INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
第 08-02-117 号
2008 年 2 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［2008 年 1 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、2008 年 1 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

「 気をつけよう　小さな油断　大きな被害 ※ 」
― 破壊型ウイルスと呼ばれる、原田ウイルスに注意！！ ―

※（第3回 情報セキュリティ標語・ポスター 2007年10月
標語部門入選作品 富山県・栃波市立庄西中学校 / 林 拓也さん）

1 月末に、「原田ウイルス」を作成した容疑者が逮捕されたとのニュースが大きく取り上げられ、IPA にも多数の相談、問合わせが寄せられました。「原田ウイルス」とは、主に Winny 等のファイル共有ソフトを利用したネットワークを介して流通するウイルスの一つです。このウイルスはファイルの削除等を行う破壊型であり、情報漏えい等を行う暴露型の Antinny 同様に悪質なものです。ファイル共有ソフトのネットワークに流通するファイルの危険性を再認識してください。

(1)原田ウイルスの特徴

原田ウイルスは、ファイル名に有名なアニメーションのタイトルやキャラクターの名前を含む映像ファイルに見せかけていることが確認されています。ファイル共有ソフトのネットワークを利用して、それら映像ファイルを求めている人を感染ターゲットにする目的であると考えられます。

このウイルスに感染すると図 1-1 の画面が表示されます。亜種の中には、人物の代わりにアニメキャラクターの画面が表示される場合もあります。表示されると同時に、パソコン内にある静止画ファイルや動画ファイルや実行ファイルなどを図 1-1 のような画像ファイルに置き換え、破壊してしまいます。

図 1-1：実行画面例

このような動作の特徴などから**「破壊型ウイルス」**とも呼ばれています。

(2)被害にあわないためには

原田ウイルスは、映像ファイルに見せかけるため、ファイルの見た目を偽装しています。このような場合、下記の方法でファイルの拡張子を確認することで、偽装されたファイルを見分けることが出来ます。拡張子とは、そのファイルが記録しているデータの種類を示すものです。

(a)拡張子の表示

Windows の初期設定では、ファイルの拡張子が表示されない設定になっています。下記の手順で拡張子を表示するように変更してください。

(i)Windows XP の場合

マイコンピュータもしくはエクスプローラのメニューバーから**[ツール]－[フォルダオプション] －[表示]タブ**を選択し、**[登録されている拡張子は表示しない]**のチェックを外す

(ii)Windows Vista の場合

スタートボタンから**[コントロールパネル]－[デスクトップのカスタマイズ]－[フォルダオプション]－[表示]タブ**を選択し、**[登録されている拡張子は表示しない]**のチェックを外す

(b)拡張子の確認方法

正しいファイルの例として、図 1-2(i)と図 1-2(ii)を示します。図 1-2(i)のファイルの拡張子は「avi」であり、動画であることを示しています。ところが図 1-2(ii)ではファイル名の末尾に「…」が表示され、拡張子が見えていません。これはファイル名が長すぎるため全てを表示できていないことを示しています。Windows ではファイル名がある一定の長さを超えると全部を表示せず、「…」で省略して表示することになっているためです。図 1-2(ii)の本当のファイル名は、「2007年10月長男運動会(小学校運動場).avi」で、正しい動画ファイルです。

