

German
Data
Security



G Data

Whitepaper 2009

Windows7のシステムセキュリティ

G Dataセキュリティラボ

マークアウレル・エスター & ラルフ・ベンツミュラー

(岸本眞輔・瀧本往人 訳)



目次

1	待ち望まれた後継 OS、Windows 7	3
2	ユーザーアカウント制御(UAC)	4
3	ファイアウォール	11
4	ファイル名拡張子	12
5	AppLocker	13
6	Windows Defender	22
7	BitLocker	24
8	BitLocker to go	25
9	結論	28

1. 待ち望まれた後継OS、Windows 7

Windows 7は、多くの企業ユーザーがその導入を躊躇したWindows Vistaの後継OSとして、2009年10月22日にリリースされました。周知のとおり、Windows Vistaは、多くのユーザーからの不満や批判に晒されました。Windows XPと比較すると、普及度やユーザー評価の観点から見て、必ずしも成功したとは言えませんでした。調査会社によるWindows 7発売前のOSシェア調査結果を見ても、Windows XPは58%、Windows Vistaは約30%でした。一世代前のモデルであるWindows XPに、シェアでこのような差がついたのは、Microsoftにとっても本望ではなかったでしょう。

さて、ユーザーも待ちわびたWindows 7とは、どのようなOSなのでしょう。

リソースへの負荷軽減、操作性の向上、セキュリティ改善、6種類もの製品エディション、Windows 7と同時に発表された次世代グラフィックAPI(DirectX-11)などがWindows 7の特長と言えるでしょう。しかし一番の改善点は、Windows Vistaでユーザーから不満に挙げられていた快適性の向上です。また一方、セキュリティについても、Windows 7ではこれまでのOSより堅牢なセキュリティを実現していると言われています。

それでは、Windows 7に導入された新セキュリティ機能や変更点について解説しながら、保護メカニズムの実効性を検証してみましょう。

2. ユーザーアカウント制御(UAC)

安全性と快適性の両立は、ソフト開発メーカーにとって常なる課題ですが、この両者を同時に実現するのは簡単ではありません。通常、両者はトレードオフの関係にあると言えます。その最も良い例が、Windows Vistaのユーザーアカウント制御(以下、UACと表記)でしょう。

UACが表示させるダイアログについては、よく知られているように、その煩雑性から多くのユーザーから批判が挙がりました。多くのユーザーは、UACを手動でオフにしてこの問題に対処しました。Vistaで新たに実装された新機能が無効化され、実質的には意味を為さなくなったのです。

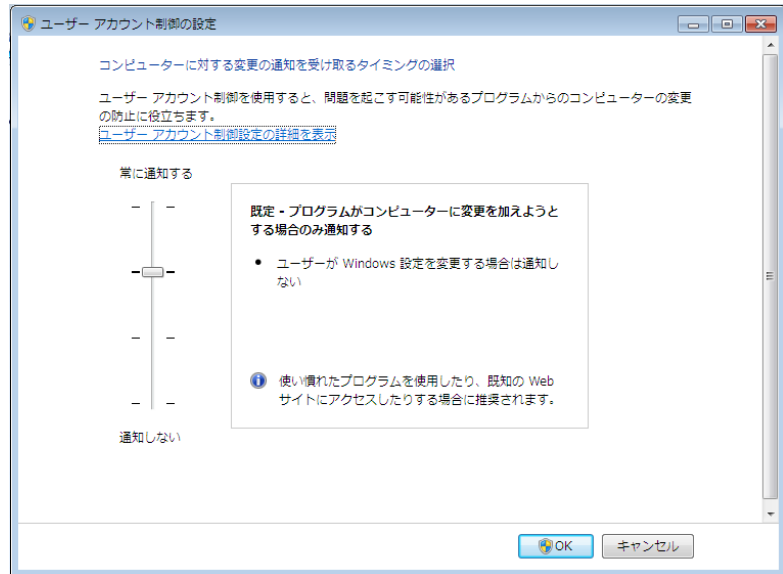
これを受けて、MicrosoftがWindows 7で講じた対策は、UAC警告表示を4段階のレベルに分けて管理するというやり方です。設定は次の4段階から選択することができるようになりました。

1. 常に通知する：プログラムやユーザーがシステムに変更を加える場合

2. プログラムがコンピュータに変更を加えようとする場合のみ通知する

3. プログラムがコンピュータに変更を加えようとする場合のみ通知する（デスクトップを暗転しない）

4. 通知しない



この設定により、UAC警告表示の設定変更自体は容易に操作できるようになりました。しかしこれは、ユーザー側の利便性向上を意図して採用された機能と思われるのですが、セキュリティの向上や改善と言える種類のものではありません。

また、UACを有効に設定しただけでは、とうてい安心な状態になったとは言えません。すでにWindows 7のベータ版の段階で、UAC解除に成功した攻撃も報告されています。

チェックされないタスク

常時監視にもかかわらず、WindowsにはUACの監視外にある自動化部分がわずかですが存在します。

スケジュール管理プログラム経由であれば、UACのダイアログを表示しなくとも、システム起動時に管理者権限から起動できます。

Windows 7における権限の管理は、簡単操作でユーザーが増加中のUNIXやMac OS Xのコンセプトに触発されて開発されたのがうかがい知れますが、対価としての安全性の犠牲は明らかです。UACの設定を低くしてしまうと、マルウェアも無警告で許可され、システム上で実行されることとなります。快適性の追求がセキュリティの足を引っ張っているのは明らかです。

3. ファイアウォール

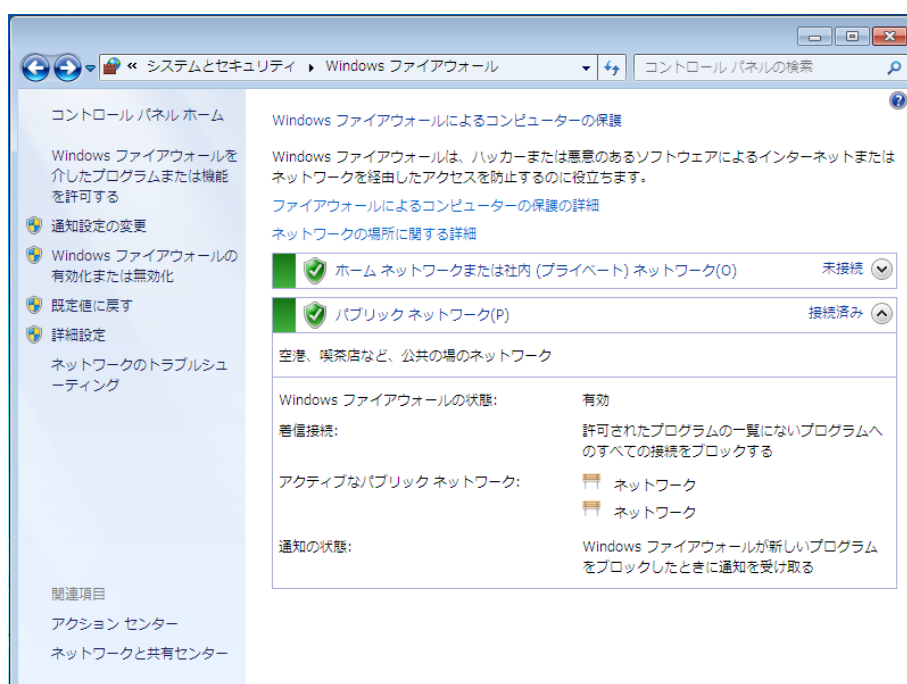
Microsoftは、これまでのOSにおけるWindowsファイアウォールに対するユーザーからの不満の声を汲み、それをWindows 7で反映させ、操作性を向上させているようです。特定のアプリケーションに対する自動でのルール作成、規則ウィザードによるルール管理で、簡単な操作を実現しています。更に、コンピュータの使用環境に応じて、設定の変更ができます。また、公共の場のネットワークで社内ネットワークより強固なルールでコンピュータを保護できます。さらに、ネットワークカード毎に異なるプロファイルを割り当てができるようになっています。

