IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2007 年 5 月 2 日
独立行政法人 情報処理推進機構

コンピュータウイルス・不正アクセスの届出状況［2007 年 4 月分］について

独立行政法人 情報処理推進機構（略称：IPA、理事長：藤原 武平太）は、2007 年 4 月のコンピュータウイルス・不正アクセスの届出状況をまとめました。

今月の呼びかけ：
「サポートが終了した OS を搭載した PC の危険性を認識しよう！！」
――　ぜい弱性(*1)が解消できず、被害に遭う可能性が極めて高い！！　――

現在、一般で広く利用されている PC の OS (オペレーティングシステム)として、Windows XP、2000、98/Me 等がありますが、Windows 98/Me は 2006 年 7 月に製造元のサポートが終了しています。

ぜい弱性とは？

情報セキュリティ分野においては、通常、システム・ネットワーク・アプリケーションまたは関連するプロトコルのセキュリティを損なうような、予定外の、望まないイベントにつながる可能性がある弱点の存在や、設計もしくは実装のエラーのことを言う。セキュリティ上の設定が不備である状態を指す場合もある。一般に、セキュリティホール（security hole)と呼ばれることもある。

しかし、当機構のウイルス・不正アクセスの相談受付状況を見ますと、Windows 98/Me の製造元によるサポートが終了した後でも、表 1 のとおり Windows 98/Me 利用者からの相談件数の割合は減少しているものの、まだ 1 割弱の方から相談を受けています。また、当機構のウイルスの届出受付状況をみますと、Windows 98/Me の製造元によるサポートが終了した後でも、表 2 のように Windows 98/Me のユーザからの届出が 2.5%ある状況です。

OS 種別	XP/Vista	98/Me	2000	Mac OS	Linux	その他
2006 年 4～7 月	82.5%	12.2%	3.2%	1.4%	0.0%	0.6%
2006 年 8 月～2007 年 3 月末	86.0%	9.0%	3.6%	1.2%	0.2%	0.1%
2006 年度通年	85.1%	9.8%	3.5%	1.3%	0.1%	0.3%

表 1：2006 年度 OS 種別相談状況

OS 種別	XP/Vista	98/Me	2000	Mac OS	Linux	その他
2006 年 4～7 月	72.5%	1.3%	5.0%	2.5%	2.5%	16.3%
2006 年 8 月～2007 年 3 月末	89.3%	2.5%	8.2%	0.0%	0.0%	0.0%
2006 年度通年	83.7%	2.1%	7.1%	0.8%	0.8%	5.4%

表 2：2006 年度 OS 種別ウイルス届出状況

一方、インターネット上には OS のぜい弱性(*1)を狙った悪意のあるプログラムが数多く存在していますが、それらは Windows 98/Me のサポートが終了した今でも、Windows 98/Me だけを対象としたものではありませんが、Windows 98/Me でも不正行為を行うことができる悪意のあるプログラムが確認されております。

以上のような状況を踏まえまして、今回サポートが終了した Windows 98/Me の利用の問題点等について緊急に呼びかけを行うこととといたしました。

参考：
マイクロソフト社の情報
Windows 98、および Windows Me に対するサポート終了のご案内
http://www.microsoft.com/japan/windows/support/endofsupport.mspx

サポートが終了した OS を搭載した PC を利用し続ける場合、以下のような問題が発生します。

(1)PC に新しいぜい弱性(*1)が発見されても、製造元からは修正プログラムが配布されません。ぜい弱性が発見されるたびに OS のぜい弱な部分が蓄積されていくこととなり、ぜい弱性だらけの PC になってしまいます。

(2)OS のサポート終了とともに、その OS の上で稼動するアプリケーションソフトの製造元もサポートを終了していくこととなります。特にウイルス対策ソフトは、製品自身のサポート終了とともにウイルスのパターン情報の更新もされなくなることが予想されることから、今後新たに出現する新種のウイルスに対応できなくなります。

(3)PC に何かトラブルが起きた場合、OS の製造元に問い合せてもサポート終了とともに「問い合せ対応」も終了することが多いため、OS のサポート終了後のトラブルについては自分で対応しなければならなくなります。

この様な状態の PC をインターネットに接続して利用した場合、以下のような被害が発生することが推測されます。

(1)「穴だらけの PC」をネットワークに接続した場合、当然ながらどこからでも自由に PC に侵入されてしまい、ウイルス感染、情報の漏えい等、いろいろな被害を受けることになります。しかも、通常はそれらの被害から PC を守るために導入しているウイルス対策ソフトも「ウイルスのパターン情報が更新されない」状態ですので、被害は広がるばかりになってしまいます。

(2)最近のインターネット上における攻撃は、ぜい弱性(*1)のある PC を狙ってくるのはもちろんですが、ぜい弱性のあるＰＣに不正なプログラムを埋め込み、そのＰＣを悪用してインターネットに接続している他の数多くのＰＣに迷惑メールを送りつけるなどの手口が増えてきています。このため、自分の PC のぜい弱性は自分自身の問題だけではすまなくなってきており、このような PC をインターネットに接続することは他の人にも迷惑をかけるということを認識してください。

