Information-technology
Promotion
Agency, Japan

プレスリリース
第 11-35-233 号
2011 年 12 月 5 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 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、2011 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

「 ぼくだけの　ひみつのかぎさ　パスワード ※1」
～インターネットサービスの不正利用がないか確認を～

※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年度実施）標語部門
金賞　松岡　稔さん（北海道　札幌市立東川下小学校5年）

2011 年 11 月に、大手インターネットショッピングサービスにて大規模な不正利用事件が発生したとの報道がありました。

事件の概要は、身に覚えのない商品購入の被害に遭うというもので、2011 年 7 月から約 4,000 件の被害が発生しています。なお、同じサービスにおいて同様の事件が、2009 年の年末から 2010 年の初めにかけても発生していました。

前回、今回とも原因は不明ですが、サービスを利用する際の ID／パスワードが窃取されて悪用された可能性が高いと考えられます。

今回報道されたサービスに限らず、インターネットサービスを利用する場合は、こうした不正利用の被害に遭わないよう、利用者側で行える確認や対策を行い、ID／パスワードを適切に管理してください。

（1）最近の不正利用の事例

2011 年に発生した、主な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（2011 年 5 月）
- 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不正利用（2011 年 6 月～7 月）
- 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（2011 年 8 月）

このように、冒頭の大手ショッピングサービスの事件も含め、2011 年は多くの不正利用事件が発生しています。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。

（2）不正利用された原因

インターネットサービスを不正利用される原因として、【i】や【ii】の手口で ID／パスワードを窃取されることが推測されます。また、被害を拡大させてしまった原因として【iii】が挙げられます。

【i】ウイルス感染

利用者のパソコンに、ID／パスワードを窃取するウイルスを感染させます。感染させる手口は、以下のケースが挙げられます。

(a) ウイルス入りファイルが添付されたメールを介して感染

ID／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。

関係機関や関係者を装い、組織や個人を絞ってウイルスを仕込んだ添付ファイルを送りつける

「標的型攻撃」メールも該当します。
（ご参考）
災害情報を装った日本語のウイルスメールについて（IPA）
http://www.ipa.go.jp/security/topics/alert20110404.html

(b) ウェブサイトの閲覧を介してウイルスを感染させる“ドライブ・バイ・ダウンロード”攻撃で感染

“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。この数年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方法で、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（ぜいじゃく）性が悪用されます。

“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。

（ご参考）
「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！」（IPA）
http://www.ipa.go.jp/security/txt/2010/12outline.html

(c) USB メモリなどの外部記憶媒体を介してウイルスに感染

USB メモリなどの外部記憶媒体は、ウイルスの感染経路の 1 つとしてよく使われます。これは、Windows パソコンの自動実行機能※2 を悪用するためです。

（ご参考）
「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！」（IPA）
http://www.ipa.go.jp/security/txt/2011/03outline.html

※2　Autorun。USB メモリなどの外部記憶媒体をパソコンに接続した際、またはアイコンをダブルクリックして開こうとした際に、媒体に保存されているファイルが自動的に実行される Windows の機能のこと。

【ii】フィッシング詐欺

フィッシング詐欺とは、実在する企業（主に銀行やクレジットカード会社）をかたったメールなどから、利用者を偽のウェブサイトに誘導し、そのウェブサイトに個人情報や ID／パスワード、口座番号やクレジットカード番号、暗証番号などを入力させて窃取し、その情報を使って金品をだまし取る詐欺行為です。

冒頭の事件に当てはめると、利用者が大手インターネットショッピングサービス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、窃取されたと考えられます。また、誘導するメールの内容も、ソーシャルエンジニアリング※3 を使った言葉巧みなものになっていると思われます。さらに、最近では既知のフィッシングの手口に、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！」（IPA）
http://www.ipa.go.jp/security/txt/2011/10outline.html

※3　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突いて、秘密情報（パスワードなど）を入手する方法。

【iii】ID／パスワードの使い回し

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／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／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／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／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。

実際に 2011 年 6 月に発生した、日本国内のインターネットバンキング不正利用の被害は、使い回しも含めた ID／パスワードの不適切な管理が、被害を大きくした原因の一つと考えられています。

（ご参考）

「国内のインターネットバンキングで不正アクセスが相次いでいる問題について」（IPA）

http://www.ipa.go.jp/security/topics/alert20110803.html

「パスワード ぼくだけ知ってる たからもの」（IPA）

http://www.ipa.go.jp/security/txt/2011/06outline.html

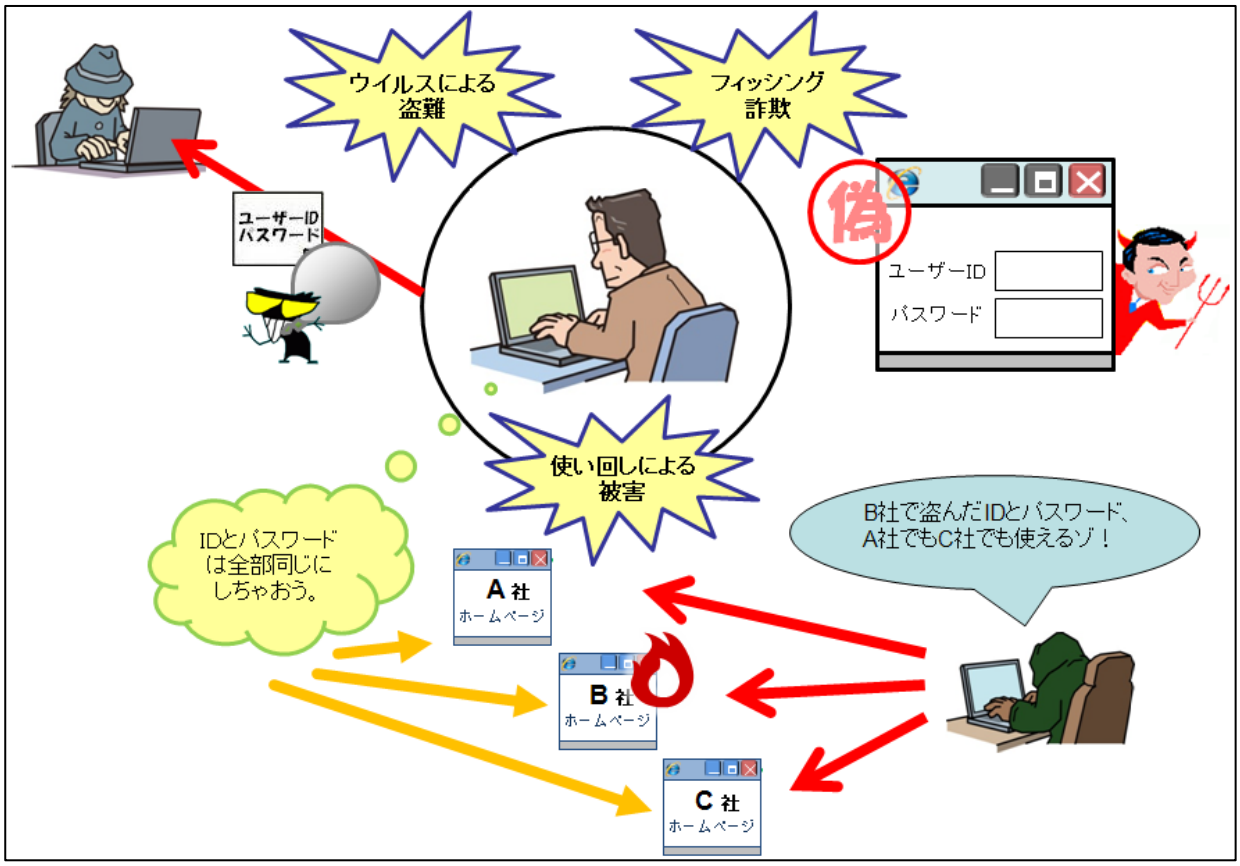

図 1-1.インターネットサービスが不正利用された原因のイメージ図

（3）対策

不正利用の被害に遭わないために、以下の対策をとるとともに、普段あまり利用していないインターネットサービスについても、ログインが可能かを定期的に確認することが重要です。**さらにその際、今後利用しないと思われるサービスに関しては登録解除することを勧めます。**

【i】基本的な対策

確実に行うべき基本的な対策は次の二つです。

●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ちながら使用する。

●使用しているパソコンの OS やアプリケーションなどの脆弱性を解消する。

最近では、“ドライブ・バイ・ダウンロード”攻撃などにより、正規のウェブサイトであっても、閲覧するだけでウイルスに感染する可能性があります。**単にウェブサイト閲覧時に気をつけるだけでは、ウイルス感染を防ぐことはできません。“ドライブ・バイ・ダウンロード”攻撃では、様々な脆弱性が悪用されるので、OS やアプリケーションなどの脆弱性を解消することは必須として、有害なウェブサイトの閲覧を防止する機能がある、統合型ウイルス対策ソフトを最新の状態で使用することが効果的です。**

