JNSA PKI & Trust Days 2021

Confidential Computingの技術動向 ～TEE/Enclaveの便利な活用例～

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

(最近) **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

はじめに

本講演では、クラウドシフトに向けて
ゼロトラスト環境でマイクロサービスの
DevOpsにAIを使ってDXします！

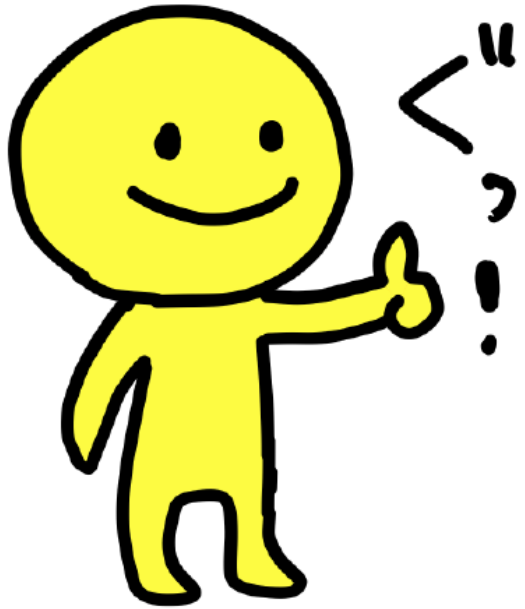
はじめに

・・・・・冗談です・・・・・

はじめに

本講演では、
TEE & Secure Enclaveの活用事例として、
Confidential Computing を 紹介します。

（注）カタカナの多さは変わってない



はじめに（続）

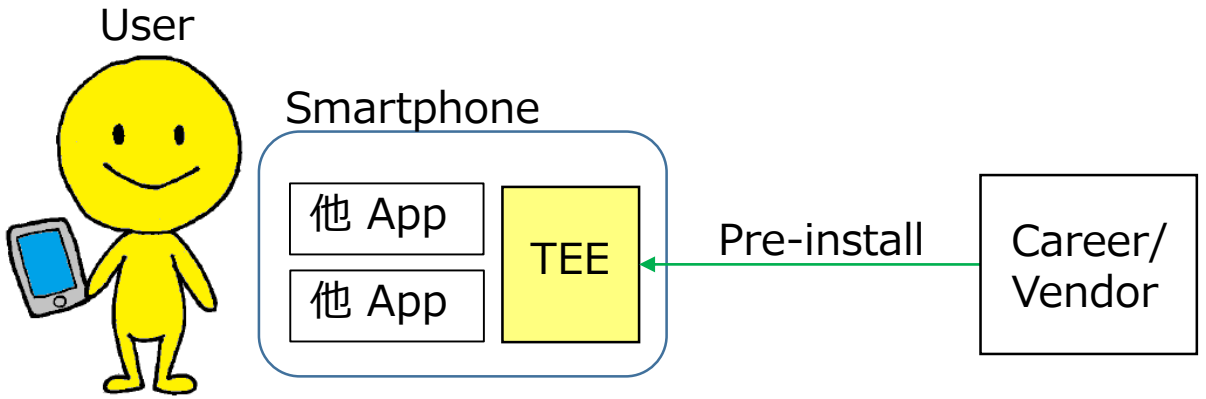
ところで、
TEE(Trusted Execution Environment)
って何ですか？？
Secure Enclave って何ですか？？

はじめに（続）

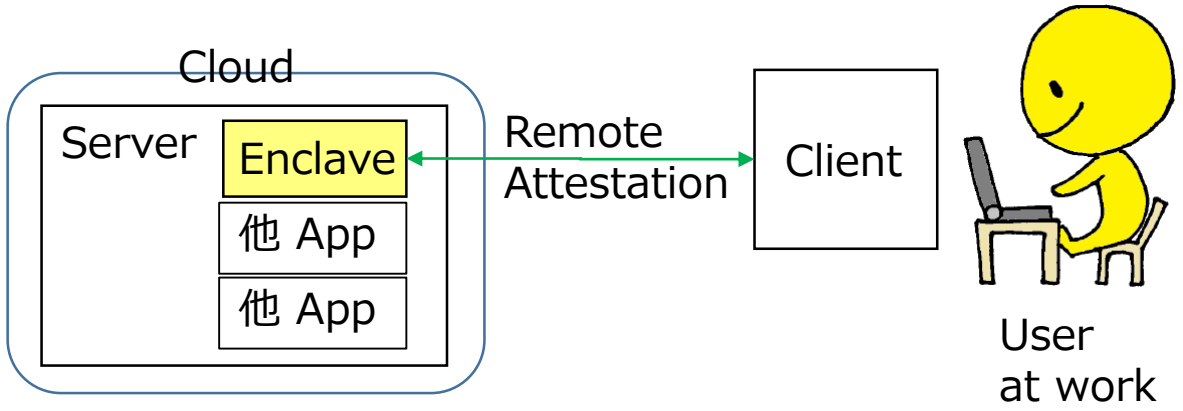
ざっくり言うと・・・

※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



はじめに（続）

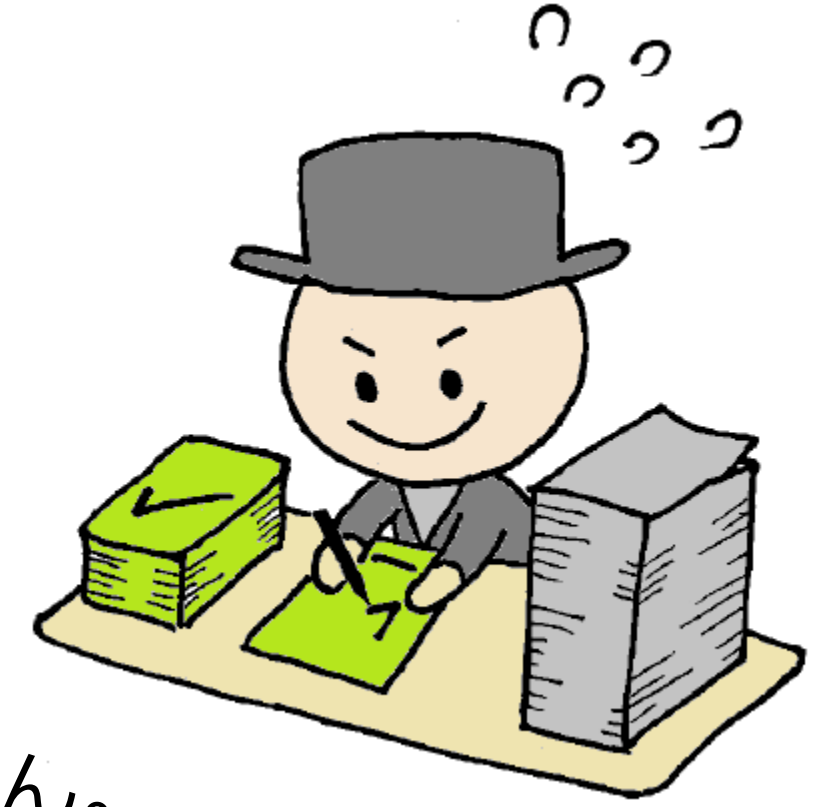
ついでに聞きたいんだけどさ、

Confidential Computing って 何？？

（上からな感じで）

※フィクションです

はじめに（続）



クラウド営業マン
「Confidential Computing では、
お客様のアプリやデータを
クラウド事業者が見ることは出来ません。
Confidentialにクラウドをご利用頂けます！」

