徹底解剖：信頼できるデバイス

インテル® vPro® プラットフォーム搭載のDellのビジネス向けPCが世界最高レベルのセキュリティを誇るビジネス向けPCとなっている理由[1]

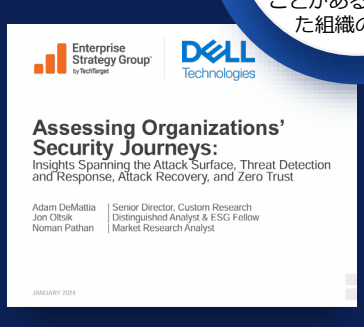
脅威の状況と課題

OS下層を標的とした攻撃ベクトルの出現により発生する新たなリスク

エンドポイント デバイスは、侵害の主なゲートウェイです。近年、ハイブリッド ワークによって攻撃対象領域が拡大するにつれ、デバイスレベルのセキュリティに関する懸念が急増しています。攻撃者は、サプライ チェーンのみならず、従来のEDRソフトウェアだけではほとんど検出できないルートキットやその他のファームウェアの脆弱性をも標的にするようになってきています。

デバイスベースの脅威は2020年から1.5倍に増加。[2]

69%
少なくとも1回はデバイスまたはBIOSレベルの攻撃を受けたことがあると報告した組織の割合[2]



新しいパソコンを調達する際の最も重要な評価基準：

- BIOSイベントの自動検出[3]
- リスクの高い構成への対処[3]

最新の脅威に対抗するには、デバイスを安全に構築する必要があります。同時に、デバイスが攻撃を捕捉して撃退するのに役立つ組み込み型セキュリティ機能を備えている必要があります。

解決策

基盤に対する攻撃について、防御、検出、対応、復旧を可能にする世界トップクラスのセキュリティを誇るビジネス向けPC[1]

フリートのセキュリティは、個々のパソコンの安全性によって決まります。とは言うものの、デバイスの信頼性と安全性を高めるにはどうすればよいのでしょうか？そのヒントが可視性と対策可能性です。より多くのデータにアクセスできれば、情報に基づいた意思決定が可能になり、新たに発生する極めて見つけにくい脅威の検出にもつながります。また、自動化は潜在的な問題の迅速な解決を可能にします。

インテル® vPro® プラットフォームを搭載したDellのビジネス向けPCのハードウェアとファームウェアの防御は、フリートに可視性と対策可能性をもたらすよう設計されています。

Dell Trusted Deviceの徹底解剖

メリット

- 厳格なサプライチェーン管理による、初回起動時からの安全性確保
- ファームウェアレベルの詳細な可視性による、BIOSの整合性維持
- 認証情報を盗もうとするマルウェアからのエンドユーザーID保護
- 「OS下層」のテレメトリーでOSレベルデータを強化し、検出、対応、修復をスピードアップ

PCのテレメトリーでセキュリティを向上

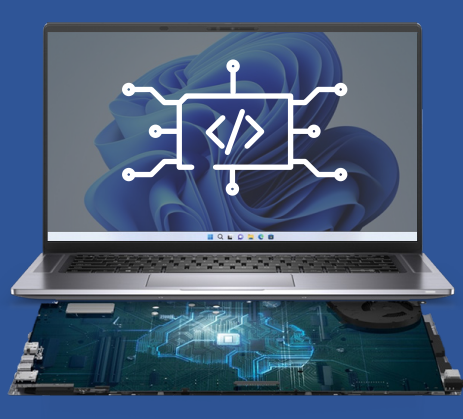
Dell Trusted Deviceアプリケーションで、ITセキュリティのギャップを縮小できます。Dell独自のテクノロジーによって業界をリードするソフトウェアプロバイダーの機能にパソコンのテレメトリーを統合し、デバイス設置環境全体のセキュリティを強化します[1]。詳細はこちら →

BIOSの整合性を維持

Dell独自のBIOS検証機能で、脅威を検知して撃退します。BIOSイメージ キャプチャで破損したBIOSを評価して修復し、将来の脅威にさらされるリスクを軽減するインサイトを獲得します[1]。詳細はこちら →

ファームウェアの整合性を検証

Dell独自のファームウェア検証は、インテル プロセッサーに搭載されたハードウェアベースのセキュリティ機能で、特権が設定されたファームウェアへの不正アクセスや改ざんを防止します。[1]



攻撃の兆候を早期発見

Dell独自の早期アラート機能であるIndicators of Attackが、行動ベースの脅威をスキャンし、被害が発生する前に検出します[1]。詳細はこちら →

既知の脆弱性をキャッチ

Dell独自の共通脆弱性識別子(CVE)検出機能が、公に報告されているBIOSセキュリティの欠陥を監視し、リスク軽減のためのアップデートを推奨します。[1] 詳細はこちら →

エンド ユーザーの資格情報を保護

Dell独自のSafeIDでユーザー アクセスを検証します。これは、ユーザー資格情報をマルウェアから隠して保護する専用のセキュリティ チップです[1]。
詳細はこちら →

パソコンのライフサイクル全体で安全性を確保

最先端の厳格なサプライ チェーン管理と、Dell独自のSecured Component Verificationなどのアドオン（オプション）で、引渡し時とライフタイム全体にわたるパソコンの整合性が保証されます[1]。
詳細はこちら →

業界でのリーダーシップ

DellのようなBIOSレベルの可視性を提供しているPCメーカーはありません[1]。

最新の脅威に対するデバイスの信頼性を維持するために何が必要かをご確認ください。

詳細はこちら →

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

A comparison of security features in Dell, HP, and Lenovo PC systems

Approach

Dell™ commissioned Principled Technologies to investigate 10 security features in the PC security and system management space:

- Support for monitoring solutions
- BIOS security and protection features
  - Platform integrity validation
  - Device integrity validation via off-site measurements
  - Component integrity validation for Intel® Management Engine (ME) via off-site measurements
  - BIOS image capture for analysis
  - Built-in hardware cache for monitoring BIOS changes with security information and event management (SIEM) integration
- Microsoft Intune management
  - BIOS setting management integrations for Intune
  - BIOS access management security enhancements for Intune
- Remote management
  - Intel vPro® remote management
  - PC management using cellular data

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

Dell Trusted Deviceの詳細情報

Latitude →

OptiPlex →

Precision →

働く場所を問わず安全性を確保するDell Trusted Workspace

組み込み型/内蔵型のハードウェア セキュリティ

追加型のソフトウェア セキュリティ

ぜひご参加ください
dell.com/endpoint-security

お問い合わせ
global.security.sales@dell.com

詳細はこちら
エンドポイント セキュリティに関するブログ→

会話に参加する
delltechnologies　@delltech

出典と免責事項

[1]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に対する評価です。すべてのパソコンで全機能を使用できるわけではありません。一部の機能については追加購入が必要です。Principled Technologiesによる検証『A comparison of security features』（2024年4月）。

[2]出典：Futurum Group、『Endpoint Security Trends, 2023』

[3]出典：デル・テクノロジーズの委託により、TechTargetのEnterprise Strategy Group部門が実施したカスタム調査アンケート『*Assessing Organizations' Security Journeys*』（2023年11月）