Information-technology Promotion Agency, Japan

第 12-12-248 号
2012 年 6 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［2012 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、2012 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

「 ソフトウェアの自動更新を利用しましょう！ 」
～MyJVN バージョンチェッカとの合わせ技で、ウイルス対策をより強固に！～

昨今、よく使われるウイルス感染の手口としてドライブ・バイ・ダウンロード攻撃※1があります。これは、OS やアプリケーションなどのソフトウェアが最新のバージョンではないパソコンの利用者が、ウイルスや不正プログラムを感染させる仕掛けが施されたウェブサイトを閲覧した時に、ウイルス感染の被害に遭うというものです。

最近では、「偽セキュリティ対策ソフト」型ウイルスを感染させる手口※2 としても多く使われていますが、**このウイルスの感染被害に遭ったパソコン利用者の多くは、ソフトウェアの更新をしていなかった**ことが確認されています。

IPA の調査※3 では、ソフトウェアの更新について「更新方法が分からない」、「手間がかかる」いった意見が多くみられました。また、定期的に更新をしていても、「更新が頻繁でいつ最新版が公開されたか分からない」といった相談もよせられています。

IPA ではそのような意見をふまえ、複数のソフトウェアのバージョン情報を同時に、簡単に調べることができ、更新に必要な詳細情報を表示する「MyJVN バージョンチェッカ」※4 を無償で公開しており、これと併用して「ソフトウェアの自動更新」の利用をおすすめしています。一度設定を行えば、定期的にソフトウェアの最新バージョンを確認し、最新バージョンがあれば更新を促す機能です。

今月の呼びかけでは、更新頻度が高いソフトウェアである Windows、Java、Flash Player、Adobe Reader の 4 つについて、「ソフトウェアの自動更新」の設定方法を説明します。

図 1-1：ソフトウェアの自動更新のイメージ図

※1 「ウェブサイトを閲覧しただけでウイルスに感染させられる"ドライブ・バイ・ダウンロード"攻撃に注意しましょう！」（IPA　2010 年 12 月の呼びかけ）

http://www.ipa.go.jp/security/txt/2010/12outline.html

※2 「今なお続く、偽の警告を出すウイルスの被害！」（IPA　2012 年 3 月の呼びかけ）
http://www.ipa.go.jp/security/txt/2012/03outline.html

※3 「2011 年度 情報セキュリティの脅威に対する意識調査」報告書
http://www.ipa.go.jp/security/fy23/reports/ishiki/

※4 「MyJVN バージョンチェッカを活用して脆弱性を解消しましょう！」（IPA　2012 年 4 月の呼びかけ）
http://www.ipa.go.jp/security/txt/2012/04outline.html

（1） ソフトウェアの自動更新の必要性

ソフトウェアの自動更新を行う必要性の説明として、主に次の 2 項目が挙げられます。

●**ソフトウェアのセキュリティ上の問題箇所である脆弱（ぜいじゃく）性を迅速に解消するため**

ソフトウェアを古いバージョンのまま使用することは、**ソフトウェアを脆弱性のある状態で使用する**ことになりかねません。最近のウイルスは、**この脆弱性を悪用してパソコンに感染被害を与えます。**こうした被害に遭わないためには、脆弱性が解消されている最新バージョンのソフトウェアを使わなければなりません。

最近では、新しい脆弱性情報が公表されるとそれを悪用したウイルスもすぐに出現しています。**面倒だからと言って最新バージョンへの更新を後回しにしていると、そうしたウイルスに感染する可能性があります。**

●**ソフトウェアの更新が不定期かつ頻繁なため**

定期的に更新が行われているソフトウェアも、**定例以外のタイミングで最新版が公開される場合があります。**また、**不定期かつ毎月のように最新版が公開されるソフトウェアもあります**ので、最新の更新情報に注意を払う必要があります。

更新をしていないパソコンを狙ったウイルス感染の手口として、主に次の 2 種類が挙げられます。

●**ウェブサイト閲覧からウイルス感染**

ウェブサイトを閲覧しただけで、パソコン利用者の意図に関わらず、ウイルスなどの不正プログラムをパソコンにダウンロードさせる手法であるドライブ・バイ・ダウンロード攻撃により、ウイルスを感染させます。IPA によせられた同じ攻撃手口による最近の感染被害相談では、「偽セキュリティ対策ソフト」型ウイルスが多く見られました。

●**メールの添付ファイルからウイルス感染**

脆弱性を悪用するウイルス入りのファイルを添付したメールを送りつけ、添付ファイルを開かせて感染させます。最近では、関係機関や関係者を装い、組織や個人に狙いを絞ってウイルスを送りつける「標的型攻撃メール」も多くなっています。

