Information-technology Promotion Agency, Japan

プレスリリース
第 11-12-213 号
2011 年 4 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［2011 年 3 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 3 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

「 無線 LAN を他人に使われないようにしましょう！ 」

近年、一般家庭の無防備な無線 LAN 環境が悪用されるといった事件が複数報道されています。セキュリティ設定が不十分な無線 LAN 環境は、悪意ある者に使われてしまう危険性があります。実際に、一般家庭の無防備な無線 LAN 環境などを含む様々な犯罪インフラ※が、国内の組織犯罪、詐欺、窃盗、サイバー犯罪等のあらゆる犯罪の分野で着々と構築され、巧妙に張り巡らされてきているという現状があります。警察庁は、2011 年 3 月 10 日に、犯罪インフラへの対策の指針となる「犯罪インフラ対策プラン」を策定するなど、取り締まりを強化する方針を打ち出しました。

自宅の無線 LAN が犯罪インフラとして悪用されないよう、セキュリティ設定を適切に行ってください。

※ 犯罪インフラとは犯罪を助長し、又は容易にする基盤のこと。基盤そのものは合法であっても、犯罪に悪用されている状態にあれば、犯罪インフラとなる。

（ご参考）
犯罪インフラ対策プラン（警察庁）
http://www.npa.go.jp/sosikihanzai/kikakubunseki/bunseki/taisakuplan.pdf

（1）無線 LAN を取り巻く問題の概要

無線 LAN は、電波を使って無線 LAN アクセスポイント（以下、「親機」）と無線 LAN 機能を持つパソコン、スマートフォン、一部のゲーム機など（以下、「子機」）との間で通信を行うネットワーク環境のことです。無線 LAN では親機と子機の双方に通信のための設定をすることで、電波の届く範囲であれば、壁などの障害物を越えて通信が可能となります。

無線 LAN は便利であると同時に、家庭内ネットワークへの侵入や、インターネットでの不正行為のいわゆる「踏み台」など、悪用の対象として狙われやすいものです。電波という目に見えない通信経路を使うということは、侵入されていることさえも気付きにくいため、注意が必要です（図 1-1 参照）。

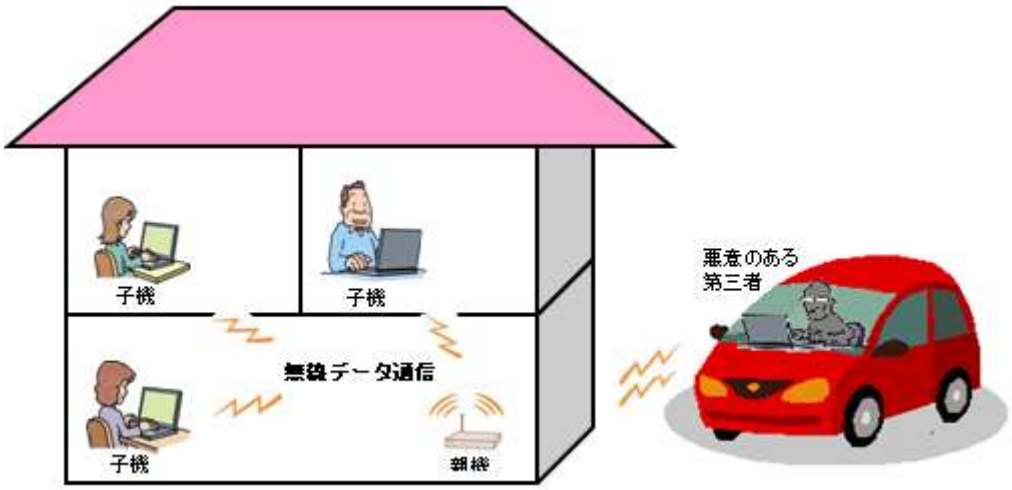

図 1-1：無線 LAN を取り巻く脅威のイメージ

（2）無線 LAN が関係した事件の実例

無線 LAN が関係した事件の実例を、表 1-1 に示します。

表 1-1：無線 LAN が関係した事件の実例

時期	内容
2008 年 6 月	インターネットに接続できる携帯ゲーム機を使用して他人の家の無線 LAN に無断で接続し、インターネットの掲示板に無差別殺人をほのめかす書き込みをしたとして、男が逮捕された。
2008 年 10 月	インターネットオークションで、児童ポルノの DVD を販売したとして逮捕された男が、他人の家の無線 LAN に無断で接続し、児童ポルノのファイルを入手していた。
2010 年 2 月	他人の家の無線 LAN に無断で接続し、あらかじめ不正に入手していた他人のクレジットカード情報を使用してインターネットで買い物をしたとして、詐欺グループのメンバー2 人が逮捕された。
2010 年 6 月	インターネットの掲示板に銀行口座を販売するなどと書き込み、現金を騙し取ったとして逮捕された男が、身元が特定できないように他人の家の無線 LAN から無断でインターネットに接続していた。

これらの実例はいずれも、無線 LAN のセキュリティ設定が不十分だったために、自宅の無線 LAN 環境を無断で使用されて、「踏み台」として悪用されてしまったケースです。これ以外にも想定される被害として、以下のようなことが考えられます。

・無線 LAN 環境に侵入され、重要な情報を盗まれる。
・通信データを盗聴される。

（3）対策

上記のような被害に遭わないためには、無線 LAN におけるセキュリティ設定が重要となりますが、そのポイントは「適切な暗号化方式の選択」と「適切なパスワードの設定」の 2 点になります。

（i）適切な暗号化方式の選択

無線 LAN の暗号化方式には大きく分けて、「**WEP**」、「**WPA**」、「**WPA2**」の 3 種類があり、最も安全な暗号化方式はこの中で最新の「WPA2」です。

「WPA2」の中にもいくつか種類がありますので、実際に暗号化方式を選択する場合、WPA2-PSK（Pre-Shared Key）という認証方式を利用したもののうち、最もセキュリティ強度が高い「**WPA2-PSK（AES）**」を選択してください。

これが選択できない場合は次善策として「WPA」の中から、WPA-PSK（Pre-Shared Key）という認証方式を利用したもののうち、最もセキュリティ強度が高い「**WPA-PSK（AES）**」を選択してください。

それ以外の暗号化方式ではセキュリティ強度が十分でないため、選択しないでください。なお、暗号化方式の詳しい説明については、以下のウェブページに記載しています。

（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

参考として、図 1-2 に親機の設定画面例を、図 1-3 に設定状態の確認画面例を示します。無線 LAN の利用者は、念のため自宅の無線 LAN の設定を確認してください。なお、画面や確認方法、設定方法は機種によって異なります。操作等については、親機の取扱説明書を参照してください。

図 1-2：親機の設定画面例

図 1-3：親機の設定状態の確認画面例

なお、**親機と全ての子機が、選択したい暗号化方式に対応していなければなりません。**つまり、親機を「WPA2-PSK（AES）」に設定した場合は、その親機に接続されている全ての子機を「WPA2-PSK（AES）」に設定する必要があります。

（ii）適切なパスワードの設定

上記の暗号化方式で使用する暗号鍵を生成するために、パスワードの設定が必要となります。パスワードを設定する際は、容易に推測されることを防ぐため、以下の注意事項に従ってください。

- 英語の**辞書に載っている単語を使用しない**
- **大文字、小文字、数字、記号の全てを含む**文字列とする
- 文字数は**最低でも 20 文字**（半角英数字＋記号の場合。最大で 63 文字）とする

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）

・テレビ会議システムが乗っ取られ、外部のコンピュータを攻撃する踏み台となっていた

・メールアカウントに不正にログインされ、迷惑メール送信の踏み台として使われた

○ 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）

・ワンクリック請求で業者に個人情報を送ってしまった

・知人のメールアドレスから届いたメールが怪しい

○ 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

3 月のウイルスの検出数※1 は、**約 2.4 万個**と、2 月の約 2.2 万個から 10.6%の増加となりました。また、3 月の届出件数※2 は、**985 件**となり、2 月の 974 件から同水準での推移となりました。

※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。
・3 月は、寄せられたウイルス検出数約 2.4 万個を集約した結果、985 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 5.8 千個**、3 位は **W32/Autorun** で**約 1.4 千個**でした。

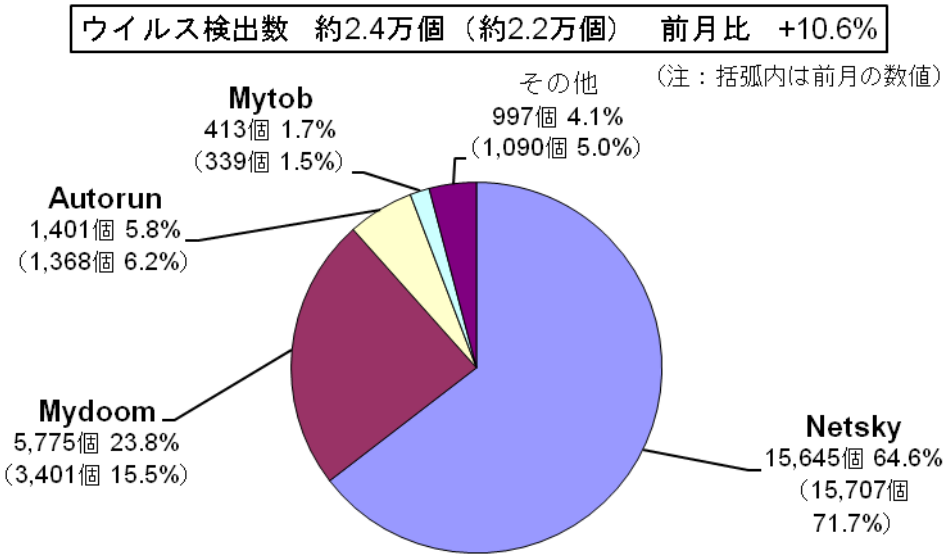

図 2-1：ウイルス検出数

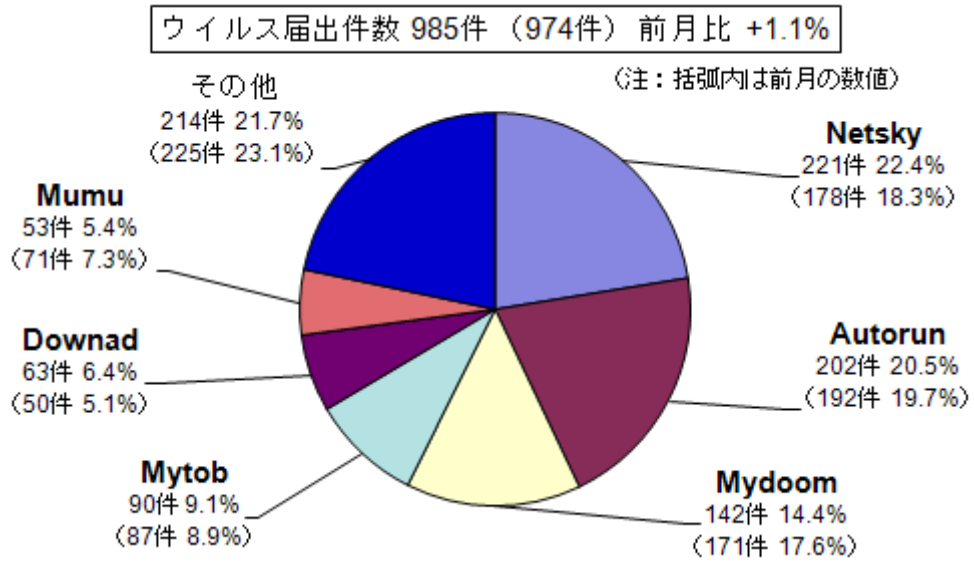

図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

2011 年 3 月の後半に、偽セキュリティソフトの検知名である FAKEAV や、パソコン内に裏口を仕掛ける BACKDOOR といった不正プログラムの増加が確認されました。

このような不正プログラムは、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、添付ファイルの取り扱いには十分注意する必要があります。

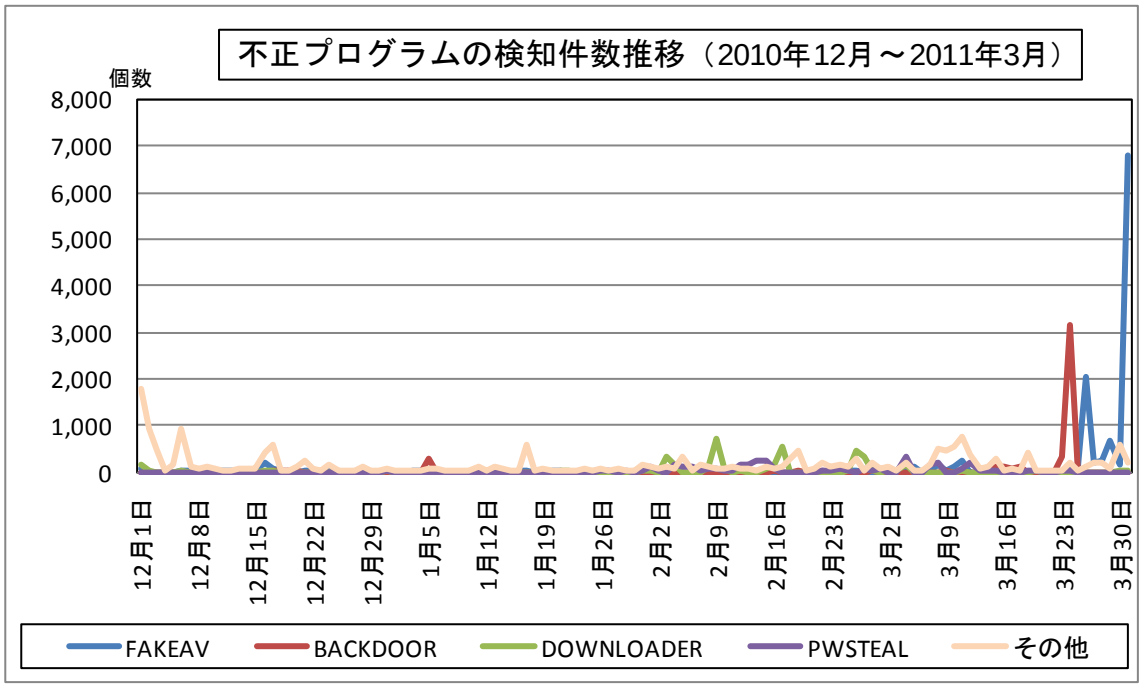

図 2-3：不正プログラムの検知件数推移

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

		10月	11月	12月	1月	2月	3月
届出(a) 計		14	14	22	12	10	6
	被害あり(b)	8	7	7	6	5	6
	被害なし(c)	6	7	15	6	5	0
相談(d) 計		40	45	27	41	23	45
	被害あり(e)	15	12	7	11	6	10
	被害なし(f)	25	33	20	30	17	35
合計(a+d)		54	59	49	53	33	51
	被害あり(b+e)	23	19	14	17	11	16
	被害なし(c+f)	31	40	35	36	22	35

（1）不正アクセス届出状況

3 月の届出件数は 6 件であり、それら全てが被害のあったものでした。

（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 10 件でした。

（3）被害状況

被害届出の内訳は、**侵入 1 件、なりすまし 5 件、**でした。

「侵入」の被害は、テレビ会議システムに、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、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（メールサーバ 2 件、オンラインゲーム 1 件、ショッピングサービス 1 件、IP 電話サービス 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、OS 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）テレビ会議システムが乗っ取られ、外部のコンピュータを攻撃する踏み台となっていた

事例	・組織内ネットワークから、外部のサーバに向けて侵入を試みるアクセスを検知。 ・調査したところ、組織内に設置してあったシスコ社製テレビ会議システムが、外部サーバに侵入するための踏み台として悪用されていたことが判明。 ・シスコ社製テレビ会議システムのファームウェア（OS）の脆弱性を突かれ、SSH※を介して管理者権限で侵入され、システムが乗っ取られていた。
解説・対策	**パソコンやサーバ以外でも、ネットワークに接続された機器の場合は、脆弱性を狙われて攻撃されるという脅威は存在します**。攻撃が成功した場合は、パソコンやサーバと同様に、外部サイトなどを攻撃する踏み台として悪用されてしまいます。テレビ会議システムのような組込機器でも、**製造元などからアップデートに関する情報を収集し、適切な対処を実施してください**。 （参考） JVN iPedia（脆弱性対策情報データベース） http://jvndb.jvn.jp/

※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）メールアカウントに不正にログインされ、迷惑メール送信の踏み台として使われた

事例	・自組織で運用しているメールサーバのログが急速に肥大化していた。その後、外部組織より、「そちらからと思われる迷惑メールが大量に届く」との報告が届いた。 ・調査したところ、メールアカウントの１つに外部から不正にログインされ、迷惑メール送信の踏み台として使われていたことが判明。 ・短時間に大量のメールを発信していたために、送信先メールサーバから受信を拒否された。それが原因でエラーメールが自組織のメールサーバに大量に届いたため、ハードディスクの空き領域を圧迫し、結果的にサーバが機能停止した。 ・詳しい原因は不明だったため、全アカウントを一旦削除し、全て新たに作成し直した。
解説・対策	原因は不明ですが、メールアカウントのパスワードが弱かったことが原因の一つとして考えられます。今後の対策としては、**パスワードを強化するのはもちろんですが、組織外からメールの送受信を許可すべきか、認証を多重化すべきか、などの検討も必要**になってきます。組織外からのメール送受信を許可する場合でも、メールサーバの監視を強化するなどして、何か問題が発生した場合に即対応できるようにしておきましょう。 （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

3 月のウイルス・不正アクセス関連相談総件数は **1,723 件**でした。そのうち**『ワンクリック請求』に関する相談**が **466 件**（2 月：473 件）、**『偽セキュリティソフト』**に関する相談が **7 件**（2 月：9 件）、**Winny に関連する相談**が **22 件**（2 月：6 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 **2 件**（2 月：0 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

		10月	11月	12月	1月	2月	3月
合計		1,813	1,692	1,536	1,463	1,521	1,723
	自動応答システム	1,065	1,036	954	892	892	1,106
	電話	675	580	531	499	570	551
	電子メール	69	72	49	64	53	58
	その他	4	4	2	8	6	8

※ 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。

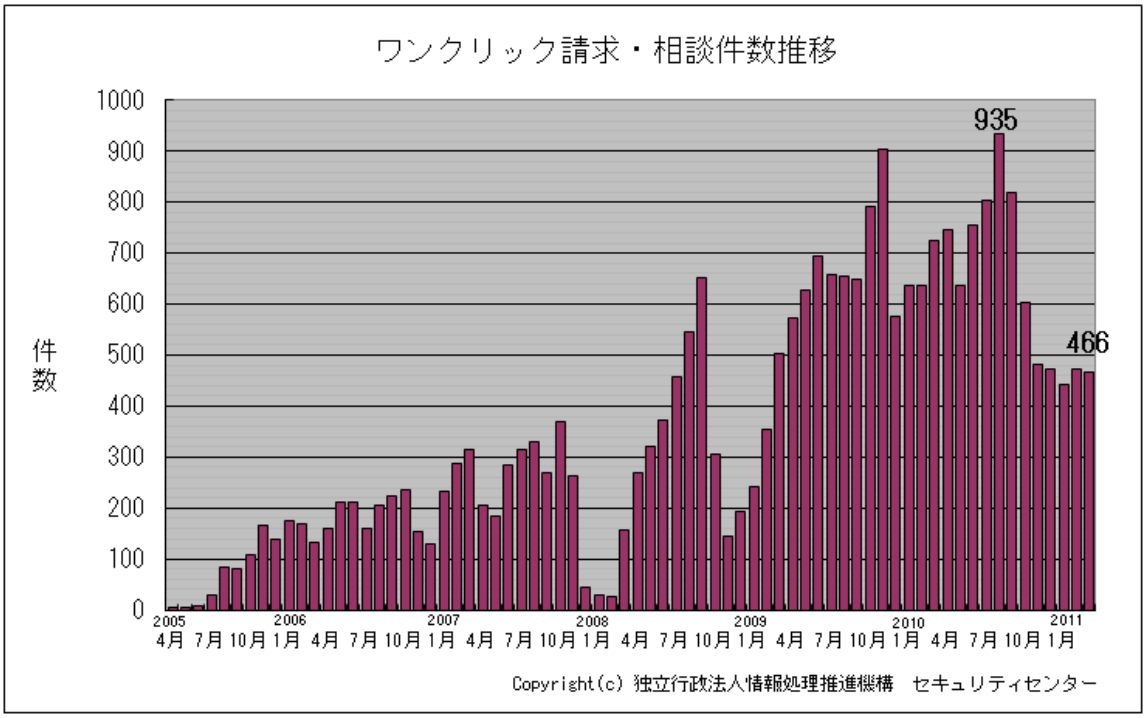

図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）ワンクリック請求で業者に個人情報を送ってしまった

	未成年の子供がアダルトサイトを閲覧していて、請求画面が出るようになり、慌てて業者に電話で連絡をとった。子供の名前と生年月日を証明するものを見せてくれれば画面を消すといわれたので、子供の保険証を写真にとってメールで送ったら、画面を消してくれた。この対応でよかったのか。
回答	相手のことをよく知らずに、保険証の写しといった重要な情報を送ることは危険です。この場合、クリックした人が未成年であったかどうかに関わらず、この契約が成立しているか否かを含め、**まず消費生活センター等へ相談する**といった対応が望ましかったと言えます。 （ご参考） 全国の消費生活センター http://www.kokusen.go.jp/map/ IPA-【注意喚起】ワンクリック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）知人のメールアドレスから届いたメールが怪しい

相談	知人のメールアドレスから届いたメールが見るからに怪しい。件名がなく、本文には怪しい URL の表記があるのみ。この URL をクリックするとどうなるのか。これは本当に知人が送ったメールなのか。
回答	当該 URL を調べた結果、**そのウェブサイトには、閲覧するだけでパソコンがウイルスに感染してしまう仕掛けが施されていました。** 知人のメールアドレスからこのようなメールが届いた原因としては、メールアドレスが詐称されていたか、もしくは知人のパソコンがウイルスに感染し、ウイルスによって今回のようなメールが送られた、ということが考えられます。 少しでも怪しいと思ったら、メールに書かれた URL は**開かずに、疑ってかかる**ことを心がけましょう。 （ご参考） 「心当たりのないメールは、興味本位で開かずにすぐ捨てよう！」 http://www.ipa.go.jp/security/txt/2008/09outline.html

5. インターネット定点観測での 3 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 3 月の期待しない（一方的な）アクセスの総数は 10 観測点で **246,123 件**、延べ発信元数※は **83,923 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 271 の発信元から 794 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。

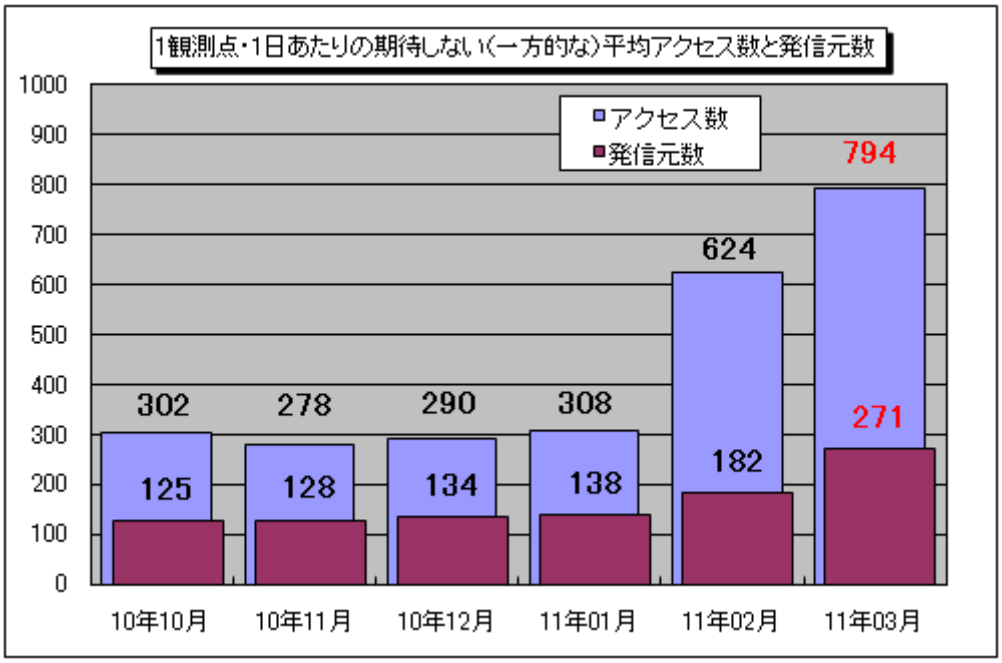

図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数

2010 年 10 月～2011 年 3 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。3 月の期待しない（一方的な）アクセスは、2 月と比べて大幅に増加しました。

2 月と 3 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。2 月に比べ、特に増加が観測されたのは 445/tcp、17500/udp、16753/udp へのアクセスでした。

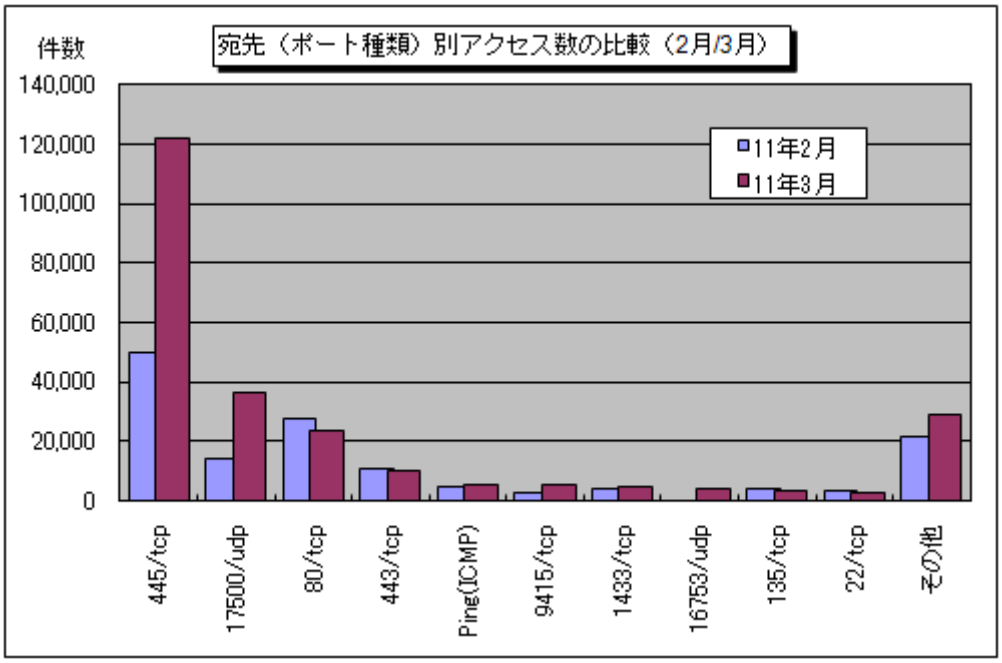

図 5-2：宛先（ポート種類）別アクセス数の比較（2 月/3 月）

445/tcp は、Windows の脆弱性を狙った攻撃を行う際に狙われる可能性が高いポートで、先月に引き続き増加していました。これは主に、アメリカとトップ 10 以外の国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） 。

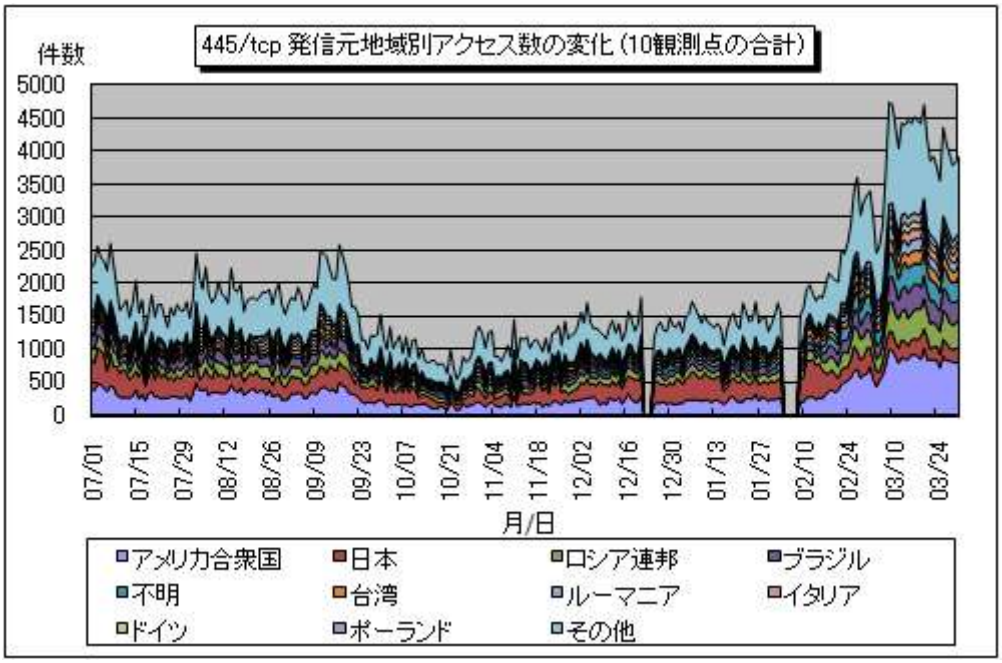

図 5-3：445/tcp 発信元地域別アクセス数の変化（10 観測点の合計）

17500/udp については、先月と同様に 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。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。

16753/udp については、3 月後半に、TALOT2 の特定の 1 観測点に対して複数の IP アドレスから送

られていたという特徴がありました（図 5-4 参照）。こ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。

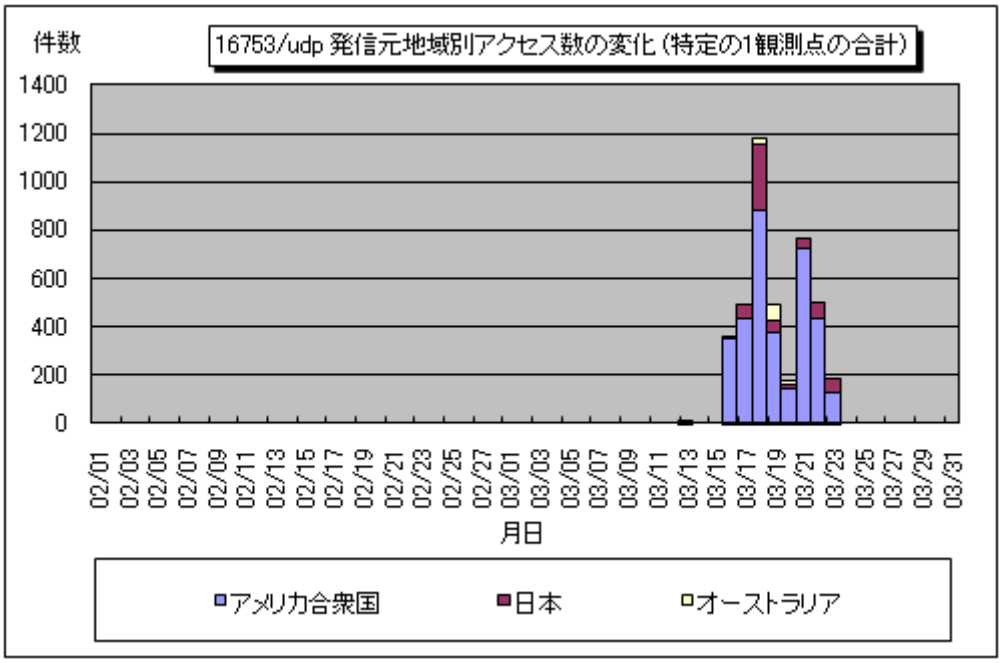

図 5-4：16753/udp 発信元地域別アクセス数の変化（特定の 1 観測点の合計）

また、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ことを 2 月に報告しましたが、80/tcp、443/tcp、25/tcp、21/tcp、22/tcp、1/tcp のポートへのミャンマーの IP アドレスからのアクセスが 3 月も観測されています（図 5-5 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、何らかの攻撃が行われている可能性もありますので、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。

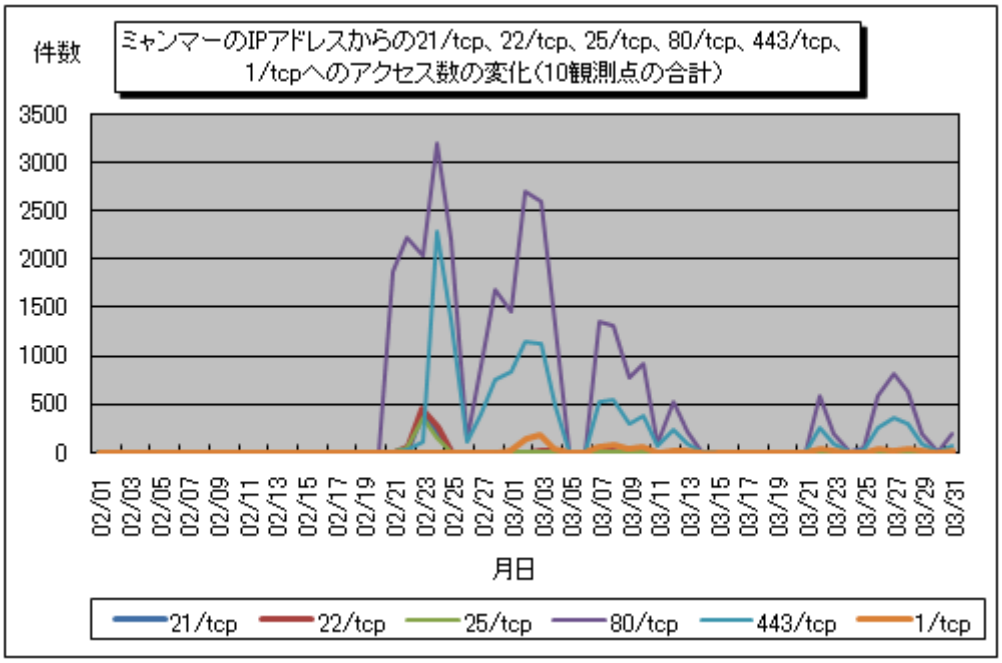

図 5-5：ミャンマーの IP アドレスからの 21/tcp、22/tcp、25/tcp、80/tcp、443/tcp、1/tcp へのアクセス数の変化（10 観測点の合計）

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/TALOT2-1104.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／木邑
Tel:03-5978-7591　Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp