INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
第 09-02-141 号
2009 年 2 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 1 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 1 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

「パソコンの脆弱性、解消されていますか？」
― あなたのパソコンはウイルスに狙われています！ ―

IPA のインターネット定点観測システム TALOT2(※)において、2008 年 10 月あたりから徐々に増え続け、1 月に入ってから急増したアクセスが観測されています。(図 1-1 参照。(1)で詳細解説)

これは 2008 年 10 月 24 日（日本時間）にマイクロソフトから緊急発表された、Windows の脆弱性(ぜいじゃくせい）MS08-067 を狙ったアクセスであった可能性があります。マイクロソフトによると、この情報が公開される 2 週間ほど前から、この脆弱性を突いた攻撃が確認されていたとのことです。

この脆弱性を突いて攻撃を行うウイルスが、複数確認されています。特に 2008 年 12 月末には Downadup.B と呼ばれる、USB メモリなどへの感染機能が追加された新しいウイルスが発見されています。今回のアクセスの急増の原因は、この機能追加されたウイルスが猛威をふるい、感染したパソコンから他のパソコンを攻撃するアクセス総数が増加したことであった可能性があります。

お使いのパソコンをウイルスに感染させないために、ウイルス対策・脆弱性対策の確実な実施が必要です。

※TALOT2 は、国内大手 ISP(インターネットサービスプロバイダ)と複数契約し一般のパソコン利用者と同等の回線を利用して、インターネット上のアクセスを観測するシステムです。

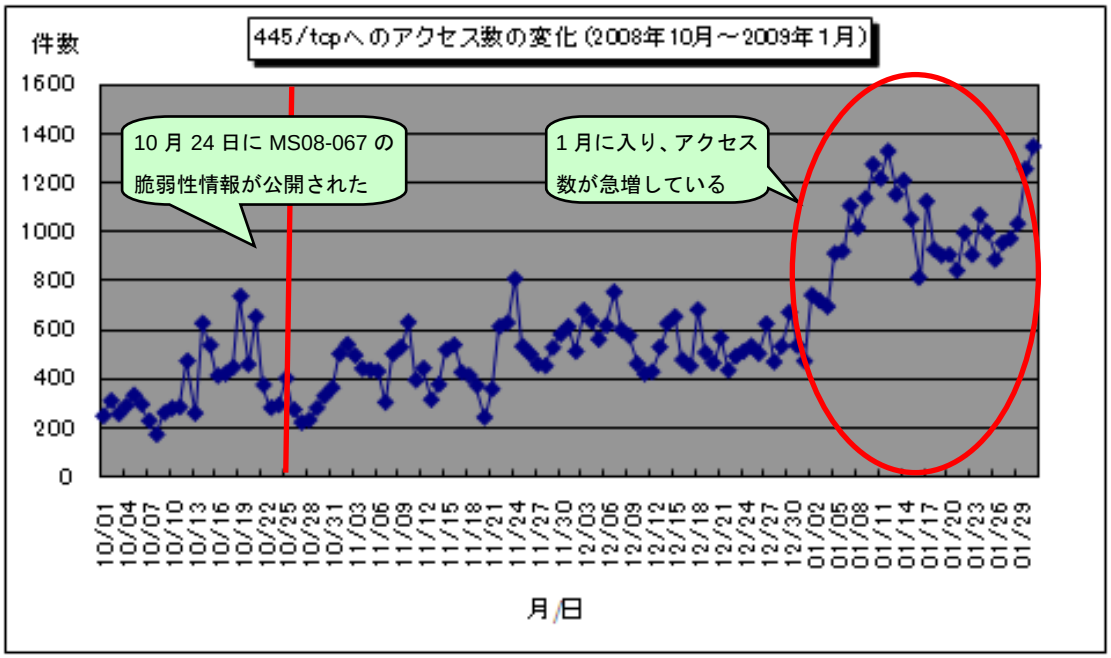


図 1-1：445/tcp へのアクセス数の変化(2008 年 10 月～2009 年 1 月)

（1）Windows の脆弱性(MS08-067)の概要

この脆弱性は、特別な細工がされたパケット(通信データ)が、攻撃対象のパソコンに送りつけられた場合に、Windows でファイルやプリンタの共有などを行うために利用されるサービス(Server サービス)において、意図せずに任意の命令が実行されてしまう可能性がある、というものです。

(ご参考)

「マイクロソフトセキュリティ情報 MS08-067 - 緊急
Server サービスの脆弱性によりリモートでコードが実行される 」
http://www.microsoft.com/japan/technet/security/bulletin/ms08-067.mspx

「Windows の Server サービスの脆弱性(MS08-067)について」(IPA)
http://www.ipa.go.jp/security/ciadr/vul/20081024-ms08-067.html

攻撃者は、攻撃対象のパソコンの Windows の Server サービスで使用されるポート(※)445/tcp に不正なパケットを送りつけることで、攻撃対象のパソコンに対してウイルスの感染、データの表示・変更及び削除、管理者権限を持つ新たなアカウントの作成などの不正アクセスを試みます。もし、パソコンの脆弱性を解消していない場合、攻撃者による不正アクセスが成功してしまい、パソコンがウイルスに感染するなどの被害が発生します。

現在確認されている、この脆弱性を悪用するウイルスについて、次節で説明します。

※ポートとは、コンピュータが外部との情報の受け渡しの際に使う、コンピュータ内の各種サービス窓口のことです。
ポートには 0 から 65535 までの値が使われるため、ポート番号とも呼ばれます。

(2) 脆弱性を悪用するウイルスの概要

この脆弱性を悪用した攻撃を行うウイルスの一つに、Downadup と呼ばれる種類のウイルスが確認されています。このウイルスは 2008 年 11 月下旬に発見され、12 月末にはその亜種である Downadup.B が発見されています。以下に、IPA で Downadup.B のウイルス検体を解析した結果を基に、ウイルスの特徴を説明します。

このウイルスは、脆弱性が解消されていないパソコンにネットワーク経由で感染したのち、そのパソコンを起点に、さらに多くのパソコンへ感染活動を試みます。このため、多数のパソコンが接続されている LAN の中で 1 台でもウイルス感染すると、その組織(企業、学校など)の LAN の中で感染が拡大する恐れがあります。(図 1-2 参照)

