第 10-21-186 号
2010 年 5 月 7 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 4 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、2010 年 4 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

「 流行のサービスを狙った攻撃に注意！ 」

最近、インターネットを利用したサービスである“Twitter（ツイッター）”、“アメーバなう”などのミニブログサービスや、“mixi（ミクシィ）”、“Facebook（フェイスブック）”などの SNS（ソーシャルネットワーキングサービス）が人気です。これらのサービスは、今の自分の行動や考えを簡単にインターネット上に発信することや、同じ趣味や考えを持つ利用者同士の交流の場として利用できることが特徴となっており、一般利用者に限らず多くの芸能人や政界財界関係者も利用しています。一方、このような人気のあるサービスは、攻撃に利用されることも少なくありません。

既にこれらのサービスを悪用した、利用者を騙す手口やウイルスを感染させようとする手口が出現しており、そのような相談も IPA に寄せられています。

新たなサービスを利用する場合は、そのサービスの特性を悪用する攻撃による被害に遭わないため、狙われるポイントを理解し、セキュリティ対策を行ってください。

（1）ミニブログサービスの特徴と攻撃手口の例

ここでは、ミニブログサービスの一つである Twitter の特徴と、攻撃手口の一例を示します。

▼Twitter の特徴

Twitter では、利用者がそれぞれ思いついた事などを「ツイート（つぶやき、投稿）」しています。Twitter には、他の利用者の「ツイート」を見るための「フォロー」という仕組みがあります。（図 1-1）。例えば、自分の好きな芸能人を「フォロー」しておけば、その芸能人の動向「ツイート（つぶやき）」を、自分の「タイムライン（「ツイート」の一覧表示機能）」からすばやく知ることができます。

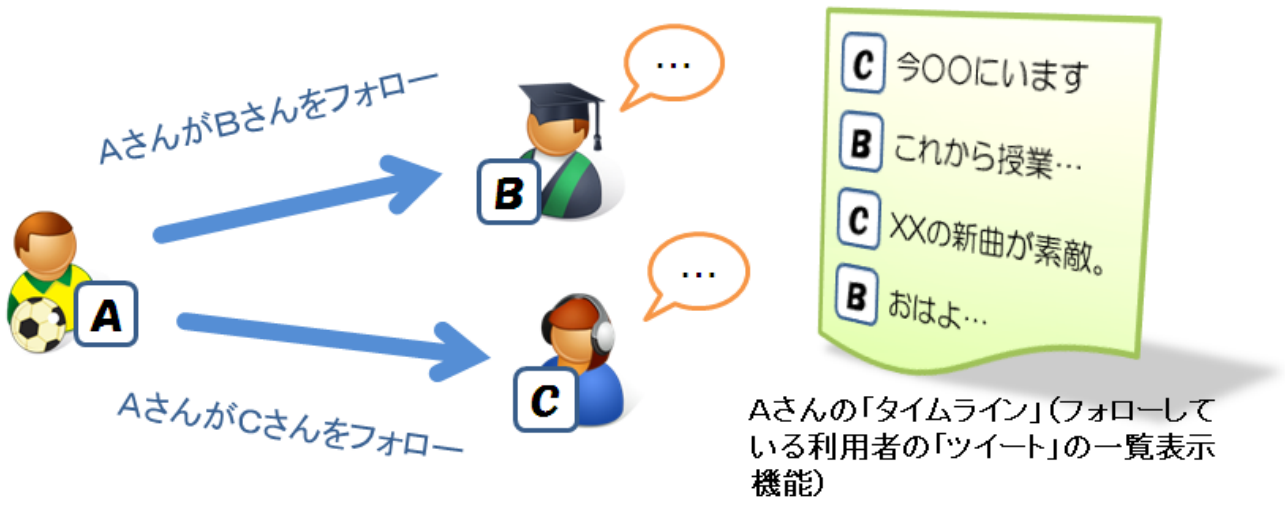


図 1-1：Twitter の仕組みのイメージ図

悪意ある攻撃者は、これらの仕組みを悪用して、利用者をウイルス感染の被害に遭わせようとします。次に、Twitter を悪用した具体的な攻撃手口の例を示します。

▼具体的な攻撃手口の例

【1】攻撃者 X が、攻撃対象者の A さんを「フォロー」します。フォローする際には、A さんからの許可は必要ありません。A さんは、X から「フォロー」されたことを知ることができます。

【2】**A さんも、自分の知らない相手である、攻撃者 X を「フォロー」します。これは一般的に「フォロー返し」と呼ばれ、あまり注意を払わずに行われがちです。**

【3】これにより、A さんの「タイムライン」に、攻撃者 X の「ツイート」が表示されるようになります。**攻撃者 X は、興味を引くような文章と共に、罠の URL（リンク）を「ツイート」します。ここで、A さんが罠の URL をクリックすると、ウイルスに感染させられてしまう危険のあるウェブサイトに誘導されてしまいます。**

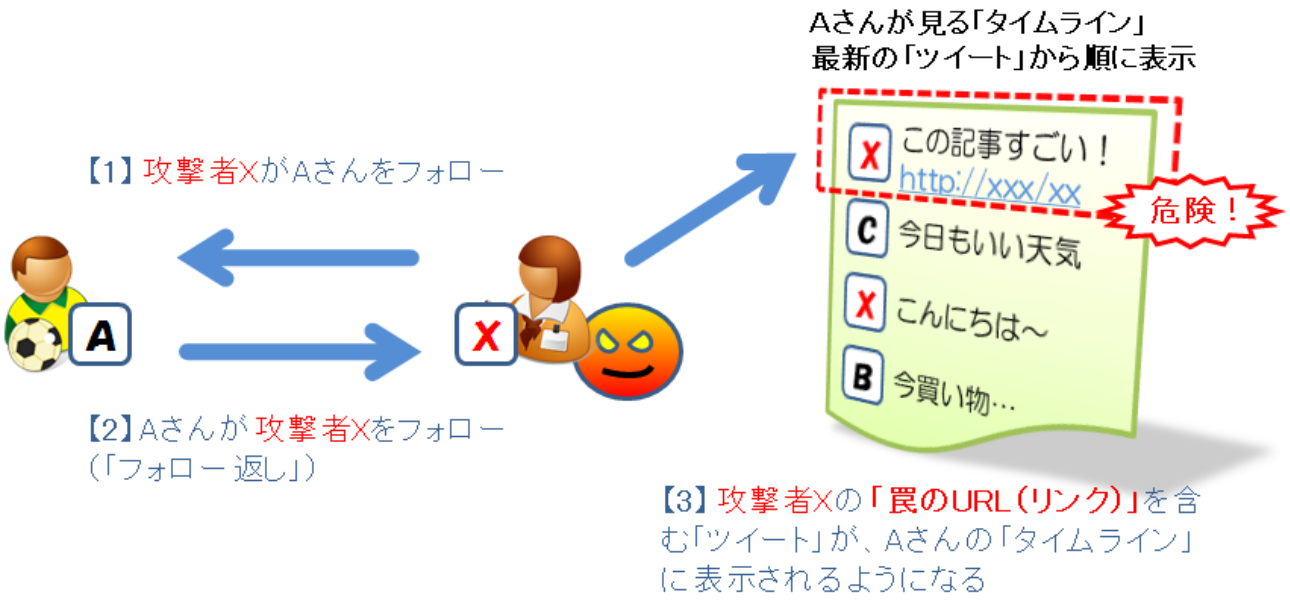


図 1-2：Twitter を悪用した攻撃手口のイメージ図

▼注意が必要な行為

上記の攻撃手口の例において、利用者として注意すべき行為を次に示します。

➢ 簡単に「フォロー」をしてしまう行為

Twitter は「フォロー」をしないと（されないと）、サービスを使う魅力は半減するかもしれませんが、確認もせず「フォロー」してしまうと、上述例のように攻撃者を簡単に招き込んでしまう可能性があります。特に“なりすまし”による詐欺などに注意が必要です。

有名人や有名企業などの“なりすまし”行為は従来からある手口で、偽物と知らずに、フィッシング詐欺サイトなどに誘導されて被害に遭う可能性があります。Twitter では、政治家や芸能人の偽物の存在が問題となっており、芸能人を「フォロー」したと思っていたら実は偽物で、騙されて偽のコンサートチケットを購入するなどの詐欺被害に遭うことも考えられます。

➢ 他者の「ツイート」に書かれている URL をクリックしてしまう行為

他者の「ツイート」に書かれている URL を簡単にクリックしてしまう行為は、“身に覚えのないメールの添付ファイルを開く”、“ブログや掲示板に書かれているリンクをクリックする”などと同じように危険なことです。特に“短縮 URL”の悪用によるウイルス感染に注意が必要です。

