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 4 月

絶え間なく変化する脅威にさらされたシンクライアントのセキュリティー評価

Toby Kohlenberg
上級情報セキュリティー・スペシャリスト
インテル IT 部門

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

John Dunlop
エンタープライズ・アーキテクト
インテル IT 部門

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

概 要

インテル IT 部門のセキュリティー・チームは、日ごろからインテルのコンピューティング・モデルを分析し、絶え間なく変化する脅威に応じるためにどのように発展させていくべきかを検討しています。一連の有名な企業や Web サイトを狙った最近のサイバー攻撃をきっかけに、シンクライアント・モデルによって提供されているセキュリティーと、同様の攻撃に対するシンクライアントの防御能力について見直しを迫られることになりました。

PC であれば、シンクライアント・モデルではあきらめざるを得ない機能を利用しながらも、同等のセキュリティー管理を導入することが可能であり、また実際にインテル IT 部門では導入もしています。

インテル IT 部門の判断によると、シンクライアントは、セキュリティー上の利点とみなされることが多い 5 つの特性を備えています。それは、物理的なデータ損失の防止、管理者権限の削除、インストールできるアプリケーションの制限、クライアントの保全性、既知の良好な状態へのロールバック機能です。

しかしインテル IT 部門では、このようなセキュリティー管理は安全な環境の構築に有効ではあるけれども、最近のサイバー攻撃までは防げなかったと考えています。

また、こうしたセキュリティー管理はシンクライアントに固有のものではないことも判明しました。PC であれば、シンクライアント・モデルではあきらめざるを得ない機能を利用しながらも、同等のセキュリティー管理を導入することが可能であり、また実際にインテル IT 部門では導入もしています。こうしたセキュリティー管理がシンクライアントや PC へ包括的に導入されてこなかったのは、クライアント・アーキテクチャーが原因ではなく、多くの場合、ユーザーの生産性が許容できないほど制限されるからです。

シンクライアントのその他の制限やコストについても検討しました。例えばシンクライアントは、モバイル・コンピューティング、インタラクティブ性や演算負荷が高いアプリケーション、ビデオなどのリッチメディアに対応できません。また、サーバーの能力とネットワーク帯域幅を十分に確保する必要があります。一部のシンクライアント・モデルの場合、シンクライアントが依存している中央ネットワーク・リソースで障害が発生すると、業務が中断する可能性があります。

インテル IT 部門の分析に基づくと、シンクライアントは、一部のニッチ用途には適しています。ただし、インテルの環境は 80% がノートブック PC であり、社内ユーザーの大半はノートブック PC が持つ機能性と柔軟性を求めています。ノートブック PC には、新しいテクノロジーの傾向やサービス提供モデルを採り入れられる利点もあります。

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。

背 景

インテル IT 部門は、61 カ国にまたがりおよそ 83,500 人の従業員を抱える極めて大規模なエンタープライズ環境をサポートしています。インテルが成長を続け、競争力を維持する源となっているのは、従業員が生み出すビジネス・イノベーションです。このビジネス・イノベーションの促進に向け、インテル IT 部門は従業員の約 80% にノートブック PC を支給しています。

サイバー攻撃は急速な高度化を遂げており、従来未知であった脆弱性を発見してから数時間以内に攻撃する、ゼロデイ攻撃に移行しつつあります。有名な企業や Web サイトを狙った最近の攻撃では、Web ブラウザーのような一般的なクライアント・ソフトウェアの脆弱性を悪用しているものもあります。

インテル IT 部門のセキュリティー・チームは、このような脅威を常時監視し、インテルのビジネスモデルやコンピューティング・モデルでの対処方法を定期的に分析しています。有名な企業や Web サイトを狙った最近のサイバー攻撃をきっかけに、シンクライアント・モデルによって提供されているセキュリティーの見直しを迫られることになりました。また、同様の攻撃が将来行われた場合にシンクライアントで防御できるかどうかについても調べることにしました。

まず、シンクライアントの特性を分析してから、同様のセキュリティー管理を PC に適用できる可能性について調査しました。次に、社内ユーザーのニーズや新しいテクノロジーの傾向を考慮に入れた上で、インテル IT 部門のクライアント戦略全体の観点から調査結果を検討しました。

クライアント・セキュリティー分析

インテル IT 部門は、シンクライアントで一般的なセキュリティー管理を、高度化する脅威への効果とともに分析しました。まず、有名な企業や Web サイトを狙った最近の攻撃のような、標的を絞ったゼロデイ攻撃を防止または軽減できるかどうか評価しています。次に、同様のセキュリティー管理を PC に適用できる可能性について分析しました。

シンクライアントでの一般的なセキュリティー管理

インテル IT 部門の判断によると、シンクライアントは、セキュリティー上の利点とみなされることが多い 5 つの主要な特性を備えています。

- **物理的なデータ損失の防止：** シンクライアント・モデルの場合、データの格納先がデータセンターに限定されているので、物理的なデータ流出のリスクが減少します。さらに、シンクライアントの多くでは、外付けメディアや USB ストレージデバイスを接続するポートがないため、クライアントからデータを直接コピーする方法が制限されています。

- **権限を持たないユーザー：** ユーザーの管理者権限を削除すると、システムファイルや設定が変更される可能性を低減できます。

- **ユーザーがインストールできるアプリケーションの制限：** 追加のアプリケーションをインストールすると、クライアント PC の脆弱面が拡大したり、システムが悪意のあるソフトウェア（マルウェア）に感染することがあるので、ユーザーはアプリケーションを追加できません。

- **クライアントの保全性：** すべてのクライアントは、既知のベースライン構成に基づく一貫した状態で維持されます。サーバーベースのイメージの利用により、一貫性を持って迅速に新しいパッチを適用できます。

- **既知の良好な状態へのロールバック機能：** シンクライアントでは多くの場合、旧バージョンの単一の仮想コンテナーファイルをリブートまたはリロードすることによって実行できます。

セキュリティー管理の価値の軽減

インテル IT 部門では、このようなセキュリティー管理は安全な環境の構築に有効ではあるけれども、最近のゼロデイ攻撃では全面的な防御をできなかったと考えています。

- **集中型データストレージ：** 従来のデータ盗難は、システム上に物理的に格納されたデータをデバイスにコピーすることで行われていました。一方、現在のデータ盗難は通常、図 1 に示すようにネットワーク経由で行われています。シンクライアントがもたらす制限では、これを防止できません。すべてのシンクライアントは高速のネットワークに接続されており、大半はインターネットに接続されています。攻撃者はこの高速ネットワークを利用して、サーバーからファイアウォール外にデータを迅速に転送できます。

- **権限を持たないユーザー：** ユーザーの管理者権限を削除すると、感染の影響を軽減したり、新しいシステムへのマルウェアの拡大を困難にします。ただし、初期段階での攻撃を防げるとは限りません。また、極端に厳しい制限を設けない限り、攻撃者はユーザーの別の権限を利用して、ユーザーがアクセス権を持つほかのシステムやデータにアクセスできます。しかも、悪用されるサービスがユーザープロセスではなくシステムプロセスとして実行される場合は、ユーザーの管理者権限を削除しても、防御効果はありません。

- **ユーザーがインストールできるアプリケーションの制限：** 必須でないアプリケーションが標的となるのであれば、インストールを禁止する制限は効果を発揮します。ただし、最近の攻撃で標的となっているのは、Web ブラウザーのように普遍的かつ必須のアプリケーションです。さらに、ビジネス PC へのソフトウェアのインストールを禁止するよりも、悪意のある Web サイトへのユーザーアクセスを制限したり、有害な Web サービスの実行を防止する方が、はるかに困難です。

- **クライアントの保全性：** 一般に、シンクライアント・モデルで使用されている集中型イメージの方が、一貫性のある最新パッチを容易に適用できます。ただし、ゼロデイ攻撃は従来未知であった脆弱性を標的にするので、この方式では攻撃を防げません。

- **既知の良好な状態へのロールバック機能：** サーバーベースのクライアント・イメージを利用したクライアント・システムのロールバックは、最近の攻撃に対しては無力です。初期段階での攻撃によって Web ベースのサービスやアカウントへのアクセス権を取得されると、攻撃後にシステムをロールバックしても、アクセス権を取り消せません。加えて、攻撃では未知の脆弱性が悪用されるので、システムへの再攻撃が容易です。

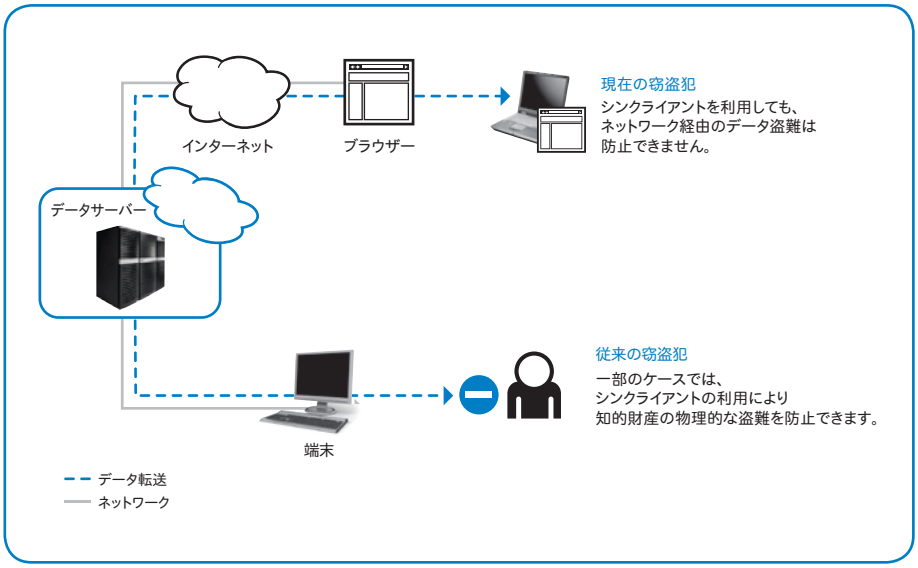

図 1. シンクライアントの場合、クライアントからの物理的なデータ盗難は防げますが、ネットワーク経由の盗難は防げません。

PC におけるセキュリティー管理

インテル IT 部門は、PC であれば、シンクライアント・モデルではあきらめざるを得ない機能を利用しながらも、同等のセキュリティー管理を導入することが可能であると判断し、実際に導入もしています。こうしたセキュリティー管理については、包括的な導入は行わずに、必要に応じて個別に採用してきました。

インテルでは、物理的なデータ盗難の防止に当たり、ディスク全体の暗号化と、エンタープライズ権限管理ツールを採用しています。グローバル・ドメイン・ポリシーや物理的なシステム改修を通じて USB メモリーや外付けストレージデバイスにロック、暗号化、または制限を適用して、これらの手段を強化できます。また、フォルダー・リダイレクションを利用すると、データをデータセンターに格納することが可能で、データセンターのみに保存するか、クライアント上にデータのミラーとして保存するかを選択できます。後者のミラー方式は、モバイル・コンピューティングにも対応しています。

管理者権限をユーザーに割り当てるかどうかの判断は、シンクライアント・モデルに固有のものではありません。ノートブック PC ユーザーの管理者権限を削除するためのツールが数多く用意されています。管理者権限を PC ユーザーに付与する必要がある場合は、サードパーティー製ソフトウェア・パッケージを利用すれば、管理者権限を管理することや、IT 管理者からの個別の許可がない限りユーザーによるアプリケーションのインストールやその他の活動を制限することができます。インテルでは、複数の手段を通じて管理者権限やユーザー権限を制限しています。

共通 OS またはアプリケーション・イメージの集中型管理は、シンクライアント・コンピューティングに固有のものではありません。例えば、クライアント・ホスト型デスクトップ仮想化を利用すると、集中管理型の OS/ アプリケーション・イメージを複数のデスクトップ PC で共有できます。今後期待されている機能としては、ユーザーの PC にダウンロードする集中管理型の仮想化クライアントがあります。また、システム・ロールバックをビジネス PC に導入できるテクノロジーが、複数の企業から提供されています。インテルでは、標準的な集中管理型のシステムおよびアプリケーション・イメージを採用しています。イメージは定期的に更新され、ロールバックの必要が生じたときに使用されています。

インテル IT 部門では現在、必要に応じてパッチを迅速に導入することにより、クライアントの保全性を維持しています。このプロセスで最も時間を要するのは、新しいパッチの導入作業ではなく、パッチのテストと検証です。テストと承認にかかる時間は、シンクライアント環境でも変わりません。PC の場合、パッチをユーザー PC に段階的に導入すれば、パッチに不具合があった場合でも、その影響を軽減できます。すべてのクライアントを同時に更新すること自体、リスクになります。

シンクライアントのセキュリティー課題

シンクライアント・モデルに固有のセキュリティー課題もあります。アプリケーションやデータを集中化することは、脅威の集中化にもつながります。シンクライアントのネットワークには、共有のデータやアプリケーションを格納するサーバーへのアクセスポイントが多数存在し、攻撃の影響が IT インフラストラクチャー全体に及ぶ可能性があります。一部のシンクライアント・モデルの場合、シンクライアントが依存している中央ネットワーク・リソースで障害が発生すると、業務が中断する可能性もあります。

個人データも含めすべてのデータを集中化すると、プライバシー上の新たな問題が生じ、国によっては規制違反になりかねません。シンクライアント・モデルは、データ流出という予期せぬ事態を招くこともあります。例えば、シンクライアント・ユーザーは情報を紙に印刷して、権限のない相手に見せる傾向があります。

セキュリティー侵害への対応に当たり、セキュリティー・スタッフは、侵害が発生したシステムと、侵害が最初に発生した日時を把握しなければなりません。実際、一部のケースでは、そのような証拠の保持が必須となります。サーバーベースのイメージからリブートしてシンクライアント・システムを既知の良好なビルドにロールバックすると、クライアント上の重要な証拠が消滅するというマイナスの結果が生じる場合があります。

高度化する脅威のもとでのセキュリティー

脅威が標的を絞ったゼロデイ攻撃に高度化していくのに応じて、従来とは異なるセキュリティー手法を採用する必要があります。IT セキュリティー・スタッフは、PC であるかシンクライアントであるかを問わず、クライアントが脆弱であることを前提にしなければなりません。

攻撃者は多くの場合、従来の手法では検出や防止が困難なカスタムのマルウェアを使用します。攻撃対象は通常、必須のビジネス・アプリケーション、OS、クラウド・ベース・サービスの一部のように、PC にもシンクライアントにも存在する普遍的な要素です。

検出をするには、検出制御と補正制御をバランスよく組み合わせ、ユーザーのアクセスや権限利用に関する高度な行動分析を行う必要があります。

いずれの制御も、導入を容易にするためにインテル® バーチャライゼーション・テクノロジー、ダイレクト I/O 向けインテル® バーチャライゼーション・テクノロジー、インテル® 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）などの新しいプラットフォーム・テクノロジーが利用できます。または、シンクライアント・モデルが必須とする共有の仮想化サーバーベース環境ではなく、個別の物理ハードウェアを利用しても導入が容易です。

例えば、サーバー上の仮想マシン（VM）内で発生した攻撃が、VM エスケープとして知られる方法で同じサーバー上の別の VM を標的にする場合があります。VM 管理層にはこの種の攻撃を防ぐことのできるネットワーク侵入防止システム（NIPS）やホストベース侵入防止システム（HIPS）と同等の信頼性の高い予

防 / 検出制御は、いまだ存在しません。VM の実行を個別のクライアント・デバイスに分散するか、プラットフォームのテクノロジーを利用してハードウェアを隔離することにより、攻撃のリスクを大幅に低減できます。

インテルの企業ニーズに対応

シンクライアントでは最近のゼロデイ攻撃を防げず、同様のセキュリティー管理は PC にも導入可能であると判断した上で、インテルの現在および将来の企業ニーズにはどのクライアントが最適であるかを分析しました。この分析は、ビジネス要件、テクノロジーの傾向、セキュリティー課題に基づいて行われています。

インテル IT 部門では、ノートブック PC は極めて広範な用途に対応し、大半のインテル従業員のニーズを満たしていると考えています。

ローカルにインストールしたアプリケーションと、ローカルの処理能力の組み合わせにより、ネットワークにアクセス不可能な場所を含め、あらゆる場所で作業できる高い柔軟性を得られます。また、障害発生時でもユーザーは一部のコンピューティング機能を利用できます。ノートブック PC は、演算負荷が高いアプリケーションやリッチメディアに対応し、ビデオや Voice over IP (VoIP) などのコミュニケーション、コラボレーション、トレーニング、リサーチにも適しています。ユーザーは幅広いソフトウェア・アプリケーションを実行可能であり、これにはビジネス・アプリケーションのほか一部の個人的なアプリケーションも含まれます (インテルでは多くの企業同様、企業リソースのこうした利用をある程度認めています)。

インテル IT 部門の戦略の一環として、社内や社外のクラウドから提供されるサービスの拡充があり、現在はアプリケーション・ストリーミングなどの新たな提供モデルを検討しています。ノートブック PC をユーザーに支給した場合、図 2 に示すように、ローカルにインストールした従来型アプリケーションを引き続き使用しながら、新たなモデルを組み合わせて実行できます。

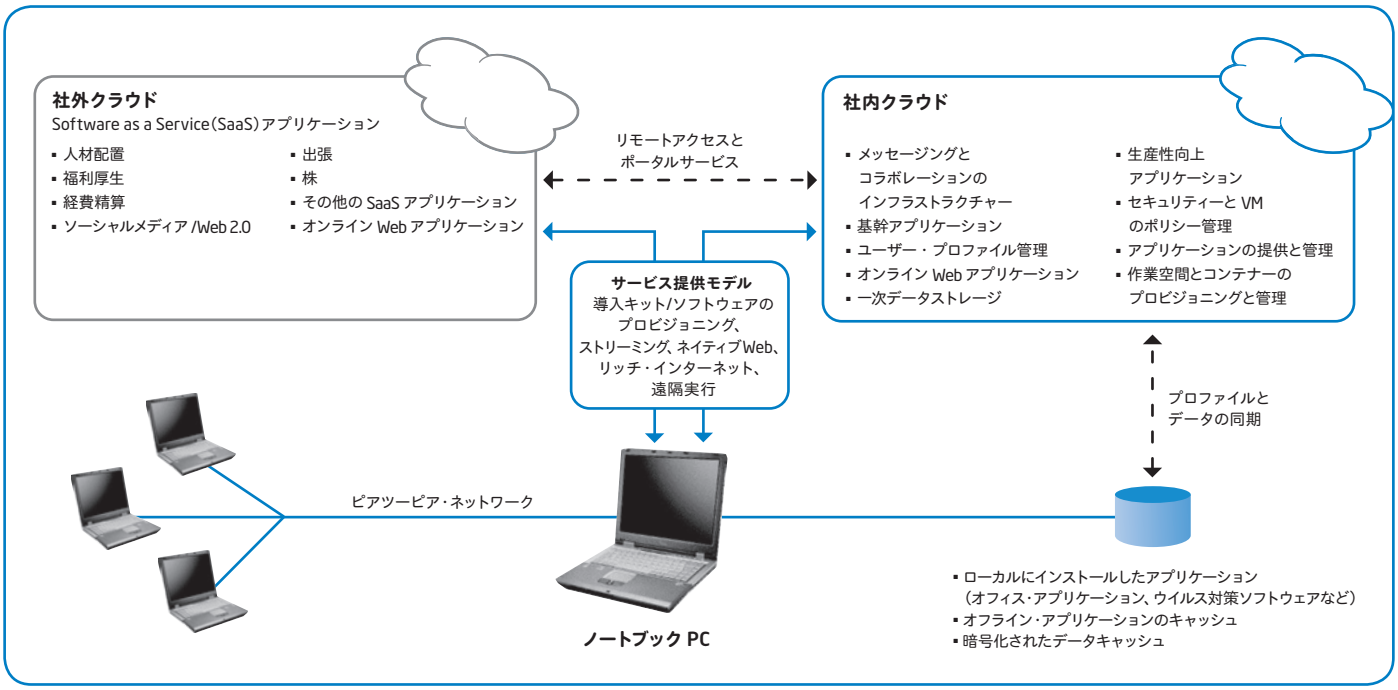

図 2. ノートブック PC では、ローカルにインストールした従来型アプリケーションを引き続き使用しながら、新たなサービス提供モデルをすべてサポートできます。

一方、シンクライアントには大きな制限があります。通常はモバイル・コンピューティングやオフライン作業のサポートが制限され、ユーザーは多くの帯域幅、グラフィックス、演算処理を必要とするアプリケーションを効果的に実行できません。

インテル IT 部門の分析によると、シンクライアントの場合、高いサーバー能力のほか、オンラインユーザーをサポートできる十分なネットワーク帯域幅を確保する必要があります。

こうした制限を踏まえ、シンクライアントはコールセンター端末、共有キオスク、製造用コントローラーのような専用用途にのみ適しているという結論に達しました。ただし分析によれば、このような用途の場合でも、インテル IT 部門はシンクライアントの利用より PC への OS ストリーミングの方が適していると考えます。その理由として、PC はワークロードをローカルで実行し、優れた応答性とユーザー体験を提供するからです。また、サーバーやネットワークに求められる能力も少なくて済みます。

将来の位置付け

今後のクライアント戦略でも、セキュリティー要件への対応、従業員の生産性向上、IT コストの削減が引き続き求められます。それと同時に、ユーザーごとのデバイス数の増加、フォームファクターの多様化、社内でのコンシューマー・テクノロジーの採用といった複雑さに対処しなければなりません。

インテル IT 部門では、新しいテクノロジー、コンピューティング・モデル、サービス提供モデルを活用して、これらの一見相反する要件を満たしていく考えです。現時点では、さまざまな社内ユーザーのニーズに応じて広範なクライアント・ソリューションを提供する分割式アプローチを計画しています。

クライアント・ホスト型デスクトップ仮想化も、検討中のオプションの 1 つです。その他のソリューションの詳細については、本ホワイトペーパー末尾の「詳細情報」を参照してください。

クライアント・ホスト型デスクトップ仮想化

クライアント・ホスト型デスクトップ仮想化は、ネイティブ（タイプ 1）の高セキュリティー・ハイパーバイザーを運用するクライアントにオンデマンドで提供される仮想化 PC 環境であり、インテル IT 部門のクライアント戦略の主要要素となっています。このソリューションを図 3 に示します。

デスクトップ仮想化はデバイスに依存しないモビリティーなど複数の利点をもたらすと、インテル IT 部門は考えています。ユーザーは、仮想コンテナーを各種のクライアント・ハードウェアにダウンロードし、同一システム上のビジネス作業空間と個人作業空間を明確に区別した上で実行できます。

必要な制御をすべて導入できるニッチな専用用途については、OS ストリーミングの利用により、可用性が高く、高度に管理、制御されたデスクトップ PC を提供することを検討しています。PC に対してストリーミングを行い、

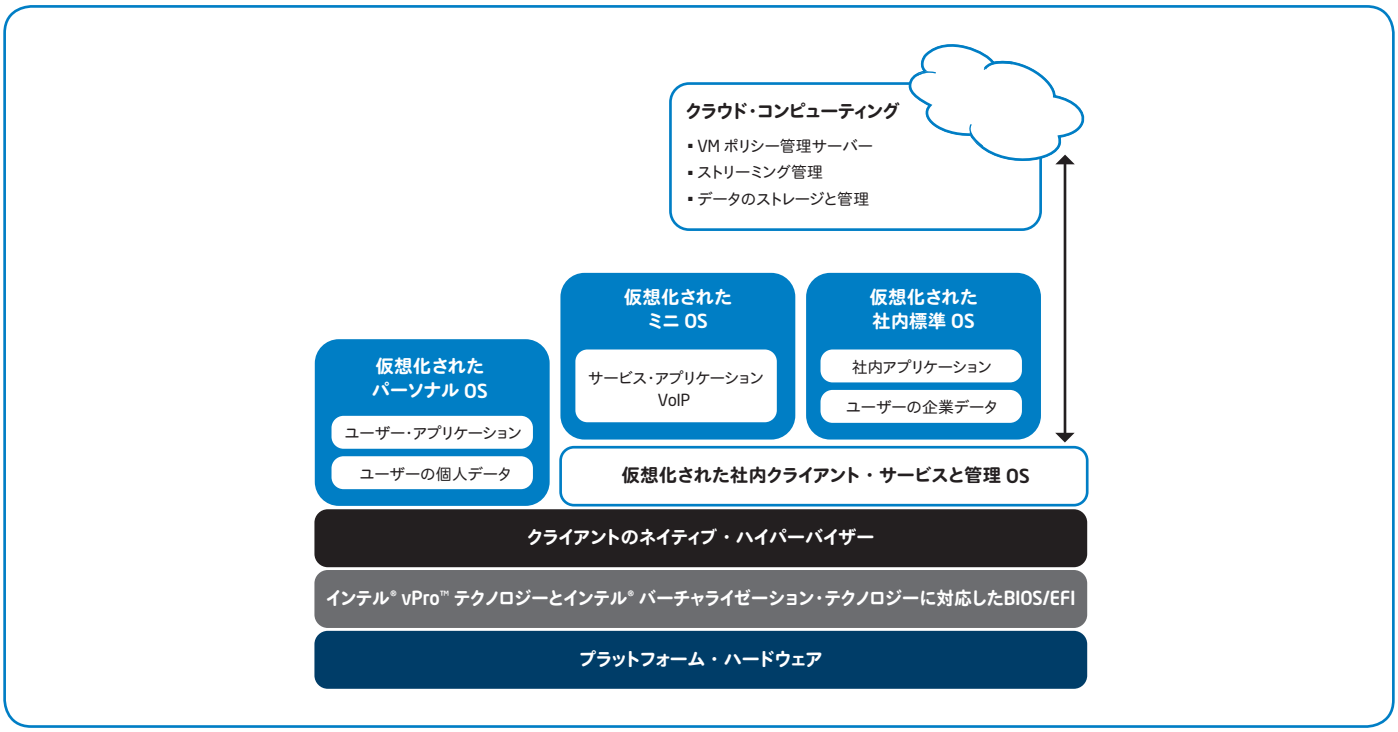

図 3. インテル IT 部門が検討中のクライアント・ホスト型デスクトップ仮想化ソリューション

サーバーベースの OS イメージを多くのデスクトップ PC 間で共有すると、シンクライアントに見られるようなパフォーマンス上の犠牲を被ることなく、集中型管理の利点を得られます。PC の場合は、ワークロードをローカルで実行して、優れたパフォーマンスを提供します。また、サーバーやネットワークに求められる能力も少なくて済みます。

まとめ

インテル IT 部門では、シンクライアントで一般的なセキュリティー管理は安全な環境の構築に有効ではあるが、最近のゼロデイ攻撃を防げなかったと考えています。また、こうしたセキュリティー管理はシンクライアントに固有のものではありません。PC であれば、シンクライアント・モデルではあきらめざるを得ない機能を利用しながらも、同等のセキュリティー管理を導入することが可能であり、また実際にインテル IT 部門では導入もしています。

機能とパフォーマンスのほか企業セキュリティーも考慮に入れた上での判断として、ノートブック PC は極めて広範な用途に対応し、大半のインテル従業員のニーズを満たしています。ノートブック PC は新たなサービス提供モデルやコンピューティング・モデルをすべてサポートできるので、将来に向けた備えが可能です。一方シンクライアントには制限があるので、インテルの環境ではニッチな専用用途にのみ適しています。

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。

- 『Enabling Device-Independent Mobility with Dynamic Virtual Clients』
- 『 クラウド・コンピューティングにはリッチ・クライアント PC』
- 『Developing an Enterprise Client Virtualization Strategy』
- 『Improving Manageability with OS Streaming in Training Rooms』

略 語

HIPS
ホストベース侵入防止システム

NIPS
ネットワーク侵入防止システム

SaaS
Software as a Service

インテル® TXT
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

VM
仮想マシン

VoIP
Voice over IP

表 1. コンピューティング・モデルとデバイスのリスト

用語	定義
アプリケーション・ストリーミング	クライアント OS はローカルにインストールされるが、アプリケーションは要求に応じてサーバーからクライアントにストリーミングされ、そこでローカルに実行される。
クラウド・コンピューティング	通常は、インターネットを介してコンピューティング・リソースやアプリケーションにアクセスすることを指す。このモデルでは、ソフトウェアは Web サーバーから配信され、データもサーバー上に置かれることがある。
クライアント・ホスト型デスクトップ仮想化	IT 部門が、OS またはアプリケーション、あるいはその両方を含む仮想イメージまたはコンテナを作成し、管理する。ただし、サーバーホスト型デスクトップ仮想化のようにサーバー上で仮想イメージを運用するのではなく、コンテナがクライアントにストリーミングされ、ローカルで実行される。
ハンドヘルド機器	スマートフォンや携帯情報端末（PDA）など、ポケットサイズのコンピューティング機器。
ノートブック PC	強力な機能セットを持ち、管理されたセキュリティーをサポートする、高度なノートブック PC。
ネットブック	一般的なコンピューティングや Web ベースのアプリケーションと電子メールの利用に適した、低価格の小型軽量ノートブック PC。一般的に、ユーザーのノートブック PC を補完するコンパニオン・デバイスとして使用される。
OS ストリーミング	OS イメージがネットワークを介してクライアントにストリーミングされ、クライアントの CPU とグラフィックスを使用してローカルに実行される。アプリケーション・データはデータセンターに格納される。クライアントには、OS のキャッシュに RAM を使用する、ハードディスク・ドライブ（HDD）非搭載の PC を使用できる。
ターミナルサービス	クライアントを単なるディスプレイおよび入力デバイスとして使用する、サーバーベースのコンピューティング・モデル。すべての処理はサーバー上で実行され、すべてのデータはデータセンターに格納される。
シンクライアント・ソリューション	他のコンピューター・リソースに依存することで従来のコンピューターの役割を実行するコンピューターまたはコンピューター・プログラム。コンピューティング・リソースまたはストレージリソース、あるいはその両方がかなり制限される。シンクライアント・ソリューションの例には、サーバーホスト型デスクトップ仮想化やターミナルサービスがある。
サーバーホスト型デスクトップ仮想化	ターミナルサービスと同じように、すべての処理とストレージは集中化され、ディスプレイはネットワークを介してクライアントにプッシュされる。ターミナルサービスとの主な相違点として、サーバーホスト型デスクトップ仮想化は、ユーザー各自の完全な仮想マシン（VM）と、OS、アプリケーション、設定を含むカスタマイズされたデスクトップをユーザーに提供できる。

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/

2010 年 9 月

322970-001JA
JPN/1009/PDF/SE/IT/NT