Information-technology Promotion Agency, Japan

第 12-17-253 号
2012 年 8 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 7 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 7 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

「 コンピュータウイルスや不正アクセスの届出にご協力ください！ 」
～ セキュリティに関する相談も受け付けています ～

IPA は、コンピュータウイルスや不正アクセスの届出機関となっています。多くの皆さまよりいただく相談・届出は、「呼びかけ」や「注意喚起」、「緊急対策」などの情報発信を行うことで、早期の被害拡大防止や再発防止に活かされています。最近の例として、たった一人からの相談を機に調査を開始し関係機関と協力することで、不正な Android アプリの流通を止めたという実績があります。この実例が示すとおり、**一人の一件の相談でも万人の被害防止につながります。**

今月の呼びかけでは、コンピュータウイルスや不正アクセス届出制度に関する目的や活用方法について説明するとともに、届出の方法、相談のコツなどをご紹介します。

皆さまからの一件でも多くの情報提供をお願いします。

（1） コンピュータウイルス・不正アクセス届出制度について

1.ウイルス･不正アクセス届出制度

コンピュータウイルスの届出は、通商産業省（現・経済産業省）のコンピュータウイルス対策基準※1に基づき 1990 年 4 月にスタートした制度です。その後、不正アクセスの届出が 1996 年 8 月に同省のコンピュータ不正アクセス対策基準※2によりスタートしました。両制度の届出機関は、いずれも IPA が指定されています。

IPA では届出の受付業務のほかに、インターネットやコンピュータ、スマートフォンなどにおけるウイルス、不正アクセスの総合的な相談対応を「情報セキュリティ安心相談窓口」で行っています。また受け付けた届出や相談は、提供者のプライバシーに配慮した上で被害等の状況を分析し検討結果を定期的に公表しています。このような活動の主な目的は、被害の予防、発見および被害の拡大・再発防止にあります。

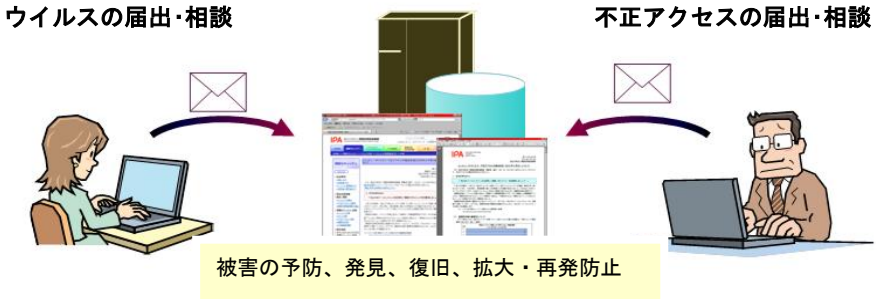

図 1-1：ウイルス・不正アクセス届出制度イメージ図

※1 コンピュータウイルス対策基準
http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm

※2 コンピュータ不正アクセス対策基準
http://www.meti.go.jp/policy/netsecurity/UAaccessCMG.htm

2.ウイルス･不正アクセス届出状況の公表

個人や企業、教育・研究・公的機関などからいただいた届出を分析し毎月公表しています。特に重要な内容については、「今月の呼びかけ」として注意を促し、必要に応じて緊急の「注意喚起」も行います。毎月行う届出の公表では、コンピュータウイルス届出状況、コンピュータ不正アクセス届出状況､相談受付状況の３項目に分けて公表しています｡**コンピュータウイルス届出状況**では、コンピュータウイルスの種類や検出数、届出数、新種ウイルスなどの動向を、**コンピュータ不正アクセス届出状況**では、毎月の届出数と相談数（被害の有無）の動向やその月において被害があった事例（オンラインゲームでのなりすましや不正プログラム埋め込みなど）を紹介しています｡また、**相談受付状況**ではウイルス・不正アクセス関連相談総件数や（ワンクリック請求、偽セキュリティソフト、Winny や不審メール関連などの）主だった相談内訳数、その動向などを紹介しています。

