IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2005 年 4 月 6 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［2005 年 3 月分］について

新種ウイルス W32/Mytob が出現

●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、2005 年 3 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．コンピュータウイルス届出状況 －詳細は別紙 1 を参照－

3 月の届出件数(*1)は、**4,846 件**となり、2 月の 4,150 件から 16.8%の増加となりました。また、ウイルスの検出数(*2)は、**約 262 万個**と、2 月の約 246 万個から 6.5%の増加となりました。

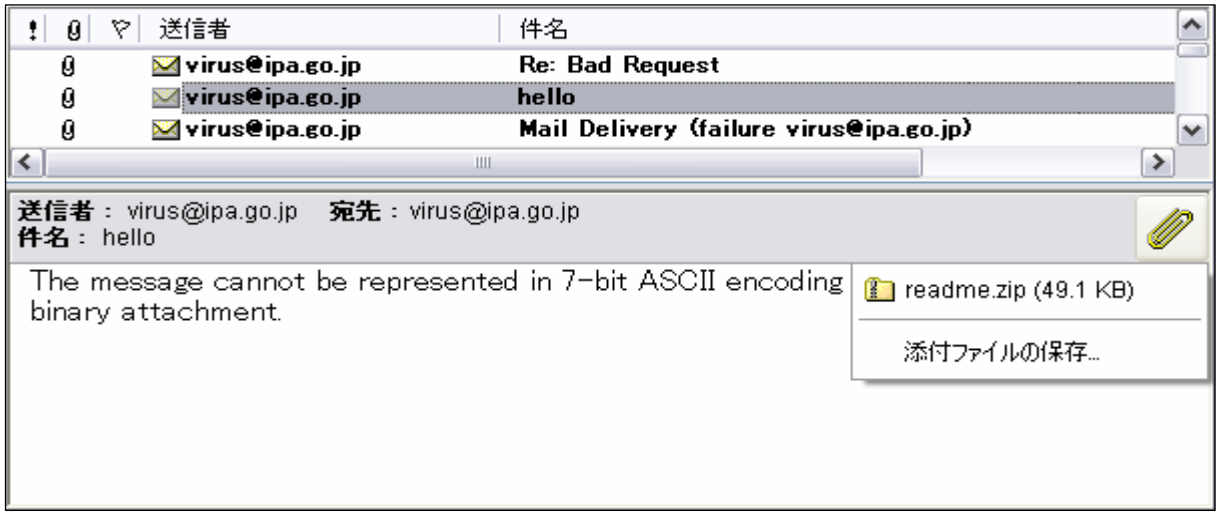
*1 届出件数： 同じ届出者から寄せられた届出の内、同一発見日で同一種類のウイルスの検出が複数ある場合は、1 日何通(個)でも届出 1 件としてカウントしたもの。
*2 検出数 ： 届出にあたり届出者から寄せられたウイルスの発見件数（通数）
・ 3 月は、寄せられたウイルス検出数約 262 万個を集約した結果、4,846 件の届出件数となっています。

W32/Netsky は **1,262 件**となり、13 ヶ月連続で千件を超える届出が寄せられました。続いて、W32/Bagle 484 件、W32/Mydoom 399 件となりました。

（1）新種ウイルス W32/Mytob が出現

3 月に初めて届出が寄せられた **W32/Mytob ウイルス**は、出現してからわずか 1 ヶ月余りで、20 種類以上もの亜種が出現しました。このウイルスは、メールの添付ファイルを介して感染を拡大する機能に加え、**Windows のセキュリティホールを悪用**し、**ネットワークに繋いだだけで感染する**機能を持つウイルスです。また、以下の特徴も有しています。

- バックドアを作成し、**外部からパソコンを操作できるようにする**
- セキュリティ関連企業の**ホームページが閲覧できなくする**
- セキュリティホールを悪用し、**ネットワークに接続しているだけで感染**する



例： W32/Mytob ウイルスのメール受信画面

感染予防対策：

W32/Mytob ウイルスに感染しないためには、**「不審な添付ファイルは開かない」**、**「ウイルス対策ソフトを最新の状態で使用する」**、**「セキュリティホールを解消する（Windows Update を実施する）」**、といった予防対策が必要です。

・ ワクチンソフトに関する情報
http://www.ipa.go.jp/security/antivirus/vacc-info.html
・ マイクロソフト：Windows Update
http://windowsupdate.microsoft.com

もしウイルス対策ソフト等で検査した結果、感染していた場合は、以下のサイトにて無償の駆除ツールが提供されていますので、駆除を実施してください。
なお、**W32/Mytob ウイルスによりサイトにアクセスできない場合**は、感染していないパソコンで駆除ツールをダウンロードし、FD や USB メモリ等でコピーして、感染したパソコン上で実行してください。

駆除ツールを利用した検査および駆除方法（無償）：
（W32/Mytob ウイルスの感染の有無の検査と、感染していた場合の駆除が可能）

・トレンドマイクロ：
http://www.trendmicro.co.jp/esolution/solutionDetail.asp?solutionId=4700
・シマンテック：
http://www.symantec.com/region/jp/avcenter/venc/data/jp-w32.mytob@mm.removal.tool.html

（2）スパイウェアや不正プログラムなどが多数出回る

ウイルスばかりでなく、スパイウェア(キーロガー等)や不正プログラム（バックドア等）などが多数出回っており、誤ってメールの添付ファイルやホームページ上から取り込まないよう以下のような注意が必要です。

1．スパイウェア対策ソフトの活用　（パソコンショップ等で入手可能）
2．不審な Web サイトへのアクセスを避ける
3．ブラウザのセキュリティレベルを高く設定する

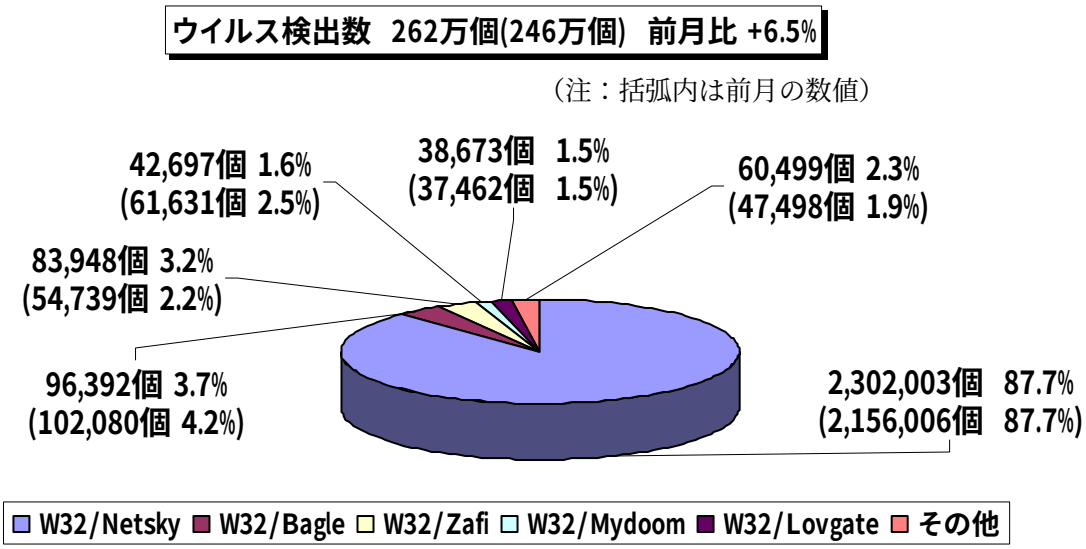
また、不正プログラムの中には、セキュリティホールを突いて侵入してくる場合もあり、Windows Update などでシステムのセキュリティホールを解消しておくことも必要です。

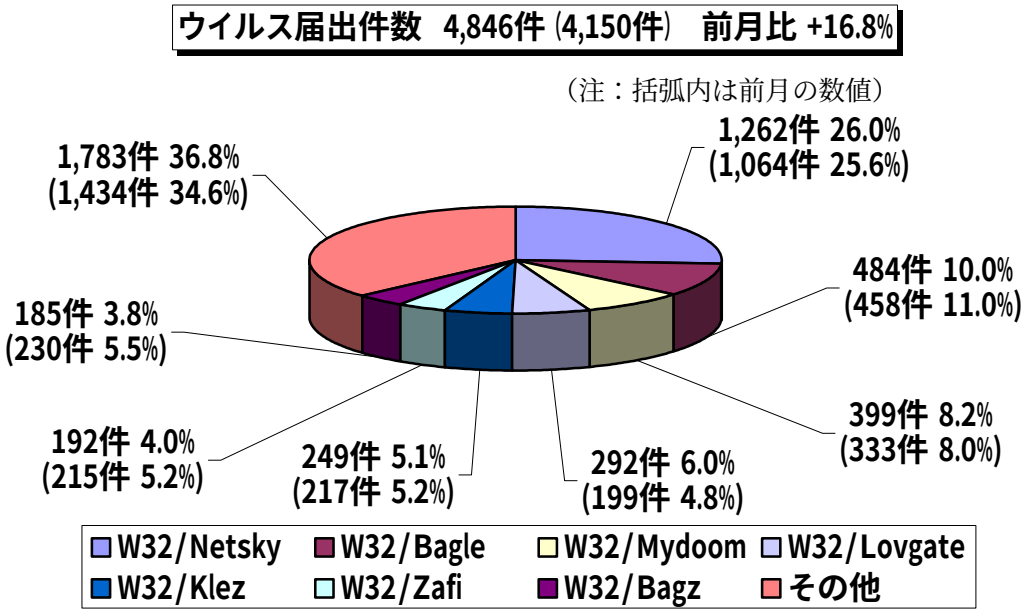
スパイウェアや不正プログラムなどによる主な被害例を下記に示します。（別紙 1. P4 も参照）

被害の内容例	当該不正プログラム等
ブラウザのスタートページを不正な Web サイトに変更されたり、アクセスした Web サイトとは違うサイトに接続されたりする。	Trojan/StartPage Trojan/Websearch
特定の Web サイトから不正なプログラムをダウンロードされ、対象のパソコンにインストールすることでマシンを乗っ取られる。	Trojan/Downloder Trojan/Dropper
侵入したパソコン上からシステム情報やパスワードなどを盗み出され、外部に送信される。	Trojan/PWSteal Trojan/IRC

（3）W32/Netsky が総検出数の約 9 割を占める

W32/Netsky の検出数が**約 230 万個**と、2 月の約 216 万個から 6.4%増加しました。また、全体の検出数（約 262 万個）も増加しておりますが、2 月は日数（28 日間）が少ないことを考慮すると、同水準で推移しているものと推計されます。
（参考：2 月の 28 日間を 31 日間として推計すると、約 270 万個である。）





2．コンピュータ不正アクセス届出状況　―詳細は別紙 2 を参照―

3 月の届出件数は 59 件と 2 月の 63 件と比較して約 6%の減少となりました。しかし、**被害届出件数は 14 件**と 2 月の 9 件より増加しました。

被害届出の内訳は、侵入 9 件、メール不正中継 1 件、その他 4 件（非正規ユーザの正規ユーザ ID 使用によるなりすまし 1 件、不正プログラムの強制ダウンロード 2 件など）でした。

侵入 9 件のうち、**Web サーバが乗っ取られ、フィッシングに悪用されたという被害事例**が 1 月、2 月に引き続き 3 月もありました。

被害事例

I. Web サーバソフトウェアの脆弱性を突かれたりパスワード管理が不備だったりしたために Web サーバに侵入され、フィッシングに悪用することを目的とした偽の Web コンテンツを設置された。

II. SSH (Secure Shell) の ID とパスワードに対する辞書攻撃や OS の脆弱性を突いた攻撃により侵入され、管理者権限パスワードの変更やファイルの改ざんが行われ、踏み台として外部へ攻撃を行われた。

III. PHP を用いた掲示板プログラム「phpBB」の脆弱性を突かれて侵入され、フォーラムログおよびサイトテンプレートが改ざんされたり、削除されたりした。

IV. インターネットのオンラインゲームサービスに不正にログインされ、ゲーム上で使用するアイテムが盗まれたり、追加されたりした。

V. アダルトサイトにアクセスしたところ、年齢認証確認画面と偽って不正なプログラムのダウンロード許可を問う画面が出て、[はい]をクリックしたら不正なプログラムがインストールされた。その後、サイト利用料金の請求画面が強制的かつ断続的に表示されるようになった。

