Information-technology
Promotion
Agency, Japan

第 13-20-288 号
2013 年 4 月 1 日
独立行政法人情報処理推進機構

今月の呼びかけ

「 どうして偽セキュリティ対策ソフトがインストールされるの？ 」
～　基本的な対策を知って、慎重にネットサーフィンしよう　～

“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、引き続き多く寄せられています。

2013 年 2 月以降は「Disk Antivirus Professional」という名称のものによる被害相談が特に多く、60 件以上の相談が寄せられています。3 月中旬から、それに代わり「AVASoft Professional Antivirus」に関する相談が増加しています（図 1 参照）。

相談者の状況を聞くと、この「Disk Antivirus Professional」や「AVASoft Professional Antivirus」がパソコンの中に侵入すると、**ブラウザなどのプログラムが正常に動作しなくなったり、ファイルが見えなくなったりします**。特にファイルが見えなくなると、重要ファイルのバックアップすらできなくなり非常に厄介です。

感染経路ははっきりしていませんが、被害者に感染した時の状況を聞くと“パソコン上のプログラムの更新を一切していなかった”、“大手検索サイトで検索した結果を片っ端からクリックした”というケースが多いようです。

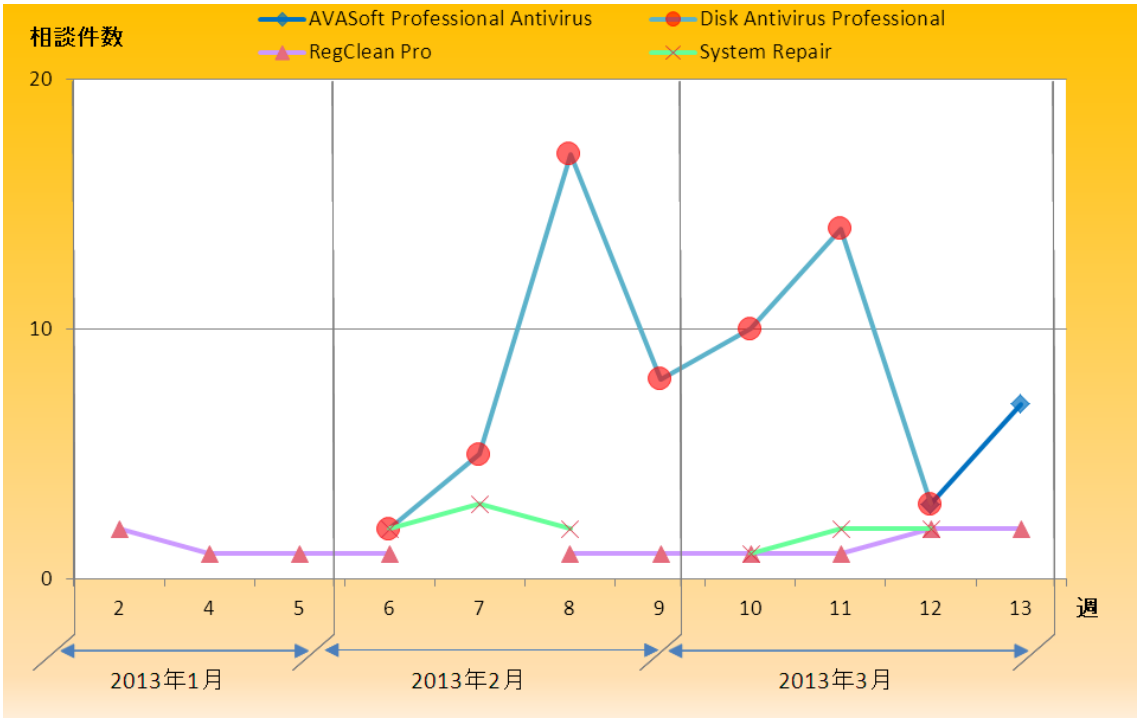

図 1：主な偽セキュリティ対策ソフト相談件数推移

「偽セキュリティ対策ソフト」型ウイルスの被害に遭わないための対策は、このウイルスに限った特別なものではなく、基本的なセキュリティ対策を漏れなく実施することです。ここでは感染させられるまでの手口を解説し、対策について説明します。

