第25回サイバー犯罪に関する白浜シンポジウム テーマ
今こそ考えるサイバー空間の「信頼」
～クラウドセキュリティとゼロトラストネットワーク～

信頼される安心を、社会へ。
SECOM

ゼロトラストにおけるトラスト

2021年5月22日

松本　泰　　セコム株式会社IS研究所

松本の自己紹介　　セコム（株）IS研究所　ディビジョンマネージャー

信頼される安心を、社会へ。
SECOM

- 1984年　UNIX上のビデオテックス・パソコン通信システムの開発に従事
- 1994年　各種インターネットサービスの設計、開発、運用に従事
- 1999年　サイバーセキュリティ事業の立ち上げに従事

ネットワークセキュリティ関係の
設計、開発運用を多く担当した

- 2003年-2007年　工学院大学「セキュアシステム設計技術者の育成」プログラム客員教授
- 2007年　経済産業省 商務情報政策局長表彰「情報セキュリティ促進部門」受賞
- 2007年-2012年　IPA 情報処理推進機構 情報セキュリティ分析ラボラトリー 非常勤研究員
- 2011年-2012年
  - 社会保障・税に関わる番号制度　情報連携基盤技術WG　構成員
  - 社会保障・税に関わる番号制度　社会保障分野サブWG　構成員
- 2013年-2014年
  - 内閣官房　パーソナルデータに関する検討委員会・技術検討WG　構成員
- 2008年-2018年　JDCC 日本データセンター協会　セキュリティWGリーダ
- 2021年4月現在
  - CRYPTREC　暗号技術検討会構成員、暗号技術評価委員会　委員、暗号技術活用委員会　委員
  - 日本ネットワークセキュリティ協会　PKI相互運用技術WGリーダ
  - 日本ネットワークセキュリティ協会　標準化部会　副部会長
  - 日本トラストテクノロジー協議会（2017年11月設立）副代表
  - JST/RISTEX　公私領域アドバイザー
  - QST　SIP光・量子技術評価委員会委員
  - 津田塾大学総合政策学部非常勤講師（情報セキュリティ論）

2001年から

ゼロトラストにおけるトラスト

- ゼロトラストネットワークにおいてNever Trust, Always Verifyの意味するところは、従来トラステッドネットワークとされてきたようなFWにより隔てられた境界内のネットワークなどをNever Trustとして、利用者(サブジェクト)と強く結びついたエッジデバイスをAlways Verifyするというものです。
- このことにより、トラステッドネットワークされてきたものに代わってトラストを形成するのが、ゼロトラストラストアーキテクチャであり、また、同時にトラストアーキテクチャと言えます。
- 先進的なゼロトラストアーキテクチャの実現のためには、エッジデバイス自体にTEE (Trusted Execution Environment)等のトラスト領域が求められますが、このような要求に対応するエッジデバイスを実現するためのプラットフォームセキュリティが近年大きな変化・進化を見せています。
- 本講演では、デジタル時代におけるトラストの役割を説明するともに、その中心的な役割を果たしつつあるエッジデバイス等におけるトラスト、そのためのプラットフォームセキュリティの技術動向について説明します。

2021年4月15日に開催した
PKI & TRUST Days online 2021
「デジタル社会におけるトラスト」「変貌するトラストアーキテクチャ」

https://www.insa.org/seminar/pki-day/2021/index.html - day1

- 講演１　宮澤慎一氏　　セコム（株）IS研究所　主務研究員
  - 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 ～
- 講演２　鈴木研吾氏　　(株)LayerX シニアセキュリティアーキテクト
  - デジタルトラストとゼロトラストネットワーク
- 講演３　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
  - 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　垣内由梨香氏　　Microsoft Corporation セキュリティ レスポンスチーム
  - プラットフォームで実装されるトラスト
- 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　　モデレータ　松本

◇概要
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。

◇キーワード
- 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
- ゼロトラストネットワーク
- コンフィデンシャルコンピューティング

ゼロトラストにおけるトラスト

（1）　トラストの話

（2）　境界線防御におけるトラスト

（3）　PKIとゼロトラスト

（4）　TEE/エンクレーブという（ゼロ）トラスト

（5）　コンフィデンシャル・コンピューティングという（ゼロ）トラスト

（6）　まとめ

トラストの話

「ゼロトラストにおけるトラスト」の前に
トラストについての理解を深める？？

（ゼロトラストの前に）トラストって何よー??

- 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。

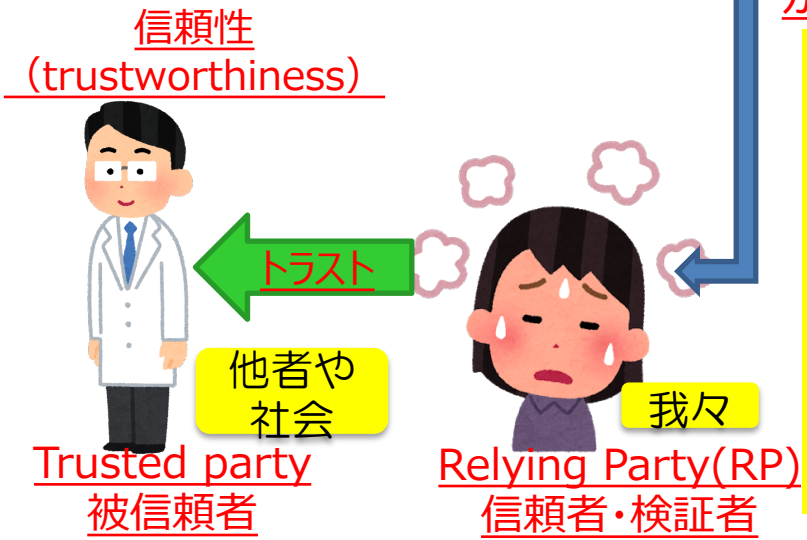
信頼―社会的な複雑性の縮減メカニズム」
https://www.amazon.co.jp/信頼―社会的な複雑性の縮減メカニズム-ニクラス・ルーマン/dp/4326651202

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」

ゼロトラストネットワークのトラスト

信頼される安心を、社会へ。
SECOM

Trusted party
被信頼者

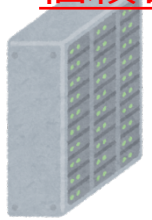
サブジェクト

UnTrusted Network
(ZeroTrust Network)

アセット

Relying Party(RP)
信頼者・検証者

トラスト ・ Always Verify



サブジェクトの
信頼性(Trustworthiness)

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.

サブジェクト情報のインプット

トラストエンジン
PDP：
Policy Decision Point

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

境界線防御におけるトラスト

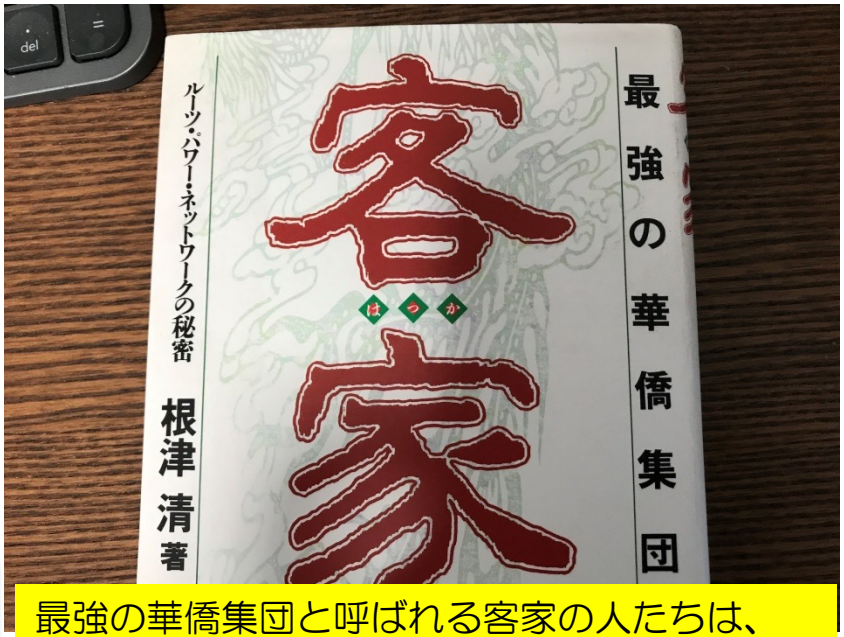
「ゼロトラストネットワークにおけるトラスト」「ゼロトラストにおけるトラスト」の意味するところを浮きぼりにするために
ゼロトラストネットワークと対比される「境界線防御におけるトラスト」を説明

境界線防御とトラストの関係

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信頼者と被信頼者が同居するトラストな領域

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？　->　現在は世界中にネットワークを張り巡らし活躍している？？

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

PKI day 2019

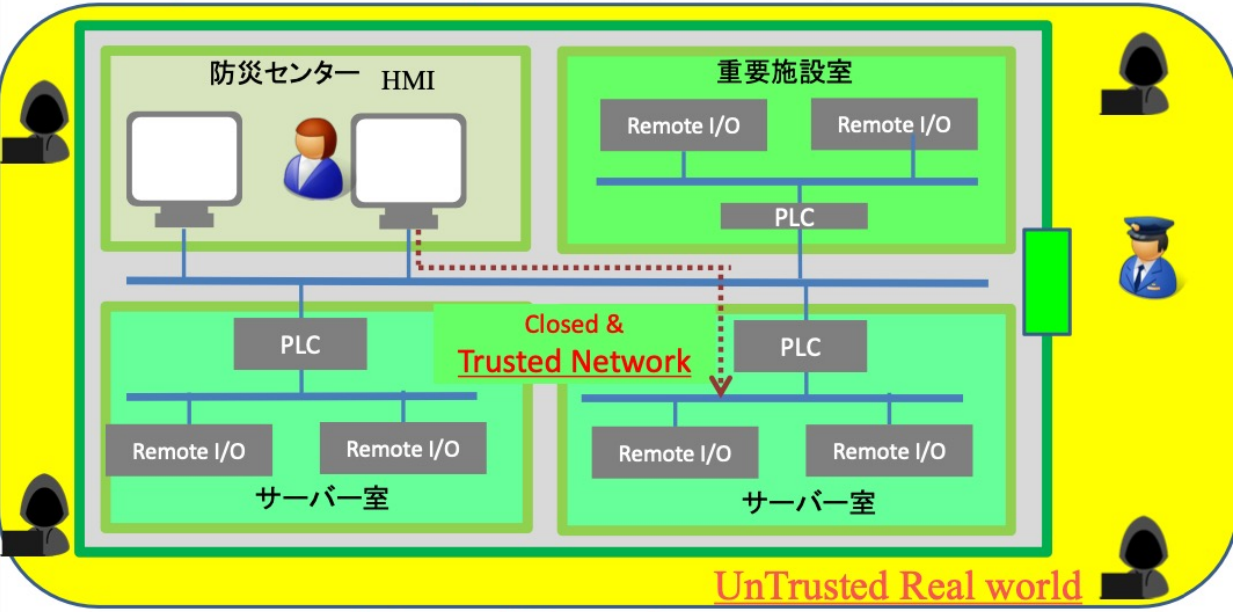
出典：
PKI Day 2019
2019年4月17日
https://www.jnsa.org/seminar/pki-day/2019/data/190417_am05_matsumoto.pdf

信頼される安心を、社会へ。
SECOM

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
- 物理的ゾーニングによる重要区画などのアクセス制御

- 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

境界線防御のトラスト

ZeroTrust Environment??

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

Trusted party
サブジェクト 被信頼者

アセット
(制御機器も
アセット)

Relying
Party(RP)
信頼者・検証者

静的なトラスト？？、暗黙のトラスト？？

信頼者と被信頼者が境界線の中にあればすべて
トラスト

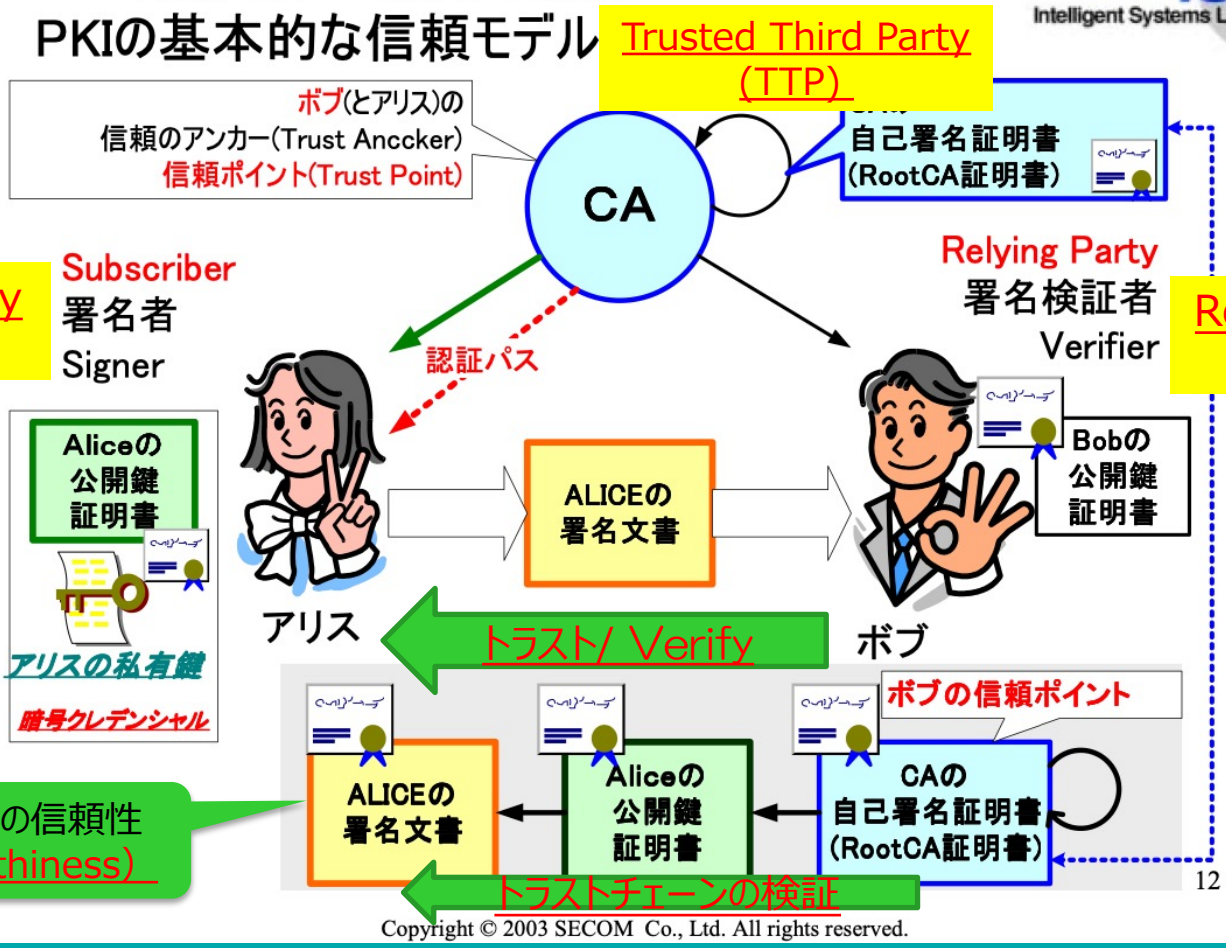
境界線防御・物理的ゾーニングによるトラストからゼロトラストネットワークへ
- 物理的制約などを脱して多様なトラストを実現できる環境・場？？
- 物理的制約などを脱することがイノベーションにつながる。

PKIとゼロトラスト

- 物理的境界・ネットワーク境界を越えるための技術
- ゼロトラストネットワーク・ゼロトラスト環境におかれるデジタル署名が付与されたデータ

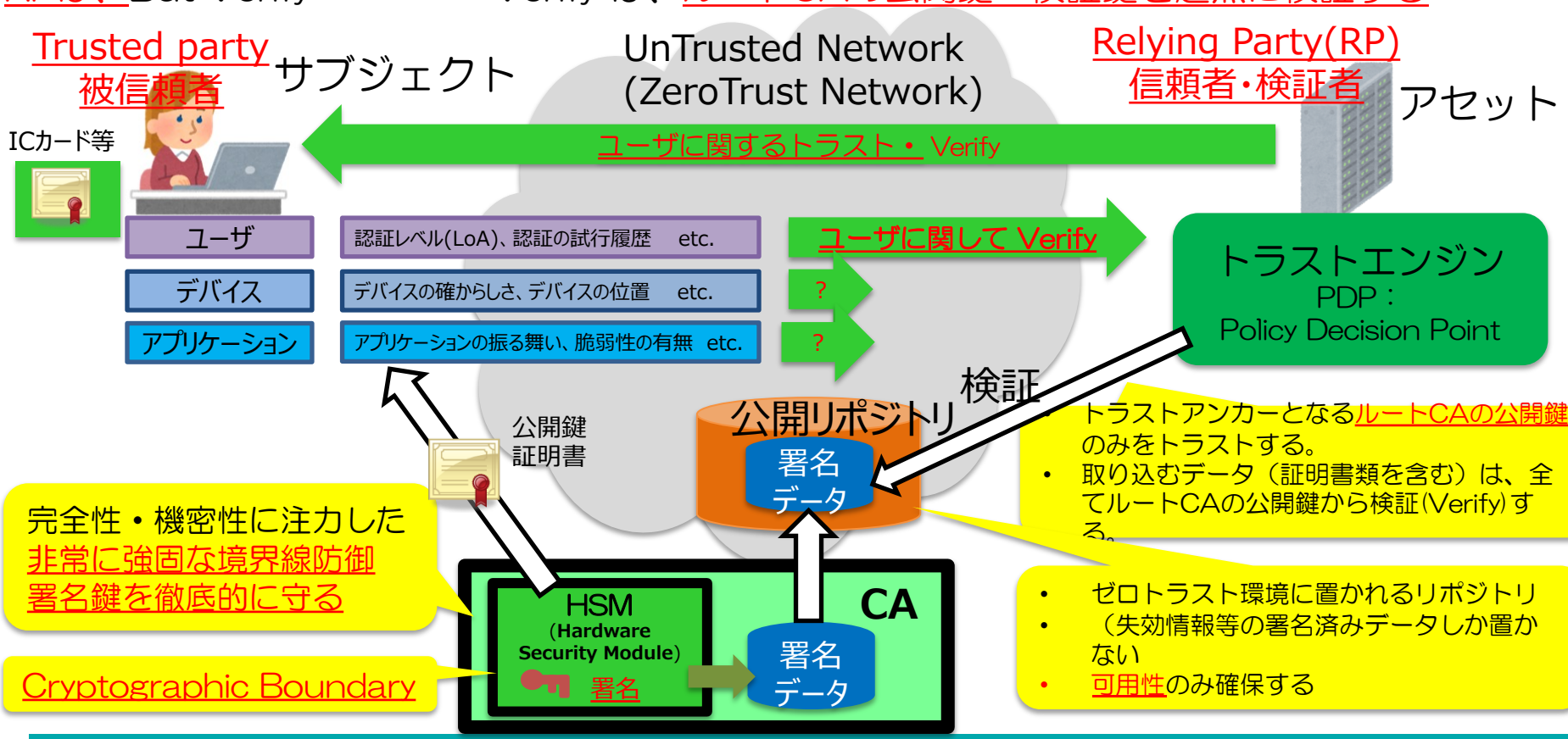
PKIの動向とPKI技術の概要

PKIの基本的な信頼モデル

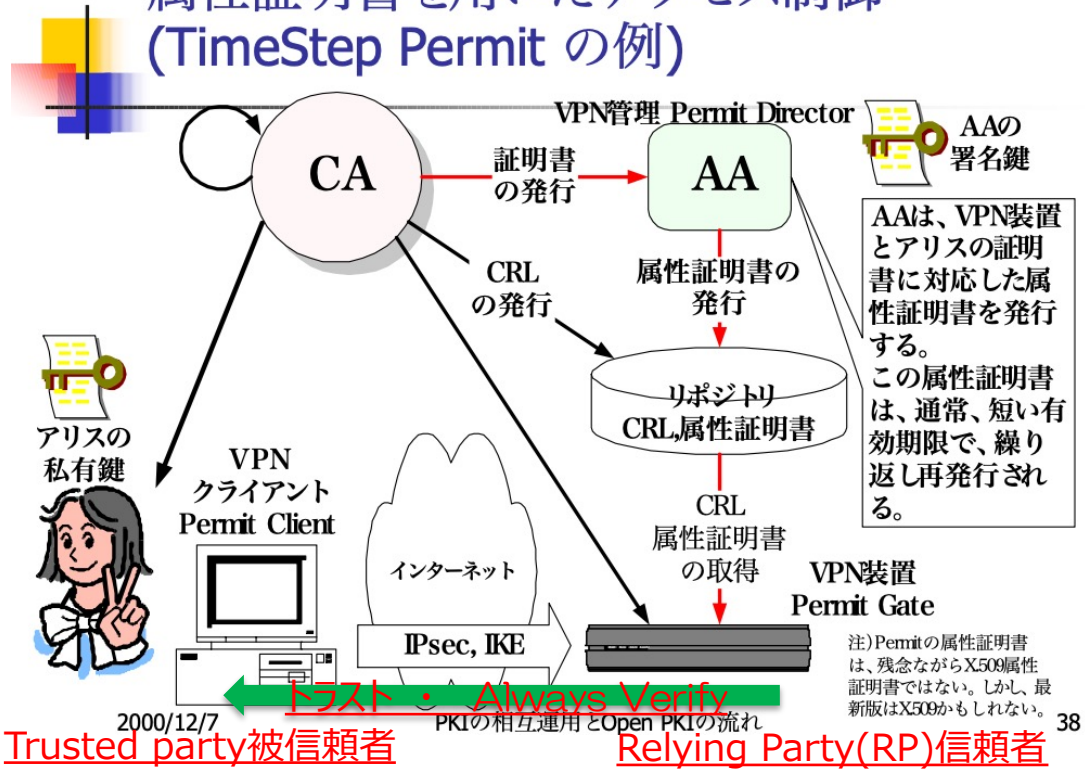


出典：
Internet Week 2003
https://www.nic.ad.jp/ja/materials/iw/2003/proceedings/
PKI ～基礎と応用～
https://www.nic.ad.jp/ja/materials/iw/2003/proceedings/T16-1-1.pdf

PKI は、「物理的境界・ネットワーク境界を越えるための技術・アーキテクチャ」
RPは、Don’t Trust -- しかし、ルートCAの公開鍵・検証鍵は、トラストする。
RPは、But Verify -- Verify は、ルートCAの公開鍵・検証鍵を起点に検証する



Never Trust, Always 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

TEE/エンクレーブという（ゼロ）トラスト

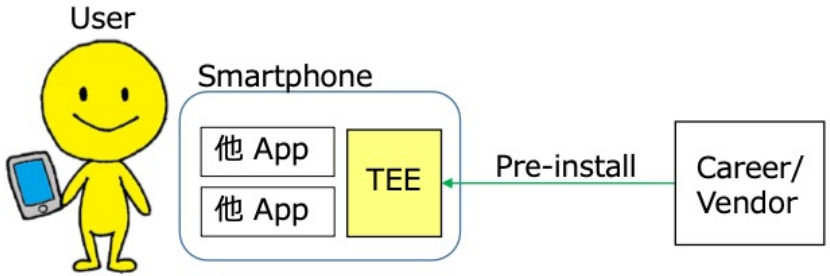
- TEE(Trusted Execution Environment)という境界線防御で守られた場所
- エンクレーブ(飛び地)という遠方の境界線

はじめに（続）

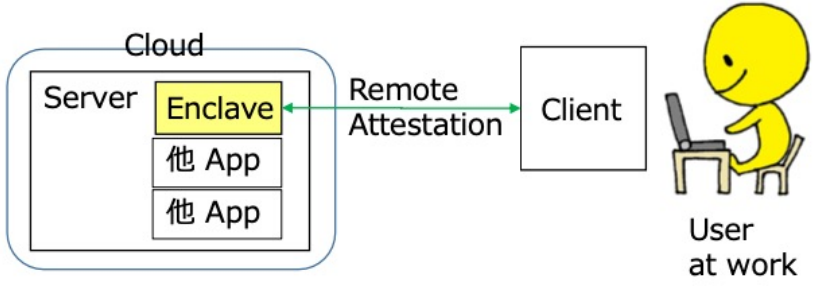
ざっくり言うと・・・

※詳細は PKI & Trust Days 2021
セコム 宮澤慎一 先輩の資料をどうぞ
「トラストを確立する技術の概要」

TEEは、Career/Vendorから見て
スマホ等端末上の“Trusted”な領域。
他Appから論理的に隔離されており、
ユーザは認証情報等の保管に使える。



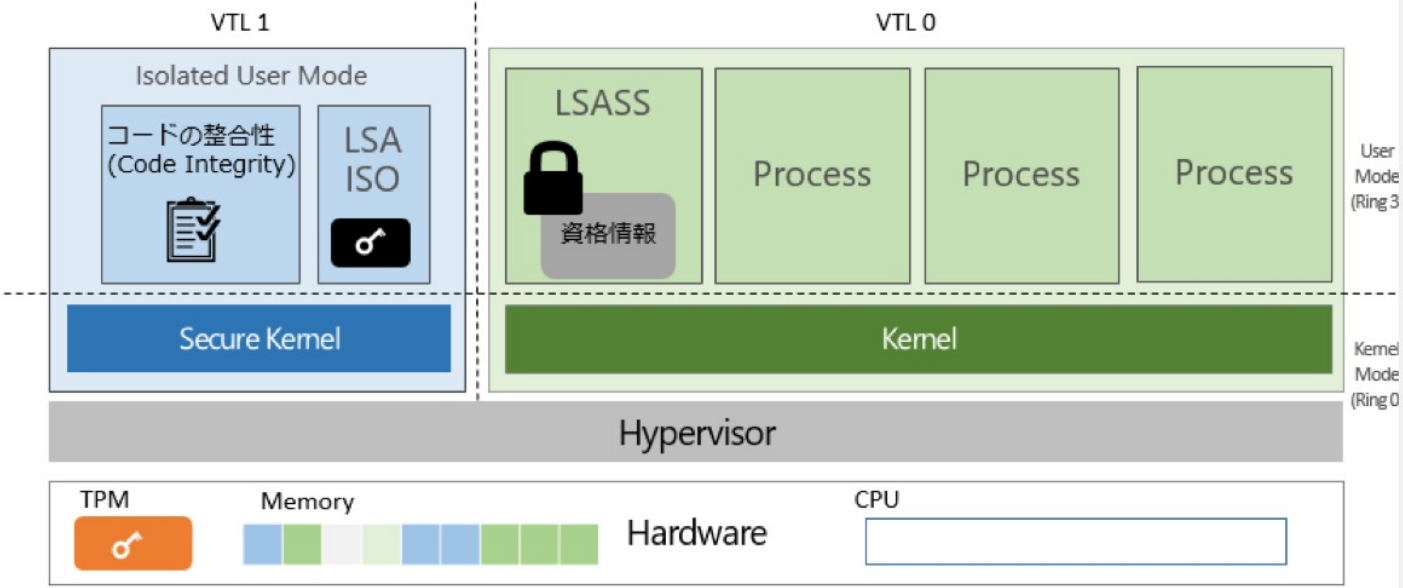
Enclave(飛び地)は、法人ユーザから見て、
クラウド/サーバ上の“Trusted”な領域。
機密なアプリ&データを、他Appから隔離して、
Confidentiality & Integrity に実行できる



出典： PKI & TRUST Days online 2021　「デジタル社会におけるトラスト」
第１日目：2021年4月15日（木）テーマ：変貌するトラストアーキテクチャ
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）
https://www.insa.org/seminar/pki-day/2021/data/0415okuda.pdf

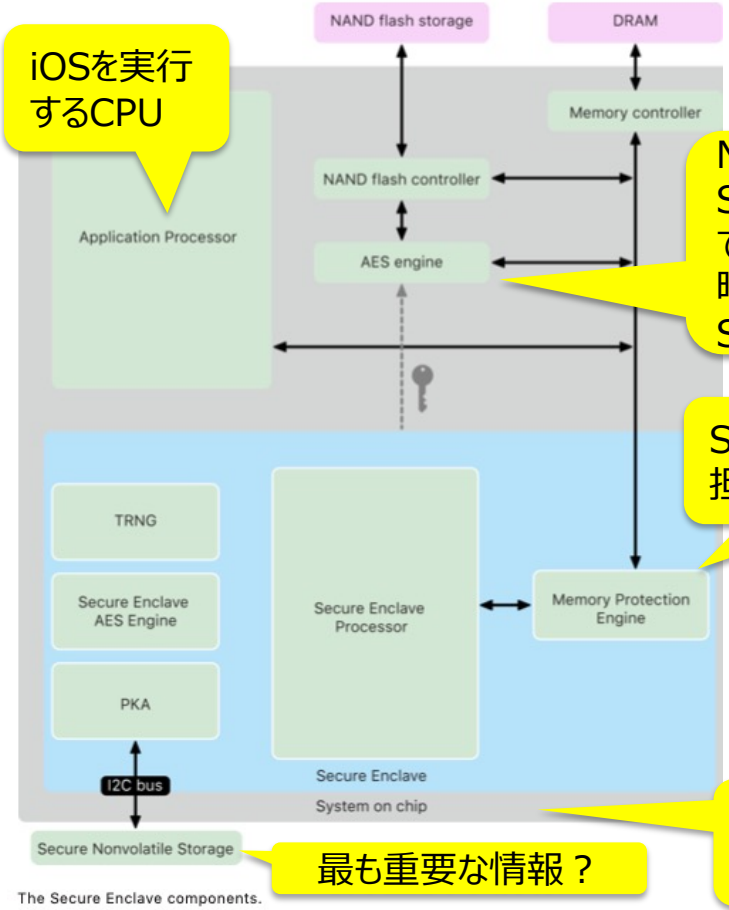
Virtualization-based security (VBS)

- Windows 10+ の多くのセキュリティ機能の基礎
- Hypervisor, SLAT, IOMMUをベースとした仮想化による保護技術



出典： PKI & TRUST Days online 2021　「デジタル社会におけるトラスト」
第１日目：2021年4月15日（木）テーマ：変貌するトラストアーキテクチャ
「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　セキュリティ プログラム マネージャー）
https://www.insa.org/seminar/pki-day/2021/data/0415_kakiuchi.pdf

Apple のSEP:セキュアエンクレーブプロセッサー？？



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

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

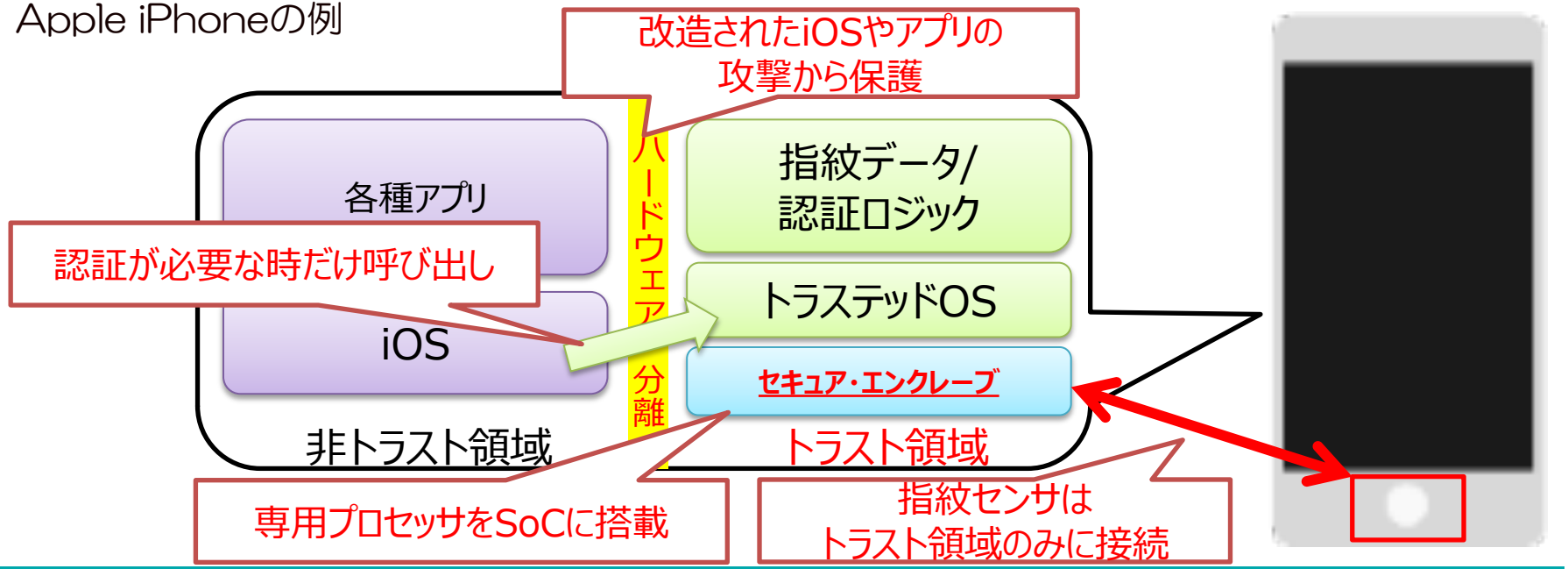
- ハードウェアセキュリティと生体認証: Secure Enclave、専用のAES暗号化エンジン、Touch ID、Face IDなど、Appleデバイスのセキュリティの基盤をなすハードウェア。
- システムのセキュリティ: 安全な起動（safe boot）、アップデート、およびAppleのオペレーティングシステムの継続的な動作を可能にする、 統合されたハードウェア機能とソフトウェア機能。
- 暗号化とデータ保護: デバイスを紛失したり盗まれたりした場合や、不正なユーザまたはプロセス（unauthorised person or process）が使用したり変更したりし ようとした場合でもユ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。

「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



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」

信頼される安心を、社会へ。 SECOM

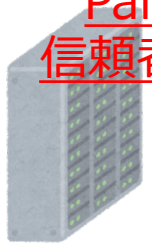
Trusted party
被信頼者

サブジェクト

ZeroTrust Environment??

アセット

Relying Party(RP)
信頼者・検証者



トラスト ・ Always Verify

TEE（Trusted Execution Environment）

ユーザ

認証

ユーザ（ローカル）認証
認証レベル(LoA)、認証の試行履歴 etc.

デバイス

検証

リモートアテステーション
デバイスの確からしさ、デバイスの位置 etc.

リモートアテステーション

トラストエンジン
PDP：
Policy Decision Point

アプリケーション

監視

アプリケーション監視
アプリケーションの振る舞い、脆弱性の有無 etc.

OS

Chain Of Trust

トラステッドOS

(ユーザ所有の)
デバイス

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

- 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
- サブジェクトの信頼性(Trustworthiness)をVerifyし、リモートアテステーションでトラストエンジンに伝える。

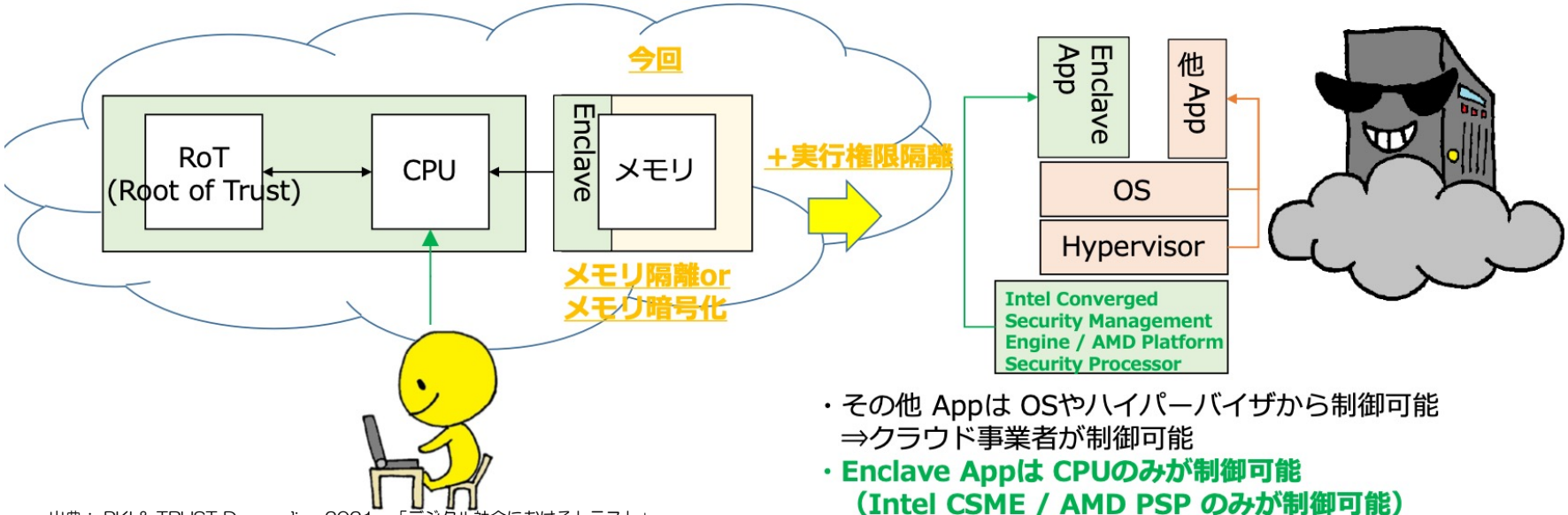
コンフィデンシャルコンピューティングという（ゼロ）トラスト

CPUに組み込まれるトラスト

Confidential Computing とは

“CPUのみ”がアプリ&データを制御可能なクラウド環境
↑**(1)CPUの階層的な権限制御(リングプロテクション)の効果！**

Thanks
セコム 宮澤さん！

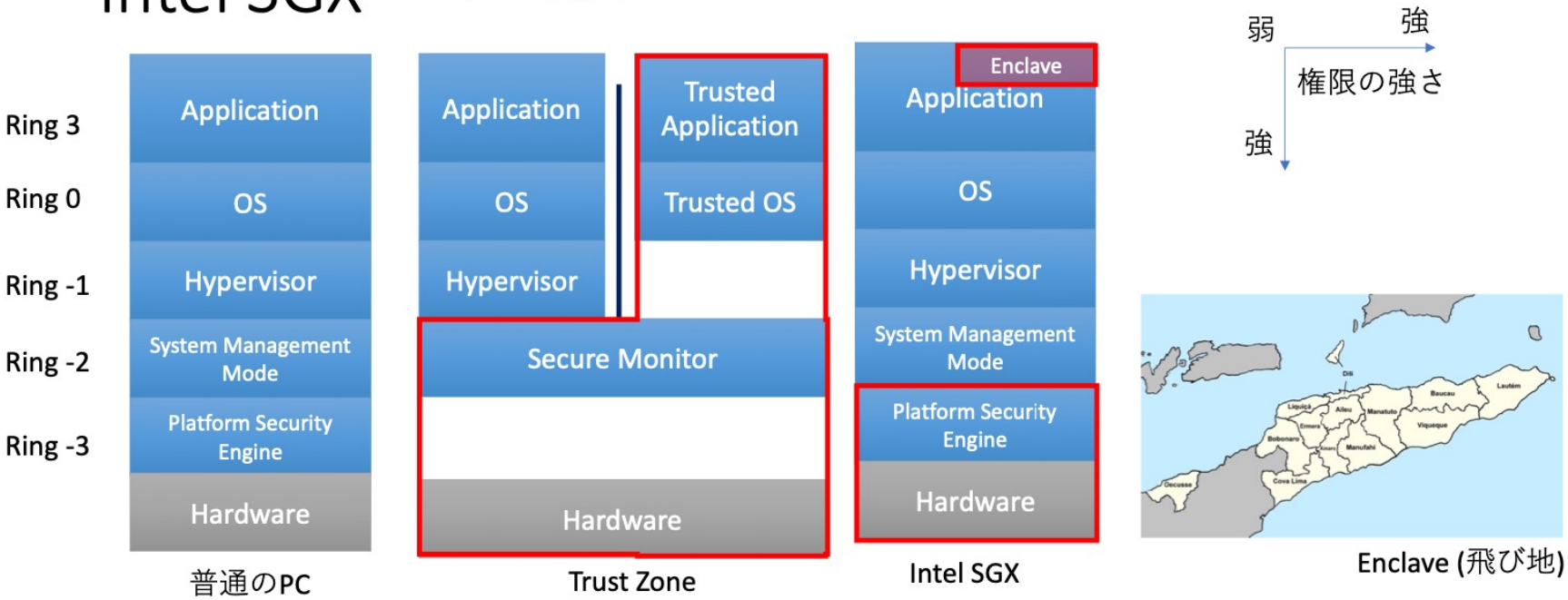


・その他 Appは OSやハイパーバイザから制御可能
⇒クラウド事業者が制御可能
・**Enclave Appは CPUのみが制御可能**
（Intel CSME / AMD PSP のみが制御可能）
⇒クラウド事業者は制御不可
（OSやハイパーバイザから制御不可）

出典： PKI & TRUST Days online 2021 「デジタル社会におけるトラスト」
第1日目：2021年4月15日（木）テーマ：変貌するトラストアーキテクチャ
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）
https://www.insa.org/seminar/pki-day/2021/data/0415okuda.pdf

Intel SGX

詳しくは後半で！



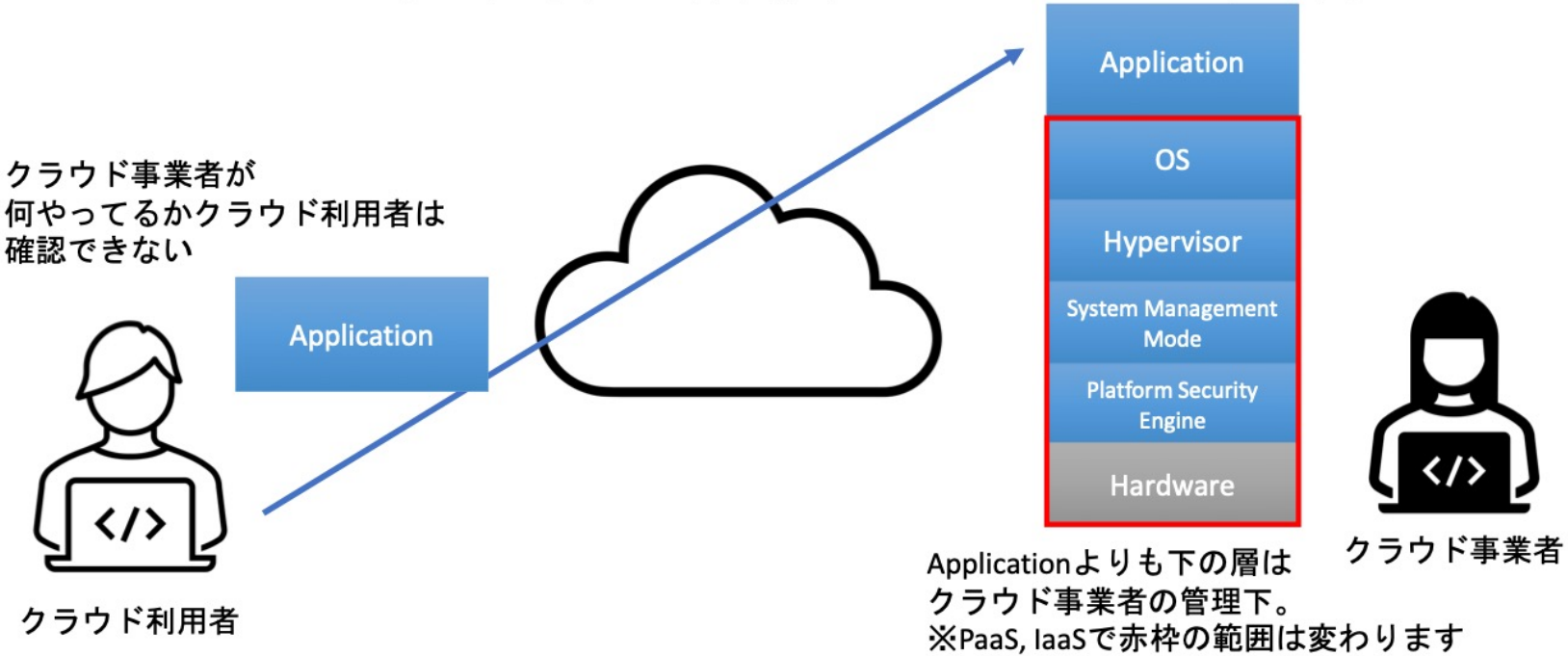
Enclave (飛び地)

※アプリケーション開発者（利用者）は赤枠を信頼する必要がある。

"Locator map of municipalities of East Timor"© J. Patrick Fischer (Licensed under CC BY 4.0)

出典： PKI & TRUST Days online 2021　「デジタル社会におけるトラスト」
第1日目：2021年4月15日（木）テーマ：変貌するトラストアーキテクチャ
「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（セコム株式会社 IS研究所 主務研究員）
https://www.insa.org/seminar/pki-day/2021/data/0415miyazawa.pdf

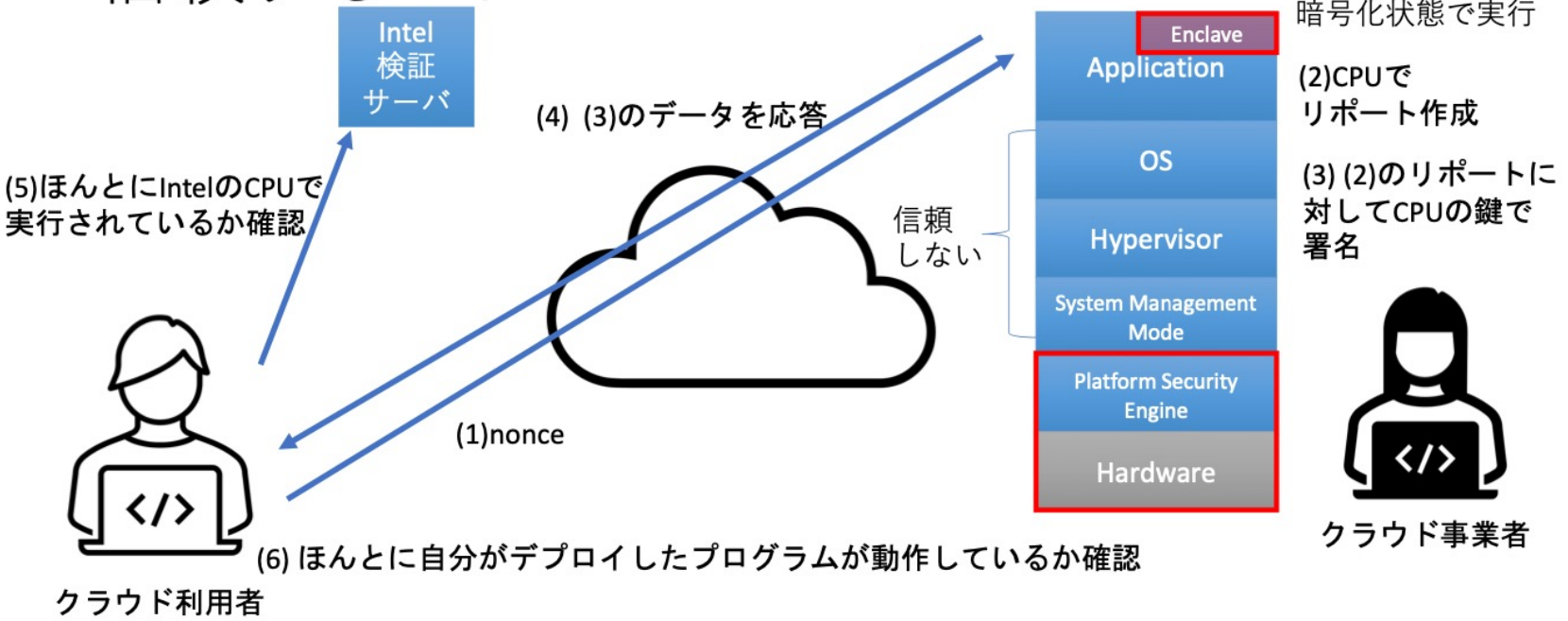
2000年後半以降のクラウドの普及
クラウド事業者を信頼してアプリ実行



2021/04/15

出典： PKI & TRUST Days online 2021　「デジタル社会におけるトラスト」
第１日目：2021年4月15日（木）テーマ：変貌するトラストアーキテクチャ
「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（セコム株式会社 IS研究所 主務研究員）
https://www.insa.org/seminar/pki-day/2021/data/0415miyazawa.pdf

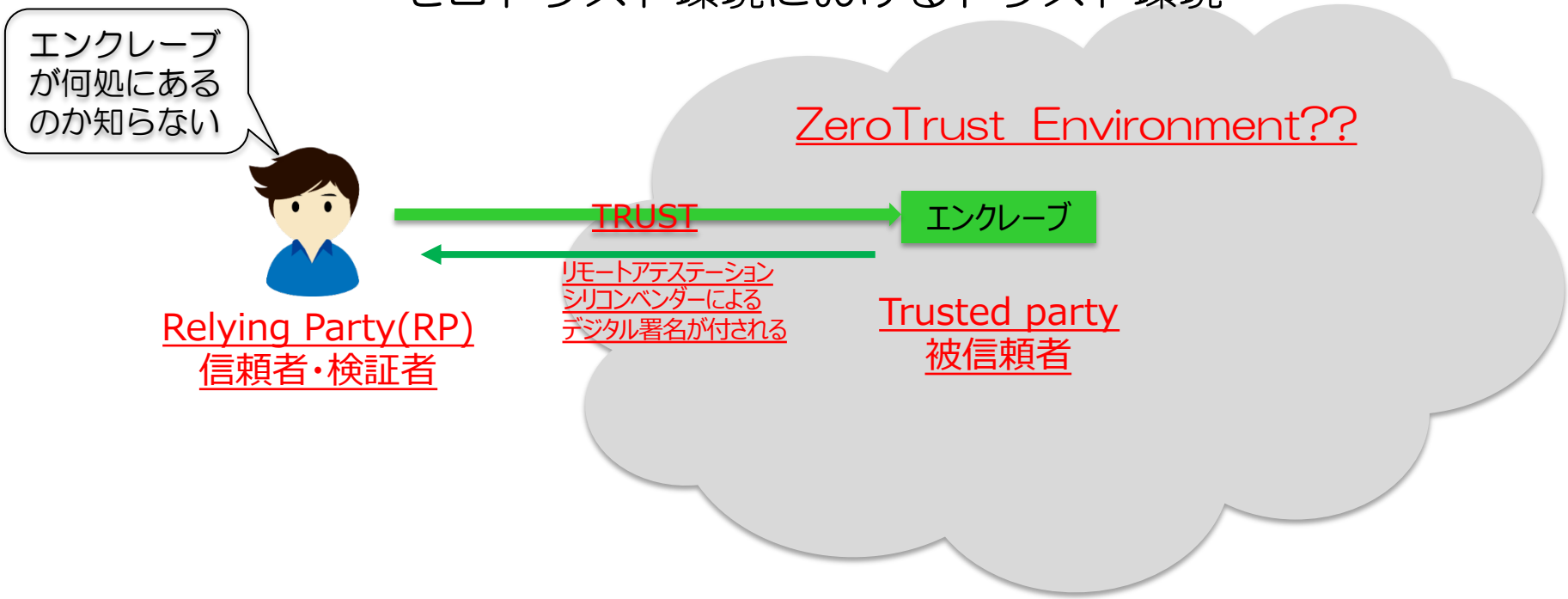
クラウド事業者よりもチップベンダーを信頼するモデル



出典： PKI & TRUST Days online 2021　「デジタル社会におけるトラスト」
第１日目：2021年4月15日（木）テーマ：変貌するトラストアーキテクチャ
「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（セコム株式会社 IS研究所 主務研究員）
https://www.insa.org/seminar/pki-day/2021/data/0415miyazawa.pdf

ゼロトラストにおけるトラスト

雲の中の「トラスト（エンクレーブ）」
→　ゼロトラスト環境におけるトラスト環境



まとめ

まとめ

- ゼロトラストネットワークでは、ネットワークを流れるトランザクションをNever Trustとして、 Always Verifyする。
- しかし、Relying Party(RP：トラストエンジン)が、「**全てを**Never Trust 」ではなく、最もトラスト出来るもの（Root CAの公開鍵・検証鍵など）をトラストアンカーとして、Trusted partyであるサブジェクトをVerifyする。
- そうした中、 TEE（Trusted Execution Environment)/エンクレーブは、ゼロトラストネットワークで利用されるデバイスにおいて重要な技術となりつつある。
- TEE/エンクレーブに関する技術は、近年急速に進歩しており、ゼロトラストネットワークから、さらにネットワーク以外も含めゼロトラスト環境におけるトラストを確立する方向にあり、ゼロトラストの意味するとことも変えていくことになるだろう。

付録

- Appleの場合
- 属性証明書とアクセス制御(PMI)

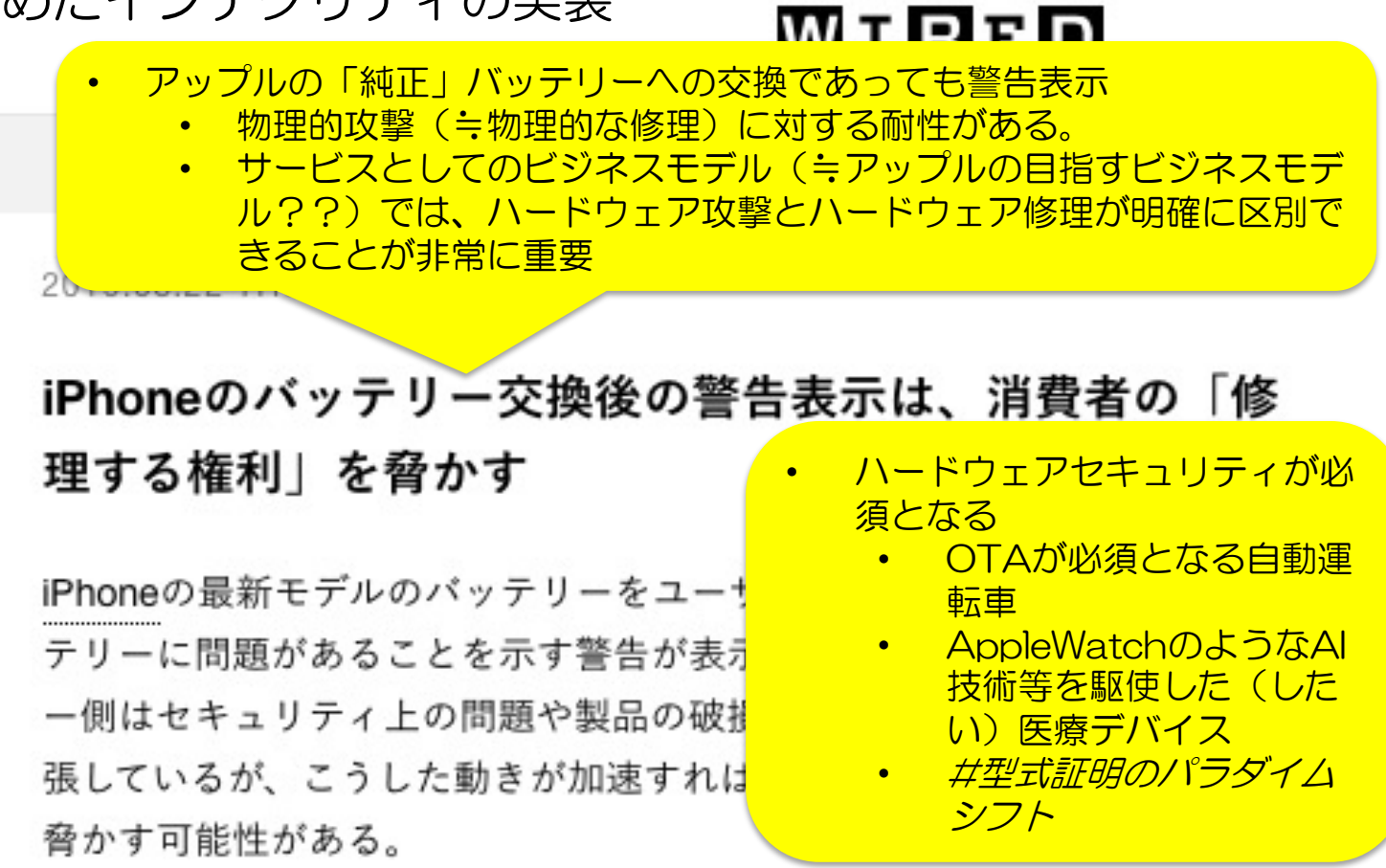
Appleの場合

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



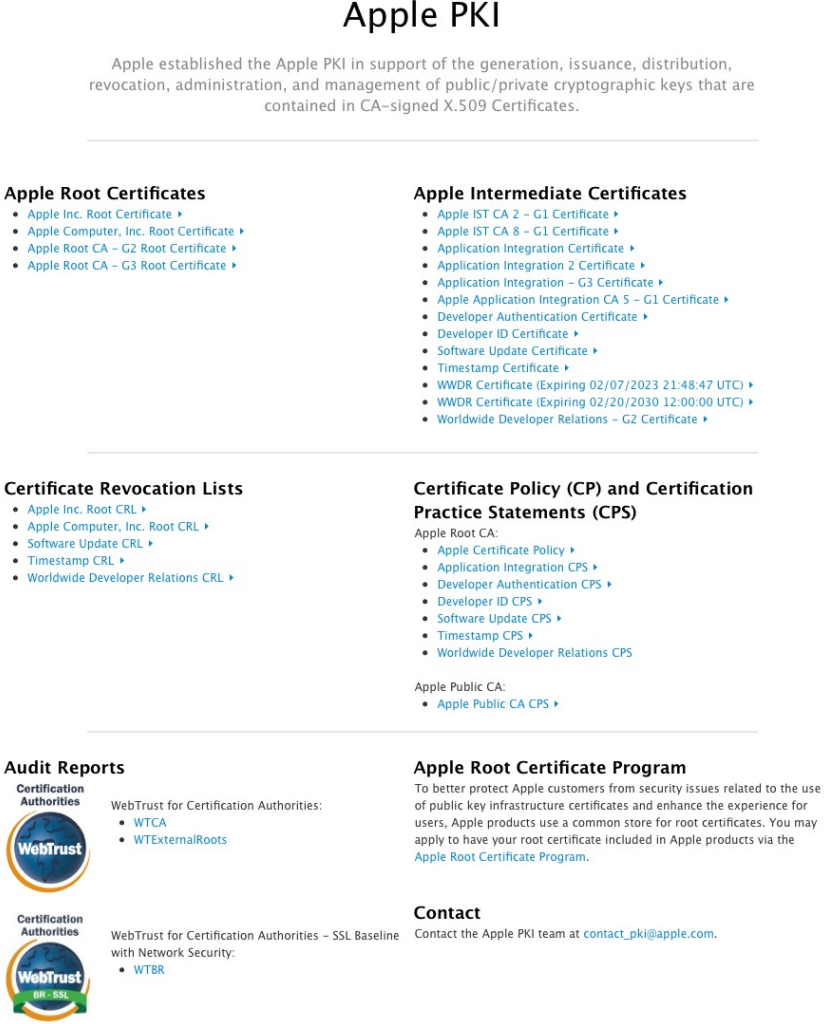
出典：iPhoneのバッテリー交換後の警告表示は、消費者の「修理する権利」を脅かす
https://wired.jp/2019/08/22/apple-iphone-battery-service-alerts/

- 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.

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

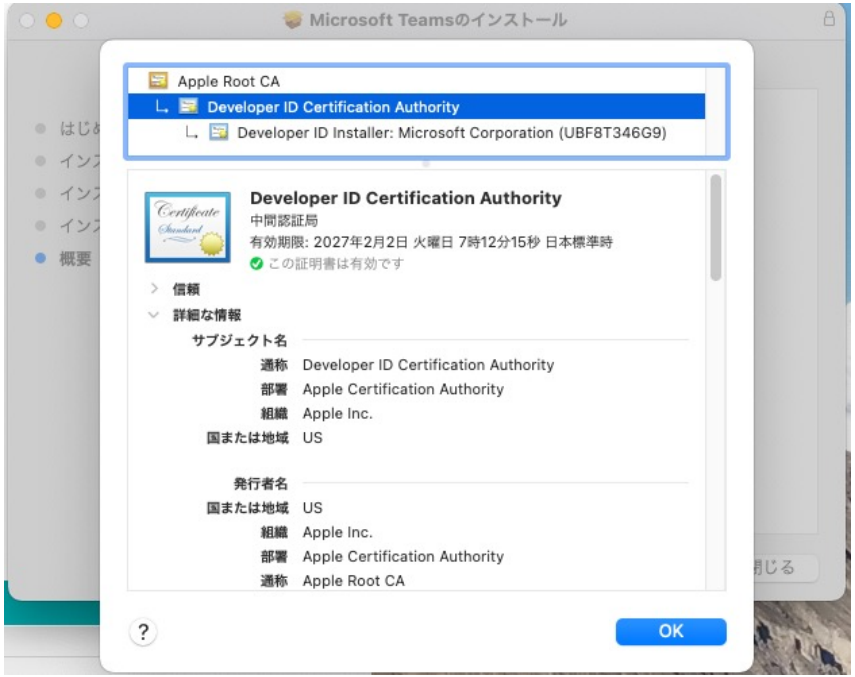
2.2. COMMUNITY AND APPLICABILITY

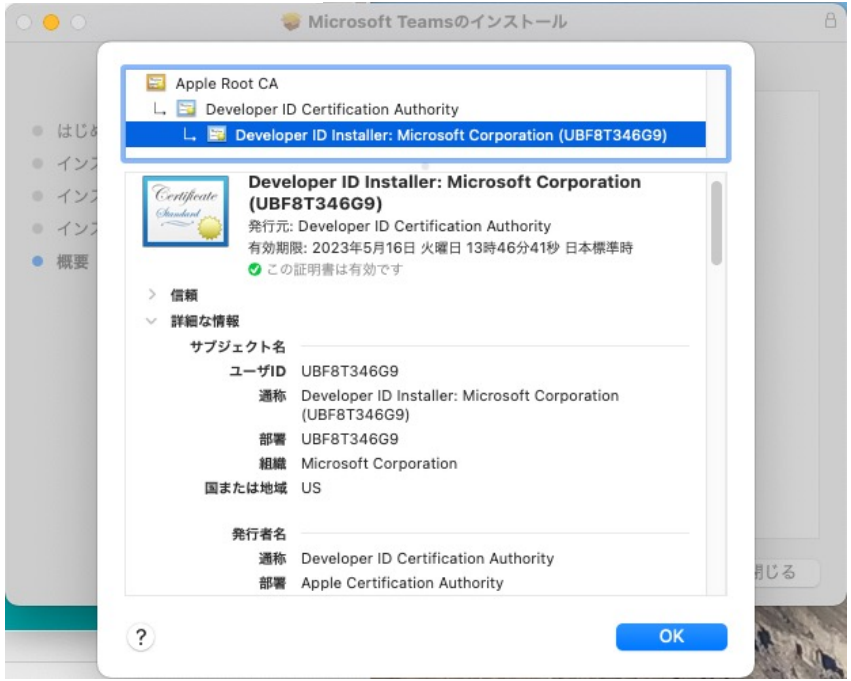
This CPS is applicable to the following certificates issued by the Developer ID Sub-CA:

- 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。

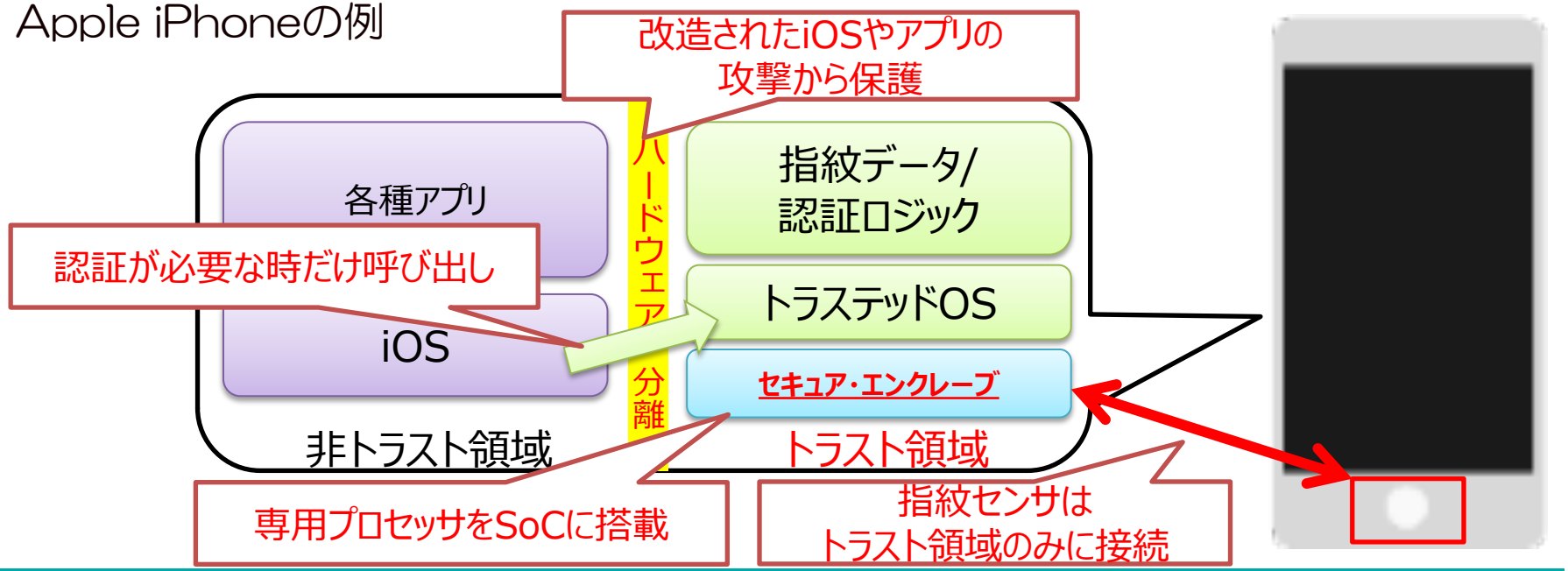
Hardware Security and Biometricsの意味するところ

信頼される安心を、社会へ。
SECOM

- 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



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

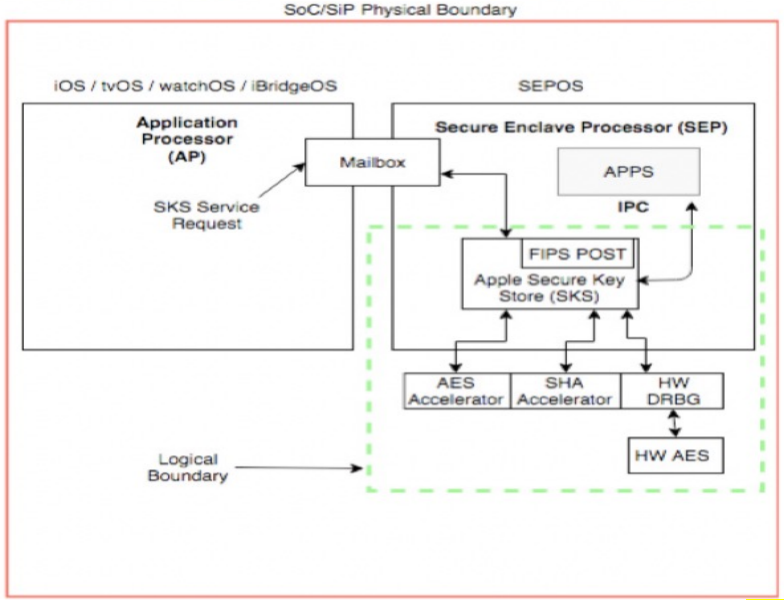


Figure 1: Cryptographic Module Block Diagram

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

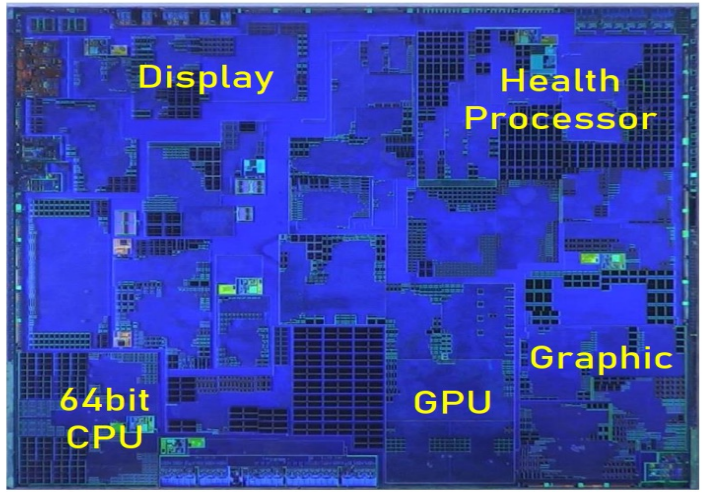
配線層剥離

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

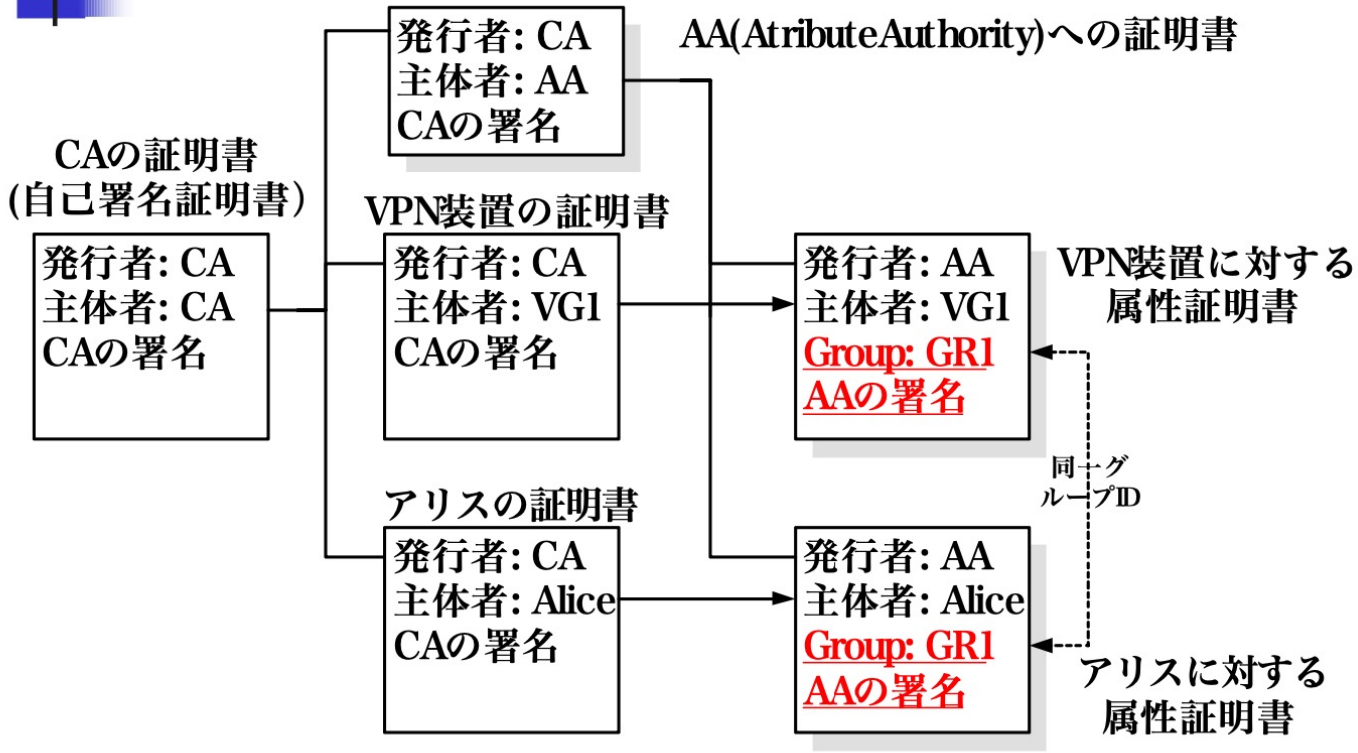
属性証明書とアクセス制御(PMI)

- 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

2000/12/7 PKIの相互運用とOpen PKIの流れ 36

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

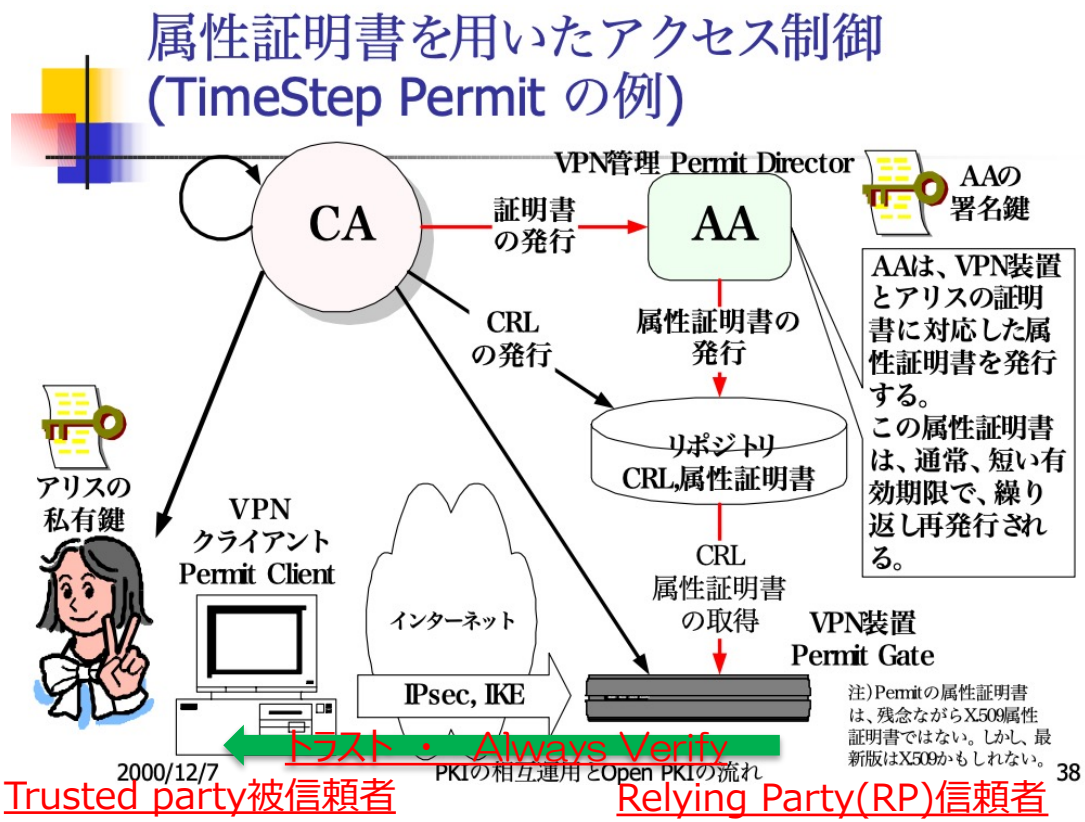
属性証明書を使用したモデル
VPNのアクセス制御の例



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

Never Trust, Always 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