プレスリリース
第 10-37-197 号
2010 年 10 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 [2010 年 9 月分] について

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、2010 年 9 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

「 迷惑メールをはじめとした様々な経路で拡散する新たなウイルスが出現！ 」

2010 年 9 月上旬、複数のセキュリティ関連組織から「迷惑メールで拡散する新たなウイルスが流行している」と注意喚起が発せられました。この新たなウイルスは、「大量メール送信型ウイルス」という、無差別に送られるメールを通じて感染を拡げるウイルスの一種で、かつ、メール以外の経路でも他のパソコンへ感染を拡げる機能を持っていました。その後、このウイルスは海外において一時的に感染が流行しましたが、現在は収束しています。

メールで感染を拡げるウイルスは過去にも多くの例があり、対策の技術が進んでいるため、今回の事例では早期に事態が収束したと考えられます。しかし、一時的とはいえ感染が流行したことは事実であり、パソコン利用者は自身における対策状況を改めて確認し、漏れがある場合には確実に対策をする必要があります。

ここでは、この新たなウイルスの概要や挙動について示すとともに、改めて利用者側の基本的な対策を説明します。

（1）新たなウイルスの概要

今回流行したウイルスには様々な別名がありますが、ここでは VBMania（ブイビーマニア）と呼びます※1。

VBMania ウイルスは、図 1-1 に示すような仕組みで感染を拡大しようと試みます。

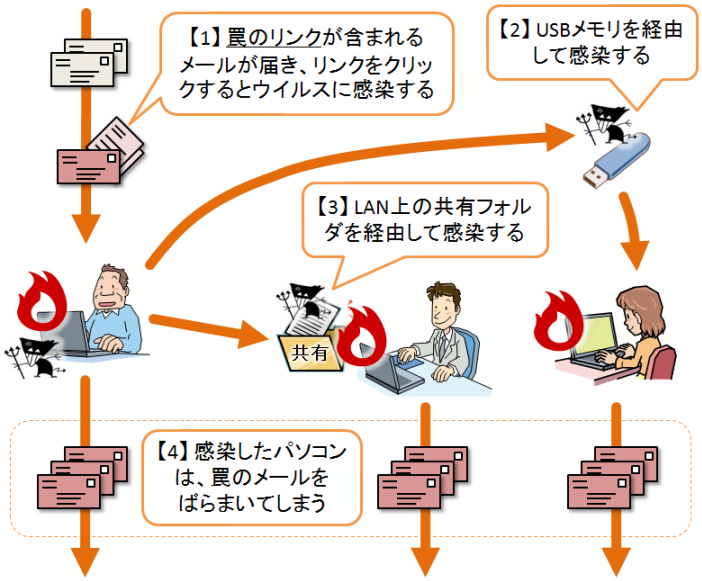

図 1-1：VBMania ウイルスの感染の仕組みのイメージ図

※1　ウイルスの名称は複数のセキュリティベンダーが別々に決めるため、様々な別名を持つ場合があります。今回のウイルスは、「Win32/Swisyn.worm.290816」「Email-Worm.Win32.VBMania.a」「W32.Imsolk.B@mm」「EmailWorm（0019e4ae1）」「WORM_MEYLME.B」「Worm:Win32/Visal.B」「W32/VBMania@MM」などという名称が付けられています。これらは、全て同じウイルスを指しています。

（2）VBMania ウイルスの詳細

IPA にて解析を行った VBMania ウイルスの一検体について、その挙動を解説します。

【1】罠のリンクが含まれるメールによる感染

まず、利用者に対して、文中に罠のリンクが含まれるメール（**罠のメール**）が届きます。そのリンク先は、一見 PDF ファイル※2 や動画ファイルに見えるよう細工されています（図 1-2）。また、メールの送信元のメールアドレスは、利用者の知人のものである可能性があります。

利用者がこの罠のリンクをクリックしてしまうと、VBMania ウイルスのダウンロードが行われます※3。この時、更に Windows やメールソフトの警告画面が表示されるかもしれませんが、それを無視して操作を続けると、ウイルスに感染させられてしまいます。

今回の場合、メールの件名は「Here you have」「Just for you」「hi」などが確認されており、メールの本文は英語で書かれていました。

※2　PDF ファイル…「Adobe Reader」などのソフトで閲覧できる文書ファイルの一種。

※3　2010 年 10 月 5 日現在、ダウンロード先がアクセス不能となっており、機能しない状態となっています。ただし、ダウンロード先が再びアクセス可能になる可能性はゼロではないため、安全というわけではありません。

