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。

前回のプレスリリースでは、『1 月の期待しない(一方的な)アクセスは、単純計算で、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、1 日当たり約 3,000 件のアクセスがあったと言うことになります。』と報告しましたが、2 月分でも 1 日当たり**約 2,370 件**のアクセスがありました。

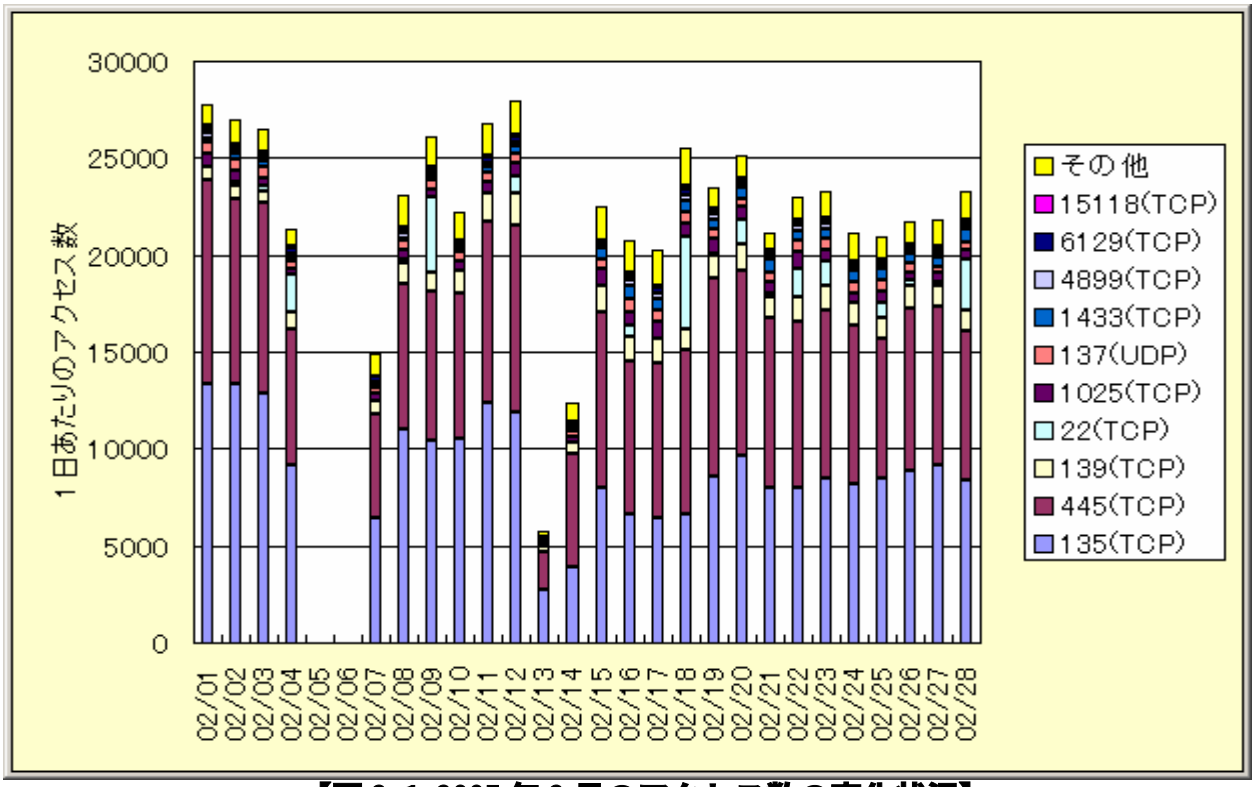
1 月に比べてややアクセス数は減少傾向にありますが、それでも状況が良くなっているわけではありません。

2．2 月のアクセス状況

2 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 **575,582 件**(Ping(ICMP)(*1)は除く)ありました。

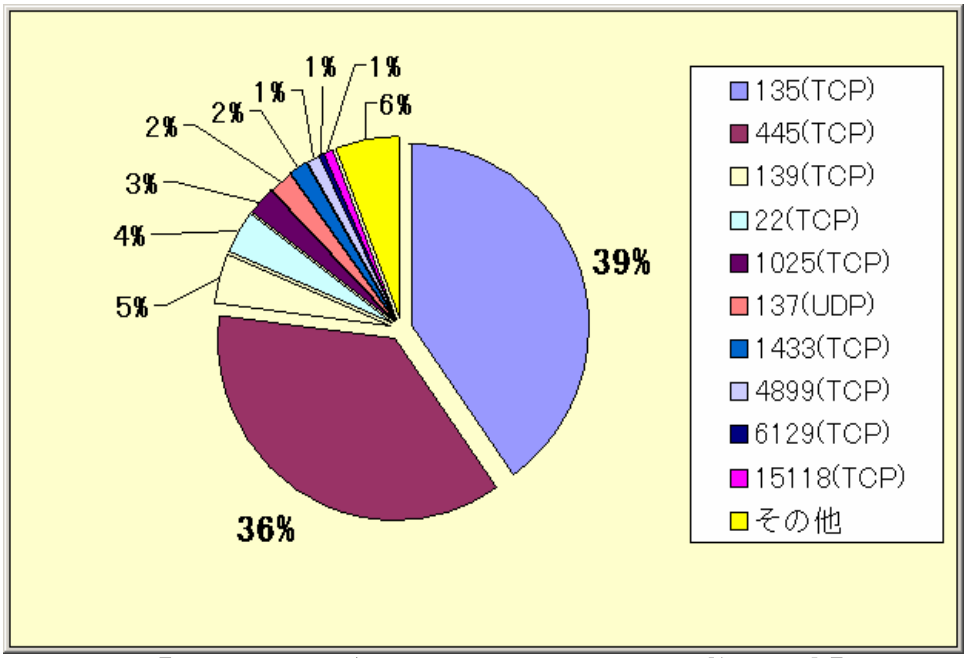
2 月は、インターネット定点観測(TALOT2)のメンテナンス作業が入ったために、数日間(2/4～2/7,2/13～2/14)観測を停止したため、図 2.1 でグラフに抜けが出ています。アクセス総数は 1 月に比べて大幅に減少していますが、終日観測を行っていた部分のみで、**1 日あたりの 1 つの観測点(一般のインターネット利用者個人と同様な環境)で約 2,370 件のアクセスがあった計算になります。**

アクセス状況(2/1 から 2/28 の 1 日毎の **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 に示します。



【図 2.1 2005 年 2 月のアクセス数の変化状況】

2 月も 1 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。



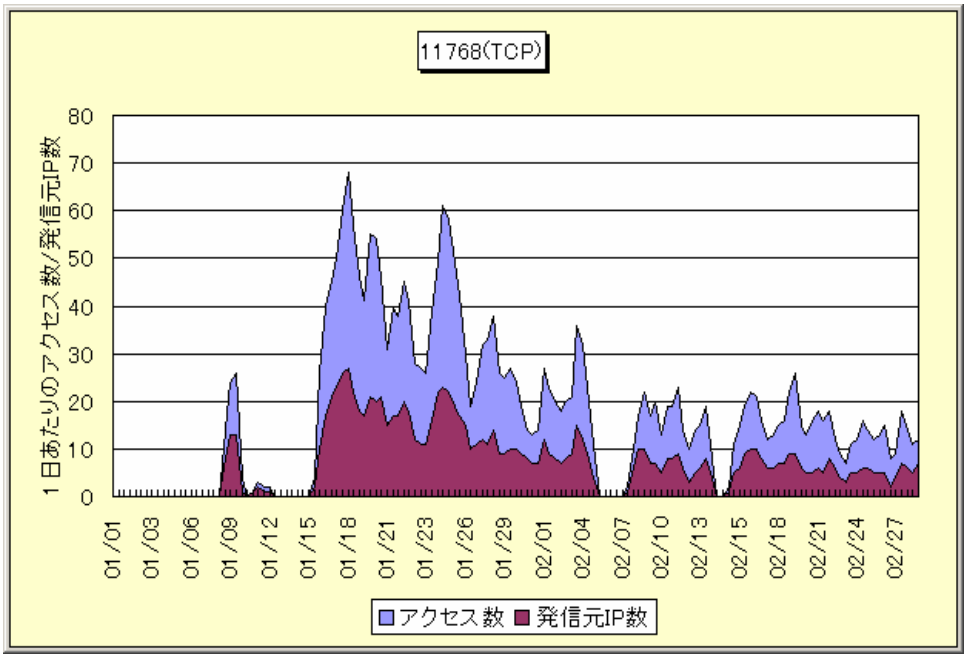
【図 2.2 2005 年 2 月の種類別アクセス数の比率】

図 2.1 や図 2.2 に表示されているアクセス数の多い **135(TCP),445(TCP),139(TCP)**のポートは、多くのワームが攻撃(感染活動)に利用するものです。これらのポートは、通常は自分の所属するネットワーク(家庭内ネットワーク/企業内ネットワーク)内でのみ使用するもので、インターネットからアクセスされるものではありません。したがって、インターネット境界でルータなどのパケットフィルタリング機能を使用して、アクセスを遮断していれば大丈夫です。また、パケットフィルタリングができない場合は、これらの攻撃(感染活動)が、コンピュータの脆弱性を狙った場合がほとんどなので、狙われている脆弱性を解消しておけばアクセスされても大丈夫です。

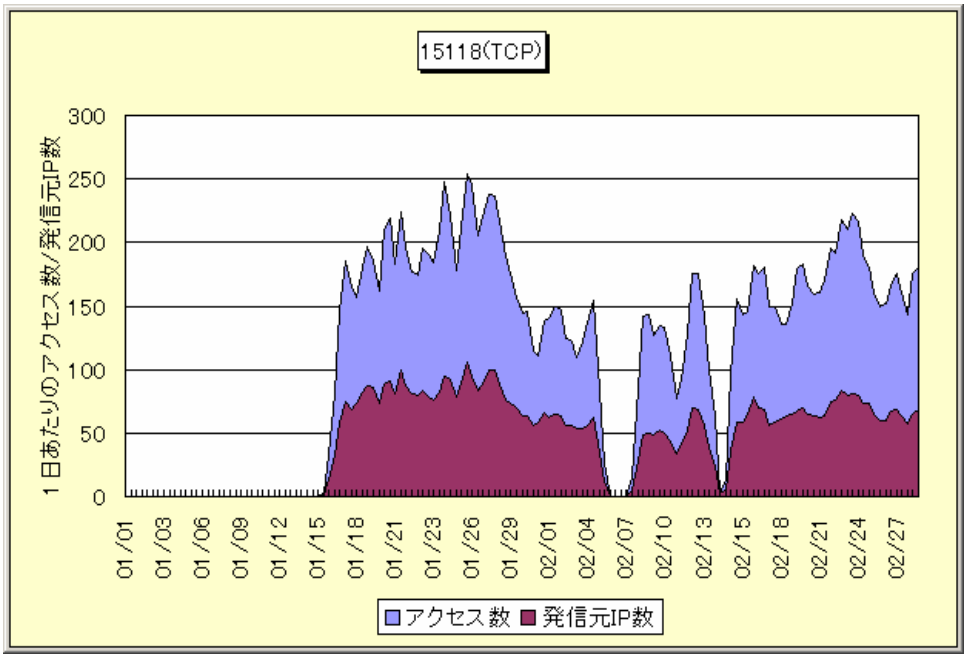
また、図 2.1 や図 2.2 に表示されている **22(TCP)**のポートへのアクセスは、一般のインターネット利用者ではあまり見られないアクセスです。このアクセスについては、IPA の定点観測環境で 22 番ポートが開いているために、集中的な攻撃(パスワードクラッキング(*5)攻撃)を受けているものです。一般的に管理用に使われる数種類のユーザ ID と、辞書に定義されているような一般的な単語あるいは良く使われる単語をパスワードとして使い、ログインしようとする攻撃(辞書攻撃(*6))です。このポートを開いている利用者(SSH(Secure Shell)の利用者)の方は、同じ攻撃を受ける可能性があるので、ご注意下さい。SSH への不正アクセスについては、2 月の『コンピュータ不正アクセス届出状況』(要旨)にも被害事例として掲載しています。

次に、図 2.1 や図 2.2 に表示されている **15118(TCP)**へのアクセスについて説明します。
1 月初旬(明確に観測されたのは 1/16 頃)から発生している **Dipnet/Oddbob/Netdepix** と呼ばれるワームが、継続して活動しているようです。
このワームは、2004 年 4 月に公開された Windows OS の脆弱性(*7) (MS04-011) を狙ったワームで、感染活動の際に 11768(TCP)および 15118(TCP)へのポートスキャン(*8)を行います。ちなみに、11768(TCP)と 15118(TCP)は**Dipnet/Oddbob/Netdepix**ワームに感染しているコンピュータに埋め込まれたバックドアが開くポートで、このポートへのアクセスは、すでに感染しているコンピュータか確認するためのポートスキャンです。すでに感染しているコンピュータには新たに感染はせず、感染していないコンピュータに対して 445(TCP)へのアクセスを通じて脆弱性を狙った攻撃をします。感染すると、いろいろな不正アクセスを行うプログラムをコンピュータに埋め込みます。

Dipnet/Oddbob/Netdepix ワームの感染活動を観測できた状況を図 2.3 および図 2.4 に示します。



【図 2.3　11768(TCP)へのアクセス状況】



【図 2.4　15118(TCP)へのアクセス状況】

今のところ、感染の中心は北米方面と観測されており、国内での感染はほとんど観測されませんが、Windows の脆弱性を解消していないコンピュータには感染する可能性があるので、コンピュータを最新の状態にしていない利用者は注意が必要です。

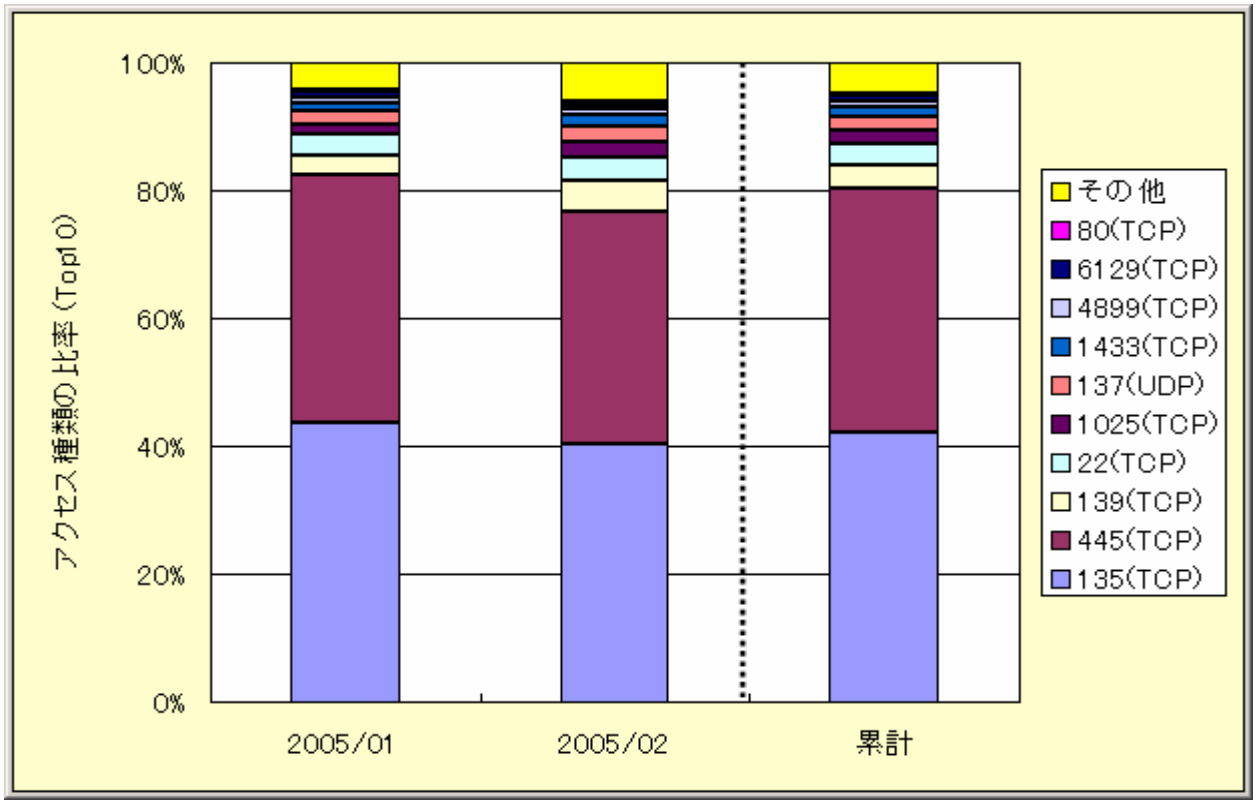
MS04-011 の脆弱性については以下のサイトを参照して下さい。

http://www.ipa.go.jp/security/news/news0404.html

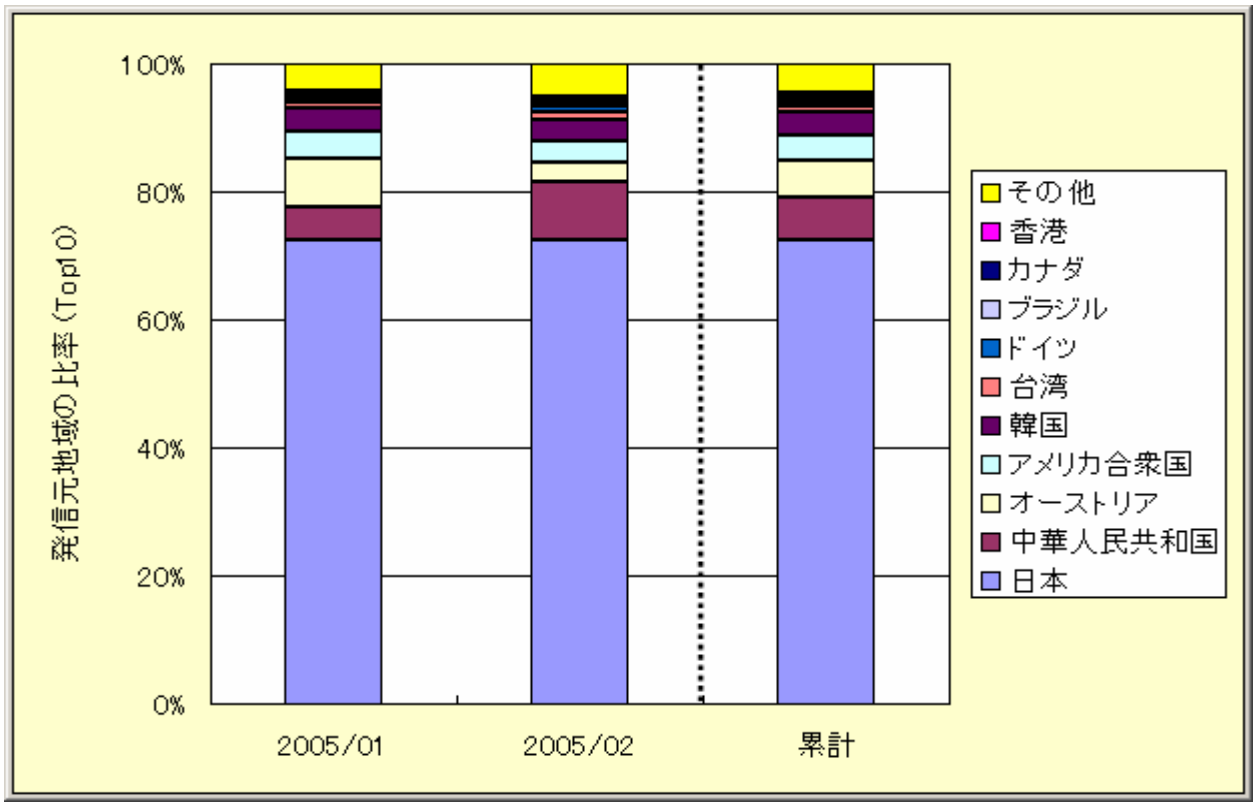
3．2月のアクセス統計情報

以下に、2005年1月～2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、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。



【図3.1　2005年1月～2月の種類別アクセス数の比率】



【図3.2　2005年1月～2月の発信元地域別アクセス数の比率】

4．２月のコラム『ルータ』

(1)インターネットからの脅威を防ぐもの…

ADSL(Asymmetric Digital Subscriber Line)やCATV(Cable TV)あるいは光ファイバーによるインターネット接続（いわゆるブロードバンド接続）が普及し、更に、常時接続をしている利用者の方が増えている状況で、期待しない一方的なアクセスが起こっていることは大きな問題です。これらのすべてのアクセスが、利用者の感染や破壊を招くわけではありませんが、利用者としてはこれらの脅威から身を守る対策が必要です。例えば･･･

- **常にＯＳやアプリケーションを最新の状態にしている(例えば Windows Update の実行)**
  →脆弱性を狙った攻撃が来ても何も起こらない
- **パーソナルファイアウォール(*9)を導入している(例えば Windows ＸＰでのファイアウォール設定)**
  →自分の期待しないアクセスは遮断している
- **不要なサービスは止めている**
  →自分の期待しないアクセスは遮断している
- **パケット(*10)フィルタリングを行う機器を導入している（ファイアウォール機器）**
  →自分の期待しないアクセスはコンピュータまで届かない

等々

これらの対策が確実に行われているのであれば、インターネットからの一方的な攻撃は防ぐことができます。

そこで、今回のテーマとして、普段あまり気にかけていない、**インターネットとの境界**で働いていて、かつ簡易なファイアウォール機器としても機能している**ルータ**について考えてみましょう。

(2)ルータって何？

ではルータとは何でしょうか。用語解説風に言うと、**ルータは、異なるネットワーク同士を相互接続するネットワーク機器**と言う事になります。一般利用者が、家庭等でインターネットを利用する場合、自身のパソコンを外部のネットワーク(プロバイダ)と繋ぐわけですが、この際にルータを使用すると、外部のネットワークと自身のコンピュータ(ネットワーク)を明確に区分けできるようになります。

例えば、家庭で ADSL 接続をする場合、ADSL モデムを使用しますが、最近の ADSL モデムには簡易なルータ機能が搭載されている場合があります。

一般的に、家庭等でインターネットを利用する場合、１つのグローバル IP アドレス(*11)（グローバルアドレス(*12)）が割り付けられますが、家庭内で複数のコンピュータを同時にインターネットに接続するような場合は、ルータは必須の機器となります。

複数のコンピュータを家庭内のネットワーク上に置いた場合、インターネット上では１つの IP アドレス(グローバル IP アドレス)しかないので、家庭内のコンピュータそれぞれにローカル IP アドレス(プライベートアドレス(*13))を設定し、これらのローカルIPアドレスから通信を行う際にグローバル IP アドレスとの対応関係を管理する必要があります。これを **NAT(Network Address Translation)機能**と呼びます。また、複数コンピュータの複数の通信を区別するためには、NAT によるIPアドレスの変換だけでなく、その上位プロトコル(*14)であるTCP/UDPのポート番号も識別する **IP マスカレード機能**も動作します。

これらの機能により、外部のネットワーク(インターネット)からの一方的なグローバルIPアドレス

に対するアクセスは、変換すべきローカル IP アドレスの対応がとれないため、アクセスが遮断できることになります(家庭内のネットワークから外部ネットワークへの通信およびそれらの正常な応答は遮断されません)。ルータ機器によっては、これらの遮断を細かく設定(ファイアウォール機能としてのパケットフィルタリング)できるものもあります。

(3)ルータ機能を使わないと・・・

ところで、オンラインネットワークゲームや P2P[*15]接続を行う場合に、グローバル IP アドレスが必要と言うことで、安易にインターネットに自身のコンピュータを直接接続する場合がありますが、このような場合は**インターネットからの脅威をすべて受け取ります**ので、別途コンピュータ上に対策(不正アクセスからの自衛策:例えばパーソナルファーアウォールの導入)が必要になります。また、一部の CATV によるインターネットの接続や光ファイバーによる接続の場合も専用のルータ機器を導入しないとインターネットに直接接続されてしまう場合もあるので、接続形態が不明の利用者は自身のネットワーク接続形態について確認(ご利用のネットワーク接続機器のマニュアルを確認するか、ご契約のプロバイダに確認)することをお勧めします。

特に、通信機器内蔵(モデム等)やカード型の通信機器を利用している場合は、基本的にルータ機能がないので、インターネットに直接接続されることになります。この場合も、別途コンピュータ上に対策が必要になります。

一昨年の夏に猛威を振るった W32/MSBlaster[*16]や W32/Welchia[*17]を例に挙げると、IPA/ISEC への問い合わせ等からも、これらのインターネットに直接接続されたコンピュータが感染したケースが多かったようです。当時は、このような状況で感染したコンピュータが企業内に持ち込まれ、さらに企業内の他のコンピュータに感染したことが話題になっていました。

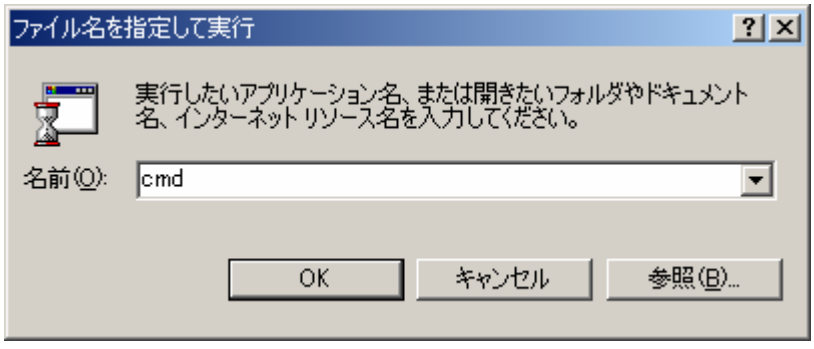
(4)ルータは働いているの？

Windows OS の搭載されたコンピュータでは、ルータが無いあるいは NAT 機能が動作していない状態でインターネットに接続しているかを簡単に検査する方法として、以下に示す方法があります。

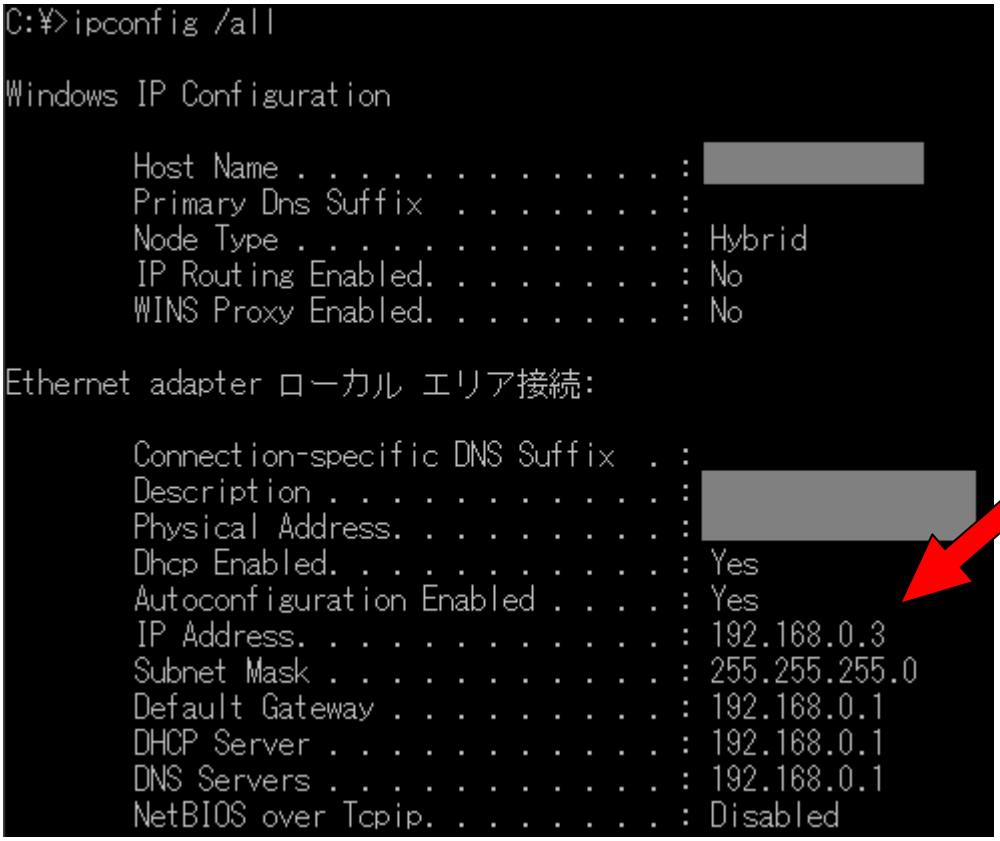
- **ipconfig** コマンドの実行

  ipconfig コマンドは Windows のネットワーク環境(設定)を確認するために使用できるコマンドです。このコマンドをコマンドプロンプトで実行すると、現在コンピュータに設定されている IP アドレスを表示することができます。

  操作手順は、Windows のスタートから「ファイル名を指定して実行(R)」を選択→名前に **cmd** を入力して OK ボタンをクリックする→コマンドプロンプト画面が開く→**ipconfig /all** を入力し Enter キーを押す(最後は右上×ボタンで終了)。



一般的に IP アドレス(IP Address：図 4.1 の矢印部分)の表示が **192.168.**で始まるようであれば(明にルータ機器でローカルアドレスを設定変更している場合は除く)、ローカル IP アドレスが使われているので、ルータ(NAT 機能)が動作していると考えてよいでしょう。



【図 4.1 ipconfig コマンドの実行例】

Windows OS の種類によっては表示内容が一部違う場合がありますのでご注意下さい。また、上の実行例では一部伏字にしてあります。

(5)ルータだって・・・

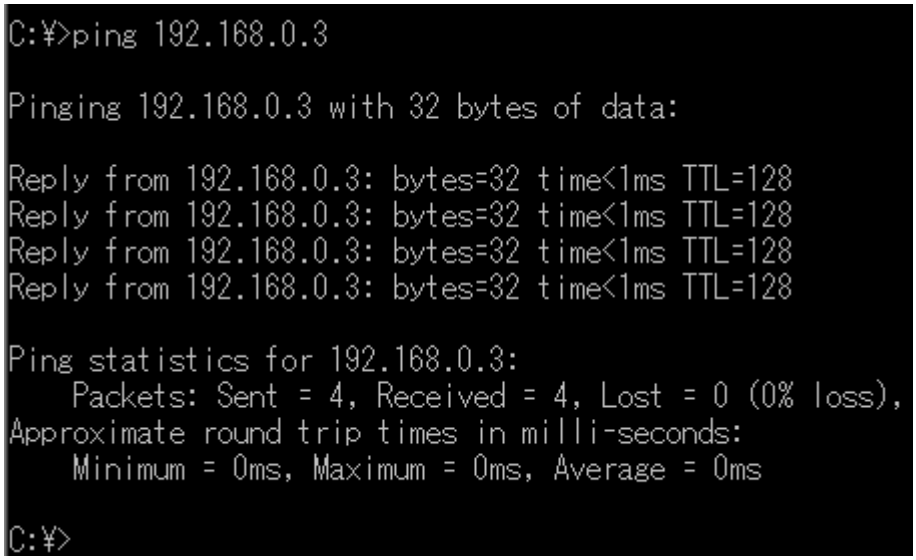
最後に、ルータ機器をお使いの皆さん、ルータのファームウェア(*18)が最新の状態であるか確認することもお忘れなく。ルータもコンピュータと同様にプログラム（ファームウェア）で動いています。ルータ機器のメーカーあるいは提供元のプロバイダのホームページで、更新情報がないか確認して下さい。

ルータ機器もコンピュータと同様に最新の状態でお使いになることをお勧めします。

『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)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。

(*6)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。

(*7)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。

(*8)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。

(*9)パーソナルファイアウォール(personal firewall)

エンドユーザが使用するパーソナルコンピュータ上で、インターネットからの不正なアクセスやワームによる攻撃を防ぐために導入するソフトウェアです。

(*10)パケット(packet)

コンピュータ間の通信において、通信先のアドレスなどの制御情報が付加されたデータの小さなまとまりのこと。データをちいさなまとまり(パケット)に分割して送受信する通信方式をパケット通信と呼ぶ。

(*11)IP アドレス(Internet protocol address)

インターネット上の番地。インターネットに接続されている個々の機器全てに割り振られる。0.0.0.0 から 255.255.255.255 までが使われ、たとえば、「172.16.2.10」などといった形式で表示される。

(*12)グローバルアドレス(global address)

インターネットに接続された機器に割り当てられた IP アドレス。インターネット上の住所にあたり、インターネット上で通信を行うためには必ず必要になる。

(*13)プライベートアドレス(private address)

組織内のネットワークに接続された機器(パソコンやプリンタ)に割り当てられた IP アドレス。組織内で自由に割り当てることができるが、そのままではインターネットを通じて通信を行うことはできない。プライベートアドレスしか持たない機器がインターネット上で通信を行うには、グローバルアドレスを割り当てられた機器に中継してもらう必要がある。

(*14)プロトコル(protocol)

通信規約。ネットワークでデータを流すための約束事をまとめたもの。

(*15)P2P(Peer to Peer)

従来のクライアント･サーバ型のように、サーバにあるデータをダウンロードしてクライアントで利用するのではなく、不特定多数のクライアント間で、サーバを介さずに、直接データのやり取りを行なうインターネットの利用形態のこと。

(*16)W32/MSBlaster

W32/MSBlaster については、以下のサイトを参照されたい。

http://www.ipa.go.jp/security/topics/newvirus/msblaster.html

(*17)W32/Welchia

W32/Welchia については、以下のサイトを参照されたい。

http://www.ipa.go.jp/security/topics/newvirus/welchi.html

(*18)ファームウェア(firmware)

パソコン本体や、モデムなどの周辺機器のハードウェアの基本的な制御を行なうために、機器に組み込まれたソフトウェア。変更が加えられることが少ないことから、ハードウェアとソフトウェアの中間的な存在としてファームウェアと呼ばれている。

ファームウェアを書き換える（アップデートする）ことによって、最新の機能に対応させたり不具合を修正したりできるが、書き換えに失敗すると、その機器が動かなくなることがあるので、慎重な作業が必要である。

・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／加藤／内山

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