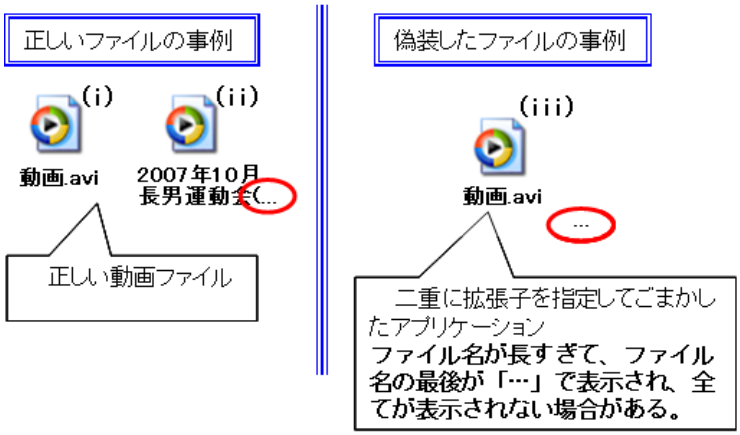


図 1-2:拡張子の見分け方例

図1-2(iii)と図1-2(i)のファイルは一見すると同じように見えますが、図1-2(iii)を良く見ると少し離れたところに「…」が表示されています。つまり、図 1-2(iii)のファイル名は長すぎるために全てが表示されていないということになります。図 1-2(iii)の本当のファイル名は「動画.avi .exe」であり、拡張子は「exe」、つまりアプリケーションプログラムです。ファイル名の途中にある大量のスペースのためにファイル名の全てが表示されず、拡張子が「exe」ではなく「avi」であると見誤ってしまいがちです。もし、図 1-2(iii)のようなファイルがウイルスだった場合、見た目で「動画」と判断してダブルクリックするとすぐにウイルス感染してしまいます。**このようなファイルが見つかった場合には、安易にクリックして開かずに、(c)の方法によりこのファイルの種類が何かを確認してください。**

(c)ファイルのプロパティでの確認方法

図1-2(iii)のファイルの拡張子は何かということを見るには、まず図 1-3(i)のようにファイルのアイコンの上で、マウスの右ボタンをクリックしてください。

次に、図 1-3(ii)のようなメニューが表示されますので、メニューの一番下にある「プロパティ」を選択します。そうすると、図1-3(iii)のような画面が表示され、「全般」タブの一番上に全体のファイル名が表示されます。この場合は、「avi」の後に多数のスペースがあり、最後にこのファイルの本当の拡張子である実行形式ファイルの「exe」が表示されています。また、「ファイルの種類」も「アプリケーション」(正しい動画ファイルの場合は「ビデオクリップ」となる)となっていますので、このファイルは動画ファイルではなく実行形式ファイルであることがわかります。これが、**ファイルの見た目を偽装するウイルスの典型的な例です。**

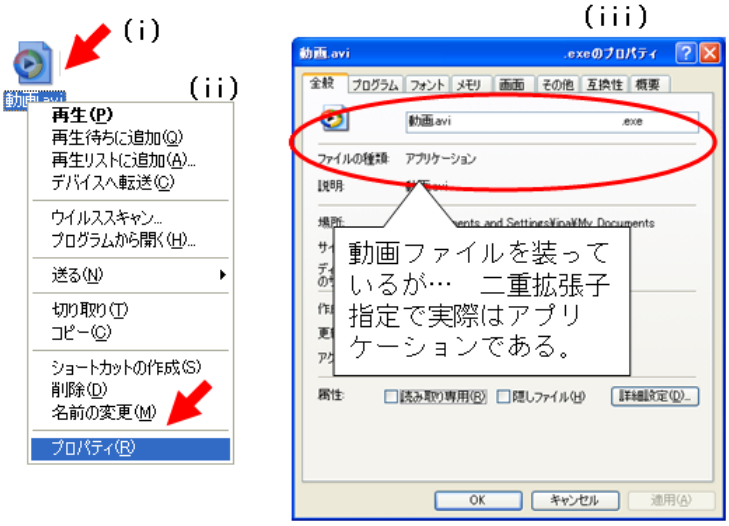


図 1-3:プロパティの確認例

(d)感染を防ぐためには

ウイルスの中には、この原田ウイルスのように、ファイルの見た目を偽装するようなウイルスがあることを認識してください。そして、利用しようとするファイルが「何か怪しいファイルだな」と感じたときは、上記の方法でそのファイルが何かということを確認してください。

