

マイクロソフト社オフィス製品に関連した 脆弱性と脅威の動向

- オフィス関連製品を介した脅威が増大傾向 -



初版 2007/02/13

1.02 版 2007/02/15

株式会社ラック

コンピュータセキュリティ研究所

目次

1. はじめに	3
2. 概要	3
3. 調査結果	4
4. 脅威	5
5. 対策	6

1. はじめに

本レポートは、当社脆弱性データベース(SNSDB)¹の情報、及び CVE²を基に、2006 年度までの脆弱性情報を調査し、近年における脆弱性(セキュリティ上の欠陥)と脅威の傾向を調査した結果を記している。本書が、情報セキュリティに対する啓発の一助として、読者の組織において有効に活用して頂けると幸いである。

※ 尚、本文書の利用は全て自己責任の下でお願いいたします。

本文書に記述を利用した結果生じるいかなる損失についても株式会社ラックは責任を負いかねます。

2. 概要

当社コンピュータセキュリティ研究所(以降、CSL)において、昨年度のソフトウェアにおける脆弱性の報告傾向を調査した結果、マイクロソフト社オフィス製品での”重大レベル”での脆弱性は、2005 年度の 6 件に対し、2006 年度は 24 件と 4 倍になっていることが判明した。(SNSDB)

中でも特筆すべき点は、マイクロソフト社が修正プログラムを公開する前に、攻撃が行われた、または、攻撃手法が確立された(所謂ゼロデイ)件数が、2005 年度は 0 件だったのに対し、2006 年度では 8 件と急増している点である。(脅威の増加)

CSL では、これらの脆弱性と脅威が急増した背景として、個人情報を狙った組織的な動きがあると推測しており、脆弱性売買ビジネス³などがその典型と捉えている。インターネット上の仮想空間では、現実社会よりも一足先にグローバル社会が現実のものとなり、すでにボーダーレスが当たり前の社会となっている側面もある。今後予想される現実社会の環境変化を考えると、マイクロソフト社製品のように大きなシェアを持っているソフトウェアは、攻撃者の格好の標的となると考えられ、今後も増加の傾向をたどると推測する。

これら攻撃者の傾向は、3S(狡猾 Shifty 見えない Stealth 標的 Snipe)となってきた。従来のように、遠隔から明らかに分かる手口で大規模に攻撃を行うのではなく、ユーザの日常操作に紛れ込むことで攻撃する傾向が強くなってきている。その代表的な手口として、圧倒的に利用者が多いオフィス製品の脆弱性が悪用されていると推測する。

¹ SNSDB http://www.lac.co.jp/business/sns/products/sns_db/index.html

² CVE <http://cve.mitre.org/>

³ 「IBM Internet Security Systems X-Force」の調査による http://www.iss.net/x-force_report_images/index.html

3. 調査結果

マイクロソフト社オフィス製品の脆弱性件数の推移は下図の通りである。これを見ると2005年以前と比較し、2006年は脆弱性の報告件数が急激に増大していることが分かる。また2006年中に報告のあった脆弱性が、ゼロデイであった割合をみるとWordに関するものが最も多い。ここでカウントしているゼロデイは公になったもののみであり、水面下にはさらに多くの脆弱性が存在するものと考えられる。

また、以前から攻撃者の標的になっているInternet Explorerに関しては、重大な脆弱性は2005年22件、2006年21件であり、ゼロデイに関しては、6件ずつとほぼ横ばいの結果であった。

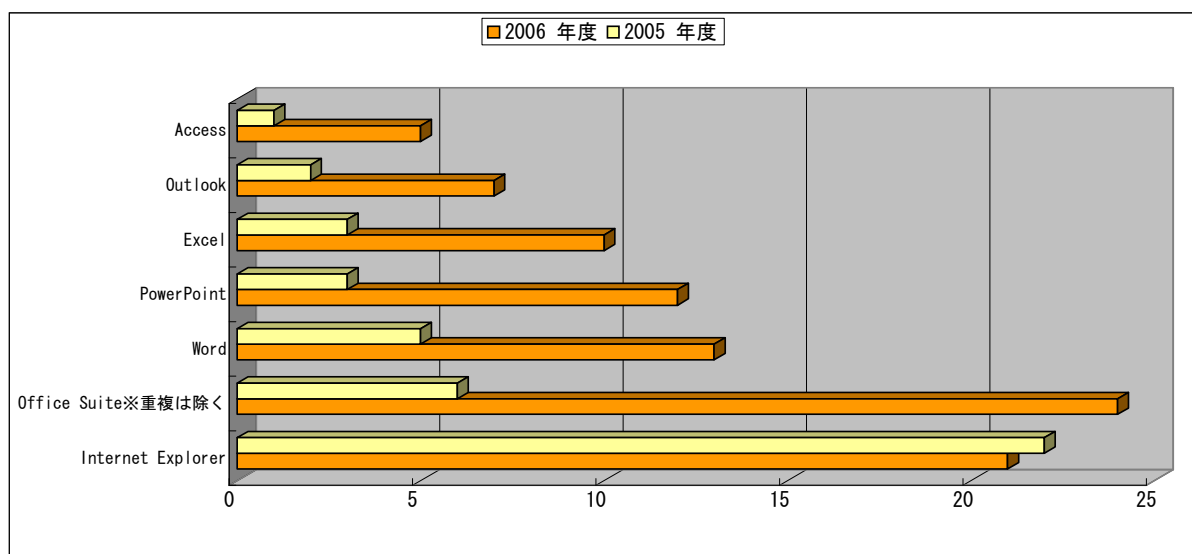


図1 脆弱性報告数(SNSDBでの比較)

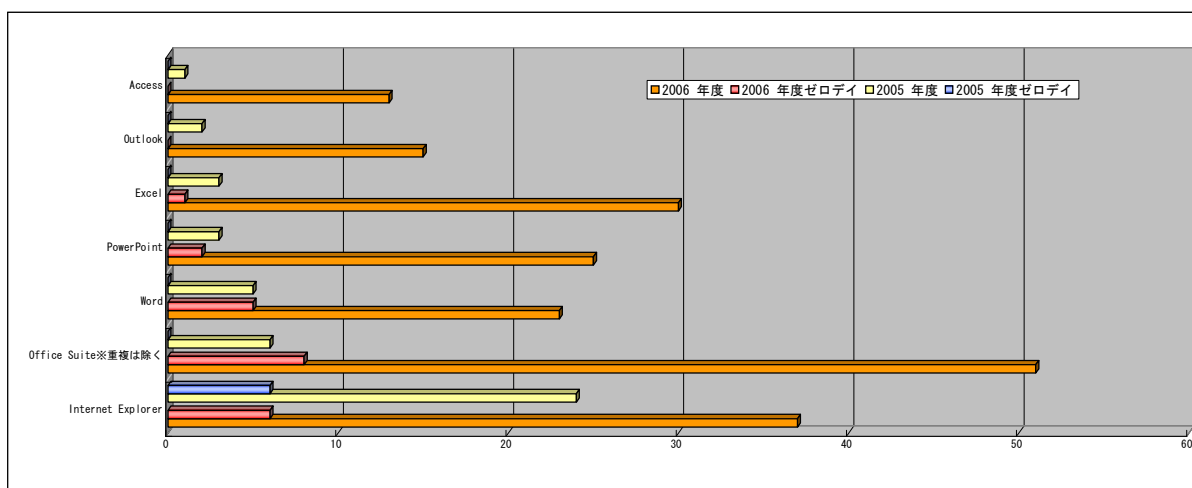


図2 脆弱性報告件数とゼロデイ件数(CVE)

4. 脅威

ゼロデイの発生が急増している為、仮に従来から推奨されている Windows アップデートや一般のウイルス対策を行っていたとしても、不正プログラムを組み込むように巧妙に細工されたドキュメントファイルをオフィス製品で閲覧した際に、スパイウェアやボット等の不正プログラムが利用者のパソコンに組み込まれ、以下に示すような危険性が增大している。

- (1) スパイウェア等が組み込まれ、情報流出が発生する
- (2) ボット等が組み込まれ遠隔から不正な操作を強いられる

これらの攻撃は、フィッシング詐欺や標的型攻撃と同じように、特定組織や特定の行動パターンを持った個人ユーザが標的となる危険性が高く、詐取される情報はキーロガー等による ID やパスワード情報などが考えられる。また、組織が対象となる場合、政府やその関係機関・金融機関・大手企業・研究機関などの内部情報が流出し、金銭で売買されてしまうことが考えられる。

5. 対策

このような脆弱性を狙った攻撃の多くは、細工が施されたドキュメントファイルを利用者に閲覧させることにより行われる。つまり、利用者にファイルを閲覧させるために様々な誘導手口を用いているということである。このような誘導手口に引っかからないように、万一引っかかってしまっても被害を最小限に抑えるために、以下の対策を推奨する。

- (1) メールに添付されてきた、または、ウェブサイト等からダウンロードした不審なドキュメントファイルは決して触れないこと。送信者が知り合いであるならば、別途問い合わせしメール本文に記載してもらうなどの工夫をする。
- (2) どうしても不審なドキュメントファイルを見る必要がある場合、消極的な対策ではあるが、危険を少しでも減らす為にマイクロソフト社以外の攻撃者が標的にしていないマイナーなソフトウェアを使用する。
- (3) マイクロソフト社 Windows Vista に OS を変更することで、ASLR 機能によりある種の欠陥 (Buffer Overflow などメモリの上書きによる攻撃手法) に対して耐性を持たせることが出来る。
- (4) 複数のウイルス対策ソフトにより確認する。例えば、VirusTotal.com などのサイトでは、無料で複数のウイルス対策ソフトウェアに対してスキャンを行うことが可能である。

VirusTotal <http://www.virustotal.com>

上記に加え、従前から言われている以下の対策は必須である。

- (5) ウイルス対策ソフトを使用する。その際に、定義ファイルは最新のものを使用する。
- (6) Windows は常に最新の状態で使用する。
- (7) Windows のファイアウォール機能を有効にする。

また、組織全体としての対策としては、以下の対策も効果的である。

- (8) ファイアウォールにて外向きの通信を分析し、不正プログラムの活動を発見する。
※但し、80/tcp を悪用される場合が多いため、URL フィルタリングや IPS 等と組み合わせるとさらに効果的
- (9) ファイルサーバ等のような、多数のユーザがアクセスするサーバに対するアクセス制御、及びロギング。

残念ながら、これらの対策を行っても完全にはならず、最終的には人的制御が課題となる。将来的には、明確な不正プログラムの組み込みへの対処は技術的な方法だけで万全となる可能性もあるが、コンピュータプログラムが高機能に、使い勝手よく、人間系に近づけば近づくほど、近年増加している「攻撃者に悪用されかねない不適切な仕様」を悪用した手口へのシフトは益々加速することが予想され、一人ひとりの注意が必要なことは当面続くと推測する。また、マイクロソフト社に限らず限らず一般消費者の利用を想定したソフトウェアを開発する組織ならびに個人は、これまで以上に、品質やセキュリティ上の欠陥への対応や利用者への適切な告知を通じ、攻撃者につけ込まれないように活動していくことが肝要と考える。

以上