INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
第 09-20-153 号
2009 年 6 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 5 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 5 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

「新型インフルエンザの注意喚起に便乗したコンピュータウイルスに注意！」
― 情報の信憑性を確かめよう ―

4 月の終わり頃から、新型インフルエンザが世界中で猛威を振るっていますが、この新型インフルエンザに関する情報提供を装って、コンピュータウイルスに感染させようとする手口が広まっています。IPA に寄せられた相談の中には、実在する研究機関を騙った偽の注意喚起メールにウイルスを添付し、パソコンに感染させようとする事例もありました。

今回のように、世界中で注目されているニュース報道の直後や、オリンピックやクリスマス、バレンタインなどの行事の直前には、それに便乗してウイルスを感染させようとする手口が多く発生します。

このようなウイルスによる感染被害に遭わないためには、自分の身に覚えのないメールの添付ファイルは開かないことが鉄則です。さらに、知り合いから届いたように見えるメールの添付ファイルであっても、不自然さが感じられる場合は念のため相手に確認してから開くようにするなど、より慎重に対応するようにしてください。

（1）新型インフルエンザの注意喚起に便乗した手口の概要

今回の手口には、次の 2 つの事例が確認されています。

（a）SEO ポイズニング（Search Engine Optimization Poisoning）

SEO とは、検索キーワードを基に、検索結果として選ばれたウェブサイトの表示順位を向上させる工夫のことです。

この手口は、検索サイトから Swine（豚）と言う検索キーワードを入力して検索を行うと、その検索結果の上位に表示されるウェブサイトの一覧の中に、悪意あるウェブサイトを紛れさせるというものです。（通常は、利用者が興味のある言葉や流行語などが検索キーワードになります。今回の手口は、新型インフルエンザが流行したことにより、Swine（豚）がキーワードとして使われました。） 利用者は、そのリンク先をクリックすることにより、悪意あるウェブサイトに誘導され、ウイルス感染の脅威にさらされてしまいます。これは、”検索結果の上位サイトをクリックしがち”、”検索結果の上位サイトは安全なサイトだと思いがち”という、利用者の心理を突いた手口と言えます。

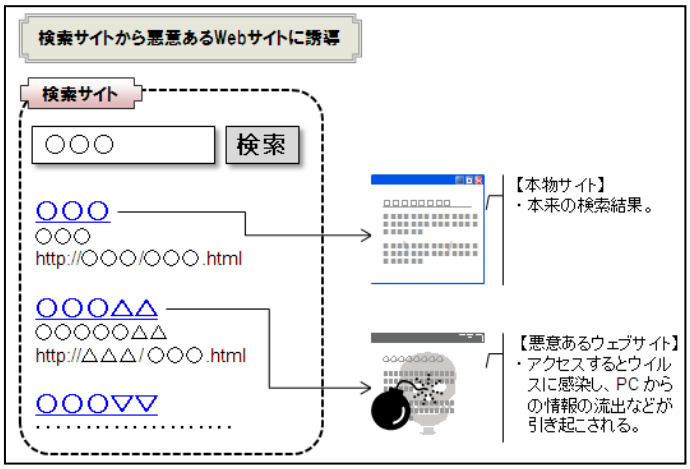


図 1-1：検索サイトから悪意あるウェブサイトに誘導

（ご参考）
「情報セキュリティ白書 2008 第 2 部 10 大脅威」（IPA）
第 7 位 検索エンジンからマルウェア配信サイトに誘導
http://www.ipa.go.jp/security/vuln/20080527_10threats.html

（b）偽の注意喚起メールからウイルスに感染

この手口は、冒頭でも説明したとおり、実在する研究機関の名前や架空組織の名前を騙り、新型インフルエンザの注意喚起情報に見せかけたファイル（今回は PDF [Portable Document Format] ファイルを添付ファイルに使用していることを確認しています）を添付したメールを送り、添付ファイルを開かせることによって、アプリケーションソフトの脆弱性（ぜいじゃくせい）を突いてウイルスを感染させようとするものです。実在する研究機関の名を騙って送信している点はとても悪質ですし、何らかの情報を詐取する意図が感じられます。

このようなメールの中には、添付ファイルを開かせるのではなく、メール本文内に書かれているリンクをクリックさせることによって悪意あるウェブサイトに誘導し、ウイルス感染の被害に遭わせようとするものもあります。

図 1-2：偽のメールからウイルスに感染

（ご参考）
「情報セキュリティ白書 2009 第 2 部 10 大脅威」（IPA）
総合第 3 位 巧妙化する標的型攻撃
http://www.ipa.go.jp/security/vuln/10threats2009.html

