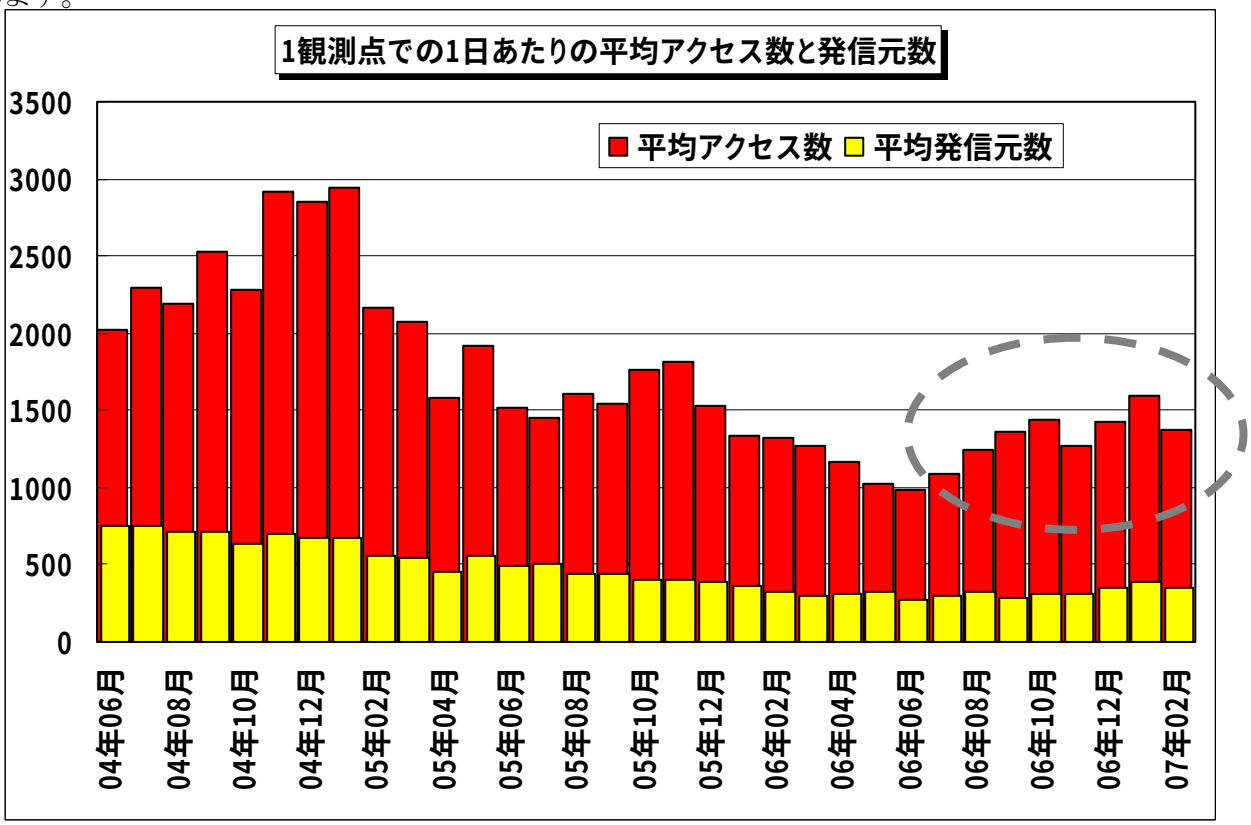
プレスリリース
2007 年 3 月 2 日
独立行政法人 情報処理推進機構

コンピュータウイルス・不正アクセスの届出状況［2007 年 2 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 2 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： 「いつも誰かにどこかから狙われています！！」
－OS 等のセキュリティ機能を使って基本の対策を実施しよう －

IPA のインターネットの観測状況をみると、昨年後半からインターネット上のセキュリティホール対策などが取られていないコンピュータを探すことを目的と考えられるアクセスの増加傾向がみられます。



このようなアクセスを行う目的として、ボット、ワーム等の不正なプログラムを感染させようとするものが考えられます。この他にも色々な脅威が考えられますので、インターネットに繋ぐと、さまざまな不正なアクセスを受ける可能性のある状態になっている事を認識して、インターネットを利用することが必要になります。

こうしたことからお使いのコンピュータを守るためには、日頃のセキュリティホール対策(OS やワープロなどの各種ソフトウェアのアップデート)の実施だけでなく、OS に内蔵された Windows ファイアウォールなどのファイアウォールの利用をお奨めします。

オンラインゲーム等の利用で Windows ファイアウォールを[無効]にするといった本来推奨されない設定をしている場合は、設定を確認して必ず[有効]に戻しましょう。

注）国内の大手インターネットサービスプロバイダー(ISP)の内、大手 10 社の ISP で日本におけるインターネット接続の 80%をカバーしており、 IPA においてもその大手 10 社の ISP と一般利用者と同じ ADSL によるインターネット接続を行って、脆弱性を突こうとするインターネット上の動きに対して状況把握などを行い、監視を継続して行っています。詳細は、別紙 4 の 4 頁を参照してください。

http://www.ipa.go.jp/security/txt/2007/documents/TALOT2-0703-kaisetsu.pdf

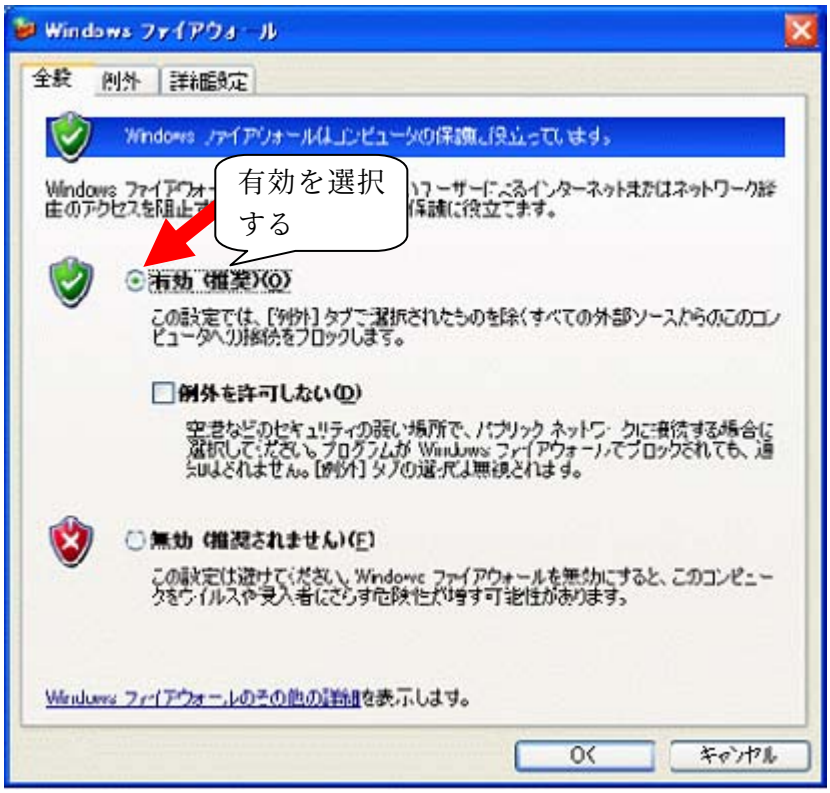
Windows ファイアウォールを有効にするための基本的な設定は以下の通りです。

● Windows XP での設定方法

操作手順:

「スタート」→「設定」→「コントロールパネル」→

「Windows セキュリティ センター」→「Windows ファイアウォール」

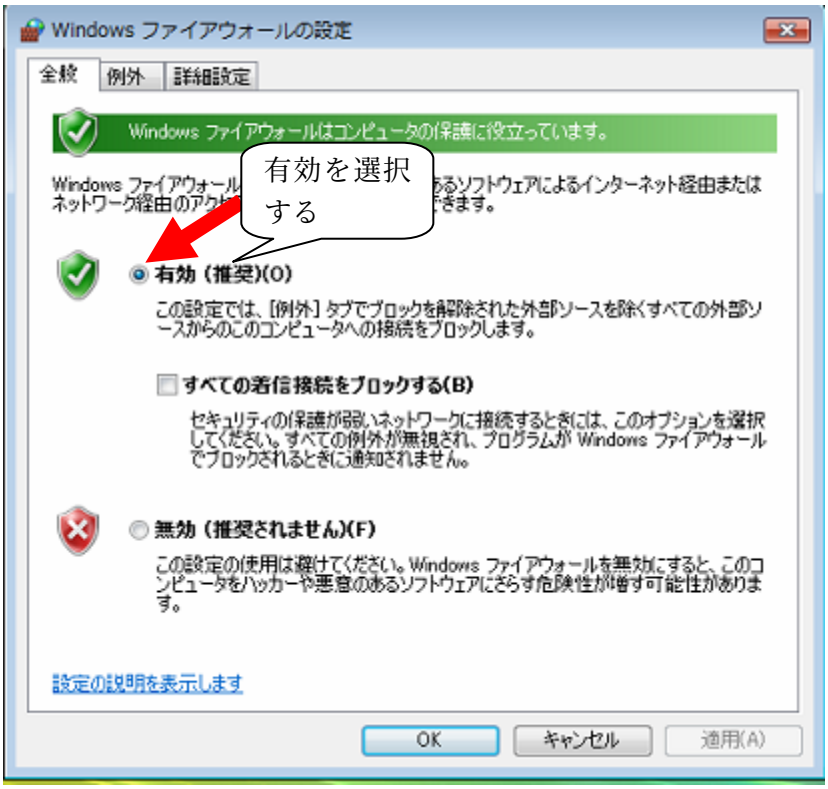


●Windows Vista での設定方法

「 」→「コントロールパネル」→「セキュリティ」→

「Windows ファイアウォールの有効化または無効化」

※管理者のパスワードまたは確認を求められた場合は、パスワードを入力するか、確認情報を提供します。



今月のトピックス

1.コンピュータ不正アクセス被害の主な事例(届出状況及び被害事例の詳細は、5 頁の「3.コンピュータ不正アクセス届出状況」を参照)

・SSH で使用するポートへの攻撃
・フィッシングサイトを設置された

2.相談の主な事例 (相談受付状況及び相談事例の詳細は、7 頁の「5.相談受付状況」を参照)

・芸能人の情報を検索していたのにアダルトサイトの請求書が
・フィッシングメールが届いた

3.インターネット定点観測(詳細は、別紙4を参照)

IPA で行っているインターネット定点観測について、初めて包括的で詳細な解説を行っています。

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 69 万個**と、1 月の 102 万個から 32.3%の減少となりました。
また、2 月の届出件数(※2)は、**3,098 件**となり、1 月の 3,513 件から 11.8%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。
・2 月は、寄せられたウイルス検出数約 69 万個を集約した結果、3,098 件の届出件数となっています。

検出数の1位は、**W32/Netsky** で**約 51 万個 、2 位は W32/Nuwar** で**約 6 万個、3 位は W32/Sality** で**約 4 万個でした。**

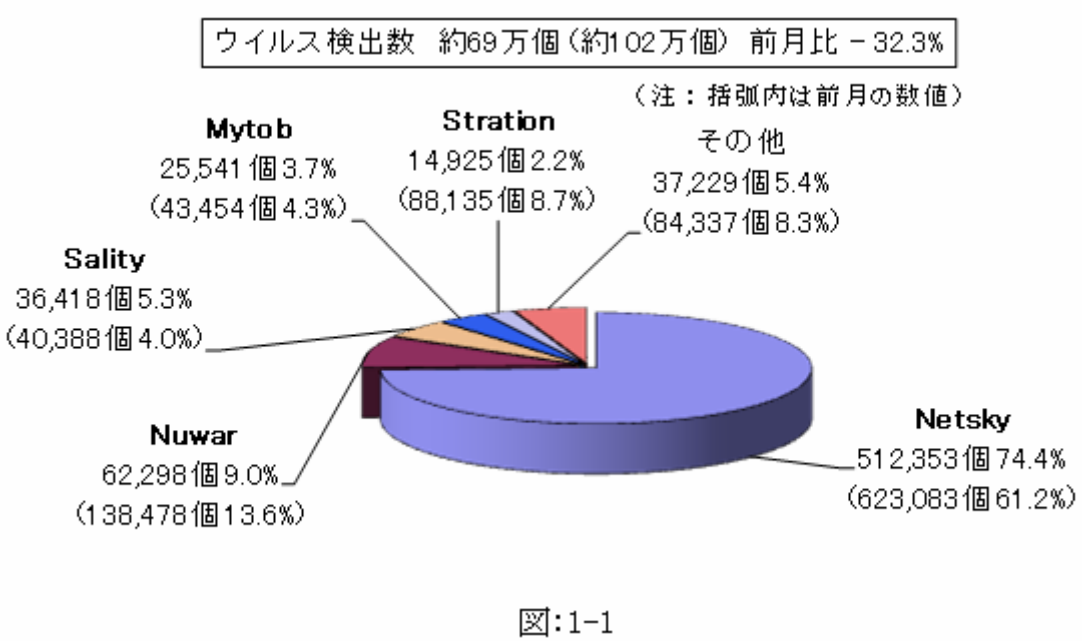
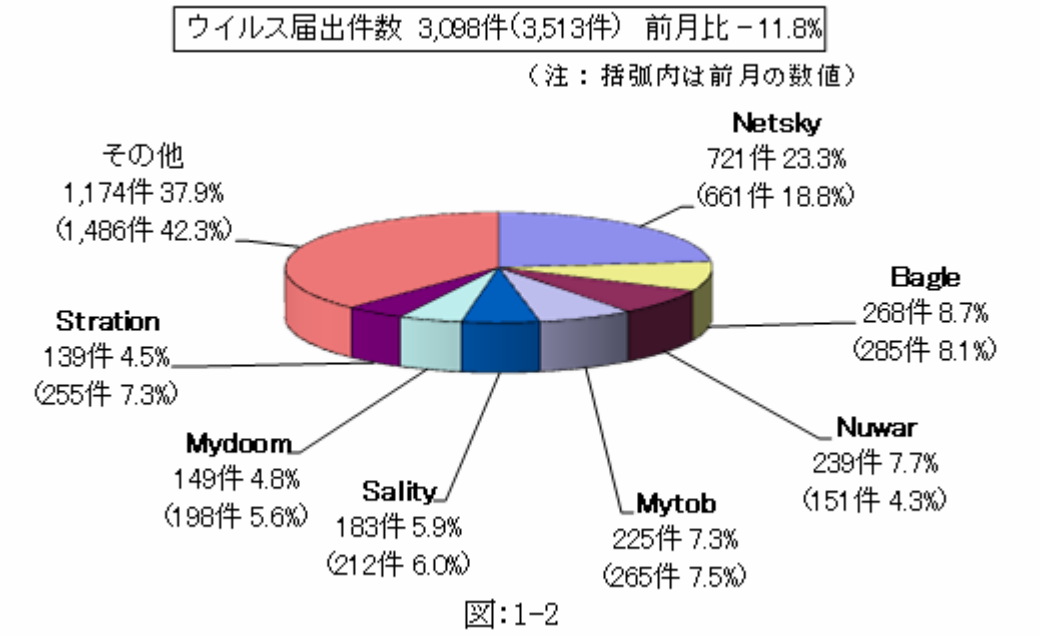


図:1-1



図：1-2

2．W32/Nuwar ウイルスが蔓延

W32/Nuwar ウイルスは、IPA に初めて届出された 2006 年 12 月から 2007 年1月、2月と継続して高水準の届出となっており、蔓延している状況を示しています。このウイルスは、感染した PC から大量のメールを配信することにより感染を拡げるタイプです。感染したユーザは、PC を乗っ取られたり、個人情報が盗まれるなどの被害に遭っています。

●ウイルスの概要

W32/Nuwar は、大量のメールを配信することにより感染を拡げるタイプのウイルスで、感染した PC の中に trojan_small という名称の他の不正なプログラムを取り込む機能を持ったファイルを作成します。その後 trojan_small が動作することにより、スパイウェアなどをインターネットから取込み、**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**などの被害を起こす可能性があります。

「マカフィー株式会社」
http://www.mcafee.com/japan/security/virN2006.asp?v=W32/Nuwar@MM
「株式会社シマンテック」
http://www.symantec.com/region/jp/avcenter/venc/data/jp-w32.mixor@mm.html
「トレンドマイクロ株式会社」
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM%5FNUWAR%2EEL

●対策

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。

- 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

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

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

		9月	10月	11月	12月	1月	2月
届出(a) 計		**46**	**22**	**24**	**10**	**32**	**23**
	被害あり(b)	21	15	8	9	22	14
	被害なし(c)	25	7	16	1	10	9
相談(d) 計		**35**	**53**	**30**	**40**	**52**	**50**
	被害あり(e)	26	37	20	23	25	28
	被害なし(f)	9	16	10	17	27	22
合計(a+d)		**81**	**75**	**54**	**50**	**84**	**73**
	被害あり(b+e)	47	52	28	32	47	42
	被害なし(c+f)	34	23	26	18	37	31

（1）不正アクセス届出状況

2 月の届出件数は 23 件であり、そのうち**被害のあった件数は 14 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 50 件（うち 8 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 28 件でした。

（3）被害状況

被害届出の内訳は、**侵入 6 件、DoS 攻撃 1 件、アドレス詐称 1 件、その他（被害あり）6 件**でした。

侵入届出の被害内容は、外部サイトを攻撃するための踏み台にされていたものが 5 件、フィッシング(*1)に悪用するためのコンテンツを設置されていたものが 1 件でした。侵入の原因は、SSH(*2)で使用するポート(*3)への攻撃を受けてパスワードが破られたと思われたこと、OS や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) SSH(*2)で使用するポート(*3)への攻撃

事例	・外部の組織から、「あなたのサイトから不正アクセス試行を連続して受けている」とメールで連絡を受けた。 ・サイトを調査したところ、SSH(*2)で使用するポート(*3)へ攻撃を受け侵入されていたことが判明。その上、不正プログラムを埋め込まれて**外部サイト攻撃の踏み台**にされていた。 ・SSH による**接続許可ドメインの制限がされていなかった**ことと、SSH ログインの**パスワードが容易に推測可能だった**ことが原因。
解説・対策	外部からの接続許可制限が無かったことで狙われてしまい、パスワードクラッキング(*4)攻撃を受けたものと思われます。さらに**踏み台として悪用され、被害を拡大させてしまった**残念な例です。 上記の問題点を改善することはもちろんですが、**SSH 運用時には、ログインの際に公開鍵認証(*5)などの強固な認証の採用を推奨します**。 止むを得ずパスワード認証を利用する場合でも、ログ(*6)のチェックをこまめに実施しましょう。攻撃の兆候を早めにつかむことができたり、外部への攻撃アクセスを把握できたりするため、例え侵入された場合でも被害を最小限に食い止めることができます。 (参考) IPA - 今月の呼びかけ(2006/6 月分) 「パスワードを一つ残らず、きちんと管理しましょう！」 http://www.ipa.go.jp/security/txt/2006/07outline.html 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

(ii) フィッシング(*1)サイトを設置された・・

事例	・自社が運用するウェブサイトを閲覧したユーザから、「サイトにアクセスすると海外の**金融機関のようなサイトにジャンプしてしまう**」との連絡が入った。 ・サイトを調査したところ、ウェブサーバ内にフィッシングに悪用するためのコンテンツデータを発見。アクセス**ログ(*6)をチェックしようとしたが、全て削除されていた**。 ・OS のアップデートを怠っていたため、ぜい弱性を突かれたのが侵入の原因と思われた。
解説・対策	企業のウェブサイトなど **24 時間稼動しているサーバは常に狙われている**ことを、改めて認識しましょう。侵入などの被害に遭わないためにも日頃からぜい弱性情報に気を配り、**セキュリティパッチをタイムリーに適用していくことが、最も基本的かつ重要な対策**となります。さらに、アクセス**ログをこまめにチェックする**ことで、万が一の際でも被害を最小限に食い止めることができます。 (参考) 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

4．相談受付状況

2 月の相談総件数は **1019 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 **287 件**(1 月 :233 件)と今までで最悪となり、その他は**『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 **22 件**(1 月 :17 件)、**Winny に関連する相談**が **14 件**(1 月 :13 件)などでした。

IPA で受け付けた全ての相談件数の推移

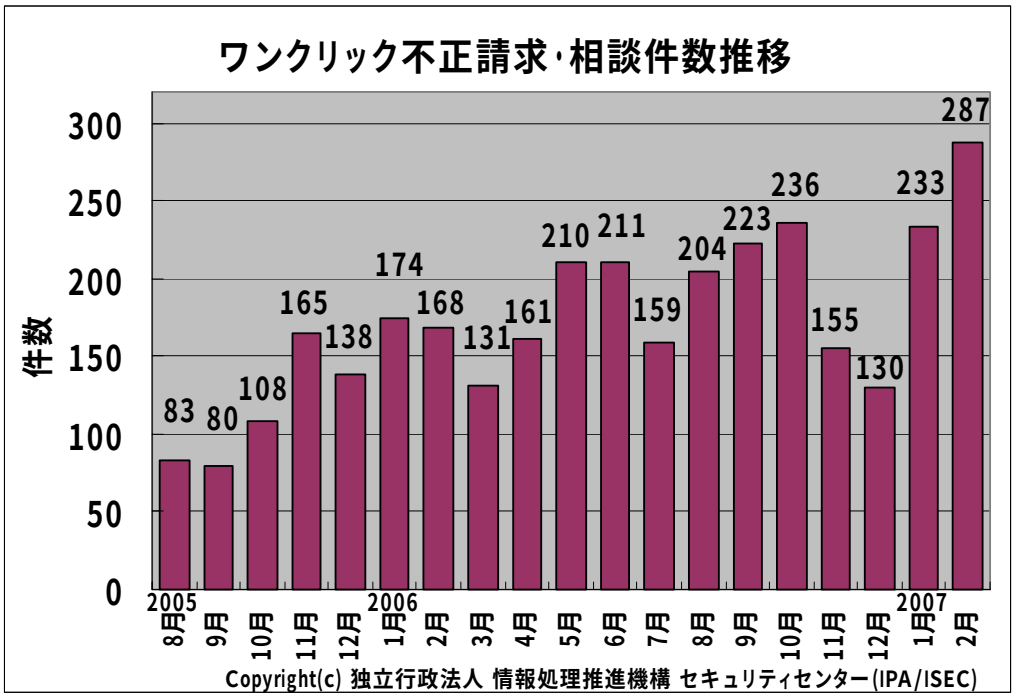
		9月	10月	11月	12月	1月	2月
合計		**933**	**1002**	**711**	**680**	**946**	**1019**
	自動応答システム	575	580	423	394	582	603
	電話	302	326	214	222	324	336
	電子メール	51	93	72	59	39	75
	その他	5	3	2	5	1	5

※ 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



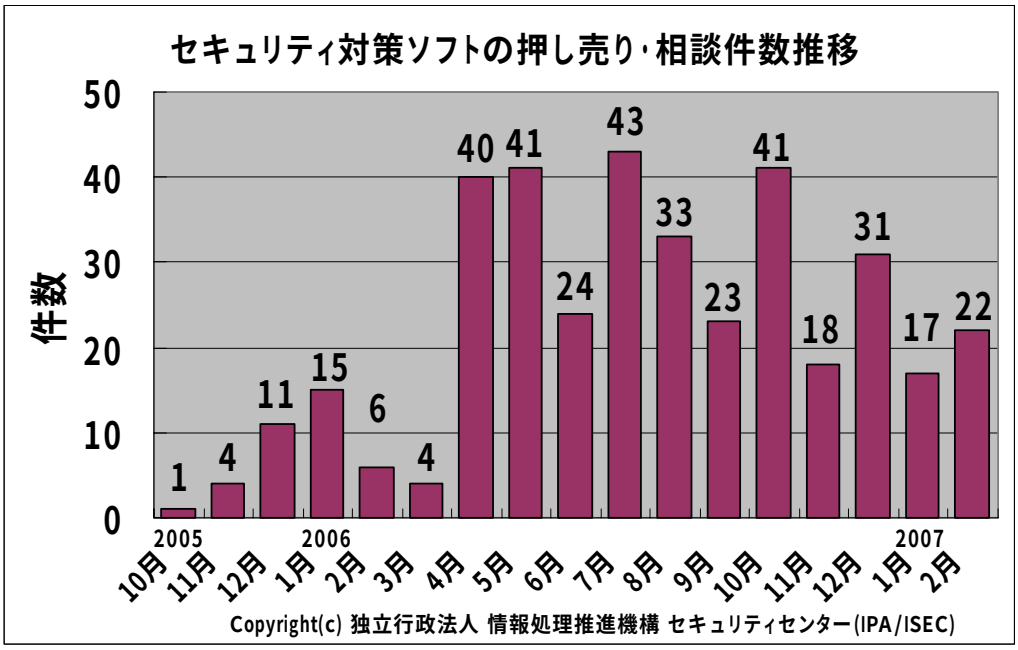
ワンクリック不正請求についての対策については下記をご参照ください。

・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) 芸能人の情報を検索していたのにアダルトサイトの請求書が！

相談	芸能人の情報を検索サイトで調べ、ファンが作ったと思われるブログを見つけた。アクセスしてみると、芸能人の画像が貼り付けてあった。「もっと見たい方はこちら」というリンクをクリックしたら、いきなりアダルトサイトにジャンプした。びっくりしたが、ちょっと興味があったので「無料動画」などと書かれていたリンクをクリックしたら、年齢認証や入会規約などが表示された。**よく読まずに[OK]をクリックしたら、サイトの利用料金の請求書が現れた**。
回答	まずは慌てずに、**パソコンを再起動してみましょう。それで請求書が現れないのであれば、何も心配する必要は無いケースがほとんどです**。2 月に IPA に寄せられたワンクリック不正請求関連相談のうち、約 3 割はこのようなケースでした。アダルトサイト以外から誘導されるケースが急増しており、油断は禁物です。**突然アダルトサイトにジャンプしたとしても興味本位でその先に進むのは控えましょう**。なお、**入会規約にはその先で提供されるサービスが有料であることが明示されているケースがほとんど**です。クリックする前に、画面に表示されているメッセージをしっかりと読むことも、被害を防止するために重要な心掛けとなります。

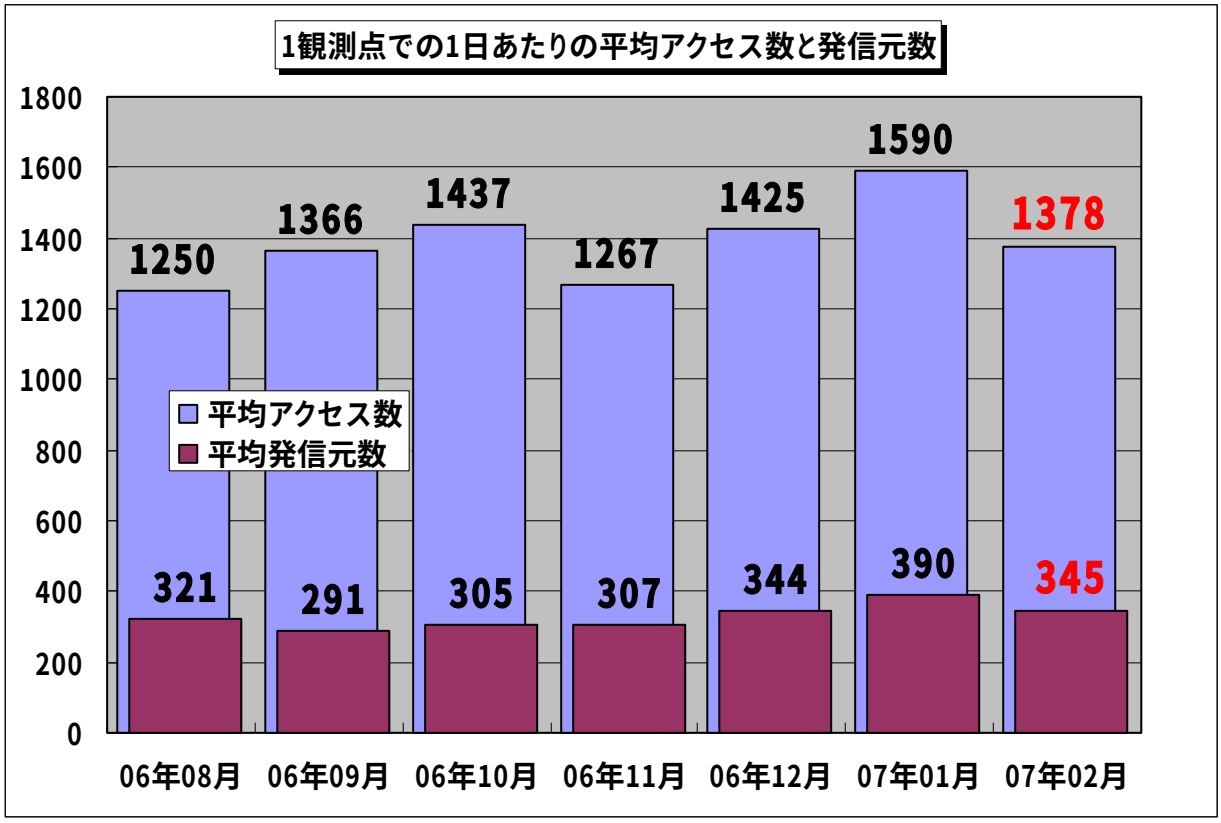
(ii) フィッシング(*1)メールが届いた？！

相談	以下のようなメールが届いたが、差出人アドレスや本文中のリンク先アドレスがヤフーではないようなので、クリックすることは控えた。 From:　"Yahoo JAPAN"〈■488700@pp.love▲.jp〉 To:　●●@yahoo.co.jp Subject: Yahoo! JAPAN - ユーザーアカウント継続手続き ---------- Yahoo! JAPAN - ユーザーアカウント継続手続き ---------- ********** このメッセージは、Yahoo! JAPAN より自動的に送信されています。 （略） Yahoo!オークションを継続してご利用いただくためには、Yahoo! JAPAN ID ユーザーアカウント更新手続きが必要です。 詳しくはユーザーアカウント継続手続きページをご覧ください http://■488700.love▲.jp/
回答	このようにサービス運用会社や金融機関からのメールと思わせ、本文中のリンクをクリックさせようとする、フィッシングの手口に注意しましょう。クリックすると、本物そっくりに作られた個人情報入力ページに誘導されてしまいます。 アドレスを見抜く知識が無い場合でも、**メール本文中にあるリンクは不用意にクリックしない**、**サービス運用会社に直接電話を掛けて確認する**、といった対策が有効です。 （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/

5．インターネット定点観測での２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 2 月の期待しない(一方的な)アクセスの総数は、10 観測点で **330,685 件**ありました。1 観測点で 1 日あたり **345** の発信元から **1,378 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、345 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】

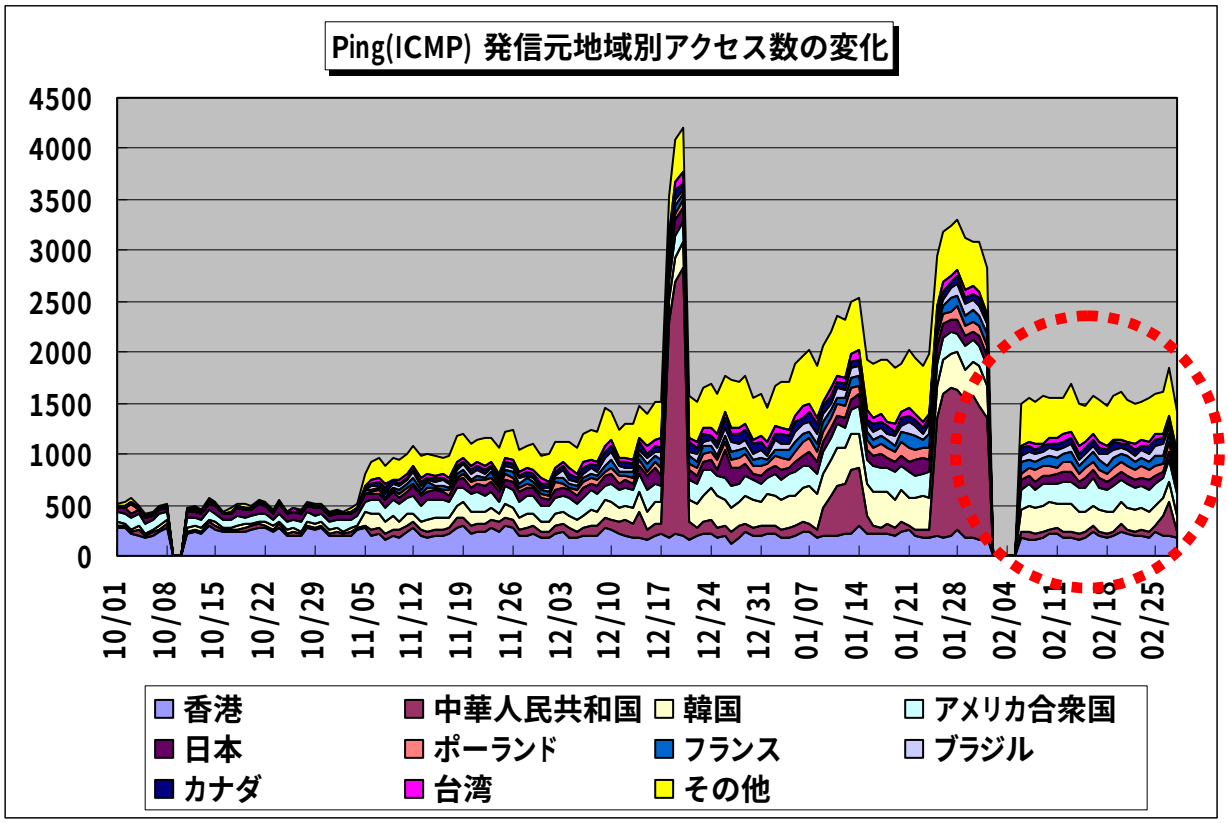
2006 年 8 月～2007 年 2 月までの各月の 1 観測点での 1 日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図 5.1 に示します。この図を見ると、期待しない(一方的な)アクセスは、2007 年 1 月に比べて多少の減少傾向で、ほぼ 2006 年 12 月の状況に戻りました。この減少傾向は、Ping(ICMP※)の安定化およびコンピュータの脆弱性を狙ったアクセスの安定化が原因と思われます。

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。

※ 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

2007 年 2 月のアクセス状況は、全体的には 2007 年 1 月とほぼ同じ状況ですが、前述したように Ping(ICMP)アクセスの安定化傾向、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)の減少傾向が見られ、ボットの感染活動が頭打ちになってきたと考えられます。
2007 年 2 月は、月初に TALOT2 システムのメンテナンスのため、2 日～5 日まで観測データがありませんが、この期間内にアクセスが安定化したようです。

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 2007 年 1 月～2 月の 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、2006 年 11 月以降の増加傾向および中国方面からの一時的な増加を示していますが、2007 年 1 月の中国方面からのアクセス増加が、2 月 6 日以降は無くなりました。他の発信元地域からのアクセスを含めて、増加傾向は安定方向へ移行しつつあるようです。これらのアクセスの原因は不明ですが、脅威は依然として続いています。

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/2007/documents/TALOT2-0703.pdf

「IPA におけるインターネット定点観測について」の解説は、こちらのサイトでご参照ください。
http://www.ipa.go.jp/security/txt/2007/documents/TALOT2-0703-kaisetsu.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) **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。

(*2) **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。

(*3) **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。

(*4) **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。
＊:総当り攻撃
何らかの規則にしたがって、文字の組み合わせを総当りで試行する攻撃方法のこと。いわゆる力ずくの攻撃方法のことで、ブルートフォース攻撃ともいう。
＊:辞書攻撃
パスワードを破るために、辞書にある単語などを片端から試行する攻撃方法のこと。

(*5) **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。

(*6) **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。

■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。