

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

サイバー脅威が姿、形を変えて巧妙化し、検出の手を逃れる中で、組織には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・アプローチが不可欠となっています。



ビジネスニーズに応える

組織を標的とする攻撃が、数と種類の両面で急増するにつれて<sup>1,2</sup>、オペレーティング・システムよりも下の表層にあたるファームウェアの脆弱性を突くエクスプロイトが多発するようになりました。<sup>3</sup> インテルは、最高情報セキュリティ責任者(CISO)など、企業および政府機関のネットワーク保護を担当する責任者と協力し、境界型セキュリティの限界を示して、「ゼロトラスト」セキュリティの概念を広めようとしています。

例えば、官民が連携してパブリック・クラウドを活用し、APIによる効率性と有効性の向上を図ることが世界中の政府機関で推進されています。しかし、こうした改革に、従来の境界ベースの防御モデルを適用することはできません。その代わりとなるのが、「無限に安全なエンティティなど1つもない」ことを前提とした、より厳格なゼロトラスト戦略です。このセキュリティ・アプローチでは、スタック全体を継続的に監視して、最上層から最下層まで、クラウドからエンドポイントまでが保護されなければなりません。

インテル® vPro® プラットフォームは、巧妙化する攻撃の増加を目の当たりにする組織に、システムを保護、検出、回復するプロアクティブなハードウェア・ベースのセキュリティ戦略を通じて、新たな脅威に対抗するゼロトラストの対策を提供します。

オペレーティング・システムより下層のセキュリティ、アプリとデータの保護、高度な脅威検出のための機能を備えたインテル® ハードウェア・シールドによって、保護が強化されます。システムが侵害された場合でも、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)により、IT部門はリモートでシステムを回復できます。インテル® トランスペアレント・サプライ・チェーンでは、サプライチェーンの可視性を高めるために、システム・コンポーネントの信頼性を追跡できます。

ビジネスニーズに応えるインテル® vPro® プラットフォームは、ビジネスクラスのパフォーマンスと体験、内蔵されたよりセキュアな基盤、IT部門への最新の運用管理機能、信頼性の高い安定したプラットフォームを提供します。

## ハードウェアを基点とすべきゼロトラストのセキュリティ・アプローチ

エンタープライズ・セキュリティをこの最新かつ総合的な視点で考えるには、ハードウェア・ベースの強固なセキュリティ基盤が欠かせません。信頼の基点を確立し、スタック全体で下層から上層方向へ行きわたらせることは、ハードウェア層でのみ可能になります。ハードウェアを基点としない信頼のチェーンなど、1階の鍵を開けたまま監視もされ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、あらゆる種類の悪意のあるコードによって、デバイスの起動時にシステムが密かに乗っ取られてしまう危険性がありますが、従来のソフトウェア・ベースのマルウェア対策アプリケーションでは通常オペレーティング・システムの範囲外は監視できないため、攻撃が検出されないままになってしまいます。

## インテル® vPro® プラットフォーム： さらにセキュアなIT環境を作るエンドポイント

インテル® vPro® プラットフォームは、企業がハードウェア基盤のセキュリティ戦略を立てられるよう、攻撃が発生する前に保護して、ユーザー体験への影響を最小限に抑えて攻撃を検出し、侵害が発生した場合には迅速に回復できるように設計されています。図1に示すように、インテル® vPro® プラットフォームにはインテル® ハードウェア・シールド、インテル® AMT、インテル® トランスペアレント・サプライ・チェーンが備わり、CISOチームが次のような最優先のセキュリティ目標を達成できるようサポートします。

- 窃取や改ざんからのデータ保護の強化
- 脅威検出の有効性の向上

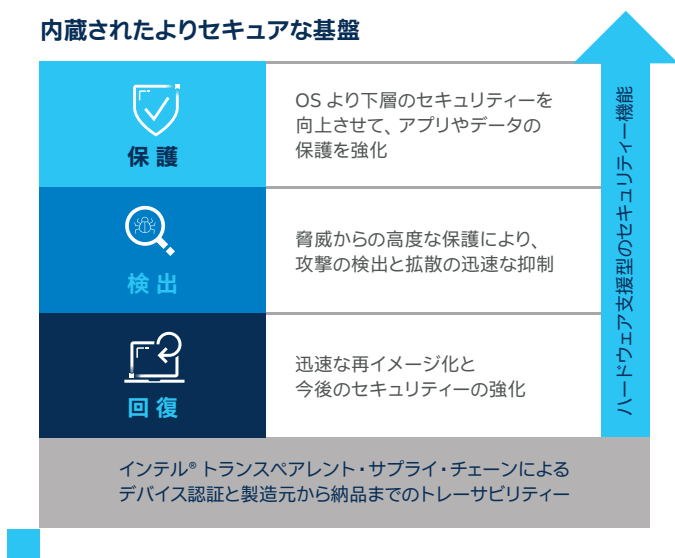


図1. エンドツーエンドのセキュリティ戦略に向けたハードウェア基盤を提供するインテル® vPro® プラットフォーム

### インテル® ハードウェア・シールドによる OSより下層のセキュリティ

最近のサイバー脅威は、OSより下層レベルでデバイスを標的にすることが多く、マルウェア対策アプリケーションの検知と監視の範囲を超えて損害を及ぼし、攻撃の痕跡さえ残さないこともあります。インテル® vPro® プラットフォームは、OSより下層を防御するインテル® ハードウェア・シールドのセキュリティ機能を使用して、BIOSとファームウェア層にもセキュリティを拡張することによって、こうした脅威に対抗します。このハードウェア・ベースのテクノロジーにより、ファームウェア（またはデバイスドライバー）のバグや脆弱性を突いて、実行時に悪意のあるコードをプラットフォームに埋め込み、そのコードが従来のマルウェア対策ソリューションから隠されてしまうリスクを軽減できます。

セキュリティ機能が内蔵されたインテル® ハードウェア・シールドは、次のような方法でファームウェア攻撃を防御します。

- ブート時に使用されたBIOSとファームウェアに対する保護手法をOSが認識できるようにする

- システムに不可欠なリソースをロックダウンして、悪意のあるソフトウェアの侵入を防ぐ
- ハードウェアとファームウェアへの不正な変更を特定できるようにする
- ファームウェア・ベースの攻撃による悪影響を低減する
- Unified Extensible Firmware Interface (UEFI) の保護と可視化により、悪意のあるコードの侵入を防ぐ

### インテル® ハードウェア・シールドによる エンドポイント・アプリケーションとデータの保護

インテル® ハードウェア・シールドにはほかにも、ハードウェア・アクセラレーションによる仮想化と暗号化を使用して、ユーザーの生産性にマイナスの影響を与えることなく、アプリケーションやデータを保護する機能があります。例えば、仮想マシン (VM) をPCのOSや別のVMから完全に分離することで、強力なセキュリティ境界を構築することが可能です。仮想化により、コンピューターを迅速に回復することもでき、仮想化されたワークロードが侵害された場合でも、ワークスペースは個別に分離されているため、ほかのワークロードに影響を及ぼすことなく、問題解決にかかる時間とコストを削減できます。

インテル® ハードウェア・シールドは、アクセラレーションされた暗号化で仮想化のアクセラレーションを補完します。データを保護するには、データとシステムメモリの暗号化を含めたすべての層で、ハードウェア・ベースのセキュリティ機能が必要です。

### 高度なサイバー脅威の検出精度を向上させる インテル® ハードウェア・シールド

最近の 익스プロイトはさまざまな手口を駆使して検出をかくぐるため、組織の資産を守らなければならないCISOやセキュリティ担当者にとって大きな悩みの種となっています。こうした攻撃の1つが、システムメモリに常駐してメモリを書き換えることで、シグネチャー・ベースのディスクスキャン検知をすり抜けるマルウェアです。インテル® ハードウェア・シールドは、高度な脅威検出機能によって、従来のマルウェア対策では防げないギャップを補います。

インテル® ハードウェア・シールドの高度な脅威検出機能は、一連のハードウェア支援型テクノロジーで構成されています。セキュリティ・プロバイダーは、これらを使用して既存のマルウェア対策ソリューションを強化することで、高度なサイバー脅威を検出できます。この機能は、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、パートナーのセキュリティ・プロバイダーに提供されます。

ユーザーの体験や生産性への影響を最小限に抑えた高度な脅威検出は、次の機能によって実現されます。

- 特定のセキュリティ・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) を使用して、メモリのマルウェア検出スキャンをオンボードのインテル® グラフィックス・エンジンにオフロードすることができます。この手法によって、パフォーマンスのオーバーヘッドを抑えながらメモリスキャンの効率を高めると同時に、最終的にシステムメモリに潜むマルウェアの検出範囲を拡大できます。既存のメリットを強化するために、近い将来、脅威検出機能セットを拡張し、ほかのセキュリティ関連機能でもこのオフロード機能が有効になる予定です。
- ターゲットを絞った 익스プロイト検出: 익스プロイトをプロファイリングし、その挙動を検知する方法として、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、ターゲットを絞った検出を行います。この機能によって非常に効果的でオーバーヘッドの低いツールが加わり、セキュリティー・プロバイダーは、侵入型攻撃のスキャン手法やシグネチャー・データベースを必要とせずに、マルウェア検出の精度を向上させることができます。この機能は、ディスクスキャナーで検知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がない脅威に対して特に有効です。

- **マルウェアからのメモリー保護**: ZDIが公開している脆弱性の半数以上を占める、ジャンプ指向/呼び出し指向プログラミング (JOP/COP) 攻撃やリターン指向プログラミング (ROP) 攻撃からメモリーを保護します。インテルのエンジニアは、第11世代インテル® Core™ vPro® プロセッサ・ファミリーで、これまで長い間ソフトウェアのみのソリューションをすり抜けてきたあらゆる種類の攻撃をシャットダウンする画期的なテクノロジーを開発しました。<sup>4</sup>

### 制御フロー・ハイジャック攻撃からの防御

制御フロー・ハイジャックは、オペレーティング・システムや、ブラウザ、読み取りツールをはじめ、多くのアプリケーションを標的としてシステムメモリーを攻撃する、急速に増加しているマルウェアの一種です。こうしたコード再利用攻撃は、攻撃者が実行メモリーから実行中の既存コードを乗っ取ってプログラムの動作に変更を加えるため、検出や防止が特に困難となっています。

インテルは、ユーザー体験への影響を最小限に抑えて、効果的なハードウェア統合型の保護を実現するために、インテル® ハードウェア・シールドの一部であるインテル® コントロールフロー・エンフォースメント・テクノロジー (インテル® CET) を開発しました。

Microsoftなどのソフトウェア開発企業は、インテル® CETを使用して、リターン指向プログラミング攻撃やジャンプ指向/呼び出し指向プログラミング攻撃などでコードが再利用されないように阻止しています。インテルはMicrosoftと緊密に連携して、Windows 10 Enterpriseおよび開発者ツールに対応できるようにしました。これにより、アプリケーションと業界全体で、制御フロー・ハイジャック攻撃からの保護を強化できます。

インテル® CETは、制御フローを乗っ取るマルウェアの攻撃を防御する、間接分岐追跡とシャドウスタックという2つの重要な機能をソフトウェア開発者に提供します。間接分岐追跡は、ジャンプ指向/呼び出し指向プログラミング (JOP/COP) 攻撃手法から防御するために、間接分岐を阻止します。シャドウスタックは、攻撃者がRET (リターン) 命令を使用して、プログラマーの意図とは異なる悪意あるコードフローをつなぎ合わせるROP攻撃手法から防御する、リターンアドレス保護を提供します。

### インテル® AMTで、侵害発生時にもリモートから回復

従業員が分散している現在の環境では、多くの業務用デバイスが企業ファイアウォールの外側にあるリモート拠点から接続しているため、攻撃の阻止と障害時の対処はますます複雑化しています。その代表的な例が、ファームウェアの脆弱性に対するリモートからの対処です。リモート管理者は通常、デバイスのOSに接続して対象のデバイス进行操作し、ソフトウェアの更新プログラムを適用しますが、ファームウェアの更新プログラムの中には、アプリケーションを介して適用するものもあり、このタイプのアプリケーションが悪意のある第三者によって不正に利用されると、貴重なデータが窃取または削除されたり、さらにはデバイスを動作可能な状態に戻すために身代金を要求されるケースもあります。リモート環

境では、被害が発生する前にデバイスに素早く物理的にアクセスして、いつでもデバイスの電源をオフにできるとは限りません。

インテル® vPro® プラットフォームでは、インテル® AMTを使用したリモート操作によって、デバイスに更新プログラムを適用して最新の状態に保ち、下位層のソフトウェアにセキュリティー・パッチを適用し、ハッカーからデバイスの制御を取り戻すことができます。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ことで、リモートサーバーに保存された安全な環境でよりセキュアに起動する能力とともに、キーボード/ビデオ/マウス (KVM) のフル機能を提供し、OSより下層でのデバイスの永続的なアウトオブバンド接続を維持できます。

インテル® AMTを使用すると、クラウド経由のインバンドでもアウトオブバンドでも、不正にアクセス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取り戻すことができるようになるだけでなく、CISOにとってはデバイスを適切に保護できるという安心感が得られます。

### インテル® トランスペアレント・サプライ・チェーンによるコンポーネントのトレーサビリティ確保

サイバー情勢はネットワーク攻撃だけにとどまりません。サプライチェーンとチャネルのセキュリティーにも懸念は高まっています。サプライチェーンのプラクティスは信頼できるソースから始まりますが、現在のプロセスでは、PCシステムがどこで、何を使って、どのように製造されているかについて、透明性もトレーサビリティも十分ではありません。

インテル® トランスペアレント・サプライ・チェーンは、システム・コンポーネントの信頼性追跡を目的とした管理方針と手順の集合です。これにはシステム・コンポーネントを製造時点から追跡するように設計された証明書ベースのツールが含まれており、Trusted Computing Group (TCG) Platform Certificate Version 1.1仕様に準拠した出力によって、偽造PCコンポーネントを識別できます。

例えば、OEMはPCを工場から出荷する前に、PCのデジタル・フィンガープリントを取得し、クラウドに格納します。PCが届いたら、顧客はまた別にデジタル・フィンガープリントを取得し、デジタル証明書で保護された元のフィンガープリントと照合します。両方のフィンガープリントが一致しない場合、顧客はそのPCをすぐに隔離し、OEMとともに調査を開始できます。

インテル® トランスペアレント・サプライ・チェーンにより、顧客に対する透明性も高まり、インテルが提供する商用システムの一部やインテル® vPro® プラットフォームを基盤とするシステムで、コンポーネント・レベルのトレーサビリティが確保され、電子部品の偽造リスクが軽減します。顧客は、製造時から初回起動時までシステムに何らかの変更が行われたかを特定する検証ツールに加えて、PCコンポーネントに関する多種多様な情報を含んだデータレポートを手に入れることも可能です。これにより、購入したPCの真正性を確保し、顧客の信頼を高めることができます。

まとめると、インテル® トランスペアレント・サプライ・チェーンにより、顧客は次のことが可能になります。

- ビジネスPC資産の詳細情報の可視化
- システムやコンポーネントの出所の追跡と検証
- ビジネスPCおよびサーバーの品質保証 (QA) の改善

## ビジネスニーズに応え、 PCにさらに安全な基盤を提供する インテル® vPro® プラットフォーム

インテルは、デバイスの安全性を維持し、最新のIT戦略に合った新しいテクノロジーを開発し続けています。サイバー攻撃から組織を守るには、適切なデバイスを選択し、更新プログラムを適用して最新の状態に保ち、サービスを階層化することが不可欠となります。エンドポイント・セキュリティはハードウェアから始まります。インテル® vPro® プラットフォームにより、現在だけでなく将来的なエンドツーエンドのセキュリティを確保する強固な基盤を構築できます。

### 詳細情報

インテル® vPro® プラットフォームのセキュリティ機能の詳細については、インテル担当者にお問い合わせいただくか、次のリンクを参照してください。

- <http://www.intel.co.jp/vPro/>
- <https://www.intel.co.jp/content/www/jp/ja/architecture-and-technology/hardware-shield.html>
- <http://www.intel.co.jp/AMT/>



<sup>1</sup> WatchGuardのレポート。「WatchGuard's Threat Lab Analyzes the Latest Malware and Internet Attacks (WatchGuard 脅威ラボの分析に基づく最新のマルウェアとインターネット脅威)」  
<https://www.watchguard.com/wgrd-resource-center/security-report-q1-2019/> (英語)

<sup>2</sup> Dark Readingの記事。「Malware Variety Grew by 13.7% in 2019 (マルウェアの亜種発見は2019年に13.7%増加)」2019年12月。<https://www.darkreading.com/threat-intelligence/malware-variety-grew-by-137-in-2019/d/d-id/1336611> (英語)

<sup>3</sup> 米国国立標準技術研究所(NIST)。国家脆弱性情報データベース。[https://nvd.nist.gov/vuln/search/results?form\\_type=Basic&results\\_type=overview&query=firmware+&search\\_type=all](https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=firmware+&search_type=all) (英語)

<sup>4</sup> インテル® コントロールフロー・エンフォースメント・テクノロジー(インテル® CET) は、ジャンプ指向 / 呼び出し指向プログラミング (JOP/COP) 攻撃、リターン指向プログラミング (ROP) 攻撃といった攻撃手法からの防御を目的に設計されています。これらの攻撃手法は、メモリーの安全性を脅かす問題として知られるマルウェアであり、ZDIが公開している脆弱性の半数以上を占めています。詳細については、<http://www.intel.co.jp/11thgenvpro/> を参照してください。絶対的なセキュリティを提供できる製品またはコンポーネントはありません。結果は異なる場合があります。

ここに記載されているすべての情報は、予告なく変更されることがあります。インテルの最新の製品仕様およびロードマップをご希望の方は、インテルの担当者までお問い合わせください。

性能は、使用状況、構成、その他の要因によって異なります。詳細については、<http://www.Intel.com/PerformanceIndex/> (英語) を参照してください。

性能の測定結果は、構成情報に記載された日付時点のテストに基づいています。また、現在公開中のすべてのアップデートが適用されているとは限りません。構成の詳細については、パフォーマンス指標を参照してください。

インテルは、これらの資料を現状のまま提供し、明示されているか否かにかかわらず、いかなる保証もいたしません。

絶対的なセキュリティを提供できる製品またはコンポーネントはありません。

実際のコストや結果は異なる場合があります。

Intel、インテル、Intelロゴ、その他のインテルの名称やロゴは、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/>

©2021 Intel Corporation。無断での引用、転載を禁じます。

2021年6月

342345-004JA  
JPN/2106/PDF/SE/NBDG/KS