別紙 3

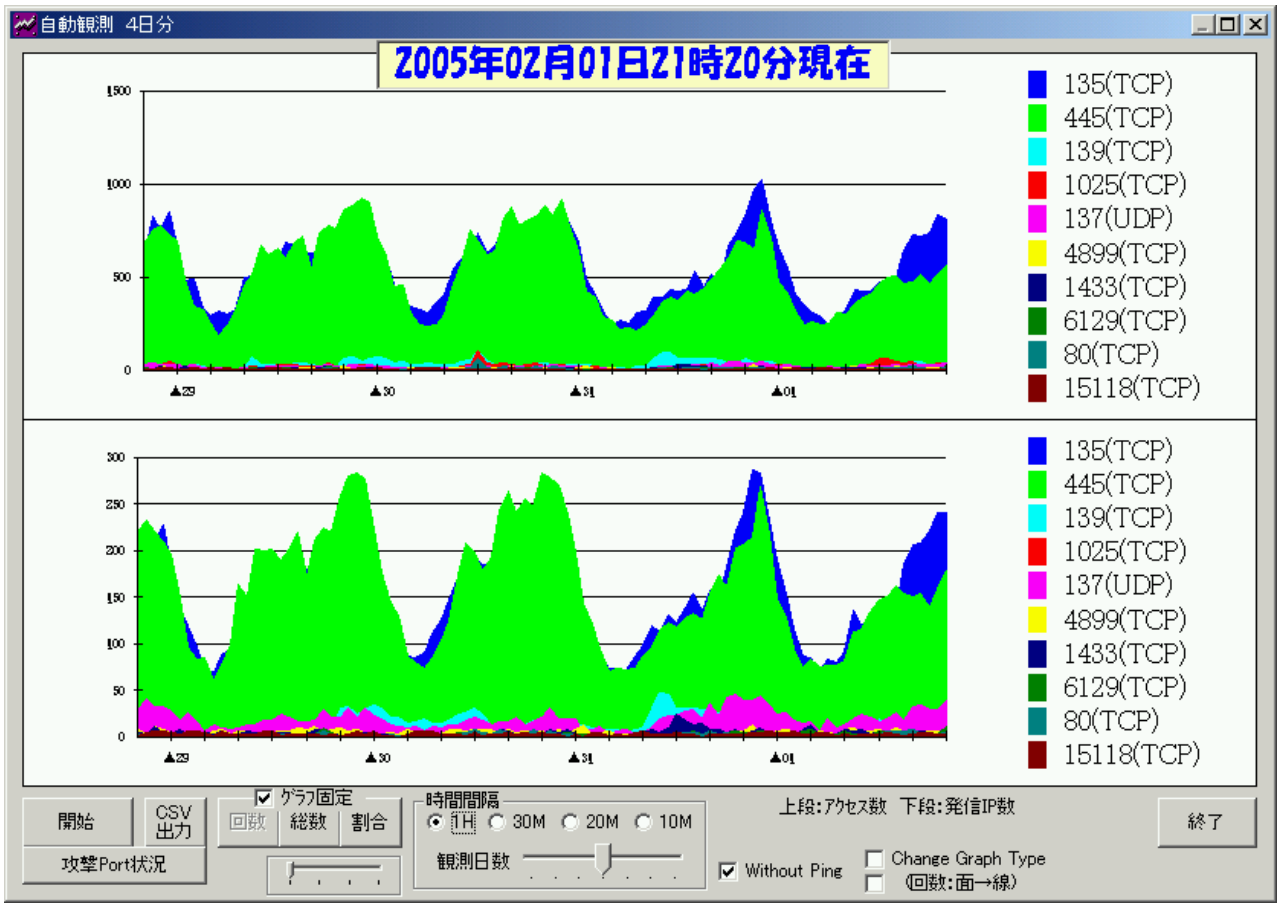
インターネット定点観測(TALOT2)での観測状況について

1．一般のインターネット利用者の皆さんへ

最近、一般のインターネット利用者から、パーソナルファイアウォール(*1:以下、文末の『用語の解説』を参照されたい)での不正アクセスログ(*2)をみて、IPA にアクセスの状況に関する問い合わせをされる方が増えてきました。特に、パーソナルファイアウォールが遮断したアクセスの警告を見て、自分のところをターゲットにして不正アクセスをしようとしているのではないかと、不安になる方もいるようです。そこで、インターネットに接続していると、通常どのようなアクセスがあり、現在、異常といえる状況にあるか判断するための一助となるように、**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、今月よりお知らせすることにしました。**

2．インターネット定点観測(TALOT2)

