会員限定

2017 年 2 月度
金融システム研究会
2017 年 2 月 16 日(木)

『なぜ「今」Windows10 が必要なのか？』

～史上最高のセキュリティ機能と
金融業界での Windows タブレットの活用法～

講師：野明 純
日本マイクロソフトWindows & デバイス営業本部

金財情報システム「金融システム研究会」事務局

CONTENTS

『なぜ「今」Windows10 が必要なのか?』
～史上最高のセキュリティ機能と金融業界での Windows タブレットの活用法～

目次

第 1 部 …… 4

Slide 2　自己紹介…… 4
Slide 3　本日の内容…… 6

サイバー攻撃のトレンド …… 6

Slide 5　サイバー攻撃の進化…… 8
Slide 6　1425% …… 8
Slide 7　脆弱性と攻撃コードの売買する組織 …… 10
Slide 8　サイバー攻撃の現状企業の 9 割は脅威が侵入済み　セキュリティ問題 サーバー ルームから役員室へ …… 10
Slide 9　情報セキュリティ 10 大脅威…… 12
Slide 10　全部偽物です（事例）…… 12
Slide 11　どんな風に狙われるか?～アカウント侵害の連鎖～ …… 14
Slide 12　Continuous Compromise Perspective …… 14

Windows10 開発におけるセキュリティ戦略 …… 16

Slide 14　今までのセキュリティ戦略 vs これからのセキュリティ戦略 …… 16
Slide 15　Windows 10 開発におけるセキュリティ戦略 …… 18

Windows10 のセキュリティ機能実装 …… 18

Slide 17　Windows 10 開発でのセキュリティ強化…… 20

1. やられないようにする …… 20

Slide 19　従来の問題点：1. やられないようにする …… 22
Slide 20 認証の強化：Windows Hello …… 22
Slide 21 FIDO Alliance…… 24
Slide 22 マルウェアからの防御：Windows Defender…… 24
Slide 23　デバイスの保護：Device Guard …… 26

2. やられている事をすぐに検知する …… 26

Slide 25　従来の問題点：2. やられている事をすぐに検知する …… 28

Slide 26　脅威をいち早く検知し、いち早く守る：Windows Defender Advanced Threat Protection（Windows ATP） … 28

3. やられても被害を小さくする …… 30

Slide 28　従来の問題点：3. やられても被害を小さくする …… 30

Slide 29　端末のリフレッシュ：Windows 10 ロックダウン …… 32

Slide 30　安全な Web 閲覧：Windows Defender application Guard（Preview） …… 32

4. やられた後でも、情報を保護する …… 34

Slide 32　従来の問題点：4. やられた後でも、情報を保護する …… 34

Slide 33　デバイスの暗号化：BitLocker と BitLocker To Go …… 36

Slide 34　ファイルの暗号化：Windows Information Protection …… 36

まとめ …… 38

Slide 36　Windows 7 との比較 …… 38

Slide 37　新しい OS ほどマルウェア感染率は低い …… 40

Slide 38　Windows 10 継続的なアップデート …… 40

第 2 部 …… 42

Slide 2　本日の内容 …… 42

金融機関でのタブレットの動向 …… 44

Slide 4　タブレット導入に関する 3 つの疑問 …… 44

Slide 5　金融機関での利用シナリオ …… 46

Slide 6　銀行業における Tablet 活用のニュース記事 …… 46

Slide 7　大手地域金融機関における Tablet 導入状況 …… 48

次世代標準機としてのタブレットの選定考慮事項 …… 48

Slide 9　Windows タブレット選定にあたっての考慮事項 …… 50

Slide 10　これからのデバイスカテゴリ …… 52

Slide11　新しいカテゴリ 2 in 1 デバイスとは？ …… 54
Slide12　情報入力方法の多様化 …… 54
Slide 13　各デバイスの比較 …… 56
Slide 14　さらに新しいカテゴリ 3 in 1 デバイスとは？ …… 56

2in1 PC の活用方法 …… 58

営業活動支援 …… 58

Slide 17　活用方法 1　お客様先で柔軟に商品を説明できる …… 58
Slide 18　活用方法 2　機会を逃さずその場での対応ができる …… 58
Slide 19　活用方法 3　本部専門スタッフによる商談のリモート支援、営業品質の向上 …… 60

