ソリューション概要

インテル® vPro® プラットフォーム
情報セキュリティー

インテル® vPro® プラットフォーム：現代の脅威に対抗するプロアクティブなデバイス保護

進化する脅威が検出を逃れる中で、ハードウェアから始まるエンドツーエンドのセキュリティー手法が必要とされています

サイバー・セキュリティーをめぐる状況はますます速いペースで変化を遂げており、組織は巧妙な攻撃の増加を目の当たりにしています。インテル® vPro® プラットフォームは、パフォーマンス、セキュリティー、安定性、運用管理性を実現するための幅広く堅牢な基盤を企業に提供するように構築されており、ハードウェア・ベースのプロアクティブな防御を通じてこれらの新しい脅威に対応する強力な手段を提供します。

オペレーティング・システムよりも下層を狙うファームウェアのエクスプロイトの増加により[1]、組織をターゲットにした攻撃は数と種類の両面で急増しています[2, 3]。最高情報セキュリティー責任者 (CISO) や最高情報責任者 (CIO) など、企業ネットワークの保護責任者は、これまでにないエンタープライズ・セキュリティー手法が必要であると認識し始めています。従来からある境界ベースの防御モデルに取って代わろうとしているのが、セキュアなエンティティーは 1 つもないという前提に基づく「ゼロトラスト」モデル戦略です。ゼロトラストのセキュリティー手法では、ソフトウェア・スタック全体を最上層から最下層まで監視して保護し、クラウドからエンドポイントまでの通信のセキュリティーを確保する必要があります。

ハードウェアに根付く必要のあるゼロトラストのセキュリティー・アプローチ

この新しい全体論的な考え方の前提になるのは、極めて堅牢なセキュリティー基盤がハードウェア内にあることです。信頼の基点を確立し、これを図 1 のように上方へ推移させてスタック全体に行き渡らせることができるのは、ハードウェア層のみです。ハードウェアに根付かないトラストチェーンは、1 階の鍵を開けたままにし、監視も付けていない建物のようなものです。このように保護が不十分だと、デバイス起動時にあらゆる種類の悪意あるコード (ルートキットやブートキットなど) がひそかにシステムを乗っ取る可能性がありますが、従来のウイルス対策アプリケーションはオペレーティング・システムの範囲外をチェックできないので検出されないままになります。

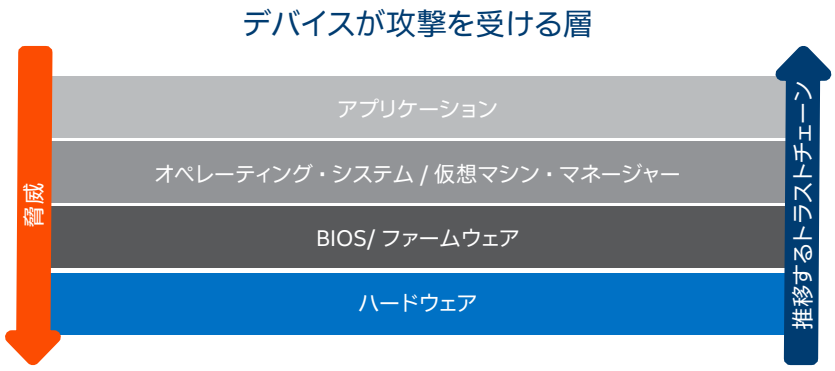

図 1. エンドツーエンドの防御には、ハードウェアに根付くセキュリティーが必要です。

インテル® vPro® プラットフォーム：さらにセキュアな IT 環境

インテルは、組織や IT プロフェッショナルが現在のセキュリティー課題を解決できるように全力で支援しています。この目的に向けて、インテル® vPro® テクノロジーはセキュリティー戦略をハードウェア上に構築できるようにします。図 2 に示すように、インテル® ハードウェア・シールドは インテル® vPro® プラットフォームの基盤として機能します。この基盤の上に構築されるのが、CISO/CIO チームが次の 4 つの最優先セキュリティー目標を達成するために役立つ機能です。

