IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2006 年 1 月 10 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 12 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 12 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：
「メールの添付ファイルやダウンロードしたファイルに要注意！！」
――　怪しいファイルの見分け方　――

1．W32/Sober の亜種の検出数が大幅増！！

2005 年 12 月は、大量メール送信型の **W32/Sober ウイルスのため、ウイルス検出数が 1 千 3 百万を超え（11 月は約 500 万）、前月比約 2.6 倍**と大幅な増加となりました。12 月の感染届出件数は 16 件でした。

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。

感染すると、パソコン内からアドレスを収集し、取得できたアドレス宛にウイルスを添付したメールを送信します。従来のメール送信型ウイルスは、パソコン起動時に 1 回から数回ウイルスメールを送るタイプ等でしたが、本ウイルスは、パソコンが動作している限り**大量のウイルスメールを繰り返し送信しつづけるように仕組まれ**ており、その結果、メールを受信する数が桁外れに多くなっているケースが見受けられました。

大量のメールを送信するため、他者に迷惑をかける恐れがあるとともに、**感染したパソコンではパフォーマンスが低下する**などの症状が起こる可能性があります。

（1）企業における対策

W32/Sober のウイルスメールを大量に受信することで、メールサーバに過負荷がかかっている場合は、負荷を軽減するため、ゲートウェイでの迷惑メールフィルタリングの要領で、W32/Sober のウイルスメールをフィルタリングすることができます。具体的には、当該ウイルスが送るメールの件名や添付ファイル名等でフィルタリングする方法です。

ご参考）
Sober ワームの変種に関する注意喚起 ＜ JPCERT/CC Alert 2005-11-25 ＞
http://www.jpcert.or.jp/at/2005/at050011.txt

（2）一般ユーザにおける対策

まずはワクチンソフトを活用してください。最新の定義ファイルに更新したワクチンソフトであれば、ウイルスメールを受信した段階で警告を表示しますので、感染を未然に防ぐことができます。

また、ワクチンソフトで検出されなくても、**拡張子が「exe」のファイルがメールに添付**されていた場合は、ウイルスや不正プログラムである可能性がありますので、安易に開かないようにしてください（通常のメールのやり取りでは、拡張子“ exe ”のファイルを送付すること自体などありません）。

もしも感染してしまった場合は、以下のサイトに修復方法を掲載しておりますので、ご参照ください。

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

2．ウイルス対策を万全に！

W32/Sober ウイルスを含め、2006 年もウイルスによる被害に遭わないよう、以下のウイルス対策 7 箇条を実践し、便利なインターネットを快適に利用するようにしましょう。

このうち、特に注意が必要な 2．の「メールの添付ファイル」と 3．の「ダウンロードしたファイル」の扱いについて詳しく紹介します。

メールは非常に便利なシステムで、インターネットに接続できれば世界中のどこに居ても、誰とでも文章やファイルのやり取りが可能になります。しかし、メールの添付ファイルとして、ウイルスが届いたり、スパイウェア等の不正プログラムが送り込まれたりします。また、ダウンロードしたファイルも映像や画像に見せかけた不正プログラムである危険性があります。

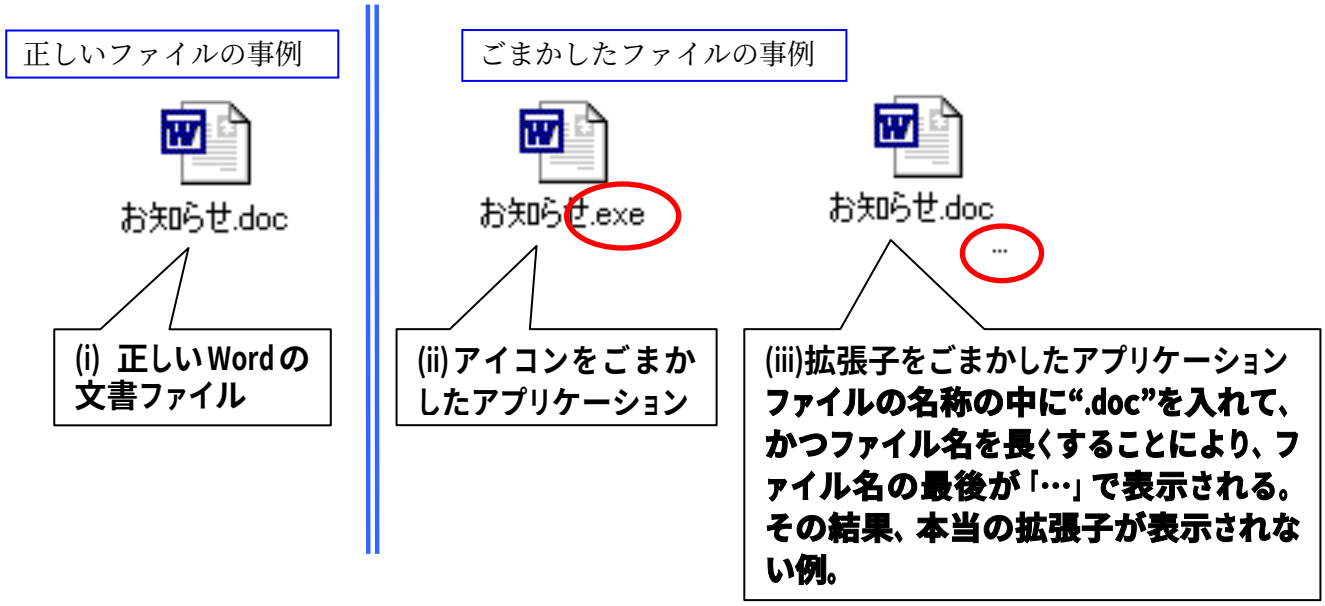
これらの危険に対処するために、**添付ファイルやダウンロードしたファイルは開く前にウイルス検査をする**ことと、**拡張子※により不審なファイルの見分け方を知る**ことが大変重要です。

※ 拡張子：ファイル名の末尾にある 3 文字程度のアルファベット

注意が必要な拡張子の一覧

これらの拡張子のファイルは、開いたとたんにパソコン上で動き始めます。もしも**これらのファイルがウイルスなどの不正プログラムである場合**、あなたのパソコンが感染することになり、個人情報が盗まれたり、ハードディスクの内容が破壊されたり、最悪の場合はパソコンが乗っ取られたりする場合もあります。

また、ウイルスによっては、ファイルタイプをごまかすために、ファイルのアイコンを詐称したり、二重に拡張子を指定したりする場合もあります。



本来、Word の文書ファイルであれば(i)のようになりますが、ファイルタイプがアプリケーションであるのに、Word ファイルのアイコンにごまかしたものは(ii)のようになります。さらに、拡張子をごまかした場合は(iii)のようになります。

以上のような怪しいファイルの見分け方を知っていると、仮に不審なファイルを入手しても危険性が判断できるため、被害を未然に防ぐことができるようになります。このような方法を知ると共に、**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になります。**

※ 拡張子を表示させるための設定方法については、以下のサイトの呼びかけをご参照ください。
コンピュータウイルス・不正アクセスの届出状況[11 月分]について
http://www.ipa.go.jp/security/txt/2005/12outline.html

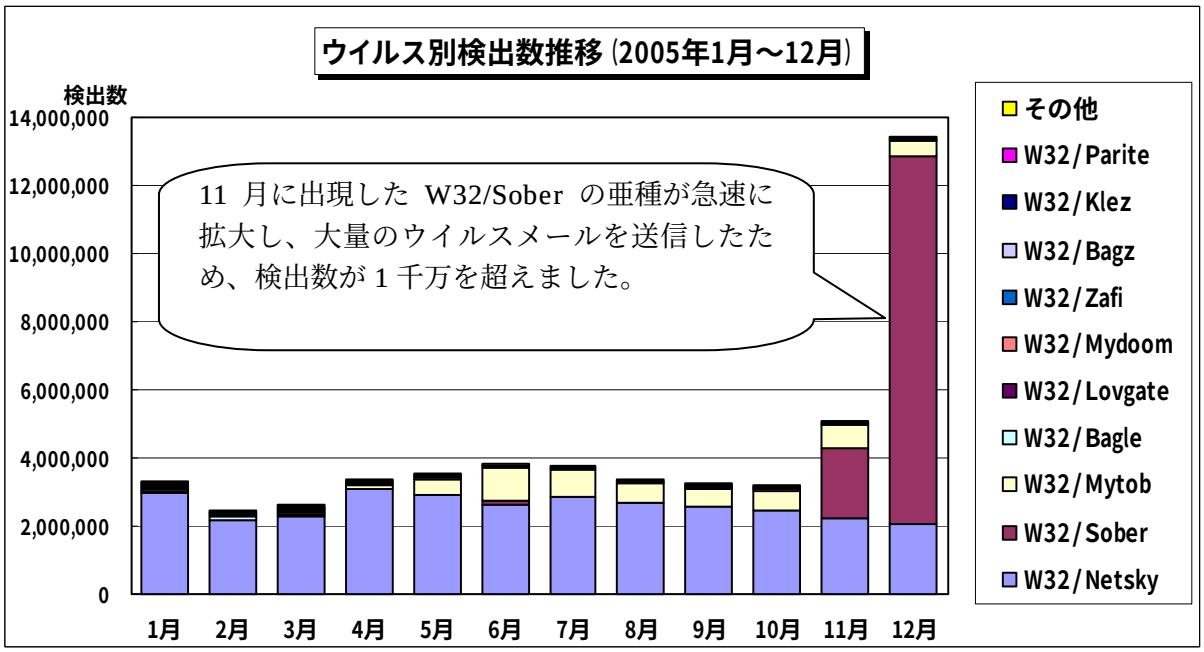
（ご参考）
パソコンユーザのためのウイルス対策 7 箇条を詳細に解説した、『ウイルス対策のしおり』の改訂版を 12 月 20 日に公開しました。ウイルス対策の参考としてご活用ください。

ウイルス対策のしおり
http://www.ipa.go.jp/security/antivirus/shiori.html

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

3．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 1,344 万個**と、11 月の約 510 万個から約 2.6 倍もの大幅な増加となりました。これは、**W32/Sober の亜種**の検出数が 11 月の 202 万個から 1,075 万個と急増したためです。また、12 月の届出件数(※2)は、**4,293 件**となり、11 月の 3,816 件から 12.5%の増加となりました。

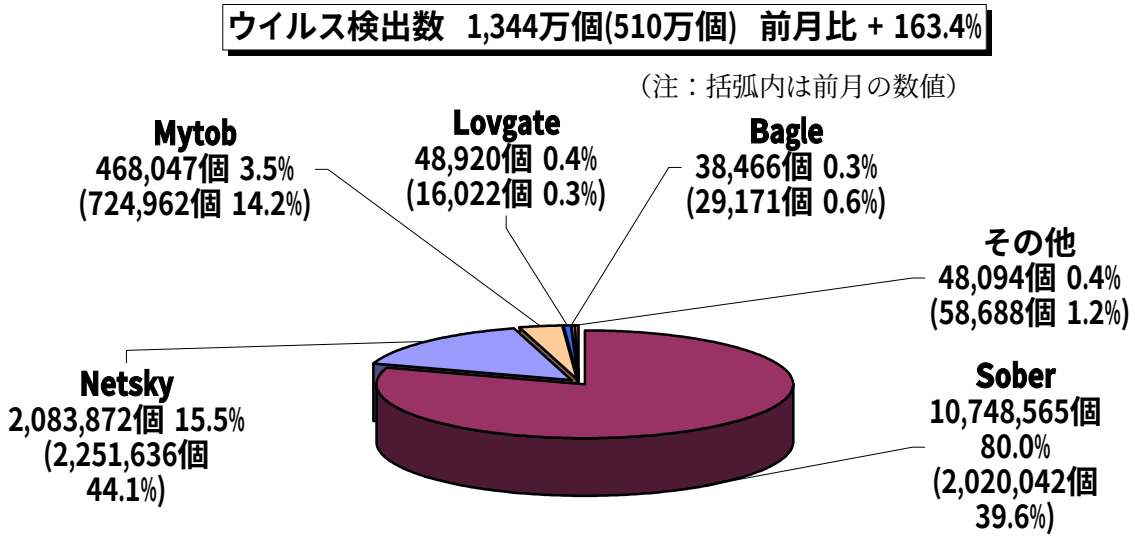


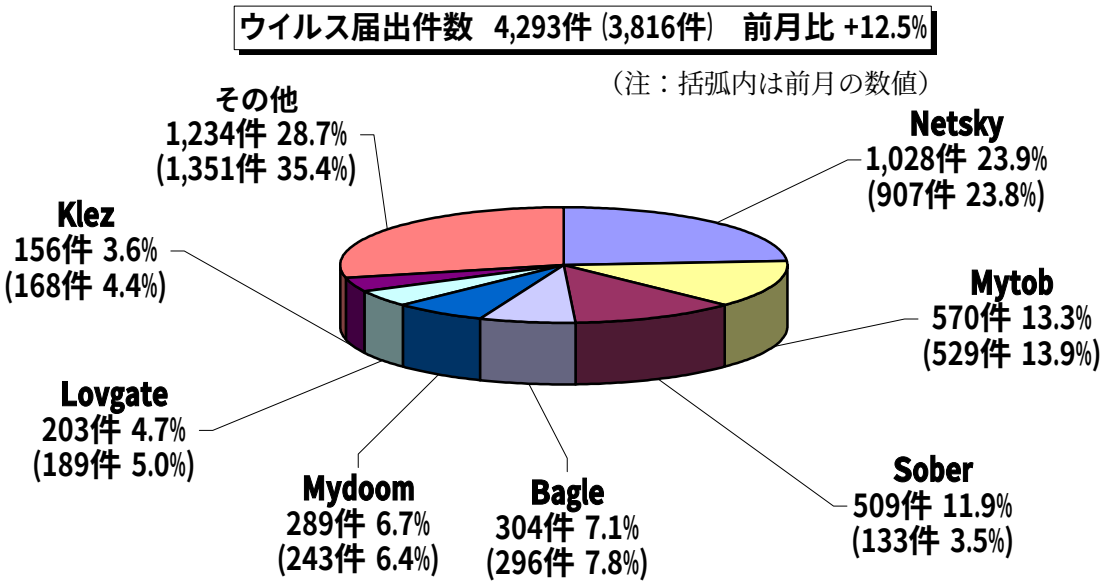
※1 検出数　：届出にあたり届出者から寄せられたウイルスの発見数（個数）
※2 届出件数：同じ届出者から寄せられた届出の内、同一発見日で同一種類のウイルスの検出が複数ある場合は、1 日何個検出されても届出 1 件としてカウントしたもの。
・12 月は、寄せられたウイルス検出数約 1,344 万個を集約した結果、4,293 件の届出件数となっています。

検出数の1位は、**W32/Sober** で**約 1,075 万個でした。**
クライアントを多く有する届出者において、実際にはゲートウェイで検査して被害を未然に防いでいるが、仮にゲートウェイで検査せずにクライアントで検査を行ったとしたときの検出数を集計しているケースを含んでいること及び W32/Sober にメールを繰り返し送信し続けるといった特性があることから、全検出数が多くなっています。
上記以外の届出者の状況を見ても、12 月に W32/Sober ウイルスの急増が見られました。
なお、11 月下旬から 12 月中旬にかけて、諸外国（米国、独国等）において、多数の W32/Sober ウイルスの感染者があったとの情報もあります。

ご参考）
WORM_SOBER.AG 感染状況（トレンドマイクロ社）
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_SOBER.AG

2 位は **W32/Netsky で約 208 万個**と 11 月の約 225 万個から 7.5%の減少となりましたが、依然として高水準で推移しました。続いて、3 位は **W32/Mytob で約 47 万個**となりました。





4．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

5．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

		7月	8月	9月	10月	11月	12月
届出(a)　計		**53**	**41**	**31**	**22**	**24**	**25**
	被害あり(b)	10	12	16	15	15	19
	被害なし(c)	43	29	15	7	9	6
相談(d)　計		**43**	**43**	**30**	**35**	**30**	**25**
	被害あり(e)	24	23	16	25	18	15
	被害なし(f)	19	20	14	10	12	10
合計(a+d)		**96**	**84**	**61**	**57**	**54**	**50**
	被害あり(b+e)	34	35	32	40	33	34
	被害なし(c+f)	62	49	29	17	21	16

（1）不正アクセス届出状況

12 月の届出件数は 25 件であり、そのうち**被害のあった件数は 19 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 25 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 12 件、メール不正中継 1 件、ワーム感染 3 件、DoS 攻撃 1 件、その他(被害あり)2 件**でした。

ここ数ヶ月届出が多く見られる、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 5 件もあり、なおも注意が必要です。

被害事例

[侵入]

（i） SSH で使用するポートへの攻撃

事例	SSH サービスへのパスワードクラッキング(*5)攻撃により、長らく使われていなかった休眠アカウント(*6)の ID とパスワードを解読されて侵入を許してしまった。侵入成功後も連鎖的に被害を受けており、計 4 台の機器で 4 つのアカウント情報を不正に取得されていた。さらに、不正プログラムを埋め込まれて実行され、怪しいサイトに IRC(*7)接続していたことを確認した。
解説・対策	休眠アカウントのパスワードは長期間変更されないまま放置されているため、辞書攻撃に晒されるとパスワードが解読されてしまう可能性が高まります。改めて、**日頃から、アカウント管理とパスワード変更管理を徹底しましょう**。また、この事例では**あるサイトに IRC 接続していたことから、ボット(*8)として操られていた可能性があります**。ボットネットの一員にさせられてしまうと、他のサーバへの攻撃をするなど迷惑行為の一端を担がされてしまい、社会的責任を問われかねません。**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。なお、相変わらず、SSH で使用するポートが狙われる機会が多いようです。**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) 不正プログラムの埋込および外部への攻撃、アカウント情報の奪取

事例	大量の不審なパケットが送信されていると、ネットワーク管理者より通報があり調査したところ、自組織で運用している DNS サーバ、Web サーバ、メールサーバに侵入されていたことが判明。どのサーバも同じユーザ ID で侵入されていた。管理者権限を取得するツールやサーバ攻撃ツールを埋め込まれたり、ウイルスに感染させられたりしており、さらに全ユーザの ID とパスワードが奪取されていた。大量の不審パケットは、外部サーバへの攻撃によるものだった。最初の侵入は発見日から2ヶ月以上前であったことが予想されたが、ログを4週間分しか保存しておらず、詳細の原因究明はできなかった。
解説・対策	侵入された上に、外部サイト攻撃の踏み台として利用されてしまっています。さらに、**DNS サーバやメールサーバも完全に支配下に置かれていたと推測され、このサーバ配下のユーザが自身の意思とは関係なく悪意あるサイトにアクセスさせられたり、メールを盗み見されたりするなどの脅威に晒されていた、ということになります**。この事例ではパスワードが推測容易なものだったことが原因のようですが、最初の侵入時のログが残っておらず、真相究明はできませんでした。**日頃からログをチェックするよう心掛けるとともに、別メディアへのログ書き出しやログサーバの導入など、ログの保管方法について必要に応じて再検討してみましょう**。 （ご参考） IPA - コンピュータ不正アクセス関連 ＦＡＱ http://www.ipa.go.jp/security/ciadr/faq01.html#Q0-5

(iii) Web メールシステムからの侵入

事例	不審なメールが届いているとの苦情が外部からあったためログを調査したところ、自組織で運用している Web メールシステムに既存ユーザに成りすまされてログインされていたことが判明。その結果、海外から迷惑メール発信の踏み台として利用されていた。さらに、不正にログインされたアカウント向けのメールはもちろんのこと、Webメールシステムにログインすることで閲覧可能な、全ユーザ情報（メールアドレスや所属･役職など）も閲覧された可能性が高い。
解説・対策	何らかの方法でアカウント情報を知られた上に、パスワードを破られてしまったのが原因と考えられます。**容易に推測されてしまうようなパスワードを設定せず、かつ定期的に変更する**などの管理徹底はもちろんのこと、**連続何回かログイン失敗するとしばらくアクセスを拒否するなど、サーバ側で工夫することも有効な対策となります**。また、Web メールシステム自体に脆弱性が無いことも、改めて確認しましょう。

[メール不正中継]

(iv) 大量のメール不正中継試行を受けたことによるシステム障害

事例	メール送受信ができなくなったため調査したところ、自組織で運用しているメールサーバがメール不正中継のリクエストを大量に受けて拒否応答を返しており、高負荷状態が続いていたことが判明。一部のメールは実際に不正中継が行われていたため、すぐさま設定を見直すとともに、メール不正中継リクエストには一切の応答を返さないようにして対処した。
解説・対策	メールを不正中継しようとするアクセスが集中したために、攻撃された訳ではなかったにもかかわらず DoS 攻撃(*11)を受けた時のようにサービス妨害をされてしまっています。**明らかに不正と思われる通信リクエストに対しては、不用意に応答しないような設定にすることが肝要です**。またこの例に限らず、**エラーメッセージについても不用意に返してしまうと、不正アクセスのためのヒントを与えることにもなりかねません**ので、同様に注意しましょう。 （ご参考） IPA - UBE（迷惑メール）中継対策 http://www.ipa.go.jp/security/ciadr/antirelay.html

6．相談受付状況

12 月の相談件数は、**653 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**は相変わらず非常に多く、**138 件**もありました。また、ワンクリック不正請求に関する相談のうち **9 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

	7月	8月	9月	10月	11月	12月
合計	**554**	**629**	**554**	**606**	**673**	**653**
自動応答システム	337	376	337	357	379	391
電話	128	179	144	165	220	194
電子メール	84	67	72	82	66	66
FAX・他	5	7	1	2	8	2

※ 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で検出されたものは全て削除しても状況は変わらない。“料金を振り込むと発行されるIDを入力すると、支払い督促画面は出なくなる”と書かれているが、本当でしょうか。それ以外に対処方法は無いのでしょうか。
回答	悪意のあるサイトであれば、料金を振り込んでもIDが発行されない可能性が高いと思われます。なお、今回検出され削除されたウイルスは、ワンクリック不正請求とは直接関係の無いものだったようです。**支払い督促画面が出なくするためには、原因となっているプログラムを特定して削除する必要がありますが、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**。ウイルス対策ソフトで検出できない場合、**Windows XP や Me であれば、「システムの復元」機能を使うと、支払い督促画面が出現する以前の状態に戻すことができる場合があります**。 (ご参考) システムの復元を使用して Windows XP を復元する方法 http://support.microsoft.com/kb/306084/ja

(ii) スパイウェア対策ソフトを騙ったスパイウェア？

相談	突然ポップアップ画面が出て「パソコンにエラーが発生しました。修理したい場合は、このプログラムをダウンロードしてください」などと書かれていた。スパイウェア対策ソフトのようだったので、クレジットカード番号を入力して購入手続きしてしまい、インストールされてしまった。後日、そのプログラムは、スパイウェア対策ソフトを騙ったスパイウェアである可能性が高いことが判明した。購入の取り消しはできるのでしょうか。また、どうやってアンインストールするのでしょうか。
回答	パソコンユーザの不安を煽るような文句を並べることで、スパイウェア対策ソフトの購入を迫るという悪質な手口のようです。**即座に判断できないようなメッセージが表示された場合は、安易に[はい]をクリックしたり、申し込みなどの手続きをしたりすることは避けましょう**。アンインストールしたい場合は、まずは**コントロールパネルの「プログラムの追加と削除」(Windows XP の場合) から削除できるかどうかを試してみましょう。ウイルス対策ソフトで削除できる場合もあるようです**。なお、購入の取り消しの可否については、クレジットカード会社や最寄りの消費者センターに相談してください。 (ご参考) 全国の消費生活センター http://www.kokusen.go.jp/map/ 国民生活センター http://www.kokusen.go.jp/

(iii) 迷惑メールが届くようになったのですが・・

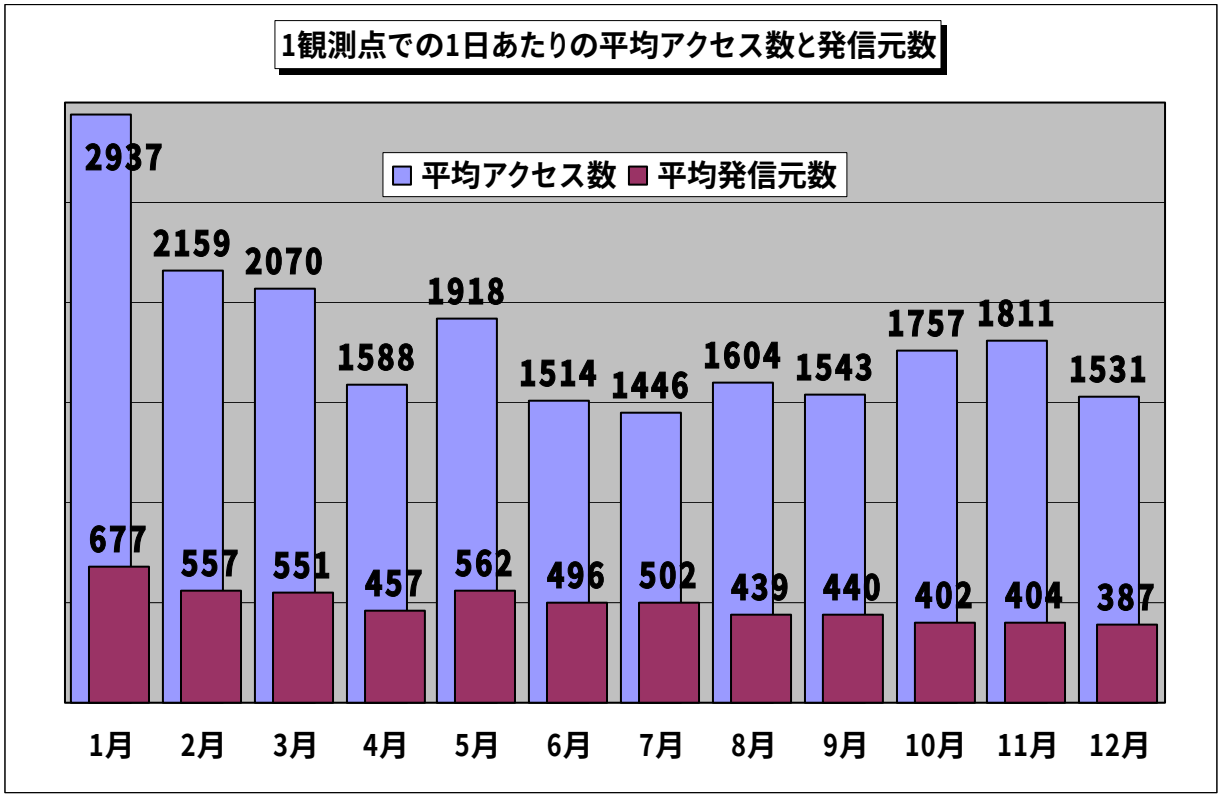
相談	出会い系やアダルト系の迷惑メールがたくさん届くようになった。届かなくする方法はあるのか。
回答	このような**迷惑メールは、技術的には送信自体を止められませんので、「送信を止めさせる」手立てが必要です**。メールヘッダ情報を基に送信元コンピュータ情報を割り出し、送信元コンピュータが所属するネットワーク（プロバイダなど）の管理者宛に対処を依頼することになります。 また、「特定電子メールの送信の適正化等に関する法律（平成 14 年法律第 26 号）」によれば、**以下の機関が相談・問い合わせ・情報提供機関として指定されています**。 (ご参考) ･出会い系サイトなどの迷惑メールに関する相談など (表示義務違反メールなどに関する情報提供、電話相談) 財団法人日本データ通信協会　迷惑メール相談センター（総務省指定機関） http://www.dekyo.or.jp/soudan/top.htm ･物品の販売などの商取引に関する迷惑メールに関する相談など (再送信禁止義務違反メールの情報提供) 財団法人日本産業協会（経済産業省指定機関） http://www.nissankyo.or.jp/ なお、「**特定電子メールの送信の適正化等に関する法律の一部を改正する法律　（平成 17 年法律第 46 号）**」が 2005 年 11 月 1 日に施行されました。これによれば、**”送信者情報を偽った送信の禁止”が新たに謳われている(第六条)ため、今回のような違法メールの取締りが強化されると思われます**。 (ご参考) 総務省 - 迷惑メール対策 http://www.soumu.go.jp/joho_tsusin/d_syohi/m_mail.html

7．インターネット定点観測での 12 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 12 月の期待しない（一方的な）アクセスの総数は、10 観測点で **474,526 件**ありました。1 観測点で 1 日あたり **387** の発信元から **1,531 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、387 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。

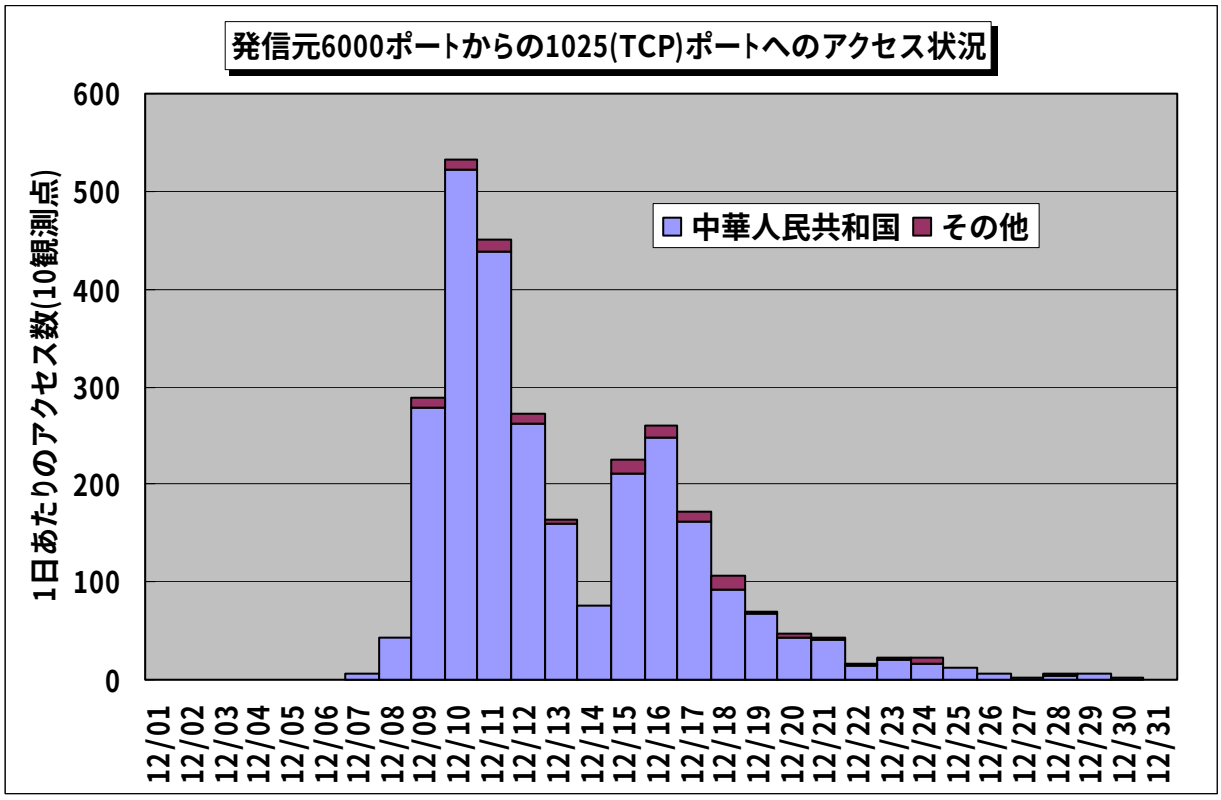
2005 年 1 月～12 月までの各月の 1 観測点での 1 日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図 5.1 に示しています。この図を見ると、2005 年の後半は、アクセス数および発信元数が同じ水準であるようです。状況は定常化していると言えます。



【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】

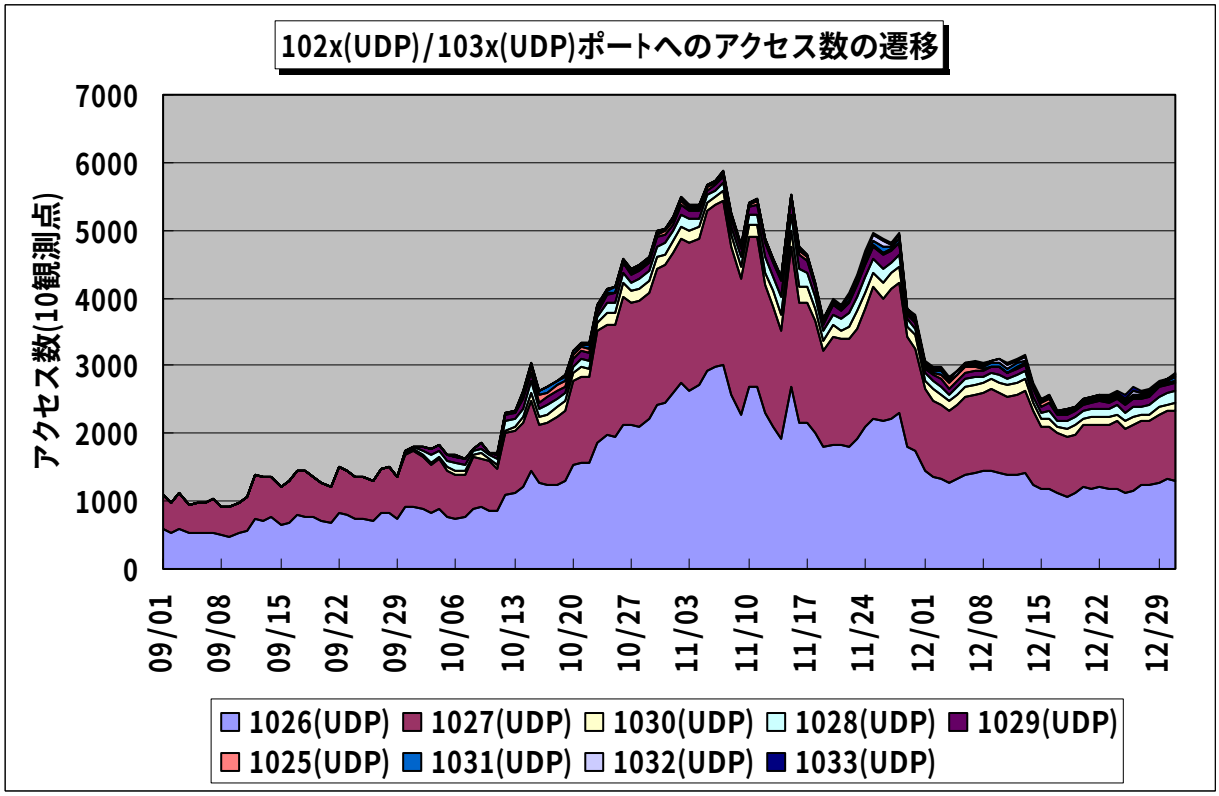
12 月の特徴的なアクセスは、**Dasher** と呼ばれるワームによる発信元 6000 ポートからの 1025(TCP)ポートへのアクセスです。このアクセスは、Windows の脆弱性(MS05-051)を狙ったもので、該当脆弱性のパッチが適用されていない状態で、インターネットに直接接続（グローバル IP で接続）されたコンピュータの場合は、感染する可能性があります。実際には、月末に向けてアクセス数は減少傾向にあるようです(図 5.2 を参照下さい)が、被害にあわないための対策は以下の通りです。

- **Windows Update (Microsoft Update) により Windows の脆弱性を解消する**
- **インターネットと直結接続している場合は、ルータ等の機器を導入する**
- **Windows XP の場合は、ファイアウォール設定を有効にする**
- **パーソナルファイアウォールを導入する**



【図 5.2　発信元 6000 ポートからの 1025(TCP)ポートへのアクセス状況】

また、10 月に発生した 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 102x(UDP)/103x(UDP)ポートへのアクセスも、10 月や 11 月に比べると減少したものの、あいかわらず継続しています(図 5.3 を参照下さい)。102x(UDP)や 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**(http://www.ipa.go.jp/security/txt/2005/documents/TALOT2-0512.pdf を参照下さい)をお勧めします。



【図 5.3 102x(UDP)/103x(UDP)ポートへのアクセス数の遷移】

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/TALOT2-0601.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) パスワードクラッキング（password cracking）
他人のパスワードを、解析するなどして探り当てること。総当り攻撃や辞書攻撃といった手法があり、クラッキング用のプログラムも存在する。

(*6) 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。

(*7) IRC（Internet Relay Chat）
チャット（接続者同士のリアルタイムな会話）システムのこと。インターネット上の IRC サーバに、専用のソフトウェアを利用してアクセスすることで、複数のユーザとの間でメッセージの交換が出来る。ファイル通信にも対応する。

(*8) 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。

(*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) 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／内山
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
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。