Information-technology
Promotion
Agency, Japan

プレスリリース
第 11-21-220 号
2011 年 6 月 3 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 5 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 5 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

「 パスワード　ぼくだけ知ってる　たからもの ※1 」

※1　第6回IPA情報セキュリティ標語・ポスターコンクール(2010年度実施)標語部門
大賞 坂井 敏法 さん(新潟県 新潟市立万代長嶺小学校)

今年 4 月から 5 月にかけて、1 億件を超える ID やパスワードを含むアカウント情報漏えい事件などが発生しました。該当するサービスの利用者は、漏えいしたアカウント情報を不正に使用される“なりすまし”（不正アクセス）を防ぐため、パスワードの変更といった対処が求められています。

今までも“なりすまし”の被害は発生していましたが、今回は漏えいした情報の量が多いため、ID やパスワードを他のサービスでも使い回ししていた利用者の情報が含まれている可能性も高く、その場合、それらのサービスにおいても“なりすまし”をされ、被害が拡大する可能性があります。

大手のウェブメールサービスのアカウント情報を盗もうとするフィッシング※2 の手口も横行しており、ID やパスワードを使い回ししていると、同様に被害拡大の原因となり得ます。

オンラインサービスでは、“なりすまし”をされた場合、金銭的な被害等を受ける危険があり、これを防ぐためには、パスワードの作成や管理に十分な注意が必要です。オンラインサービスで利用する ID やパスワードは、それを悪用しようとしている者に常に狙われていることを意識し、適切に管理してください。

※2　フィッシング（Phishing）：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利用して偽のウェブページに誘導し、それを見た利用者の ID やパスワードなどを詐取しようとする行為のこと。

（1）ID やパスワードを使い回すことの危険性

近年は数多くのオンラインサービスが存在しており、利用者は各サービスについてそれぞれ ID やパスワードを登録、管理することになります。この際、覚えきれないといった理由で、同じ ID やパスワードを登録する“使い回し”が行われがちですが、使い回しをすると、そのうち一つのサービスでアカウント情報が漏えいした場合、連鎖的になりすまし被害が拡大する恐れがあります。

次に、使い回しにより発生しうる被害拡大の一例を説明します（図 1-1 参照）。

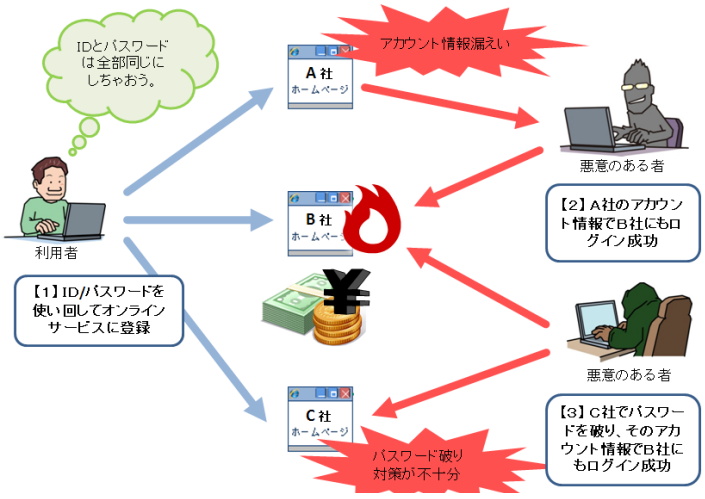

図 1-1：ID やパスワード使い回しによる危険性

【1】ID やパスワードを使い回してオンラインサービスに登録

複数のサービス（図では A、B、C 社）の利用者が、パスワード管理を簡略化するために、各社にログインするための ID やパスワードを全て同じにしていたとします。

【2】A 社のアカウント情報で B 社にもログイン成功

A 社で情報漏えい事件が発生してパスワード情報が流出してしまい、悪意ある者が、流出した情報を元に B 社のウェブサイトへのログインを試行すると、B 社でもログインに成功してしまうケースです。

【3】C 社でパスワードを破り、そのアカウント情報で B 社にもログイン成功

悪意ある者が、パスワードを破ろうとする総当たり攻撃※3 や辞書攻撃※4 への対策が不十分な C 社のウェブサイトで、ID やパスワードを入手します。その情報をもとに、B 社のウェブサイトでログイン試行すると、B 社でもログインに成功してしまうケースです。

※3　何らかの規則にしたがって文字の組み合わせを総当たりで試行する、いわゆる力ずくの攻撃方法。

※4　辞書にある単語などを組み合わせながら試行する攻撃方法。

パスワードの使い回しをしないことは、“なりすまし”の**被害を拡大させない**ための重要なポイントの一つです。

根本的に“なりすまし”の**被害に遭わない**ためには、ID やパスワードを扱う上での基本的な対策が必要です。

（2）なりすまし対策の基本

“なりすまし”対策の基本は、**パスワードの強化・保管・利用**の 3 点に集約できます（図 1-2 参照）。この 3 点のうち、1 点でもおろそかにしてはいけません。

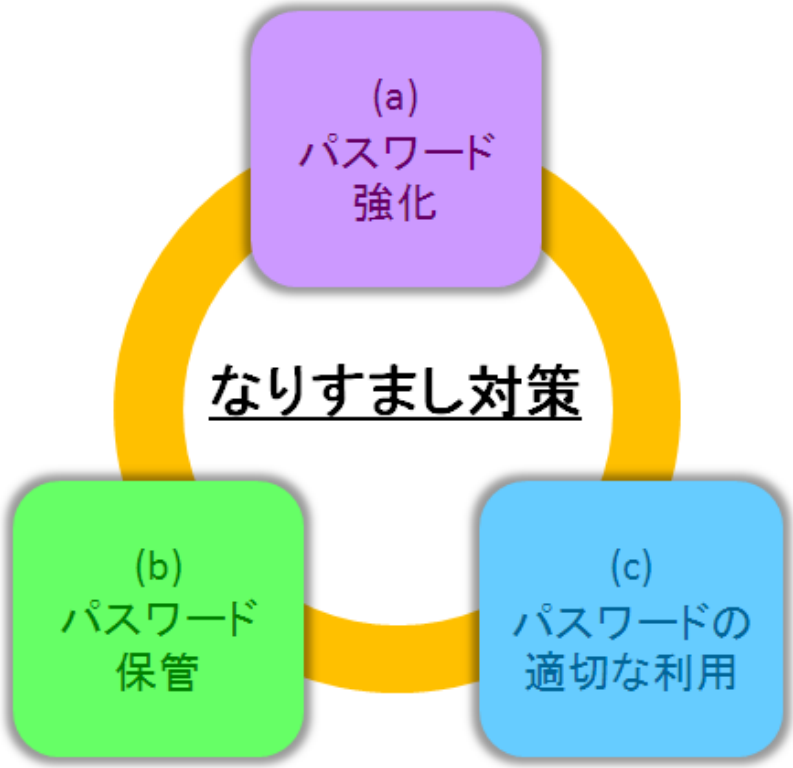

図 1-2：なりすまし対策

以下のポイントを参考に、ID やパスワードの管理を適切に実施してください。

（a）パスワードを強化する

破られやすいパスワードを使用していると、総当たり攻撃や辞書攻撃を受けることによりパスワードを破られる危険性が高くなります。次の条件を満たすよう、破られにくいパスワードを使用し

てください。

- 英字（大文字、小文字）・数字・記号など使用できる文字種全てを組み合わせる
- 8 文字以上にする
- 辞書に載っているような単語や名前（人名、地名）を避ける

（b）パスワードを適切に保管する

破られにくいパスワードを作成したあとは、その保管について以下の項目にも注意してください。

- パスワードをメモする時は、ID と別々にする

  長く複雑なパスワードを作成すると、記憶するのは大変です。この場合、紙にメモしても構いませんが、ID とパスワードは別々に保管することを勧めます。仮にパスワードが知られたとしても、どの ID に対応するパスワードなのかがわからなければ、なりすましは難しくなります。

- 定期的に棚卸しをする

  古い ID 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。利用サービスを定期的に棚卸しして、利用しないサービスに関しては登録解除することを勧めます。

（c）パスワードを適切に利用する

サービス利用時にパスワードを入力する際にも注意が必要です。

- ネットカフェなど、不特定多数が利用するパソコンでは、ID やパスワードを入力しない

  破られにくいパスワードを設定していても、ネットカフェ内のパソコンにパスワードを盗むウイルスが仕掛けられていたら簡単に盗まれてしまいます。自分の管理下にないパソコンでは、ID やパスワードを必要とするオンラインサービスの利用は避けるようにしてください。

- ワンタイムパスワードなどのサービス（二要素認証、二段階認証等）を利用する

  オンラインバンキングやオンラインゲームなどでは、その時だけ有効なパスワードを発行する「ワンタイムパスワード」というサービスを提供していることがあります。ID やパスワードを盗むウイルスに感染していても、一度きりのパスワードのため、仮に盗まれてもその後悪用されることはありません。また、フィッシングの手口に引っ掛かり、ID やパスワードを盗まれたとしても、同様に、悪用されることはありません。ただし、ワンタイムパスワードのトークン[※5] を他人に渡さない、トークンに表示されているパスワードを他人に教えない、信頼できるサイトに対してのみパスワード入力する、などの基本的対策は必須です。

  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お知らせメールを送信する機能（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。

  ※5　トークン（Token）：利用者の認証をより確実にするために使用する、ハードウェアまたはソフトウェアのこと。ハードウェアの場合には、ポケットに入る程度に小さなものが多く、時刻に基づくワンタイムパスワードを表示したり、暗号鍵や生体認証のための情報を格納しておくなどの機能がある。

上記のなりすまし対策を行っていても、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。

さらに、OS（オペレーティングシステム）やアプリケーションソフトの脆弱性対策も必須です。

また、Internet Explorer などのブラウザには、ID やパスワードを保存する機能がありますが、保存された情報を盗むウイルスも確認されています。盗まれるリスクを減らすため、ブラウザには ID やパスワードを保存しないようにすることを勧めます。

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）
- ウェブメールサービスに勝手にログインされて、アカウントを削除されてしまった
- "ガンブラー"によるものと思われる被害

○ 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）
- FBI から怪しいメールが届いた？
- オンラインゲームで不正アクセスを受けた

○ 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

5 月のウイルスの検出数※1 は、**約 2.3 万個**と、4 月の約 2.6 万個から 11.4%の減少となりました。また、5 月の届出件数※2 は、**1,049 件**となり、4 月の 1,138 件から 7.8%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。
- 5 月は、寄せられたウイルス検出数約 2.3 万個を集約した結果、1,049 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 1.5 万個**、2 位は **W32/Mydoom** で**約 5.6 千個**、3 位は **W32/Autorun** で**約 0.7 千個**でした。

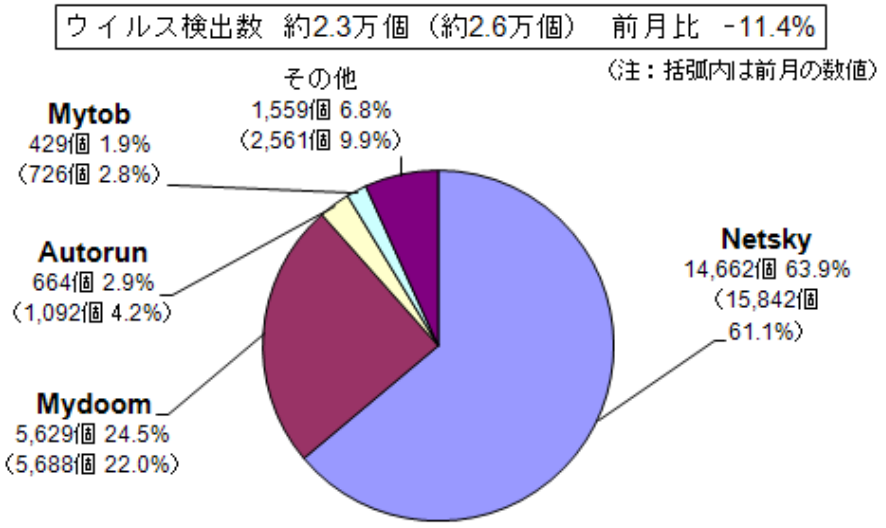

図 2-1：ウイルス検出数

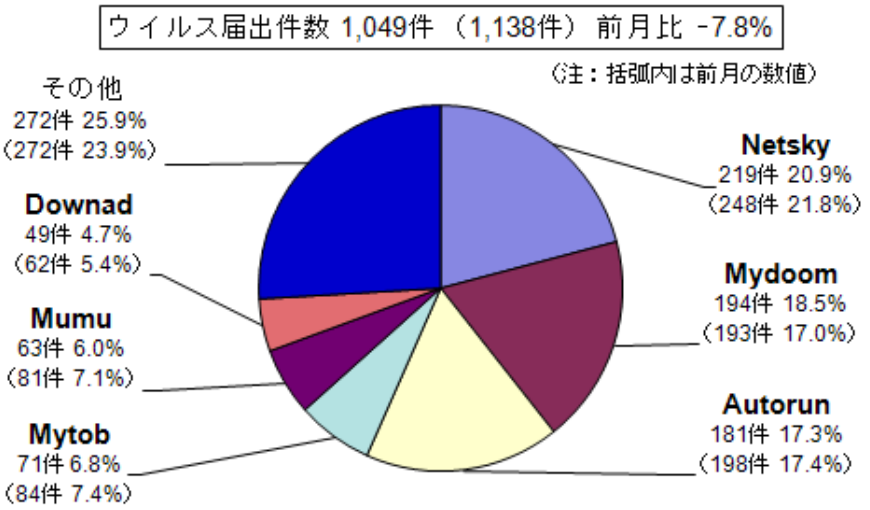

図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

５ 月は、パソコン内に裏口を仕掛ける BACKDOOR や、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（図 2-3 参照）。

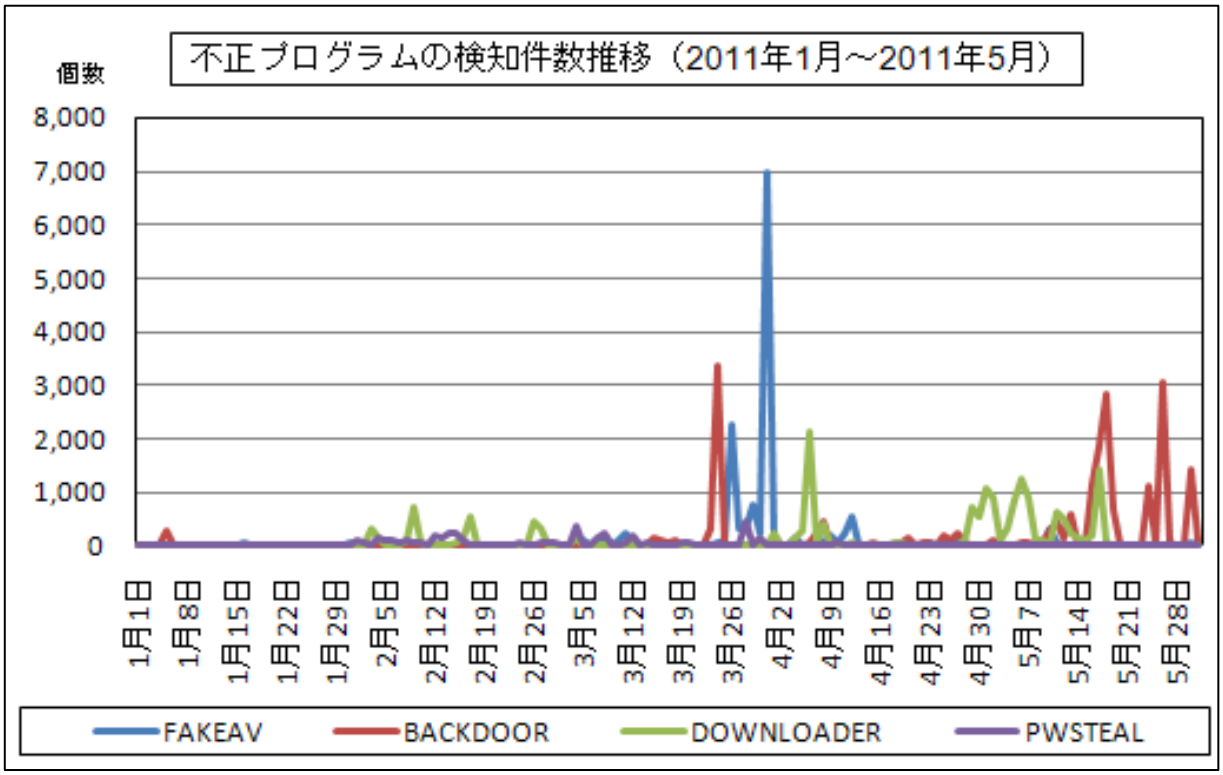

図 2-3：不正プログラムの検知件数推移

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

		12月	1月	2月	3月	4月	5月
届出(a) 計		22	12	10	6	5	7
	被害あり(b)	7	6	5	6	5	6
	被害なし(c)	15	6	5	0	0	1
相談(d) 計		27	41	23	45	38	55
	被害あり(e)	7	11	6	10	10	14
	被害なし(f)	20	30	17	35	28	41
合計(a+d)		49	53	33	51	43	62
	被害あり(b+e)	14	17	11	16	15	20
	被害なし(c+f)	35	36	22	35	28	42

（1）不正アクセス届出状況

５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６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55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４件、なりすまし２件**でした。

「侵入」の被害は、サーバの脆弱性を突かれてサーバ内に不審なファイルを置かれて、データベース内の情報を盗まれたものが１件、ウェブページが改ざんされていたものが３件（内、フィッシング※に悪用するためのコンテンツ設置１件）でした。侵入の原因は、バージョンが古かったものが１件、脆弱なパスワード設定が１件、アクセス制限の設定ミスが１件でした（他は原因不明）。

「なりすまし」の被害は、フリーのウェブメールサービスに何者かにログインされてメールを勝手に送信されていたものが１件、オンラインサービスに何者かにログインされてアカウントごと削除されていたものが１件でした。

※フィッシング（Phishing）： 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利用して偽のウェブページに誘導し、それを見た利用者の ID やパスワードなどを詐取しようとする行為のこと。

（4）被害事例

［なりすまし］

（i）ウェブメールサービスに勝手にログインされて、アカウントを削除されてしまった

事例	・普段利用しているウェブメールサービスに突然ログインできなくなった。 ・サービス提供会社に問い合わせたところ、自分以外の第三者がログインして「ID 削除」を行ったとのこと。 ・パスワードを盗まれたと思うが、盗まれた原因は分からない。
解説・対策	強固なパスワードを設定するとともに、ID やパスワードの使い回しは避けましょう。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お知らせメールを送信する機能（ログインアラート機能）**を提供している場合があります。自分以外の誰かがログインした際に、お知らせメールが届けば、不正ログインに早く気付くことができ、被害を最小限に留めることができます。この機能は、フィッシングの手口に引っ掛かり、ID やパスワードを盗まれた場合でも、有効に働きます。

［侵入］

（ii）"ガンブラー"によるものと思われる被害

事例	・自社ホームページを閲覧すると、ウイルス対策ソフトのウイルス警告が出てきた。 ・ウェブサイトのコンテンツを調査したところ、HTML ソースに、悪意あるサイトへ誘導するためのスクリプトが挿入されていることが判明。 ・すぐに ftp パスワードを変更した。今後の対策として、ftp 接続を許可する接続元 IP アドレスに制限を加えた。
解説・対策	減少傾向ではありますが、いまだにガンブラーによるものと思われる被害が続いています。典型的なガンブラーの被害を防ぐための対策として、「ftp アクセスの制限」は有効です。その他、「ftp アカウントのパスワード強化」や「ウェブサイト更新専用パソコンの導入」も有効な対策です。 （参考） IPA - 2010 年 4 月の呼びかけ「ウェブサイトの管理方法を再確認しましょう！」 http://www.ipa.go.jp/security/txt/2010/04outline.html