“短縮 URL”は、長い URL 文字列を短縮して利用できるサービスです。

例：”http://www.ipa.go.jp/security/personal/yobikake/index.html”を短くすると、
“http://〇〇〇〇/5G5G3g”となります。“〇〇〇〇”は短縮サービスを行うサイト名になり、“/”から後ろの文字はサービスサイト側が任意に設定したものになります。

Twitter は、1 回で入力できる文字数の制限があり、長い URL が収まりきらないことがあるため、リンクを提示する際に短縮 URL がよく使われます。短縮 URL は、クリックするまでどのようなウェブサイトに誘導されるかわからず､ウイルスを感染させようとするサイトへ誘導される可能性があります。

▼対策

- “なりすまし”を見抜くことは簡単ではありませんが、「フォロー」する相手が芸能人や企業であれば、所属会社や各企業の問合せ先、公式ウェブサイトなどで確認することが可能です。見知らぬ他者とコミュニケーションを行う際には、相手が悪意のある人物である可能性があることを意識してください。

- “短縮 URL”をクリックする前に、“短縮 URL”を本来の URL で表示するツールやサービスを使用し、URL の信頼性を確認してください。

（2）基本的な対策

上述した個別の対策も必要ですが、以下の基本的な対策は必ず行ってください。

- 使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てください。
- 使用している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ください。
  （ご参考）「MyJVN バージョンチェッカ」（IPA）
  http://jvndb.jvn.jp/apis/myjvn/#VCCHECK
  ※ 2010 年 4 月末日現在、Windows XP と Vista に対応しています。
- ウイルス対策ソフトは、ウイルス定義ファイルを最新の状態で使用してください。なお、迷惑メールの閲覧防止機能や、有害なウェブサイトの閲覧防止機能などが一つになった、統合型ウイルス対策ソフトの使用を推奨します。
- 万が一、ウイルスなどに感染してしまった場合に備えて、重要なデータのバックアップを行ってください。

今回は Twitter を例に挙げて攻撃手口や対策を示してきましたが、このような攻撃は、従来のサービスであるブログや掲示板、メールでも発生していました。「新しいサービスだから大丈夫」ということはなく、利用者に便利で人気のサービスであれば、悪意ある攻撃者もそうしたサービスを悪用することを理解するとともに、基本的な対策を実施した上でサービスを利用してください。

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、6 頁の「3.コンピュータ不正アクセス届出状況」を参照）
- SSH で使用するポートへの攻撃で侵入された
- パスワード再発行の仕組みが悪用され、オンラインゲームのアカウントが乗っ取られた

○ 相談の主な事例 （相談受付状況および相談事例の詳細は、8 頁の「4.相談受付状況」を参照）
- ワンクリック不正請求の被害から復旧できない
- 無線 LAN のセキュリティ設定について

○ 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。

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

4 月のウイルスの検出数（※1）は、**約 4 万個**と、3 月の約 5.8 万個から 31.9%の減少となりました。また、4 月の届出件数（※2）は、**1,077 件**となり、3 月の 1,484 件から 27.4%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。
・4 月は、寄せられたウイルス検出数約 4 万個を集約した結果、1,077 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 3.2 万個**、2 位は **W32/Mydoom** で**約 5 千個**、3 位は **W32/Autorun** で**約 1 千個**でした。

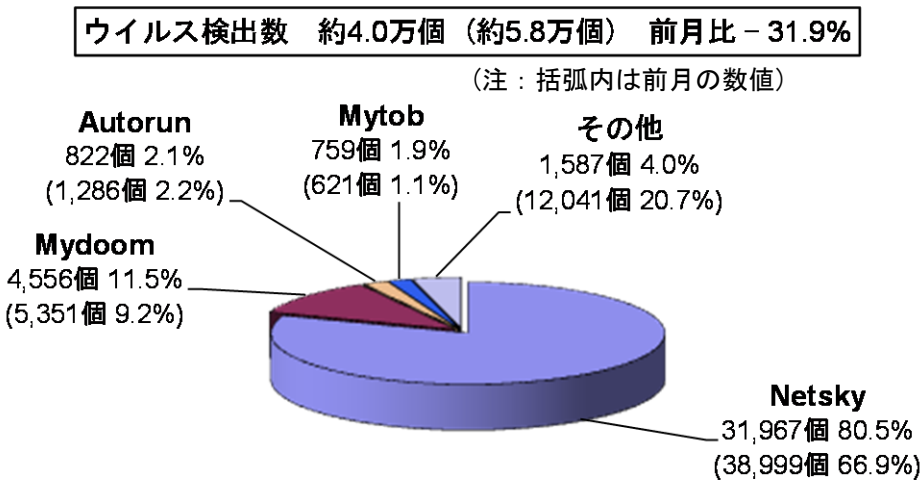


図 2-1：ウイルス検出数

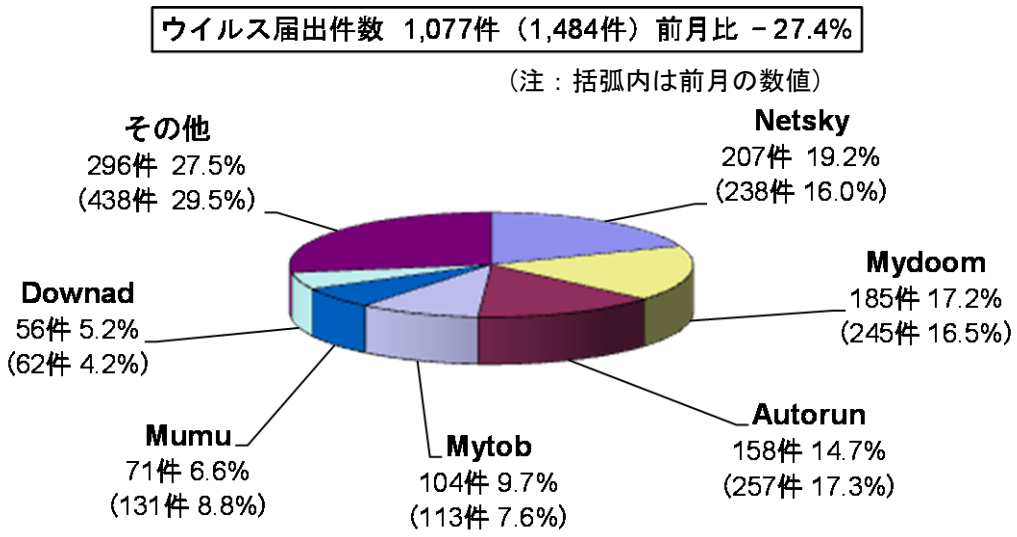


図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

2010 年 4 月の不正プログラムの検知状況は、3 月と同様に大きな変化はありませんでした（図 2-3 参照）。しかし、これらの不正プログラムは、1 月や 2 月に確認されたようにいつ急増するかわかりません。

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いため、メールの添付ファイルの取り扱いには継続して注意を払う必要があります。また、不正プログラムの配信には、ボット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/

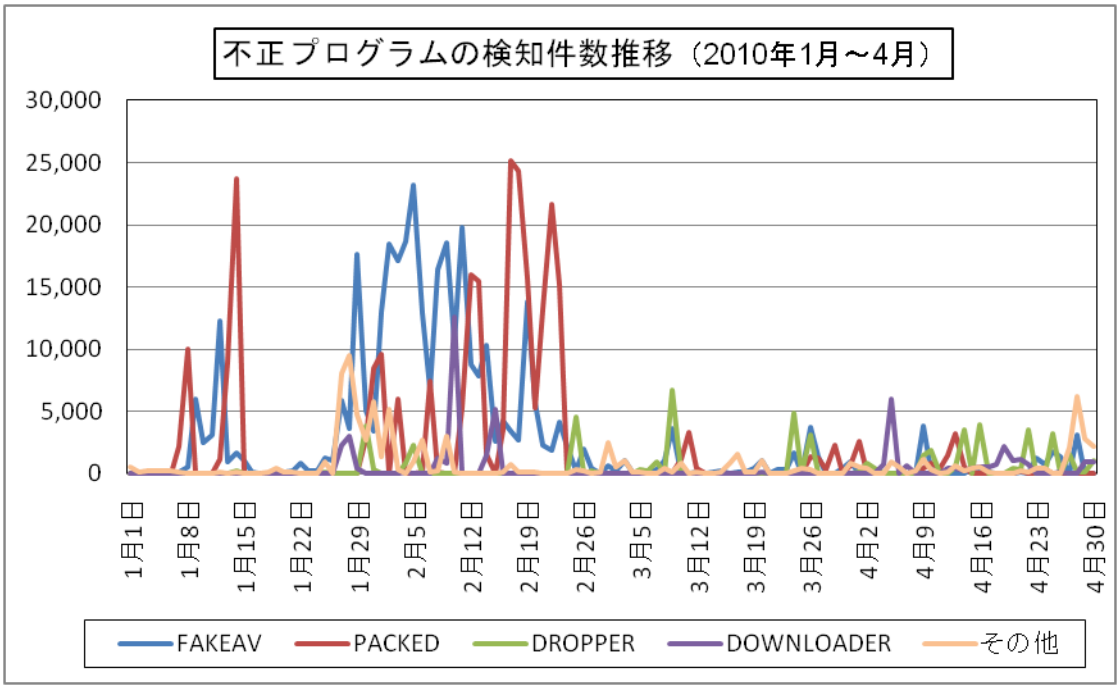


図 2-3：不正プログラムの検知件数推移

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

		11月	12月	1月	2月	3月	4月
届出(a) 計		11	9	20	27	19	11
	被害あり(b)	6	6	12	17	13	10
	被害なし(c)	5	3	8	10	6	1
相談(d) 計		34	22	67	47	60	39
	被害あり(e)	14	14	34	28	23	16
	被害なし(f)	20	8	33	19	37	23
合計(a+d)		45	31	87	74	79	50
	被害あり(b+e)	20	20	46	45	36	26
	被害なし(c+f)	25	11	41	29	43	24

（1）不正アクセス届出状況

4 月の届出件数は 11 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 39 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 16 件でした。

（3）被害状況

被害届出の内訳は、**侵入 5 件、なりすまし 3 件、不正プログラム埋め込み 1 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 2 件（内 1 件は不正なコードの挿入）、ウェブサーバ内に他サイトを攻撃するための不正プログラムを置かれ踏み台として悪用されていたものが 2 件、認証が必要な掲示板に勝手に書き込まれていたものが 1 件、でした。侵入の原因は、詳細は追い切れていないが“ガンブラー”の手口だと推測されるものが 1 件、ID/パスワード管理不備（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）が 1 件、ウェブアプリケーション（FCKeditor）の脆弱性を突かれたと思われるものが 1 件、設定不備が 1 件、などでした。

「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、他 1 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）SSH で使用するポートへの攻撃で侵入された

事例	・自社内からインターネットにつながらなくなった。 ・原因を調査する過程で、SSH で使用するポートから侵入され、ログファイルなどを削除されていたことが判明。 ・さらに、外部サイトの SSH で使用するポートに対してログインを試みていた形跡があった。 ・長期間ログインされていなかったアカウントのパスワードが破られたことが原因と思われた。
解説・対策	パスワード認証は、時間を掛ければいつかは破られる、という原則を再認識しましょう。ログのチェック、接続許可制限などの対策が有効ですが、SSH 運用時には、ログインの際に**公開鍵認証※などの強固な認証の採用を推奨**します。 また、**定期的にアカウントの利用状況を確認し、不必要なアカウントは廃止**するなどして、管理が手薄になることを避けましょう。 （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

※公開鍵認証…公開鍵と秘密鍵のペアで利用者個人の認証を行う方式のこと。

［なりすまし］

（ii）パスワード再発行の仕組みが悪用され、オンラインゲームのアカウントが乗っ取られた

事例	・ある日、ヤフーアカウントのログイン履歴を確認したら、明らかに自分によるものではないログインが成功しているのを発見。 ・不審に思い、他のサービスの状態を確認したところ、あるオンラインゲームの自分のアカウントが乗っ取られてアイテムが盗まれていることが判明。このゲームを始める際、連絡先として登録したのが、ヤフーのメールアドレスだった。 ・ゲームの ID とヤフーID が同じ文字列であり、かつヤフーアカウントのパスワードは推測が容易なものであった。このため、ヤフーのパスワードが破られヤフーアカウントが乗っ取られたことで、結果的に第三者によるオンラインゲームのログインパスワード再発行が成功したことが原因と推測。 ・今後は、ヤフーの“ログインアラート”サービスを使うこととした。
解説・対策	オンラインゲームサイトのパスワード再発行の仕組みが悪用された例です。**強固なパスワードを設定するとともに、ID やパスワードの使い回しは避けましょう**。オンラインサービスの中には、**ログインしたタイミングでお知らせメールを送信する機能**が提供されていることがあります。自分以外の誰かがログインした際に、お知らせメールが届けば、不正ログインに早く気付くことができ、被害を未然に防ぐことができます。 （参考） IPA -「ID とパスワードを適切に管理しましょう」 http://www.ipa.go.jp/security/txt/2010/03outline.html

4. 相談受付状況

4 月のウイルス・不正アクセス関連相談総件数は **2,110 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 **747 件**（3 月：725 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 **23 件**（3 月：12 件）、**Winny に関連する相談**が **11 件**（3 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 **4 件**（3 月：1 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

		11月	12月	1月	2月	3月	4月
合計		2,315	1,794	2,150	1,789	2,000	2,110
	自動応答システム	1,340	1,138	1,160	977	1,057	1,194
	電話	918	602	910	736	846	835
	電子メール	53	52	78	70	92	81
	その他	4	2	2	6	5	0

※ 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。

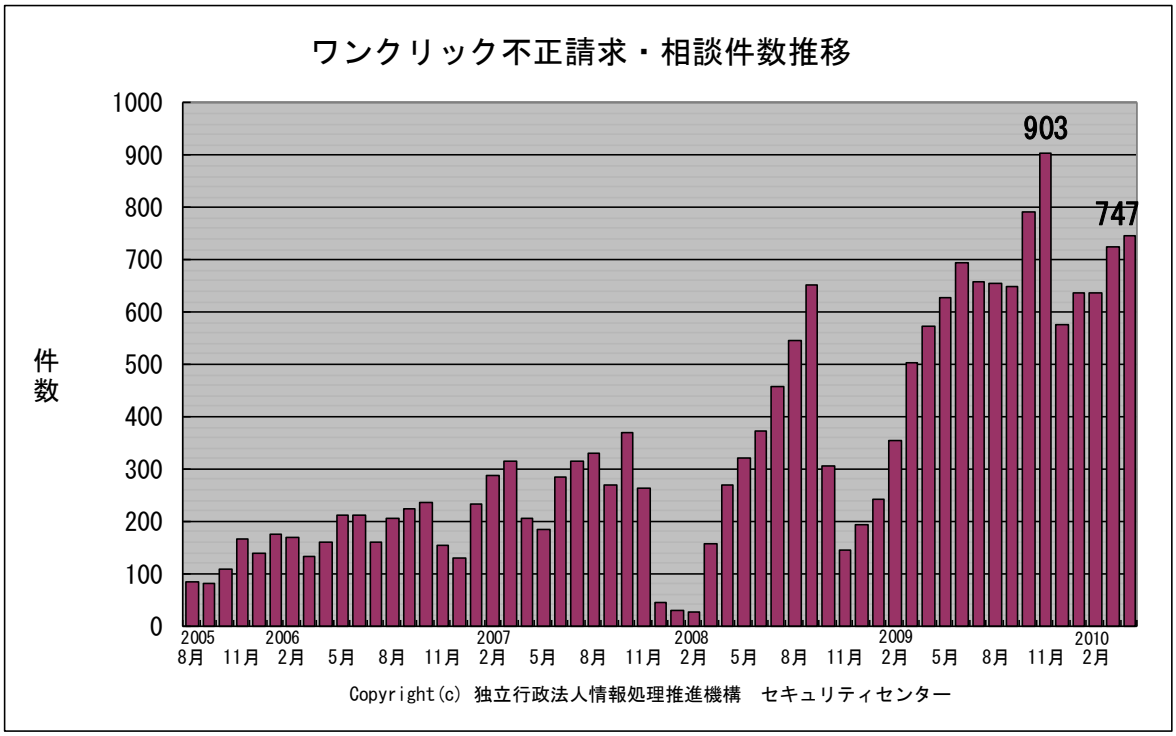


図 4-1：ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

（i）ワンクリック不正請求の被害から復旧できない

相談	アダルトサイトを見たことで請求書が定期的に出現するようになったため、IPA に相談したところ、「システムの復元」をするように案内された。アダルトサイトを見たのは、去年の 11 月。しかし、システムの復元ポイントは現在から 12 月のものまでしか保存されていなかったため、11 月以前の状態が保存されておらず、システムの復元ができない。
回答	システムの復元に使用するハードディスク領域には限りがあります。この領域がいっぱいになると、古い物から順に、復元ポイント情報が削除されていきます。ワンクリック不正請求に限らず、**パソコンの様子がおかしい！と思ったらできるだけ早く「システムの復元」をすることをお勧めします**。 （ご参考） IPA -【注意喚起】ワンクリック不正請求に関する相談急増！ パソコン利用者にとっての対策は、まずは手口を知ることから！ http://www.ipa.go.jp/security/topics/alert20080909.html

（ii）無線 LAN のセキュリティ設定について

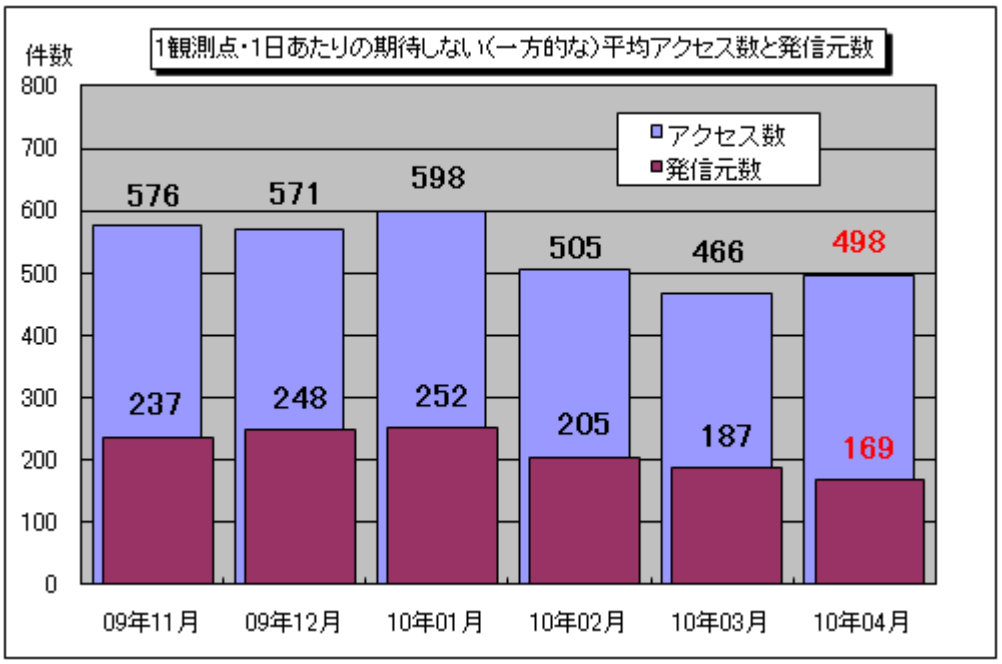
相談	無線 LAN を家庭で使っている。無線 LAN は、正しく設定しないと他人に利用される危険性があると聞いた。他人にアクセスさせないように対策したいが、自分では知識に乏しく、作業できそうにないのですが。
回答	無線 LAN 設定の基本は、“通信の暗号化”です。その際、**適切な暗号化方式（WPA2 および AES）を選択することと、パスワードを 20 文字以上にすることが重要**です。 親機ー子機間で WPS（Wi-Fi Protected Setup）などの“設定容易化機能”が使えると、設定が楽です。 それでも難しい場合は、**有償の訪問設定サービスを利用するのも良い**でしょう。パソコン購入店や無線 LAN 機器メーカーなどに相談してみましょう。 （ご参考） IPA - 一般家庭における無線 LAN のセキュリティに関する注意 http://www.ipa.go.jp/security/ciadr/wirelesslan.html

5. インターネット定点観測での 4 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 4 月の期待しない（一方的な）アクセスの総数は 10 観測点で **149,345 件**、延べ発信元数（※）は **50,563 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 169 の発信元から 498 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。

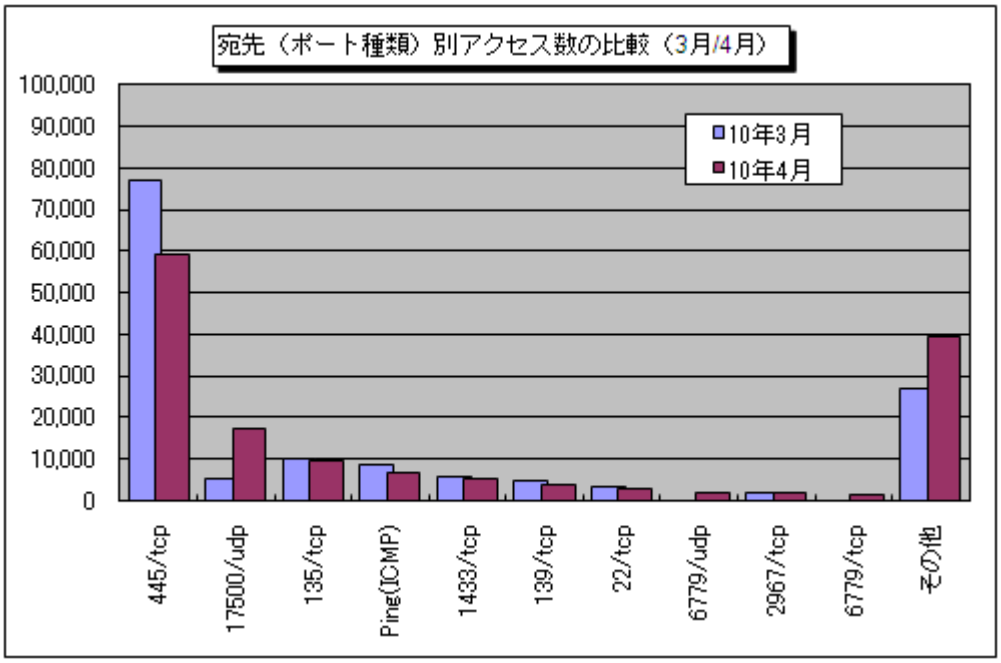


【図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数】

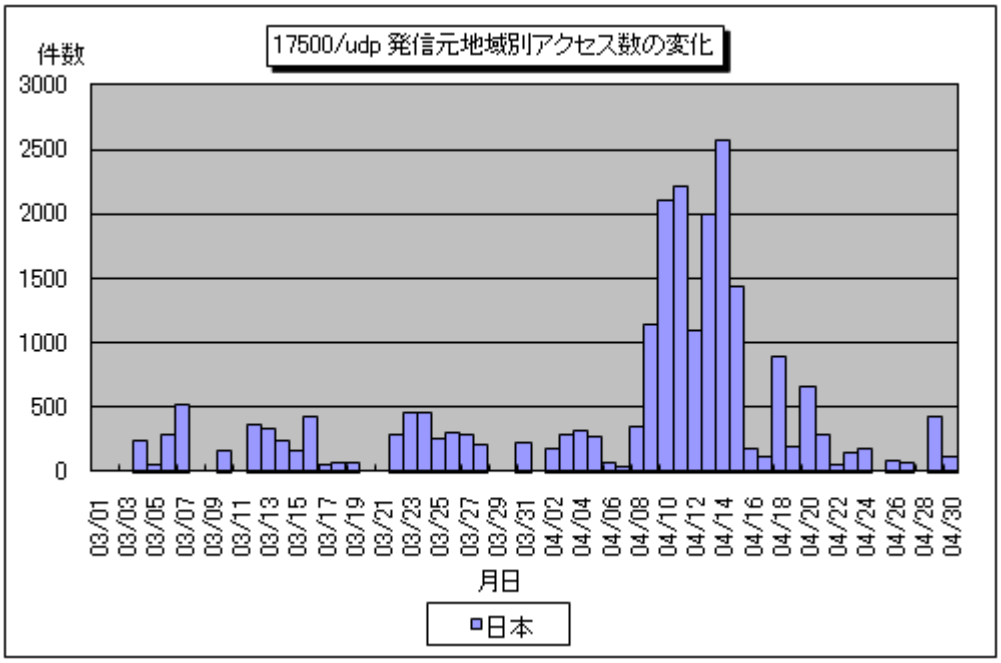
2009 年 11 月～2010 年 4 月までの各月の 1 観測点・1 日あたりの平均アクセス数とそれらのアクセスの平均発信元数を図 5-1 に示します。4 月の期待しない（一方的な）アクセスは、3 月と比べて増加しました。

3 月と 4 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 3 月に増加が観測されていた 17500/udp へのアクセスが、さらに大幅な増加を示していました（図 5-3 参照）。こ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、3 月は全く観測されなかった 6779/tcp および 6779/udp へのアクセスが、多く観測されました。これらのポートは、特定のアプリケーションで使用されるポートというわけではなく、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、いずれも特定の 1 観測点でしか観測されていませんでした。



【図 5-2：宛先（ポート種類）別アクセス数の比較（3 月/4 月）】



【図 5-3：17500/udp 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/2010/documents/TALOT2-1005.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