Windows 8
セキュリティ Overview

Fourteenforty Research Institute, Inc.
株式会社 フォティーンフォティ技術研究所
http://www.fourteenforty.jp

Ver 2.00.01

Windows 8

- 2012年10月にリリース予定のMicrosoftの新しいOS
- Windows 8 ユーザーインターフェース（これまでMetro UIと呼ばれていたもの）が注目されている
- セキュリティに関しても多くの新機能

※ この資料はWindows 8 Release Preview時点の内容です

Windows 8 セキュリティ

注目キーワード

- Windows Defender
- Smart Screen
- Secure Boot
- AppContainer
- Windows Exploit Mitigation

Windows Defender

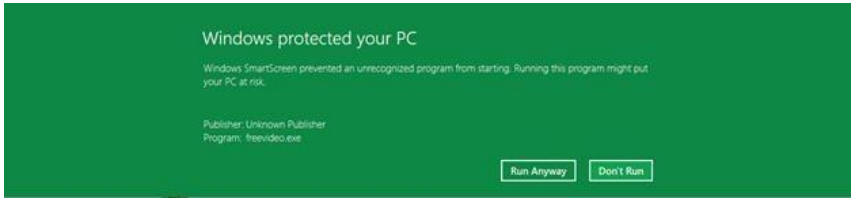
- Windows 8に標準搭載されるマルウェア対策機能
- Windows Vista, Windows 7ではアンチスパイウェアとして、標準搭載されていた機能
- これまでSecurity Essentialsで提供されていた機能が統合された形に
  →アンチマルウェア機能も持つように
  →基本的なマルウェア対策はこれだけで可能に
- シグニチャによるマルウェア検知
  （http://blogs.msdn.com/b/b8_ja/archive/2011/09/21/10214849.aspxより）
- 一部、Security Essentialsよりも機能的に少ない
  →スケジュールスキャンなどの項目がない

Smart Screen

- Windows 8に標準搭載されるウェブコンテンツ、ファイルのフィルタリング機能
- Smart Screen自体はこれまでIE8に搭載されていた(URLのフィルタリング)
- Windows8からはダウンロードしたファイルの実行もフィルタ
- ウェブコンテンツの表示、またはファイルの実行時に、そのコンテンツやファイルに危険性があるかサーバーに問い合わせて確認

IE9のウェブコンテンツの
SmartScreenフィルター

Windows 8の
SmartScreenフィルター



図は
http://windows.microsoft.com/ja-jp/internet-explorer/products/ie-9/features/smartscreen-filter
http://blogs.msdn.com/b/b8_ja/archive/2011/09/21/10214849.aspx
より引用

Secure Boot

- 既存のBIOS代わり、セキュアなブートプロセスを提供できるUEFI (Unified Extensible Firmware Interface)を利用したブート時のプロテクション

BIOSによるブート：OSのブートローダが脆弱

- The BIOS starts any OS loader, even malware

UEFIによるブート：ブートローダは検証されてから実行される

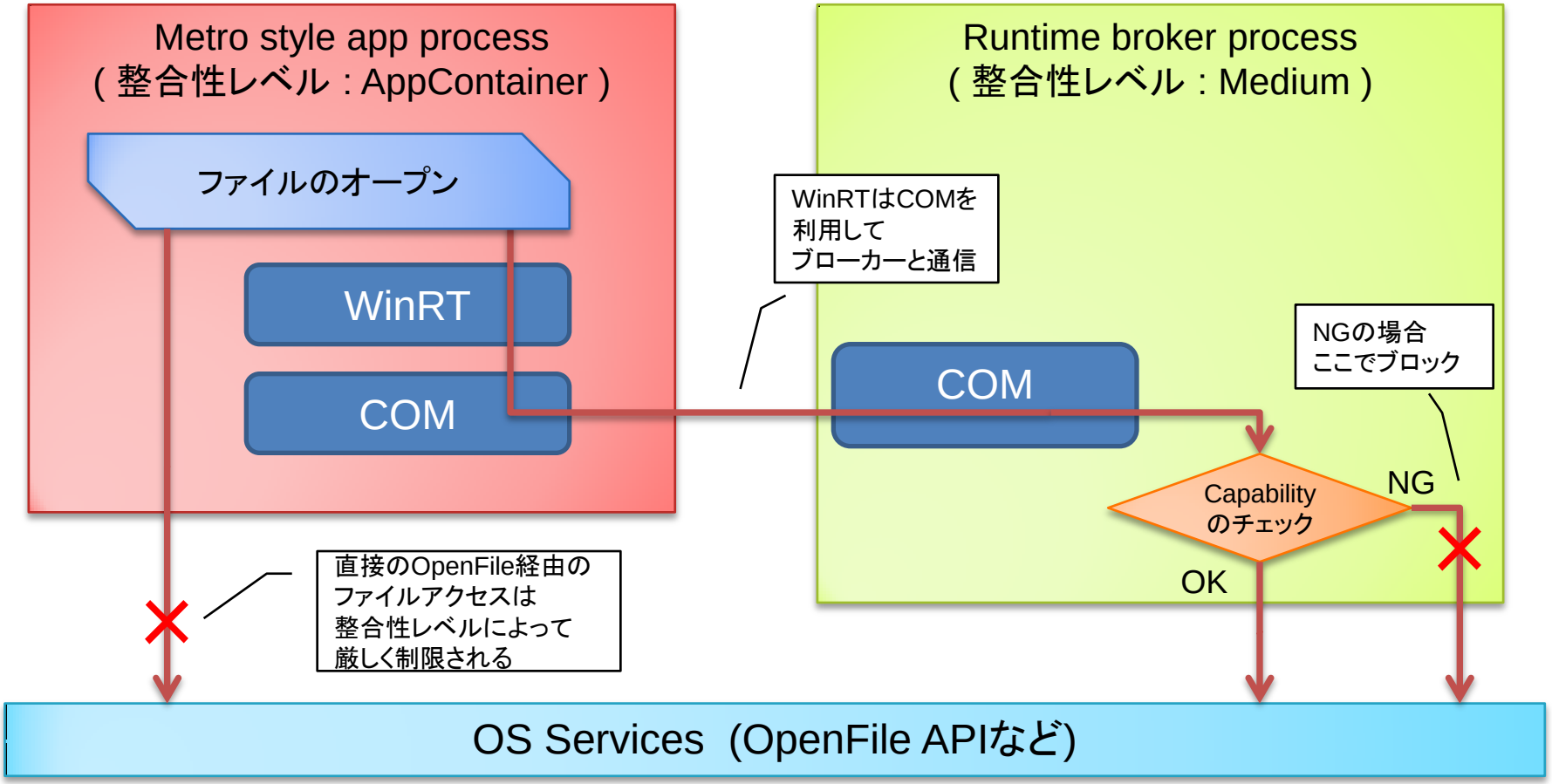
- UEFI will only launch a verified OS loader – such as in Windows 8
- Malware cannot switch the boot loader

図は http://blogs.msdn.com/b/b8/archive/2011/09/22/protecting-the-pre-os-environment-with-uefi.aspx より引用

AppContainer

- 新たなアプリケーション形式、Metro style appで適用されるサンドボックス環境
- プロセスに新たな整合性レベル(AppContainer)が適用される
- ファイルの読み書き、ネットワーク通信などを直接行うことが大きく制限されている
- Capabilityと呼ばれるアプリケーションの権限によって読み書きできるファイル、ネットワーク通信の可否などが決まる
- ブローカープロセスを通してファイルアクセス、ネットワーク通信などを行う

AppContainerでのファイルアクセス例



※ WinRT ・・・ Windows Runtime。Metro style appが利用するAPI。

Windows Exploit Mitigations

- 多くのExploit回避技術が改良、追加されている。
  - Enhanced /GS
  - Sealed Optimization
  - Virtual Table Guard
  - ASLR Enhancement
  - Heap Protection Enhancement
  - Kernel Enhancement

- これらについては、次回のMonthly Researchで詳しく紹介予定

まとめ

- Windows 8には、いままでにない多くのセキュリティ機能が追加された
- 既存のExploit技術では、攻撃がより難しくなってきている
- しかし、新たな機能やモデルが追加されたことで、新たな攻撃の可能性も

  - http://www.itmedia.co.jp/enterprise/articles/1208/01/news051.html
  - https://media.blackhat.com/bh-us-12/Briefings/Tsai/BH_US_12_Tsai_Pan_Exploiting_Windows8_WP.pdf