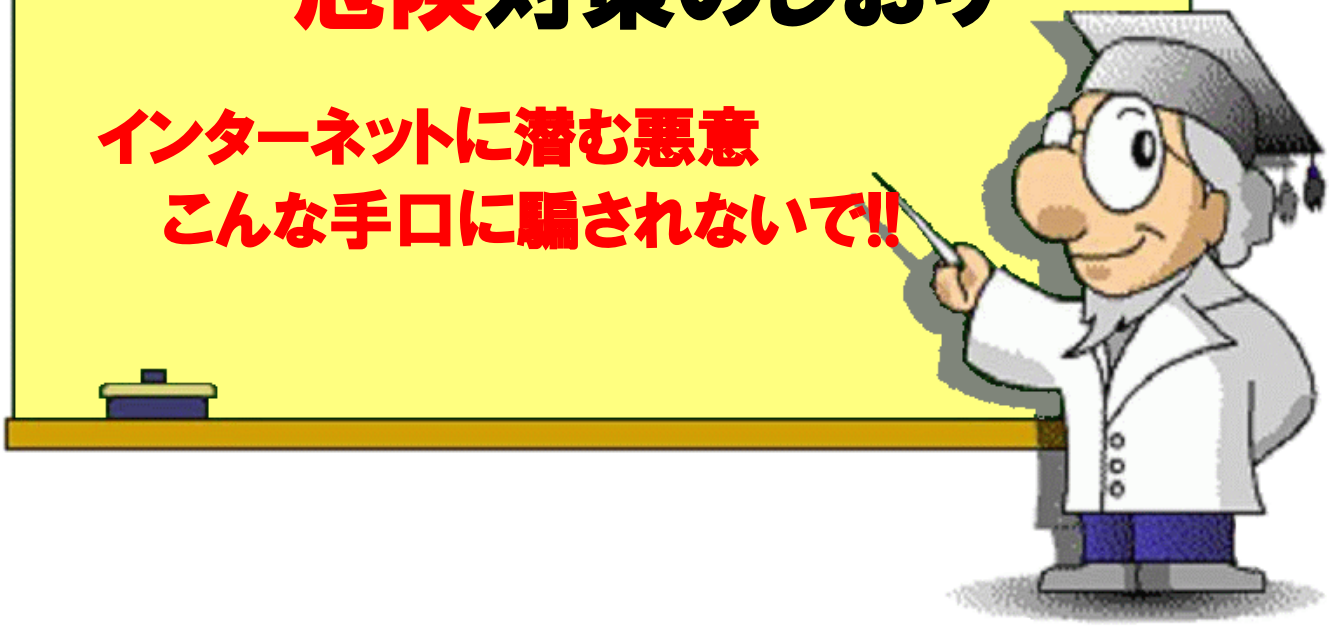
IPA 対策のしおり シリーズ (6)

インターネット利用時の危険対策のしおり

インターネットに潜む悪意
こんな手口に騙されないで!!



IPA 独立行政法人 情報処理推進機構
セキュリティセンター

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

2012年6月8日 第4版

1. インターネット上での悪意

インターネットを利用して様々なことができるようになってきました。ところが、インターネット上にはいろいろな悪意が存在します。一般の利用者が遭遇する悪意には、ウイルスメール*1、スパムメール*2と言ったメールがらみの悪意や、フィッシング*3と言った詐欺を目的とした行為、不正なプログラムを埋め込むために用意された悪意のあるウェブサイト、さらには、ネットワークを通じて感染活動や攻撃を行うボット*4やワーム*5と言ったウイルスの数々…。数えあげるのも大変な状況です。

そこで、悪意のある行為について、一般利用者向けにまとめてみました。

2. 悪意の傾向

一昔前のインターネット上での悪意は、コンピュータウイルスによる利用者への妨害行為が主流でした。しかしながら、近年の悪意は金銭の詐取を目的としたものに変わってきているようです。そのため、悪意のある行為が行われても、利用者が気付かないものが増えています。

また、ウイルスに関しては、亜種の発生頻度が高まるとともに、限られた範囲でのみ感染する地域性も生まれてきており、ウイルス対策ソフト*6でも検知が追いつかない（あるいはできない）状況も見受けられるようになっています。

さらに、悪意のある行為は、複合化の傾向があり、セキュリティ対策もウイルス対策ソフト単独では不十分な状況になっています。

3. 攻撃者の変化

技術不足によりクラッカー*7にはなりきれないスクリプトキディと呼ばれる人たちは、昔から存在していました。クラッカーやセキュリティ研究者が公開した情報を利用することで、不正プログラムの作成や不正アクセスを行う人たちです。彼らは、興味本位やいたずらのつもりで不正行為を行っていました。