（2）偽の注意喚起メールに添付されていたウイルスの概要

今回、実際に出回っていた偽の注意喚起メールを IPA で入手し、添付ファイルの解析を行い検出したウイルスについて、以下の動作を確認しました。

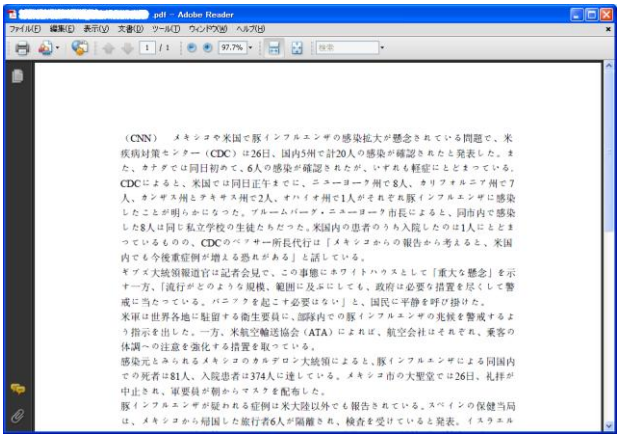
・Trojan.Pidief.C

このウイルスは、PDF ファイルを閲覧するためのアプリケーションソフト、Adobe Reader または Adobe Acrobat の脆弱性を突いて、Windows パソコンに感染するウイルスです。ただし、最新版の Adobe Reader、Adobe Acrobat （Reader、Acrobat 共に、2009 年 5 月現在の最新バージョンは 9.1.1 です）では当該脆弱性が解消されているため感染しません。

（ご参考）
「JVNDB-2009-001131 Adobe Reader および Adobe Acrobat における任意のコードが実行される脆弱性」（JVN iPedia 脆弱性対策情報データベース）
http://jvndb.jvn.jp/ja/contents/2009/JVNDB-2009-001131.html

添付された PDF ファイルを開いて **Trojan.Pidief.C** に感染すると、**Trojan-Proxy.Win32.Agent.blp** という別のウイルスがインストールされ、それによってダミーの PDF 文書が表示されます（図 1-3 参照）。こうすることで、ウイルスに感染したことに気付きにくくなっています。さらに、**Trojan-Proxy.Win32.Agent.blp** は、悪意あるウェブサイトにアクセスし、他のウイルスをダウンロードします。

なお、今回解析した **Trojan.Pidief.C** は、脆弱性が解消されていればウイルスには感染せず、ダミーの PDF 文書は表示されませんでした。（図 1-4 参照）。



（CNN） メキシコや米国で豚インフルエンザの感染拡大が懸念されている問題で、米疾病対策センター（CDC）は26日、国内5州で計20人の感染が確認されたと発表した。また、カナダでは同日初めて、6人の感染が確認されたが、いずれも軽症にとどまっている。CDCによると、米国では同日正午までに、ニューヨーク州で8人、カリフォルニア州で7人、カンザス州とテキサス州で2人、オハイオ州で1人がそれぞれ豚インフルエンザに感染したことが明らかになった。ブルームバーグ・ニューヨーク市長によると、同市内で感染した8人は同じ私立学校の生徒たちだった。米国内の患者のうち入院したのは1人にとどまっているものの、CDCのベアサー所長代行は「メキシコからの報告から考えると、米国内でも今後重症例が増える恐れがある」と話している。

ギブズ大統領報道官は記者会見で、この事態にホワイトハウスとして「重大な懸念」を示す一方、「流行がどのような規模、範囲に及ぶにしても、政府は必要な措置を尽くして警戒に当たっている。パニックを起こす必要はない」と、国民に平静を呼び掛けた。

米軍は世界各地に駐留する衛生要員に、部隊内での豚インフルエンザの兆候を警戒するよう指示を出した。一方、米航空輸送協会（ATA）によれば、航空会社はそれぞれ、乗客の体調への注意を強化する措置を取っている。

感染元とみられるメキシコのカルデロン大統領によると、豚インフルエンザによる同国内での死者は81人、入院患者は374人に達している。メキシコ市の大聖堂では26日、礼拝が中止され、軍要員が朝からマスクを配布した。

