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

1．一般のインターネット利用者の皆さんへ

2005 年 2 月より IPA/ISEC 発行のプレスリリースにおいて、IPA で実施しているインターネット定点観測の観測状況を、お知らせしています。

一般のインターネット利用者個人と同様な環境に観測点を持つインターネット定点観測(TALOT2)において、1 つの観測点でのインターネットからの期待しない(一方的な)アクセスは、1 日あたりに平均すると、2005 年 1 月：約 3,000 件, 2005 年 2 月：約 2,370 件でしたが、2005 年 3 月にも**約 2,100 件**のアクセスがありました。

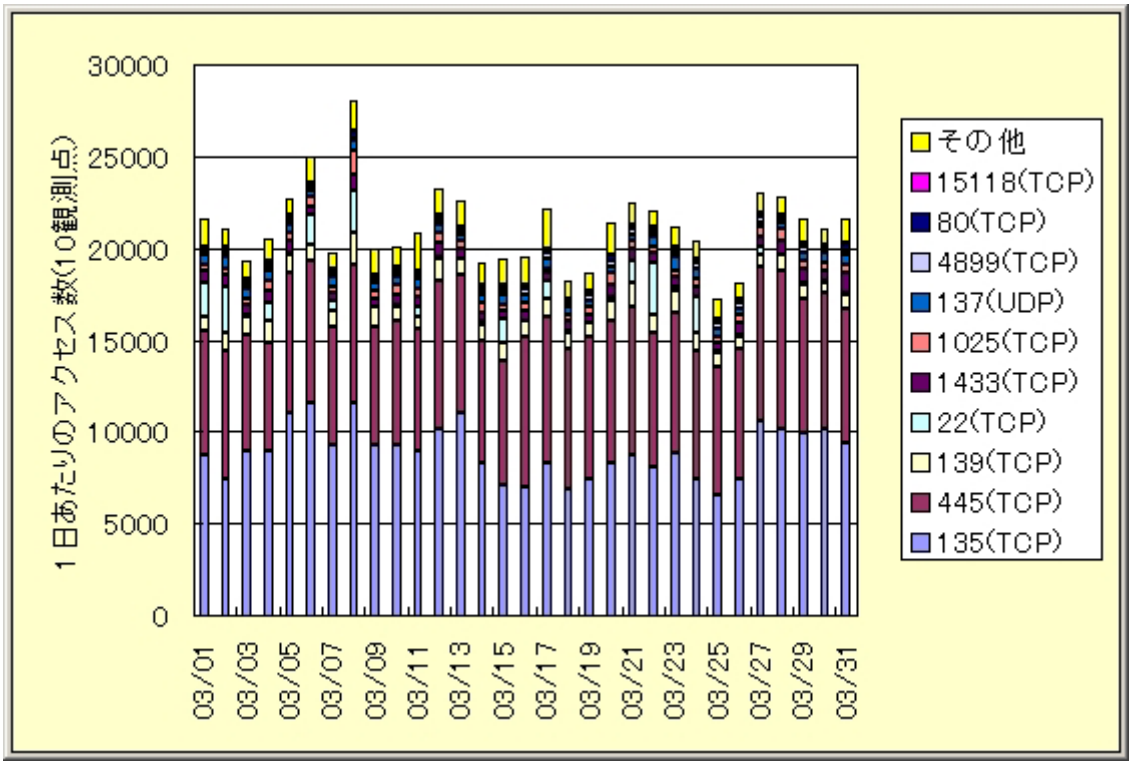
2005 年 2 月からみて、アクセス数については横ばい傾向となっており、インターネットからの脅威が改善された気配はありません。

2．3 月のアクセス状況

3 月の期待しない(一方的な)アクセスは、10 個の観測点の合計で **654,936 件**(Ping(ICMP)[(*1)]は除く)ありました。

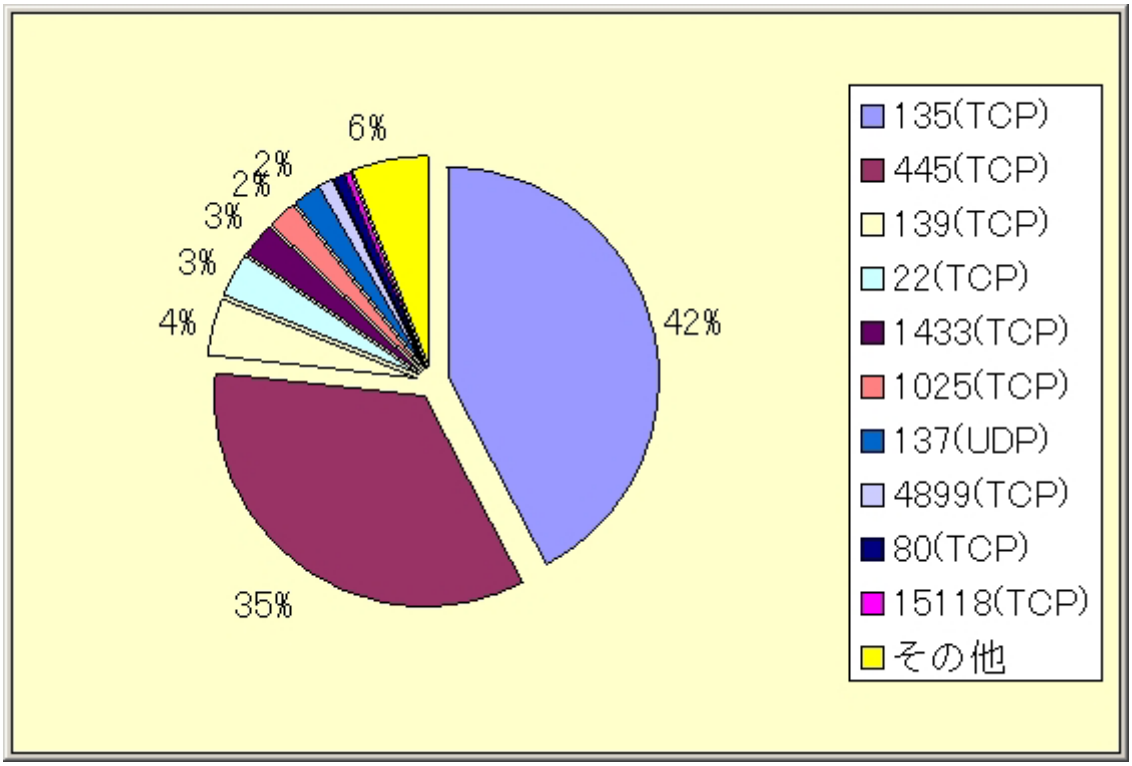
3 月は、**1 日あたりに平均すると、1 つの観測点(一般のインターネット利用者個人と同様な環境)で約 2,100 件のアクセスがあった計算になります。**

