Information-technology
Promotion
Agency, Japan

第 12-04-240 号
2012 年 2 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［2012 年 1 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 1 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

「 スマートフォンでもワンクリック請求に注意！ 」

2012 年 1 月、ウェブサイト閲覧者のパソコンにウイルスを感染させ、アダルトサイトの料金請求画面を貼り付けて消えないようにしたとして、ワンクリック請求を行っていた業者が不正指令電磁的記録供用（いわゆる、コンピューターウイルスの供用）容疑で逮捕されました。

また、同月に、Android OS のスマートフォンで、不正なアプリ（以下、ここでは便宜上、不正なアプリを「ウイルス」と呼びます）を用いて、パソコンのワンクリック請求のように料金請求画面を出し続けるという事例が確認されました。この事例では、ウイルスに感染すると、当該スマートフォンの電話番号やメールアドレスなどの情報が、自動的にワンクリック請求を行っている業者に伝わる仕組みになっていました。こうなると、ワンクリック請求を行っている業者が、ウイルス感染したスマートフォンの所有者にいつでも連絡することができてしまうため、パソコンにおける被害状況と比較し、手口が悪質化しているといえます。

ここでは、このような手口を明らかにするとともに、被害に遭わないための対策を解説します。

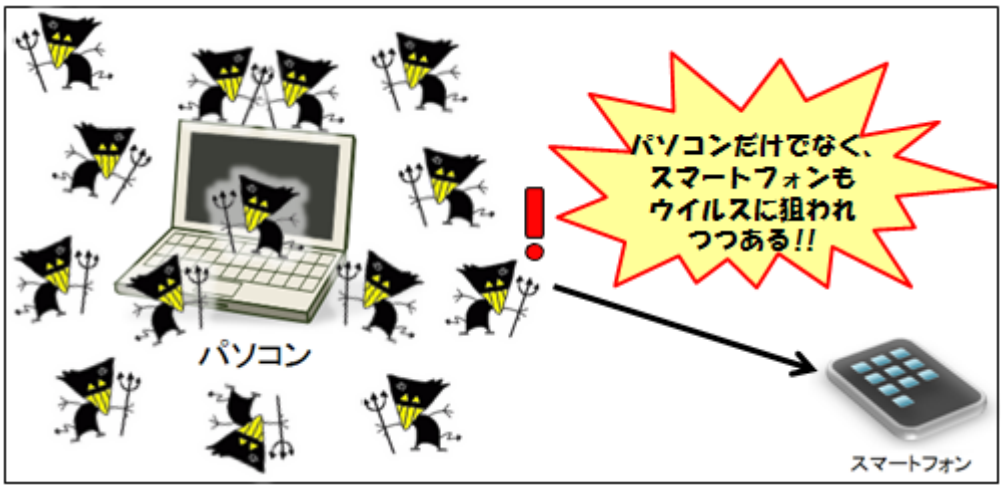

図 1-1：スマートフォンがウイルスに狙われつつあるイメージ図

（1） 実際の被害事例

（i）ワンクリック請求を行うウェブサイトへの誘導の手口

スマートフォン利用者を、ワンクリック請求を行うウェブサイトに誘導する手口としては、以下の方法が考えられます。

- 不特定多数に、当該サイトの URL を掲載した迷惑メールを送り、興味を持ったスマートフォン利用者にアクセスさせて誘導する手口。
- 検索サイトの検索結果の上位に当該サイトを紛れ込ませる SEO（Search Engine Optimization）ポイズニングという手法を使って、特定のキーワードに興味を持ったスマートフォン利用者にアクセスさせて誘導する手口。

（ii）IPA が検証した実際の被害事例

IPA が検証したスマートフォンにウイルスを感染させる手口は、以下の手順で行われていました。ここでは、Android OS を使用している「GALAXY Tab SC-01C（Android OS 2.2）」で確認した画面を元に説明します。

1. まず、（i）に記載したような方法でスマートフォン利用者を、ワンクリック請求を行うウェブサイトの入りロサイトに誘導します（図 1-2）。

図 1-2：ワンクリック請求を行うウェブサイトの入りロ

2. 1.で動画コンテンツにアクセスしようとすると、年齢認証画面に移動します（図 1-3）。
3. 2.で「18 歳以上」のボタンを押すと、「再生専用アプリ」をダウンロードするように促されます（図 1-4）。しかし、ここでダウンロードされるのは再生専用アプリをかたったウイルスです。
4. 3.で「再生専用アプリダウンロード」ボタンを押すと、アプリのファイルがダウンロードされます。このファイルにタッチすると、インストールをブロックした旨の画面が表示されます（図 1-5）。この画面は、使用中のスマートフォンで「提供元不明のアプリ」をインストールしない設定にしている場合に表示されます。