では、実際の操作感はどうでしょうか。ルール作成やルール移行などのユーザビリティについては、それほど高いとは言えないのではないのでしょうか。

Windows 7におけるUACは、大多数の一般ユーザーにとっては、複雑で混乱を招きかねず、誤設定や誤操作に導く可能性も十分に考えられ

ます。一回の誤クリックで、インターネットに接続できなくなったり、ネットワーク内のプリンタを利用できなく恐れがあります。したがって初心者のユーザーには、ファイアウォールの操作に対して確認作業を任せるのは、最善の解決策ではないでしょう。もちろん、ユーザーのコンピュータ知識によりますが、初心者レベルのユーザーが安心して利用できる自動処理型のファイアウォールを搭載すべきではないのでしょうか。

また、以前と変わらず、ファイアウォールの完全無効化も可能です（マルウェアによる無効化の恐れもあります）。通常のセキュリティ製品に搭載されるファイアウォールの自動保護は、Windows ファイアウォールは未搭載です。市販のセキュリティ製品のファイアウォールと比較すると、一歩劣っている感じが拭いきれません。



4. ファイル名拡張子

ファイル名拡張子は、Windows 9xの時代からセキュリティ専門家が、その悪用の危険性を繰り返し指摘してきた問題ですが、Microsoftは、Windows 7でもこれまでの姿勢を崩さず、既知のデータタイプの拡張子は表示させていません。

相変わらずWindows 7のデフォルト設定では、アイコンとファイル名のみが表示され、「.exe」「.scr」「.doc」などのファイル拡張子は表示されません。つまり、攻撃者は適当なアイコンを使って、実行可能なファイルを偽装できるのです。実行可能なファイルが下の図のように、PDFのアイコンで偽装されていたとすると、ひと目見ただけでは単なるPDFファイルと思い込みクリックして感染する恐れがあります。

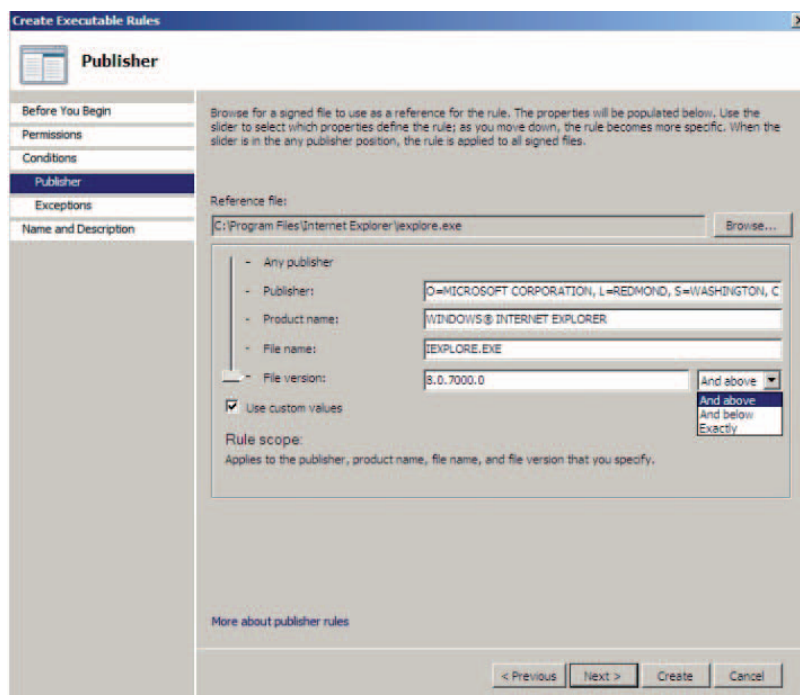


Windows 7でも、UACのダイアログ表示でユーザーを混乱に導くでなく、犯罪者に悪用されるとわかっている手口は放置せずに早急に改善されるべきでしょう。

5. AppLocker

AppLockerは、企業ネットワーク内などでユーザー側での実行を許可するアプリケーションを指定し制御する機能です。この機能自体は、Windows XPやWindows Vistaのソフトウェア制御ポリシー(Software Restriction Policy)でも可能でしたが、企業での導入率は低く、ユーザーに受け入れられたとは到底言えないものでした。これを受け、Windowsはルールの改良を迅速かつ集中的に行ったようです。更新の度に新たなハッシュ値を生成し、これをキーにしてアプリケーションを区分します。アプリケーションのデジタル署名に基づいてアプリケーションを制御する発行元ルールでは、発行元、製品名、ファイル名、ファイルのバージョンに基づき、特定のアプリケーションだけをブロックすることも可能です。

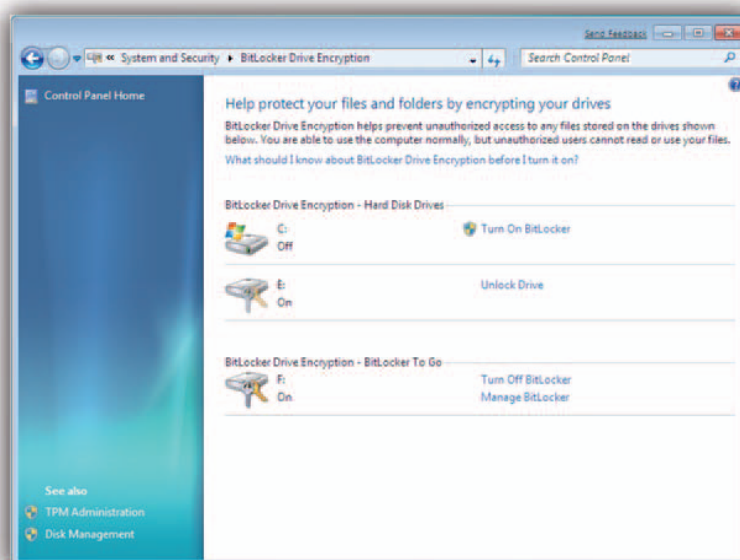
AppLockerは、マルウェアに対する効果的な対策といえるでしょう。発行元ルールによってユーザー側の制御操作も楽になっています。しかしながら、一方で証明書もキャンセルできるため、保護作用も一時的なものになってしまう恐れもあります。



6. Windows Defender

Windows Defenderは、Windows Vista後、確固たるWindowsの構成要素となった、アンチスパイウェア機能です。

しかし、スパイウェア機能の比較テストでは、Windows Defenderの結果は思わしくありません。数ヶ月前の比較テストの結果では、インストール済みのスパイウェアは20%程度のみを検出するにすぎませんでした。また、スパイウェアをインストールするウェブサイトの検出も37.5%にとどまりました。これは、Windows Defenderが、ハッシュベースの検出方法を採用し、URLフィルタを実装していないためです。これは、Windows Defenderにとって大きな弱みです。



MicrosoftはWindows Defenderだけで完全にウイルス対策ができるは考えていません。Windowsが危険と判断するWindowsの脅威とスパイウェアを対象としています。このことをWindowsユーザーは把握した上で、利用すべきでしょう。

7. BitLocker

情報を暗号化して保護することは、ますます重要になってきています。

Microsoftは、Windows VistaからBitLockerを搭載しました。

Windows 7でも同じ機能が搭載されていますが、Windows Vistaでは、後々にBitLockerを利用する場合に、システムパーティションを縮小しなければならないという問題がありました。Microsoftは、後にBitLockerの操作を容易にするBitLocker ドライブ準備ツールを提供しました。

BitLockerは、Windows 7においては、Ultimate EditionとEnterprise Editionでのみ利用できます。

Windows 7では、インストール時に、200MB (Windows Recovery Environmentがインストールされている場合は、400MB) のBitLockerパーティションを作成します。BitLockerは、標準ではコンピュータに搭載されるTPMを利用して管理します。コンピュータにTPMチップが搭載されていない場合は、暗号化キーをUSBメモリへ保存させることもできます。なお、USBメモリを利用する場合は、コンピュータの起動時に、USBメモリをコンピュータに接続する必要があります。

BitLockerは、オープンソースのTrue Cryptと比べると多少面倒なところはあるものの、復号キーをActive Directoryに保存することができる興味深いオプションであることは疑う余地もありません。万が一、ユーザーがパスワードを忘れたり、USBメモリを紛失した場合は、アドミニストレーターがファイルへアクセスする事ができる解決策も提供されています。この機能が悪用される可能性は、Active Directoryの保護と相関関係にあります。

8. BitLocker to go

BitLocker to goは、Windows 7から搭載された新機能です。BitLocker to goでは、USBメモリやSDカードなどのリムーバブルディスクの暗号化に対応し、パスワードやスマートカードで暗号化を簡単に解除できます。また、通常のBitLocker同様に、Active Directoryでパスワードを忘れたときに必要な復元用の復号キーを共有フォルダで管理保存できます。加えてActive Directoryと連携させて、ユーザーに強制的にBitLocker to goを使用させることもできます。また、BitLocker to goで暗号化されたデータは、Windows XPやWindows Vista下でも読み込めますが、パスワード入力後にハードディスクにデータをコピーする必要があります。リムーバブルメディアへの書き込みはできません。

セキュリティの観点からは、暗号化されていない可能性のあるハードディスクへデータをコピーすることは、好ましいとは言えないでしょう。

9. 結論

Windows 7はどれだけの安全性を確保したのでしょうか。また、Windows 7には、従来のセキュリティ製品は必要ないのでしょうか。

Windowsは、Windows Vistaに数多くの新セキュリティ機能を開発し、それらを搭載しました。しかし、Vistaに搭載された機能は、大部分が企業ユーザーに向けて開発された機能です。コンシューマー向けの部分はおまけ程度にすぎません。BitLocker、BitLocker to go、さらにAppLockerは、UltimateやEnterprise Editionにしか搭載されていません。一般ユーザーに提供されるセキュリティは、Windows Vistaで確立したセキュリティのマイナーチェンジ版の提供と言えます。セキュリティ技術を扱いやすくしたに過ぎないのです。

UACは4段階の設定を用意した事で初心者ユーザーの誤操作発生の要因となる可能性がある

ファイル拡張子が未表示、犯罪者に細工や悪用される可能性がある

Windows Defenderだけで適切な保護が提供されているようにユーザーを錯覚させている

Windows 7には、新たな保護機能が実装されました。しかし、Windows Vistaで導入された機能ほど大幅な変更はありません。

多くの保護機能ではすり抜けが可能です。また、現在破ることができない機能においても、マルウェア作者がWindows 7の保護システムを破る攻撃方法を生み出すのは、時間の問題でしょう。

昨今のマルウェアの増加比率やWindows 搭載のフィーチャーの質を考慮すると、Windows OSだけで、様々なマルウェアからコンピュータを適切に保護することは困難です。コンピュータを適切に保護するには、信頼のおけるセキュリティソフトをインストールし、更新やウイルススキャンを定期的に行うことで、保護することが重要です。

付表：Windows 7の6バージョンによって提供されるプロテクション

機能	用途	Starter	Home Basic	Home Premium	Professional	Enterprise	Ultimate
EFS	ファイル暗号化						
AppLocker	アプリケーション動作制御						
Bitlocker	ドライブ暗号化						
BitLocker to go	リムーバブルメディア暗号化						
UAC	ユーザーアカウント制御						
Windows Defender	スパイウェア監視						
Windows Firewall	不正アクセス防止						
DEP	バッファ オーバーラン攻撃阻止						