セキュリティ …… 60

Slide 21　活用方法 1　時間や場所を問わず行内システムに安全にアクセス …… 62
Slide 21　活用方法 2　セキュリティを確保しながら、ペーパーレス化を実現 …… 62
Slide 23　活用方法 3　常に安心。万が一の時も安心の端末管理 …… 64
Slide 24　活用方法 4　持ち出し専用デバイスを標準機能で実現 …… 64
Slide 25　活用方法 5　セキュアな情報共有 …… 66

生産性向上 …… 66

Slide 27　活用方法 1　Office ファイルの編集を行外でできる …… 68
Slide 28　活用方法 2　ペーパーレス会議 …… 68
Slide 29　活用方法 3　行内、行外、位置情報に合わせてアプリを制御 …… 70

導入事例 …… 70

Slide31　明治安田生命保険相互会社様 …… 72
Slide32　みちのく銀行様 …… 72
Slide33　北國銀行様 …… 74
Slide 34　ふくおか FG 様 …… 74
Slide 35　十八銀行様 …… 76

◆ 質疑応答 …… 78

皆さまこんにちは。私は日本マイクロソフトでWindows クライアントのプリセールスのエンジニアを担当しております野明と申します。本日は貴重なお時間をいただきまして誠にありがとうございます。

今日の前半は、まず Windows10 が 2015 年 7 月 29 日にリリースさせていただいて、もう 1 年半近く経過しています。多くの金融機関さまを含め、私はいろいろなお客さまを担当しているのですが、Windows10 の展開が、国内、海外を含めてすごく進んでいます。今コンシューマを含めて Windows10 の端末が 4 億台ぐらい世の中に展開されています。すべての端末が Windows10 になっているお客さんは正直まだまだいないのですが、今年 4 月以降、Windows10 の展開計画を立てられているお客さまは非常に多いです。

やっぱり、Windows7 がかなりつくりが良い OS だったので、なんで 10 にしないといけないかという理由をすごく聞かれます。今回、一つテーマとしましては、セキュリティ機能が 7 と比較してもかなり強化されています。なので、まず 10 のセキュリティの部分にどういったものがあるかを理解していただきたいと思います。

第 2 部は、PC を外に持ち出して仕事をするという新しいワークスタイルに取り組まれているお客さまが非常に多いです。マイクロソフトも、今私が使っているような Surface Book とか Surface Pro 4 といったタブレットを使って外で活用しようというお話がすごく増えてきています。なので、弊社でも金融機関向けにいろいろなタブレットのご提案をさせていただいておりますので、今日は金融機関でどういう使い方をしているか、実際にデモをご紹介させていただき、2 部構成という形で進めさせていただきたいと思います。

第 1 部

Slide 2　自己紹介

簡単に自己紹介をさせていただきます。

2000 年に旧富士総合研究所、今のみずほ情報総研に入りまして、6 年、富士総研で COBOL の開発とか、有担保受付審査という住宅ローンの審査システムなどをつくっていました。

2006 年に日本マイクロソフトに入って現在に至っていますが、ずっとプリセールスという活動を行っています。最初はセキュリティ製品を 6 年ぐらいやっておりまして、その後に Windows Server、あとはパブリッククラウドであります Azure といったところのプリセールスを担当しておりまして、2015 年、Windows10 をリリースする前から、今の Windows10 のプリセールスに携わっているという形になっています。

あとはゴルフとか趣味をほどほど書いていますけれども、Facebook、LinkedIn がありますので、今日お名刺交換をさせていただいてももちろんいいのですが、Facebook とか LinkedIn で探して友達申請いただければ、そこからいろいろな輪が広がっていくと思いますので、ぜひご興味のある方は登録いただければと思います。

Slide 1-2

自己紹介

- 2000年　富士総合研究所 (現みずほ情報総研)　入所
- 2006年　日本マイクロソフト　入社
- セキュリティ製品のプリセールスエンジニアを6年担当し、
  Windows Server、Azure のプリセールスエンジニアを経て、
  現在 Windows 10 のプリセールスエンジニアを担当
- 趣味ゴルフ、7歳、4歳、7か月3人の子供、Facebook “野明　純”、LinkedIn “Jun Noake”

2

Slide 3　本日の内容

「本日の内容」です。

まず、皆さまにはもう釈迦に説法になっているかもしれませんが、今のトレンドですね。私どもはよく「理解して怖がろう」といっています。むやみに怖がっても不安をあおり立てるだけなので、正確に今どういうことが起きているかを理解することが重要だと思います。

あと、こういったサイバー攻撃がどんどん進歩しているなか、Windows10 はどういった開発ポリシーでつくられているか。

また具体的に、Windows10 はどういったセキュリティ機能を実装しているかというところをお話ししていきたいと思います。

サイバー攻撃のトレンド

Slide 1-3

本日の内容

- サイバー攻撃のトレンド
- Windows 10 開発におけるセキュリティ戦略
- Windows 10 のセキュリティ機能実装
- まとめ

サイバー攻撃のトレンド

Slide 5　サイバー攻撃の進化

最初のテーマである「サイバー攻撃のトレンド」というお話を進めていきたいと思います。

これは、横軸が「年」です。2003 年から 2012 年。縦軸が攻撃の「複雑度」。どれだけ巧妙になってきているか。

2003 年～ 2004 年というのは WindowsXP がリリースされた時期ですが、攻撃する側もすごく幼稚な感じだったんですね。なので、スクリプトキディズなんていうふうに呼んでいました。そういった人は有名なクラッカー、ハッカーがつくったものをダウンロードしてきて、不特定多数の PC に投げつける。昔はすごく派手なウイルスが多かったんです。花火が上がったり、PC が真っ黒になってしまうとか、そういうことをやって喜んでいた。動機はすごく単純で、自己顕示欲を出したい。おれはこんなすごいことをやったんだぞ、と言いたかっただけなんですね。

そのころのセキュリティの考えというのはアンチウイルスソフト、あと WindowsXP だと、日本でかなり物議を醸しましたけれども、XP の SP2 で出てきた Windows ファイアウォール、そういったものを入れて、端末の要塞化みたいな考えを持っていました。なので、アンチウイルスソフト、パーソナルファイアウォールは必須みたいな時代でしたね。

これが 2005 年になると、Windows も Vista であったり 7 とか出てきていたと思いますが、攻撃者側もかなり巧妙になってきました。現在でもやられている企業もありますが、標的型攻撃に代表されるようなものです。たとえばマイクロソフトは自社のアンチウイルスソフトを使っているのですが、そのアンチウイルスソフトに感染しないウイルスをつくって、メールで送り込んで、変な URL を踏ませて感染させるなんていうことが簡単にできてしまいます。

もうアンチウイルスソフトだと守れない時代になってきています。

攻撃者側もすごく巧妙になってきて、かつ、動機がお金を稼ぐということに完全にシフトしてきています。

ランサムウェアといって、パソコンに感染するとファイルに暗号がかかってしまう。個人のパソコンでそんなものに感染すると、家族、子どもの写真が暗号化解除しないと見れなくなってしまうなんていうウイルス――ランサムウェアも流行っています。これは今かなり攻撃が増えてきているのですごく話題になっていますが、昔からあるものです。

なので、アンチウイルスソフトだけだとやっぱり防げなくなってきています。

さらに「2012 年以降」とありますが、国家犯罪。この前、トランプの大統領選挙でもロシアからハッキングを受けていたとか、あとは、ご存じかもしれませんけれども、イランの核施設に対して攻撃するというかなりニッチなウイルスがあります。それに感染すると、遠心分離機の加速器を変える、そうすると原子炉が暴走してしまう、そういったかなりニッチなものも出てきて国家犯罪にもなってきています。

なので、昔の考えだと今のセキュリティ対策はできないですね。

Windows10 というのはどんどん進化していく OS です。Windows10 の次は 11 出るの？ 12 出るの?とよく聞かれるのですが、出ないです。10 は年 2 回機能アップデートをして、セキュリティの機能をどんどん追加していきます。攻撃者側に Windows10 を使っているお客さまを攻撃するのは面倒くさいなと思わせるのがマイクロソフトの考えになっておりますので、どんどんセキュリティの機能を追加して Windows10 は進化していくという形になっています。

Slide 6　1425%

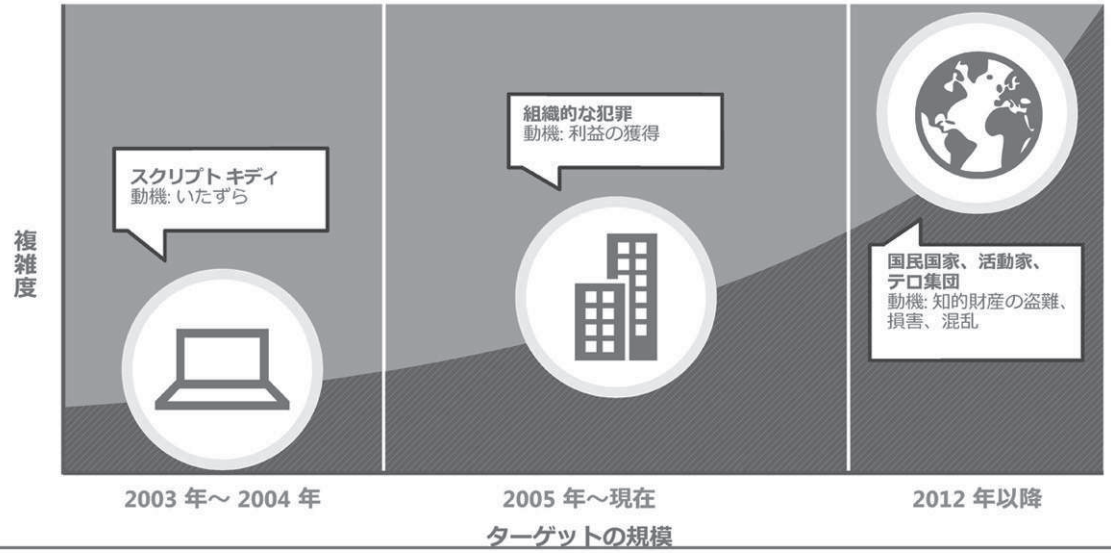
次の「1425%」とは何かというと、攻撃者側の ROI なんですね。

1 万円入れるとリターンが 14 万バックしてくる。こんなおいしいビジネスは世の中にない。1 万円が 14 万だとそうでもないかもしれないですけれども、1,000 万かけてリターンが何億となってくると、それはほんとおいしいビジネスです。なので、たとえば日本とかは裕福であれですけど、ブラジルであったり東欧のあまり裕福でない国は、組織立って外資の会社を攻撃してお金をゆするという形がビジネスとして成り立っている現状です。

こういった ROI のなかで、攻撃者側はすごくお金を儲けているという形になります。

Slide 1-5

サイバー攻撃の進化



5

Slide 1-6

1425 %

出典 : Trustwave
https://www2.trustwave.com/GSR2015.html

Slide 7　脆弱性と攻撃コードの売買する組織

攻撃者側も、彼ら自身でハッカーを雇ってやるということもできるのですが、それだとやっぱり効率が悪い。なので、ZERODIUM という闇のアングラサイトみたいな、ここで攻撃コードを売買しているというブラックマーケットが存在しています。

お手元の資料を見ていただくと、iOS が普及しているので、それだけすごく高い値段で取引されています。50 万ドルで取引されていたりもします。

このへんを見ていただくと Windows があったり Office があったり、いろいろな製品の脆弱性、攻撃コードといったものが裏で取引されています。

なので、攻撃者側はこういったブラックマーケットで攻撃コードを買ってきて攻撃をする。そうすると「1425％」のリターンが返ってくる。マーケットとして成り立っている、というのが現状です。

こういったことを踏まえると、守る側はやられて当然、攻撃されて当然と思っていただかないと、昔のような考えだとなかなか守りきれないというのが出てくるかと思います。

Slide 8　サイバー攻撃の現状企業の 9 割は脅威が侵入済み　セキュリティ問題 サーバー ルームから役員室へ

これはちょっとビジーなスライドになっているのであとで参考で見ていただければいいですが、ほとんど 9 割の会社が攻撃されています。何かしらの形で侵入されています。

重要になるのはここです。侵入から発見されるまで気付いていないというお客さまが非常に多い。平均値をとってだいたい 240 日ぐらい気付いていない。少し前に年金機構さんで大きな情報漏えいがありましたけれども、あれもじつは感染していたことにまったく気付いていなかった。

今のウイルスは最初はすごく小さなモジュールなんです。ウイルス自体が FTP ソフトみたいに日々アップロードしてくる。気付いたら、いろんなボットネットをつくるようになっていたり、ファイルをいろんなところにアップロードしてしまう、そういったものにどんどん進化していきます。なので、気付いたころには手遅れ。もう情報漏えいしてしまっているというケースが非常に多くなっています。

このあたりのデータは世の中に出ているものをかき集めてきているので、ご参考程度に見ていただければいいですけれども、発見されるまでに非常に時間がかかっているということを頭の片隅に置いていただければと思います。