Windows 10
セキュリティリスク抑制効果調査報告 Phase1

CONTENTS

本レポートの概要

- 80%超の国内企業は、クライアントOSとして既にメインストリームサポートが終了したWindows 7を利用している。
- 攻撃技術の研究が進み、Windows 7ではセキュリティ面で不十分である。
- Windows 10ではOS標準として大幅なセキュリティ機能の強化が行われており、セキュリティ面の向上は勿論、総合的なITコストを削減することができる。
- ビジネス用途のWindows 10では、アップデートのサービシングモデルにCBB（Current Branch for Business）、LTSB（Long Term Servicing Branch）の2種類があるが、国内ではLTSBを利用しようとする傾向が強い。LTSBを前提とした運用は、ITの進化に対応できない可能性がある。

FFRI 株式会社 FFRI

1 Windows 7の誤った安心感

1.1. 進歩する攻撃技術

2009年10月22日に販売開始となったWindows 7も6年超が経過しており、既にメインストリームサポートが終了し、延長サポート期間に入っている。ところが多くの国内ユーザー企業では、クライアントOSとしてWindows 7を利用しているのが実情だ[1]。

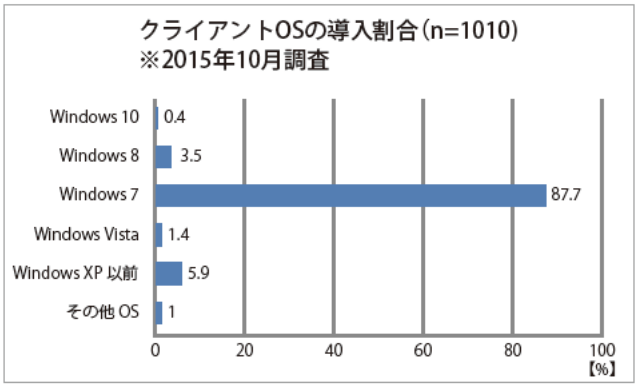

図 1　クライアント OS の導入割合（※脚注 1 に基づき独自に作成）

Windows 7の販売が開始された2009年と現在では攻撃技術に大きな隔たりがあり、「Windows 7を使っていれば安全」とは言い切れない。なぜならその隔たりとは、攻撃者がWindows 7に搭載された様々なセキュリティ技術を調査・分析することで生み出したセキュリティ技術の回避手法や脆弱性だからである。

1　http://www.juas.or.jp/servey/it16/it16_ppt.pdf
33p「<クライアントOS> Windows XPの2014 年4 月9 日サポート終了を受けて、Windows 7の導入がさらに進み、導入割合は約9割となった」

1.2. 標的型攻撃はなぜ止まらないのか？

特定組織を狙った標的型攻撃が問題となっている。精緻に作られたメールに不正なファイルが添付されており当該ファイルの実行を誘導するケース、メール本文に記載されたURLから罠サイトへのアクセスを誘導するケースが多い。Windows 7は、過去の経験からこうした脅威への対策として様々な機能を搭載している。具体的にはデータ実行防止(DEP)、アドレス空間配置のランダム化(ASLR)と言った脆弱性緩和技術、ユーザーアカウント制御(UAC)による誤操作・不正操作の自動実行防止機能が挙げられる。

しかし、現在こうした機能の調査・分析が進み、いくつかの技術的な条件を満たす必要はあるもののこれら機能を回避、対抗する手法が発見されている。

脆弱性攻略技術と脆弱性緩和技術の歴史は古く、イタチごっこを繰り返しながら双方の技術が進歩してきた。脆弱性緩和技術の進歩に伴い、脆弱性攻略の技術制約が増加し、たとえ脆弱性があってもそれを悪用することが難しい状況となっている。一方で攻略の難易度は上がっても脆弱性が存在する以上、その可能性をゼロにすることはできない。マイクロソフト社が発行しているMicrosoft Security Intelligence Report第16版からのデータを以下に引用する。

