Information-technology Promotion Agency, Japan

第 12-15-251 号
2012 年 7 月 4 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［2012 年 6 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、2012 年 6 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

「 フィッシングに注意するとともに、自分が加害者にならないよう気をつけよう！ 」
～ 不正アクセス禁止法が改正されました ～

最近、“海外のウェブサービスのパスワードが大量に流通している”との報道がありました。一方、国内の企業においても、インターネット利用者の多くが複数サイトで同じ ID とパスワードを使いまわしている状況に目を付けて、不正に取得した ID とパスワードのリストを悪用して不正アクセスを試みる、「パスワードリスト攻撃」が確認されています※1。

今年 3 月に不正アクセス禁止法が改正され、5 月に改正法が施行されたことにより、パスワードを不正に取得・保管・提供する行為や、騙してパスワードを窃取しようとする行為（フィッシング）も取り締まりの対象になりました。

自分のパスワードも狙われているという現実を知るとともに、改正法を理解することで、 自分の身を守るだけではなく、他人のパスワードの取り扱いにも気を配って、社会全体で犯罪を抑止しましょう。

※1 警察庁 - 平成 23 年中の不正アクセス行為の発生状況等の公表について
（ここでは「不正ログイン攻撃」として紹介されています）
http://www.npa.go.jp/cyber/statics/h23/pdf040.pdf

（1） フィッシングの手口

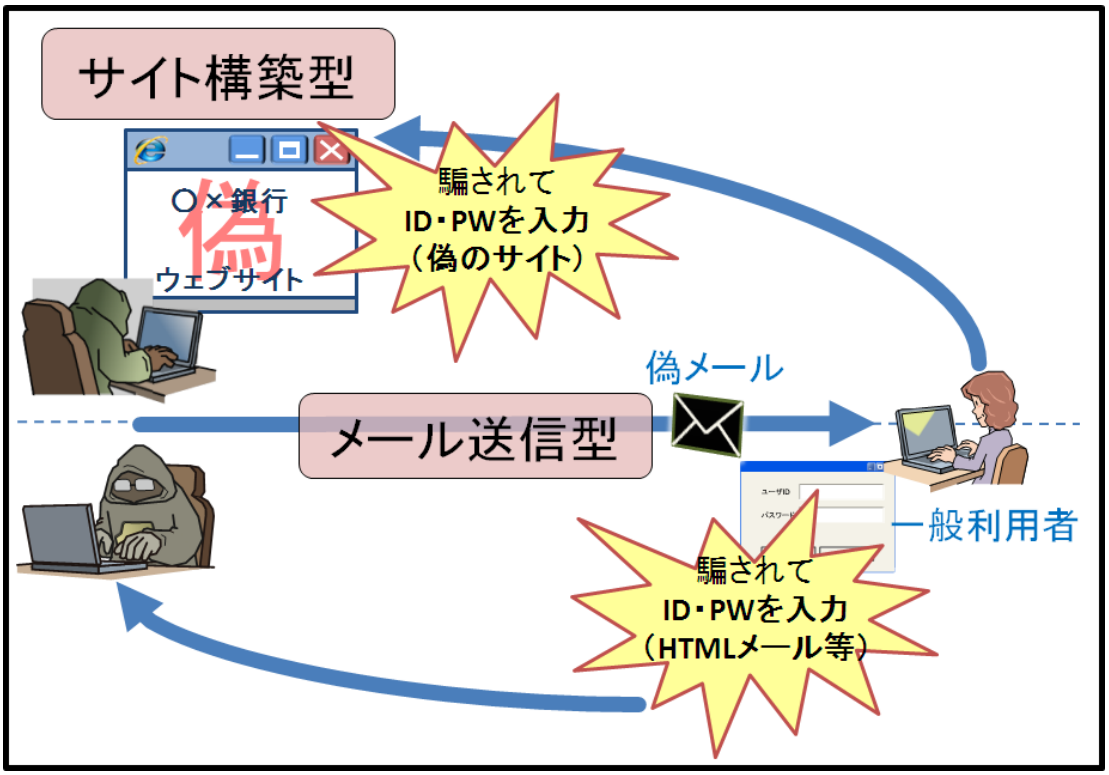

図 1-1：フィッシング手口「サイト構築型」と「メール送信型」のイメージ図

フィッシングとは、正規のサービス提供企業を装ったメールを送り、ID やパスワードなどのログイン情報や、さらに住所、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不正に窃取する行為のことです。

その手口は、偽のウェブサイトへ誘導するもの（サイト構築型）と、メールそのものに ID とパスワードを入力させる仕掛けが施されているもの（メール送信型）の、2 通りに大別されます※2。

※2 禁止・処罰するフィッシング行為の類型（「不正アクセス行為の禁止等に関する法律の解説」p.12）
http://www.npa.go.jp/cyber/legislation/pdf/1_kaisetsu.pdf#page=12

サイト構築型

攻撃者が、正規のウェブサイトを模倣した偽のウェブサイト（フィッシングサイト）をインターネット上に設置して、そこに誘導した利用者に ID とパスワードを入力させる手口です。概ね以下の流れで攻撃が行われます。

