2014年4月9日

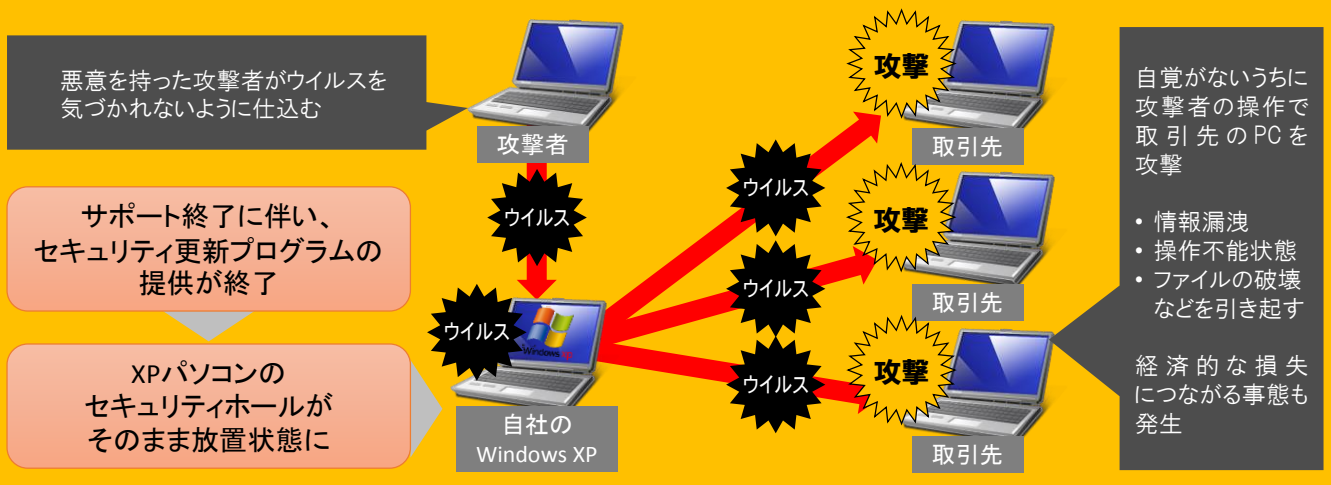
Windows XP サポート終了

他人事では済まされないセキュリティのリスク

こんな誤解をしていませんか？

サポートが終了しても **まだまだ使えるから** 大丈夫	漏洩して困るような **機密情報がないから** 大丈夫	**ウイルス対策ソフトが入っているから** 大丈夫
セキュリティ更新プログラムの提供が終了し、脆弱性が飛躍的に向上するため、ネットワークに接続して利用することは非常に危険です。攻撃者の格好の的となるためです。	メールのアドレス帳にある取引先の連絡先なども重要な機密情報です。また、自社のPCが踏み台となって、取引先にウイルスを勝手に送りつけることもあります。	セキュリティ上の脅威には、OS更新プログラムの適用、マルウェア対策をはじめとする多角的な防御策が必要です。ウイルス対策ソフトだけで対応することは、もはや困難です。

サポート終了に伴う、セキュリティのリスク例



サポートが終了するOSの継続利用に伴うリスク

Windows XPのサポート終了を受け、Windows XP上の様々なソフトウェアのサポートが終了し、機能改善と脆弱性対策が終了します。

このことは、攻撃者にとっては好都合で、脆弱性を見つけた場合は、広く応用でき、修正されることもありません。攻撃者は攻撃への対策が甘い方を狙った方が目的をかなえることが容易なので、広く使われているXPは格好の攻撃対象になります。

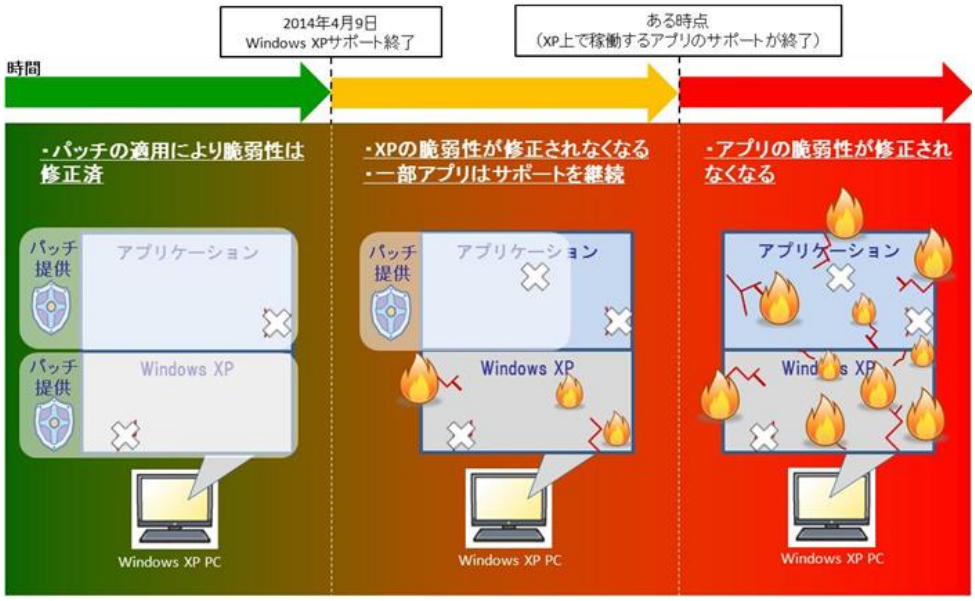


図1:XPサポート終了以降のリスクの変遷イメージ

Windows XPは脆弱性対策が行われている、今の状態でも、マルウェア感染率は最新のWindows 8の6倍以上だとする報告があります。

このような危険と隣り合わせのパソコンを使い続けることが以下のことが発生する可能性があり、特に事業者は事業そのものを失うことにつながります。

- ✗ 取引先メールアドレスが流出する
- ✗ 蓄積されたメールの情報が流出する
- ✗ 電子ファイルが流出する
- ✗ 蓄積されたメール情報が消去される
- ✗ 電子ファイルが消去される

一般に深刻なのは個人情報の流出とされており、1件あたり平均で3787万円もの損害賠償が発生するという調査結果があるほどです。しかしながら、失うものは信用です。自社を経由してウイルスが広がった場合も、取り引き先様の信用を失います。

外部への被害が無かったとしても、XP購入の頃から蓄積された、重要な記録や電子書面を失うことで、事業の継続が困難になります。

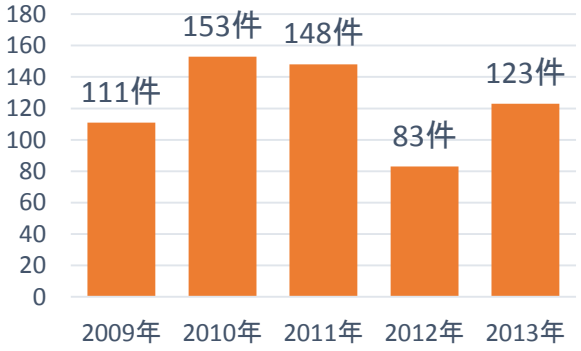


図2:Windows XPの既知の脆弱性の件数

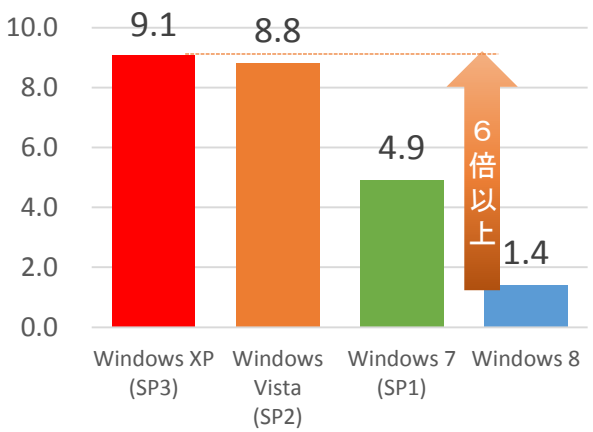


図3:2013年第二4半期のOS別マルウェア感染率
「マイクロソフトセキュリティインテリジェンスレポート」
第15版より

銀行取引、クレジットカードでの決済など「お金を電子的に扱う」ことが増えています。この分野に使うパソコンとしてXPを使い続けることは事故を待つようなものです。

このような、状況であることをご理解いただき、それでも尚XPを使う必要がある場合は、パソコン購入以上の費用がかかりますが、延命対策を行うことはできます。

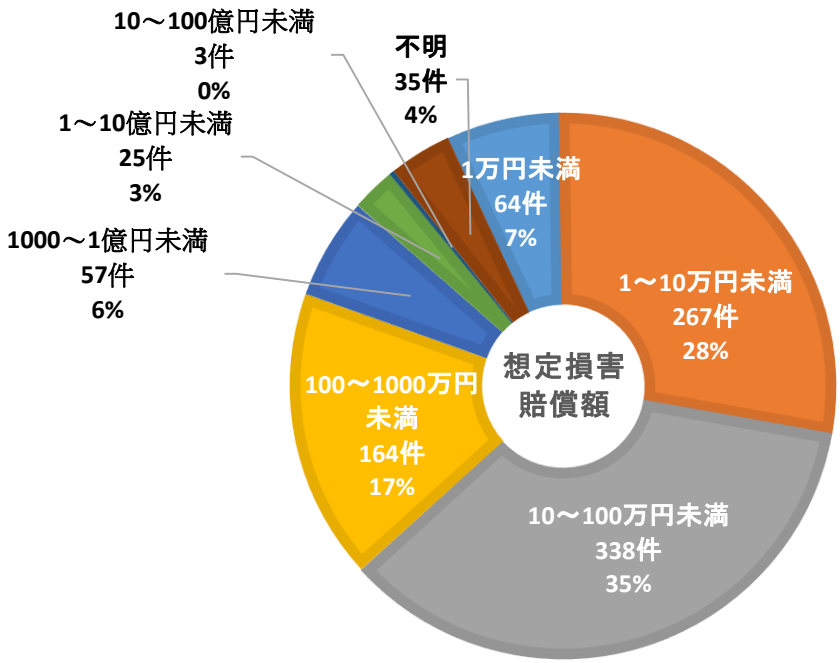
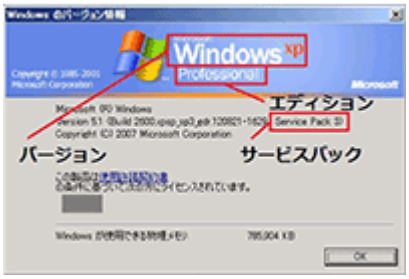


