Information-technology Promotion Agency, Japan

プレスリリース
2013 年 1 月 22 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および相談受付状況 [2012 年年間]

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、2012 年年間のコンピュータウイルス・不正アクセスの届出[1]状況および相談受付状況をまとめました。

1. コンピュータウイルス届出状況

2012 年の届出件数は 10,351 件（内、感染被害届出は 7 件）と、2011 年の 12,036 件から約 14%の減少となりました。また、2012 年の年間検出数は 249,940 個と、2011 年の 278,935 個から約 10%の減少となりました。

ウイルス別届出件数では、XM/Mailcab の届出件数が 2012 年 4 月の最初の届出から少しずつですが増加する傾向がありました。

ウイルス別検出数では、W32/Mydoom、W32/Netsky が多く検出されました。

2. 不正プログラム上位 10 種類の検出状況

2012 年の不正プログラム上位 10 種類の合計検出数は、230,450 個と、2011 年の 324,056 個から約 29%の減少となりました。

主に正規のソフトウェアなどを装って感染を試みる Trojan/Horse、オンラインバンキングの ID／パスワードを窃取する Bancos、偽セキュリティソフトの検知名である Fakeav が多く検出されました。

3. コンピュータ不正アクセス届出状況

2012 年の届出件数は合計 121 件（前年比約 17%増）であり、そのうち被害があった件数は 105 件（前年比 40%増）と全体の約 87%を占めました。また、実際に被害があった届出（105 件）のうち、原因の内訳は ID・パスワード管理不備が 18 件、古いバージョン使用・パッチ未導入が 15 件、設定不備が 7 件などでした。

4. 相談受付状況

2012 年のウイルス・不正アクセス関連の相談総件数は 11,950 件でした。そのうち『ワンクリック請求』に関する相談が 2,755 件、『偽セキュリティソフト』に関する相談が 354 件、Winny に関連する相談が 125 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 40 件などでした。

◆ 本リリースの詳細は、http://www.ipa.go.jp/security/txt/2013/2012outline.html をご参照ください。

■ 本件に関するお問い合わせ先
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
■ 報道関係からのお問い合わせ先
IPA 戦略企画部 広報グループ　横山／佐々木
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp

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

1. コンピュータウイルス届出状況

（1）2012 年総括

2012 年のウイルス届出件数※1 状況は、2011 年から減少での推移となりました（図 1-1 参照）。ウイルス別届出件数では、**W32/Mydoom** の届出が最も多くありました。また、マクロウイルスの一種である **XM/Mailcab** の届出が、2012 年 4 月の最初の届出から少しずつですが増加傾向にありました（図 1-2 参照）。2012 年 12 月現在では少し減少傾向になりましたが、しばらくの間は感染活動に注意が必要です。

2012 年のウイルス検出数※2 は、**W32/Mydoom** が全体の半数以上を占め、増加傾向にあります（図 1-3 参照）。対照的に **W32/Netsky** は減少傾向にあり、2012 年は届出件数、検出数とも **W32/Mydoom** に逆転された形となりましたが、それでも全体の 1/3 弱の検出数となりました。**W32/Mydoom や W32/Netsky は、自分の複製をメールの添付ファイルに付けてばら撒いて感染拡大していくウイルスなので、このウイルスに感染しているサーバーやパソコンが未だに多く存在していると言えます。**

2012 年 1 月は **W32/Downad** の検出数が非常に多かったですが、これは特定の企業で検出されたものです。W32/Downad は Windows の脆弱性を悪用して感染活動を行うため、標的型攻撃を行うための足掛かりとして使われることがありますが、ウイルス対策ソフトで検知できていたことがわかっています。

2012 年 4 月の検出数総数が少ないことが図 1-3 からわかりますが、これは届出自体が少なかったからです。

2012 年 11 月は **W32/IRCbot** の検出数が一時的に増加しました。こちらも同様に特定の企業で検出されたものです。W32/IRCbot も Windows やプログラムの脆弱性を悪用して感染活動を行うため、1 月と同様に標的型攻撃の足掛かりとして使われていた可能性があります。

2012 年の不正プログラム検出数※3 は、主に正規のソフトウェアなどを装って感染を試みる **Trojan/Horse**、インターネットバンキングの ID／パスワードを窃取する **Bancos**、偽セキュリティソフトの検知名である **Fakeav**、が多く検出されました（図 1-4 参照）。

2012 年 4 月の検出数総数が少ないことが図 1-4 からわかりますが、これは届出自体が少なかったからです。

2012 年 5 月に Trojan/Horse が多いのは、特定の企業からの 4 月の届出が 5 月に行われたためです。（検出数は、届出を受理した日で集計しています。）

2012 年 7 月の検出数総数が多いのは、特定の企業に対して Adware と Bancos が送られたためです。

2012 年 9 月は Invo の数が多くなっています。こちらも特定の企業に対して多く送られたためです。

ウイルスや不正プログラムの検出数を見ると、かなりのウイルスや不正プログラムがパソコンの手前まで届いていることがわかります。しかし、**ウイルス対策ソフト等を使用することで感染被害に遭わずに済んでいると言えます。**

※1 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。

※2 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）。

※3 ここでいう「不正プログラム検出数」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

（2）ウイルス感染被害届出

2012 年のウイルス感染による被害届出は **W32/Antinny** が 1 件、**W32/Palevo** が 1 件、**W32/Downad** が 1 件、**W32/Fujacks** が 1 件、**W32/Dorkbot** が 3 件、の合計 7 件でした（表 1-1 参照）。

感染経路は、外部からの媒体が 2 件、メールが 3 件、ダウンロードファイルが 1 件、不明が 1 件、でした。

感染原因は、Winny でダウンロートしたファイルを実行したためが 1 件、対策ソフトのパターンファイルが古かったためが 1 件、メールに書かれている URL からファイルをダウンロードして実行したためが 3 件、不明が 2 件、でした。

発見方法は、目視が 3 件、外部からの連絡が 2 件、他のウイルス対策ソフトに変更した時に発見されたのが 1 件、ウイルス対策ソフトのパターンファイルが更新されていなかったため更新後に発見されたのが 1 件、でした。

W32/Dorkbot の届出は、全てインターネット電話サービスの一つである Skype を利用していて感染被害に遭ったものでした。これは、自分の知り合いから届いたメッセージの中に書かれている URL をクリックして、ダウンロードしたファイルを実行すると感染被害に遭ってしまうというものです。感染すると、Skype の連絡帳に登録している利用者に同じメッセージを送信します。

このウイルスは、届出された時点ではほとんどのウイルス対策ソフトで検出されないウイルスでした。

知り合いからのメッセージであっても、怪しいと感じたらクリックをしたり、ダウンロードしたファイルを実行したりせず、送信者である知り合いに確認を取るなどをしてから、クリックや実行することを推奨します。

（3）届出件数

2012 年の届出件数は **10,351 件**となりました。下記グラフ（図 1-1）は、IPA が受け付けた 1 年ごとの届出件数の推移を示したものです。

図 1-1 で示すように、届出件数は 2011 年の **12,036 件**から **1,685 件の減少**での推移となりました。

2012 年に届出されたウイルスの種類は 127 種類（2011 年は 125 種類）で、そのうち 2012 年に初めて届出されたウイルスは 14 種類（2011 年 20 種類）でした。なお、その内の 5 種類は携帯端末のウイルス（2011 年 7 種類）で全て AndroidOS を感染対象としたウイルスでした。

127 種類の内、Windows/DOS ウイルス 82 種類 9,038 件、スクリプトウイルス及びマクロウイルス 36 種類 1,223 件、携帯端末のウイルス 8 種類 89 件、Linux ウイルス 1 種類 1 件、でした。

