IT@Intel ホワイトペーパー

インテル IT 部門

IT ベスト・プラクティス

情報セキュリティー

2011 年 1 月

情報セキュリティーの再構築による ビジネスの機敏性の向上

Omer Ben-Shalom
インテル IT 部門
プリンシパル・エンジニア

Manish Dave
インテル IT 部門
上級セキュリティー・エンジニア

Toby Kohlenberg
インテル IT 部門
上級セキュリティー・アナリスト

Dennis Morgan
インテル IT 部門
セキュリティー・ストラテジスト

Stacy Purcell
インテル IT 部門
上級セキュリティー・アーキテクト

Alan Ross
インテル IT 部門
上級プリンシパル・エンジニア

Timothy Verrall
インテル IT 部門
プリンシパル・エンジニア

Tarun Viswanathan
インテル IT 部門
セキュリティー・アーキテクト

インテル IT 部門では、この手法によって高度なユースケースの革新的なソリューションを提供し、実際にリスク軽減の成果を上げています。

概 要

インテル IT 部門は、新しいテクノロジーと利用モデルの迅速な導入を可能にし、絶え間なく脅威の変化する環境における保護を強化するために、5 年にわたるインテルの情報セキュリティー・アーキテクチャーの根本的な再設計作業に着手しました。

IT のコンシューマー化やクラウド・コンピューティングなどの重要な戦略を推進するために設計されたこのアーキテクチャーは、企業セキュリティーの全く新たな手法を実現するものです。このアーキテクチャーは、従来の企業セキュリティー・モデルに比べて、より柔軟かつ動的できめ細かいセキュリティー管理を可能にします。例えば、このアーキテクチャーは、ユーザーがいる場所や使用しているデバイスの種類（例えば、信頼度の高いノートブック PC か、信頼度の低い個人所有のスマートフォンか）などに起因するリスクレベルの変化に応じて、ユーザーのアクセス権限を動的に調整するように設計されています。また、このアーキテクチャーは、攻撃が不可避であることを前提として、生存可能性を重視しています。

新しいアーキテクチャーは、以下の 4 本の柱に基づいています。

- **信頼度計算：**信頼度計算は、特定のリソースに対するユーザーのアクセスの可否と、許可されるアクセスのタイプを動的に決定します。この計算は、ユーザーのクライアント機器の種類とその利用されている場所、要求されているリソースの種類、利用可能なセキュリティー管理機能などに基づいて行われます。

- **セキュリティー・ゾーン：**インテルの環境は、重要なデータが置かれ、アクセスが厳しく制御される信頼ゾーンから、重要度の低いデータが置かれ、より幅広いアクセスが許可される非信頼ゾーンまで、複数のゾーンに分割されます。ゾーン間の通信は、制御と監視の対象となります。これにより、あるゾーンが攻撃を受けた場合に他のゾーンに問題が広がることを防ぎます。

- **バランスのとれた管理：**このモデルでは、攻撃を防げなかった場合の回復能力と柔軟性を高めるため、ファイアウォールなどの予防的管理以外に、発見的管理と修復的管理のバランスが重視されます。

- **ユーザー境界とデータ境界：**インテル IT 部門は、企業ネットワークの境界を保護するだけでは不十分であり、ユーザーとデータを新たなセキュリティー境界として保護する必要があると考えています。

このモデルを完全に実現するためのセキュリティー技術の中には、まだ実用化されていないものもあります。インテルは、信頼度計算などの機能を支えるテクノロジーの開発を積極的に推進しています。

インテル IT 部門では、すでにこのアーキテクチャーの導入に着手しており、約 5 年にわたってインテル全社への導入を進める予定です。この手法によって高度なユースケースの革新的なソリューションを提供し、実際にリスク軽減の成果を上げています。

目 次

IT@Intel

IT@Intel は IT プロフェッショナル、マネージャー、エグゼクティブが、インテル IT 部門のスタッフや数多くの業界 IT リーダーを通じ、今日の困難な IT 課題に対して成果を発揮してきたツール、手法、戦略、ベスト・プラクティスについて詳しく知るための情報源です。詳細については、http://www.intel.co.jp/jp/go/itatintel/ を参照してください。あるいは御社担当のインテル社員までお問い合わせください。

ビジネス課題

インテルの企業セキュリティーの要件は急速に変化し、広がりを見せています。これは、クラウド・コンピューティングや IT のコンシューマー化などの新しい利用モデルの採用と、絶え間なく脅威の変化する環境によるものです。

インテルのリスク・プロファイルを図 1 に示します。また、主要なトレンドについて以下に説明します。

IT のコンシューマー化

移動機会の多いインテルの従業員は、スマートフォンなどの個人で所有しているコンシューマー機器を仕事においても利用したいと望んでいます。従業員がいつでもどこでも情報にアクセスしてコラボレーションができれば、生産性は大きく向上します。インテル IT 部門では、すでにこのような要求に応えて、従業員が所有するスマートフォンやタブレットから電子メールなどの企業データへのアクセスを限定的に許可しています。[1]

こうしたトレンドが広まるにつれて、増え続けるあらゆる形態のクライアント機器からインテルのリソースへアクセスするための一定レベルの権限を、従業員に対して与える必要が生じています。しかし、これらの機器の多くは、ノートブック PC よりはるかに弱いセキュリティー管理機能しか持っていません。

