INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
第 08-08-123 号
2008 年 5 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 4 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 4 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

「 公的機関になりすましたメールに注意してください！！ 」

最近、官邸や警察機関などから発信されたと見せ掛けたメールが出回っていることが報告されています。また、2008 年 4 月に、IPA の名を騙（かた）って、特定の組織にメールの添付ファイルとしてウイルスを送りつける事例が表面化しました。

これらは、いずれもメールを送りつけた相手に何とか添付ファイルを開かせようとするために、公的機関を装ったものです。たとえ、送信元メールアドレスに「.go.jp」があったとしても注意が必要です。

今回確認された事例は、特定の組織を狙ってメールを送りつける「標的型攻撃」と呼ばれるものです。この攻撃で利用された手法を理解するとともに、後述する対策の実施をお願いします。

(1)今回の標的型攻撃の手法

今回の攻撃に用いられた手法について、2008 年 4 月に表面化した IPA の事例により説明します。

これは、2008 年 2 月 26 日に IPA の脆弱性対策情報データベースに掲載された PDF 文書ファイル作成、閲覧ソフト(以下「PDF ソフト」という)の脆弱性(http://jvndb.jvn.jp/contents/ja/2008/JVNDB-2008-001090.html)を悪用して、利用者がメールに添付されていた PDF ファイルを Windows 版の PDF ソフトで開くと同時にウイルスが実行されるようになっていました。

図の 1-1 に、添付されていた PDF ファイルの構造を示します。

利用者が Windows 上で、この PDF ファイルを利用しようと開こうとすると、パソコン内の PDF ソフトが実行されて、まず(a)の部分が PDF 文書として認識されます。

この PDF 文書は一見すると普通の PDF 文書であり、内容も既存の資料を使用するなどしていますので、利用者は気づきにくくなっています。

ところが、(a)の PDF 文書には JavaScript（簡易的なプログラム）を利用した悪意のあるプログラムが仕組まれています。

PDF ソフトに脆弱性があると、(a)の PDF 文書を表示すると同時に、裏で脆弱性を利用して悪意のあるプログラムが実行されてしま

図 1-1 添付された PDF ファイルの構造

い、(b)のプログラムが利用者のパソコン内に作成されます。
次にパソコン内に作成された(b)のプログラムが実行されることにより、(c)ウイルス本体、(d)ウイルス感染後に利用する PDF 文書を利用者のパソコン内にコピーして、これらを実行することによりウイルスに感染することになります。
このウイルスは、以下のような特徴を持っています。

(i) WindowsNT、2000、XP、2003 Server、Vista(32 ビット)のみの OS(オペレーティングシステム)で実行されます。
ただし、今回の PDF ソフトで見つかった脆弱性は、Windows だけでなく、Macintosh、Solaris、Linux にも影響が及びますので、念のため Windows 以外の OS の利用者の方も、脆弱性の修正を行うことが望まれます。

(ii)ウイルスが実行されると Windows の標準のプログラムと同じように登録されるため、Windows の OS を起動するたびにウイルスが実行されます。

(iii)実行されたウイルスは、攻撃者が用意したインターネット上のサーバにアクセスして、そのサーバに利用者のパソコン名、OS のバージョン、IP アドレスなどの情報を送信します。
また、このサーバから利用者のパソコン対して、以下のような命令を出すことが可能となり、ウイルス感染してしまったパソコンでは、様々な被害が想定できます。

・パソコン内のドライブ、フォルダ、ファイルの一覧の送信
・任意のファイルの送受信、変更、削除
・パソコンでのコマンドの実行とその出力結果の送信
・プログラムの実行　等

また、本来(d)の PDF 文書は、ウイルス感染のためには必要ないものです。しかし、ウイルス感染と同時にこの PDF 文書を表示することにより、利用者がウイルスに感染したことに気付きにくくなってしまいます。

(2)対策

「標的型攻撃」は、攻撃対象を特定の組織、人などに限定しており、しかも巧妙に細工されたりしているため、簡単には表面化しない攻撃です。
「標的型攻撃」と疑われるメールが届いた場合は、不用意に添付ファイルを開くことはせず、当該機関に、本物のメールかどうかを問い合わせましょう。
また、以下のような対策を実施することにより相当数の被害を防止することができます。

(i)一般のパソコン利用者
一般のパソコン利用者の方は、標的型攻撃を受ける可能性は低いですが、万が一のため以下のような対策を実施することをお勧めします。

(a)基本的な対策
OS、アプリケーション、ウイルス対策ソフトを常に最新の状態に更新して、脆弱性を可能な限りなくす。

(b)銀行、カード会社、有料会員サイト等と偽ったメールとして利用者に届く可能性が考えられますので、疑わしいメールを受け取った場合には、送信元の会社に連絡し、届いたメールの内容を確認するなどして、安易に本文中の URL をクリックしたり、添付されているファイルを開いたりしないように注意して下さい。

(c)メールに添付されているファイルが、実行可能プログラム以外のファイル（例えばオフィスソフトの文書、PDF ファイル、映像・音声ファイルなど）であっても、とにかく自分には思い当たらない、関係がないなどのメールは決して開かないことです。

(ii)企業などのシステム管理者向け

(a)基本的な対策

OS、アプリケーション、ウイルス対策ソフトを常に最新の状態に更新して、脆弱性を可能な限りなくす。

(b)エラーで戻って来るメールのチェック

今回の標的型攻撃は、偽装された送信元のメールアドレス宛にエラーメールが返信されて来たことがきっかけとなって発見されました。返信されて来るエラーメールの中には、今回のように標的型攻撃の対象となった痕跡を見つけられることがあります。

(c)企業内ネットワーク環境の見直し

IPA が実施した「近年の標的型攻撃に関する調査研究報告書」(http://www.ipa.go.jp/security/fy19/reports/sequential/)」において、感染後のウイルスがHTTP、HTTPSの通信を利用している場合が報告されていますので、以下のような対策を実施することでウイルスの動作を未然に防ぐことが出来ます。

・不必要な外向きの TCP ポートを全て閉じます。

・TCP80番、443番において、それぞれHTTP、HTTPS以外の通信を検知したら通信を遮断します。または、HTTP(TCP80番)、HTTPS(TCP443番)においては、プロキシサーバ経由でのみ外部との接続を許可します。

もし、標的型攻撃を受けていることが判明した場合には、システム管理者は「対策方法」を企業内利用者へ周知徹底させるとともに、企業外からの問合わせに対応するための窓口を設置する等の対策を迅速に行って下さい。

(ご参考)

「Adobe Reader と Acrobat 8 のセキュリティアップデート公開」
http://www.adobe.com/jp/support/security/advisories/apsa08-01.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
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

・オンラインゲームサイト内で知り合った人に騙された？

○ 相談の主な事例 （相談受付状況及び相談事例の詳細は、7 頁の「4.相談受付状況」を参照）

・自社で出していないはずのメールが、宛先不明で戻って来る

・懸賞サイトで応募したら迷惑メールが？

○ 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。
・ゴールデンウィーク中の 135/tcp、445/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 21 万個**と、3 月の約 21 万個から同水準での推移となりました。
また、4 月の届出件数(※2)は、**1,703 件**となり、3 月の 1,651 件から 3.1%の増加となりました。

※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。
・4 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、1,703 件の届出件数となっています。

検出数の1位は、**W32/Netsky** で**約 19 万個 、2 位は W32/Mytob** で**約 5 千 3 百個、3 位は W32/Mimail** で**約 1 千 4 百個でした。**

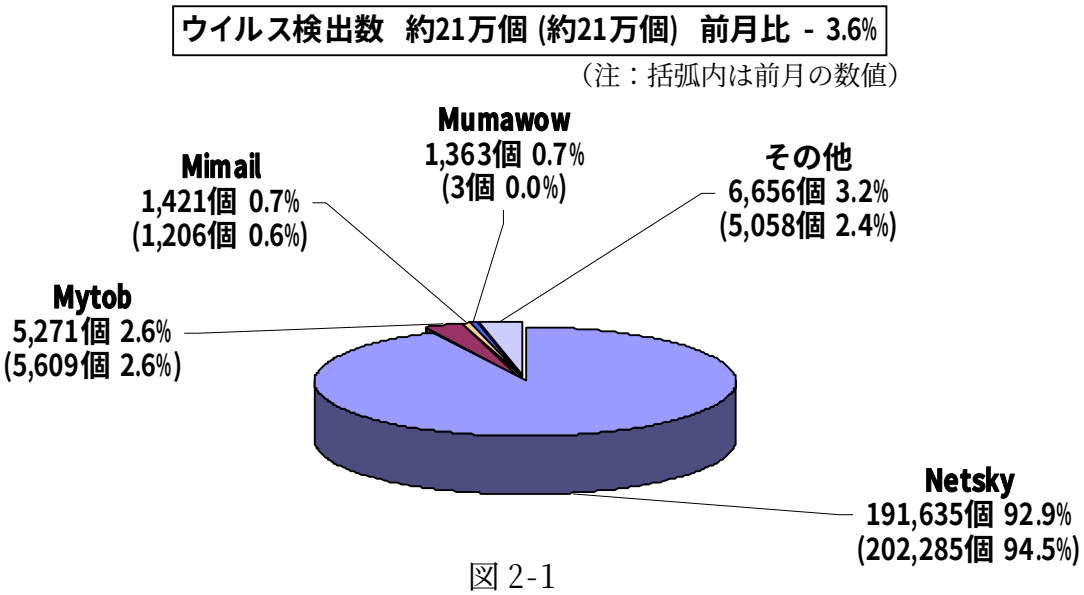

図 2-1

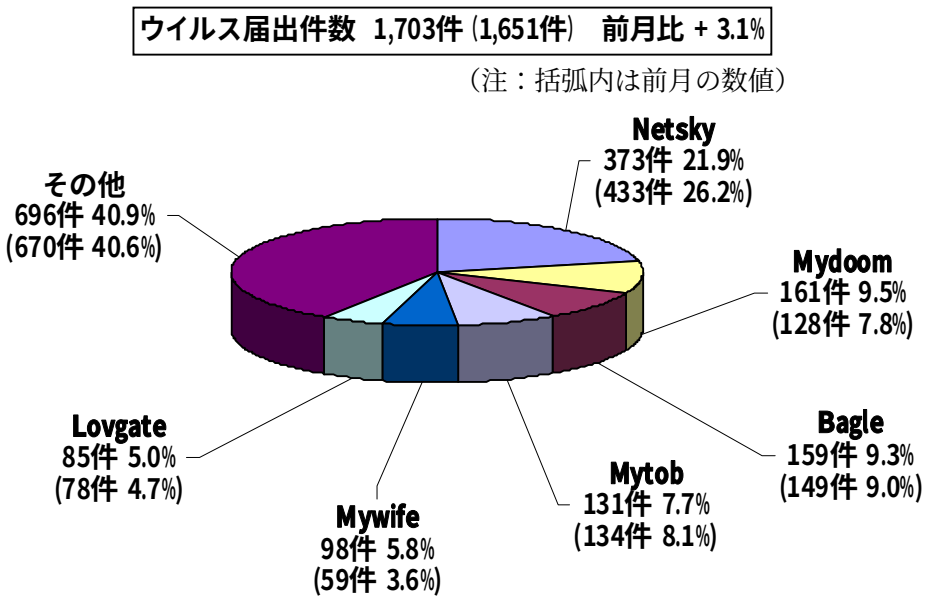

図 2-2

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－

表 3-1　不正アクセスの届出および相談の受付状況

		11月	12月	1月	2月	3月	4月
届出(a) 計		**15**	**14**	**8**	**4**	**19**	**14**
	被害あり(b)	11	7	7	4	13	10
	被害なし(c)	4	7	1	0	6	4
相談(d) 計		**31**	**21**	**24**	**29**	**35**	**56**
	被害あり(e)	17	16	15	10	15	31
	被害なし(f)	14	5	9	19	20	25
合計(a+d)		**46**	**35**	**32**	**33**	**54**	**70**
	被害あり(b+e)	28	23	22	14	28	41
	被害なし(c+f)	18	12	10	19	26	29

（1）不正アクセス届出状況

4 月の届出件数は 14 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。

（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 56 件（うち 6 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 31 件でした。

（3）被害状況

被害届出の内訳は、**侵入 3 件、アドレス詐称が 3 件、その他（被害あり）4 件**でした。

侵入届出の被害は、SQL インジェクション攻撃を受けクレジットカード情報などが漏れてしまったものが 1 件、他サイト攻撃の踏み台として悪用されたものが 2 件でした。侵入の原因は、ウェブアプリケーションの脆弱性によるものが 1 件、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 件でした。

その他（被害あり）の被害として、オンラインゲームサイトに本人になりすまして何者かにログインされ、ゲーム内で使うアイテムなどが奪取されたものが 2 件、何らかの方法でウイルスなどを埋め込まれ、外部サイト攻撃の踏み台として使われていたものが 2 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	・ファイアウォールのログをチェックしたところ、自組織で運用しているサーバから外部に向けて不審なアクセスがあることを発見。 ・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。 ・管理者アカウントのパスワードが変更され、外部サイト攻撃のためのツールが埋め込まれた上、**一部のシステムコマンドが悪意のあるものに置き換えられていた**。ファイアウォールのログにあったのは、**外部サイト攻撃ツールによる通信**と思われる。 ・**新規構築中のサーバであり、油断してパスワードを推測容易なものにしてしまった**ことが、原因と思われた。 ・IDS (侵入検知装置) を導入していたため発見が早く、被害を最小限に抑えることができた。
解説・対策	外部からアクセス可能な経路のパスワードは、たとえ暫定的な処置だとしても本運用と同等の扱いをすべきです。また、**システムコマンドが不正なものに置き換えられていますので、ルートキット※を埋め込まれている可能性が非常に高い**です。この場合、侵入・改ざんの影響範囲を正確に把握することが困難ですので、サーバは再構築することが基本となります。 (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 (rootkit) …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)オンラインゲームサイト内で知り合った人に騙された？

事例	・オンラインゲームサイト内で知り合った人と**チャット中、“便利なツールだから”とあるソフトをダウンロードするようしつこく勧められた**。結局、根負けし、ダウンロードしてインストールしてしまった。 ・**そのツールは実はウイルスだった**。ウイルスによって、ゲームサイトへのログインパスワードが盗まれてしまったようだ。 ・盗まれたパスワードを悪用され、自分が**ゲーム内で使っている登場人物のキャラクターデータが盗まれてしまっていた**。
解説・対策	言葉巧みに相手をだまし、必要なデータや情報を手に入れるという、**ソーシャルエンジニアリング**で被害に遭った例です。ネット上の交流では、顔見知りでもないのに油断しがちですので、注意しましょう。また、出所の分からないプログラムは、絶対にインストールしてはいけません。 (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

4 月の相談総件数は **938 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 **268 件**（3 月：157 件）となり、3 月からさらに増加しました。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 **2 件**（3 月：9 件）、**Winny に関連する相談**が **8 件**（3 月：6 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

	11月	12月	1月	2月	3月	4月
合計	**911**	**389**	**408**	**350**	**654**	**938**
自動応答システム	520	222	219	192	373	514
電話	337	109	151	110	214	335
電子メール	52	56	38	47	66	87
その他	2	2	0	1	1	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。

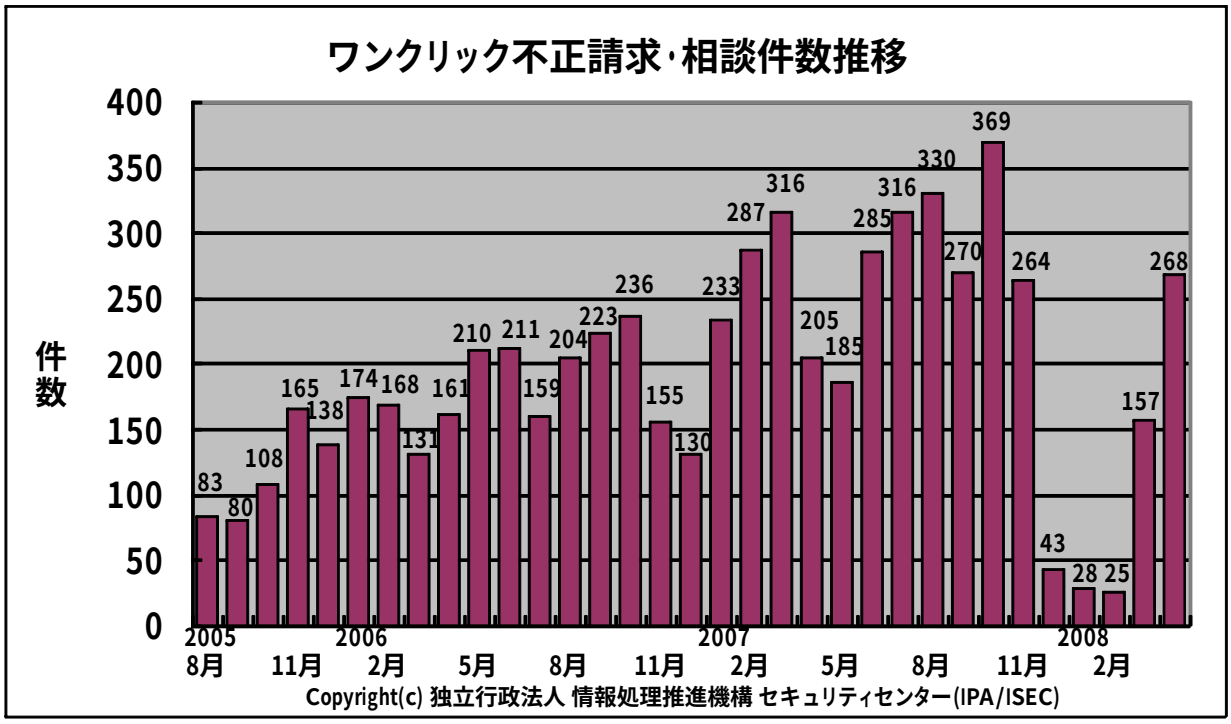

図 4-1　ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

(i) 自社で出していないはずのメールが、宛先不明で戻って来る

相談	宛先不明でエラーとなったメールが、数百通、会社のメールサーバに返送されて来る。エラーとなったメールの差出人には自社のアドレスが設定されていたが、実際には存在しないアカウントであった。メールサーバのログを見ても、自社から発信されたメールではないことが分かる。なぜこんなことが起こるのか。
回答	**メールの差出人欄は、簡単に偽装できてしまいます**。何者かが、貴方の会社のメールアドレスを差出人として偽装し、迷惑メールを送っていると予想されます。技術的にはメールの発信自体を止めることはできないため、根本的な対処は困難です。 **企業のアドレスが詐称された場合は、外部から苦情が寄せられる可能性もあります**。迷惑メールの発信源であると疑われないためにも、**運用管理的な対策として次の対策を取ることをお勧めします**。 ・**問い合わせ窓口を一本化する** ・**メールアドレスが詐称された旨を（ウェブ上等で）広報する** （ご参考） IPA - 「IP アドレス、メールアドレス等の詐称への対策」 http://www.ipa.go.jp/security/ciadr/cm01.html#spoofing

(ii) 懸賞サイトで応募したら迷惑メールが？

相談	懸賞サイトにアクセスし、プレゼントに応募した。その後、出会い系サイトから数十通の迷惑メールが届いた。止める方法は無いのか。
回答	技術的にはメールの発信自体を止めることはできません。**プロバイダやメールソフト、セキュリティ対策ソフトの迷惑メールフィルタ機能を利用**するのが、現実的な解となります。**恒久的対策としては、メールアドレスを変更する**ことになります。 悪質なサイトでは、表向きは懸賞サイトなのに、裏ではアドレスや個人情報を収集して他に転用している場合もあるようです。今後は、**信頼できるか分からない業者には、不用意にアドレスを教えない**ことが一番の予防策となります。どうしても相手にアドレスを教えなくてはならない場合は、念のため、変更もしくは削除しても良いアドレスを教えることをお勧めします。 （ご参考） 財団法人日本データ通信協会　迷惑メール相談センター http://www.dekyo.or.jp/soudan/

5．インターネット定点観測での 4 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 4 月の期待しない（一方的な）アクセスの総数は、10 観測点で **206,970 件**あり、且つ発信元の総数は 10 観測点で **77,804** ありました。1 観測点で 1 日あたり **259** 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、259 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。

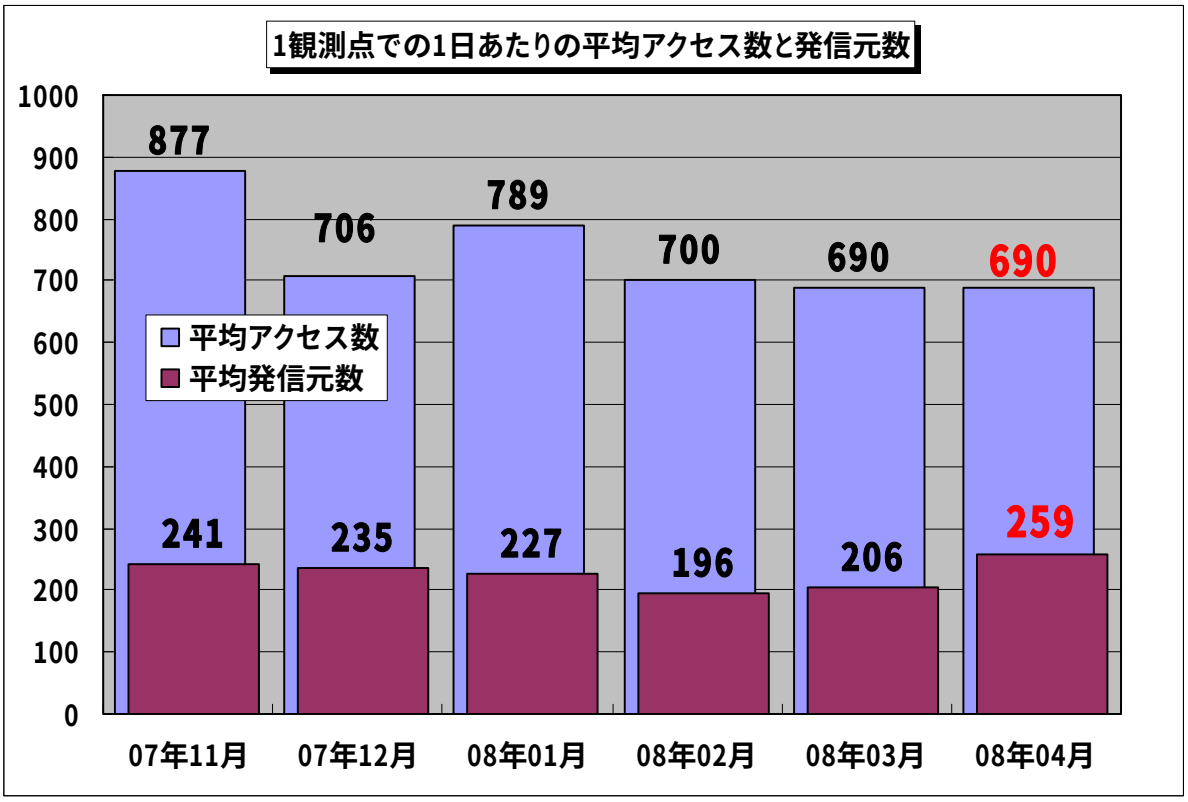

図 5-1：1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数

2007 年 11 月～2008 年 4 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、4 月の期待しない（一方的な）アクセスは 3 月とほぼ同水準であり、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。

4 月の後半辺りに 139/tcp ポートや、445/tcp ポートへのアクセスが一時的に多く見受けられました。これはゴールデンウィークに入り、自宅でパソコンを利用する人が増え、そのパソコンがボットに感染していた為にそこからのアクセスが一時的に増加した可能性が考えられます。

これらのポートは保護の甘いファイル（ネットワーク）共有や Windows の脆弱性を突いて狙われる可能性が高いポートです。

図 5-2、図 5-3 に 2008 年 4 月の 139/tcp、445/tcp ポートへの発信元地域別アクセス数の変化を示します。

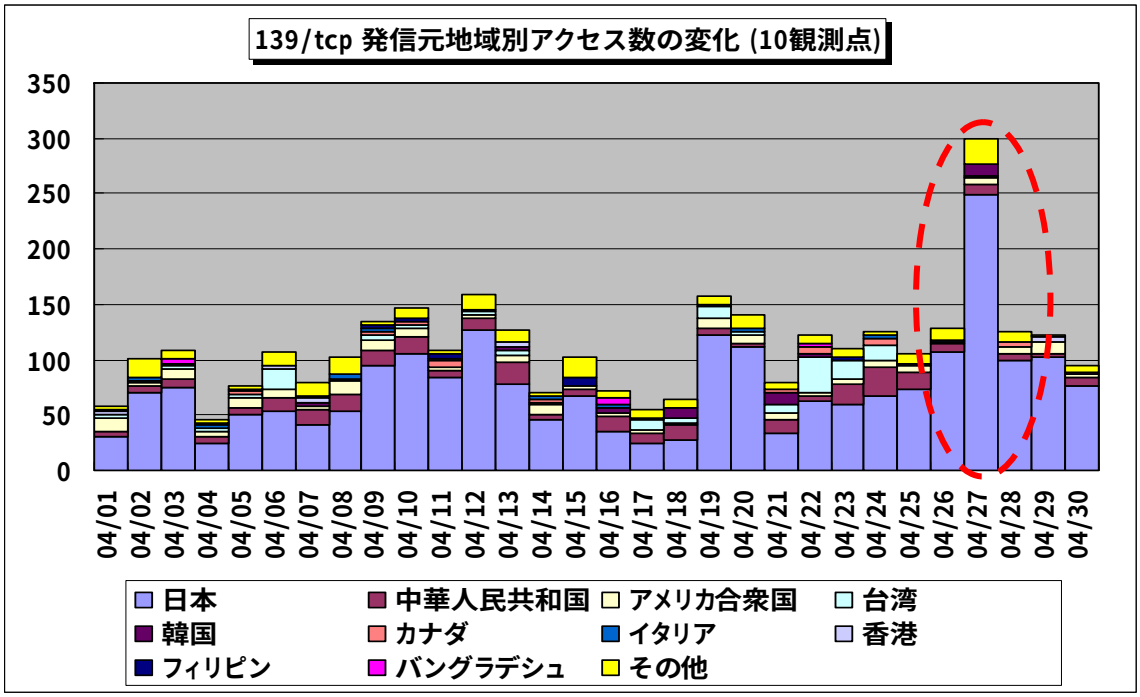

図 5-2: 139/tcp ポートへの発信元地域別アクセス数の変化

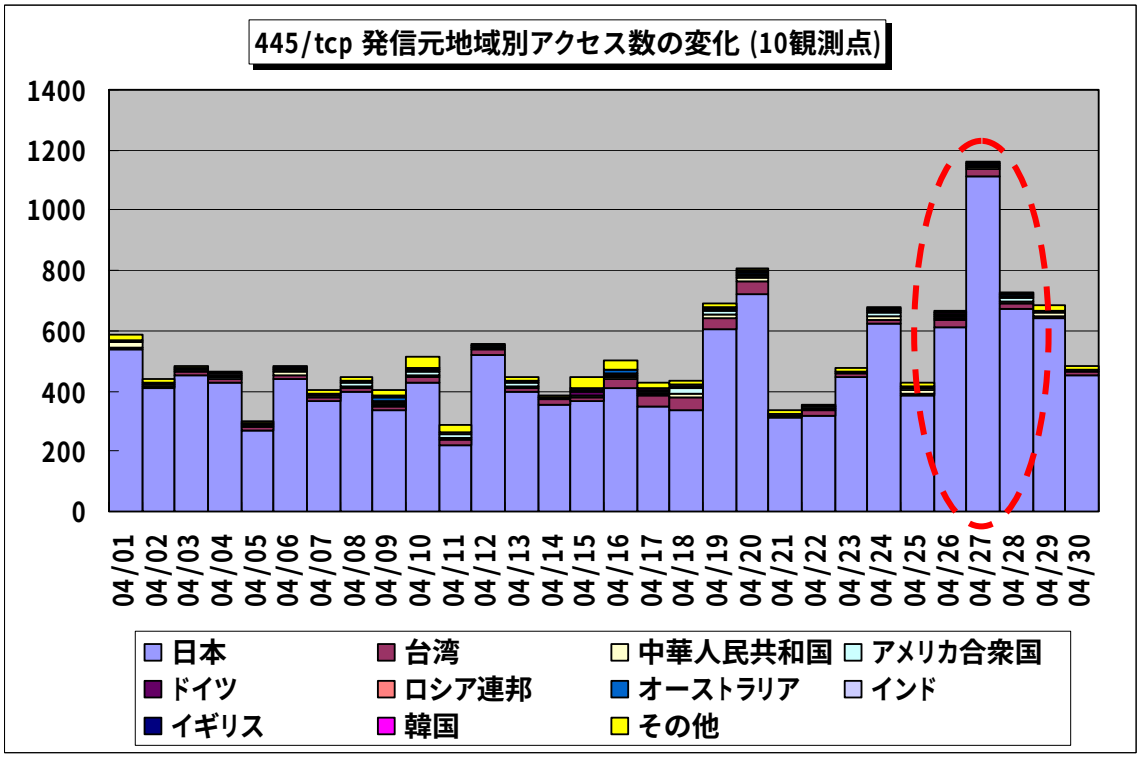

図 5-3: 445/tcp ポートへの発信元地域別アクセス数の変化

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/TALOT2-0805.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