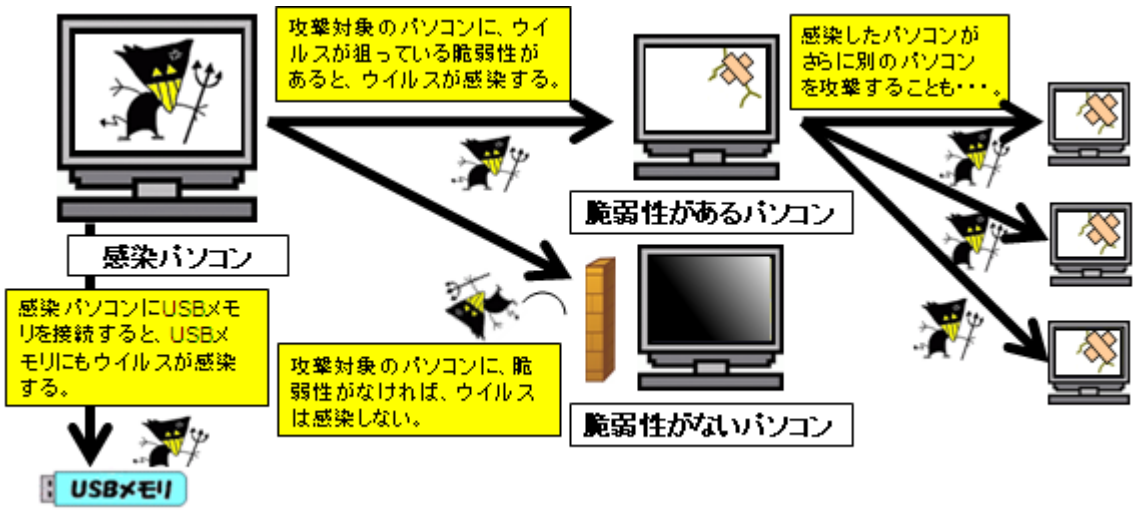


図 1-2：脆弱性を悪用するウイルスの動作例

なお、亜種である Downadup.B の特徴として、USB メモリなど外部記憶媒体への感染機能が新たに追加されたことが挙げられます。**1 月に入り 445/tcp へのアクセスが急増したのは、自宅などで Downadup.B ウイルスに感染してしまった USB メモリを組織の LAN 内のパソコンで利用した結果、組織内のパソコンがウイルス感染し、組織の LAN の中で感染が拡大したことが原因ではないか**と考えられます。ウイルスの亜種発生をきっかけとしてウイルス感染パソコンが増加し、それに伴い他の

パソコンを攻撃するアクセス総数も増加したのではないか、ということです(図 1-1)。
その他、悪意のあるサイトに接続し、他のウイルスのダウンロードを試みることも判明しています。
このウイルスに感染した場合の症状として、IPA の解析結果から以下のことが起こる可能性が確認されています(全ての症状が出るとは限りませんし、今後は他の症状が出る可能性があります)。

・ウイルス対策ソフトのウェブサイトへのアクセスが制限され、ウイルス定義ファイルの更新が妨害される。
・マイクロソフトのサイトへのアクセスが制限され、Windows Update が妨害される。

(3) 被害に遭わないための対策

この脆弱性を狙った攻撃による被害を、未然に防ぐための対策を以下に示します。

(a) 脆弱性の解消

基本的な対策としては、この脆弱性を解消することに尽きます。この脆弱性が解消されているか分からない場合は、Windows Update を試してみて、未適用のセキュリティパッチが残っていないか確認してください。未適用のものが残っていた場合は、直ちに適用して、脆弱性を解消してください。
また、ウイルス対策ソフトメーカーが無料で提供しているオンラインスキャンのサイトには、パソコンの脆弱性の有無をチェックできるものもあります。そのようなサイトを利用してパソコンの状態を確認することも有効です。

(ご参考)
「Microsoft Update と Windows Update の利用の手順」(マイクロソフト)
http://www.microsoft.com/japan/athome/security/mrt/wu.mspx
「トレンドマイクロ オンラインスキャン」(トレンドマイクロ)
http://www.trendmicro.co.jp/hcall/scan.htm
「シマンテックセキュリティチェック」(シマンテック)
http://www.symantec.com/region/jp/securitycheck/

(b) ウイルス対策ソフトの活用

ウイルスによる感染被害を防ぐための対策としては、ウイルス対策ソフトの活用が有効です。ただし、新種のウイルスが次々と発生しているため、必ず最新の状態に保っておくことが重要です。最新の状態でない場合は、直ちにウイルス定義ファイルを更新してください。

(c) パーソナルファイアウォールの活用

パーソナルファイアウォールとは、外部からの不正な攻撃を遮断したり、内部からの不正な通信(感染ウイルスによる外部ネットワークとの通信など)を遮断したりする機能のことです。ウイルス対策以外の機能も併せ持つ統合型のセキュリティ対策ソフトに、この機能が備わっている場合があります。
お使いのウイルス対策ソフトにこの機能が備わっている場合は、常に最新の状態に保ってください。備わっていない場合は、Windows ファイアウォール機能を有効にして使うことを心掛けてください。ただし、Windows XP のファイアウォール機能は、内部から外部への不正な通信に対応していないことを理解して、内部から外部への不正な通信を遮断できる製品の導入を検討する必要があります。
特に、組織の LAN 内のパソコンが 1 台でもウイルスに感染してしまった場合、パーソナルファイアウォールが十分に機能していないと、組織の LAN の中で感染が一気に拡大する恐れがあります。

(d) USB メモリ経由による感染への対策

USB メモリ利用時は以下のことに注意して、ウイルスの感染を未然に防ぎましょう。

・自身が管理していない USB メモリや所有者の不明な USB メモリは、自身のパソコンには接続しない。
・自身が管理していないパソコンや不特定多数が利用するパソコンには、自身の USB メモリを接続しない。

（4）ウイルスに感染した場合のパソコンの復旧方法

ウイルスに感染してしまい、その後にウイルスを駆除できたとしても、ウイルスによって変更されてしまったシステムの設定などは元に戻っていません。

ウイルス駆除後でもパソコンが正常に動作していないと思われる場合は、「システムの復元」を実施してください。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」が失敗した場合は、パソコンを初期化してください。

（a）「システムの復元」による復旧

Windows XP や Vista には、パソコンの動作が不安定になるなど、使用するのに支障がある場合に、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、任意の日を自動的に選んで保存しているシステムの情報を基に、パソコンを以前の状態に復元するというものです。以下のマイクロソフトのウェブサイトを参考にして、「システムの復元」を行ってください。

ただし、選択した任意の日から現在までに、アプリケーションソフトウェアのインストール、 アップデートなどをした場合は、それらの情報は消えてしまいますので、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)
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(マイクロソフトの「PC とーく」の情報)
http://support.microsoft.com/kb/934854/ja

（b）パソコンの初期化

初期化とは、パソコンを購入した時の状態に戻す作業です。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。

作業する前に重要なデータを、ウイルスに感染していない外部記憶媒体(USB メモリや CD-R、外付け HDD など)にバックアップしてから作業を行ってください。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」
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(届出状況及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)

・OS コマンドインジェクション攻撃で侵入された
・SQL インジェクション攻撃が集中し、ウェブサイトが閲覧しにくくなった

○ 相談の主な事例 (相談受付状況及び相談事例の詳細は、8 頁の「4.相談受付状況」を参照)

・会社でしばらく席をはずしていて、戻って来たらウイルス警告が・・
・ウイルス対策ソフトの契約切れを放置していたらウイルス感染

○ 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。

・脆弱性を突く攻撃と思われる 445/tcp へのアクセスに注意！
・ウェブメールシステムを狙った攻撃と思われる 80/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 15.9 万個**と、12 月の約 17.3 万個から 8.0%の減少となりました。
また、1 月の届出件数(※2)は、**1,860 件**となり、12 月の 1,795 件から 3.6%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。
・1 月は、寄せられたウイルス検出数約 15.9 万個を集約した結果、1,860 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 13.7 万個** 、2 位は **W32/Mytob** で**約 5 千個**、3 位は **W32/Downad** で**約 5 千個**でした。

ウイルス検出数　約15.9万個（約17.3万個）　前月比－8.0%

（注：括弧内は前月の数値）

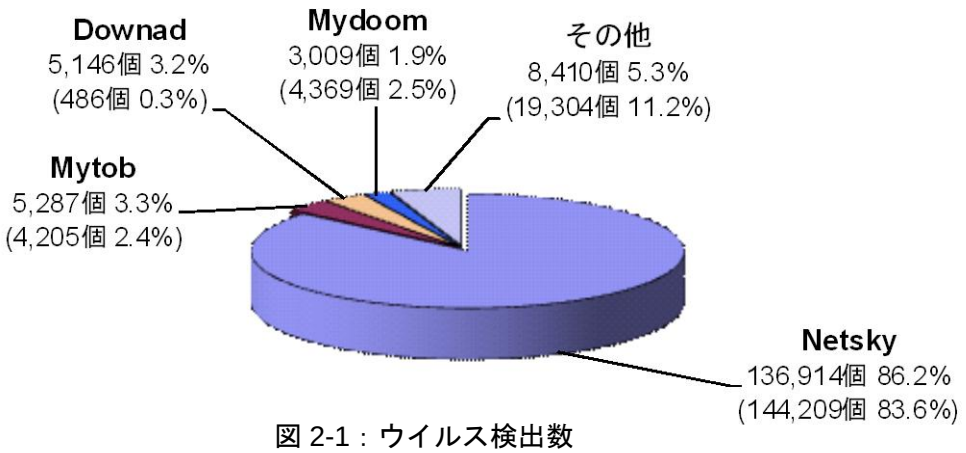


図 2-1：ウイルス検出数

ウイルス届出件数　1,860件（1,795件）前月比 +3.6%

（注：括弧内は前月の数値）

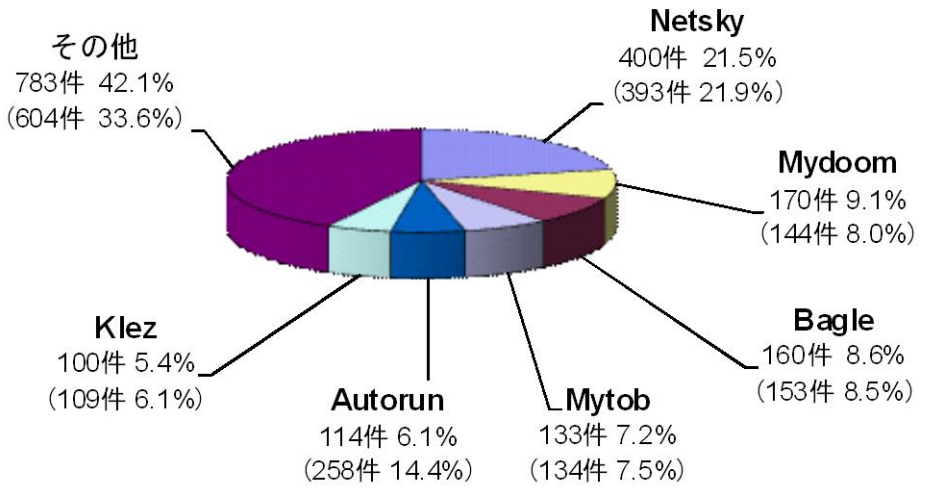


図 2-2：ウイルス届出件数

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

		8月	9月	10月	11月	12月	1月
届出(a) 計		15	14	17	18	10	10
	被害あり(b)	10	12	12	12	7	7
	被害なし(c)	5	2	5	6	3	3
相談(d) 計		25	38	58	39	38	29
	被害あり(e)	13	20	22	19	19	13
	被害なし(f)	12	18	36	20	19	16
合計(a+d)		40	52	75	57	48	39
	被害あり(b+e)	23	32	34	31	26	20
	被害なし(c+f)	17	20	41	26	22	19

(1)不正アクセス届出状況

1 月の届出件数は 10 件であり、そのうち何らかの被害のあったものは 7 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 29 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 13 件でした。

(3)被害状況

被害届出の内訳は、**侵入 3 件、DoS 攻撃 1 件、アドレス詐称 1 件、その他(被害あり)2 件、**でした。

侵入届出の被害は、SQL※インジェクション※攻撃を受け、結果としてデータベース内のデータを改ざんされたものが 2 件、OS コマンドインジェクション攻撃を受け、システム内に被害を受けたものが 1 件、でした。侵入の原因は、3 件全てが、脆弱性を突かれたことによるものでした。

※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。

(4)被害事例

[侵入]

(i) OS コマンドインジェクション攻撃で侵入された

事例	・cron※のレポートメールを確認していたところ、普段は送られて来ない、ログ以外のものが送られて来たのに気付いた。 ・調査したところ、cron の設定ファイルに不正なコマンドが追加されており、そのコマンド実行時にエラーが出ていたことが原因であることが判明。 ・さらに調査を進めたところ、使用せずに放置していた Wiki※システムに脆弱性があり、OS コマンドインジェクション攻撃を受けていたことが分かった。各種ログファイルが削除されたり、バックドアが仕掛けられたりしていた。また、rootkit によって主要コマンドが改ざんされ、侵入しているユーザの存在が隠ぺいされていた。 ・ファイアウォールやファイル改ざん検知システムを導入していたが、今回の攻撃に対しては有効ではなかった。
解説・対策	普段使わないシステムやサービスが稼働していると、セキュリティ対策に抜けが生じやすくなります。**不要なサービスは停止し、必要最小限のものだけ起動し、それらをきちんと管理**しておきましょう。 (参考) 脆弱性対策のチェックポイント http://www.ipa.go.jp/security/vuln/20050623_websecurity.html IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html

※cron : あらかじめ設定しておいたコマンドを、スケジュールに沿って自動実行する UNIX のデーモン(プログラム)のこと。
※Wiki : ウェブブラウザから、ウェブサーバ上のコンテンツを編集することができるようにするシステムのこと。

[DoS]

(ii) SQL インジェクション攻撃が集中し、ウェブサイトが閲覧しにくくなった

事例	・公開ウェブサーバに不具合があり、調査したところ、大量の不正アクセス試行(SQL インジェクション攻撃)を受けていたことがログで判明。 ・幸い、SQL インジェクション攻撃対策が効いて、侵入や改ざんの被害は無かったものの、全体に占める攻撃アクセスの比率が最大で約 75%(通常は 1%未満)に達し、ウェブサーバの負荷が増大してウェブサイト閲覧などに支障が出た。 ・ファイアウォールで、攻撃元の IP アドレスをフィルタしても、状況は変わらなかった。 ・攻撃は、サーバを停止していた定例の休業日明けには、ぱったりと収まっていた。
解説・対策	サーバの負荷を増加させてサービス妨害を仕掛ける攻撃が目的ではなかったようですが、**結果的に DoS 攻撃を受けたような状況と同等**になっています。幸い、この事例では定例のサーバ停止期間後には攻撃が収まっていましたが、**攻撃が継続しているのにサーバを止められない場合には、上位のプロバイダでの対処が有効**になる場合があります。 (参考) JPCERT/CC　技術メモ - サービス運用妨害攻撃に対する防衛 http://www.jpcert.or.jp/ed/2001/ed010005.txt JPCERT/CC　インシデント対応(レスポンス)概要 http://www.jpcert.or.jp/ir/

4. 相談受付状況

1 月の相談総件数は **960 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 **243 件**(12 月 : 194 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 **11 件**(12 月 : 13 件)、**Winny に関連する相談**が **8 件**(12 月 : 6 件)、などでした。(**「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**は **0 件**)

表 4-1　IPA で受け付けた全ての相談件数の推移

	8月	9月	10月	11月	12月	1月
合計	1,616	2,154	1,171	713	839	960
自動応答システム	994	1,302	677	363	458	529
電話	548	755	441	288	331	390
電子メール	69	93	47	62	49	39
その他	5	4	6	0	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。

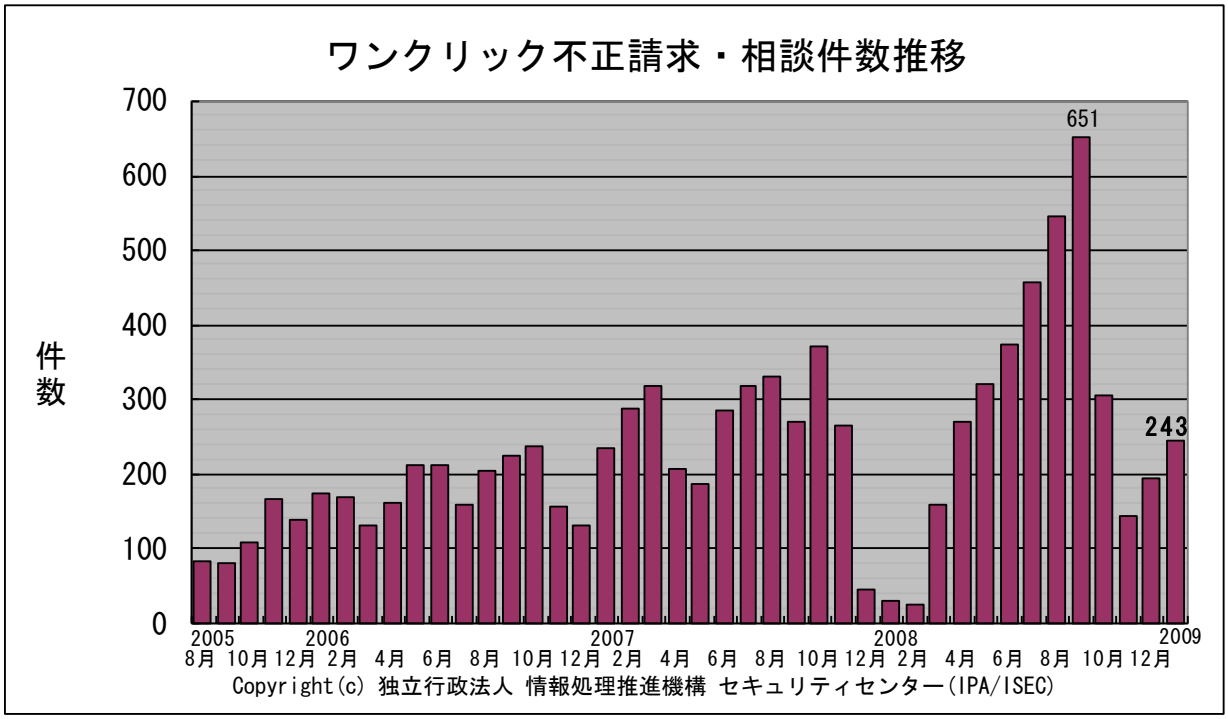


図 4-1　ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

(i) 会社でしばらく席をはずしていて、戻って来たらウイルス警告が・・

相談	会社のパソコン。しばらく席をはずし、戻って来たらパソコンの画面にウイルス警告が出ていた。 ウイルス名：Mal_otorun 1 感染ファイル：autorun.inf 自分では、何か操作した覚えは無い。
回答	検知されたウイルスは、USB メモリを媒介として感染を広げるタイプのものです。**誰かが、USB メモリ感染型ウイルスに感染した USB メモリを、貴方のパソコンに接続して何か操作をしようとし、その際にパソコン側のウイルス対策ソフトで検知された**模様です。 このように、たとえ相手に悪意が無くても、不用意に USB メモリを接続されると自分のパソコンがウイルスに感染してしまう可能性があります。会社で離席する際は、**スクリーンセーバにパスワードを掛け、自分のパソコンが他人に勝手に使われないようにしましょう**。 (ご参考) IPA - 呼びかけ：「外部記憶メディアのセキュリティ対策を再確認しよう！ 」 http://www.ipa.go.jp/security/txt/2008/12outline.html

(ii) ウイルス対策ソフトの契約切れを放置していたらウイルス感染

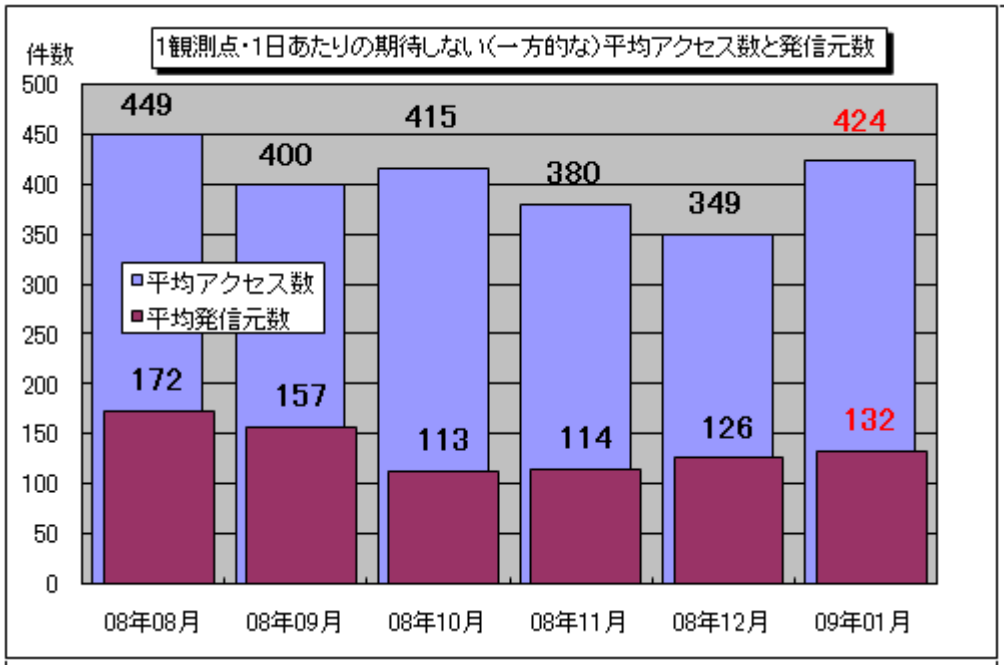
相談	ウイルス対策ソフトの契約が切れたことを示す画面が出ていたが、忙しかったので放置していた。ようやく時間が取れたので、ウイルス対策ソフトの契約を更新した。すぐにウイルス定義ファイルを更新し、パソコン内を手動でウイルスチェックしたら、ウイルスが 42 件も見つかった。
回答	**契約の切れたウイルス対策ソフトでは、日々新しく出現するウイルスの新種を検知することができません**。 ウイルスは、日々新しいものが発見されています。新しいウイルスを検知するためには、最新のウイルス定義ファイルが必要です。最新のウイルス定義ファイルに更新するためには、ウイルス対策ソフトの契約期間内である必要があります。**ウイルス対策ソフトの契約が切れる前に、確実に更新作業をしておきましょう**。 （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 1 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 1 月の期待しない(一方的な)アクセスの総数は 10 観測点で **131,296 件**、総発信元(※)は **41,171 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 132 の発信元から 424 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。



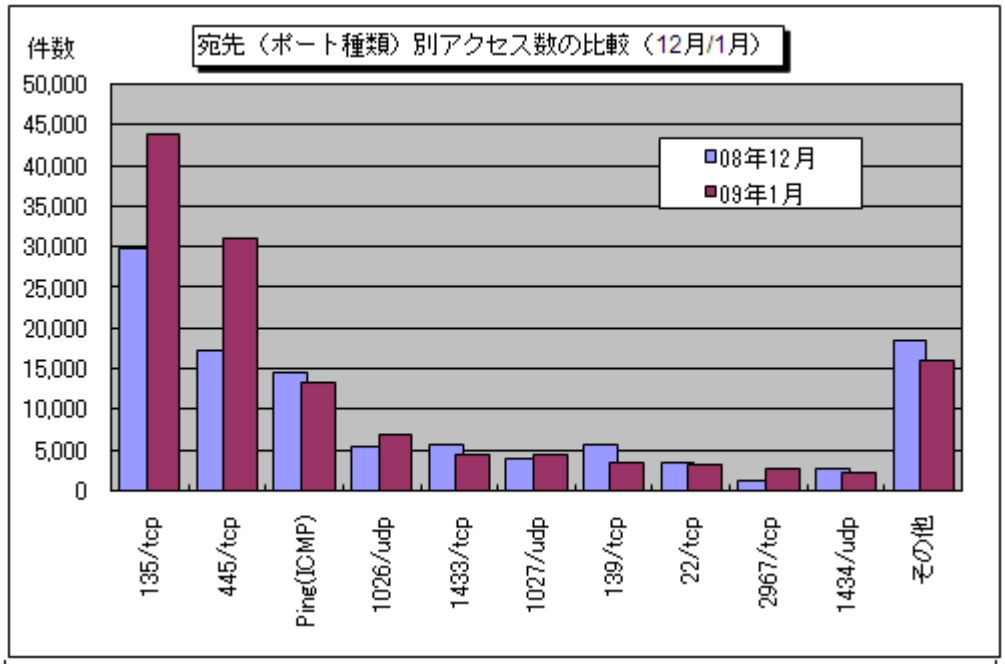
【図 5-1 1 観測点・1 日あたりの期待しない(一方的な)平均アクセス数と発信元数】

2008 年 8 月～2009 年 1 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。1 月の期待しない(一方的な)アクセスは 12 月と比べて増加しました。

2008 年 12 月と 2009 年 1 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。

12 月よりアクセス数が大幅に増加したのは、445/tcp、135/tcp でした。これらのポートは Windows の脆弱性(ぜいじゃくせい)を狙った攻撃を行う際に狙われる可能性が高いポートです。445/tcp へのアクセスの増加については、別紙 3 で説明します。

なお、135/tcp へのアクセスの増加について、詳細の原因は不明ですが、今後も引き続き注意が必要です。



【図 5-2 宛先(ポート種類)別アクセス数の比較(12 月/1 月)】

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/TALOT2-0902.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