INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
第 08-13-128 号
2008 年 8 月 4 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 7 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 7 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

「 脆弱性(※1)対策は抜かりなく実施しよう！」
― Flash Player などのプラグインの更新をお忘れなく ―

7 月に IPA で解析を行ったウイルスの中に、Flash Player の脆弱性（ぜいじゃくせい）を悪用して感染するものが見つかりました。Flash Player は、ウェブブラウザなどのアプリケーションソフトに追加機能を提供する『プラグイン』というプログラムの代表的なものの一つで、ほとんどのウェブブラウザに組み込まれています(※2)。

Flash Player の脆弱性を解消していない状態で、脆弱性を悪用する Flash コンテンツ（ウイルス）が掲載されたウェブサイトを閲覧した場合、それだけで**ウイルスに感染してしまいます**。そして、このようなウェブサイトが増えてくると、**被害が広範囲に及ぶ可能性があります**。

Flash Player などのプラグインについても、他のプログラムと同様に脆弱性対策は必要です。**お使いの全てのウェブブラウザに対してプラグインのバージョンを最新にして、脆弱性を解消して下さい**。

※1 脆弱性（Vulnerability）
一般にソフトウェア等のセキュリティ上の弱点を指します。セキュリティホール（Security Hole）とも呼ばれます。
※2 出典：アドビシステムズ株式会社の統計（http://www.adobe.com/products/player_census/flashplayer/）

(1)プラグインの概要

プラグインとは、ウェブブラウザなどのアプリケーションソフトに組み込むことによって，追加機能を提供するプログラムのことです。（図 1-1 参照）

例えばウェブブラウザ上で、Adobe Reader のプラグインを利用すれば、PDF（Portable Document Format）ファイルを閲覧することができ、QuickTime のプラグインを利用すれば、動画ファイルなどを再生することができます。同様に Flash Player のプラグインを利用すれば、Flash コンテンツなどの再生を行うことができます。

このように、プラグインを利用することで、アプリケーションソフトの機能拡張を実現できます。

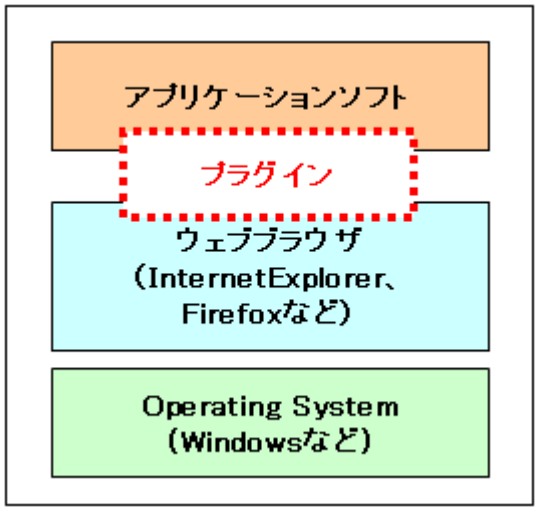

図1-1 プラグインの概念図

(2)Flash Player の問題点

Flash Player の脆弱性を悪用する Flash コンテンツ（ウイルス）が掲載されたウェブサイトが増えてくると、ウイルスに感染する被害が、広範囲に及ぶ可能性があります。この被害を防ぐためには、最新版の、脆弱性のない Flash Player を使う必要があります。しかし、Flash Player は他のプラグインとは異なり、現状、以下の問題が存在するため、脆弱性が存在する古いバージョンのまま使われがちになります。

(a) パソコンの購入時から既にインストールされている場合もあるなど、ほとんどのウェブブラウザに組み込まれており、ユーザが意識せずに利用していることが多い。
(b) 自動更新の仕組みがない上に、実際の更新作業手順が複雑である。
(c) 使用しているウェブブラウザ毎に更新を行う必要があることが見落とされがちである。

