IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
第 08-03-118 号
2008 年 3 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 2 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 2 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

「 いつも見ていたウェブサイトなのにウイルス検知？ 」
― ウェブサイトに仕掛けられたワナに注意！！ ―

「毎日見ている企業や個人のウェブサイトなのに、今日見たら突然、ウイルス対策ソフトがウイルスを発見した！」 といった相談事例が増えています。これは、当該のウェブサイトに脆弱性（ぜいじゃくせい）※があり、その脆弱性を利用した不正アクセスにより侵入され、ウイルスを感染させるように、ウェブページを改ざんされてしまうことが主な原因です。

※脆弱性 （Vulnerability）
情報セキュリティ分野においては、通常、システム・ネットワーク・アプリケーションまたは関連するプロトコルのセキュリティを損なうような、予定外の望まないイベントにつながる可能性がある弱点の存在や、設計もしくは実装のエラーのことを言います。セキュリティ上の設定が不備である状態を指す場合もあります。一般に、セキュリティホール（Security Hole）と呼ばれます。

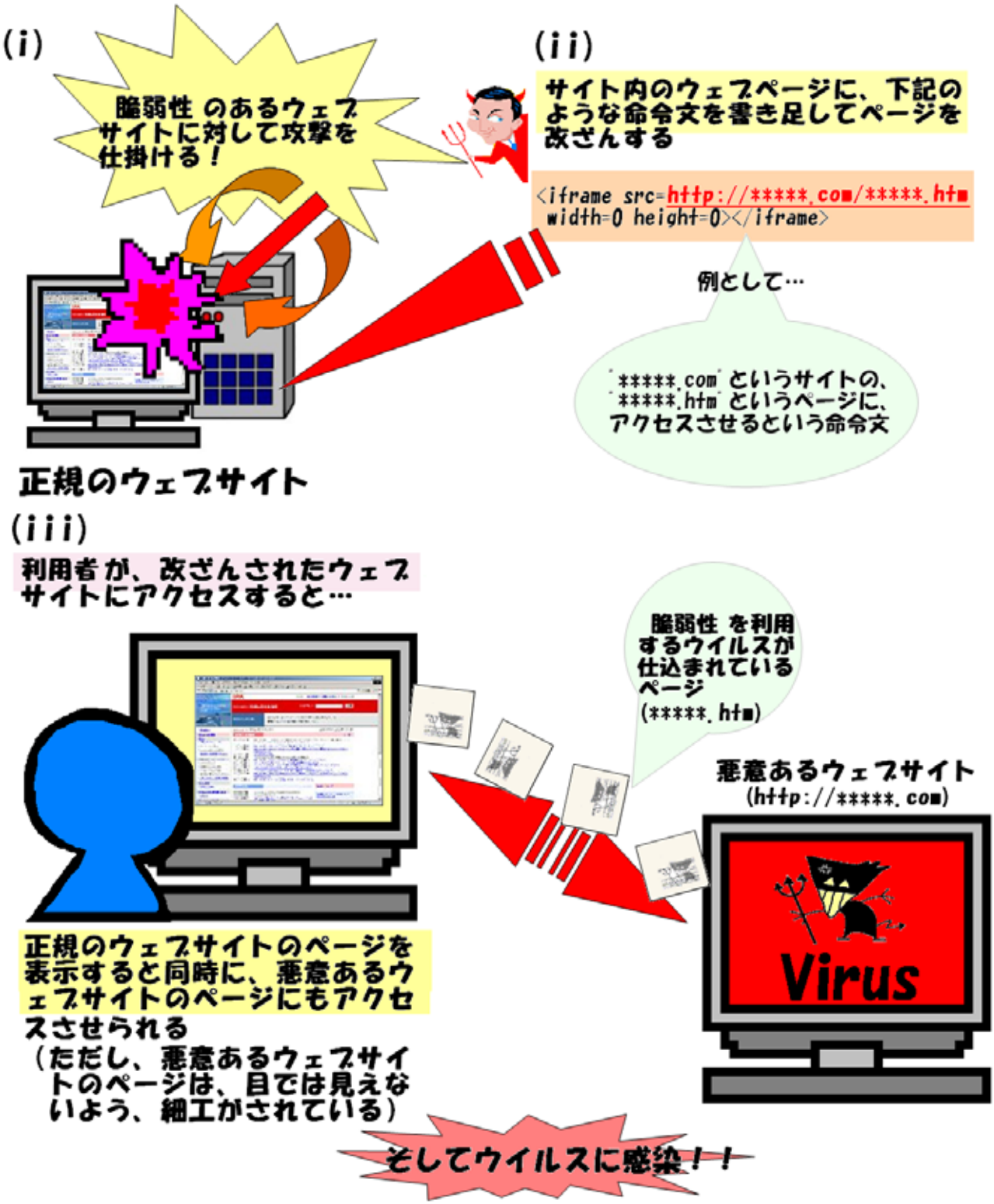
(1)脆弱性による感染の仕組み

攻撃者はどのような方法で、ウェブサイトの利用者にウイルスを感染させるのかを簡単に説明します。

(i)まず、攻撃者はインターネットを介して脆弱性のあるウェブサイトを探し出し、その脆弱性を利用してウェブページを改ざんします。

(ii)改ざんする内容としては、例えば、”利用者にはわからないように、ウイルスが仕込まれているウェブページにアクセスさせる”といった命令文を、当該ウェブページに埋め込みます。

(iii)利用者が、改ざんされたウェブサイトを見に行き、命令を埋め込まれたウェブページを表示します。その結果、命令文が実行されて、利用者にわからないようにウイルスが仕込まれたウェブページにもアクセスすることになり、利用者のパソコンがウイルスに感染させられてしまいます。このウイルスが仕込まれたウェブページは、画面上に表示されないように細工が施されているため、見た目には見えないようになっています。



(2)対策

