IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2006 年 5 月 2 日
独立行政法人 情報処理推進機構

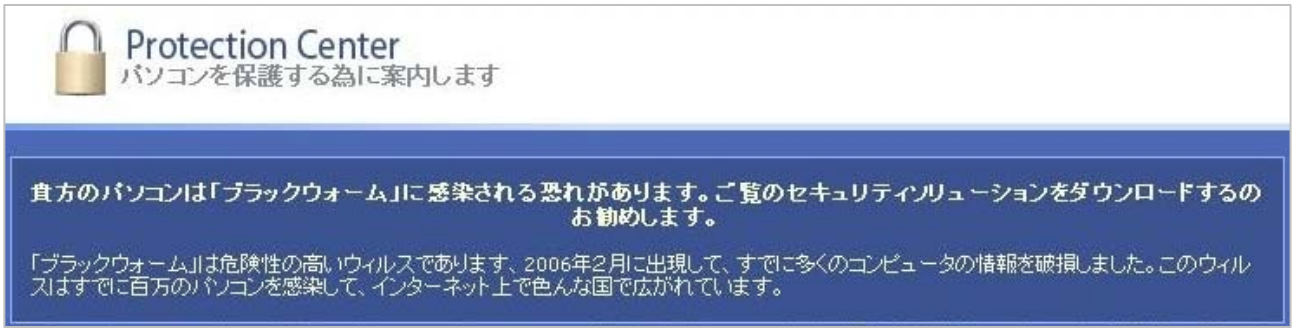
コンピュータウイルス・不正アクセスの届出状況［2006 年 4 月分］について

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、2006 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：
「セキュリティ対策ソフトウェアの押し売りに注意！！」
―― 怪しげな警告を真に受けるな！！ ――

4 月は、セキュリティ対策ソフトの押し売りのような行為に関する相談が 40 件と、3 月の 4 件から急増しました。以下のような表示が突然出現し、「セキュリティ対策ソフトウェア」と称するもののダウンロードを奨める手口などについてです。表示に従って「セキュリティ対策ソフトウェア」をダウンロードしてインストールすると、クレジット決済によって購入するまで、しつこく購入を促すメッセージを表示し続けます。こうした表示が、ユーザの業務などの妨げとなり、根負けして購入することになってしまったという事例がありました。

【事例 1】



【事例 2】

【事例 3】

事例1のように、少し妙な日本語のメッセージを表示して「セキュリティ対策ソフトウェア」と称するものを販売しようとする例があります。このようなメッセージが表示されても、実際には、ほとんどの場合、ウイルスに感染していません。ユーザを脅して押し売りをするようなものです。このメッセージ

に従い、ソフトウェアをインストールすると、パソコンに不具合が生じる例も報告されています。

正規のセキュリティ対策製品の製造・販売者からは、事例にある脅しのようなメッセージを一方的に送りつけることはありません。慌ててダウンロードすることのないようご注意ください。

それでも、「感染しているかもしれない」と心配な場合は、以下のサイトで無料のオンラインスキャンを利用できますので、検査してください。

オンラインスキャン（ウイルス検査サービス）

◆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

また、メッセージが頻繁に表示される場合は、本件のような広告を表示する不正なソフトウェアが入っている可能性がありますので、同様にオンラインスキャンで検査してください。

◆スパイウェアガイド - オンライン スパイウェア検出
http://www.shareedge.com/spywareguide/txt_onlinescan.php