- 脅威の検出の有効性を高める
- 盗用および改ざんからのデータ保護を強化する
- ID およびアクセス保護を改善する
- セキュリティー侵害後の復旧時間を短縮する

脅威の検出における有効性を向上するため、インテル® vPro® プラットフォームはインテル® スレット・ディテクション・テクノロジー (詳しくは後述) を提供しています。盗用および改ざんからのデータ保護を強化するためには、暗号化アクセラレーションや高エントロピーの鍵を生成するインテル® セキュアキーなどのデータ暗号化機能を提供しています。また、インテル® vPro® プラットフォーム・インフラストラクチャーはさまざまな多要素認証ソリューションをサポートすることで、ID およびアクセス保護の強化を可能にしています。最後に、インテル® アクティブ・マネジメント・テクノロジー (詳しくは後述) を通じて、より迅速な復旧時間を実現します。

インテル® vPro® プラットフォームだけで使用できるインテル® ハードウェア・シールド

現代のサイバー脅威は、オペレーティング・システム (OS) より下層レベルのデバイスをターゲットにすることが多々あります。この場合、マルウェア対策アプリケーションの認知および監視対象から外れるので、実際に損害が生じ、痕跡も隠されてしまいます。インテル® vPro® プラットフォームはこのような脅威に対抗するため、インテル® ハードウェア・シールドと呼ばれ、BIOS およびファームウェア層にもセキュリティーを適用する新しいセキュリティー・テクノロジーを使用しています。このハードウェア・ベースのテクノロジーは、ファームウェア (またはデバイスドライバー) のバグまたは脆弱性を使用して悪意のあるコードが実行中のプラットフォームに注入され、従来のウイルス対策ソリューションから隠されるリスクを軽減するのに役立ちます。

インテル® ハードウェア・シールドは、ファームウェア攻撃を防ぐために役立つセキュリティー機能を内蔵しており、次の機能によってファームウェア攻撃の阻止を強化します。

- 実行時に BIOS 内のメモリーアクセスを制限することで、悪意のあるコードが注入されるのを防ぎます。
- ファームウェアからアクセスできないインテルのハードウェア保護型コード環境で、OS およびハイパーバイザーを動的に起動します。この方法では、オペレーティング・システムと仮想化環境が、ハードウェアになりすましたマルウェアではなくインテルのハードウェアで直接実行されていることを確認できます。
- ブート時に使用された BIOS およびファームウェアの保護方法をオペレーティング・システムから認識できるようにします。

残りのスタックをよりセキュアに維持するには、強力なセキュリティー基盤が必要です。インテル® ハードウェア・シールドは、立ち上げとオペレーティング・システムの起動から実行中までにわたってマシンを保護することで、企業のファイアウォールの内外を問わず、組織内のすべての PC に堅牢なセキュリティー基盤を提供します。

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)

従業員が分散している現在の環境では、数多くの企業デバイスが企業ファイアウォールの外側のリモート・ロケーションにあるため、攻撃の防止と対応は複雑化する一方です。その良い例に、ファームウェアの脆弱性へのリモート対応があります。リモート管理者は通常、デバイスの操作とソフトウェア・パッチの適用のため、デバイスの OS に接続しなければなりません。しかし、ファームウェア・パッチが OS ブート前に実行されるアプリケーションに適用される場合もあれば、OS より下層のデバイス・ファー

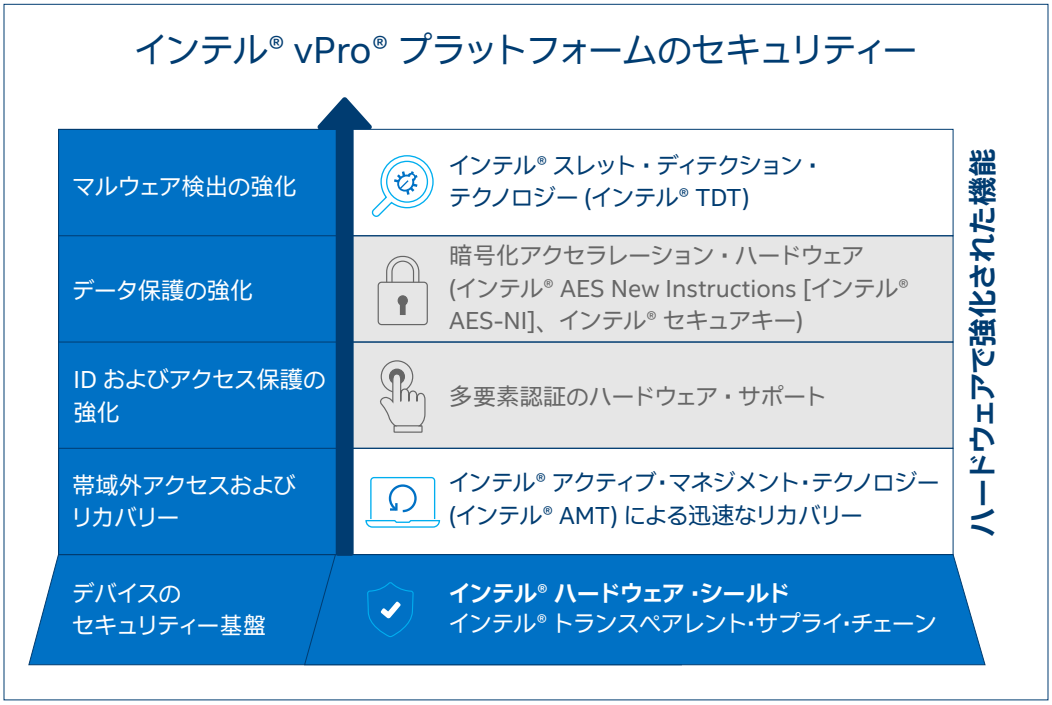

図 2. インテル® vPro® プラットフォームは、エンドツーエンドのセキュリティー戦略に必要とされる堅牢な基盤を提供します。

ムウェアを物理的に操作するために IT 技術者が必要になる場合もあります。最終的にデバイスのセキュリティーが侵害されると、デバイスの制御が悪意ある行為者の手に渡って、有用なデータが盗用または削除される恐れがあり、場合によってはデバイスを取り戻すための身代金が要求されかねません。リモート・ロケーションから操作する場合、実際の被害が生じる前に物理的にアクセスして素早くデバイスの電源を落とすことは常に実現可能とは限りません。

インテル® vPro® プラットフォームは、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) と呼ばれる機能を通じて、低レベルのソフトウェア・パッチを適用する方法とデバイス制御をハッカーから取り戻す方法を提供します。インテル® AMT とインテル® エンドポイント・マネジメント・アシスタント (インテル® EMA) ソフトウェア管理ツールを組み合わせると、オペレーティング・システムより下層でデバイスに対して持続的に帯域外接続できるので、フルキーボード、ビデオ、マウス (KVM) 機能を可能にし、リモートサーバーに保管された安全な環境を使用してよりセキュアな方法でブートできます。インテル® AMT があれば、クラウド経由の帯域外でも帯域内でも、セキュリティー侵害されたシステムやフリーズしたシステムの制御を安全に回復できるので、CISO はデバイスの安全性を確保できるという安心感を得ることができます。

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)

最近のエクスプロイトはさまざまなテクニックを使用して検出を逃れており、この問題は、CISO をはじめ、組織資産を守る必要のあるセキュリティー責任者を悩ませています。このようなテクニックの 1 つに、システムメモリー内に常駐 (してメモリーを変更) することで、シグネチャー・ベースのディスク・スキャン・テクニックを回避するマルウェアがあります。インテル® vPro® プラットフォームは、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) により、従来のマルウェア対策保護にあるギャップを埋めています。

一連のハードウェア支援型テクノロジーであるインテル® TDT を使用することで、セキュリティー・プロバイダーは既存のマルウェア対策ソリューションを強化し、高度なサイバー脅威を検出することができます。インテル® TDT は、ソフトウェア開発キット (SDK) およびリファレンス・ソリューションとして、パートナー・セキュリティー・プロバイダーに提供されます。

インテル® TDT が提供する機能は以下のとおりです。

- 特定のセキュリティー・ワークロード向けの**シリコン・アクセラレーション**。Accelerated Memory Scanning (AMS) を使用すると、マルウェア向けのメモリー・スキャニングをオンボードのインテルのグラフィックス・エンジンにオフロードできます。この方法では、メモリーのスキャン効率を高めながらパフォーマンスのオーバーヘッドを低く抑えられるだけでなく、最終的に、システムメモリー内に潜むマルウェアの検出範囲を広げることができます。近い将来、インテル® TDT の機能セットは既存の利点に基づいて拡張される予定であり、このオフロード機能がその他いくつかのセキュリティー関連機能にも適用されます。
- ターゲットを絞った検出による**エクスプロイト検出**はインテル® TDT が持つもう 1 つの強力な機能で、人工知能 (AI) とインテル独自のハードウェア・テレメトリーを組み合わせることで、エクスプロイトをプロファイリングしてその挙動を検出します。この機能は有効性が高くオーバーヘッドの低いツールとなるので、セキュリティー・プロバイダーは、侵入型のスキャンテクニックやシグネチャー・データベースを使用せずにマルウェア検出を進歩させることができます。この機能は、ディスクスキャナーに検出されないマルウェアやゼロデイ攻撃など、検出すべきシグネチャーを持たない脅威に対して特に有効です。

企業向けに構築され、よりセキュアな PC 基盤を提供する インテル® vPro® プラットフォーム

インテルは組織が日常的に直面する脅威をふまえた上で、デバイスのセキュリティー確保に役立つ新技術の開発を継続していきます。エンドポイント・セキュリティーの出発点はハードウェアにあります。インテル® vPro® プラットフォームは、現在から将来にわたってエンドツーエンドのセキュリティーを実現できる確固たる基盤の構築に貢献します。

インテル® vPro® プラットフォームのセキュリティー機能について、さらに詳しい情報をお求めの場合は、インテルの担当者までお問い合わせいただくか、以下のリンクを参照してください。

- http://www.intel.co.jp/vPro/
- http://www.intel.co.jp/hardwareshield/
- http://www.intel.co.jp/AMT/

[1] National Institute of Standards and Technology (NIST)、National Vulnerability Database、https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=firmware+&search_type=all (英語)

[2] WatchGuard、『WatchGuard's Threat Lab Analyzes the Latest Malware and Internet Attacks』、http://www.watchguard.com/wgrd-resource-center/security-report-q1-2019/ (英語)

[3] Dark Reading、『Malware Variety Grew by 13.7% in 2019』、2019 年 12 月、http://www.darkreading.com/threat-intelligence/malware-variety-grew-by-137--in-2019/d/d-id/1336611 (英語)

インテル® テクノロジーの機能と利点はシステム構成によって異なり、対応するハードウェアやソフトウェア、またはサービスの有効化が必要となる場合があります。実際の性能はシステム構成によって異なります。**絶対的なセキュリティーを提供できる製品やコンポーネントはありません。**詳細については、各システムメーカーまたは販売店にお問い合わせいただくか、http://www.intel.co.jp/ を参照してください。

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。原典を確認し、ほかの情報も参考にして、参照しているデータが正確かどうかを確認してください。

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、特定のソフトウェア、またはサービスの有効化が必要となる場合があります。各システムメーカーまたは販売店にお問い合わせください。

Intel、インテル、Intel ロゴ、Intel vPro は、アメリカ合衆国および / またはその他の国における Intel Corporation またはその子会社の商標です。
* その他の社名、製品名などは、一般に各社の表示、商標または登録商標です。

インテル株式会社
〒100-0005 東京都千代田区丸の内 3-1-1
http://www.intel.co.jp/

©2020 Intel Corporation. 無断での引用、転載を禁じます。
2020 年 8 月

342345-003JA
JPN/2008/ PDF/CB/MKTG/SI