IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2006 年 3 月 3 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［2006 年 2 月分］について

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、2006 年 2 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。

今月の呼びかけ：
「ファイル交換ソフトに潜む情報漏えいの危険性！！」
―― それでも貴方は使いますか？ ――

最近、Winny というファイル交換ソフトを介した情報漏えい事故が多数報道されています。これらのほとんどが Winny を利用して感染を拡大する W32/Antinny というウイルスに感染することにより発生しています。

W32/Antinny ウイルスは、**「お宝画像」、「個人情報」のような多数の人が興味をもつ単語を含むファイル名で Winny のネットワークに流通しており、Winny を利用してダウンロードしたそれらのファイルをユーザが実行することにより情報漏えい事故が起きています**。

Winny の利用者は複数のファイルを1つのファイルにまとめて圧縮し流通させることが多く、そのような圧縮ファイルを装った W32/Antinny ウイルスもあります。ユーザがそのウイルスファイルをクリックしたとき、圧縮ファイルの内容を見ることができないことに不審を抱かぬよう、図 1.1 のような偽のメッセージをウイルスが表示し、ユーザに感染を気づかせないようにします。

図 1.1 ウイルスが表示させる偽メッセージの例

このウイルスに感染すると、**パソコン内の送受信メールや Word や Excel 等のデータファイルが集約され、公開フォルダにコピー**されてしまいます。公開フォルダにコピーされるということは、Winny を利用しているユーザ誰もが、そのファイルを入手できるということです。図 1.2 に示すように、一旦 Winny のネットワークに流出したデータは、不特定多数が保有することになり、事実上、回収することは不可能です。

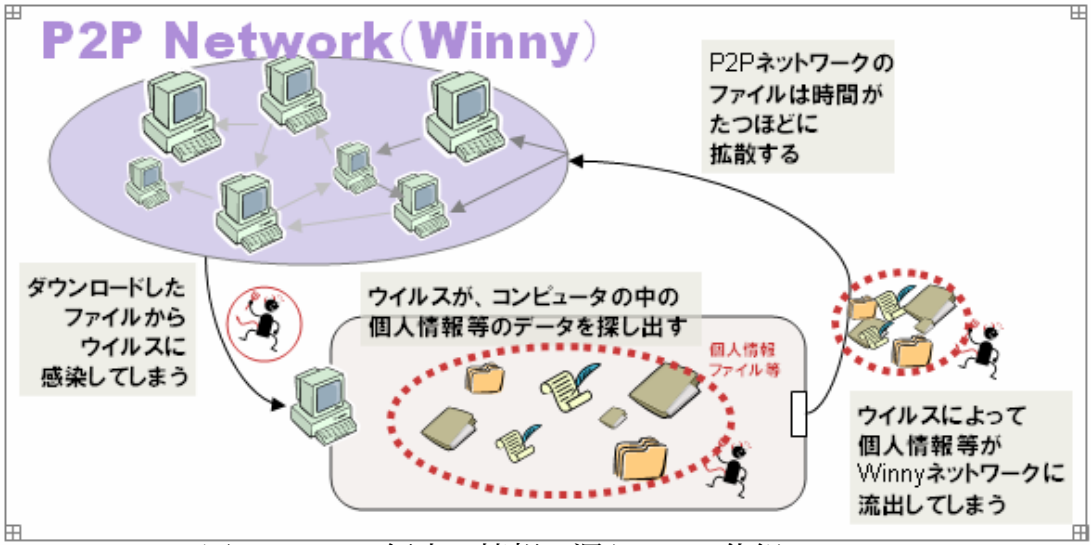


図 1.2 Winny 経由で情報が漏えいする仕組み

感染を未然に防ぐためには、パターンファイルを最新にしたウイルス対策ソフトを利用することが重要です。ただし、W32/Antinny ウイルスの亜種が次々に発生しているため、検出できないこともありますので、ダウンロードしたファイルを安易に実行しない（圧縮ファイルの解凍も含む）ことも必要です。なお、感染に気付いた場合もそうでない場合も、マイクロソフト社より駆除ツールが提供されていますので、検査することをお勧めします。