図1－3：年齢認証画面

図1－4：アプリのダウンロード確認画面

図1－5：アプリのインストールをブロックした画面

5. 4.でインストールのブロックを解除するために、「設定」ボタンを押すと、設定変更画面に移動します（図 1-6）。購入時の状態では、「提供元不明のアプリケーションのインストールを許可」の項目にチェックは入っていません。
6. サイトに書かれている「アプリのインストール方法」に従って操作を進めます。5.で「提供元不明のアプリケーションのインストールを許可」の項目にチェックを入れます（図 1-7）。
7. スマートフォンの「戻る」ボタンを押し、先ほどダウンロードしたアプリのファイルをタッチすると、アプリケーションのインストールの確認画面が表示されます（図 1-8）。

図1－6：設定変更画面1

図1－7：設定変更画面2

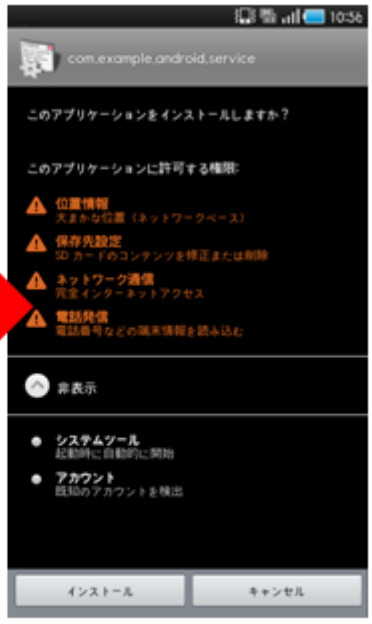

図1－8：インストールの確認画面

図 1-8 に表示されている「このアプリケーションに許可する権限：」の項目を詳しく見てみると、例えば「電話発信」など、動画の「再生専用アプリ」に必要とは思えない不自然な項目があることがわかります（図 1-9）。なお、表示される項目の内容と数は、サイトにアクセスするタイミングや機種によって変化する場合があります。

