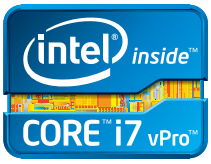
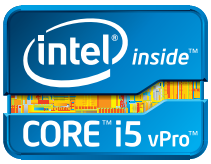
クライムウェアからの保護：第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリー

ホワイトペーパー

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリー





概 要

今日の巧妙なサイバー犯罪者は、ビジネス・クライアントにクライムウェア（犯罪行為を目的として作られたマルウェア）を仕込むための新しい手法を次々と見出しています。そして、これらの犯罪行為を支えるステルス型ウイルスやプログラムコードは、ウイルス検出機能やオペレーティング・システム（OS）から検出やアクセスが不可能な階層に侵入します。最近では、このような潜伏性の高いマルウェアがセキュリティー専門家によって多く確認されており、企業の IT 部門は、こうした数々のクライムウェアから IT システムを保護する必要性に迫られています。

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーは、OS よりも深い階層となるハードウェアとファームウェア上で機能するビルトインのセキュリティー技術[1] によって、このようなセキュリティーの新しい課題に応えます。インテルのセキュリティー技術は、脅威管理の強化、ID 窃取の検出と防止、暗号強度と安全性の向上、企業データとビジネス・クライアントの盗難防止などを実現します。また、もし被害に遭ったときには、修復のためのコストを削減できるように支援します。

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーに統合されたセキュリティー技術は、既存のテクノロジーでは到達できなかったセキュリティー・レベルでビジネス・クライアントを強固に保護します。このホワイトペーパーでは、インテルのプロセッサーに組み込まれているセキュリティー技術の概要とともに、IT 部門の最も厳しいセキュリティー課題に対してこれらの技術がどのように役立つかを解説します。

目 次

企業 IT に求められる新たな脅威の管理

ますます顕在化する情報セキュリティーの課題

かつてのアマチュアハッカーが、ウイルスの流布によって広範囲にわたる脅威を生み出していた時代と異なり、今日のサイバー犯罪者は、より標的を絞った攻撃を企てています。企業スパイ活動、企業活動の妨害、機密データの流出、ハクティビズム（政治的ハッキング活動）など、彼らが特定の標的とその攻撃結果を意識して作成するマルウェアは、従来のウイルスと比べるとはるかに潜伏性が高く、検出や修復も困難です。

サイバー犯罪者たちは、ステルス型の手法を通じて企業の IT システムにクライムウェアを送り込みます。そして、クライムウェアが標的となるシステムを見つけたら、オペレーティング・システム（OS）を超えて、より深い階層に侵入します。これらのプログラムコードは、OS から認識やアクセスが不可能な領域に潜伏し、攻撃活動、検出と駆除が困難な方法による自己増殖、ID の窃取などを実行する機会が訪れるのをひたすら待ち続けます。

Stuxnet のマルウェア病理学と Zeus によって提供されるツールキットは、このようなサイバー犯罪者がいかに巧妙で、しかも大きな被害をもたらす隠れたバグの作成がいかに簡単であるかを示しています。これらは、まさに情報セキュリティーにおける新種の脅威といえます。そして、インテルのグループ企業である McAfee のセキュリティー専門家によれば、このような新種の攻撃が企業に対して実行される頻度はさらに高まっていくと予想されています。[2]

進化するビジネスによってセキュリティーの課題がさらに複雑化

最近の脅威は、データ、デバイス、アプリケーションとユーザー間のやり取りを巧みに利用します。このため、ビジネスの運営モデルが進化するとともに、攻撃の機会も増える結果となっています。

仮想デスクトップやクラウドに基づく各種サービスといった新しいサービス・デリバリー・モデルによって、高度な脅威からインフラストラクチャーを保護する課題がますます増大しています。Web ベースのアプリケーション、企業ネットワークや機密性の高いアカウントへのアクセス、電子メールなど、コミュニケーションのための出入り口は、これらの脅威がデータの損失、ID の窃取、不正侵入などの攻撃を行う機会を与えます。

また、常に安全性を確保しなければならないモバイル機器が多様化することで、セキュリティーの問題がさらに複雑化しています。ノートブック PC の普及に加えて、スマートフォンやタブレットといったさまざまなモバイル機器が主流になり、クライムウェアの侵入経路も増加しています。IT 部門は、これらのあらゆる脅威から企業の IT システムを確実に守らなければなりません。そのためには、こうしたマルウェアの攻撃に対してだけでなく、従来ながらの物理的な盗難の防止や被害の軽減にも取り組む必要があります。

保護戦略

サイバー攻撃から企業を守るには、攻撃に立ち向かうすべての領域で強固な戦略が求められます。こうした戦略には以下のようなものが挙げられます。

脅威の管理：潜伏しているプログラムコードをウイルス検出 / 駆除ソフトウェアによって検出、特定、阻止するだけでなく、OS よりも深い階層でマルウェアの侵入口となる脆弱性を保護します。

ID とアクセスの管理：ユーザーが確かに本人であること、そして窃取した ID によるマルウェアのなりすましでないことを確認します。

データ損失の防止：ビジネス・クライアントとデータの盗難による損害から企業を守ります。また、暗号化手法そのものが破られないように、今日において最高レベルの暗号化技術を適用します。

監視、通知、修復：マルウェアが脆弱性を見つけ出す前に、こうした脆弱性をあらかじめ認識、解決することで、脅威の予防と管理を実現します。また、攻撃に対する予防に加え、攻撃を受けた際に必要とされる修復のためのコストと労力を軽減します。

OS よりも深い階層で働く強力なセキュリティー

今日のクライムウェアの実情を見ると、非常に巧妙なソフトウェアは、ウイルス検出ツールによる検出と駆除が困難な階層に弱点を見つけ出し、そこから侵入しています。こうした悪質なプログラムコードに対処するには、高度なウイルス検出 / セキュリティー・ソフトウェアを補完、支援するハードウェア・ベースのソリューションが必要になります。そして、これらのソリューションは、OS よりも深い階層で動作することにより、脅威が脆弱性を利用して侵入や攻撃を試みようとしたときに、その脅威を素早く検出、ブロックします（図 1）。

ビルトインのセキュリティー機能を搭載したビジネス・クライアント

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載したビジネス・クライアントでは、OS よりも深い階層となるプロセッサー・シリコン、プラットフォーム・ハードウェア、ファームウェアの中にセキュリティー技術が組み込まれています。インテルのテクノロジーは、脅威の管理、ID とアクセスの管理、データ損失の防止、監視 / 通知 / 修復など、高度なセキュリティーが求められる最前線で威力を発揮します。インテルのテクノロジーとそこに組み込まれているツール群は、ソフトウェア・ベースの脅威に対する検出、ID 窃取の回避と予防、暗号強度のさらなる強化を実現します。また、PC の物理的な盗難に対するコストを最小化するとともに、盗難や紛失に遭った PC が見つかったときには、その復旧作業も支援します。

インテルの最新テクノロジーに対応したビジネス・クライアントを導入することで、IT 部門は、予防と修復のためのコストを抑えながら、今日の巧妙なステルス型クライムウェアによる攻撃を防ぐことができます。

ここでは、こうした最前線のセキュリティー対策がどのような方法によって可能になるのか、またインテルのテクノロジーがどのような仕組みで今日の高度な脅威から企業 IT を防御しているのかを説明していきます。

図 1. インテルのセキュリティーを支える 3 本の柱：企業の IT 環境を保護する包括的なアプローチ

脅威の管理

あらゆる有害なルートキット型マルウェアからの保護

今日の巧妙なサイバー犯罪者は、ルートキット、ゼロデイの脆弱性に対する知識、アプリケーション・メモリーへのウイルス侵入などにより、アンチウイルス・ソフトウェアから認識、アクセスできない領域に悪意のあるプログラムコードを隠そうとします。これらのコードは未検出のまま潜伏し、やがて OS によって実行されたり、仮想化環境に埋め込まれたり、知らない間に通常のアプリケーション・プロセスとして呼び出されたりします。

インテルのセキュリティー技術は、半導体チップに組み込まれた次のような機能によって高度な攻撃からシステムを保護し、脅威の管理を実現します。

- 権限昇格攻撃を用いたマルウェアからの保護
- 安全な「信頼のルート（root of trust）」を仮想化環境に提供
- メインメモリーを監視してマルウェアの侵入をチェック
- デバイスを隔離してダイレクト・メモリー・アクセス（DMA）攻撃から保護

OS より深い階層での保護

インテルのプロセッサーに数世代前から実装されているインテル® エグゼキュート・ディスエーブル・ビットは、データメモリー上に置かれた悪意のあるプログラムコードの実行を未然に防ぐことで、多数のビジネス・クライアントをバッファー・オーバーフロー攻撃から守ってきました。しかし、最新の脅威は、アプリケーション・メモリー空間内に悪意のあるコードを挿入し、アプリケーション向けに想定された特権レベルで実行しようとします。

インテル® エグゼキュート・ディスエーブル・ビットの後継となるインテル® OS ガード[3] は、データメモリー空間の保護に加えて、アプリケーション・メモリー空間でも悪意のあるプログラムコードが実行されるのを防ぎ、これらのコードによる権限昇格攻撃からシステムを保護します。このよう

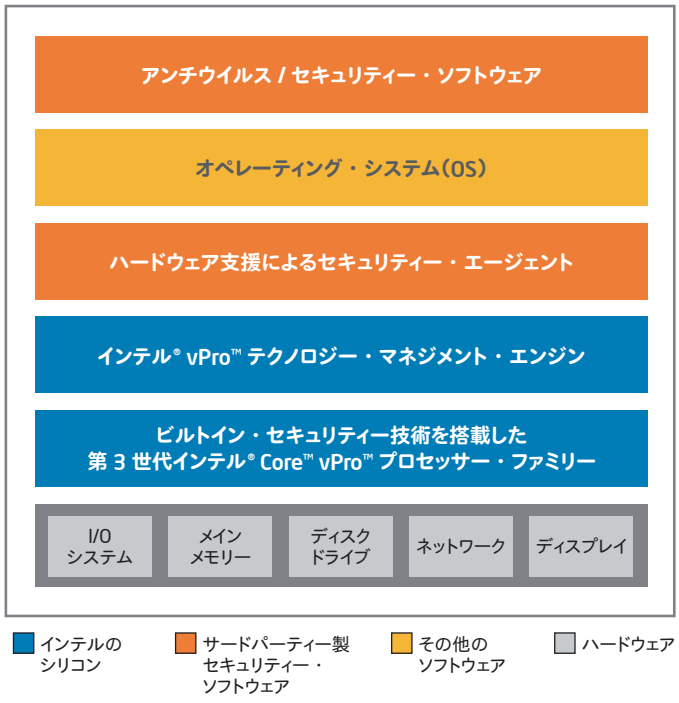


図 2. ハードウェア・レベルで実装されたインテルのビルトイン・セキュリティー機能

に、OS より深い階層でシステムを保護することによって、高度なウイルスとそれがもたらす被害から企業を守ります。

仮想領域の保護

クラウド・ベース・コンピューティングや仮想デスクトップなどの新しいサービス・デリバリー・モデルは、IT 部門に新たな課題を与えています。未検出のプログラムコードが仮想マシン（VM）の起動時に侵入すると、企業の仮想システム全体（エンドユーザー自身が利用する仮想デスクトップ環境またはそのサービス全体）に被害を及ぼします。インテル® バーチャライゼーション・テクノロジー [4]（インテル® VT）に対応した新しいセキュリティー・アプリケーションを含む、インテルのビルトイン・セキュリティー技術は、サービス・デリバリー・レベルそして仮想化された各クライアントという、物理環境と仮想化環境の双方に対する保護を支援します。

インテル® トラステッド・エグゼキューション・テクノロジー [5]（インテル® TXT）は、ホスト上で起動される VM に対してハードウェア・ベースの「信頼のルート（root of trust）」を確立します。インテル® TXT は、既知の良好なホスティング環境を測定し、その条件および状態を信頼できる基準として格納します。ホストシステムの起動時には、インテル® TXT が既知の正常な測定値と照らし合わせながら主なコンポーネントの動作を検証し、ホスティング環境が信頼できると判断された場合にのみ VM を起動します。VM が起動されると、インテル® TXT がこの VM 向けに割り当てたメモリー・パーティションを同一システム上の他のソフトウェアから隔離し、ホストまたは他の VM 環境を経由して実行される可能性のある攻撃から VM を保護します。アプリケーションまたは VM がシャットダウンされると、インテル® TXT がメモリー空間の内容を完全に消去してから安全にソフトウェアを終了させて、ソフトウェア上のデータが他のアプリケーションや環境に流出しないようにします。このように、インテル® TXT は、ハードウェアによって支援されたセキュリティー技術であり、クライアント・ソフトウェアを破壊しようとするルートキット型マルウェアから物理環境と仮想化環境の双方を保護します。

インテル® バーチャライゼーション・テクノロジーは、数世代にわたるインテル® プロセッサーにおいて、信頼できるセキュリティー技術として仮想化環境の堅牢性とパフォーマンスの向上に寄与してきました。インテル® VT は、インテル® VT-x とダイレクト I/O 向けインテル® VT（インテル® VT-d）という 2 つの要素によって、それぞれ特定のセキュリティー保護機能を提供します。

- **インテル® VT-x** は、各 VM の実行環境を隔離しながら、同時にメインメモリーを監視します。これにより、1 つの VM 環境内にすでに潜伏もしくはこれから侵入しようとしているマルウェアが、同一ホスト上の他の VM に悪影響を及ぼしません。
- **ダイレクト I/O 向けインテル® VT（インテル® VT-d）**は、仮想デバイス、そしてそのデバイスに割り当てられたメモリー空間と仮想アドレスを隔離します。マルウェアをはじめとする脅威が、デバイスに割り当てられたメモリー空間に直接アクセスできなくなるため、DMA アクセスを利用した攻撃を防げます。

ID とアクセスの管理

本人確認のための機能

ID の漏洩を起因とする企業への標的型攻撃は、その件数を年々増加させています。企業は、このような問題に対処するため、自社のシステムにアクセスする際に、安全性の高い資格情報を用いてユーザー認証を行うようにしています。しかし、ソフトウェアのみの資格情報は、OS やアプリケーションから見える場所に格納されるため、巧妙なステルス型クライムウェアによる窃取や破壊に対して脆弱な状態となります。そこで、多くの企業ではハードウェア・トークン、スマートカード、USB キーなどを導入することで、こうしたリスクを軽減していますが、これらのソリューションに対するハードウェア・キーの配布（プロビジョニング）、管理、サポートには多くのコストがかかります。

インテル® アイデンティティー・プロテクション・テクノロジー [6]（インテル® IPT）は、ハードウェア・レベルのビルトイン・セキュリティー機能を通じて、従来型のディスクリート・トークンやスマートカードを使用することなく、ID 窃取からシステムを保護するセキュリティー製品スイートとなります。インテル® IPT は、ディスクリート・トークンならではの強力なセキュリティーと、ソフトウェア・ベース・ソリューションならではの優れた運用性や情報漏洩に対する迅速な対応力を兼ね備えています。

インテル® アイデンティティー・プロテクション・テクノロジー

セキュリティーの専門家は、固定パスワードなどの一要素認証では不十分であることを認めています。このため、多くの企業では、セキュリティー強度の高い二要素認証を使用して、VPN ログインや Web ポータルなどのアクセスポイントを保護したり、電子メールのセキュリティー確保や文書の暗号化などを行っています。二要素認証の形式としては、ワンタイムパスワード（OTP）トークンと公開鍵基盤（PKI）証明書の 2 種類が一般的です。そして、これらの多くはディスクリート・トークンやスマートカード上に組み込まれています。

このようなハードウェア・ベースの ID 保護手段によって、正当な権限を持つユーザーのみが保護されたネットワークとアカウントにアクセスできるようになり、不正行為の大幅削減もしくは撲滅につなげています。しかし、企業での運用経験や最近の出来事から、以下のようないくつかの課題も明らかになってきました。[7]

- ユーザーが資格情報を紛失、忘却することで、ヘルプデスクに大きな負担がかかっています。
- トークン、スマートカード、付加的な管理ソフトウェアに多くのコストがかかっています。
- 最近発生したトークンに内蔵されたシードに関する情報の漏えい事件により、物理トークンの交換コストとトークンを交換するまでの生産性低下が大きな問題として取り上げられています。物理トークンの交換自体は可能ですが、実際に交換するまではさまざまな攻撃に対して脆弱な状態であり続けます。

一部のセキュリティー・ソリューションは、ハードウェア・セキュリティーの運用保守コストを省くために、OTP トークンと PKI 証明書を PC 上に格納しています。これにより、必要に応じてこれらの証明書情報を簡単に無効化したり、再びプロビジョニングしたりできます。しかし、このようなソフトウェア・ベースのソリューションでは、証明書情報が OS やアプリケーションから見える場所に格納されるため、標的型攻撃のリスクをさらに増大させる結果となります。

ハードウェア・ベースのセキュリティーとソフトウェア・ベースの利便性を両立

インテル® IPT は、OS とアプリケーションからアクセスできないシリコンチップの内部に、OTP トークンや PKI 証明書を格納します。そして、これらの証明書情報に対する無効化、再プロビジョニング、管理も容易に行

えます。さらに、パスワードや PIN（暗証番号）などの適切な認証情報が入力されたときにのみ、鍵情報にアクセスできます。これにより、物理トークンの紛失に関わる問題が解消されます。

インテル® IPT は、ハードウェア・ベースのソリューションによる強力なセキュリティーと、ソフトウェア・ベースの柔軟性や優れたコスト効率を両立させることで、以下のような機能を提供します。

- マルウェアがアクセスできないシリコンチップの内部（ソフトウェアや OS よりも深い階層）で OTP 資格情報や PKI 証明書を保護します。
- 実際のユーザーだけが入力できる環境下で適切な認証が実行されたときに限り、鍵情報へとアクセスできるようにします。
- ユーザーのデータ入力を OS やアプリケーションから見えないようにすることで、キーロガーやスクリーン・スクレーパーによるリスクを排除します。

ユーザー入力の保護

最近見られる一部の攻撃によれば、認証パスワードと暗証番号がキーロガーによって取得され、機密データにアクセスされる危険性が出ています。プロテクテッド・トランザクション・ディスプレイ対応インテル® IPT は、OS やデバイスドライバーから見えない階層でユーザー入力の取得と表示を行います。キーロガーやフレーム・バッファー・リーダーのプログラムコードは、ユーザーの活動を全く読み取れなくなるため、キーロガーやスクリーン・スクレーパーによる ID 窃取を防止できます。

容易に導入可能な OTP 認証機能対応のインテル® IPT

多くの企業は、主要な認証プロバイダーのうち 1 社を選び、OTP ソリューションを導入しています。こうした OTP 認証機能を備えたインテル® IPT は、現在のシステムに最小限の変更を加えるだけで利用でき、ハードウェア・ベースの強力なセキュリティーとソフトウェア・ベースの利便性を同時に提供します。自社の PC を第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリー搭載クライアントへと移行していく中で、これまでと同じ認証プロバイダーを利用しながら、新しい PC にハードウェア・ベースの OTP 資格情報を配備し、物理的なトークンを段階的に撤去していくことが可能です。OTP 認証機能を備えたインテル® IPT は、すでに大手ベンダーの多くがサポートしています。

PKI 機能を備えたインテル® IPT にも迅速に移行可能

PKI 証明書に基づくセキュリティー・ソリューションを導入している企業は、PKI 機能を備えたインテル® IPT を導入することで、ハードウェア・ベースの強力なセキュリティーを維持しながら、証明書の管理を簡略化できます。PKI 機能を備えたインテル® IPT は、Symantec* Managed PKI Solution と互換性があり、現在のシステムに最小限の変更を加えるだけで利用できます。自社の PC を第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリー搭載クライアントへと移行していく中で、これまでと同じ認証プロバイダーを利用しながら、新しい PC にハードウェア・ベースの PKI 証明書を配備し、物理的なスマートカードを段階的に撤去していくことが可能です。

データ損失の防止

データの安全性を確保

ビジネスデータは、さまざまな形式で多くのシステムに保管され、しばしば企業の物理的境界を越えて外部に移送されます。例えば、スマートフォン上の電話帳や通信データ、ノートブック PC 上にあるマーケティングや事業計画関連の文書、サーバー上の知的財産や設計データなどは、さまざまなデバイスからローカルアクセス、もしくは公衆ネットワーク上のセキュアなトンネルやプライベート・ネットワークを経由してリモートアクセスが行われます。このため、携行しているデバイスとこれらのデバイスに紐付く重要なデータ（転送時または保管時）を脅威から守ることは、IT 部門にとって大きな課題となります。

インテルのビルトイン・セキュリティー技術は、データとこれらのデータを格納しているビジネス・クライアントの両方に対して、以下のような機能を通じてデータの損失を防ぎます。

- 暗号化 / 復号処理の高速化
- 暗号化アルゴリズムのシード生成に使用される、安全で高性能な真の乱数生成
- 物理デバイスに対するセキュリティー技術

全社規模での暗号化を実現

重要なデータの保護のためには、何よりも優先してデータの暗号化を行うべきです。強固な暗号化を行わないと、窃盗犯たちが、長年蓄積してきた知識情報という企業の最重要資産へと簡単にアクセスできてしまうからです。これに対し、ディスク全体もしくは選択したファイル / フォルダーに暗号化を施すことによって、企業の機密情報におけるセキュリティーを確保できます。しかし、オンザフライ方式の暗号化 / 復号を実行すると、これまではクライアントのパフォーマンスが低下して従業員の生産性に悪影響を及ぼしていました。このため、企業の多くは、全社規模で暗号化を導入することに強いためらいを感じています。

Advanced Encryption Standard（AES）アルゴリズムは、OS やセキュリティー・ソフトウェアの暗号化 / 復号プロセスに広く採用されている標準的な暗号化規格です。インテル® AES New Instructions[8]（インテル® AES-NI）は、AES の処理を高速化する 7 つの新しい命令から構成されており、McAfee* Endpoint Encryption など、インテル® AES-NI に最適化されたアプリケーションの暗号化 / 復号処理を最大 4 倍に高速化します。インテル® AES-NI に最適化された暗号化製品を導入することによって、パフォーマンスと生産性の低下を回避できます。また、第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載した最新のビジネス・クライアントを導入することで、全社規模での暗号化が可能になります。

これにより、従業員の生産性を高いレベルで維持しながら、データの安全性も同時に確保できます。

真の乱数生成

安全性が守られた暗号化の処理は、一般的にクライアント内の疑似乱数ジェネレーターによって提供される乱数シード（乱数生成に用いられる初期値）から始まります。乱数の品質が高ければ高いほど予測しにくくなり、同時にセキュリティーも向上します。また、乱数の生成処理がしっかりと保護されていれば、暗号化の安全性も高められます。しかし、生成された乱数がメインメモリー上に格納されるシステムでは、高度なマルウェアによって危険にさらされます。

インテル® セキュアキー [9] は、乱数のクリーンな生成源として、マルウェアから認識、アクセスできないハードウェア内で乱数を生成する機能を提供します。ここでは、自律的に動作し、すべての機能が揃ったデジタル乱数ジェネレーターがプロセッサー・パッケージ内に搭載され、チップセットに依存しない形で実装されています。

インテル® セキュアキーは、次のような機能を備えています。

- NIST SP 800-90 規格に準拠し、NIST FIPS 140-2 Level 2 の認証も取得しています。
- 新しいプロセッサー命令を使用し、どのような特権レベルからでも、あらゆるアプリケーションに対して容易にアクセスできます。
- 外部からシステムの状態が全く見えず、メインメモリーを含めてどこにも格納されることがない「閉じたシステム」を提供します。

インテル® セキュアキーは、以下のようなソフトウェア・アプリケーション、サービス・プロバイダー、ソフトウェア・ベンダーなどにメリットをもたらします。

- 証明書を発行するセキュリティー・ソフトウェア・ベンダー
- SSL 暗号化通信が可能な Web ブラウザー
- データ暗号化ソリューション・プロバイダー
- オペレーティング・システム（OS）

インテル® セキュアキーは、システムのパフォーマンスを低下させることなく、暗号化による保護をさらに促進します。

紛失したノートブック PC の保護

ノートブック PC に保管されている企業データの保護は、IT 部門にとって最も重要な課題ですが、モバイル利用に関する厳格なポリシーを適用している場合でも、しばしば大きな困難を伴います。これは、産業スパイ活動や企業秘密の窃取をたくらむ犯罪者たちが、モバイル機器の脆弱性をよく理解しているためです。

世界中の空港では、毎日数百台のノートブック PC が紛失したり、盗難に遭っていますが、こうした PC の大半には機密データが保管されています。第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーに組み込まれているインテル® アンチセフト・テクノロジー [10]（インテル® AT）は、紛失したり、盗難に遭ったノートブック PC とそのデータを自己防衛する機能を提供し、ノートブック PC に保管されている企業データを守ります。また、インテル® AT を導入することで、紛失したノートブック PC の現在位置を IT 部門に報告したり、PC が見つかったときにリモート操作によってシステムを復元することも可能です。

ノートブック PC 上でインテル ® AT を有効にすると、IT 部門のセキュリティー管理者が PC に対する脅威を事前に定義できます。例えば、窃盗犯によって誤ったログイン ID が入力される、脅迫されたユーザーが偽のログイン ID を入力する、企業ネットワークへの接続時に PC が定期的なチェックインを怠るといった脅威が挙げられます。IT 管理システムがこのような脅威を検出すると、PC に対してポイズンピル（端末の機能を無効化するメッセージ）を送信し、PC を即座にロックします。

インテル® AT では、システムがロックされると以下の操作が行われ、ノートブック PC とそのデータのどちらも使用できなくなります。

- ノートブック PC に組み込まれたすべてのセキュリティー鍵を一時的に利用不可（または利用不能）にし、ID の窃取に利用されないようにします。ただし、これらの鍵は IT 部門によって復元可能です。
- ディスクドライブへのアクセスとデータの復号を不可能にすることで、ディスク上のデータにアクセスされることを防ぎます。仮にディスクドライブを他のデバイスに接続したとしてもアクセスできません。
- ロックされたノートブック PC に新しいドライブを接続しても、PC はいっさい動作しません。このため、OS インストール済みのドライブから OS を起動したり、新しいドライブに OS の再インストールを行うことはできません。
- ノートブック PC が 3G ネットワークへの接続機能をサポートしている場合には、PC 自身の GPS 位置情報を IT 部門に送信できます。

ノートブック PC がエンドユーザーの手元に戻ってきたときには、ユーザー自身が IT スタッフに連絡して適切な認証を行ったり、IT 部門のリモート操作によってシステムを正常な状態に復元できます。エンドユーザーもしくは社内の技術スタッフは、これまでのように数時間や数日ではなく、わずか数分という短い時間で ID の鍵情報を復元し、システムのロックを解除して再び使用可能な状態に戻せます。

このように、ハードウェアで支援されたインテルのビルトイン・セキュリティー技術は、外出先でもノートブック PC とそのデータをさまざまな脅威から守ります。

インテル® vPro™ テクノロジーによる監視、通知、修復

脅威の検出、IT 管理システムへの通知、データ復元とユーザーの生産性回復といった一連の管理プロセスには、多くの時間とコストがかかります。そして、時間が経過すればするほど、脅威がもたらす潜在的なコストも大きなものになります。

インテルのビルトイン・セキュリティー技術とインテル® アクティブ・マネジメント・テクノロジー [11]（インテル® AMT）は、修復と管理のコストを最小限に抑えながら、IT 部門の認知、制御、応答能力を最大限に高めます。これらの技術は、第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載したビジネス・クライアントの重要な要素であり、以下のような機能を提供します。

- ユーザーが脅威を知覚する前であっても、ノートブック PC 上で脅威の自動的な検出、システムロック、脅威の通知が行えます。また、リモート操作によるシステムの修復もサポートしています。
- ハードウェアとソフトウェアのリモート資産管理機能により、すべてのセキュリティー・ソフトウェアとセキュリティー・データベースが最新の状態であることを確認できます。
- 業務時間外でシステムの電源がオフになっている場合でも、クライアント上で重要なソフトウェアのダウンロードと更新作業を自動的に行えます。[12]
- 実行中の重要なセキュリティー・エージェントを自動的に検出し、エージェントが見つからないか、アクティブになっていないときには通知を行います。
- ネットワーク・トラフィックのフィルタリングと脅威を受けたときの通信切断を自動的に行います。
- ビジネス・クライアントにリモートからアクセスし、技術スタッフがそのクライアントの前に座っているかのような完全な操作環境を提供します。

監視と予防

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載したビジネス・クライアントは、システムの健康状態の常時監視、ハードウェアおよびソフトウェアの資産管理、検出された異常に対する適切な応答によって、クライアントそれぞれが高度な自衛能力を維持します。

修復よりも予防を重視することの優位性

実際に起こってしまったリスクに対処するよりも、潜在的なリスクを検出して事前に回避するほうが容易で、コストもかかりません。そこで、第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載したビジネス・クライアントは、ハードウェアおよびソフトウェアの定期的な資産管理、健康状態の監視、異常の報告などを通じて、リスクの事前回避を優先します。

これらのビジネス・クライアントは、監視したすべての活動と状態の記録を不揮発性メモリーに保持します。IT スタッフまたは自動化されたコンソールは、この不揮発性メモリーからいつでもビジネス・クライアントの情報を取得できます。ソフトウェアの資産管理は、ソフトウェアが最新の状態であるかどうかや、リスクにさらされているかどうかをチェックし、事前に決められたスケジュールに従ってソフトウェアの自動更新を行います。ここでは、リスクの高いアプリケーションを直ちに更新し、リスクの低いアプリケーションを業務時間外に更新することで、業務へのインパクトを最小限に抑えつつ高いセキュリティーを維持します。また、ファームウェアやハードウェアが危険な状態にあると判断された場合には、リモートからファームウェアの更新を行ったり、ハードウェアに対して必要に応じた更新または交換のフラグを立てられます。IT 部門は、このような予防措置によってコストの削減を図ることができ、さらには各 PC の資産状態を正確に把握することで、社内のビジネス・クライアントをどのように管理すべきかを効率よく的確に判断できるようになります。

重要なエージェントに対する動作状態の自動監視と通知を常に実施

IT 集中管理システムの中には、ネットワーク経由でリモート・クライアントのポーリングを行い、アンチウイルス・ソフトウェアや暗号化ソフトウェアなど、重要なセキュリティー・エージェントが実際に動作状態にあるかどうかを監視するものがあります。通常、脅威が検出されていないときには、エージェントが存在し、アクティブな動作状態となっています。しかし、このようなエージェント監視で積極的な通知を受けるためには、貴重なネットワーク帯域を消費します。また、外出先でノートブック PC を使用しているときなど、管理システムとの間でネットワーク接続を維持できない場合は、重要なエージェント監視が中断されてしまいます。

インテル® AMT に対応したビジネス・クライアントには、自律的に動作するセルフポーリング・エージェントがシステム内部に組み込まれています。このセルフポーリング・エージェントは、重要なソフトウェアの存在を監視し、その状態を記録していきます。ポーリングの結果は、システムの不揮発性メモリーにすべて保管されるため、IT 部門はこれらの情報に対してリモートからいつでもアクセスできます。

システムに不可欠なソフトウェアの存在が正しく通知されない場合、インテル® AMT は管理コンソールに連絡して IT 部門に異常を知らせたり、IT ポリシーに従ってクライアントの安全性を確保します。クライアントが管理システムからのネットワーク・ポーリングに応答する代わりに、クライアント自身が自律的に監視を行うことで、ネットワークへの接続性によらずクライアントが常時保護されます。また、システムが正常に動作しているときには、ネットワーク帯域も無駄に消費されません。このように、IT 部門が直接介入しない形で自動的に監視が行われることで、コストを効果的に抑えながら、より高度なクライアント保護を実現します。

ネットワークの自動監視と適切な応答によって感染の拡大を防止

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載したビジネス・クライアントは、ネットワーク・トラフィックの監視などを通じて、さまざまなタイプの侵入手段からシステムを守ります。このようなネットワーク監視と保護のプロセスは、実行中に破壊されるおそれのあるソフトウェアではなく、ネットワーク・アダプターのハードウェア内で処理されます。

IT 部門は、セキュリティー応答のトリガーとなるネットワーク・フィルターを事前に定義することで、ネットワーク上のクライアントと企業資産を保護できます。ここでは、ネットワークの脅威を検出するために以下のような通信状況を監視します。

- ネットワーク・アダプターで受信した**トラフィックのタイプ**を監視することで、データに埋め込まれた脅威からシステムを保護します。
- （デスクトップ・クライアント内の）**ネットワーク・アクティビティー・レート**を監視することで、分散型サービス拒否攻撃（DDoS 攻撃）からシステムを保護します。

システムが脅威を検出すると、DDoS 攻撃が継続されないように、システム自身が自らをネットワークから切り離して感染の拡大を防ぎます。ネットワークの切断は、OS のネットワーク・スタックではなく、ネットワーク・アダプターによってハードウェア的に処理されます。これにより、すでに侵入しているおそれのあるステルス型クライムウェアからもアクセスできないハードウェア内の階層でシステムを確実に隔離します。

ここでは、アウトオブバンドで修復を行うためのネットワーク経路だけが開放された状態となるため、IT 部門はリモートからシステムを管理し、正常な状態に復旧することができます。

管理者が自席にいながら対応できるリモート修復によってサポートコストを最小化

標準的な企業において、デスクサイド・サポートやサービスセンターへの問い合わせが、PC の全トラブル件数に対して小さな比率にもかかわらず、IT 管理予算の大部分を占めていることが業界の調査によって分かっています。また、外部から頻繁に攻撃を受けているような状況下では、これらの攻撃に対するサポートによってさらに多くのコストが必要になります。リモート修復機能は、オンサイトサポートに関連するコストを最小限に抑え、従業員の生産性を迅速に回復させることで、こうしたクライアント・サポートに関する課題に応えます。

IT スタッフは、リモート KVM（キーボード、ビデオ、マウス）制御機能 [13] を備えたインテル® AMT によって、自分の席を離れることなくビジネス・クライアントをリモートから完全に制御し、以下のような操作を実行することができます。

- クリーンな状態で再起動を行うか、クリーンなローカル / リモートイメージ、診断サーバー、修復サーバー、その他のデバイスに起動デバイスをリダイレクトする**リモート / リダイレクト・ブート**を行えます。
- **Serial-Over-LAN（SOL）コンソール・リダイレクション**により、OS 外の環境でキーボードを制御し、エンドユーザーの手を煩わせることなく、サービスセンターから BIOS 設定変更などの操作を行えます。
- **資産情報にアクセス**することで、検出不可能もしくは故障したハードウェア・コンポーネントの特定やソフトウェア・バージョン情報の確認をいつでも行えます。
- BIOS の問題、OS のブルースクリーン障害、OS やアプリケーションの

フリーズ、パッチ適用時の障害といった複雑な問題、もしくはその他の深刻なソフトウェア問題に対して、エンドユーザーの手を煩わせることなく、**PC のトラブルシューティング・セッションを実行**できます。

- **BIOS、デバイスドライバー、OS の起動状態をチェック**することで、システム起動プロセスの問題点を特定できます。
- **BIOS 設定の更新**、BIOS バージョンの特定、最新バージョンへの BIOS アップデートといった手段によって、BIOS に起因する特定の問題を解決します。
- 不揮発性メモリーから**イベントログを持続的にアップロード**することで、温度の急激な上昇、不正なソフトウェアのダウンロードといった、システム障害の要因となる一連のイベントを迅速に特定できます。
- 削除または破壊された .DLL などのファイルの新しいコピーをクライアントに送り込むことで、**OS の修復作業**を行えます。
- **OS の再構築、アップグレード**、ハードディスク・ドライブの完全なイメージ復元をリモートから実行できます。

このように、ハードウェア・ベースの高度な運用管理機能によって、システムの保護と修復を自動的かつ簡単に実行できるようになり、クライアントのサポートコストが削減されます。

まとめ

今日のサイバー犯罪者は、ステルス型の新しいアプローチによって企業や団体に対する標的型攻撃を行っています。第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載したビジネス・クライアントは、ハードウェア・ベースのビルトイン・セキュリティー技術によって、これらの脅威に立ち向かいます。インテルのセキュリティー技術は、OS よりも深い階層で動作するハードウェア支援型の高度なセキュリティー・エージェントを提供します。

- インテル® OS ガード、インテル® TXT、インテル® VT は、OS よりも深い階層にマルウェアが侵入するのを防ぐことで、IT 部門による脅威の管理を支援します。
- PKI 機能を備えたインテル® IPT、OTP 認証機能を備えたインテル® IPT、プロテクテッド・トランザクション・ディスプレイ対応インテル® IPT は、ハードウェア・ベースの高度なセキュリティーとソフトウェア・ベースの利便性および修復対応能力を両立させることで、重要な ID が窃取されるのを防ぎます。
- インテル® AES-NI とインテル® セキュアキーは、より安全で高速な暗号化処理を実現します。
- インテル® AT は、外出先でノートブック PC とそのデータを保護します。
- インテル® vPro™ テクノロジー [14] は、脅威の予防や修復にかかる労力とコストを軽減します。

第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーを搭載したシステムのみがサポートする、これらのビルトイン・セキュリティー技術は、持続的に発生する今日の高度な脅威や標的型攻撃からデータとネットワークを守り、企業とデータの安全性をさらに高めます。第 3 世代インテル® Core™ vPro™ プロセッサー・ファミリーの詳細については、http://www.intel.co.jp/vpro/ を参照してください。

[1] すべての条件下で絶対的なセキュリティーを提供できるコンピューター・システムはありません。内蔵セキュリティー機能は、一部のインテル® Core™ プロセッサーで提供されているものであり、別途ソフトウェア、ハードウェア、サービスまたはインターネットへの接続、あるいはその両方が必要となる場合があります。結果はシステム構成によって異なります。詳細については、各 PC メーカーにお問い合わせください。

[2] McAfee Labs の「2012 年の脅威予測」レポート（http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf（英語））

[3] 絶対的なセキュリティーを提供できるシステムはありません。第 3 世代インテル® Core™ vPro™ プロセッサーと対応するオペレーティング・システムを搭載したインテル® OS ガード対応システムが必要です。詳細については、各システムメーカーにお問い合わせください。

[4] インテル® バーチャライゼーション・テクノロジーを利用するには、同テクノロジーに対応したインテル® プロセッサー、BIOS、および仮想マシンモニター（VMM）を搭載したコンピューター・システムが必要です。機能性、性能もしくはその他の特長は、ご使用のハードウェアやソフトウェアの構成によって異なります。ご利用になる OS によっては、ソフトウェア・アプリケーションとの互換性がない場合があります。各 PC メーカーにお問い合わせください。詳細については、http://www.intel.com/go/virtualization/（英語）を参照してください。

[5] すべての条件下で絶対的なセキュリティーを提供できるコンピューター・システムはありません。インテル® トラステッド・エグゼキューション・テクノロジー（インテル® TXT）を利用するには、インテル® バーチャライゼーション・テクノロジー、インテル® TXT に対応したプロセッサー、チップセット、BIOS、Authenticated Code モジュール、インテル® TXT に対応した Measured Launched Environment（MLE）を搭載するコンピューター・システムが必要です。さらに、インテル® TXT を利用するには、システムが TPM v1.s を搭載している必要があります。詳細については、http://www.intel.com/technology/security/（英語）を参照してください。

[6] すべての条件下で絶対的なセキュリティーを提供できるシステムはありません。インテル® アイデンティティー・プロテクション・テクノロジー（インテル® IPT）を利用するには、インテル® IPT に対応した第 2 世代または第 3 世代インテル® Core™ プロセッサーを搭載したシステム、および同テクノロジーに対応したチップセット、ファームウェア、ソフトウェア、インテル® IPT に対応した Web サイトが必要です。各システムメーカーにお問い合わせください。データやシステムの紛失や盗難など、サービス利用の結果生じたいかなる損害に対してもインテルは責任を負いません。詳細については、http://ipt.intel.com/（英語）を参照してください。

[7] Techspot の「Chinese hackers target smart cards to grab US defense data」（http://www.techspot.com/news/47053-chinese-hackers-target-smart-cards-to-grab-us-defense-data.html（英語））

[8] インテル® AES New Instructions（インテル® AES-NI）を利用するには、インテル® AES-NI に対応したプロセッサーを搭載したコンピューター・システム、および命令を正しい手順で実行する他社製ソフトウェアが必要です。インテル® AES-NI は、一部のインテル® Core™ プロセッサーで利用できます。提供状況については、各 PC メーカーなどにお問い合わせください。詳細については、http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/（英語）を参照してください。

[9] 絶対的なセキュリティーを提供できるシステムはありません。第 3 世代インテル® Core™ vPro™ プロセッサーとインテル ® セキュアキーをサポートするために最適なソフトウェアを搭載したインテル® セキュアキー対応 PC が必要です。詳細については、各システムメーカーにお問い合わせください。

[10] すべての条件下で絶対的なセキュリティーを提供できるシステムはありません。インテル® アンチセフト・テクノロジーを利用するには、同テクノロジーに対応したチップセット、BIOS、ファームウェア、ソフトウェアを搭載したシステムと、同テクノロジーに対応したサービス・プロバイダーのサービスへの加入が必要です。対応状況と機能については、各システムメーカーとサービス・プロバイダーにお問い合わせください。データやシステムの紛失や盗難など、サービス利用の結果生じたいかなる損害に対してもインテルは責任を負いません。詳細については、http://www.intel.com/go/anti-theft/（英語）を参照してください。

[11] 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）によって可能となるセキュリティー機能は、インテル® AMT に対応したチップセット、ネットワーク・ハードウェア、ソフトウェア、および企業 LAN へ接続されていることが必要です。ホスト OS ベースの VPN 上や、ワイヤレス接続時、バッテリー駆動時、スリープ時、ハイバネーション時、電源切断時には、インテル® AMT を利用できないことや、一部の機能が制限されることがあります。セットアップには構成が必要となり、管理コンソールへのスクリプトや既存のセキュリティー・フレームワークへの統合、新しいビジネスプロセスの変更や導入を必要とする場合もあります。詳細については、http://www.intel.co.jp/amt/ を参照してください。

[12] システム上で Client Initiated Remote Access（CIRA）を利用するには、有線または無線 LAN に接続する必要があります。この機能は、公衆無線 LAN スポットや、接続に「click to accept（クリックによる同意）」が必要な場所では利用できない場合があります。

[13] リモート KVM（キーボード、ビデオ、マウス）制御を利用できるのは、インテル® Core™ i5 vPro™ プロセッサーおよびインテル® Core™ i7 vPro™ プロセッサーでプロセッサー・グラフィックスを有効にした場合のみです。ディスクリート・グラフィックスはサポートされません。

[14] インテル® vPro™ テクノロジーは高度な機能であり、利用するにはセットアップと有効化を行う必要があります。利用できる機能と得られる結果は、ハードウェア、ソフトウェア、IT 環境のセットアップと構成によって異なります。詳細については、http://www.intel.com/technology/vpro/（英語）を参照してください。

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/

2012 年 10 月

327161-001JA
JPN/1210/PDF/SE/MKTG/YM