Microsoft 社 - 悪意のあるソフトウェアの削除ツール
http://www.microsoft.com/japan/security/malwareremove/default.mspx

個人情報保護やセキュリティの観点から、多くの企業ではファイル交換ソフトの利用が禁止され、個人情報や機密情報の社外持ち出しも禁止されています。このようなルールが整備されていても、漏えい事故は度々発生しています。自分だけは大丈夫という認識は大きな間違いです。
情報漏えいを起こした個人に対する罰則として、停職や減給などの処分が下されている例が報道されています。また、当事者となった企業･組織への影響は計り知れません。
ファイル交換ソフトに潜む危険を理解し、同じ事故を繰り返さないようにしてください。
なお、ファイル交換ソフトを利用した違法なデータのやり取りは論外です！

― ファイル交換ソフト使用上の注意事項 ―

1.ファイル交換ソフトの使用条件は決められていますか。
(1)業務で必要ということで入れているのか？
(2)使用することを許可制にしているか？
(3)管理は充分であるのか？
2.クライアントのパソコンにおけるウイルス対策状況を把握していますか。
(1)クライアントのパソコンにウイルス対策ソフトを装備しているか？
(2)パターンファイルを更新しているか？

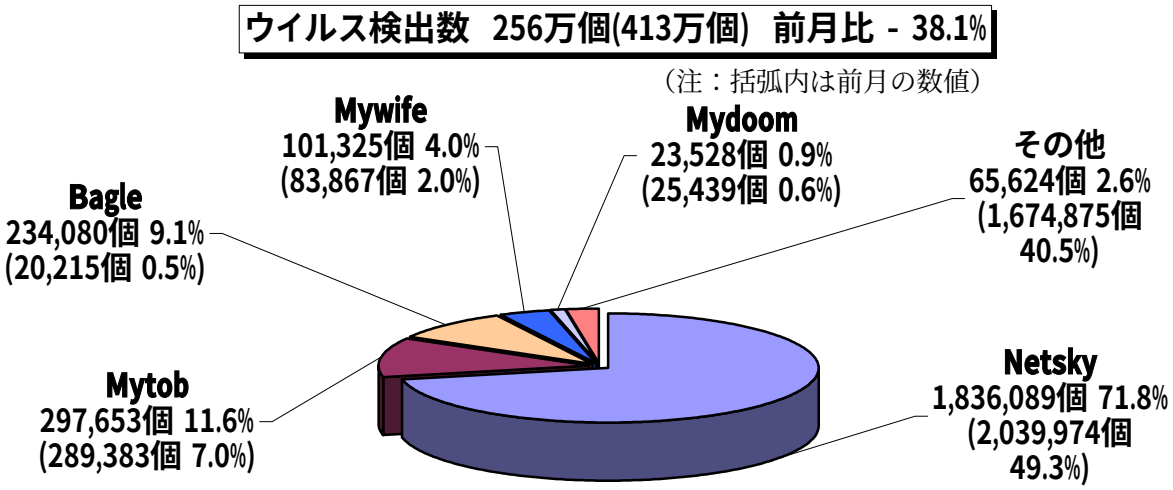
（参考）IPA – ファイル交換ソフト使用上の注意事項
http://www.ipa.go.jp/security/topics/20050623_exchange.html

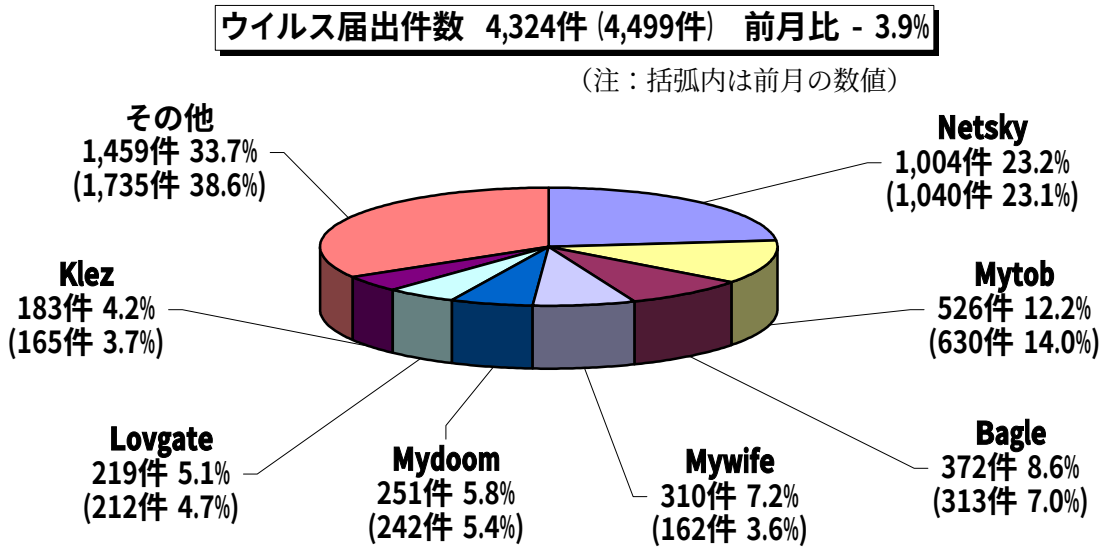
1．コンピュータウイルス届出状況 ―詳細は別紙 1 を参照―

ウイルスの検出数(※1)は、**約 256 万個**と、1 月の約 413 万個から約 4 割の減少となりました。12 月に多数の検出が寄せられた W32/Sober の当該亜種が完全に収束したためです。
また、2 月の届出件数(※2)は、**4,324 件**となり、1 月の 4,499 件から 3.9%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（個数）
※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 日何個検出されても届出 1 件としてカウントしたもの。
･2 月は、寄せられたウイルス検出数約 256 万個を集約した結果、4,324 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 184 万個 、2 位は W32/Mytob** で**約 30 万個、3 位は W32/Bagle** で**約 23 万個でした。**





2 月には、**OSX/Inqtana という、Macintosh を対象としたウイルスの届出**がありました。このウイルスは、Macintosh 環境でもウイルスが動作できることを証明するために作成されたといわれており、感染が拡大しているわけではありません。しかし、ウイルスといえば Windows でしか動作しないということではなく、Macintosh でも Linux でもウイルスが蔓延する可能性がありますので、日頃からウイルス情報等を確認し、ウイルス対策を実施しておきましょう。

2．スパイウェアについて

スパイウェア(*1)による主な被害は以下のものがあります。

- メールアドレスの漏えい
- オンラインバンキングなどのアカウントとパスワードの漏えい
- クレジットカード番号などの個人情報の漏えい

また、二次的な被害として、上記の情報が悪用され、なりすましによる金銭的な被害の発生がマスコミにより報道されています。

相談としては、アダルトサイトで画像をクリックしただけでスパイウェアがインストールされ、普段使用しているメールアドレスが抜き取られるといった事例が多く見られます。

スパイウェアの被害に遭うと、気付かないうちに上記の漏えいが起きてしまいます。以下に掲げる対策を実施すると共に、安易にダウンロードしない等の注意を払い、被害に遭わないようご注意ください。

(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する
(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
補足：自分で管理できないコンピュータでは、重要な個人情報の入力を行わない

スパイウェア対策のしおり
http://www.ipa.go.jp/security/antivirus/shiori.html
今月の呼びかけ:「スパイウェアにだまされるな！！」 ― 怪しいファイルの見分け方 ―
http://www.ipa.go.jp/security/txt/2005/12outline.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

		9月	10月	11月	12月	1月	2月
届出(a) 計		**31**	**22**	**24**	**25**	**50**	**26**
	被害あり(b)	16	15	15	19	13	15
	被害なし(c)	15	7	9	6	37	11
相談(d) 計		**30**	**35**	**30**	**25**	**43**	**42**
	被害あり(e)	16	25	18	15	23	24
	被害なし(f)	14	10	12	10	20	18
合計(a+d)		**61**	**57**	**54**	**50**	**93**	**68**
	被害あり(b+e)	32	40	33	34	36	39
	被害なし(c+f)	29	17	21	16	57	29

(1) 不正アクセス届出状況

2 月の届出件数は 26 件であり、そのうち**被害のあった件数は 15 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 42 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 24 件でした。

(3) 被害状況

被害届出の内訳は、**侵入 9 件、DoS 攻撃 2 件、アドレス詐称 1 件、その他(被害あり)3 件**でした。
侵入届出のうち、**SSH(*2)で使用するポート(*3)への攻撃を受けた結果侵入されたという届出が 7 件と相変わらず非常に多く、引き続き注意が必要です**。その他、Web サーバに侵入されてフィッシングに悪用するための Web コンテンツを設置された届出が 1 件ありました。

被害事例

[侵入]

(i) SSH(*2)で使用するポートへの攻撃

事例	・ネットワーク管理者が、「不審な通信をしている」との通報を外部から受けた。 ・調査の結果、SSH で使用するポートへ攻撃を受け、**ID とパスワードが同一であったアカウント(*4)から侵入されていた**ことが判明。 ・ボット(*5)と思われる不正なプログラムを置かれていた。さらに当該プログラムは外部の IRC(*6)サーバとの間で通信を行っていたことも分かった。
解説・対策	全く同様の原因による侵入事例は他にも 2 件ありました。改めて、**アカウント管理とパスワード変更管理を徹底しましょう**。これらの例に限らず、外部からの通報により初めて気付くケースが多いようです。**常日頃からアクセスログ(*7)をチェックして一刻も早く攻撃の兆候を掴み、必要な対策を講じることが重要です**。また、侵入後の振る舞いとしては、ボットの指令用として運用されている IRC(*6)サーバから攻撃などの指示を受け取りボットとして操られていたり、SSH スキャンツール(*8)を埋め込まれて他サイト攻撃の踏み台として利用されたりと、**他サイトに危害を及ぼすケースがほとんど**のようです。知らぬ間に迷惑行為に加担してしまうことのないよう、絶対に侵入を許してはなりません。**SSH 運用時には、ログインの際に公開鍵認証(*9)などの強固な認証を採用することを推奨します**。 (参考) IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/20060131_websecurity.html

[DoS]

(ii) 大量の不正アクセス試行のため接続障害発生

事例	・個人運用のメールサーバにて、メールの送受信に障害が発生。 ・インターネット側から、当該サーバに向けて、存在しないユーザアカウントを使って接続を試みるアクセスがあったことを確認。 ・侵入は許していないものの、メールサーバが高負荷となったため、メールサービスが妨害されていた。
解説・対策	不正アクセス試行の目的は分かりませんが、先月から同様の届出が、被害なしのものも含め計 3 件来ていることもあり、今後も注意が必要です。**インターネット側からメールの送受信の要求を受ける必要が無いのであれば、ポートを閉じるなどの対策を講じましょう**。**ポートを空けておく必要があるのであれば、通信相手を特定すべくアクセス元 IP アドレスを制限したり、サーバの負荷を上げないために、エラーメッセージを返すことなくパケット破棄したりするなどの対策を講じましょう**。 (参考) IPA - コンピュータ不正アクセス被害防止対策集 http://www.ipa.go.jp/security/ciadr/cm01.html#DoS

4．相談受付状況

2 月の相談件数は、**834 件**でした。そのうち、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るなど、いわゆる**『ワンクリック不正請求』に関する相談**は相変わらず非常に多く、**168 件**もありました。また、ワンクリック不正請求に関する相談のうちほぼ **9 割が、スパイウェアなどの不正なプログラムを埋め込まれたケース**となっています。＜ワンクリック不正請求相談件数推移…7 月：28 件、8 月：83 件、9 月：80 件、10 月：108 件、11 月：165 件、12 月：138 件、1 月：174 件＞。

（注：先月発表した 1 月のワンクリック不正請求相談件数に誤りがありました。正しくは、174 件です。ここで訂正するとともに、お詫びいたします。）

IPA で受け付けた全ての相談件数の推移

	9月	10月	11月	12月	1月	2月
合計	**554**	**606**	**673**	**653**	**748**	**834**
自動応答システム	337	357	379	391	425	479
電話	144	165	220	194	228	258
電子メール	72	82	66	66	87	90
FAX・他	1	2	8	2	8	7

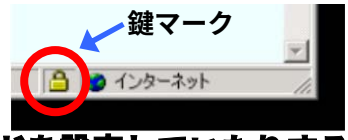
※ IPA では、コンピュータウイルス・不正アクセス、その他情報セキュリティ全般についての相談を受け付けています。
メール：virus@ipa.go.jp（ウイルス）、crack@ipa.go.jp（不正アクセス）
電話番号：03-5978-7509（24 時間自動応答、ただし IPA セキュリティセンター員による相談受付は休日を除く月～金の 10:00～12:00、13:30～17:00 のみ）
FAX：03-5978-7518（24 時間受付）

※ 「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

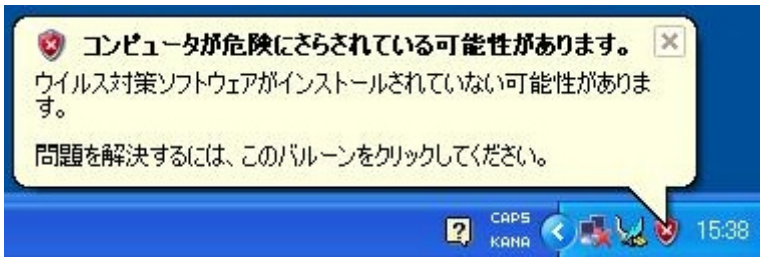
※ 合計件数には、「不正アクセスの届出および相談の受付状況」における『相談(d) 計』件数を内数として含みます。

主な相談事例は以下の通りです。

(i) パスワードについて

相談	会員制のサイトにログインする際に、パスワード欄には「＊＊＊」などと伏せ字で表示されていますが、通信の途中で盗み見られることはあるのでしょうか。
回答	**一般的には手元で「＊＊＊」となっていても、実際にネットワーク上を流れる際には伏せ字ではなく平文です**ので、盗み見られるとパスワードが解読されてしまいます。**ただ、暗号化通信の場合は、もしネット上で盗み見られても解読は出来ません**。暗号化通信の場合は、インターネットエクスプローラ画面の右下部分に鍵のマークが現れます。アドレスは、通常は http:// で始まりますが、暗号化通信（SSL通信）の場合は https:// となっています。なお、  **ネット上で盗み見られなくても、簡単なパスワードを設定していたりすると、比較的容易に破られてしまいます**。解読されにくいパスワード設定方法については、次の情報をご参照ください。 (参考) 「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#spe1

(ii) 「コンピュータが危険にさらされている可能性があります」と表示されます

相談	パソコンを使っていると、画面右下あたりに「コンピュータが危険にさらされている可能性があります」と表示されます。ウイルスに感染しているのでしょうか。 
回答	これは、お使いの**パソコンにウイルス対策ソフトが導入されていない場合などに、Windows XP が発する警告メッセージです。このメッセージが出たからといって、必ずしもパソコンがウイルスに感染している訳ではありません**。しかしながら、ウイルス感染を未然に防ぐためにも、ウイルス対策ソフトを導入することを、強くお勧めします。 (参考) "コンピュータが危険にさらされている可能性があります" のメッセージについて http://support.microsoft.com/default.aspx?scid=kb;JA;883807

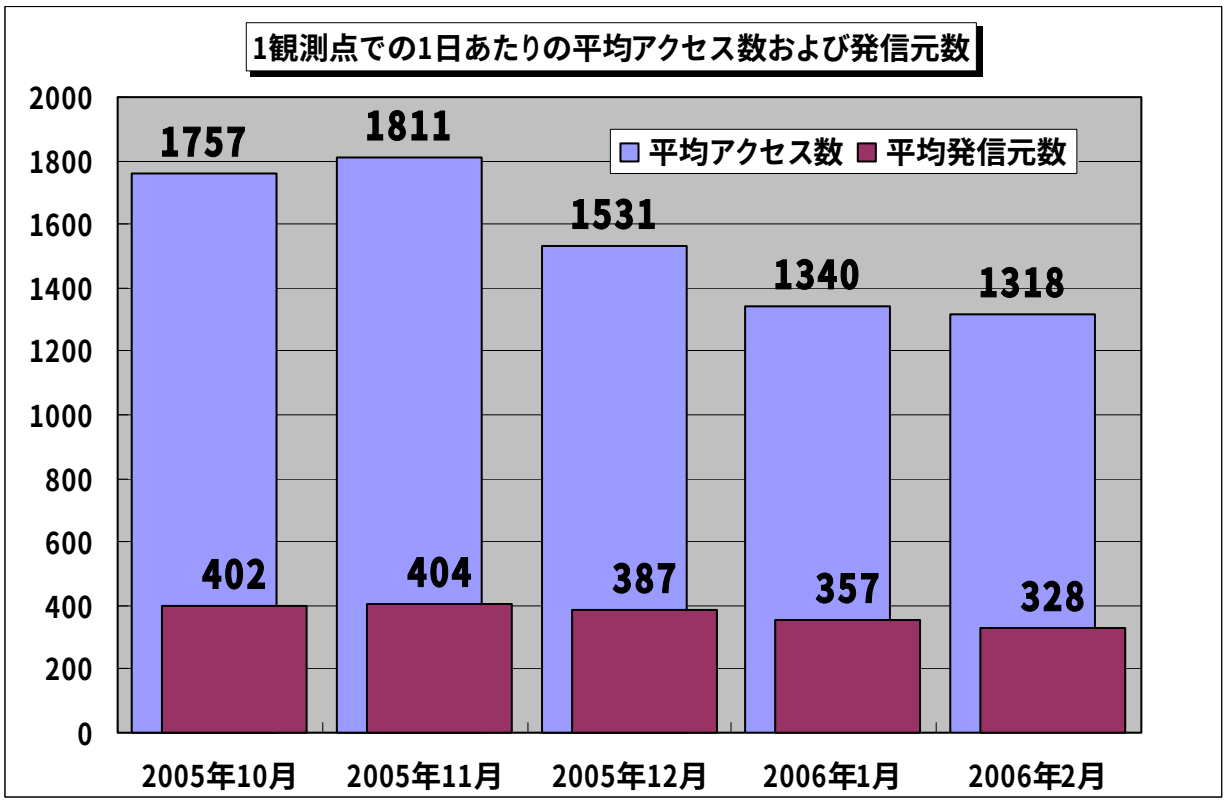
なお、依然として多数の相談件数を占めるワンクリック不正請求に関する対策情報は、以下のサイトに掲載しておりますので、ご参照ください。

IPA - 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

5．インターネット定点観測での２月のアクセス状況

インターネット定点観測(TALOT2)によると、2006 年 2 月の期待しない（一方的な）アクセスの総数は、10 観測点で **316,533 件**ありました。1 観測点で 1 日あたり **328** の発信元から **1,318 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、328 人の見知らぬ人(発信元)から、発信元一人当たり 4 件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。



【図 5.1　1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数】

2005 年 10 月～2006 年 2 月までの各月の 1 観測点での 1 日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図 5.1 に示しています。この図を見ると、期待しない（一方的な）アクセスは、発信元数も含めて、緩やかに減少傾向にあるようです。さらに、アクセス内容についても定常化(後述の統計情報を参照下さい)していると言えます。

2 月のアクセス状況は、1 月の状況とほぼ同じようです。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、特にアクセス数の多い 135(TCP)ポート,445(TCP)ポートへのアクセスは、Windows の脆弱性を狙っています。

また、一時的ではありますが、Microsoft SQL Server[A]の稼動するサーバを狙ったアクセス[1433(TCP)ポートへのアクセス]も増加しました。

さらに、統計情報等には出ていませんが、パスワードクラッキングでのシステムへの侵入を目的とした、MySQL[B]の稼動するサーバを狙ったものと思われるアクセス[3306(TCP)ポートへのアクセス]や SSH(*2)を狙ったアクセス[22(TCP)ポートへのアクセス]も見受けられます。

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を心掛け、さらに利用するアプリケーションのパスワード強化や接続認証の強化を実施して下さい。

[A] マイクロソフト社の SQL データベース

[B] オープンソース SQL データベース

一般のコンピュータ利用者は、これらの不正なアクセスによる感染を予防するために、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やパーソナルファイアウォール等の有効利用をお勧めします。

特記事項

2006 年 2 月の実際の観測データのうち、特定の観測点に集中して発生したアクセスがあります。この観測データについては、報告の統計情報にそぐわないため、除外してあります。

除外した観測データは、いわゆる P2P ファイル交換ソフトが使用するアクセスでした。

TALOT2 ではインターネットの一般利用者と同様の環境で観測するために、不定期に観測点の IP アドレスを変更します。これらのIPアドレスの、以前の利用者が、P2P ファイル交換ソフトを使用していたようで、これらのIPアドレス宛てに他の利用者から接続要求が、観測点に送られてきたようです。

今回 TALOT2 で観測された上述のアクセスのうち特に目立ったものは、1 箇所の発信元から、特定観測点のIPアドレスに対して、30 秒間隔で 3 回ずつのアクセスが繰り返し行われ、そのアクセスが 4 日間も継続したことです。これは、P2P ファイル交換ソフトを自動的に動作させ、アクセスを続けていたものと思われます。

このような状況が発生する可能性は、以前に比べて多くなっているようで、P2P ファイル交換ソフトのものと思われるアクセスが多く見受けられます。P2P ファイル交換ソフトの利用者が増加していることを示しているようです。

P2P ファイル交換ソフトを利用する方は、このような状況が発生することを認識し、ソフトの利用の際は、通信の相手が正しいことを確認していただきたいと思います。場合によっては、DoS 攻撃(*10)とみなされる可能性もあります。十分注意して下さい。

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/2006/documents/TALOT2-0603.pdf

『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) スパイウェア (spyware)
利用者や管理者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラム等。

(*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) 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。

(*6) 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。

(*7) 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。

(*8) SSH スキャンツール
サーバで SSH サービスが動作しているかを調べるためのツール。パスワードを破るための機能を持ったものもある。

(*9) 公開鍵認証
公開鍵と秘密鍵のペアでユーザ個人の認証を行う方式のこと。

(*10) DoS 攻撃 (Denial of Services)
サーバに大量のデータを送って過大な負荷をかけ、サーバのパフォーマンスを極端に低下させたり、サーバを機能停止に追い込んだりする攻撃のこと。

■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

お知らせ

『情報セキュリティ対策ベンチマークシステム』の紹介

IPA では、**「情報セキュリティ対策ベンチマークシステム」**を Web サイト上に公開しております。
情報セキュリティ対策ベンチマーク
http://www.ipa.go.jp/security/benchmark/

本システムは、企業を対象としたもので、セキュリティ対策状況及び企業情報に関する設問(計40 問)に答えることにより、セキュリティ対策の取組状況を自己採点できるシステムです。

診断結果は、「貴社のスコア」と「望まれる水準」とが同時に表示され、各社が優先的に取り組むべきセキュリティ対策項目が明らかになります。また、推奨される取り組み事例も提示しますので、今後の対策を強化する上での具体的な改善策がわかります。

30 分程度で自己採点できますので、ぜひ、今後のセキュリティ対策の参考とすべく、ご活用ください。

『ＩＰＡ債務保証制度』の紹介

IPA 債務保証制度では、**ソフトウェア業だけでなく、あらゆる業種の企業を対象**に、情報セキュリティ対策をはじめとするソフトウェアの開発･導入（外注を含む。）に必要な資金に対して、**無担保で保証**を行うことにより、資金調達の支援を行っています。
本制度の詳しい内容につきましては、下記の連絡先までお問い合わせいただくか、ＩＰＡホームページをご覧ください。

記

･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　･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 金融推進グループ TEL：03-5978-7505
･URL：http://www.ipa.go.jp/software/hosyo/

【活用事例紹介】
食品加工業であるＡ社は、顧客情報に関する個人情報保護対応や、業務の効率化を図ることを目的に、新たに自社の業務管理システムのソフトウェアを外注で開発。１５百万円の資金調達が必要なため、ＩＰＡ債務保証制度を活用。