ウェブサイトの利用者が、そのウェブサイトに脆弱性があるかどうかを確認することは困難であるため、上記のような被害を防止するにはウェブサイトの作成者や運営者が適切な対策を取ることが望まれます。

(i)ウェブサイト作成者

ウェブページは、それぞれのウェブサイトで独自に作成されている場合が多く、セキュリティをどこまで考慮しているかは、その作成者の能力に委ねられています。ウェブページに脆弱性が発見された場合、すでに運用を開始しているウェブページに対策を施すのは困難なことが多いため、作成段階から脆弱性を作らないための取り組みが必要となりますので、以下のサイトを参考にしてウェブサイトの作成を心がけてください。

(ご参考)
「安全なウェブサイトの作り方」
http://www.ipa.go.jp/security/vuln/websecurity.html
「セキュア・プログラミング講座」
http://www.ipa.go.jp/security/awareness/vendor/programmingv2/

(ii)ウェブサイトの運営者

ウェブサイトの運営者としては、以下の対策を実施することが必須項目として挙げられます。

(a)ウェブサイトのウェブページ(html※)や、ウェブサーバの基本ソフト(OS)、インストールされているアプリケーションソフトや、ネットワークサーバソフトなどを常に最新の状態にし、脆弱性を解消しておく。

(b)ウェブサイトのウェブページなどが改ざんされていないか、定期的にチェックする。(市販されている改ざん検知ツールの導入などをお勧めします)

(c)ウェブサイトを稼動させているサーバが、不正に侵入されないように管理する。

※ html → Hyper Text Markup Language の略。ウェブページを記述するための言語。

(ご参考)
「知っていますか？脆弱性(ぜいじゃくせい)―アニメで見るウェブサイトの脅威と仕組み―」
http://www.ipa.go.jp/security/vuln/vuln_contents/
「ウェブサイト運営者のための脆弱性対応ガイド」
http://www.ipa.go.jp/security/fy19/reports/vuln_handling/
「JVN iPedia 脆弱性対策情報データベース」
http://jvndb.jvn.jp/

(iii)利用者の対策

ウェブサイトの利用者は、被害に遭わないために以下の対策を必ず行ってください。

(a)パソコンの基本ソフト(OS)や、パソコンにインストールされているアプリケーションソフト(ワープロ、表計算、音楽再生、動画閲覧ソフトなど)を、常に最新の状態にし、脆弱性を解消しておく。

(b)ウイルス対策ソフトのウイルス定義ファイルを、最新の状態にして常に使用する。

(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

最近では、検索サイトから何らかのキーワードを入力して検索を行うと、その検索結果の上位サイトに、悪意あるサイトが紛れていることがあります。これは、検索サイトの検索機能を利用した手口で、SEO ポイズニング(Search Engine Optimization Poisoning)と呼ばれており、”検索結果の上位サイトはクリックしやすい”、”検索結果の上位サイトは安全なサイトだ”という、利用者の心理を突いてリンク先をクリックさせようとします。
検索サイト側でも、悪意あるサイトは表示しないように対策を施しておりますが、利用者の方もリンク先をクリックする前に、URL を確認するなどの注意が必要です。

リンク先を閲覧した際、少しでもおかしいと思ったら、すぐに戻るか、ページを閉じるなどをして、先に進まないようにしてください。

これは、正規サイトの脆弱性を利用して改ざんする手口と異なりますが、このようなことからでもウイルスに感染する可能性もありますので、手口として覚えておいてください。

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）
・昔 Winny を使っていたが‥
・パソコン初期化後に Winny を使っていたが‥

○ 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 を狙ったアクセスが増加中！

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 26 万個**と、1 月の約 31 万個から 16.6%の減少となりました。
また、2 月の届出件数(※2)は、**1,854 件**となり、1 月の 2,046 件から 9.4%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。
・2 月は、寄せられたウイルス検出数約 26 万個を集約した結果、1,854 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 24 万個 、2 位は W32/Mytob** で**約 5 千 6 百個、3 位は W32/Fujacks** で**約 4 千 5 百個でした。**

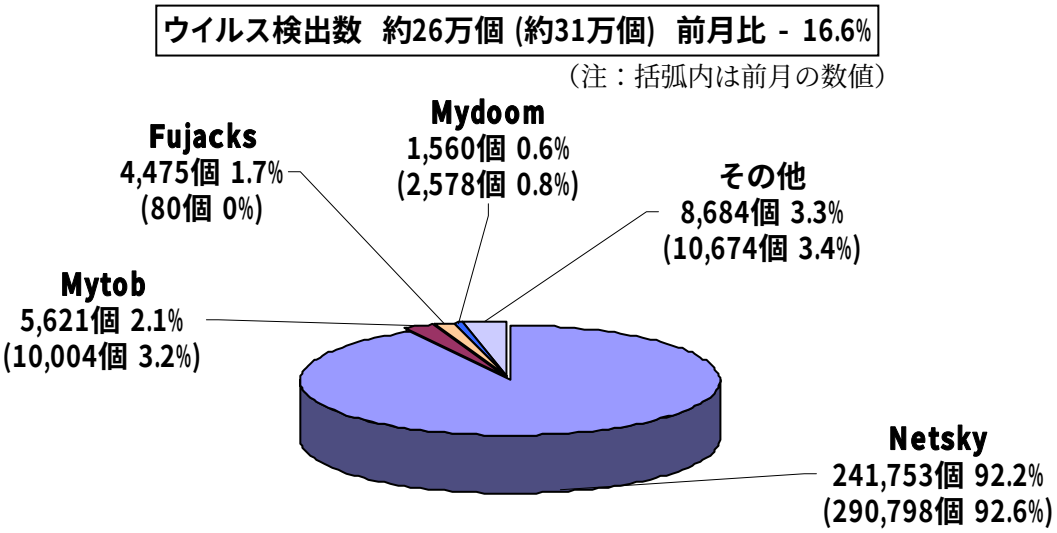


図 2-1

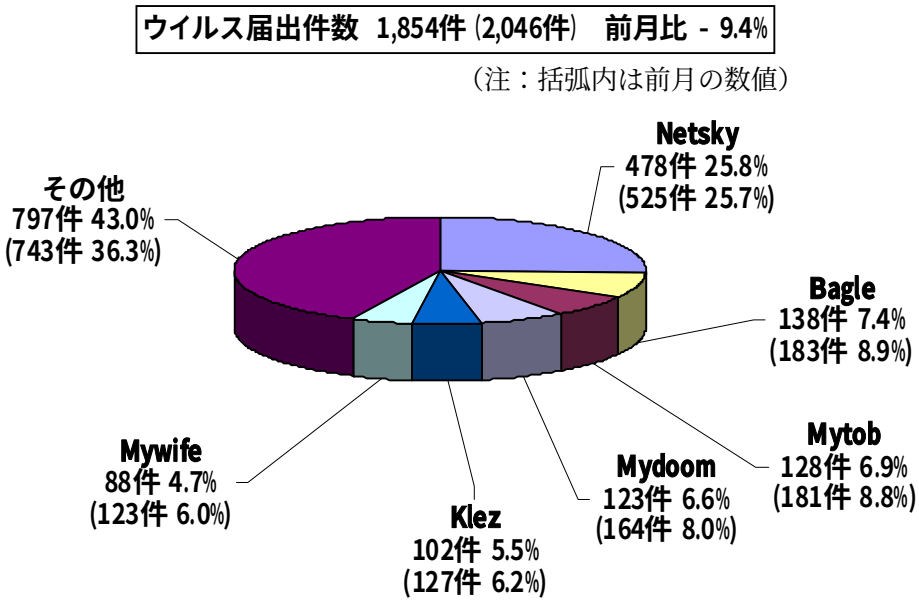


図 2-2

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

		9月	10月	11月	12月	1月	2月
届出(a) 計		10	10	15	14	8	4
	被害あり(b)	8	9	11	7	7	4
	被害なし(c)	2	1	4	7	1	0
相談(d) 計		27	37	31	21	24	29
	被害あり(e)	12	22	17	16	15	10
	被害なし(f)	15	15	14	5	9	19
合計(a+d)		37	47	46	35	32	33
	被害あり(b+e)	20	31	28	23	22	14
	被害なし(c+f)	17	16	18	12	10	19

（1）不正アクセス届出状況

2 月の届出件数は 4 件であり、それら全てが**被害のあった**ものでした。

（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 29 件であり、そのうち何らかの被害のあった件数は 10 件でした。

（3）被害状況

被害届出の内訳は、**侵入 1 件、DoS 攻撃 1 件、その他（被害あり）2 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マシンから、不正アクセスの事前調査とみられる通信がある」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、管理者権限を奪取されていたことが判明。 ・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。 ・当該サーバは**試験運用的な位置付けであり、本来やるべきセキュリティ設定や監視が手薄になっていた**ため、侵入に気付かなかった。
解説・対策	たとえ**試験運用であっても、インターネットに接続し外部からアクセス可能な状態にするのであれば、セキュリティ設定で手を抜いてはいけません**。 パスワード認証は、時間を掛けられればいつかは破られる、という原則を再認識しましょう。ログのチェック、接続許可制限などの対策が有効ですが、**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。 (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。 ・気が付くと、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無くなっていた。 ・記憶をたどると、ゲーム内のチャットで相手に提示された URL をクリックした後に、今回の現象が起きたような気がする。
解説・対策	URL をクリックした際、見るだけで**ウイルスを仕込まれてしまうようなウェブサイトに誘導されてしまった**と思われます。その**ウイルスが、オンラインゲームのログイン ID とパスワードを盗み取る機能を持っていた可能性があります**。 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

2 月の相談総件数は **350 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 **25 件**（1 月：28 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 **11 件**（1 月：10 件）、**Winny に関連する相談**が **9 件**（1 月：17 件）などでした。

IPA で受け付けた全ての相談件数の推移

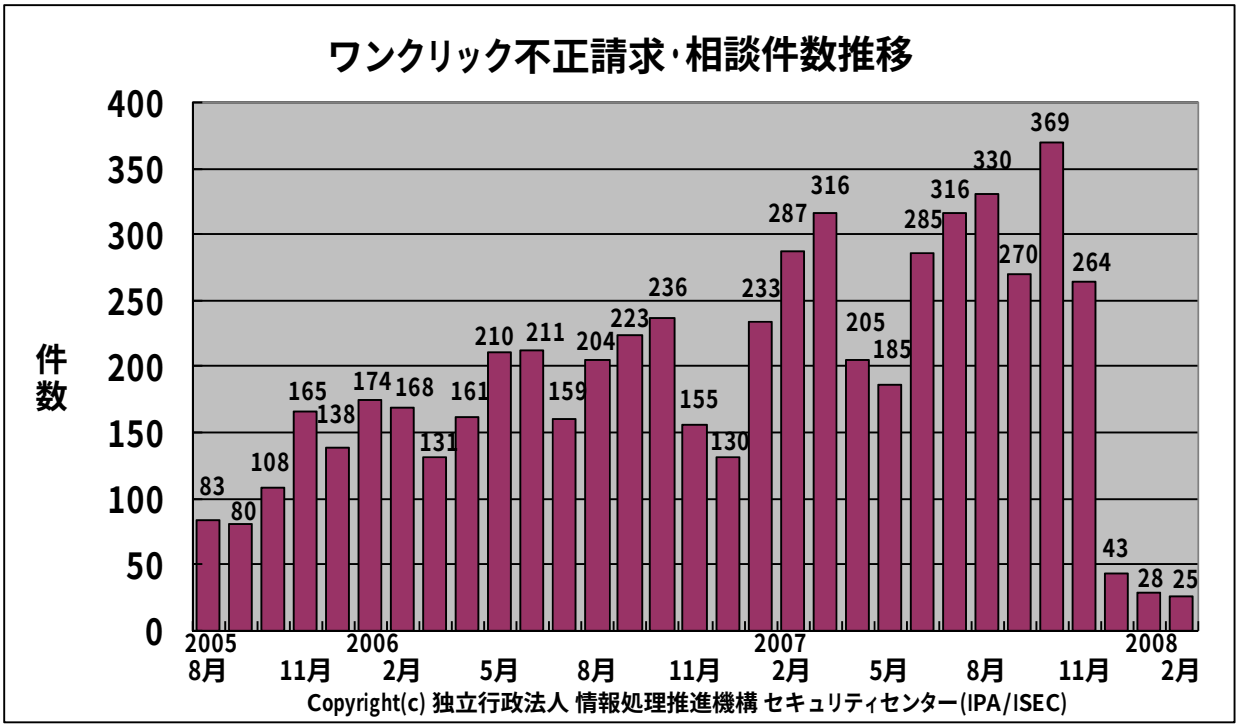
		9月	10月	11月	12月	1月	2月
合計		**910**	**1128**	**911**	**389**	**408**	**350**
	自動応答システム	544	669	520	222	219	192
	電話	310	397	337	109	151	110
	電子メール	55	57	52	56	38	47
	その他	1	5	2	2	0	1

※ 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。

（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) 昔 Winny を使っていたが・・

相談	何年か前まで Winny を使っていた。その時にダウンロードしたファイルが、ハードディスクに残っている。これらがウイルスに感染していることはあるのか。開いてもいいのか。
回答	Winny を始めとする**ファイル共有ソフトのネットワークに流通しているファイルは、そのほとんどが出所の不明なファイルであり、ウイルスである可能性が高い**と言えます。ウイルスの種類によっては、アイコンの見た目を偽装しているものもあるため、**見た目に騙されて不用意に開くとウイルス感染してしまう**場合もあります。 　なお、ウイルス対策ソフトでも検知できないウイルスも存在します。**出所不明なファイルは、ウイルスチェックするまでもなく、削除するのが賢明**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

(ii) パソコン初期化後に Winny を使っていたが・・

相談	以前、パソコンを初期化した後、Winny を使っていたことがある。ウイルスに感染する可能性はどのくらいあったのか。仮にウイルスに感染していた場合、パソコンを初期化する前にパソコン内にあったデータが流出することはあるのか。
回答	ファイルの種類を見分ける知識があれば、ウイルスに感染する可能性は、多少は減るでしょう。しかし、**ファイルを手当たり次第に開いていた場合は、ウイルスに感染していた可能性が高い**と言えます。 現在、Antinny のような暴露型ウイルスには、パソコンを初期化する以前のデータを復帰させてまで流出させてしまうような機能はありません。しかしながら、**“データ流出”ということに、少しでも不安があるのなら、Winny などのファイル共有ソフトは使うべきではありません**。何か問題が発生してからでは、取り返しがつきません。 （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

5．インターネット定点観測での２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 2 月の期待しない（一方的な）アクセスの総数は、10 観測点で **189,006 件**ありました。1 観測点で 1 日あたり **196** の発信元から **700 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、196 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。

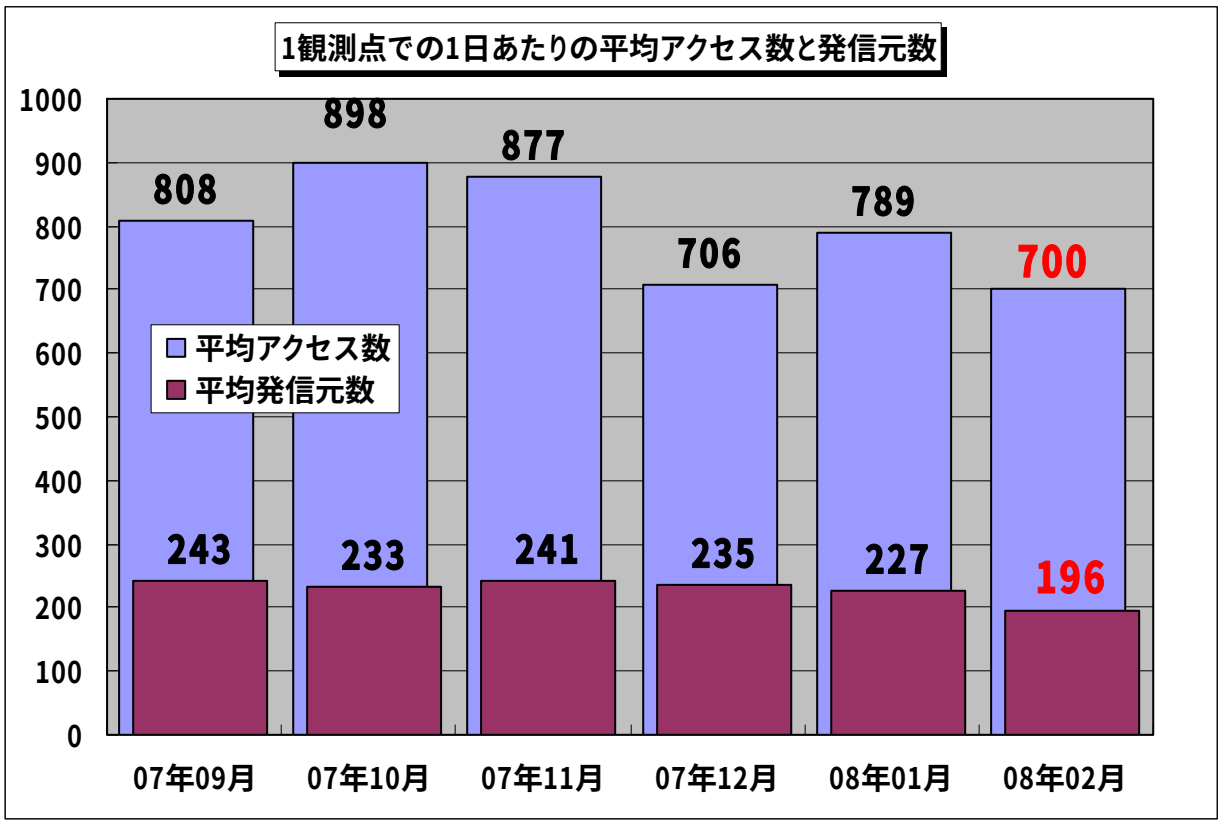


図 5-1：１観測点での１日あたりの期待しない(一方的な)アクセス数および発信元数

2007 年 9 月～2008 年 2 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、2 月の期待しない（一方的な）アクセスは 1 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 2 月のアクセス状況は、1 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。ただ、Windows の脆弱性を狙った、135/tcp、445/tcp へのアクセスや、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 へのアクセスは 1 月と同じ水準で観測されました。

※ 2 月 2 日～3 日は、TALOT2 のシステムメンテナンスのため、観測データがありません。今月の報告書は、この 2 日間を除外して統計情報を作成している事をご了承下さい。

（1）5900/tcp を狙ったアクセス

2 月の後半には、5900/tcp へのアクセスが増加しました。これは、RealVNC クライアントが RealVNC サーバへ接続するときに使用するデフォルトのポートです。発信地域元のほとんどは、日本からでした。（図 5-2 参照）

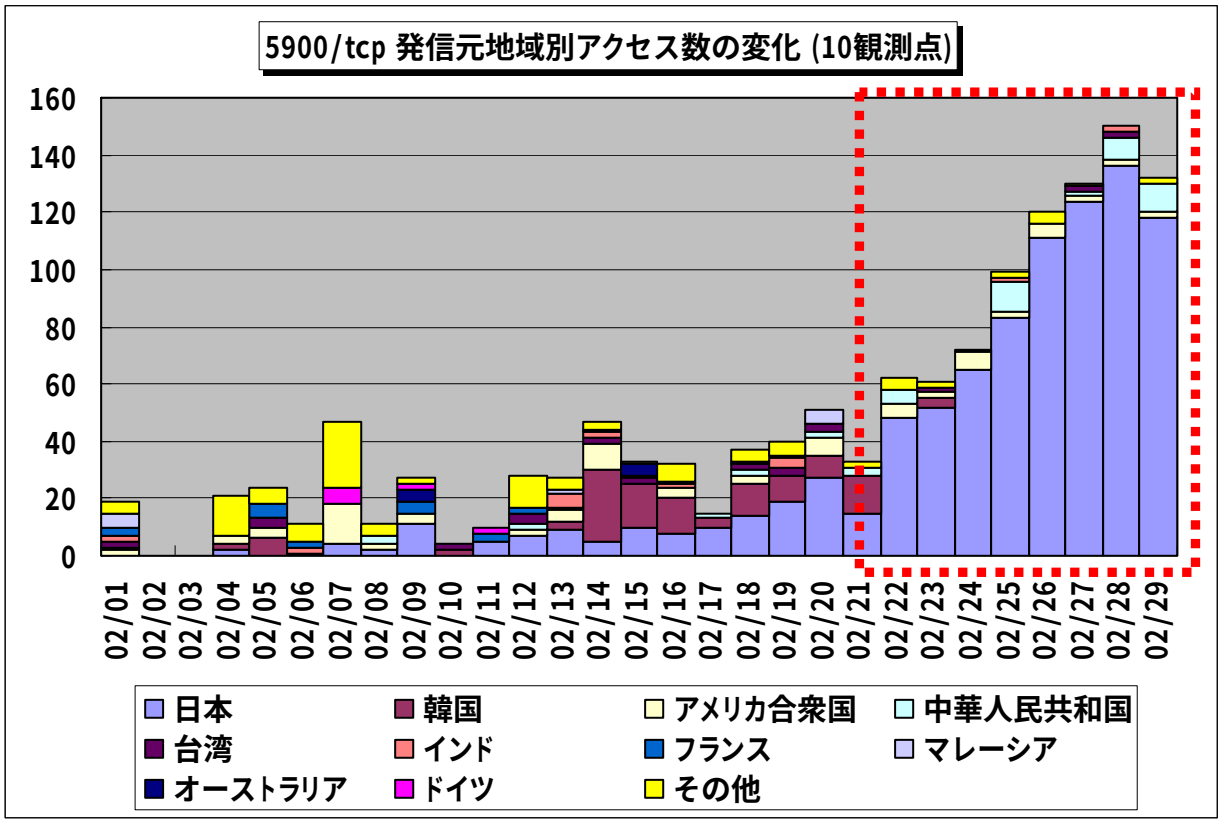


図 5-2：5900/tcp ポートへの発信元地域別アクセス数の変化

RealVNC は、リモートのコンピュータを遠隔操作するためのソフトウェアですが、2006 年 5 月に、”認証なしに端末にリモートアクセスできてしまう脆弱性”が公開されています。対策は、バージョンアップです。

（参考情報）

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

この脆弱性情報の公開の後、RealVNC に関する新しい脆弱性情報は特に公開されていませんが、攻撃者からみれば、リモートアクセスサービスは不正アクセスの足がかりとして有効なものです。

観測では、5900/tcp へのアクセスと同時に Windows の脆弱性を狙った 135/tcp、445/tcp も同時にアクセスするものも多く見受けられます。このことから、これらの不正アクセスは、ツールによって攻撃されている可能性が高く、広範囲に攻撃を行う可能性も考えられます。

RealVNC などのリモートアクセスツールをお使いの方は、配布元などの情報を確認し、お使いのツールが最新のものであるか確認することをお勧めします。

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/TALOT2-0803.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