

コンピュータウイルス・不正アクセスの届出状況 [2011 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：藤江 一正）は、2011 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

「災害情報に便乗した罠（わな）に注意！」

東日本大震災により被災された皆さまに対し、心よりお見舞い申し上げます。

こうした災害に便乗し、被災者や被災地の復興支援者、災害情報に敏感になっている方々を騙（だま）そうとしたり、ウイルス感染させたりすることを目的とした罠メールが確認されています。パソコンの利用者は、こうした被害に遭わないためにもどのような手口の罠メールが存在するのかを理解し、少しでも不自然さを感じるメールはすぐに捨てるなど、慎重に対応するようにしてください。

（ご参考）

東北地方太平洋沖地震に便乗した悪さ（IPA 情報セキュリティブログ）

<http://plaza.rakuten.co.jp/ipablog/diary/201103250000/>

(1) 罠メールの手口の概要

今回確認された罠メールの手口は、次の 3 つに分類されます。

表 1-1：罠メールの手口の分類と詳細

分類	詳細
デマ（混乱）	<p>●チェーンメール</p> <p>これは、メールを「出来るだけ多くの人へ連鎖的に送る」ことを目的としており、内容に関係なく迷惑メール行為に当たります。内容によっては、受信者の不安感をいたずらに煽ることになり、その不安が連鎖的に広がることで風評被害を引き起こす原因にもなります。今回は、原発・放射線関連情報や節電の呼びかけ、寄付・募金や救援物資に関するメールが確認されています。</p> <p>（ご参考）</p> <p>東日本大震災 関連メール情報（迷惑メール相談センター）</p> <p>http://www.dekyo.or.jp/soudan/eq/</p>
詐欺	<p>●義援金詐欺メール</p> <p>これは、メール内に書かれているリンクをクリックさせて、被災者への義援金を騙し取る目的のウェブサイトへ誘導する、いわゆるフィッシング詐欺の手口です。</p> <p>（ご参考）</p> <p>義援金詐欺等の悪質なメールにご注意ください！（総務省）</p> <p>http://www.soumu.go.jp/menu_kyotsuu/important/42233.html</p>

ウイルス感染	<p>●ウイルス感染を目的としたメール（ウイルスメール）</p> <p>災害情報に見せかけた、ウイルスメールが確認されています。一見信頼できる情報のように見せかけるために、メール表題や添付ファイル名、本文がもっともらしい日本語になっていることがほとんどです。このメールの受信者は、このメールが信頼できるものと思込み、添付ファイルを開くと、パソコンがウイルスに感染してしまいます。</p> <p>以下に、IPA で確認しているウイルスメールの表題例を示します。</p> <ul style="list-style-type: none"> ➤ 被災者の皆様、とくにお子さんをお持ちの被災者の皆様へ ➤ 被ばくに対する防護対策について ➤ 全国へ計画停電のお知らせについて ➤ 福島原発最新状況 <p>次に、IPA で確認しているウイルスメールの添付ファイル名の例を示します。</p> <ul style="list-style-type: none"> ➤ 放射線被ばくに関する基礎知識 第1報.doc、第2報.doc ➤ mSv（ミリシーベルト）で示した図解.doc ➤ 放射能が関東の人間に与える影響.doc ➤ 福島原発.doc ➤ 3月30日放射線量の状況.doc 避難場所一覧表.xls ➤ 安定ヨウ素剤の服用量及び服用方法 <p>（ご参考）</p> <p>IPA－災害情報を装った日本語のウイルスメールについて http://www.ipa.go.jp/security/topics/alert20110404.html</p>
--------	---

上述した手口の中でも、ウイルスメールには特に注意しなければなりません。次項では、今回実際にIPAで確認した罠メールについて説明します。

(2) ウイルスメールの詳細

(i) メール本文

メールが信頼できるものだと信じ込ませるための細工が、メール本文に施されています。図 1-1、図 1-2 は、今回確認されたウイルスメールの本文例です。

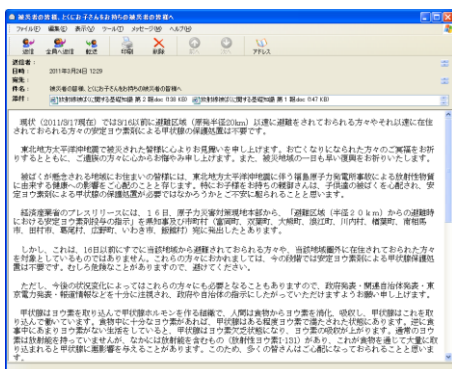


図 1-1：メール本文例 1

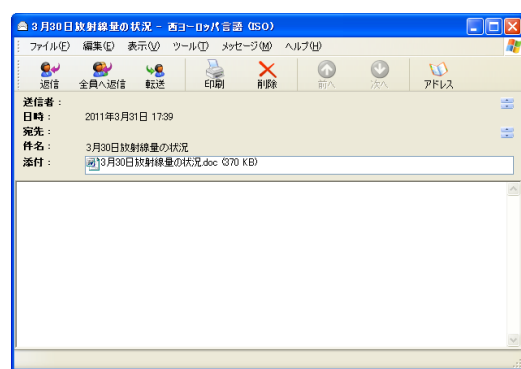


図 1-2：メール本文例 2

図 1-1 のメール本文には、このメールの送信者として詐称された組織の文書が、そっくりそのまま引用されています。こうすることで、当該組織からの本物のメールと思込ませて添付ファイルを開かせます。