（1） 「偽セキュリティ対策ソフト」型ウイルスの概要

「偽セキュリティ対策ソフト」型ウイルスとは、“ウイルスに感染している”、“解決するために有償版の製品が必要”といった偽のメッセージを表示して、クレジットカード番号などを入力させて金銭を騙し取るタイプのウイルスです。

正規のセキュリティ対策ソフトと区別がつかないような画面と共に、ウイルス対策ソフトを連想させるソフト名とアイコンが表示されるため、注意が必要です。

この他にも、下記の「偽セキュリティ対策ソフト」型ウイルスに関する相談も IPA に寄せられています。亜種も含め、多種のウイルスが広くばら撒かれていることが推測されます。

・AVASoft Professional Antivirus
・System Repair
・System Progressive Protection
・Live Security Platinum
・Smart Fortress

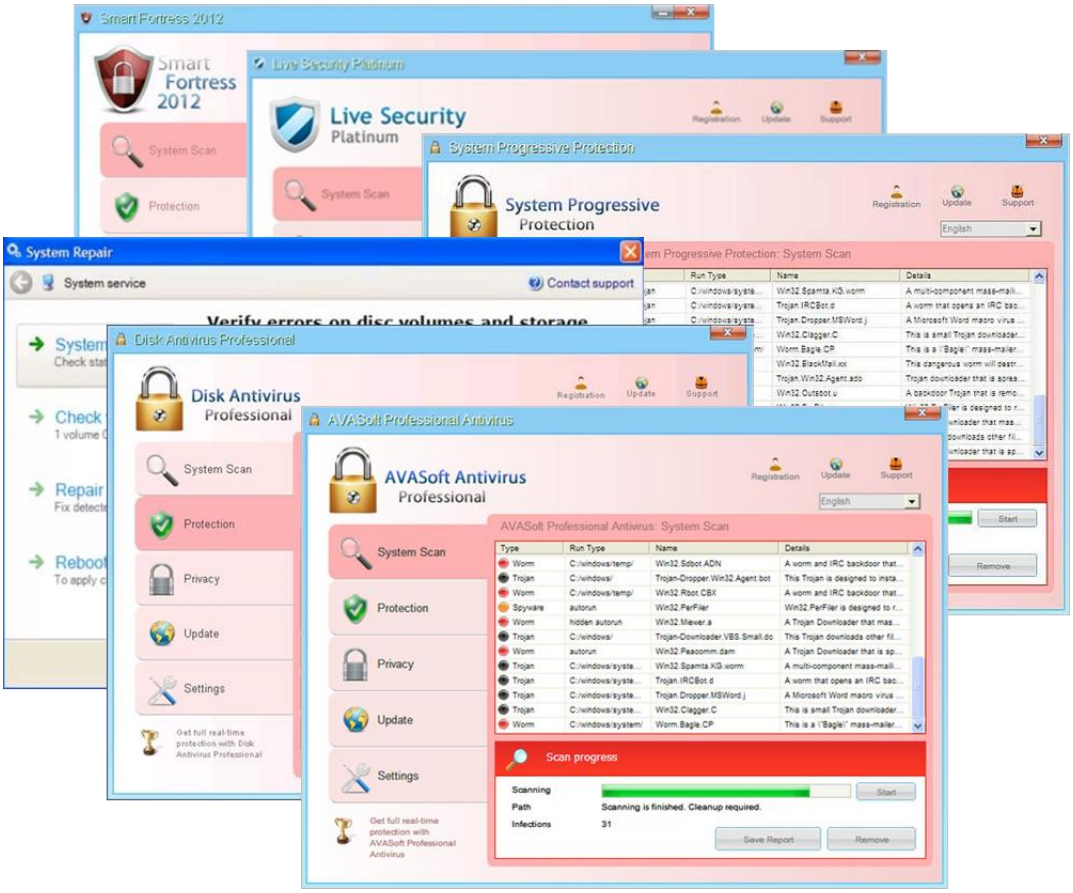

図 2：過去に IPA に相談があった「偽セキュリティ対策ソフト」型ウイルスの画面（一部）

この種のウイルスの中には、ウイルスの駆除やパソコンからのデータの退避（バックアップ）作業を妨害するものもあるため、深刻な被害となる場合があります。「偽セキュリティ対策ソフト」型ウイルスについての詳細は、以下の 2012 年 3 月の呼びかけも参照してください。

