

進化するウイルス 対策の常識が変わる

日経パソコン編集長

PC Online編集長

藤田 憲治

今日お話しすること

- 最近のウイルスの動向について
- ウイルスの最新手口と脅威
- 日経パソコンが実施したウイルス対策ソフトの性能テストの結果
- これからのウイルス対策

急増する新種・亜種のウイルス

●20年間分の2倍が1年で出現



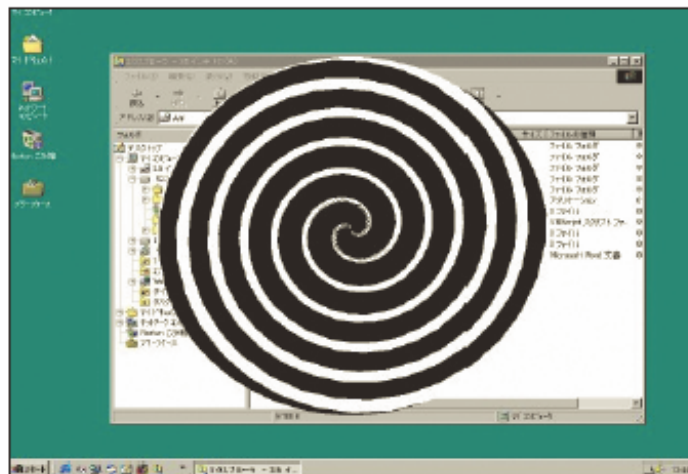
初めて1万種類を超えたのが1991年。しばらく1万から3万台を上下。

1997年に13万種類と急増し、2004年まで十数万台を増減。

2005年に前年の2倍以上となる33万種類、2006年に97万種類、2007年に5倍以上となる549万種。

2008年については未公表。2007年の3倍以上になると見積もっているところもある。

何故、ウイルスは激増したのか？



2000年ごろまで、ウイルス作者の主な目的はいたずら。画面上に画像などを表示して驚かしたりすることを目的としていた

ばれないように活動。大規模感染は起こさない

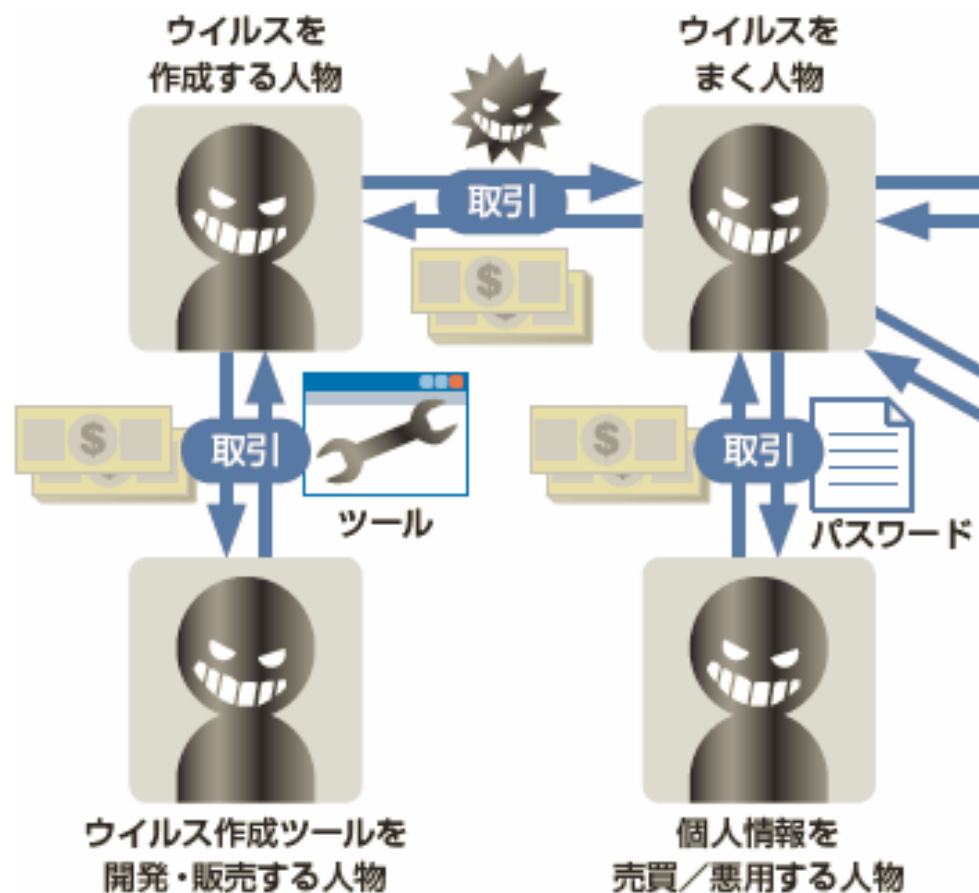
目的が「金もうけ」に変化

- ・PCに保存したクレジットカード情報や個人情報などをウイルスを使って盗み出し、お金に換える
- ・ウイルスでPCを乗っ取り、それらを貸し出すビジネスも
- ・感染パソコンを借りるのは、主に迷惑メール送信事業者
- ・多数の感染パソコンを踏み台にして迷惑メールを送信

ウイルス作者のやる気がアップ

2004年以降

ウイルスの作成・流通がビジネスに



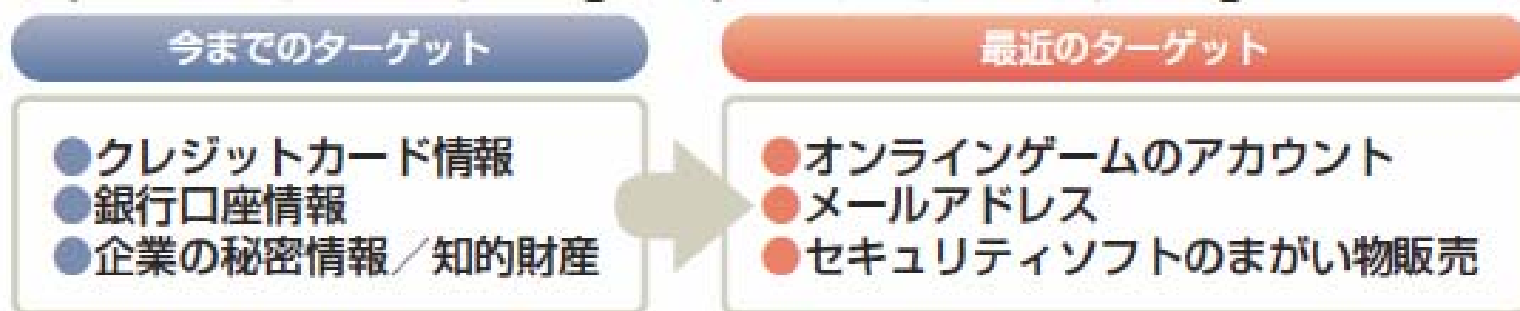
ウイルスがお金になることが分
かると、犯罪組織などが相次い
で参入。ウイルスはビジネス
ツールの一つになった。組織化
と分業化が進み、現在では、ウ
イルス作者と、ウイルス感染パ
ソコンを悪用する人物は異なる
ことがほとんど。ウイルスやウ
イルス作成ツール、ウイルス感
染パソコンなどは金銭で取引され
ている

闇市場で売買される「商品」

| 商品／サービス | 価格／料金 |
|-------------------------------------|-------------------------------------|
| 銀行口座情報 | 10ドルから1000ドル |
| クレジットカード情報(セキュリティコード付き) | 50セントから12ドル |
| クレジットカード情報 | 10セントから25ドル |
| メールアドレス | 1MB(およそ4万件)当たり30セントから40ドル |
| メールアカウントのパスワード | 4ドルから30ドル |
| 個人情報ひとそろい(住所、氏名、生年月日、電話番号、社会保障番号など) | 90セントから25ドル |
| 商品の換金サービス | 商品価格の8%から50% |
| 詐欺サイトのホスティング | 1週間当たり2.5ドルから100ドル(サイト作成は5ドルから20ドル) |

この表は、米シマンテックが2008年11月に公開した調査資料の情報を基に作成(調査期間は2007年7月から2008年6月まで)
闇市場の一つは「インターネット・リレー・チャット(IRC)」

今の流行は「コツコツ」稼ぐ



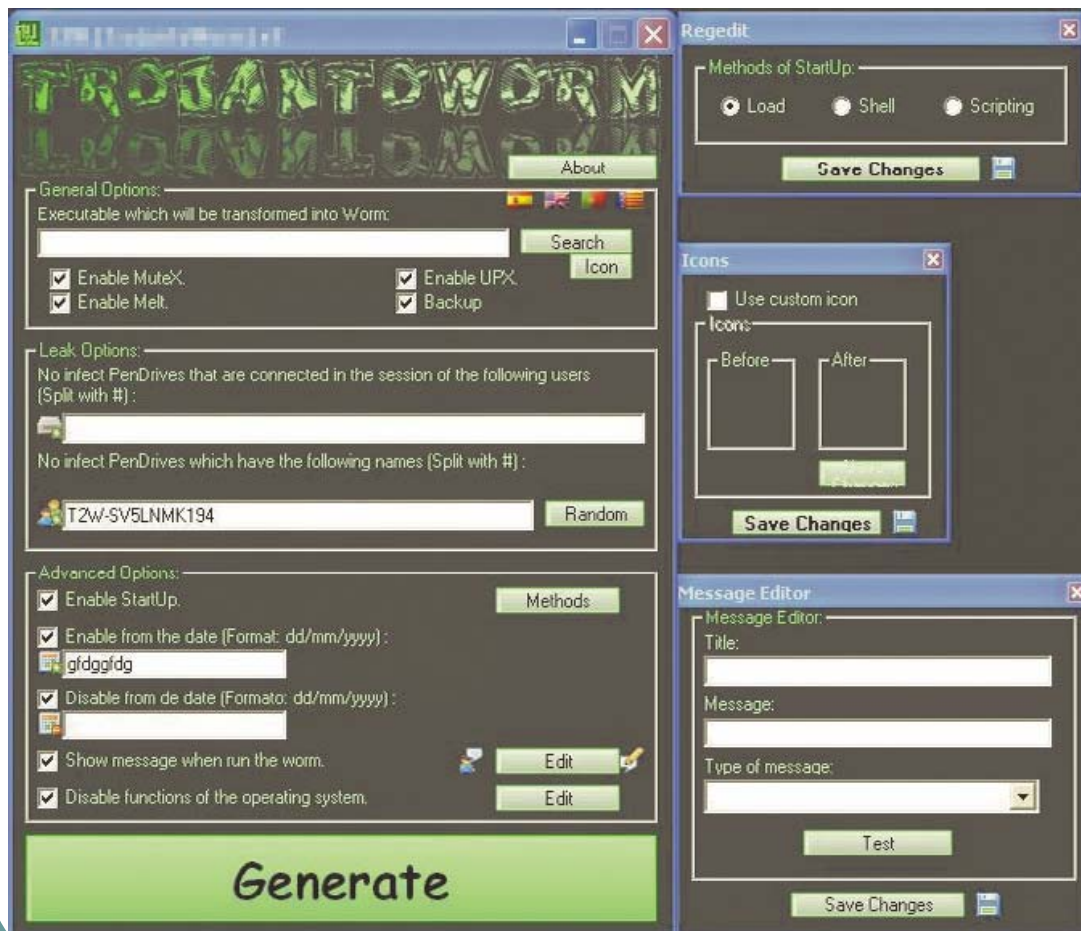
カード情報や口座情報は、金額的には大きいものの、捕まりやすい。リターンは大きいですが、リスクも大きい。今は、金額的には小さいものの、捕まる可能性が小さいものにシフトしている。

その一例が、オンラインゲームのアカウント。盗んだアカウントでそのユーザーになりすまし、ゲームで使われている仮想通貨やアイテムを、別のユーザーや仲介業者に販売してお金に換える。

メールアドレスもその一つ。価格は安いですが、ばれる恐れはほとんどない。メールアドレスは多数のユーザーに知らせておくものなので、流出に気付いたとしても、ウイルスに盗まれたとは思わない。

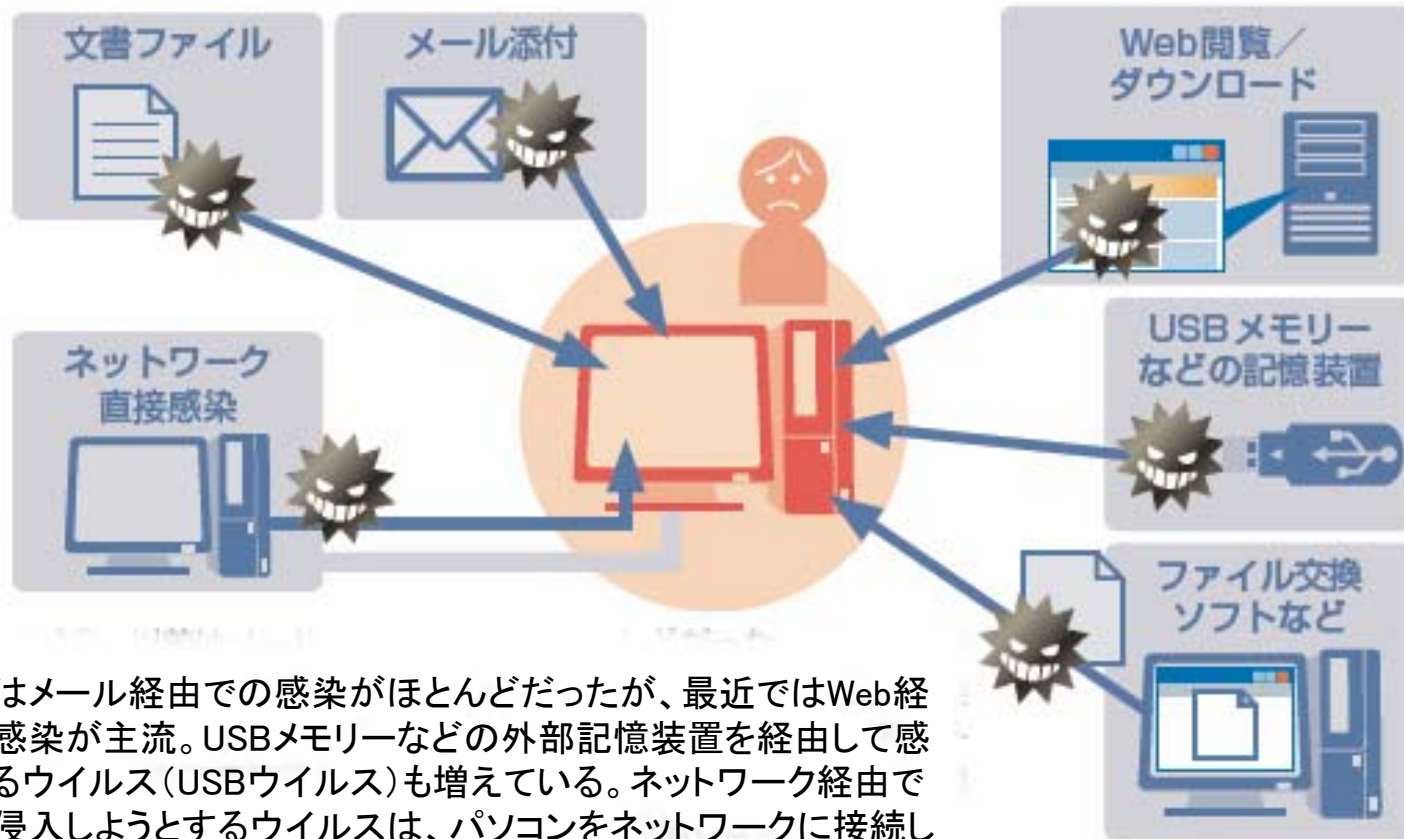
ウイルスに感染したパソコンのユーザーに、自発的にお金を払わせる手口もある。偽ソフト(セキュリティソフトのまがい物)を売りつけるのだ。攻撃者はユーザーをだまして、ウイルスの一種である偽ソフトをインストールさせる。偽ソフトは偽のウイルス警告を表示。ウイルスを駆除したければ、お金を払って有料版を購入するよう迫る。

誰でもウイルスを作れる？



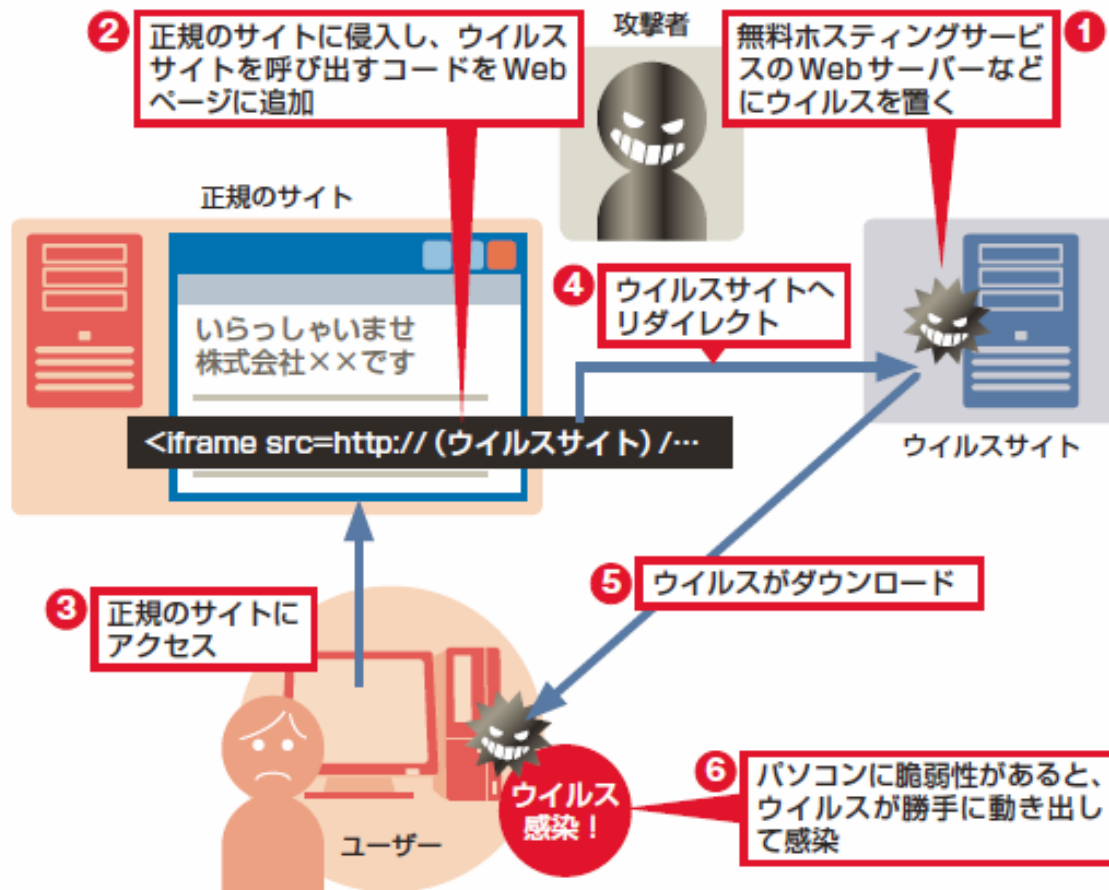
ウイルス作成ツールの一例。新種を次々と生み出せるのは、こういったツールが出回っているため。ツールを使えば、スキルのないユーザーでも、複雑な挙動をする新種ウイルスを簡単に作成できる。以前は、多くのツールがインターネットで公開されていたが、最近では商品として売買されることが多い

ウイルスはどこからでもやって来る



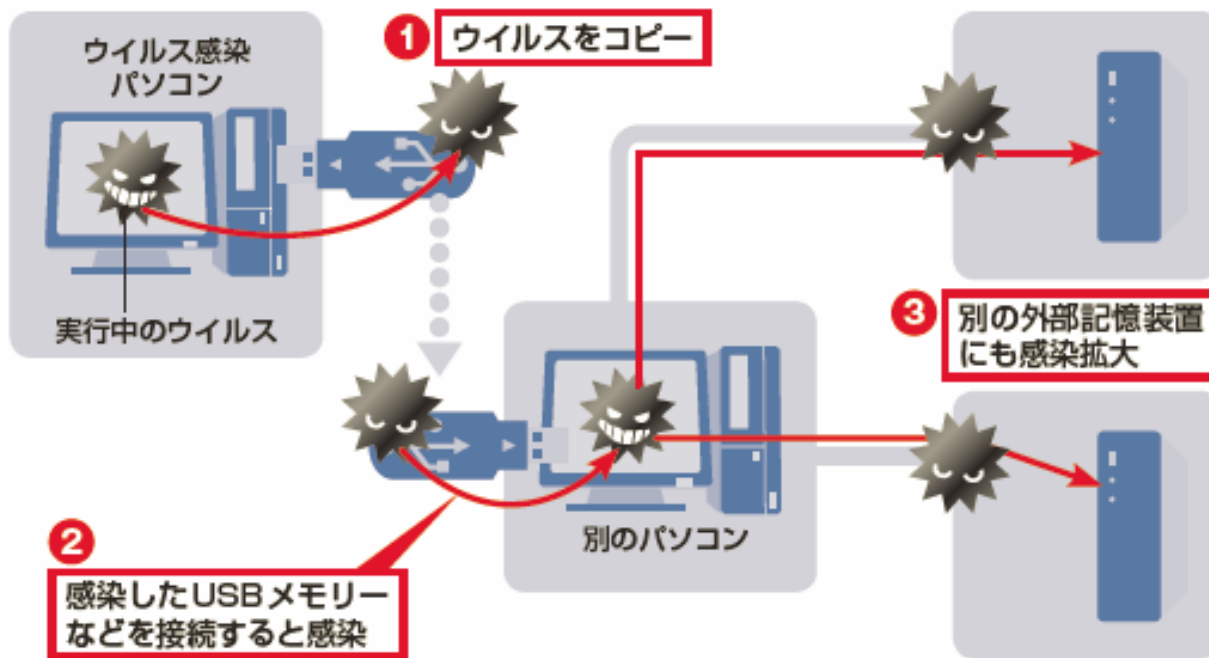
以前はメール経由での感染がほとんどだったが、最近ではWeb経由の感染が主流。USBメモリーなどの外部記憶装置を経由して感染するウイルス(USBウイルス)も増えている。ネットワーク経由で直接侵入しようとするウイルスは、パソコンをネットワークに接続しただけで感染する恐れがある

有名企業や組織のサイトを乗っ取る



有名な企業や組織のサイトが不正侵入されて、Webページが改ざんされる事件が相次いでいる。特に、ブラウザやプラグインなどの脆弱性を悪用して侵入することが多い。「自分は怪しいサイトにアクセスしないので大丈夫」という声もあるが、それだけでは感染を防げない

PCにメモリーを接続するだけで感染



USB ウイルスの実体は、Windowsパソコンで動作するプログラム。USBウイルスに感染しているパソコンにUSBメモリーを接続すると、ウイルスは自分自身をコピー。コピーされたウイルスは“眠っている”状態で、そのままでは動作しない。そのUSBメモリーを別のパソコンに接続すると、Windowsの自動再生機能により、ウイルスがそのパソコンに読み込まれて動き出す。そのパソコンに別の外部記憶装置を接続すると、その装置にも感染が広がる

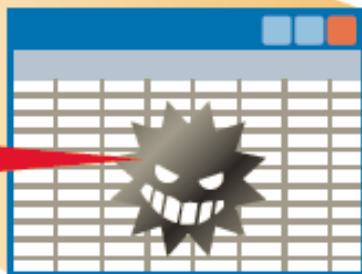
OfficeもPDFも、安全なファイルはない



細工が施された
文書ファイル

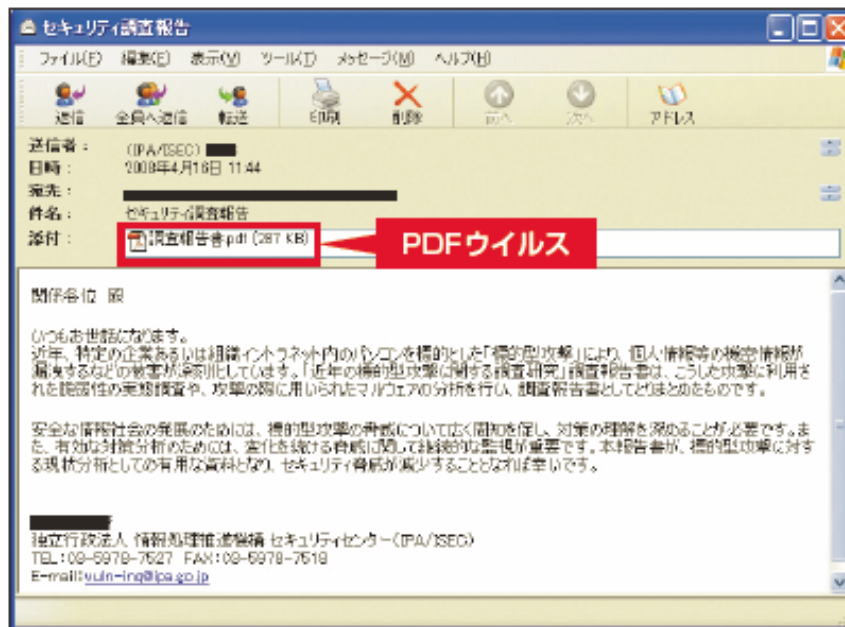
1 ファイルをオフィスソフト
で読み込んでオープン

2 脆弱性を突いて、
ファイル中の
ウイルスが起動



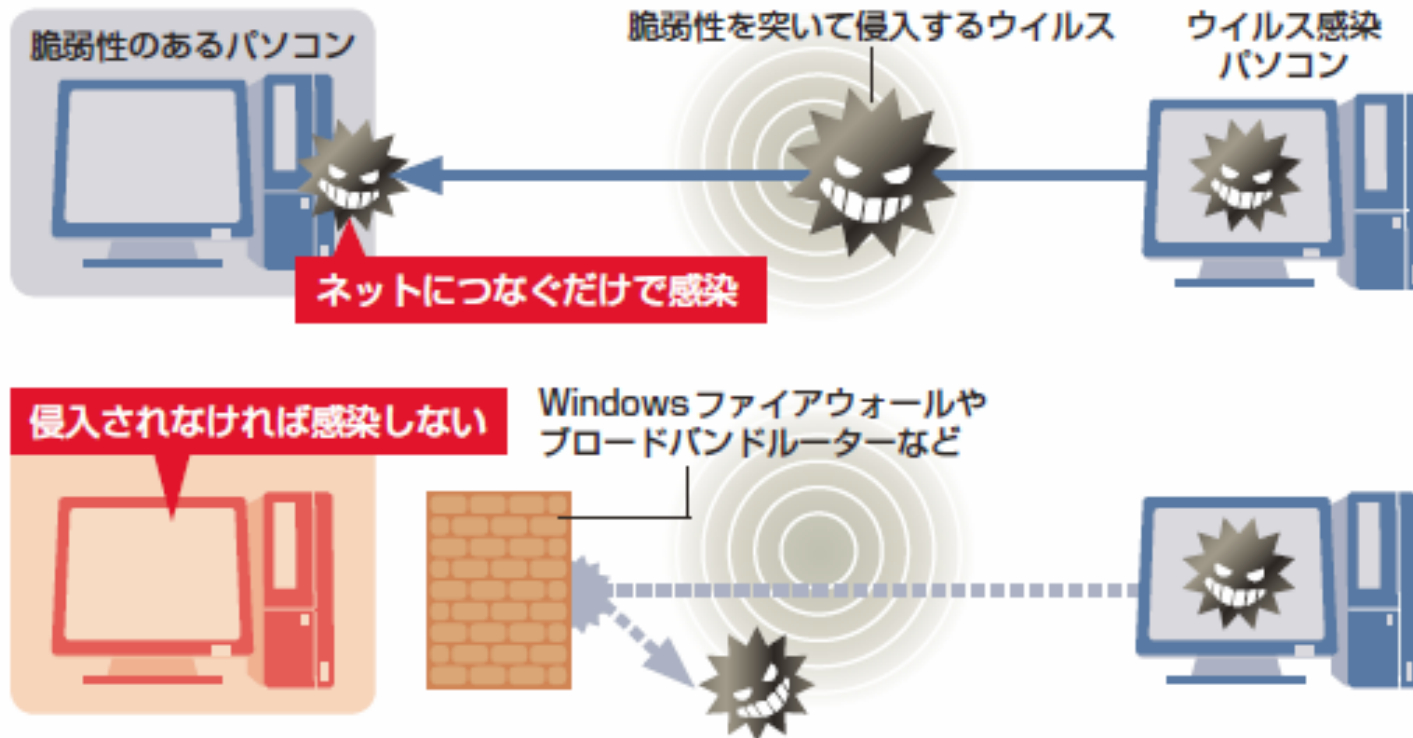
脆弱性のあるオフィスソフト

●IPAをかたる「PDFウイルス」出現



ウイルスの多くは実行形式(プログラム)。表向きは文書ファイルだが、中にウイルスが仕込まれていて、オフィスソフトなどの脆弱性を悪用して動き出す。2005年以降、マイクロソフトのOffice や 太郎などの脆弱性を悪用するウイルスが多数出現。2007 年以降になると、Adobe Reader の脆弱性を突く「PDF ウイルス」が続出

ネットにPCを接続しただけで感染



2003年に大流行した「ブラスター」や、2008年10月以降流行している「ダウンアド」のように、Windowsの脆弱性を突いて侵入しようとするウイルスは、ネットワークに接続しただけで感染する恐れがある。ファイアウォールやブロードバンドルーターを利用していれば、たとえ脆弱性があったとしても、ウイルスの侵入・感染を防げる

ウイルス対策ソフトは完璧ではない

- 日経パソコンで2008年9月に実施。代表的なウイルス対策ソフト7製品でテスト。
- 746種類の既知ウイルスの検出テストでは、7製品ともほぼ100%を検出
- 5285種類のウイルス（既知と未知の両方を含む）に対するテストでは、すべての対策ソフトが100%の検出率を達成できず。

未知ウイルスに対するテスト結果



ネットブックの流行で危険が...？

大ブームのネットブック。ネットブックを2万～3万円で買った人が、お金を出してセキュリティ対策ソフトを購入するのだろうか？また、1年ごとに更新するのだろうか？

無防備なネットブックが増えれば増えるほど、ウイルス作者は大喜び。セキュリティに対する注意喚起の必要性が高まっている。



最新のウイルス対策－7カ条



これからのウイルス対策（まとめ）

- ウイルス対策ソフトとパーソナルファイアウォールを導入
- セキュリティアップデートは確実に
- 「怪しそうな」サイトには近づかない
- 知らない人からのメールやスパムと思われるメールに添付されたファイルを開かない
- 問題が起こってもすぐに復旧できるように、まめにバックアップやリカバリー対策を

（システム管理者の皆様へ）

- 上記の対策を徹底するために
「検疫ツール」「資産管理ツール」などの導入、
アクセスするWebサイトも制限、バックアップを徹底

ご静聴ありがとうございました

引き続き、
日経パソコンならびに
PC Onlineを
よろしくお願い致します