IEICE DPF研究会 2021

Trustを巡る技術動向
～Confidential Computingを中心に～

NTTセキュアプラットフォーム研究所
奥田哲矢

自己紹介

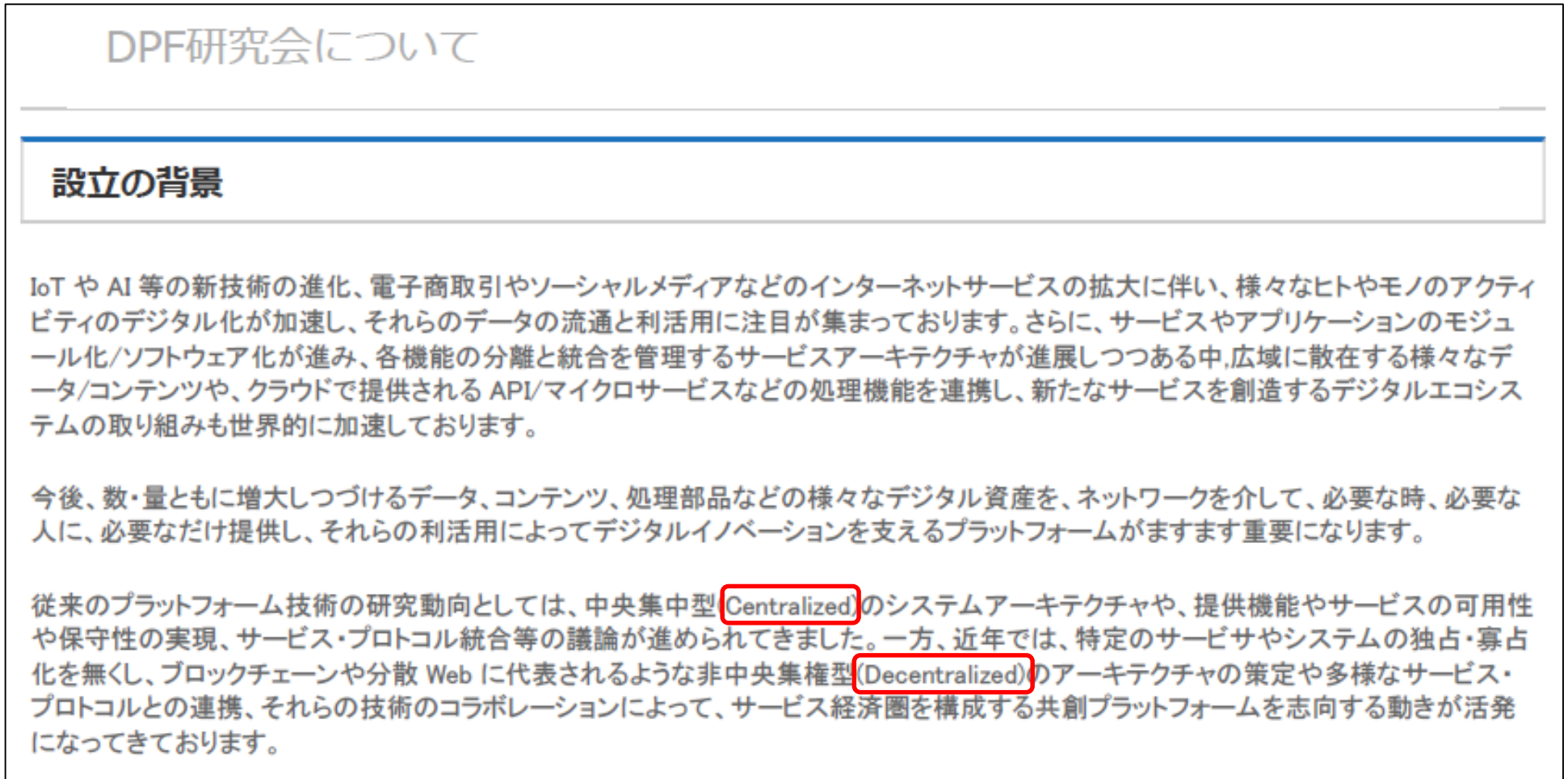
(元々) ポータルサイト**goo**でPM&SE(エンジニア)を4年

(3-4年前) **SSL/TLS** 執筆 & 事業問合せ窓口
OAuth & OpenID Connect 後輩指導しながら勉強
TEE (OpenEnclave etc.) 後輩指導しながら勉強

(直近) TEEプロトコル開発 & 事業導入
社内ではトラスト基盤SGを名乗る

今回の招待講演を頂いて(1/3)

「何を話そうかなぁ」→ DPF研究会様の設立趣旨に
“Centralized”, “Decentralized” があるなぁ。これにしよう。



DPF研究会について

設立の背景

IoT や AI 等の新技術の進化、電子商取引やソーシャルメディアなどのインターネットサービスの拡大に伴い、様々なヒトやモノのアクティビティのデジタル化が加速し、それらのデータの流通と利活用に注目が集まっております。さらに、サービスやアプリケーションのモジュール化/ソフトウェア化が進み、各機能の分離と統合を管理するサービスアーキテクチャが進展しつつある中,広域に散在する様々なデータ/コンテンツや、クラウドで提供される API/マイクロサービスなどの処理機能を連携し、新たなサービスを創造するデジタルエコシステムの取り組みも世界的に加速しております。

今後、数・量ともに増大しつづけるデータ、コンテンツ、処理部品などの様々なデジタル資産を、ネットワークを介して、必要な時、必要な人に、必要なだけ提供し、それらの利活用によってデジタルイノベーションを支えるプラットフォームがますます重要になります。

従来のプラットフォーム技術の研究動向としては、中央集中型(Centralized)のシステムアーキテクチャや、提供機能やサービスの可用性や保守性の実現、サービス・プロトコル統合等の議論が進められてきました。一方、近年では、特定のサービサやシステムの独占・寡占化を無くし、ブロックチェーンや分散 Web に代表されるような非中央集権型(Decentralized)のアーキテクチャの策定や多様なサービス・プロトコルとの連携、それらの技術のコラボレーションによって、サービス経済圏を構成する共創プラットフォームを志向する動きが活発になってきております。

今回の招待講演を頂いて(2/3)

「何を話そうかなぁ」→ DPF研究会様の設立趣旨に

「デジタルサービスやコンテンツを、欧州域内の国境を越えて流通するデジタル市場構築を政策目標とし、GDPRを始めデータ保護法制の整備が進められています。」とあるなぁ。これも話そう。

「DPF研究会について」より抜粋

世界レベルの研究動向を鑑みると、欧州では、デジタルサービスやコンテンツを、欧州域内の国境を越えて流通するデジタル市場構築を政策目標とし、GDPR を始めデータ保護法制の整備が進められています。現在は、欧米を中心として分散型プラットフォームの研究も強く志向されており、我が国においても同分野の国際競争力の強化が求められています。したがって、この特別研究専門委員会を通じ、我が国における幅広いコミュニティーの叡智を結集させることで、プラットフォーム技術/サービスネットワーク技術に対する研究開発を強化・活性化し、国際競争力を高め、欧米に並ぶ研究開発拠点としての我が国の地位確立を目指していく必要があります。

上記の背景に基づきデジタルサービス・プラットフォーム技術特別研究専門委員会の活動を行って参ります。本特別研究委員会は、デジタルサービスを支えるプラットフォーム技術とサービスネットワーク技術を主体的に捉え、次世代のネットワーク基幹技術となる新領域の技術研究を推進/発展させて参ります。具体的な社会実践と実用サービスへの適用を考慮したサプラットフォーム技術/サービスネットワーク技術の研究開発を活性化し、今後の社会展開を目指します。本特別研究専門委員会は、平成 31 年 5 月 1 日に設立し、平成 33

今回の招待講演を頂いて(3/3)

「何を話そうかなぁ」→ DPF研究会様の講演依頼文より

「セキュリティ特集」の研究会

テーマ：　データ活用、プライバシー、セキュリティ、トラスト
（サプライチェーン情報管理、分散暗号、サイバー・フィジカルセキュリティ
デジタル庁関連、IPFS（分散WEB）、Trusted WEB）

→データ活用, トラストを中心に、
サプライチェーン, Trusted Webを含めて喋ろう。

自己紹介（続き）

特集：ウェブを基盤とした社会
Webを支える通信技術～SSL/TLS，PKI，トラスト～
奥田 哲矢(https://www.jstage.jst.go.jp/search/global/_search/-char/ja?item

【自身と”Centralized”の関わり】

・「Webを支える通信技術～SSL/TLS, PKI, トラスト～」, 2020年4月.
・ Internet Week 2018/2019仙台にて、WebPKIに関する招待講演

【自身と”Decentralized”との関わり】

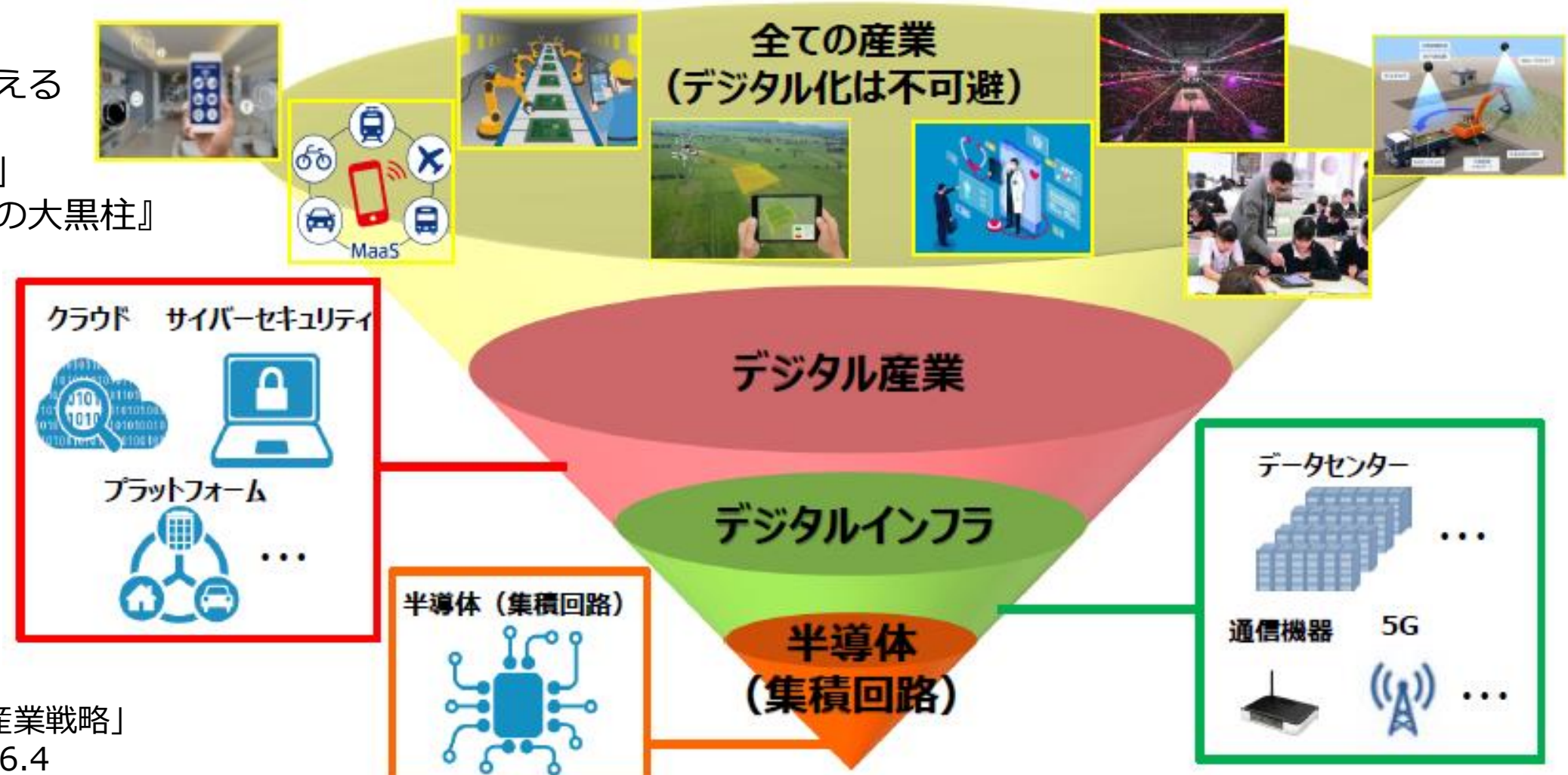
・暗号と情報セキュリティシンポジウム2019
　ブロックチェーンⅡ セッション座長
・Certificate Transparencyを用いた研究, 国際会議採択2件
　※ブロックチェーンの亜種とも言える（Merkle-Hash tree + 複数Centralized）

【自身と”データガバナンス”の関わり】

・「高品質・高信頼なデータ流通でデータ中心社会を実現する次世代データハブ技術
　（キーワード：データ流通, データ中心社会, データガバナンス）」自社記事に執筆協力

デジタル社会のサプライチェーンは半導体というハードウェアに辿り着く

『デジタル社会を支える
「デジタル産業」
「デジタルインフラ」
「半導体」は、国家の大黒柱』



（出典）
「半導体・デジタル産業戦略」
経済産業省, 2021.6.4

一方、近年のデジタル社会について、アカデミックの源流はどこにあるのか

■近年の経済安全保障, サプライチェーンセキュリティに密接な概念として、Digital Sovereignty という考え方が存在する。

□The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, Philosophy & Technology, Springer, 12 August 2020

以下抜粋

「the fight for digital sovereignty, that is, for the control of data, software (e.g. AI), standards and protocols (e.g. 5G, domain names), processes (e.g. cloud computing), hardware (e.g. mobile phones), services (e.g. social media, e-commerce), and infrastructures (e.g. cables, satellites, smart cities), in short, for the control of the digital. 」

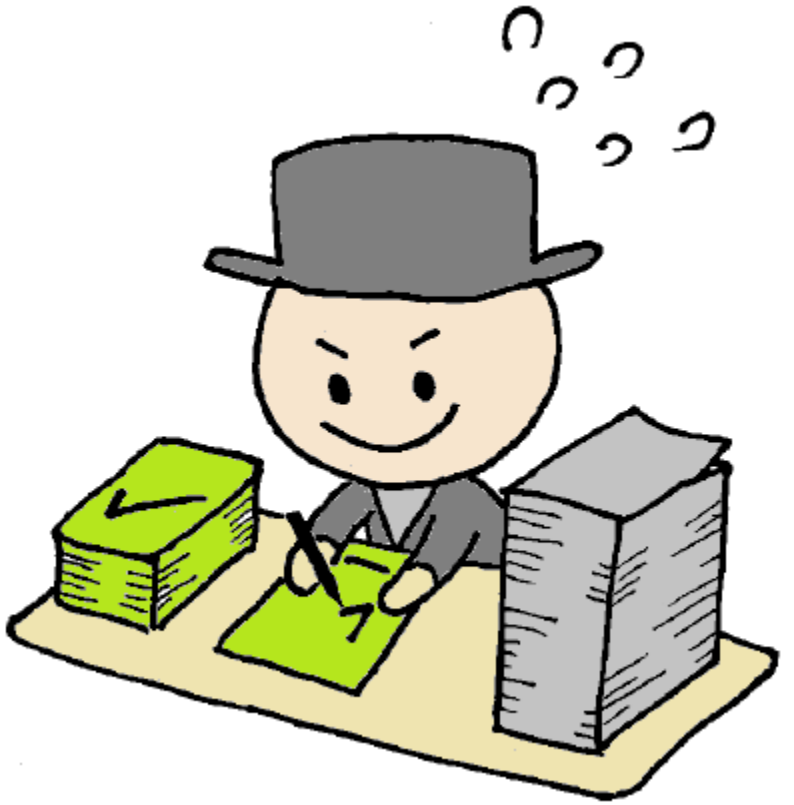
一方、近年のデジタル社会について、アカデミックの源流はどこにあるのか

■Digital self-determination
(哲学,心理学,法学等の多様な観点の研究領域)

→ Data sovereignty, Data governance
(cf. Snowden)

→ Data localization, Data residency
(cf. GDPR)

→ Data Free Flow with **Trust** の提唱へ
(cf. GAIA-X)



Trust とは？

※個人の感想です

信頼「光秀、お前に任せとくわー」

信託「プロの投資家なら大丈夫よね」

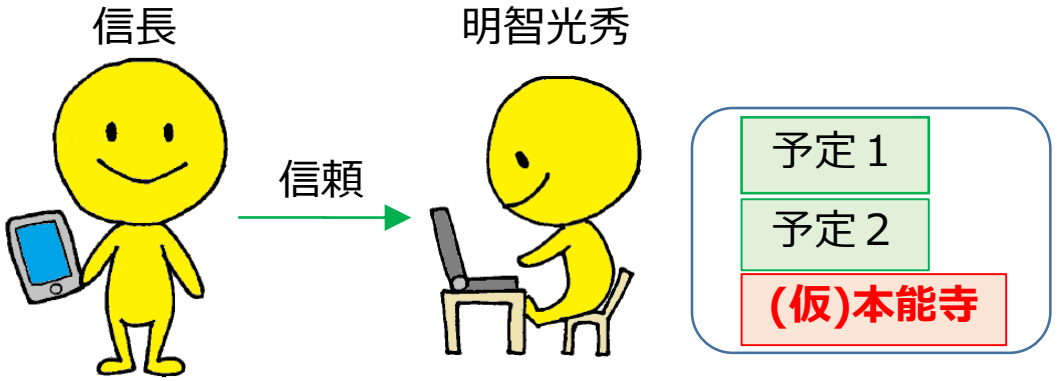
信任「私に清き一票を！Trust Me !!」

・・・で、安心してたら、エライ目に合うのが世の常

※個人の感想です

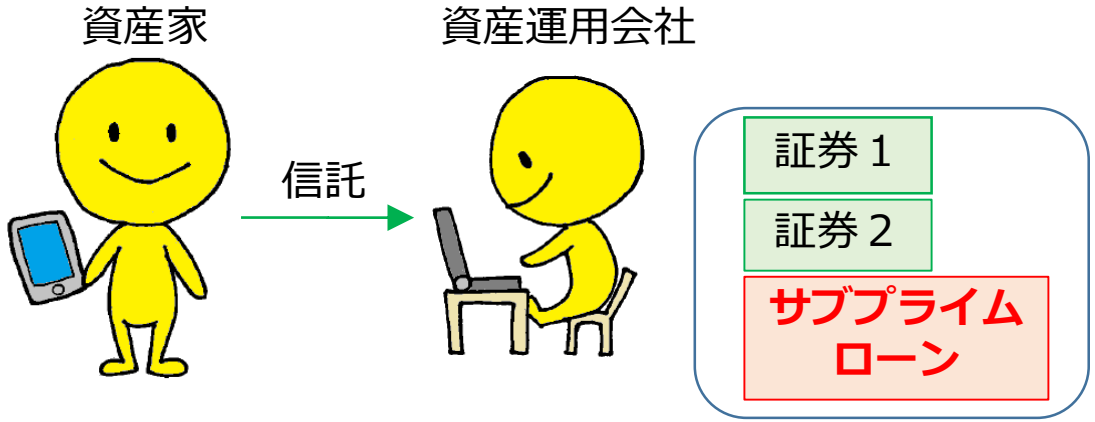
信頼

「この『(仮)本能寺』って
何の予定だろう？？」



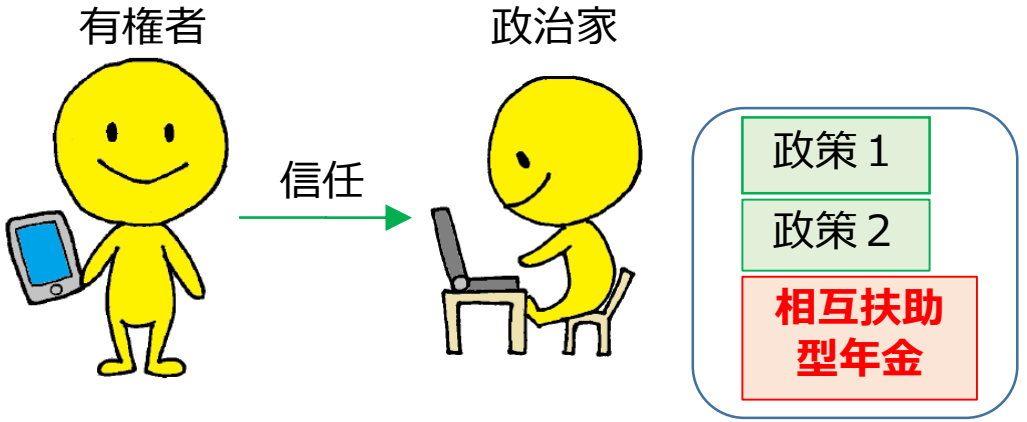
信託

「サブプライムローンって
利率すごいですね！」



信任

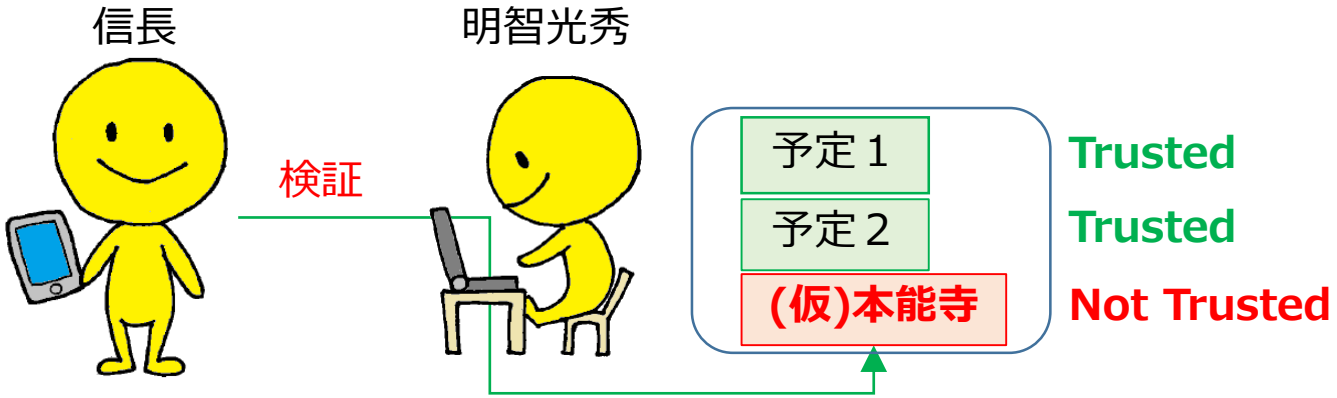
「保育園の増設、頑張ってください！
年金は相互扶助型で維持?? ふーん??」



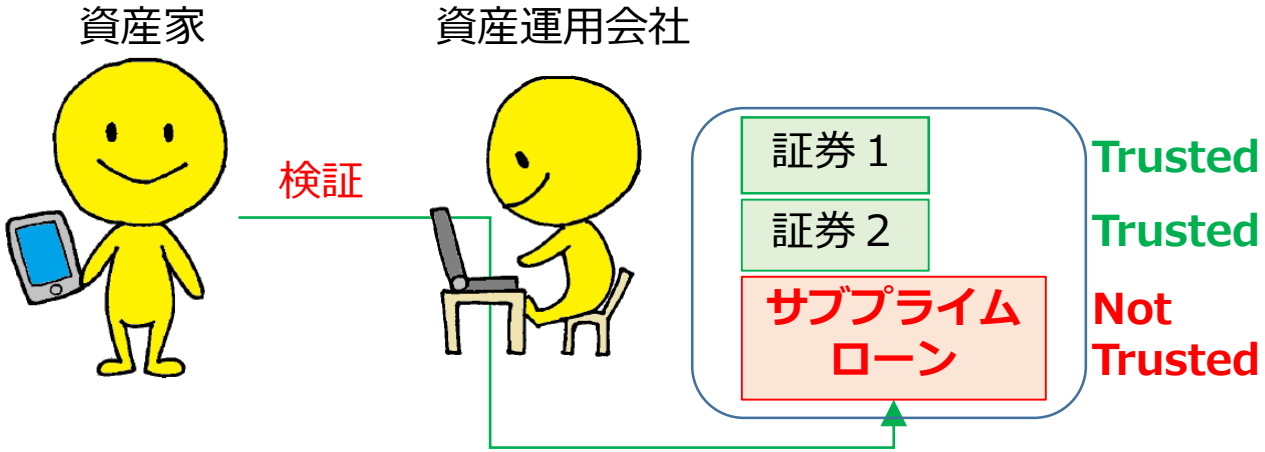
それぞれが、
より良い人生を歩むためには、どうすべきだったか？

※個人の感想です

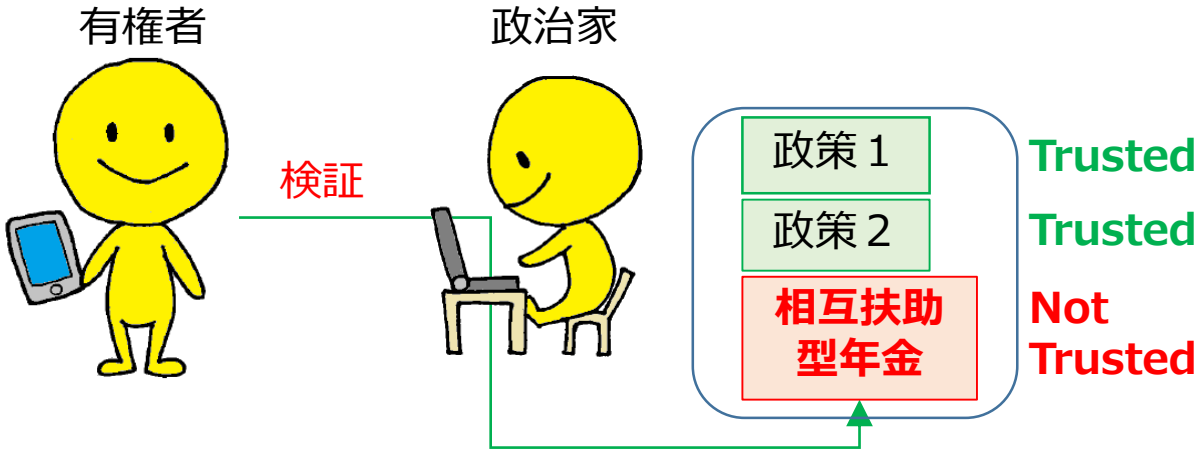
検証「光秀さぁ、この『(仮)本能寺』って何？」



検証「サブプライムローン、返済率が高くないって聞いたんですけど」



検証「保育園の増設は、賛成だけど、年金制度は、積立型に移行すべき！」



本講演のベースにある考え方

基本、**社会は何らかの信頼(Trust)を基に出来ている。**

セコム 島岡先生
「皆が自動車の仕組みを理解して乗ってる訳ではないでしょ。
自動車メーカを信頼して乗ってるでしょ。それがTrustですよ。」

→但し、**（無条件に）信頼する対象(Trusted)が少ない方が、確実性の高い事業運営が出来る。**

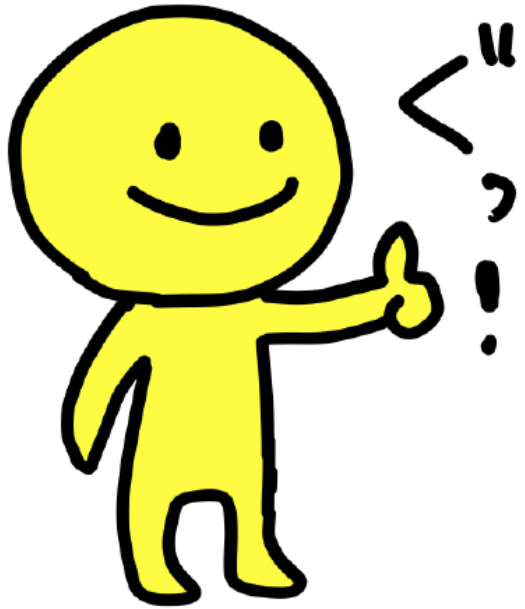
セコム 松本さん他「Don’t Trust, but Verify!!」

“Trusted”に関するトレンド

【データ主権と分散システム】

- Trusted Web
  - Integrity Verification
- Trusted Cloud
  - Confidential Computing

(上記サービスの構成要素として、
TEE(Trusted Execution Environment),
Remote Attestation, Root of Trust)

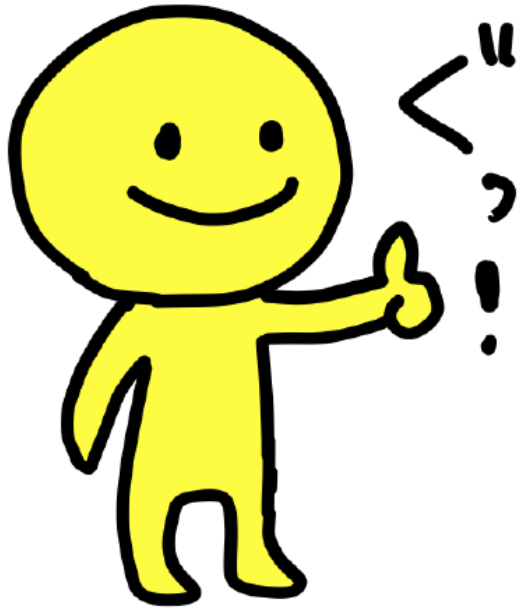


“Trusted”に関するトレンド

【データ主権と分散システム】

- **Trusted Web**
  - **Integrity Verification**
- Trusted Cloud
  - Confidential Computing

(上記サービスの構成要素として、
TEE(Trusted Execution Environment),
Remote Attestation, Root of Trust)



Trusted Webとは？

■Trusted Web

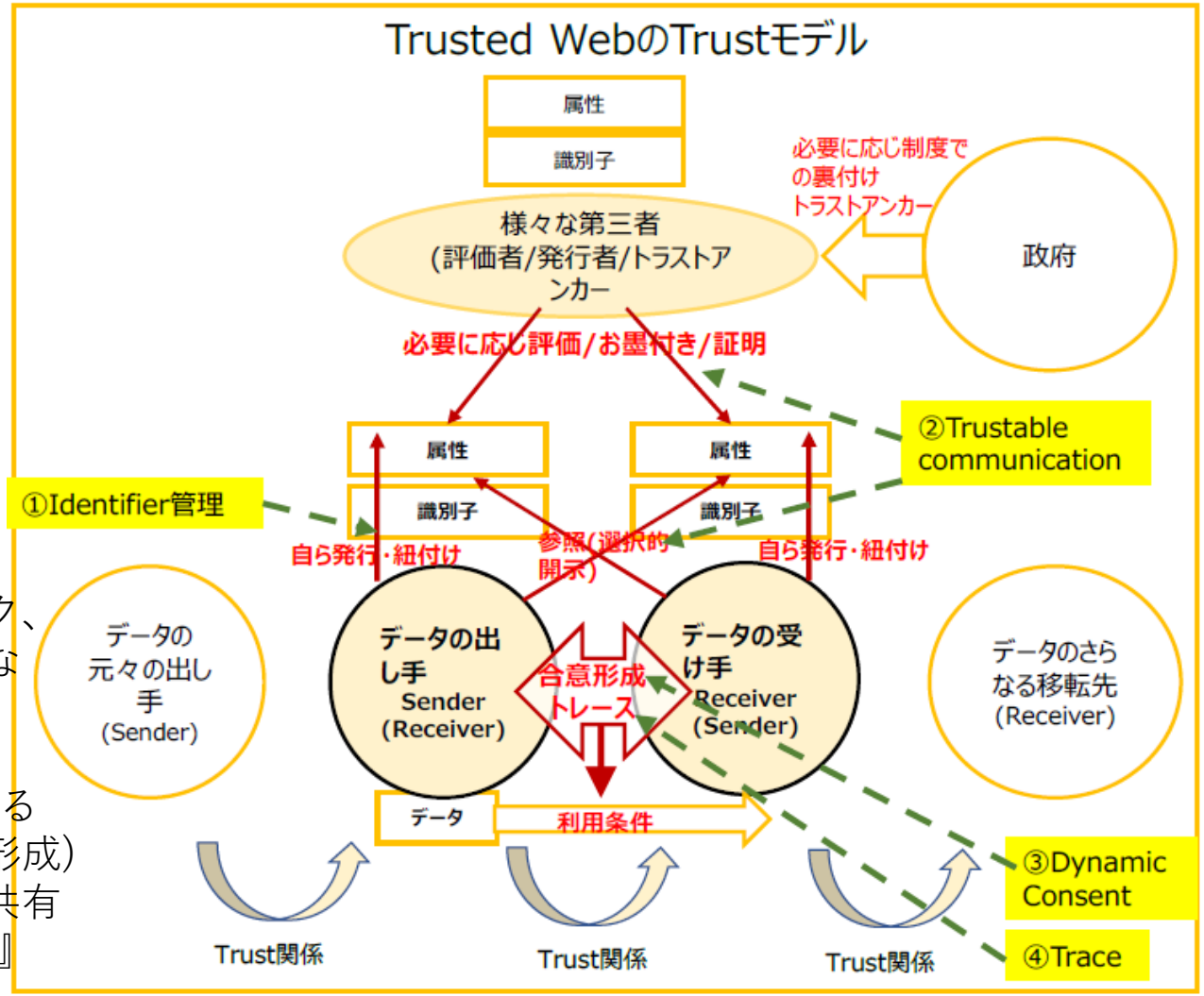
（出典）内閣官房デジタル市場競争会議
『デジタル市場の目指すべき姿として、“一握りの巨大企業への依存”でも、“監視社会”でもない第三の道として、
・多様な主体による競争
・信頼（トラスト）の基盤となる「データ・ガバナンス」
・「トラスト」をベースとしたデジタル市場
の実現を目指すとの提言』『その実現の一つの方策として、「データ・ガバナンスの在り方をテクノロジーで変える分散型の“Trusted Web”の実現」が提言された。』

→目的意識は共感できる部分が多い。
『フェイクニュースなど流れるデータの信頼性への懸念、プライバシー侵害リスク、勝者総取りに伴う単一障害点のリスク、サイロ化した産業データの未活用など、デジタル化の中で様々なペインポイントが生じている。』

ここが ”Root of Trust”

『・マルチステークホルダーによるガバナンス（Trustを裏付ける経路や連鎖を分散協業して支える、ルールや運用について合意形成）
・信頼できる情報が価値を持ち、不知の者同士でもデータの共有が容易となる等により、新たな経済的価値の創出が期待される』

（出典）Trusted Web推進協議会
Trusted Web ホワイトペーパー Ver1.0

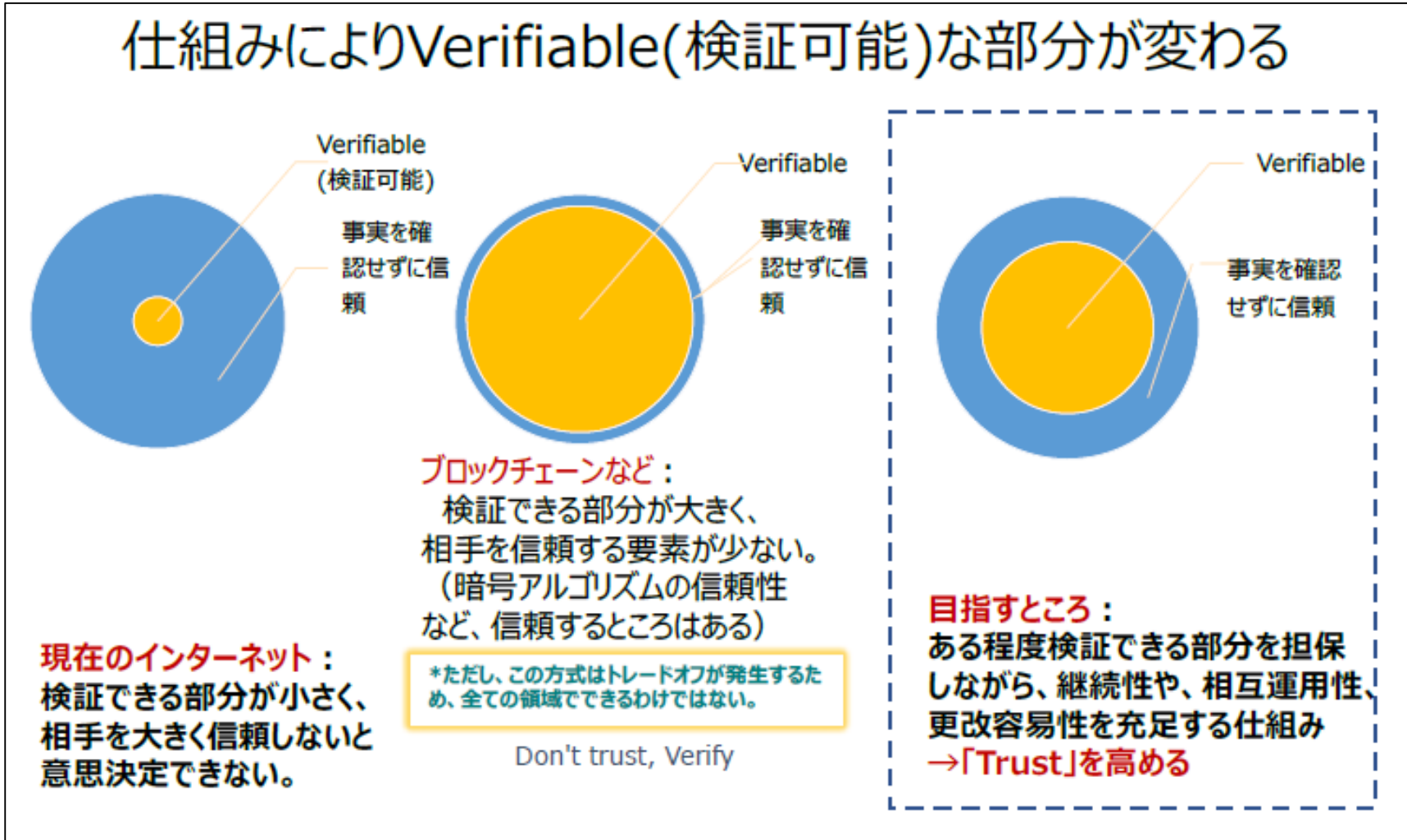


Integrity Verificationとは？

■ **Integrity Verification** は、
無条件のTrustを抑制できる。

（出典）Trusted Web推進協議会
Trusted Web ホワイトペーパー Ver1.0

「Don’t Trust, but Verify!!」



（余談）Verifiability と Security

安全♪安全♪

すべての階層において、レビュアにより
検証可能であること(Verifiable)が、安全性の前提となる
レビュアは外部を含めて多い方が良いため、
OSSであること、情報公開されていることは、
安全性の向上につながる。(cf. WhiteHat)

暗号利用システム
(IAM, KMS, 等)

システム設計, 開発, 試験の各プロセスで
セキュリティシステム技術者達によるレビュー
CMVP, CC, FIPS, PCI-DSS等の外部監査で
セキュリティシステム技術者達によるレビュー

形式検証
(Formal Verification)
モデル検査
(Model Checking)

Root of Trust は
ここの負荷を低減?

暗号利用ソフトウェア
(OpenSSL, 等)

ソフトウェア設計, 開発, 試験の各プロセスで
セキュリティソフトウェア技術者達によるレビュー
OSSであれば、OSSコミュニティで
セキュリティソフトウェア技術者達によるレビュー

形式検証
(Formal Verification)
モデル検査
(Model Checking)

暗号プロトコル
(SSL/TLS, 等)

主にIETF標準化のプロセスで
セキュリティプロトコル技術者達によるレビュー
IACRを含む情報セキュリティ査読付き会議で
暗号学者＆セキュリティ研究者達によるレビュー

安全性証明
(Cryptographic Analysis)
形式検証
(Formal Verification)

暗号プリミティブ
(公開鍵, AES, 等)

NISTコンペティションおよび
IACR査読付き会議で
暗号学者達によるレビュー

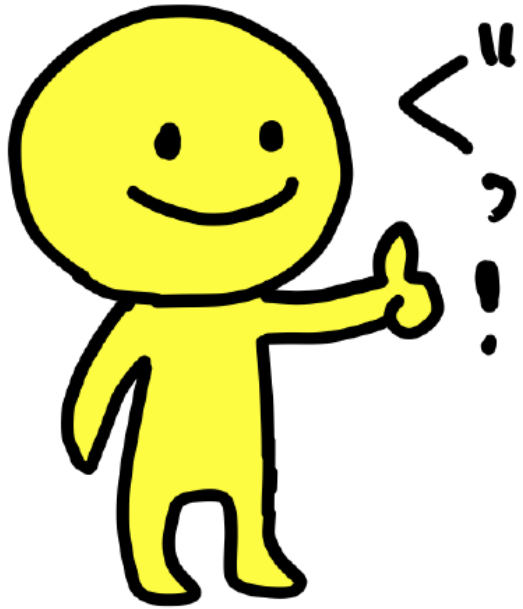
安全性証明
(Cryptographic Analysis)

“Trusted”に関するトレンド

【データ主権と分散システム】

- Trusted Web
  - Integrity Verification
- **Trusted Cloud**
  - **Confidential Computing**

(上記サービスの構成要素として、
TEE(Trusted Execution Environment),
Remote Attestation, Root of Trust)



Trusted Cloudとは？

■ **Trusted Cloud**

(https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud)

Draft NISTIR 8320 Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases, May 2021

（サプライチェーンを含めて）PC/サーバやデータセンタの
セキュアブートをハードウェアベースで強化する技術体系、
Platform Integrity Verificationに多く言及

さらに、近年流行の**Confidential Computing**へ

Confidential Computingとは？

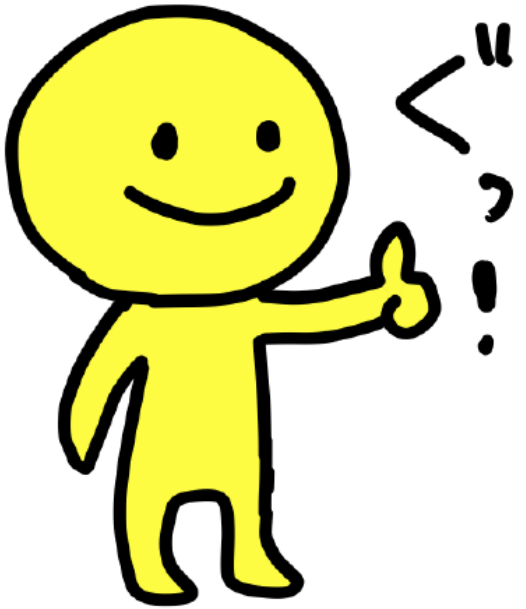
Confidential Computing って 何ですか？？

Confidential Computingとは？

■情報セキュリティの文脈では一般に
Confidentiality(秘匿性), Integrity(完全性), を中心に議論

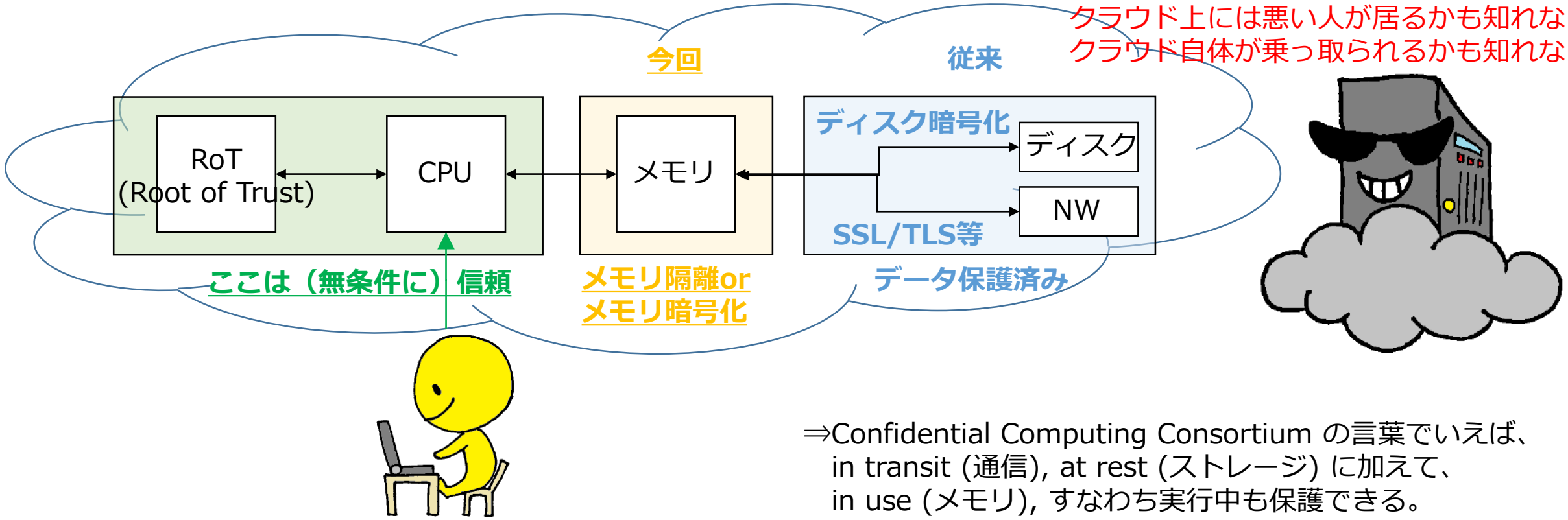
→改めてgoo辞書で調べてみよう
Confidential(信用の置ける, 頼りになる),
Confident(固く信じて), Confidence(信頼,信用,信任),
Integrity(正直,誠実,高潔),(一貫性,統一性,整合性)

→結論をざっくり言えば、**Integrityが検証&制御された**
クラウド環境を、Confidentialに利用するサービスです。



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
＝**(0)“CPUのみ”を信頼して利用可能なクラウド環境**

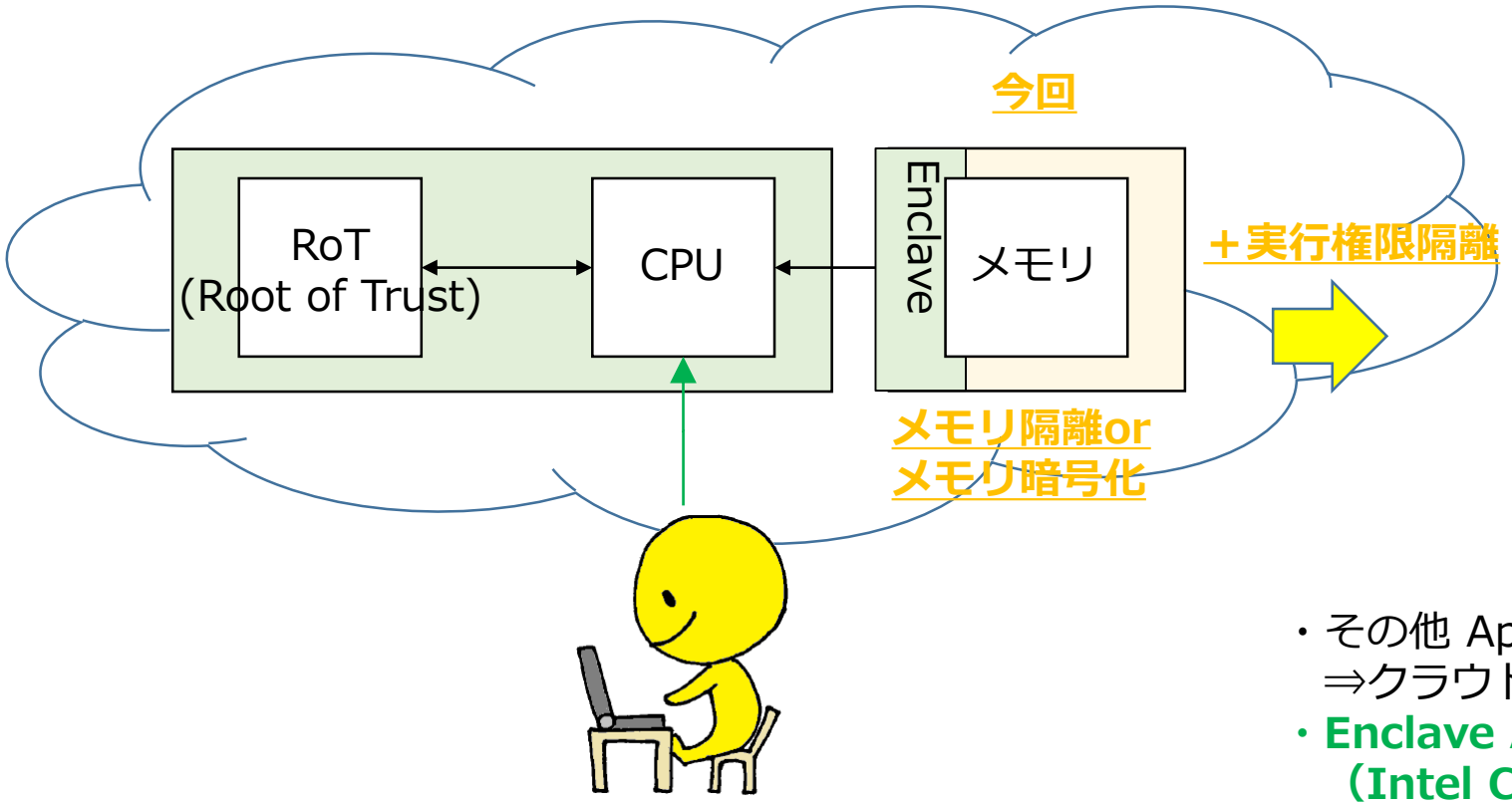


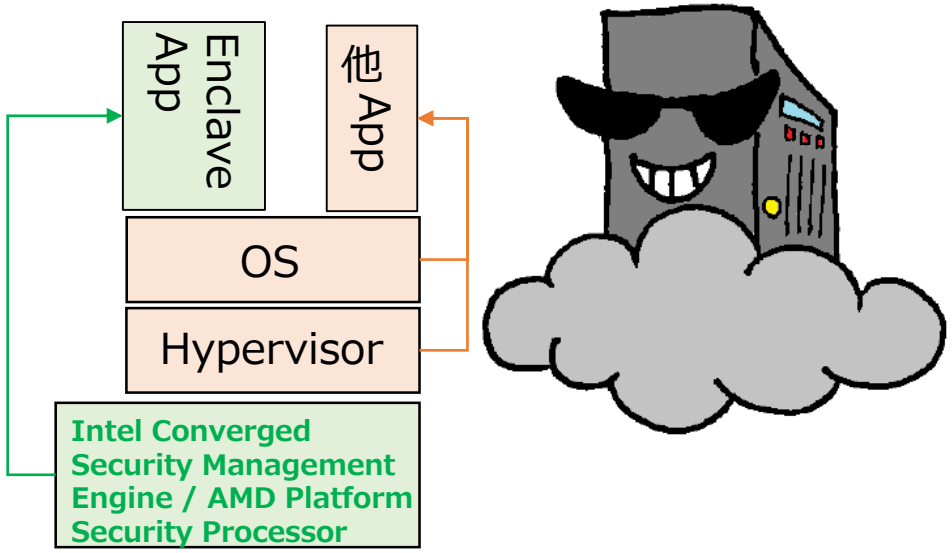
⇒Confidential Computing Consortium の言葉でいえば、
in transit (通信), at rest (ストレージ) に加えて、
in use (メモリ), すなわち実行中も保護できる。

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！



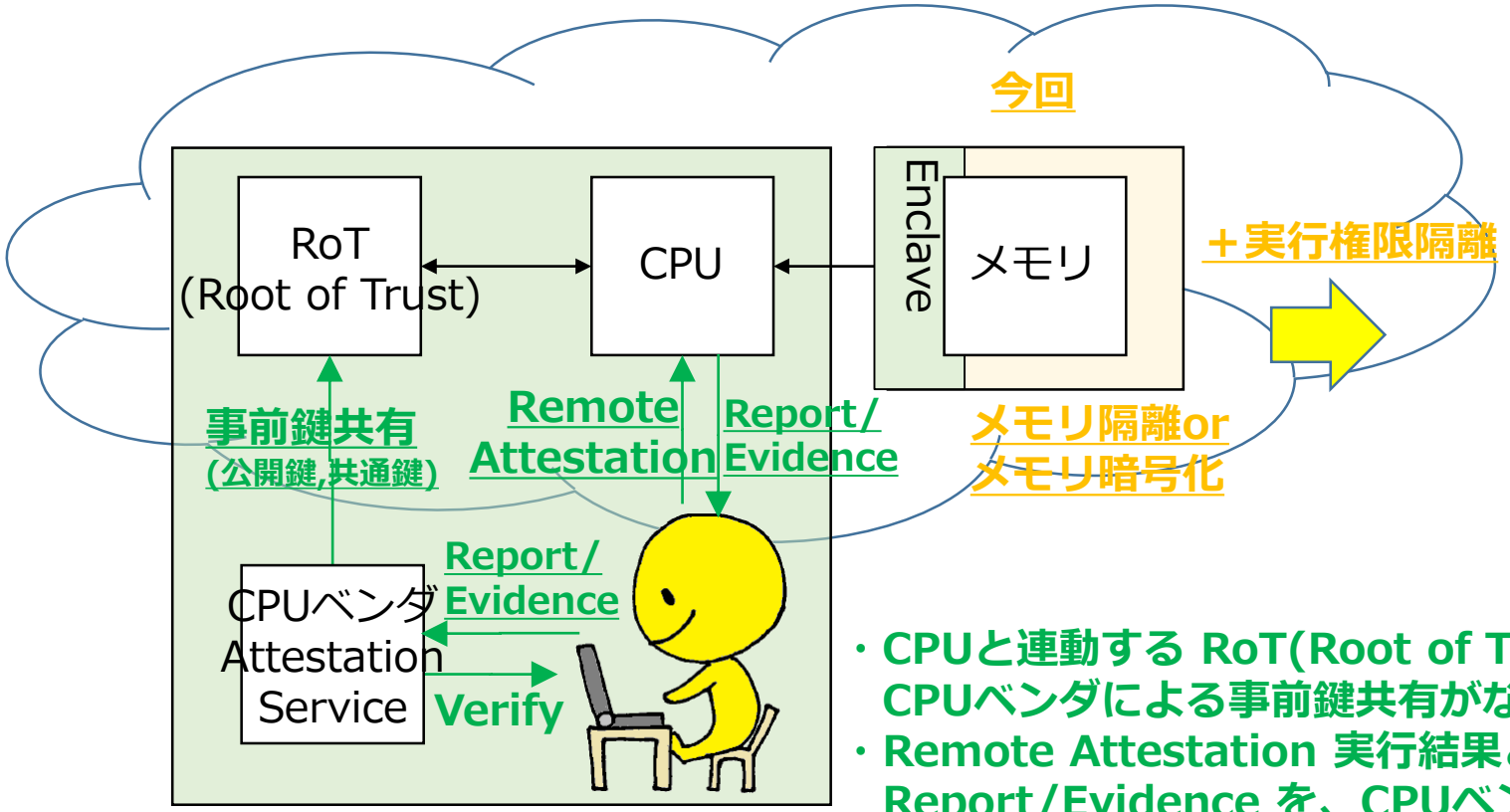


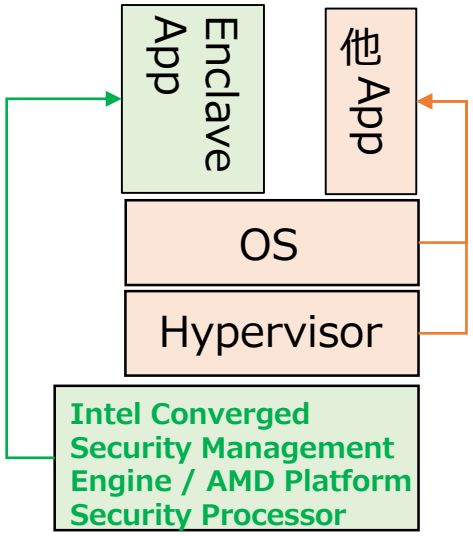
・その他 Appは OSやハイパーバイザから制御可能
⇒クラウド事業者が制御可能

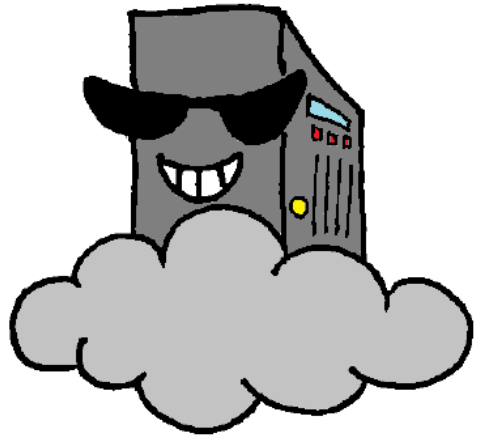
・**Enclave Appは CPUのみが制御可能**
（Intel CSME / AMD PSP のみが制御可能）
⇒クラウド事業者は制御不可
（OSやハイパーバイザから制御不可）

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
↑**(2)Remote Attestation により(PKI的に)信頼を連鎖！**



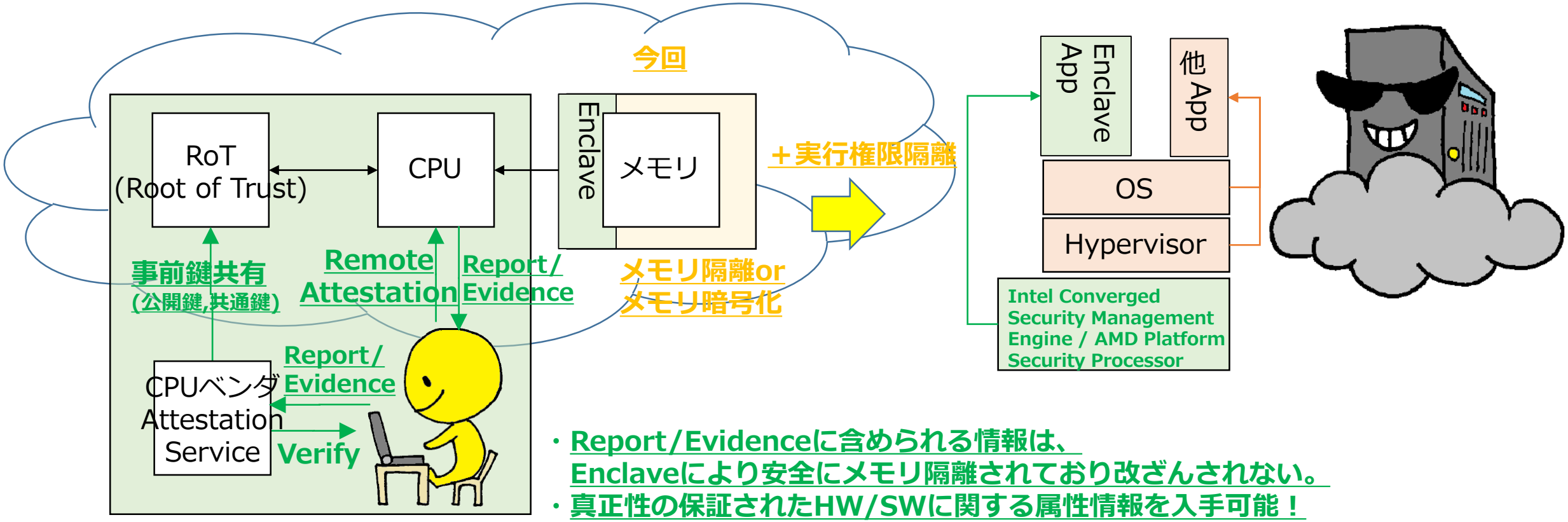




・CPUと連動する RoT(Root of Trust) に、
CPUベンダによる事前鍵共有がなされている。
・Remote Attestation 実行結果として得られる、
Report/Evidence を、CPUベンダの管理する
Attestation Service に問い合わせることで、
Report/Evidence の真正性を検証できる。

Confidential Computing とは

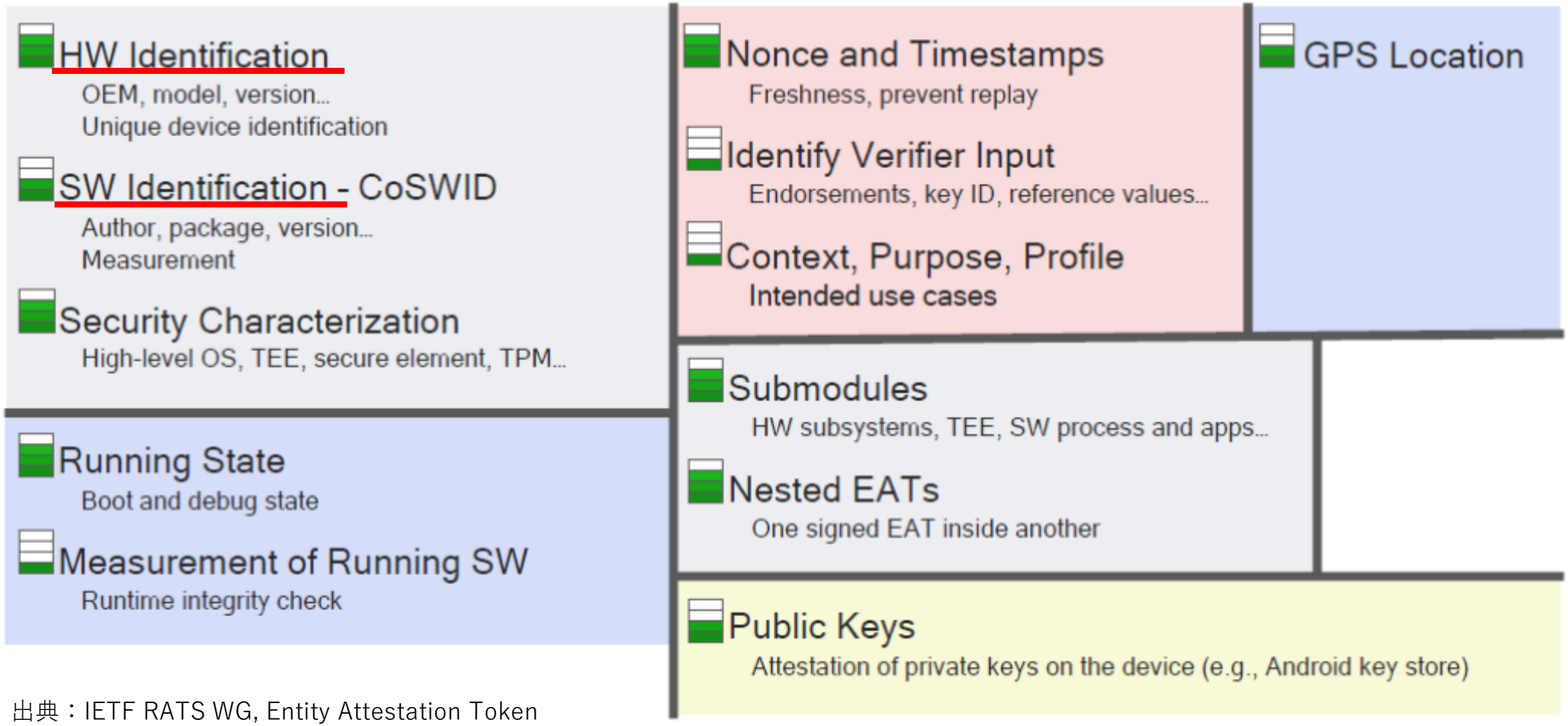
“CPUのみ”がアプリ&データを制御可能なクラウド環境
↑**(3)Report/Evidenceに(証明書的に)属性情報を含められる！**



・Report/Evidenceに含められる情報は、
Enclaveにより安全にメモリ隔離されており改ざんされない。
・真正性の保証されたHW/SWに関する属性情報を入手可能！

（参考）IETF RATS WG Entity Attestation Token

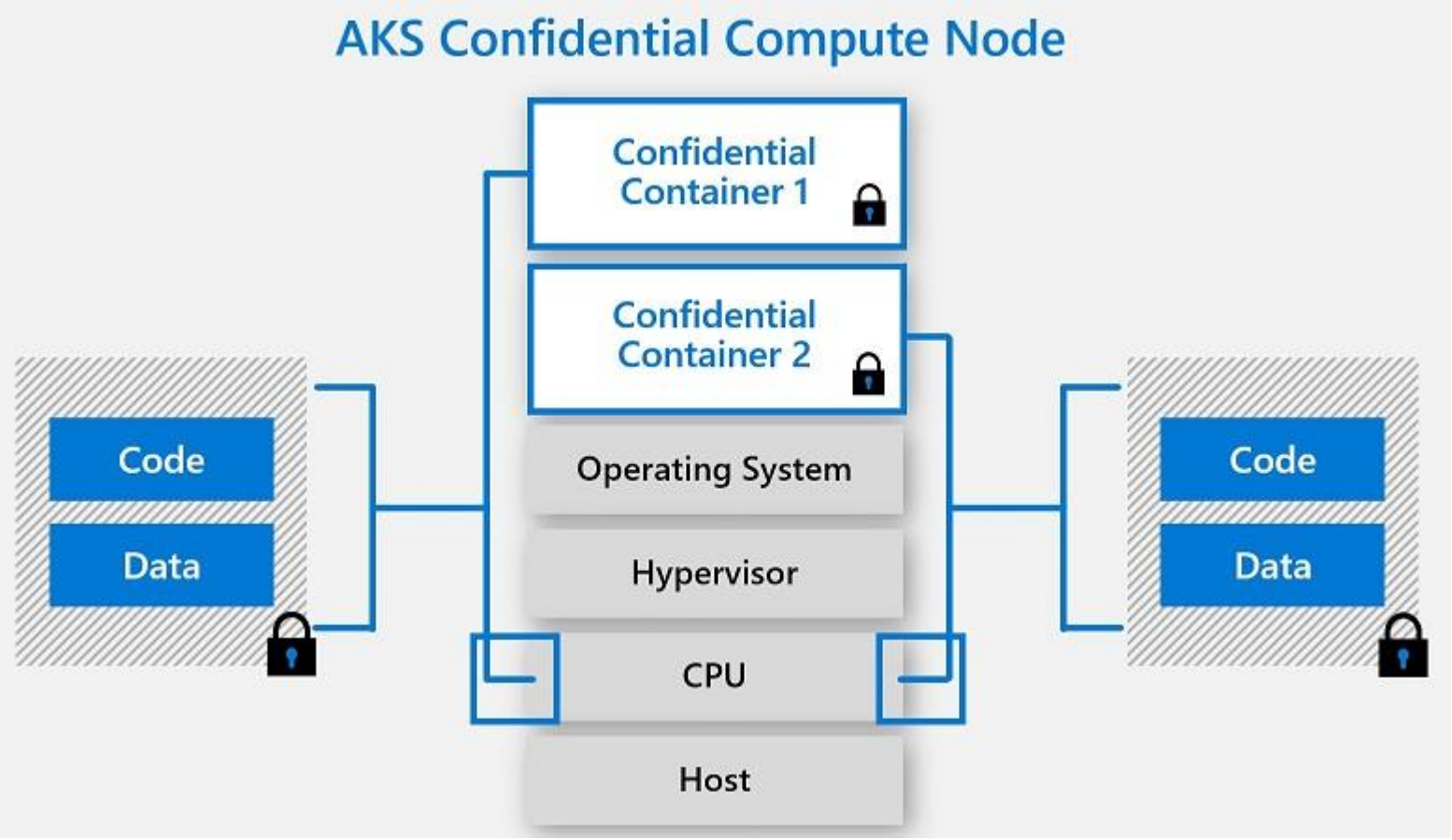
- **Remote Attestation により、HW-ID, Manufacturer, model, version, SW-ID, Author, package, version, Measurement(code hash etc.)等の真正性を保証**



出典：IETF RATS WG, Entity Attestation Token

(応用例1) Confidential VM,コンテナ

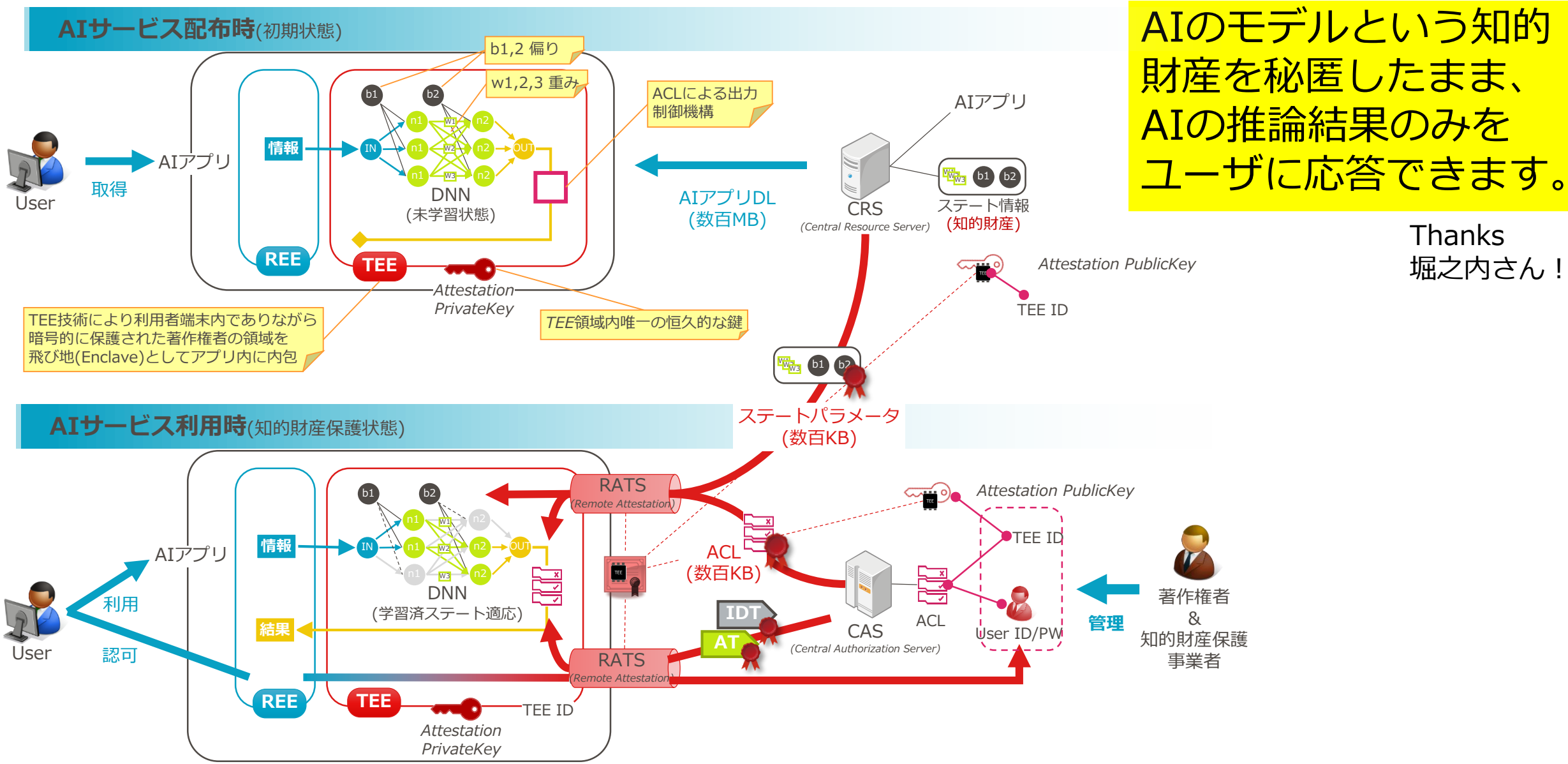
クラウド上の作成済みのVMやコンテナを、TEE/Enclave上に
そのまま移行して、クラウド事業者から秘匿することが出来ます。



近年トレンドとなっている
コンテナ型の環境と相性が良い。

（出典）
Azure Kubernetes Service の
コンフィデンシャル コンピューティング
ノード (パブリック プレビュー)

(応用例2) Confidential AI,機械学習

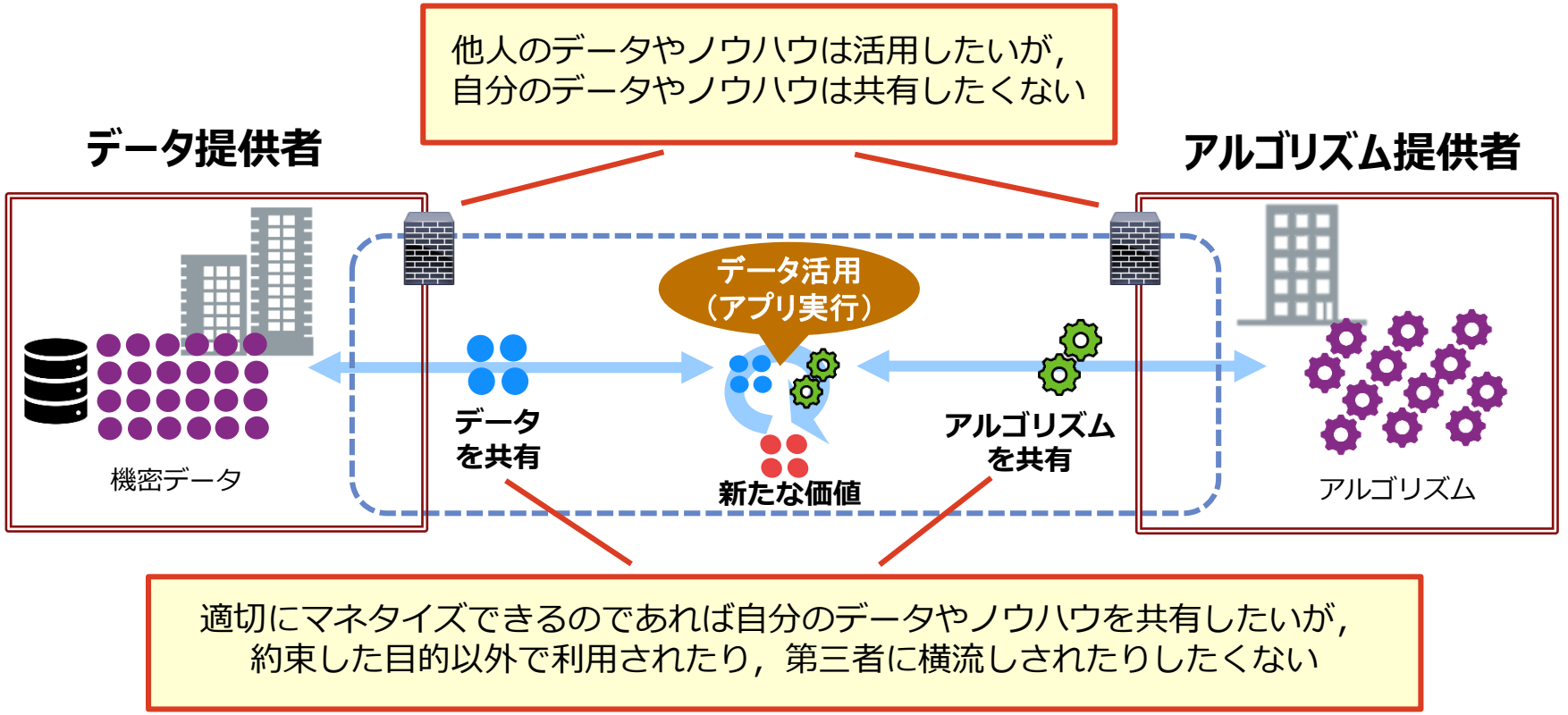


AIのモデルという知的財産を秘匿したまま、AIの推論結果のみをユーザに応答できます。

Thanks
堀之内さん！

(応用例3) Confidential 企業間コラボ

事前の信頼関係のないパートナー企業間であっても、
アプリ＆データを秘匿したまま、計算結果のみを享受できます。



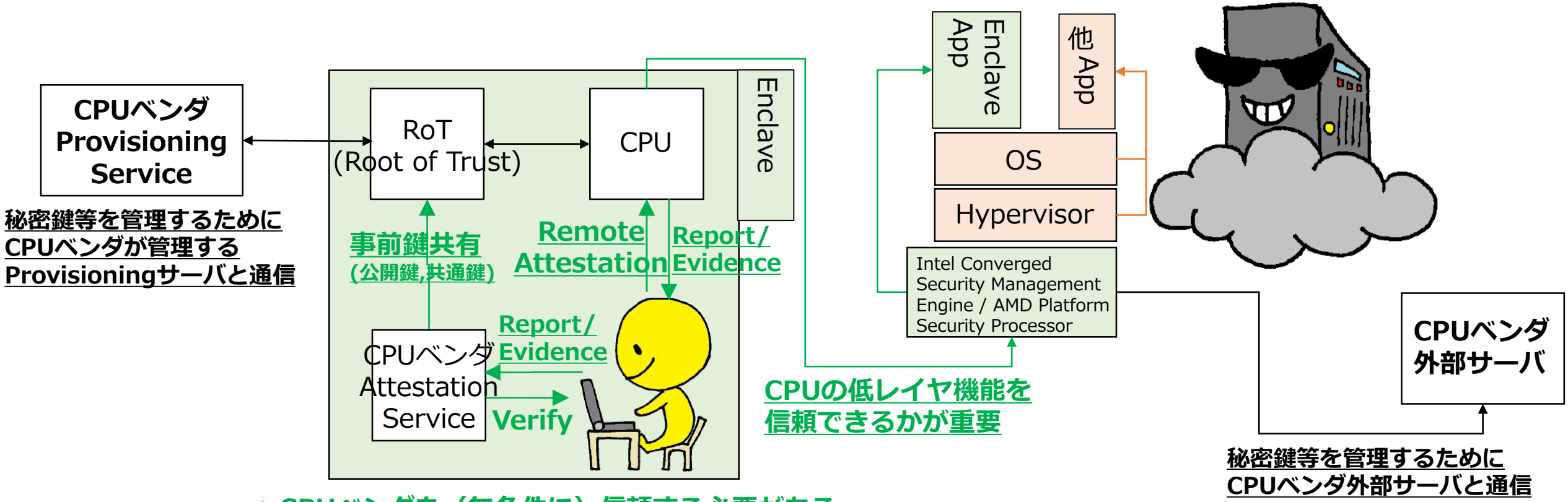
NTT技術ジャーナル2020年12月号
NTT技術ジャーナル2021年4月号

CPUベンダを信頼するモデルの是非

もう少し聞きたいんだけどさ、
CPUベンダを信頼するモデルは大丈夫なの？？

疑問：CPUベンダは信頼して良いのか？

“CPUのみ”を信頼して利用可能なクラウド環境
↑**CPUベンダを”信じるか信じないかは貴方次第”(某都市伝説風)**



⇒ **CPUベンダを（無条件に）信頼する必要がある。**
クラウド事業者を（無条件に）信頼する必要は無くなる。

CPUベンダを信頼するモデルの是非

回答：**社会は何らかの信頼(Trust)を基に出来ている。**

セコム 島岡先生
「皆が自動車の仕組みを理解して乗ってる訳ではないでしょ。
自動車メーカを信頼して乗ってるでしょ。それがTrustですよ。」

→但し、**（無条件に）信頼する対象(Trusted)が少ない方が、確実性の高い事業運営が出来る。**

セコム 松本さん他「Don’t Trust, but Verify!!」

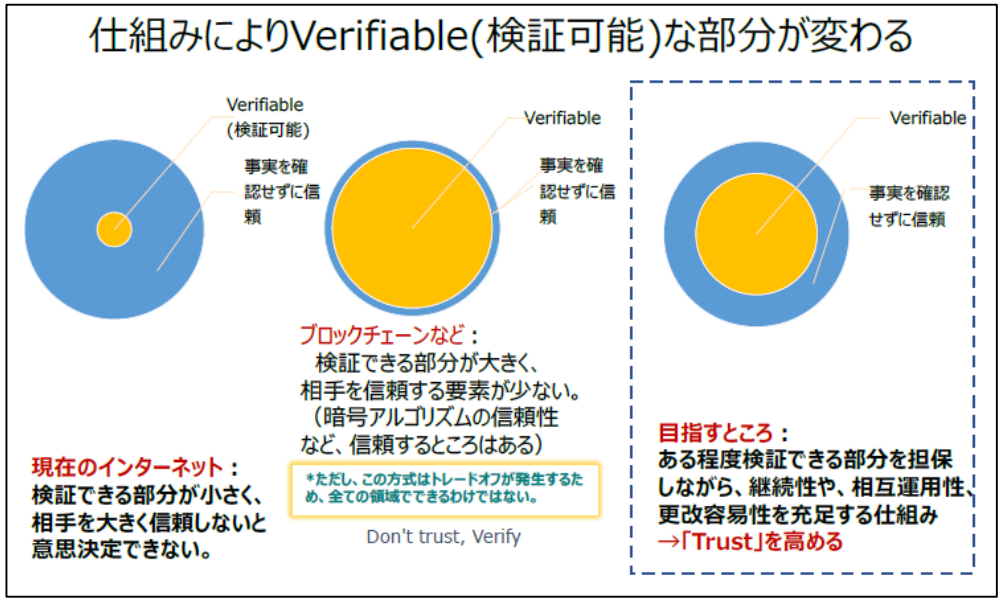
→煎じ詰めれば、誰を何を信頼して、
クラウドという目の前に実体の無いサービスを利用するか。

**信頼する対象は、CPUベンダでも良いし、GAFAMでも良いし、
お近くのNTTでも良いし、顔なじみのITベンダでも良い。**

Confidential Computing と Verifiability

（無条件に）信頼する対象(Trusted)が少ない方が確実性の高い事業運営が出来る

→なお、Platform Integrity Verificationは、今回のクラウドセキュリティ対策と同時に、サプライチェーンセキュリティ対策になり得る。



（出典）Trusted Web推進協議会
Trusted Web ホワイトペーパー Ver1.0

Confidential Computing

（無条件に）信頼すべき領域を最小化する仕組み

Client

Remote Attestation

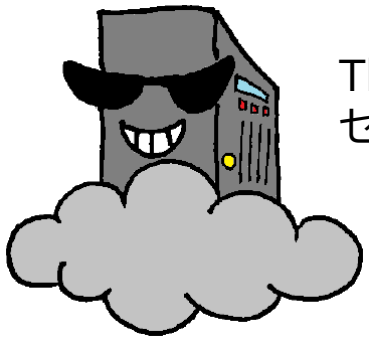
ここに機密なデータを凝縮する

Cloud ↓

Enclave　Server

(宮澤定義) Platform Security Engine

ここを基点に↑
信頼できる領域を作る



Thanks
セコム 宮澤さん！

Confidential Computing の課題は？

・CPUサイドチャネル対策

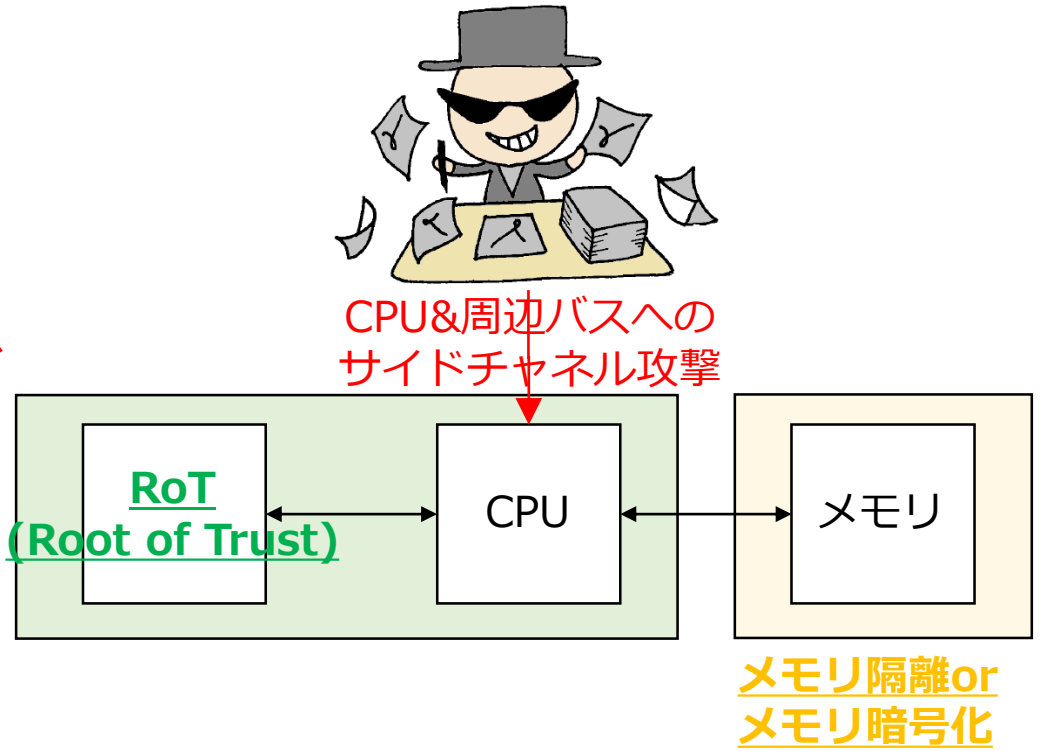
Thanks
NTT 順子さん！
弾くん！

⇒CPUおよび周辺バスを含めて、
キャッシュタイミング攻撃などのサイドチャネル攻撃が知られており、
Confidential Computing Consortiumでは、あらゆる攻撃に対策するとは宣言していない様子

・各種レギュレーション対応

Thanks
NTT 千田さん！

⇒**国内では個人情報保護法、**
海外ではGDPR, CCPA 等の一般的な法規制に加えて、
業界毎のレギュレーションについて、
Confidential Computing でクリア出来るのかは、
ベンダ各社に問い合わせる必要がある。



（余談）アカデミックの Confidential Computing に対する動向

・ACM Magazines, February 2021, 「Toward Confidential Cloud Computing: Extending hardware-enforced cryptographic protection to data while in use」

→著者はMicrosoft, 暗号学者として有名な Cédric Fournet を含む。

・IEEE SPECTRUM, May 2020, 「What Is Confidential Computing? Big tech companies are adopting a new security model called confidential computing to protect data while it’s in use」

・IEEE Symposium on Security and Privacy (S&P), May 2020,「Enabling Rack-scale Confidential Computing using Heterogeneous Trusted Execution Environment」

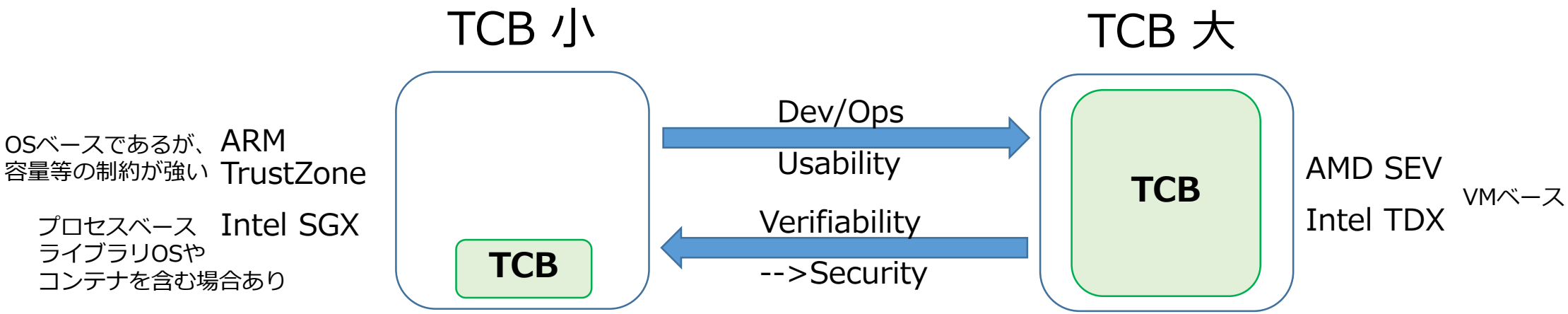
→サイバーセキュリティのトップ国際会議 IEEE S&P に遂に採録された

→産業界から出てきた Confidential Computing について、
アカデミックサイドも看過できなくなってきている様子。

（余談）CPUベンダの Confidential Computing に対する動向

・2015年リリース以降、Intel SGX(Software Guard Extensions) が中心的な地位を占めていた。
　Microsoft, IBM に導入されてサービスインしてきた。
→2020年、Google から Confidential VM が リリースされて、
　IBM, Microsoft 等も、AMD SEV(Secure Encrypted Virtualization)との提携を発表した。
→Intelは、Intel TDX(Trust Domain Extensions)で、AMD SEVに対抗提案している様子。

→背景に、TCB(Trusted Computing Base)に関する思想の違いがある。
TCBが小さいほど、ソフトウェアを検証し易くセキュリティを高めやすいが、 **Verifiability → Security**
TCBが大きいほど、特にVM/コンテナに一致させれば使い勝手が良くなる。



（余談）業界各社の Confidential Computing に対する動向

・DevOpsの関心の高さもあり、Deployを重視したプロダクトが流行ってる印象
　下記は Azure Kubernetes Service でenablerとして提供されている Fortanix

1. Bring your Container based Apps

2. Create Confidential Container with few clicks

3. Deploy Confidential Containers

（出典）
Fortanix

（余談）業界各社の Confidential Computing に対する動向

・**Microsoft**：Development向けに強い。WSL2 & VScodeで覇権奪回。
Open Enclave, for SGX & OPTEE, SGX版は導入実績も複数聞く。
Deployment向けは複数enabler(3rd-party)と連携して提供。
アカデミックにおける発信頻度が非常に高く、情報公開に積極的。

・**Intel**：Development向けIntel SGX SDKに加えて、
Deployment向けGraphene-SGXをFortanixと共同開発。

・**Red Hat**：Deployment向けに注力している。
Enarx, for SEV & SGX (※発表時点ではSGX版は未動作の様子)
Kubernetesの商用向け製品であるOpenShiftを提供しており、
VM/コンテナへの親和性と、IBMのマルチクラウド戦略で、
非常に良いポジショニングを取っている。＃羨ましい

・**ARM**：データセンタ向けNeoverseをAWSに提供。市場へ本格参入を目指す。
ARMv9でConfidential Compute Architectureを導入する情報あり。
Deployment向けとしてVeracruzの研究開発を進めている。

Open Enclave SDK

Development

Intel SGX SDK

Graphene-SGX

SCONE

Occlum

Enarx

Deployment

Veracruz

（余談）業界団体の Confidential Computing に対する動向

- 2019年10月：Confidential Computing Consortium 発足
  Linux Foundation 傘下で、各OSS開発を進める。
- CPUベンダ：Intel, ARM, 後にAMD, NVIDIA も参画
- クラウド：Google Cloud, Microsoft, 中国勢, ・・・AWSは未加入の様子
- SWベンダ：VMware, Red Hat

Confidential Computing Consortium を設立、設立メンバーとオープン ガバナンス構造を発表

By The Linux Foundation | 10月 17, 2019

（出典）
Linux
Foudation

業界最大のテクノロジーリーダーが、次世代のクラウドおよびエッジ コンピューティングのコンピューショナルな信頼とセキュリティを向上

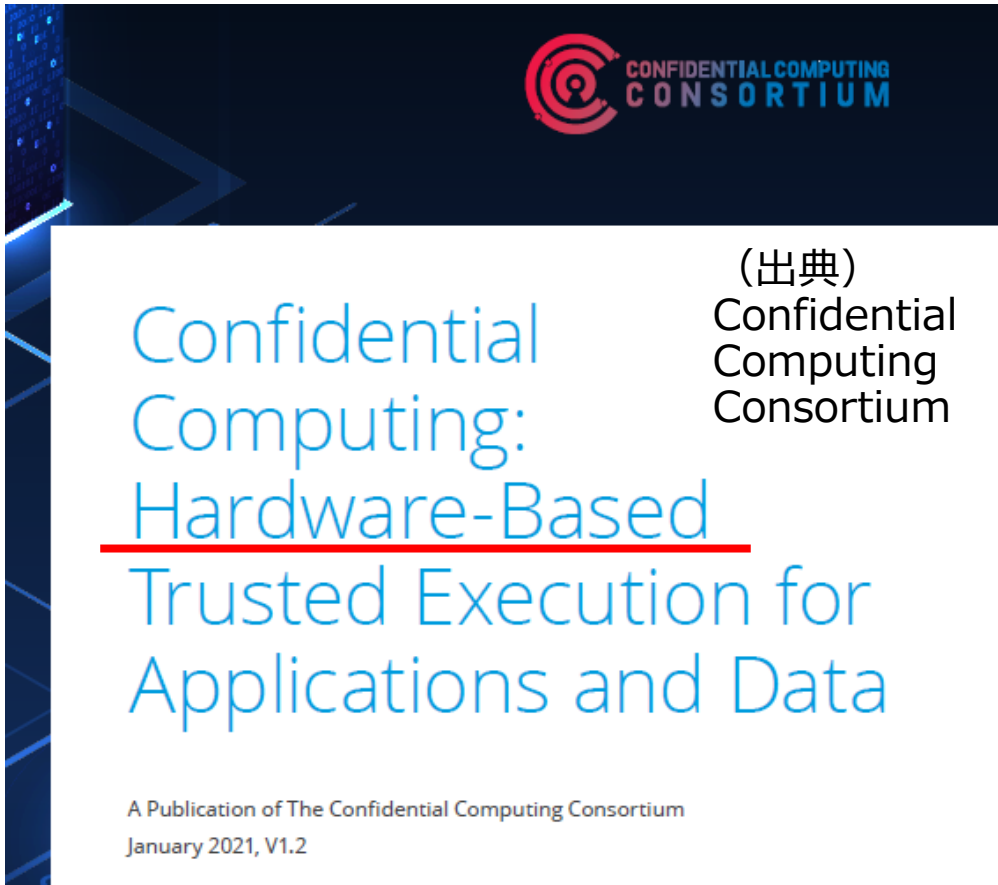
2019年10月17日 サンフランシスコ発 – Linux Foundation のプロジェクトで、コンフィデンシャル コンピューティングの定義と導入促進に取り組むコミュニティ Confidential Computing Consortium は、コンソーシアムの正式な設立と、設立時のプレミアメンバー Alibaba、Arm、Google Cloud、Huawei、Intel、Microsoft、Red Hat、およびゼネラルメンバー Baidu、ByteDance、decentriq、Fortanix、Kindite、Oasis Labs、Swisscom、Tencent、VMware を発表しました。

（余談）業界団体の Confidential Computing に対する動向

・Confidential Computing Consortium に AWSは未加入の件

・Confidential Computing Consortium では、
「**Hardware-Based** Trusted Execution」に重点を置く。

・AWS Nitro Enclaves は**ハイパーバイザベース**。
（AWS Nitro Security Chip, Graviton2 プロセッサと
Nitro Enclaves の関係は明に語られていない様子）
※各種isolation機能については、
DockerあるいはVM相当という印象を受ける。
→**今後の情報公開に期待！！**



（出典）
Confidential Computing Consortium

ハードウェア Root of Trust を重視する動向

- **Confidential Computing**とは、
  CPUベンダ提供の**ハードウェア(Root of Trust)**から
  信頼の連鎖(Chain of Trust) を 提供する仕組み

（と思ってる）

→ GAFAM等の大手ITベンダ各社 が、

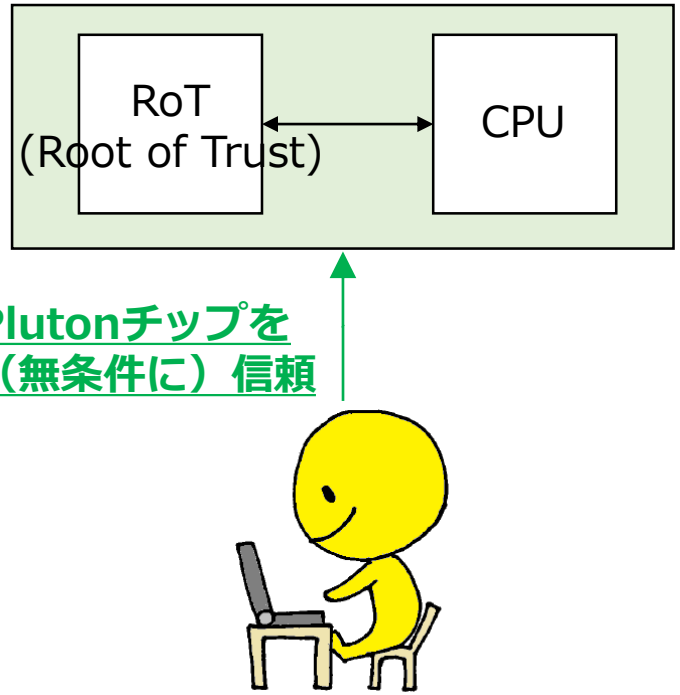
それぞれに**自社製ハードウェア(Root of Trust)**と
自社製Chain of Trustを提供開始/提供検討中

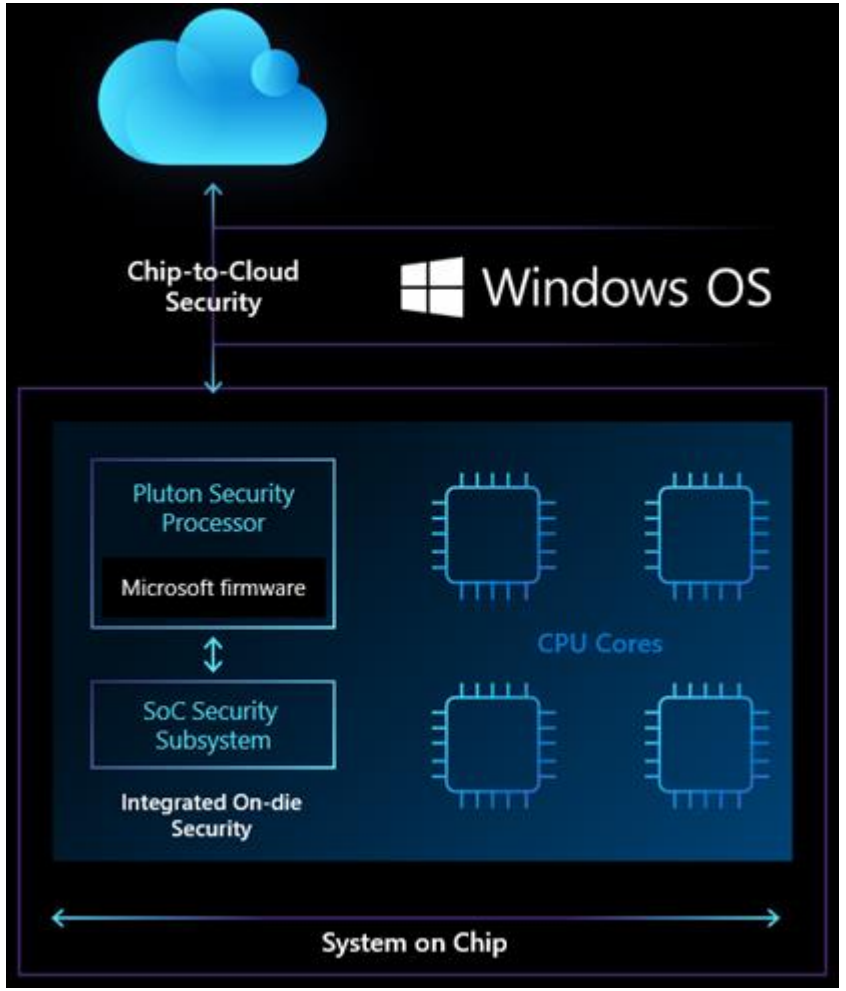
（と思って進めてる訳ではないと思うが）

Microsoftの自社製ハードウェア

Pluton:
CPUと同じパッケージ内部に、
TPM相当のRoT(Root of Trust)を同梱することで、
外部バスへのサイドチャネル攻撃等に対策した、
Microsoft自社製ハードウェア

※詳細は PKI & Trust Days 2021
「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）



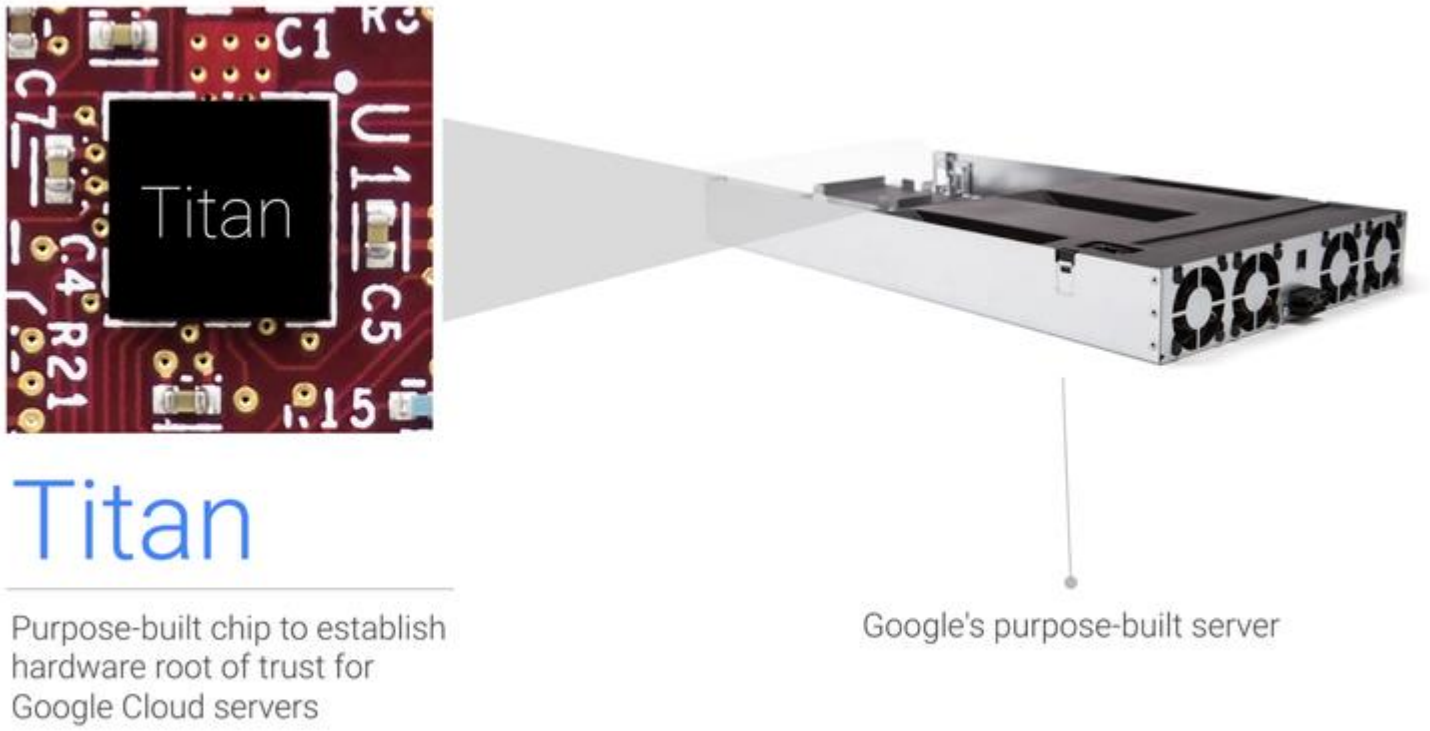


（出典）
Microsoft Pluton Processor のご紹介
– Windows PC の 未来に向けて
設計されたセキュリティチップ

Amazonのサーバ向けハードウェア

AWS Nitro Security Chip, AWS Graviton2

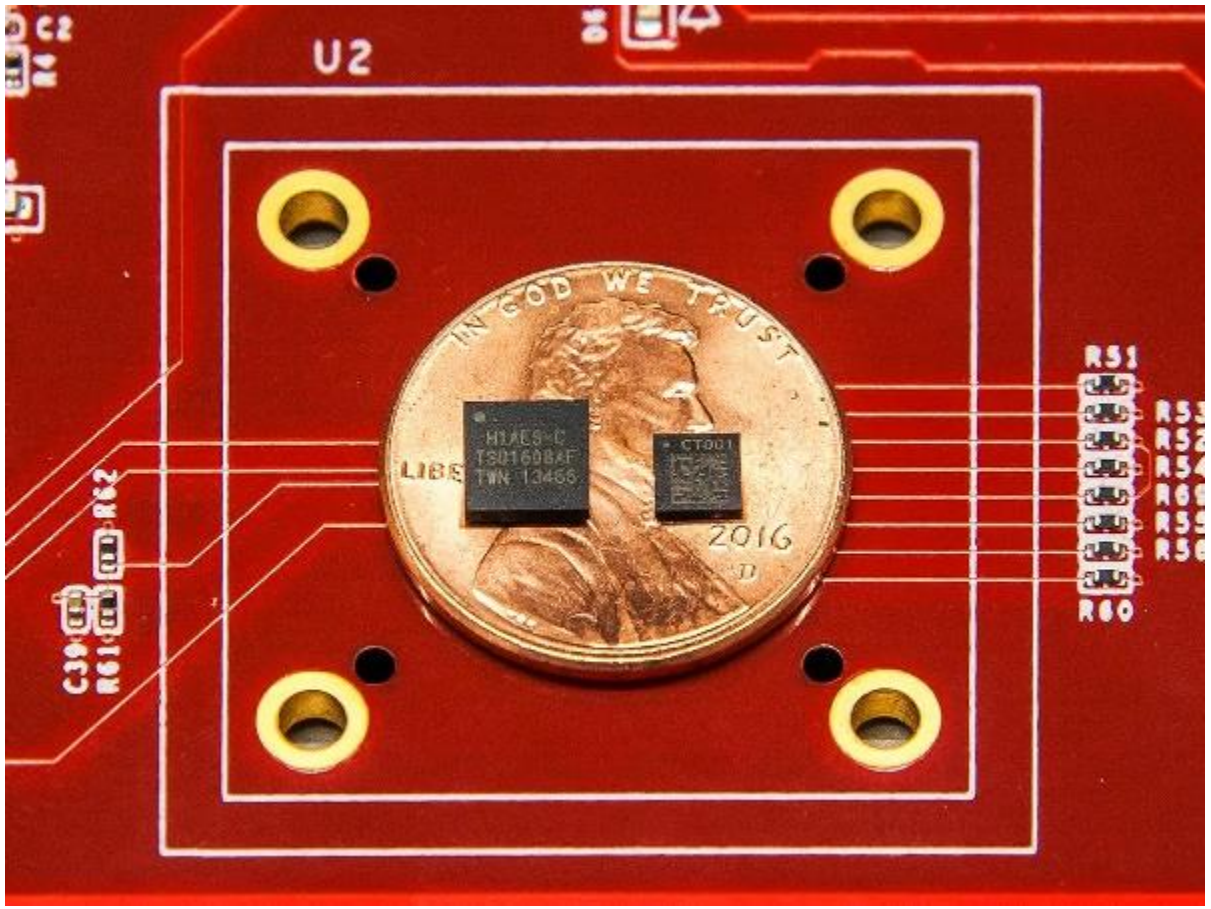
Googleのサーバ向けハードウェア



各マシンにおけるファームウェアのロードと、同社のデータセンター内におけるその他の暗号化機能の提供をセキュアにするための「**hardware root of trust**」（ハードウェアに根ざした信頼性）の実現に向け、Titanがいかに機能するのかについて説明している。

（出典）ZDNet 「グーグル、セキュリティチップ「Titan」の詳細を説明」

Googleのスマートフォン向けハードウェア



『スマートフォン「Pixel 3」に搭載されたグーグルのセキュリティチップ「Titan M」（写真右）と、サーヴァー向けの「Titan」（写真左）。PHOTOGRAPH COURTESY OF GOOGLE』

（出典）WIRED 「グーグル「Pixel 3」のセキュリティチップは、こんな場面で真価を発揮する」

（出典）CNET
「グーグル、デジタルキーやモバイルIDの導入促す「Android Ready SE Alliance」発表」

『SEはセキュアエレメントの略で、Googleの「Titan M」チップなど、耐タンパー性を備えたディスクリートハードウェアのことだ。（中略）
最近のスマートフォンは多くがSEを搭載している。このアライアンスの目的は、「Pixel」デバイスでTitan Mチップを耐タンパー性の**ハードウェアエンクレーブ**として利用する方法について、AndroidのOEMメーカー各社の仕様を標準化することだ。』

各社各種のRoot & Chain of Trust

各社各種のRoot & Chain of Trust(と解釈できる)施策を推進している。
ハードウェアベースの場合と、そうでない場合がある。

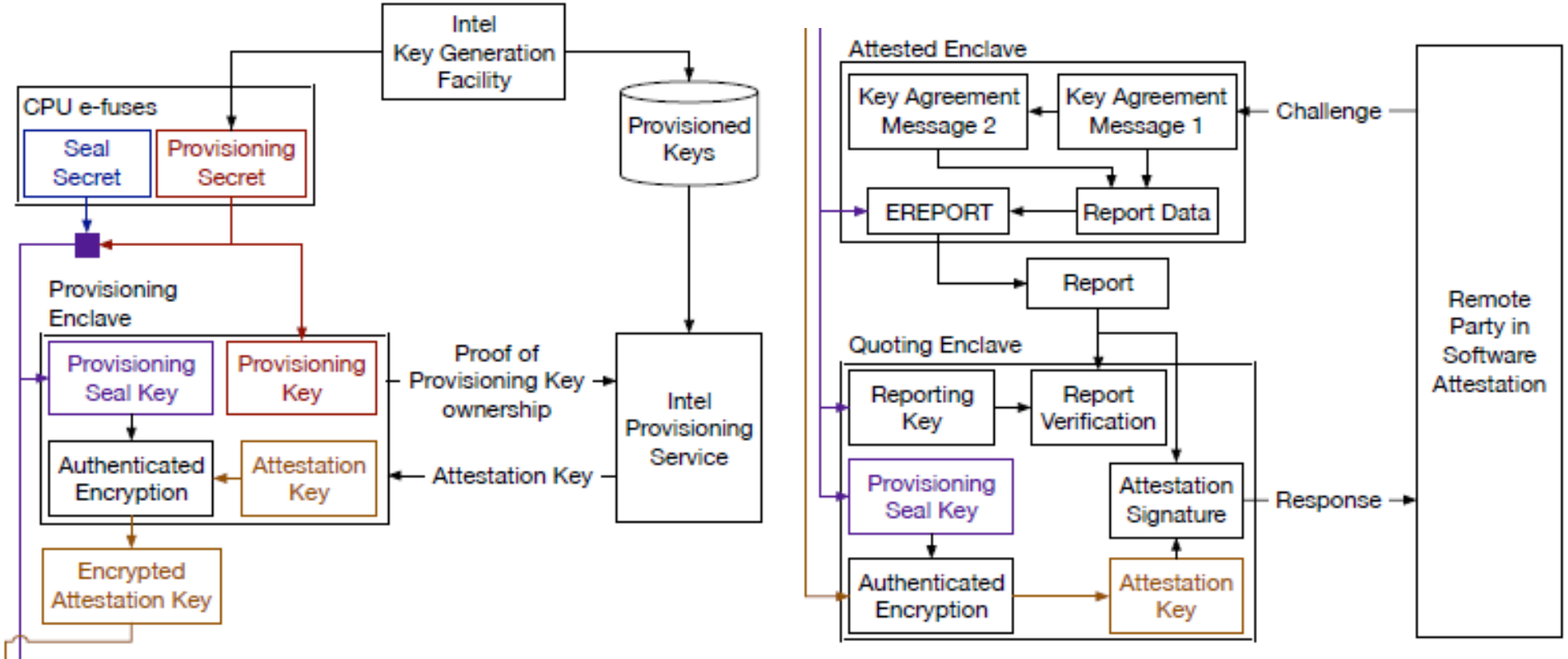
※緑字は言及済み
※赤字は以降で紹介します

【ヒトのRoot & Chain of Trust】
・国家/マイナンバー/JPKI
・GAFAM/ID/決済サービス
Google(TEE/SE/Titan-m), Apple(TEE/SE/Secure Enclave Processor),
Facebook(Libra/Diem), Microsoft(DID/VC) ※後者2点はBlockchainベース

【モノのRoot & Chain of Trust】
・クラウド Google(Titan), Microsoft(Pluton),
Amazon(AWS Nitro Security Chip) ※Nitro EnclaveはHypervisorベース
・CPU/MPU Intel(SGX,TDX), AMD(SEV), ARM(CCA,Trustzone)
・IoT/サプライチェーン
Google(OpenTitan), Microsoft(Pluton), TCG(TPM), FIDO(FIDO)

Root & Chain of Trust 事例 (Intel SGX)

・初期鍵は、工場出荷時にCPU内のe-fuseに焼き付けられている。
　ざっくり、Sealing用の共通鍵と、Provisioning用の秘密鍵が入ってる。
　Provisioning Keyは、IPS(Intel Provisioning Service)で
　Attestation Keyと交換される**(!)**→Attestation KeyでReportに署名を打つ。
→RP(Relying Party)は、IAS(Intel Attestation Service)に署名を検証させる。



（出典）
Intel SGX Explained,
IACR ePrint, 2016

Root & Chain of Trust 事例 (Intel SGX DCAP)

- Intel SGX DCAP (Data Center Attestation Primitives)
  データセンタやクラウド事業者(3rd-party)が、
  自前でAttestation Serverを運用するための拡張機能
- PCK (Provisioning Certification Key) と証明書が、
  3rd-partyに配布され、中間CA的な役割を持つ。

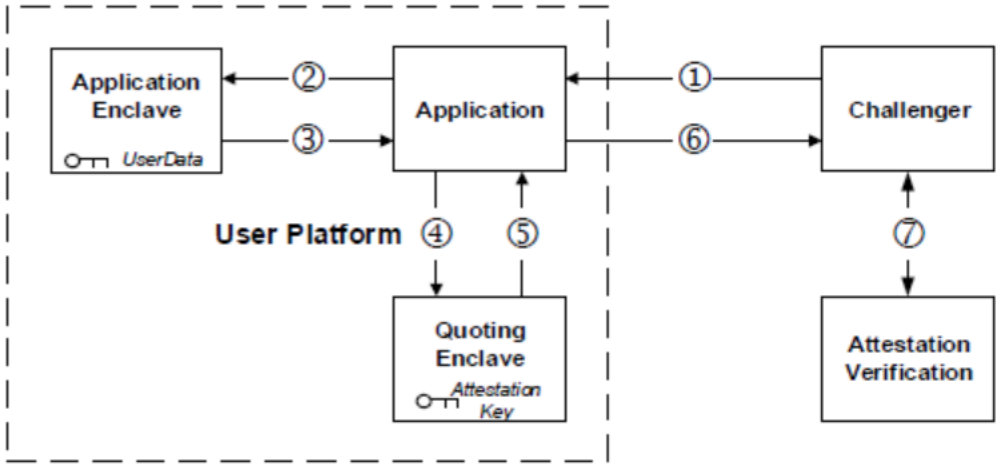


Figure 1: Attestation Flow

（出典）
intel-sgx-support-for-third-party-attestation, Intel Corporation, 2018

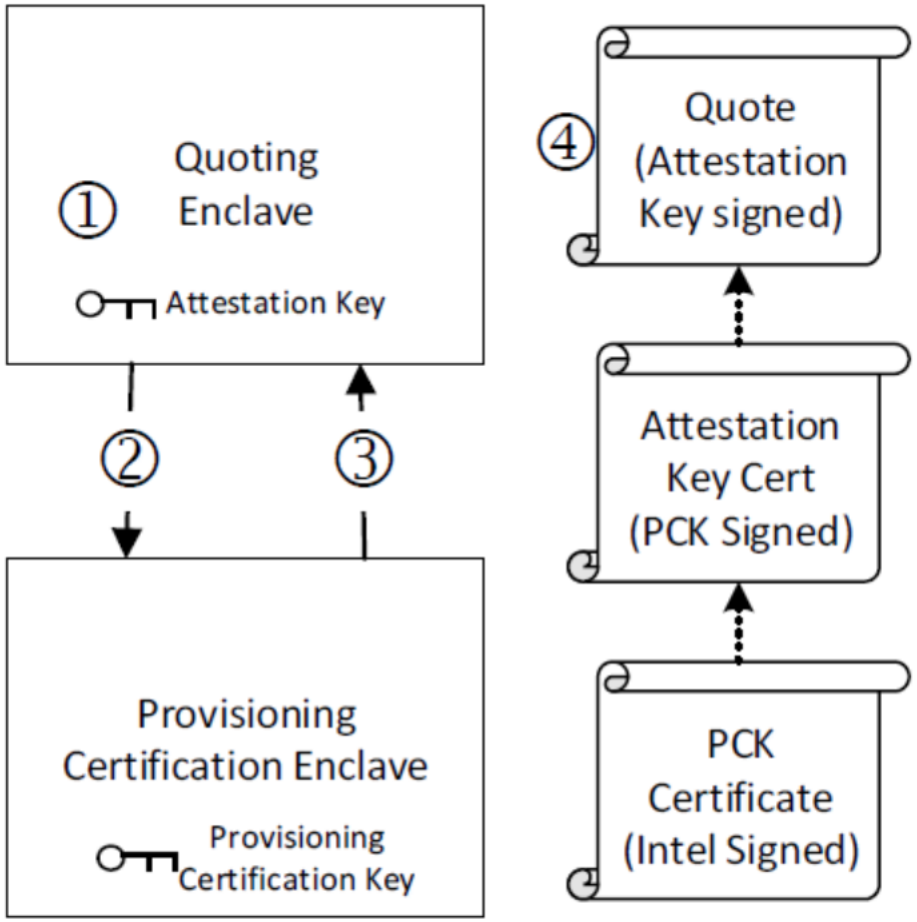


Figure 3: Quote Certificate Chain

Root & Chain of Trust 事例 (AMD SEV)

・ルート証明書は2つある。
AMD Root と Owner CA (＝プラットフォーム事業者に対応)
・CPU固有の鍵がOTP-Fuseに焼き付けられている。
Chip Endorsement Key ⇒ これがRoTとして機能。
・Platform Endorsement Key は、
Chip Endorsement Key と Owner CA で二重に署名される。
・Platform Endorsement Key から、
DH鍵シェアやトランスポート鍵が生成される。

※これらは、当該論文著者のファームウェア解析により
得られた結果で、AMDが公式に公開している内容ではない様子

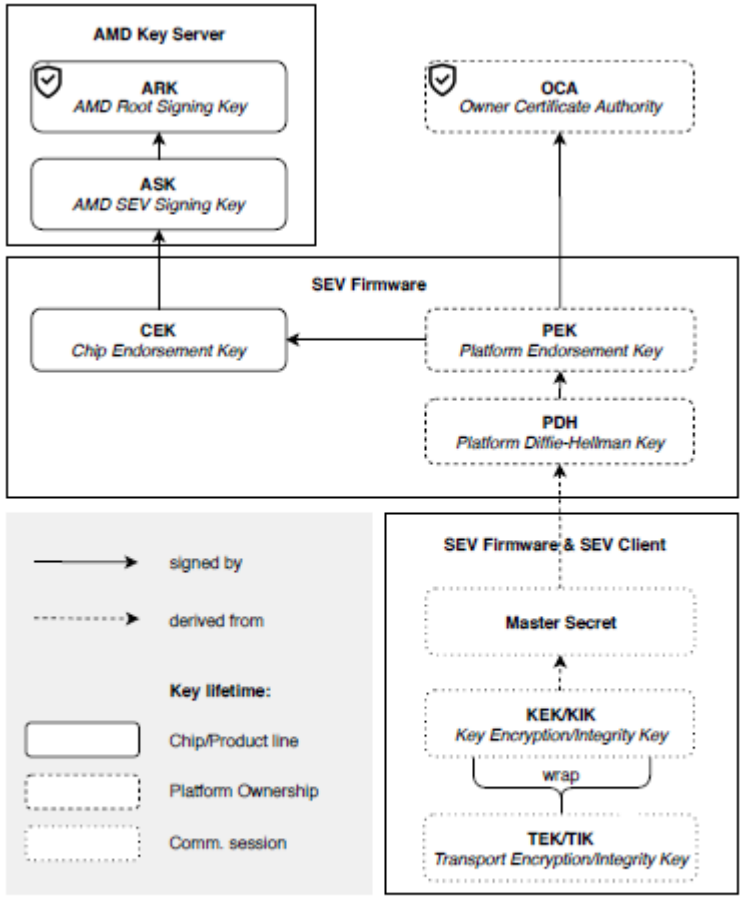


Figure 1: Cryptographic keys in SEV. A shield denotes the key as the root of trust for the corresponding certificate chain. Boxes show the scope of the respective keys.

(出典)
Analyzing AMD SEV's Remote Attestation, ACM CCS, 2019

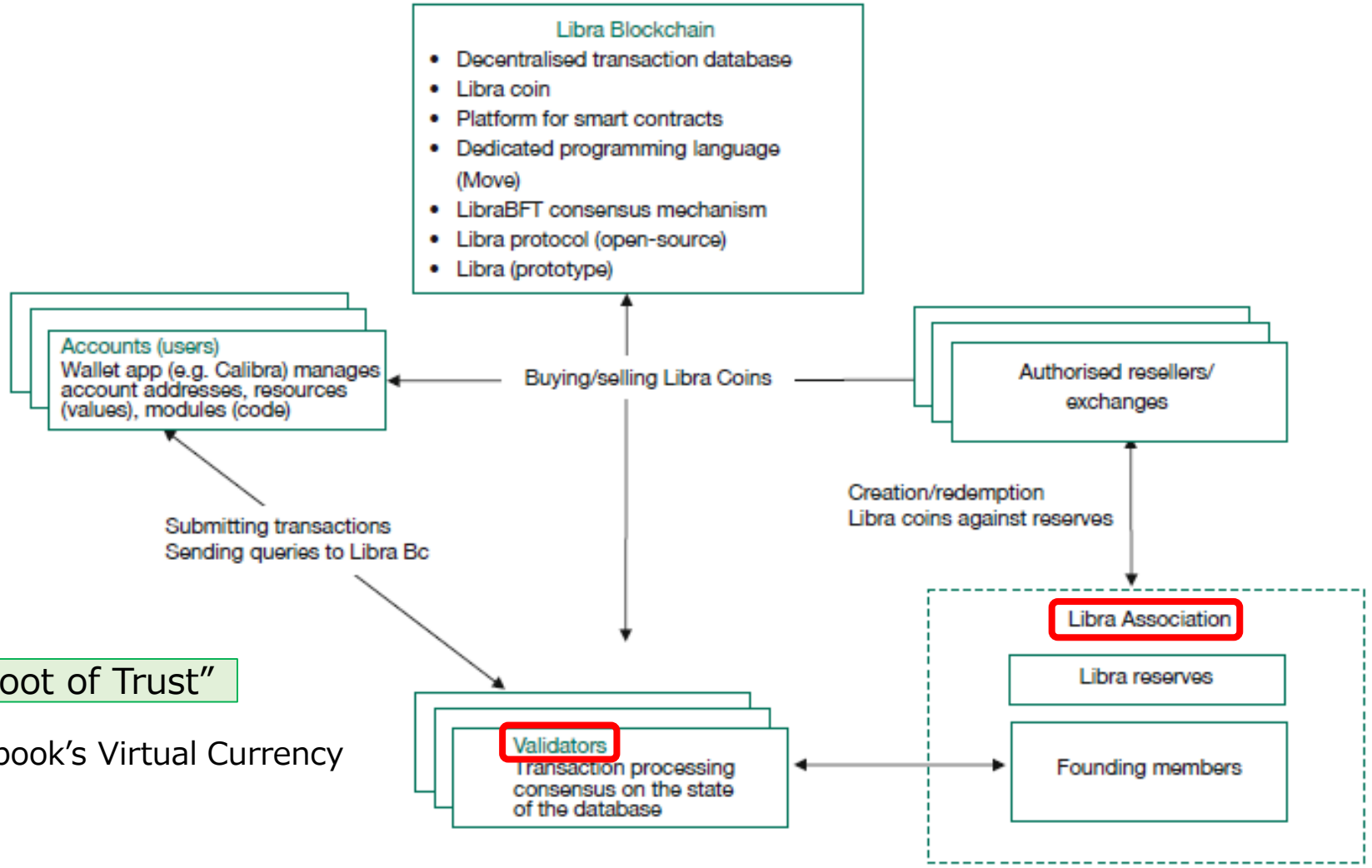
Root & Chain of Trust 事例 (Facebook(Libra/Diem))

『Maintaining the integrity of the system by preventing double spending of monetary units, manipulation attacks from outside the system or theft of private keys are common challenges of distributed ledger systems.

Furthermore, the Libra Blockchain is at least for the time being a 'permissioned' blockchain, as validators require specific permission from the Association, rather than automatically receiving the status of a validator if certain predefined technical requirements are met.』

→検証者(validators)は、Libra Associationから特別な許可を得る必要がある（=事実上のAuthority）ここが "Root of Trust"

Figure 1
The basic architecture of the Libra ecosystem



（出典）Libra — A Differentiated View on Facebook's Virtual Currency Project, Volker Brühl, Intereconomics ,2020

Root & Chain of Trust 事例 (Microsoft (Decentralized ID/Verifiable Credentials))

・SSI(Self-Sovereign Identity)という構想を実現するための方式として
DID(Decentralized Identity) & VC(Verifiable Credentials)が存在

・MirosoftがDID&VCサービスを2021年提供開始。“ION(Identity Overlay Network)”というブロックチェーンベースの仕組み, DIDと並列してDecentralized PKI, “SideTree”というプロトコルを開発。

・SideTreeプロトコルは、ビットコインとIPFSのオーバーレイ(L2)（右図参照）

・コンセンサスアルゴリズムとしては、ビットコイン側にProof of Workはある、
SideTree仕様には、Proof of Fee という文言もある(MAY), PKIに関する記載が多数
IPFSは、Content-addressable storage (Distributed Hash Table)であり、
IPFS単体ではByzantine問題は存在

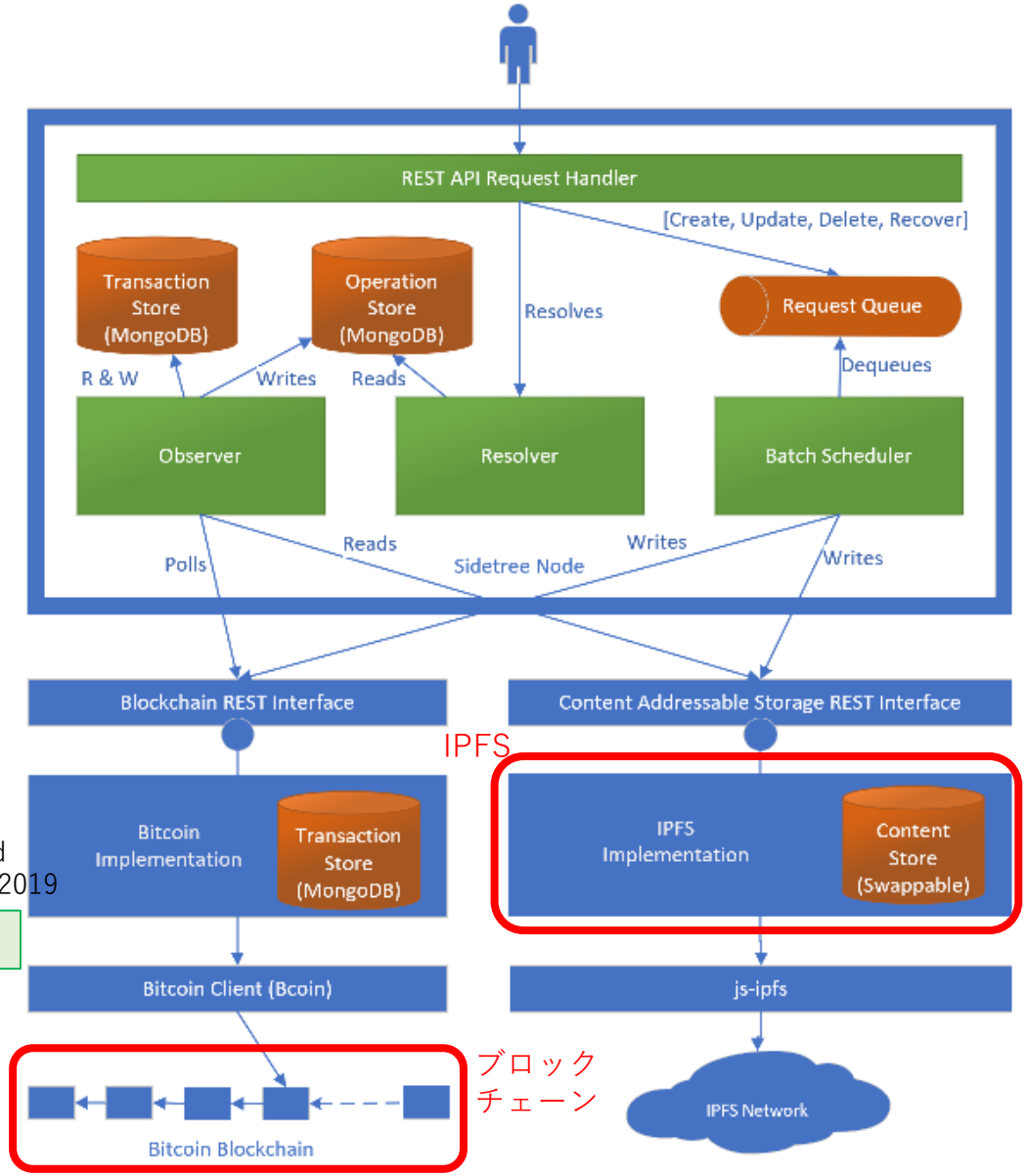
When Blockchain Meets Distributed File Systems: An Overview, Challenges, and Open Issues, IEEE Access, 2020
A Survey of DHT Security Techniques, ACM Computing Surveys, 2011

・IONの仕組み上, 追加のコンセンサスは必要無いと書かれているが、
上記の階層構造の中で、”Proof of Fee” が機能している様子。
また、ノードを管理運用している中で数社は公表されている。

Toward scalable decentralized identifier systems, Microsoft, 2019

”Trusted Node”??

(Permission-lessと書かれているが、ID管理という機微な仕組みをすべて市場原理に任せるとは想像し難い?? 一定のガバナンスが必要とされるかと想像。”Proof of Fee”がポイントか?? →厳密にはMSのDID/VC担当者さんに講演をお願いしたい！)



（出典）Sidetree Core Node.js Reference Implementation Document

本日の論点まとめ

- ”Centralized”と”Decentralized”は、
  Chain of Trust, Root of Trust (署名鍵,合意形成を含む) を巡る議論
  （と思ってる）

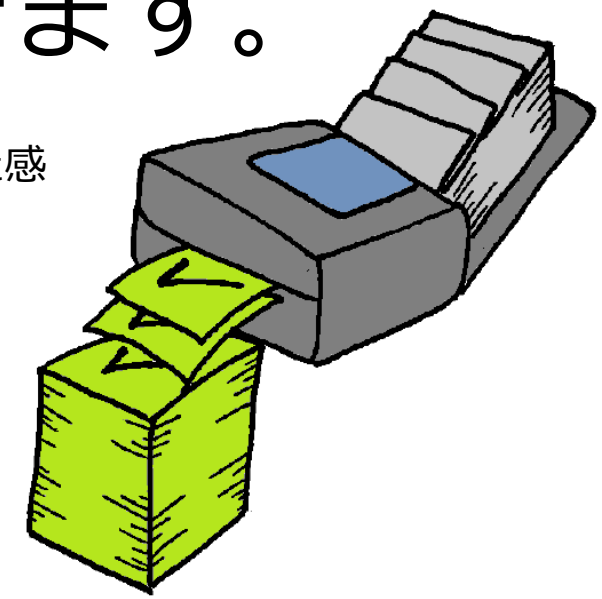
- PKIベースかBlockchainベースかを問わず、
  サービス設計やサービス利用で重要なことは、
  「**そのサービスにおける**
  Root of Trust は何か, Chain of Trust は何か」
  を見極めること(Verification)（かも知れない）

→上記ポイントを抑えれば、
  ステークホルダ間でより議論が深まる（はず）

おわりに

NTTグループは、
お客様に安心してご利用いただけるような、
ICTサービスと技術を提供していきます。

※取って付けた感



免責事項

・本講演の見解は、講演者自身によるものであり、
　所属組織による公式な見解とは関連ございません。

・本講演の記載および発言について、
　訂正すべき箇所があれば、ご指摘頂けますと幸いです。

・講演中の会話表現については、フィクションです。

※取って付けた感

（参考）今回は扱えなかったキーワード群 (1/2)

紙面の都合上、Trust関連で今回は扱えなかったキーワードにポインタを張っておきます。

・Trusted Computing：
TPM(Trusted Platform Module)の話。2000年代からあるはず。
DRM云々の議論も有り、歴史を紐解くだけでボリュームが凄いので、今回は割愛。
現代版の振り返りは、右記資料参照「PKI & Trust Days 2021, トラストを確立する技術の概要, セコム 宮澤慎一」

・Trustworthy Computing：Microsoftの戦略の話。2000年代。

・Trusted Network Connect：TPMを活用したネットワークセキュリティの話。2000年代からある。

・ゼロトラストネットワーク：鈴木研吾さんの著書を参照
＋ NIST SP800-207「ゼロトラストアーキテクチャ Zero Trust Architecture」

・米国政府関連:Trust Framework, Trusted Internet Connection, 等々

・欧州政府関連:Trust Service, eIDAS, 右記資料群参照「PKI & Trust Days 2021, デジタルトラストにおける法と技術のあり方」
（cf. トラストサービス推進フォーラム, デジタルトラスト協議会）

・最近のデータ流通関連では GAIA-X, DATA Trust (弊社商標らしい), 情報銀行(信託=Trust) 等々

・・・その他にも沢山あると思います。すべてを拾い切れずに申し訳ないです。

（参考）今回は扱えなかったキーワード群 (2/2)

紙面の都合上、Trust関連で今回は扱えなかったキーワードにポインタを張っておきます。

・Trust over IP Foundation
Linux Foundation 傘下で発足。Accenture, IBM, MasterCard, 等
Self-Sovereign Identityを推進する Sovrin Foundation と連携

全体的に、目的および手段共に、Trusted Web推進協議会の取組みに似てる。
目的としては、インターネットへの“digital trust layer”のオーバーレイを志向。
実現手段としては、ブロックチェーン(Hyperledger Aries)＋W3C Verifiable Credentials
Microsoftによる、ION(Identity Overlay Network)+DID+VCと方向性は近しい。
GAFAの加入が見られないことから、Decentralized Identityを志向していると思われる。

”digital trust” は “cryptographic trust at the machine layer” と
“human trust at the business, legal, and social layers” で実現されるとしている。
これらをプロトコルスタックに“dual stack” designとして反映しようとしている。
（the ToIP Governance Stack for human trust and the ToIP Technology Stack for technical trust）

eKYCがスコープに入ってて、Trust(信頼)というよりCredit(信用)な印象もある

（参考）The Creation of the Trust over IP (ToIP) Foundation, Sovrin Foundation, 2020.

・・・その他にも沢山あると思います。すべてを拾い切れずに申し訳ないです。

Special Thanks

・色々と情報交換ありがとうございました！
セコム 松本 泰 様, 宮澤 慎一 様
・Intel SGXの入門に誘ってくれてありがとう！
Y! 彈 雄一郎 君

さいごに
沢山のイラストを提供してくれた
長津先生に大いなる感謝を込めて

（参考）TEE/Enclave とは？

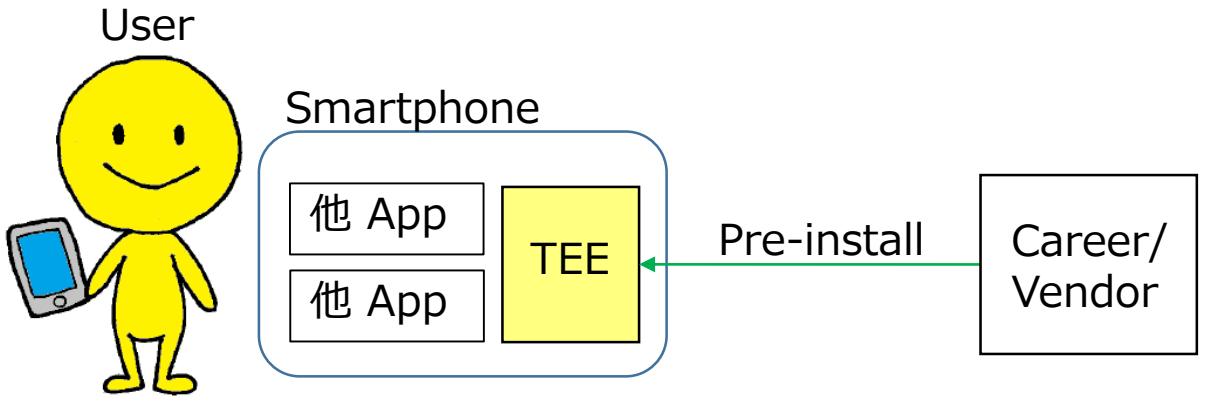
そもそも、
TEE(Trusted Execution Environment)
って何ですか？？
Secure Enclave って何ですか？？

（参考）TEE/Enclave とは？

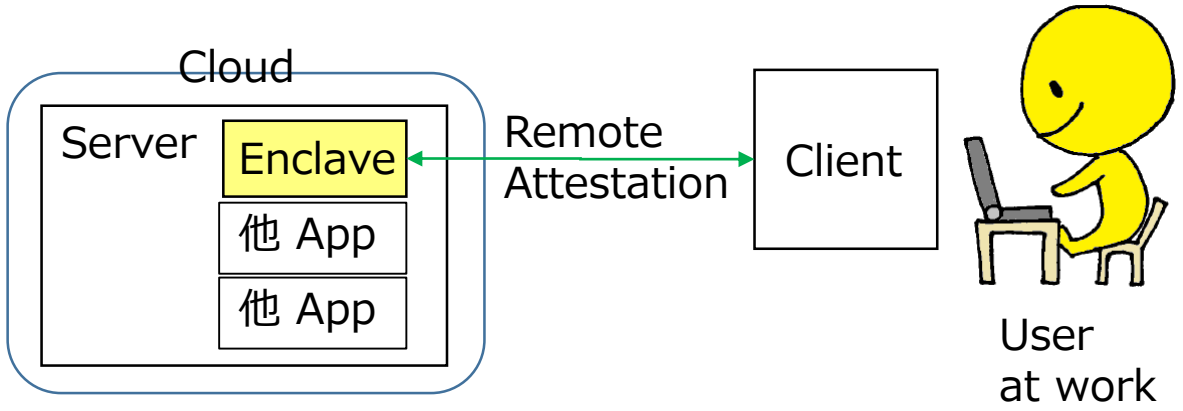
※詳細は PKI & Trust Days 2021
セコム 宮澤慎一 先輩の資料をどうぞ
「トラストを確立する技術の概要」

ざっくり言うと・・・

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。

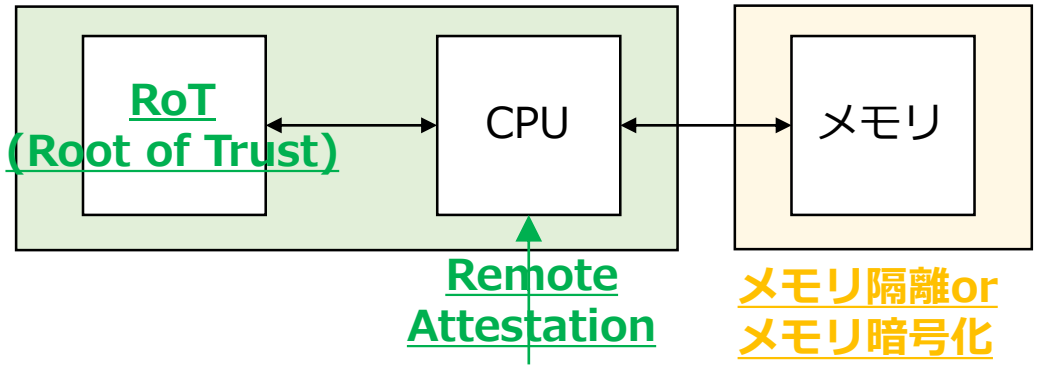


Enclave(飛び地)は、法人ユーザから見て、
クラウド/サーバ上の“Trusted”な領域。
機密なアプリ&データを、他Appから隔離して、
Confidentiality & Integrity に実行できる



（参考）TEE/Enclaveの定義

（アナザースカイ風に）
「貴方にとって、TEE/Enclaveとは？」



⇒下記3点の特徴を有するメモリ領域と考えます。 Thanks
NTT 千田さん！

(1)TEE/Enclave内のデータが外部から閲覧できないこと、
　TEE/Enclave内のアプリが外部から改ざんできないこと

(2)耐タンパ性を有する秘密鍵格納モジュール(**Root of Trust**)がEnclaveと共に存在すること

(3)Enclaveが動作するハードウェア、および、
　Enclave上で動作するソフトウェアを含めた“アイデンティティ”情報を、
　Enclave利用者が遠隔から検証できること(**Remote Attestation**) . 検証情報に基づいて、
　Enclave利用者がEnclaveとセキュアチャネルを確立できること(**Attested TLS**).