しかしながら、近年ではウイルス作成ツール*8やルートキット*9と呼ばれるプログラムを利用することで、知識や技術がなくとも高度な機能を持ったウイルスを作成できる環境が用意されています。技術の追求ではなく、ウイルスを利用することを目的とする人たちが増えてきたようです。つまり、実社会の悪人がインターネット上にも進出してきたと言うことになります。

結果、攻撃者の目的が自己顕示ではなく、金銭の詐取になってきているようです。

インターネットの裏社会では、ウイルス作成ツールやルートキットが組織的に作成され、未公開のぜい弱性情報や管理されたボットネットワークを含めた不正行為を行うための環境が売買されています。

4. メールやインスタントメッセージサービス(IM)を介した悪意

代表的な、メールやインスタントメッセージサービス(IM)*10を介した悪意には、以下のものがあります。

- **ウイルス付きメール**
- **不当な広告や勧誘を行うスパムメールあるいはメッセージ**
- **不当なプログラムをダウンロードさせることが目的のウェブサイトに誘うメールあるいはメッセージ**
- **フィッシング目的のメールあるいはメッセージ**
- **利用者の不安を煽るデマメールあるいはメッセージ**

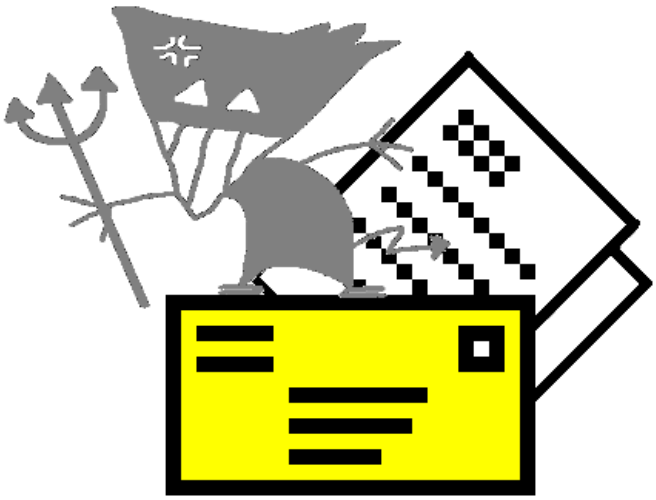
(1) ウイルス付きメール

ウイルス付きメールは、一般的に不特定多数の利用者に対して送信されます。ウイルスそのものが添付ファイルとして送られてくるメールのほか、メールを処理するメーラー*11のぜい弱性を利用したウイルスメールも存在します。

例えば、

- 私の写真です
- OS の修正プログラムです
- プレゼントです
- 大切なお知らせです
- 秘密の情報です
- 漏えい情報です

など、あなたにメールを開かせようとします。



このようなウイルス付きメールには、ウイルス対策ソフトの利用や、サービスを受けているプロバイダが提供するウイルスチェックサービスの利用が有効です。

しかし、これらのソフトやサービスを過信してはいけません。これらは、シグネチャ*12ベースの対策が主流であり、既知のウイルスにのみ有効で、最新のウイルスには無効な場合があります。

対策としては、以下の点に注意して**ウイルス対策ソフトを利用**すること、

- **ウイルス定義ファイル*13を常に最新のものにする**
- **定期的にウイルス検査を実施する**

さらには、

- **メーラーやオペレーティングシステム(OS)のぜい弱性を解消する**
- **メールサーバが提供するメールフィルタリングサービス*14を利用する**

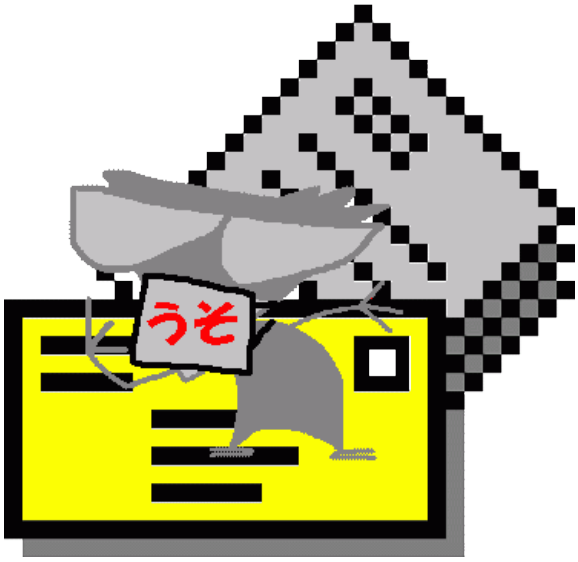
最後に一番重要な対策として、

- **見知らぬ人からのメールや添付ファイルは安易に開かない**
- **見た目が壊れたようなメールは開かない**
- **宛先不明で戻ってきたように見せかけたメールにも注意**

