プレスリリース
第 09-10-146 号
2009 年 4 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 [2009 年 3 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 3 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

「“セキュリティの警告”画面を知っていますか？」
― そこには被害に遭わないためのヒントが書かれています ―

IPA に寄せられる「ワンクリック不正請求」に関する相談件数は、2008 年 9 月の 651 件をピークに一時減少しましたが、最近 4 カ月では再び急激に増加しています(図 1-1 参照)。3 月には、**「ワンクリック不正請求」の累計相談件数が 10,000 件を突破**しました。

増加した要因の 1 つとして、新たな手口を利用するサイトが複数現われたことが挙げられます。新たな手口では、パソコンの設定が改ざんされてしまうため、完全に元の状態に戻すことが困難になります。

このような手口を利用するサイトは今後も増加する可能性がありますが、予防対策は従来から変わりません。Windows が表示する“セキュリティの警告”画面やそのメッセージの意味を確認し、被害に遭わないように注意してください。

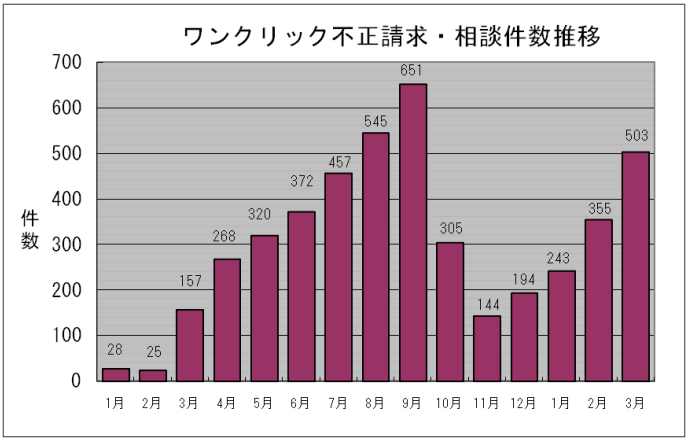


図 1-1：ワンクリック不正請求の相談件数推移

(1)「ワンクリック不正請求」とは

「ワンクリック不正請求」とは、アダルトサイトで動画を観ようと画像をクリックして次へ次へと進んで行った利用者に対し、悪意ある者が本人の意思に反して会員登録し料金を請求する手口です。アニメやゲームなど、アダルト以外のサイトから誘導されることも多く、年齢・性別を問わず、多くの相談が寄せられています。

(a) 従来の手口

不正請求を行うサイトにアクセスし、[無料]や[サンプル]といったボタンを押すと、料金の請求画面を表示する、ウイルスなどの悪意のあるプログラム(exe 形式)がダウンロード、インストールされます。その結果、パソコンを起動すると当該プログラムが自動実行され、毎回、請求画面が表示されるようになってしまいます。(パソコンがインターネットに接続されていなくても請求画面が表示されます。)

この場合の対処方法は、インストールされたプログラムを削除することです。ウイルス感染後であっても、概ね、ウイルス対策ソフトで対応が可能です。

(b) 新たな手口

2 月頃に現れた新たな手口は、従来のように悪意のあるプログラム(exe 形式)をインストールすることなく、そのプログラムがパソコンの設定を改ざんすることで、パソコンの起動時にウェブブラウザを利用してインターネット上のアダルトサイトに勝手に接続し、

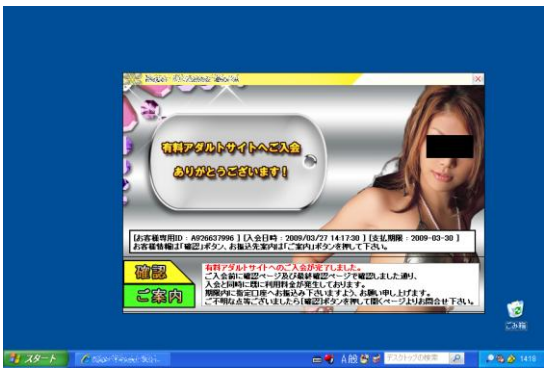


図 1-2：新たな手口で表示された、消せない画面の例

請求画面を表示させるというものです。

この手口でウェブブラウザに表示された請求画面は、右上の×ボタンで閉じたり、画面の端に移動したりといった操作ができない仕掛けになっており、表示を止めることができません(図 1-2 参照)。
この場合、ウイルスがパソコン内に潜んでいる訳ではないため、**症状が出てしまうと、現状のウイルス対策ソフトでは対応できません。**

実際に行う対処方法は、ウェブブラウザでアダルトサイトに勝手に接続するように設定された命令を解除することです。そのためには、「システム構成ユーティリティ」(※1)を利用して、追加されたスタートアップ項目を解除します。こうすることで、パソコン起動時に、アダルトサイトに接続させられることはなくなります。ただし、完全に設定情報を元に戻すためには、システム設定データ(レジストリ)を編集する必要がありますが、このデータに対して誤った編集を行うと、必要なプログラムが起動しなくなる危険があります。

このように、一度被害に遭ってしまうと、完全に復旧するためには専門的な知識が必要になるなど、対処することは非常に困難です。

※1　Windows のシステム構成の問題を診断、修復するためのソフトウェア。これを用いてシステム構成を変更することで、Windows 起動時に悪意あるプログラムが自動起動される設定を解除することができる。但し、Windows 2000 には装備されていない。

(2) 対策

(a) 予防策

被害に遭わないための対策は、Windows の機能である“ファイルのダウンロード-セキュリティの警告”画面に表示された内容をよく読み、安易に[実行]ボタンを押さないことです(図 1-3 参照)。
この“警告”画面は、画像や動画を再生するときに表示されるものではありません。悪意がある可能性のあるプログラムをパソコンに取り込もうとしていることを警告する画面です。ホームページを閲覧しているとき、この警告画面が表示されたら[キャンセル]ボタンを押して、悪意のあるプログラムを取り込まないようにしてください。

ただし、悪意のあるプログラムではないと判断できた場合でも、ソフトウェアをダウンロードする際は[保存]を選択してダウンロードし、ウイルス対策ソフトで検査してから開く(実行する)ようにしてください。

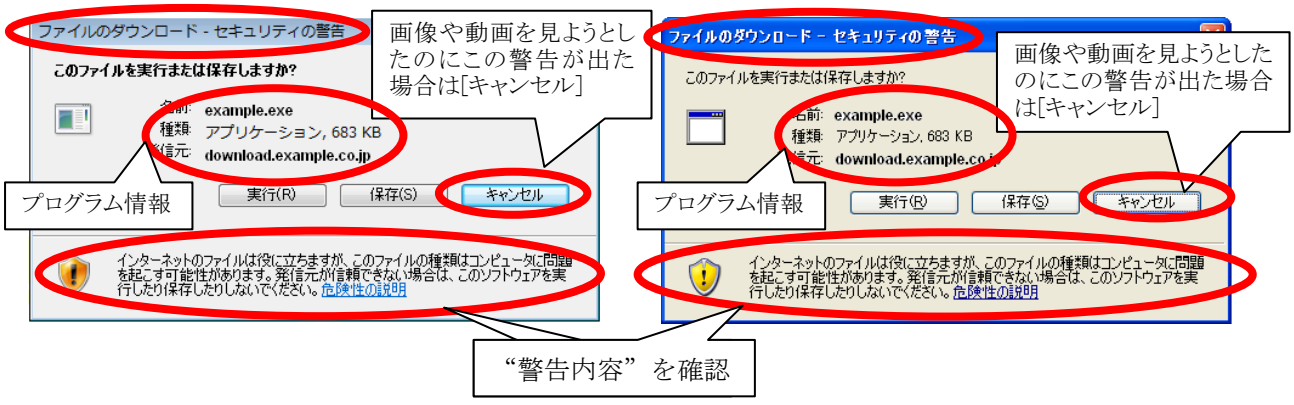


図 1-3：Internet Explorer の“セキュリティ警告”画面の例

被害が報告されたウェブサイトの中には、図入りの説明を用意し、言葉巧みに“セキュリティの警告”画面で[実行]ボタンをクリックさせるように仕向けるなど、手口が巧妙になっている事例が確認されました(図 1-4 参照)。ウェブサイトの説明を鵜呑みにせず、メッセージ等をよく読んで、少しでもおかしいと感じたらそこから先には進まないようにしてください。

