プレスリリース
2006 年 4 月 5 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［2006 年 3 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、2006 年 3 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：
「知っていますか？ ファイル交換ソフトを使うと、不特定多数の利用者間であなたのパソコンのデータも共有されているということを！」
―― 単に興味本位で利用するのは止めましょう！！ ――

ファイル交換ソフト Winny を介して官公庁や大企業の重要情報漏えい事件は相変わらず多く報道されています。しかしこれは最近始まったことではなく、実は 2 年も前から、Winny を利用している中小企業のデータや個人ユーザのプライベートな情報の漏えいが確認されています。

ここで、Winny によるファイル交換の仕組みについて改めて確認してみましょう。**Winny ネットワークで共有されているファイルを他者のパソコンからダウンロードできるということは、自身のパソコン内のフォルダも不特定多数の Winny ユーザ間で共有されている**ということなのです（Winny の利用者数は 50 万人以上と言われています）。

つまり、ウイルス感染の有無に関係なく、公開したくないファイルを誤って公開用フォルダに置いてしまったり、公開したくないフォルダを自身の誤操作により「公開」として設定してしまったりすると、公開したくないデータが公開されてしまいます。**この仕組みを、Winny という“道具”の持つ危険性として理解できないのであれば、始めから Winny を利用すべきではありません。**

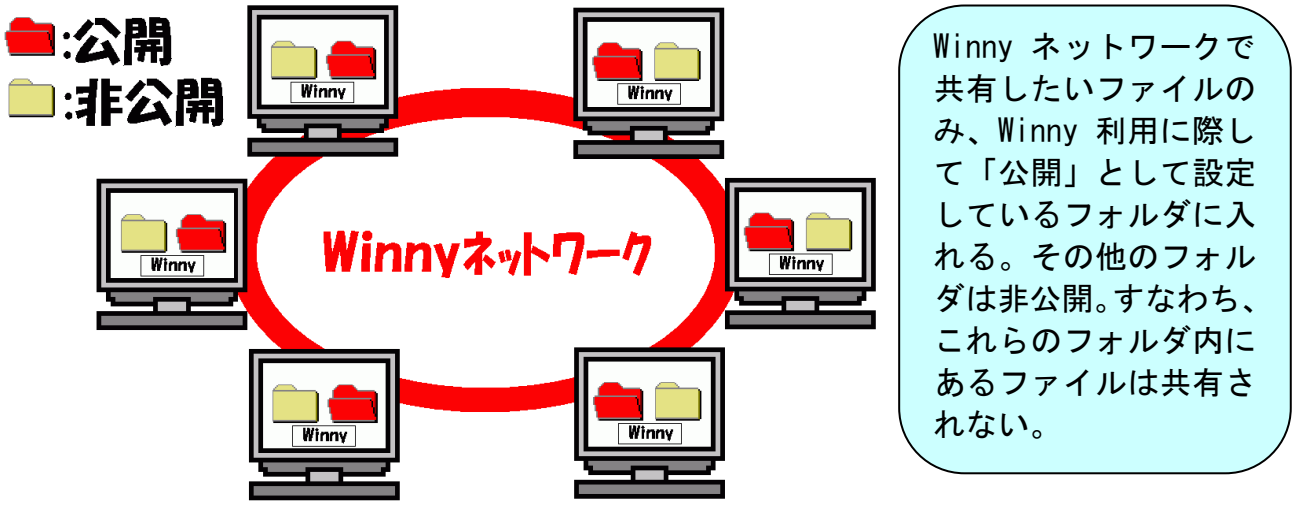


図 1.1 Winny によるファイル交換ネットワークの仕組み

ひとたびウイルスに感染すると、公開したくないファイルをいくら慎重に管理していたとしても、自身の意思に反して「公開」として扱われてしまう場合があります。従来からある Winny 関連ウイルス（Antinny）は、パソコン内の特定の種類のファイル（画像、文書、表計算、メールなど）を Winny の公開用フォルダにコピーしてしまいます。

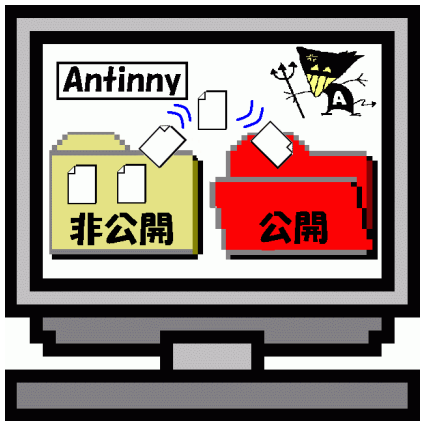


図 1.2 Antinny による情報漏えいのイメージ

2006 年 3 月には、感染するとパソコン内のほとんどのフォルダ内のファイルを Winny ネットワーク上に「公開」してしまう新種のウイルス（Exponny）が発見されました。

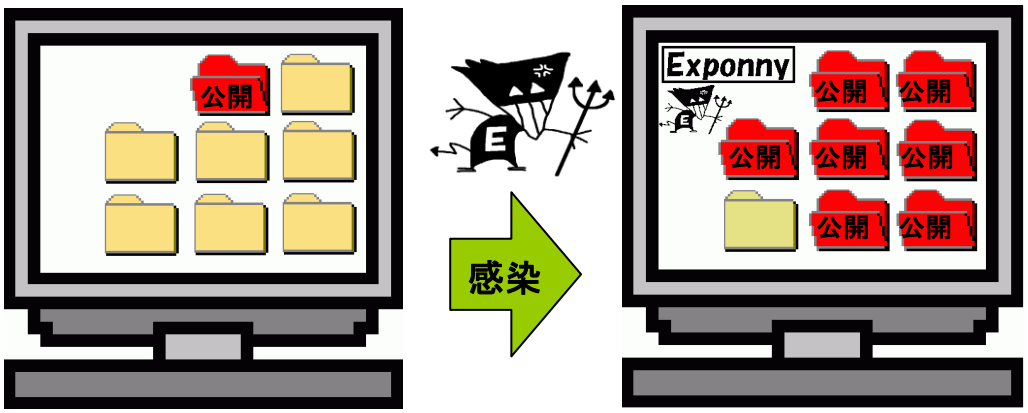


図 1.3　Exponny による情報漏えいのイメージ

ウイルスに感染しないためには、まずは、**出所不明で信用できないファイルを安易に開かない**ことが大前提です。しかしながら、**Winny を始めとしたファイル交換ネットワークで流通しているファイルのほとんど全てが、正に「出所不明で信用できないファイル」であるのが実情**であり、実際、魅力的なファイル名に偽装されたウイルスファイルが多く流通しています。すなわち、**ファイル交換ネットワークからファイルをダウンロードして開くという行為は非常に危険な行為**であることを認識し、**単に興味本位で Winny を利用することは厳に慎むことが必要です**。もちろん、Winny 以外のファイル交換ソフト利用についても、同様の注意が必要です。

1. コンピュータウイルス届出状況　－詳細は別紙 1 を参照－

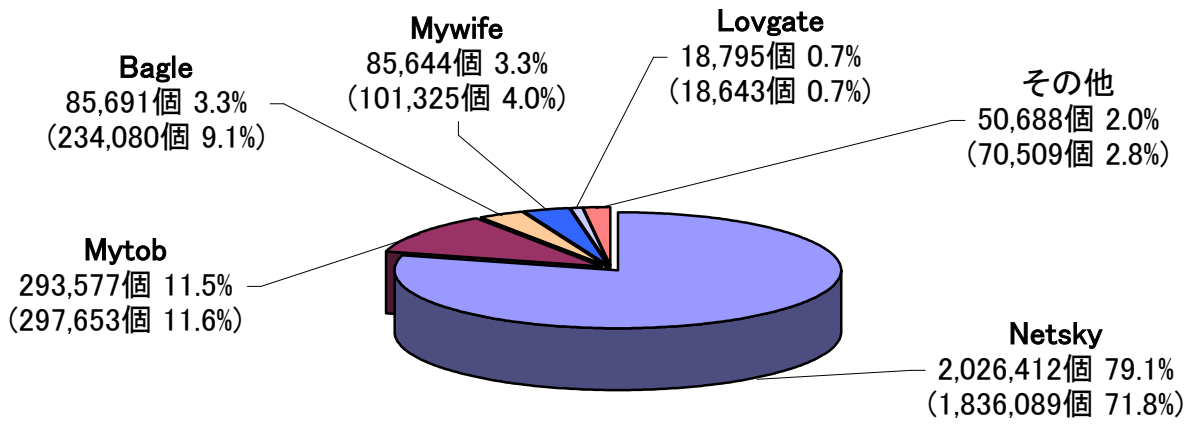
ウイルスの検出数(※1)は、**約 256 万個**と、2 月の約 256 万個から同水準での推移となりました。また、3 月の届出件数(※2)は、**4,270 件**となり、2 月の 4,324 件から 1.2%の減少となりました。

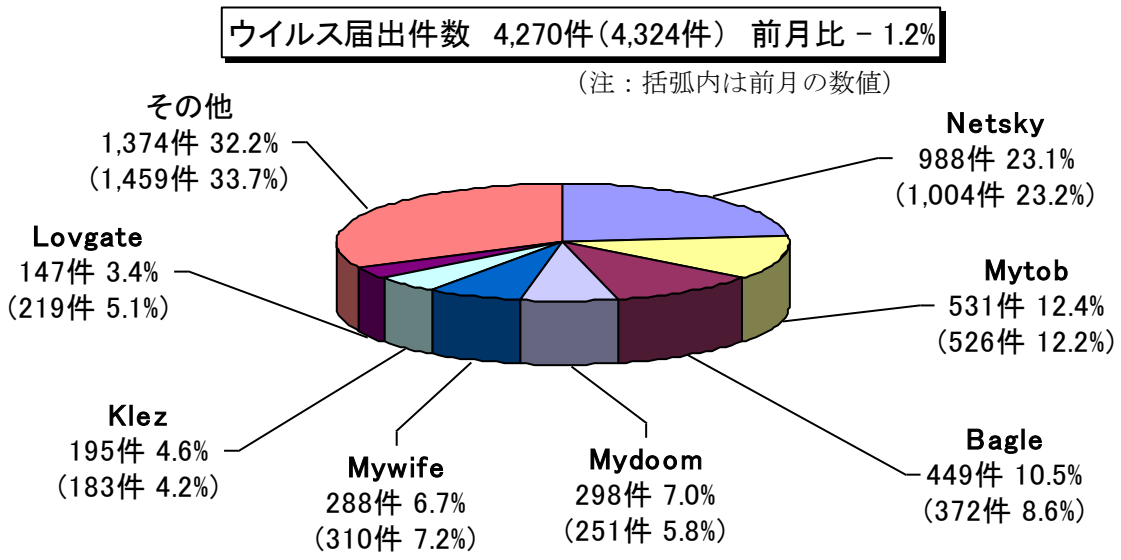
※1 検出数　：届出にあたり届出者から寄せられたウイルスの発見数（個数）
※2 届出件数：同じ届出者から寄せられた届出の内、同一発見日で同一種類のウイルスの検出が複数ある場合は、1 日何個検出されても届出 1 件としてカウントしたもの。
・3 月は、寄せられたウイルス検出数約 256 万個を集約した結果、4,270 件の届出件数となっています。

検出数の1位は、**W32/Netsky で約 203 万個 、2 位は W32/Mytob で約 29 万個、3 位は W32/Bagle で約 9 万個でした。**

ウイルス検出数　約256万個（約256万個）前月比 + 0.1%

（注：括弧内は前月の数値）





2. スパイウェアについて

スパイウェア(*1)による相談事例として、アダルトサイト等で画像をクリックしただけでスパイウェアがインストールされ、普段使用しているメールアドレスが抜き取られるといったものが多く寄せられています。

このような被害を分析すると、警告を無視して、自分でスパイウェアをインストールしてしまっているケースが多いようです。具体的な例を以下のサイトに掲載しておりますので、被害に遭わないよう対策の参考にしてください。

今月の呼びかけ:「警告を無視すると不正プログラムがインストールされる？！　」
　― 警告画面を軽視していませんか？ ―　【2006 年 1 月分】
　http://www.ipa.go.jp/security/txt/2006/02outline.html

また、一般的なスパイウェア対策として以下を参考にしてください。

(1)　スパイウェア対策ソフトを利用し、定期的な定義ファイルの更新およびスパイウェア検査を行う
(2)　コンピュータを常に最新の状態にしておく
(3)　怪しいサイトや不審なメールに注意する
(4)　コンピュータのセキュリティを強化する
(5)　万が一のために、必要なファイルのバックアップを取る
補足：自分で管理できないコンピュータでは、重要な個人情報の入力を行わない

スパイウェア対策のしおり
http://www.ipa.go.jp/security/antivirus/shiori.html

3. 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

		10月	11月	12月	1月	2月	3月
届出[a] 計		**22**	**24**	**25**	**50**	**26**	**38**
	被害あり[b]	15	15	19	13	15	10
	被害なし[c]	7	9	6	37	11	28
相談[d] 計		**35**	**30**	**25**	**43**	**42**	**24**
	被害あり[e]	25	18	15	23	24	12
	被害なし[f]	10	12	10	20	18	12
合計[a+d]		**57**	**54**	**50**	**93**	**68**	**62**
	被害あり[b+e]	40	33	34	36	39	22
	被害なし[c+f]	17	21	16	57	29	40

（1）不正アクセス届出状況

3 月の届出件数は 38 件であり、そのうち**被害のあった件数は 10 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 24 件（うち 7 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 12 件でした。

（3）被害状況

被害届出の内訳は、**侵入 6 件、その他（被害あり）4 件**でした。
侵入届出の内訳は、Web サーバに侵入されてフィッシング(*2)に悪用するための Web コンテンツを設置された届出が 1 件、SSH(*3)で使用するポート(*4)への攻撃を受けた結果侵入されたという届出が 1 件、などでした。

被害事例

［侵入］

（i） フィッシングサイトを設置された・・

事例	・「Web サイトが踏み台にされていませんか」との通報を外部から受けた。 ・調査の結果、フィッシングに悪用するための Web コンテンツを勝手に設置されていたことが判明。侵入されたのは MacOS X で運用していたサーバ。 ・セキュリティパッチを適用していなかった上に、不要なサービスを起動していたため、外部から攻撃を受けて侵入を許してしまったものと推測された。

解説・対策	**MacOS でも、OS や Web サーバソフトのアップデートを怠っていると、Windows と同様に、脆弱性を突かれて侵入を許してしまいます**。特にここ数年は、フィッシングなどの新たな情報セキュリティ上の脅威が出現しているため、利用している OS にかかわらず、不正アクセスやウイルスに対して注意が必要です。OS のみならず、Web サーバなどのアプリケーションについてもセキュリティパッチ適用を忘れずに実施しましょう。また、攻撃の糸口を与えないためにも、不要なサービスは止めましょう。 (参考) アップル社 - MacOS X ソフトウェアアップデート http://www.apple.com/jp/macosx/upgrade/softwareupdates.html IPA - 情報セキュリティ白書 2006 年版 http://www.ipa.go.jp/security/vuln/20060322_ISwhitepaper.html IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/20060131_websecurity.html

[その他（被害あり）]

（ii） ルータが攻撃を検知するのですが・・

事例	・ルータのセキュリティ機能により、IP スプーフィング攻撃(*5)及び TCP SYN フラッド攻撃(*6)が頻繁にブロックされるようになった。 ・その後、攻撃は検知されなくなったが、パソコンの電源を入れてしばらくすると CPU 負荷が 100%のままとなり、ルータの LAN 側アクセスランプが点滅を繰り返すようになった。WAN 側へのアクセスは無い模様。ADSL モデムの電源を切っても、状況は変わらない。 ・CPU 負荷が 100%のままのため、パソコンが使えない。
解説・対策	確かな原因は不明ですが、何らかの理由により**外部サイトを攻撃するためのツール（ボット(*7)など）がパソコン内に埋め込まれている**と思われます。可能性として、自身でボットなどの不正なプログラムを実行してしまったか、ルータに脆弱性が存在していた場合にその脆弱性を突かれて侵入された、などが考えられます。今回のケースでは、ルータのセキュリティ機能が、LAN 内のパソコンから外部への攻撃をブロックしているものと思われます。まずは、ウイルス定義ファイルを最新の状態に更新して、パソコン内のウイルスチェックを実施してみましょう。何も検出されない場合は、パソコンの初期化が必要となります。 (参考) IPA - コンピュータ不正アクセス被害防止対策集 http://www.ipa.go.jp/security/ciadr/cm01.html#DoS IPA - 情報セキュリティ白書 2006 年版 http://www.ipa.go.jp/security/vuln/20060322_ISwhitepaper.html

4. 相談受付状況

IPA では、最近のファイル交換ソフト(Winny)ネットワークを介して感染するウイルス(W32/Antinny)等による情報漏えい問題に対応して、予防・対処方法情報を提供するために、3 月 20 日に **Winny 緊急相談窓口（Winny119 番）** を新たに開設しました。

この影響もあってか、3 月の相談総件数は **1056 件**と、激増しました。そのうち、**Winny に関連する相談**は **196 件**(2 月:3 件)、**『ワンクリック不正請求』に関する相談**は **131 件**(2 月:168 件)でした。

IPA で受け付けた全ての相談件数の推移

		10月	11月	12月	1月	2月	3月
合計		**606**	**673**	**653**	**748**	**834**	**1056**
	自動応答システム	357	379	391	425	479	659
	電話	165	220	194	228	258	296
	電子メール	82	66	66	87	90	99
	その他	2	8	2	8	7	2

※ 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。

Winny 関連の、主な相談事例は以下の通りです。

(i) Antinny に感染している？

相談	Winnyを利用している。情報漏えいが不安なので、Antinnyなどのウイルスに感染していないかどうか、確認したい。
回答	**ウイルス対策ソフトを利用し、パソコン内にウイルスがあるかスキャンします。** ◆主なワクチンベンダーの Web サイト等一覧 http://www.ipa.go.jp/security/antivirus/vender.html いくつかのセキュリティベンダーは、ウイルススキャンを無料で行えるオンラインサービスを提供しています。 **◆シマンテック　セキュリティチェック** http://www.symantec.com/region/jp/securitycheck/ **◆トレンドマイクロ　オンラインスキャン** http://www.trendmicro.co.jp/hcall/ **◆マカフィー　フリースキャン** http://www.mcafee.com/japan/mcafee/home/freescan.asp さらに、マイクロソフト社より提供されている「悪意のあるソフトウェアの削除ツール」を使えば、Antinny ウイルスの検索と駆除を行うことができます。 **◆Microsoft 社 － 悪意のあるソフトウェアの削除ツール** http://www.microsoft.com/japan/security/malwareremove/ なお、上記に示した手段は、既知のウイルスに対して有効なものです。新しい亜種には対応していない可能性があり、感染していないと言い切ることはできません。**出所不明のファイルを開いてしまったなどの心当たりがある場合は、パソコンを初期化することをお勧めします。**

(ii) Winny が入っている？

相談	自分では Winny を入れた覚えは無いが、パソコンに Winny が入っていないかどうか、確認したい。
回答	**Winny は自動的にインストールされるものではない**ので、自身で入れた覚えが無いのであれば、基本的には Winny は入っていないはずです。しかし、パソコンを複数人で共有している場合は、自分以外の誰かが Winny を入れている可能性もあります。一部のベンダから無償で提供されている、**Winny そのものを検知するツール**でチェックしてみましょう。 (参考) シマンテック －Winny 検索ツールについて http://www.symantec.com/region/jp/winny/winny_tools.html アークン －ScanIF Winny 対応版 https://www.ahkun.jp/resource/dl.html

（iii）Winny は入れていないから…

相談	パソコンに Winny が入っていないことが確認できたから、情報漏えいは起きていないですよね？
回答	情報漏えいを引き起こすウイルスは、Antinny 以外にもあります。中でも、2006 年 2 月に発見された**通称「山田オルタナティブ」ウイルスは、Winny を利用していないパソコンからでも情報漏えいを引き起こします**。このウイルスは、Winny を利用しなくても感染しますので、**Winny 利用者以外でも油断は禁物です**。改めて原点に立ち返り、ウイルス対策の基本を徹底しましょう。 （参考） IPA － パソコンユーザのためのウイルス対策 7 箇条 http://www.ipa.go.jp/security/antivirus/7kajonew.html

なお、Winny に関連してよくある質問や対策情報は、以下のサイトに掲載しておりますので、ご参照ください。

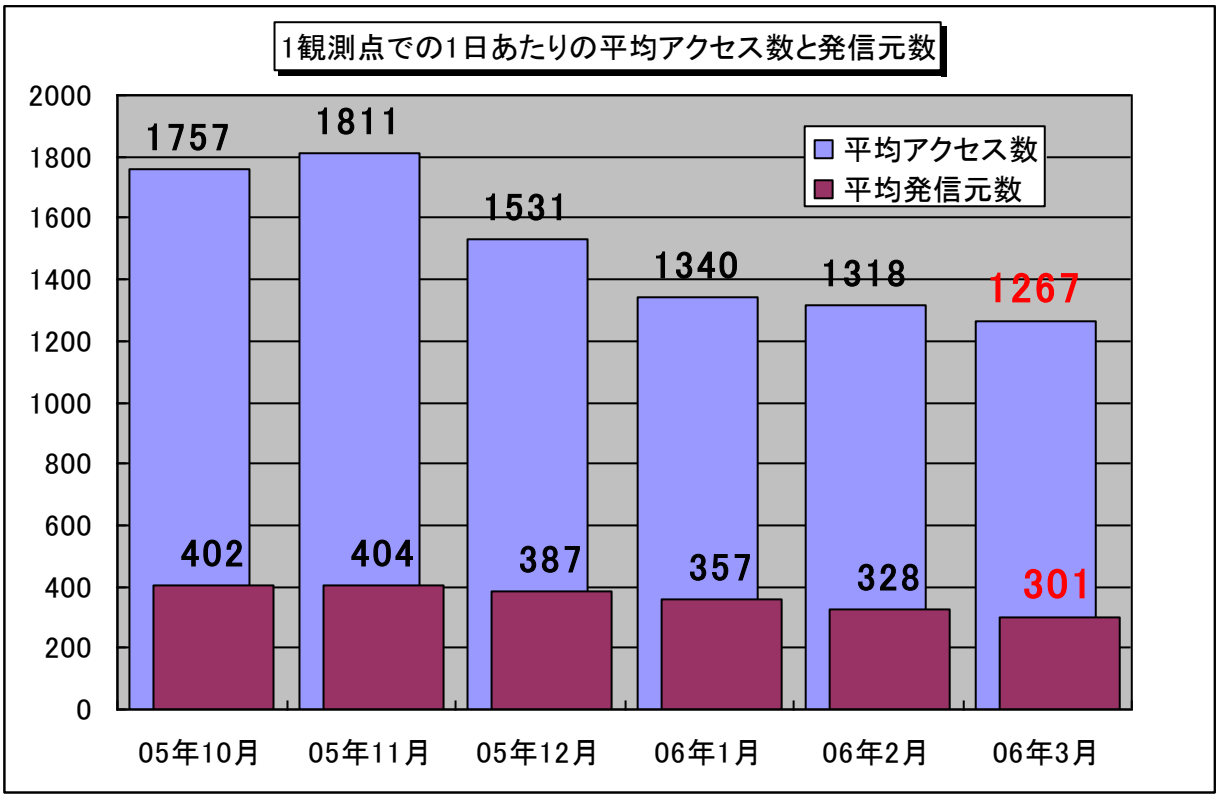
IPA － Winny による情報漏えいを防止するために
http://www.ipa.go.jp/security/topics/20060310_winny.html

IPA － Winny、Antinny に関する FAQ
http://www.ipa.go.jp/security/virus/faq/winny_qa.html

5. インターネット定点観測での 3 月のアクセス状況

インターネット定点観測(TALOT2)によると、2006 年 3 月の期待しない(一方的な)アクセスの総数は、10 観測点で **392, 728 件**ありました。1 観測点で 1 日あたり **301** の発信元から **1, 267 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、301 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 5.1　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】

2005 年 10 月～2006 年 3 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 5.1 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、発信元数も含めて、緩やかに減少傾向にあるようです。さらに、アクセス内容についても定常化していると言えます。

3 月のアクセス状況は、2 月とほぼ同じ状況です。Windows の脆弱性を狙っていると思われる不正なアクセスが多いようで、これらのアクセスの多くは、ボットに感染したコンピュータから送信されていると思われます。

特にアクセス数の多い 135(TCP)ポート,445(TCP)ポートへのアクセスは、Windows の脆弱性を狙っています。

また、Windows Messenger サービスを悪用したポップアップスパムメッセージの 1026(UDP)/1027(UDP)ポートへのアクセスも、あいかわらず継続(緩やかな増加傾向)しています。最近は、ウイルス対策や不正アクセス対策を勧めるポップアップメッセージやネットサーフィン時のアドウェアによるポップアップ広告等も多いので、これらの内容に騙されないように注意して下さい。1026(UDP)/1027(UDP)ポートへのアクセスの対策としては、管理された LAN(企業内 LAN 等)以外では、Windows Messenger サービスを止めることをお勧めします。

一般のコンピュータ利用者は、これらの不正なアクセスによる感染を予防するために、自分のコンピュータを最新の状態に保ち、ウイルス対策ソフトやパーソナルファイアウォール等の有効利用をお勧めします。

さらに、ウイルス対策や不正アクセス対策に利用する各種の対策ソフト(最近では、ウイルス対策ソフトだけでなくパーソナルファイアウォール機能や個人情報流出を防止する機能などを組み合わせた製品が増えているようです)については、信頼のおけるベンダーのものを利用することをお勧めします。

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/2006/documents/TALOT2-0604.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/jp/default.asp

『用語の解説』

(*1) 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。

(*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 Web 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) SSH (Secure SHell)
ネットワークを介して別のコンピュータにログインしたり、遠隔地のマシンでコマンドを実行したり、他のマシンへファイルを移動したりするために使うプロトコルもしくはプログラムのこと。ネットワーク上を流れるデータは暗号化されるため、インターネット経由でも一連の操作を安全に行なうことができる。

(*4) ポート (port)
コンピュータが外部との情報の受け渡しの際に使う、コンピュータ内の各種サービス窓口のこと。ポートは 0 から 65535 までの値が使われるため、ポート番号とも呼ばれる。

(*5)IP スプーフィング攻撃 (IP Spoofing attack)
送信元の IP アドレスを偽装して、相手にパケットを送る攻撃手法のこと。

(*6) TCP SYN フラッド攻撃 (TCP SYN flooding attack)
サーバの機能を低下させたり停止させたりする DoS 攻撃(*8)の手法の一つで、TCP の接続手順を悪用したもの。

(*7) 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。

(*8) DoS 攻撃 (Denial of Services)
サーバに大量のデータを送って過大な負荷をかけ、サーバのパフォーマンスを極端に低下させたり、サーバを機能停止に追い込んだりする攻撃のこと。

■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

お知らせ

『情報セキュリティ対策ベンチマークシステム』の紹介

IPA では、**「情報セキュリティ対策ベンチマークシステム」**を Web サイト上に公開しております。
情報セキュリティ対策ベンチマーク
https://isec.ipa.go.jp/benchmark-new/

本システムは、企業を対象としたもので、セキュリティ対策状況及び企業情報に関する設問(計40 問)に答えることにより、セキュリティ対策の取組状況を自己採点できるシステムです。

診断結果は、「貴社のスコア」と「望まれる水準」とが同時に表示され、各社が優先的に取り組むべきセキュリティ対策項目が明らかになります。また、推奨される取り組み事例も提示しますので、今後の対策を強化する上での具体的な改善策がわかります。

30 分程度で自己採点できますので、ぜひ、今後のセキュリティ対策の参考とすべく、ご活用ください。

「情報セキュリティ対策」の標語募集のお知らせ

IPA では、情報セキュリティ対策の意識を高め、コンピュータウイルスやコンピュータへの不正な侵入による被害などを少なくできるよう、「情報セキュリティ対策」の標語を、全国の小学生・中学生・高校生から募集しています。
入選作品は、報道発表を行い、また、IPA のホームページにも掲載します。

■募集期間:2006 年 3 月 13 日(月)～4 月 28 日(金)
■応募方法: 電子メール isec-hyogo@ipa.go.jp
FAX 03-5978-7518
■賞　金 :特賞(10 万円)、金賞(7 万円)、銀賞(5 万円)、銅賞(3 万円)

応募資格や応募方法など、詳細については以下のサイトをご参照ください。

標語で学ぼう セキュリティの大切さ
http://www.ipa.go.jp/security/kobo/17fy/hyogo/