3/1 から 3/31 のアクセス状況(1 日あたりの 10 観測点へのアクセス数の変化)について図 2.1 に、種類別アクセス数の比率について図 2.2 に、さらに 1/1 から 3/31 のアクセス状況を図 2.3 に示します。

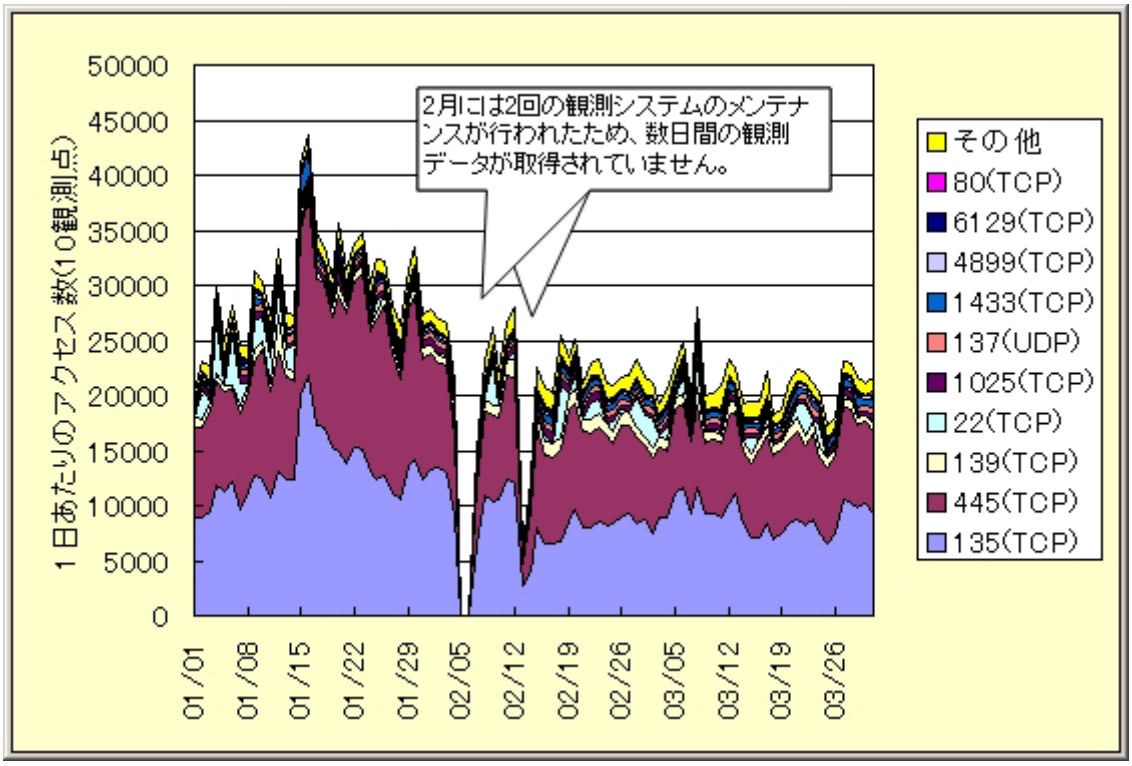


【図 2.1 2005 年 3 月の一方的なアクセス状況】

3月も1月～2月と同じように、ボット系と呼ばれるワーム[*2] (トロイの木馬[*3])が猛威を振るっており、グラフに示された 22(TCP)を除くほとんどのポート[*4]に対するアクセスは、このボット系のアクセスと思われます。