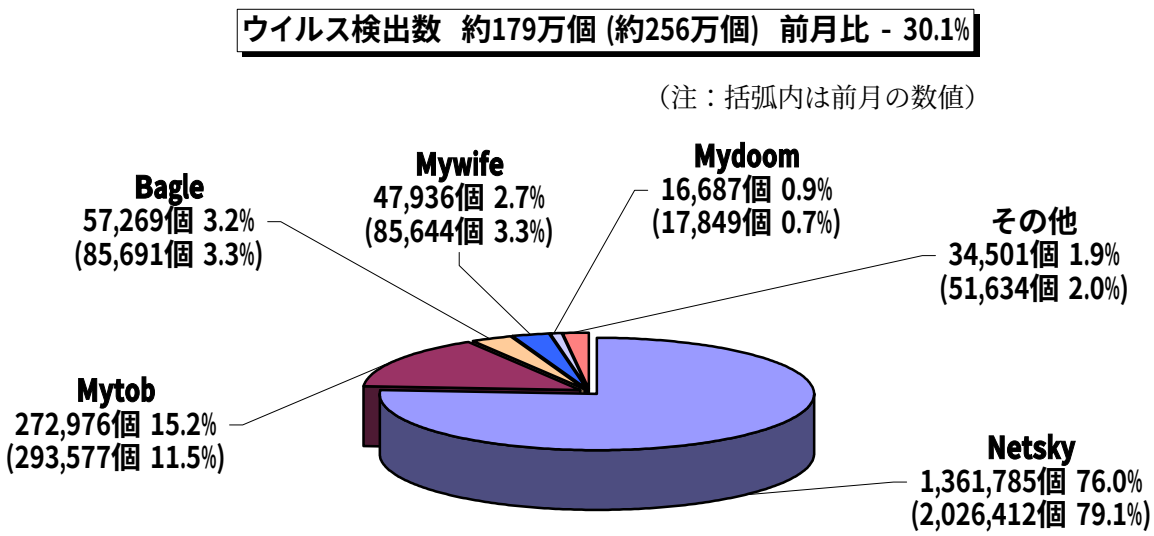
1．コンピュータウイルス届出状況　－詳細は別紙１を参照－

ウイルスの検出数(※1)は、**約 179 万個**と、3 月の約 256 万個から約 3 割の減少となりました。届出上位のウイルスはすべて検出数が減少（下図参照）していますが、特に W32/Netsky の検出数が 3 月の約 203 万個から 4 月の約 136 万個と、67 万個減少したことが大きく貢献しています。

また、4 月の届出件数(※2)は、**3,537 件**となり、3 月の 4,270 件から 17.4%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。
・4 月は、寄せられたウイルス検出数約 179 万個を集約した結果、3,537 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 136 万個 、2 位は W32/Mytob** で**約 27 万個、3 位は W32/Bagle** で**約 6 万個でした。**



図：1-1

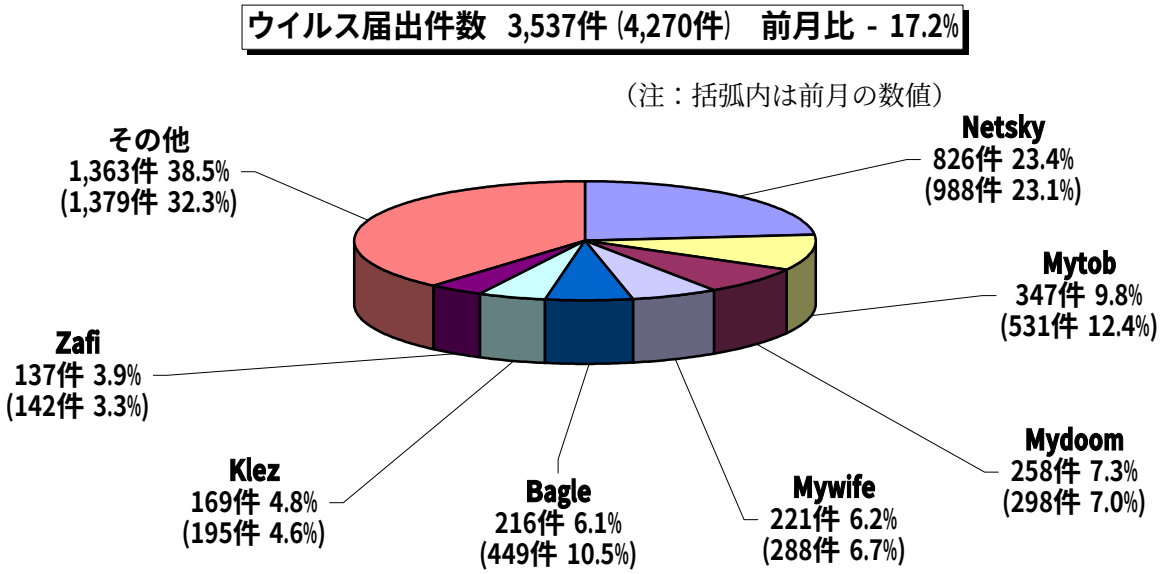


図:1-2

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継続して多数寄せられています。

このような被害事例では、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。少しでも怪しいと思ったら、ファイルの"種類"やファイルの"発行元"情報をチェックし、安全が確認された場合以外は [実行] や [実行する] をクリックしないようにしましょう。

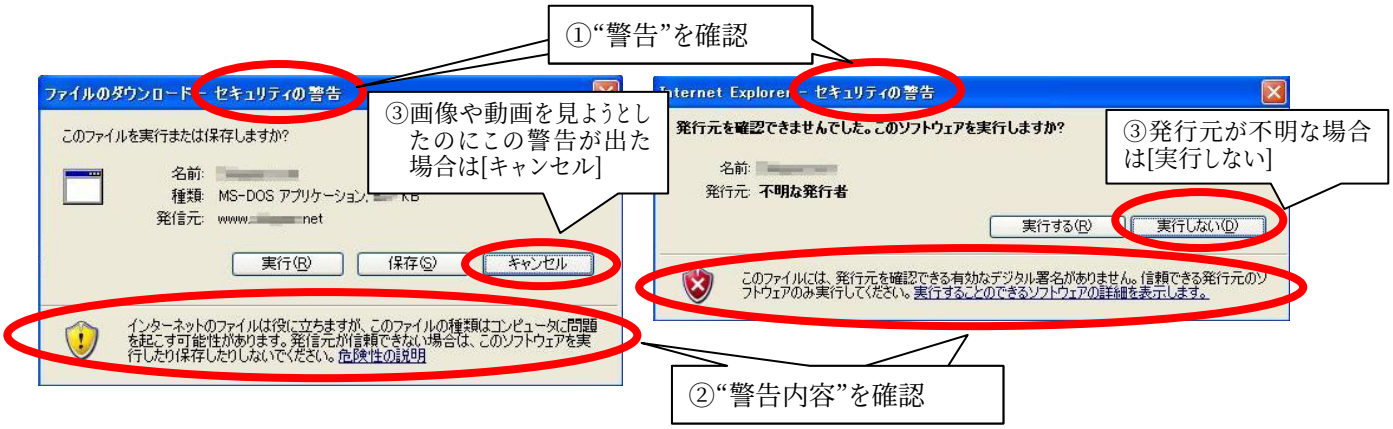


図:2-1

(ご参考)
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

　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

		11月	12月	1月	2月	3月	4月
届出(a) 計		**24**	**25**	**50**	**26**	**38**	**15**
	被害あり(b)	15	19	13	15	10	7
	被害なし(c)	9	6	37	11	28	8
相談(d) 計		**30**	**25**	**43**	**42**	**24**	**27**
	被害あり(e)	18	15	23	24	12	15
	被害なし(f)	12	10	20	18	12	12
合計(a+d)		**54**	**50**	**93**	**68**	**62**	**42**
	被害あり(b+e)	33	34	36	39	22	22
	被害なし(c+f)	21	16	57	29	40	20

（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 7 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 27 件（うち 3 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 15 件でした。

（3）被害状況

被害届出の内訳は、**侵入 5 件、DoS 攻撃 1 件、その他(被害あり)1 件**でした。

侵入届出の内訳は、SQL(*2)インジェクション攻撃(*3)でシステムを乗っ取られたものが 1 件、Web サーバに侵入されてフィッシング(*4)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(*5)で使用するポート(*6)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) SQL(*2)インジェクション攻撃(*3)による侵入

事例	・Web サーバを経由して SQL(*2)インジェクション攻撃(*3)を受け、システムを乗っ取られた。攻撃の踏み台として使うための、ツールを埋め込まれていた。 ・SQL インジェクション攻撃への対策を済ませた後でも、入り口である Web サーバへの攻撃が執拗に続いており、ネットワーク負荷が相当なものになっていた。
解説・対策	この事例では、ハッカー組織のものと思われる海外のサイトに、自組織のみならず多数の IP アドレスが晒されていたのが原因と思われました。IP アドレスを変更して、その後の攻撃を回避予定とのことでしたが、変更後の IP アドレスが再掲載されてしまっては、どうしようもありません。このような場合、アクセス元が海外など、**ご自身で対応依頼するのが難しい場合は、JPCERT コーディネーションセンターに対して、「インシデント報告の届出」をすることにより、発信元サイトに連絡をもらえる場合がある**ようです。詳細については、JPCERT コーディネーションセンターにご相談ください。 (参考) 有限責任中間法人 JPCERT コーディネーションセンター http://www.jpcert.or.jp/ IPA - 情報セキュリティ白書 2006 年版 http://www.ipa.go.jp/security/vuln/20060322_ISwhitepaper.html

(ii) ホームページ改ざん

事例	・自組織で運用しているホームページのトップページが改ざんされていることを発見。 ・以前、当該サーバが故障した時、ハードディスク増設とデータ移動を実施した。その際、アクセス権限の付与が正しく行われていなかったため、本来アクセスできないはずのユーザにアクセスされてしまったのが原因と考えられる。
解説・対策	通常はしっかりとアクセス管理されていても、何か非定型・非日常的なイベントが発生すると、チェックすべきことをうっかり見逃してしまいがちです。**何かの作業後には、以前と同等のセキュリティ強度が保たれているか、チェックすることを忘れないようにしましょう**。 (参考) 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）]

（iii） 成りすまし

事例	・フリーメール(*7)のサイトにログインできなくなった。どうやら、パスワードを変更されているようだった。 ・「おかしなメールが何通も来ている」と友人から携帯電話にメールがあった。よくよく話を聞くと、フリーメールのサイトに登録してあった個人情報、やり取りしていたメールの内容などを片っ端からアドレス帳に記載されていたアドレス宛に送信されていた模様。 ・その他に所有していた他サイトのアカウントも不正に使用され、勝手にメールを送られていた。
解説・対策	フリーメールサービスのサイトによっては、ID があらかじめ第三者にも分かるようになっているものもあり、この場合はパスワードだけ分かれば、その人に成りすましてログインされてしまいます。**語数の短いパスワードですと、比較的簡単に破られてしまいます**。 ログインされた後にサイトへの登録情報（個人情報や合言葉など）を変更されると、元の利用者は二度とログインできない状態に陥ってしまいます。まずは、**加入しているサービスのサイト管理者に連絡を取り、対処を依頼しましょう**。 なお、他人の ID を勝手に使い、本人に成りすまして使用するという行為は、法律に触れます(不正アクセス禁止法)。**警察機関に被害届を提出することで、捜査が開始される場合もあります**。 (参考) 「たかがパスワード、されどパスワード」（一般ユーザ向け） http://www.ipa.go.jp/security/crack_report/20020606/0205.html#spe1 都道府県警察本部のサイバー犯罪相談窓口等一覧 http://www.npa.go.jp/cyber/soudan.htm

4．相談受付状況

4 月の相談総件数は **904 件**と、相変わらず高水準で推移しています。そのうち、セキュリティ対策ソフトの押し売りのような行為に関する相談が **40 件**と、特に目立ちました（3 月：4 件）。その他は、**『ワンクリック不正請求』に関する相談**が **161 件**（3 月：131 件）、**Winny に関連する相談**が **83 件**（3 月：196 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		**673**	**653**	**748**	**834**	**1056**	**904**
	自動応答システム	379	391	425	479	659	510
	電話	220	194	228	258	296	306
	電子メール	66	66	87	90	99	86
	その他	8	2	8	7	2	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。

セキュリティ対策ソフトの押し売りのような行為に関する、主な相談事例は以下の通りです。

(i) ホームページを見ていたら突然警告が・・

相談	ネットサーフィンをしていたら突然、「**貴方のパソコンは『ブラックウォーム』に感染される恐れがあります**」と書かれたページが表示された。さらに、「**現在使用てるアンチウィルスは個人情報の伝送を防ぐことができません。貴方のコンピュータをすべての脅威を防ぐ為、ご覧のプログラムをダウンロードして下さい：**」と表示された。ダウンロードすべきなのでしょうか。 （**今月の呼びかけ：　【事例１】参照**）
回答	ホームページを見ていただけなのに**一方的に警告が出た場合は、「アヤシイ」と認識すべき**です。**正規のセキュリティ対策製品であれば、事例にある脅しのようなメッセージを表示することはありません**。画面に出ている情報をよく読むと、おかしな日本語になっていることが分かります。**少しでも「アヤシイ」と思ったら、安易に「次へ」や[OK]、[ダウンロード]などをクリックしてはいけません**。ウイルスやスパイウェアに感染しているかどうか心配な場合は、以下のサイトでオンラインスキャン（無料）をしてみましょう。 (参考) ◆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 また、メッセージが頻繁に表示される場合は、本件のような広告を表示する不正なソフトウェアが入っている可能性がありますので、同様にオンラインスキャンで検査してみましょう。 ◆スパイウェアガイド - オンライン スパイウェア検出 http://www.shareedge.com/spywareguide/txt_onlinescan.php

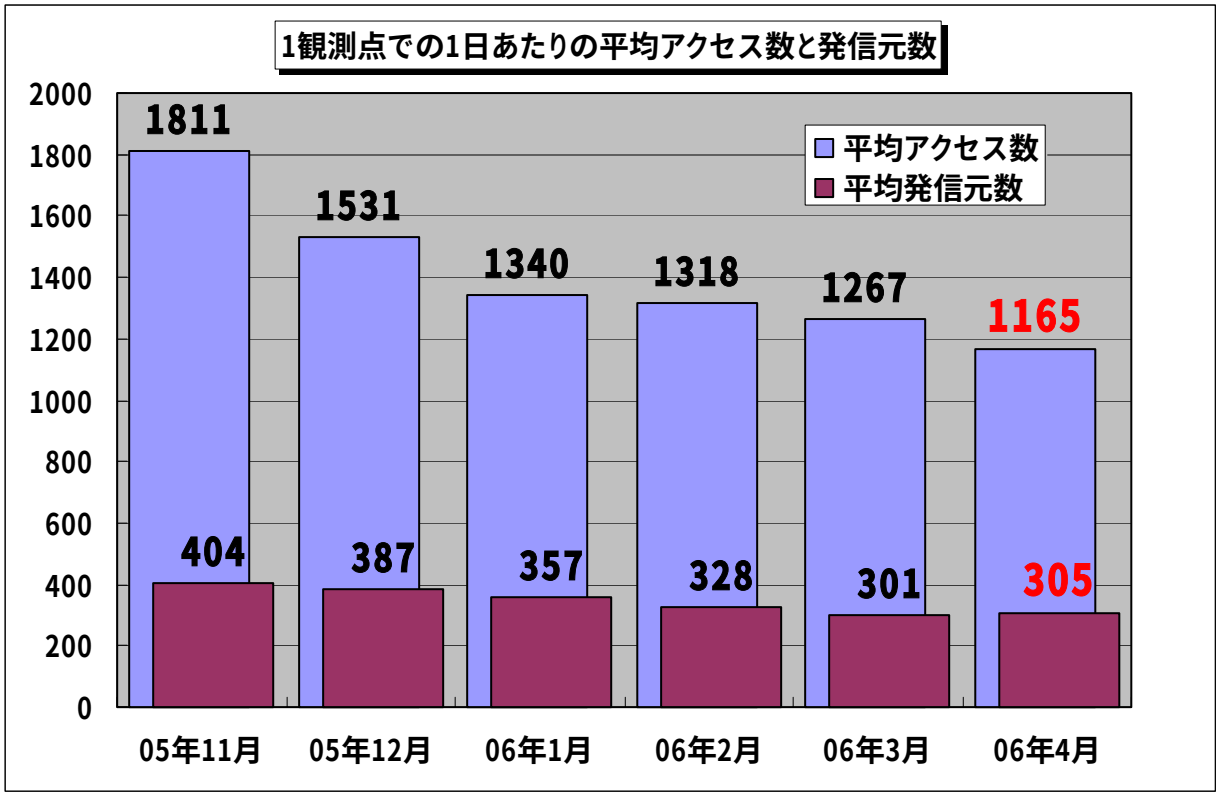
(ii) 言われるがままに購入、インストールしたのですが・・

相談	インターネット利用中に突然、セキュリティ対策製品の広告が表示された。クレジットカード番号を入力して購入しインストールしたが、その直後からパソコンが正常に動作しなくなった。これは正規の製品なのか。また、返品できるのか。
回答	相談者からの情報により、そのソフトベンダのものと思われるホームページを見てみましたが、**製造・販売元の企業情報や連絡先が不明確であり、製品としての信頼度は低い**と思われます。もし**詐欺だとすれば、返品は難しい**と思われます。**クレジットカード番号は、即座に変更すべき**でしょう。なお**支払いに関しては、クレジットカード会社や最寄りの消費生活センターに相談してみましょう**。 なお、当該のセキュリティ対策製品をうまくアンインストールできなかったり、パソコンの調子が悪い状態が続いたりするようなら、解決方法としては基本的にはパソコンを初期化するしかありません。(Windows Me か XP であれば、「システムの復元」で復旧できる場合もあります) (参考) 全国の消費生活センター http://www.kokusen.go.jp/map/ 都道府県警察本部のサイバー犯罪相談窓口等一覧 http://www.npa.go.jp/cyber/soudan.htm

5．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、2006 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 **349,562 件**ありました。1 観測点で 1 日あたり **305** の発信元から **1,165 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、305 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 11 月～2006 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 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、緩やかに減少傾向にあるようです**。アクセス内容については、定常化(後述の統計情報を参照下さい)していると言えますが、特異性があるために統計情報から除外しているアクセスは、先月に引き続き、多いようです。

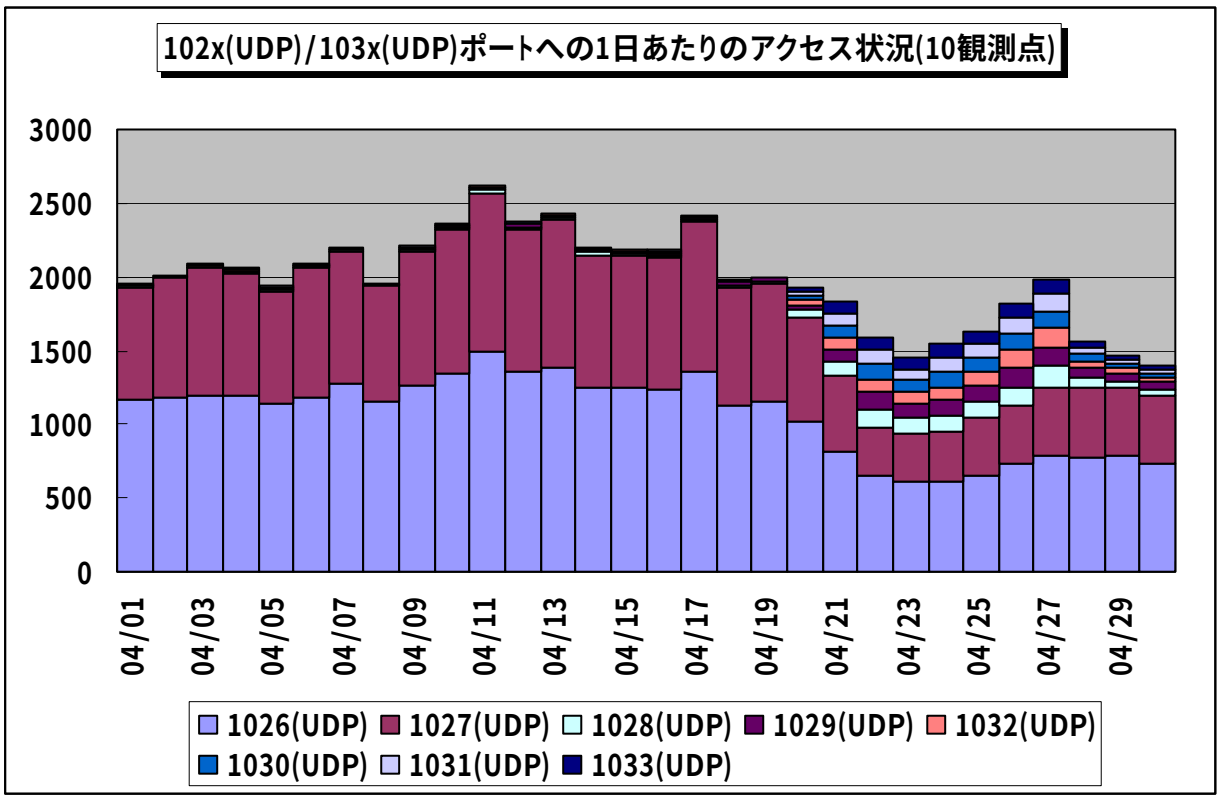
- SSH(Secure Shell)を狙ったアクセス
- 他のコンピュータを狙った SYN FLOOD 攻撃の痕跡
- P2P ファイル交換の接続要求と思われるアクセス

4 月のアクセス状況は、3 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は、継続していますが、月の後半で減少傾向がみられます。ただし、1028(UDP)/1029(UDP)/103x(UDP)ポートへのアクセスについて同時期に増加傾向

がみられました。アクセスの内容は同一のようです。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。102x(UDP)/103x(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。



【図 5.2　Window Messenger サービスを悪用したアクセスの状況】

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/TALOT2-0605.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) SQL (Structured Query Language)
リレーショナルデータベースマネジメントシステム (RDBMS) において、データの操作や定義を行うための問合せ言語のこと。構造化問い合わせ言語とも言う。元々は IBM 社が作った言語であるが、現在ではアメリカ規格協会(ANSI)や JIS で標準化されている、世界標準規格。

(*3) SQL インジェクション攻撃
データベースに対する問合せのデータ中に、攻撃者が意図的に SQL 文を混ぜ込んでおき、SQL サーバ内部でその SQL コマンドを不正に実行させてしまう攻撃手法のこと。

(*4) 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搾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。

(*5) 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。

(*6) 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。

(*7) フリーメール (free mail)
インターネットを利用して、無料で電子メールをやり取りできるサービスのこと。

■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

『自社のセキュリティ対策自己診断テスト』

～ 情報セキュリティ対策ベンチマーク ～

IPA では、**「自社のセキュリティ対策自己診断テスト（情報セキュリティ対策ベンチマーク）」**を Web サイト上に公開しております。

自社のセキュリティ対策自己診断テスト（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。