【1】攻撃者がフィッシングサイトを設置
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フィッシングサイトを設置します。

【2】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偽メール（フィッシングメール）を送信します。メールの本文には、【1】のフィッシングサイトへのリンクが記されています。

【3】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リンクをクリックすると、【1】のフィッシングサイトに誘導されます。

【4】攻撃者がアカウント情報を入手
利用者が、画面の見た目だけで判断し、偽のウェブサイトと気付かずにアカウント情報（ID やパスワードなど）を入力してしまうと、それらの情報が攻撃者に渡ってしまいます。

【5】攻撃者が不正入手したアカウント情報を悪用
攻撃者は、入手したアカウント情報を使い、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。さらに他のサイトでのログインを試みる場合もあります。

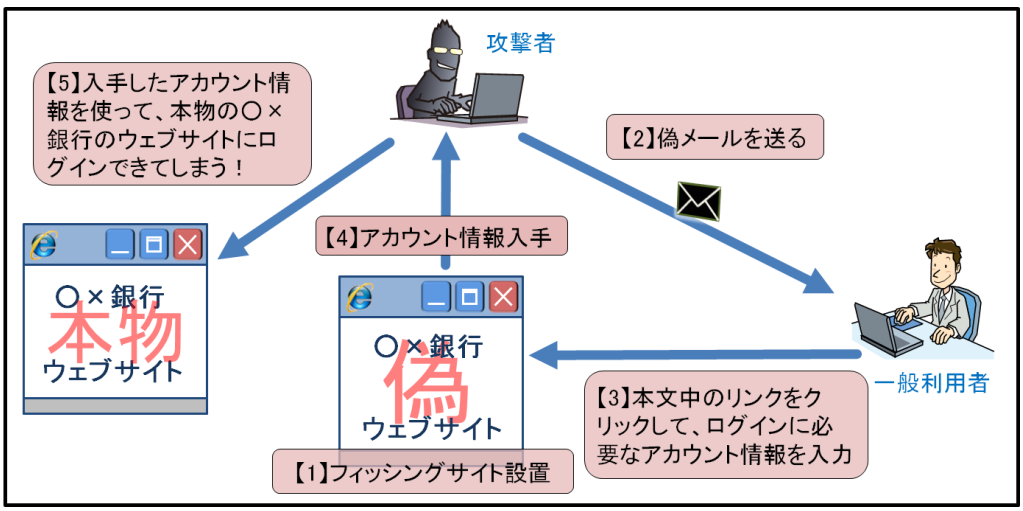

図 1-2：「サイト構築型」フィッシング被害の一連の流れのイメージ図

メール送信型

フィッシングサイトを用いず、メールそのものに ID とパスワードを入力させる仕掛けが施されているタイプです。メールに施されている仕掛によって「送信プログラム添付型」「HTML メール型」に分かれます。

