プレスリリース
第 09-44-168 号
2009 年 11 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 [2009 年 10 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 10 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

「偽のセキュリティ対策ソフトの脅威が再び拡大！」
― 手口を知って被害を未然に防ごう ―

毎月の IPA へのウイルス届出において、「偽セキュリティ対策ソフト」を購入させようとする不正プログラム（以降、ウイルスとして扱います）の検出数（※）が約 1 年ぶりに増加傾向を見せており（図 1-1 参照）、「偽セキュリティ対策ソフト」の脅威が再び拡大しつつあると言えます。

「偽セキュリティ対策ソフト」とは、「ウイルスに感染している」といった嘘の警告メッセージや、偽物の「ウイルス検出画面」を表示させ、ウイルスを駆除するには有償版の製品が必要であるとして、購入サイトに誘導するウイルスのことです。

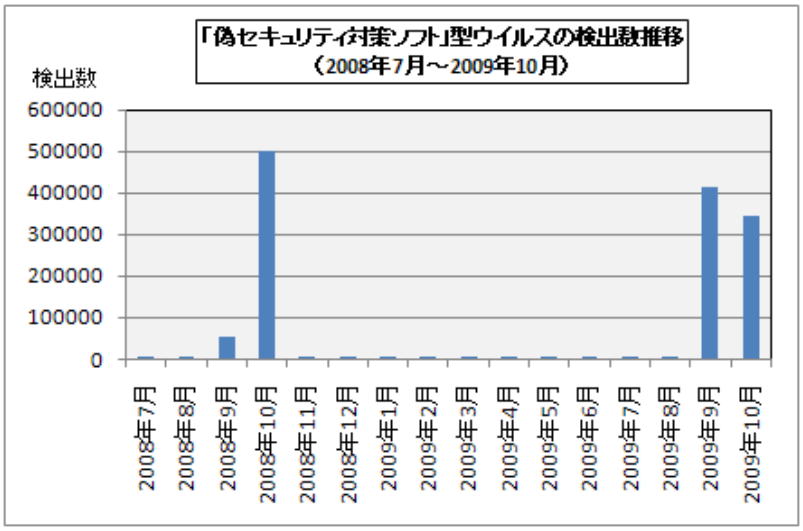


図 1-1：「偽セキュリティ対策ソフト」型ウイルスの検出数推移（2008 年 7 月～2009 年 10 月）

以降で解説する最近の「偽セキュリティ対策ソフト」型ウイルスの手口を確認し、被害を未然に防いでください。

※ 検出数 ： ウイルス届出者から寄せられたウイルスの発見数（個数）の当該月の総合計のこと

（1）感染の手口

IPA では最近の「偽セキュリティ対策ソフト」型ウイルスの感染の手口として、下記のような事例を確認しています。

（i）迷惑メールに添付されているファイルを開くことで感染

マイクロソフト社や、実在する有名海外企業を騙った迷惑メールが広範囲に配布されたことが推察できます（図 1-2 参照）。メールには、外部のサイトから「偽セキュリティ対策ソフト」をダウンロードするためのウイルス（ダウンローダー）が埋め込まれたファイルが添付されており、それを開くことで、利用者が知らないうちに「偽セキュリティ対策ソフト」がインストールされるという仕組みになっていました（図 1-3 の【感染の手口 1】参照）。

図 1-2：IPA が確認した、海外企業を騙った迷惑メールの例

（ご参考）
「マイクロソフト社を騙るマルウエア添付メールに関する注意喚起」（2009 年 10 月 20 日公開）（JPCERT/CC）
http://www.jpcert.or.jp/at/2009/at090022.txt

（ii）不正なスクリプトを埋め込まれたウェブサイトを閲覧することで感染

悪意ある者が、正規のウェブサイトに不正なスクリプト（プログラム）を埋め込んでおき、利用者がそのウェブサイトを閲覧すると、裏でそのスクリプトが別の不正サイトにアクセスし、利用者のパソコンに「偽セキュリティ対策ソフト」型ウイルスをダウンロードさせられてしまうといった被害が確認されています（図 1-3 の【感染の手口 2】参照）。この場合、利用者のパソコンに導入されている OS やアプリケーション（Adobe Flash Player や Adobe Reader など）の脆弱性が悪用されます。

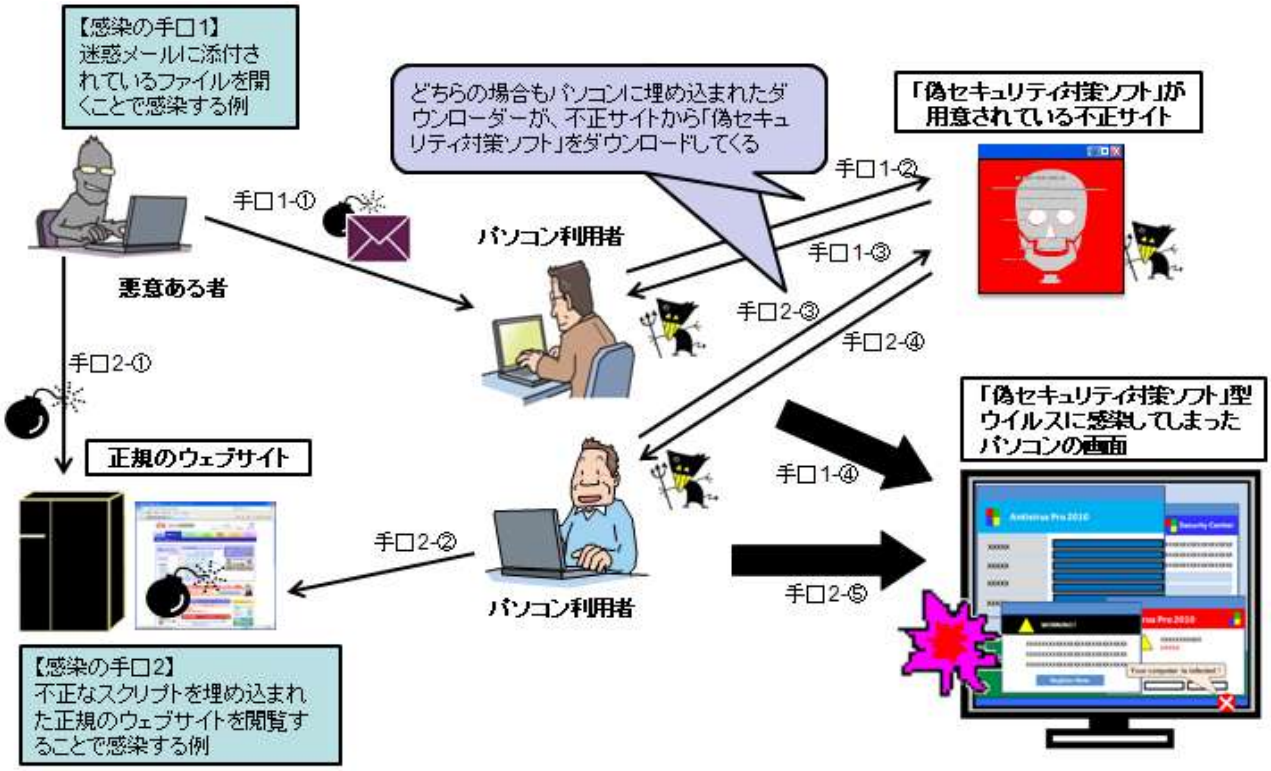


図 1-3：「偽セキュリティ対策ソフト」型ウイルスの感染手口のイメージ

（2）予防策

「偽セキュリティ対策ソフト」型ウイルスの被害を未然に防ぐために、次の対策を行ってください。

（a）迷惑メールへの対応

「（1）感染の手口」の（i）の事例のような、実在する組織を騙ってメール受信者を信用させようとする迷惑メールへの対処は、“自分の身に覚えのないメールは開かない”ことです。特に、そのようなメールの添付ファイルはウイルスである可能性が高いため、絶対に開いてはいけません。場合によっては送信元の組織に連絡をとり、メールの真偽を確かめることも有効です。少しでも怪しいと感じたら、細心の注意を払うことがウイルス感染を予防するための適切な対応です。

（b）脆弱性対策

「（1）感染の手口」の（ii）の事例のように、正規のウェブサイトを閲覧するだけで、OS やアプリケーションの脆弱性を突かれて被害に遭う場合があります。また、ウェブサイトのページを編集しているパソコンに脆弱性が存在していると、ウェブサイトに不正なスクリプトを埋め込まれて、ウェブサイトの閲覧者に被害を与えることにもなりかねません。予防策は、使用している OS とア

プリケーション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ておくことです。

（c）ウイルス対策

上記の個別の予防策に加えて共通した予防策として、信頼のおけるウイルス対策ソフトを常に最新の状態で使用することが重要です。

また、これからウイルス対策ソフトを購入する場合は、信頼のおけるウイルス対策ソフトメーカーの製品を購入してください。そのためには、インターネットのダウンロード販売で購入せず、パソコンショップなどでの店頭購入を推奨します。

（3）感染時の症状

IPA で入手した「偽セキュリティ対策ソフト」型ウイルスを検証したところ、次のような症状を確認しました。

- タスクバーに×マークのアイコンが出現し、「Your Computer is infected!（あなたのパソコンはウイルスに感染しています！）」という警告メッセージがしつこくポップアップ表示される。
- 突然、「Antivirus Pro 2010」というセキュリティ対策ソフトらしき画面が出現し、ウイルスチェックが開始される。ウイルスチェック終了後、ウイルスが複数検出されたという嘘の結果が表示され、駆除するには有償版製品の購入が必要であるという警告画面が複数表示される。
- Windows の「セキュリティセンター」の画面に似せた英語表記の画面が現れ、セキュリティに問題があるように警告し、有償版製品を購入するように訴える。