4. 相談受付状況

5 月のウイルス・不正アクセス関連相談総件数は **1,640 件**でした。そのうち**『ワンクリック請求』に関する相談**が **519 件**（4 月：455 件）、**『偽セキュリティソフト』**に関する相談が **3 件**（4 月：6 件）、**Winny に関連する相談**が **5 件**（4 月：13 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 **8 件**（4 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

		12月	1月	2月	3月	4月	5月
合計		1,536	1,463	1,521	1,723	1,608	1,640
	自動応答システム	954	892	892	1,106	997	950
	電話	531	499	570	551	555	620
	電子メール	49	64	53	58	50	62
	その他	2	8	6	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。

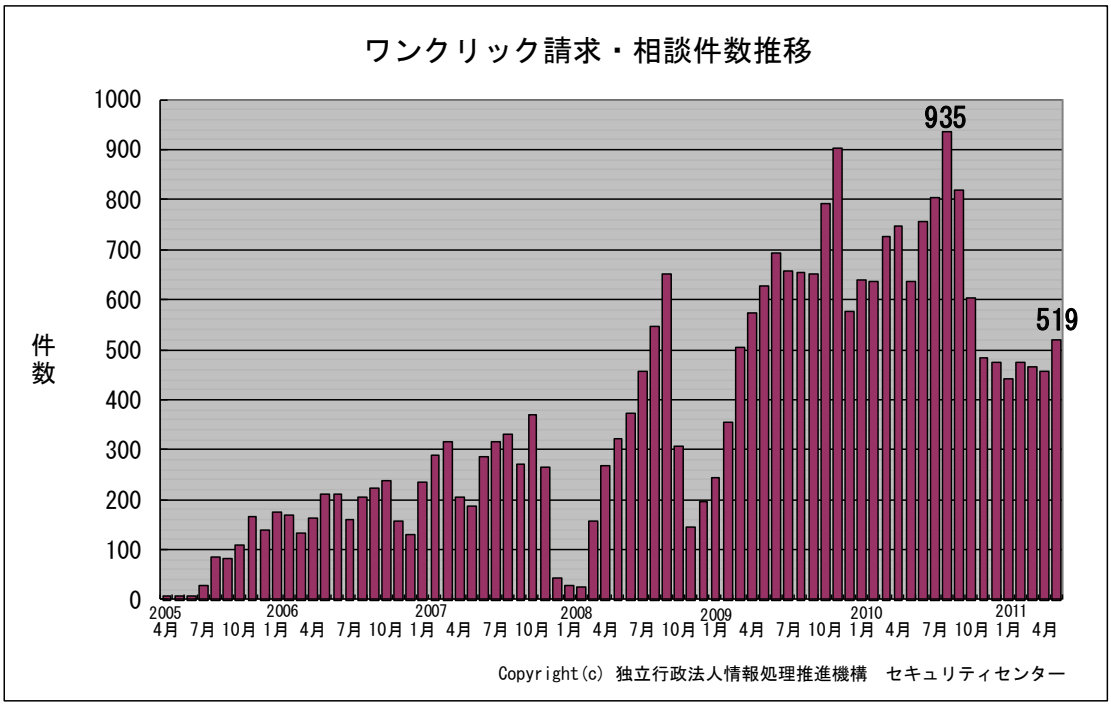

図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）FBI から怪しいメールが届いた？

相談	FBI（米連邦捜査局）と思われるメールアドレスから、「You visit illegal websites（あなたは違法なウェブサイトを閲覧した）」という件名の、添付ファイル付きのメールが届いた。本文も英語で書かれており、“多数の違法なウェブサイトにあなたの IP アドレスが記録されていたので、添付ファイルの質問に答えてください”といった内容。心当たりはないが、なぜこのようなメールが届いたのか。
回答	送信元を偽装し、不特定多数を狙った罠メールと思われます。類似したメールが出回っているという注意喚起が、2011 年 5 月上旬に海外のセキュリティ企業から発信されています。**添付ファイルを開くとウイルスに感染するようです**。 悪意ある者は言葉巧みにターゲットにウイルスを感染させようとするので、身に覚えのないメールが届いても、不用意に反応しないようにしてください。 （ご参考） IPA-2011 年 5 月の呼びかけ「 災害情報に便乗した罠（わな）に注意！ 」 http://www.ipa.go.jp/security/txt/2011/05outline.html

（ii）オンラインゲームで不正アクセスを受けた

相談	いつも使っているオンラインゲームサイトにログインしたら、昨日まであったはずのアイテムとゲーム内通貨が盗まれたらしく、なくなっていた。 実はこのことが起きる数日前に、ゲームにログイン中に誰かに上書きログイン（二重ログイン）されて、接続が切れたことがあった。それで念のため、パスワードを変更したが、それでも不正アクセスされてしまったということになる。相手はどのようにして不正アクセスが行えたのか。
回答	パスワードを破る手段として、総当り攻撃※などのように、ある程度時間のかかる方法の場合、一旦パスワードを変更してしまえば、再度破るまでにしばらく時間がかかるはずです。 今回のケースはパスワードを変更したにも関わらず、あまり時間を置かずに再度破られたということなので、よほど安易なパスワードを設定していたか、**パソコン自体にパスワード情報を盗むウイルスが感染していた可能性が高い**と思われます。 ウイルス感染が原因の場合、ウイルス対策ソフトでウイルスを駆除する必要がありますが、ウイルスチェックで何も見つからなかった場合でも安心はできませんので、念のためパソコンを一度初期化することをお勧めします。 （ご参考） IPA-2009 年 10 月の呼びかけ「 あなたのオンラインゲームのキャラクターは狙われています！ 」 http://www.ipa.go.jp/security/txt/2009/10outline.html

※総当り攻撃：何らかの規則にしたがって文字の組み合わせを総当りで試行する、いわゆる力ずくの攻撃方法。

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 5 月の期待しない（一方的な）アクセスの総数は 10 観測点で **189,497 件**、延べ発信元数※は **78,227 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 252 の発信元から 611 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。

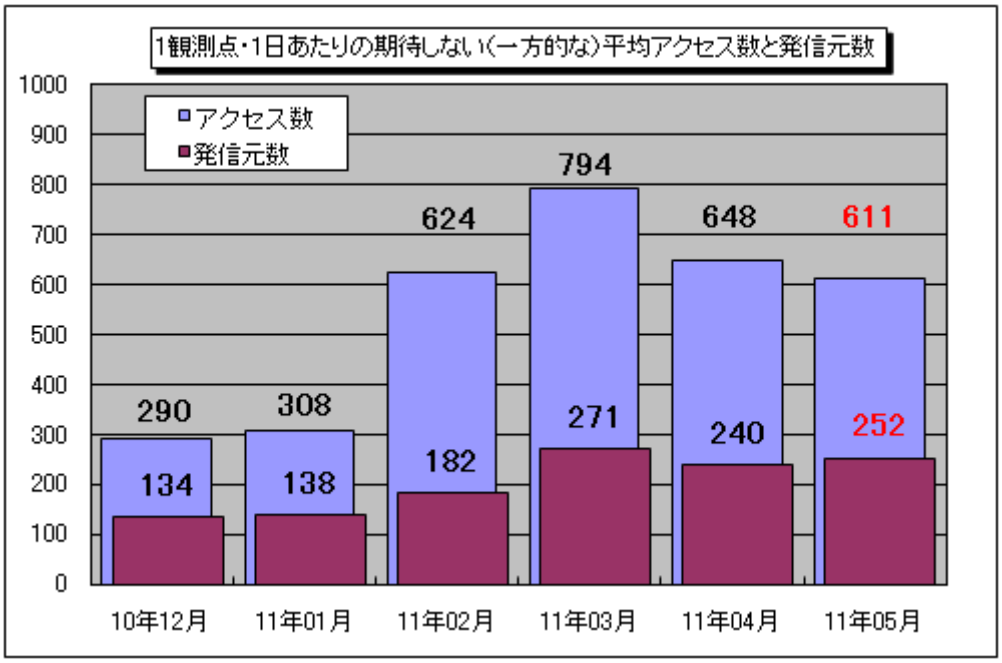

図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数

2010 年 12 月～2011 年 5 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。5 月の期待しない（一方的な）アクセスは、4 月と比べて減少しました。

4 月と 5 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。4 月に比べ、増加が観測されたのは 10394/udp 、10394/tcp、その他へのアクセスでした。

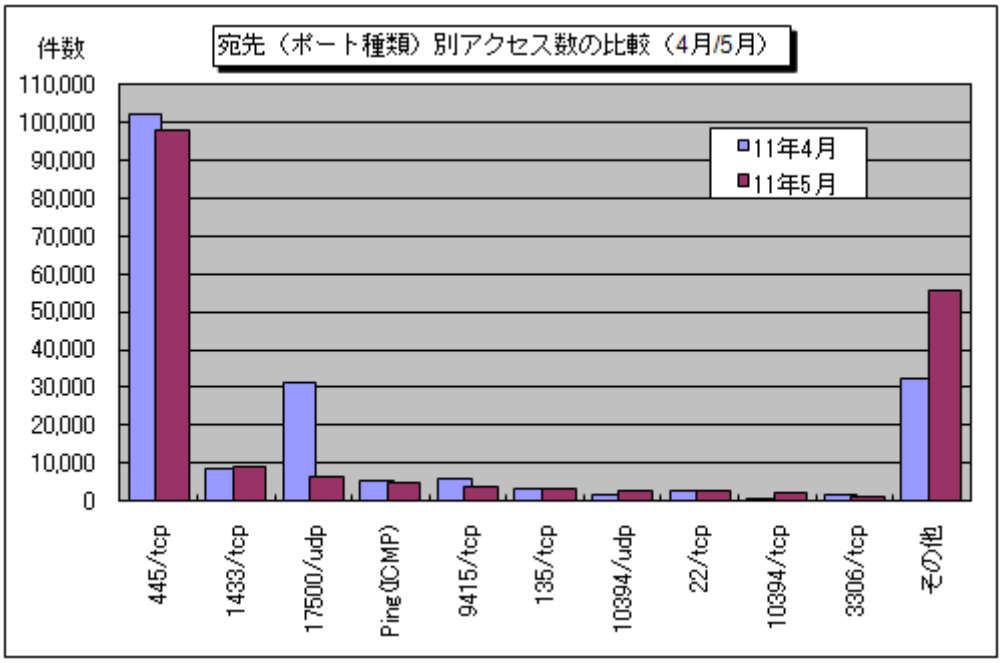

図 5-2：宛先（ポート種類）別アクセス数の比較（4 月/5 月）

10394/udp と 10394/tcp については、5 月 22 日の周辺に、増加が観測されていました（図 5-3 参照）。これらのポートはいずれも、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。これらのアクセスは、特定の 1 観測点でしか観測されていませんでしたが、1 つの発信元からというわけではなく、複数の発信元からのアクセスが観測されていました。

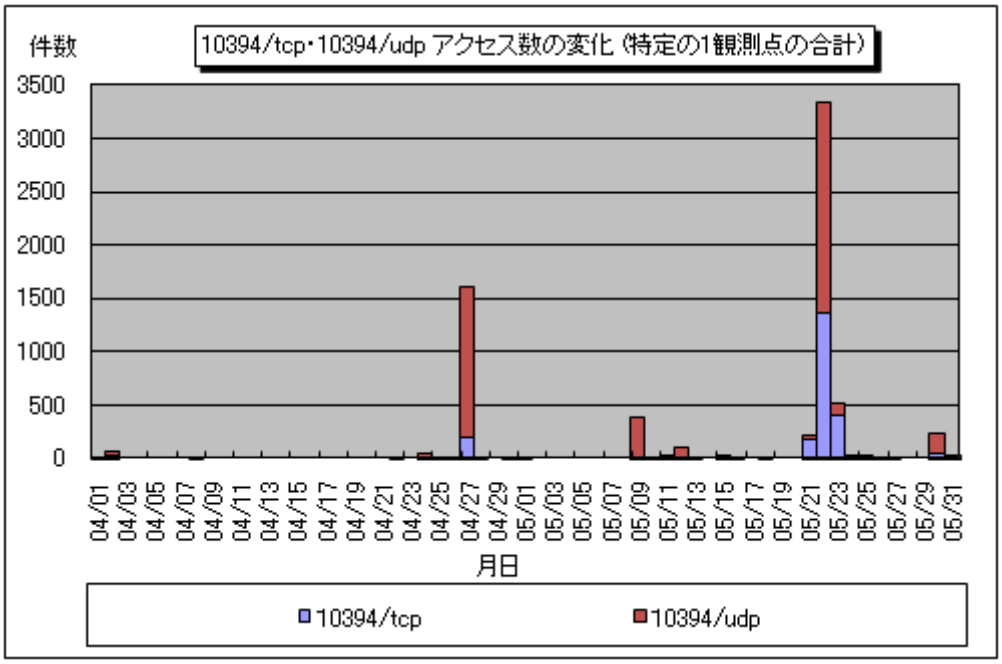

図 5-3：10394/tcp・10394/udp アクセス数の変化（特定の 1 観測点の合計）

その他へのアクセスの増加について、解析した結果、TALOT2 の特定の観測点に対し、5 月 20 日から 23 日の間に、アメリカ合衆国の特定の IP アドレスの 80/tcp からのアクセスが観測されました（図 5-4 参照）。これらのアクセスは、全て SYN/ACK パケットだったことから、TALOT2 で使用しているアドレスが、DoS 攻撃（SYN Flood 攻撃）(*1) の攻撃者が発信元詐称に利用したアドレスと一致したために、標的となった組織からの SYN/ACK パケット（跳ね返りパケット (*3)）が大量に届いていた可能性があるということです。

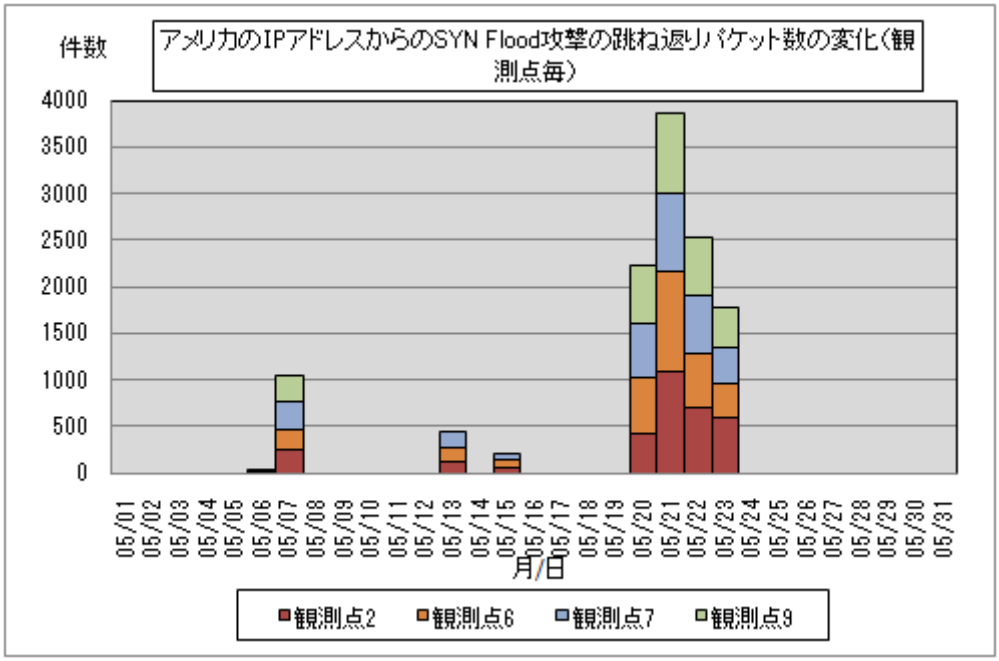

図 5-4：アメリカの IP アドレスからの SYN Flood 攻撃の跳ね返りパケット数の変化（観測点毎）

なお、5 月 26 日にも、中国の特定の IP アドレスの 7001/tcp からのアクセスが観測されていました（図 5-5 参照）。これらのアクセスも、全て SYN/ACK パケットだったことから、TALOT2 で使用しているアドレスが、攻撃者が発信元詐称に利用したアドレスと一致したために、標的となった組織からの SYN/ACK パケットが大量に届いていた可能性があるということです。

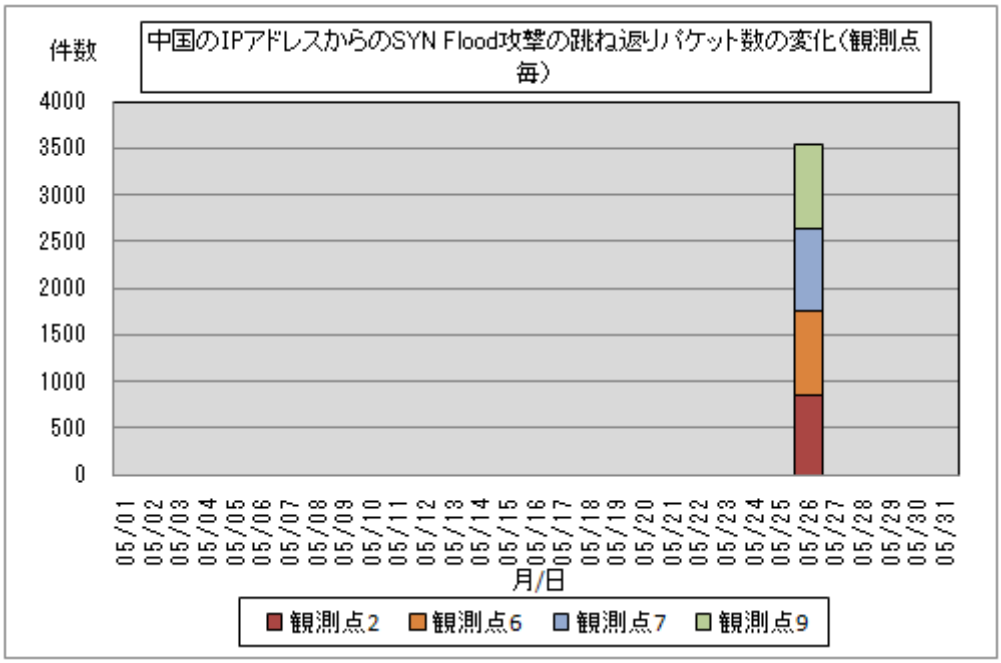

図 5-5：中国の IP アドレスからの SYN Flood 攻撃の跳ね返りパケット数の変化（観測点毎）

(*1):DoS 攻撃（SYN Flood 攻撃）

「サービス妨害攻撃」Denial of Service の略から DoS 攻撃と呼ばれ、標的マシンにおけるサービス機能を停止または低下させる攻撃のこと。この DoS 攻撃の 1 つに、標的マシンに「過負荷を与える攻撃」 として SYN Flood 攻撃があります。これは、標的マシンに対して発信元アドレスを詐称した SYN パケット（3 ウェイ・ハンドシェーク (*2) での接続確立の最初に送られるパケット）を大量に送りつけ、確立途中状態の接続を大量作成するものです。

(*2):3 ウェイ・ハンドシェーク

TCP で通信を行う際に、最初に行われる通信確立のための手順を、3 ウェイ・ハンドシェークと言います。この手

順により、通信を行う相手同士が通信の準備ができたことを確認できるわけです。

以下にA とB の通信確立の手順を示します。

①A からB へSYN パケットの送信

②B からA へACK+SYN パケットの送信

③A からB へACK パケットの送信

これで、AB 双方の通信が確立されます。

(*3):跳ね返りパケット

DoS 攻撃（SYN Flood 攻撃）において攻撃者が詐称した発信元アドレスに、標的マシンから大量の SYN+ACK パケットが返信されてくることです。

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/TALOT2-1106.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