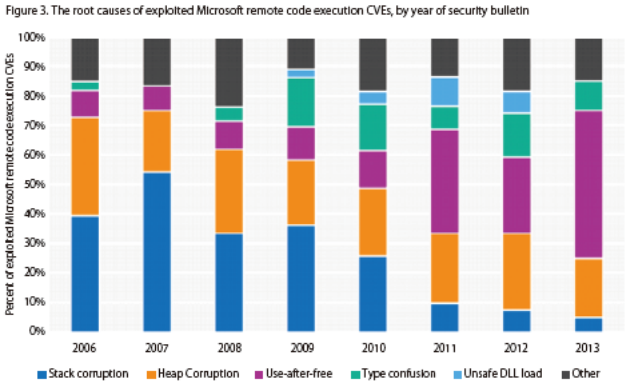

図 2　マイクロソフト製品に対するリモートからのコード実行脆弱性の原因と内訳

上図は、毎年発見・報告されたマイクロソフト製品に対するリモートからのコード実行脆弱性についてその原因と割合をプロットしたものだ。特徴的な点として以下が挙げられる。

- Stack corruptionに起因した脆弱性の割合が減少している

- User-after-free及びType confusionに起因した脆弱性の割合が増加している

前者は、技術的にはDEPやASLRにより緩和可能な種別の脆弱性であり、Windows 7の導入に伴い減少していると推察される。一方で後者は、そうした状況を受けてより攻撃を成功させる可能性が高いものとして悪用の比率が増加していると考えられる。実際にAdobe Flash Player等のサードパーティー製品を対象としたUser-after-freeによる脆弱性攻撃は現在でも絶えず発見されており、またそうした脆弱性が実際の標的型攻撃等でも悪用されている。

一方でUACは、Windows Vista以降のOSで搭載された機能であり、ユーザーがシステムに対する変更等の操作を行う際にダイアログ・ボックスによる許可・不許可の選択を強制する機能だ。これにより管理者アカウントでログオンし、システムを利用していた場合になんらかの理由でマルウェアを実行してしまった、させられてしまったとしても一定の段階でダイアログ・ボックスが表示され、処理が中断される。しかし、UACに関してもそれを回避する手法が発見・報告されており、当該手法を利用したマルウェアも確認されている。

- 標的型攻撃で利用されるRAT「PlugX」

http://www.iij.ad.jp/company/development/report/iir/021.html

- Dridexが用いる新たなUAC回避手法 (2015-02-09)

https://www.jpcert.or.jp/magazine/acreport-uac-bypass.html

このように攻撃者はOSが備えるセキュリティ技術を入念に調査・分析し、着実にその弱み、盲点を突いてくる。個別の脆弱性として修正プログラム等により対応できるケースもあるが、設計に関わる問題については修正プログラムによる根本解決が困難なケースもある。こうした事情からシステムのセキュリティレベルを評価する上で「どのOSを利用しているか?」を無視することはできない。

2 Windows 10の技術優位性とコスト優位性

2.1. 最新 OS の強み

Windows 10では前述のような問題に対抗する機能を新たに搭載している。その一つとして制御フローガード(CFG)が挙げられる。CFGはその名称通りコード実行の連続性を確認、保証する技術である。前述のUser-after-freeを悪用して攻撃を行う場合、正規のコードから本来プログラム上に存在しない悪意のコードへの呼び出しが行われる。CFGは、こういったコードの流れを監視し、事前に呼び出し先コードが正規のコードか否かの確認を行う。これにより不正なコードの呼び出しを検知した際に、コード呼び出しを行わずプログラムの実行を終了させる。今後イタチごっこが進むことで攻撃手法のトレンドが変化する可能性はあるが、CFGは現在主流となっている攻撃手法の一つに対する確かな対策技術だと言える。

