INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
第 11-07-209 号
2011 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［2011 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：藤江 一正）は、2011 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

「 USB メモリ等に対する“自動実行（オートラン）”機能を無効化しましょう！ 」
～ Windows Update することで対応できます！ ～

USB メモリ等の外部記憶媒体を介してウイルスに感染する被害が多く発生しています。IPA が 2010 年に実施した調査※1 では、発見したウイルスの侵入経路として「外部媒体、持ち込みパソコン」によるものが 48%もありました。また、原子力発電所の制御システムを狙ったとされるウイルス※2 も、USB メモリを介した感染を意図していたとされています。

USB メモリ等の外部記憶媒体を介したウイルス感染方法が使われる要因の一つとして、Windows パソコンの「自動実行」機能※3 が挙げられます。これは、USB メモリなどの外部記憶媒体をパソコンに接続しただけで、その中に保存されているファイルを自動的に実行する機能のことで、“オートラン”とも呼ばれています。この機能を無効にすることで、USB メモリ等を介したウイルス感染の危険を軽減することができます。

IPA は、以前も“オートラン”の無効化について呼びかけたことがありますが、2011 年 2 月から、無効化する手順がより簡単になりましたので、改めて“オートラン”やそれを悪用するウイルス、被害を防ぐための対策について説明します。

(1)”オートラン”とは

Windows の“オートラン”とは、CD、DVD、USB 経由で接続するメモリや外付けハードディスク等の外部記憶媒体をパソコンに接続した際に、その中に保存されているプログラムや動画を自動的に実行、再生する機能です。

この機能を悪用するウイルスは、次のような動作で感染活動を行います（図 1-1 参照）。

【1】 ウイルスが混入した USB メモリを接続した、不審なメールの添付ファイルを開いたといった原因により、ウイルスに感染しているパソコンがあります。
【2】 そのパソコンに USB メモリを接続すると、ウイルスは USB メモリにウイルス自身のコピーを作成して潜伏します。同時に、“オートラン”を悪用するための命令を仕掛けます。
【3】 ウイルスが潜伏している USB メモリを、ウイルス対策が不十分な別のパソコンに接続して利用すると、“オートラン”によりウイルスが自動実行されます。これにより、このパソコンもウイルスに感染させられてしまいます。
【4】 以上の動作の繰り返しで、連鎖的に感染が広がる可能性があります。

※1 2009 年 国内における情報セキュリティ事象被害状況調査
http://www.ipa.go.jp/security/fy21/reports/isec-survey/
※2 Stuxnet と呼ばれるウイルスによるもの。詳細は、IPA テクニカルウォッチ『新しいタイプの攻撃』に関するレポートを参照のこと。http://www.ipa.go.jp/about/technicalwatch/20101217.html
※3 初期状態で有効なのは Windows XP、Vista、Windows Server 2003、2008。Windows 7 は初期状態で無効。

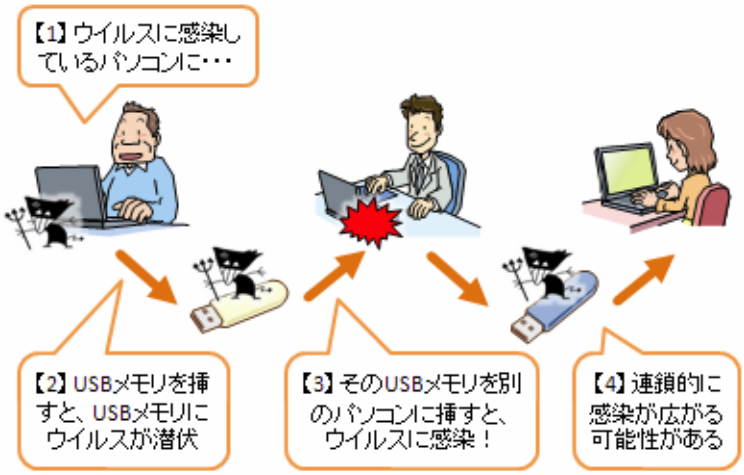

図 1-1：“オートラン”を悪用したウイルスの感染動作

(2)”オートラン”を悪用するウイルスの例

“オートラン”を悪用するウイルスは、珍しいタイプではなく、一般化しています。例えば W32/Virut ウイルスのように、出現した当初はその機能がなくても、その後に出現した亜種には“オートラン”を悪用して感染する仕組みが追加された事例も確認しています。

IPA に寄せられた届出をみると、2011 年 2 月の届出件数の上位 10 種に W32/Autorun、W32/Downad、W32/Sality や W32/Virut といった“オートラン”を悪用して感染を拡大するウイルスが多数入っています。特に W32/Autorun は、この一年間、月平均約 170 件の届出がありました。

これらのウイルスに感染すると、USB メモリ等を介して感染被害が拡大する恐れがあるとともに、セキュリティソフトが使えなくなる、オンラインゲームのアカウント情報などのパソコン内の情報が外部に漏えいする、といった被害が発生する危険性があります。

また、IPA 情報セキュリティ安心相談窓口※4 へは、以下のような相談も寄せられています。

- 自宅のパソコンにあるデータを USB メモリにコピーして、その USB メモリを会社のパソコンに接続したらウイルスが検出された。原因を調査したら、自宅のパソコンが“オートラン”を悪用するウイルスに感染していた。
- パソコンに USB メモリを接続して作業をしてから、セキュリティベンダーのウェブサイトが閲覧できなくなった。原因を調査したら、接続した USB メモリにウイルスが混入していた。

このような相談は毎月のように寄せられており、依然として、“オートラン”を悪用するウイルスによる被害が発生しています。

(3)”オートラン”の無効化手順

“オートラン”を無効化※5 する方法は複数ありますが、日本マイクロソフト社提供のパッチ※6 をインストールする方法が簡単です。今までは専用のダウンロードサイトにアクセスし、利用者のパソコンの OS に適合するパッチを選択してインストールする必要がありましたが、2011 年 2 月 9 日（日本時間）から、Windows Update でも配布されるようになりました。これにより、利用者のパソコンに適合するパッチが自動的に選択・表示されるため、容易にインストールすることができます。

なお、Windows 7 については初期状態で“オートラン”は無効ですので、作業の必要はありません。

※4 IPA が国民に向けて開設している、マルウェア（不正なプログラム）および不正アクセスに関する総合的な相談窓口。
http://www.ipa.go.jp/security/anshin/

※5 ここで紹介する無効化とは、USB メモリ等が接続された場合に“オートラン”を無効化し、CD、DVD ドライブのみで“オートラン”が動作するように制限するものです。

※6 パッチ（patch）：脆弱性等の不具合を解消するためのプログラム。修正プログラム、更新プログラムともいう。

また、既にパッチをインストールしているパソコンでは、更新プログラムのリストに表示されませんので、作業する必要はありません。

パッチのインストールは、まず Windows Update にアクセスし、図 1-2 の画面が表示されたら、それぞれ以下の手順で行います。これで、“オートラン”を無効にすることができます。

- Windows Vista
  「重要」の項目にある「KB971029」の番号が記載されたパッチを選択してインストールします。
- Windows XP
  「優先度の高い更新プログラム」の項目にある「KB971029」の番号が記載されたパッチを選択してインストールします。

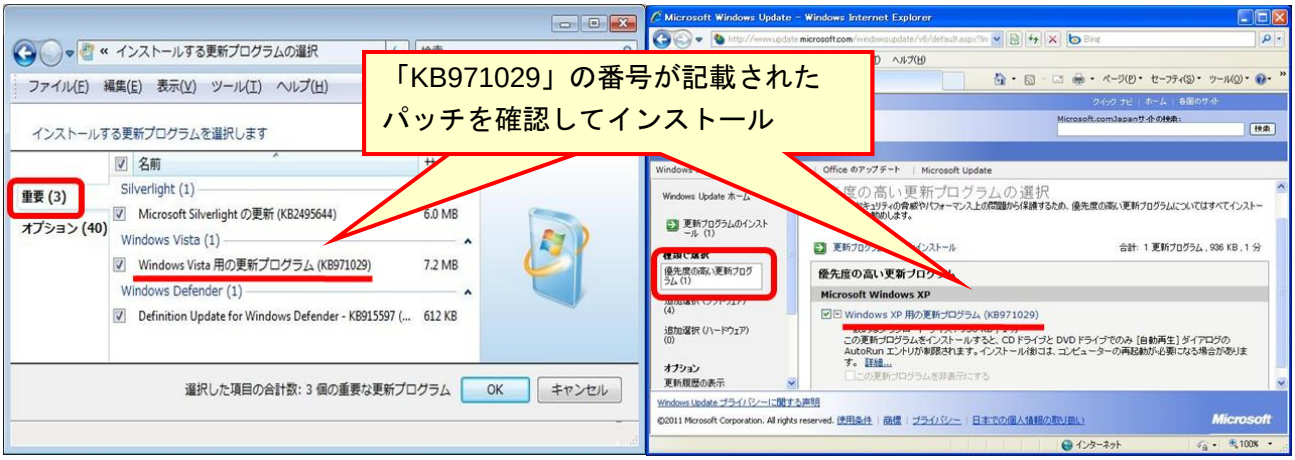

図 1-2：Windows Update の画面（左：Vista、右：XP）

企業等の情報システム管理者向けの情報として、グループポリシーによる設定をすることで、“オートラン”を無効化する方法もあります（詳細は以下のサイト参照）。

（ご参考）
Windows で自動実行機能を無効にする方法（日本マイクロソフト社）
http://support.microsoft.com/kb/967715/ja

なお、“オートラン”が無効になっているか確認するためのツールとして、IPA では「MyJVN セキュリティ設定チェッカ」を提供しています。このツールを利用することで、お使いのパソコンにおける“オートラン”の設定が確認できますのでご活用ください。

（ご参考）
MyJVN セキュリティ設定チェッカ（IPA）
http://jvndb.jvn.jp/apis/myjvn/#CCCHECK

（4）ウイルス感染予防策

（i）技術的対策を実施する

“オートラン”を無効にするとともに、次の技術的対策を併せて実施することで、ウイルスに感染する危険を減らすことができます。また、これらの対策は、“オートラン”を悪用するウイルスだけでなく、ウイルス全般に対して効果がありますので、ウイルスによる感染被害を防ぐために実施してください。

- ウイルス対策ソフトの利用
  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ようにしてください。これにより、USB メモリ等の外部記憶媒体が接続された際に検査され、ウイルス感染を防ぐことができます。

- 脆弱性を解消する（Windows Update の利用）

  OS やアプリケーションソフトには、次々と脆弱性が発見されています。新たな脆弱性を悪用するウイルスが出現し、“オートラン”を無効化していても USB メモリを接続しただけでウイルスに感染してしまう事態が起きる可能性もあります。利用しているパソコンの OS やアプリケーションソフトは、常に最新の状態に更新することで、脆弱性を解消してください。

  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アプリケーションソフトのバージョンが最新であるかを、簡単な操作で確認できるツール「MyJVN バージョンチェッカ」を無償で公開しています。本ツールの確認対象は、今までにウイルス等の攻撃に悪用されたことがある注意すべきソフトですので、ぜひご活用ください。

（ii）USB メモリなどを利用する際の注意事項

“オートラン”は、USB メモリの他、外付けハードディスク、デジカメ、ミュージックプレイヤー、SD メモリカードなど、パソコンに接続してデータをやり取りする外部記憶媒体が対象になります。これらを取り扱う際は、以下のことに注意してください。

- 自身が管理していないパソコンや不特定多数が利用するパソコンに、むやみに自身の USB メモリ等を接続しない。
- 自身が管理していない USB メモリや所有者不明な USB メモリを、むやみに自分のパソコンに接続しない。

（ご参考）

「Microsoft Update を使用してコンピューターを最新の状態に保つ」（日本マイクロソフト社）
http://www.microsoft.com/japan/protect/computer/updates/mu.mspx

「マイクロソフト　セキュリティ情報センター」（日本マイクロソフト社）
http://www.microsoft.com/japan/security/sicinfo/default.mspx

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

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）
- サーバが不正なプログラムを動かされて、外部のコンピュータを攻撃していた。
- ウェブサービスのログイン履歴に身に覚えのない海外からのログイン記録があった

○ 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）
- 偽セキュリティソフトの警告は本当か
- Internet Explorer のタイトルバーに「Hacked by Godzilla」と出ている

○ 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－

2 月のウイルスの検出数※1 は、**約 2.2 万個**と、1 月の約 2.3 万個から 2.7%の減少となりました。また、2 月の届出件数※2 は、**974 件**となり、1 月の 1,106 件から 11.9%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 2.2 万個を集約した結果、974 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 1.6 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。

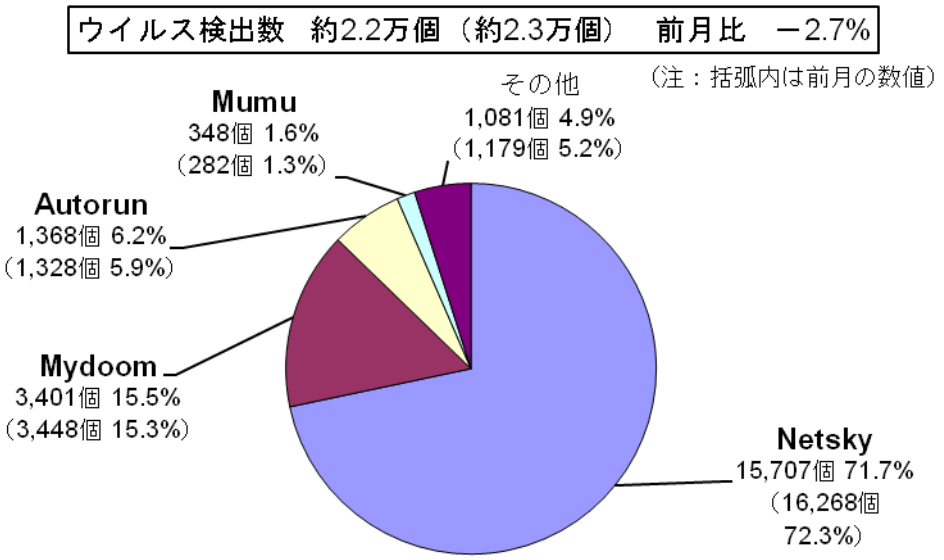

図 2-1：ウイルス検出数

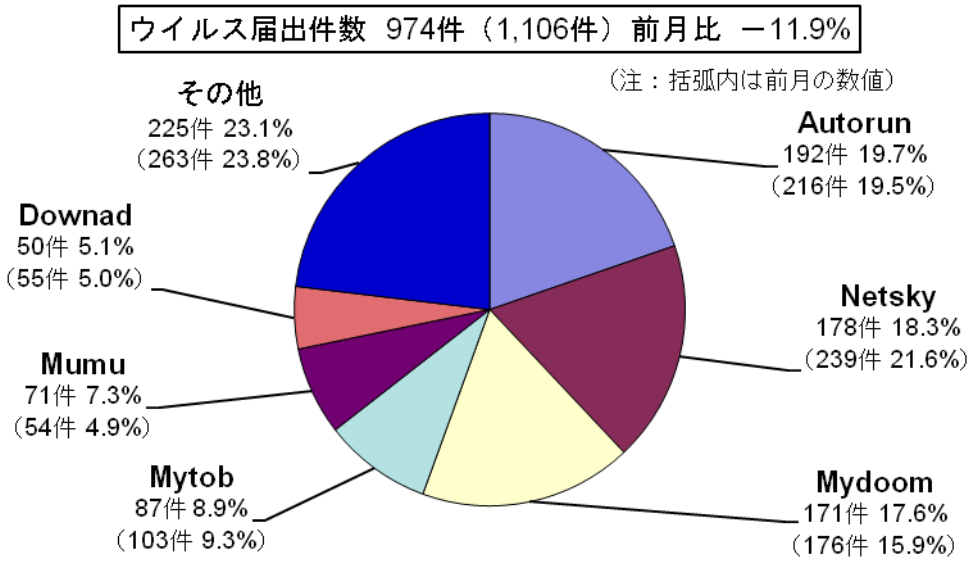

図 2-2：ウイルス届出件数

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		15	14	14	22	12	10
	被害あり(b)	10	8	7	7	6	5
	被害なし(c)	5	6	7	15	6	5
相談(d) 計		47	40	45	27	41	23
	被害あり(e)	8	15	12	7	11	6
	被害なし(f)	39	25	33	20	30	17
合計(a+d)		62	54	59	49	53	33
	被害あり(b+e)	18	23	19	14	17	11
	被害なし(c+f)	44	31	40	35	36	22

（1）不正アクセス届出状況

2 月の届出件数は 10 件であり、そのうち何らかの被害のあったものは 5 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 23 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 6 件でした。

（3）被害状況

被害届出の内訳は、**侵入 2 件、なりすまし 1 件、不正プログラム埋め込み 1 件、DoS 攻撃 1 件、**でした。

「侵入」の被害は、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。「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（ウェブサービス 1 件）、でした。

「侵入」の原因は、ID／パスワードの管理不備が 1 件、サーバの設定不備が 1 件、でした。

（4）被害事例

［侵入］

（i）サーバが不正なプログラムを動かされて、外部のコンピュータを攻撃していた。

事例	・外部から、「そちらのサーバから攻撃を受けた」と連絡があった。 ・該当サーバを調べた所、使用していないと思われていた SSH※ポートが開いており、リモート接続が可能な状態になっていた。 ・ログイン ID とパスワードが同じ綴りのアカウントが存在し、このアカウントを使って侵入された。 ・外部のコンピュータを攻撃する、不正なプログラムを動かされていた。
解説・対策	サーバの設定不備と、ログイン ID／パスワードの管理不備が重なった残念な例です。**SSH は、攻撃者がコンピュータを乗っ取る手段としてよく悪用されます。リモート接続を行う必要がない場合は、SSH ポートを閉じてください。** ID／パスワードの管理も、セキュリティ対策の上では大切なことです。**パスワードは推測されにくくすると共に、不要なアカウントは削除してください。** （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

※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。

［なりすまし］

（ii）ウェブサービスのログイン履歴に身に覚えのない海外からのログイン記録があった

事例	・最近、迷惑メールが多く届くようになったので、不審に思い利用中のウェブサービスのログイン履歴を確認したところ、身に覚えのない海外からのログイン成功の記録が残っていた。 ・ウェブメールにアクセスされていたが、何をされたのかは不明。 ・パスワードを盗まれたからだと思うが、盗まれた原因は分からない。
解説・対策	パスワードが盗まれた原因として、ID／パスワードを盗むウイルスの感染被害、ID などから推測された、家族や知人などに教えている、自分が管理していない、または共用で使用しているパソコンからのサービス利用、などが考えられます。また、**同じ ID／パスワードを、今回被害に遭ったウェブサービス以外（例えばブログやショッピングサイトなど）にも使っていた場合、そちらから情報が流出したことにより、今回のウェブサービスに被害が及んだ可能性も考えられます。** 今できる対処として、使用パソコンの初期化をお勧めします。初期化後は、OS やアプリケーションソフトの脆弱性を解消、ウイルス対策ソフトを最新の状態で使用し、被害に遭ったウェブサービスのパスワードはより複雑で、推測されにくいものに変更してください。さらに、同じパスワードを使用しているウェブサービスがあれば、全て異なるパスワードに変更してください。 （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

2 月のウイルス・不正アクセス関連相談総件数は **1,521 件**でした。そのうち**『ワンクリック請求』に関する相談**が **473 件**（1 月：442 件）、**『偽セキュリティソフト』**に関する相談が **9 件**（1 月：17 件）、**Winny に関連する相談**が **6 件**（1 月：3 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**（1 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

		9月	10月	11月	12月	1月	2月
合計		2,102	1,813	1,692	1,536	1,463	1,521
	自動応答システム	1,142	1,065	1,036	954	892	892
	電話	872	675	580	531	499	570
	電子メール	85	69	72	49	64	53
	その他	3	4	4	2	8	6

※ 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。

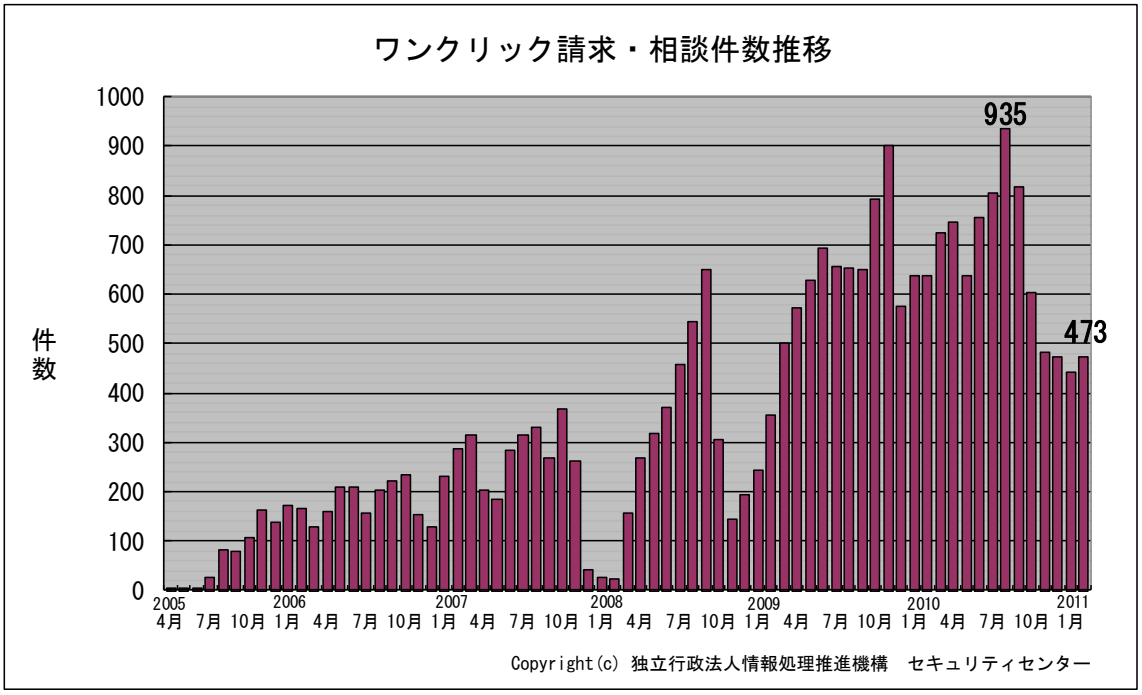

図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）偽セキュリティソフトの警告は本当か

相談	普段からパソコンにセキュリティソフトを入れて使っている。ある時、家族の者がパソコンでどこかのウェブサイトを見た後に、画面に見慣れないセキュリティソフトらしき画面が出現して、スパイウェアに感染しているという警告を出していた。 対処に関しては、もともと入っているセキュリティソフトのメーカーに相談して対応してもらうつもりだが、本当にスパイウェアに感染していないか心配。
回答	ご家族の方が悪意のあるウェブサイトを閲覧した際に、パソコンが「偽セキュリティソフト」型ウイルスに感染したと思われます。対処に関してウイルス対策ソフトのメーカーに相談することは賢明です。 また、この場合の、“スパイウェアに感染しているという警告”は**不安を煽るための手口であり、実際はその画面自体が悪質なウイルス**によって表示されています。 なお、正規のセキュリティソフトを使っていたとしても、今回のようにすり抜けて感染してしまうこともあるので、普段から閲覧するウェブサイトに注意を払うとともに、Windows やアプリケーションなどの脆弱性対策にも十分注意してください。 （ご参考） 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）Internet Explorer のタイトルバーに「Hacked by Godzilla」と出ている

相談	数日前から、Internet Explorer でヤフーのトップページを開くと、タイトルバーの部分に「Yahoo! Japan - Hacked by Godzilla」と出るようになった。 この現象は何が原因なのか。どうしたら元に戻すことができるのか。  ※本画像は相談内容を元に IPA が独自に作成したイメージです
回答	このような現象は W32.VBS.Godzilla というウイルスに感染することで発生します。 このウイルスは **USB メモリなどを介して感染を広げるタイプ**ですので、事象が発生する前に USB メモリなどを使用した際に感染したのではないでしょうか。 お使いのウイルス対策ソフトのウイルス定義ファイルを最新版に更新して駆除を試みてください。駆除できない場合はパソコンを初期化することをお勧めします。 （ご参考） W32.VBS.Godzilla （スパイウェアガイド） http://www.shareedge.com/spywareguide/product_show.php?id=3562

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、2011 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 **143,494 件**、延べ発信元数※は **41,803 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 182 の発信元から 624 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。

※2 月 4 日～8 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、2 月の観測データは、この 5 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。

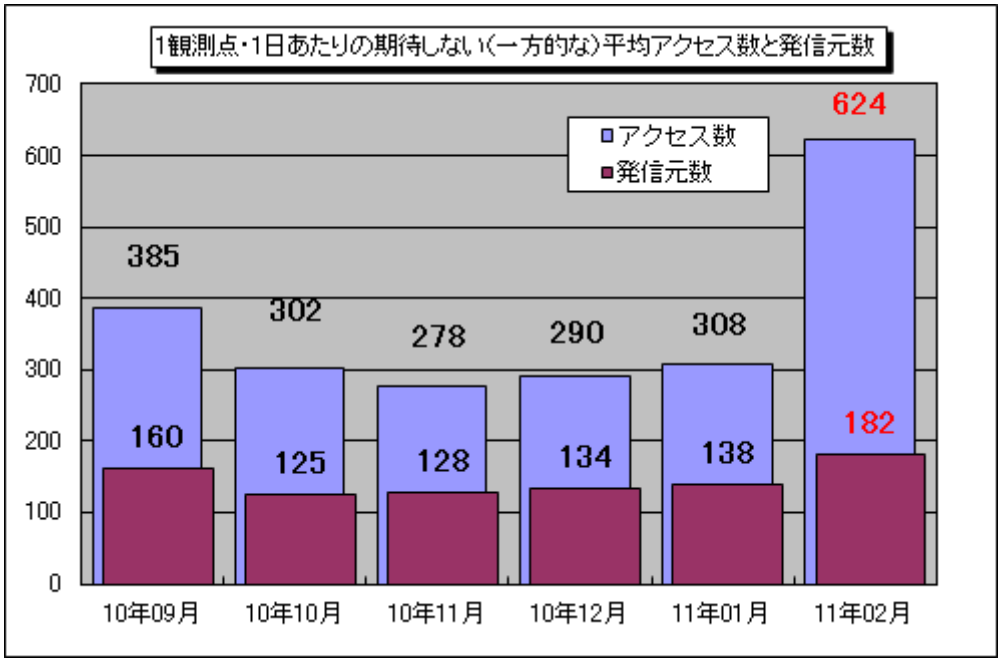

図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数

2010 年 9 月～2011 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 月と 2 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。1 月に比べ、比較的増加が観測されたのは 80/tcp、17500/udp、443/tcp、25/tcp へのアクセスでした。

17500/udp については、2010 年 9 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（図 5-3 参照）。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。

また、2 月は 80/tcp、443/tcp、25/tcp の増加が観測されていますが、これは 2 月 21 日以降にミャンマーの IP アドレスからのアクセスが TALOT2 の複数の観測点で増加したためです。上記のポートの他、

21/tcp、22/tcp でも同様の IP アドレスからのアクセスの増加が観測されています（図 5-4 参照）。定点観測を行っている他の組織の中にも類似した傾向を観測しているところもあり、原因に関しては現在調査中ですが、何らかの攻撃が行われている可能性もありえるので、引き続きこれらのポートへのアクセスに注意していきます。

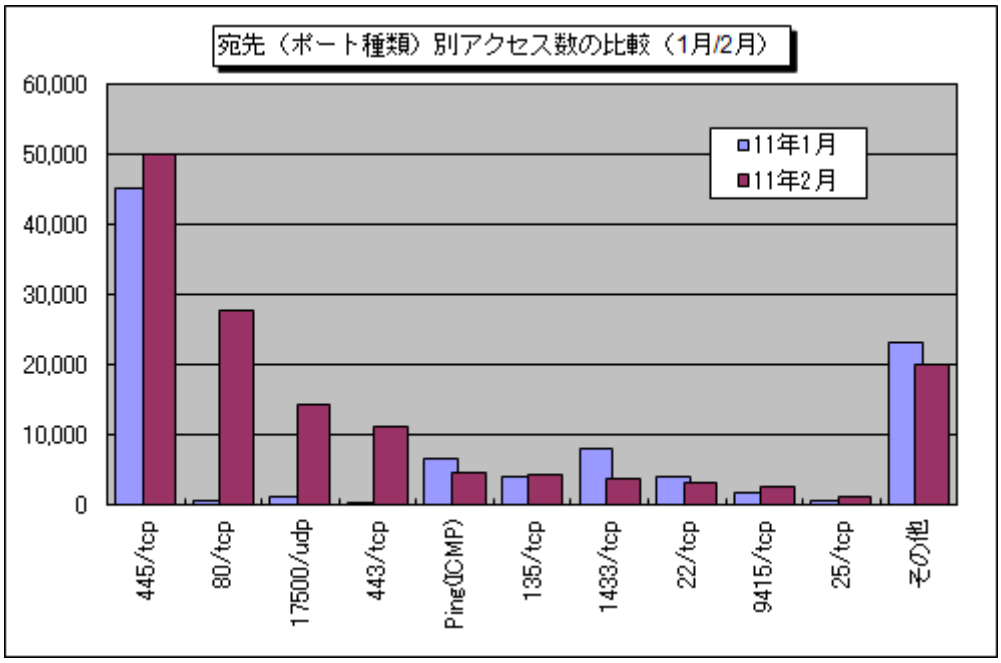

図 5-2：宛先（ポート種類）別アクセス数の比較（1 月/2 月）

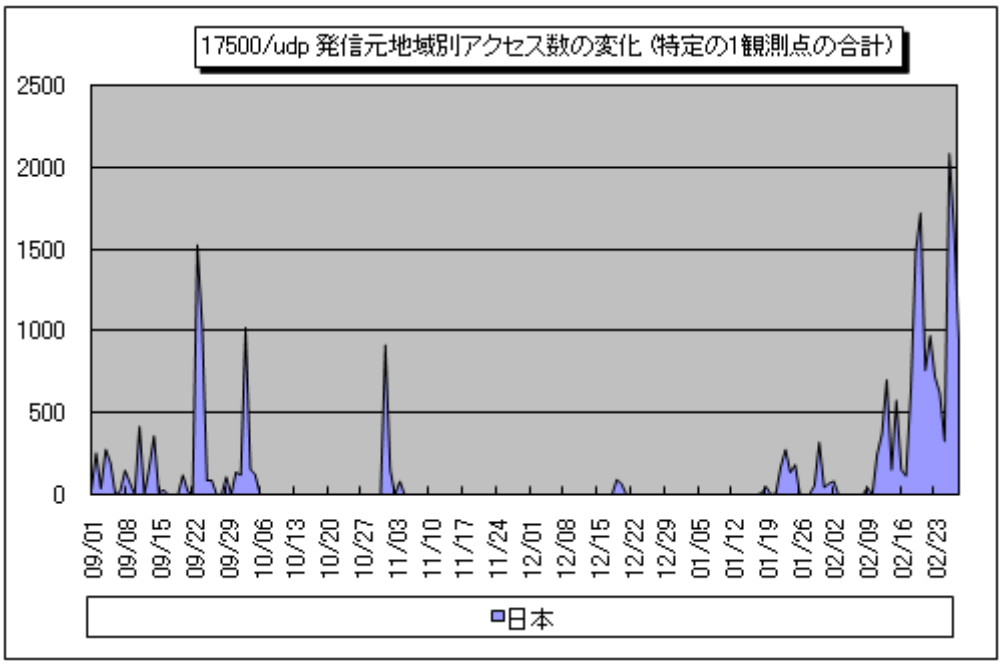

図 5-3：17500/udp 発信元地域別アクセス数の変化（特定の 1 観測点の合計）

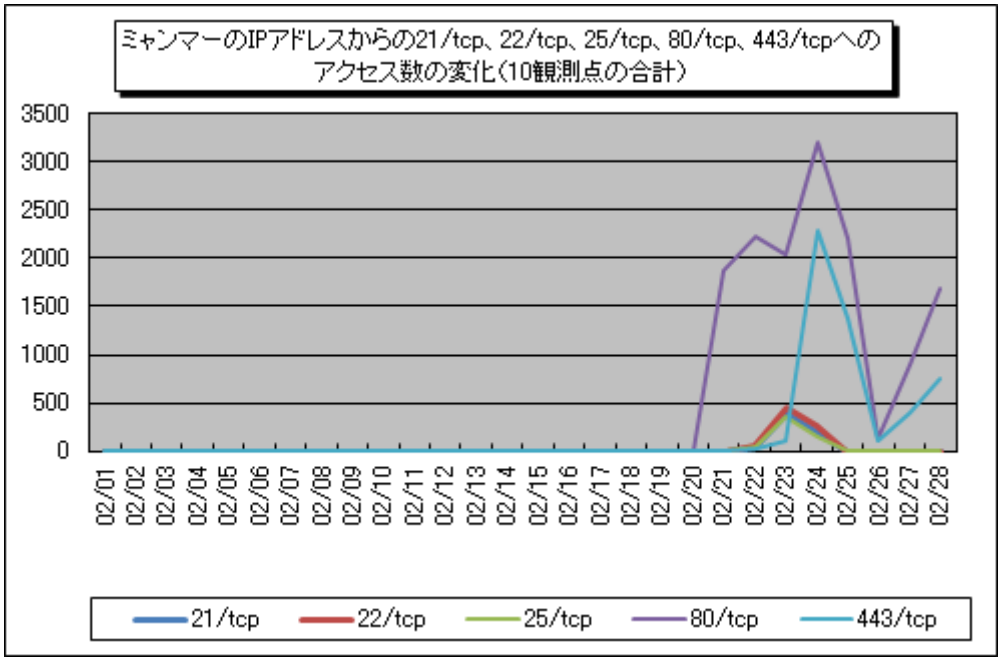

図 5-4：ミャンマーの IP アドレスからの 21/tcp、22/tcp、25/tcp、80/tcp、443/tcp へのアクセス数の変化

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/TALOT2-1103.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