IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2005 年 7 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 6 月分］について

ファイル交換ソフトに潜むワナ！

●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 6 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。なお、2005 年上半期（1～6 月）の届出状況を別紙 2、4 に集計しました。

1．コンピュータウイルス届出状況 －詳細は別紙 1,2 を参照－

ウイルスの検出数(※1)は、**約 385 万個**と、5 月の約 355 万個から 8.5%の増加となりました。また、6 月の届出件数(※2)は、**4,928 件**となり、5 月の 5,021 件から若干の減少となりました。

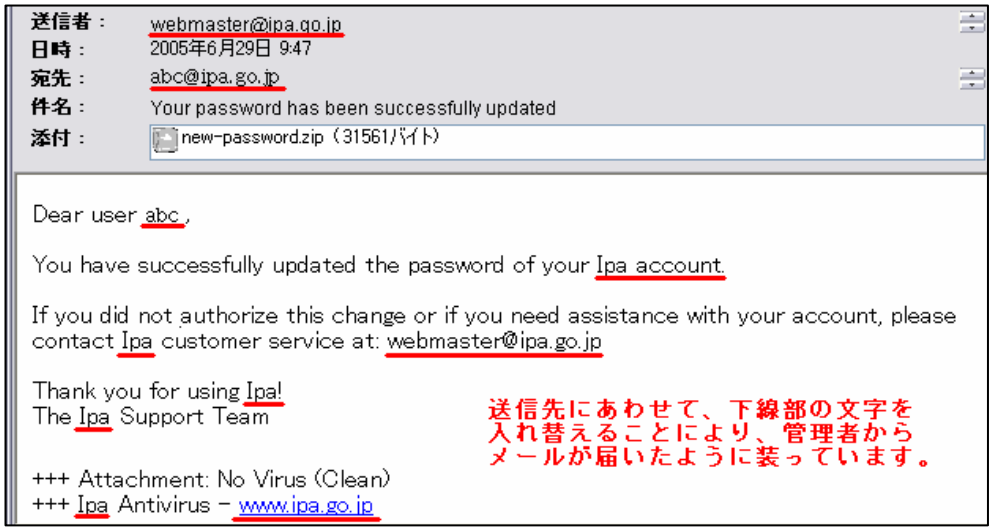
※1 検出数 ： 届出にあたり届出者から寄せられたウイルスの発見件数（通数）
※2 届出件数： 同じ届出者から寄せられた届出の内、同一発見日で同一種類のウイルスの検出が複数ある場合は、1 日何通(個)でも届出 1 件としてカウントしたもの。
・6 月は、寄せられたウイルス検出数約 385 万個を集約した結果、4,928 件の届出件数となっています。

W32/Netsky の検出数は、**総検出数の 7 割を占める約 265 万個**（届出件数 **1,122 件**）となり、16 ヶ月連続でトップの届出が寄せられました。続いて、**急増している W32/Mytob 約 94 万個（699 件）**、W32/Sober 約 10 万個（54 件）、W32/Bagle 約 4 万個（316 件）となりました。

また、度々発生している**ファイル交換ソフトによる情報漏えい**の事象を受け、6 月には緊急対策情報を公開しました。

（1）W32/Mytob の亜種の巧妙な手口に注意！

3 月に出現して以降、次々に亜種が発生している **W32/Mytob** ウイルスに、新たなタイプが現れました。このウイルスは、以下のようなウイルスメールを送りつけ、システム管理者であるかのような送信者名を詐称し、パスワード更新などシステム管理に関する情報提供であるように見せかけるなどにより、あたかも組織の管理者から送信されたように装っています。



このようなメールを受信した場合、

(i) 安易に添付ファイルを開かない
(ii) ウイルスチェックをし、ウイルスかどうかを確認する
(iii) 送信の事実があるか、組織の管理者へ確認する

といった注意を払い、被害を未然に防ぐようにしましょう。

（2）W32/Netsky が総検出数の約 7 割！　W32/Mytob が急速に増加！

W32/Netsky の検出数が**約 266 万個**と、5 月の約 289 万個から約 8.0%の減少となりました。しかし、継続して亜種が出現している **W32/Mytob** の検出数が、5 月の約 45 万個から約 94 万個へと 2 倍以上に増加しました。それにより、全体の検出数（約 385 万個）も 8.5%の増加となりました。

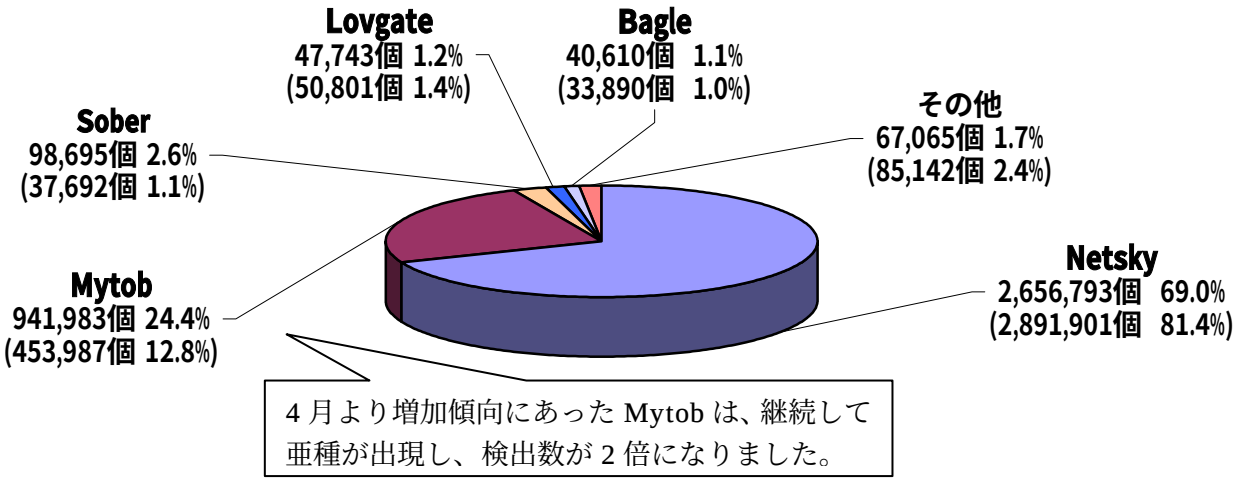
W32/Mytob は、3 月に出現してから **4 ヶ月余りの期間に 70 種類を超える亜種**が発生しています。これに対して **W32/Netsky** は、出現から **4 ヶ月で約 20 種類の亜種**の発生でしたので、W32/Mytob は 3 倍以上も多い状況となっています。このように亜種が短期間に多数発生することは、当該ウイルスの感染の拡大および蔓延につながりますので、注意が必要です。

亜種とは？

亜種とは、最初に発見された元のウイルス(原型)に対して機能の追加や動作を変更するなどの改変がなされ、作り出されたものです。ウイルス定義ファイル(パターンファイル)を更新しないと新しい亜種に対応できず、検出することができないケースがほとんどですので、ウイルス対策ソフトを常に最新の状態に保つことが重要です。