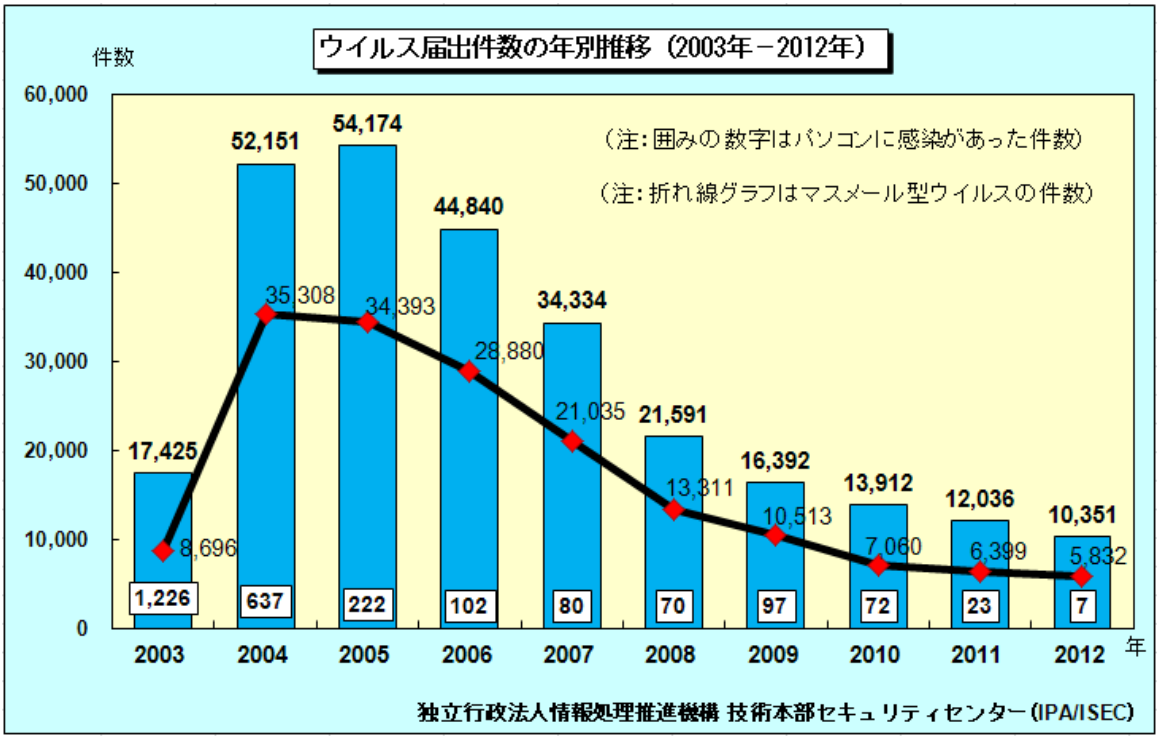


図 1-1：ウイルス届出件数の年別推移（2003 年－2012 年）

2012 年のウイルス感染による被害届出は **7 件**でした。感染ウイルス名※4 は、**W32/Antinny** が **1 件**、**W32/Palevo** が **1 件**、**W32/Downad** が **1 件**、**W32/Fujacks** が **1 件**、**W32/Dorkbot** が **3 件**、でした。詳細は以下の通りです。

表 1-1：ウイルス感染被害届出詳細

ウイルス名	届出種別	ウイルス対策ソフト	感染経路	感染原因	発見方法	対処
W32/Antinny	一般法人	不明	ダウンロードファイル	社員が自宅パソコンで Winny を使い、ダウンロードしたファイルを実行したため	外部からの連絡	パソコンの廃棄
W32/Palevo	教育機関	有（最新）	外部からの媒体	不明	目視	不明
W32/Downad	一般法人	有（最新ではない）	外部からの媒体	ウイルス対策ソフトのパターンファイルが古かったため	ウイルス対策ソフトのパターンファイルを更新した時	パソコンの初期化
W32/Fujacks	一般法人	有（最新）	不明	不明	他のウイルス対策ソフトに変更してウイルススキャンを行った時	ウイルス対策ソフトを変更後に発見・駆除
W32/Dorkbot	個人	不明	メール	メールに書かれている URL からファイルをダウンロードして実行	目視	システムの復元
W32/Dorkbot	個人	有（最新）	メール	メールに書かれている URL からファイルをダウンロードして実行	外部からの連絡	実行したファイルの削除
W32/Dorkbot	一般法人	有（最新）	メール	メールに書かれている URL からファイルをダウンロードして実行	目視	ウイルス対策ソフトを最新の状態にして駆除

※4： ウイルスの詳しい概要は、「IPA に届けられたウイルス」http://www.ipa.go.jp/security/virus/virus_main.html を参照してください。

（4）ウイルス別届出件数

2012 年年間のウイルス別届出件数は、**W32/Mydoom** が **2,428 件**、**W32/Netsky** が **1,982 件**、**W32/Autorun** が **776 件**、でした（図 1-2 参照）。

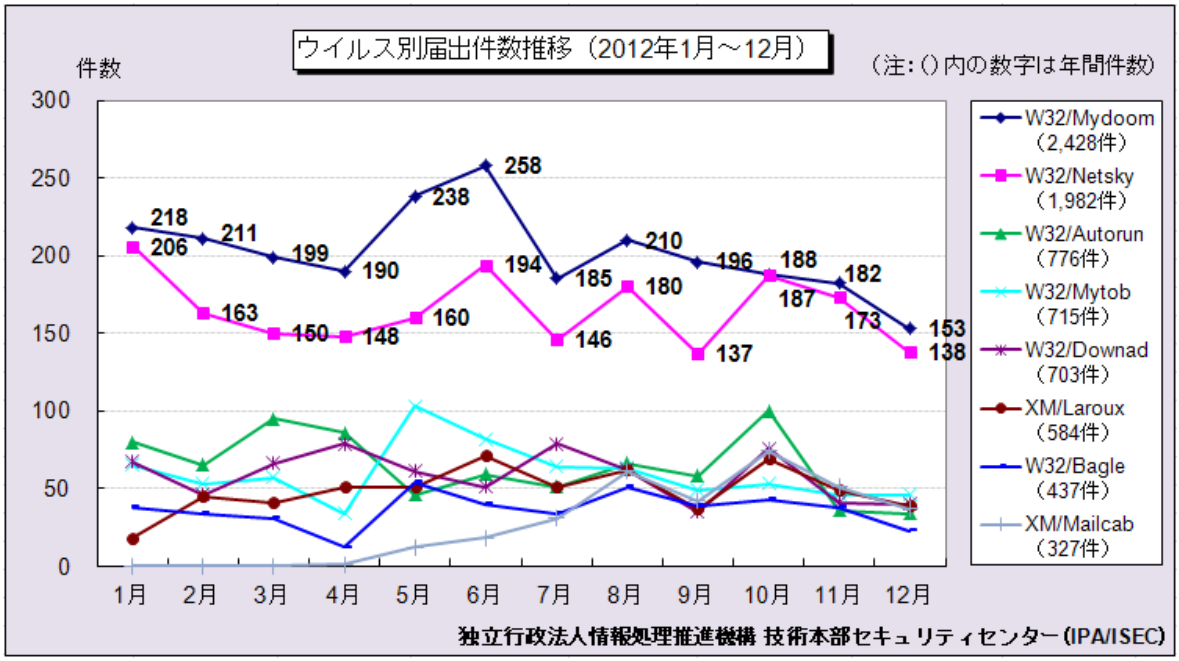


図 1-2：ウイルス別届出件数推移（2012 年 1 月～12 月）

（5）ウイルス検出数

2012 年年間のウイルス検出数は **249,940 個**と、2011 年年間の **278,935 個**から **28,995 個の減少**での推移となりました（図 1-3 参照）。

