IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2005 年 12 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［2005 年 11 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、2005 年 11 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：「スパイウェアにだまされるな！！」
―― 怪しいファイルの見分け方 ――

11 月には、相手にスパイウェアを送りつけて銀行の口座情報を盗み出し、不正送金をした犯人が逮捕されました。普段、メールの添付ファイルの扱いに注意を払っている人でも、うっかりファイルを開いてしまい、ウイルスやスパイウェアに感染してしまう例が多く報告されています。それはなぜでしょうか。

それは、**メールに添付されたファイルの種類を確認せずにファイルを開いたら、実はそれがウイルスやスパイウェアそのものだった**ということです。では、ファイルを開く前にどうやって見分ければ良いのでしょうか？

対策方法は、『**ファイルの拡張子を確認する**』ことです。

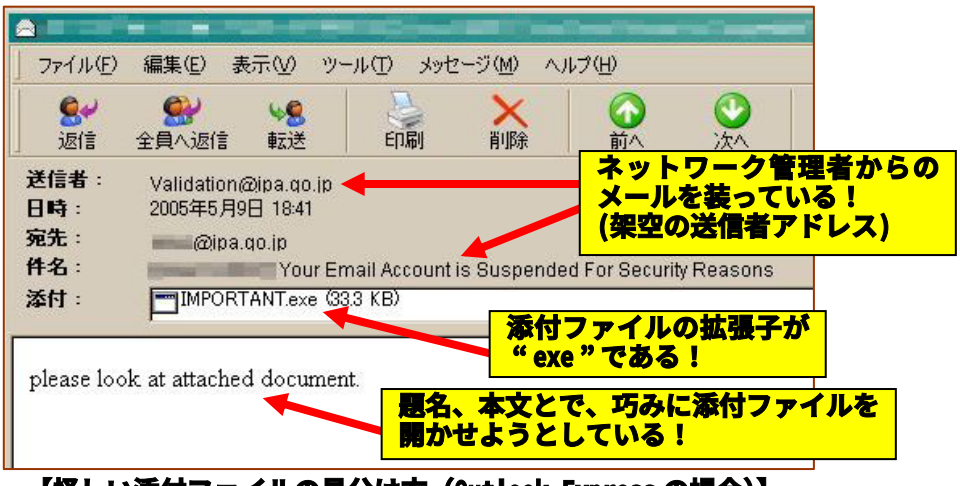
Windows の場合、ファイルの拡張子とアイコンによって、そのファイルの種類を判別できます（右表参照）。

【ファイルの種類とアイコン、拡張子の対応表】

ファイルの種類	アイコン例	ファイル名＋拡張子の例
zip 圧縮ファイル		圧縮ファイル.zip
画像ファイル		画像.jpg
文書ファイル		文書.doc
動画ファイル		動画.wmv 動画.mpg
テキストファイル		テキスト.txt
実行形式ファイル		実行ファイル.exe

ウイルスやスパイウェアなどの**不正プログラムは、ほとんどが拡張子“exe”である実行形式のファイルです**。しかし、通常のメールのやり取りでは拡張子“exe”のファイルを添付することはほとんどありません。

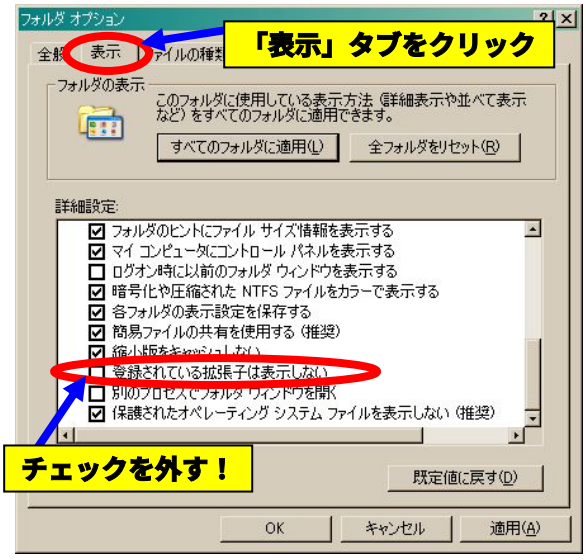
つまり、**メールの添付ファイルの拡張子が“exe”だった場合は、ファイルを開かずにメールを即削除することが、感染を防ぐためには一番簡単で最良の方法**となります。



【怪しい添付ファイルの見分け方（Outlook Express の場合）】

ところで、**インターネットの Web サイトからダウンロードしたファイルの場合**はどうやって見分けるのでしょうか？

この場合も、ファイルを開く前にファイルの拡張子とアイコンによって、そのファイルの種類を判別できます。しかし、**Windows の初期設定では拡張子が表示されないようになっています**ので、マイコンピュータもしくはエクスプローラのメニューバーから[ツール]―[フォルダオプション] を選択し、**[登録されている拡張子は表示しない]** の**チェックを外し**、拡張子を表示させるようにします（右図参照）。



ここでは、動画ファイル（らしきもの）をダウンロードした場合、アイコンとファイル名がどう見えるかを例に示します（下表参照）。なお、この例のように**ファイルの見た目（アイコン）は、偽装されている場合もあります**ので、**アイコンだけを見てファイルの内容を判断するのは危険です**。

本当に動画ファイルであれば、拡張子は.wmv や.mpg などになっているはずです。**拡張子が.exe であった場合は、ウイルスやスパイウェアである可能性があります**。また、例３のように、**拡張子が二重に付与されている場合は、見た目の拡張子にだまされる恐れがありますので、特に注意が必要です**。

	ファイルの内容	「登録されている拡張子」の表示設定	
		表示しない場合	表示する場合
例１	動画ファイル	動画	動画.wmv
例２	スパイウェアの可能性あり	動画	動画.exe
例３	スパイウェアの可能性あり	動画.wmv	動画.wmv.exe

アイコンが偽装されている！

拡張子が“ exe ”なので、動画ファイルではない！

ニセの拡張子に注意！

なお、**メールの添付ファイルやインターネットからダウンロードしたファイルを開く際には、事前に必ずウイルスチェックをすることを忘れないでください**。もしウイルスやスパイウェアなどが何も検出されない場合でも、新種の不正プログラムである可能性もありますので、**信頼できない相手からメールで送られて来たファイルや、信頼できないサイトからダウンロードしたファイルは、不用意に開かないという心掛けが大事です**。

（ご参考）

IPA - メールの添付ファイルの取り扱い ５つの心得
http://www.ipa.go.jp/security/antivirus/attach5.html

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

IPA - パソコンユーザのためのスパイウェア対策 ５ 箇条
http://www.ipa.go.jp/security/antivirus/spyware5kajyou.html

1．コンピュータウイルス届出状況　－詳細は別紙 1 を参照－

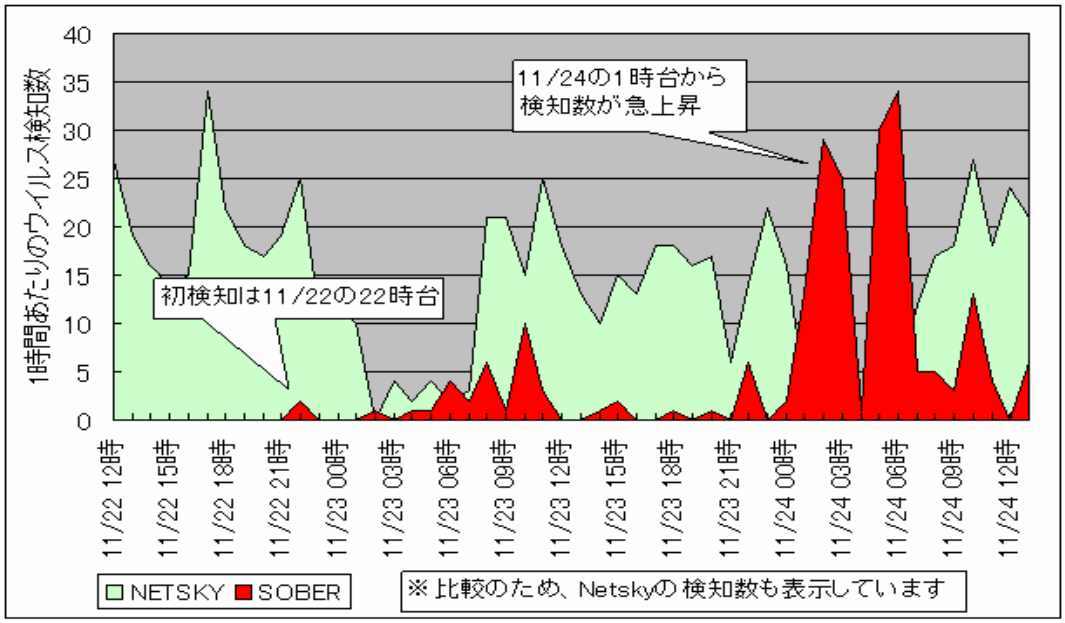
ウイルスの検出数(※1)は、**約 510 万個**と、10 月の約 319 万個から 60.1%と大幅な増加となりました。これは、W32/Sober の亜種の検出数が 202 万個寄せられたためです。また、11 月の届出件数(※2)は、**3,816 件**となり、10 月の 4,071 件から 6.3%の減少となりました。

※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。
・11 月は、寄せられたウイルス検出数約 510 万個を集約した結果、3,816 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 225 万個**、2 位は **W32/Sober で約 202 万個**、3 位は **W32/Mytob で約 72 万個**となっています。

（1）W32/Sober の亜種が急速に拡大！

11 月 22 日に出現した **W32/Sober の亜種**は、W32/Netsky を上回るペースで大量のウイルスメールを送信し、わずか 1 週間でウイルス検出数トップ 2 になりました。



