日本総研
The Japan Research Institute, Limited

②詳細解説＜仕組み・理論＞編

安全なデータ活用を可能にする「TEE」
― Confidential AIの基盤技術の動向と検証 ―

株式会社日本総合研究所　先端技術ラボ

2026年8月14日

［お問い合わせ］
執筆者：先端技術ラボ　森 毅、藤後 英哲
本レポートに関するお問い合わせにつきましては、当社ホームページの お問い合わせフォーム よりご連絡ください。

日本総研
The Japan Research Institute, Limited

目次

本シリーズの読み方

- 本シリーズは①概説・市場動向・戦略編、②詳細解説<仕組み・理論>編、③実践・技術検証編の3部構成から成る。
- 読者の役割や関心領域に応じ、推奨する参照ルートを以下に示す。

種別	主な内容	主な読者
①概説・市場動向・戦略編	TEEの概説・市場動向／ユースケース・戦略的示唆	経営層・企画部門・非技術者
②詳細解説<仕組み・理論>編（本書）	TEEの仕組み・信頼モデル・脅威モデル・性能理論の技術リファレンス	リードエンジニア・ITアーキテクト
③実践・技術検証編	Azure実機での構築手順・機能検証・性能実測と運用課題	開発エンジニア・検証担当者

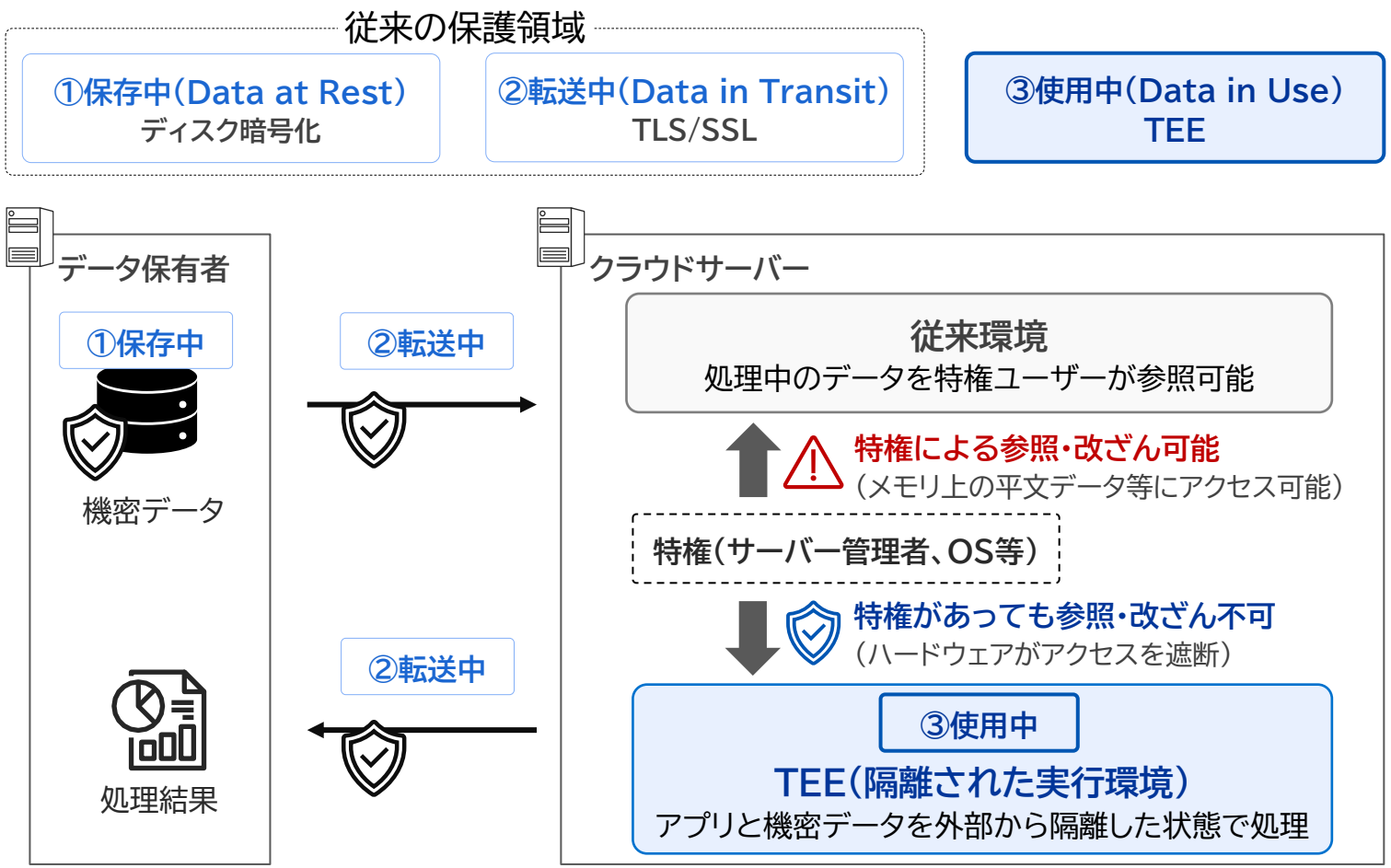
想定読者別の読み方

- **経営層・企画：**
  ①概説・市場動向・戦略編を通読（必要に応じて②詳細解説編の第8章<脅威モデルと攻撃手法>、③実践・技術検証編の第7章<まとめ>を参照）
- **リードエンジニア・ITアーキテクト：**
  ①概説・市場動向・戦略編の第4章<GPU TEE>～第6章<適用事例>→ ②詳細解説編を通読 → ③実践・技術検証編から必要な結果を参照
- **開発エンジニア・検証担当者：**
  ③実践・技術検証編をメインに、①の第5章<エコシステム>、②詳細解説編の第5章<アテステーション章>等を参照
- **リスク管理・監査担当者：**
  ①概説・市場動向・戦略編の第2章<背景>・第7章<技術展望と提言>の残存リスク→ ②詳細解説編の第8章<脅威モデルと攻撃手法>

※ 役職によらず、TEEの基礎知識の習得には「①概説・市場動向・戦略編」の通読を推奨

TEE（Trusted Execution Environment）とは

- TEEとはシステム管理者やOSであっても中身を覗き見ることのできない保護された実行環境のこと。
- 従来はシステム構造上アクセス可能であった特権ユーザーからも機密データを保護し、使用中データ（Data in Use）の保護とともにConfidential AI（機密データを保護したままAI処理を行う技術）を実現する基盤技術となる。



特権ユーザーからも隔離する価値

人や運用ルールに依存した使用中データの保護から、ハードウェアによる物理的なアクセス遮断へ転換することで、インフラ管理者からの**機密データのクラウド利活用**や**セキュアな企業間データ連携**が実現可能になる。

ユースケース例

- クラウド上で提供されている外部AIモデル・サービスを使用して顧客情報を処理する。
- 運用者やデータ提供者がデータを覗き見出来ない仕組みを構築し、技術的な安全性の担保によって企業間でデータを連携・分析処理し、新たな知見を得る。
- クラウド使用時の漏洩リスクを下げることにより審査を短縮し、データ活用を加速させる。

日本総研 The Japan Research Institute, Limited

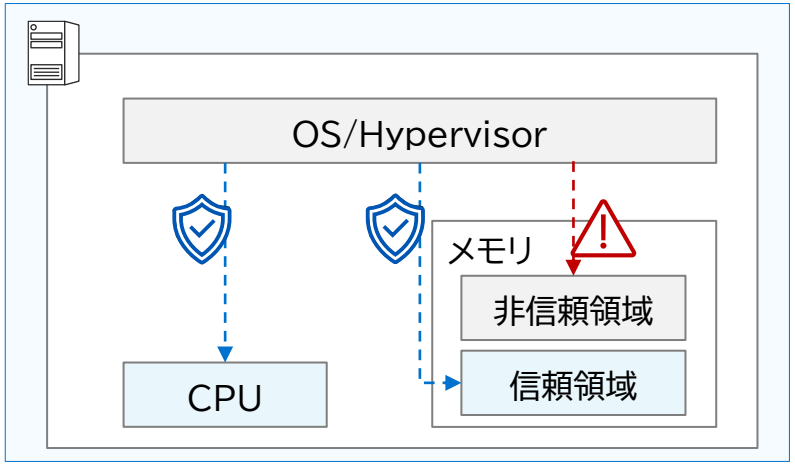
TEEの構成要素

- TEEは「隔離された領域」、「メモリ暗号化」、「アテステーション」の3つの要素からなる。
- 隔離が「アクセスさせない」、暗号化が「見られても読めない」、アテステーションが「正しい環境かを外部から検証できる」性質の実現を担い、全体としてTEEの信頼性を構成する。

隔離された領域（Hardware Isolation）

OS等から完全に切り離された、TEEの核となる**「保護された専用の処理領域（エンクレーブ等）」**を、CPUのハードウェア機能によって構築する。

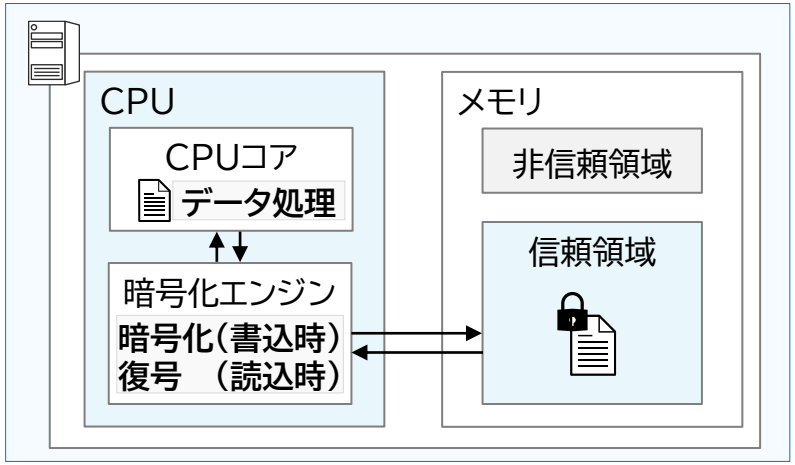
OSのウイルス感染や管理者権限の悪用からも領域内のデータを保護する。



メモリ暗号化（Memory Encryption）

保護された領域内で処理されているデータが、一時的に外側（メモリ等）へ書き出される際、ハードウェアレベルで自動的に暗号化を行う。

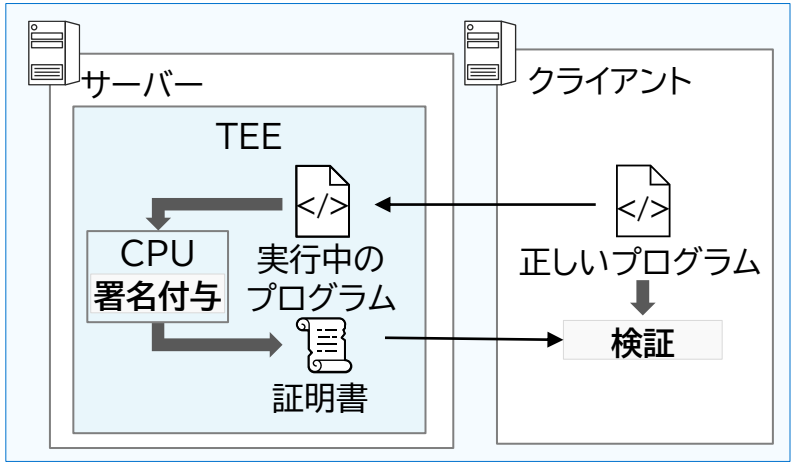
メモリに対する物理的な攻撃に対しても、暗号化により保護する。



アテステーション（Remote Attestation）

「意図したプログラムが安全な保護領域で実行されていること」を、ハードウェア発行の証明書を用いて外部から検証・証明する。

不正な環境や意図しないプログラムへの機密データの連携を防ぐ。

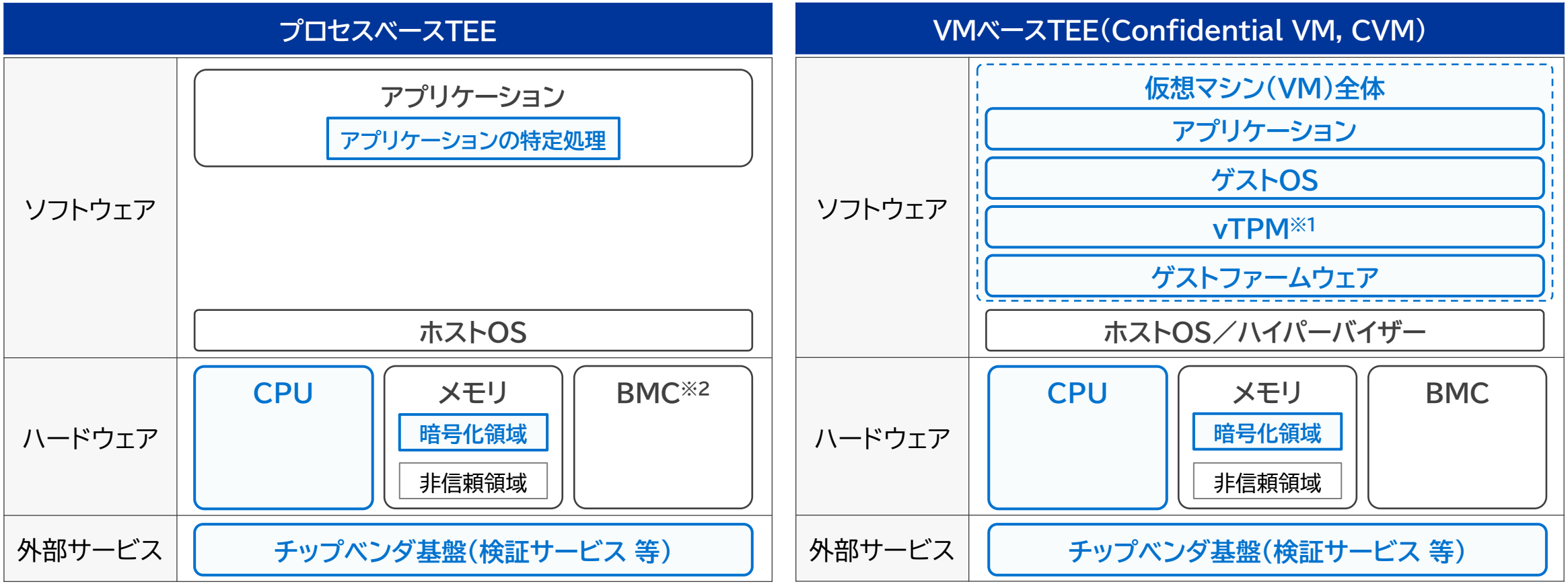


本資料における3つの要素は、Confidential Computing Consortium（CCC）の整理に基づく。古典SoKでは「Isolated Execution」、「Secure Storage（Sealing）」、「Remote Attestation」、「Trusted I/O」を中核機能とし、「Memory Encryption」はIsolationを物理攻撃に対して成立させる実装手段として扱っている。Arm TrustZoneはMemory Encryption機構を持たないTEEである。

日本総研 The Japan Research Institute, Limited

保護単位によるTEEの分類

- TEEを実現するために信頼する範囲(TCB:Trusted Computing Base)によって、プロセスベースTEEとVMベースTEEに大別される。
- TCBが広いほど移植性が高くなるが、守るべき箇所も増えるためセキュリティリスクが相対的に高くなる。



※1 TPM(暗号鍵の安全な保管や、システムの改ざん検知を行うセキュリティチップ)をソフトウェアで仮想化したもの。ロード時にCPUによって計測され、保護領域内で安全に動作する。
※2 BMC(Baseboard Management Controller):クラウド事業者がサーバーを遠隔管理するための特権を有したチップ。CPUの動作も観測できるがTEEでは信頼領域外。

（参考）ルートオブトラストとは

- ルートオブトラスト（Root of Trust：RoT）＝信頼の連鎖の出発点となる「それ以上さかのぼって検証できない」構成要素のこと。
- TEEのRoTは製造時にチップへ焼き込まれた鍵と改変不能なブートROMであり、全ての信頼がここから連鎖する。

RoTを起点とする信頼の連鎖

RoTの性質

- **それ自体は検証できない**
  ハードの耐タンパ技術で守られている信頼の起点（＝Root of Trust）
- **侵害されると連鎖全体が崩壊する**
  RoTの鍵が漏えいすれば、その上の計測・署名・アテステーションの全てが信頼を失う
- TEEのRoTはCPU内の鍵
- GPUではGSP＋OTP焼込み公開鍵がGPU側のRoTとなる。CPUと独立のRoTを持つことがComposite TEE構成の前提

ルートオブトラストの例

	パスポート	PKI（サーバ証明書）	TEE（vTPM）
RoT（信頼の起点）	政府（発行元）	ルートCA	CPU内のフューズ鍵（チップ固有鍵）＋ベンダー（Intel/AMD）のルート証明書
RoTによる証明書の発行	パスポートを政府が一度発行	サーバ証明書をCAが一度発行	ハードウェアレポート（RoT由来の鍵で署名）がvTPMの鍵を一度endorse（保証）
毎回の証明	本人が写真と一致することを見せる	サーバが秘密鍵の所持を毎回証明	vTPMが毎回AK（Attestation Key）でQuoteに署名
検証者の確認	入国審査官が「政府の印」を確認	クライアントがCA署名を検証	検証者がvTPM署名とハードレポートへの束縛を確認

検証者は毎回発行元（RoT）に問い合わせず、発行元の署名を信頼の根として、その場で検証可能

Intel SGX｜エンクレーブとEPC

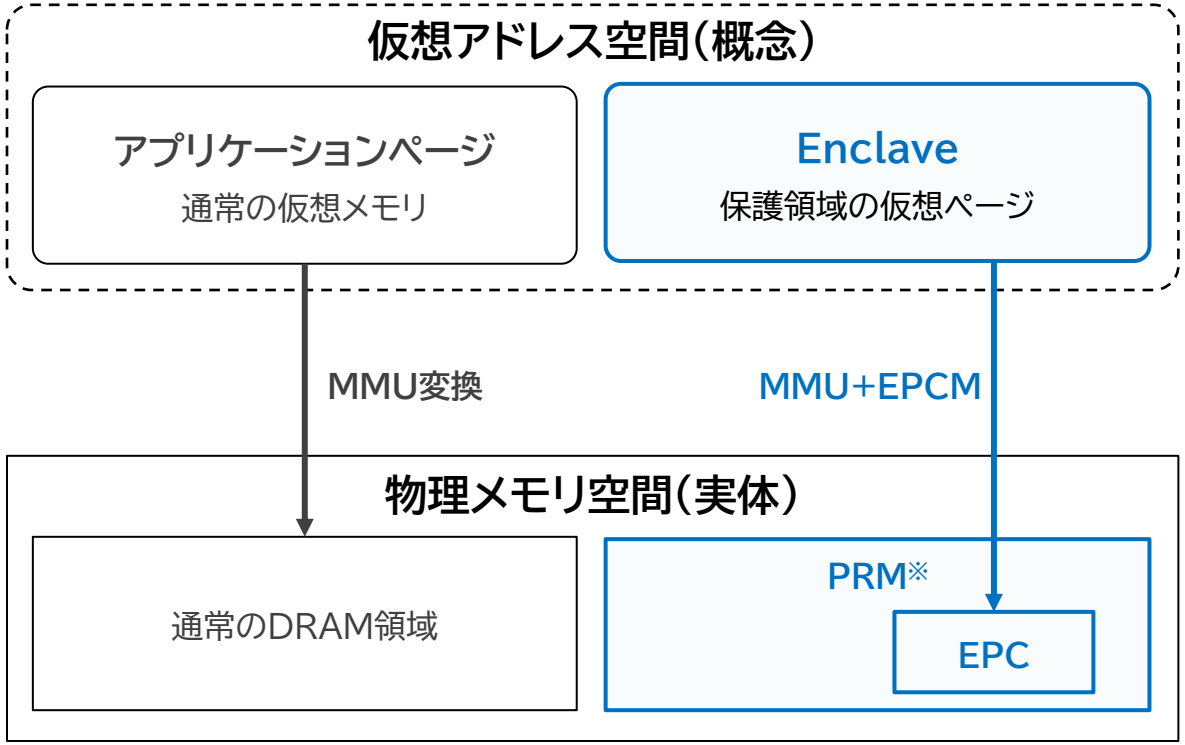
- SGXはプロセスベースTEEの代表的な実装手法。
- CPUがアクセスを制御するメモリ領域(エンクレーブ)をプロセス内部に配置することで、OSやハイパーバイザをTCBに含めることなく保護する。

エンクレーブ

- 機密性の高いコードやデータを実行するための隔離環境。
- OSやハイパーバイザー(管理者権限)すら信用せずに、悪意ある特権アクセスからも保護する。
- 2015年の第6世代Coreプロセッサ(Skylake)以降に採用されているIntel SGX(Software Guard Extensions)というTEE技術において、その中核的な概念。

EPC(Enclave Page Cache)

- エンクレーブを配置するために、物理メモリ上に確保された専用領域。
- CPUがハードウェアレベルで隔離・暗号化しており、この領域内のデータが外に出る場合は自動的に暗号化される。
- 容量に上限があり、溢れた場合は暗号化したまま通常DRAMへスワップされる。



※PRM(Processor Reserved Memory):システム起動時に、BIOS/UEFIの設定を通じて予約・隔離された物理メモリの一部。

出所:Intel, Intel® Software Guard Extensions(2015)、Enclave Memory Measurement Tool for Intel® SGX Enclaves

日本総研 The Japan Research Institute, Limited

Intel SGX｜TCB最小化の設計思想と制約

- SGXはVMのゲストOSすらTCBから除外する「TCBの最小化」により強固なセキュリティを実現する。
- 一方、EPC容量やシステムコール、移植性等に制約が存在する。

SGXにおけるTCB	SGXにおけるTCB外

• CPU
• エンクレーブ
  • アプリケーションの信頼領域
  • メモリの信頼領域
	• アプリケーションの非信頼領域
	• ゲストOS Kernel
	• Hypervisor
	• ホストOS Kernel

VMベースTEEではTCBに含まれる範囲

セキュリティレベルが高い	• TCBが最小（CPU＋エンクレーブのみ）で、OS・Hypervisorの脆弱性の影響を受けない • 攻撃面が小さく、鍵管理や高機密の小規模処理に最適
EPCの容量制約	• PRMがBIOS/UEFIで固定確保されている 旧Core世代SGX（～2020）：128MB、 Scalable SGX（Xeon）：最大512GB/ソケット • 超過した分はOSが暗号化したままページングされる。そのため、大規模なデータを処理する際はページングのオーバーヘッドが大きくなる
システムコールが利用不可能	• OSがTCB外なため、エンクレーブ内から直接read/write/socketが出来ない • システムコールを実施する際はOCALL※（EEXIT→syscall→EENTER）が必要となる。そのため、I/Oが多い場合オーバーヘッドが大きくなる
移植コストが高い	• 既存アプリの一部はsyscallが必要なものがあるため、そのままエンクレーブ内で実行はできない。そのため、移植のコストが発生する • LibOS※等で移植コストを抑えられるものの、TCBが拡大するためトレードオフの関係にある

※1 OCALL（Outside Call）：エンクレーブ内から非信頼領域への呼び出し ※2 LibOS（ライブラリOS）：OSの機能をライブラリとしてパッケージ化したもの

出所：Intel, Intel® Software Guard Extensions（2015）、Enclave Memory Measurement Tool for Intel® SGX Enclaves

（参考）Intel SGXの適用領域の変化

- 初代SGX（Core世代）は整合性ツリー付きMEEで完全なリプレイ防御を持つ代わりに、容量が128MBに制約されており、現在は非推奨（削除）となっている。
- Scalable SGX（Xeon世代）はツリーを撤廃しTME-MK（AES-XTS）へ移行、最大512GB/ソケットに大容量化を実現してサーバー用途へ一本化された。

項目	初代SGX（Core世代）	Scalable SGX（Xeon世代）
対象世代・時期	第6世代Core（2015）～第10世代（～2020頃）	第3世代Xeonスケーラブル（2021）～
EPC容量	128MB（PRM上限。後期256MB）	最大512GB／ソケット
メモリ暗号化	MEE：AES-CTR＋encrypt-then-MAC	TME-MK：AES-XTS（マルチ鍵）
完全性・リプレイ防御	整合性ツリー＋バージョンカウンタで暗号学的に完全（MAC不整合時はメモリコントローラが停止）	暗号学的ツリー・MACは撤廃。EPCMによるアクセス制御（論理的整合性）に依存
位置づけ	クライアント向けは2021年末に非推奨化	サーバ／クラウドの主流（DCAP前提）

初代SGXは整合性ツリーによる性能低下（2.2～14%）と128MBの容量制限を抱えていたが、Scalable SGXではツリーを撤廃することで性能低下を抑えた大容量化（最大512GB）を実現している。

出所：C. Shepherd, K. Markantonakis, Trusted Execution Environments, Springer（2024）等を基に作成

Intel TDX｜CPUモード(SEAM)と専用モジュールによる制御

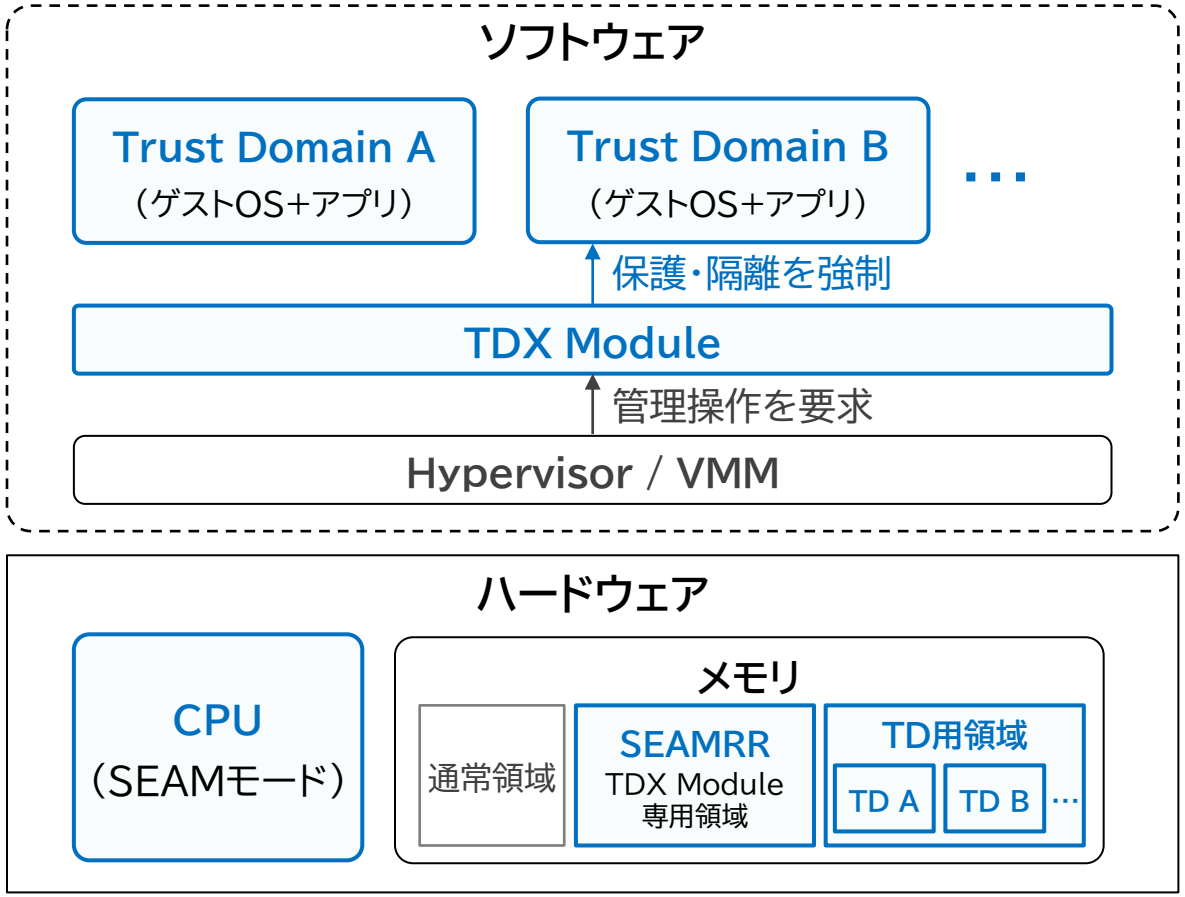
- TDXはIntelが2023年に導入したCVM(VMベースのTEEの実装手法)。
- CPUがハードウェアレベルで隔離・暗号化したVM(Trust Domain)を構築することで、ハイパーバイザをTCBに含めることなく、ゲストOSを含む実行環境全体を保護する。

Trust Domain(TD)

- 仮想マシン(VM)全体を一つの「信頼ドメイン」として隔離し、実行するための環境。
- 2023年の第4世代Xeonスケーラブル・プロセッサ(Sapphire Rapids)以降に採用されているIntel TDXにおいて、その中核的な概念。

Intel TDX Module

- 信頼ドメイン(TD)の構築や管理を行うために、CPUの特殊な実行モード(SEAM)で動作するセキュアなソフトウェア層。
- Intel署名済みのソフトウェアであり、TDXにおけるTCBの一部。
- ハイパーバイザとTDの間に立ち、メモリの暗号鍵管理やアクセス制御をハードウェアと連携して行うことで、VM間の隔離と安全性を担保する。



出所:Intel, Intel® TDX Module Base Architecture Specification(2025)

AMD SEV-SNP｜専用プロセッサによる制御

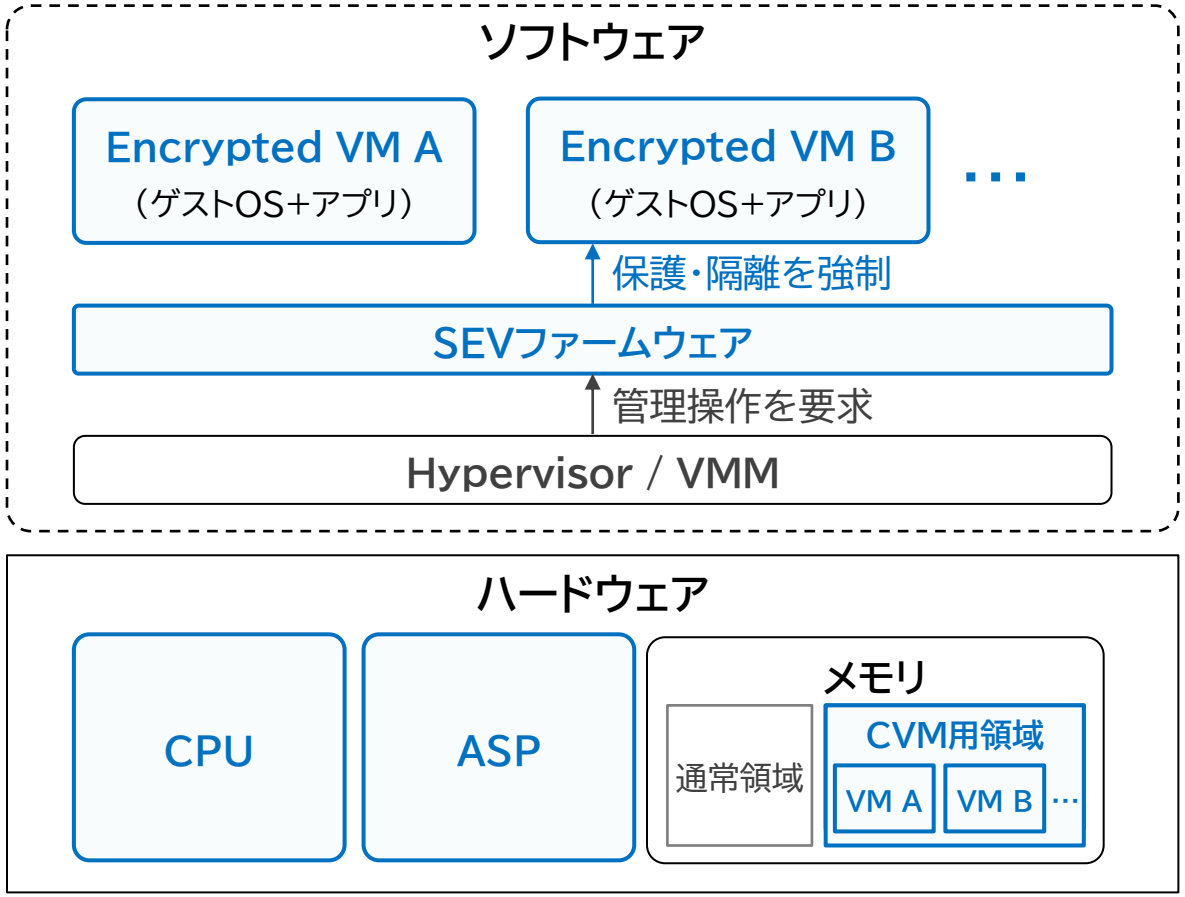
- SEV-SNPはTDXと同じくCVM（VMベースのTEEの実装手法）の一つ。
- セキュリティ管理を独立した専用プロセッサ（ASP※）が担う点において、TDXとは実装アプローチが異なる。

Encrypted VM

- 仮想マシン（VM）全体を、ハードウェア（AES-128等）によって暗号化・隔離して実行するための環境。
- AMD EPYCプロセッサの第1世代（SEV）から導入され、第3世代（Milan-SNP）でメモリ整合性保護（SNP）が追加された。

AMD Security Processor（ASP）

- VMの構築や鍵管理、整合性チェックを行うために、CPU内に独立して搭載されたセキュリティ専用プロセッサ（ARMコア）。
- メインCPU（x86コア）から物理的・機能的に独立しており、AMD署名済みのファームウェアを実行することで、ハイパーバイザを信頼することなくVMを保護する。



出所：AMD, SEV Secure Nested Paging Firmware ABI Specification Rev.1.58（2025）

日本総研 The Japan Research Institute, Limited

ゲストOSを含むTCB設計の影響

- CVMのTCBはCPUに加え、ゲストOSとVM上のアプリも含む。
- プロセスベースのTEEと比較し移植性が向上するが、TCBが拡大したためOS等の脆弱性の影響を受ける。

CVMにおけるTCB	CVMにおけるTCB外

• CPU
• 制御モジュール・プロセッサ
• ゲストVM（CVM）
  • ゲストOS
  • アプリケーション
  • メモリ
	• Hypervisor
	• ホストOS
	• 他のVM

セキュリティレベルのトレードオフ	• ゲストOS全体がTCBに含まれるため、OS等の脆弱性の影響を受ける（アタックサーフェスはプロセスベースのTEE（SGX等）より広い） • ゲストOSの堅牢化・最小化が運用の要点
メモリのスケーラビリティ	• メモリの専用領域の制限がなく、システムメモリ（RAM）をそのまま利用可能 • 大規模なデータを割り当ててもページングのオーバーヘッドが発生しにくい
システムコールが利用可能	• OSカーネルがTCBに含まれているため、VM内のアプリは通常通りシステムコールを利用可能
移植コストが低い	• 既存アプリを修正することなく、バイナリそのままで実行可能。コード内で信頼領域と非信頼領域を意識する必要がない

日本総研 The Japan Research Institute, Limited

Intel TDXとAMD SEV-SNPの比較

- いずれもCVMを実現する技術であり、主な保護対象や目的は共通。
- TDXはCPUの機能拡張（動作モード）で制御するのに対し、SEV-SNPは独立した専用プロセッサで制御する点で実装アプローチが異なる。

項目	Intel TDX	AMD SEV-SNP
保護単位	VM（Trust Domain：TD）	VM（Encrypted VM）
管理主体	**TDX Module** **（CPUのSEAMモードで動作するIntel署名ソフトウェア）**	**ASP（CPU内蔵の独立セキュリティプロセッサ）** **＋AMD署名ファームウェア**
メモリ暗号化	TME-MK （AES-XTS・TDごとに個別の鍵）	ハードウェア暗号化エンジン （AES・VMごとの個別鍵はSEV側の機能）
整合性保護	TDX Module ＋Secure EPT（アドレス変換の保護）	RMP （Reverse Map Table：ページ所有権のハードウェア管理）
アテステーション	DCAP構成（TD Report ＋ PCK証明書 ＋ Intel PCS） ※vTPM構成も一般的	SNP Report＋VCEK／VLEK証明書＋AMD KDS ※vTPM構成も一般的
対応世代	第4世代Xeonスケーラブル（2023）～	EPYC第3世代 Milan（2021）～ ※SNP対応
主要クラウドベンダにおける採用	Azure（DCesv5）／GCP（C3）	Azure（DCasv5・NCC H100 v5）／GCP（N2D）

（参考）Arm社のTEE技術

- Arm社はスマートフォンの生体認証等で20年以上利用されてきたTEE技術（TrustZone）の実績をベースに、クラウド市場や高度なオンデバイスAIの要求に応えるArm CCAへと対応領域を拡張している。

項目	Arm CCA（次世代のTEE）		Arm TrustZone（従来のTEE）
状態	Normal World	一般的なOSや普通のアプリが動作するオープンな実行空間	
	Secure World	指紋や暗号鍵等、端末自体の秘密を安全に処理・保管する共有のTEE。 端末メーカーやチップベンダーが利用する。	
	Realm World	一般の開発者やユーザーが個別に・動的に作成できるTEE。	
	Root World	各状態の切り替えやメモリ割り当てをコントロールする空間	
アテステーション	CCA Token（IETFのEAT規格 RFC 9334 に準拠）		チップベンダーやセキュアOSベンダーの**独自実装**
実績・展開状況	Armv9-A（アーキテクチャ名）で展開。モバイルが先行し、サーバー向けはこれから本格化の予定		2003年の発表以降、20年以上にわたりスマホの生体認証や決済の裏側で使われている業界標準

富士通 FUJITSU-MONAKA

富士通の次世代Armプロセッサ「FUJITSU-MONAKA」（2027年提供予定）は、Armv9のRME（Realm Management Extension）ベースでCCAを実装予定。Realm分離をアクセラレータへ拡張しエンドツーエンドのConfidential AIを実現する構想も公表しており、国産サーバにおけるTEEの選択肢として注目されている。

出所：Arm Developer Blog「How Fujitsu implemented confidential computing on FUJITSU-MONAKA with Arm CCA」／富士通研究所技術ブログ（2024-2025）

CPU TEE実装の比較表

- 目的や要件に合わせて、最小TCBで厳密に保護するプロセス型のSGXと、アプリ無改修でクラウドへ展開できるVM型のTDXやSEV-SNPを使い分けることが重要である。

観点	Intel SGX	Intel TDX	AMD SEV-SNP	(参考)Arm CCA
保護単位	プロセス(エンクレーブ)	VM(Trust Domain)	VM(Encrypted VM)	VM相当(Realm)
TCB	CPU＋エンクレーブ(最小)	CPU＋TDX Module＋ゲストOS	CPU＋ASP FW＋ゲストOS	CPU＋RMM＋ゲストOS
メモリ暗号化・完全性	TME-MK＋EPCM (初代はMEE＋整合性ツリー)	TME-MK＋Secure EPT	AESエンジン＋RMP	MEC(実装依存)
アテステーション	DCAP Quote (MRENCLAVE)	TD Report／vTPM	SNP Report(VCEK/VLEK)／vTPM	CCA Token(EAT準拠方向)
移植コスト	高(SDK移植 or LibOS利用)	低(既存アプリ無改修)	低(既存アプリ無改修)	低(既存アプリ無改修)
主な用途	**鍵管理・小規模秘匿処理**	**クラウドCVM**	**クラウドCVM**	**クラウドCVM モバイル・エッジ(見込み)**

出所:Intel, Intel® SGX／Intel® TDX Module Base Architecture Specification、AMD, SEV-SNP Firmware ABI Specification、Arm, Realm Management Extension System Architecture 等を基に作成

メモリ暗号化の必要性

- ハードウェアによる隔離（アクセス制御）はソフトウェア攻撃には有効であるが、CPU外にあるメモリやメモリバスのデータは透過的なメモリ暗号化で保護する必要がある。

攻撃種別	概要	メモリ暗号化の効果
コールドブート	電源遮断直後や再起動時に、DRAM内に一時的に残留する物理データを直接読み取る	○ メモリ上のデータが常時暗号化されているため、未復号のデータしか取得できない
バスプロービング	CPUとDRAMを結ぶ物理メモリバスにプローブ（計測器）を接続し、通信信号を傍受する	○ CPU外へ送出される直前に暗号化されるため、バス上の信号から平文を解読不能
DIMM抜取り・移設	稼働中・停止時にDIMMを取り外し、攻撃者の別マシンに挿入してメモリ内容を直接解析する	○ 復号鍵は元のCPU内部（レジスタ等）にのみ保持され、外部抽出や別環境での復号ができない
パターン解析	同一アドレスの暗号文の変化や一致を外部から観測し、データの状態変化を推測する（TEE.Fail等）	△ 固定鍵＋固定カウンタの暗号化ではデータ変化の特定を防ぎきれず、完全に防ぐには整合性保護（RMP等）が必要

出所：Intel, Intel® Architecture Memory Encryption Technologies Specification Rev.1.7（2026）、AMD, AMD Memory Encryption（2021）

（参考）CPUに対するサイドチャネル攻撃

- メモリ暗号化等に比べ難易度は高いものの、CPU（キャッシュや投機的実行）を標的としたサイドチャネル攻撃のリスクが研究・顕在化している。
- 複雑化するCPU脆弱性への迅速なパッチ適用や高度なコア分離を求め、インフラ層の防御をクラウド事業者に委ねる活用トレンドがある※

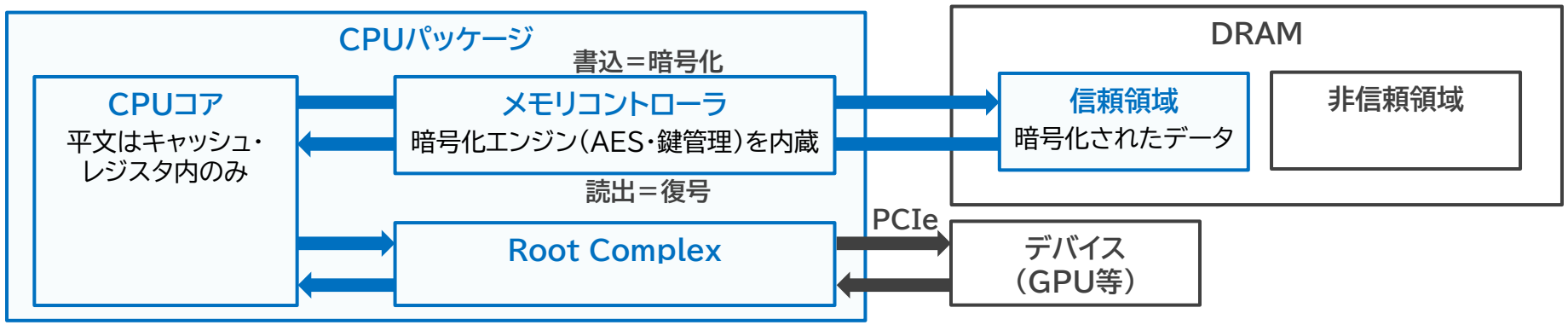
攻撃種別	代表例	概要	対応
電圧・電力 （フォールト注入）	Plundervolt （S&P 2020）	CPUの電圧制御（DVFS）を操作して演算誤りを意図的に誘発し、処理中の鍵情報を抽出する。	マイクロコード更新
投機実行・キャッシュ	• Foreshadow/L1TF • SGXPectr • ZombieLoad	投機実行の痕跡やキャッシュ共有のアクセス時間差（タイミング攻撃）から、TEE内部の秘密を推測する。	マイクロコード ＋設計の改訂
性能カウンタ	CounterSEVeillance （NDSS 2025）	CPUの性能モニタリングユニット（PMC）の計測値から、CVM内の命令実行パターンやメモリアクセス挙動を推測する。	ファームウェア更新 ・カウンタの参照制限

※TEEを「クラウド事業者を信用しない」ために用いる場合は矛盾したセキュリティモデルとなる。
サイドチャネル対策とのトレードオフや信頼境界の設定は、システムの要件定義次第である。

出所：K. Murdock et al., Plundervolt, IEEE S&P（2020）／J. Van Bulck et al., Foreshadow, USENIX Security（2018）／S. Gast et al., CounterSEVeillance, NDSS（2025）

メモリ暗号化の構造と採用技術

- 低レイテンシ化のため認証なしのAES-XTSを採用し、CPU内部で保持する鍵により透過的な暗号化を行う。
- TEE（CVM）では、複数鍵を用いてVMごとにメモリを暗号分離する手法が採用されている。



鍵はCPU内部で生成・保持されるため、OS／Hypervisor／管理者も取得不可能

暗号化エンジンの機構	提供	特徴
TME	Intel	システム全体を単一鍵で暗号化する汎用機能
TME-MK	**Intel**	**複数鍵を持ち、VM・ドメイン単位で分離**
SME／TSME	AMD	AES-128でメモリを暗号化。TSME BIOS設定で全体を透過的に常時暗号化
SEV(-ES／-SNP)	**AMD**	**VMごとに個別鍵を割り当てて暗号化・分離**

モード	認証（完全性）	特徴	主な用途
AES-XTS	**なし （機密性のみ）**	**ブロック単位で独立に暗号化。 暗号サイズは平文と同じで、 低レイテンシ**	**メモリ暗号化 （TME／SME）**
AES-GCM	あり （MACタグを付与）	認証付き暗号。改ざんを検知できるが、タグ分だけデータサイズが増える	• PCIe・I/O暗号化（バウンスバッファ） • TLS

太字：CVMで利用される暗号化機構・採用モード

日本総研 The Japan Research Institute, Limited

メモリ暗号化を補完する整合性保護とリプレイ防御

- CVMでは低レイテンシ維持のため、MAC等による検証ではなく、RMPやSecure EPTで不正書込を事前に遮断する方式が主流。
- 物理改ざんへの暗号学的耐性（MAC/Integrity Tree）を抑える代わりに、追加コストほぼゼロでハイパーバイザ等からの不正を防止する。

保護機構	防ぐ攻撃	仕組み	実装例
RMP （Reverse Map Table）	リマッピング・ 不正書込	物理ページの所有VM・状態を管理し、不一致な書込を拒否	AMD SEV-SNP
Secure EPT / Nested Page Table保護	アドレス変換の改ざん	Hypervisorによる不正なページ対応替えを遮断	• SEV-SNP • Intel TDX
MAC（暗号学的完全性）	暗号文の改ざん	キャッシュライン単位のMACで改ざんを検出（リプレイは検出不可）	• 初代SGX（MEE） • TDX（Ciモード） Scalable SGXはMACを持たず、EPCMのアクセス制御（論理的整合性）に依存
バージョンカウンタ＋ Integrity Tree	リプレイ攻撃	書込みごとに版数を進め、書き戻しを検知	クライアント版SGX（MEE）のみ

遮断による対策の優位性

- GCM（検出型）は読み出すたびに中身を検証するため、タグの計算・置き場のコストがデータパスに乗る
- RMP／NPTは中身を検証せず、Hypervisorが TEEのページに書き込みや対応付けの変更ができないように遮断
  （書き換えが起きなければ検証は不要）
- チェックはアドレス変換時にページ単位で実施し、結果はTLBにキャッシュ → 追加コストほぼゼロで低レイテンシを維持

アテステーションの意義と信頼の連鎖

- アテステーションは「今動いているコードと環境が正しいか」を署名付きで証明する仕組み。
- クラウド事業者や管理者を信頼せずに実行環境を検証できる。

信頼できる実行環境（Trusted Execution Environment）

- 利用者が「保護された状態で、想定通りのコードが動いているか」を検証できる環境
- クラウド事業者や管理者を信頼せずに利用可能

▲ **証明書の内容を利用者側のポリシーと照合することでTEEの信頼を確立**

アテステーション＝署名付き証明書（Report／Quote※）の生成と検証

- TEE種別、TCBバージョン、コードのハッシュ（MRENCLAVE／Measurement）、ノンス、署名、タイムスタンプ等を含む署名付きデータ
- 検証サービスにより利用者が合致時のみ鍵を渡す

▲ **製造時に焼きこまれた鍵から連なる署名の連鎖が、ソフトウェア攻撃者に対する偽造困難性を担保する**

信頼の連鎖（Chain of Trust）

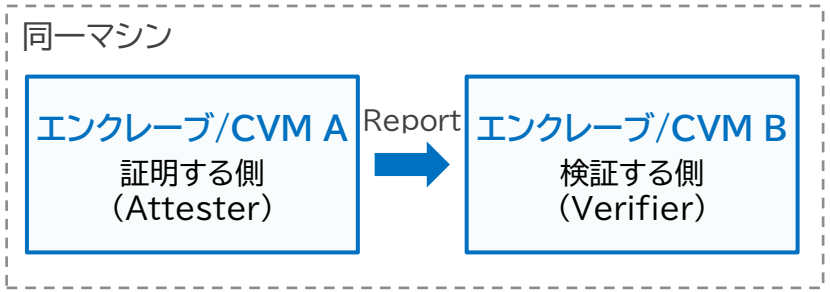
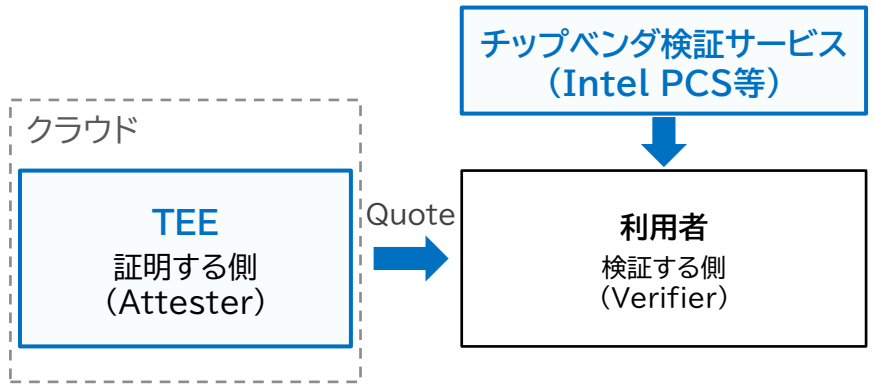
① 製造時鍵	② Quote／Report	③ 検証サービス	④ 利用者の検証
CPU／GPUに焼き込まれた鍵がRoot of Trust（信頼の起点）	TCBバージョンやコードのMeasurementを含んだ署名付きのデータを生成	Intel PCS／AMD KDS／Azure MAA等が証明書を提供	ポリシーに合致した時のみ鍵を渡す

※Report:同一チップ内で検証を行うため、CPUが生成するローカル用の証明データ。同一マシン内での相互認証や、Quote生成の基礎データとして利用される。
Quote:外部から検証できるよう、Reportを公開鍵暗号で再署名した送信用の証跡データ。遠隔地の利用者がネットワーク経由でTEEの正当性を確かめる際に利用される。

出所：Intel, Intel® SGX DCAP ECDSA Attestation Orientation Guide、AMD, SEV-SNP Attestation: Establishing Trust in Guests

アテステーションの種類

- アテステーションは検証者の位置により「ローカル（Report）」と「リモート（Quote）」に分類される。
- クラウド環境（CVM）の安全な利用や鍵交付には、外部から検証を行う「リモートアテステーション」が不可欠である。

項目	ローカル	リモート
検証者の位置	同一マシン内の別エンクレーブ	外部のサービス／利用者
主な用途	初期鍵交換、エンクレーブ間認証 ※SGXではQuoting EnclaveがReportを検証し、同一CPU上で動作することの確認とリモートRAの前段を担う	クラウド上のTEE検証、KMS連携
代表実装	SGX Local Attestation	DCAP（SGX/TDX）、SEV-SNP Quote、TDX Quote
イメージ図		

アテステーションのフロー｜Intel DCAP

- Intel CAをルートとするPCK証明書チェーンに基づき信頼を検証する。
- Intel PCSから最新のTCB情報やCRL(失効リスト)を取得・照合することで、クラウド／オンプレ問わず柔軟な検証を可能にする。

Quoteの構造

- TEE種別、TCBバージョン、Enclave IDハッシュ(MRENCLAVE)、ナンス、署名等を含む構造化データからなる。
- QE※1がアテステーションキー(PCE※2がPCK鍵で保証した鍵)で署名し、検証者に提出する

PCK証明書(Provisioning Certification Key)

- CPU個体に紐づく証明書。Intel PCS(Provisioning Certification Service)から取得する。
- 検証時はCRL(失効リスト)と併せて照合される。証明書チェーンのルートはIntelに存在する。

① アプリケーションがQuote生成を要求する

↓

② QEがPCK鍵で保証されたアテステーションキーを用いてQuoteに署名する

↓

③ 検証者がQuoteとPCK証明書を受領する

↓

④ Intel PCSから最新のTCB情報・CRLを取得する

↓

⑤ ポリシーを照合する

DCAPの検証フロー※3

※1:Intelが提供・署名する特別なシステムエンクレーブ。CPU内部で生成されたローカル用データ(Report)を検証し、外部送信用のリモート証跡(Quote)へと変換・署名する役割を担う。
※2:Intelが署名済のシステムエンクレーブ。CPU製造時にフューズに焼き込まれた秘密の値からPCK秘密鍵を導出して、署名を行う。
※3:SGXのリモートアテステーションにはEPID(プライバシ保護グループ署名・旧方式)とDCAP(ECDSA・データセンタ向け、現在の主流)の2系統がある。

日本総研
The Japan Research Institute, Limited

vTPMベースのアテステーション

- SEV-SNP／TDXなどはvTPM※を通じてゲストOS内からアテステーション情報を取得できるため、CPUベンダーの差異を意識せず、TPMツールを流用可能。
- 主要クラウドのCVMでは、vTPM経由で取得する構成が一般的である。

生のハードウェアレポートによるアテステーション

SEV-SNP VM
AMD専用IFで
Reportを取得

SNP Report →

検証系統A
VCEK証明書／
AMD KDS連携

TDX VM
Intel専用IFで
Reportを取得

TD Report →

検証系統B
PCK証明書／
Intel PCS連携

取得IF・形式・証明書チェーンが異なり、取得コードも検証も2系統必要

vTPM方式のアテステーション

SEV-SNP VM
vTPM(TPM 2.0)を
起動時にロード

AK Quote →

TDX VM
vTPM(TPM 2.0)を
起動時にロード

AK Quote →

共通の検証系統
Quote署名検証＋PCR照合
（AMD／Intel共通）
※初回のみEKの裏付け確認
にKDS／PCS照合が必要

**CPUベンダー固有の処理は初回のEK確認だけに局所化され、
定常的な検証は共通化される**

※vTPM(仮想TPM)：CVMの保護境界内で動作するTPM 2.0準拠のソフトウェアTPM。ハードウェア内蔵ではなく、VM起動時にソフトウェアとしてロードされ、そのロード自体がCPUベースのアテステーション(launch measurement)で計測・保証される。

日本総研
The Japan Research Institute, Limited

アテステーションの運用課題

- アテステーションは導入後の環境追随が不可欠であり、TCB更新や証明書失効への対応遅れはサービス停止（鍵リリース拒否）につながる。
- ライフサイクル管理の自動化と、稼働セッションに変化を反映する「再アテステーション機構」の確立が重要である。

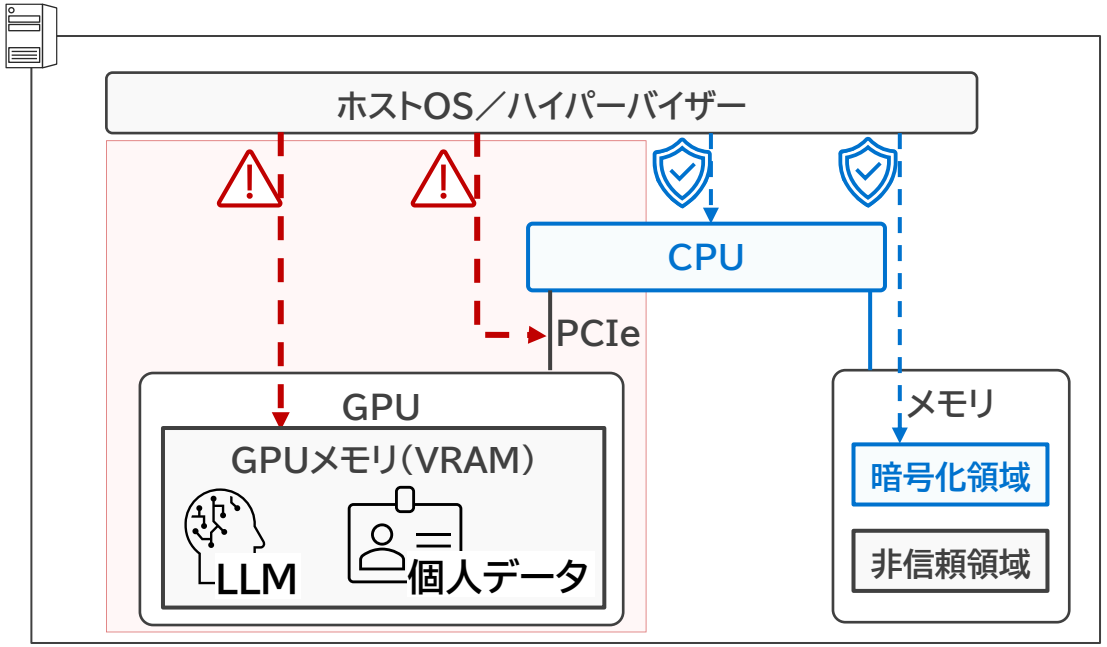
課題	変化の起点	現象と影響	個別対応	全体対応
TCB更新への追随（TCB Recovery）	ベンダー起因	脆弱性対応でベンダーが新TCBを配布し、旧TCBの検証は段階的に不合格化。追随が遅れると鍵リリース拒否・サービス停止	ベンダー通知の監視と早期パッチ適用、失敗時のフォールバック	再アテステーション ＝ 証跡の鮮度を保つ仕組み nonce再発行・トークン有効期限・TCB変化（TCB Recovery）・鍵ローテーションをトリガに証跡を再取得し、過去証跡の使い回しを防ぐ。 左記の変化は再アテステーションを実施した時点で初めて稼働中のセッションに反映されるため、トークン有効期限と鍵ローテーションで波及までの時間に上限を設ける。
証明書失効への追随（CRL管理）		旧PCK／EK証明書が失効しCRLが更新される。反映を怠ると失効済み証明書を受理	CRLの定期取得・自動反映、失効チェックの強制	
移行期間の扱い（Grace Period）		新旧TCBが混在し旧TCBを一時許容。期限を決めないと例外が常態化	許容期限のポリシー明示、超過アラートと強制失効	
期待値（Measurement）の管理	自社起因	アプリ・OS更新のたびMeasurementが変化。同期を怠ると正規リリースが不合格、または検証が形骸化	ビルド再現性＋CI/CDで期待値を自動算出・配布	

GPU TEEの必要性

- 近年急速に普及し注目されているLLMの推論では、一部で企業秘密とされる「モデルの重み」や、機微データが含まれ得る「入出力」がGPU上に滞在する。
- そのため、CPU TEEだけでは保護範囲が不十分であり、GPU自体を保護境界（信頼境界）に取り込む必要がある。

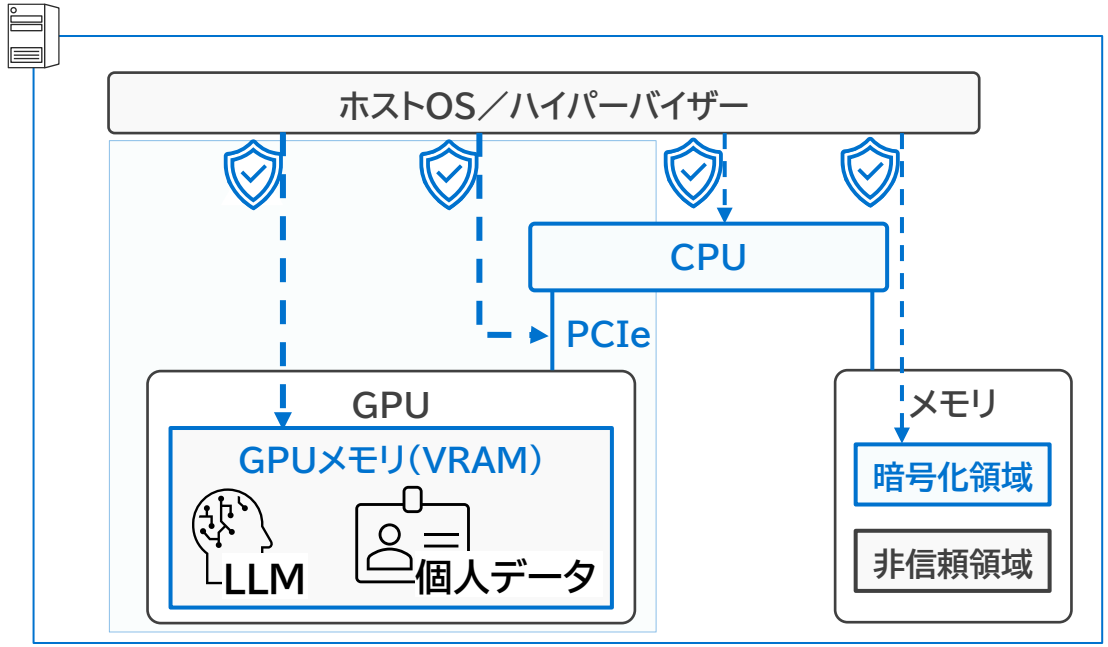
CPU TEEのみ（GPU TEE非対応）

GPUメモリ（VRAM）やCPU-GPU間の通信路（PCIe）が
暗号化されていないため、データ漏洩・改ざんのリスクが残る



GPU TEE導入時

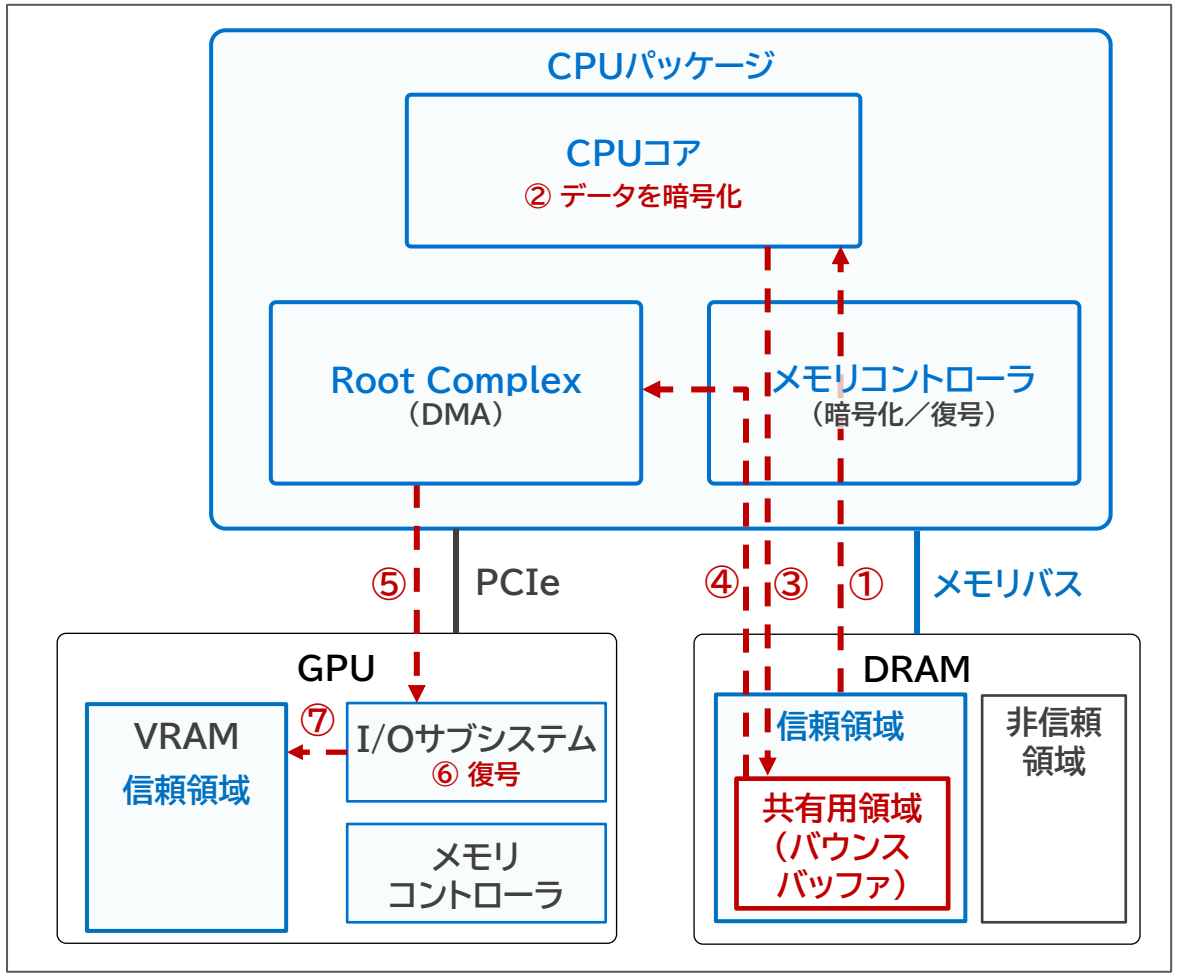
VRAMや通信（PCIe）まで暗号化が拡張され、GPUで処理
するAIモデルや入力データを保護した環境で実行可能



※GPU TEEの中核要素は3点：①GSP（GPU System Processor）＝GPU側のRoT（鍵保持・アテステーション署名・CCモード制御）、②VRAM暗号化、③PCIe経路の保護。

データ転送時のオーバーヘッド

- H100世代のGPU TEEとCPU TEE間は直接のメモリアクセスが出来ないため、共有領域を経由した転送が必要。
- アプリ／ドライバ層での暗号化処理とバウンスバッファの往復コピーにより、データ転送量に比例した大きなオーバーヘッドが発生する。



DRAM内データのGPUへの転送フロー

① 信頼領域内データをCPU(コア)が読む
DRAM→メモリコントローラ(復号)→CPUコア

② CPUコアがデータを暗号化する

③ 暗号文をCVMの共有領域(バウンスバッファ)に書き込む
CPU→メモリコントローラ→DRAM

④ Root ComplexのDMAが③を読む
DRAM→メモリバス→メモリコントローラ→Root Complex(DMA)

⑤ GPUにデータを転送する
Root Complex→PCIe→GPU

⑥ GPU内のI/Oサブシステムで復号

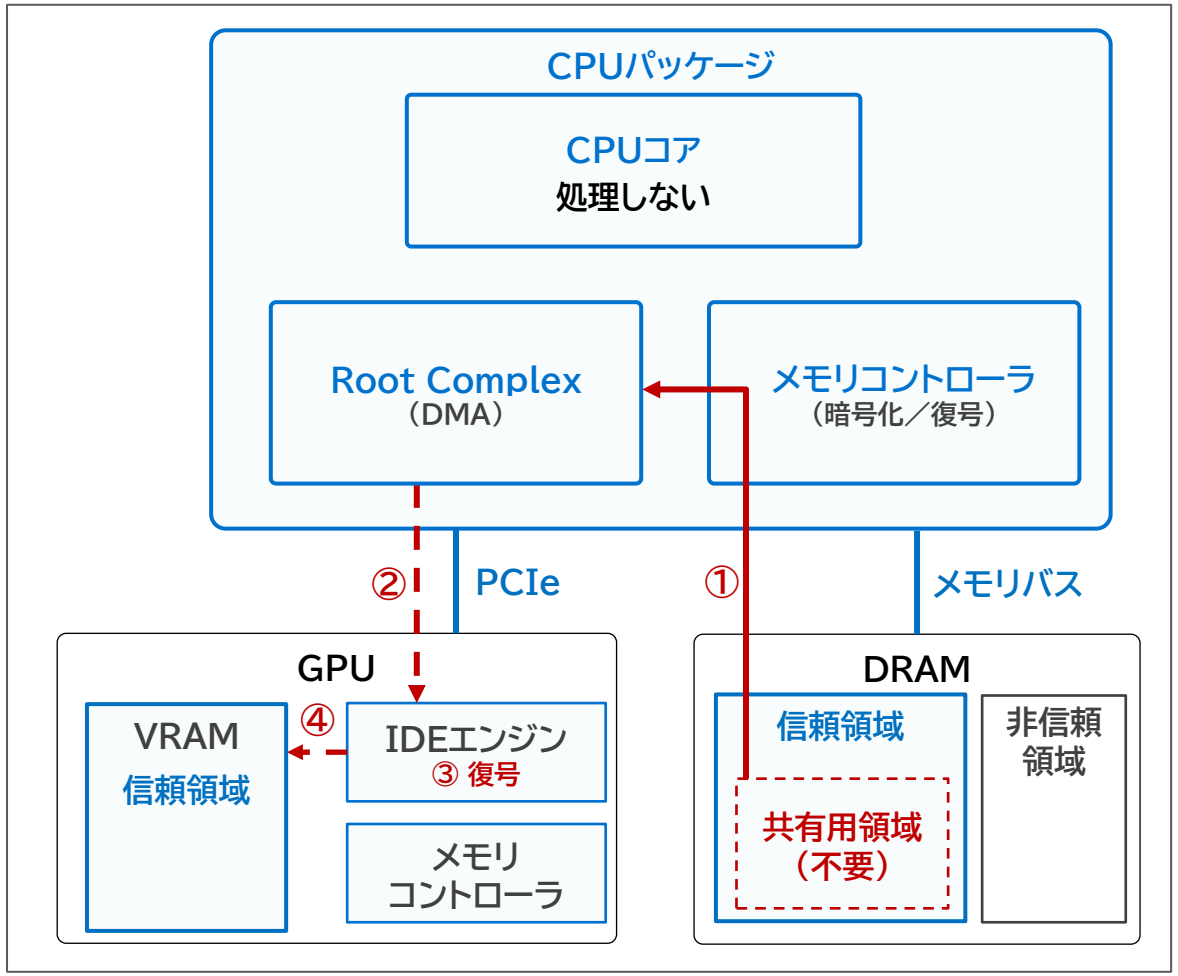
⑦ VRAMの信頼領域に配置

暗号化コピー(②③)と共有用領域の往復が、転送データ量に比例するオーバーヘッドの主因

出所:NVIDIA, Confidential Compute on NVIDIA Hopper H100(2023)、NVIDIA Secure AI with Blackwell and Hopper GPUs v1.3(2025)等を基に作成

Blackwell世代のインライン暗号化

- Blackwell世代ではPCIe IDE/TDISPの採用により、CPU TEEの信頼領域からGPUへダイレクトにDMA転送が可能となる。
- ハードウェアによるインライン暗号化でバウンスバッファへのコピー処理を排除しデータ転送のボトルネックを解決する。



Secure PCIe/PCIe IDEによる転送の流れ

① GPUのDMAが信頼領域を直接読み出す(メモリコントローラが復号)
DRAM→メモリコントローラ(復号)

② Root ComplexのIDEエンジンがPCIeパケット(TLP)をハードウェアで暗号化して転送

③ GPU側のIDEが復号

④ VRAMの信頼領域に直接配置

項目	H100世代(前ページ)	Blackwell世代
転送経路	共有用領域(バウンスバッファ)を経由	**信頼領域から直接DMA可能**
暗号化の主体	CPUコア(アプリ／ドライバ層)	**PCIe IDE(ハードウェア)**
コピー回数	暗号化コピー×2＋DMA	**DMAのみ**
オーバーヘッド	転送データ量に比例して増加	大幅に削減(ハードウェア処理)
対応CPU/PCIe	Sapphire Rapids／Genoa世代・PCIe 5.0	Granite Rapids／Turin以降・PCIe 5.0(ECN)/6.0

出所:NVIDIA, NVIDIA Secure AI with Blackwell and Hopper GPUs v1.3(2025)、Unified Deployment Guide for Confidential Computing v7.1(2026)等を基に作成

（参考）「TEE-I/O」の標準規格

- ホストCPUの保護境界をGPU等の外部デバイスまで安全に拡張する概念を「TEE-I/O」と呼ぶ。
- 単一の技術ではなく、3つの標準（SPDM・IDE・TDISP）を相互に組み合わせることで実現されている。

標準	策定団体	役割
SPDM	DMTF	デバイスの認証・計測値（Measurement）の取得・セッション鍵の交換
IDE	PCI-SIG	PCIeパケット（TLP）をAES-GCMで暗号化し、経路の機密性・完全性を保護
TDISP※1	PCI-SIG	デバイスをTEEへ安全に割り当てる手順・状態遷移を規定（全体の束ね役）

※1ホスト側の対応実装：Intel TDX Connect、AMD SEV-TIOがTDISP系仕様を採用。
NVIDIA BlackwellのTEE-I/Oもこれら3つの標準の組合せで構成される。

① SPDMでデバイスを認証し、計測値を取得する

↓

② IDEストリームを確立し、PCIe経路の暗号鍵を設定する

↓

③ TDISPでデバイスIF（TDI※2）をLOCKし、構成を固定する

↓

④ TEE側が計測値をポリシー照合（アテステーション）する

↓

⑤ 合格後にRUNへ遷移し、暗号化DMAで利用を開始する

信頼確立のフロー

※2 TEE Device Interface

出所: DMTF, Security Protocol and Data Model (SPDM) Specification, DSP0274; PCI-SIG, Integrity and Data Encryption (IDE); PCI-SIG, TEE Device Interface Security Protocol (TDISP)

日本総研 The Japan Research Institute, Limited

主要ハードウェアベンダーのGPU TEE接続比較

- CPU TEEとデバイスを接続する仕様は各ベンダーが整備中であり、実運用ではNVIDIAが先行する。
- 基本原理（デバイス側のアテステーション・相互検証・パス暗号化）は共通だが、採用される仕様と成熟度に差がある。

ベンダ・製品	アプローチ	特徴	成熟度
NVIDIA H100／H200	バウンスバッファ方式のGPU CC	量産実機あり。NRASによるアテステーション	実運用段階（2024～）
NVIDIA Blackwell	TEE-I/O（インライン暗号化）	バウンスバッファ不要。性能制約を根本から解消	出荷開始。本格展開はこれから
NVIDIA Rubin	ラックスケールCC	NVLinkスイッチを含むラック全体を単一な安全なドメインに統合可能	次世代以降 （2026年後半以降～）
AMD MI300X系	SEV-SNP対応ホストとの連携	EPYCとの親和性。ROCmエコシステム	計画・初期プレビュー
Intel TDX Connect	TDX＋TDISPでデバイス接続保護	GPUに限らずアクセラレータ全般に一般化	仕様策定・実装進行中
Arm CCA	Realm＋RMMにデバイスを取込む	モバイル・エッジ推論向けに発展の可能性	仕様段階・実製品待ち

技術的共通項：
①デバイスがAttestation Reportを生成できる、②CPU TEEと相互検証（mutual attestation）する、③PCIe等のバスを暗号化する
という3条件が「GPU TEE」の要件と言える。

日本総研 The Japan Research Institute, Limited

GPU TEE実装の比較表

- GPU TEEの基本構造（VRAM暗号化・RoT・アテステーション）は共通しており、主な差異は「PCIe経路の暗号化方式」と「マルチGPU・運用制約」に存在する。
- 実システムの選定・設計においては、転送性能（インライン暗号化の有無）に加え、仮想化制約（MIG不可等）や対応ソフトウェアの考慮が不可欠。

観点	NVIDIA H100 CC	NVIDIA Blackwell	AMD MI300X（計画）
VRAM暗号化	AES-XTS		AES-XTS＋SEV-SNP連携
PCIe経路	**AES-GCM（バウンスバッファ経由）**	**IDE／TEE-I/O（直接DMA）**	**SEV-TIO（検討中）**
アテステーション	NRAS＋EAT（RFC 9334）		SEV-SNP互換の仕様予定
ファームウェアRoT	GSP＋OTP公開鍵		SoC内のセキュアMCU
マルチGPU	NVLink暗号化・GPU間相互認証 ※CC有効時はMIG/vGPU不可（GPU丸ごと1台＝1 CVMに占有）		Infinity Fabric暗号化
対応ソフトウェア	CUDA／TensorRT等ほぼ既存のまま		ROCm系（対応待ち）

Composite Attestationの必要性

- Composite Attestationとは、CPUとGPUという独立した保護境界のレポートをバインドし、「1つの不可分な組（ペア）」として証明する技術である。
- CPUとGPUの個別検証では防げない「別マシンGPUへのすり替え（リレー攻撃）」を機械的に排除し、複合環境全体の信頼を確立するために必要である。

CPU TEE単体（DCAP）

主な流れ

① 検証者がNonceを発行
② CPU TEEがQuoteを生成
③ 証明書チェーン＋ポリシー照合
④ 合格でCPU TEEへ鍵をリリース

CPU TEEが本物で
正しい状態であることを保証する

GPU側の保証が不在のため、CPUからGPUへの転送経路で、データの改ざん・漏洩を防御不能

CPU・GPUを独立に検証

主な流れ

① CPU QuoteをDCAPで検証
② GPU ReportをNRASで検証
③ それぞれ合格なら利用開始

CPU TEEとGPU TEEが
個別に本物であることを保証する

それぞれの保証が「同じマシンの組」であることを保証しない。別マシンの検証済みGPUのReportを盗用された場合、検証をすり抜けて悪意ある未検証のGPUへデータが流出する。（リレー攻撃）

Composite Attestation

主な流れ

① CPU・GPU双方のReportに同一のNonceを付与
② CPU・GPU両Reportを取得
③ TEE間の相互認証・チャネル鍵確立
④ 同一Nonce・期待値・TCBをAND判定で検証

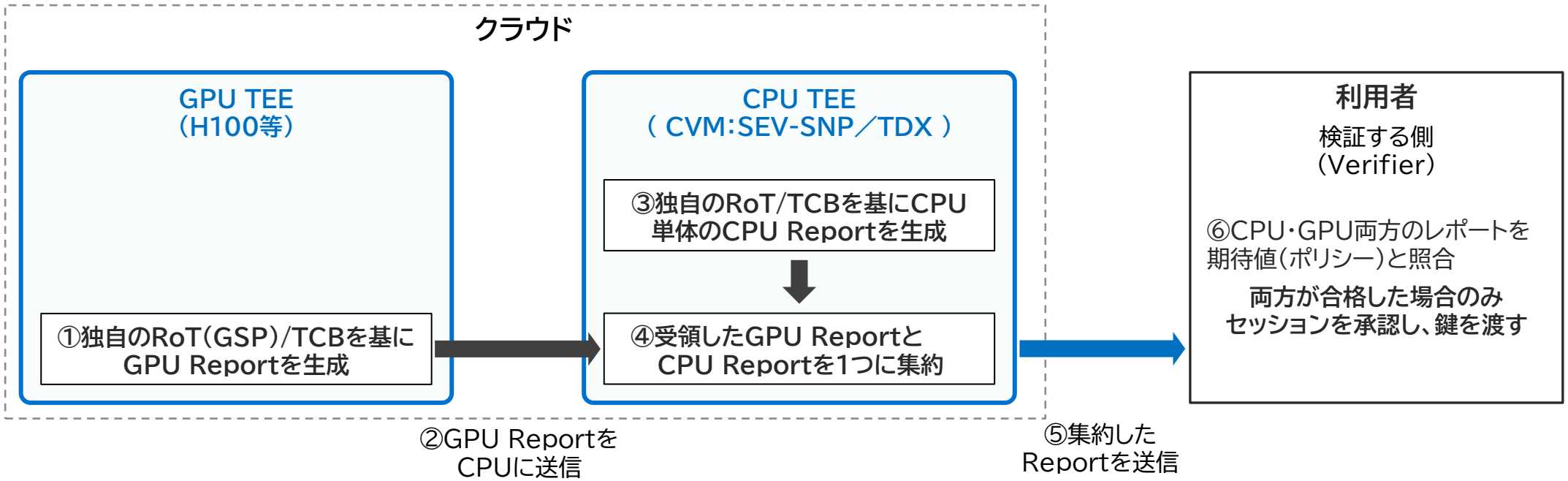
個々の保証と、同一のペアの結合
であることを保証する。

TEEが「個々の箱の正しさ」を保証するのに対し、**Composite Attestationは「箱と箱のつなぎ目」**を保証する。鍵の行き先が検証済みのセッションに固定され、すり替えを機械的に拒否できる。
※ただし保証されるのは設計上の結合であり、実装がCPU個体への束縛を欠く場合、物理攻撃前提での証跡の借用（TEE.Fail）が残る。実機での結合検証（同一nonce封入・相互認証）は追加検証課題。

出所：C. Wang, J. Huang et al., SoK: Analysis of Accelerator TEE Designs, NDSS（2026）、NVIDIA, NVIDIA Attestation Documentation、TEE.fail, IEEE S&P（2026）

Composite Attestation構成の全体像

- Composite AttestationではCPU TEEがハブとなり、GPU TEEから回収したレポートと自らのレポートを1つに集約して検証者へ一括送信する。
- 検証者が集約レポートを一括照合し、双方の適合を確認した時点でのみセッションを承認して暗号鍵をリリースする。



2つのReportを「同一セッションの組」として束ねる検証(アテステーション)が
Composite Attestation

信頼チェーンの構築｜CPU起点／GPU起点

- Composite AttestationによるTEE環境の信頼チェーンには、ユーザーデータ保護を軸とする「CPU起点」と、モデルIP保護を軸とする「GPU起点」の2つの設計パターンが存在する。
- 現行の実装ではCPU起点が主流だが、将来的には（Blackwell世代やTEE-I/Oの浸透により）保護対象（データ／モデル）に応じた柔軟な信頼チェーンの選択が可能となる。

観点	CPU TEE起点（アプリ主導）	GPU TEE起点（モデル主導）
主に守る資産	ユーザーの入力・セッション・アプリの秘密	モデル重み（知的財産）
信頼チェーンの形	検証者がCPU TEEを検証 →CPU TEEがGPU TEEを検証し、データを渡す	モデル提供者がGPU TEEを検証 →重みを直接GPUへ供給 通信経路としてCPUを経由するがCPU側に平文が現れない
鍵のリリース条件	鍵はCPU TEEのReport合格でリリース。 アプリがGPUを検証してから渡す（重みはCPU TEEを経由）	重みの鍵はGPUのReport合格を条件に、GPUの セッション鍵へ直接包んで渡す
適するユースケース	BtoBの機密推論、個人データ処理	モデルの配布・レンタル、IP保護

両者は排他的ではなく「どの秘密の鍵を、どちらのReport合格にひも付けるか」という配線の設計選択である。
取れる起点はRoT構成（SoK 3型 → 次頁）で決まる。

※GPU TEE起点は理論上の設計選択肢である。現行NVIDIA GPU CCではGPUの証明がCVM（CPU側）経由でのみ信頼に根付くため、
単独の信頼起点としては留保が必要（将来のMix型：Blackwell＋TDX Connectで実現見込み）。

SoK分類(Host型／Acc型／Mix型)による比較

- どちらの信頼起点(アプリ主導／モデル主導)を採用できるかは、ハードウェアのRoT構造(Host型／Acc型／Mix型)によって技術的に決定される。
- 現行のAcc型(H100)から次世代のMix型(Blackwell)へ進化することで、CPUとGPUが対等に相互検証する理想的な信頼チェーンが完成する。

型	Host型 (Host-centric)	Acc型 (Accelerator-centric)	Mix型 (Mixed)
RoT(信頼の起点)の所在	CPU TEEのみがRoTを持ち、 デバイスは信頼境界の延長として扱う	デバイス(GPU)が独自のRoTを内蔵し、 CPUから独立	CPU・デバイス双方がRoTを持ち、 相互認証で結合
取れる起点／主導役	CPU起点のみ(アプリ主導)	CPU起点主導 (GPU起点は理論上可能だが制約あり)	両起点 (CPU・GPUの対等な相互検証)
代表例	Intel TDX Connect	NVIDIA H100 CC (現状の商用主流)	Blackwell＋TDX Connect (TEE-I/O密結合)

実装上のポイント: Host型はアプリ主導のみ。Acc型(H100)はGPU独自RoTを持つがCVM依存が残る。両起点を対等かつ高度に融合できるMix型(Blackwell世代)で本命化する見込み。

出所:C. Wang, J. Huang, et al., SoK: Analysis of Accelerator TEE Designs, NDSS (2026) 等を基に作成

日本総研
The Japan Research Institute, Limited

TEEの脅威モデルの前提と想定する攻撃者

- TEEはすべての攻撃を防ぐ「万能の技術」ではなく、悪意あるOSや同居テナントからの保護を主目的として設計されている。
- 物理改造やサプライチェーン、アプリ自身のバグなど、TEEの防御対象外となる脅威は運用プロセスや開発統制で補完する必要がある。

脅威カテゴリ	具体像	TEEの防御範囲	補完策
特権ソフトウェア攻撃者	悪意のOS／ハイパーバイザ、クラウド管理者	○ 防御対象（設計の中核）	—
同居テナント	同一ホスト上の他VMからの共有資源経由の攻撃	○ 防御対象（隔離・鍵分離）	サイドチャネルは個別に評価
物理アクセス攻撃者	DC内部者によるバス傍受・機器改造（TEE.Fail等）	△ 従来は対象外（Intel/AMDの公式見解）	物理セキュリティ、 在証明型RA（POE/DCEA）
サプライチェーン	製造・配送・保守段階での改ざん、署名鍵流出	× 対象外	調達管理・ベンダー監査
TEE内アプリの脆弱性	エンクレーブ／CVM内のバグ・悪意コード	× 対象外（中身までは守らない）	セキュア開発・コード監査・最小化
可用性（DoS）	リソース枯渇・起動妨害	× 対象外	冗長化・SLA

TEEの保護範囲と対象外の脅威を正しく特定し、責任分界を明文化することが、TEEを導入したシステム設計検討の要点

特権ソフトウェア（OS/Hypervisor）からの攻撃

- TEEは、OSやHypervisorが侵害された状態であっても、ハードウェアレベルでメモリの「盗み見・改ざん・すり替え」を拒否する。
- 外部からの悪意のある入力による脆弱性はハードウェアでは防げないため、TEE内の実装側での対応が必要である。

攻撃手法	手法	TEEの防御機構
メモリの直接読出し	特権を用いてTEE領域のメモリを参照する	ハードウェアアクセス制御（EPCM等）＋メモリ暗号化 特権ユーザーからの平文の取得を拒否
不正書込み・改ざん	HypervisorがTEEページへ書き込む	RMP（SEV-SNP） / Secure EPT（TDX） による書き込み制限 特権OSからの不正な書き換え・改ざんを遮断
リマッピング・エイリアシング	アドレス変換表を書き換えてページをすり替える	RMP / Nested Page Table による対応関係の固定 物理アドレスの不正なすり替えを拒否
リプレイ攻撃	過去の正しい暗号文を書き戻す	整合性ツリー（SGX）やCVMの書き込みアクセス制御 過去の古い暗号文への巻き戻しを検知・拒否
DMA攻撃	周辺デバイスから直接メモリへアクセスする	IOMMU＋ハードウェアによるフィルタリング 周辺デバイスからのメモリ直接アクセスを遮断
インターフェース攻撃（Iago※等）	悪意のsyscall戻り値等でTEE内のアプリを騙す	TEEの防御対象外のため、TEE内アプリ側の防御的実装（入力検証・LibOSの堅牢化）が必要

※ S. Checkoway, H. Shacham, ”Iago Attacks: Why the System Call API is a Bad Untrusted RPC Interface”, SOSP (2013)

（参考）物理サイドチャネル攻撃｜TEE.Fail

- TEE.FailというDDR5メモリバスへのインターポーザ（傍受用の中間基板）挿入による受動的な物理攻撃が公表されている。（2025年10月公表・IEEE S&P 2026）
- 決定的暗号化（AES-XTS）の「同一アドレスでは同一平文→同一暗号文」という性質を突き、比較的安価な装置で成立する。

攻撃の仕組みと影響

TEE.Failの仕組み

- DDR5メモリバスに中間基板（インターポーザ）を挿入し、トラフィックを受動的に傍受する。
- AES-XTSのTweakはアドレス依存のため、同一アドレスの書込みは同一平文→同一暗号文となる。
- 暗号を解読するのではなく、暗号文の一致・変化のパターンから内容を推定する。
- Intel TDX／Scalable SGX、AMD SEV-SNP（DDR5世代）が対象。

攻撃による影響

- CPU固有のアテステーション署名鍵（ECDSA）が抽出されると、偽造されたQuoteがアテステーションを通過する。
- GPU証跡がCPUに束縛されないため、別マシンの正規GPU証跡を使いまわすことが可能になる。

ベンダーの見解と対策

ベンダーの見解

- Intel/AMDともに**「物理攻撃は脅威モデル（保護対象）の範囲外」**との立場※であり、データセンターの物理警備で防ぐべき範疇としている。

対策の方針

- 物理セキュリティの前提化：ホスト（DC）側の物理的なアクセス統制が担保されていることを、信頼の大前提として明示する。
  「クラウドベンダを信用する」ことも対策の一つ
- 所在証明型RA（リモートアテステーション）の検討：「どこで動いているか」を物理筐体に紐づけて証明する新技術の採用。
  例：Intel POE（プラットフォーム所有者証明）、Flashbots DCEA / Proof of Cloud（vTPMで物理筐体に束縛）
- メモリ保護機能の根本強化：完全性・鮮度保証（リプレイ防止）を持つ次世代メモリ保護の導入（現在は研究段階）。

出所：TEE.Fail, IEEE S&P (2026), Intel POE (2026), Flashbots DCEA (arXiv:2510.12469, 2025) 等

※ Intel TDX Spec / AMD SEV-SNP Spec (AMD-SB-3040)

CVM(SEV-SNP)系の最新攻撃事例

- 2025年に相次いで発表されたSEV-SNPへの攻撃研究は、GPU固有ではなくCPU(CVM)の初期化処理やサイドチャネル等を狙ったもの。
- CPU側が侵害されると束ね役としての信頼が崩れComposite Attestation全体のリスクとなるため、ベンダーのセキュリティ通知監視と迅速なTCB Recovery(FW更新)が不可欠となる。

攻撃名	発表	機構	影響	対応
RMPocalypse	CCS 2025 (CVE-2025-0033)	RMP初期化時の欠陥を突き RMP保護を無効化する	SEV-SNPの完全性保証の迂回	AMDファームウェア修正
CounterSEVeillance	NDSS 2025	性能カウンタを介したサイド チャネル攻撃	CVM内の命令・秘密の推測	カウンタの仮想化・制限
Heracles	CCS 2025	ページ移動機能と暗号Tweak を悪用した選択平文攻撃	メモリ内容の推測	暗号文隠蔽・ページ移動 制限の適用等

出所:RMPocalypse, CCS (CVE-2025-0033) / CounterSEVeillance, NDSS / Heracles, CCS 等を基に作成

TCBの大きさとリスク・移植性のトレードオフ

- TCB（信頼領域）が拡大するほど潜在的な攻撃面や脆弱性リスクが増大するため、「TCBの最小化」を意識した構成選定が求められる。
- 「移植性の高さ（無改修）」と「セキュリティ範囲の絞り込み」はトレードオフの関係にあり、保護資産と脅威モデルに応じたバランス評価が不可欠である。

構成	TCBの範囲	攻撃面	移植コスト
SGX（プロセス型）	CPU＋エンクレーブのみ	OS・Hypervisorの脆弱性の影響を受けない	SDK移植やLibOSが必要なため高い
CVM（TDX／SEV-SNP）	CPU＋TDX Module／ASP FW＋ゲストOS全体	ゲストOS・カーネルの脆弱性が影響	無改修で移植可能なため低い
Composite Attestation構成	CPU側TCB＋GPU側TCBの和集合	結合部（アテステーション連携）の検証も必要	無改修で移植可能なため低い

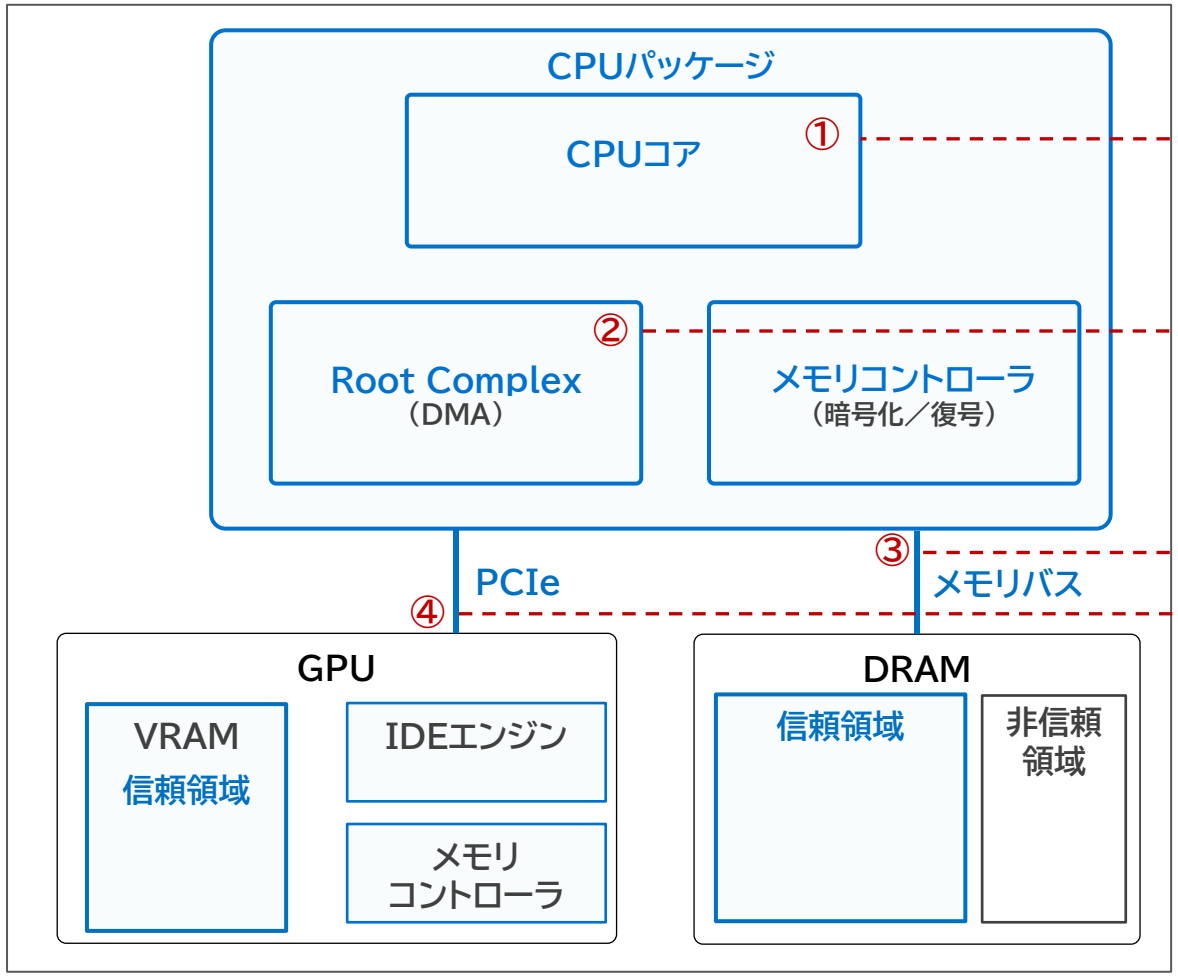
「TCBは可能な限り小さく単純に」はセキュリティ設計の古典的な規範である。TCBの拡大は攻撃面・バグ混入・監査コストの要因となる。

CVM系の運用ではゲストOSの最小化・堅牢化（Confidentialコンテナ向け軽量OS等）、
GPU TEEではファームウェアの期待値管理とTCB Recovery追随が攻撃面を抑える要点となる。

出所：M. Bursell, ”Trust in Computer Systems and the Cloud”, Wiley（2021）等を参考に作成

暗号化オーバーヘッドの発生源

- 暗号化オーバーヘッドは4要因に大別され、特に「CPU-GPU間のバウンスバッファ転送」が最大のボトルネック。
- 「回数依存の固定コスト（境界遷移）」はバッチ化・常駐化で、「データ量依存の比例コスト（転送）」はTEE-I/O等のハードウェア化で削るのが基本戦略。



① 境界の遷移（回数比例の固定コスト）
VM Exit／OCALL等の保護環境／非保護環境の切り替えと検証。
I/O・割込み・syscallが多いワークロードほど累積する

② アドレス変換・整合性チェック（ほぼゼロ）
RMP／Secure EPTの所有権照合。ページ単位で行われ、
結果はTLBにキャッシュされるため追加コストはほぼゼロ

③ メモリバス暗号化（データ量比例）
メモリコントローラのAES-XTS暗号化・復号。
ハードウェア実装で通常は数%以下に収まる

④ CPU-GPU転送（データ量比例・最大の発生源）
共有用領域（バウンスバッファ）への暗号化コピーが転送量に比例して発生する。
TEE-I/Oではハードウェア化され大幅削減

コストの2分類
固定コスト（①）＝回数比例 → バッチ化・常駐化で対策
比例コスト（③④）＝データ量比例 → ハードウェア化・転送削減で対策

出所：NVIDIA, Secure AI with Blackwell and Hopper GPUs、Confidential Computing on NVIDIA Hopper GPUs: A Performance Benchmark Study（arXiv:2409.03992）等を基に作成

日本総研 The Japan Research Institute, Limited

ワークロード別のTEE性能影響の傾向

- TEEの性能影響は一律ではなく、CPU演算・メモリ処理では「ほぼゼロ」だが、ストレージI/OやCPU-GPU間転送では顕著な低下が生じる。
- システム設計時はアプリケーションのI/O・通信プロファイルに即した評価が不可欠となる。

ワークロード	影響傾向	公表値・主要メカニズム
CPU演算集約	ほぼ同等	sysbench等でNative比ほぼ同等（オーバーヘッドは数%未満）
メモリ帯域	概ね同等	メモリ暗号化回路（AES-XTS等）のハードウェア処理により影響は軽微
ストレージI/O（書込み）	低下	暗号化処理およびI/O操作に伴う境界遷移（hypercall）の累積によるもの
Webサーバ（小レスポンス多数）	低下	高頻度なコンテキストスイッチ（境界遷移・割り込み）の固定コストが支配的
GPU推論（計算部分）	小さい	LLM推論等のGPU内で完結する計算はNative比数%未満（<5%）
GPU推論（データ転送）	低下	バウンスバッファ（Shared Memory）を経由した暗号化コピーが発生するため
起動・初期化	SGXで大	TEE構築・メモリページ検証に伴う初期化コスト（※常駐化により対応可能）

（参考）公式・公表値：NVIDIAはH100 CCのLLM推論スループットへの影響を概ね数%（＜5%）と説明。独立ベンチマーク（arXiv:2409.03992）でも大半のクエリで5%未満・大型モデルではほぼゼロで、主因はCPU-GPU転送と報告されている。
影響はワークロードの通信・I/Oプロファイルに依存するため「TEEは一律○%遅い」という一般化は困難

出所：NVIDIA公表資料／Confidential Computing on NVIDIA Hopper GPUs: A Performance Benchmark Study（arXiv:2409.03992）／実機での検証等を基に作成

CUDA Graphs等を用いた最適化余地(理論)

- CUDA Graphsは、複数のGPU処理をグラフとして記録・再実行することで、CPU側のカーネル起動時のオーバーヘッドを削減する。
- TEE環境でもCPU側の処理負荷や待ち時間の削減が期待できるが、その効果はワークロードや実装方式に依存する。

CUDA Graphsによる削減

カーネル起動ごとのオーバーヘッド

- 従来方式では、カーネルごとにCPU側で起動準備と投入処理が発生する。
- 小規模なカーネルを多数実行する処理では、この起動コストが処理時間に占める割合が大きくなる。

CUDA Graphsによる削減メカニズム

- 多数のカーネル起動列を1つのグラフとして記録し、以降は1回の投入で一括実行(launch回数を削減)。
- カーネルごとのCPU処理を削減し、CPU側の起動オーバーヘッドとGPUの待機時間を抑制。

適用要件

- 入力テンソルの形状(Tensor Shape)や実行フローが固定(静的)であること。
- 動的バッチ適用時はパディングや個別グラフ構築(Re-capture)等の実装が必要。

その他の最適化余地

- **転送の集約**:ピン留めメモリ、バッチ化、非同期転送により、CPU・GPU間の転送回数と待ち時間を削減。
- **演算融合**:カーネル数自体を減らし、起動オーバーヘッドを圧縮。
- **推論サーバの常駐化**:モデルロード・初期化・アテステーションの一回コストをセッション間で共有。

出所: NVIDIA, CUDA Programming Guide - CUDA Graphs

TEE選択の判断軸

- 保護単位・TCBサイズ・性能・移植コスト・エコシステム成熟度・規制要件・運用体制の観点で、ユースケースに合わせて選ぶことが望ましい。
- 無改修での移植性と汎用性の高さから、大半のユースケースではCVM（またはCVM＋GPU TEE）が選択肢（標準）となると思料。

判断軸	問い	指針
保護単位	何を保護境界に入れるか	プロセス単体（SGX）／ 仮想マシン全体（CVM）／ GPU組み合わせ
TCBとセキュリティ	最小TCBが必須か	鍵管理・高機密の小規模処理はSGX。一般的な汎用ユースケースはCVMを選択
性能	I/O・転送・小リクエストは多いか	汎用処理はCVM。I/O・転送高負荷時はバッチ化・常駐化を前提に事前評価
移植コスト	既存アプリを無改修で動かすか	無改修ならCVM系が必須。SGXはSDK移植またはLibOSの適用が前提
エコシステム成熟度	商用サポート・運用ツールはあるか	CVM＋H100 CC構成がクラウド事業者の商用実績・サポートで先行
規制・監査要件	検証可能な証跡が必要か	全構成共通でリモートアテステーション証跡の取得・保存・照合運用が必要
運用体制	TCB Recovery・CRL管理を回せるか	検証基盤とFW更新プロセスの整備が導入の前提条件

出所：Intel、AMD、Arm、NVIDIA各社のTEE仕様・公開資料を基に日本総研が作成

日本総研

The Japan Research Institute, Limited