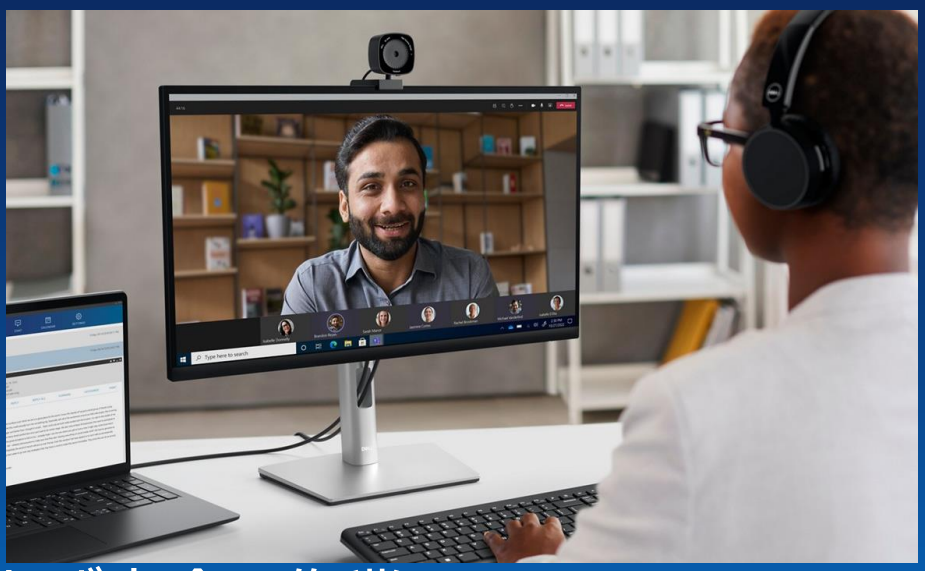
## 詳細を見る

# Dell Trusted Workspace



## 場所を問わず安全に作業

今日のクラウドベースの世界に合わせて構築された、ハードウェアとソフトウェアの防御機能をご活用ください。

ハイブリッドな働き方の普及で、組織は新たな攻撃ベクトルにさらされています。敵対者による攻撃はいっそう高度化しています。効果的なエンドポイント セキュリティを実装するには、デバイス、ネットワーク、クラウドを保護するマルチレイヤー防御が必要になります。

ハードウェアとソフトウェアを保護する包括的なポートフォリオで、攻撃対象領域を縮小し、常に最新の脅威の一歩先を行くことができます。

**ポートフォリオの詳細情報 →**

業界で最高クラスの安全性を誇るビジネス向けPC[1] →

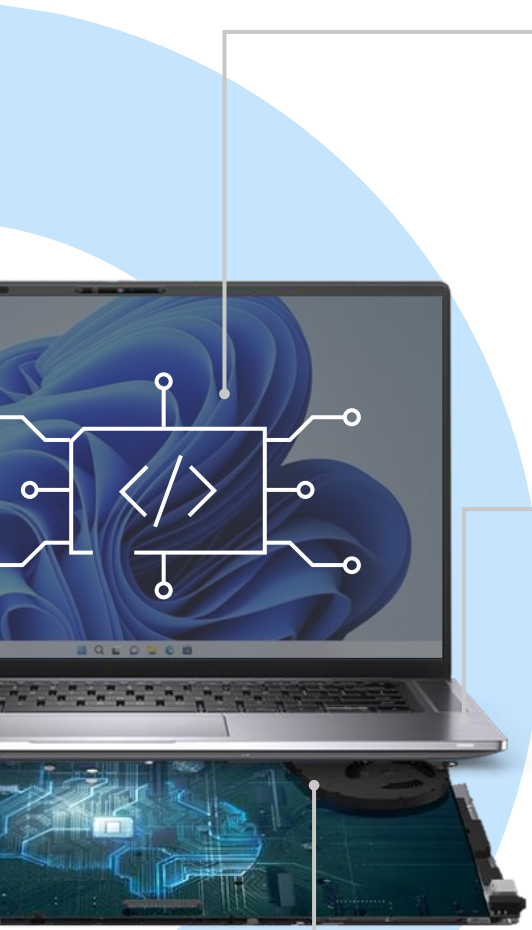
管理対象デバイス全体のセキュリティを強化するソフトウェア →



DELL Technologies

## Dell Trusted Workspace

# マルチレイヤー防御



### 多層型
### **ソフトウェア セキュリティ**

厳選されたパートナー エコシステムによるソフトウェアで、高度な脅威に対する防御を多層化できます。複数のセキュリティ機能が統合され、効率が向上し、さまざまなメリットがあります。

### 内蔵型
### **ハードウェアとファームウェアのセキュリティ**

業界で最高クラスの安全性を誇るビジネス向けPC[1]で、システム基盤に対する攻撃を検出し、防御できます。BIOS/ファームウェアとハードウェアのレベルでの深層防御で、デバイスが常に保護されます。

PCテレメトリーと業界をリードするソフトウェアを統合し、管理対象デバイス全体のセキュリティを向上させているのはデル・テクノロジーズだけです[1]。

### 組み込み型
### **サプライ チェーン セキュリティ**

最初の起動時からデバイスのセキュリティが確保され、安心して作業できます。PCのセキュアな設計、開発、テストで製品の脆弱性がもたらすリスクを抑え、厳格なサプライ チェーン管理で製品の改ざんリスクも低減します。

場所を問わずに発生する脅威を防止、検出し、迅速に対応できます

**Dell SafeGuard and Response**

**Dell SafeData**

進化する脅威から常に保護

**Dell SafeBIOS**

**Dell SafeID**

**Dell SafeShutter**

納品時にハードウェアに改ざんがないことを確認

**Dell SafeSupply Chain**

**Dell Trusted Workspace -** 組み込み型/内蔵型のセキュリティ

# 業界最高レベルの安全性を誇るビジネス向けPC[1]

## 最初の起動時から安全性を確保

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、PCの整合性が保証されます。

詳細はこちら →

## BIOSの整合性を維持

Dell独自のBIOS検証機能**SafeBIOS**で、脅威を検知して撃退できます。破損したBIOSを評価して修復し、将来脅威にさらされるリスクを軽減するためのインサイトを得ることもできます。

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。

## 攻撃の兆候を早期発見

Dell独自の早期アラート機能**Indicators of Attack**は、振る舞いに基づいて脅威をスキャンし、被害が発生する前に検出します。

## エンド ユーザーの資格情報を保護

Dell独自の**SafeID**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。

詳細はこちら →

## 画面上のプライバシーを確保

センサー対応のWebカメラ**SafeShutter**は、ビデオ会議アプリケーションと同期して自動的に開閉します。

## PCのテレメトリーでセキュリティを向上

**Dell Trusted Deviceソフトウェア**で、ITセキュリティのギャップを縮小できます。業界をリードするソフトウェア プロバイダーの機能にPCのテレメトリーを統合したDell独自のテクノロジーが、管理対象デバイス全体のセキュリティを向上させます[1]。詳細はこちら →

## Dell Trusted Deviceの詳細情報

Latitude →

OptiPlex →

Precision →



DELL Technologies

**Dell Trusted Workspace** - 多層型セキュリティ

# 管理対象デバイス全体のセキュリティを強化するソフトウェア

## Dell SafeGuard and Responseで高度なサイバー攻撃を阻止

場所を問わずに発生する脅威を防止、検出し、迅速に対応できます。人工知能と機械学習を利用して、エンドポイントへの攻撃をプロアクティブに検出すると同時に、セキュリティのエキスパートが、エンドポイント、ネットワーク、クラウド全体で脅威を探索し、特定された脅威からの修復を支援します。

### パートナー

CrowdStrike Falcon® →

VMware Carbon Black →

Secureworks® Taegis™ XDR →

## Dell SafeDataで、デバイスとクラウドのデータを保護

ユーザーがどこにいても、安全にコラボレーションできます。Netskopeはクラウドのセキュリティとアクセスに対してデータ中心のアプローチを取り、場所を問わずにデータとユーザーを保護します。Absoluteは、企業のファイアウォール外の可視性、保護、データ保全の機能を持ちます。

### パートナー

Absolute：エンドポイント、アプリケーション、ネットワークの自動修復 →

Netskope：Security Service Edgeソリューションの詳細 →

## デル・テクノロジーズのセキュリティ サービスについて

Dellのサービスでは、お客様がセキュリティを自分で管理することも、専門家に管理を任せることもできます。デル・テクノロジーズのフルマネージド360° SecOpsソリューションは、IT環境のセキュリティ脅威を防止、対応し、脅威からの復旧を支援します。

Managed Detection and Response Pro Plusの詳細を見る →



DELL Technologies

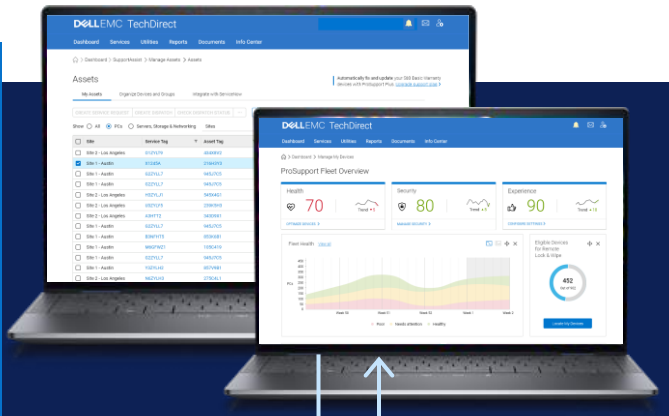
**Dell Trusted Workspace** - ハードウェア支援型セキュリティ

# 統合セキュリティ

**ソフトウェアのみの対策では、進化するサイバー脅威を防御しきれません。ハードウェア支援型の保護で、エンドポイントの攻撃対象領域を縮小できます。**

最新の脅威から環境を保護するには、ハードウェアとソフトウェアの防御を連動させる必要があります。Dellは、業界をリードするセキュリティ パートナーと協力して、豊富なデバイスレベルのテレメトリーと最先端の脅威検知機能を組み合わせ、管理対象デバイス全体のセキュリティを向上させます。

- ✓ **攻撃対象領域を縮小**
- ✓ **脅威検出の向上**
- ✓ **デバイスの信頼性を維持**
- ✓ **プロバイダーとの連携**

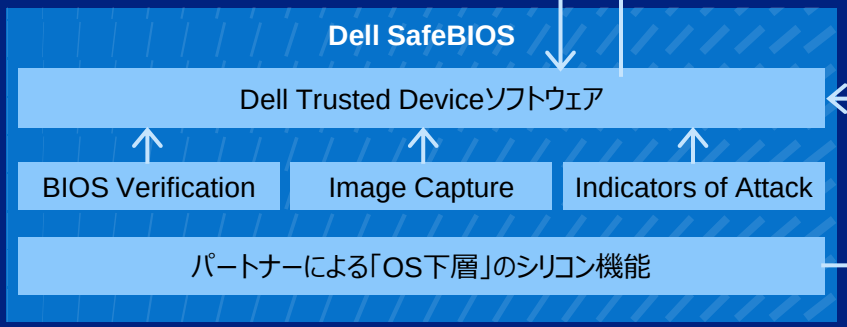



PCテレメトリーと業界をリードするソフトウェアを統合し、管理対象デバイス全体のセキュリティを向上させているのは**デル・テクノロジーズだけ**です[1][2]

## 多層型
ソフトウェア セキュリティ

OS

## 内蔵型ハードウェア/ファームウェア セキュリティ





## 組み込み型
サプライ チェーン セキュリティ




DELL Technologies

# 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

## 多層型ソフトウェア セキュリティ

マルチレイヤー防御によって攻撃対象領域を減らし、長期的なサイバー レジリエンスを強化できます。

**Webサイト**
dell.com/endpoint-security

**お問い合わせ**
global.security.sales@dell.com

**詳細を読む**
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**
LinkedIn/delltechnologies
X @delltech

**出典と免責事項**

[1]デル・テクノロジーズの社内分析（2023年9月）に基づきます。インテル®プロセッサー搭載のPCに対する評価です。すべてのPCで全機能を使用できるわけではありません。一部の機能は追加購入が必要です。提供状況は地域によって異なります。

[2]CrowdStrike Falcon Insight XDRとVMware Carbon Black Audit and Remediationでご利用いただけます。



DELL Technologies