trustor

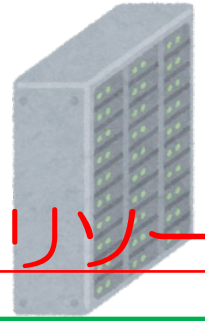
ID管理

Always Verify

Never Trust

サブジェクト

サブジェクトの
信頼性(Trustworthiness)

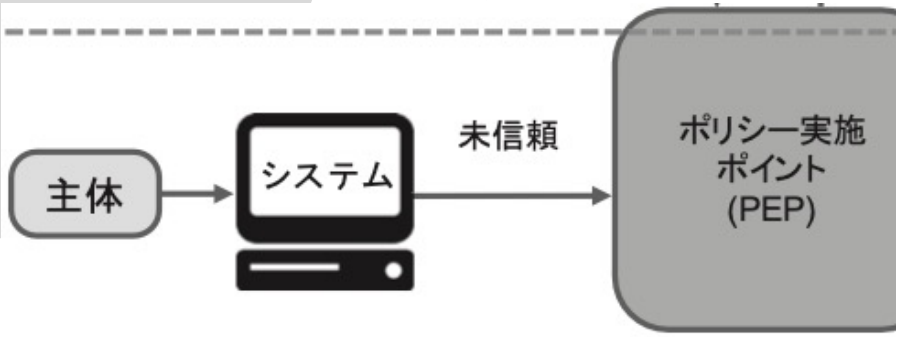


リソース

ユーザ	ユーザの確らしさ 認証の試行履歴　etc.
デバイス	デバイスの確からしさ デバイスの位置　etc.
アプリケーション	アプリケーションの確らしさ 脆弱性の有無　etc.

always verify
Trustworthinessの検証

トラストエンジン
PDP：
Policy Decision Point



Always Verifyの実装となるリモートアテステーション
リモート認証(Authentication)ではなくリモートアテステーションの要求
リモートのターゲット（サブジェクト）が「意図通り」動いているのか？

出典
https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog

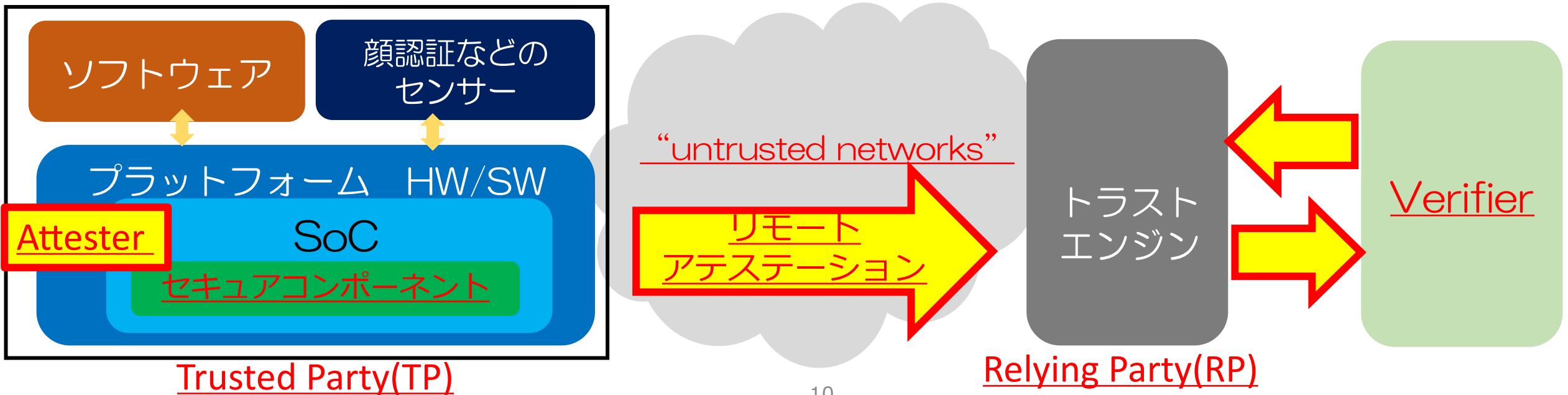
- On the Internet, Nobody Knows You're a Dog
- 「インターネットでは、実はキミが犬だって事を誰も知らないのさ」
- 1993年7月5日　米国の雑誌『The New Yorker』