（2） 届出や相談を発端として「呼びかけ」や「注意喚起」を実施した最近の事例

1.ウイルスを使ったフィッシング詐欺の実例（2011 年 10 月の呼びかけ※3）

2011 年 9 月の届出において、これまでのものとは異なるウイルスを組み合わせた新たなフィッシング手法を確認し、同年 10 月に「呼びかけ」を行いました。この事例では、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、というものでした。IPA では実際の偽の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示しました。

※3 ウイルスを使った新しいフィッシング詐欺に注意！（IPA 2011 年 10 月の呼びかけ）

http://www.ipa.go.jp/security/txt/2011/10outline.html

2.Android におけるワンクリック請求の実例（2012 年 2 月の呼びかけ※4）

2012 年 1 月の届出により、Android OS のスマートフォンにおいて、不正なアプリ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、という事例を確認しました。

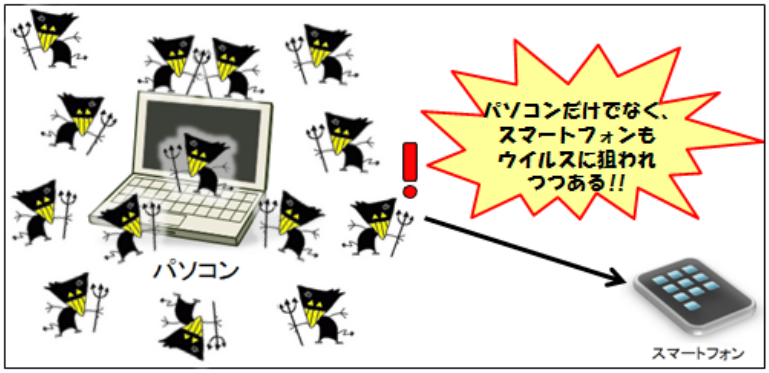

図 1-2：スマートフォンがウイルスに狙われつつあるイメージ図

この事例では、不正アプリをインストールしてしまうと、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者に伝わる仕組みになっていました。この様なしくみは、パソコンにおけるワンクリック請求と比較して悪質なものであり、より被害が出る可能性がありました。そこで同年 2 月の「呼びかけ」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、万一、不正アプリを入れてしまった場合の対処方法などを示しました。

※4 スマートフォンでもワンクリック請求に注意（IPA 2012 年 2 月の呼びかけ）

http://www.ipa.go.jp/security/txt/2012/02outline.html

3.Android の不審なアプリの実例（2012 年 5 月の注意喚起[※5]）

2012 年 4 月に、ある一人の男性から寄せられた相談をきっかけに、不審な動きをする Android アプリが、一般的に利用されているポイント交換サイトで紹介され、多くの人がダウンロードしているという実態を確認しました。その不審なアプリは、スマートフォン利用者が強い興味を抱きそうな名称が使われ、また IPA で解析した結果、そのアプリを実行すると端末情報や、アドレス帳の中身などの個人情報を外部に送信することがわかりました。そのため、悪質な行為に利用される危険性が高いと判断し同年 5 月に、不審なアプリの名称を公開するとともに、その手口を明らかにし、被害に遭わないための対策を示した緊急の注意喚起を実施しました。また、国内のセキュリティベンダーに対し情報を提供し、更に関係機関に連絡したことによって、この不審なアプリは、即日ダウンロードができなくなりました。