図 1-2：パソコン利用者を狙ったウイルス感染攻撃のイメージ図

こうしたウイルス感染が元となり、不正アクセスや情報漏えい、ネットバンキングやインターネットサービスの不正利用、さらには悪意のある者に勝手に操作され、他のパソコンを攻撃するために使われてしまうことも考えられます。

このように、ウイルスの感染被害に遭わないようにするには、ソフトウェアの更新が非常に大事ですが、更新作業が面倒で更新を行っていない、というパソコン利用者は少なくありません。そのような利用者は、「ソフトウェアの自動更新」を設定してください。

(2) 設定方法

以下に、Windows 7 を例として各ソフトウェアの自動更新の設定方法を記します。

※ Windows XP 及び Vista の設定方法は下記サイトを参照してください。
ソフトウェアの自動更新の設定方法（IPA）
http://www.ipa.go.jp/security/anshin/faq/faq-9-3.html

a. Windows の自動更新

1. ［スタート］ボタンをクリックして［コントロールパネル］をクリックします。［コントロールパネル］が見当たらない場合は、［スタート］ボタンから［プログラムとファイルの検索］にカタカナで“コントロール”と入力して Enter キーを押してください。カテゴリ表示（図 1-3）の場合は、［システムとセキュリティ］をクリックすると、［システムとセキュリティ］画面が表示されます（図 1-4 参照）。