・・・御社はどのように反応されますか？？

※フィクションです

はじめに（続）

ある顧客Aの反応
「クラウド事業者を信頼(Trust)して使ってます」

ある顧客Bの反応
「クラウドシフトとDXは 弊社の課題であるが、
　機密情報を預けるのは リスク管理として如何なものか？」

・・・御社はどんな感じですか？

※フィクションです

本日の目次

■（基本編）

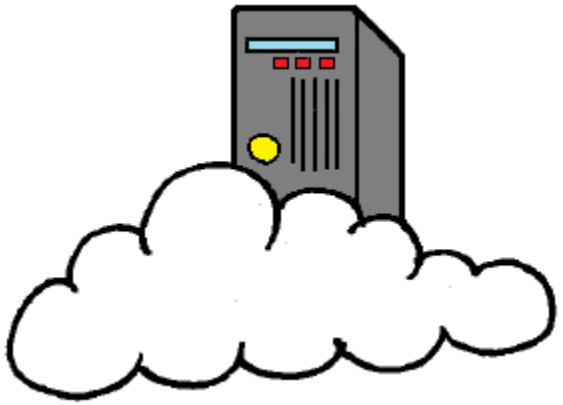
はじめに

Confidential Computing を直感的に理解する

Confidential Computing と PKI & Trust

Confidential Computing サービス事例紹介

（弊社 Confidential Computing 取り組み事例紹介）



■（応用編）

アカデミックの視点、CPUベンダの視点、

業界団体の視点、業界各社の視点、PKI/鍵管理の視点

■（パネルディスカッション導入用）

Confidential Computing と ゼロトラストNW を “トラスト最小化” の視点で整理する

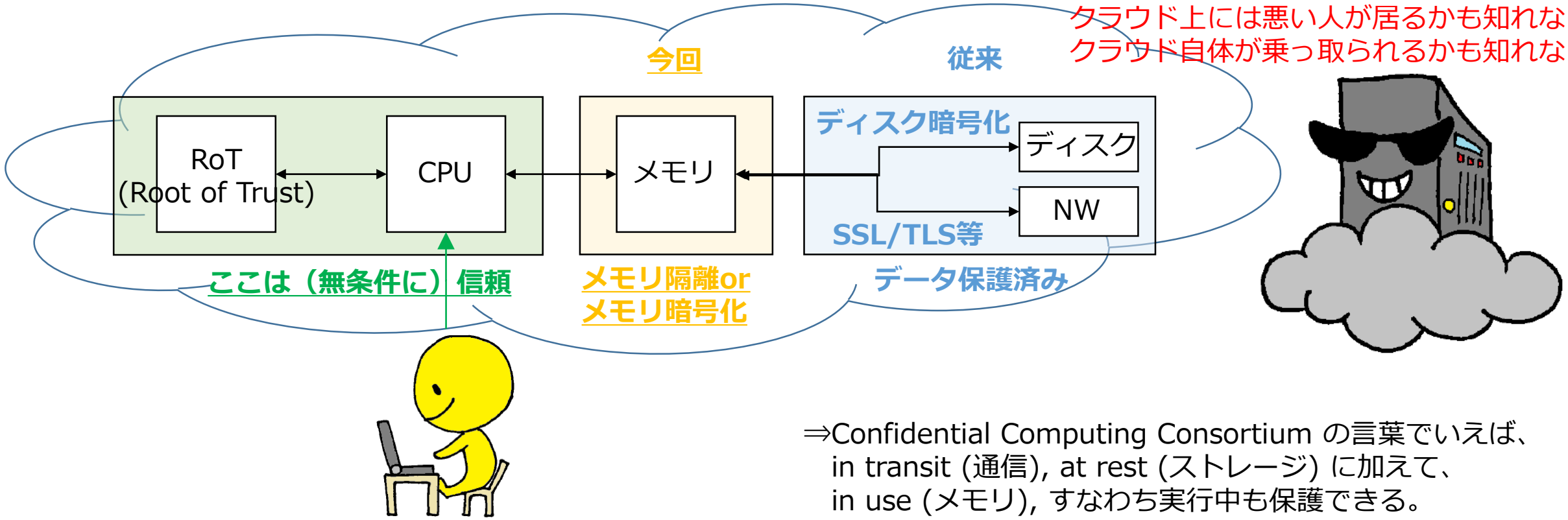
Confidential Computing とは

もう少し技術的に聞きたいんだけどさ、
Confidential Computing って 何？？

※人によって求められる
粒度・イメージは異なりますが

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**

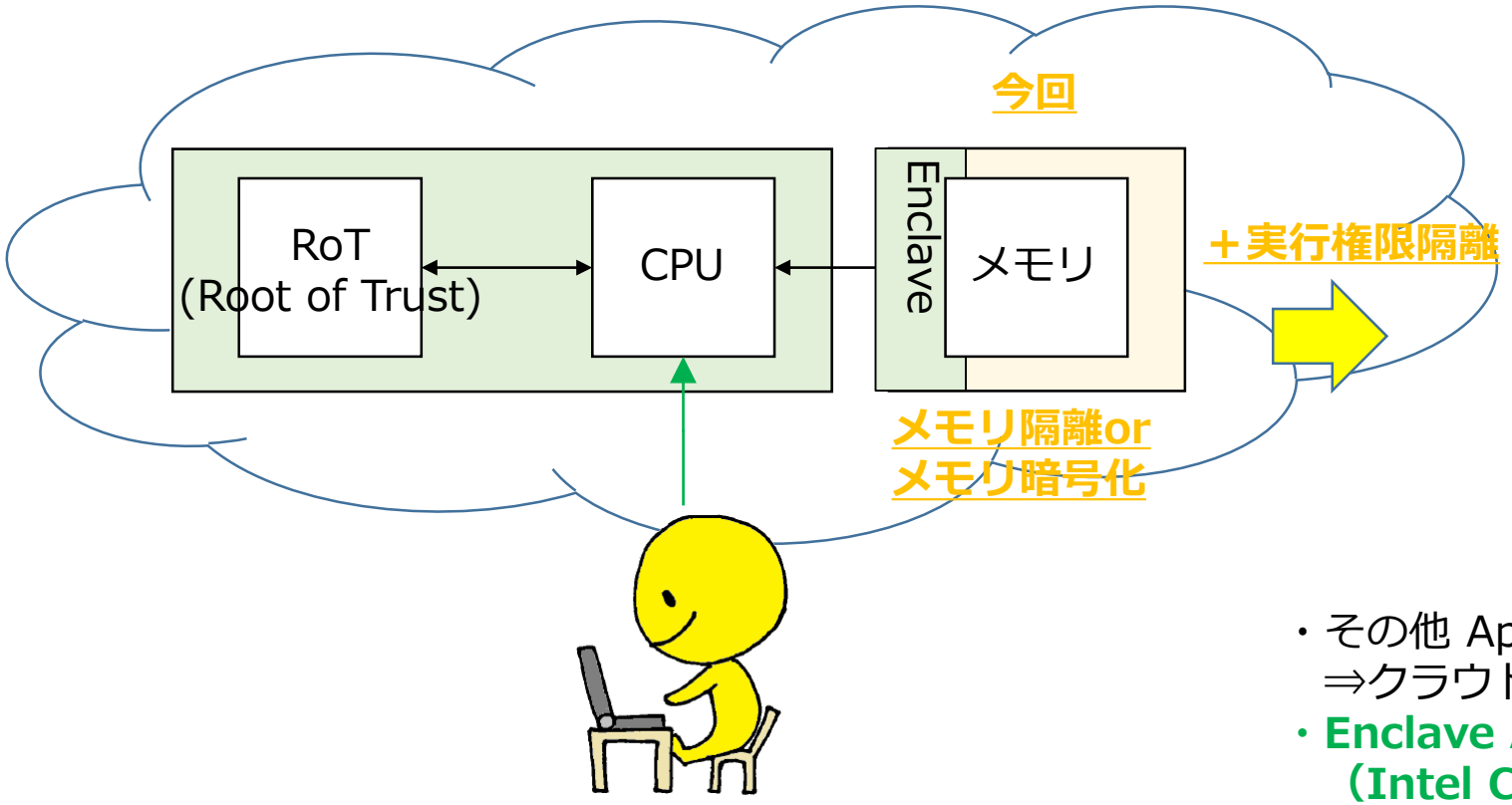


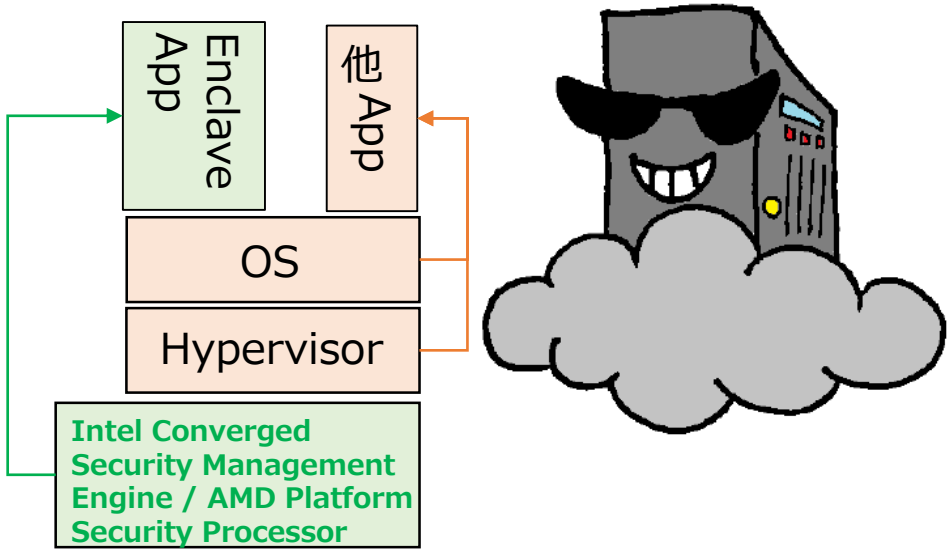
⇒Confidential Computing Consortium の言葉でいえば、
in transit (通信), at rest (ストレージ) に加えて、
in use (メモリ), すなわち実行中も保護できる。

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！



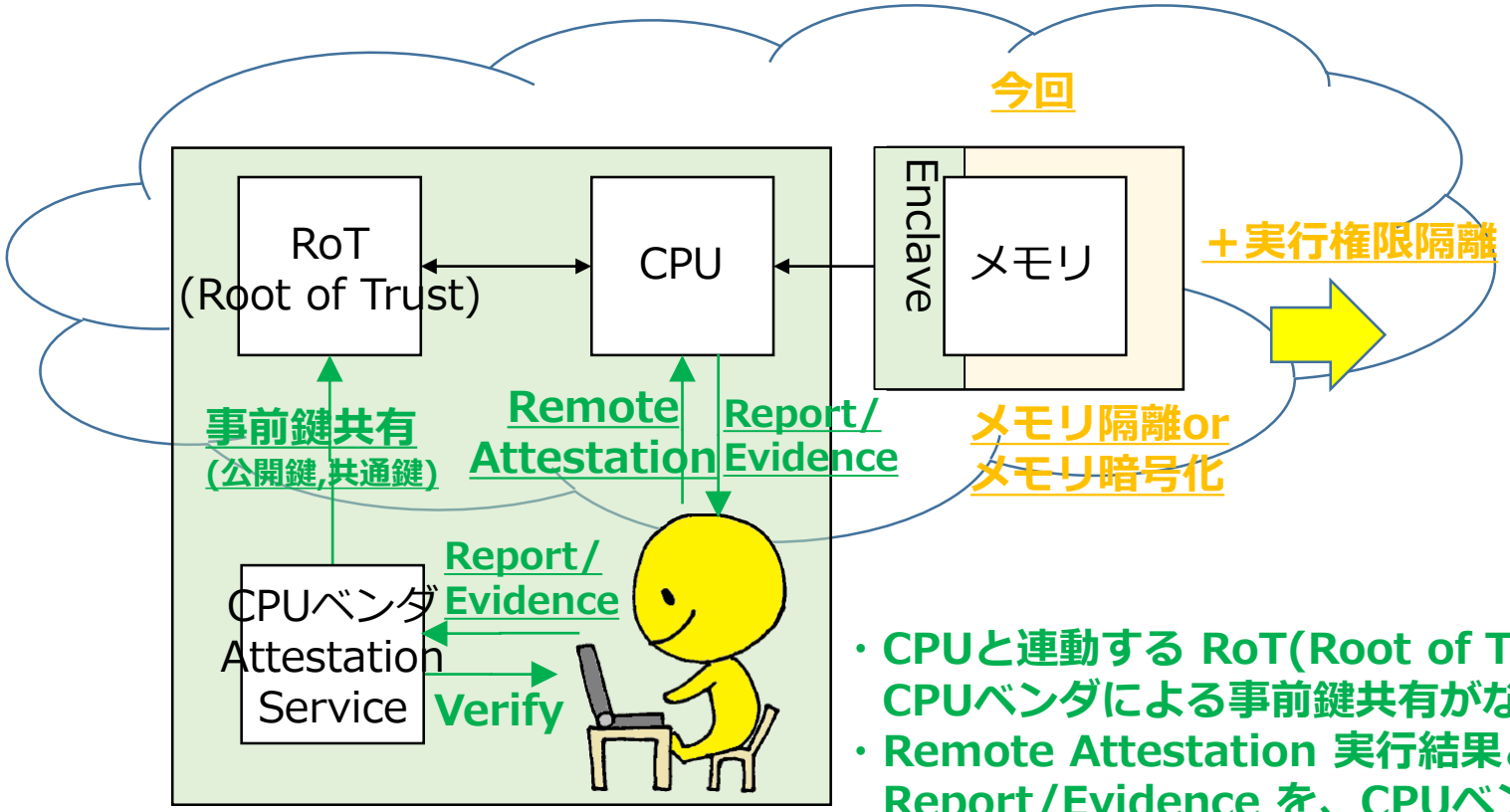


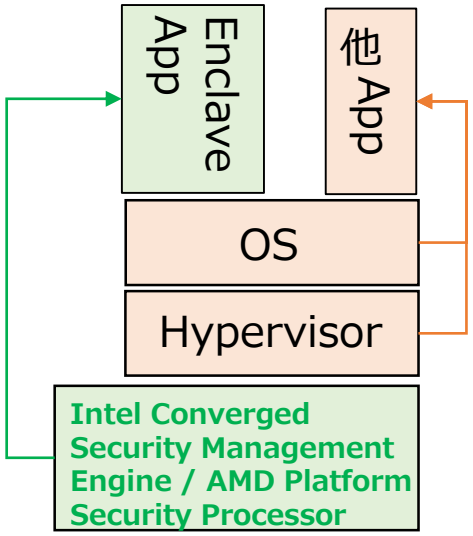
・その他 Appは OSやハイパーバイザから制御可能
⇒クラウド事業者が制御可能

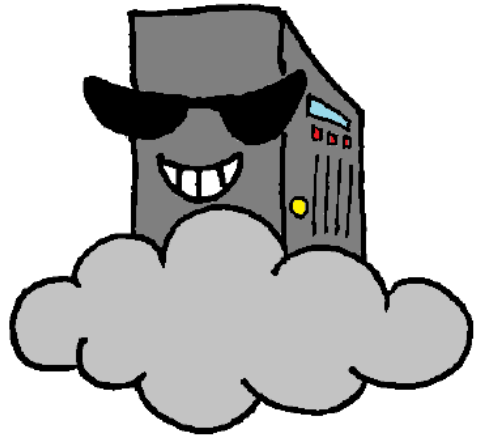
・**Enclave Appは CPUのみが制御可能**
（Intel CSME / AMD PSP のみが制御可能）
⇒クラウド事業者は制御不可
（OSやハイパーバイザから制御不可）

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！**



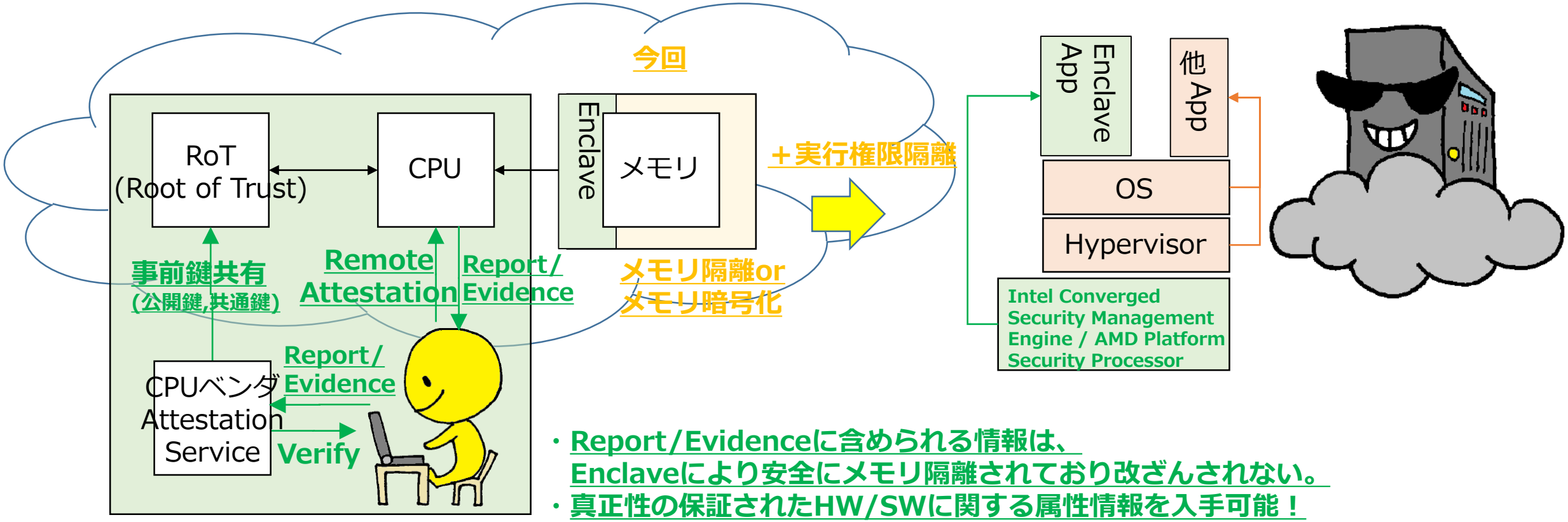




・CPUと連動する RoT(Root of Trust) に、
CPUベンダによる事前鍵共有がなされている。
・Remote Attestation 実行結果として得られる、
Report/Evidence を、CPUベンダの管理する
Attestation Service に問い合わせることで、
Report/Evidence の真正性を検証できる。

Confidential Computing とは

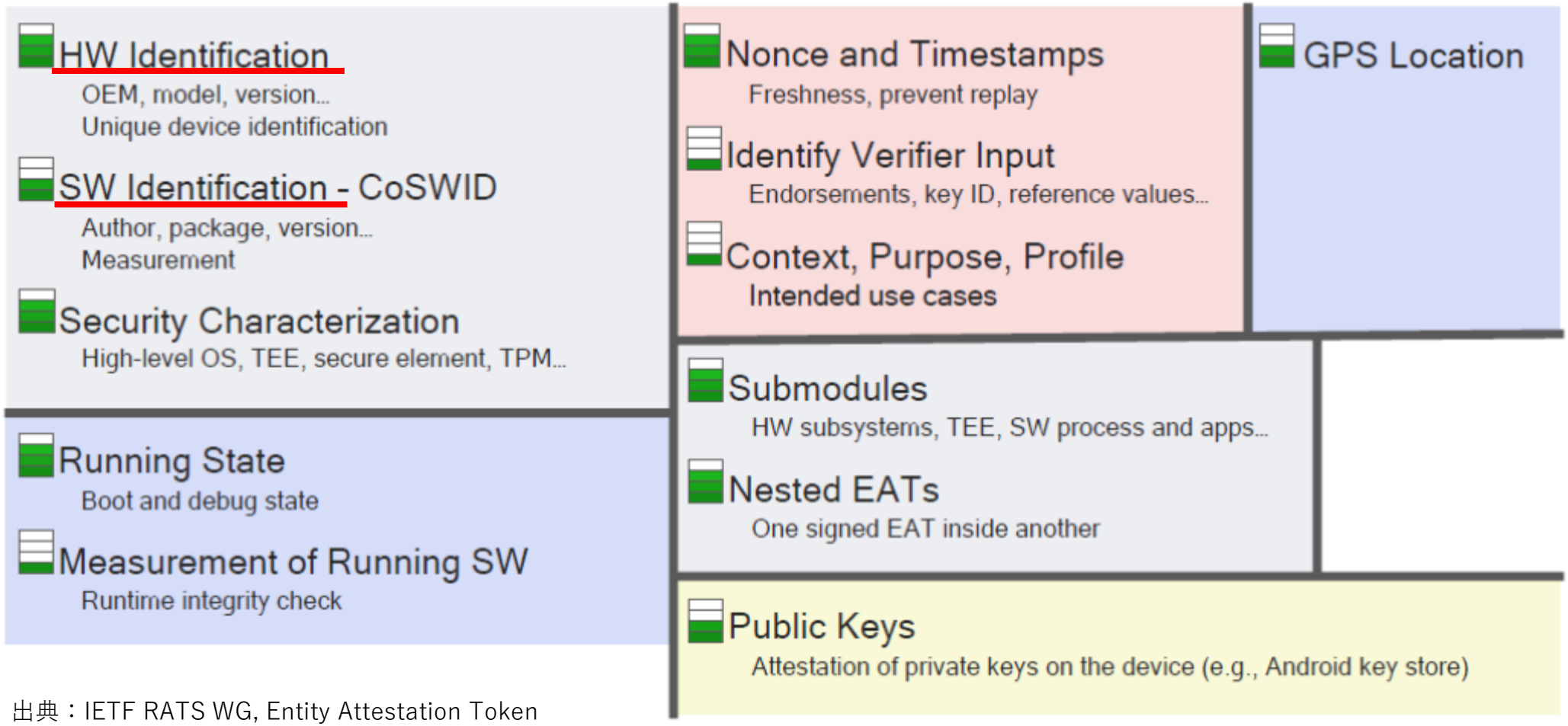
“CPUのみ”がアプリ&データを制御可能なクラウド環境
↑**(3)Report/Evidenceに(証明書的に)属性情報を含められる！**



・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**



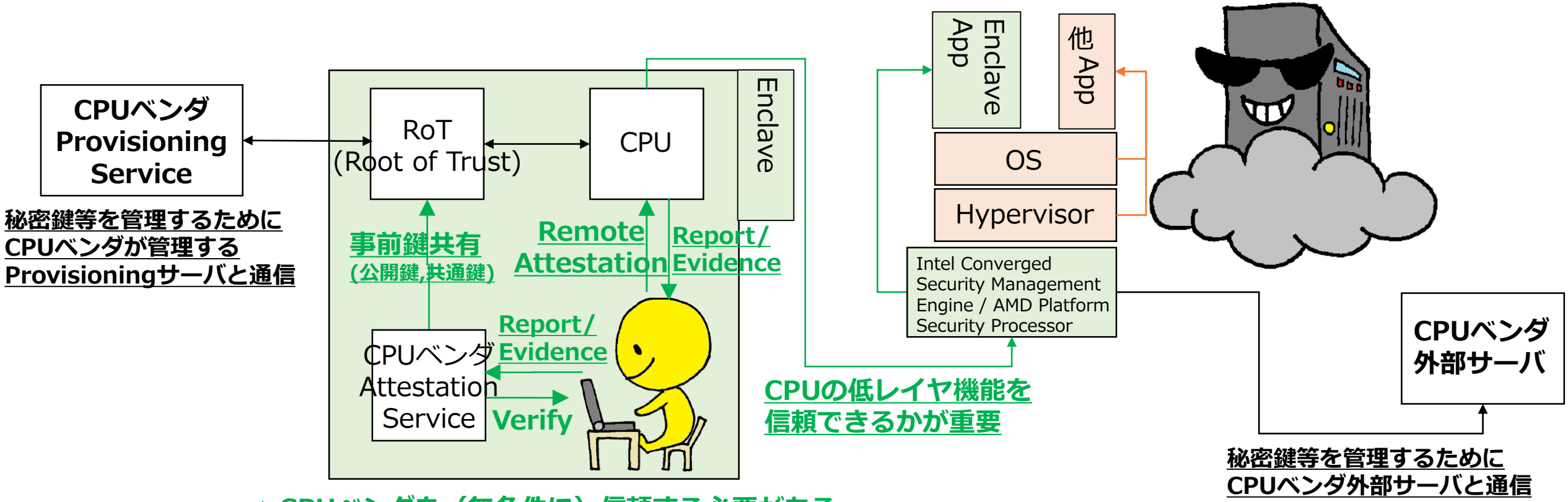
出典：IETF RATS WG, Entity Attestation Token

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？？
（上からな感じで）

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。」

Take
Away !!

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

→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。**

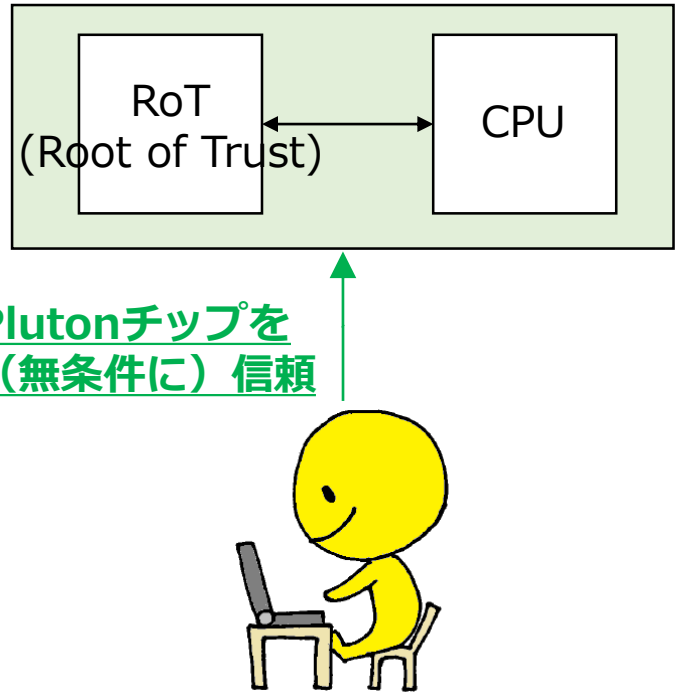
誰を信頼するか≒利用すべきサービス

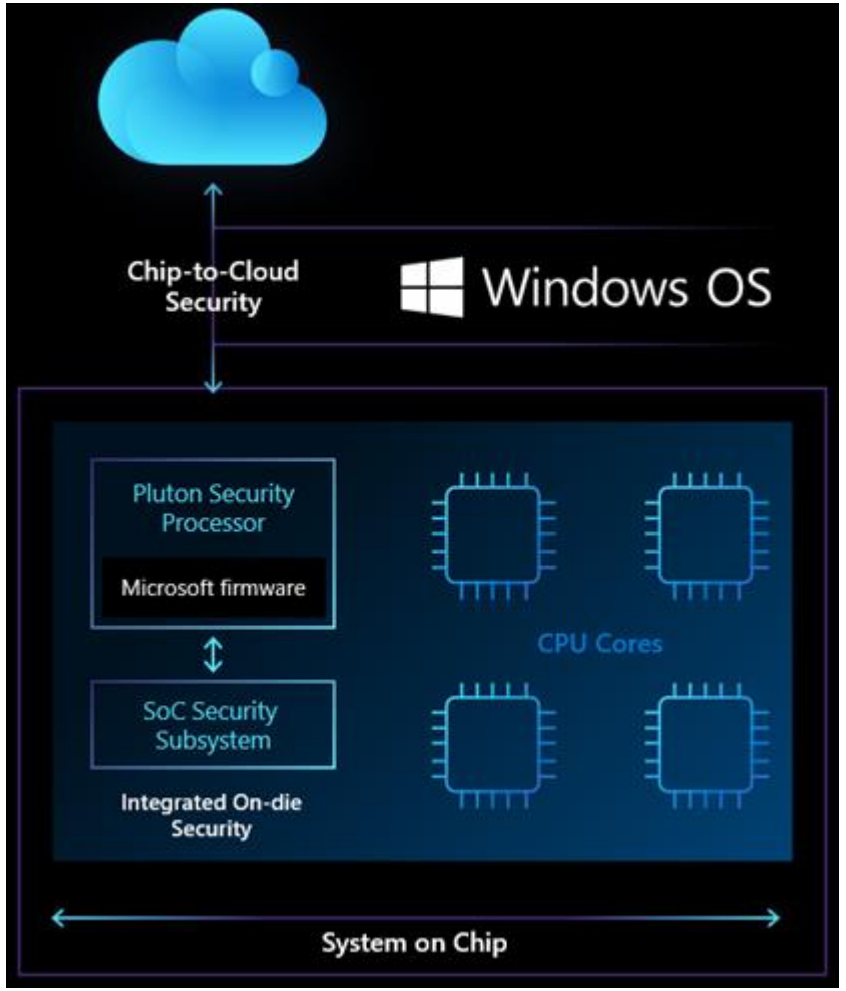
- CPUベンダを信頼する貴方
  → Confidential Computing
  あと、自社エンジニアへの投資と信頼を忘れないこと
- GAFAMを信頼する貴方
  → Google, Amazon, Microsoft が、
  それぞれに**自社製ハードウェア**を検討中 (次ページ以降で紹介)
  あと、自社エンジニアへの投資と信頼を忘れないこと
- ITベンダを信頼する貴方
  → **マネージドサービス**という選択肢。(次ページ以降で紹介)

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yurika先生のコーナーで！



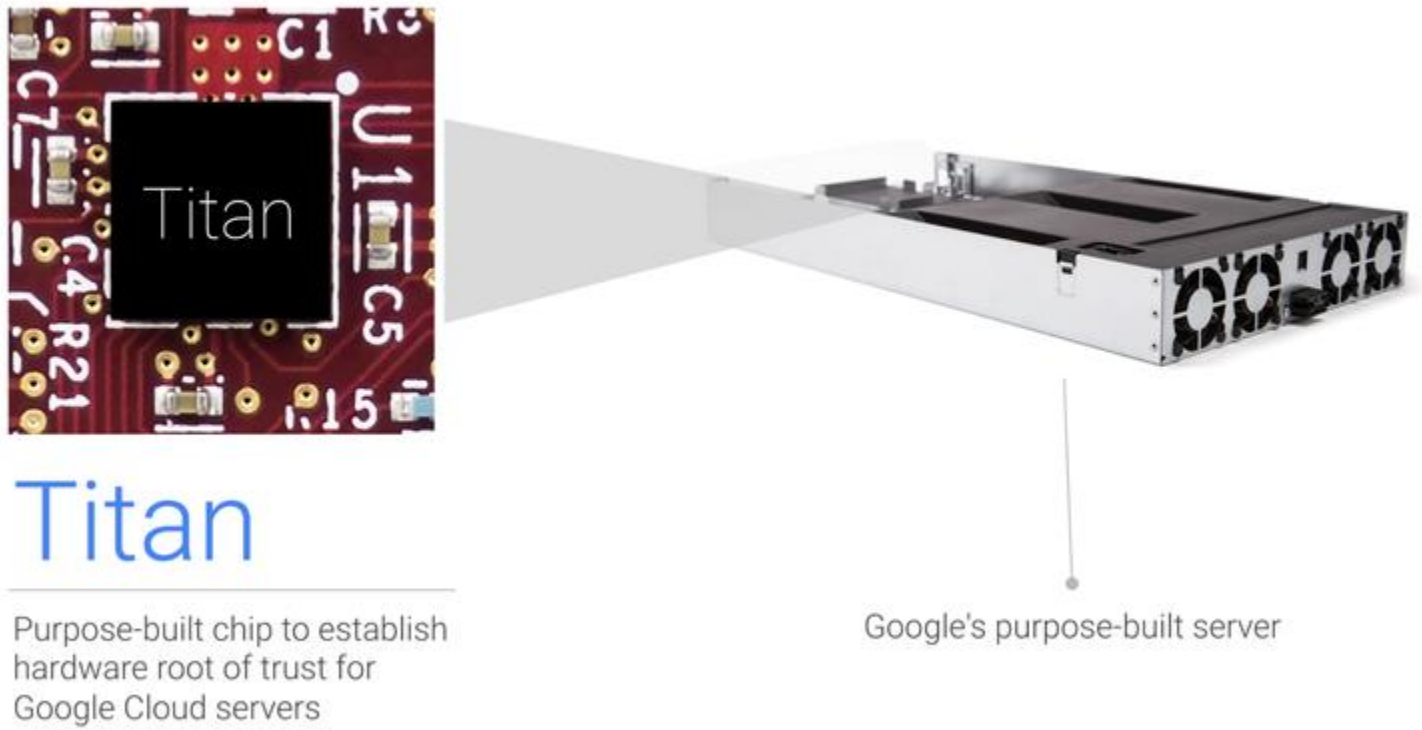


（出典）
Microsoft Pluton Processor のご紹介
– Windows PC の 未来に向けて
設計されたセキュリティチップ

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

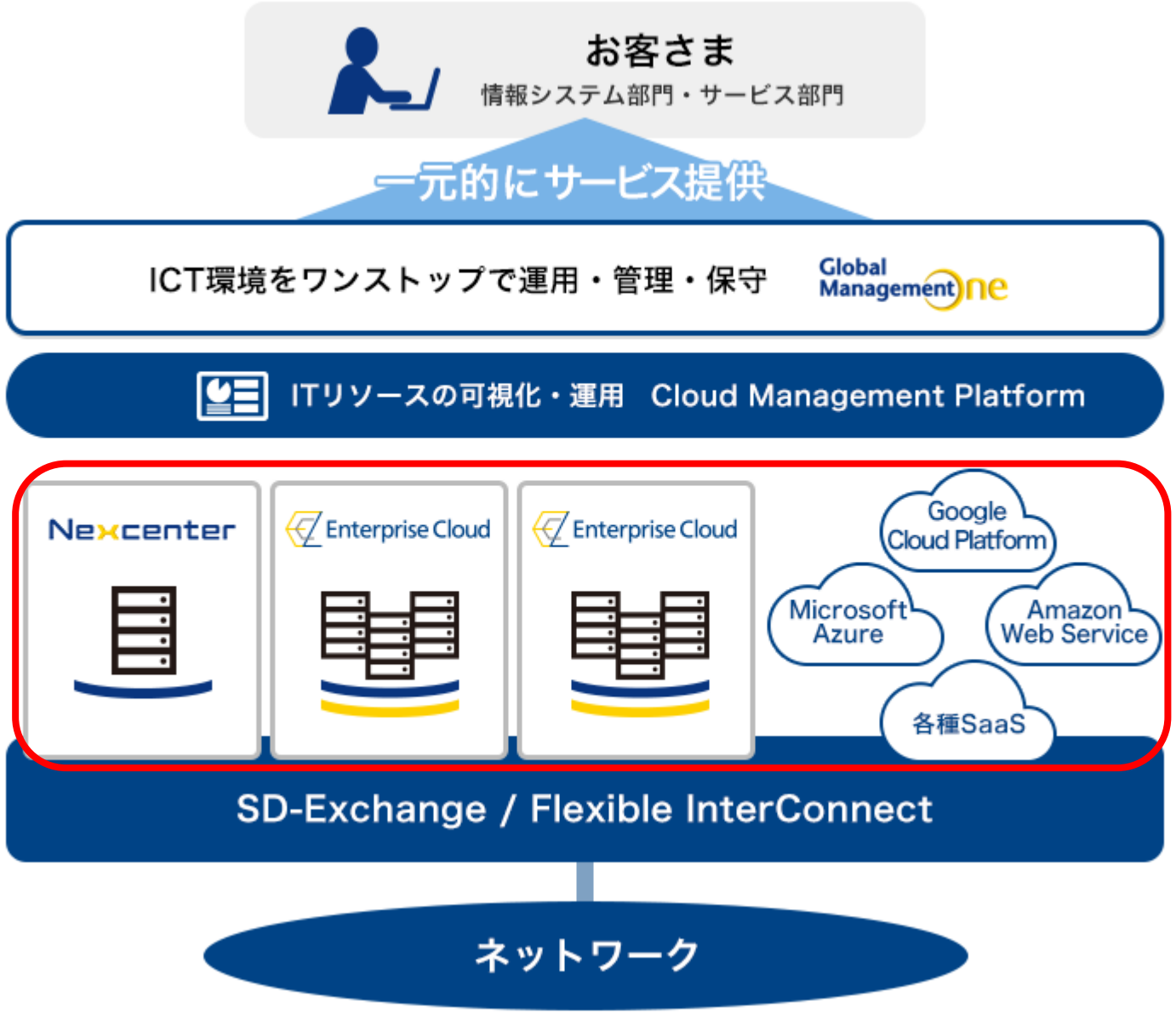


（出典）ZDNet 「グーグル、セキュリティチップ「Titan」の詳細を説明」

誰を信頼するか≒利用すべきサービス

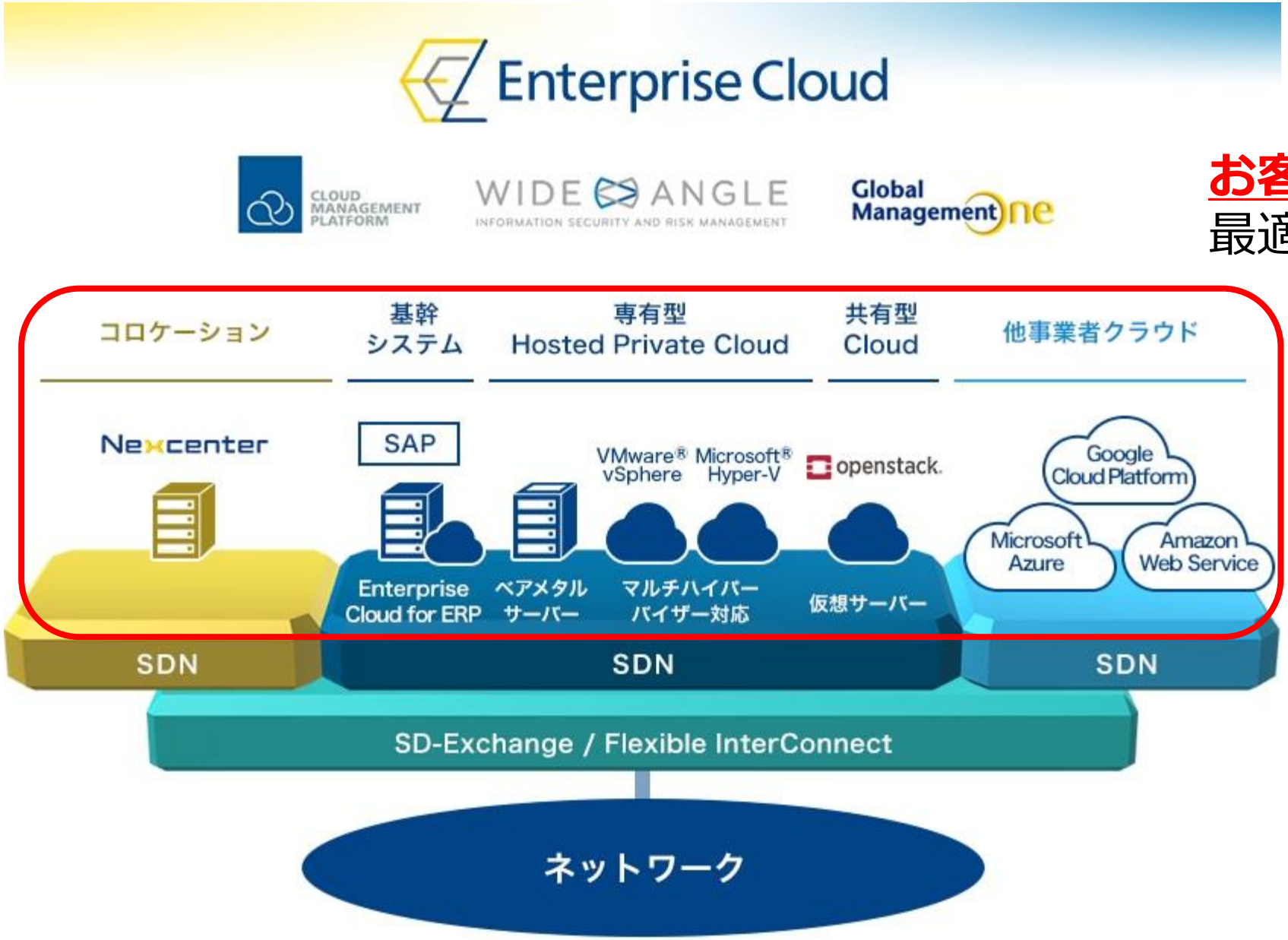
- CPUベンダを信頼する貴方
  → Confidential Computing
  あと、自社エンジニアへの投資と信頼を忘れないこと
- GAFAMを信頼する貴方
  → Google, Amazon, Microsoft が、
  それぞれに**自社製ハードウェア**を検討中
  あと、自社エンジニアへの投資と信頼を忘れないこと
- ITベンダを信頼する貴方
  → **マネージドサービス**という選択肢。 (次ページ以降で紹介)

NTTのマネージドサービス

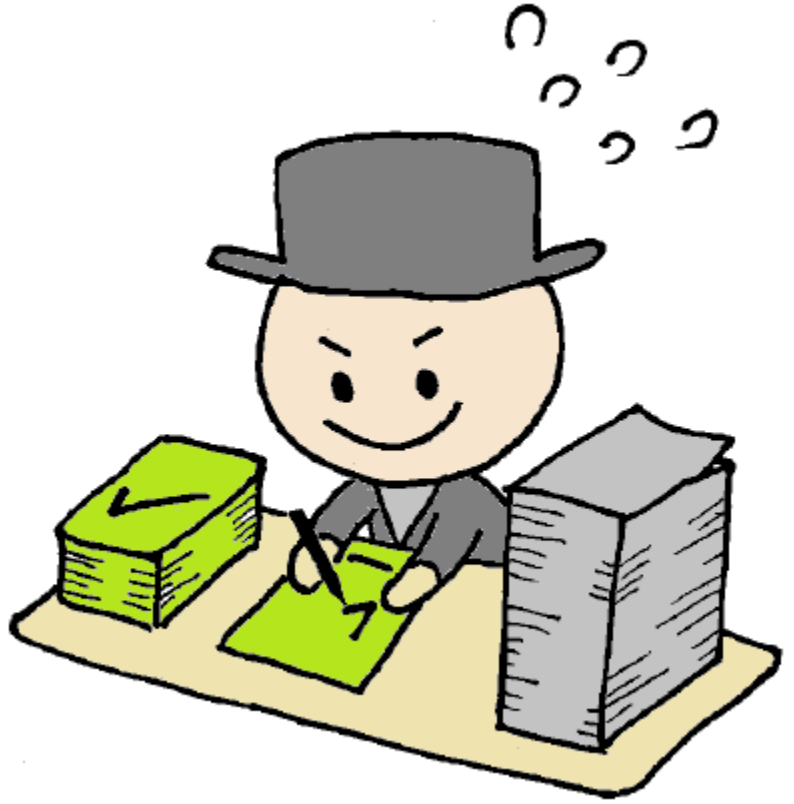


マルチクラウドの体制で
最適なICTサービスを提供

NTTのハイブリッドクラウド



お客様の事業内容に合わせて
最適なクラウドサービスを提供



あれ、本講演って、
NTTさん、サービスの宣伝ですか？？

⇒本題の Confidential Computing に戻りましょう。

Confidential Computingで新しいこと

つまり、Confidential Computing ってさ、
クラウド事業者のマーケティング施策ってこと？？

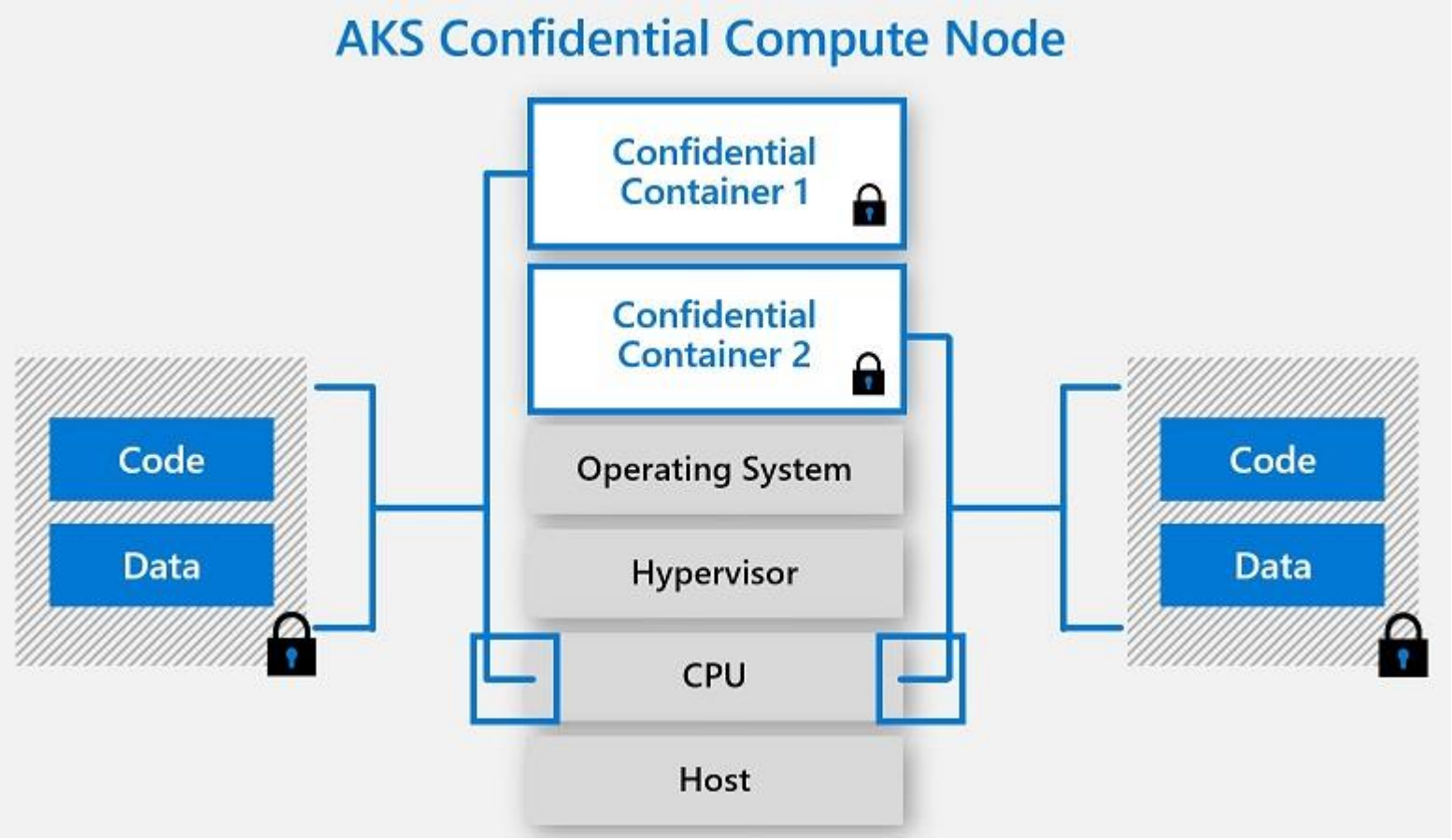
（鋭い質問）

⇒ 実はですね・・・
　ちょっと新しいサービスが作れます。

（次ページ以降で紹介）

(応用例1) Confidential VM,コンテナ

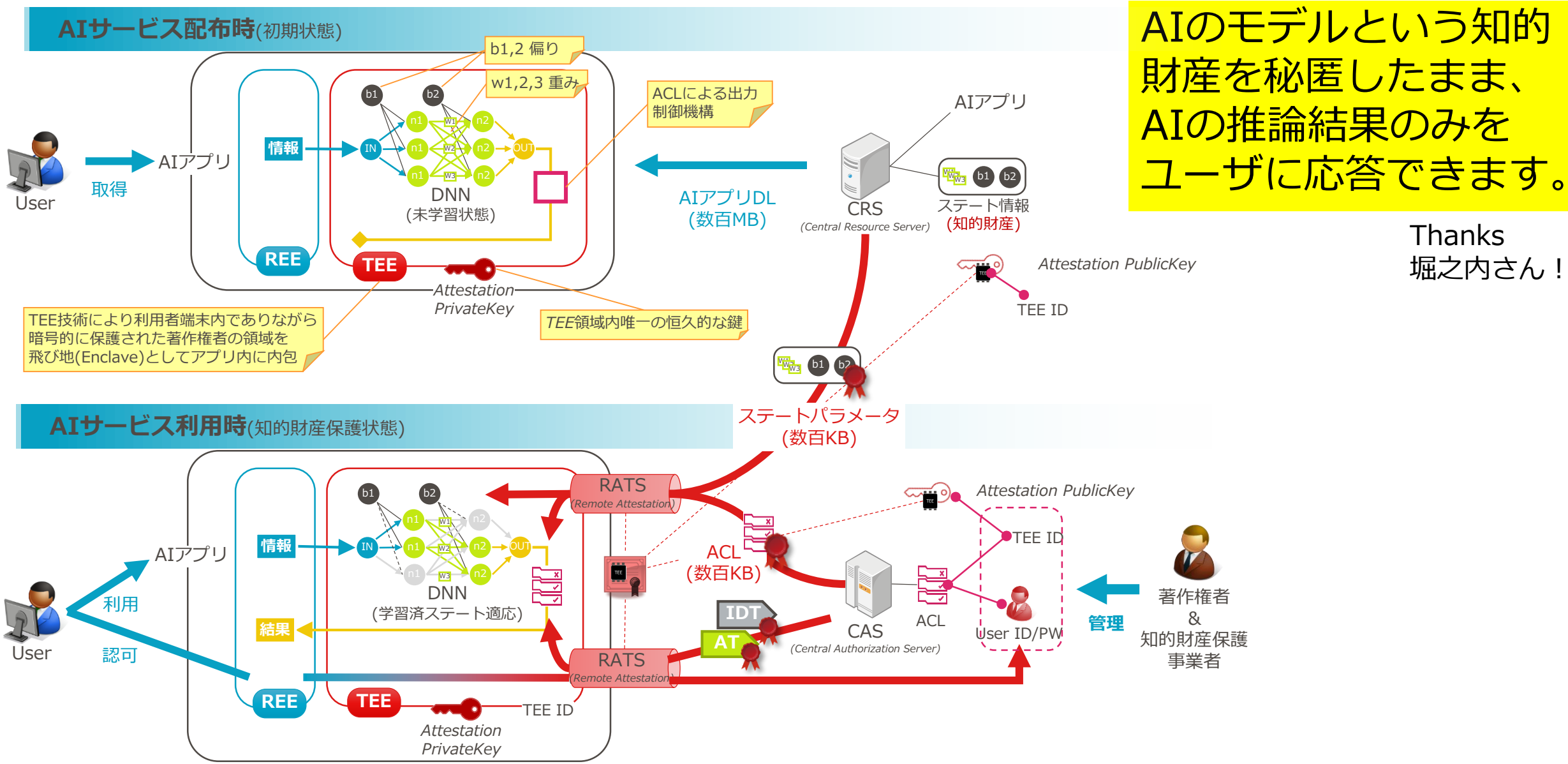
クラウド上の作成済みのVMやコンテナを、TEE/Enclave上に
そのまま移行して、クラウド事業者から秘匿することが出来ます。



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

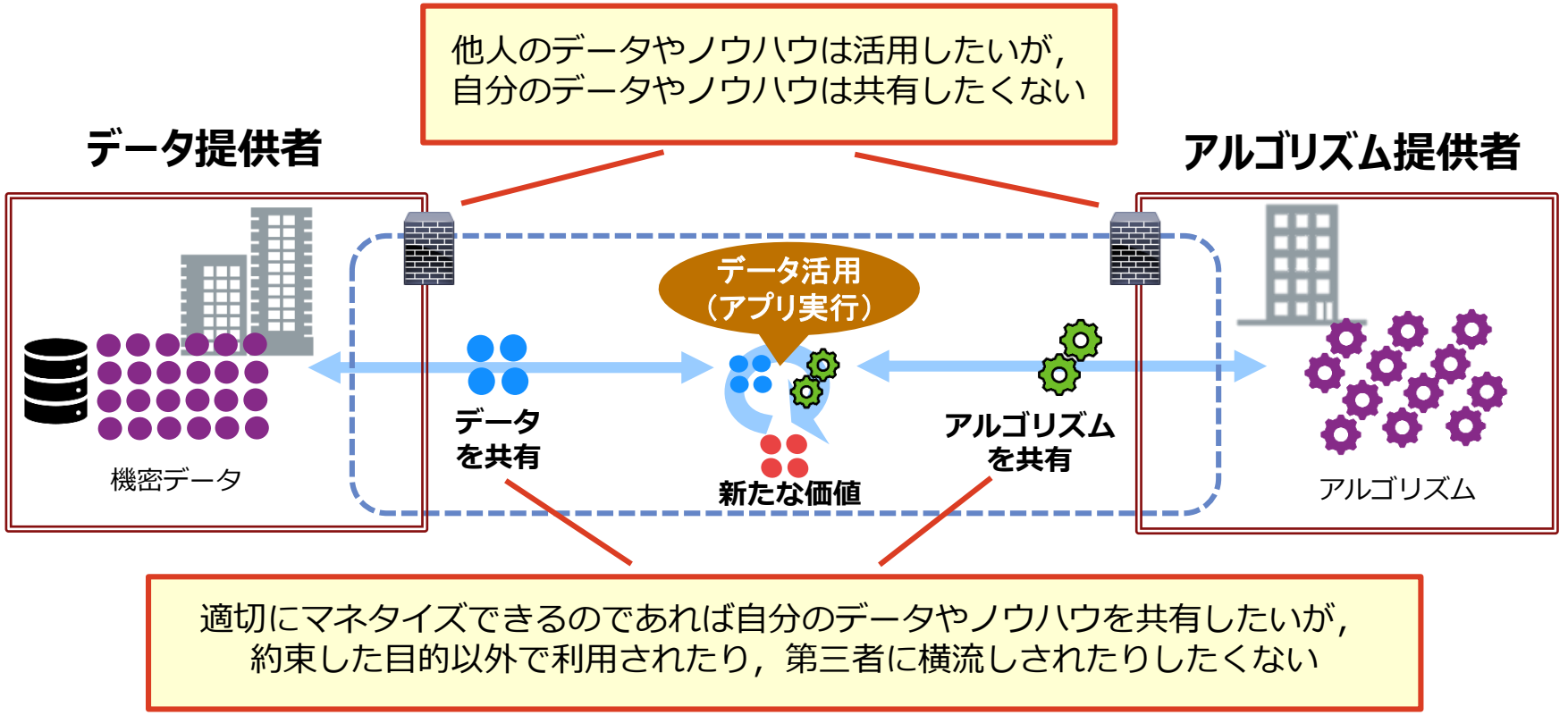


AIのモデルという知的財産を秘匿したまま、AIの推論結果のみをユーザに応答できます。

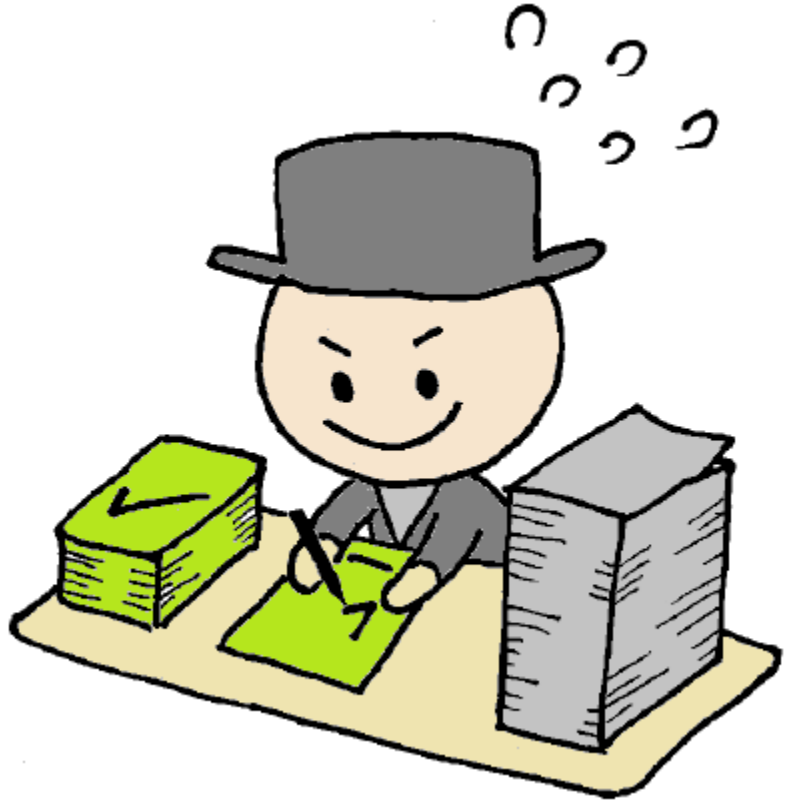
Thanks
堀之内さん！

(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



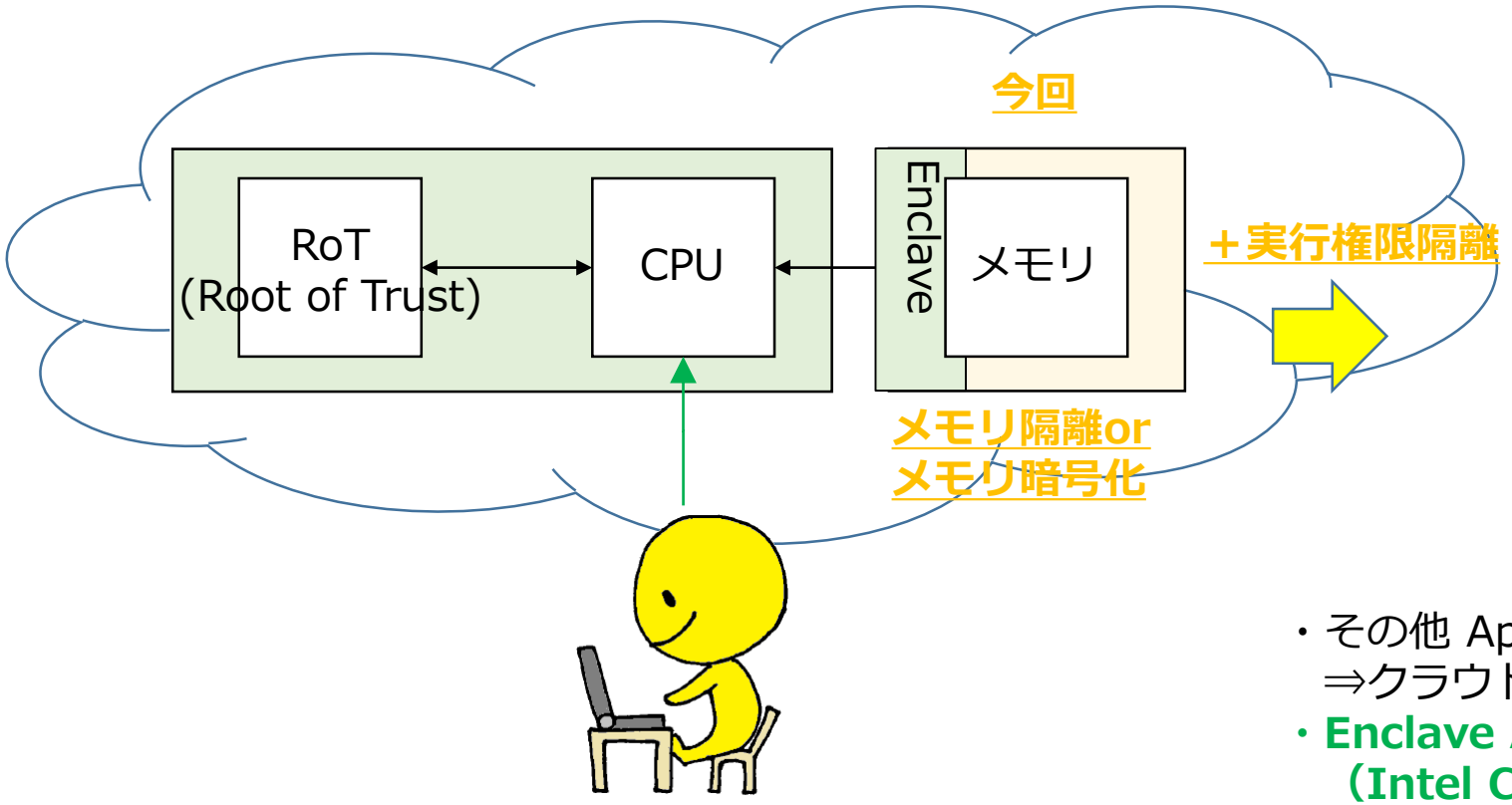
あれ、本講演って、
NTTさん、サービスの宣伝ですか？？

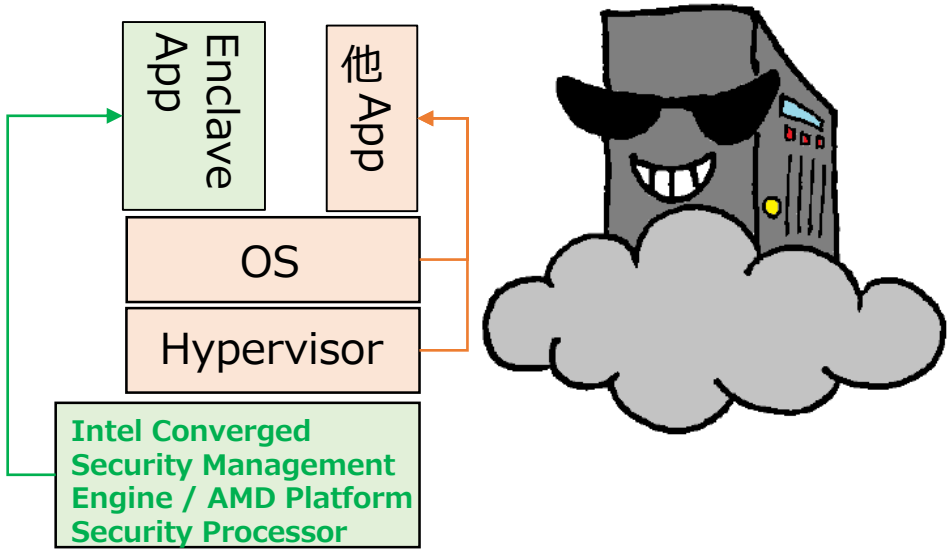
⇒最後に Confidential Computing の特徴を復習します。

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
↑**(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！



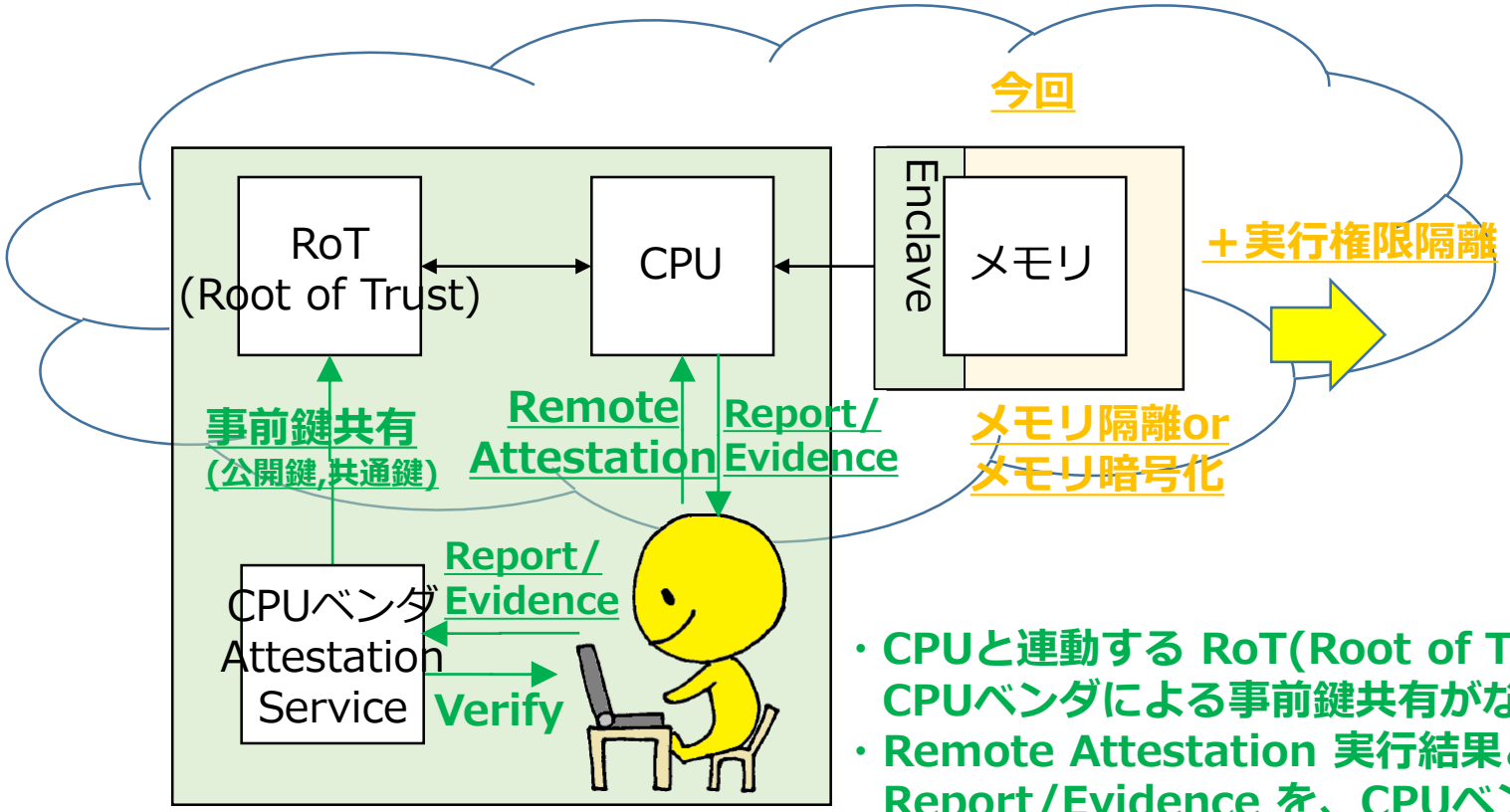


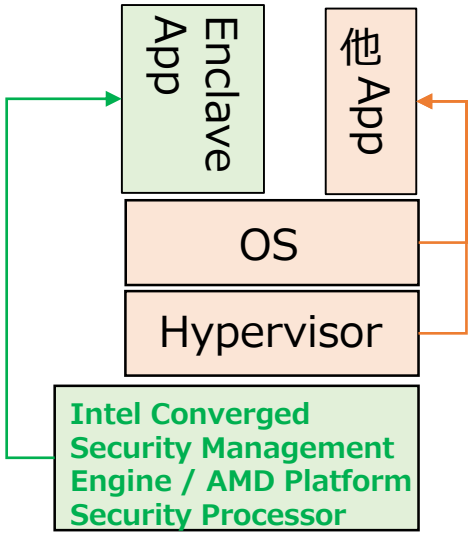
・その他 Appは OSやハイパーバイザから制御可能
⇒クラウド事業者が制御可能

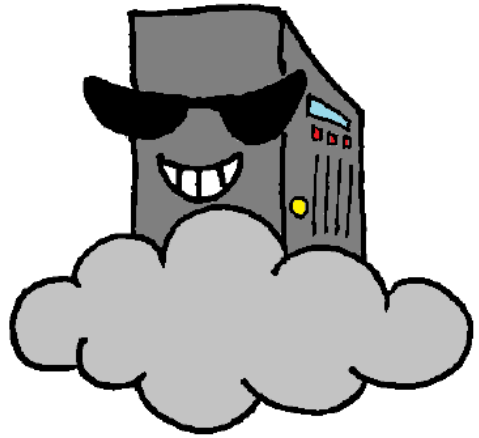
・**Enclave Appは CPUのみが制御可能**
（Intel CSME / AMD PSP のみが制御可能）
⇒クラウド事業者は制御不可
（OSやハイパーバイザから制御不可）

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！**



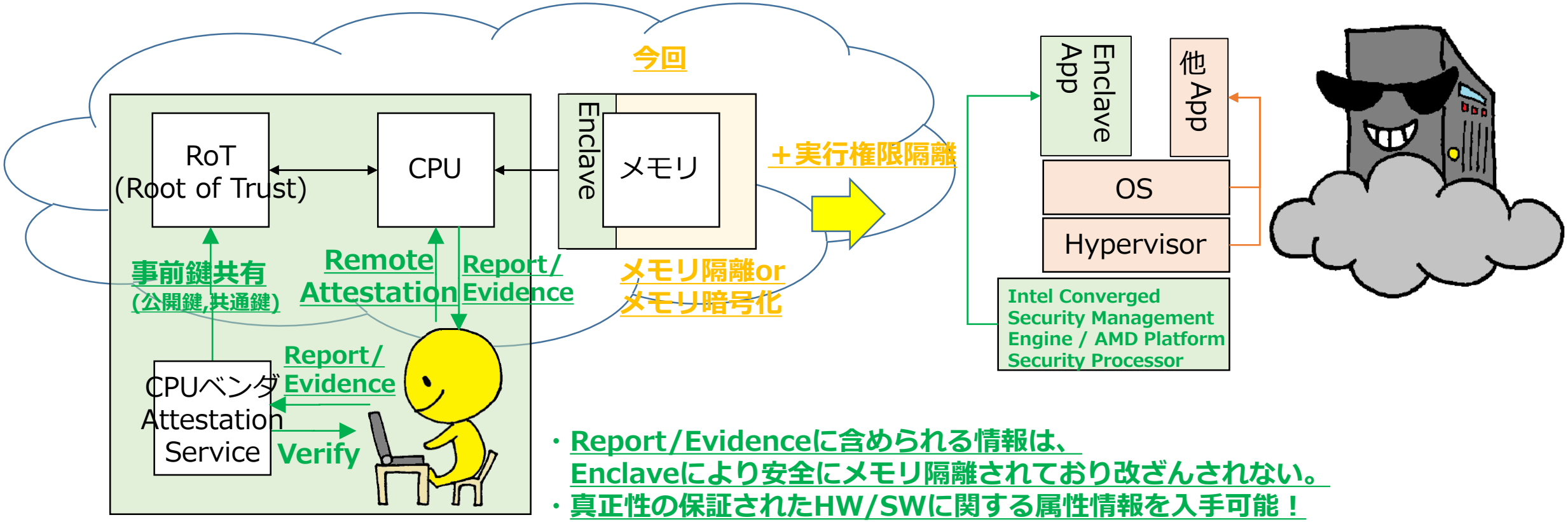




・CPUと連動する RoT(Root of Trust) に、
CPUベンダによる事前鍵共有がなされている。
・Remote Attestation 実行結果として得られる、
Report/Evidence を、CPUベンダの管理する
Attestation Service に問い合わせることで、
Report/Evidence の真正性を検証できる。

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！**

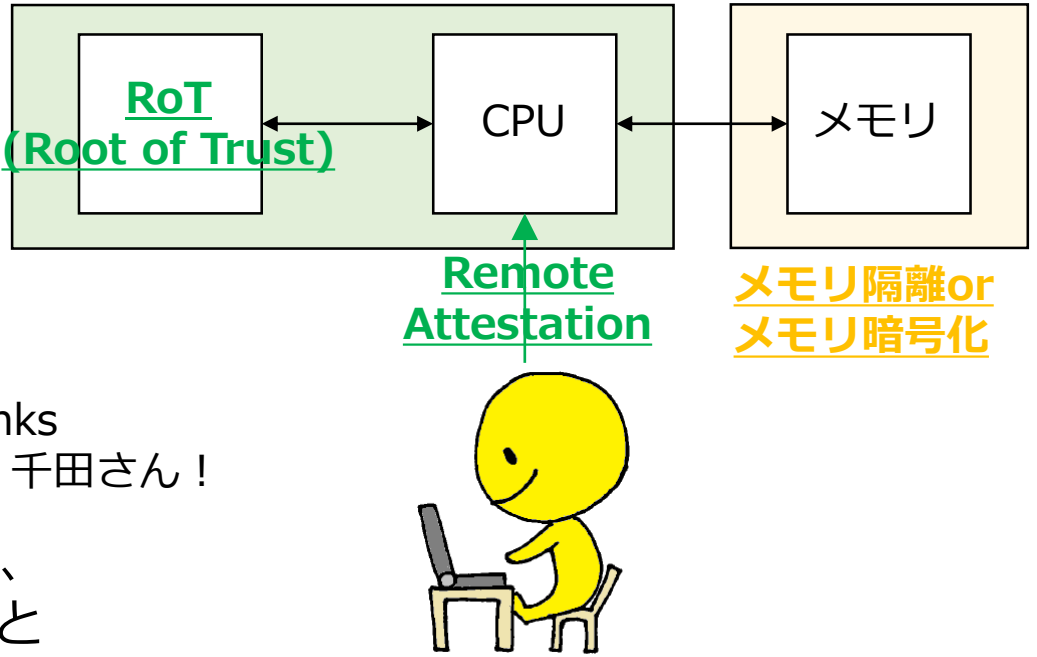


・Report/Evidenceに含められる情報は、
Enclaveにより安全にメモリ隔離されており改ざんされない。
・真正性の保証されたHW/SWに関する属性情報を入手可能！

TEE/Enclaveの定義

Take Away !!

（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**).

Confidential Computing の課題は？

・CPUサイドチャネル対策

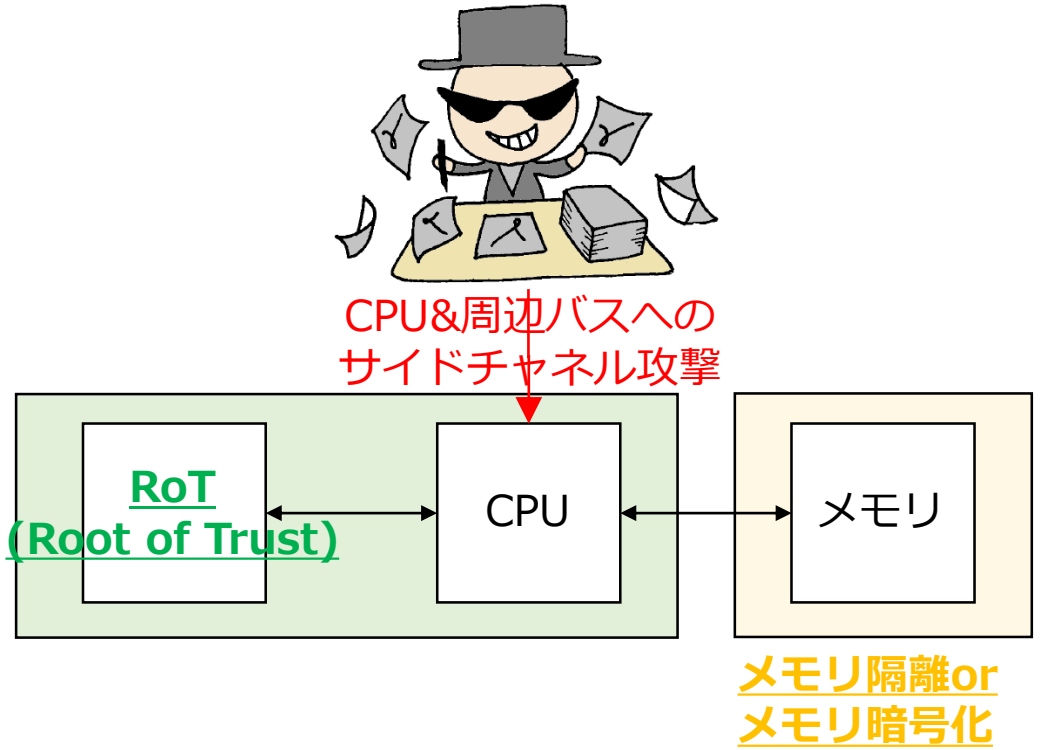
Thanks
NTT 順子さん！
　　弾くん！

⇒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！

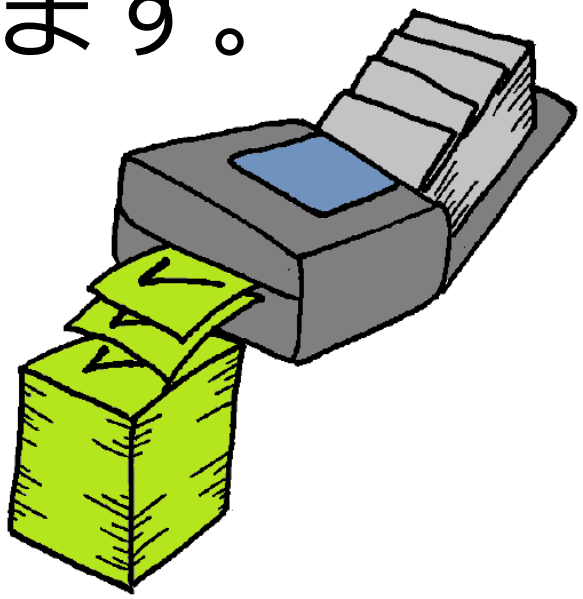
⇒国内では個人情報保護法、
海外ではGDPR, CCPA 等の一般的な法規制に加えて、
業界毎のレギュレーションについて、
Confidential Computing でクリア出来るのかは、
ベンダ各社に問い合わせる必要がある。



おわりに

NTTグループは、各社クラウドを含めて、
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



ここから応用編

■（応用編）

アカデミックの視点、CPUベンダの視点、

業界団体の視点、業界各社の視点、PKI/鍵管理の視点

→ここからマシンガンで行きます！！

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」

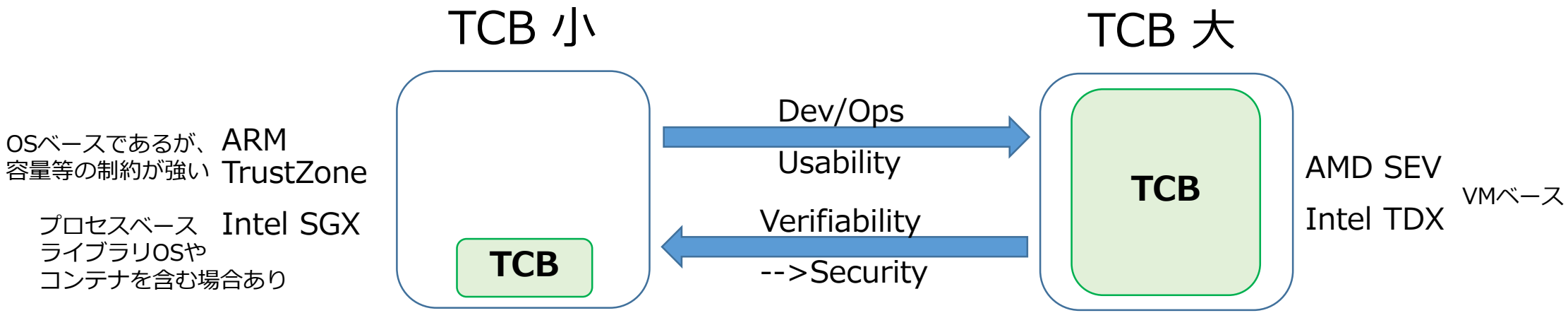
→サイバーセキュリティのトップ国際会議 IEEE S&P に遂に採録された

→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。

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。



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テーショナルな信頼とセキュリティを向上

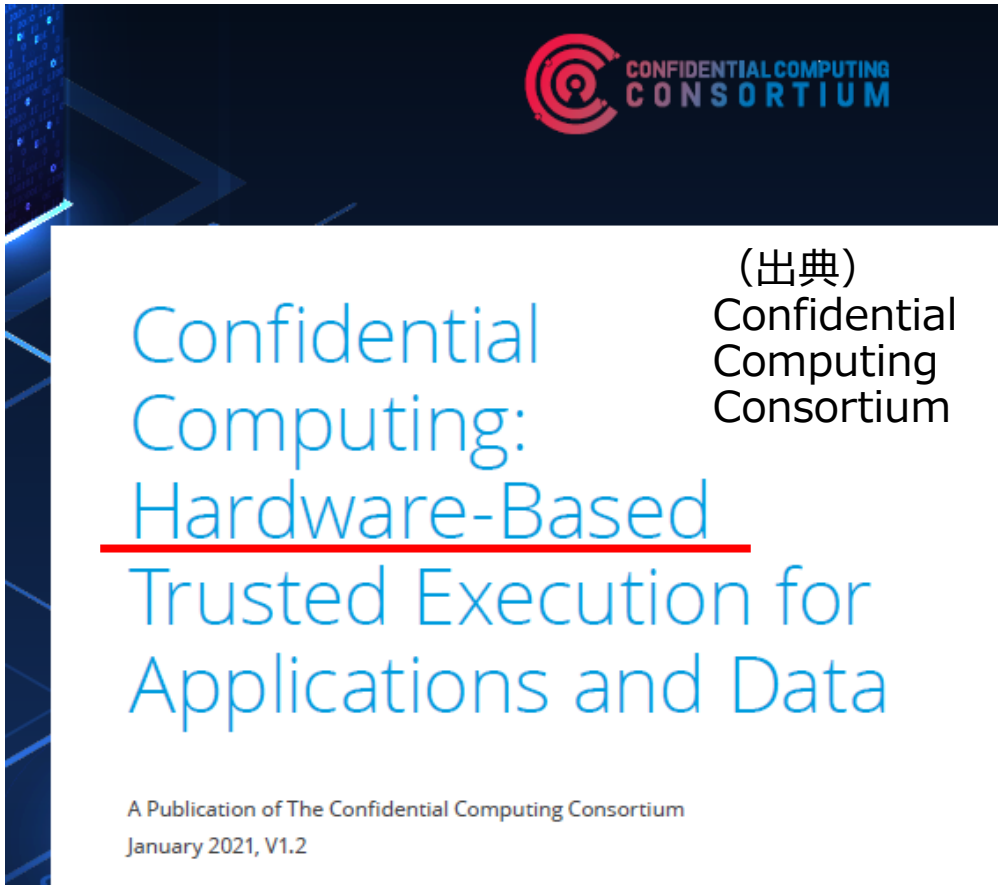
2019年10月17日 サンフランシスコ発 – Linux Foundation のプロジェクトで、コンフィデンシャル コンピューティングの定義と導入促進に取り組むコミュニティ Confidential Computing Consortium は、コンソーシアムの正式な設立と、設立時のプレミアメンバー Alibaba、Arm、Google Cloud、Huawei、Intel、Microsoft、Red Hat、およびゼネラルメンバー Baidu、ByteDance、decentriq、Fortanix、Kindite、Oasis Labs、Swisscom、Tencent、VMware を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

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

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

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

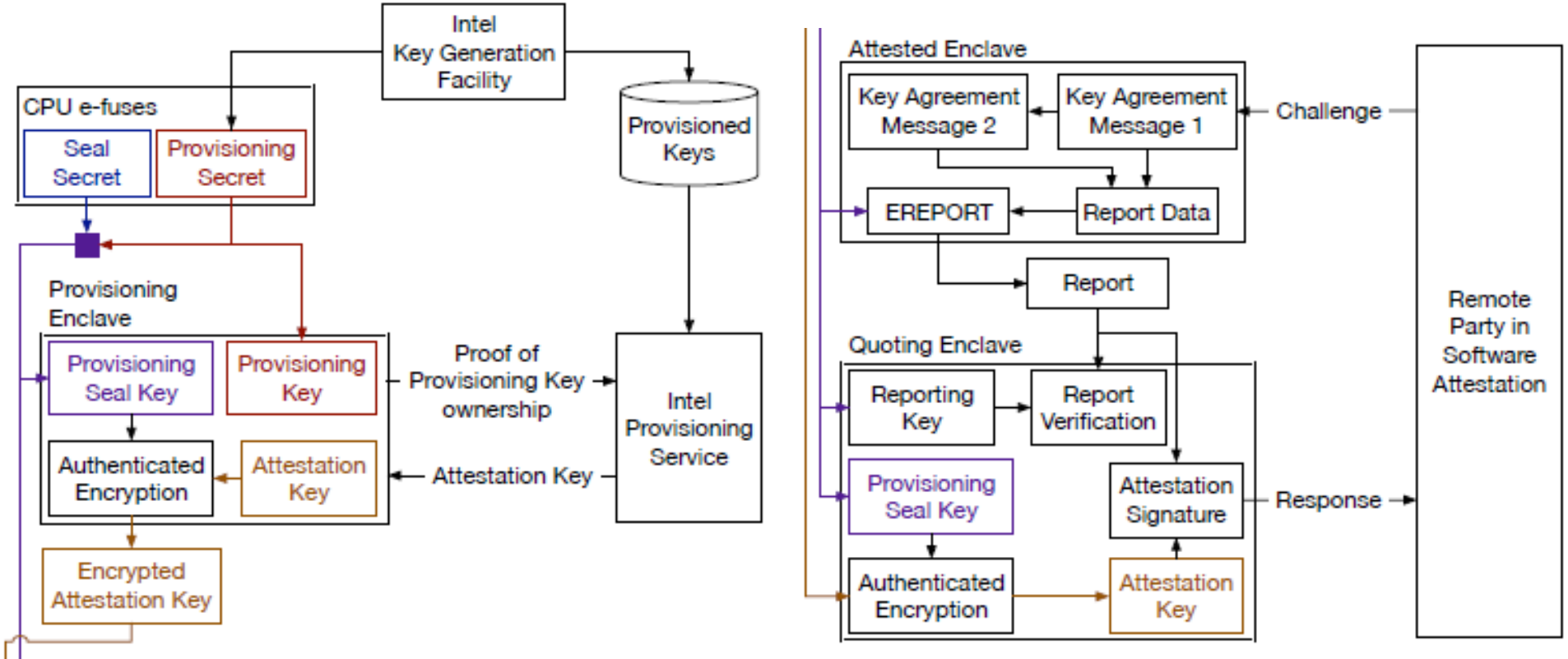
Enarx

Deployment

Veracruz

PKI/鍵管理の視点で見た 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

PKI/鍵管理の視点で見た 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。

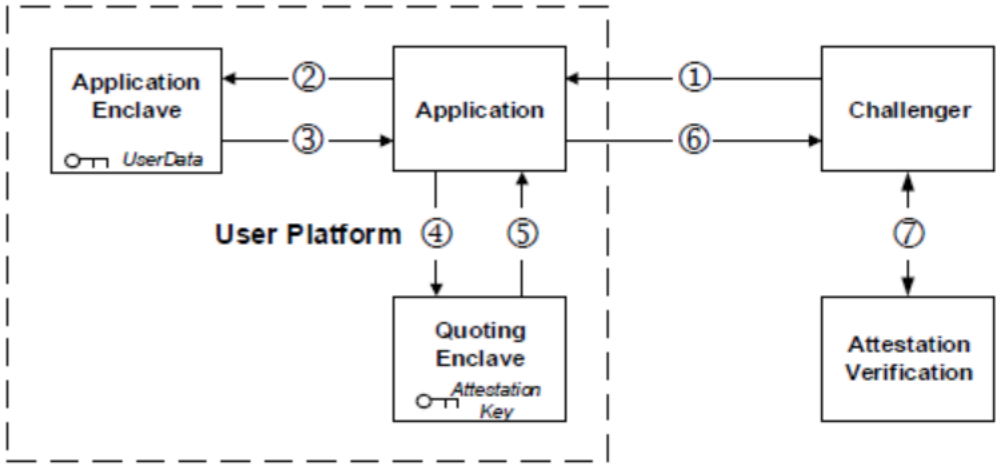


Figure 1: Attestation Flow

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

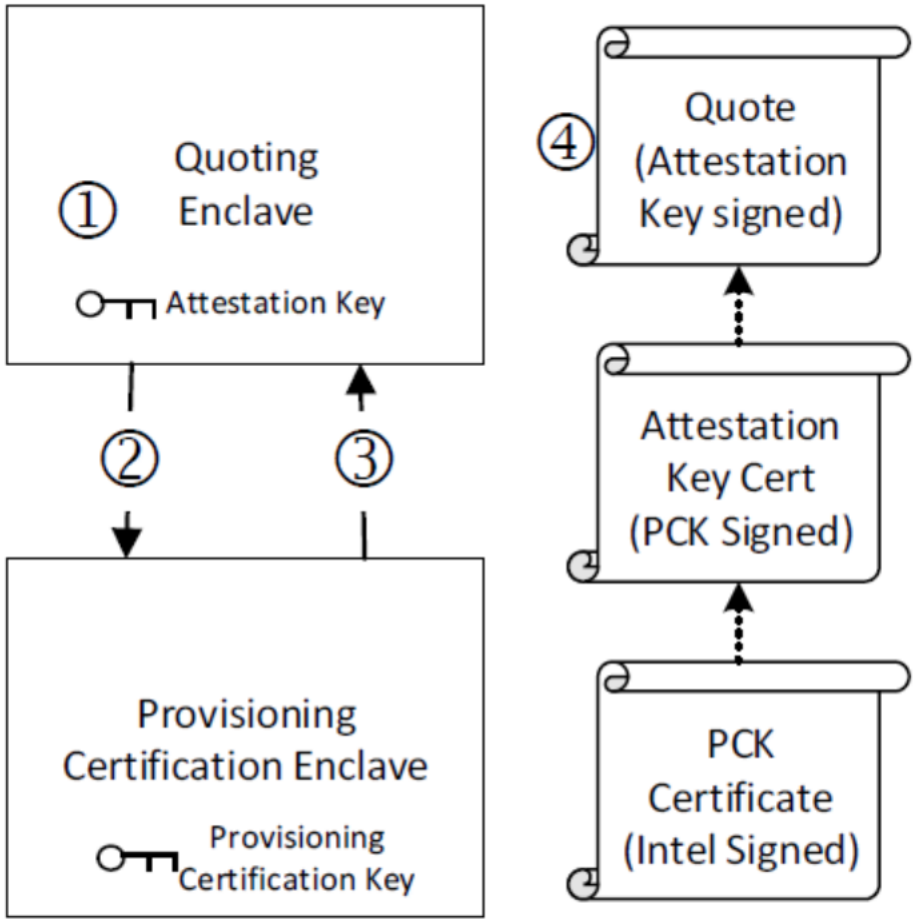


Figure 3: Quote Certificate Chain

PKI/鍵管理の視点で見た 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訳ではない様子

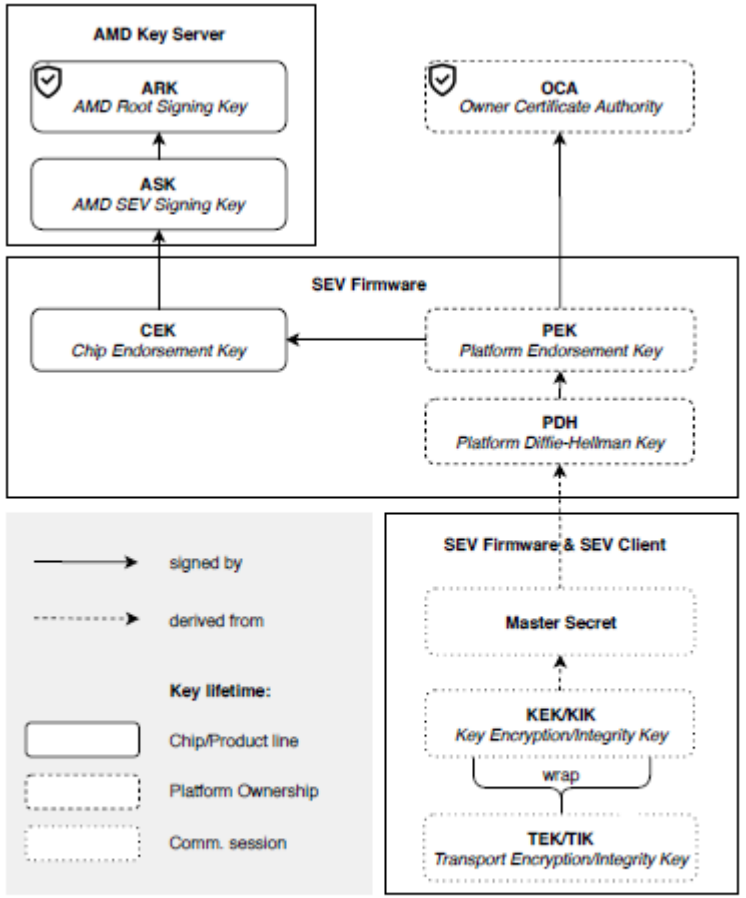


Figure 1: Cryptographic keys in SEV. A shield denotes the key as the root of trust for the corresponding certificate chain. Boxes show the scope of the respective keys.

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

■（パネルディスカッション導入用）Confidential Computing, ゼロトラストNW, トラスト

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

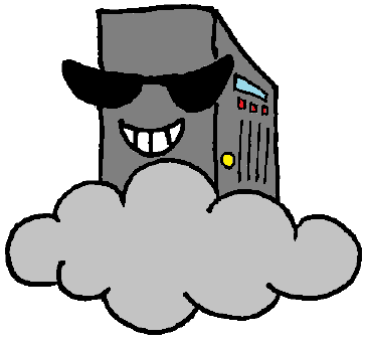
ここに機密なデータを凝縮する

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

ゼロトラストNW

（無条件に）信頼できる領域が最小化された世界

社内NW or Cloud

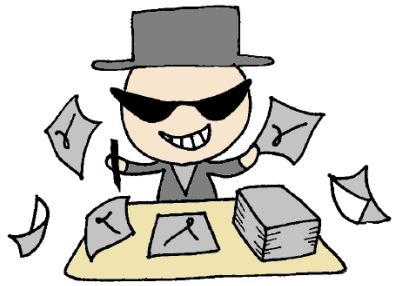
Authorization

Trust Engine

Authentication

Client

ここを基点に
信頼できる領域を広げる



（雑談用）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, BlackHat)

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)

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

Special Thanks

・ディレクションありがとうございました！
JNSA / セコム 松本 泰 様
・色々と情報交換ありがとうございました！
セコム 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