Information-technology
Promotion
Agency, Japan

第 12-05-241 号
2012 年 3 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 2 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 2 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

「 今なお続く、偽の警告を出すウイルスの被害！ 」

2012 年に入り、"ウイルスに感染している"、"ハードディスク内にエラーが見つかりました"といった偽の警告画面を表示し、それらを解決するためとして有償版製品の購入を迫る、「偽セキュリティ対策ソフト」型ウイルスの相談・届出が多く寄せられており、2 月は特に、感染被害に遭った利用者からの相談（相談数 24 件の内、20 件が感染被害の相談）・届出が目立ちました（図 1-1）。

こうした相談や届出の事例として、「そのようなソフトウェアをインストールしていないのに、画面が出てきて勝手にパソコン内を調べ始めた。」という旨の内容が多く見られました。これらの事例では、「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として、脆弱（ぜいじゃく）性を解消していないパソコンに対してウェブサイト閲覧時にウイルスを感染させる、ドライブ・バイ・ダウンロード攻撃が行われていました。

また、偽の警告画面に表示される製品名称は、正規のウイルス対策ソフト名に似せたものの他に、"System Check"、"RegClean Pro"など、パソコン内を診断するツールを連想させる名称となっており、利用者が元々使用しているソフトウェアとの判別がつきにくくなっていると考えられます。

以下では、2011 年 12 月から 2012 年 2 月に届け出られた感染被害についての分析とウイルスの特徴を元に、被害に遭わないための対策を説明します。

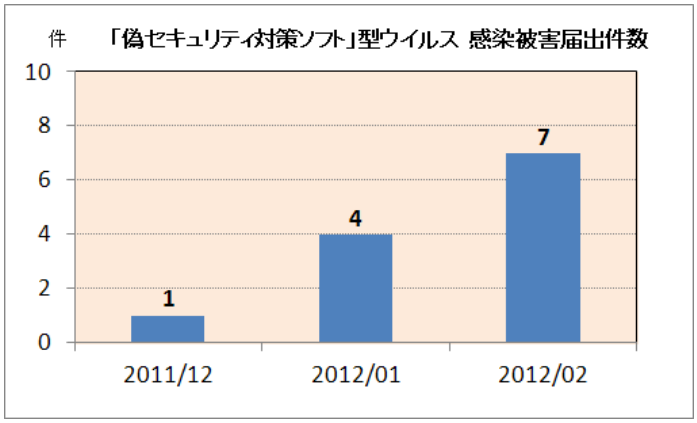

図 1-1：「偽セキュリティ対策ソフト」型ウイルス　感染被害届出件数

（1） 感染被害届出の分析

2011 年 12 月から 2012 年 2 月に届け出られた感染被害 12 件について、ウイルス対策ソフトの使用有無を確認したところ、以下の結果となりました。

表 1-1：ウイルス対策ソフトの使用有無

使用	11 件
未使用	0 件
不明	1 件

また、ウイルス対策ソフトを使用していた届出者 11 件は、全て定義ファイルを最新の状態に更新して使用していました。

このことから、今回届出のあった「偽セキュリティ対策ソフト」型ウイルスは、**ウイルス対策ソフトを最新の状態で使用していても、感染被害に遭う可能性※1 が高かったことが伺えます。**

※1 ウイルス対策ソフトによっては、翌日には検知可能になったという報告もありました。

さらに感染経路を確認したところ、12 件中 11 件が、ウェブサイトを閲覧した時にウイルスをダウンロードさせられて感染被害に遭ってしまう、ドライブ・バイ・ダウンロード攻撃によるものでした。

（ご参考）

「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）

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

「情報セキュリティ白書 2011 ～広がるサイバー攻撃の脅威、求められる国際的な対応～」（IPA）

第 II 部 2011 年版 10 大脅威『進化する攻撃…その対策で十分ですか？』 P.15～16 参照

http://www.ipa.go.jp/security/publications/hakusyo/2011/hakusho2011.html

IPA では以前にも、「偽セキュリティ対策ソフト」型ウイルスの注意喚起を行っています。その時の主な感染経路はメールによるもので、ウイルスが埋め込まれた添付ファイルを開くことで、感染するというものでした。

（ご参考）

「偽の警告を見分けよう！」（IPA）

http://www.ipa.go.jp/security/txt/2008/11outline.html

「偽のセキュリティ対策ソフトの脅威が再び拡大！」（IPA）

http://www.ipa.go.jp/security/txt/2009/11outline.html

「深刻化する偽セキュリティ対策ソフトの被害！」（IPA）

http://www.ipa.go.jp/security/txt/2010/06outline.html

図 1-2 は、IPA に寄せられた「偽セキュリティ対策ソフト」型ウイルスの検出数について、2008 年 9 月から 2012 年 2 月までの推移を示したものです。**以前はメールを使って大量にばらまかれていたため、大量に検出されていましたが、2011 年以降は極端に減っています。これは、攻撃手口の主流が、メールの大量ばらまきからドライブ・バイ・ダウンロード攻撃に移った**ためです。

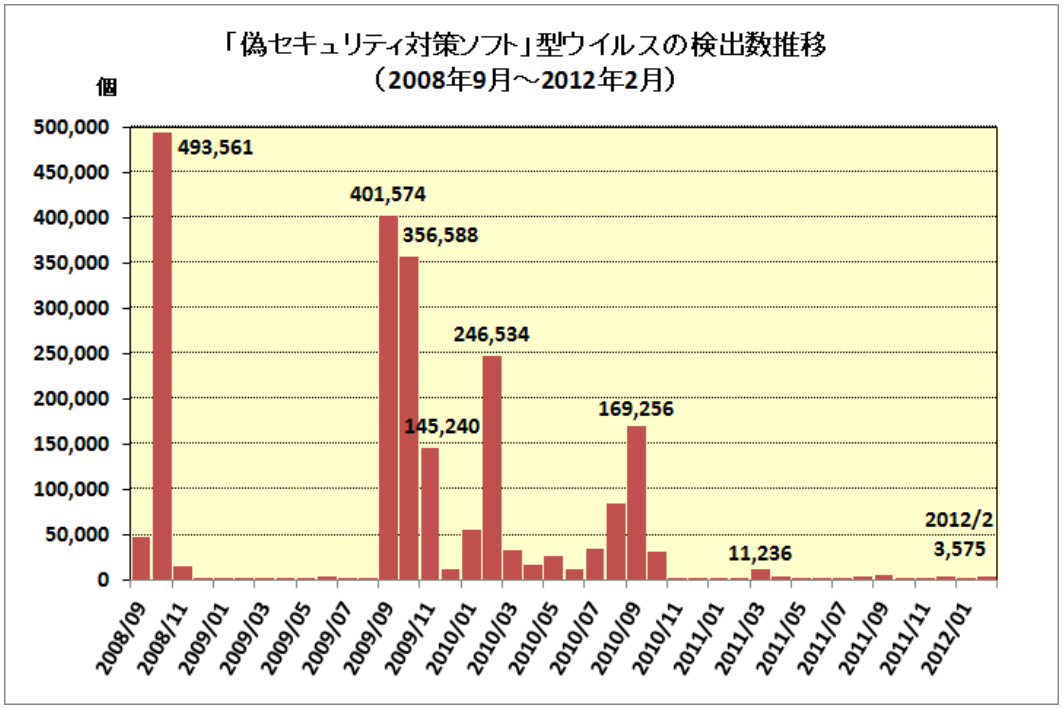

図 1-2：「偽セキュリティ対策ソフト」型ウイルスの検出数推移（2008 年 9 月～2012 年 2 月）

(2) 「偽セキュリティ対策ソフト」型ウイルスの特徴

IPA に寄せられた「偽セキュリティ対策ソフト」型ウイルスの特徴を、"System Check"を例に説明します。

1. 突然デスクトップ上に、パソコン内を勝手にチェックし始める画面が表示されます（図 1-3）。この画面を表示している間、**利用者にはわからないように、複数のウェブサイトにアクセスをして、何らかのプログラムをダウンロードしようとしていました。**このプログラムがどういうものなのか実際に確認はできませんでしたが、**別のウイルスを感染させようとしている可能性があります。**

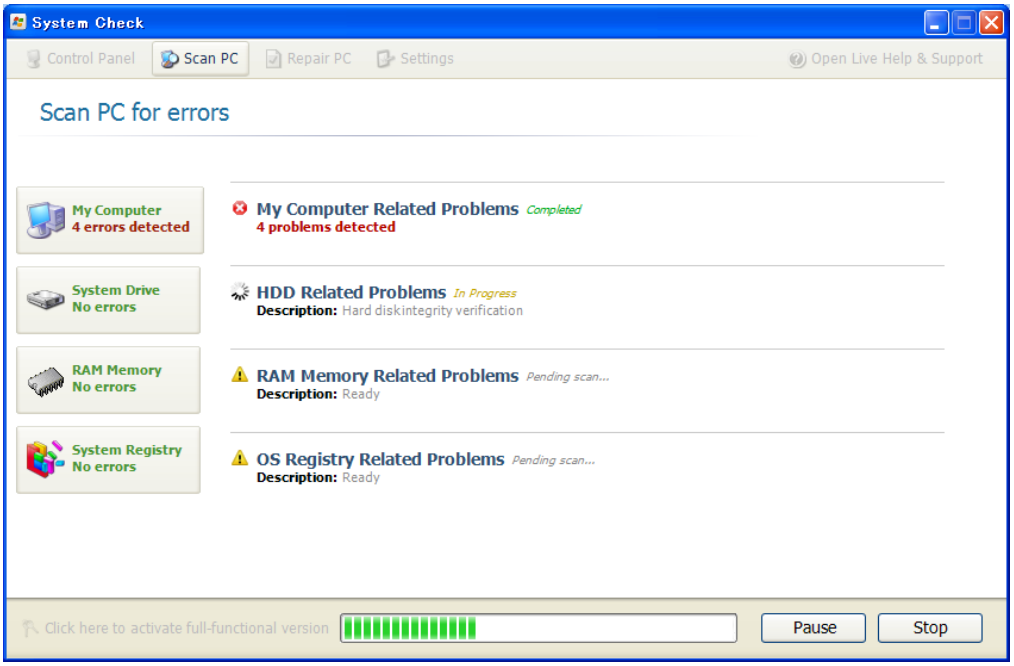

図 1-3：パソコン内をチェック中の画面

2. 一通りチェックが終了し、しばらくすると問題解決を促す画面が表示されます（図 1-4）。**相談の中には、この問題解決の画面がいくつも表示される、デスクトップの背景が黒くなってパソコンそのものが動かなくなる、といった事例も報告されています。**

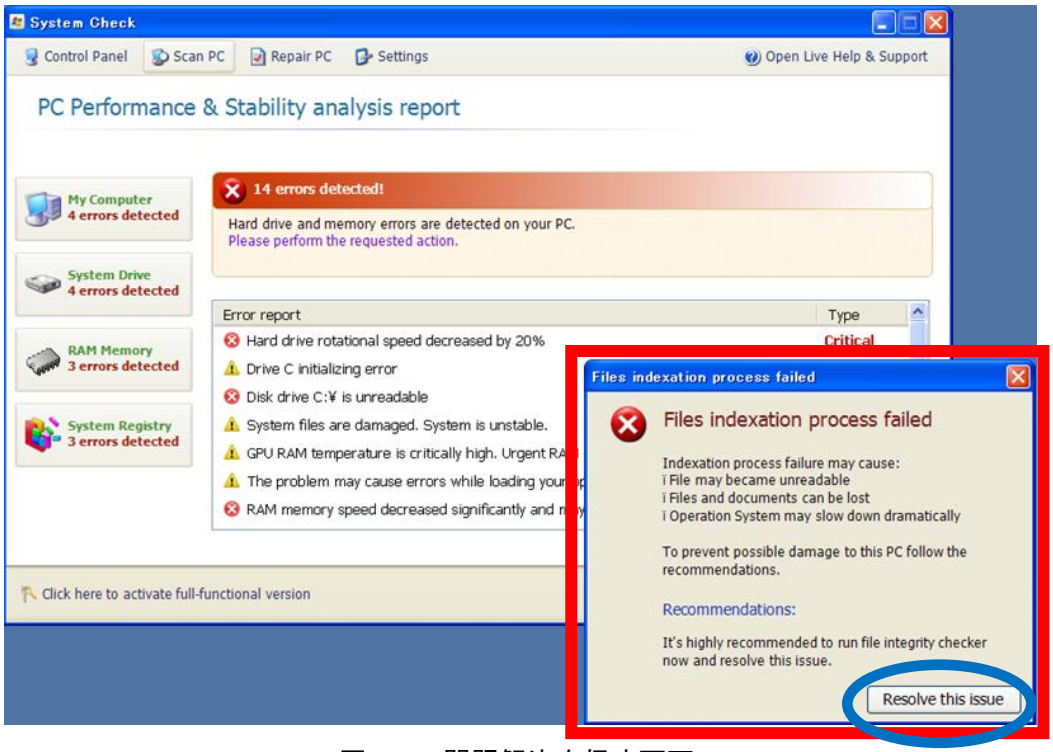

図 1-4：問題解決を促す画面

3. 図 1-4 の画面の［Resolve this issue］ボタンをクリックすると、クレジットカードを使って有償版製品の購入を迫る画面が表示されます（図 1-5）。一見、ウェブブラウザーの画面に見えますが、実はブラウザーを模した偽の入力画面です。**アドレスバーの部分が緑色になっており、いかにも安全なサイトとの通信に見せていますが、そもそもブラウザーではないため、安全なサイトとの通信が行われている保証はありません。クレジットカード番号を入力してしまうと、不正利用される危険があります。**

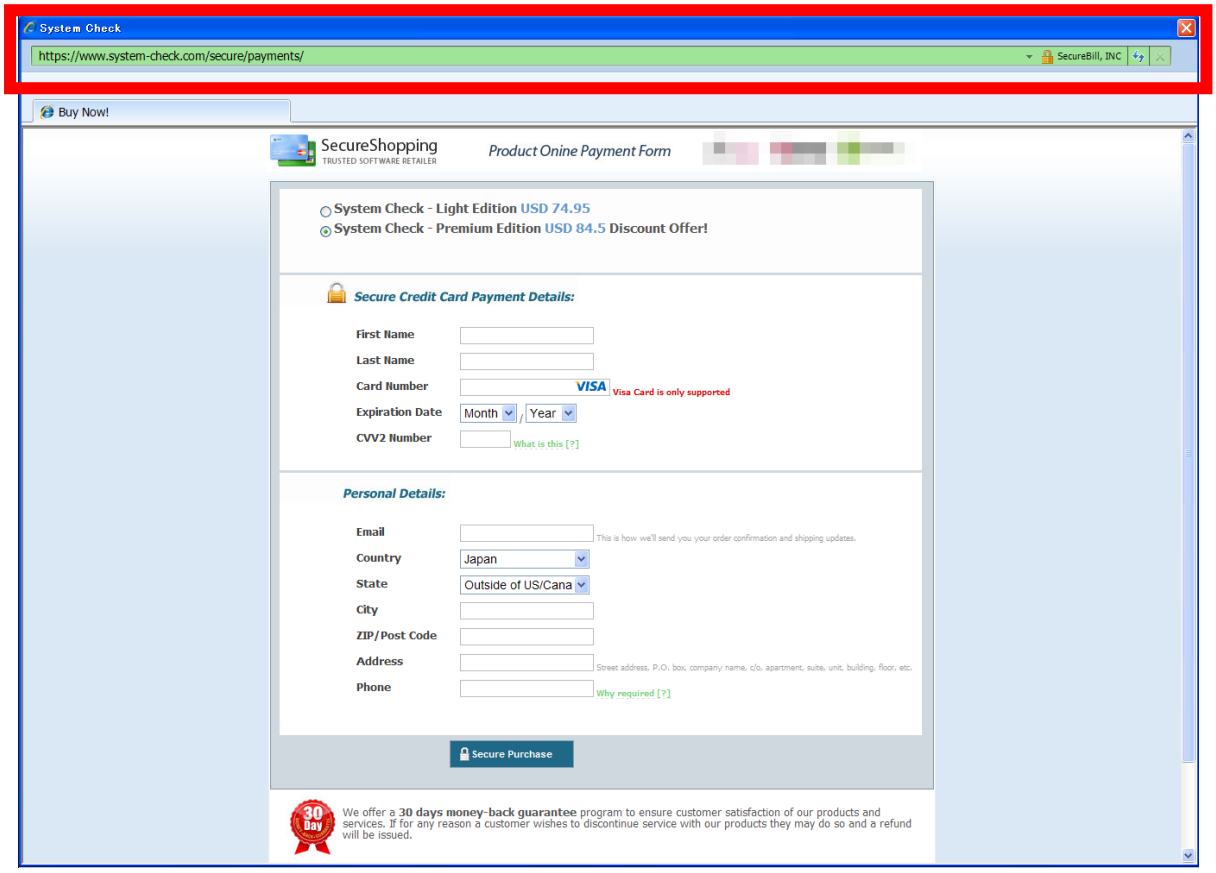

図 1-5：有償版製品の購入を迫る画面

その他の特徴として、**スタートメニューから［コントロールパネル］や、［アクセサリ］などを表示させないようにしたり、インターネットのお気に入りの中身を削除したりします。これは、ウイルスを駆除されないようにするためと考えられます。**

さらに、デスクトップ上のアイコン、パソコン内のほとんどのファイルやフォルダを消してしまいます。なお、実際に削除するのではなく、ファイルやフォルダを「隠しファイル」表示に設定して、あたかも消えたように見せます。

こうすることにより、パソコンがより深刻なダメージを受けていると思わせて、有償版製品を購入させようとしていると考えられます。

（3） 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、以下に示す基本的な対策が重要ですが、まずは**自分が使用しているウイルス対策ソフトを把握しておくことも重要です。**

（i）脆弱性の解消

（1）の分析で述べましたが、感染被害の多くは"ドライブ・バイ・ダウンロード"攻撃によるものです。この攻撃は、OS やアプリケーションソフトの脆弱性を悪用するため、古いバージョンのままにしておかず、常に最新の状態に保つことが一番の対策になります。

IPA では、パソコンにインストールされているソフトウェア製品のバージョンが最新であるかを、簡単な操作で確認するツール「MyJVN バージョンチェッカ」を無償で公開しているので、ぜひご

活用下さい。

（ご参考）

MyJVN バージョンチェッカ（IPA）

http://jvndb.jvn.jp/apis/myjvn/vccheck.html

（ii）重要なデータのバックアップ

今回感染被害に遭った 12 名の内、7 名がパソコンを初期化することにより復旧していました。このようなことで、パソコンそのものが動かなくなってしまう場合に備え、重要なデータは外部記憶媒体等へバックアップすることをお勧めします。

（iii）ウイルス対策ソフトの使用

ウイルス対策ソフトを導入し、ウイルス定義ファイルを最新に保ちながら使用してください。

なお、"ドライブ・バイ・ダウンロード"攻撃を行うなどの有害なウェブサイトの閲覧を防止する機能がある、統合型セキュリティソフトを使用することで、（1）で挙げた感染被害についても、未然に防ぐことができた可能性があります。

（4） 感染時の対処方法

万が一ウイルスに感染してしまった場合、**一番の対処方法としてパソコンの初期化**をお勧めしています。これは、**"ドライブ・バイ・ダウンロード"攻撃などから感染被害に遭った場合、複数のウイルスに感染している可能性があるためです。（2）の例で示した"System Check"についても、何らかのプログラムをダウンロードしようとしていることがわかっています。**

たとえ感染の症状が改善されたとしても、少しでもおかしいと感じることがあれば、データのバックアップを先に行ってからパソコンの初期化を行うことをお勧めします。

簡単に初期化ができない場合もあると思われます。その際は以下の対処で復旧を試みてください。

- パソコンが操作できる状態であれば、最新のウイルス対策ソフトでパソコンのスキャンを行い、ウイルスの駆除を試みます。
- ウイルス対策ソフトでの駆除ができない場合は、「システムの復元」による復旧を試みます。パソコンが操作できない、ウイルス対策ソフトによる駆除ができない、あるいは「システムの復元」がうまくいかない、といった場合は、パソコンを「セーフモード」で起動した上で、これらの作業を再度試みます。

  （ご参考）

  「Windows での「システムの復元」の実施手順」（IPA）

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

  「Windows XP をセーフモードで起動する方法」（Windows XP）（日本マイクロソフト社）

  http://support.microsoft.com/kb/880414/ja

  「コンピュータをセーフモードで起動する」（Windows Vista）（日本マイクロソフト社）

  http://windows.microsoft.com/ja-jp/windows-vista/Start-your-computer-in-safe-mode

  「コンピューターをセーフモードで起動する」（Windows 7）（日本マイクロソフト社）

  http://windows.microsoft.com/ja-JP/windows7/Start-your-computer-in-safe-mode
- パソコンのシャットダウン操作すらできない状態であれば、本体の電源ボタンをしばらく押し続け、強制的に電源を切ってから、「セーフモード」での起動を行います。

デスクトップ上のアイコンや、ファイル／フォルダが消えてしまった場合は、ウイルスが「隠しファイル」設定にしている可能性があります。以下のサイトを参考にしてファイルやフォルダを表示させてください。

（ご参考）
Windows の隠しファイルや隠しフォルダーを表示する方法（日本マイクロソフト社）
http://support.microsoft.com/kb/2453311/ja

なお、ウイルスによって購入を迫られる有償版製品を購入しても、状況が改善する保証はありませんので、支払いをすべきではありません。

万が一、クレジットカード番号を入力して有償版製品を購入してしまった場合、その情報を不正利用される可能性がありますので、お使いのクレジットカード会社に連絡し、カード番号を変更することをお勧めします。また購入してしまった場合の代金返金などに関しては、お使いのクレジットカード会社か、お近くの消費生活センターにご相談下さい。

（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/

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）
- オンラインゲームのアカウントが乗っ取られた
- 遠隔操作ツールを埋め込まれ、結果としてフィッシングに悪用するページを設置された

○ 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）
- シャットダウン時に、他の人がログオンしているメッセージが出てくる
- IPA から添付ファイル付きの注意喚起メールが届いた

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

2 月のウイルスの検出数※1 は、**15,804 個**と、1 月の 28,459 個から 44.5%の減少となりました。また、2 月の届出件数※2 は、**833 件**となり、1 月の 941 件から 11.5%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。
・2 月は、寄せられたウイルス検出数 15,804 個を集約した結果、833 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で **7,832 個**、2 位は **W32/Mydoom** で **5,823 個**、3 位は **W32/Mytob** で **642 個**でした。

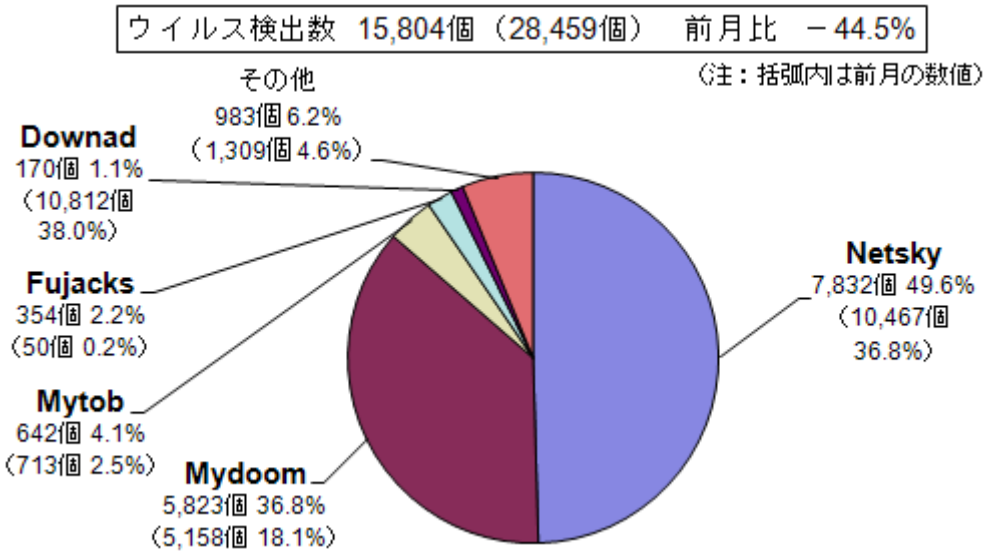

図 2-1：ウイルス検出数

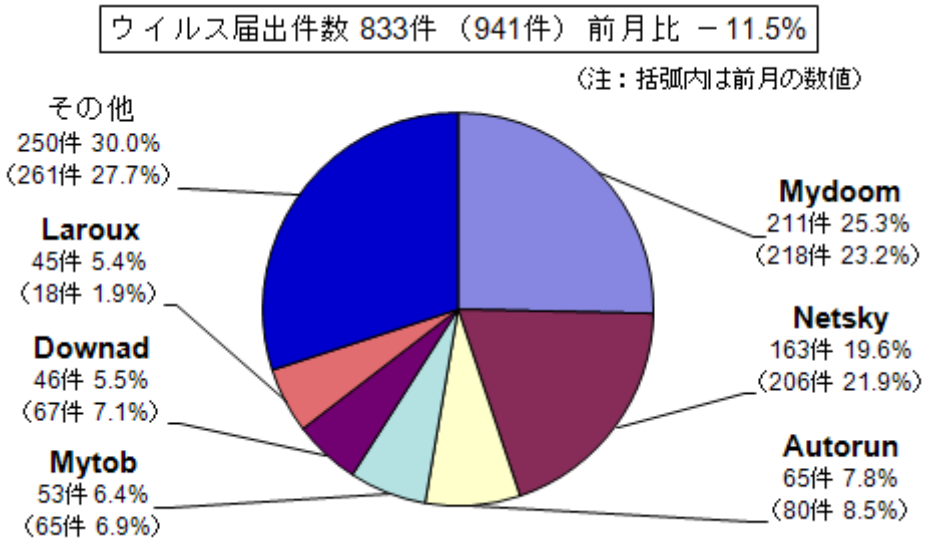

図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

2 月は、パソコン内に裏口を仕掛ける BACKDOOR と、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、他の不正プログラムよりも多く検知されました（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

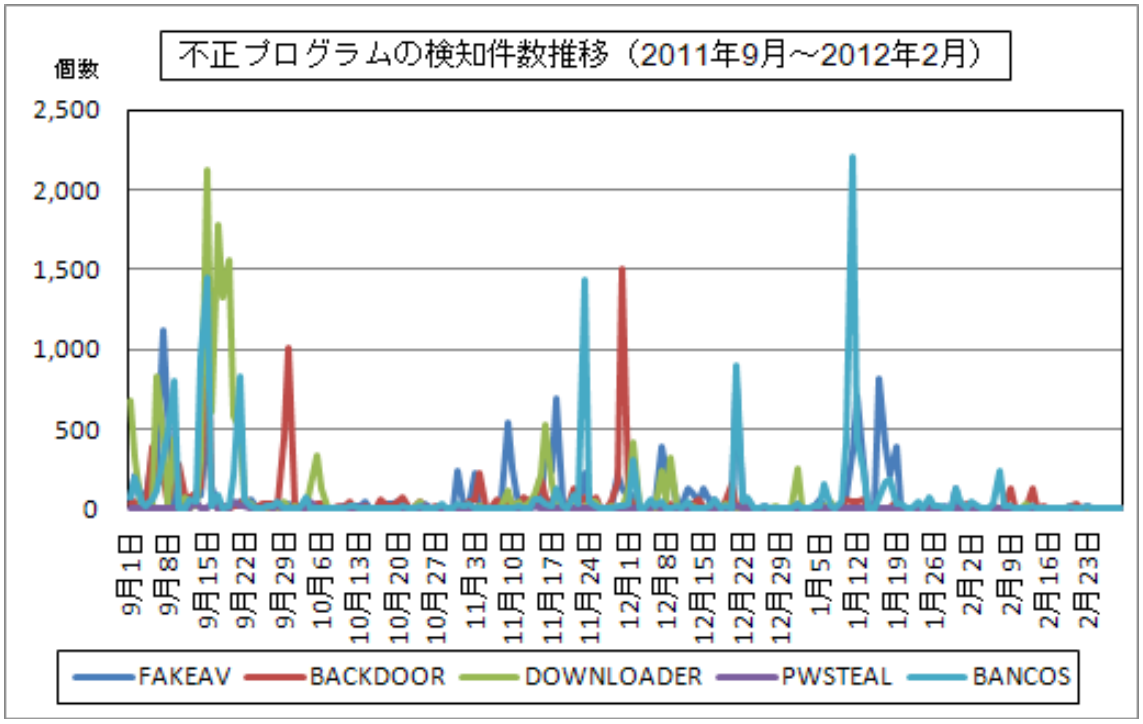

図 2-3：不正プログラムの検知件数推移

（3）参考情報

「DNS changer」について

ウイルスの中には、お使いのパソコンに感染した後、パソコン自身の DNS 設定や、家庭内に設置したルーターの DNS 設定を勝手に変更するものがあります。

DNS 設定には、ウェブ閲覧などの際に参照する DNS サーバーの IP アドレスが記載されています。この DNS 設定の IP アドレスを不正な DNS サーバーを指し示すものに変えることで、攻撃者はパソコン利用者の通信を不正なサイトへ誘導することが可能になります。

現在、欧米ではこのような悪さをする「DNS Changer」と呼ばれるウイルスが猛威を振るっているとの情報があります。実際の被害として、**アドレスを正しく打ち込んだとしても実際には本来のものとは異なる別のウェブページが表示されたり、ウェブページ内に埋め込まれている広告バナーが悪意あるサイトへのリンクを含む広告バナーに勝手に入れ替わっていたりする事例が確認されています。**

「DNS Changer」ウイルスに感染したまま放置した場合、もしくはウイルスは駆除したが、勝手に変更された DNS 設定を元に戻していない場合、上記のような予期せぬサイトへの接続などだけでなく、不正な DNS サーバーが停止させられたりすることで、ウェブ閲覧がすべてできなくなる恐れがあります。

日本では、現状では特に感染が起こっているとの報告はありませんが、今後は注意が必要です。

上記の症状が出ているなど、不安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。

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

		9月	10月	11月	12月	1月	2月
届出(a) 計		**7**	**15**	**7**	**7**	**8**	**13**
	被害あり(b)	5	8	5	7	7	9
	被害なし(c)	2	7	2	0	1	4
相談(d) 計		**31**	**46**	**69**	**42**	**35**	**37**
	被害あり(e)	8	7	14	13	9	14
	被害なし(f)	23	39	55	29	26	23
合計(a+d)		**38**	**61**	**76**	**49**	**43**	**50**
	被害あり(b+e)	13	15	19	20	16	23
	被害なし(c+f)	25	46	57	29	27	27

（1）不正アクセス届出状況

２月の届出件数は 13 件であり、そのうち**何らかの被害のあったものは９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37件であり､そのうち何らかの被害のあった件数は14件でした。

（3）被害状況

被害届出の内訳は、**侵入７件、なりすまし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５件（内、フィッシングに悪用するためのコンテンツ設置１件）、侵入後に DoS 攻撃の踏み台に悪用されていたものが２件でした。侵入の原因は、脆弱なパスワード設定が２件、phpMyAdmin のバージョンが古かったものが１件、サーバーの設定不備が１件でした（他は原因不明）。

「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、掲示板に管理者権限でログインされて勝手に内容を変更されたものが１件でした。

（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	・自分がログインしていない時期に何者かがログインした形跡があり、その後ログインできなくなった。その者がログイン後にパスワードを変更したと考えられる。 ・ゲーム内で所有アイテムが全て売却され、ゲーム内所持金も全て使われていた。 ・こうしたなりすまし行為に対しては、どのように対応したら良いか。警察に被害届けを出すと受理してくれるのか。
解説・対策	被害届けの提出は、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は、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） IPA -「オンラインゲームを楽しむ前にチェックしておきたい 3 つのセキュリティポイント」 http://www.ipa.go.jp/security/personal/onlinegame/ 「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/ インターネット安全・安心相談（警察庁） http://www.npa.go.jp/cybersafety/

［侵入］

（ii）遠隔操作ツールを埋め込まれ、結果としてフィッシングに悪用するページを設置された

事例	・組織外から「そちらのウェブサイトに、フィッシングに悪用するためのページがある」との連絡が入った。すぐに確認すると、FTP 用公開サーバーがクレジットカード会社のログインページを模したフィッシングサイトとして公開されていた。 ・調査したところ、サーバーに「Kryptonic Ghost Command Pro」という遠隔操作ツールが埋め込まれていた。また動作試験用のアカウントが残ったままだった。 ・当該アカウントが乗っ取られた後に「Kryptonic Ghost Command Pro」を埋め込まれ、フィッシングサイトに改ざんされたものと推測。
解説・対策	インターネットにサーバーを公開する場合、**悪意ある者に狙われて悪用されるかもしれない、ということを念頭に置いた対策が必要**です。特に今回のようにウェブサーバーとして公開していなくても、一旦侵入を許すと悪意あるウェブサイトとして公開されてしまうケースもあります。 フィッシングサイトへの改ざんは外部からの指摘により初めて気が付くことが多く、発見の遅れが被害の拡大につながる恐れがあります。**システム管理者は以下の対策を実施**するよう心がけてください。 ・適切なパスワード設定と管理を行う ・脆弱性を解消する（OS だけではなく、ウェブアプリケーションなども忘れずに） ・外部からのアクセス制限やセキュリティ設定を適切に行う （不要なサービスは停止する） ・こまめなログの確認 ・可能であれば、ファイル改ざん検知システムの導入 （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

2 月のウイルス・不正アクセス関連相談総件数は **1,073 件**でした。そのうち**『ワンクリック請求』に関する相談**が **218 件**（1 月：338 件）、**『偽セキュリティソフト』**に関する相談が **24 件**（1 月：18 件）、**Winny に関連する相談**が **25 件**（1 月：11 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 **2 件**（1 月：4 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

		9月	10月	11月	12月	1月	2月
合計		1,551	1,496	1,420	1,312	1,302	1,073
	自動応答システム	936	865	746	790	760	645
	電話	554	564	561	451	485	362
	電子メール	52	55	102	65	49	62
	その他	9	12	11	6	8	4

※ 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。

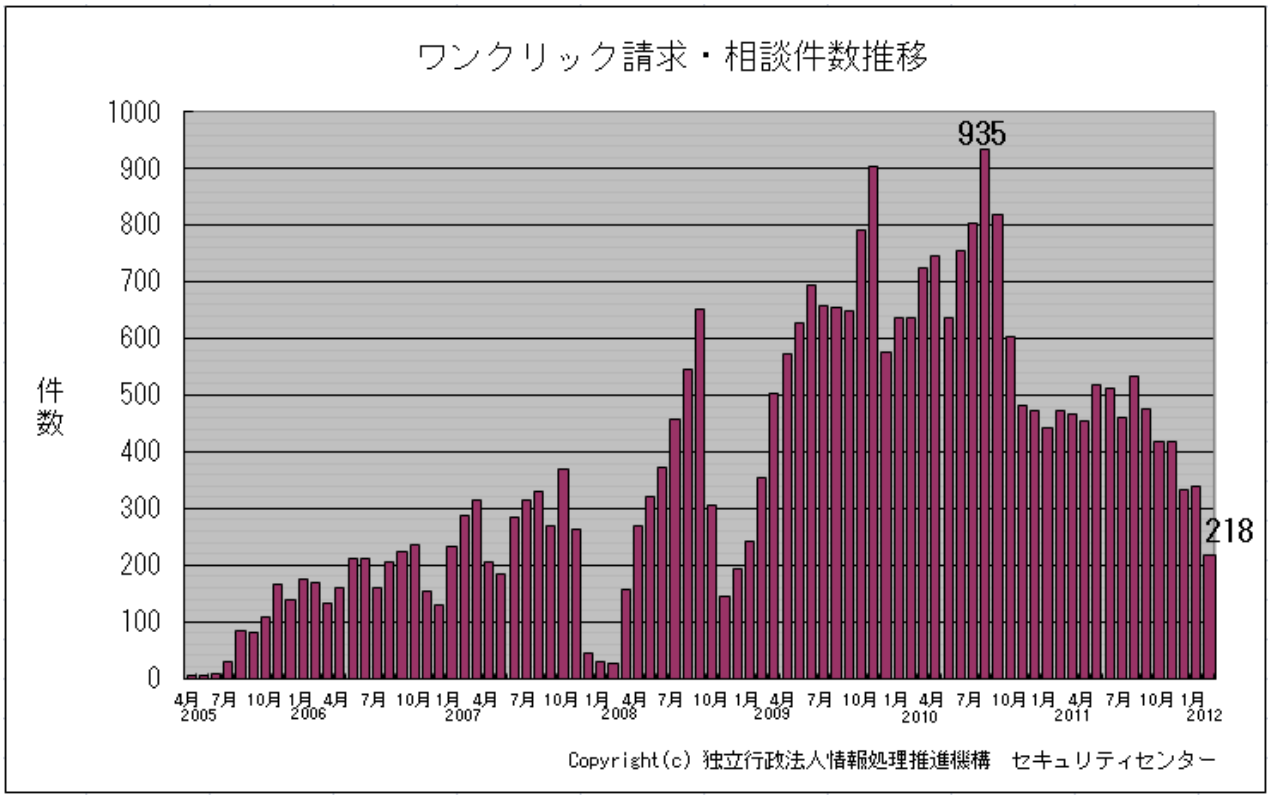

図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）シャットダウン時に、「他の人がログオンしている」とのメッセージが出てくる

	Windows パソコンをシャットダウンしようとすると、「ほかの人がこのコンピュータにログオンしています」というメッセージが出てくる。何者かがパソコンに不正アクセスしているのではないか？
回答	そのメッセージは、誰かがパソコン内の共有フォルダにアクセスしている場合や、別のユーザーから「ユーザーの切り替え」でログオンした場合に出てくるメッセージですが、それ以外に、自分一人だけ使用していても出てくる場合があります。簡単にいえば、自分を含め、**ログオンしたままのユーザーがいるにも関わらずシャットダウンしようとした際に出る**メッセージです。 例えば、パソコンの前から長時間離席してロック画面になり、そのままシャットダウンしようとすると、上記メッセージが出ることがあります。 上記メッセージが出た後にそのままシャットダウンしてしまうと、その時ログオン中の全てのユーザーの作業中データ等が消えてしまいますので、シャットダウン前に各ユーザーでログオフした後に、シャットダウンすることを勧めます。

（ii）IPA から添付ファイル付きの注意喚起メールが届いた

相談	独立行政法人情報処理推進機構（IPA）を差出人とした注意喚起メールを受け取った。メールにはファイルが添付されている。メールには、不審なメールに添付されたファイルを開いたり、リンクをクリックしたりしないように書かれている。このメールをどのように扱えばよいのか？
回答	あなたが受け取ったメールは、IPA からの注意喚起メールではありません。基本的に、IPA から不特定多数の方々へ注意喚起メールを送ることはしませんし、メールニュース登録者へファイルを添付したメールを送ることはしないというルールで運用しているからです。 昨今、不審なメールを受け取った場合の対処の訓練を行う組織が増えています。 組織によっては、不審なメールを受け取ったときの対処方法（インシデントレスポンス）を定めていることがあります。 **安易に不審メールに記載された送付元、連絡先にコンタクトすることは好ましくありません。そのようなメールを受け取った場合は組織の情報システム部門に連絡し、組織的な対処方法に従うようにしてください。** （ご参考） IPA テクニカルウォッチ『標的型攻撃メールの分析』に関するレポート ～ だましのテクニックの事例 4 件の紹介と標的型攻撃メールの分析・対策～ http://www.ipa.go.jp/about/technicalwatch/20111003.html IPA 対策のしおりシリーズ http://www.ipa.go.jp/security/antivirus/shiori.html コンピュータセキュリティインシデント対応ガイド（NIST SP800-61） http://www.ipa.go.jp/security/publications/nist/documents/SP800-61-rev1-J.pdf IT セキュリティ予防接種調査報告書 2009 年度（JPCERT/CC） http://www.jpcert.or.jp/research/#inoculation2009

『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