IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2005 年 8 月 4 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 7 月分］について

スパイウェアの脅威！

●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 7 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－

ウイルスの検出数(※1)は、**約 379 万個**と、6 月の約 385 万個から 1.7%の減少となりました。また、7 月の届出件数(※2)は、**4,536 件**となり、6 月の 4,928 件から 8.0%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。
・7 月は、寄せられたウイルス検出数約 379 万個を集約した結果、4,536 件の届出件数となっています。

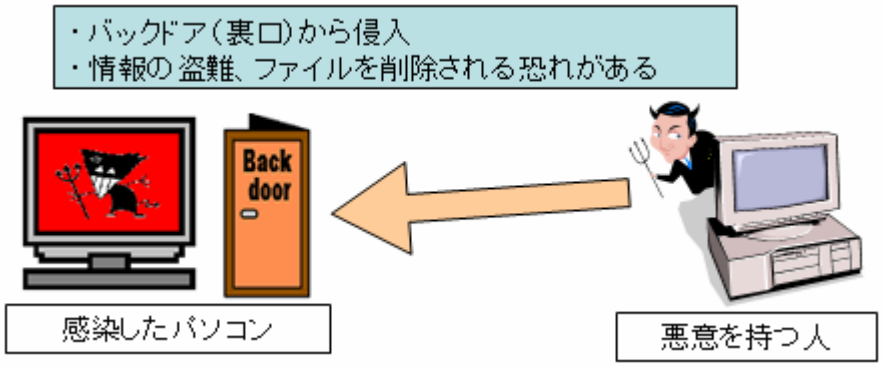
W32/Netsky の検出数は、**総検出数の 75%を占める約 284 万個**（届出件数 **1,125 件**）となり、17 ヶ月連続でトップの届出が寄せられました。続いて、**W32/Mytob 約 80 万個（638 件）**、W32/Bagle 約 5 万個（284 件）、W32/Lovgate 約 4 万個（249 件）となりました。
また、**スパイウェアによる被害発生を受け、7 月には緊急対策情報を公開**しました。

（1）新種ウイルス W32/Reatle(リアトル)出現！

W32/Reatle ウイルスが 7 月に出現しました。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経路に加え、Windows のセキュリティホールを悪用することで、ネットワーク経由でも感染します。

このウイルスに感染すると、以下の活動を行います。

(i) バックドア（裏口）を設定する
外部から侵入され、ファイルを削除されたり、情報を盗まれる可能性があります。
(ii) 特定のサイトへ DoS（サービス妨害）攻撃を仕掛ける
被害者から加害者へとなってしまいます。
(iii) 他の不正プログラムを勝手にダウンロードする
スパイウェアなどがダウンロードされ、さらに深刻な被害をもたらす可能性があります。



感染被害に遭わないために、ウイルス対策ソフトの活用、セキュリティホールの解消を日頃から継続することが重要です。

感染してしまった場合は、以下のサイトで専用の駆除ツールが提供されていますので、利用して対処してください。

W32.Reatle@mm 駆除ツール（シマンテック社）
http://www.symantec.com/region/jp/avcenter/venc/data/jp-w32.reatle@mm.removal.tool.html
「システムクリーナー」の使用方法（トレンドマイクロ社）
http://www.trendmicro.co.jp/esolution/solutionDetail.asp?solutionId=4700

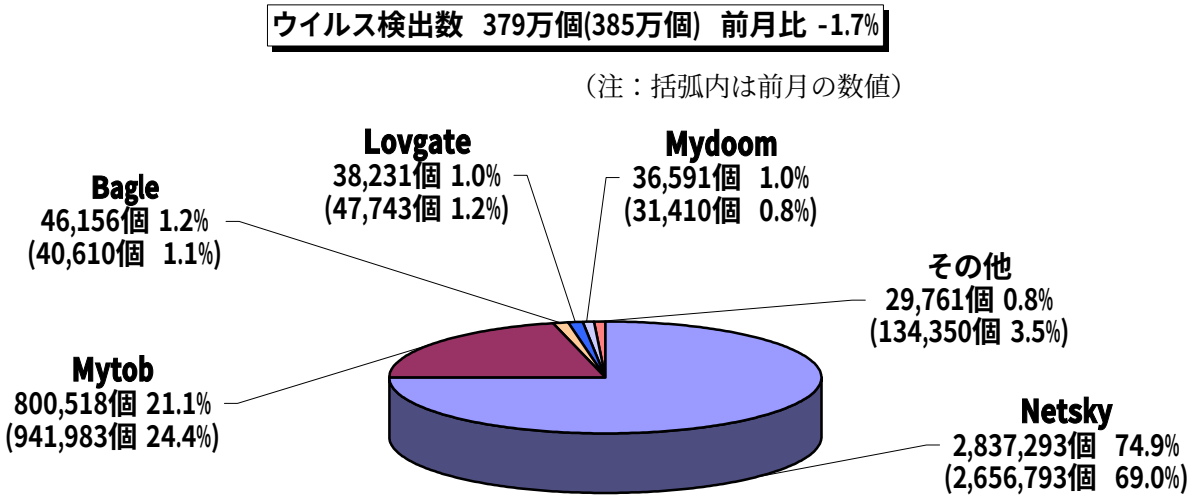
（2）W32/Netsky が総検出数の 75%を占める！

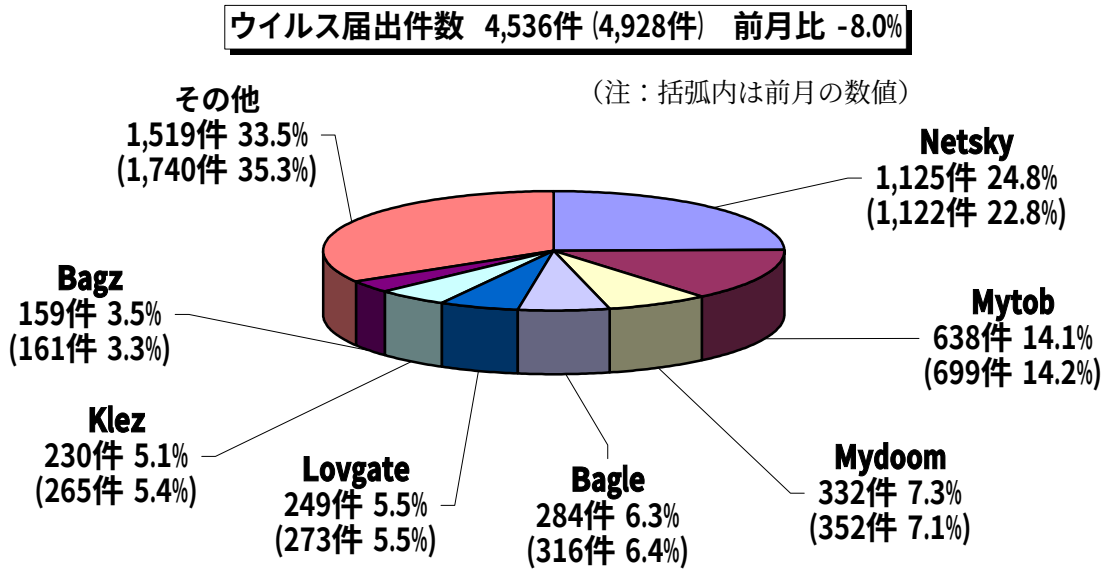
W32/Netsky の検出数が**約 284 万個**と、6 月の約 266 万個から約 6.8%の増加となりました。また、3 月に出現してから毎月増加していた **W32/Mytob** の検出数は、6 月の約 94 万個から約 80 万個と、初めて減少に転じました。

W32/Netsky が継続して高い割合を占めている理由として、感染していることに気付かずに、ウイルスメールを撒き散らしている状況が推測されます。自分は大丈夫と思っている方も、念のため駆除ツールで検査することをお勧めします。また、知り合いの方にもこの状況をお知らせしてください。

駆除ツールを利用した検査方法（無償）
（ Netsky 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）

・シマンテック社
http://www.symantec.com/region/jp/sarcj/data/w/w32.netsky@mm.removal.tool.html
・トレンドマイクロ社
http://www.trendmicro.co.jp/esolution/solutionDetail.asp?solutionId=4700
・マカフィー社
http://www.mcafeesecurity.com/japan/security/stinger.asp
・マイクロソフト社
http://support.microsoft.com/?kbid=890830





2．スパイウェアについて

ウイルスばかりでなく、パソコン内の情報を収集して外部に送信するスパイウェアが出回っており、金銭的被害も発生しております。誤ってメールの添付ファイルを開いたり、ホームページ上から取り込んでしまわないよう注意が必要です。

例えばIPAに発見･被害報告が寄せられている主なスパイウェアには以下のものがあります。

Trojan/Lineage（リネージュ）
**　オンラインゲームへのログインID、パスワードを収集し、外部に送信する**
Trojan/Myftu（マイフツ）
**　メールアドレスを取得し、外部に送信する**

Trojan/Myftu（マイフツ）は、アダルトサイト等で画像をクリックすることでパソコンにダウンロードされ、メールアドレスが収集されます。収集されたアドレスが**振り込め詐欺に利用**されるケースが確認されています。（このような被害に遭わないための対策は、本紙5.をご参照ください。）

3．コンピュータ不正アクセス届出状況（相談を含む）　―詳細は別紙2を参照―

（1）不正アクセス届出状況

7月の届出件数は53件であり、そのうち**被害のあった件数は10件**でした。

	2月	3月	4月	5月	6月	7月
被害あり	9	14	24	11	22	10
被害なし	54	45	24	83	2	43
計（件数）	63	59	48	94	24	53

（2）不正アクセス等の相談受付状況

不正アクセスに関連した相談件数は42件（うち9件は届出件数としてもカウント）であり、そのうち何らかの被害のあった件数は23件でした。

（3）被害状況

被害届出の内訳は、**侵入 3 件、メール不正中継 1 件、DoS 2 件、アドレス詐称 1 件、その他(被害あり)3 件**でした。また、相談の中には、パソコンに不正なプログラムを仕込まれた上にメールアドレスを盗まれて、振り込め詐欺のメールを送りつけられた、という事例がありました。＜被害事例(vi)参照＞

被害事例

[侵入]

(i) サーバ監視システムがメールサーバの高負荷状態を検知したため調査したところ、spam(*1)メールが大量に送信されていたことが、サーバのログから判明。その後の調査で、侵入者が SSH(*2)に使用するポート(*3)からサーバに侵入し、システム内部から spam メールを送信していたことが分かった。このポートは、保守作業のために開けており、かつ管理者権限ユーザアカウント(*4)のパスワードが容易に推測可能であったことが原因と思われる。**（解説、対策については 3．(4)参照）**

(ii) インターネットと LAN との境界に設置したサーバの動作が遅くなっていた。数日後、アクセスログを調査したところ、数日間に渡って管理者権限ユーザのアカウントに対してパスワードアタックを仕掛けられていたことが判明。結果としてパスワードが奪取されてサーバへの侵入を許してしまい、さらにはフィッシングに悪用するための Web コンテンツを勝手に設置させられてしまっていた。**（解説、対策については 3．(4)参照）**

[DoS]

(iii) Web サーバの 80 番ポートに、不正なものと思われる大量のアクセスが集中したため、数時間の間、外部から Web コンテンツが閲覧不能になった。特定の IP アドレスからのアクセスを制限することで復旧した。

[メール不正中継]

(iv) 送信した覚えの無いメールが、宛先不明のエラーで返送されて来た。メールヘッダを調査したところ、自ドメイン内のメールサーバから送信されているらしいことが判明。原因は不明だが、メールサーバが不正中継に利用されている可能性があり、メールサーバの設定を再確認した。

[その他]

(v) 銀行のオンライン取引に必要な ID やパスワードが不正に奪取されたらしく、預金が勝手に他の口座へ送金されてしまった。その後の調査で、キーロガー(*5)と呼ばれるタイプのスパイウェアを埋め込まれたものと判明。さらに、Web ブラウザの設定が勝手に変更されたり、保存していたファイルが破壊されていたりしており、キーロガー以外にも、何らかの不正なプログラムを埋め込まれていたと思われる。最終的にはパソコンを初期化して対応した。**（解説、対策については 3．(5)参照）**

(vi) 不審なメールが届き、本文中にあった URL をクリックしたところ、アダルトサイトにジャンプした。画像をクリックしたらファイルダウンロードの確認画面が出たため、[OK]ボタンを押した。ダウンロードしたファイルをダブルクリックしたら、デスクトップ上に「請求書」アイコンが貼り付いていた。中身を見ると、「□□サイトへの入会ありがとうございます。○日以内に、△△円お振込みください」などと書かれていた。メールアドレスは知らせていないはずなのに、数分後から料金支払いの督促メールが届き始め、そ

の後も毎週のように督促メールが届く。その後、ウイルスチェックしたところ、メールソフトに設定していた自分のメールアドレス情報を盗み出すタイプのスパイウェアが検出された。**（解説、対策については３．(5)参照）**

（4）解説と対策：サーバへの侵入防止対策を再度確認！

被害事例(i)、(ii)では、**侵入の原因がパスワードクラック**となっています。推測されにくいパスワードを設定するのは当然ですが、不用意にポートを開けていると時間は掛かるものの比較的容易にパスワードが破られてしまいます。また、**外部からアクセス可能なユーザアカウントに管理者権限を付与してあると、万が一侵入された場合のリスクが高くなってしまいます**。今回のケースではさらに、侵入後に外部に spam メールを撒き散らしたりフィッシングサイトを設置されていたりと、加害者とみなされてしまいかねない状況になっていました。**外部からアクセス可能にするユーザや経路は最小限に抑えると共に、アクセス権限が適切に付与されているか、確認しましょう**。

(ご参考)
「リモートアクセス環境におけるセキュリティ」
http://www.ipa.go.jp/security/awareness/administrator/remote/

（5）解説と対策：スパイウェアが引き金となって不正アクセス？！

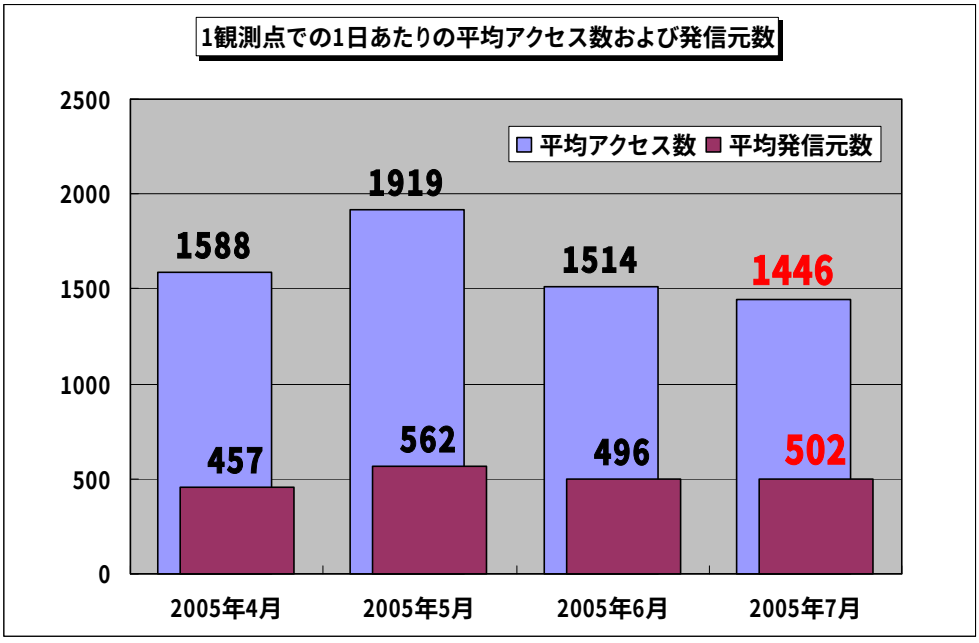
被害事例(v)、(vi)では、**情報を盗み出すタイプのスパイウェアが埋め込まれてしまったために、銀行口座情報やメールアドレスが外部に漏れてしまいました**。このことが原因となって、銀行口座に不正にアクセスされて預金を引き出されてしまったり、「振り込め詐欺」メールが届き始めたりといった被害に遭ってしまいました。**身に覚えの無いメールの添付ファイルを安易に開くことや出所の不明な怪しいファイルをダウンロードして開くことは避けるとともに、セキュリティソフトを導入するなどして被害予防対策をとりましょう**。万が一、情報が漏れてしまっても、**銀行口座の引出限度額設定などのサービスを利用していたり、「振り込め詐欺」メールに対して安易に反応したりしなければ、被害を最小限に食い止めることが出来ます**。（スパイウェア対策については、本紙 5.も参照してください。）

(ご参考)
国民生活センター 「クリックでパソコン画面上へ自動的に請求書が作成される手口」
http://www.kokusen.go.jp/soudan_now/d_seikyu.html

４．インターネット定点観測での７月のアクセス状況

インターネット定点観測(TALOT2)によると、2005 年7月の期待しない（一方的な）アクセスの総数は、10観測点で**448,232件**ありました。1観測点で1日あたり**約500**の発信元から**約1,450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。言い換えれば、**あなたのコンピュータは、毎日、平均して、500 人の見知らぬ人から、3 件ずつの不正と思われるアクセスを受けている**と言うことになります。



今月の注意ポイント

- SQL サーバを狙っていると思われる不正なアクセスが急増しています。システムの管理者は、サーバに脆弱性がないか確認し、常に最新の状態に保つことに心掛けて下さい。ただし、SQL サーバをインターネットに直接公開する必要はないと考えられます。明に公開しているシステムの管理者は、システムの見直しをお勧めします。

- コンピュータの画面に、セキュリティ強化を促し、特定のWebサイトへ勧誘するメッセージ(以下に例)を表示させるアクセスが増加しています。このメッセージには操作指示が書かれていますが、従う必要はなく、表示された画面は×ボタン(矢印部分)で終了して下さい。ちなみに、Windows XP ユーザの場合は、OS により提供されるファイアウォール機能を有効にすると、これらのメッセージは表示されなくなります。

- ファイル共有を狙っていると思われるアクセスも、あいかわらず多いようです。インターネットに対してファイル共有を公開する理由はありませんが、パスワードの強化や脆弱性などを解消した、強固な環境で対応して下さい。

以上の問題に対して、詳細はこちらのサイトをご参照ください。
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
http://www.ipa.go.jp/security/txt/2005/documents/TALOT2-0508.pdf

5．今月の呼びかけ：「 スパイウェアの脅威！ 」

―― 気付かぬうちに侵入されていませんか？ ――

インターネットバンキングの利用者をターゲットとしたスパイウェアが原因で不正送金を行われたり、メールアドレスを盗み出すスパイウェアが原因で勝手にアダルトサイトに登録されて利用料金請求のメールが送りつけられたりといった被害事例がありました。

この他にもオンラインゲームのログインパスワードを収集したり、パソコンの設定を勝手に変更してしまうなど、多数のスパイウェアが出回っています。

これらの被害に遭わないよう、以下の**スパイウェア対策 5 箇条**を参考に、対策を実施してください。

1. スパイウェア対策ソフトを利用し、定期的な定義ファイルの更新およびスパイウェア検査を行う
2. コンピュータを常に最新の状態にしておく
3. 怪しいサイトや不審なメールに注意
4. コンピュータのセキュリティを強化する
5. 万が一のために、必要なファイルのバックアップを取る

詳細はこちらのサイトをご参照ください。
パソコンユーザのためのスパイウェア対策 5 箇条
http://www.ipa.go.jp/security/antivirus/spyware5kajyou.html

（ご参考）
スパイウェアによる被害の防止に向けた注意喚起
http://www.ipa.go.jp/security/topics/170720_spyware.html

～夏休み(長期休暇)における対策のお願い～

お盆休みや夏休みで、長期の一斉休暇を行う組織においては、長期休暇中にトラブルが発生した場合、対処が遅れて大きな被害になる可能性があります。

下記の「夏休み前に対策を」を参照して、休暇に入る前にセキュリティの設定を再確認することを推奨します。

夏休み前に対策を
http://www.ipa.go.jp/security/topics/alert170804.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) 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。

(*2) 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。

(*3) ポート (port)
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。

(*4) アカウント (account)
コンピュータやネットワーク上の資源を利用出来る権利のこと、または利用する際に必要な ID のこと。

(*5) キーロガー (key logger)
キーボードから入力された情報を記録するプログラムのこと。

■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