ハードウェア支援型
エンドポイント・セキュリティー機能を
リモートワーカーに提供する
インテル® vPro® プラットフォーム

最新のインテル® vPro® プラットフォームは、
強化されたセキュリティー環境の中で、
従業員のリモートワーク体験を向上させます。

intel®

オフィス外で仕事をするなら避けられない セキュリティーの優先課題

オフィス回帰の動きが進んでいますが、リモートワークを望む従業員は、今も多くいます。リモートワークによりPCの個人的な利用とビジネスでの利用の境界線が曖昧になっているため、明確なガイドラインやテクノロジーによる保護機能がないと、セキュリティーのリスクが倍増する可能性があります。

- **保護されていないWi-Fiネットワーク:** 自宅、ホテルのロビー、コーヒーショップで仕事をしている人は、ファイルをダウンロードしたり、保護されていないウェブサイトにアクセスしたりして、さまざまな種類の攻撃や不正行為に、その会社のネットワークをさらす可能性があります。また家庭用Wi-Fiネットワークは、多くの場合、複数のデバイス(ルーター、IoTデバイス、スマートホームのデバイス)に接続されているため、侵入を簡単に許してしまう可能性もあります。

- **ファイアウォールがない無防備な接続:** リモートで仕事をしている場合、使用しているデバイスがVPNやファイアウォールのような従来のネットワーク・セキュリティー対策で常時保護されているとは限らないため、多くの企業や組織がゼロトラスト・セキュリティーの原則を採用しています。

- **フィッシング攻撃:** E-メールやテキストメッセージは、認証のなりすましが簡単にできるため、リモートで働く従業員が送信元を確認できないメッセージを開いてしまい、ランサムウェア攻撃の被害に遭う可能性があります。

- **保護されていないデバイス:** データの漏えいやプライバシー侵害などのリスクは、ノートブックPCの画面を通行人に見られてしまう可能性のある公共エリアで座っている場合や、仕事をしている人がノートブックPCのある場所から離れたり、車内に置きっ放しにしたりする場合に発生します。

企業や組織は、これらのリスクを軽減するために、セキュリティー・ソフトウェアをはじめとする、さまざまなベスト・プラクティスやテクノロジーを実装する必要があります。とはいえ、セキュリティー・ソフトウェアが原因でノートブックPCのパフォーマンスが低下することもあります。では、従業員のリモートワーク体験やPCのパフォーマンスを損なうことなく、最新のセキュリティー機能を各PCで活用し、新たな脅威への対策を継続的に更新できるようにするために、企業はどうしたらよいでしょうか。

目 次:

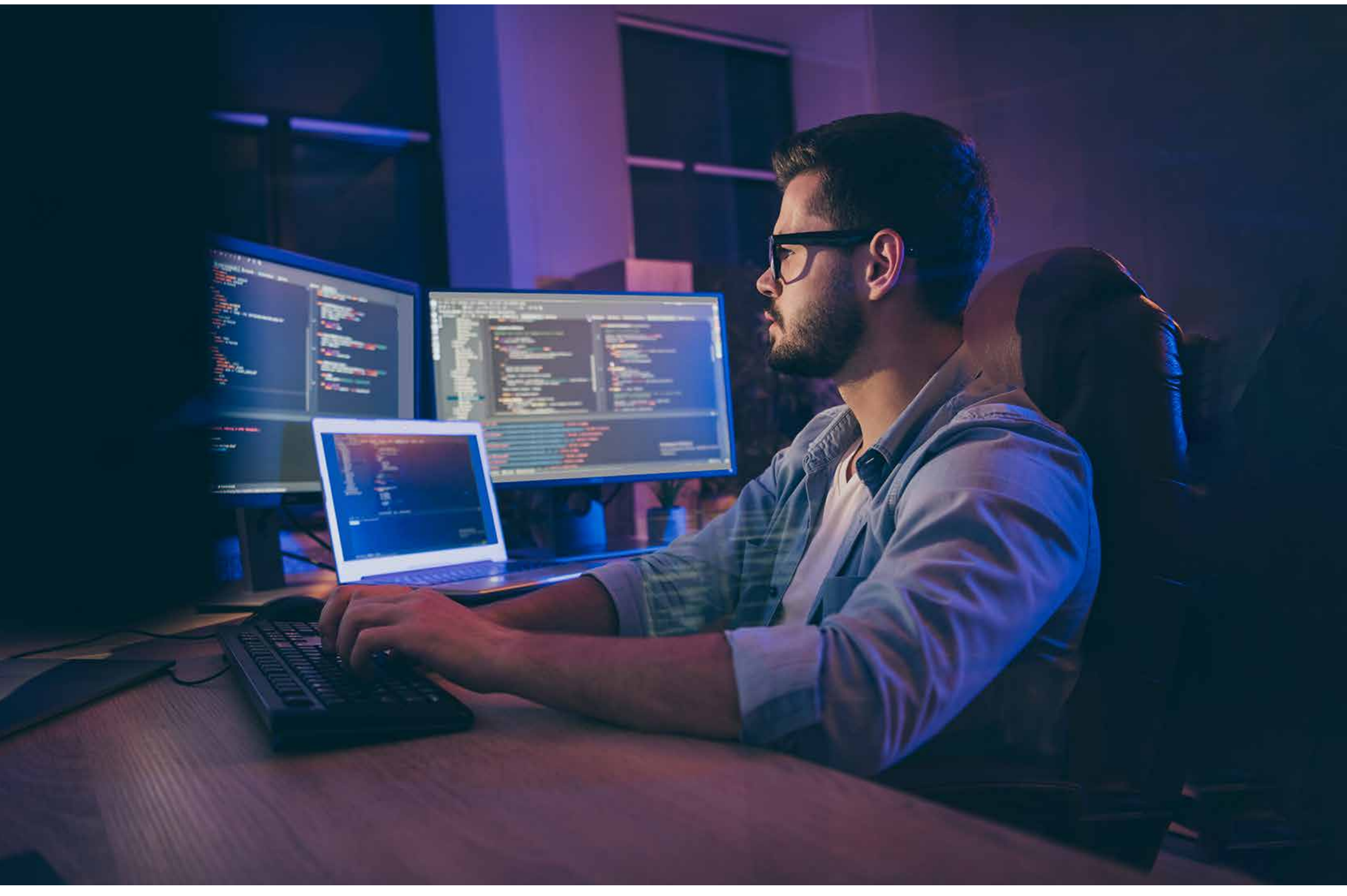
インテル® vPro® プラットフォーム：コンピューティングのセキュリティー確保と管理を行う、現代の働く人のためのテクノロジー

あらゆる企業や組織が、サイバー脅威の阻止、ユーザーの生産性向上、ITにかかる時間とコストの節約を可能にするPCを必要としています。インテル® vPro® プラットフォームは、ユーザーの生産性を維持しながら、ITにかかわる企業や組織がPCをより良く制御できるよう、ハードウェアとソフトウェアのテクノロジーを統合したビジネス・コンピューティングの基盤です。インテル® vPro® プラットフォームは、ハードウェア支援型の保護機能により、導入直後からPCとデータを保護します。

また、リモート管理機能が搭載されているため、さまざまな場所で働く従業員を遠隔からサポートできます。[1] 独自のハードウェア・ベースの多層セキュリティー機能を兼ね備え、リモートワークのパフォーマンス維持に貢献します。

インテル® vPro® プラットフォームは、Windows Hello Enhanced Sign InやMicrosoft Active Directory for Windows Serverといったフェデレーションの ID ソリューションをサポートし、スタックのあらゆる層におけるセキュリティーを強化します。さらに、その次の層の保護もサポートしています。例としては、Microsoft Defender for Businessやオペレーティング・システム（OS）下層のOEM製セキュリティー・ソフトウェアの統合といった、エンドポイント検知・対応（EDR）ソリューションが挙げられます。

数百人を対象に調査を行ったところ、インテル® vPro® プラットフォームを搭載したノートブックPCやデスクトップPCの方が未搭載のPCに比べて高速で優れていたと回答した人は91%に上りました。[2]



仕事用 PC のセキュリティー強化

インテル® vPro® プラットフォームは、さまざまな場所にいるリモートワーカーのために設計された包括的なセキュリティー機能を通じて、あらゆる場所にある PC を保護することが可能です。この機能を利用すると、企業は離れた場所にあるデバイスにパッチを適用し、セキュリティー対策を最新の状態に更新し続けることができます。インテルは、パフォーマンスを向上させ、ユーザー・エクスペリエンス (UX) を損なうことなく、セキュリティー機能の効果を高められるよう、業界をリードする EDR ソリューションと連携を図っています。

何より優れている点は、機能の多くは導入直後から使用可能な状態になっているため、企業や組織側で実装を簡素化できることでしょう。

表 1. インテル® vPro® プラットフォームのセキュリティー機能のほとんどは実装済みで、構成は不要

インテル® vPro® プラットフォームのセキュリティー・テクノロジー	導入直後から使用可能
インテル® ハードウェア・シールド	✓
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)	✓
インテル® スレット・ディテクション・テクノロジー (インテル® TDT)	✓

インテル® ハードウェア・シールド

インテル® ハードウェア・シールドは、コンピューティング・スタック全体を保護するためのテクノロジー群です。インテル® ハードウェア・シールドは、ソフトウェア・ベースのセキュリティーとは異なり、OS 下層のセキュリティー機能を提供し、ファームウェア・レベルやハードウェア・レベルに対する攻撃に有効です。またハードウェア・アクセラレーターを用いた仮想暗号化により、アプリケーションやデータを保護する機能も提供し、高度な脅威の検知と保護を行い、最適なパフォーマンスを維持します。

OS 下層のセキュリティーが重要な理由とは

OS 下層のセキュリティー機能は、ハードウェアやファームウェアに対する不正な変更を特定し、Unified Extensible Firmware Interface (UEFI) の保護機能や可視性を利用することにより、コード・インジェクションの防止につなげています。インテル® vPro® プラットフォームの機能の多くは、OEM がバンドルで提供する OS 下層のセキュリティー・パッケージで利用されています。

図 1. インテル® vPro® プラットフォームに搭載されたインテル® ハードウェア・シールドは、OS 下層を含む、あらゆる層で PC を保護

インテル® スレット・ディテクション・テクノロジー(インテル® TDT)

インテル® TDT は、ハードウェア・ベースの監視機能を利用して、悪意のある行為を検知・防止することにより、ランサムウェア、クリプトマイニング、メモリースキャン攻撃の防止に役立っています。

インテル® TDT は、ハードウェアのテレメトリーやアクセラレーション機能を利用する一連のテクノロジーです。生データを収集して分析、ポリモーフィック・マルウェア、クリプトマイニング、ファイルレス・スクリプト、そのほかの標的型攻撃をリアルタイムで特定し、エンドユーザーへの影響を最小限に抑えます。

インテル® TDT では、誤検知アラートを減らすために、マシンラーニング(ML)ヒューリスティックを活用しています。また Microsoft Defender for Endpoint、CrowdStrike、Fidelis といったエンドポイントデバイスを継続的に監視する、エンドポイント検知・対応(EDR)ソリューションのパフォーマンス向上にも役立っています。メモリースキャン機能を、CPU から補助的なグラフィックス・プロセシング・ユニット(GPU)にオフロードする処理を通じて、セキュリティー・ソフトウェア・ソリューションのリソース消費を減らし、従業員の UX を全体的に向上させています。

EDR ソリューションは CPU のメモリースキャン・パフォーマンスを4倍から7倍ほど向上させることができるため、必要に応じてより幅広く、スキャンを使用することが可能になります。[3] 例えば CrowdStrike は、最近、CrowdStrike Falcon sensor for Windows にインテル® TDT のアクセラレーテッド・メモリー・スキャンを導入しました。可視性を向上することでメモリー内の脅威を検知できるようにして[4]、2022年に検知された全攻撃の71%を占めるファイルレス脅威に対して保護を行う、新たな層を追加するためです。[5]

インテル® TDT は EDR ソリューションと連携し、既知の攻撃と未知の攻撃の最大97%を検知できました。[6]

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）

インテル® CET は高度な緩和テクノロジーであり、いわゆるリターン指向プログラミング、ジャンプ指向プログラミング、コール指向プログラミング（ROP/JOP/COP）攻撃に対する保護に貢献しています。このような攻撃はメモリーの安全性の脆弱な部分を悪用し、一般的にはブラウザーや会議ツールといった接続アプリが狙われます。

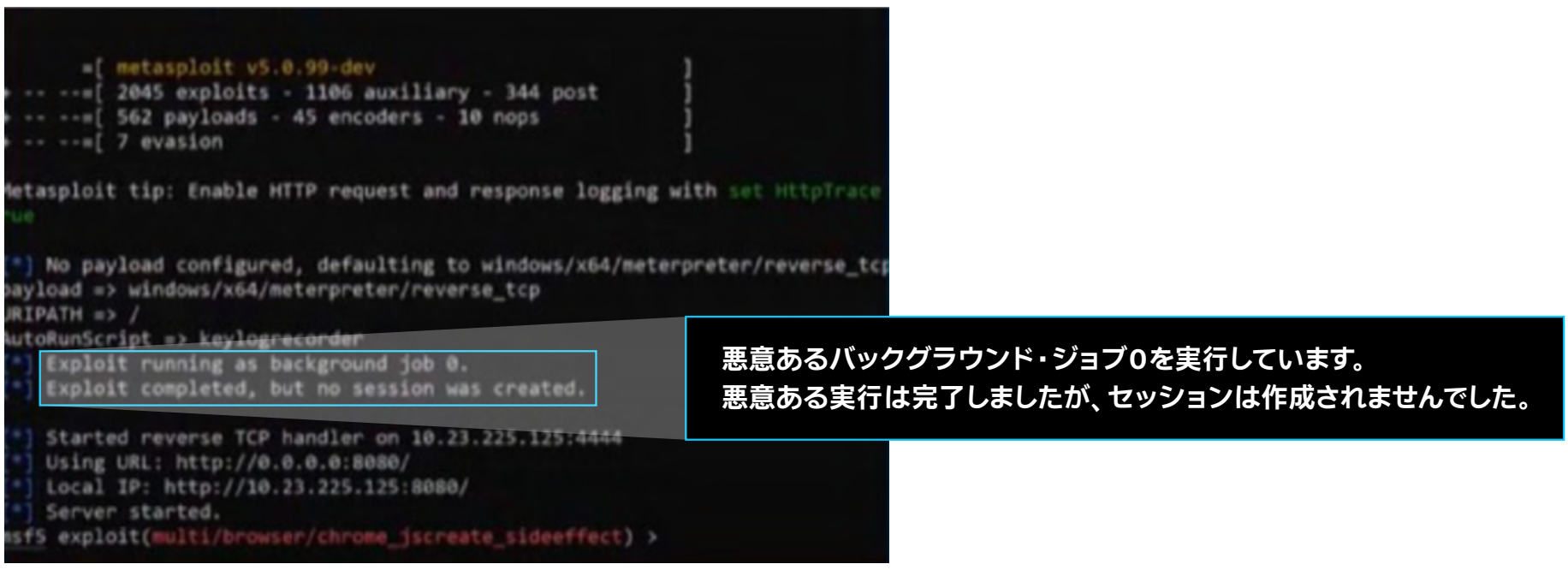


図2. ブラウザーのリンクをクリックする行為など、検知が困難で実行が容易な攻撃のリスクを軽減するインテル® CET

例えば攻撃者は、実行可能なメモリー上で実行されている既存コードの一部を利用して、システム・コンポーネントを改変することが可能です。このような攻撃は長い間、ソフトウェア・ベースのセキュリティーをかいくぐってきたため、特に警戒が必要です。

インテル® CET は、ソフトウェアのセキュリティー機能を補完して、ROP/JOP/COP 攻撃に対応すると同時に、より高いレベルのセキュリティーを提供します。[7] あるレポートによると、インテル® CET の実装は「ROP やそのほかのコントロールフロー・ハイジャック・テクノロジーの使用を排除する大きな一歩」と考えられています。[7] インテル® CET は Microsoft によって Windows OS に採用され、Windows10 バージョン 20H1 以降に導入されています。また Linux カーネルをサポートするようにも開発されており、Google Chrome および関連ブラウザーの、セキュリティー上重要なブラウザーに対応しています。[7]

インテル® バーチャライゼーション・テクノロジー（インテル® VT）

リモートワークによって、仮想化ベースのセキュリティー（VBS）の普及に拍車がかかっています。ITチームは、Windows 10 やWindows 11 に対応するポリシーを利用しながら、インテル® vPro® プラットフォームのセキュリティー機能を有効活用することが可能です。インテル® VT はインテル® vPro® プラットフォームを搭載しているPCで利用可能です。アクティビティーのパーティショニング、ワークロードの分離、組込み管理、レガシー・ソフトウェアの移行、災害時のリカバリーの使用に対応できるようになります。企業は、仮想化を通じ、1台のサーバー上の独立したパーティションに複数のオペレーティング・システムや複数のアプリケーションを実行させられるため、ワークロードの分離が可能になり、マルウェアが簡単に拡散する機会を減らすことができるようになります。分離は、従業員が仕事とプライベートの両方でPCを使用する可能性のあるハイブリッド・ワークでは特に重要です。

仕事での使用とプライベートでの使用を分離

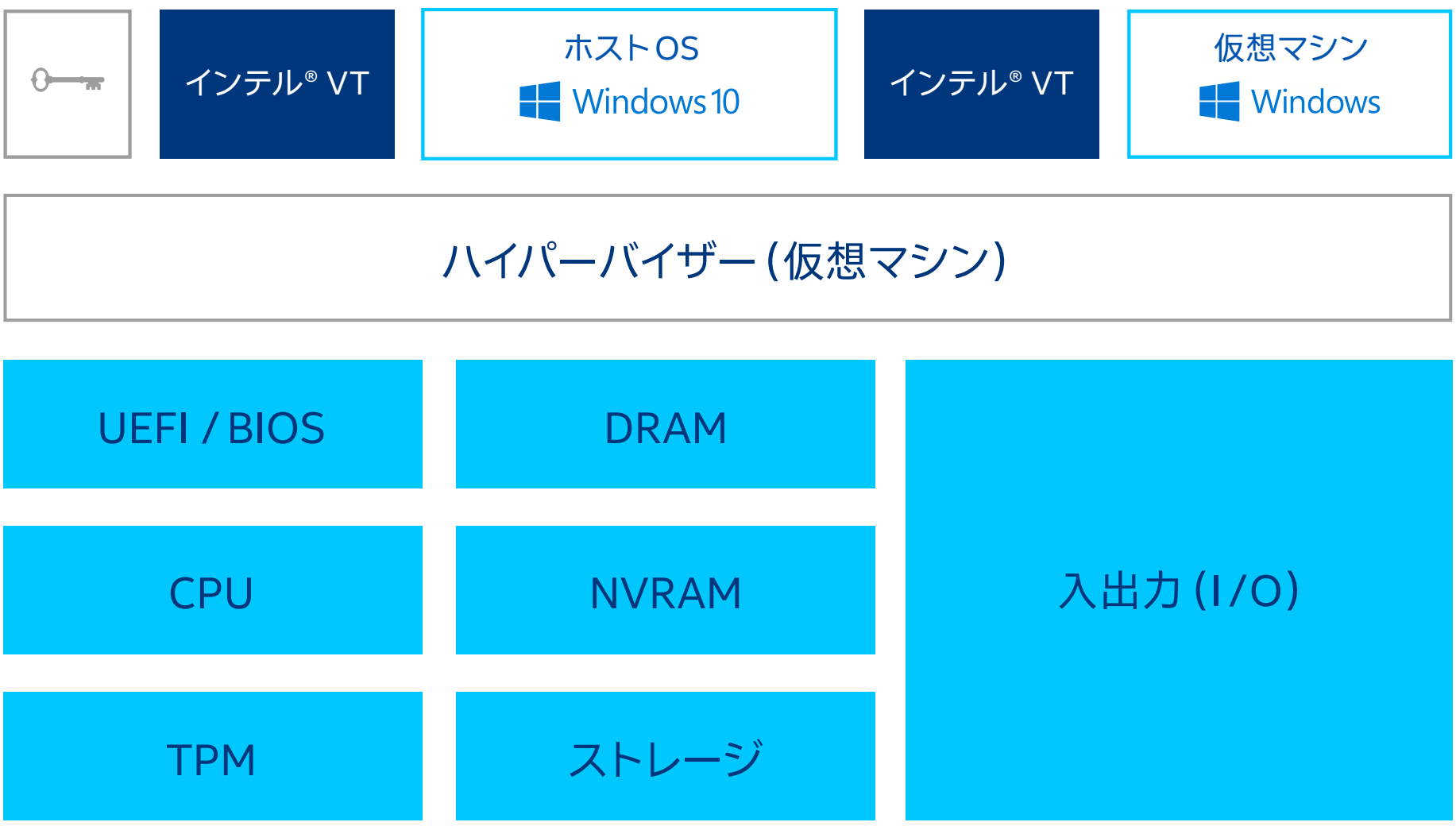


図3. インテル® vPro® プラットフォーム上のインテル® VT がワークロードの分離を可能にし、分離された仮想マシン（VM）の作成をサポートすることにより、攻撃対象領域だけでなく、マルウェアがリソース全体に固着・拡散する可能性も縮小

インテル® トータル・メモリー・エンクリプション - マルチキー (インテル® TME - MK)

インテル® TME-MK は、OS やアプリケーション・データなど、DRAM 内のシステムメモリーのセクションを暗号化して、物理的なコールドブート攻撃から保護します。このテクノロジーを通じて、仮想コンテナや仮想マシンが複数のキーを使用して異なるメモリー領域を暗号化できるようになるため、データを分離してセキュリティーを強化できます。

インテルの Wi-Fi 近接センシング

インテルの Wi-Fi 近接センシングは、リモートワーカーが公共エリアやシェアオフィスにいるときでも、難しい設定なしにデバイスを保護するテクノロジーです。このテクノロジーは、無線信号を利用して周囲の動きを検知します。ユーザーがノートブック PC から離れると、テクノロジーがその動きを感知してデバイスを自動的にロックします。ユーザーが戻ってきて作業を再開すると、この機能が PC のスリープ状態を解除して使用できる状態にします。

インテルの Wi-Fi 近接センシングが、ユーザーのノートブック PC のロックやスリープ解除のタイミングをインテリジェントに検知

Walk Away Lock (立ち去り施錠) 機能[8]

立ち去ったユーザーを Wi-Fi が感知し、PC を数秒でロック

セキュリティー

ユーザーが PC のロックを忘れる → 人の不在を確認 → PC を自動的にロック

Wake on Approach (接近による施錠解除) 機能[8]

戻ってきたユーザーを Wi-Fi が感知し、PC のスリープを数秒で解除

利便性

人の存在を検知 → PC のスリープ状態を自動的に解除 → ログイン画面を表示

インテル® リモート・セキュア・イレース (インテル® RSE)

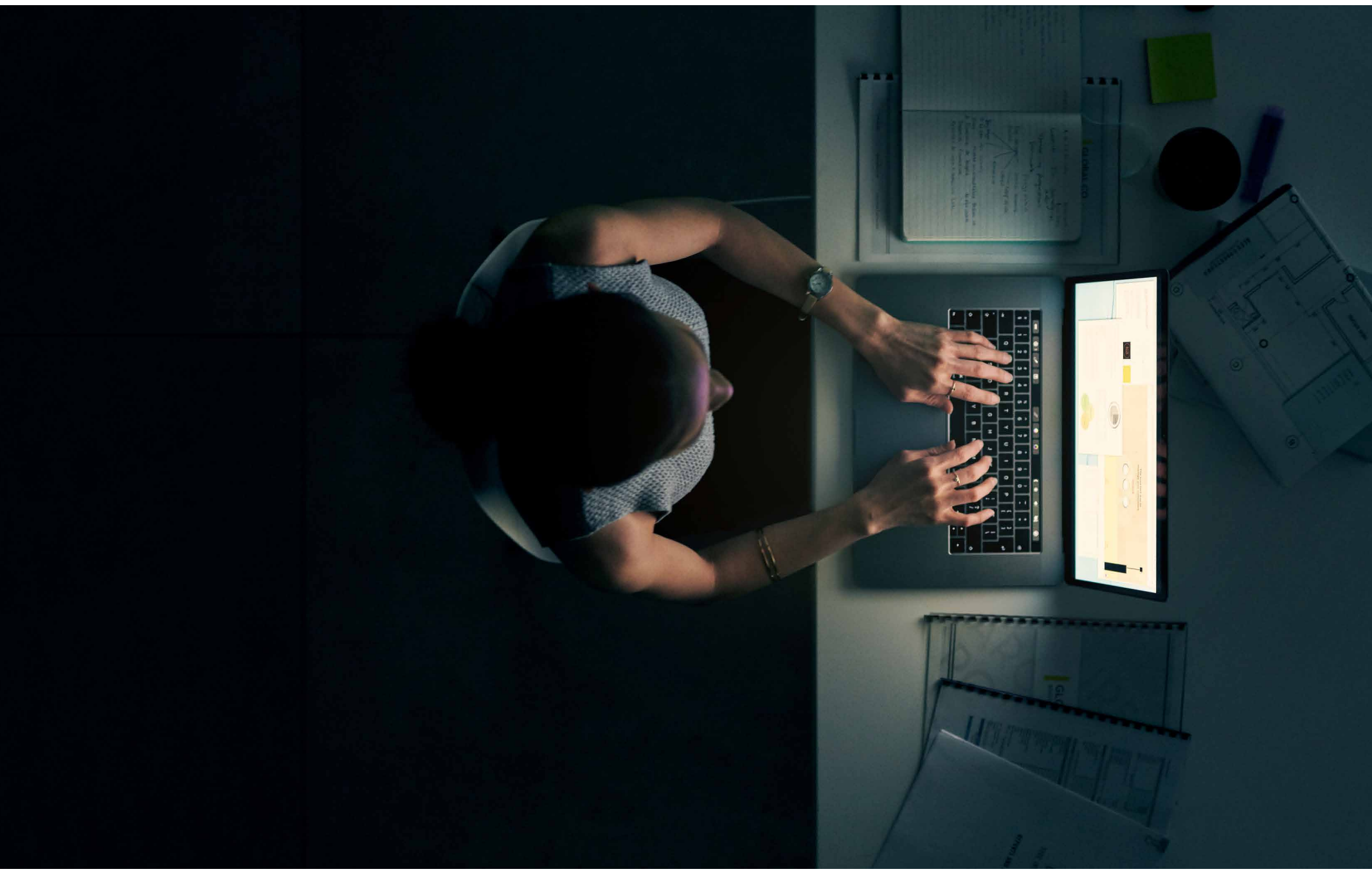
PC を処分する、別の目的に再利用する、修理に出す、紛失したなどの場合、情報セキュリティー・ポリシーでデータの「消去」が求められることが多くあります。消去はその場で作業しても難しく、時間がかかります。リモートでは、ほぼ不可能となるでしょう。インテル® RSE は、リモートでドライブの内容を安全に消去します。インテル® アクティブ・マネジメント・テクノロジー (インテル® AMT) を介して使用可能です。[9]

ゼロトラスト対策により、働く場所を問わずサポート可能に

インテル® vPro® プラットフォームに組込まれているセキュリティー機能は、数種類のハードウェア攻撃対策を通じてPCの攻撃対象領域の縮小に役立っています。インテル® vPro® プラットフォームは、ゼロトラスト・セキュリティーの考えに則り、リモートワークをサポートするように設計されており、ユーザーの認証を確実に行い、各デバイスの健全性とアプリケーションへのアクセスを検証します。

インテル® vPro® プラットフォームにより強化されたセキュリティー機能の有効性は、さまざまな研究を通じて裏付けられています。インテル® vPro® プラットフォームを採用したデバイスを主に使用していて5,000人以上の従業員を抱える企業や組織は、インテル® vPro® プラットフォームを使用していない企業や組織と比較して、セキュリティー侵害の年間平均件数が少ないと報告されています。[10]

- インテルのテクノロジーを使用していない企業や組織では、重大な侵害が年間平均で3.9件報告されているのに対し、インテルのテクノロジーを使用している企業や組織では、年間平均で2.8件となっています。[11]
- インテルのテクノロジーを使用している企業や組織では、外部からの攻撃、内部でのインシデント、サードパーティー・サプライヤーを巻き込んだ攻撃またはインシデント、資産の損失や盗難による侵害を経験する可能性が低い傾向にありました。[12]
- 調査対象となったIT担当者の92%がインテル® vPro® プラットフォームを使って管理するようになったノートブックPCやデスクトップPCは、以前よりも安全性が増したと回答しています。[2]
- インテル® vPro® プラットフォームのハードウェア・ベースのセキュリティー機能をすべて活用すると、攻撃対象領域を最大70%縮小することが可能です。[7]



セキュリティーとパフォーマンスの底上げ

インテル® vPro® プラットフォームが搭載されたデバイスは、リモートワークとセキュリティーが両立するよう設計されています。世代を重ねていくごとに、インテル® vPro® プラットフォームは継続してセキュリティーの改革に注力し、企業が不正行為をはたらく人より常に一歩先にいられるよう、たゆまぬ努力を行っています。業界をリードするOS下層の保護から始まった取り組みは、現在のインテル® Core™ プロセッサー（第13世代）に進化しました。OS上層のセキュリティーを強化するだけでなく、不正行為から企業を守り、ITにかかわる貴重な時間を取り戻すのに貢献します。

インテル® vPro® プラットフォームは、企業のファイアウォールの内側に常駐する各種の機能やセキュリティー機能を最適化することにより、ビジネスにとって極めて包括的なセキュリティーを提供します。[13]

従業員のユーザー・エクスペリエンスとセキュリティーを向上させ、実情にふさわしいビジネス・コンピューティングを実現

インテル® vPro® プラットフォームが採用されている最新PCの詳細をはじめ、
従業員が享受できる利点、ビジネスで得られる利点を紹介しています。

1. インテル® スタンダード・マネージャビリティーとインテル® AMTはどちらも、プロビジョニングされたWindowsPC上のリモート・アウトオブバンド機能をサポートしますが、リモートKVM（キーボード、ビデオ、マウス）制御をサポートするのは、インテル® AMT対応のWindows向けインテル® vPro® Enterpriseプラットフォームのみとなります。
2. アメリカ、イギリス、ドイツ、日本、中国でインテル® vPro® プラットフォームを使用している世界各地の企業のITDM（IT意思決定者）416名を対象に行った調査に基づいています。対象者の92%が「同意する」あるいは「強く同意する」と回答しました。実際の結果は異なる場合があります。出典：Forrester Consulting「エンドポイント標準としてのインテル® vPro® プラットフォームのTotal Economic Impact™（総合的経済効果）」調査依頼：インテル、2021年1月。https://www.intel.co.jp/content/www/jp/ja/business/enterprise-computers/resources/vpro-platform-tei-case-study.html
3. インテル® TDT APIを介した統合GPUにオフロードしたメモリースキャンに基づいており、CrowdStrikeのブログに記載されているとおり、結果としてCPUをスキャンする方法よりも3倍から7倍高速化します。詳細はintel.com/performance-vpro（英語）を参照してください。
4. CrowdStrike「CrowdStrike Falcon® Enhances Fileless Attack Detection with Intel Accelerated Memory Scanning Feature」2022年3月。crowdstrike.com/blog/falcon-enhances-fileless-attack-detection-with-accelerated-memory-scanning/（英語）
5. CrowdStrike「2023 Global Threat Report」2023年。https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf（英語）
6. SE Labs「Enterprise Advanced Security（Ransomware）：Intel」2023年2月。https://selabs.uk/reports/enterprise-advanced-security-ransomware-intel-threat-detection-technology-2023-02/（英語）
7. IOActive「13th Generation Intel Core Attack Surface Study」調査依頼：インテル、2023年3月。intel.com/content/dam/www/central-libraries/us/en/documents/2023-03/ioactive-intel-13th-generation-attack-surface-study-summary-report.pdf（英語）
8. 「Walk Away Lock（立ち去り施錠）機能」と「Wake on Approach（接近による施錠解除）機能」はWindows 11でサポートされています。インテルのWi-Fi近接センシングは、現在インテル® Evo™ デザイン、またはインテル® vPro® プラットフォームが搭載されているWindows PCでのみ利用可能です。
9. お使いのデバイスがインテル® RSEをサポートしているかどうかについては、OEMにご確認ください。
10. Forrester Consulting「インテル® vPro® プラットフォームが実現するハードウェア支援型セキュリティー機能のTotal Economic Impact™（総合的経済効果）」調査依頼：インテル、2022年9月。https://www.intel.co.jp/content/www/jp/ja/business/enterprise-computers/resources/impact-of-vpro-hardware-enabled-security-paper.html
11. 「[プロセッサー]搭載[デバイス]に発生したセキュリティー侵害は、過去1年間、所属する組織で何件ありましたか?」という質問に対し、エンドポイント管理を担当する世界中のIT意思決定者（ITDM）719人が回答した結果に基づいています。出典：2021年、インテルの委託でForrester Consultingによって行われた調査。
12. 「所属する組織が過去12カ月以内に侵害を経験したと、先ほど回答した方に質問です。侵害はその組織でどのように発生しましたか?」という質問に対し、エンドポイント管理を担当する世界中のITDM（IT意思決定者）239人が回答した結果に基づいています。出典：2022年9月、インテルの委託でForrester Consultingによって行われた調査。
13. 2023年3月時点で、インテル® vPro® プラットフォームがあらゆる規模のビジネスに提供している、他社の追随を許さない組み合わせに基づいています。具体的には、OSの上層および下層のセキュリティー機能、アプリの保護、データの保護、脅威に対する高度な保護の組み合わせ、さらに製品の設計、製造、サポートに対するインテルのセキュリティー・ファーストのアプローチが挙げられます。インテル® vPro® プラットフォーム上に構築されるビジネス向けPCはすべて、独自のハードウェア・ベースのセキュリティー機能を含む厳密な仕様に関して検証済みです。詳細はintel.com/Performance-vPro（英語）を参照してください。実際の結果は異なる場合があります。

通知と免責事項

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、www.intel.com/PerformanceIndexを参照してください。

性能の測定結果は構成情報に記載された日付時点のテストに基づくものです。また、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、公開されている追加情報を参照してください。

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。

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。実際のコストと結果は異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。ほかの情報を参考にして、正確さを評価してください。

356510-001JA
JPN/2403/PDF/TAG/MKTG/SI