このような問題を抱えていることを認識し、常に最新版の Flash Player を使うように心がけることが重要です。

(3)Flash Player の脆弱性を悪用するウイルスについて

IPA で解析を行ったウイルスについて説明します。このウイルスは、Flash Player の脆弱性を悪用します。この脆弱性は、悪意のある Flash コンテンツを開くことによって、任意の命令が実行されてしまうというものです(※3)。この脆弱性がある Windows 版 Flash Player で、当該ウイルスが組みこまれた Flash コンテンツが掲載されたウェブサイトを、閲覧しただけで、このウイルスに感染してしまいます（図 1-2①及び②）。

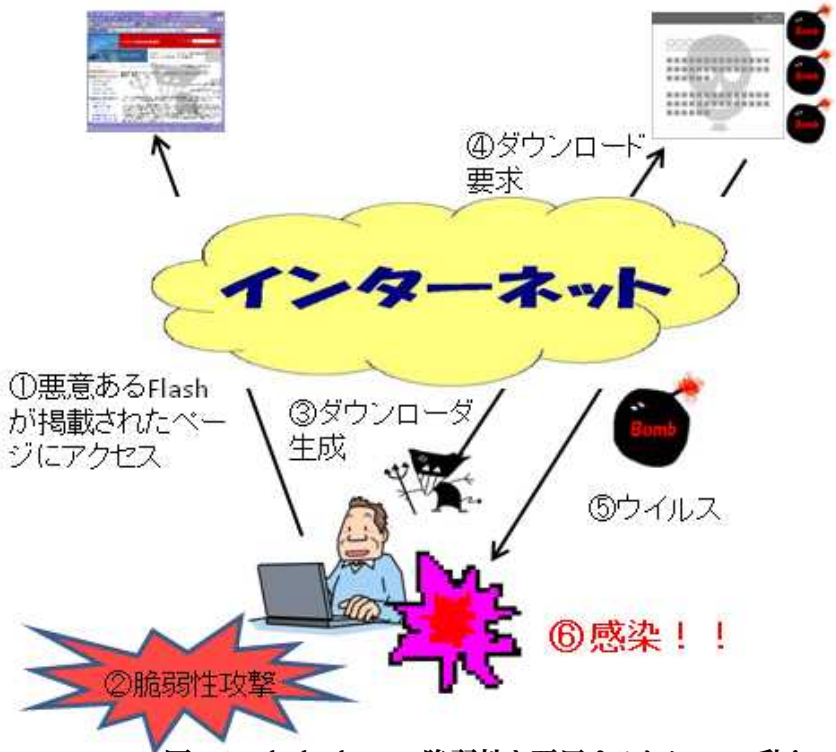

図1-2 Flash Playerの脆弱性を悪用するウイルスの動き

このウイルスが感染すると、ダウンローダ（ダウンロード支援ツール）として動作し（図 1-2③及び④）、特定のウェブサイトから、別のウイルスを取り込みます（図 1-2⑤）。取り込まれたウイルスは、「orz.exe」の名前で保存され、同時に実行されます（図 1-2⑥）。

ウイルスが取り込まれてしまったパソコンでは、個人情報が盗まれたり、パソコンが乗っ取られたりするなどの被害を受ける可能性があります。

ウイルス対策ソフトを最新の状態で使っていたとしても、ウイルスを検知できない場合もあります。そのため、脆弱性を解消することは必須です。以下に示す手順（(4) および (5)）を参考に、Flash Player の確認をして下さい。

※3 JVNDB-2008-001284：http://jvndb.jvn.jp/contents/ja/2008/JVNDB-2008-001284.html

(4)Flash Player の確認手順

お使いのウェブブラウザに、Flash Player がインストールされているかの確認を行うため、「Adobe Flash Player サポートセンター（http://www.adobe.com/jp/support/flashplayer/）」のページから「Adobe Flash Player バージョン確認テスト」をクリックして下さい。Internet Explorer(以下、IE とする)を使った場合の表示例を図 1-3 に示します。この手順はどのウェブブラウザを使っても確認できます。なお、**お使いのウェブブラウザ全てについて、この手順を実施して下さい**。

図 1-3　Flash Player のバージョンテストの表示例 (IE の場合)

ウェブブラウザに Flash Player がインストールされていない場合は、図 1-3 の点線枠部分が図 1-4 のように表示されます。この場合、更新作業は必要ありません。

図1-3の点線枠部分が図1-5のようにバージョン情報が表示される場合、ウェブブラウザにFlash Playerがインストールされています。この場合、表示されたバージョン情報と、図1-3の画面を下にスクロールすることで表示される「現在のFlash Playerバージョン」(図1-6) の該当するウェブブラウザのバージョンとを比較し、最新バージョンかどうかを確認して下さい。

Flash Player のバージョンが最新 (図 1-6 の該当ウェブブラウザが示すバージョンと一致) の場合は作業終了です。最新でない (図 1-6 の該当ウェブブラウザが示すバージョンに満たない) 場合は「(5) Flash Player の更新手順」に進み、最新版への更新を行って下さい。

図 1-4　Flash Player のインストールされていない場合に図 1-3 の点線枠部分に表示されるメッセージ例

図 1-5　Flash Player のインストールされている場合に図 1-3 の点線枠部分に表示されるメッセージ例

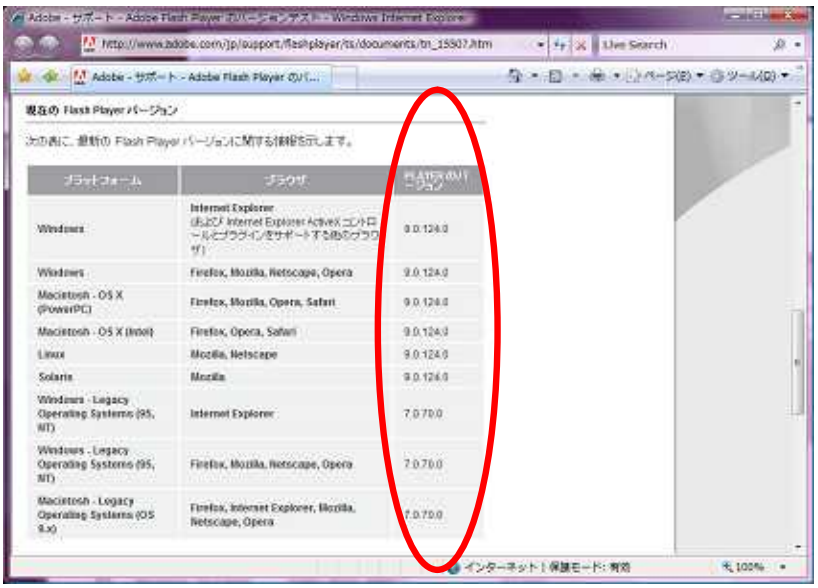

図 1-6　「Flash Player バージョン」の表示例

(5) Flash Player の更新手順

まずインストールされている Flash Player をアンインストールします。アンインストールの手順を以下に示します。

＜アンインストール手順＞

(i) 以下のサイトから「Adobe Flash Player アンインストーラ」をダウンロードします。
http://support.adobe.co.jp/faq/faq/qadoc.sv?230810+002

(ii) 全てのアプリケーションを終了してから、アンインストーラを実行します。

(iii) パソコンを再起動します。

次に以下の専用サイトから最新版の Flash Player をインストールしますが、ウェブブラウザが IE の場合とそれ以外 (Firefox、Opera、Safari など) の場合で手順が異なるので、ここでは分けて説明します。

＜インストール手順＞

【IE の場合】

(i) 図 1-7 に示す通り、IE のインターネットゾーンのセキュリティレベルが「高」に設定してある場合、インストールができないので、Flash Player 導入に必要なウェブサイトを「信頼済みサイト」に追加する必要があります。手順はインターネットオプション画面 (「スタート」→「コントロールパネル」→「インターネットオプション」) からセキュリティタブを指定し、「信頼済みサイト」を指定した状態で「サイト」ボタンをクリックし、表示されたウィンドウから以下のサイトを追加登録して下さい。
http://*.adobe.com
http://*.macromedia.com

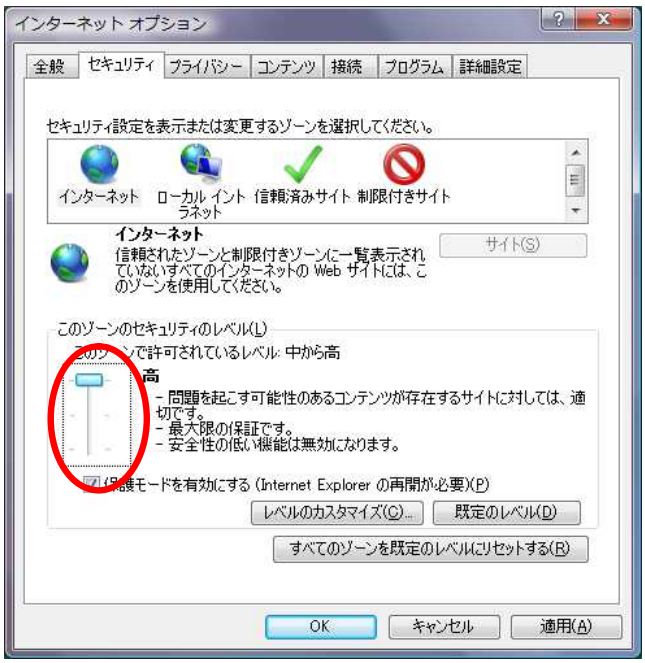

図 1-7 IE のインターネットゾーンのセキュリティレベル設定画面の表示例

(ii) 次に IE でインストール専用サイト (http://www.adobe.com/go/JP-H-GET-FLASH) を開き、「今すぐインストール」のボタンをクリックします。
このとき、同時にインストールするオプションとして「無償 Google ツールバー」のチェックボックスが有効になっていますが、特に必要なければチェックを外し無効にしておいて下さい。

【IE 以外の場合】

(i) ウェブブラウザでインストール専用サイト (http://www.adobe.com/go/JP-H-GET-FLASH) を開き、「今すぐインストール」のボタンをクリックします。

(ii) 「install_flash_player.exe を開く」というダイアログ・ボックスが表示されるので「ファイルを保存」をクリックし、ファイルをダウンロードします。保存場所は適宜指定して下さい。

(iii) ウェブブラウザを終了し、ダウンロードした「install_flash_player.exe」を実行します。

どちらの場合も、Flash Player のインストール完了後、再度「(4) Flash Player の確認手順」を実施し、Flash Player のバージョンが最新になっているか確認して下さい。

(ご参考)
Web ブラウザを使い続けるための“お勧め”設定【プラグイン編】
http://itpro.nikkeibp.co.jp/article/COLUMN/20080605/306754/

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、7 頁の「3.コンピュータ不正アクセス届出状況」を参照）

・SQL インジェクション攻撃によってデータベースが改ざんされた
・オンラインゲームで、誰かが自分になりすましてアイテムなどを処分

○ 相談の主な事例 （相談受付状況及び相談事例の詳細は、9 頁の「4.相談受付状況」を参照）

・いつも見ていたサイトにアクセスしたらウイルス検知
・個人でサーバを立てて運用しているサイトが攻撃を受けた？

○ 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。

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 19.1 万個**と、6 月の約 23.6 万個から 19.1%の減少となりました。
また、7 月の届出件数(※2)は、**1,448 件**となり、6 月の 2,002 件から 27.7%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。
・7 月は、寄せられたウイルス検出数約 19.1 万個を集約した結果、1,448 件の届出件数となっています。

検出数の1位は、**W32/Netsky で約 18 万個 、2 位は W32/Mytob で約 3 千個、3 位は W32/Mydoom で約 2 千個でした。**

