IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2005 年 6 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 5 月分］について

ウイルスが引き起こす情報漏えい！！

●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 5 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－

5 月の届出件数(※1)は、**5,021 件**となり、5 千件を超える届出が寄せられたのは、2004 年 11 月以来 6 ヶ月振りとなりました。また、ウイルスの検出数(※2)は、**約 355 万個**と、4 月の約 338 万個から 5.3%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）
・5 月は、寄せられたウイルス検出数約 355 万個を集約した結果、5,021 件の届出件数となっています。

W32/Netsky は **1,128 件**となり、15 ヶ月連続でトップの届出が寄せられました。続いて、W32/Mytob 584 件、W32/Mydoom 446 件、W32/Bagle 336 件となりました。

（1）新種ウイルス W32/Wurmark 出現！

5 月に初めて届出された **W32/Wurmark 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ウイルスであり、従来のウイルスと変わりません。しかし、感染するとキーボードからの入力を記録する「キーロガー」と呼ばれるプログラムを埋め込みます。これにより、キーボードから入力、記録された**個人情報が外部に流出**する可能性があります。

届出上位の **W32/Netsky** や **W32/Mytob** などには、外部から侵入され、**パソコン内の情報が盗まれる**危険性があります。これらは、バックドア(裏口)を仕掛ける機能があるからです。

バックドアとは？
ターゲットのコンピュータへ侵入するための「裏口」。ウイルスによっては、外部から感染したパソコンを操作するための窓口として、バックドアを設置する種類がある。

今までのウイルスは、感染してもウイルスメールを撒き散らしたり、パソコンの動作が遅くなったりする等の被害でしたが、最近のウイルスに感染すると、情報が漏えいする危険が高まっています。

漏えいした情報を悪用されると、オンラインゲームに不正にログインされアイテムを売られてしまったり、ネット銀行で不正な取引をされたりと、金銭的な被害を受ける可能性もあります。

これらのウイルスによる被害を防止するためには、
(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必ず実施してください。

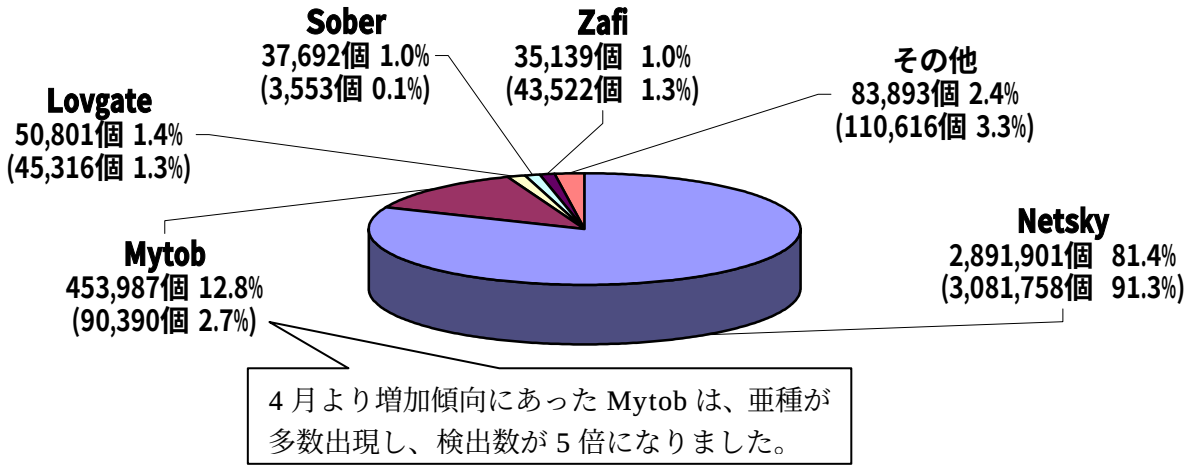
- ワクチンソフトに関する情報
  http://www.ipa.go.jp/security/antivirus/vacc-info.html
- マイクロソフト：Windows Update
  http://windowsupdate.microsoft.com

(2) W32/Netsky が総検出数の約 8 割を占める！ W32/Mytob が急速に増加！

W32/Netsky の検出数が**約 289 万個**と、4 月の約 308 万個から 6.2%の減少となりましたが、**W32/Mytob** の検出数が 4 月の 9 万個から約 45 万個へと 5 倍に増加しました。また、全体の検出数（約 355 万個）も 5.3%の増加となりました。

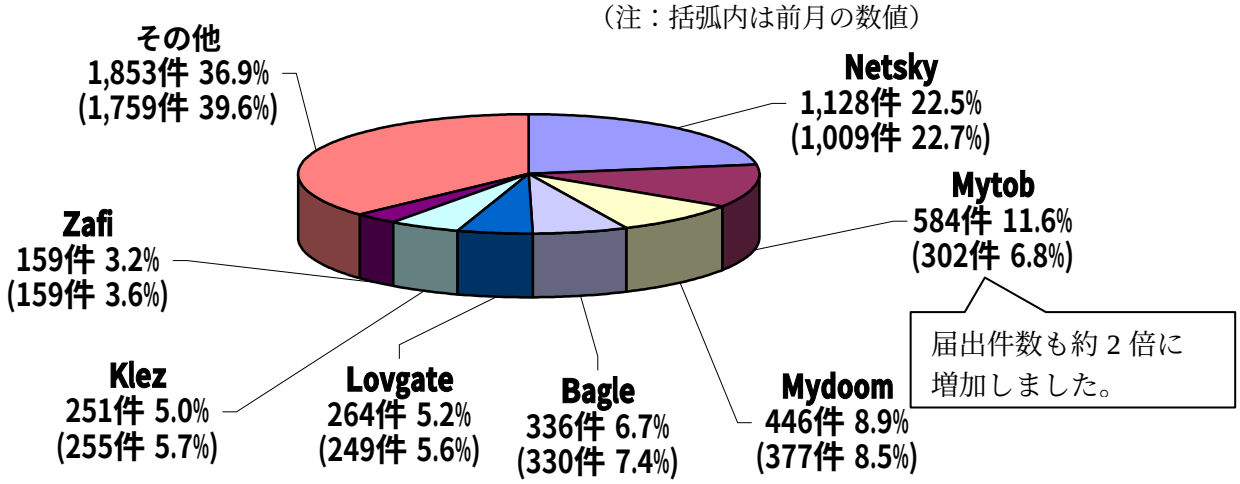
ウイルス検出数　355万個(338万個)　前月比 +5.3%

（注：括弧内は前月の数値）



ウイルス届出件数　5,021件 (4,440件)　前月比 +13.1%

（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 2 を参照－

5 月の総届出件数は 94 件であり、4 月の 48 件と比較してほぼ倍増となりました。そのうち**被害のあった件数は 11 件**であり、4 月の 24 件からほぼ半減しました。

（1）被害状況

被害届出の内訳は、**侵入 10 件、DoS 1 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 7 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 1 件、**フィッシング詐欺に悪用するための偽コンテンツを設置された事例**が 3 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てしまう仕組みを埋め込まれているのを発見。改ざん行為と修復作業のいたちごっこが繰り返された。改ざん箇所の調査を進めるうちに、データベースでの改ざん形跡が発見されるなどし、最終的には一時的なサイト閉鎖に追い込まれた。原因は不明(届出元で引き続き調査中)。

(ii) Web サーバに侵入され、フィッシング詐欺に悪用するための不正なコンテンツ(某オンライン送金サービスの偽サイト)を設置された。さらに、spam(*1)送信の踏み台にさせられていた。外部から連絡があり発覚。原因は不明。

(iii) Web サーバに侵入され不正なコンテンツやファイルが設置されているのを発見。さらに、IRC(*2)を利用してデータを外部に送信しようとした形跡を発見した。サーバ用セキュリティツールの動作は、停止させられていた。syslog(*3)によるログ転送設定の不備のためファイアウォールのログ保全が出来ておらず、原因究明に支障を来たした。

(iv) ルータの設定変更自動通知があったため不審に思い調査したところ、サーバへの侵入・ファイルの改ざんを発見。ルータの設定ファイルが書き換えられていること、不正なプロセスが起動していることを確認するとともに、ルートキット(*4)を発見。原因は不明だが、情報セキュリティ管理は ISMS(*5)に則って実施していたために発見や事後対応が早く、被害を最小限に食い止められた。

(v) 「外部サイトを攻撃している」との通報で調査したところ、サーバに侵入され、管理者権限を持つユーザアカウントが作成されているのを発見。一部ファイルが書き換えられたりログが消去されたりした上、パケットモニタリングツールが設置されていた。ユーザアカウントのパスワードの管理不備およびセキュリティパッチ未適用が原因と思われる。

[DoS]

(vi) ルータに対して、SYN フラッド攻撃(*6)があったことを示すログデータを発見した。幸い、ルータのブロック機能で守られていた上にアクセス頻度が低かったため、ルータのダウンは免れた。

（2）Web アプリケーションの運用について再確認！

被害事例(i)では、**セキュリティパッチ適用や外部からのサーバアタック診断を適切に**

実施していたにも関わらず、サーバへの侵入を許す結果となってしまっています。このサイトでは、単に情報を公開するだけのコンテンツに加え、利用者からの書き込みを受け入れる仕組み（掲示板やサービス申込みフォームなど）もありました。こうしたサイトでは**OS やサーバソフトの脆弱性対策に加え、利用者からの入力を受け付ける Web アプリケーションの処理方法が適切かどうかのチェックなども必要**となり、対策範囲が広範に渡ってしまうケースが多いと思われます。**セキュリティ対策を施す範囲とその内容について、再確認しましょう**。

(ご参考)
「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

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

「コンピュータ・セキュリティ ～2004 年の傾向と今後の対策～」
http://www.ipa.go.jp/security/vuln/20050331_trend2004.html

（3）ログデータの管理と保全は確実に！

被害事例(iii)では、**ログ管理方法として syslog** を使い、ファイアウォールでログを記録し他のコンピュータ上で運用している **syslog サーバにログデータを転送する仕組み**が構築されていました。この方法では、**ログ一括管理やログ改ざん防止といったメリット**がある反面、**ログデータ転送失敗の可能性があるというデメリット**もあります。今回はこのデメリットが表に出てしまった形ではありますが、ログを保存し定期的に解析することは、不正アクセスの検知や事故発生時の原因究明のために非常に重要な対策となります。**ログデータの管理や運用方法について、設定ミスが無いかなど、再確認しましょう**。

（ご参考）
「セキュアな Web サーバーの構築と運用」
http://www.ipa.go.jp/security/awareness/administrator/secure-web/

（4）情報セキュリティ管理について再確認！

被害事例(iv)では、サーバへの侵入を許してしまってはいますが、**侵入や改ざんを検知する仕組みを導入しており、早期の発見が出来ました**。この仕組み以外にも、定期的なログ参照による異常の有無確認、セキュリティパッチリリースの確認および適用、適切なアクセス権限割り当て、入退室管理されたサーバルームに機材を設置するなど、**あらかじめ組織内で決められた情報セキュリティ管理の規定に従って対策を講じており、被害を最小限に食い止めることが出来ました**。この機会に、保護すべき情報資産の内容や対策方法について改めて検討するなど、情報セキュリティ管理について再確認しましょう。

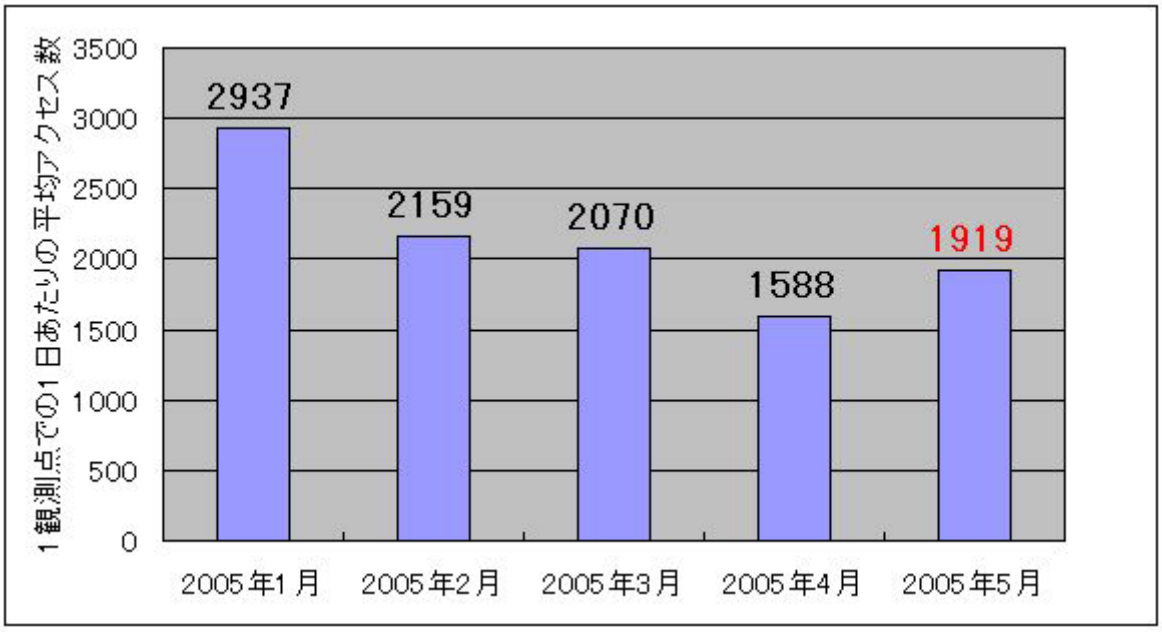
（ご参考）
「読者層別：情報セキュリティ対策 実践情報」
http://www.ipa.go.jp/security/awareness/awareness.html

財団法人 日本情報処理開発協会 － ISMS 制度推進室
http://www.isms.jipdec.jp/

3．インターネット定点観測での５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 5 月の期待しない（一方的な）アクセスの総数は、10 観測点で **594,960 件**ありました。これは、1 観測点で 1 日あたり**約 1,900 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】

5 月中旬には Microsoft の Windows 上で動作する SQL Server を探す目的と思われる宛先ポート **1433(TCP)へのポートスキャン**が、広い範囲で増加（通常の4～5倍程度）しました。

また、観測データとしては公開していませんが、あいかわらず SSH（Secure Shell）を通してコンピュータに侵入しようとするパスワードクラッキングアクセス(**22(TCP)へのアクセス**)も続いています。

これらのアクセスが、コンピュータへの侵入を狙う目的のものであることは明らかです。前述の**「２．コンピュータ不正アクセス届出状況」**にも示す通り、コンピュータの管理者の方には、管理するコンピュータの再点検を行うことを、お勧めします。

4．今月の呼びかけ：「 ホームページに潜む危険 」
―― 被害を未然に防ぐために ――

5 月の事例として、改ざんされたホームページを閲覧することにより、**不正なプログラムを自動的にダウンロードされてしまう**ものがありました。これは、普段見ているサイトでも、いつの間にか不正なプログラムを取り込まされてしまう危険が潜んでいるということです。

このような被害が起きる原因は、Internet Explorer 等の**ブラウザにセキュリティホールがあり、それを悪用されている**ためです。

被害に遭わないための対策として、**セキュリティホールを解消しておくことが必須**事

項となります。下記サイトなどを参考に、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を適用する、もしくは、回避策を実施する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) 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、個人的、宗教的なものも含めて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。

(*2) IRC （Internet Relay Chat）
チャット（接続者同士のリアルタイムな会話）システムのこと。インターネット上の IRC サーバに、専用のソフトウェアを利用してアクセスすることで、複数のユーザとの間でメッセージの交換が出来る。ファイル通信にも対応する。

(*3) syslog
ログデータに関するフォーマットや通信規約のこと。

(*4) ルートキット （rootkit）
攻撃者がコンピュータに不正侵入した後に利用するためのソフトウェアをまとめたパッケージのこと。一般的には、ログ改ざんツールやバックドアツール、改ざんされたシステムコマンド群などが含まれる。

(*5) ISMS （Information Security Management System ： 情報セキュリティマネジメントシステム）
企業などの組織が自らの情報セキュリティを確保し維持するために、あらかじめ定めたセキュリティポリシーに基づき必要なセキュリティレベルを決めてセキュリティ管理体制を構築し、さらに定期的に監査を実施し、必要に応じて対策の見直しするといった PDCA サイクルを継続的に運用していく枠組みのこと。

(*6) 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。

■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