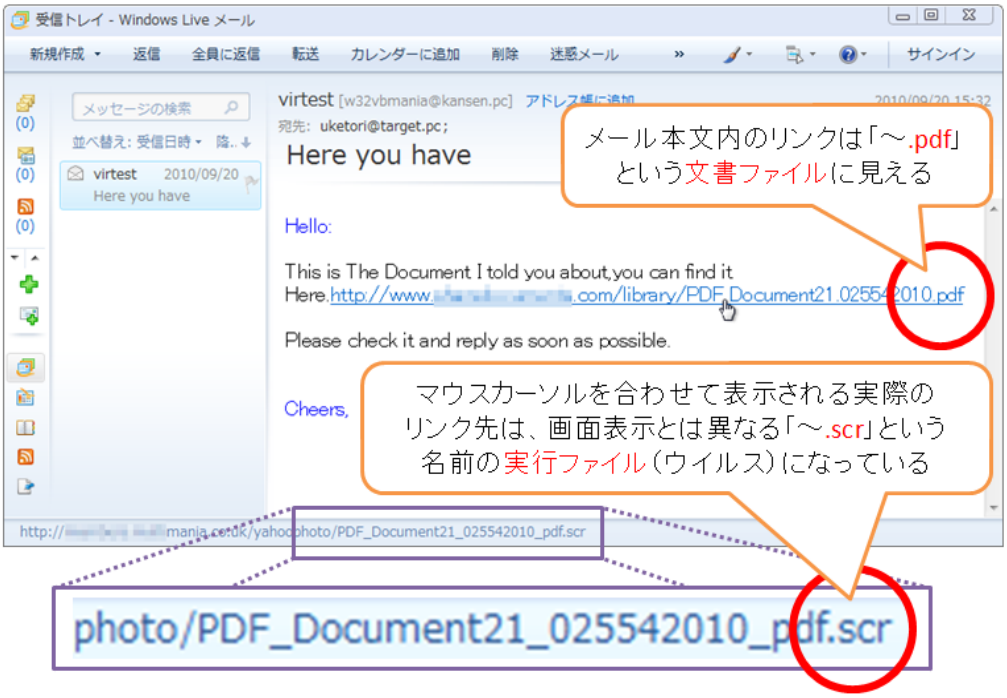

図 1-2：VBMania ウイルスの罠のメールの一例（「Windows Live メール」での表示）

このようにして VBMania ウイルスに感染させられたパソコンを起点として、続いて【2】～【4】で示す感染拡大活動が行われることが分かりました。

【2】USB メモリを経由する感染

ウイルスに感染したパソコンに USB メモリなどを接続すると、ウイルスはそこに自分自身のコピーを作成し、Windows の「自動実行」機能を悪用する細工を施します。

その USB メモリを、「自動実行」機能を無効化していない他の Windows パソコンに接続すると、そのパソコンもウイルスに感染させられてしまいます。

【3】LAN 上の共有フォルダを経由する感染

ウイルスに感染したパソコンから、家庭内／企業内ネットワーク（LAN）上の他のパソコンに対して、「共有フォルダ」の機能を通じて、ウイルスファイルのコピーが行われる場合があります。コピーされたウイルスファイルの外見は、PDF ファイルなどに偽装されています。

他のパソコンで、いつの間にか置かれているこのウイルスファイルをダブルクリックして開くと、そのパソコンもウイルスに感染させられてしまいます。

【4】罠のメールの無差別送信による感染拡大

ウイルスに感染したパソコンから、利用者の意図に反して、パソコン内のメールソフト※4のアドレス帳に登録してあるメールアドレスに対して、罠のメール（【1】で説明したもの）が送信されてしまいます。その際のメールの差出人には、同じくメールソフトに登録してある利用者自身のメールアドレスが使われます。この感染活動の繰り返しにより、大量の罠のメールが流通することになります。

※4　解析結果よりマイクロソフト社のオフィス製品に付属している「Outlook」というソフトのデータが悪用されることを確認していますが、他のメールソフトが狙われる可能性もあります。

その他の悪意のある動作

その他、本ウイルスは次の悪意のある動作を行います。

- パソコンにインストールされているウイルス対策ソフトやセキュリティソフトの動作を妨害し、無効化させようとします。
- インターネットから別のウイルスをダウンロードし、パソコンに感染させようとします※5。

※5　2010 年 10 月 5 日現在、上記「※3」と同様、ダウンロード先はアクセス不能となっています。

参考として、本ウイルスに関して技術的な情報を掲載している、各セキュリティソフトベンダーのウェブページを次に示します。

（ご参考）

「ViruslistJP.com - ウイルス分析」（カスペルスキー社）
http://www.viruslistjp.com/viruses/alerts/?alertid=203996091

「W32.Imsolk.B@mm | Symantec」（英語）（シマンテック社）
http://www.symantec.com/business/security_response/writeup.jsp?docid=2010-090922-4703-99

「ソースネクスト・スタイル・セキュリティ」（ソースネクスト社）
http://sec.sourcenext.info/vsinfo/?code=0818

「WORM_MEYLME.B - 概要」（トレンドマイクロ社）
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_MEYLME.B

「Encyclopedia entry: Worm:Win32/Visal.B」（英語）（マイクロソフト社）
http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3aWin32%2fVisal.B

「W32/VBMania@MM | ウイルス情報 | マカフィー」（マカフィー社）
http://www.mcafee.com/japan/security/virV.asp?v=W32/VBMania@MM

（3）事前対策

VBMania ウイルスのように、感染拡大にメールを使う手口自体は新しいものではなく、今後も同様の手口を使うウイルスが出現する可能性があります。図 1-3 に示すように、多段階の基本的なウイルス対策／迷惑メール対策を実施することが効果的です。

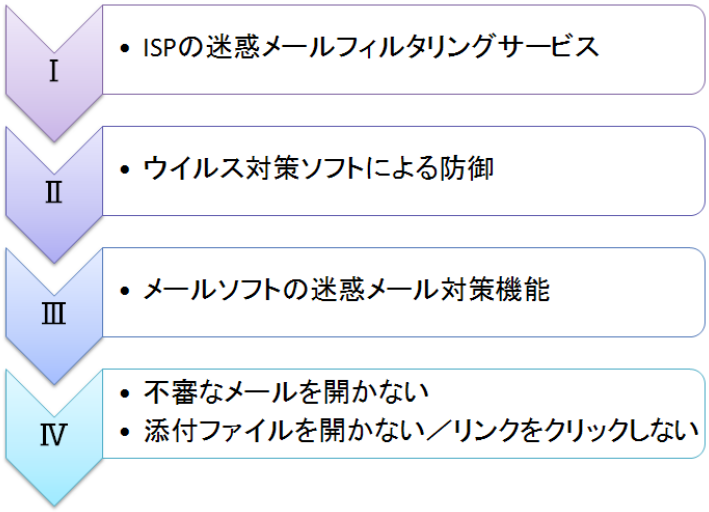

図 1-3：迷惑メールなどへの多段階の対策

（Ⅰ）ISP が提供する迷惑メールフィルタリングサービスの利用

ISP（インターネット接続業者）が「迷惑メールフィルタリングサービス」といったサービスを提供している場合があります。このサービスでは、広告や出会い系への勧誘等の迷惑メールの他、ウイルス感染の危険があるメールも届かないようにブロックする効果が得られる可能性があります。

サービスの内容などについて、契約中の ISP へ確認し、サービスの利用を検討してください。

（Ⅱ）ウイルス対策ソフトによる防御

ウイルス対策ソフトは万能ではありませんが、重要な対策の一つです。ウイルス対策ソフトを導入し、ウイルス定義ファイルを最新に保つことで、ウイルスの侵入阻止や、侵入したウイルスの駆除ができます。近年のウイルスは、パソコンの画面の見た目では感染していることが分からないものが多いため、ウイルスの発見と駆除には、ウイルス対策ソフトが必須です。

一般利用者向けのウイルス対策ソフトとしては、ウイルスの発見と駆除だけでなく、罠のメールに書かれたリンクから危険なウェブサイトへ誘導された際にブロックを行う機能などを備える、**「統合型」**と呼ばれるものを推奨します。

（Ⅲ）メールソフトの迷惑メール対策機能の利用

メールソフトに、「迷惑メール対策」といった機能が付いている場合があります。こちらも、ISP による「迷惑メールフィルタリングサービス」と同様に、罠のメールの回避に効果が得られる可能性があります。

「迷惑メール対策」機能とは、不要なメールや罠のメールを「迷惑メール」（または「スパムメール」など）といったフォルダに振り分けてくれる機能です。この機能の設定方法については、使用しているメールソフトのマニュアルやヘルプ等を参照してください。

なお、この設定を行うと、必要な（迷惑メールではない）メールが「迷惑メール」として誤判断され、見落としてしまう可能性もありますので、注意してください。

（Ⅳ）不審なメールを開かない・クリックしない

様々な対策を行っていても、手元に罠のメールが届いてしまうことは十分にありえます。基本的なことですが、身に覚えのないメールについては開かないようにし、添付ファイルやメール内のリンクをクリックしないよう注意してください。

過去に罠のメールの件名に日本語を使うウイルスの事例もあったため、日本語だからといって油断はできません。罠のメールには、興味を引く内容や、何かの料金請求に見せかけたもの、あるいは「これはあなたの写真ですか？」という言葉など、クリックさせて罠にかけるための工夫が施されています。

また、メールを操作している時、セキュリティの警告画面等が表示された場合は、警告に書かれている内容をよく確認し、危険そうであれば「キャンセル」やウインドウの×ボタンを押して、先に進まないようにしてください。

【補足】「USB メモリ感染型ウイルス」への対策

（2）の【2】で説明したとおり、VBMania ウイルスは USB メモリ等を経由した感染拡大機能を持っているため、「USB メモリ感染型ウイルス」の一種であるとも言えます。この種のウイルスに対しては、Windows に搭載されている「自動実行」機能を無効化することで、「USB メモリを接続しただけで感染」という危険を避けることができます。

「自動実行」機能の無効化は、VBMania ウイルス以外の「USB メモリ感染型ウイルス」への対策にもなりますので、Windows XP または Windows Vista をお使いの方は、次のウェブページを参考に対策を行ってください※6。

※6　Windows 7 では「自動実行」機能が無効化されているため、対策は不要です。

（ご参考）

「Windows での「自動実行」機能の無効化手順」（IPA）

http://www.ipa.go.jp/security/virus/autorun/

（4）感染時の対処

VBMania ウイルスに感染した疑いがある場合、ウイルス対策ソフトが無効化されている可能性があります。また、感染している間に接続した USB メモリ、外付けハードディスク、携帯音楽プレイヤーや、家庭内／企業内ネットワーク上のパソコンに、ウイルスのコピーが作られている可能性があります。

いくつかのセキュリティソフトベンダーから、無償で利用可能な駆除ツールが提供されているため、まずはウイルスの駆除を試みてください。

なお、この VBMania ウイルス自体は駆除できても、破壊された環境が完全に戻るとは言いきれません（例えば、無効化されたウイルス対策ソフトを元に戻せるかは分かりません）。ウイルスを一旦駆除したら、**重要なデータのバックアップを取得し、パソコンを初期化する（買った時の状態に戻す）ことを勧めます。**

参考として、各セキュリティソフトベンダーの駆除ツールのウェブサイトを紹介します。

（ご参考）

「Kaspersky Virus Removal Tool 2010」（カスペルスキー社）

http://support.kaspersky.com/viruses/avptool2010

※「Installation Guide of Kaspersky Virus Removal Tool 2010」というリンクから駆除ツールの説明ページに進むことができます。

「W32.Imsolk.B@mm Removal Tool | Symantec」（シマンテック社）

http://www.symantec.com/ja/jp/business/security_response/writeup.jsp?docid=2010-091320-4721-99

「マカフィー株式会社 | McAfee Labs (旧 AVERT) | ウイルス駆除ツール」（マカフィー社）

http://www.mcafee.com/japan/security/stinger.asp

※「W32/VBMania@MM Stinger」というリンクから駆除ツールがダウンロードできます。

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）
- ウェブアプリケーションの脆弱性を突かれ、ウェブコンテンツを改ざんされた
- ftp アカウント情報が漏れて、ウェブコンテンツを改ざんされた？

○ 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）
- Security Tool というソフトウェアの画面が表示されて、パソコンが正常に動かない
- 子どもがアダルトサイトを閲覧してしまい、請求画面が表示されるようになった

○ 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

9 月のウイルスの検出数※1 は、**約 3.4 万個**と、8 月の約 4.5 万個から 23.1%の減少となりました。また、9 月の届出件数※2 は、**1,082 件**となり、8 月の 1,177 件から 8.1%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。
・9 月は、寄せられたウイルス検出数約 3.4 万個を集約した結果、1,082 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 2.7 万個**、2 位は **W32/Mydoom** で**約 4 千個**、3 位は **W32/Waledac** で**約 1 千個**でした。

ウイルス検出数 約3.4万個（約4.5万個） 前月比 －23.1%

（注：括弧内は前月の数値）

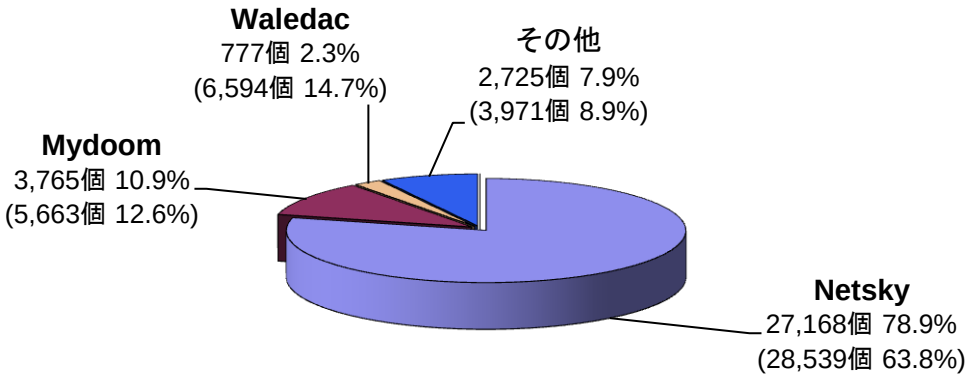

図 2-1：ウイルス検出数

ウイルス届出件数 1,082件（1,177件）前月比 －8.1%

（注：括弧内は前月の数値）

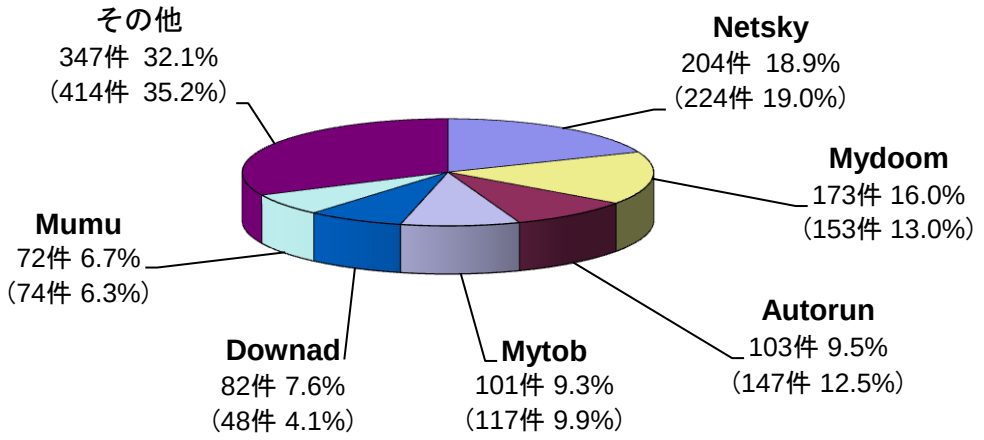

図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

2010 年 9 月の不正プログラムの検知状況は、MALSCRIPT や FAKEAV が急増した事例が確認されました（図 2-3 参照）。MALSCRIPT は、ホームページなどの HTML ファイルに悪質なスクリプトが含まれている場合に検知される名称になります。このような HTML ファイルを脆弱性のあるパソコンで閲覧すると、自動的にウイルスがダウンロードされ、感染してしまう可能性があります。日頃から、脆弱性対策を実施しておくことを勧めます。

なお、FAKEAV は偽セキュリティ対策ソフトです。

（ご参考）

IPA ― 「"ガンブラー" の手口を知り、対策を行いましょう」※1.(5)対策を参照
http://www.ipa.go.jp/security/txt/2010/02outline.html

IPA -「 深刻化する偽セキュリティ対策ソフトの被害！ 」
http://www.ipa.go.jp/security/txt/2010/06outline.html

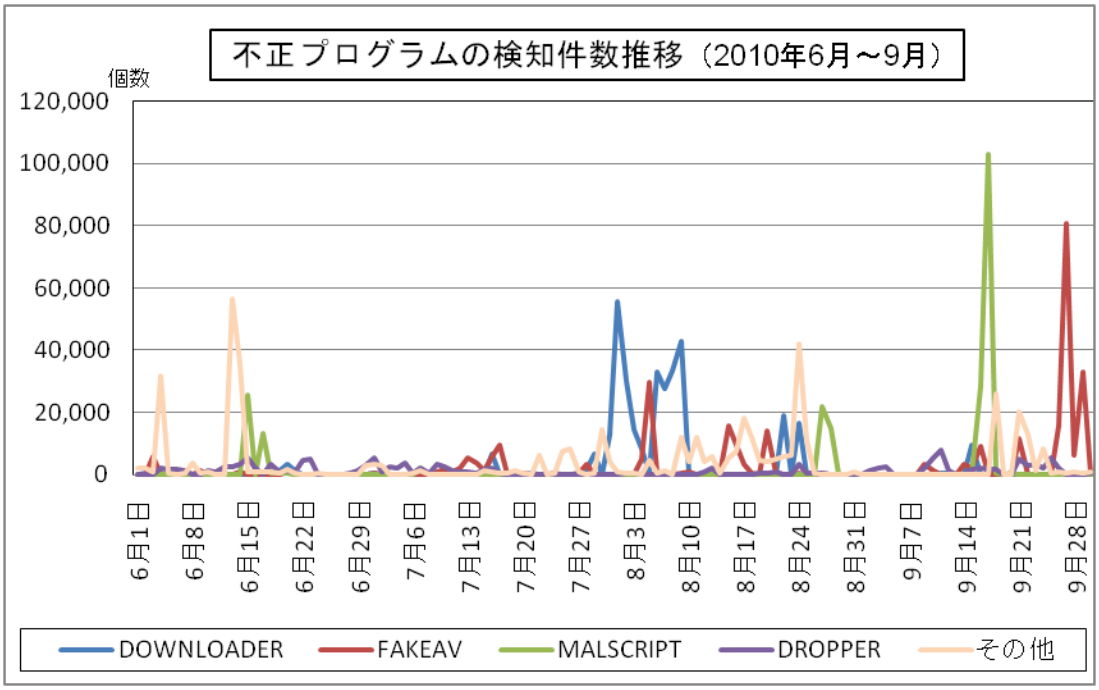

図 2-3：不正プログラムの検知件数推移

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

		4月	5月	6月	7月	8月	9月
届出(a) 計		11	8	15	14	18	15
	被害あり(b)	10	5	13	9	12	10
	被害なし(c)	1	3	2	5	6	5
相談(d) 計		39	52	77	44	56	47
	被害あり(e)	16	22	50	23	16	8
	被害なし(f)	23	30	27	21	40	39
合計(a+d)		50	60	92	58	74	62
	被害あり(b+e)	26	27	63	32	28	18
	被害なし(c+f)	24	33	29	26	46	44

（1）不正アクセス届出状況

9 月の届出件数は 15 件であり、そのうち何らかの被害のあったものは 10 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 47 件（うち 6 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 8 件でした。

（3）被害状況

被害届出の内訳は、**侵入 5 件、DoS 攻撃 2 件、不正プログラム埋め込み 2 件、その他（被害あり）1 件**でした。

「侵入」の被害は、ウェブページが改ざんされていたものが 3 件、外部サイトを攻撃するツールを埋め込まれて踏み台として悪用されていたものが 2 件、でした。侵入の原因は、脆弱なパスワード設定が 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）、ウェブアプリケーションの脆弱性を突かれたものが 1 件、でした（他は原因不明）。

「不正プログラム埋め込み」の被害は、組織の LAN に接続しているパソコンがウイルスに感染し、外部ネットワークなどにアクセスを試みていたものが 2 件でした。

※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）ウェブアプリケーションの脆弱性を突かれ、ウェブコンテンツを改ざんされた

事例	・ウェブコンテンツに改ざんの形跡を発見。身に覚えのない、外部サイトを自動的に参照する iframe タグが挿入されていた。 ・調査したところ、ウェブサイト上で使っていた CMS（Contents Management System）のプラグインに脆弱性があるらしく、そこを突かれて結果的にウェブコンテンツが改ざんされたらしいことが判明。 ・今後は、WAF（Web Application Firewall）を導入してセキュリティを強化する予定。
解説・対策	ウェブアプリケーションの脆弱性はよく狙われますが、そのプラグインもプログラムの一つであり、同様に脆弱性対策が必要となります。土台となるウェブアプリケーションのバージョン管理はもちろん、プラグインについても常に最新版に更新しておくなど、確実なバージョン管理を実施しましょう。 （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

（ii）ftp アカウント情報が漏れて、ウェブコンテンツを改ざんされた？

事例	・自社のウェブコンテンツを閲覧していた所、一部に、身に覚えのない表示（外国語に見えるが、文字化けかもしれない）を発見。 ・同時に、ウイルス対策ソフトが「トロイの木馬が検知されました」との警告を出した。 ・調査したところ、ウェブコンテンツ更新用の ftp サーバのログに、不審なアクセス 1 件を発見。前後の時間関係より、このアクセスで改ざんされたものと推測。 ・ウェブコンテンツは一旦全て削除し、新たにアップロードし直した。 ・なぜ ftp アカウント情報が漏れていたのかは不明。
解説・対策	改ざんの内容は不明ですが、**原因は ftp サーバへの不正アクセスによる侵入のようです**。いまだにガンブラー型攻撃と同様の手法が続いているということです。**ガンブラー型攻撃の手口を復習するとともに、適切な対策を実施しましょう**。 （参考） IPA - 2010 年 4 月の呼びかけ「ウェブサイトの管理方法を再確認しましょう！」 http://www.ipa.go.jp/security/txt/2010/04outline.html

4. 相談受付状況

9 月のウイルス・不正アクセス関連相談総件数は **2,102 件**でした。そのうち**『ワンクリック請求』に関する相談**が **820 件**（8 月：935 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 **13 件**（8 月：15 件）、**Winny に関連する相談**が **3 件**（8 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 **2 件**（8 月：2 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

	4月	5月	6月	7月	8月	9月
合計	2,110	1,881	1,983	2,133	2,432	2,102
自動応答システム	1,194	1,091	1,022	1,142	1,298	1,142
電話	835	714	829	924	1,053	872
電子メール	81	76	129	66	75	85
その他	0	0	3	1	6	3

※ 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。

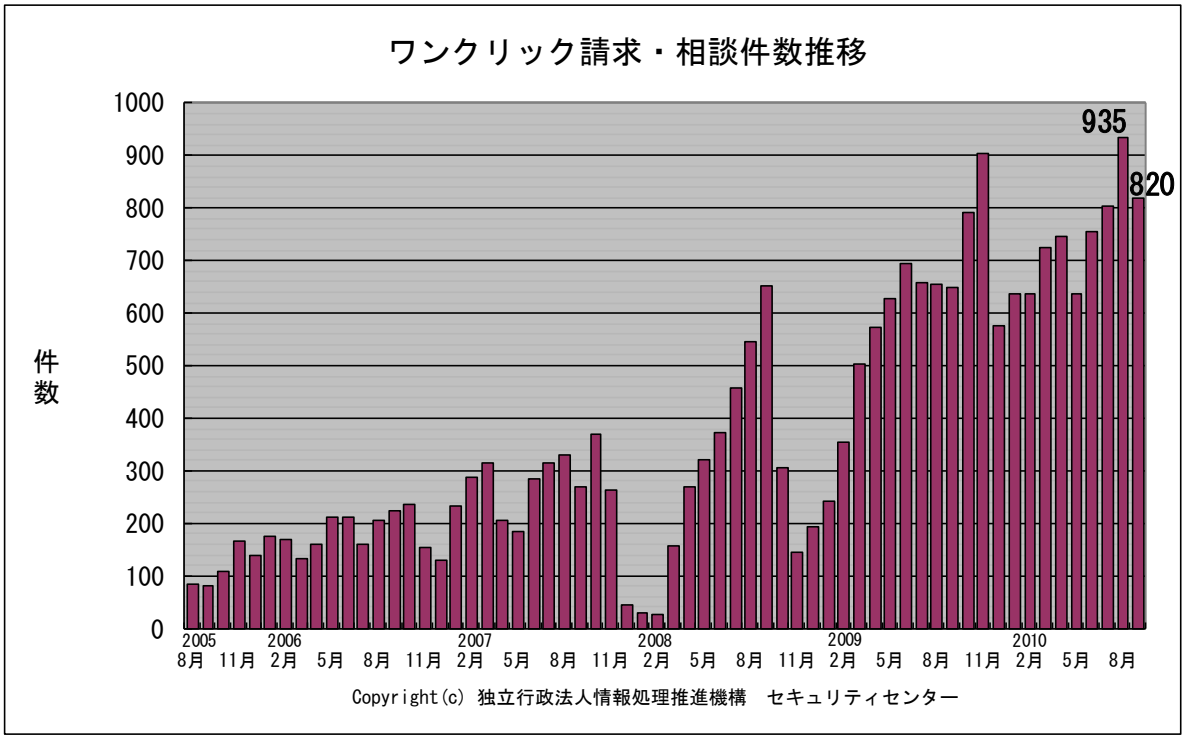

図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）Security Tool というソフトウェアの画面が表示されて、パソコンが正常に動かない

相談	いつも使用しているインターネット通販サイトを閲覧していたら、画面右下から英語で書かれたバルーンメッセージが表示された。何かと思い、そのメッセージをクリックしたところ、Security Tool という身に覚えのないソフトウェアの画面が表示されて、その後もパソコンを起動するたびに表示されるようになった。ホームページを見ていたりすると、この画面が出てきてパソコンが正常に動かなくなることがある。どうしたらこのソフトウェアを削除できるのか。
回答	相談者はいわゆる、**偽セキュリティ対策ソフト型ウイルス**の感染被害に遭っています。これは、9 月 24 日に発生した事件（某広告配信サーバが不正アクセスによって改ざん）により、この広告配信を受けていた多くのウェブサイトを閲覧しただけでこうしたウイルスに感染してしまう状態になっていたことが原因と思われます。解決策としては、OS が Windows XP、Vista、7 であれば、**システムの復元機能を使って、パソコンを Security Tool 画面が表示された日よりも前の日の状態まで戻すことをお勧め**しています（詳細は下記サイトを参照）。システムの復元が正常に完了したら、正規のウイルス対策ソフトを使用してパソコン内をウイルスチェックしておきましょう。セーフモードからでもシステムの復元機能が正常に動かない場合は、パソコンの初期化をすることになります。**正規のウイルス対策ソフトは、ほとんどの偽対策ソフト型ウイルスの感染被害を防いでくれますので、最新の状態にして使用しましょう。** （参考） IPA ‐ 2010 年 6 月の呼びかけ「深刻化する偽セキュリティ対策ソフトの被害！」 http://www.ipa.go.jp/security/txt/2010/06outline.html

（ii）子どもがアダルトサイトを閲覧してしまい、請求画面が表示されるようになった

相談	・子どもが動画サイトからアダルトサイトへ行ってしまい、何回か OK ボタンをクリックしたところ、請求画面が表示される様になった。 ・子どもが興味半分でアダルトサイトを見てしまい、訳もわからずにクリックをしていたら請求画面が張り付いて消えなくなった。 （このほか、同様の事例が多数あり）
回答	**ワンクリック請求の被害相談は、老若男女を問わず寄せられています。**こうした被害は、アダルトサイトを興味本位でクリックして進んでいけば、未成年者であろうと簡単に遭遇してしまいます。解決策としては、OS が Windows XP、Vista、7 であれば、システムの復元機能を使って、パソコンを請求画面が表示された日よりも前の日の状態まで戻すことをお勧めしています。 **未成年者が使用するパソコンには、有害サイトをブロックするサービスやソフトウェアを導入することで、保護者が許可しないサイトへのアクセスを未然に防止することができます。**また、様々な機能を持った「統合型」ウイルス対策ソフトと呼ばれるものには、有害サイト閲覧防止機能を持っているものが多いですので、これから購入される方にはお勧めです。 （参考） IPA ‐ ワンクリック請求に関する注意喚起 http://www.ipa.go.jp/security/topics/alert20080909.html

5. インターネット定点観測での 9 月のアクセス状況

インターネット定点観測（TALOT2）によると、2010 年 9 月の期待しない（一方的な）アクセスの総数は 10 観測点で **115,566 件**、延べ発信元数※は **48,095 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 160 の発信元から 385 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。

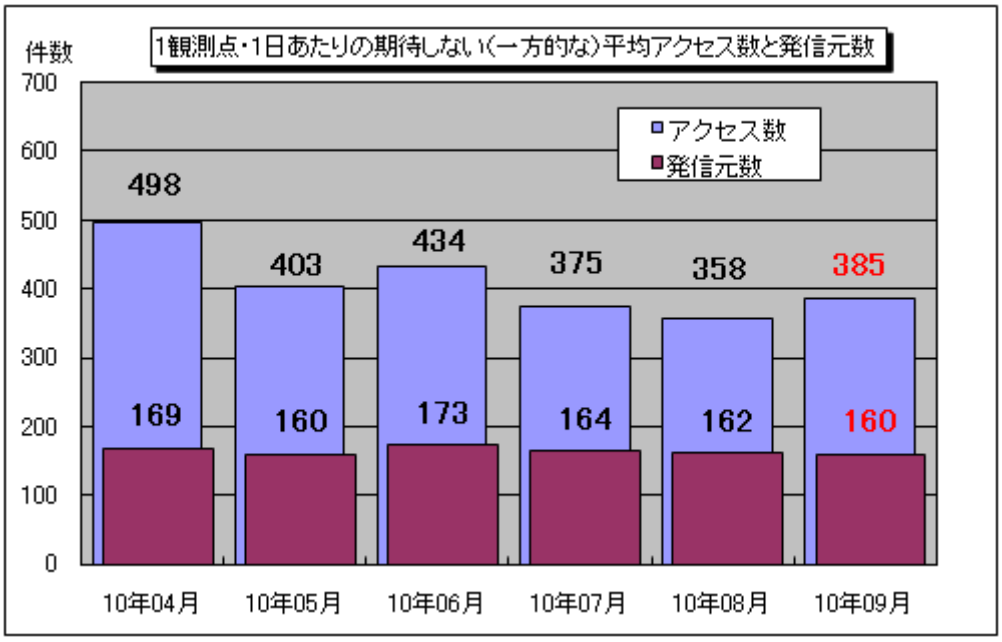

図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数

2010 年 4 月～2010 年 9 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。9 月の期待しない（一方的な）アクセスは、8 月と比べて増加しました。

8 月と 9 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。これをみると、8 月に比べて大幅に増加していたのは、17500/udp と 9415/tcp へのアクセスでした。

17500/udp については、2010 年 4 月頃にも一時期増加が観測されており、今回も以前と同様に TALOT2 の特定の 1 観測点に対して同一セグメント内の複数の IP アドレスから規則的な間隔で送られていたという特徴がありました。このポートに対してブロードキャストを送信する一般利用者向けのソフトウェアの存在が確認されていることから、このソフトウェアを使用しているパソコン利用者による通信であった可能性があります。複数の IP アドレスから送られていたのは、当該パソコンがネットワークに接続する度に IP アドレスが変化していたためと思われます。なお、他の観測点ではブロードキャストが到達しない仕様のようなので、当該アクセスは観測されていません。

9415/tcp については、2010 年 5 月頃に一時的な増加を観測し、その後減少したかに見えましたが、8 月後半から再び増加してきました。このアクセスは TALOT2 の複数の観測点に対して海外（主に中国）の複数の発信元からのアクセスが多いという特徴がありました（図 5-3 参照）。このポートに関しては中国のあるサイトで公開されている、プロキシ機能を持つソフトウェアがこのポートで待ち受けを行うことが確認されており、可能性として悪意ある者がこのソフトウェアを踏み台としてウェブサーバ等へ

の攻撃に使うために、このソフトウェアがインストールされたパソコンを探索していたものだったと考えられます。

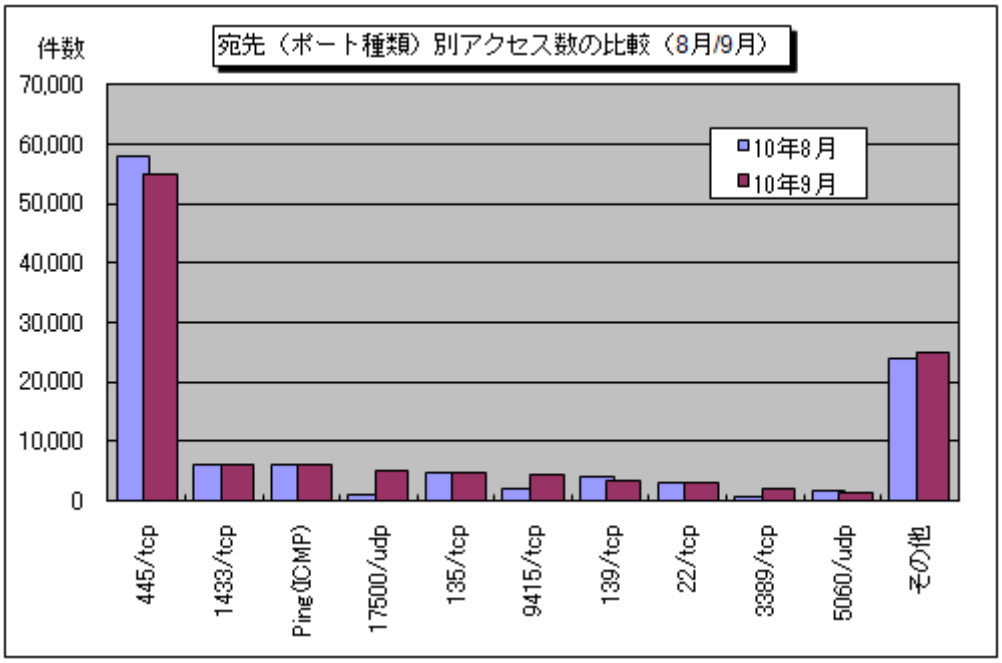

図 5-2：宛先（ポート種類）別アクセス数の比較（8 月/9 月）

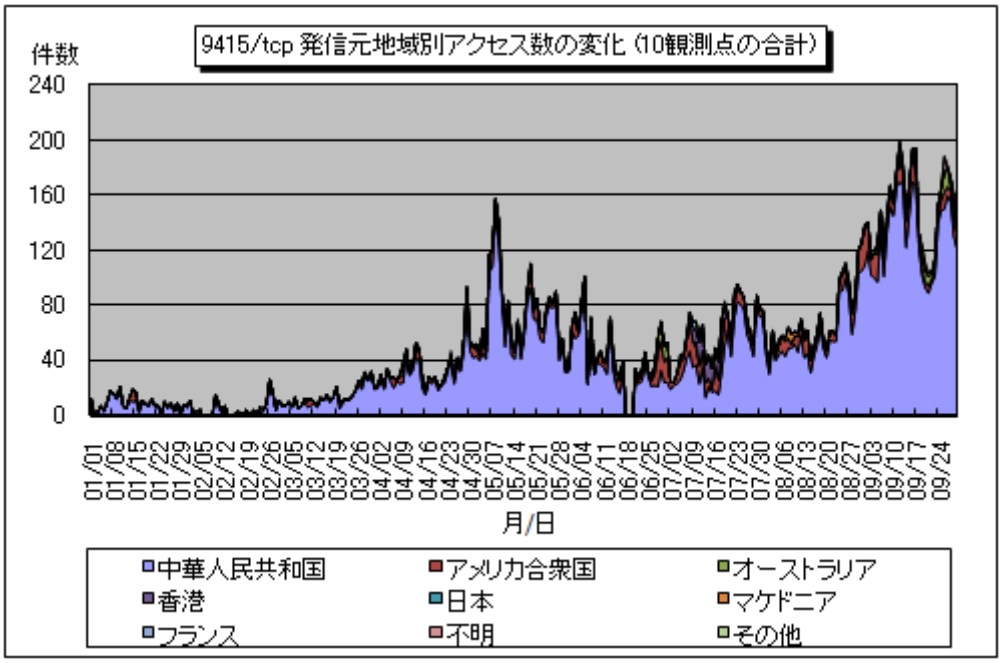

図 5-3：9415/tcp 発信元地域別アクセス数の変化（10 観測点の合計）

※6 月 18 日～20 日は保守作業のため、システムを停止しています。

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/TALOT2-1010.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　加賀谷／花村／古川
Tel:03-5978-7527 Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp