日本総研
The Japan Research Institute, Limited

①概説・市場動向・戦略編

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

日本総研 The Japan Research Institute, Limited

エグゼクティブサマリ

TEEの概要

- TEE(Trusted Execution Environment)とは、OSやクラウド事業者であっても内部を覗き見ることができない保護環境である。
- ①CPUの機構による物理的な隔離、②メモリの暗号化、③アテステーションによる環境の検証の3要素で構成される。
- 機密データを秘匿したままLLM等のAIモデルで処理する「Confidential AI」を実現する基盤技術としても注目されている。

主要トピック

①Data in Use保護の要件化

- EU DORA法(2025年1月適用)では、「使用中のデータ」を含む暗号化方針の整備が金融機関に要求されている。
- EU AI Actの実施規範でもモデル保護策として言及されているほか、国内のガバメントクラウド調達仕様書でも言及がされている。

②TEEのAI領域への用途拡大

- 元々TEEは生体認証・決済・鍵管理などモバイル向けの認証技術として普及してきた。
- データ活用の進展によりサーバー・クラウド上の処理中のデータ保護へと領域が拡大。
- 2023年のNVIDIA H100(TEE対応GPU)の登場により、AI領域への適用が加速。

③本番フェーズへの移行

- グローバル大企業の75%がTEEの採用に着手(うち本番運用は18%)。
- Apple・Meta・Googleが数十億ユーザー規模の本番運用を開始。
- ミドルウェア等のエコシステムが成熟し、PoCから本番運用へのプロセスが確立。

普及に向けた課題

- 専門人材と判断基準の不足:自社にノウハウや比較基準がなく、技術的な検証・選定が進まない。
- 導入・運用コスト:対応ハードの調達難や実用的パッケージの不足により、導入・運用コストが増大。
- ガイドラインの未整備:明確な法解釈やガイドラインがなく、コンプライアンス上の効果が不明瞭。

展望と推奨アクション

短期(1～2年)
要件把握・初期対応
規制動向を踏まえた機密データの棚卸しを行い、実証実験(PoC)による初期検証に着手する。

中期(3～5年)
ガバナンス確立・事業化
技術的証明に基づくガバナンスを確立し、データを秘匿したまま掛け合わせる連携事業を創出する。

長期(～10年)
普及・安定運用
全データ処理での保護を標準前提とし、業界横断のセキュアなデータ連携基盤の安定運用を実現する。

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（本書）	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	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

ご監修

- 本シリーズは、情報セキュリティ大学院大学 須崎教授のご監修のもと作成している。

須崎有康
情報セキュリティ大学院大学 教授
プライバシーテック協会 アドバイザー
TCG Invited Expert

主な研究業績

1. Kenichiro Muto and Kuniyasu Suzaki, What Enables Trust in IMA-Based Remote Attestation for CVMs?, The International Conference on Availability, Reliability and Security (ARES), 2026.
2. Kuniyasu Suzaki, Kenta Nakajima, Tsukasa Oi, and Akira Tsukamoto, TS-Perf: General Performance Measurement of Trusted Execution Environment and Rich Execution Environment on Intel SGX, Arm TrustZone, and RISC-V Keystone, IEEE Access , 2021.
3. Kuniyasu Suzaki, Akira Tsukamoto, Andy Green, Mohammad Mannan, Reboot-Oriented IoT: Life Cycle Management in Trusted Execution Environment for Disposable IoT devices, Annual Computer Security Applications Conference (ACSAC), 2020.

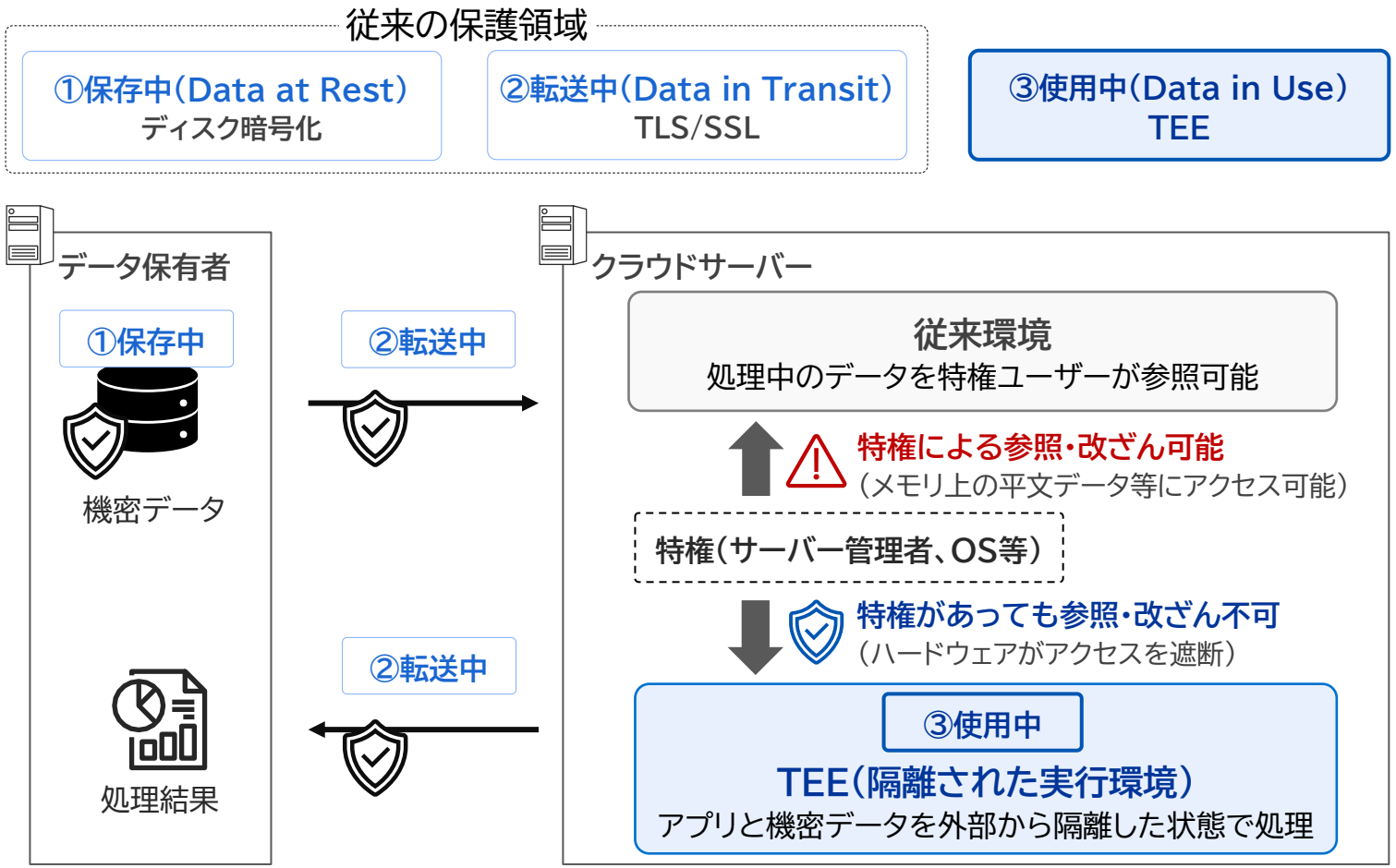
プロフィール

1991年 東京農工大学大学院博士後期課程中退。同年、通商産業省工業技術院電子技術総合研究所に入所。1997-8年 オーストラリア国立大学の客員研究員。2001年 改組により国立研究開発法人産業技術総合研究所。2001年 イリノイ大学アーバナ・シャンペーン校の客員研究員。2009年 東京大学より博士（情報理工学）。2022年9月より本学教授。情報処理学会、電子情報通信学会、IEEE各会員。2010年IPA日本OSS貢献者賞。2025年 TCG Award

観点	コメント
レポートの難易度	本シリーズはTEEを「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部で扱ったものです。①は、概説から規制・市場・事例を中心に、経営者やITに携わる人が読み通せる内容になっています。一方で、②詳細解説＜仕組み・理論＞編・③実践・技術検証編は、実際にTEEの適用を検討する技術者が読むべき水準まで踏み込んでおり、幅広い読み手を意識した構成になっています。
TEEをビジネス活用するにあたってのアドバイス	TEEは、保存中・転送中に続く「使用中（Data in Use）」のデータ保護を実現する重要な技術です。一方で、ルートオブトラスト（信頼の起点、RoT）から積み上げるシステム全体の信頼の連鎖やアテステーションの検証は複雑であり、「何を信頼し、何を検証し、何を運用で補うか」という適切な信頼設計が求められます。 正しく実装・運用するための基礎を習得することが必要です。
TEEの展望	EUのDORA・AI法や国内の改正個人情報保護法など、データ保護への規制要請が高まり、AIが普及した現代において、TEEはデータを保護する中核技術の一つとして、今後ますます重要な役割を担うと考えます。本シリーズを出発点に、最新動向を継続的に追いかけながら活用を進めていくことを期待します。

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

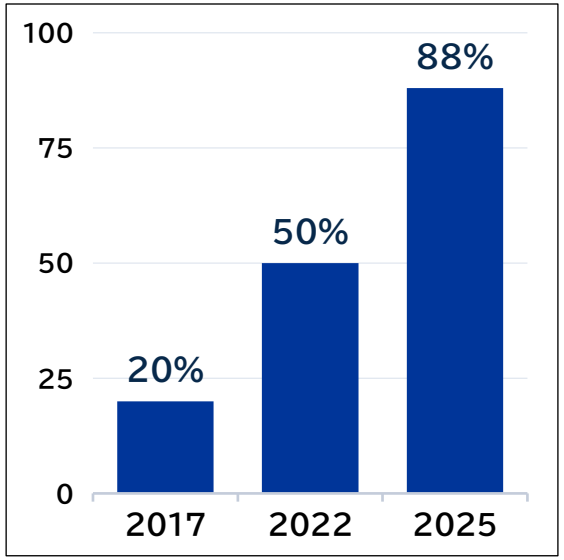
- クラウド上で提供されている外部AIモデル・サービスを使用して顧客情報を処理する。
- 運用者やデータ提供者がデータを覗き見できない仕組みを構築し、技術的な安全性の担保によって企業間でデータを連携・分析処理し、新たな知見を得る。
- クラウド使用時の漏洩リスクを下げることにより審査を短縮し、データ活用を加速させる。

AI・データ利活用における機密データ保護のジレンマ

- 生成AIの普及によりAI・データ利活用が急進する一方、データ保護規制やプライバシー保護への懸念から「機密データを活用できない」ジレンマが生じている。
- この活用と保護のギャップを埋め、データを守りながら使う技術として、「PETs（プライバシー強化技術）」への期待が高まっている。

AI活用の進展

- **導入の標準化：**
  企業の88%が1業務以上でAIを定常的に利用（前年78%）。生成AIは約3年で世界人口の53%に普及している。
- **投資の本格化：**
  世界の企業AI投資額は5,817億ドル（前年比+130%）に達し、生成AIおよびAIエージェントの領域がその中心を占める。



企業のAI導入率（1業務以上で定常利用）

データ保護の要請強化

- 保護法は172の国・地域へ拡大（世界人口の約8割）。GDPR累計制裁金は71億ユーロに達し、執行が本格化。
- 生体・要配慮情報など機微データの規制が強化。日本でも令和8年改正により課徴金・生体情報規律を導入。
- 企業の64%が生成AIへの入力による機密情報漏洩を懸念しており、モデルの学習や共有に活用できないデータが拡大している。
- 消費者の50%がAIに懸念。33%はデータの扱いを理由に利用企業を変更している。

両者のギャップを埋める技術として、PETs（ Privacy Enhancing Technologies、プライバシー強化技術）が注目されている

代表的なPETs：秘密計算・TEE　合成データ　連合学習　匿名加工・仮名化　差分プライバシー

出所：Stanford HAI「AI Index Report 2025」、McKinsey「The State of AI（2025年）」、Cisco「Global AI Readiness Index」