２０２３年現在の課題
あんた（TP:Trusted Party）が犬でないことは分かったし、あんたが、私（RP: Relying Party）が信頼しているAさんであることも分かった。
けど、あんたのスマフォ（TP）は、大丈夫なの。乗っ取られているよみたいよ。

IETF Remote ATtestation ProcedureS (rats)WG
リモートアテステーションの標準化における用語

https://datatracker.ietf.org/wg/rats/about/

- 従来からの「デバイスの識別・認証」だけでなく、デバイス（ターゲット）の利用時における様々な信頼性（trustworthiness）の証明（アテステーション）
- ターゲットの状態などを報告するAttester という小人さん？　（署名者）
- ターゲットが意図通りの状態を保っているか判断するVerifier　（署名検証者）



リモートアテステーションにおける信頼(trust)と信頼性（trustworthiness）

出典： RFC 9334. Remote ATtestation procedureS (RATS) Architecture
https://datatracker.ietf.org/doc/html/rfc9334

- 原文
  - Amongst other things, this document is about trust and trustworthiness.
  - Trust is a choice one makes about another system.
  - Trustworthiness is a quality about the other system that can be used in making one's decision to trust it or not.
  - This is subtle difference and being familiar with the difference is crucial for using this document.
  - Additionally, the concepts of freshness and trust relationships with respect to RATS are elaborated on to enable implementers to choose appropriate solutions to compose their Remote Attestation Procedures.
- 仮訳
  - 中でも、このドキュメントはトラスト（trust）と信頼性（trustworthiness. ）について書かれています。
  - トラストとは、他のシステムに対して行う選択です。
  - 信頼性（Trustworthiness）とは、他のシステムをトラストするかどうかの判断に利用できる、他のシステムに関する品質です。
  - これは微妙な違いであり、この違いをよく理解しておくことはこのドキュメントを使う上で非常に重要です。
  - さらに、RATSに関する鮮度とトラスト関係の概念について詳しく説明し、実装者がリモートアテステーション手続きを構成するために適切なソリューションを選択できるようにする。

ターゲットの信頼性（Trustworthiness）を伝えるリモートアテステーションは Trust mechanism 。

IETF rats WG. Remote Attestation Procedures Architecture

https://datatracker.ietf.org/doc/html/rfc9334

2章. レファレンス・ユースケース. -- 7つのユースケース

今風のユースケース（デジタル社会的）

- 2.1. ネットワークエンドポイントアセスメント(Network Endpoint Assessment)
  - Attester ゼロトラスネットワークにおけるエッジデバイスなど
  - RP （Relying Party） リソース・トラストエンジン
- 2.2. 機械学習モデルの保護 → AIエッジにおける学習済み機械データの保護
- 2.3. 機密データ保護 → コンフィデンシャルコンピューティング

- 2.4. 重要インフラストラクチャ制御 → デジタルツイン・サイバーフィジカルシステム
- 2.5. TEEのプロビジョニング（ Trusted Execution Environment Provisioning)
  - IETF TEEP WG https://datatracker.ietf.org/wg/teep/about/

ここで活動中

- 2.6. ハードウェアウォッチドッグ
- 2.7. FIDO バイオメトリクス認証（ Biometric Authentication）
  - ローカル認証につかう認証デバイス（ Authenticator）の信頼性（Trustworthiness）をリモートへ伝える（アテステートする）。
    - Ex. iOS. 14. から組み込まれた WebAuthN
      - https://developer.apple.com/videos/play/wwdc2020/10670/