1「エンタープライズ環境でのパーソナル・ハンドヘルド機器の利用と情報セキュリティーの確保」、インテル株式会社（2011 年 2 月）。

インテルのリスクを高めることなく、新しい機器に迅速に対応し、より広範囲にわたるアプリケーションとデータへのアクセスを可能にする、新しいセキュリティー・アーキテクチャーが必要です。クライアント機器のセキュリティー管理機能に基づいて、許可されるアクセスレベルと実行されるモニタリングを動的に調整する必要があります。例えば、従業員がスマートフォンなどの安全性の低いデバイスを使用する場合は、管理された安全な PC を使用する場合に比べて、重要な企業リソースに対するアクセス権限を制限しなければなりません。

新しいビジネス要件

インテルは内部成長と企業買収を通じて新規市場の開拓を進めています。また、ビジネスパートナーとのオンライン・コラボレーション用システムも開発しています。その結果、より広範囲にわたるユーザー（その多くはインテルの従業員ではありません）にインテルのリソースへのアクセスを許可する必要が生じています。

インテル IT 部門では、このような拡大に対応し、また促進するため、インテルのデータを新規顧客に提供するオンライン・セールス・ポータルなどの新しいシステムを導入しています。また、買収した企業をスムーズに統合し、必要なリソースへのアクセスを可能にする必要もあります。つまりは、新しいユーザーからのアクセスを素早く可能にする一方で、リスクを最小限に抑え、必要なリソースへの管理されたアクセスだけを選択的に許可する必要があります。

クラウド・コンピューティング

インテル IT 部門では、仮想化インフラストラクチャーに基づくプライベート・クラウドを構築しており、重要性の低いアプリケーションについ

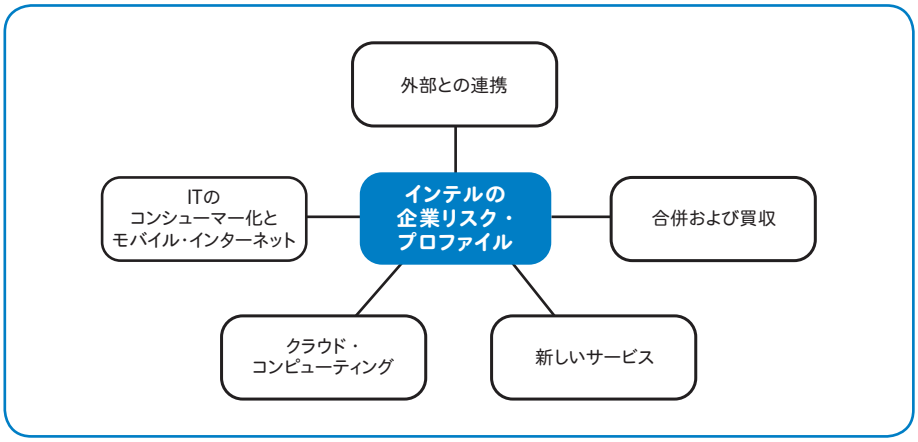

図 1. セキュリティー要件の高度化が、新しいセキュリティー・アーキテクチャーの必要性を高めています。

ては外部クラウドサービスの利用も検討しています。クラウド環境では、システムとデータは仮想化され、状況に応じて物理的または論理的にさまざまなネットワークの場所へと移行されます。このため、システムとデータの場所が固定的であることを前提とした、ファイアウォールなどの従来のセキュリティー管理手法を使用してアクセスを制限することは難しくなります。ネットワーク内のリソースの場所に関係なくリソースそれ自体を対象とする、よりきめ細かく、動的な管理が必要です。また、プラットフォームの保護と、転送中および保管時のデータの保護を強化するセキュリティー技術も必要です。インテル IT 部門では、このような機能を備えたインテル® プロセッサー搭載サーバーのテクノロジー評価を行っています。

絶え間なく脅威の変化する環境

我々をとりまく環境における脅威は急速に変化しています。攻撃者は、長時間にわたるアクセスを確保するため、ますます発見されにくい手法を利用して、ひそかに侵入して検出を免れるマルウェアを作成しています。脅威の数が増え、新しいタイプのマルウェアが出現し続ける状況では、攻撃は不可避であると想定する必要があります。

従来の企業セキュリティー・アーキテクチャーは、主にネットワークの境界に置かれるファイアウォールなどの予防的管理に依存してきました。しかし、インテル IT 部門では、単にアクセスを防ぐだけでなく、より広範囲にわたるユーザーとデバイスに管理されたアクセスを提供することへと重点を移しています。さらに、環境における脅威は絶え間なく変化しているため、攻撃の発生を前提とせざるを得ません。ひとたび攻撃者が企業環境へのアクセスを手にしてしまうと、予防的管理は回避され、その効果を失います。ネットワーク境界の管理は今後も重要ですが、それ以外に、攻撃者が企業環境にアクセスした後の生存可能性と回復能力を高めるツールを重視する必要があります。

新しいアーキテクチャーの必要性

インテル IT 部門は、セキュリティー要件が進化し、拡大する現状において、従来の企業セキュリティー戦略ではもはや不十分であると考えています。より柔軟で動的なアーキテクチャーによって、新しいデバイス、利用モデル、機能の導入を迅速化し、ますます複雑化する環境全体でセキュリティーを確保し、急速に脅威の変化する環境に対応する必要があります。

そのため、インテル IT 部門では、部門全体からメンバーを集めたチームを結成し、企業セキュリティーへの斬新なアプローチの創出、新しい要件に対応するアーキテクチャーのゼロからの設計、この新しいアーキテクチャーをインテルの既存 IT 環境に導入するプロセスの計画に取り組むことにしました。

セキュリティー・アーキテクチャー

インテル IT 部門のセキュリティー・アーキテクチャー・チームは、5 年にわたるインテルのセキュリティー・アーキテクチャーの根本的な再設計作業に着手しました。この計画は、企業セキュリティーの全く新しい手法を実現するものです。

私たちの目標は、柔軟性と従業員の生産性を高めると同時に、IT のコンシューマー化、クラウド・コンピューティング、より広範囲にわたるユーザーからのアクセスなどの新しいビジネス要件と技術トレンドをサポートするアーキテクチャーを開発することです。同時に、このアーキテクチャーは、ますます複雑化して悪質となった脅威の増え続ける環境に対して、攻撃面を削減し、生存可能性を高めるように設計されています。

インテル IT 部門では、5 年の期間を設定して新しいアーキテクチャーの導入に取り組むことにしました。これは、IT 部門全体で広範囲にわたる活動が必要であり、必要なテクノロジーの中にはまだ実用化されていないものもあるためです。

このアーキテクチャーは、二者択一的で固定的な従来のエンタープライズ向け信頼モデルを超えるものです。従来のモデルでは、ユーザーは一般的に、すべてのリソースへのアクセスを許可されるか拒否されるかのいずれかになり、一度許可されたアクセスのレベルは変化しません。新しいアーキテクチャーでは、こうした従来のモデルは、特定のリソースへのアクセスをよりきめ細かく管理できる、動的な複数層の信頼モデルに置き換わります。つまり、個々のユーザーが許可されるアクセスレベルは、ユーザーが信頼性の高い管理された PC でネットワークにアクセスしているか、それとも管理対象外の個人のスマートフォンでアクセスしているかなど、さまざまな要因に基づいて時間とともに動的に変化します。

情報セキュリティーの 5 つの法則

インテルの新しいセキュリティー・モデルは、攻撃が不可避であることを前提としています。したがって、攻撃を防げなかった場合の生存可能性と回復能力を確保することがカギとなります。インテルの情報セキュリティー統括責任者 兼 情報リスク & セキュリティー担当ジェネラル・マネージャーである Malcolm Harkins が考案した、情報セキュリティーの 5 つの法則から、攻撃の発生が避けられない理由を理解できます。

1. **情報は自由であろうとする。**
   人々は情報を話し、投稿し、共有しようとします。そのことによってリスクが増大します。

2. **プログラムにはエラーが含まれている。**
   100% エラーのないソフトウェアは存在しません。

3. **サービスは常時オンにされる。**
   一部のバックグラウンド・プロセスは、常に動作している必要があり、攻撃者に悪用されるおそれがあります。

4. **ユーザーは何でもクリックしたがる。**
   ユーザーには、Web リンク、ボタン、プロンプトなどを目にするとクリックしてしまう傾向があります。マルウェアの作成者は、こうした性質を知った上で利用しようとします。

5. **セキュリティー機能は悪用される可能性がある。**
   セキュリティー・ツールも、他のソフトウェアと同じように攻撃者によって悪用されるおそれがあります。したがって、法則 2、3、4 はセキュリティー機能についても当てはまります。

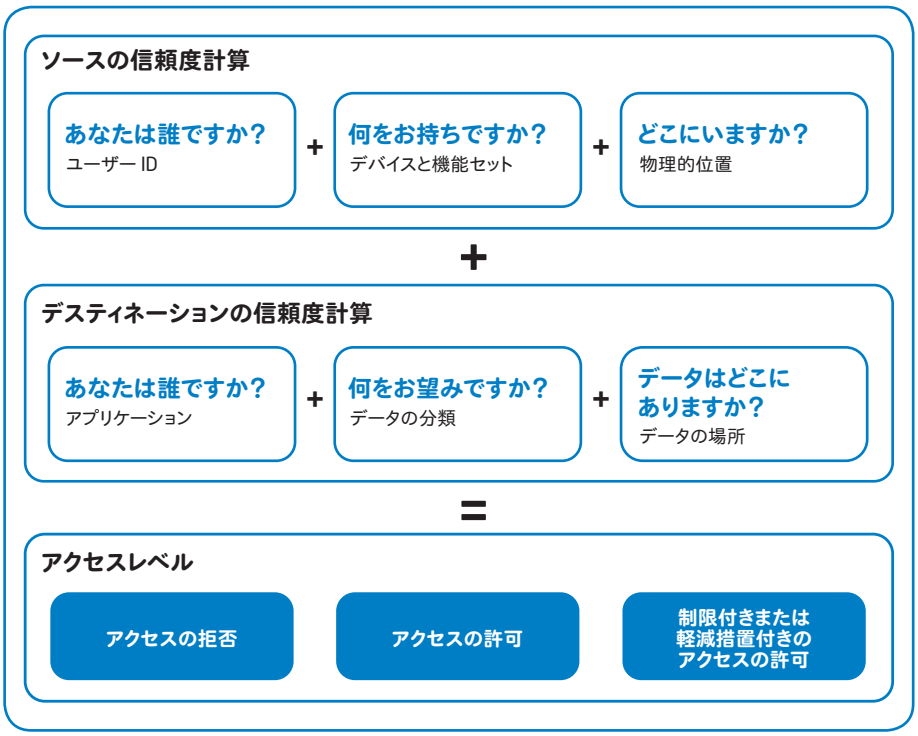

図 2. 信頼度計算は、ソースとデスティネーションについて、「誰が」、「何を」、「どこで」を考慮に入れます。

新しいアーキテクチャーは、以下の 4 本の柱に基づいています。

信頼度計算：この独自のアーキテクチャー要素を使用して、特定のリソースに対するユーザーのアクセスの可否と、許可されるアクセスのタイプを動的に決定します。この計算は、ユーザーのクライアント機器の種類とその利用されている場所、要求されているリソースの種類、利用可能なセキュリティー管理機能などに基づいて行われます。

セキュリティー・ゾーン：インテルの環境は複数のセキュリティー・ゾーンに分割されます。重要なデータが置かれ、アクセスが厳しく制御される信頼ゾーンから、重要度の低いデータが置かれ、より幅広いアクセスが許可される非信頼ゾーンまで、各種のセキュリティー・ゾーンが設定されます。ゾーン間の通信は、制御と監視の対象となります。これにより、承認済みのリソースのみにアクセスを制限し、攻撃が複数のゾーンに広がることを防ぎます。

バランスのとれた管理：このモデルでは、攻撃を防げなかった場合の回復能力と柔軟性を高めるため、ファイアウォールなどの予防的管理以外に、発見的管理と修復的管理のバランスが重視されます。

ユーザー境界とデータ境界：インテル IT 部門は、企業ネットワークの境界を保護するだけでは不十分であり、ユーザーとデータを新たなセキュリティー境界として保護する必要があると考えています。

これらの 4 本の柱について、以下に詳しく説明します。

信頼度計算

信頼度計算は、急速に増え続けるデバイスと利用モデルに対応する柔軟性を実現するために不可欠な役割を果たします。

この計算により、ユーザーが現在使用しているクライアント機器やネットワークなど、さまざまな要因に基づいて、許可されるアクセスのレベルや実行されるモニタリングのレベルを動的に調整できます。

信頼度計算は、要求する側（ソース）と要求される情報（デスティネーション）の間のやり取りの信頼度を計算します。この計算は、ソーススコアとデスティネーション・スコアで構成され、リスクの軽減に利用できる管理機能も考慮に入れられます。図 2 に示すように、この計算の結果によって、ユーザーのアクセスの可否と、許可されるアクセスのタイプが決まります。この計算には、得られたデータは常に信頼できるとは限らないという問題に対処するため、スコアの各要素の信頼性も考慮に入れられます。

信頼度計算に必要な技術の中には、まだ実用化されていないものもあります。インテルは、情報セキュリティー業界におけるこうした技術の開発を積極的に推進しています。

ソーススコア

ソース（要求する側）の信頼度は、以下の要因に基づいて計算されます。

「誰が」：アクセスを要求しているユーザーまたはサービスの ID と、使用される認証メカニズムに対するインテルの信頼レベル（ユーザーが申告している身元をどの程度信用できるか）。

「何を」：デバイスのタイプ、デバイスの管理機能、インテル IT 部門がデバイスの管理機能を検証する能力、インテル IT 部門がどの程度デバイスを管理しているか。例えば、管理されたノートブック PC は、個人が所有する管理対象外のスマートフォンよりも信頼度が高くなります。

「どこで」：ユーザーまたはサービスの場所。例えば、インテルの企業ネットワーク内にいるユーザーは、公衆ネットワークを介して接続しているときよりも信頼度が高くなります。ユーザーがいる地域など、他の要因も考慮に入れられることがあります。

デスティネーション・スコア

このスコアは上と同じ 3 つの要因に基づいて計算されますが、これらの要因は、デスティネーション（ソースがアクセスしようとしている情報）の観点から考慮されます。

「誰が」：要求されたデータを保管するアプリケーション。エンタープライズ権利管理（ERM）などの一部のアプリケーションは、より厳密に情報を管理できるため、信頼レベルが高くなります。

「何を」：要求されている情報の機密度と、漏えいが起こった場合の回復能力などの要因。

「どこで」：データが置かれるセキュリティー・ゾーン。

利用可能な管理機能

信頼度計算では、ゾーンで利用可能なセキュリティー管理機能も考慮に入れられます。アクセスの可否を制御する機能しか利用できなけ

れば、他の選択肢がないため、必要なアクセスを拒否せざるを得ないことがあります。しかし、アクセスレベルをきめ細かく管理できる各種の予防的管理機能、詳細なログ、高度に調整された発見的管理機能、問題からの回復 / 修復機能が利用できれば、リスクを増やさずにアクセスを許可することができます。

信頼度の計算

信頼度計算では、ソーススコアとデスティネーション・スコアを加算して、初期信頼度レベルを求めます。次に、利用可能な管理機能を考慮に入れて、アクセスの可否とアクセスレベルに関する最終的な決定を下します。この計算はポリシー決定点（PDP）によって実行されます。PDP は、認証インフラストラクチャーに含まれる論理的エンティティーであり、一連のポリシーに基づいてアクセス制御の決定を下します。

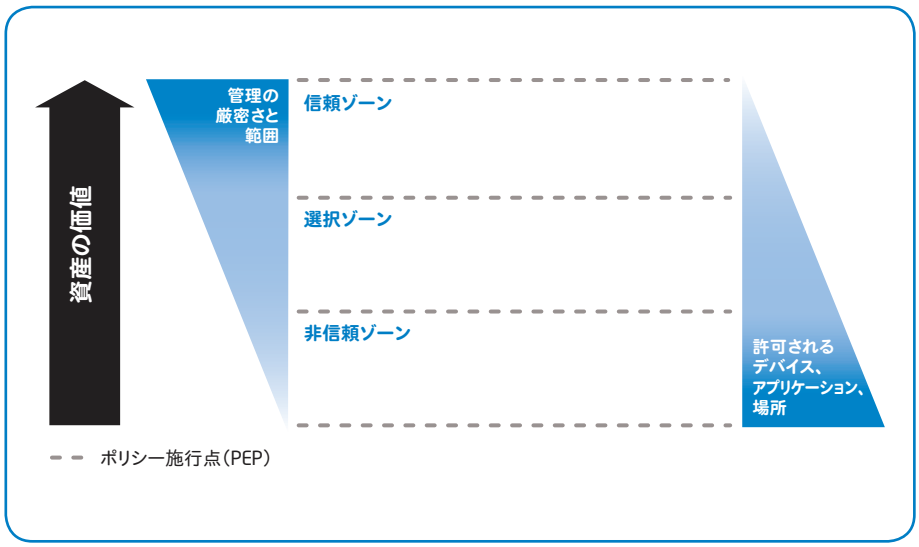

図 3. 資産価値が高いほど、管理はより厳密かつ広範囲にわたり、アクセスを許可されるデバイス、アプリケーション、場所の数は減少します。

計算の結果に基づいて、PDP は以下のことを決定します。

- アクセスの許可。
- アクセスの拒否。
- 制限付きまたは軽減措置付きのアクセスの許可。

信頼度計算により、特定のインテルのリソースに対するアクセスについて、きめ細かい管理を動的に適用できます。

例えば、トラステッド・プラットフォーム・モジュール（TPM）、衛星測位システム（GPS）機能付き無線データ通信カード、フルディスク暗号化などの追加ハードウェア機能を搭載したインテル® Core™ vPro™ プロセッサー搭載ノートブック PC を使用する場合は、個人のスマートフォンを使用する場合よりも多くのリソースへのアクセスを許可されます。また、スマートフォンを使用する場合は、公衆キオスクを使用する場合よりも多くのリソースへのアクセスを許可されます。

さらに、インテルのネットワークに直接接続する場合は、公衆ネットワークを介して接続する場合よりも広範囲にわたるアクセスを許可されます。管理された PC のようにセキュリティー・レベルの高いデバイスであっても、デバイスの位置を確認できない場合は、アクセスレベルが制限されます。

信頼度計算でスマートフォンの機種を区別することもできます。スマートフォンの管理機能、認証機能、インストールされているアプリケーションに基づいて、さまざまなレベルのアクセスを許可できます。

ビジネスの必要上、接続またはトランザクションを行わなければならないにもかかわらず、アクセスを許可するには信頼レベルが不十分であるという状況も考えられます。こうした状況でも、信頼度計算の結果によっては、制限付き、またはリスク軽減のための補完的制御を加えたアクセスを許可することが決定されます。例えば、ユーザーに読み取り専用アクセスが許可されたり、追加のモニタリング機能が適用される場合にのみアクセスが許可されることがあります。1 つの手法として、要求された情報をユーザーのデバイス上に表示するだけで、実際にはユーザーのデバイスに情報を転送しないシステムを使用する方法があります。

セキュリティー・ゾーン

インテル IT 部門では、インテルの環境を複数のセキュリティー・ゾーンに区分けしています。重要性の低いデータやシステムへのアクセスを提供する非信頼ゾーンから、重要なデータとリソースが置かれる信頼ゾーンまで、各種のセキュリティー・ゾーンが設定されます。

図 3 に示すように、高い信頼レベルを要求するゾーンには重要な資産が置かれるため、より厳密かつ広範囲にわたる管理機能で保護され、アクセス可能なデバイスとアプリケーションの種類も制限されます。ただし、高信頼ゾーンへのアクセスを許可されるデバイスはより高性能でもあり、企業データの作成や修正など、低信頼ゾーンでは許可されない操作を実行できます。

この手法でインフラストラクチャーを管理すれば、各ゾーンに適正なレベルのセキュリティー管理機能を適用し、セキュリティー・リソースを効果的に利用できます。これにより、従業員はリスクの低い活動にはスマートフォンなどの幅広いデバイスを選択することができ、ユーザー体験が向上します。

ゾーンへのアクセス権限は、信頼度計算の結果に基づいて決定され、ポリシー施行点（PEP）によって制御されます。PEP は、ファイアウォール、アプリケーション・プロキシー、侵入検知 / 予防システム、認証システム、ログシステムなど、各種の管理機能で構成されます。

ゾーン間の通信は、厳しい制限、監視、管理の対象となります。インテル IT 部門では、各ゾーンを異なる物理 LAN または仮想 LAN（vLAN）上に配置することにより、ゾーンを分割しています。PEP はゾーン間の通信を制御します。これにより、1 つのゾーンが攻撃されても、その問題が他のゾーンに広がることを防止できます。また、問題が広がった場合は、それを検出する機会が増えます。さらに、アプリケーション・プロキシーなどの PEP 管理機能を使用して、必要に応じて低信頼ゾーン内のデバイスとアプリケーションに、高信頼ゾーン内の特定のリソースに対する管理された制限付きアクセス権限を与えることができます。

インテル IT 部門では、セキュリティー・ゾーンに非信頼ゾーン、選択ゾーン、信頼ゾーンの 3 つのカテゴリーを想定しています。各ゾーンには複数のサブゾーンが含まれます。

非信頼ゾーン
非信頼ゾーンには、信頼度の低いエンティティーからアクセスできるデータとサービス（またはそれらに対するインターフェイス）が置かれます。これにより、他のゾーンに置かれる重要なリソースのリスクを高めることなく、スマートフォンなどの管理対象外のデバイスから限られたリソースへの幅広いアクセスを許可できます。非信頼ゾーンは、企業の電子メールや予定表などの企業リソースへの制限付きアクセスを提供します。また、単にインターネットへのアクセスを提供することもあります。

インテル IT 部門では、非信頼ゾーンを攻撃や侵入のリスクの高い危険な領域と見なしています。したがって、リスクを軽減するための発見的管理と修復的管理に重点が置かれます。これには、疑わしい挙動を検出する高度なモニタリングと、ネットワーク・ベースのシステム遮断や状況に応じたユーザー権限の削除などの修復機能が含まれます。

インテル IT 部門では、必要に応じて、非信頼ゾーンから高信頼ゾーン内のリソースへの管理されたアクセスを提供する予定です。例えば、スマートフォンを使用している従業員が、信頼ゾーンに置かれた顧客データへの制限付きの読み取り専用アクセスを許可される場合や、スマートフォンで信頼ゾーン内のディレクトリー・サーバーにアクセスし、電子メールを送信する場合などが考えられます。インテル IT 部門では、アプリケーション・プロキシーを使用して、このような管理されたアクセスを提供する予定です。安全な仲介者として機能するこれらの PEP 管理機能は、デバイスからの要求を評価して、信頼ゾーン内のリソースから情報を収集し、その情報をデバイスに転送します。

選択ゾーン
選択ゾーンでは、非信頼ゾーンより強い防護が提供されます。選択ゾーン内のサービスの例として、委託業者、ビジネスパートナー、従業員が、管理対象のクライアント機器または一定レベルの信頼度を持つ管理対象外のデバイスを使用してアクセスする、アプリケーションとデータが挙げられます。選択ゾーンには、重要なデータや価値の高いインテルの知的財産は置かれません。選択サブゾーンでは、さまざまなサービスまたはユーザーへのアクセスが提供されます。非信頼ゾーンと同様に、必要に応じて、アプリケーション・プロキシーを使用して選択ゾーン内のリソースにアクセスできます。

信頼ゾーン
信頼ゾーンには、インテルの重要なサービス、データ、インフラストラクチャーが置かれます。信頼ゾーンでは高度なセキュリティーが確保され、ロックダウンされます。信頼ゾーン内のサービスの例として、データセンター・サーバーやネットワーク・インフラストラクチャーへの管理者アクセス、工場のネットワークと機器、ERP アプリケーション、知的財産を含む設計エンジニアリング・システムなどが挙げられます。したがって、これらのリソースへの直接アクセスは、企業ネットワーク内にある信頼度の高いシステムにのみ許可されます。すべてのアクセスは厳密にモニタリングされ、異常な動作があれば直ちに検出されます。

バランスのとれた管理

過去 10 年にわたり、企業セキュリティーの重点は、ファイアウォールや侵入防止システムなどの予防的管理に置かれていました。この手法には、明らかな利点があります。問題が発生した後でその問題を修正するよりも、攻撃を事前に予防する方がコストがかかりません。また、ファイアウォールがいつ侵入の阻止に成功したかもひと目で確認できます。

しかし、新しいセキュリティー・モデルでは、次のような理由から予防的管理と発見的管理（モニタリング）および修復的管理のバランスをとることが要求されます。

まず、新しいモデルでは、アクセスの防止ではなく、広範囲にわたるユーザーとデバイスからのアクセスを許可し、制御することに重点が置かれます。また、絶え間なく脅威の変化する環境の下では、攻撃は不可避であること、そしてどんな予防的管理も失敗する可能性があることを前提にする必要があります。ひとたび攻撃者が企業環境へのアクセスを手にしてしまうと、予防的管理は回避され、その効果を失います。

発見的管理の利用を増やし、修復的管理を積極的に導入することで、幅広いアクセスを許容することのリスクを軽減できます。これらの管理により、攻撃を防げなかった場合の生存可能性と回復能力も向上します。

インテル IT 部門は、セキュリティー・ビジネス・インテリジェンス（セキュリティー BI）を使用して、モニタリングによって収集したデータを分析し、相関性を評価することで、起こり得る攻撃を検出し、防止しています。例えば、セキュリティー BI は、同時に 2 カ所からログインしているユーザーなどの異常な状況を検出し、防止できます。

予防的管理、発見的管理、修復的管理のバランスは、セキュリティー・ゾーンによって異なります。例えば、非信頼ゾーンでは、ごく限られたリソースに対して幅広いアクセスを許可し、発見的管理と修復的管理の利用を増やすことでリスクを軽減します。各タイプの管理の中で冗長性を確保すれば、さらに保護を強化できます。

発見的管理と予防的管理には、次のような使用例が考えられます。

- インテルの従業員が、インテル以外の電子メールアドレスに機密文書を送信しようとしています。監視ソフトウェアは、このような操作を検出すると、ファイアウォールの外側への文書の送信を停止し、送信者のデバイスに確認メッセージを表示します。従業員が確認メッセージに応答すると、文書の送信が実行されます。重要な機密文書の場合は、編集済みのバージョンが送信されることもあります。

- ERM で保護された文書を不適切な方法で利用すると、その文書へのアクセス権限が失効します。

- システムは特定の文書へのアクセスを許可し、ユーザーの操作を追跡します。ユーザーは少数の文書なら問題なくダウンロードできますが、数百本の文書をダウンロードしようとすると、システムはダウンロードの速度を落とし（例えば、チェックアウトされる文書を一度に 10 本までに制限し）、ユーザーの上司に警報を送信します。そして、上司の承認が得られれば、ユーザーにはより高速なアクセスが許可されます。

- ウイルスに感染したシステムが検出されると、そのシステムは修復ネットワーク上に置かれ、他のシステムから隔離されて、企業情報やアプリケーションへのアクセスが制限されます。この状態のシステムは、企業資産へのアクセス機能を一部保持しますが、必要に応じてインシデントに対応できるように、すべての動作が詳しく記録されます。

- システムへの攻撃が判明した場合、IT 部門はそのシステムの最近のすべての動作と他のシステムとのやり取りを調査します。これらのシステムについては、追加モニタリングが自動的に有効にされます。

ユーザーとデータ：新しい境界

新しいデバイスの増加と、いつでもどこでも情報にアクセスしたいというユーザーの要求の高まりとともに、従来の企業ネットワークのセキュリティー境界の有効性は急速に低下しています。

つまり、ネットワーク境界の防御は、単独ではますますその効果を失っているのです。今後もネットワーク境界の保護は重要ですが、それに加えて、保護すべき重要な資産である、インテルの知的財産、インフラストラクチャー、その他の重要なデータ、システムに重点を置いて、従来の保護機能を補完する必要があります。

これらの資産を保護するため、新しいセキュリティー・アーキテクチャーでは、データそれ自体とデータにアクセスするユーザーという 2 つの境界を防御の対象に加えます。

データ境界

重要なデータは、作成、保管、転送など、あらゆる時点で保護されなければなりません。この目的で、インテル IT 部門では、ERM やデータ漏えい防止（DLP）などの技術を導入して、データに電子透かしやタグを適用し、データそれ自体に保護機能を統合しています。例えば、ERM により、文書の作成者は、文書の有効期間全体を通して文書へのアクセス権限を持つユーザーを厳密に定義し、アクセス権限をいつでも失効させることができます。

ユーザー境界

ユーザーはさまざまな理由でセキュリティーのリスクになります。ユーザーは頻繁にソーシャル・エンジニアリング攻撃の標的となります。ユーザーの個人情報はソーシャル・ネットワーキング・サイトで簡単に入手できることが多いため、このような攻撃に対する脆弱性はさらに高まります。またユーザーは、電子メールの悪意あるリンクをクリックする、マルウェアをダウンロードする、データを保管した携帯型機器を紛失するなどの問題を起こすことがあります。

発見的管理を利用して、より安全な行動様式を奨励できます。例えば、機密文書をファイアウォールの外側に送信しようとしたユーザーに警告を送れば、今後のユーザーのセキュリティー意識を高めることが可能となります。また、トレーニングやインセンティブなどの活動を組み合わせることで、情報セキュリティーとプライバシー保護を企業文化に浸透させられることも判明しています。インテル IT 部門で

セキュリティー・アーキテクチャーの運用例：あるインテル社員の一日

この例（図 4 を参照）では、新しいセキュリティー・アーキテクチャーによって、インテルの営業社員が必要な情報にどのようにアクセスするかを 1 日の流れに沿って説明します。このアーキテクチャーは、ユーザーのデバイスと所在に基づいてアクセスのレベルを動的に調整し、異常な動作がないかを監視して、インテルのセキュリティーを保護します。

1. **営業社員が客先を訪問します。**移動中にこの社員は個人のスマートフォンを使用しており、非信頼ゾーン内のサービスへのアクセスのみを許可されます。この状況で、社員は、信頼ゾーン内の ERP システムから抽出される最近の注文情報などの限られた顧客情報を閲覧できます。しかし、こうした操作を行うには、仲介者として機能して信頼ゾーンを保護するアプリケーション・プロキシー・サーバーを経由しなければなりません。このアプリケーション・プロキシー・サーバーは、ユーザーからの情報要求を評価し、ERP システムにアクセスし、取得した情報をユーザーに転送します。

   スマートフォンから異常に多数の顧客記録の要求があった場合、それはスマートフォンの盗難を示す兆候と判断され、そのスマートフォンからのそれ以上のアクセスは遮断されます。また、異常なアクセスの原因を確認するために、その社員のすべてのデバイスからのシステムアクセスに対するモニタリングが強化されます。

2. **社員が客先に到着し、インテルが保有するノートブック PC からインテルのネットワークにログインします。**このノートブック PC はスマートフォンよりも信頼度が高いため、社員は、価格情報の閲覧や発注など、選択ゾーンでの利用が可能な機能に対してもアクセスできます。これらの要求は、アプリケーション・プロキシーによって信頼ゾーン内の ERP システムに中継されます。

3. **社員がインテルのオフィスに帰社し、企業ネットワークに接続します。**ここで、社員は信頼度の高い場所から信頼度の高いデバイスを使用しているので、信頼ゾーン内の ERP システムに直接アクセスできます。

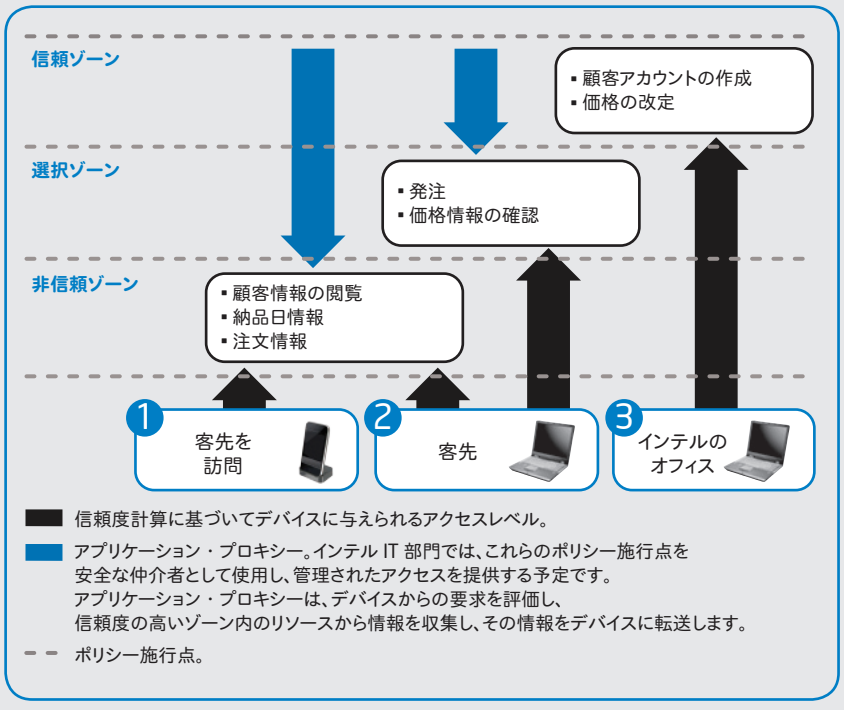

図 4. 新しいセキュリティー・アーキテクチャーは、インテルの情報資産を保護しながら、職務の遂行に必要な情報を社員に提供します。

は、従業員が自己責任で企業情報と個人情報を保護するように奨励しています。

まとめ

インテルの企業セキュリティー・アーキテクチャーは、新しい利用モデルや新たな脅威への対応など、急速に進化するさまざまな要件を想定して設計されています。私たちの目標は、新しいサービスや機能の導入の迅速化と、生存可能性の向上を両立させることです。

インテル IT 部門では、約 1 年前にこのアーキテクチャーの導入に着手し、約 5 年をかけてインテル全社への導入を進める予定です。この構想は、すでにいくつかの成果を上げています。インテル IT 部門では、この手法によって難しいユースケースにソリューションを提供し、実際にリスク軽減の成果を上げています。例えば、バランスのとれた管理と信頼ゾーンの導入により、従業員が保有するデバイスから企業ネットワークへのアクセスが可能となりました。このモデルの採用によって、セキュリティー・コストを削減できたプロジェクトもあります。

インテル IT 部門では、このアーキテクチャーは、クラウド・コンピューティングのセキュリティー問題の解決にも有効であると考えています。このため、システムとデータの場所が固定的であることを前提とした、ファイアウォールなどの従来のセキュリティー管理手法を使用してアクセスを制限することは難しくなります。新しいアーキテクチャーは、信頼度計算などのツールを利用して、特定のリソースへのアクセスをより動的にきめ細かく管理できます。また、発見的管理と修復的管理の利用を増やし、現時点で利用できる予防的管理の弱点を補強できます。

このモデルを完全に実現するために必要なセキュリティー技術の中には、まだ実用化されていないものもありますが、どれも近い将来には実現されるはずです。インテルは、信頼度計算など、すべての必要な機能を支えるテクノロジーの研究開発を積極的に支援しています。同時に、このアーキテクチャーの利点をフルに活用するため、開発から運用に至るまで、インテル IT 部門のすべての活動に新しいアーキテクチャーを適用する作業を進めています。

詳細情報

- 「エンタープライズ環境でのパーソナル・ハンドヘルド機器の利用と情報セキュリティーの確保」http://download.intel.com/jp/business/japan/pdf/323956-001JA.pdf

略語

BI	ビジネス・インテリジェンス
DLP	データ漏えい防止
ERM	エンタープライズ権利管理
ERP	エンタープライズ・リソース・プランニング
GPS	衛星測位システム
PDP	ポリシー決定点
PEP	ポリシー施行点
TPM	トラステッド・プラットフォーム・モジュール
vLAN	仮想 LAN

インテル IT 部門のベスト・プラクティスの詳細については、http://www.intel.co.jp/jp/go/itatintel/ を参照してください。

この文書は情報提供のみを目的としています。この文書は現状のまま提供され、いかなる保証もいたしません。ここにいう保証には、商品適格性、他者の権利の非侵害性、特定目的への適合性、また、あらゆる提案書、仕様書、見本から生じる保証を含みますが、これらに限定されるものではありません。インテルはこの仕様の情報の使用に関する財産権の侵害を含む、いかなる責任も負いません。また、明示されているか否かにかかわらず、また禁反言によるとよらずにかかわらず、いかなる知的財産権のライセンスも許諾するものではありません。

Intel、インテル、Intel ロゴ、Intel Core、Intel vPro は、アメリカ合衆国およびその他の国における Intel Corporation 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/

©2011 Intel Corporation.　無断での引用、転載を禁じます。
2011 年 5 月

324166-001JA
JPN/1105/PDF/SE/IT/NT