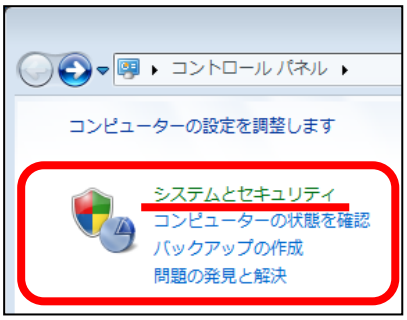

図 1-3：Windows 7　コントロールパネル　カテゴリ画面

2. ［Windows Update］項目の“自動更新の有効化または無効化”をクリックすると、［設定の変更］画面が表示されます（図 1-5 参照）。

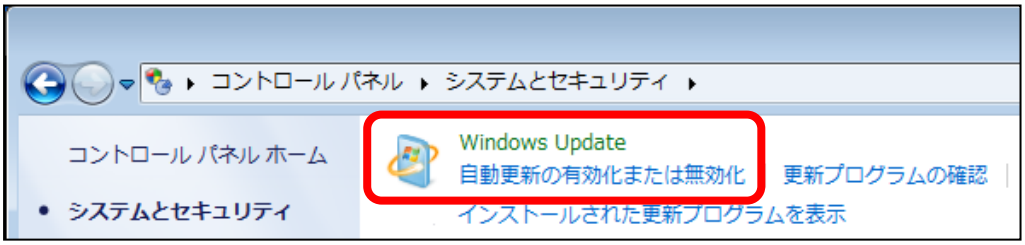

図 1-4：Windows 7　システムとセキュリティ画面

3.［重要な更新プログラム］項目を、“更新プログラムを自動的にインストールする（推奨）”に変更して、更新曜日と時刻を設定します（図 1-5）。

図 1-5：Windows 7　設定の変更画面

b. <u>Java（JRE）の自動更新</u>

1.［スタート］－［コントロールパネル］より、［プログラム］をクリック（図 1-6）すると、［プログラム］画面が表示されます（図 1-7 参照）。

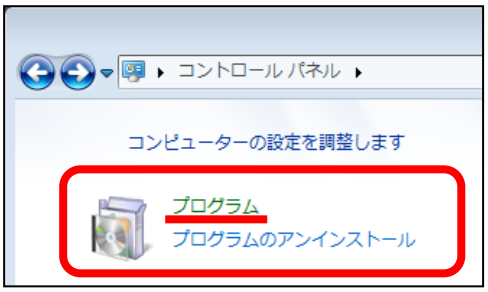

図 1-6：Windows 7　コントロールパネル　カテゴリ画面

2.［Java］アイコンをクリックすると、［Java コントロールパネル］画面が表示されます（図 1-8 参照）。

※Java がインストールされていない場合、［Java］アイコンは表示されません。

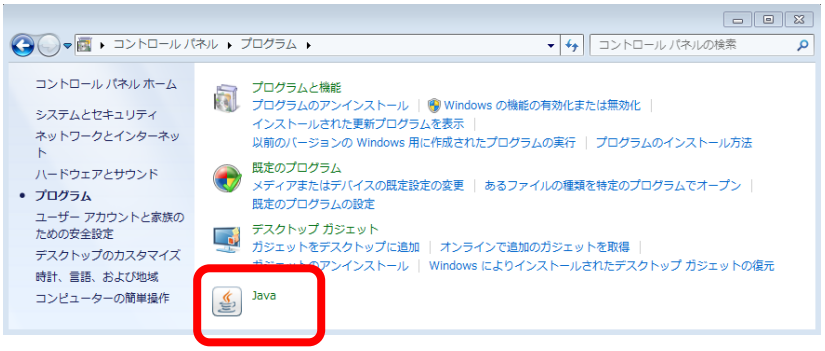

図 1-7：Windows 7　プログラム画面

3.Java コントロールパネル画面の、“更新”タブをクリックして、“更新を自動的にチェック”にチェックを入れます。次に、［拡張］ボタンをクリックすると、更新頻度と曜日・時刻の設定が行えます。設定後は、［OK］ボタンをクリックして内容を保存します。

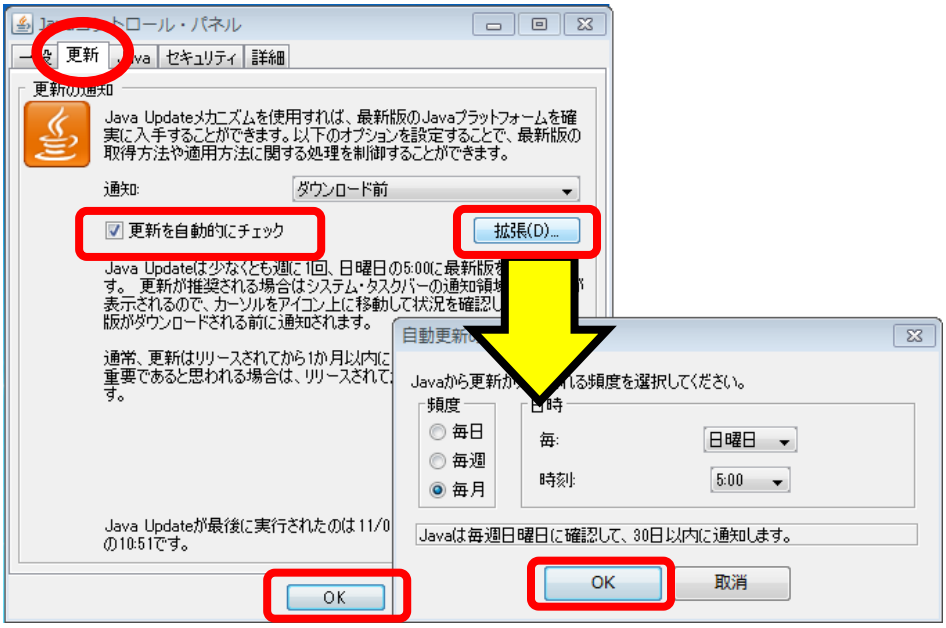

図 1-8：Java コントロールパネル

c. Flash Player の自動更新

1.［スタート］－［コントロールパネル］より、［システムとセキュリティ］をクリック（図 1-9）すると、［システムとセキュリティ］画面が表示されます（図 1-10 参照）。

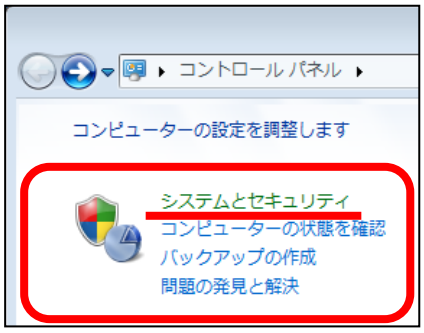

図 1-9：Windows 7　コントロールパネル　カテゴリ画面

2.［Flash Player］アイコンをクリックすると、［Flash Player 設定マネージャー］画面が表示されます（図 1-11 参照）。

※Flash Player がインストールされていない場合、［Flash Player］アイコンは表示されません。

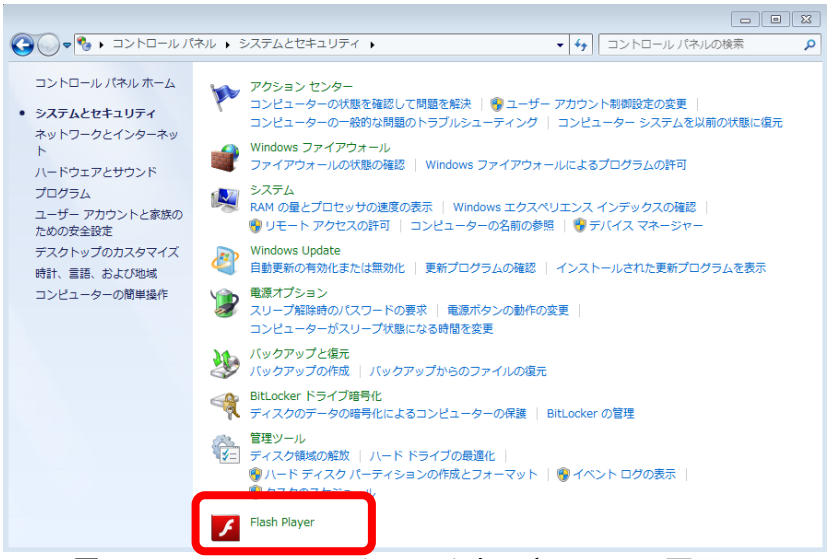

図 1-10：Windows 7　システムとセキュリティ画面

3.Flash Player 設定マネージャー画面の、“高度な設定”タブをクリックして、“アップデートがある場合に自動的にインストールする（推奨）”を選択します。設定後は、画面右上の×ボタンをクリックして設定を終了します。

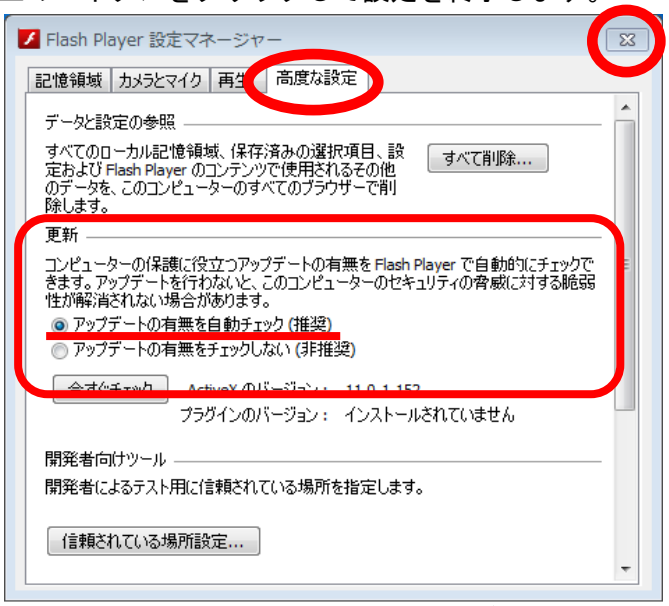

図 1-11：Flash Player 設定マネージャー画面

d. Adobe Reader の自動設定

※Adobe Reader の自動更新機能は、バージョン 9.3.2 から使えるようになっています。なお、今回の参照画面はバージョン 10.1.3 を使用しています。

1.Adobe Reader を起動して、メニューバーの“編集”－“環境設定”をクリックします。

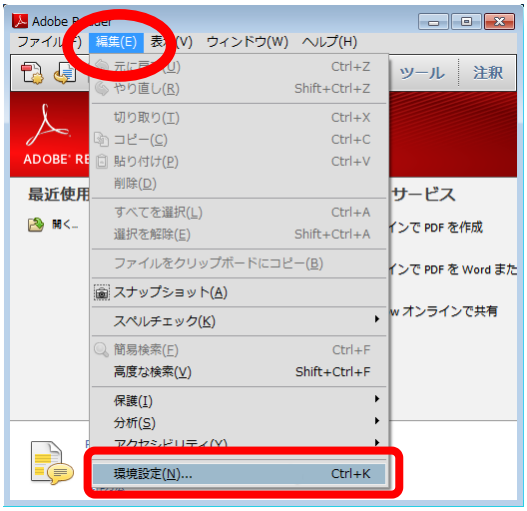

図 1-12：Adobe Reader　起動画面

2.［環境設定］画面が表示されたら、“アップデーター”を選択して、“自動的にアップデートをインストールする”を選択します。

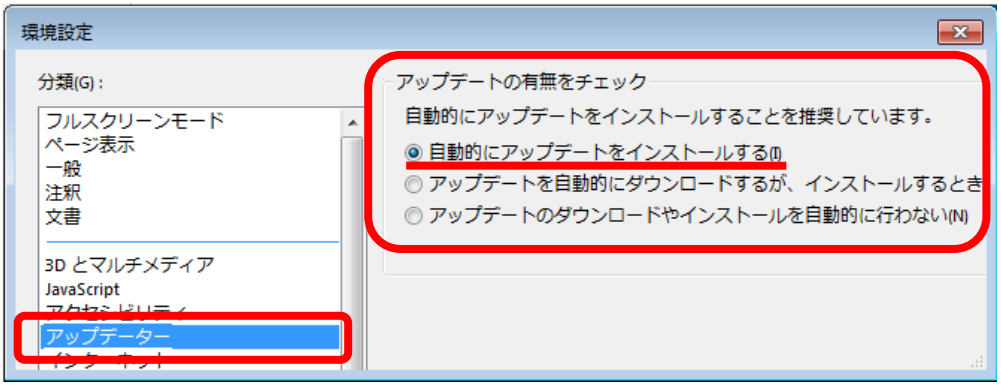

図 1-13：Adobe Reader　環境設定画面

（3） 設定の注意

各ソフトウェアの自動更新を設定するにあたり、次の点に注意してください。

- パソコンの動作が遅くなる場合がある
  ソフトウェアの自動更新中は、パソコンの動作が遅くなる場合があります。自動更新のタイミングを設定可能な場合は、動作に影響が生じない時刻を選んでください。
- 自動更新の設定ができない場合がある
  企業・組織でお使いのパソコンでは、自動更新の設定を個々人に行わせないようにしている場合があります。自動更新設定の可否については、システム管理者やパソコン管理者に確認してください。

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、10 頁の「3.コンピュータ不正アクセス届出状況」を参照）
・古いメールアカウントを不正使用され、大量のスパムメールを送信された
・突然、オンラインゲームにログインできなくなった

○ 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）
・ノートパソコンに USB メモリを挿したまま使用しても大丈夫か
・スマートフォンにおけるアプリケーションのインストールについて

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

5 月のウイルスの検出数※1 は、**20,236 個**と、4 月の 10,339 個から 95.7%の増加となりました。また、5 月の届出件数※2 は、**970 件**となり、4 月の 732 件から 32.5%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。
・5 月は、寄せられたウイルス検出数 20,236 個を集約した結果、970 件の届出件数となっています。

検出数の 1 位は、**W32/Mydoom** で **9,688 個**、2 位は **W32/Netsky** で **7,934 個**、3 位は **W32/Mytob** で **1,190 個**でした。

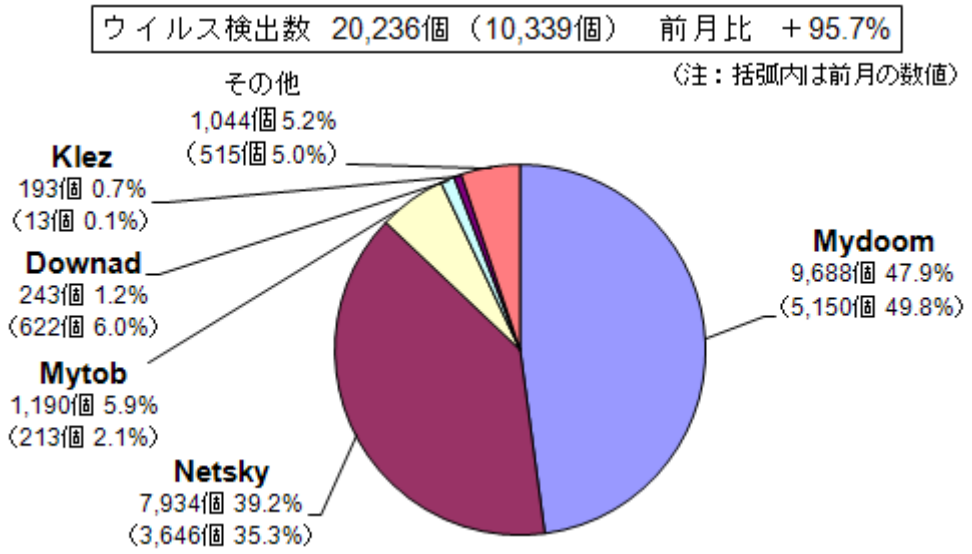

図 2-1：ウイルス検出数

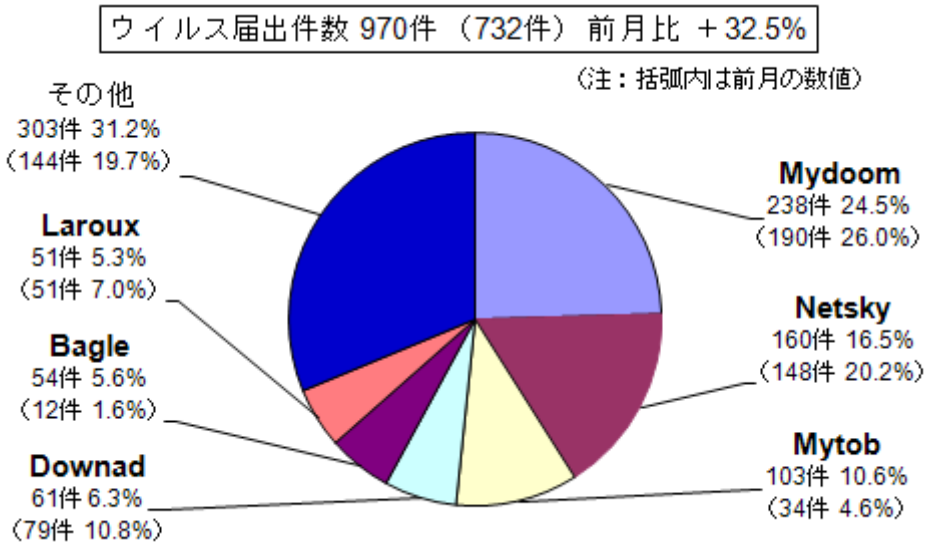

図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

5 月は、特に目立った動きはありませんでした（図 2-3 参照）。

※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

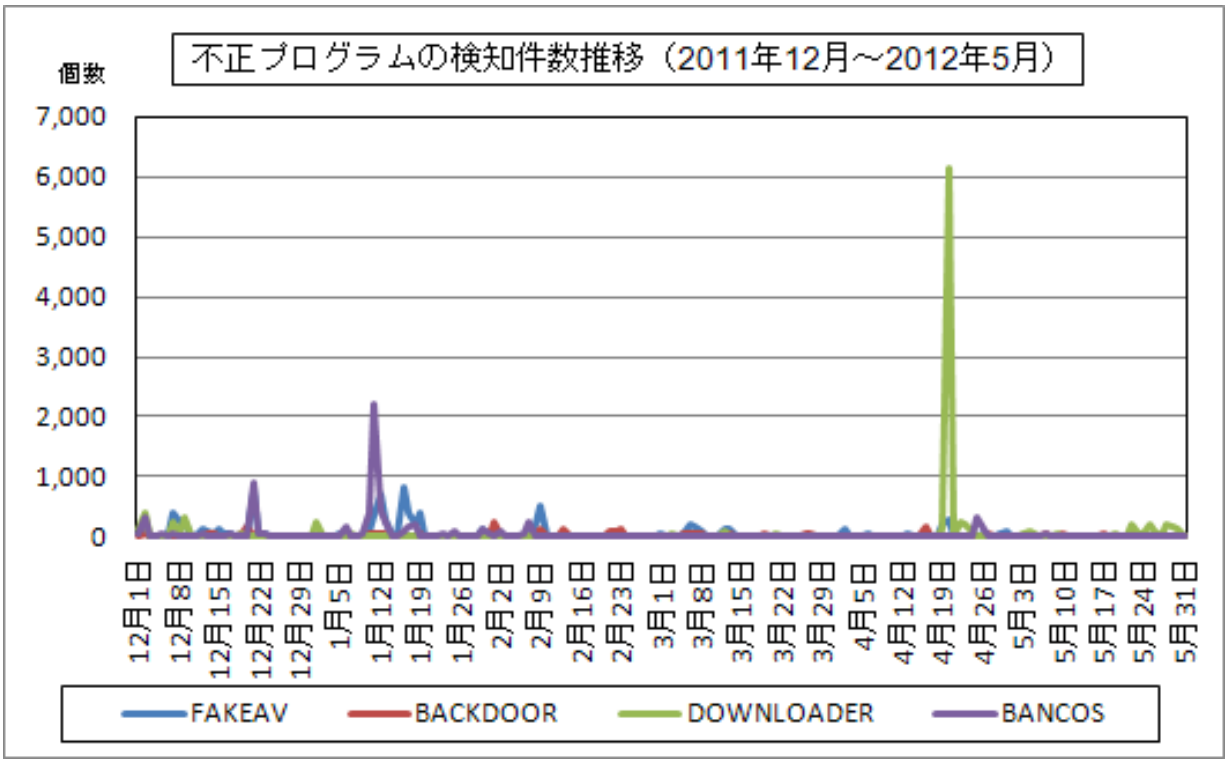

図 2-3：不正プログラムの検知件数推移

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

		12月	1月	2月	3月	4月	5月
届出[a] 計		7	8	13	5	9	10
	被害あり[b]	7	7	9	4	7	6
	被害なし[c]	0	1	4	1	2	4
相談[d] 計		42	35	37	54	46	50
	被害あり[e]	13	9	14	10	9	17
	被害なし[f]	29	26	23	44	37	33
合計[a+d]		49	43	50	59	55	60
	被害あり[b+e]	20	16	23	14	16	23
	被害なし[c+f]	29	27	27	45	39	37

（1）不正アクセス届出状況

５月の届出件数は 10 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50件であり､そのうち何らかの被害のあった件数は17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２件、不正プログラム埋め込み２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２件でした。侵入の原因は、サーバー管理ツールの脆弱性を悪用されたものが１件でした（他は原因不明）。

「なりすまし」の被害は、スパム配信として悪用されていたものが１件、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。

（4）被害事例

［なりすまし］

（i）古いメールアカウントを不正使用され、大量のスパムメールを送信された

事例	・当社（ISP 事業者）の利用者向けに提供しているメールサービスにおいて、一部の利用者から大量のスパムメールが送信された。 ・調査の結果、スパムメール送信に悪用されたアカウントはいずれも古いアカウントで、長期間パスワードが変更されていなかった。 ・原因調査の一環として、当社への攻撃や情報漏えいについても調査したが、現状その痕跡は見つかっていない。従って、利用者のパスワード管理不備もしくはパスワードクラックによるものと推測している。
解説・対策	**長期間パスワードが変更されていないメールアカウントは、不正使用目的で狙われやすくなります。** メールアカウントについては、不正アクセス対策のためシステム上である程度長く複雑なパスワードしか設定できないように強制することが必須ですが、万一パスワードを不正使用されても被害を最小限に抑えるために、定期的にパスワード変更を強制させるシステムにすることも有効です。一定期間ログインのないアカウントを一時的に無効化することも対策になります。 古いアカウントがそのまま残っていると悪用される恐れがあります。特に学校など、定期的に人員が入れ替わる組織の場合は、年度の節目などでアカウントの棚卸をすることを勧めます。

［なりすまし］

（ii）突然、オンラインゲームにログインできなくなった

事例	・ある日突然、オンラインゲームへのログインができなくなった。 ・原因は不明だが、何者かに不正にアクセスをされ、パスワードを変更されたと考えられる。 ・ログインできないので、自分のキャラクターが現在どうなっているかすら分からない状況。 ・こうしたなりすまし行為に対してはどうしたら良いのか。警察に被害届を出すと受理してくれるのか？
解説・対策	自分では気がつかないうちに、他人にアカウント情報が知られてしまったと考えられます。アカウント情報は、他人に教えないのは当然ですが、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もあります。面倒でも、**サービスごとに ID とパスワードを変更することを勧めます**。 被害届の提出は、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。 （ご参考） 「あなたの知らないうちに ID、パスワードが盗まれています！」（日本オンラインゲーム協会） http://www.japanonlinegame.org/ss/index.html 「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/

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 **934 件**でした。そのうち**『ワンクリック請求』に関する相談**が **243 件**（4 月：131 件）、**『偽セキュリティソフト』**に関する相談が **21 件**（4 月：26 件）、**Winny に関連する相談**が **3 件**（4 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 **3 件**（4 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

		12 月	1 月	2 月	3 月	4 月	5 月
合計		**1,312**	**1,302**	**1,073**	**772**	**750**	**934**
	自動応答システム	790	760	645	427	428	490
	電話	451	485	362	287	270	363
	電子メール	65	49	62	49	50	78
	その他	6	8	4	9	2	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。

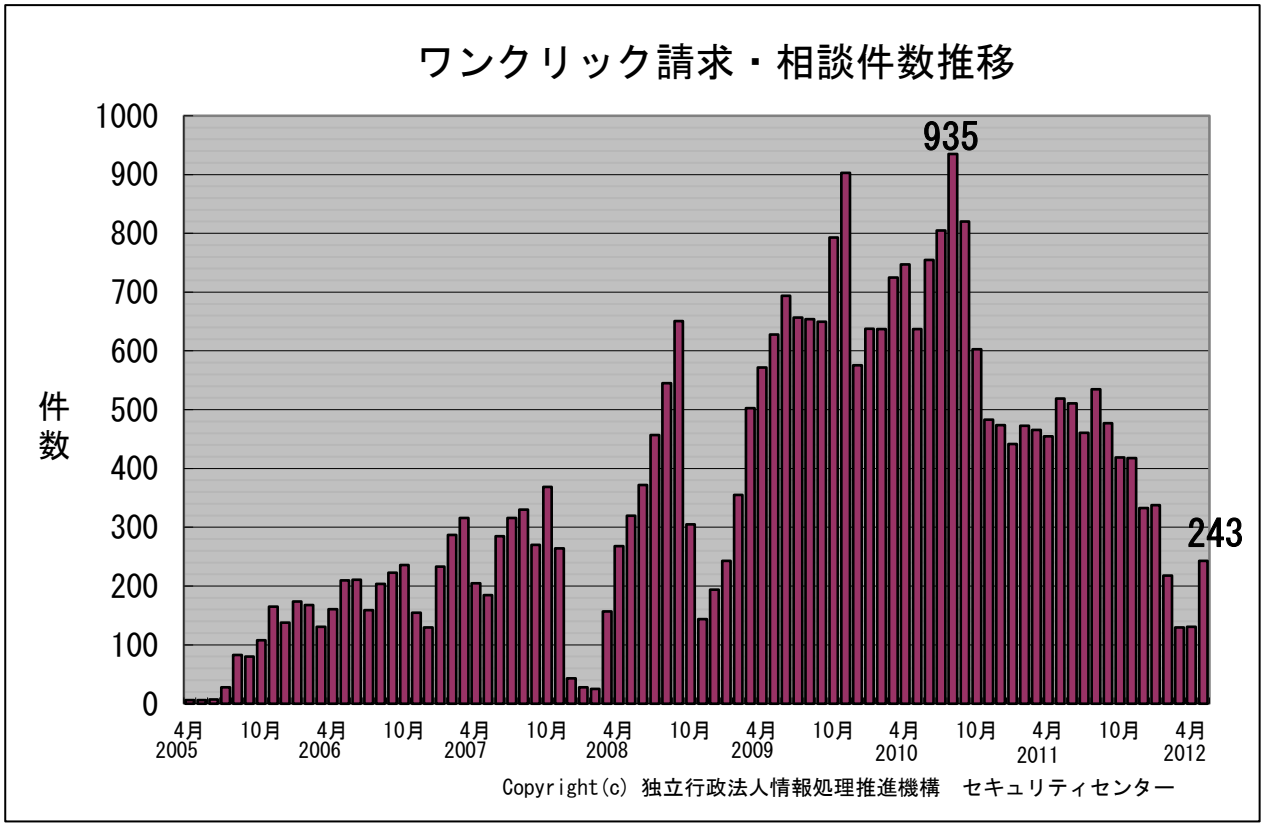

図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）ノートパソコンに USB メモリを挿したまま使用しても大丈夫か

相談	ノートパソコンを利用しているが、いつも USB メモリを挿したままの状態でインターネットにつないだり、文書作成ソフトのアップデートを行ったりしている。この場合、ウイルス感染などで USB メモリのデータが外部に流出してしまう恐れはあるのか。
回答	データを外部に流出させるウイルスに感染した場合は、C ドライブなどローカルのハードディスク同様に、接続された USB メモリのデータが外部に流出することが考えられます。そのようなことを避ける為、**USB メモリを使用していない時は、外しておくこと**をお勧めします。また、USB メモリだけではなく、**microSD カードやスマートフォンなど外部記憶媒体として扱われる機器などをパソコンにつなぐ場合も同様に注意**してください。 （ご参考） IPA-【注意喚起】「USB メモリのセキュリティ対策を意識していますか？」 －USB メモリの安全な使い方を知ろう－ http://www.ipa.go.jp/security/txt/2009/05outline.html IPA- USB メモリを経由したウイルス感染に気をつけましょう！ ～ウイルスの侵入経路トップは外部記憶媒体～ http://www.ipa.go.jp/security/keihatsu/pr2012/general/04_usb_flash_drive.html

（ii）スマートフォンにおけるアプリケーションのインストールについて

相談	スマートフォン（Android）に〇〇というアプリをインストールしようとしたら、権限許可の画面で「電話通知、携帯ステータス、ネットワーク通信」等が出てきた。このアプリに、このような権限は必要なのか。
回答	アプリをインストールする際に、様々な権限（パーミッション）を要求してきたとのことですが「この様な権限は必要ない」と思ったのであれば**一旦、踏みとどまり、不安を解消してからインストールをしてください。**実際に求めてくる権限について、確実に正当かどうかを判断する事は非常に難しいのが実情です。そこでインストール前の判断材料として「5 月の呼びかけ」で紹介した**「一歩踏み込んだおすすめの対策」**を実施してください。**具体的には、「レビュー記事に悪い評判は書かれていないか」「アプリ開発者が他に公開しているアプリの評判に、悪いものがないか」「開発者やアプリ名をインターネットで検索して、悪い評判や噂などはないか」などをチェックするということです。**その他「5 月の呼びかけ」には「**スマートフォンを安全に使うための六箇条**」など基本的な事項が記載されていますので、ぜひ確認してください。 （ご参考） IPA- 【注意喚起】「あなたを狙うスマホアプリに要注意！」 ～不正なアプリをインストールしてしまわないために～ http://www.ipa.go.jp/security/txt/2012/05outline.html

『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