●送信プログラム添付型

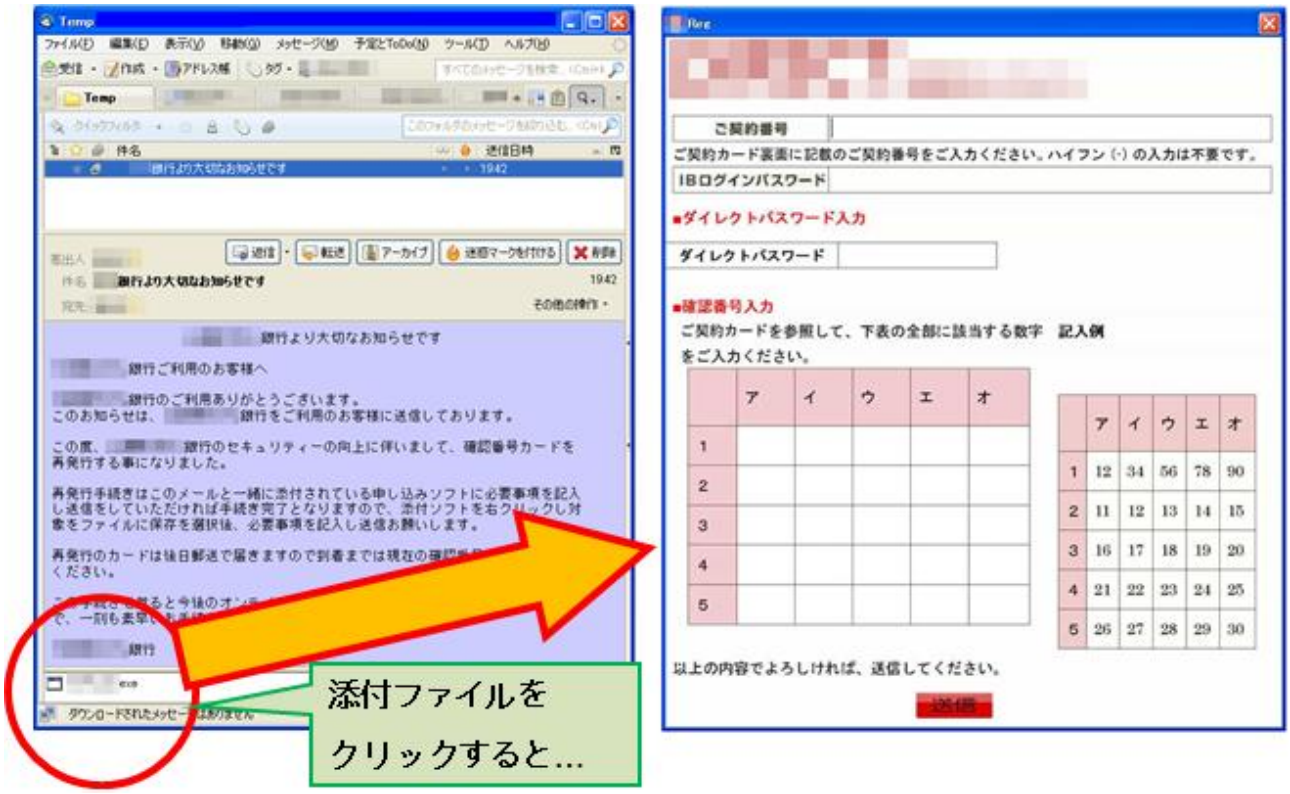

図 1-3：「送信プログラム添付型」の例

図 1-3 は、国内の大手銀行を装い不正プログラムが添付された、実際のメールです。

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。**通常、このような依頼がメールで送られることはありません。**

情報を入力し「送信」ボタンをクリックすると、入力した情報が外部のサーバーに送信され、攻撃者の手に渡ります。その結果、攻撃者がインターネットバンキングにログインして送金手続きなどを実施することが可能になります。

●HTML メール型

HTML を使用し、メール本文欄に本物のウェブサイトのような画面を表示し、利用者を騙して ID とパスワードを入力させる手口です。ID とパスワードを入力し「確認」等のボタンをクリックすることで、入力した情報が盗まれる可能性があります※3。

※3 フィッシング対策協議会 - 実在する銀行をかたるフィッシング
http://www.antiphishing.jp/news/alert/20120404bankdaiwa.html

(2) フィッシングへの対応と対策

フィッシングの被害者にならないように普段から注意するとともに、被害拡大防止のため、フィッシング行為を発見したら**すぐに通報**してください。

以下に、発見時の通報先と、被害に遭わないための注意点について説明します。

発見時の通報先

●フィッシングサイト発見時

自社のサイトを模倣したフィッシングサイトを公開された場合や、個人の方でフィッシングサイトを発見した場合は、下記に連絡してください。

フィッシング 110 番
http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm
JPCERT/CC
http://www.jpcert.or.jp/form/

●フィッシングメール受信時

フィッシングメールと思しきメールを受信した場合は、下記に連絡してください。

フィッシング 110 番
http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm
フィッシング対策協議会
https://www.antiphishing.jp/consumer/rep_phishing.html

●もしフィッシングの被害に遭ってしまったら

具体的な被害の相談については、サービス提供会社と、最寄りの警察署にご相談ください。併せて、フィッシング 110 番に情報提供をしてください。

フィッシング 110 番
http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm

自分が被害に遭わないために（注意のポイント）

●ID とパスワードの使い回しを避ける

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それぞれの 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。

不正に取得した ID とパスワードを悪用して不正アクセスを試みる「パスワードリスト攻撃」による被害を防ぐためにも、ID とパスワードの使い回しを避けることを勧めます。

●メールの内容に注意する

暗証番号や本人の個人情報をメールで問い合わせることはまずありません。そのようなメールはフィッシングメールと断定できるので、個人情報を入力しないようにしてください。

●添付ファイルに注意する

メールに不審なファイルが添付されていた場合、「送信プログラム添付型」の可能性があるので、開かずにメールそのものを削除してください。

●URL のドメイン名などに注意する

ウェブサイトで ID とパスワードや、暗証番号、クレジットカード番号などを入力する時は、ブラウザの URL 欄に正しいドメイン名が表示されていることを確認してください。そして、URL 欄のすぐ横が**緑色の場合は団体名、青色の場合はドメイン名**が表示されるので、アクセス先と一致していることを確認してください。

（緑色でも、ウェブサイトの運用管理業者が表示されて、アクセス先の団体と異なる場合があります。不明な場合はウェブサイトの問い合わせ先に確認してください。）

Internet Explorer の場合

・青色の鍵マークが表示されている場合、鍵マークをクリックして、表示されているサイト名が、アクセスしているサイトと合致していることを確認してください（図 1-4 参照）。

・緑色の場合、表示されている団体名が、アクセスするサイトの団体名と合致していることを確認してください（図 1-5 参照）。

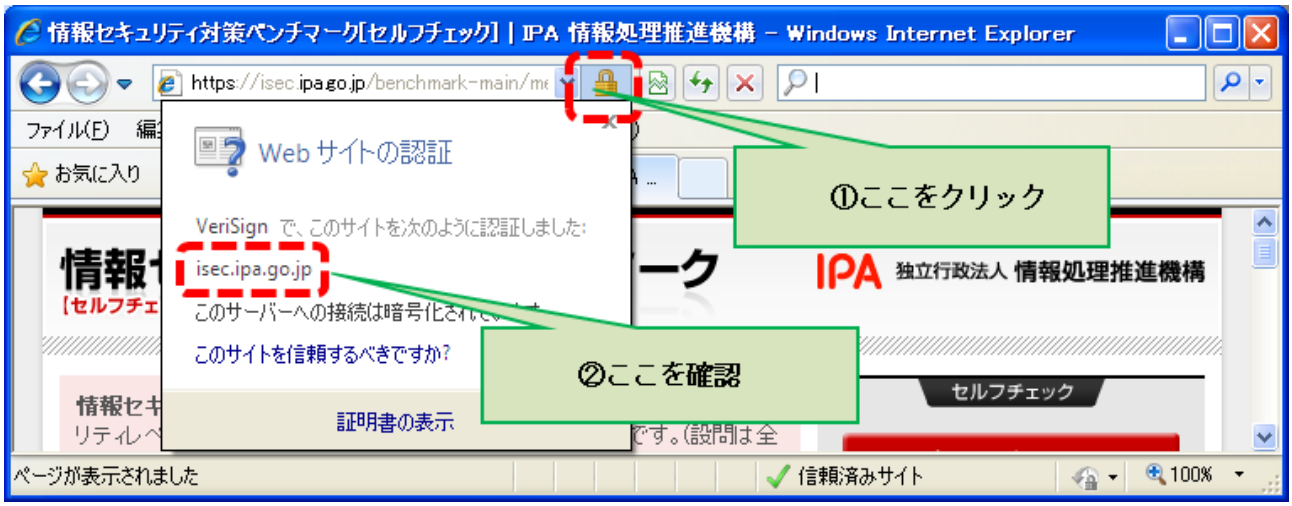

図 1-4：Internet Explorer での表示例（青色）

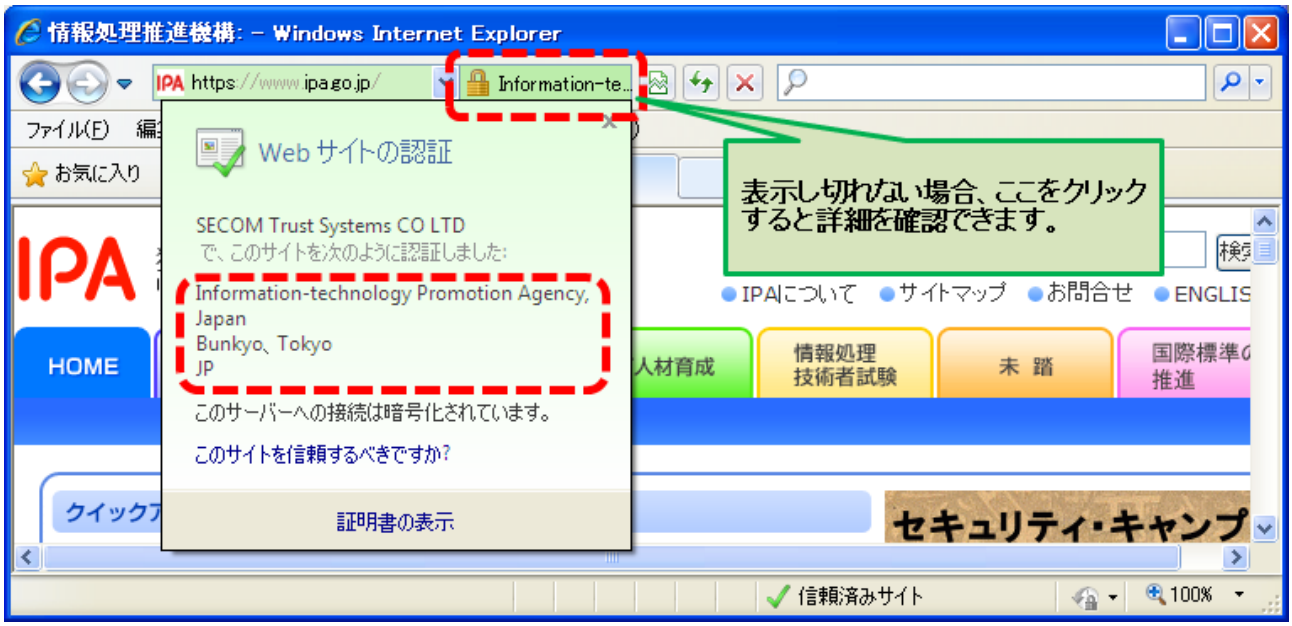

図 1-5：Internet Explorer での表示例（緑色）

Firefox の場合

・青色の場合、表示されているドメイン名が、アクセスするサイトのドメイン名と合致していることを確認してください（図 1-6 参照）。

・緑色の場合、表示されている団体名が、アクセスするサイトの団体名と合致していることを確認してください（図 1-7 参照）。

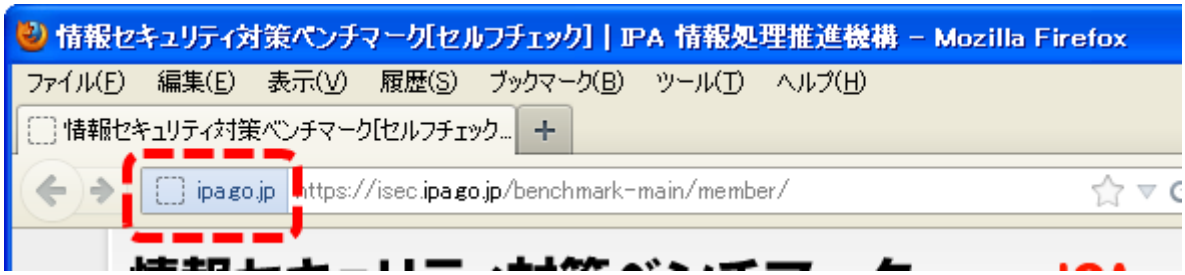

図 1-6：Firefox での表示例（青色）

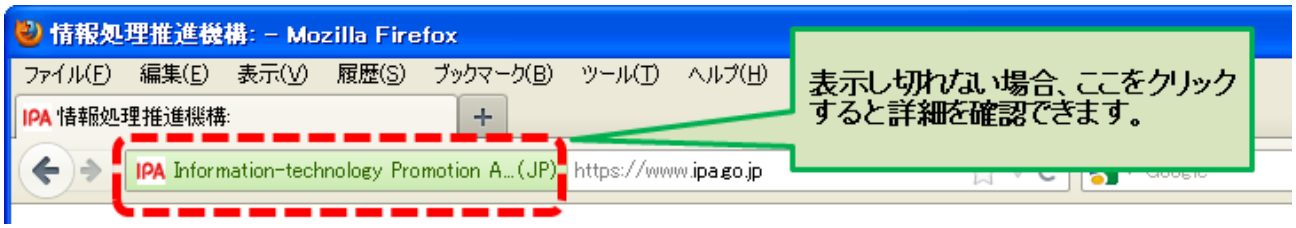

図 1-7：Firefox での表示例（緑色）

（3） 改正法施行における注意事項

法改正以降、フィッシングを仕掛ける以外にも、ID やパスワードを不正に「取得」「保管」「提供」することが法律に抵触し、罰せられる恐れがあります。自分では「そんなつもりはなかった」と思っていても、知らないうちに法律違反をしてしまう可能性があるので注意が必要です。

避けるべき行為：

・不正アクセス行為を目的として、他人の ID やパスワードを紙や USB メモリ等で受け取ること
・不正アクセス行為を目的として、掲示板で公開された他人の ID やパスワードを、パソコン内に保存すること
・不正アクセス行為を目的として、掲示板で公開された他人の ID やパスワードを、自分のブログや他の掲示板に転載したり、メールで他者に送付したりすること

これらの行為が意図して実施されたと認められると、法律違反として罰せられる場合があります。海外のウェブサービスで流出した ID やパスワードを自分のブログで紹介する行為など、今までは法律違反にあたらなかった行為でも、今後は法律違反により罰せられる恐れがありますので、ご注意ください。

ただし、以下の場合は意図して「取得」「保管」しているわけではないので法律違反にはなりません※4

・インターネット検索中に偶然他人の ID やパスワードが表示された場合
・他人の ID やパスワードを一方的に電子メールで送りつけられた場合

※4 不正アクセス行為の禁止等に関する法律の一部を改正する法律の概要
http://www.npa.go.jp/cyber/legislation/pdf/5_kaiseigaiyou.pdf

「今月の呼びかけ」で不明な点がありましたら、「情報セキュリティ安心相談窓口」までお問い合わせください。

「情報セキュリティ安心相談窓口」
・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相談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）

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、11 頁の「3.コンピュータ不正アクセス届出状況」を参照）

・オンラインゲームのアカウントが乗っ取られた

・バックドアを仕込まれて、スパムメール送信の踏み台として悪用された

○ 相談の主な事例 （相談受付状況および相談事例の詳細は、13 頁の「4.相談受付状況」を参照）

・友人からメールが届き、記載の URL をクリックしてしまったが大丈夫でしょうか

・スマートフォンにおける改造行為とは何でしょうか

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

6 月のウイルスの検出数※1 は、**21,990 個**と、5 月の 20,236 個から 8.7%の増加となりました。また、6 月の届出件数※2 は、**958 件**となり、5 月の 970 件から 1.2%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。
・6 月は、寄せられたウイルス検出数 21,990 個を集約した結果、958 件の届出件数となっています。

検出数の 1 位は、**W32/Mydoom** で **11,395 個**、2 位は **W32/Netsky** で **7,800 個**、3 位は **W32/Mytob** で **1,541 個**でした。

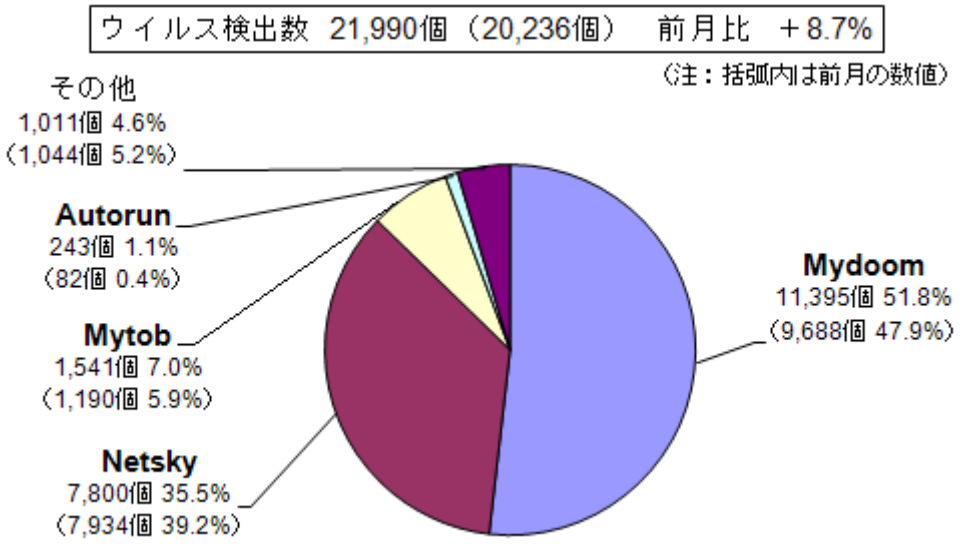

図 2-1：ウイルス検出数

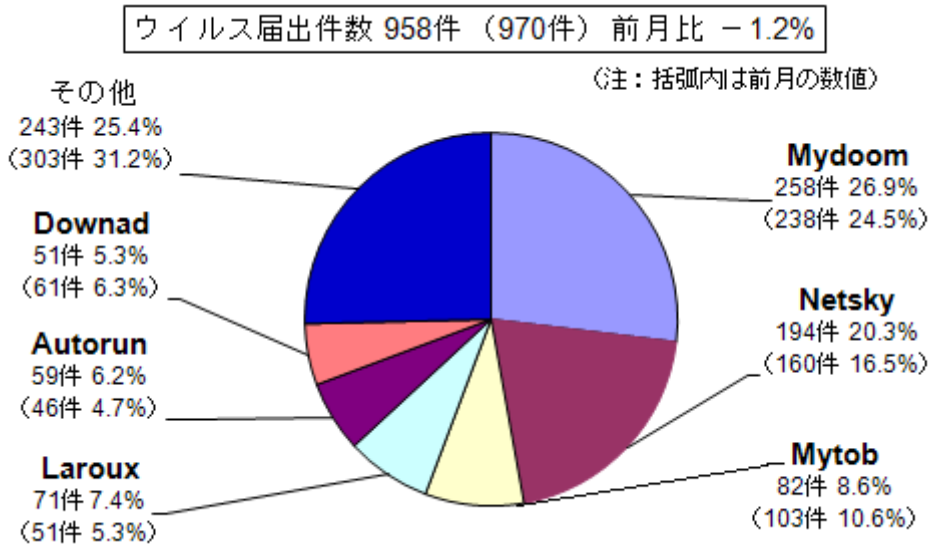

図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

6 月の不正プログラムの検出数※1 は、**25,399 個**と、5 月の 80,999 個から 68.6%の減少となりました。

検出数の 1 位は、オンラインバンキングの ID／パスワードを窃取する **Bancos** で **5,417 個**、2 位は、偽セキュリティソフトの検知名である **Fakeav** で **3,897 個**、3 位は、広告を表示させるプログラムの総称である **Adware** で **2,190 個**、でした。

以下、正規のソフトウェアなどを装って感染を試みる Trojan/Horse、別のウイルスを感染させようとする Downloader、パソコン内に裏口を仕掛ける Backdoor、の順でした。

※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）

※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

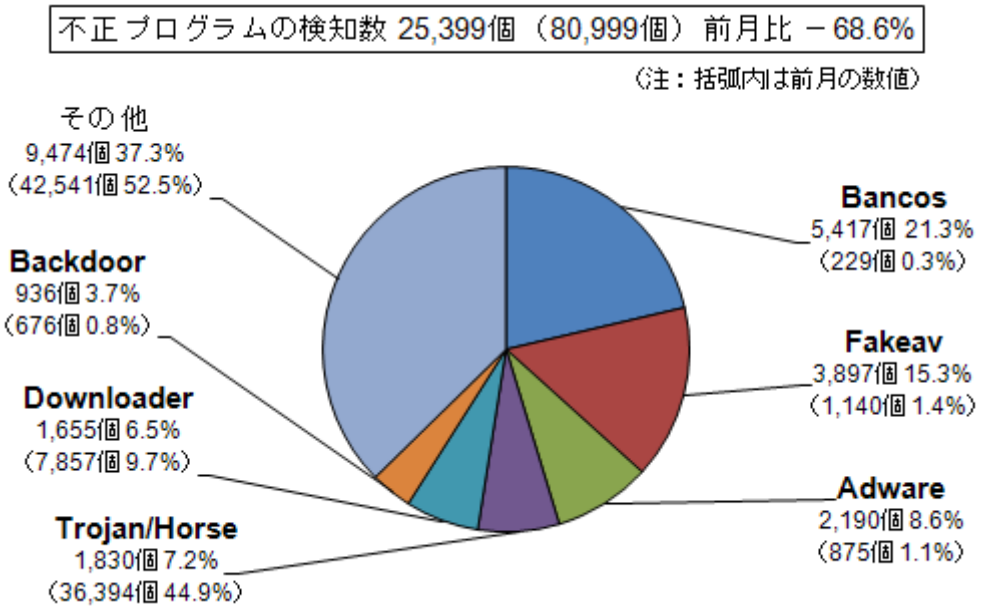

図 2-3：不正プログラムの検知数

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

		1月	2月	3月	4月	5月	6月
届出[a] 計		8	13	5	9	10	2
	被害あり[b]	7	9	4	7	6	2
	被害なし[c]	1	4	1	2	4	0
相談[d] 計		35	37	54	46	50	38
	被害あり[e]	9	14	10	9	17	12
	被害なし[f]	26	23	44	37	33	26
合計[a+d]		43	50	59	55	60	40
	被害あり[b+e]	16	23	14	16	23	14
	被害なし[c+f]	27	27	45	39	37	26

（1）不正アクセス届出状況

６月の届出件数は２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12件でした。

（3）被害状況

被害届出の内訳は、**なりすまし１件、不正プログラム埋め込み１件**、でした。

「なりすまし」の被害は、オンラインゲーム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件でした。

「不正プログラム」の被害は、バックドア※1 を埋め込まれてスパムメール配信に悪用されていたものが１件でした。

※1 バックドア（backdoor）：コンピュータへの侵入者が、侵入成功後にそのシステムに再侵入するために準備する仕掛け。いわゆる「裏口」の侵入経路。

（4）被害事例

［なりすまし］

（i）オンラインゲームのアカウントが乗っ取られた

事例	・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ようとしたが、パスワードが勝手に変更されたためログインできない。さらに登録メールアドレスも変更されたため、パスワード再発行の手続きを取れなくなってしまった。 ・実はこのことが起きる以前にも、パスワードがいつの間にか変わっていたことが数回あり、その都度パスワードの再発行処理を行っていた。 ・パスワードを変更したにも関わらず、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。
解説・対策	パスワードを破る手段として、総当り攻撃※2 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考えられます。 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。**

［不正プログラム埋め込み］

（ii）バックドアを仕込まれて、スパムメール送信の踏み台として悪用された

事例	・当校からスパムメールが送信されている、という通報を外部から受けた。 ・調査の結果、校内のパソコン１台がウイルス感染によりバックドアを仕込まれていて、海外へのスパムメール配信の踏み台に悪用されていた。 ・即刻そのパソコンをネットワークから隔離した後、最新の駆除ツールによりウイルスを駆除した。また同一ネットワーク内の全パソコンも同様に確認し、ウイルス感染が拡大していないことを確認した。
解説・対策	**バックドアを仕込まれた場合、目に見える被害（今回はスパムメール配信の踏み台）以外にも何をされているか不明と言えます。**ルートキット※3 を仕込まれた場合に限らず、パソコンにウイルス感染したウイルスは駆除ツールなどでは検知できない場合があるので、パソコンの初期化も検討してください。 スパムメール送信の踏み台や不正中継に悪用されると、ブラックリストに掲載されてしまい、通常業務に支障が出ることもあります。ここでいうブラックリストとは、過去にスパムメール送信に悪用されたことのあるメールサーバーや、メール不正中継可能なメールサーバーの一覧のことです。 一度ブラックリストに掲載されると、特定の宛先にメール送信できなくなることがあります。もしブラックリストに掲載されてしまった場合は、そのリストを掲載しているサイト宛に削除を依頼することになります。 （ご参考） IPA - UBE（迷惑メール）中継対策 http://www.ipa.go.jp/security/ciadr/antirelay.html

※2 総当たり攻撃 ： 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。
※3 ルートキット（rootkit）： 攻撃者がコンピュータに侵入した後に利用するためのソフトウェアをまとめたパッケージのこと。一般的には、ログ改ざんツールやバックドアツール、改ざんされたシステムコマンド群などが含まれる。動作中のプロセスやファイル、システム情報などを不可視化し、これらツール群の存在が利用者に察知されないようになっていることが多い。

4. 相談受付状況

6 月のウイルス・不正アクセス関連相談総件数は **1,097 件**でした。そのうち**『ワンクリック請求』に関する相談**が **319 件**（5 月：243 件）、**『偽セキュリティソフト』**に関する相談が **10 件**（5 月：21 件）、**Winny に関連する相談**が **3 件**（5 月：3 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**（5 月：3 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

		1 月	2 月	3 月	4 月	5 月	6 月
合計		**1,302**	**1,073**	**772**	**750**	**934**	**1,097**
	自動応答システム	760	645	427	428	490	578
	電話	485	362	287	270	363	439
	電子メール	49	62	49	50	78	79
	その他	8	4	9	2	3	1

※ 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。

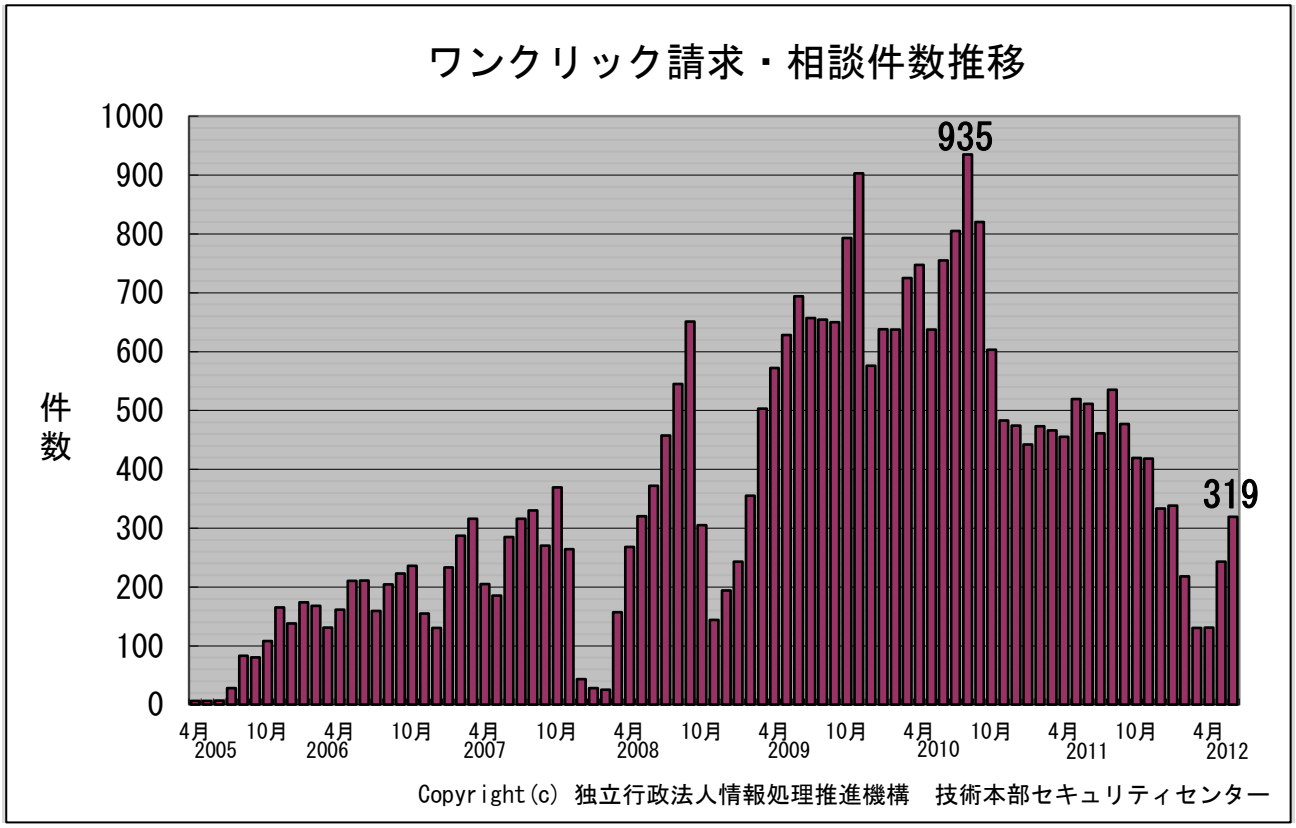

図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）友人からメールが届き、記載の URL をクリックしてしまったが大丈夫でしょうか

相談	私の利用しているフリーメール宛てに、友人から件名は空欄で本文に URL だけが貼ってある不審なメールが届いた。友人が「写真か何かを送ったのだろう」と思いそのURL をクリックしてしまった。ウイルスに感染してしまったでしょうか。
回答	不審なメールが届いたとの事ですが、送信者を知っているなら最初に直接、送信の有無を確認して下さい。ウイルス感染の可能性については、まず**ご利用のウイルス対策ソフトを最新の状態にし全体をスキャン**して下さい。また他社製品の**オンラインスキャンを併用するなど多角的にスキャン**をして下さい。ウイルスが見つかった場合ウイルス対策ソフトでも削除可能ですが、万一を考えると Windows であれば「システムの復元」や「パソコンの初期化」をして下さい。 今後の対策として不審なメールが届いても、安易に URL をクリックしたりしないようにして下さい。 （ご参考） IPA-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

（ii）スマートフォンにおける改造行為とは何でしょうか

相談	スマートフォンを安全に使うための六箇条:「②スマートフォンにおける改造行為を行わない。」　これは、具体的にどのような改造行為のことですか
回答	「スマートフォンにおける改造行為」とはメーカーや携帯会社で元々設定していた権限を改変し、正規ではない OS を入れること等により、これまで出来なかったアプリの導入や操作を実現するような行為のことです。いわゆる iPhone など iOS 端末における「Jailbreak」や Android 端末における「root 権限奪取行為」などのことを指します。 　これらの行為により、利用出来ないアプリが使える様になったり、使えない機能が利用できるようになりますが、元々システムが持っている安全機構がうまく働かないなど大変危険です。また故障しても改造品である為、サポート対象外になることがあります。 **絶対に「スマートフォンにおける改造行為」は行わないようにして下さい。**

『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／青木
Tel:03-5978-7591　Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp