IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2006 年 8 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［2006 年 7 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、2006 年 7 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：
「おかしいと思ったらすぐ引き返そう！！」
― 怪しいサイトに近づかない、怪しいと思ったら先に進まないように ―

2006 年 7 月も、依然としてワンクリック不正請求や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多数寄せられています。

相談件数の推移（2006 年 4 月～7 月）

	4 月	5 月	6 月	7 月
ワンクリック不正請求	161 件	210 件	211 件	159 件
セキュリティ対策ソフトの押し売り行為	40 件	41 件	24 件	43 件
相談総件数	904 件	846 件	773 件	767 件

これらでは、

- ◆ 主にアダルトサイトで、画像や動画が無料で閲覧できますといった文句で惑わせて、悪意あるプログラムをダウンロードさせて、パソコンに請求書を表示させる。（次頁参照）
- ◆ バナー広告(*1)に「ウイルスに感染している」といった表示（次頁参照）をして、セキュリティ対策ソフトの購入を迫る。（P9：相談事例参照）

など、利用者を騙すための巧妙な手口が使われています。

また、相談事例をみると、このような問題のあるサイトへアクセスさせるため、以下のような方法で利用者を導くことが確認されています。

問題のある怪しいサイトへ導く方法（相談事例より）

- ● スパム(*2)メールによる手口
  広告メールなど、迷惑メールの本文に記載されているリンクをクリックして、怪しいサイトへ飛ばされるケース。

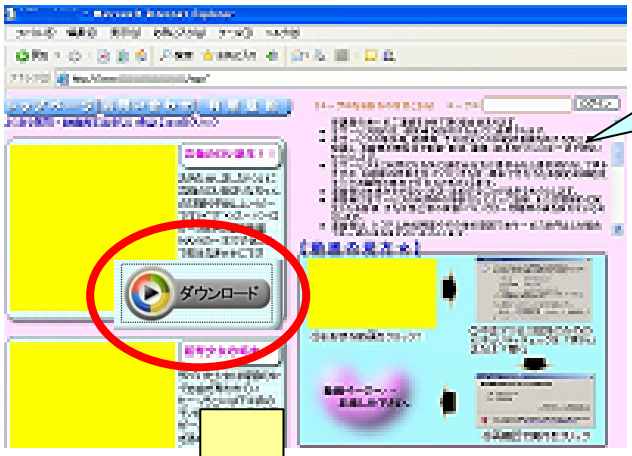
- ● ブログのトラックバック(*3)による手口
  ブログにトラックバックにより掲載されているリンクが、ブログの記事と関係ないもので、クリックして怪しいサイトへ飛ばされるケース。

上記いずれも、記載されているリンクをクリックしなければ被害に遭うことはありませんので、安易にクリックしないようにすることが肝要です。うっかりクリックして、意図しない妙なサイトにアクセスしてしまった場合には、すぐに**引き返す**（ページを閉じる）ことが有効な対策となります。

(*1) Web サイトに貼り付けられている広告画像のこと。クリックすることで、広告主の Web サイトにジャンプするようになっている。
(*2) 迷惑メールとも呼ばれる。宣伝や嫌がらせなどの目的で不特定多数に大量に送信されるメールのこと。
(*3) ブログの機能の一つ。自身のサイト内に、他のブログを参照しリンクを張って記事を書いた場合に、リンク先のサイトに対し「リンクを張った」ことを自動的に通知する仕組みのこと。

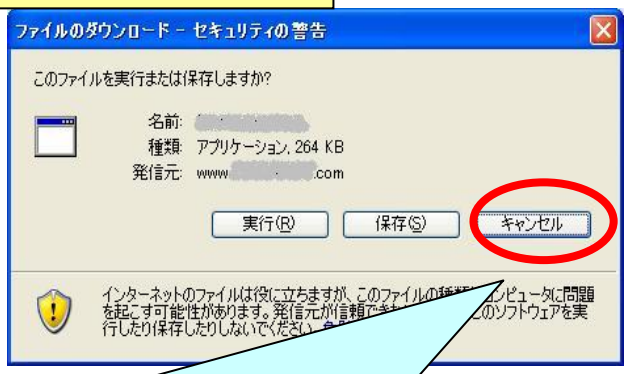
自ら意識してアクセスしているページであっても、怪しげなサイトでは、画像を表示するように見せかけて、悪意あるプログラムをダウンロードさせるような仕組みが設けられていることもありますので、ご注意ください。

【悪意あるプログラムをダウンロードさせるケース】



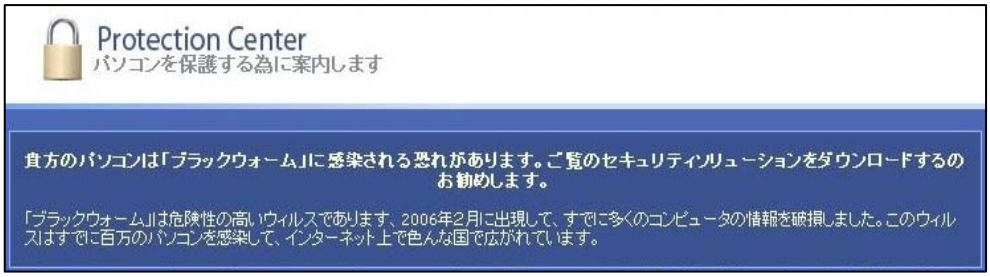
無料の動画や画像だと思って「ダウンロード」ボタンをクリックすると、「セキュリティの警告」画面が表示されます。これは、Windows の機能によって表示され、それ以上進むとセキュリティ上の問題が生じる可能性を示しています。

