IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2005 年 5 月 10 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 4 月分］について

W32/Mytob ウイルスの亜種が大量に出現！！

●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 4 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－

4 月の届出件数(*1)は、**4,440 件**となり、3 月の 4,846 件から 8.4%の減少となりました。また、ウイルスの検出数(*2)は、**約 338 万個**と、3 月の約 262 万個から 29.0%の増加となりました。

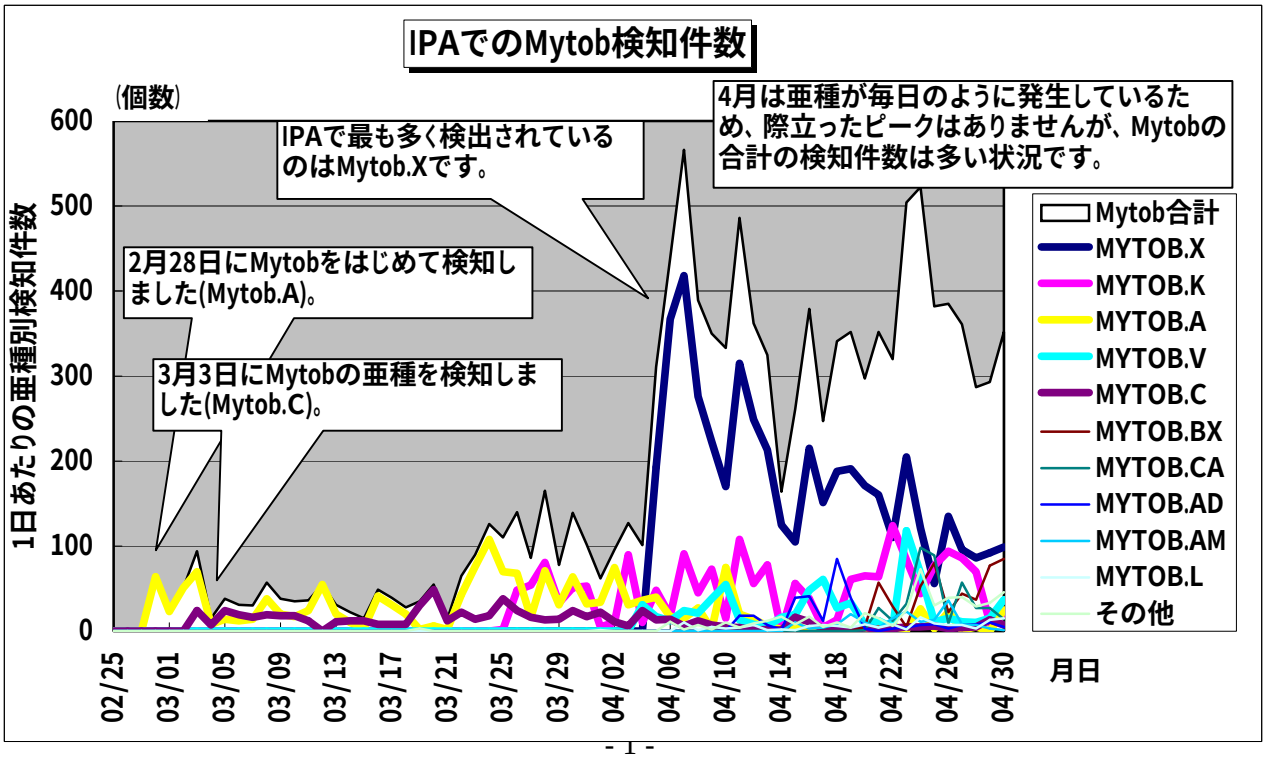
*1 届出件数： 同じ届出者から寄せられた届出の内、同一発見日で同一種類のウイルスの検出が複数ある場合は、1 日何通(個)でも届出 1 件としてカウントしたもの。
*2 検出数 ： 届出にあたり届出者から寄せられたウイルスの発見件数（通数）
・4 月は、寄せられたウイルス検出数約 338 万個を集約した結果、4,440 件の届出件数となっています。

W32/Netsky は **1,009 件**となり、14 ヶ月連続でトップの届出が寄せられました。続いて、W32/Mydoom 377 件、W32/Bagle 330 件、W32/Mytob 302 件となりました。

（1）W32/Mytob の亜種が大量出現！

3 月に初めて届出された **W32/Mytob ウイルス**は、多数の亜種が短期間に出現し、現在（5/10）までに 70 種類以上となっています。1 日平均 1 種類が出現している計算になりますが、実際は 4 月にその多くが出現し、1 ヶ月で約 50 種類となっています。（届出の大多数を占めている W32/Netsky 出現時よりも、短い期間に多数の亜種が出現しています。）

その多くの亜種の中で、IPA では、4 月初めに出現した Mytob.X の検出数が最も多くなっています。



亜種が短期間に出現すると、**ウイルス定義ファイル（パターンファイル）が対応する前に、新しいウイルスの亜種を受信する可能性が高くなります**。ウイルス対策ソフトで検出されないからといって、添付ファイルを開くと、ウイルスに感染してしまいます。
こまめにウイルス定義ファイルを更新することを心がけ、それでも怪しい添付ファイルは開かない等、予防対策を継続して実施してください。

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。

W32/Mytob 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、コンピュータを**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。
感染すると、以下の活動を行います。特にバックドアから侵入された場合は、**ファイルの削除や不正プログラムの埋め込みなど、様々な被害が発生する危険性**があります。

(i)　大量のウイルスメールを送信する（マスメール型）
(ii)　バックドアを仕掛け、外部からパソコンを操作できるようにする
(iii) ワクチンベンダー等のホームページの閲覧を妨害する

W32/Mytob ウイルスに感染しないためには、

(i)　不審な添付ファイルは開かない
(ii)　ウイルス対策ソフトを最新の状態で使用する
(iii) セキュリティホールを解消する（Windows Update を実施する）

といった予防対策を実施してください。

・　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

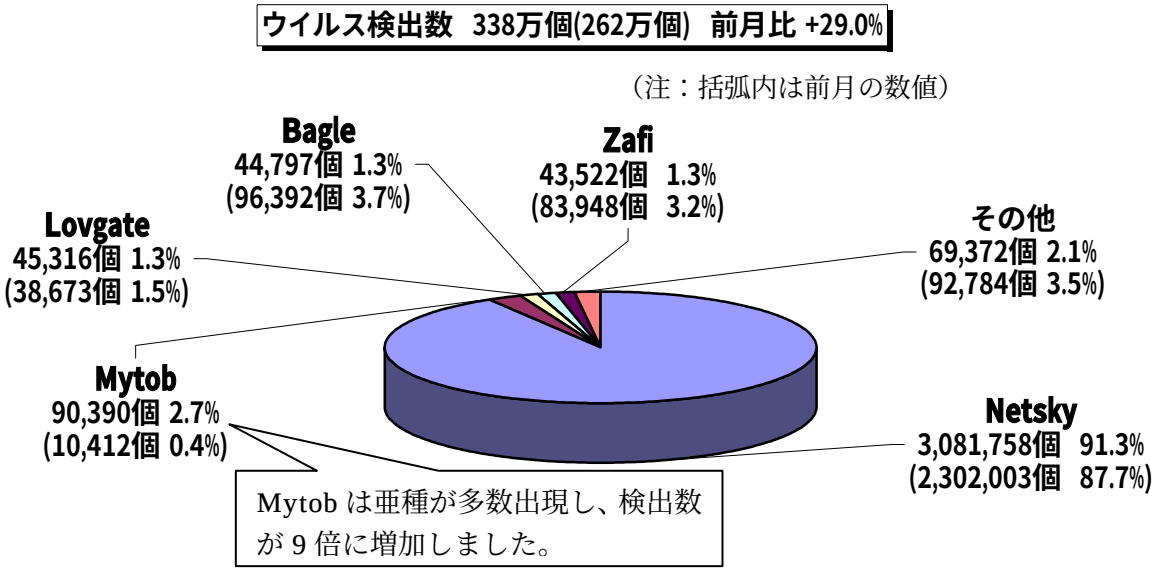
もしウイルス対策ソフト等で検査した結果、感染していた場合は、以下のサイトにて無償の駆除ツールが提供されていますので、駆除を実施してください。
なお、**W32/Mytob ウイルスによりサイトにアクセスできない場合**は、感染していないパソコンで駆除ツールをダウンロードし、FD や USB メモリ等でコピーして、感染したパソコン上で実行してください。

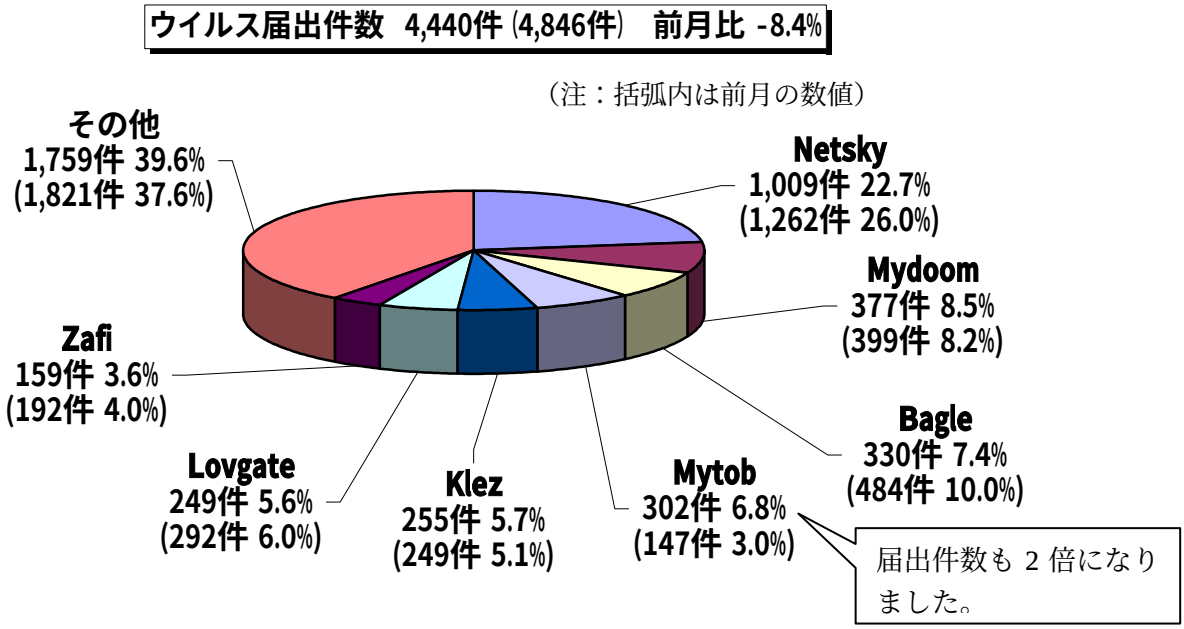
駆除ツールを利用した検査および駆除方法（無償）：
（W32/Mytob ウイルスの感染の有無の検査と、感染していた場合の駆除が可能）

・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）W32/Netsky が総検出数の約 9 割を占める

W32/Netsky の検出数が**約 308 万個**と、3 月の約 230 万個から 33.9%の増加となりました。また、全体の検出数（約 338 万個）も 29%の増加となりました。





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―

4 月の総届出件数は 48 件であり、3 月の 59 件と比較して約 19%の減少となりました。そのうち**被害のあった件数は 24 件**であり、3 月の 14 件より約 71%増加しました。

（1）被害状況

被害届出の内訳は、**侵入 8 件、DoS 8 件、アドレス詐称 1 件、その他 7 件**（成りすまし 1 件、不正プログラムの埋め込みの疑い 4 件、不正なネットワークモニタリングの疑い 2 件）でした。

侵入 8 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 3 件あり、内 1 件は日中情勢に関連してサイバー攻撃を受けたと思われるものでした。

被害事例

[侵入]

(i) OS(Windows や Linux など)の脆弱性を突かれてサーバに侵入され、不正にファイルを置かれたりレジストリを変更されたりした。

(ii) サーバ内に不正なアカウントを作成され、さらに不正なプログラムファイルを置かれて動作させられていた。

(iii) 管理者権限を不正に奪取されて Web サーバに侵入され、不正にファイルを置かれたり Web ページを改ざんされたりした。データベースシステムに対する SQL(*1)インジェクション攻撃(*2)が原因。

[DoS]

(iv) SSH(*3)で使用するポート(*4)への不正なアクセスが多発したため、サーバがダウンした。

[成りすまし]

(v) インターネットオークションで ID･パスワードを、本人に成りすまされて使われ、不正に商品を落札された。

[不正プログラム埋め込みの疑い]

(vi) 不正なプログラムがいつの間にか埋め込まれており、意図しないインターネット接続が実行されようとしていた。パソコンの設定を変えられていたり、見覚えの無いフォルダが作成されていたりした。

(2) Web アプリケーションの運用に注意！

データベースシステムに対する **SQL インジェクション攻撃によって管理者権限を奪取され、Web ページを改ざんされた被害**では、**Web アプリケーションによる、利用者からの問合せデータ(クエリ)内容チェックが不完全であるという脆弱性があったことが根本的な原因**となりました。攻撃者がその脆弱性を突くために、問合せデータ中に、管理者用ユーザ ID のパスワードを変更するような不正な SQL 文を意図的に混ぜ込んでいたものと思われます。この例に限らず、利用者からの入力を受け付ける Web アプリケーションでは、利用者の入力内容に対するチェックが妥当かどうか、再確認しましょう。

(ご参考)
「セキュアプログラミング講座」
http://www.ipa.go.jp/security/awareness/vendor/programming/intro.html

(3) ID やパスワードを盗まれないように！

インターネットオークションで使う ID･パスワードを不正に使われた被害では、住所、氏名やネット決済情報などの個人情報も同時に入手されていたと推測され、さらに被害が拡大する恐れがありました。原因として、ID･パスワードの設定不備や管理不備といった理由の他に、最近では不正なプログラムによってキー操作が読み取られてしまうこともあります。

こうしたリスクを少しでも回避するために、**自分が普段使っていないパソコンでの、個人情報の入力や ID・パスワードの入力が必要なページの閲覧は、控えるべき**でしょう。特に、

インターネットカフェなど、公共の場に設置されているパソコンでの、そのようなページの閲覧は、避けましょう。

（4）Web サーバの管理を怠りなく！

Web サーバに侵入され、Web コンテンツを改ざんされたり不正なプログラムを埋め込まれたりする被害が相次いでいます。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て二次被害が生じる可能性もあります。特に最近は、政治的な理由から無差別にサイバー攻撃を受ける可能性も高まっているようです。

しかし、これらの被害は、**管理者の ID やパスワードの管理、OS や Web アプリケーションのセキュリティパッチ適用など、基本的な対策で防げることがほとんど**です。被害の拡大を防ぐためにも、改めてサーバ管理を再確認しましょう。

（ご参考）

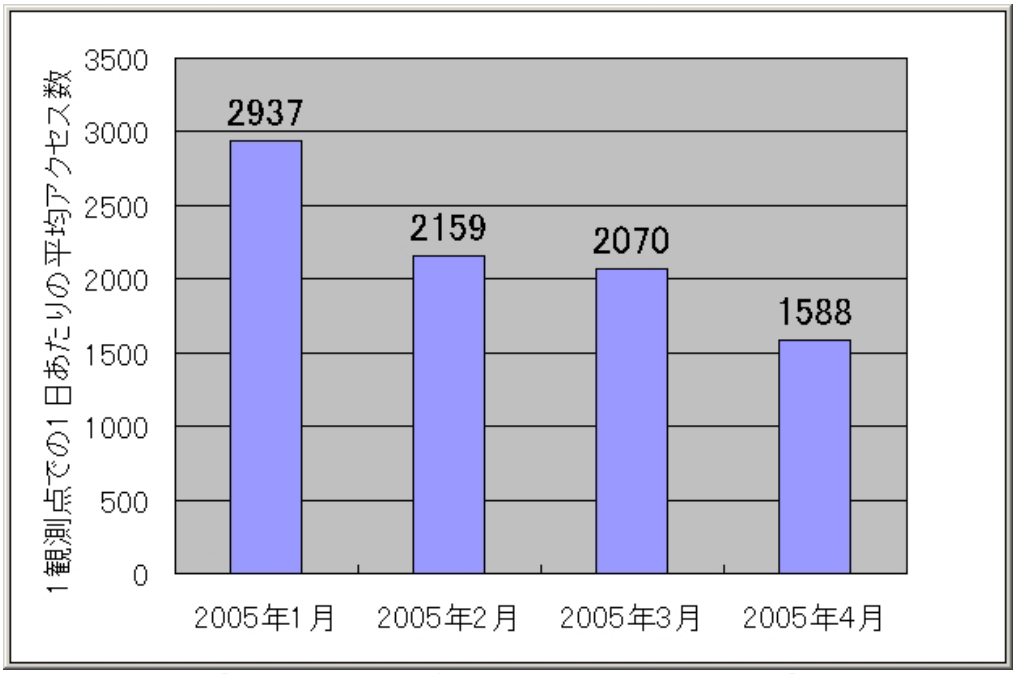
「情報セキュリティ対策実践情報　システム管理者向けのページ」
http://www.ipa.go.jp/security/awareness/administrator/administrator.html

「ソフトウエア等の脆弱性関連情報に関する届出状況[2005 年第 1 四半期（1 月～3 月）]」
http://www.ipa.go.jp/security/vuln/report/vuln2005q1.html

3．インターネット定点観測での 4 月のアクセス状況　－詳細は別紙 3 を参照－

インターネット定点観測(TALOT2)では、2005 年 4 月の期待しない（一方的な）アクセスの総数は、10 観測点で **476,320 件**ありました。これは、1 観測点で 1 日あたり**約 1,600 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。



【1日あたりの期待しない(一方的な)アクセス】

インターネットを利用される皆さんのネットワーク環境において、以下に示す対策をお勧めします。

- ルータやファイアウォールでの継続的な防御
- コンピュータの状態を最新なものにしておくためのパッチの適用(WindowsUpdate等)や、使用するアプリケーションのバージョンアップ
- ウイルス対策ソフトやウイルス対策ベンダーが提供するオンラインウイルス検査による、定期的なウイルスチェックの実施
- サーバ等を利用されている方は、不要なサービスの停止
  (詳細は「SOHO・家庭向けの情報セキュリティ対策マニュアル（Ver1.20）」
  http://www.ipa.go.jp/security/fy14/contents/soho/mokuji.html
  を参照下さい)

4．今月の呼びかけ：「セキュリティホールを解消しよう！」
―― 被害を未然に防ぐために ――

近年の傾向として、セキュリティホール（安全上の欠陥）が公開されてから、その欠陥を悪用する手法が登場するまでの期間が短縮されてきています。2001 年頃は、半年～数年かかっていたのが、2003 年頃には、10 日間～数週間という期間になってきています。

4 月 13 日に公開された Windows のセキュリティホール（Microsoft Windows の TCP/IP の脆弱性 (MS05-019)）を悪用する手法も 4 月 28 日には現れており、修正プログラムを適用する等の対策を実施していないと、いつ被害にあってもおかしくない状況です。

セキュリティホールが公開されたら、早急に修正プログラムの適用、もしくは、回避策を実施することが被害を未然に防ぐための重要な対策になります。下記サイトなどを参考に、お使いのパソコンを最新の状態に保つようにしてください。

（ご参考）

・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/

・日本の Linux 情報
http://www.linux.or.jp/

『用語の解説』

(*1) SQL (Structured Query Language)
リレーショナルデータベースマネジメントシステム(RDBMS)において、データの操作や定義を行うための問合せ言語のこと。構造化問い合わせ言語とも言う。元々は IBM 社が作った言語であるが、現在ではアメリカ規格協会(ANSI)や JIS で標準化されている、世界標準規格。

(*2) SQL インジェクション攻撃
データベースに対する問合せのデータ中に、攻撃者が意図的に SQL 文を混ぜ込んでおき、SQL サーバ内部でその SQL コマンドを不正に実行させてしまう攻撃手法のこと。

(*3) SSH (Secure SHell)
ネットワークを介して別のコンピュータにログインしたり、遠隔地のマシンでコマンドを実行したり、他のマシンへファイルを移動したりするために使うプロトコルもしくはプログラムのこと。ネットワーク上を流れるデータは暗号化されるため、インターネット経由でも一連の操作を安全に行なうことができる。

(*4) ポート
コンピュータが外部との情報の受け渡しの際に使う、コンピュータ内の各種サービス窓口のこと。ポートは 0 から 65535 までの値が使われるため、ポート番号とも呼ばれる。

■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