

コンピュータウイルス・不正アクセスの届出状況 [2011 年 12 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 12 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

「安全を 未来に届ける セキュリティ ※¹」

※¹ 第7回IPA情報セキュリティ標語・ポスターコンクール(2011年実施) 標語部門
金賞 坂井 泰法さん(新潟県 新潟市立宮浦中学校)

2011 年は重大な情報セキュリティ事件が相次いで発生した年でした。9 月に発生した重工業企業の情報流出や、10 月に発生した衆議院・参議院を標的としたサイバー攻撃は記憶に新しいところです。

その他にも以下の事例がありました。

- スマートフォンの流行に伴う、スマートフォン（特に Android 端末）を狙ったウイルスの増加
- 震災情報を装ったウイルスメールの出現（3 月～4 月）
- ゲーム会社の運営するネットワークサービスからの大規模な情報漏えい（4 月）
- 相次ぐウェブサイト改ざん

今や IT を利用する全ての人々にとって、インターネット上の事件は他人事ではなく、セキュリティ対策は全利用者にとって必須のものとなっています。

今月の呼びかけでは、2011 年に目立った「標的型攻撃※²」「インターネットサービスの不正利用」の 2 点について振り返り、解説するとともに対策を示します。

※² 標的型攻撃：特定の組織や個人を標的として、重要情報や知的財産などを不正に取得することを目的に行われるサイバー攻撃。

(1) 標的型攻撃

(i) 近年のサイバー攻撃の特徴と、動機の変化

企業・組織をとりまく近年のサイバー攻撃では、攻撃者の動機の変化と、攻撃に使われる手口の巧妙化が特徴的です（図 1-1 参照）。

サイバー攻撃を行う者の動機は、「いたずら」や「能力の誇示」ではなく、数年前から「金銭目的」「組織活動の妨害」に変化しています。金銭目的の場合、攻撃者は初めから組織の内部にある金銭的価値のある情報（機密情報・個人情報など）を狙っており、これを窃取し、最終的に金銭化することが目的です。従って、情報の流出が発生した場合、何らかの形で悪用される可能性が高く、組織活動に大きな被害を及ぼします。

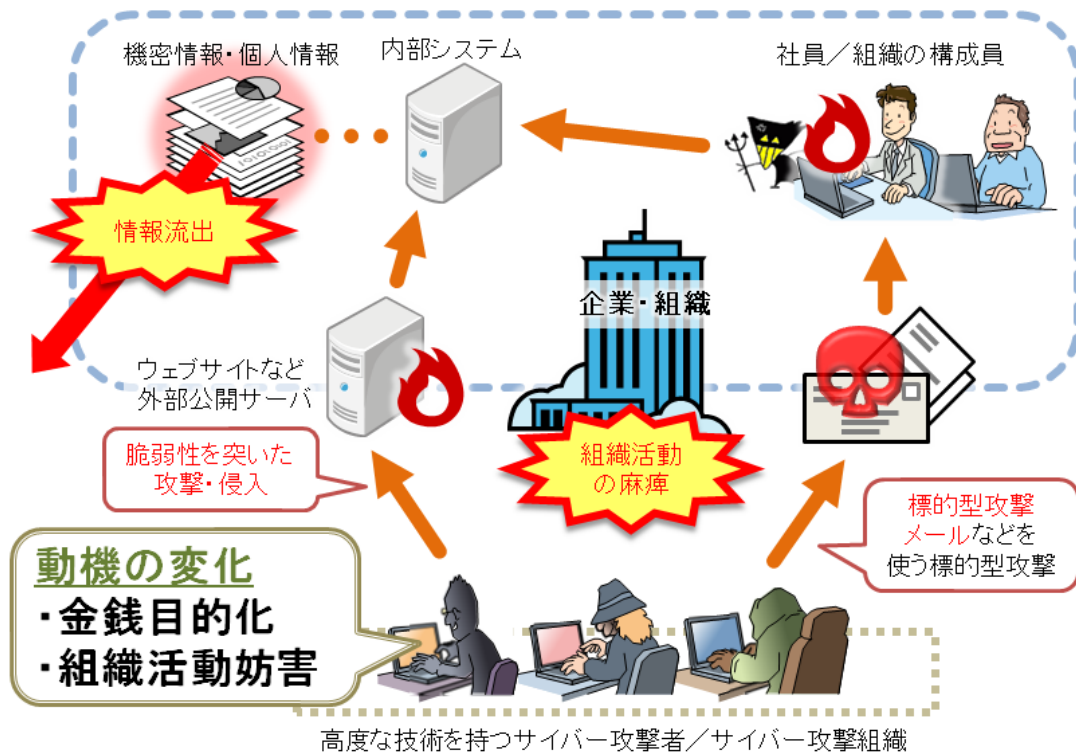


図 1-1：近年のサイバー攻撃の特徴

サイバー攻撃の中でも 2011 年は特に攻撃の対象とする組織や個人を絞った「標的型攻撃」の多さが目立ちました。経済産業省が実施したアンケート調査^{※3}によると、「標的型攻撃」を受けた経験のある企業は、2007 年には 5.4%でしたが、2011 年には 33%に増加しています。

標的型攻撃には様々な手法がありますが、攻撃対象ごとに作成したウイルスメールを送る「標的型攻撃メール」が主流です。無作為にばら撒かれているウイルスメールとは異なり、本物らしい差出人やメール本文、ウイルス対策ソフトで検出されにくいウイルスを使うなどの特徴があります。

※3 「最近の動向を踏まえた情報セキュリティ対策の提示と徹底」（経済産業省）

<http://www.meti.go.jp/press/2011/05/20110527004/20110527004.html>

(ii) 標的型攻撃メールによる被害の実例

標的型攻撃メールの添付ファイルを開いたり、メール本文に記載されている URL をクリックしたりすることで、パソコンがウイルスに感染します。その結果、パソコン内のファイルを外部に送信されて情報が漏えいしたり、パソコンを外部から乗っ取られて組織内のサーバーに不正アクセスされる、などの被害が発生します。

パソコンにウイルスを感染させる手口として、以下の実例があります。

- ワードプロソフト、Adobe Reader、Flash Player、JRE、ウェブブラウザなど、データファイルを開いたり、ウェブサイトを参照したりするのに利用されるアプリケーションに存在する脆弱（ぜいじゃく）性が悪用されて、添付ファイルを開いた際にパソコンがウイルス感染。
- RLO（Right-to-Left Override）^{※4}の手口により添付ファイルの拡張子が偽装されていて、添付ファイルを文書ファイルと思いクリックしてしまった結果、パソコンがウイルス感染。

※4 RLO（Right-to-Left Override）：特殊な制御文字を使用して、ファイル名の文字の並びを「左→右」から「右→左」に変更する機能。

(iii) 標的型攻撃メールへの対策

(a) 利用者個人でできる対策

- 標的型攻撃メールでは、細工した PDF ファイルなど、パソコン内のソフトウェアの脆弱性を悪用し、ウイルスに感染させようとする手口が使われます。ウイルス対策ソフトを利

用するとともに、IPA が公開している「MyJVN バージョンチェッカ」などを活用し OS やアプリケーションを常に最新のものに保ち、脆弱性を解消するよう努めてください。

(ご参考)

「MyJVN バージョンチェッカ」(パソコン内のソフトウェアをチェックするツール)

<http://jvndb.jvn.jp/apis/myjvn/#VCCHECK>

- 「標的型攻撃のメールを見抜き、開かない」、「不審なメールを受信したら組織内で周知する」といった人による対策も重要です。

組織内の全ての人に標的型攻撃メールが届く可能性がありますので、全利用者において、脅威の理解と注意が必要です。また、不審なメールを受信した時、組織としてどのように対応するのか(注意の周知手順など)のルールを確立してください。

(ご参考)

「実例から分かる標的型攻撃メールの『違和感に気付くポイント』と『違和感に気付いた後の対策ポイント』」

<http://www.ipa.go.jp/security/vuln/report/newthreat201006.html>

「情報窃取を目的として特定の組織に送られる不審なメール『標的型攻撃メール』」

<http://www.ipa.go.jp/security/virus/fushin110.html>

(b) 経営層、システム管理部門、システム管理者向け

“罨(わな)のメールを見抜く”ための訓練・対策である、JPCERT/CC(一般社団法人 JPCERT コーディネーションセンター)による「IT セキュリティ予防接種」※5の実施結果と、効果的な実践方法に関する調査結果が公開されています。こちらも併せて参考にしてください。

※5 「IT セキュリティ予防接種」: 職員のセキュリティ意識向上などを目的として、組織に対して擬似的に標的型攻撃を行うこと。職員に標的型攻撃メールを配送した後は、最後に種明かしをして不安を払拭するとともに、調査結果をフィードバックし職員の啓発を行うことが通常。

(ご参考)

「IT セキュリティ予防接種調査報告書 2009 年度」(JPCERT/CC)

<http://www.jpCERT.or.jp/research/#inoculation>

(c) 標的型メールに関する相談先

IPA では、標的型攻撃が多発している深刻な事態を受け、早期の攻撃情報の収集・分析・共有を図り、予防・対処方法などの情報を提供するための特別相談窓口を設置しております。

標的型攻撃メールと思われるメールを受信した場合には下記連絡先までご連絡ください。

- 標的型サイバー攻撃の特別相談窓口

TEL: 03-5978-7509 FAX: 03-5978-7518

(2) インターネットサービスの不正利用

(i) 不正利用の現状

2011 年に発生した不正利用の事例を以下に挙げます。

- 大手インターネットサービスプロバイダーでの、第三者のなりすましによる、商品に交換できるポイントの盗難(5月、100件以上・総額10万円相当の被害)
- かまぼこ販売サイトのシステム管理会社から、顧客のクレジットカード情報が流出(5月、約200件・約200万円の被害)
- 日本国内の大手・地方銀行のインターネットバンキングにおける相次ぐ不正利用(累計約3億円の被害)
- 科学雑誌出版社のウェブサイトへの不正アクセスに起因した、個人情報・カード情報の漏えいと不正利用(8月、10数件のクレジットカード不正利用)
- 大手インターネットショッピングサービスにおける大規模な不正利用事件(11月、約4,000件の被害)

このように 2011 年は多くの不正利用が発生しています。情報が漏えいしたか否かが不明である不正アクセスの被害も含めると、その件数はさらに多くなり、また、一度に漏えいした情報量や、被害を受けた顧客数の多さも目立ちます。

(ii) 不正利用の原因

インターネットサービスを不正利用される原因として、以下の (a)、(b)、(c) の手口で ID とパスワードを窃取されることが挙げられます。

(a) メールの添付ファイルや USB メモリを介してウイルスに感染

ID とパスワードを窃取するウイルスを添付したメールを送りつけ、その添付ファイルを開かせることで、利用者のパソコンにウイルスを感染させます。

USB メモリなどの外部記憶媒体も、ウイルスの感染経路の 1 つとしてよく使われます。

(b) ウェブサイトの閲覧を介してウイルスに感染

この数年で、ウェブサイトの閲覧でパソコンにウイルスを感染させる手口の主流となった攻撃手法に“ドライブ・バイ・ダウンロード”が挙げられます。これは、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で、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。この手口で ID とパスワードを窃取するウイルスをパソコンに感染させられると、利用者の知らない間に ID とパスワードが奪われてしまいます。

“ドライブ・バイ・ダウンロード”攻撃を行うウェブサイトへの誘導方法としては、メールをはじめ、mixi、Facebook などの SNS（ソーシャルネットワーキングサービス）や、Twitter などのマイクロブログサービスにおいて、本文やコメントに書かれている URL を言葉巧みにだましてクリックさせる手法が使われます。

(c) フィッシング詐欺

インターネットショッピングサービスや銀行をかたったメールから偽のウェブサイトに誘導され、そこで ID/パスワードを入力してしまい、窃取される場合です。誘導するメールの内容も、ソーシャルエンジニアリング^{※6}を使った言葉巧みなものになっています。さらに、最近では既知のフィッシング詐欺の手口に、ウイルスを組み合わせた新しい攻撃手法も出現しており、注意が必要です。

（ご参考）

「ウイルスを使った新しいフィッシング詐欺に注意！」

<http://www.ipa.go.jp/security/txt/2011/10outline.html>

※6 ソーシャルエンジニアリング（social engineering）：人間心理や社会の盲点を超えて、秘密情報（パスワードなど）を入手する方法。

(iii) 不正利用の被害拡大の原因

通常一つのインターネットサービスに対しては、一つの ID とパスワードを登録・管理しますが、この際に覚えきれないといった理由から、複数のサービスで同じ ID とパスワードを登録する“使い回し”を行ってしまう場合があります。ID とパスワードを使い回してしまうと、そのうちの一つのインターネットサービスで ID とパスワード情報が漏えいしただけで、他のインターネットサービスも連鎖的に不正利用され、被害が拡大する恐れがあります（図 1-2 参照）。

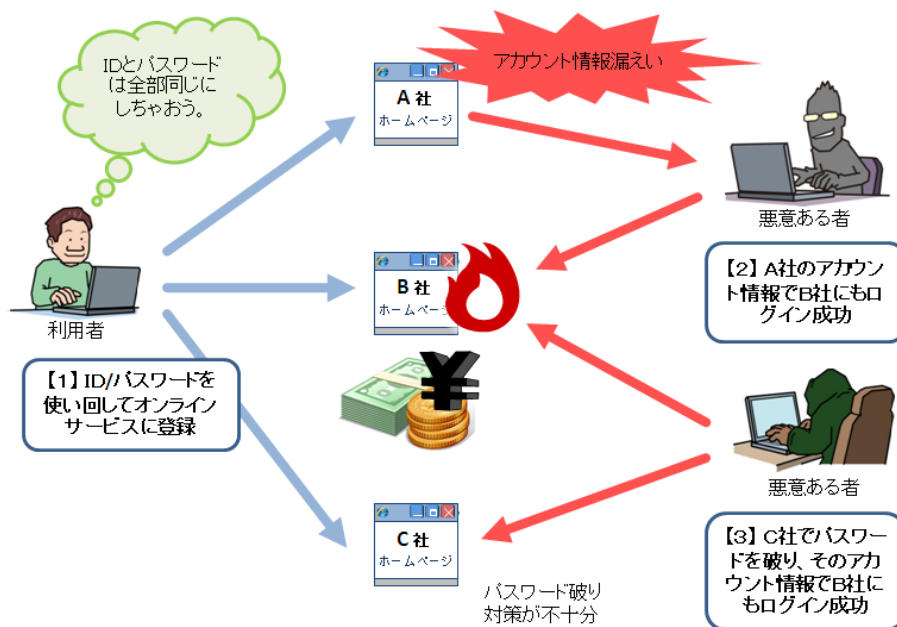


図 1-2 : ID とパスワードを使い回す危険性

(iv) 対策

(a) ID とパスワードの適切な管理

ID とパスワードの使い回しをすることで、“なりすまし”の被害が拡大する可能性があります。“なりすまし”の被害に遭わないよう、ID とパスワードを扱う上での基本的な対策を、次の三つの点を通じて実施してください。

- パスワードの強化…使用できる文字種（大小英文字、数字、記号）全てを組み合わせ、8文字以上のパスワードとする。辞書に載っているような単語や人名を避ける。
- パスワードを適切に保管…ID とパスワードを紙などにメモする場合は、それぞれを別の紙にメモするなどして保管する。
- パスワードの適切な利用…自分が管理していないパソコン（例えばネットカフェなどの不特定多数が利用するパソコン）では、インターネットサービスにログインしない。

（ご参考）

「パスワード ぼくだけ知ってる たからもの」

<http://www.ipa.go.jp/security/txt/2011/06outline.html#5>

(b) OS やプログラムの最新化とウイルス対策の利用

上述の“なりすまし”対策を実施していても、セキュリティ対策の基本であるウイルス対策ソフトの導入は必須です。オンラインサービスへログインする時に利用者が入力したID やパスワードを盗み取るウイルス（キーロガー）が確認されています。このようなウイルスに感染して情報を盗まれないために、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。

(c) ログインアラート機能の利用

オンラインサービスによっては、ログインしたタイミングでそれをメールで通知する機能（ログインアラート機能）を提供している場合があります。身に覚えのないログインアラートメールが届いた場合は、即座にアカウントをロックすることにより、被害を最小限に留めることができます。

(3) 2012 年の展望

『企業は情報が狙われ、個人は金銭が狙われる』傾向がより強まると考えられます。特に金銭が絡むサービスは全て脅威にさらされると言っても過言ではないでしょう。

(i) 対象のボーダーレス化

2011 年は特定の業界や政府関係機関が、標的型攻撃の主な攻撃対象となっていました。その傾向は続きますが、さらに 2012 年はあらゆる業種の企業にとって標的型攻撃が大きな脅威になると

思われます。

一例として、ある企業の秘密情報の入手を企てる者が、その社員の SNS のページから友人を割り出して、まずはその友人のパソコンを標的に攻撃してウイルス感染させることで、最終的に目的の企業の秘密情報を入手する、といったシナリオが考えられます。こうしたシナリオは以前からありますが、昨今の SNS 利用の広がりによって、第三者が他人の交友関係を把握することが容易になっており、言わば「踏み台」として利用するためにあらゆる企業や個人が狙われることが考えられます。

(ご参考)

『『新しいタイプの攻撃』の対策に向けた設計・運用ガイド』

<http://www.ipa.go.jp/security/vuln/newattack.html>

(ii) 今まで狙われなかった無料サービスも狙われる

パスワードの使い回しをしている人を狙って、今後は金銭と関係無いサービスも攻撃対象となるケースが増加する可能性があります。

有料サービスでも同じ ID とパスワードを使い回していた場合、結果的に金銭的被害に遭う可能性が高くなります。有料・無料に関係無く安易なパスワードは避け、さらにパスワードは使い回さないようにしてください。

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、9 頁の「3.コンピュータ不正アクセス届出状況」を参照）
 - ・サーバーの脆弱性を悪用され、ウェブページを改ざんされた
 - ・サーバー上の実行ファイルを差し替えられ、外部から接続可能な状態にされた
- 相談の主な事例（相談受付状況および相談事例の詳細は、11 頁の「4.相談受付状況」を参照）
 - ・ Facebook に、自分になりすましたと思われるアカウントを見つけた
 - ・いつも使っているオンラインショッピングサイトから、心当たりのない商品の購入通知メールが送られてきた
- インターネット定点観測（13 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

12月のウイルスの検出数^{※1}は、**13,259個**と、11月の20,585個から35.6%の減少となりました。また、12月の届出件数^{※2}は、**764件**となり、11月の1,115件から31.5%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の。

・12月は、寄せられたウイルス検出数13,259個を集約した結果、764件の届出件数となっています。

検出数の1位は、**W32/Netsky**で**6,425個**、2位は**W32/Mydoom**で**4,666個**、3位は**W32/Downad**で**674個**でした。

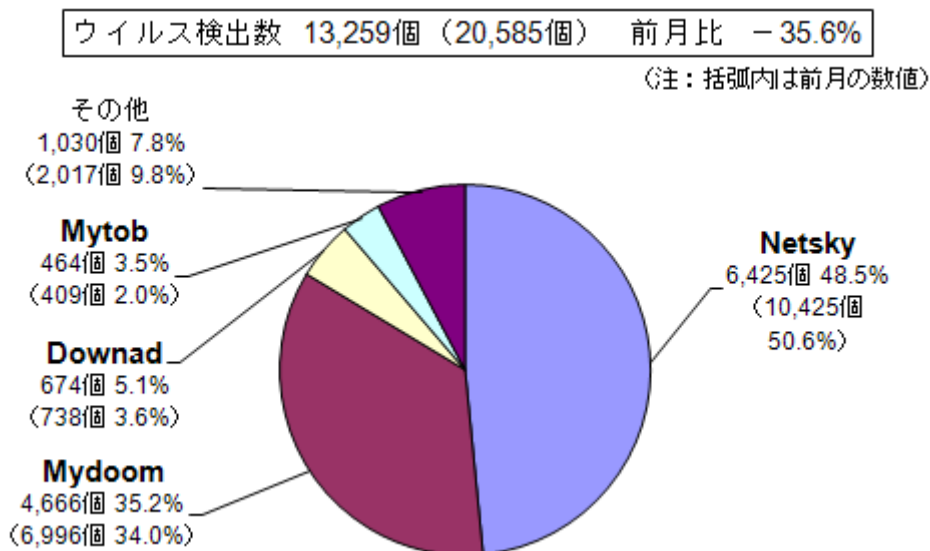


図 2-1：ウイルス検出数

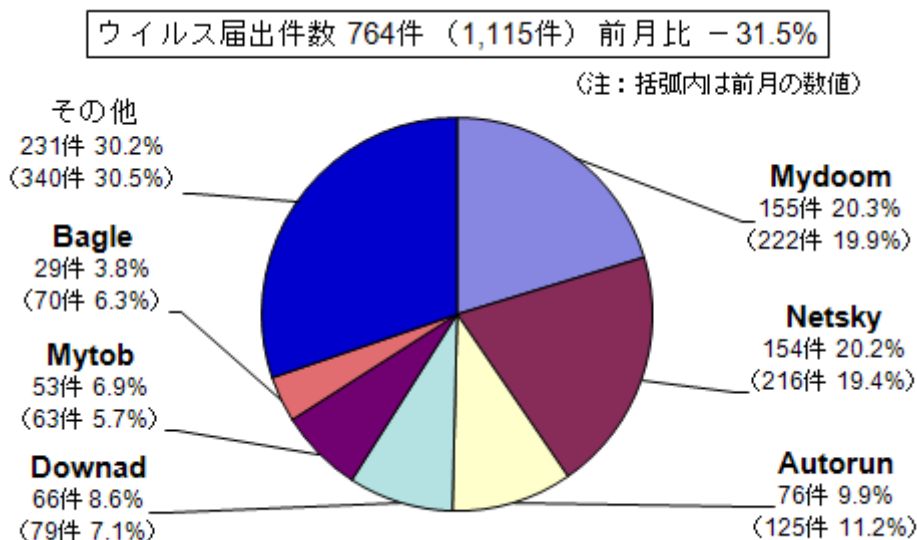


図 2-2：ウイルス届出件数

(2) 不正プログラムの検知状況

12月は、特に目立った動きはありませんでした。また、9月に大幅に増加したRLTRAPは、12月前半に1日だけ多く検知された日がありました(図2-3参照)。

※ここでの「不正プログラムの検知状況」とは、IPAに届出られたものの中から「コンピュータウイルス対策基準」におけるウイルスの定義に当てはまらない不正なプログラムについて集計したものです。

※コンピュータウイルス対策基準：平成12年12月28日(通商産業省告示第952号)(最終改定)(平成13年1月6日より、通商産業省は経済産業省に移行しました。)

「コンピュータウイルス対策基準」(経済産業省)

<http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm>

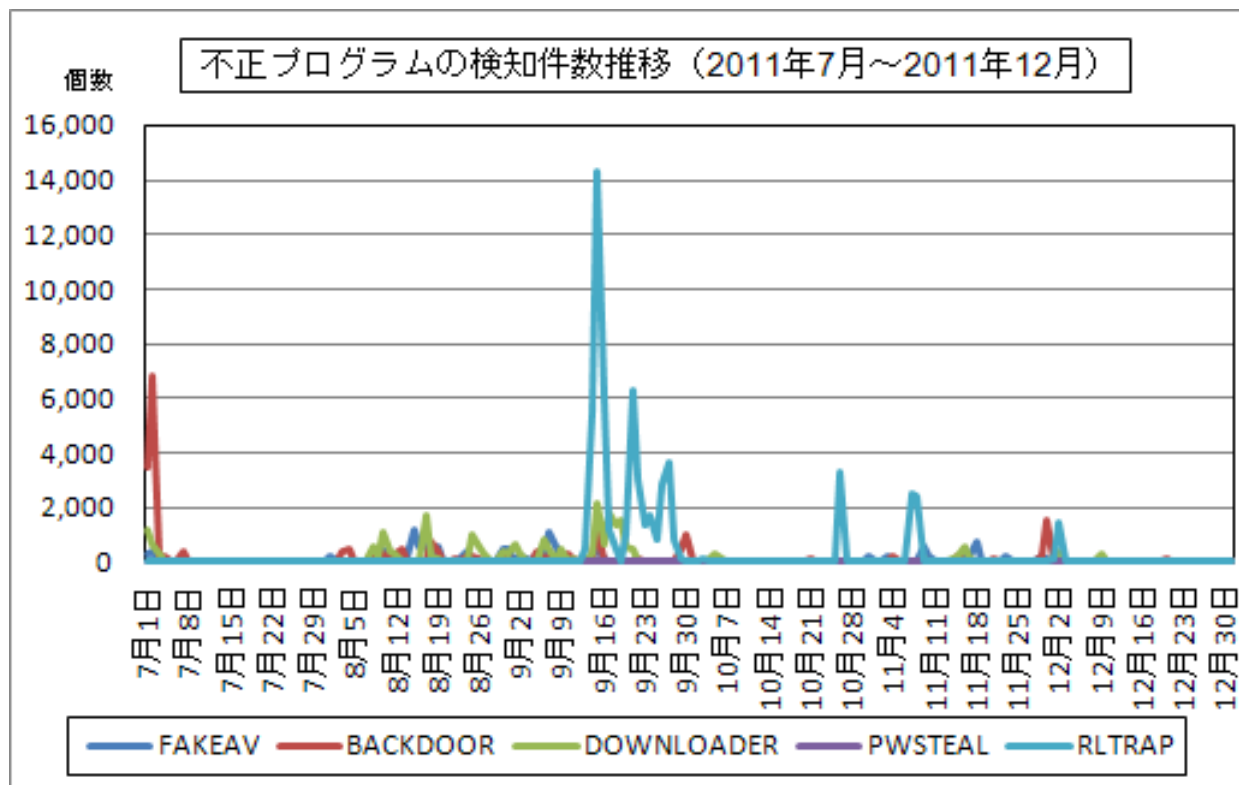


図2-3：不正プログラムの検知件数推移

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

	7月	8月	9月	10月	11月	12月
届出^(a) 計	8	10	7	15	7	7
被害あり ^(b)	5	8	5	8	5	7
被害なし ^(c)	3	2	2	7	2	0
相談^(d) 計	47	37	31	46	69	42
被害あり ^(e)	15	13	8	7	14	13
被害なし ^(f)	32	24	23	39	55	29
合計^(a+d)	55	47	38	61	76	49
被害あり ^(b+e)	20	21	13	15	19	20
被害なし ^(c+f)	35	26	25	46	57	29

(1) 不正アクセス届出状況

12月の届出件数は7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42件であり、そのうち何らかの被害のあった件数は13件でした。

(3) 被害状況

被害届出の内訳は、**侵入4件、不正プログラム埋め込み3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1件、SQLインジェクション攻撃を受けてデータを削除されたものが1件、他サイト攻撃の踏み台として悪用されたものが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やウェブアプリケーションの脆弱性を突かれたものが2件、でした。

(4) 被害事例

[侵入]

(i) サーバーの脆弱性を悪用され、ウェブページを改ざんされた

事例	<ul style="list-style-type: none">・ レンタルサーバー運営会社からウェブサイト改ざんに対する注意喚起があり、念のため全コンテンツを精査したところ、改ざんの形跡を発見。自動的に外部サイトにリダイレクトされるようになっていた。・ サーバー管理用にウェブサイト上で使っていた CMS (Contents Management System) に脆弱性があり、それを悪用されてウェブコンテンツを改ざんされた。・ CMS は最新版に更新する予定。
解説・対策	<p>インターネット越しにサーバーを管理できるようにする場合、悪意ある者に狙われて悪用されるかも知れない、ということ念頭に置いた対策が必要です。有名なツールであれば、特に狙われやすいと言えます。脆弱性の解消はもちろんのこと、WAF (Web Application Firewall) を導入してサイト全体のセキュリティを強化することも有効です。</p> <p>2011 年後半から、レンタルサーバーの利用者から、CMS の脆弱性を悪用されてウェブサイトを改ざんされる被害の届出と相談が増えています。セキュリティ対策をレンタルサーバー業者に一任するのではなく、提供サービスや使用ツールを自社で把握し、それぞれについて脆弱性を解消するよう努めてください。</p> <p>(ご参考)</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>

[侵入]

(ii) サーバー上の実行ファイルを差し替えられ、外部から接続可能な状態にされた

事例	<ul style="list-style-type: none">・ 学内設置の公開用ウェブサーバーから、海外に不審なパケットが断続的に送信されていることを発見した。・ 該当サーバーを調査したところ、普段動作させていないサービスが動作しており、その実行ファイルが別のものに差し替えられていた。具体的には、本来「Microsoft Office Diagnostics Service」サービスの実行ファイルである「Odserv.exe」の中身が、Telnet サービスの実行ファイル (Tlntsvr.exe) に差し替えられていた。・ その結果、サーバー上で Telnet サービスが稼働し、外部からの接続を受け付けていたものと思われる。また差し替えられたファイルは、そのプロパティから、中国語版 Windows に含まれている Tlntsvr.exe と推測される。差し替えられた原因と経緯は今のところ不明。・ 該当サーバーは初期化した。また今後の対策として、ネットワーク監視サービスの導入を検討中。
解説・対策	<p>サーバーに埋め込まれていたプログラムが何だったのか明らかにされた貴重な例です。それ以外にも別の不正プログラムを埋め込まれている可能性も否定できないため、やはりサーバーの初期化が必要です。また、当該サーバーを経由して、学内の他のサーバーにも侵入されている恐れがあるので、学内サーバーの総点検を勧めます。</p> <p>(ご参考)</p> <p>IPA - ウェブサイト運営者のための脆弱性対応ガイド http://www.ipa.go.jp/security/fy19/reports/vuln_handling/</p>

4. 相談受付状況

12月のウイルス・不正アクセス関連相談総件数は**1,312件**でした。そのうち『ワンクリック請求』に関する相談が**333件**（11月：418件）、『偽セキュリティソフト』に関する相談が**8件**（11月：11件）、Winnyに関連する相談が**7件**（11月：35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**6件**（11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

	7月	8月	9月	10月	11月	12月
合計	1,490	1,651	1,551	1,496	1,420	1,312
自動応答システム	889	958	936	865	746	790
電話	540	639	554	564	561	451
電子メール	54	50	52	55	102	65
その他	7	4	9	12	11	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。

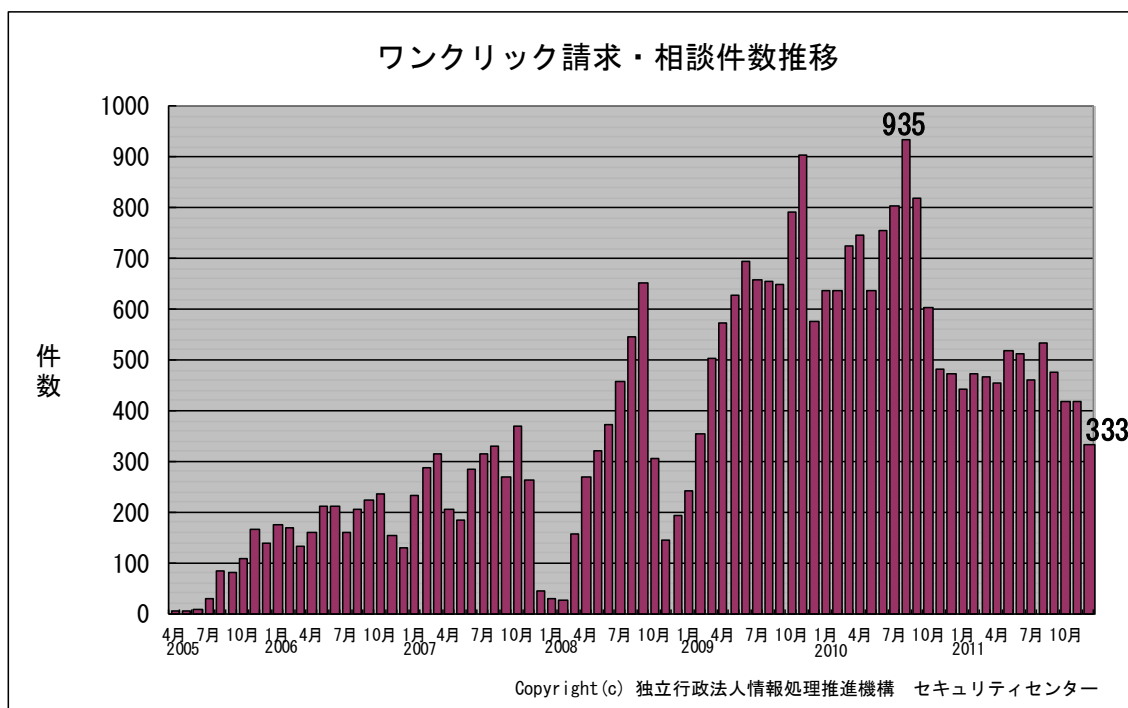


図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

(i) Facebook に、自分になりすましたと思われるアカウントを見つけた

相談	インターネットの検索サイトで自分の名前を入力して検索すると、自分では登録した覚えのない Facebook アカウントのページが表示された。私になりすました、偽のアカウントと思われる。 削除を要請したいが、どうしたらいいか分からない。
回答	Facebook は、世界中で利用されている SNS (ソーシャルネットワーキングサービス) の一つです。多くの著名人も登録しており、本人になりすました偽物が存在するといったことも問題になっています。Facebook では、他人になりすましてアカウントを作成することは規約違反にあたります。自分の写真が使われているなど、明らかに自分になりすましていると思われるアカウントを発見した場合、以下の Facebook ヘルプセンターのページの、「偽アカウントを報告するにはどうすればよいですか」の手順に従い、早急に通報することをお勧めします。 (ご参考) 違反の報告 (Facebook ヘルプセンター) http://ja-jp.facebook.com/help/?page=204546626249212

(ii) いつも使っているオンラインショッピングサイトから、心当たりのない商品の購入通知メールが送られてきた

相談	いつも使っているオンラインショッピングサイトから、心当たりのない商品の購入通知メールが送られてきた。サイト側に確認したところ、不正アクセスの疑いがあるということで、クレジットカードによる代金の引き落としはキャンセルしてもらえた。また、クレジットカード番号は変更した。 パスワードを単純なものにしていたのがいけなかったと思う。また当該サイト以外のサービスでも同じパスワードを使い回しているのだが、危険か。
回答	パスワードが単純だったために簡単に破られ、第三者から当該アカウントに不正アクセスされて勝手に商品購入の手続きを行われてしまったものと思われます。早急に当該サイトのパスワードをできるだけ複雑なものに変更することはもちろん、連鎖的に不正アクセスの被害が拡大することを防ぐため、同じパスワードを使い回している全てのサービスについて、複雑かつ異なるパスワードに変更してください。 (ご参考) IPA-2011 年 11 月の呼びかけ「ぼくだけの ひみつのかぎさ パスワード」 http://www.ipa.go.jp/security/txt/2011/12outline.html

5. インターネット定点観測での12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12月の期待しない（一方的な）アクセスの総数は10観測点で**81,017件**、延べ発信元数[※]は**30,870箇所**ありました。平均すると、**1観測点につき1日あたり144の発信元から324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。

※12月26日～31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、12月の観測データは、この6日を除外して統計情報を作成しています。

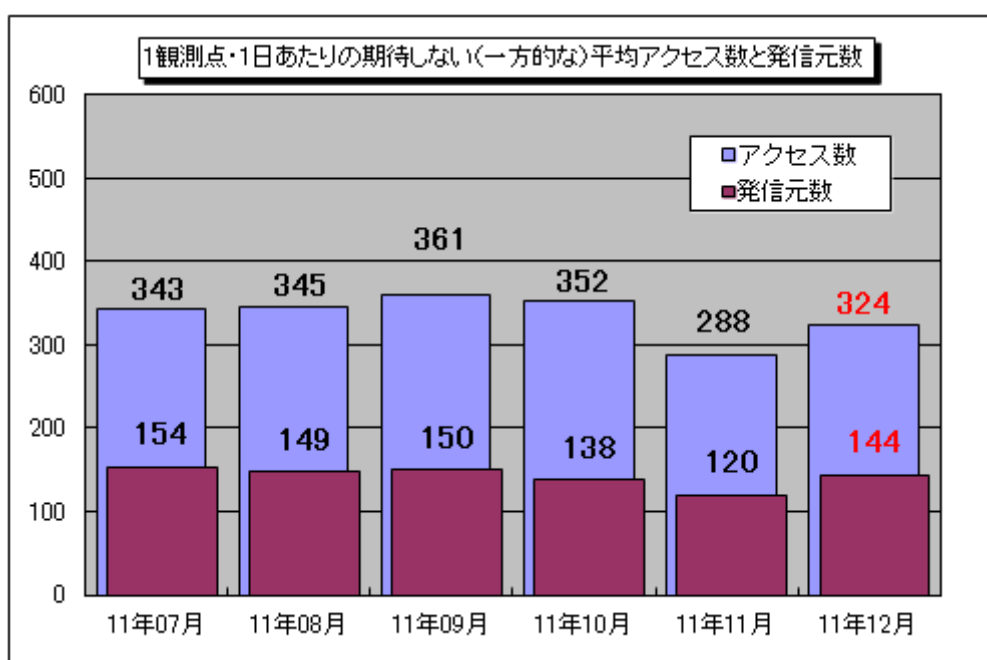


図5-1：1観測点・1日あたりの期待しない（一方的な）平均アクセス数と発信元数

上記グラフは2011年7月～2011年12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示しています。12月の期待しない（一方的な）アクセスは、11月と比べて増加しました。

11月と12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。これを見ると、11月は少なかった24529/tcpや8612/tcpへのアクセスが、12月は増加していました。

24529/udp、および8612/udpについては、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、ともに特定の1観測点のみで観測されていました。

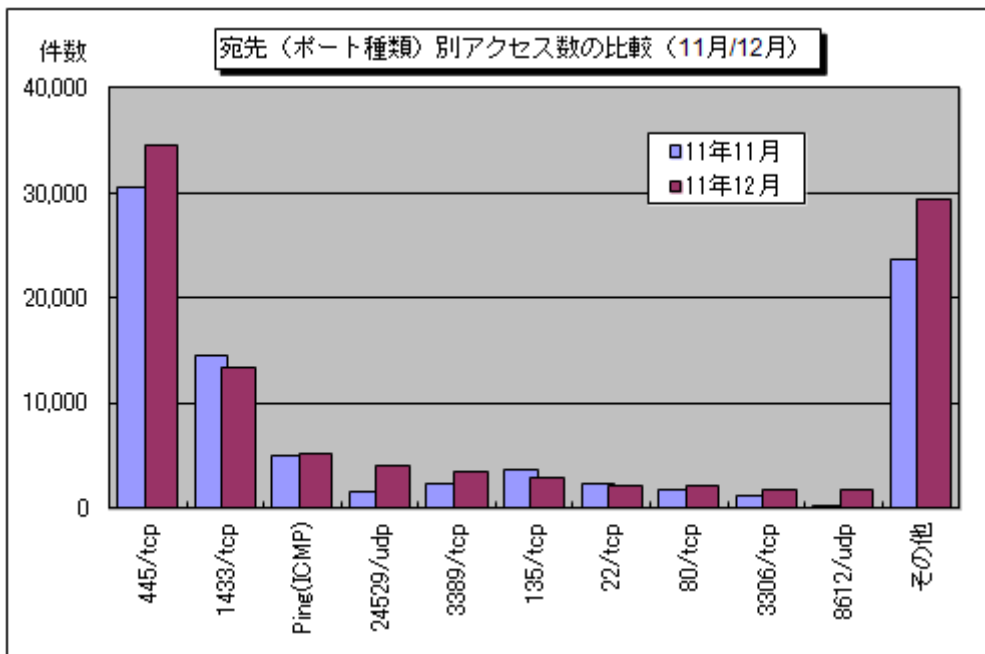


図 5-2：宛先（ポート種類）別アクセス数の比較（11月/12月）

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/TALOT2-1201.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/>

株式会社カスペルスキー：<http://www.viruslistjp.com/analysis/>

■お問い合わせ先

IPA 技術本部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