SOPHOS

Windows Vista:
ビジネス環境での安全性

マイクロソフト社がWindows XP® のリリースから5年を経てリリースするWindows Vista™の大きな特徴のひとつに、脆弱性を削減し、マルウェア（悪意のあるソフトウェア）などの脅威を阻止するセキュリティ機能があげられます。新規のセキュリティ機能が数多く導入され、安全性の強化が図られています。この文書では、Windows Vistaのセキュリティ機能をビジネスユーザーの観点から分析します。

A Sophos white paper

2007年1月

Windows Vista: ビジネス環境での安全性

概要

マイクロソフト社の最新OSであるWindows Vistaには、ユーザーインターフェースからOSのコア部分に至るまで幅広く新規の機能が導入されています。しかし、Windows XPに比較してVistaで最も重要視されたのはセキュリティ関連機能の充実です。Vistaでのセキュリティ機能の強化にはセキュリティステータスの監視とレポート、攻撃を呼び込む脆弱性の削減、スパイウェアへの防御、OSカーネルに変更を加える悪意のあるプログラムを阻止するメカニズム、ブラウザやファイアウォール機能の強化などがあります。

> 当社のWindowsの次期バージョン[Vista]への投資を見ていただけば、セキュリティ分野に費やした時間が突出していることがおわかりいただけるでしょう。マイクロソフトはこの分野で大きな責任を果たします。
>
> Bill Gates氏　RSA Conference 2006（米カリフォルニア州サンノゼ）

Windows Security Center

Windows Security Center（WSC）はシステムのバックグラウンドで動作し、コンピュータ上のセキュリティソフトのステータスを監視、レポートします。Windows XP SP 2で最初にリリースされ、Vistaではその他のセキュリティ機能やサードパーティ製のセキュリティソフトとの連携性が強化されています。

Windows XPでは、WSCはファイアウォールの監視、アンチウイルスソフトの自動アップデートのステータスのチェックのみがサポートされていましたが、Vistaではアンチスパイウェアアプリケーションの監視もサポートされています。Internet Explorer 7のセキュリティ設定の監視機能とユーザーアカウント制御機能もサポートされています。

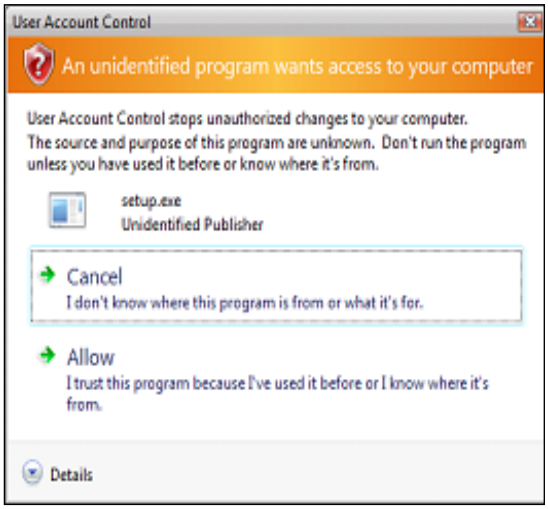
WSC強化の背景には、エンドユーザーへの警告を明示的に表示することによってセキュリティに対するユーザーの意識を高める意図があります。これはホームユーザー向けには非常に好ましい機能ですが、企業や組織（教育機関、政府機関などを含みます。）においてはわずらわしく不適当な機能として警告表示が無効にされてしまう可能性があります。

セキュリティベンダーの一部には、WSCと同等の機能を持つ自社の製品をインストールした際にWSCが自動的に無効化されないことについて否定的な見解を示しているベンダーもありますが、ソフォスではOSにビルトインの集中レポート機能について他ベンダーがコメントすべき立場にはないというスタンスをとっています。

ユーザーアクセス制御（UAC）

ユーザーアカウント制御（UAC: User Account Control）はWindows Vistaで最も重要なセキュリティ機能のひとつです。攻撃の危険性を最小限に抑え、エンドユーザーに与えられたローカル管理者権限の範囲でマルウェアのインストールを阻止するものです。Windows XPでは、デフォルトで管理者権限が与えられていましたが、Vistaではアカウ

ントに「StandardUser（スタンダードユーザー）」「Administrator（管理者）」の2種類のセキュリティトークンが生成されます。デフォルトでは、アプリケーションにはスタンダードユーザーの権限が与えられ、エンドユーザーが関与しなくてもアプリケーションを実行させることができます。しかし、実行に管理者権限が必要なアプリケーションでは管理者トークンが必要となり、プログラムの実行を許可するかあるいはキャンセルするかを明示的に選択しないと実行することができません。



VistaのUAC: セキュリティレベルを強化

> マイクロソフトはUACを導入するにあたって、パフォーマンスとセキュリティのトレードオフという重大な課題に直面し、決断に迫られました。現時点ではこの機能を完全に無効化する人は多いかもしれませんが、それは大変危険です。
>
> Ed Bott氏　Microsoft Report[1]

UACによってレジストリとファイルシステムへのアクセスがデフォルトで厳格化されることは、セキュリティ面においては大きな進歩といえます。この機能により、自身をWindowsシステムフォルダなどに自動的にコピーしたりレジストリキーを書き換えるマルウェアを阻止することができます。また、スタンダードユーザー権限を使うことで、メモリ中の他のプロセスを書き換えるマルウェア（パーソナル/クライアントファイアウォールを回避する手口として用いられます）を阻止することもできます。

しかし、UACではエンドユーザーに対して頻繁に警告が発せられるため、技術的な知識が十分でない詳しくないユーザーにとってはわずらわしいものとなります。危険なのは、エンドユーザーが、警告が表示された際に必要性をよく考慮せずに機械的に「許可」を選んでしまうことです。あるいはUAC機能自体を無効にしてしまうケースも考えられます（実際に、ベータ版をテストした人の中にも、UACを無効にした人はたくさんいます）。

Windows Defender

Windows DefenderはWindows Vistaにビルトインされたアンチスパイウェアのプログラムです。スパイウェアその他不要なプログラムを検知し削除します。このソフトはマイクロソフトの自動アップデート機能でアップデートされ、ソフト内で定義された脅威を検知、削除します。

しかし、Windows DefenderはWindows XP SP2以降、またはWindows Server 2003 SP1以降のみをサポートし、Windows 95/98/Me/2000などは対象となっていません。また、コンシューマをターゲットにしているため、マルチプラットフォーム環境のネットワークに対応する集中管理機能が提供されていません。

カーネルプロテクション

OSカーネルには、Kernel Patch Protection（KPP、またはPatchGuard）と、コード署名テクノロジを利用したドライバ署名管理機能が導入されています。

KPPは、64-Bit対応のVistaに組み込まれている機能で、OSカーネルに悪質なプログラムを書き込んでセキュリティに深刻な脆弱性をもたらし、システムの安定性、信頼性、パフォーマンスなどを損なうマルウェアを阻止します。ボットやスパイウェアなど、マルウェアや業務上不要と思われるソフトの実行を隠す『ルートキット』などがありますが、KPPはカーネルが不正に拡張されたり置き換えられたりするのを防ぎます。

KPPは32-bit対応のVistaでは導入されていません。セキュリティソフトを含む多くのプログラムのカーネルスペースの利用方法が必ずしも明らかではなく、KPPが導入されると既存アプリケーションとの互換性が損なわれる可能性があるためです。そのため、32-bit版ではルートキットによる攻撃に対する脆弱性が残っているといえます。しかし、この問題はコード署名テクノロジによって回避できます。

VistaのKPP機能によって自社のソフトウェアが「ロックアウトされてしまう」との懸念を表明しているセキュリティベンダーもありましたが、これは64-bit版においてカーネル使用の仕様を変更する必要があったからです。

マイクロソフト社がカーネルインターフェースを強化したことにより、すべてのセキュリティベンダーで対応が必要となった経緯がありますが、この機能強化によるメリットは対応の煩雑さのデメリットをはるかに上回ります。マイクロソフト社のテクノロジは、高いセキュリティ機能を備えている場合であっても、マルウェア作成者の攻撃の対象になりやすく、集中的に研究されて新規のマルウェアが作成される可能性が非常に高いという一面はありますが、いずれにしてもKPP機能を備えたWindows Vistaは、ユーザーにとって非常に有用であり、セキュリティベンダーもその功績を高く評価すべきです。

