Information-technology
Promotion
Agency, Japan

プレスリリース
第 11-33-231 号
2011 年 10 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 9 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 9 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

「 ウイルスを使った新しいフィッシング詐欺に注意！ 」

先月の呼びかけでは、SpyEye ウイルスによるインターネットバンキングでの不正利用事件を取り上げました。その SpyEye ウイルスはキーボードで入力した内容を盗むウイルスでしたが、IPA では 2011 年 9 月、異なる手口でインターネットバンキングのログイン情報を盗む事例を確認しました。

その手口は、既存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手法です。銀行を装った偽のメールにウイルスが添付されており、ウイルスを実行するとログイン情報や乱数表の内容の入力を促す画面が現れ、メールの指示に従って入力してしまうと悪意ある者にその情報が渡ってしまう、というものです。実際にこの手口により銀行口座から総額数百万円を引き出される被害が発生しています。

IPA では実際の偽メールを入手しウイルスを解析しました。その解析結果から、ウイルスの概要と、実行されるとどのような動作をするのかを示すとともに、被害に遭わないための対策を紹介します。

（1）フィッシングとは？

フィッシング（Phishing）とは、金融機関（銀行やクレジットカード会社）などを装ったメールを送り、電子メールの受信者に偽のウェブサイトにアクセスするよう仕向け、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を詐取する行為のことをいいます。

以下に、典型的なフィッシング被害の一例を説明します（図 1-1 参照）。

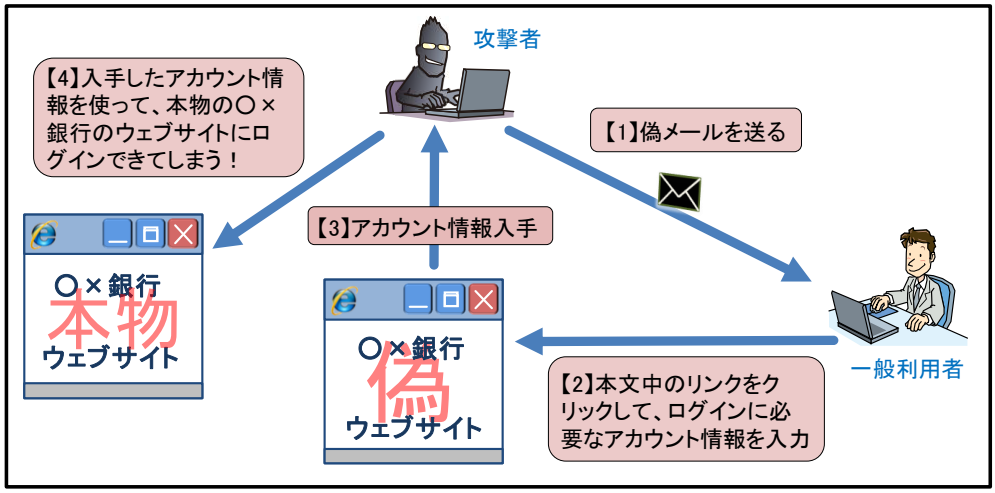

図 1-1：フィッシング被害の一連の流れのイメージ図

【1】攻撃者が偽メールを送信

攻撃者が、正規のウェブサービスや金融機関など実在する会社を装ったメールを無差別に送信します。

【2】利用者がメール本文中のリンクをクリック

メール受信者が、そのメールを信用してメール本文中の URL をクリックすると、事前に用

意された偽のウェブサイトに誘導されます。

【3】攻撃者がログイン情報を入手

偽のウェブサイトと気付かずにログイン情報（ID やパスワードなど）を入力してしまうと、そのアカウント情報が攻撃者に渡ってしまいます。

【4】攻撃者が実際のウェブサイトにログイン

攻撃者は、入手したログイン情報を使い、利用者になりすまして本物のウェブサイトにログインします。

（2）ウイルスを使った新しいフィッシング手口の概要

以下に、IPA で確認したウイルスの挙動と一連の手口を解説します。

【1】きっかけとなるメール（フィッシングメール）

国内の大手銀行を装った文面で、ウイルスが添付されたメールです（図 1-2 参照）。

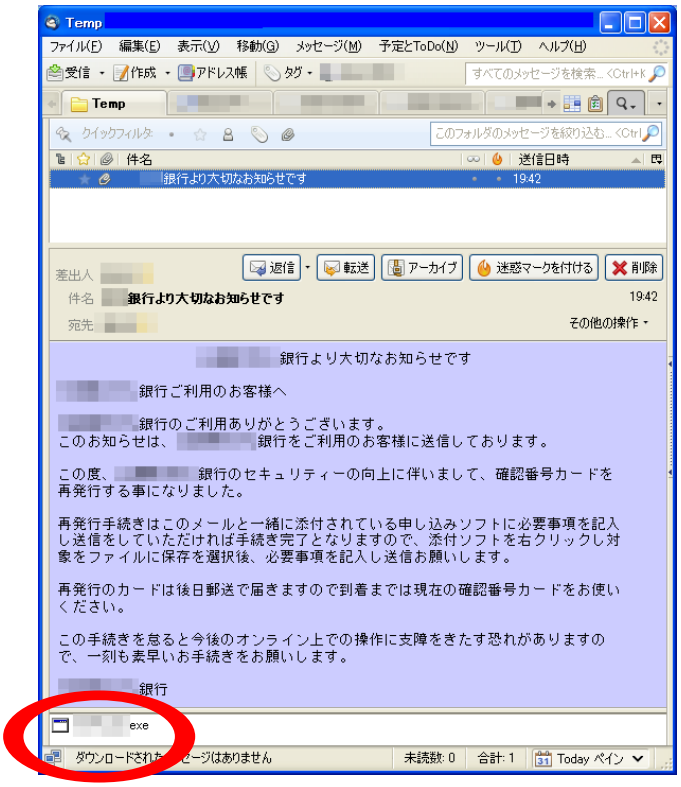

図 1-2：メール本文例

該当メールの添付ファイルを調査した結果、「Banker」や「Jginko」と呼ばれるウイルスの一種でした。アイコンの見た目が実在する銀行のロゴマークと同じもので、これは受信者がついクリックしてしまう効果を狙っていると思われます（図 1-3 参照）。

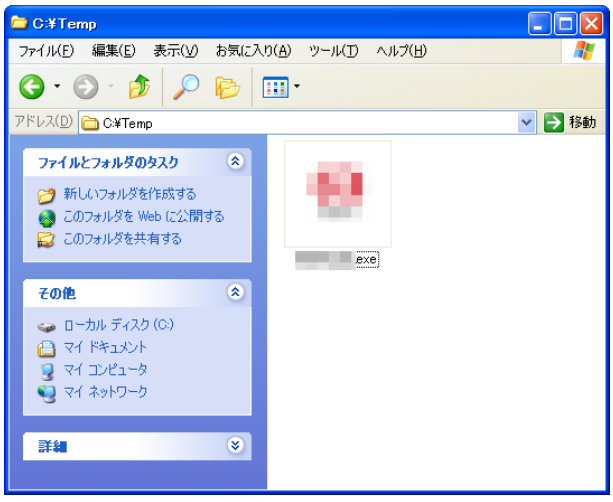

図 1-3：ウイルスのアイコンを表示したイメージ

【2】ログイン情報入力画面

メールの文面に従い、添付ファイルを開くと、送金手続きの際などに必要な契約者番号やパスワード、乱数表の情報全てを入力するように促す画面が現れます（図 1-4 参照）。**通常、このような依頼がメールで来ることはあり得ません。**

図 1-4：情報入力を促す画面のイメージ（表示内容はウイルスによって異なります）

【3】ログイン情報を送信

情報を入力し「送信」ボタンをクリックすると、外部のサーバーに、情報入力済みの画面を画像データとして送信しようとします。

外部サーバーへの接続に失敗した場合には、文字化けしたメッセージが表示されます。日本語環境で文字化けするこの文字列は、中国語簡体字として表示すると「连接失败」となり、これは「接続の失敗」を意味します。このことから、このウイルスは中国語を理解する人物によって作成された可能性があります。

図 1-5：接続失敗時のエラーと思われるメッセージ

【4】悪意ある者がログイン可能に

結果的に、契約者番号、複数のパスワード、乱数表に書かれた全ての情報が相手に知られるため、これらのアカウント情報を基に、悪意ある者がインターネットバンキングサイトにログインし、送金手続きなどをすることが可能になります。

（3）対策

従来のフィッシングの手口では、悪意ある者が偽のウェブサイトを開設し、その上で利用者を偽サイトに誘導する必要がありましたが、今回のケースでは、メールの添付ファイルそのものにアカウント情

報を入力させる仕掛けが施されており、仕組みとしては単純といえます。
単純であるが故に、基本的な対策を確実に実施することが大切です。

【i】フィッシング対策

① メールの真偽の確認

金融機関等から来たと思われるメールでも、内容を慎重に確認してください。そもそも**カード番号や暗証番号を入力するような依頼がメールで届くことはありません**。もしそのようなメールが金融機関等から届いた場合は、送信元に電話で問い合わせたり、ウェブサイトのお知らせ欄を見たりして、その情報（メール）の真偽を確認してください。電話で問い合わせをする時は、メール本文に記載されている連絡先ではなく、口座開設時に送付された書類を見る等、正しいと確証が持てる連絡先に電話してください。

② メール記載のリンクに注意

メール本文内にあるリンク先に不用意にアクセスしないことも重要です。当該銀行等のウェブサイトを確認する場合は、メール中のリンクからアクセスするのではなく、ブラウザの「お気に入り」や「ブックマーク」に正しいアドレスを登録しておき、常にそちらからアクセスすることを勧めます。

（ご参考）
フィッシング対策協議会
http://www.antiphishing.jp/

【ii】ウイルス対策

① 添付ファイルの取扱い

メールに添付ファイルがあった場合は、常にウイルスの可能性を疑ってください。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うメールであれば、相手に確認を取るか、メールそのものを読まずに削除してください。

② ウイルス対策ソフトの活用

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。前述の事例におけるウイルスについても、ウイルス対策ソフトが導入済であればメール受信時や添付ファイル保存時、またはファイルを開く際にウイルスとして検出することができます。

【iii】事後対応

万一、インターネットバンキングの不正利用の被害に遭ってしまった場合は、当該銀行への問い合わせをしてください。多くの銀行では、ウェブサイトのトップページから問い合わせができるようになっています。さらに、ウイルスに感染していない、自分自身が管理している安全なパソコンから、インターネットバンキングで使用しているパスワードを変更してください。**今回紹介した「Banker」や「Jginko」のように乱数表を入力するタイプのフィッシング詐欺に遭ってしまった場合は、乱数表の内容を既に知られてしまっているので、乱数表カードの交換や、口座を開設し直す、といった対処が必要です。**

なお、ID やパスワードの管理が本質的な対策の一つですので、それに関しては、2011 年 6 月の呼びかけを参照してください。

（ご参考）
IPA - 2011 年 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

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）
- ・SQL インジェクション攻撃でログイン情報などを盗まれた
- ・オンラインゲームのアカウントが乗っ取られた

○ 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）
- ・楽天のサービスで不正アクセスの被害にあった
- ・以前、入れていたファイル共有ソフトによって情報漏えいがあったか心配している

○ 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

9 月のウイルスの検出数※1 は、**21,291 個**と、8 月の 25,143 個から 15.3%の減少となりました。また、9 月の届出件数※2 は、**906 件**となり、8 月の 931 件から 2.7%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。
・9 月は、寄せられたウイルス検出数 21,291 個を集約した結果、906 件の届出件数となっています。

検出数の 1 位は、**W32/Mydoom** で **9,525 個**、2 位は **W32/Netsky** で **9,194 個**、3 位は **W32/Autorun** で **553 個**でした。

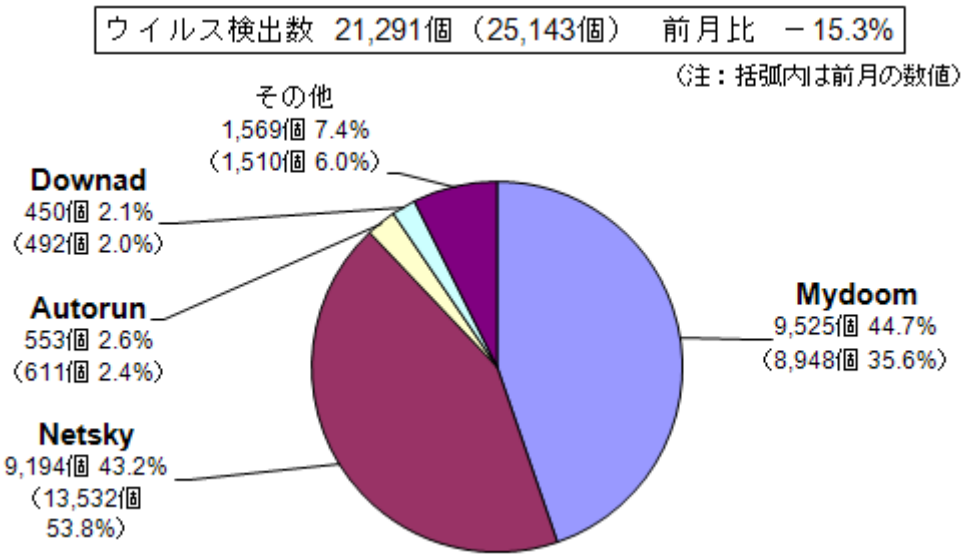

図 2-1：ウイルス検出数

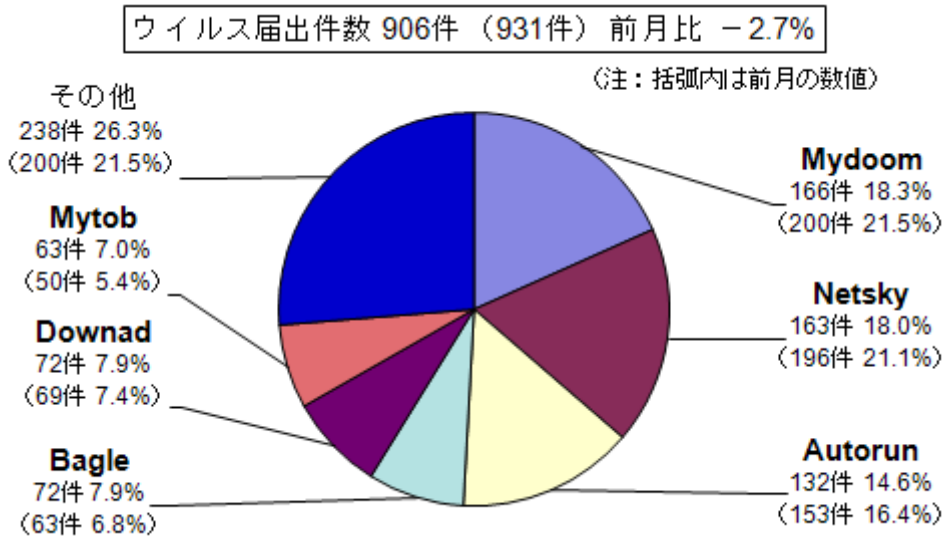

図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

9 月は、別のウイルスを感染させようとする DOWNLOADER といった不正プログラムが増加傾向となりました。また、RLTRAP という不正プログラムが 9 月に入ってから大幅に増加しました（図 2-3 参照）。RLTRAP は、利用者がファイルの拡張子を誤認してしまうように、ファイル名に細工を施された不正プログラムの一般名と思われます。

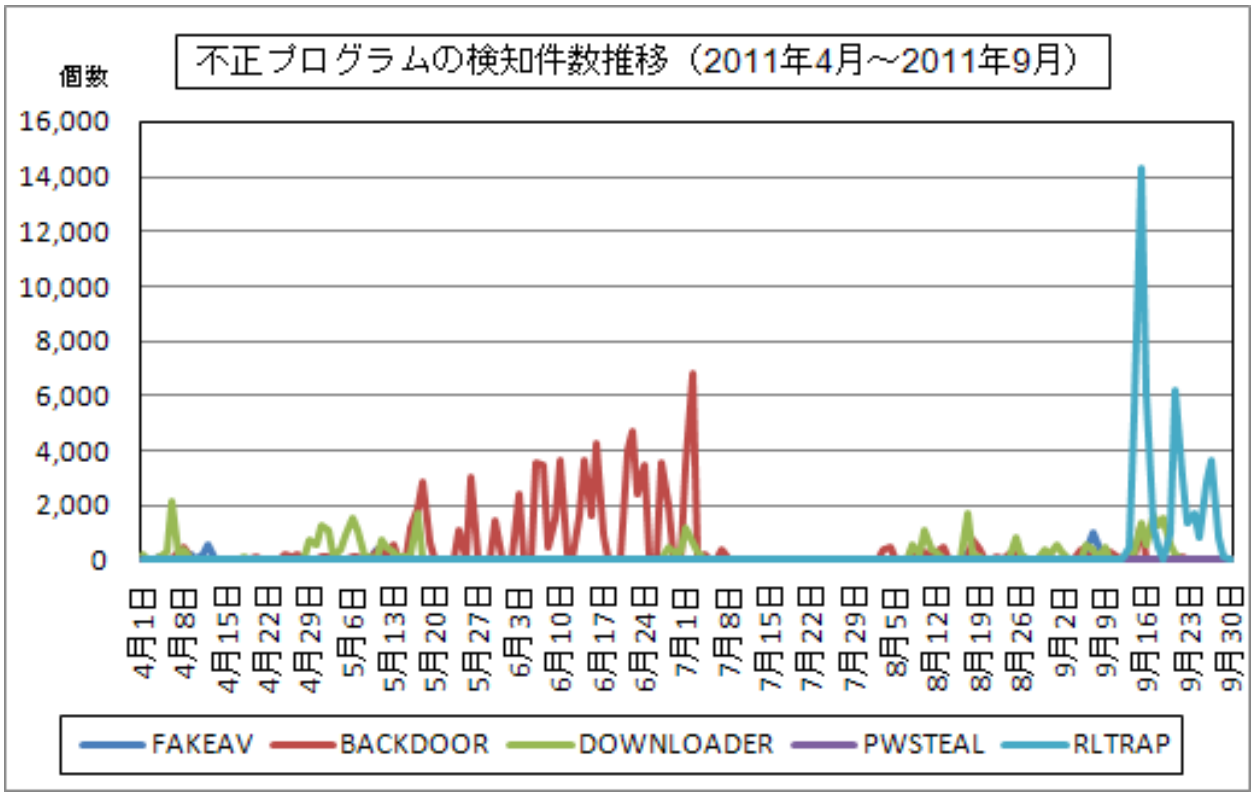

図 2-3：不正プログラムの検知件数推移

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

		4月	5月	6月	7月	8月	9月
届出(a)　計		5	7	9	8	10	7
	被害あり(b)	5	6	9	5	8	5
	被害なし(c)	0	1	0	3	2	2
相談(d)　計		38	55	32	47	37	31
	被害あり(e)	10	14	7	15	13	8
	被害なし(f)	28	41	25	32	24	23
合計(a+d)		43	62	41	55	47	38
	被害あり(b+e)	15	20	16	20	21	13
	被害なし(c+f)	28	42	25	35	26	25

（1）不正アクセス届出状況

９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31件であり､そのうち何らかの被害のあった件数は８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、データベースからログイン情報等が盗まれたものが１件、でした。侵入の原因は、ウェブアプリケーションの脆弱性を突かれたものが１件でした（他は原因不明）。

「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（オンラインゲーム３件）、でした。

（4）被害事例

［侵入］

（i）SQL インジェクション攻撃でログイン情報などを盗まれた

事例	・公開しているウェブサイトのレスポンスが異常に遅いので調査したところ、不正アクセスの痕跡を見つけた。 ・アクセスログを詳しく解析したところ、不正アクセスの原因は SQL インジェクション攻撃と判明。 ・攻撃を受けた箇所は２年前に対策済だったが、ページ更新時にソースのデグレード※が発生してしまい、結果として該当箇所のみ対策されていない状態となり、そこを突かれて攻撃されてしまった。

解説・対策	対策済であったにも関わらず、ソースのデグレードにより問題が再発してしまった例です。 脆弱性の解消は、出来る限り行うのはもちろんですが、意図しない事故や人為的ミスに備えた多段防御として、WAF（Web Application Firewall）導入によるウェブサイト全体のセキュリティ強化も有効な対策になります。 （参考） 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/ IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html IPA - Web Application Firewall 読本 http://www.ipa.go.jp/security/vuln/waf.html

デグレード※：プログラム修正時に、修正部分以外の箇所が以前の状態に戻ってしまうこと。

［なりすまし］

（ii）オンラインゲームのアカウントが乗っ取られた

事例	・ゲーム内で「ゲームで使えるお金をあげる」と言われたので、その相手にパスワードを教えたところ、後日ログインできなくなった。 ・その相手がログイン後にパスワードを変更したと考えられる。 ・こうしたなりすまし行為は、警察に被害届けを出すと受理してくれるのか？
解説・対策	パスワードを他人に教えてしまったことで、アカウントを奪われ、さらにパスワード等の登録情報までもが変更されてしまいました。**たとえ親しい友人であっても、パスワードは絶対に教えてはいけません。**パスワードを自分から教えてしまうと、不正アクセス禁止法の適用外となる可能性もあります。 パスワードを自分から教えなくても、SNS（ソーシャルネットワーキングサービス）などのアカウント情報と同じものを使っていると、そうしたサービスの自己紹介などから推測される可能性があります。面倒でも、サービスごとに異なるパスワードを設定することを勧めます。 **被害届けの提出は、ゲーム運営業者側で行うことになりますので、まずはゲーム運営業者に問い合わせをしてください。**場合によっては、警察に被害状況を申告するようにゲーム運営業者から指示されることもありますので、その際には最寄りの警察署に対処方法について相談してください。なお、ゲーム運営業者に問い合わせても、あまり良い対応を行ってもらえない場合、最寄りの消費生活センターに相談することをお勧めします。 （参考） IPA - 「オンラインゲームを楽しむ前にチェックしておきたい 3 つのセキュリティポイント」 http://www.ipa.go.jp/security/personal/onlinegame/ 「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/ 警察庁 - インターネット安全・安心相談 http://www.npa.go.jp/cybersafety/

4. 相談受付状況

9 月のウイルス・不正アクセス関連相談総件数は **1,551 件**でした。そのうち**『ワンクリック請求』に関する相談**が **477 件**（8 月：535 件）、**『偽セキュリティソフト』**に関する相談が **2 件**（8 月：7 件）、**Winny に関連する相談**が **19 件**（8 月：7 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**（8 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

		4月	5月	6月	7月	8月	9月
合計		1,608	1,640	1,692	1,490	1,651	1,551
	自動応答システム	997	950	999	889	958	936
	電話	555	620	639	540	639	554
	電子メール	50	62	50	54	50	52
	その他	6	8	4	7	4	9

※ 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。

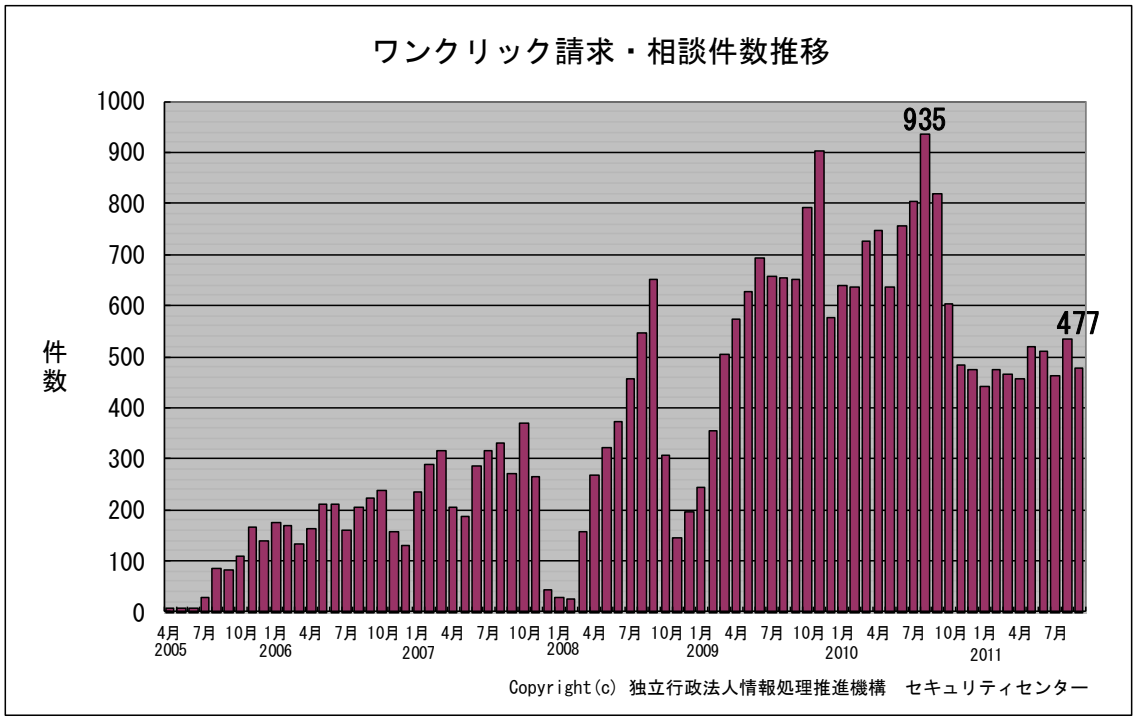

図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）楽天のサービスで不正アクセスの被害にあった

相談	楽天のサービスを利用しているが、心当たりのない決済がされていることに気付いた。ログインの際のパスワードを破られて不正アクセスされた可能性が高い。このような被害に遭った場合、どういった行動をとればいいか分からない。 （このほか、同様の事例が 3 件）
回答	**まずは早急に今回の件を楽天側に連絡してください**。以下に紹介した楽天のページに、サービス毎の連絡先情報が書かれています。 また、今後同じような被害に遭わないために、パスワードのセキュリティ対策を見直すことをお勧めします。 （ご参考） 楽天サービスにおける不正利用への対策【末尾に連絡先情報あり】 http://corp.rakuten.co.jp/security/knowledge/answer.html IPA-2011 年 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

（ii）以前、入れていたファイル共有ソフトによって情報漏えいがあったか心配している

相談	以前、ファイル共有ソフトを使ってみようとパソコンに入れたことがある。しかし、設定がうまくいかず、結局使用するには至らなかった。この状況でパソコンから情報漏えいが起こりえたか心配している。また、パソコンにファイル共有ソフトが残っていないかも心配している。確認する方法はないか。
回答	ファイル共有ソフトを使用するには至らなかったということは、ファイル共有ソフトのネットワークに接続できていないので、**情報漏えいの心配はありません**。 また、IPA が提供している「情報漏えい対策ツール」を活用することで、パソコンにファイル共有ソフトが残っていないか確認することができます。ご利用を希望される場合は、以下のページから申し込みを行ってください。 （ご参考） IPA-「情報漏えい対策ツール」 http://www.ipa.go.jp/security/winny119/

5. インターネット定点観測での 9 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 9 月の期待しない（一方的な）アクセスの総数は 10 観測点で **108,576 件**、延べ発信元数※は **45,285 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 150 の発信元から 361 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。

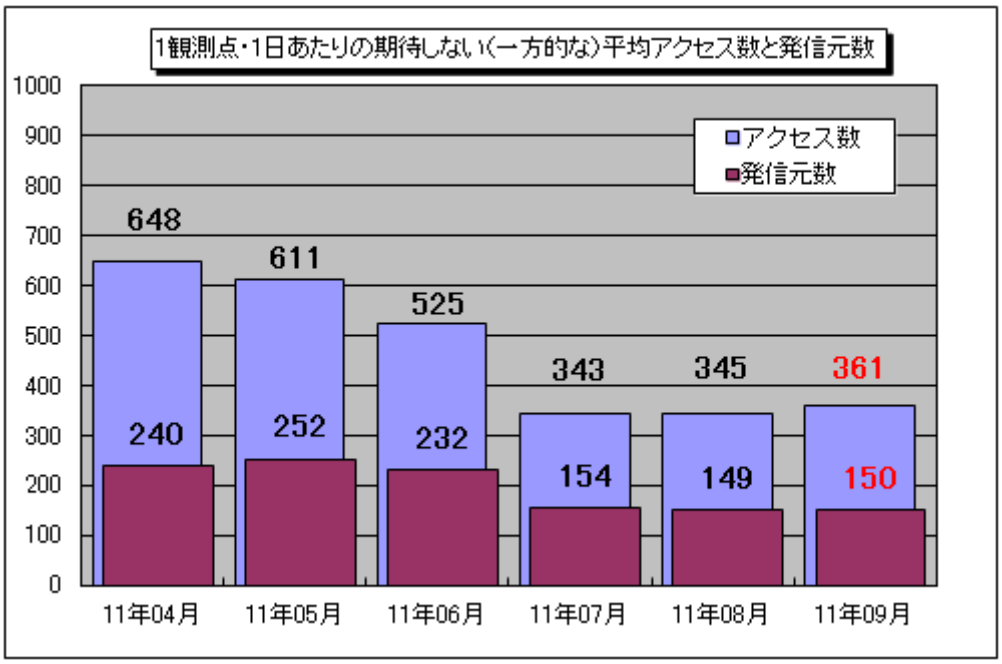

図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数

上記グラフは 2011 年 4 月～2011 年 9 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。9 月の期待しない（一方的な）アクセスは、8 月と比べてやや増加しました。

8 月と 9 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。これを見ると各ポートへのアクセス数において、8 月と比べてそれほど目立った変化はありませんでしたが、2011 年 9 月のレポートで 8 月の後半に増加が観測されたと報告しました 3389/tcp へのアクセスは、その後一時的に減少したのち、再び増加傾向を示しました（図 5-3 参照）。

3389/tcp は、主に RDP※1 で使用されるポートであり、このポートを悪用して Windows 端末に感染を広げる「Morto※2」と呼ばれるウイルスが 2011 年 8 月に見つかっているため、このアクセスがウイルスの感染活動によるものだった可能性があります。

IPA へのウイルス届出状況において、現時点で「Morto」に関する届出はありませんが、Windows 上でリモートデスクトップなどの機能を使用している方は、ウイルスの感染被害に遭わないために、ウイルス対策を再確認するとともに、ログインの際のパスワードを強化するなどの対策を行うことをお勧めします。

※1 RDP（Remote Desktop Protocol）：遠隔で Windows 端末の操作ができるリモートデスクトップ機能などで使われるプロトコルのこと。

※2 Morto：RDP を悪用して Windows 端末に感染するウイルスの一種。感染すると 3389/tcp にポートスキャンを行いリモートデスクトップ機能が有効な端末を探索し、発見した端末に対してパスワードクラッキングを試みる。

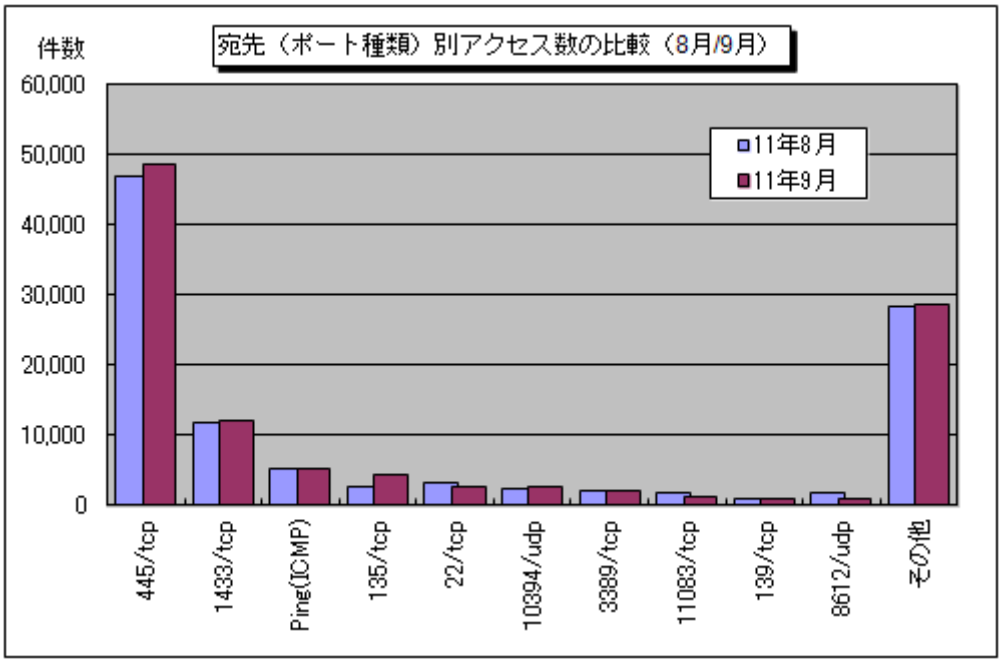

図 5-2：宛先（ポート種類）別アクセス数の比較（8 月/9 月）

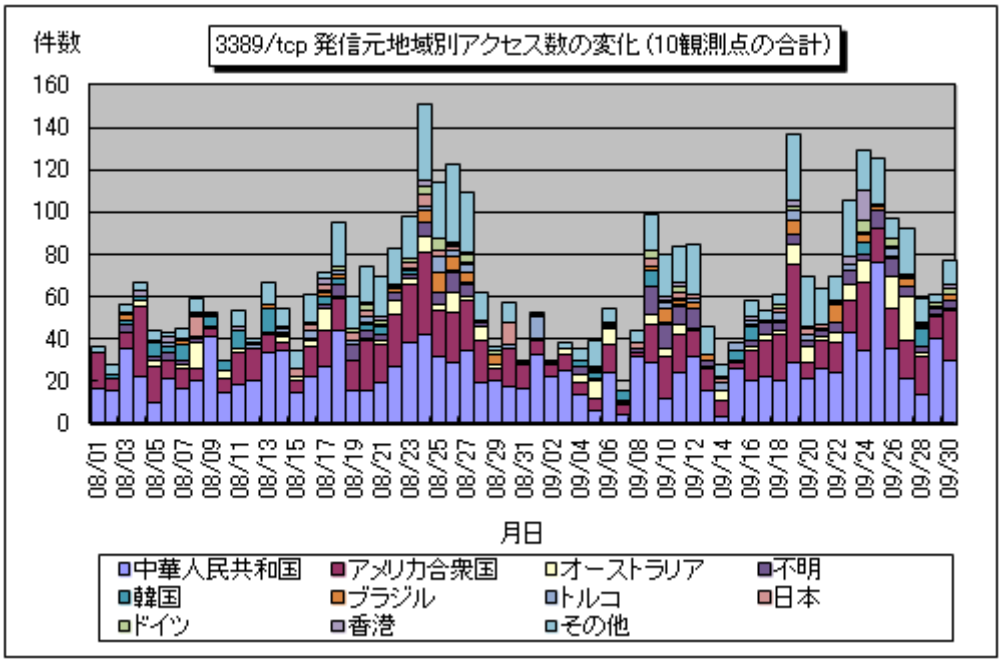

図 5-3：3389/tcp 発信元地域別アクセス数の変化（10 観測点の合計）

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/TALOT2-1110.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