ウイルス検出数　約19.1万個 (約23.6万個)　前月比 - 19.1%

（注：括弧内は前月の数値）

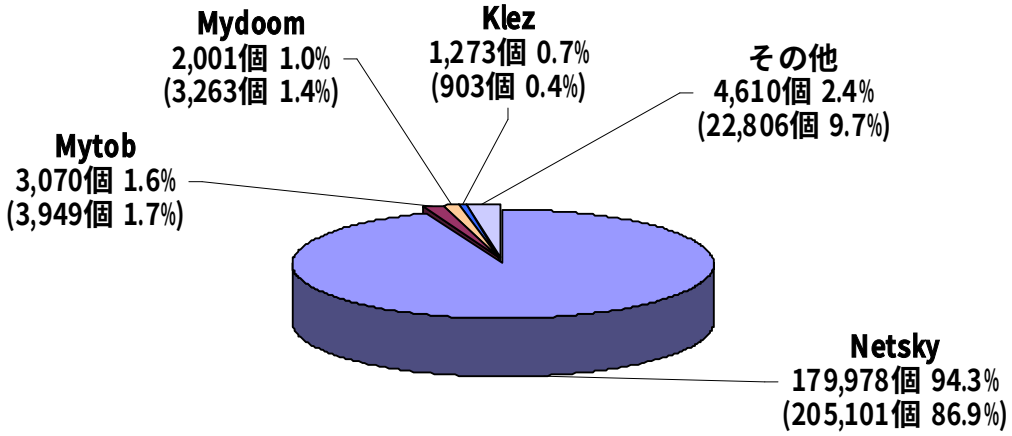

図 2-1

ウイルス届出件数　1,448件 (2,002件)　前月比 - 27.7%

（注：括弧内は前月の数値）

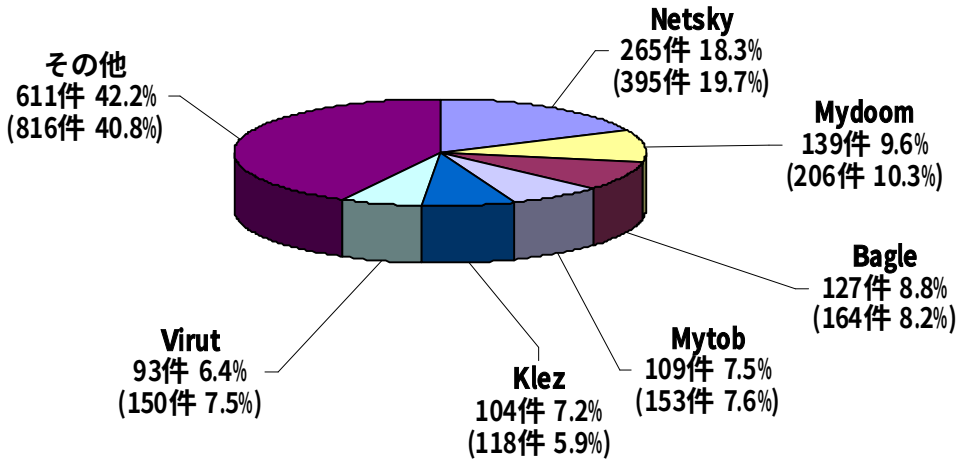

図 2-2

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

		2月	3月	4月	5月	6月	7月
届出(a) 計		4	19	14	4	13	19
	被害あり(b)	4	13	10	4	11	18
	被害なし(c)	0	6	4	0	2	1
相談(d) 計		29	35	56	37	36	49
	被害あり(e)	10	15	31	18	15	26
	被害なし(f)	19	20	25	19	21	23
合計(a+d)		33	54	70	41	49	68
	被害あり(b+e)	14	28	41	22	26	44
	被害なし(c+f)	19	26	29	19	23	24

（1）不正アクセス届出状況

7 月の届出件数は 19 件であり、そのうち何らかの被害のあったものは 18 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 49 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 26 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 2 件、アドレス詐称が 2 件、その他（被害あり）8 件**でした。

侵入届出の被害は、SQL※インジェクション※攻撃を受けて結果としてウェブページコンテンツを改ざんされたものが 2 件、他サイト攻撃の踏み台として悪用されたものが 3 件、ftp サーバ経由で侵入され、ウェブページコンテンツを改ざんされたものが 1 件、でした。侵入の原因は、脆弱性によるものが 2 件、推測され易いパスワードが破られたものが 2 件、サーバのネットワーク設定の不備が 1 件、ftp アカウント情報の悪用によるものが 1 件、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 5 件（ネットオークション 3 件、オンラインゲーム 2 件）、などがありました。

※SQL（Structured Query Language）…リレーショナルデータベースマネジメントシステム（RDBMS）において、データの操作や定義を行うための問合せ言語のこと。
※SQL インジェクション…データベースへアクセスするプログラムの不具合を悪用し、正当な方法以外でデータベース内のデータを閲覧したり書き換えしたりする攻撃のこと。

（4）被害事例

［侵入］

（ⅰ）SQL インジェクション攻撃によってデータベースが改ざんされた

事例	・自社サイト管理者が、データベースのメンテナンスのためにデータベース内のデータにアクセスしたところ、ウイルス対策ソフトがウイルスを検知した。 ・データベースのテーブルを調査したところ、本来無いはずの、不審なサイト上の JavaScript ファイルを参照させるスクリプトが、 <script src=http://www.(省略).com/ngg.js></script> のように埋め込まれ、改ざんされていたことが判明。 ・SQL インジェクションの脆弱性を突かれて攻撃されたことが原因であった。
解説・対策	この事例のように、データベース内のデータを直接チェックすることで、SQL インジェクション攻撃で改ざん被害を受けていないかを簡易的に判断することもできるでしょう。ただ、**SQL インジェクション攻撃は、データ改ざんのみならず、データ窃取のためにも使われます**。**詳細のチェックのためには、日々のログの確認や、ツールによる確認が必要**となります。 （参考） 安全なウェブサイト運営入門 http://www.ipa.go.jp/security/vuln/7incidents/ ウェブサイトの脆弱性検出ツール iLogScanner http://www.ipa.go.jp/security/vuln/iLogScanner/

［その他（被害あり）］

（ⅱ）オンラインゲームで、誰かが自分になりすましてアイテムなどを処分

事例	・ある日突然、オンラインゲームのサイトに自分の ID でログインできなくなった。 ・サイト運営者に調査を依頼したところ、何者かがログインして、ゲーム内の自分のキャラクタが所持していたアイテムや通貨を放出していたことが判明。 ・ゲームサイトへのログイン時、ID やパスワードをパソコン内に自動保存させていたため、何らかの方法で読み取られた可能性も否定できない。
解説・対策	はっきりした原因は分かりませんでしたが、**一般的に、パソコン内にログイン ID やパスワードを保存してあると危険**です。誰かがそのパソコンを操作したらパスワードを知らなくてもログインできますし、ウイルスに感染してパスワードが盗まれてしまうこともあるからです。もし被害に遭ったら、すぐにサイト管理者に通報するとともに、警察機関に被害届を出しましょう。 （参考） 警察庁 － インターネット安全・安心相談 http://www.cybersafety.go.jp/

4．相談受付状況

7 月の相談総件数は **1387 件**であり、過去最多の件数となりました。そのうち**『ワンクリック不正請求』に関する相談**が **457 件**（6 月：372 件）と**大幅に増加し、過去最悪**となりました。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 **14 件**（6 月：14 件）、**Winny に関連する相談**が **4 件**（6 月：4 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

	2月	3月	4月	5月	6月	7月
合計	**350**	**654**	**938**	**1080**	**1211**	**1387**
自動応答システム	192	373	514	649	693	817
電話	110	214	335	379	456	500
電子メール	47	66	87	48	60	70
その他	1	1	2	4	2	0

※　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。

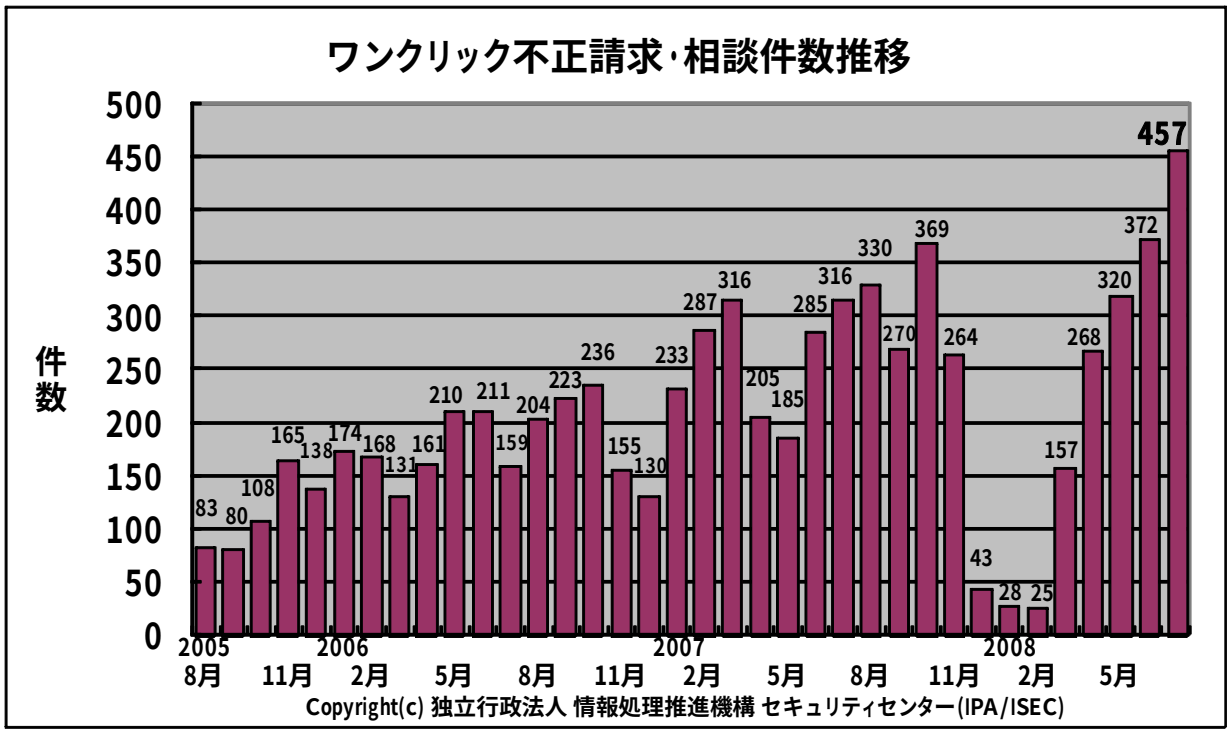

図 4-1　ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

(i) いつも見ていたサイトにアクセスしたらウイルス検知

相談	ある有名な企業のサイトにアクセスしたら、ウイルス対策ソフトがウイルスを検知した。このサイトは毎日見ているもの。前日も見ていたが、何も反応は無かった。これはどういうことか。
回答	企業の**サイトが、悪意ある者によって改ざんされていた**ようです。改ざんの結果、その企業**サイトにアクセスするだけで、ウイルスをダウンロードさせられてしまう仕掛け（スクリプト）が埋め込まれていました**。この仕掛けは、OS やアプリケーションの脆弱性を攻撃するものですので、**脆弱性を解消しておけば、ウイルスをダウンロードさせられることはありません**。Microsoft Update や、使っているアプリケーションの更新作業を実施することで、OS やアプリケーションを常に最新の状態にしておきましょう。 （ご参考） 呼びかけ：「いつも見ていたウェブサイトなのにウイルス検知？」 http://www.ipa.go.jp/security/txt/2008/03outline.html

(ii) 個人でサーバを立てて運用しているサイトが攻撃を受けた？

相談	突然、ウェブサーバに対して大量のリクエストが殺到し、サーバがダウンした。攻撃元と思われる IP アドレスは、様々であった。数時間経って、ようやく落ち着いた。
回答	攻撃されたというサイトの URL で検索を掛けたところ、**相談者のサイトに書かれていた記事が某有名ニュースサイトに紹介されていた**ことが分かりました。その**ニュースサイトを見た人々が、リンクをクリックして一斉に当該サイトにアクセスしたために、一時的に DoS 攻撃を受けたような状況になってしまっていた**ようです。 （ウェブサーバのアクセスログを確認してもらったところ、相談者のサイトへのリンク元ページの情報である「**Referer 情報**」は、正に当該ニュースサイトの URL でした）

5．インターネット定点観測での７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 7 月の期待しない（一方的な）アクセスの総数は 10 観測点で **148,028 件**、総発信元数(※)は **63,407 箇所**ありました。1 観測点で見ると、1 日あたり **205** の発信元から **478 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、205 人の見知らぬ人(発信元)から、それぞれ約 2 件ずつの不正と思われるアクセスを受けている**ということになります。

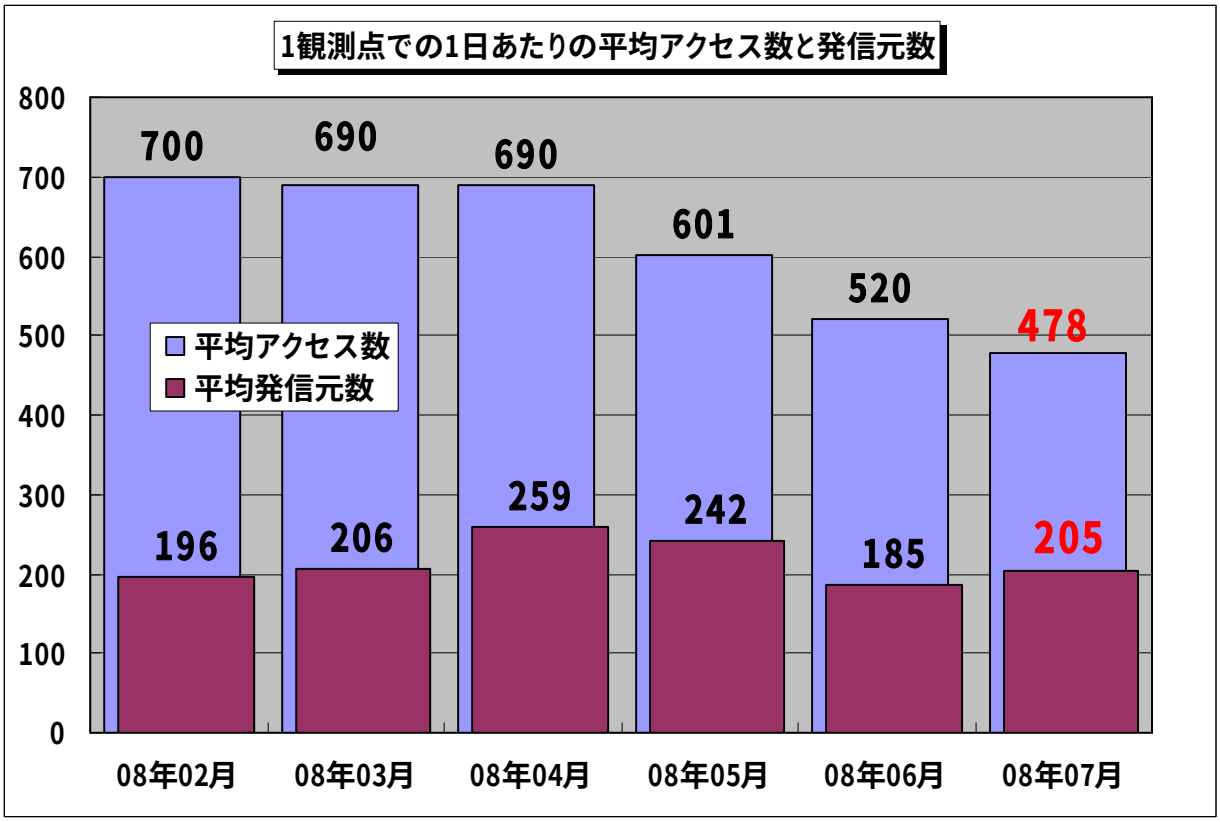

図 5-1：１観測点での１日あたりの期待しない(一方的な)アクセス数および発信元数

2008 年 2 月～2008 年 7 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、7 月の期待しない（一方的な）アクセスは 6 月と比べて減少しており、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。

2008 年 7 月のアクセス状況が、6 月と比べて減少した原因は、主に Windows のファイル共有やプリンタ共有の脆弱性を狙った不正アクセスと思われる 445/tcp へのアクセスと、Windows Messenger サービスを利用したポップアップ(スパム)メッセージを送信するアクセスである 1028/udp へのアクセスが減少したためです。その他のポートへのアクセス数については大きな変化はありませんでした。

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/TALOT2-0808.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