# Windows 7
# セキュリティ機能評価報告書

## 要約版

2009/8/31

**Fourteenforty Research Institute, Inc.**
株式会社フォティーンフォティ技術研究所

# 1. 概要

この文書では、Windows 7、Internet Explorer 8(以下 IE)、Microsoft Office Isolated Conversion Environment(以下 MOICE)のセキュリティ機能について評価し、レポートする。

本調査では、当初既存のマルウェアがどの程度 Windows 7 上で動作するかを調査する予定であったが、典型的なマルウェアを Windows 7 上で稼働させたところ、正しく動作しなかった事から、典型的なマルウェアのデータ構造や挙動を再現することにより、Windows 7 のセキュリティ機能の有効性の検証を行った。検証で得た考察は以下の通りである。

1. **Windows 7 のセキュリティ機能の有効性は高い**

Windows 7 のセキュリティ機能の有効性は高く、Windows 7 上で安定して動作する既存のマルウェアは、少ないものと考えられる。

また、AppLocker による実行プログラムの制限は有効性が高く、利用を検討すべきである。

2. **Windows 7 においても、ウィルス対策ソフトウェアの利用が不可欠である**

Windows 7 においても、マルウェアの動作を阻止しきれない可能性があることから、アンチウイルスソフトでカバーする必要がある。このような観点から、マイクロソフトが無償のウィルス対策ソフトウェア(MSE: Microsoft Security Essentials)を提供する意義は大きい。

また、Windows 7 では、攻撃が成立するパターンが極めて限定的であることから、弊社"Yarai"のようなヒューリスティックなアプローチの有効性が高く、Windows 7+MSE に性能のよいヒューリスティック型のウィルス対策ソフトウェアの組合せることで、現段階で最も安全なシステムを構築できる。

3. **最新のアプリケーションを利用すべきである**

最新のアプリケーション(PDF, Office 等)は、DEP を有効にする等、セキュリティ対策が進んでおり、攻撃を阻止できる可能性が高い。最新のアプリケーションを利用すべきである。

4. **全てのアプリケーションは積極的に DEP を利用すべきである**

多くの攻撃は、アプリケーションの脆弱性を利用しているが、これに対して DEP の有効性が極めて高い。攻撃の対象がマイクロソフト製品から他社アプリケーションへ移行している現状を考えると、全てのアプリケーションは、DEP が有効な状態で出荷することが極めて重要である。

**表 1 検証項目と検証結果の概要**

| 検証項目 | 検証結果 |
|---|---|
| マルウェアの実行テスト | 1. 6種の検体の実行を試みたが、実行できるマルウェアはなかった。 |
| GENO ウィルス型<br>Drive-by-Download マルウェア | 1. URL 中に埋め込まれたダウンロードスクリプトは、IE8 の XSS フィルタで防ぐことができたが、HTML 中に埋め込まれスクリプトは、XSS フィルタの対象になっていないことから、ダウンロードすることができた<br>2. ダウンロードした、攻撃コードを含んだ PDF ファイルは、DEP により攻撃コードの実行が阻止された<br>3. DEP を無効にした場合、テンポラリフォルダに実行ファイルを作成する事ができるが、ProgramFiles 等の保護されたフォルダに書き込むことはできない<br>4. テンポラリフォルダにプログラムを作成した場合、AppLocker で実行を制限している場合は、AppLocker で実行を阻止することができた<br>5. ダウンロードするファイルを、DLL 形式にすることで、任意のプロセスの実行が可能であることを確認した<br>6. AppLocker で、DLL についても実行の制限を行った場合、DLL 形式を使った攻撃も阻止することができた。 |
| MyDoom 型<br>メール添付型マルウェア | 1. メーラの標準設定により、添付ファイルの実行が阻止された<br>2. 設定を変更し実行させると、セキュリティの警告ダイアログが表示された<br>3. 「実行」した場合、AppLocker の設定により実行が阻止された<br>4. AppLocker を無効にするとマルウェアが起動するが、整合性レベル等により、特定のフォルダ（共有フォルダ、ログオンユーザーのフォルダ）を除いて、ファイルの作成に失敗する。<br>5. AppLocker が有効な場合、これらのフォルダに書き込まれたプログラムは実行が阻止される事から、何らかの理由で、マルウェアがこれらのフォルダに実行ファイルの作成に成功した場合でもマルウェアの起動を阻止することができる。 |
| Trojan-Dropper.MSWord.1Table.ef 型<br>Word を使ったマルウェア | 1. Word 2003 + Office 2007 互換パックでは、MOICE によってドキュメントの読み込み時にエラーとなり、Word 2007 でも、同様にファイルの読み込み時にエラーとなり、マルウェアの実行を阻止することができた。<br>2. MOICE を無効にし、Word 2003 で開いたところ、DEP が無効になっていることから、一部修正を加えることで、マルウェアを稼働させることができた。<br>なお、Word 2007 の場合、DEP が有効であることに加え、XML フォーマットに Exploit コードを書き込む必要がある事から、Windows 7 + Word 2007 の組み合わせでこのタイプのマルウェアを稼働させる事は、極めて困難と考えられる。 |

## 2. 評価方法概要

評価は OS として Windows XP SP3、Windows 7の2つの環境を用意し、それぞれ表 2 に示した設定を行った。それぞれの環境で3つのシナリオを用い、Windows 7 でのセキュリティ機能が有効に働くかを検証した。シナリオによってはここに示した環境を変更しながら調査を行った部分もあるが、それについてはそれぞれのシナリオで記した。

**表 2 比較環境**

| OS | Windows XP SP3 | Windows 7 Ultimate |
|---|---|---|
| IE Version | 8.0.6001.18702 | 8.0.6001.18702 |
| IE セキュリティレベル | 中高 | 中高 |
| IE 保護モード | - | ON |
| メーラ | Outlook Express | Windows メール |
| Adobe PDF Link Helper | 8.0.0.456 | 8.0.0.456 |
| UAC (User Account Control) | - | ON |
| AppLocker | - | 既定の規則を作成・適用 |
| DEP (Data Execution Prevention) | OptIn | OptIn |
| ASLR (Address Space Layout Randomization) | - | ON(Default) |
| Windows Firewall | On | On |
| Office Version | Office 2003 SP なし 11.5604.5606 | Office 2003 SP なし 11.5604.5606 |

各環境におけるユーザー権限は管理者権限として操作を行った。ただし、Windows 7 では UAC は On であり、すべてのアプリケーションは低い権限のまま動作させた。

なお、この文書内で IE、Acrobat Reader、Office、Word という言葉が用いられた場合、特に断りのない限りここで示したバージョンのアプリケーションを指しているものとする。