例えば、今回の事例とは直接関係ありませんが、IPA に寄せられた相談事例では、「アダルトサイトの入口ページに『利用料金が発生する』旨の案内が記載されているにも関わらず、よく読まなかった」、「『どうせ嘘だろう』と軽く考えてクリックして先に進んで行ったあげく、請求画面が表示されるようになってしまった」というものが大多数を占めていました。ウェブサイトに記載された注意事項などをよく確認していれば被害は未然に防止できますので、利用者はクリックする前に十分注意してください。(図 1-5 参照)。

図 1-4：[実行]をクリックさせるための説明画面

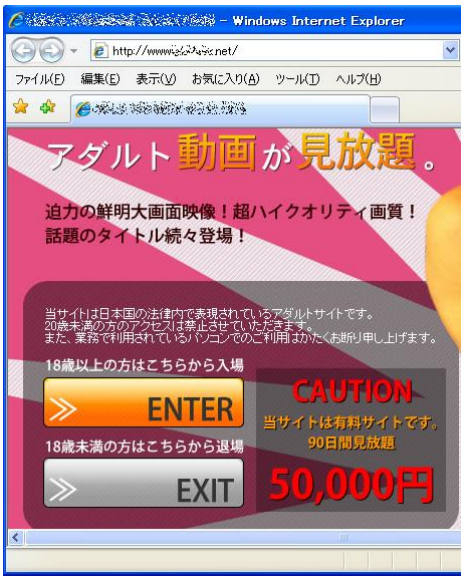


図 1-5：サイトの入口にある料金表示例

(b) 事後対策

Windows XP や Windows Vista には、システムの復元機能があります。この機能を利用し、料金請求画面が表示される前の状態にシステムを復元することで解決できます。

（ご参考）

「システムの復元のやり方」（マイクロソフト社）

http://www.microsoft.com/japan/windowsxp/pro/business/feature/performance/restore.mspx

システムの復元が正常に完了しない場合は、システム設定データ(レジストリ)を編集する方法もありますが、操作を誤るとパソコンが起動しなくなる危険があります。知識がない(自信がない)場合は、編集しないようにしてください。

なお、対処方法がわからない場合は IPA にご連絡ください。以下の窓口にて電話対応しておりますので、パソコンを操作できる状態でご相談ください。

コンピュータウイルス 110 番

電話番号：03-5978-7509 (24 時間自動応答、ただし相談員による
相談受付は休日を除く月～金の 10:00～12:00、13:30～17:00 のみ)

(ご参考)

「ワンクリック不正請求に関する注意喚起」(IPA)

http://www.ipa.go.jp/security/topics/alert20080909.html

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、5 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で侵入されたようだが・・
・侵入され、ホームページのデータが消去された

○ 相談の主な事例 (相談受付状況及び相談事例の詳細は、7 頁の「4.相談受付状況」を参照)
・インターネット上に自分の作ったデータが流出？
・Windows 98 や Me で使えるウイルス対策ソフトはあるか

○ 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 11.9 万個**と、2 月の約 12.8 万個から 7.7%の減少となりました。
また、3 月の届出件数(※2)は、**1,674 件**となり、2 月の 1,463 件から 14.4%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。
・3 月は、寄せられたウイルス検出数約 11.9 万個を集約した結果、1,674 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 10.5 万個** 、2 位は **W32/Mytob** で**約 5 千個**、3 位は **W32/Mydoom** で**約 3 千個**でした。

ウイルス検出数　約11.9万個（約12.8万個）　前月比－7.7%
（注：括弧内は前月の数値）

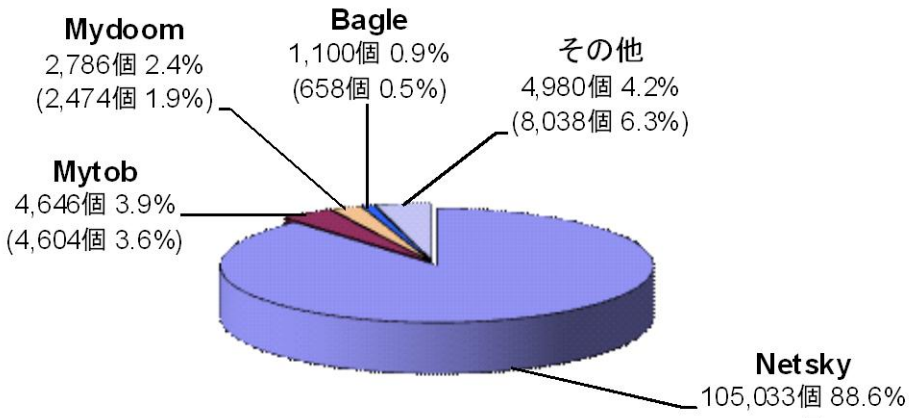


図 2-1：ウイルス検出数

ウイルス届出件数　1,674件（1,463件）前月比 ＋ 14.4%
（注：括弧内は前月の数値）

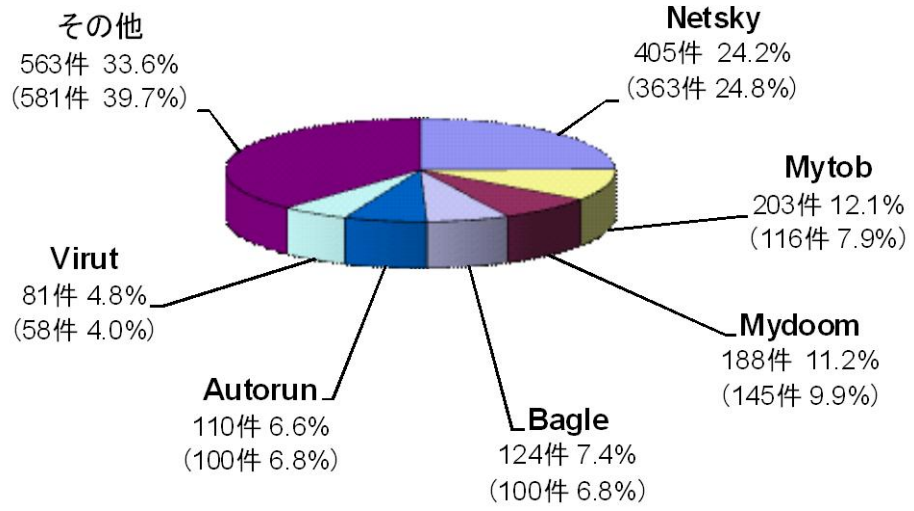


図 2-2：ウイルス届出件数

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

		10月	11月	12月	1月	2月	3月
届出(a) 計		**17**	**18**	**10**	**10**	**9**	**20**
	被害あり(b)	12	12	7	7	6	13
	被害なし(c)	5	6	3	3	3	7
相談(d) 計		**58**	**39**	**38**	**29**	**35**	**40**
	被害あり(e)	22	19	19	13	14	11
	被害なし(f)	36	20	19	16	21	29
合計(a+d)		**75**	**57**	**48**	**39**	**44**	**60**
	被害あり(b+e)	34	31	26	20	20	24
	被害なし(c+f)	41	26	22	19	24	36

(1)不正アクセス届出状況

3 月の届出件数は 20 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 40 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 11 件でした。

(3)被害状況

被害届出の内訳は、**侵入 4 件、不正プログラム埋込 9 件、**でした。

「侵入」の被害は、SQL※インジェクション※攻撃を受け、サーバ上でコマンドを実行されたものが 1 件、他サイト攻撃の踏み台として悪用されたものが 2 件、ウェブサーバ内のコンテンツデータが消去されたものが 1 件、でした。侵入の原因は、脆弱性を突かれたことによるものが 1 件、SSH※で使用するポートへのパスワードクラッキング※攻撃と思われるものが 1 件、その他のパスワードクラッキング攻撃と思われるものが 1 件、でした(残りの 1 件は原因不明)。

※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。
※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) SQL インジェクション攻撃で侵入されたようだが・・

事例	・IPA の SQL インジェクション検出ツール「iLogScanner」でログをチェックしたところ、攻撃が成功していたと思われる形跡が数万件検知された。半年も前から、攻撃が続いていたようだ。 ・しかし、組織の幹部はこの事実を公にしない方針らしく、さらなる調査を進めることができない。 ・とりあえず、データベースを使ったコンテンツ公開は停止し、ウェブアプリケーションの見直しを開始した。
解説・対策	データベースをウェブサイトのコンテンツとしてそのまま利用している場合、**SQL インジェクション攻撃によってデータベース内データを改ざんされると、サイトを閲覧しに来た一般のパソコンユーザが被害に遭う場合があります**。まずは不正アクセス被害の全貌を調査し、影響範囲を明らかにすることが最優先です。**被害状況の把握や復旧には専門的な知識や技術が必要になりますので、自組織での対応が無理な場合は、情報セキュリティの専門企業へ調査を依頼しましょう**。万が一、不正アクセスの影響が組織の外部にまで及んでいる恐れがある場合は、その事実内容や対応方法を告知することが望まれます。 組織の幹部には、脆弱性の内容や、脆弱性が原因となって起こる問題点を説明し、二次被害が生じないような対策をとるべく、協力を求めると良いでしょう。次の資料を参考にしてください。 (参考) IPA -知っていますか？脆弱性 (ぜいじゃくせい) http://www.ipa.go.jp/security/vuln/vuln_contents/ IPA - ウェブサイト運営者のための脆弱性対応ガイド http://www.ipa.go.jp/security/fy19/reports/vuln_handling/ IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html

(ii) 侵入され、ホームページのデータが消去された

事例	・自社のウェブサイトのページが表示されなくなったため調査したところ、サーバ上のホームページ用のディレクトリが消去されていたことが判明。 ・ログをチェックしたところ、管理用以外の IP アドレス(海外)からのアクセス痕跡が認められた。 ・セキュリティ対策のため、システム設定の変更や IDS※の導入作業の途中であった。
解説・対策	システム設定変更などの作業中に、一時的にセキュリティが弱くなる状態があったのかもしれません。作業は、一旦全てのサービスを停止し、オフライン状態で実施するのが理想です。もしくは作業中だけでも、外部からのログインを禁止するなどの措置が有効でしょう。 (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

※IDS (Intrusion Detection System)： システムに対する侵入／侵害を検出・通知するシステムのこと。

4. 相談受付状況

3 月の相談総件数は **1406 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 **503 件**(2 月：355 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 **3 件**(2 月：17 件)、**Winny に関連する相談**が **6 件**(2 月：7 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**(2 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

		10月	11月	12月	1月	2月	3月
合計		1,171	713	839	960	1,051	1,406
	自動応答システム	677	363	458	529	521	758
	電話	441	288	331	390	472	597
	電子メール	47	62	49	39	57	49
	その他	6	0	1	2	1	2

※ 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。

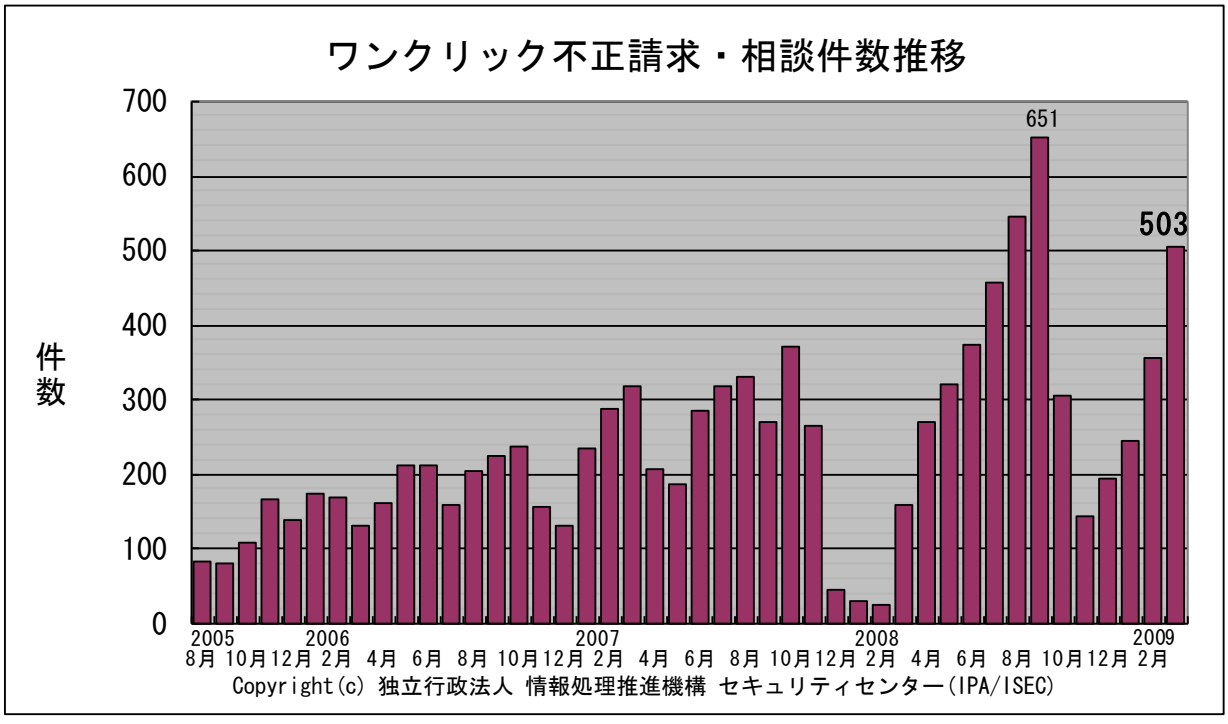


図 4-1　ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

(i) インターネット上に自分の作ったデータが流出？

相談	Google で情報を検索していたら、自分が作成したと思われる名簿ファイルや日記ファイルがヒットした。ウイルスに感染して、パソコンからデータが流出したのか？
回答	**パソコン内のデータが、検索結果に表示されている可能性があります**。「Google デスクトップ」というアプリケーションがインストールされているのではないでしょうか。このアプリケーションが入っていると、情報検索の際、パソコン内も検索範囲になります。最近では、購入時からプリインストールされていることもあります。コントロールパネルから、パソコン内にインストールされているプログラム一覧を確認することができます。

(ii) Windows 98 や Me で使えるウイルス対策ソフトはあるか

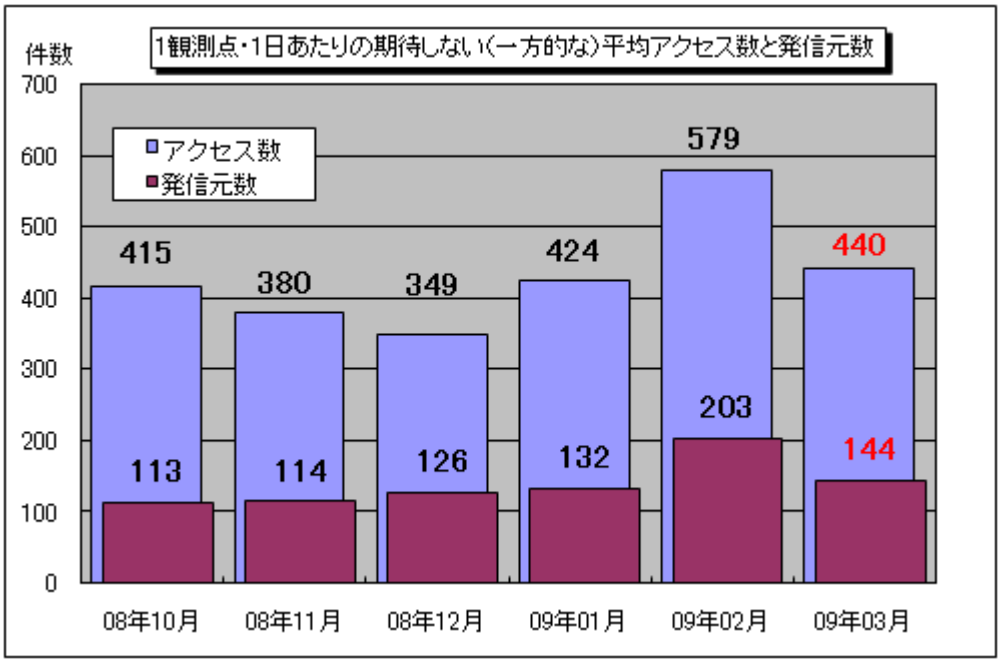
相談	メールを送受信したり、ちょっとホームページを見るくらいしかパソコンを使わないので、今でも Windows 98 を使い続けている。ウイルスが心配なのでウイルス対策ソフトを入れようと思うが、ソフト販売店には売っていなかった。どうすれば良いか。
回答	**Windows 98 や Me は、セキュリティ上の問題が解決されませんので、今後の利用はお勧めしません。既にマイクロソフトによるサポートが終了しており、脆弱性が発見されても修正プログラムは提供されない**ためです。脆弱性の種類によっては、パソコンをインターネットにつないでいるだけで、ウイルスに感染してしまう場合があります。**悪意のあるサイトを閲覧しただけで、ウイルスに感染してしまう場合もあります**。セキュリティ対策の基本は、脆弱性の解消です。逆に言えば、**脆弱性を解消していなければ、他にどんな対策をしていても片手落ちになる**ということです。 **「インターネットにつながないから問題無いでしょう」という意見もありますが、安全とは言えません**。最近は USB メモリを介してデータ交換をする機会が多くなっており、USB メモリを媒介として感染を広げるウイルスが多く出回っているためです。 (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

5. インターネット定点観測での 3 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 3 月の期待しない(一方的な)アクセスの総数は 10 観測点で **136,437 件**、総発信元(※)は **44,646 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 144 の発信元から 444 件のアクセスがあった**ことになります(図 5-1)。

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。



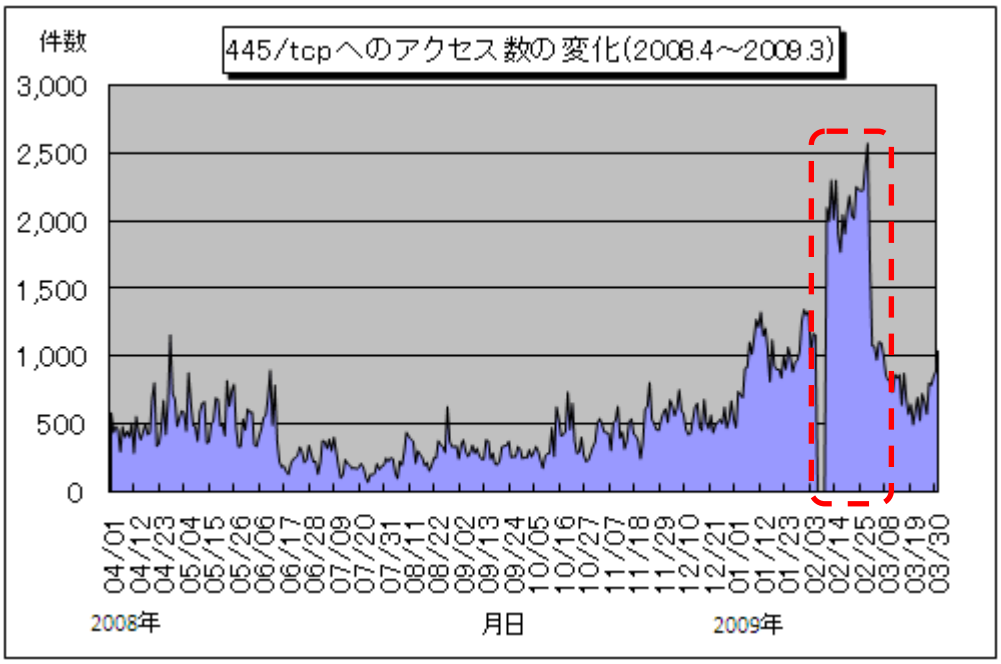
【図 5-1 1 観測点・1 日あたりの期待しない(一方的な)平均アクセス数と発信元数】

2008 年 10 月～2009 年 3 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。3 月の期待しない(一方的な)アクセスは 2 月と比べて大幅に減少しました。

(1) 445/tcp へのアクセス

2 月と比較して 3 月は 445/tcp へのアクセスが大幅に減少しましたが、過去 1 年間を通してみると、2 月はアクセス数が特別多かったに過ぎず、3 月は 2 月より前の水準に戻ったと言えます (図 5-2 参照)。

445/tcp へのアクセスが 2 月に増加したタイミングはメンテナンスによるシステムの停止がきっかけでしたが､3 月に減少したタイミングも不定期に行っている TALOT2 の観測点の変更がきっかけでした。それぞれのタイミングで 445/tcp へのアクセス数が大きく変化したことについて、本質的な要因は特定できておりません。



【図 5-2 445/tcp 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/2009/documents/TALOT2-0904.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