プレスリリース
第 09-22-154 号
2009 年 7 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 [2009 年 6 月分] について

IPA（独立行政法人情報処理推進機構、理事長：西垣 浩司）は、2009 年 6 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

「あなたのウェブサイト、改ざんされていませんか？」
― ウイルスばらまきサイトに仕立て上げられているかもしれません ―

最近、企業や個人が運営しているウェブサイトを改ざんされる事例が多く発生しています。改ざんされたウェブサイトには、閲覧した利用者のパソコンをウイルスに感染させる仕掛けが組み込まれている場合があります。その結果、改ざんされたウェブサイトの利用者から、「ウイルスを検知した」、「ウイルスに感染した」といった届出や相談が IPA に寄せられています。

改ざんされたウェブサイトの運営者は、被害者に留まらず、ウェブサイト利用者のパソコンにウイルスを感染させてしまう加害者となります。このような被害の拡大を防ぐため、ウェブサイトの管理者は、管理しているウェブサイトが改ざんされていないか確認し、ウイルスの“ばらまきサイト”に仕立て上げられないようにしてください。

（1）ウェブサイト改ざんの概要と主な原因

ウェブサイト改ざんの原因として、ftp※のアカウント情報を盗まれた事例がありました。盗んだ ftp アカウント（ID/パスワード）を使い、正規のユーザになりすまして、改ざんしたページをウェブサーバに公開（アップロード）するというものでした。

ftp のアカウント情報を盗む手口としては、スパイウェアをターゲットのパソコンに送り込むなどの方法が一般的です。

※File Transfer Protocol の略。ネットワークでファイルを転送するためのプロトコル。

改ざんされたウェブページには不正なスクリプトが埋め込まれ、そのページを閲覧した一般利用者を、ウイルスが仕掛けられた悪意あるウェブサイトにアクセスさせます。一般利用者が悪意あるウェブサイトを閲覧した場合、利用者のパソコンに脆弱性があると、それを悪用されウイルスに感染させられてしまいます（図 1-1 参照）。

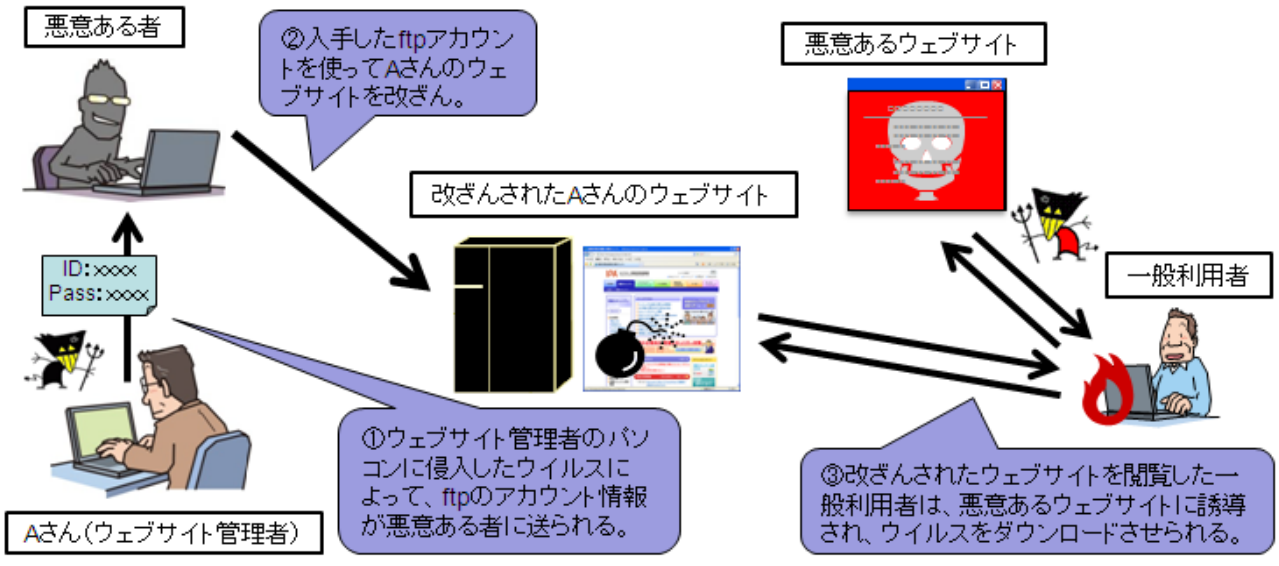


図 1-1：ウェブサイトの改ざんからウイルスに感染するまでの流れ

（2）改ざんの有無のチェック方法

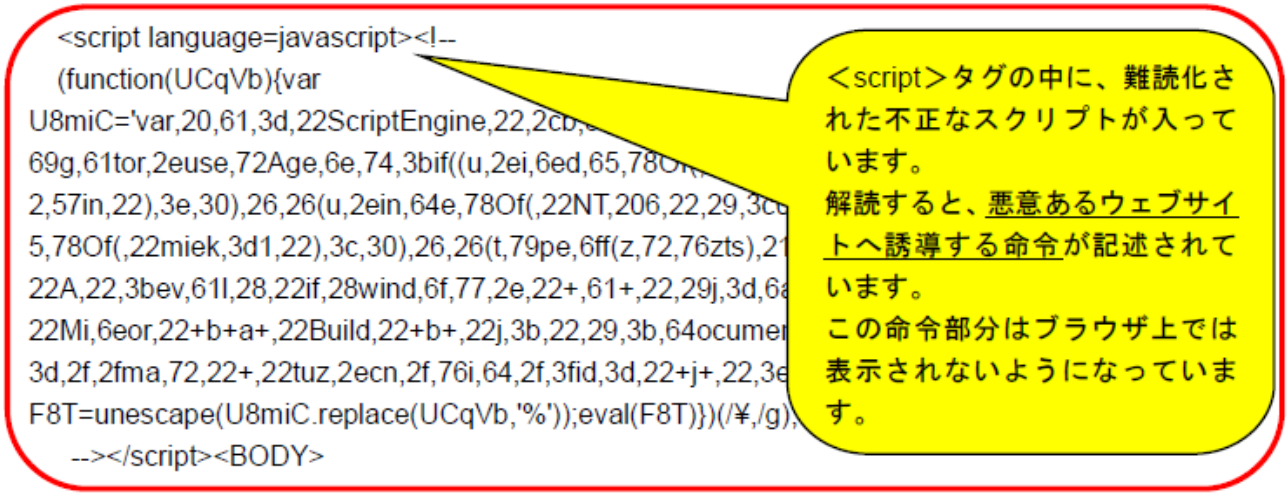
ウェブサイト管理者は、自身が管理するウェブサイトの利用者に、ウイルスを感染させている可能性があることを認識し、以下の点を参考に改ざんの有無をチェックしてください。

（a）ウェブサイト上の全ページのソースを確認

ウェブサイト上に公開されている全ページについて、不正なスクリプトが含まれていないかを確認してください。同様に、ウェブページを編集するパソコンに保存されているページもチェックしてください。ウェブページのブラウザ上での見た目は、改ざんされる前と区別がつかないため、ホームページの編集ソフト等でページのソースを表示して確認します。

今回、以下のスクリプトが改ざんにより追記された事例が確認されていますので、同様の意味不明な文字列が含まれていないかをチェックしてください。

【不正なスクリプトのサンプル】



（b）ftp へのアクセスログを確認

今回のケースでは、ftp のアカウントを不正に利用され、正常なページに不正なスクリプトを埋め込む事例が確認されています。自分がアクセスしていない日時に、ftp のアクセスが行われていないかを確認してください。

特に、企業の場合は、ftp のアクセスログを定期的にチェックし、予防策として以下の項目の実施を推奨します。

・ftp のアクセス制限（アクセスできる IP アドレスを制限する、VPN で接続するなど）。
・改ざん検知システムやサービスを導入する。

上述のように、自身でウェブサイトをチェックし、改ざん箇所を発見することが望まれますが、ウェブサイト利用者から指摘されることで、改ざんが発覚するケースがあります。このような場合を想定し、メールアドレスのみでもよいので、ウェブサイト上への連絡先の掲載を勧めます。

改ざんされた状態が長くなればなるほど、利用者に被害が拡大する恐れがあります。もし改ざんされた場合でも、早期の対応が可能となるように準備してください。

（3）改ざんされた場合の対処方法

ウェブサイトが改ざんされた場合、被害の拡大を防ぐために早急な対応が求められます。まずは、ウェブサイトを一旦公開停止した上で、原因究明および修正作業を実施してください。

ftp のログに不審なアクセスログがあった場合、ウェブページの公開に利用している ftp アカウントを乗っ取られて、悪意あるページをアップロードされている可能性があります。ただちに、ftp アカウントのパスワードを変更し、その後、正規のページに不正なスクリプトが含まれていないことを確認した上で、改ざんされたページと置き換えて、再公開してください。

パスワードの変更後も同様の手口で再度改ざんされた場合は、パスワードの変更を行ったパソコンがスパイウェアに感染して、情報が漏えいしている可能性が高いと考えられます。パソコンを不正なプログラムがないクリーンな状態に（初期化）してから再度パスワードを変更し、再公開を実施してください。

原因を排除し、改ざんページの修正、再公開を完了させた後、ウェブサイトの利用者に向けた、改ざんの事実とウイルスに感染する危険性があった旨の注意喚起、および謝罪文を掲載することを勧めます。また、利用者からの問い合わせ対応を行う窓口を用意することが望ましい対応といえます。

なお、ウェブサイト改ざん、ウイルス感染などの被害に遭った際は、IPA への届出を可能な限り行ってください。IPA では、ウイルスや不正アクセスに関する届出を受け付けており、届け出られた情報を統計的に分析し、個人や組織を特定できる情報を除いた上で、毎月公開しています。また、対策情報を発信する際にも活用しています。

（ご参考）
「情報セキュリティに関する届出について」（IPA）
http://www.ipa.go.jp/security/todoke/

（4）利用者側の対策

利用者が、改ざんされたウェブページを閲覧しウイルスに感染する場合、画面上に何も表示されず、見た目でウイルス感染に気づけないことが大きな脅威となります。さらに、感染しても特に見た目にわかる症状が表れないケースが多くあります。
このようなウイルス感染を防ぐため、以下の対策を実施してください。

（a）脆弱性を解消する
Windows や Mac OS などの OS、Microsoft Office や Adobe Reader などのアプリケーションソフトには、脆弱性が発見されています。最新版への更新や、修正プログラムを適用することで、脆弱性を解消してください。
（ご参考）
「JVN iPedia 脆弱性対策情報データベース」（JVN）
http://jvndb.jvn.jp/

（b）ウイルス対策
ウイルス対策ソフトのパターンファイルを常に最新の状態に更新して、ウイルス検知機能を常時有効にして使用してください。

（5）ウイルスに感染した際の症状

改ざんされたウェブサイトを閲覧した結果、悪意あるサイトに誘導され、ウイルスに感染した場合、感染したパソコンには以下の症状が起こる可能性があります。

- Microsoft Update のサイトへのアクセスが妨害され、脆弱性の解消ができない。
- セキュリティ対策ソフトベンダのサイトへのアクセスが妨害され、ウイルス情報が確認できない、パターンファイル（ウイルス定義ファイル）の更新もできない。
- コマンドプロンプト（cmd.exe）やレジストリエディタ（regedit.exe）が起動できない。

このような症状が確認された場合は、ウイルスに感染している可能性が高いです。さらに、複数のウイルスに感染しているケースもあります。復旧方法は、必要なデータファイルをバックアップした上で、ウイルスを完全に取り除くため、パソコンを初期化することです。

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（届出状況および被害事例の詳細は、5 頁の「3.コンピュータ不正アクセス届出状況」を参照）
- TCP SYN Flood 攻撃を受け、サービス提供が不可能になった
- オンラインゲームサイトで騙されてパスワードを盗まれた

○ 相談の主な事例 （相談受付状況および相談事例の詳細は、7 頁の「4.相談受付状況」を参照）
- ウイルス対策ソフトを使っていれば、OS のアップデートをしなくてもウイルス感染しない？
- Windows 98 や Me のパソコンでも、ネットにつながなければ安全？

○ インターネット定点観測（9 頁参照。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。

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 8.7 万個**と、5 月の約 11.5 万個から 24.4%の減少となりました。
また、6 月の届出件数(※2)は、**1,460 件**となり、5 月の 1,387 件から 5.3%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。
・6 月は、寄せられたウイルス検出数約 8.7 万個を集約した結果、1,460 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 7 万個**、2 位は **W32/Downad** で**約 6 千個**、3 位は **VBS/Solow** で**約 3 千個**でした。

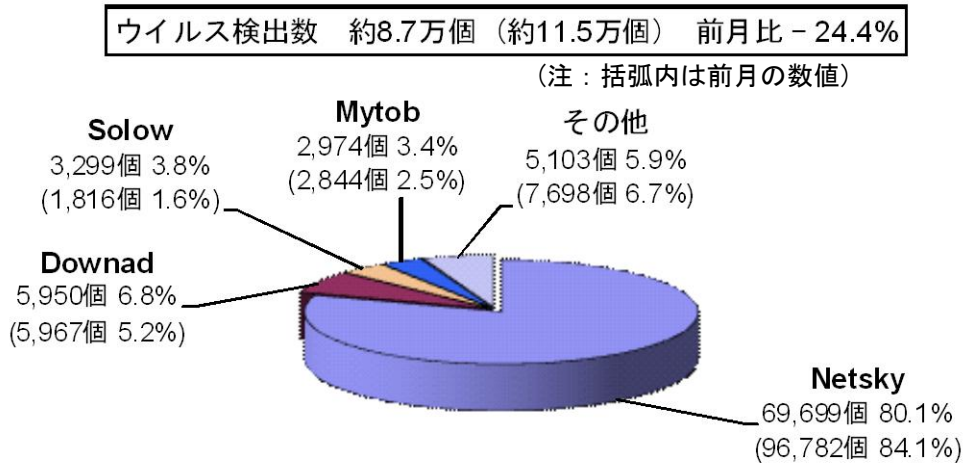


図 2-1：ウイルス検出数

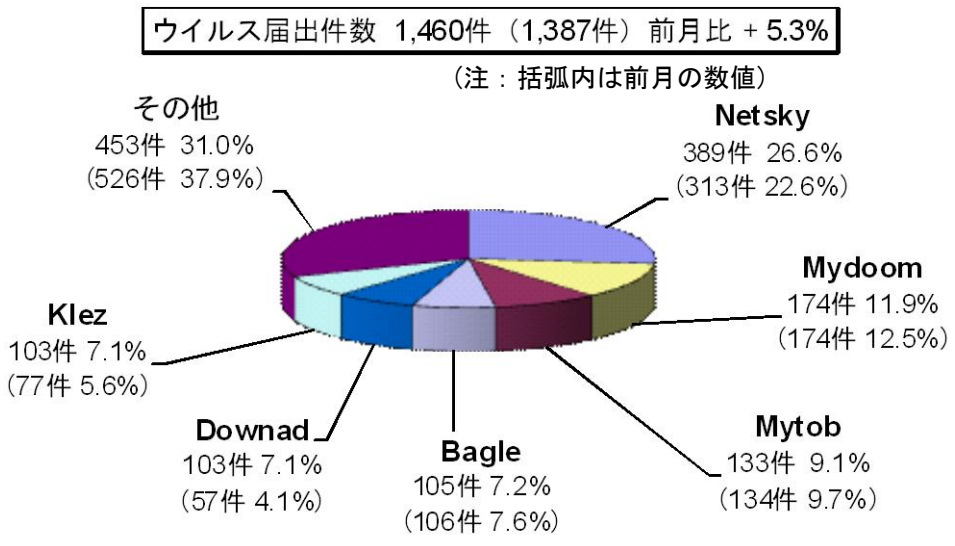


図 2-2：ウイルス届出件数

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

		1月	2月	3月	4月	5月	6月
届出(a) 計		10	9	20	9	8	7
	被害あり(b)	7	6	13	6	6	6
	被害なし(c)	3	3	7	3	2	1
相談(d) 計		29	35	40	39	45	35
	被害あり(e)	13	14	11	11	16	9
	被害なし(f)	16	21	29	28	29	26
合計(a+d)		39	44	60	48	53	42
	被害あり(b+e)	20	20	24	17	22	15
	被害なし(c+f)	19	24	36	31	31	27

（1）不正アクセス届出状況

6 月の届出件数は 7 件であり、そのうち何らかの被害のあったものは 6 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 35 件（うち 1 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 9 件でした。

（3）被害状況

被害届出の内訳は、**侵入 1 件、DoS 攻撃 1 件、なりすまし 3 件、不正プログラム埋め込み 1 件、**でした。

「侵入」の被害は、他サイト攻撃の踏み台として悪用されたものでした。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※攻撃でした。

※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

[DoS]

（i）TCP SYN Flood 攻撃※を受け、サービス提供が不可能になった

事例	・レンタルサーバや ASP の事業を営んでいる企業で、突然、ファイアウォールの負荷が激増し、顧客に提供していたサービス全体が停止した。 ・調査したところ、TCP SYN Flood 攻撃※を受けており、30 分間で 1 億パケットのアクセスが来ていたことが判明。 ・攻撃対象となっていたサーバの IP アドレスを一時的に変更して対処したが、ほどなくして変更後の IP アドレス宛に攻撃パケットが到達するようになった。 ・攻撃対象となったアドレスを使用していたレンタルサーバの顧客のドメインは 100 以上あった。攻撃対象ドメインを絞り込んだところ、オンラインゲーム関連の RMT（リアルマネートレーディング）サイトが狙われていたらしいことが分かった。 ・当該ドメインの DNS の A レコードを一時的に操作し、攻撃パケットが組織内に到達しないようにした。攻撃は、2 日間に渡って行われていたようだ。
解説・対策	同時期に、他の多くの RMT サイトも攻撃を受けていた模様です。**サーバのレンタルを行っている事業者の場合、ある顧客のサーバが攻撃を受けると、他の顧客のサーバアクセスにも影響が出てしまう可能性があります**。今回被害を受けた企業では、攻撃を受けた際、他の顧客への影響を最小限にするため、ネットワーク構成やシステム構成を見直すことにしたようです。また、レンタルサーバ事業者として、顧客が公開しているサービス内容を把握しておくのも、原因の切り分けの参考となる場合もあるでしょう。 （参考） JPCERT/CC　技術メモ - サービス運用妨害攻撃に対する防衛 http://www.jpcert.or.jp/ed/2001/ed010005.txt

※TCP SYN Flood 攻撃 ： サーバの機能を低下させたり停止させたりする DoS 攻撃の手法の一つで、TCP の接続手順を悪用したもの。

[なりすまし]

（ii）オンラインゲームサイトで騙されてパスワードを盗まれた

事例	・オンラインゲームサイトでゲーム中、サイト運営者と名乗る人から「不正アクセスあり」とのチャット要求があった。 ・運営者がパトロールでもしているのかと思い、チャットに応じた。確認と称し、ID とパスワードを聞かれたので、相手に教えた。 ・その後、当該 ID のパスワードが変更され、乗っ取られてしまった。
解説・対策	運営者を名乗り、**ソーシャルエンジニアリング**の手法で ID やパスワード情報を聞き出す手口です。**通常、サイト運営者であっても、ゲーム中で ID やパスワードを聞くことは無いはずです**。相手の言うことを鵜呑みにせず、何事も慎重に行動すべきです。被害に遭ってしまったら、サイト運営者や警察機関に相談しましょう。 （参考） 警察庁 - インターネット安全・安心相談 http://www.npa.go.jp/cybersafety/

4. 相談受付状況

6 月のウイルス・不正アクセス関連相談総件数は **1,898 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 **694 件**（5 月：628 件）となり、**過去最悪記録を更新**しました。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 **6 件**（5 月：2 件）、**Winny に関連する相談**が **13 件**（5 月：5 件）、**「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」に関する相談**が **0 件**（5 月：5 件）、などでした。

表 4-1　IPA で受け付けた全てのウイルス・不正アクセス関連相談件数の推移

		1月	2月	3月	4月	5月	6月
合計		960	1,051	1,406	1,668	1,765	1,898
	自動応答システム	529	521	758	962	992	1,081
	電話	390	472	597	651	710	777
	電子メール	39	57	49	55	58	37
	その他	2	1	2	0	5	3

※ 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）、fushin110@ipa.go.jp（不審メール 110 番）、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。

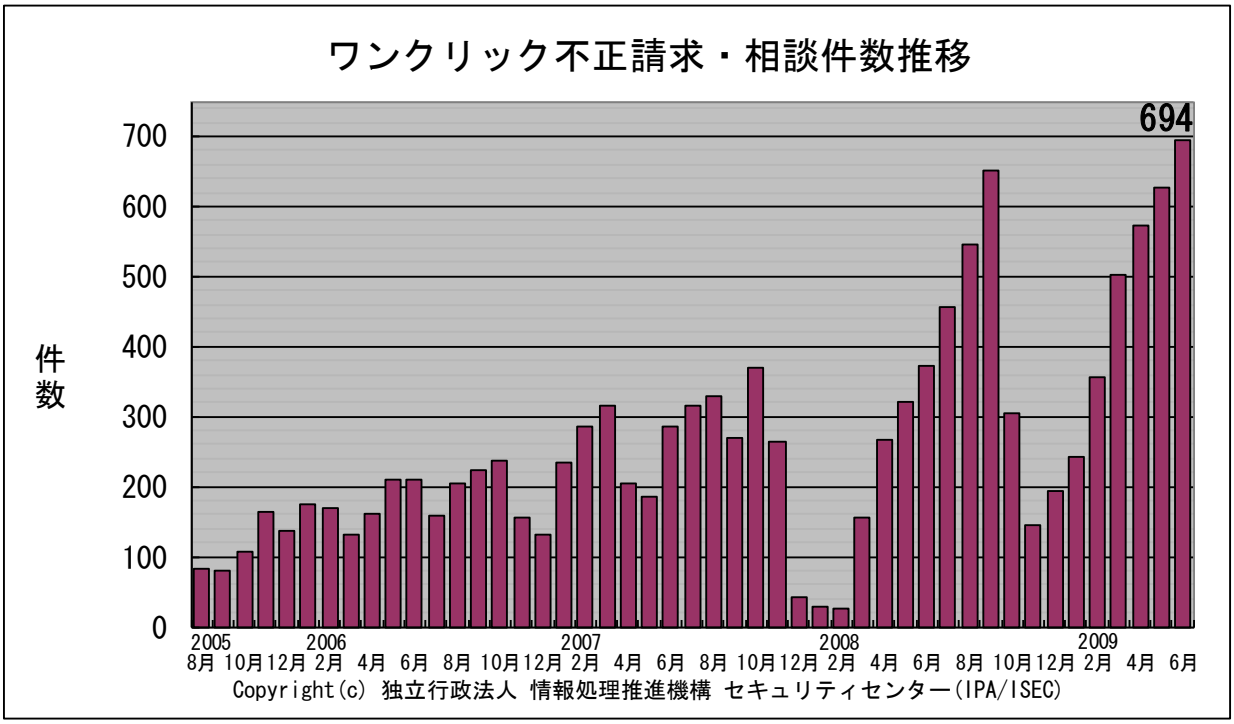


図 4-1　ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

（i）ウイルス対策ソフトを使っていれば、OS のアップデートをしなくてもウイルス感染しない？

相談	組織内で、Windows 2000 と Windows XP のパソコンを利用している。ウイルス対策ソフトを導入し、ウイルス定義ファイルを常に最新の状態にしておけば、Windows Update などしなくても、ウイルスに感染しませんよね？
回答	その考えは間違っています。**Windows Update などで脆弱性を解消しておかないと、ウイルスに感染する可能性は高い**と言えます。 今回の件をたとえ話で解説してみます。 　パソコン　…　家（建物） 　ウイルス対策ソフト　…　家のドアや窓からの出入りを監視するもの ここで、Windows Update を実施していない状態というのは、「家に欠陥がある状態」を指します。すなわち、「壁が崩れていた」「屋根に穴が開いていた」というようなことが想定されます。つまり、脆弱性がある状態だと、常識では考えられないような方法で侵入されたりする、ということです。 **脆弱性の解消は、セキュリティ対策の基本**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

（ii）Windows 98 や Me のパソコンでも、ネットにつながなければ安全？

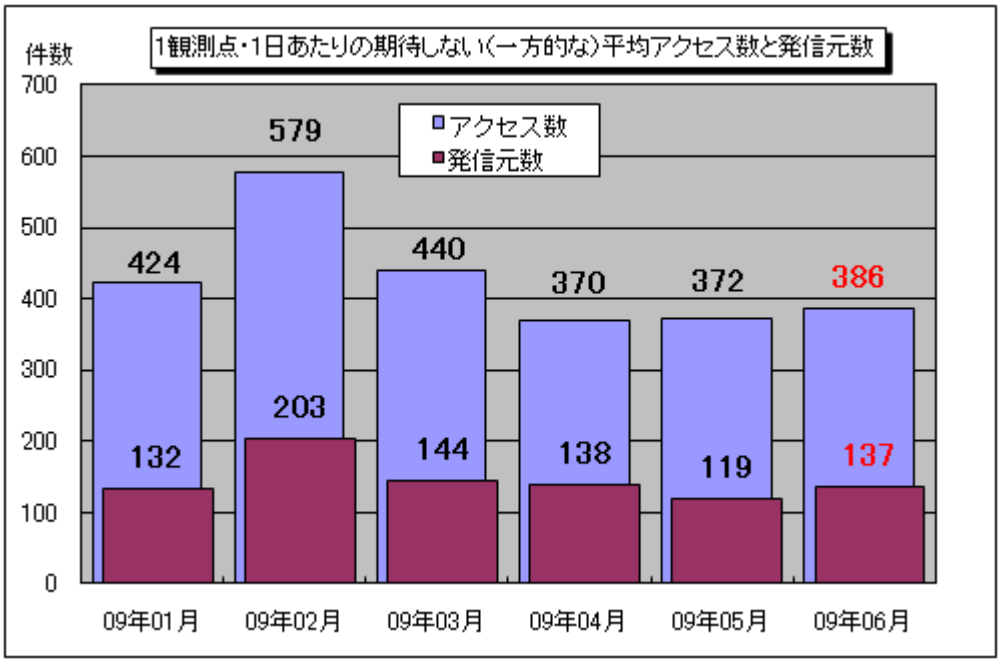
相談	Windows 98 のパソコンを持っています。しばらく使っていなかったのですが、今後、ワープロや表計算の用途のみで利用したいと思います。インターネットや家庭内 LAN につながない環境であれば、ウイルス感染のリスクは全く無いと考えて良いのでしょうか。
回答	**ネットワークにつながなくても、他のパソコンとの間でデータのやり取りをするのであれば、ウイルス感染のリスクはゼロではありません。最近では、USB メモリを介して感染するウイルスが猛威をふるっています**ので、特に注意が必要です。また、**Windows98/Me はマイクロソフト社によるサポートが切れておりますので、脆弱性が発見されても修正プログラムは提供されず、非常に危険な状態**です。仮に、ウイルス対策ソフトが対応していたとしても、土台となる OS 自身に問題があるのですから、ウイルス対策機能が正しく動作する保証はありません。つまり、メーカのサポートが終了した OS を使用する場合は、無防備な状態で使うしかありません。当然、危険な状態ですから、当機構ではメーカのサポートが終了した OS を使用することは推奨しておりません。 （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

5. インターネット定点観測での 6 月のアクセス状況

インターネット定点観測(TALOT2)によると、2009 年 6 月の期待しない(一方的な)アクセスの総数は 10 観測点で **115,860 件**、総発信元(※)は **41,065 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 137 の発信元から 386 件のアクセスがあった**ことになります（図 5-1 参照）。

総発信元（※）：TALOT2 にアクセスしてきた発信元の総数。同一発信元から同一の観測日・観測点・ポートに複数アクセスがあった場合でも、発信元数は 1 としてカウント。

TALOT2 における各観測点の環境は、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。



【図 5-1 1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数】

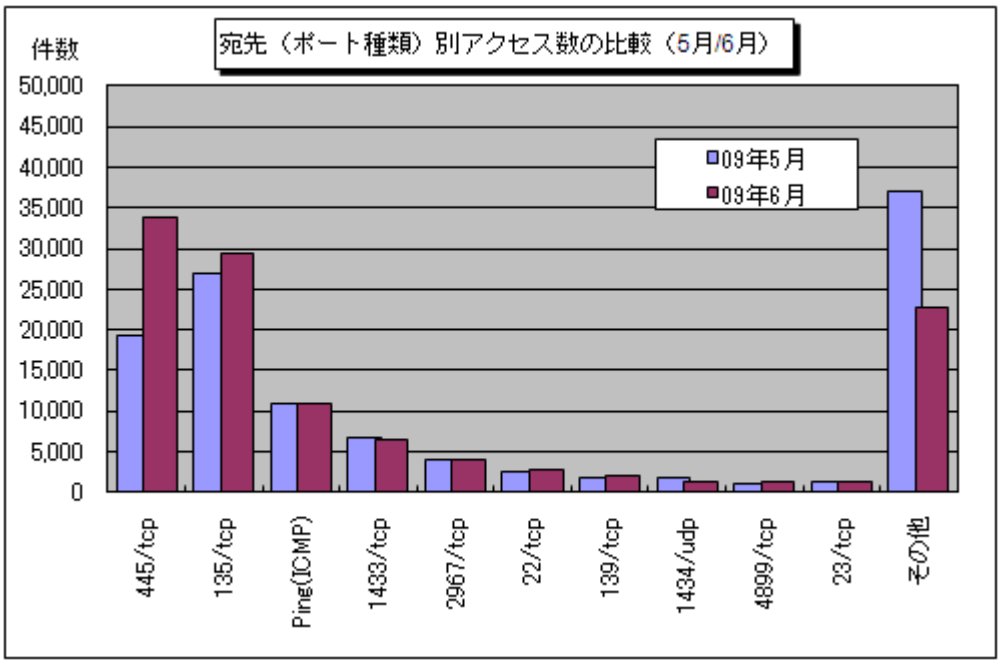
2009 年 1 月～2009 年 6 月までの各月の 1 観測点・1 日あたりの平均アクセス数とそれらのアクセスの平均発信元数を図 5-1 に示します。6 月の期待しない(一方的な)アクセスは、5 月と比べて若干ですが増加しました。

5 月と 6 月の宛先(ポート種類)別アクセス数の比較を図 5-2 に示します。

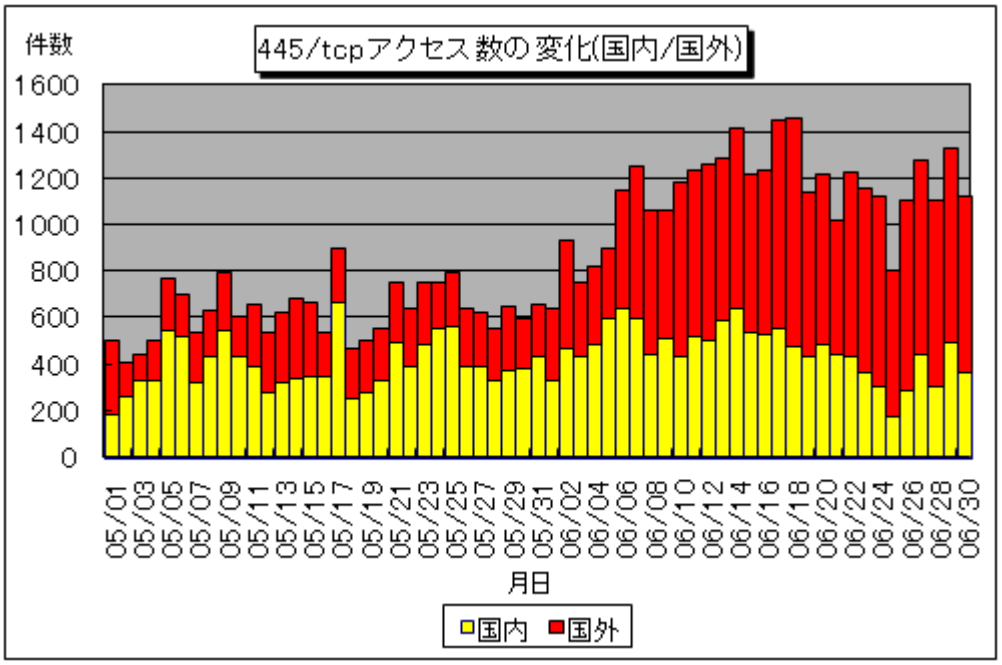
6 月は 5 月に比べ、445/tcp へのアクセスが大幅に増加していました。これは 5 月に比べ、国外からのアクセスが増加したためです(図 5-3 参照)。国外からのアクセスが増加した原因については特定できておりませんが、特定の発信元からのアクセス回数が増加したわけではなく、国外からの発信元数自体が増加したことでアクセス数の増加につながっていました。

また、定点観測を行っている他の組織においても、445/tcp へのアクセスにおいて、国外の発信元数が増加してきているという情報があります。

それ以外のポートへのアクセスについて、大きく変化のあったポートはありませんでしたが、アクセス数の多い上位 10 ポート以外のポートへのアクセスが大幅に減少していました。



【図 5-2 宛先(ポート種類)別アクセス数の比較(5 月/6 月)】



【図 5-3 445/tcp アクセス数の変化(国内/国外)】

以上の情報に関して、詳細はこちらをご参照ください。

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/2009/documents/TALOT2-0907.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
IPA 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