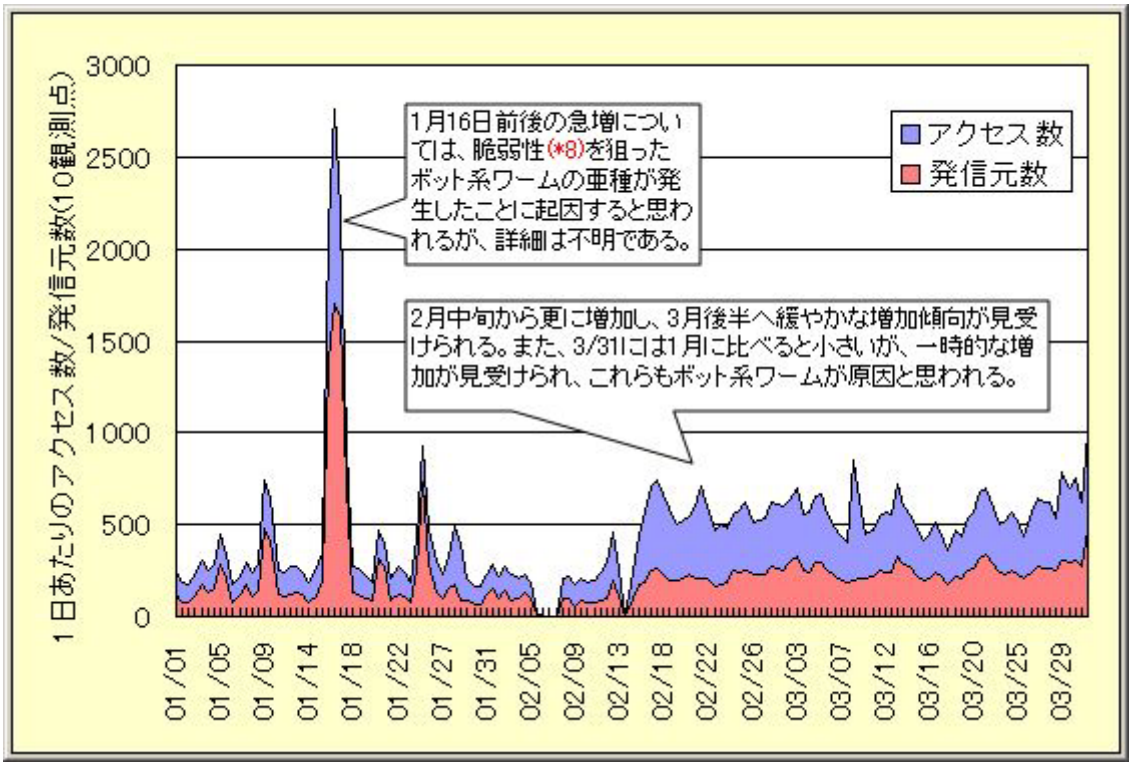


【図 2.2 2005 年 3 月の宛先(ポート種類)別アクセス数の比率】

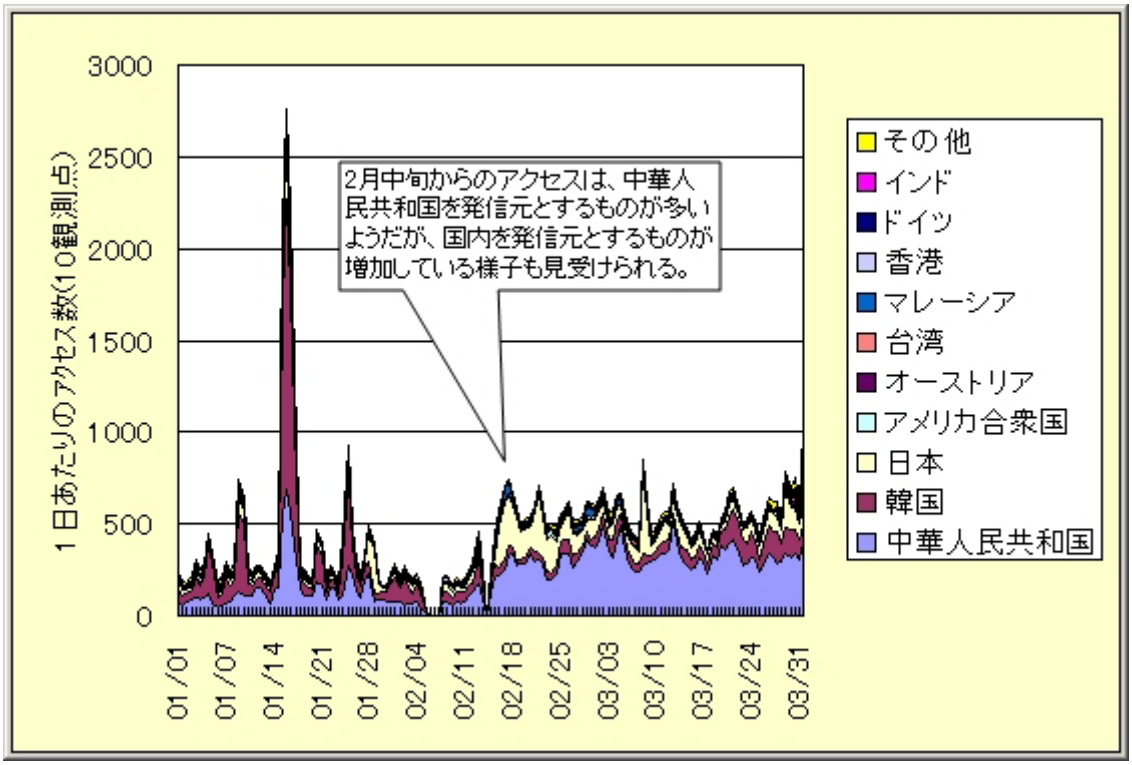


【図 2.3 2005 年第一四半期の一方的なアクセス状況】

2 月中旬くらいから 1433(TCP)へのポートスキャン[*5]が、緩やかな増加傾向にあるようです(図 2.4 および図 2.5 を参照されたい)。特に 3 月の後半で、アクセス数そのものより発信元の数が一時的に増加するような状況も見受けられました。このポートを開いている利用者(SQL Server の利用者)は、何らかの不正なアクセスを受ける可能性が増えていますので、お使いのシステムに脆弱性がないかどうか、ご確認下さい。

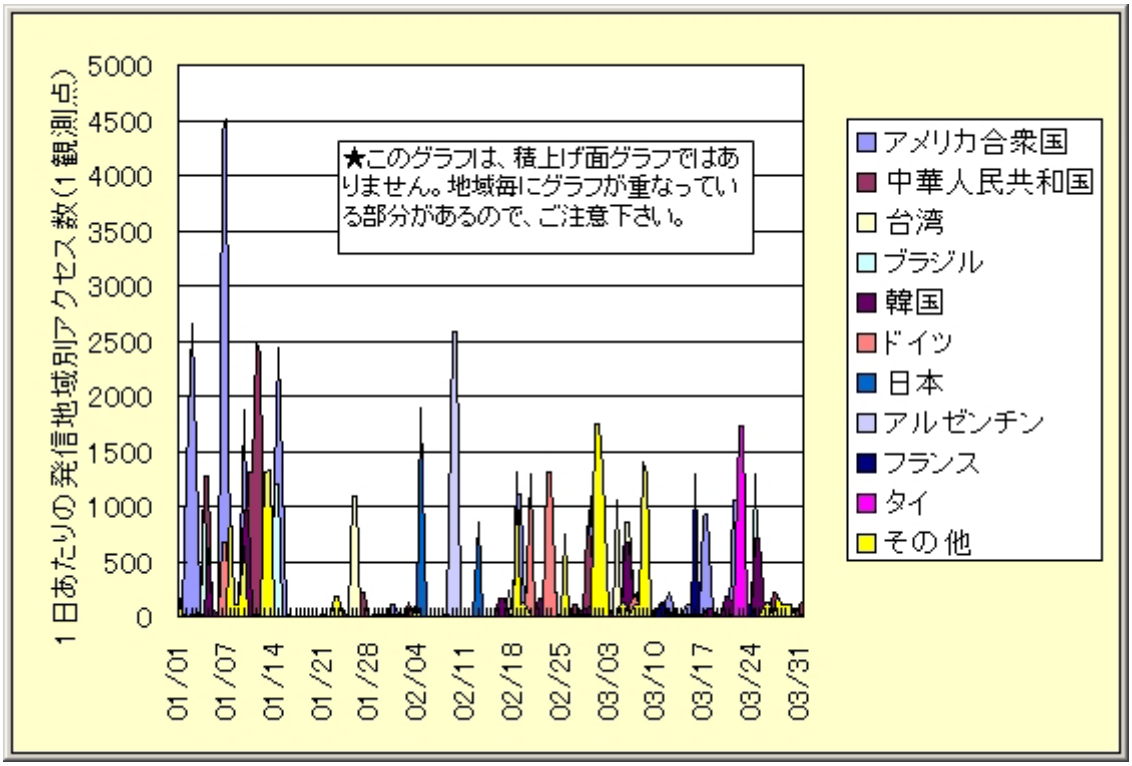


【図 2.4 2005 年第一四半期の 1433(TCP)へのアクセス/発信元数の状況】



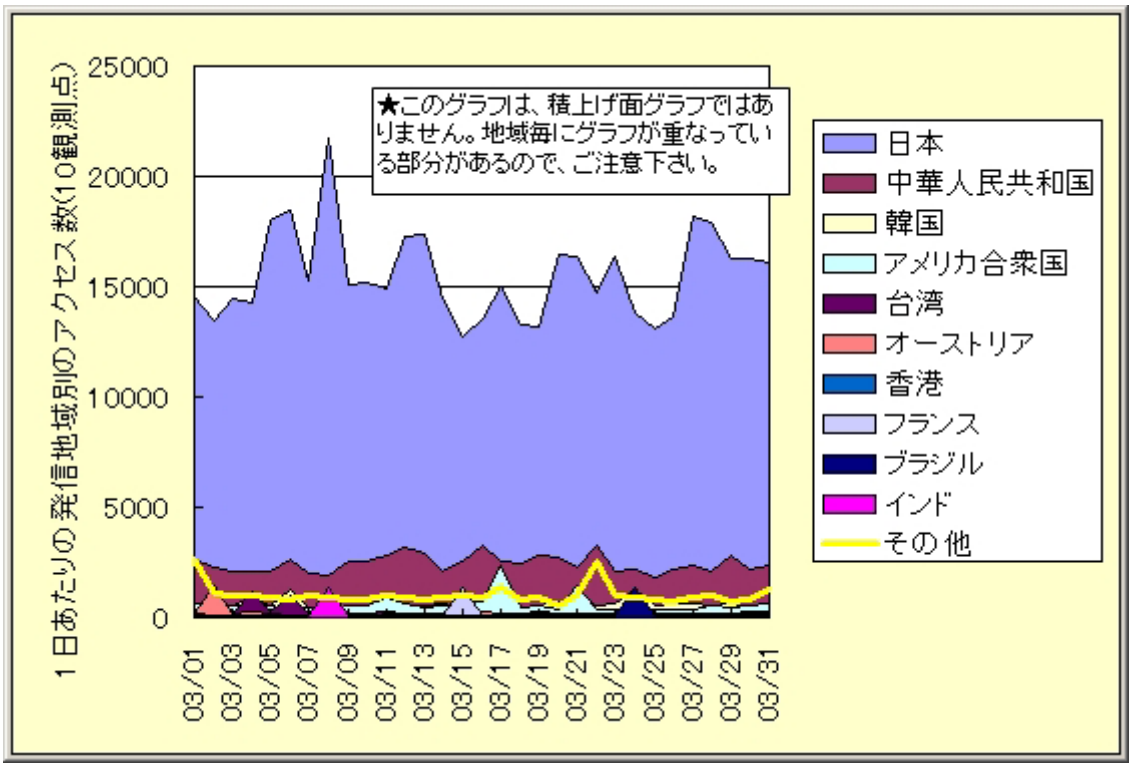
【図 2.5 2005 年第一四半期の 1433(TCP)へのアクセス状況(発信地域別)】

また、図 2.1 や図 2.2 に表示されている **22(TCP)**のポートへのアクセスは、一般のインターネット利用者ではあまり見られないアクセスです。このアクセスについては、IPA の定点観測環境で 22 番ポートが開いているために、集中的な攻撃(パスワードクラッキング(*6)攻撃)を受けているものです。一般的に管理用に使われる数種類のユーザ ID と、辞書に定義されているような一般的な単語あるいは良く使われる単語をパスワードとして使い、ログインしようとする攻撃(辞書攻撃(*7))です。このポートを開いている利用者(SSH(Secure Shell)の利用者)の方は、同じ攻撃を受ける可能性があるので、ご注意下さい。図 2.6 に 3 月の 22(TCP)へのアクセス状況について示します。



【図 2.6 2005 年 3 月の 22(TCP)へのアクセス状況(発信地域別)】

3 月の期待しない(一方的な)アクセスの発信元地域は、1 月～2 月と同じように、国内が多いようです(図 2.7 を参照されたい)。国内からのアクセスについで、中華人民共和国や韓国からのアクセスが目立ちます。発信元地域の状況変化については、後述の 3 月のアクセス統計情報(図 3.2)を、参照されたい。

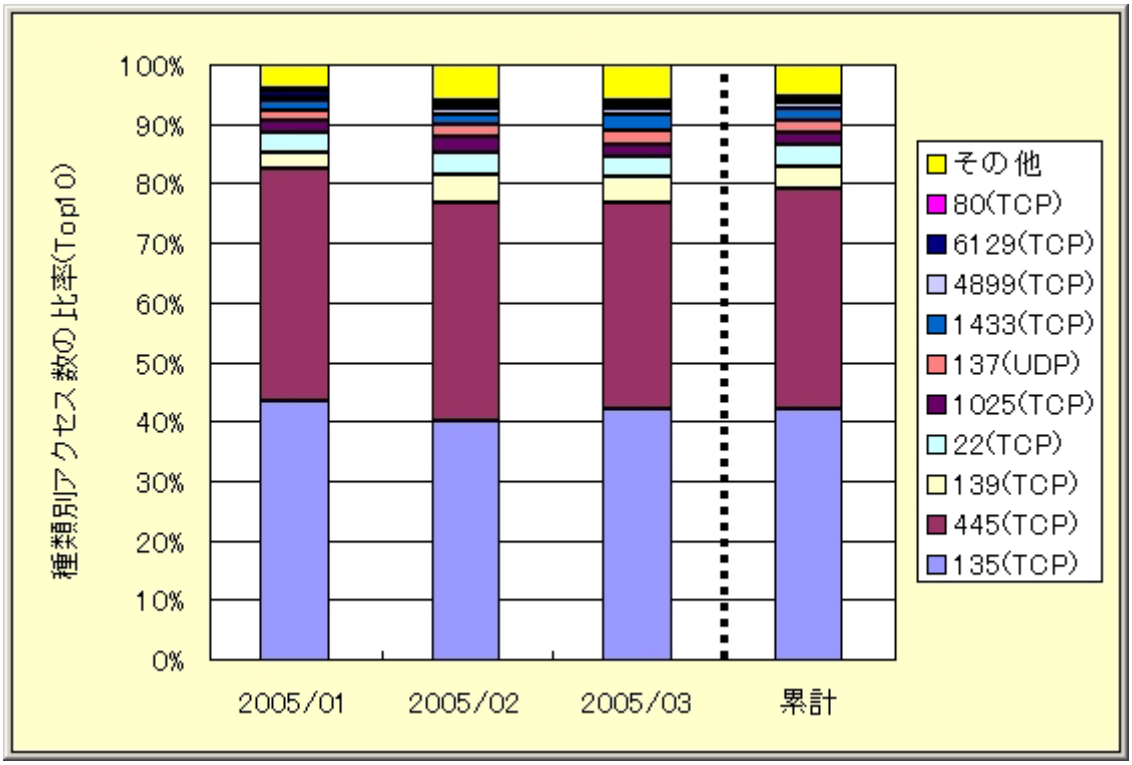


【図 2.7 2005 年 3 月の発信地域別アクセス状況】

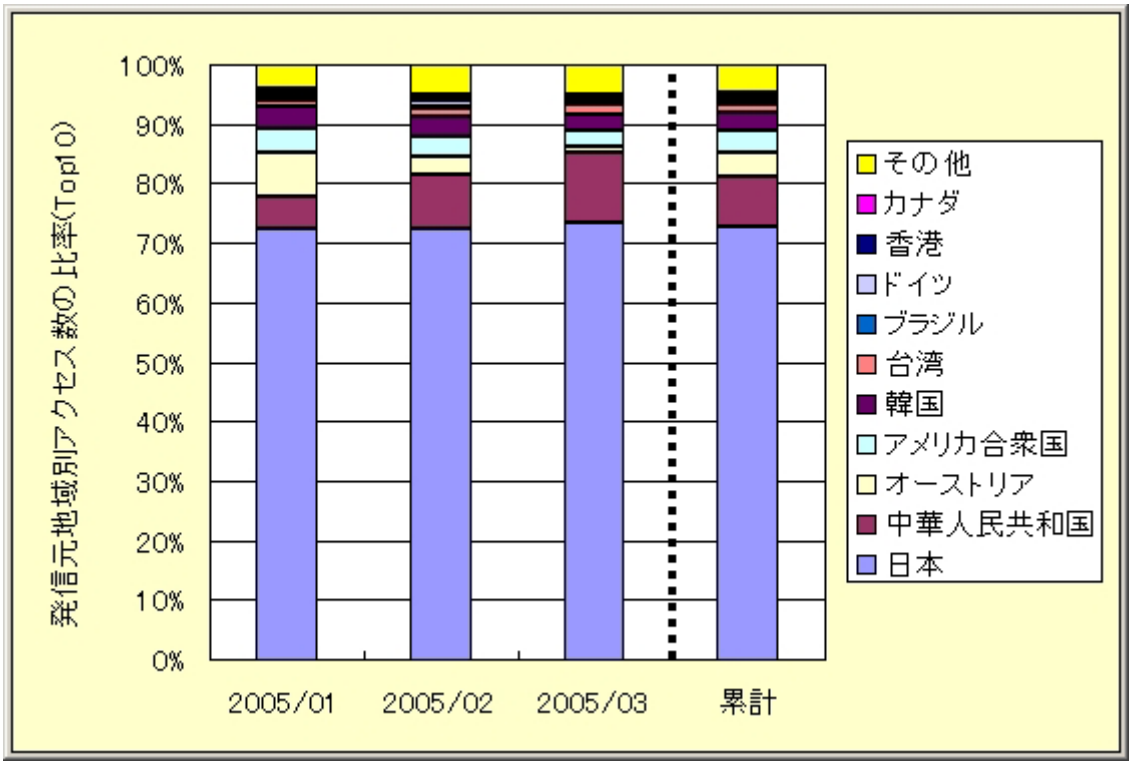
3．3月のアクセス統計情報

以下に、2005年1月～3月の種類別アクセス数の比率の変化(図3.1)、および発信元地域別アクセス数の比率の変化(図3.2)を示します。

アクセスの種類については、特に大きな変化は見受けられません。発信元地域については、あいかわらず国内からのアクセスが多いようですが、比率的にオーストリアからのアクセスが減少傾向で、中華人民共和国からのアクセスが増加傾向にあるようです。



【図3.1　2005年1月～3月の種類別アクセス数の比率】



【図3.2　2005年1月～3月の発信元地域別アクセス数の比率】

4．3月のコラム『もうひとつの定点観測』

(1)ウイルスメールの定点観測

インターネットからの脅威と言う意味では、インターネットからの直接的なアクセス(期待しないアクセス)だけでなく、ウイルスメールや不正な Web サイトの脅威も存在します。

一昔前のウイルスメールは、利用者のメールを発信する行為に便乗して感染(拡散)活動を行っていました。しかしながら、最近のウイルス(メール)は、いわゆるマスメーリング機能を持ち、感染者が持つ不特定多数のメールアドレス(メーラーの持つアドレス帳内のアドレスだけでなく参照した Web サイトのキャッシュデータ上にあるアドレスも利用される)から、さらに多くのメールアドレスを捏造して、感染活動を行っています。これらの状況から、広く知られたメールアドレスを持つ企業や個人利用者へは、より多くのウイルスメールが送信されることになります。

不正な Web サイトを受動的に定点観測するのは難しいとしても、ウイルスメールについては、定点観測することは可能です。

インターネットからの直接的なアクセスを、ルータやファイアーウォール, IDS を利用して観測することができるように、ウイルスメールについては、ウイルス対策ソフト（いわゆるウイルスウォール）を利用して観測することができます。