図4：個人情報漏えい事故1件当たりの想定損害賠償額
「2012年 情報セキュリティインシデントに関する調査報告書【上半期 速報版】Ver.1.1」NPO日本ネットワークセキュリティ協会 セキュリティ被害調査ワーキンググループ 情報セキュリティ大学院大学 原田研究室 廣松研究室より

2014年4月9日にサポートが終了する製品

Windows XP

■バージョンの確認方法
1. [スタート] メニューから [ファイル名を指定して実行] をクリックします。
2. 2.winver と入力し [OK] をクリックするとバージョンが表示されます。



Office2003

■バージョンの確認方法
1. Word、Excel などの Office 製品を起動します。
2. [ヘルプ]、[バージョン情報] をクリックするとバージョンが表示されます。

Internet Explorer 6

■バージョンの確認方
1. Internet Explorer を起動し、[ヘルプ] メニューから [バージョン情報] をクリックすると、バージョンが表示されます。

マルウェアとは：
コンピュータの利用者が意図しない動作をする不正なプログラムをマルウェアと呼んでいます。具体的にはコンピュータウイルス、個人情報を盗むキーロガーやリモートから不正にパソコンを操作するバックドアなどのスパイウェア、強制的に広告を表示するアドウェア、嘘の情報で購入を促す偽セキュリティ対策ソフト、アダルトサイト等の請求画面を表示しつづけるワンクリウェアなどが含まれます。

対策1：OSの移行

OSの移行には、予算や移行期間などにより複数の選択肢があります。ご自身の環境にあった方法で早期の移行をすることをおすすめします。

現状PCの使用を続ける場合でも、古いハードウェアはハードディスクの故障時期も近くなっていることになるので、計画的にPCの入れ替えを計画することを推奨します。

1 PCを買い替える

十分な予算が確保できる場合には、Windows7/8を搭載したPCへの買い替えが望ましいでしょう。

2 PCは買わずにアップグレード

現状のPCがシステム要件を満たしている場合には買い替えずに、OSやアプリケーションをアップグレードできます。

3 現状PCをリフォーム

現状のPCがシステム要件を満たしている場合に、工場出荷状態にクリーニングしてOSからセットアップを行います。

4 リサイクルPCを利用する

現状のPCを下取りに出し、それよりも状態の良い再生中古PC購入して最新OSを使用する方法もあります。

Windows 8/8.1 システム要件

- CPU: PAE、NX、SSE2 をサポートする 1 GHz 以上のプロセッサ
- メモリ: 1 GB (32 ビット) または 2 GB (64 ビット)
- ハード ディスクの空き領域: 16 GB (32 ビット) または 20 GB (64 ビット)
- グラフィックス カード: Microsoft DirectX 9 グラフィックス デバイス (WDDM ドライバー付き)

対策2：リスク緩和策

やむを得ない事情により移行が間に合わない場合には、リスク緩和策を取りつつ、移行計画を立てて速やかに移行を進めることを推奨します。

■ オフラインの利用に切り替えられる場合

1. Windows XP の使用はオフラインに限定する
2. USBメモリなどの外部情報媒体の自動実行機能を無効化する等、ネットワーク以外からの攻撃リスクを低減するための対策を行う

   「自動実行（オートラン）」機能を悪用し、USBメモリなどを経由して感染を広げる「USBメモリ感染型ウイルス」の被害が続いています。この種のウイルスに対しては、パソコンの「自動実行」機能を無効化することが有効な対策となります。
   詳しい手順等は、IPA独立行政法人情報処理推進機構の『Windowsでの「自動実行」機能の無効化手順』のページ
   http://www.ipa.go.jp/security/virus/autorun/ をご参照ください。

■ オンラインで利用せざるを得ない場合

1. サポートが継続しているウィルス対策ソフト、マイクロソフト社の無償ツールEMET等の攻撃対策ツールを活用し、攻撃の検知・回避を行う
2. サポートが継続しているアプリケーションを最新に保ち、サポートが終了したアプリケーションは代替アプリケーションに切り替える

監修・作成：株式会社匠技術研究所

アプリケーション、OS、ネットワーク全般をトータルに判断して最適な移行方法を提案します。買い替えるだけでなく、継続利用が必要なものは安全に使えるようにし、コストを抑える工夫をいたします。
是非一度ご相談ください。

情報をつなぎ、人を結ぶ

神奈川県川崎市麻生区多摩美1-12-11　https://www.takumigiken.biz/　電話　044-959-5612