プレスリリース
第 09-05-144 号
2009 年 3 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 2 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 2 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

「ウイルスは進化しています！日々のセキュリティ対策を怠らずに！」
― ますます進むウイルスの”多機能化” ―

W32/Virut と呼ばれるウイルスの IPA への届出が、2008 年末から徐々に増えています。このウイルスが初めて IPA に届出されたのは 2006 年 8 月であり、比較的古いウイルスであると言えますが、当初より感染・拡散機能が強化された亜種が活発に活動し、感染が拡大している可能性が考えられます。

お使いのパソコンが W32/Virut に感染した場合、Windows が正常に動作するために必要なシステムファイルが破壊されてしまい、正常な状態に戻す事が困難になります。

このようなウイルス感染の被害に遭わないために、Windows Update などにより、お使いのパソコンの脆弱性（ぜいじゃくせい）を確実に解消しておくとともに、ウイルス対策ソフトなどを使った対策を、しっかりと実施しましょう。また、万が一ウイルス感染の被害に遭った場合に備えて、重要なデータのバックアップを定期的に行いましょう。

（1）W32/Virut の特徴

IPA への W32/Virut ウイルスの届出件数は、最近 1 年間ではほぼ毎月上位 10 位以内に位置しています。また、外部機関の報告からも、W32/Virut の亜種が多数検出されていることが分かります。

(ご参考)
「2008 年 12 月度　サイバークリーンセンター活動実績」
https://www.ccc.go.jp/report/200812/0812monthly.html

IPA で W32/Virut の亜種を解析した結果を基に、特徴を説明します。以下の方法で感染と拡散を繰り返し、活動範囲を広げていきます。

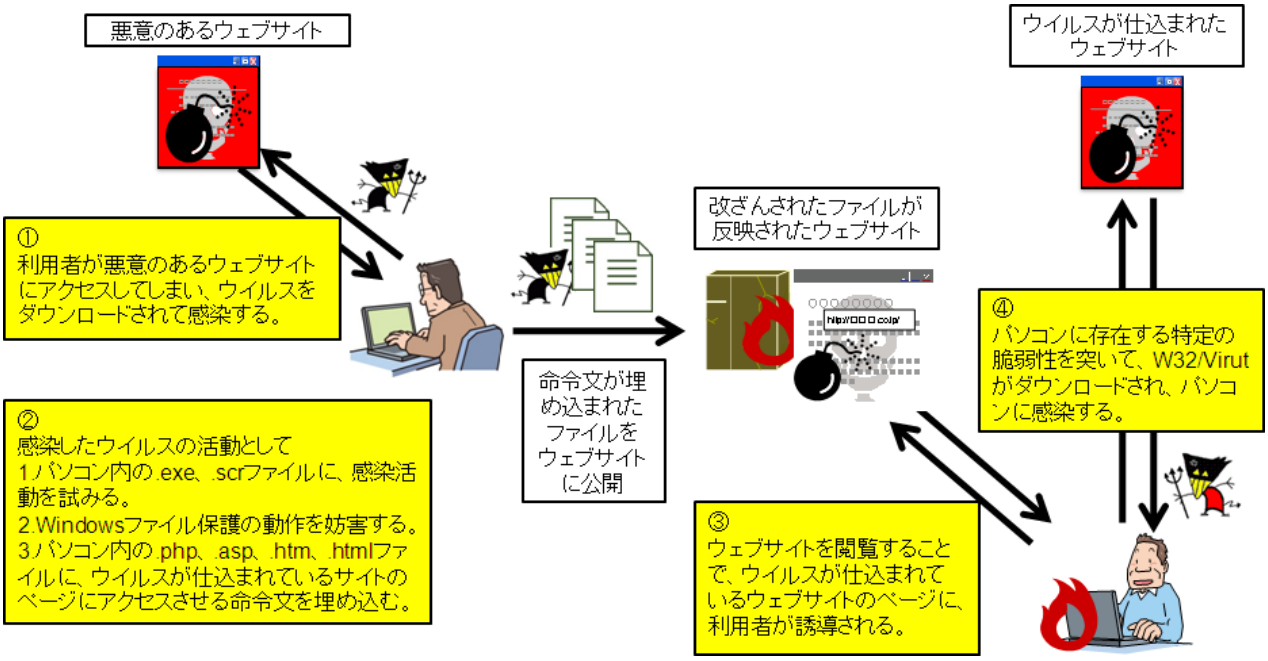


図 1：W32/Virut の感染活動

(a) まず、利用者が誘導されるなどして、悪意あるウェブサイトより W32/Virut ウイルスをパソコンにダウンロードさせられることによって感染します(図 1 の①)。感染したウイルスは、パソコン内にある、「exe」(※1)、「scr」(※2)の拡張子を持つファイルに対して感染活動を行います(図 1 の②の 1.)。ただし、ウイルス自身の動作に支障を来たすプログラムファイルには感染しません。

※1 exe：実行形式のプログラムやアプリケーションを示す拡張子
※2 scr：Windows で使われるスクリーンセーバーを示す拡張子

(b) 感染したウイルスは、さらにパソコン内にある「php」、「asp」、「htm」、「html」の拡張子を持ったファイルに、W32/Virut が仕込まれているウェブサイトにアクセスさせる命令文を埋め込み、拡散活動を行います(図 1 の②の 3.)。
これらのファイルは、主にホームページを作成する時に使用するため、命令文を埋め込んだままアップロード、公開してしまうことになります。
このウェブサイトにアクセスをすると、その利用者のパソコンに、W32/Virut が感染してしまう可能性があります(図 1 の③)。
この時、W32/Virut はアクセスをした利用者のパソコンに対して、特定の脆弱性が存在するかを解析し、存在すればその脆弱性を利用して W32/Virut を感染させます(図 1 の④)。

このようにして、W32/Virut は最初に感染した利用者以外のパソコンに対しても、ウイルス感染の被害に遭わせるということを認識してください。

(2) 主な被害内容

今回 IPA で解析した W32/Virut の亜種に感染した場合、次の被害が発生することが確認されています。

(i)パソコンの中にあるプログラムファイルやスクリーンセーバーファイルに感染が広がる。
(ii)Windows ファイル保護(※3)機能の動作が妨害される。
(iii)Windows ファイアウォールの設定が無効にされる。
(iv)パソコン内にある、「php」、「asp」、「htm」、「html」の拡張子を持ったファイルに対して、悪意のある外部のウェブサイトにアクセスさせる命令文が埋め込まれ、ファイルが改ざんされる。

※3 Windows ファイル保護：パソコンが正常に動作するために必要なファイルを、勝手に置き換えられないように保護する、Windows の機能のこと。

(i)の結果、パソコン内に感染ファイルが増えてしまい、駆除が困難になってしまいます。さらに(ii)により、Windows が正常に動作するために必要なシステムファイルへの感染行為を阻止できなくなり、結果としてパソコンの動作が不安定になる可能性があります。また(iii)により、パソコンの防御が薄くなってしまい、危険な状態になります。もし、感染者がホームページを作成し公開していた場合、(iv)により悪意あるサイトへのリンクが含まれたページを公開することになってしまい、そのホームページを閲覧した利用者のパソコンにも被害が及ぶ可能性があります。

このような被害を受けてしまった場合、パソコンが正常に動作する保障はなく修復も困難になるため、パソコンを購入した時の状態に戻すしか、パソコンを正常な状態に戻す方法はありません。

(3) 対策

(a) 感染予防策

まず、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てください。また、W32/Virut は、感染しようとするパソコンに脆弱性があるか解析し、あれば感染活動を開始しますので、OS やご使用の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てください。そのほかに、重要なデータは、

ウイルスに感染してしまってもすぐ復旧できるように、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）へバックアップをしておきましょう。

(b) 感染後の対応

(2)でも記しましたが、ウイルスの被害を受けてしまった場合、パソコンを正常な状態に復旧させることは非常に困難です。また、たとえウイルスの駆除が成功し、正常に復旧できたとしても、W32/Virut は駆除されると別のウイルスに変化し、利用者の気付かない所で、さらに他のウイルスをダウンロードしようとする機能があることも確認しています。つまり、このウイルスに感染した場合は、影響がどこまで及んでいるか分からない状態になるということです。よって、W32/Virut の感染が確認された場合は、**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」
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
「ボット対策について」(IPA)
http://www.ipa.go.jp/security/antivirus/bot.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、5 頁の「3.コンピュータ不正アクセス届出状況」を参照)
・SQL インジェクション攻撃でデータを改ざんされた

○ 相談の主な事例 (相談受付状況及び相談事例の詳細は、7 頁の「4.相談受付状況」を参照)
・友人からもらった USB メモリからウイルス感染？
・あるソフトを使い続けたいため、OS を最新の状態にアップデートしたくない

○ インターネット定点観測(9 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。
・Symantec 製品の脆弱性を狙った 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 12.8 万個**と、1 月の約 15.9 万個から 19.1%の減少となりました。
また、2 月の届出件数(※2)は、**1,463 件**となり、1 月の 1,860 件から 21.3%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。
・2 月は、寄せられたウイルス検出数約 12.8 万個を集約した結果、1,463 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 11.3 万個** 、2 位は **W32/Mytob** で**約 5 千個**、3 位は **W32/Mydoom** で**約 2 千個**でした。

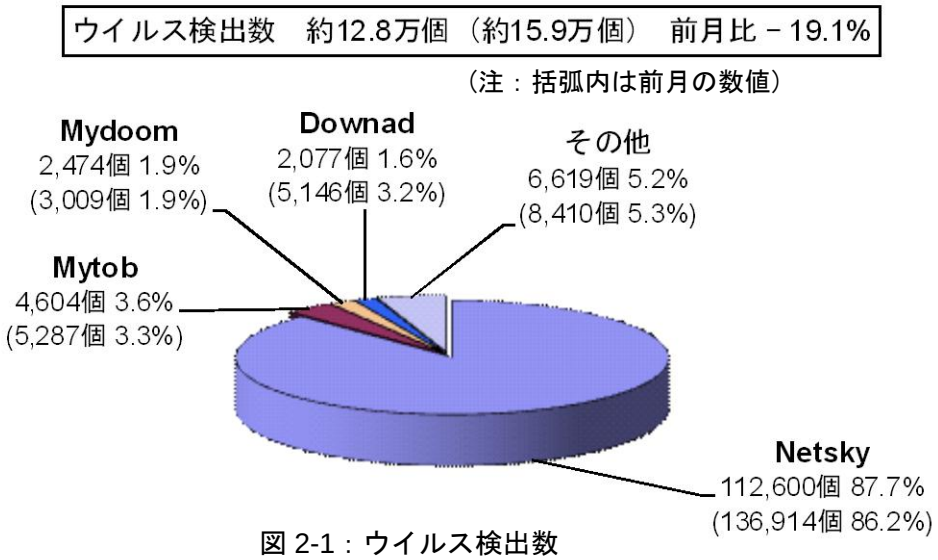


図 2-1：ウイルス検出数

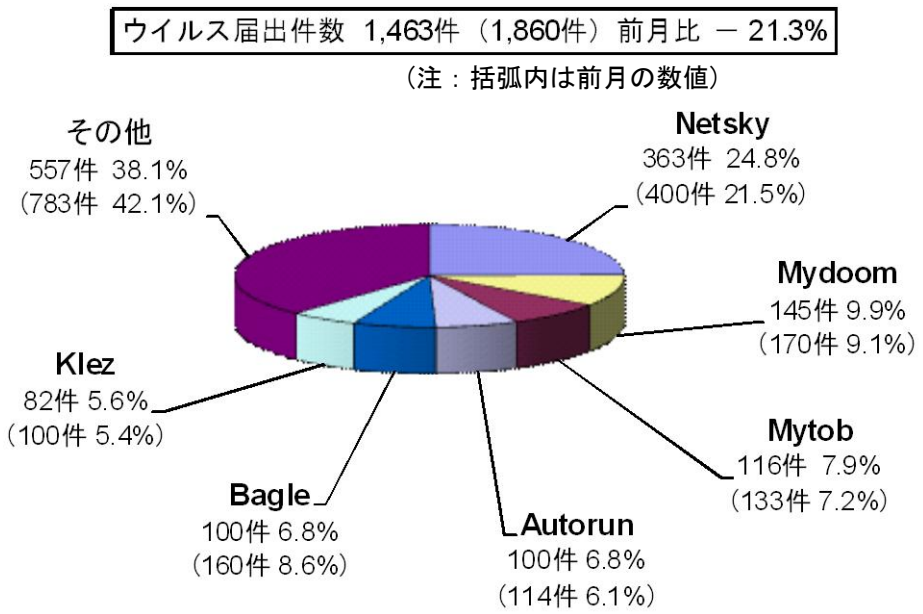


図 2-2：ウイルス届出件数

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

		9月	10月	11月	12月	1月	2月
届出(a) 計		14	17	18	10	10	9
	被害あり(b)	12	12	12	7	7	6
	被害なし(c)	2	5	6	3	3	3
相談(d) 計		38	58	39	38	29	35
	被害あり(e)	20	22	19	19	13	14
	被害なし(f)	18	36	20	19	16	21
合計(a+d)		52	75	57	48	39	44
	被害あり(b+e)	32	34	31	26	20	20
	被害なし(c+f)	20	41	26	22	19	24

(1)不正アクセス届出状況

2 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 35 件(うち 2 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 1 件、DoS 攻撃 1 件、なりすまし 3 件、不正プログラム埋込 1 件、**でした。

「侵入」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でした。侵入の原因は、脆弱性を突かれたことによるものでした。「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(オンラインゲーム 2 件、オンラインのコミュニケーションサイト 1 件)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) SQL インジェクション攻撃でデータを改ざんされた

事例	・ウェブサイト上での商品カタログ表示サービスに使っているデータベースのメンテナンス作業中、データベース内のデータに不審なスクリプトが追加され改ざんされていたことに気付いた。 ・調査したところ、SQL インジェクション攻撃を受けたことによる改ざんであることが判明。改ざんによって追加されたスクリプトによって、当該サイトを閲覧してきた顧客のパソコンが、ウイルスをダウンロードさせられる可能性があったことが分かった。 ・大量の SQL インジェクション攻撃のアクセスによって、ウェブサーバの応答が悪くなり閲覧しにくくなる不具合も生じた。 ・サイトに生じた不具合について、特にサイトにアクセスして来た顧客向けに、ウイルス感染の可能性やウイルスチェック方法についてウェブサイトで情報を提供。
解説・対策	問題のあったサイトは、ウェブサイトにアクセスして来た顧客のリクエストに応じて、データベースで管理している商品情報を、カタログとして随時ピックアップして見せる、という仕組みになっていました。**カタログデータが改ざんされたため、カタログを閲覧した顧客にまで被害がおよぶ可能性があることを忘れてはいけません。** 顧客がサイトを閲覧したことによってウイルス感染するなどの二次被害を防ぐため、**いち早くウェブサイトなどで事実関係を公表するとともに、対策方法についても告知することが、ウェブサイトを公開している企業としての義務**と言えます。 なお、改ざん被害への最大の対策は、脆弱性を作り込まないこと、です。次の資料を参考にしてください。 (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

2 月の相談総件数は **1051 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 **355 件**(1 月：243 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 **17 件**(1 月：11 件)、**Winny に関連する相談**が **7 件**(1 月：8 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**(1 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

		9月	10月	11月	12月	1月	2月
合計		2,154	1,171	713	839	960	1,051
	自動応答システム	1,302	677	363	458	529	521
	電話	755	441	288	331	390	472
	電子メール	93	47	62	49	39	57
	その他	4	6	0	1	2	1

※ 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。

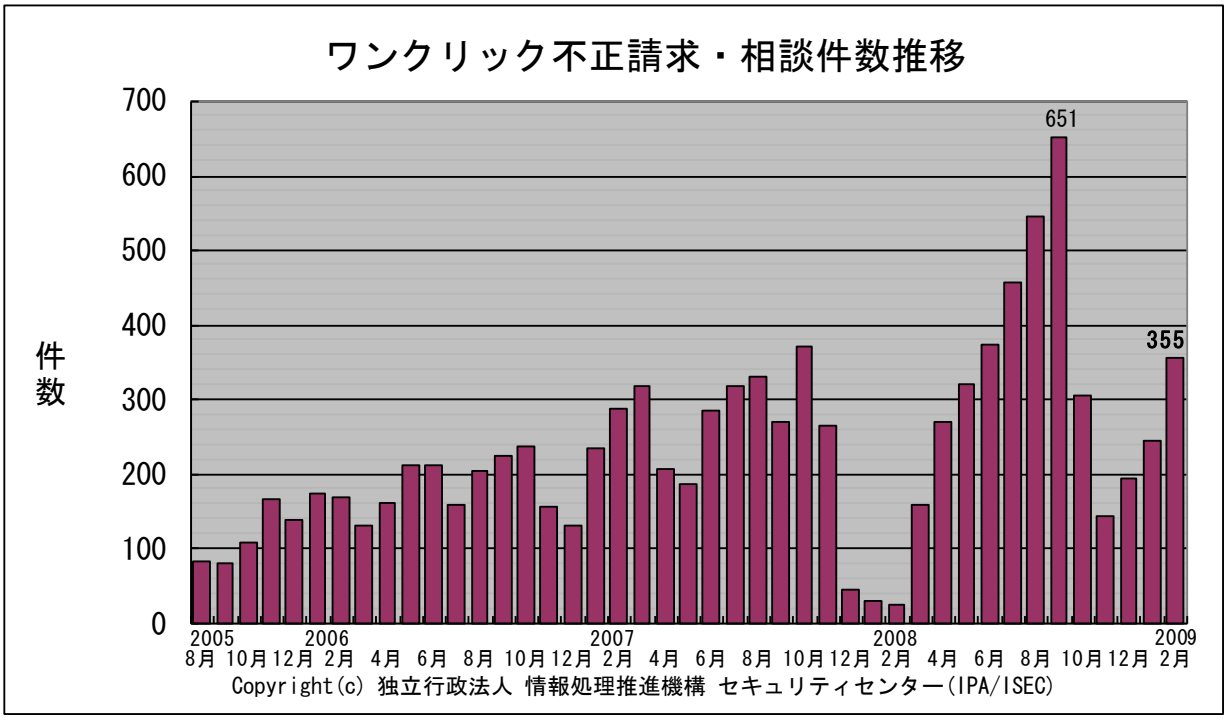


図 4-1　ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

(i) 友人からもらった USB メモリからウイルス感染？

相談	USB メモリを友人からもらった。その USB メモリを自分のパソコンに挿してからというもの、パソコンの調子が悪い。今思えば、USB メモリをパソコンに挿した際、デスクトップに見慣れないアイコンが出来ていた。ウイルス対策ソフトは入れていなかった。オンラインスキャンができるサイトでウイルスチェックしたら、ウイルスがたくさん検知された。パソコンは初期化した。今後、どうすれば良いのか。
回答	**もらった USB メモリ内に、USB メモリ感染型ウイルスが入っていた可能性が高い**と言えます。ご友人も知らないうちに USB メモリにウイルスが感染していたとすれば、**ご友人のパソコンもウイルス感染している可能性が高い**といえます。まずはご友人に、ウイルスチェックするよう知らせましょう。 今後、ウイルス感染防止のため、OS やアプリケーションを最新の状態に保つとともに、ウイルス対策ソフトを導入し、ウイルス定義ファイルを常に最新の状態にしておきましょう。 今後、**他人のものや拾ったものなど、自分が管理していない USB メモリやメモリカードを、不用意に自分のパソコンに挿すのは控えた方が良い**でしょう。 (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) あるソフトを使い続けたいため、OS を最新の状態にアップデートしたくない

相談	Windows XP SP1 を使っている。XP の最新版は SP3 であることは知っているが、自分が愛用しているソフトが使えなくなると聞いているため、SP3 へのアップデートに踏み切れない。ルータを使用し、メールの送受信はテキスト形式で行い、怪しいメールは一切開いていないので、セキュリティ対策していると言えるのではないか。なお、メールソフトの送信済みフォルダを見ても、怪しいメールは入っていないため、ウイルス感染によるメール発信は無いと信じている。
回答	**Windows XP SP1 は、既にマイクロソフトによるサポートが終了しており、脆弱性が発見されても修正プログラムは提供されません**。脆弱性の種類によっては、パソコンをインターネットにつないでいるだけで、ウイルスに感染してしまう場合があります。**悪意のあるサイトを閲覧しただけで、ウイルスに感染してしまう場合もあります**。セキュリティ対策の基本は、脆弱性の解消です。逆に言えば、**脆弱性を解消していなければ、他にどんな対策をしていても片手落ちになる**ということです。 あるソフトを使いたいがために、セキュリティ対策が疎かになるようでは、本末転倒です。OS を最新の状態に更新することを前提として、善後策を検討することをお勧めします。 なお、ウイルス感染によってメール送信の踏み台にされた場合、ウイルス自身がメールを送信するのが一般的ですので、メールソフトの送信済トレイにウイルスの形跡は何も残らないでしょう。 （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

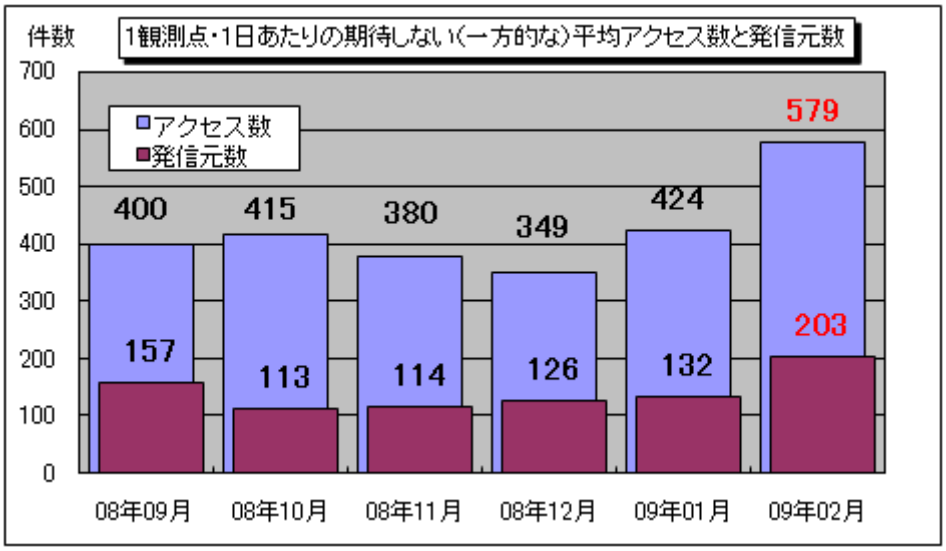
5. インターネット定点観測での 2 月のアクセス状況

インターネット定点観測(TALOT2)によると、2009 年 2 月の期待しない(一方的な)アクセスの総数は 10 観測点で **138,944 件**、総発信元(※)は **48,671 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 203 の発信元から 579 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。

※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。そのため、2 月の観測データは、この 4 日間を除外して統計情報を作成しています。

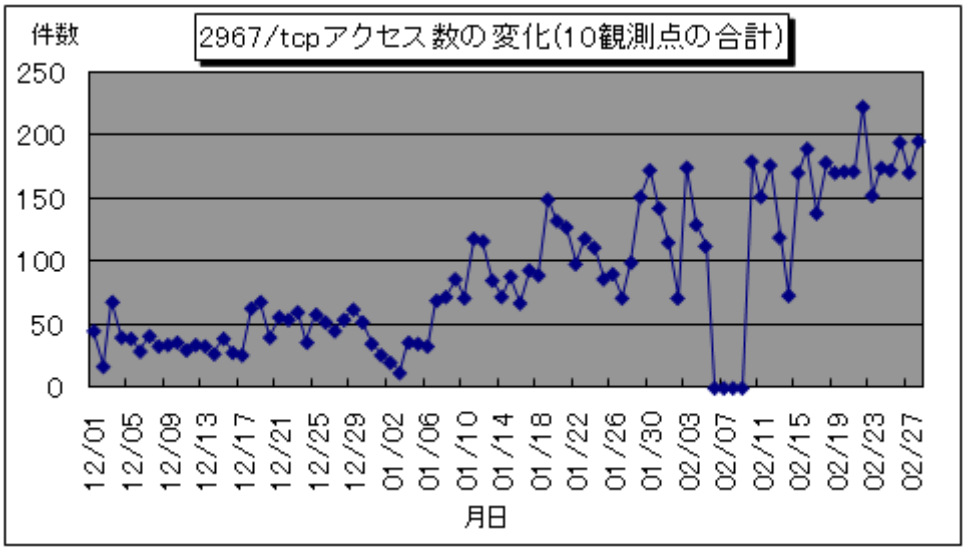


【図 5-1 1 観測点・1 日あたりの期待しない(一方的な)平均アクセス数と発信元数】

2008 年 9 月～2009 年 2 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。2 月の期待しない(一方的な)アクセスは 1 月と比べて大幅に増加しました。

(1) 2967/tcp へのアクセス

2967/tcp へのアクセスが 1 月に入ったあたりから増加し、2 月に入りさらに増加していました(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。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)」2006 年 5 月 25 日発表
http://www.symantec.com/region/jp/avcenter/security/content/2006.05.25.html

今でもこの脆弱性を狙った攻撃が行われている可能性があります。Symantec Client Security や Symantec AntiVirus の利用者は、Live Update によりプログラムを最新にすることで脆弱性を解消することができます。利用者は、利用しているプログラムが最新であるか確認してください。特に、利用期限が終了していて最新のプログラムに更新できない方は、最新版を購入して使用してください。
日頃から JVN などの脆弱性対策情報ポータルサイトを確認して、お使いの製品の脆弱性対策を迅速に行えるようにしてください。

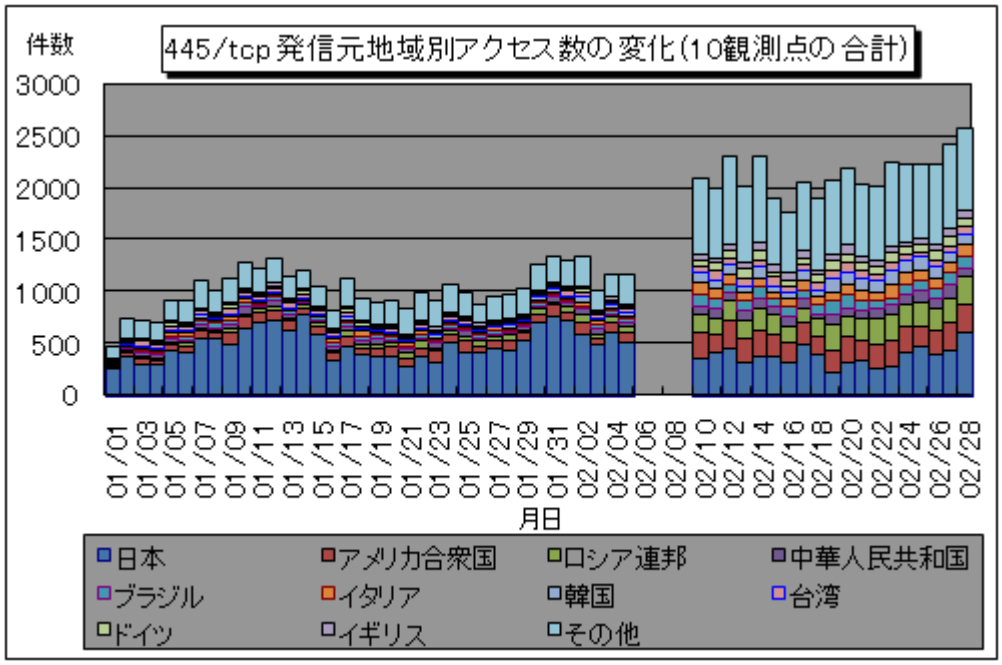
（ご参考）
「JVN (Japan Vulnerability Notes)」（脆弱性対策情報ポータルサイト）
http://jvn.jp/
「JVN iPedia 脆弱性対策情報データベース」
http://jvndb.jvn.jp/

(2) 445/tcp へのアクセス

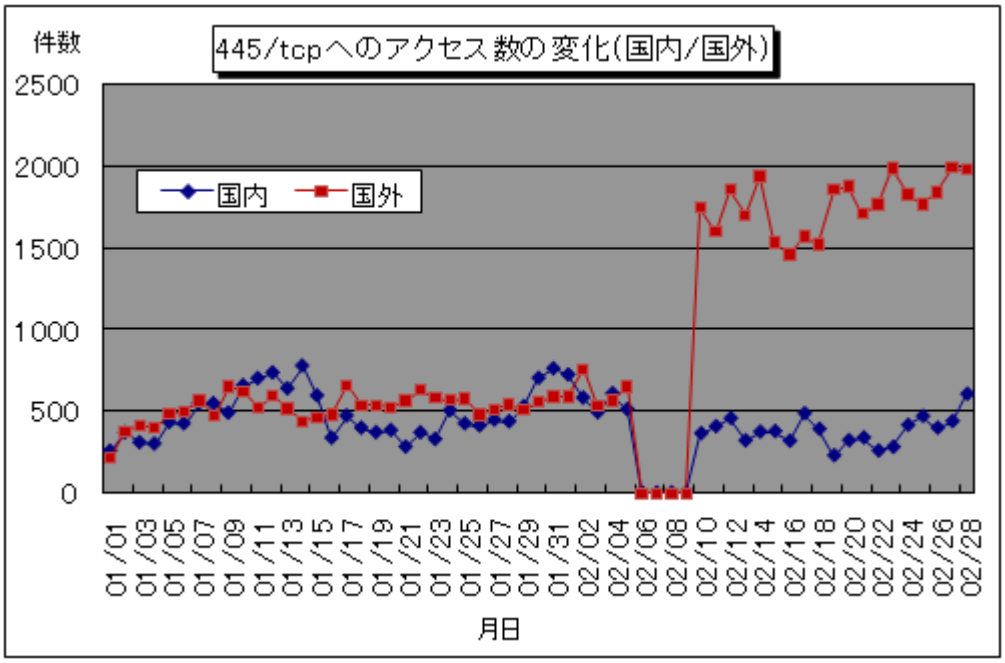
445/tcp へのアクセスは、1 月に既に多くのアクセスが観測されていましたが、2 月にはさらに多くのアクセスが観測されました（図 5-3 参照）。1 月の報告で解説した状況が続いているものと思われます。

（ご参考）
2009 年 1 月の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

ところで、2 月 6 日～9 日のシステム停止期間の前後でこのポートへのアクセス状況を比較しところ、国内からのアクセスが減少していたにもかかわらず、国外からのアクセスが大幅に増加していたことが分かりました(図 2-3 参照)。
システム停止期間の前後で、IP アドレスのネットワークセグメントが変わっていたことも要因の一つとして考えられるでしょう。



【図 5-3 445/tcp 発信元地域別アクセス数の変化】



【図 5-4 445/tcp へのアクセス数の変化(国内/国外)】

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/TALOT2-0903.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