プレスリリース
第 10-01-174 号
2010 年 1 月 6 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 12 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 12 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

「忘れないで　あなたのそばの黒い影　対策一つで白い光へ ※」
― 2009 年を振り返り、セキュリティ対策を再確認しよう ―

※　第 5 回 IPA 情報セキュリティ標語・ポスターコンクール（2009 年度実施）　標語中学生の部　入選作品

2009 年のウイルス感染経路について改めて確認すると、2008 年よりも巧妙で広範囲からウイルスを感染させる仕組みになっている様子が伺えます。中でも、改ざんされた企業や個人のウェブサイトを閲覧した利用者のパソコンに感染するウイルスや、USB メモリなどの外部記憶媒体を介して感染が拡大するウイルスは、今現在でも猛威をふるっています。

このようにしてパソコンに感染したウイルスは、他のパソコンに感染を拡げたり、別のウイルスを呼び込んで感染させようとしたりと、感染したパソコンの被害だけでなく、そのパソコンの周囲のパソコンにも被害を及ぼすことになります。

こうしたウイルス感染の被害に遭わないよう、2009 年に起こったウイルス感染の事象を振り返り、ウイルスの感染経路を知って、セキュリティ対策を再確認しましょう。

（1）主な事象の詳細と対策

2009 年に起こったウイルス感染の事象のうち、特徴的な 4 つの事象について説明します。また、それぞれの対策も示します。

（a）改ざんされた企業や個人のウェブサイトを閲覧してウイルスに感染
（b）USB メモリなどの外部記憶媒体を介してウイルスに感染
（c）メールの添付ファイルで送られてくるウイルスに感染（「偽セキュリティ対策ソフト」型ウイルス、特定企業を狙ったメールからのウイルス感染）
（d）悪意あるウェブサイトに誘導されてウイルス等に感染

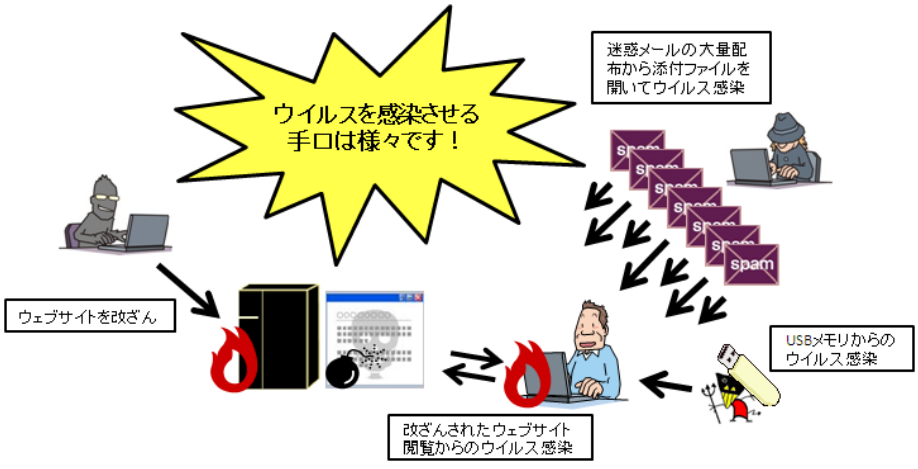


図 1-1：ウイルスを感染させる様々な手口のイメージ図

（a）改ざんされた企業や個人のウェブサイトを閲覧してウイルスに感染

この事象では、悪意ある者がウェブサイト管理者のパソコンから盗んだftp※のアカウント情報（ユーザID、パスワード）でウェブサイトに不正アクセスし、そのウェブサイトの閲覧者にウイルスを感染させるように改ざんします。ftpのアカウント情報が盗まれる手口としては、ウイルス（スパイウェア）に感染させられて、盗まれた事例を確認しています。

改ざんされたウェブサイトの閲覧者は、パソコンに脆弱性（セキュリティホール）が存在する場合、それを悪用されてウイルスに感染させられてしまいます。

感染したウイルスは、利用者のオンラインバンキングやオンラインゲームのアカウント情報などを盗んだり、パソコン内の重要なファイルを破壊したりと、様々な被害を起こす可能性があります。

このウイルスは、2009年5月～6月にかけて世界各地で猛威をふるいました。一旦は終息したと思われましたが、2009年11月頃から再び感染を拡げている状態です。IPAにも、「改ざんされたため修正したウェブサイトが、再び改ざんされた」、「あるウェブサイトにアクセスした途端にウイルスを検知した」など、届出や相談が寄せられています。

ウェブサイト管理者、ウェブサイト利用者は、日ごろから以下の対策を実施するようにしてください。

※ File Transfer Protocol の略。ネットワークでファイルを転送するためのプロトコル。

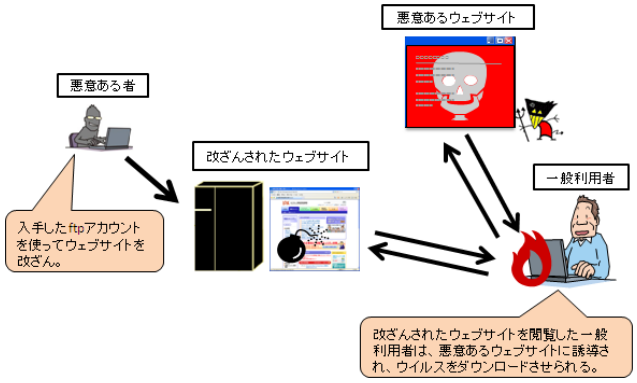


図 1-2：ウェブサイトの改ざんからウイルスに感染するまでの流れ

●ウェブサイト管理者側の対策

・ウェブサイト上の全ページの内容について、身に覚えのないスクリプトが埋め込まれていないか確認しましょう。
・ftpのアクセスログから、管理者がアクセスしていない日時にftpのアクセスがないか確認しましょう。
・ftpでアクセスできるパソコンは、IPアドレスによって制限しましょう。
・ウェブサイト改ざん検知システムやサービスを導入・運用しましょう。

