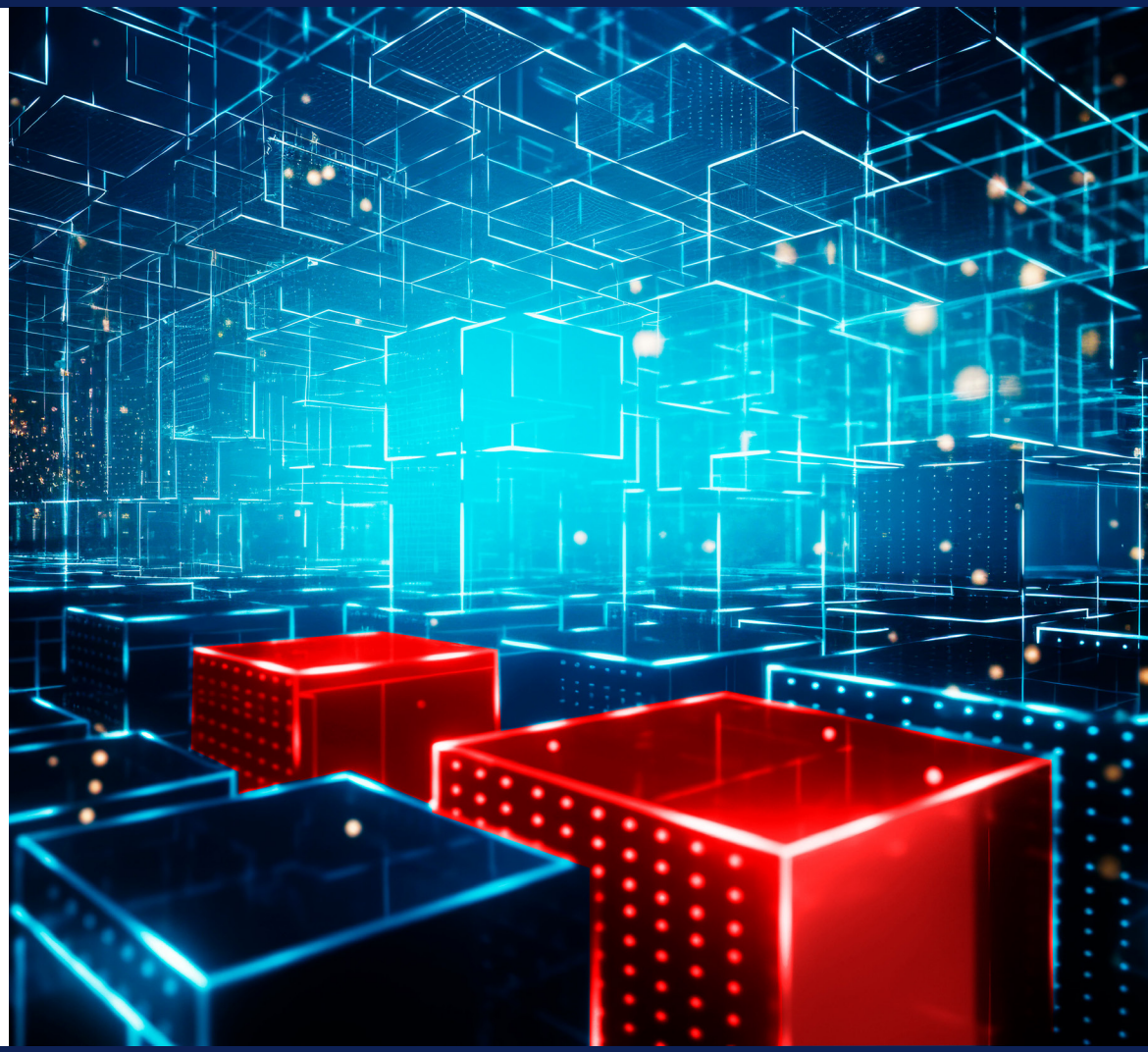
エンドポイントでAIを安全に活用するには

安全な最新デバイスと攻撃者の視点で、
オンデバイスAIワークロードを保護。



概要

オンデバイスAIには大きなメリットがありますが、サイバー リスクも伴います。このe-bookでは、組織の安全を確保してエンドポイントでAIイノベーションを活用する方法を説明します。

目次

オンデバイスAIの攻撃対象領域

潜在的な攻撃対象

最先端テクノロジーは、未知の新しい領域であるがゆえに、必ずサイバーセキュリティリスクが伴います。クラウド コンピューティングやブロックチェーンをはじめとする数多くのテクノロジーで、この現象は確認されています。オンデバイスAIにも同じことが言えます。このリスクを軽減する鍵は、いつものように、未知の領域に光を当てることです。

攻撃対象領域の最小化に必要なセキュリティについて議論する前に、何をなぜ保護するのかを知ることが有益です。オンデバイスAIを取り巻く環境を、複数の企業が入居する商業ビルの配管システムのように考えてください。これらの配管は、建物全体に水やガスを供給するなど、さまざまな用途に使われています。配管を通る物質の汚染や途絶、物質を運ぶ配管の損傷や破損が発生すると、配管は本来の機能を果たせなくなります。配管自体もそこを流れる物質も、それぞれの用途を満たすために正常に機能している必要があります。 ►

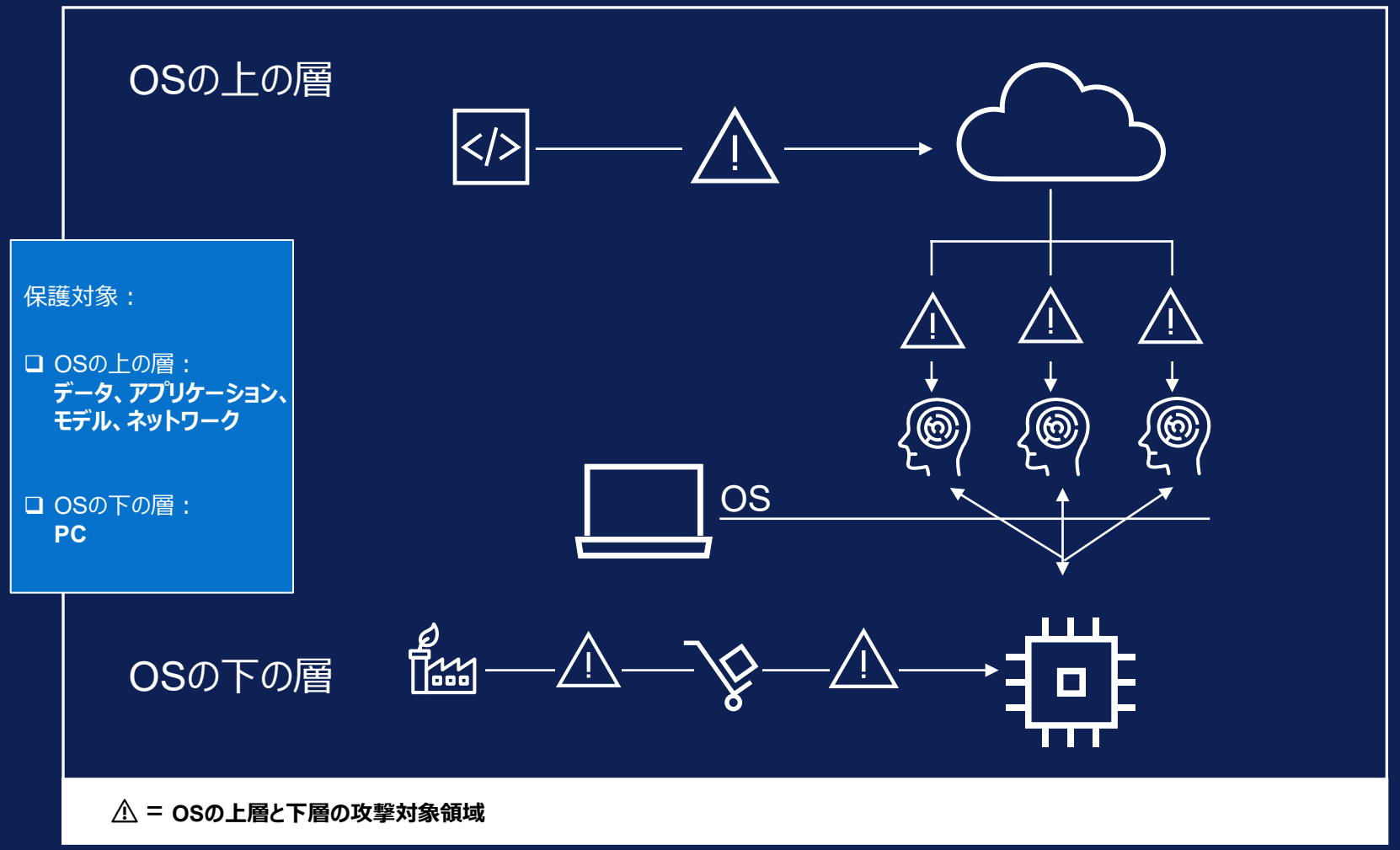
オンデバイスAIの攻撃対象領域（続き）

潜在的な攻撃対象（続き）

エンドポイントのAIに当てはめてみましょう。

- 配管は、お客様のインフラストラクチャ、つまりパソコンや企業ネットワークであり、仕事の手段と場所を提供します。
- 配管を流れる物質は、さまざまなAIユースケースを支えるデータ、アプリケーション、モデルであり、仕事に必要な資産とリソースを提供します。

ご推測のとおり、サイバー攻撃者はその両方を標的にします。身代金目的でIPを盗んで保持したり、データやモデルを改ざんして業務に影響を及ぼしたりする可能性があります。いずれの場合も、その結果は深刻です。財務的な損害や評判の低下をもたらし、規制当局による調査を受けることになりかねません。►



エンドポイントでのセキュリティ リスク

攻撃者の侵入手口

次に、攻撃者が両方の標的にアクセスするために取りうる手口を説明します。

デバイスの侵害。Forrester Research, Inc.の『Endpoint Security Market Insights』（2025年3月）が示すように、パソコンは最新のサイバー脅威の主要な標的の1つです。この種の攻撃は、オンデバイスAIによる処理が開始される前に発生する可能性があります。つまり、**ハードウェアまたはソフトウェアのサプライ チェーン攻撃です。**サプライ チェーンには、悪意のある第三者が回路やファームウェアなどのコンポーネントを改ざんして、後に悪用可能な脆弱性を仕込む可能性のあるポイントが、数百とまではいかなくても数十はあります。ある投資会社に偽造コンポーネントを搭載した新品のパソコンが納入されたらどうでしょうか。大惨事が起きることは想像できます。

IDの侵害。認証情報の盗難または侵害に関連する侵害は、最も急速に増加している攻撃ベクトルの1つです。これは不思議なことではありません。攻撃者も有効な認証情報を使用すれば、パソコンにログインし、企業ネットワーク内を自由に移動して、長期間検出されないまま潜伏できます。IBMの最新の『データ侵害のコストに関する調査』によると、こうした侵害の特定と封じ込めには平均292日かかっており、調査された攻撃ベクトルの中で最長です。このレベルのアクセスは、脅威アクターが無視できない価値があります。実際、Zscalerの調査によると、悪意のある者は生成AIを活用して認証情報の盗難方法を進化させ、フィッシング攻撃を高度化し、拡大しています。機密性の高いトレーニングや推論データ、またはモデル自体に対するこのような不正アクセスは、**モデル サプライ チェーン攻撃**として分類されます。

内部関係者による脅威。最近の調査によると、**悪意のある内部関係者による攻撃**は、他の攻撃ベクトルと比較してコストが最も高く、平均499万米ドルとなっています。内部関係者による攻撃は、ハードウェア サプライ チェーン、ソフトウェア サプライ チェーン、モデル サプライ チェーン全体で発生する可能性があることに注意しなければなりません。►

エンド ユーザーが**フィッシング**Eメールに騙されるまで60秒未満（中央値）*

認証情報の侵害の発見から封じ込めまで平均292日**

悪意のある内部関係者による攻撃のコストは平均499万米ドル**

*出典：*Verizon『2024 Data Breach Investigations Report』*（2024年）
**出典：IBM『データ侵害のコストに関する調査』、2024年

講じるべき対策

リスク軽減要因

これらの攻撃対象は根本的に新しいものではなく、攻撃者の最終目標でもありません。私たちは、いつものように、お客様のデバイスのセキュリティとレジリエンスを確保することに注力したいと考えます。**多層対策**により、攻撃対象領域を縮小し、不審な行動を即座に発見できます。

ゼロトラストの考え方は、すべてのパソコンのリスクを軽減します。決して信頼せず、常に確認し、継続的に監視するというこうした原則により、攻撃者の一歩先を行くことができます。攻撃を完全に阻止することは不可能です。強固なセキュリティ体制を確立するには、ITエコシステム全体の**可視化と制御**が必要です。

そうしたフレームワークを念頭に置いて、インフラストラクチャ（特にAIと連携するシステムおよびプロセス）を再評価してください。どのような対策を講じれば、デバイスの侵害、IDの侵害、内部関係者による脅威のリスクを最小限に抑えられるでしょうか？ ►

ゼロトラスト原則は、リスクに対して防御し、サイバー活動の影響範囲を縮小する上で役立ちます

講じるべき対策（続き）

リスク軽減要因（続き）

対策は大きく2つのカテゴリーに分けられます。

「OSの下層」のセキュリティで、お客様が使用するAIデバイスを保護します。この保護は次の2つの点から行っています。

- **安全に構築された**デバイスを通じて、すべてのパソコンを保護します。これはセキュア バイ デザイン、つまり安全な設計原則に従い、安全なサプライ チェーンで構築されたAI PCを使用することを意味します。
- **セキュリティが組み込まれた**デバイスを通じて、すべてのパソコンを保護します。安全なAI PCには、BIOSレイヤーおよびシリコン レイヤーまで可視化できる保護層が、すぐに使用できる状態で組み込まれています。

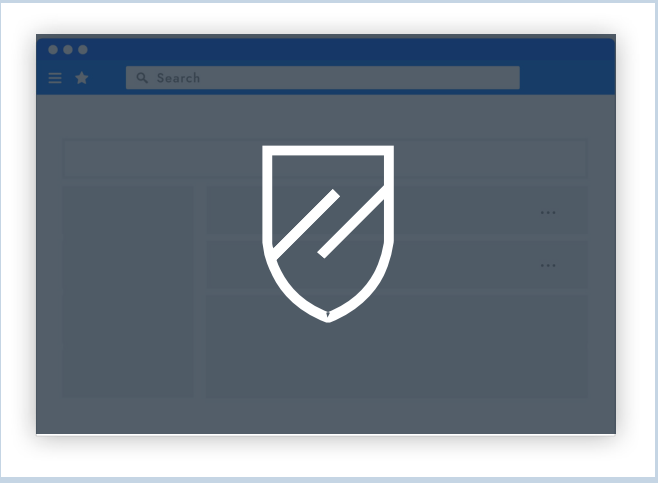
「OSの上層」のセキュリティで、AIモデルへのアクセスを保護します。ソフトウェア セキュリティを通じて、お客様が使用するデータとモデル、企業ネットワークを保護します。機械学習のセキュリティ運用を保護し、導入されたAIワークロードのネットワーク トラフィックを監視することが不可欠です。 ►

OSの下層のセキュリティ

安全なAI PC

ハードウェアとファームウェアのセキュリティ、サプライ チェーンのセキュリティ、コア シリコン

OSの上層のセキュリティ



ソフトウェア セキュリティ

エンドポイント、ネットワーク、クラウド環境向けの追加のセキュリティ レイヤー

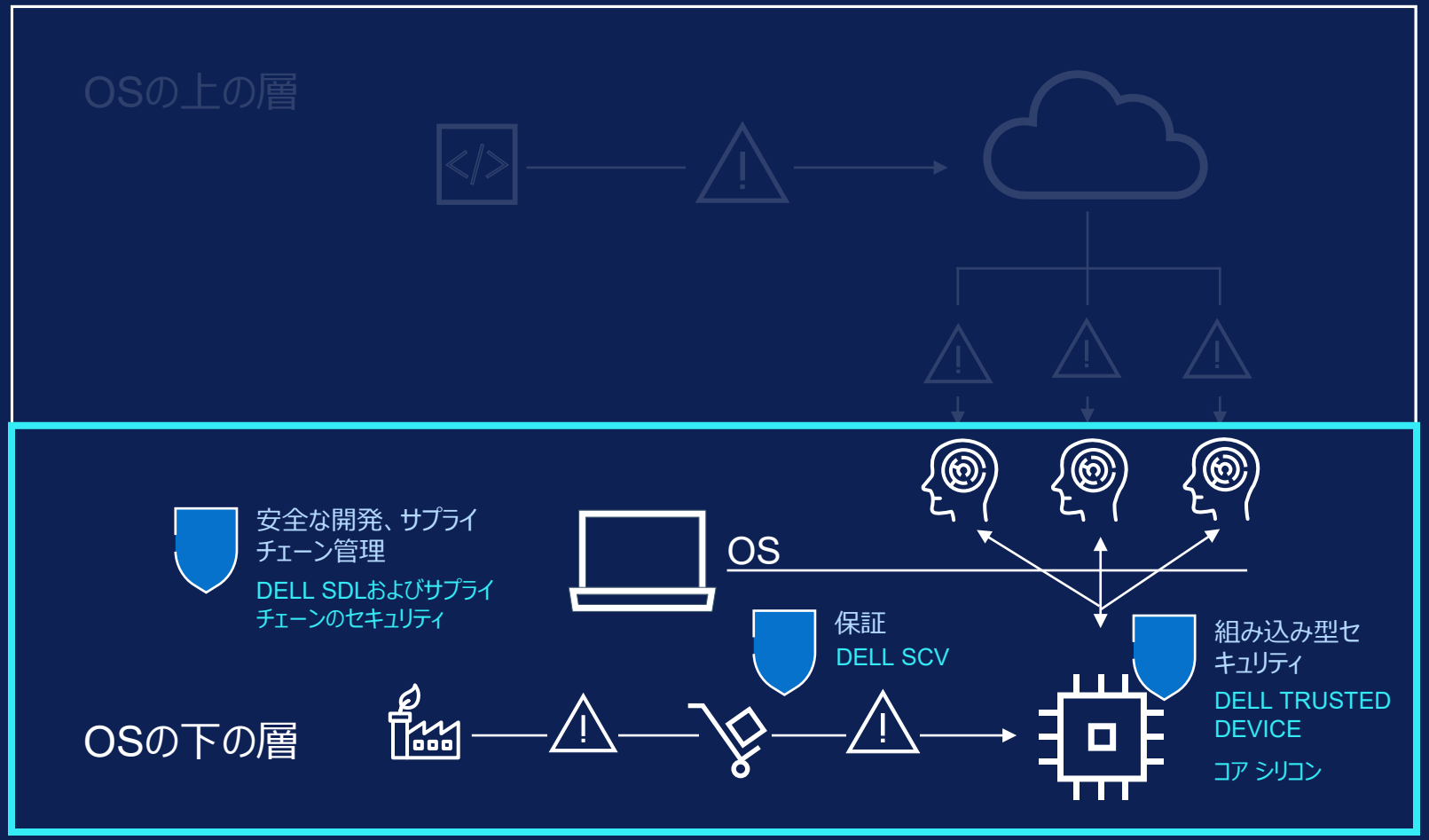
すべてを統合するセキュリティ サービスと専門技術を提供します。

すべてのパソコンへのベスト プラクティス適用

Dell AI PCですべてのパソコンの基盤となるセキュリティを確保する仕組み

これを支援するのがDell Trusted Workspaceです。当社の技術者は攻撃者の視点を深く理解した上で、ビジネス向けAI PCのセキュリティを構想し、設計しています。

OSの下層では、安全な設計、厳格なサプライ チェーン管理、オプションのサプライ チェーン保証で、パソコンの初回起動時からその安全性を確保します。内蔵型のハードウェアとファームウェアのセキュリティで、使用中のパソコンを保護します。例えば、Dell独自*のBIOSレベルの改ざん検出(Dell SafeBIOS)および不正アクセスから保護するパスワードレス認証セキュリティ(Dell SafeID)などがあります。さらに、インテル®シリコン テクノロジーが、AI PCクライアントで使用されるAIのさまざまな側面を保護するための基盤を提供します。例えば、インテルにより、ディスク上のモデル暗号化が高速化し、クライアント上の静止AIデータが保護されます。►



すべてのパソコンへのベスト プラクティス適用（続き）

Dell AI PCですべてのパソコンの基盤となるセキュリティを確保する仕組み（続き）

このOSの下層のセキュリティを補完するために、当社のパートナーであるAbsoluteのPersistenceテクノロジーを工場で組み込み、パソコン ライフサイクル全体の可視性と制御性をさらに向上させることができます。例えば、配送中のデバイスの位置情報取得や最悪のシナリオでの重要なアプリケーションの自動修復などが可能になります。

Dellは、実際にCrowdStrike Falcon XDRやAbsolute Secure Accessなどのソフトウェア パートナー ソリューションのエコシステムを厳選して、ゼロトラスト原則を適用し、モデル サプライ チェーンを**OSの上層**での不正アクセスから保護しています。こうしたソリューションを使用すると、きめ細かなアクセス制御（ロールベースのアクセス制御(RBAC)など）を使用してポリシーを作成、適用し、悪意のある内部関係者がAIモデルに対してアクセスや操作を行うリスクを軽減できます。 ►

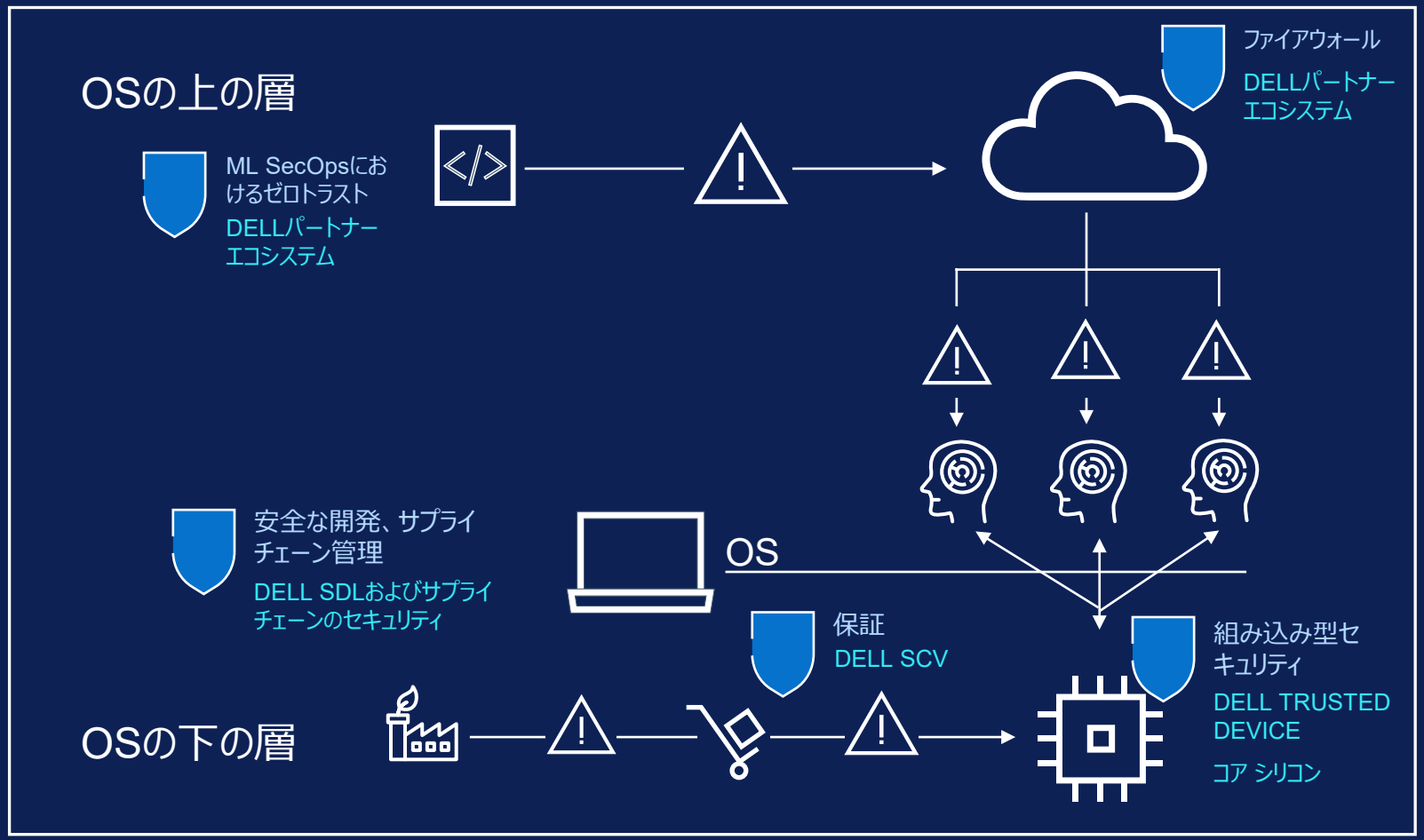
すべてのパソコンへのベストプラクティス適用（続き）

Dell AI PCですべてのパソコンの基盤となるセキュリティを確保する仕組み（続き）

これらが一体となったのが、***AI向けセキュリティです。***こうした機能がオンデバイスAIワークロードをサイバー攻撃から保護するため、お客様はイノベーションとビジネスの成功に専念できます。►

ハードウェアとソフトウェアによる連携防御で高度なエンドポイント攻撃を阻止

DellはインテルおよびCrowdStrikeと連携して、OSの下層と上層をハードウェア支援型セキュリティと統合しています。
詳細はこちら >



重要なポイントと次のステップ

DellでエンドポイントのAIを保護

Absoluteが実施したCISOに関する最近の調査によると、企業はAIに期待しているものの、その対応は遅れています。数百万台のデバイスを分析した結果、パソコンユーザー層が新しいAI機能を広く活用できていないことが明らかとなりました。**Dellはすべてをまとめるお手伝いができます。**

最新の安全な基盤の上でAIモデルを開発、導入しませんか。Windows 10のサポートは2025年10月に終了します。多くのパソコンで、セキュリティ更新プログラム、機能アップデート、Windows 10のサポートを利用できなくなります。古いデバイスはWindows 11の要件を満たしていない場合があり、最新のパフォーマンス、セキュリティ、AIの拡張機能を利用できなくなります。**Dell ProまたはDell Pro Max（インテル® Core™ Ultra プロフェッサーおよびインテル vPro®搭載）**にアップグレードすると、**世界で最も安全なビジネス向けAI PC***で、セキュリティのメリットを大いに活用し、AIワークロードを保護できます。►

Windows 10のサポートが10月に終了します。

最新のインテル搭載Dell AI PCにアップグレードして、セキュリティのメリットと強化されたAI機能を大いに活用しましょう。

Dell Pro ● Dell Pro Maxをストアで見る

世界で最も安全なビジネス向けAI PC*

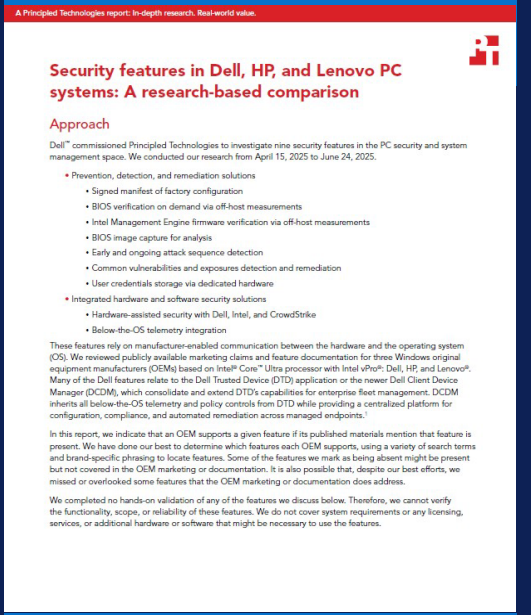
セキュリティ体制を強化するための付加価値の高いソフトウェアとサービスをご覧ください。

ソフトウェアおよび統合

サービス

業界でのリーダーシップ

Principled Technologiesの調査によると、インテル搭載DellビジネスAI PCのセキュリティは同業他社と比較して優れている


A Principled Technologies report: In-depth research. Real-world value.

Security features in Dell, HP, and Lenovo PC systems: A research-based comparison

Approach

Dell™ commissioned Principled Technologies to investigate nine security features in the PC security and system management space. We conducted our research from April 15, 2025 to June 24, 2025.

- Prevention, detection, and remediation solutions
  - Signed manifest of factory configuration
  - BIOS verification on demand via off-host measurements
  - Intel Management Engine firmware verification via off-host measurements
  - BIOS image capture for analysis
  - Early and ongoing attack sequence detection
  - Common vulnerabilities and exposures detection and remediation
  - User credentials storage via dedicated hardware
- Integrated hardware and software security solutions
  - Hardware-assisted security with Dell, Intel, and CrowdStrike
  - Below-the-OS telemetry integration

These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original equipment manufacturers (OEMs) based on Intel® Core™ Ultra processor with Intel vPro®: Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device (DTD) application or the newer Dell Client Device Manager (DCDM), which consolidate and extend DTD's capabilities for enterprise fleet management. DCDM inherits all below-the-OS telemetry and policy controls from DTD while providing a centralized platform for configuration, compliance, and automated remediation across managed endpoints.[1]

In this report, we indicate that an OEM supports a given feature if its published materials mention that feature is present. We have done our best to determine which features each OEM supports, using a variety of search terms and brand-specific phrasing to locate features. Some of the features we mark as being absent might be present but not covered in the OEM marketing or documentation. It is also possible that, despite our best efforts, we missed or overlooked some features that the OEM marketing or documentation does address.

We completed no hands-on validation of any of the features we discuss below. Therefore, we cannot verify the functionality, scope, or reliability of these features. We do not cover system requirements or any licensing, services, or additional hardware or software that might be necessary to use the features.

調査結果を読む

免責事項

*Principled Technologiesによるサードパーティー分析（インテル プロセッサー搭載Dellビジネス向けAI PCとHPおよびLenovoを比較）（2025年7月）に基づきます。世界のパソコン市場に関するDellの社内分析（2024年10月）に基づきます。インテル® プロセッサー搭載のパソコンが対象です。一部のパソコンでは利用できない機能があります。一部の機能については追加購入が必要です。

詳細はこちら：

お問い合わせ先： Global.Security.Sales@Dell.com

ソリューションの詳細： Dell.com/Endpoint-Security

Dellをフォロー： LinkedIn @DellTechnologies | X @DellTech

Dellのエンドポイント セキュリティについて

セキュリティは、あらゆる規模の組織にとっての難題です。**豊富な経験を持つセキュリティ/テクノロジー パートナーと提携すれば、エンドポイント セキュリティをモダナイズできます。**

Dell Trusted Workspaceは、エンドポイントのセキュリティ確保を支援し、ゼロトラスト対応のモダンなIT環境の構築を促進します。Dellが独自に提供する、ハードウェアおよびソフトウェア保護の包括的なポートフォリオで、攻撃対象領域を縮小し、サイバー レジリエンスを向上させましょう。当社のきめ細かい防御ベースのアプローチでは、組み込み型の保護と継続的な警戒を組み合わせることで脅威を回避します。エンド ユーザーの生産性を維持しつつ、IT部門は、現代のクラウドベースのビ環境向けに構築されたセキュリティ ソリューションにより、自信を持って業務を遂行できます。