IPA では、IPA のメールサーバの手前に置かれたウイルスウォールを利用して、ウイルスメールの定点観測を実施しています。

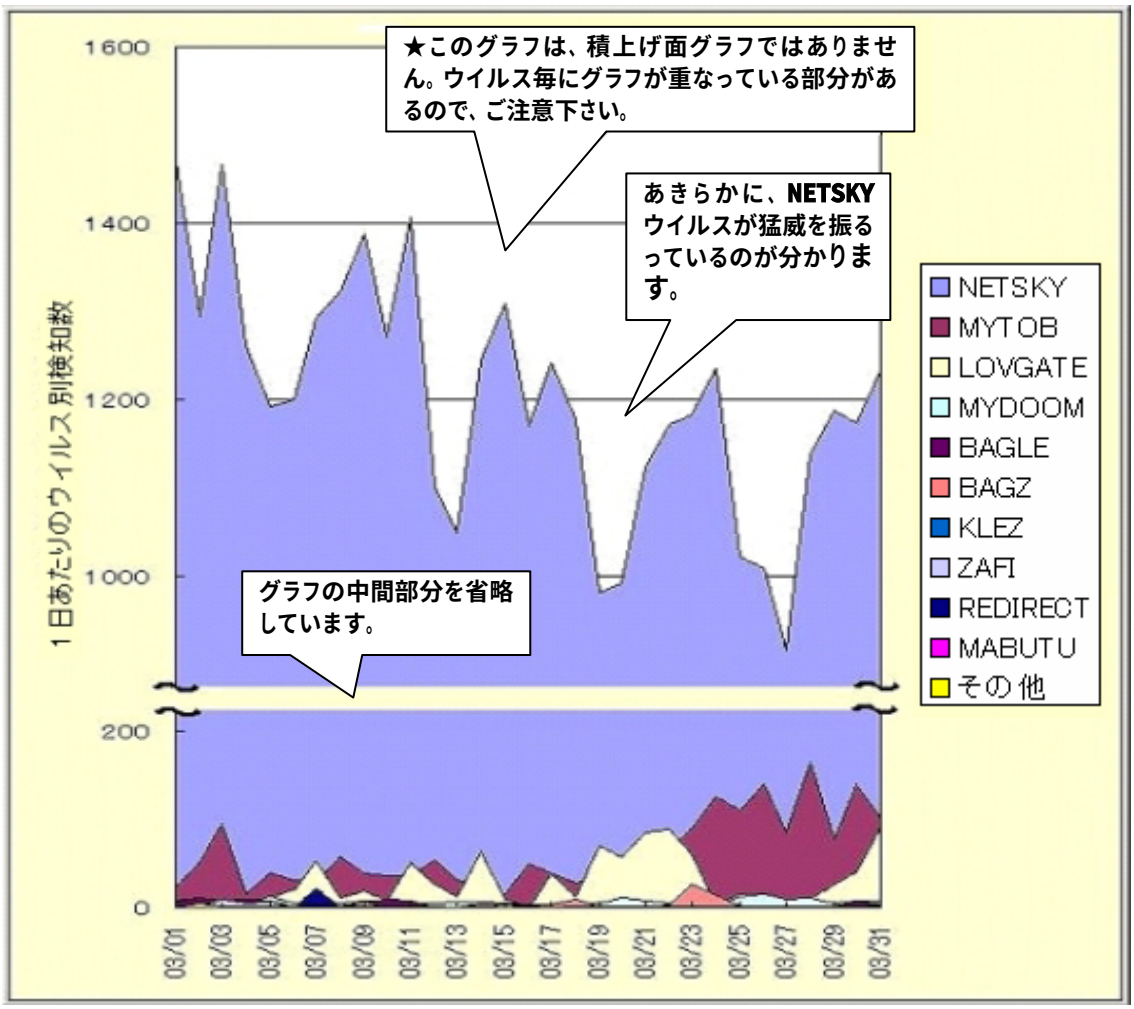
(2) IPA でのウイルスメール定点観測

先に述べたように、IPA では、IPA のメールサーバとインターネット境界の間に設置したウイルスウォールの、ウイルスメール検知ログから、ウイルスメールの定点観測を実施しています。図 4.1 に 2005 年 3 月の検知状況を示します。

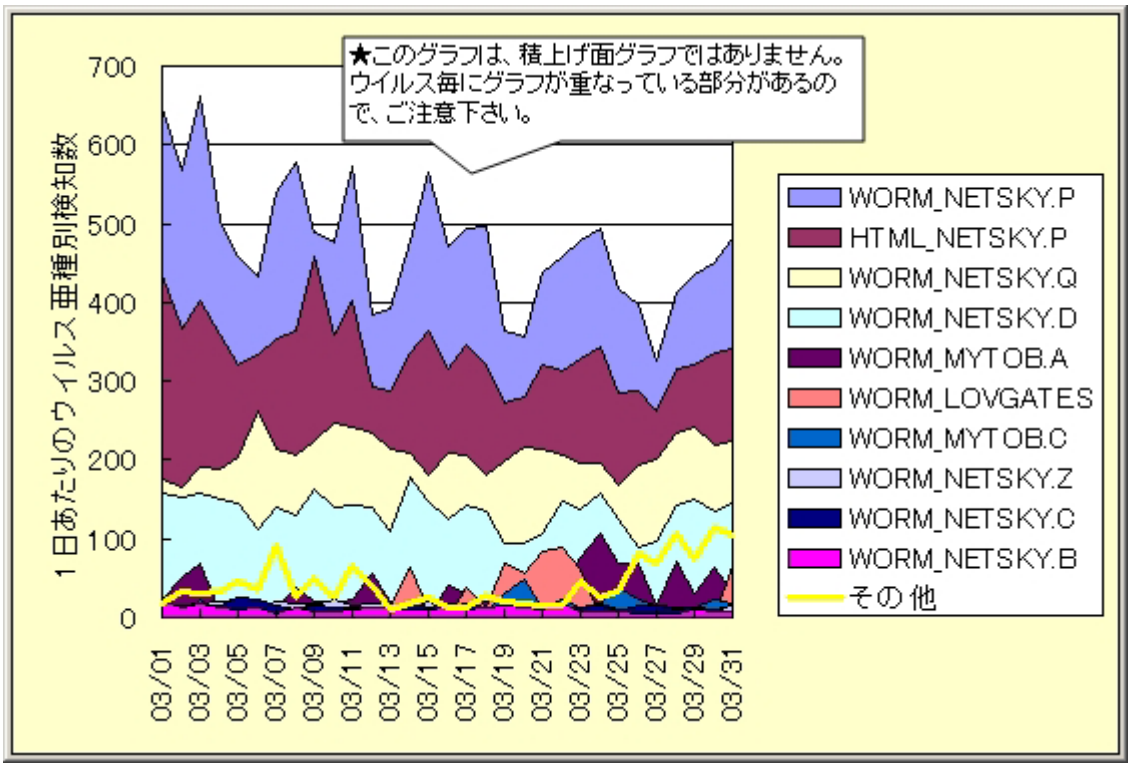
2005 年 3 月の IPA でのウイルス検知件数は、1 日あたり **1,307** 件で、3 月1日～3 月 31日で合計 **40,510** 件でした。また、図 4.1 でも分かるように、あいかわらず **NETSKY** ウイルスが猛威を振るっているのが明らかです。ただし、NETSKY ウイルスについては、3 月の検知状況を見る限り、緩やかな減少傾向にあるようです。
また、この検知件数には、NETSKY のような狭義のウイルスだけでなく、トロイの木馬等も含まれています（ウイルスウォールで検知したすべての広義のウイルスをカウントしています）。当然のことながら、この検知実績は IPA へのウイルス発見届出としても届出しています。

IPA での検知実績が、インターネット上のすべてのメール利用者と同じであるかどうかは、明確ではありませんが、このような観測が広く行われるようになれば、言い換えれば、インターネット上の、数多くのウイルスウォールでウイルスメールの定点観測を行うことができれば、新種のウイルスメールや、ウイルスの増加･減少傾向を観測することができます。

このような、ウイルスメールを定点観測するネットワークが構築できれば、ウイルスの発生や感染活動の状況について、より的確な情報発信ができるようになると思われ、新たな定点観測の仕組みを作ることも重要なことではないかと考えています。



【図 4.1　IPA での 2005 年 3 月のウイルス検知状況】

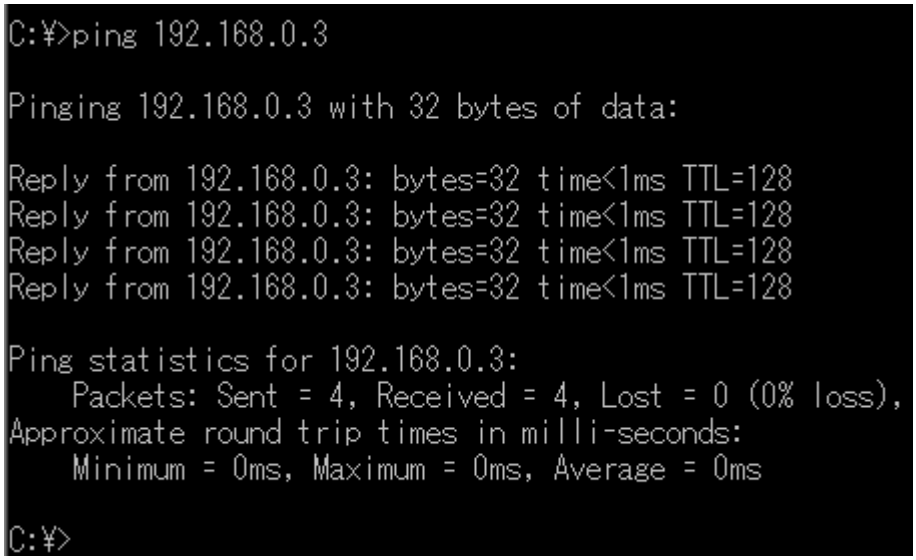


【図 4.2　IPA での 2005 年 3 月のウイルス(亜種)検知状況】

『用語の解説』

(*1)Ping(ICMP)

インターネットやイントラネットなどの TCP/IP ネットワーク上で、特定のIPアドレスを割り振られた機器が接続されているか診断するプログラム。診断する機器の IP アドレスを指定すると、ICMP(Internet Control Message Protocol：IP のエラーメッセージや制御メッセージを転送するプロトコル)を使って通常 32 バイト程度のデータを送信し、相手の機器から返信があるかどうか、返信がある場合はどのくらい時間がかかっているか、などの診断結果を得ることができる。



【ping コマンドの実行例】

(*2)ワーム(worm)

通常のウイルスは感染対象のプログラムを必要としますが、ワームは、感染対象となるプログラムがなく、自分自身の複製をコピーして増殖します。

ネットワーク内を這い回る虫のように見えることから、この名称が付けられました。

(*3)トロイの木馬(trojan horse)

便利なソフトウェアに見せかけて、ユーザに被害を与える不正なプログラムです。感染機能は持っていませんので、感染増殖することはありません。

トロイの木馬の内部に隠していたウイルスをパソコンに組み込む、パソコン内部の秘密のファイルをインターネット上に送信する、ファイルやディスク内容を破壊するなど、さまざまな被害をもたらします。

感染増殖はしないので、ワクチンソフトでは、基本的にトロイの木馬を検出の対象外としています。信頼できないサイトに便利なツールとして掲載されていても、そのプログラムはむやみにダウンロードして実行しないようにしましょう。「怪しいプログラムは実行しない」という原則を守れば、トロイの木馬の被害を防ぐことができます。

(*4)ポート(port)

コンピュータ内の各種サービスの窓口のことです。ポートは 0 から 65535 までの数字が使われるためポート番号とも呼ばれます。

(*5)ポートスキャン(port scan)

攻撃･侵入の前段階として、標的のコンピュータの各ポートにおけるサービスの状態を調査すること。

(*6)パスワードクラッキング(password cracking)

本人認証のためにパスワードを利用しているシステムにおいて、本人の知識によらずにパスワードを得るための分析行為。パスワードクラックということもある。

(*7)辞書攻撃(dictionary attack)

パスワードの割り出しや暗号の解読に使われる攻撃手段の１つで、辞書にある単語を片端から入力して試す手法。

(*8)脆弱性(vulnerability)

情報セキュリティ分野における脆弱性とは、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いいます。オペレーティングシステムの脆弱性や、アプリケーションシステムの脆弱性があります。また、ソフトウェアの脆弱性以外に、セキュリティ上の設定が不備である状態も、脆弱性があるといわれます。脆弱性は、一般に、セキュリティホール(security hole)と呼ばれることもあります。

近年ソフトウェアの脆弱性について、広い語感を与える vulnerability を整理し、予定されたセキュリティ仕様を満たさないものを狭義の vulnerability とし、仕様上のセキュリティの欠如を Exposure(露出)として区別する動きがあります。

このほかにも、広義には vulnerability もしくは security hole と呼ばれながらも、ソフトウェア自体の問題ではない論点には、弱いパスワード等の本人認証の回避問題、設定ミスによる問題があります。

・コンピュータ不正アクセス被害の届出制度について

コンピュータ不正アクセス被害の届出制度は、経済産業省のコンピュータ不正アクセス対策基準に基づき、’96 年 8 月にスタートした制度であり、同基準において、コンピュータ不正アクセスの被害を受けた者は、被害の拡大と再発を防ぐために必要な情報をＩＰＡに届け出ることとされています。

ＩＰＡでは、個別に届出者への対応を行っていますが、同時に受理した届出等を基に、コンピュータ不正アクセス対策を検討しています。また受理した届出は、届出者のプライバシーを侵害することがないように配慮した上で、被害等の状況を分析し、検討結果を定期的に公表しています。

○コンピュータ不正アクセス対策基準

・通商産業省告示第３６２号　平成 8 年 8 月 8 日制定
・通商産業省告示第５３４号　平成 9 年 9 月 24 日改訂
・通商産業省告示第９５０号　平成 12 年 12 月 28 日改訂
・経済産業省告示第３号　　平成 16 年 1 月 5 日改訂

■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／内山
Tel:03-5978-7527 Fax:03-5978-7518 E-mail:isec-info@ipa.go.jp