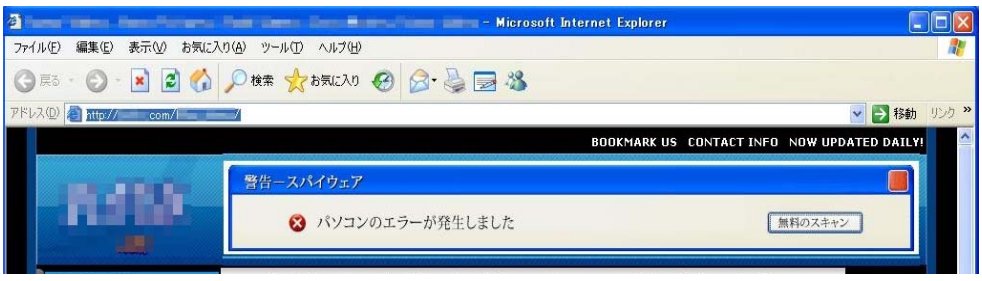
セキュリティの警告画面



「セキュリティの警告」画面で、「実行」をクリックして進むと、悪意あるプログラムをインストールすることになってしまいます。
この警告画面は、非常に危険である旨を表していますので、引き返す（キャンセルをクリックする）ようにして、悪意あるプログラムの侵入を防ぐようにしましょう。

【セキュリティ対策ソフトの押し売り行為のケース】





バナー広告に、“ウイルスに感染している”、”パソコンのエラーが発生した”等のメッセージを表示して、ユーザの不安を誘います。文法がおかしな日本語表示もあるので、注意深く読めば見分けられます。

このような広告が表示されたら、引き返す（ページを閉じる）ようにしましょう。

ワンクリック不正請求やセキュリティ対策ソフトの押し売り行為は、金銭を詐取することを目的としています。利用者を騙すために、利用者の心理を逆手に取った、巧妙な手口が使われています。そのため、正規のセキュリティ対策ソフトの導入やセキュリティホールを解消するといった技術的対策だけでは対処できないことがあります。

技術的対策に加え、**怪しいサイトに近づかない、安易にプログラムをダウンロード・実行しない**など、普段からの心構えが重要になります。

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 154 万個**と、6 月の 164 万個から 5.9%の減少となりました。
また、7 月の届出件数(※2)は、**3,455 件**となり、6 月の 3,547 件から 2.6%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。
・7 月は、寄せられたウイルス検出数約 154 万個を集約した結果、3,455 件の届出件数となっています。

検出数の1位は、**W32/Netsky で約 124 万個 、2 位は W32/Mytob で約 11 万個、3 位は W32/Bagle で約 9 万個でした。**

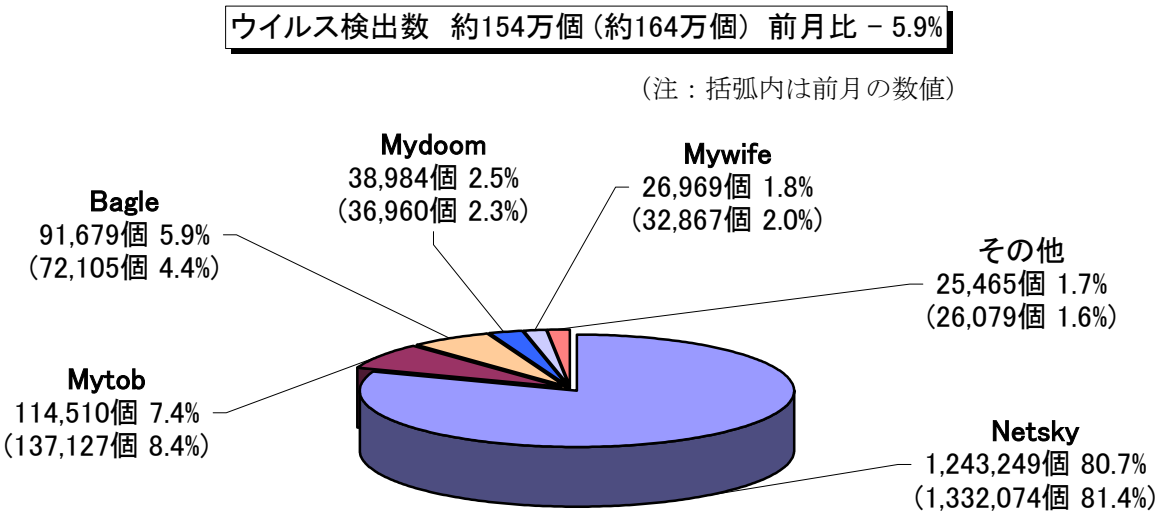


図:1-1

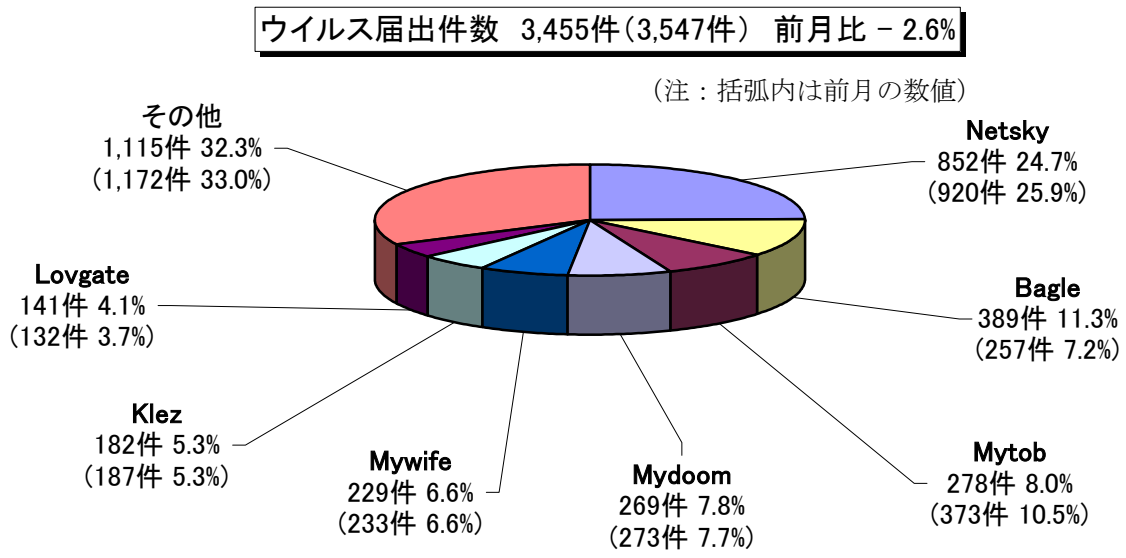


図:1-2

2. 依然として相談の多いスパイウェアによる被害

多くの相談が寄せられている**「ワンクリック不正請求」**などは、スパイウェア(*4)による被害の一例です。スパイウェアはその種類毎に、予め収集する情報(メールアドレス、クレジットカード番号等)などがプログラムされています。スパイウェアに感染すると、これらの情報が気付かないうちに盗まれ、以下のような被害が起こってしまいます。

【事例】
- **メールで不正な請求書が送られてくる。**(無料の画像などと思ってダウンロードしたときに、スパイウェアが埋め込まれ、メールアドレスを盗まれた。)
- **なりすましにより、銀行の預金が不正に引き出される。**(スパイウェアが埋め込まれ、オンラインバンキングの ID とパスワードが盗まれた。)

これらの被害に遭わないよう、以下に掲げる対策を実施すると共に、P2 の例を参考に、安易にダウンロードしない(引き返す)等の注意を払うようにしましょう。

(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(Windows Update の利用など)
(3) 怪しいサイトや不審なメールに注意する
(4) コンピュータのセキュリティを強化する(Windows XP のファイアウォール機能を有効にする、ブラウザのセキュリティレベルを高くするなど)
(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

以上の対策は、自ら管理できるコンピュータに対して実施するものになります。自分で管理できないコンピュータ(例えば、インターネットカフェやオープンな場所での共用のコンピュータなど)では、上記のような管理がなされているかどうかなど不明ですので、個人情報などの重要な情報の入力は行わないようにしましょう。

(参考)
スパイウェア対策のしおり
http://www.ipa.go.jp/security/antivirus/shiori.html

なお、「スパイウェアに侵入されているかもしれない」と心配な場合、以下のサイトで無料のオンラインスキャンを利用できますので、まずは検査してみてください。

【オンラインスキャンを利用できるサイト】

◆シマンテック セキュリティチェック
http://www.symantec.com/region/jp/securitycheck/
◆トレンドマイクロ オンラインスキャン
http://www.trendmicro.co.jp/hcall/
◆マカフィー フリースキャン
http://www.mcafee.com/japan/mcafee/home/freescan.asp
◆スパイウェアガイド - オンライン スパイウェア検出
http://www.shareedge.com/spywareguide/txt_onlinescan.php

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

		2月	3月	4月	5月	6月	7月
届出(a) 計		26	38	15	13	22	15
	被害あり(b)	15	10	7	6	20	8
	被害なし(c)	11	28	8	7	2	7
相談(d) 計		42	24	27	23	32	31
	被害あり(e)	24	12	15	11	19	18
	被害なし(f)	18	12	12	12	13	13
合計(a+d)		68	62	42	36	54	46
	被害あり(b+e)	39	22	22	17	39	26
	被害なし(c+f)	29	40	20	19	15	20