Web サーバ管理者は、サイトがフィッシングへ悪用されないよう注意！

Web サーバに侵入され、フィッシングに悪用するための偽コンテンツを設置されるという被害が相次いでいます。外部からの指摘により初めて気が付くケースが多くなっており、発見の遅れが被害の拡大につながる恐れがあります。

システム管理者が行うべき対策として、

(1) 適切なパスワード設定と管理を行う

(2) 脆弱性を解消する (OS だけではなく、Web アプリケーションなども忘れずに)

(3) 外部からのアクセス制限やセキュリティ設定を適切に行う (不要なサービスも停止する)

(4) こまめなログの確認

(5) 改ざん検知システムの導入

などの対策を行うことが必要です。

(ご参考)

「情報セキュリティ対策実践情報 システム管理者向けのページ」
http://www.ipa.go.jp/security/awareness/administrator/administrator.html

「消費者向け電子商取引サイトの運用における注意点」
http://www.ipa.go.jp/security/vuln/20050304_ec_security.html

3．インターネット定点観測での 3 月のアクセス状況 ―詳細は別紙 3 を参照―

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**ありました。

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、

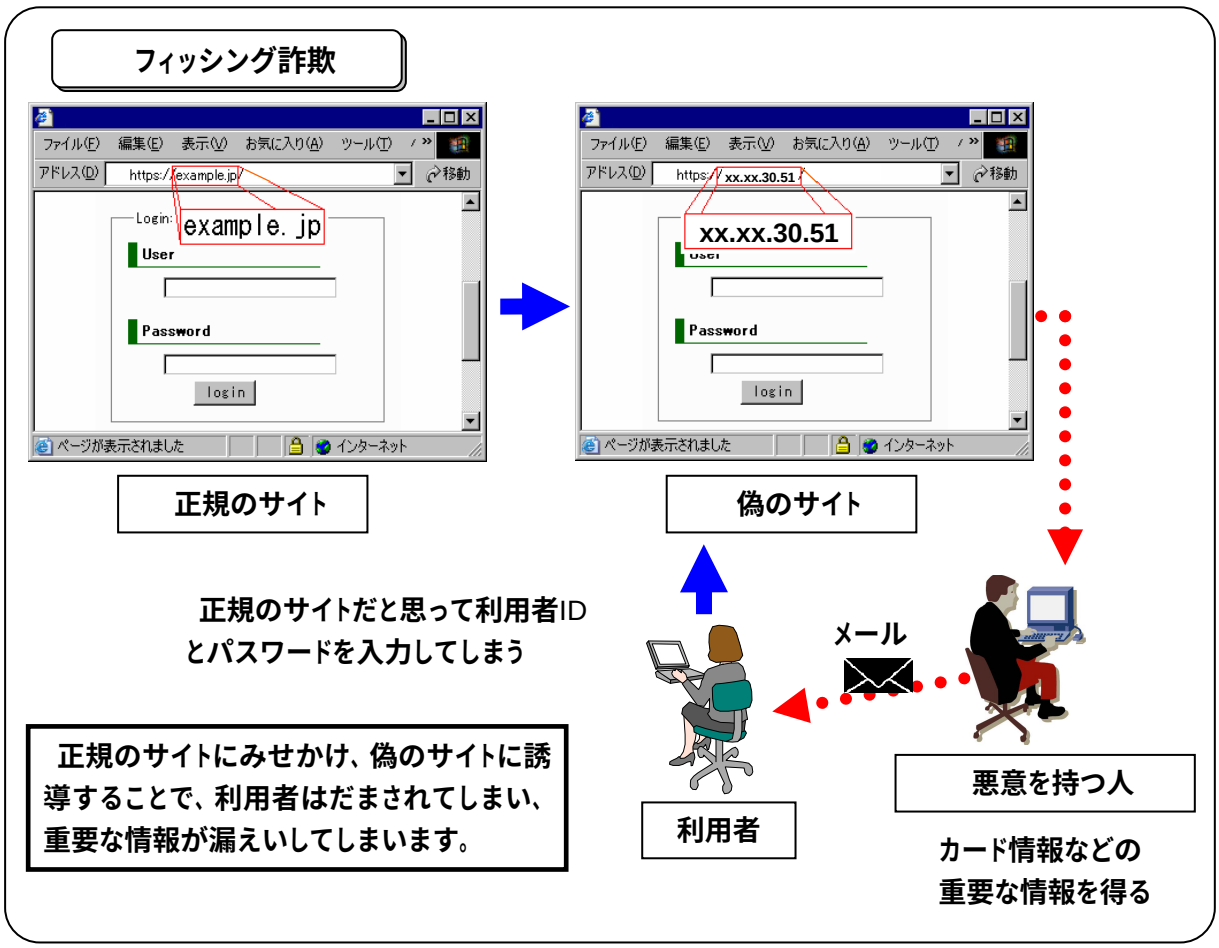
1 日あたりに平均すると、2005 年 1 月：約 3,000 件, 2005 年 2 月：約 2,370 件でしたが、2005 年 3 月にも**約 2,100 件**のアクセスがありました。

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。

4．今月の呼びかけ：「個人情報の漏えいを未然に防ごう！」

―― だまされる前に落ち着いて対処しよう ――

金融機関等の企業が送信者であるメールを装い、メールの受信者に偽のホームページにアクセスするよう仕向け、そのページにおいて個人の金融情報（クレジットカード番号、有効期限、ＩＤ、パスワード等）を入力させるなどして個人情報を不正に入手するような行為である「フィッシング」の発見・被害報告が相次いでいます。



メールを利用したフィッシングでは、受信側で拒否することが難しいのが実情です。しかしながら、メールを受信したユーザが正しい知識を持ち、正しい行動を取ることで未然に防ぐことが出来ます。

ポイント１：　**メールで個人情報を確認する行為自体、通常あり得ない。**

通常、金融機関がクレジットカード番号や有効期限・インターネットバンキングの ID やパスワードなどについて、メールで確認を求めることはありません。不審な点がある場合は、メール本文に書かれているホームページアドレスからではなく、ブックマークなどから本物サイトのトップページにアクセスし、そのような事実があるかどうかチェックしてみましょう。必要に応じて、本物サイトの問合せ窓口などを利用して確認してみるのも良いでしょう。

ポイント２：　**メールの本文中にあるホームページアドレスを安易にクリックしない。**

フィッシングに限らず、悪意を持って設置されている Web サイトには、閲覧するだけで不正なプログラムを埋め込まれてしまうような悪質なものもあります。メール本文に書かれているホームページアドレス（リンク）をクリックする前に、メールそのものが信頼出来るものなのかどうか、チェックしてみましょう。

ポイント３：　**メールの送信元を安易に信用しない。**

送信元メールアドレスの表示は、簡単に偽装されてしまいます。必要に応じて、メールのヘッダ情報などを参照して、送信元情報をチェックすることが出来ます。

また、**ウイルスやワームなどの不正なプログラムの中には、感染するとパソコンの中にある個人情報などを外部に発信してしまうものもあります**。この 4 月からは個人情報保護法が全面施行されることもあり、企業内のパソコンから個人情報が漏えいすることは、企業の信用そのものを傷つけてしまいかねません。個人ユーザにとっても、個人情報が漏えいすることにより、詐欺などのトラブルに巻き込まれることになりかねません。

このような被害を未然に防ぐために、**ウイルス対策ソフトの活用、ソフトウェア（OS、Web ブラウザ、メールソフトなど）の脆弱性解消など、予防対策を継続して行ってください**。

（ご参考）
・ワクチンソフトに関する情報
http://www.ipa.go.jp/security/antivirus/vacc-info.html

・Windows Update（マイクロソフト社）
http://windowsupdate.microsoft.com/

・ソフトウェアアップデート（アップルコンピュータ社）
http://www.apple.co.jp/ftp-info/

・「ブラウジングと電子メールの安全性を強化する」（マイクロソフト社）
http://www.microsoft.com/japan/security/incident/settings.mspx

■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