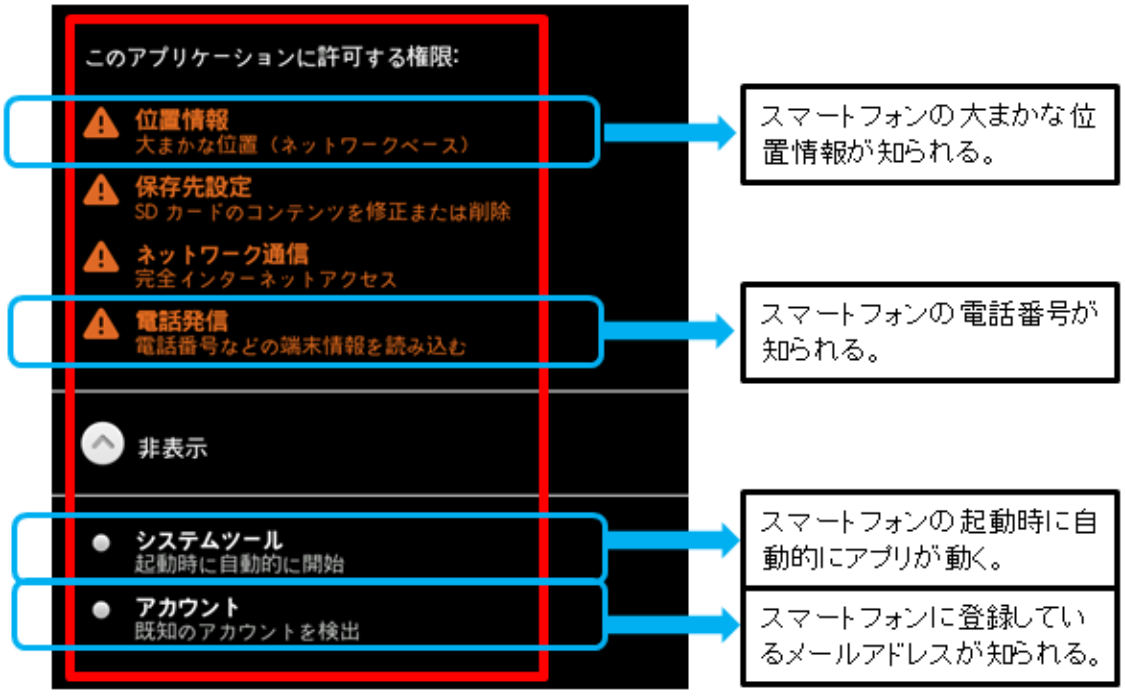

図 1-9：「このアプリケーションに許可する権限：」の表示例

8. 7 で「インストール」ボタンを押すと、アプリのインストールが完了します（図 1-10）。すなわち、ウイルスのインストールが完了したということです。
9. 8 で「開く」ボタンをクリックすると、料金請求の画面が表示されます（図 1-11）。この画面は、ブラウザーを閉じてもしばらくすると勝手に立ち上がります。なお、8.で「完了」ボタンを押したとしても、しばらくするとこの画面が勝手に立ち上がります。
10. 9 で「OK」ボタンを押して、画面の下方向にスクロールすると、ウイルスが感染したスマートフォンの電話番号やメールアドレスが表示されていることがわかります（図 1-12）。この情報は同時に、ワンクリック請求を行っている業者に伝わっています。

図1－10：インストール完了画面

図1－11：料金請求画面1

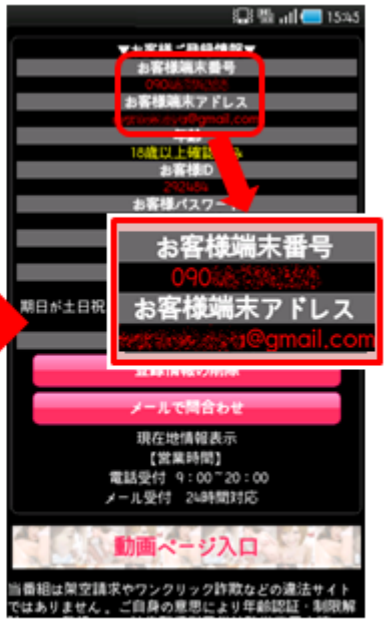

図1－12：料金請求画面2

11. スマートフォンのアプリ一覧画面には先ほどインストールが完了したウイルスアプリのアイコンが追加されていました（図 1-13）。

図 1-13：追加されたアプリのアイコンの表示例

12. 今回検証したスマートフォンに、後日、業者から督促の SMS（Short Message Service）が

届いていました（図 1-14）。SMS は送信相手の電話番号にメッセージを送信するサービスなので、業者に電話番号が伝わっていることは明白です。この場合、業者からの SMS を受け取らないようにするには、各携帯電話会社が提供している SMS 拒否設定機能を利用するか、電話番号を変更するなどの対処が必要になります。

図 1-14：SMS で届いた督促メッセージ例

なお、今回 IPA が確認したウェブサイトは、確認した日の数日後にはウイルスを悪用しないタイプのウェブサイトに変化していました。これは、2012 年 1 月に、**パソコン版のワンクリック請求を行っていた業者が不正指令電磁的記録供用容疑で逮捕されたことで、スマートフォン版のワンクリック請求を行っている業者が警戒したためと思われます。**

今後、ふたたび同様の手口を使うウェブサイトが出現しないとは限りませんので、次項で説明する「ウイルスに感染しないための対策」を、日頃から実施するよう心掛けてください。

（2） ウイルスに感染しないための対策

このようなウイルスに感染しないためには、**パソコンと同様に信頼できない場所からダウンロードしたファイルを不用意にインストールしないことが重要**です。また、以下に示す対策も有効です。

（i）セキュリティアプリを入れておく

スマートフォンにセキュリティアプリを入れて最新の状態に保っておくことで、このようなウイルスの感染を事前に食い止めてくれる場合があります。

（ii）信頼できない場所からアプリをインストールしない設定にしておく

スマートフォンで使用するアプリは、Android 端末であればアプリの審査や不正アプリの排除を実施している場所（米 Google 社の「Android Market」）など信頼できる場所からインストールするようにしてください。そのために、スマートフォンに「提供元不明のアプリ」をインストールしない設定にした状態で使用するようにしてください。どうしても提供元不明のアプリをインストールしなければならないときは、一時的にこの設定を解除して、目的のアプリをインストールしたのち、再度設定を元に戻すことを忘れないでください。