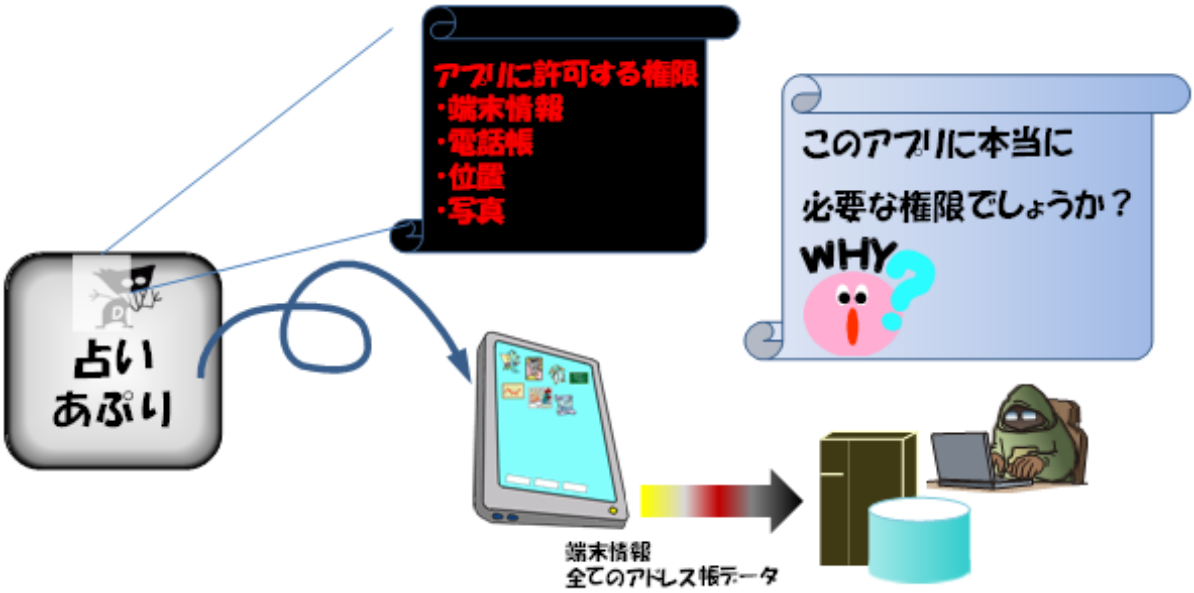

図 1-3：不審なアプリが情報を流出させるイメージ図

※5 Android OS を標的とした不審なアプリに関する注意喚起（IPA 2012 年 5 月の注意喚起）

http://www.ipa.go.jp/security/topics/alert20120523.html

（3）届出、相談の方法について

IPA で受付ける届出の種類としては、コンピュータウイルスに関する届出、不正アクセスに関する届出のほかに脆弱性関連情報※6 の届出があります。コンピュータウイルス、不正アクセスに関する、主に技術的な相談を受け付けています。以下ではウイルス・不正アクセスの届出と相談の活用方法を紹介します。

※6 脆弱性関連情報の届出（IPA）

http://www.ipa.go.jp/security/vuln/report/

1.届出の方法

「コンピュータウイルスに関する届出」および「不正アクセスに関する届出」は、それぞれ専用の届出様式が IPA のウェブページ※7 にあります。届出の際は、少なくとも連絡先と具体的な現象を記載いただき E-mail などで送付してください。内容に応じて、IPA 側から返信させていただき、詳しくおたずねさせていただきます。まずは、届出をご提出いただくことが重要となります。なお、すでに情報が整理できている場合や今までに届出のご提出経験がある方は、届出様式に沿って記入、送付してください。ご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」までお気軽にお問い合わせください。

※7 情報セキュリティに関する届出について（IPA）

http://www.ipa.go.jp/security/todoke/

届出いただく主な内容	**・お届けいただく方の連絡先など** 例：お名前や会社名、電話番号、メールアドレス ・具体的な**状態**（ウイルス名や不正アクセスの内容など） ・届出に至る**経緯**

まずは、ご連絡ください。

	届出先
E-mail	ウイルス届出　　：　virus@ipa.go.jp 不正アクセス届出：　crack@ipa.go.jp ※このメールアドレスに特定電子メールを送信しないでください。
FAX	03-5978-7518
郵送	〒113-6591 東京都文京区本駒込 2-28-8 文京グリーンコート　センターオフィス 16 階 IPA セキュリティセンター「情報セキュリティ安心相談窓口」宛

