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と従業員の生産性

2010 年 11 月

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

Rob Evered
インテル IT 部門
情報セキュリティー・スペシャリスト

Jerzy Rub
インテル IT 部門
情報リスクおよび
セキュリティー・マネージャー

概 要

インテル IT 部門では、従業員が所有するハンドヘルド機器をエンタープライズ環境に統合する試みを積極的に進めています。インテル IT 部門では、IT のコンシューマー化（従業員が各自のパーソナル機器を使用して企業データにアクセスすること）が職場環境における重要なトレンドであることを以前から認識していました。そこで、インテルの法務部、情報セキュリティー部門、人事部との緊密な連携の下、インテルの情報セキュリティー・ポリシーに適合するソリューションの実現に取り組んできました。

インテルでは、データと知的財産の侵害に対する防御策を十分に講じた上で、従業員が各自のワークスタイルに合った各自の業務に有益なツールを選ぶことを許可し、従業員の生産性と満足度を向上させています。

2010 年 1 月、インテル IT 部門は、従業員が所有するハンドヘルド機器を業務に使用することを許可する新しいプログラムを導入しました。従業員の反応は非常に好意的で、最初の 1 カ月で 3,000 名を超える従業員が参加しました。2010 年 9 月現在、インテルのコンピューティング環境には 20,000 台以上のハンドヘルド機器が含まれ、そのうち約 6,500 台は、企業情報へのアクセスが可能な、従業員が所有する機器です。2010 年 7 月には、個人所有のタブレットの使用を許可する新しいプログラムを開始しました。個人所有の PC の使用はまだ許可されていませんが、契約社員についてはこの可能性を検討中です。

ここに至るまでに、インテル IT 部門は次のような活動に取り組んできました。

- インテルの法務部および人事部との 1 年以上にわたる協力に基づく、インテルの情報セキュリティー要件に適合するパーソナル機器ポリシーの定義と導入。
- ソーシャルメディアを利用した 6 カ月以上にわたる従業員との対話による、従業員のワークスタイルとサポートへの要求の理解。
- 新しい認証方法やデバイス管理ポリシーなど、企業の情報と知的財産を保護する技術的ソリューションの開発。
- 情報セキュリティーに関するユーザーのトレーニングと、パーソナル機器ポリシーに関する IT 部門のサービスデスク・スタッフのトレーニングの実施。

インテル IT 部門は、自社環境におけるトレンドとテクノロジーを上手に管理することで、多くのセキュリティー問題を回避できました。IT のコンシューマー化に伴うセキュリティーの問題を無視したり、個人所有のデバイスの業務での使用を禁止していたら、多くの問題が発生していたはずです。

インテルでは、データと知的財産の侵害に対する防御策を十分に講じた上で、従業員が各自のワークスタイルに合った各自の業務に有益なツールを選ぶことを許可し、従業員の生産性と満足度を向上させています。

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 IT 部門では、多くの企業の IT 部門と同様に、自社環境でのパーソナル（個人所有）ハンドヘルド機器の使用を禁止していました。しかし、IT のコンシューマー化とともに、各種のパーソナル・ハンドヘルド機器を使用して企業情報にアクセスしたい従業員の要求に応えるという困難な課題に直面しています。

10 年前には、インテルの従業員は高度なテクノロジーを利用するために出社していました。現在では、さまざまなコンシューマー機器が利用可能になり、職場の PC やプリンターより高機能な PC やプリンターを自宅に所有する従業員も増えています。また、ユーザーが IT 部門に期待することも変わってきました。現在では、基本的なコンピューター・トレーニングやソフトウェア・トレーニングを提供する必要はなくなりました。ユーザーはすでにコンピューターの経験を積んでおり、IT 部門が持っていないプラットフォームを使用しているユーザーも増えています。また、これまで以上に広いエリアでインターネットへのアクセスが可能です。

エンタープライズ環境における パーソナル機器の利点

インテルの移動の多いユーザーは、最新のシステム、サービス、機能を利用して仕事をしたいと望んでいます。そのために、しばしばハンドヘルド機器をコンパニオン・デバイスとして使用し、企業が所有するノートブック PC の有用性を拡張しようとします。この方法なら、自宅や外出先から簡単に情報にアクセスできます。

例えば、多くのユーザーは、各自の社内カレンダーとサードパーティーの Web ベースのカレンダー・ユーティリティーを同期させることで、パーソナル機器を使用してどこからでも業務カレンダーにアクセスできることを望んでいます。その動機として、手軽で効率的、かつ最も生産的なやり方で自分の仕事を進めたいという要求があります。

多くの従業員は、こうした慣行から生じる情報セキュリティーの問題を考慮していません。しかし、インテル IT 部門にとって、情報セキュリティーは非常に重要です。インテル IT 部門では、すべてのパーソナル機器の使用を禁止するポリシーを継続する可能性についても検討しましたが、分析の結果、このようなポリシーを強制した場合、ソフトウェアとサポートのコストが数百万ドルもかかる上に、ユーザーの生産性にも悪影響を与えることがわかりました。

このような手法では、インテル IT 部門は、ユーザーがインストールしようとするアプリケーションを漏れなく検証しなければならなくなります。それでは、高度な技術を持つ専門化したインテルの 8 万人のユーザーの柔軟性が大きく損なわれます。また、従業員の自由を尊重するインテルの企業文化と IT に対するユーザーの期待を大きく変えなければならない上に、新しいラボ・ネットワークの導入や、大量の新しいハードウェアとネットワーキング機器の設置が必要になります。

インテルでのパーソナル機器の利用は勢いを増しており、それに対応してポリシーを変更する必要がありました。インテル IT 部門は、IT のコンシューマー化のトレンドがユーザーと IT 部門双方に次のような大きな利点をもたらす可能性を認識し、IT のコンシューマー化を受け入れることにしました。

- **生産性の向上：**ユーザーが各自のワークスタイルと好みにあったデバイスを選択できるため、生産性と柔軟性が向上します。
- **運用管理機能の向上：**ユーザーが受け入れられるプログラムを提供することで、IT 部門は、ユーザーの行動パターンを認識し、ユーザーの行動に影響を与えるサービスを提供できます。これにより、IT リスクのレベルを明確に理解でき、リスクを積極的に管理できます。
- **ビジネス継続性の向上：**会社から提供されるノートブック PC が動作しない場合でも、パーソナル・ハンドヘルド機器が部分的なバックアップを提供するため、ユーザーは仕事を続けられます。
- **紛失の防止：**インテル社内のデータによると、ユーザーは企業の資産より自分の所有物の方を注意深く管理する傾向があり、企業所有の機器よりも個人所有の機器の方が紛失件数が少なくなります。このことが情報セキュリティーの実質的な向上につながります。

- **セキュリティーの強化：**IT のコンシューマー化を無視するのではなく、そのトレンドを管理し、主導することにより、情報セキュリティーの強化が可能です。

インテル IT 部門は、IT のコンシューマー化の一部分を許可し、インテルの情報セキュリティーとプライバシーの要件に適合させることに、組織を挙げて取り組んできました。

ユーザーの要求と情報セキュリティーの両立

新しいテクノロジーが登場するたびに、インテル IT 部門は情報セキュリティーの保護策を講じなければなりません。ここでの課題は、ユーザーの要求と情報セキュリティーの両方をできる限り満足させるポリシーを策定することです。

一般的に、ユーザーが新しいテクノロジーを採用し始める時点では、セキュリティーの脅威は最小限にとどまるため、必要以上に大きなサポートコストがかかることはありません（図 1 を参照）。ユーザーの需要がピークに達する段階では、多くの人がそのテクノロジーに関する経験を蓄積し、攻撃を開始するようになるため、セキュリティーの脅威が増大し、サポートコストは増加します。この段階（図中の B 点）で、テクノロジーのセキュリティーを確保するためのリソースの配分が必要になります。しかしこの場合、投資収益率は理想的なケースよりも小さくなります。これは、他の新しいテクノロジーが利用可能になり、従来のテクノロジーに対するユーザーの需要が減少し始めるためです（C 点）。

インテル IT 部門の分析では、ユーザーの需要と情報セキュリティーの両方が比較的高いレベルにある A 点で、新しいテクノロジーを採用するのが最善の手法と言えます。

ソリューション

インテル IT 部門では、IT のコンシューマー化が従業員と IT 部門の双方に利点をもたらす可能性を認識し、およそ 3 年前から、このトレンドから生じる独自のセキュリティー問題の特定、ユーザーの行動調査、IT コンシューマー化ポリシーの要件の定義を始めました。

これらの作業には、インテルの法務部および人事部との密接な協力が必要でした。インテル IT 部門では、パーソナル（個人所有）機器の利用によるさまざまなセキュリティー・リスクに対し、法律的な契約とトレーニングによって対処しました。このトレーニングは、ユーザーの行動の改善、ユーザーの支援、最新の状態を維持する責任の徹底を目的とするものです。

IT のコンシューマー化の基盤は、20 年前にインターネット、電子メール、Web サイトの登場によって築かれました。図 2 は、インテルの段階的なアプローチによってエンタープライズ環境で一部のパーソナル機器の使用が許可されるに至る、IT のコンシューマー化のプロセスを示しています。

インテル IT 部門が導入したポリシーは、エンタープライズ環境における個人所有のハンドヘルド機器の使用を許可することで、モビリティーと柔軟性を求めるユーザーのニーズをサポートします。このポリシーに基づいて、将来は他の個人所有デバイスの使用も許可できます。

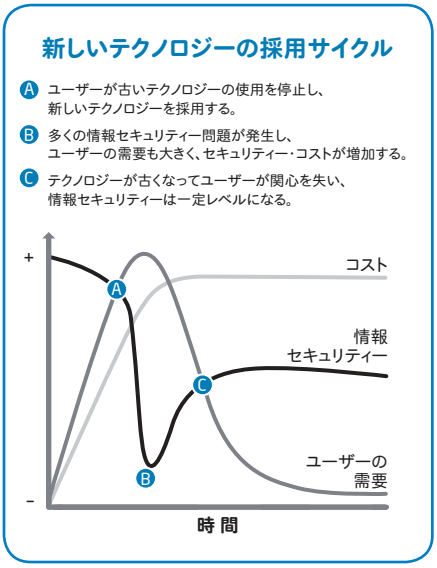

図 1. ユーザーの需要がまだ比較的大きく、情報セキュリティーのリスクが許容範囲内である A 点で、新しいテクノロジーを採用するのが最善です。

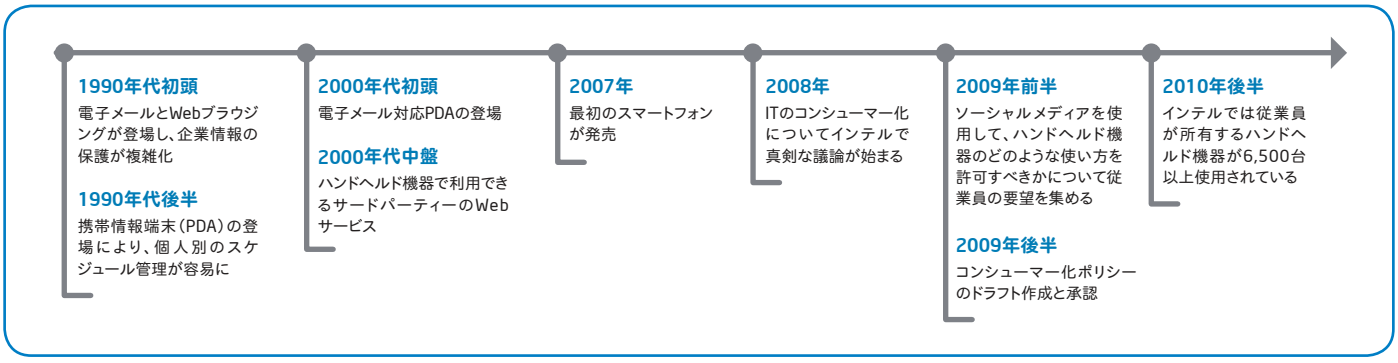

図 2. インテル IT 部門は、20 年にわたる IT のコンシューマー化のトレンドに対応したポリシーの策定を段階的に進めてきました。この作業には全体で 18 カ月以上かかりました。

セキュリティーの問題

企業が所有するハンドヘルド機器上で動作するアプリケーションの検証と制御は、比較的簡単に行えます。パーソナル機器の場合は、従業員が自分で選んだアプリケーションをインストールできるため、このプロセスはそれほど簡単ではありません。インテル IT 部門では、IT 部門が機器のテスト、制御、更新、接続の切断、リモートからのデータ消去、ポリシーの適用を実行するのに十分な情報セキュリティーを確保するために、ハンドヘルド機器の最小限のセキュリティー仕様を次のように定義しました。

- 電子メールの受信には 2 ファクター認証が必要
- 暗号化を使用したセキュアなストレージ
- セキュリティー・ポリシーの設定と制限
- インテルとの間のセキュアな情報送信
- リモートワイプ機能
- サーバー側での一定のファイアウォール機能と侵入検知システム（IDS）機能
- セキュリティー規則に適合するパッチ運用管理 / 適用ソフトウェア
- 端末側にアンチウイルス・ソフトウェアがなくても機能する、サーバー側からのウイルスチェック機能

アンチウイルス・ソフトウェアについては、インテルのモバイル機器に対するウイルス攻撃を分析した結果、企業情報を標的とするウイルスはごくわずかしかなく、ほとんどがテキストメッセージの送信またはユーザーの電話帳の攻撃を行うものでした。将来はマルウェアの増加が予想されますが、現時点では企業情報に対する実際の脅威は低レベルにとどまります。

また、パーソナル機器上にインストールされるソフトウェアの設定ガイダンスと、インストールされるアプリケーションの標準セットも提供されます。

セキュリティーを重視した IT コンシューマー化ポリシーの設計

パーソナル・ハンドヘルド機器による企業情報へのアクセスを許可するポリシーの設計に当たって、まず従業員がこれまでどのようにパーソナル機器を使用してきたか、どのような目的でパーソナル機器を使用しているか、インテル IT 部門に何を期待しているかを確認する必要がありました。次に、インテルの法務部および人事部と協力して、パーソナル・ハンドヘルド機器による企業情報へのアクセスの許可に伴う問題点に対処しました。さらに、ポリシーの策定後、ポリシーの遵守に関するサービスデスク・スタッフと従業員のトレーニングを実施する必要がありました。

ユーザーのニーズの理解

ユーザーの好みや行動に関する問いに答えられるのはユーザー本人だけであることが、すぐに明らかになりました。そこで、社内ブログを通じて従業員と直接対話し、インテル IT 部門のコンシューマー化ポリシーの策定についてオープンに議論することにしました。インテルの法務部と人事部は、ブログのような制約のない環境でポリシーについて議論すると、あらゆる応答がポリシーそのものと受け取られるおそれがあると考え、この試みに抵抗を示しました。したがって、インテル IT 部門はポリシーに関する約束や断言はしていないことを、すべてのコミュニケーションで明確に示す必要がありました。このためにネガティブなトーンを感じさせないよう、以下の例に示すように、誠実な会話のスタイルで語りかけました。

> *「インテルがコンシューマー化の問題をどのように扱うべきかに関するご意見を、これから 1 カ月にわたって募集します。注意：これは実験的な試みです。これまでインテルは、ポリシーの策定に関して従業員の皆様と直接議論したことはありません。忌憚のない率直なご意見をお寄せください！*
>
> *皆様のフィードバックは専門家と意思決定者によって検討され、今後のコンシューマー化ポリシーに反映されることがあります。ただし、ご意見が常に取り上げられるとは限りません。」*

ブログの設計に当たって、コミュニケーションの専門家に相談し、ユーザーの行動を意識して質問を作成しました。意味のある回答を引き出すような質問を作成することが重要でした。上位レベルの質問の例には、以下のものがあります。

- どのような目的で、ご自分の機器を仕事に使いたいですか？
- ご自分の機器を仕事に使うために、あきらめてもいいことは何ですか？
- パーソナル機器はあなたのお仕事にどのように役立っていますか？

ノートブック PC とシンクライアントの比較

インテル IT 部門では、企業または従業員が所有するスマートフォンやタブレットなどのハンドヘルド機器によって補完されるノートブック PC に、自社の IT 環境を標準化しています。このソリューションは、情報セキュリティーを損なうことなく、従業員の生産性を向上させます。

シンクライアント・コンピューティング・モデルは、管理サーバーに情報を格納し、特定のデバイスに限りその情報へのアクセスを許可するものです。インテル IT 部門の分析では、このモデルは絶対確実な企業情報保護の手段とは言えません。

シンクライアントは、限られた特定のアプリケーションには有効ですが、一般的にはユーザーのモビリティー、生産性、創造性が制約を受けるようです。また、シンクライアントによるセキュリティーの向上と見なされる多くの点については、注意深く再検討する必要があります。インテル IT 部門の分析では、シンクライアント環境における情報セキュリティーのリスクの多くは、消滅したのではなく単に移動しただけです。例えばシンクライアントは、通常はノートブック PC と同レベルの情報セキュリティー保護機能を備えていないにもかかわらず、インターネットに接続して情報をエクスポートできるため、情報のリスクが増大します。したがって、性能の低いシンクライアントの利用によって生産性が低下する一方、セキュリティー上の利点はほとんど得られませんでした。

- 機器を自由に選べる代わりに、セキュリティーにもっと注意を払っていただけますか？　多少面倒になってもかまいませんか？

質問の多くは、これと同様の情報を従業員から集めるものです。ユーザーの仕事に必要なアプリケーションの質問と必要な機能の質問は重複するように思われます。しかし、ユーザーは 2 つの質問に異なる解釈を下し、異なる応答を返します。これは利用パターンと好みについて幅広く把握するのに効果的です。この例では、アプリケーションの質問は、機能を暗示するとともに、特定のソリューションも明らかにします。それに対して、機能の質問は、全体的な好みや、スケジュール管理や電子メールなどの一般的な作業へのニーズを確認します。

この対話への参加者の多さは、パーソナル機器を使って仕事をしたいユーザーの欲求の強さを浮き彫りにしました。実に 8,000 名以上の従業員が回答を寄せました。実際、ユーザーの回答が非常に熱心で示唆に富んでいたため、ブログの開設期間は 1 カ月から 6 カ月に延長されました。

質問に対するユーザーの回答が、ユーザーの仕事の進め方についての IT 部門の前提に新たな光を投げかけることもありました。例えば、基本的に同じ業務を担当する 2 人の営業担当者が、デバイスについては全く異なる好みを示しました。1 人は、アプリケーションのダウンロード、電子メールのチェック、空港のラウンジや無線 LAN スポットの場所の表示が可能なデバイスが必要であると主張しました。もう 1 人は、自分のデバイスに不要な機能が多すぎることに不満を述べ、通話ができてバッテリーが長持ちする携帯電話があれば十分だと語りました。

インテルの法務部と人事部のサポート

IT コンシューマー化ポリシーの策定には、インテルの法務部と人事部のサポートが必要でした。法務部と人事部は、ポリシーの検証と適用、電子情報開示（e-Discovery）、監査と調査などに関与しました。

これらの観点から、法務部と人事部はブログの内容を細かくチェックしました。IT 部門は、法務部と人事部からのフィードバックをユーザーとの対話に反映させました。IT 部門は、この機会を利用して、IT のコンシューマー化の実情と、IT のコンシューマー化がインテルにもたらす潜在的な利点（および潜在的なリスク）について、法務部と人事部を啓発することにしました。このような連携により、各部門は目標とソリューションの整合性を確保し、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使用を許可する試みに対するユーザーからの非常に積極的な反応を共有することができました。

エンドユーザー・ライセンス契約（EULA）の作成

インテル IT 部門のポリシー策定活動の結果、ポリシーに基づいて情報セキュリティーに対処するエンドユーザー・ライセンス契約（EULA）が作成されました。実際には、EULA は新しいポリシーではありません。EULA は、インテルの既存の雇用契約条件に則ってビジネス目的での個人資産の利用について定めているため、ユーザーにとって予想しやすい共通のポリシーとなっています。

EULA は、ユーザーがデバイスを使ってできることとできないことを明確に指定します。例えば、データストレージとバックアップの節では、次のように規定しています。

> *「あなたは、インテルの行動規範に従って、あなたの所有物内のインテルのデータを適切に管理し、保護する責任を負います。すなわち、あなたは暗号化ソリューションのインストールを要求される場合があります。また、ロック解除された機器へのアクセスをインテルの従業員以外の者に許してはなりません。あなたの機器にインテルのデータが置かれている場合、そのデータのバックアップ先は、インテルが所有する機器に限られます。」*

現在のところ、インテルのポリシーでは、スマートフォンやタブレットなどの個人所有のハンドヘルド機器のほか、大容量ストレージ用の USB メモリーと、ビジネスパートナーが所有する一部の機器のみが許可されています。インテル IT 部門では、EULA の適用範囲を広げて、事実上あらゆる種類の個人所有の機器に適用しようとしました（ただし、ホーム PC など一部の機器の使用は、インテルではまだ許可されていません）。

2 年間の策定と修正のプロセスを経て、パーソナル機器と企業の機器の両方を対象とするひとつの EULA が導入されました。EULA は特定のアプリケーションに限定されるものではなく、少なくとも 6 カ月先までの開発予定に対応します。インテルは四半期ごとに EULA を見直し、テクノロジーとユーザーの要求の変化に対して、EULA が提供する法律的なセキュリティー保護が最新の状態を維持しているかを確認します。ユーザーは、新しいテクノロジーに移行するときに EULA の再契約を行います。

個人所有のハンドヘルド機器の使用を申請した 6,500 名を超えるインテル従業員のうち、およそ 50% は EULA への署名を拒否しました。この反応は、従業員に対するトレーニングとコミュニケーションの必要性を浮き彫りにしています。これらの従業員は、新しい契約条件には一切署名しようとしないでしょう。EULA に署名しない従業員は、パーソナル機器を使用して企業の情報にアクセスすることはできません。

EULA は、ユーザーが許されることと許されないことを規定する以外に、法務部と人事部の問題にも対応します。

プライバシーの問題

インテル法務部との協力に当たって、「企業情報」、「従業員が所有するデータ」、「個人データ」の概念を定義する必要がありました。

- 企業情報とは、インテルが所有するデータまたは知的財産です。
- 従業員が所有するデータとは、To-Do リストやレシピを集めたものなど、従業員が所有するデータです。
- 個人情報とは、住所や医療データなど、個人情報保護法によって管理されるデータです。

インテル IT 部門では、個人情報と企業情報が混在することをできる限り避けようとしていますが、ハンドヘルド機器は通常はこうした機能をサポートしていません。例えば、カレンダー・アプリケーション上には個人情報と企業情報が混在しています。ハンドヘルド機器上では、しばしばユーザーの個人データと企業データが混在しています。したがって、ユーザーは、調査が行われる場合、インテルがユーザーのデバイスの引き渡しを要求し、ユーザーの個人データを見る可能性があることを理解する必要があります。

人事部の問題

従業員は労働時間に見合った報酬を得なければなりません。インテルの EULA は、この問題について次のように具体的に規定しています。

> *「非裁量従業員は、正規の労働時間外に仕事上の電子メールをチェックする場合、報酬を得るべき仕事をしているのであり、この労働時間をタイムカード上で申告しなければなりません。非裁量従業員は、自主的に未申告の労働をすることはできません。非裁量従業員が、労働時間に対して適切な報酬を得ていないと思われる場合や、労働時間を申告せずに仕事をするように強制されていると思われる場合は、人事部の法務チームに対し、あるいはインテルの企業倫理レポート Web サイトから、直ちにその旨を報告してください。」*

電子情報開示（e-Discovery）の問題

e-Discovery への対応には困難が予想されましたが、結果的には簡単に解決されました。ハンドヘルド機器上でデータを生成するローカル・アプリケーションを IT 部門が導入しない限り、ハンドヘルド機器とインテルの間の接続手段は電子メールだけです。したがって、すべての e-Discovery は、インテルの電子メールサーバー上で実行可能です。

従業員は独自のやり方でコンテンツを作成することがわかりました。例えば、従業員はホワイトボードの写真を撮影し、電子メールに添付して同僚に送信しています。インテル IT 部門は、電子メールサーバー上でこの情報を収集できます。情報がどこに置かれるか、ハンドヘルド機器上にどのようなコピーが置かれるかは、大部分はポリシーと監査によって管理されます。

インテルが所有していない機器から企業情報を収集すると、問題が発生する可能性があります。インテルは、同期をとっていないデバイス上で企業情報を利用することを許可していません。またインテルは、ユーザーに法的情報保留が課されることを通告する条項を EULA に追加しました。

> *「法的情報保留が適用される場合、インテルから要求があった場合は、ご使用の機器を引き渡さなければなりません。機器上のすべてのファイルのコピーをとらなければならない場合があります。関連するファイルはインテルの法的処置に使用されることがあります。このプログラムへの参加により、インテル法務部が必要と判断したときはいつでも、インテル法務部があなたの機器上の情報の調査や複製を実行することに同意したことになります。*
>
> *法的情報保留通告が課される従業員は、利用できるサービスの制限を受けることがあります。ご使用の機器で利用できるサービスについては、ご自分の責任において、IT 部門の e-Discovery チームに確認してください。」*

調査および監査方法の変更

ユーザーは、EULA の中で、インテルがユーザーのパーソナル機器を調査できることに同意します。しかし、エンタープライズ環境へのパーソナル機器の統合により、インテルの調査チームは仕事の進め方を変える必要が出てきました。ユーザーに意識させずにパーソナル機器を調査することは、企業が所有する機器の調査よりもはるかに困難です。したがって、インテル IT 部門は、どのような行動に対してパーソナル機器の引き渡しを求め、調査を行う必要があるかを注意深く定義しました。また、そもそもパーソナル機器の調査が必要にならないような方法でサービスのパッケージとリリースを行うように努めています。

ユーザーとサービスデスク・スタッフのトレーニング

パーソナル機器を適切に管理するには、ポリシーを策定するだけでは不十分です。ポリシーがどのような意味を持ち、パーソナル機器上の情報をどのように保護するかについて、ユーザーのトレーニングを行う必要がありました。

例えば、ブログでのユーザーとの対話から、パーソナル機器にインテルの情報が保存されている場合でも、その機器を家族に貸すのを断るユーザーはおよそ 3 分の 1 にすぎないことがわかりました。このような行動が企業情報にもたらす危険についてユーザーを啓発することで、行動様式の改善を通じた情報セキュリティーの強化を図れる可能性があります。

また、IT サービスデスク・スタッフが EULA に関するユーザーの質問に間違った回答をし、それが原因で EULA の一部が効力を失うことを防ぐため、EULA に関する質問に対する答え方のトレーニングが必要であることもわかりました。例えば、インテル IT 部門がパーソナル機器に対してどのような形式のモニタリングを実行しているかについて質問された場合、サービスデスク・スタッフは、将来のパーソナル機器のモニタリングに関するインテルの決定を法律的に妨げるような回答をしないように注意しなければなりません。サービスデスク・スタッフとエンドユーザーに対するこうしたトレーニングには、よくある質問（FAQ）の利用が効果的です。

技術的な注意点

パーソナル機器ポリシーの導入に当たり、最大の技術的課題のひとつは、ファイアウォールの認証に関する問題です。IT 部門が管理しているシステムについては、ユーザーが知っている情報（パスワード）とユーザーが所有している物（登録済みのノートブック PC）の 2 つのファクターによる認証が行われます。しかし、未知のデバイスについては、ひとつの認証基準しか利用できません。

したがって、エンタープライズ環境でパーソナル機器の利用を許可するための興味深い課題のひとつは、どのようにパーソナル機器上の情報（ユーザーに所属しない情報）を利用してネットワーク認証を行うかということです。従業員がネットワーク認証情報を所有していると、ユーザーが自分のデータを他のデバイスに移動してネットワークにアクセスした場合、インテルには懲戒処分の根拠がありません。例えば、ユーザーがモバイル機器のハードウェアを所有している場合、その機器の International Mobile Equipment Identity（IMEI）番号はユーザーに所属するため、インテルはその情報を使用してデバイスを認証することができません。

この問題に対処するため、現在インテル IT 部門では、事前に定義された電話番号にテキストメッセージを送信しています。このテキストメッセージがユーザーのパスワードになります。このシナリオでは、電話番号が「持っていなければならない」認証ファクターになり、テキストメッセージが「知っていなければならない」認証ファクターになります。

また、デバイス管理では、ひとつのソリューションですべてのデバイスとアプリケーションに対応できるわけではありません。インテルのデバイス管理ポリシーは、デバイスが紛失または盗難にあう場合を想定して設計されて

います。したがって、悪意のある攻撃に対しては、デバイス自体の保護機能の有効性を想定しています。つまり、デバイス上のデータの暗号化、間違ったパスワードの入力が所定の回数に達した場合のデータの自己消去、IT 部門によるリモートからのデバイス上のデータ消去が可能でなければなりません。インテルのパーソナル機器ポリシーでは、ユーザーは紛失や盗難が起こる前にデータ管理を徹底することを求められます。

また、必要なセキュリティー・レベルはサービスによって異なります。例えば、会議室予約システムには、販売管理データベースほど高いセキュリティー・レベルは必要ありません。したがって、会議室予約システムは、IT 部門の管理制御がそれほど厳格でないデバイス上で利用できます。インテル IT 部門では、階層型の運用管理システムを開発しました。図 3 にこのシステムを示しています。

結 果

エンタープライズ環境での個人所有のハンドヘルド機器の使用を許可するインテルのポリシーが導入されてから、ほぼ半年が経過しました。最初の 1 カ月で 3,000 名のインテル従業員がプログラムに参加しました。現在、インテルの環境では 20,000 台のハンドヘルド機器が利用されており、そのうち 6,500 台はインテルの従業員が個人で所有する機器です。2010 年 7 月には、個人所有のタブレットの使用を許可する新しいプログラムがスタートしました。

このような成果は、以下の 3 本の柱からなる手法によって達成されました。

- 従業員が個人所有デバイスを使ってできることとできないことを、従業員が理解できる表現で厳密に規定した EULA
- 新しい認証方法などの技術的ソリューションによる情報の保護
- 企業情報にアクセスできるデバイスを家族や友人に貸さないことなど、ユーザーに対する情報セキュリティーのトレーニングによるパーソナル機器の使用方法の改善

このような手法により、インテルの情報セキュリティー基準を損なうことなく、個人所有のハンドヘルド機器をインテルのインフラストラクチャーに統合することに成功しました。

その結果、パーソナル機器から送信される電子メールの数と削減できた労働時間によって測定される生産性が大きく向上しました。また、適切にセキュリティー管理されたデバイスが多数利用可能になったため、社内ネットワーク上の未承認デバイスが大幅に減少し、現時点で 0.5% 未満になりました。

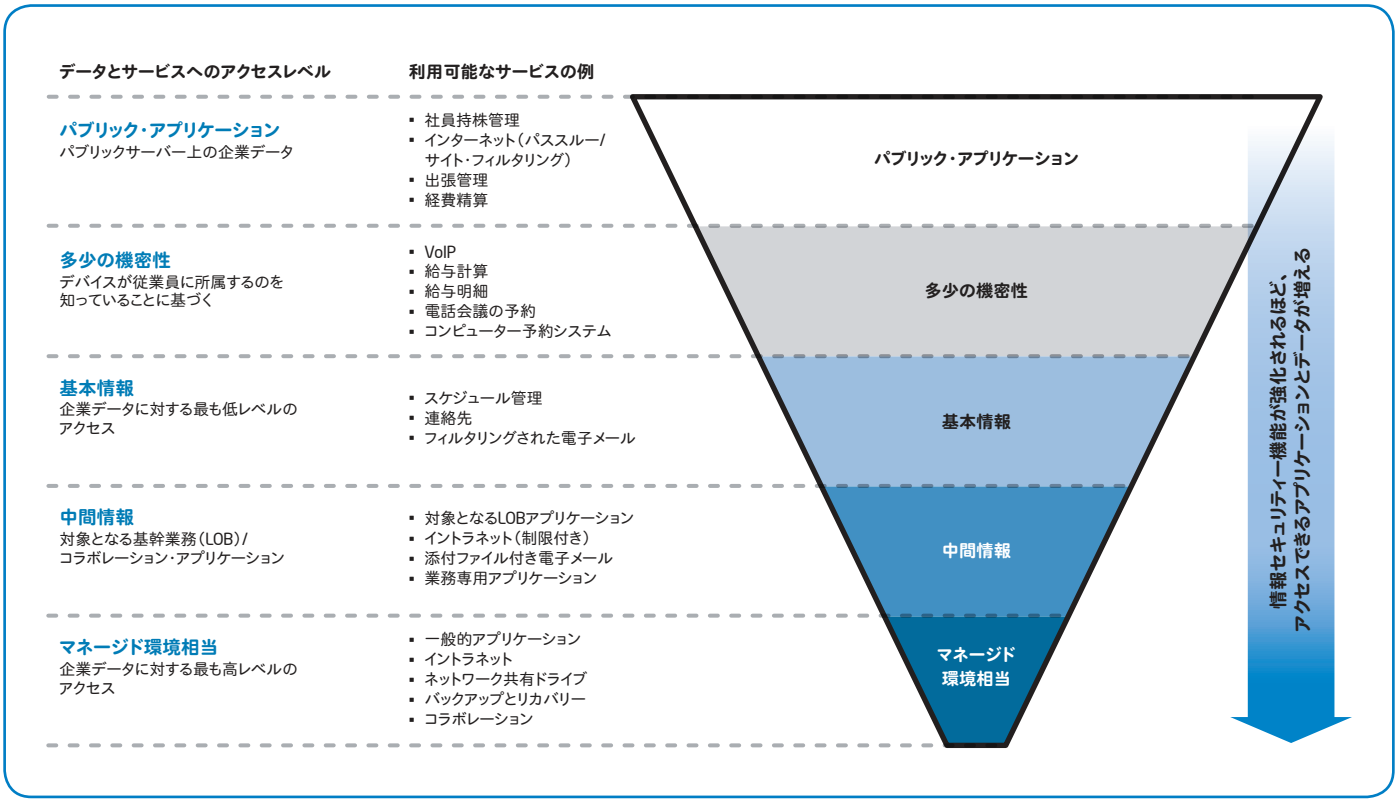

図 3. 階層型のデバイス運用管理手法により、情報とアプリケーションの重要度に合わせた運用管理レベルを設定できます。

今後の計画

ハンドヘルド機器は、インテルの従業員がメインで使用する PC と組み合わせて使用する補助的なデバイスであり、ノートブック PC に代わるものではありませんが、インテルの IT インフラストラクチャーの重要な構成要素です。インテル IT 部門では、将来パーソナル機器の運用管理をノートブック PC と同じ方法で行えるように、ユーザー機能の強化とデバイス管理機能の向上のための予算を用意しています。

運用管理チームは、レポーティング機能とセキュリティー管理機能を向上させた、新しい管理コンソールの開発を進めています。この新しい運用管理システムは、2010 年末までに導入される予定です。

インテル IT 部門では、パイロット・プロジェクトを通じて、企業所有および個人所有のハンドヘルド機器の次のような利用モデルとサポートモデルについて調査しています。

- 企業所有のハンドヘルド機器を使用して、サプライヤーからの電子メールを受信
- 企業所有または個人所有の低コストのハンドヘルド機器を使用して、インテル IT 部門のサーバーからの電子メールを受信
- 接続用ポータルを使って任意のハンドヘルド機器の利用を許可するが、オフラインでの情報の利用は許可しない

また、ハンドヘルド機器からアプリケーションへのアクセス改善に取り組むチームも活動しています。例えば、個人所有のハンドヘルド機器からインテルのイントラネットへのアクセスがまもなく可能になります。また、他のインテル従業員を探して連絡をとるときに一般的なソーシャルメディア・アプリケーションの利用を許可する案についても検討中です。ソーシャルメディアの利用は、インテルの社内従業員名簿よりも好まれているようです。

まとめ

インテル IT 部門では、職場環境における大きなトレンドである IT のコンシューマー化について、3 年にわたる積極的な調査を行ってきました。これまでに、包括的な情報セキュリティー・ポリシーの策定、ユーザーとサービスデスク・スタッフに対する情報セキュリティー・ポリシーのトレーニング、インテルの情報セキュリティー要件に適合する技術的ソリューションの開発を進めてきました。これらの成果に基づいて、インテル IT 部門は、インテルの企業データを危険にさらすことなく、IT のコンシューマー化の利点を活用しています。

エンタープライズ環境でパーソナル機器を使用したいという従業員の要求にうまく対応するには、このトレンドを無視するのではなく、将来を見据えて予測することが重要でした。他社との対話から、何も対策をとらないために自社の環境の管理に失敗している事例が多いことがわかりました。インテルの成功は、公平な手法でポリシーを策定したことにも基づいています。パーソナル機器の各利用モデルは一貫性をもって扱われます。ある従業員がポリシーに反した行動を取った場合、それがすでに広く行われていることであればその対策をとることは難しいでしょう。ポリシーで認めてしまうか、全体に禁止する必要があります。

現在インテルでは、移動の多いユーザーは、ノートブック PC と組み合わせて使用する補助的なデバイスとして、個人所有または企業所有のハンドヘルド機器を使用できます。同じ業務を担当する従業員でも好みは異なるため、各自のワークスタイルに合ったハンドヘルド機器の使用を許可することで、従業員の生産性と満足度の向上を実現できます。

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。

略 語

EULA	エンドユーザー・ライセンス契約
FAQ	よくある質問
IDS	侵入検知システム
IMEI	International Mobile Equipment Identity（国際移動体装置識別番号）
LOB	基幹業務
PDA	携帯情報端末

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 年 2 月

323956-001JA
JPN/1102/PDF/SE/IT/NT