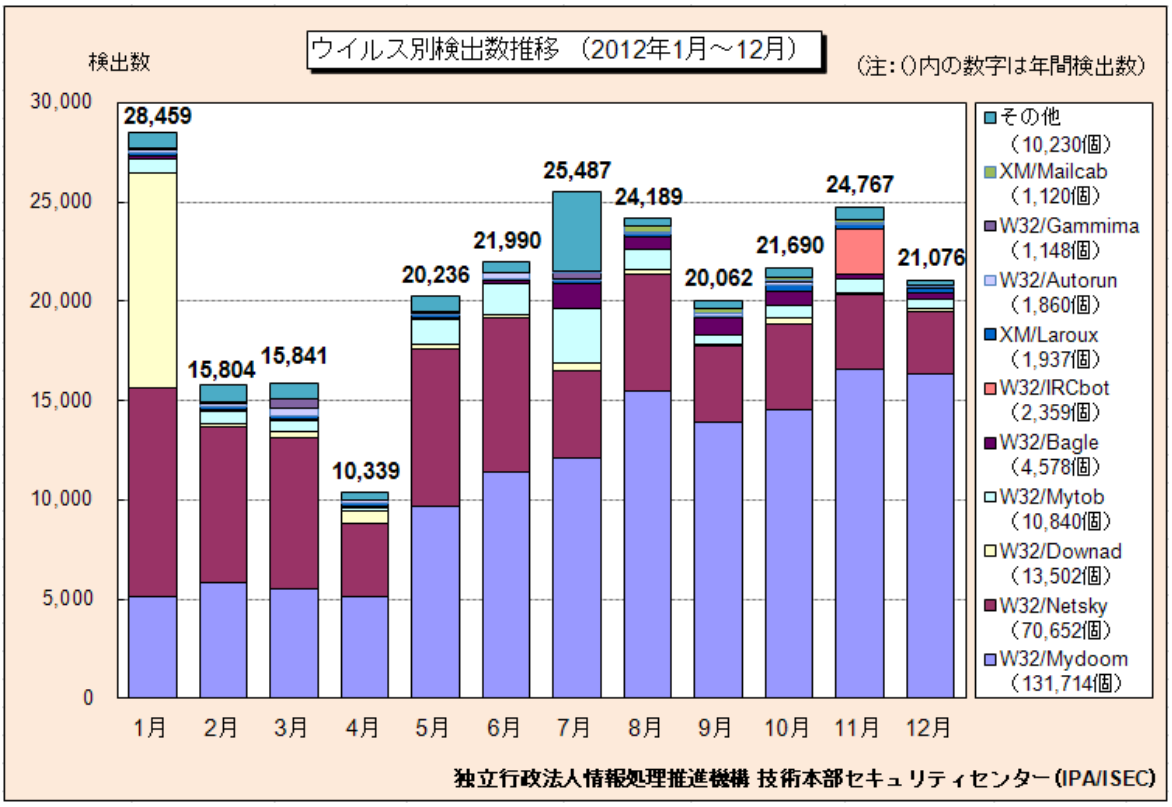


図 1-3：ウイルス検出数の推移（2012 年 1 月～12 月）

（6）不正プログラム検出数

2012 年の不正プログラム上位 10 個の検出数は **230,450 個**と、2011 年の **324,056 個**から、**93,606 個の減少**での推移となりました（図 1-4 参照）。

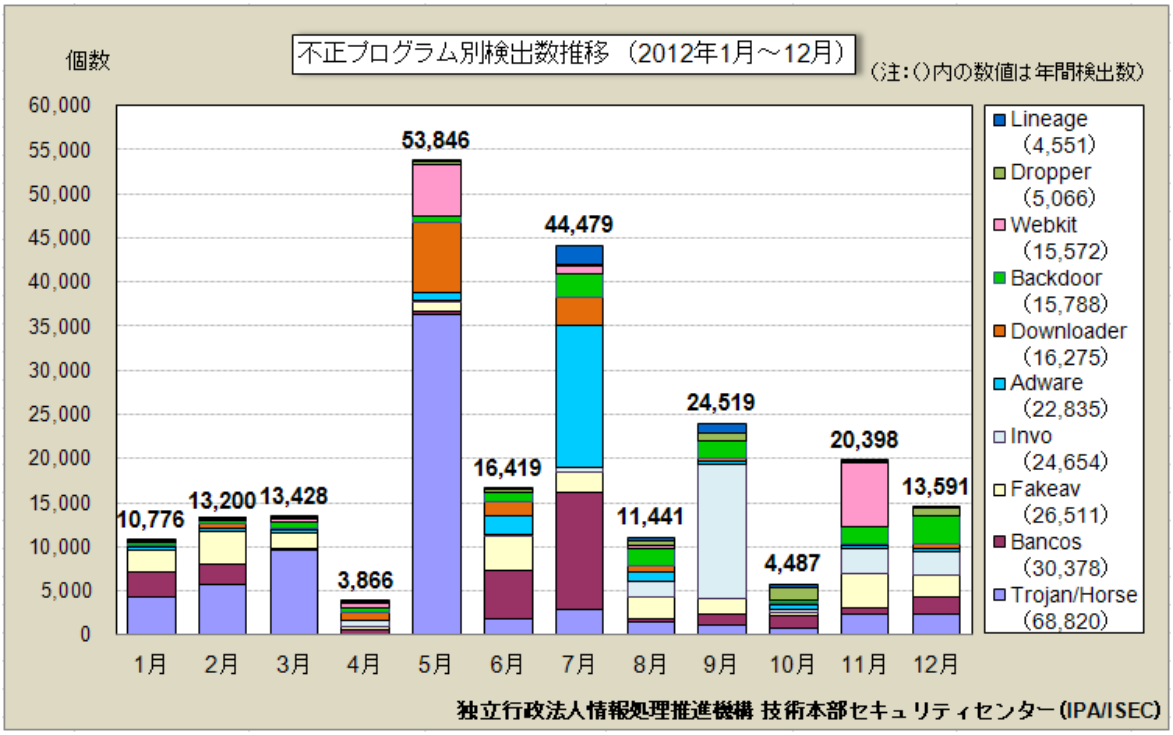


図 1-4：不正プログラム検出数の推移（2012 年 1 月～12 月）

・コンピュータウイルスに関する届出制度について

コンピュータウイルスに関する届出制度は、経済産業省のコンピュータウイルス対策基準に基づき、平成 2 年 4 月にスタートした制度であり、コンピュータウイルスを発見したものは被害の拡大と再発を防ぐために必要な情報を IPA に届け出ることとされています。

IPA では、個別に届出者への対応を行っていますが、同時に受理した届出等を基に、コンピュータウイルス対策を検討しています。また受理した届出は、届出者のプライバシーを侵害することがないように配慮した上で、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。

〇コンピュータウイルス対策基準
平成 7 年 7 月 7 日（通商産業省告示第 429 号）（制定）
平成 9 年 9 月 24 日（通商産業省告示第 535 号）（改定）
平成 12 年 12 月 28 日（通商産業省告示 第 952 号）（最終改定）
〇経済産業大臣が別に指定する者
平成 16 年 1 月 5 日（経済産業省告示 第 2 号）

■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
E-mail: isec-info@ipa.go.jp

2. コンピュータ不正アクセス届出状況

（1）年間総括および対策情報

2011 年は CMS（Content Management System）の脆弱性を悪用したウェブサイト改ざんの届出が増加しましたが、2012 年はそれに加えてサーバー管理ツールの脆弱性悪用したウェブサイト改ざんの届出が目立ちました。また、その被害原因の多くが不明なケースだったことから、こうした改ざんを行うための攻撃手口の巧妙化が伺えます。ウェブ改ざんのその他の原因としては、コンテンツファイルのアップロード時に使用する **FTP アカウントの情報を窃取**されたものが、2011 年と同様に多数発生しました。アップロードに使用するパソコンのウイルス感染が原因と考えられます。

ウェブサイト上で対策を施しても、パソコンから FTP アカウント情報が漏えいしてしまったら意味がありません。ウェブサイト管理者は、システム管理者向け対策のみならず、パソコン上での対策として個人向け対策の実施が必要です。

システム管理者向け対策

- **ID やパスワードの厳重な管理及び設定**
- **セキュリティホールの解消（パッチ適用不可の場合は、運用による回避策も含む）**
- **ルータやファイアウォールなどの設定やアクセス制御設定**
- **こまめなログのチェック**

個人向け対策

- **ウイルス対策ソフトを、常に最新の状態にして利用**
- **Windows Update や Office Update など､OS やアプリケーションソフトのアップデート**
- **パスワードの設定と管理（複雑化、安易に他人に教えない、使い回しをしない、など）**
- **ルータやパーソナルファイアウォールの活用の検討**
- **無線 LAN の暗号化設定確認（WEP は使用せず、できる限り WPA2 を使用する）**

ウェブ改ざん以外のケースでは、なりすましによってオンラインゲームなどのサービスを勝手に使われて金銭被害が出たケースや、SSH で使用するポートへの攻撃で侵入（ID、パスワードの設定不備や不明が主な原因）され、他のコンピュータを攻撃するための踏み台に悪用されていた被害も目立っていたことが挙げられます。主に原因不明なケースが多く見受けられますが、基本的なセキュリティ対策が効果的であることに変わりはありません。下記情報を参考にしてください。

システム管理者向け情報

- 「icat」サイバーセキュリティ注意喚起サービス
  http://www.ipa.go.jp/security/vuln/icat.html
- 「情報セキュリティに関する啓発資料」
  http://www.ipa.go.jp/security/fy18/reports/contents/
- 「脆弱性対策のチェックポイント」
  http://www.ipa.go.jp/security/vuln/20050623_websecurity.html
- 「安全なウェブサイトの作り方　改訂第 6 版」
  http://www.ipa.go.jp/security/vuln/websecurity.html
- 「JVN（Japan Vulnerability Notes）」　※脆弱性対策情報ポータルサイト
  http://jvn.jp/
- 「SQL インジェクション攻撃に関する注意喚起」
  http://www.ipa.go.jp/security/vuln/documents/2008/200805_SQLinjection.html
- 「古いソフトウェア製品を利用しているウェブサイトへの注意喚起」
  http://www.ipa.go.jp/security/vuln/documents/2009/200903_update.html
- 「ウェブサイト管理者へ：ウェブサイト改ざんに関する注意喚起」
  http://www.ipa.go.jp/security/topics/20091224.html
- 「IPA メールニュース」登録

http://www.ipa.go.jp/about/mail/

エンドユーザ・ホームユーザ向け情報

・「ここからセキュリティ」情報セキュリティ・ポータルサイト
http://www.ipa.go.jp/security/kokokara/

・「IPA セキュリティセンター・個人ユーザ向けページ」
http://www.ipa.go.jp/security/personal/

・「Microsoft セキュリティセンター」（日本マイクロソフト社）
http://www.microsoft.com/ja-jp/security/default.aspx

・MyJVN（セキュリティ設定チェッカ、バージョンチェッカ）
http://jvndb.jvn.jp/apis/myjvn/

・「国内のインターネットバンキングで不正アクセスが相次いでいる問題について」
http://www.ipa.go.jp/security/topics/alert20110803.html

（2）被害事例

［侵入］

（i）CMS のプラグイン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	・外部から「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、確かに一部のページにて改ざんされていることが判明した。 ・ページの表示画面が、宗教的メッセージと思われる絵と文章に改ざんされていた。改ざん内容を精査したところ表示内容の変更だけであり、幸いサイト閲覧者にウイルス感染など二次被害を及ぼすようなものではなかった。 ・Joomla!という CMS※1 の機能拡張用プラグインである JCE※2 の脆弱性を悪用されてサーバーにバックドア を埋め込まれたことが原因であった。そのバックドア経由でサーバーに侵入されて改ざんされてしまった。 ・被害後は Joomla!を使用を取りやめ、サイト更新時には HTML を直接変更する運用に移行した。
解説・対策	Joomla!に限らず、各種 CMS には機能拡張用のプラグインが提供されている場合が多いですが、そのプラグインにも脆弱性が発見される場合があります。そうしたプラグインを導入した際には、CMS 本体に加えて、導入したプラグインすべてに対して、最新バージョンを使用するなどの脆弱性対策を実施する必要があります。 CMS もしくはそのプラグインの脆弱性を悪用されてしまった場合、最新版にバージョンアップすることが基本ですが、ユーザーサポートが期待できる商用製品への移行や、場合によっては本事例のように CMS の使用を取りやめることも選択肢の一つです。 （ご参考） ・IPA ― ウェブサイトの管理に利用される CMS もしくは CMS プラグインの脆弱（ぜいじゃく）性に注意 http://www.ipa.go.jp/security/vuln/report/vuln2012q2.html#t03

※1 CMS（Content Management System）： ウェブページのコンテンツ（テキストや画像など）を統合的に管理するためのアプリケーションソフト。

※2 JCE：Joomla!のウェブページを編集するための編集ソフト。

［DoS］

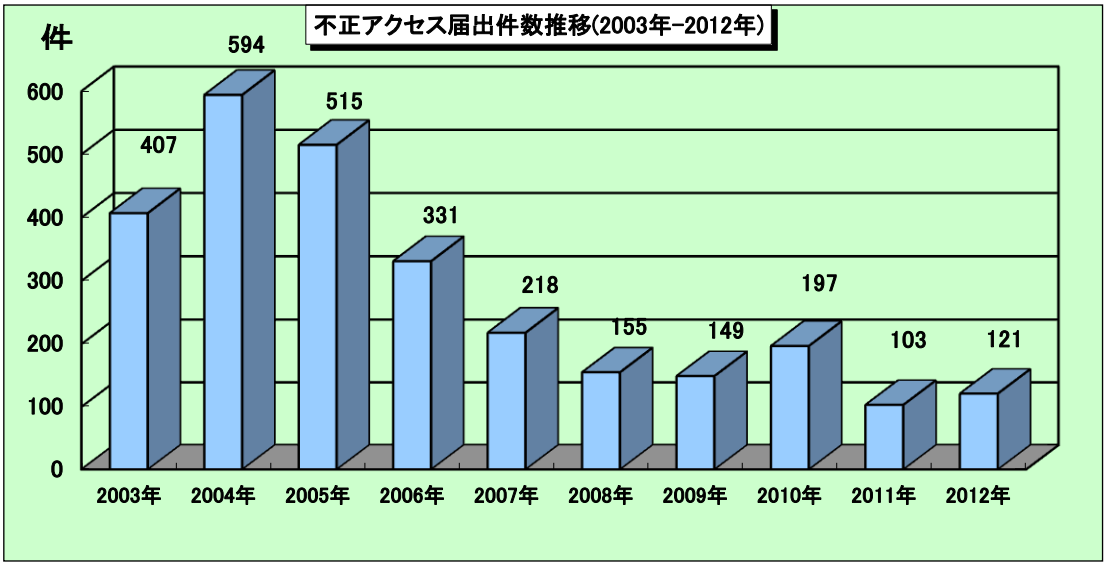
（ii）複数の IP アドレスから大量のアクセスを受けて、インターネット回線が麻痺した

