製品概要

セキュリティー強化
インテル® Xeon® スケーラブル・プロセッサー

インテル® セキュリティー・エンジンによるイノベーションの加速とデータ保護の強化

パフォーマンスを維持しながらデータの機密性とコードの完全性を保護する、インテル® Xeon® スケーラブル・プロセッサーに実装されたインテル® セキュリティー・エンジン

インテル® Xeon® スケーラブル・プラットフォームを使用したコンフィデンシャル・コンピューティングの実現：プライバシーを保護しつつ、データを活用

現在では、格納されているデータや転送中のデータは暗号化することが標準的な手順となっています。しかし、データ保護において企業が直面している問題は、データがプロセッサーやメモリーでアクティブに使用されている場合です。このとき、個人を識別できる情報、医療の記録、金融取引といった機密データは、不正利用、不慮の漏えい、コンプライアンス違反といった潜在的リスクに対して脆弱になりかねません。

コンフィデンシャル・コンピューティングを使用すれば、機密データをほかのソフトウェア、協働作業者、クラウド・プロバイダーにさらすことなく、データからインサイトを抽出したり、AI モデルの学習処理を行うことができます。これによって、これまで機密性の高さや規制といった理由から分析などの目的に利用するのは難しかったデータを、ビジネスに活用できるようになる機会が大きく広がります。

デュアルソケットのインテル® Xeon® スケーラブル・プロセッサー搭載サーバーでは、最大 1TB のデータをインテル® ソフトウェア・ガード・エクステンションズ（インテル® SGX）のエンクレーブ内で処理でき、大規模データセットを必要とするアプリケーションの可能性が広がります。学習や処理の完了後は、個人情報を削除または再暗号化してから、エンクレーブを離れることが可能です。

インテル® Xeon® スケーラブル・プロセッサーを基盤としたセキュリティー・テクノロジーによるデータ活用とデータ転送の高速化

データは技術革新を加速させる原動力です。企業はデータを活用することで、不正の検出から、すぐに反応できるサプライチェーンの構築、画期的な AI モデルの学習処理まで、あらゆることを実現できます。データからビジネスインサイトを抽出できる企業ならば、前進のスピードも速く、さらに先へ向かうことができるでしょう。

インテル® Xeon® スケーラブル・プロセッサーに内蔵のセキュリティー・テクノロジーは、機密データや規制対象のデータであっても分析に利用できるようにし、イノベーションの加速につなげることを目的に設計されました。インテル® SGX は、実際に使用中のデータを保護する、独自のテクノロジーです。インテル® Xeon® スケーラブル・プロセッサーを使用する企業は、インテル® SGX を有効にすることで、機密データを分析や AI モデルの対象から除外することなく、データ・エンクレーブをアクセス制限付きで構築できます。この隔離された環境によって、企業は最も機密性の高いデータから、その機密性を維持したまま価値を抽出できるようになります。

インテル® SGXと インテル® TDXの実装による コンフィデンシャル・コンピューティングの導入

インテル® SGXを実装したコンフィデンシャル・コンピューティングでは、アプリケーション、VM、コンテナ、または機能レベルでの隔離が可能です。クラウド、エッジ、オンプレミスの環境を問わず、機密性の高い演算やデータのプライバシーとセキュリティーを高く維持し、クラウド・サービス・プロバイダー、不正な管理者アクセス、OS、外部の権限付きアプリケーションからでさえも確実に保護されます。

インテル® SGXは、データセンター向けとして最も導入と研究が進んだ信頼性の高い実行環境(TEE)であり、システム内の攻撃面を最小限に抑えることができます。[1] インテル® Xeon® スケーラブル・プロセッサーに内蔵されたこの機能によって、複数のクラウドとエッジを横断してコンフィデンシャル・コンピューティング・ソリューションが実現されます。

インテル® SGXに備わるハードウェア・ベースのセキュリティー・ソリューションは、独自のアプリケーション隔離技術により使用中のデータを保護します。特定のコードやデータを盗聴/改ざんから防ぐことで、開発者は機密データをエンクレーブ内で処理できるため、アプリケーションのセキュリティーが強化され、データの機密性が保護されます。

インテルでは今後、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)によって、さらに保護を強化していく予定です。この新しいツールは、2023年から一部のクラウド・プロバイダー経由で利用開始となり、仮想マシン(VM)レベルでの隔離と機密性の保持が可能になります。インテル® TDXでは、ゲストOSとVMアプリケーションを、クラウドホスト、ハイパーバイザー、プラットフォーム上の別のVMから隔離します。アプリケーション・レベルで隔離するインテル® SGXよりも信頼境界は大きくなりますが、インテル® TDXはアプリケーション・エンクレーブよりも、機密性の高いVMの大規模な導入と管理を簡単に行えるように設計されました。

インテル® SGXとインテル® TDXを備えたインテルのコンフィデンシャル・コンピューティング・テクノロジーの幅広いポートフォリオによって、各企業は必要なセキュリティーのレベルを選択して、個々のビジネスニーズや規制要件に対応できます。

成功事例:インテル® Xeon® スケーラブル・プロセッサーが実現するセキュリティーによるイノベーションの加速

英国の住宅金融組合 **Nationwide Building Society** は、インテル® SGXとインテル® Xeon® スケーラブル・プロセッサーを導入することで、厳格化する本人確認手続き(KYC)規制へのコンプライアンス遵守を効率化しました。

詳細を見る ›

ペンシルベニア大学では、インテル® Xeon® プロセッサーとインテル® SGXを使用し、独自開発の3DResUnet腫瘍セグメンテーション・モデルを実装しました。その結果、腫瘍と正常な組織の境界検出精度が大幅に向上しました。

事例を読む ›

コンフィデンシャル・コンピューティングに最適な選択肢

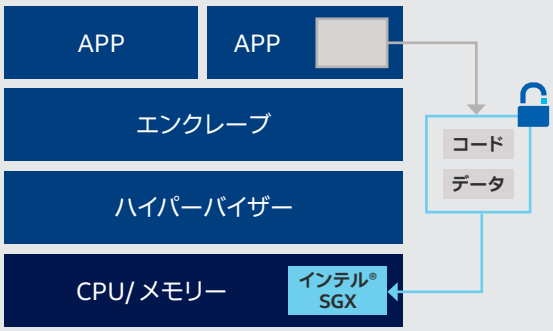

図1. 極めて機密性の高いデータを最大1TB容量のエンクレーブに隔離してデータを保護するインテル® SGX

インテル® SGXのユースケース

人工知能(AI)/ マシンラーニング(ML)

プライバシー保護規制への遵守を徹底したうえで、AI/MLを使用して機密データや規制対象データを処理できます。

クラウド・インフラストラクチャー

サービス・プロバイダーや外部のパブリック・クラウド・テナントからのデータへのアクセスを制限します。

信頼できるマルチパーティー・コンピューティング/ マルチパーティー分析

機密データの機密性を確保しながら、複数パーティー間でクラウド内の共有データを使用し共同作業を行うことができます。

安全な鍵管理

暗号鍵の保護にエンクレーブを使用し、ハードウェア・セキュリティー・モジュール(HSM)のような機能を提供します。

ブロックチェーン

トランザクションの処理、合意、スマート契約、キーストレージのプライバシー保護とセキュリティーを強化します。

ネットワーク機能仮想化(NFV)

仮想化されたネットワーク機能の信頼性を確立します。

インテル® クリプト・アクセラレーションの活用によるセキュリティーの強化と適切なパフォーマンスの維持

現在のデータセンターでは、従来の境界防御に加え、ネットワーキング、ストレージ、データ圧縮まで広い範囲にわたる処理が暗号技術に依存しています。暗号処理が増えれば、CPUで実行しなければならない暗号化のサイクル数が爆発的に増加するのも当然です。

その結果、パフォーマンスやユーザー体験に影響が及ぶことも考えられます。第4世代インテル® Xeon® スケーラブル・プロセッサーに組み込まれた高度な暗号化アクセラレーション技術によって、暗号化セキュリティーの水準が高まり、パフォーマンスの向上、シームレスなユーザー体験が可能になりました。しかも、データセンターにコアやプロセッサーを追加する必要がありません。

インテル® クイックアシスト・テクノロジー（インテル® QAT）は、成熟したデータ圧縮/暗号化アクセラレーターとして、転送中データの圧縮/解凍と暗号化のワークロードに、第4世代インテル® Xeon® スケーラブル・プロセッサーで新たに内蔵されました。インテル® QATは、演算負荷の高いワークロードをオフロードすることで、コアの演算能力を別のワークロードに解放できるため、コストを大幅に削減し、圧縮データのフットプリントを縮小します。[2]

インテル® クリプト・アクセラレーションの命令セットでは、鍵長を大きくし、アルゴリズムを強化して、データの暗号化タイプを増やすなど、より強固な暗号プロトコルを使用することで[3]、ユーザー体験への影響を最小限に抑えました。暗号化アルゴリズムの高速化によって、ユーザーにはパフォーマンスの向上、サービスレベル・アグリーメント（SLA）への対応、大半は暗号化処理に費やされる演算サイクル数の削減といったメリットがもたらされます。

インテル® クリプト・アクセラレーションが暗号化演算のアルゴリズム・レベルでもたらすメリットは、主に次の3つの領域でのパフォーマンス向上です。

公開鍵暗号化：Secure Sockets Layer（SSL）、フロントエンド・ウェブ、公開鍵基盤（PKI）などの用途で、公開鍵の暗号化/復号処理を最大6倍高速化。[4]

一括暗号処理：インテル® アドバンスト・ベクトル・エクステンション（インテル® AVX-512）により、セキュアなデータ伝送、ディスクの暗号化、ストリーミング動画の暗号化などの用途で、暗号処理を最大4倍高速化/強化。[5,6]

ハッシュ化：Secure Hash Algorithm 1（SHA-1）、Secure Hash Algorithm 2（SHA-2、SHA-256とも呼ばれる）など、SSLで使用するデジタル署名、認証、整合性チェックなどの用途で、セキュアなハッシュ・パフォーマンスを最大2倍高速化。[7]

Microsoft、SAP、Oracleをはじめとする企業が提供する商用ソフトウェア・パッケージの多くは、インテル® クリプト・アクセラレーションのメリットを有効活用できるように最適化されています。オープンソースのソフトウェアは、Linuxディストリビューション、NGINX、Java OpenJDKランタイム、OpenSSLライブラリーなど数多くありますが、インテル® クリプト・アクセラレーションに対応するようインテルによって最適化済みです。

Crypto APIツールキットのような開発者向けツールを使用すると、インテル® SGXのエンクレーブ内でより安全に暗号化処理を実行できます。さらに、インテル® インテグレーテッド・パフォーマンス・プリミティブ（インテル® IPP）の暗号化ライブラリーでは、利用可能なCPU機能を自動的に利用します。また、OpenSSL対応のインテル® QATエンジンでは、ネットワーク・セキュリティー・ソフトウェア・ソリューションに対しインテル® クリプト・アクセラレーションが透過的に有効になります。

インテル® Xeon® スケーラブル・プロセッサーに内蔵された暗号化アクセラレーション技術を活用することで、暗号化処理にかかる演算サイクル数を削減し、開発期間の短縮、DevOps効率の向上、社内のユーザー体験の向上を図ることができます。

規制遵守を徹底したうえでデータ分析をスピードアップ

企業にとって価値のあるデータには、欧州の一般データ保護規則（GDPR）、米国の医療保険の携行性と責任に関する法律（HIPAA）、中国の個人情報保護法（PIPL）のように、厳しいプライバシー保護規制が適用されるのが原則です。こうした規制を侵害すると、高額の罰金などの罰則が科されることになるため、企業や組織にとって機密データのフル活用にはリスクが伴います。個人を識別できる情報を使用する場合の回避策としては、徹底的な匿名化といった方法もありますが、分析プロセスに長い時間がかかり、精度の低下にもつながりかねません。インテル® Xeon® スケーラブル・プロセッサーと内蔵のインテル® SGXテクノロジーを使用すれば、企業は暗号化されたエンクレーブを作成でき、この内部ならばデータとアプリケーションの機密性が確保されるので、コンプライアンスを遵守しながらデータの可用性高めることができます。

「2023年までに、
世界人口の65%の個人情報が最新の
プライバシー保護規制の
対象となる見込み（現在は10%）」
— Gartner[8]

機密データ共有の障壁を解消

複数の組織間でデータを共有すると、例えばニューラル・ネットワークの学習処理などで、精度が大幅に向上し、処理スピードが格段に上がります。インテル® Xeon® スケーラブル・プロセッサーは、連合学習などの信頼できるマルチパーティー・コンピューティング・モデルを実装することで、機密データの共有を可能にします。インテル® Xeon® スケーラブル・プロセッサーと内蔵インテル® SGXのエンクレーブを利用すると、複数パーティー間で機密データをプールし、共同分析のメリットを共有することができ、プライベート・データが第三者にさらされるリスクもありません。インテル® SGXの認証機能によって、エンクレーブ内ではソフトウェアが完全に想定どおりにすべてのパーティー間で事前に合意済みの方法で動作している、という信頼性が高まります。

Boschのセキュリティー課題の解決をサポート

インテルは、トップクラスのエンジニアリング企業であるBoschと、ソフトウェア・イノベーション企業のEdgeless Systemsと協働し、Boschの自律運転支援プロジェクトの開発期間短縮に取り組みました。Boschでは、コンピューター・ビジョン・モデルの学習処理に、自動車が走行する予定の道路や場所で実際に撮影した動画と画像を使用します。この映像には、人物の顔やナンバープレートといった規制対象となる個人を識別できる情報が含まれるため、Boschの従業員がアクセスできるように匿

名化する必要がありました。ただし、データを匿名化すると、多くの場合 AI 学習処理の精度が低下してしまいます。そこで Bosch はインテル® SGX を導入し、インテル® SGX のデータ・エンクレーブ内で実際の映像を変更することなくモデルの学習処理を行うことで、データ・プライバシー関連の規制を遵守したまま、処理速度をスピードアップし、出力品質を向上できました。

クラウドとデータセンターにおける信頼の拡大と拡張

インテルのセキュリティー・テクノロジーによって、企業は機密データの漏えいリスクを低減しながら、クラウドが持つ柔軟性と拡張性のメリットを有効活用できます。インテル® Xeon® スケーラブル・プロセッサーを使用したコンフィデンシャル・コンピューティングでは、機密データがクラウド・プロバイダーのソフトウェア、管理者、外部のテナントから隔離されます。データの所有者は、リモート認証によって、エンクレーブが本物であること、最新であること、想定したソフトウェアのみを実行していることを確認できます。

インテル® Xeon® スケーラブル・プロセッサーを選択しデータを活用してさらに多くのことを実行

インテル® SGX をはじめ、多様なセキュリティー機能を内蔵したインテル® Xeon® スケーラブル・プロセッサーは、世界中のクラウド・プロバイダーやシステムメーカーを通じて利用できます。このプロセッサーを新たなサービスの提供、取引価値の増幅、金融犯罪の防止、研究開発サイクルの短縮などに活用すれば、機密情報や貴重な規制対象のデータを運用するアプリケーションの進歩を加速することが可能です。未来はデータを持つ人の手中にあり、インテル® アクセラレーター・エンジンならば、より早くその未来に到達できます。

インテル® セキュリティー・エンジンが、ビジネスにとって最も重要なワークロードでピーク性能を達成し、セキュリティーを最大限に強化する方法については、以下のページを参照してください。

Intel – Confidential Computing

1 インテル® ソフトウェア・ガード・エクステンションズによるデータ保護

2 https://www.intel.com/content/www/us/en/developer/articles/technical/offloading-compression-and-encryption-in-ceph.html（英語）

3-7 ソリューション概要「Tapping into Cryptographic Acceleration」（インテル）。https://www.intel.co.jp/content/dam/www/central-libraries/us/en/documents/2022-08/tapping-into-cryptographic-acceleration-sb.pdf（英語）

8 「Gartner Says By 2023, 65% of the World's Population Will Have Its Personal Data Covered Under Modern Privacy Regulations」（Gartner、2020 年 9 月）。https://www.gartner.com/en/newsroom/press-releases/2020-09-14-gartner-says-by-2023--65--of-the-world-s-population-w/（英語）

性能は、使用状況、構成、その他の要因によって異なります。詳細については Performance Index サイトを参照してください。

性能の測定結果は、構成に示されている日付時点のテストに基づいています。また、現在公開中のすべてのアップデートが適用されているとは限りません。構成の詳細については、補足資料を参照してください。絶対的なセキュリティーを提供できる製品またはコンポーネントはありません。

実際のコストや結果は異なる場合があります。

ワークロードと構成については、https://www.intel.com/processorclaims/（英語）: 4th Generation Intel® Xeon® Scalable Processors の各項目を参照してください。結果は異なる場合があります。

インテルのテクノロジーを使用するには、対応したハードウェア、ソフトウェア、またはサービスの有効化が必要となる場合があります。

インテルは、サードパーティーのデータについて管理や監査を行っていません。ほかの情報も参考にしてデータの正確さを評価してください。

各アクセラレーターの利用可否は SKU ごとに異なります。製品の詳細については、Intel Product Specifications を参照してください。

インテルは人権を尊重し、人権侵害の発生を回避するように尽力しています。詳しくはインテルの Global Human Rights Principles（世界人権の原則）をご覧ください。インテルの製品とソフトウェアは、国際的に認められている人権を侵害しない、または侵害の原因とならないアプリケーションのみに使用されることを目的としています。

インテルのテクノロジーを使用するには、対応したハードウェア、ソフトウェア、またはサービスの有効化が必要となる場合があります。

インテル株式会社

〒100-0005 東京都千代田区丸の内 3-1-1
http://www.intel.co.jp/

2023 年 7 月

356212-001JA
JPN/2307/PDF/SE/MKTG/TK