プレスリリース
第 11-02-205 号
2011 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 [2010 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：藤江 一正）は、2010 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

「 忘れるな　ウイルス今も　進化中　地道にやろう　アップデート ※1 」

※1　第 6 回 IPA 情報セキュリティ標語・ポスターコンクール（2010 年度実施）標語部門
高校生の部 銅賞　林　聖悟 さん （埼玉県　立教新座高等学校 2 年）

2010 年は、正規ウェブサイト閲覧によるウイルス大量感染被害、ウイルス作成者の逮捕、情報漏えい被害の続発など情報セキュリティ上の出来事がありました。以下に挙げた事例はその代表的なものです。

- 大手企業ウェブサイトから個人のブログサイトまで、多くの正規ウェブサイト改ざん被害、改ざんされたウェブサイトを閲覧した利用者にウイルス感染被害（1 月～12 月）。
- 不正アクセスによる情報流出の被害（3 月、9 月、11 月、12 月）や、人為的な機密情報流出事件（10 月、11 月）。
- ウイルス作成者の再逮捕（8 月）や、ウイルスを悪用した詐欺行為での初の逮捕者（5 月）。
- 周辺国との政治的問題に起因した、公共、民間を問わず多くのウェブサイトでの改ざん被害（9 月）。

また、パソコン利用者を狙う手口の多様化も進みました。

今月の呼びかけでは、2010 年を振り返り、特に身近な情報セキュリティ上の脅威の中から以下の 3 つを取り上げて解説と対策方法を示すとともに、2011 年の展望として、脅威（攻撃手口）の方向性を考察します。

（1）“ドライブ・バイ・ダウンロード（Drive-by Download）” ※2 を取り巻く攻撃手法の変遷
（2）騙しのテクニックの変遷
（3）スマートフォンを巡る情報セキュリティの脅威の現状

※2 「ウェブサイトを閲覧しただけでウイルスに感染させられる"ドライブ・バイ・ダウンロード"攻撃に注意しましょう!」（IPA、2010 年 12 月の呼びかけ）
http://www.ipa.go.jp/security/txt/2010/12outline.html

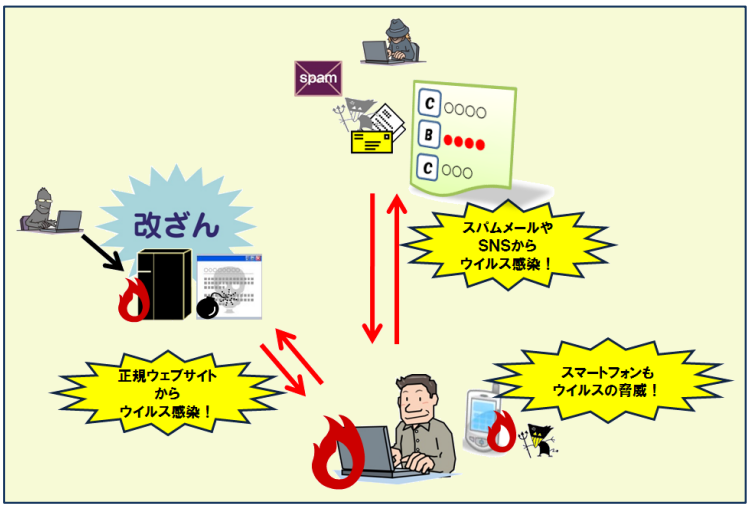

図 1-1：さまざまなウイルス感染や脅威のイメージ図

（1）“ドライブ・バイ・ダウンロード”を取り巻く攻撃手法の変遷

2010 年のセキュリティインシデント（情報セキュリティに関連する事件や事故）を振り返ると、“ドライブ・バイ・ダウンロード”攻撃の巧妙化が目立った一年でした。いわゆる“ガンブラー”※3 も、この攻撃手法を利用しており、この数年でパソコンにウイルスを感染させる攻撃手法の主流となりました。

“ドライブ・バイ・ダウンロード”攻撃の被害を防ぐためには、（i）悪意あるウェブサイトへの誘導手法、（ii）正規のウェブサイトの改ざん手法、（iii）ウイルスの感染手法、といった一連の手法を理解しておく必要があります。各々が“ドライブ・バイ・ダウンロード”攻撃を構成する手法であり、個別に変遷してきているためです。以下に、ドライブ・バイ・ダウンロードを取り巻く一連の攻撃手法について、個別に解説します。

※3 「"ガンブラー" の手口を知り、対策を行いましょう」（IPA、2010 年 2 月の呼びかけ）
http://www.ipa.go.jp/security/txt/2010/02outline.html

（i）悪意あるウェブサイトへの誘導手法

以前は、自分から怪しいウェブサイトを閲覧しなければ、ウイルス感染の危険は避けられると考えられていましたが、最近では、正規ウェブサイトが“ドライブ・バイ・ダウンロード”攻撃を行うウェブサイトにされてしまっている場合があります。

そうしたウェブサイトに誘導するため、例えば、SEO（Search Engine Optimization：特定の検索キーワードに対する検索結果として、特定のウェブサイトの表示順位を向上させる手法）を用いて、“ドライブ・バイ・ダウンロード”攻撃を行うウェブサイトを検索結果の上位に紛れ込ませる手法が見られます（図 1-2 参照）。この場合、わなのリンクに気付かない利用者はそのリンクをクリックすることにより、悪意あるウェブサイトに誘導されてしまいます。こうしたウェブサイトは、検索サイト側の監視で発見されるとすぐに検索対象から除外されますが、除外されるまでの期間が長くなると被害が大きくなってしまう恐れがあります。

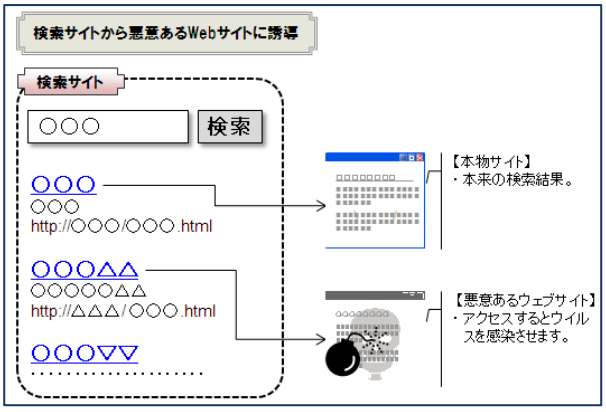

図 1-2：SEO を悪用したイメージ図

（ii）正規ウェブサイトの改ざん手口

2010 年 9 月に、ウェブサイト自体を改ざんするのではなく、企業などがウェブサイトを構成するために外部から導入する部品（バナー広告など）のデータ内に、悪意あるウェブサイトへの誘導命令を紛れ込ませていた事例を確認しました。これは、ウェブサイトを構成する部品の提供会社のサーバ内のデータを改ざんするという、新しい手口※4 でした。また、ウェブサイトの改ざん手口として、これまでは SQL インジェクションが多く見られましたが、2009 年からはいわゆるガンブラー※5 攻撃で使われた、ftp アカウント窃取による不正アクセス手法が多用されています。これらはいずれも、ウェブページ内に、悪意あるウェブサイトへ誘導するための「命令文」を埋め込む手法です。