このようにWindows 10ではCFGの他にも以下のような新たな機能が搭載されており、これまで以上の多層防御がOS標準で実現されている。

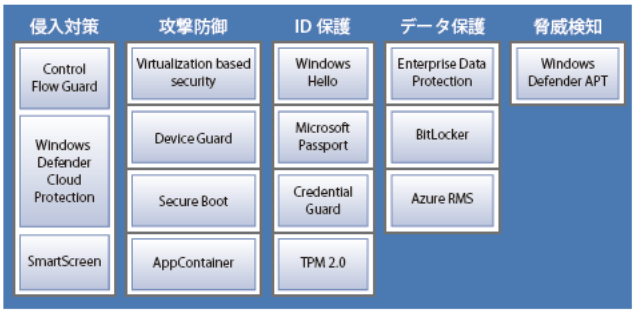

図 3　Windows 10 のセキュリティ多層防御

本節では、上記のうちSmartScreen、Virtualization based securityに基づいたDevice Guard及びCredential Guard、Microsoft Passport及びWindows Helloについて紹介したい。

2.1.1. SmartScreen

SmartScreenは、ドライブバイダウンロードやフィッシングと言ったWebアクセスに関する脅威、スパムや不審メールなどメールに関する脅威へのフィルタリング機能である。この機能自体は、Windows 10以前から搭載されているが、Windows 10からはInternet Explorer 11及び新Webブラウザである Microsoft Edgeの両方に対して適用されている(図 4)。前述の通り標的型攻撃では罠サイトへのアクセスをメールから誘導するケースが多い。また、近年では、オンライン広告を利用して悪性サイトへの誘導を行う「マルバタイジング(Malvertising)」も問題となっている。マイクロソフト社では、Bing、Windows Defender等の様々な取り組みからこうした悪性サイトの情報を収集している。SmartScreenは定期的に当該情報をダウンロード、更新することで端末からのWebアクセス発生時に悪性サイトへのアクセスをブロックする。前述のCFGが悪性サイトに誘導され、脆弱性攻撃を受けた際の攻撃成功率を低減される緩和策であったのに対し、SmartScreenはそもそも悪性サイトへのアクセスを防止する策だと言える。

	フィッシング詐欺検出確認	SmartScreen®					
OS	Windows Vista	Windows Vista / Windows 7		Windows 7	Windows 8 Internet Explorer 10	Windows 8.1 Internet Explorer 10 / Internet Explorer 11	Windows 10 Internet Explorer 11 / Edge
ブラウザ	Internet Explorer 7	Internet Explorer 8	Internet Explorer 9	Internet Explorer 10 Internet Explorer 11			
URL 評価（フィッシングサイト）	○	○	○	○	○	○	○
URL 評価（マルウェアサイト）	×	○	○	○	○	○	○
アプリケーション評価（ダウンロード時）	×	×	○	○	○	○	○
アプリケーション評価（実行時）	×	×	×	×	○	○	○
Windows 統合	×	×	×	×	○	○	○
ドライブバイ評価	×	×	×	×	×	×	○*

* Windows 10 November Update で提供開始（Windows 10 Version 1511 以降で利用可能） ** 対象製品はクライアント OS のみ記載

図 4　SmartScreen の OS/ ブラウザ別機能対応表
※出典：https://news.mynavi.jp/itsearch/article/all/1462

2.1.2. Virtualization based security に基づいた Device Guard 及び Credential Guard

Windows 10ではVirtualization based security(VBS)と呼ばれる仮想化技術を利用した環境分離技術を搭載している。これにより一台のハードウェア上でユーザーが操作を行う通常のシステム環境と高度なセキュリティが必要となる機能を行う環境を異なる仮想マシンに分離することができる。このVBSに基づいて実現される機能がDevice Guard及びCredential Guardである。

Device Guardは、カーネルモードで動作するコードの整合性を保証するKMCI(Kernel-mode code integrity)及びユーザーモードで動作するコードの整合性を保証するUMCI(User-mode code integrity)から構成される。KMCIでは、例えばデジタル署名が未署名のドライバの実行を禁止することができる。一方、UMCIは、アプリケーションの実行ファイルのハッシュ値等、一定の規則に基づいて実行の許可・禁止、イベントログへの情報出力等の設定を行うことができる。そのため事前にこうした整合性ポリシーを作成し、配布・適用することでマルウェアのようなプログラム、モバイルコードの実行を防止することできる。また、Device Guard自体の整合性検証を行う処理は、前述の異なる仮想マシン環境内に存在するため通常のシステム環境から改ざん等の侵害を行うことができない。

Credential Guardは、Windowsが内部的に保持している資格情報を異なる仮想マシン環境内で保持・管理する仕組みだ。従来ドメインに対する認証情報のキャッシュ等はLSAと呼ばれるプロセスによって管理されていた。LSA自体は、ユーザー空間で動作する1プロセスであるため管理者アカウント等による適切な権限さえあれば、他のプロセスからプロセス内のメモリに干渉し、キャッシュされた資格情報を窃取、悪用するという攻撃が可能であった。この攻撃こそ悪名高いPass the Hash攻撃である。Pass the Hash攻撃は国内外の様々なインシデントでの利用が報告されており、有名な事例としては2011年9月に発生した日本、米国等の防衛産業企業を狙った標的型攻撃2が挙げられる。Windows 8.1ではPass the Hash攻撃への対策が施されているが完全なものではない。その意味でCredential Guardは、資格情報の管理を異なる仮想マシン環境で実現するため技術的に抜け漏れがない対策だと言える。

2 http://itpro.nikkeibp.co.jp/article/COLUMN/20110926/369417
防衛産業企業を狙った標的型攻撃が発覚、「多層防御」を考察する

2.1.3. Microsoft Passport 及び Windows Hello

Windows 10では、Microsoft Passport及びWindows Helloによるパスワードを使わない認証を利用することができる。従来システムへのログオン等の認証ではユーザー名及びパスワードを利用する方式が一般的である。しかし、この方式は以下のような課題を抱えている。

- **ユーザー名及びパスワードが漏洩した場合、誰でもその情報を利用して当該ユーザーになりすますことができる。これは、異なるシステム間で同じパスワードを使い回していた場合、特に大きな問題となる。**
- **認証の強度を保つためには、十分に長いパスワード、英数字記号、大文字小文字等が組み合わされた複雑なパスワードを利用する必要があるが、これはユーザービリティを低下させる。**

この解決策としてWindows 10では、Windows Helloと呼ばれる生体認証をOS標準で利用することができる。指紋センサーやカメラ等のセンサーが搭載されていた場合はそれぞれ指紋認証、顔認証、虹彩認証を利用すること可能である。また、こうしたセンサーが搭載されていない場合は、Microsoft Passportとして提供されるPINコードによる認証を利用することができる。Windows Helloの設定を行う際、まず始めにPINコードの設定を行う必要がある。その後、生体情報の登録と併せて自動的にデバイスに紐付いた公開鍵・秘密鍵のペアが作成、登録される。Microsoft PassportのPINコードもデバイスに紐付いたものとなるため仮にPINコードが漏洩してもそのPINコードを他のデバイスから利用することはできない。攻撃者は、対象のデバイスに物理的にアクセスするか、デバイスを攻撃する必要があるため認証情報漏洩によるなりすましの脅威を大幅に低減することが可能となる。

2.2. アンチウイルスソフトはもう要らない？

Windows 10では、Windows Defenderによるアンチウイルス機能が標準搭載されている。Windows Defenderは登場した当初はアドウェア及びスパイウェア向けの対策ソフトウェアであったが、Windows 8及び8.1以降はMicrosoft Security Essentialsと統合されたアンチウイルスソフトウェアとして提供されている。こうしたOS標準の仕組みは、サードパーティーのアンチウイルス製品と比べて導入の手間を省くことができ、また運用に必要となる管理機能をSystem Center等の統一的な仕組みで実現できるため、総合的なITコストを削減することができる。

一方で以前からマイクロソフト社と言うソフトウェアベンダーが無償で提供を開始したソフトウェアと言うこともあり、その検知能力を疑問視するユーザーが一定数居ることは否めない。アンチウイルス製品の第三者評価機関であるAV Comparativesが2016年4月に実施した評価結果を以下に示す。

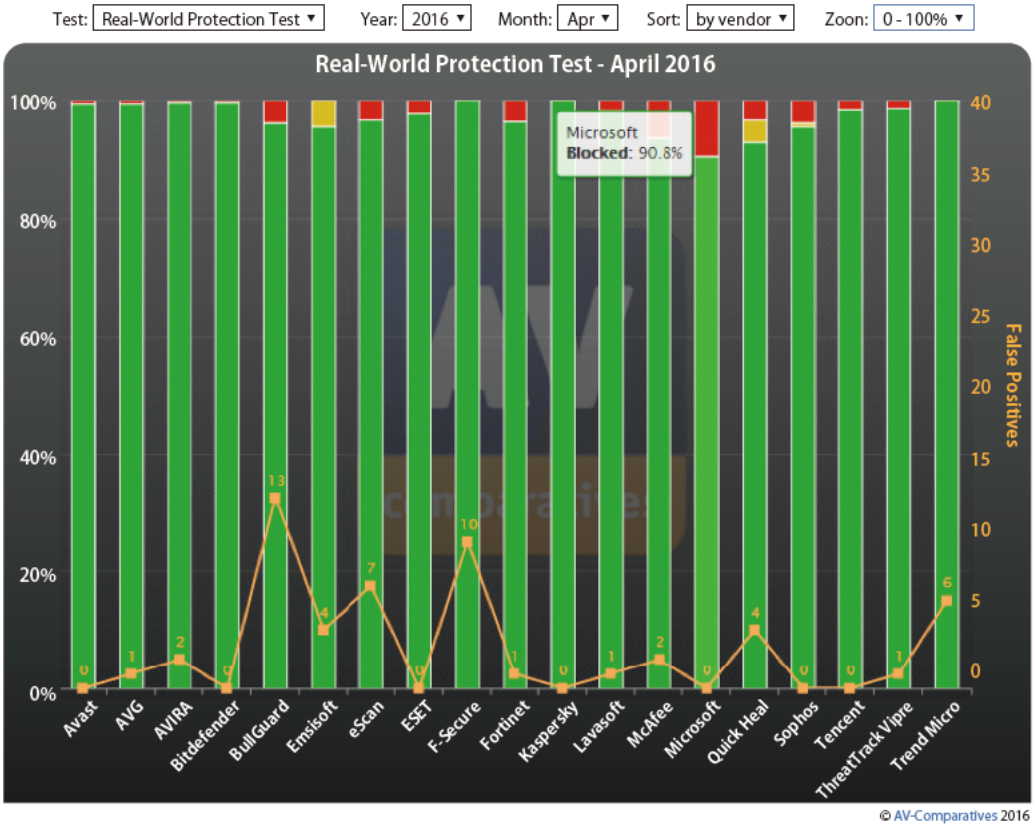

図 5　Real-World Protection Test の結果 (2016 年 4 月)　出典：http://chart.av-comparatives.org/chart1.php

上図は、Real-World Protection Testsと呼ばれる評価の結果であり、テスト実施時点で実際に流行しているマルウェアを利用した検知有無の結果をプロットしている。Microsoftは、正常検知率90.8%、誤検知率0%と言う結果となっている。正常検知率はあいにく全ベンダー中最も低いスコアとなっているが、マイクロソフト社ではこのテストでは評価の対象になっていないSmartScreenを併用することで、精度の高い検知を実現していると主張している。SmartScreenの評価が実施されていないため、判断が難しい面があるが、検知手法が異なる二つの対策を組み合わせることは、有効性が高いと考えられる。アンチウイルス製品のライセンス費用と言う費用対効果の面で議論の余地があるだろう。