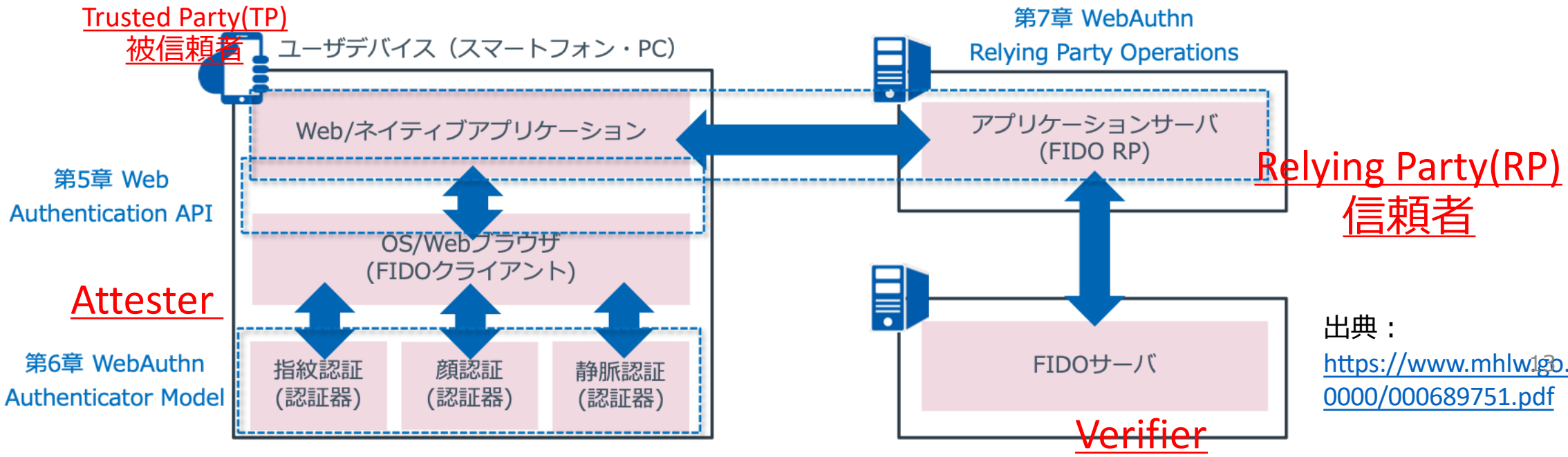
JNSA

WebAuthnではFIDOクライアントであるWebブラウザがサポートすべきAPI仕様を中心に記載されている。

ローカル認証に使用する認証デバイス（Authenticator）の信頼性（Trustworthiness）をリモートへ伝える（アテステート）

WebAuthn概要

- WebAuthnは2019年3月にWorld Wide Web Consortium(W3C)にて勧告された。
- WebAuthn仕様のうち主要項目として、FIDOクライアントがサポートすべきAPI(第5章)、認証器モデル(第6章)、RP(Relying Party、アプリケーション)側の操作(第7章)、Attestationのフォーマット仕様(第8章)が定められている。

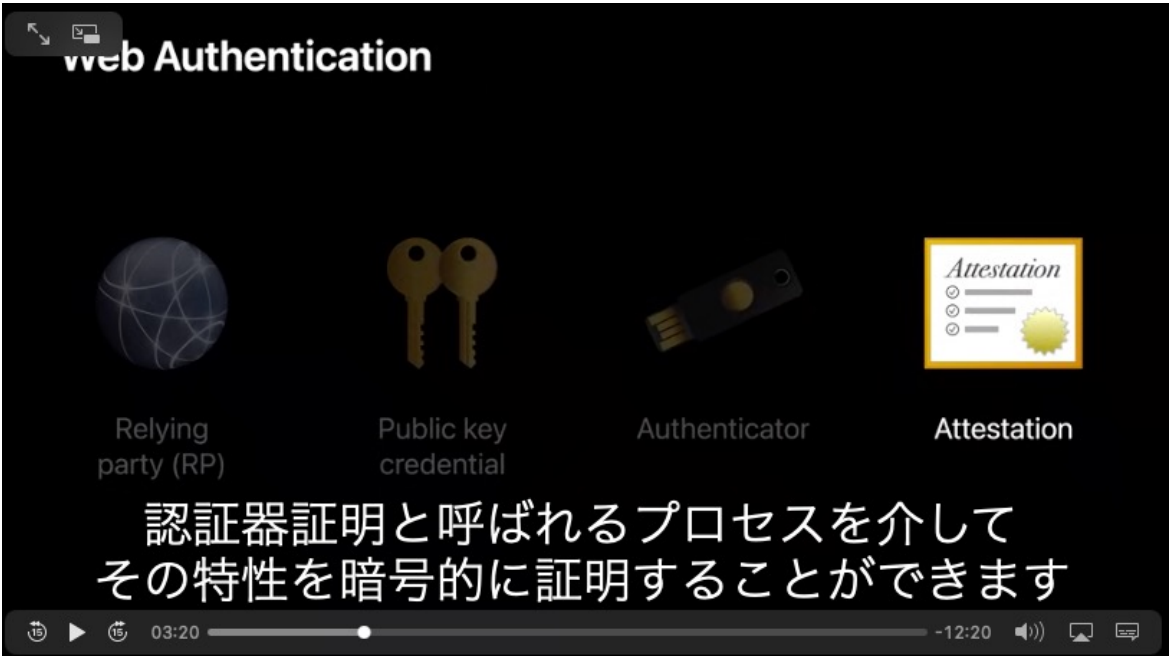


出典：
https://www.mhlw.go.jp/content/12600000/000689751.pdf

Apple のWebAuthn. -- Apple のFIDO2対応実装

出典： Meet Face ID and Touch ID for the web
https://developer.apple.com/videos/play/wwdc2020/10670/

- 「Face ID and Touch ID」は、ローカル認証
- リモートのサービスは、如何にローカル認証をトラストするのか？



3分17秒

Fourth, authenticators can, if necessary, prove their properties cryptographically via a process called attestation.

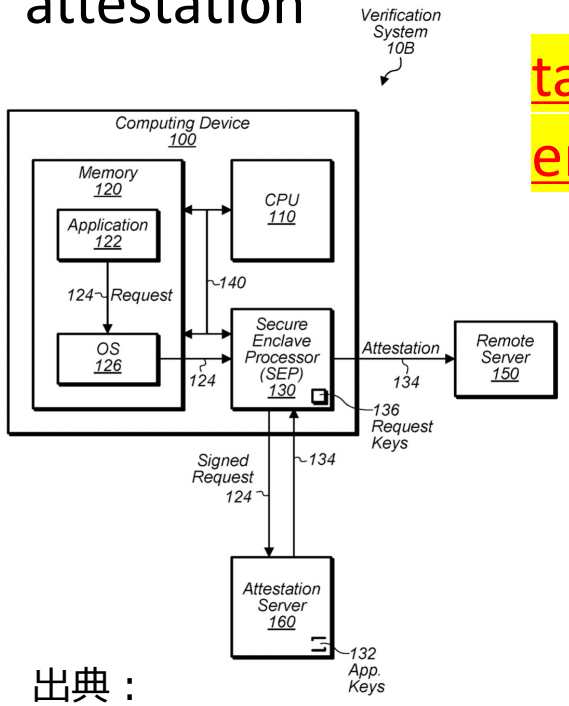
４分52秒

An authenticator like the iPhone is called a platform authenticator, because the authenticator is a feature built into the platform. There are two important properties that Apple builds into the authenticator. The first one, as we saw, is the Face ID and Touch ID, which is used to verify users' identity.
The second one is Secure Enclave, which is a processor that manages all the private keys and guarantees that they cannot leave the device.

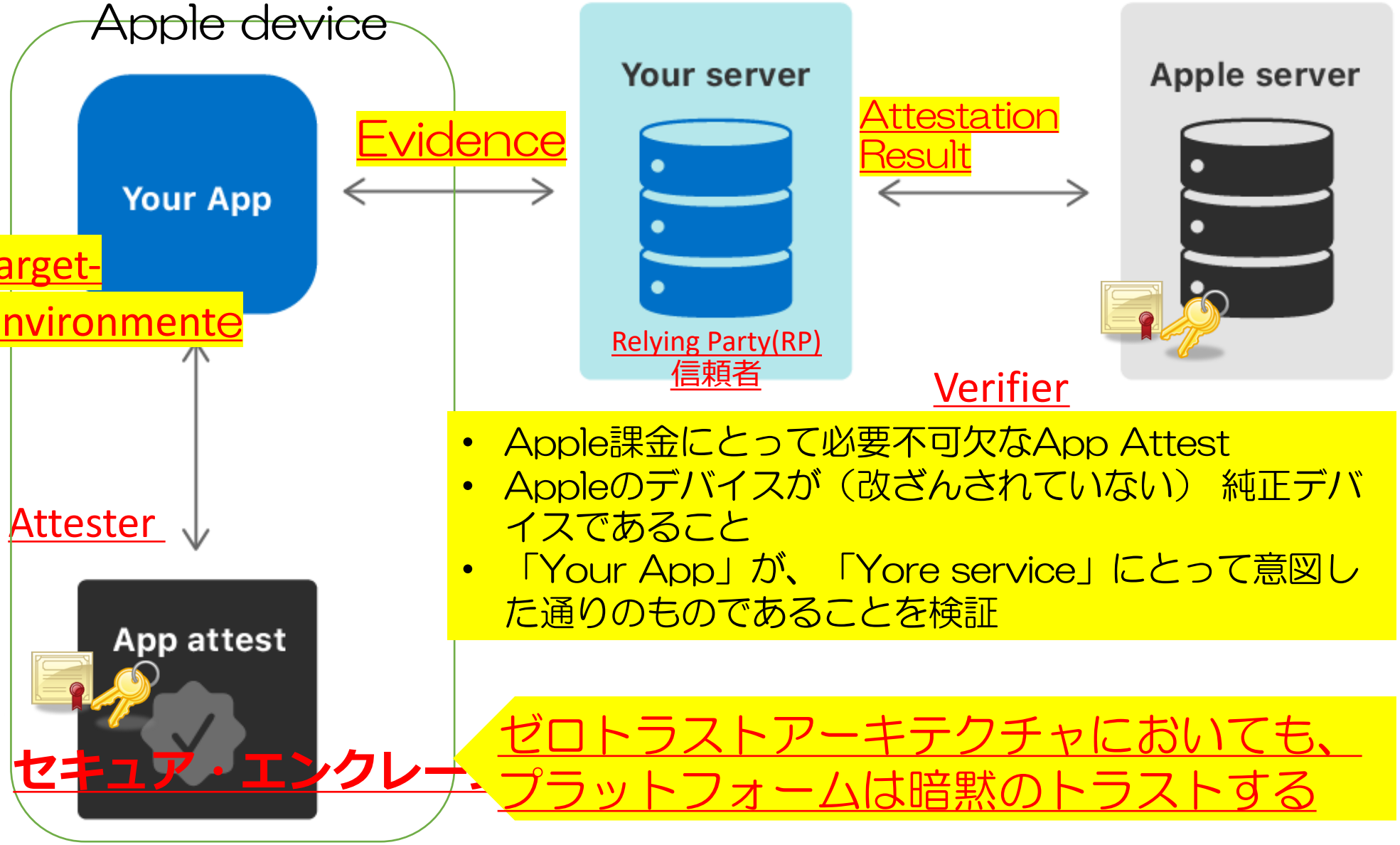
ゼロトラストにおける暗黙のトラスト　Apple のApp. Attestation

出典：　https://developer.apple.com/documentation/devicecheck/validating_apps_that_connect_to_your_server

Apple社の特許
Application integrity attestation



出典：
Application integrity attestation
https://patents.google.com/patent/US20200159966A1/



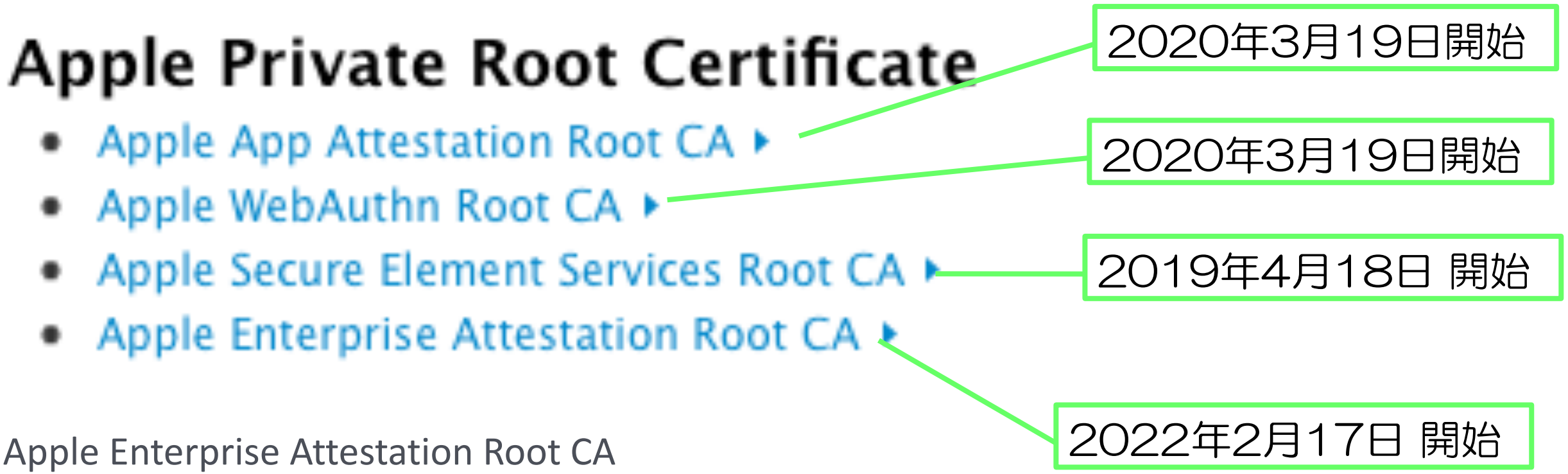
- Apple課金にとって必要不可欠なApp Attest
- Appleのデバイスが（改ざんされていない） 純正デバイスであること
- 「Your App」が、「Yore service」にとって意図した通りのものであることを検証

ゼロトラストアーキテクチャにおいても、プラットフォームは暗黙のトラストする

リモートアテステーションのためのPKI&CA（Certification Authority）認証局

Apple Private PKI

https://www.apple.com/certificateauthority/private/



Apple Enterprise Attestation Root CA
iOS 16 からサポートされた企業におけるゼロトラスト実現のために管理対象デバイスのアテステーション (Managed Device Attestation)

Always Verifyの実装となるリモートアテステーション

- ゼロトラストアーキテクチャにおいては、
  - サブジェクトの信頼性（trustworthiness)を、トラストエンジン・リソースがalways verifyすることにより明示的なトラストを得る（ explicit trust ）
  - → このalways verifyは、プロトコル的には、リモートアテステーション、プリミティブ的には、ほぼ、デジタル署名の検証
- ゼロトラストアーキテクチャにおけるalways verify ・リモートアテステーションのための「暗黙のトラスト」
  - このalways verifyでは、信頼の起点に「暗黙のトラスト」を置くことが必要になる
  - （1） プラットフォームに実装されるHW Root Of Trust、Chain Of Trustなど
  - （2） ID基盤などにおけるトラストチェーンのトラストアンカーとなる公開鍵（公開鍵証明書）
- ゼロトラストアーキテクチャは、
  - 暗黙のトラストを置くに値するプラットフォームセキュリティ技術の進化が可能にしたとも考えられる
    - → 技術的には、コンシューマ向けのスマフォが、技術（＋ビジネス）を確立させた
    - → もうひとつは、ゲーム機
  - → 現在、劇的な進化の途中。さまざまなtrustworthinessの検証が可能になりつつある。

参考

Apple課金（税）と言うビジネスモデルを支えるシステムのデジタルトラスト
Apple が作り出すエコシステム

~~不正改造~~

~~サイバー攻撃~~

~~プライバシ侵害~~

サブスクリプション・サービス

サービス
アプリ

サービス提供

サービスプロバイダー

Relying Party（RP）

Apple
デバイス

TRUST

デバイス＆アプリの
健全性の証明
attestation

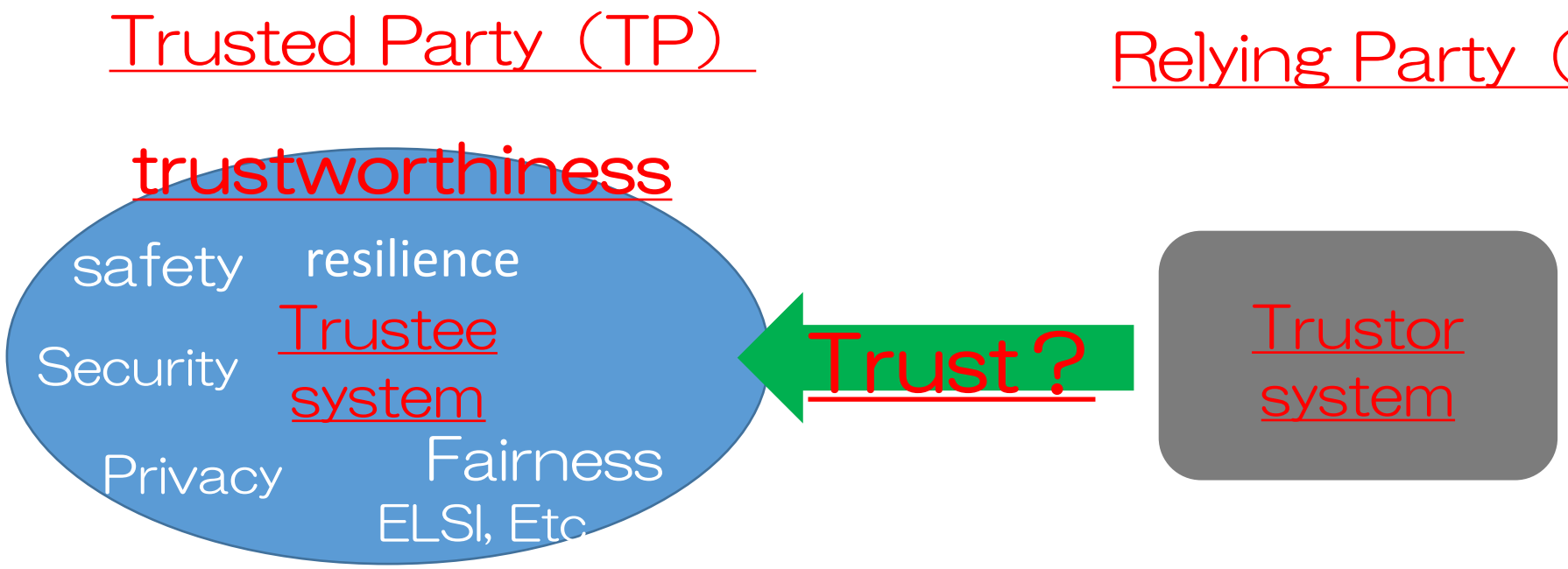
APPLE課金

- デバイスの健全性の維持
- （出荷後の）機能の拡張

デバイスの供給
（社会インフラの提供）

Apple

trustworthiness とトラストないしトラストメカニズムの関係



- Trustee（トラストの対象）は、システム
  - トラストの対象が、AIとか、膨大な数のIoTデバイスとか。
- Trustor（トラストする側）も、システム
  - → 過去からのトラスト研究の範疇外？？ → ここが変貌している？？

デジタル社会における「サイバーセキュリティ」「データプライバシー」「システムのデジタルトラスト」の関係

ソフトウェア
更新
新機能追加

System Of Systems
trustworthiness

System Of Systemsの
トラスト管理へ

Trusted Party（TP）

trustworthiness
safety
resilience
Trustee
system
Security
Privacy
Fairness
ELSI, Etc

不正改造
サイバー攻撃
プライバシ侵害

trust

明示的なトラスト
（Explicit Trust）

Relying Party（RP）

Trustor
system

ゼロデイ
攻撃

製品、サービスなどの
認証（型式認証など）

Digital Trsutwhothiness Certification

トラストサービス

trust

Trustor
system

21