サポートされていない OS に存在するぜい弱性を突く攻撃による感染例

したがって、サポートが終了した OS を搭載した PC を利用するということは、上述したように非常に危険な行為であるということをよく理解していただき、できることなら使用しないことが望ましいです。どうしてもお使いになりたい場合は、インターネットはもとより社内や家庭のネットワークにも接続しない状態で利用することをお勧めします。

今月のトピックス

1.コンピュータ不正アクセス被害の主な事例(届出状況及び被害事例の詳細は、5 頁の「2.コンピュータ不正アクセス届出状況」を参照)

・SQL インジェクション攻撃を受け侵入、ウェブページ改ざん
・フィッシングサイトを設置された

2.相談の主な事例 (相談受付状況及び相談事例の詳細は、7 頁の「3.相談受付状況」を参照)

・ウイルス対策ソフトで検知できない何かに感染？！
・Winny でダウンロードしたファイルからウイルス感染

3.インターネット定点観測(詳細は、別紙 3 を参照)

IPA で行っているインターネット定点観測について、詳細な解説を行っています。

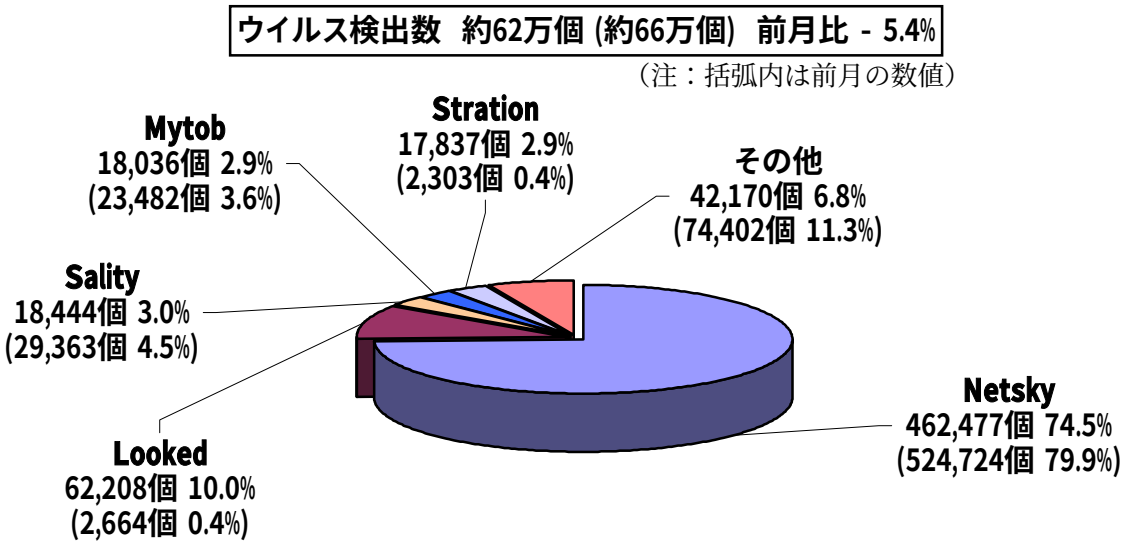
・ボットに感染したパソコンが多数存在！ ボット駆除ツールで検査を！

1．コンピュータウイルス届出状況　－詳細は別紙１を参照－

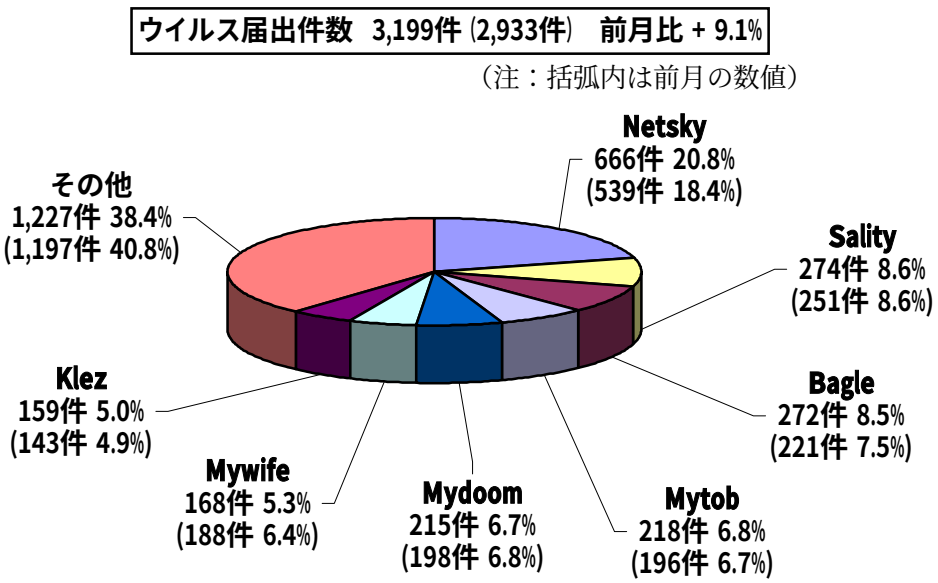
ウイルスの検出数(※1)は、**約 62 万個**と、3 月の 66 万個から 5.4%の減少となりました。
また、4 月の届出件数(※2)は、**3,199 件**となり、3 月の 2,933 件から 9.1%の増加となりました。

※1 検出数　：届出にあたり届出者から寄せられたウイルスの発見数（個数）
※2 届出件数：同じ届出者から寄せられた届出の内、同一発見日で同一種類のウイルスの検出が複数ある場合は、1 日何個検出されても届出 1 件としてカウントしたもの。
・4 月は、寄せられたウイルス検出数約 62 万個を集約した結果、3,199 件の届出件数となっています。

検出数の1位は、**W32/Netsky** で**約 46 万個 、2 位は W32/Looked** で**約 6 万個、3 位は W32/Sality** で**約 2 万個でした。**



図：1-1



図：1-2

2．コンピュータ不正アクセス届出状況（相談を含む）　－詳細は別紙 2 を参照－

不正アクセスの届出および相談の受付状況

		11月	12月	1月	2月	3月	4月
届出(a) 計		**24**	**10**	**32**	**23**	**13**	**15**
	被害あり(b)	8	9	22	14	9	12
	被害なし(c)	16	1	10	9	4	3
相談(d) 計		**30**	**40**	**52**	**50**	**43**	**31**
	被害あり(e)	20	23	25	28	20	20
	被害なし(f)	10	17	27	22	23	11
合計(a+d)		**54**	**50**	**84**	**73**	**56**	**46**
	被害あり(b+e)	28	32	47	42	29	32
	被害なし(c+f)	26	18	37	31	27	14

（1）不正アクセス届出状況

4 月の届出件数は 15 件であり、そのうち**被害のあった件数は 12 件**でした。

（2）不正アクセス等の相談受付状況

不正アクセスに関連した相談件数は 31 件（うち 4 件は届出件数としてもカウント）であり、そのうち何らかの被害のあった件数は 20 件でした。

（3）被害状況

被害届出の内訳は、**侵入 7 件、アドレス詐称 2 件、その他（被害あり）3 件**でした。

侵入届出の被害内容は、フィッシング(*2)に悪用するためのコンテンツを設置されていたものが 3 件、サイト内データの改ざんが 2 件、外部サイトを攻撃するための踏み台にされそうになっていたものが 2 件でした。侵入の原因で、プログラムのぜい弱性(*1)を突かれたものが 5 件ありました（OS1 件、SQL インジェクション(*3)1 件、FTP サーバ 1 件、コンピュータの遠隔操作ソフト 2 件）。

被害事例

[侵入]

(i) SQL インジェクション(*3)攻撃を受け侵入、ウェブページ改ざん

事例	・「お宅のウェブサイトにアクセスするとウイルス警告が出る」との通報を受けた。 ・調査の結果、ウェブアプリケーションが SQL インジェクション攻撃を受け侵入を許し、ウェブページが改ざんされていたことが判明。改ざん内容は、ウイルスが置かれている悪質なサイトへのリンクを追加する、というもの。Windows のアニメーションカーソル処理のぜい弱性(*1)を突くタイプのウイルスだった。 ・侵入者は侵入成功後、外部サイト攻撃ツールをダウンロードしルートキット(*4)を実行。その後、ウェブページを改ざんしたものと思われた。 ・事後対策として OS インストールから再構築し、データベースを扱う権限の最小化を図るとともに、不要なストアドプロシージャ(*5)を削除した。
解説・対策	攻撃ツールを埋め込まれ、外部攻撃のための踏み台サーバとして悪用されてしまった例です。特に、**“Windows のアニメーションカーソル処理のぜい弱性”を突くゼロデイ攻撃(*6)の踏み台となっていた**点は深刻な問題と言えます。 ウェブアプリケーションのぜい弱性を解消するのはもちろんのこと、**ログ監視やウェブページ改ざん監視の強化**を図る必要があるでしょう。 (参考) IPA - 情報セキュリティ白書 2007 年版 http://www.ipa.go.jp/security/vuln/20070309_ISwhitepaper.html IPA - 安全なウェブサイトの作り方 改訂第 2 版 http://www.ipa.go.jp/security/vuln/websecurity.html

(ii) フィッシング(*2)サイトを設置された

事例	・外部機関から「あなたのサイトには某銀行に似せたフィッシングサイトが設置されている」との通報を受けた。 ・調査の結果、その事実が確認されたため、即当該ファイルを削除。ログ(*7)によれば、最初の侵入痕跡から 3 週間以上経ってから当該ファイルを設置されていたことが判明。 ・さらに異なる外部機関から同様の通報を受けたため調査したところ、再度フィッシングコンテンツが設置されていた。しかし今度は管理者権限でもディレクトリを削除できなかった。とりあえずディレクトリごと移動した。 ・使っていないはずの、FTP サーバが動いていたことが原因。古いバージョンであり、ぜい弱性を突かれて任意のコードを実行され、侵入を許していた。
解説・対策	侵入を許してしまった場合、原因が分からなければ何度でも同じ手口で侵入されてしまいます。この事例では、使っていないと思っていた、ぜい弱性を含んでいたプログラムが動いていたのが原因でした。**不要なプログラムは削除し、不要なサービスは停止するとともに、ログのチェックを密にし、侵入の兆候に一刻も早く気付く**ことが大切です。 (参考) IPA - 安全なウェブサイトの作り方 改訂第 2 版 http://www.ipa.go.jp/security/vuln/websecurity.html

3．相談受付状況

4 月の相談総件数は **827 件**でした。そのうち**『ワンクリック不正請求』に関する相談**が **205 件**(3 月:316 件)、**『セキュリティ対策ソフトの押し売り』行為**に関する相談が **17 件**(3 月:23 件)、**Winny に関連する相談**が **7 件**(3 月:5 件) などでした。

IPA で受け付けた全ての相談件数の推移

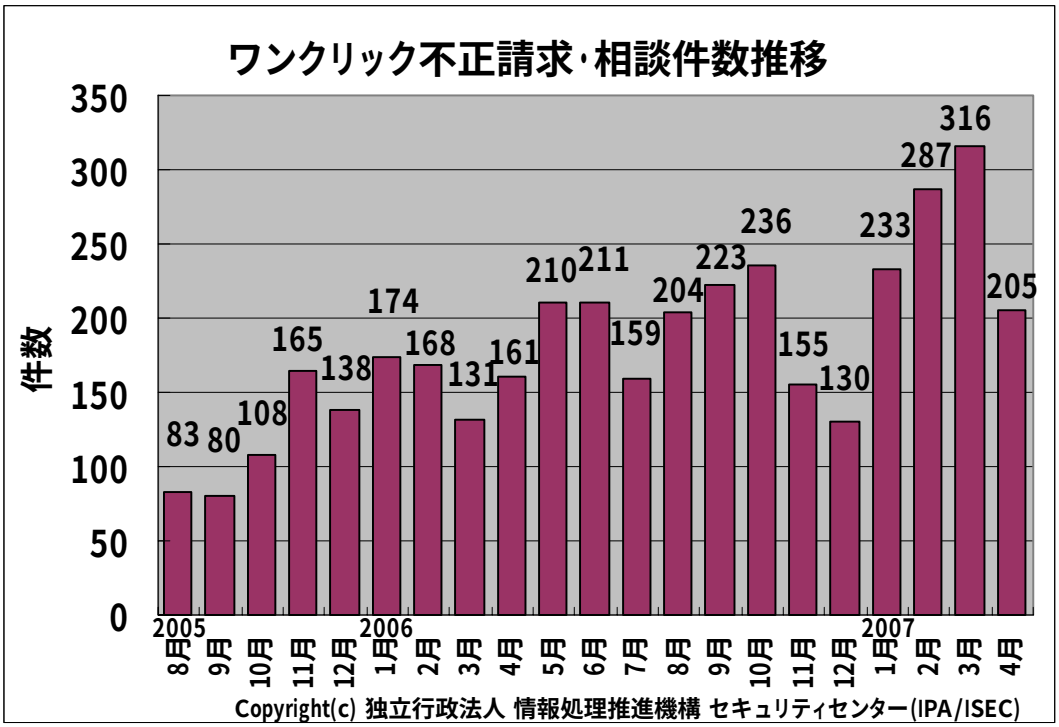
	11月	12月	1月	2月	3月	4月
合計	**711**	**680**	**946**	**1019**	**1127**	**827**
自動応答システム	423	394	582	603	697	486
電話	214	222	324	336	376	279
電子メール	72	59	39	75	54	58
その他	2	5	1	5	0	4

※ IPA では、コンピュータウイルス・不正アクセス、Winny 関連、その他情報セキュリティ全般についての相談を受け付けています。
メール: virus@ipa.go.jp (ウイルス)、crack@ipa.go.jp (不正アクセス)、
winny119@ipa.go.jp (Winny 緊急相談窓口)、isec-info@ipa.go.jp (その他)
電話番号: 03-5978-7509 (24 時間自動応答、ただし IPA セキュリティセンター員による相談受付は休日を除く月～金の 10:00～12:00、13:30～17:00 のみ)
FAX: 03-5978-7518 (24 時間受付)

※ 「自動応答システム」 : 電話の自動音声による応対件数
「電話」 : IPA セキュリティセンター員による応対件数

※ 合計件数には、「不正アクセスの届出および相談の受付状況」における『相談[d] 計』件数を内数として含みます。

(参考) ワンクリック不正請求相談件数の推移

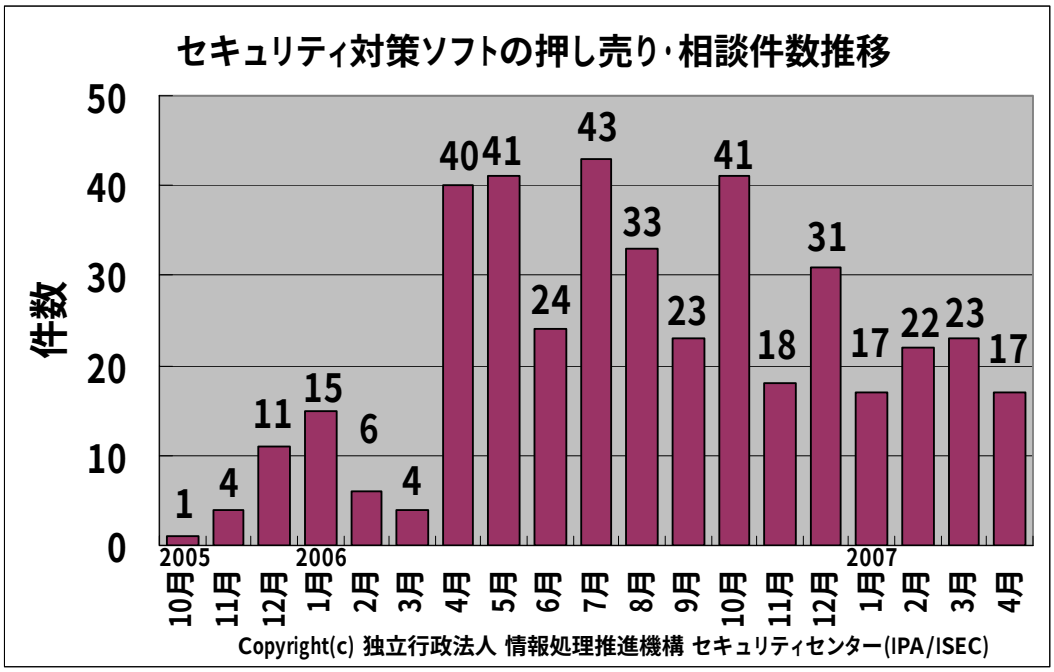


ワンクリック不正請求についての対策については下記をご参照ください。

・コンピュータウイルス・不正アクセスの届出状況[9 月分および第 3 四半期]について
2. ワンクリック不正請求
http://www.ipa.go.jp/security/txt/2006/10outline.html

・コンピュータウイルス・不正アクセスの届出状況[8 月分]について
2. 依然として相談の多いワンクリック不正請求による被害
http://www.ipa.go.jp/security/txt/2006/09outline.html

（参考）セキュリティ対策ソフトの押し売り・相談件数の推移



セキュリティ対策ソフトの押し売り行為については下記をご参照ください。

・2006 年 5 月の呼びかけ:「セキュリティ対策ソフトウェアの押し売りに注意！！」
http://www.ipa.go.jp/security/txt/2006/05outline.html

主な相談事例は以下の通りです。

(i) ウイルス対策ソフトで検知できない何かに感染？！

相談	見覚えの無いファイルやフォルダがあるなど、いつも状況が違うのに気が付きました。ウイルス対策ソフトのウイルス定義ファイルを最新にしようとしても、途中で止まってしまい、更新できません。どうすれば良いのでしょうか。
回答	既に、新種のウイルスに感染している可能性があります。**無償のオンラインウイルススキャンや、スパイウェア(*8)検知サービス、ボット(*9)駆除ツールを利用してみましょう**。しかし、ウイルス対策ソフトの動作を邪魔するような悪質なウイルスに感染していると、パソコンを初期化するしかない場合もあります。 (ご参考) トレンドマイクロ(ウイルスバスターオンラインスキャン) http://www.trendflexsecurity.jp/security_solutions/housecall_free_scan.php シマンテック(Security Check) http://www.symantec.com/region/jp/securitycheck/ マカフィー(フリースキャン) http://www.mcafeesecurity.com/japan/mcafee/home/freescan.asp マイクロソフト(Windows Live OneCare) http://onecare.live.com/site/ja-JP/default.htm スパイウェアガイド(ネクステッジテクノロジー) http://www.shareedge.com/spywareguide/txt_onlinescan.php サイバークリーンセンター(総務省･経済産業省 連携プロジェクト) https://www.ccc.go.jp/

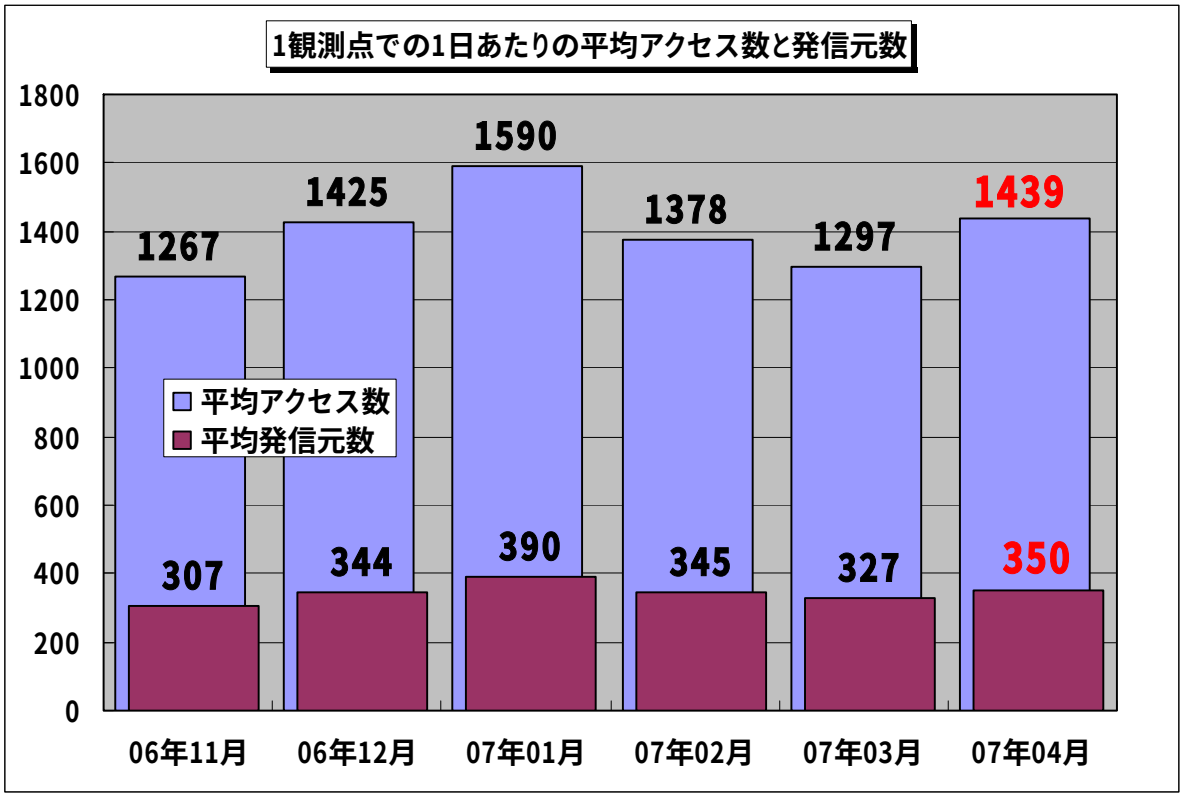
(ii) Winny でダウンロードしたファイルからウイルス感染

相談	4 月の始めに、以前から興味のあった Winny を、よく分からないまま使用。その後、ウイルスチェックしたら数種の Antinny ウイルスが検出された。アップロードフォルダを指定するための情報ファイルが存在していないので、情報流出はありませんよね？
回答	この時点で情報流出が無いと決め付けるのは早計です。Winny を動かしていたパソコン内に、漏れては困るデータがあったのであれば、それらが漏れたかも知れないという前提で行動すべきです。まずは検出されたウイルスの名前から、その動作を調べるとともに、影響が及ぶと思われる範囲に連絡を入れ、適切な対処をしましょう。 そもそも、**ファイル交換ソフトの原理を理解せずに興味本位で使うことは非常に危険な行為であることを、改めて認識しなければなりません**。何か問題が発生してからでは、取り返しがつきません。 (ご参考) IPA – Winny による情報漏えいを防止するために http://www.ipa.go.jp/security/topics/20060310_winny.html

4．インターネット定点観測での 4 月のアクセス状況

インターネット定点観測(TALOT2)によると、2007 年 4 月の期待しない（一方的な）アクセスの総数は、10 観測点で **431,643 件**ありました。1 観測点で 1 日あたり **350** の発信元から **1,439 件**のアクセスがあったことになります。

TALOT2 での 1 観測点の環境は、インターネットを利用される一般的な接続環境と同一なので、インターネットを利用される皆さんの環境へも同じくらいの一方的なアクセスがあると考えられます。言い換えれば、**あなたのコンピュータは、毎日、平均して、350 人の見知らぬ人(発信元)から、発信元一人当たり 4 件の不正と思われるアクセスを受けている**と言うことになります。



【図 4.1　1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数】

2006 年 11 月～2007 年 4 月までの各月の 1 観測点での 1 日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図 1.1 に示します。この図を見ると、期待しない（一方的な）アクセスは、2007 年 3 月に比べて多少の増加傾向ですが、全体的なアクセス内容については、定常化していると言えます。

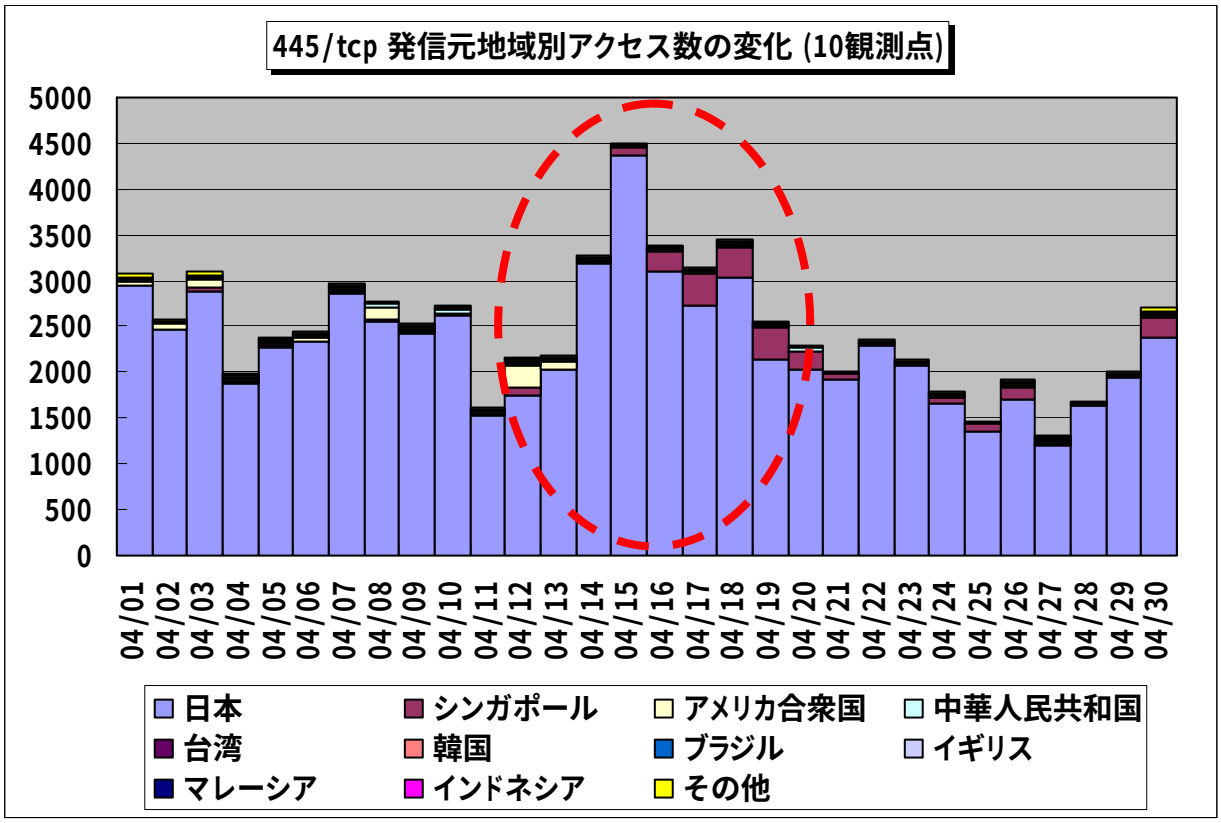
2007 年 4 月 13 日に、Windows 2000 Server や Windows Server 2003 が備えている、DNS（Domain Name System）サーバーサービスのぜい弱性がマイクロソフトから発表されました。このぜい弱性に対する攻撃(検証)コードが公開されており、ぜい弱性を狙った新しいワームや、攻撃コードが仕込まれたボットが広がっている可能性があります。

<参考情報>

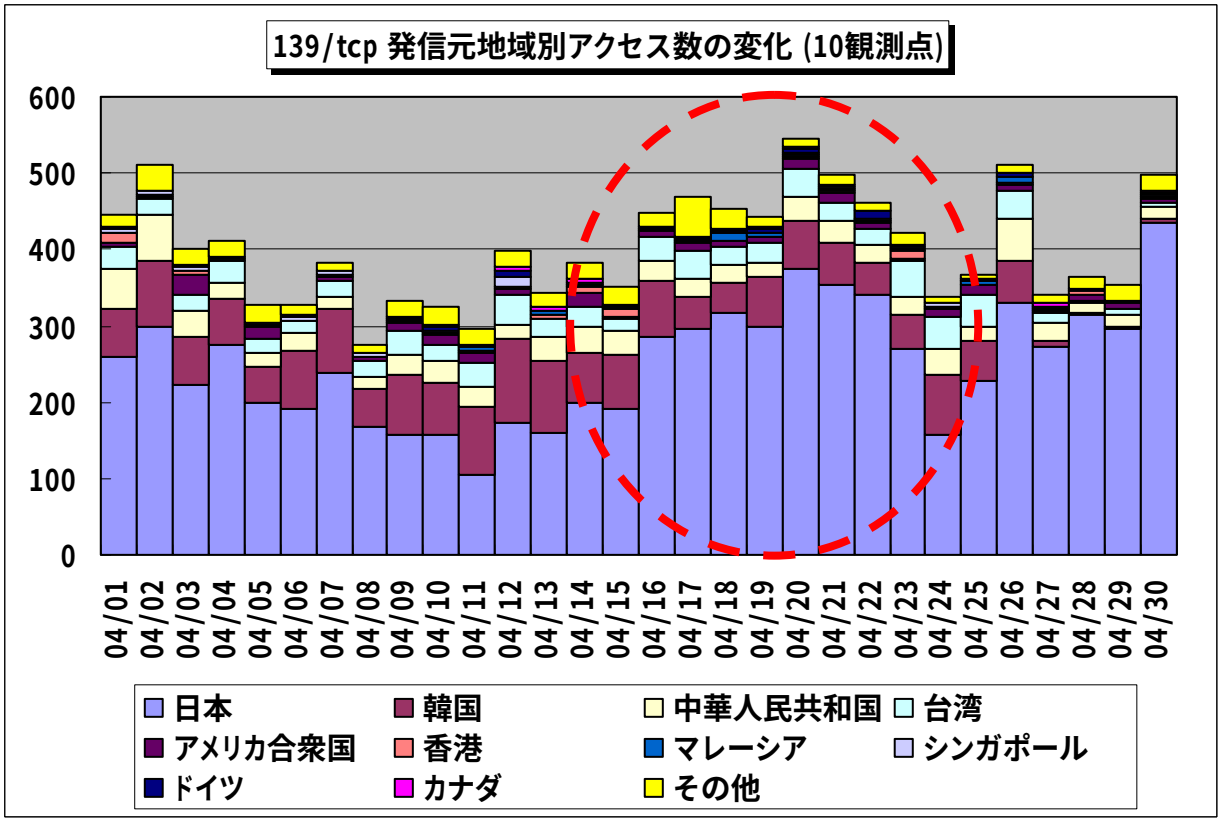
■ Windows DNS サーバー の RPC の脆弱性により、リモートでコードが実行される
http://www.microsoft.com/japan/technet/security/advisory/935964.mspx

図 4.2、図 4.3 に、445/tcp、139/tcp ポートへの発信元地域別アクセス数の変化を示します。これらの図を見ると、マイクロソフトから発表のあった 4 月 13 日以降に、国内を発信元とするアクセスが

増加しているのがわかります。



【図 4.2　2007 年 4 月の 445/tcp ポートへの発信元地域別アクセス数の変化】



【図 4.3　2007 年 4 月の 139/tcp ポートへの発信元地域別アクセス数の変化】

2007 年 4 月 25 日に、総務省と経済産業省の連携プロジェクト、「ボット対策プロジェクト」の取り

組み対策における中間発表があり、2006 年 12 月から 2007 年 3 月末までに、ISP（インターネットサービスプロバイダ）を通じて、約 6000 名のユーザーに対しボット感染の注意喚起メールを送った所、約 3 割のユーザーが駆除ツールをダウンロードしたとの発表がありました。
これを見てもわかる様に、わかっているだけで約 7 割のユーザーが、いまだにボット感染しているコンピュータを起動していると言うことになります。

以上の情報に関して、詳細はこちらのサイトをご参照ください。
別紙 3_インターネット定点観測（TALOT2）での観測状況について
http://www.ipa.go.jp/security/txt/2007/documents/TALOT2-0705.pdf

---

『他機関・ベンダーの各種統計情報は以下のサイトで公開されています。』
@police：http://www.cyberpolice.go.jp/
トレンドマイクロ株式会社：http://www.trendmicro.com/jp/
マカフィー株式会社：http://www.mcafee.com/japan/

『用語の解説』

(*1) **ぜい弱性** (vulnerability)
情報セキュリティ分野においては、通常、システム・ネットワーク・アプリケーションまたは関連するプロトコルのセキュリティを損なうような、予定外の、望まないイベントにつながる可能性がある弱点の存在や、設計もしくは実装のエラーのことを言う。セキュリティ上の設定が不備である状態を指す場合もある。一般に、セキュリティホール（security hole)と呼ばれることもある。

(*2) **フィッシング** (Phishing)
正規の金融機関など実在する会社のメールやウェブページを装い、それを見た利用者の ID やパスワードなどを詐取しようとする行為のこと。「釣り」を意味する「fishing」が語源だが、ハッカーの命名規則に則って"f"を"ph"に置き換えたという説、「洗練された」という意味の英語 "sophisticated"と"fish"とを組み合わせた造語という説、"password harvesting fishing"の短縮形という説、などがある。

(*3) **SQL インジェクション** (SQL injection)
データベースアクセスのために SQL 文を用いるプログラムにおいては、SQL 文を構成する際、プログラム中の式の値を SQL 文に埋め込む場合には、引用符で括られる文字列について、引用符が含まれているならばそれをエスケープ処理しなければならない。これを怠ると、正当なデータに対して SQL 文の実行がエラーとなる不具合が生じる。このバグが悪意ある者によって与えられ得る文字列を扱う箇所に存在すると、それはセキュリティ上のぜい弱性となる。攻撃者が悪意あるコマンドを与えると、データベースの内容を改ざんや情報を盗み出されるなどの被害が生じる。このような攻撃を SQL インジェクション攻撃と呼び、その原因箇所を同ぜい弱性と呼ぶ。

(*4) **ルートキット** (rootkit)
攻撃者がコンピュータに侵入した後に利用するためのソフトウェアをまとめたパッケージのこと。一般的には、ログ改ざんツールやバックドアツール、改ざんされたシステムコマンド群などが含まれる。

(*5) **ストアドプロシージャ** (stored procedure)
データベースに対する一連の処理手順を手続きとしてまとめ、データベース管理システムに保存したもの。

(*6) **ゼロデイ攻撃** (zero-day attack)
製品開発者が製品のぜい弱性に関する修正を行う前に、そのぜい弱性に対して行われる攻撃のこと。

(*7) **ログ** (log)
コンピュータの利用状況やデータ通信の記録のこと。一般的に、操作を行った者の ID や操作日時、操作内容などが記録される。

(*8) **スパイウェア** (spyware)
利用者や管理者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラム等のこと。

(*9) **ボット** (bot)
コンピュータウイルスの一種で、コンピュータに感染し、そのコンピュータを、ネットワーク(インターネット)を通じて外部から操ることを目的として作成されたプログラムのこと。

■お問い合わせ先
独立行政法人 情報処理推進機構 セキュリティセンター
花村／加賀谷／宮本
Tel:03-5978-7527 Fax:03-5978-7518 E-mail:isec-info@ipa.go.jp