標的型攻撃やメールのばらまき型攻撃に代表される現在の攻撃は、攻撃者は事前にアンチウイルス製品で検知できないマルウェアを用意して利用するため攻撃発生時点ではどのベンダーかに依らずマルウェアを検知できないケースが多い。その後、攻撃の進行、マルウェア検体の拡散に伴いアンチウイルスベンダーでパターンが生成され、防御可能な状態に移行する。このパターン生成に要する時間はアンチウイルスベンダーによってまちまちではあるが通常数時間から数日程度である。一方で攻撃発生から終息までの時間も短期化しており、早いものでは2～3時間で終息に至るケースもある。こうしたケースで利用されるマルウェアは攻撃毎に使い捨てられるためパターンが生成された時点で、既にそのパターンには価値

がない。マイクロソフト社では、Office 365のユーザーが拡大したことに伴い、Office 365で提供しているマルウェア対策を通じて、直接入手できる検体が格段に増えている。一方で、こうした現況を踏まえるとシステムのマルウェアに対する防御力は、パターンが存在しない状態で「どの程度マルウェア検知できるか」と言う“基礎検知力”が重要だと言える。これについても既に導入がアナウンスされているWindows Defender ATP(Advanced Threat Protection)によるクラウド上でのサンドボックス分析やSafeLinkで検知したマルウェアについても検体を収集することで、検知能力の拡大を図っている。今後こうしたOS標準での取り組みが進むことで従来型のアンチウイルス製品はその存在意義を問われことになるだろう。

3 Windows 10移行において考慮すべき「サービシングモデル」

3.1. 広がる他国とのIT利用力の差

前述のようにWindows 10は、Windows 7リリース以降に積み上げられた攻撃技術の進歩に対して確かな防御機能を搭載、提供している。セキュリティ面で言えばこれだけで十分Windows 10にアップグレードする価値がある。但し、Windows 10への移行について海外、国内ではやや異なる状況が見受けられる。

Windows 10のビジネス向けのサービシングモデルはCBB(Current Branch for Business)とLTSB(Long Term Service Branch)の2つが存在する。CB(Current Branch)と呼ばれるコンシューマー向けのモデルでは常に最新の状態へ自動的に更新される。CBBは、これに対してCBへのリリースから約4ヶ月後にアップデートがリリースされるモデルである。つまり、業務への影響を考慮し、検証等に必要となる移行への猶予期間が設けられているわけだ。マイクロソフト社は、コンシューマーではCB、ビジネスでもCBBの利用を推奨している。

一方で、国内企業でのWindows 10への移行はLTSBと呼ばれるモデルを前提にしているケースが多い。CB・CBBではアップデートの内容が新機能への対応、セキュリティ更新プログラムの適用であるのに対してLTSBではセキュリティ更新プログラムの適用のみとなる。アップデートの適用自体は、CBと同様のタイミングであり、機能固定のまま(新機能追加がないまま)最大で10年間サポートされる。CB及びCBBの最短サポートライフ期間がそれぞれ4ヶ月、8ヶ月であることを考えると10年は非常に長い。

どのサービシングモデルを利用するかは業務及びシステムの特性に合わせて最適なものを選択すれば良いが、検証及びアップデートに伴うコストを敬遠してCBBではなくLTSBを選択するケースがあるのではないだろうか。欧米では、新たな機能を積極的に評価し、業務に取り込むことで変化していく風潮が強い。CBBを選ぶか、LTSBを選ぶかはまさにこういった変化し続ける能力を試されている。

株式会社 FFRI

お問い合わせ先

株式会社 FFRI　経営管理本部 経営企画部 IR 広報担当
TEL : 03-6277-1811　E-Mail : pr@ffri.jp
URL : http://www.ffri.jp