（iii）アプリをインストールする前に、アクセス許可を確認する

アプリをインストールする際に表示される「このアプリケーションに許可する権限：」の一覧には必ず目を通し、不自然な項目や疑問に思う項目の許可を求められた場合には、そのアプリのインストールを中止するようにしてください（図 1-15）。

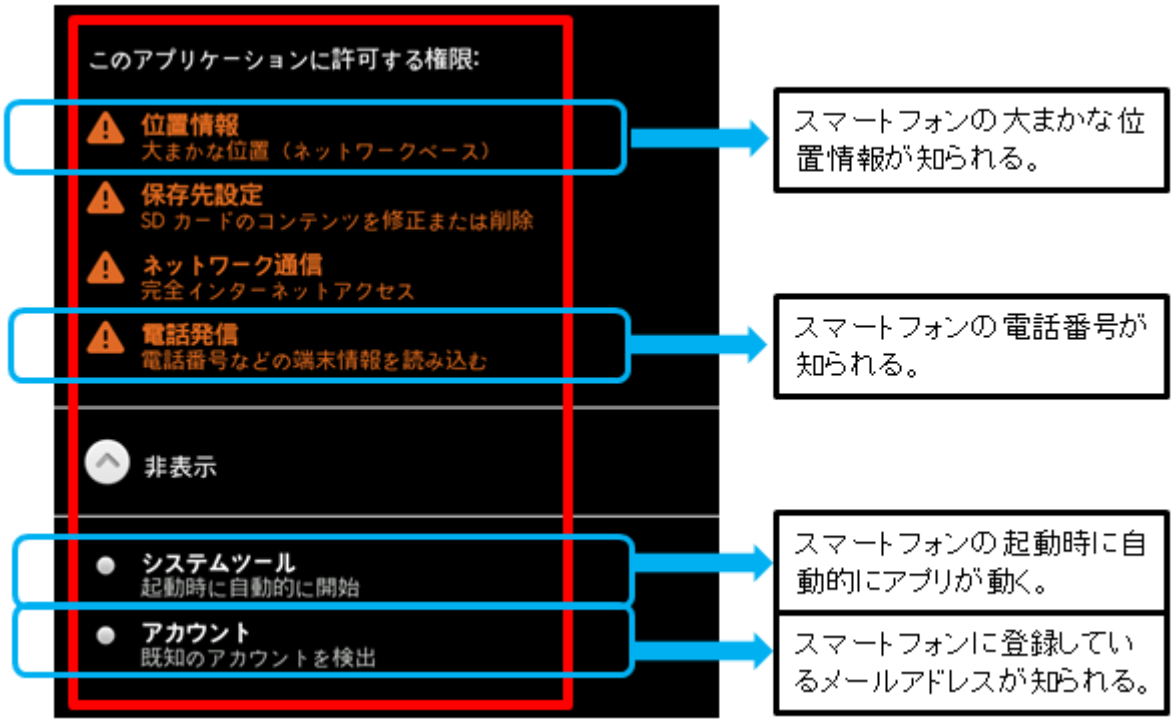

図 1-15：「このアプリケーションに許可する権限：」の表示例

（3） 万がーウイルスに感染してしまった場合の対処方法

万がースマートフォンがこのようなウイルスに感染してしまった場合、**現状ではインストールしたアプリを削除することで、料金請求画面をふたたび表示させないようにすることができます。**

アプリの削除方法は Android OS のバージョンや機種によって異なります。詳細については、お使いの通信キャリアや携帯電話ショップ等にお問い合わせください。

しかし、スマートフォンの電話番号やメールアドレスが伝わっているため、ワンクリック請求を行っている業者から連絡がくる可能性があります。**当該業者から電話やメールで連絡が来たとしても、会話をしたり、メールを返信したりしないでください。それでも執拗に連絡が来る場合は、最寄りの消費生活センターや、警察に相談することをお勧めします。**

（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/
IPA-2011 年 8 月の呼びかけ「スマートフォンを安全に使おう！」
http://www.ipa.go.jp/security/txt/2011/08outline.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、9 頁の「3.コンピュータ不正アクセス届出状況」を参照）
・スパムメール送信の踏み台として悪用されて、メールサーバーがブラックリストに掲載された
・アカウント情報が漏れて、ウェブコンテンツを改ざんされた
○ 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）
・IPA と間違えて別の組織にワンクリック請求の対処を依頼してしまった
・ブラウザーの画面内に常に広告が出るようになった