●ウェブサイト利用者側の対策

・アプリケーションソフトの脆弱性（セキュリティホール）を解消しましょう。
（ご参考）
「JVN iPedia 脆弱性対策情報データベース」（Japan Vulnerability Notes）
http://jvndb.jvn.jp/
・ウイルス対策ソフトのパターン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。

ウェブサイト管理者、ウェブサイト利用者とも、下記のウェブページを参照してください。
（ご参考）
「あなたのウェブサイト、改ざんされていませんか？」（IPA）
http://www.ipa.go.jp/security/txt/2009/07outline.html#5

（b）USB メモリなどの外部記憶媒体を介してウイルスに感染

この事象では、USB メモリなどの外部記憶媒体（以下、USB メモリ）を介して、ウイルス感染の被害が拡大していきます。例えば、USB メモリにウイルスが感染している状態で、その USB メモリをパソコンに接続すると、Windows の自動実行機能が悪用されパソコンがウイルスに感染します。パソコンに感染したウイルスは、ネットワークに繋がっているパソコンや、ウイルスに感染したパソコンに接続された他の USB メモリに感染を拡げていきます。場合によっては、感染したウイルスはパソコンの動作を遅くしてしまうこともあります。

このウイルス感染の被害は 2008 年 11 月頃から報告があり、2009 年 2 月～5 月にかけては、民間企業や自治体のパソコンが大規模な被害に遭ったケースがありました。

この手口への対策としては、次の 2 点が有効です。

図 1-3：USB メモリを介してウイルスに感染するイメージ図

●USB メモリ利用時の対策

・自分自身が管理していない USB メモリは、自身のパソコンに不用意に接続しない。
・自分自身が管理していないパソコンや、不特定多数が使用するパソコンには、自身の USB メモリを不用意に接続しない。
・自分自身の USB メモリを、職場で使用しているパソコンに勝手に接続しない、また、職場で使用している USB メモリを、自宅で使用しているパソコンに不用意に接続しない。

●Windows の設定（自動実行機能の無効化）による対策

・ウイルスに感染している USB メモリをパソコンに接続した場合でも、パソコンがウイルス感染しないように、Windows の設定において自動実行機能を無効化することを推奨します。無効化の設定方法は、下記のウェブページを参照してください。Windows 7 の利用者は、Windows Vista の例を参考にしてください。

（ご参考）
「USB メモリのセキュリティ対策を意識していますか？」（IPA）
http://www.ipa.go.jp/security/txt/2009/05outline.html#5

また、次のツールを利用することで、自動実行機能が無効になっているかのチェックができ、設定が有効の場合は、その設定の変更方法を参照することもできます。USB メモリによるウイルス感染を防ぐ手段の一つとして活用してください。

（ご参考）
MyJVN セキュリティ設定チェッカ（Japan Vulnerability Notes）
http://jvndb.jvn.jp/apis/myjvn/#CCCHECK

（c）メールの添付ファイルで送られてくるウイルスに感染

この事象は、メールの添付ファイルをクリックさせることにより、添付ファイルに仕込んだウイルスを感染させようというものです。

こうした手口の例として、2009 年 6 月に、実在する研究機関の名前を騙り新型インフルエンザの注意喚起と偽った、ウイルスが仕込まれた添付ファイル付きメールが特定の企業に送られてきた事例（標的型攻撃）がありました。さらに、2009 年 9 月～12 月にかけては、マイクロソフトから

のセキュリティ対策情報などと偽り「偽セキュリティ対策ソフト」型ウイルスに感染した添付ファイル付きメールが広範囲に大量送信されたことや、政府機関を装い、暗号関連のプロジェクト関係者あてに不審メールが送られたことを確認しました。

この手口では、言葉巧みに情報を聞き出すソーシャルエンジニアリングの手法で様々な文面を使い、なんとかしてメールや添付ファイルを開かせようとします。

この事象への対策として、次のことに気をつけましょう。

●迷惑メールの対策

・普段やり取りがない送信者から添付ファイル付きメールが届いた場合、メールや添付ファイルをすぐに開いたり、本文中に書いてあるリンク先をクリックしたりしない。また、知り合いからのメールであっても、メールの内容が不自然だと感じた場合は、すぐに開いたりせず、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。

・少しでも怪しいと思うメールであれば、メールや添付ファイルを開かずに削除しましょう。

気になるメールタイトルや内容であっても、不用意にメールや添付ファイルを開かないことが重要です。迷惑メールは、多くの人が注目するニュースや季節の催し物に乗じて増えることが予想されます。2010 年は、冬季オリンピックやサッカーの世界大会などがあり、その前後に迷惑メールが増えることが予想されますので気をつけましょう。

（ご参考）

「偽のセキュリティ対策ソフトの脅威が再び拡大！」（IPA）

http://www.ipa.go.jp/security/txt/2009/11outline.html#5

「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！」（IPA）

http://www.ipa.go.jp/security/txt/2009/06outline.html#5

（d）悪意あるウェブサイトに誘導されてウイルス等に感染

この事象は、利用者が芸能ニュースや投稿動画の閲覧サイト、アニメやゲームの情報サイトを閲覧している時に、「もっと詳しい内容はこちら」のように、さらに興味を引く内容が書かれているように思えるリンク先をクリックすることで、悪意あるサイトに誘導されてそのままウイルスに感染させられるというものです。多くの場合、利用者自らがウイルスを取り込むように仕向けられる手口となっています。

このような悪意あるウェブサイトは、アダルトサイトの料金請求画面を表示し続けるものや、広告画面を次々に表示するものが多くなっています。特にアダルトサイトの料金請求画面が消えないという相談は、2009 年も多くありました。

この手口への対策として、次のことに気をつけましょう。

●悪意あるウェブサイトからのウイルス感染対策

・興味本位で、リンク先を不用意にクリックしないこと。

・少しでも怪しいと感じた場合、それ以上クリックをして先に進まないこと。

・悪意あるサイトでは、ページ内にある動画の再生ボタンや「ダウンロード」と書かれた画像などをクリックすると図 1-4 が表示されますが、単に動画の再生や画像を閲覧するだけであれば、こうした画面は表示されません。図 1-4 の「セキュリティの警告」とタイトルに書かれた画面が表示された場合、ここで「実行」をクリックすると、自らウイルスを取り込んでしまい感染することになります。この場合は「キャンセル」をクリックして、先に進まないでください。

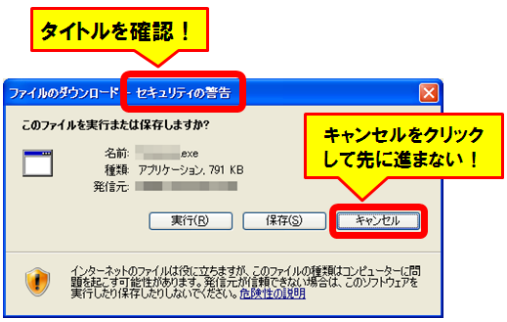


図 1-4：Internet Explorer の「セキュリティの警告」画面の例

アダルトサイトの請求画面が消えないといった内容の詳しい手口については、下記を参照してください。

（ご参考）

「ワンクリック不正請求に関する注意喚起」2009 年 12 月 3 日更新（IPA）

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

「インターネットは自己責任！！『はい』をクリックしたのはあなたです。」（IPA）

http://www.ipa.go.jp/security/txt/2009/12outline.html#5

「あなたのブラウザ、乗っ取られていませんか？」（IPA）

http://www.ipa.go.jp/security/txt/2009/09outline.html#5

（2）共通的対策

2009 年の特徴的なウイルス感染の事象を記しましたが、これらの共通点は、**利用者に気づかれないように巧妙な仕組みで感染させる**ことです。

ウイルスに感染すると、利用者が気づかないうちに他の利用者のパソコンにウイルスを感染させてしまったり、自分はウイルス感染の被害者と思っていたのが、他の利用者のパソコンにウイルスを感染させる加害者になってしまったりと、ウイルス感染に気がつかなければ、大規模な被害をもたらしてしまう可能性があります。

これらウイルスの脅威は、今後も継続すると考えられますので、利用者はこれからもウイルス感染の被害に遭わないためには、絶対に無防備なパソコンでインターネットに接続したり、USB メモリなどを簡単に接続したりすることのないように注意してください。

IPA が従来から注意喚起を続けている基本的な対策を実施することにより、ウイルスによる被害の大部分を防ぐことができますので、利用者は最低限、以下の基本的な対策の実施を心がけてください。

●基本的対策

・利用しているパソコンの OS（オペレーティングシステム）を最新の状態に更新し、脆弱性（セキュリティホール）を解消しておきましょう。また、お使いのパソコンにインストールされているアプリケーションソフト（インターネット閲覧ソフト、メールソフト、動画閲覧ソフト、ドキュメントファイル閲覧ソフトなど）の修正プログラムを適用し、最新のバージョンに更新して脆弱性（セキュリティホール）を解消しておきましょう。

・お使いのウイルス対策ソフトのパターンファイルを最新の状態にして、ウイルス検知機能を有効にして使用しましょう。

なお、万が一、ウイルス感染などでパソコンそのものが動作しなくなる場合に備えて、重要なデータは外部記憶媒体（CD-R などの光学メディアや外部接続 HDD などを推奨）へバックアップしておきましょう。

（ご参考）

Microsoft Update 利用の手順（マイクロソフト社）

http://www.microsoft.com/japan/security/bulletins/j_musteps.mspx

JVN（Japan Vulnerability Notes：脆弱性情報ポータルサイト）

http://jvn.jp/

対策のしおりシリーズ（IPA）

http://www.ipa.go.jp/security/antivirus/shiori.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、8 頁の「3.コンピュータ不正アクセス届出状況」を参照）
- ウェブサイトに不正なコードを挿入された
- オンラインのポイントサービスサイトで、不正に換金された

○ 相談の主な事例 （相談受付状況および相談事例の詳細は、10 頁の「4.相談受付状況」を参照）
- ウイルス対策をしていれば、Windows Update はしなくても良い？
- ファイル共有ソフトで入手したファイルを開いたら、多くのファイルがタコのアイコンになった

○ インターネット定点観測（12 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

12 月のウイルスの検出数（※1）は、**約 6.6 万個**と、11 月の約 7 万個から 5.7%の減少となりました。また、12 月の届出件数（※2）は、**981 件**となり、11 月の 1,140 件から 13.9%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。
・12 月は、寄せられたウイルス検出数約 6.6 万個を集約した結果、981 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 5.4 万個**、2 位は **W32/Mydoom** で**約 4 千 4 百個**、3 位は **W32/Whybo** で**約 3 千 3 百個**でした。

ウイルス検出数 約6.6万個（約7万個） 前月比－5.7%

（注：括弧内は前月の数値）

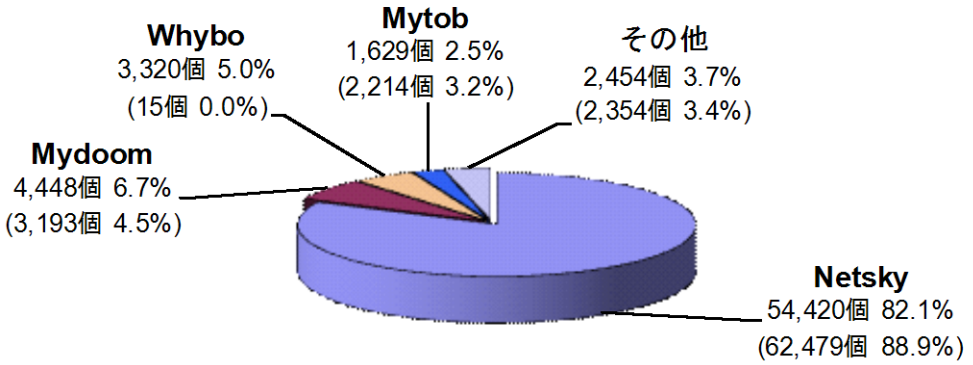


図 2-1：ウイルス検出数

ウイルス届出件数 981件（1,140件） 前月比 －13.9%

（注：括弧内は前月の数値）

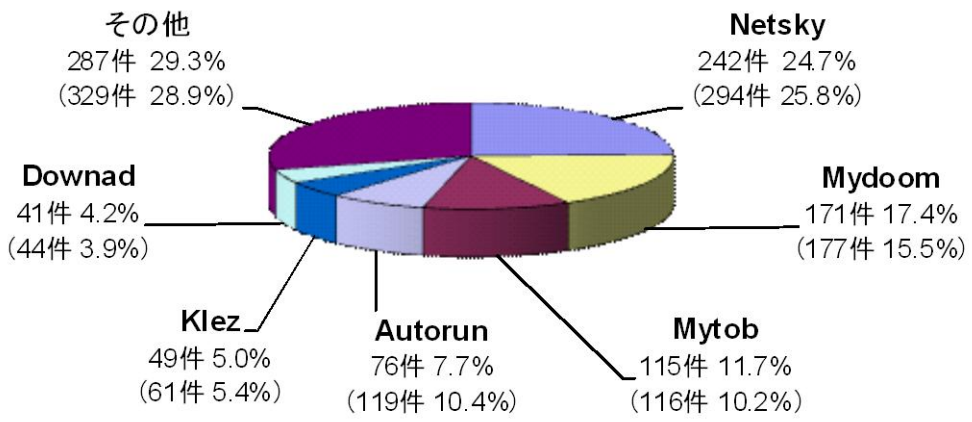


図 2-2：ウイルス届出件数

(2) 不正プログラムの検知状況

2009 年 9 月に急増した「偽セキュリティ対策ソフト」型ウイルス（FAKEAV）の検知件数は、減少傾向にあり、11 月以降、ほとんど確認されないレベルにまで減少しました（図 2-3 参照）。

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推測され、いつ急増するかわかりませんので、継続して注意を払う必要があります。

サイ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。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/

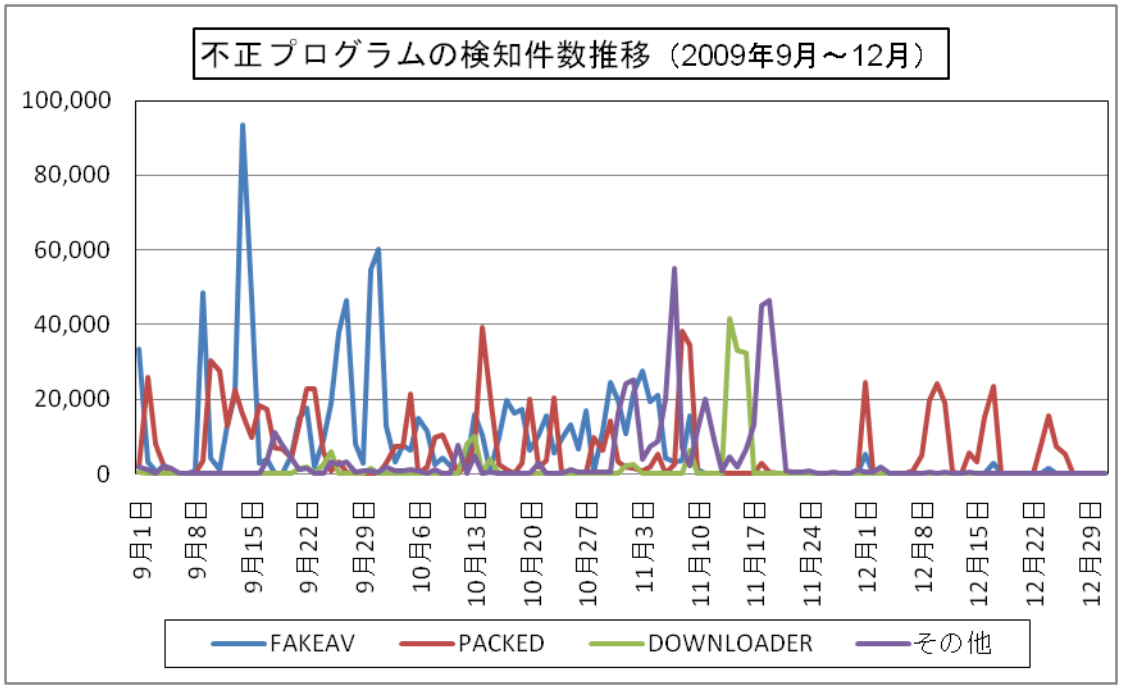


図 2-3：不正プログラムの検知件数推移

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

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

（1）不正アクセス届出状況

12 月の届出件数は 9 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 22 件（うち 5 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 14 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 2 件、その他（被害あり）1 件、**でした。

「侵入」の被害は、ウェブページに不正なコードを挿入されたものが 1 件、ウェブサーバ内にあったメルマガ配信用アドレス情報などが消去されたものが 1 件、ファイアウォールソフトが無効にされたりファイルを改ざんされたりしたものが 1 件、でした。侵入の原因は、ウェブページ更新者のパソコンがウイルス感染してサイト更新用 ftp アクセスのアカウント情報を盗まれたものが 1 件、メルマガ配信用 CGI の脆弱性を突かれたものが 1 件、でした（残りの 1 件は原因不明）。

「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 2 件（オンラインゲーム 1 件、他）でした。

（4）被害事例

［侵入］

（i）ウェブサイトに不正なコードを挿入された

事例	・自身が管理するウェブページが、文字化けして正しく表示されなくなった。 ・調査したところ、サイト更新の際に使う php ファイルなどが改ざんされ、不正なコードを含んだ HTML ファイルを書き出していたことが判明。 ・ウェブページ更新者のパソコンがウイルス感染しており、サイト更新の際に ftp アカウント情報が盗まれたものと推測。それによって、不正アクセスを受けていたと考えられる。 ・サイト更新を許可するパソコンを限定することで対処した。
解説・対策	悪意あるサイトへジャンプさせるためのスクリプトを挿入されたものと思われます。自身の**サイトを閲覧して来た利用者は、同時に悪意あるサイトに誘導され、場合によってはウイルス感染させられてしまう状況であった**と推測されます。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。 （参考） IPA -「 あなたのウェブサイト、改ざんされていませんか？ 」 http://www.ipa.go.jp/security/txt/2009/07outline.html

［なりすまし］

（ii）オンラインのポイントサービスサイトで、不正に換金された

事例	・オンラインでポイントを貯めて、商品と交換したり換金したりできるサービスを利用していた。 ・ある日、ログインできなくなっていることに気付き、サイト運営者に問い合わせたところ、登録してあった自分の連絡先メールアドレスが身に覚えの無いものに変更されていることが分かった。 ・さらに、貯めてあったポイントが全て電子マネーに換金されていた（5000 円分）。
解説・対策	**単にパスワードを推測されてしまったか、パスワードを盗み取るウイルスに感染していたか、という原因が考えられます**。原因が不明な場合は、念のためパソコンは初期化した方が良いでしょう。その上で、パスワードを複雑なものへと変更しましょう。**被害内容の復旧については、サイト運営業者に問い合わせ**ていただくことになります。場合によっては、警察に被害状況を申告するように指示されることもありますので、まずは最寄りの警察署に電話し対処方法について相談してください。なお、ゲーム運営業者に問い合わせても、あまり良い対応を行ってもらえない場合、最寄りの消費生活センターに相談することをお勧めします。 （参考） IPA - 「あなたのオンラインゲームのキャラクターは狙われています！」 http://www.ipa.go.jp/security/txt/2009/10outline.html 「全国の消費生活センター等」（国民生活センター） http://www.kokusen.go.jp/map/ 警察庁 - インターネット安全・安心相談 http://www.npa.go.jp/cybersafety/

4. 相談受付状況

12 月のウイルス・不正アクセス関連相談総件数は **1,794 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 **576 件**（11 月：903 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**（11 月：6 件）、**Winny に関連する相談**が **6 件**（11 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 **1 件**（11 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

	7月	8月	9月	10月	11月	12月
合計	1,708	1,792	1,653	2,049	2,315	1,794
自動応答システム	923	1,015	915	1,157	1,340	1,138
電話	736	702	676	843	918	602
電子メール	47	68	60	45	53	52
その他	2	7	2	4	4	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。

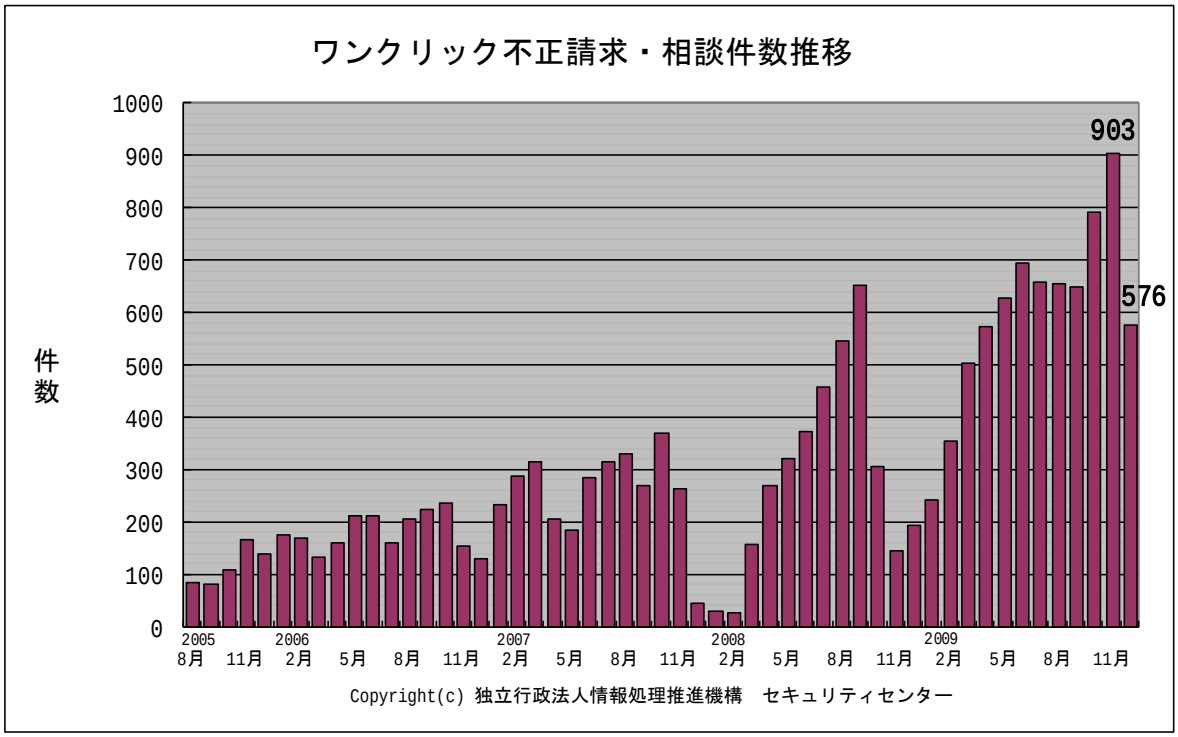


図 4-1：ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

（i）ウイルス対策をしていれば、Windows Update はしなくても良い？

相談	ウイルス対策ソフトを入れているので、Windows Update はしなくても良いのですよね？　もし、それでも Windows Update が必要であるなら、ウイルス対策ソフトは完璧ではないということですか。Windows Update は何かと面倒なので、できればやりたくない。
回答	**ウイルス対策の一環として、Windows Update は必須**です。Windows Update は、セキュリティ上の問題を引き起こす可能性のある個所（脆弱性）を修正するものです。**脆弱性の解消は、全てのセキュリティ対策の基本と言っても良い**でしょう。なお、脆弱性対策は Windows のみならず､全てのアプリケーションについて実施する必要があります。Adobe Flash Player など主要なアプリケーションについては、自動でバージョンチェックができるツールを、IPA が提供しています。 （ご参考） IPA - MyJVN バージョンチェッカ http://www.ipa.go.jp/security/vuln/documents/2009/200911_myjvn_vc.html

（ii）ファイル共有ソフトで入手したファイルを開いたら、多くのファイルがタコのアイコンになった

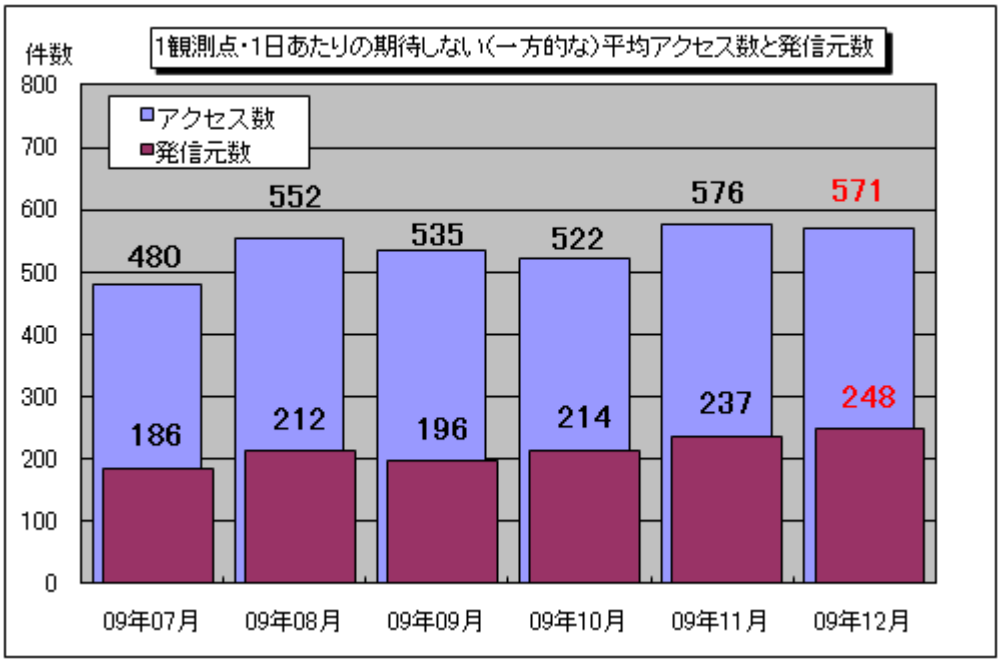
相談	【相談 1】ファイル共有ソフトで映画のファイルをダウンロードした。ファイルを開いたら、パソコンに保管してあった動画や画像**ファイルが全てタコの画像で上書き**されてしまった。 【相談 2】Winny でスクリーンセーバーのファイルをダウンロードした。ファイルを開いたら、パソコンに保管してあった映画などのファイルが全て**イカの画像で上書き**されてしまった。ウイルスチェックしたが、何も検知されない。
回答	ファイルの名前や見た目のアイコンに騙され、ウイルスのファイルを自ら開いて感染したようです。2008 年 2 月の呼びかけで取り上げた「原田ウイルス」と同様に**“破壊型”ウイルスであり、データを元に戻すことは困難**です。 なお、Winny などのファイル共有ネットワークには、原田ウイルスのような“破壊型”の他に、Antinny のような“暴露型”など、凶悪なウイルスが多数流通しています。不特定多数が参加するファイル共有ネットワークは危険だという認識を持つべきです。**ウイルスに感染したくなければ、ファイル共有ソフトを使わないに越したことはありません。** （ご参考） IPA -「気をつけよう 小さな油断 大きな被害」 http://www.ipa.go.jp/security/txt/2008/02outline.html

5. インターネット定点観測での 12 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 12 月の期待しない（一方的な）アクセスの総数は 10 観測点で **176,871 件**、延べ発信元数 (※) は **76,781 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 248 の発信元から 571 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。

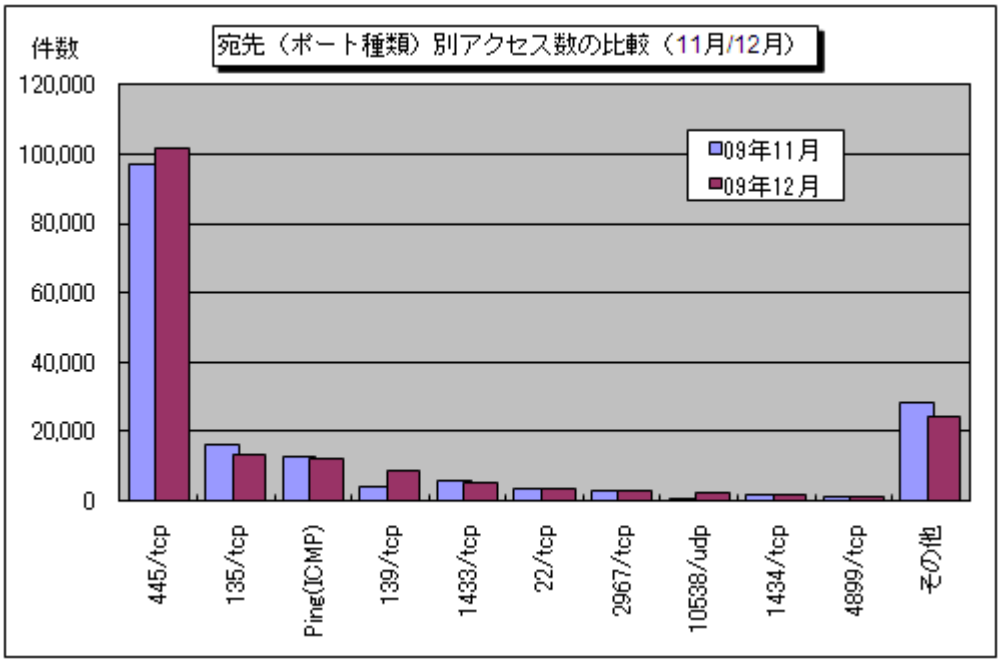


【図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数】

2009 年 7 月～2009 年 12 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。12 月の期待しない（一方的な）アクセスは、11 月と比べてほぼ同程度でした。

11 月と 12 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。11 月に比べ増加率が高かったのは 139/tcp へのアクセスで、11 月の約 2.2 倍でした。これは 11 月の下旬から国内からのアクセスが増加し、その状態が継続していたためです。この時期に国内の発信元からのアクセスが増加していた原因は特定できておりません。

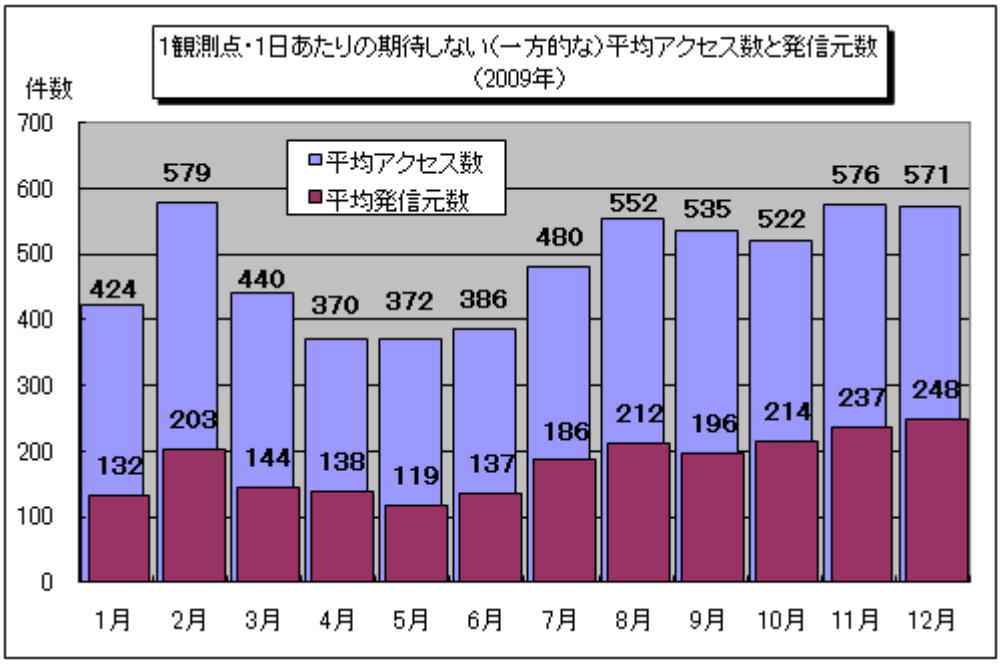
また、これまではそれほど多く観測されていなかった 10538/udp へのアクセスが、12 月 14 日に急増していました。このアクセスが何を目的としたものだったかは不明ですが、多数の発信元から特定の 1 観測点のみで観測されたアクセスでした。



【図 5-2：宛先（ポート種類）別アクセス数の比較（11 月/12 月）】

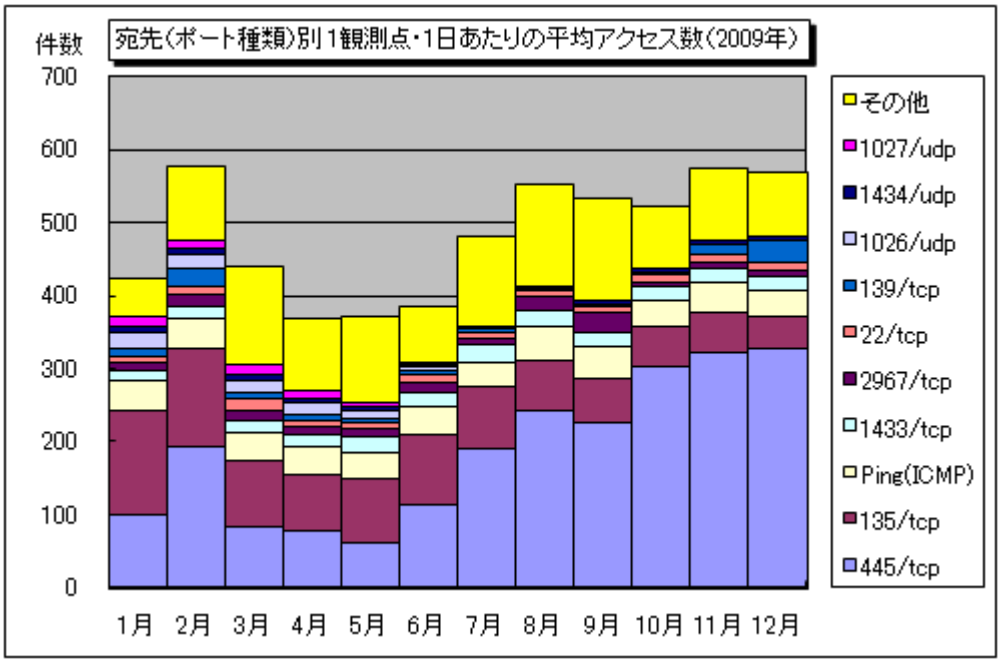
（1）2009 年のアクセス状況

2009 年 1 月～2009 年 12 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 5-3 に示します。アクセス数について年間を通してみると、アクセス数の多かった 2 月からいったん減少しましたが、その後再び増加に転じ、結果的に 2 月の水準まで戻った形と言えます。



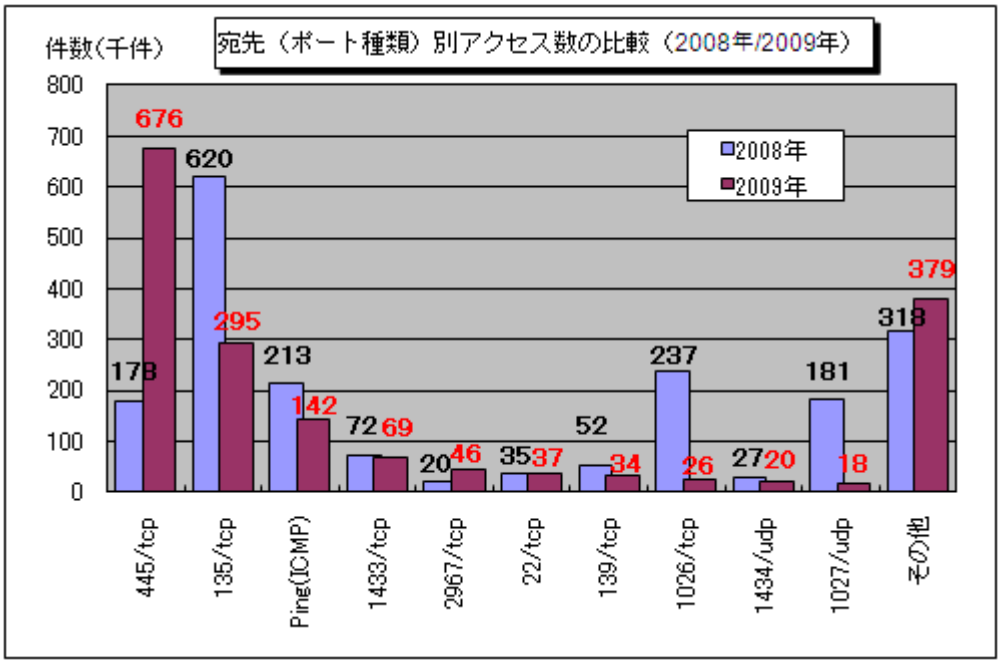
【図 5-3：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数】

図 5-3 の平均アクセス数を宛先（ポート種類）別で表したものを図 5-4 に示します。この図をみると、当初全体のアクセス数に対して支配的だった 135/tcp へのアクセスは次第に減少していきましたが、逆に 445/tcp へのアクセスが顕著な増加傾向を示し、結果的には全体の半数以上を占める形となりました。



【図 5-4：宛先（ポート種類）別 1 観測点・1 日あたりの平均アクセス数（2009 年）】

次に、2008 年と 2009 年の宛先（ポート種類）別アクセス数の比較を図 5-5 に示します。2008 年からアクセス数が大幅に増加したのは 445/tcp であり、約 50 万件の増加（2008 年比で 380%）でした。逆に大幅な減少を示したのは 135/tcp であり、約 33 万件の減少（2008 年比で 48%）でした。また、1026/udp、および 1027/udp へのアクセスについても大幅な減少が見られますが、これはそれまで継続的に観測されていたアクセスが 2009 年 6 月中旬以降ほとんど観測されなくなったためです。



【図 5-5：宛先（ポート種類）別アクセス数の比較（2008 年/2009 年）】

2009 年の TALOT2 のアクセス状況において、特徴的なのは 445/tcp へのアクセスの大幅な増加と言えます。445/tcp へのアクセスは、2008 年 10 月 24 日（日本時間）に Windows の脆弱性情報（MS08-067）が公開されたあたりから徐々に増加しています。2008 年 10 月からの 445/tcp へのアクセス数の変化を図 5-6 に示します。

この脆弱性を悪用して攻撃を行うウイルスとして Downad（別名 Conficker）と呼ばれるウイルスが、脆弱性情報の公開直後から確認されており、このウイルスによる感染被害も国内外問わず報告さ

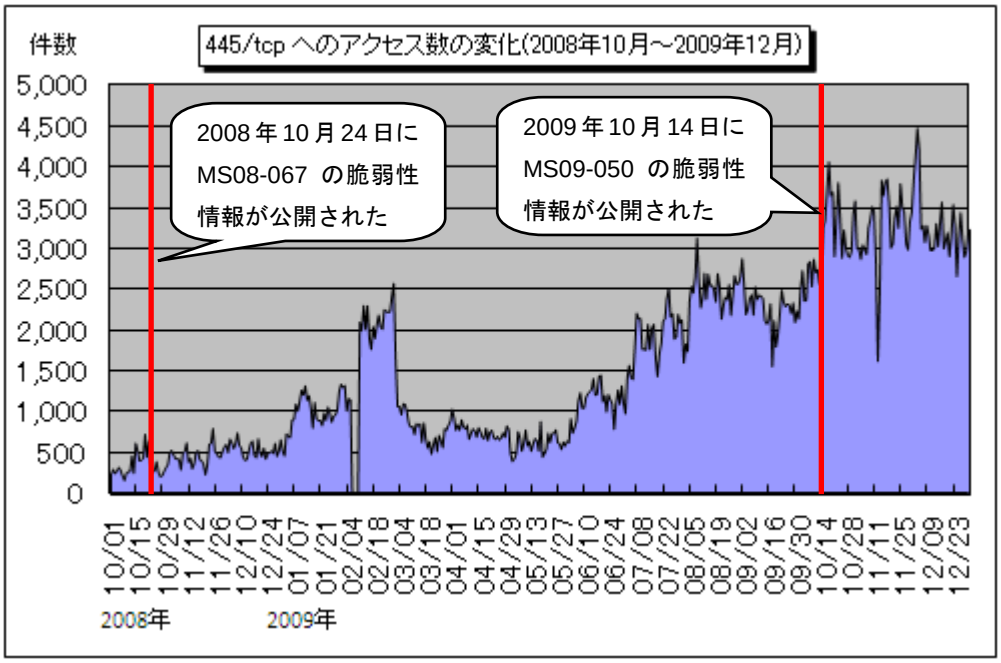
れています。また、USB メモリなどの外部記憶媒体への感染機能を備えるなど、これまでに亜種の発生も複数確認されており、今後もこのウイルスについては継続して注意する必要があります。

（ご参考）
「マイクロソフトセキュリティ情報 MS08-067－緊急」
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
IPA からの呼びかけ－「パソコンの脆弱性、解消されていますか？」
http://www.ipa.go.jp/security/txt/2009/02outline.html

また、2009 年 10 月 14 日（日本時間）には、上記の脆弱性以外にも 445/tcp にアクセスすることで悪用される脆弱性情報（MS09-050）が公開されました。このように 2009 年は、複数の脆弱性に対する攻撃と思われる行為が絡み合って 445/tcp へのアクセスが増加していたと考えられます。

（ご参考）
「マイクロソフトセキュリティ情報 MS09-050－緊急」
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

※2009 年 2 月 6 日～9 日は、TALOT2 のメンテナンスのため、システムを停止しています。



【図 5-6：445/tcp へのアクセス数の変化（2008 年 10 月～2009 年 12 月）】

Windows の脆弱性を悪用した攻撃による被害を防ぐための対策は、Microsoft 社から毎月提供される修正プログラムを迅速、且つ確実に適用させることです。併せて、ウイルス感染による被害に遭わないために、ウイルス対策ソフトを常に最新の状態にして使うことが基本的な対策となります。

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/TALOT2-1001.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