プレスリリース
第 08-23-133 号
2008 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［2008 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：西垣 浩司）は、2008 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

「今一度、パスワードを点検しましょう！」
― あなたのパスワード、破られない自信がありますか？ ―

9 月に IPA に寄せられた相談・届出の中に、「登録しているオークションサイトに、身に覚えのない商品が自分の ID で出品されている」といった、アカウント*1 を不正に利用されたという被害が複数ありました。

相談の中には、パスワードに数字だけの組み合わせや、簡単な英単語を設定していたために、容易にパスワードが見破られて、アカウントを不正に利用されたと推測されるケースがありました。

オークションサイト等のサービスでは、アカウントを不正に利用されると金銭的な被害が発生する危険があります。このような被害に遭わないために、パスワードの作成や管理には、十分な注意が必要です。

(1)被害内容と原因

IPA に寄せられた相談の被害事例は、新聞でも何度か報道されています。それによると、オークションサイトのアカウントが盗まれて、不正に利用されたといった被害が多数確認されています。中には、本人が知らないあいだに大量の商品をオークションに出品されてしまい、その手数料をオークションサイトから請求されるといった金銭に関わる被害が起きています（図 1-1 参照）。

今回の被害の多くは、安易なパスワードを設定していたことが原因のひとつとして推測されます。相談事例の中にも、パスワードを「数字だけの組み合わせ」、「簡単な英単語」で設定していたというものがありました。このような安易なパスワードでは、辞書攻撃*2 等により短時間にパスワードを解読されてしまい、アカウントの不正利用に繋がる危険性が高くなります。

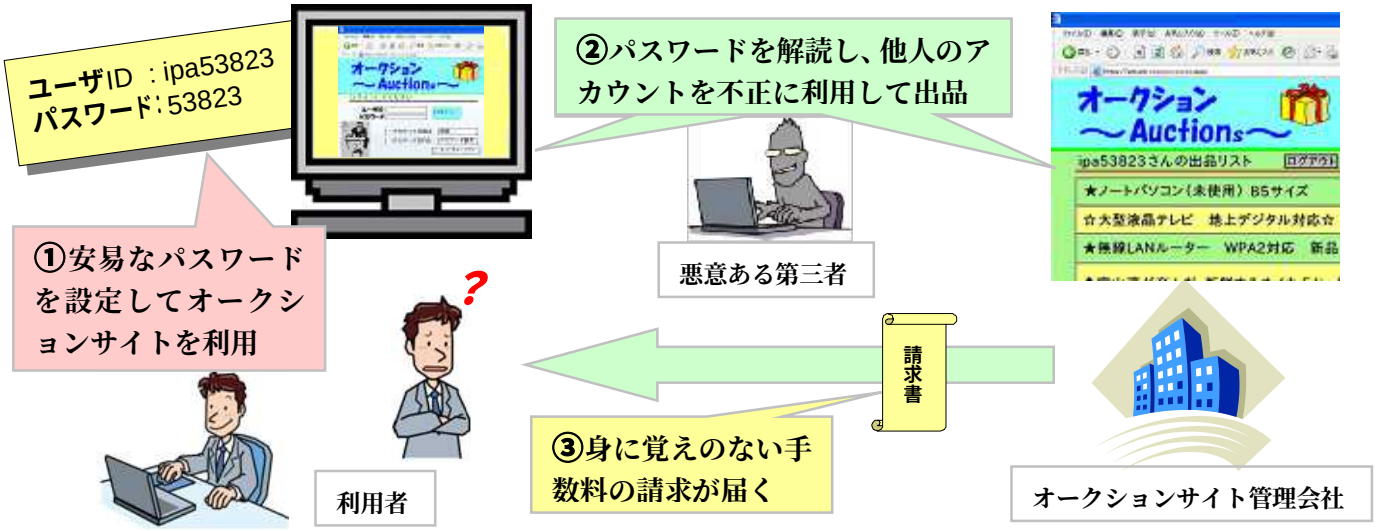

図 1-1：アカウントを不正利用されるイメージ

＊1：アカウント(account)： 情報システム（サービス）を利用する権限のこと。情報システムでは、ID（ユーザ ID）とパスワードを発行することで、その ID が利用できる範囲（権限）を決めて、パスワードにより本人確認を行う。
＊2：辞書攻撃： 辞書にある単語などを片端から試行する攻撃方法のこと。

(2)強いパスワードとは

オークション等のサービスを提供するウェブサイトでは、パスワードを作成する際、「英字、数字、記号をランダムに組み合わせて、8 文字以上にしましょう」という注意事項が記載されているケースがよくあります。これは強い（破られにくい）パスワードを作成するポイントとなります。

つまり、現在の最新パソコンの処理能力でもパスワードを解読するための計算が何千年もかかるのであれば、それは解読できないことと同一であると考えられます。したがって、一般的にはパスワードに使用する文字の種類を多くしたり、桁数を大きくしたりすれば、強い（破られにくい）パスワードであるということがいえます。

表 1-1 はパスワード解析ツールを使用して解読時間を試算した結果です。これによると、英字（大文字、小文字区別有）と数字を組み合わせて 8 桁のパスワードを作成した場合、解読には最大で約 50 年（すべての組み合わせを試算した場合）かかります。このように、3 種類(62 文字数)で 8 桁のパスワードを作成すれば、パスワードの強度は十分と言えるでしょう。表 1-1 を参考に、強度の違いを確認して、破られにくいパスワードを作成するようにしてください。

表 1-1：使用できる文字数と入力桁数によるパスワードの最大解読時間

使用する文字の種類	使用できる文字数	最大解読時間			
		入力桁数			
		4 桁	6 桁	8 桁	10 桁
英字（大文字、小文字区別無）	26	約 3 秒	約 37 分	約 17 日	**約 32 年**
英字（大文字、小文字区別有）＋数字	62	約 2 分	約 5 日	**約 50 年**	**約 20 万年**
英字（大文字、小文字区別有）＋数字＋記号	93	約 9 分	約 54 日	**約 1 千年**	**約 1 千万年**

※すべての組み合わせを試すために必要な時間を計算。
記号は 31 文字使用できるものとした。
使用パソコン OS：Windows Vista Business 32bit 版
プロセッサ：Intel Core 2 Duo T7200 2.00GHz 、メモリ：3GB

8 桁以上の長いパスワードであっても、推測しやすいもの（ID と同一、数字だけの組み合わせ、辞書に載っている単語の組み合わせなど）は避けるようにしましょう。

(3) 対策

以下のポイントを参考に、アカウントの管理を適切に実施してください。

⒜ パスワード作成のポイント

オークション等のサービスの提供元によっては、使える文字の種類や桁数に制限がありますが、⑵ の表 1-1 を参考にして使える文字の種類はできるだけ多く使い、原則 8 桁以上を設定するようにしてください。

⒝ パスワード管理に関するポイント

・ <u>パスワードの保管について</u>

長く複雑なパスワードを作成すると、記憶するのは大変です。この場合、紙にメモしても構いませんが、ID とパスワードは別々に保管することをお勧めします。仮にパスワードが知られたとしても、どの ID に対応するパスワードなのかがわからなければ意味がありません。

・ 定期的に変更する

強い（破られにくい）パスワードであると思っていても、長期間利用していると漏えいする危険がありますので、定期的に（例えば毎月）変更することを強くお勧めします。

なお、定期的に変更する際、2 種類のパスワードを交互に使用することは、変更する意味をなくしますので行わないでください。

(c)パスワード利用に関するポイント

・ ログイン履歴を確認する

利用しているサービスにより異なりますが、ログインすると、過去のログイン履歴を確認できる場合があります。自分がログインした覚えのない記録があるなど、不正利用に早く気がつけば、被害の拡大を防ぐことができます。定期的にログイン履歴を確認し、不審な記録があれば、直ちにサイト管理者に連絡し、アカウントの利用停止の手続きなどを依頼してください。

・ ネットカフェなど、不特定多数が利用するパソコンでは、ID、パスワードを入力しない

複雑なパスワードを設定していても、そのパソコンにスパイウェアが仕掛けられていたら簡単に盗まれてしまいます。自分が管理しているパソコン以外では、ID とパスワードを必要とするオークション等のサービスの利用は避けるべきです。

・ フィッシング対策

フィッシングとは、金融機関（銀行やクレジットカード会社）などを装った電子メールを送り、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を詐取する行為のことをいいます。近年は、金融機関に限らず、オークションサイトなど、ID とパスワードを必要とするサービスを装った事例も確認されています。ログインする際は、接続しているサイトが正しいか確認してください。

なお、本人確認などの問い合わせがメールで届いた場合、メールに記載されているリンクを安易にクリックせず、送信元に電話するなどの手段で真偽を確認するようにしましょう。

(ご参考)

IPA-フィッシング(Phishing)対策

http://www.ipa.go.jp/security/personal/protect/phishing.html

フィッシング対策協議会

http://www.antiphishing.jp/

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「3.コンピュータ不正アクセス届出状況」を参照）

・SSH で使用するポートへの攻撃で侵入された

・自組織から発信されたようになりすまされたメールが出回っている

○ 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「4.相談受付状況」を参照）

・オークションサイトへの不正アクセス対策として、サイト側に対処を依頼したい

・インターネットの儲け話サイトを信じてお金を振り込んでしまった

○ 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。

・設定不備のプロキシサーバを探索していると思われるアクセスに注意！

2．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 22 万個**と、8 月の約 19 万個から 15.1%の増加となりました。
また、9 月の届出件数(※2)は、**1,875 件**となり、8 月の 1,811 件から 3.5%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（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 22 万個を集約した結果、1,875 件の届出件数となっています。

検出数の1位は、**W32/Netsky で約 19 万個 、2 位は W32/Autorun で約 1.2 万個、3 位は W32/Virut で約 9 千個でした。**

ウイルス検出数　約22万個 (約19万個)　前月比 + 15.1%
（注：括弧内は前月の数値）

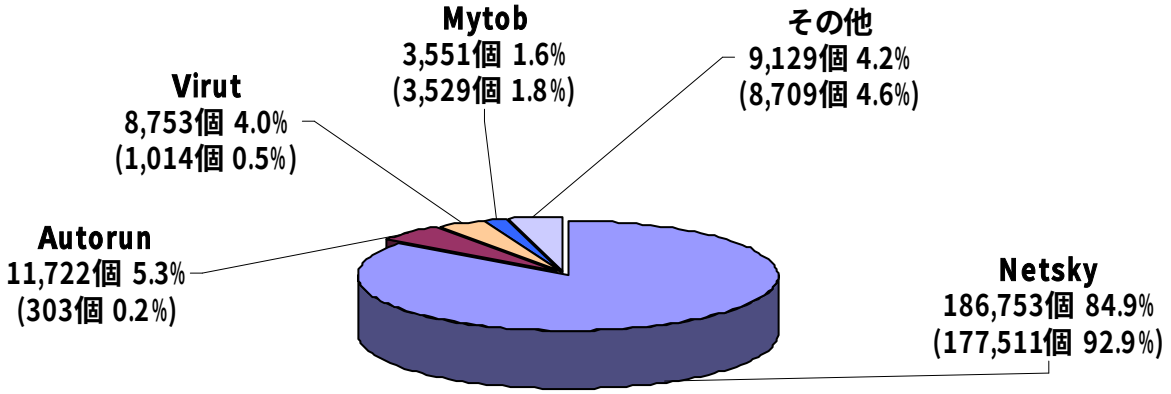

図 2-1

ウイルス届出件数　1,875件 (1,811件)　前月比 + 3.5%
（注：括弧内は前月の数値）

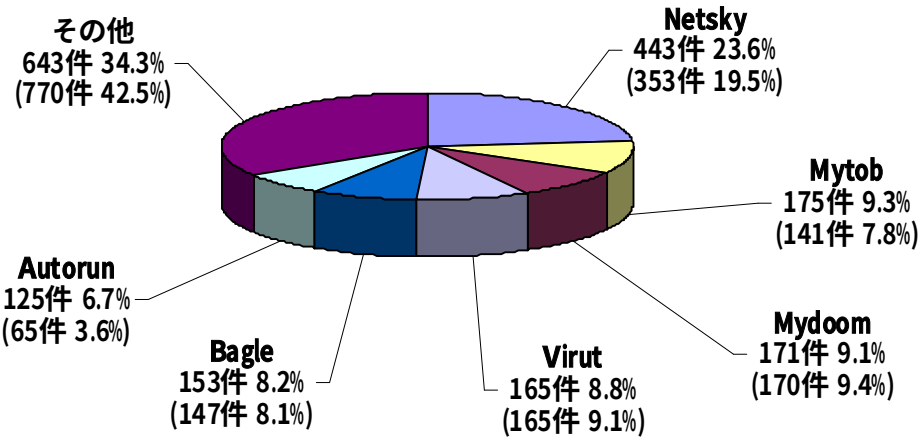

図 2-2

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―

表 3-1　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		14	4	13	19	15	14
	被害あり(b)	10	4	11	18	10	12
	被害なし(c)	4	0	2	1	5	2
相談(d) 計		56	37	36	49	25	38
	被害あり(e)	31	18	15	26	13	20
	被害なし(f)	25	19	21	23	12	18
合計(a+d)		70	41	49	68	40	52
	被害あり(b+e)	41	22	26	44	23	32
	被害なし(c+f)	29	19	23	24	17	20

（1）不正アクセス届出状況

9 月の届出件数は 14 件であり、そのうち何らかの被害のあったものは 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 38 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 20 件でした。

（3）被害状況

被害届出の内訳は、**侵入 6 件、DoS 攻撃が 1 件、アドレス詐称が 1 件、その他（被害あり）4 件**でした。

侵入届出の被害は、他サイト攻撃の踏み台として悪用されたものが 4 件、データベース内のデータを改ざんされたものが 1 件、などでした。侵入の原因は、SSH※で使用するポートへのパスワードクラッキング※攻撃によるものが 3 件、などでした。

その他（被害あり）の被害として、オンラインサービスのサイトに本人になりすまして何者かにログインされ、サービスを勝手に利用されていたものが 2 件（ネットオークション 1 件、オンラインゲーム 1 件）、などがありました。

※SSH（Secure SHell）…ネットワークを介して遠隔のコンピュータと通信するためのプロトコルの一つ。
※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。ブルートフォース攻撃（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。

（4）被害事例

[侵入]

（i）SSH で使用するポートへの攻撃で侵入された

事例	・社内のサーバをチェックしたところ、SSH で使用するポート経由でパスワードクラッキング攻撃を受け、一般アカウントが不正にログインされていたことが判明。 ・root 権限は奪われていなかったが、4 種の不正プログラムを埋め込まれ、外部サイト攻撃の踏み台として使われてしまっていた。 ・埋め込まれていた不正プログラムは、**1.外部サイトへの DoS 攻撃ツール、2.バックドアツール（サーバ/クライアント）、3．SSH 脆弱性の攻撃ツール、4．侵入後、サーバ内でカーネルの脆弱性を突いて root 権限を奪うツール**、であった。 ・**社内サーバは本来、厳格な規定に則り管理・運用されているが、本サーバの管理者はそれらのルールを知らず、勝手にサーバを設置**していた。さらに、パスワード設定が、推測容易なものになっていた。
解説・対策	事象としてはありがちですが、サーバに埋め込まれていた不正プログラムが何だったのか明らかにされた、貴重な例です。**明らかに、悪意ある者が当該サーバを操作し、他のサーバを攻撃しようとしていた**ことが伺えます。このように、**セキュリティの弱いサーバは、他のサイトを攻撃するための踏み台として乗っ取られるかも知れないという脅威に常に晒されています。管理や設定の抜けが無いか、今一度、確認しましょう**。 （参考） IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html

[アドレス詐称]

（ii）自組織から発信されたようになりすまされたメールが出回っている

事例	・自組織の広報用メールアドレスが差出人となっている不審なメールが、自組織の関係者宛に送られていることが判明。当該メールは、自組織からは発信されていないことを確認。 ・内容は、**自組織から過去に実際にアナウンスした注意喚起文を引用**し、「なりすましメールに注意すること」などが書かれていた。**“対策を強化するため、添付ファイルを開いてください”との文面も。おそらく、何らかのウイルスであると思われる**。 ・当該メールのヘッダを調査したところ、真の発信元は海外の模様。
解説・対策	このように、特定の範囲の利用者宛に、彼らに関係があると思わせる文面で偽のメールを送り付ける、いわゆる“**標的型攻撃**”が最近増加しています。この**攻撃の特徴や、対処方法については、以下のページを参照してください**。 （参考） IPA - 情報詐取を目的として特定の組織に送られる不審なメールの相談窓口「不審メール 110 番」を設置 http://www.ipa.go.jp/security/announce/20080929.html

4．相談受付状況

9月の相談総件数は**2154件**であり、過去最多だった先月をさらに大幅に上回る件数となりました。そのうち**『ワンクリック不正請求』に関する相談**が**651 件**(8 月:545 件)と**4 カ月連続で過去最悪記録を更新し、危機的状況が続いています**。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**過去最悪の50 件**(8 月:18 件)、**Winny に関連する相談**が**4 件**(8 月:5 件)などでした。

表 4-1　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		**938**	**1080**	**1211**	**1387**	**1616**	**2154**
	自動応答システム	514	649	693	817	994	1302
	電話	335	379	456	500	548	755
	電子メール	87	48	60	70	69	93
	その他	2	4	2	0	5	4

※ 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。

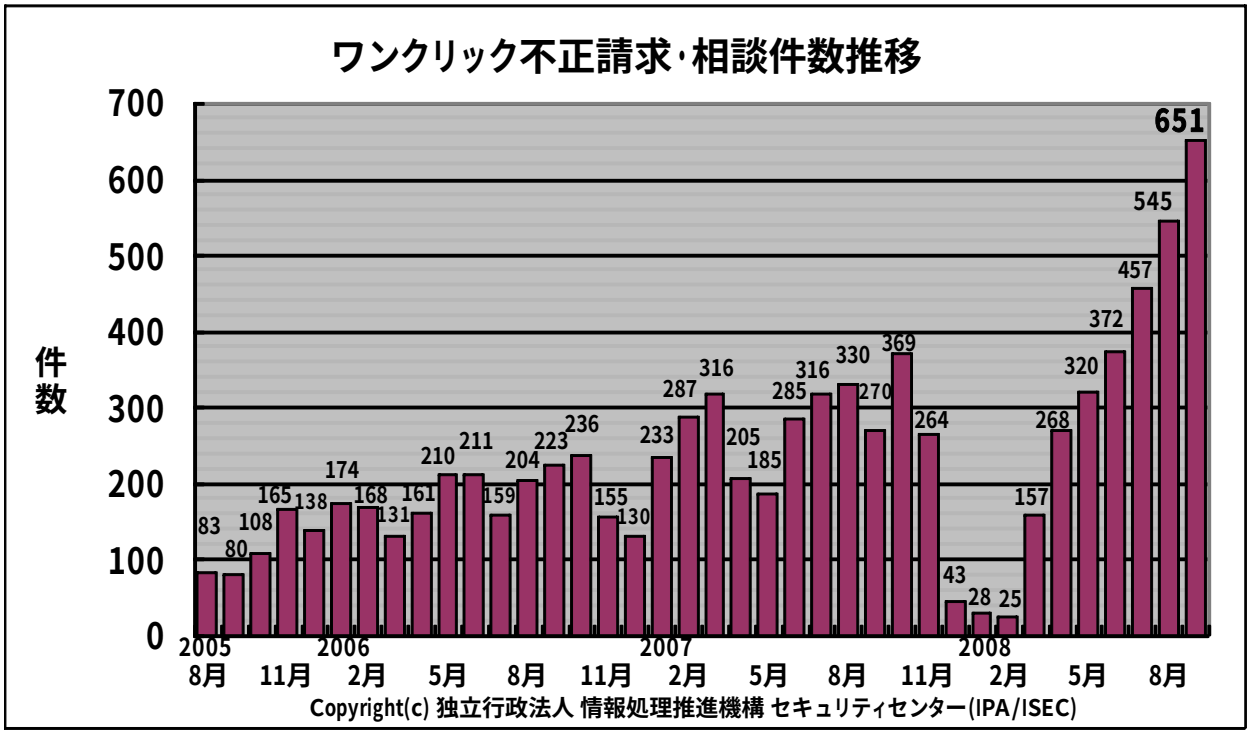

図 4-1　ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

(i) オークションサイトへの不正アクセス対策として、サイト側に対処を依頼したい

相談	自分が利用しているネットオークションサイトでは、自分のアカウント(ID)のログイン履歴を確認できる。それによれば、数ヶ月間、国内の特定の IP アドレスから継続して自分の ID に対してログインを試みていることが分かった(全てログイン失敗)。このままでは、パスワードを破られるのは時間の問題であり、オークションサイト側にアクセス制限などを依頼したが、全て断られた。被害を未然に防ぐためにサイト側へ何か要請をしようと思うが、どんな内容が効果的か教えてほしい。また、差し当たって個人でできる対策は何か。
回答	**サイト側への要請としては、少なくてもパスワード総当たり攻撃だけは排除してもらうことを主張してはどうでしょうか**。例えば、連続して 3 回パスワードを間違った場合はアカウントを一時的にロックしてもらうなど。 個人でできる対策としては、**強固なパスワードを設定する**とともに、その**保管に注意**し、かつ**定期的にパスワードを変更**すること、となります。 ※本紙の「１．今月の呼びかけ」を参考にしてください。 （ご参考） 警察庁 - インターネット安全･安心相談 http://www.cybersafety.go.jp/

(ii) インターネットの儲け話サイトを信じてお金を振り込んでしまった

相談	インターネットで、お金儲け話が書かれているサイトを見付けた。儲けるための情報を入手するためにお金を振り込んだが、結局、お金は儲からなかった。どうすれば良いか。
回答	**根拠の無い架空の儲け話の情報を売る、詐欺の可能性が高い**です。お金を取り戻せる可能性は低いでしょう。 **世の中、そんな都合の良い話が転がっている訳がありません。騙されないように、用心が必要です。ネット上では、詐欺師があの手この手であなたを狙っています。ネットの世界も“現実”であることを忘れずに、慎重に行動しましょう**。 （ご参考） 呼びかけ:「ネット上の誘惑に負けるな！！」 http://www.ipa.go.jp/security/txt/2006/12outline.html 警察庁 - インターネット安全･安心相談 http://www.cybersafety.go.jp/

5．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、2008 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 **119,926 件**、総発信元数(※)は **47,248 箇所**ありました。1 観測点で見ると、1 日あたり **157** の発信元から **400 件**のアクセスがあったことになります。

※**総発信元数**：TALOT2 にアクセスしてきた発信元の総数。なお、同一発信元から同一観測日・観測点・ポートにアクセスがあった場合は 1 つの発信元としてカウント。

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、157 人の見知らぬ人(発信元)から、それぞれ約 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。

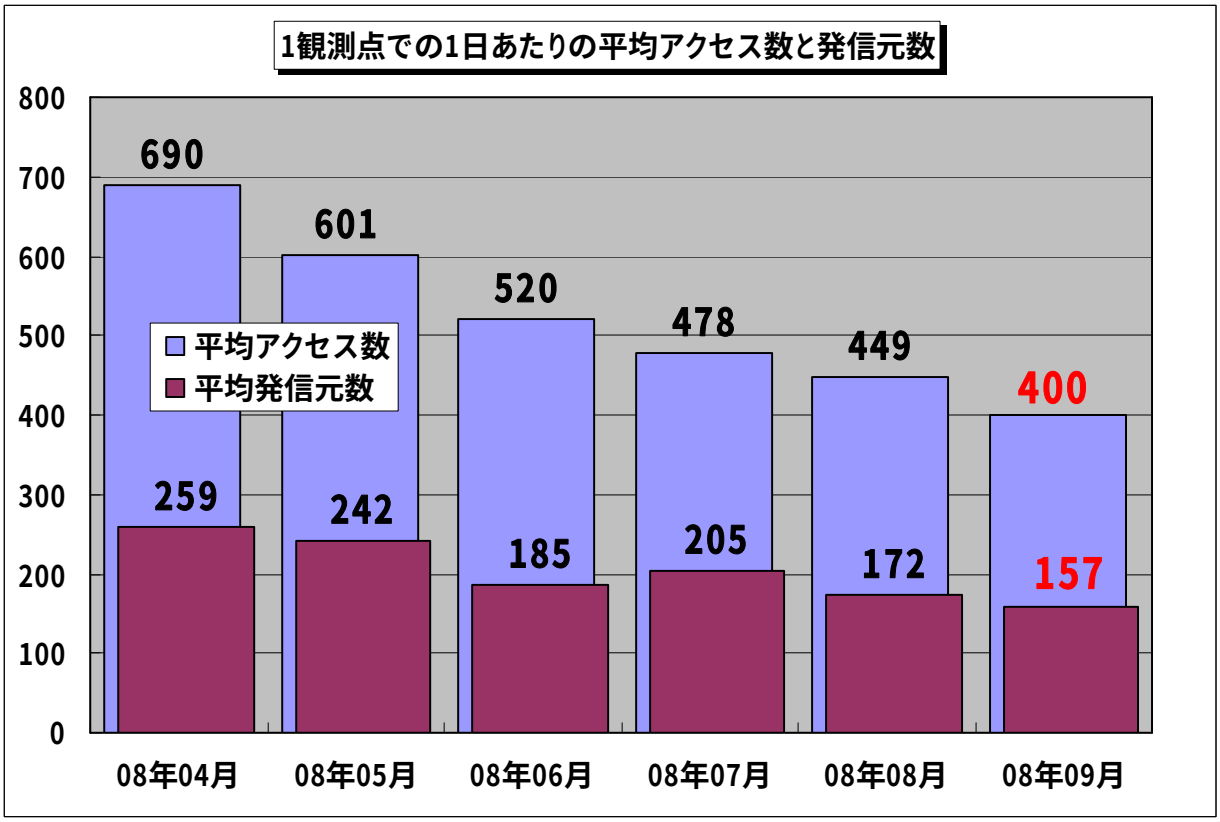

図 5-1：1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数

2008 年 4 月～2008 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 5-1 に示します。この図を見ると、9 月の期待しない（一方的な）アクセスは 8 月と比べて若干減少しており、過去 6 ヶ月間を通してみても、減少傾向を示していると言えます。

（1）設定不備のプロキシサーバ(※1)を探索していると思われるアクセス

9 月 13 日から 17 日にかけて、TALOT2 の 7 観測点において、8080/tcp および 6588/tcp へのアクセス急増が観測されました（図 5-2 参照）。

発信元は全て中華人民共和国の特定の IP アドレスでした。

8080/tcp および 6588/tcp はプロキシサービスで利用されることの多いポートです。

これらのアクセスは、外部から迷惑メールの送信などに利用できるプロキシサーバ（オープンプロキシという）がないかを探索している可能性があります。また、短期間におなじ観測点に数百回も

アクセスしているので、探索のためのツールをテストしている可能性もあります。
　これらのアクセスにより、攻撃者にオープンプロキシであると判断されたプロキシサーバは、迷惑メールの送信などの踏み台として利用されることがあります。
　プロキシサーバを運用しているシステム管理者は、お使いのプロキシサーバが外部から利用されないように、サーバ設定を再度確認して下さい。

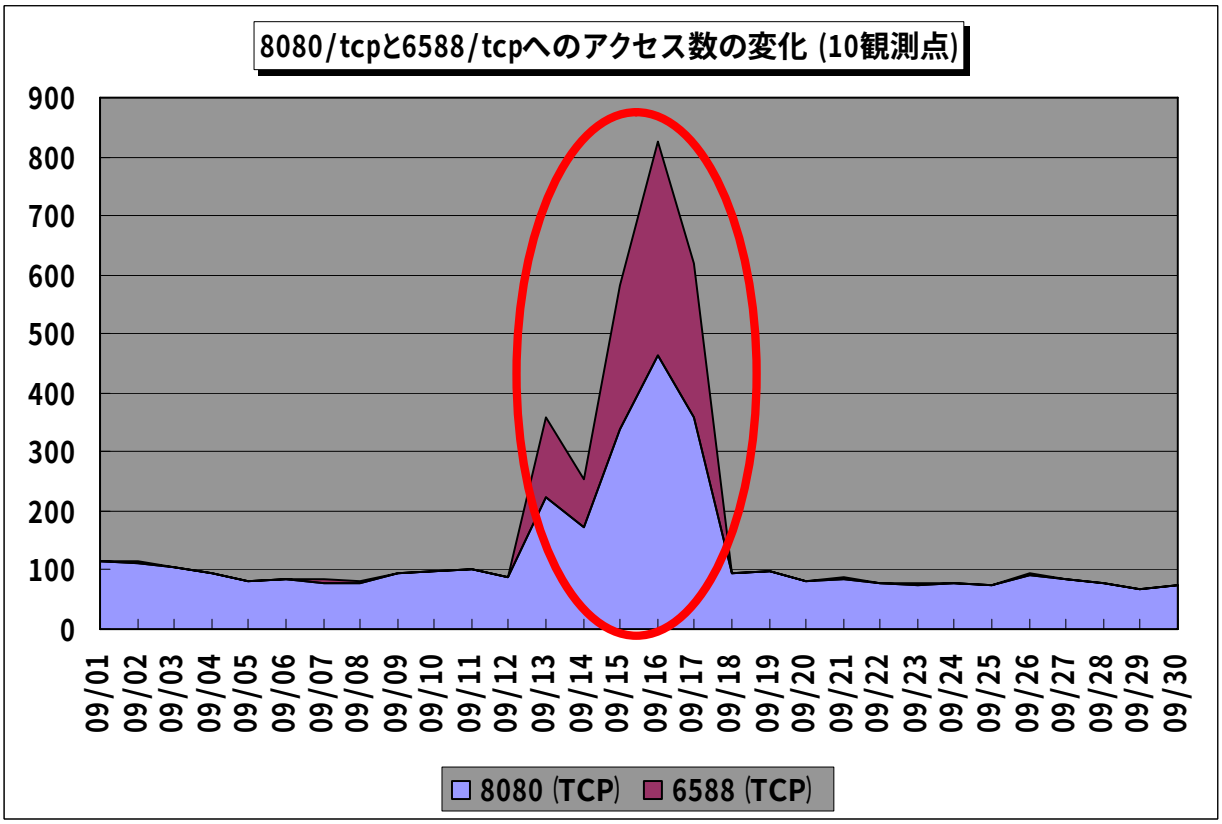

図 5-2：8080/tcp と 6588/tcp へのアクセス数の変化

※1：プロキシサーバ：通信を代理で行うサーバのことを言います。主に企業などの組織で、内部ネットワークとインターネットの接続地点で、通信のセキュリティ確保と高速アクセスを実現させるために利用されることが多い。

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/2008/documents/TALOT2-0810.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／大浦
Tel:03-5978-7527 Fax:03-5978-7518 E-mail:isec-info@ipa.go.jp