このような確認を行うことで、原田ウイルスのようなウイルスから、少しでも感染を防ぐことができます。もし、原田ウイルスのような特徴を持つファイルが見つかったら、何もしないで**直ぐに削除してください。さらに Windows の場合はファイルの削除等を行うと「ゴミ箱」にファイルが移動しますが、念のためファイルを移動した後、ゴミ箱を空にすることをお勧めします。**

(3)感染した場合

原田ウイルスに感染した場合は、「(1)原田ウイルスの特徴」で記述したようにパソコン内のアプリケーションプログラム、映像データやデジカメで撮影した写真など個人の重要な情報が破壊されてしまい、残念ながら通常では復元する方法はありません。

破壊された情報を復元する方法は、**外部のハードディスクや DVD、CD 等の記録媒体に保存した情報からの復旧**しかありません。いつ被害に遭うかわかりませんので、常日頃から定期的に「バックアップ」をとることをお勧めします。

(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

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

○ 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
・オンラインゲーム上で使うアイテムや通貨が消失した

○ 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 でダウンロードしたファイルで、原田ウイルスに感染
・Cabos でダウンロードしたファイルでウイルス感染？

○ 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。
・135/tcp 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 31 万個**と、12 月の約 34 万個から 8.5%の減少となりました。
また、1 月の届出件数(※2)は、**2,046 件**となり、12 月の 2,239 件から 8.7%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。
・1 月は、寄せられたウイルス検出数約 31 万個を集約した結果、2,046 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 29 万個 、2 位は W32/Mytob** で**約 1 万個、3 位は W32/Mydoom** で**約 2 千 5 百個でした。**

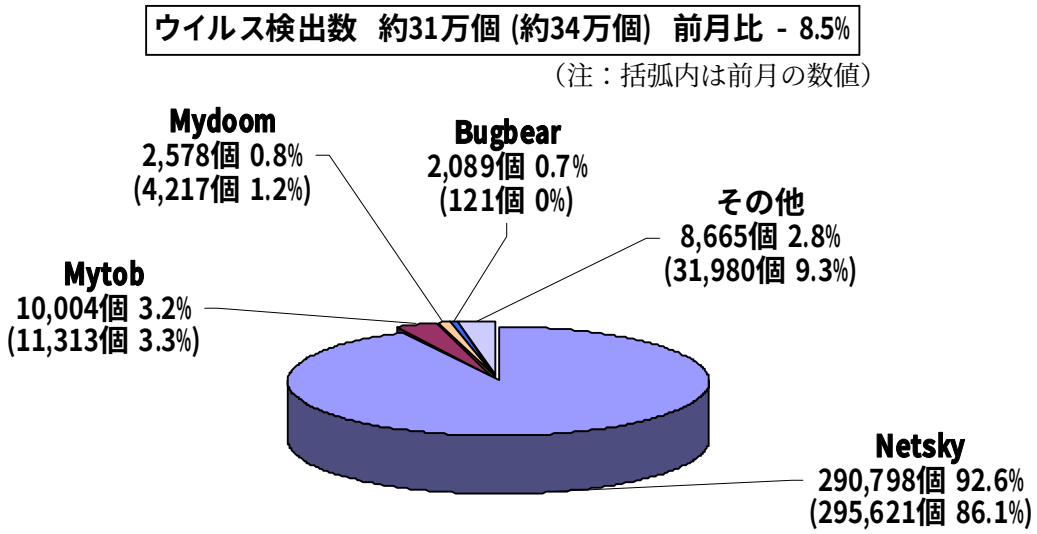


図 2-1

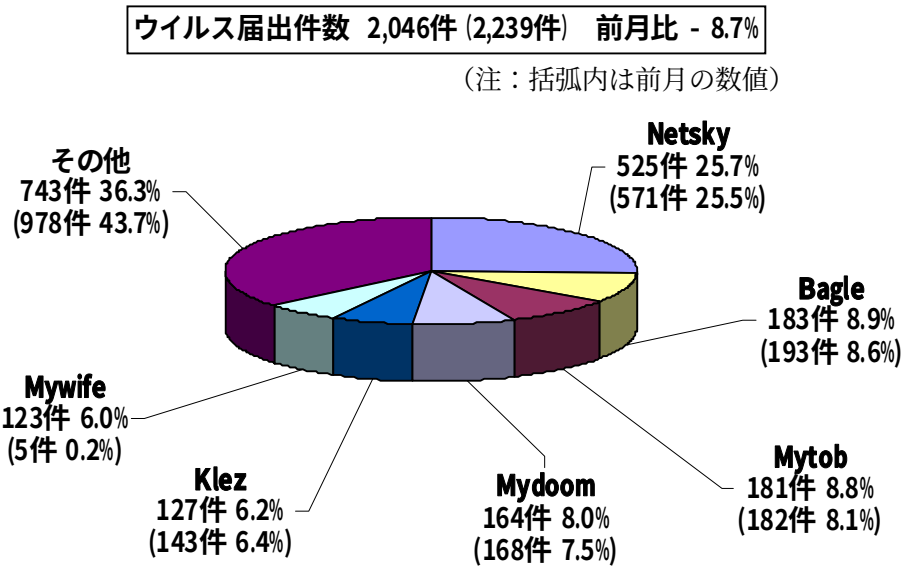


図 2-2

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

		8月	9月	10月	11月	12月	1月
届出(a) 計		16	10	10	15	14	8
	被害あり(b)	13	8	9	11	7	7
	被害なし(c)	3	2	1	4	7	1
相談(d) 計		23	27	37	31	21	24
	被害あり(e)	15	12	22	17	16	15
	被害なし(f)	8	15	15	14	5	9
合計(a+d)		39	37	47	46	35	32
	被害あり(b+e)	28	20	31	28	23	22
	被害なし(c+f)	11	17	16	18	12	10

（1）不正アクセス届出状況

1 月の届出件数は 8 件であり、そのうち**被害のあった件数は 7 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 24 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 15 件でした。

（3）被害状況

被害届出の内訳は、**侵入 3 件、その他（被害あり）4 件**でした。

侵入届出の被害は、3 件全てが他サイト攻撃の踏み台として悪用されたものでした。侵入の原因としては、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2件、ftpd（ftp サーバのプログラム）のぜい弱性への攻撃によるものが1件、でした。

その他（被害あり）の被害として、オンライン RPG（ロールプレイングゲーム）上で自分のキャラクターのアイテムやゲーム内の通貨が消失していたものが 1 件ありました。

※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。 ・当該サーバを調査したところ、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、結果的に侵入を許していたことが判明。 ・さらに、外部サイト攻撃のためのツールが埋め込まれ、実行されていたことも確認できた。 ・組織のルールとして、**SSH 運用時は公開鍵認証※とするポリシーになっていたが、これに違反し、パスワード認証で運用されていた**。
解説・対策	**組織のポリシーを遵守していれば、被害を免れていた**と思われる事例です。ポリシーを守る意識を醸成するとともに、改めて、組織のポリシーの内容の意味を理解する必要があるでしょう。管理する側としても、定期的にチェックする機会を設けられると良いでしょう。 (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

※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。

[その他（被害あり）]

(ii) オンラインゲーム上で使うアイテムや通貨が消失した

事例	・オンライン RPG (ロールプレイングゲーム) の会員である。 ・ある日、帰宅してパソコンを起動したところ、「回線が切断された」とのログが表示された。 ・不審に思い調査したところ、ゲーム内のキャラクターが持っていたアイテムやゲーム内通貨が消失していることを確認。原因は不明。
解説・対策	このような事例では、一般的にはログイン時のパスワードが破られたのが原因であることがほとんどです。**パスワードは推測されにくいもの** (可能な限り多くの文字種使用、辞書に無い文字列、長い文字列) とし、**定期的に変更することが有効な対策**となります。 原因究明にはアクセスログの解析が不可欠です。ゲーム運営会社に相談するとともに、警察機関への被害届出を検討すべきでしょう。 (参考) 警察庁 - インターネット安全・安心相談 http://www.cybersafety.go.jp/

4．相談受付状況

1 月の相談総件数は **408 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 **28 件**(12 月：43 件)、**Winny に関連する相談**が **17 件**(12 月：19 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 **10 件**(12 月：11 件) などでした。

IPA で受け付けた全ての相談件数の推移

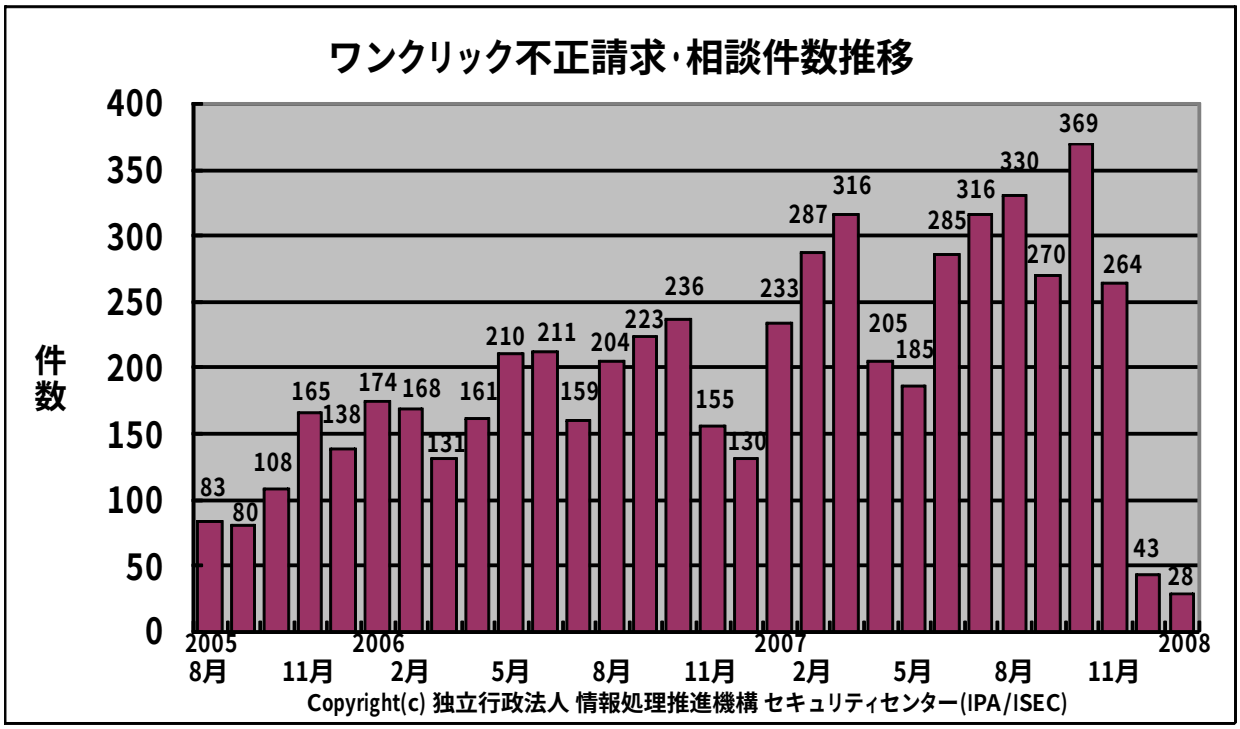
		8月	9月	10月	11月	12月	1月
合計		**1013**	**910**	**1128**	**911**	**389**	**408**
	自動応答システム	593	544	669	520	222	219
	電話	374	310	397	337	109	151
	電子メール	43	55	57	52	56	38
	その他	3	1	5	2	2	0

※ 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



主な相談事例は以下の通りです。

(i)Winny でダウンロードしたファイルで、原田ウイルスに感染

相談	Winny でダウンロードしたファイルを、動画だと思って開いたら、「原田ウイルスＯＯ（ダブルオー）」などという画面が表示された。見た目のアイコンは動画、ファイルの拡張子はスクリーンセーバである scr に見えたが、その後ろに大量のスペースが続き、その先に本当の拡張子 exe が付いていた。パソコン内のプログラムや画像のファイルが、「原田ウイルスＯＯ」と書かれた画像で上書きされ、破壊されてしまった。ウイルス対策ソフトを購入して使っていたが、何も検知してくれなかった。幸い、データのバックアップを取っていたので、1時間ほどで復旧できた。
回答	ウイルスによって破壊されたデータは、元に戻すことが困難です。日頃、重要なデータのバックアップを取っておくことが、有効な対策となります。 　なお、**Winny などのファイル共有ネットワークには、原田ウイルスのような“破壊型”の他に、Antinny のような“暴露型”など、凶悪なウイルスが多数流通**しています。不特定多数が参加するファイル共有ネットワークは危険だという認識を持つべきです。**ウイルスに感染したくなければ、ファイル共有ソフトを使わないに越したことはありません**。 （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

(ii) Cabos でダウンロードしたファイルでウイルス感染？

相談	ファイル共有ソフト Cabos でダウンロードしたファイルを開いたら、突然パソコンの電源が OFF になった。再度電源を入れると、画面に“**In God We Trust**”などと英語の文章が出て、その後は全く操作ができない。ウイルスに感染したのか？ウイルス対策ソフトは、何も検知しなかった。どうすれば良いのか。
回答	ウイルス対策ソフトで検知できない、新しいウイルスに感染した可能性が高いです。しかし、パソコンが正常に起動しないことにはウイルス駆除作業は困難です。**Windows XP であれば、「回復オプション」で起動すると復旧できることがあります**。もしダメだった場合は、パソコンを初期化することになります。 なお、**ウイルス対策の観点で見れば、出所の不明なファイルを開くことは最も危険な行為**です。そのようなファイルばかり流通しているファイル共有ネットワークの危険性を、改めて認識すべきです。 （ご参考） マイクロソフト - 前回正常起動時の構成機能を使用してコンピュータを起動する http://support.microsoft.com/kb/307852/ja

5．インターネット定点観測での１月のアクセス状況

インターネット定点観測(TALOT2)によると、2008 年 1 月の期待しない（一方的な）アクセスの総数は、10 観測点で **244,657 件**ありました。1 観測点で 1 日あたり **227** の発信元から **789 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、227 人の見知らぬ人(発信元)から、発信元一人当たり約 3 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。

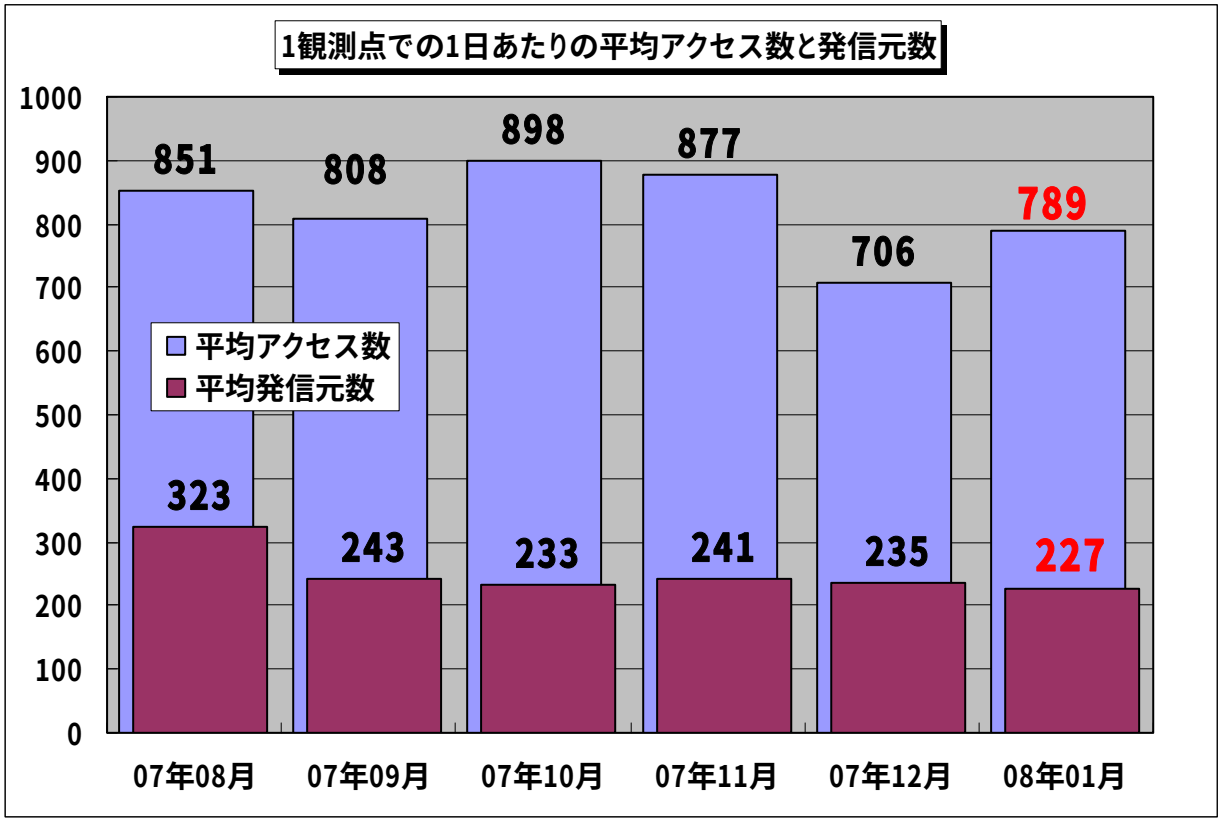


図 5-1：１観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数

2007 年 8 月～2008 年 1 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、1 月の期待しない（一方的な）アクセスは昨年 12 月よりも若干ですが増加しましたが、全体的なアクセスの内容としては、定常化していると言えます。

2008 年 1 月のアクセス状況は、昨年 12 月よりも、若干ですが増加しました。これは、Windows のぜい弱性を狙っていると思われる、135/tcp のアクセスが増加したのが原因です。また、昨年 12 月にアクセスが多かった、Windows Messenger サービスを悪用してポップアップメッセージを送信するアクセスの内、1028/udp のアクセス（主な発信元地域はカナダ）が減少しました。

（1）135/tcp を狙ったアクセス

1 月は 135/tcp へのアクセスが増加しました。これは、Windows のぜい弱性を狙っていると思われるアクセスで、最近では、2007 年 10 月に Microsoft 社から MS07-058 のセキュリティ情報が公開されてから、主に日本を発信元地域とした、135/tcp へのアクセスが増加傾向にありました。

（参考情報）
- 2007 年 10 月の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
- Microsoft セキュリティ情報（MS07-058） RPC の脆弱性により、サービス拒否が起こる (933729)
  http://www.microsoft.com/japan/technet/security/bulletin/MS07-058.mspx

11 月、12 月は、135/tcp のアクセスは減少していましたが、1 月に入り、中華人民共和国を発信元地域としたアクセスが、少しずつですが増加しています（図 5-2 参照）。

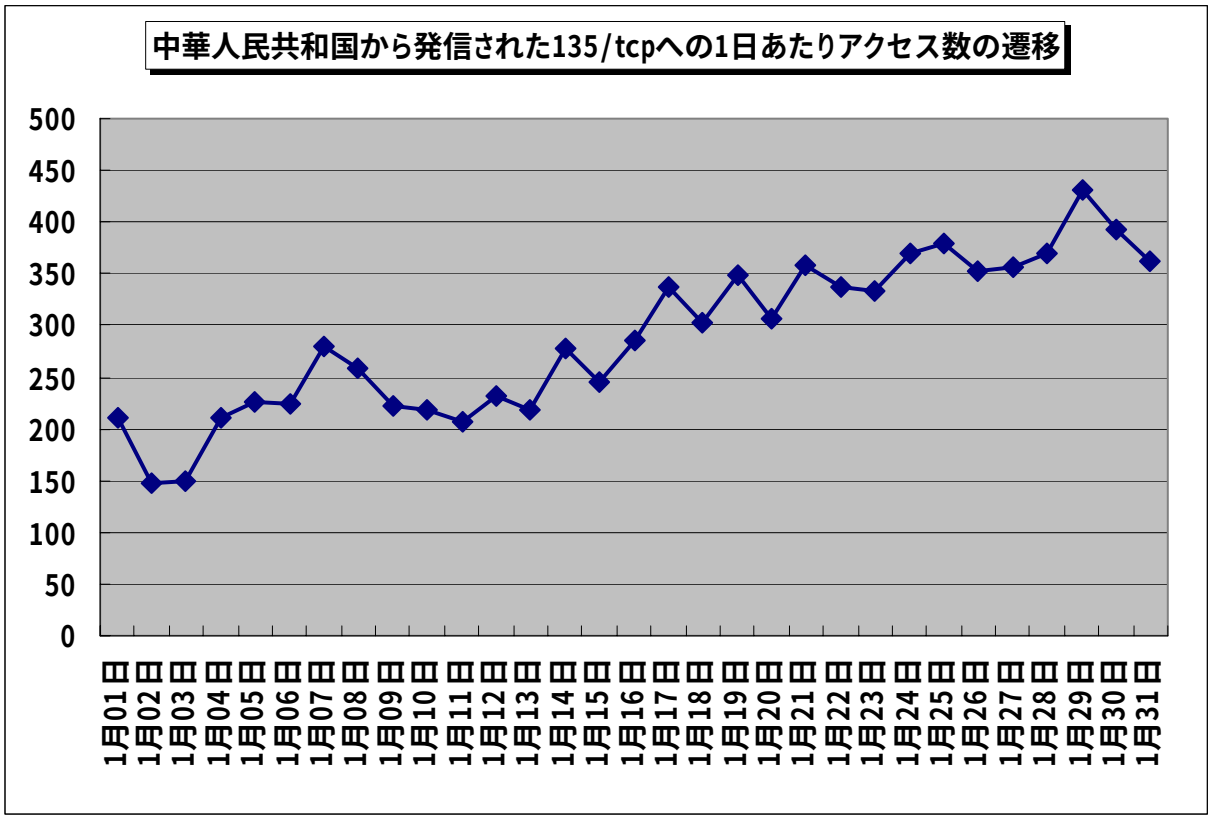


図 5-2：中華人民共和国から発信された 135/tcp への 1 日あたりアクセス数の遷移

この様なアクセスは、主にボットウイルスからと思われます。今後増える可能性は十分ありますので、以下の資料を参考にしてもらい、ボット対策および不正アクセス対策を実施して下さい。

（参考情報）
- ボット対策のしおり／不正アクセス対策のしおり
  http://www.ipa.go.jp/security/antivirus/shiori.html
- 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/
- 感染防止のための知識（サイバークリーンセンター）
  https://www.ccc.go.jp/knowledge/

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/2008/documents/TALOT2-0802.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