IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2005 年 9 月 5 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 8 月分］について

気付かぬうちにボットに感染していませんか？

●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 8 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 337 万個**と、7 月の約 379 万個から 11.0%の減少となりました。また、8 月の届出件数(※2)は、**4,470 件**となり、7 月の 4,536 件から 1.5%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。
・8 月は、寄せられたウイルス検出数約 337 万個を集約した結果、4,470 件の届出件数となっています。

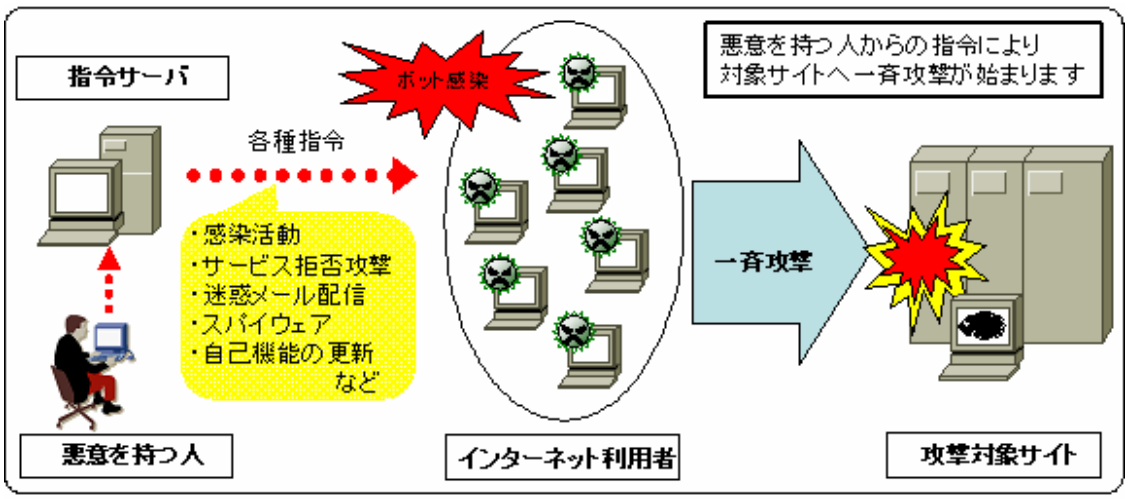
W32/Netsky の検出数は、**総検出数の約 8 割を占める約 267 万個**（届出件数 **999 件**）となり、18 ヶ月連続でトップの届出が寄せられました。続いて、**W32/Mytob 約 57 万個（536 件）**、W32/Bagle 約 3 万個（303 件）、W32/Mydoom 約 3 万個（352 件）となりました。

また、**Windows の脆弱性(セキュリティホール)を突いたワームが複数種発生したことを受け、8 月には緊急対策情報を発信**いたしました。

（1）Windows の脆弱性を突いたワームが複数種発生！

8 月 10 日にマイクロソフト社より公開された **Windows の脆弱性を悪用するワーム**（**W32/Zotob、W32/IRCbot、W32/Bobax**）が次々に出現しました。これらのワームは、インターネットに接続しているだけで感染する可能性のあるタイプで、**W32/Zotob と W32/Bobax** の亜種の中にはメールの添付ファイルとして感染する機能も有しているものもあります。

また、これらのワームは**ボット**(*1)**としての機能も有しており、感染すると外部からの指令を受けて、特定のサイトへ攻撃を行ったり、迷惑メールの発信元として利用されたり、他者への攻撃の踏み台として使われてしまう危険性**もあります。



図：ボットの仕組み(例)
「コンピュータ・セキュリティ ～2004 年の傾向と今後の対策～」より
http://www.ipa.go.jp/security/vuln/20050331_trend2004.html

ご参考）
Microsoft 社 Windows の脆弱性（MS05-039）を突いたワームが複数種発生！！
http://www.ipa.go.jp/security/ciadr/vul/20050817.html
ボット対策について
http://www.ipa.go.jp/security/antivirus/bot.html

今回、Windows の脆弱性が公開されてから、その脆弱性を悪用するワームが出現するまでの経緯は次のようになっています。

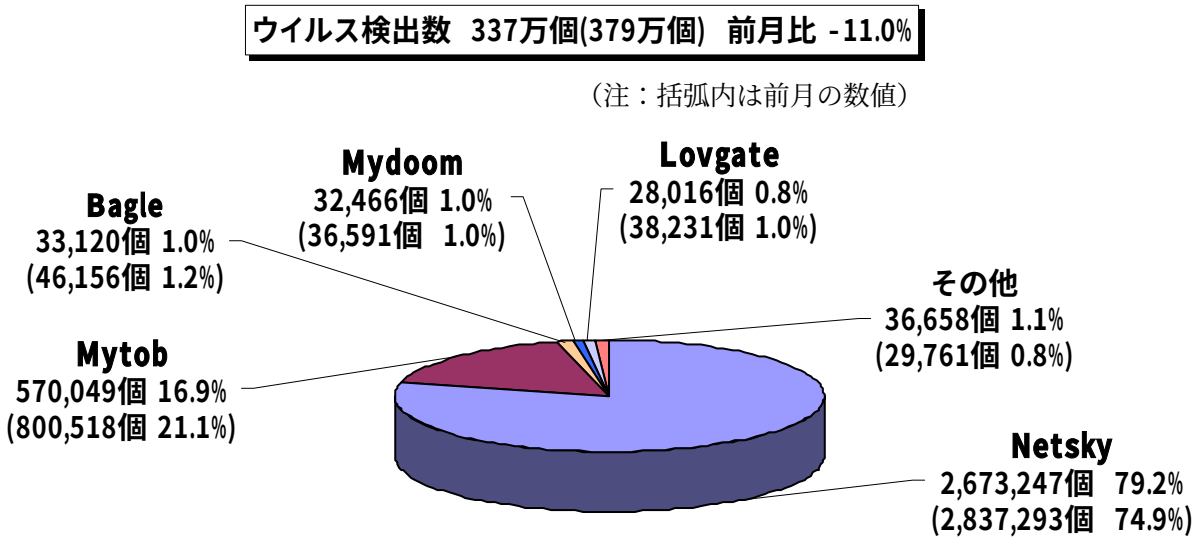
時間	経過
2005 年 8 月 10 日	Microsoft Windows のセキュリティ修正プログラム(MS05-039) 公開
2005 年 8 月 12 日頃～	MS05-039 の脆弱性を攻略する攻撃コードがメーリングリストやインターネット上に公開され始める
2005 年 8 月 15 日～	MS05-039 の脆弱性を悪用したワームが出現

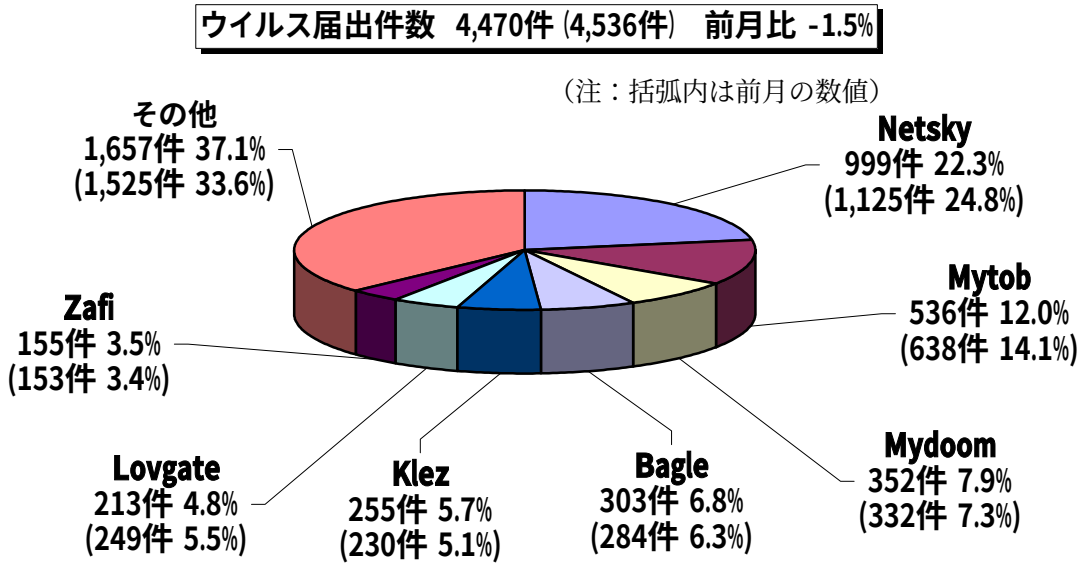
このように、脆弱性が公開されてからそれを悪用するワームが出現するまでの期間が非常に短くなっています。脆弱性が修正されていれば、被害に遭う可能性を低減できますので、なるべく早期に Microsoft Update を行うなど、脆弱性の解消を行うことが重要です。
また、ウイルス対策ソフトも活用し、外部からの侵入を防ぐとともに、週 1 回はパソコン内を検査して感染の有無を確認するようにしましょう。

