IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2006 年 12 月 4 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 11 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 11 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： 「ネット上の誘惑に負けるな！！」
－ 貴方は様々な仕掛けで狙われている！？ －

最近、バナー(*1)広告をクリックして、広告主のホームページにアクセスし、怪しいセキュリティ対策ソフトをインストールしてしまったとか、オンライン詐欺に遭ってしまったという被害の相談が多数寄せられています。

バナー広告とは？
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。

図 1：バナー広告のサンプル

具体的には、以下のようなバナー広告がホームページに掲載されていて、その内容を安易に信じてしまい、被害にあっているものです。

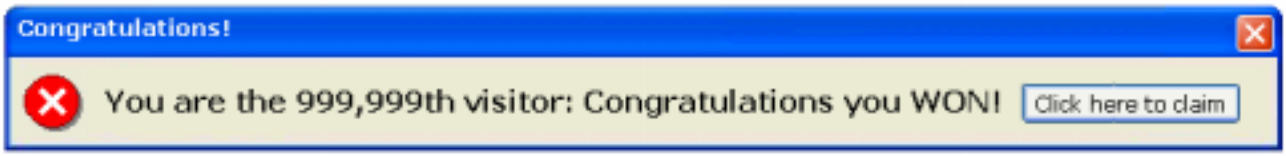


図 2

図 2 は、「あなたは 999,999 人目の訪問者です。おめでとう！」といった内容を表示するもので、クリックすると、住所や名前、メールアドレスを入力する画面になります。ここで入力してしまうと、登録したメールアドレスに当選通知などが届きますが、賞品などが送られてくることはありません。反対に、入力した個人情報などが悪用される危険性があります。

ホームページに掲載されている情報を安易に信用して、個人情報を入力してしまわないよう注意が必要です。（P9：相談事例参照）

図 3

図 3 は、「Drive Cleaner」というセキュリティ対策ソフトを装ったもので、バナー広告に「エラーが検出されました」といった表示をします。このメッセージに驚いてクリック

すると、「当該ソフトウェアをインストール」するように促され、エラーを修復するにはクレジットカード番号を入力して購入するよう求められます。

さらに、バナー広告からアクセスしてしまうケースと同様に、メールに記載されたリンクやブログに掲載されたリンクをクリックすることでも怪しいサイトに導かれてしまうことがあります。少しでも不審な点があれば、その先に進まないようにすることが最善の対策になります。

もしも被害にあってしまった場合は、IPA や最寄りの消費生活センター、クレジットカード会社などに相談してください。

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 158 万個**と、10 月の 117 万個から 34.7%の増加となりました。
また、11 月の届出件数(※2)は、**3,664 件**となり、10 月の 3,696 件から 0.9%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。
・11 月は、寄せられたウイルス検出数約 158 万個を集約した結果、3,664 件の届出件数となっています。

検出数の1位は、**W32/Netsky** で**約 80 万個 、2 位は W32/Looked** で**約 37 万個、3 位は W32/Stration** で**約 24 万個でした。**

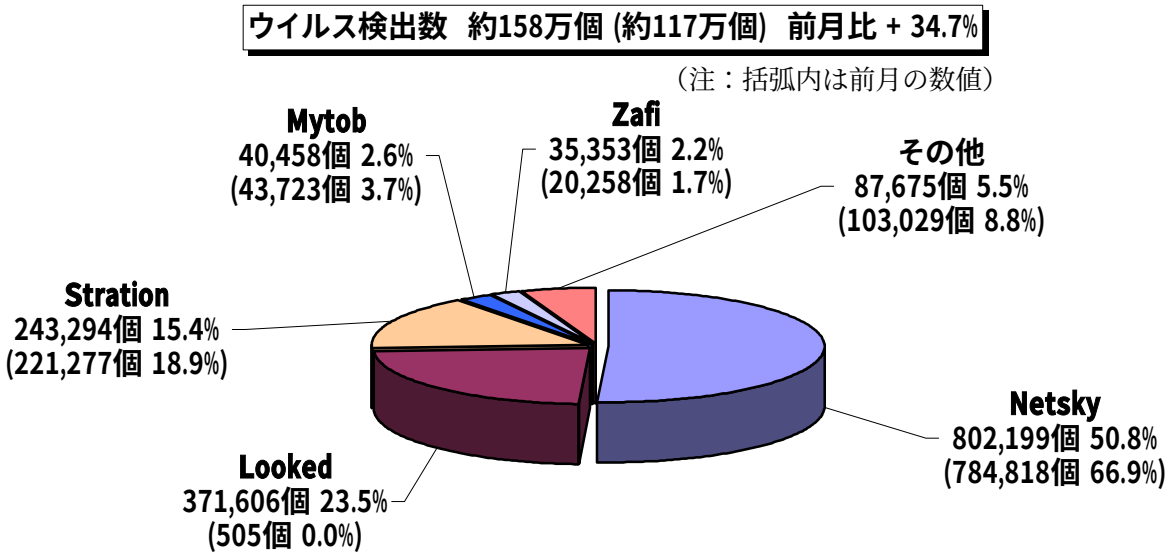
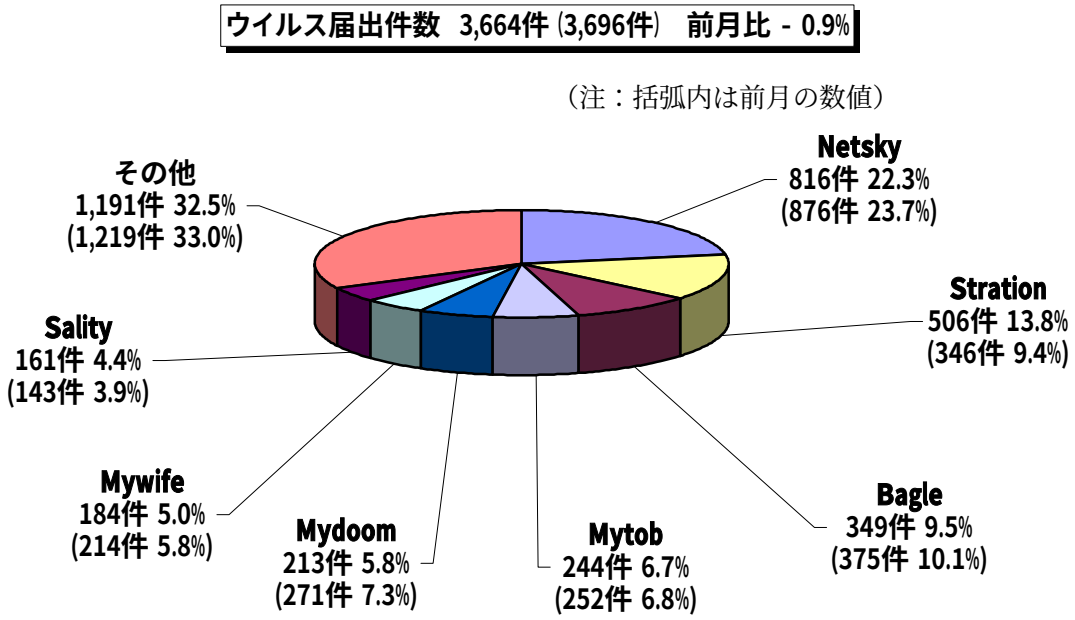


図:1-1



図：1-2

W32/Looked の解説

2006 年 9 月に発生した W32/Looked の亜種（別名 W32/Philis）が、10 月の検知件数 505 個から 11 月には約 37 万個と、急速に感染を広げました。

このウイルスはファイル感染型で、メールの添付ファイルや、ファイル交換ソフトでダウンロードされるファイルに感染しており、それらのファイルを開くとウイルスに感染することになります。
感染すると、当該パソコン内の実行型ファイルにウイルスコードを付加し、インターネットオンラインゲームのパスワードを盗み出す、スパイウェアを生成します。

感染してからでは対処が困難になるなど、被害が拡大する恐れがありますので、メールの添付ファイルを安易に開く、怪しい Web サイトに行かないなど、基本的なことを注意してください。また、ウイルス対策ソフトのパターンファイルを最新の状態に更新して、感染を予防するようにしてください。

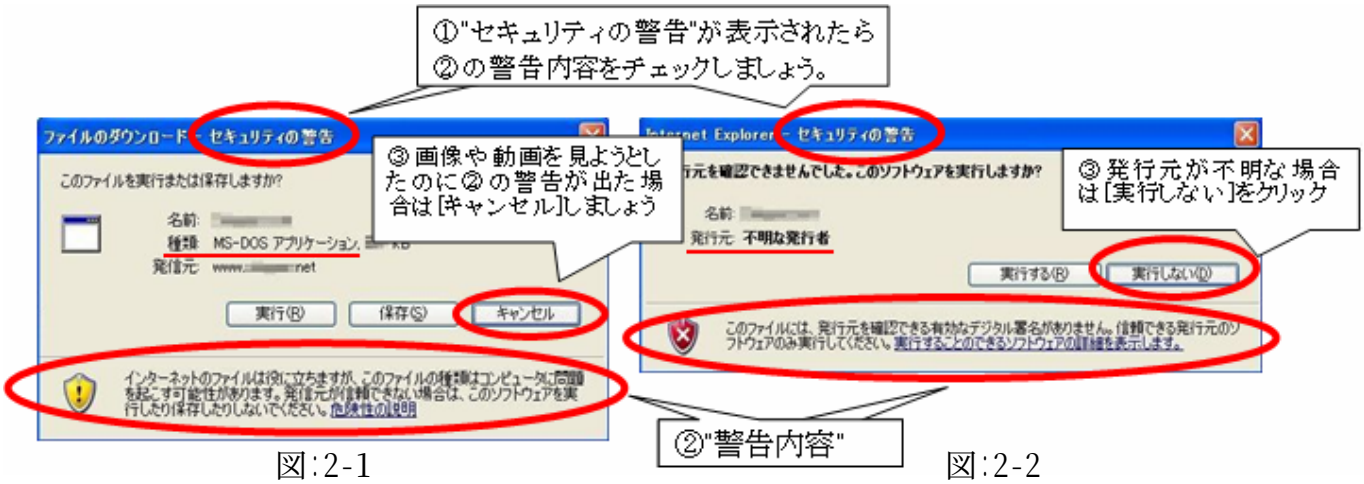
2．依然として多数の相談が寄せられているワンクリック不正請求について

2006 年 11 月も、ワンクリック不正請求に関する相談が依然として多数（155 件）寄せられています。
これらの相談は、アダルトサイト等で無料画像や無料動画と思ってクリックしただけで、料金を請求する悪意あるプログラムが取り込まされる被害にあったというものです。

このような事例では、以下の図に示すようなセキュリティ警告を無視して、自分で問題のプログラムを取り込んでしまっているケースがほとんどです。

動画や画像を表示するだけであれば、図のようなセキュリティの警告画面は表示されません（まず図 2-1 の警告画面が表示されます。このとき「実行」を選択すると図 2-2 の警告画面が表示されます）。

セキュリティの警告が表示されたら、ファイルの「種類」やファイルの「発行元」の情報をチェックし、安全が確認された場合以外は［実行］や［実行する］をクリックしないようにしましょう。



図：2-1　　図：2-2

（ご参考）

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

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

		6月	7月	8月	9月	10月	11月
届出(a) 計		**22**	**15**	**50**	**46**	**22**	**24**
	被害あり(b)	20	8	30	21	15	8
	被害なし(c)	2	7	20	25	7	16
相談(d) 計		**32**	**31**	**24**	**35**	**53**	**30**
	被害あり(e)	19	18	13	26	37	20
	被害なし(f)	13	13	11	9	16	10
合計(a+d)		**54**	**46**	**74**	**81**	**75**	**54**
	被害あり(b+e)	39	26	43	47	52	28
	被害なし(c+f)	15	20	31	34	23	26

（1）不正アクセス届出状況

11 月の届出件数は 24 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 30 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 4 件、メール不正中継 1 件、DoS 攻撃 1 件、アドレス詐称 2 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、フィッシングに悪用するためのコンテンツを設置されていたものが 2 件、などでした。侵入の原因として、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事例が 1 件ありました。

被害事例

[侵入]

(i) SSH(*2)で使用するポート(*3)への攻撃

事例	・サーバ管理者が SSH でログイン出来なくなった。 ・調査したところ、SSH の設定ファイルにエラーがあったためと判明。そのファイルの更新日時に SSH でログインしていたアカウント(*4)のユーザによれば、アクセスした覚えは無いとのこと。よって、組織外の第三者の不正アクセスによるファイル改ざんと判断。 ・破られたと見られるアカウントは、**簡易な初期パスワードのまま変更されていなかったため、容易に推測されてしまった**ものと思われた。 ・対策の第一段階として、まずは組織外からの SSH アクセスをファイアウォールで制限することにした。
解説・対策	本来、初期パスワードは、あくまでもアカウントを発行する際に必要なために作成した仮のものです。**アカウントの所有者は、アカウント発行通知を受け取ったら即、パスワードを変更すべき**です。今回のケースでは、「**初期パスワードでも簡易のものではなく、ランダムに発生した長い文字列にする**」「**同じパスワードを一定期間以上続けて使えなくする仕組みにする**」といった対策も有効です。さらに、**日々アクセスログ(*5)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。 (参考) IPA ‐ 今月の呼びかけ (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) サイトへのパスワードクラッキング(*6)攻撃

事例	・自社で運用しているオンライン証券取引サイトのログチェック時、通常の 10 倍以上多くのログインアクセスが認められたため、不正アクセスを疑い調査を開始。 ・簡易なパスワードを設定していた 26 のアカウントでパスワードが破られ、不正にログインされていたことが判明。 ・ログインの際のパスワード入力リトライは 9 回までに制限していたが、**旧システムのぜい弱なパスワード（4 桁）を変更せずそのまま使用していた**アカウントなどがログインを許してしまっていた。

解説・対策	適切なログチェックのおかげで、被害を最小限に食い止められた良い例です。しかし、金融取引サイトという性格上、通常のサイトよりもさらに出来うる限りの不正利用防止策を講じておく必要があるでしょう。事例(i)で紹介したものの他に、「**ログイン後の取引の重要度に応じてパスワードを多重化する**」「**固定パスワードの他に、乱数表を使用したパスワードも併用する**」などの対策も有効です。 (参考) IPA ‐ 今月の呼びかけ (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

4．相談受付状況

11 月の相談総件数は **711 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 **155 件** (10 月：236 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 **18 件** (10 月：41 件)、**Winny に関連する相談**が **12 件** (10 月：12 件) などでした。

IPA で受け付けた全ての相談件数の推移

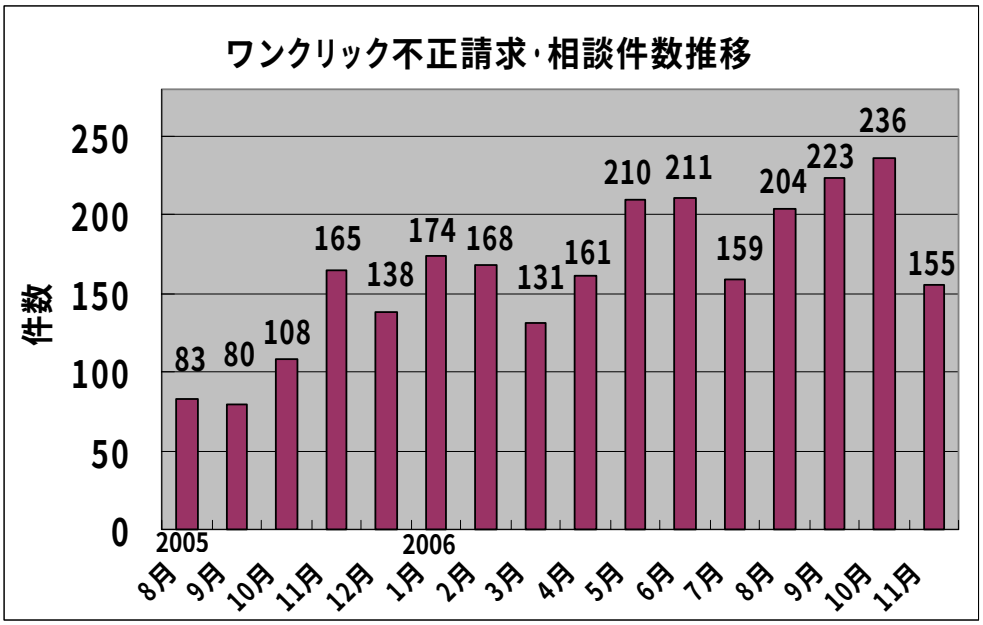
	6月	7月	8月	9月	10月	11月
合計	**773**	**767**	**793**	**933**	**1,002**	**711**
自動応答システム	423	444	460	575	580	423
電話	283	257	280	302	326	214
電子メール	64	66	48	51	93	72
その他	3	0	5	5	3	2

※ 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



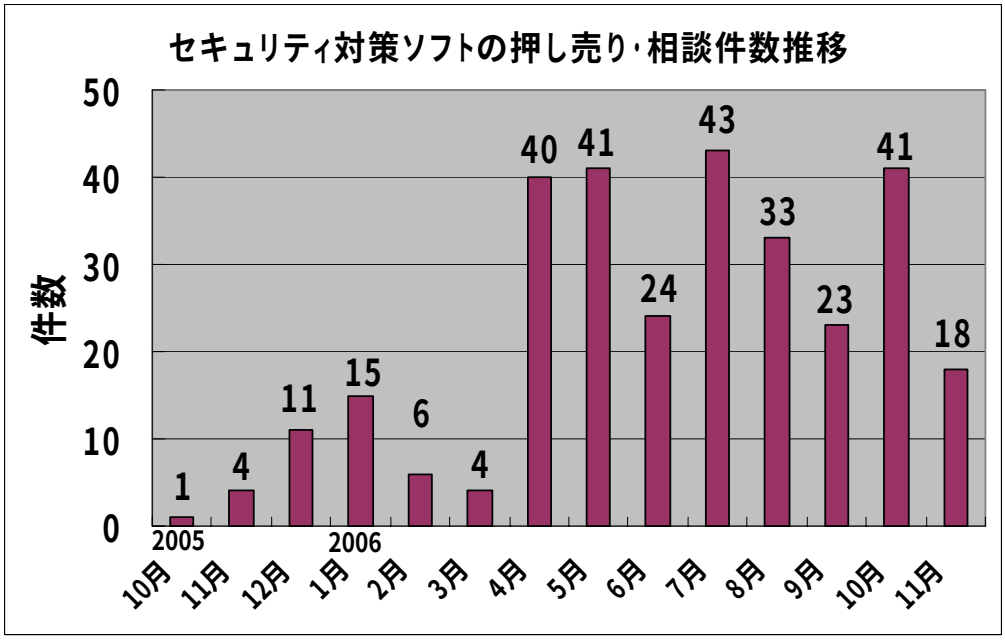
ワンクリック不正請求についての対策については下記をご参照ください。

･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) ウイルスを削除しても、またすぐ感染？

相談	メールを受信した時に、ウイルスに感染したようです。**ウイルス対策ソフトが検知して削除してくれるのですが、他のメールを受信する際にまたウイルス検知の警告が出ます**。ウイルスが削除されていないということでしょうか。どうしたら、完全に削除できるのでしょうか。
回答	**ウイルス対策ソフトが発するメッセージをよく読みましょう**。このケースでは、メールをパソコン内のメールソフトで受信する直前に、ウイルス対策ソフトがウイルスを検知して削除した、というメッセージのはずです。つまり、**パソコン内のウイルス感染を検知したのではなく、ウイルスがパソコン内に侵入しようとする水際で排除した、という嬉しいお知らせなのです**。安心してください。

(ii) YouTube サイトで詐欺？

相談	YouTube のサイトでビデオを観ていた際、サイトの片隅にあったバナー(*1) に「**おめでとうございます！　あなたは 999,999 人目のお客様です！**」と英語で書かれていたのでクリックしてみた。すると、**賞金を請求するために必要とのことで住所氏名、メールアドレスなどを入力させられ**、さらにフリーロトのサイトにジャンプしてしまった。数回ゲームをした後、**クレジットカード番号の入力を促されたが、“怪しい”と感じて入力はしなかった**。しかし、フリーロトサイトからメールが届いていた。請求書などが来るのか？
回答	サイト側にはメールアドレスを知られているため、迷惑メールが届き始める可能性があります。請求書が来るかどうかは、サイトによって異なるでしょう。**まずはメールアドレスを変更し、様子を見ましょう**。そもそも、**信頼できるか分からないサイトで不用意に個人情報を入力すべきではありません**。**有名なサイトだからといって、そこにあるバナーまでもが信頼できるとは限りません**。うまい話の裏には、ワナが待ち受けていることが往々にあります。**ネットの世界だからといって油断せず、甘い誘惑に負けないようにしましょう**。万が一、契約に関するトラブルに巻き込まれてしまったら、最寄りの消費生活センターに相談しましょう。 (ご参考) IPA ‐ 今月の呼びかけ (7 月分) 「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 国民生活センター ‐ 全国の消費生活センター http://www.kokusen.go.jp/map/

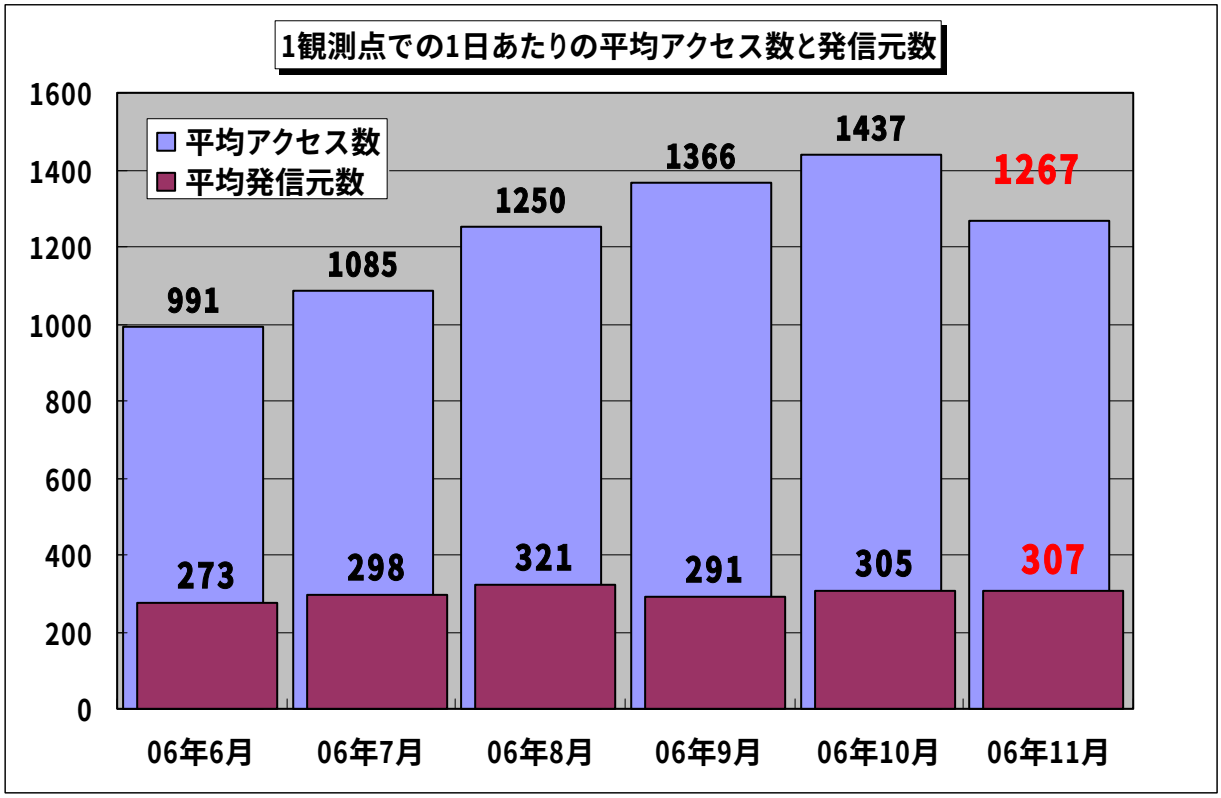
(iii) ファイル共有ソフトでウイルス感染＋情報流出？

相談	ファイル共有ソフト**「LimeWire」「cabos」「share」「WinMX」などを使用**。数日前、**パソコン起動時にドクロマークが表示され、一切の操作を受け付けなくなった**。新しいハードディスクに載せ換えて、リカバリーを実施。後から調べたら、Antinny 系のウイルスらしいことが分かったが、ウイルス対策ソフトでは何も見付からない。**仕事関係のファイルがパソコンに入っていた**。今後、どうすれば良いか。
回答	暴露系ウイルスに感染している可能性が非常に高いと言えます。**まずは流出した可能性のあるファイルを特定し、影響が及ぶと思われる関係先に一刻も早く報告して善後策を検討しましょう**。 ファイル共有ソフトの使用には、その特性上、たとえウイルスに感染していなくても自分の操作ミスなどで誤って意図しないファイルを公開してしまうリスクがあります。メリットだけに注目してしまい、リスクについてもきちんと認識できないのであれば、ファイル共有ソフトは使うべきではありません。**仕事のファイルが入っているパソコンでファイル共有ソフトを動かすなど、言語道断です**。ファイル共有ソフトの利用は、こうした危険と隣り合わせの行動であることを改めて認識しましょう。 （ご参考） IPA - Winny による情報漏えいを防止するために http://www.ipa.go.jp/security/topics/20060310_winny.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

5．インターネット定点観測での 11 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 11 月の期待しない（一方的な）アクセスの総数は、10 観測点で **380,054 件**ありました。1 観測点で 1 日あたり **307** の発信元から **1,267 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、307 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 6 月～2006 年 11 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、7 月以降増加傾向でしたが、11 月は 8 月と同レベルまで減少しました**。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。

11 月のアクセス状況は、全体的には 10 月とほぼ同じ状況ですが、10 月のファイル交換関連と思われるポートへのアクセスは減少しました（図 5.1.1）。

はじめにファイル交換について説明します。ファイル交換とは、ファイル交換ソフトを利用して特定のコンピュータどうしで直接ファイル（データ）を交換することです。

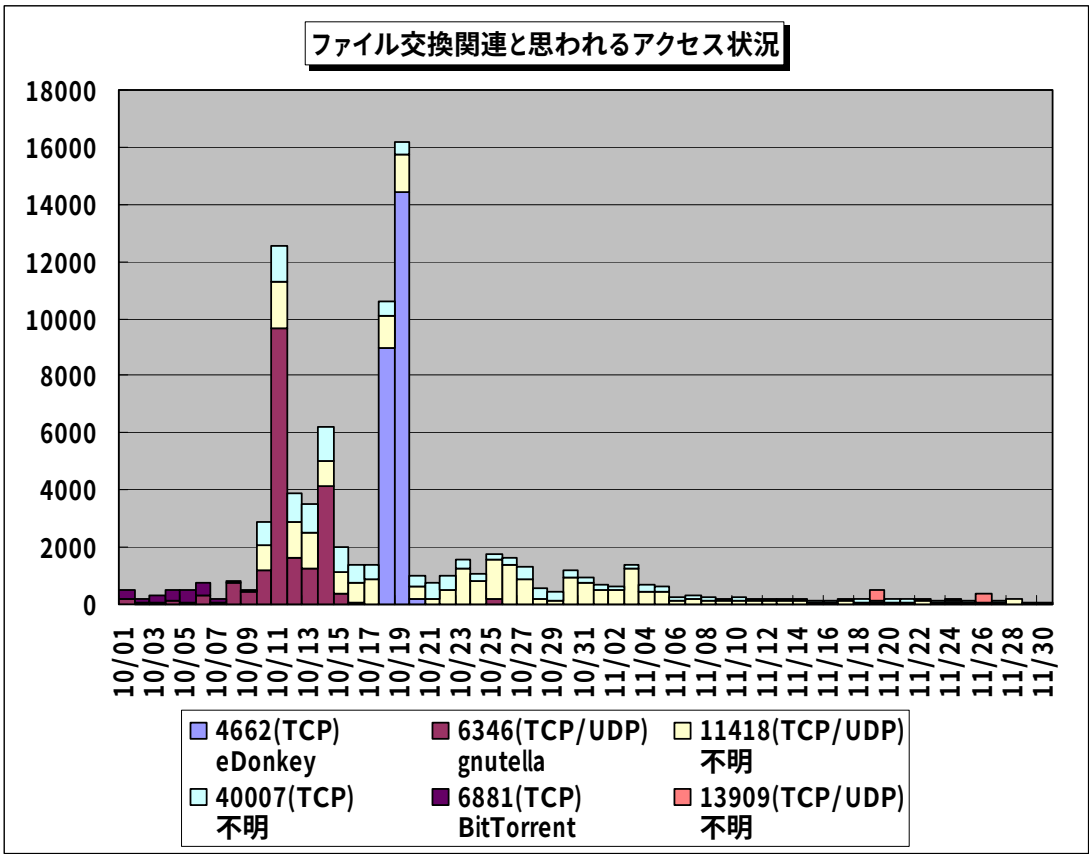
ファイル交換の方法にはいろいろありますが、ファイル交換を行うための情報を管理するサーバを中心としたファイル交換ネットワークを組む方式と、ファイル交換ソフトを介して数多くのコンピュータが直接ファイル交換ネットワークを組む方式がほとんどです。

ファイル交換を行うコンピュータは、一般的に、そのコンピュータが使っている IP アドレスによって特定されます。交換できるファイルの情報と、この IP アドレスの情報等がファイル交換ネットワーク上を流れることになります。

ところで、一般的なインターネットの利用者のコンピュータは、利用するプロバイダを介してネットワーク上の空いている IP アドレスを動的に割り当てられるのが普通です。そのため、ファイル交換を利用するコンピュータの IP アドレスも、ネットワークとの接続を行うたびに、違う IP アドレスになります。このため、ファイル交換を行っていたコンピュータがネットワークから切断されても、ファイル交換ネットワーク上には、以前使っていたIPアドレスの情報が残ってしまう場合があります。この残ってしまったIPアドレスが、同じプロバイダ内の違う利用者のコンピュータに割り当てられ、このコンピュータに対して、同じファイル交換ソフトを利用する別のコンピュータからファイル交換の接続要求（アクセス）がくることになります。

図 5.1.1 に示すアクセスのほとんどが、このような状況で発生したアクセスと考えられます。

ただし、これらのアクセスについては、特定観測点における特異アクセスと言うことで、本資料の各種統計データからは除外しているので注意して下さい。



【図 5.1.1 2006 年 10 から 11 月のファイル交換関連と思われるアクセス数の遷移】

これらのアクセスを行っていると予測されるファイル交換ソフトと発信元については、以下の通りです。

- eDonkey と呼ばれるファイル交換ソフトのデフォルトポートである 4662(TCP)ポートへのアクセスの発信元はスペイン方面がほとんどですが、11 月には 1 件も観測されませんでした
- gnutella 系のファイル交換ソフトのデフォルトポートである 6346(TCP/UDP)ポートへのアクセスの発信元は日本国内がほとんどでした
- ファイル交換ソフトの特定はできません(不明)が 11418(TCP/UDP)ポートへのアクセスの発信元は台湾方面がほとんどでした
- これもファイル交換ソフトの特定はできません(不明)が 40007(TCP)ポートへのアクセスの発信元も日本国内がほとんどでした
- BitTorrent 系のファイル交換ソフトのデフォルトポートである 6881(TCP)ポートへのアクセスの発信元も日本国内がほとんどでした
- これもファイル交換ソフトの特定はできません(不明)が 13909(TCP/UDP)ポートへのアクセスの発信元はオランダ方面がほとんどでしたが、このアクセスは 11 月から観測されました

著作権のあるデータ（ファイル）を非合法にファイル交換する人たちがいるため、最近ではサーバを中心に持つタイプのファイル交換では、サーバが閉鎖に追い込まれたり、違法なファイル交換を行った人が逮捕されたりという事件も起こっています。

さらに、ファイル交換を介した情報漏えい事故も多発しているため、ファイル交換を問題視する傾向もあるようです。最近では、航空自衛隊の内部情報がファイル交換ソフト Winny を介して漏洩した事故がテレビや新聞でも報道されていました。ファイル交換ソフトの利用者には、ファイル交換の仕組みをご理解いただき、さらなる注意を払ってください。

また、特定のＩＰアドレスに、前述のようなアクセスが集中すると、該当 IP アドレスを割り振られたコンピュータでは、あたかもＤｏＳ攻撃を受けているような状況となる場合もあります。このようなアクセスは、ほとんどがファイル交換を自動化して利用している場合に発生するものと考えられます。ファイル交換の利用者の方には、このような状況を理解いただき、ファイル交換の接続先の確認をあらかじめ行ってから、アクセスするように心掛けてください。

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/TALOT2-0612.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) **バナー** (banner)
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) **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) **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。

(*5) **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。

(*6) **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。

■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。