IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
第 07-16-111 号
2007 年 10 月 2 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［2007 年 9 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、2007 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. 今月の呼びかけ

今月の呼びかけ： 「 ボットの脅威をご存知ですか？ 」
― ウイルスの一種であるボットに注意しましょう！ ―

9 月に IPA へ寄せられた届出や相談の中で、「プロバイダから『貴方のパソコンがボットに感染していますので対策をお願いします』と連絡があったのですが」と、ボットに感染したと思われる方からの相談が複数寄せられました。
ボット感染の脅威及び対策の必要性を認識して、対策を実施することにより、ボット感染の予防、早期発見、駆除を確実に行っていただくようお願いします。

(1) ボットの脅威

ボットはコンピュータウイルス等と同様な方法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。

ボットに感染したコンピュータは、攻撃者が用意した指令サーバなどに自動的に接続され「ボットネットワーク」といわれる数台～数十万台で構成されるネットワークの一部として組込まれてしまいます。

ボットネットワークに組み込まれたコンピュータは、攻撃者の指令サーバなどから遠隔操作され、**スパムメールの大量送信**や、**特定サイトへのサービス妨害攻撃（DoS:Denial of Services）**などに利用されます。

最近では「ボットネットワーク」を時間貸ししたり、ボットによって窃取した個人情報を販売したりするなど、犯罪に利用して利益を得る行為が確認されています。

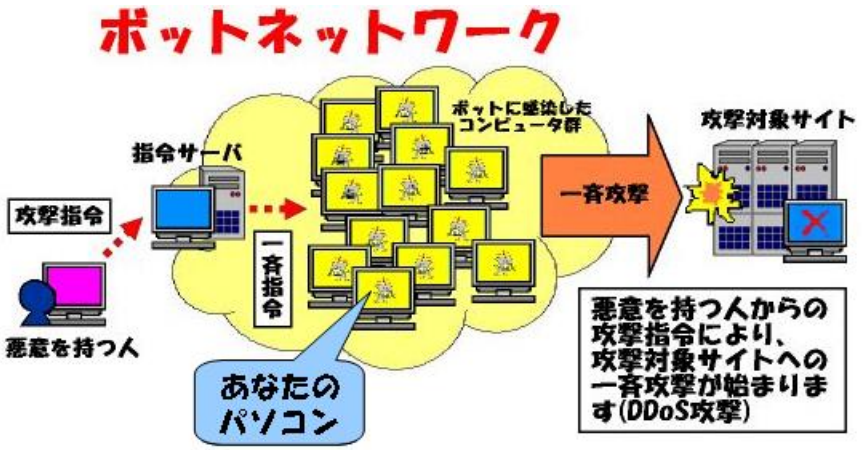


図 1-1：ボットネットワークの脅威

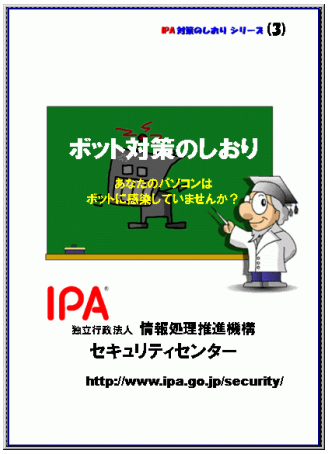
(2) ボット感染の特徴

いままでのボットは、**メールの添付ファイルを開くことによる感染**や、**ぜい弱性を突いた攻撃による感染など**が主な感染経路でした。

しかし**最近では、ボットが埋め込まれたウェブページを閲覧することによる感染の被害が多くなり**、感染経路が利用者にはわかりにくくなってきています。

また、ボットに感染しても特別な症状が出ないことが多く、感染前と同じようにコンピュータを使用できるなど、利用者がボットに感染したことに気が付きにくい特徴があります。

(3) 一般ユーザ向けボット対策のポイント



(a)ウイルス対策ソフトやスパイウェア対策ソフトの導入と、それらのソフトが使用するパターンファイル等の定期的な更新を行う(ボットは短期間でバージョンアップする機能があるため、パターンファイルの更新は非常に大事である)
(b)見知らぬメールの添付ファイルは安易に開かない
(c)不審なウェブサイトの閲覧を控える
(d)ブラウザ等のセキュリティ設定を高く設定する
(e)迷惑(スパム)メールなどに表示されているリンクはクリックしない(見ないで廃棄するのが望ましい)
(f)インターネット接続には、ルータやパーソナルファイアウォールを利用する
(g)コンピュータ上のOSやアプリケーションを常に最新の状態にする(Microsoft Update の実行など)

詳細は、「ボット対策のしおり ver.5 2007 年 6 月 1 日発行」をご参照ください。
http://www.ipa.go.jp/security/antivirus/documents/3_bot_v5.pdf

コンピュータがボットに感染していた場合、**駆除することが唯一の対策**となります。また、利用者はボット感染に気付きにくいため、プロバイダなどの第三者からの連絡によって初めて感染が発覚することが多く見受けられます。**プロバイダなどからボット感染について注意喚起のメールが送られてきましたら、そのメールは無視しないで、メールの内容に従って駆除を実施する、(5)で紹介するサイバークリーンセンターが提供する駆除ツールでボットを駆除してください。**

(4) ウェブ運営者等におけるボット対策のポイント

最近、MPack と呼ばれる攻撃ツールを利用されウェブサイトが乗っ取られるなどの被害が増加しています。(http://www.jpcert.or.jp/at/2007/at070016.txt)
ウェブ運営者及びサーバ管理者は、運営しているサーバが、知らないうちにボットなどの感染活動の拠点にならないようにするために以下に示すような対策を行う必要があります。

(a)ウェブアプリケーションのぜい弱性が無いかをチェックし、ボットの感染用に改ざん(ウイルスの埋め込みなど)されないように対策する
(b)ウェブサーバ上の OS やアプリケーションを常にぜい弱性の無い状態とする
(c)サイトを閲覧してウイルス対策ソフトが反応したとの問合せなど、ウェブサイトに異常が見つかったら、即座にウェブサイトを閉鎖するなど被害拡大防止の措置をとる

(5) IPA のボット対策への取り組み

IPA は、2006 年 12 月より開始された総務省及び経済産業省の合同プロジェクトである「ボット対策事業」において、「ボット」を撲滅することを目的として設立された、サイバークリーンセンター(Cyber Clean Center, https://www.ccc.go.jp/)の運営に協力しています。
サイバークリーンセンターでは、インターネットにおける脅威となっているボットの特徴を解析するとともに、ユーザのコンピュータからボットを駆除するためのツール及び必要な情報をユーザに提供する活動を行っています。また、IPA は「ボット感染予防推進グループ」として感染予防対策ベンダに対してボットの検体を提供することにより、感染予防及び再発防止の推進を行っています。

サイバークリーンセンターの活動実績を「2007 年 8 月度　サイバークリーンセンター活動実績」（https://www.ccc.go.jp/report/200708/0708monthly.html）で公開していますので、参考にして下さい。

2. IPA で行っているウイルス対策の取り組みに関連した情報の紹介

●情報漏えい発生時の対応ポイント集

－情報が漏えいしてしまった時、何をすべきか!! －

本小冊子は、情報漏えいインシデント対応マニュアルを整備していない中小企業などにおいて、情報漏えい事故が発生した場合、何をする必要があるか、何に気をつけなければいけないかを経営者をはじめとする対応チームの方々が短時間に理解し、速やかに適切な対応ができるように分かりやすく解説しています。

■目次

第 1 版　2007/08　発行

URL　http://www.ipa.go.jp/security/awareness/johorouei/

今月のトピックス

○ コンピュータ不正アクセス被害の主な事例（届出状況及び被害事例の詳細は、6 頁の「4.コンピュータ不正アクセス届出状況」を参照）

・フィッシングに悪用するためのコンテンツを設置された
・サーバが不正ログイン試行を受けている

○ 相談の主な事例（相談受付状況及び相談事例の詳細は、8 頁の「5.相談受付状況」を参照）

・メールの本文にあったリンクをクリックしたら、ウイルス警告が！
・Winny で情報が漏えいしてしまった・・・

○ インターネット定点観測（詳細は、別紙 3 を参照）

IPA で行っているインターネット定点観測について、詳細な解説を行っています。

・リモートでアクセスするコンピュータを狙ったアクセスに注意！

3. 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 44 万個**と、8 月の 49 万個から 11.4%の減少となりました。
また、9 月の届出件数(※2)は、**2,426 件**となり、8 月の 2,806 件から 13.5%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(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。
・9 月は、寄せられたウイルス検出数約 44 万個を集約した結果、2,426 件の届出件数となっています。

検出数の1位は、**W32/Netsky で約 40 万個 、2 位は W32/Mytob で約 1.5 万個、3 位は W32/Bagle で約 5 千個でした。**

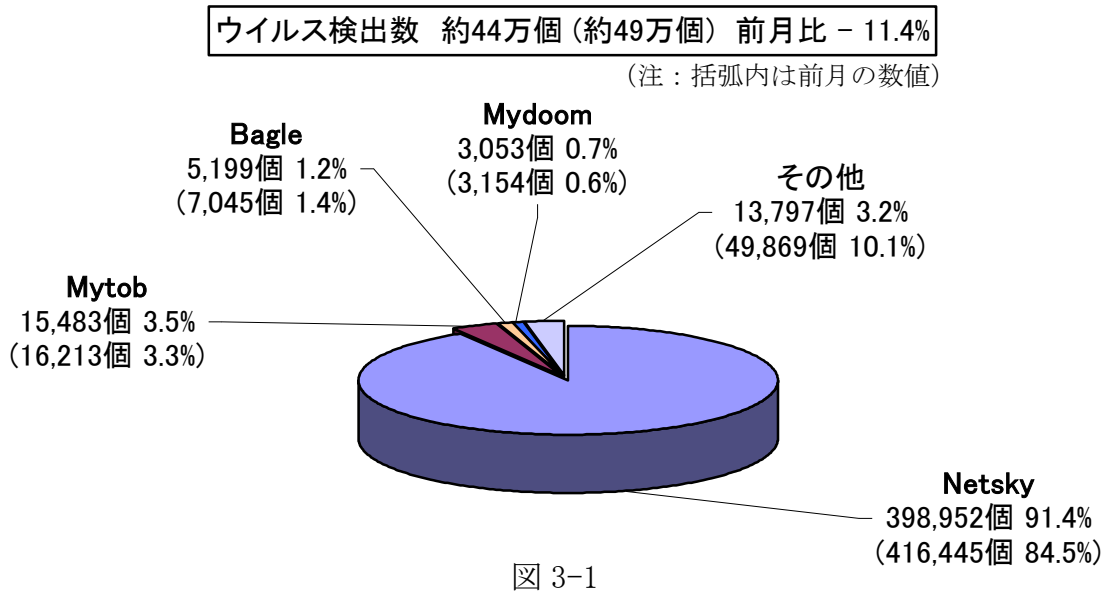


図 3-1

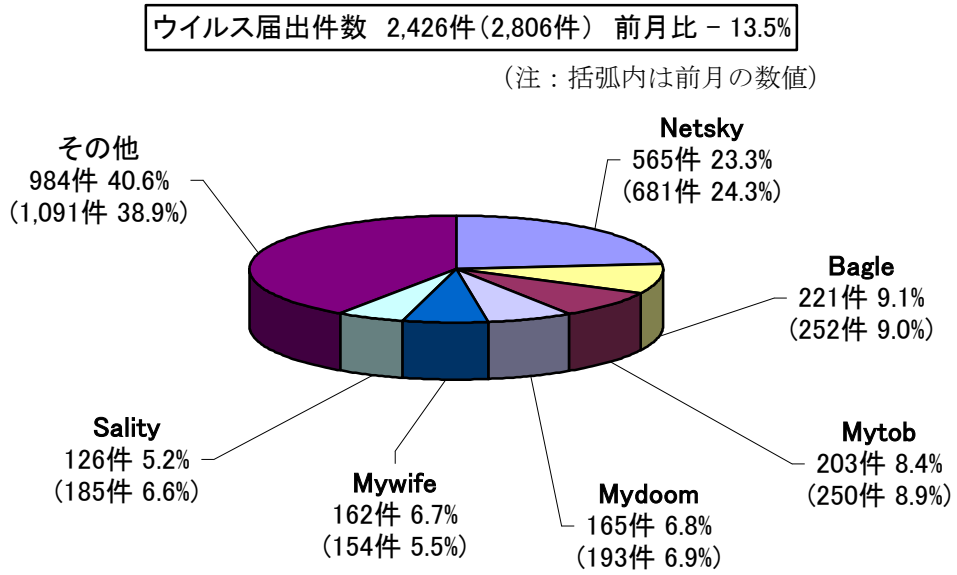


図 3-2

4. 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		**15**	**19**	**41**	**10**	**16**	**10**
	被害あり(b)	12	13	36	8	13	8
	被害なし(c)	3	6	5	2	3	2
相談(d) 計		**31**	**37**	**27**	**25**	**23**	**27**
	被害あり(e)	20	21	11	11	15	12
	被害なし(f)	11	16	16	14	8	15
合計(a+d)		**46**	**56**	**68**	**35**	**39**	**37**
	被害あり(b+e)	32	34	47	19	28	20
	被害なし(c+f)	14	22	21	16	11	17

(1) 不正アクセス届出状況

9 月の届出件数は 10 件であり、そのうち**被害のあった件数は 8 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 27 件（うち 4 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 12 件でした。

(3) 被害状況

被害届出の内訳は、**侵入 2 件、アドレス詐称 1 件、その他（被害あり）5 件**でした。

侵入届出の被害内容は、フィッシング※に悪用するためのコンテンツを設置されていたものが 1 件、などでした。侵入の原因は、サーバ OS のぜい弱性放置によるものが 1 件などでした。

※フィッシング（Phishing） … 正規の金融機関など実在する会社を装ったメールを利用して偽のウェブページに誘導し、それを見た利用者の ID やパスワードなどを詐取しようとする行為のこと。

（4）被害事例

［侵入］

（i）フィッシングに悪用するためのコンテンツを設置された

事例	・自社のウェブサイトのコンテンツ作成業者から、「ウイルスファイルが置かれている」との申告があった。 ・調査したところ、スクリプトファイルや、フィッシングに悪用するための不正なコンテンツファイルが置かれていたことが判明。 ・原因は不明。
解説・対策	フィッシングで奪取した**個人情報を外部に送信するための、スクリプトファイルも同時に設置されていた**ようです。このスクリプトがウイルスとして検知されていました。フィッシングサイトとして悪用されると、被害者であると同時に加害者にもなってしまいます。**サーバの脆弱性対策や、改ざん検知といった対策が有効**です。 （参考） IPA - 情報セキュリティ白書 2007 年版 http://www.ipa.go.jp/security/vuln/20070309_ISwhitepaper.html

［アクセス形跡（未遂）］

（ii）サーバが不正ログイン試行を受けている

事例	・外部に公開しているサーバが、海外の IP アドレスから不正ログイン試行を受け続けている。 ・ログインは成功していないが、今後が心配。どうすればよいか。 ・外部からの接続は、国内からしか許可したくない。
解説・対策	今後も侵入を許さないためには、下記の対策が有効です。 **・公開サーバの OS やその他ソフトウェアのぜい弱性を常に解消しておく。** **・ファイアウォールを設置する。** **・アクセス制限を施す。**（例：特定の IP アドレス範囲やドメインのみ許可する、特定の IP アドレス範囲や国のドメインのみ拒否する、など） **・アクセスログ※をこまめにチェックする。** **・可能であれば、IDS※/IPS※を設置する。** （参考） IPA - 安全なウェブサイトの作り方 改訂第 2 版 http://www.ipa.go.jp/security/vuln/websecurity.html

※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。
※IDS（Intrusion Detection System）… システムに対する侵入／侵害を検出・通知するシステムのこと。
※IPS（Intrusion Prevention System）… システムに対する侵入／侵害を阻止するシステムのこと。

5. 相談受付状況

9 月の相談総件数は **910 件**でした。そのうち**『ワンクリック不正請求』に関する相談**が **270 件**(8 月:330 件)でした。その他は、**『セキュリティ対策ソフトの押し売り』行為**に関する相談が **12 件**(8 月:13 件)、**Winny に関連する相談**が **4 件**(8 月:6 件)などでした。

IPA で受け付けた全ての相談件数の推移

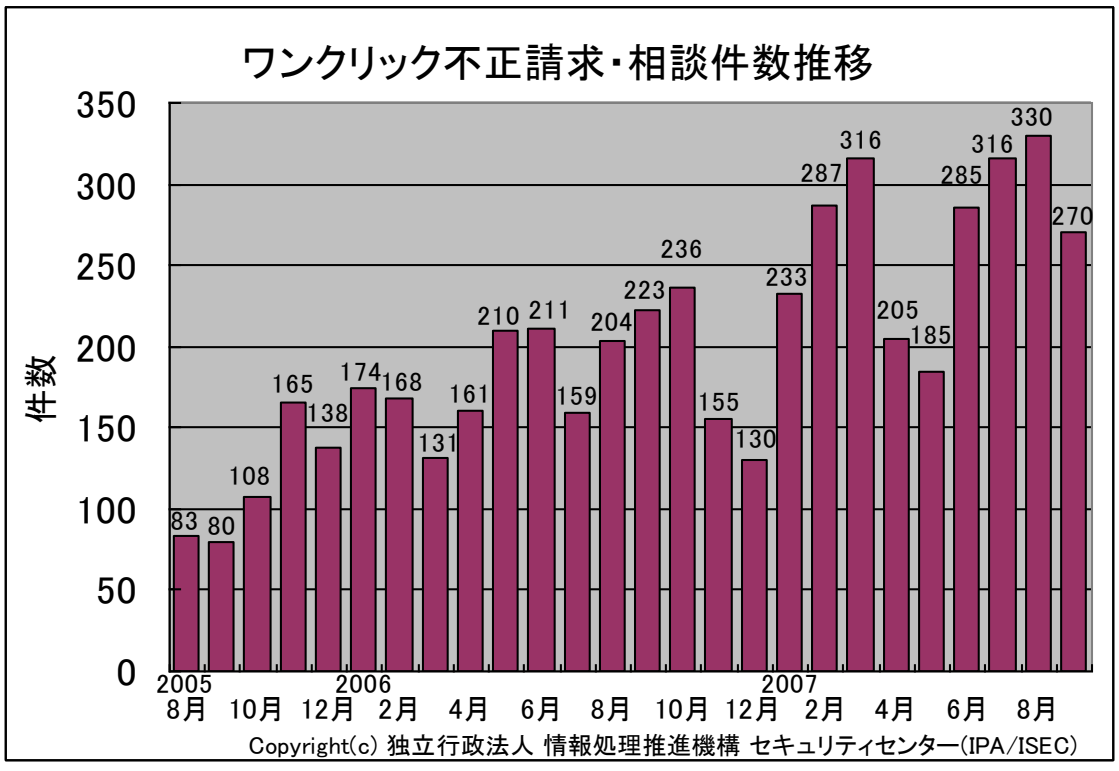
	4月	5月	6月	7月	8月	9月
合計	**827**	**814**	**932**	**1162**	**1013**	**910**
自動応答システム	486	484	537	694	593	544
電話	279	254	339	402	374	310
電子メール	58	69	53	65	43	55
その他	4	7	3	1	3	1

※ IPA では、コンピュータウイルス・不正アクセス、Winny 関連、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)、
winny119@ipa.go.jp (Winny 緊急相談窓口)、isec-info@ipa.go.jp (その他)
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。

(参考) ワンクリック不正請求相談件数の推移



主な相談事例は以下の通りです。

（i）メールの本文にあったリンクをクリックしたら、ウイルス警告が！

相談	組織内のほとんどのメールアドレス宛に、ウイルスが添付されたメールが送りつけられた。差出人は、組織内の人間を装っているが、実在しないもの。メール本文や添付ファイル名は、業務に関連があるように見えるものであった。添付ファイルを開いてしまったパソコンからは、外部のある特定の IP アドレスに向けて何やら怪しいアクセスをしている。
回答	特定の組織を狙った、**スピア型**攻撃※と思われます。通常のウイルス対策はもちろんのこと、この場合は**“こんなメールが届いたら注意！”といった組織内への注意喚起が最も重要**です。また、**ウイルスは実行形式の他に、ワープロなど文書ファイル内に仕込まれている場合もあります**ので、特に注意が必要です。 （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

※スピア型攻撃 … 特定の組織や個人を狙って行われる攻撃のこと。

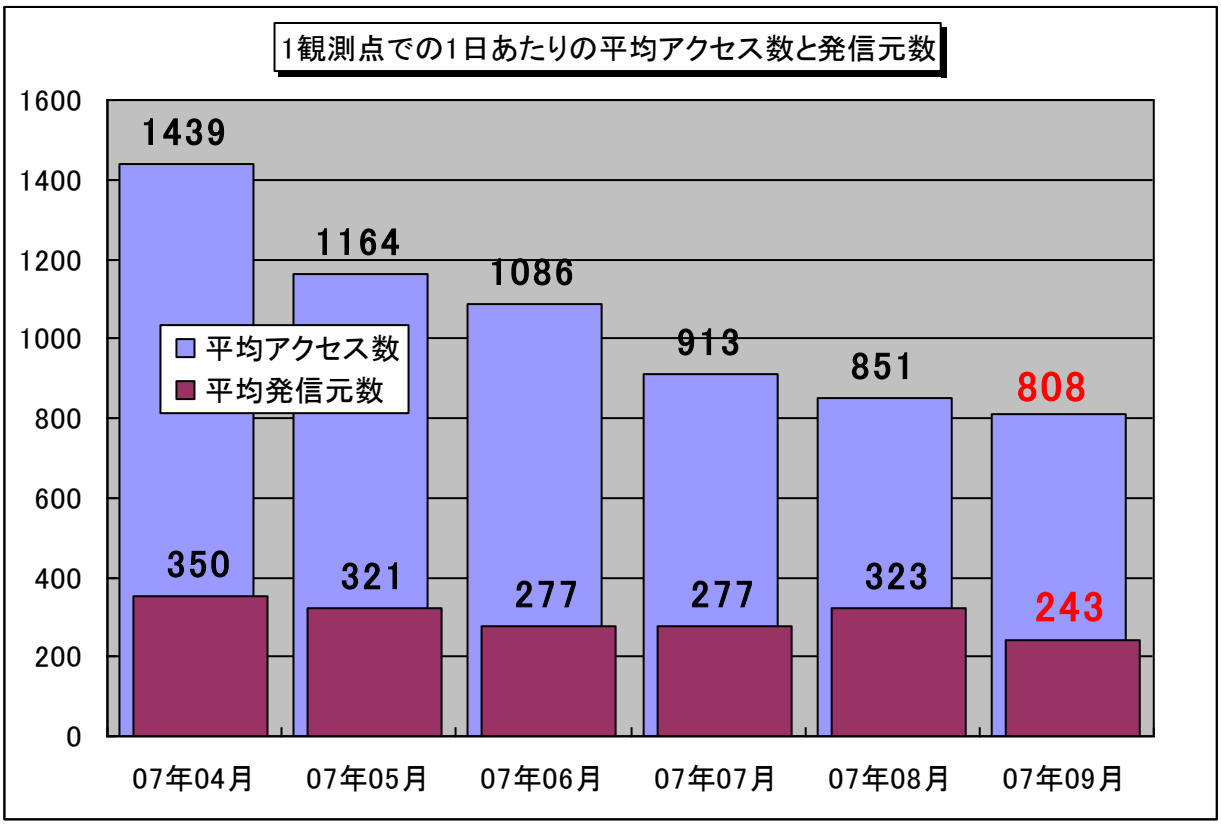
（ii）Winny で情報が漏えいしてしまった・・・

相談	外部の人間から、「御社の内部情報が Winny ネットワーク上に流れていますよ」と通報を受けた。内部調査したところ、社内の Winny ユーザが私用パソコンで仕事のデータを扱っており、パソコンに暴露型ウイルスが感染して流出したらしい。今後、どうすればよいのか。
回答	**情報漏えい事件が起こってしまった場合は、「情報漏えいによる直接的・間接的被害を最小限に抑える」ことが最優先**です。誤った対応は、かえって被害を拡大してしまいます。下記ポイント集を参考にして、適切な対処を実施してください。 （ご参考） IPA － 情報漏えい発生時の対応ポイント集 http://www.ipa.go.jp/security/awareness/johorouei/

6. 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、2007 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 **242, 378 件**ありました。1 観測点で 1 日あたり **243** の発信元から **808 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、243 人の見知らぬ人(発信元)から、発信元一人当たり約 3 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 6-1　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】

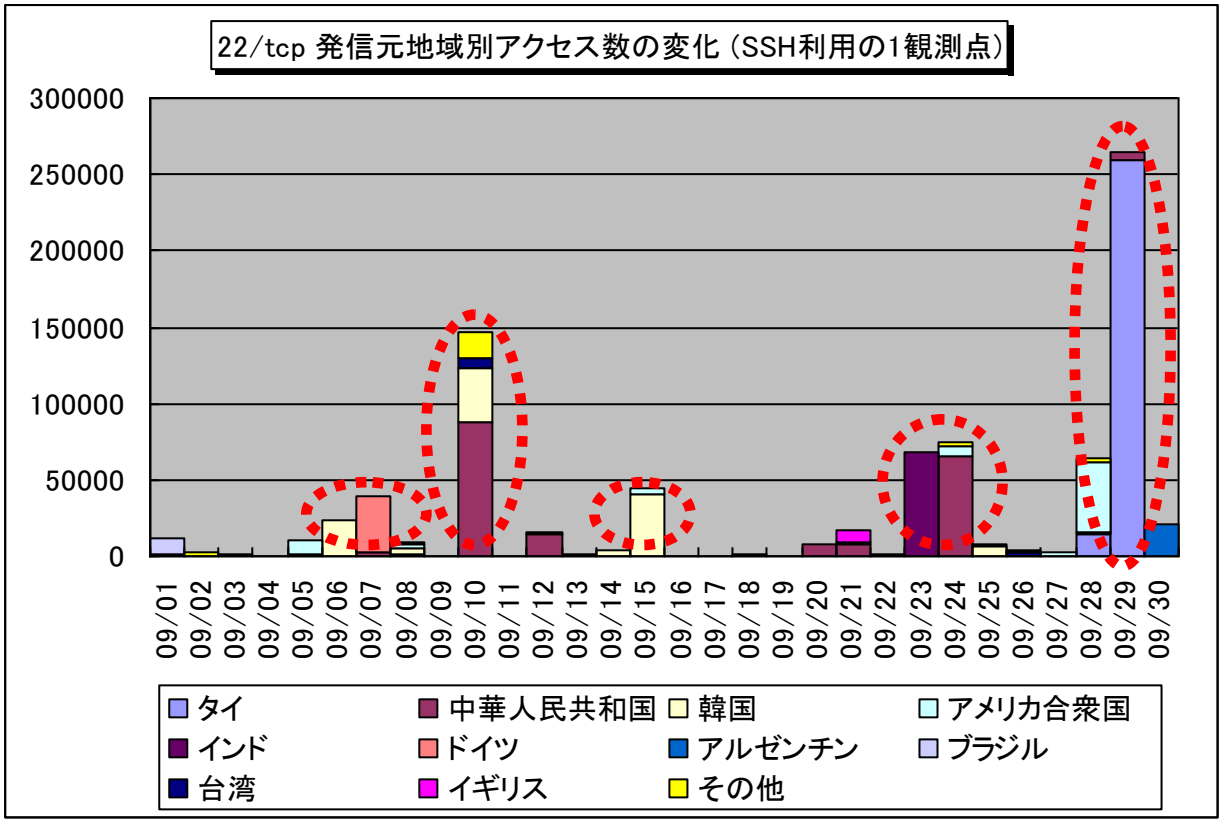
2007 年 4 月～2007 年 9 月までの各月の 1 観測点での 1 日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図 6-1 に示します。この図を見ると、期待しない（一方的な）アクセスは、3 ヶ月連続で 1000 を切り、緩やかな減少傾向にあります。

2007 年 9 月のアクセス状況は、7 月、8 月と同じ様な感じで減少傾向にありますが、2007 年 1 月～9 月と、ほとんど変わらない状況です。そうした中において、リモートでアクセスするコンピュータを狙ったアクセスが多く見受けられました。

(1) SSH を利用しているサーバを狙ったアクセス

SSH(Secure Shell:遠隔地にあるコンピュータに、リモートでアクセスする為に、通信路を暗号化することで安全性を高めたコマンド実行ツール)を利用しているコンピュータへのアクセスは、安易なパスワードで設定されているコンピュータを狙ったアクセスと思われます。

図 6-2 は、TALOT2 のメンテナンス用に SSH を利用している観測点の、22/tcp ポートへのアクセス数を示したものです。



【図 6-2 2007 年 9 月の 22/tcp ポートへの発信元地域別アクセス数の変化(SSH 利用の 1 観測点)】

この様に、1 日に数万～数十万回のアクセス※1 がくる場合があります。こうしたアクセスに応答するコンピュータに対しては、パスワードを破るための攻撃(ブルートフォース攻撃※2)を行なってきます。

※ 1 これらのアクセスは、特定観測点に対するものなので、統計情報にそぐわないため除外してあります。この他に、P2P ファイル交換ソフトが使用するアクセスも同様です。
全体的なアクセス数は減少していますが、この様な特定観測点のアクセスを含めて見てみると、決して期待しないアクセスが減少している訳ではありません。

※ 2 ブルートフォース攻撃とは、総当り攻撃とも呼ばれ、パスワードを破るためにありとあらゆる解読方法を使用して攻撃する手法です。

IPA に届けられた不正アクセスの情報では、ID やパスワードの不備が原因であった事例が年々増加しています。
システム管理者は、利用するアプリケーションの ID やパスワードの再確認や、接続認証の強化を実施して下さい。また、サーバに脆弱性がないかの確認も行って下さい。

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/2007/documents/TALOT2-0710.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/japan/

■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／宮本
Tel:03-5978-7527 Fax:03-5978-7518 E-mail:isec-info@ipa.go.jp