事例	・自宅のインターネット回線を使ってゲームサーバーを公開※3 しており、不特定多数の利用者が遊べるようにしていたが、ある日突然、自宅のパソコンからインターネットに接続できなくなった。 ・自宅のルータのログを確認すると、ある特定の IP アドレスから大量のパケットを送信されていた。DoS 攻撃により、自宅のインターネット回線の帯域を使い果たされたと考えられる。 ・ファイアウォールで当該 IP アドレスを拒否しても、次の日には IP アドレスを変えてアクセスしてくるため、対策してもキリがない。 ・このような DoS 攻撃に対する効果的な対策がわからず、困っている。
解説・対策	オンラインゲームに限らず、サーバーを外部に公開すると IP アドレスが外部に知られるため、常に攻撃を受ける可能性があります。特に一般家庭のインターネット回線の場合、回線の帯域が貧弱な場合が多く、DoS 攻撃に対して弱いと言えます。 一般に自宅でサーバーを運用したい場合、回線の帯域を増強するか、大容量のインターネット回線を利用できるデータセンターへ移設する、といったことが考えられますが、DoS 攻撃よりも怖いのはサーバーへの侵入です。 サーバーに侵入されてしまうと、そのサーバーを踏み台にして、さらに自宅の他のパソコンにまで侵入される恐れや、外部の別のサーバーに対する不正アクセスに悪用されてしまう恐れがあります。 自宅のサーバーを公開する場合、まずはしっかりセキュリティ対策を実施する必要があります。その上で DoS 攻撃への対策を講じてください。 （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 ・IPA ―「サービス妨害攻撃の対策等調査」報告書 http://www.ipa.go.jp/security/fy22/reports/isec-dos/index.html

※3 ゲームサーバーを公開： ゲームによっては、ゲームサーバーを許可なく公開することを禁じているものもあるので、公開する際には事前に確認する必要がある。

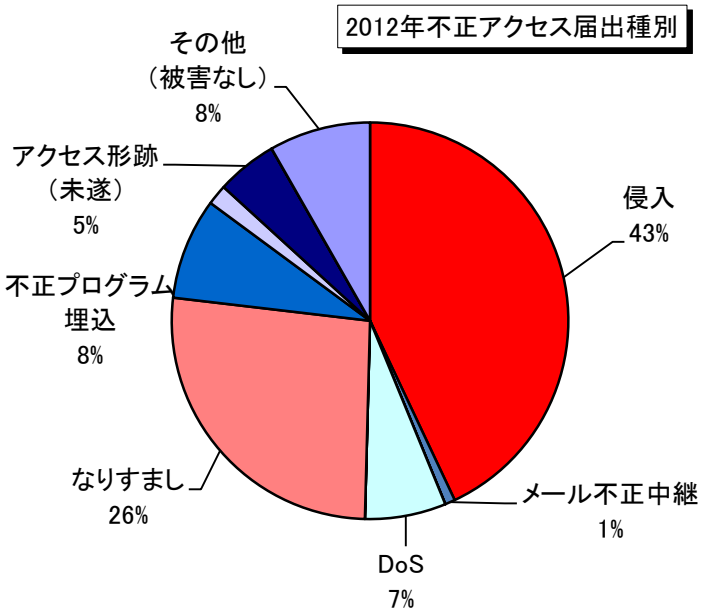
（3）届出件数

2012 年の年間届出件数は **121 件**となり、2011 年の届出件数 103 件から 18 件（約 17%）**増加しました**。なお、下記グラフは、過去 10 年間に IPA セキュリティセンターが受け付けた届出件数の推移を示したものです。



（4）届出種別

2012 年は 2011 年と比べて、「侵入」「なりすまし」などの届出数が増加し、結果として被害のあった総件数が増加しました。

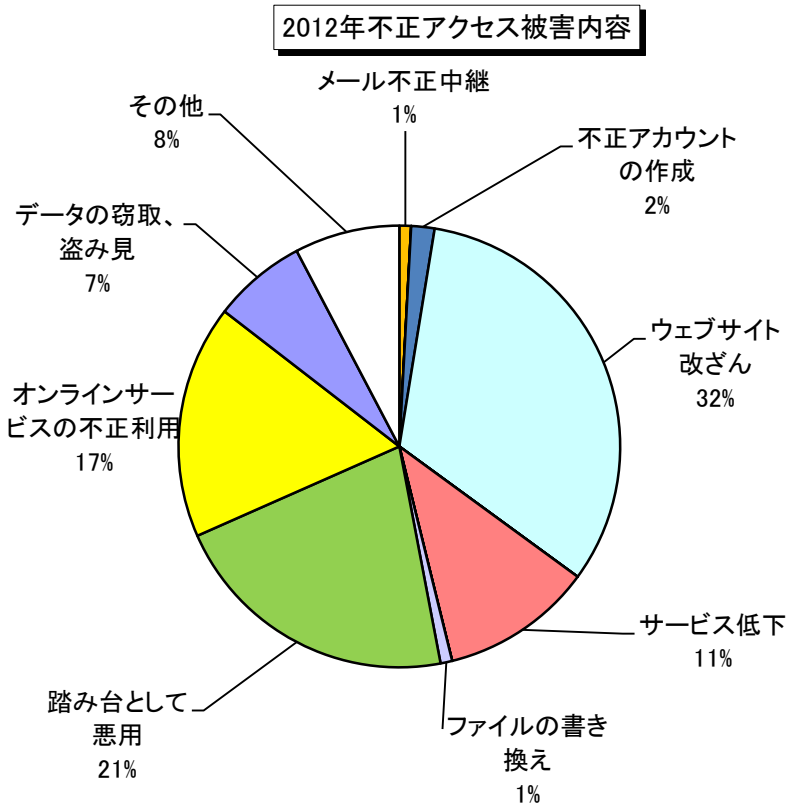


届出種別	2012 年	2011 年
侵入	52	39
メール不正中継	1	1
ワーム感染	0	0
DoS(サービス妨害)	8	5
アドレス詐称	0	0
なりすまし	32	25
不正プログラム埋込	10	5
その他（被害あり）	2	0
アクセス形跡（未遂）	6	21
ワーム形跡	0	0
その他（被害なし）	10	7
合計　（件）	**121(105)**	**103(75)**

※網掛け部分とカッコ内の数字は、被害があった届出種別を示しています。

（5）被害内容

届出のうち実際に被害があったケースにおける被害内容の分類です。被害件数は前年から 30 件（40%）増加しました。特に「**ウェブサイト改ざん**」の届出件数が大きく増加しています。

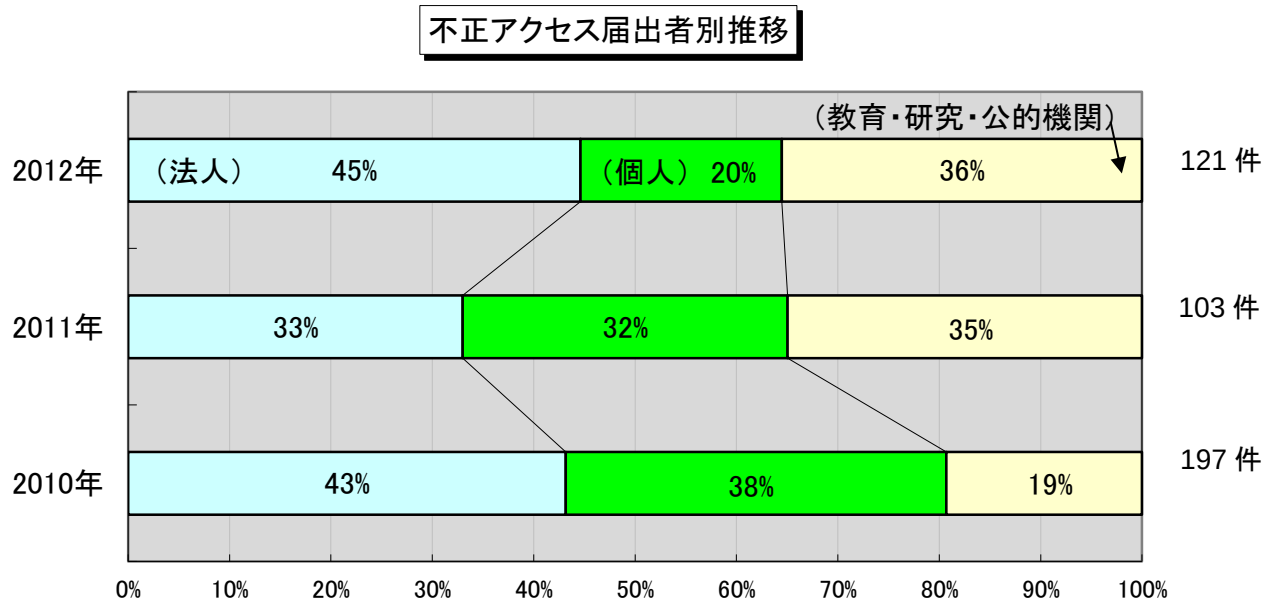


被害内容	2012 年	2011 年
メール不正中継	1	1
サーバーダウン	0	0
不正アカウントの作成	2	1
ウェブサイト改ざん	38	13
パスワードファイルの盗用	0	0
サービス低下	13	7
オープンプロキシ	0	0
ファイルの書き換え	1	4
踏み台として悪用	25	27
オンラインサービスの不正利用	20	17
データの窃取、盗み見	8	8
その他	9	3
合計　（件）	**117(※)**	**81(※)**

※実被害届出１件に複数の被害内容が存在するケースもあるため実被害届出件数合計と一致していません。

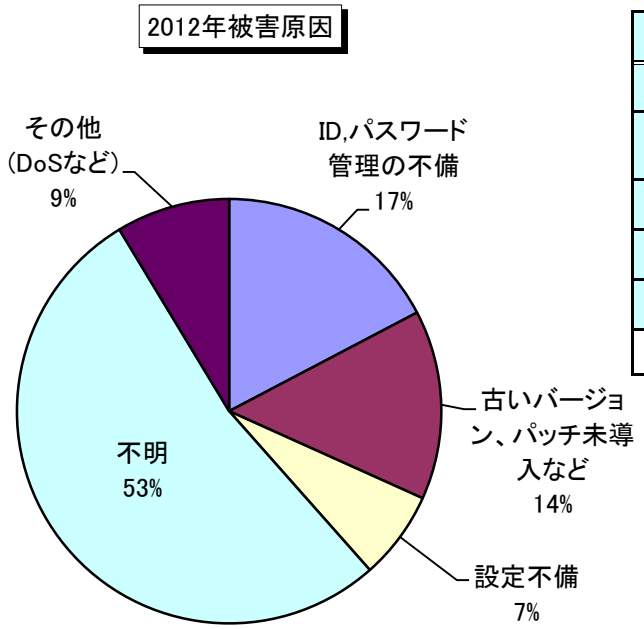
（6）被害内容

届出者別の内訳は、「**法人**」からの届出割合が前年から増加しました。一般企業のウェブサイトの改ざん被害が増加したことが一因です。



（7）被害原因

実際に被害があった届出を原因別分類に見ますと、ID・パスワード管理・設定の不備が 18 件（17%）、古いバージョン使用・パッチ未導入などが 15 件（14%）、設定不備が 7 件（7%）、となっています。原因が不明なケースは 56 件（53%）と、2011 年と同様に全体の半数近くを占めていることから、**不正アクセスの原因究明が困難な事例が多くなっている**ということが推測されます。



被害原因	2012 年	2011 年
ID,パスワード管理の不備	18	15
古いバージョン使用、パッチ未導入など	15	12
設定不備	7	11
不　明	56	32
その他（DoS など）	9	5
合計　（件）	**105**	**75**

■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

E-mail: isec-info@ipa.go.jp

3. 相談受付状況

（1）2012 年総括

2012 年 1 月～12 月のウイルス・不正アクセス関連の相談総件数は **11,950 件**でした。そのうち**『ワンクリック請求』に関する相談**が **2,755 件**、**『偽セキュリティソフト』**に関する相談が **354 件**、**Winny に関連する相談**が **125 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 **40 件**などでした。

2012 年のウイルス・不正アクセス関連の全体相談件数の推移を図 3-1 及び表 3-1 に示します。3 月及び 4 月の相談件数の一時的な落ち込みは、”2012 年度第 3 四半期の総括”でも言及しましたが、2011 年 12 月に起きた”**ワンクリック詐欺逮捕**”の影響、10 月の相談件数の一時的な増加は、昨年マスコミに大きく取り上げられた”**遠隔操作ウイルス**”の影響と推定され、届出月によって多少の増減が見うけられましたが、全体的には、ほぼ横ばいとなっています。

またワンクリック請求、偽セキュリティソフト、Winny、不審メールなどの相談項目ごとに集計した場合、ワンクリック請求及び Winny に関する相談件数は、ほぼ横ばいで推移、偽セキュリティソフトに関する相談は増加傾向にありました。

さらに、近年話題の多い「スマートフォン」のキーワードを含む相談推移をみた場合、”2012 年第 3 四半期の総括”でも示したように、件数はまだ少ないものの、明確に増加傾向を示しており、今後ますます増加していくものと考えられます。