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.html

【ii】メールは簡単に開かない・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、不用意に開いたり、メール本文に書いてあるリンクを安易にクリックしたりしないことが重要です。**また、知り合いからのメールであっても、少しでも不自然に思う箇所があれば警戒心をもち、安易に添付ファイルを開いたり、リンクをクリックしたりしないことが重要です。**

本当にその送信者が送ったメールなのかを確認をする際は、メールの中に書かれている連絡先ではなく、出来る限り自身で調べた連絡先に電話で確認することを勧めます。

【iii】フィッシング対策

フィッシング対策は、上述した【i】と【ii】の対策を行い、金融機関等から来たと思われるメールでも、内容を慎重に判断してください。

メールや電話で、「システムに問題が発生したため、パスワードを送ってください」など、もっともらしい口実の問い合わせがあったとしても、パスワードを他人に教えてはいけません。**パスワードは、本人しか知らないという前提のもと、本人確認に利用されるものです。たとえオンラインサービスの提供会社やシステム管理者であっても、パスワードを聞いてくることはありません。**

【iv】ID／パスワードの適切な管理と利用ウェブサイトの確認

ID／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／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**…記憶するのが大変なパスワードの場合は、紙にメモしても構わないが、その際、ID とパスワードは別々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。ワンタイムパスワードなど（二要素認証、二段階認証等）を採用しているサービスを利用する。

普段利用していないインターネットサービスを放置していると、時間をかけてパスワードを破られる危険性が高まります。そうしたサービスへのログインが可能かの確認を、定期的に行ってください。

【v】不正利用の被害に遭ってしまったら

もし、インターネットサービスに登録してあるクレジットカードの明細書に身に覚えのない請求があるなど、不正利用の被害に遭ってしまったら、直ちにクレジットカード会社とインターネットサービス事業者に不当な請求であることを報告し、対応を求める事をお勧めします。また、このとき消費生活センターに相談することも有効です。場合によっては、警察に被害状況を申告するように指示されることもありますので、その際は最寄りの警察署に対処方法などを相談してください。

（ご参考）

全国の消費生活センター等（国民生活センター）

http://www.kokusen.go.jp/map/

都道府県警察本部のサイバー犯罪相談窓口等一覧

http://www.npa.go.jp/cyber/soudan.htm

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）

・サーバーの設定不備の悪用により侵入され、ファイルを改ざんされた

・オンラインショップに勝手にログインされて、身に覚えのない料金を請求された

○ 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）

・なるべくお金をかけずにパソコンのウイルス対策を実施したい

・企業のウェブサイトを閲覧してウイルス感染してしまった

○ 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

11 月のウイルスの検出数※1 は、**20,585 個**と、10 月の 20,409 個から 0.9%の増加となりました。また、11 月の届出件数※2 は、**1,115 件**となり、10 月の 795 件から 40.3%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 20,585 個を集約した結果、1,115 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で **10,425 個**、2 位は **W32/Mydoom** で **6,996 個**、3 位は **W32/Downad** で **738 個**でした。

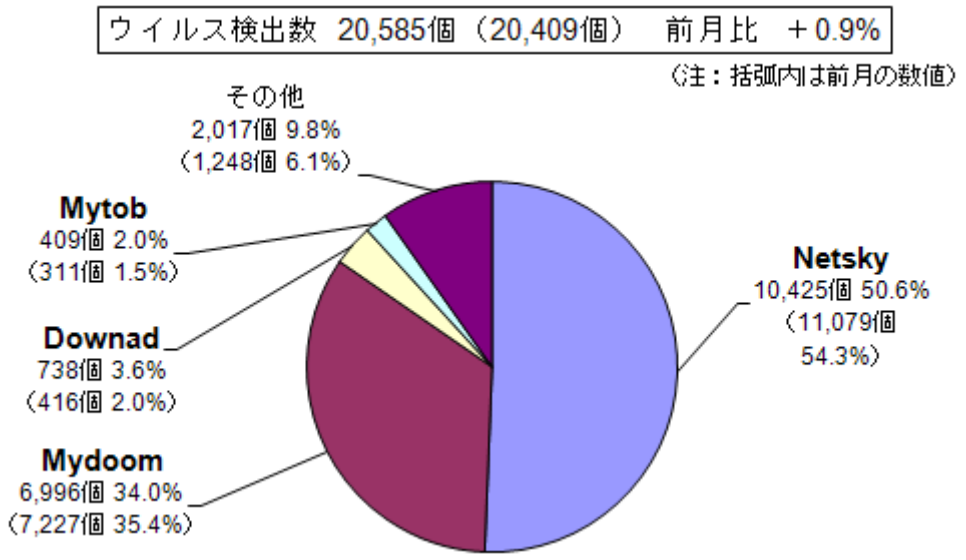

図 2-1：ウイルス検出数

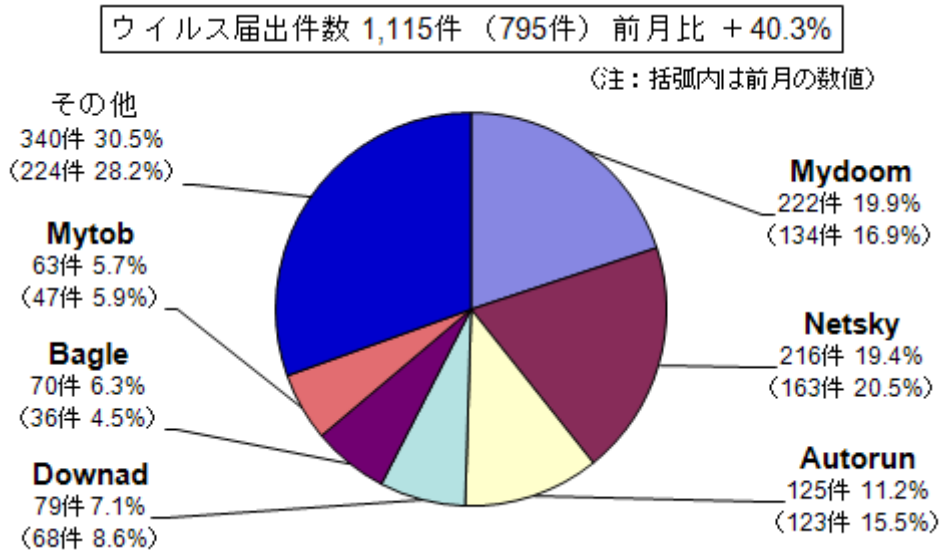

図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

11 月は、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が増加傾向となりました。また、9 月に大幅に増加した RLTRAP は、11 月前半に 2 日だけ多く検知された日がありました（図 2-3 参照）。

※.ここでいう「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

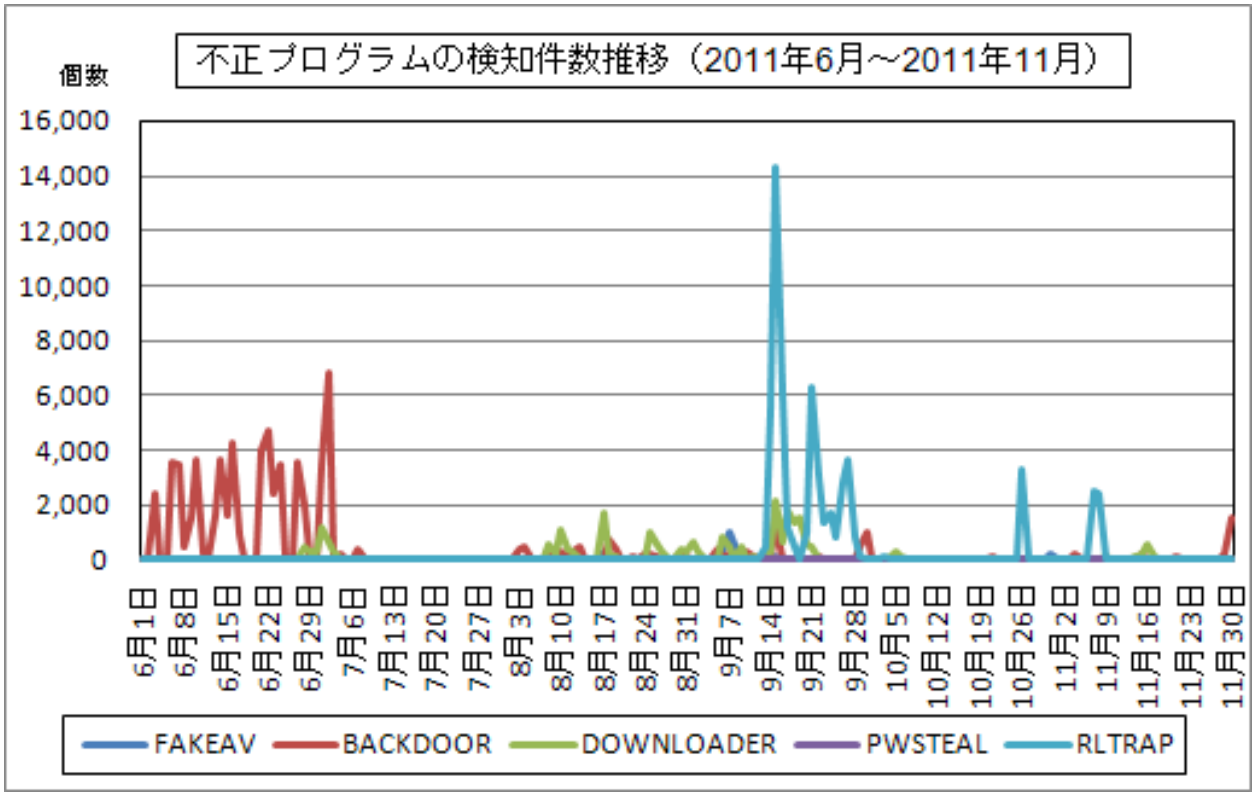

図 2-3：不正プログラムの検知件数推移

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

		6月	7月	8月	9月	10月	11月
届出[a] 計		**9**	**8**	**10**	**7**	**15**	**7**
	被害あり[b]	9	5	8	5	8	5
	被害なし[c]	0	3	2	2	7	2
相談[d] 計		**32**	**47**	**37**	**31**	**46**	**69**
	被害あり[e]	7	15	13	8	7	14
	被害なし[f]	25	32	24	23	39	55
合計[a+d]		**41**	**55**	**47**	**38**	**61**	**76**
	被害あり[b+e]	16	20	21	13	15	19
	被害なし[c+f]	25	35	26	25	46	57

（1）不正アクセス届出状況

11 月の届出件数は 7 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69件であり､そのうち何らかの被害のあった件数は14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 2 件、DoS 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踏み台として悪用されていたものが 1 件、サーバーの設定不備の悪用によりサーバー内の構成ファイルを改ざんされたものが 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ていたものが 1 件、オンラインショッピングに第三者にログインされ、サービスを勝手に利用されていたものが 1 件、でした。

（4）被害事例

［侵入］

（i）サーバーの設定不備の悪用により侵入され、ファイルを改ざんされた

事例	・レンタルサーバー業者から「御社サイト内のあるディレクトリに、改ざんが原因と思われる不正なファイルが存在する」との連絡が入った。 ・パソコンのブラウザから、当社ウェブサイトの当該ディレクトリにアクセスすると、強制的に別サイトに移動させられる状態になっていた。 ・即座に該当ディレクトリを書き込み禁止に設定し、本当に不要であることを確認した後、ディレクトリを削除した。 ・前回のサイト更新時の作業ミスにより、不要ディレクトリが削除されずに残ってしまっていた。結果として該当ディレクトリが管理対象外となってしまい、適切なディレクトリ設定が実施されていなかった。

解説・対策	削除すべきディレクトリが残ったまま放置されていたことが原因でした。セキュリティ対策を実施したつもりでも、書き込み可能なディレクトリが一つ残っているだけで、ディレクトリ内のファイルを改ざんされたり、さらには踏み台として外部サーバーの攻撃に不正使用される恐れもあります。 使われなくなったディレクトリ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。**定期的にサーバー内のディレクトリ構成を確認**することを勧めます。平行して、**サーバーで動作させる機能やサービスについても定期的に確認**すると良いでしょう。 （ご参考） IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html

［なりすまし］

（ii）オンラインショップに勝手にログインされて、身に覚えのない料金を請求された

事例	・チケット販売専門のオンラインショップを利用している。ある日突然、身に覚えの無いチケットの申込完了メールが届いた。 ・支払い方法をクレジットカードではなくコンビニ支払いにしていたので、すぐに代金が引き落とされる訳ではないが、支払わないとキャンセルではなく、料金滞納扱いになる可能性があるとのこと。 ・ショップ側には身に覚えの無い旨を連絡し、ショップ利用時のログインパスワードを変更した。 ・なぜ勝手になりすましログインをされたのか、原因は分からない。
解説・対策	不正利用の発覚直後に対処したことにより、その後の被害拡大を防げた例です。不正利用発覚後はすぐにショップに連絡して、ログインパスワードを変更してください。もしアカウントが完全に乗っ取られてパスワード変更すら出来なくなってしまった場合も、ショップに連絡してください。本人確認後にアカウントを取り戻すことができる場合があります。 本件の原因は不明ですが、パスワードが単純だったために第三者に推測されてなりすましログインをされた可能性があります。**パスワードは複雑な文字列にし、複数のオンラインサービスを利用する場合はそれぞれ別のパスワードにすること**を勧めます。 （ご参考） IPA – 6 月の呼びかけ「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

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 **1,420 件**でした。そのうち**『ワンクリック請求』に関する相談**が **418 件**（10 月：419 件）、**『偽セキュリティソフト』**に関する相談が **11 件**（10 月：7 件）、**Winny に関連する相談**が **35 件**（10 月：12 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**（10 月：9 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		1,692	1,490	1,651	1,551	1,496	1,420
	自動応答システム	999	889	958	936	865	746
	電話	639	540	639	554	564	561
	電子メール	50	54	50	52	55	102
	その他	4	7	4	9	12	11

※ 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。

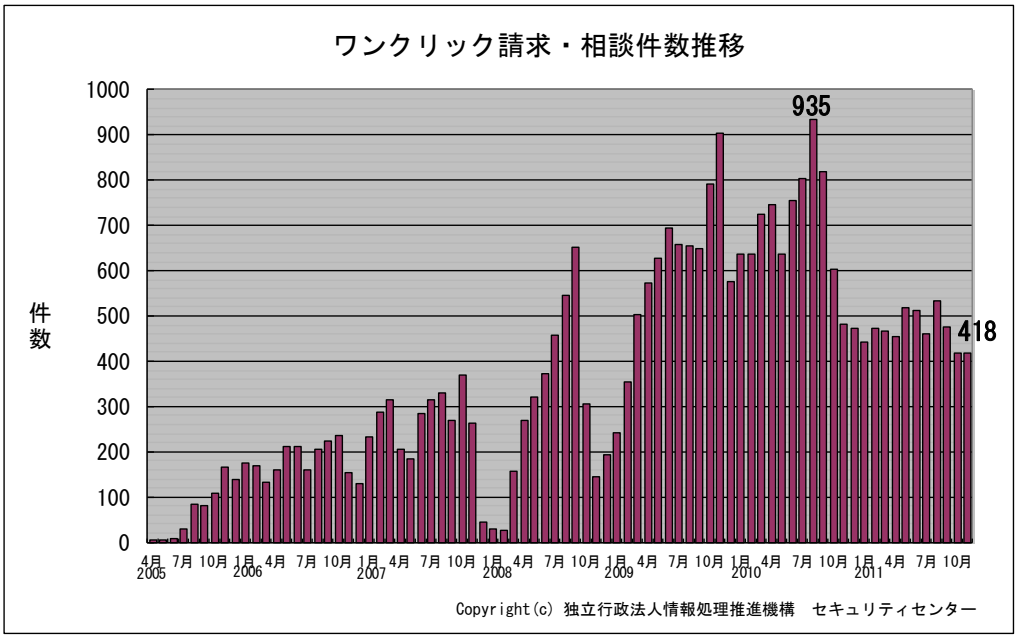

図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）なるべくお金をかけずにパソコンのウイルス対策を実施したい

相談	自宅でパソコンを使い始めたが、経済的にあまり余裕がないので、ウイルス対策にはなるべくお金をかけたくない。 どうしたらなるべくお金をかけずにウイルス対策を実施できるか。
回答	ウイルス対策ソフトには無料のものと有料のものがあります。 **無料のものは費用がかかりませんが、使用方法が分かりづらい、基本的にサポートがないなど、初心者には不向きと言えます**。また、インターネットから入手できるものの中には、**偽物のウイルス対策ソフトも存在するため、非常に危険です**。 有料のものは、最初に購入代金がかかり、契約更新時に更新料がかかるものがほとんどです。しかし、その分メーカーのサポートがあり、ウイルス対策だけでなく、総合的なセキュリティ対策ができるものが多いです。利用するソフトの選択に悩む場合は、パソコンショップなどの店頭で店員に相談してください。

（ii）企業のウェブサイトを閲覧してウイルス感染してしまった

相談	ある企業のウェブサイトにアクセスしたところ、突然ブラウザが強制終了してしまい、再度起動してもすぐにフリーズしてしまうようになった。 ウイルス対策ソフトを入れていなかったので、ウイルスに感染してしまったのか。
回答	当該企業のウェブサイトが改ざんされて、アクセスしたパソコンにウイルスを感染させる仕掛けが埋め込まれていた可能性が高いです。 ウイルス対策ソフトを入れていれば、感染を防げた可能性がありますので、今後は**ウイルス対策ソフトを最新の状態に保って使うことをお勧めします**。また、**OS やアプリケーションの脆弱性を解消しておくことも、今回のようなウイルス感染を防ぐための重要な対策になります**。 （ご参考） IPA-2010 年 5 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!」 http://www.ipa.go.jp/security/txt/2010/12outline.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、2011 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 **86,568 件**、延べ発信元数※は **36,259 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 120 の発信元から 288 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。

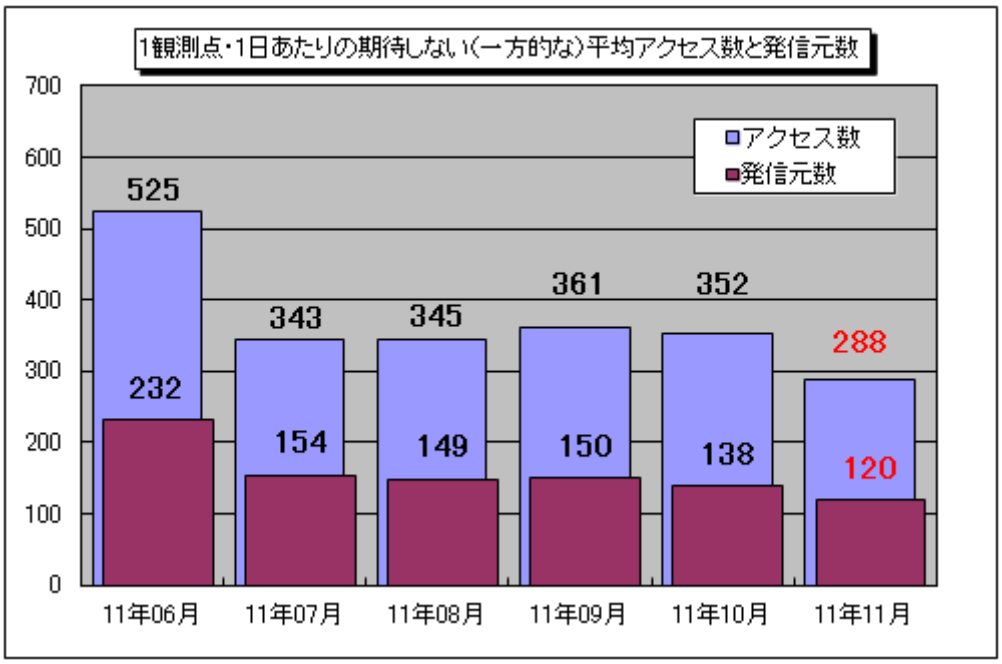

図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数

上記グラフは 2011 年 6 月～2011 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示しています。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。これを見ると TOP10 以外のポートへのアクセスが大幅に減少しましたが、それ以外でアクセス数が大きく変化したポートはありませんでした。

しかし、前月までは TOP10 に挙がってこなかった 8909/tcp へのアクセスが、中国および、アメリカを中心に 2011 年 8 月以降、徐々に増加傾向を示していました（図 5-3 参照）。

8909/tcp は、ある中国の動画共有サイトの動画ダウンロードソフトの通信ポートとして利用されており、このソフトをパソコンにインストールして特定の条件下で使用すると、そのパソコンが公開プロキシサーバーとして動作しまうことが確認されています。悪意ある者がこのソフトがインストールされたパソコンを踏み台としてウェブサーバ等への攻撃に使うために、このソフトがインストールされたパソコンを探索していたものだった可能性があります。

（ご参考）

8909/TCP に対するアクセスの増加について（警察庁）

http://www.npa.go.jp/cyberpolice/detect/pdf/20110905.pdf

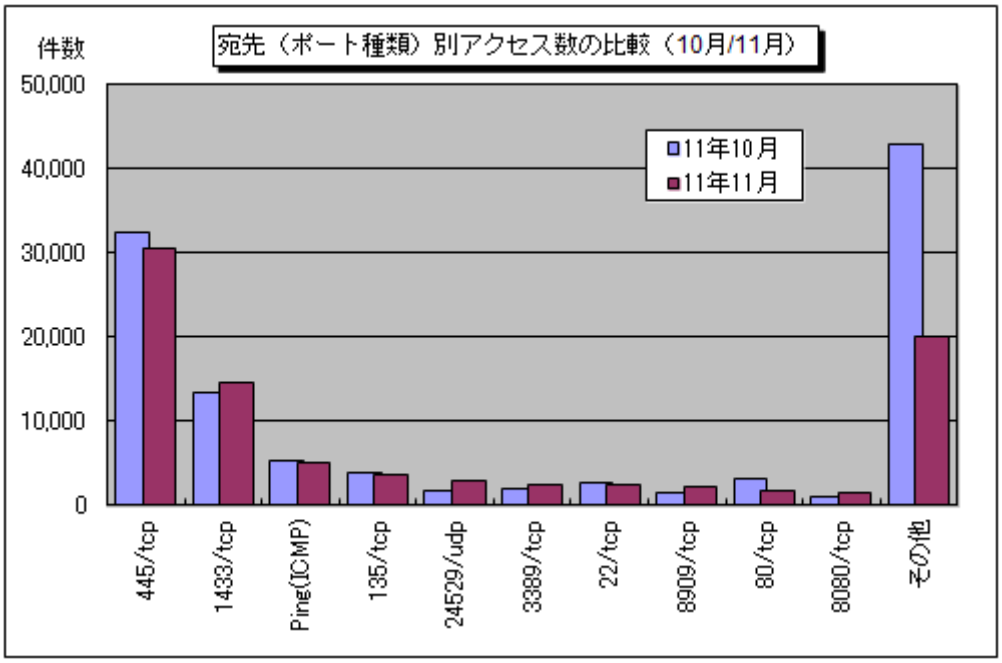

図 5-2：宛先（ポート種類）別アクセス数の比較（10 月/11 月）

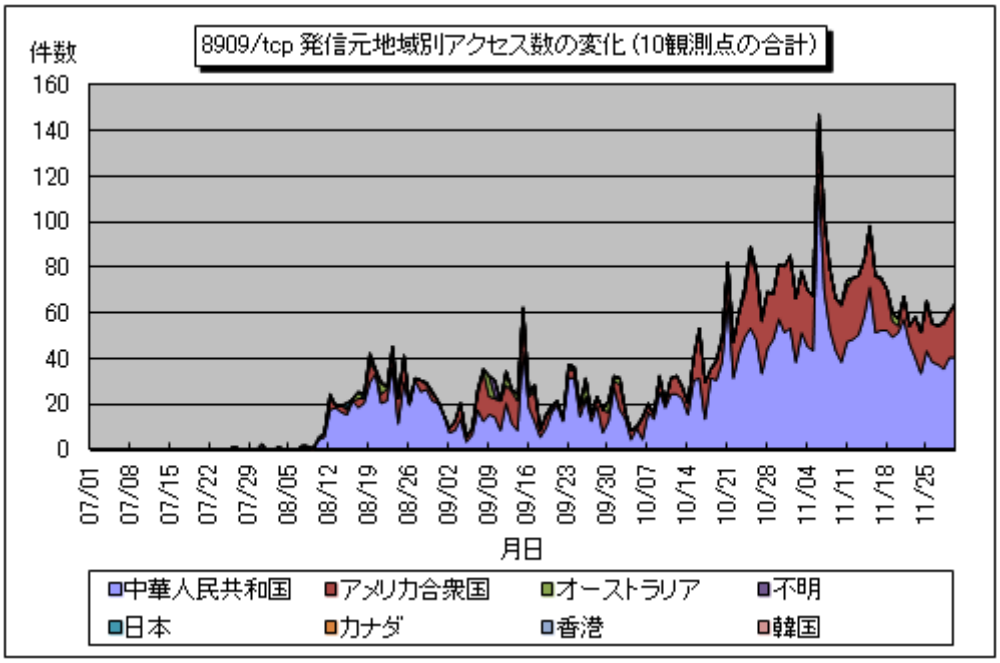

図 5-3：8909/tcp 発信元地域別アクセス数の変化（10 観測点の合計）

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/TALOT2-1112.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