豚インフルエンザが疑われる症例は米大陸以外でも報告されている。スペインの保健当局は、メキシコから帰国した旅行者6人が隔離され、検査を受けていると発表。イスラエル

図 1-3：感染した場合

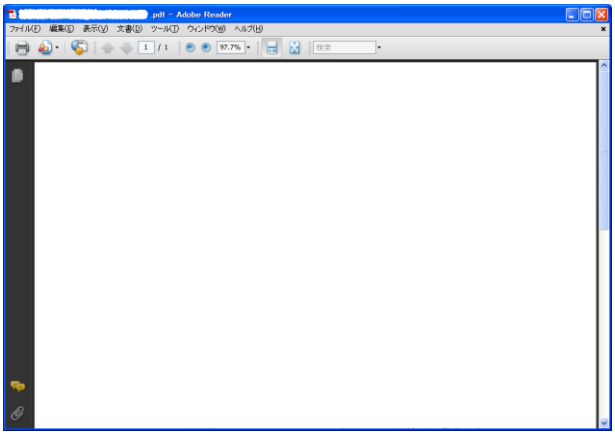


図 1-4：感染しなかった場合

（ご参考）
「公的機関になりすましたメールに注意してください！！」（2008 年 4 月の呼びかけ）
http://www.ipa.go.jp/security/txt/2008/05outline.html

その他に、**Trojan.Win32.Chifrax.a** と称されるウイルスを検出しました。このウイルスは、2007 年 10 月には発見されていますが、今回解析した検体は新たに作り直されたウイルスです。

このウイルスは、キーロガーとして動作します。キーロガーとは、キーボードから入力した情報を記録するプログラムで、個人情報を詐取しようとします。

（3）対策

（a）怪しいサイトやメールを見分ける方策

（1）の（a）SEO ポイズニングの場合、検索結果に表示されるウェブサイトが悪意あるものかどうかは、書かれているリンクを見ただけでは簡単には分かりません。ただ、検索結果に表示されるウェブサイト名やリンクが、入力した検索キーワードとまったく関係のない表示であるなど、少しでも怪しいと思うリンク先であれば、クリックをしてアクセスすることは止めましょう。

IPA では、このようなウェブサイトの危険性を利用者に代わって判断するサービスを行っていますので、ぜひご利用ください。

（ご参考）
「悪意あるサイトの識別情報および対策情報提供システム（TIPS）」を利用したウェブサイト情報提供サービスを開始 （IPA）
http://www.ipa.go.jp/security/isg/tips.html

（1）の（b）偽の注意喚起メールを含めた迷惑メールなどの場合、普段やり取りがない送信者からのメールが届いたら、すぐに開いたり、中に書いてあるリンク先をクリックしたりしないでください。可能であれば送信者と連絡を取り、本当にその送信者が送ったメールなのかを確認しましょう。

ただし、確認をする際は、メールの中に書かれている連絡先には連絡をせず、出来る限り自分で連絡先を調べて電話で確認することを勧めます。

添付ファイルがあるメールであれば、普段やり取りのある送信者からのメールでも、送信者と連絡を取って確認しましょう。今回のように、普段やり取りのない相手から、突然に注意喚起の内容でメールが届くことはまずあり得ないことと思います。少しでも怪しいと思うメールであれば、確認を取るか、開かずに削除することが一番の対策です。

今回の偽の注意喚起メールの場合、添付ファイルを開くことによって、Adobe Reader および Adobe Acrobat の脆弱性を突いてウイルスを感染させる手口でしたので、使用するアプリケーションソフトの脆弱性は可能な限り解消してください。

（ご参考）
「緊急対策情報 Adobe Reader および Acrobat の脆弱性について」（IPA）
http://www.ipa.go.jp/security/ciadr/vul/20090311-adobe.html

IPA では、今回の事例のような情報詐取を狙ったメールに関する相談窓口を設置しています。

（ご参考）
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の相談窓口「不審メール 110 番」（IPA）
http://www.ipa.go.jp/security/virus/fushin110.html

（b）基本的なウイルス対策
今回の事例からも見てとれるように、最近ではどこのサイトが安全か、どのメールを信用していいのかの判断が非常に難しくなっており、いつどこでウイルスに感染するかわからない状況となっています。このため、ウイルスの感染を防ぐ基本的な対策として、次の 3 つについては必ず実施しましょう。

・OS や、使用しているアプリケーションソフトを常に最新の状態に更新して、脆弱性を可能な限り解消しましょう。
・ウイルス対策ソフトのウイルス定義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ましょう。
・万が一、ウイルスに感染した場合を考えて、重要なデータは外部記憶媒体（USB メモリや外付け HDD など）にバックアップしておきましょう。

（ご参考）
「Microsoft Update と Windows Update の利用の手順」（マイクロソフト社）
http://www.microsoft.com/japan/athome/security/mrt/wu.mspx
「JVN iPedia 脆弱性対策情報データベース」（JVN）
http://jvndb.jvn.jp/

（c）感染後の対応
ウイルスの感染被害に遭ってしまった場合、お使いのウイルス対策ソフトより、ウイルス定義ファイルを最新の状態にしてからパソコン内のウイルスチェックを行ってください。
ウイルスを駆除できたとしても、パソコンが正常に動作していないと思われるのであれば、「システムの復元」を実施してください。これは、Windows XP、Windows Vista に搭載されている機能で、パソコンの情報を過去の状態に戻す機能です。なお、選択した日付から現在までに作成した文書や送受信したメール情報およびホームページへのアクセス履歴やお気に入りは消えません。以下のマイクロソフトのサイトを参考にして、「システムの復元」を行ってください。

（ご参考）
「システムの復元 Windows XP」（マイクロソフト社）
http://www.microsoft.com/japan/windowsxp/pro/business/feature/performance/restore.mspx
「Windows Vista のシステムの復元の解説」（マイクロソフト社「PC とーくの情報」）
http://support.microsoft.com/kb/934854/ja

システムの復元が正常に完了しない場合は、パソコンを購入した時の状態に戻す作業（初期化）を行ってください。
実際の作業方法は、取扱説明書に記載されている「購入時の状態に戻す」などの手順に沿って作業してください。なお、作業を行う前には、重要なデータのバックアップを忘れずに行ってください。また、バックアップしたデータは、パソコンに戻す前にウイルス対策ソフトでウイルスチェックし、ウイルスが含まれていないことを確認してください。

（ご参考）
「パソコンユーザのためのウイルス対策 7 箇条」（IPA）
http://www.ipa.go.jp/security/antivirus/7kajonew.html
「パソコンユーザのためのスパイウェア対策 5 箇条」（IPA）
http://www.ipa.go.jp/security/antivirus/spyware5kajyou.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）
- ウェブページ内に不正なスクリプトを埋め込まれた
- SPAM メール中継の踏み台にされた

○ 相談の主な事例 （相談受付状況および相談事例の詳細は、8 頁の「4.相談受付状況」を参照）
- オンラインゲームのサイトで不正アクセスされたようだ
- 無料のはずのフリーメールが？

○ 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。
- 2967/tcp へのアクセスに注意！

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 11.5 万個**と、4 月の約 15.6 万個から 26.1%の減少となりました。
また、5 月の届出件数(※2)は、**1,387 件**となり、4 月の 1,438 件から 3.5%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。
・5 月は、寄せられたウイルス検出数約 11.5 万個を集約した結果、1,387 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 9.7 万個**、2 位は **W32/Downad** で**約 6 千個**、3 位は **W32/Mydoom** で**約 4 千個**でした。

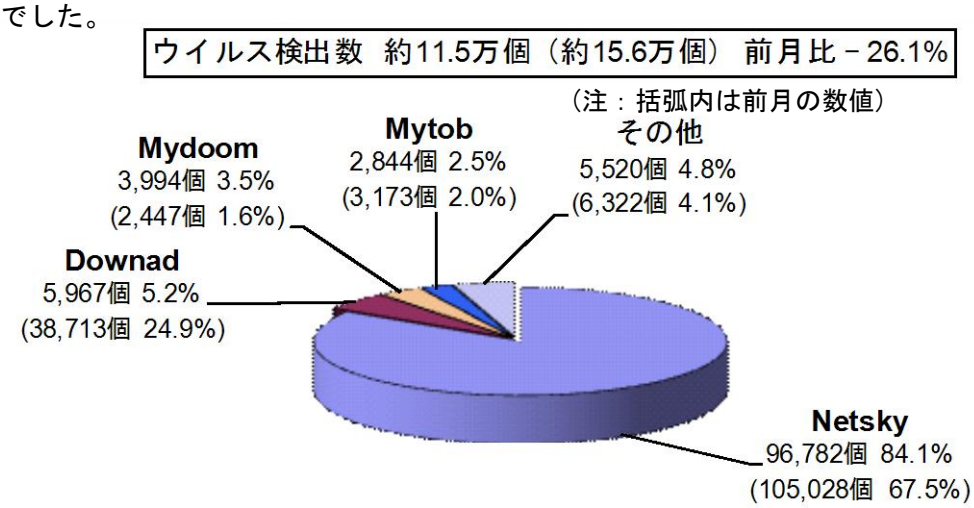


図 2-1：ウイルス検出数

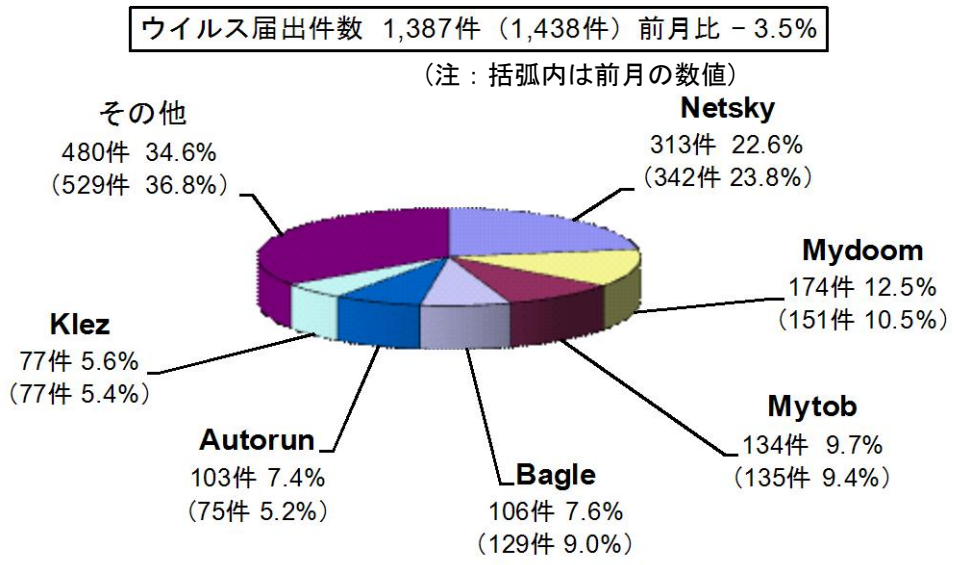


図 2-2：ウイルス届出件数

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

		12月	1月	2月	3月	4月	5月
届出(a) 計		**10**	**10**	**9**	**20**	**9**	**8**
	被害あり(b)	7	7	6	13	6	6
	被害なし(c)	3	3	3	7	3	2
相談(d) 計		**38**	**29**	**35**	**40**	**39**	**45**
	被害あり(e)	19	13	14	11	11	16
	被害なし(f)	19	16	21	29	28	29
合計(a+d)		**48**	**39**	**44**	**60**	**48**	**53**
	被害あり(b+e)	26	20	20	24	17	22
	被害なし(c+f)	22	19	24	36	31	31

（1）不正アクセス届出状況

5 月の届出件数は 8 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 45 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 16 件でした。

（3）被害状況

被害届出の内訳は、**侵入 4 件、メール不正中継 1 件、DoS 攻撃 1 件、**でした。

「侵入」の被害は、ウェブページ内に不正なスクリプトを埋め込まれていたものが 3 件、ウェブページ内の個人情報を不正に閲覧・改ざんされていたものが 1 件、でした。侵入の原因は、ウェブページ更新用パソコンがウイルス感染して FTP アカウント情報を盗まれたと思われるものが 2 件、ウェブサイ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、でした（残りの 1 件は原因不明）。

※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） ウェブページ内に不正なスクリプトを埋め込まれた

事例	・自社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警告を出した。 ・調査したところ、自社ウェブサイト内の約 100 個の html ファイルと js ファイルに不正なスクリプトを埋め込まれていたことが判明。自社サイトにアクセスし改ざんされたページを閲覧した一般利用者などのパソコンは、外部のサイトに飛ばされるようになっていた。当該外部サイトには、パソコン内のアプリケーションの脆弱性を突き、ウイルスをダウンロードさせようとする仕掛けが成されていた。 ・スクリプト埋め込みの改ざん行為は、ウェブサーバへの FTP アクセスで行われていたことが、FTP ログによって分かった。FTP アカウントやパスワードが盗まれた原因は不明だが、ウェブページ更新用パソコンがウイルスに感染したためと推測される。 ・FTP ログインパスワードを変更したが、再度改ざんされたため、許可 IP アドレス以外からの FTP アクセスを制限することで対処した。
解説・対策	最近、同じようなことが起きていると思われるサイトが多く見受けられます。最悪の場合、顧客などが自社サイトを閲覧して来た際に、知らぬ間にウイルス感染させられてしまいます。サイト運用側でウイルス対策はもちろんのこと、意図しないウェブページ書き換え検知を実施したり、ウェブサイトへの FTP アクセス制限を施したりすることが有効です。なお、通常の FTP アクセスはパスワードが平文で送られてしまいます。**セキュアなファイル転送には、FTPS（File Transfer Protocol over SSL/TLS）、SFTP（SSH File Transfer Protocol）、scp（Secure Copy）、VPN などを使うのが有効**でしょう。

[メール不正中継]

（ii） SPAM メール中継の踏み台にされた

事例	・会社のメールサーバに、1 日足らずで 3000 通を超える SPAM メールを受けた。それらの半分以上は SPAM メールとして社内メールサーバでブロックされていた。その後も断続的にアクセスが来る。 ・調査したところ、宛先が自社内ではなく、不正に中継しようとするメールアクセスであったことが判明。メール不正中継防止設定に不備があり、中継を許していた。 ・以前はファイアウォールで中継防止設定をしていたが、最近 UTM※に入れ替え、中継設定がうまくいっていなかったようだ。
解説・対策	この事例では、初めはメール不正中継に悪用されていることに気付きませんでした。一度は症状が収まったものの、2 週間後に再発していました。そこで根気強く調査を進めたところ、最近、ファイアウォールから UTM に機器入れ替えをしたことが原因であることに気が付くことが出来ました。 **不正中継を放置すると、ブラックリストに掲載されてしまい、メールの送り先でブロックされたりすることがあるため、注意が必要**です。メールサーバの第三者中継の可能性について、簡易的にチェックできるサイトもありますので、定期的にチェックしてみるのも良いでしょう。 （参考） RBL　JP – Third Party Relay Check http://www.rbl.jp/svcheck.php

※UTM（Unified Threat Management）：統合脅威管理、またその機器のこと。ファイアウォール・不正侵入防止・アドレスフィルタ・ウイルス検知などの複数機能が 1 台の機器に統合されている。

4. 相談受付状況

5 月の相談総件数は **1,765 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 **628 件**（4 月：572 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 **2 件**（4 月：3 件）、**Winny に関連する相談**が **5 件**（4 月：4 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 **5 件**（4 月：0 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

		12月	1月	2月	3月	4月	5月
合計		839	960	1,051	1,406	1,668	1,765
	自動応答システム	458	529	521	758	962	992
	電話	331	390	472	597	651	710
	電子メール	49	39	57	49	55	58
	その他	1	2	1	2	0	5

