2023年11月

コンフィデンシャル・コンピューティング ISV 支援パッケージ

ISV がインテル製品搭載ソリューションで顧客のビジネス上の課題にいかに対応できるか

コンフィデンシャル・コンピューティングとは？

コンフィデンシャル・コンピューティングとは？

コンフィデンシャル・コンピューティングは、機密データを使用したインサイトの導出や
AI モデルのトレーニングを実行でき、しかもそのデータをほかのソフトウェア、コラボレーター、
クラウド・プロバイダーなどに公開することがありません
これにより、以前なら取り扱いの難しかった非常に機密性の高いデータや、規制の厳しいデータについても、
企業が分析やその他の目的のために有効活用できる可能性が広がります

コンフィデンシャル・コンピューティングは、
ソフトウェア・セグメントの中でも、
ハードウェアやサービスを追い抜いて**最大かつ最も急成長している市場セグメント**です

わずか数年のうちに、**コンフィデンシャル・コンピューティングは、使用中のコードやデータをエンドツーエンドで保護する強力で新たな手段として幅広く注目され、躍進しています**

コンフィデンシャル・コンピューティングの必要性

連続的なデータ保護にある大きな溝を埋める

保管中のデータ	転送中のデータ	使用中のデータ
ストレージの暗号化	ネットワーク暗号化	コンフィデンシャル・コンピューティング

Everest Group®

Everest Group によると、この「データ・セキュリティーにおける次の未開拓分野は…急成長への準備が整っています」
2021年には 19 億ドルだったグローバル市場は、クラウドおよびセキュリティーのプロジェクトの牽引により、2026年まで合わせて年間 40% ～ 95% の割合で成長すると見込まれています。

コンフィデンシャル・コンピューティング

セクター & ユースケース

セクター

ユースケース

コンフィデンシャル・コンピューティング

主な AI ユースケース

マルチパーティー機械学習

センシティブな顧客データの機密性とプライバシーを損なうことなく、機械学習の力を活用

ビジネス概要

コンフィデンシャル・コンピューティングによるマルチパーティー機械は、以下の分野で特に有用です

ヘルスケア

データの力を活用することで、患者の機密情報を漏洩させることなく、より高度な調査研究が可能です

金融サービス

マネーロンダリングやテロ活動の資金調達に対抗しながら、潜在的な不正行為の予測精度を向上できます

顧客ケーススタディー

ヘルスケア

規制対象データによる共同コンピューティング

BeeKeeperAI™ NOVARTIS

状況

Novartis Biome は、希少疾患の診断モデルと治療法を開発しています。希少疾患の情報は少なく、複数の病院や研究機関に分散しています

課題

患者情報は非公開であり、厳しい規制があります。病院は、データを外部に移すことや、非公開の記録を BeeKeeperAI や Novartis に開示することを望んでいません

ソリューション

各病院の現場にインストールされたインテル® ソフトウェア・ガード・エクステンションズ（インテル® SGX）対応の BeeKeeperAI ノードがプライベート・データを分析し、クラウドに おけるマスターモデルのウェイトを更新します。Novartis も BeeKeeperAI の社員も、規制対象の健康記録を見たり保存したりすることはありませ

BeeKeeperAI™

「[コンフィデンシャル・コンピューティング・プラットフォーム] により、アルゴリズム検証のサイクルタイムが半分に短縮されます。また、コストもほぼ半減します。このように時間やコストが節約されることで、一般化できるアルゴリズムの学習、検証、市場投入にかかる時間が大幅に短縮されます。そして、CCP の基礎となるテクノロジーやプロセスが成熟していくにつれ、さらなる時間短縮とコスト削減が見込まれます」**BeeKeeperAI, Inc、Co-founder and Chief Commercial Officer、MaryBeth Chalk 氏**

ホワイトペーパー

臨床 AI アルゴリズムの開発を加速

顧客ケーススタディー

高セキュリティーのキー保護

Fortanix®

状況

キーと証明書の急増により、強力な
保護と一元管理が求められています。
HSM ソリューションは高価であり、
クラウド・ソリューションは CSP
のセキュリティーとコンプライア

