プレスリリース
第 10-27-190 号
2010 年 7 月 5 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 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：藤江 一正）は、2010 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

「 サポートが終了した OS は危険です！ 」

IPA では、2007 年 5 月公開の「今月の呼びかけ」(※1)で、サポートが終了した OS（Operating System）を使うことの危険性を取り上げましたが、IPA に寄せられる相談には、依然として Windows 98/Me 等のサポートが終了した OS の利用者からのものが含まれています。また、これらの OS を使うことの危険性を認識していない、企業のシステム担当者からの相談もありました。

2010 年 7 月 13 日（米国時間）には、多数の利用者がいると推測される Windows 2000 や Windows XP Service Pack 2（SP2）のマイクロソフト社によるサポートが終了します(※2)。このため、改めて、サポートが終了した OS を使うことの危険性と、今後の対処方法について説明します。

(※1)「サポートが終了した OS を搭載した PC の危険性を認識しよう！！」（IPA, 2007 年 5 月の呼びかけ）
http://www.ipa.go.jp/security/txt/2007/05outline.html#5

(※2)「Windows Vista RTM / Windows XP Service Pack 2 (SP2) / Windows 2000 (Server / Professional) 製品のサポート終了についてのご案内」（マイクロソフト社）
http://www.microsoft.com/japan/windows/lifecycle/default.mspx

（1）OS のサポート終了時期とその危険性

（i）OS 別の利用状況とサポートの終了時期

直近の 1 年間（2009 年 7 月 1 日～2010 年 6 月 30 日）に IPA に寄せられた相談について、相談者が利用していた OS の種別の分布を表 1-1 に示します。2006 年 7 月にマイクロソフト社によるサポートが終了して約 4 年が経過している Windows 98/Me の利用者は 94 件（1.3%）となっています。これらの利用者は、現在、修正プログラムも提供されない上に、その OS 上で動作するセキュリティ対策ソフトのサポートもない状態で利用しているため、外部からの攻撃に対して無防備であり、非常に危険です。

表 1-1：相談者が利用していた OS 種別

OS 種別	Windows 7	Windows Vista	Windows XP	Windows 2000	Windows 98/Me	Mac OS	その他
相談件数	313	2,207	4,249	100	94	26	45
割合	4.4%	31.4%	60.4%	1.4%	1.3%	0.4%	0.6%

注) 全相談中、OS 種別が判別できた事案のみ集計。

（ii）サポートが終了した OS を利用することの危険性

サポートが終了した OS を使うことの最大の問題は、その OS に対する**修正プログラムが製造元から提供されなくなる**ことです。修正プログラムが提供されないということは、OS の脆弱性が発見されても、それを解消することができなくなることを意味します。

脆弱性が存在する OS を搭載したパソコンには、次のような危険性があります。

- インターネットを経由して脆弱性を悪用する攻撃を受けると、パソコンへの侵入などの不正アクセスを許してしまう。
- 悪意あるウェブサイトを閲覧するだけで、ウイルスに感染させられてしまう。

上記のような不正アクセスやウイルス感染の被害を受けたパソコンは、**第三者を攻撃するための踏み台として利用される可能性があり、その場合、自分以外のインターネット利用者に対して攻撃をしてしまう危険性があるということを認識してください。**

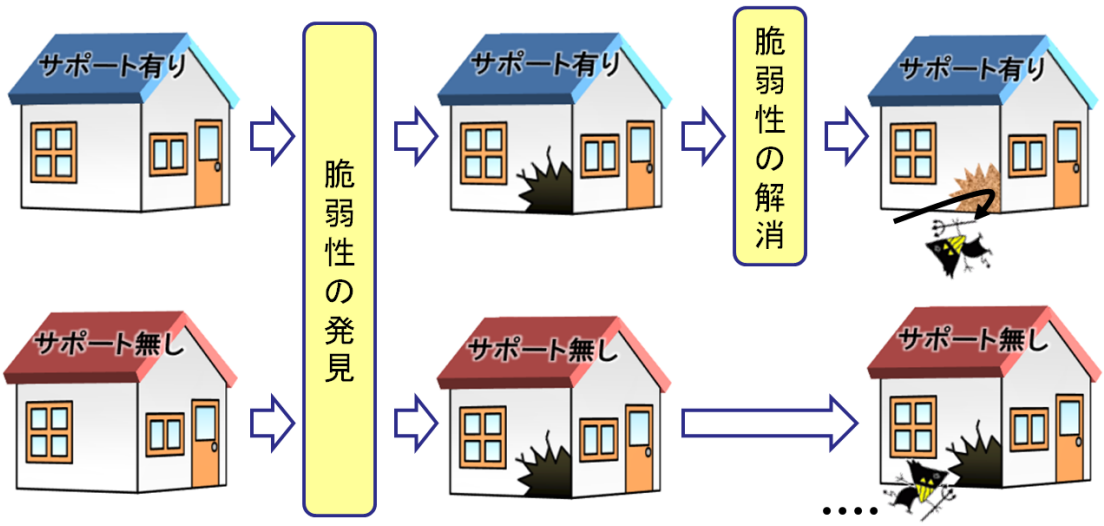


図 1-1：サポート終了 OS を家にたとえた場合のイメージ図

また、サポートが終了した OS 上で動作するアプリケーションソフトのサポートも終了していくという問題があります。特に、セキュリティ対策ソフトのサポートが終了すると、製造元から新種のウイルスに対応するためのパターンファイルが提供されなくなり、新たに発生したウイルスに対する防御力が低下してしまいます。

（2）サポート終了 OS の対処方法

Windows の利用者は、まず、OS のバージョンを以下の手順で確認し、次項で OS 毎の対処方法を参照してください。Mac OS 等の Windows 以外の OS の利用者は、製造元からのサポート情報を参照し、最新の状態にバージョンアップしてください。

【Windows のバージョン確認手順】
（i）「スタートボタン」→「ファイル名を指定して実行」をクリック
（ii）表示された画面に「winver」と入力して「OK」ボタンをクリック
（iii）「Windows のバージョン情報」のウィンドウが表示されます
※（i）で「ファイル名を指定して実行」メニューがない場合は、「スタートボタン」をクリックして表示される「プログラムとファイルの検索」、または「検索の開始」と表示されている入力欄に「winver」と入力し、Enter キーを押してください。

（a）Windows XP や Vista の場合

Windows XP や Vista は一部のバージョンでサポートが終了しますが、OS を最新のバージョンにすれば、マイクロソフト社によるサポートは継続します。以下の表 1-2 を参考に、OS が最新のバージョンになっているか確認し、最新でない場合は、Microsoft Update または Windows Update を実施し、最新の状態にしてください。

表 1-2：各 OS の最新バージョン

製品名	最新のバージョン（2010 年 7 月現在）
Windows XP	Service Pack 3
Windows Vista	Service Pack 2

（ご参考）
「Microsoft Update を使用してコンピューターを最新の状態に保つ」（マイクロソフト社）
http://www.microsoft.com/japan/protect/computer/updates/mu.mspx

（b）Windows 98/Me の場合

Windows 98/Me は 2006 年 7 月にマイクロソフト社によるサポートが終了していますので、(1）で示したようにこれらの OS を使い続けることは危険です。

特に、これらの OS が搭載されたパソコンをインターネットに接続して利用した場合、ウイルス感染などの可能性が高まりますので、インターネットへの接続は控え、できるだけ速やかに、最新の OS が搭載されたパソコンに買い換えることを勧めます。

（c）Windows 2000 Server / Professional の場合

Windows 2000（Server / Professional）については、2010 年 7 月 13 日（米国時間）にサポートが終了しますので、それ以降も使い続けることは、(1）で示した危険を伴うことになります。できるだけ速やかに、サポートが継続している OS に移行することを勧めます。

特に、Windows 2000 Server でインターネット上にサービスを提供している場合は、脆弱性を解消することができない危険な状態のまま、外部からの攻撃にさらされることになります。もしウイルス感染の被害を受けた場合、サービスの利用者にも被害が拡大してしまう可能性が高いので、最新の OS に移行する等の対応が急務といえます。

しかしながら、システムの移行作業に時間を要する場合や経済的理由など、サポートが終了しても早期に対応することが困難なケースも想定されます。その場合、一時的な回避策として、脆弱性を悪用する攻撃を防御するツールを利用する方法があります。このようなツールを使い、脆弱性を悪用する攻撃を防御しながら、移行作業の検討・実施を行うようにしてください。

なお、この回避策を実施しても脆弱性が根本的に解消されるわけではありませんので、あくまでもセキュリティ上のリスクを軽減するための手段であることを認識してください。

（ご参考）
「サポートが終了する Windows を利用しているシステム管理者への注意喚起」（IPA）
http://www.ipa.go.jp/about/press/20100705.html

最後に、サポートが終了した OS が搭載されたパソコンを利用することの危険性を認識した上で、どうしてもそのパソコンを使い続ける必要がある場合は、ウイルス感染や不正アクセスの被害を予防するために、**できる限りインターネットには接続しないこと**、また、**他のパソコンと USB メモリなどを介するデータのやり取りを行わないこと**を勧めます。

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、6 頁の「3.コンピュータ不正アクセス届出状況」を参照）
- “ガンブラー”の手口によるウェブサイト改ざん被害
- パスワード再発行の仕組みが悪用され、オンラインゲームのアカウントが乗っ取られた

○ 相談の主な事例 （相談受付状況および相談事例の詳細は、8 頁の「4.相談受付状況」を参照）
- 携帯電話をパソコンに接続したら、パソコンがウイルス感染した！？
- 家族のためを思って有害サイトを調べていたら、自分がワンクリック不正請求の罠に・・

○ インターネット定点観測（10 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

6 月のウイルスの検出数（※1）は、**約 4.1 万個**と、5 月の約 5 万個から 18.8%の減少となりました。また、6 月の届出件数（※2）は、**1,245 件**となり、5 月の 1,084 件から 14.9%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 4.1 万個を集約した結果、1,245 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 3.3 万個**、2 位は **W32/Mydoom** で**約 4 千個**、3 位は **W32/Autorun** で**約 1 千個**でした。

ウイルス検出数 約4.1万個（約5.0万個） 前月比－18.8%

（注：括弧内は前月の数値）

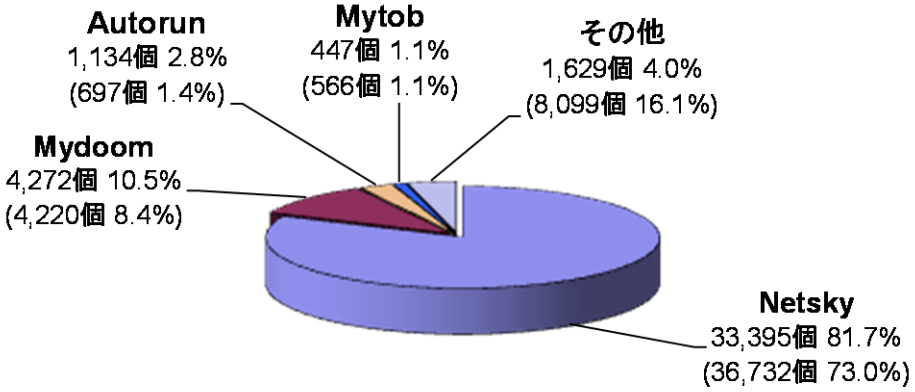


図 2-1：ウイルス検出数

ウイルス届出件数 1,245件（1,084件）前月比 ＋14.9%

（注：括弧内は前月の数値）

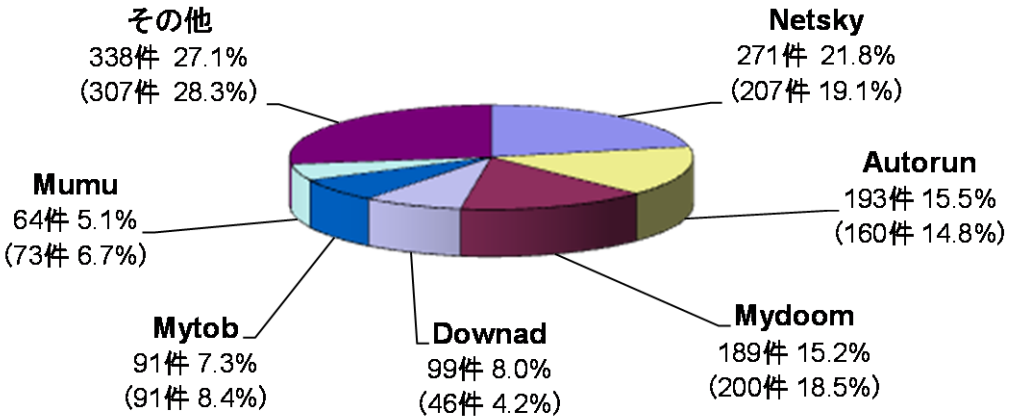


図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

2010 年 6 月の不正プログラムの検知状況では、ADCLICKER の検知数が急増したことが確認されました。（図 2-3 参照）。

ADCLICKER とは、一般的に、ホームページ上の広告を自動的にクリックする動作を行うものです。この動作が行われても、パソコンの画面上にホームページが表示されることはありませんので、パソコンの利用者は気付かないと推測されます。ただし、複数の亜種があり、パソコン画面上に広告を表示させるタイプもあります。

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いため、感染を防止するために、添付ファイルの取り扱いには常に注意を払う必要があります。また、不正プログラムの配信には、ボット※1 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※2 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/

※1　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。

※2　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/

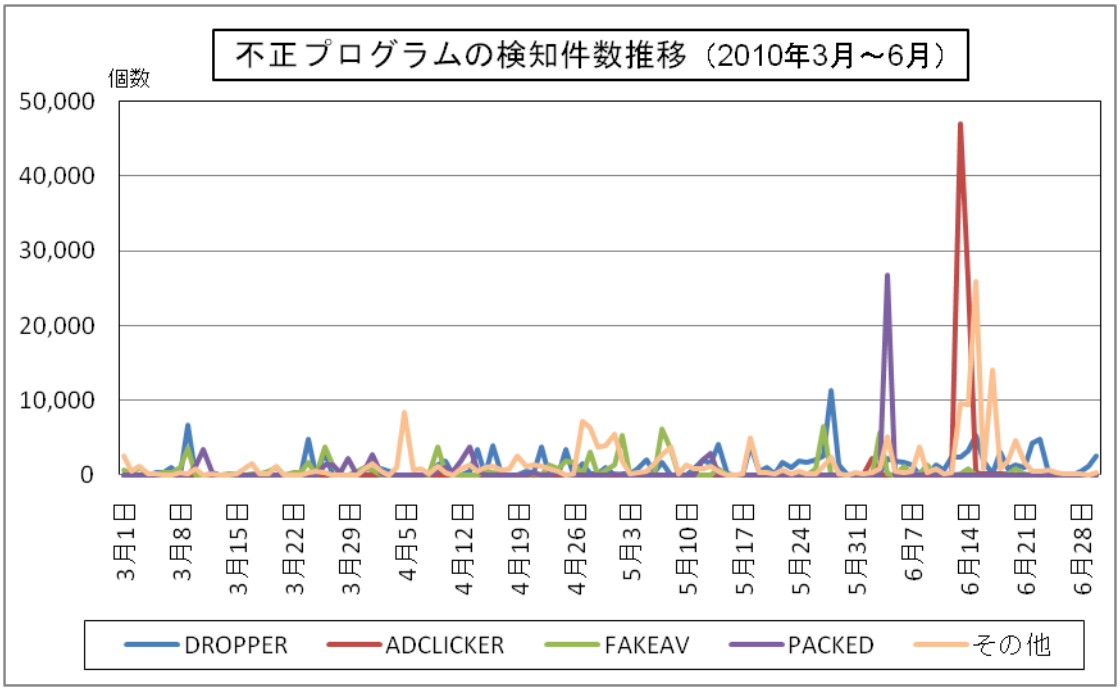


図 2-3：不正プログラムの検知件数推移

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

		1月	2月	3月	4月	5月	6月
届出(a) 計		20	27	19	11	8	15
	被害あり(b)	12	17	13	10	5	13
	被害なし(c)	8	10	6	1	3	2
相談(d) 計		67	47	60	39	52	77
	被害あり(e)	34	28	23	16	22	50
	被害なし(f)	33	19	37	23	30	27
合計(a+d)		87	74	79	50	60	92
	被害あり(b+e)	46	45	36	26	27	63
	被害なし(c+f)	41	29	43	24	33	29

（1）不正アクセス届出状況

6 月の届出件数は 15 件であり、そのうち何らかの被害のあったものは 13 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 77 件（うち 8 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 50 件でした。

（3）被害状況

被害届出の内訳は、**侵入 3 件、なりすまし 9 件、その他（被害あり）1 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 3 件（全て不正なコードの挿入）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 3 件でした。

「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 9 件）でした。

（4）被害事例

［侵入］

（i）“ガンブラー”の手口によるウェブサイト改ざん被害

事例	・レンタルサーバでウェブサイトを運用している。ある日、サイト閲覧者から「サイトを見るとウイルスが検知される」との通報があった。 ・ウェブサイトのコンテンツを調査したところ、HTML ソースに、悪意あるサイトへ誘導するためのスクリプトが挿入されていることが判明。 ・さらなる調査の結果、ウェブページ更新用に使用していたパソコンがウイルスに感染しており、ftp のアカウント情報が盗まれたものと断定。 ・盗まれた ftp アカウントでウェブサーバに不正アクセスされ、ウェブページ改ざん行為が行われていた。 ・ウイルスに感染していたパソコンは社員自宅にあった、私物だった。
解説・対策	ガンブラーによるウェブサイト改ざん被害は、今でも多くの発見報告が IPA に寄せられています。今回の事例では、会社のウェブページ更新に私物パソコンが使われていたことが問題であると言えます。今後の対応として、「**ftp アクセスの制限**」と「**ウェブサイト更新専用パソコンの導入**」は特に有効でしょう。 （参考） 2010 年 4 月の呼びかけ「ウェブサイトの管理方法を再確認しましょう！」 http://www.ipa.go.jp/security/txt/2010/04outline.html

［なりすまし］

（ii）パスワード再発行の仕組みが悪用され、オンラインゲームのアカウントが乗っ取られた

事例	・オンラインゲームサイトにログインできなくなったため、パスワードを再発行すべく、あらかじめ登録してあるメールアドレス宛に新しいパスワードを送ってもらった。このメールアドレスは、あるフリーメールサービスのもの。 ・改めてオンラインゲームにログインしてみたところ、一部アイテムと全てのゲーム内通貨が無くなっていることに気付いた。 ・調査したところ、フリーメールサービスに、身に覚えのないログイン履歴があったことから、何者かがパスワード再発行手続きのために、フリーメールに不正アクセスしたものと推測。 ・ログイン ID とパスワードは、フリーメールサービスとオンラインゲームとで、全く異なる文字列を使用していた。なぜ破られたのか、全く見当がつかない。
解説・対策	オンラインゲームサイトのパスワード再発行の仕組みが悪用された例です。フリーメールサービスのパスワードがどうやって破られたのかは分かりませんが、**ログインしたタイミングでお知らせメールを送信する機能が提供されているフリーメールサービスを利用すれば、自分以外の誰かがログインした際にお知らせメールが届き、被害を未然に防ぐことができます**。 （参考） IPA -「ID とパスワードを適切に管理しましょう」 http://www.ipa.go.jp/security/txt/2010/03outline.html

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 **1,983 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 **755 件**（5 月：637 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 **7 件**（5 月：27 件）、**Winny に関連する相談**が **2 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：4 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		2,150	1,789	2,000	2,110	1,881	1,983
	自動応答システム	1,160	977	1,057	1,194	1,091	1,022
	電話	910	736	846	835	714	829
	電子メール	78	70	92	81	76	129
	その他	2	6	5	0	0	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。

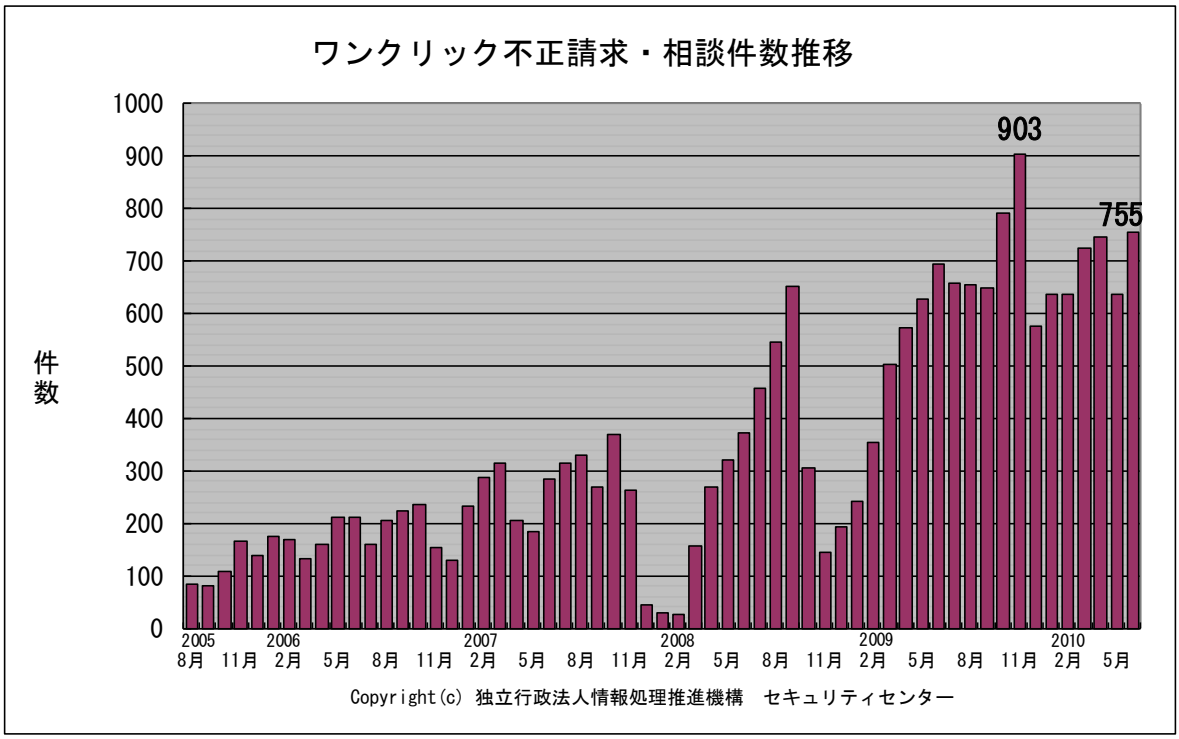


図 4-1：ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

（i）携帯電話をパソコンに接続したら、パソコンがウイルス感染した！？

相談	パソコンから携帯電話を充電しようとして、USB ケーブルで接続したところ、携帯電話のメモリカードにウイルスが感染していたため、パソコンにもウイルス感染してしまった。同じようにデジタルオーディオ機器やゲーム機からでも、感染する可能性はあるのか。
回答	このメモリカードは、USB 感染型ウイルスに感染していたようです。どのようにして、携帯電話のメモリカードにウイルスが感染したのかは不明ですが、**パソコンと USB ケーブルなどで接続され、外部記憶媒体として認識されるものであれば、USB 感染型ウイルスの感染先、もしくは感染元になる可能性はあります。**ウイルスに感染したメモリカードなどは、フォーマットを行い、中身を全て消去してから使用してください。**大事なデータが入っているパソコンには、管理されていない USB メモリなどの外部記憶媒体を安易に接続しない**ことが一番です。**接続されるパソコン側では、ウイルス対策ソフトなどの使用や、接続した際にウイルスが勝手に起動しないように Windows の「自動実行機能」を無効**にする、などの対策を行ってください。 （参考） サイバークリーンセンター – USB 感染型ウイルスとは https://www.ccc.go.jp/detail/autorun/ IPA - Windows での「自動実行」機能の無効化手順 http://www.ipa.go.jp/security/virus/autorun/

（ii）家族のためを思って有害サイトを調べていたら、自分がワンクリック不正請求の罠に・・

相談	【例 1】学生の孫がいるので有害なサイトは見せたくない。だが有害サイトとはどのようなものなのか判らない。自分で調べていると、アダルトサイトの入会手続き完了となってしまい、請求画面が表示されるようになり、消去できない。 【例 2】息子が怪しいサイトを見ていないか、インターネットの閲覧履歴を調べていたら、間違ってアダルトサイトに登録してしまい、請求画面が表示されるようになった。
回答	どちらも家族を思っての行動ですが、結局はアダルトサイトに誘導され、ページに書かれている内容を自分でキチンと確認しないまま、ワンクリック不正請求サイトで「はい」ボタンを複数回クリックして先に進み、ワンクリック不正請求の被害に遭っています。**サイトの検証をされる場合、まずは好奇心を抑えた上で、画面上にでてくる確認メッセージなどはよく読み、先に進むかの判断をしてください。** **なお、未成年者がいる家庭では、有害サイトのブロックが有効です。具体的には、ウェブフィルタリングソフト／URL フィルタリングソフトの利用や、有害サイトをブロックする機能を持つ統合型セキュリティ対策ソフトの使用、プロバイダによる有害サイトブロックサービスの利用、が該当します。** （参考） IPA – ワンクリック不正請求に関する注意喚起 http://www.ipa.go.jp/security/topics/alert20080909.html

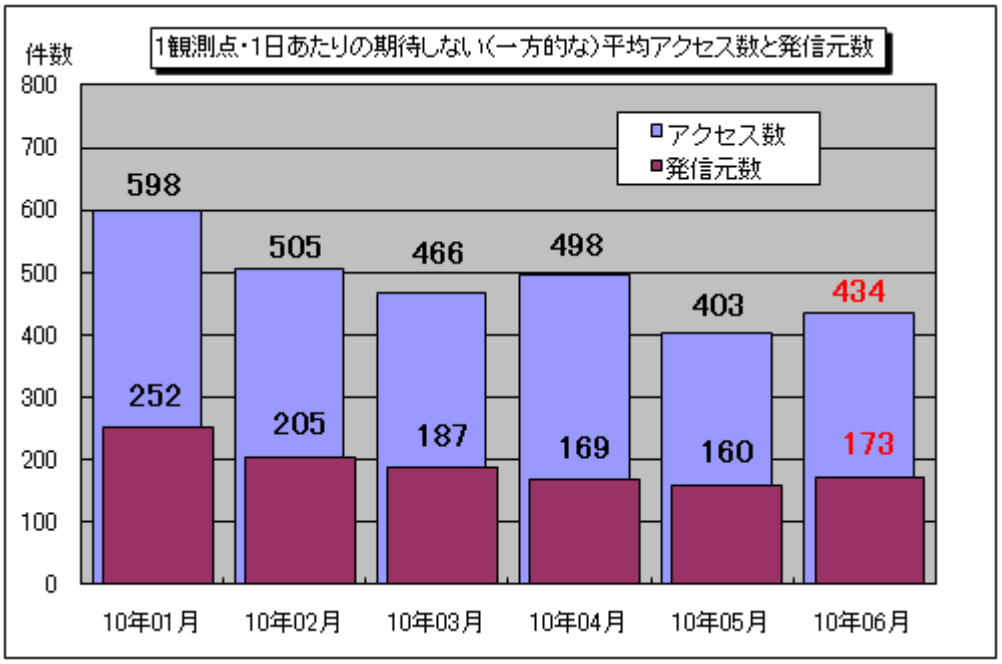
5. インターネット定点観測での 6 月のアクセス状況

インターネット定点観測（TALOT2）によると、2010 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 **117,157 件**、延べ発信元数 (※) は **46,800 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 173 の発信元から 434 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。

※6 月 18 日～20 日は、保守作業のため、システムを停止しています。そのため、6 月の観測データは、この 3 日間を除外して統計情報を作成しています。なお、通常は常時稼働しています。

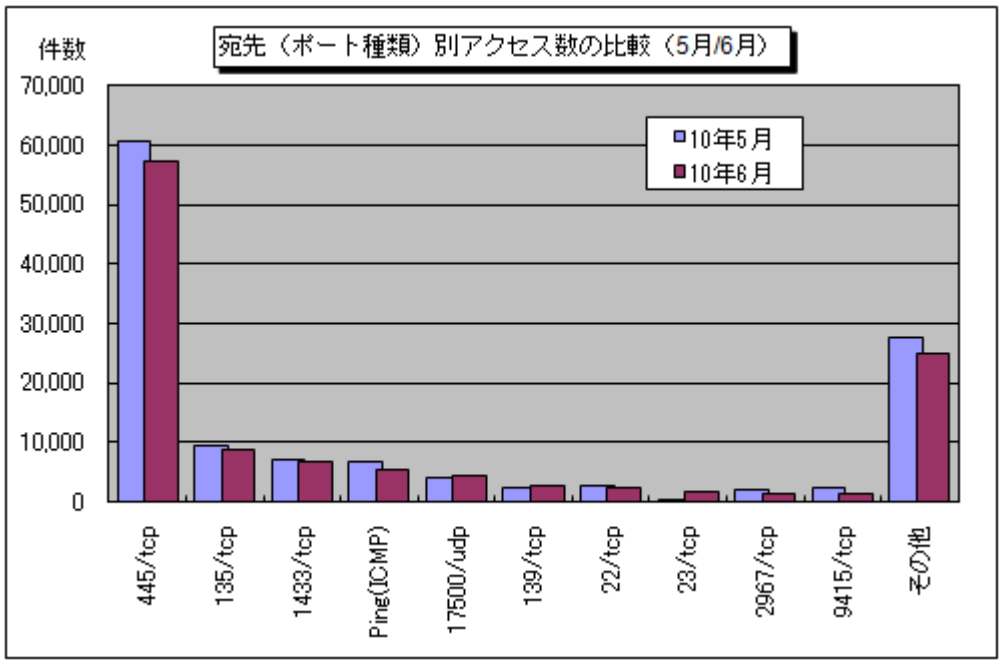


【図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数】

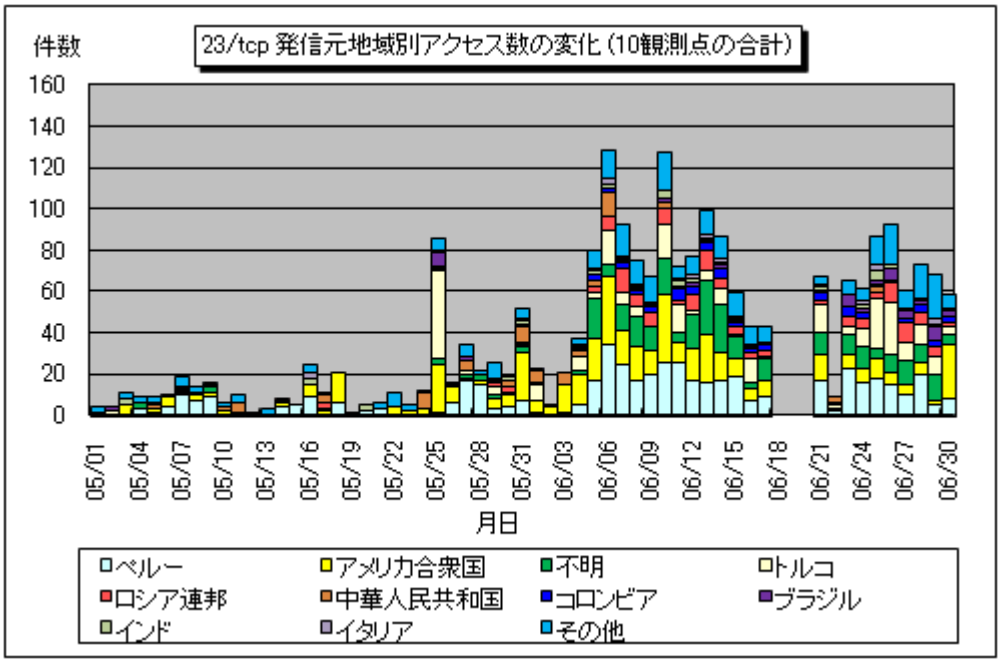
2010 年 1 月～2010 年 6 月までの各月の 1 観測点・1 日あたりの平均アクセス数とそれらのアクセスの平均発信元数を図 5-1 に示します。6 月の期待しない（一方的な）アクセスは、5 月と比べて増加しました。

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。これをみると、5 月に比べ特に増加が観測されたのは 23/tcp へのアクセスでした。

このアクセスは 5 月下旬から TALOT2 の複数の観測点で増加しており、発信元はペルー、アメリカ等海外の多数の箇所でした（図 5-3 参照）。23/tcp は一般的に telnet で使用されるポートですが、今回アクセスが増加していた原因は不明です。また、定点観測を行っている他の組織においても同様の増加傾向が見られていたことから、広い範囲でこの現象が発生していたと思われます。



【図 5-2：宛先（ポート種類）別アクセス数の比較（5 月/6 月）】



【図 5-3：23/tcp 発信元地域別アクセス数の変化（10 観測点の合計）】

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/TALOT2-1007.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