プレスリリース
2007 年 4 月 3 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 3 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 3 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：
「警告画面を無視していませんか？」
――　不正プログラムを取り込まないために、
警告が出たら先に進まないこと！！　――

IPA に寄せられるワンクリック不正請求の相談件数が、2007 年 2 月に引き続き過去最悪の記録を更新し、3 月は **316 件**となりました。（詳細は、P7 ワンクリック不正請求相談件数の推移を参照）

Windows では、通常のホームページに掲載された写真や動画をクリックすると、パソコンに既にインストールされている画像表示ソフトや動画再生ソフトが起動します。しかし、ワンクリック不正請求画面を表示するウイルスなどの悪意あるプログラムが写真や動画に見せかけてホームページに置かれていた場合には、その写真や動画をクリックすると、Windows はプログラムをダウンロードして当該プログラムを実行するかどうかの**警告画面**（図a）を表示します。そのようなときは、**先には進まず、[キャンセル]をクリック**してください。

図aの警告画面の説明
警告画面には、ファイルの「名前」、ファイルの「種類」、ファイルの「発信元」欄があります。図の例では、「種類」が「アプリケーション」となっていますが、これはプログラムであることを意味します。画像などをダウンロードしようとしたときにプログラムであるのは、問題があることを意味します。「種類」や「発信元」などの欄を確認し、**自分が要求したものと異なるときは、[キャンセル]**をクリックしてください。

Windows Vista の例　　Windows XP の例

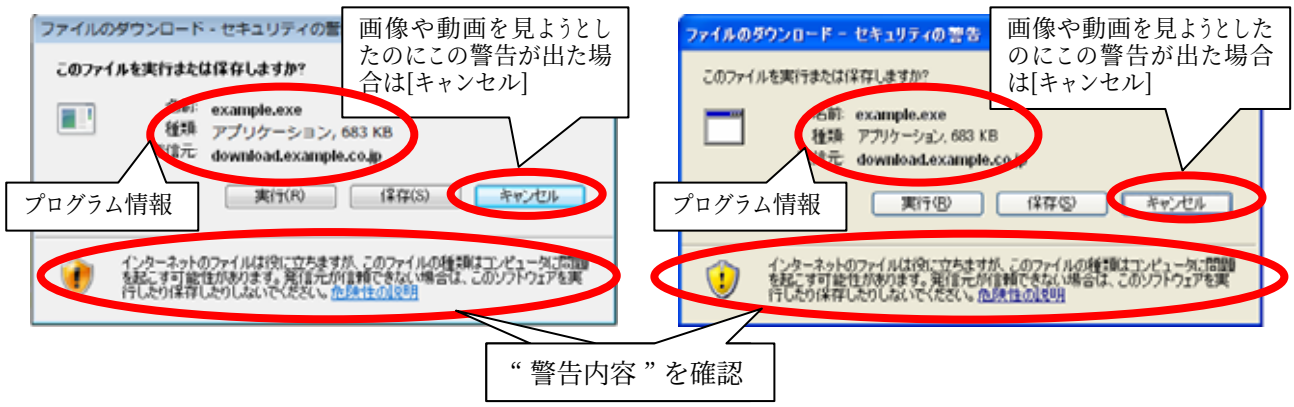
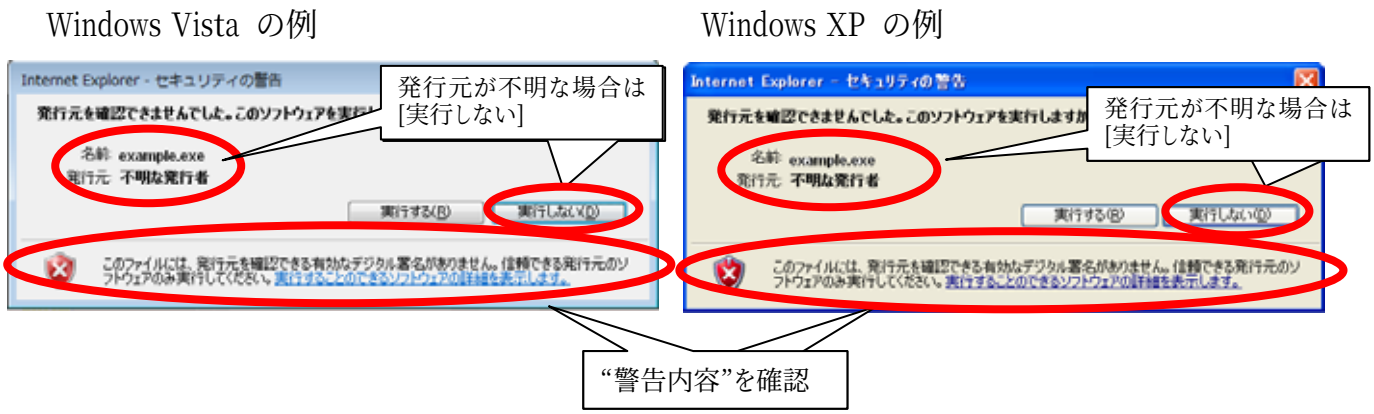


図 a：Windows Vista/Windows XP でのファイルのダウンロードの警告画面

図aの警告画面で**[実行]**をクリックすると、ユーザのパソコンにプログラムがダウンロードされて、そのプログラムを実行するかどうかの警告画面(図b)が表示されます。

Windows では、プログラムの発行元が正統なものであるかどうかを証明する仕組みを活用してい

ます。この警告画面で、「発行元」の欄をみれば、証明された発行元であれば、その発行元の名称が表示されます。図bの例では、**発行元が不明**とされており、この発行元を信頼することはできません。したがって、**先に進まないようにしてください（[実行しない]をクリック）。**



図b：Windows Vista/Windows XP での Internet Explorer の警告画面

Windows Vista では、ユーザの意図しない操作、または許可するつもりのない操作を実行しようとするプログラムの起動を防ぐため、ワープロやドライバソフト等のプログラムをインストールする場合やシステムの設定変更を行う場合に、新しい機能である「ユーザアカウント(*1)制御」(UAC：User Account Control)という機能により図 c のような画面が表示されます。

万が一、図bの警告画面で **[実行する]** をクリックした場合であっても、UAC 機能の画面が表示されますので、再度、「発行元」及び警告内容を確認してください。

例として、図cの場合は、発行元欄が「認識できない発行元」と表示されていますので、**実行しないようにしてください（[キャンセル] をクリック）。**

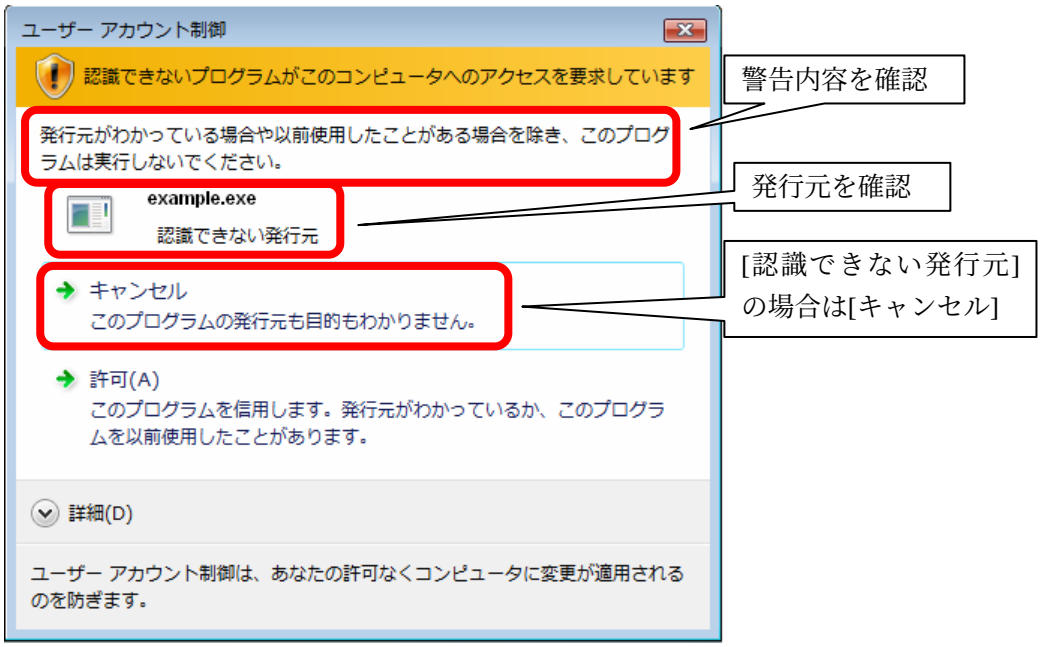


図 c：UAC の警告メッセージ例

このように、Windows Vista ではユーザが不正なプログラムを誤って実行しようとした場合でも、UAC 機能により警告画面が表示されて警告を促すことにより、ウイルスやスパイウェアなど悪意あるソフトが不用意にインストールされることを未然に防いでいます。