2.相談について

IPA では「情報セキュリティ安心相談窓口」にて、コンピュータウイルスや不正アクセスについての技術的な相談対応を、下記の時間帯で電話やメールなどで行っています。**ご相談の際は、事前に状況を整理し、できるだけ多くの情報をスムーズにお伝えいただければ、迅速に対応することができます**。ご相談内容に応じて現在の状態の説明や、復旧方法、今後の防止策などをご案内させていただいております。IPA のウェブサイト「情報セキュリティ安心相談窓口」内に記載の「よくある相談と回答（FAQ）※8」もあわせてご覧ください。

※8 よくある相談と回答（FAQ）（IPA）
http://www.ipa.go.jp/security/anshin/

相談の際 お伺いする内容	・オペレーティングシステム（OS）の**種類**や**アップデート状況** 例：Windows **7**、Mac OS**10.××**、Android**2.3.3**、iOS**5.1.1** など 例：自動更新機能による最新の状態、セキュリティパッチの適用状況など ・お使いの**セキュリティソフト名**と定義ファイル**更新状況** ・パソコンにインストールされている主な**アプリケーションのバージョン** 例：Adobe Flash Player、Adobe Reader、Java ・お使いの**ウェブブラウザの種類、PDF ファイル閲覧ソフト等** 例：Internet Explorer 9、PDF は Adobe Reader を使用して閲覧 ・**具体的な状態**（メッセージ、ウイルス名、メールタイトルなど） ・事象が発生したと思われる**要因、日時、きっかけ**など ・ご相談前に行った**対処内容（対策）**

まずは、ご相談ください。

	安心相談窓口の問合せ先
電話	03-5978-7509 （オペレータ対応は、平日の 10:00～12:00 および 13：30～17:00）
E-mail	anshin@ipa.go.jp ※このメールアドレスに特定電子メールを送信しないでください。
FAX	03-5978-7518
郵送	〒113-6591 東京都文京区本駒込 2-28-8 文京グリーンコート　センターオフィス 16 階 IPA セキュリティセンター「情報セキュリティ安心相談窓口」宛

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）

・サーバー管理ツールの脆弱性を悪用されて、ウェブサイトを改ざんされた

・公開を想定していないファイルを参照された

○ 相談の主な事例 （相談受付状況および相談事例の詳細は、12 頁の「4.相談受付状況」を参照）

・パソコンの動きが遅くなったが、どうしたらよいでしょうか

・「現金 1680 万円をもらってください」というメールについて

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

7 月のウイルスの検出数※1 は、**25,487 個**と、6 月の 21,990 個から 15.9%の増加となりました。また、7 月の届出件数※2 は、**877 件**となり、6 月の 958 件から 8.5%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。

検出数の 1 位は、**W32/Mydoom** で **12,115 個**、2 位は **W32/Netsky** で **4,372 個**、3 位は **W32/Mytob** で **2,750 個**でした。

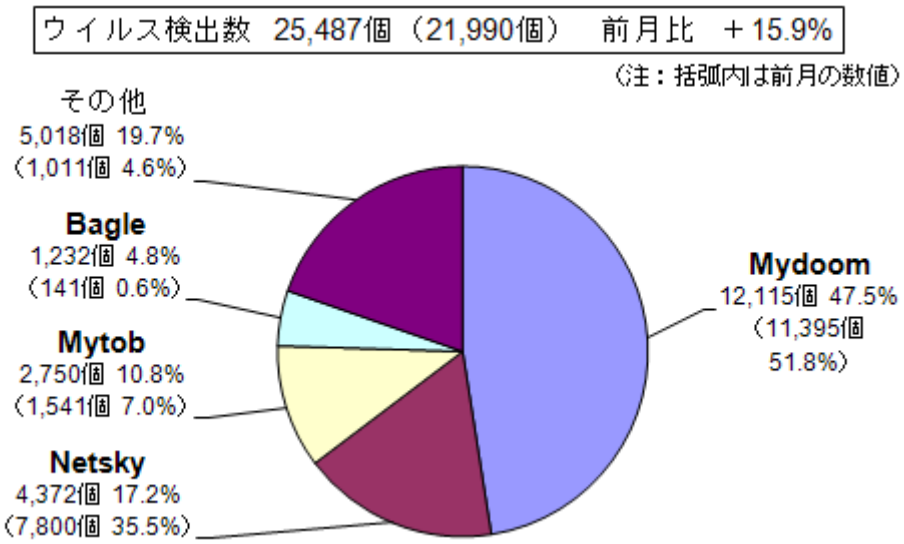

図 2-1：ウイルス検出数

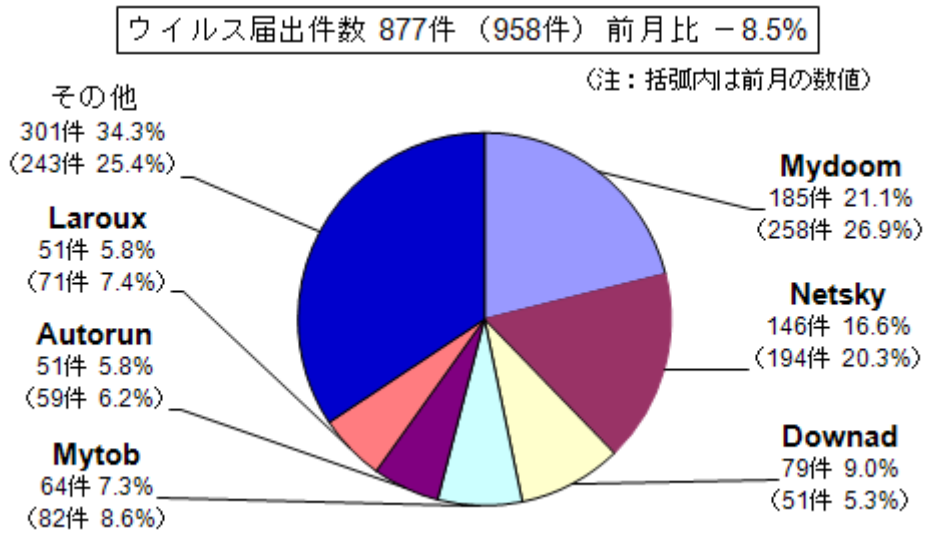

図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

7 月の不正プログラムの検出数※1 は、**100,367 個**と、6 月の 25,399 個から 295.2%の増加となりました。

検出数の 1 位は、広告を表示させるプログラムの総称である **Adware** で **16,042 個**、2 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 **13,326 個**、3 位は、悪意あるスクリプト文が書かれたプログラムの総称である **Malscript** で **5,039 個**、でした。

以下、別のウイルスを感染させようとする Downloader、正規のソフトウェアなどを装って感染を試みる Trojan/Horse、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

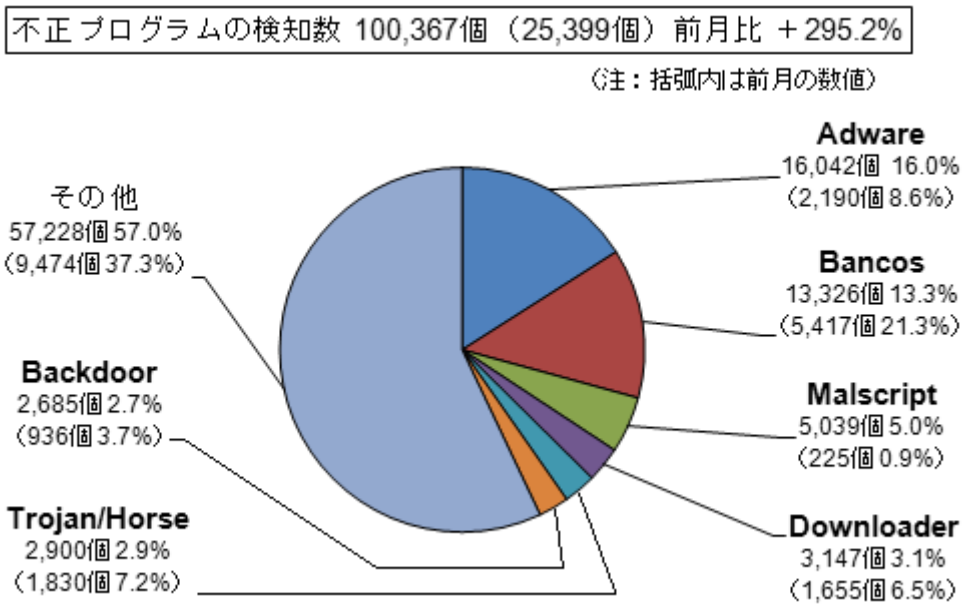

図 2-3：不正プログラムの検知数

7 月は、**Fakeav** の感染被害の届出が大幅に増加しました。こうした「偽セキュリティソフト」型ウイルスの感染被害に遭うと、正常な復旧が困難となる場合がありますので、以下のサイトを参考にして感染被害に遭わないよう、パソコンの対策をお願いいたします。

（ご参考）

「今なお続く、偽の警告を出すウイルスの被害！」（IPA）
http://www.ipa.go.jp/security/txt/2012/03outline.html

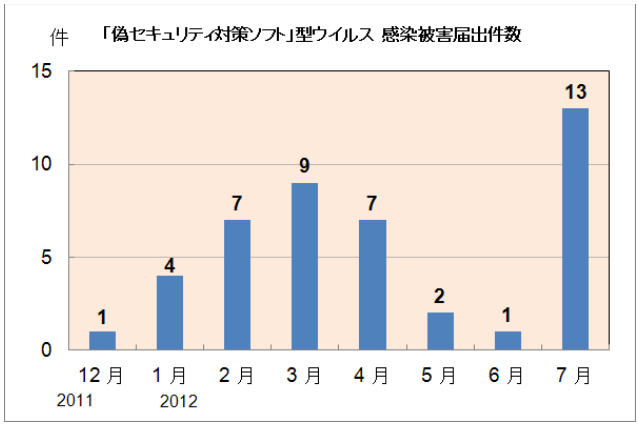

図 2-4：「偽セキュリティ対策ソフト」型ウイルス　感染被害届出件数

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

		2月	3月	4月	5月	6月	7月
届出[a] 計		13	5	9	10	2	19
	被害あり[b]	9	4	7	6	2	18
	被害なし[c]	4	1	2	4	0	1
相談[d] 計		37	54	46	50	38	54
	被害あり[e]	14	10	9	17	12	26
	被害なし[f]	23	44	37	33	26	28
合計[a+d]		50	59	55	60	40	73
	被害あり[b+e]	23	14	16	23	14	44
	被害なし[c+f]	27	45	39	37	26	29

（1）不正アクセス届出状況

7 月の届出件数は 19 件であり、そのうち何らかの**被害のあったものは 18 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54件であり､そのうち何らかの被害のあった件数は26件でした。

（3）被害状況

被害届出の内訳は、**侵入 8 件、なりすまし 4 件、不正プログラム埋め込み 3 件、DoS 攻撃 2 件、その他 1 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 7 件、アカウントを不正に作成されていたものが 1 件、でした。侵入の原因は、サーバー管理ツールやコンテンツマネージメントシステムの脆弱性を悪用されたものが 4 件でした（他は原因不明）。

「なりすまし」の被害は、メールアカウント悪用されてスパムメールを送信されたものが 2 件、ポイント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、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、でした。

（4）被害事例

［なりすまし］

（i）サーバー管理ツールの脆弱性を悪用されて、ウェブサイトを改ざんされた

事例	・当社のウェブサイトを改ざんされて、閲覧者が他サイトに勝手に誘導されるようになっていた。その転送先は不正なサイトで、接続すると不正プログラムをダウンロードさせられるものだった。 ・改ざんの原因は、サーバーを遠隔操作するためのサーバー管理ツールのバージョンが古く、旧バージョンの脆弱性を悪用されたものだった。
解説・対策	当該サーバーを遠隔操作するために作動していた**サーバー管理ツールの脆弱性を悪用**されてことが原因でした。サービスを即座に停止した上で、**最新バージョンに移行**してください。 脆弱性対策のための情報収集として、日頃からレンタルサーバ業者のウェブサイト（レンタルサーバご利用の場合）や、各種ツールやサーバソフトの開発元のウェブサイトなどを確認することを勧めます。 7 月は、「Parallels Plesk Panel」というサーバー管理ツールの脆弱性を悪用された不正アクセスの届出が多く寄せられました。届出が多いということは、実際に攻撃も頻繁に発生していると推測されますので、利用者は注意してください。

［その他］

（ii）公開を想定していないファイルを参照された

事例	・当校のウェブサーバー内の設定ファイルやパスワードファイルを参照するアクセス試行があった。ネットワーク侵入検知監視サービス業者からの連絡で判明。 ・念のためサーバー上の各種設定を確認すると、ウェブコンテンツを格納するディレクトリ以外のファイルに対して参照要求があった時に、許可する場合があることが分かった。 ・ウェブコンテンツ作成業者に即座に修正させるとともに、今後セキュリティ上の対策を講じるよう指示した。
解説・対策	「ディレクトリ・トラバーサル攻撃」を受けた例です。 ウェブアプリケーションにおけるファイル名指定の実装に問題がある場合、攻撃者に任意のファイルを指定され、ウェブアプリケーションが意図しない処理を行ってしまう場合があります。「ディレクトリ・トラバーサル攻撃」とは、この脆弱性を悪用した攻撃手法です。 **この攻撃を受けると、サーバー内のファイルを閲覧・改ざん・削除される恐れがあります。個人情報などの重要情報をウェブサーバー内に保存しているサイトは、特に注意が必要です。** （ご参考） IPA - パス名パラメータの未チェック／ディレクトリ・トラバーサル http://www.ipa.go.jp/security/vuln/vuln_contents/dt.html ウェブアプリケーションにおいて発生し得る脆弱性は、上記以外にも「SQL インジェクション」、「クロスサイトスクリプティング」など多岐にわたります。運営するウェブサイトの状況や性質に合わせて、対策を検討してください。 （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

7 月のウイルス・不正アクセス関連相談総件数は **921 件**でした。そのうち**『ワンクリック請求』に関する相談**が **216 件**（6 月：319 件）、**『偽セキュリティソフト』**に関する相談が **23 件**（6 月：10 件）、**Winny に関連する相談**が **4 件**（6 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 **3 件**（6 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

		2 月	3 月	4 月	5 月	6 月	7 月
合計		**1,073**	**772**	**750**	**934**	**1,097**	**921**
	自動応答システム	645	427	428	490	578	530
	電話	362	287	270	363	439	342
	電子メール	62	49	50	78	79	46
	その他	4	9	2	3	1	3

※ 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。

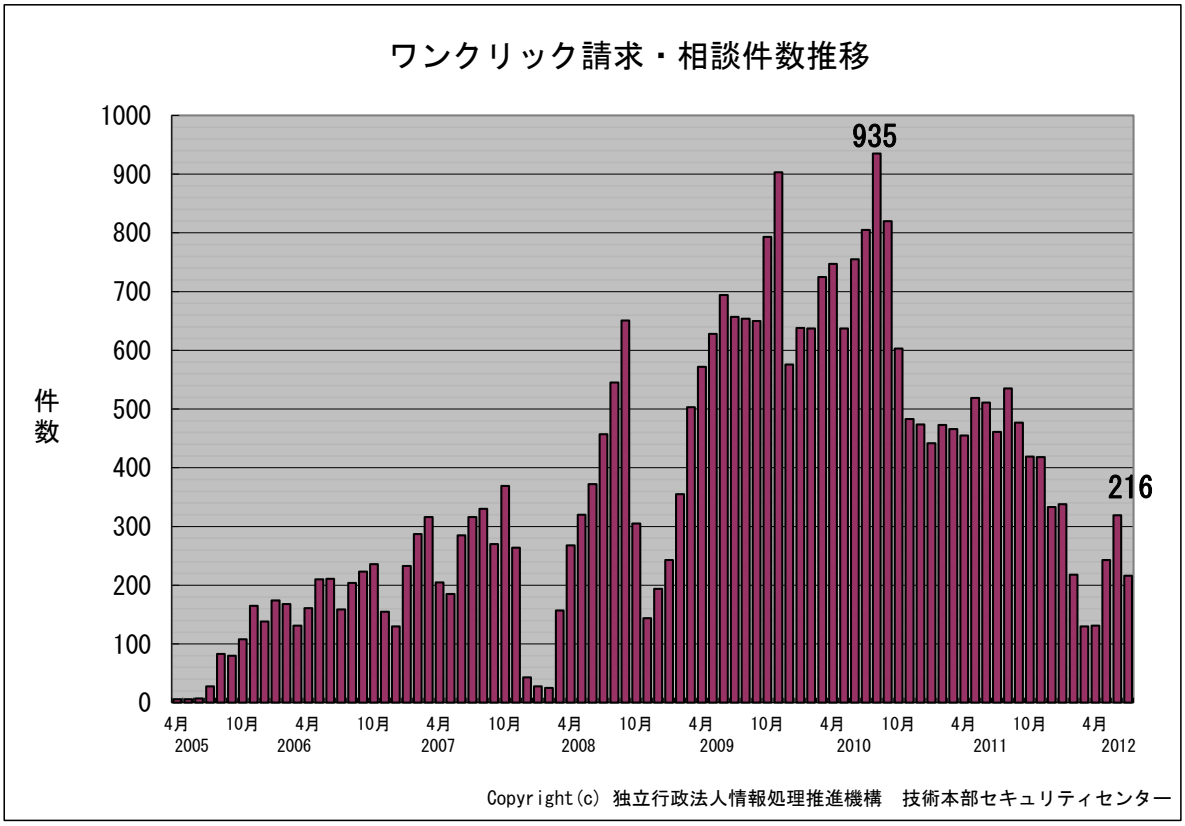

図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）パソコンの動きが遅くなったが、どうしたらよいでしょうか

相談	最近、パソコンの動きが遅くなり、知らない間にツールバーにいろいろ表示されるようになった。どうしたらよいでしょうか。
回答	パソコンの動きが遅いということであれば、**タスクマネージャ**で CPU 使用率の高いアプリを確認するというのも 1 つの方法です。「知らない間にツールバーにいろいろと表示されるようになった」のであれば、これは意図せず何かのソフト（Adware 的なもの）を入れてしまった可能性があります。**「プログラムの追加と削除」や「ブラウザのアドオンの管理」**から、不明なアプリや使用していないアプリが紛れ込んでいないか確認してください。 どのアプリが原因かわからない場合は、パソコンが快適に使えていた時期に戻すために、システムの復元を実施することも有効です。どうしても直らない場合は、システムの初期化も検討してください。修復後は、忘れずに OS やご利用アプリのアップデートのほか、セキュリティソフトのウイルス定義ファイルを常に最新化してください。 （ご参考） IPA-MyJVN バージョンチェッカ http://jvndb.jvn.jp/apis/myjvn/

（ii）「現金 1680 万円をもらってください」というメールについて

相談	昨日から突然「現金をあげる」というメールが頻繁に届くようになりました。最初に届いたのは「現金 1680 万円の準備が完了しました。こちらに返信ください。」というメールでした。メールの内容は一貫して「お金を受け取ってほしい」という内容で、一番下に会社らしき名称の記載がある。気になるので返信したいのですが、これは本当の話でしょうか？
回答	これは、よくある**迷惑メール**です。最初にメール受信者に興味を抱かせ、出会い系サイトに勧誘し、メール交換をもちかけることによって、高額な利用料を支払わせる手口であることが多いです。 一般に、このような**おいしい話は世の中にありません。**一度よく冷静に考えてみるとわかるでしょう。 今後もメールが絶えず来て迷惑な場合は、メールソフトやプロバイダなどの**フィルタリング機能**を利用することや、場合によってはメールアドレス変更などもご検討ください。あまりにも、多く届く場合は「迷惑メール相談センター 」に相談してください。 （ご参考） 財団法人 日本データ通信協会　迷惑メール相談センター http://www.dekyo.or.jp/soudan/ihan/

『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