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

1 月のウイルスの検出数※1 は、**28,459 個**と、12 月の 13,259 個から 114.6%の増加となりました。また、1 月の届出件数※2 は、**941 件**となり、12 月の 764 件から 23.2%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。
・1 月は、寄せられたウイルス検出数 28,459 個を集約した結果、941 件の届出件数となっています。

検出数の 1 位は、**W32/Downad** で **10,812 個**、2 位は **W32/Netsky** で **10,467 個**、3 位は **W32/Mydoom** で **5,158 個**でした。

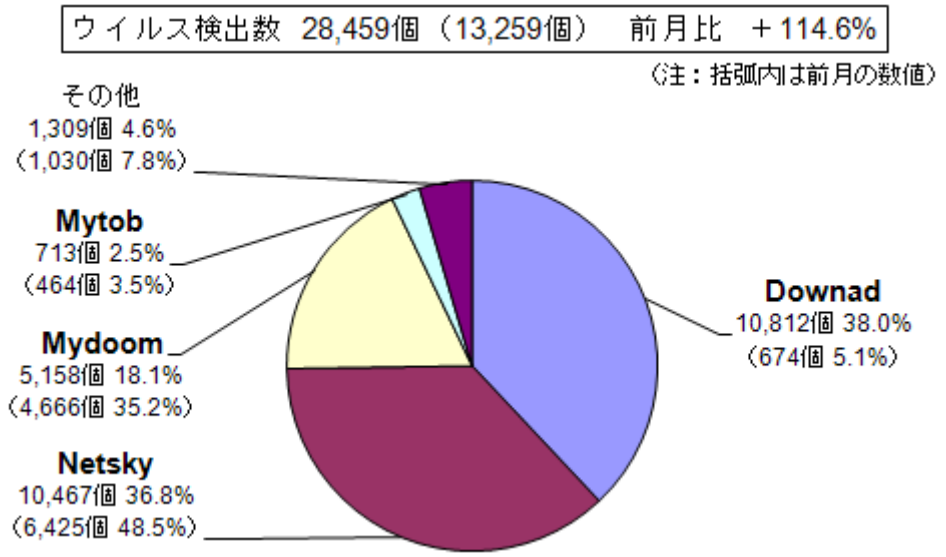

図 2-1：ウイルス検出数

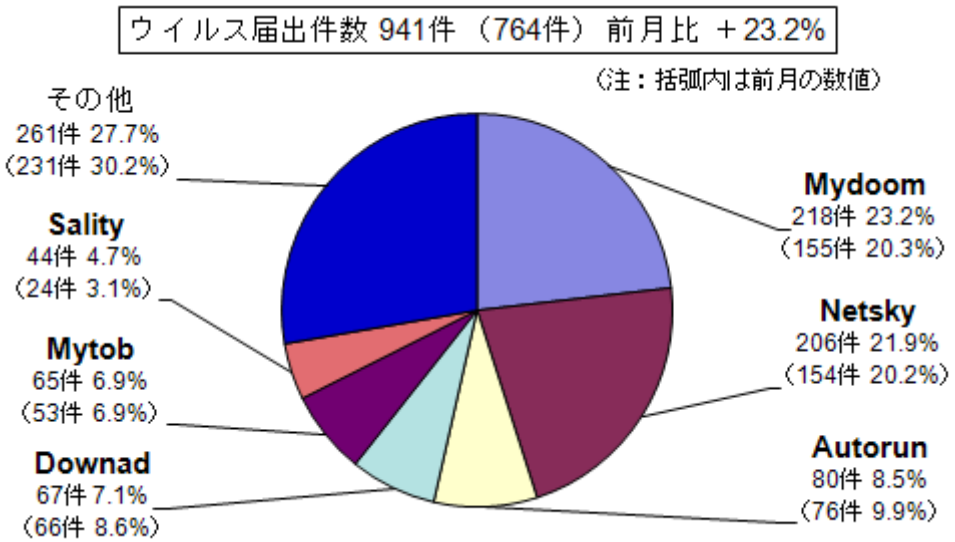

図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

1 月は、オンラインバンキングの ID／パスワードを詐取する BANCOS という不正プログラムが多く検知されました（図 2-3 参照）。また、9 月に大幅に増加した RLTRAP は、1 月の検知数は 7 件だけに留まり、この攻撃は終息したと考えられます。