【図：IPA における検知状況】

このウイルスは、メールの添付ファイルとしてユーザに届き、そのファイルを開くと感染します。巧妙な手口として、**送信者アドレスに FBI や CIA のアドレスを利用**し、受信者に添付ファイルを開くように促している点があります。メールを読んだ方は、FBI から警告が届いたと勘違いし、内容を確認するために添付ファイルを開いて感染してしまうケースがあったようです。

IPA の緊急対策情報
「W32/Sober」ウイルスの亜種に関する情報
http://www.ipa.go.jp/security/topics/newvirus/sober.html

メールの添付ファイルには、ウイルスなどの不正プログラムが仕掛けられているケースが多いので、添付ファイルの取り扱いには十分注意しましょう。

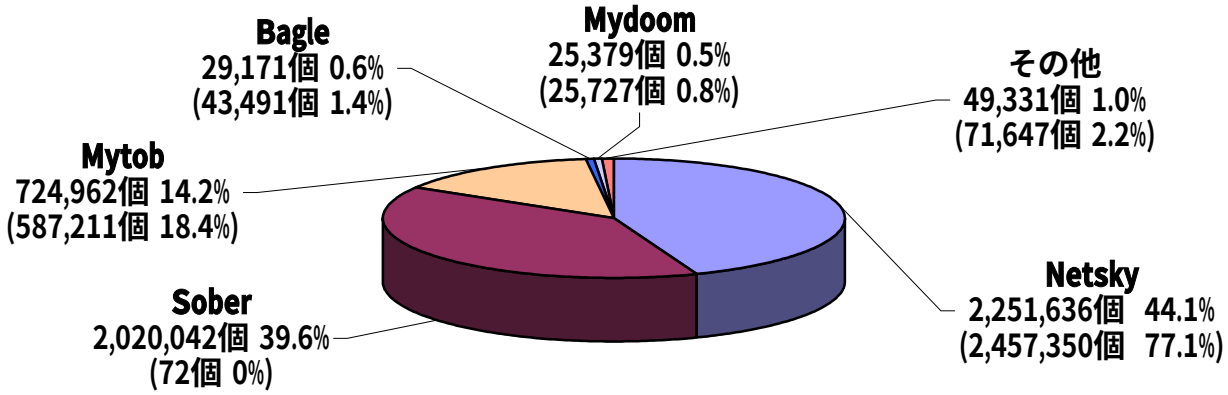
メールの添付ファイルの取り扱い 5 つの心得
http://www.ipa.go.jp/security/antivirus/attach5.html

（2）W32/Sober の検出数が急激に増加！

11 月に出現した **W32/Sober の亜種**が、短期間に大量のウイルスメールを発信したことにより、**約 202 万個**もの届出が寄せられました。また、**W32/Netsky** も**約 225 万個**と、10 月の約 245 万個から 8.4%の減少となりましたが、依然として高水準で推移しています。

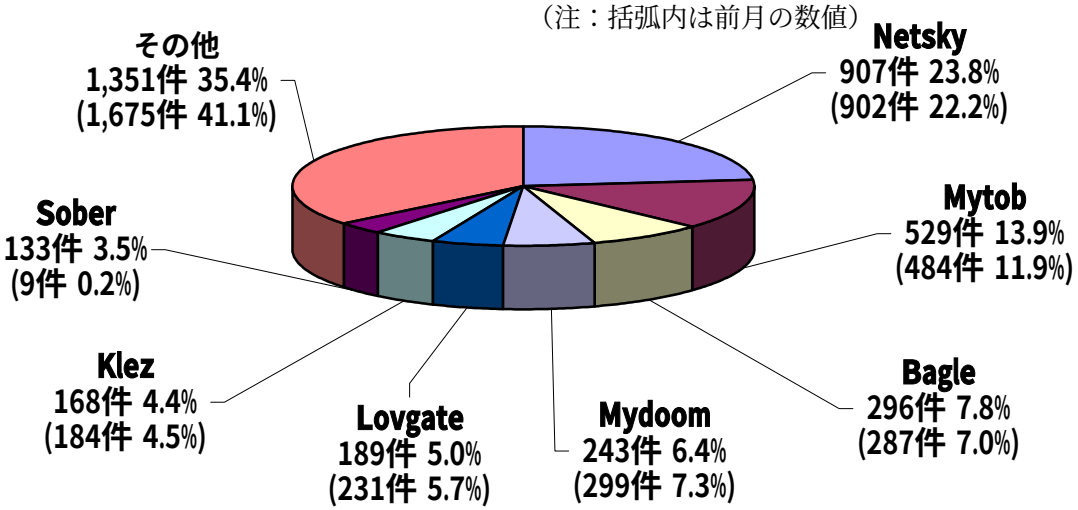
ウイルス検出数　510万個(319万個)　前月比 + 60.1%

（注：括弧内は前月の数値）



ウイルス届出件数　3,773件 (4,071件)　前月比 -7.3%

（注：括弧内は前月の数値）



2．スパイウェアについて

最近、オンラインバンキングで使用する口座情報･パスワードを詐取するために、スパイウェア(*1)を利用するなど、金銭を目的とした不正行為が見受けられます。以下に掲げる対策を実施すると共に、銀行側が提供している各種セキュリティ対策（ソフトウェアキーボード(*2)、乱数表　等）を利用するなど、被害に遭わないようご注意ください。

（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［まめに修正プログラムを適用する］
（3）　怪しいサイトや不審なメールに注意
（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

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

		6月	7月	8月	9月	10月	11月
届出(a) 計		**24**	**53**	**41**	**31**	**22**	**24**
	被害あり(b)	22	10	12	16	15	15
	被害なし(c)	2	43	29	15	7	9
相談(d) 計		**37**	**43**	**43**	**30**	**35**	**30**
	被害あり(e)	22	24	23	16	25	18
	被害なし(f)	15	19	20	14	10	12
合計(a+d)		**61**	**96**	**84**	**61**	**57**	**54**
	被害あり(b+e)	44	34	35	32	40	33
	被害なし(c+f)	17	62	49	29	17	21

（1）不正アクセス届出状況

11 月の届出件数は 24 件であり、そのうち**被害のあった件数は 15 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 30 件（うち 6 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 18 件でした。

（3）被害状況

被害届出の内訳は、**侵入 11 件、アドレス詐称 1 件、その他(被害あり)3 件**でした。
なお、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は 4 件もあり、今後も注意が必要です。

被害事例

[侵入]

(i) SSH で使用するポートからの侵入

事例	外部からの通報を受け調査したところ、ある非管理者権限アカウント(*5)へのログイン試行が成功していたことが判明。その結果、サーバに侵入されてポートスキャンツール(*6)や SSH スキャンツール(*7)を埋め込まれ、外部への攻撃を続けていた。パスワードが推測され易いものだったのが原因だが、さらに侵入後に何らかの原因で管理者権限への昇格を許していた。不正アクセスの試みは侵入の約 1 ヶ月前から続いていたが、管理者は気付いていなかった。
解説・対策	パスワード管理の不徹底が根本要因でしたが、**一般アカウントの権限昇格が行われたことが被害を拡大させてしまっています**。セキュリティパッチ(*8)の適用を再確認するとともに、外部から接続可能なアカウントの管理見直しが必要でしょう。また、**常日頃からアクセスログ(*9)をチェックして一刻も早く攻撃の兆候を掴み、必要な対策を講じることが重要**です。さらに、**SSH 運用時には、ログインの際に公開鍵認証(*10)などの強固な認証を採用することを推奨します**。 (ご参考) OpenSSH http://www.openssh.com/ja/ IPA - セキュアな Web サーバの構築と運用 ～ OpenSSH のインストールと設定 http://www.ipa.go.jp/security/awareness/administrator/secure-web/chap4/4_openssh.html IPA - セキュアな Web サーバの構築と運用 ～ ユーザ認証 http://www.ipa.go.jp/security/awareness/administrator/secure-web/chap6/6_userauth-1.html

(ii) 初期状態のマシンへの攻撃

事例	システムをインストールしたばかりのマシンに管理者権限でログインし、放置しておいたところ、画面にドクロマークが表示されてフリーズ(*11)していた。レスキューディスクを用意していたが全く役に立たず、再度インストールすることになった。
解説・対策	**インストールしたばかりの状態や買ったばかりの状態では、最新のセキュリティパッチが適用されていません**。そのままインターネットに接続した場合、その脆弱性を突かれて攻撃されると、いとも簡単に侵入を許してしまいます。こうならないためにも、初期化したコンピュータをインターネットに接続する際には、 ・接続する前に、オフラインで入手したセキュリティパッチを適用する ・ファイアウォールなどで守られたネットワークに接続する ・ウイルス対策ソフトやパーソナルファイアウォールソフトを導入する といった対策が有効になります。**インターネットに接続したら、まずはセキュリティパッチの適用を最優先に実施しましょう。** (ご参考) マイクロソフトアップデート http://update.microsoft.com/microsoftupdate/ 「日本の Linux 情報」 - バグ・セキュリティ情報 - http://www.linux.or.jp/

(iii) SQL インジェクションによる攻撃

事例	オンラインショップシステムを受託運用しており、その利用者から、決済に使用しているクレジットカードが不正利用されている可能性があるとの問い合わせを受けログ解析調査したところ、不正アクセスの形跡を確認した。流出した情報には氏名情報は無かったが、カード番号と有効期限のみで決済可能なオンラインゲームサイトでの不正利用が確認された。その後の調査で、不正アクセスの原因はSQL インジェクションであることが判明。
解説・対策	このケースでは夏にシステム変更を実施していましたが、その際、システムの一部で SQL インジェクションへの対策漏れが生じていたようです。一度対策を実施したとしてもそれで安心せず、**日頃からログを注意して監視したり、セキュリティ監査を受けたりすることなどが、対策漏れを防ぐための手立てになります**。特に、システム変更の際には、以前と同様のセキュリティ強度が保たれているか、確認が必要となるでしょう。 （ご参考） JPCERT/CC - 管理者のためのセキュリティ推進室（第 2 回） http://www.jpcert.or.jp/magazine/atmarkit/ 経済産業省 - 情報セキュリティ監査企業台帳 http://www.meti.go.jp/policy/netsecurity/is-kansa/

[その他]

(iv) 不正プログラム埋め込みの疑い

事例	勝手に知らないホストに接続してメールを送受信しようとしたり、デフラグが勝手に実行されたりした。さらに、何も操作していないのに突然ウイルス実行警告が発せられたりした。色々調べてみると、ファイルが削除されていることに気付いた。ウイルス対策ソフトは導入済み。
解説・対策	日頃からウイルス対策を講じているユーザでも、ウイルスやスパイウェアなどの不正プログラムを埋め込まれてしまうケースが多く報告されています。不正プログラムを実行させようとして、利用者の心理を巧みに利用した手口も横行しているため、**単に技術的対策のみでは予防が不十分になりつつあります。怪しいプログラムのファイルを自分で見分けるなどの“心掛け”が重要になります**。 （本紙冒頭の『今月の呼びかけ』も参考にしてください） （ご参考） IPA - メールの添付ファイルの取り扱い 5 つの心得 http://www.ipa.go.jp/security/antivirus/attach5.html 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 IPA - パソコンユーザのためのスパイウェア対策 5 箇条 http://www.ipa.go.jp/security/antivirus/spyware5kajyou.html

4．相談受付状況

11 月の相談件数は、**673 件**でした。そのうち、アダルトサイトを閲覧した後に「振り込め詐欺」のメールを送りつけられるなど、いわゆる**『ワンクリック不正請求』に関する相談**は、10 月の 1.5 倍以上の**165 件**となり、ますます増加していく傾向にあります。また、ワンクリック不正請求に関する相談のうち **8 割以上が、スパイウェアなどの不正なプログラムを埋め込まれたケース**となっています。＜ワンクリック不正請求相談件数推移…7 月：28 件、8 月：83 件、9 月：80 件、10 月：108 件、**11 月：165 件**＞。

IPA で受け付けた全ての相談件数の推移

		6月	7月	8月	9月	10月	11月
合計		**511**	**554**	**629**	**554**	**606**	**673**
	自動応答システム	289	337	376	337	357	379
	電話	143	128	179	144	165	220
	電子メール	67	84	67	72	82	66
	FAX・他	12	5	7	1	2	8

※ IPA では、コンピュータウイルス・不正アクセス、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）
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。

主な相談事例は以下の通りです。

(i) アダルトサイトでワンクリックしたら・・・

相談	ワンクリック不正請求のサイトに引っ掛かり、“請求書”アイコンがデスクトップに貼り付いた。その後、数分ごとに支払い督促の画面が出現する。ウイルス対策ソフトは日々更新しており、手動スキャンしたら何個か検出されたため、削除した。それでも、支払い督促画面が出現し続けます。
回答	ワンクリック不正請求の手口に使われる不正プログラムは、日々新種のものが出現しています。そのため、**ウイルス対策ソフトによっては検出できないケースが相次いでいます**。この場合、**日にちをおいて再度スキャンすると検出されることが多い**ようです。一刻も早く原因を突き止めたい場合は、**他のウイルス対策ソフトの無償オンラインスキャンや製品体験版をダウンロードして利用することで、検出されることもあります**。

(ii) 新手のワンクリック詐欺？・・・

相談	「月収○万円確実」という題名の迷惑メールが届いた。その本文中に、「サンプル」と題して URL が紹介されていた。このリンク先にはトロイの木馬型の不正プログラムがあり、クリックすることでダウンロードが開始されるようになっていた。
回答	個人情報を盗み出すためのスパイウェアなどの不正なプログラムを埋め込もうとする手口は、日々新しいものが出て来ています。特に最近は、人間の心理を巧みに突いて来るような手口が多く見受けられるようです。**怪しいメールを受信したら、添付ファイルが無いからといって油断せず、さらに題名や本文の内容に惑わされることなく、すぐに削除**してしまいましょう。**間違っても、安易に本文中の URL をクリックしてはいけません**。

(iii) 迷惑メール

相談	出会い系やアダルト系の迷惑メールが届くようになった。よく見ると、差出人も自分のアドレスになっている。もしかすると、自分が差出人に仕立て上げられた同様の迷惑メールが、友人などに届いているかもしれない。
回答	メールが受信される際に、**迷惑メールフィルタに引っ掛かりにくくするため、迷惑メール送信者が故意に差出人と宛先とを同じにしている**と思われます。よって、他の人宛のメールの差出人が貴方のメールアドレスになっている可能性は低いでしょう。

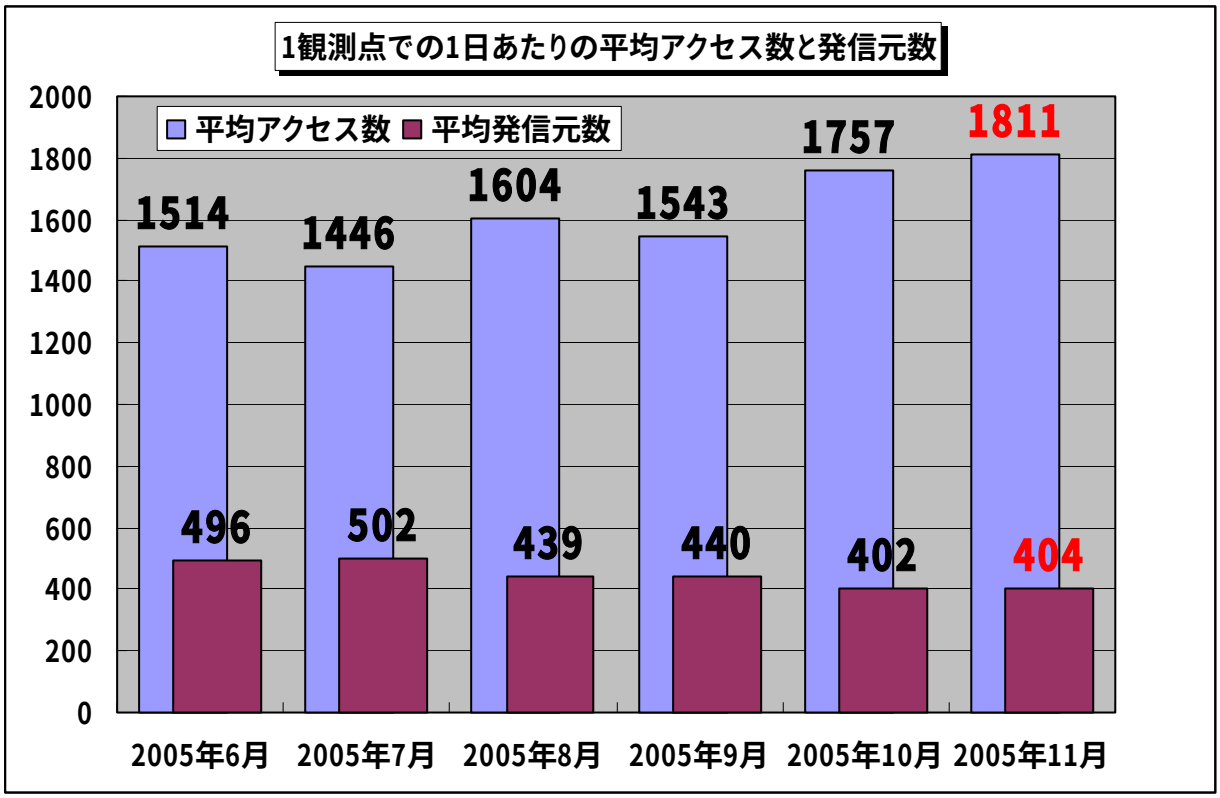
5．インターネット定点観測での 11 月のアクセス状況

インターネット定点観測(TALOT2)によると、2005 年 11 月の期待しない（一方的な）アクセスの総数は、10 観測点で **543,415 件**ありました。1 観測点で 1 日あたり **404** の発信元から **1,811 件**のアクセスがあったことになります。

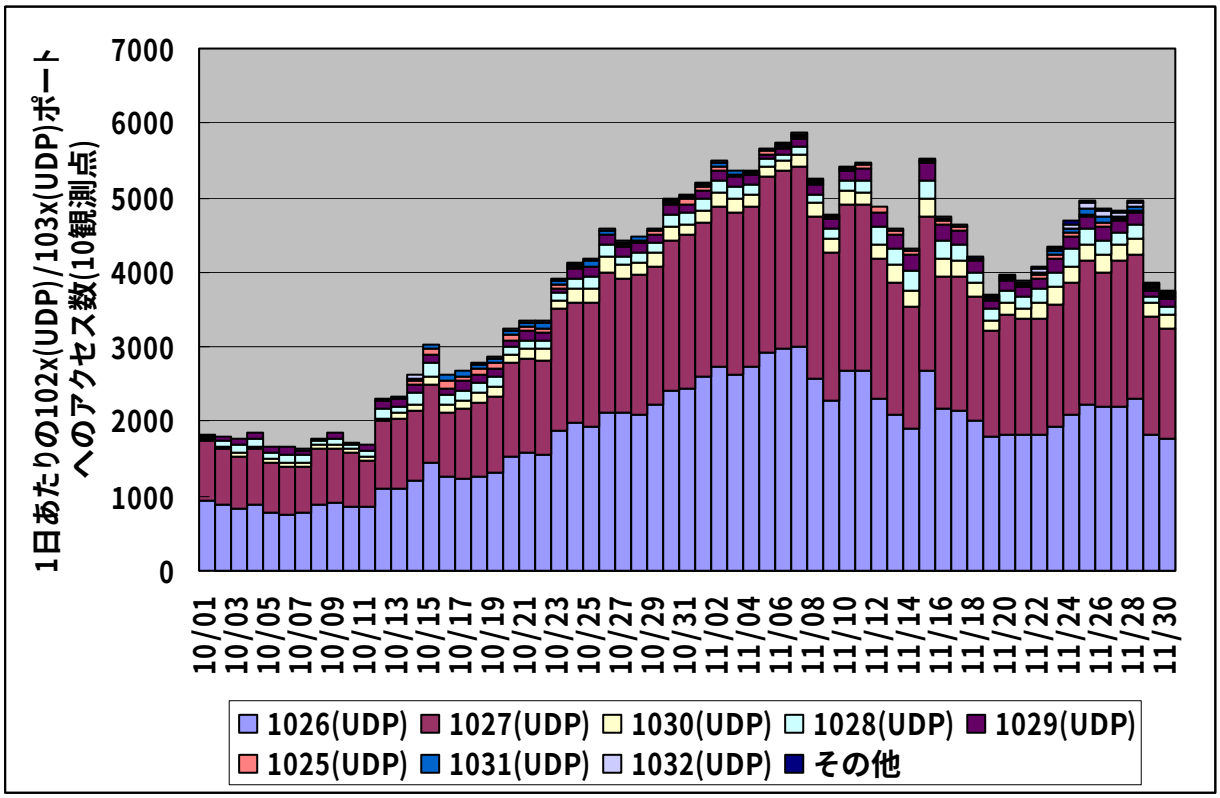
TALOT2 での 1 観測点の環境は、インターネットを利用される一般的な接続環境と同一なので、インターネットを利用される皆さんの環境へも同じくらいの一方的なアクセスがあると考えられます。言い換えれば、**あなたのコンピュータは、毎日、平均して、404 人の見知らぬ人(発信元)から、発信元一人当たり 4～5 件の不正と思われるアクセスを受けている**と言うことになります。

11 月の特徴的なアクセスは 10 月から引き続き発生している 102x(UDP)/103x(UDP)ポート)のアクセスです。11 月のアクセス数と発信元数の関係を図 1 でみると、ここ数ヶ月と比べて、発信元数が減少している割にはアクセス数が多い状況です。この理由として挙げられるのが、これらの 102x/103x(UDP)へのアクセスの増加です。

10 月のレポートでは 1026(UDP)/1027(UDP)ポートへのアクセスが、Windows Messenger 機能を利用したポップアップメッセージを送りつけるものと報告しましたが、その後の調査で、他の 102x(UDP)/103x(UDP)へのアクセスも同じ内容であることが分かりました。メッセージが表示されるだけであれば、パソコンを操作する上では邪魔な存在ということで、特に害のあるアクセスではありませんが、『メッセンジャ サービスのバッファ オーバーランにより、コードが実行される (828035) (MS03-043) 』のパッチが適用されていない場合は、リモートからコードが実行される危険性があります。



【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】

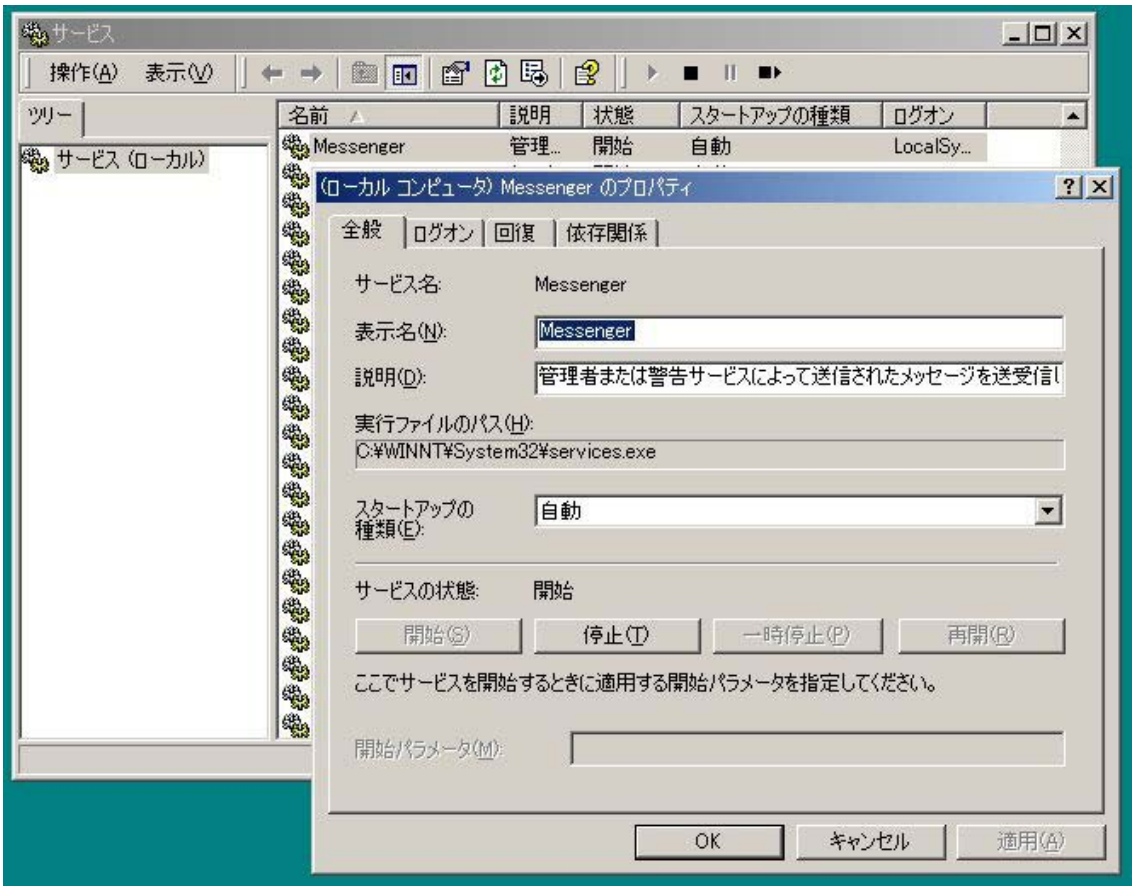


【図 5.2 10 月～11 月の 102x(UDP)/103x(UDP)ポートへのアクセス状況】

STOP! WINDOWS REQUIRES IMMEDIATE ATTENTION.
Windows has found CRITICAL SYSTEM ERRORS.
To fix the errors please do the following:
1. Download Registry Repair from: http://www.********.com
2. Install Registry Repair
3. Run Registry Repair
4. Reboot your computer
FAILURE TO ACT NOW MAY LEAD TO DATA LOSS AND CORRUPTION!

【図 5.3 ポップアップメッセージの例】

- ポップアップメッセージが頻繁に表示されるようであれば、表示を抑止することができます。
  - Windows XP の場合は、「スタート」の「コントロールパネル」から「パフォーマンスとメンテナンス」を選択し、「管理ツール」の「サービス」を起動する。
  - Windows 2000 の場合は、「スタート」の「設定」から「コントロールパネル」を選択し、「管理ツール」の「サービス」を起動する。
  - サービスの画面で Messenger の項目を見つけ、状態が「開始」であれば、この項目を選択し、マウスの右ボタンクリックにより、プロパティを表示する(図 5.2 を参照下さい)。
  - Messenger はデフォルトの状態で、「スタートアップの種類」が「自動」で「サービスの状態」は「開始」となっています。
  - 「(ローカル コンピュータ)Messenger のプロパティ」画面の「スタートアップの種類」を「無効」に変更する(右端の▼で選択できます)。
  - 「サービスの状態」にある「停止」ボタンを押す。
  - Windows XP の場合は、ファイアウォール機能も有効にして下さい。
  - ただし、企業内 LAN 等で使用しているコンピュータの場合は、システム管理者の指示に従って下さい。



【図 5.3 Messenger サービスの停止方法】

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/2005/documents/TALOT2-0512.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）
利用者の個人情報やアクセス履歴などの情報を詐取し、利用者以外のものに自動的に送信するソフトウェア。

(*2) ソフトウェアキーボード（software keyboard）
キーボードを使わずに、マウスでクリックすることで文字入力を可能にするソフトウェアのこと。「仮想キーボード」や「スクリーンキーボード」、「キーボードエミュレータ」などと呼ばれることもある。

(*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) アカウント（account）
コンピュータやネットワーク上の資源を利用出来る権利のこと、または利用する際に必要な ID のこと。

(*6) ポートスキャンツール
サーバ内で動作しているアプリケーションや、OS の種類の情報などから、セキュリティホールを探すためのツール。侵入の準備行為に利用されることが多い。

(*7) SSH スキャンツール
サーバで SSH サービスが動作しているかを調べるためのツール。パスワードを破るための機能を持ったものもある。

(*8) パッチ（patch）
脆弱性などを解消するための、修正プログラムのこと。

(*9) 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。

(*10) 公開鍵認証
公開鍵と秘密鍵のペアでユーザ個人の認証を行う方式のこと。公開鍵はサーバ側で管理し、秘密鍵は個人で管理し、これらによりユーザ認証を行う。

(*11) フリーズ (freeze)
コンピュータの動作が停止し、キーボード入力やマウス操作が受け付けられなくなってしまうこと。

■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／内山
Tel:03-5978-7527 Fax:03-5978-7518 E-mail:isec-info@ipa.go.jp

『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
http://www.ipa.go.jp/security/benchmark/

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。