ウイルス検出数　385万個(355万個)　前月比 +8.5%

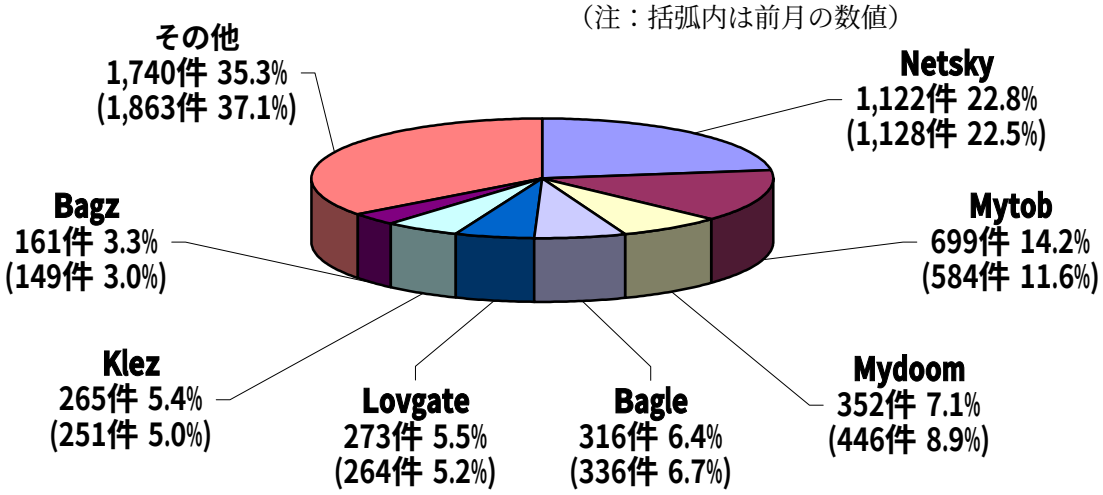
（注：括弧内は前月の数値）



4 月より増加傾向にあった Mytob は、継続して亜種が出現し、検出数が 2 倍になりました。

ウイルス届出件数　4,928件 (5,021件)　前月比 -1.9%

（注：括弧内は前月の数値）



2．コンピュータ不正アクセス届出状況　－詳細は別紙 3,4 を参照－

6 月の届出件数は 24 件であり、5 月の 94 件と比較して約 75%の減少となりました。そのうち**被害のあった件数は 22 件**であり、5 月の 11 件から倍増しました。

また、不正アクセスに関連した相談件数は 37 件（うち 2 件は届出件数としてもカウント）であり、そのうち被害のあった件数は 22 件でした。

（1）被害状況

被害届出の内訳は、**侵入 10 件、メール不正中継 2 件、ワーム感染 3 件、DoS 4 件、アドレス詐称 1 件、その他(被害あり)2 件**でした。侵入 10 件のうち、**Web サーバに侵入され Web コンテンツを改ざんされたという被害事例**が 5 件ありました。そのうち、**利用者がホームページを閲覧しただけでウイルスに感染する仕組みを埋め込まれていた事例**が 5 月に引き続き 2 件ありました。

被害事例

[侵入]

(i) Web サーバに侵入され、利用者が Web コンテンツを閲覧しただけで、不正なプログラムをダウンロードさせられるサイトへ誘導されてしまう仕組みを埋め込まれているのを発見。一度修正したが、その後再度同様の改ざんを受けていることが発覚。レンタルサーバを利用しており原因究明が難航したが、サーバ上で動作させていた掲示板プログラム「phpBB(*1)」の脆弱性を突かれたものと思われる。**（解説、対策については 2．(2)参照）**

(ii) Web サーバ上のプロセス一覧に不審なものを発見し調査したところ、バックドアが仕掛けられているのを発見。サーバ上で動作させていた cgi(*2)の脆弱性を突かれたのが原因と思われる。**（解説、対策については 2．(2)参照）**

(iii) 一般ユーザ権限で Web サーバに侵入され、さらにサーバ内部で管理者権限を奪取され、ファイルを改ざんされた。全てのログが削除されており、侵入後の行動については不明。最初に侵入を許した原因は、ログイン ID とパスワードの管理不備。管理者権限を奪取された原因は、Linux の既知の脆弱性を突かれたのが原因と思われる。**（解説、対策については 2．(3)参照）**

[DoS]

(iv) 通信障害が起きたため調査したところ、少なくても 1 秒間に 100 万パケット以上の SYN フラッド攻撃(*3)を受けていることが判明。ルータの使用率が 100%となり、通信が不能となった。ルータの DoS 攻撃対策機能を駆使しても対応し切れず、最終的にはプロバイダに対して、該当 IP アドレス宛のパケットを全て破棄する設定を施してもらい回復した。**（解説、対策については 2．(4)参照）**

[アドレス詐称]

(v) spam(*4)メールを受け取ったというクレームがあり調査したところ、差出人を自組織のアドレスと詐称された迷惑メールが大量に配信されているらしいことが判明。さらに、それらのメールが宛先不明のエラーのため、自組織宛に大量のリターンメールが届いた。

[その他]

(vi) Web サーバ上で運用しているオンラインゲームで、不正なデータ(ゲームのスコア情

報)を cgi に送信された。その結果、一般利用者が閲覧可能なランキング表に不正なスコアが表示されてしまった。幸い、サーバへの侵入は確認されなかった。スコア情報のやり取りは暗号化や比較チェックなどの処理がされていたが、そのロジックが解析されてしまったのが原因と推測される。**（解説、対策については 2．(2)参照）**

（2）Web アプリケーションの運用について再度確認！

被害事例(i)、(ii)、(vi)では、**Web アプリケーションの脆弱性を突かれての被害となっています。**Web アプリケーションの脆弱性を突かれると、データベース改ざんや個人情報漏えいなどの大規模な被害につながる恐れがあります。**Web サーバのセキュリティ対策やサーバが設置されているネットワークのセキュリティ対策のみならず、サーバ上で動作する Web アプリケーションのセキュリティ対策も抜かりなく実施しましょう**。

(ご参考)
「ウェブサイトのセキュリティ対策の再確認を ～脆弱性対策のチェックポイント～」
http://www.ipa.go.jp/security/vuln/20050623_websecurity.html

（3）ID、パスワードやユーザの管理について再確認！

被害事例(iii)では、**単純なパスワードを設定していた一般ユーザが居たために簡単にサーバに侵入を許してしまいました**。さらに、ネットワーク内部でサーバ OS の脆弱性を悪用され、管理者権限も奪取されてしまいました。このように、**一箇所でもセキュリティホールが残っていると、その他のセキュリティ対策が意味の無いものになってしまいます**。外部から接続可能になっている一般ユーザの ID やパスワードに関しても設定内容には十分な注意を払うとともに、**パスワードの複雑度チェックや定期的更新を促すような仕組み、通信経路の暗号化などを実施することが有効な対策となるでしょう**。

(ご参考)
「たかがパスワード、されどパスワード」(一般ユーザ向け)
http://www.ipa.go.jp/security/crack_report/20020606/0205.html
「パスワードの管理と注意」(システム管理者向け)
http://www.ipa.go.jp/security/fy14/contents/soho/html/chap1/pass.html
「日本の Linux 情報」 - バグ･セキュリティ情報 -
http://www.linux.or.jp/

（4）DoS 攻撃を受けた際の対応について再確認！

被害事例(iv)では、DoS 対策機能を備えた比較的高性能なルータを使用していたにもかかわらず、回線を管理する上位プロバイダにパケット破棄を依頼するしか手立てがありませんでした。この事例の他にも、短時間に大量のメールを送られたり Smurf 攻撃(*5)を受けたり、といった届出がありました。普段から、攻撃を受けた際の対応を想定しておくことが重要です。また、IDS(*6)や IPS(*7)といった、セキュリティシステムを導入するのも有効な対策となるでしょう。

(ご参考)
CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks
http://www.cert.org/advisories/CA-1996-21.html
CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks
http://www.cert.org/advisories/CA-1998-01.html

3．インターネット定点観測での 6 月のアクセス状況　―詳細は別紙 5 を参照―

インターネット定点観測(TALOT2)によると、2005 年 6 月の期待しない（一方的な）アクセスの総数は、10 観測点で **454,153 件**ありました。1 観測点で 1 日あたり**約 1,500 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。

これらの一方的なアクセスが最も脅威となるのは、コンピュータを無防備な状態（ルータやファイアウォール機器で守られていない状態）でインターネットに直結した場合です。

止むを得ず直結する場合は、つなぐ前に、以下に示す対策を、必ず実施してください。

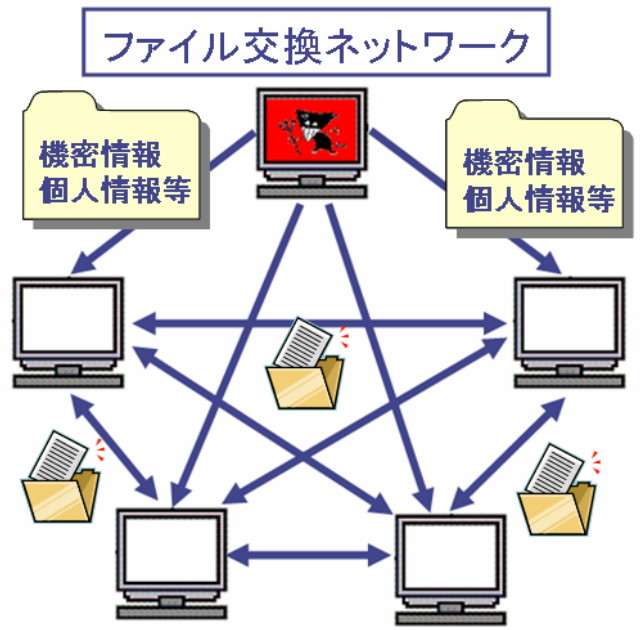
- **OS にファイアウォール機能が搭載されている場合は、その機能を正しく動作させる**
- **OS にファイアウォール機能が搭載されていない場合は、できる限り、パーソナルファイアウォールアプリケーションを導入し、正しく動作するように設定する**
- **コンピュータの OS やアプリケーションを最新の状態にする(例えば Windows Update の実施)**
- **不必要なファイル共有指定を外す**

4．今月の呼びかけ：「 ファイル交換ソフトに潜むワナ！ 」

―― 情報の管理は万全ですか？ ――

Winny に代表されるようなファイル交換ソフトによる、情報漏えいが度々発生しています。漏えいが起きた原因のほとんどは、Winny を悪用する **W32/Antinny** というウイルスに感染してしまったからです。

W32/Antinny は、ファイル交換ソフトを通じて、感染を拡大します。このウイルスに感染すると、パソコン内の Word や Excel 等のファイルが公開されてしまいます。これにより、ファイル交換ソフトのユーザであれば、誰もが入手可能となり、情報が漏えいしてしまうことになります。



不特定多数が接続しているネットワークに流出したら
回収は事実上不可能

ウイルスに感染しないためのウイルス対策はもちろんですが、使用している**パソコン内の情報が不特定多数のユーザに閲覧可能な状態になる危険性を認識**し、ファイル交換ソフトの使用について、問題点がないか確認することをお勧めします。

（ご参考）ファイル交換ソフト使用上の注意事項
http://www.ipa.go.jp/security/topics/20050623_exchange.html

『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://www.trendmicro.com/jp/
マカフィー株式会社：http://www.mcafee.com/jp/default.asp

『用語の解説』

(*1) phpBB
スクリプト言語 PHP で作成された、電子掲示板プログラムのこと。Web アプリケーションの一種。

(*2) cgi （Common Gateway Interface）
Web サーバが、クライアントからのリクエストに応じて Web サーバ上で外部プログラムを動作させ、その処理結果をクライアントに送信するための仕組みのこと。

(*3) SYN フラッド攻撃 （SYN flooding attack）
サーバの機能を低下させたり停止させたりする DoS 攻撃の手法の一つで、TCP の接続手順を悪用したもの。

(*4) spam
ジャンクメール、バルクメール、また単に「迷惑メール」とも呼ばれる。商用目的かどうかによらず、宣伝や嫌がらせなどの目的で不特定多数に大量に送信されるメールのこと。

(*5) Smurf 攻撃
DoS 攻撃（サービス妨害攻撃）のひとつ。ICMP における「指図されるブロードキャスト（directed broadcast）」の機能を悪用する。ICMP エコー要求パケットの発信元のアドレスに標的の IP アドレスを設定し、宛て先にブロードキャストアドレスを設定して送信することにより、このパケットを受け取った多数のホストが一斉に標的のホストに ICMP エコー応答パケットを送りネットワーク帯域の渋滞をもたらす。攻撃者が利用する攻略プログラムのひとつの名前にちなんで、Smurf Attack と呼ばれている。

(*6) IDS （Intrusion Detection System）
システムに対する侵入／侵害を検出･通知するシステムのこと。 システムを監視し、セキュリティポリシーを侵害するような行為を検出した場合に、その行為を可能な限り早く管理者に伝えるとともに、調査分析の作業を支援するために必要な情報を保存･提供することが目的である。

(*7) IPS （Intrusion Prevention System）
システムに対する侵入／侵害を阻止するシステムのこと。異常を検知した際に自動的に通信を停止する機能を有したものであり、一般的には IDS の発展形と言える。

■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