これらの症状が図 1-4 のように一つの画面に表示されて、最終的にはクレジットカード番号の入力を促されることになります。

図 1-4：「偽セキュリティ対策ソフト」型ウイルスに感染した Windows 画面の例

信頼のおけるウイルス対策ソフトは、このように急に警告メッセージを出すことはありません。万が一、使用中のパソコンが、図 1-4 のような状態になってしまった場合、「偽セキュリティ対策ソフ

ト」型ウイルスに感染している可能性が高いと言えます。ウイルスに感染してしまった原因の一つとして、お使いのウイルス対策ソフトが最新の状態でなかったことが考えられます。しかし、これらの症状が発生した後で、ウイルス対策ソフトを最新の状態にして、ウイルスを駆除しようとしても、最近のウイルスは様々な妨害策を講じ、駆除されないようにする場合があります。

最新のウイルス対策ソフトを使用しても症状が治まらない場合は、次項の「(4) 事後対策」を参照してください。

(4) 事後対策

最新のウイルス対策ソフトを使用しても症状が治まらない場合、次に示す「システムの復元」を行ってください。それでも症状が改善されない場合、もしくは、「システムの復元」が失敗する場合は、パソコンの初期化を実施してください。

(a)「システムの復元」による復旧

Windows XP や Windows Vista、Windows 7 には、パソコンの動作が不安定になるなど、使用に支障がある状態に陥った場合、以前の状態に戻すことができる「システムの復元」という機能があります。これは Windows が自動で定期的に保存しているシステムの情報を基に、パソコンの状態を元に戻す機能です。

下記のマイクロソフトのウェブページを参考にして、「システムの復元」を行ってください。ただし、復元対象として指定した日から現在までに行った、アプリケーションソフトウェアのインストール、アップデートの情報は消えてしまいますので、これらはシステム復元後に再度実施してください。

（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」（マイクロソフト社の「PC と一く」の情報）
http://support.microsoft.com/kb/934854/ja

「Windows 7 の機能：システムの復元」（マイクロソフト社）
http://windows.microsoft.com/ja-JP/windows7/products/features/system-restore

(b) パソコンの初期化

パソコンを購入した時の状態に戻す初期化という作業を実施します。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。

作業前に、重要なデータの外部媒体（USB メモリや CD-R、外付け HDD など）へのバックアップを推奨します。

（ご参考）

「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

「パソコンユーザのためのスパイウェア対策 5 箇条」
http://www.ipa.go.jp/security/antivirus/spyware5kajyou.html

「メールの添付ファイルの取り扱い 5 つの心得」
http://www.ipa.go.jp/security/antivirus/attach5.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、7 頁の「3.コンピュータ不正アクセス届出状況」を参照）
- ウェブアプリケーションの脆弱性を突かれて侵入され、ファイルを置かれた
- 不正プログラムを埋め込まれ、他サイト攻撃のための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）
- 会社のパソコンでアダルトサイトを見ていたら、請求書が消えなくなった
- 社内のパソコン数十台がウイルス感染？

○ 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

10 月のウイルスの検出数（※1）は、**約 7 万個**と、9 月の約 7.6 万個から 7.8%の減少となりました。また、10 月の届出件数（※2）は、**1,210 件**となり、9 月の 1,301 件から 6.9%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。
- 10 月は、寄せられたウイルス検出数約 7 万個を集約した結果、1,210 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 5.9 万個**、2 位は **W32/Mydoom** で**約 3 千 3 百個**、3 位は **W32/Mytob** で**約 2 千 8 百個**でした。

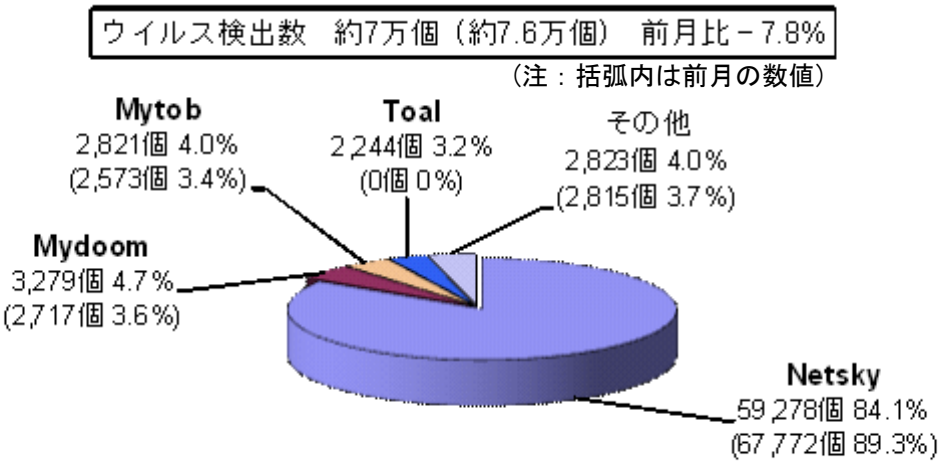


図 2-1：ウイルス検出数

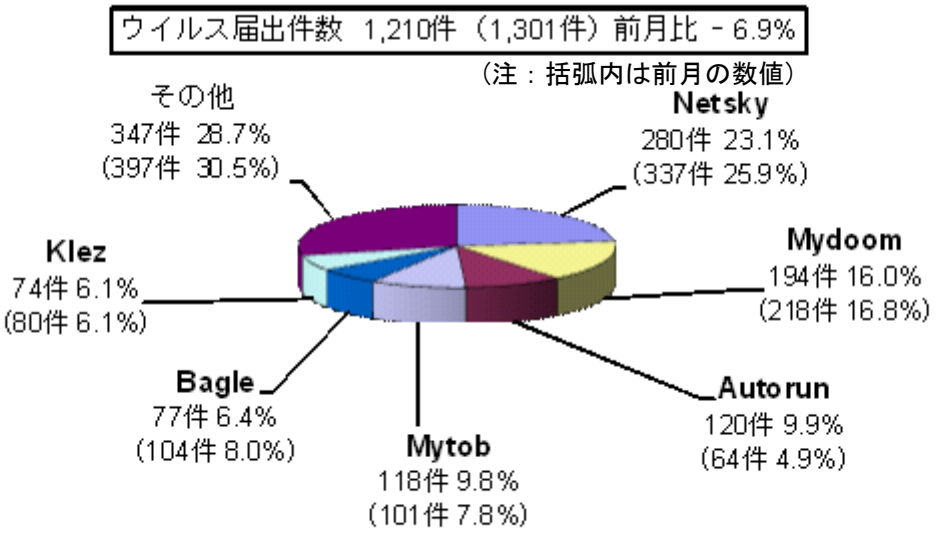


図 2-2：ウイルス届出件数

(2) 不正プログラムの検知状況

2009 年 9 月、「偽セキュリティ対策ソフト」型ウイルスの検知件数が急増しました（図 2-3 参照）。

「1.今月の呼びかけ」でも紹介しましたように、「偽セキュリティ対策ソフト」に感染させるための、FAKEAV が添付されたメールが大量に配信されたことによるものと推測されます。

FAKEAV に感染すると、最悪の場合、復旧には初期化が必要になるなど、深刻な被害が発生する危険性が高いことから、継続して注意を払う必要があります。

なお、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多数出回っており、図 2-3 からもわかる通り、特定の期間に急増するなど、不自然な傾向が見て取れます。これは、ボット等によりメール配信が行われているためと思われます。

サーバークリーンセンターでは、ボットに関する対策や駆除ツールを提供しています。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を実施するようにしてください。

（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/

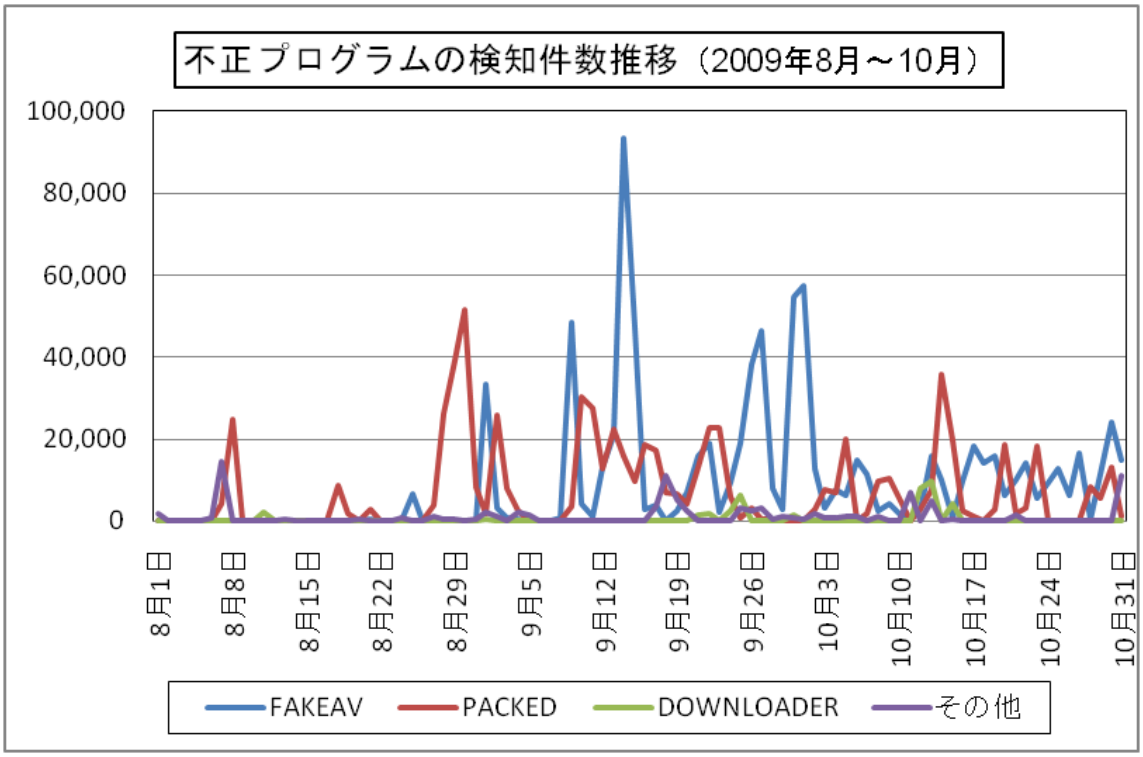


図 2-3：不正プログラムの検知件数推移

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

		5月	6月	7月	8月	9月	10月
届出(a) 計		8	7	14	20	11	21
	被害あり(b)	6	6	6	12	8	14
	被害なし(c)	2	1	8	8	3	7
相談(d) 計		45	35	24	39	44	34
	被害あり(e)	16	9	3	17	13	11
	被害なし(f)	29	26	21	22	31	23
合計(a+d)		53	42	38	59	55	55
	被害あり(b+e)	22	15	9	29	21	25
	被害なし(c+f)	31	27	29	30	34	30

（1）不正アクセス届出状況

10 月の届出件数は 21 件であり、そのうち何らかの被害のあったものは 14 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 34 件（うち 4 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 6 件、メール不正中継 1 件、DoS 攻撃 1 件、なりすまし 6 件、**でした。

「侵入」の被害は、ウェブサーバ内にファイルを置かれたりファイルを破壊されたりしたものが 3 件、他のサイトを攻撃するための踏み台として悪用されていたものが 2 件、サーバ内データの窃取が 1 件、でした。侵入の原因は、ウェブアプリケーションの脆弱性を突かれたものが 3 件（うち 2 件は phpMyAdmin の脆弱性）、パスワード管理不備が 2 件、設定不備が 1 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が 6 件（オンラインゲーム 5 件、ショッピングポータル 1 件）でした。

（4）被害事例

[侵入]

（i）ウェブアプリケーションの脆弱性を突かれて侵入され、ファイルを置かれた

事例	・オープンソース CMS（Contents Management System）である Geeklog を運用しているサーバに、見知らぬテキストファイルが置かれているのを発見。 ・テキストファイルには、「Hacked by S.W.A.T」と書かれていた。 ・調査したところ、Geeklog に付属していた別のアプリケーション（FCKeditor）に存在していた脆弱性を突かれて攻撃されていたことが判明。 ・すぐに、FCKeditor を最新の状態に更新した。
解説・対策	FCKeditor は**他のアプリケーションに付属していたものであるため、単独のアプリケーションという認識が薄かった**ものと思われます。**大元となるアプリケーション**（この場合は Geeklog）**に関する脆弱性情報を注意深くチェックする必要があります。** （参考） Geeklog - 過去に配布した FCKeditor の脆弱性をアタックされる事例報告 http://www.geeklog.jp/article.php/security_fckeditor20090828 JVNDB-2009-001890 - FCKEditor におけるディレクトリトラバーサルの脆弱性 http://jvndb.jvn.jp/ja/contents/2009/JVNDB-2009-001890.html

（ii）不正プログラムを埋め込まれ、他サイト攻撃のための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、不審なアクセスを多数受けている」との連絡が入った。 ・調査したところ、あるサーバに、他のマシンの脆弱性を探査する不正プログラムなどが置かれ、稼動状態になっていたことが判明。結果として、他のサーバを攻撃するための踏み台となっていた。 ・当該サーバに登録されていた、あるアカウントのパスワードが破られて侵入されていた。 ・その**パスワードは、初期状態からアカウント主により変更されておらず、推測が容易なままであった。**
解説・対策	利用者によっては、初期パスワードを変更せずにそのまま継続して使用することもあるでしょう。**初期パスワードは仮のものという位置付けですが、乱数を利用して規則性を無くし、推測しにくくすべき**です。 （参考） 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

4. 相談受付状況

10 月のウイルス・不正アクセス関連相談総件数は **2,049 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 **793 件**（9 月：650 件）と、過去最悪となりました（図 4-1 参照）。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 **6 件**（9 月：6 件）、**Winny に関連する相談**が **3 件**（9 月：0 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**（9 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

		5月	6月	7月	8月	9月	10月
合計		1,765	1,898	1,708	1,792	1,653	2,049
	自動応答システム	992	1,081	923	1,015	915	1,157
	電話	710	777	736	702	676	843
	電子メール	58	37	47	68	60	45
	その他	5	3	2	7	2	4

※ 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。

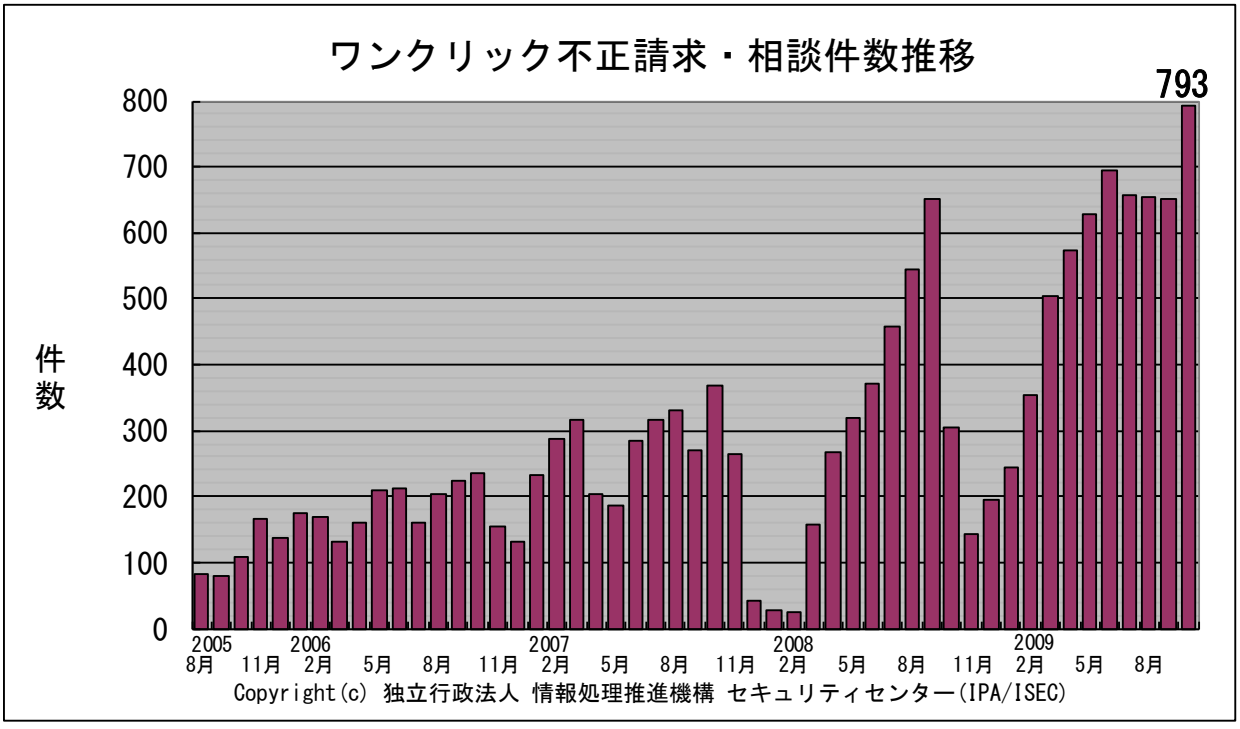


図 4-1：ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

（i）会社のパソコンでアダルトサイトを見ていたら、請求書が消えなくなった

相談	会社のパソコンでコッソリとアダルトサイトを見ていた。無料で動画を見られるというのでクリックして進んで行ったら、「登録が完了しました」と表示され、料金請求画面が消えなくなった。IPA に問い合わせ、ウイルスに感染したことが原因と分かった。一度 IPA に対処方法を聞いたが、「管理者権限が必要」というメッセージが出てエラーとなり、処置できない。管理者権限を持つアカウントでログオンしても、処置できない。 （**この相談の他、会社でアダルトサイトを見た際のトラブルが 10 件以上あり**）
回答	会社のパソコンで「制限付きアカウント」の場合は、パソコンの復旧作業に支障が出ることがあります。自分のアカウントに一時的に管理者権限を付与すると、対処が可能になるはずですが、会社のシステム管理者に事情を説明する必要があります。 そもそも、会社でアダルトサイトを閲覧することは許可されているのでしょうか。会社によっては、罰則規程があるでしょう。 **アダルトサイトに限らず、世の中にはウイルスを埋め込もうとする悪意あるサイトが多数存在します**。ウイルスの種類によっては、社内の他のパソコンに感染を広げてしまうものもありますから、もし当事者になってしまったら、その責任は重大です。**就業時間内に、業務に関係ないサイトの閲覧は慎みましょう**。 （ご参考） IPA - 【注意喚起】ワンクリック不正請求に関する相談急増！ http://www.ipa.go.jp/security/topics/alert20080909.html

（ii）社内のパソコン数十台がウイルス感染？

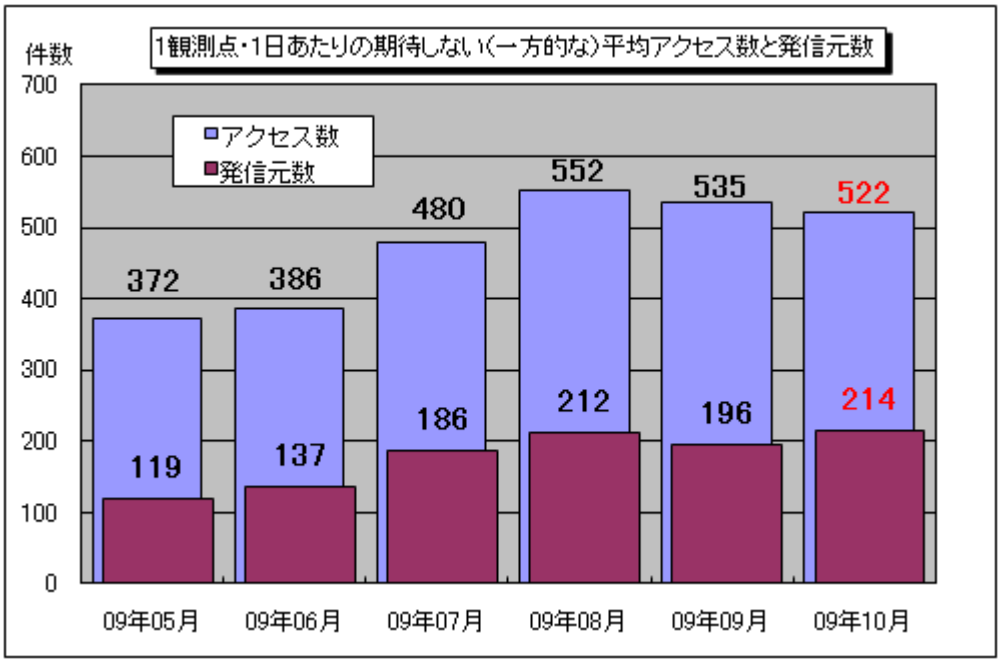
相談	社員が海外出張し、**現地で受け取ったデータを USB メモリに入れ**、帰国した。自席のパソコンにデータを移そうと、**USB メモリを挿したら、パソコンが正常に動作しなくなった**。同時に、社内で稼働しているサーバも正常に動作しなくなった。さらに、社内で使っている他のパソコン約 50 台の動作もおかしくなった。症状は以下の通り。 ・日本語入力ができない ・サーバに、**見た目はフォルダのアイコンなのに、拡張子が .exe のファイルがある** ・後日、ウイルス対策ソフトでウイルスが検知されて削除した。しかし、「ファイルの拡張子を表示する」という**設定が、すぐに無効にされる**症状は変わらず。
回答	**USB メモリ感染型ウイルスの中には、ネットワーク共有フォルダに自分自身をコピーしたり、他のマシンの脆弱性（MS08-067）を突いたりして感染を広げるものがあるため、ウイルスが社内に蔓延してしまった**ようです。 さらに、**現状では検知できない、他のウイルスにも新たに感染している**ようです。 業務用の多数のパソコンがウイルス感染し、かつ未知のウイルスにも侵されている状況ですと、**セキュリティ専門の業者に対処を依頼することが解決への近道かもしれません**。 （ご参考） IPA - 2009 年 5 月の呼びかけ「USB メモリのセキュリティ対策を意識していますか？」 http://www.ipa.go.jp/security/txt/2009/05outline.html

5. インターネット定点観測での 10 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 10 月の期待しない（一方的な）アクセスの総数は 10 観測点で **161,716 件**、延べ発信元数（※）は **66,430 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 214 の発信元から 522 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】

2009 年 5 月～2009 年 10 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。10 月の期待しない（一方的な）アクセスは、9 月と比べて若干減少しました。

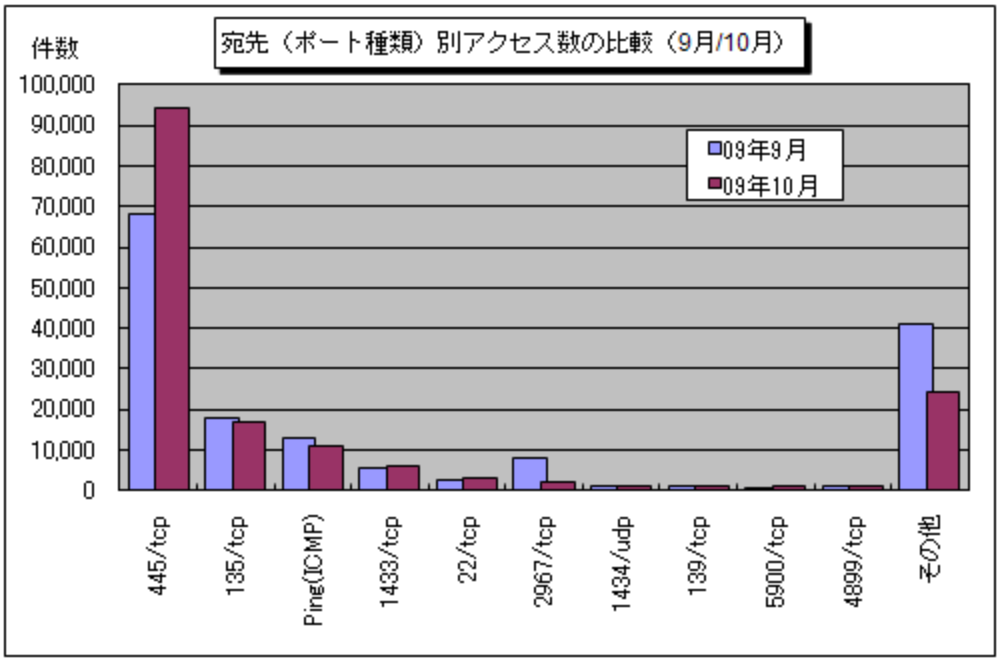
9 月と 10 月の宛先（ポート種類）別アクセス数の比較を図 5-2 に示します。

9 月と 10 月のアクセス数を比較したところ、445/tcp へのアクセスが 9 月に比べて約 1.4 倍に増加していました。

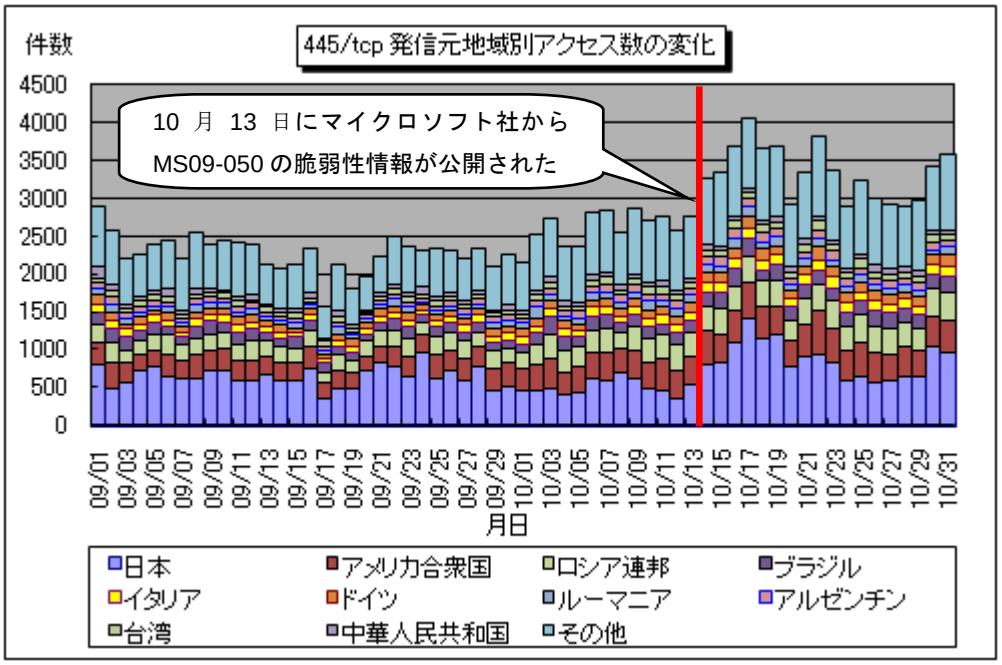
445/tcp は Windows の脆弱性（MS08-067）を悪用するワームなど、ウイルスによって狙われる可能性の高いポートとして有名です。2009 年 10 月 13 日（米国時間）にマイクロソフト社から公開された「Windows における SMBv2（※）の脆弱性（MS09-050）」も、445/tcp を悪用するものでした。

TALOT2 では、脆弱性情報が公開されたあたりから 445/tcp へのアクセスの若干の増加が観測されていたことから、この脆弱性を悪用しようとするなんらかの動きがあった可能性があります（図 5-3 参照）。この脆弱性は、脆弱性情報の公開と同時に提供された修正プログラムを適用することで恒久的な処置が可能ですので、まだ適用されてない場合はただちに実施してください。

SMBv2（※）： SMB（Server Message Block）とは、既定で Windows ベースのコンピュータ上で使用されるファイル共有プロトコルです。 SMBv2 (SMB Version 2.0) とはこのプロトコルに対する更新で、Windows Server 2008、Windows 7 および Windows Vista を実行しているコンピュータでのみサポートされています。



【図 5-2：宛先（ポート種類）別アクセス数の比較（9 月/10 月）】



【図 5-3：445/tcp 発信元地域別アクセス数の変化（10 観測点の合計）】

＜参考情報＞

■「SMBv2 の脆弱性により、リモートでコードが実行される」(マイクロソフト社)
http://www.microsoft.com/japan/technet/security/bulletin/MS09-050.mspx

■「Microsoft Windows における SMBv2 の脆弱性（MS09-050）について」（IPA）
http://www.ipa.go.jp/security/ciadr/vul/20091014-ms09-050.html

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/TALOT2-0911.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