EU規制・ガイドラインのセキュリティ要件におけるTEEの位置づけ

- EU DORA法、EU AI Actの両規定において、TEEの使用は明文化されていないものの、使用中データの保護をはじめとした規定を満たすための現実解として位置づけられる。
- 実際にAI Act実施規範では、モデルパラメータの保護策としてTEEを名指しで例示している。

規制・ガイドライン	領域・対象	要求内容（青字：該当箇所）	TEEの位置づけ
DORA（デジタルオペレーショナルレジリエンス法）	金融	従来の主な暗号化対象であった保存中・転送中データに加え、「使用中データ（Data in Use）」の暗号化・保護方針の整備を要求 （ICTリスク管理RTS＝委任規則（EU） 2024/1774 第6条（暗号化ポリシー）・第7条（鍵管理））	○ 「TEE」の指定はないが、要求を満たすほぼ唯一の現実的な実装手段
		委託先ICTサービスの監査・検査・検証可能性の確保を要求 （本則＝規則（EU） 2022/2554 第28～30条（ICT第三者リスク管理・契約必須条項））	△ TEEの一要素であるアテステーション※が実行環境の安全性を客観的に示す説明手段の一つ
EU AI Act（EU人工知能法）	AI	学習・テストデータの管理と機密性、追跡可能性・説明責任、サイバー攻撃への耐性を高リスクAIに要求 規則（EU） 2024/1689 第10条（データガバナンス）・第13条（透明性）・第15条（正確性・堅牢性・サイバーセキュリティ）	△ TEEは機密性・説明責任・堅牢性を満たす実装手段の一つ
EU AI Act 実施規範		システミックリスクを持つ汎用AIのモデルパラメータ保護策として「使用中のパラメータの保護＝アテステーション付きTEE等のConfidential Computing（以下CC）技術の展開」を例示 GPAI向け行動規範 Safety & Security章	◎ 規制関連文書が保護策としてTEE/Confidential Computingを明記

※処理環境が安全で改ざんされていないことを、技術的・客観的に証明する仕組み。詳細はp.14参照

出所：EU「Digital Operational Resilience Act （DORA）（Regulation （EU） 2022/2554）」、EU「EU AI Act（Regulation （EU） 2024/1689）」、EU「Cyber Resilience Act （CRA）（Regulation （EU） 2024/2847）」、IDC「Unlocking the Future of Data Security」（2025年11月）等を基に日本総研作成

国内規制・ガイドラインのセキュリティ要件におけるTEEの位置づけ

- 国内での検討はEUより遅れており、2026年8月時点ではTEEを直接対象とする法的規制はもとより、使用中データの制度的な保護義務すら存在しない。
- しかし、実務レベルのガイドラインやクラウド調達要件では先行してTEEへの言及が始まっており、いずれ全般的な法規制や統一基準へ波及していくと考えられる。

規制・ガイドライン	領域・対象	関連する要求内容（青字：該当箇所）	TEEの位置づけ
個人情報保護法	個人情報	「高度な暗号化」等がなされている場合、漏えい報告・本人通知を免除 （施行規則7条）	△　「高度な暗号化」の実装手段の一つ
個人情報保護法 （令和8年改正）	個人情報	統計作成・AI開発目的に限り同意なき第三者提供等を許容する際の担保要件。 （施行（公布から2年以内）までに政令・GLで具体化） （新30条の2等）	△　「統計にのみ利用」の技術的担保としてTEEの位置づけが決まり得る
金融庁サイバーセキュリティGL（2024.10）/ FISC安全対策基準（第12版）	金融	重要データの保存・通信時の暗号化、データライフサイクル管理を要求 （FISC 実務基準3・4等） 委託先・再委託先の安全対策実施状況の監査・モニタリングを要求 （FISC監査基準【監1】（システム監査体制・実施）等）	△　委託先監査・モニタリングの実装手段の一つ 使用中の保護の要求がないためTEEの記載も無し
3省2ガイドライン（厚労省医療情報GL v6.0／経産・総務省GL）	医療	保存・通信の暗号化、外部委託・クラウド利用時の安全管理を要求 （システム運用編 6.9 技術的安全管理対策／企画管理編 6.4 外部委託等）	△　委託先監査・モニタリングの実装手段の一つ 使用中の保護の要求がないためTEEの記載も無し
ガバメントクラウドCSP調達技術要件	政府・公共	暗号化・分離された仮想マシンおよび、信頼済みコードのみがアクセス可能なハードウェア隔離環境（TEE）を要求 （項番25・26「機密コンピューティング環境」）	○　クラウド調達スペックとして国内で先駆けて使用中保護要件を組み込んだ例。ただし、利用自体は任意であり、制度的な利用義務化には至っていない
重要情報を扱うシステムの要求策定ガイド（IPA）	産業横断	自律性の確保のため計算途上のデータ暗号化の確保を要求 （2.2自律性確保のための要求項目一覧）	○　データ連携のパターンの一つとして「特殊なハードウェア機能」（≒TEE）の使用が明記。ただし、法的規制・義務ではない

出所：個人情報保護委員会「個人情報保護法」、金融庁「金融分野におけるサイバーセキュリティに関するガイドライン（2024年10月）」、金融情報システムセンター「FISC安全対策基準（第12版）」、厚生労働省「医療情報システムの安全管理に関するガイドライン 第6.0版」、デジタル庁「ガバメントクラウド標準仕様書」、IPA「重要情報を扱うシステムの要求策定ガイド」等を基に日本総研作成

米国における経営戦略としてのTEE実装

- 米国に使用中データの保護の直接的な法的義務はなく、法整備も州単位が中心であるなど、EUのような包括的な規制環境ではない。
- それでも米国Big Techはプライバシーを「競争優位性の源泉」として自社サービスに自発的にTEEを組み込んでおり、近いうちにこれら先端企業のアーキテクチャがデファクトスタンダードになると考えられる。

TEEが組み込まれた各社のConfidential AIサービス

Apple社－Private Cloud Compute（PCC）

Apple Intelligenceのクラウド推論基盤。プログラムを完全に外部公開し、本当に安全かをいつでも検証できる透明性を確保。

“ … personal user data sent to PCC isn’t accessible to anyone other than the user – not even to Apple. ”

出所：Apple.「Private Cloud Compute Security Guide」（参照 2026-08-10）.

Google社－Private AI Compute

Geminiの処理を「スマホの端末内（オンデバイス）と同等」のプライバシー保護で提供。処理が終了した瞬間にデータをサーバー内から削除する「短命化（エフェメラル）設計」を採用。

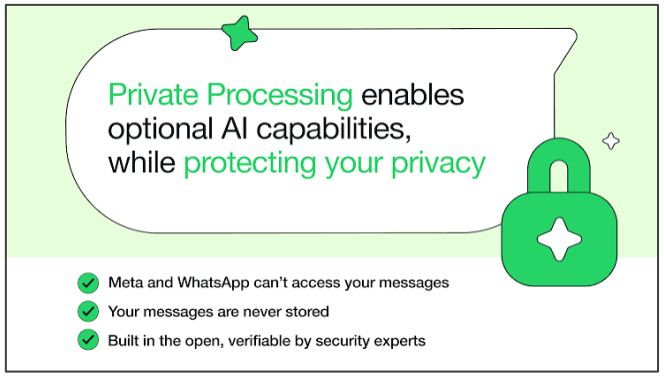
“ … ensuring your personal data stays private to you and is not accessible to anyone else, not even Google. ”

出所：Google.「Private AI Compute: our next step in building private and helpful AI」（参照 2026-08-10）.

Meta社－WhatsApp Private Processing

メッセージ要約等のAI処理を、Meta自身にも見えない形で提供。外部の専門機関による厳格な監査をパスし、結果を公表している。

“ … no one except you and the people you’re talking to can access or share your personal messages, not even Meta or WhatsApp. ”



出所：Meta.「Building Private Processing for AI tools on WhatsApp」（参照 2026-08-10）.

AI時代のデータ活用と保護を両立する「TEE」の台頭

- AIによる機密データ保護の需要が高まる中、規制と市場の両面からTEEの採用が推進されている。
- 技術の周辺環境も整い、概念実証から実導入のフェーズへと移行している。

背景①　機密データ利用需要(p.6)

- 企業におけるAI活用の主流化に伴い、価値の高い機密データをクラウド上のAIで処理・活用する需要が急増。
- 一方で、漏洩への懸念から企業が機密データの外部提供に慎重になっており、活用しきれない課題が生じている。

背景②　規制主導(p.7,8)

- DORA法やAI Act等で「使用中データ」の暗号化やモデルパラメータの保護を要求。
- これらの高度な要件を満たすための実効性の確保が急務となっている。

背景③　技術主導(p.9)

- Apple、Google、Meta等がプライバシー保護を「競争優位の源泉」とし強固な保護を実現したアーキテクチャを実装。
- 数十億ユーザー規模での本番採用により、これらのアーキテクチャがデファクトになりつつある。

一連の課題・要件に応える最適解：TEE

TEEの実導入を後押しする環境変化

インフラの進化

CPU TEEの進化による汎用処理の保護に加え、GPU TEEの商用化(Azure、GCP等)により高度なAIワークロードまで保護範囲が拡大している。

導入ハードルの低下

ミドルウェアや各種サービスが充実し、既存システムの大幅な改修が不要に。新規システムの構築も低コストかつ迅速に実現可能となっている。

市場フェーズの移行

Gartnerが2026年の戦略的トレンドに選出。市場は「概念実証(PoC)」から「本番環境への導入」フェーズへと移行。

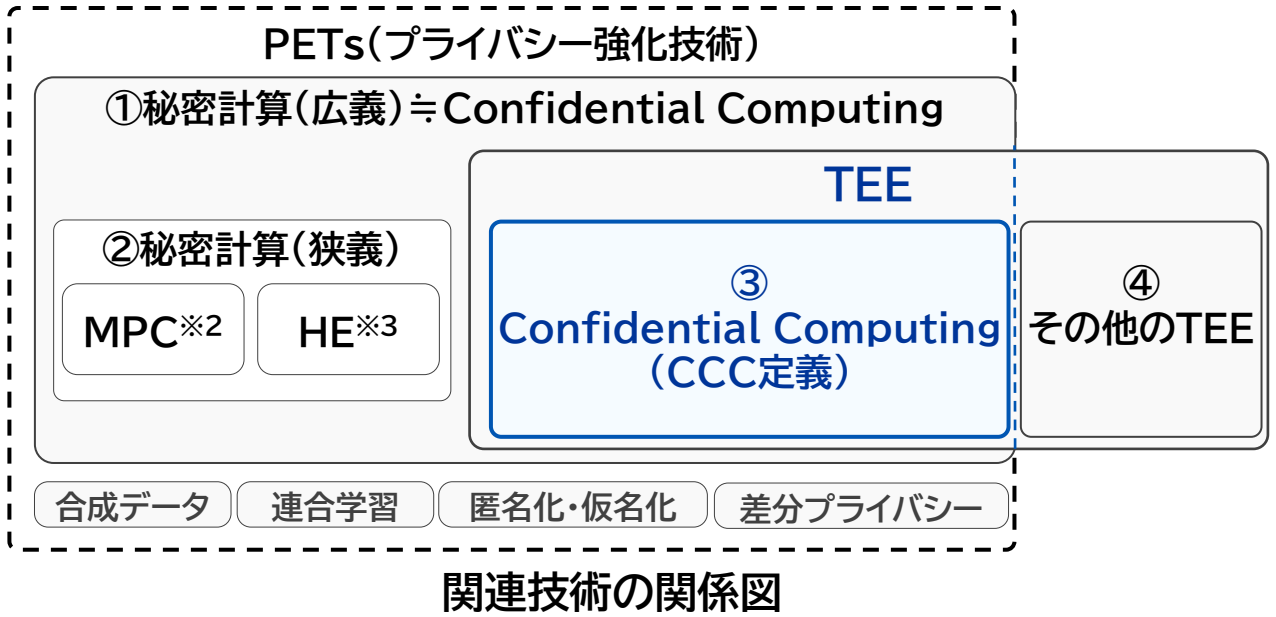
出所：Gartner「Gartner Top 10 Strategic Technology Trends for 2026」(2025年10月)

（参考）「Confidential Computing」等の関連用語との関係

- Confidential Computing（CC）とは、TEE等を利用して処理中のデータを保護した状態で実行する技術カテゴリ。
- 中でも業界団体のCCC（Confidential Computing Consortium）は、ハードウェアベースのTEE内で演算を行うものに限定して定義しており、この定義においてTEEはConfidential Computingの唯一の実現手段である。

CCCによるConfidential Computingの定義

- 「**ハードウェアベースの認証済み**※1**の信頼できる実行環境（TEE）**内で計算を実行することにより、使用中のデータを保護する技術」
- 提供する3つの性質：データの機密性／データの完全性／コードの完全性
- クラウド事業者やOS管理者であっても、TEE内のデータ・コードにアクセスできない



関連技術の関係図

① 秘匿したまま処理する技術の総称。TEEを用いたものを「ハードウェア型の秘密計算」として含む。

② 暗号ベースの秘密計算のみを指す。この定義においてTEEを用いた「ハードウェア型のConfidential Computing」は含まれない。

③ TEEのうち、アテステーションを伴い、使用中データの保護に用いるもの。**本シリーズの対象**

> **派生・注目領域**
> 中でも、LLM等の**AIモデルの安全な活用に特化したもの**を**「Confidential AI」**と呼ぶ

④ TEEのうち、モバイルDRM・鍵管理・生体認証といったPETsに含まれない用途に用いるもの。

※1 初期のCCCのホワイトペーパーにはattestability（構成証明可能性）はオプションの性質であったが、2022年の定義改定で”hardware-based, **attested** TEE”と、定義の必須要素となっている
※2 MPC：Multi-Party Computation（マルチパーティ計算） ※3 HE：Homomorphic Encryption（準同型暗号）

（参考）Confidential Computing以前のTEE

- Confidential Computing以前のTEEは、主に暗号鍵・生体情報・コンテンツ・決済情報を対象にした「小規模で静的なデータの保管・照合」が主な用途。
- スマートフォン等でTEEが活用される中で技術が成熟し、現在では「大規模なデータの高度な処理」へと用途が拡張されている。

①　初期の用途：セキュアエレメントとTPM（2000年代前半～）

- 基本コンセプト：小さな隔離領域に秘密情報を閉じ込める
  適用先：SIMカードや銀行ICカードのセキュアエレメント
- PC向けTPM：起動プロセスの検証と、BitLocker等の暗号鍵の安全な保管

主に「小規模・静的なデータの保管庫」として機能し、ハードウェアトラストの土台を形成

②　モバイルへの普及：Arm TrustZone等（2004年頃～）

- 生体・決済情報の保護：指紋・顔データの照合やモバイル決済の資格情報をメインOSから隔離
- コンテンツ保護（DRM）：動画配信の暗号鍵とHDの再生権限をTEE内で厳密に管理

身近なデバイスで、TEEによる機密データの保護が標準的な技術として浸透

③　隔離環境の強化：Apple Secure Enclave等（2013年～）

- 専用プロセッサへの隔離：Apple Secure Enclaveにおいて、Touch ID／Face IDの照合とパスコード処理をメインCPUから物理的に分離（SEP）
- 物理的な防御の強化：ハードウェアレベルでの試行回数制限総当たり攻撃を物理的に阻止

「管理者（Apple自身）すらデータに触れられない」という徹底的なプライバシー保護を実現

④　サーバー・クラウドへの展開とCCの確立（2015年～現在）

- サーバー向けTEEの登場：Intel SGX等により、データセンターやパブリッククラウド領域へ用途が拡張
- CCC設立（2019年）：業界団体が立ち上がり、「Confidential Computing」の概念が本格的に確立

「静的なデータの保管・照合」から、「クラウド上の大規模データを処理中も保護する」用途へと拡張

日本総研 The Japan Research Institute, Limited

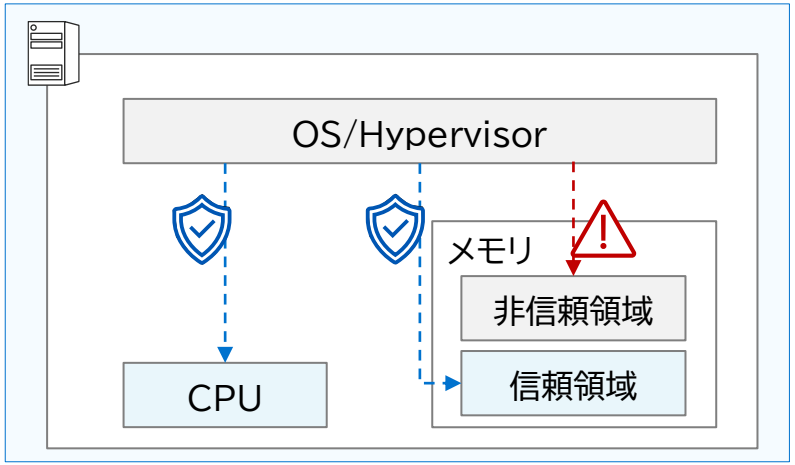
TEEの構成要素

- 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。

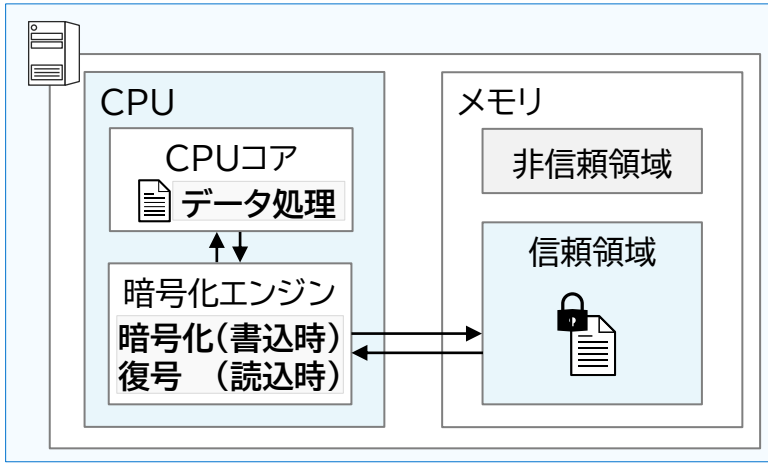
OSのウイルス感染や管理者権限の悪用からも領域内のデータを保護する。



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。

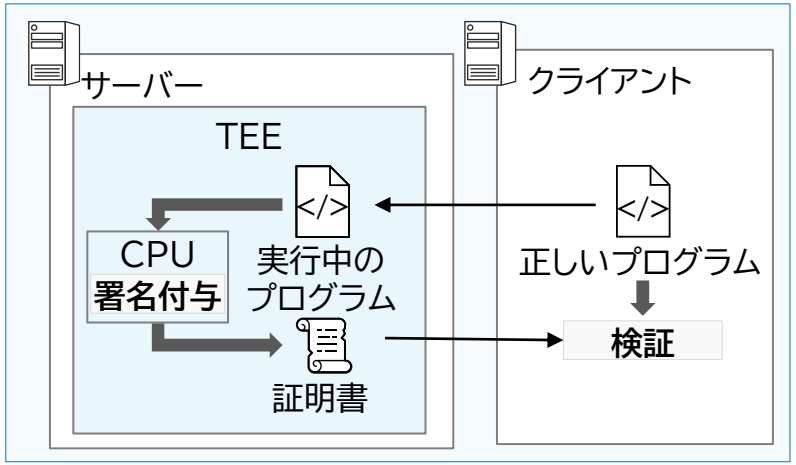
メモリに対する物理的な攻撃に対しても、暗号化により保護する。



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。

出所：Confidential Computing Consortium「A Technical Analysis of Confidential Computing」（v1.3、2022年）、Schneider et al.「SoK: Hardware-Supported Trusted Execution Environments」（2022年）

日本総研 The Japan Research Institute, Limited

（参考）アテステーション（Remote Attestation）

- 「隔離された領域」と「メモリ暗号化」がTEEホスト側（クラウド基盤等）の保護機能であるのに対し、アテステーションは外部の利用者がその安全性をリモートから検証するための仕組みである。
- クラウド事業者に対する安全性を技術的に検証できるこの仕組みが、Confidential AIの重要な基盤である。

事業者への信頼を前提とするクラウド利用

第三者の検証手段無し

クラウド事業者・データ提供先

改ざん参照リスクのある環境

利用者側からリスクが見抜けない

- 外部攻撃によるプログラム改ざん
- クラウド事業者／特権ユーザーによる参照

鍵・機密データの送信

利用者

- 相手のセキュリティ対策や契約内容を暗黙に信頼
- 稼働中の安全性を技術的に裏付ける手段が存在しない

不正な環境への送信や、クラウド事業者によるデータ閲覧のリスクを排除できない

リモートアテステーションによる安全性検証を前提とする利用

チップベンダー検証サービス（Intel/AMD/NVIDIA等）

署名の照会※

クラウド事業者・データ提供先

TEE
証明する側（Attester）

①証明書生成
実行中のコードと初期状態のハッシュ値（計測値）を計測し、CPUの秘密鍵で署名した証明書を生成

②証明書送信

利用者
検証する側（Verifier）

③検証
チップベンダへの照会でCPU署名の正当性を確認した後、計測値が利用者が想定する値と一致するか照合

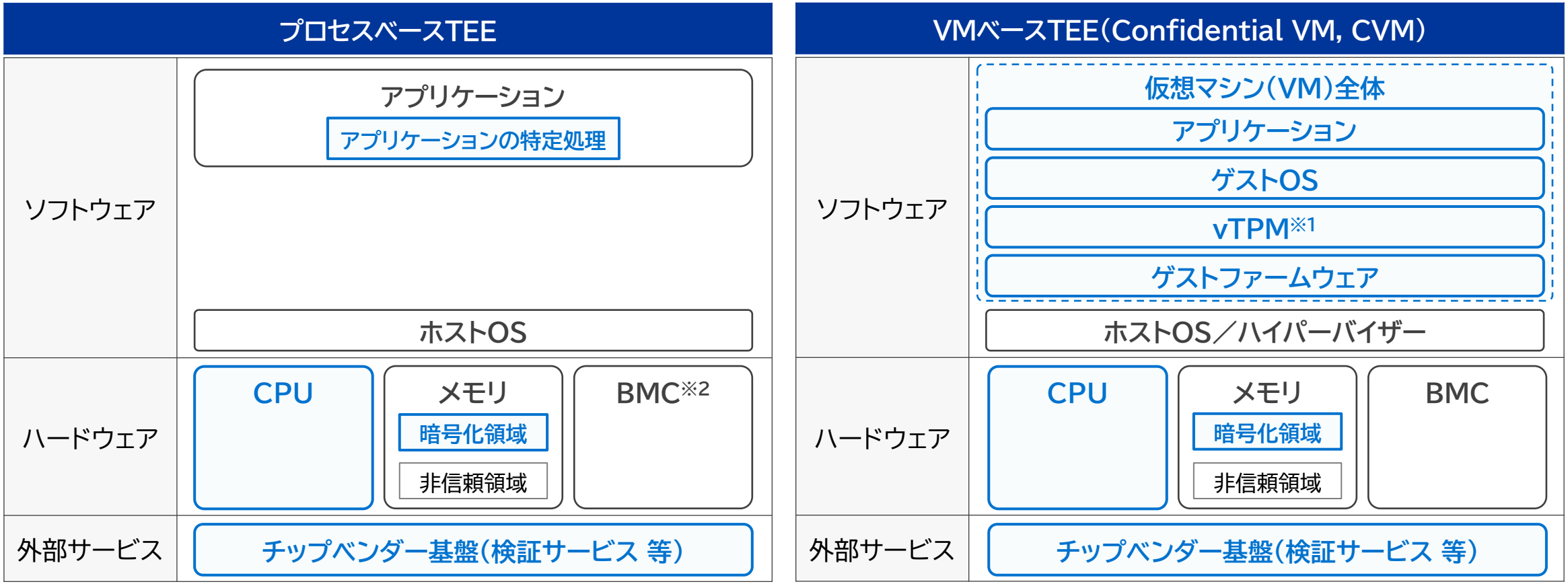
④検証結果に応じた接続制御

✓計測値が期待値と一致　→ この環境に鍵・機密データを渡す
×計測値が期待値と不一致 → 鍵やデータを渡さずに接続を拒否

※ベンダーへの照会はリアルタイム通信のほか、ローカルに保持したキャッシュ情報等を用いたオフライン検証も可能

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。

TEEの主要な実装

- 現在のAI・データ利活用における主流は、既存のアプリを無改修で保護できるVMベースTEE（TDX / SEV-SNP）。
- プロセスベースTEE（SGX）は、暗号鍵管理などTCBを可能な限り小さくすべき用途で利用されている。

技術	ベンダー	保護単位による分類	特徴・採用状況
SGX	Intel	プロセスベースTEE	• 最小のTCBにより、高いセキュリティ水準を実現 • クライアント向けCPU（Coreシリーズ等）でのサポートは2021年末に非推奨となったが、サーバー向けのXeonシリーズでは継続してサポートされている • 暗号鍵管理や小規模な秘匿処理などの用途に用いられる
TDX	Intel	VMベースTEE	• 第4世代Xeon（2023～）より提供開始 • 既存のアプリケーションやOSを改修することなく、保護環境へ移行可能 • AzureやGCPなどの主要クラウドで採用
SEV-SNP	AMD	VMベースTEE	• EPYC Milan（2021年～）より提供開始 • 既存のOSやアプリを改修することなく、そのまま保護環境へ移行可能 • Azure、GCP、AWS等の主要クラウドのConfidential VMで最も広く採用 • NVIDIA H100などのGPU TEEとの組み合わせ実績においても先行

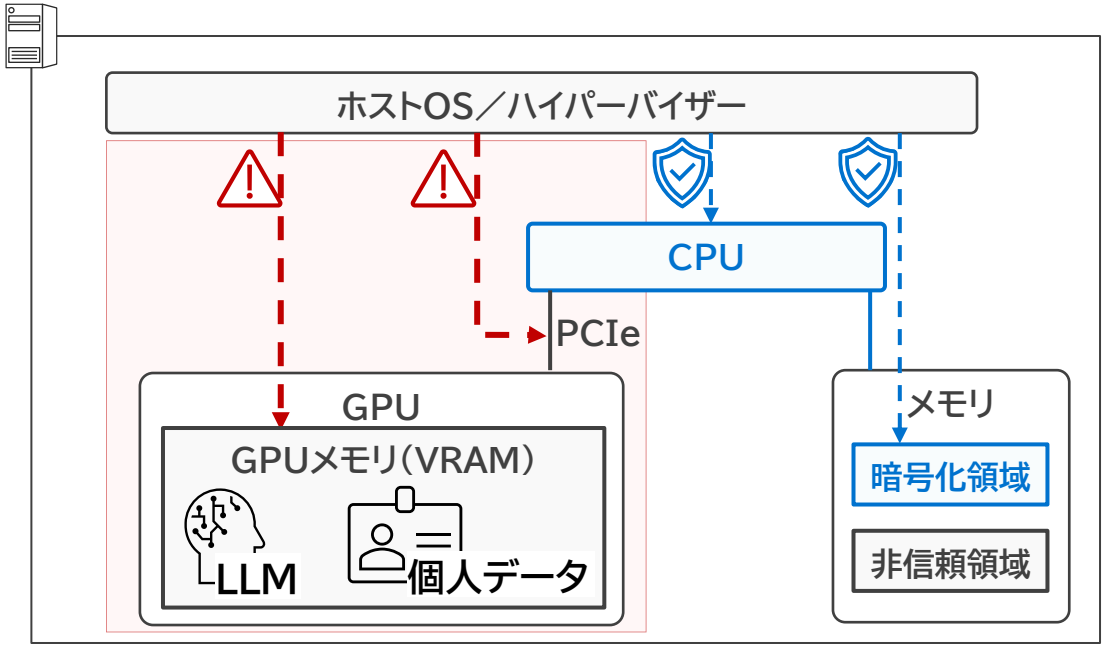
日本総研 The Japan Research Institute, Limited

生成AI活用におけるGPU TEEの必要性

- 生成AI・LLM処理の主軸がGPUへ移行したことで、従来のCPU TEEだけではGPU上のデータやモデルが保護領域外に置かれる。
- GPUまで信頼領域を拡張するGPU TEEを導入することで、AIモデルやモデルへの入力データをエンドツーエンドで保護可能になる。

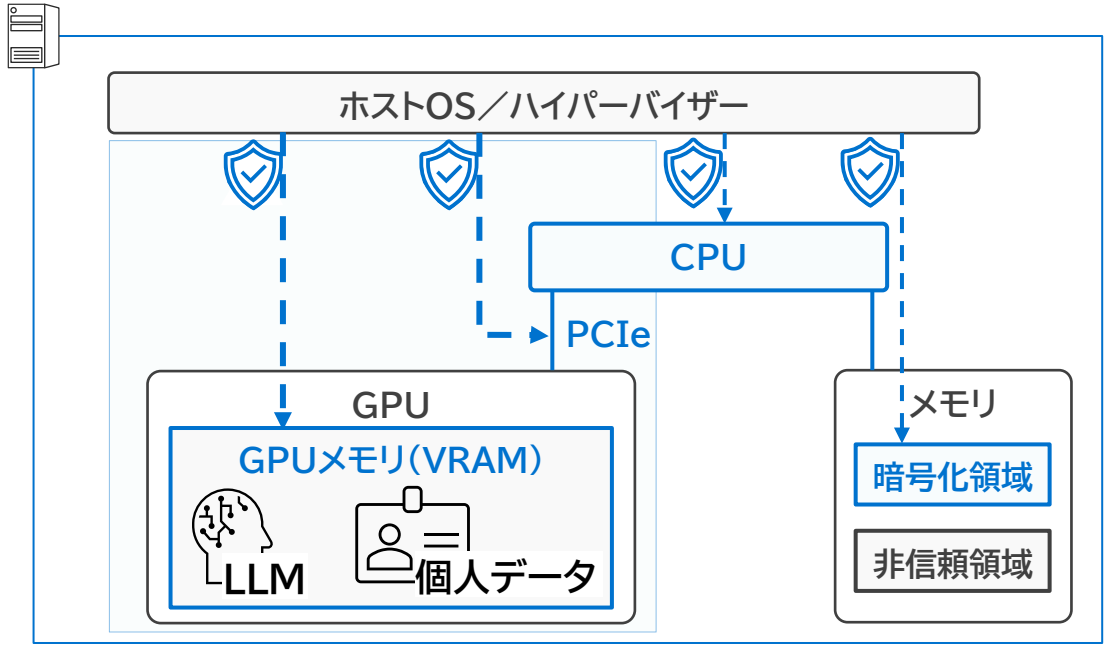
CPU TEEのみ（GPU TEE非対応）

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



NVIDIAにおけるGPU TEEの導入ロードマップ

- GPU TEE市場はNVIDIAが先行しており、GPU単体の保護からサーバーラック全体の保護へと段階的に進展。
- 世代交代に伴いデータ転送時のオーバーヘッドが軽減され、最新世代では超大規模AIの高速処理が想定されている。

世代	対象GPU	保護方式の概要	特徴・採用状況
Hopper （2023年～）	H100 / H200	制御ソフトを介した暗号化	• 業界初の商用GPU TEE機能を搭載 • CPU-GPU間のデータ転送時にオーバーヘッドが発生 • 1台のGPUを分割共有する機能（MIG）とTEEの併用に制限
Blackwell （2025年～）	B100 / B200 / GB200	ハードウェアエンジンによる 直接かつ高速な暗号化	• データ転送時のオーバーヘッドを大幅に解消すると公称 • 既存のAIプログラムを改修せずにそのまま安全に実行可能とされる • MIGとTEEの併用制限が解消され、分割共有時でも個別に暗号保護が可能
Vera Rubin （2026～27年見込み）	NVL72等	サーバーラック内の全GPUと 内部の通信路を一括で暗号化	• 数十台規模のGPUを結合する超大規模AIモデルに対応予定 • 高い安全性を維持したまま大規模処理のパフォーマンス最大化を目指す計画

出所：NVIDIA「Secure AI with Blackwell and Hopper GPUs」（WP-12554-001、2025年8月）、同社発表資料（参照 2026-08-10）

日本総研 The Japan Research Institute, Limited

主要CPUベンダーのGPU TEE対応アプローチ

- GPU TEEの導入には接続するCPU側の対応が不可欠であり、Intel・AMDを中心に標準規格（TDISP等）への対応が進行。
- クラウド基盤で標準化を主導するIntel/AMDに対し、Armはエッジ端末や各種アクセラレータ（NPU/GPU）まで見据えた柔軟な連携を推進。

ベンダ	接続方式・仕様	主な特徴とアプローチ	開発フェーズ・採用状況
AMD	SEV-SNP / SEV-TIO （TDISP準拠）	• 自社でCPU・GPU双方を開発する強みを活かし、一体型チップ（MI300A等）によってCPU-GPU間のオーバーヘッドを最小化 • 標準的なPCIe接続（SEV-TIO）により他社製GPU TEEとの連携にも対応	• SEV-SNPは実用化済み • SEV-TIOはロードマップに基づき初期プレビュー・検証段階
Intel	TDX Connect （TDISP準拠）	• 業界標準団体（PCI-SIG）を主導し、オープンな他社連携を推進 • NVIDIA等のサードパーティ製GPU TEEとの相互運用性を最重視	• 標準規格（TDISP）の策定に合わせた実装および検証が進行中
Arm	Arm CCA 拡張 （アクセラレータ連携）	• モバイル・エッジ機器やオンデバイスAI向けに、省電力・低遅延な接続へ最適化 • CPU領域から機器内部の各種アクセラレータ（NPU/GPU）TEEへ柔軟に接続保護	• 仕様策定およびパートナー企業との共同開発段階 • 富士通の次世代CPU「MONAKA」（2027年予定）等へ実装予定

出所：AMD「SEV-TIO ホワイトペーパー」、Intel「Intel TDX Connect Architecture Specification」、Arm「Arm Confidential Compute Architecture 仕様」、PCI-SIG「TDISP」等を基に日本総研作成

GPU TEE導入における実務課題と対応策

- GPU TEEは生成AI活用における高度なデータ保護を可能とする一方で、CPU/GPUにまたがる複合的な管理や標準規格の未確立により、運用負荷や導入コストが増大する課題が存在する。
- アテステーションの自動化サービスの登場・拡充や業界標準規格への統合が進むことで、これらの実務課題は順次解消に向かうと期待される。

実務課題	具体的な内容・課題の背景	導入・運用における対応策・展望
統合チェックの困難さ	• CPUとGPUを「セット」で同時に検証※する必要があり、片方だけのチェックでは処理全体の安全を保証できない	• 同時に相互検証を行う統合検証システムの構築
特定メーカーへの依存	• 現在主流の技術では、GPUの安全性確認が「CPU側のシステム」に依存する	• CPUとGPUが独立して安全性を証明できる標準設計の登場・標準化待ち
検証データ形式のばらつき	• 安全を証明するデータの形式がメーカーごとに異なるため、マルチベンダー構成時のシステム開発コストが上昇する	• 業界標準規格（TDISP等）への統一による標準化
運用・アップデートの二重化	• OSやドライバ、セキュリティパッチの管理が「CPU用」と「GPU用」の2系統になり、保守・監視の手間が倍増する	• クラウド側が提供するアテステーションの自動化サービス（SaaS等）の活用による運用の省力化

※Composite Attestationと呼ばれる

市場の採用状況－全体と業界別・国別の内訳

- グローバルの大企業を対象にした調査では、75%がConfidential Computingの採用に着手している。本番運用(全体平均18%)に絞ると、金融(37%)やカナダ(26%)において採用率が高い。
- TEE採用により説明責任の向上に効果を感じている一方で、運用の複雑さや人手不足が共通の課題となっている。

全体で **75%** の組織がConfidential Computingの採用に着手
(パイロット・技術検証: 57% 、本番運用 18%)

▼ 主な業界・国別の本番運用採用率(平均採用率18%)

業界別採用率

① 金融 37%
② 医療 29%
③ 政府 21%

コンプライアンスや監査対応が動機となり、規制業種において先行的に採用

国別採用率

① カナダ 26%
② アメリカ 24%
③ 中国・イギリス 20%

北米が先行して採用。欧州は厳格なデータ規制環境があるにもかかわらず本番導入は遅行

導入によるメリット

- データの完全性の向上(88%)
- 技術的裏付けのある機密性(73%)
- 規制対応の改善(68%)

TEEの特徴である「隔離環境による機密性・完全性の担保」と「アテステーションによる技術的証明」が、そのまま導入メリットとして評価されている。

導入時・運用時の課題

- アテステーションによる検証の複雑さ(84%)
- 「ニッチな技術である」という誤解(77%)
- スキル不足・人材不足(75%)

技術の仕様そのものよりも、運用体制の構築に課題

出所:IDC White Paper (2025年11月) / CCC(2025年12月)
調査におけるConfidential Computingの定義はTEEを用いたハードウェアベースのConfidential Computingのこと

導入効果が大きい業界

- 機微なデータを保有する金融・医療・広告・公共分野において、Confidential Computingによるデータ保護の導入効果が大きい。
- 2024年以降は、通信・コンシューマ向けAI分野での全世界のユーザーを対象にした導入が本格化し、市場が急拡大している。

業界	主なユースケース	動向
金融	• AML(マネーロンダリング対策)の共同分析 • 与信・不正検知におけるAI推論	• 本番採用率37%と全業界で最も先行 • 金融サイバーレジリエンス法(DORA)対応が追い風
医療・ヘルスケア	• 複数病院間でのセキュアなデータ連携 • 創薬・臨床研究の共同分析 • 機密性の高いゲノム解析	• 多者間データ連携の優先度が78%と突出(IDC調べ) • 厳格な医療データ規制(HIPAA等)との整合性が主因
広告・小売	• データクリーンルーム※を用いた顧客データ連携・広告効果測定 • IoT・POS等のコネクテッド製品の保護	• 3rd Party Cookie制限後の「1st Partyデータ連携基盤」として普及期へ • EU CRA(2027年本格適用)により、小売・メーカーにデジタル製品のセキュリティ要件が課され、組込みTEE(TrustZone等)と接点
公共・防衛	• 機微な国家・市民データのクラウド処理 • データ主権(Data Sovereignty)対応	• ソブリンクラウド要件や政府調達において「使用中の保護」が論点化 • 先行事例:イスラエル国防省におけるCC基盤の採用
通信・コンシューマ向けAI	• メッセージングAIや端末連携AIにおけるプライバシー保護	• Apple・Meta・Google等が本番適用済み(2024-2025年) • 「プライベートAI」における標準的なアーキテクチャの型へ

※データクリーンルームとは企業間で安全にデータを共有・処理する環境の総称。実装や仕様はサービスによって異なる。

出所:IDC「Unlocking the Future of Data Security」(2025年11月)、各社公表資料(参照 2026-08-10)

業界団体と標準化の動き

- Confidential Computingの定義から、ハードウェア間の通信仕様、デバイス認証に至るまで、多数の団体が関与している。
- 各レイヤーでの標準化が進むことでベンダー間の互換性・連携性が高まり、ユーザー企業が容易に導入できるエコシステムが形成されつつある。

団体	参画プロセス	概要	主な活動・成果物
CCC	概念定義・エコシステム形成	Linux Foundation傘下の業界横断コンソーシアム（2019年設立） **参画：Intel, AMD, NVIDIA, Arm, Microsoft, Google 等**	• Confidential Computingの定義策定 • OSS育成（Gramine, Occlum, Veraison等） • 市場調査・普及啓発
IETF RATS WG	通信・接続の標準化	インターネット技術の標準化機関（IETF）における、アテステーション作業部会 **主導：Cisco, Microsoft 等**	• リモートアテステーションのアーキテクチャ標準（RFC 9334） • EAT（アテステーション結果のデータフォーマット）
PCI-SIG		PCIe（高速バスインターフェース）の規格策定・標準化団体 **主導：Intel, AMD, NVIDIA, Qualcomm 等**	• IDE（PCIe経路上のデータ通信を保護する暗号化機能の仕様） • TDISP（デバイスをTEEに安全に接続する・割り当てるためのプロトコル・アーキテクチャ） **※次世代GPU TEE（TEE-I/O）の土台となる技術**
DMTF		システムやプラットフォーム管理の標準化団体 **主導：Dell, HPE, Lenovo, Broadcom 等**	• SPDM （ハードウェア間の認証や計測値取得を行う通信プロトコル・データモデル）
TCG	デバイス・認証の基盤仕様	ハードウェアベースの信頼（Trust）に関する仕様を策定する標準化団体 **主導：NVIDIA, Infineon, Microsoft 等**	• TPM 2.0 / DICE **※CVM環境で主流となるvTPMアテステーションの基盤仕様**
GlobalPlatform		モバイル・組込み機器向けセキュアコンポーネントの標準・認証団体。ArmやApple等も関与 **主導：Arm, Trustonic, Qualcomm 等**	• TEEに関する仕様（API・保護プロファイル）の策定および認証制度

出所：各団体公式サイト（参照 2026-08-10）、Confidential Computing Consortium「Confidential Computing Consortium White Paper」（2025年）等を基に日本総研作成

エコシステムのレイヤーマップ

- エコシステムは主要な4層の技術レイヤーと、それらを横断的に検証するアテステーションで構成される。
- レイヤー間の統合・相互接続は発展途上のため、現時点では垂直統合されているサービスの利用が現実的である。

アプリケーション／ソリューション

TEEの保護環境を活用し、具体的な機能やSaaSとして価値を提供する

ソリューション:各社のConfidential AI **SaaS/サービス:**データクリーンルーム等の連携サービス

ミドルウェア／ランタイム

既存のアプリを改修せずにTEE上で実行可能にし、下位レイヤーとの連携を仲介する

商用ベンダー: Anjuna, Fortanix **OSS:**CoCo(Confidential Containers), Gramine等

クラウドインフラ

TEEハードウェアを用いた安全な仮想サーバーを、IaaS/PaaSとして提供する

IaaS: Azure CVM/AGC, GC Confidential VM, AWS Nitro, OCI

TEEハードウェア

物理的なCPU/GPUレベルで隔離実行環境を生成し、信頼の起点を担保する

アーキテクチャ: Intel TDX, AMD SEV-SNP, Arm CCA, NVIDIA H100 CC等

アテステーション

各レイヤーの実行環境を横断的に検証し、安全性が証明された環境にのみ暗号鍵を払い出す

①証明データ生成 TEEハードウェア

▼

②証明データ収集 ミドルウェア／ランタイム

▼

③正当性の検証 検証サービス

▼

④鍵取得 アプリケーション

検証サービス
Microsoft Azure Attestation(MAA),
Intel Trust Authority(ITA)等

日本総研 The Japan Research Institute, Limited

クラウドインフラ3社の提供サービス

- CPU TEE（CVM）は大手3社で標準機能として定着が進む一方、GPU TEEの提供はAzureが先行。
- Google Cloudは独自基盤や連携機能で追随。AWSは独自のNitroアーキテクチャを貫いており、GPU未対応など他のエコシステムとは異なるアプローチを採用。

クラウドベンダ	CPU TEE（シリーズ名）	GPU TEE（シリーズ名）	エコシステム対応（インフラ層以外）	特徴・戦略
Microsoft Azure	• SEV-SNP（DCasv5） • TDX（DCesv5） • SGX（DCsv3）	• SEV-SNP + H100 CC（NCC H100 v5） **一般提供済み**	• MAA **アテステーション** • Azure AI Confidential Inferencing **アプリケーション**	• 対応チップが最も多く、成熟したCC基盤 • 金融や医療など、規制業種における採用実績が多い
Google Cloud	• SEV-SNP（N2D） • TDX（C3）	• TDX + H100（A3） **プレビュー展開**	• Confidential Space **ミドルウェア** • ハードウェア独自TPU TEE（Private AI Compute） **ハードウェア**	• 独自に提供しているミドルウェア（Confidential Space）を活用し、他組織間のセキュアなデータ連携を容易にする
AWS	• Nitro Enclaves 独自アーキテクチャによる設計。信頼の起点がAWSに存在する。	**未提供**	• 独自アテステーション仕様 **アテステーション**	• 「AWSの運用者でもデータにアクセスできない」独自の仕組み（Nitro System）を主張

出所：Microsoft、Google Cloud、Amazon Web Services各社公式ドキュメント（参照 2026-08-10）等を基に日本総研作成

日本総研 The Japan Research Institute, Limited

主要ベンダー・OSS｜ミドルウェア・ランタイム

- ミドルウェア・ランタイムにおいては商用ベンダー3社とOSSが主な選択肢。
- 「アプリ改修なしのTEE化」と「アテステーション・鍵管理の運用の簡略化」が競争軸。

商用ベンダー

Anjuna Security（米国）

Seaglass（ランタイム）
Northstar（統合管理・DCR）

- アプリを改修せずに主要TEE（SGX / TDX / SEV-SNP / GPU CC）に幅広く対応。
- 分散するSeaglass（実行環境）をNorthstar（コンソール）で統合管理する。
- イスラエル国防省や米大手銀行など、厳格なセキュリティが求められる機関で採用されている。

Fortanix（米国）

CCM（ランタイム）
DSM（統合管理）
Armet AI（AI SaaS）

- 既存のアプリを改修せずにTEE環境へ移行でき、CCMでライフサイクルを管理。
- Data Security Manager（DSM）による極めて強固な鍵管理と統合。
- Confidential AIに特化した専用プラットフォーム「Armet AI」を展開。

Edgeless Systems（ドイツ）

Constellation（K8s基盤）
Continuum（AIランタイム）
Privatemode AI（AI SaaS）

- アプリを改修せずにKubernetesクラスタ全体をConfidential化する基盤（Constellation）を提供。
- TEE上でのセキュアなLLM推論SaaS（Privatemode AI）。
- オープンソース志向が強い開発アプローチを採用している。

OSS

- Confidential Containers（CoCo）：Kubernetes上のCVMコンテナ技術
- Gramine：SGX向けの軽量なLibOS※
- Occlum：Ant Group発（CCCへ寄贈済み）のLibOS

採用時の考慮点
商用サポートが存在しないため、トラブルシューティングを含めて、自社で運用できる体制があるかどうかがポイント

LibOS（ライブラリOS）：ファイル操作などのOS機能をライブラリ化してアプリに直接組み込む技術。アプリと保護環境（TEE）を仲介することで、既存アプリのコードを書き換えずにそのまま動かすことが可能。

海外主要ベンダー｜アプリケーション

- 海外（欧米）では特定業界（金融・防衛・ヘルスケア等）の厳格な要件に特化したDCR/PETs専業プレイヤーが先行。
- ミドルウェア層のベンダーもConfidential AI等のアプリケーション領域へ進出している。

Decentriq（スイス）

TEE型データクリーンルーム　（DCR）

- 欧州GDPR適合に特化したTEE型クリーンルーム。
- メディア・広告・ヘルスケア分野でのデータ連携事例が豊富。
- スイス発のプラットフォームとして、防衛・公共機関にも採用されている。

Duality（米国）

ハイブリッド PETs ソリューション（データ連携プラットフォーム）

- 秘密計算（MPC/FHE）とTEEを組み合わせた複合型のプラットフォーム。
- 米国政府機関・国防関連や国際金融での高度な導入実績。
- 国境を越えたデータ分析やマネロン対策に強み。

BeeKeeperAI（米国）

Sightline　（Confidential AI）

- 医療機関とAI開発者を安全に接続するヘルスケア特化型DCR/Confidential AI基盤。
- 患者データを外部に開示することなく、マルチセンターでのAIアルゴリズム検証・学習を実現。
- HIPAA等の厳格な医療プライバシー要件に対応。

Anjuna Securityの「Northstar」、**Fortanix**の「Armet AI」、**Edgeless Systems**の「Privatemode AI」と、ミドルウェアベンダーがアプリケーション領域に進出している。

背景には「CVMがクラウドの標準機能に取り込まれ、ミドルウェア単体では差別化が困難な点」、「生成AIサービスの普及によりConfidential AIの需要が増加している点」があげられる。

出所：Duality、Decentriq、BeeKeeperAI各社公式サイトおよび公表資料（参照 2026-08-10）

国内主要ベンダー｜アプリケーション

- 国内市場ではプライバシー保護・法規制対応を強みとする「専業スタートアップ」と、自社インフラ・技術を持つ「大手IT・通信」がTEEアプリケーションを展開している。
- 単一のアプリケーションだけでなく、暗号基盤やミドルウェアまで垂直統合で提供するソリューションが多い。

Acompany

AutoPrivacy DataCleanRoom（DCR）
Confidential AI Suite（Confidential AI）

- AutoPrivacy：TEE空間上で動作するデータクリーンルーム（DCR）基盤。
- LLM/RAG利用時の機密データ漏洩を防ぐConfidential AI Gateway機能を提供。
- AWS/GCP/Azure/Snowflake間のマルチクラウド環境に対応。

EAGLYS

ALCHEMISTA（データ連携プラットフォーム）
DataArmor（ミドルウェア）

- ALCHEMISTA: マテリアルズ・インフォマティクス（MI）領域に特化し、企業間で機密データやAIモデルを安全に相互利用するデータ連携プラットフォーム。
- DataArmor：準同型暗号 × TEEによる暗号化データの集計・AI解析ミドルウェア。

NEC

秘密計算ソリューション（ソリューションの総称）

- クラウドTEE技術を活用し、複数組織のデータを秘匿したまま統合・集計・分析する実行環境を提供。
- 行政・ヘルスケア・金融等の高度なセキュリティ要求に対応する組織間のデータ連携システムに対応。

NTTデータグループ

析秘TEE（データ連携プラットフォーム）

- TEE領域内で処理を行うため、既存の任意解析ロジックをコーディング変更なしで安全に実行するデータ連携プラットフォーム。
- 金融の不正検知や医療・製造領域等において、組織間での機密データ・ロジックの持ち寄りによる共同分析を支援。

※国内企業は単一のアプリケーションの提供にとどまらず、ミドルウェアやコンサル・運用支援など統合的なソリューションを提供することが多い。

出所：Acompany、EAGLYS、NTTデータグループ、NEC各社公式サイトおよび公表資料（参照 2026-08-10）

TEEを活用する代表的な実装パターン

- 実装は大きく分けて「Confidential AI」、「データクリーンルーム」、「暗号鍵管理」の3つ。
- TEEの活用にあたっては、「保護対象」と「非信頼対象」を明確にし、目的に合致したアーキテクチャを選定することが重要である。

実装パターン	守る対象	疑う相手	概要・特徴	代表的なサービス・企業
Confidential AI				
エンタープライズ向け	• 自社の入力データ • 自社のAIモデル	クラウドインフラ事業者	自社専用のクラウド環境で、機密データを用いたAI推論・学習を安全に実施する	• BeeKeeperAI • Privatemode AI • Azure AI Confidential Inferencing
コンシューマ向け	• 一般消費者の入力データ（写真、チャット文章等）	AIサービス提供事業者	一般消費者のデータをサービス提供者に盗み見されることなく、スマホOS等と連携した高度なクラウドAIを活用する	• Apple PCC • Meta WhatsApp PP • Google PAIC
データクリーンルーム	• 各社が連携する生データ	共同で利用する取引先クラウド事業者	複数組織が互いに生データを開示することなく、共同でデータ分析や機械学習を行う	• GC Confidential Space • Acompany（AutoPrivacy） • Decentriq
双方向秘匿AI推論	• 開発元のAIモデル • 導入側のクエリ	取引相手（AI開発元等）クラウド事業者	AI開発元のモデルと、ユーザー企業の機密データの双方を秘匿したまま推論を実行し、結果のみを得る	• Anjuna Seaglass • Fortanix Armet AI
鍵管理	• 暗号鍵、認証トークン等	内部のシステム管理者 外部のサイバー攻撃者	デジタル資産や社内システムのコアとなる鍵情報を、クラウド上で漏洩しないよう安全に運用・管理する	• Fireblocks • Fortanix DSM

日本総研 The Japan Research Institute, Limited

主な事例一覧

- コンシューマ向けAIでの本番運用から企業間データ連携まで、業界を問わずTEEの導入が本格化している。

分野	導入組織(国・地域)	概要	パターン	段階
AI	Apple(米)	クラウドAI推論時のユーザーデータを保護し、即時破棄・外部監査可能な透明性ログを提供する基盤を稼働	②	本番
AI	Meta(米)	運営元すらユーザーのプロンプトを覗き見できないメッセージAIを、高度なデュアルTEEアーキテクチャで実装	②	本番
AI	Google(米)	Geminiの処理をオンデバイスと同等のプライバシー保護レベルで実行し、データの短命化(エフェメラル処理)を担保	②	本番
SNS	TikTok(中国)	運営元や特定国家からの不正アクセス懸念を払拭するため、TEEによるデータの物理的隔離と監査体制を導入	②	本番
金融	MonetaGo(インド)	複数銀行が顧客データを秘匿したままTEE上でハッシュ値を突合し、貿易金融の二重融資をリアルタイムで検知	③	本番
金融	Swiss Re(スイス)	海上保険の領域において、競争上の懸念から共有が困難な船舶データ等を安全に統合し高度なリスク分析を実現	③	実証
金融	Royal Bank of Canada(カナダ)	銀行と提携事業会社が顧客プライバシーを厳格に担保しつつデータを安全に結合し、高度なマーケティング分析を実施	③	実適用
広告	TransUnion(米)	広告主の顧客データと自社データをTEE上で安全に突合し、プライバシーを保護しつつ高度な広告効果測定を実施	③	実証
広告	高級車ブランド(ドイツ)	Cookieを用いずに自社顧客データを活用してスイスの主要メディアで広告を配信。その際、データを相互に開示せずに照合	③	実適用
医療	iCARE4CVD(欧州)	機密性の高い患者データをTEE上で統合・処理し、プライバシーを保護しながら心血管疾患に関する高度な医療データ分析と予測モデル開発を実行	④	実適用
医療	モアハウス医科大学×ScriptChain Health(米)	心不全患者の臨床データとAIモデルをTEE上で統合し、データとアルゴリズムの双方を秘匿しながら患者発見AIの精度検証を実行	④	実証
医療	PurpleLab(米)	機微な医療リアルワールドデータ(RWE)と他組織のデータを、プライバシー規制を遵守しつつクリーンルームで共同分析	③	実証
製造	三菱ケミカル×大塚化学(日本)	マテリアルズ・インフォマティクスにおいて、互いの機密データ(素材の配合等)を秘匿したまま共同分析し開発を加速	③	実適用
製造	巴川コーポレーション×日立ハイテク(日本)	複数企業にまたがる製造データをTEE上で統合・解析し、品質低下の要因特定と製造条件の最適化を実証	③	実証
防衛	イスラエル国防省(イスラエル)	トップシークレットのAIワークロードや機密データを、セキュリティ要件を満たしたままパブリッククラウドのTEE環境へ安全に移行	①	本番
防衛	米国海軍(U.S. Navy)(米)	外部クラウドの機密GPU環境(TEE)において、軍事機密データを保護したまま独自のAI・LLMワークロードを安全に稼働	①	実証
行政	つくば市(日本)	マイナンバーカードとTEEを用いたインターネット投票を見据え、投票内容の確実な秘匿集計システムを実証	①	実証

(実装)パターン

① Confidential AI (エンタープライズ)
② Confidential AI (コンシューマ)
③ データクリーンルーム
④ 双方向秘匿AI推論

段階

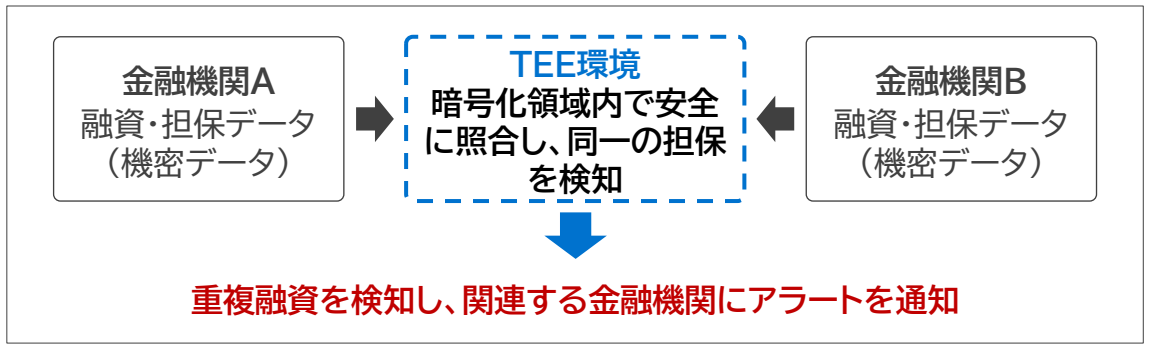
実証 技術検証・PoC ➡ 実適用 パイロット・限定的な利用 ➡ 本番 本番稼働・商用利用

事例詳細：金融

- 高度な機密性が求められる金融領域では、競合する機関同士が顧客の取引情報を秘匿したまま安全に連携し、業界全体をまたぐ不正検知やリスク管理の高度化に活用されている。

貿易金融における二重融資の検知（MonetaGo）

- 機密保護の観点から金融機関同士で生データを直接共有できず、同一の担保を用いた組織横断的な二重融資（重複融資）詐欺の検知が困難。
- MonetaGoはConfidential Computingを採用。各組織のデータを互いに開示せず、暗号化領域内で安全に照合する環境を構築。
- 金融機関ごとの顧客・取引データの機密性を完全に保護したままクロス組織でのデータ分析を実現し、重複融資詐欺を効果的に検知・防止。



出所：AMD.「MonetaGo uses Confidential Computing to detect duplicate financing fraud through secure cross-organization data analysis」（参照 2026-08-10），図は同資料を基に日本総研作成

海運データの安全な分析実証（Swiss Re）

- 海上保険（船舶や貨物など）の精緻なリスク評価や市場ベンチマークの作成には、元受保険会社が持つ詳細な契約データや損害履歴が不可欠。しかし、これらは競争上の機密性が高いビジネスデータであり、再保険会社を含む外部への提供に対するハードルが高い。
- Decentriqのデータクリーンルームを採用し、元受保険会社の「機密なポートフォリオデータ」とSwiss Reの「高度なリスク分析モデル」を連携。互いに生データを一切明かすことなく、完全に暗号化された領域内で安全に集計・分析する環境を構築。
- 元受保険会社は自社の顧客データを外部に漏らすことなく、市場全体とのベンチマーク比較や精確なリスク診断が可能に。Swiss Re側もプライバシーの完全保証によってデータ連携の障壁を取り払い、より最適化された海上再保険プログラムの提供を実現。

出所：Intel.「Intel, Decentriq, and Swiss Re Improve Data Privacy」（参照 2026-08-10）

事例詳細：医療・製薬

- 厳格なプライバシー保護が求められる医療・製薬領域では、各種法規制を遵守しながら組織の壁を越えた臨床データの連携を実現し、生データを開示せずに新薬開発や共同研究を推進する事例が実用化されている。

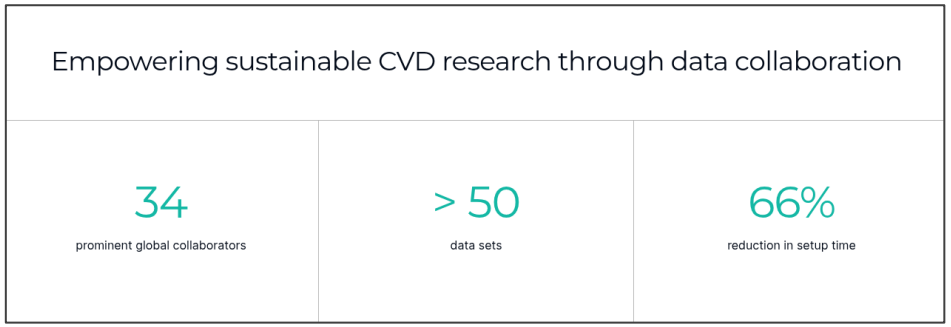
機微なリアルワールドデータの共同分析（PurpleLab）

- 製薬・ライフサイエンス企業において、SNS広告が患者行動に与える影響の測定が長年の課題。HIPAA等の厳格な規制により機微な医療データ（RWE）を外部へ持ち出せず、メディア側も非開示のため直接の紐付けが困難。
- ヘルスケア分析のPurpleLabはDecentriqのTEEを活用したクリーンルームを採用。SNS側の「広告露出データ」と自社の「医療データ（処方・請求）」を、互いに生データを開示せず暗号化領域内で安全に照合・分析する環境を構築。
- 規制を遵守しつつ、業界で初めて「SNS広告接触」と「患者アウトカム（処方変化や受診）」を直接紐付けた効果測定を実現。施策全体のROI可視化を可能にし、主要SNSプラットフォームで導入が進行中。

出所：Decentriq.「PurpleLab and Decentriq close measurement gap in life sciences」（参照 2026-08-10）.

心疾患データの安全な産学データ連携（iCARE4CVD）

- 心疾患の早期診断・個別化治療に向けたAI開発において、30以上の産学機関による100万人規模の医療データ統合が必要な一方、厳格な規制やデータ機密の保護が障壁となっていた。
- iCARE4CVDコンソーシアムはDecentriqを採用。互いに生データを開示せず、暗号化領域内で患者レベルの統合データ分析やAIモデル構築を安全に行える環境を確立。
- プライバシーを完全に保護したまま、パートナー企業のデータ連携・準備時間を66%削減。大規模なデータ集積とAIモデル開発を迅速化し、心疾患の早期発見や最適治療の実現を加速。



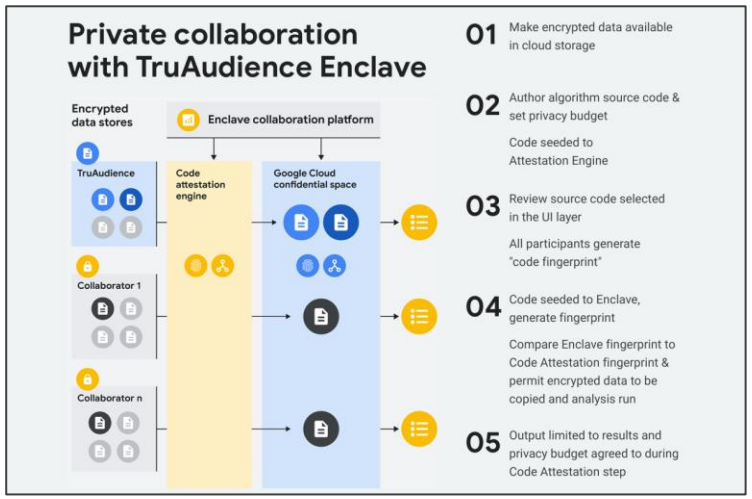
出所：Decentriq.「iCARE4CVD consortium and Decentriq」（参照 2026-08-10）.

事例詳細：広告・小売

- サードパーティCookie規制が進む広告・小売領域では、自社の優良顧客データを外部に渡すことなく異業種と連携し、消費者の権利を保護したままマーケティングの最適化や新たな価値の創出に利用されている。

3rd Party Cookieに依存しない効果測定（TransUnion）

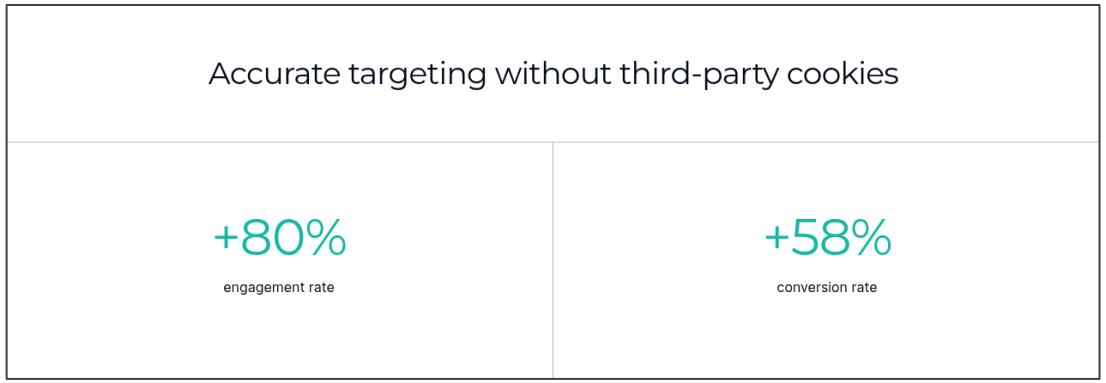
- Cookie規制が強化される中、広告パブリッシャーにとって、個人に関するデータを広告主に渡すことなく広告の効果測定を行うことが課題。
- Google CloudのConfidential Computing（TEE）基盤上にデータクリーンルームを構築し、集計結果のみを出力することで、個人データを開示しないまま個人単位の広告効果測定を実行。
- 副次的にデータ提供時の契約や審査プロセスの簡易化も実現。



出所：Google Cloud.「TransUnion redefines user-based measurement with trusted execution environments and Google Cloud」（参照 2026-08-10）.

Cookieを用いない 広告の実証（ドイツ高級車ブランド）

- 自社顧客データを広告配信に用いるニーズがあるが、メディア側と個人データを相互に開示できない。
- Decentriqのデータクリーンルーム上で、ブランドの自社データとメディア側のデータを照合。誰もデータを見られない状態で類似顧客層を特定し、スイスのメディア枠に配信。
- 従来の3rd Party Cookieによる配信と比較して、インプレッション数-33%でエンゲージメント率+80%、コンバージョン率+58%を実現。



出所：Decentriq.「Leading luxury car brand improves ad efficiency using first-party data within Swiss premium publisher inventory」（参照 2026-08-10）.

事例詳細：製造

- 自社の技術ノウハウを完全に保護しつつ、企業間を横断した品質改善や、マテリアルズ・インフォマティクス（MI）を用いた共同開発を加速させる取り組みが国内で先行。
- 海外に比べ多数の組織が分業する日本の製造業特有のサプライチェーン構造が背景。

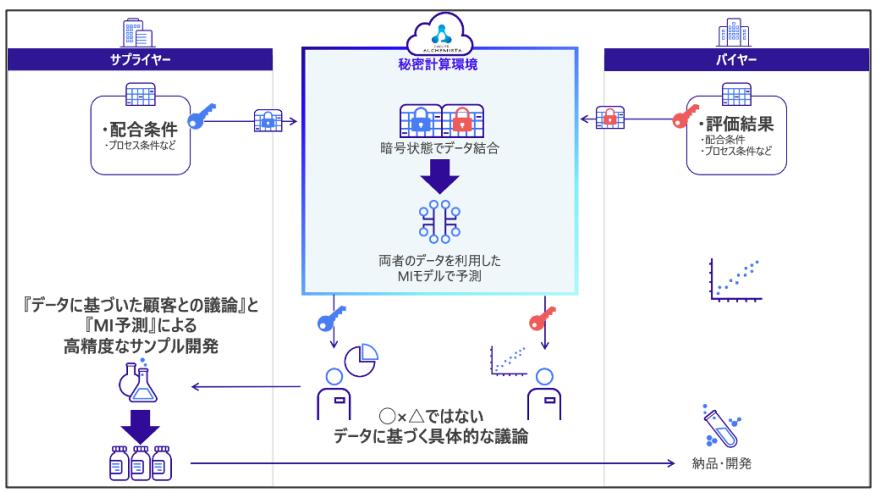
サプライチェーン横断の品質要因解析（巴川×日立ハイテク）

- 電池・半導体開発の最適化にはサプライチェーン横断でのデータ連携が不可欠だが、企業間で材料データや製造データを直接共有することは困難。
- EAGLYSのConfidential Computing基盤「EAGLYS ALCHEMISTA」を活用し、巴川コーポレーションの「材料データ」と日立ハイテクの「検査・計測データ」を、互いに元データを秘匿したまま安全に連携・分析する基盤を構築。
- 機密データを掛け合わせたAI分析により、新素材の開発期間短縮や製造プロセスの品質向上を目指す実証を開始。

出所：日立ハイテク.「EAGLYS、巴川コーポレーション、日立ハイテク、電池・半導体領域における秘密計算AIを活用した企業間データ連携の実証実験を開始」（参照 2026-08-10）

素材開発におけるMI共同分析（三菱ケミカル×大塚化学）

- 化学素材の開発には企業間のデータ連携が有効だが、配合や製造プロセス等のコア技術（生データ）の開示は困難。
- 「EAGLYS ALCHEMISTA」を活用し、三菱ケミカルと大塚化学がそれぞれ保有する「材料データ」や「開発ノウハウ」を、互いに元データを秘匿したまま安全に連携・分析する基盤を構築。
- 機密データの安全な掛け合わせにより新たな知見を創出。また、通常2～3年を要する開発期間を1年未満へ短縮。



出所：EAGLYS.「EAGLYS ALCHEMISTAを活用し、三菱ケミカル・大塚化学が材料開発期間を大幅短縮 ～通常2-3年の開発期間を1年未満に短縮、ビジネスレベルの材料作成に成功～」（参照 2026-08-10）

TEEの限界と残存リスク

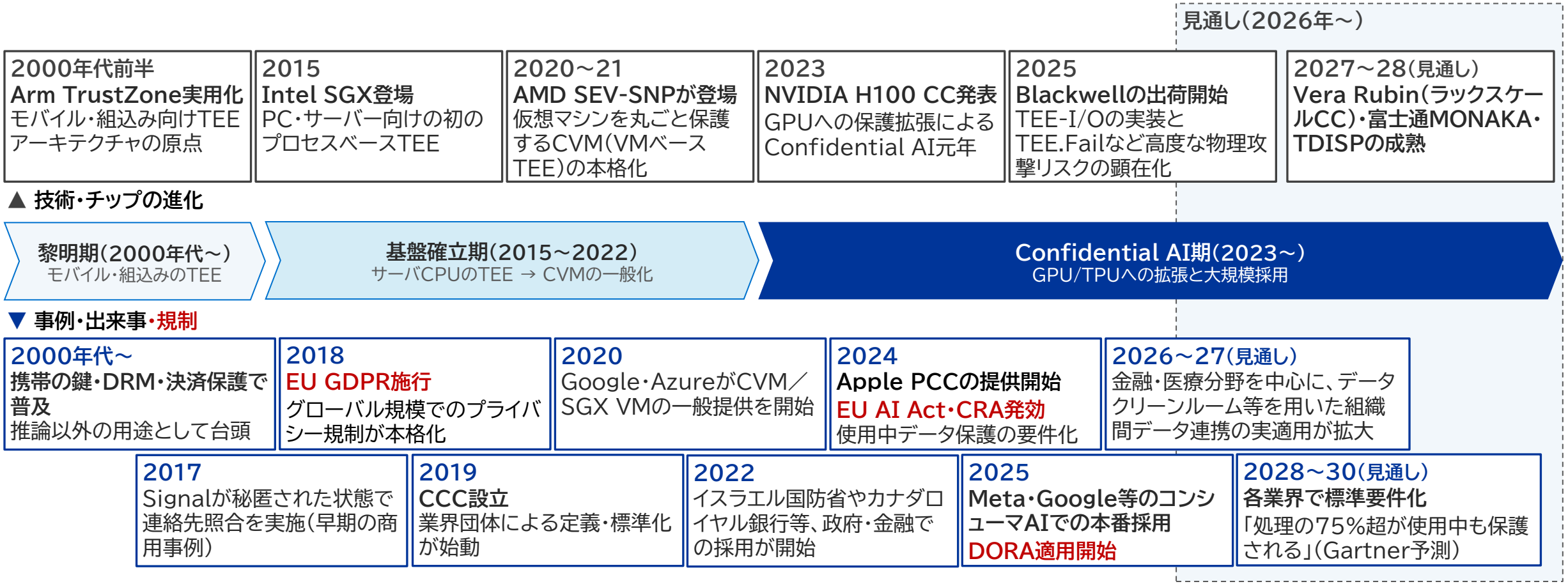
- TEEはあらゆるリスクからシステムを完全に保護する銀の弾丸ではない。
- 技術的保護の限界を正しく見極め、物理的対策・第三者監査・運用プロセスを含めた「多層的な防御」を設計することが、本番運用において絶対条件となる。

リスク	内容	示唆・対策
物理攻撃 （例：TEE.Fail）	• DDR5メモリバスへの機器挿入により暗号文パターンを傍受し、署名鍵の抽出や証跡の偽造を実証。Intel/AMDは「物理攻撃は脅威モデル外」としている	• ホストの物理セキュリティ（入退室管理等）を信頼の前提とする • 物理筐体に紐付けて証明を行うアテステーション技術を活用する
ソフトウェア攻撃研究 （2025年に複数報告）	• SEV-SNPへのRMPocalypse等、設計や実装の弱点を突く攻撃と修正のイタチごっこが常態化	• ベンダーからのセキュリティ通知を常時監視し、TCB Recovery（FW更新に伴う再アテステーション）のプロセスを運用に組み込む
実装・運用の欠陥	• MetaのWhatsApp事例（事前監査）では高深刻度の欠陥を多数検出。TEE自体は堅牢でも、その上のアプリやアテステーション実装に脆弱性が潜む可能性がある	• 第三者機関によるコード・アーキテクチャ監査を実施する • 「TEE＋監査＋運用」のセットで安全性を保証する
外部サービスへの依存	• システム全体の内製は極めて困難であり、外部サービスに依存するのが現実的。一方、これらベンダー提供の基盤自体が侵害された場合に、自社システムも脅威に晒される • クラウド事業者を信用しない目的でTEEを使用する場合、検証ロジックにそれら事業者が提供するツールを使用することは矛盾を含む	• どの外部コンポーネントに依存しているか（TCBの定義）をアーキテクチャ設計時に明確化する • 用途・非信頼対象に応じて、サードパーティの検証サービスを採用するなど、トラストの設計を正確に行う

出所：TEE.Fail 論文（IEEE S&P 2026）、RMPocalypse 論文（CCS 2025）、Trail of Bits 監査報告（2026年4月）、IDC「Unlocking the Future of Data Security」（2025年11月）等を基に日本総研作成

技術・市場ロードマップ

- TEEは2030年に向けて「次世代インフラの標準要件」として定着していく見通しである。
- 金融や医療などの特定業界を筆頭に先進企業は次なる競争優位の源泉として動き始めている。先進的なデータビジネスを検討する企業においても、将来の標準化を見据えた早期の取り組みが不可欠である。



出所:各社公表資料、Gartner「Gartner Top 10 Strategic Technology Trends for 2026」(2025年10月)等を基に日本総研作成。2026年以降は公表ロードマップ・アナリスト予測に基づく見通し

展望と普及に向けた残存課題

- 要素技術の多くは本番環境での本格稼働に適する水準に到達している。
- 普及に向けたボトルネックは「技術」、「ベンダー」、「ユーザー」、「法制度」の4観点に集約されるが、インフラの標準化や官民主導のルールメイキングにより、導入ハードルは解消されていく見込みである。

	課題	展望
技術・インフラ	• ノウハウを持つ人材の不足により、導入の検討自体が立ち上がらない • 技術の採用に際して中立的な比較指標や基準がなく、導入に結び付かない • TEE対応GPUの環境整備と調達のハードルによるコストの増大	• 業界団体や第三者機関によるベンチマーク・ガイドラインが整備されることで、ソリューションの比較検討が容易になり、導入に向けた意思決定プロセスが確立する • 「GPUリソースの共有機能とTEEの併用」や「TEE対応のCPU-GPU間通信の高速化」が標準技術として確立し、対応GPUの市場供給が拡大することで、現実的なコストでの運用が可能になる
ベンダー	• 単なる「TEE対応インフラの提供」にとどまる付加価値の欠如 • 業界別の標準構成や、法規制に準拠した責任分界モデル等、ユーザー目線でのパッケージ化が不足している	• 付加価値の欠如は市場の未成熟・法規制の未整備も一因である。TEEの利用が広く普及することで、法規制に準拠した責任分界の明確化や容易にビジネスに組み込むパッケージングといった付加価値がより効果を増す • 技術的な導入ハードルが下がり、インフラ単体での差別化が難しくなるにつれて、ベンダー間の競争軸が変化し、実運用を直接支援するソリューション化が加速する
ユーザー	• セキュリティ技術単体に対する積極的な購買・投資意欲は低い • 自社内でTEE環境を構築・運用するためのスキルもモチベーションも不足している	• ユーザーが自ら技術を選ぶのではなく、業務SaaSやクラウド基盤の裏側に、TEEが標準機能として組み込まれる形での普及が進む • 自社でインフラを構築・運用することから、ベンダーが提供するサービスの「安全性（アテステーション等の検証結果）を確認して利用する」ことが役割として定着する
法規制・ルール	• 定型的な法解釈や、実務に即したガイドラインが未整備 • コンプライアンス上の影響が不明瞭なことで保守的な企業が導入を躊躇する	• 法改正などに伴い、「特定の技術的保護を講じていれば適法とする」といった、技術と法律を結びつけるルールメイキングが官民主導で進み、導入に向けた意思決定プロセスが容易になる

日本総研 The Japan Research Institute, Limited

TEE活用に向けた推奨アクションプラン

- 高まるデータ保護要請を競争優位の源泉へと転換するために、「規制対応」・「事業創出」・「インフラ基盤」の3軸で段階的な移行を推進することが求められる。
- 短期的には要件把握と技術検証を早期に完了させ、中長期的には機密データを安全に掛け合わせるデータ連携エコシステムの確立で市場を先行する。

戦略	短期(1～2年) 要件把握・初期対応	中期(3～5年) ガバナンス確立・事業化	長期(～10年) 普及・安定運用
守り 規制・コンプライアンス対応	• EU DORA法、AI Act等における「使用中データの保護」要求の自社事業への影響評価 • 機密データ(顧客情報・生体情報等)とその取扱要件の棚卸	• アテステーション(技術的な安全性証明)を前提とした、新たな社内審査プロセスの構築 • 機密データの活用に向けた、社内セキュリティガイドラインへの「Data in Use保護」の反映	• データ主権(Data Sovereignty)要請への完全準拠と、クロスボーダーでのデータ流通網の確立 • 「全データの使用中保護」を前提とした、コンプライアンス監査の自動化の実現
攻め データ連携・新規事業創出	• これまで「セキュリティ上の懸念」で活用できなかった機密データ(ノウハウ・高価値データ)の棚卸 • データクリーンルーム等を活用した、異業種・競合間での安全なデータ共有モデル(PoC)の策定 • 自社データ・AIモデルの安全な外部提供シナリオの検討	• TEEを活用した新規データ連携ビジネス(Confidential AI基盤)の商用展開 • 自社の生データやコアノウハウを秘匿したまま、他社データと安全に掛け合わせ、自社事業の高度化・収益化を図るエコシステムの構築	• 業界横断でのセキュアなデータエコシステムの確立と、プラットフォームの主導 • 社会課題解決(創薬、高度な金融犯罪対策など)に向けた大規模データ連携の定常的運用
基盤 ITインフラ調達・運用ガバナンス	• クラウド活用を前提としたITインフラ、およびセキュリティ要件の検討 • 既存システムを改修せずに移行可能なミドルウェアの検証	• 扱うデータの機密性やユースケースに応じた、クラウドインフラ調達基準への「機密コンピューティング要件」の組み込み • 複雑なアテステーション検証を自動化するマネージドサービスの導入 • 新たな運用体制の構築(システム管理部門とセキュリティ部門における責任分界の明確化)	• マルチテナント環境・ラックスケール等、次世代TEE基盤の全面採用による運用最適化 • すべてのAIおよびデータ処理基盤におけるゼロトラスト・アーキテクチャの実現

まとめ

- 規制強化と技術の成熟に伴い「TEEによる使用中データの保護」が重視される中で、将来のデファクト化を見据えたガバナンス構築と本番検証に着手することが望ましい。

1.背景 第2章	「機密データをAIで活用したい」というビジネスニーズと、「AIに入力する際の情報漏洩」への懸念が対立。さらにEU DORA法をはじめ「使用中データ保護」の規制化が進展。この課題に対し、TEE等のPETs（プライバシー強化技術）が現実解として台頭し、データ活用において「安全性」が新たな選択軸となり、市場構造の変化を引き起こしている。
2. 技術 第3・4章	TEEは「物理的な隔離・メモリ暗号化・アテステーション（技術的証明）」の3要素で構成されるハードウェアベースのトラスト基盤である。「GPU TEE」の商用化により、LLM等のAI処理まで保護範囲が劇的に拡大し、性能オーバーヘッドも実用域に達した。普及に向けた課題は「対応GPUの市場流通」と「リソース共有をはじめとした環境整備・運用コストの最適化」に集約される。
3. 市場 第5章	グローバル企業の75%が採用に着手する一方、本番稼働は18%（金融37%・医療29%）にとどまり、このギャップの解消が技術の普及の焦点となる。Gartnerが2026年の戦略トレンドに選出し「2029年に75%超が使用中保護を前提とする」と予測するように、数年内にクラウドインフラのデファクトスタンダード（標準要件）となる見通しである。
4. 事例 第6章	実用性はBig Tech（Apple・Meta・Google）の数十億ユーザー規模での本番運用により実証済みである。エンタープライズ領域でも、データクリーンルームによる異業種連携（製造業のMI連携、金融の不正検知等）が稼働している。エコシステムも拡充し、「自前でインフラを構築する」のではなく「既存サービスを組み合わせて使う」土台が整いつつある。
5. 展望 第7章	普及に向けた主な課題は、技術ではなく「導入に向けた評価基準の不在」「運用スキームの未確立」にある。欧州のDORA法やAI Actをはじめグローバルで規制対応が進む中、国内でも令和8年の改正個人情報保護法がデータ連携の契機となり得るため、施行までの期間を見据えたガバナンス体制の検討を進めることが望ましい。

日本総研

The Japan Research Institute, Limited