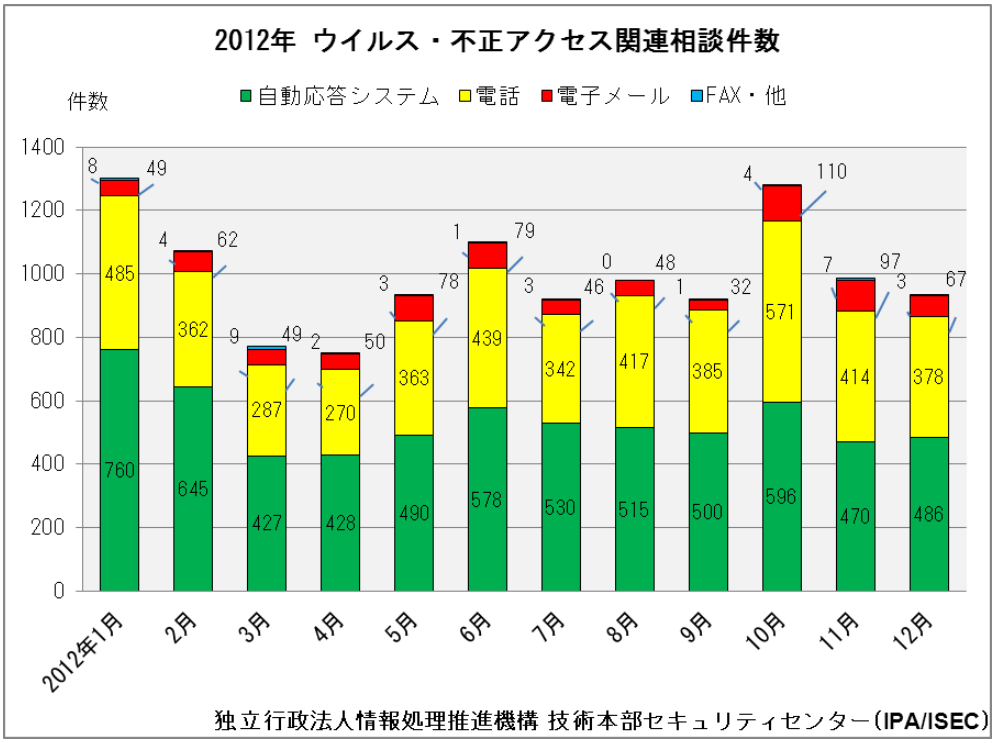


図 3-1：2012 年ウイルス・不正アクセス関連の相談総件数推移

表 3-1 ウイルス・不正アクセス関連の相談件数

		2012 年											
		1 月	2 月	3 月	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月
合計		11,950											
		1,302	1,073	772	750	934	1,097	921	980	918	1,281	988	934
	自動応答システム	760	645	427	428	490	578	530	515	500	596	470	486
	電話	485	362	287	270	363	439	342	417	385	571	414	378
	電子メール	49	62	49	50	78	79	46	48	32	110	97	67
	FAX・他	8	4	9	2	3	1	3	0	1	4	7	3

（2）相談事例

主な相談事例は以下の通りです。

（i）不審なソフトウェアをダウンロードしてしまいインターネットへのアクセスができません。

相談	あるWebサイトを訪問した時、ポップアップ画面が立ち上がり、この画面を閉じようとクリックしていたら、知らない間に不審なソフトウェアをダウンロードし、インストールさせられたようです。インターネットにアクセスしようとすると、このソフトウェアが”不審なWebサイトにアクセスしようとしています”と警告画面を表示して妨害し、インターネットへのアクセスができません。対策を教えてください。
回答	ご相談者様はいわゆる”偽セキュリティソフト”言われるウイルスソフトウェアに感染してしまったものと考えられます。この部類のソフトウェアは、”パソコンのスピードを速くするソフト”とか、”ウイルスを発見するソフト”など、一見、有益そうなソフトウェアに見えますが、実際は偽の警告を発して製品の購入を迫るソフトウェアですので、ポップアップ画面で購入をせまられてもクレジットカード番号などを入力しないで下さい。もし、既にクレジットカード番号などを入力してしまった場合は、消費クレジットカード会社及び消費生活センターなどに相談し、念のためカード番号を変えるなどの検討を行って下さい。また感染したパソコンの対策ですが、このようなウイルスソフトウェアに感染した場合、IPAでは感染前の状態にパソコンを戻す、「システムの復元」を推奨しております。それでも不具合が解消されない場合は、「パソコンの初期化」を行って頂きますようお願いいたします。また、今後このような被害を防ぐために、使用しているオペレーションシステム、アプリケーションソフト、ウイルス対策ソフトは常に最新の状態に保つようにしてください。 （ご参考） 「今なお続く、偽の警告を出すウイルスの被害！」 http://www.ipa.go.jp/security/txt/2012/03outline.html#5

（ii）インターネットバンキングで不審なポップアップ画面に認証番号などを入力してしまいました。

相談	ログインしたら、ポップアップ画面が開き、ログインパスワードや合言葉の入力を求められたため、これに入力してしまいました。後になってニュースなどで知ったのですが、インターネットバンキングのログイン画面を装う手口の犯行が多発しているとのこと、どのようにすれば良いでしょうか？
回答	通常と異なる環境からログインした場合などに、パスワードとは別に合言葉をいれる画面に移る（リスクベース認証を求められる）こともあるかもしれませんが、インターネットバンキングで、ログインパスワードと合言葉を同時に入力させる不審なポップアップ画面に入力されたということで、まずは、至急ご利用のインターネットバンクの相談窓口に正しい入力画面かどうか確認し、不審な入力画面であったなら、当該口座からの払い出しなどが行われないように相談して下さい。その後、ご利用のウイルス対策ソフトを最新の状態にしてパソコン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、多角的なスキャンも実施することをお奨めします。ウイルスが見つかった場合、ウイルス対策ソフトで削除可能と考えますが、万一を考え「システムの復元」や「パソコンの初期化」を行い、その後に正規のログイン画面からログインパスワードや合言葉を変更するようお奨め致します。また、今後このような被害を防ぐために、使用しているオペレーションシステム、アプリケーションソフト、ウイルス対策ソフトは常に最新の状態に保つようにしてください。 （ご参考） 「ネット銀行を狙った不正なポップアップに注意！」 http://www.ipa.go.jp/security/txt/2012/12outline.html#5

（3）相談内容の詳細分析

表 3-2 に 2011 年と 2012 年の相談件数を比較したものを示します。これに示すよう、2012 年の全体相談件数は 2011 年に比べ、減少する傾向にありました。これは、”2012 年度第 3 四半期の総括”で分析したとおり、相談内容に大きな割合を占めるワンクリック請求に関するよくある質問に対しての回答を準備したためであることが、2012 年のワンクリック請求に関する注意喚起ページの参照件数（約 18 万 9 千回/年 ＝ 1 万 5750 回/月）からも伺えます。

偽セキュリティソフトの相談件数は、これまで 2～3 年周期で増減を繰り返す傾向がみられ、2010 年から 2011 年前半にかけて相談件数が減少する傾向がみられましたが、2011 年後半から 2012 年にかけては増加する傾向を示しました。これは新種の偽セキュリティソフトが市場に出現しはじめたことを示すものと考えられます（図 3-3 参照）。また、これに関する 2012 年の特記事項として、**偽セキュリティソフトの「凶悪化」**があげられます。偽セキュリティソフトは以前から存在し、これまでに多くの相談がよせられていますが、昨年末に現れた偽セキュリティソフトは、「インターネットへのアクセスを完全にできなくする」、「システムの復原を実施しようとした場合、その操作を妨害する」など、**一度感染してしまった場合、パソコンを初期化せざるを得ない**状況まで追い込む偽セキュリティソフトの相談が寄せられました。

表 3-2. 2011 年と 2012 年の相談件数の比較表

年及び件数等		相談件数 全体	ワンクリック 請求	偽セキュリティソフト	Winny	不審メール	スマートフォン
2012 年	件数	11,950	2,755	354	125	40	273
2011 年	件数	18,567	5,509	96	151	38	126
増減値	件数	−6,617	−2,754	258	−26	2	147
増減値	(%)	−36%	−50%	269%	−17%	5%	117%

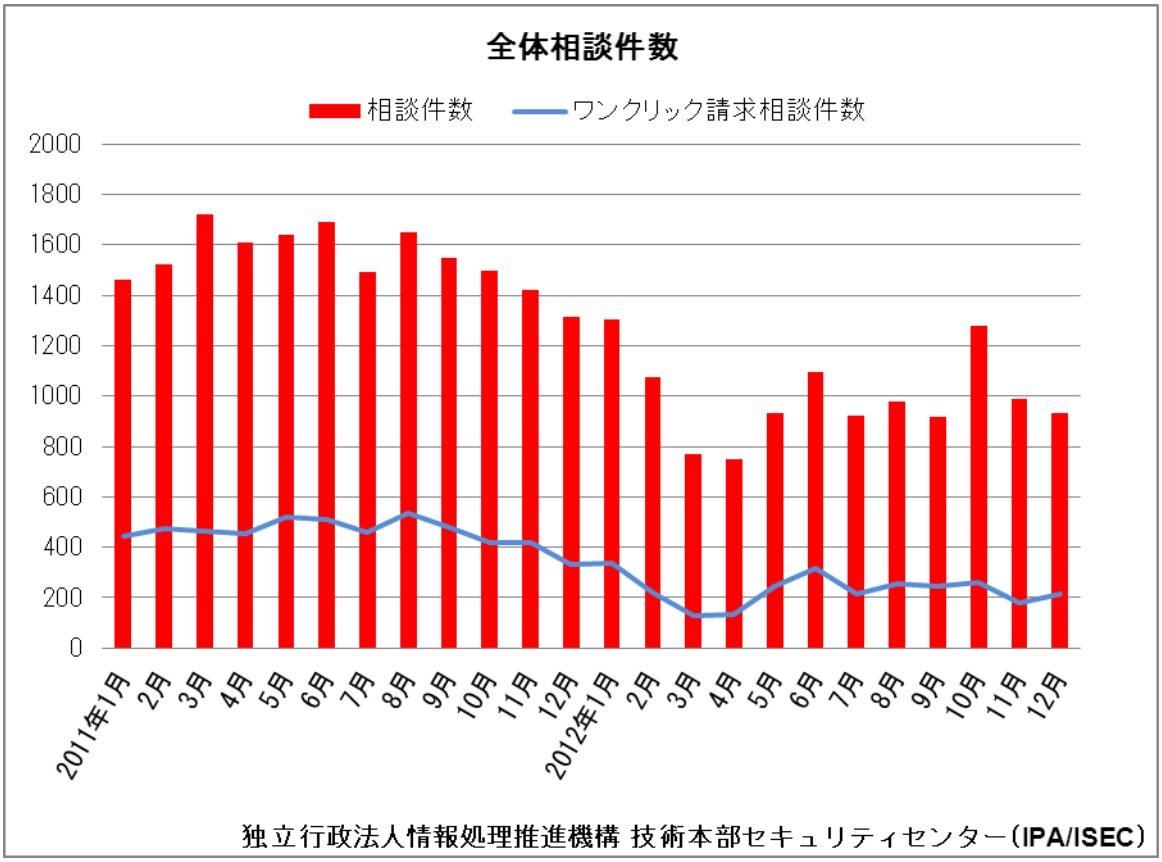


図 3-2：2011 年～2012 年全体相談件数推移

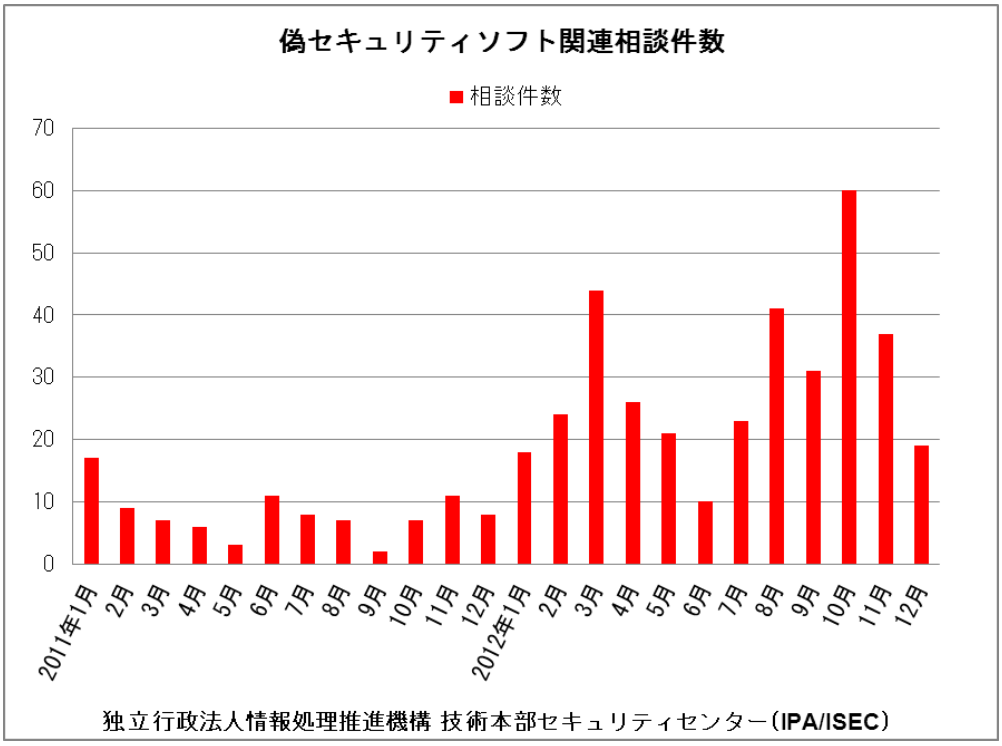


図 3-3：偽セキュリティソフトの相談件数推移

図 3-4 は、今後着目すべき相談項目の例として、スマートフォン関連の相談について、キーワードで集計を行ったものを示します。この結果から、近年のスマートフォンの普及に関連して相談が増えていることが確認でき、これに関する相談は、今後ますます増加するものと予想しています。

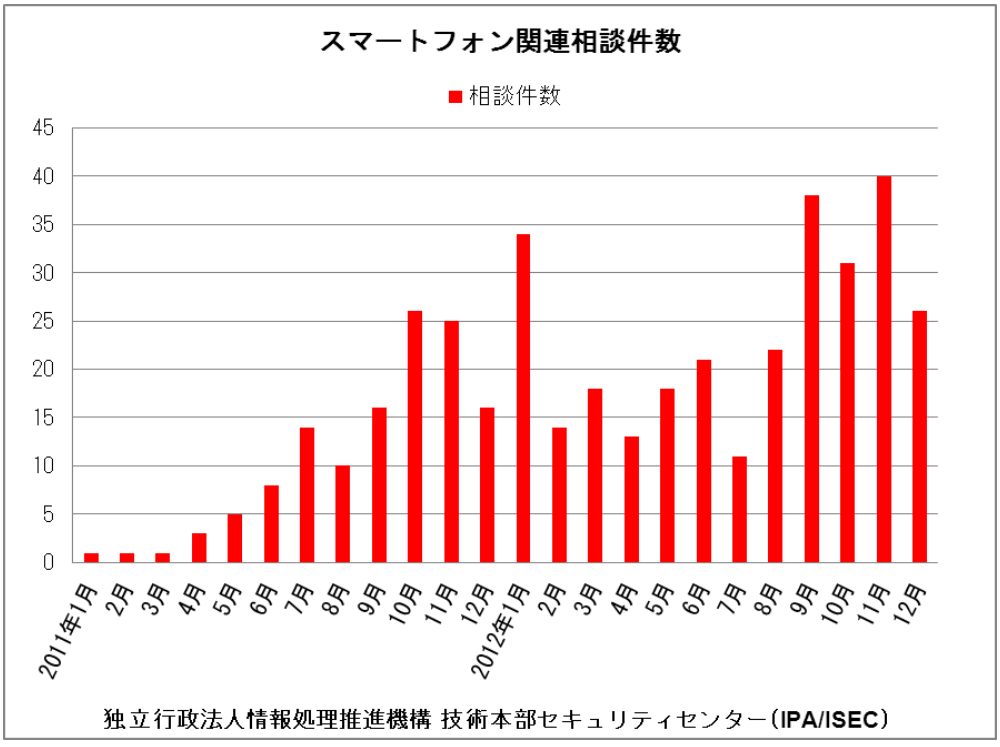


図 3-4：スマートフォン関連の相談件数推移

■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
E-mail: isec-info@ipa.go.jp