Windows　Office

Windows XP/Office 2003 をご利用のお客様へ

サポート終了の重要なお知らせです。

他人事では済まされないセキュリティのリスク

ある日突然、取引先に被害を与えるかもしれない…。サポート終了に伴う、セキュリティのリスクとは?

昨今、メディアで取り上げられることも多い、ウイルスや不正アクセスによるサイバー攻撃。にもかかわらず「うちは関係無い」「個人情報は所有していないから大丈夫だ」「ウイルス対策ソフトを入れている」といった考えで、ついつい他人事としてとらえがちではないでしょうか?
Windows XP/Office 2003 のサポートが終了すると、セキュリティの脆弱性が大きくなるため、これを機に、悪意をもった攻撃者達が、静かに広範囲な攻撃を開始すると想定されています。これらの攻撃によって、あなたの会社の情報が漏洩するだけではなく、知らず知らずの間にサイバー攻撃の「踏み台」となって、大事な取引先に多大な被害を与えることも、十分に起こりえるのです。

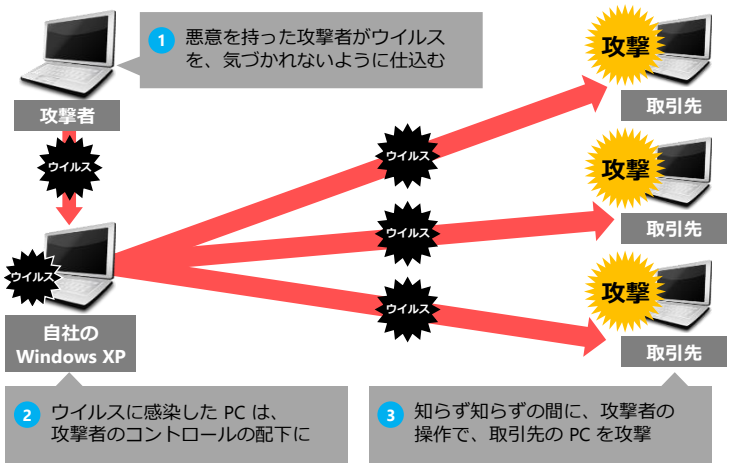
サポート終了に伴う、セキュリティのリスク例 (標的型攻撃)

サポート終了に伴いセキュリティ更新プログラムの提供も終了

悪意をもった攻撃者が、静かに、かつ、広範囲に攻撃を開始

知らず知らずの間に踏み台となり、自社の PC が取引先を攻撃・・・

取引に影響を与えることも



こんな誤解をしていませんか?

ご注意ください!

サポートが終了しても、まだまだ使えるから大丈夫

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。

漏洩して困るような機密情報がないから大丈夫

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。

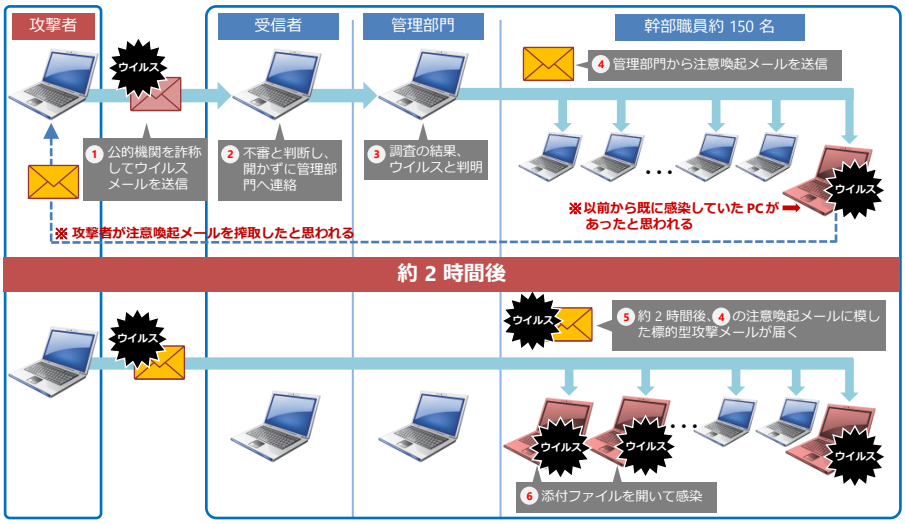
ウイルス対策ソフトが入っているから大丈夫

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。

セキュリティ事故で甚大な経済的損失を被らず、安心して IT を活用していただくためには、2014 年 4 月のサポート終了までに、最新版の Windows と Office に移行する必要があります。

詳しいや移行方法やよくあるご質問はこちらまで　http://aka.ms/xp_sec

身近に起こった攻撃の実例

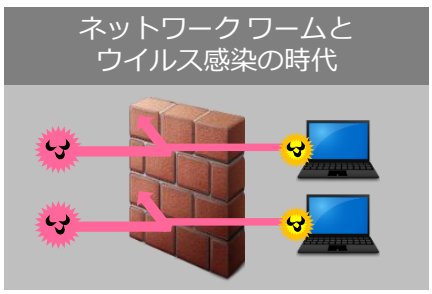


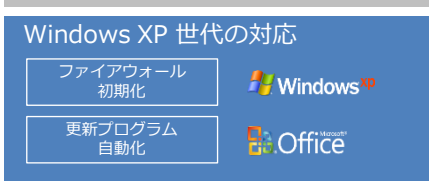
1. 最初に、官公庁や公的機関を詐称して、実行形式のウイルスを添付した標的型攻撃メールが 2 通届いた。
2. 不審なメールと判断した受信者はメールの添付ファイルを開かず、被害に遭わなかった。
3. 連絡を受けた管理部門が添付ファイルを調べると、キー ロガー機能を持つウイルスと判明した。
4. 管理部門より、1 の標的型攻撃メールに関する注意喚起をテキスト本文のみのメールで、海外拠点を含めた幹部職員約 150 名に送った。
5. 約 2 時間後に、4 の注意喚起メールを加工して、ウイルスを埋め込んだ PDF ファイルを添付した標的型攻撃メールが同じ 150 名に届いた。
6. 正規の注意喚起メールと信じた約 10 名の受信者が添付ファイルを開き感染してしまった。

※「IPA テクニカル ウォッチ標的型攻撃メールの分析に関するレポート」より

この事例では、組織内に限定した業務連絡メールを加工していることから、少なくとも 1 人以上の職員のメールがすでに窃取されていたと考えられる。標的型メール攻撃は、数カ月から数年続いている場合が多く、このインシデント以前に、すでに標的型攻撃メールの被害に遭っていた職員がいた可能性がある。

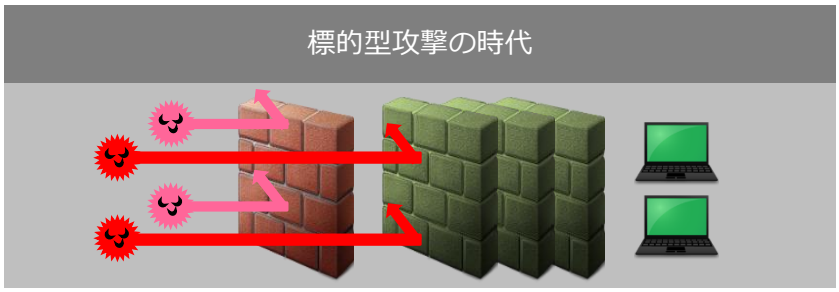
変化するセキュリティの脅威への対応

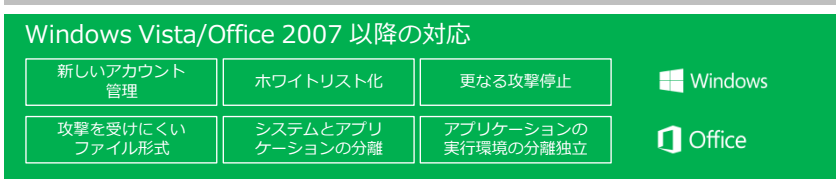




愉快犯の時代

無差別に自動で感染を広めようとするウイルスで、インターネットにアクセスしただけで感染するものもあるが防御策もたてやすい。ファイアウォールや脆弱性を防ぐ更新プログラム、ウイルス対策ソフトなどで対策が可能。
(例: 2003 年のブラスター)

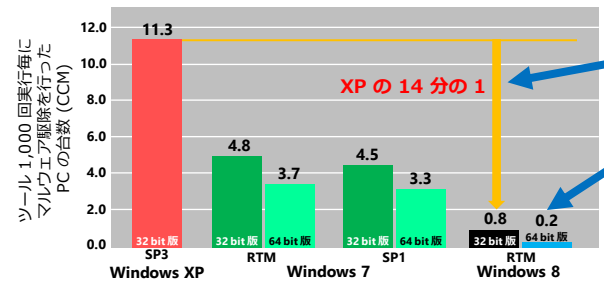




標的型攻撃へ変化

あたかも実際の要件のような件名のため、添付ファイルを開き、かつ、気づかないうちに感染。そこから、更に感染を広げるようなウイルスを自動的にダウンロードし、踏み台となってウイルスをまき散らすこともある。最新の Windows では、不正なプログラムを動作させない「**新しいアカウント管理**」や「**ホワイトリスト化**」を実装。また、最新の Office では、ウイルスを組み込むことが困難な「**攻撃を受けにくいファイル形式**」の採用や、万が一ウイルスが組み込まれても、システムに影響を与えずにファイルを開くことのできる「**システムとアプリケーションの分離**」の仕組みなどを導入。これらの「多層防御」により、日毎高まる脅威に対応している。

新しい Windows ほどマルウェア感染率は低い



Windows 8 の感染率は Windows XP SP3 と比較して 14 分の 1

過去から一貫した傾向として、より新しいオペレーティング システム/サービス パックほど感染率は低い

※出典: 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 14 版

製品に関するお問い合わせは、次のインフォメーションをご利用ください。

■ インターネット ホームページ **http://www.microsoft.com/ja-jp/**
■ マイクロソフト カスタマー インフォメーション センター **0120-41-6755** (9:00 ～ 17:30 土日祝日、弊社指定休業日を除きます)
■ マイクロソフト ボリューム ライセンス コールセンター **0120-737-565** (9:00 ～ 17:30 土日祝日、弊社指定休業日を除きます)

※携帯電話からでもご利用いただけます。電話番号のおかけ間違いにご注意ください。

Microsoft

日本マイクロソフト株式会社
〒 108-0075　東京都港区港南 2-16-3 品川グランドセントラルタワー