プレスリリース
第 10-32-193 号
2010 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 [2010 年 7 月分] について

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、2010 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

「 この画面が出たら要注意！ 」
― 一向に減らないワンクリック請求の被害 ―

IPA に寄せられる「ワンクリック請求」に関する相談件数が、2010 年 6 月で累計 2 万件を超えました。毎月の相談件数においても、2010 年に入ってから常に 600 件以上で推移しており、一向に被害が減少していません（図 1-1 参照）。これらのほとんど全てが、アダルトサイトに関係する被害でした。

被害が減らない要因としては、「ワンクリック請求」を行うウェブサイトと、このようなウェブサイトの罠を知らないパソコン利用者の両者が、未だ多数存在していることが挙げられます。

ここでは、改めて「ワンクリック請求」の被害に遭わないための注意点を解説します。

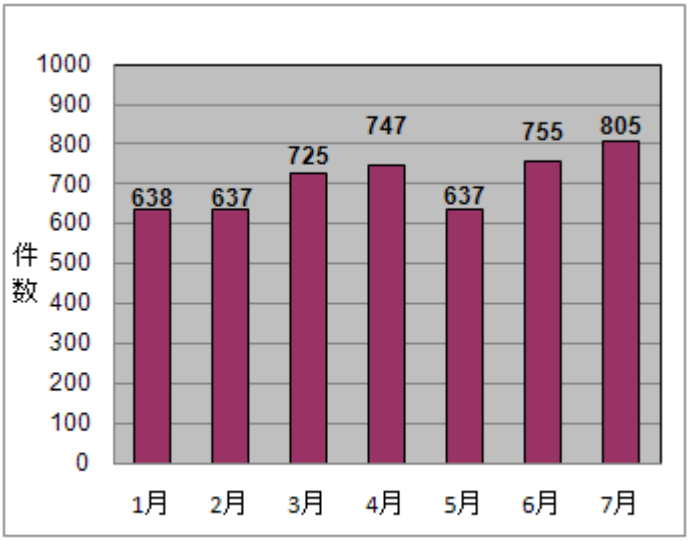


図 1-1：ワンクリック請求・相談件数推移（2010 年）

(1)「ワンクリック請求」の現状

「ワンクリック請求」では、例えば、アダルトサイトで無料の動画を見るつもりで、不用意にクリックし、先に進んでいくことで、利用者のパソコンにマルウェア※を埋め込まれ、図 1-2 のような料金請求画面が数分おきに表示されるようになるなどの事象が発生します。

IPA ではこのような仕掛けが施されたアダルトサイトが、毎月 10 サイト程度新規公開（リニューアルを含む）されていることを確認しており、それらを含め、常時 20 サイト以上の「ワンクリック請求」を行うウェブサイトが稼働していることを確認しています。

図 1-2：アダルトサイトの料金請求画面例

このようなウェブサイトの手口は以前からほぼ変化しておらず、パソコン利用者の無警戒な行動が、こうした被害が後を絶たないことにつながっていると考えられます。

※ マルウェア：コンピュータの利用者が意図しない動作をする不正なプログラムの総称。

この脅威の手口と対策について、以下に詳しく解説しています。

（ご参考）
「ワンクリック請求に関する注意喚起」（IPA）
http://www.ipa.go.jp/security/topics/alert20080909.html

（2）被害に遭わないために最低限注意すべきこと

IPA への相談内容は、アダルトサイトの動画コンテンツのページで、動画に見せかけたリンクを罠と知らずにクリックすることで、パソコンにマルウェアを埋め込まれるというものがほとんどです。

しかし、1 回クリックしただけでマルウェアを埋め込まれることはありません。マルウェアを埋め込まれてしまう前に、いくつかの特徴的な画面を経ています。ここでは、2 つの特徴的な画面（図 1-3[A]、[B]）を例に挙げて説明します。

パソコン利用者は、いくつかのアダルトサイトを経て、「はい」「いいえ」などと判断を促される画面（図 1-3[A]）に誘導されます。この画面では、**「はい」や「いいえ」のボタンが強調されている**ことが特徴です。**このような画面を見た場合には、“もしかして、罠ではないか？”と疑いを持つ慎重さが求められます。**

IPA で確認している主なサイト 9 種類の特徴的な画面を次項で紹介しますが、それら以外でも不用意に「はい」をクリックせず、落ち着いて画面に書かれている内容を確認し、少しでも“怪しいかも？”と思った場合には画面右上の×ボタンをクリックしてウィンドウを閉じてください。

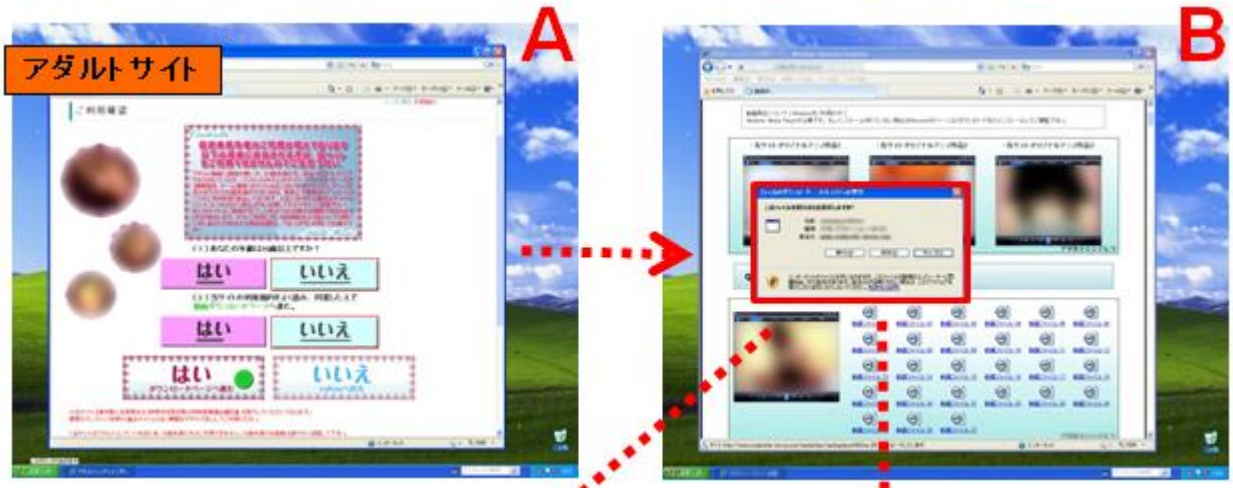
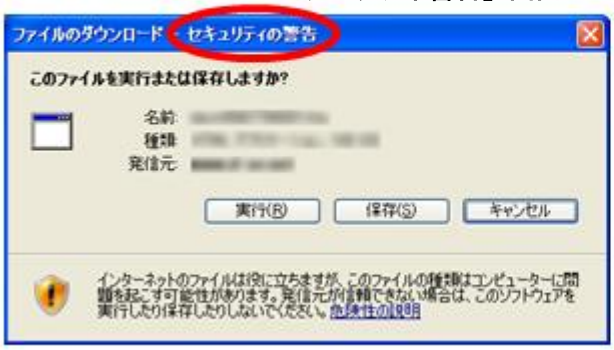


図 1-3：特徴的な 2 つの画面例

Windows XP の「セキュリティ警告」画面



Windows 7/Vista の「セキュリティ警告」画面

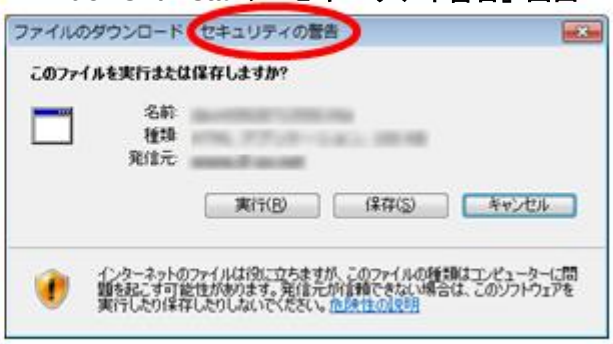


図 1-4：「セキュリティの警告」画面例（図 1-3[B]の拡大図）

図 1-3[A]で「はい」をクリックして先に進み、動画を見ようとしてさらにクリックすると、図 1-3[B]の画面が現れます。図 1-3[B]の画面を拡大したものを図 1-4 に示します。**通常の動画サイトであれば、画面上の再生ボタンをクリックすると動画の再生が始まるはずです。動画を見ようとしただけで図 1-4 の画面が現れたら、“もしかして、罠ではないか？”と疑ってください。**

図 1-4 の画面をよく見ると、「**セキュリティの警告**」と書かれていることが分かります。これは、**何らかのプログラムがダウンロードされ、パソコン上で実行されようとしている時に表示される**ものです。ここでこの**警告を無視して「実行」ボタンをクリックすると、自分自身の手でパソコンにマルウェアを埋め込んでしまう**ことになります。**動画を見ようとしただけでこのような画面が表示されたら、「実行」や「保存」のボタンを押すべきではありません。**

（3）IPA に相談があったサイト

IPA に相談があった主なサイト 9 種類の画面（図 1-3[A]に代表される画面）を図 1-5 に示します。今後もこれらに似たサイトの出現が予想されますが、画面の特徴をつかんでおき、不用意な行動は慎んでください。

図 1-5：IPA で確認している主なサイト 9 種類の特徴的な画面例

（4）最後に

万が一、パソコンに料金請求の画面（図 1-2）が表示されるようになり、料金支払いについて心配に思う場合でも、絶対に業者に連絡を取ったりせずに、最寄りの消費生活センター等に相談してください。

（ご参考）
「全国の消費生活センター等」（国民生活センター）
http://www.kokusen.go.jp/map/
「インターネットをめぐる消費者トラブル＃１」（消費者庁）
http://www.caa.go.jp/adjustments/pdf/091203adjustments_1.pdf

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、7 頁の「3.コンピュータ不正アクセス届出状況」を参照）
・phpMyAdmin の脆弱性を突かれ、結果としてフィッシングに悪用するページを設置された
・外部サイト攻撃ツールを埋め込まれ、踏み台として悪用された

○ 相談の主な事例 （相談受付状況および相談事例の詳細は、9 頁の「4.相談受付状況」を参照）
・OS のサポートが終了してもウイルス対策ソフトがあれば全くの無防備ではない？
・親戚にパソコンを貸したら、アダルトサイトの請求画面が表示されるようになって戻ってきた

○ インターネット定点観測（11 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－

（1）ウイルス届出状況

7 月のウイルスの検出数※1 は、**約 4.7 万個**と、6 月の約 4.1 万個から 15.9%の増加となりました。また、7 月の届出件数※2 は、**1,209 件**となり、6 月の 1,245 件から 2.9%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。
・7 月は、寄せられたウイルス検出数約 4.7 万個を集約した結果、1,209 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 3.1 万個**、2 位は **W32/Autorun** で**約 9 千個**、3 位は **W32/Mydoom** で**約 5 千個**でした。

ウイルス検出数　約4.7万個（約4.1万個）　前月比＋15.9%

（注：括弧内は前月の数値）

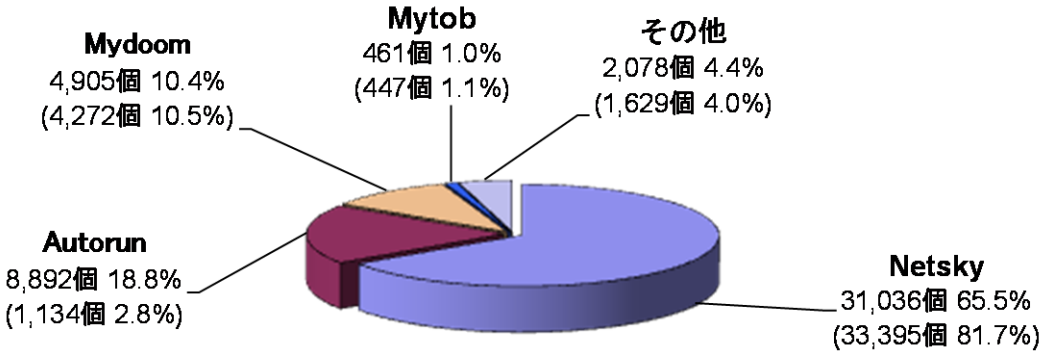


図 2-1：ウイルス検出数

ウイルス届出件数　1,209件（1,245件）前月比 －2.9%

（注：括弧内は前月の数値）

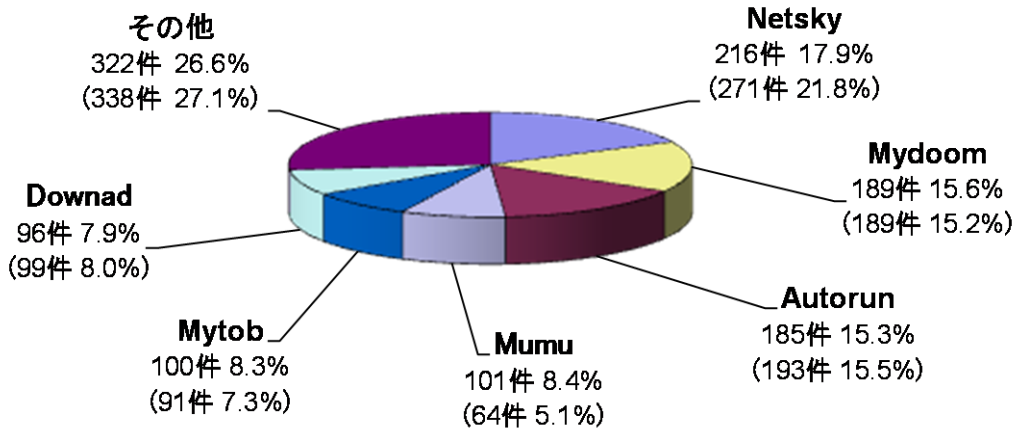


図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

2010 年 7 月の不正プログラムの検知状況は、6 月の ADCLICKER のように急増した事例はありませんでしたが、FAKEAV や DOWNLOADER の増加が確認されました（図 2-3 参照）。

このような不正プログラムはメールの添付ファイルとして配布されるケースが多く、そのメールの配信にはボット※3 に感染したパソコンが悪用されることがあります。

サイバークリーンセンター※4 では、ボットに関する対策や駆除ツールを提供しています。不正プログラムのメール配信に加担することがないよう、ボットに感染していないか確認するとともに、不正プログラムを取り込まないようにするなど、感染防止のための対策実施が必要です。

（ご参考）
「感染防止のための知識」（サイバークリーンセンター）
https://www.ccc.go.jp/knowledge/

※3　ボットとは、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。

※4　サイバークリーンセンターとは、総務省・経済産業省が連携して実施するボット対策プロジェクトです。
（参考）サイバークリーンセンターについて
https://www.ccc.go.jp/ccc/

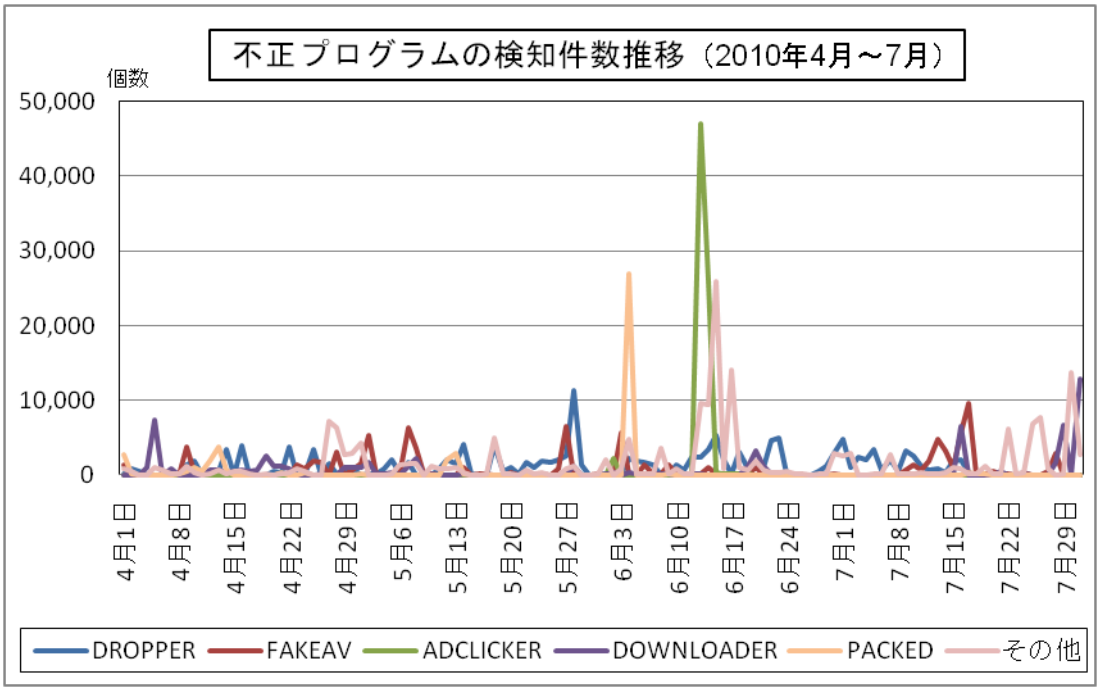


図 2-3：不正プログラムの検知件数推移

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		27	19	11	8	15	14
	被害あり(b)	17	13	10	5	13	9
	被害なし(c)	10	6	1	3	2	5
相談(d) 計		47	60	39	52	77	44
	被害あり(e)	28	23	16	22	50	23
	被害なし(f)	19	37	23	30	27	21
合計(a+d)		74	79	50	60	92	58
	被害あり(b+e)	45	36	26	27	63	32
	被害なし(c+f)	29	43	24	33	29	26

（1）不正アクセス届出状況

7 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 9 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 44 件（うち 3 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 23 件でした。

（3）被害状況

被害届出の内訳は、**侵入 5 件、DoS 攻撃 1 件、なりすまし 3 件、**でした。

「侵入」の被害は、ウェブページが改ざんされていたものが 2 件（不正なコードの挿入 1 件、フィッシングに悪用するためのコンテンツ設置 1 件）、外部サイトを攻撃するツールを埋め込まれ、踏み台として悪用されていたものが 3 件でした。侵入の原因は、詳細は判明していないが“ガンブラー”の手口だと推測されるものが 1 件、phpMyAdmin の脆弱性を突かれたものが 1 件でした（他は原因不明）。

「なりすまし」の被害は、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（オンラインゲーム 3 件）でした。

（4）被害事例

［侵入］

（i）phpMyAdmin の脆弱性を突かれ、結果としてフィッシングに悪用するページを設置された

事例	・組織外から「そちらのウェブサイトに、フィッシングに悪用するためのページがある」との連絡が入った。 ・調査したところ、ある部門のウェブページが、eBay のサインインページを模した内容に改ざんされていたことが判明。 ・当該ウェブサーバでは CMS（Content Management System）を導入しており、その管理用に phpMyAdmin（MySQL をネットワーク越しに管理するための DB 接続クライアント）も利用していた。 ・phpMyAdmin の脆弱性を突かれ、php の遠隔操作ツールを埋め込まれたことが原因で、ウェブページを改ざんされたものと推測。
解説・対策	**インターネット越しにサーバを管理できるようにする場合、悪意ある者に狙われて悪用されるかもしれない、ということを念頭に置いた対策が必要**です。有名なツールであれば、特に狙われやすいと言えます。脆弱性の解消はもちろんのこと、WAF（Web Application Firewall）を導入してサイト全体のセキュリティを強化することも有効です。 （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

（ii）外部サイト攻撃ツールを埋め込まれ、踏み台として悪用された

事例	・組織外から「あなたの管理するサーバから、SSH※で使うポートへパスワードクラッキング※攻撃を多数受けている」との連絡が入った。 ・調査したところ、root 権限を奪取された上、外部サーバの SSH で使うポートへの攻撃ツールや IRC サーバツール、ボットなどを埋め込まれていることが判明。 ・通常アカウント経由でサイト侵入されていたが、侵入後に Linux カーネルの脆弱性を突かれて root 権限への昇格が成功していた痕跡があった。 ・ログファイルが改ざんされたようで、侵入の原因は現状では追い切れていない。
解説・対策	**脆弱性を放置していたため、被害が拡大してしまった**残念な例です。root 権限を奪われ、IRC サーバツールやボットまで埋め込まれているため、完全にサーバを乗っ取られていたと思われます。今後は、**脆弱性の解消やサーバログの定期的確認など、基本に立ち返った対策が求められます**。 （参考） IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html

※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. 相談受付状況

7 月のウイルス・不正アクセス関連相談総件数は **2,133 件**でした。そのうち**『ワンクリック請求』に関する相談**が **805 件**（6 月：755 件）、**『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 **5 件**（6 月：7 件）、**Winny に関連する相談**が **3 件**（6 月：2 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 **1 件**（6 月：0 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

	2月	3月	4月	5月	6月	7月
合計	1,789	2,000	2,110	1,881	1,983	2,133
自動応答システム	977	1,057	1,194	1,091	1,022	1,142
電話	736	846	835	714	829	924
電子メール	70	92	81	76	129	66
その他	6	5	0	0	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）、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。

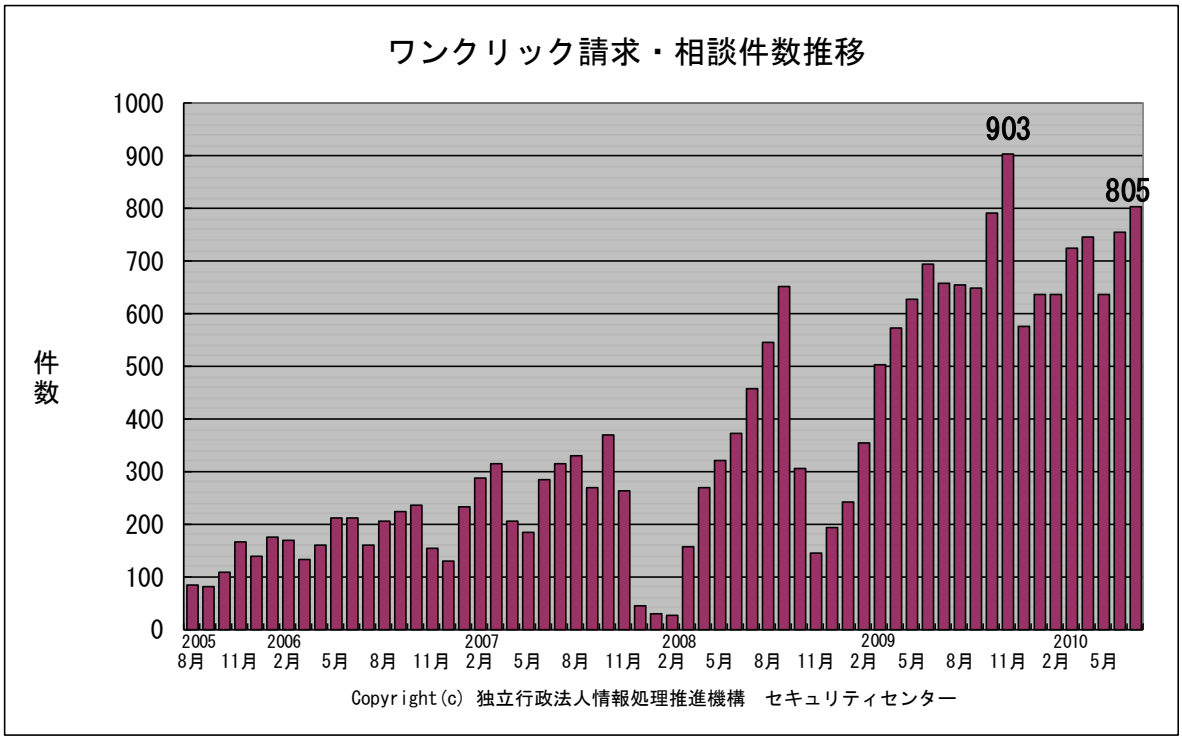


図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）OS のサポートが終了してもウイルス対策ソフトがあれば全くの無防備ではない？

相談	一般論として、OS のサポートが終了しても、ウイルス対策ソフトをインストールして、最新の状態で使用しておけば、全くの無防備な状態ではないと思うのだが…。
回答	**一般的にアプリケーションソフトは、サポートの終了した OS 上での動作は保証されません**。これは、ウイルス対策ソフトも例外ではありません。**しかし、OS のサポートが終了した後でも、ウイルス対策ソフトがその OS をサポートすることを明記していれば、防御機能はあるという認識で良い**と考えます。ただ、従来からあるパターンマッチング方式によるアンチウイルス機能と、脆弱性攻撃の検知および防御機能とでは、中身が全く異なるため、どんなウイルス対策ソフトでも大丈夫な訳ではないことに注意してください。さらに、**これは恒久的対策では無く、あくまでも“つなぎ”的な措置であることを認識しておくことが重要**です。 （参考） IPA ‐2010 年 7 月の呼びかけ「サポートが終了した OS は危険です！」 http://www.ipa.go.jp/security/txt/2010/07outline.html

（ii）親戚にパソコンを貸したら、アダルトサイトの請求画面が表示されるようになって戻ってきた

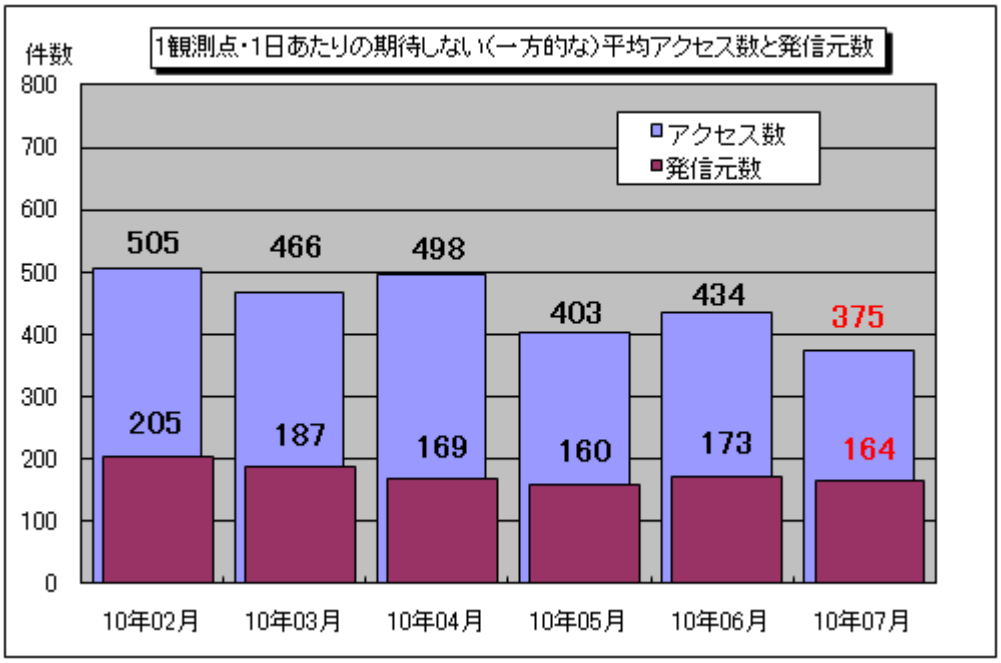
相談	親戚が家に遊びに来たのでパソコンを貸してあげたところ、アダルトサイトの請求画面が表示され続ける状態になって戻ってきた。これはどういうことか。直すには初期化しかない？
回答	親戚の方がアダルトサイトを閲覧して、ワンクリック請求の手口に引っ掛かり、ウイルスに感染しています。**Windows XP／Vista／7 のパソコンであれば、システムの復元機能を使用し、パソコンを貸した日よりも前の日の状態に戻すことをお勧めします**。システムの復元を行ってもまだ請求画面が表示されるのであれば、パソコンの初期化が必要です。 **重要な情報を扱っているパソコンは、ウイルス感染のリスクを減らすためにも、たとえ相手が身内でも、安易に貸すことは控えてください。** （参考） IPA – ワンクリック請求に関する注意喚起 http://www.ipa.go.jp/security/topics/alert20080909.html

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、2010 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 **116,141 件**、延べ発信元数※は **50,845 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 164 の発信元から 375 件のアクセスがあった**ことになります（図 5-1 参照）。

※ 延べ発信元数：TALOT2 の各観測点にアクセスしてきた発信元を単純に足した数のことを、便宜上、延べ発信元数とする。ただし、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は、発信元数を 1 としてカウントする。

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】

2010 年 2 月～2010 年 7 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。7 月の期待しない（一方的な）アクセスは、6 月と比べて減少しました。

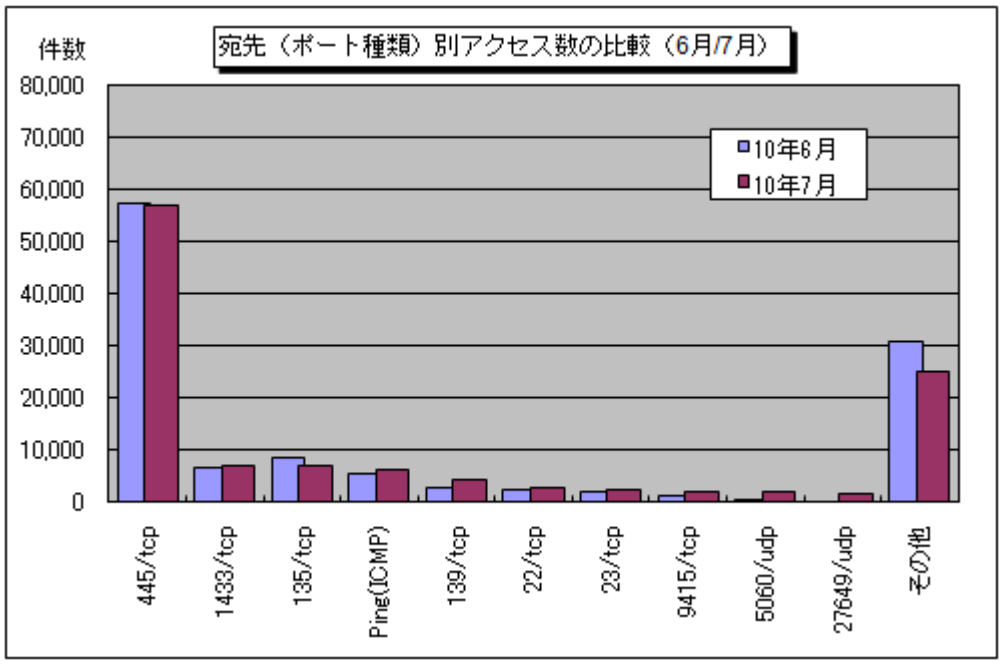
6 月と 7 月の宛先（ポート種類）別アクセス数の比較を図 5-2 に示します。これをみると、これまでは上位に挙がって来なかった 27649/udp や、5060/udp へのアクセスが上位にランクされました。

27649/udp に関しては、7 月上旬に TALOT2 の 1 つの観測点に海外の多数の発信元からのアクセスが観測されていました。このポートは特定のアプリケーションで使用されるポートというわけではなく、このアクセスが何を目的としたものだったかは不明です。

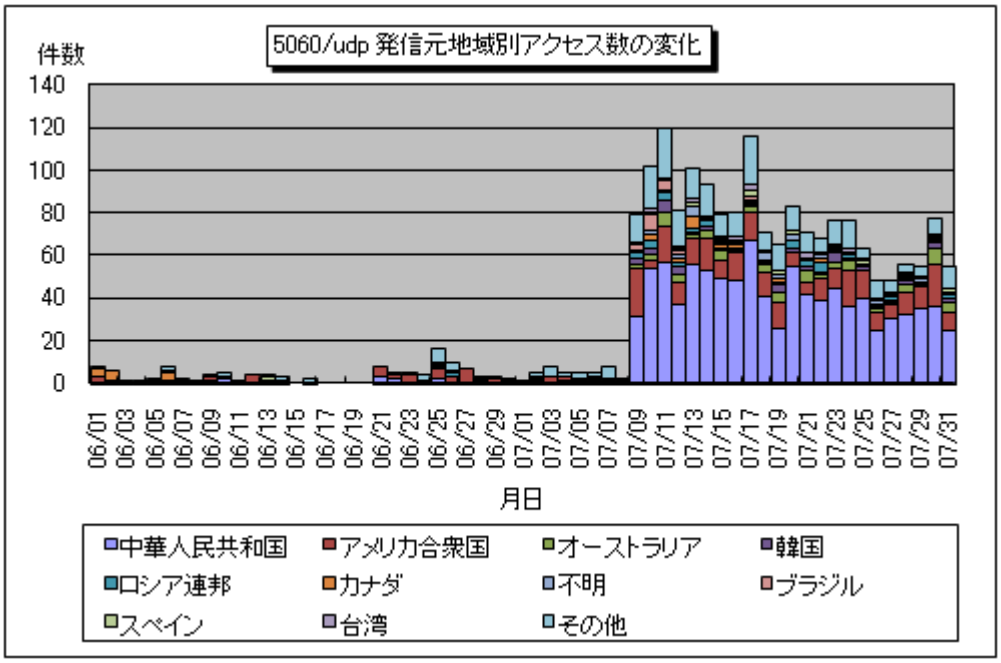
また、5060/udp に関しては、7 月 9 日から TALOT2 の複数の観測点で多く観測され始めました（図 5-3 参照）。この現象は他の定点観測を行っている組織でもほぼ同様に観測されており、広い範囲で発生していたと思われます。なお、5060/udp は一般的に SIP※サーバで利用されるポートであり、このアクセスが SIP サーバに対しての何らかの攻撃を目的としたものだった可能性があるため、SIP サーバを運用している場合は、何らかの影響を受けていないか確認してみることをお勧めします。

※SIP（Session Initiation Protocol）：IP 電話などに用いられる通信プロトコルのこと。

（ご参考）
5060/UDP に対するアクセスの増加について（警察庁）
http://www.npa.go.jp/cyberpolice/detect/pdf/20100714.pdf



【図 5-2：宛先（ポート種類）別アクセス数の比較（6 月/7 月）】



【図 5-3：5060/udp 発信元地域別アクセス数の変化】

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/2010/documents/TALOT2-1008.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。』
一般社団法人 JPCERT コーディネーションセンター：http://www.jpcert.or.jp/
@police：http://www.cyberpolice.go.jp/
フィッシング対策協議会：http://www.antiphishing.jp/
株式会社シマンテック：http://www.symantec.com/ja/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