などが有効です。

(2) 不当な広告や勧誘を行うスパムメールあるいはメッセージ

不当な広告や勧誘を行うスパムメールあるいは IM からのスパムメッセージは、いろいろな理由で、急増することがあります。いままでにこのようなメールやメッセージを受け取ったことがない人もいれば、突然来るようになった人もいます。なかには、大量のメールやメッセージを受け取っている人もいます。大量に受け取ってしまう原因としては、自身のメールアドレスや IM 登録名がインターネット上で広く公開されてしまったことが考えられます。



これらのメールやメッセージについては、開いたり、読んだりするだけでは特に問題は発生しませんが、誘いに乗ると厄介なことに巻き込まれる可能性がありますので注意して下さい。特に金儲けの話や出会い系の話は、サイバー犯罪に巻き込まれる可能性があります。詳しくは以下のサイトをご覧下さい。

■ 警察庁 サイバー犯罪対策
http://www.npa.go.jp/cyber/

(3) 不当なプログラムをダウンロードさせることが目的のウェブサイトに誘うメールあるいはメッセージ

出会い系を含むアダルトサイトへ誘うメールあるいは IM からのメッセージや、金儲けの方法を謳ったメールあるいはメッセージに記述されたリンク(URL)には注意が必要です。

多くの**ワンクリック詐欺サイト**（後述）がこの方法を利用しており、不当な請求書が表示されるだけでなく、スパイウェア*[15]をダウンロードされ、あなたの個人情報が盗み出されることもあります。

対策としては、

- **見知らぬ人からのメールや添付ファイルは安易に開かない**
- **甘い誘いには慎重に**
- **ブラウザのセキュリティレベルを高く設定する**
- **パソコンの OS が発信する警告メッセージに注意する**

などが有効です。

(4) フィッシング目的のメールあるいはメッセージ

銀行や信販会社を装った、フィッシングサイトへ誘うメールや、偽のオンラインショッピングサイトや懸賞サイトへ誘うメールやメッセージにも注意が必要です。

メールやメッセージの中に記載されたリンク(URL)をクリックすると、そこは偽のサイト(フィッシングサイト)である可能性があります。メールやメッセージ、あるいはリンク先のウェブサイトの内容を安易に信用すると、あなたの個人情報を盗み出されることになります。

盗み出された個人情報が悪用されることで、銀行口座から勝手にお金を引き出されたり、受け取ってもいない商品の支払い請求がきたりする場合があります。いわゆる、なりすまし行為によって、被害にあうケースです。

対策としては、

- **銀行や信販会社からのメールを安易に信用しない**
- **リンクに頼らず、直接、銀行や信販会社のウェブサイトあるいは電話連絡で確認する**
- **リンク先の Web アドレスを確認する**
- **個人情報の入力画面では暗号通信(SSL)*[16]が行われているか確認する**

