INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
第 07-17-112 号
2007 年 11 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 10 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 10 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。

1．今月の呼びかけ

今月の呼びかけ：　「 安易なクリックが危険を招く！！ 」
― 好奇心だけで先に進むと、危険が待っている！？ ―

従来から、IPA に寄せられる相談の中で一番件数が多い相談が「ワンクリック不正請求」に関してのもので、10 月の相談件数は **369** 件でした。過去最高の 2007 年 8 月の 330 件を超え、史上最悪となっています。

相談の中でも、特に「請求書が表示され、消えなくなってしまいました。」といったものが多くありますが、これはウイルス感染によるものです。ウイルス感染により請求書が表示されるまでには、アダルトサイトなどの危険なサイト内を安易にクリックし続けて先に進んでいるためです。ユーザ自身の興味本位による操作がこのような被害を招いていることを認識して、自身の行動に注意していただくようお願いします。

図 1-1：請求書例

以下に、請求書が表示されるウイルスに感染するまでの典型例を示します。

(1)警告画面

通常の動画サイトであれば、画面上の再生ボタンをクリックすると動画の再生が始まります。ところが、被害に遭われた方から報告を受けたいくつかのアダルトサイトでは、**動画の再生ボタンをクリックすると、「ファイルのダウンロード - セキュリティの警告」画面が表示されます。**

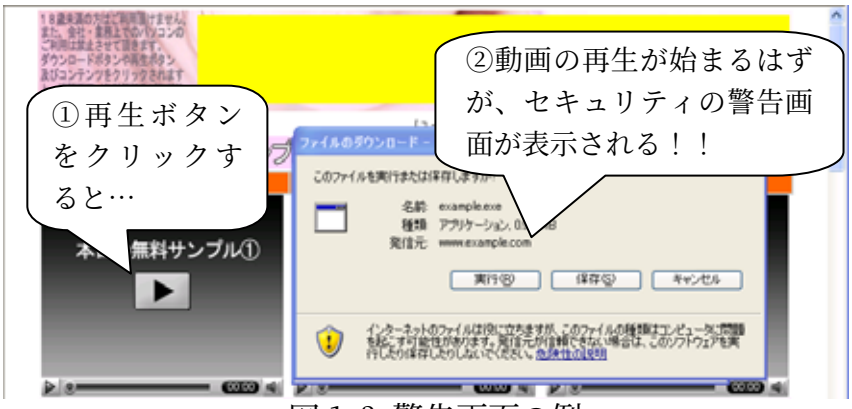


図 1-2：警告画面の例

無料のサンプル動画を再生するつもりで再生ボタンをクリックしたのに、セキュリティ警告の画面が表示されたということは、このサンプル動画の画面の作成者は、利用者に何か悪意のあるプログラムをダウンロードさせようとしていることになります。従って、この時点で**「キャンセル」ボタンをクリックして、これより先に進まないで下さい。**

(2)再度の警告

しかし、図 1-2 の警告画面でそのまま**[実行]**ボタンを押す、または**[保存]**ボタンで一旦パソコンに保存し、その後保存したファイルを実行すると、図 1-3 のような「本当にダウンロードしたソフトウェアを実行するか」という確認をするため、**「Internet Explorer - セキュリティの警告」**画面が表示されます。

Windows では、ダウンロードするソフトウェアの発行元が正当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」**の欄には、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1-3の例では、発行元が**「不明な発行者」**となっており、画面下部にも警告が表示されています。この発行元を信頼することはできません。このような場合は、**[実行しない]**ボタンをクリックして、ここから**先に進まないようにしてください。**

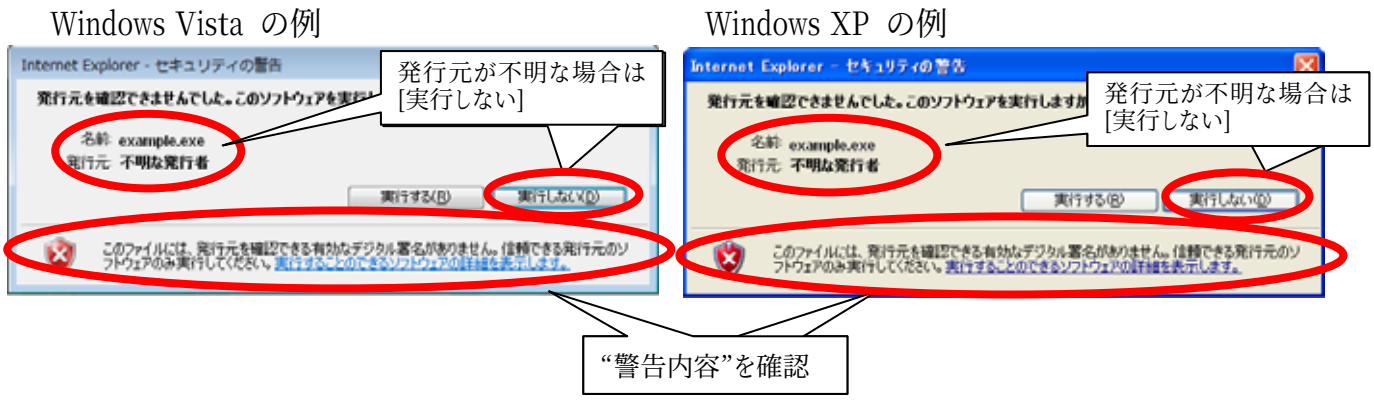


図1-3：Internet Explorerのセキュリティ警告画面

(3)警告を無視すると

それでも、図1-3の例で**[実行する]**ボタンをクリックして先に進んでしまった場合、例えば**「年齢を確認する」**画面や、**「利用規約などを表示した最終確認」**画面が表示されます。そして、図1-4の**「年齢を確認する」**画面で「はい」ボタンをクリックして、図1-5の「画面再生」のような画面が表示された後**「OK」**ボタンをクリックしてしまうと、ウイルスに感染して請求書の画面（図1-1）が表示されて、消えなくなってしまいます。

図1-4：年齢確認画面の例

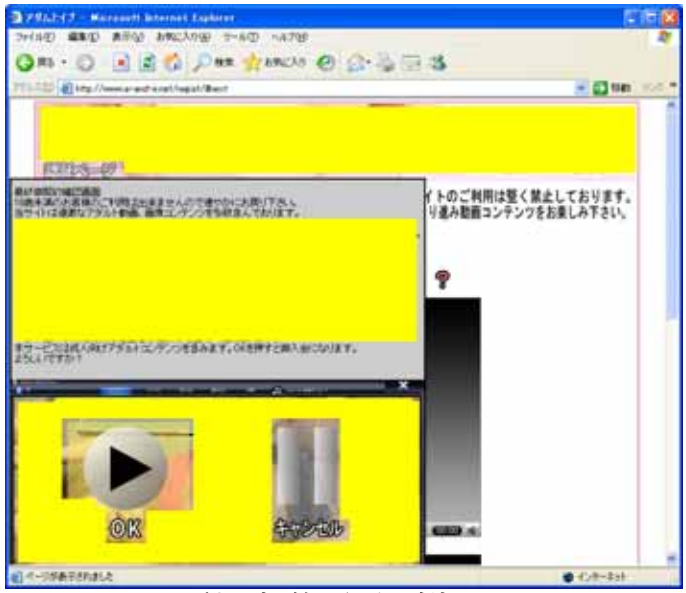


図1-5：利用規約画面の例

相談の中には、**「画面を見ただけで、勝手に表示されました」**とか、**「軽い気持ちで閲覧しただけで何もしていません」**と言われる方がおられます。しかし、図1-2から図1-5の画面に至るまでに**最低でも4回も画面をクリックしていることになります。**

このように、図1-1のような請求書が表示されるまでには、ご自身がいくつもの操作を行っている事を再認識して、ここで説明したような画面が表示されたら、どこでウイルスに感染するかわかりませんので、このようなサイトからはすぐに離れることが重要です。

(4)被害に遭わないためには

ワンクリック不正請求の被害に遭わないためには、**「アダルトサイトに行かないこと」**が最大の対策です。しかし、最近は**「ペットの写真を見ていたら、アダルトサイトが表示された」、「芸能人の情報を見ていたら、アダルトサイトに行ってしまった」**など、アダルトとは関係の無いサイトからでも、アダルトサイトへ導かれてしまったという報告を多数受けています。

このようなサイトを閲覧中に、アダルトサイトが表示されても好奇心や興味本位でボタン等をクリックしないで、悪意のあるサイトが存在していることを認識していただき、絶対にそれ以上先に進まないでください。

(5)万が一請求書が表示された場合には

図 1-1 のような請求書が表示された場合でも、慌てないようにしましょう。決してすぐに**お金を振り込んだり、請求書の連絡先にメールや電話で問い合わせをしたりしてはいけません。**一旦パソコンを再起動して、請求書が表示されるかを確認してください。再起動後に請求書が表示されなければ、そのまま無視してください。再起動後も請求書が表示される場合には、不正プログラムが埋め込まれていますので、以下の**「システムの復元機能でシステムの状態を以前の正常な状態に戻す」**を行ってください。それでも請求画面が消えない場合は、お使いのパソコンを初期化する必要があります。

(a)システムの復元機能でシステムの状態を以前の正常な状態に戻す

以下のマイクロソフトのホームページを参考にして、「システムの復元」機能を使用してシステムを請求書が表示される前の日に戻すことを行ってください。

「システムの復元のやり方」
http://www.microsoft.com/japan/windowsxp/pro/business/feature/performance/restore.mspx

(b)パソコンの初期化

パソコンを購入した時の状態に戻す作業を実施します。

実際の作業方法は、購入時に添付されている説明書に記載されている「購入時の状態に戻す」等の手順に沿って作業してください。作業する前に重要なデータを外部媒体等に必ずバックアップしてから作業を行って下さい。

また、以下の基本的なセキュリティ対策も忘れずに行ってください。

・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　等

「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
「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
「ワクチンソフトに関する情報」
http://www.ipa.go.jp/security/antivirus/vacc-info.html
「Microsoft Update と Windows Update の利用の手順」(マイクロソフト社)
http://www.microsoft.com/japan/athome/security/mrt/wu.mspx

今月のトピックス

○ 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「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で侵入された
・フィッシングサイトを設置された

○ 相談の主な事例 （相談受付状況及び相談事例の詳細は、8 頁の「4.相談受付状況」を参照）

・Winny ネットワークに会社情報が漏洩したらしい・・・
・ウイルス感染？

○ 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。

・Windows の脆弱性を狙ったアクセスに注意！

2．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 50 万個**と、9 月の 44 万個から 15.2%の増加となりました。
また、10 月の届出件数(※2)は、**2,419 件**となり、9 月の 2,426 件から同水準での推移となりました。

※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。
・10 月は、寄せられたウイルス検出数約 50 万個を集約した結果、2,419 件の届出件数となっています。

検出数の1位は、**W32/Netsky** で**約 44 万個 、2 位は W32/Looked** で**約 2.5 万個、3 位は W32/Mytob** で**約 1.5 万個でした。**

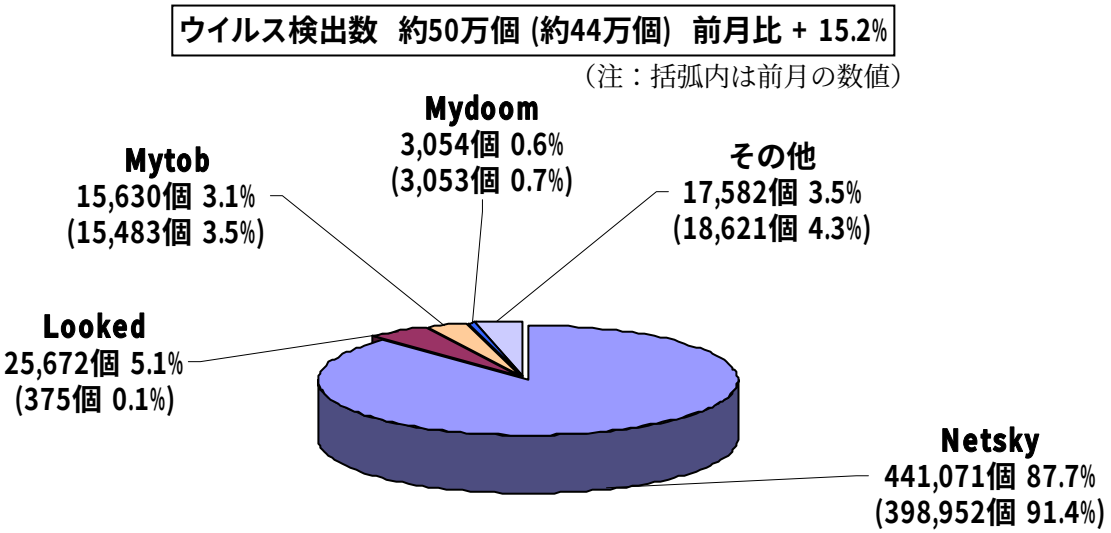


図 2-1

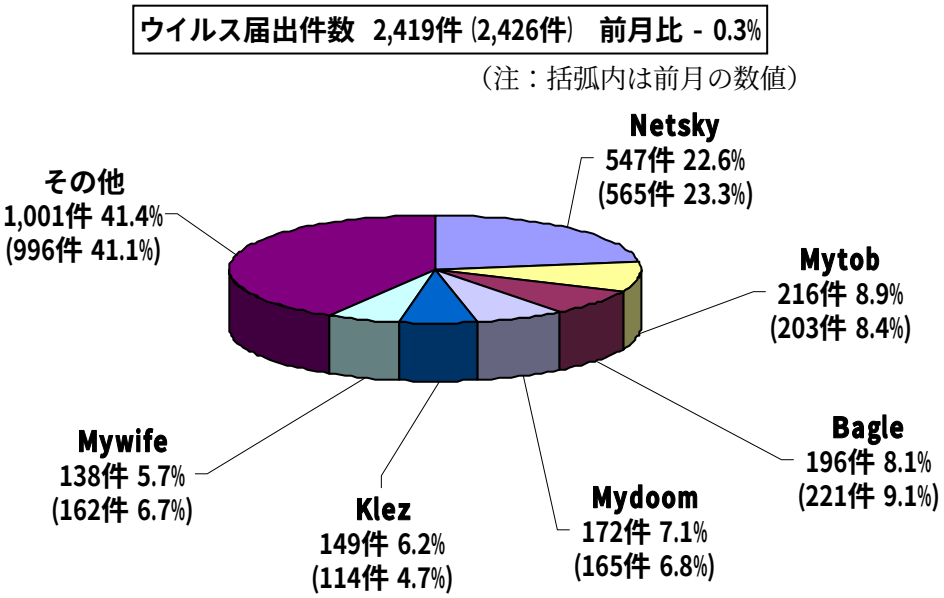


図 2-2

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

		5月	6月	7月	8月	9月	10月
届出(a) 計		**19**	**41**	**10**	**16**	**10**	**10**
	被害あり(b)	13	36	8	13	8	9
	被害なし(c)	6	5	2	3	2	1
相談(d) 計		**37**	**27**	**25**	**23**	**27**	**37**
	被害あり(e)	21	11	11	15	12	22
	被害なし(f)	16	16	14	8	15	15
合計(a+d)		**56**	**68**	**35**	**39**	**37**	**47**
	被害あり(b+e)	34	47	19	28	20	31
	被害なし(c+f)	22	21	16	11	17	16

（1）不正アクセス届出状況

10 月の届出件数は 10 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 37 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 22 件でした。

（3）被害状況

被害届出の内訳は、**侵入 3 件、DoS 攻撃 1 件、アドレス詐称 2 件、その他（被害あり）3 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なっていたものが 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 1 件、などでした。侵入の原因は、SSH※で使用するポートへのパスワードクラッキング※攻撃によるものが 1 件、サーバ OS のぜい弱性放置によるものが 1 件、などでした。

※フィッシング（Phishing）…正規の金融機関など実在する会社を装ったメールを利用して偽のウェブページに誘導し、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。
※SSH（Secure SHell）…ネットワークを介して遠隔のコンピュータと通信するためのプロトコルの一つ。
※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。ブルートフォース攻撃（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。

(4) 被害事例

[侵入]

(i) SSH※で使用するポートへの攻撃で侵入された

事例	・外部より、「貴方の管理しているサーバから攻撃を受けている」と連絡があった。 ・アクセスログ※を調査したところ、不特定多数の IP アドレスより SSH で使用するポートにパスワードクラッキング※攻撃を受けていたことが判明。 ・推測が容易なパスワードが設定されていたアカウントで、不正にログインされていた。さらに、そのアカウントが管理者権限に昇格されていた。 ・操作ログには、外部サーバへの攻撃コマンドを実行していた形跡があった。
解説・対策	侵入を許し、さらに外部サイト攻撃の**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。SSH で使用するポートへの攻撃は相変わらず多いようです。**SSH 運用時には、ログインの際に公開鍵認証※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、ログのチェックをこまめに実施するのはもちろんのこと、IP アドレスやドメインなどによる接続許可制限を施したり、無制限にパスワードクラッキングされ続けないような対策（一定回数のログイン失敗で、アカウントをロックするなど）をしたりすることが有効です。 （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

※SSH（Secure SHell）…ネットワークを介して遠隔のコンピュータと通信するためのプロトコルの一つ。
※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。
※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。ブルートフォース攻撃（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。
※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。

(ii) フィッシング※サイトを設置された

事例	・自分が管理するウェブサイトを閲覧したユーザから、「ある金融機関に似せたページがある」との連絡があった。 ・調査したところ、サーバに侵入され、フィッシングに悪用するためのコンテンツデータを設置されていたことを確認。 ・OS のぜい弱性の修正プログラムが長らく適用されていなかったことが原因。 ・組織内で運用しているセキュリティポリシー（OS のアップデート実施）が守られていなかったのも一つの要因。
解説・対策	OS を始めとして、**使用している全てのソフトウェアのぜい弱性解消は、最も基本的なセキュリティ対策**です。ソフトウェアのぜい弱性情報やアップデート情報をこまめにチェックし、対応漏れが生じないように注意しましょう。さらに、システム管理者としては、**セキュリティポリシーの遵守状況の定期的監査を実施**するなどの措置が必要になるでしょう。 （参考） JVN（Japan Vulnerability Notes） http://jvn.jp/

※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。

4．相談受付状況

10 月の相談総件数は **1128 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 **369 件**（9 月：270 件）と、過去最高記録を大幅に更新しました。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 **16 件**（9 月：12 件）、**Winny に関連する相談**が **11 件**（9 月：4 件）などでした。

IPA で受け付けた全ての相談件数の推移

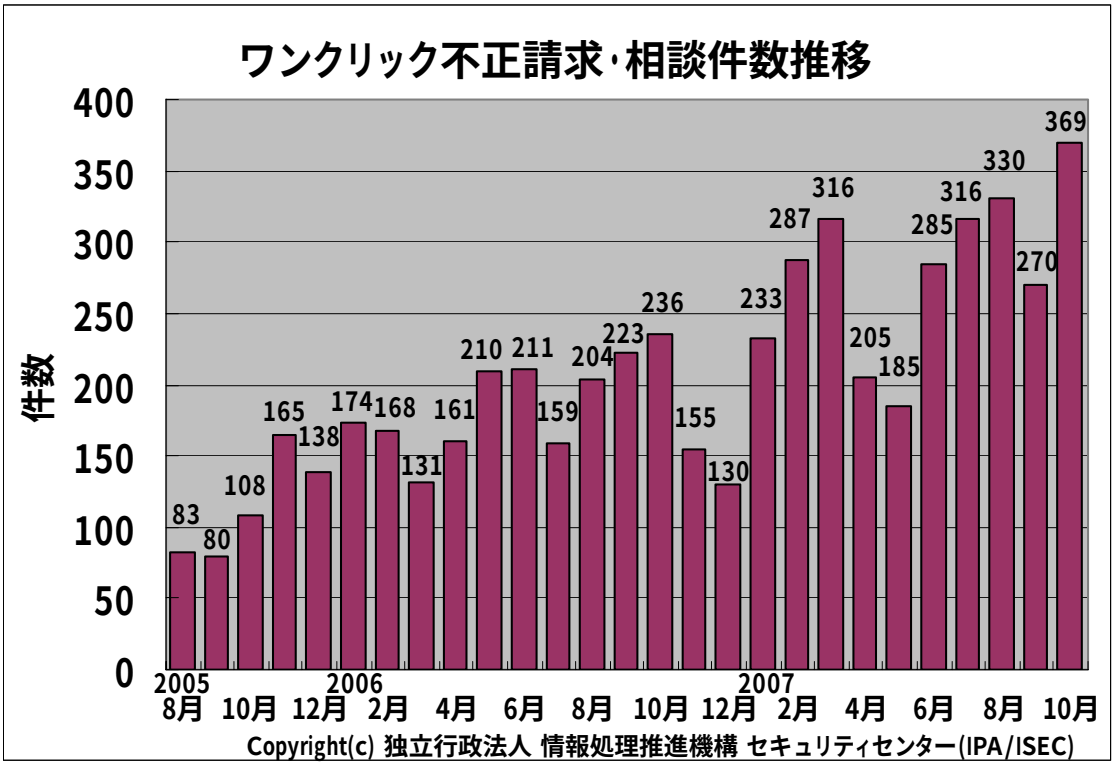
		5月	6月	7月	8月	9月	10月
合計		**814**	**932**	**1162**	**1013**	**910**	**1128**
	自動応答システム	484	537	694	593	544	669
	電話	254	339	402	374	310	397
	電子メール	69	53	65	43	55	57
	その他	7	3	1	3	1	5

※ 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



主な相談事例は以下の通りです。

(i) Winny ネットワークに会社情報が漏洩したらしい・・・

相談	某掲示板サイトに、自社の情報が Winny ネットワークに漏れているとの書き込みがあったようだ。外部から匿名の電話で通報が入った。会社としては、どうすればよいか？
回答	「**情報漏えいによる直接的・間接的被害を最小限に抑える**」ことを念頭において行動する必要があります。 ・外部からの問い合わせ・苦情対応窓口の一本化 ・事実関係の確認（漏えいした情報の現物の入手および確認） ※専門のセキュリティ業者に依頼するのが無難 ・社内の当事者の調査 ・被害者への連絡、謝罪 を真っ先に実施し、あとは下記ポイント集を参考にして行動しましょう。 （ご参考） IPA - 「情報漏えい発生時の対応ポイント集」 http://www.ipa.go.jp/security/awareness/johorouei/

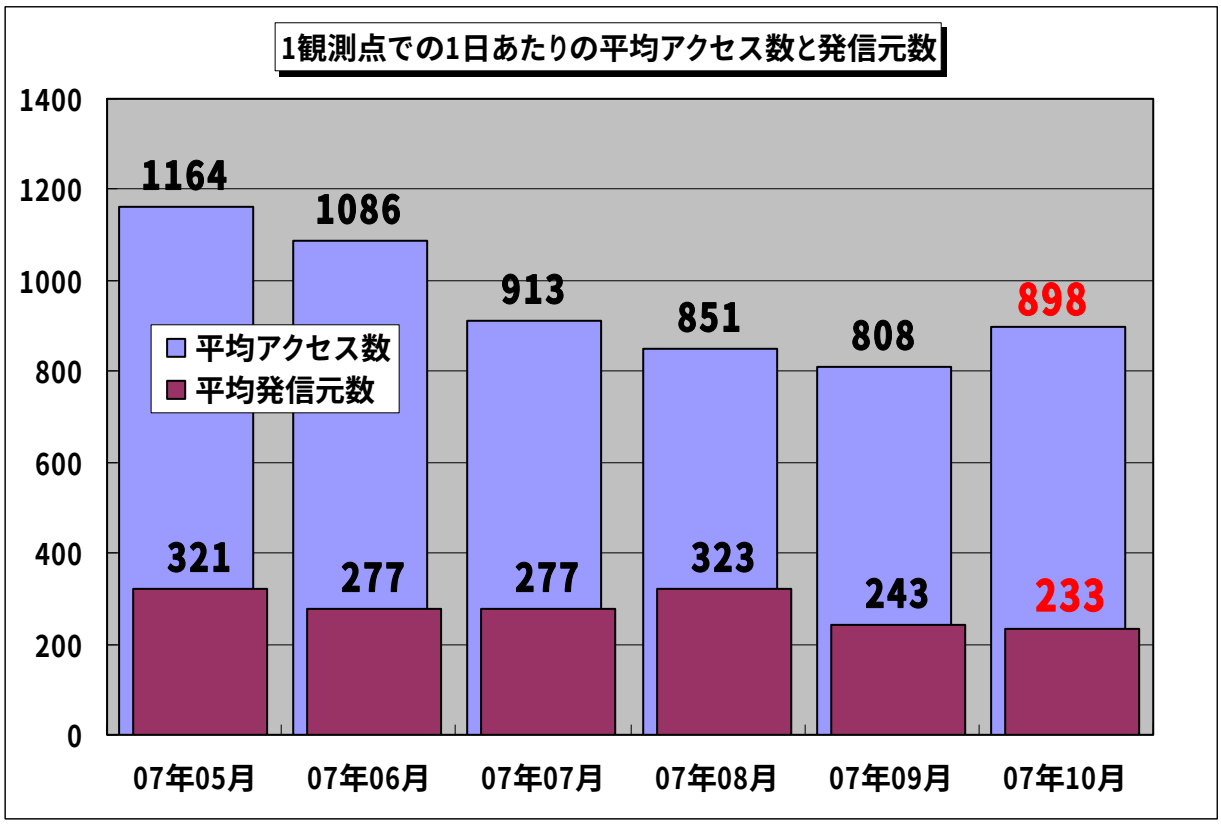
(ii) ウイルス感染？

相談	昨日まではパソコンは正常に動いていた。今日になったら、電源を入れても画面に何も映らない。真っ暗な画面のままで、ピーピーと音が断続的に出ている。多分、ウイルスに感染したのだと思う。
回答	ウイルスに**感染しているかどうかは、ウイルス対策ソフトでチェックするのが基本**です。この症状だけでは、何とも判断が出来ません。**パソコンが正常に起動しないのは、機械的故障の場合もあります**。何でもウイルスのせいにせず、まずはメーカに問い合わせをすべきです。 （ご参考） 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 10 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 10 月の期待しない（一方的な）アクセスの総数は、10 観測点で **278,497 件**ありました。1 観測点で 1 日あたり **233** の発信元から **898 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、233 人の見知らぬ人(発信元)から、発信元一人当たり約 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】

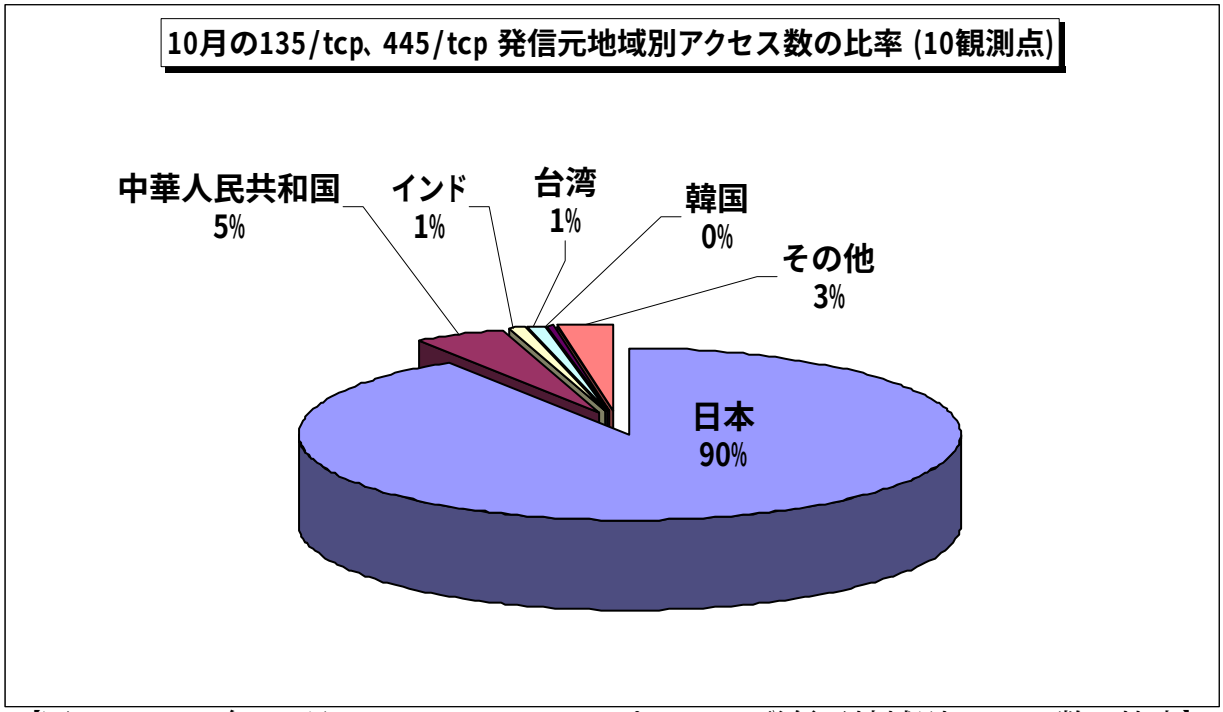
2007 年 5 月～2007 年 10 月までの各月の 1 観測点での 1 日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図 5-1 に示します。この図を見ると、期待しない（一方的な）アクセスは、9 月より若干ですが増加傾向にあります。

2007 年 10 月のアクセス状況は、8 月、9 月に比べると若干ですが増加しました。これは、Windows の脆弱性を狙っていると思われる、135/tcp、445/tcp のアクセスが増加したのが原因です。

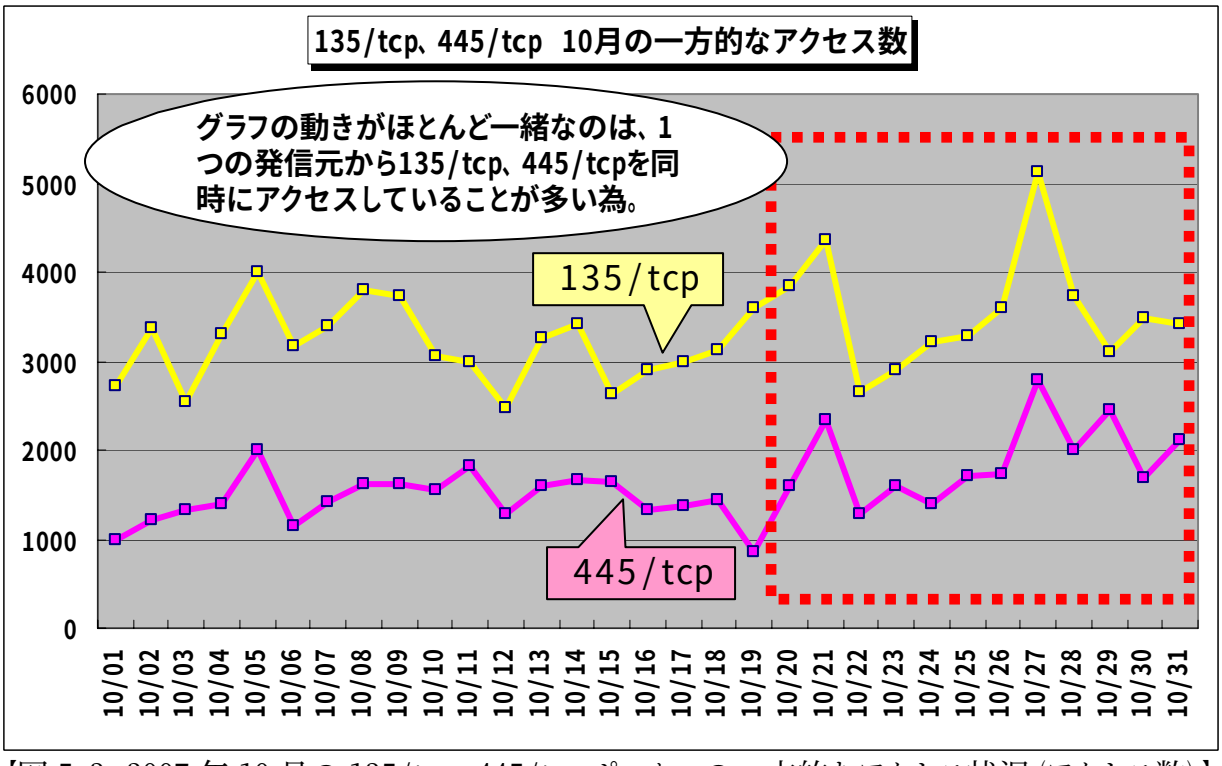
(1) Windows の脆弱性を狙ったアクセス

135/tcp や、445/tcp へのアクセスは、Windows の古い脆弱性（MS03-026、MS04-011）を狙ったアクセスと思われますが、今でも頻繁にアクセスがあるポートでもあります。最近では、ボットに感染したコンピュータが、さらにボットの感染を広げようとするアクセスが主流と思われます。

発信元地域は、ほとんどが日本からのアクセスです（図 5-2 参照）。また、1 つの発信元から 135/tcp と 445/tcp に対して、数回～数百回のアクセスを同時に行なっていることもわかっています（図 5-3 参照）。これを見る限り、ボットに感染しているコンピュータが、日本にもまだまだ多いと言えます。



【図 5-2 2007 年 10 月の 135/tcp、445/tcp ポートへの発信元地域別アクセス数の比率】



【図 5-3 2007 年 10 月の 135/tcp、445/tcp ポートへの一方的なアクセス状況（アクセス数）】

(参考情報)

■ 総務省･経済産業省 連携プロジェクト Cyber Clean Center サイバークリーンセンター
https://www.ccc.go.jp/

■ ボットの駆除手順
https://www.ccc.go.jp/flow/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/2007/documents/TALOT2-0711.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/

■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