ビジネス概要

第 4 世代インテル® Xeon® スケーラブル・プロセッサー
セキュリティー

ゼロトラスト・セキュリティー戦略の信頼性

インテルの技術活用による、徹底したセキュリティー、ID、プライバシー、コンプライアンス管理の実現。

あらゆる業界のグローバル企業が、より安全でサステナブルなデジタル技術の急速な採用を進め、最新化や画期的なイノベーションの活性化およびビジネス目標の発展を目指しています。イノベーションの多くは、クラウド、エッジ、モバイルでの採用によって推進されますが、個別プロジェクトの多くでサイバーセキュリティーへの厳格な対応が必要になります。実際、企業 にとってサイバーリスクは、ビジネス全体の深刻なリスクとなり、役員レベルの課題となっています。

サイバーセキュリティーは全世界でビジネス目標に組み込まれるようになりました。ゼロトラスト・セキュリティー戦略が確立され、ビジネスの優先事項の保全にはテクノロジーの導入が不可欠です。企業は、ハードウェアとソフトウェアのスタックの最適化に伴い、ビジネスインサイトと意思決定につながるインテリジェンスをより安全に加速する必要があります。

企業が規模の拡大、コストの削減、新しいサービスの提供を目指す中、テクノロジーによる持続的なビジネス価値の向上は、かつてないほど重要です。セキュアでスケーラブルなプラットフォームを使うことにより、企業は現在および将来においてさまざまなシステムの拡張に求められるパフォーマンスを実現することができます。新しいアプリケーション向けにシステムをカスタマイズして複雑化してしまうリスクを回避することができるのです。

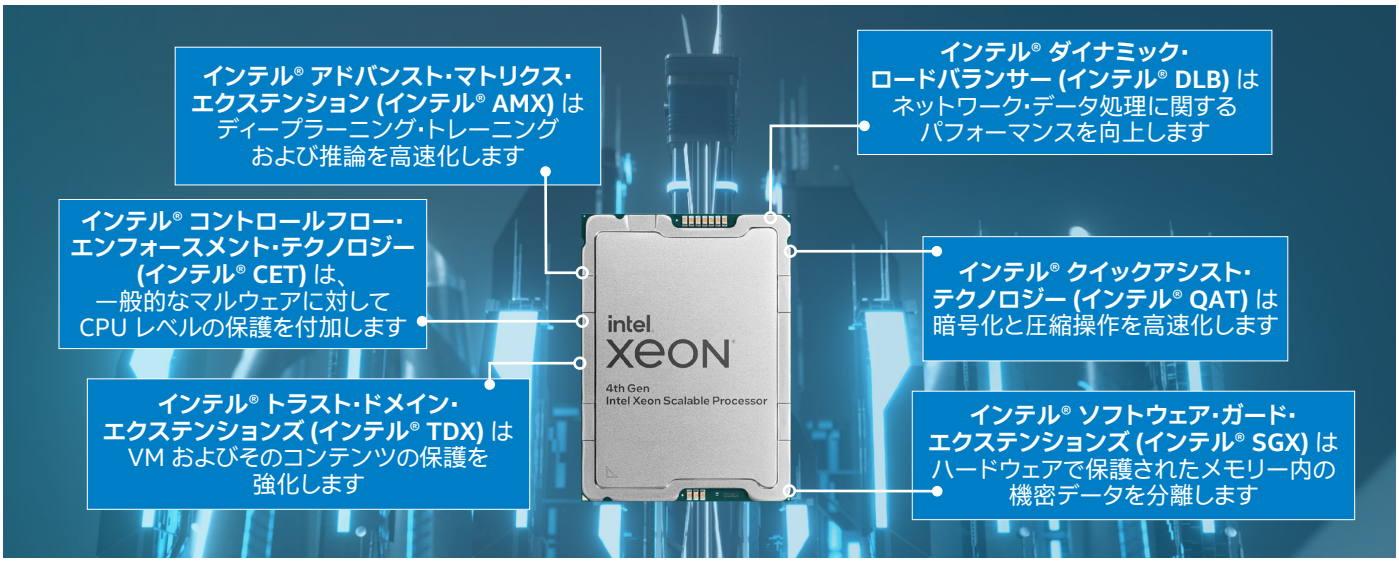
63% の企業が **サイバー攻撃を経験**[1]

37 日間 + **$2.4M** **攻撃からの回復に要する平均値**[1]

88% の役員が **サイバーセキュリティーをビジネスの優先事項と認識**[2]

インテルのテクノロジーによりセキュリティー・アプローチを加速

ビジネスを守り、確信を持てるイノベーションを。企業がオンプレミスあるいはクラウドのどちらを導入していても、データ保護とコンプライアンスの準拠はますます重要です。第 4 世代インテル® Xeon® スケーラブル・プロセッサー・ファミリーを採用したデータセンターは、絶えず変容する脅威の中で、先進の検証済みのセキュリティー技術でデータ保護を実現しながらビジネスのコラボレーションやインサイトを得る新たな機会を引き出します。たとえば、機密データや規制されたデータを使っているような場合でもデータ保護をサポートします。最新の内蔵アクセラレーターにより、AI、分析、ネットワーク、ストレージ、HPC などの急速に増加するワークロード・タイプ全般においてパフォーマンスを強化します。



主要なセキュリティーのユースケース

データ保護

精密さや高速製造を必要とする自動化機能向けにデータプロセスの確保が重要な製造業、あるいは患者の電子カルテを保護する上でデータの安全性が不可欠な医療分野など、あらゆる業界において自社および顧客のデータ保護は最優先事項です。

パフォーマンス・プルーフポイント

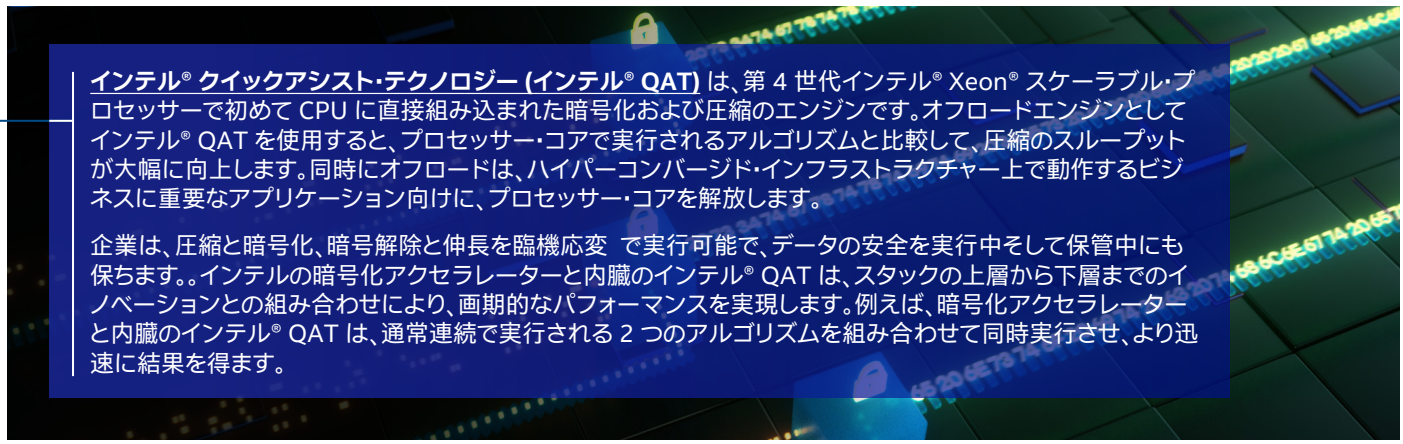
最大 **95%** 少ない コア数 ＋ 最大 **2 倍** 高いレベルの 1 圧縮スループット

インテル® QAT を使用した第 4 世代インテル® Xeon® Platinum 8490H と前世代との比較[3]

要求 :

企業が行う最新化に伴い、コンピューティング、ネットワークおよびストレージのインフラを集約が必要です。まとまりのある自動化された効率的な管理の導入です。集約されたインフラストラクチャーにおいて、保管時、移動時、使用時など、あらゆる段階でのデータの保護が重要です。また、これにより重要なワークロードのパフォーマンスを損なわれることがあってはなりません。ハイパーコンバージド・インフラストラクチャー (HCI) は、通常、この最新化されたインフラストラクチャーのオンプレミスとエッジで使用され、大規模なハイブリッド・クラウド導入の一環として、データベース、分析、エンタープライズ・リソース・マネジメント (ERP) またはカスタマー・リレーション・マネジメント (CRM) のソフトウェア、バーチャル・デスクトップ (VDI) あるいは生産性やコラボレーションのアプリケーションなど、幅広いワークロードをサポートします。

回答 :



インテル® クイックアシスト・テクノロジー (インテル® QAT) は、第 4 世代インテル® Xeon® スケーラブル・プロセッサーで初めて CPU に直接組み込まれた暗号化および圧縮のエンジンです。オフロードエンジンとしてインテル® QAT を使用すると、プロセッサー・コアで実行されるアルゴリズムと比較して、圧縮のスループットが大幅に向上します。同時にオフロードは、ハイパーコンバージド・インフラストラクチャー上で動作するビジネスに重要なアプリケーション向けに、プロセッサー・コアを解放します。

企業は、圧縮と暗号化、暗号解除と伸長を臨機応変　で実行可能で、データの安全を実行中そして保管中にも保ちます。。インテルの暗号化アクセラレーターと内臓のインテル® QAT は、スタックの上層から下層までのイノベーションとの組み合わせにより、画期的なパフォーマンスを実現します。例えば、暗号化アクセラレーターと内臓のインテル® QAT は、通常連続で実行される 2 つのアルゴリズムを組み合わせて同時実行させ、より迅速に結果を得ます。

パフォーマンス・プルーフポイント

最大 **2.5 倍** スループット (RPS) の向上

最大 **74%** P99 のレイテンシー を低減

最大 **12%** CPU 使用率 を低減

第 4 世代インテル® Xeon® Platinum 8480+ プロセッサー上で 2 つのインテル® クイックアシスト・テクノロジー (インテル® QAT) デバイスによりアクセラレーションなしのソリューションと比較[4]

コンフィデンシャル・コンピューティングによる事業目的の保護

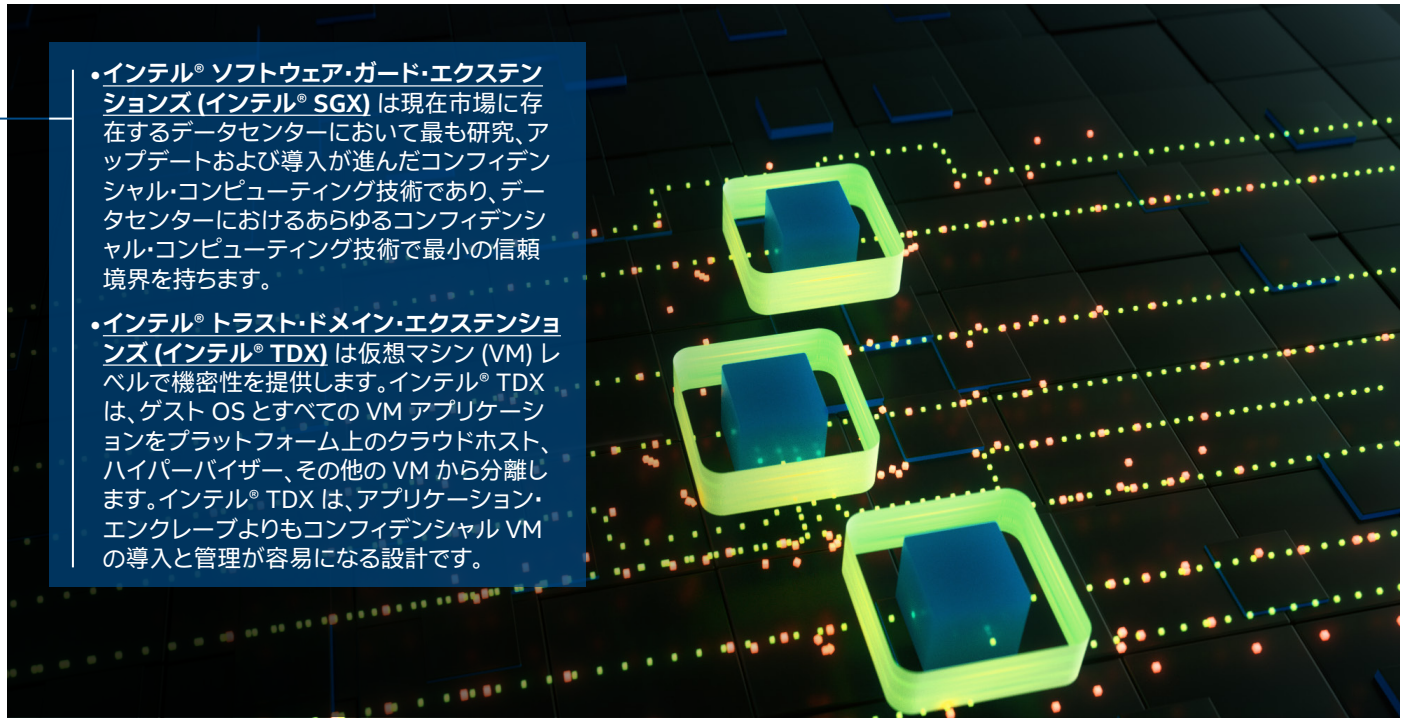
企業は、ゼロトラスト・セキュリティー戦略の一環として、厳格なセキュリティー、ID、コンプライアンスの管理に力を注いでいます。コンフィデンシャル・コンピューティングにより、政府機関のデータの安全を保持したり、金融機関や銀行の顧客のトランザクション・データを保護するなど、多くのビジネス目的において、データ・プライバシー、セキュリティー、コンプライアンスを確保できます。

要求：

コンフィデンシャル・コンピューティングは、ハードウェアベースのメモリー保護により機密データの分離を強化します。企業は、機密性データや規制されたデータをクラウドで共有する必要がある一方、アクセス制限されたエンクレーブ内でより効果的に保護を続ける必要があります。データは、イノベーションと進歩の原動力です。企業は、詐欺行為の検出や、より応答性に優れたサプライチェーンの開発、画期的な AI モデルのトレーニングなど、あらゆるチャレンジの達成にデータを活用しています。したがって、革新的なソリューション、プロセスの自動化、そして心地よいカスタマー・エクスペリエンスの提供ペースを加速しながら、データのプライバシーおよびコンプライアンスを厳格に確立するのは、テクノロジーの最新化を図る企業の最優先事項の 1 つです。

回答：

保管中や転送中のデータに対する従来の暗号化とは異なり、コンフィデンシャル・コンピューティングは、使用中のデータの保護やプライバシーを強化する設計です。こうしたプライバシーの保護は、分散型ネットワークにおいて規制されたデータやその他の機密データを含むワークロードを継続的に保護する上で非常に重要で、費用、スケーラビリティー、俊敏性などのクラウドの利点を活用できます。インテル® SGX およびインテル® TDX により、インテルのコンフィデンシャル・コンピューティング技術の幅広いポートフォリオから、企業はビジネスニーズと規制要件を満たすセキュリティー・レベルの選択が可能です。



- **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)** は現在市場に存在するデータセンターにおいて最も研究、アップデートおよび導入が進んだコンフィデンシャル・コンピューティング技術であり、データセンターにおけるあらゆるコンフィデンシャル・コンピューティング技術で最小の信頼境界を持ちます。
- **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)** は仮想マシン (VM) レベルで機密性を提供します。インテル® TDX は、ゲスト OS とすべての VM アプリケーションをプラットフォーム上のクラウドホスト、ハイパーバイザー、その他の VM から分離します。インテル® TDX は、アプリケーション・エンクレーブよりもコンフィデンシャル VM の導入と管理が容易になる設計です。

さらに、**インテル® コントロール・フロー・エンフォースメント・テクノロジー (インテル® CET)** はゼロトラスト・セキュリティー戦略に貢献し、エンクレーブ外で実行されるソフトウェアの脅威防御機能を拡張します。マルウェアで広く使用される手法である制御フロー・ハイジャック攻撃を通じて、正規コードの悪用からの防御に役立ちます。

ネットワーク管理とネットワーク・セキュリティー・アプライアンス

将来、新しいデジタルや自動化の体験は、いつでも、どこでも、どのデバイスでも動作するセキュリティー、コラボレーション、そしてコミュニティー環境を必要とします。従業員、サプライヤー、パートナー、顧客は、「総合的な体験」を提供するプラットフォームを必要としています。それぞれの目的を満たす、安全性と柔軟性に優れ、テクノロジーやデータを効率的に提供するパワフルで適応力のあるツールを装備したプラットフォームです。それは業務上の快適につながります。

要求 :

ネットワークやデータへのより安全なリモートからのアクセスの必要性は、接続性の向上とセキュリティー技術への必要性を伴います。これらの機能により、企業はあらゆる場所からサービスを安全かつ効率的に管理し、必要に応じた最新のレポートを得られます。導入と管理がさらに容易になり、互換性も実質的にすべてのネットワーク接続デバイスと可能で、パフォーマンス、セキュリティー、スケーラビリティーの目標達成を助けます。

パフォーマンス・プルーフポイント

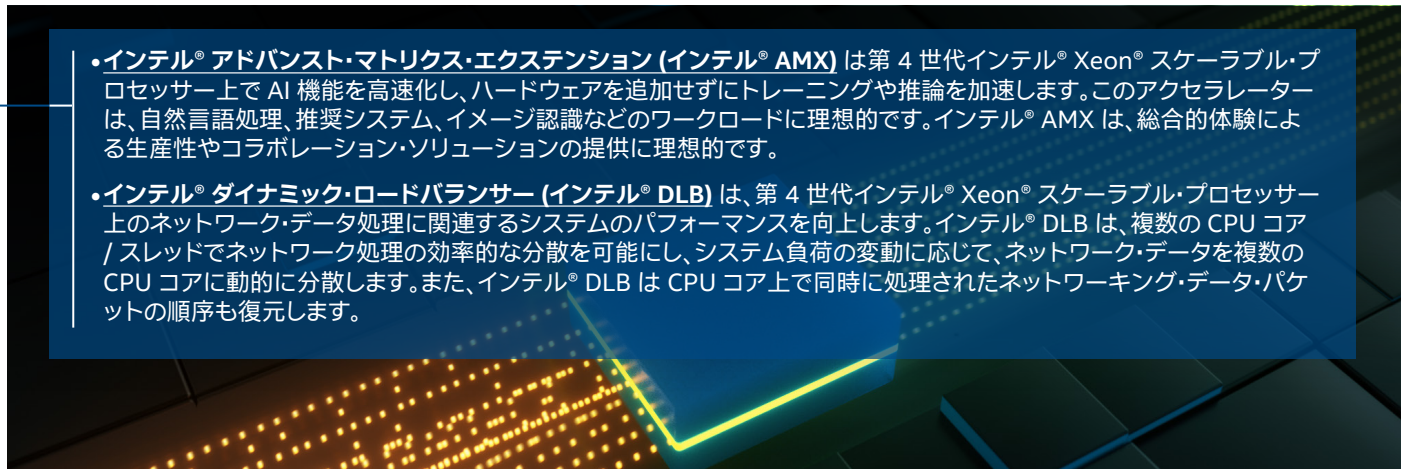
5.7 倍から 10 倍 の PYTORCH リアルタイム推論のパフォーマンス向上[5]

3.5 倍から 10 倍 の PyTorch トレーニングのパフォーマンス向上[6]

内蔵インテル® AMX (BF16) と前世代 (FP32) との比較

回答 :

ネットワーク・セキュリティー・アプライアンスのネットワークとアプリケーションのセキュリティーを保護し、暗号化トラフィックを迅速に処理して、ネットワーク分析、コンテンツ検査、マルウェア検出に AI 主導のアプローチを採用することができます。第 4 世代インテル® Xeon® スケーラブル・プロセッサー・ファミリーは、新しい命令、より高速な DDR5 メモリー、PCIe Gen 5 帯域幅により、高いパフォーマンスとスルー プットを提供します。新しい内蔵アクセラレーターにより、AI、暗号化、ロードバランスが高速化し、CPU コアリソースを解放しながらパフ ォーマンスを最適化します。



- **インテル® アドバンスト・マトリクス・エクステンション (インテル® AMX)** は第 4 世代インテル® Xeon® スケーラブル・プロセッサー上で AI 機能を高速化し、ハードウェアを追加せずにトレーニングや推論を加速します。このアクセラレーターは、自然言語処理、推奨システム、イメージ認識などのワークロードに理想的です。インテル® AMX は、総合的体験による生産性やコラボレーション・ソリューションの提供に理想的です。
- **インテル® ダイナミック・ロードバランサー (インテル® DLB)** は、第 4 世代インテル® Xeon® スケーラブル・プロセッサー上のネットワーク・データ処理に関連するシステムのパフォーマンスを向上します。インテル® DLB は、複数の CPU コア / スレッドでネットワーク処理の効率的な分散を可能にし、システム負荷の変動に応じて、ネットワーク・データを複数の CPU コアに動的に分散します。また、インテル® DLB は CPU コア上で同時に処理されたネットワーキング・データ・パケットの順序も復元します。

さらに

インテル® Optane™ パーシステント・メモリーを追加しデータセットの増加に合わせて手頃な値段でメモリー容量を増やせば、同等のシステム費用でより多くの VM を使用できます。[7] ネットワーク、ストレージ、演算性能をさらに強化するために、CPU の使用率を改善しながら、インテル® インフラストラクチャー・プロセシング・ユニット (インテル® IPU) に重いタスクをオフロードします。

既存のインフラストラクチャーとの容易な統合

セキュリティー技術は、ゼロトラスト・セキュリティーのフレームワークや戦略に貢献し、セキュリティー文化に対して責任あるアプローチを実現します。

インテルは、革新を続け、安全な基盤を構築し、ID、アクセス、コンプライアンス管理で機能するデータ層やインフラストラクチャー層にセキュリティー・ソリューションを提供します。導入準備が整えば、適切なコンサルティング、ガイダンス、具体的な手順で迅速かつ確実な最新化をサポートします。インテル® パートナー・アライアンスが提供する、AI、クラウド、ハイパフォーマンス・コンピューティング、その他のソリューション領域に関する会員限定のリソースは、顧客に向けたさらなる価値のプランニング、構築、提供を助けます。大規模なパートナー関係、ソリューション、経験により、インテルは安全で持続可能なビジネスの優先事項の実行を助けます。テクノロジーや全世界に広がる大規模なパートナー関係 (CSP, ISV, SI, OEM など) を活用し、ビジョンやイノベーションを現実に変えます。

裏付けとなる統計データ

インテルの豊富な選択肢は **50,000 以上の**インスタンス・タイプ、サイズ、地域など多岐にわたります。競合との比較において **6 倍の規模**。[8]

デジタル・トランスフォーメーション行程における経営者のビジネス優先事項

企業のリーダー (テクノロジーとビジネス双方) によるデジタル・トランスフォーメーションへの投資は、2022年から 2024年の間に 6.3 兆米ドルに達し、2024年までにすべての IT 支出の 55% を占めると予想されています。[9] このビジネス概要は、変革の進む将来におけるビジネスの成功のためにリーダーが重視する主なビジネス優先事項と、第 4 世代インテル® Xeon® スケーラブル・プロセッサーなど、インテルのハードウェア、ソフトウェア、サービスがこれらの優先事項の達成を、どのように助けるのかを説くシリーズの一部です。

- **セキュリティー (本資料):** 厳格なセキュリティーを達成し、ゼロトラスト・セキュリティー戦略に貢献
- **AI:** データ分析と AI を採用して重要な成果へと導く
- **クラウド:** ハイブリッド、マルチクラウド、インテリジェント・エッジ全体の戦略の実行
- **従業員体験の再定義:** 境界のないインタラクティブな就業体験の活用
- **ESG:** 環境 | 社会 | ガバナンス (ESG) における公平な成果と責任の醸成

詳細を見る

www.intel.co.jp/xeon/scalable

www.intel.com/security (英語)

[1] Accenture、2019年11月19日。"AI: Built to Scale."https://www.accenture.com/us-en/insights/artificial-intelligence/ai-investments.

[2] AI 推論ワークロードを実行する、世界中に導入されたデータセンター・サーバーのインテルの市場モデリングに基づく (2021年12月時点)。

[3] [N16] は、intel.com/processorclaims (英語) 4th Gen Intel Xeon Scalable processors をご覧ください。結果は状況によって変わります。

[4] [W5] はintel.com/processorclaims (英語) 4th Gen Intel Xeon Scalable processors をご覧ください。結果は状況によって変わります。

[5] [A17] は intel.com/processorclaims (英語) 4th Gen Intel Xeon Scalable processors をご覧ください。結果は状況によって変わります。

[6] [A16] は intel.com/processorclaims (英語) 4th Gen Intel Xeon Scalable processors をご覧ください。結果は状況によって変わります。

[7] 第 3 世代インテル® Xeon® スケーラブル・プロセッサー vs AMD EPYC。構成の詳細 [126-130] は www.intel.com/3gen-xeon-config (英語) をご覧ください。

[8] 出典: Historical Liftr Insights Component tracker data および Intel internal preliminary analysis 2022年9月2日時点。

[9] IDC、2021年10月。"IDC FutureScape: Worldwide Digital Transformation 2022 Predictions." https://www.idc.com/getdoc.jsp?containerId=US47115521.

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、https://www.intel.com/PerformanceIndex (英語) を参照してください。

パフォーマンス実績は構成情報に記載された日に実施した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、公開されている構成情報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やコンポーネントはありません。

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。正確さを評価するには、他のソースを参照する必要があります。

コストと結果は状況によって変わります。

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。

ここに記載されているインテル製品に関する侵害行為または法的分析に関連して、本書を使用または使用を促すことはできません。本資料を使用することにより、ユーザーは、インテルに対し、本資料で開示された内容を含む特許クレームで、その後に作成したものについて、非独占的かつロイヤルティー無料の実施権を許諾することに同意することになります。

説明されている製品には、エラッタと呼ばれる設計上の不具合が含まれている可能性があり、製品が公開されている仕様とは異なる場合があります。現在確認済みのエラッタについては、インテルまでお問い合わせください。

1122/MH/MESH/350497-002US