THE LINUX FOUNDATION | Research

CONFIDENTIAL COMPUTING CONSORTIUM

機密コンピューティングの事例

保護された機密データ プロセスによるビジネス価値の提供

Suzanne Ambiel

2024 年 7 月

機密コンピューティングの事例

機密コンピューティング コンソーシアム

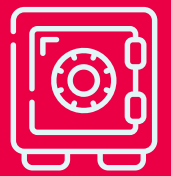
ベンダー、クラウド提供者、開発者が**一体となり**、Trusted Execution Environment（TEE）技術と標準の採用を加速します。

機密コンピューティング

ハードウェア ベースの認証済みTEEで計算を実行することによる使用中の**データ セキュリティを強化**します。

機密コンピューティング

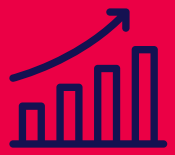
ハードウェア ベースの認証済みTEE環境で計算を実行することによる使用中の**データを保護**します。



機密コンピューティングのユースケース

ビジネス価値の提供：

生活の向上、新薬の発見、窃盗犯の逮捕、データの改ざんから保護します。



機密コンピューティングのユースケース

パブリック クラウドの導入：機密性の高いワークロードをパブリック クラウドにセキュアに展開し、データ プライバシーとセキュリティの懸念に対応します。

機密コンピューティングのユースケース

新市場への進出：

機密データを暗号化し、国境で制限されたアクセスを維持することで、GDPRおよびHIPAAコンプライアンスを強化します。

機密コンピューティングのユースケース

機密AIの導入：

モデルとデータをライフサイクル全体で保護し、安全なトレーニング、推論、データ プライバシーを確保します。

機密コンピューティングのユースケース

AI投資の保護：

モデルとデータをセキュアに保護し、サードパーティやパブリック クラウド提供者からのアクセスを制御します。

機密コンピューティングのユースケース

より良いキャンペーンを構築し、新規顧客を獲得：

ターゲットを絞ったキャンペーンを展開し、個人情報を保護した上で顧客の行動を理解するためにデータを**セキュアに**共有します。

機密コンピューティングのユースケース

疑わしい取引の特定：

マネー ロンダリングを特定するためにデータをプールすると同時に、顧客のプライバシーに関する世界の銀行規制要件を充足します。

機密コンピューティングのユースケース

命を救い、患者の治療の転帰を改善：プライバシーを守り、規制要件を満たしながら、患者データをセキュアに分析することで、より早く病気を発見し、革新的な治療計画を立案します。

機密コンピューティングのユースケース

新薬の開発：研究機関とコラボレートしながら、患者データを保護し、規制コンプライアンスを確保し、倫理基準を維持します。

目次

はじめに

業種、業務、企業規模にかかわらず、今日のビジネス リーダーは、規制や業界特有の法律を厳格に遵守しながら、プライバシーを損なうことなく、企業や顧客のデータをいかに安全かつセキュアに収集、蓄積、活用するかというデータ課題に立ち向かわなければなりません。また、人工知能（AI）や AI/ 機械学習（ML）の台頭と、これらのイニシアチブを推進するための膨大なデータ要件により、この課題はさらに緊急性を増しています。

ストレージやネットワークの暗号化技術は、保存時や転送中のデータを保護する手段を提供しますが、使用中のデータは脆弱なままです。データが暗号化されていない状態で処理されると、データの改ざんや漏洩を引き起こす可能性があります。

逃した機会：クラウド コンピューティングとマルチパーティ データ コラボレーション

多くの企業にとって、データは新たなリスクを導入するにはあまりにも貴重です。データ漏洩や改ざんの恐れがあるため、これらの企業はデータの配布や使用を制限しています。クラウド コンピューティングを活用する機会を放棄する企業もあれば、リスクを軽減するために企業指定のサイロにデータを保管する企業もあります。このようなデータ分離戦略によって、企業はデータをビジネスの成長、業務効率の改善、顧客基盤の拡大に役立てることができなくなります。

異業種やサードパーティとのコラボレーションもまた、チャンスを逃す可能性があります。サードパーティのデータにセキュアにアクセスし、社内の独自データを補強できれば、企業は未知のパターンを検出したり、新製品を開発したりすることができます。サードパーティのデータは、大規模な AI モデルのトレーニング、研究の検証、市場機会の発見にも不可欠です。医療や金融サービスなどの業界の企業にとって、厳しいデータ保護とプライバシー規制は、コンプライアンス違反に対する潜在的な罰則と相まって、多くの組織がこのような新しい機会への参加を見送るか制限せざるを得ません。

機密コンピューティングによるデータとコードの保護

データを保護しながら共有し、処理する方法が欠けていると、企業のゴール達成能力に影響を及ぼします。競争上の優位性、新製品開発、運用コストの削減、市場シェアの拡大、投資収益率（ROI）の向上など、多くの問題があります。しかし、機密コンピューターによる戦略を採用することで、これらの可能性を引き出すことができます。

機密コンピューティングは、保護された信頼された実行環境（Trusted Execution Environment : TEE）を提供し、未承認のソフトウェアや管理者、共有インフラ上の他のテナントから見えないようにデータを処理します。使用中のデータはセキュアであり、権限のない第三者はデータを変更することも、見ることもできません。この保護はアプリケーションにも及びます。TEE はアプリケーションの完全性を保証し、改ざんや盗難からアプリケーションを保護します。

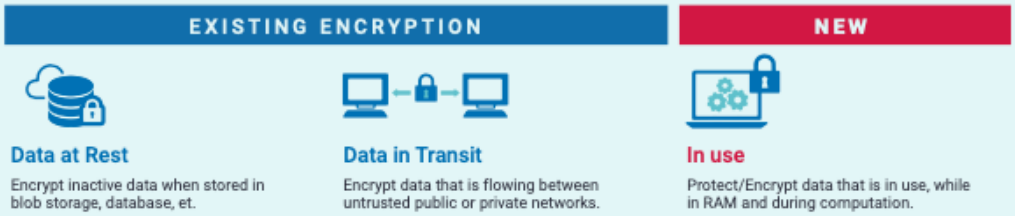
機密コンピューティングの力

機密コンピューティングでは、あなたのデータはあなたのデータのままであり、権限のないユーザーに見られたり、改ざんされたり、盗まれたりすることはありません。データは、保存時、転送時、使用時の 3 つのモードすべてで保護されます。機密コンピューティング プラットフォームは、業界を超えたイノベーションとコラボレーションのための保護された基盤を提供します。組織は機密コンピューティングを使用して、データのサイロ化を解消し、パブリッククラウドの導入を可能にし、グローバルなデータ プライバシー コンプライアンス要件を満たします。

医療および製薬企業では、安心安全にマルチパーティ データ コラボレーションを行うことができるため、新しい治療法の模索、新薬の開発、患者の転帰の改善を以前よりも効果的に行うことができます。金融サービス企業にとって、機密コンピューティングはイノベーションを促進するだけでなく、マネー ロンダリングやその他の金融犯罪を検知するため

- **機密コンピューティング：**機密コンピューティングは、認証済みの Trusted Execution Environments（TEE）の構築を通じて、“使用中”のデータとコードを保護するハードウェアベースの技術ソリューションです。機密コンピューティングは、機密データにエンドツーエンドのセキュリティを提供し、そのライフサイクル全体を通じて不正なエンティティからデータを保護することを目的としています。
- **TRUSTED EXECUTION ENVIRONMENT（TEE）：**使用中に、権限のないエンティティがデータまたはコードを変更、削除、または閲覧できないように、データの完全性、データの機密性、およびコードの完全性を提供する環境のことを指します。
- **エンクレーブ：**エンクレーブとは、TEE 内のセキュアで隔離されたメモリ部分のことで、機密データやコードを安全に処理することができます。TEE は、包括的なセキュア環境を提供するためにプロセッサ レベルで実装されます。エンクレーブは、TEE 内の特定の実装であり、機密性の高いコードやデータをさらに隔離するために作成されます。
- **アテステーション：**アテステーションは、信頼された実行環境（Trusted Execution Environment：TEE）内のソフトウェアとハードウェアコンポーネントの完全性と真正性を、暗号署名された証明によって検証することです。このプロセスにより、TEE が機密データを扱うために信頼される前に、変更されていない本物のコードを実行していることが保証されます。
- **データのライフサイクル：**データは、保存状態（ストレージ内）、移動中（ネットワーク上）、使用中（処理中）の 3 つのモードのいずれかです。今日の暗号化技術は、最初の 2 つのモードに取り組んでいます。機密コンピューティングは、セキュアな処理環境を構築することで、最後のモードである使用中のデータをハードウェアで保護します。

アーキテクチャや技術実装を含む機密コンピューティングの詳細については、“**A Technical Analysis of Confidential Computing**”と“**Confidential Computing: Hardware-Based Trusted Execution for Applications and Data**”をご覧ください。



のセキュアな業界横断コラボレーションを可能にします。

以下の各ユースケース概要では、機密コンピューティングを用いて組織が企業データの価値を安全でセキュアかつ信頼性をもって活用する上でどのように役立つかをご紹介します。機密コンピューティング ソリューションを選択し、データを活用することで、組織はビジネスを成長させ、クライアント、患者、顧客により良いサービスを提供し、困難なデータ課題に取り組み、法規制コンプライアンスの要求に正面から対応することができます。

- 機密データ クリーン ルームが効率的なマーケティング成果を実現
- セキュアなデータ処理がパブリック クラウドの導入を実現
- 認証と Secure Enclave でグローバル データ保護とコンプライアンスを強化
- 機密コンピューティングが企業向け機密 AI を後押し
- マルチパーティ データ コラボレーションがマネーロンダリング撲滅に貢献
- プライバシーを保護するデータ集約は、より良い医療の転帰につながる

機密コンピューティングの詳細については、Confidential Computing Consortium（CCC）をご覧ください。

機密データ クリーン ルームが効率的なマーケティング成果を実現

産業 : すべての産業のマーケティング ストラテジスト、デジタルメディアと広告

課題 : ファーストパーティのデータとサードパーティの cookie の排除が不十分であると、マーケティングと広告ターゲティングの精度や効果を低下させ、広告費のリターンを低下させます。

解決策 : 機密コンピューター対応のデータ クリーン ルームは、ファーストパーティ データをサードパーティ データでセキュアに充実化することができます。

利益 :

1. マーケティングと広告プログラムの結果を改善し、ROI を向上させる
2. 見込み客と顧客のプロファイルを強化して市場シェアを拡張する
3. データ漏洩のリスクを低減し、その後の規制や法的処罰を軽減する

「サードパーティの Cookie は、何十年もの間、インターネット広告を支えてきました。その廃止に伴い、出版社やブランドは、プライバシー優先の世界で顧客にリーチする全く新しい方法を再考する必要があります。Decentriq と機密コンピューティングにより、Goldbach は信頼レイヤーを実現し、ブランドはコンプライアンス リスクなしにファーストパーティ データを利用することができます。」[1]

—JOCHEN WITTE, CTO, GOLDBACH GROUP AG

概要

小売とマーケティングのパイオニア、John Wanamaker 氏はこう宣言したと伝えられています。「広告宣伝費の半分は無駄になっています。」彼がこの言葉を口にしてから 125 年近くが経ちますが、今でもその言葉は真実味を帯びています。デジタルと従来のメディアを横断してマーケティングと広告の ROI を正確に測定することは、最高のマーケターやエージェンシーでさえも難しいことです。

実際の顧客とのインタラクティブやトランザクションから収集されたファーストパーティ データは、行動や購買パターンに関するある程度の洞察を組織に提供します。しかし、それは 1 つの関係をカバーするだけであり、市場の競合他社であれ、単なる補完的な製品プロバイダーであれ、顧客が他のブランドとどのように相互作用しているかについての洞察に欠けています。

以前は、サードパーティの Cookie はその追加データを取得し、顧客のより完全な全体像を描くために役立っていました。このようにファースト データとサードパーティ データを組み合わせることで、パーソナライズされた体験を構築し、ターゲットを絞ったマーケティング取り組みや広告キャンペーンを推進し、新しい製品やサービスを生み出すための不可欠な基盤となりました。

今日、個人を特定できる情報（Personally Identifiable Information : PII）と呼ばれるファーストパーティ データはさまざまな規制によって保護されており、厳格なデータ セキュリティと保護の必要性が高まっています。また、共有やサードパーティとのコラボレーションを阻む障壁にもなっています。最もよく知られ、広く引用されているのが、E.U. の GDPR です。さらに、従来のサードパーティの Cookie が制限されることで、組織が利用可能な顧客ペルソナデータの量も制限されます。

このため、組織はデータセットが減少し、顧客行動に関する視野が狭まる可能性があり、広告やデジタル マーケティングの取り組みの半分が最も効果的であるのか、再び疑問に思うことになります。

1 https://www.decentriq.com/products/media-advertising

解決策：機密コンピューティングが可能にするデータ クリーン ルーム

機密コンピューティングは、この課題に対する解決策を提供します。データの目次を明らかにすることなくデータを接続、処理できるセキュアな環境を構築することで、組織はファーストパーティ データをサードパーティーの追加データで充実させることができます。

データ クリーン ルームと呼ばれるこの環境では、複数のデータ提供者がファーストパーティ データをセキュアに接続し、これまで利用できなかった幅広いデータセットからインサイトを得ることができます。ユーザーは、データ漏洩のリスクや規制上の課題を抱えることなく、”そっくりさん”のオーディエンス プロファイルを作成することができます。より大規模なデータプールへのアクセスにより、企業はこれらのインサイトを利用して、より効率的なマーケティングや広告プログラムを設計し、見込み客のパイプラインを購入準備の整った顧客で満たすことができます。メディア企業はまた、プライバシーを損なったり、国際的なプライバシー法や地域のプライバシー法に抵触したりすることなく、データを収益化することができます。

「機密コンピューティングとデータ クリーン ルームは、合法的かつ効率的な方法で情報を交換する絶好の機会を提供しています。これにより、より良いメディア プランニングと広告、より正確なターゲティングが可能になり、最終的には、すべてのデータ保護規制を遵守しながら、より多くの収益を上げることができます。」[2]

—ZHAO WANG, HEAD OF DATA TECHNOLOGY, RINGIER

2 How Decentriq Empowers Swiss Businesses to More Privacy and Security

もっと詳しく

- **Enhancing Privacy and Data Protection With Confidential Computing** (Zonar)
- **Is Your Organization Ready for a‘ Cookie-Less” World?** (Decentriq)
- **Improving Ad Efficiency Through First-Party Data Collaboration** (Dencetriq)
- **Reducing Marketing Costs With Tailored Lookalike Audiences** (Decentriq)
- **Sharing Data Across Organizations Without Sharing** (Enclaive)

保護されたデータ プロセスがパブリック クラウドの導入を可能に

産業 : すべての産業の CIO、CISO、CTO

課題 : クラウド コンピューティングはスケールと有利な経済性を約束しますが、クラウド提供者や他のテナントに専有データを公開するリスクは、クラウドの採用の可能性を制限します。

利益 : 機密 VM とエンクレーブで保護されたパブリック クラウドにアプリケーションとデータを展開します。

BENEFITS:

1. クラウドの経済性、スケーラビリティー、柔軟性
2. ハードウェアによるデータとアプリケーションのセキュリティ、プライバシー、制御

概要

ほぼすべての業界で、パブリック クラウドは広く採用されています。その利点は広く認知されています：柔軟性、スケーラビリティー、コスト管理、ポータビリティーなどです。しかし、その人気とは裏腹に、リスクがないわけではないことを認識することが不可欠です。共有インフラ上で専有データや高度に規制されたデータをクラウドで処理すると、データやアプリケーションが漏洩、盗難、侵害されるリスクが生じます。

Enclaive 社の CTO である Sebastian Gajek 氏によると、「パブリック クラウドは、多くの利点を提供する一方で、インフラの共有やマルチテナント環境における潜在的な脆弱性により、セキュリティ上の疑問が生じることが多い」と言います[3]。多くの企業にとって、信頼できる唯一の解決策は、ワークロードとデータをオンプレミスに維持することです。

「エンクレーブは、同じシステム上で動作する他のアプリケーションやサービスから分離されているため、攻撃対象は最小限に抑えられます。企業が”クラウドファースト”を考える今日、このテクノロジーは非常に重要です。セキュリティやコンプライアンス上の懸念から、これまではクラウドへのアップロードが考慮されていなかったワークロードも、このサービスを利用できるようになりました。」[4]

—SEBASTIAN GAJEK, CTO, ENCLAIVE

機密コンピューティングでアプリケーションとデータを保護する

今日の主要なクラウドプロバイダーは、機密コンピューティングに解決策を提供することで、この課題に対処しています。業界アナリストは、機密コンピューティングは最も機密性の高いアプリケーションとそのデータにとっても、クラウド コンピューティングをより安全にするための実行可能な解決策であると考えています。機密コンピューティングは、Trusted Execution Environment（TEE）またはエンクレーブと呼ばれる、セキュアなハードウェア ベースの処理環境を提供し、機密データやアプリケーションをさらに保護します。

3 Five Reasons Why a Confidential Cloud Trumps a Public Cloud

4 Five Reasons Why a Confidential Cloud Trumps a Public Cloud

TEE では、アプリケーションとそのデータは他のすべてのユーザーやオペレータから隔離されます。クラウド提供者でさえも、権限のない第三者はデータやコードにアクセスすることができません。この解決策では、ハードウェアによってデータの機密性とアプリケーションの完全性が強化され、データだけでなくアプリケーションのセキュリティとプライバシーも強化されます。セキュアな隣人、ハッカー、その他の潜在的なセキュリティ脅威は大幅に変更され、最小限に抑えられます。機密性の高いデータや規制対象のデータを持つ組織にとって、この保護と保証レベルの強化は、クラウドにおける新たな運用モデルへの扉を開くことになります。

アプリケーションとデータを機密コンピューティング VM またはエンクレーブでクラウドにデプロイすることで、組織はクラウド コンピューティングの利点をすべて享受しながら、漏洩から保護されたセキュアな環境でサードパーティからのアクセスからデータとアプリケーションを保護することができます。

機密コンピューティング ベースのパブリック クラウド解決策を採用することで、企業は最も機密性の高いデータや規制対象データであっても、クラウド コンピューティングの多くの利点を享受することができます。

もっと詳しく

- **Five Reasons Why a Confidential Cloud Trumps a Public Cloud** (Enclaive)
- **Confidential Computing** (Google)
- **Azure Confidential Computing—Protect Data in Use** (Azure)
- **O.C. Tanner Protects Customer Data Across Hybrid, MultiCloud, and Multi-Site Environments** (Fortanix)

機密コンピューティングが企業向け機密 AI を強化

産業 : すべての産業の CTO、CISO、CPO、CIO

課題 : AI モデルと関連データは、保護されないまま放置されると、盗難、改ざん、コンプライアンス違反のリスクにさらされます。

解決策 : 機密コンピューティングを使用した AI モデルの展開と運用の解決策

利益 :

1. 独自のデータ、アルゴリズム、モデルへの投資を保護
2. クラウド コンピューティングの経済性とスケールを活用
3. コストを削減し、市場投入までの時間を短縮

概要

AI のトランスフォーマーとしての可能性は、今日あらゆる組織にとって最重要課題であり、投資、発明、革新への意欲はあらゆる業界に及んでいます。Menlo Ventures によると、今日の企業は AI 関連テクノロジーに年間 750 億ドル以上を投資しています。[5] その支出の大部分は、組織のイノベーションと収益マシンの心臓部である製品開発とエンジニアリング部門で行われています。ビジネスと投資を保護するためには、こうしたイニシアチブの基盤を形成する独自のデータとアルゴリズムを、競合他社や改ざんの可能性からセキュアに保護する必要があります。

バランスを取る：セキュリティ対アクセス

適切なデータ ガバナンスとセキュリティは、企業の成功と AI の解決策の展開にとってクリティカルです。社内のデータストアを OpenAI や Anthropic のようなサードパーティのファウンデーション モデルやクラウド提供者がホストするモデルにセキュアに接続することは、多くのビジネスリーダーにとってリスクの高い行動であり、採用の障壁となります。AI / ML モデルをオンプレミスのみで運用すると、社内のコンピューター リソースを大量に消費するだけでなく、成果も制約されます。ファーストパーティのデータのみにアクセスが制限されるため、結果が不完全または最適でない可能性があります。

しかし、クラウド コンピューティングの利用には大きなリスクが伴います。AI を活用した製品やサービスの構築にはコストと時間がかかり、独自のデータやカスタム アルゴリズムに依存するため、侵害の標的になりやすいのです。クラウド提供者のグローバルな性質は、データ保護法が地域によって異なるため、複雑なコンプライアンス上の課題ももたらします。クラウドサービスでは、機密情報を外部のサーバーに転送する必要があるため、データの所有権、管轄権、管理について疑問が生じ、さらにリスクが高まります。

単なる AI ではなく、機密 AI

AI で保護が必要なのはデータだけではありません。モデル、重み付け、アルゴリズム、そして結果、これらすべてをプライベートかつセキュアに保つ必要があります。エンタープライズ AI を機密コンピューティング環境に導入することで、保護はデータからモデル、アプリケーションにまで及びます。機密コンピューティングは、クラウド提供者によるデータの閲覧、改ざん、盗用を防止します。TEE はモデルも保護し、改ざんや汚染を防止することで、モデル結果の統合を保証します。Translational Genomics Research Institute の VP of Scientific Computing である Glen Otero 氏は以下のように述べています。「コンピューティング中にアルゴリズムだけでなくデータの保護も提供できる機密コンピューティングは、今後 5 ～ 10 年のデータ プライバシーと AI モデリングの将来にとってデフォルトの要件になるでしょう。」[6]

5 Source: Menlo Ventures, The State of Generative AI in the Enterprise, 2023

6 TGen Secures Genome Data for Richer Healthcare AI Models With Fortanix Confidential Computing

医療提供者や金融サービス企業にとって、AI はモデルやアプリケーションによって消費される規制の厳しいデータ量に起因する独自の課題をもたらします。機密コンピューターは、モデルとデータを不正アクセスから保護する信頼された実行環境を提供するため、これらの新しい AI 対応イニシアチブは、プライバシー、セキュリティ、および倫理的な懸念を満たしながら結果を出すことができます。

さらに機密 AI の環境は、常に機密性を保持しながら、セキュアでコンプライアンスに準拠したサードパーティ データの利用を可能にします。企業や顧客の個人データを保護しながら、サードパーティの LLM にアクセスし、活用することができます。

このようにプライバシーとセキュリティが保証されることで、組織は AI をより自信を持って導入し、投資することができます。機密性の高いコンピューター環境が投資を保護します。

もっと詳しく

- **How Jamworks Protects Confidentiality While Integrating AI Advantages** (IBM)
- **TGen Secures Genome Data for Richer Healthcare AI Models With Fortanix Confidential Computing** (Fortanix)
- **Privacy-Preserving Data-Collaboration Methods That Accelerate Healthcare Innovation** (Intel)

「機密コンピューティング プラットフォーム（CCP）は、アルゴリズムを検証するサイクルタイムを半分に短縮することができます。コストもほぼ半分になります。このようなコスト削減により、一般化可能なアルゴリズムのトレーニング、検証、市場投入をより迅速に行うことができます。そして、CCP の基礎となるテクノロジーとプロセスが成熟するにつれて、より速く、より低コストになっていくでしょう。」[7]

—MARYBETH CHALK, CO-FOUNDER AND CHIEF COMMERCIAL OFFICER, BEEKEEPERAI, INC.

7 Accelerating Development of Clinical AI Algorithms

機密コンピューティングがグローバルなデータ保護に貢献

「機密コンピューティング…それは、顧客のデータをセキュア化し、欧州のニーズに対応したGDPR およびSchrems II コンプライアンスを確保するための明確な選択肢でした。」[8]

—GORDON WADDELL, SENIOR VICE PRESIDENT OF SOFTWARE DEVELOPMENT, ZONAR

産業：すべての産業の CTO、CIO、CISO/CPO

課題：あらゆる種類のデータに対するコンプライアンス要件は増加の一途をたどっており、セキュリティやプライバシーに関する技術、監査、報告書作成にかかるコストは、IT 予算の中でますます増大しています。

解決策：機密コンピュータの採用による解決策は確実で、証明され、監査可能な結果を、コスト効率よく、一貫して提供します。

利益：

1. コンプライアンスの合理化によるコスト削減
2. 柔軟性の向上
3. 認証、監査可能なデータ セキュリティとプライバシー

概要

個人情報の保護を目的としたデータ コンプライアンス規制は、ますます広まり、複雑化し対応が難しくなっています。あらゆる種類の消費者データに適用される規制の地方版、地域版、全国版が存在するため、コンプライアンス上の課題は目まぐるしく変化しています。

GDPR から HIPAA まで、あなたのビジネスが患者、顧客、見込み客、サードパーティ提供者のデータを扱うのであれば、たとえ地理的に国境を越えていても、これらの規則が適用されます。さらに、これらの規制は一般的に、企業の規模や所在地に関係なく適用されます。また、すべてのデータについて、最も厳格な規則をデフォルトにするのが安全です。

特にクラウド コンピューティング戦略を導入している場合、このような状況は非常に困難なデータ管理とプロセスにつながります。データによっては、コンプライアンスを確保するために、クラウド環境やデータセットを地域ごとに保護する必要があります。一部の企業にとって、この問題はあまりにも複雑で、罰則も厳しく、コンプライアンス コストも高すぎるため、ビジネスを制限したり、有望なパートナーシップを見送ったりせざるを得ません。

信頼された実行と認証：強力な組み合わせ

規制対象データを機密コンピューティング環境に置くことで、規制機関が提起する多くの課題に対処できます。機密コンピューティングによる解決策では、TEE またはエンクレーブが、TEE へのアクセスを明示的に許可されていないソフトウェアや個人からデータを分離し、保護します。さらに認証は、TEE が本物であり、正しく動作していることを暗号的に確認します。このシナリオでは、TEE が保護と隔離を提供し、アテステーションが保証を提供します。

組織が新たなビジネス パートナーシップを追求したり、新たな市場に進出したりする際には、データを保護し、データをセキュアに処理する手段を提供することが成功の鍵となります。機密コンピューティング プラットフォームが提供する保護機能により、組織はデータ管理に関する規制強化の課題に対応できるようになり、CIO や CISO も多少安心できます。

もっと詳しく

- **Zonar Helps Ensures GDPR and Schrems II Compliance by Enhancing Privacy and Data Protection** (Google, Zonar)

8 Zonar Helps Ensures GDPR and Schrems II Compliance by Enhancing Privacy and Data Protection

金融サービス

マルチパーティのデータコラボレーションがマネー ロンダリング対策を支援

産業 : 金融サービスの CTO、CLO、CIO、CISO/CPO、GM、プロダクト マネージャー

課題 : 金融機関は顧客データを保護すると同時に、犯罪収益の受領を防止するための厳格なマネーロンダリング防止規制を遵守しなければなりません。

解決策 : 機密コンピューティングによる解決策により、複数の金融機関の取引データをセキュアにプールします。

利益 :

1. 迅速な検知で時間とコストを節約します。
2. 保証された結果でコンプライアンスの要求をサポートします。
3. 効率的なマルチパーティ コラボレーションでコストを削減し、成功率を高めます。
4. パターン認識、アルゴリズム開発、予測モデリングにより不正検知を迅速化します。

「決済における不正は、クライアントにとって毎年数十億ドル規模の大きな問題です。金融犯罪の防止は、銀行として個々で解決できる問題ではなく、集団で解決する必要があります。」[10]

—ISABEL SCHMIDT, CO-HEAD OF GLOBAL PAYMENTS PRODUCTS AT BNY MELLON, A MEMBER OF THE SWIFT NETWORK

概要

多国籍密輸業者、麻薬シンジケート、制裁を受けた企業や国。これらはすべて金融取引を行い、その業務において公的銀行や金融機関に依存しています。どのような顧客であっても、金融機関は厳しい規則に対処しなければなりません。一方では、厳格な個人情報保護規則を遵守し、顧客データを保護する必要があり、他方では、マネー ロンダリング防止法や顧客を知る”know your customer”法の強化により、金融機関は顧客データを非常に慎重に調査しなければなりません。この緊張関係が、特に金融機関同士の取引における異常の迅速な発見を困難にしています。金融データがこのようにサイロ化されているからこそ、犯罪者たちは不正行為を隠蔽することができるのです。

犯罪者は、金融機関間で迅速かつ密かに資金を移動させることで、グローバルな金融ネットワークを悪用し、気付かれることなくその隙をすり抜けることができます。United Nations Office の Drugs and Crime によると、毎年 2 兆ドルもの不正資金がグローバルな金融ネットワークを通じてマネー ロンダリングされています。[9]

この流れを食い止めるため、金融機関は規制、報告要件、法律が増え続けており、これに従わなければ多額の罰則が課せられます。今日、金融機関は厳格なデューデリジェンスと業務手続きを実施しなければなりません。コンプライアンスを証明するための監査可能な記録を用いて、制限されたセクター、制裁を受けた個人または団体、あるいは犯罪的手段による支払いを無意識のうちに処理していないことを確認しなければなりません。

9 https://www.unodc.org/unodc/en/money-laundering/overview.html

10 Swift Innovates With Azure Confidential Computing To Help Secure Global Financial Transactions

コンプライアンス違反の代償は甚大で、数億ドルから数十億ドルに達する罰則が科されることも少なくありません。しかし、マネー ロンダリングを摘発するのは困難です。マネー ロンダリングを示す可能性のある異常なデータについては、一企業のデータセットでは不十分ですが、機関全体のデータを集約すれば不正取引が明らかになるかもしれません。しかし、こうした情報を共有すること、特にサードパーティや競合他社と共有することは、リスクも伴います。情報漏えいは、厳しい金銭的な罰則だけでなく、企業イメージの風評被害にもつながりかねません。

高度なデータ共有とリスク軽減のための機密コンピューティングの活用

悪者がグローバル ネットワークを悪用するのと同様に、金融機関もマネー ロンダリングに対抗するために同じネットワークを活用する必要があります。データセットが増えれば増えるほど、パターン認識は指数関数的に向上します。データが豊富であればあるほど、結果は良好になります。データをプールし、他の金融機関や利害関係者と安全にコラボレートすることで、より早く検知することができ、時間とコストを節約することができます。これは特に機密コンピューターに適したタスクです。コラボレーションに使用される 2 つの方法は、マルチパーティ データ共有と連合学習モデルです。

機密コンピューティング環境でのマルチパーティによるデータ共有は、すべての参加者のデータが非公開かつセキュアに保たれることを保証し、露出や汚染の脅威を排除します。機密コンピューティングを利用することで、金融機関はデータ クリーン ルーム（管理されたセキュアな環境）にアクセスすることができます。この環境では、機密性と規制コンプライアンスを確保するために、個人を特定できる生の情報を公開することなく、複数の当事者からデータをプールします。

連合方式は、データセットが大きすぎたり、機密性が高すぎたり、規制が厳しすぎたりして、オフプレミスに移動したり、社内のプライベート クラウド インスタンスを超えて共有したりできない場合によく用いられます。このシナリオでは、機関の内部システムがすべてのデータをローカルに保存します。

各機関はモデルやアプリケーションをセキュアに共有し、ローカルで処理します。すべての関係者は、共有された共通のモデルやアプリケーションから得られる統合結果から利益を得ます。

どちらのシナリオにおいても、機密コンピュータ環境が提供する保護により、参加機関はデータが侵害や漏洩から保護されるという確信を得ることができます。

もっと詳しく

- **Swift Innovates With Azure Confidential Computing** To Help Secure Global Financial Transactions (Microsoft)
- **MonetaGO Detects Duplicate Financing Fraud** (Google / AMD)
- **Applications for Digital Fraud Defense** (FiVerity)

医療＆メディカル リサーチ

プライバシー保護されたデータ集約でより良い転帰が得られる

産業 : 医療提供者、メディカル リサーチ、製薬

課題 : 患者データは最も高度に規制されたデータタイプの 1 つで、コラボレーションとデータ共有はほとんど禁止されていますが、より良い転帰とコスト削減が期待できます。

解決策 : 機密コンピュータが可能にするデータ集約により、医療提供者は患者のプライバシーを守りながら、患者の転帰や研究の成果を向上させることができます。

利益 :

1. 患者ケアと転帰の改善
2. より効率的な診断と治療によるコスト削減
3. 臨床医と医師の学習の強化
4. より大規模で多様な臨床試験

概要

患者データは、最も扱いにくいデータの 1 つです。その収集、使用、保存、アクセス、プロセスは高度に管理されており、様々な法律、規制、監督機関によって規制されています。米国では HIPAA が最も有名です。患者のプライバシーを侵害した場合の罰則は厳しく、評判や金銭的な負担も大きいため、医療データの管理者はいかなる理由であれ、誰とも共有したがらないのです。しかし、この情報を共有することで、患者や医療提供者に直接もたらされる利点があります。

より良い医療と患者の転帰を実現するためには、医療提供者間で患者データを集約することが重要です。集約された患者データは、医療機関や病院間の効率的な連携ケアを可能にしたり、専門的な医療を促進するのに役立ちます。また、特に患者数の少ない地方の医師が、より良い患者の転帰を実現するのにも役立ちます。より多くのデータが手元にあれば、医師は症状の比較、病気の診断、高度な治療計画の推奨を迅速に行うことができます。

臨床研究者や製薬会社にとって、新薬や治療法の開発・承認にはデータが必要です。成功には、高品質で大量のデータセットへのアクセスが不可欠です。臨床試験や高度な医学研究には、電子カルテを含む実世界のデータが必要ですが、それらは多くの場合、複数の医療提供者、臨床医、国にまたがって配布されています。これらの団体や管轄区域は、アクセスを厳しく制限したり、禁止したりするため、アクセスへの障壁はしばしば乗り越えられないように見えます。情報を共有しながら患者データを保護する手段がないため、臨床試験はさらに困難なものになっています。

代替方法

データの集約やコラボレーションに代わる方法としては、匿名化やクレンジングによる PII の排除などがあります。しかし、これらの方法は面倒で非効率的です。各機関が異なるデータの命名、保管、キュレーションの標準に従うため、データを正規化する障壁は高くなります。匿名化されたデータは、リアルタイムで結果を得られないことが多く、あいまいな結果をもたらすこともあります。

マルチパーティによるデータ共有およびコラボレーション契約の締結もオプションの 1 つです。しかし、学術機関、病院、医療提供者、または個々の医師の間で、コンプライアンスに準拠したセキュアな生の患者データを共有する契約を締結し、維持することは時間がかかり、規制上および法律上の課題が山積しています。

Intel の Health and Life Science 担当 General Manager である Chris Gough 氏は、次のように述べています。「保護された医療データの収集と分析には、複数の医療機関やシステムにまたがるデータの機密性や分散性などの課題があり、患者のプライバシーを強力に保護する必要があります。」[11]

共有は思いやり

データを共有することで、医療専門家は医療を画一的なモデルから、より的確で的を絞った介入へとシフトさせることができ、費用対効果の高い方法で患者の転帰と生活の質を向上させることができます。専門的で複雑なニーズを持つ患者に対しては、集約されたデータにより、より効率的な複数の医療機関間の治療プログラムが可能になります。臨床試験が複雑化する中、コラボレーションを可能にしながら患者のプライバシーとデータ セキュリティに対応できるシステムの構築は、新たな治療法の発見に不可欠です。

患者データの集約とコラボレーションには多くの利点があるにもかかわらず、患者のプライバシーとデータ保護の敷居が高いため、これらの利点には手が届きません。非効率的で非準拠なデータ共有方法では、医療提供者は診断、治療、ケアに役立つ限られた情報しか得られないデータセットに制限されます。これでは新薬の開発には十分ではありません。

機密コンピューティングは、医療機関や医療提供者間で患者データを効率的かつ安全に共有・集約するために、医療提供者に理想的なセキュアなマルチパーティ コラボレーションや連携学習の解決策を提供することができます。

医療専門家は、患者のプライバシーが保護されデータが安全であることを認識しながら、より良い転帰を患者に提供することができます。患者は、治療や診察にかかる時間を短縮することで、より早く健康を取り戻すことができます。機密コンピューティングが可能にする医療提供者間の連携ケアプランは、あらゆる種類の医療現場での摩擦を軽減します。医師や臨床医にとっても、追加症例や代替治療計画に触れることで利点があります。研究者にとっては、プールされたデータと研究機関間のコラボレーションにより、革新的な治療法を生み出し、治療法の市場投入を加速することができます。

「Leidos は、臨床情報システムに関連する技術的課題と、情報をセキュアに共有するための信頼できるコンピューティング環境を構築する必要性を理解しています。“機密コンピューティング”は、この分野における厳しいコンプライアンス規制を満たしながら、自信を持ってデータをプライベートかつセキュアに共有できるパートナーのエコシステムを構築するために必要な基盤を提供してくれます。」[12]

—ERIKA KILLIAN, FDA PORTFOLIO DIRECTOR, LEIDOS

もっと詳しく

- **Intel Teams With Leidos, Fortanix To Accelerate Clinical Trials** (Intel, Leidos, Fortanix)
- **Privacy-Preserving Data-Collaboration Methods That Accelerate Healthcare Innovation** (Intel, BeekeeperAI)
- **Healthcare Data Collaboration by the Numbers: Balancing Progress and Privacy** (Decentriq)
- **Decentriq To Facilitate Analysis of Data From Over 1M Cardiovascular Disease Patients** (Decentriq)

11 Intel Teams With Leidos, Fortanix To Accelerate Clinical Trials

12 Ibid, Intel Teams With Leidos, Fortanix To Accelerate Clinical Trials

結論

機密コンピューティングはより良い結果をもたらす

生活を改善し、新薬を発見し、泥棒を捕まえ、データを改ざんから守るには？　機密コンピューティングならすべて可能です。

組織が機密コンピューティングを採用する場合、どのような状態であっても、データ セキュリティに対する強力で包括的なコミットメントを示すことになります。ハードウェア ベースの TEE を従来のデータ暗号化テクノロジーとともに実装することで、組織のデータは保存中や転送時だけでなく、使用時にも保護されます。これらの解決策はコードの完全性も保証します。TEE がアプリケーションを保護する場合、コードの改ざん、汚染、盗用は不可能です。

利点は、新しいビジネスの実現、コンプライアンスの強化、新製品開発と展開の合理化など、さまざまな業界に及びます。

- 企業のマーケティング担当者にとって、ファーストパーティ データをサードパーティ データでセキュアに充実化することで、マーケティング キャンペーンの効率を高め、不要で非生産的なキャンペーン活動を減らし、顧客満足度を向上させることができます。
- CIO や CISO にとって、独自のモデルを構築、運用、調整するためのセキュアで確実なプライベート環境は、カスタム AI や機密 AI の可能性を現実のものにします。
- グローバルな金融サービス機関にとって、競合する可能性のある他の金融機関やサードパーティと顧客データや取引データをプールできることは、不正行為の防止、融資業務の改善、イノベーションの加速に役立つ可能性があります。
- 医療提供者にとっては、自らのコレクションをはるかに超えた大規模で多様なデータセットにアクセスすることで、より迅速で正確な疾病診断と最適な治療計画が可能になり、患者の転帰を改善しながらコストを削減し、患者のデータ プライバシーを守ることができます。
- 製薬会社や医学研究者にとって、データ共有は、より大規模で、より効果的な可能性のある臨床試験への扉を開き、新しい革新的な治療法をより早く提供することを可能にします。

ここに掲載されているストーリーは、Intel、Google、Decentriq、Microsoft、BeeKeeperAI などの業界リーダーやイノベーターの経験に基づくものです。TikTok のような組織は、ユーザーや顧客との信頼関係を構築するために、機密コンピューティングの新しい利用法を実験し続けています。プライバシーの保護されたデータ共有を含む 4 つの異なるユースケースを開発中の TikTok は、そのゴールをサポートするために機密コンピューティングに注目しています。TikTok の Developer Advocacy とオープンソース担当マネージャーである Vini Jaiswal 氏と TikTok の Research Scientist である Mingshen Sun 氏は、「1 億 7,000 万人のユーザーを相手にしているため、プライバシーは当社（TikTok）の最重要イニシアチブの 1 つです。」と言います。機密コンピューティングは、TikTok がすべてのユーザーと顧客に対して信頼、プライバシー、セキュリティの約束を提供し続けるための数多くの方法の 1 つです。

しかし、機密コンピューティングの導入はここで止まる必要はありません。米国を拠点とするソフトウェア会社 Hushmesh が機密コンピューティングの可能性について語るのを聞くと、チップ レベルから始まる普遍的な“ゼロトラスト”モデルを実装するための機密コンピューティングに基づく未来のインターネットについて学ぶことになります。その世界では、プライバシーとセキュリティは追加機能ではなくなり、さまざまなソフトウェアを通じて実装され、インフラストラクチャーの上に階層化されるでしょう。その代わりに、データのセキュリティとプライバシーは、インフラストラクチャーに生まれつき備わっているもの、つまりチップに自動的に組み込まれているものであり、人間が追加したり管理したりするものではなくなります。Hushmesh の CEO である Manu Fontaine は以下のように述べています。「機密コンピューティングは、あらゆるもの、あらゆる人に対するエンドツーエンドの暗号セキュリティを完全に自動化するグローバルなインフラと情報空間の創造を可能にすると考えています。」これは機密コンピューティングの大きなビジョンです。

方法論

この調査は、Linux Foundation Research Team が 2024 年 2 月から 5 月にかけて実施し、Confidential Computing Consortium がスポンサーとなっています。プロジェクト チームは、一連の一次調査インタビューと、コンソーシアム メンバーのコントリビューションによる二次調査を実施しました。また、詳細な文献調査、市場調査レポート、アナリスト レポート、ベンダーの Web サイト、メディア記事、ベンダー主催のホワイトペーパ ーから、さらなる洞察を収集しました。

謝辞

概要の作成を指導し、研究参加者を特定したことから、報告書作成中の思慮深く徹底的なレビューと解説に至るまで、貴重な貢献をしてくれた Mike Ferron-Jones に感謝します。

著者について

Suzanne Ambiel はテクノロジー業界のベテランで、フォールト トレラント コンピューティングから VM、コンテナ、オープンソース ソフトウェアまで幅広い経験を有しています。VMware（現 Broadcom）に在職中は、OSPO の戦略とコミュニケーションを主導し、ブランド リサーチとインサイトのマネージャーも務めました。元 Linux Foundation Board member および LF Research Advisory Board member として、今日のデジタル世界でオープンソースが果たす役割が不可欠であり、拡大していることを個人的に観察してきました。

付録

インタビューした参加者及びコントリビューター

Vini Jaiswal, TikTok
Mingshen Sun, TikTok
Dayeol Lee, TikTok
Manu Fontaine, Hushmesh
Marcus Hartwig, Google
Stanislav Nikolskiy, GenoMex
Malini Bhandaru, Intel
Mike Ferron-Jones, Intel
Mona Vij, Intel
Paul O’Neill, Intel
Nikolas Molyndris, Decentriq
Andrew Knox, Decentriq
Emily Fox, Red Hat
Mike Bursell, Confidential Computing Consortium

Confidential Computing Consortium 発行の追加資料

Common Terminology for Confidential Computing

Confidential Computing—The Next Frontier in Data Security

A Technical Analysis of Confidential Computing v1.2

Confidential Computing: Hardware-Based Trusted Execution for Applications and Data

Confidential Computing in Financial Services: Use Cases for Data Security

Confidential Computing Consortium YouTube Channel

CONFIDENTIAL COMPUTING CONSORTIUM

Linux Foundation がスポンサーする CCC は、ハードウェア ベースの TEE を使用して使用中のデータをセキュア化し、オープン コラボレーションを通じて機密コンピューティングの採用を加速するプロジェクトに焦点を当てたコミュニティです。CCC は、ハードウェア ベンダー、クラウド プロバイダー、ソフトウェア開発者を集め、TEE 技術と標準の採用を促進しています。

本訳文について

この日本語文書は、**The Case for Confidential Computing** の参考訳として、The Linux Foundation Japan が便宜上提供するものです。英語版と翻訳版の間で齟齬または矛盾がある場合（翻訳版の提供の遅滞による場合を含むがこれに限らない）、英語版が優先されます。

この日本語文書を引用する際には、下記の一文を記載してください。
引用：The Case for Confidential Computing 参考訳（The Linux Foundation Japan 提供）

翻訳協力：富田明男・富田佑実

THE LINUX FOUNDATION | Research

2021 年に設立された **Linux Foundation Research** は、拡大するオープンソース コラボレーションを調査し、新たな技術トレンド、ベストプラクティス、オープンソース プロジェクトのグローバルな影響に関する洞察を提供しています。プロジェクトのデータベースやネットワークを活用し、定量的・定性的手法のベストプラクティスにコミットすることで、Linux Foundation Research は世界中の組織のためとなるオープンソースに関する洞察を得るためのライブラリを構築しています。

この著作物を参照する場合は、以下のように引用してください：Suzanne Ambiel,“ The Case for Confidential Computing: Delivering Business Value Through Protected, Confidential Data Processing,” The Linux Foundation, July 2024.