UAC 機能は、**初期状態では有効になっていますので、無効にしてはいけません。**

（ご参考）
Windows Vista デベロッパー センター > セキュリティ
http://www.microsoft.com/japan/msdn/windowsvista/security/

IPA - クリックしただけで料金請求された場合の対応方法について
http://www.ipa.go.jp/security/ciadr/oneclick.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

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、6 頁の「2.コンピュータ不正アクセス届出状況」を参照)
・cgi の脆弱性
・フィッシングの被害

2.相談の主な事例 (相談受付状況及び相談事例の詳細は、9 頁の「3.相談受付状況」を参照)
・安全なアダルトサイトを探していたのに
・偽造ソフトの被害？！

3.インターネット定点観測(詳細は、別紙 3 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、詳細な解説を行っています。
・リモートアクセスサーバーの管理体制に注意！

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 66 万個**と、2 月の 69 万個から 4.6%の減少となりました。
また、3 月の届出件数(※2)は、**2,933 件**となり、2 月の 3,098 件から 5.3%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。
・3 月は、寄せられたウイルス検出数約 66 万個を集約した結果、2,933 件の届出件数となっています。

検出数の1位は、**W32/Netsky** で**約 52 万個 、2 位は VBS/Solow** で**約 4 万個、3 位は W32/Sality** で**約 3 万個でした。**

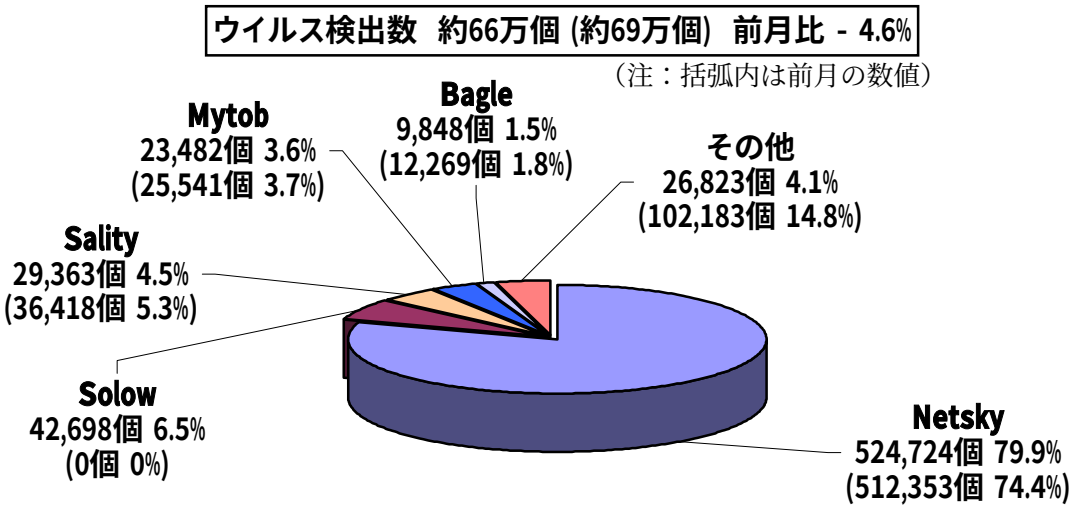


図:1-1

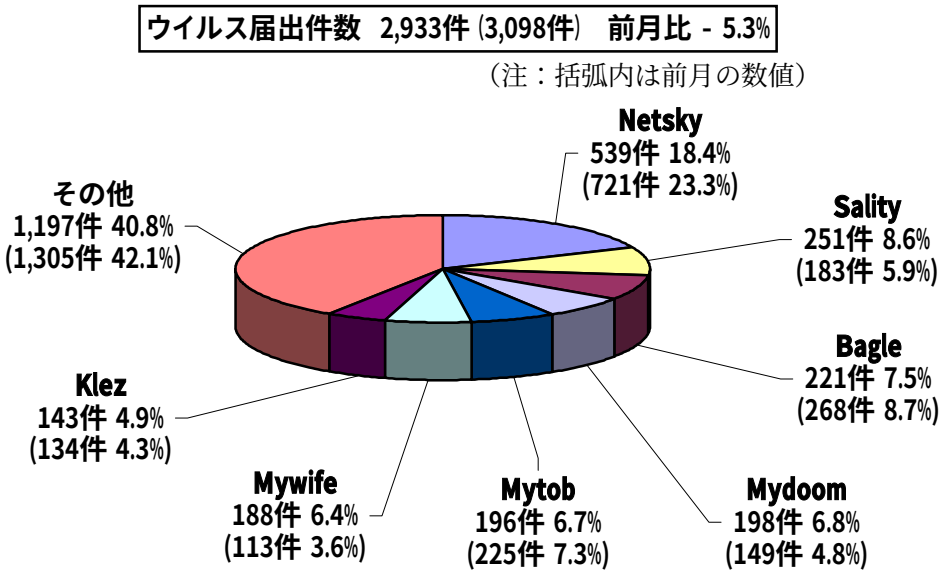


図:1-2

2．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

		10月	11月	12月	1月	2月	3月
届出(a) 計		**22**	**24**	**10**	**32**	**23**	**13**
	被害あり(b)	15	8	9	22	14	9
	被害なし(c)	7	16	1	10	9	4
相談(d) 計		**53**	**30**	**40**	**52**	**50**	**43**
	被害あり(e)	37	20	23	25	28	20
	被害なし(f)	16	10	17	27	22	23
合計(a+d)		**75**	**54**	**50**	**84**	**73**	**56**
	被害あり(b+e)	52	28	32	47	42	29
	被害なし(c+f)	23	26	18	37	31	27

（1）不正アクセス届出状況

3 月の届出件数は 13 件であり、そのうち**被害のあった件数は 9 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 43 件（うち 4 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 20 件でした。

（3）被害状況

被害届出の内訳は、**侵入 2 件、DoS 攻撃 1 件、アドレス詐称 2 件、その他（被害あり）4 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 1 件、サーバ内のデータが破壊されていたものが 1 件でした。侵入の原因は、SSH(*2)で使用するポート(*3)へのパスワードクラッキング攻撃(*4)を受けてパスワードが破られたことと、cgi(*5)の脆弱性を突かれたことでした。

被害事例

[侵入]

(i) cgi(*5)の脆弱性を突かれての侵入でデータが破壊された

事例	・データベースを運用しているウェブサーバが、突然停止した。 ・調査したところ、データベースファイルが破壊されたためと判明。 ・ウェブサーバで動作していた cgi プログラムの脆弱性を突かれて OS コマンドインジェクション攻撃を受けサーバに侵入され、不正なプログラムを起動されたことが原因であった。
解説・対策	最近の**攻撃はツールによって自動化され、無差別に大量に行われる**という特徴があります。**日頃から注意してログ(*6)監視していないと気付きにくい**のが現実です。データベースを運用しているサーバが侵入されると情報漏えいにつながることが多く、その対応費用は膨大なものになるため、注意が必要です。 対策として**最も重要なのは、アプリケーション開発段階からセキュリティを意識し、脆弱性を排除すること**です。アプリケーション完成前に十分なペネトレーションテスト(*7)を実施しましょう。 アプリケーション運用に際しては IDS(*8)/IPS(*9)を導入することで、外部からの攻撃に対して、より早く適切な対処ができます。 (参考) IPA - 情報セキュリティ白書 2007 年版 http://www.ipa.go.jp/security/vuln/20070309_ISwhitepaper.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

[フィッシング]

(ii) フィッシング(*10)の被害に遭った？

事例	・オークションサイトである商品に入札しようとしたが、自分のアカウント(*11)が利用停止状態になっていることに気付いた。理由は、「違法な商品を出品していたため」となっていたが、自分には身に覚えが無い。 ・思えば 2 週間前に、オークションサイトのアカウントの使用継続確認のメールが届いており、メールから導かれたサイト上で ID・パスワード・クレジットカード番号を入力してしまっていた。そのメールを再度確認してみたら、差出人は明らかにオークションサイトのものではなかった。
解説・対策	オークションサイトからのメールであると見せ掛けたニセのメールに騙されてフィッシングサイトに誘導され、個人情報を盗まれてしまった可能性が高いです。一刻も早くクレジットカード会社に連絡し、カード番号を変更する必要があります。 通常、**メールで誘導したサイトでクレジットカード番号を入力させるようなことはありません**。被害に遭わないために、**メール本文中にあるリンクは安易にクリックしないことが肝要**です。さらに念のため、こまめにサイトにアクセスし、不正に利用されていないかチェックするなどの自衛策も必要です。 (ご参考) フィッシング対策協議会 http://www.antiphishing.jp/

3．相談受付状況

3 月の相談総件数は **1127 件**となり、今までの最高を記録しました。そのうち**『ワンクリック不正請求』に関する相談**が **316 件**（2 月：287 件）とさらに最悪の記録を更新し、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 **23 件**（2 月：22 件）、**Winny に関連する相談**が **5 件**（2 月：14 件）などでした。

IPA で受け付けた全ての相談件数の推移

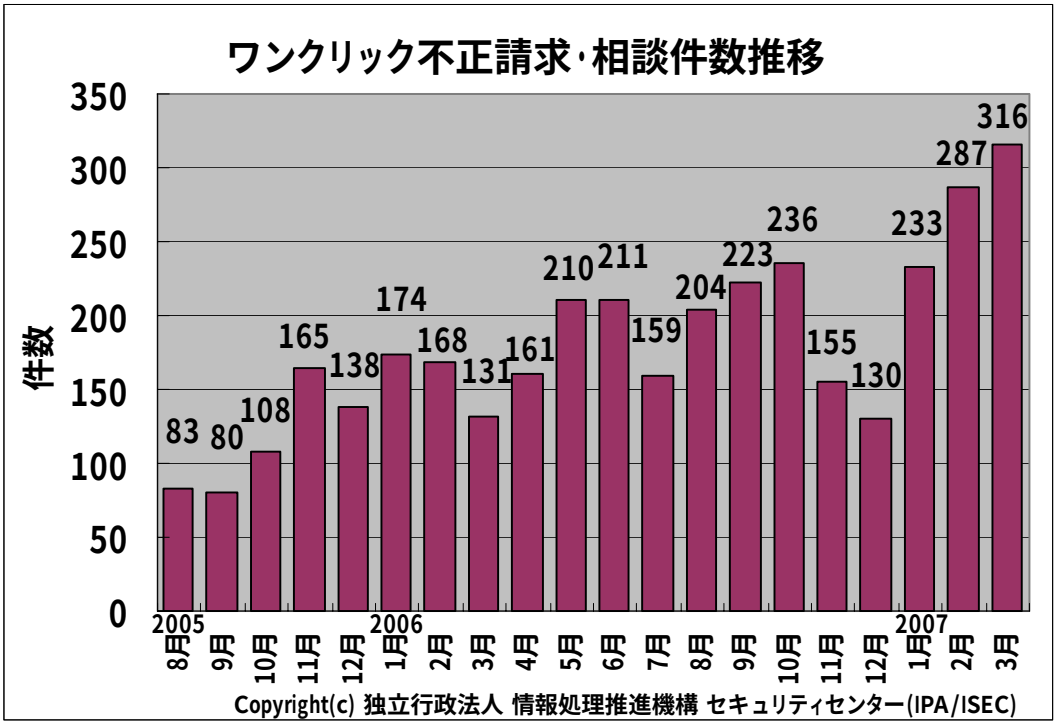
	10月	11月	12月	1月	2月	3月
合計	**1002**	**711**	**680**	**946**	**1019**	**1127**
自動応答システム	580	423	394	582	603	697
電話	326	214	222	324	336	376
電子メール	93	72	59	39	75	54
その他	3	2	5	1	5	0

※ 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

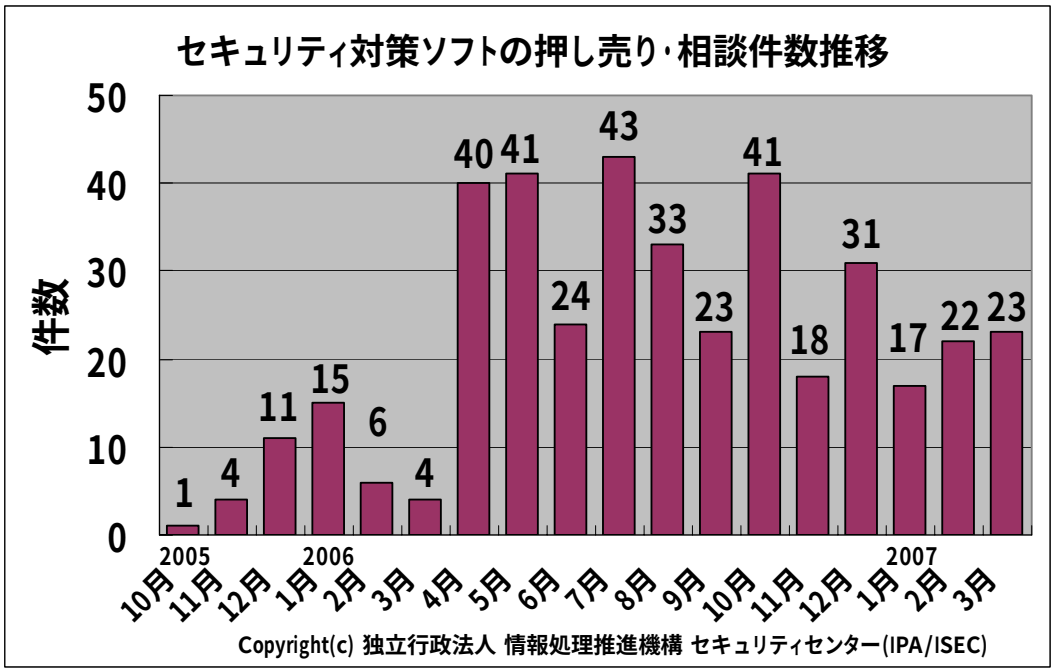


ワンクリック不正請求についての対策については下記をご参照ください。

・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) 安全なアダルトサイトを検索していたのに・・・

相談	最近はアダルトサイトでの詐欺が多いと聞いていたので、安全なサイトを探そうと思った。大手ポータルサイトからの**検索で、キーワードを「エロサイト」「だまされない」としてヒットしたサイトにアクセス**した。動画ファイルと思われるリンクをクリックしたら、年齢確認画面が出たがよく確認せずに[OK]をクリック。その結果、**「ご登録ありがとうございます」という料金請求画面が表示された**。  図 3-1:ポータルサイトにおける検索の様子
回答	自分の意図とは裏腹に、簡単にワンクリック不正請求のワナに掛かっています。不正請求を行っている業者は、ユーザが検索しがちなキーワード(今回の場合、「エロサイト」や「だまされない」)でヒットするように不正請求サイトを構築しているようです。**検索でヒットしたサイトは、安全なものばかりではないことを十分認識し、注意してアクセスしなければなりません**。 (ご参考) IPA - 2006/12 月の呼びかけ「ネット上の誘惑に負けるな!!」 http://www.ipa.go.jp/security/txt/2006/12outline.html#5 IPA - 2006/8 月の呼びかけ「おかしいと思ったらすぐ引き返そう!!」 http://www.ipa.go.jp/security/txt/2006/08outline.html#5

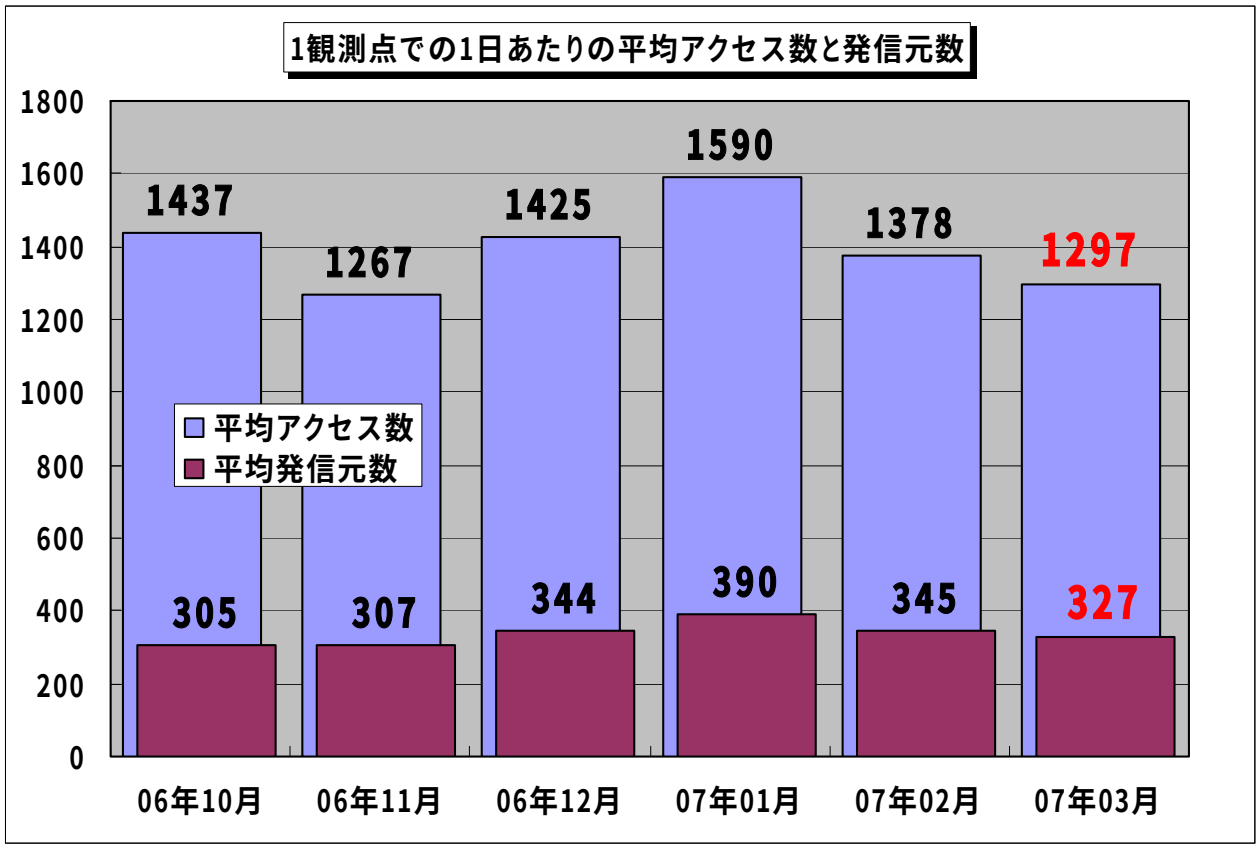
(ii) 偽造ソフトの被害?!

相談	ある日を境として、パソコン画面の右下に「お客様は偽造ソフトウェアの被害に遭われた可能性があります」と表示されるようになった。ウイルスに感染したのか。パソコンは自作のもので、知人から譲り受けたもの。  図 3-2:警告画面
回答	マイクロソフト社が 2007 年 2 月から提供している、ソフトウェア違法コピー対策用プログラム(Windows Genuine Advantage Notifications)が発しているメッセージです(2007 年 1 月発売の Windows Vista には、最初から組み込まれています)。その**パソコンにインストールされている Windows は正規のものではなく、違法コピー品や海賊版である可能性がある**ということです。パソコンの入手元に問い合わせましょう。もし正規品でなかった場合は、正規のライセンスを購入する必要があります。 (ご参考) マイクロソフト – Windows Genuine Advantage Notifications の概要 http://www.microsoft.com/genuine/AboutNotifications.aspx

4．インターネット定点観測での３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 3 月の期待しない（一方的な）アクセスの総数は、10 観測点で **402,140 件**ありました。1 観測点で 1 日あたり **327** の発信元から **1,297 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、327 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 4.1　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 10 月～2007 年 3 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 4.1 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 2 月に比べて多少の減少傾向で、ほぼ 2006 年 11 月の状況に戻りました。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ます。

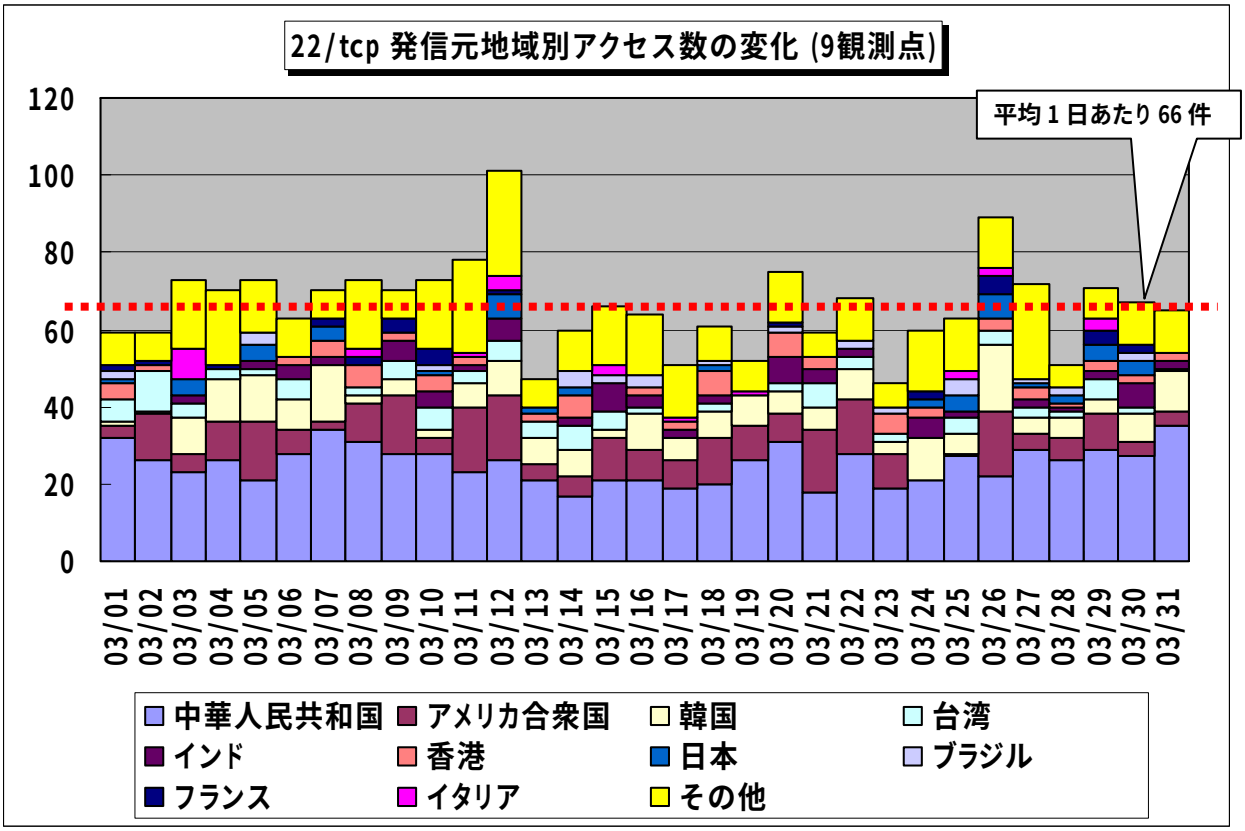
2007 年 3 月のアクセス状況は、全体的には 2007 年 2 月とほぼ同じ状況です。ただし、リモートアクセスで操作されるパソコンの脆弱性を突いて攻撃するアクセスは、インシデント(*11)事例の報道もあり、さらなる注意が必要です。

22/tcp へのアクセスは、SSH (Secure Shell) Server を探し出し、脆弱なパスワード認証を破ることを目的としたアクセスであると考えられます。このアクセスに応答するコンピュータに対しては、パスワードを破るためにブルートフォース攻撃や辞書攻撃(*4)を仕掛けます。このことにより、脆弱な（安易な）パスワード設定の場合は、破られる可能性が高くなります。

SSH (Secure Shell) を使用している企業では、サーバ等の管理体制とセキュリティポリシーの見直し、監視体制の強化をお願いします。

<参考情報>

■ 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



【図 4.2 22/tcp 発信元地域別アクセス数の変化(9 観測点)】

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/TALOT2-0704.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) **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。

(*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) **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。

(*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。

(*7) **ペネトレーションテスト** (Penetration Test)
システムを実際に攻撃することで、脆弱性が無いか確認するテスト手法のこと。

(*8) **IDS** (Intrusion Detection System)
システムに対する侵入／侵害を検出・通知するシステムのこと。システムを監視し、セキュリティポリシーを侵害するような行為を検出した場合に、その行為を可能な限り早く管理者に伝えるとともに、調査分析の作業を支援するために必要な情報を保存・提供することが目的である。

(*9) **IPS** (Intrusion Prevention System)
システムに対する侵入／侵害を阻止するシステムのこと。異常を検知した際に自動的に通信を停止する機能を有したものであり、一般的には IDS の発展形と言える。

(*10) **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。

(*11) **インシデント** (incident)
情報セキュリティ分野において、情報セキュリティリスクが発現・現実化した事象のこと。

■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。