※4 「ウェブサイトを閲覧しただけでウイルスに感染させられる"ドライブ・バイ・ダウンロード"攻撃に注意しましょう!」（IPA、2010 年 12 月の呼びかけ）
http://www.ipa.go.jp/security/txt/2010/12outline.html

※5 「ウェブサイトの管理方法を再確認しましょう！ ～ "ガンブラー"による被害はいまだに続いています ～」（IPA、2010 年 4 月の呼びかけ）
http://www.ipa.go.jp/security/txt/2010/04outline.html

（iii）悪意あるウェブサイトからのウイルス感染の手法

2010 年は、“ドライブ・バイ・ダウンロード”攻撃を行うため、以下の手法がウイルスの感染機能として使用されました。

- アプリケーションの脆弱性を悪用…Adobe Reader、Flash Player、JRE など。
- Windows の脆弱性を悪用…Windows シェルの脆弱性（MS10-046）。これは、細工されたショートカットファイル（lnk ファイル）が入っているフォルダを開くだけで、このファイルに触れなくてもウイルスを感染させることができる、新しい攻撃手口※6 でした。

※6 「新たな攻撃手口で、USB メモリなどを介して感染拡大するウイルスが出現！」（IPA、2010 年 9 月の呼びかけ）
http://www.ipa.go.jp/security/txt/2010/09outline.html

●被害予防策

最近は、どのウェブサイトを閲覧したらウイルスに感染するのか、専門家でさえわからないのが現状です。よって、ウェブサイト閲覧時に気をつけるだけでは、ウイルス感染を防ぐことはできません。ウイルスを感染させる手口として、（iii）で示した様々な脆弱性が悪用されますので、**使用しているパソコンの OS やアプリケーションなどの脆弱性を解消しておくことは必須です。その上でさらに、有害なウェブサイトの閲覧ブロック機能がある統合型ウイルス対策ソフトを最新の状態で使用することが効果的です。**また、OS やアプリケーションの脆弱性情報を日頃から収集しておくことも、万が一の際に適切な対処をするために役立ちます。

なお、IPA では利用者のパソコンにインストールされている主なソフトウェア製品のバージョンが最新であるかを、簡単な操作で確認するツール「MyJVN バージョンチェッカ」を無償で公開しています。

このツールを含めたウェブサイトには、毎月 100 万程度のアクセス（2010 年 1 月には 400 万程度のアクセスを記録）があり、日頃から定期的に利用されています。なお、2010 年 11 月から Windows 7 でも使えるようになりました。

（ご参考）
「MyJVN バージョンチェッカ」（IPA）
http://jvndb.jvn.jp/apis/myjvn/#VCCHECK

（2）騙しのテクニックの変遷

最近は偽装によって利用者を騙す手口が多くなっています。時節柄送られてくるグリーティングカードなどを装ったスパムメールや、流行のウェブサービス［mixi、Facebook などの SNS（ソーシャルネットワーキングサービス）や Twitter などのマイクロブログサービス、YouTube などの動画投稿サイト］を悪用するなど、数々の手口がありました。ここでは、そうした騙しのテクニックについて解説します。

（i）流行のサービスを悪用した攻撃

攻撃者は、SNS 内のサービスや機能を使い、以下のような手口を悪用して利用者を騙します。

- 人間の欲を刺激する記事を投稿し、リンクをクリックするよう仕向ける
  例えば Twitter で、「〇〇がタダでもらえる」「1,000 ドル分のギフトカードをもらえる」など偽の「ツイート（つぶやき、投稿）」を送り、記事中のリンクをクリックするよう利用者を誘惑します。記事中のリンクをクリックした利用者は、フィッシングサイトやウイルスを感染させるサイトに誘導されてしまいます。
- 短縮 URL※7 サービスの悪用
  これは、“http://”からはじまる長い URL 文字列を短くしてくれるサービスです。短縮 URL は、Twitter などの文字制限のあるマイクロブログによく使われますが、便利な半面、本来の URL が隠されてしまうため、悪意あるウェブサイトへ誘導する手法として悪用されてしまっています。

※7 「流行のサービスを狙った攻撃に注意！」（IPA、2010 年 5 月の呼びかけ）
http://www.ipa.go.jp/security/txt/2010/05outline.html

（ii）メールを悪用した攻撃（便乗ウイルスなど）

これは、利用者の友人や知人からと思わせるメール、利用者に有益な製品などの情報メールだと

偽って一方的にメールを送りつける手口です。こうしたメールには、ウイルスを感染させるウェブサイトに誘導する URL や、ウイルスを仕込んだファイルが添付されており、クリックをして閲覧したり開いたりするとウイルス感染の被害に遭います。利用者は、知り合いからと思わせるメールや、自分に関係のある有益な情報のメールだと思いこむため、安易にクリックしてしまう傾向があります。

こうしたメールの内容は、利用者の興味を引くもの（スポーツの国際大会や人気ゲームの情報、企業の製品情報など）や、流行のキーワードに便乗したものなどがあります。

●被害予防策

上述した攻撃は、ほとんどが利用者を油断させる手口でした。**まず「美味しい話」であっても、自分に関係がないメッセージやメールであれば、無視をするかすぐに削除すべきです。また、知り合いからのツイートやメッセージ、メールであっても、少しでも不自然に思う箇所があったらまずは疑ってかかり、安易に添付ファイルを開いたり、URL をクリックしたりしないことが重要です。**短縮 URL については、本来の URL に変換して表示するツールやサービスを利用することで、元の URL を知ることが可能です。

日頃からニュースサイトなどで情報を収集することで新しい騙しの手口をいち早く知り、被害予防に役立てることができます。

（3）スマートフォンを巡る情報セキュリティの脅威の現状

携帯電話の一種として普及が進むスマートフォンですが、パソコンと同様に OS に脆弱性が見つかったり、スマートフォンに感染するウイルスが確認されたりしています。今後はスマートフォンの利用者数が更に多くなることが見込まれ、スマートフォンを標的とした攻撃が増加していくものと思われます。

（i）攻撃事例

スマートフォンに感染するウイルスが、既に複数発見されています。攻撃者はウイルスを、スマートフォンのシステムのアップデートファイルや、便利なアプリケーションソフトなどと偽ってインストールさせることで感染させます。主な脆弱性情報やウイルス感染事例を示します。

iPhone（Apple iOS）

- PDF ファイルの処理に関する脆弱性と、権限の昇格が可能になる脆弱性が見つかりました。
- 壁紙を変えてしまうウイルスが発見されました。保護機能を解除（いわゆる Jail Break：脱獄）した iPhone のみに感染します。

Android（Google Android）

- Android 標準ウェブブラウザに、利用者の情報を盗み出すことができてしまう脆弱性が見つかりました。スマートフォン本体やメモリカードに保存されたファイルも盗まれる恐れがあります。
- SMS（Short Message Service：文字数の少ないメールのやりとりを携帯電話同士で行うサービス）による送金サービスを悪用するウイルスがロシアで発見されました。動画再生ソフトを装い、インストールするよう仕向ける感染手口です。感染すると、ウイルスが SMS メールを勝手に送信します。海外では SMS を使った送金サービスがあるため、ウイルスが SMS メールを送るだけで、犯罪者は不正に金銭を受け取ることができます。
- 利用者の位置情報を勝手に外部に送信するウイルスが発見されました。普通のアプリケーションソフトを装い、Android Market（Android 端末用アプリケーションの配布・販売を行うサイト）で配信されていました。

●被害予防策

ウイルスに感染しないためにも、パソコンと同様に脆弱性を解消することが最も重要です。OS およびアプリケーションは、常に最新の状態を維持しましょう。なお、インストールするアプリケーションは、かならず信頼のおけるサイトから入手することが重要です。

- Apple iOS

  アプリケーションは、Apple 公式サイトである、App Store からのみ入手できます。App Store で入手したアプリケーションは、アップデート版の有無確認やアップデート適用が一元的に実施可能ですので、随時チェックすることをお勧めします。また、**iOS の保護機能を解除（“Jail Break”：脱獄）すべきではありません。**

- Google Android

  アプリケーションは、アップデート版の有無確認やアップデート適用が一元的に実施可能である、Android Market などから入手するようにし、個人サイトや信頼性判断が難しいサイトからの入手は極力避けましょう。なお、各種マーケットから入手する場合でも、インターネットで事前にアプリケーション名などで情報を検索し、悪い評判が無いかどうかを確認することをお勧めします。また、信頼性の低いアプリケーションを自分で不用意にインストールしてしまわないためにも、**Android の設定で「提供元不明のアプリケーションのインストールを許可」のチェックが外れているかの確認をしましょう。**

（4）2011 年の展望

上述した 3 つの脅威については、2011 年もその脅威は増大すると思われます。以下に、3 つの脅威の 2011 年の展望について示します。

●“ドライブ・バイ・ダウンロード”を取り巻く攻撃手法

悪意あるウェブサイトに直接誘導する手口として、SEO ポイズニング※8 を多用する傾向が強まると考えられます。それは、利用者がインターネットを使う際、「まず検索をする」という行為が定着しており、検索結果に悪意あるウェブサイトを紛れ込ませておけば、利用者が検索結果のリンク先をクリックし、ウイルス感染させることができるからです。そして、今後もより効率的にウイルスをばら撒くような手口の巧妙化が懸念されるため、常に新しい情報に注意を向けておく必要があります。また、脆弱性が発見されるたびに、それが悪用される傾向は変わらないと思われます。脆弱性の内容によっては新しい攻撃手法が考え出され、今までには無かった感染形態を持つ新たなウイルスが出現することも予想されます。

※8 SEO ポイズニング：SEO の手法を悪用し、悪意あるウェブサイトへのリンクを検索結果内に紛れ込ませる手口

●騙しのテクニック

利用者のセキュリティ意識の向上や ISP（インターネット・サービス・プロバイダ）などによるスパムメール対策の推進により、攻撃者が利用者を騙す手口として、スパムメールだけではなく、SNS などを悪用するようになりました。今後もこの傾向は続くと思われます。

●スマートフォンを巡る情報セキュリティの脅威

パソコンと同様に、スマートフォンでも脆弱性を悪用して“ドライブ・バイ・ダウンロード”攻撃が多く行われると思われます。

感染するウイルスの種類によっては、アドレス帳からの個人情報漏えいや、金銭詐取など、甚大な被害が発生する可能性も考えられます。

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、ウェブサイトに不正アクセスされた

・サーバ設定ミスにより、外部より攻撃ツールを埋め込まれ、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、10 頁の「4.相談受付状況」を参照）

・契約プロバイダから、「あなたのパソコンで著作権侵害となる行為が行われている」というメールが来た

・USB メモリ感染型ウイルスに感染した

○ 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 2.3 万個**と、11 月の約 3.2 万個から 28.2%の減少となりました。また、12 月の届出件数※2 は、**874 件**となり、11 月の 1,094 件から 20.1%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。

・12 月は、寄せられたウイルス検出数約 2.3 万個を集約した結果、874 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 1.7 万個**、2 位は **W32/Mydoom** で**約 3 千個**、3 位は **W32/Autorun** で**約 1 千個**でした。

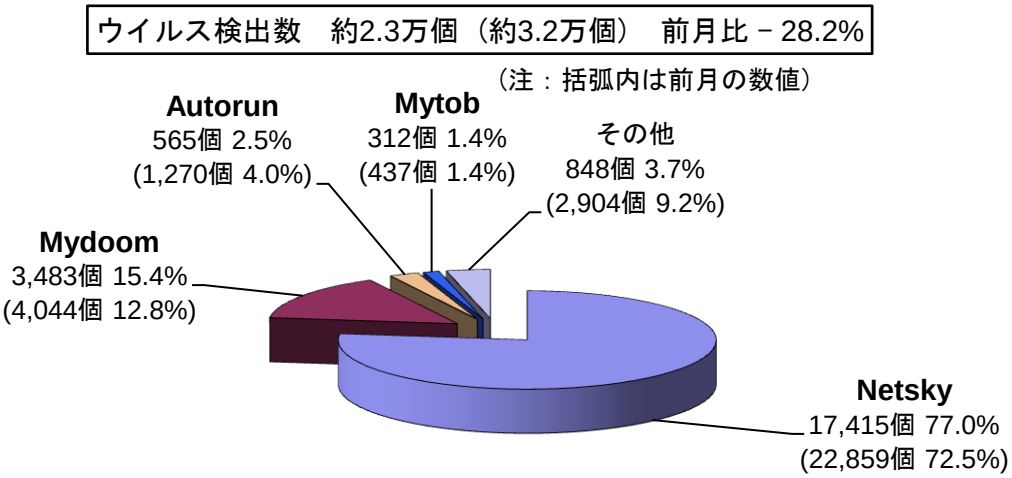

図 2-1：ウイルス検出数

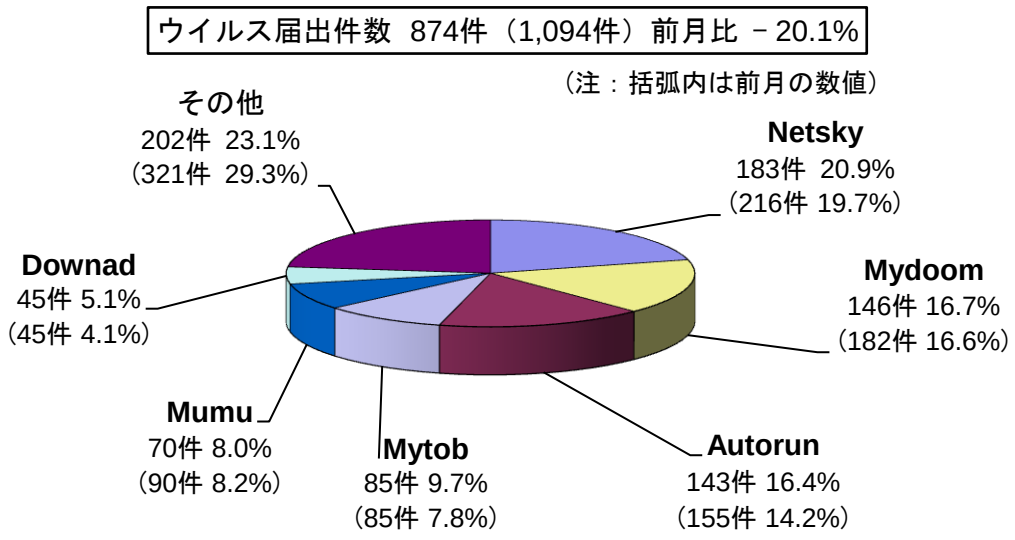

図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

2010 年 12 月の不正プログラムの検知状況は、9 月に確認されたような急増した事例はなく、10 月以降、同様の傾向となっています（図 2-3 参照）。

不正プログラムは、メールの添付ファイルとして配布されるケースが多く、そのメールの配信にはボット※3 に感染したパソコンが悪用されることがあります。

サイバークリーンセンター※4 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。不正プログラムの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実施が必要です。

（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/

※3 ボットとは、コンピュータウイルス等と同様な方法でコンピュータに感染し、そのコンピュータをネットワークを通じて、外部から操ることを目的として作成されたプログラムです。

※4 サイバークリーンセンターとは、総務省・経済産業省が連携して実施するボット対策プロジェクトです。

（ご参考）

サイバークリーンセンターについて

https://www.ccc.go.jp/ccc/

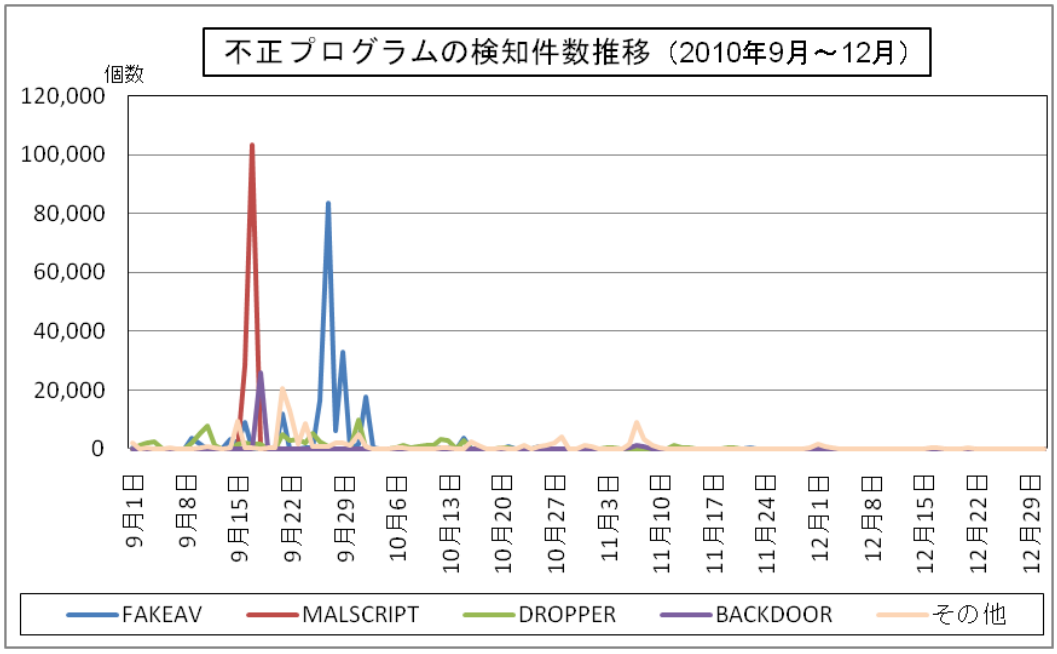

図 2-3：不正プログラムの検知件数推移

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	18	15	14	14	22
	被害あり(b)	9	12	10	8	7	7
	被害なし(c)	5	6	5	6	7	15
相談(d)　計		44	56	47	40	45	27
	被害あり(e)	23	16	8	15	12	7
	被害なし(f)	21	40	39	25	33	20
合計(a+d)		58	74	62	54	59	49
	被害あり(b+e)	32	28	18	23	19	14
	被害なし(c+f)	26	46	44	31	40	35

（1）不正アクセス届出状況

12 月の届出件数は 22 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 27 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 7 件でした。

（3）被害状況

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

「侵入」の被害は、データの窃取が 1 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 1 件、不正アカウントの作成が 1 件、その他が 2 件、でした。侵入の原因は、サーバの設定不備が 2 件、OS 及び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、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、ウェブサイトに不正アクセスされた

事例	・公開しているウェブサイトに、不正アクセスの痕跡を見つけた。ウェブサイトのアクセスログ解析ツールから異常な数値を発見したことで発覚。 ・アクセスログを詳しく解析したところ、不正アクセスの原因は SQL インジェクション攻撃と判明。 ・使用していたウェブアプリケーションに、SQL インジェクション攻撃に対する脆弱性が存在し、それを悪用されて攻撃を受けたことが原因。
解説・対策	ウェブアプリケーションの脆弱性を悪用された事例です。**使用しているウェブアプリケーションの脆弱性情報は、日頃から収集をして常に認識をしておきましょう。**また、脆弱性の解消は、出来る限り行うのはもちろんですが、WAF（Web Application Firewall）を導入してウェブサイト全体のセキュリティを強化することも有効な対策になります。 （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）サーバ設定ミスにより、外部より攻撃ツールを埋め込まれ、踏み台として悪用された

事例	・外部からの攻撃により、外部攻撃ツールを埋め込まれていることを確認。 ・IRC サーバへの接続の踏み台にもされていた。 ・サーバのアカウント情報を奪取され、そのアカウントを使ってサーバに侵入したと思われる。 ・サーバを調べたところ、サーバ設置業者による設定ミスを発見。 ・他のコンピュータからのアクセス制限を行うための設定ファイル、"/etc/hosts.allow"と"/etc/hosts.deny"ファイルに誤りがあり、外部からの侵入が容易になっていたことが原因。
解説・対策	設定業者の不注意により起こってしまった事例です。**インストールされているソフトウェアを含めたサーバの設定内容は、サーバを運用する側も把握をしておくことが重要です。** 外部攻撃ツール以外にも、不正なものが埋め込まれている可能性が高いと思われます。サーバは初期化し再構築することが基本となります。 （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

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 **1,536 件**でした。そのうち**『ワンクリック請求』に関する相談**が **474 件**（11 月：483 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 **10 件**（11 月：18 件）、**Winny に関連する相談**が **4 件**（11 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 **0 件**（11 月：10 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		2,133	2,432	2,102	1,813	1,692	1,536
	自動応答システム	1,142	1,298	1,142	1,065	1,036	954
	電話	924	1,053	872	675	580	531
	電子メール	66	75	85	69	72	49
	その他	1	6	3	4	4	2

※ IPA では、「情報セキュリティ安心相談窓口」を開設し、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：anshin@ipa.go.jp
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。

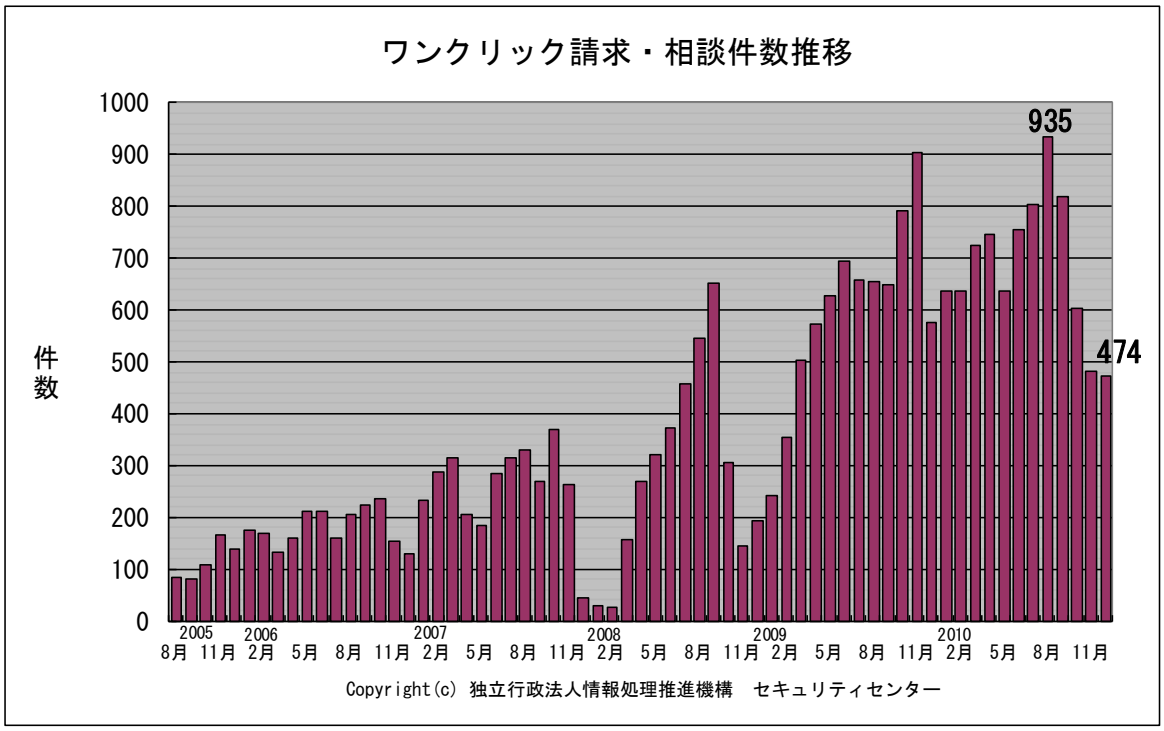

図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）契約プロバイダから、「あなたのパソコンで著作権侵害となる行為が行われている」というメールが来た

相談	私が契約しているプロバイダより、「お客様のログイン ID で接続している端末に割り当てられた IP アドレスで、著作権侵害となる行為が行われている」といった内容のメールが来た。 何のことか分からず困っているが、どのようにしたら良いのか？
回答	提示のあったプロバイダのメールの内容から推察するに、**Winny のようなファイル共有ソフトを使用しているということはないでしょうか**。貴方に心当たりがなければ、ご家族のどなたかが使用している可能性が考えられます。 著作権侵害については、当相談窓口でアドバイスできることはありませんが、Winny のようなファイル共有ソフトを使用していると、ウイルスに感染して貴方のパソコン内の情報が漏えいしてしまう可能性がありますのでご注意ください。 なお、2010 年 1 月 1 日から警察機関がファイル共有ネットワークを監視しており、実際に著作権違反で逮捕者がでているという報道もありますので、心当たりがある場合は、速やかに適切な対処をされることをお勧めします。 （ご参考） IPA－Winny による情報漏えいを防止するために http://www.ipa.go.jp/security/topics/20060310_winny.html

（ii）USB メモリ感染型ウイルスに感染した

相談	ウイルス対策ソフトの更新期限が切れているノートパソコンに USB メモリを挿してから、マイクロソフトやシマンテックなどのウェブサイトへの接続が不可になった。 その USB メモリをウイルス対策ソフトが有効なパソコンに挿したら W32.Downadup というウイルスが検知された。 ノートパソコンをパソコンメーカーに見てもらったところ、初期化を勧められたが、なるべく初期化は避けたい。
回答	W32.Downadup というウイルスは Windows の脆弱性を悪用するタイプで、**USB メモリを感染経路とする機能を持つことが確認されており**、ノートパソコンのウイルス対策ソフトの期限を更新していれば感染を防げた可能性が高いです。マイクロソフトやシマンテックなどのウェブサイトへの接続が不可になるのもこのウイルスの妨害活動によるものと思われます。 ウイルス対策ソフトを更新することで、ウイルスを駆除できる場合もありますが、それでもうまくいかないということであれば、初期化することをお勧めします。 （ご参考） IPA－2009 年 2 月の呼びかけ「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

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、2010 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 **81,226 件**、延べ発信元数※は **37,550 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 134 の発信元から 290 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。

※12 月 22 日～24 日は、保守作業のため、システムを停止しています。そのため、12 月の観測データは、この 3 日間を除外して統計情報を作成しています。なお、通常は常時稼働しています。

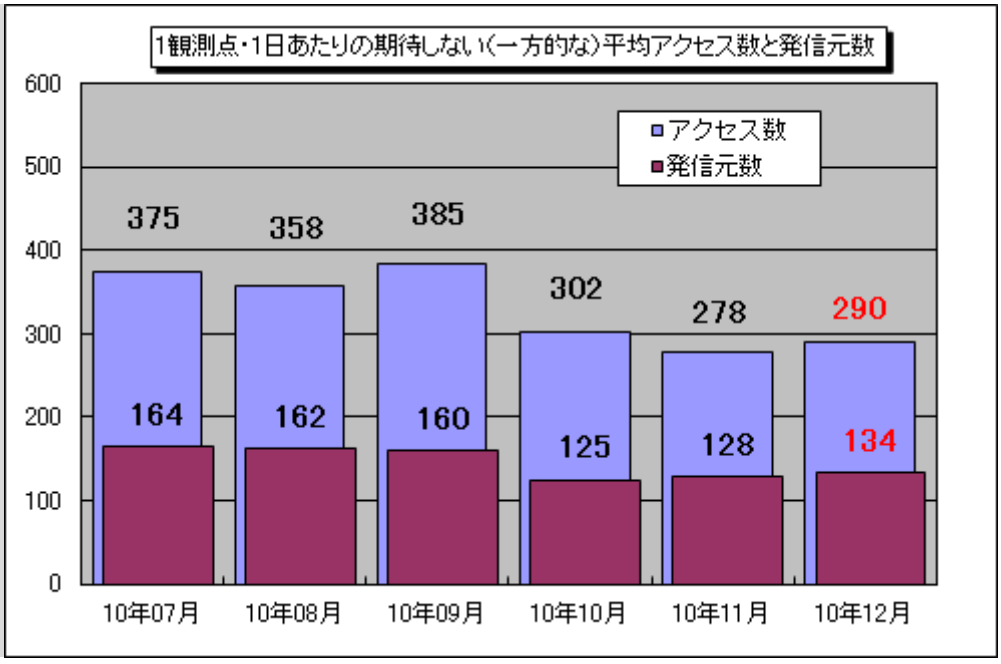

図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数

2010 年 7 月～2010 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 月と比べて増加しました。

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、特に増加が観測されたのは 445/tcp へのアクセスでした。

445/tcp は、先月に引き続き増加していましたが、これは主にアメリカと日本からのアクセスが増えたことによるものでした（図 5-3 参照）。

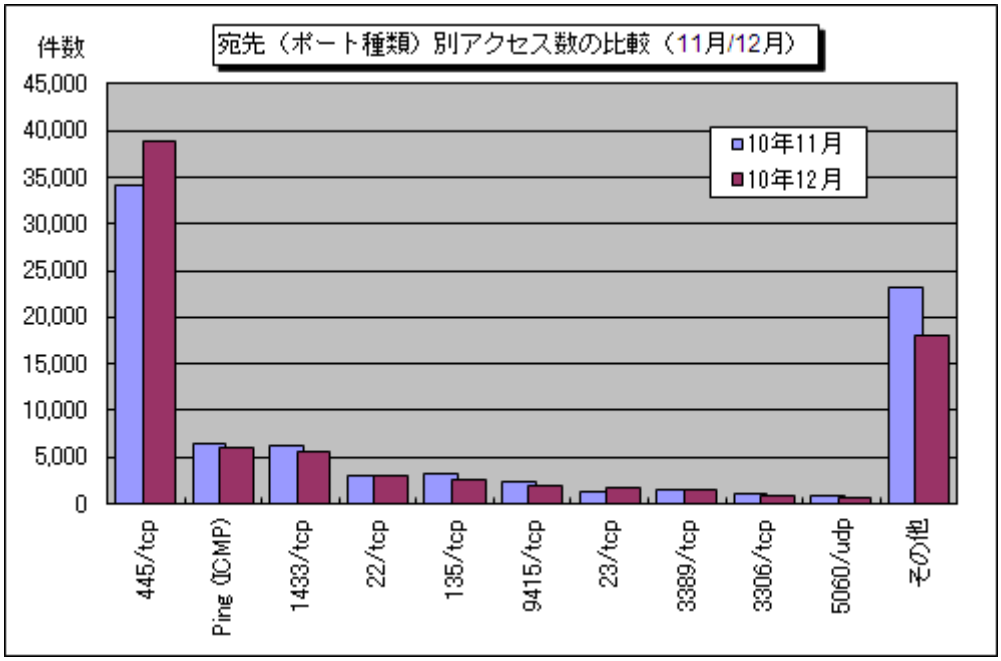

図 5-2：宛先（ポート種類）別アクセス数の比較（11 月/12 月）

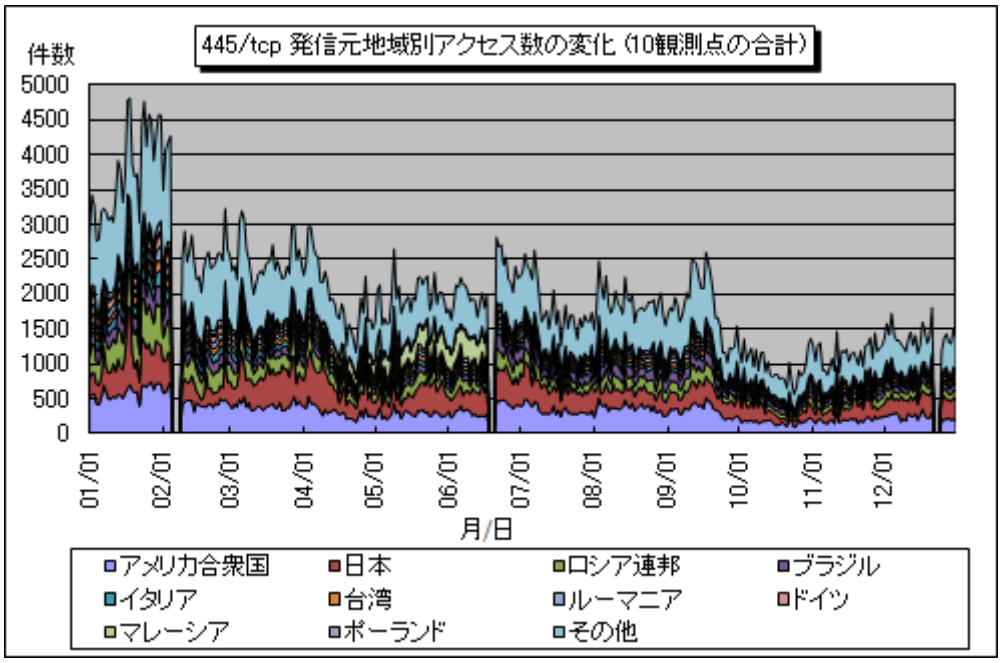

図 5-3：445/tcp 発信元地域別アクセス数の変化（10 観測点の合計）

（1）2010 年のアクセス状況

2010 年 1 月～2010 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 5-4 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 1 月から減少傾向にあり、4 月、6 月、9 月に増加が見られましたが、最終的に 1 月の約半分の水準まで減少しました。

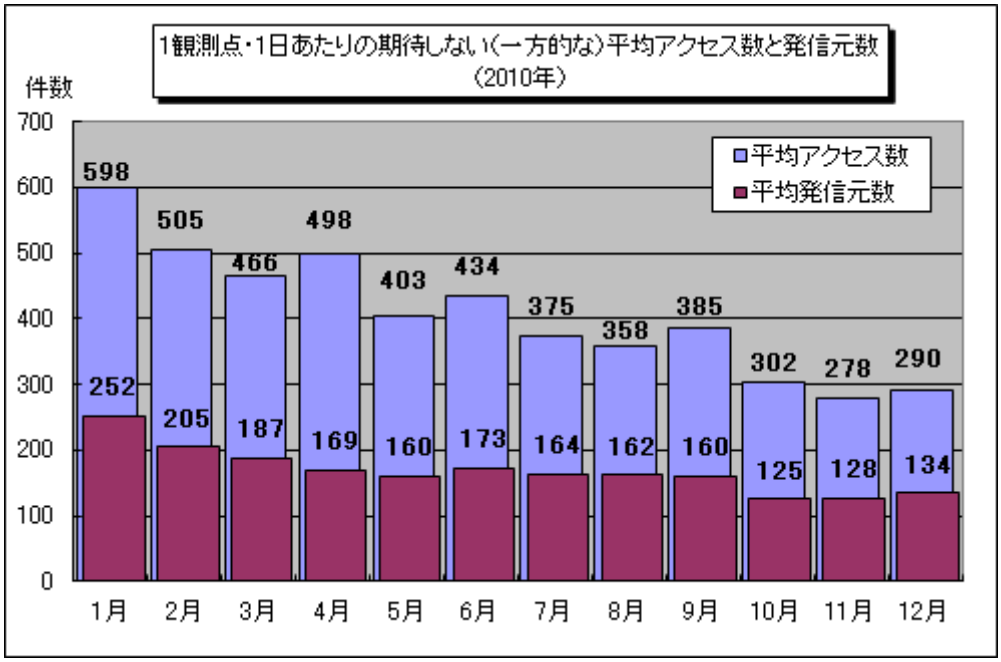

図 5-4：1 観測点・1 日あたりの期待しない(一方的な)平均アクセス数と発信元数

図 5-4 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 5-5 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 445/tcp へのアクセスは減少が顕著で、最終的に全体の半数までに減少する形となりました。

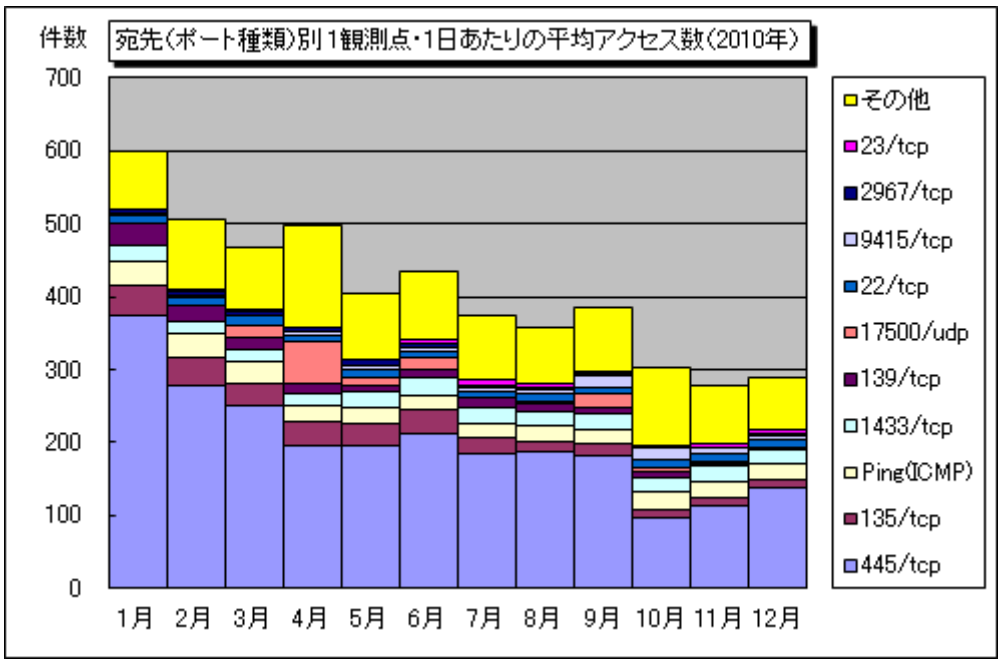

図 5-5：宛先（ポート種類）別 1 観測点・1 日あたりの平均アクセス数

次に、2009 年と 2010 年の宛先（ポート種類）別アクセス数の比較を図 5-6 に示します。2009 年からアクセス数が増加したのは 445/tcp、17500/udp、9415/tcp であり、445/tcp は約 3 万件の増加、17500/udp は約 4 万件の増加、9415/tcp は、約 2 万件の増加でした。逆に減少したのは 135/tcp、Ping（ICMP）、2967/tcp であり、135/tcp は約 21 万件の大幅な減少、Ping（ICMP）は約 6 万件の減少、2967/tcp は約 3 万件の減少でした。

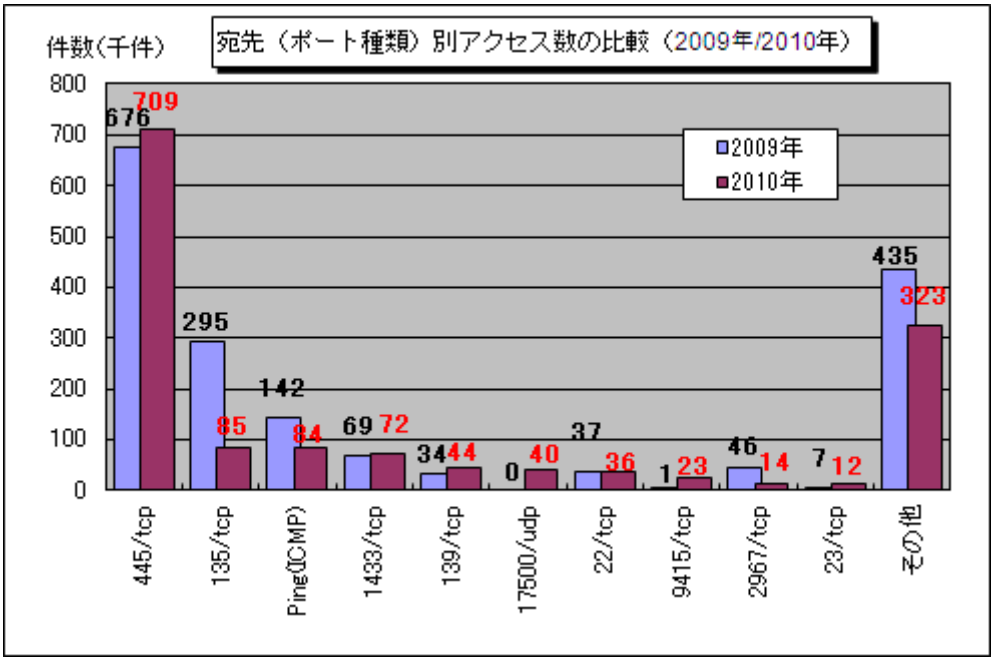

図 5-6：宛先（ポート種類）別アクセス数の比較（2009 年/2010 年）

2010 年の TALOT2 のアクセス状況において、特徴的なのは 17500/udp と 9415/tcp へのアクセスの大幅な増加と言えます。17500/udp へのアクセスの特徴としては、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点が挙げられます。このアクセスについて調査したところ、17500/udp に対してブロードキャストを送信するアプリケーションが存在することが分かったため、これが原因の一つと考えられます。複数と思われていた発信元 IP アドレスは、実はパソコンを立ち上げる度に変化していた 1 箇所のパソコンで、そのパソコンからのブロードキャストが TALOT2 の観測点に届いていた可能性があります。なお、他の観測点はブロードキャストが端末に到達しない仕様のようなので、当該アクセスは観測されませんでした。

また、9415/tcp については、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。

2010 年 1 月からの 17500/udp へのアクセス数の変化を図 5-7 に示します。

2010 年 1 月からの 9415/tcp へのアクセス数の変化を図 5-8 に示します。

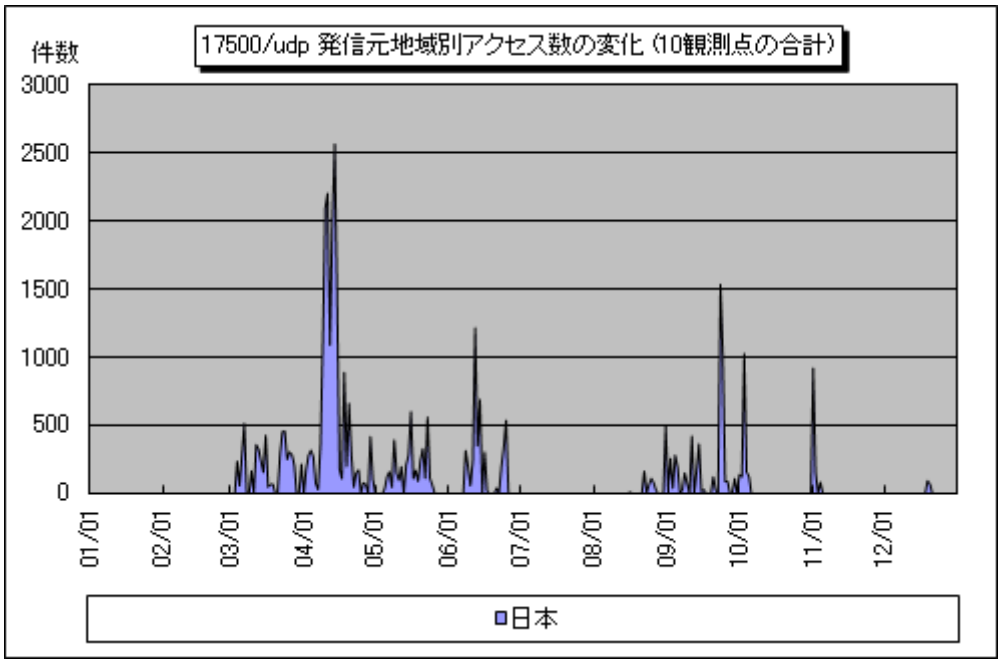

図 5-7：17500/udp 発信元地域別アクセス数の変化

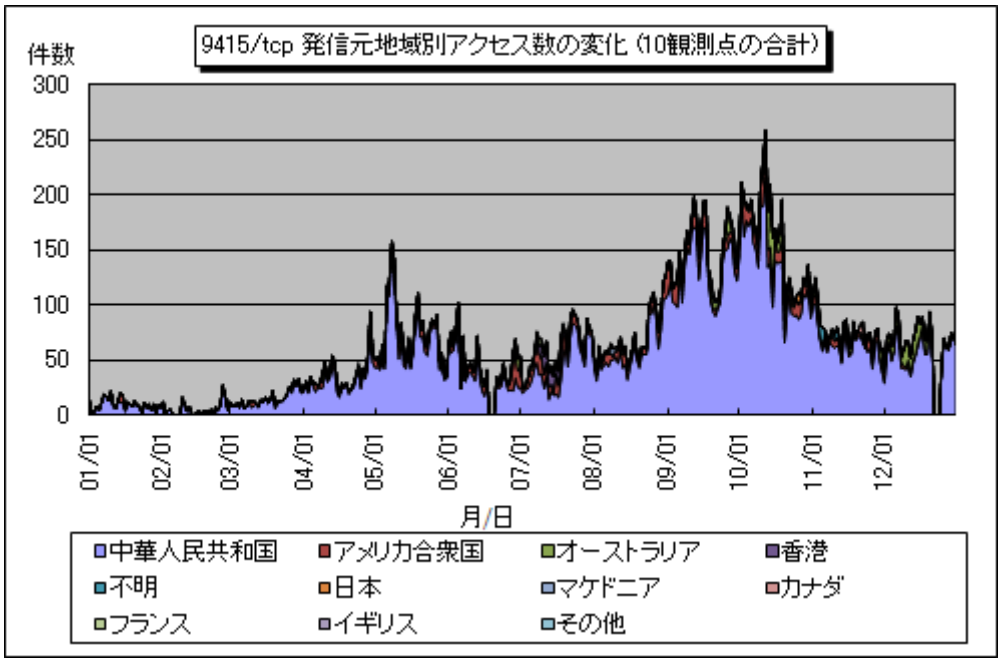

図 5-8：9415/tcp 発信元地域別アクセス数の変化

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/2011/documents/TALOT2-1101.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／宮本／古川
Tel:03-5978-7591　Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp