プレスリリース
第 10-44-202 号
2010 年 12 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 11 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 11 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！」

2009 年から 2010 年にかけて猛威を振るったガンブラー※1 ではウェブサイトを閲覧しただけで、利用者のパソコンにウイルスを感染させられてしまう“ドライブ・バイ・ダウンロード（Drive-by Download）”攻撃の手法が使われていましたが、この手法を用いて国内の多数のウェブサイトに影響を及ぼした新たな攻撃が、2010 年 9 月と 10 月に相次いで発生しました。今後も様々な形で“ドライブ・バイ・ダウンロード”攻撃が行われると思われるため、引き続き注意が必要です。

ここでは、改めて“ドライブ・バイ・ダウンロード”攻撃について整理するとともに、ウェブサイト管理者、パソコン利用者の対策について解説します。

※1 「"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

（1）“ドライブ・バイ・ダウンロード”攻撃とは

“ドライブ・バイ・ダウンロード”攻撃とは、ウェブサイトを閲覧した際に、パソコン利用者の意図に関わらず、ウイルスなどの不正プログラムをパソコンにダウンロードさせる攻撃のことをいいます。“ドライブ・バイ・ダウンロード”攻撃では、主に利用者のパソコンの OS やアプリケーションなどの脆弱性が悪用されます。

攻撃の主な流れについて図 1-1 を例に説明します。

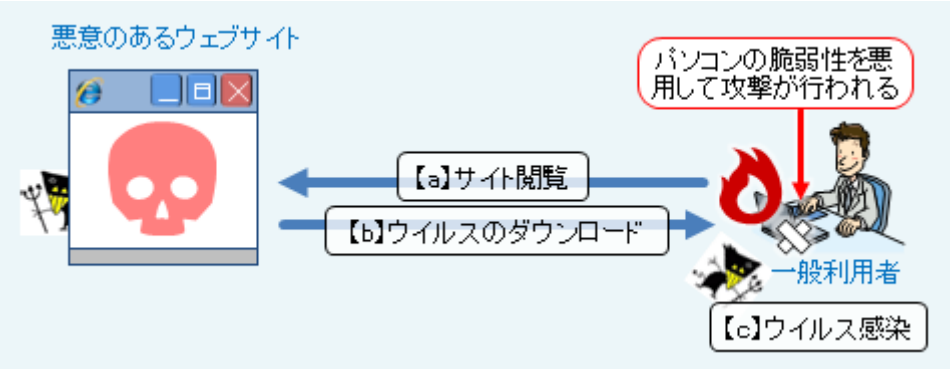

図 1-1：”ドライブ・バイ・ダウンロード”攻撃のイメージ

- パソコン利用者が悪意あるウェブサイトを閲覧する（図中【a】）。
- 利用者のパソコンの脆弱性を突かれて、ウイルスをダウンロードさせられる（図中【b】）。
- 利用者のパソコンにウイルスを感染させられる（図中【c】）。

（2）最近の“ドライブ・バイ・ダウンロード”攻撃の事例について

“ドライブ・バイ・ダウンロード”攻撃を使った事例としては、2009 年から 2010 年にかけて猛威を振るった、ガンブラーが有名ですが、2010 年 9 月には広告配信サービス会社のサイトを改ざんするという新たな手法を使って国内の多数のウェブサイトに影響を及ぼした攻撃が発生しました。ガンブラーの場合も広告配信サイト改ざんの事例の場合も、正規のウェブサイトを改ざんすることによって、上記（1）で説明した“ドライブ・バイ・ダウンロード”攻撃を応用した、閲覧者を悪意あるウェブサイトに誘導するための仕掛けを施すという手法が使われていました。

ガンブラーの場合と広告配信サイト改ざんの事例の場合の違いは、攻撃者が改ざんする箇所にありました。具体的な違いは以下のとおりです。

(i)ガンブラーの場合

ガンブラーの場合は、攻撃者が正規のウェブサイト自体を直接改ざんすることで、当該ウェブサイトの閲覧者が、意図せずに悪意あるウェブサイトに誘導され、ウイルスをダウンロードさせられていました（図 1-2 参照）。

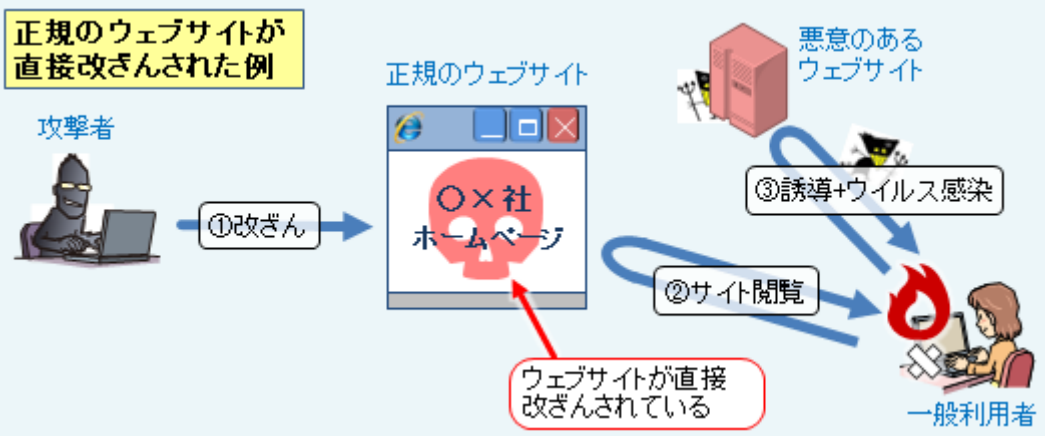

図 1-2：正規のウェブサイトが直接改ざんされた例のイメージ

(ii)広告配信サイト改ざんの事例の場合

広告配信サイト改ざんの事例の場合は、ガンブラーのようにウェブサイト自体が改ざんされたわけではなく、ウェブサイトを構成する部品（バナー広告など）が改ざんされていました。攻撃者がウェブサイトを構成する部品を提供している企業のサーバに侵入し、部品を改ざんすることにより、その企業から部品の提供を受けている企業のウェブサイトの閲覧者が、意図せず悪意あるウェブサイトに誘導され、ウイルスをダウンロードさせられるというものでした（図 1-3 参照）。この事例の場合、正規のウェブサイト側で作成した部分には改ざん箇所が見つからないため、問題箇所の特定が非常に困難です。

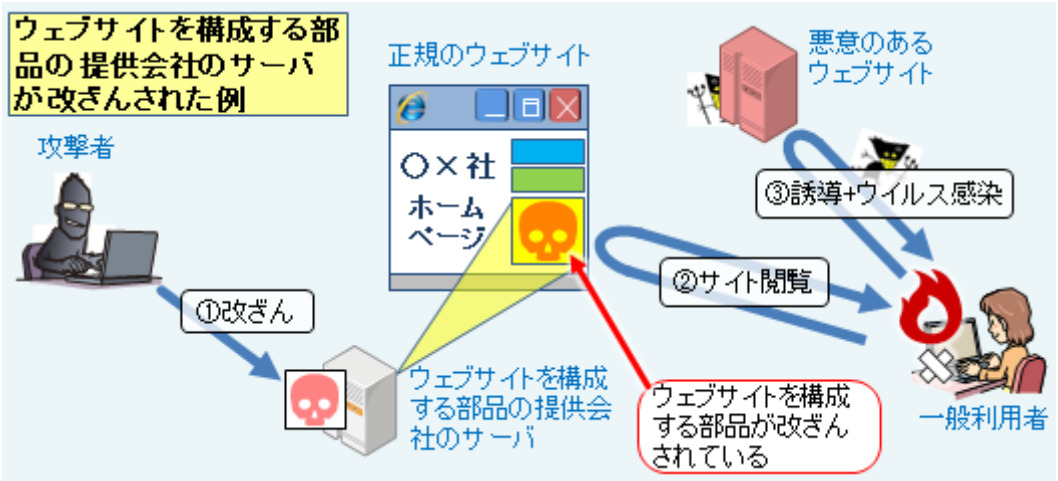

図 1-3：ウェブページを構成する部品の提供会社のサーバが改ざんされた例のイメージ

このように今回紹介した新たな事例では、問題箇所を発見しにくいため対策が非常に困難ですが、(3)

項に示すような被害軽減策がありますので、利用することをお勧めします。

（3）ウェブサイト管理者向けの対策（被害軽減策）

今回紹介した事例に適用できるウェブサイト管理者向けの被害軽減策を、以下に説明します。

（i）セキュリティ専門会社が提供しているサービスの利用

今回紹介した事例における被害を軽減する方法としては、セキュリティ専門会社が提供するサービスを利用することが挙げられます。自身の管理するウェブサイトが、改ざんされていないか、また”ドライブ・バイ・ダウンロード”攻撃に使われていないかを監視するサービスが有効です。

（ii）複数のウイルス対策ソフトによるウェブサイトのチェック

複数種類（なるべく多い方がよい）のウイルス対策ソフトを用意し、それぞれのウイルス対策ソフトをインストールしたパソコンを使って、自組織のウェブサイトを定期的にチェックします。複数のウイルス対策ソフトでチェックを行うことで、問題箇所を発見できる可能性が高まります。

また、今回のように自身で作成したウェブサイト自体には改ざん箇所が見当たらないにも関わらず、ウェブサイトの閲覧者から、「あなたの会社のウェブサイトを閲覧したら、ウイルス対策ソフトがウイルスを検知した」などといった連絡があった場合は、IPA に相談してください。

（ご参考）
情報セキュリティ安心相談窓口（IPA）
http://www.ipa.go.jp/security/anshin/
ウェブサイト管理者へ：ウェブサイト改ざんに関する注意喚起
一般利用者へ：改ざんされたウェブサイトからのウイルス感染に関する注意喚起（IPA）
http://www.ipa.go.jp/security/topics/20091224.html

（4）パソコン利用者向けの対策

今回紹介した新たな事例は、ウェブサイト管理者にとっては非常に厄介なものですが、パソコン利用者の対策はこれまでと変わりません。このような攻撃に対する「被害に遭わないための対策」と、被害にあった場合の「復旧のための対策」を以下に示します。

（i）被害に遭わないための対策

このような攻撃の被害に遭わないためには、Windows などの OS や、アプリケーションの脆弱性を解消しておくことが重要です。一般的に利用の多いアプリケーションは狙われやすい傾向にあるため、脆弱性を解消して、常に最新の状態で使用してください。IPA では利用者のパソコンにインストールされている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」を公開しています。

（ご参考）
MyJVN バージョンチェッカ（IPA）
http://jvndb.jvn.jp/apis/myjvn/#VCCHECK
「ホームページからの感染を防ぐために」（サイバークリーンセンター）
https://www.ccc.go.jp/detail/web/

また、最近では、ガンブラーや今回紹介した新たな事例のように、正規のウェブサイトが改ざんされ、危険な状態になっている場合があります。このようなサイトからのウイルス感染を防ぐためには、ウイルス対策ソフトの利用が必須です。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ってください。

（ii）復旧のための対策

ウェブサイトを閲覧した後、明らかにパソコンの動作がおかしくなり、ウイルスに感染した可能

性があると感じられるにも関わらず、ウイルス対策ソフトによるウイルスの発見や駆除ができない場合、IPA では、確実にウイルスを除去する手段として、パソコンの初期化（購入時の状態に戻す）をお勧めします。

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、6 頁の「3.コンピュータ不正アクセス届出状況」を参照）
- ウェブサイト内に不正なページを追加されていた
- 特定の IP アドレスから大量のアクセスを受けた

○ 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）
- 自宅の無線 LAN ルーターに見覚えのない機器が接続されている
- 会社のパソコンに USB メモリを挿したらウイルスが見つかった

○ 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

11 月のウイルスの検出数※1は、**約 3.2 万個**と、10 月の約 3.4 万個から 7.2%の減少となりました。また、11 月の届出件数※2は、**1,094 件**となり、10 月の 996 件から 9.8%の増加となりました。

※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。
- 11 月は、寄せられたウイルス検出数約 3.2 万個を集約した結果、1,094 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 2.3 万個**、2 位は **W32/Mydoom** で**約 4 千個**、3 位は **W32/Autorun** で**約 1 千個**でした。

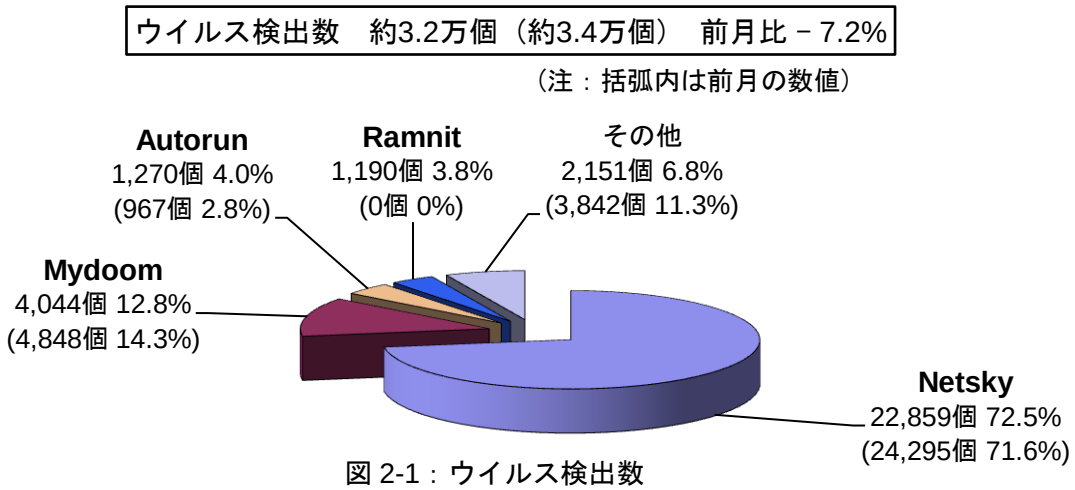

図 2-1：ウイルス検出数

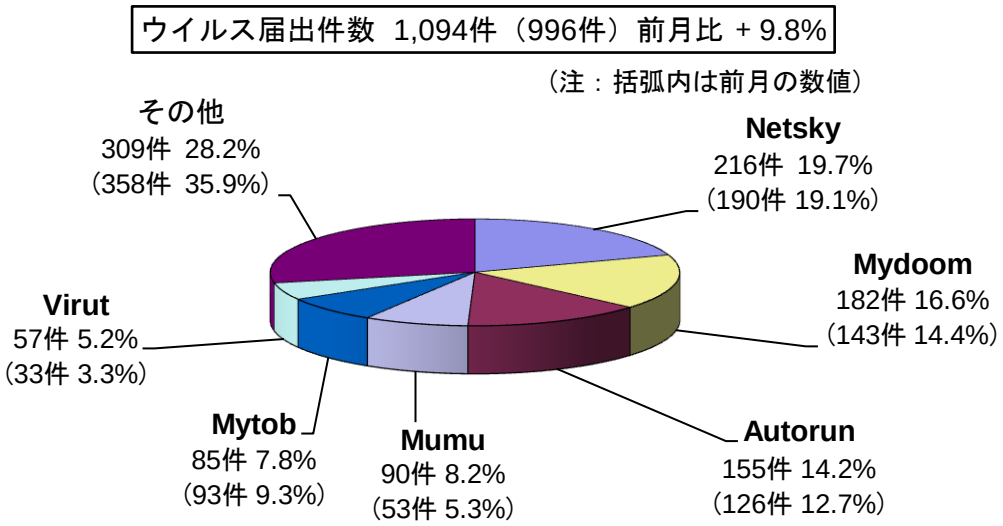

図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

2010 年 11 月の不正プログラムの検知状況は、急増した事例は確認されず、10 月と同様の傾向となりました（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/

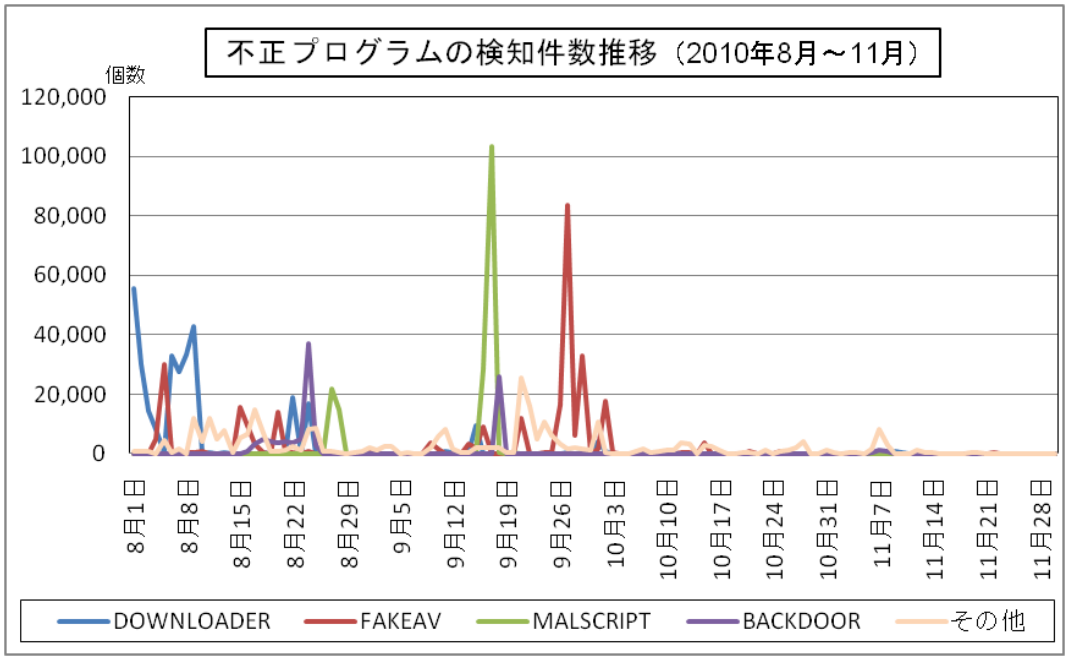

図 2-3：不正プログラムの検知件数推移

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

		6月	7月	8月	9月	10月	11月
届出(a)　計		15	14	18	15	14	14
	被害あり(b)	13	9	12	10	8	7
	被害なし(c)	2	5	6	5	6	7
相談(d)　計		77	44	56	47	40	45
	被害あり(e)	50	23	16	8	15	12
	被害なし(f)	27	21	40	39	25	33
合計(a+d)		92	58	74	62	54	59
	被害あり(b+e)	63	32	28	18	23	19
	被害なし(c+f)	29	26	46	44	31	40

（1）不正アクセス届出状況

11 月の届出件数は 14 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 45 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 12 件でした。

（3）被害状況

被害届出の内訳は、**侵入 4 件、DoS 攻撃 1 件、なりすまし 2 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、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 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 1 件、でした（他は原因不明）。

（4）被害事例

［侵入］

（i）ウェブサイト内に不正なページを追加されていた

事例	・公開しているウェブサイト内に、身に覚えのない不正なページが追加されていた。外部からの連絡で発覚。 ・ウェブサイト管理用ページから、不正にログインされて改ざんされたものと判明。 ・アクセスログを解析したところ、特定サーバを介しての不正なアクセスが見受けられた。 ・サイト管理用の ID とパスワードが比較的推測され易いものだったことが原因と思われた。
解説・対策	サイト管理用の ID／パスワードに対して、**ブルートフォース攻撃（総当り攻撃）や辞書攻撃を受けたと思われます。**定期的な ID／パスワードの変更や、ウェブサイトのチェックを行うことをお勧めします。また、こうした管理画面は、**IP アドレスによるアクセス制限を施し、決められた管理パソコン以外のアクセスを遮断**する対策が有効です。 （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

［DoS］

（ii）特定の IP アドレスから大量のアクセスを受けた

事例	・通販を行っているサイトに対して、特定の IP アドレスから大量のアクセスを受け、その影響でウェブサイト全体のレスポンスが低下した。 ・複数店舗全ての商品情報に対して、短時間に大量のアクセスがあった。 ・その結果、一般利用者のアクセスについてレスポンスが著しく遅くなり、サイト内のサービスが利用不能になった。 ・大量にアクセスしてくる IP アドレスに対して、ファイアウォールで遮断をすると、別の IP アドレスから同様のアクセスがくる状況。
解説・対策	今回のようなアクセスは、通常の利用形態ではあまり考えられないものですが、**こういったアクセスの極端な集中を想定した、システム構成やネットワーク構成の見直しを行うこともよいでしょう。**第三者のパソコンを踏み台にして攻撃している可能性も考えられますので、**特定の IP アドレスからのアクセスであれば、該当 IP アドレスを管理しているプロバイダに相談することをお勧めします。また、大量のアクセスが継続しているが、システムの停止は許されないといった場合には、上位のプロバイダでの対処が有効**になる場合があります。 （参考） JPCERT/CC - 技術メモ - サービス運用妨害攻撃に対する防衛 http://www.jpcert.or.jp/ed/2001/ed010005.txt

4. 相談受付状況

11 月のウイルス・不正アクセス関連相談総件数は **1,692 件**でした。そのうち**『ワンクリック請求』に関する相談**が **483 件**（10 月：603 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 **18 件**（10 月：13 件）、**Winny に関連する相談**が **8 件**（10 月：7 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 **10 件**（10 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

		6月	7月	8月	9月	10月	11月
合計		1,983	2,133	2,432	2,102	1,813	1,692
	自動応答システム	1,022	1,142	1,298	1,142	1,065	1,036
	電話	829	924	1,053	872	675	580
	電子メール	129	66	75	85	69	72
	その他	3	1	6	3	4	4

※ 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。

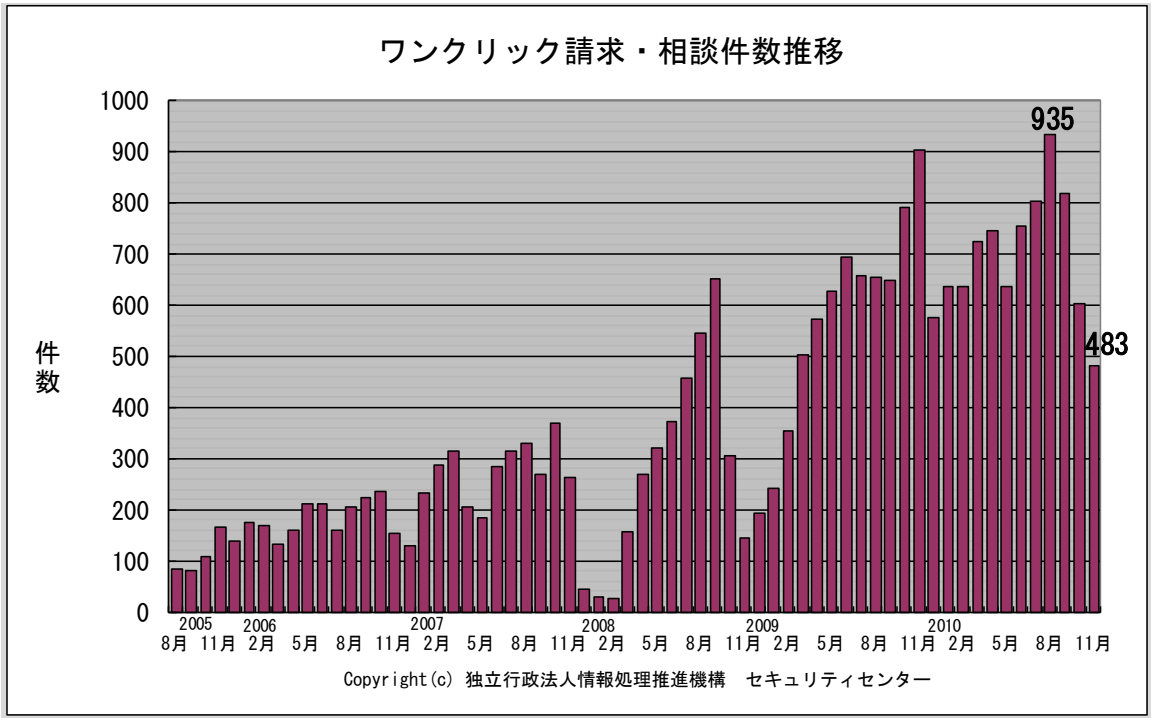

図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）自宅の無線 LAN ルーターに見覚えのない機器が接続されている

	自宅の無線 LAN アクセスポイントの接続状況を確認してみたところ、「XX-XX-iPhone」という見覚えのない機器名が登録されていることに気づいた。家族の中で iPhone を使用している者はいないので、なぜ登録されているのか分からない。
回答	無線 LAN 通信の暗号化設定をしていなかったために、**自宅周辺で見知らぬ iPhone 利用者が貴方の無線 LAN アクセスポイントに“ただ乗り”していたのだと思われます**。 無線 LAN を無防備な状態にしていると、無線 LAN 環境を勝手に使用されたり、通信内容を傍受されたりする可能性があります。 無線 LAN を安全に使うためには、**適切な暗号化方式（WPA2 および AES）を選択し、パスワードを 20 文字以上にすることが重要**です。 （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

（ii）会社のパソコンに USB メモリを挿したらウイルスが見つかった

相談	普段から USB メモリを使って、会社のパソコン（ウイルス対策ソフトあり）と自宅のパソコン（ウイルス対策ソフトなし）の間で業務文書のやり取りをしていた。ある時、USB メモリを会社のパソコンに挿したら、「ウイルスが検出されました」とウイルス対策ソフトが警告を出した。どうしたらいいか。
回答	会社のパソコンについては、ウイルス感染前にウイルス対策ソフトが検知していますので感染していないと思いますが、ウイルス対策ソフトが入っていない自宅のパソコンには感染している可能性が高いです。 会社で使用しているウイルス対策ソフトならば検知可能ということですので、同じメーカーの**ウイルス対策ソフトを購入し自宅のパソコンをチェックしてみることをお勧めします**。 一歩間違えば、会社のパソコンにもウイルスが感染していた可能性があります。**社内で USB メモリを使うルールについて、改めて検討をすべき**です。 （ご参考） IPA－2009 年 5 月の呼びかけ「 USB メモリのセキュリティ対策を意識していますか？」 http://www.ipa.go.jp/security/txt/2009/05outline.html

5. インターネット定点観測での 11 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 11 月の期待しない（一方的な）アクセスの総数は 10 観測点で **83,479 件**、延べ発信元数※は **38,329 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 128 の発信元から 278 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。

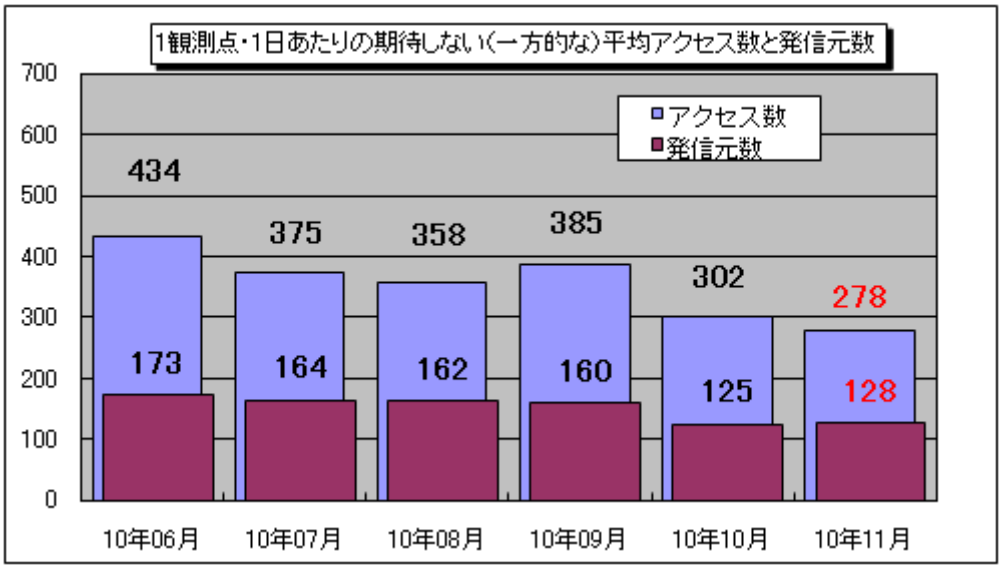

図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数

2010 年 6 月～2010 年 11 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。11 月の期待しない（一方的な）アクセスは、10 月と比べて減少しました。

10 月と 11 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、10 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。これは、10 月の下旬から TALOT2 の複数の観測点に対して海外の複数の発信元からのアクセスが増えたものでした。

また、6 月、8 月、9 月の報告で取り上げました 9415/udp へのアクセスは、10 月の中旬をピークに、減少に転じている傾向が観測されていました（図 5-3 参照）。この 9415/udp 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いますが、このポートを探索する中国からのアクセスが減少したことが要因と推測されます。

（ご参考）

2010 年 5 月のインターネット定点観測（TALOT2）での観測状況について（IPA）
http://www.ipa.go.jp/security/txt/2010/documents/TALOT2-1006.pdf
2010 年 8 月のインターネット定点観測（TALOT2）での観測状況について（IPA）
http://www.ipa.go.jp/security/txt/2010/documents/TALOT2-1009.pdf
2010 年 9 月のインターネット定点観測（TALOT2）での観測状況について（IPA）
http://www.ipa.go.jp/security/txt/2010/documents/TALOT2-1010.pdf

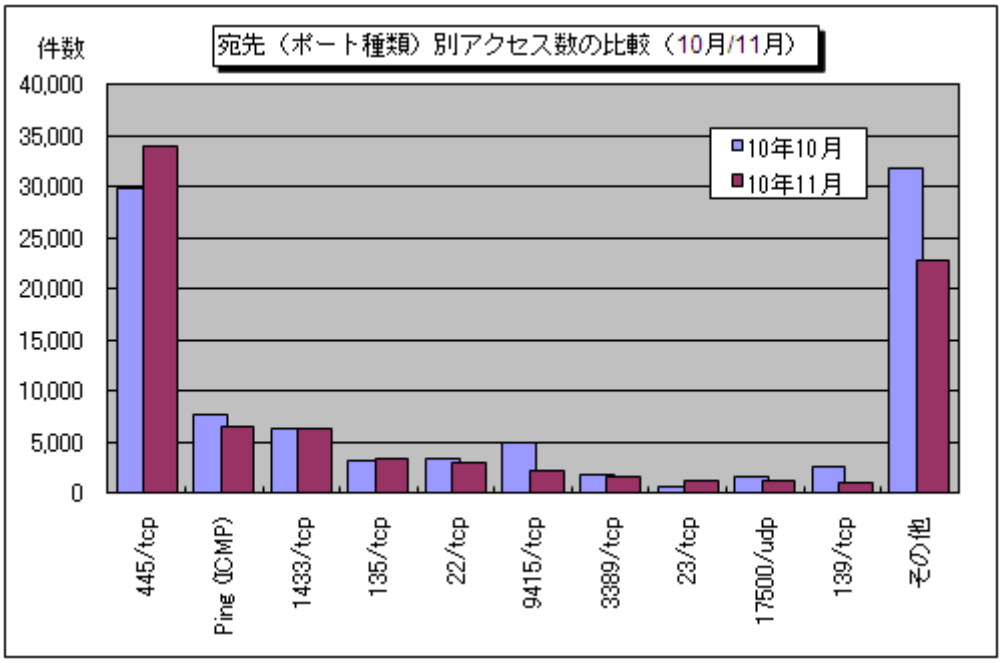

図 5-2：宛先（ポート種類）別アクセス数の比較（10 月/11 月）

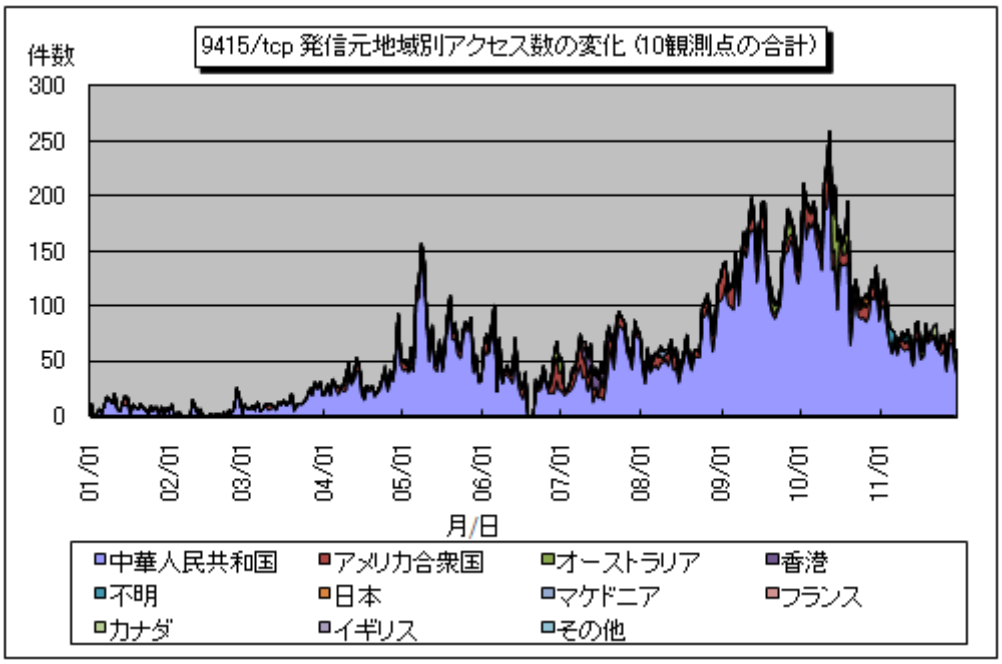

図 5-3：9415/tcp 発信元地域別アクセス数の変化（10 観測点の合計）

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/TALOT2-1012.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