（ご参考）

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

(2)　「偽セキュリティ対策ソフト」型ウイルスの手口

悪意ある者（攻撃者）がセキュリティの弱いウェブサイトを改ざんします（図３の①）。罠を仕掛けておき、一般利用者が閲覧（図３の②）するのを待ちます。

その後、セキュリティ対策が実施されていないパソコンで当該ウェブサイトを閲覧すると、自動的に悪意あるウェブサイトに誘導されて（図 3 の③）、ウイルスが自動的にダウンロードされて感染してしまいます。

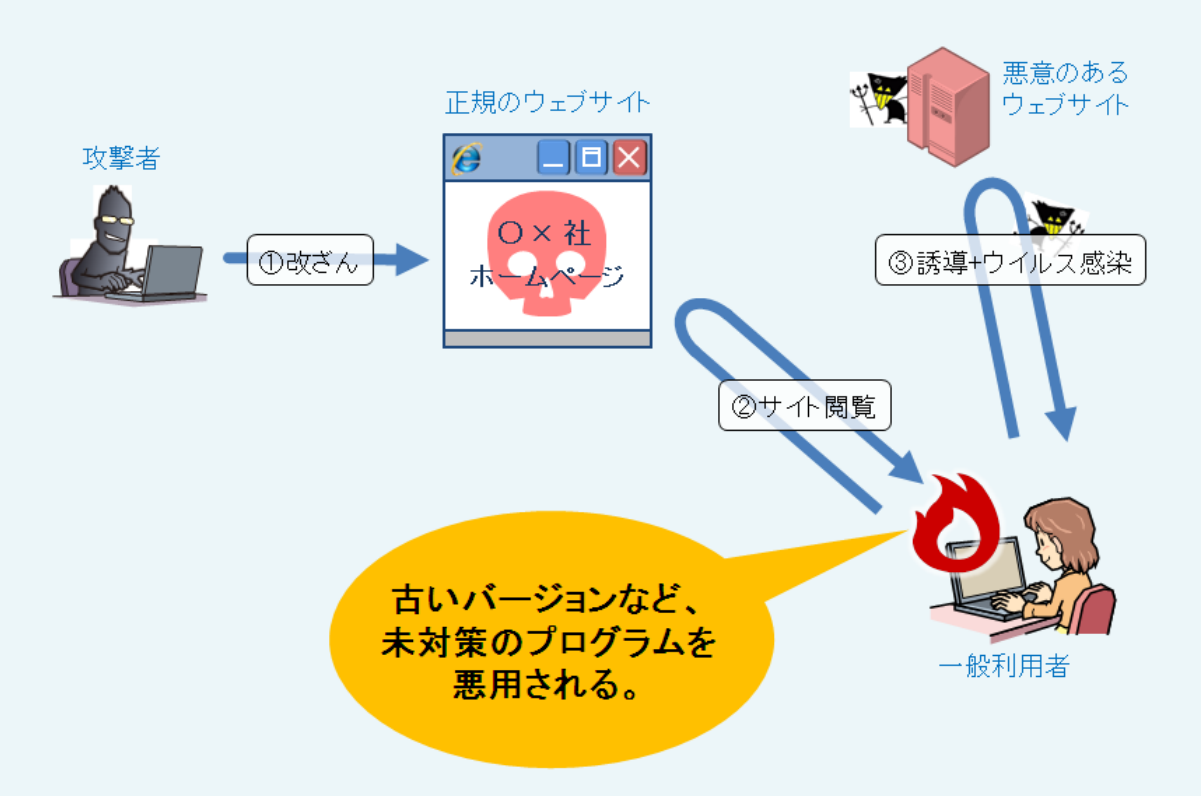

図３:「偽セキュリティ対策ソフト」型ウイルスに感染するまでのイメージ図

そのような状態でネットサーフィンしていると、突然パソコン内部のウイルスチェックをしているかのようなアニメーションが表示され（図 4）、不正プログラム、アドウェア、スパイウェアといった脅威を「検出」し、たくさんのウイルスが見つかったという英語の警告が表示されます（図 5）。

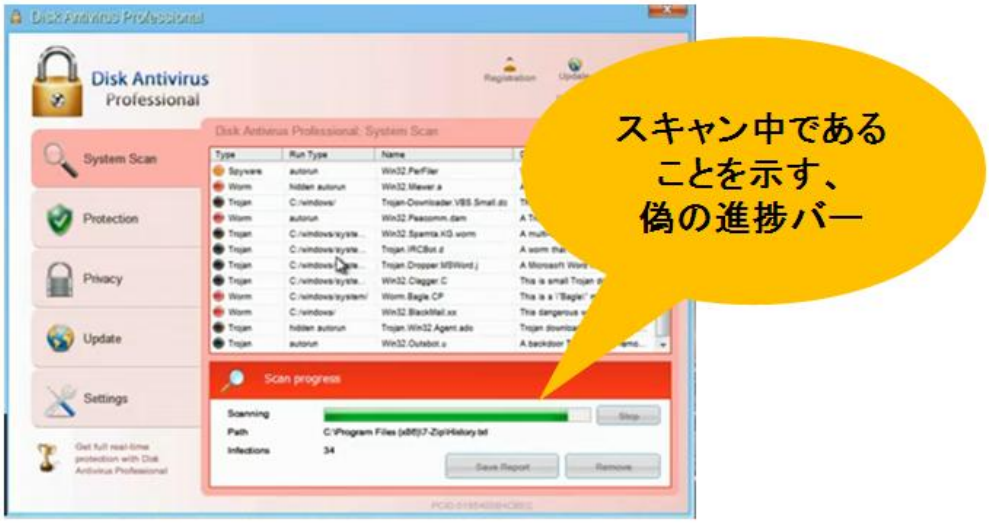

図４:「Disk Antivirus Professional」による偽のスキャン中画面

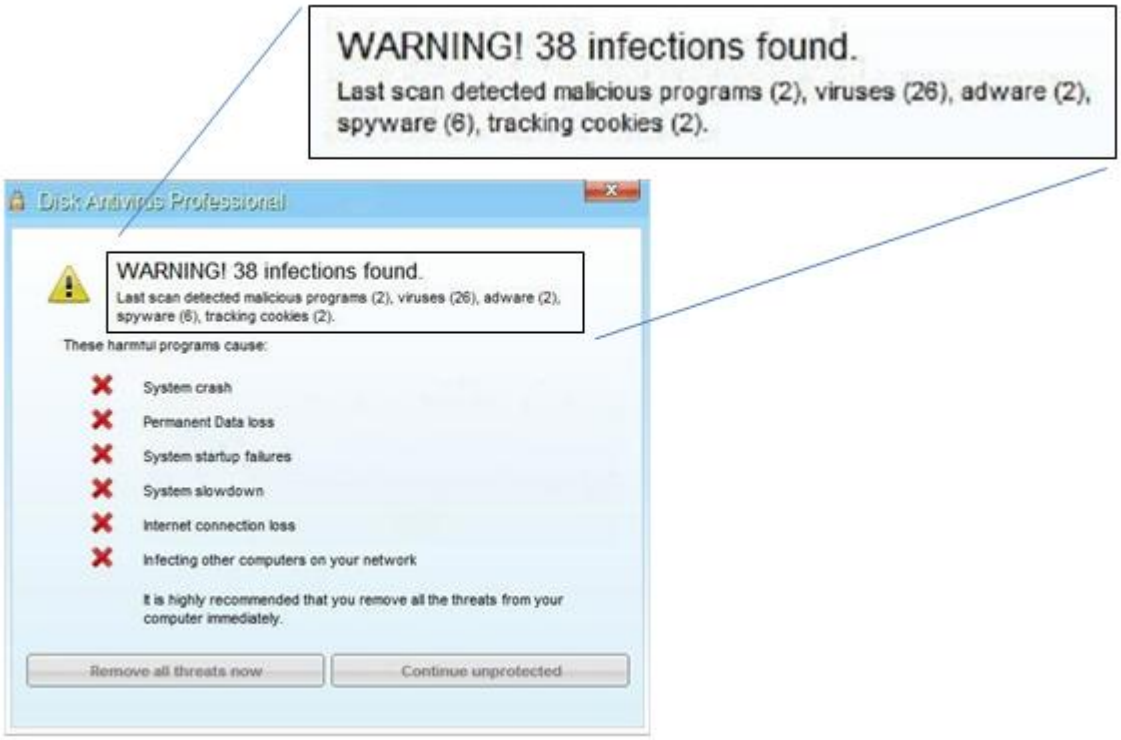

図 5：「Disk Antivirus Professional」が表示する偽のスキャン結果画面

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、ブラウザのお気に入りの中身を削除したりします。これは、この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かけます。 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利用者に思わせて、有償版製品を購入させようとしていると考えられます（図 6）。

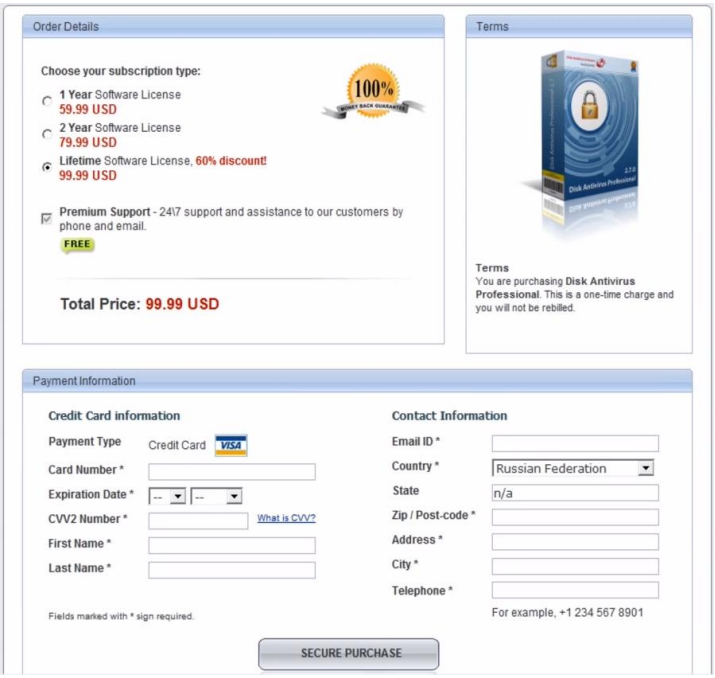

図 6：「Disk Antivirus Professional」が表示する偽の購入画面

ネットサーフィンをする個人利用者が「偽セキュリティ対策ソフト」型ウイルスの被害に遭わないための事前対策と、公開しているウェブサイトやブログが攻撃者の踏み台となって「偽セキュリティ対策ソフト」型ウイルスの被害者を生まないためにサイト管理者が行うべき対策は、次の（3）に示すとおりです。

（3） ウイルスの被害に遭わない対策と、被害者を生まない対策

(i) 一般利用者向け対策

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。

① OS と各種プログラムを常に最新状態にする（パソコンの脆弱性を解消する）

IPA へのウイルス届出によると、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 や各種プログラムの脆弱性を悪用するため、古いバージョンのままにせず、常に最新の状態に保つことが一番の対策になります。

Java、Flash Player、Adobe Reader は特に狙われやすいので、更新通知が画面に表示されたらその都度更新してください。

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ます。ぜひご活用ください。

（ご参考）

MyJVN バージョンチェッカ（IPA）
http://jvndb.jvn.jp/apis/myjvn/

かつては「怪しいサイトを閲覧しなければ大丈夫」と言われていた時期もありましたが、近年ではどのサイトが不正に改ざんされているか分からないため、セキュリティ対策を実施していないパソコンでインターネットを利用することは非常に危険です。従って、利用者自身で対策をして自衛することが不可欠です。

② ウイルス対策ソフトを“意識しながら”使用する

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。“ドライブ・バイ・ダウンロード”攻撃※1 を行うような有害なウェブサイトを閲覧することを防止する機能（ウェブレピュテーション機能など）を持つ、統合型セキュリティソフトを使用することで、感染被害を未然に防げる場合があります。

また、自分が使用しているウイルス対策ソフトの名称や動作を把握しておくことも大切です。普段から把握していることで、何か警告が表示された時に「偽セキュリティ対策ソフト」型ウイルスかどうかを判別しやすくなります。

※1 “ドライブ・バイ・ダウンロード”攻撃：ウェブサイトを閲覧した際に、パソコン利用者の意図に関わらず、利用者のパソコンにウイルスをダウンロードさせて感染させる攻撃。

③ 重要なデータを定期的にバックアップする

ウイルス感染に限らず、パソコンの故障など様々な原因によって、パソコン内のデータが失われる可能性があります。重要なデータは定期的にバックアップを行ってください。「偽セキュリティ対策ソフト」型ウイルスの中には、パソコンからのデータのバックアップ作業を妨害するものもあり、被害に遭った後では手遅れになってしまう場合があります。

定期的に、重要なデータを外部記憶媒体などにバックアップすることを勧めます。

パソコンにプログラムをインストールするなど、**パソコンに対して重要な変更を加えるタイミングで**バックアップすることも有効です。

市販のバックアップソフトを利用する方法もあります。クラウドを利用したオンラインバックアップ機能を持つ製品や、リカバリー機能を兼ね備えた製品もありますので、用途と目的に応じて製品を選択するといいでしょう。

また高度な知識が少し必要になりますが、Windows に付属の「バックアップと復元」や「ファイル履歴機能」を使用するのも良いでしょう。

（ご参考）

バックアップと復元（Windows 7）

http://windows.microsoft.com/ja-jp/windows7/products/features/backup-and-restore

ファイル履歴を使用する方法（Windows 8/Windows RT）

http://windows.microsoft.com/ja-jp/windows-8/how-use-file-history

(ii)　サイト管理者が行うべき対策

ウェブサイトが改ざんされてウイルスをばら撒くようなサイトにされてしまうと、一般利用者が閲覧した時にウイルス感染させてしまう恐れがあります。改ざんされてしまうと、ウイルスをばら撒いてしまうだけでなく、他のサーバーへの攻撃時の踏み台として悪用されるなど、被害が計り知れませんので、サイト管理者は自身が管理するウェブサイトが改ざんされないよう、適切に運用する必要があります。

サーバーが不正アクセスを受けて改ざんされないようにするには、サーバー上で以下の対策を行うことが有効です。

・サーバーの脆弱性の解消
・アカウント管理の見直し
・ウェブサイトを更新できる場所（IP アドレスなど）を限定
・ウェブサイト更新専用パソコンの使用

詳細は以下をご覧ください。

（ご参考）

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 テクニカルウォッチ

「2012 年の不正アクセス届出から読み解く、ウェブ改ざん被害の事例、傾向と対策」

http://www.ipa.go.jp/about/technicalwatch/20130213.html

（4） 被害時の対処方法

「偽セキュリティ対策ソフト」型ウイルスに感染してしまった場合、第一の対処方法としてパソコンの初期化を勧めています。他のウイルスも同時にパソコンに侵入している恐れがあるためです。実際、パソコンへの感染時に別のプログラムをダウンロードしようとする事例も確認しています。

しかし、事情によりすぐには初期化ができない場合もあると思います。その場合、次善の策として、以下の対処で復旧を試みてください。そしてデータのバックアップ後、初期化するなどしてください。

① 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。

② デスクトップ上のアイコンなど、パソコン内のファイル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。保存しておきたいファイルをバックアップするためには、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

③ ウイルス対策ソフトでの駆除ができない場合には、「システムの復元」による復元を試みます。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」が正常に終了しない、といった場合には、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。
「セーフモード」でも「システムの復元」が失敗する場合には、パソコンを初期化してください。

（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

④ パソコンのシャットダウン操作すらできない状態の場合、パソコン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」で起動します。詳しくは、パソコンの取り扱い説明書を参照するか、パソコンメーカーの問い合わせ窓口に確認してください。

なお、偽の表示によって購入を迫られて有償版製品を購入しても、その後状況が改善するとは限らないので、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勧めます。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/

（5） こんなときは…

急に見たことのないセキュリティソフトの画面が出てきたり、ウイルスをばら撒くようにウェブサイトを改ざんされてしまったりした場合には、IPA 安心相談窓口までご連絡ください。

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

※：迷惑メール対策などで「メールの受信/拒否設定」が設定されている場合、IPA からのメールを受信できない場合があります。 IPA からの返信メールを受信できるように、「anshin@ipa.go.jp」や「ipa.go.jp ドメイン」からのメールを受信できるように設定をしてください。

■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／田中
Tel:03-5978-7591　Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp