IT@Intel ホワイトペーパー
インテル IT 部門
ビジネス・ソリューション
2010 年 5 月

フルディスク暗号化の導入による企業情報の保護

概 要

インテル IT 部門は、インテルの知的財産と従業員の個人情報の保護を強化するため、2009 年以降、従業員に支給される会社所有のすべてのノートブック PC へのフルディスク暗号化の導入を開始しました。この手法によりデータ、アプリケーション、OS、空き容量を含むディスクドライブ全体が暗号化されるため、万一システムが紛失や盗難にあっても、悪意のある個人がデータにアクセスすることは不可能になります。インテル IT 部門は、12 カ月間で社内にある対象ノートブック PC の 75% 以上にフルディスク暗号化を導入しました。

インテルの成功はインテルの知的財産の上に築かれています。情報こそインテルの基盤であり、情報の管理について誤りをおかすことは誰にも許されません。

– インテル コーポレーション
CIO
Diane Bryant

インテル IT 部門は、暗号化プログラムをスムーズに導入するため、段階的に計画を実施しました。業務の中断を最小限に抑えるため、2009 年前半は、従業員が自分の都合に合わせて暗号化ソフトウェアをインストールできる「プル型」の導入を推進しました。そして、社内のノートブック PC の 70% に暗号化プログラムのインストールが完了するという目標が達成された時点で、残りのすべてのノートブック PC に対して暗号化ソフトウェアのインストールを強制する「プッシュ型」の導入に切り替えました。

インテル IT 部門では、次のような複数の戦略に基づいて導入プロセスを管理しました。

- 導入を実施する前に、運用スタッフおよびサービス・デスク・スタッフのためのトレーニング、リソース、運用管理インフラストラクチャーを用意する。
- 自動化されたクライアント・インストール・パッケージを開発し、インストール・プロセスをできる限り簡略化する。
- 定期的なミーティングを行い、経営幹部およびグループ管理者と情報を共有し、迅速な意思決定によって導入時に発生する問題に対処できるようにする。
- 暗号化が完了したノートブック PC の台数とサービス・デスク・コールの件数に関する測定基準を基に進捗状況を管理することで、暗号化の導入率、スケジュール目標、サポートサービスの負担のバランスをとる。
- エンドユーザー向けのトレーニングとリソースを通じて、あるいは経営幹部からターゲットとなるユーザー宛に電子メールを送るなどして、暗号化の導入を促進する。

こうした周到かつ多彩な戦略により、導入スケジュールの積極的な推進、従業員の生産性に与える影響の最小化、（暗号化の導入に関する問題の解決に付随した）サポートサービスの過大な負担の回避など、さまざまな問題にバランス良く対応することが可能となりました。IT 部門の予測では、最後のプッシュ型導入フェーズによって残りのノートブック PC へのフルディスク暗号化導入を 2010 年半ばまでに完了するという目標はほぼ達成できそうです。

Rex Rountree
インテル IT 部門
暗号化サービス・マネージャー

Carol Kasten
インテル IT 部門
e-Discovery/
調査チーム・マネージャー

Michael Amirfathi
インテル IT 部門
エンジニアリング情報保護 /
暗号化サービス・マネージャー

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。

背 景

業界の動向によると、近年、セキュリティー攻撃はこれまで以上に深刻化し、より標的を絞った、経済的な動機に基づく、組織的な行動になっています。インテル IT 部門の内部リスク分析では、インテルで重大なセキュリティー違反が 1 回発生した場合、直接的なコストだけで 500 万米ドル以上の損害をもたらすという結果も出ています。

インテル IT 部門は、このような増大する脅威とデータの紛失や盗難によって発生する損失コストに対処するため、2008 年後半、従業員に支給されるすべてのノートブック PC にフルディスク暗号化を導入することを決定しました。フルディスク暗号化の導入によって、データ、アプリケーション、OS、空き容量を含むディスクドライブ全体が暗号化されるため、万一システムが紛失や盗難にあっても、悪意のある個人がデータにアクセスすることは不可能になります。フルディスク暗号化が適切に導入されれば、従業員の積極的な関与をまったく必要としない、強力かつ自動的なセキュリティー・ソリューションが実現します。フルディスク暗号化は成熟した技術を基盤としており、すべてのノートブック PC への導入が可能であり、他のテクノロジーとの組み合わせにおける基礎的なセキュリティー・レイヤーを提供します。

ただし、インテルの従業員の 80% がノートブック PC を使用しており、フルディスク暗号化の導入はその全員に影響を与えるため、大きなリスクを伴うことも計画の開始時点で判明していました。こうしたリスクを軽減するため、導入戦略は慎重に計画されました。計画を実行に移す前に、表 1 に示す要件を明確化した上で、暗号化製品と供給ベンダーの広範囲にわたる評価、トレーニングの準備を行い、リソースと運用管理インフラストラクチャーを確立しました。[1]

製品評価プロセスでは、アナリストのレポートや第三者機関のレビューによる暗号化製品の調査、インテルのラボでの製品テスト、大規模な暗号化の導入をすでに実施していた同業他社の聞き取り調査を行いました。こうした評価と聞き取り調査のプロセスは、暗号化ソリューションの決定に役立っただけでなく、実際の導入時に陥りやすいミスや誤操作、既知の最適手法（BKM）を確認する上でも効果があり、導入計画全体に大きな影響を与えました。表 2 には、同業他社の聞き取り調査から得られた結果をまとめています。

1 このプロセスの詳細については、『Strengthening Enterprise Security through Notebook Encryption』（英語）、インテル コーポレーション（2008 年 12 月）を参照してください。

ソリューション

インテル IT 部門は、慎重な計画と準備に基づき、2009 年前半、すべての対象ノートブック PC の暗号化を 1 年以内に完了するという積極的な目標の下で暗号化ソリューションの導入を開始しました。短い期間を設定した結果、従業員の生産活動の中断、運用への影響、サービス・デスク・スタッフの負担が最小限に抑えられました。

導入計画

インテル IT 部門では、スムーズなインストール・プロセスを実現するため、まずは運用スタッフとサービス・デスク・スタッフのためのトレーニング、リソース、運用管理インフラストラクチャーを準備しました。また、エンドユーザー向けに、対象を絞ったコミュニケーション、リソース、トレーニング資料を作成しました。

運 用

インテル IT 部門は、初期導入とその後の更新、ノートブック PC のリカバリー、電子情報開示（e-Discovery）、モニタリング、監査のための運用チームを編成しました。リカバリーと e-Discovery のプロセスは特に重要です。これらのプロセスでは、法律的要件およびインテルが定めた要件の遵守と、エンドユーザーの個人情報の保護を両立する必要があります。インテルではすでにこれらのプロセスを処理する包括的な認証フレームワークを確立していたため、このフレームワークを拡張して、ノートブック PC の暗号化に適用しました。例えば、退職した従業員のノートブック PC にアクセスするには、該当する法務マネージャー、業務マネージャー、および技術マネージャーの承認が必要となります。

サービスデスク

サポートスタッフには、暗号化ソフトウェアのダウンロード、インストール、プロビジョニング、その後の問題解決について従業員をサポートできるようにするためのトレーニング資料と問答集を用意しました。調査の結果

表 1. インテル IT 部門によるフルディスク暗号化導入の要件

要 件	説 明
セキュリティーの相互運用性	暗号化ソリューションには、インテルの既存のノートブック PC 向けセキュリティー・ソリューションとの整合性と相互運用性が必要とされます。また、暗号化ソリューションは、ノートブック PC 上に安全な暗号化鍵ストレージを確保し、マルチファクター認証をサポートする必要があります。さらに、法令および各種規制への対応のため、連邦情報処理標準（FIPS）や米国国立標準技術研究所（NIST）などの標準的な認証規格に準拠していなければなりません。
エンタープライズ運用管理機能	管理効率の向上のため、暗号化ソリューションには、インテル® vPro™ テクノロジーとの相互運用性をはじめとする、既存の管理ツール / プロセスとの整合性が必要とされます。
ノートブック PC ユーザーへの影響の最小化	業務の中断、トレーニング、サービスデスクの負担を最小限に抑えるため、暗号化ソリューションの導入はノートブック PC ユーザーにとって簡単な作業でなければなりません。ノートブック PC のパフォーマンスへの影響も最小限に抑える必要があります。従業員のワークフローの中断など、生産性の低下は望ましくありません。
スムーズな導入	この暗号化ソリューションでは、インテル IT 部門の既存のノートブック PC 運用管理インフラストラクチャーを利用した自動化された導入プロセスがサポートされる必要があります。また、インストールの失敗時に手作業によるサポートのコストが生じないように、導入時の問題の検出用および解決用ツールを準備しておく必要があります。
OS の互換性	暗号化ソリューションは、インテルのノートブック PC 環境で使用されているすべての OS および OS バージョンとの完全な互換性を備えている必要があります。
対象となるノートブック PC の要件	暗号化の対象となるのは、インテル® Core™2 Duo プロセッサー以降のプロセッサーを搭載したノートブック PC に限られます。これより古いプロセッサーを搭載したノートブック PC に暗号化プログラムをインストールすると、パフォーマンスが大幅に低下することが判明したため、このような決定に至りました。

表 2. 同業他社の聞き取り調査から得られたフィードバック

要 件	具体的なニーズ
データの損失	今回の聞き取り調査の対象企業からは、導入時のデータ損失は報告されていません。ただし、暗号化ベンダーが提供するツールを使用して、ノートブック PC 上のデータを復元する必要があったという事例も多少見られました。
ディスク・エラー・スキャン	導入前のディスク・エラー・スキャン・ユーティリティーとデフラグ・ユーティリティーの実行が、導入時のエラー回避にかなり有効であることが判明しています。これらのユーティリティーを実行しなかった企業では、導入の失敗率が 1 ～ 2% に達しました。かつては、暗号化プロセスの実行中にハードディスク・ドライブの不良セクターが検出された場合、システムがクラッシュすることがありました。しかし、現在の先進的なソリューションは、不良セクターが検出されると自動的にインストールを中止します。インストールを再試行する前に、システム上でディスクエラーのスキャンを実行できます。
導入期間	導入期間は、18 カ月で 6,000 台から、3 カ月で 15,000 台まで、各企業間で非常に大きな差があります。ただし、このような違いは、選択した暗号化製品よって生じるものではなく、その企業の戦略と社内の IT 問題に左右されるようです。
サービス・デスク / サービス・サポート・コールの件数	すべての調査対象企業で、初期導入時にはサービス・デスク / サービス・サポート・コールの件数が増えましたが、数週間以内に通常の件数に戻りました。
リカバリーと電子情報開示（e-Discovery）	リカバリーおよび e-Discovery のツールとプロセスに関する問題は報告されていません。

では、ユーザーからの質問はパスフレーズの作成と再設定に集中するだろうと予想されました。パスフレーズは暗号化プログラムの起動に必要とされます。パスフレーズは、複数の単語からなり、各単語の間にはスペースを含む覚えやすいフレーズ（文など）を使って設定されます。インテル IT 部門では、シングルサインオン（SSO）認証ではなく、パスフレーズ認証を採用しました。これは、パスフレーズの方が長くて複雑で、セキュリティーの強化につながるためです。

エンドユーザー

インテル IT 部門は、導入の実施前に従業員向けメッセージを作成し、すべてのノートブック PC ユーザーに電子メールで送信しました。これらのメッセージでは、暗号化の必要性と、暗号化の導入と使用によって予想される結果が詳しく説明されました。ユーザーは、新しいパスフレーズの要件について理解し、ディスク暗号化プロセスの実行中に発生する多少のパフォーマンス低下に備える必要がありました。そのため、フルディスク暗号化を実行した後も、システムの通常の使用時にはパフォーマンスの低下は感じられないことも説明されました。ただし、スタートアップ、シャットダウン、ハイバーネーションへの移行 / 復帰時には、多少のパフォーマンス低下が感じられる場合もあります。また、ソリッドステート・ドライブ（SSD）の動作速度はハードディスク・ドライブ（HDD）より高速なため、SSD を搭載したノートブック PC では、暗号化プログラムのインストール後のパフォーマンスの低下が多少大きくなることが予想されます。こうしたパフォーマンス低下とその解決方法の詳細については、「ソリッドステート・ドライブの導入」を参照してください。さらに、処理速度が向上した新しいノートブック PC では、暗号化プログラムのインストール後のパフォーマンス低下はほぼ無視できそうなことも説明されました。

インストール・プロセスをできる限り簡単にするため、従業員向けイントラネット上に作成した Web サイト上に、自動化されたクライアント・インストール・パッケージを用意しました。この Web サイトには、ダウンロード可能な暗号化プログラムのほか、簡易インストール手順書などのトレーニング資料、対象システムの要件、従業員のセキュリティー意識を高めるための資料、経営幹部が全社規模での暗号化の重要性を説明するビデオ、よくある質問（FAQ）が掲載されました。

段階的導入

ノートブック PC ユーザーの生産性への影響を最小限に抑えるため、「プル型」の導入プロセスを実施して、従業員が自分のスケジュールに合わせて暗号化プログラムをインストールし、HDD を暗号化できるようにしました。従業員は自分の都合の良いときにインテル IT 部門のダウンロード・サイトから暗号化プログラムをダウンロードし、インストール、プロビジョニングを実行しました。そして、ノートブック PC ユーザーの 70% が暗号化プログラムをダウンロードした段階で、まだ暗号化されていないすべてのノートブック PC に対して暗号化ソフトウェアを「プッシュ」することで、規則遵守の強制を開始しました。

インテル IT 部門では、まずは対象を絞り込んだ小規模な導入を行うことで、暗号化ソリューションとプロセスを徹底的にテストしました。それぞれの事例ごとの技術的な問題点と運用上の問題点を記録し、適切な解決策を作成しました。また、これらのテスト導入に合わせて導入計画プロセスの調整を行い、導入結果に基づいてインフラストラクチャーとトレーニング・プログラムを見直しました。

インテル IT 部門は、図 1 に示す 4 つの導入フェーズを定義しました。

- **小規模な評価：**約 20 人のエンドユーザーへの導入（全員が暗号化チームの同僚）。
- **概念実証：**さまざまなエンジニアリング・グループとカスタマー・サポート・グループに属する 100 人のエンドユーザーで構成される、より大規模なテストグループへの導入。これらのユーザーは、平均的なエンドユーザーよりもコンピューターに関して詳しい知識を持ち、実際に問題が発生する前に問題の解決に取り組む傾向を有します。
- **完全な実稼動環境でのパイロット：**幅広い業務に携わる 1,000 人のエンドユーザーへの導入による、最終的なフル導入のシミュレーション。このグループのテストでは、すべてのユーザーを効果的にサポートできることが確認され、全社規模の導入時に発生しそうな問題が明らかになりました。
- **一般ユーザーへの導入：**残りのすべてのノートブック PC への暗号化プログラムの導入。このフェーズでは、まずプル型の導入を実施し、ノートブック PC の 70% が暗号化された段階でプッシュ型の導入に切り替えました。現在はこの一般ユーザーへの導入フェーズが進められており、社内のすべてのノートブック PC のうち 75% 以上は暗号化が完了しています。

進捗状況の管理

インテル IT 部門は、導入プロセス全体を通して定期的なミーティングを行うことで、上層部と情報を共有し、迅速な意思決定を可能にしました。こうしたミーティングには、以下のメリットがありました。

- プロジェクトの進捗状況を確認し、技術的な課題と導入時の問題について議論することで、そうした問題の適切な管理が可能となる。
- 暗号化の導入による業務への影響についての理解が深まり、効果的かつタイムリーな対応が行われる。
- 経営幹部との間で進捗状況が共有され、問題と解決策についての検討が行われる。

インテル IT 部門は、導入計画の完了まで 1 年という積極的なスケジュール目標を設定しました。このスケジュールの達成という目標と、サポートサービスへの負担、従業員の生産性への影響を最小限に抑えるという目標の間では、慎重なバランス調整が必要となります。そのため、導入プロセスの測定基準を確立し、それを使って追跡調査することで、導入の進捗状況のモニタリングと導入戦略の調整を可能としました。

- **全体的な導入の進捗状況：**インテル IT 部門は、経営幹部およびグループ管理者と協力して、社内の導入目標を明確化しました。これらの目標に従って、導入プロセスのモニタリング方法を決定し、スケジュールに対する実際の進捗状況を測定しました。この進捗状況の管理は、どの時点でプル型からプッシュ型の導入に切り替えるかを決める上で非常に重要でした。
- **サービス・デスク・コールの件数：**暗号化に関連するコールの件数と理由を追跡調査しました。そして、コール件数が上限を超えた場合は、従業員の参加促進のための電子メール・キャンペーンを減らすことで、導入のペースを抑制しました。

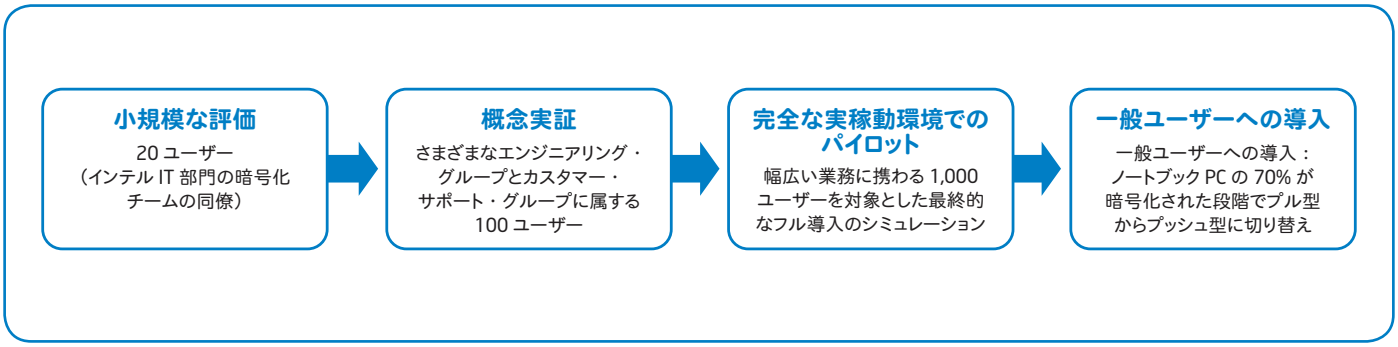

図 1. インテル IT 部門は、フルディスク暗号化を 4 つのフェーズで導入することで、一般ユーザーへの導入の前に暗号化ソリューションを徹底的にテストしました。

暗号化導入の促進

従業員の生産性への影響をできる限り軽減するため、初期のプル型導入フェーズでは、従業員が自分の都合の良いときに暗号化プログラムをインストールできるようにしました。しかし、この決定により、多くの PC で暗号化の導入が遅れてしまいました。インストールにかかる手間と時間やその他の問題についての情報を、同僚から耳にしたりインテル IT 部門からのメッセージやトレーニング資料から得た結果、暗号化プログラムのインストールを延期する従業員が続出してしまいました。

IT 部門が用意したインストール手順では、従業員は業務時間中、ネットワークに接続しているときに Web サイトに登録して暗号化プログラムをダウンロードし（このプロセスの所要時間は約 10 分）、ノートブック PC を使用しない夜間や週末に暗号化プロセスを実行するように推奨していました。この実行には、HDD の容量と動作速度に応じて 2 ～ 4 時間ほどかかります。

インストール率を上げるため、インテル IT 部門はこの問題にもできる限り迅速に対処しました。インストール時に陥りやすいミスや誤操作を避けられるようにインストール手順書の改善を進める一方、導入を促進するためのメッセージの配布を開始しました。

- 暗号化の重要性について説明するポスターをサービス・デスク・センターに掲載し、ノートブック PC を持ち込むすべてのユーザーがポスターを目にするようにしました。
- 暗号化の重要性について説明し、暗号化プログラムのインストールを従業員に勧めるインテルの CEO および CIO 名義の電子メールメッセージを送信しました。図 2 に示すように、CEO からの電子メールの送信後、暗号化プログラムのインストール件数は 8 倍に増えました。暗号化プログラムの導入の成功に、上級管理者のサポートは不可欠でした。
- 人事データなどの最重要データが置かれた高リスクなノートブック PC 群の優先度を引き上げ、できる限り早い時点で暗号化プログラムが導入されるようにしました。高リスクデータを扱うユーザーに電子メール・キャンペーンの対象を絞り、最新型 PC への更新の優先度を引き上げることで、彼らの PC への導入を迅速に進めました。
- 電子メールによるキャンペーン規模は、サービスデスクに寄せられる暗号化に関連するコール件数に応じて調整しました。コール件数が事前に決めたしきい値を下回った場合は電子メール・キャンペーンのメッセージ数を増やし、より多くの従業員に暗号化プログラムのインストールを促しました。サービスデスクおよびサービス・サポート・コールの件数が事前に決めたしきい値を上回った場合は、電子メール・キャンペーンの規模を縮小しました。

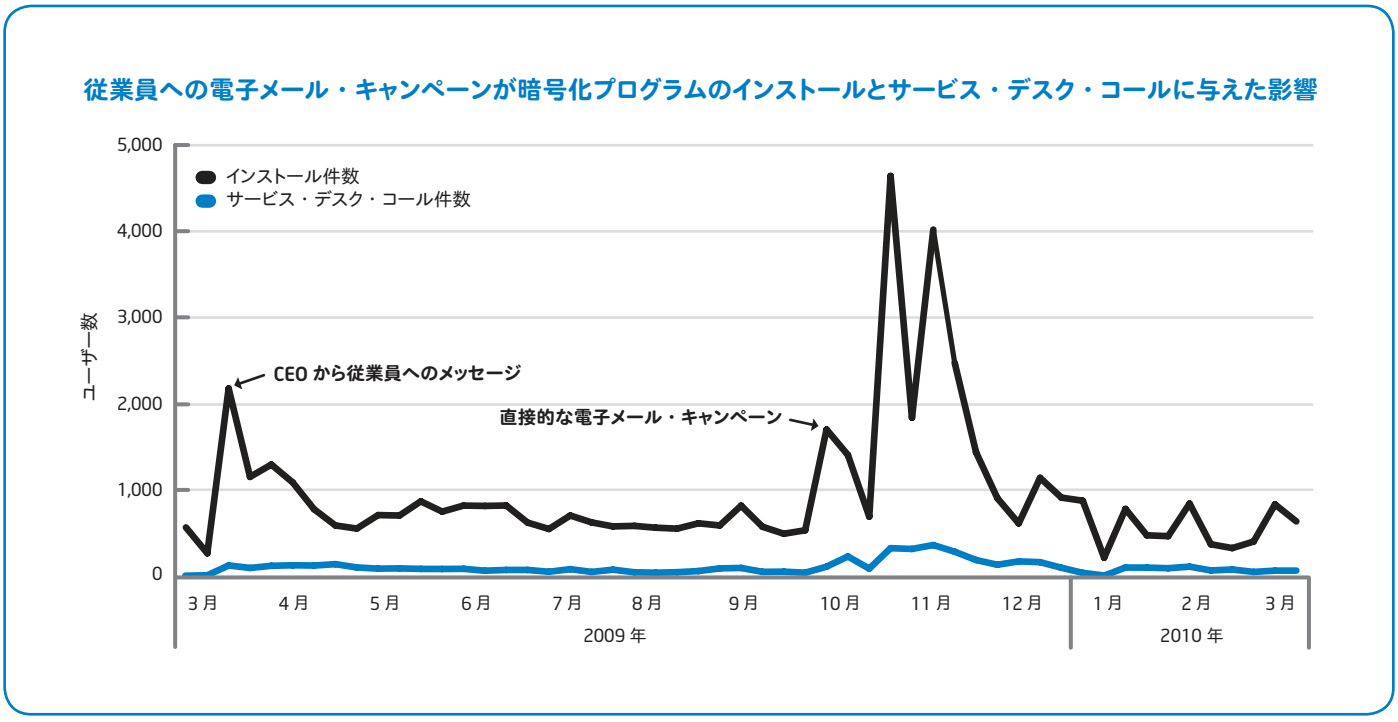

図 2. インテルの経営幹部からの電子メールメッセージの送付とインテル IT 部門のエンドユーザー向け電子メール・キャンペーンにより、暗号化プログラムのインストール件数とサービス・デスク・コール件数が増加しました。コール件数が上限を超えた場合は、これらのコミュニケーションを減らすことで導入ペースを遅らせました。

運用管理の向上によるセキュリティーの強化

従業員のノートブック PC のセキュリティーを確保するには、データの暗号化だけでは不十分です。セキュリティー確保のためには、効果的なクライアント運用管理によって、システム構成全体のセキュリティーを強化する必要があります。従業員のノートブック PC（およびデスクトップ PC）をより効果的に、より低いコストで管理できるように、インテル IT 部門は現在、社内のクライアント・システムとサポート・インフラストラクチャーをアップグレードしてインテル® vPro™ テクノロジーを利用するプロセスを数年かけて推進しています。2009 年末の時点では、約 50,000 台のインテル® vPro™ テクノロジー対応 PC の導入とプロビジョニングが完了しました。

インテル® vPro™ テクノロジーに対応したクライアント・システムには、セキュリティー、メンテナンス、資産管理を向上するハードウェア・ベースの機能がビルトインされています。これらの PC には、システムの電源がオフだったり、OS がダウンしていたり、ソフトウェア・エージェントが無効化されていたり、あるいは HDD が故障している状況でも、承認された運用管理アプリケーションとサポートスタッフが有線および無線ネットワークを介してアクセスすることが可能です。

インテル IT 部門は、生産性の向上とサポートコストの削減を実現する、インテル® vPro™ テクノロジーの複数のユースケース・シナリオを作成しました。例えば、そうしたシナリオの中には、リモートからのユーザーのパスフレーズの再設定を支援するものがあります。サービスデスクは、数分間で PC の管理を引き継ぎ、リモートからパスフレーズ再有効化コードを入力できます。パスフレーズ再有効化コードは、26 ～ 32 文字の英数字文字列です。リモートから文字列を入力することは、時間の短縮につながる上、サービスデスクのスタッフとユーザー間の伝達ミスによるエラーが減少します。インテル® vPro™ テクノロジーのリモート運用管理機能に関連するこれらのユースケースの詳細については、ビデオ「3 Use Cases with Intel vPro technology」（英語）（http://communities.intel.com/docs/DOC-4165/）をご覧ください。

新しいサポートプロセスの導入

初期の試験的な導入段階おけるサービスデスクの主な課題とは、ノートブック PC ユーザーに対して、新しいパスフレーズの作成に関する指針を提供することでした。インテルの従業員は、従来はノートブック PC を使用する前に 2 つのパスワード（システムの起動に必要な HDD 認証パスワードと、OS ログオンパスワード）を入力する必要がありました。各従業員の HDD のフルディスク暗号化の完了後、HDD 認証パスワードは廃止され、ノートブック PC 暗号化パスフレーズに置き換えられました。

インテル IT 部門では、新しい暗号化ソリューションの導入時には、パスワードの長さと強度要件をより厳しくすることが重要であると考えました。すべての従業員は、従来の OS ログオンパスワードの使用を続ける一方、この新しい要件に応えるために暗号化ソリューション用の新しいパスフレーズを作成する必要がありました。

当初は、複数の単語から構成され、各単語の間にはスペースを含む覚えやすいフレーズ（文など）を使って設定されるパスフレーズの概念を、多くの従業員はよく理解できませんでした。彼らは、（スペースを含まない長いパスワードのような）複雑で長めの文字列を登録したため、しばしばパスフレーズを忘れてしまい、サービスデスクに連絡することになりました。

こうした混乱を避けるため、インテル IT 部門では暗号化プログラムのインストール指示の内容を見直し、その手順を明確化し、強度の強いパスフレーズの設定方法についての誤解の解消に努めました。電子メールとインテルの従業員向けイントラネット・ポータルを通じて指針を提供するほか、パスフレーズの問題に対処するサービス・デスク・スタッフの研修も行いました。また、暗号化ベンダーのツールを使用してリモートから暗号化パスフレーズを再設定するためのトレーニングを、サービス・デスク・スタッフを対象に実施しました。やがて、自分用の暗号化プログラムのインストールが終わった従業員たちが、覚えやすい安全なパスフレーズの設定方法について同僚に教えるようになりました。

パスフレーズを忘れた場合のリカバリーの失敗の回避

パスワードを忘れた従業員がサービスデスクに連絡すると、サービス・デスク・スタッフは一度限り有効な一時的な再有効化コードを提供します。しかし、再有効化コードを使用してパスフレーズ要求を回避し、再びログオンした後、パスフレーズを変更しないままログアウトしてしまう従業員も少なくありませんでした。この場合、システムの再構築とバックアップからのデータリカバリーが必要になります。こうした問題が頻発した結果、サポートプロセスが変更され、サービス・デスク・スタッフは従業員による再有効化コードを使用したノートブック PC へのログオンを手助けするだけでなく、従業員が直ちにパスフレーズを再設定するように指導することにしました。サービス・デスク・スタッフは、このプロセスについて電話でユーザーに説明しました（このプロセスの所要時間は 15 ～ 20 分）。あるいは、ノートブック PC 上でインテル® vPro™ テクノロジーが有効になっていれば、サービス・サポート・スタッフは同じプロセスをリモートから 3 ～ 5 分以内に実行できます（上記の「運用管理の向上によるセキュリティーの強化」を参照）。

e-Discovery 実行時のハードディスクへのアクセス

従業員がすでにインテルを退職している場合に備えて、サービス・デスク・スタッフは、e-Discovery を利用してノートブック PC 上のデータにアクセスできるようにする必要がありました。そのためにインテル IT 部門は新しいプロセスを確立しました。このプロセスでは、適切な承認を得た上で、サービス・デスク・スタッフの支援により、e-Discovery のスタッフは、一時的な再有効化コードを使って返却されたノートブック PC にログオンし、直ちにパスフレーズを再設定してノートブック PC 上のデータにアクセスします。

導入時の問題への対処

インテル IT 部門は、導入プロセス全体を通して、以下に示すさまざまな課題に対処しました。

企業データのバックアップ

導入前に行われた他社との対話によって、データリカバリー用の全社規模のバックアップ・プロセスの必要性が確認されました。暗号化プロセスは HDD のすべてのセクターに影響を与えるため、暗号化プロセスの実行中に HDD の不良セクターが検出された場合、システムクラッシュが発生してデータが永久に失われるおそれがあります。

予防手段として、従業員が暗号化プログラムをインストールする前に HDD のバックアップをとる必要がありました。しかし、一部のインテルの施設では、すべてのシステムのバックアップをとるのに必要な機能やストレージ容量が不足していることがわかりました。このため、一部の地域では、このような状況が改善されるまで、暗号化の導入の延期を強いられました。しかし、暗号化プログラムの導入前にデータのバックアップを要求したことにより、自分自身のデータのバックアップ方法を習得している従業員の数が以前よりも増加するという、副次的なメリットがもたらされました。

資産管理情報の更新

従業員に連絡して暗号化プログラムをインストールしてもらうためには、すべてのノートブック PC とその使用者の完全なリストを用意する必要がありました。しかし、それまでのインテルの資産管理システムの情報は古くなっていることが判明しました。このため、より正確な情報が得られるように、資産管理システムが改善されました。

新しいノートブック PC と古いノートブック PC の区別

古いノートブック PC に暗号化プログラムをインストールした場合、パフォーマンスが大幅に低下することが判明しました。この問題に対処するため、暗号化プログラムのインストール対象をインテル® Core™2 Duo プロセッサー以降のプロセッサーを搭載したノートブック PC のみとすることを決定しました。古いノートブック PC は 2 ～ 4 年ごとの定期的な PC 更新サイクル内に新しいノートブック PC に更新され、そのすべてに暗号化プログラムが導入されました。

構成の互換性の問題の特定

インテル社内のノートブック PC の約 10% は、特殊なビジネス要件への対応のため、インテルの標準ビルドとは異なる独自構成になっていました。これらの構成については、暗号化プログラムの導入時に独自の修正措置が必要でした。インストール時の問題発生と生産性の低下を避けるため、ユーザーが暗号化プログラムを導入する前に、これらの独自構成を簡単に特定するための方法が必要になりました。

インテル IT 部門は、独自のプラットフォーム・ビルドと標準プラットフォーム・ビルドを識別できるアプリケーションを開発し、インストール時に従業員が独自の構成を扱える手順を用意することにしました。互換性のない暗号化プログラムや代替暗号化プログラムがノートブック PC にインストールされていた場合は、新しい暗号化プログラムをインストールする前に古いプログラムを削除する方法が従業員に指示されました。複数のビルドや特殊なシステム環境（複数のブートシステム、複数のパーティション、複数の仮想化環境など）で構成されたノートブック PC については、インストール時にそれらの環境を管理する方法が従業員に提示されました。

ソリッドステート・ドライブの導入

インテル IT 部門は、インテル® SSD の評価を実施し、その大きな利点（IT サポートコストの削減、ユーザーの生産性の向上など）を確認した後、インテルの標準 IT ビルドの一環として SSD を搭載したノートブック PC の導入を開始しました。SSD の導入は、暗号化導入プロセスの進行中に決定されました。SSD は HDD よりもデータアクセスがはるかに高速なため、当初、暗号化プログラムのインストール後のドライブ性能の低下率は HDD に比べて大きくなりました。

インテル IT 部門は、この問題を解決するため、暗号化ベンダーと協力して、SSD の特性に対応した暗号化プログラムの再設計に取り組みました。暗号化ベンダーは、コードのパフォーマンスの向上、256 ビット暗号化と 128 ビット暗号化を選択できるオプション、インテル® Core™ i5 プロセッサー搭載の新しいノートブック PC でのみ利用可能なインテルのデュアルコア・テクノロジーとインテル® ハイパースレッディング・テクノロジーの活用を実現しました。この再設計により、暗号化プログラムのパフォーマンスは 2 倍に向上しました。

結 果

現在、インテルの対象ノートブック PC の 75% 以上で暗号化が完了し、プッシュ型の導入が順調に進行中です。暗号化プログラムの導入スケジュールは、当初想定された 1 年から 18 カ月に延長されましたが、これにより、インテルのエンドユーザーには質の良いサポートが提供され、サポートスタッフへの過度の負担も回避されました。2010 年半ばまでには、残りのノートブック PC への暗号化もすべて完了する見通しです。

次のステップ

インテル IT 部門は暗号化ベンダーと協力して、暗号化製品の次のリリースでは、インテル® Core™ i5 プロセッサー / インテル® Core™ i7 プロセッサー搭載ノートブック PC の大幅に向上したパフォーマンスを活用できるようにする予定です。また、次のリリースでは、インテル® AES New Instructions（インテル® AES-NI）向けに最適化された新しいソフトウェアも利用できるようになるでしょう。プロセッサーにビルトインされたこれらの命令によって、高速かつ安全なデータの暗号化 / 復号が実現されます。これにより、暗号化プログラムのインストールの高速化と、スタートアップ、シャットダウン、ハイバーネーションへの移行 / 復帰時の大幅なパフォーマンス向上が期待されます。

まとめ

インテル IT 部門は、フルディスク暗号化の導入プロセス全体を通してさまざまな戦略を駆使し、一つひとつの課題を着実に解決してきました。従業員のトレーニング、経営幹部およびグループ管理者とのメッセージの伝達、サポートプロセスの変更、技術的な問題や運用上の問題の解決、暗号化ベンダーとの協力による暗号化プログラムのパフォーマンス向上と技術的問題の解決など、多くの課題に対してこうした戦略は効果を上げました。

2010 年前半までに、インテルの従業員は対象となるすべてのノートブック PC の 70% にフルディスク暗号化プログラムをインストールしました。これはプル型からプッシュ型導入への切り替えの目安となる値です。この段階で、残りのノートブック PC へのインストールを確実に進めるため、暗号化プログラムのプッシュ型導入が開始されました。2010 年中頃までに、残りのノートブック PC の暗号化はすべて完了する見通しです。

暗号化プログラム導入の最終段階としては、インテル IT 部門が管理するすべてのノートブック PC へのプッシュ型導入が完了した後、暗号化のエキスパートで構成されるチームが、インテル IT 部門の管理対象ではない、特に注意すべき残りのすべてのノートブック PC に、手作業で暗号化プログラムを導入する予定です。

苛烈なサイバー攻撃やノートブック PC の紛失に関連するリスクとその損失コストは、年ごとに増大し続けています。このような状況において、インテル IT 部門は、これまで以上に緻密なエンタープライズ・セキュリティー戦略の重要性を学んできました。インテル IT 部門が進めているフルディスク暗号化の導入は、このような戦略の重要な一環を成すものです。

詳細情報

その他の IT@Intel ホワイトペーパーについては、http://www.intel.co.jp/jp/go/itatintel/ を参照してください。

- 「Strengthening Enterprise Security through Notebook Encryption」（英語）、インテル コーポレーション（2008 年 12 月）
- 「Enterprise-wide Deployment of Notebook PCs with Solid-State Drives」（英語）、インテル コーポレーション（2009 年 8 月）

略 語

BKM	既知の最適手法
FAQ	よくある質問
FIPS	連邦情報処理標準
HDD	ハードディスク・ドライブ
インテル® AES-NI	インテル® AES New Instructions
NIST	米国国立標準技術研究所
SSO	シングルサインオン
SSD	ソリッドステート・ドライブ

最新トピックに関するインテルの IT リーダーのコメントについては、http://www.intel.co.jp/jp/go/itatintel/ 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/

2011 年 12 月

323002-001JA
JPN/1112/PDF/SE/IT/NT