プレスリリース
第 08-05-120 号
2008 年 4 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［2008 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：西垣 浩司）は、2008 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。

1．今月の呼びかけ

「 オフィスソフトの文書ファイルにウイルスが！ 」
― アプリケーションの脆弱性を突くウイルスに注意！！ ―

3 月初めに、例えば北京オリンピックに関するスケジュール表のような情報を表示すると同時に悪さをするウイルスが発見されました。このウイルスの実体は、従来から多く見られる実行形式のプログラムファイルではなく、表計算ソフトのデータファイル形式でした。

表計算ソフトのデータファイル形式のウイルスとしては、従来からマクロウイルスが存在しています。マクロウイルスは、表計算ソフトなどで利用者の作業を簡略化する目的で処理を自動化するためのプログラム（マクロ）を悪用したウイルスです。これは、表計算ソフトの機能の一つであるマクロを無効にすれば感染しません。しかし、今回のウイルスは表計算ソフトの脆弱性（ぜいじゃくせい）を突いて感染するためマクロウイルスとは対策が異なり、注意が必要です。

(1)ウイルスの概要

このいわゆる「北京オリンピックウイルス」の仕組みを、図 1-1 を基に説明します。

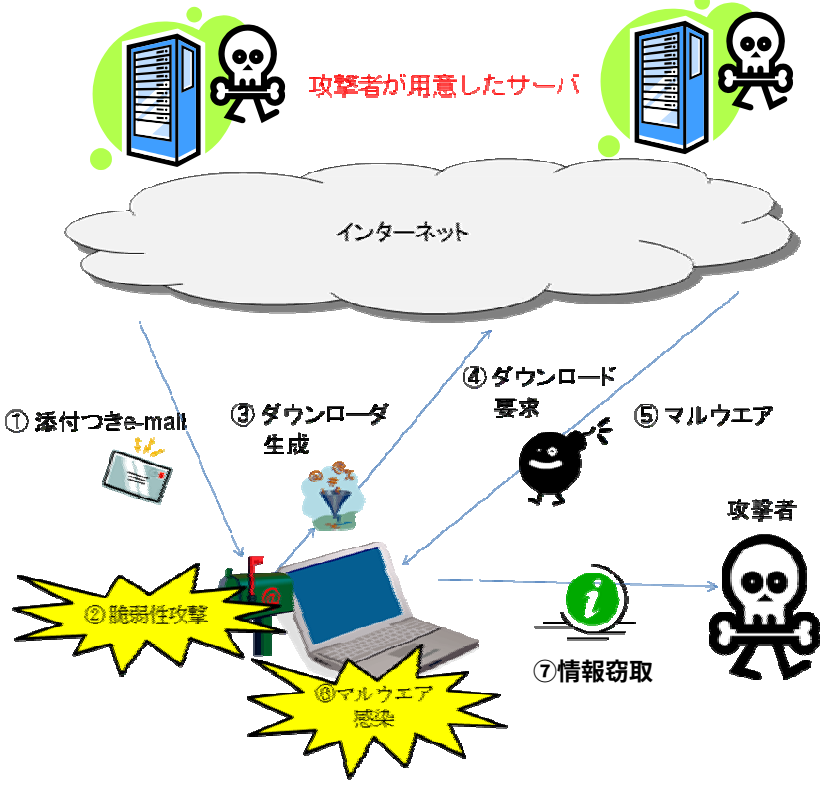


図 1-1 「北京オリンピックウイルス」の動き

ウイルスは、主にメールの添付ファイルとして、利用者の手元に届きます。そのファイルを開くと、表計算ソフトが起動し、ウイルスが仕込まれたワークシートファイルが読み込まれます。表計算ソフ

トの脆弱性が解消されていない場合、ウイルスの動作が開始されます。その際、ウイルスは偽スケジュール情報のワークシートを表示させ、利用者の注意を逸らします。その裏で「北京オリンピックウイルス」はダウンローダ（ダウンロード支援ツール）を作成し、攻撃者が用意したサーバから他のマルウェア（ウイルスなど悪意あるプログラムの総称）をダウンロードして実行することにより、情報窃取などの悪さを行います。これらのウイルスの多くは、標的型攻撃によって特定の企業や組織のアドレス宛メールの添付ファイルとして送られていました。そのため、無差別にばら撒かれた場合に比べると、ウイルス対策ソフトでの対応が遅くなり、検出が困難になる傾向にありました。このような攻撃は、最近増えてきていますので、事前の対策の重要性を良く認識してください。
(ご参考)
近年の標的型攻撃に関する調査研究－調査報告書－
http://www.ipa.go.jp/security/fy19/reports/sequential/