図 1-2 のメール本文には何も書かれていません。しかし、何も書かれていないことで添付ファイルの内容を確認したくなる心理を突いていると考えられます。

(ii) 添付されているウイルス

ウイルスメールの添付ファイルを調べた結果、添付されていたウイルスは Mdropper と呼ばれるものでした。このウイルスは、日本マイクロソフト社のアプリケーションソフトである Word や Excel のドキュメントファイル内に、それらソフトの脆弱性（ぜいじゃくせい）を悪用する命令が仕込まれたものです。すなわち、ウイルスファイルのアイコンや拡張子は、Word や Excel そのものであるため、見た目ではウイルスかどうかの判断ができません（図 1-3 参照）。Mdropper は、さらに別のウイルスを呼び込む悪さをしますが、呼び込まれる別のウイルスが何なのかは感染時期によって異なり、どのような症状が出るかは一概には言えません。

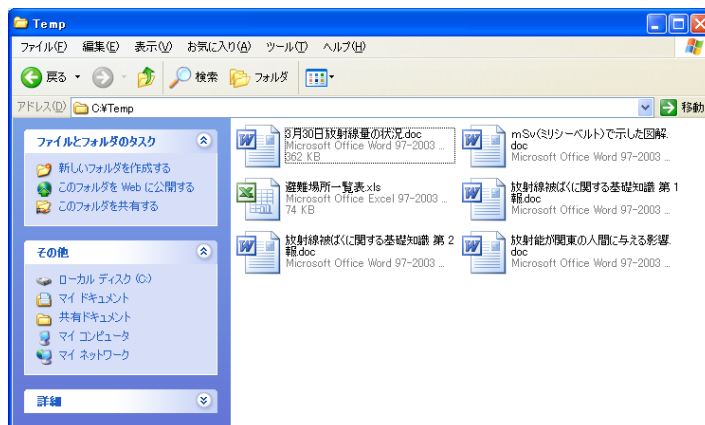


図 1-3：ウイルスメールの添付ファイル

悪用される脆弱性は次の 2 つです。

- Microsoft Office Word の脆弱性（MS10-087：CVE-2010-3333）
<http://www.microsoft.com/japan/technet/security/bulletin/ms10-087.msp>
- Microsoft Office Excel の脆弱性（MS09-067：CVE-2009-3129）
<http://www.microsoft.com/japan/technet/security/bulletin/ms09-067.msp>

(3) 対策

(i) 簡単にメールは開かない・クリックしない

普段やり取りがない送信者からのメールが届いたら、すぐに開いたり、中に書いてあるリンクをクリックしたりしないでください。可能であれば送信者と連絡を取り、本当にその送信者が送ったメールなのかを確認してください。ただし、確認をする際は、メールの中に書かれている連絡先には連絡をせず、出来る限り自分で連絡先を調べて電話で確認することを勧めます。

添付ファイルがあるメールであれば、普段やり取りのある送信者からのメールでも用心し、少しでも不自然だと思ふメールであれば、相手に確認を取るか、開かずに削除することが最善策です。

(ii) 脆弱性の解消

使用しているパソコンの、OS（オペレーティングシステム）やパソコンに導入しているアプリケーションソフトについては、できる限り最新版に更新し、脆弱性を解消してください。

（ご参考）

「Microsoft Update 利用の手順」（日本マイクロソフト社）

http://www.microsoft.com/japan/security/bulletins/j_musteps.msp

「JVN iPedia 脆弱性対策情報データベース」（JVN）

<http://jvndb.jvn.jp/>

IPA では、ウイルスによって狙われることが多いアプリケーションソフトについて、それらがパソコンに導入されているか、および最新版となっているか否かをチェックできるツールを公開しています。詳しくは、下記の「MyJVN バージョンチェッカ」のウェブページを参照してください。

（ご参考）

「MyJVN バージョンチェッカ」（JVN）

(iii) ウイルス対策ソフトによる防御

ウイルス対策ソフトは万能ではありませんが、重要な対策の一つです。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つことで、ウイルスの侵入阻止や、侵入したウイルスの駆除ができます。近年のウイルスは、パソコンの画面の見ただけでは感染していることが分からないものが多いため、ウイルスの発見と駆除には、ウイルス対策ソフトが必須です。

一般利用者向けのウイルス対策ソフトとしては、ウイルスの発見と駆除だけでなく、罠メールに書かれたリンクから危険なウェブサイトへ誘導された際にブロックを行う機能などを備える、「統合型」と呼ばれるものを推奨します。

(iv) 復旧のための対策

パソコンの画面の見ただけでは感染していることが分からないが、怪しい添付ファイルを開いてしまったなどでパソコンの動作がおかしいと感じた場合は、お使いのウイルス対策ソフトで、ウイルス定義ファイルを最新の状態にしてからパソコン内のウイルスチェックを行ってください。

ウイルスを駆除できたとしても、パソコンが正常に動作していないと思われるのであれば、「システムの復元」を実施してください。これは、Windows XP、Vista、7に搭載されている機能で、パソコンの情報を過去の状態に戻すことができます。なお、「システムの復元」を実施しても選択した日付から現在までに作成した文書や送受信したメール情報およびホームページへのアクセス履歴やお気に入りが消えることはありません。以下のマイクロソフトのサイトを参考にして、「システムの復元」を行ってください。

(ご参考)

「Windows XP 機能別紹介：システムの復元」(Windows XP) (日本マイクロソフト社)

<http://www.microsoft.com/japan/windowsxp/pro/business/feature/performance/restore.msp>

「システムの復元とは」(Windows Vista) (日本マイクロソフト社)

<http://windows.microsoft.com/ja-JP/windows-vista/What-is-System-Restore>

「Windows 7 の機能：システムの復元」(Windows 7) (日本マイクロソフト社)

<http://windows.microsoft.com/ja-JP/windows7/products/features/system-restore>

なお、下記のウェブページにて、Windows を「セーフモード」で起動し、「システムの復元」を実施するための具体的な手順を案内しています。

(ご参考)

IPA「Windows での「システムの復元」の実施手順」

<http://www.ipa.go.jp/security/restore/>

システムの復元が正常に完了しない場合は、パソコンを購入した時の状態に戻す作業（初期化）を行ってください。

実際の作業方法は、パソコンに付属の取扱説明書に記載されている「購入時の状態に戻す」などの手順に沿って作業してください。なお、作業を行う前には、重要なデータのバックアップを忘れずに行ってください。また、バックアップしたデータは、パソコンに戻す前にウイルス対策ソフトでウイルスチェックし、ウイルスが含まれていないことを確認してください。

(ご参考)

IPA「パソコンユーザのためのウイルス対策 7 箇条

<http://www.ipa.go.jp/security/antivirus/7kajonew.html>

IPA「パソコンユーザのためのスパイウェア対策 5 箇条

<http://www.ipa.go.jp/security/antivirus/spyware5kajyou.html>

(4) 復旧・復興の支援活動をされている皆さまへ

今回の災害において復旧・復興支援活動をされている皆さまへのお願いです。

支援物資として送られる中古のパソコンは、最近では稼働していなかったものが多いと思われます。そのようなパソコンは、最近までの脆弱性が解消されていないため、ウェブページ閲覧やメールをする際にウイルス感染の被害に遭う可能性が高まります。被災地で稼働させる前に、OS やアプリケーションソフトを最新の状態に更新してください。

なお、Windows 98/Windows Me/Windows 2000 といった OS は日本マイクロソフト社によるサポートが既に終了しているため、脆弱性の解消を行うことができません。よって、インターネットに接続するだけで脆弱性を突かれてウイルス感染するなど、非常に危険な状態に陥る可能性が高くなります。これらの OS が入っているパソコンを被災地に送ることは、控えてください。

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、8 頁の「3.コンピュータ不正アクセス届出状況」を参照）
 - ・ サーバの設定不備を突かれて侵入され、ファイルを置かれた
 - ・ 古いメールアカウントを不正使用され、自ドメインから大量のメールを送信された
- 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）
 - ・ 企業のウェブサイトが改ざんされた場合の対処方法と、開示すべき情報を知りたい
 - ・ ウェブメールの管理事務局から怪しいメールが届いた
- 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

4月のウイルスの検出数※1は、約2.6万個と、3月の約2.4万個から6.9%の増加となりました。また、4月の届出件数※2は、1,138件となり、3月の985件から15.5%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を。

・4月は、寄せられたウイルス検出数約2.6万個を集約した結果、1,138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5.7千個、3位はW32/Autorunで約1.1千個でした。

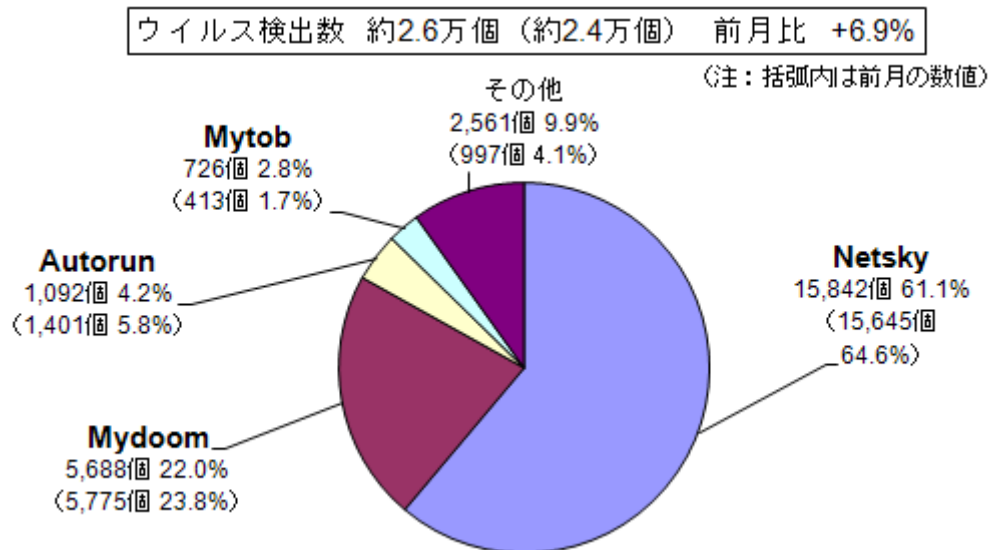


図 2-1：ウイルス検出数

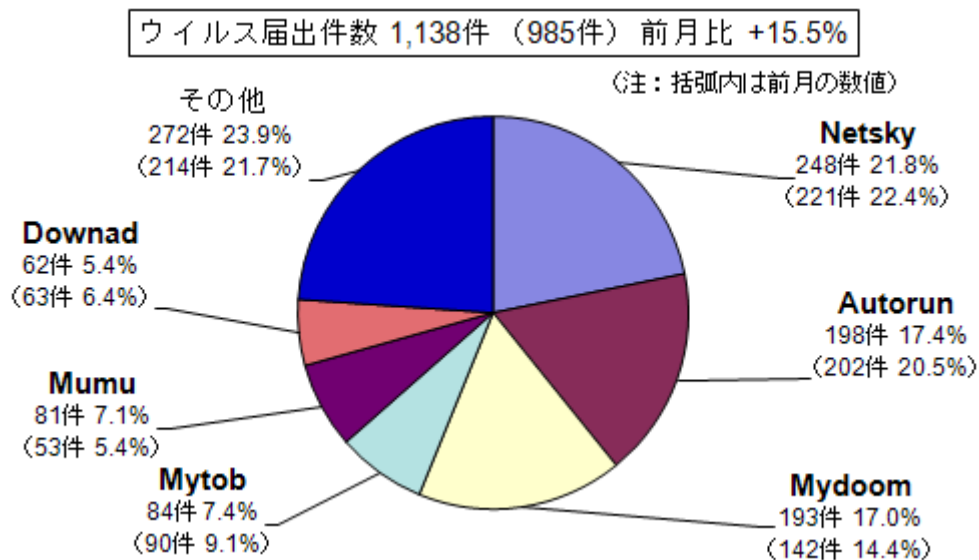


図 2-2：ウイルス届出件数

(2) 不正プログラムの検知状況

4月は、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は減少傾向となりました（図2-3参照）。

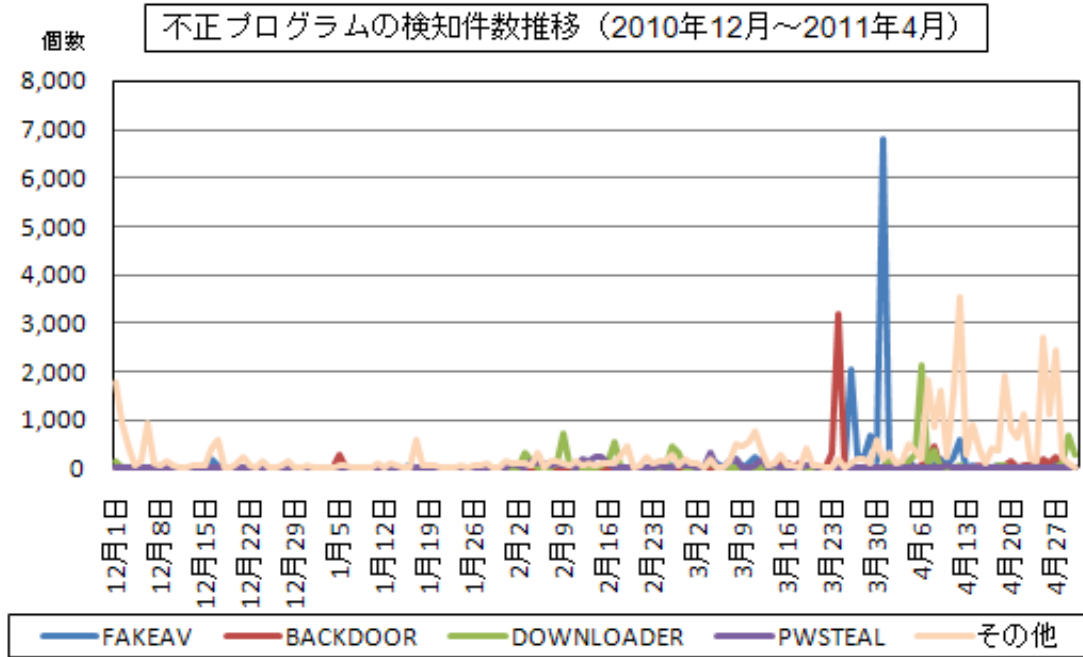


図2-3：不正プログラムの検知件数推移

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	14	22	12	10	6	5
被害あり ^(b)	7	7	6	5	6	5
被害なし ^(c)	7	15	6	5	0	0
相談^(d) 計	45	27	41	23	45	38
被害あり ^(e)	12	7	11	6	10	10
被害なし ^(f)	33	20	30	17	35	28
合計^(a+d)	59	49	53	33	51	43
被害あり ^(b+e)	19	14	17	11	16	15
被害なし ^(c+f)	40	35	36	22	35	28

(1) 不正アクセス届出状況

4月の届出件数は5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38件であり、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、メール不正中継1件、不正プログラム埋め込み1件、なりすまし2件でした。

「侵入」の被害は、サーバの設定不備を突かれてウェブサーバ内に不審なファイルを置かれたものが1件、でした。「不正プログラム埋め込み」の被害は、組織のLANに接続しているパソコンがウイルスに感染し、外部ネットワークなどにアクセスを試みていたものが1件、でした。「なりすまし」の被害は、フリーのウェブメール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が1件、メールアカウント管理不備により古いアカウントが使用されていたものが1件でした。

(4) 被害事例

[侵入]

(i) サーバの設定不備を突かれて侵入され、ファイルを置かれた

事例	<ul style="list-style-type: none">・ 組織外から「ウェブサーバに対するアップロードの通信を検知した」との連絡が入った。・ 調査したところ、当該サーバの WebDAV ディレクトリに、見知らぬファイルが置かれているのを発見。・ 当該サーバには XAMPP (ウェブアプリケーション群を 1 つにまとめたパッケージ) がインストールされており、XAMPP の WebDAV 機能にて使用されるデフォルトの認証情報でログインが可能な状態だった。・ 事後対策として、WebDAV 機能は不要であると判断したため、削除した。
解説・対策	<p>使われていない機能が設定不備のまま放置されていたことが原因でした。使われていない機能やサービスは、管理や監視の対象から外れることになるため、セキュリティ対策漏れにつながります。当初は必要だった機能でも、現在は不要になっている可能性があります。サーバで動作させる機能やサービスの棚卸しを、定期的を実施することをお勧めします。</p> <p>(参考)</p> <p>IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html</p>

[なりすまし]

(ii) 古いメールアカウントを不正使用され、自ドメインから大量のメールを送信された

事例	<ul style="list-style-type: none">・ 組織外から「あなたの管轄内のメールアドレスから大量のフィッシングメールが送信されている」との連絡が入った。・ 調査したところ、外部から退職者のアカウントを使用したメール送信要求があり、結果的に自ドメインから大量のメールを送信していた。・ 不正使用されたアカウントを即時削除した。アクセス元の IP アドレスとドメインからのメール送信要求を拒否するようにした。
解説・対策	<p>退職者のメールアカウントを廃棄せず放置しているうちに、第三者に乗っ取られてしまった例です。また外部からのメール接続を許可していたことも一因です。古いアカウントが残っていると、退職者にそのまま使われ続けたり、今回のケースのように第三者に乗っ取られたりする恐れがあります。メールアカウントに限らず、ユーザアカウントの棚卸しを定期的を実施することをお勧めします。特に異動や退職が多数発生する年度の変わり目の時期には、可能な限り棚卸しを実施してください。</p>

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**1,608件**でした。そのうち『ワンクリック請求』に関する相談が**455件**(3月:466件)、『偽セキュリティソフト』に関する相談が**6件**(3月:7件)、Winnyに関連する相談が**13件**(3月:22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**1件**(3月:2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		1,692	1,536	1,463	1,521	1,723	1,608
自動応答システム		1,036	954	892	892	1,106	997
電話		580	531	499	570	551	555
電子メール		72	49	64	53	58	50
その他		4	2	8	6	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対応件数

「電話」：IPAセキュリティセンター員による対応件数

※ 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。

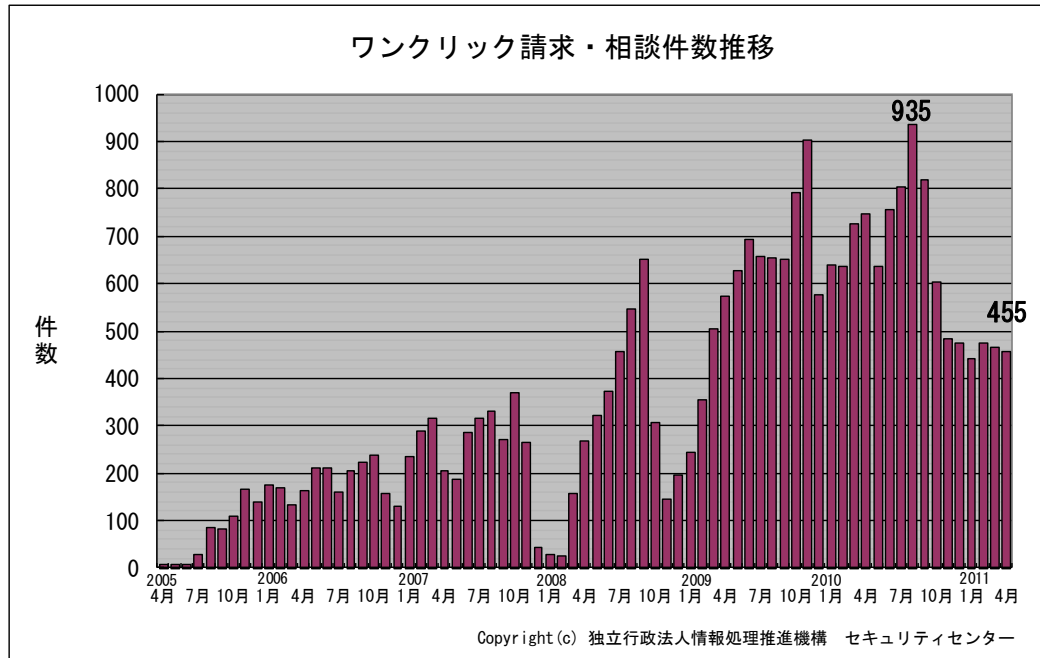


図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

(i) 企業のウェブサイトが改ざんされた場合の対処方法と、開示すべき情報を知りたい

相談	顧客から、“貴社のウェブサイトが改ざんされている”という報告を受けた。この場合どのような対処を行い、どういったところまで情報開示するのがいいのか。
回答	<p>この場合、ウェブサイトを開覧したパソコンにウイルスを感染させてしまう可能性があるため、早急に改ざんの有無をチェックしてください。</p> <p>その結果、ウェブサイトを開覧したパソコンにウイルスを感染させる仕掛けが施されていた場合、早急な対応が求められます。直ちにウェブサイトを一旦公開停止した上で、原因究明および修正作業を実施してください。自身での対応が難しい場合は、セキュリティサービス会社に依頼することをお勧めします。</p> <p>改ざん箇所を排除し、改ざんページの修正/再公開を完了させた後、ウェブサイトの利用者に向けた、改ざんの事実とウイルスに感染する危険性があつた旨の注意喚起、および謝罪文などを掲載することをお勧めします。</p> <p>(ご参考)</p> <p>IPA-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 http://www.ipa.go.jp/security/topics/20091224.html</p>

(ii) ウェブメールの管理事務局から怪しいメールが届いた

相談	<p>先日、利用しているウェブメールの管理事務局から、「期限までに名前やアカウントのパスワードなどの情報を送らないとデータが消える」という内容のメールが届き、慌てて指示された情報をメールで送ったところ、翌日、ウェブメールにログインできなくなりました。</p> <p>しかも、ウェブメールのアドレス帳に登録してあつた知人から、「あなたから『海外旅行中に盗難に遭い、お金に困っている』という内容のメールが送られてきた」という報告を受けた。</p> <p>これは一体何が起きたのか。</p>
回答	<p>これはメールによる典型的なソーシャルエンジニアリングの手口です。ソーシャルエンジニアリングとは、人間の心理的な隙や、行動のミスにつけ込んで個人が持つ秘密情報を入手する方法のことです。</p> <p>あなたのパスワードを入手した第三者がウェブメールアカウントを乗っ取り、勝手にメールを送ったと思われます。</p> <p>通常、ウェブメールの管理事務局であってもパスワードの情報を聞いてくることはありません。このようなメールが届いても、すぐ鵜呑み（うのみ）にせず、直接サービス運営元に問い合わせるなどの手段をとることをお勧めします。</p> <p>(ご参考)</p> <p>IPA-2010年3月の呼びかけ「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</p>

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、2011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194,413件、延べ発信元数[※]は71,935箇所ありました。平均すると、1観測点につき1日あたり240の発信元から648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向的アクセスがあると考えられます。

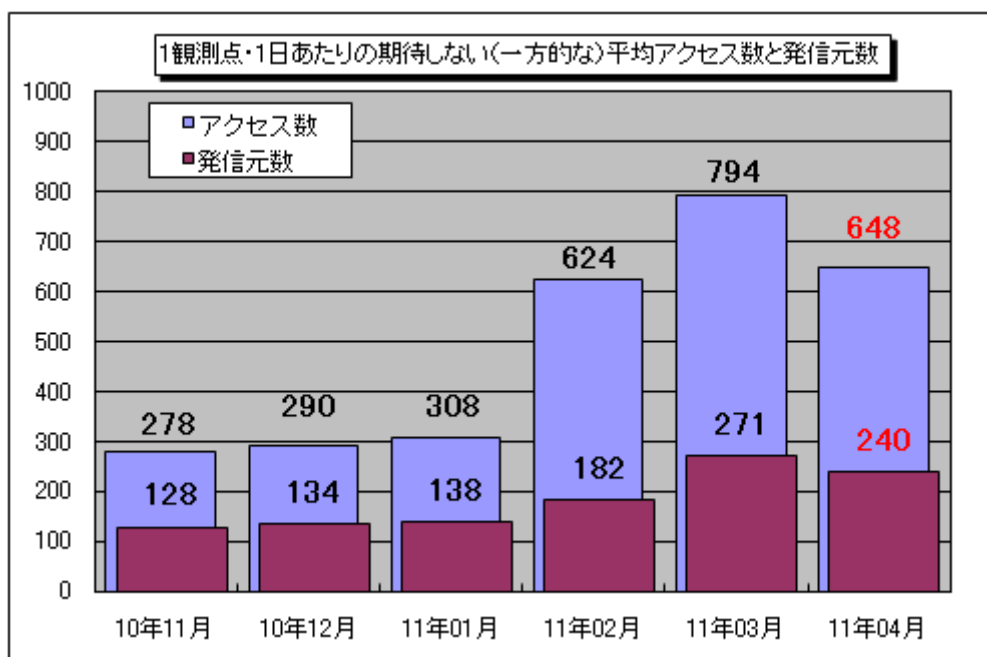


図5-1：1観測点・1日あたりの期待しない（一方的な）平均アクセス数と発信元数

2010年11月～2011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月と比べて減少しました。

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。3月に比べ、増加が観測されたのは29979/tcpへのアクセスでした。

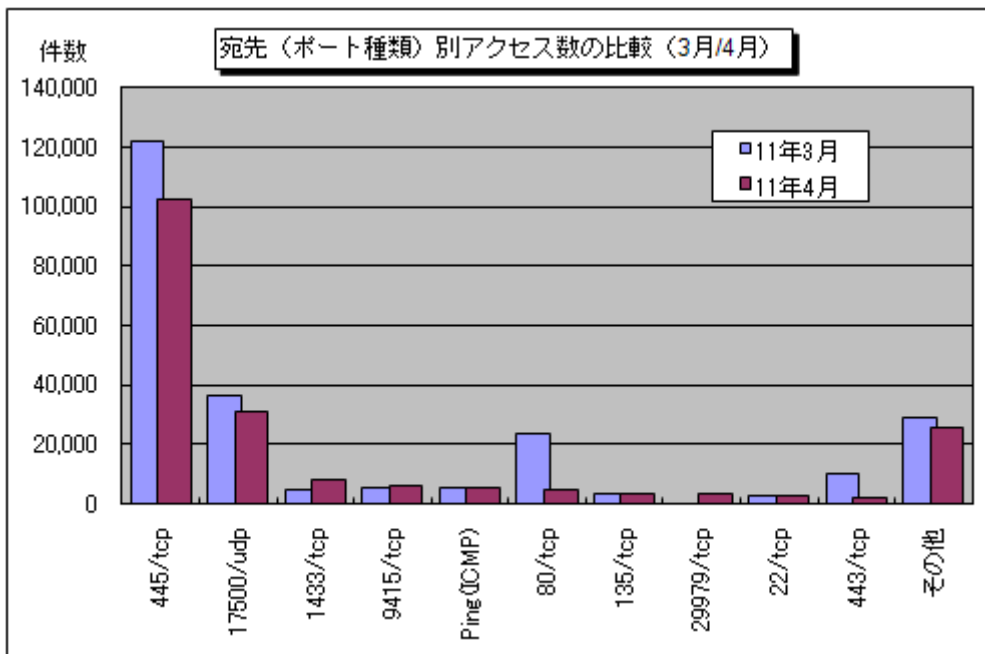


図 5-2：宛先（ポート種類）別アクセス数の比較（3月/4月）

29979/tcp については、4月4日に、TALOT2 の特定の1観測点に対して特定の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 5-3 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。

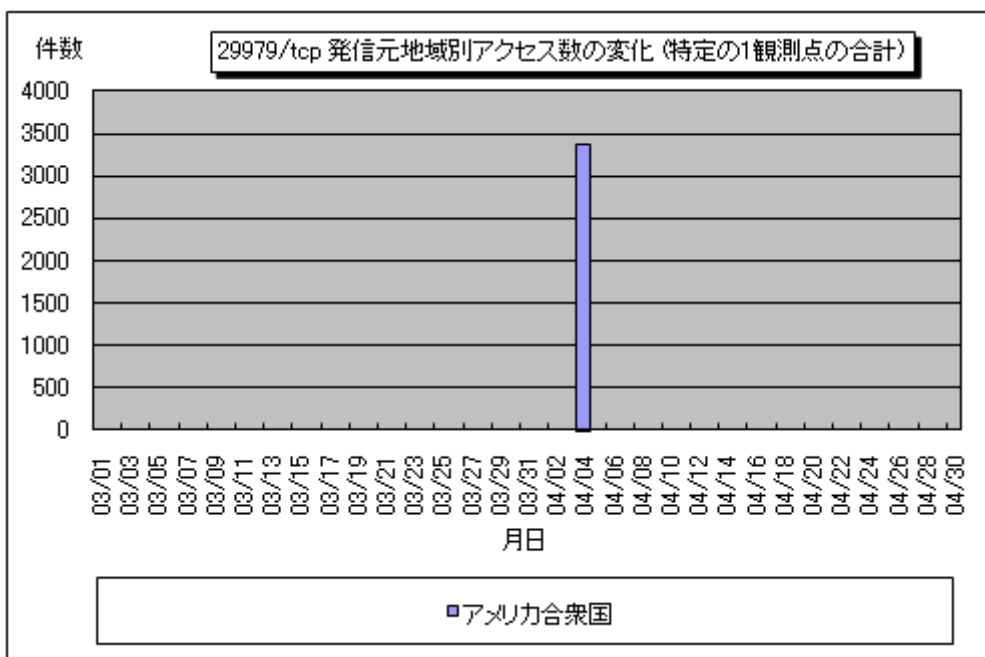


図 5-3：29979/tcp 発信元地域別アクセス数の変化（特定の1観測点の合計）

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3月に報告しましたが、80/tcp、443/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4月も観測されました（図 5-4 参照）。

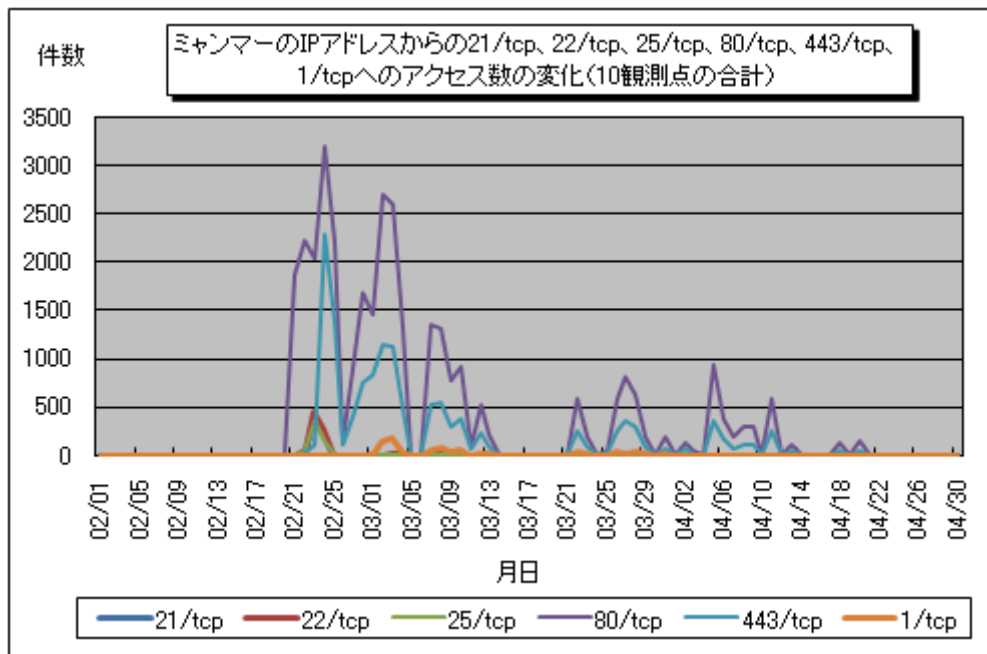


図 5-4 : ミャンマーの IP アドレスからの 21/tcp、22/tcp、25/tcp、80/tcp、443/tcp、1/tcp へのアクセス数の変化 (10 観測点の合計)

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/TALOT2-1105.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／宮本

Tel:03-5978-7591 Fax:03-5978-7518

E-mail: isec-info@ipa.go.jp