(1) 不正アクセス届出状況

7 月の届出件数は 15 件であり、そのうち**被害のあった件数は 8 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 31 件（うち 5 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 5 件、DoS 攻撃(*5) 2 件、アドレス詐称 1 件**でした。
侵入届出の内訳は、Web ページの改ざんが 1 件、サーバ内データの奪取や破壊が 2 件、などでした。

被害事例

［侵入］

（i）ホームページの改ざん

事例	・一般公開しているホームページが改ざんされているのを、自身で発見。 ・OS のぜい弱性を放置していたのが原因で、侵入されたものと思われた。 ・ハードディスク容量が不足していたために、ぜい弱性の**修正プログラム適用を怠っていた**。
解説・対策	この事例では、**ぜい弱性の存在は分かっていたのに、その緊急性を理解していなかった**ために対応が遅れ、結果として被害を受けてしまっています。情報セキュリティ上の**脅威や、想定される被害を正しく理解した上で、対策を適切かつタイムリーに実施していくことが非常に重要**です。今回のケースでは、別途ハードディスクを増設するか、現在よりも大容量のハードディスクに換装した上で、修正プログラムを適用するという対策が必要です。 （参考） IPA － 脆弱性対策のチェックポイント http://www.ipa.go.jp/security/vuln/20050623_websecurity.html IPA － 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/20060131_websecurity.html

（ii） 無線 LAN ルータ(*6)への侵入

事例	・無線 LAN ルータ(*6)の設定画面にログインしようとしたところ、既に何者かがログインしていることが判明。 ・ログインしているユーザの IP アドレスは、組織外のものであった。 ・ルータの**管理用パスワードが設定されていなかった**のが原因。まさか外部からアクセスされ、ログインされるとは思ってもいなかった。
解説・対策	この事例では、どこからルータの設定画面にログインされたのかを明確にする必要があります。もし外部から管理画面にログイン可能なようになっていたとしたら、その是非を見直す必要があります。**外部からのログインを許可していなかったとしたら、何らかの原因で以前より内部ネットワークに侵入されており、内部からログインされたということも考えられます**。ルータの設定を再確認するとともに、内部ネットワークに接続されているマシンが**ウイルスに感染して外部からの侵入の踏み台になっていないか、確認**しましょう。 もし**ルータの組み込みソフトウェアにぜい弱性が存在する場合は、ルータの設定とは全く無関係に、外部から直接侵入を許してしまいかねません**。当該組み込みソフトウェアが最新のものであるかどうか、確認しましょう。 **ルータの管理用パスワード設定は、企業ユーザや一般家庭ユーザの区別無く**、外部からの不正ログインを防ぐためのみならず、管理者以外が勝手に設定を変更できないようにするために**必須のもの**です。**購入したら、何よりも先に設定すべき**でしょう。 （参考） IPA － 今月の呼びかけ： 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 － 情報セキュリティ白書 2006 年版 http://www.ipa.go.jp/security/vuln/20060322_ISwhitepaper.html

[DoS 攻撃(*5)]

（iii） Web サーバへの攻撃

事例	・自身が運用する Web サーバに対し約 2 時間、Web ページ再読み込みのリクエストを連続的に受けた。 ・Web サーバはリクエストを処理し切れず、応答が無い状態に陥った。 ・対策として、**リクエストが集中していたページを一時的に閉鎖**するとともに、**アクセス元の IP アドレスをフィルタリング**した。
解説・対策	この事例では、まずは不正アクセスの原因を排除し、さらに根本的対策を取ることで、被害を最小限に食い止めることができました。**原因を的確に把握し、適切な対処をタイムリーに実施することができた、良い例**です。 （参考） IPA － コンピュータ不正アクセス被害防止対策集 http://www.ipa.go.jp/security/ciadr/cm01.html#DoS

4. 相談受付状況

7 月の相談総件数は **767 件**でした。内訳は、**『ワンクリック不正請求』に関する相談**が **159 件**(6 月 :211 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 **43 件**(6 月 :24 件)、**Winny に関連する相談**が **12 件**(3 月 :196 件、4 月 :83 件、5 月 :28 件、6 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

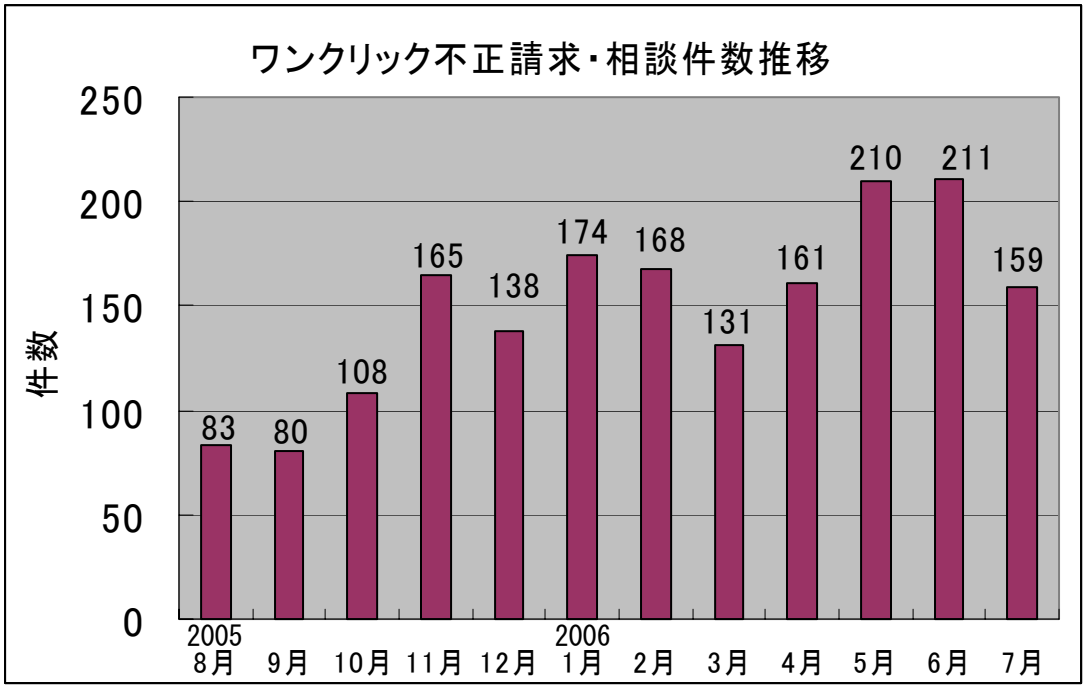
	2月	3月	4月	5月	6月	7月
合計	**834**	**1056**	**904**	**846**	**773**	**767**
自動応答システム	479	659	510	484	423	444
電話	258	296	306	295	283	257
電子メール	90	99	86	63	64	66
その他	7	2	2	4	3	0

※ 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)

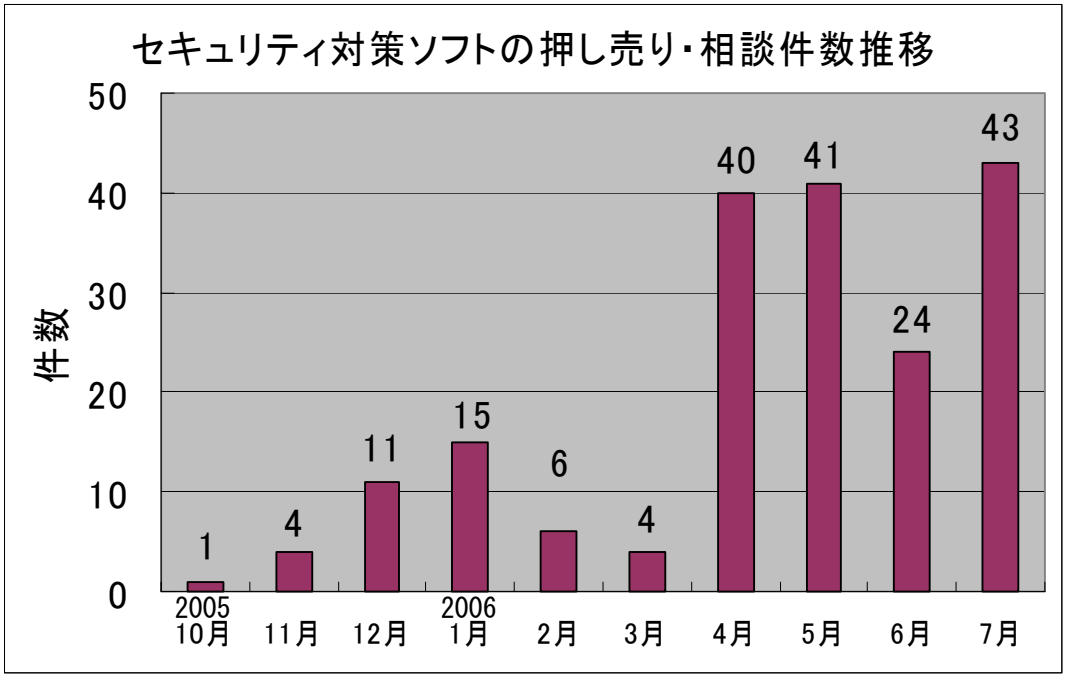
※ 「自動応答システム」 : 電話の自動音声による応対件数
「電話」 : IPA セキュリティセンター員による応対件数

※ 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。

ワンクリック不正請求相談件数の推移



セキュリティ対策ソフトの押し売り・相談件数の推移



主な相談事例は以下の通りです。

（i）以前よく見ていたページを久しぶりに訪問したら警告が！

相談	以前よく見ていて[お気に入り]に入れていたサイト(日本語)にアクセスしたら、以前とは全く違う英語のサイトになっていた。さらに、「あなたのパソコンはウイルスに感染しています」などという警告画面が出て来て、ウイルス対策ソフトの導入を勧められた。これは信頼できるものなのか。
回答	この事例では、何らかの理由により**ホームページが悪意のある者によって乗っ取られていたようです。信頼できるサイトからのリンクでも、このようなことが起こり得ます**ので、ジャンプした先で不用意に[はい]や[OK]などをクリックしないようにしましょう。 ところで、**正規のセキュリティ対策製品の製造・販売者からは、事例にある脅しのようなメッセージを一方的に送りつけることはありません。**慌ててダウンロードすることのないよう注意しましょう。 (ご参考) 今月の呼びかけ：「 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

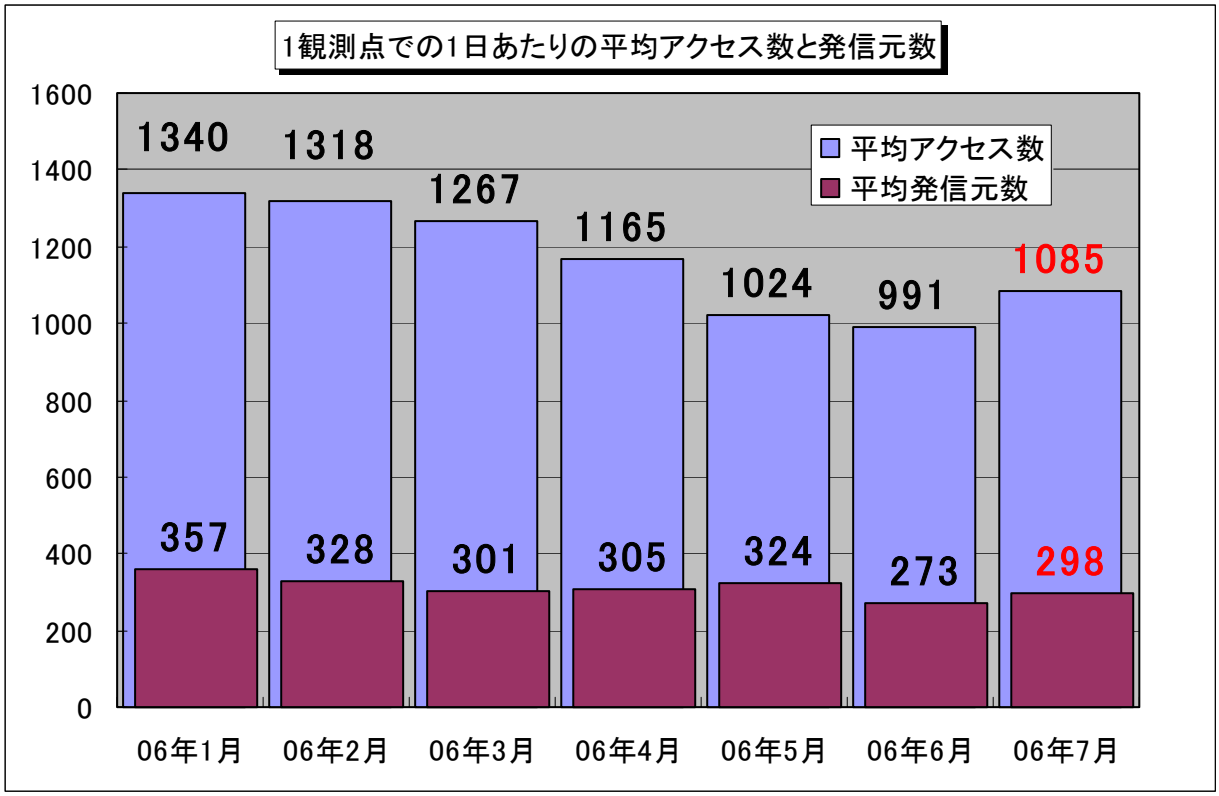
（ii）言われるがままインストールしたらパソコンの調子が悪くなった

相談	「あなたのパソコンはウイルスに感染しています」などという警告画面が出ていたが、しばらく放っておいたら画面が動かなくなった。仕方なく、言われるがままウイルス対策ソフトをダウンロードし購入。それからパソコンが起動できなくなってしまった。
回答	そもそも、**信頼できないソフトを動かしてしまったら、何が起こるか分かりません**。インストールする前に、十分に確認する必要があります。正常に起動できなくなった場合は、Windows XP ならシステムの復元で復旧できる場合もありますが、パソコンを初期化することが望ましいと言えます。

5. インターネット定点観測での 7 月のアクセス状況

インターネット定点観測(TALOT2)によると、2006 年 7 月の期待しない(一方的な)アクセスの総数は、10 観測点で **336,361 件**ありました。1 観測点で 1 日あたり **298** の発信元から **1,085 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、298 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 1 月～2006 年 7 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 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、先月より微増しました。アクセス内容については、定常化していると言えます。

7月のアクセス状況は、6 月とほぼ同じ状況です。Windows のぜい弱性を狙っていると思われる不正なアクセスが多いようで、これらのアクセスの多くは、ボットに感染したコンピュータから送信されていると思われます。また、月末にかけて、これらのアクセス(数)が増加傾向なので、注意が必要です。

特にアクセス数の多い 135(TCP)ポート,445(TCP)ポートへのアクセスは、Windows のぜい弱性を狙っています。また、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1026(UDP)/1027(UDP)ポートへのアクセスは、継続しています。

また、6 月分の詳細資料(別紙 3)で特集を行った、ネットワークからの **22(TCP)ポートを狙ったパスワードクラッキング攻撃**(解説_1)や、リモートアクセスツール **RealVNC のぜい弱性**(解説_2)を狙っていると思われる 5900(TCP)ポートへのアクセスについても、継続的に発生しています。どちらのアクセスも、リモートから攻撃先のコンピュータへ侵入を試みるものであり、このようなツールを利用して、サーバを運用しているシステムの管理者は、運用方法の再点検やぜい弱性の解消を怠らないようにして下さい。

特に、7 月の 22(TCP)ポートを狙ったパスワードクラッキング攻撃は、TALOT2 観測での記録的な数値を示しました。月後半の 3 日間に以下に示すアクセスがあり、ほとんど DoS 攻撃(*5)を受けているような状況でした。

- 発信元がアメリカ方面、10 時間のあいだに **242,511** 回のアクセス→ 6.7 回/秒
- 発信元が韓国方面、4 時間半のあいだに **63,098** 回のアクセス→ 3.9 回/秒
- 発信元がアメリカ方面、1 時間 45 分のあいだに **33,959** 回のアクセス→ 5.4 回/秒

(解説_1) **22(TCP)ポートを狙ったパスワードクラッキング攻撃**

ログイン ID やパスワードを変更させながらログインを繰り返すことで、システムへの侵入を試みる、SSH(Secure Shell:通信路を暗号化することで安全性を高めたリモートからのコマンド実行ツール)を狙った 22(TCP)ポートへのアクセス。

TALOT2では、SSH への攻撃の実情を調べるために、SSH を利用しています。この SSH の利用する 22(TCP)ポートに対するポートスキャンおよび実際のパスワードクラッキング攻撃が、他の不正なアクセスとともに観測することができます。

攻撃者は、開いている(応答のある)22(TCP)ポートを見つけると、ID やパスワードを変更させながら、ログイン操作を繰り返し実行します。

SSH を利用する観測点で観測されたパスワードクラッキング目的のアクセスについては、特定観測点への攻撃であることから、本レポート内の観測データから除外してありますので、ご注意下さい。

(解説_2) **RealVNC のぜい弱性**

遠隔操作ソフトである RealVNC Server には、クライアント認証の回避が可能な脆弱性が存在します。以下のサイトを参照下さい。

■ JVNVU#117929 RealVNC Server に認証回避が可能な脆弱性
http://jvn.jp/cert/JVNVU%23117929/index.html

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/TALOT2-0608.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) **バナー広告**（banner advertisement）
Web サイトに貼り付けられている広告画像のこと。クリックすることで、広告主の Web サイトにジャンプするようになっている。

(*2) **スパム**（spam）
ジャンクメール、バルクメール、また単に「迷惑メール」とも呼ばれる。商用目的かどうかによらず、宣伝や嫌がらせなどの目的で不特定多数に大量に送信されるメールのこと。

(*3) **トラックバック**（track back）
ブログの機能の一つ。自身のサイト内に、他のブログを参照しリンクを張って記事を書いた場合に、リンク先のサイトに対し「リンクを張った」ことを自動的に通知する仕組みのこと。

(*4) **スパイウェア**（spyware）
利用者や管理者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラム等のこと。

(*5) **DoS 攻撃**（Denial of Services attack）
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。

(*6) **ルータ**（router）
異なるネットワークを接続したり中継したりする通信機器のこと。

■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 Web 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）
https://isec.ipa.go.jp/benchmark-new/

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。

お知らせ

「情報セキュリティ標語 2006」の入選作品

コンピュータウイルスの感染やコンピュータへの不正な侵入、 ワンクリック詐欺などの被害に遭わないよう、 特に若年層の「情報セキュリティ対策」の意識を高めるために、本年 3 月より全国の小学生・中学生・高校生から募集していたもので、全国 118 の小・中・高等学校の中から 1, 101 件の応募があり、以下の 10 作品が入選しました。

区分	作品	学校 / 受賞者氏名
大賞	ネットで繋がる無限の世界　明暗決めるはあなたの手	神奈川・慶應義塾湘南藤沢高等部 / 清水　優香子（しみずゆかこ）
高校生の部		
金賞	人々の　意識で変わる　セキュリティ	埼玉県・県立越谷北高等学校 / 浅井　慧（あさいあきら）
銀賞	ケータイは持って天国　落として地獄	岐阜県・県立可児工業高等学校 / 田口　史武（たぐちふみたけ）
銅賞	手軽でも　忘れるなかれ　セキュリティ	埼玉県・立教新座高等学校 / 松下　成昭（まつしたしげあき）
中学生の部		
金賞	ネットワーク　便利と危険は　紙一重	茨城県・つくば市立吾妻中学校 / 藤井のど佳（ふじいのどか）
銀賞	情報は　流れだしたら　止まらない	埼玉県・三郷市立早稲田中学校 / 増田　恵子（ますだあやこ）
銅賞	気をつけよう　インターネットの落とし穴	兵庫県・加古川市立中部中学校 / 遠入　和也（えんにゅうかずや）
小学生の部		
金賞	ぼくだけは　感染しないよ　大間違い	岐阜県・大垣市立墨俣小学校 / 古澤健太郎（ふるさわけんたろう）
銀賞	パスワード　ともだちにだって　ないしょだよ	愛知県・名古屋市立滝ノ水小学校 / 森　明日翔（もりあすか）
銅賞	セキュリティ　あなたが守る　あなたの身	千葉県・千葉市立若松台小学校 / 山崎　緑（やまざきみどり）

これは、韓国の韓国情報保護振興院（KISA）との共同事業の一環として実施したものです。

KISA とは、韓国の情報通信部（日本の総務省に相当）の外郭団体で、韓国国内の情報や情報システムを保護するための政策を実施し、インターネット上での事件・事故への対応をするなど、安全なネットワーク環境を提供するために必要な技術の普及及び研究開発を行う韓国政府出資の機関です。

KISA では、毎年 6 月を情報化月間と定め、6 月第 3 週及び第 4 週をセキュリティ週間として、情報セキュリティを主題とする各種イベントを実施しています。その中に、情報セキュリティ標語・ポスターの公募展があり、2006 年 6 月に実施した公募展の結果、次ページ以降の作品の入選が決定しました。

KISA 情報セキュリティ標語入選作品一覧

大賞(高)「정보보안 생명처럼 정보윤리 가훈처럼」
(情報セキュリティ　生命のように　情報倫理　家訓のように)
장미연（Jang,Mi-Yeon）/ 서울세종고등학교（SeoulSeJong 高等学校）

金賞(小)「건전한 사이버문화 어린이들 눈귀 된다」
(健全なサイバー文化　子供たちの目鼻となる)
윤여은（Yun,Yeo-Eun）/
남원교룡초등학교（NamWonGyoRyong 初等学校）

(中)「클릭! 정보보호, 엔터! 건전문화」
(クリック!　情報セキュリティ、エンター!　健全文化)
김동욱（Kim,DongWook）/ 배재중학교（BaeJae 中学校）

(高)「조심앞에 웃는 정보 방심앞에 우는 재산」
(用心前に笑う情報　油断前に泣く財産)
모윤광（Mo,Yun-Kwang）/ 안산공업고등학교 AnSanGongUp 高等学校）

銀賞(小)「로그아웃 안된 나의 정보 내 재산이 로그아웃 됩니다」
(ログアウト　気の毒な私の情報　私の財産がログアウトになります)
노은지（No,Eun-Ji）/ 송호초등학교（SongHo 初等学校）

(中)「안전하게 다운받고 건전하게 사용하자」
(安全にダウンして　健全に使用するようになる)
김지현（Kim,Ji-Heun）/ 청하중학교（ChungHa 中学校）

(高)「정보유출! 오늘의 무관심 내일의 큰재앙」
(情報流出! 今日の無関心　明日の大災害)
이세미（Lee,Se-Mi）/ 국립국악고등학교（GookRipGookAk 高等学校）

銅賞(小)「컴퓨터속 폭력 세상 어린이가 죽어가요」
(コンピュータの中の暴力　世の中では子供が死んでいきます)
유지은（Yu,Ji-Eun）/ 춘당초등학교（ChoonDang 初等学校）

(中)「정보유출 한순간 정보보호 한평생」（情報流出一瞬　情報保護一生）
박하연（Park,Ha-Yeon/ 울산옥현중학교（WoolSanOkHyun 中学校）

(高)「전자서명 생활화로 전자거래 안전하게」
(電子サイン習慣化で　電子商取引安全に)
심재표（Sim,Jae-Pyo）/ 북평고등학교（BookPyung 高等学校）

MS 賞(小)「몰래 빼낸 남의정보 썩어가는 나의양심」
(密かに抜き取った他人の情報　すぐに認める私の良心)
이연수（Lee,Yeon-Soo）/ 풍천초등학교（PoongChun 初等学校）

(中)「새나가는 개인정보 사라지는 신용」（漏れる個人情報　消える信用）
황민욱（Hwang,Min-Wook）/ 별망중학교（ByulMang 中学校）

(高)「정보 보호의 지름길! 보안 패치의 생활화」
(情報保護の近道！　保安パッチの習慣化)
김상엽（Kim,Sang-Yeop）/ 인덕고등학교（InDuk 高等学校）

IPA 賞（小）「버릴 것은 인터넷 범죄 지킬 것은 사이버 예절」
（捨てることはインターネット犯罪　守ることはサイバーの礼儀）
이두리（Lee,Doo-Ri）/ 금오초등학교（GeumO 初等学校）

（中）「쉽게얻는 남의정보 쉽게잃는 나의정보」
（簡単に貰うのは他人の情報　簡単に失うのは自分の情報）
황지혜（Hwoang, Ji-Heo）/ 상일중학교（SangIl 中学校）

（高）「매주 토요일 바이러스 점검 매일 매일 개인정보 점검」
（毎週土曜日　ウイルス点検　毎日毎日　個人情報点検）
김윤아（Kim, Yun-A）/ 안산공업고등학교（AnSanGongUp 高等学校）