（参考情報）
マイクロソフト社： Microsoft Update http://update.microsoft.com/
シマンテック社： http://www.symantec.com/region/jp/
トレンドマイクロ社： http://www.trendmicro.co.jp/home/
マカフィー社： http://www.mcafee.com/jp/default.asp

（2）W32/Netsky が総検出数の約 8 割を占める！

W32/Netsky の検出数が**約 267 万個**と、7 月の約 284 万個から 5.8%の減少となりました。また、**W32/Mytob** の検出数は約 57 万個となり、7 月の約 80 万個から 28.8%の減少となりました。





2．スパイウェアについて

ウイルスばかりでなく、スパイウェア(*2) (キーロガー(*3)等)やその他の不正プログラム（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

IPA に発見･被害報告が寄せられている主な不正プログラムには以下のものがあります。

被害の内容例	当該不正プログラム等
オンラインゲームへのログイン ID、パスワードやメールアドレスを収集し、外部に送信する。	Trojan/Lineage Trojan/Myftu
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

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宛に請求書を送るなど、振り込め詐欺に利用されるケースが確認されています。

（ご参考）
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

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－

不正アクセスの届出および相談の受付状況

		4月	5月	6月	7月	8月
届出(a) 計		**48**	**94**	**24**	**53**	**41**
	被害あり(b)	24	11	22	10	12
	被害なし(c)	24	83	2	43	29
相談(d) 計		**28**	**47**	**37**	**43**	**43**
	被害あり(e)	13	25	22	24	23
	被害なし(f)	15	22	15	19	20
合計(a+d)		**76**	**141**	**61**	**96**	**84**
	被害あり(b+e)	37	36	44	34	35
	被害なし(c+f)	39	105	17	62	49

IPA で受け付けた相談件数の推移

		4月	5月	6月	7月	8月
合計		**553**	**461**	**511**	**554**	**629**
	自動応答システム	374	242	289	337	376
	電話	115	118	143	128	179
	電子メール	61	92	67	84	67
	FAX・他	3	9	12	5	7

※　IPA では、コンピュータウイルス･不正アクセス、その他情報セキュリティ全般についての相談を受け付けています。電話番号：03-5978-7509（24 時間自動応答）

※　「自動応答システム」：電話の自動音声による応対件数
「電話」：オペレータによる応対件数

（1）不正アクセス届出状況

8 月の届出件数は 41 件であり、そのうち**被害のあった件数は 12 件**でした。

（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 43 件（うち 5 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 8 件、DoS 攻撃 2 件、その他(被害あり)2 件**でした。また、相談の中には、アダルトサイトを閲覧した後に「振り込め詐欺」のメールを送りつけられた、という事例が先月に引き続き、多数ありました＜被害事例(v)参照＞。

被害事例

[侵入]

(i) ネットワーク機器への侵入

事例	ルータなどのネットワーク機器数台に侵入され、パスワードが勝手に変更されていたり、ログ(*4)記録機能などを無効にされていたりした。内部ネットワークからのみならず、外部からルータなどへ telnet(*5)接続が可能になっており、かつ接続用パスワードと管理者権限パスワードが同じだったため、外部から telnet 接続へパスワードアタックを受けて侵入を許した上に管理者権限でルータなどの設定を変更されてしまった可能性が高い。
解説・対策	**ルータなど、コンピュータネットワーク間を接続する機器に侵入されて設定改変の被害を受けてしまっています**。今回の事例ではネットワーク運用に関して致命的な被害はありませんでしたが、**ネットワーク機器によっては、管理者権限でログインすると、その組織で運用しているネットワークの情報(機器、構成など)が容易に調べることが出来る**ようになっています。通常、ネットワーク構成情報は、企業などにとって秘密情報です。それらの情報を悪用されると、容易に不正アクセスが行われてしまったり、ネットワークに重大な障害を引き起こされてしまったりする恐れがあります。**ネットワーク機器についても、コンピュータなどと同様にセキュリティパッチを当てる、アクセス制限を適切に行うなどのセキュリティ対策が必須**です。

(ii) レンタルで間借りしていたサーバへの侵入

事例	商用レンタルサーバを間借りして Web サイトを運用していた。このサーバを間借りしていた、自身とは無関係の他のユーザが運用していたサイトが cgi(*6)の脆弱性を突かれて攻撃され、レンタルサーバそのものの管理者権限が奪われた。その結果、当該レンタルサーバ上の全ユーザの Web コンテンツが改ざんされた。この件から 1 ヶ月以上経った頃、同サーバ上のシステム管理者権限で IRC(*7)プログラムの起動が行われた。調査したところ、複数回、サーバに侵入されていたことが判明。最初の侵入時にユーザ管理情報を盗まれ、その後、比較的推測され易いパスワードを設定していたユーザのアカウントから侵入されたものと思われる。これらの事象は、レンタルサーバの常時監視システムが警告を発したことで、発見されたものである。
解説・対策	**自身に非が無くてもサーバへの侵入や改ざんの被害を受けてしまっています**。レンタルサーバの**セキュリティ対策は、通常はレンタルサーバ会社側に事実上委ねてしまうことになると思われますが、その対策内容や補償内容について改めて確認をしておく必要があるでしょう**。さらに、自身で管理運用しているサーバで発生した障害対策のみならず、自身の管理管轄外で発生した障害時の対応についても、取り決めておく必要があるでしょう。また、**自身がレンタルサーバ上で運用している Web アプリケーションなどについても、脆弱性がないか調査するなど、セキュリティ対策を再確認**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

[DoS 攻撃]

（iii）ネットワーク内外部からのパスワードアタック

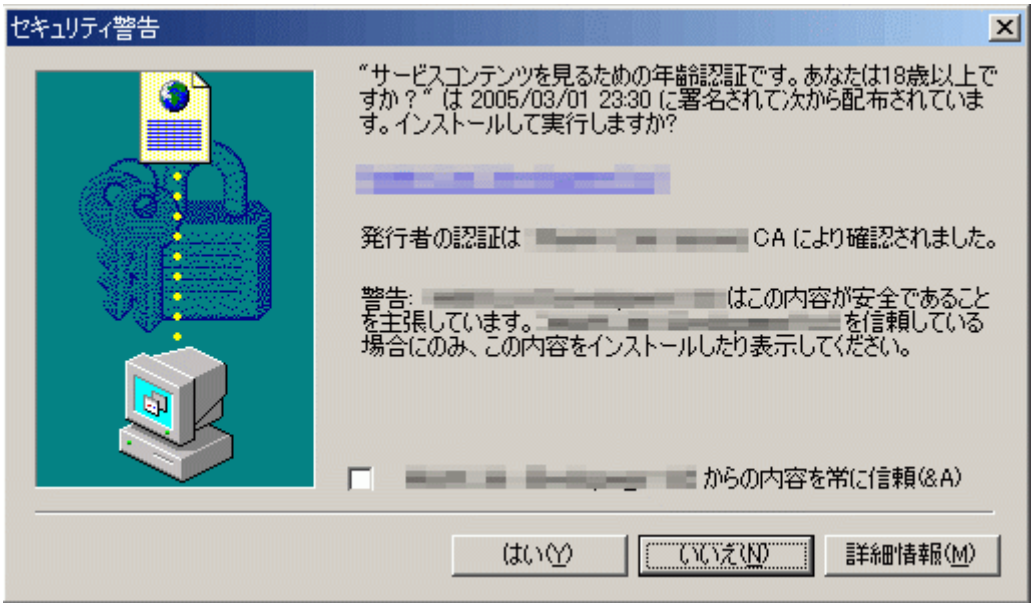
事例	内部および外部ネットワークから、数分間の間に数百から数千アクセスのパスワードアタックを受けた。侵入は許さなかったもののサーバの負荷が過大となり、サーバの処理能力が一時的に著しく低下した。
解説・対策	特定サイトや特定ポートへの攻撃については、**ルータなどにおけるフィルタリング**により対処出来る場合があります。もしくは、**アクセスを受け付ける IP アドレス範囲をあらかじめ制限**しておくことも有効です。また普段から、**本来のサービスに非常に多くのリクエストが来た場合の想定をしておくのも良い**でしょう。

[その他]

（iv） スパイウェアの侵入

事例	ウイルス対策ソフトは導入していたが、メール送受信に支障が出たりウイルス対策ソフトの動作が異常になったりするなどの状況に陥った。パケットモニタリングソフトで調査したところ、特に何も動作させていないはずのパソコンから、送信パケットが不自然に多く出ていることが判明。スパイウェア対策ソフトを導入してスキャンしたところ、数種の不正なプログラムが検出された。
解説・対策	最近のウイルス対策ソフトは、スパイウェア対策機能が付加されているものが多くありますが、スパイウェアによっては検出されないものがあるのも事実です。より万全な対策をとるためには、**パーソナルファイアウォールソフトやスパイウェア対策に特化した専用ソフトなども活用することを推奨**します。 （ご参考） 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

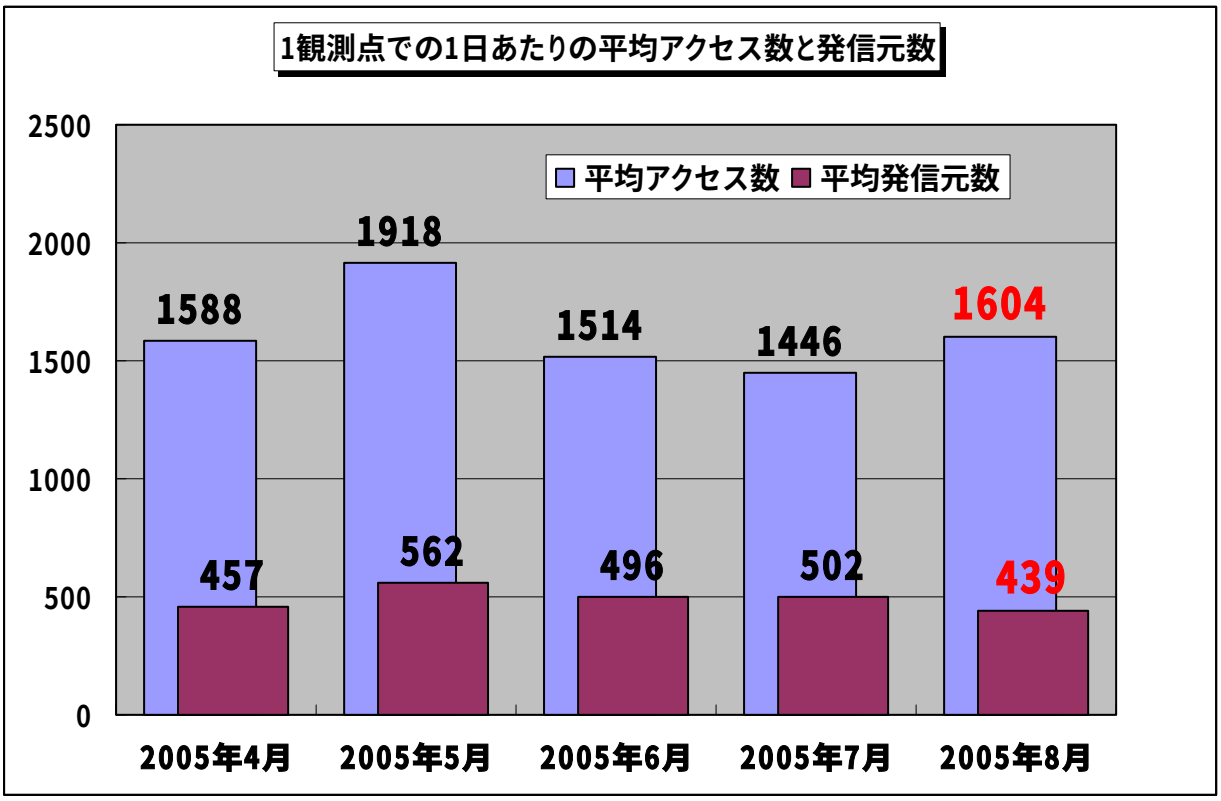
(v)　アダルトサイトでの不正プログラムダウンロード

事例	パソコンで、出会い系サイトやアダルトサイトをたまたま訪れた際、画像をクリックしたら 18 歳以上かどうかの年齢確認画面になったため「はい」をクリックしたところ、途端に何かデータがダウンロードされたような画面になり、さらに「入会ありがとうございます」などというメッセージとともに自分のメールアドレスが表示されていた。その後、数分毎に料金の請求画面が現れたり、料金支払いの督促メールが届いたりするようになった。ウイルス対策ソフトでスキャンしても、何も検出されない。
解説・対策	興味本位で訪れたサイトで言葉巧みに騙され、メールアドレスを盗み出したりする不正プログラムをダウンロードさせられています。**年齢確認に見えた画面は、実はよく見るとファイルのダウンロードとインストールを問うもので、「はい」をクリックすると即、不正プログラムがダウンロードされて実行される仕組みになっていました。**  その結果、**料金請求画面や支払い督促メールに悩まされることになってしまいました**。ウイルス対策ソフトやスパイウェア対策ソフトでも検出されなかったため、最終的にはパソコンを初期化することになってしまいました。インターネットには、この例に限らず、危険がたくさん潜んでいます。特に、"有料"となっているアダルトサイトには今回の事例のような罠が待ち受けていることがあります。**会員登録する意思が無いのであれば最初から近づかない**、登録するとしても会員規約などをよく読んで内容を確認する、**ファイルのダウンロードには細心の注意を払う**、などの自己防衛策が必要です。 (ご参考) 「クリックしただけで料金請求された場合の対応方法について」 http://www.ipa.go.jp/security/ciadr/oneclick.html

4．インターネット定点観測での 8 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 8 月の期待しない（一方的な）アクセスの総数は、10 観測点で **497,340 件**ありました。1 観測点で 1 日あたり **439** の発信元から **1,604 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、440 人の見知らぬ人から、発信元一人当たり 3～4 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

- あいかわらず、Windows の脆弱性を狙っていると思われる不正なアクセスが多いようです。これらのアクセスの多くは、ワームに感染したコンピュータから送信されていると思われます。昨今の状況から考えて、最近ボットと呼ばれるワームが流行していることから、これらのアクセスを行っているワームもボットである可能性が高いと思われます。
- 特にアクセス数の多い 135(TCP),445(TCP)へのアクセスは、Windows の古いタイプの脆弱性を狙っていると思われ、これらのアクセスの多くが国内発信であることから、国内でのボットの感染が広がっていることが予測されます。
- 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。
- 一般のコンピュータ利用者は、これらのボットに感染しないために、自分のコンピュータを最新の状態に保ち、ウイルス対策ソフト等を有効利用することをお勧めします。

以上の情報に関して、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/TALOT2-0509.pdf

5．今月の呼びかけ：「 ボットの脅威！ 」

―― 気付かぬうちにボットに感染していませんか？ ――

ボットとは、コンピュータウイルスの一種で、コンピュータに感染し、そのコンピュータを、ネットワーク(インターネット)を通じて外部から操ることを目的として作成されたプログラムです。

感染すると、自らネットワークを通じて外部の指令サーバと通信を行い、外部からの指示によりスパムメール送信活動や DoS 攻撃などの活動を実行します。さらに、自分自身のバージョンアップや、指示を待つ指令サーバの変更なども行います。

同一の指令サーバの配下にある複数(数千、数万になる場合もある)のボットは、指令サーバを中心とするネットワークを組むため、ボットネットワークと呼ばれています。これらのボットネットワークが、フィッシング目的などのスパムメールの大量送信や、特定サイトへの DDoS 攻撃などに利用されると、とても大きな脅威になります。

ボットなどのウイルスに感染し、被害者から加害者にならないために、以下の対策を実施してください。

（1） ウイルス対策ソフトやスパイウェア対策ソフトの導入および定義ファイル等の定期的な更新とウイルス検査の実施
（2） 見知らぬメールの添付ファイルは安易に開かない
（3） 不審な Web サイトの閲覧を控える
（4） ブラウザ等のインターネットオプションの有効利用
（5） スパムメールなどの、甘い誘いのリンクはクリックしない
（6） インターネット接続でのルータの利用やパーソナルファイアウォールの導入と、それらの正しい設定・運用
（7） コンピュータ上の OS やアプリケーションを常に最新状態にしておく(Windows Update の実行など)

詳細はこちらのサイトをご参照ください。

ボット対策について
http://www.ipa.go.jp/security/antivirus/bot.html
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

『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) ボット (bot)
コンピュータウイルスの一種で、コンピュータに感染し、そのコンピュータを、ネットワーク(インターネット)を通じて外部から操ることを目的として作成されたプログラム。

(*2) スパイウェア (spyware)
利用者の個人情報やアクセス履歴などの情報を詐取し、利用者以外のものに自動的に送信するソフトウェア。

(*3) 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。

(*4) ログ (log)
コンピュータの利用状況やデータ通信の記録のこと。一般的に、操作を行った者の ID や操作日時、操作内容などが記録される。

(*5) telnet (テルネット)
インターネットなどのネットワークにおいて、ネットワークに接続されたコンピュータを手元の端末から遠隔で操作する際に使うプログラム、または通信規約のこと。

(*6) 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。

(*7) 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。

■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