IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2005 年 10 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 9 月分］について

ボットやスパイウェアに侵入されていませんか？

●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 9 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－

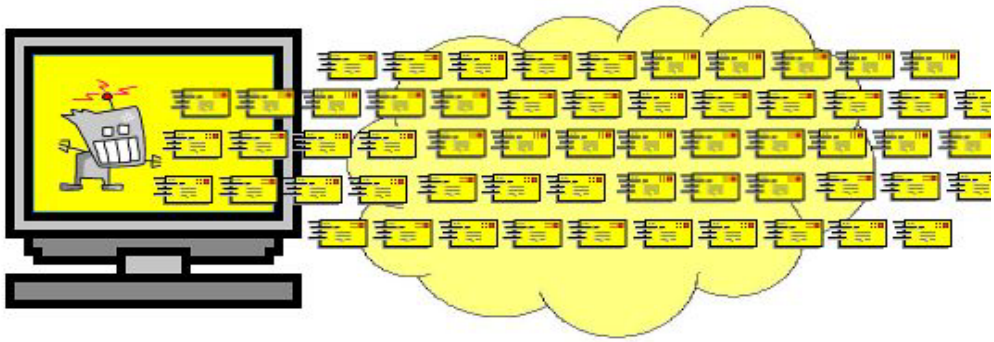
ウイルスの検出数(※1)は、**約 323 万個**と、8 月の約 337 万個から 4.2%の減少となりました。また、9 月の届出件数(※2)は、**4,723 件**となり、8 月の 4,470 件から 5.7%の増加となりました。

※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。
・9 月は、寄せられたウイルス検出数約 323 万個を集約した結果、4,723 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で総検出数のおよそ 8 割にあたる**約 256 万個**、2 位は **W32/Mytob** **約 51 万個**となっており、これら上位 2 種の検出数がいずれも減少した結果、総検出数は減少しています。一方、下記のとおり新種のウイルスが相次いで出現するなどにより、届出件数は増加となっています。

（1）ボットの機能を有したウイルスが出回る！

8 月に出現した Windows のセキュリティホールを悪用する **W32/Bobax**、**W32/Zotob**、**W32/IRCbot** 及び、依然として亜種が多数出現している **W32/Mytob** は、**ボット**(*1)**としての機能も有しています。**感染すると、外部からの指令を受けて、**スパムメールの発信元として利用**されたり、**特定のサイトを攻撃するための踏み台**にされたりする可能性があります。



スパムメール送信活動（多量のスパムメールを送信する）

攻撃の踏み台としてパソコンを使われてしまうと、感染した被害者という立場から、攻撃を行う加害者の立場に変わってしまいます。他者を攻撃する加害者とならないためにも、ウイルス対策を行うことが重要です。

IPA では、情報化月間の活動の一環として、ボットについて、性状や動作を整理して、概要と対策をまとめたしおりを作成しました。ボット対策の参考としてご活用ください。

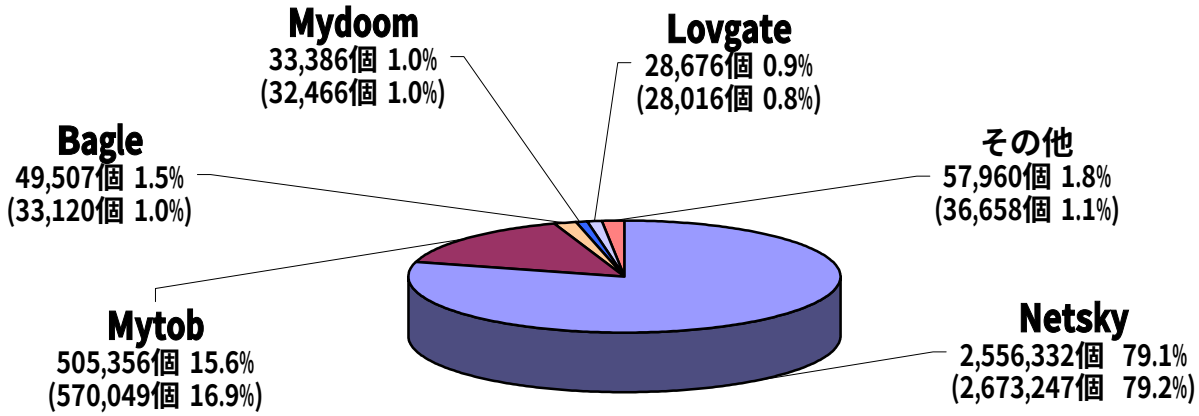
ボット対策のしおり
http://www.ipa.go.jp/security/antivirus/shiori.html

（2）W32/Netsky が総検出数の約 8 割を占める！

W32/Netsky の検出数が**約 256 万個**と、依然として総検出数の約 8 割を占める状況となっていますが、8 月の約 267 万個から 4.4%の減少となりました。また、**W32/Mytob** の検出数も 8 月の約 57 万個から約 51 万個と、11.3%の減少となりました。

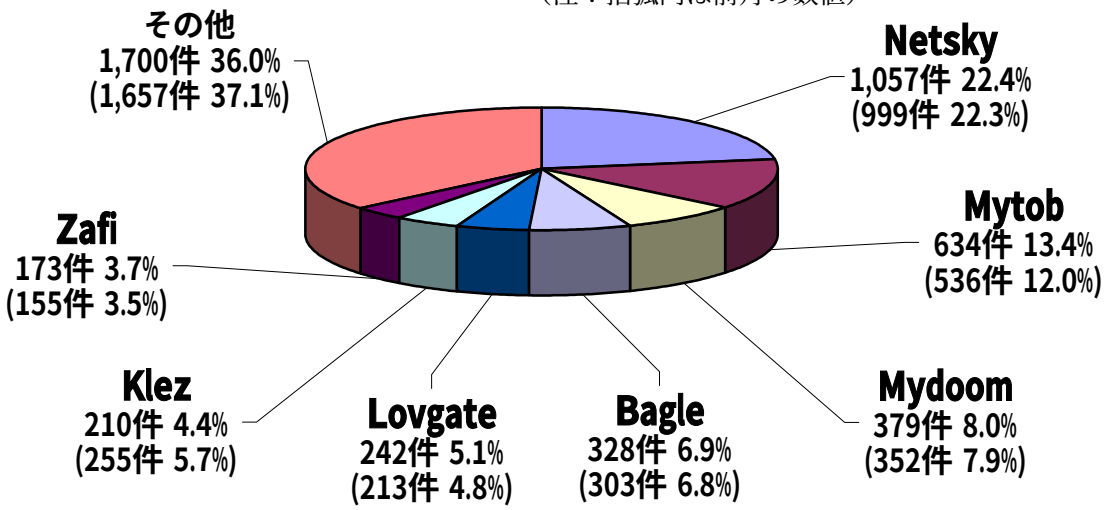
ウイルス検出数　323万個(337万個)　前月比 -4.2%

（注：括弧内は前月の数値）



ウイルス届出件数　4,723件 (4,470件)　前月比 +5.7%

（注：括弧内は前月の数値）



2．スパイウェアについて

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てしまうものや、Internet Explorer のスタートページを変更してしまうものなど、様々なスパイウェア(*2)等の不正プログラムが出回っています。

このようなウイルス以外の不正プログラムの被害に遭わないよう、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 は、NPO 日本ネットワークセキュリティ協会（JNSA）と共同で、スパイウェアについて定義づけを行い、対策をまとめたしおりを作成しました。スパイウェア対策の参考としてご活用ください。

スパイウェア対策のしおり
http://www.ipa.go.jp/security/antivirus/shiori.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	9月
届出[a] 計		**48**	**94**	**24**	**53**	**41**	**31**
	被害あり[b]	24	11	22	10	12	16
	被害なし[c]	24	83	2	43	29	15
相談[d] 計		**28**	**47**	**37**	**43**	**43**	**30**
	被害あり[e]	13	25	22	24	23	16
	被害なし[f]	15	22	15	19	20	14
合計[a+d]		**76**	**141**	**61**	**96**	**84**	**61**
	被害あり[b+e]	37	36	44	34	35	32
	被害なし[c+f]	39	105	17	62	49	29

IPA で受け付けた全ての相談件数の推移

	4月	5月	6月	7月	8月	9月
合計	**553**	**461**	**511**	**554**	**629**	**554**
自動応答システム	374	242	289	337	376	337
電話	115	118	143	128	179	144
電子メール	61	92	67	84	67	72
FAX・他	3	9	12	5	7	1

※ 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、ただし IPA セキュリティセンター員による相談受付は祝日を除く月～金、10:00～12:00、13:30～17:00 のみ）
※ 「自動応答システム」：電話の自動音声による応対件数
「電話」：IPA セキュリティセンター員による応対件数
※ 合計件数には、「不正アクセスの届出および相談の受付状況」における『相談[d] 計』件数を内数として含みます。

（1）不正アクセス届出状況

9 月の届出件数は 31 件であり、そのうち**被害のあった件数は 16 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 30 件（うち 6 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 16 件でした。

（3）被害状況

被害届出の内訳は、**侵入 8 件、ワーム感染 2 件、DoS 攻撃 2 件、アドレス詐称 2 件、その他(被害あり)2 件**でした。

侵入 8 件のうち、**SSH(*3)で使用するポート(*4)への攻撃が原因であったものが 5 件と大多数を占めており、今後も注意が必要です＜被害事例(ⅰ)参照＞**。 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、いわゆる『ワンクリック詐欺』**の事例が先月に引き続き、多数ありました＜7 月：28 件、8 月：83 件、9 月：80 件＞。

被害事例

[侵入]

（ⅰ） SSH で使用するポートへの攻撃

事例	SSH で使用するポートにパスワードクラッキング(*5)を受けてサーバに侵入された。侵入用のアカウント(*6)を作成されたり、IRC(*7)サービスを起動されたり、他のサーバに対する SSH パスワードクラッキング攻撃の踏み台にさせられていた。最終的にはウイルスがシステムに感染し、再起動不能にさせられた。OS（Linux）に対するセキュリティパッチ適用は成されていなかった。
解説・対策	安易なパスワードは、パスワード解析ツールなどで容易に解読されてしまいます。外部からアクセス可能なアカウントに設定する**パスワードは、推測容易なものは避けるとともに定期的に変更する**など、管理を徹底しましょう。また、OS の脆弱性を突かれないようにするためにも、**セキュリティパッチ適用をこまめにチェック**しましょう。さらに、**外部からアクセス可能にするアカウントや経路は最小限に抑えると共に、不用意に高いアクセス権限が付与されていないか、確認**しましょう。 （ご参考） IPA - 「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 IPA - 「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/

[ワーム感染]

（ii） 不正プログラムの埋込および外部への攻撃

事例	ファイアウォールソフトが、ワームやトロイの木馬など不正プログラムによる攻撃を遮断したためログ(*8)を調べてみたところ、遮断された通信が、自身のコンピュータから外向きのものだったこと、発信元である IP アドレスが自身のコンピュータに割り振られたものであることが判明。自身のコンピュータが数種の不正プログラムを埋め込まれており、それらが外部のコンピュータへ攻撃を仕掛けていた可能性が非常に高い。原因は不明。
解説・対策	ログの読み方が分からないと、こうした結論に達することは出来ませんでした。日頃からファイアウォールやウイルス対策ソフトなど、**自身が利用中のセキュリティ対策ソフトの使い方に精通しておく**ようにするとともに、**問題が生じた際の問い合わせ先（プロバイダ、セキュリティソフトベンダなど）を明確にしておきましょう**。 また、このケースでは、ウイルス対策ソフトが導入されていましたが、残念ながらウイルスは検出されていなかったようです。**ウイルス対策ソフトを過信せず、ファイルの取り扱いやウェブサイト閲覧時の基本的対策について再確認しましょう**。 （ご参考） IPA - パソコンユーザのためのウイルス対策 7 箇条 http://www.ipa.go.jp/security/antivirus/7kajonew.html IPA - 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

[その他]

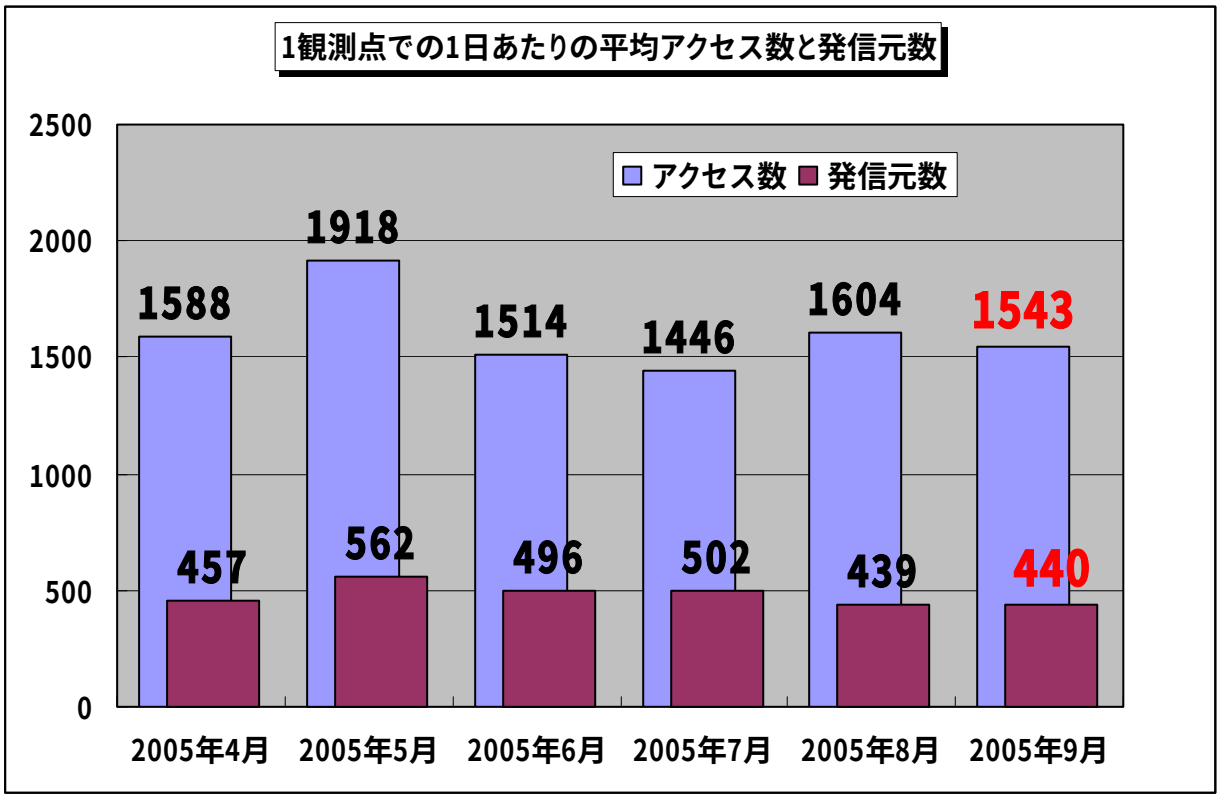
（iii）ネットオークションでの成りすまし

事例	クレジットカードで、身に覚えの無い請求があったため調査したところ、自身が登録していたネットオークションサイトで自分に成りすまされて ID を使われ、物品を出品されていた形跡があることが判明。その物品が落札されたため、システム手数料が発生していた。
解説・対策	**推測され易いパスワードを設定していたことが原因**と思われます。パスワード管理を改善するとともに、**こまめにサイトにアクセスし、不正に利用されていないかチェックするなどの自衛策も必要**です。万が一、不正に利用された場合でも金銭的被害を最小限に食い止めるために、決済専用の銀行口座を利用するのも有効な対策です。 （ご参考） IPA -「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

4．インターネット定点観測での９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 9 月の期待しない（一方的な）アクセスの総数は、10 観測点で **462,928 件**ありました。1 観測点で 1 日あたり **440** の発信元から **1,543 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 3.5 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。これは、2005 年 8 月とほぼ同じ状況です。



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/TALOT2-0510.pdf

5．今月の呼びかけ：「 ウイルス検査を定期的に行いましょう！ 」
―― 気付かぬうちに侵入されていませんか？ ――

IPA に寄せられた相談事例

A) パソコンの動きが遅いのでウイルス検査を実施したら、**1 年前からウイルスに感染していたことが判明**した。

B) デスクトップ上に請求書が表示されたので、あわててウイルス検査を行ったら、**メールアドレスを収集するスパイウェアと大量メール送信型のウイルスに感染していたことが判明**した。

このように、普段はウイルス検査を行わずにパソコンを利用していると、いつの間にか感染し、気付かない内に加害者となり、ウイルスを撒き散らしたり、迷惑メールの発信元として利用されていたりすることがあります。

ボットやスパイウェアに侵入されていないか、ウイルスに感染していないか、**少なくとも週 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**。

また、セキュリティホールを解消しておくことで、被害に遭う可能性を低減することができます。Windows ユーザは Microsoft Update を行うなど、日頃から継続して対策を実施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

『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) 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 (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。

(*5) パスワードクラッキング (password cracking)
他人のパスワードを、解析するなどして探り当てること。総当り攻撃や辞書攻撃といった手法があり、クラッキング用のプログラムも存在する。

(*6) 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。

(*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。

(*8) 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。

■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

お知らせ

ＩＰＡ債務保証制度の紹介

ＩＰＡ債務保証制度では、セキュリティソフトウェアの開発等に係る必要資金に対して、無担保の保証を行うことにより、資金調達の支援をしております。本制度については、ＩＰＡホームページ又は下記の連絡先までお問い合わせください。

○保証額：融資額の 95%以内　　○保証融資限度額：1 件あたり 150 百万円以内
○保証期間：3 年以内（一般債務保証制度）、5 年以内（新技術債務保証制度）
○保証料率：年 0.75%（連帯保証人 2 名以上の場合等は年 0.5%）
○連絡先：ＩＰＡ 金融推進部　℡：03-5978-7505
URL：http://www.ipa.go.jp/software/hosyo/

【活用事例紹介】

製造業であるＡ社は、個人情報保護への対応や業務の効率化を図ることを目的に、新たなセキュリティソフトウェアを外注で開発[注]するため、30 百万円の資金調達が必要であった。このため、ＩＰＡ債務保証制度（一般債務保証制度）を利用して、金融機関から融資（融資額 30 百万円、融資期間 3 年）を受け、セキュリティソフトウェアを開発、導入した。

注）セキュリティソフトウェアを外注で開発する場合は、新たな開発行為があるので債務保証制度の対象になります。一方、パッケージソフトウェアを購入する場合は、新たな開発行為がないので対象になりません。