ホワイトペーパー: OSの上層、内部、および下層に広がるセキュリティの実現

デルとインテルは、法人向けPCにゼロトラストの原則を用いて、企業と従業員のセキュリティを担保します。

2022年4月

エグゼクティブ・サマリー

- ビジネスデータの安全性を維持することは困難な作業であり、組織のネットワーク外で運用されるエンドポイントの急増と脅威ベクトルの絶え間ない進化によって複雑化しています。
- デルとインテルの長年にわたる協業関係は、法人のお客様のネットワークセキュリティを維持するというコミットメントの共有に基づいています。
- セキュリティに対する当社の包括的なアプローチでは、従来の攻撃に対するソフトウェアベースの「Above the OS（OS上層）」保護に加え、インテルによるシリコン（IC）ベースの保護、およびデバイスの最も深いレベルを標的とする攻撃から防御するハードウェアベースの「Below the OS（OS下層）」保護機能を採用しています。
- 更にこのアプローチに加え、デルとインテルは、プラットフォームが市場に出て悪意のある攻撃者からの攻撃を受けた場合にプラットフォーム・セキュリティを継続的に確保するための学習とポリシー更新に投資をし続けています。

このホワイトペーパーのトピックス

セキュリティ基盤

安全な開発ライフサイクル

デルとインテルは、セキュリティを最重要の要素として製品を設計し、リリース前に厳密にテストします。

サプライチェーン・セキュリティ

保護はサプライチェーンに沿って実施され、工場を出た後もデバイスの安全性を確保します。

包括的な防御態勢

OS下層セキュリティ

ハードウェアベースのセキュリティ機能により、基盤となるレイヤをターゲットとする脅威から保護します。

OS上層＆内部セキュリティ

ソフトウェアベースのセキュリティテクノロジーとシリコンベースの保護は、ともにデバイスの総体的なセキュリティに不可欠です。

継続的なサポート

デルとインテルは、自社製品のセキュリティ確保、脆弱性へのパッチ適用、リコンベースのOSセキュリティ対策に取り組んでいます。

主要なセキュリティトレンド

78%

調査対象となった**セキュリティ専門家の78%**が、従業員が**在宅勤務をしているために攻撃が増加した**と回答しました[1]。

62%

欧州連合（EU）のサイバーセキュリティ機関が調査した**サプライチェーン攻撃の62%**は、**サプライヤへの誤った信頼が原因でした**[2]。

8%

ランサムウェアは依然としてほとんどの組織にとって最大の脅威であり、**2021年には前年比で8%増加しました**[3]。

44%

最近の調査では、**組織の44%**が過去12ヶ月間に**ハードウェアレベルまたはBIOSレベルの攻撃**を少なくとも1回受け、**16%が複数回の攻撃を受けたことがある**ことが判明しています[4]。

1. 「Surge in Cyberattacks Targets the Anywhere Workforce」（VMware、2021年）
2. 「Threat Landscape for Supply Chain Attacks」（ENISA、2021年）
3. 「2021 State of the Threat」（Secureworks、2021年）
4. 「デル・テクノロジーズ、サイバー攻撃に対する企業のレジリエンス（回復力）を確立するためのセキュリティー ソリューションとサービスを発表」（デル・テクノロジーズ、2020年）

エンドポイントの脆弱性、それはすなわちビジネスの脆弱性

名前の知られたグローバルブランドが重大なセキュリティ侵害に遭い、ネガティブな事実を公表してその評判に大きなダメージを受ける様子を数ヶ月ごとに目にします。ビジネスオーナーやセキュリティの専門家は、自分たちのデバイスに潜んでいる見過ごされた脆弱性やソフトウェアに潜んでいる未知で悪用可能な脆弱性によって、自分たちも危険にさらされているのではないかと心配しています。ネットワークのセキュリティを確保し、データの安全な運用を実現するために、自社のITチームを信頼できる場合もありますが、製造や開発を自ら管理していない状況で、ビジネスを行うために不可欠なすべてのエンドポイントとアプリケーションを信頼するにはどうすればよいでしょうか。

デルとインテルは、ビジネスデバイスとネットワークを確実に保護する唯一の方法は、ハードウェアとソフトウェアのセキュリティテクノロジーを調和させることであると考えています。私たちのチームは密接に統合されたハードウェアとソフトウェアの堅固なセキュリティ機能を作るために協力してきましたが、他のプロバイダはこれに力を入れてこなかった可能性があります。

ハードウェアベースの潜在的な脆弱性に対処することなく、ソフトウェアのみのソリューションを行い、デバイスの完全性を実現できたという誤った認識を持ってしまうことがあります。ソフトウェアのみのソリューションの限界を理解することが重要です。ソフトウェアだけに頼ることで、ソフトウェアが動作しているハードウェアが攻撃に対して脆弱になる可能性を残しているのです。要するに、ハードウエアが安全でなければ、ソフトウエアは安全ではないのです。

他のプロバイダは、デバイスを保護するために「壁に囲まれた庭」を作ろうとしており、そうしたアプリやサービスにはユーザーの柔軟性を限定する制限が組み込まれています。これは一般消費者向けには妥当かもしれませんが、デバイスを完全に活用する自由を犠牲にしており、ビジネス的な意味では悪い面しかありません。このアプローチはまた、一般的な構成による脆弱性を露呈させようと、攻撃者にますますそのようなシステムを狙って破壊しようと仕向けてしまう可能性もはらんでいます。

簡単に言えば、消費者向けデバイスに使用するセキュリティ対策を法人向けデバイスに適用すると、攻撃者にとってより魅力的なターゲットとなることがあります。そのため、デルとインテルは、セキュリティに対してこれまでとは異なる全体的なアプローチをとっています。

デルとインテルは組込み型のハードウェアベースのセキュリティを提供

デバイスやネットワークを安全にするための複雑さや懸念は、お客様にとって頭を悩ませるポイントです。そのため、デルは、セキュリティを考慮して設計されたデバイスをお客様に提供し、お客様が本当に重要な業務に集中できるようにすることが使命であると考えています。

デルとインテルの共同エンジニアリング関係は数十年に及び、特にBtoB市場において、お客様のデータを安全に保つことに常に焦点を当ててきました。デルはインテルとのパートナーシップを通じて、あらゆる規模の企業およびあらゆる市場において、従業員向けデバイスの主要プロバイダとして認められています。

デルの法人向けデバイスにはどのような機能が搭載されているのでしょうか。インテルとデルは、法人向けPCのライフサイクル全体を通じて、テクノロジー、ツール、ポリシーを組み合わせ、お客様とそのビジネスにエンドツーエンドのセキュリティを提供しています。

セキュリティ設計思想

インテルとデルは、今日の脅威の先を見据えて、アタック・サーフェスを最小に抑え、法人向けデバイスのセキュリティを確保するために、将来のシステムを設計します。

輸送中の保護

デバイスがユーザーの手に渡る前においてデバイスの完全性を保護し、部品の調達、組立て、配送の全体を通じたセキュリティを維持するためのテクノロジーとポリシーを用意しています。

進化する脅威に対する防御

デルでは、Dell Trusted Deviceテクノロジーとインテル® ハードウェア・シールド機能によってハードウェアベースのセキュリティを採用し、防御、検知、対応のフレームワークを通じてデバイスの防御機能を強化しています。
さらに、デルとインテルには、攻撃者より先に製品を調査して新しい脆弱性を発見することに特化したセキュリティチームがあります。迅速にパッチを適用して、お客様とチームのセキュリティを確保します。

このホワイトペーパーでは、デルとインテルが協力して、セキュリティを最も深いレベルに組み込んだ法人向けPCプラットフォームを開発し、お客様のデバイスをライフサイクル全体に渡り、次の入替えまで、そしてそれ以降に渡って保護する方法について説明します。

会議室からプラットフォーム保護は始まっている

計画・評価・分析

デルとインテルの専門家は、それぞれ最新のプラットフォームとチップセットを設計する前に、将来のセキュリティニーズに対応し、必要なセキュリティ関連の法令を満たすために、プラットフォームにどのような機能を持たせる必要があるかについて、厳格なパラメータを設定します。このプロセスは、将来起こり得るセキュリティとプライバシーのリスクと、それらに対処するために必要な活動について協議して決定することから始まります。この評価は、アーキテクチャの評価対象となるセキュリティ目標を定義するために使用されます。
この情報に基づいて、デルとインテルのセキュリティチームは、この概念アーキテクチャに「敵」側の考え方を適用して脅威モデルを開発し、潜在的な緩和する必要のある脆弱性やその標的型攻撃を調査します。この演習では、BIOS、ファームウェア、およびハードウェア設計の潜在的な脆弱性の検知と軽減について、大幅な改善が行われます。

セキュリティ中心の設計

脅威の評価が完了し、攻撃対象となるアタック・サーフェスは何か、テストをどこに集中すべきかを定義するモデルが作成されると、エンジニアは製品コードの開発を開始します。前の段階で定義されたセキュリティ目標は、開発のこの段階におけるガイダンスを提供し、製品がお客様のニーズを満たしているかどうかを判断する基準となります。

検証とテスト

開発ライフサイクルの開始時に設定されたセキュリティ目標を満たすまでコードが改良されると、製品は厳密なテストプロセスに進みます。
これらのテストは通常、セキュアなコードレビューと静的コード分析から始まります。静的コード分析は、欠陥を発見して修正するための特別なツールを使用する自動化されたプロセスです。より複雑なコードを持つ製品の中には、手動のレビュープロセスに移行するものもあります。このプロセスでは、セキュリティの専門家が製品コードを1行ずつレビューして、これまで知られていない問題点を見つけ、安全な方法で設計されていることが確実になるよう手助けします。
最後に、熟練した「ハッカー」のチームが投入され、侵入テストその他のレッドチームとしての活動を行って、それ以前の段階で見落とされた潜在的な脆弱性を見つけ出します。これらの発見事項は、リスクに基づいて再度検証され、追加で特定された問題は文書化され、修正されます。

リリースとポストリリース

厳密にテストされ、最初に定義されたセキュリティ目標を満たしているか、それを上回っていることが確認されると、その製品はいつでも市場にリリースできる状態です。しかし、ここまでの各フェーズは、セキュアな開発ライフサイクルのほんの一部にすぎません。デルとインテルにとって、プラットフォームのセキュリティは継続的な取り組みです。私たちのチームは、攻撃者に悪用される前に脆弱性を発見し、セキュリティアップデートを開発してパッチを適用します。
エンドツーエンドのセキュリティに対するデルとインテルの取り組みの一例として、デバイスの組み立てから配送までの安全なサプライチェーンに力を注いでいることが挙げられます。サプライチェーンを狙うのは、悪意のある攻撃者の中で最も急速に増加しているベクトルの1つです。次のセクションでは、お客様の玄関口まで配送されたデバイスが最初の起動時から安全であることを確実にするために、デルとインテルがサプライチェーンのリスクをどのように軽減しているかを詳しく説明します。

サプライチェーンの信頼性は、デバイスセキュリティの基本

部品やデバイスが工場を出てから目的地に到着するまでの間には、多くのことが起こり得ます。サプライチェーンの各ステップには、従業員、ビジネス、およびお客様を潜在的な攻撃から解放する新しいベクトルがあります。デルとインテルは、お客様のビジネスに導入される前の製品のセキュリティを確保し、従業員に持たせる前にデバイスの信頼性を自己検証できるようにするための、ツール、テクノロジー、およびプロセスを開発しました。

ソース

デルは、デバイスとそのコンポーネントの品質と安全性を確保するために、厳格なパートナー審査プロセスを採用しています。また、これらのパートナーは、デルの包括的なサプライチェーン・セキュリティ基準への準拠を確認するため、定期的に監査を受けています。

製造

デルのデバイス製造においては、デルのサプライチェーン・セキュリティ基準に準拠していることに加え、偽造部品がサプライチェーンに入り込まないよう、製造中に頻繁に部品をテストします。このリスクをさらに軽減するため、高リスクの特定のコンポーネントには固有の部品識別番号（PPID）ラベルが貼付されます。このラベルには、サプライヤ、部品番号、製造国、製造日に関する情報が記載されています。これにより、デルはそうした部品を識別、認証、追跡し、最終的に検証して出荷されたデバイスそのものをお客様が確実に受け取ることができるようにします。

配送

デルの貨物は、改ざん防止シールやドアロック機構、輸送中に貨物内のデル製デバイスが改ざんされたことを検出するための様々な追跡装置など、何重もの物理的セキュリティによって保護されています。デルのデバイス自体にも、改ざん検知テクノロジーが搭載されています。デル・テクノロジーズのSafeSupply Chainソリューションは、サプライチェーン・セキュリティを提供し、更に改ざん防止シールやNISTレベルのハードドライブ・ワイプなどを用いて、クリーンなデバイスであることを確実にします。

検証

デルの法人向けデバイスは、暗号技術を用いて電子署名されたプラットフォーム証明書が付属した状態で出荷されます。この証明書は、製造、組立て、テスト、および統合時にプラットフォームのスナップショット属性を取得します。これらのプラットフォーム属性は、ハードウェアの“Root of Trust”としてTrusted Platform Module（TPM）を使用して特定のデバイスに暗号化された状態で紐づけられます。

デルは、インテルプロセッサーを搭載した法人PC向けのDell Secured Component Verification（SCV）ソリューションにTrusted Computing Groupのプラットフォーム証明書を実装しました。SCVは、サポート対象のデル製デバイスについて、暗号化された署名付きの証明書をIT部門に提供します。SCVでは、安全な自己検証ツールを使用して、IT環境への移行時にハードウェアの完全な整合性を確保し、デルの法人PCと主要部品が注文通りに組み立てられたかどうかをお客様が確認できるようにします。

同様に、インテルは長年にわたり、ベースとなるデジタルサプライチェーンの透明性とトレーサビリティをベンダーが備えるようにしてきました。インテル® トランスペアレント・サプライ・チェーン（インテル® TSC）は、インテル® TSCのWebポータルでIT部門が利用できるクラウドAPIを使用して、インテルベースのプラットフォームをサポートするためのTCGプラットフォーム証明書およびコンポーネントデータを提供します。デルとインテルは独立したソリューションを実装することを選択しましたが、TCGプラットフォーム証明書はインテル® TSCとDell SCVの共通の要素です。この共通性によって互換性と相互運用性が提供され、企業や政府機関の購入者はTCGプラットフォーム証明書を導入して、インテルベースのデバイスのデジタルサプライチェーンのセキュリティ保証を向上させることができます。

組込みのセキュリティ・テクノロジーが脅威の防御、検知、対応に役立つ

包括的なセキュリティとは、ソフトウェアでソフトウェアを保護するという従来のモデルを超えて、デジタルセキュリティ、安全性、プライバシーに対する新しい種類の脅威に対応することを意味します。ハードウェアベースの「OS下層」セキュリティ技術と組み合わせることで、サプライチェーン上で最も一般的に発生する脅威の亜種を含む根本的な攻撃の防止と検知を行い、HW/SWスタックのすべてのレイヤを保護することができます。デルとインテルの共同エンジニアリングの関係では、部品レベルとプラットフォームレベルの両方で、複雑なテクノロジーの織り成す技術を使用して、この攻撃対象となる脅威面をカバーすることに重点を置いています。他のデルおよびインテルのツールとテクノロジーに加えて、インテル® ハードウェア・シールドおよびデルのSafeBIOSフレームワークは、デルの法人向けデバイスを使用するユーザーに、組込み型のハードウェアベースの保護を提供します。

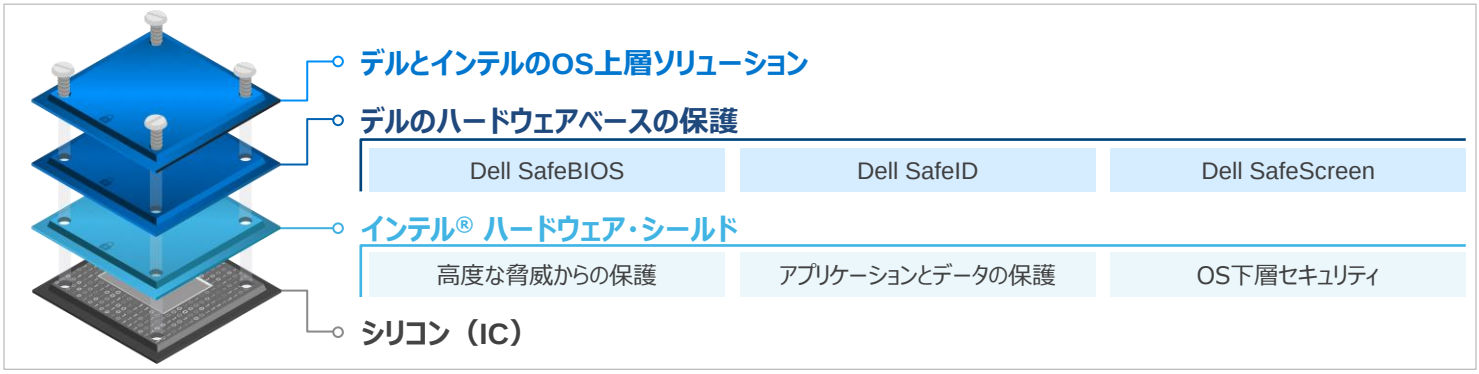


図1：インテル® ハードウェア・シールドおよびデルのハードウェアベースの保護機能は、プラットフォームの基礎部分への攻撃に対する防御に役立つセキュリティレイヤです。

インテル® ハードウェア・シールド

インテルのハードウェア・シールドは、インテル vPro® プラットフォーム上で動作するすべてのデル製法人向けデバイスに付属しており、コンピューティングスタックのすべてのレイヤを保護するためのハードウェア拡張セキュリティ機能を提供します。

インテル ハードウェア・シールドは、Advanced Threat Protection、Application and Data Protection、およびBelow the OS Securityで構成され、20を超える革新的なセキュリティテクノロジーを備えています。デルは、これらの機能のほとんどすべてを活用して、基本的な機能を活用したセキュリティソリューションを開発し、市場で最も安全な法人向けデバイスの1つをお客様に提供しています。これらのソリューションには、Dell SafeBIOSフレームワーク、Dell SafeID、およびDell SafeScreenが含まれ、現在および将来の脅威に対してさらに高いレベルのセキュリティを提供します。

Dell SafeBIOSフレームワーク、Dell SafeID、およびDell SafeScreen

Basic Input Output System（BIOS）の保護は、デバイスのセキュリティに不可欠です。攻撃者がデバイスのBIOSを破壊することに成功した場合、デバイスアーキテクチャ内においてBIOSだけが持つ特権的な地位のために、デバイス全体を制御できるようになってしまいます。この重要なレイヤーを保護するために、デルの法人向けデバイスにはSafeBIOSが付属しています。SafeBIOSは、BIOS攻撃の防止、BIOSが侵害されているかどうかの検知、および異常が見つかった場合のIT部門への警告による対応を支援する一連のツールです。

デルの一部の法人向けデバイスにはDell SafeIDも搭載されています。SafeIDは、エンドユーザーのログイン認証情報を専用のセキュリティチップに保存することで、アクセス認証情報を探して盗むマルウェアからユーザーを保護します。マルウェアは、ビジネスネットワーク全体を危険にさらすおそれのある侵入行為です。

更に、Dell SafeScreenを一部の法人向けデバイスに搭載することで、エンドユーザーは個人情報を保護しながらどこからでも作業できます。Dell SafeScreenは、統合されたデジタルプライバシー画面とセンサー対応のWebカメラによって、機密情報や認証情報を物理的な脅威から保護します。

OS下層セキュリティは、デルがデバイスを保護するために採用している包括的なアプローチの一部にすぎません。

デルの商用デバイスをより完全に保護するため、デルとインテルは、OS内およびOSより上位のセキュリティ・ソリューションにも多大な投資を行っています。これらの機能は、データおよびアプリケーション層における追加の保護レイヤーを提供することにより、高度な攻撃者による高度な脅威からデバイスを保護することを支援するものです。

デル＋インテルのOS上層ソリューションがエンドポイント・セキュリティを確保

OS下層への攻撃の脅威が高まっているのと同時に、OS上層の保護もこれまで以上に重要になっています。リモートおよび外出先で作業するエンドユーザーの数が飛躍的に増加しているため、脅威が発生した場合にそれを防御、検知、対応するインテリジェントなソリューションが必要です。Dell Trusted Devicesエンドポイントセキュリティポートフォリオには、Dell SafeGuardとResponse、Dell SafeData、VMware Workspace ONE®などのオプションソフトウェアが含まれており、ビジネスリーダーにエンドポイントを保護するために必要なものを提供します。インテル® Control-flow Enforcement Technologyなどのインテルのセキュリティ機能がシリコンの深く組み込まれているため、OSを標的とした攻撃から保護できます。また、インテル・ハードウェア・シールド内の他の機能により、OSより下層が保護され、アプリケーションとデータが守られ、高度な脅威からの保護が提供されます。

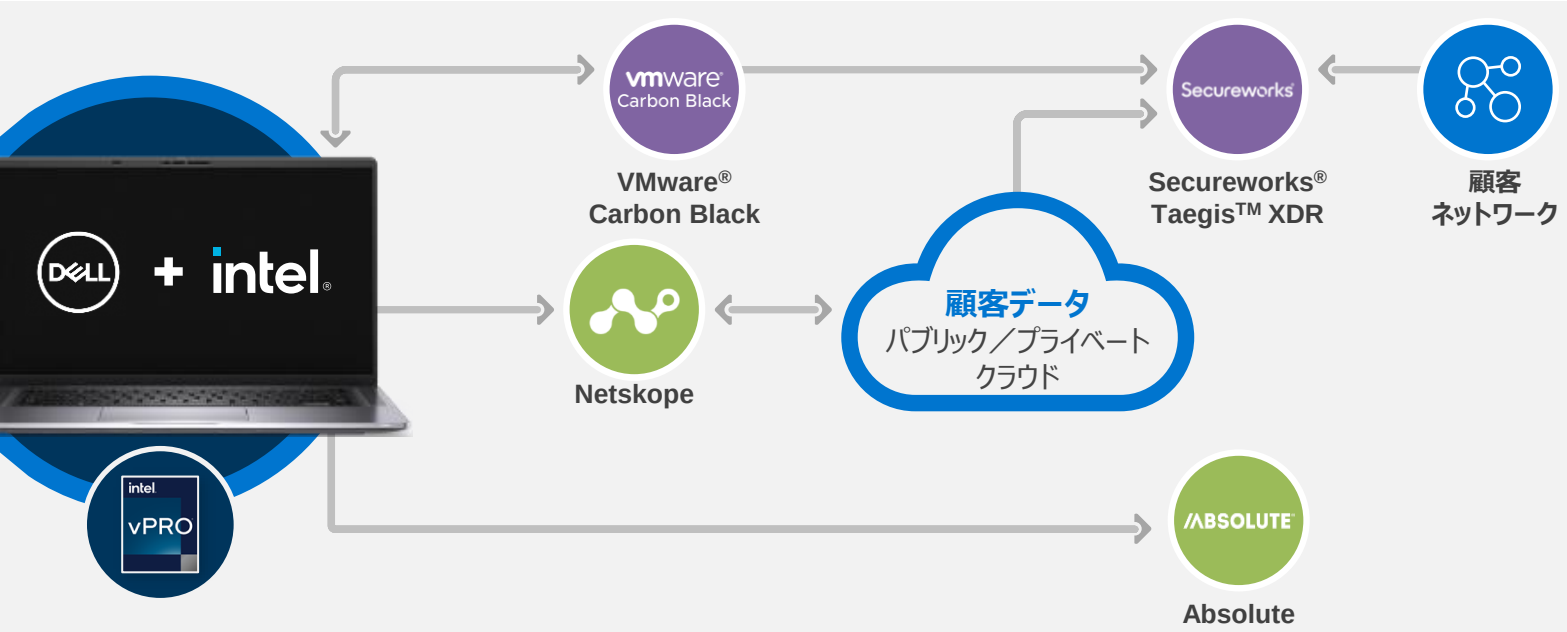


図2：Dell Trusted Deviceエンドポイントセキュリティ・ポートフォリオは、インテルのvProハードウェアベースのセキュリティ機能と組み合わせることで、ICチップからクラウドまでの効率的なセキュリティパフォーマンスを提供します。

Dell SafeGuard and Responseは、**VMware® Carbon Black**と**Secureworks® Taegis™ XDR**によって提供され、次世代のウイルス対策ソフトウェアと、エンドポイント、ネットワーク、クラウド上のセキュリティ・テレメトリ分析を組み合わせたものです。Dell SafeGuard and Responseは、企業が組織全体にわたって高度な脅威を検知、調査、対応することを支援します。

Dell SafeDataは、機密情報を暗号化し、**Netskope**と**Absolute**によってデータを保護します。これらのアプリケーションは、クラウドベースのアプリケーションに可視性、モニタリング、およびデータ損失防止を提供し、悪意のある攻撃が発生した場合にエンドポイントアプリケーションを元の安全な状態に復元します。

VMware Workspace ONE®は、アクセス制御、アプリケーション管理、マルチプラットフォーム・エンドポイント管理を統合することで、あらゆるデバイス上のあらゆるアプリケーションをシンプルかつ安全に配信および管理する、インテリジェンス駆動型のデジタル・ワークスペース・プラットフォームです。**新しくインテル vPro®プラットフォームテクノロジーとVMware Workspace ONEが最近統合されたことにより、ITチームはエンドポイントの優れたセキュリティと、ICチップからクラウドまでの管理というメリットを得ることができます。**

デルとインテルのOS上層およびOS下層セキュリティフレームワークは、法人向けデバイスを保護するための包括的なアプローチを提供しますが、当社はセキュリティの専門家として、絶対に安全なデバイスはないということを認識しています。そのため、リリース後のセキュリティに力を注ぐことにおいても業界をリードし、リリース後もデバイスのセキュリティを何年も維持できるようにしています。

デルとインテルは、リリース後のプラットフォームの持続的なセキュリティに投資

デルとインテルは、製品のライフサイクル全体にわたってセキュリティを確保するために、多大な投資を継続的に行ってきました。デバイスやプラットフォームが市場に投入されると、デルとインテルのチームは製品の脆弱性を積極的に調査し続けます。インテルにとって、このプロセスには、研究者や大学と協力して、悪意ある攻撃者よりも先に悪用の可能性を見つけ、見つかった脆弱性に迅速にパッチを適用し、セキュリティの抜け穴を塞いだ後に報告することが含まれます。

この取り組みの一環として、インテルは業界で最も優れたバグバウンティプログラムの1つに投資し、その成果は、2021年に外部から発見された脆弱性の86%をカバーしています。このプログラムを通じて発見されたCVE（Common Vulnerabilities and Exposures）や社内外の研究者によって発見されたCVEは、公開データベースに記録されます。リリース後の脆弱性監視と報告におけるリーダーとして、インテルはほとんどの競合他社よりも多くの潜在的脆弱性を記録しパッチを適用しており、透明性とデバイスのセキュリティに対するインテルのコミットメントに及ばないチップメーカーに先んじた存在であり続けています。

広範なプログラムを通じて発見されたCVEに対応するため、インテルは製品で実行されているすべてのシステムにIntel Platform Updatesを定期的に配布しています。このロールアウトは、CSP、ISV、OEM/ODM、SIなど、インテルのパートナー・エコシステムによる検証を必要とする広範なプロセスです。

特定された製品の脆弱性の開示と対応の調整は、デルとインテルそれぞれの専門の製品セキュリティ・インシデント対応チームが行います。両チームは協力して、CVEが迅速かつ安全に処理されるよう支援し、CVEがもたらすリスクを効果的に軽減します。

デルとインテルは、お客様に継続的なサポートを提供し、ITチームの負担を軽減するために、これらの投資を行いました。当社では、研究者、セキュリティアーキテクト、およびサイバーフォレンジックアナリストを雇用して、お客様のビジネスの安全性を維持し、チームが従業員に最高の仕事をさせることに集中できるよう支援しています。

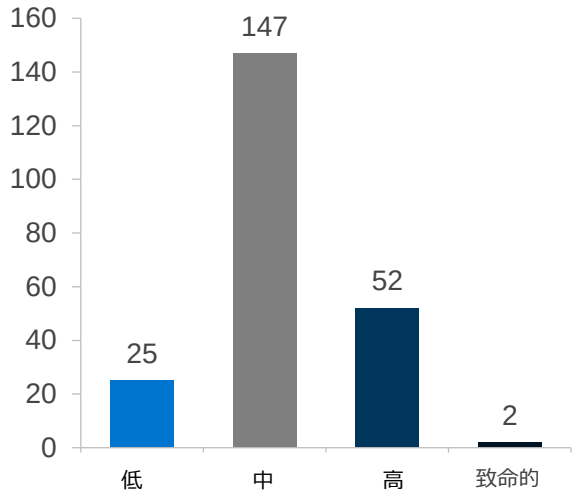


図3： 2021年に社内外の研究者によって発見されたインテル製品のCVEの件数

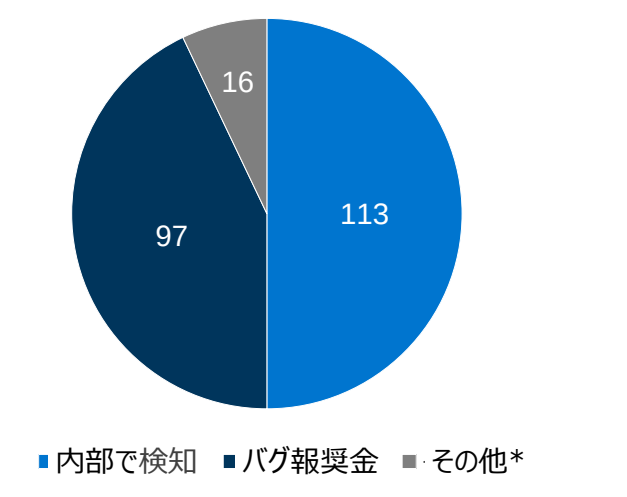


図4： 社内外のチームが、悪用される前にインテルプラットフォームの脆弱性を発見し、パッチを適用した。

デルとインテルは、成長を続けるお客様のビジネスを保護するために尽力

サイバーセキュリティの戦いの勝敗は、脅威インテリジェンスを収集、分析、対応する能力で決まります。

今日の攻撃者は革新的です。ほとんどのセキュリティソリューションがソフトウェアのセキュリティのみに焦点を当てていることを理解しているので、攻撃者はOS下層とサプライチェーンを、セキュリティを侵害し、貴社のビジネスに大きな損害を与えるための新たな手段と考えています。

このような悪意ある攻撃者たちに先んじてビジネスを保護するために、今日のリーダーたちは、従業員に法人向けデバイスを持たせる際に、シリコンの奥深くに組み込まれたハードウェアベースのセキュリティ技術が重要であると考えなければなりません。

デルとインテルは数十年にわたって法人向けデバイス分野で提携しており、業界で最も安全性の高い法人向けデバイスの1つとしてお客様の信頼を得ています。

私たちの共同の専門知識と共同エンジニアリングの関係は、その一貫した研究、勤勉さ、そして革新を通して、ハッカーたちの先を行くことを可能にします。インテルとデルは、数十年にわたって法人向けデバイス分野をリードしてきました。膨大な量のデータとテレメトリを絶えず利用して、共通のお客様のデバイスのセキュリティを継続的に強化しています。私たちの各分野の第一人者たちは、定期的に集まり、今日の包括的なセキュリティとはどのようなものか、明日はどのようなものになるのか、そして私たちの製品がサイバーセキュリティの最先端に確実にとどまるためには何に力を注ぐことが必要なのかについて議論します。

世界トップクラスのサプライチェーンセキュリティ、ハードウェアベースの保護、継続的なサポートにより、デルとインテルはダークウェブからビジネスデータを保護するように設計された商用デバイスをお客様とお客様のビジネスに提供する準備が整っています。デルのデバイスプログラムの詳細、およびビジネス目標の達成を支援する方法については、今すぐデルの営業担当者にお問い合わせください。

詳細はこちら...

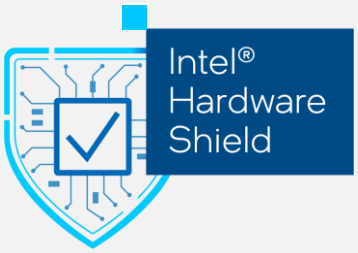
...デル・テクノロジーズの製品について

デル・テクノロジーズのセーフティおよびセキュリティのページ
Dell Trusted Devicesのページ
Dell Trusted Device Below-the-OSのホワイトペーパー
Dell SafeGuard and Responseのデータシート
Dell SafeBIOSのデータシート
Dell Supply Chain Assuranceの概要

...インテルの製品について

インテル vPro® プラットフォームのセキュリティ宣言
インテル® ハードウェア・シールドのページ
インテル® ハードウェア・シールドのホワイトペーパー
インテル Advanced Threat Protectionのホワイトペーパー
インテル バーチャライゼーション・テクノロジーのホワイトペーパー
インテル OS下層のセキュリティのホワイトペーパー
インテル トランスペアレント・サプライ・チェーンのページ
インテル2021製品セキュリティレポート

インテル® ハードウェア・シールド・テクノロジー搭載の Windowsベース・デバイス



OS下層セキュリティ

アプリケーションとデータの保護

高度な脅威からの保護

インテル® vPro® プラットフォームで動作するデルのすべての法人向けデバイスには、インテルのハードウェア・シールドが含まれています。インテルのハードウェア・シールドは、デル製デバイスの完全に統合された基盤として、OSの上層、内部、下層を保護し、デルのフルスタック・セキュリティの取り組みを強化します。

OS下層セキュリティ

BIOSおよびブートフロー保護テクノロジーによって提供

- インテル® BIOS Guard
- インテル® Boot Guard
- インテル Firmware Guard Update/Recovery
- インテル® Platform Trust Technology （インテル® PTT）
- Tunable Replica Circuit： フォルト・インジェクション検出
- インテル® Runtime BIOS Resilience
- インテル® System Resources Defense
- インテル® Trusted Execution Technology （インテル® TXT）
- インテル® System Security Report

アプリケーションとデータの保護

仮想化ベースのセキュリティによって実現

- インテル® Virtualization Technology （インテル® VT-x）
- インテル® Virtualization Technology for Directed I/O （インテル® VT-d）
- インテル® Virtualization Technology – Redirect Protections （インテル® VT-rp）
- モードベース実行制御
- カーネルDMA保護
- インテル® Total Memory Encryption（インテル® TME）
- インテル® Total Memory Encryption – Multi-Key （インテル® TME-MK）
- インテル® Advanced Encryption Standard New Instructions（インテル® AES-NI）
- 高度な割り込み設定コントローラの仮想化

高度な脅威からの保護

CPUの動作監視とGPUのオフロードで有効化

- インテル® Threat Detection Technology （インテル® TDT）
- インテル® TDT Accelerated Memory Scanning
- インテル® TDT Anomalous Behavior Detection
- インテル® TDT Advanced Platform Telemetry
- インテル® Control-flow Enforcement Technology （インテル® CET）

デルの法人向けデバイスは、設計から配送そしてその先まで、エンドツーエンドのセキュリティを完備

設計

プランニング、評価、分析

セキュリティ中心の設計

検証とテスト

リリース

お客様のもとへ

安全な施設、入念な審査を経たスタッフ、高頻度で監査を受ける信頼できるパートナーが、組み立てられた製品が安全なデバイスとして当社の工場から出荷されることを確実にします。

Dell Secured Component Verification* またはインテル® vPro® プラットフォームを使用したインテル® Transparent Supply Chain ツールには、ハードウェアベースのセキュリティ検証機能が組み込まれています。

デルのデバイスは、入念な審査を経たロジスティクス・プロバイダにより配送され、物理的なセキュリティレイヤと改ざん検知テクノロジーによって保護されます。

使用時

デルとインテルのセキュリティソリューション

Dell SafeGuard and Response

Dell SafeData

VMware Workspace ONE®

OS上層

OS下層

デルのプロテクション

- Dell SafeBIOS
- Dell SafeID
- Dell SafeScreen

インテル® ハードウェア・シールド

- 高度な脅威からの保護
- アプリケーションとデータの保護
- OS下層セキュリティ

デルとインテルのセキュリティチームによる継続的なサポートと脅威の監視

図5： デルとインテルが協力して、お客様のビジネスに安全なシステムを提供

* 現在、米国連邦政府のみで利用可能