(2)脆弱性について

表計算ソフトに関する脆弱性として最近のものでは、アプリケーションなどの脆弱性の対応状況を公開している JVN iPedia（脆弱性対策情報データベース）によれば次のものが確認されています。

Microsoft Excel におけるメモリ破壊の脆弱性（JVNDB-2008-001031）
注)カッコ内は JVN iPedia の登録番号
http://jvndb.jvn.jp/contents/ja/2008/JVNDB-2008-001031.html

(ご参考)
JVN iPedia（脆弱性対策情報データベース）
http://jvndb.jvn.jp/

この脆弱性は 2008 年 1 月 15 日に発見されたものであり、3 月 12 日にこの脆弱性の修正プログラムが発表されるまでの約 2 ヵ月間、根本的な解決策が無い状態が続いていました。この脆弱性の影響範囲は、Windows 版の表計算ソフトに留まらず、Macintosh 版の表計算ソフトにも及んでいました。さらに、当該表計算ソフトに留まらず、表計算ファイル簡易表示ソフトにも及んでいました。

JVN iPedia には、ここで取り上げた表計算ソフトのみならず、次のようにワープロソフトや PDF 表示ツールなどの脆弱性および対策情報も掲載されています。

表 1-1 アプリケーションに関する脆弱性（抜粋）

影響のあるアプリケーション	狙われた脆弱性
表計算ソフト	Microsoft Excel の脆弱性 (JVNDB-2008-001168～73)
統合オフィスソフト	Microsoft Office の脆弱性 (JVNDB-2007-000117)
ワープロソフトなど	ジャストシステム製品の脆弱性 (JVNDB-2007-001067)
PDF 表示ツールなど	Adobe Acrobat などの脆弱性 (JVNDB-2008-001090～95)
マルチメディアプレーヤなど	RealNetworks 製品の脆弱性 （JVNDB-2007-000904～08）

(3)対策

上述のように、広く利用されているアプリケーションにも脆弱性が存在しています。製品開発者は脆弱性が発見されるとそれを解消して、自社のウェブサイトや JVN iPedia などでアプリケーション

の更新情報を公開します。このため、製品開発者や JVN iPedia から提供されるアプリケーションの脆弱性情報やバージョン更新履歴を定期的にチェックし、アプリケーションを常に最新の状態に更新して安全に利用できるようにしておくことが、今回の「北京オリンピックウイルス」などに感染しない方法として最も重要です。

その他、パソコンおよびインターネットの利用者は、被害に遭わないために以下に挙げる対策を必ず行ってください。Windows ユーザも、Macintosh ユーザも、同様の対策が必要です。

(a) 信頼できないメールに添付されているファイルは、オフィスの文書、PDF、映像・音声ファイル、実行可能プログラムなど、どんなファイルでも決して開かない。信頼できないサイトからダウンロードしたファイルも同様。

(b) ウイルス対策ソフトのウイルス定義ファイルを、常に最新の状態に更新して使用する。

(c) パーソナルファイアウォールを導入し、許可したアプリケーションやポート番号によるもの以外の外部への通信を遮断する。

(ご参考)
「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

Macintosh で Office をお使いの場合[Mactopia ダウンロード コーナー](マイクロソフト社)
http://www.microsoft.com/japan/mac/download/default.mspx

Mac OS サービスおよびサポート(アップル社)
http://www.apple.com/jp/support/osfamily/

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、5 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
・ウェブサイトのコンテンツが繰り返し改ざんされる

○ 相談の主な事例 (相談受付状況及び相談事例の詳細は、7 頁の「4.相談受付状況」を参照)
・Winny を使っていてウイルス感染し、個人情報が流出した
・Linux のサーバがウイルス感染?

○ 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。
・5900/tcp を狙ったアクセスに継続して注意!

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 21 万個**と、2 月の約 26 万個から 18.3%の減少となりました。
また、3 月の届出件数(※2)は、**1,651 件**となり、2 月の 1,854 件から 10.9%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。
・3 月は、寄せられたウイルス検出数約 21 万個を集約した結果、1,651 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 20 万個 、2 位は W32/Mytob** で**約 5 千 6 百個、3 位は W32/Mydoom** で**約 1 千 2 百個でした。**

ウイルス検出数　約21万個 (約26万個)　前月比 - 18.3%

（注：括弧内は前月の数値）

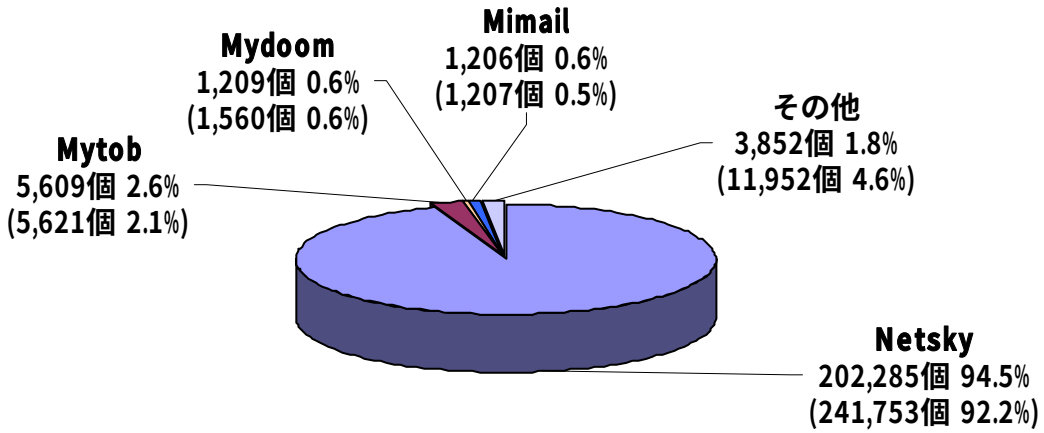


図 2-1

ウイルス届出件数　1,651件（1,854件）　前月比 - 10.9%

（注：括弧内は前月の数値）

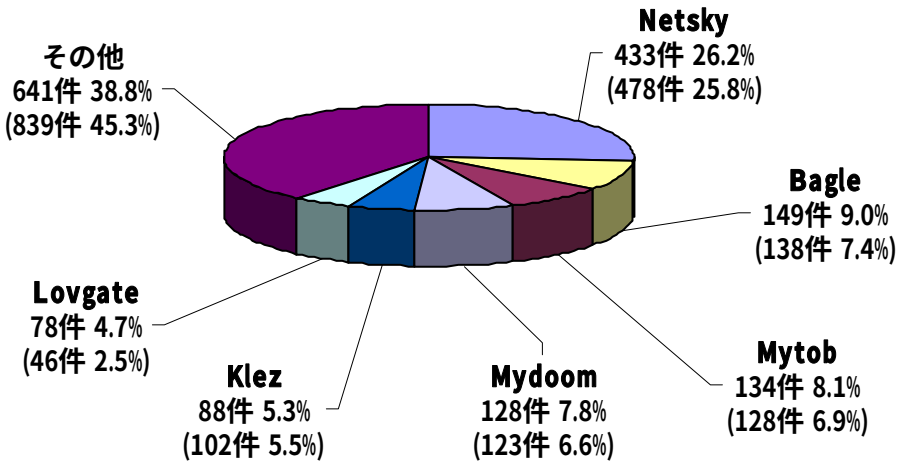


図 2-2

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－

表 3-1　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		10	15	14	8	4	19
	被害あり(b)	9	11	7	7	4	13
	被害なし(c)	1	4	7	1	0	6
相談(d) 計		37	31	21	24	29	35
	被害あり(e)	22	17	16	15	10	15
	被害なし(f)	15	14	5	9	19	20
合計(a+d)		47	46	35	32	33	54
	被害あり(b+e)	31	28	23	22	14	28
	被害なし(c+f)	16	18	12	10	19	26

（1）不正アクセス届出状況

3 月の届出件数は 19 件であり、そのうち何らかの被害のあった件数は 13 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 35 件（うち 10 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 8 件、DoS 攻撃 1 件、アドレス詐称が 1 件、その他（被害あり）3 件**でした。

侵入届出の被害は、他サイト攻撃の踏み台として悪用されたものが 4 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 5 件、などでした。

その他（被害あり）の被害として、ネットオークションで何者かによって本人になりすまされ不正利用されたものが 1 件、CSRF※の脆弱性を抱えるサイトにログイン中に、悪意ある URL をクリックしてしまい、会員制サイトに登録してあった氏名やメールアドレス情報が他人に送られてしまったものが 1 件、などがありました。

※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。
※CSRF（Cross-Site Request Forgeries）…ウェブサイトの脆弱性を利用した攻撃手法。会員制のサイトにログイン中に、悪意あるサイトに誘導された際、自分の意図しないリクエストを会員制サイト側に送られてしまうことなどを言う。例えば会員制の掲示板サイトに、自分の意図しない投稿がされたりするといった現象が発生する。

(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マシン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、ルートキット※や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。 ・**パスワードが破られたアカウントは、パスワードがユーザ名そのものであった**ため、推測が容易であった模様。 ・マシン担当者は、**当該マシンは外部からの SSH アクセスは出来ないものと認識していたが、実際は違っていた**。
解説・対策	パスワードを複雑にし、推測が容易でなくするのは言うまでもありません。しかし、今回の事象では、**アクセス制限に対するマシン担当者の思い違いが問題**となりました。外部からのアクセス制限については、システム管理者に再度確認するなどの対処が必要でしょう。 (参考) IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html

※ルートキット…攻撃者がコンピュータに侵入した後に利用するためのソフトウェアをまとめたパッケージのこと。一般的には、ログ改ざんツールやバックドアツール、改ざんされたシステムコマンド群などが含まれる。動作中のプロセスやファイル、システム情報などを不可視化し、これらツール群の存在がユーザに察知されないようになっていることが多い。

(ii) ウェブサイトのコンテンツが繰り返し改ざんされる

事例	・自分が管理するウェブサイトのコンテンツが、数時間おきに書き換えられる。そのページにアクセスすると、ウイルスが検知されたとの警告が出る。 ・ウェブサイトへのコンテンツファイル送信用の ftp アクセスのパスワードを何回変更しても状況は変わらない。
解説・対策	**パスワードを破られたことによる侵入ではなく、ウェブサイトの脆弱性を突かれたことが侵入や書き換えの原因**と思われます。今回の事象では、サイトで動作していたウェブアプリケーションに SQL インジェクション攻撃※を受けた際、そのアプリケーションに脆弱性があったため、コンテンツとして表示するために用意してあったデータベースのデータに、悪意あるサイトへのリンク情報が埋め込まれてしまったものと思われます。悪意あるサイトにアクセスすると、ウイルスがダウンロードされてしまう仕組みになっていました。**サイト管理者は、脆弱性の意味を理解した上で、脆弱性解消などの適切な対処を実施する必要があります**。 (参考) IPA - 知っていますか？脆弱性(ぜいじゃくせい) http://www.ipa.go.jp/security/vuln/vuln_contents/ IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html

※SQL インジェクション攻撃…データベースアクセスのために SQL(Structured Query Language)文を用いるプログラムにおいては、SQL 文を構成する際、プログラム中の式の値を SQL 文に埋め込む場合には、引用符で括られる文字列について、引用符が含まれているならばそれをエスケープ処理しなければならない。これを怠ると、正当なデータに対して SQL 文の実行がエラーとなる不具合が生じる。このバグが悪意ある者によって与えられ得る文字列を扱う箇所に存在すると、それはセキュリティ上のぜい弱性となる。攻撃者が悪意あるコマンドを与えると、データベースの内容を改ざんや情報を盗み出されるなどの被害が生じる。このような攻撃を SQL インジェクション攻撃と呼び、その原因箇所を同ぜい弱性と呼ぶ。

4．相談受付状況

3 月の相談総件数は **654 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 **157 件**(2 月：25 件)となり、最近 3 カ月の減少傾向から一転、急増しました。これは、昨年 11 月に業者が逮捕された後、ほとぼりが冷めて来たものと思われます。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 **9 件**(2 月：11 件)、**Winny に関連する相談**が **6 件**(2 月：9 件)などでした。

表 4-1　IPA で受け付けた全ての相談件数の推移

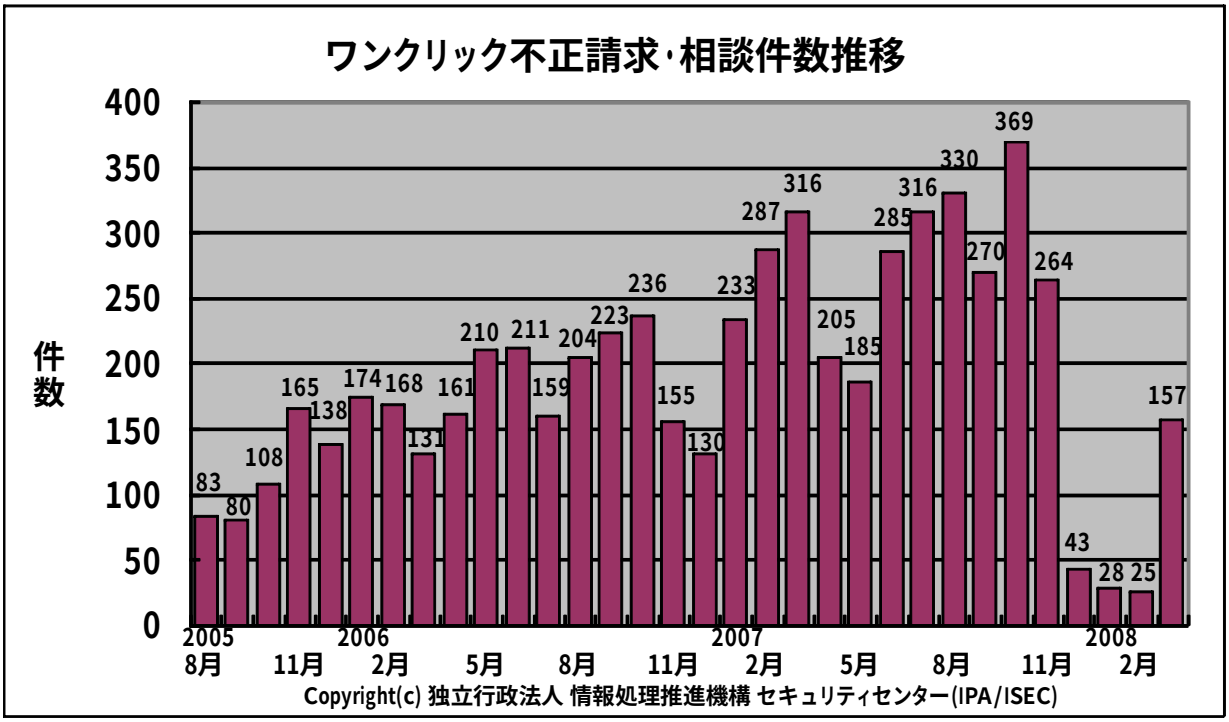
		10月	11月	12月	1月	2月	3月
合計		**1128**	**911**	**389**	**408**	**350**	**654**
	自動応答システム	669	520	222	219	192	373
	電話	397	337	109	151	110	214
	電子メール	57	52	56	38	47	66
	その他	5	2	2	0	1	1

※ 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。

表 4-2　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 を使っていてウイルス感染し、個人情報が流出した

相談	あるマンガ本のデータを Winny でダウンロードした。圧縮されていたファイルを解凍するといくつかのファイルが現れ、**順番にクリックして開いていったら、そのうちの一つがウイルスだったようだ。アイコンはフォルダの姿をしていた**。その後もしばらくインターネットに接続していた。その後調査したところ、**自分では Winny でアップロードしたファイルは無く設定も変えていないはずなのに、アップロードされていた個人情報入りファイルがいくつかあった**。それらのファイルは、自分で撮影したデジカメの写真やメールの送受信データであった。Winny はすぐ削除した。この時点で、情報の流出は止まったと考えてよいか。
回答	フォルダをクリックしたはずが実はウイルスだったという、アイコンの見た目を偽装したウイルスに引っ掛かってしまった典型的な例です。特に、映画・音楽・書籍をコピーしたような、**違法に流通しているデータと思わせるようなファイル名として流通しているファイル内に、ウイルスが含まれている傾向がありますので**、注意が必要です。 なお、Winny を削除したからといって、すぐに情報流出が止まる訳ではありません。一次流出元としての貴方のパソコンからは流出は止まりますが、**既に他のパソコンにダウンロードされてしまったファイルの流出は止めることが困難**です。 違法行為を止めるのはもちろんですが、**出所の不明なファイルを開いたら何が起こるか分からないという根本的な危険性を、改めて認識し直すべき**です。**安易にファイル共有ソフトを使うことは、厳として慎むべき**です。 （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) Linux のサーバがウイルス感染？

相談	Linux で構築したウェブサーバを外部に公開している。プロバイダから、「貴方のマシンはボットに感染している」と指摘され、接続を止められてしまった。ログを見たが、特に変わった様子は見受けられない。
回答	サーバに**侵入され、ボットを埋め込まれてしまった**ものと思われます。ボットネットワークを構成するマシンの一つとして悪用され、他のマシンを攻撃していたものと推測されます。最近では、**サーバの脆弱性を突かれて侵入されるケースが多く報告されています**。サーバ OS やウェブアプリケーションの脆弱性解消や、安全性向上のための各種設定などの対策をとる必要があります。 （ご参考） IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html

5．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、2008 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 **213,755 件**ありました。1 観測点で 1 日あたり **206** の発信元から **690 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、206 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。

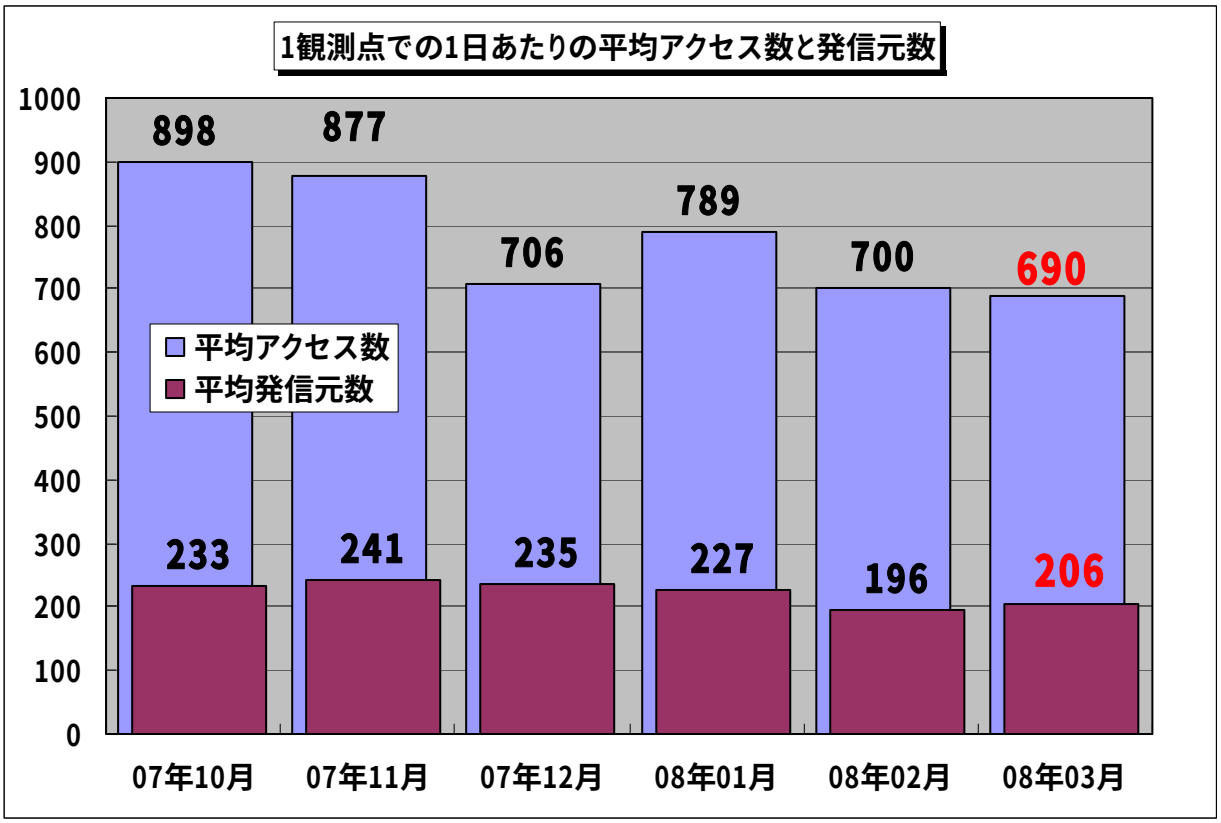


図 5-1：1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数

2007 年 10 月～2008 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 5-1 に示します。この図を見ると、3 月の期待しない（一方的な）アクセスは 2 月よりも減少しましたが、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 3 月のアクセス状況は、2 月よりも減少しました。これは、全体のアクセス数そのものが減少したためです。特に発信元地域が中華人民共和国からの、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、1026/udp、1027/udp へのアクセスや、発信元地域がカナダからの 1028/udp へのアクセスが、一定期間ですが減少しました。（図 5-2、5-3 参照）

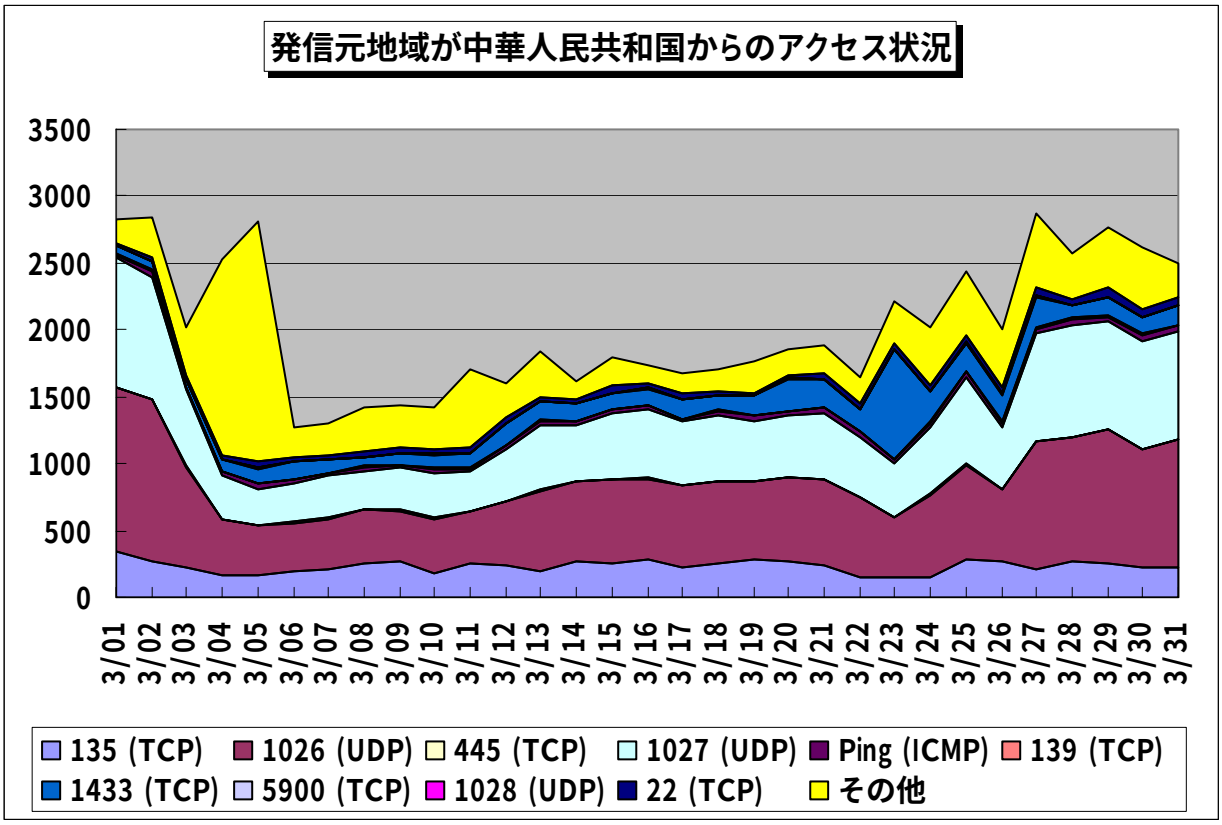


図 5-2: 2008 年 3 月　発信元地域が中華人民共和国からのアクセス状況

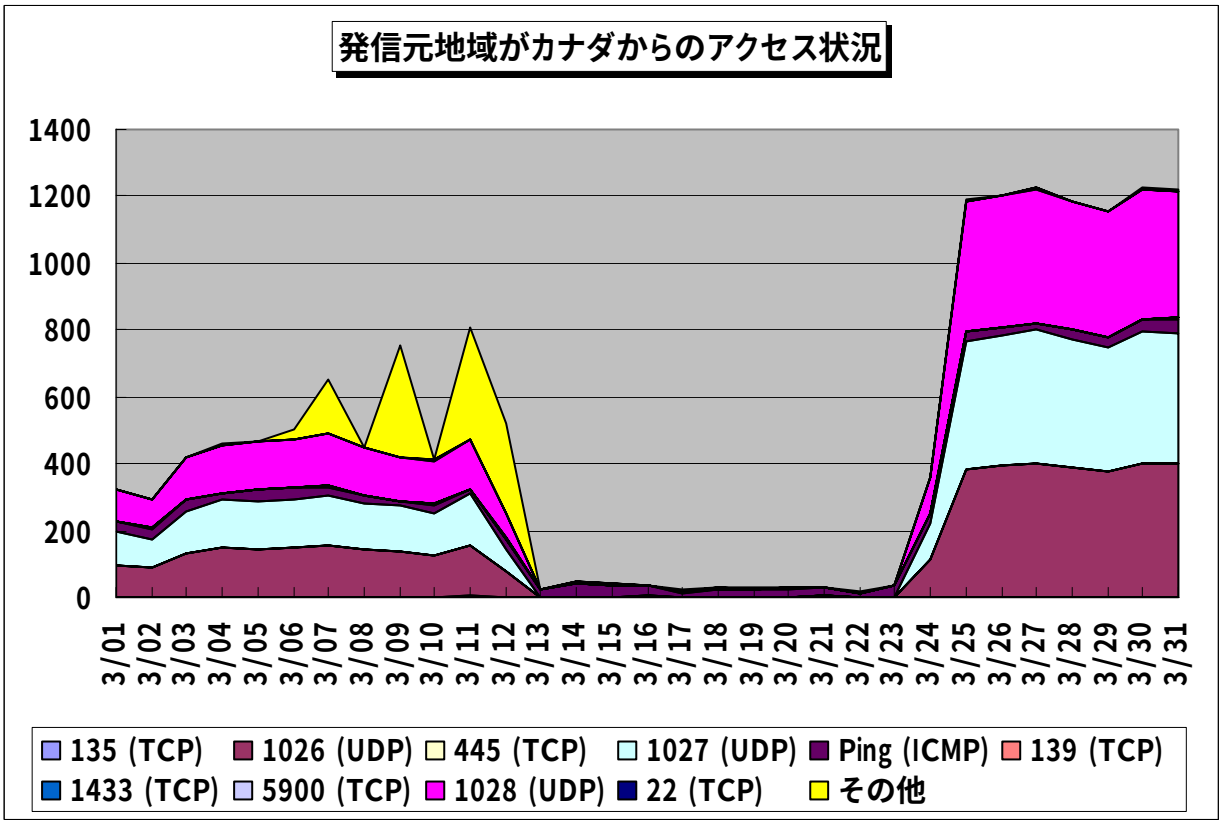


図 5-3: 2008 年 3 月　発信元地域がカナダからのアクセス状況

2 月の後半から増加していた、5900/tcp（コンピュータを遠隔操作するためのソフトウェア、Real VNCが使用するデフォルトのポート）へのアクセスは、3 月の始めまで増加しました（図 5-4 参照）。現在は落ち着いた感じには見えますが、引き続き注意が必要です。

（ご参考）

■ 2008 年 3 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/2008/documents/TALOT2-0803.pdf

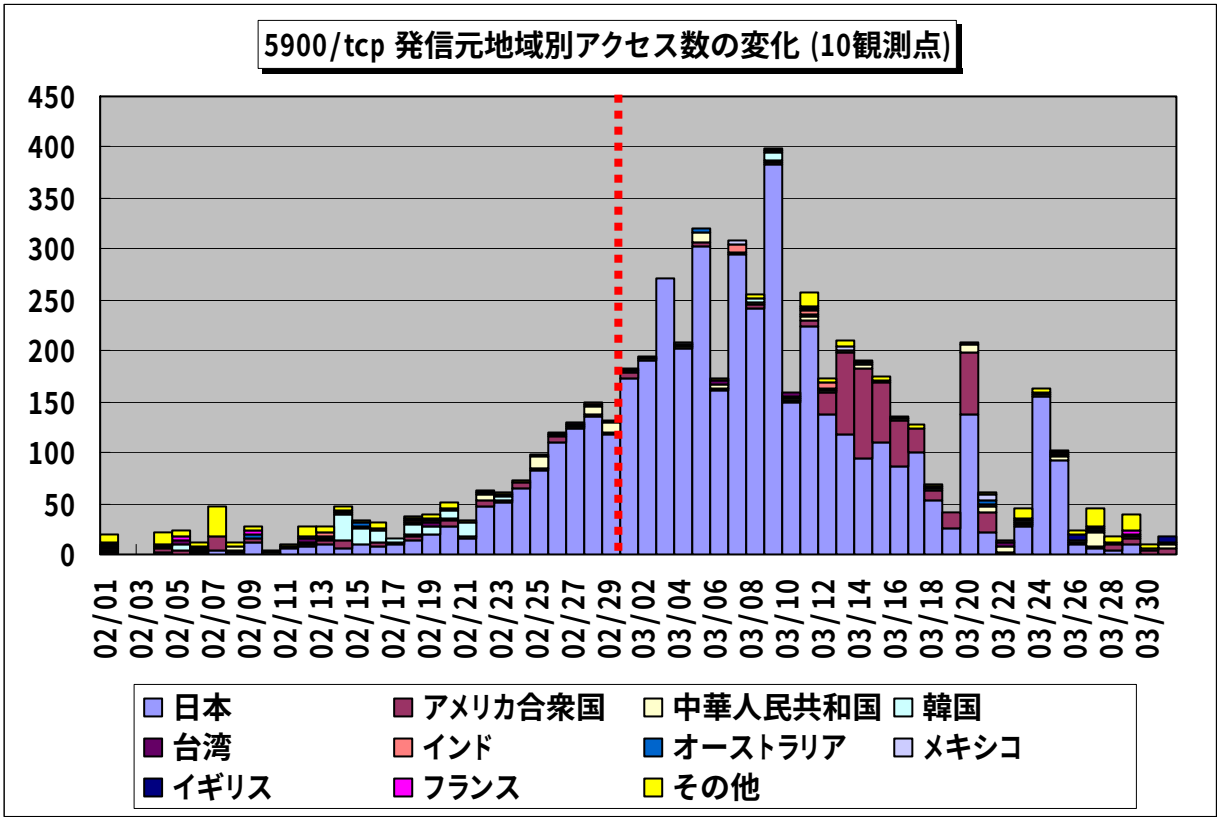


図 5-4: 2008 年 2 月～3 月　5900/tcp ポートへの発信元地域別アクセス数の変化

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/TALOT2-0804.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://jp.trendmicro.com/jp/home/
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／大浦
Tel:03-5978-7527 Fax:03-5978-7518 E-mail:isec-info@ipa.go.jp