課題

クラウドのホストから技術的に
分離された HSM のようなセキュ
リティーを備えた、スケーラブル
な
ソフトウェア・ベースのキー
管理システムを構築する

ソリューション

Fortanix は、インテル® SGX 上の
Self-Defending KMS ソフトウェアを
ベースとして、外的やクラウド・プロ
バ
イダーからキーと証明書を保護し、
所有者の秘密事項をその管理下に
置けるようにします

Fortanix®

インテル® SGX を有効化しても高パフォーマンスを維持
複数インスタンス構成を実装することで、スループットが大幅に向上しています。インテル® SGX を有効化しても、こうした
パフォーマンスの強化への影響は最小限に留まるため、組織はセキュリティーとパフォーマンスを同時に高められます。

ソリューション・スナップショット

機密 AI データ インテル セキュリティ ソリューション - Fortanix

中国の顧客ケーススタディー

データの価値を発掘

Chuanglin Technology

状況

企業のデータとプライバシーのセキュリティー確保は、データベースやハードウェアのメーカーが直面する、よくある問題です

課題

従来のデータ暗号化テクノロジーは、ハードディスク・ストレージとネットワーク通信のみを暗号化するもので、その有効性は、サーバーの制御権限が漏洩していないという前提に基づいています。サーバーの制御がインターセプトされた場合、使用中のデータは第三者に盗まれたり、改ざんされたりする可能性があります。

ソリューション

Chuanglin Technologyとインテルは、インテル® SGXメモリー暗号を使用した、グラフ・データベースのデータ暗号化リューションを共同で立ち上げました。このソリューションは、Galaxybaseの究極のパフォーマンスを保証し、メモリーセーフなグラフ・データベース製品を生み出すものです

Chuanglin Technology により作成された新世代のグラフ・データベースである Galaxybase が、高品質でセキュリティーの
高いデータサービスを提供したり、データの相互接続を効率的に認識したりでき、企業が安定した方法でデータの価値を具現化できるのは、インテル® SGX メモリー暗号化テクノロジーのおかげであると考えられます。

プレスリリース

コンフィデンシャル・コンピューティングでインテルが提供しているもの

インテルは最も包括的な
セキュリティー・ポートフォリオを提供

インテル® ソフトウェア・ガード・エクステンションズ
(インテル® SGX)

アプリケーションの分離

インテル® トラスト・ドメイン・
エクステンションズ
(インテル® TDX)

仮想マシンの隔離

インテル® Trust Authority

マルチクラウドとハイブリッド・クラウド向けの独立した信頼性検証サービス

ソフトウェア・ソリューション、クラウド、OEM、システム・インテグレーターのエコシステム

インテルのセキュリティー・ファーストの開発とライフサイクル・サポート

*インテル® TDX は、一部のクラウド・プロバイダーを通じて利用可能です。

インテルのトラステッド・エグゼキューション環境

アプリケーション・レベルの分離: インテル® SGX

特長

- クラウド・プロバイダーやその他のテナントからの分離
- 信頼境界と潜在的攻撃面の縮小
- コードの検査と監視が容易
- VM、クラウドネイティブ・コンテナー、ベアメタルで導入可能

考慮事項

- アプリには、特定の開発またはカスタマイズが必要な場合があります。
- エンクレーブ外への頻繁な通話は、パフォーマンスに影響を与える可能性があります。

VM レベルの分離: インテル® TDX

特長

- クラウド・プロバイダーやその他のテナントからの分離
- 既存アプリケーションへの移植作業を最小限に抑えます。
- 企業全体への導入の義務化にも対応
- 簡単なインスタンス構成設定が可能

考慮事項

- 信頼境界の拡大 (ゲスト OS、すべてのアプリ、VM 管理者)
- ゲスト OS とハイパーバイザーの更新により、再検証が可能
- より詳細な認証

インテル® Trust Authority

ゼロトラストを可能にし、プライベート・クラウドのセキュリティーでパブリック・クラウドの柔軟性を実現。

インテル® Trust Authority は、ゼロトラスト原則に基づき、コンフィデンシャル・コンピューティングに
セキュリティーの強化と保証をもたらす、ソフトウェアとサービスの新しいポートフォリオです。
第 1 世代では、インテル® Trust Authority は、（インテル® SGX）および（インテル® TDX） に基づ

トラステッド・エグゼキューション環境(TEE)

独自の認証サービスを構築するためのコストや複雑さを伴うことなく、ゼロトラストの信条を導入

詳細情報

コンフィデンシャル・コンピューティング支援パッケージ

製品概要

Noname の導入事例

Thales の導入事例

Zscaler の導入事例

説明ビデオ

インテル® Trust Authority
その仕組み

インテル® Trust Authority を開始する

1

- ワークロード向けのインテル® SGX または仮想マシン (VM) 向けのインテル® TDX に基づくコンフィデンシャル・コンピューティング環境 (TEE) インスタンスを設定するか、クラウド・インフラストラクチャー・プロバイダーにリクエストします。

2

- これらのコンフィデンシャル・コンピューティング環境で特定し、実行可能にします。
- これは、インテル® SGX (Gramine または別のクライアント・ライブラリーにより実現される) を使用してアプリケーション・レベルで実施することも、インテル® TDX を使用して VM レベル

3

- インテル® Trust Authority 認証キーを取得する登録をしてください。
- ワークロード (インテル® SGX) または VM (インテル® TDX) のクライアント・ライブラリーにキーを入力し、SaaS と直接通信して、TEE を確認できます。

インテル® Trust Authority に登録するには、intel.com/trustauthority にアクセスするか、trustauthority@intel.com までお問い合わせください。

インテル® Trust Authority セキュリティー・ソリューションの詳細はこちら

コンフィデンシャル・コンピューティング

インテル® SGX 向けソフトウェア＆ソリューション・エコシステム

商用サポート付きソリューション　　自分で構築

商用ソリューション・プロバイダー

anjuna
cosmian
CYBERNETICA
decentriq
EDGELESS SYSTEMS
Fortanix
Mithril Security
Opaque
enclaive
SCONTAIN
HUB SECURITY
secretarium

すぐに導入可能な厳選されたコンテナ（2023年 Q1 まで）

PyTorch
redis
scikit learn
Spark
TensorFlow

開発者向けツール

GRAMINE
SCONE
Occlum
Mystikos
Teaclave
Open Enclave SDK
intel
Intel SGX SDK

システム・インテグレーター

accenture
KPMG
Capgemini
IBM
Atos
leidos
avanade

ハイパーバイザー（SGX）

KVM 5.13 以降
vmware vSphere 8

* Azure Marketplace で入手可能

インテル® TDX の提供状況

インテル® TDX　　3 つの主要クラウド・プロバイダー

ビューで
提供されている第 4 世代インテル® Xeon® スケーラブル・インスタンスで利用可能で

各クラウド・プロバイダーの提供内容の詳細については、以下のロゴをクリックしてください。

Microsoft Azure　Alibaba Cloud　Google Cloud

IBM Cloud
*パブリック・プレビュー
TBA

インテル® TDX は、次のゲスト OS ベンダーで有効になっています。

Red Hat　SUSE　Canonical Ubuntu

*インテル® TDX は、2024年、第 5 世代インテル® Xeon® スケーラブル・プロセッサー・ファミリーにより一般的に利用可能になります。

開始方法

インテル® ソフトウェア・ガード・エクステンションズ（インテル® SGX）

詳しくはこちら　今すぐ開始

クラウド・サービス・プロバイダー

詳細についてはロゴをクリック

Azure　CORE　OVHcloud　phoenixNAP GLOBAL IT SERVICES
swisscom　IBM Cloud　CloudSigma

OEM

詳細についてはロゴをクリック

Hewlett Packard Enterprise　SUPERMICRO

トレーニングとドキュメント

トレーニング・ビデオ　テクニカル・ライブラリー　ソリューション概要

インテル® トラスト・ドメイン・エクステンションズ（インテル® TDX）

詳しくはこちら

ドキュメント

開発者向けトラスト・ドメイン・セキュリティー・ガイダンス

今すぐ開始

インテル® トラスト・ドメイン・エクステンションズ（インテル® TDX）モジュールのダウンロード

インテル® トラスト・ドメイン・エクステンションズ（インテル® TDX）ローダー

競合製品との比較

	インテル® SGX	インテル® TDX	AMD SEV-SNP	AWS Nitro Enclaves	NVIDIA H100 GPU 上のコンフィデンシャル・コンピューティング
クラウド・インフラストラクチャー・プロバイダーのハードウェア / ファームウェア、ハイパーバイザー、およびクラウド管理スタックを信頼境界から除外	●	●	●		●
複数のクラウド・プロバイダーを通じて利用可能で、マルチソーシングが容易	●	●[1]	●		●
移植、再設計、再パッケージが、ほとんどあるいはまったく不要でレガシー・アプリケーションに対応する設計		●	●		⊙[2]
ハードウェアの真正性と正しい TEE 起動の認証	●	●	●	●	●
TEE に読み込まれたソフトウェア・イメージの整合性の認証	●	⊙[3]	⊙[3]	●	
機密データは、指定されたアプリケーション・コードのみからアクセス可能。VM 管理者、ゲスト OS、その他のアプリやクラウドスタックからはアクセス不可	●				
仮想化不要で「ベアメタル」サーバーに導入可能	●				●
ロウハンマー保護を追加するための、ハードウェア・ベースの暗号化メモリー整合性オプション	●				
インテルの独立したトラストサービス（開発コード：Project Amber）との互換性	●	●			
2023年3月時点の競合製品データ資料			リンク、リンク	リンク、リンク、リンク	リンク

[1] インテル® TDX インスタンスは、2023年中に一部のクラウド・プロバイダーで利用可能になる予定であり、それぞれ異なります
[2] GPU 上で動作するレガシーコードで、変更がほとんどあるいはまったく不要です。CPU を使用するワークロードの一部は、CPU ベースの TEE と、PCIe 通信を保護する手段を組み込む必要があります。
[3] 利用可能なハードウェア・テクノロジーに備わっている機能ではありませんが、クラウドまたは認証サービス・プロバイダーにより提供される付加機能として実現可能です。

コンフィデンシャル・コンピューティングに
インテルを選ぶ理由

コンフィデンシャル・コンピューティングにインテルを選ぶ理由

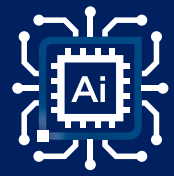
多様なセキュリティーのニーズを満たすテクノロジーの選択肢

インテルのみがアプリの分離（インテル® SGX）と VM の分離（インテル® TDX）の両方を提供しており、顧客はさまざまなセキュリティーのレベルに合わせてソリューションを正確に調整できます

幅広いソリューションのエコシステム

インテルは、何十もの ISV およびクラウド・プロバイダーと提携して、機密 AI、分析、ブロックチェーン、データベースなどのホスティングサービスやソフトウェア・ソリューションを提供しています

インテルのエキスパートとソリューション・パートナーにアクセス



インテルのエキスパートが、ソリューション・アーキテクチャー、パートナーマッチング、POC
リソース、導入のトラブルシューティングによりお客様を支援します

詳細については、PSAM に

次のステップ

教育

コンフィデンシャル・コンピューティング
の価値、そして顧客の環境を
安全に保つため、またマルチパーティー・コンピューティングを実現するために、多くのエンドユーザー・アプリにとって
コンフィデンシャル・コンピューティングを活用することがいかに
必要であるかを理解してください

関与

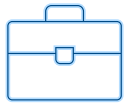
インテル PSAM に連絡して、
エコシステムにおけるインテルの
コンフィデンシャル・コンピューティング
におけるテクニカル・ポートフォリオ
への理解を深めましょう

インテル® パートナー・アライアンスはどう支援できるのか

インテル® パートナー・アライアンスに登録する

インテル® パートナー・アライアンスのメンバーになると、グローバル市場への参入、高度なトレーニング、キャンペーン・サポートなど、御社のニーズに合うメンバー限定のビジネス確立の機会を得られます

トレーニングとコンピテンシー

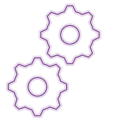


インテル® パートナー・ユニバーシティーに入会すると、知識を身につける
ための先進テクノロジーに関する専門トレーニング、コンピテンシー・プログラム、そして特典が提供されます

マーケティング・リソース

インテル® ソリューション・マーケットプレースとインテル® マーケティング・スタジオへのエントリーは、御社製品やサービスに対する需要を増やす助けになります

価値ある報奨



対象となる活動でポイントを獲得し、メンバーのステータスを向上させ、
ビジネス確立のためのさらなるリソースにアクセスしましょう

まだメンバーでない場合は
今すぐ登録

メンバーシップの特典

ポイントを獲得

インテル® パートナー・アライアンスの中で最も人気があり、際だった特典の 1 つは、インテルがパートナーに対して付与するポイントです。これは、
インテルによるビジネスの成果や、優先度の高い活動への取り組みをたたえるためのものです。

インテル® パートナー・アライアンスでは、ポイントを獲得する方法が 1,000 以上あり、

クラウド・インサイダー・コミュニティー

インテル® クラウド・インサイダー・コミュニティーは、継続的に更新される世界水準のクラウドコンテンツとツールを提供します。メンバーは、仲間やエコシステムとつながり、革新的な共同クラウド・ソリューションを市場に投入する機会を得ることができます

詳細情報

インダストリー・インサイト

ゴールドメンバーとチタンメンバーは、特別に用意された四半期毎のインダストリー・インサイトにアクセスして、
成長を促進できます

詳細情報

金銭的インセンティブ

メンバーになると、製品マーケティングの成功を促進する、強力な市場開発基金の活用やインセンティブ・プログラムへの参加が可能となります

インテル® パートナー・アライアンス・アクセラレーター・イニシアチブやその他金銭的インセンティブについては PSAM にお問い合わせください

カスタマー・サポートにアクセスする方法

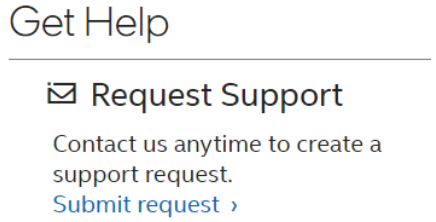
Intel Virtual Assistant

このチャットボットは、パートナー・アライアンスの各ウェブページの右下に設置されており、ほとんどの質問に対するセルフヘルプ、またはライブサポート・エージェントへのクイックリンクを提供します。

「ブレード」に関するヘルプを入手

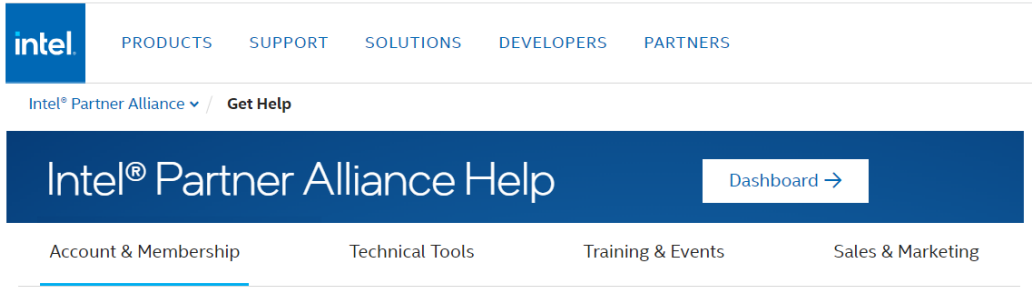
オンライン・サポートのリクエストを送信します。

このリンクは、パートナー・アライアンスのウェブサイトでは、多くのページのフッターに表示されています。



パートナー・アライアンスの「サポート」ページ

サポートページでは、パートナー・アライアンスのメンバーが
利用できるほとんどのツールや特典に関する詳細なセルフ



リソース

クラウド TV

インテル® クラウド TV は、お客様を成功に導くため、
クラウド・コンピューティングのニュース、トレンド、戦略を
探ります

クラウドでの Sapphire Rapids

クラウド資産を保護する方法について

クラウドにおけるセキュリティー

クラウドにおけるセキュリティーの課題

クラウド・ソリューションズ・アーキテクトの認証

CSA カリキュラムの修了により、クラウド・インスタンスの詳細、トピック、
ソリューションに関する専門家レベルの知識を得ることができます

このカリキュラムは、クラウドへのソリューション実装に関する最低 2 年間の

得られるもの

クラウド・テクノロジーとソリューション・アーキテクチャーに関連する知識とスキルを向上させ、
クラウド・ソリューションの設計と実装を強化します。
オンライン向けにデザインされたインタラクティブなコースとレッスンにより、最新の業界トレンドの理解を深めることで、学習者は自分のペースで進み、勤務時間と個人的な時間の中断を最小限に抑えることができます。
ハンズオン・ラボから高度な知識を得て、コンテナ・オーケストレーション、AI ワークロード、およびクラウドベースの CI/CD パイプラインによるインスタンス・チューニングから、幅広いクラウド・ワークロードにわたる高度な
クラウド・アプリケーションについて深く掘り下げることができます。
ホスト型 / プロクター型の試験に基づいて、業界で認められた認証と資格情報を取得できます。

今すぐセルフペースのオンライン認証トレーニングを開始

コンフィデンシャル・コンピューティング
情報とリソース

30-3-30

コンフィデンシャル・コンピューティング 30-3-30

ビデオ

コンフィデンシャル・コンピューティングの概要

セキュリティーが課題

研究論文

新しい AI ワークフローにおけるデータとモデルの保護

テクノロジー関連記事

コンフィデンシャル・コンピューティングの現状

クラウド・セキュリティーの概要

ブログ

パフォーマンスとサイバーセキュリティーの新しいパラダイム

セキュリティーの第一歩はインテルから

コンフィデンシャル・コンピューティング
DevOps とクラウド・アーキテクト向けリソース

テクノロジー・ペーパー

コンフィデンシャル・コンピューティングで AI 推論を高速化

インテル® Security Engines でイノベーションを加速し、データ保護を強化

ホワイトペーパー

NEW クラウド・セキュリティーの脅威に打ち勝つ方法

NEW コンフィデンシャル・コンピューティングでソブリン・ランディング・ゾーンを実現

ニュースレター

インテル® デベロッパー・ゾーン・ニュースレター

コミュニティー

インテルのコミュニティー

セキュリティー・コミュニティー・パートナー

ビデオ

インテルのセキュリティー・アクセラレーターに関する動画

その他のリソース

性能指標

第 4 世代インテル® Xeon® スケーラブル・プロセッサー・ファミリー

録画ウェビナー

クラウド・ソリューション・アーキテクト（CSA）Tech Talk：第 4 世代インテル® Xeon® スケーラブル・プロセッサー・ファミリーでクリティカルなワークロードを加速

ライブウェビナー

クラウド・ソリューション・アーキテクト（CSA）Tech Talk：第 4 世代インテル® Xeon® スケーラブル・プロセッサー・ファミリーで TCO を削減し、効率性を向上

追加トレーニング

コンピテンシーと認証

コンフィデンシャル・コンピューティングのトレーニングのリンク

セキュリティー・トレーニングのリンク

コース / トレーニング

トピック - オーディエンス
サイバー・セキュリティーのレジリエンスを高めるための、3 つの主要テクノロジー DevOps、クラウド・アーキテクチャー – コンフィデンシャル・コンピューティング
IOT ソリューション向けエンドツーエンド・セキュリティー DevOps
エッジツークラウド・セキュリティー DevOps、クラウド・アーキテクチャー
仮想プライベート・クラウド、クラウド・ネットワーキング、クラウド・セキュリティー DevOps
インテルの製品とソリューションにおけるセキュリティー価値 すべて
クラウドでのアプリケーションの保護 DevOps
クラウド・コンピューティングにおけるセキュリティー DevOps, クラウド・アーキテクト

トピック - オーディエンス
仮想プライベート・クラウド、クラウド・ネットワーキング、クラウド・セキュリティー DevOps、クラウド・アーキテクチャー
ビジネスの会話におけるセキュリティー クラウド・アーキテクチャー、経営幹部
インテル® アーキテクチャー向け暗号化入門 DevOps
インテルの製品とソリューションにおけるセキュリティー価値 DevOps、クラウド・アーキテクチャー

セキュリティー・トレーニングのリンク

オンライン・チュートリアル

トピック - オーディエンス
インテル® ハードウェア・シールドのセキュリティー機能を有効にする方法 DevOps – エンドポイント・セキュリティー


intel