Internet Explorer 7

Windows Vistaでは、ビルトインのWebブラウザ、Internet Explorer 7（IE7）が提供されています。IE7には、フィッシングやスプーフィング攻撃などからコンピュータを保護する機能強化が含まれています。IE7の保護モードを選択すると、悪意のあるWebサイトやマルウェアによるデータや設定の削除や変更ができないように保護されます。

この機能は、Windows Integrity Controlと呼ばれる新しいメカニズムによって実現されたもので、あらゆるプロセスに保全レベルを割り当て、各レベルでシステムオブジェクト（レジストリ、ファイルシステム、その他のプロセスなど）へのアクセスを制限します。

セキュリティレベル	定義
低	Untrusted（信頼されない）
中	一般的なユーザープロセス デフォルト値
システム	システムへの無制限のアクセス
高	ファイルのインストールが可能 管理者権限のあるプロセス

Windows Integrity Controlが提供する
4つのセキュリティレベル

保護モードでは、IEは「低セキュリティ」レベルで実行されます。これは通常のユーザープロセスよりも低いレベルです。信頼されたゾーン以外ではダウンロードされたプログラムは低セキュリティレベルを引き継ぎ、それよりも高いセキュリティレベルの環境では実行できないため、システムとブラウザの連携によって悪意のあるプログラムやPUA（業務上不要と思われるアプリケーション: Potentially Unwanted Program）の実行が阻止されます。

IE7ではフィッシングフィルターも提供されており、機密情報を盗むフィッシングサイトにアクセスしたと思われる場合には警告を表示してユーザーの安全を守ります。フィルターはWebサイトのコンテンツを分析してフィッシング技術の特性を備えていないかを確認し、グローバルで提供されているデータを参照して、アクセスしようとしているWebサイトが信頼できるかどうかを判定します。

マイクロソフト社のプライバシーポリシーと、同社に情報が提供されることについてはさまざまな議論があり、抵抗感を持つ人も存在しますが、マイクロソフト社は、フィッシングフィルターが個人を特定できる情報を送付することはない、と言明しています。しかし、実際、広告主に対して『豊富なWeb統計情報』[2]の提供を謳っているMSNが、同時にIP&URLデータベースを管理しているという事実も一方で興味をひきます。

Windows Firewall

Windows Vistaには新規のファイアウォールが含まれています。これはWindows XP SP2のファイアウォールを改良したもので、アプリケーションレベルの送信フィルタリングにネットワークロケーションのプロフィールを含むように変更されているため、ユーザーがロケーションごとに個別のルールを適用することができます。

しかし、ファイアウォールのデフォルトの設定はXP

Windows Vistaをより安全に活用するためのチェックリスト

Windows Vistaは従来のWindows OSに比較して非常にセキュアなOSです。一般にOSの移行にあたってその安定性や品質を考慮して長期間のテストや検証期間を設ける組織は多いと思われますが、Windows Vistaについては、その優れたセキュリティ機能を導入してビジネスの安全性を高めるため、できるだけ早い時期に移行することをお勧めします。以下に、Windows Vistaをより安全に活用するためのチェックリストを記します。

1. Sophos Anti-Virusなど、アンチウイルスソフトをインストールして既知、亜種、新種のマルウエアを阻止しましょう。
2. Windows Vistaの最新のパッチが自動的にアップデートされるように設定して、脆弱性を修正しましょう。最低限、深刻なセキュリティパッチは必ず適用しましょう。
3. より高度なセキュリティを必要とするシステムにはWindows Vista 64-bit版を採用し、カーネルパッチプロテクション機能でマルウェアを阻止しましょう。
4. 使用中のセキュリティ対策ソフト、特に特にHIPS（ホスト侵入防止システム）機能がWindows Vista 64-bit版をサポートするかを確認しましょう。
5. エンドユーザーがUAC(ユーザーアカウント制御)機能の利点を十分に利点を理解して使用できるよう、トレーニングを実施しましょう。
6. リモート接続のユーザー環境では、WSC（Windows Security Center）を活用しましょう。ただし、ネットワーク中のコンピュータの集中管理機能を持つセキュリティソフトを使用している場合はWSCの通知機能をオフにするなど、最適な使用法を検討しましょう。
7. Vistaに対応し組織内のすべてのエンドポイントに対してポリシーの設定・施行、最新の対策の迅速な適用などを集中管理できるソリューションを導入しましょう。ソフォスのエンドポイントセキュリティは、Vista（32-bit/64-bit）に対応します。

SP2と同等で、デフォルトポリシーではすべての送信トラフィックを許可するという問題点もあります。

加えて、グループポリシーによる管理が可能にもかかわらず、エンタープライズ全体を集中管理する可視的な監視ツール、ポリシー設定機能がなく、集中コンソールからエンタープライズレベルのセキュリティ管理を実行する機能が提供されていない点も課題です。

その他のセキュリティ機能

その他、Windows VistaにはWi-Fiセキュリティ、マルチファクターのオーセンティケーション（認証）、BitLockerデータプロテクション、NAP（ネットワークアクセスプロテクション）クライアント、オーディット機能の強化などが含まれています。

Windows Vistaで は、WPA2（Wi-Fi Protected Access 2）プロトコルをサポートしており、デフォルト設定ではワイアレスネットワークはより安全です。

また、スマートカードやその他のシステム（バイオメトリック（生体認証）によるWindowsオーセンティケーションなど）へのAPIを提供し、ハッカーやパスワードクラッキング、ソーシャルエンジニアリング手法などによる不正な侵入を阻止します。

暗号化機能の強化により、組織の知的財産の窃取や喪失が防御されます。Window Vistaは、たとえば従業員の所属するグループによって特定のドキュメント、ファイル、ディレクトリ、マシンなどへのアクセスを制御し、情報漏えいを防ぎます。暗号キーはスマートカード上に保管することはできません。BitLockerディスク暗号システムによって、リムーバブルディスクからのブートなどの手段によるハッキングも防御します。

NAPクライアントは、悪意のある侵入や保護されていないコンピュータからのネットワークへのアクセスを阻止します。なお、この機能に必要なサーバーコンポーネントはWindows Serverの次期バージョン（コード名Longhorn: 2007年中にリリース予定）で提供される予定です。

その他、Windows Vistaは、コンプライアンスに対応する機能として、リソースへのより厳密なモニタリングおよびログアクセス機能を提供します。たとえば、機密性のあるデータへの未承認のユーザーによるアクセスを特定することなどが可能となります。

まとめ

マイクロソフト社はWindows Vistaのセキュリティ機能開発に多大なリソースを費やしました。その結果、Windows Vistaには多くの有用なセキュリティ機能が導入され、特にホームユーザーの安全性は非常に高まっています。しかし、どんなに多くのマルウェア対策機能が提供されていても、『絶対的に安全なOS』というものは存在せず、常に新しいマルウェア発生の危険があります。Windows Vistaのセキュリティ機能にもかかわらず、リリース後、Vistaを標的にしたマルウェアは必ず出現することでしょう。重要な機密情報を扱うビジネスユーザーに対応するため、マイクロソフト社には今後もマルウェア対策の技術の向上、サポートサービスの提供、OSのパッチ提供、集中管理機能の提供などが求められます。

◆

ソフォスの脅威対策ソリューション

Sophos Anti-Virus for Windows 2000/XP/2003/Vistaは、Windows Vista 32-bit/64-bitに対応し、Behavioral Genotype Protection（振る舞い検出型遺伝子脅威検知技術）によって新種のマルウェアや亜種を高精度に検知、阻止します。

出展

1 blogs.zdnet.com/Bott/

2「Microsoft's Vista won't stop the Windows security aftermarket」 Yankee Group Research, Inc. 2006年5月

ソフォスについて

ソフォスは法人向けに統合脅威管理ソリューションを提供する世界的なリーディングカンパニーです。グローバル企業、SMB市場、教育機関、政府機関、金融業、製造業など、あらゆる規模、分野の組織をセキュリティ脅威から保護し、世界150カ国以上で3,500万人以上のお客様にご導入いただいております。セキュリティ分野で20年以上におよぶ実績と経験をベースに、ソフォスのセキュリティ解析センターが、ウイルス/スパムなどを組み合わせた複雑な脅威に迅速に対応し、常時最新の対策をご提供します。その高品質な技術力とサービスは多くのお客様から高い評価をいただいております。

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

ソフォス株式会社

〒231-0062 神奈川県横浜市中区桜木町1-1-8 日石横浜ビル15F
Tel. 045-227-1800 Fax. 045-227-1818 Email. sales@sophos.co.jp

SOPHOS
WWW.SOPHOS.CO.JP