※ 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。

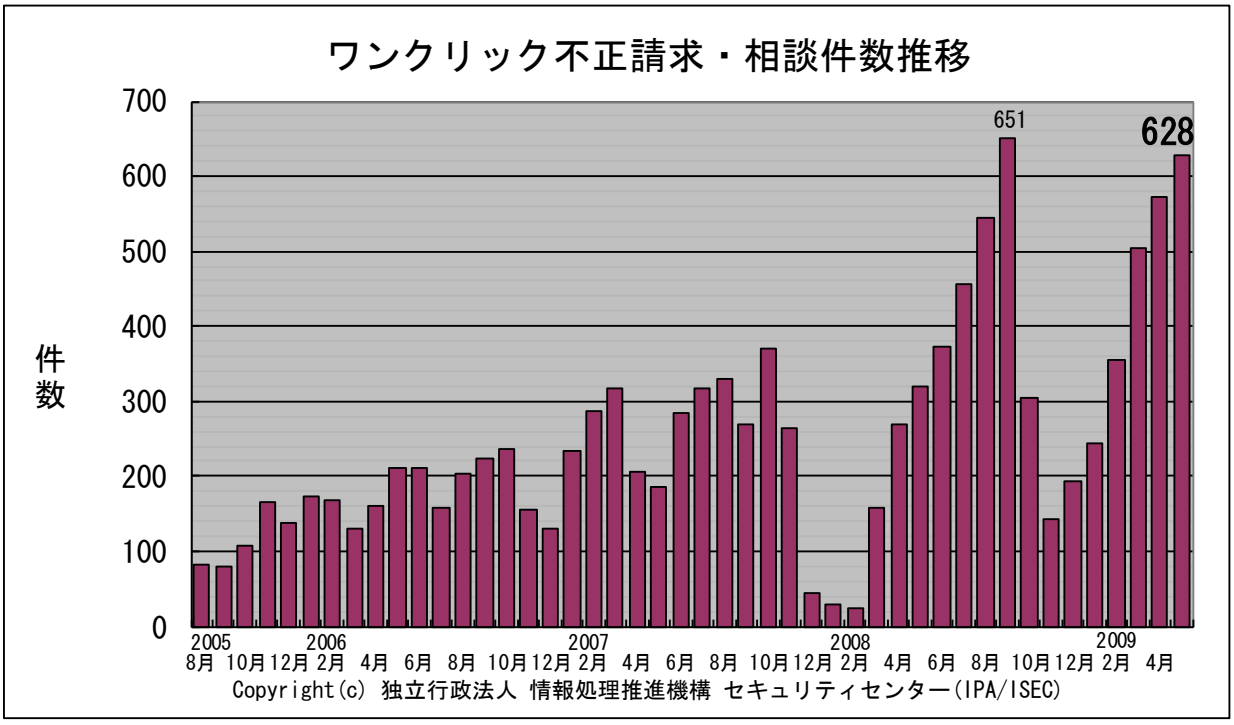


図 4-1　ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

（i） オンラインゲームのサイトで不正アクセスされたようだ

相談	あるオンラインゲームサイトで、有料のサービスを利用している。ある日、サイト内で使用する有料のポイントが勝手に使われていることに気付いた。サイト運営者に連絡したら、「警察など公的な機関からの要請があれば、ログなどの調査を開始する」との回答。警察に相談したら、「被害の主体であるサイト運営者からの被害届出が無いと、事件として扱えない」と言われた。消費者センターに相談したら、警察に届出しろと言われた。八方塞がり状態。どうしたらよいか。
回答	この場合、サイト利用者の被害は間接的であり、直接被害を受けているのはサイト運営者だということのようです。よって、**サイト運営者側が被害状況調査をしてくれないことには、話が始まりません**。サイト運営者が、顧客の訴えに耳を貸してくれないようなら、消費者センターに間に入ってもらい、話を進めましょう。 （ご参考） 全国の消費生活センター http://www.kokusen.go.jp/map/

（ii） 無料のはずのフリーメールが？

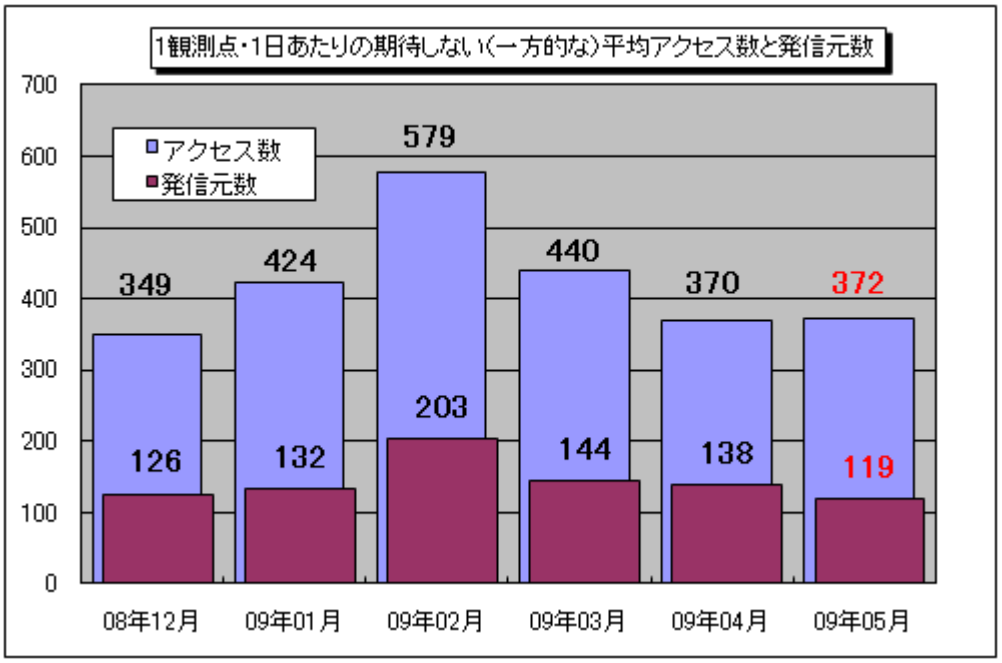
相談	ある有名なフリーメールを使用している。しばらく使っていなかったが、最近、また使い始めた。そのフリーメールの運営者からメールが来た。「メールの振り分けが悪くてサーバの障害が起きている。無償で復旧できる範疇を超えているので、料金が発生する恐れがある」と書かれていた。こんなことはあるのか。
回答	フリーメール事業者を装った、架空請求メールである可能性があります。**送られて来たメールの内容に疑問があれば、送り主であるサービス運営者に問い合わせることをお勧めします**。その際は、送られて来たメール本文にある連絡先ではなく、**サービス運営者の公式ウェブサイトなどに掲載されている、信頼できる連絡先に問い合わせる**ようにしましょう。 もし「お金を振り込んでしまった」、「しつこく請求されている」ということがありましたら、警察機関に相談することをお勧めします。 （ご参考） 警察庁 - インターネット安全・安心相談 http://www.npa.go.jp/cybersafety/

5. インターネット定点観測での 5 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 5 月の期待しない（一方的な）アクセスの総数は 10 観測点で **115,336 件**、総発信元（※）は **36,779 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 119 の発信元から 372 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。

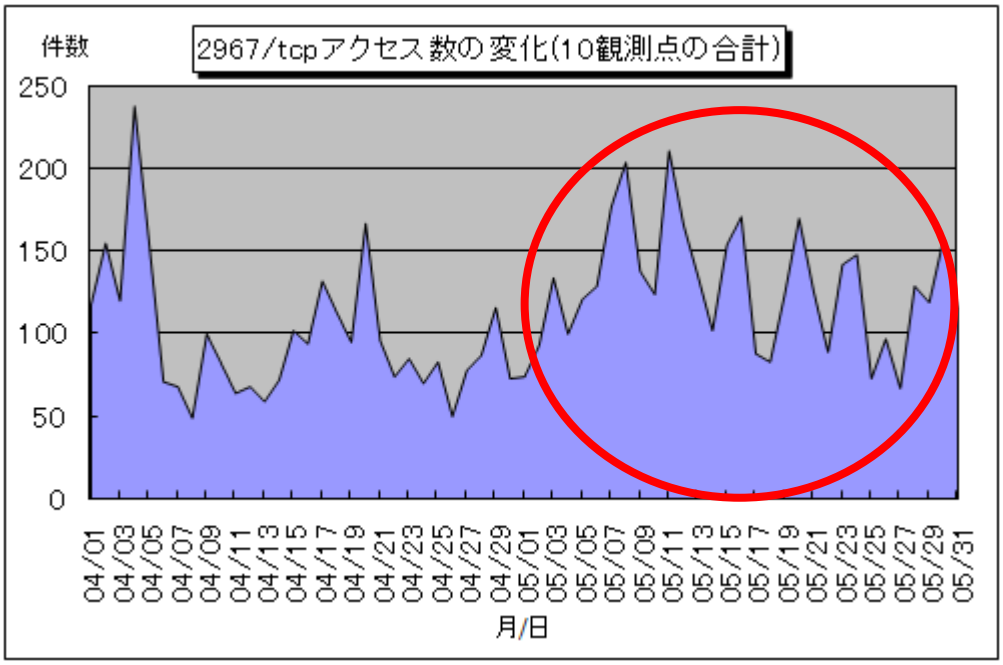
TALOT2 における各観測点の環境は、インターネットを利用される一般的な接続環境と同一なので、インターネットを利用される皆さんの環境へも同じくらいの一方的なアクセスがあると考えられます。



【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】

（1）2967/tcp へのアクセス

2967/tcp へのアクセスが、5 月に入ったあたりから増加傾向を示していました（図 5-2 参照）。



【図 5-2 2967/tcp アクセス数の変化（10 観測点の合計）】

2967/tcp は Symantec 製品がデフォルトで使用するポートです。このポートが攻撃に利用される脆弱性としては、過去に『Symantec Client Security および Symantec AntiVirus に特権昇格の脆弱性（SYM06-010）』が公開されています。

この脆弱性は、影響を受ける製品（Symantec Client Security や Symantec AntiVirus など）において、攻撃者によってファイルの取得または削除が可能となり、システムが破壊される可能性がある、というものです。

（ご参考）
「Symantec Client Security および Symantec AntiVirus に特権昇格の脆弱性（SYM06-010）」
http://www.symantec.com/region/jp/avcenter/security/content/2006.05.25.html

製品の脆弱性が解消されていないと、その脆弱性を突いた攻撃を受ける可能性があります。そのような被害に遭わないためには、常に脆弱性情報に注意し、お使いの製品の脆弱性が公開されたら、できるだけ早くその脆弱性を解消することが重要です。

日頃からお使いの製品のベンダーのホームページや、JVN などの脆弱性対策情報ポータルサイトを確認して、製品の脆弱性対策を迅速に行えるようにしてください。

（ご参考）
「JVN （Japan Vulnerability Notes）」（脆弱性対策情報ポータルサイト）
http://jvn.jp/
「JVN iPedia 脆弱性対策情報データベース」
http://jvndb.jvn.jp/

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/TALOT2-0906.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