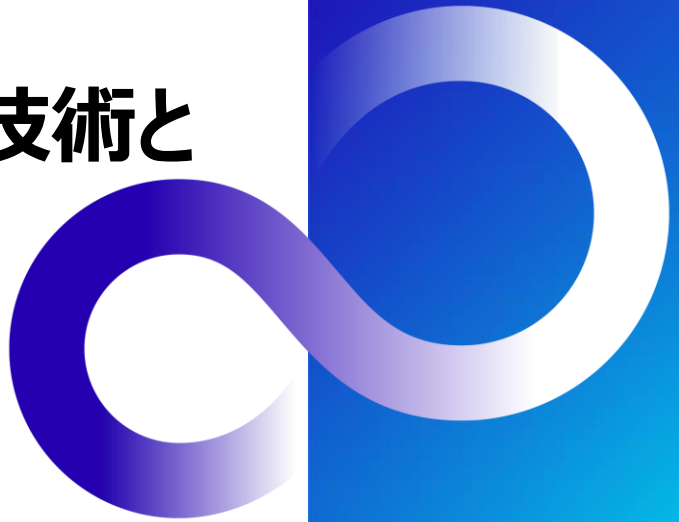
資料1-2

総務省様主催 | 情報通信審議会 情報通信技術分科会 IPネットワーク設備委員会
電気通信事業におけるパブリッククラウドシステム利用に関する検討作業班（第1回）ご紹介

FUJITSU

Confidential Computing 技術と富士通の取り組みご紹介



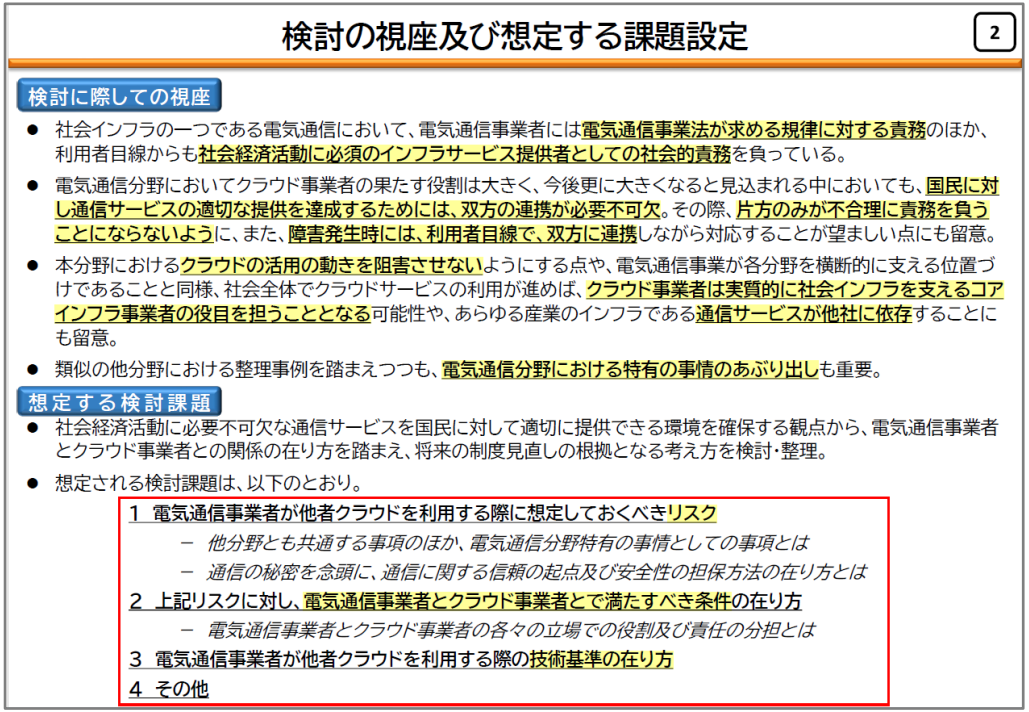
2025/7/28

富士通株式会社
先端技術開発本部

この成果は、NEDO(国立研究開発法人新エネルギー・産業技術総合開発機構)の助成事業の結果得られたものです。

はじめに

- **「通信に関する信頼の起点及び安全性の担保方法のあり方」に関し、弊社開発中のプロセッサも採用するConfidential Computing技術を紹介します。**



検討の視座及び想定する課題設定 2

検討に際しての視座

- 社会インフラの一つである電気通信において、電気通信事業者には電気通信事業法が求める規律に対する責務のほか、利用者目線からも社会経済活動に必須のインフラサービス提供者としての社会的責務を負っている。
- 電気通信分野においてクラウド事業者の果たす役割は大きく、今後更に大きくなると見込まれる中においても、国民に対し通信サービスの適切な提供を達成するためには、双方の連携が必要不可欠。その際、片方のみが不合理に責務を負うことにならないように、また、障害発生時には、利用者目線で、双方に連携しながら対応することが望ましい点にも留意。
- 本分野におけるクラウドの活用の動きを阻害させないようにする点や、電気通信事業が各分野を横断的に支える位置づけであることと同様、社会全体でクラウドサービスの利用が進めば、クラウド事業者は実質的に社会インフラを支えるコアインフラ事業者の役目を担うこととなる可能性や、あらゆる産業のインフラである通信サービスが他社に依存することにも留意。
- 類似の他分野における整理事例を踏まえつつも、電気通信分野における特有の事情のあぶり出しも重要。

想定する検討課題

- 社会経済活動に必要不可欠な通信サービスを国民に対して適切に提供できる環境を確保する観点から、電気通信事業者とクラウド事業者との関係の在り方を踏まえ、将来の制度見直しの根拠となる考え方を検討・整理。
- 想定される検討課題は、以下のとおり。

1 電気通信事業者が他者クラウドを利用する際に想定しておくべきリスク
  - *他分野とも共通する事項のほか、電気通信分野特有の事情としての事項とは*
  - *通信の秘密を念頭に、通信に関する信頼の起点及び安全性の担保方法の在り方とは*

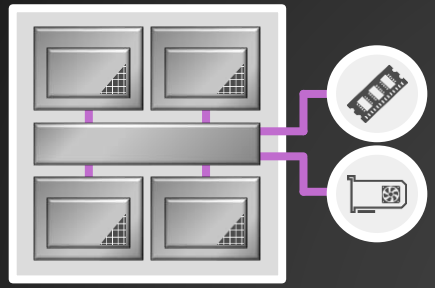
2 上記リスクに対し、電気通信事業者とクラウド事業者とで満たすべき条件の在り方
  - *電気通信事業者とクラウド事業者の各々の立場での役割及び責任の分担とは*

3 電気通信事業者が他者クラウドを利用する際の技術基準の在り方

4 その他

資料88-7
「電気通信事業におけるパブリッククラウドシステム利用について」
より抜粋

FUJITSU-MONAKA



- Armv9-A Architecture
- 3D chiplet
  - Core die 2nm
  - SRAM die/IO die 5nm
- Ultra low voltage for energy-efficiency
- DDR5 12 channels
- Air cooling Water cooling
- Arm SVE2 for AI and HPC
- 144 cores x 2 sockets (288 cores per node)
- Confidential Computing for security
- PCI Express 6.0 (CXL3.0)

FUJITSU

デジタル社会を実現する
次世代高性能・省電力・国産プロセッサ

高速なデータ処理基盤
AIワークロードを中心とした
コンピューティングの高速処理を
実現(競合CPU比2倍)

省電力とパフォーマンスの両立
高い電力効率により
CO2排出と電力コストを
大きく削減(競合CPU比2倍)

ゴール

信頼性とセキュリティ
メインフレームで培ってきた
安定稼働技術と
クラウド活用に向けた高いセキュリティを実現

使いやすさ
Armソフトウェアエコシステムを
利用可能
サービス・ソフトウェア・ハードウェアの
全体を通した協調設計

自社設計のマイクロアーキテクチャや
低電圧技術などの当社独自技術により実現

Confidential Computingご紹介

Confidential Computingの必要性

FUJITSU

背景

- 社会課題としての要請：クラウドが標準インフラに。セキュアな環境の提供が急務

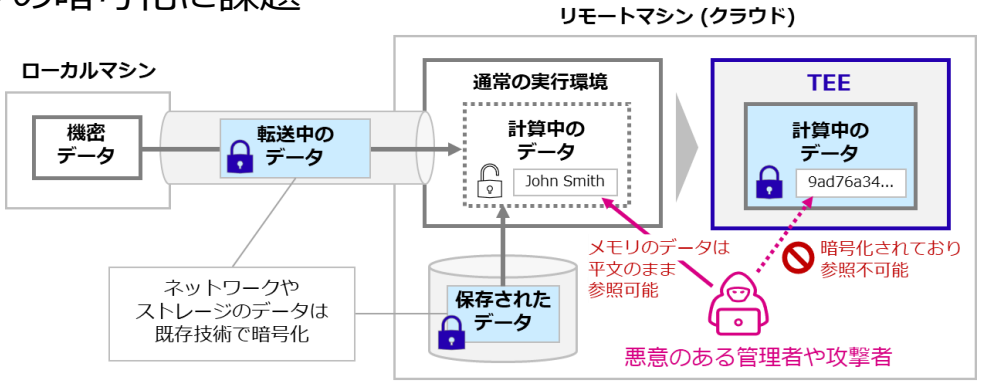
  IPA(独立行政法人 情報処理推進機構)による「重要情報を扱うシステムの要求策定ガイド」公開(2023年7月)
  → 自律性確保のための対策として「計算途上のデータ暗号化の確保」について言及

A-11	計算途上のデータ暗号化の確保	ハードウェアへの攻撃や管理者権限を有する運用者の不正などによって、メモリからデータの中身を読み取ろうとしても、読み取らせないようにする。	• 特に重要なデータを扱うアプリケーションについて、例えば、ハードウェア技術を用いて、計算機のメモリ上などに格納される全ての一時的な計算結果が暗号化・隔離されるような仕組みにより、運用者などからも秘匿される機能を提供すること。 • 当該隔離機能は鍵管理機能と連動し、計算結果の隔離機構外部との全てのやり取りが暗号化され、当該アプリケーションを利用している者以外に解読されないこと。 • 当該隔離機能の利用に際し、信用しなければならないトラストアンカー（CPUチップベンダー・鍵管理装置ベンダーなど）を確認すること。 ※計算途上のデータ暗号化のためには、特殊なハードウェアやソフトウェアに限定されるなどの現時点では課題があり、その対応状況はIPAサイトにて共有する。

出典) https://www.ipa.go.jp/digital/kaihatsu/t6hhco0000006s3t-att/system-youkyu-guide.pdf

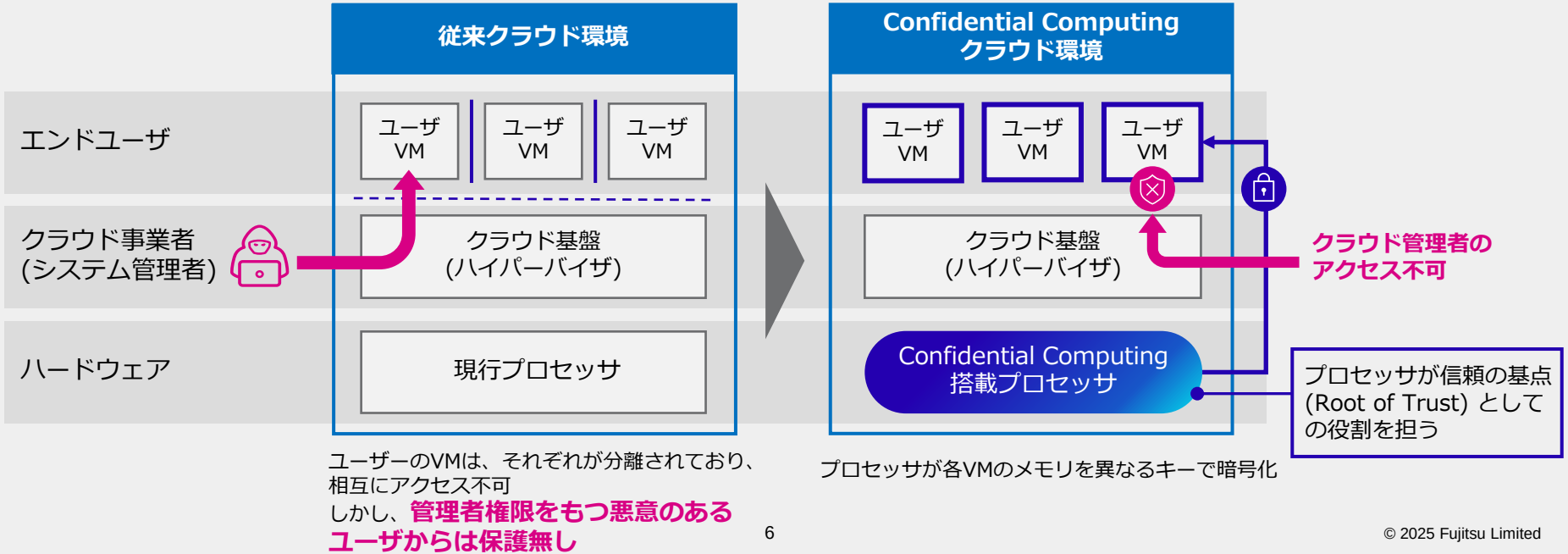
- 暗号化技術の状況：計算中のメモリ上のデータの暗号化に課題

暗号化対象	対応技術（例）
保存されたストレージデータ (Data at Rest)	SED(Self Encryption Drives) LUKS (Linux), BitLocker (Windows)
通信中のネットワークデータ (Data in Transit)	SSL/TLS IPsec
計算中のメモリ上データ (Data in Use)	Confidential Computing: プロセッサHWによる暗号化された実行環境 (TEE) TEE: Trusted Execution Environment



クラウドセキュリティの強化

- Confidential Computingによるクラウド上のユーザデータ保護
  - プロセッサがVM毎に異なるキーを生成し、VMのメモリ全体を暗号化
    - 暗号キーはプロセッサのハードウェアで管理されており、プロセッサ外からはアクセス不可
  - 管理者権限を持つユーザ(クラウド管理者や攻撃者など)からの不正アクセスを防止



Confidential Computing提供状況

- プロセッサのCC技術
  - CPUのCC技術は、アプリケーションの修正を必要としない仮想マシン(VM)単位で保護する方式が台頭
    ※本資料ではVM方式のCC技術を中心に説明しています。
  - NVIDIAがCCに対応したGPU(H100以降)を提供開始

ベンダー	名称	方式 (隔離単位)	アプリ修正
Intel	SGX	プロセス	必要
	TDX	VM	**不要**
AMD	SEV	VM	**不要**
Arm	CCA	VM	**不要**

- クラウドでのCC提供状況
  - ハイパースケーラーは、主要CPUのCC技術をベースに各社独自にCCサービスを提供開始

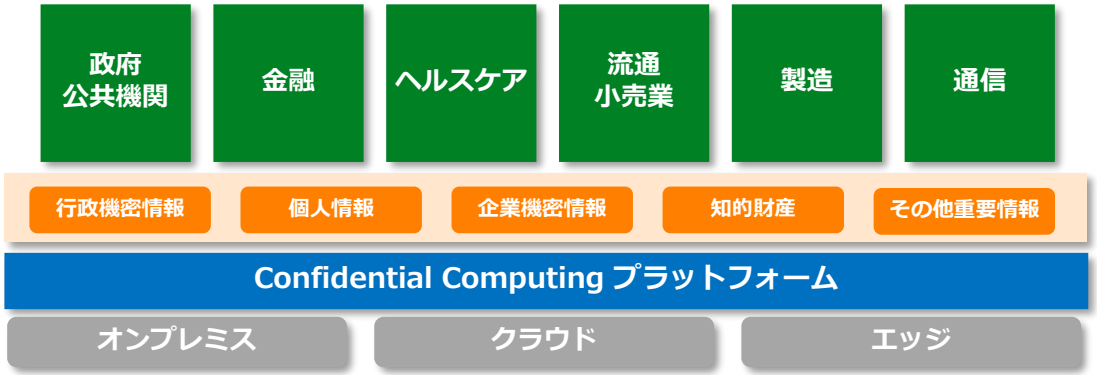
クラウド	提供状況 (2025年7月現在、当社調べ)
Amazon Web Services (AWS)	独自ハードのNitroによるCCサービスを提供。AMDベースのサービスも提供開始。
Microsoft Azure	AMD/Intelベースで包括的なCCサービスを提供。GPUにも対応し、ISVソリューションも提供。
Google Cloud Platform (GCP)	AMD/IntelベースでCCプラットフォームサービスを提供。VMサービスはGPUに対応。
Oracle Cloud Infrastructure (OCI)	AMDベースのCCサービスを提供開始。現状はVMサービスのみ。

  - 一方、オープンソース(OSS)や商用製品によるCC開発も進められており、今後、国内や中小規模のクラウドでのCCサービス展開が期待される

ユースケースと市場規模

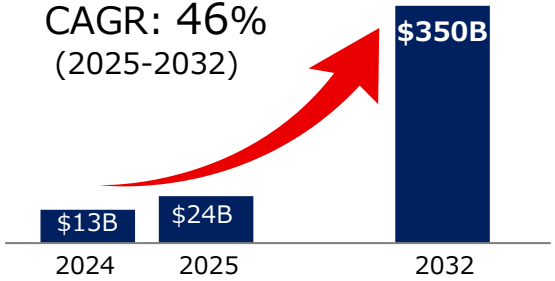
- Confidential Computingユースケースの例
  - クラウドセキュリティ
    - 機密情報や個人情報などを扱うワークロードを**オンプレからクラウドへ移行** (例：機密VM/コンテナサービス)
  - Confidential AI
    - データ漏洩リスクなしに、**高性能なAIサービスを利用** (例：LLMプロンプトやRAG機密データの保護)
  - データクリーンルーム (マルチパーティコラボレーション)
    - データ秘匿性を維持したまま、**複数の企業・組織間でデータを利活用** (例：不正取引検出、医療診断など)

- 主な対象領域



◆ CC市場規模

2032年に 3500億ドル (約52兆円)

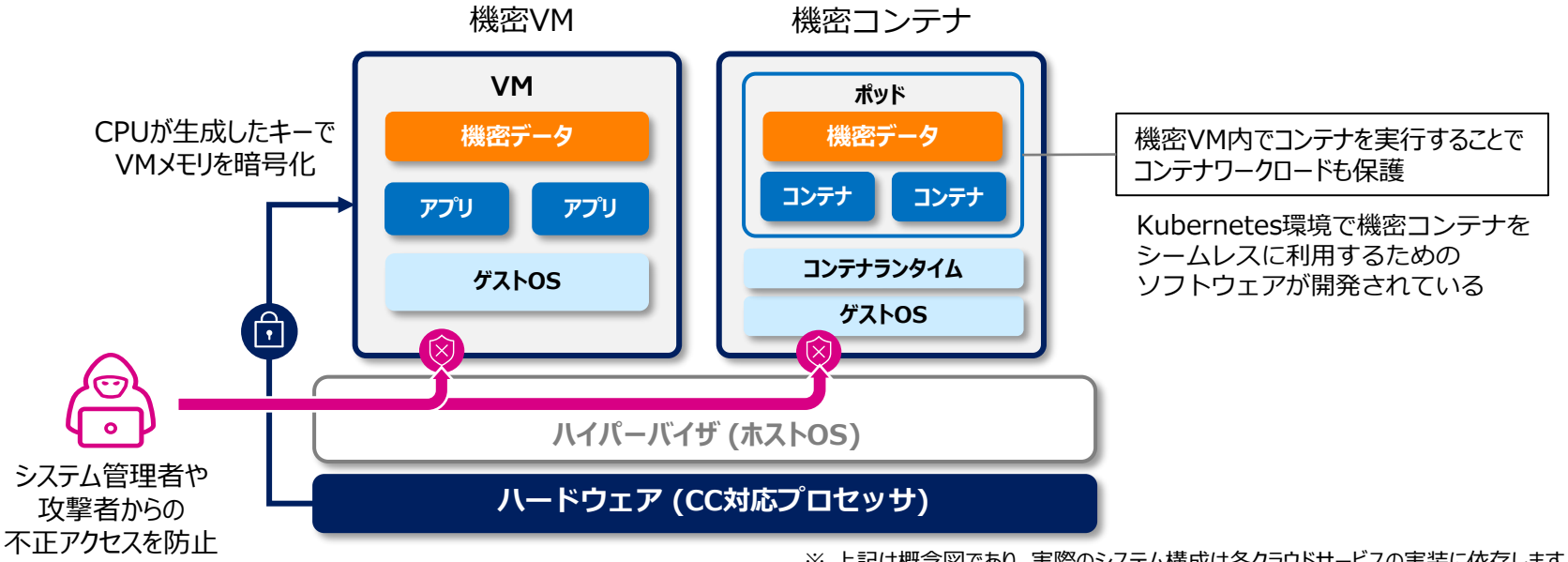


出展：Fortune Business Insights
https://www.fortunebusinessinsights.com/confidential-computing-market-107794

Confidential Computingプラットフォーム

FUJITSU

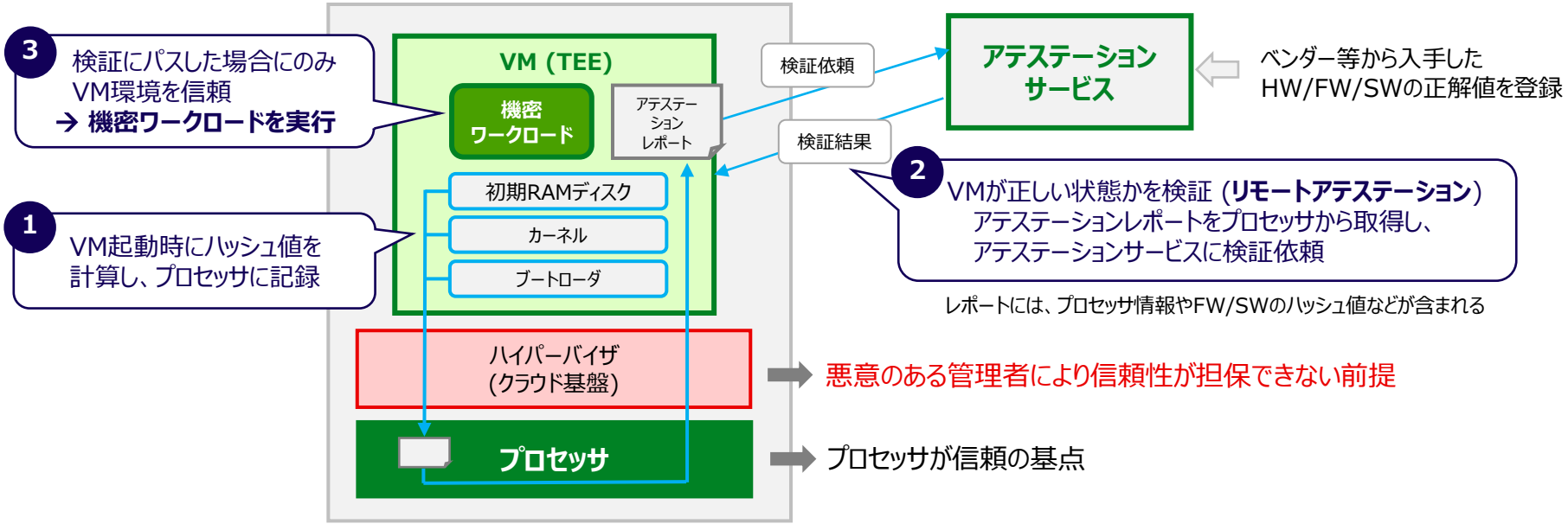
- VM形式とコンテナ形式によるCC実行プラットフォーム
  - **機密VM**　　VM単位でメモリを暗号化し、VM上の機密データやアプリを保護
  - **機密コンテナ**　クラウドネイティブなコンテナワークロードを機密VM内で実行



※ 上記は概念図であり、実際のシステム構成は各クラウドサービスの実装に依存します。

Confidential Computing構成機能

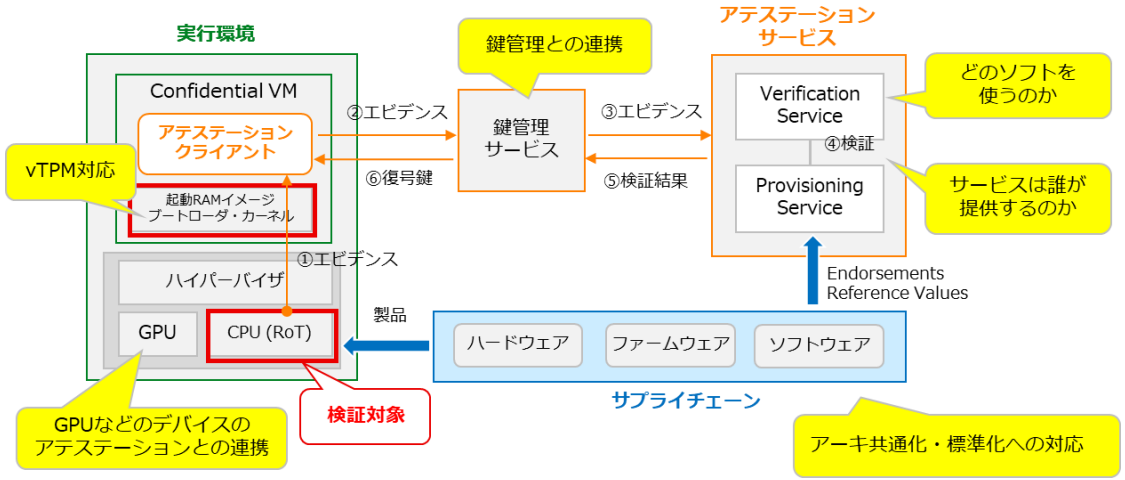
- TEE (Trusted Execution Environment)：ハードウェアによって隔離された実行環境
  - プロセッサによってTEE内のメモリは暗号化され、外部からのアクセスや改ざんを防止
- アテステーション (構成証明)：機密データを扱う処理を実行する前に、TEE環境の正当性を検証
  - TEEを構成するコンポーネント(HW/FW/SW)が正しいこと(改ざんされていない)ことを検証



リモートアテステーション

- リモートアテステーションの実装
  - アテステーションサービスはCPUベンダーやクラウドベンダーにより提供されることが多い
    例）Intel Tiber Trust Authority, Microsoft Azure Attestation, Google Cloud Attestation など
  - ユーザの要件に合わせて、ユーザ自身の環境でサービス運用することも可能
  - RFC-9334(RATSモデル)により標準化されており、オープンソース(OSS)の実装も進められている

■OSS活用におけるリモートアテステーションの基本フローと課題



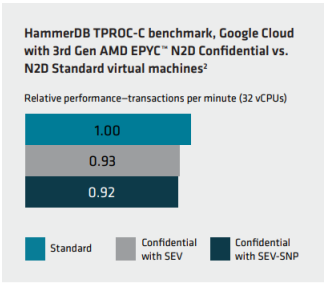
- リモートアテステーションは開発途上の技術
- 現在はCPUベンダーやクラウドベンダーが独自仕様によりアテステーションサービスを実装
- OSSコミュニティでは仕様標準化やアーキ共通化が議論されている

性能影響について

- CCによる性能劣化は**数%～10%程度**と小さい (ワークロードに依存)

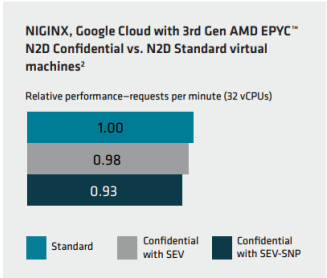
GCPにおけるAMD SEV-SNPインスタンスの性能

データベース



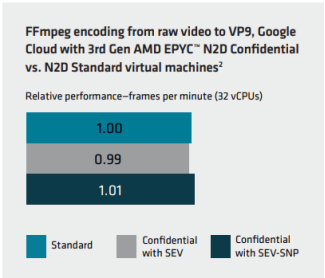
8%劣化

Webサーバ



7%劣化

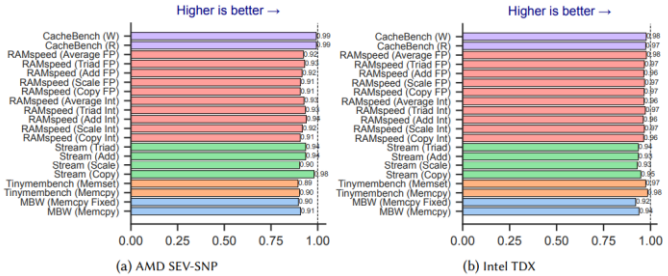
ビデオエンコード



劣化なし

出展：Confidential Computing Performance with AMD SEV-SNP Google Cloud N2D VM Instances
https://www.amd.com/content/dam/amd/en/documents/epyc-business-docs/performance-briefs/confidential-computing-performance-sev-snp-google-n2d-instances.pdf

メモリ性能ベンチマーク (Phoronix Memory Test Suite)



AMD SEV-SNP
1～10%劣化

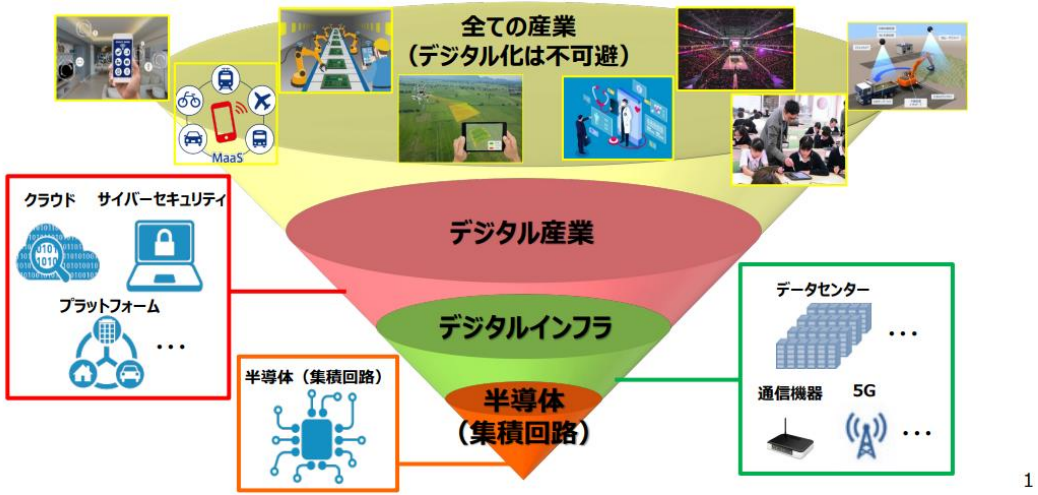
Intel TDX
2～8%劣化

出展：Confidential VMs Explained: An Empirical Analysis of AMD SEV-SNP and Intel TDX
https://syssec.dpss.inesc-id.pt/papers/misono_sigmetrics25.pdf

富士通の取り組み

富士通の取り組み：プロセッサ開発

- Confidential Computingはデジタル社会のサプライチェーンの源流である半導体設計の段階でセキュリティを担保する技術
  → **信頼できるベンダーにより設計された半導体であることが重要**



出典)https://www.meti.go.jp/press/2021/06/20210604008/20210603008-3.pdf

富士通は日本国内で設計したプロセッサにより重要データを保護

富士通の取り組み：Arm CCA開発

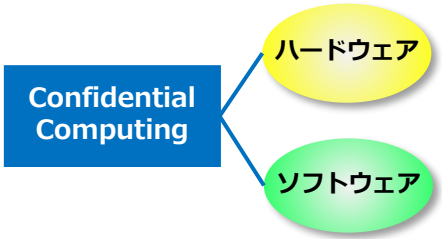
- Arm CPUによるConfidential Computing実現と普及促進

Arm CCA (Confidential Compute Architecture)
- Armv9-Aアーキテクチャで導入されたArm CPUにおけるConfidential Computing技術
- VMごとに異なるキーでメモリを暗号化 (AMD SEVやIntel TDXに相当する技術)

強固なデータセキュリティ基盤の実現に向けて、ハード・ソフト両面で、関係機関やパートナーとともに技術開発に取り組んでいます。

Confidential Computingの定義 (※)

Confidential Computing protects data in use by performing computation in a **hardware-based**, **attested** Trusted Execution Environment

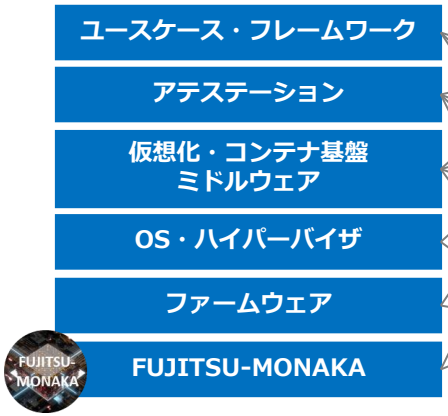


✓ 改ざんできないハードウェアが信頼の基点
✓ 国産プロセッサとしての高い信頼性

✓ ファームから上位MW層までオープンソース実装による高い利便性と透明性
✓ リモートアテステーションによる効率的なTEE検証技術

(※) https://confidentialcomputing.io/about/

CC構成コンポーネント



連携機関・パートナー

Confidential Computing社会実装に向けて

FUJITSU

- 課題：Confidential Computing技術のサービス適用拡大
- 取り組み：ユーザー運用視点での技術開発・適用シーンの開拓
  - 基盤技術の強化
  - ユースケースの拡充
  - 法規制・ガイドラインの整備
  - 国内のConfidential Computing認知度の向上

FUJITSU-MONAKA x Arm CCAによるデータセキュリティ基盤

ハードウェア	ソフトウェア	アテステーション	ユースケース
国産CPUによる 高い信頼性	**業界標準OSS**による 高い汎用性と 最新技術の活用	**パートナー連携**による 仕様標準化と 運用技術の確立	**フレームワーク拡充**に よるユースケースの 実装効率化

Thank you