国内でインターネットを利用する一般利用者のうち、**80%以上が大手プロバイダ 10 社に加入しています。**IPA では、これらの多くの**一般のインターネット利用者の皆さんと同様の環境**である ADSL によるプロバイダ接続を大手プロバイダ 10 社と行い、常時インターネットからの一方的な(期待しない)アクセスを観測しています。



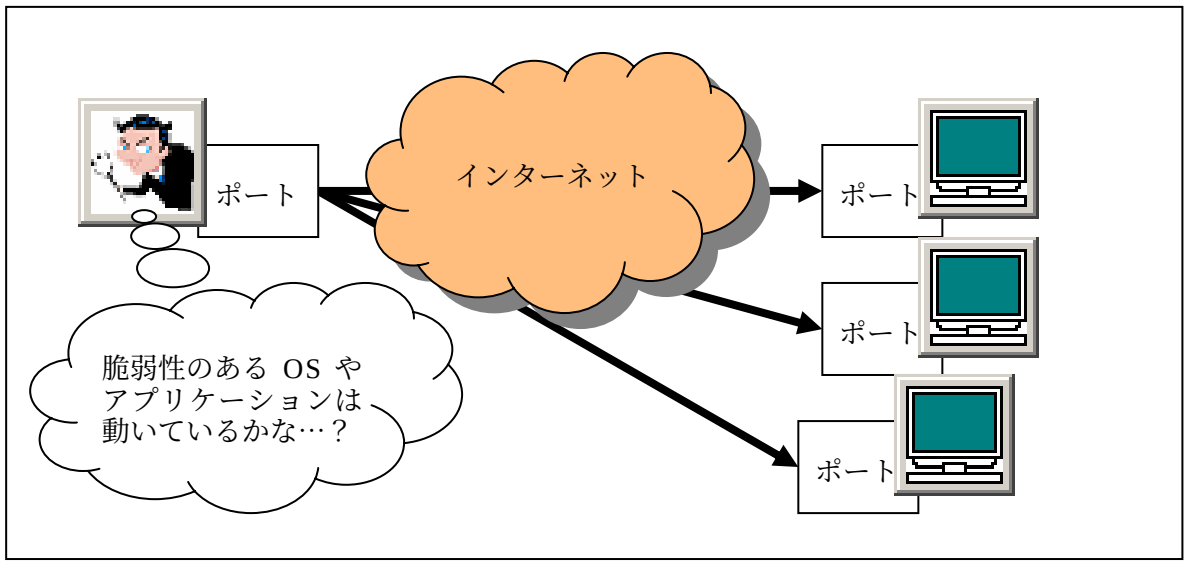
【図 2.1　TALOT2 観測画面の例 アクセス数と発信 IP 数の状況観測画面】

3．インターネットからの期待しないアクセス

インターネットに接続しますと、悪意のある無しに関わらず何らかのアクセスが必ずやってきます。一般的に、インターネット利用者のコンピュータでは、自分から発信したアクセスに対して、インターネットから返信のかたちでアクセスがあるのが普通です。期待しないアクセスとは、自分からのアクセスではなく、一方的にインターネットからくるアクセスのことです。期待しないアクセスは通常、攻撃ツール（プログラム）を利用して自動的に行われますので、個人、法人などに関係なく無差別に、ランダムな IP アドレスに向けて、頻繁に行われます。インターネットに接続している限り、このようなアクセスを受ける可能性があります。

特に多いのが、攻撃・侵入(不正アクセス)の前段階として、標的のコンピュータの各ポート(*3)におけるサービスの状態を調査するポートスキャン(*4)と呼ばれるアクセスです。

特に、最近はワームが蔓延しているため、毎日複数回、何らかのアクセスが来る可能性があります。



インターネットからの期待しないアクセスは、特定のプロバイダに加入していると多いとか少ないとか言うことではなく、先に述べたように、プロバイダから割り振られた IP アドレスに対して、無差別に、ランダムに、頻繁に行われています。

これらのアクセスが狙う(宛先)ポートが開いていない状態であれば、これらのアクセスによるトラブルや被害は起こりません。また、パーソナルファイアウォールやＯＳに付属しているファイアウォール機能で、これらのアクセスを遮断しているのであれば、同様に、トラブルや被害は起こりません。

また、ファイアウォール機能等を利用していない環境でも、**利用者 ID やパスワードの設定や管理が十分であり、コンピュータ上の脆弱性(*5)の解消(例えば Windows Update の定期的な適用)が行われていれば、これらのアクセスからのトラブル防止を行うことができます。**

インターネットの利用者の皆さんには、状況をご理解いただき、適切な対策を講じていただきたいと思います。

4．不正なアクセスへの加担

次のような理由でウイルス(ワーム(*7)やトロイの木馬(*8)を含む)に感染した場合、今度は、**皆さんが不正アクセスの踏み台にされる場合があります。**

- ウイルス付きのメール
- インターネットからの不正なアクセス
- 不適切なサイトの閲覧あるいは不適切なプログラムのダウンロード
- ピアツーピア(*9)でのファイル交換による不適切なプログラムのダウンロード

このような状況になると、ご自身のコンピュータのトラブルや被害だけでなく、他のインターネット利用者の方へも迷惑をかけることになります。

現在、インターネット上に流れている多くの期待されないアクセスは、一部のクラッカー(*6)のアクセスよりも、こういったウイルスに感染したコンピュータから発信されているアクセスのほうがはるかに多いと言われています。

後述する【図 5.3　2005 年 1 月のアクセス発信地域の状況】を見ていただいても、期待しないアクセスの実に **70%以上が国内のコンピュータから発信**されています。ただし、一般的に攻撃ツールが使われた不正なアクセスの場合、発信側と受信側(ターゲット)は IP アドレスが近いところが狙われる傾向にあり、近しい IP アドレスを持つ海外の発信元もあるわけです。

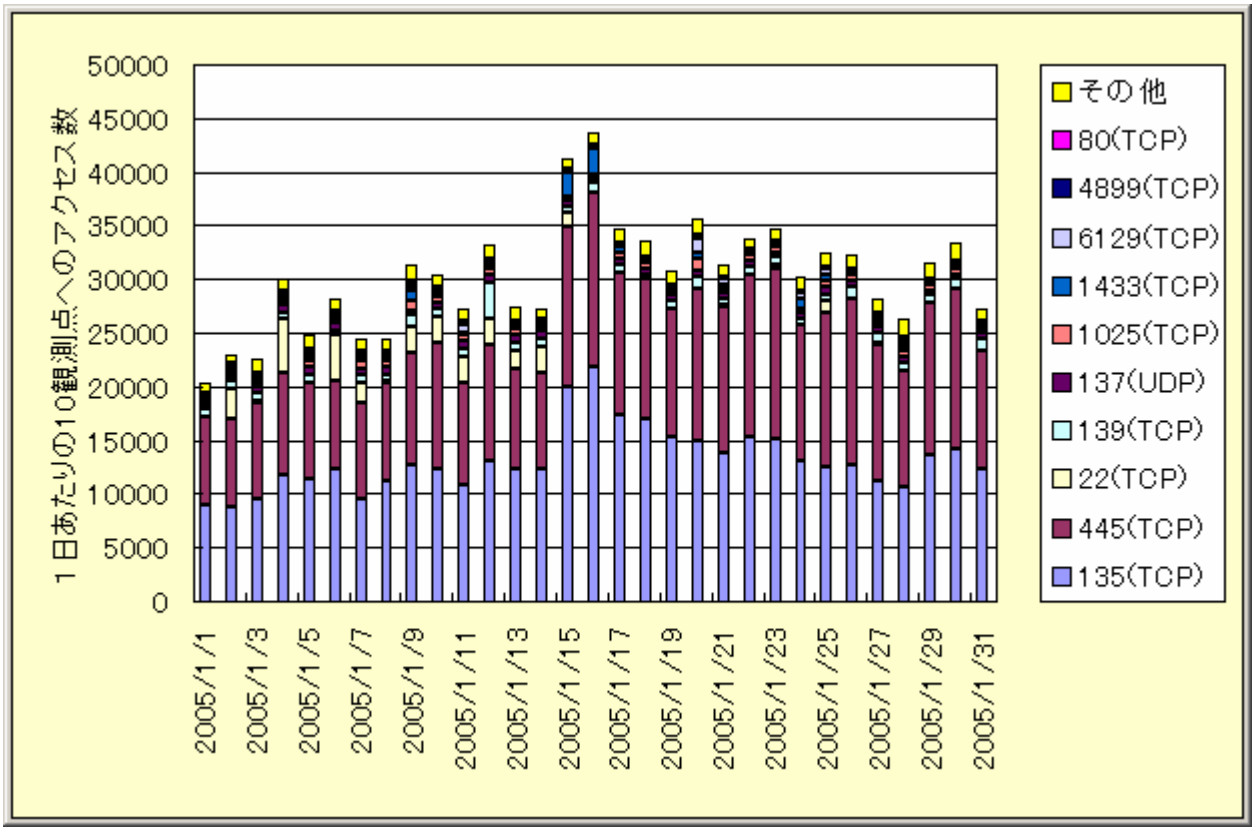
このような状況では、皆さんのコンピュータも踏み台にされている可能性があります。不正アクセスを未然に防ぐ対策も必要ですが、既に感染してしまっているかどうかの確認も重要です。感染しているかの確認には、最新のウイルス定義ファイルが取り込まれたウイルス対策ソフトによる検査や、ウイルス対策ソフトのベンダーから提供されている無償のオンラインウイルス検査を利用することをお勧めします。

i) トレンドマイクロ On-Line Scan
   http://www.trendmicro.co.jp/hcall/scan.htm
ii) シマンテック Security Check
   http://www.symantec.com/region/jp/securitycheck/index.html
iii) マカフィー・フリースキャン
   http://www.mcafeesecurity.com/japan/mcafee/home/freescan.asp

5．1 月のアクセス状況

1 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 908,934 件ありました。単純計算でも、**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。**

アクセス状況について以下のグラフ(1/1～1/31 の 1 日毎の 10 観測点へのアクセス数の変化)に示します。



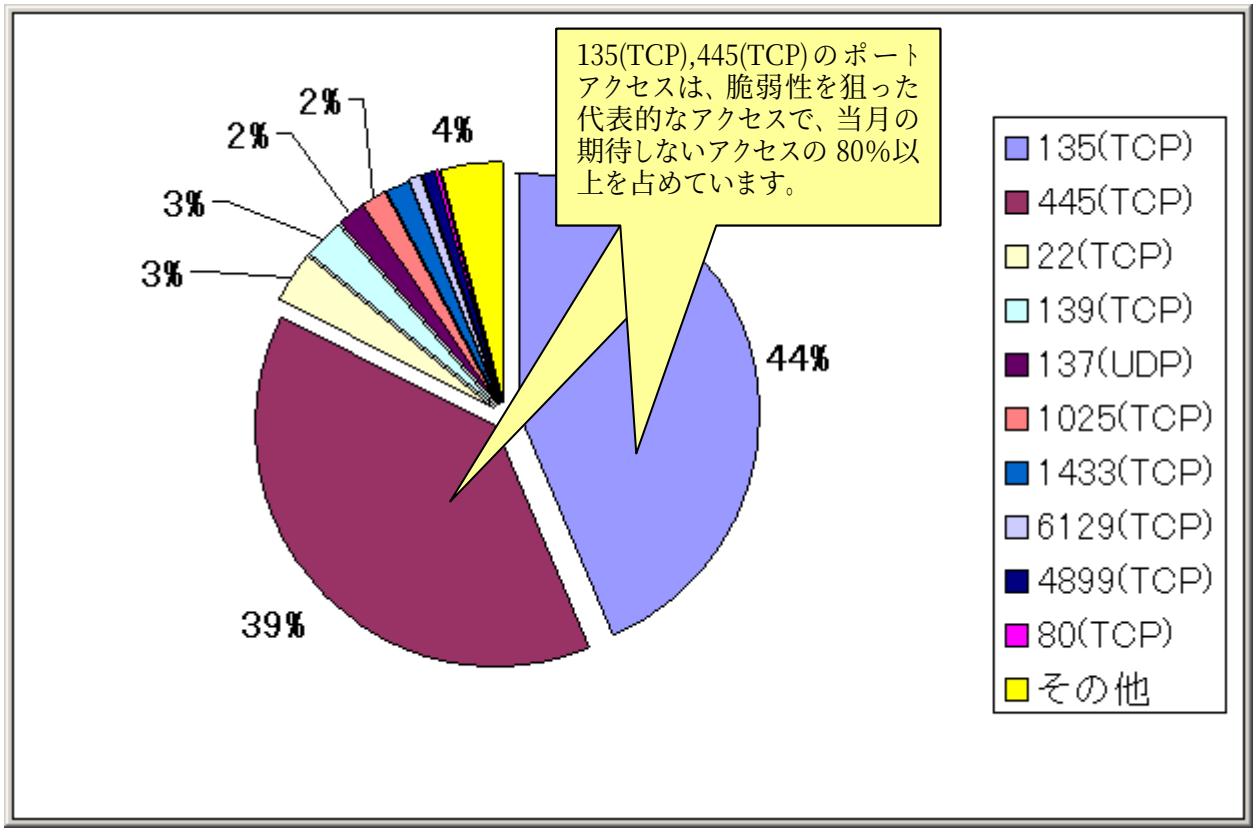
【図 5.1　2005 年 1 月のアクセス数の変化状況】

2004 年 3 月以降、ボット系と呼ばれるワーム(トロイの木馬)が猛威を振るっており、グラフに示されたほとんどのポート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。ボット系のワームは、標的となるコンピュータの OS やアプリケーションの脆弱性を狙っています。ボット系のワームに感染すると、上記のような不正アクセスを行うだけでなく、感染したコンピュータにバックドア(*10)を仕掛けられ、個人情報等が盗まれたり、コンピュータを乗っ取られたりする場合もあります。

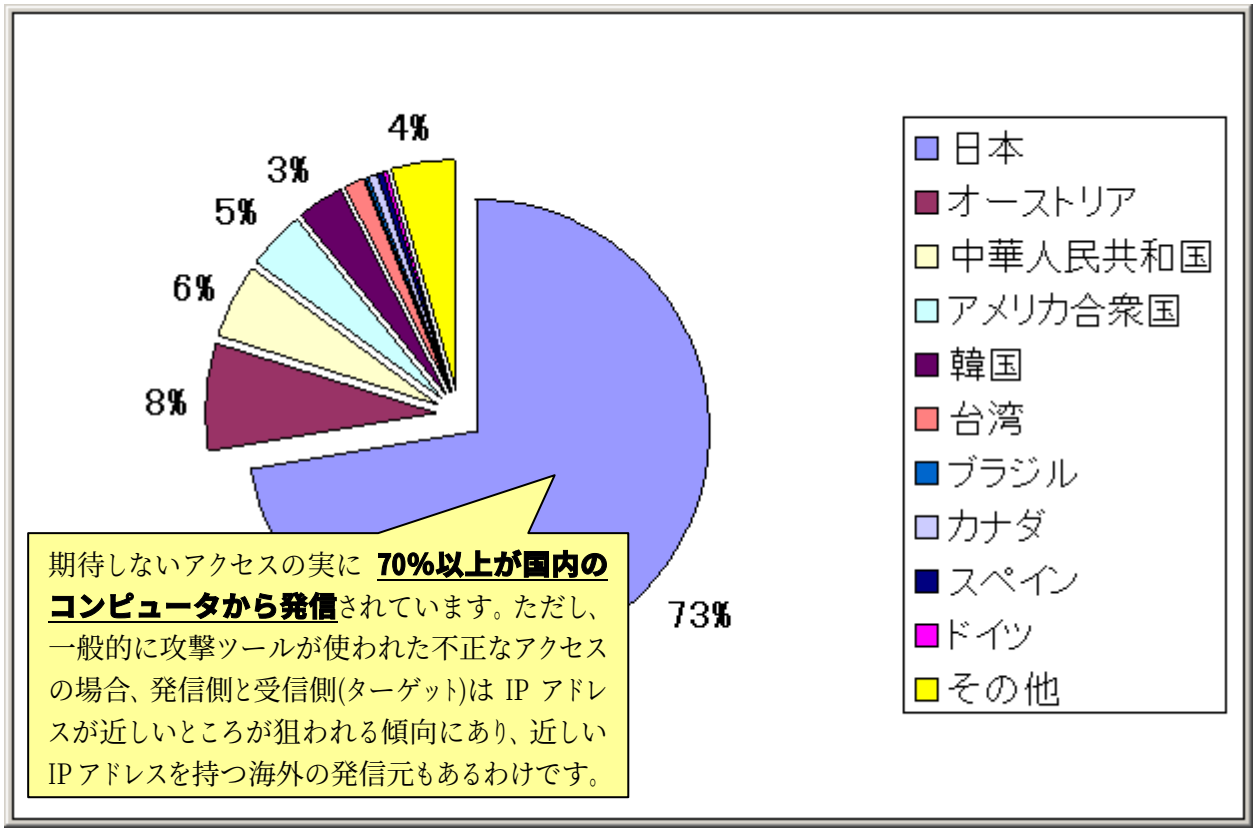
グラフ中の上位の 135(TCP),445(TCP)のポートアクセスは、脆弱性を狙った代表的なアクセスで、当月の期待しないアクセスの 80%以上を占めています(【図 5.2　2005 年 1 月のアクセス種類の比率状況】を参照されたい)。

ただし、グラフ中の 22(TCP)のポートに対するアクセスについては、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 の定点観測環境で開いているポートであるために、集中的な攻撃(パスワードクラッキング攻撃)を受けているものです。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。

今月のアクセス状況からは、ボット系の猛威以外に特に大きな問題となりそうなものは見受けられませんでした。



【図 5.2　2005 年 1 月のアクセス種類の比率状況】



【図 5.3　2005 年 1 月のアクセス発信地域の状況】

『用語の解説』

(*1) 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。

(*2)ログ(log)

コンピュータの利用状況やデータ通信の記録。操作を行った者のIDや操作日時、操作内容などが記録される。

(*3)ポート(port)

IP アドレス（コンピュータ）毎の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。

(*4)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。

(*5)脆弱性(vulnerbility)

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。

(*6)クラッカー（cracker）

一般に攻撃者（attacker）や侵入者（intruder）などの悪者を表現するのに使われています。

(*7)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。

(*8)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。

(*9)ピアツーピア(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、不特定多数の個人間で、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。

(*10)バックドア(backdoor)

コンピュータシステムへの侵入者が侵入後、そのシステムに再侵入するために準備する仕掛け。

・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