※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

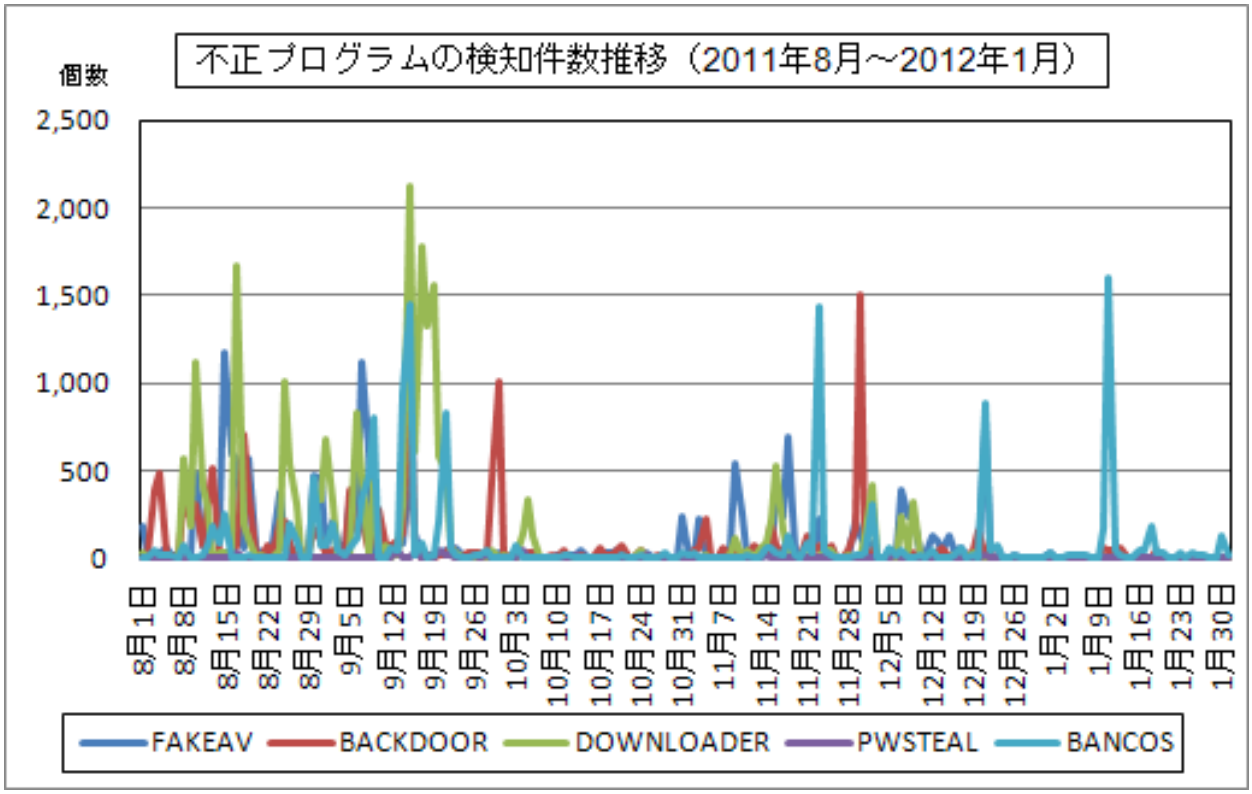

図 2-3：不正プログラムの検知件数推移

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

		8月	9月	10月	11月	12月	1月
届出[a] 計		10	7	15	7	7	8
	被害あり[b]	8	5	8	5	7	7
	被害なし[c]	2	2	7	2	0	1
相談[d] 計		37	31	46	69	42	35
	被害あり[e]	13	8	7	14	13	9
	被害なし[f]	24	23	39	55	29	26
合計[a+d]		47	38	61	76	49	43
	被害あり[b+e]	21	13	15	19	20	16
	被害なし[c+f]	26	25	46	57	29	27

（1）不正アクセス届出状況

１月の届出件数は８件であり、そのうち**何らかの被害のあったものは７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35件であり､そのうち何らかの被害のあった件数は９件でした。

（3）被害状況

被害届出の内訳は、**なりすまし４件、侵入２件、メールの不正中継１件**、でした。

「なりすまし」の被害は、メールアカウント管理不備によりアカウントを使用されてスパムメールを送信されたものが２件、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が１件、などでした。

「侵入」の被害は､コンテンツ管理ツールを悪用されてウェブページを改ざんされていたものが１件、PHP の設定不備を突かれてデータを盗み取られたものが１件、でした。侵入の原因は、脆弱なパスワード設定が１件、PHP の設定不備が１件、でした。

（4）被害事例

［侵入］

（i）スパムメール送信の踏み台として悪用されて、メールサーバーがブラックリストに掲載された

事例	・学内のメールサーバーにおいて、大量の未送信メールが蓄積しエラーが多発していることを発見した。 ・調査すると、スパムメール送信の踏み台としてサーバーが悪用されており、ある学生のメールアドレスから大量のスパムメールが送信されていた。その影響で本学の送信サーバーが一時ブラックリストに掲載され一部の宛先へメール送信ができなくなった。業務に支障の出る職員もいた。 ・当該学生のパスワードが漏えいしたことが原因と考えられる。改めて学生全員に、複雑なパスワードの使用と厳重な管理について注意喚起した。
解説・対策	自身の運営するメールサーバーがスパムメールの送信元や不正中継に悪用されると、今回のケースのようにブラックリストに載ってしまい、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です。 **ブラックリストに掲載されているサーバーからのメールを受信拒否するメールサーバーが存在するので、一度ブラックリストに掲載されると、今回のケースのように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

［侵入］

（ii）アカウント情報が漏れて、ウェブコンテンツを改ざんされた

事例	・「御社のウェブサイトが改ざんされている」との連絡を受けた。 ・確認すると、自社サイトを閲覧した際、強制的に別サイト（中国のハッカー団体と思われるサイト）に移動させられる状態になっていた。 ・Tomcat の管理画面にログインする時のパスワードが推測しやすいものになっており、そこから侵入された可能性が高い。
解説・対策	公開サーバーであれば、通常のアクセスだけではなく、攻撃の意図や悪意のあるアクセスもサーバーに到達するものと想定した対策が必要です。 サイト管理用ツールを社外から利用する運用形態の場合、ログインする時の**パスワードを複雑で推測困難なものにすることが絶対に必要**です。ログイン可能な接続元 IP アドレスを制限することも有効です。 Tomcat に限らず、全ての機能やサービスについて定期的な棚卸しを勧めます。現状にそぐわない設定の修正や、不要な機能の削除など、公開サーバーの管理者は常にセキュリティ向上に努めてください。 （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

4. 相談受付状況

1 月のウイルス・不正アクセス関連相談総件数は **1,302 件**でした。そのうち**『ワンクリック請求』に関する相談**が **338 件**（12 月：333 件）、**『偽セキュリティソフト』**に関する相談が **18 件**（12 月：8 件）、**Winny に関連する相談**が **11 件**（12 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 **4 件**（12 月：6 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

		8月	9月	10月	11月	12月	1月
合計		1,651	1,551	1,496	1,420	1,312	1,302
	自動応答システム	958	936	865	746	790	760
	電話	639	554	564	561	451	485
	電子メール	50	52	55	102	65	49
	その他	4	9	12	11	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。

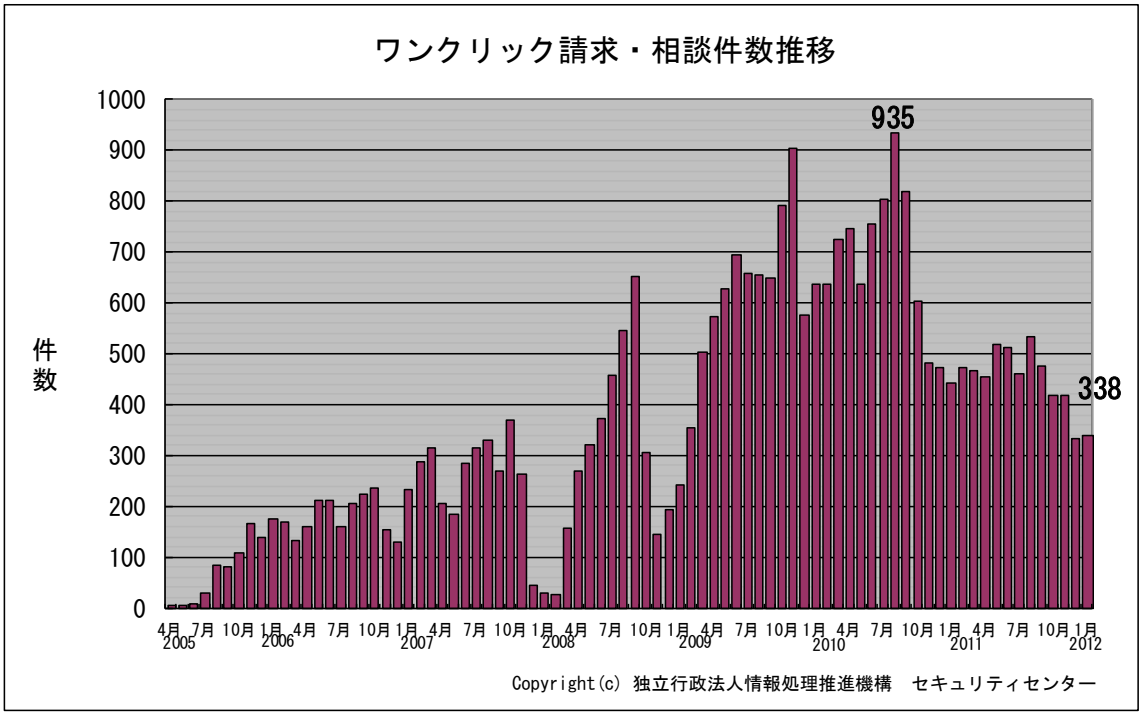

図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）IPA と間違えて別の組織にワンクリック請求の対処を依頼してしまった

相談	パソコン上にアダルトサイトの請求画面が張りついて消えなくなった。 消費生活センターに相談したところ、請求画面を削除する方法については IPA のウェブサイトを参照するように案内されたので、検索サイトで“IPA”を検索して、検索結果の上位に表示されたアドレスを IPA と思い込んでアクセスした。 有料のサービスだったが電話対応してくれそうだったので、指示に従い請求画面を削除することができた。しかし、改めて当該サイトを確認してみたところ、IPA ではなかったことに気付いた。 IPA で検索したはずなのに、一体どういうことなのか。
回答	あなたが対処を依頼した組織は、IPA とは無関係の別の組織です。 **検索サイトでキーワード検索を行う際、必ずしも目的の情報が上位に表示されるとは限りません**。また、**検索サイトによっては、検索結果より上位に広告スポンサーの情報が表示される場合があります**。 検索サイトで目的の情報を探す場合、検索結果に表示されるタイトル、アドレス、説明書きなどを十分確認し､間違った情報にアクセスしないようにしてください。なお、IPA が公開しているワンクリック請求に関する情報については、以下のページを参照してください。 （ご参考） IPA-「【注意喚起】ワンクリック請求に関する相談急増！ パソコン利用者にとっての対策は、まずは手口を知ることから！」 http://www.ipa.go.jp/security/topics/alert20080909.html

（ii）ウェブブラウザーの画面内に常に広告が出るようになった

相談	いつの間にか、ウェブブラウザーの右下隅に広告が表示されるようになった。 さらに、ウェブブラウザーの上部に見知らぬツールバーも表示されていた。 自分で何かダウンロードしたような覚えはない。どうしたら消えるのか。
回答	**お使いのウェブブラウザーに、広告を表示するためのアドオン（プラグインとも呼ばれる）が組み込まれたと考えられます**。 Internet Explorer の場合、「ツール」→「アドオンの管理」で、現在ブラウザーに組み込まれているアドオンを確認できます。その中で該当するアドオンを「無効化」または「削除」することで解決する場合があります。なお、「無効化」「削除」を実施する場合は、誤って必要なアドオンを「無効化」「削除」することの無いよう、注意してください｡不明点がある場合はパソコンの購入店やメーカーに相談することを勧めます。 **アプリケーションやアドオンを導入したタイミングで、同時に別のアドオンも導入されることがあります**。その場合、導入前に確認画面が表示されることがあるので、内容を良く確認し、不必要なものを導入しないよう心掛けてください。 なお、アドオンの中には、Adobe Flash Player のように初めから多くのブラウザーに組み込まれているものがありますが、**アドオンのバージョンが古いと、悪意のあるウェブサイトを閲覧しただけで、アドオンの脆弱性を突かれてウイルス感染してしまう恐れがあります**。 パソコンの脆弱性解消のためにはアプリケーションソフトの更新が重要ですが、アドオンの更新は忘れがちです。アドオンの更新も忘れずに実施してください。 （ご参考） MyJVN バージョンチェッカ http://jvndb.jvn.jp/apis/myjvn/

『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