変貌するトラストアーキテクチャ

エンクレーブ・TEEが作り出すSociety5.0時代のトラスト

2021年4月15日
JNSA PKI相互運用技術WGリーダ
松本　泰（セコム株式会社 IS研究所）

PKI&TRUST Days online 2021
「デジタル社会におけるトラスト」 開催趣旨

- デジタル社会におけるトラスト（デジタルトラスト）の重要性が高まっています。トラストは、過去から社会を支えている仕組みとして存在してきたと言えますが、デジタルにより大きく社会が変化する中、新たなトラストの仕組みが求められているのが現在だと考えられます。
- PKI&TRUST Days online 2021ではこうした認識の元、初日は、デジタルトラストに対応するコンピュータアーキテクチャの変化から、ゼロトラストアーキテクチャ、コンフィデンシャルコンピューティング等の「変貌するトラストアーキテクチャ」について、その仕組みを紐解いた上で技術的な方向性を議論します。
- ２日目は、デジタル社会におけるトラストの重要性が高まる中、トラストの確立に向けて大きな課題となっている法と技術の整合などの「デジタルトラストにおける法と技術のあり方」について議論します。

（デジタルトラスト・ゼロトラストの前に）トラストって何よー??

信頼される安心を、社会へ。 SECOM

- トラストについて、
  - ドイツの理論社会学者であるニクラスルーマン1968年の著作「信頼―社会的な複雑性の縮減メカニズム」の中で、古典的トラストは「社会生活の基本的な事実である。(中略)こういうこと(社会生活)が可能であるのは、我々が他者や社会に対して一定の信頼をおいているからにほかならない」
  - トラストのメカニズム → 「複雑性を縮減するメカニズム」
- トラスト自体の研究の変遷
  - 哲学 → 社会学 → 心理学(人が判断を行うメカニズム) → （デジタルトラスト???）
- 情報分野に近接する分野におけるトラストの研究　1990年台半ばから
  - Computational Trust　信用スコア??
  - Trust in Automation　人間工学の分野、人は機械をどう信頼し共同作業を行うのか？
- 最近のトラストの議論が多い情報分野
  - 人工知能分野のELSI (Ethics, Legal and Social Issues:倫理的・法的・社会的課題)、FAccT (Fairness, Accountability and Transparency)
  - 「ディープラーニング」 → なぜ、その結果を出したのか分からない。

信頼―社会的な複雑性の縮減メカニズム」
https://www.amazon.co.jp/信頼―社会的な複雑性の縮減メカニズム-ニクラス・ルーマン/dp/4326651202

基本的な用語の理解
--普遍的な概念としてのトラスト--

- Trusted party
  - 被信頼者
  - トラストされる対象者
- Relying Party(RP)
  - 信頼者・検証者
- Trustworthiness
  - 信頼者が被信頼者に期待する（信頼したい）性質？？
    - 信頼性？？（XXの信頼性）
- 「信頼性」の英語訳？？？
  - Reliability??
  - Dependability??
  - Credibility??
  - Authenticity??
  - Trustworthiness

医療の信頼(Trust)と信頼性（trustworthiness） を支える制度等
・医師資格という国家資格
・医師免許証という医師資格の証明
・医療機関の認可制度（開設許可）
その他
・医療の公平性を支える国民皆保険制度

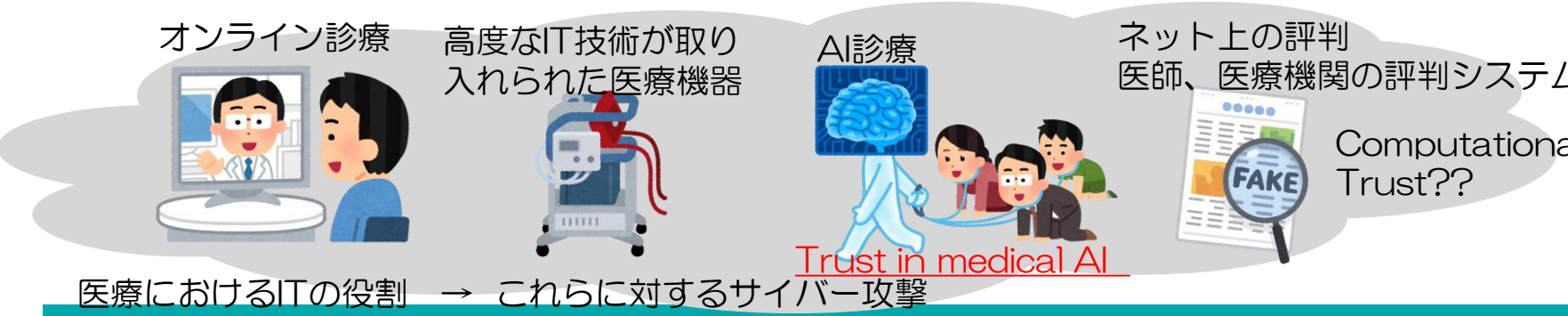
「社会的な複雑性の縮減メカニズム」がインプットされる

ニクラスルーマンの言うところの「こういうこと(社会生活)が可能であるのは、我々(Relying Party)が他者や社会(Trusted party)に対して一定の信頼をおいているからにほかならない」

「デジタル社会におけるトラスト」
従来からのトラスト「社会的な複雑性の縮減メカニズム」に対して
さらに複雑性が増すデジタル社会　例えば　AI医療時代の医療のトラストは？

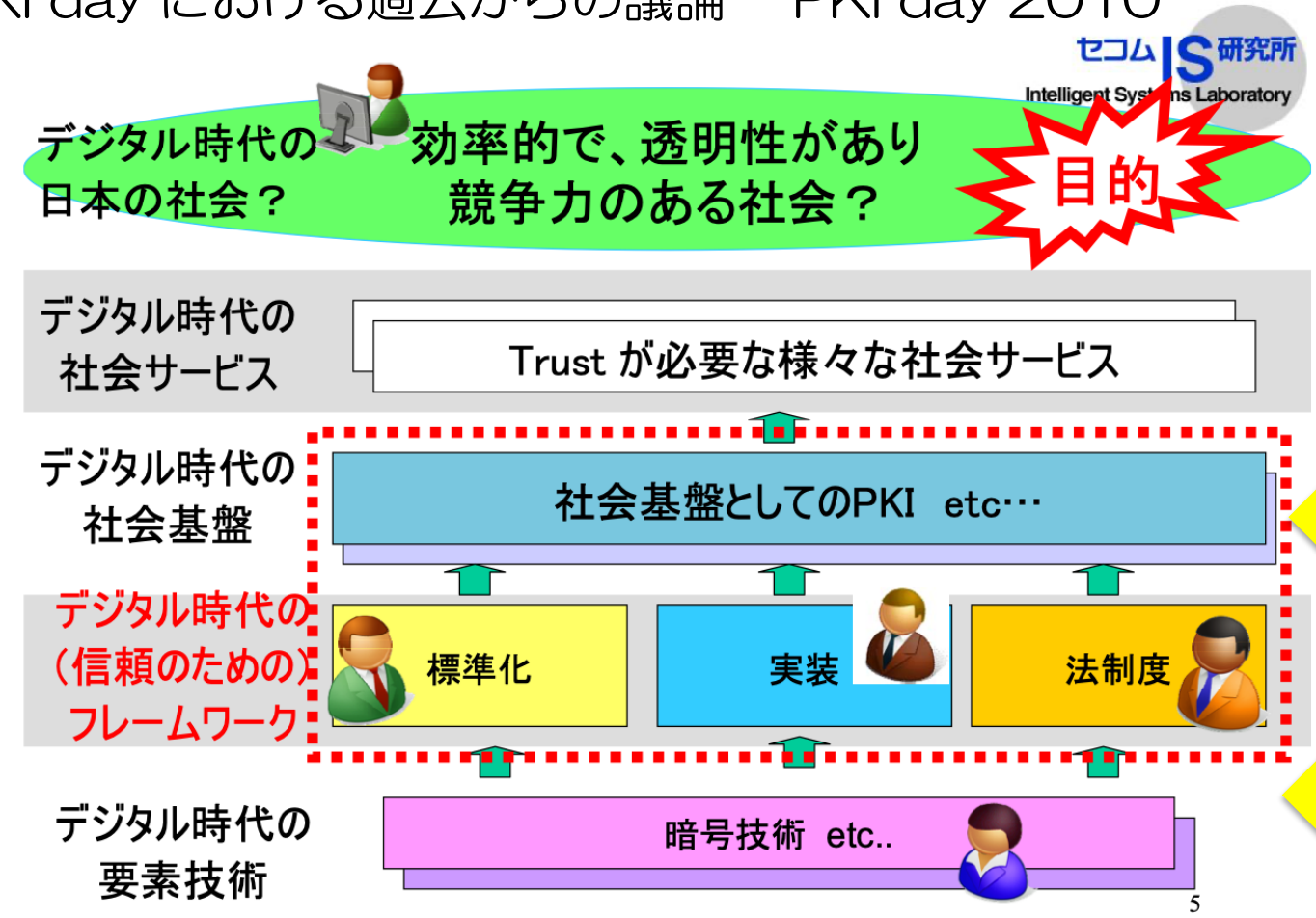
・デジタルにより社会が変革
・変革する社会、複雑性が増すデジタル社会において「社会的な複雑性の縮減メカニズム」の再構築が必要になっている？？（仮説）
・「変貌するデジタルトラストアーキテクチャ」（4月15日）
・「デジタルトラストにおける法と技術のあり方」（4月16日）

複雑な医療システムの信頼性（trustworthiness）
→信頼性（trustworthiness）の意味が多義的になる



医療におけるITの役割　→　これらに対するサイバー攻撃

PKI day における過去からの議論　PKI day 2010



出典：
PKI day 2010
社会基盤としてのPKI
https://www.jnsa.org/seminar/pki-day/2010/data/5_a_matsumoto.pdf

「デジタルトラストにおける法と技術のあり方」
（4月16日）
トラストサービスを中心に

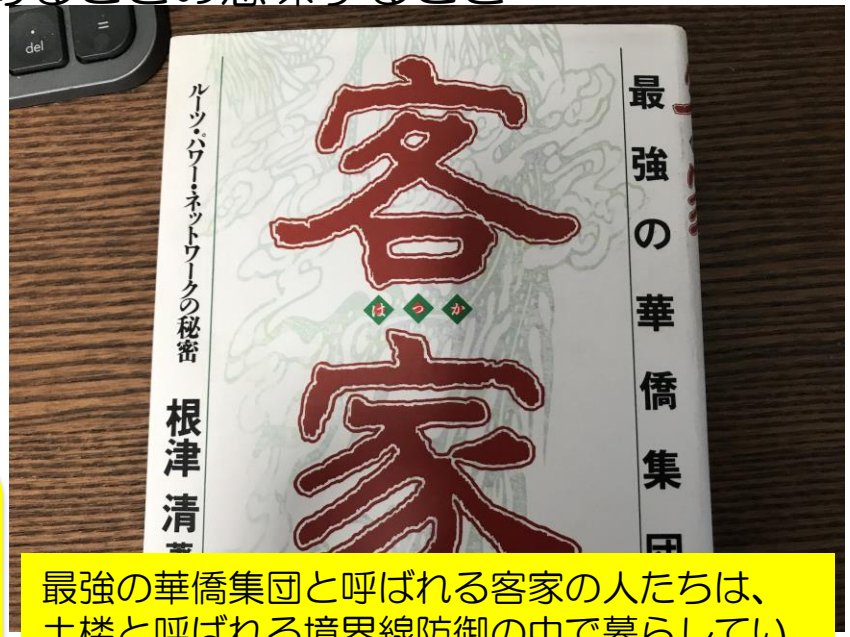
「変貌するデジタルトラストアーキテクチャ」
（4月15日）
コンピューターアーキテクチャに組み込まれる暗号技術によるトラスト

本日のテーマ「変貌するトラストアーキテクチャ」のキーワード
「エンクレーブ・TEE(Trusted Execution Environment)」
トラスト自体ではなくトラストを作れる環境・場（物理的空間、ネットワークゾーン、etc…）　→　それがエンクレーブ（飛び地）であることの意味すること

外壁
客家の人たちにとっての境界線防御

客家の土楼
客家の人たちにとって
TEE
Trusted Execution
Environment

出典：客家（はっか、ハッガー、ハッカ）福建土楼
https://ja.wikipedia.org/wiki/福建土楼



最強の華僑集団と呼ばれる客家の人たちは、土楼と呼ばれる境界線防御の中で暮らしていた？　->　現在は世界中？？

客家(はっか)―最強の華僑集団 ルーツ・パワー・ネットワーク
https://www.amazon.co.jp/gp/product/447817041X/ref=ppx_yo_dt_b_asin_title_o00_s00?ie=UTF8&psc=1

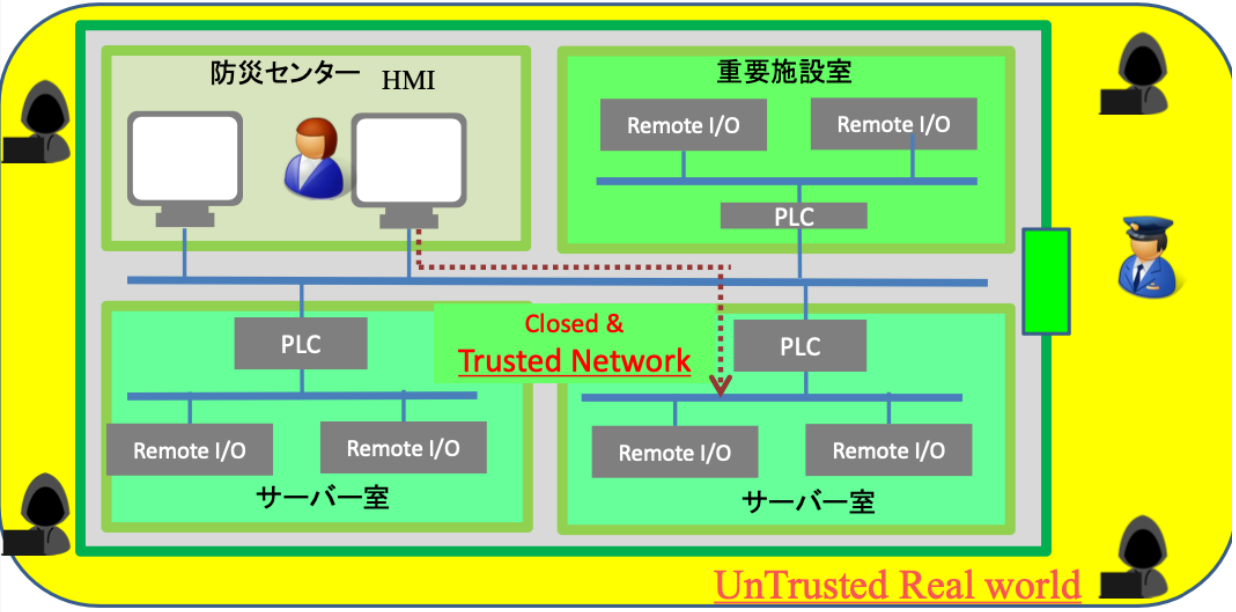
出典：
PKI Day 2019
2019年4月17日
https://www.jnsa.org/seminar/pki-day/2019/data/190417_am05_matsumoto.pdf

信頼される安心を、社会へ。
SECOM

セコムIS研究所
Intelligent Systems Laboratory

重要インフラにおける物理セキュリティによるトラスト セキュリティ区画とセキュリティ境界におけるアクセス制御

Closed & Trusted Networkのセキュリティ ≒ 物理セキュリティ



こうした「Closed & Trusted Network」も、価値の創造のために様々な接続（Connected）が求められつつある

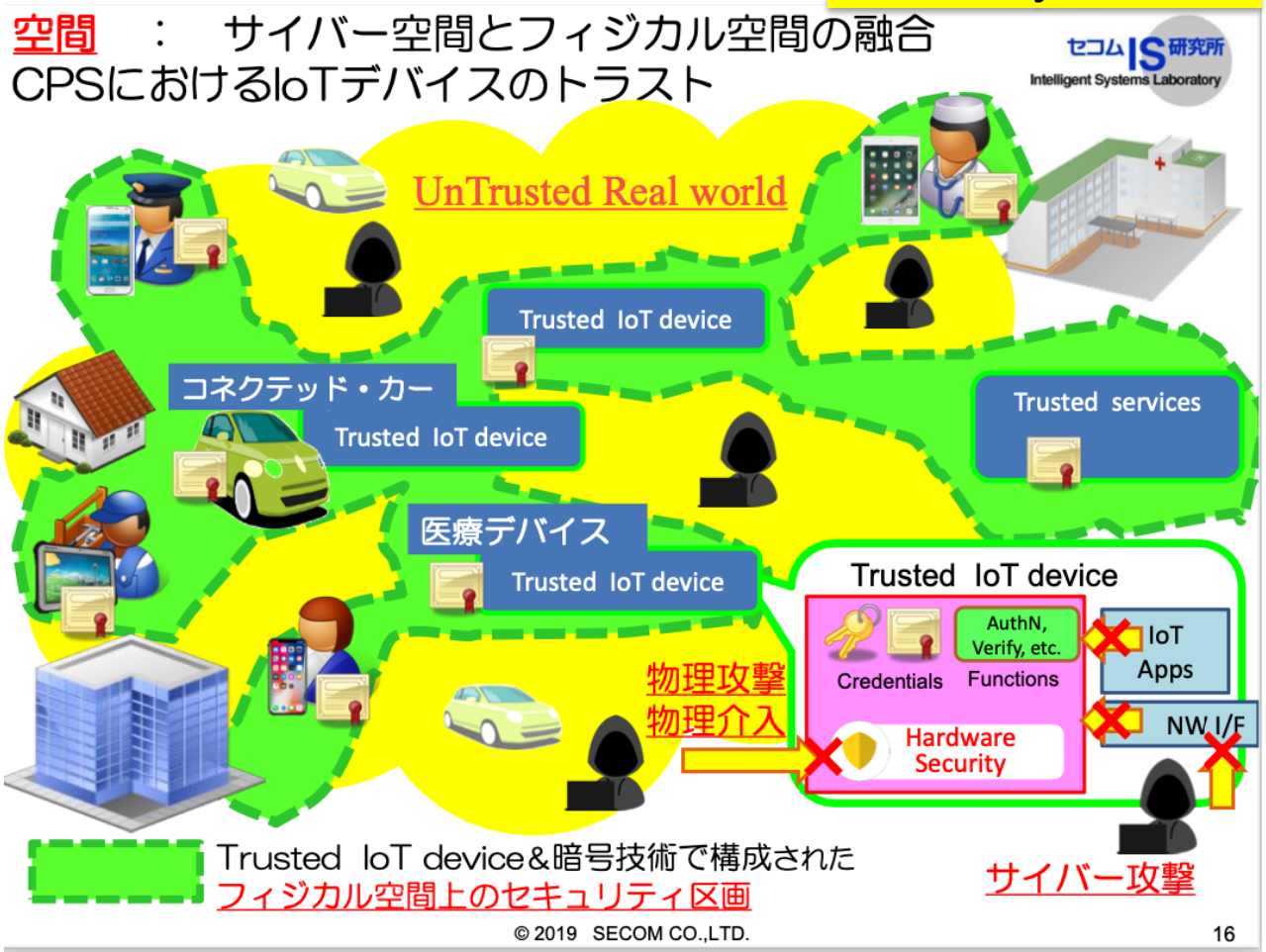
トラストな空間　セキュリティ区画

・物理的ゾーニングで守られたトラストな場に構築されるトラステッドネットワーク

・物理的に異なる場所を繋ぐ専用線（専用線によりトラストな場の拡大）
・物理的に離れた場所も含んだトラステッドネットワーク

・ゼロトラストネットワーク
・物理的制約などを脱して多様なトラストを実現できる環境・場？？
・物理的制約などを脱することがイノベーションにつながる。

PKI day 2019



出典：
PKI Day 2019
2019年4月17日
https://www.jnsa.org/seminar/pki-day/2019/data/190417_am05_matsumoto.pdf

信頼される安心を、社会へ。
SECOM

・Trusted IoT devices （trusted smart devices）は、ゼロトラストネットワークでは、“untrusted networks”において利用されるデバイスとして必要。

・Cyber Physical Systems (CPS)では、“Untrusted real world”において利用されるデバイスとして必要。

エンクレーブ・TEEなどが作り出すSocity5.0時代のトラスト
スケールアウトするトラストへの要求??

- これまでのスケールアウト　　クラウドコンピューティング
  - 2005年出版GOOGLEクラウドの核心--巨大データセンターの変貌と運用の経済学
- スケールアウトするトラスト??　-> スケールアウトは、Socity5.0時代的要求？？
  - 膨大な数のデバイス、あらゆるもののConnect化、スマート化、これらのためのトラスト
  - コフィデンシャルコンピューティング（の経済学???）
    - HWRoot Of Trust・ Cryptographic Boundary をトラストの起点に、（PKIのような）暗号鍵の関係性で実現されるトラストモデルをベースに「 Trust Boundary」をスケーラブルに拡張する技術に思える。
  - トラステッドデバイス（トラステッドIoTデバイス）（の経済学???）
    - 既に膨大な数のスマートフォンに組み込まれている TEE(Trusted Execution Environment)
    - IoTデバイスへのセキュリティ要求が（プラットフォームセキュリティ）、そのまま（ファブレス）シリコンベンダーが設計するSoC(System-on-a-chip)へ
    - ＃超巨大印刷工場であるTSM＊が、ただひたすら輪転機を回す

参考スケールアウトするIoTデバイスのトラスト

講演&パネルディスカション
アーキテクチャの変貌の観点から新たなトラストの仕組み

- 講演１
  - トラストを確立する技術の概要 ～どのような技術がなぜ作られてきたのか ～
  - 宮澤慎一氏　セコム（株）IS研究所　主務研究員
- 講演２
  - デジタルトラストとゼロトラストネットワーク
  - 鈴木研吾氏　　(株)LayerX シニアセキュリティアーキテクト
- 講演３
  - Confidential Computing の技術動向　～TEE/Enclaveの便利な活用例～
  - 奥田哲矢氏　NTTセキュアプラットフォーム研究所　研究主任
- 講演４
  - プラットフォームで実装されるトラスト
  - 垣内由梨香氏　　Microsoft Corporation セキュリティ レスポンスチーム
- パネルディスカション
  - 変貌するトラストアーキテクチャ

変貌するトラストアーキテクチャー
４つの講演とキーワードとの関係

信頼される安心を、社会へ。
SECOM

デジタルトラストアーキテクチャの要素技術をベースにトラストが構築されつつある
ゼロトラストネットワークとConfidential Computing

講演２
デジタルトラストとゼロトラストネットワーク

講演３
Confidential Computing の技術動向

講演１　トラストを確立する技術の概要
HW Root OF Trust
セキュアーブート
セキュアエンクレーブ・TEE
リモートアテステーション

講演４
プラットフォームで実装されるトラスト

プラットフォームに組み込まれて行くデジタルトラストアーキテクチャ

「デジタルトラストに対応するコンピュータアーキテクチャの変化」
コンピュータアーキテクチャ自体に暗号技術（主に公開鍵暗号技術）が取り込まれて行く
→　デジタル・トラストアーキテクチャ

パネルディスカション

(1). Don’t Trust,　But Verify　の意味するところ
(2). 美味しいエンクレーブの作り方？？
(3).　エンクレーブ・TEEが作り出すデジタルトラスト

Don’t Trust, But Verify　の意味するところ
→ 公開鍵暗号の公開鍵（Public key）は、検証鍵（Verification key）

- ゼロトラストネットワーク
  - Don’t Trust　　何をトラストしない？　　-- ネットワーク？？
  - But Verify　　何をベリファイする？（何をトラストしてベリファイする？）
- TEE・エンクレーブを利用したコンフィデンシャルコンピューティング
  - Don’t Trust
    - クラウドサービスプロバイダー、システムソフト（OS）とか
  - But Verify　（Intel SGXの場合）
    - エンクレーブ利用者（Relying Party:信頼者)は、インテルのCPUとインテルのアテステーションサービス（アテステーションの署名）のみをトラストする
    - PKI（Intel SGX PKI)的には、トラストアンカー（ Intel SGX PKIのRootCA証明書の公開鍵)からのトラストチェーンの検証(Verification)
- Apple Mac.　のゼロトラスト（コンピューターユーザー??）
  - Intel版　　T2チップ、　ARM版　　M1 chip.
- Android スマートデバイスのゼロトラスト
  - ARM IP coreを組み込むSoC ベンダーが提供するアテステーション？？

Don’ t Trust, But Verify　の意味するところ
PKIのモデルとゼロトラスト

Cryptographic Boundary

完全性・機密性に注力した
非常に強固な境界線防御
署名鍵を徹底的に守る

HSM
(Hardware
Security Module)
署名

署名
データ

- トラストアンカーとなるルートCAの公開鍵のみをトラストする。
- 取り込むデータ（証明書類を含む）は、全てルートCAの公開鍵から検証（Verify)する。

公開鍵
証明書

サブジェクト

ゼロトラスト環境

リポジトリー

署名
データ

アセット

トラストエンジン
PDP：
Policy Decision Point

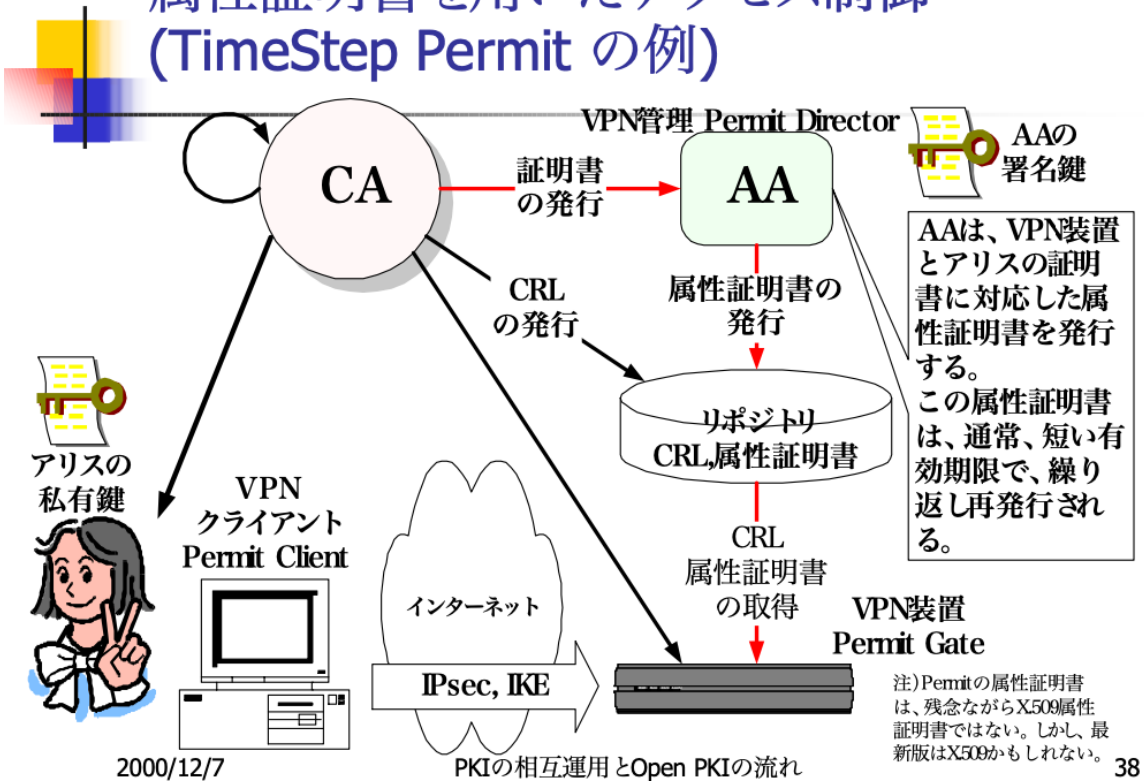
- ゼロトラスト環境に置かれるリポジトリ
- 署名済みデータしか置かない
- 可用性のみ確保する

Trusted party
被信頼者

Relying Party(RP)
信頼者・検証者

トラスト　・　Always Verify

Don’t Trust, But Verify　の意味するところ
→ 公開鍵暗号の公開鍵（Public key）は、検証鍵（Verification key）



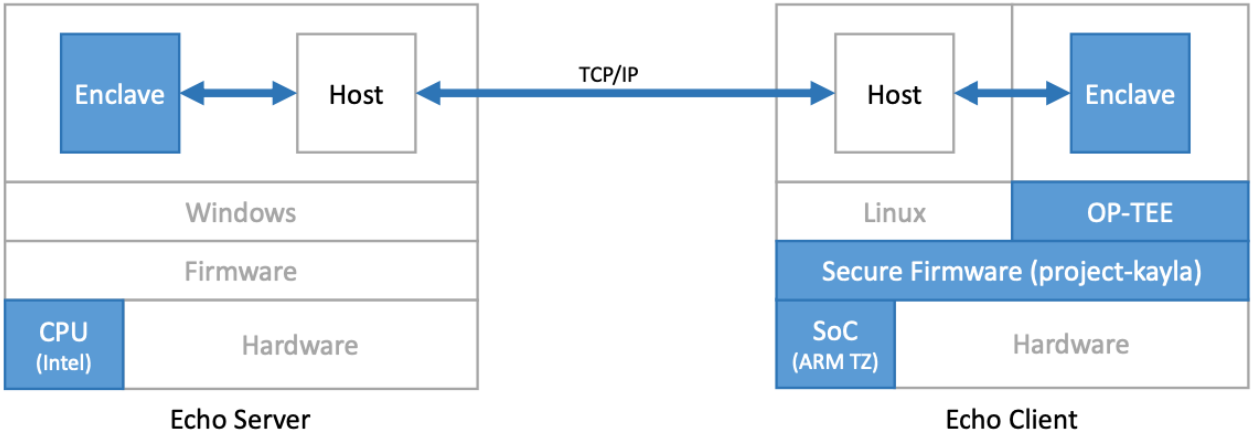
- Verify？？？
  - VPN装置は、FIPS140-2レベル２認証取得（ハードウェアセキュリティを具備している）
  - VPN装置内に格納されたRoot CAの公開鍵（検証鍵）がトラストアンカー
  - Relying Party としてのVPN装置は、トラストアンカー（公開鍵）から検証できる署名データ（公開証明書、属性証明書）以外は信頼しない（ゼロトラスト）。

日本インターネット協会(IAJ)セキュリティ部会主催の第2回セキュリティフォーラム　2000年12月7日
https://www.iajapan.org/bukai/isec/forum/2000/20001207report.html

Trusted party被信頼者　Relying Party(RP)信頼者

Don’t Trust, But Verify　の意味するところ
コンフィデンシャルコンピューティングの世界観？
→　Trusted Component以外は、ゼロトラスト？

Example using “Echo” Sample

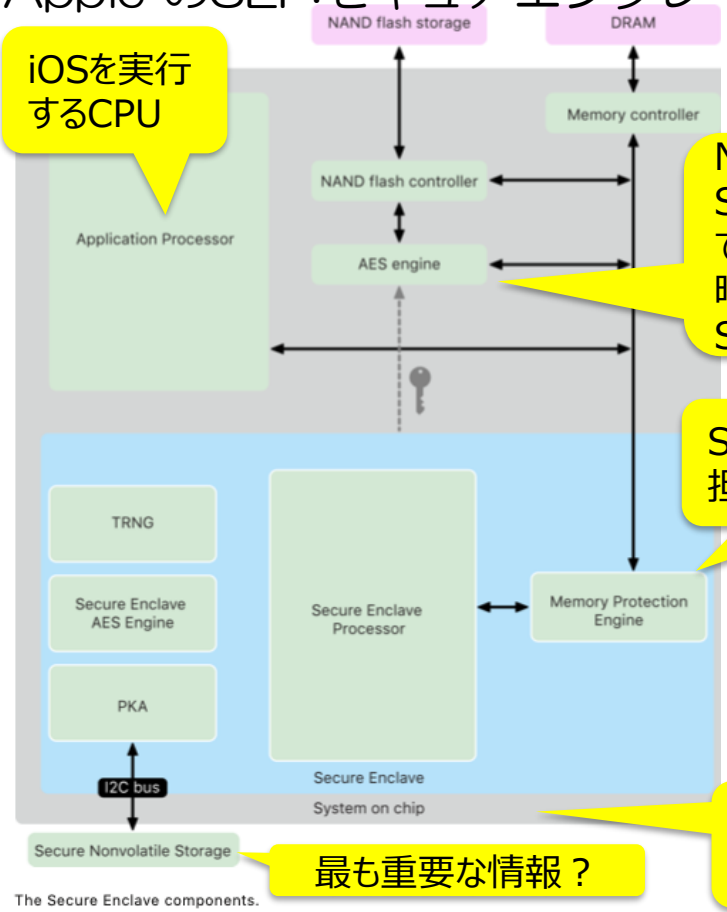


出典：
Open Enclave SDK　by. Dave Thaler
https://siot-hackathon.github.io/slides/teep02.pdf

Trusted Component

SIOT Hackathon

美味しいエンクレーブの作り方？？
Apple のSEP:セキュアエンクレーブプロセッサー？？



The Secure Enclave components.

iOSを実行するCPU

NANDもDRAMもSoCから出る時点で全て暗号化
暗号化鍵管理はSEPが担う

SEPがメモリ管理を担っている

最も重要な情報？

これ全部でSystem-on-a-chip

- 「セキュアエンクレーブプロセッサー」というネーミングはミスリード？？
  - エンクレーブ・TEE自体は、アプリケーションプロセッサーのメモリ空間上にある？？
  - エンクレーブを設定するのは、「セキュアエンクレーブプロセッサー」の役割？？

Apple Platform Security
February 2021

出典
Apple. Platform Security **February 2021**
https://manuals.info.apple.com/MANUALS/1000/MA1902/en_US/apple-platform-security-guide.pdf

参考　　Appleの場合　-- エンクレーブ・TEEを中心に垂直統合を進めるAppleにおけるトラストの実装

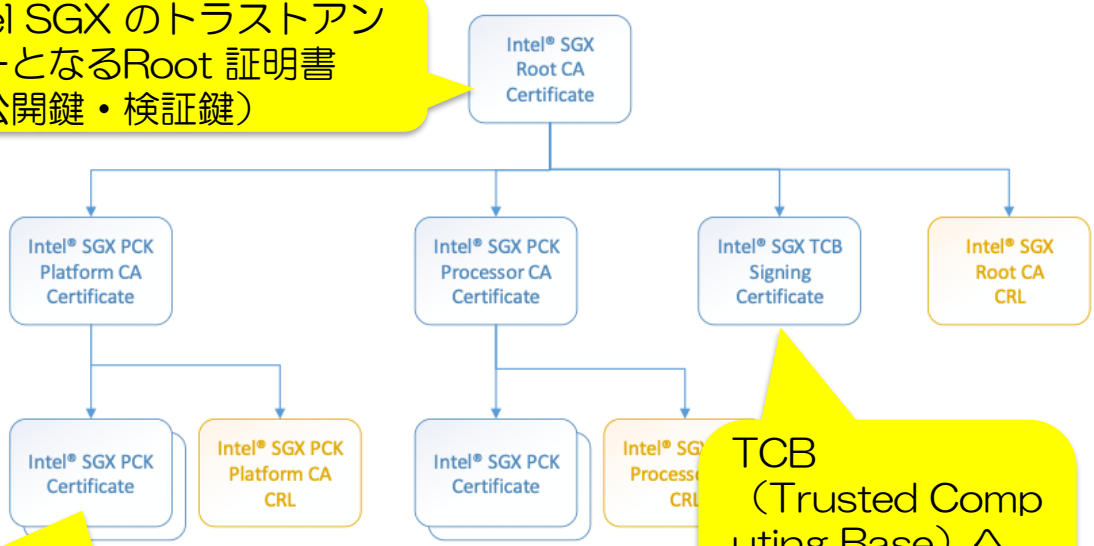
美味しいエンクレーブの作り方？？

Intelの描くゼロトラスト？-- CPUアーキテクチャに組み込まれたPKI

CPUは、自分自身組み込まれた公開鍵（検証鍵）を頼りに自律的にエンクレーブを作り出す？？

ゼロトラスト環境に置かれるIntel SGX CPUは如何に外界をトラストするのか？

Intel SGX のトラストアンカーとなるRoot 証明書（公開鍵・検証鍵）

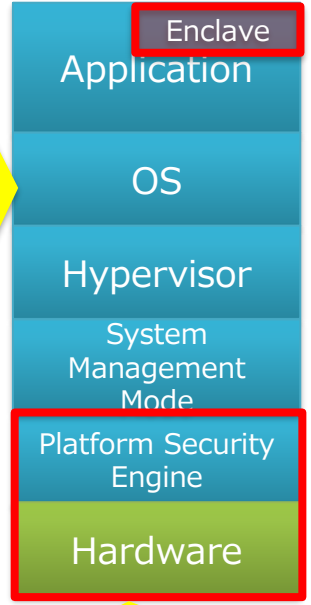


ure 2-1: Certificate Hierar

SGXのプラットフォーム（TCB等の構成証明？？）証明書

TCB（Trusted Computing Base）へのコード署名に利用される公開鍵証明書？？

出荷されたCPUは、CPUを組み込むデバイスも製造者も、サービスもトラストせず、トラストアンカーとなる「公開鍵・検証鍵」から検証できるものだけをトラストしてエンクレーブまでを作る？？



トラストアンカーとなるRoot証明書（公開鍵・検証鍵）が組み込まれたCPU

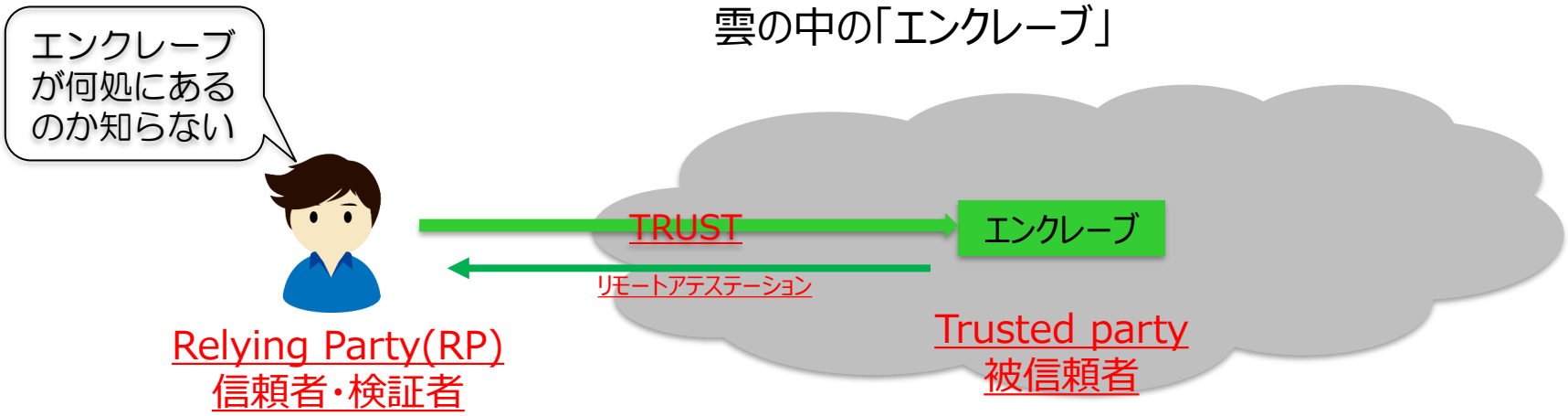
出典： Intel® SGX PCK Certificate and Certificate Revocation List Profile Specification
https://download.01.org/intel-sgx/latest/dcap-latest/linux/docs/Intel_SGX_PCK_Certificate_CRL_Spec-1.4.pdf

エンクレーブ・TEEが作り出すSociety5.0時代のトラスト

信頼される安心を、社会へ。
SECOM

- セキュリティとトラストのアプローチの観点の違い
  - セキュリティ的なアプローチ
    - コネクテッドな社会を実現するためには、セキュリティが必要
    - 後付け的な個別・分野別対処、人的対処になりがち→ スケールアウトが難しい？？
  - トラスト的なアプローチ
    - 場所に捉われないトラスト（エンクレーブ・TEE）を作り出すことが出来れば、イノベーションにつながる　->　そのためには、スケールアウトするトラスト・経済学が必要（プラットフォーマ的発想と類似）　参考スケールアウトするIoTデバイスのトラスト
- 二つのトラスト自体ではなくトラストを作れる環境・場
  - クラウドのエンクレーブ・TEE -> コフィデンシャルコンピューティング
    - 雲の中の「エンクレーブ」
  - エッジのエンクレーブ・TEE
    - ゼロトラストネットワークではなく「ゼロトラスト環境のトラステッドエッジ」
    - リアルワールドの中のエンクレーブ(Trusted IoT デバイス)

雲の中の「エンクレーブ」


エンクレーブ
が何処にある
のか知らない
雲の中の「エンクレーブ」
TRUST
エンクレーブ
リモートアテステーション
Relying Party(RP)
信頼者・検証者
Trusted party
被信頼者

ゼロトラストネットワークではなく「ゼロトラスト環境のトラステッド・エッジ」

- TEEは、 Relying Partyであるトラストエンジンからみてトラストな領域
- このトラストの領域から周囲をVerifyする？？
- リモートアテステーションを行う

①ユーザ（ローカル）認証

ゼロトラスト環境

TEE
①ユーザ（ローカル）認証
②アプリケーション監視
③リモートアテステーション

②アプリケーション監視

アプリケーション

Chain Of Trust

トラステッドOS

HWRoT･セキュア･エンクレーブ
耐タンパー、Cryptographic Boundary

OS

（ユーザ所有の）デバイス

Trusted party
被信頼者

③リモートアテステーション

トラスト ・ Always Verify

アセット

トラストエンジン
PDP：
Policy Decision Point

Relying Party(RP)
信頼者・検証者

ゼロトラストネットワークにおける
信頼性（trustworthiness）は、主に
被信頼者であるサブジェクトのセキュリティ

サブジェクト

信頼性
（trustworthiness）

アプリケーション	アプリケーションの振る舞い 脆弱性の有無、etc..
ユーザ	認証レベル（LoA）、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.

アセット

トラストエンジン
PDP：
Policy Decision Point

Trusted party
被信頼者

トラスト ・ Always Verify

Relying Party(RP)
信頼者

Society5.0時代のトラスト
リアルワールドの中のエンクレーブ（Trusted IoT デバイス）

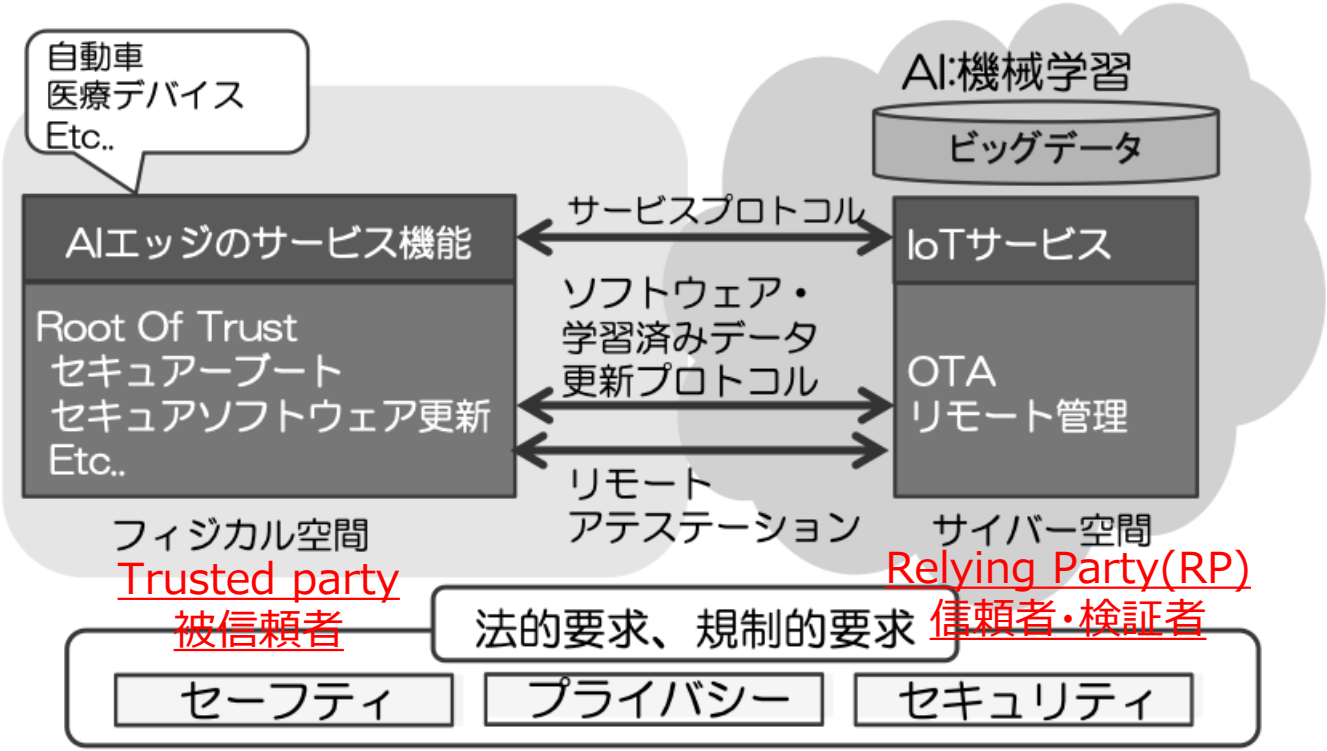


図1. AIエッジ、機械学習、規制の関係

参考
サイバーフィジカルシステムにおけるトラスト
（society5.0時代におけるデジタルトラスト）

出典：
JNSAPress
AI・IoT によるイノベーションを支える暗号技術によるトラスト
https://www.jnsa.org/jnsapress/vol47/2_kikou-2.pdf

付録（参考）

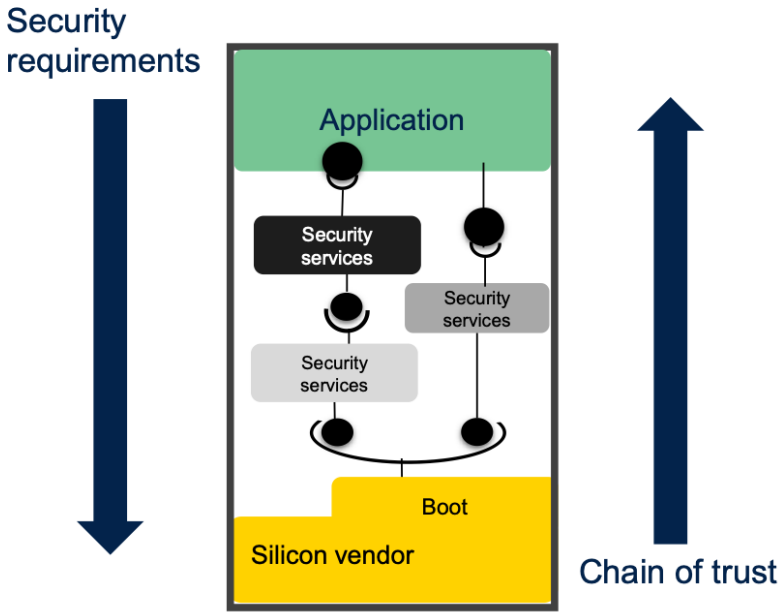
- スケールアウトするIoTデバイスのトラスト
  - 「HW Root OF Trust、セキュアーブート、セキュアエンクレーブ・TEE、リモートアテステーション」
- Appleの場合
  - エンクレーブ・TEEを中心に垂直統合を進めるAppleにおけるトラストの実装
- サイバーフィジカルシステムにおけるトラスト（ society5.0時代におけるデジタルトラスト）
  - サイバーフィジカルシステムにおけるデジタルトラストのための利用されていくであろうTEE/Enclave
- 属性証明書とアクセス制御(PMI)

スケールアウトするIoTデバイスのトラスト

- HW Root OF Trust
- セキュアーブート
- セキュアエンクレーブ・TEE
- リモートアテステーション

HW Root OF Trust からの　Chain Of Trust

Step 3: Proof Compliance with Requirements



出典：
Cybersecurity Standardization
Future scheme：consumer IoT
https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021/presentations/04-02-wuidart

Rely on Composition Model
→ SESIP* methodology

Security based on an economy of scale

スケールアウトするトラスト

Security based on economy of scale
→　プラットフォーマー的発想

従来企業的発想では
「セキュリティはコストがかかる」
「HW Root Of Trust」はコストがかかる。

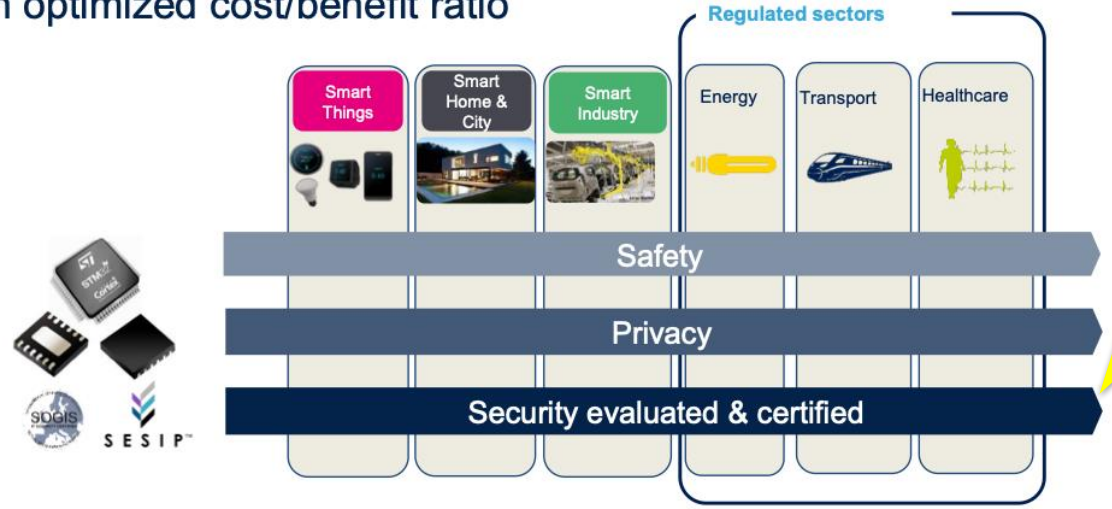
HW Root OF Trust ≒ **Silicon Root of Trust**

信頼される安心を、社会へ。
SECOM

Our Security Challenge

Provide devices with adequate security features/foundations

- for the entire eco-system, worldwide
- at an optimized cost/benefit ratio



規制や認証（Certified）等により、共通のセキュリティ要件が明確になり。

様々な分野のデバイスの共通の要求としてのプラットフォーセキュリティとなり。

このプラットフォーセキュリティを具備したSoC(System-on-a-chip）がシリコンベンダーにより設計され、大量に配布されていく。

出典：
https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021/presentations/04-02-wuidart

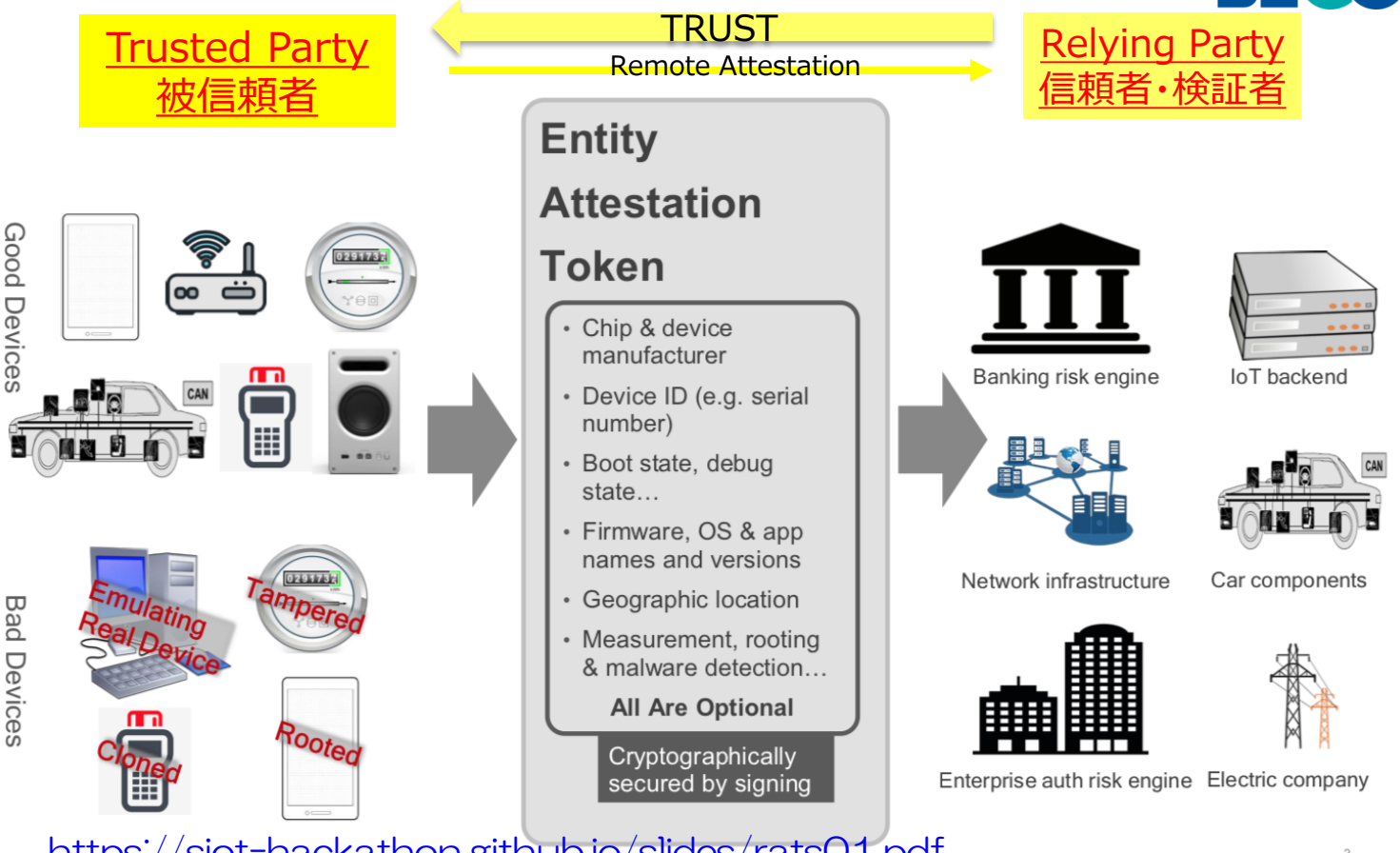
life.augmented

IoTのリモートアテステーション　（Remote Attestation）

信頼される安心を、社会へ。
SECOM

Relying Party
（信頼者）から
みたトラストの観
点からの
Bad devices

リモートアテステー
ションには、使えな
い。



出典：　https://siot-hackathon.github.io/slides/rats01.pdf

サイバーフィジカルシステムにおけるトラスト
-- society5.0時代におけるデジタルトラスト --

- サイバーフィジカルシステムにおけるデジタルトラストのための利用されていくであろう TEE/Enclave

サイバーフィジカルシステム　≒　IoT ・BD・AI

信頼される安心を、社会へ。
SECOM

法と技術アーキテクチャ

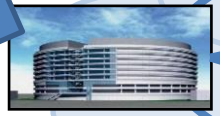
技術

技術アーキテクチャと
ビジネス・デザイン

法制度

AIなどによる処理

ビジネス



ビッグデータの収集

情報と情報がつながるサイバー空間

フィジカル空間に還元
新たな価値の創造

デジタル・ツイン

高機能なエッジAI

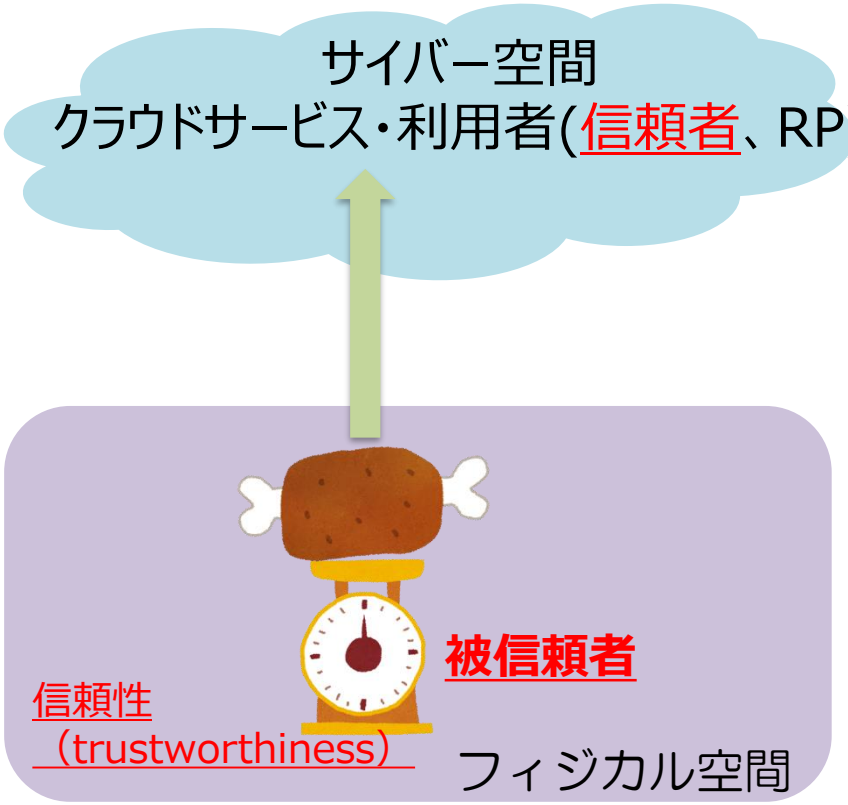
学習済
モデル

フィジカル空間における
サービスイノベーション

膨大な数のIoTデバイス

人と人、人とモノ、モノとモノがつながるフィジカル空間

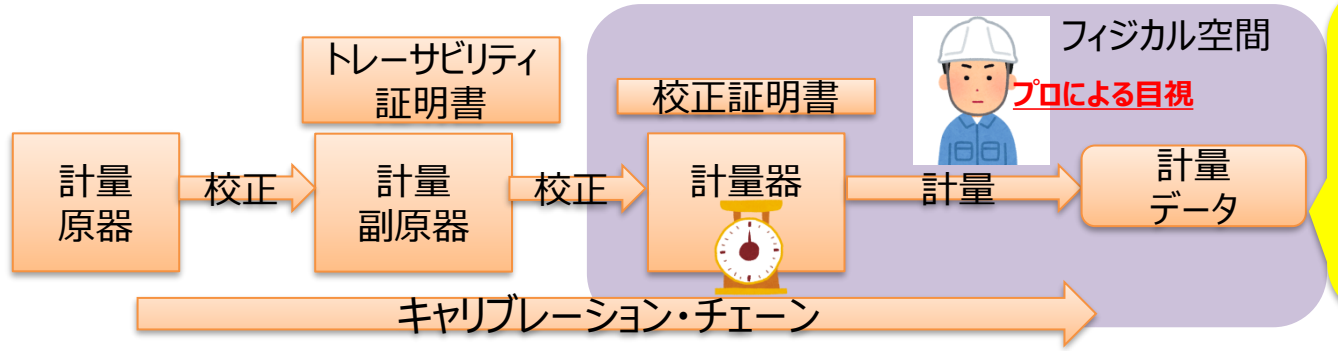
サイバーフィジカルシステムにおけるトラスト
フィジカル空間にある「はかり」をサイバー空間から利用するというシナリオ



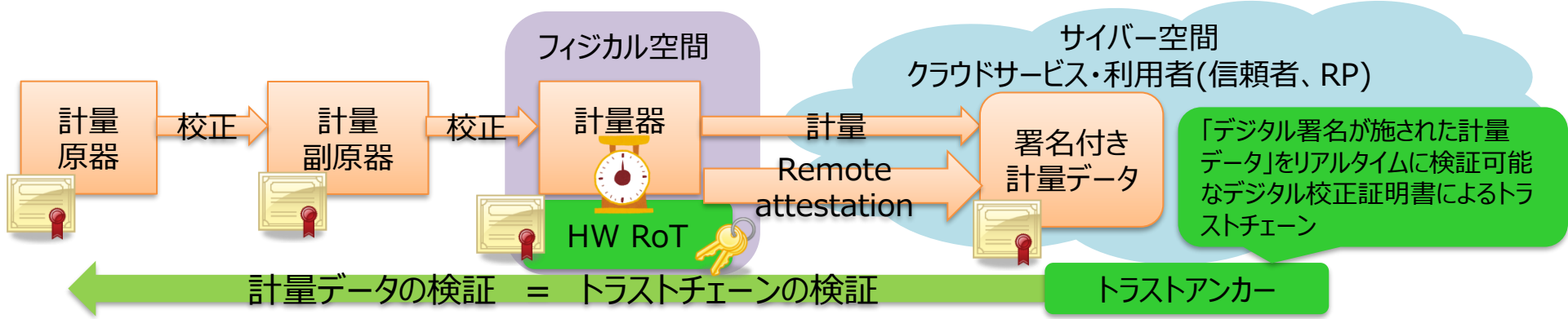
- 「測る」ということに関しては
  - クラウドサービスは、信頼者
  - はかりは、被信頼者
- では被信頼者である「はかり」の信頼性（Trustworthiness）は？
  - クラウドサービスは、「はかり」の信頼性について何を知りたいのか？
  - リモート（クラウドサービス）に、重さを伝えるための「はかり」というIoTデバイスセキュリティも信頼性の一つの要素
  - しかし、はかりの信頼性としてクラウドサービス伝えらいことは？？？

PKI・トラスト技術の役割　-- サイバーフィジカルシステムにおけるトラスト

例えば、計量（計測）データの信頼性（Trustworthiness）では



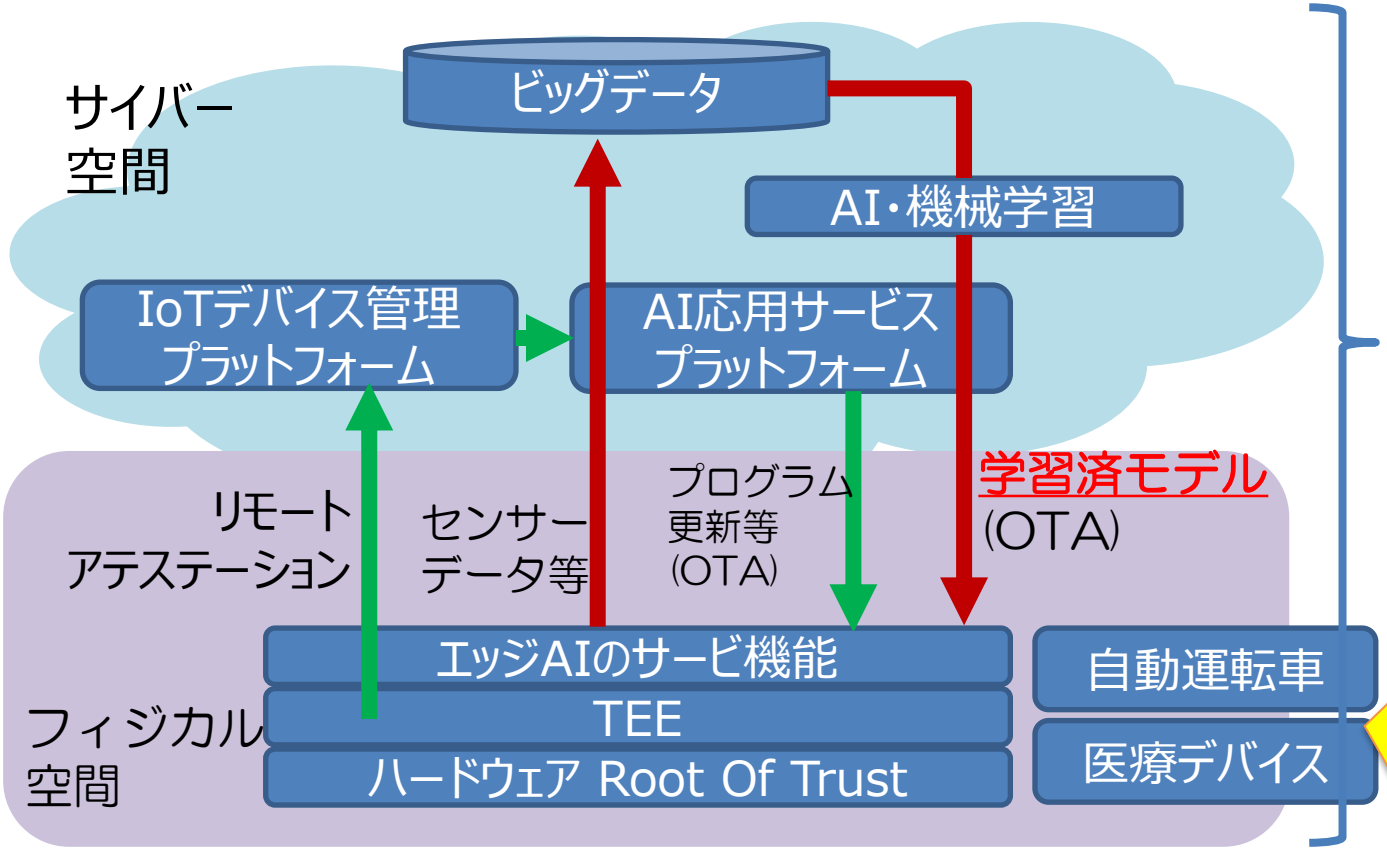
計量（計測）データの信頼性（Trustworthiness）で最も重要なことは、計量器、計量データのキャリブレーション・チェーン が証明、保証されていること。



「デジタル署名が施された計量データ」をリアルタイムに検証可能なデジタル校正証明書によるトラストチェーン

PKI・トラスト技術の役割　→　デバイス・データの信頼性（Trustworthiness）をRPに伝える
→ 人の目視に頼らず、デバイス・データの信頼性（Trustworthiness）が検証できること

サイバーフィジカルシステムにおけるトラスト技術
⇒　デジタルツイン・エッジAIを含むインテグリティ



- 膨大な数のIoTデバイス
- 高機能なエッジAI
- この循環に対するインテグリティがサイバーフィジカルシステムのトラストを支える

フィジカル空間における法的・規制的要求
- セーフティー
- プライバシー
- セキュリティ

トラスト・ビジネスデザイン的観点 – スケールアウト

信頼される安心を、社会へ。
SECOM

クラウドとIoTデバイスが持つ、暗号鍵とクレデンシャルにより強固なIoTのトラストを実現する。

クラウド

強固な物理セキュリティ環境のデータセンターにおけるトラストな運用

大量の（TEE&ハードウェアセキュリティを具備した）IoTデバイスをセキュアにクラウドからリモート管理
→ スケールアウトするプラットフォーマのビジネスモデル

クラウドからみてトラストな実行環境（TEE）

便利なIoTデバイスによるサービスを享受したいが、ネットワーク＆デバイスの管理はしたくない利用者

高機能なIoT ソフト

TEE

ハードウェアセキュリティ
HW Root of Trust

HOME

IoTデバイスからすると管理者不在で信頼できない環境（ゼロトラストネットワーク）

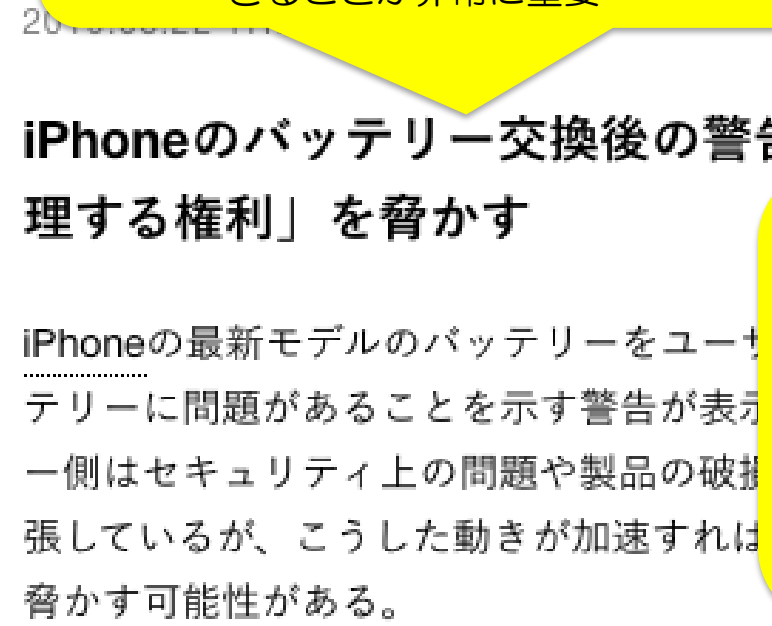
Appleの場合

エンクレーブ・TEEを中心に垂直統合を進める
Appleにおけるトラストの実装

購入したApple 製品は、購入者のモノ？？
ハードウェアも含めたインテグリティの実装

修理する権利の話
right-to-repair

- アップルの「純正」バッテリーへの交換であっても警告表示
  - 物理的攻撃（≒物理的な修理）に対する耐性がある。
  - サービスとしてのビジネスモデル（≒アップルの目指すビジネスモデル？？）では、ハードウェア攻撃とハードウェア修理が明確に区別できることが非常に重要


NEWS

iPhoneのバッテリー交換後の警告表示は、消費者の「修理する権利」を脅かす

iPhoneの最新モデルのバッテリーをユー
テリーに問題があることを示す警告が表
一側はセキュリティ上の問題や製品の破
張しているが、こうした動きが加速すれ
脅かす可能性がある。

出典：iPhoneのバッテリー交換後の警告表示は、消費者の「修理する権利」を脅かす
https://wired.jp/2019/08/22/apple-iphone-battery-service-alerts/

- ハードウェアセキュリティが必須となる
  - OTAが必須となる自動運転車
  - AppleWatchのようなAI技術等を駆使した（したい）医療デバイス
  - *#型式証明のパラダイムシフト*

Your Computer Isn't Yours

https://sneak.berlin/i18n/2020-11-12-your-computer-isnt-yours.ja/

- きたよ。ついに起こった。気がついたかい？
- もちろん、リチャード・ストールマンが 1997 年に予言した世界のことを言ってる。コリイ・ドクトロウが警告したものでもある。
- 最近のバージョンの macOS では、君はコンピューターの利用ログを記録されていて、ログデータを送信されることなしには、電源を入れてコンピューターを使うことも、テキストエディターや電子書籍リーダーを起動して書いたり読んだりすることもできない。
- 最近のバージョンの macOS では、君が実行しているすべてのプログラムのハッシュ値（固有識別子）を OS が Apple に送信していることがわかった。多くの人はこのことに気がついていなかった。なぜならログの送信はこっそり行われていて失敗したときも痕跡を残さないし、君がオフラインのときには何もしないようになっているからだ。しかし今日、ログ送信先のサーバーが不調をきたし、プログラムが障害回避処理のパスを通らなかったせいで、インターネットに接続した状態の Mac ではアプリを起動することができなかった。
- ログ送信処理はインターネット経由で行われているから、サーバーは君の IP アドレスを知ることができるし、もちろんそのログ送信処理がいつ行われたかも把握できる。 IP アドレスからは都市や ISP レベルの大体の位置情報がわかるし、こんな感じの情報でテーブルを組むことができる。
- 日付、時刻、コンピューター、 ISP 、市、州、アプリケーションハッシュ
- Apple は（もしくはそれ以外の誰だって）これらのハッシュ値は調べることができる。 App Store にあるアプリすべて、 Creative Cloud アプリ、 Tor ブラウザー、クラッキングもしくはリバースエンジニアリングツール、何でもだ。
- つまり Apple は君がいつ家にいるかわかるってことだ。君がいつ仕事に行ってるかも。どんなアプリをそこで起動して、どのくらいの頻度で使っているかも。君がいつ Premier を友だちの家の Wi-Fi ごしに開いたか、いつよその街のホテルで Tor ブラウザーを起動したかを知っている。
- 「誰が気にするもんか？」君はそう言うだろう。
- えーっとね、これは Apple のことだけじゃないんだよ。 Mac から送られる情報は Apple の手元だけにとどまるわけじゃないんだ。
- これらの OCSP リクエストは暗号化されることなく送信されている。ネットワークを監視できる人は誰だって見ることができる。君の ISP や回線を盗聴してる人もだ。
- これらの情報はサードパーティー（ Akamai ）の CDN を経由して収集されている。
- 2012 年の 10 月から Apple はアメリカ軍の諜報機関がやってる PRISM スパイプログラムの一員になっていて、連邦警察と軍が望めば令状なしでこれらのデータへ自由にアクセスすることが可能になっている。彼らは 2019 年の前半に 18,000 回以上、後半には 17,500 回以上も情報照会を実施している。
- このデータは君の生活や習慣を解き明かすための十分な材料になるだろうし、君につきまとう誰かが君の生活行動パターンを突き止めるのを可能にするだろう。ある種の人にとってはこれは物理的な危険をもたらすことだってある。
- （続く）

Apple PKI

Apple established the Apple PKI in support of the generation, issuance, distribution, revocation, administration, and management of public/private cryptographic keys that are contained in CA-signed X.509 Certificates.

Apple Root Certificates

- Apple Inc. Root Certificate
- Apple Computer, Inc. Root Certificate
- Apple Root CA – G2 Root Certificate
- Apple Root CA – G3 Root Certificate

Apple Intermediate Certificates

- Apple IST CA 2 – G1 Certificate
- Apple IST CA 8 – G1 Certificate
- Application Integration Certificate
- Application Integration 2 Certificate
- Application Integration – G3 Certificate
- Apple Application Integration CA 5 – G1 Certificate
- Developer Authentication Certificate
- Developer ID Certificate
- Software Update Certificate
- Timestamp Certificate
- WWDR Certificate (Expiring 02/07/2023 21:48:47 UTC)
- WWDR Certificate (Expiring 02/20/2030 12:00:00 UTC)
- Worldwide Developer Relations – G2 Certificate

Certificate Revocation Lists

- Apple Inc. Root CRL
- Apple Computer, Inc. Root CRL
- Software Update CRL
- Timestamp CRL
- Worldwide Developer Relations CRL

Certificate Policy (CP) and Certification Practice Statements (CPS)

Apple Root CA:

- Apple Certificate Policy
- Application Integration CPS
- Developer Authentication CPS
- Developer ID CPS
- Software Update CPS
- Timestamp CPS
- Worldwide Developer Relations CPS

Apple Public CA:

- Apple Public CA CPS

Audit Reports

Certification Authorities WebTrust

WebTrust for Certification Authorities:

- WTCA
- WTExternalRoots

Certification Authorities WebTrust BR - SSL

WebTrust for Certification Authorities – SSL Baseline with Network Security:

- WTBR

Apple Root Certificate Program

To better protect Apple customers from security issues related to the use of public key infrastructure certificates and enhance the experience for users, Apple products use a common store for root certificates. You may apply to have your root certificate included in Apple products via the Apple Root Certificate Program.

Contact

Contact the Apple PKI team at contact_pki@apple.com.

信頼される安心を、社会へ。

SECOM

Appleの製品・サービスのビジネスモデル＆トラストを支えるApple のPKI

- Apple Root CA
  - Apple Application Integration CA (AAI Sub-CA)
  - Worldwide Developer Relations CA (WWDR Sub-CA)
  - Software Update Sub-CA
  - Developer ID Sub CA
  - General Timestamp CA

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

Apple Root CA

Developer ID Sub- CA

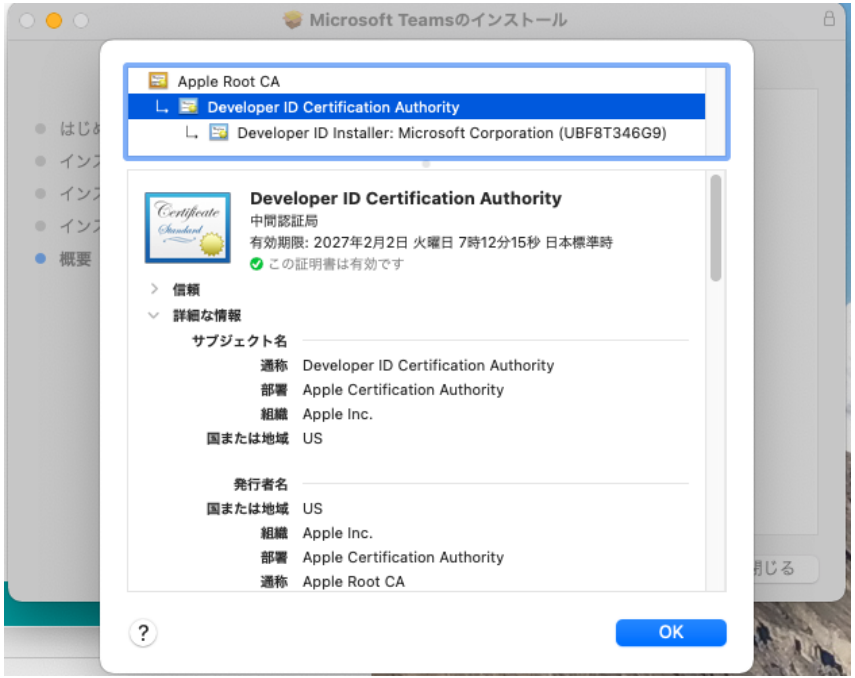
2.2. COMMUNITY AND APPLICABILITY

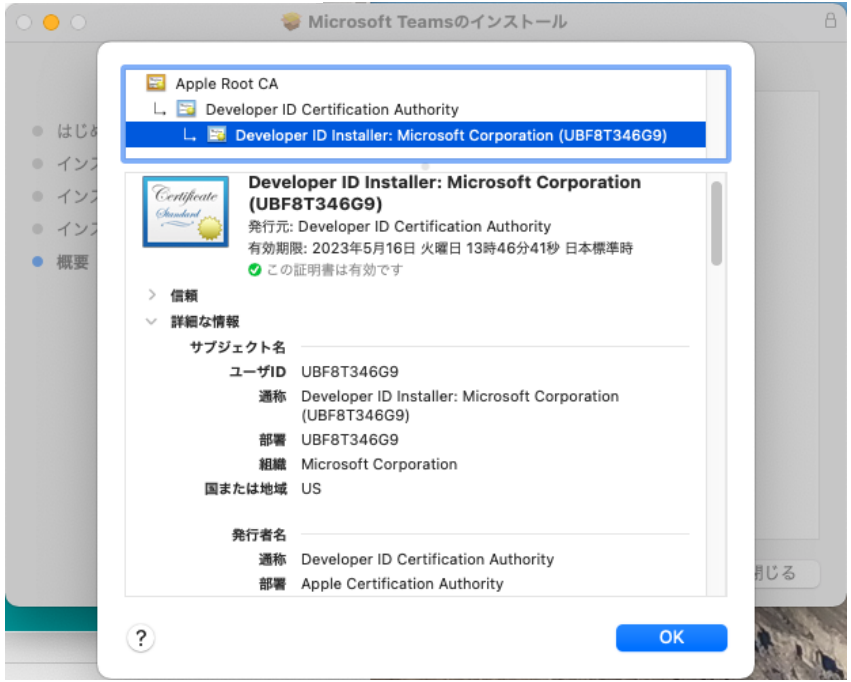
This CPS is applicable to the following certificates issued by the Developer ID Sub-CA:

- Developer ID Installer Package Signing Certificates
- Developer ID Application Code Signing Certificates
- Developer ID Application and Kernel Extension Code Signing Certificates

Certificates used exclusively for functions internal to Apple Products and/or Apple processes are not included within the scope of this CPS.

出典：
https://images.apple.com/certificateauthority/pdf/Apple_Developer_ID_CPS_v3.1.pdf





Appleの製品・サービスのビジネスモデル＆トラストを支える Apple のPKIから発行される様々なデジタル証明書

信頼される安心を、社会へ。
SECOM

- WWDR iOS Software Development Certificates (“iOS Development Certificates”)
- WWDR iOS Software Submission Certificates (“iOS Submission Certificates”)
- WWDR Apple Push Notification service Development SSL Certificates (“Development SSL Certificates”)
- WWDR Apple Push Notification service Production SSL Certificates (“Production SSL Certificates”)
- WWDR Push Certificate Signing Request Signing Certificates (“Push CSR Signing Certificates”)
- WWDR Safari Extension Signing Certificates (“Safari Certificates”)
- WWDR Mac App Development Certificates (“Mac App Development Certificates”)
- WWDR Mac App Submission Certificates (“Mac App Submission Certificates”)
- WWDR Mac Installer Package Submission Certificates (“Mac Installer Package Submission Certificates”)
- Mac App Store Application Signing Certificates (“Mac App Store Application Certificates”)
- Mac App Store Installer Package Signing Certificates (“Mac App Store Installer Package Certificates”)
- Mac App Store Receipt Signing Certificates
- Mac Provisioning Profile Signing Certificates
- Pass Certificates
- Website Push Notification Certificates
- OS X Server Authentication Certificates
- VoIP Services Push Certificates
- Apple Pay Merchant Certificates
- Apple Pay Pass Certificates
- TestFlight Distribution Certificates
- WatchKit Services Certificates
- Apple Pay Provisioning Encryption Certificates
- Enhanced Pass Certificates
- tvOS Application Signing Certificates
- WWDR Apple Push Services Client Authentication G2 Certificates
- Apple Pay Merchant Client Authentication Certificates
- WWDR Apple Development Signing Certificates ("Apple Development Certificates")

出典：
https://images.apple.com/certificateauthority/pdf/Apple_WWDR_CPS_v1.22.pdf

Appleプラットフォームのセキ ュリティ（2020年春）

https://manuals.info.apple.com/MANUALS/1000/MA1902/ja_JP/apple-platform-security-guide-j.pdf

- ハードウェアセキュリティと生体認証: Secure Enclave、専用のAES暗号化エンジン、Touch ID、Face IDなど、Appleデバ イスのセキュリティの基盤をなすハードウェア。
- システムのセキュリティ: 安全な起動（safe boot）、アップデート、およびAppleのオペレーティングシステムの継続的な動作を可能にする、 統合されたハードウェア機能とソフトウェア機能。
- 暗号化とデータ保護: デバイスを紛失したり盗まれたりした場合や、不正なユーザまたはプロセス（unauthorised person or process）が使用したり変更したりし ようとした場合でもユーザデータを保護するアーキテクチャと設計。
- Appのセキュリティ: Appの安全なエコシステムを提供し、プラットフォームの整合性（platform integrity）を損ねることなく安全にApp を実行で きるようにするソフトウェアおよびサービス。
- サービスのセキュリティ: 識別、パスワード管理、支払い、通信、紛失したデバイスの発見のためのAppleのサービス。
- ネットワークのセキュリティ: 安全な認証（secure authentication）と転送データの暗号化を可能にする業界標準のネットワークプロトコル。
- デベロッパキット: プライバシーを守って家や健康を安全に管理するためのフレームワークと、Appleのデバイスとサービスの 機能を他社製Appにまで拡張するためのフレームワーク。
- 安全なデバイス管理: Appleデバイスを管理し、不正使用を防ぎ、紛失または盗難時にリモートワイプを可能にする方法。
- セキュリティとプライバシーの認証（Certifications）: ISO認証（Certifications）、暗号認定（validation）、コモンクライテリア認証（Certification）、およびCommercial Solutions for Classified(CSfC)プログラムに関する情報。

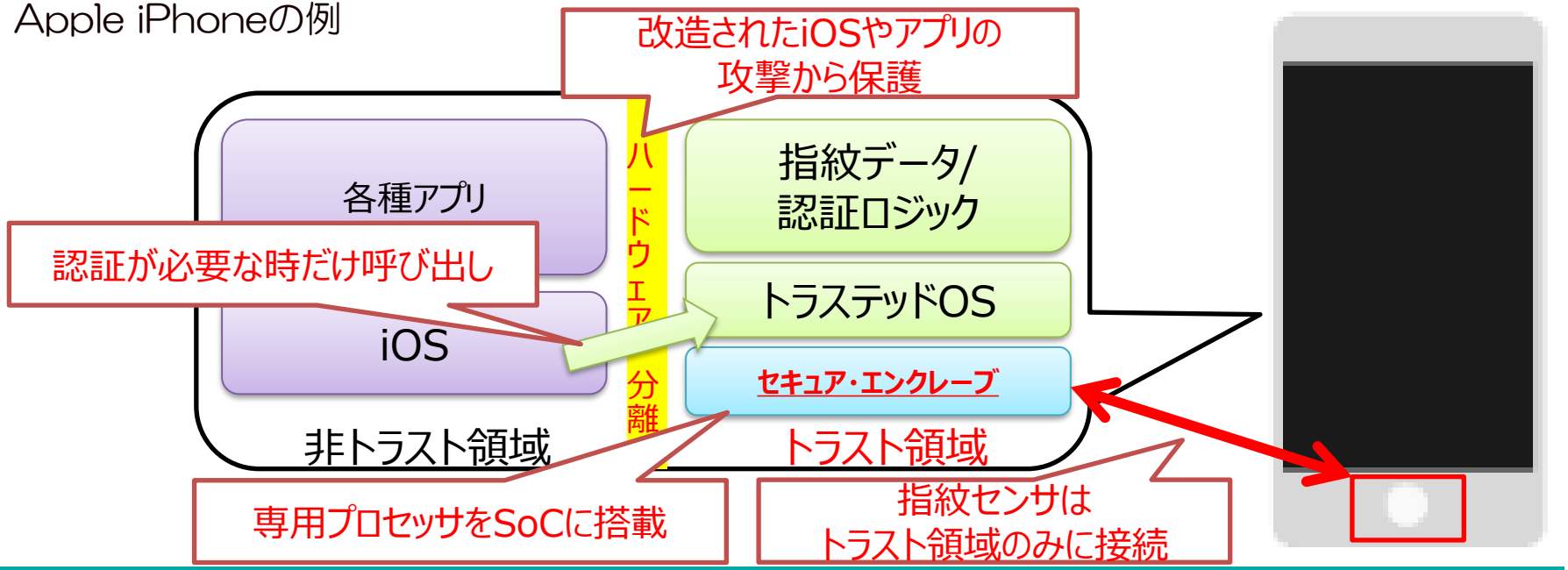
＊＊＊　英語版の最新版は、 Apple Platform Security　February ２０２１だが、ここの記述は同じ

「ハードウェアセキュリティと生体認証: Secure Enclave、専用のAES暗号化エンジン、Touch ID、Face IDなど、Appleデバイスのセキュリティの基盤をなすハードウェア」これの意味するところ

- 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（TEE）
- 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



MacおよびiPadのハードウェアマイク切断

https://support.apple.com/ja-jp/guide/security/secbbd20b00b/1/web/1#spaceexplored

- Apple T2セキュリティチップを搭載したすべてのMacポータブルは、蓋が閉じられるたびにマイクを確実に無効にするハードウェア切断機能を備えています。T2チップを搭載した13インチのMacBook ProおよびMacBook Airコンピュータと15インチのMacBook Proポータブル（2019年以降）では、この切断機能はハードウェアのみに実装されています。macOSでルート権限またはカーネル権限を持つソフトウェアとT2チップ上のソフトウェアも含め、どのソフトウェアも蓋が閉じられているときにはマイクを使用できません。（カメラは、蓋が閉じられているときには視野が完全に覆い隠されるため、ハードウェアで切断されません。）
- 2020年以降のiPadのモデルもハードウェアマイク切断に対応しています。MFI準拠のケース（Appleで販売しているものなど）がiPadに装着され、閉じているときには、マイクがハードウェアで切断されるため、マイクのオーディオデータはどのソフトウェアからも使用できなくなります。iPadOSのルートまたはカーネル権限を使用しても、ファームウェアが危殆化された場合も使用できません。

心電図機能を持ったApple （watch) の場合
Apple Secure Key Store Cryptographic Module, v1.0
FIPS 140-2 Non-Proprietary Security Policy

Apple Watch Series 1 with Apple S1P CPU	SEPOS for S1P under watchOS 4
Apple Watch Series 3 with Apple S3 CPU	SEPOS for S3 under watchOS 4

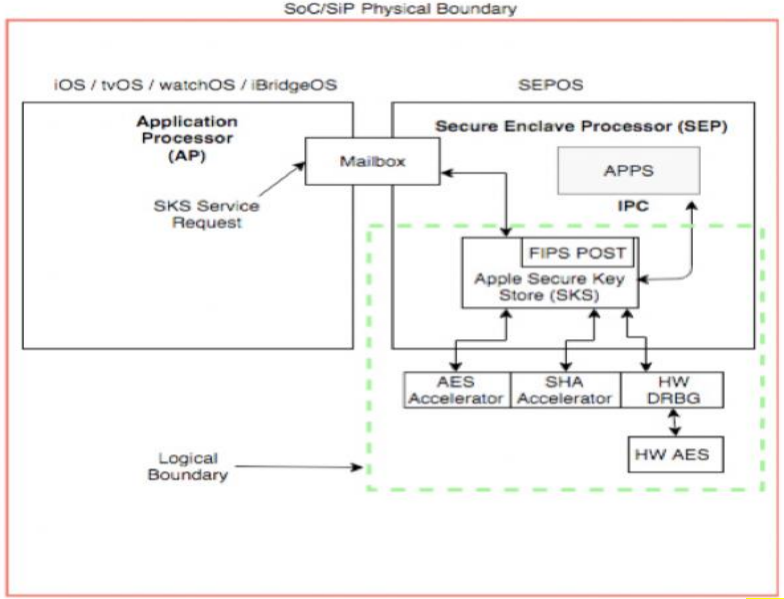


Figure 1: Cryptographic Module Block Diagram

https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3223.pdf

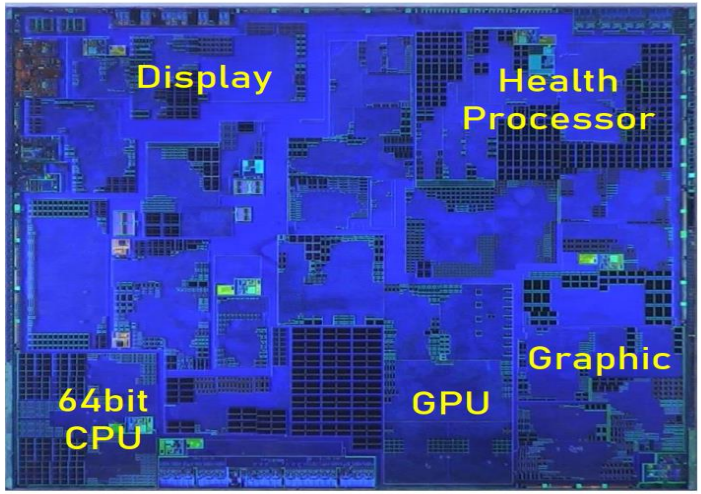
配線層剥離

300φ 1508個
Silicon Cost ¥576

TSMC 10nm Process

CPU
64bit Dual Core
2 x Faster then S3

GPU
Display Controller
Audio Controller
DDR Controller



出典： テカナリエレポート TLSR242号 2018年10月26日

SoCに組み込まれたセキュアエンクレーブ・プロセッサーは、Apple watch を利用する様々なサービス（医療サービスなどの規制産業も含む）にトラストの起点を提供している。

属性証明書とアクセス制御(PMI)

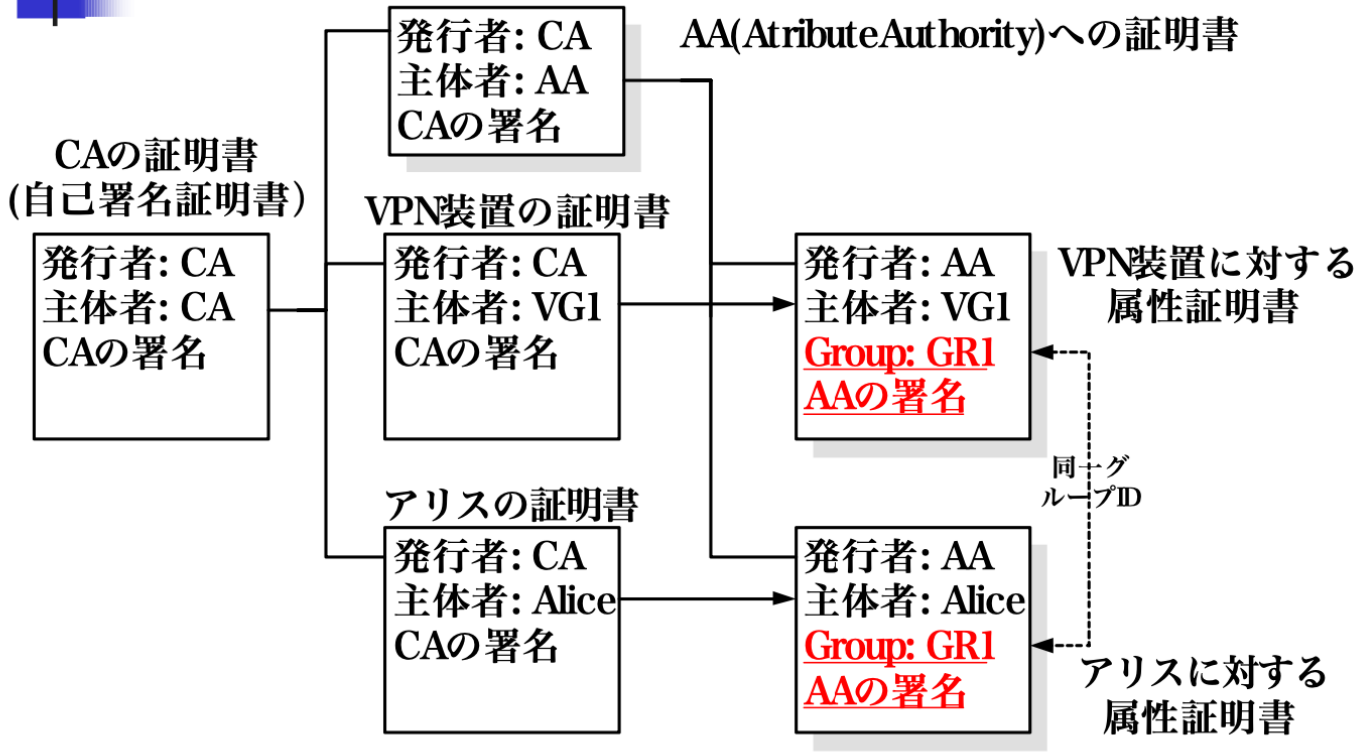
日本インターネット協会(IAJ)セキュリティ部会主催の第2回セキュリティフォーラム
2000年12月7日
https://www.iajapan.org/bukai/isec/forum/2000/20001207report.html

属性証明書とアクセス制御(PMI)

- PMI(権限管理基盤)
  - Privilege Management Infrastructure
  - PMIはユーザーの権限を制御するためのインフラ
- 属性証明書（Attribute Certificate）
  - 属性認証機関(AA)が発行
  - 証明書に添付する主体者の属性を指定
- 公開鍵証明書と属性証明書の関係
  - 公開鍵証明書はパスポートのようなもの
    - 固定的な属性は、公開鍵証明書にも入る
  - 属性証明書はパスポートに添付する査証(ビザ)のようなもの
- 標準的な属性として
  - グループ名
  - 役職名
  - セキュリティ区分などが用意される

日本インターネット協会(IAJ)セキュリティ部会主催の第2回セキュリティフォーラム
2000年12月7日
https://www.iajapan.org/bukai/isec/forum/2000/20001207report.html

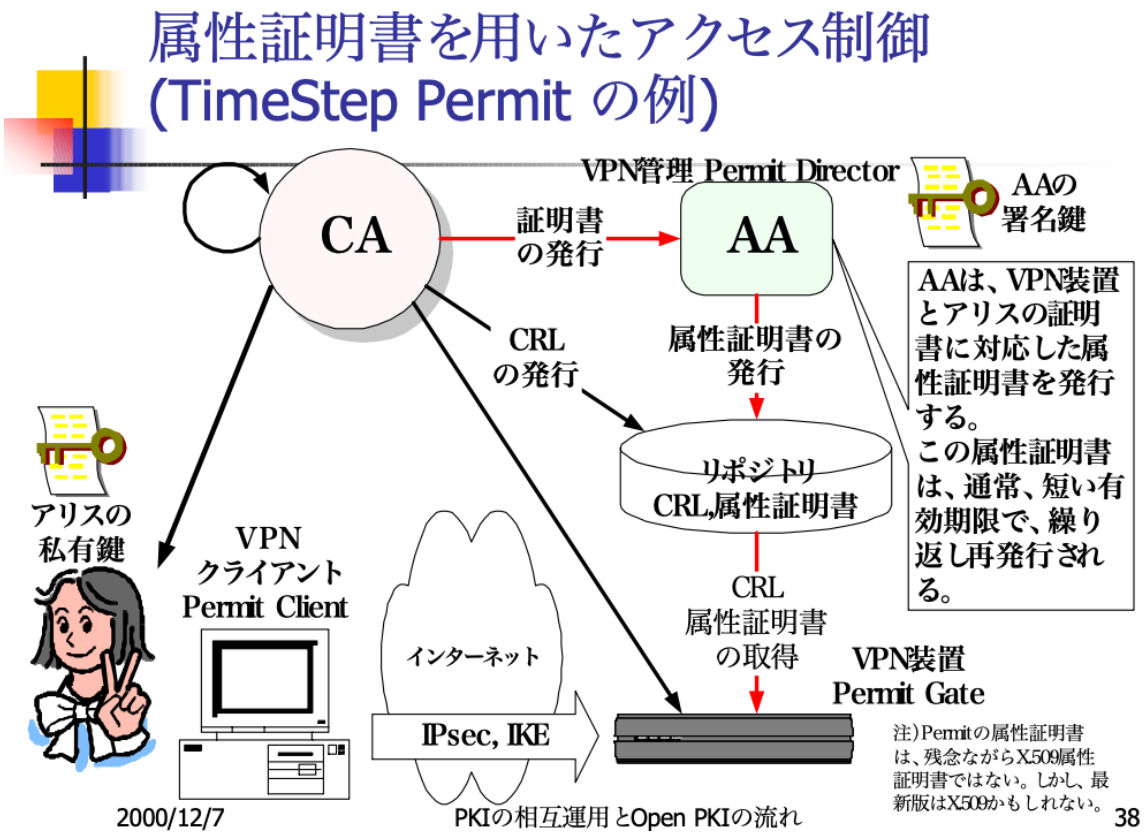
属性証明書を使用したモデル
VPNのアクセス制御の例



2000/12/7 PKIの相互運用とOpen PKIの流れ 37

日本インターネット協会(IAJ)セキュリティ部会主催の第2回セキュリティフォーラム 2000年12月7日
https://www.iajapan.org/bukai/isec/forum/2000/20001207report.html

Don’t Trust, But Verify　の意味するところ
→ 公開鍵暗号の公開鍵（Public key）は、検証鍵（Verification key）



- Verify？？？
  - VPN装置は、FIPS140-2レベル２認証取得（ハードウェアセキュリティを具備している）
  - VPN装置内に格納されたRoot CAの公開鍵（検証鍵）がトラストアンカー
  - Relying Party としてのVPN装置は、トラストアンカー（公開鍵）から検証できる署名データ（公開証明書、属性証明書）以外は信頼しない（ゼロトラスト）。

日本インターネット協会(IAJ)セキュリティ部会主催の第2回セキュリティフォーラム　2000年12月7日
https://www.iajapan.org/bukai/isec/forum/2000/20001207report.html

Trusted party被信頼者　　Relying Party(RP)信頼者