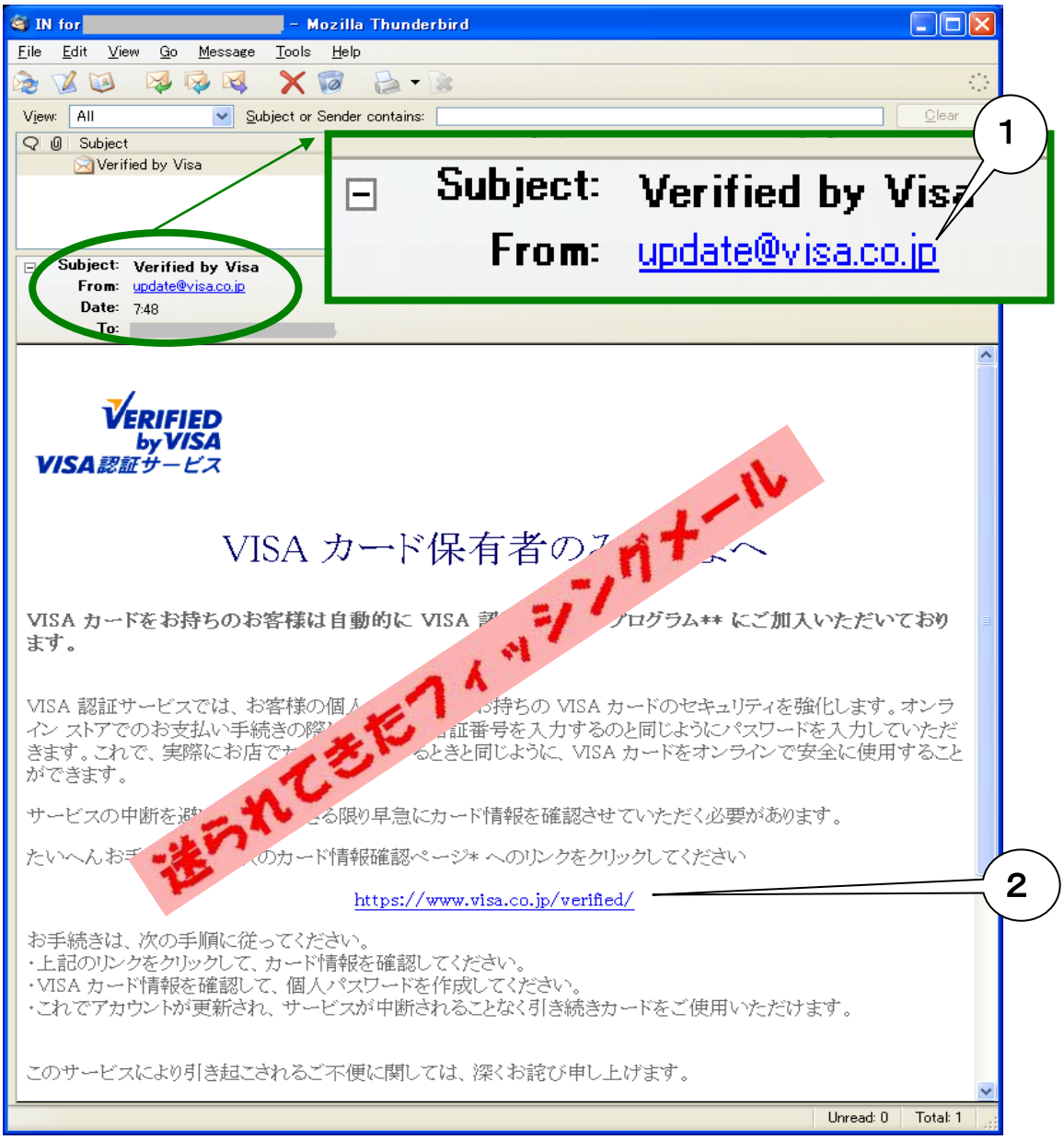
【確認方法】
個人情報などの重要な情報を入力する金融機関等のウェブサイトでは SSL を使用して通信を暗号化するのが一般的です。
利用者が SSL によりウェブサイトと接続されているときは、アドレス欄に「https://」と表示され、ブラウザの鍵マークがつながった状態で表示されていることを確認します。

などが挙げられますが、フィッシングサイトであるか見抜くのは、専門家でも難しいと言われています。最新のブラウザには、フィッシング対策機能が組み込まれているものが増えてきています。こういった最新のブラウザを利用するのも効果的ですが、対策の 2 番目に挙げた方法が一番確実な対策です。**自分で情報の真偽を確認する**と言うことです。

なお、フィッシングサイトによる個人情報の流失以外にも、推測されやすい利用者 ID・パスワードの利用、不特定多数の利用者のいるネットカフェなどでの個

人情報の入力などによっても、なりすまし行為の被害にあう可能性がありますので、注意して下さい。

以下に 2004 年 11 月に発見された VISA を騙ったフィッシングメールの例を示します。



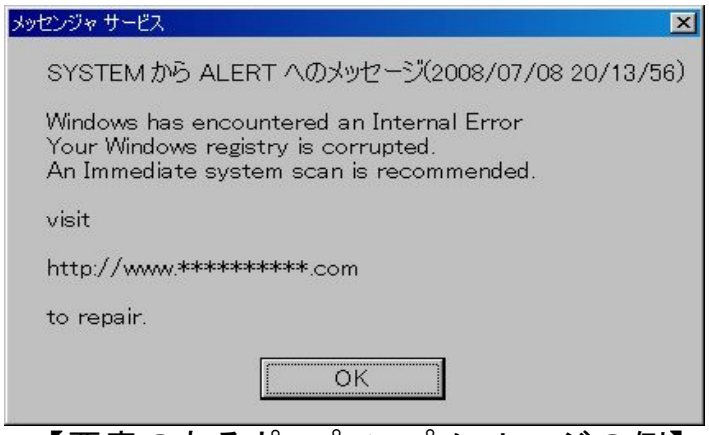
① 送信元が update@visa.co.jp の送信元詐称メール

② 文中のリンク https://www.visa.co.jp/verified/ は、VISA の正規の URL に見えるが、HTTP のソースでは http://xxx.196.163.74/verified/ を指していた。クリックするとフィッシング サイトへジャンプし、カード番号や ID 番号の入力を促す

(5) 利用者の不安を煽るデマメールあるいはメッセージ

偽の情報をメールやポップアップメッセージで送りつけ、利用者の不安を煽るものがあります。

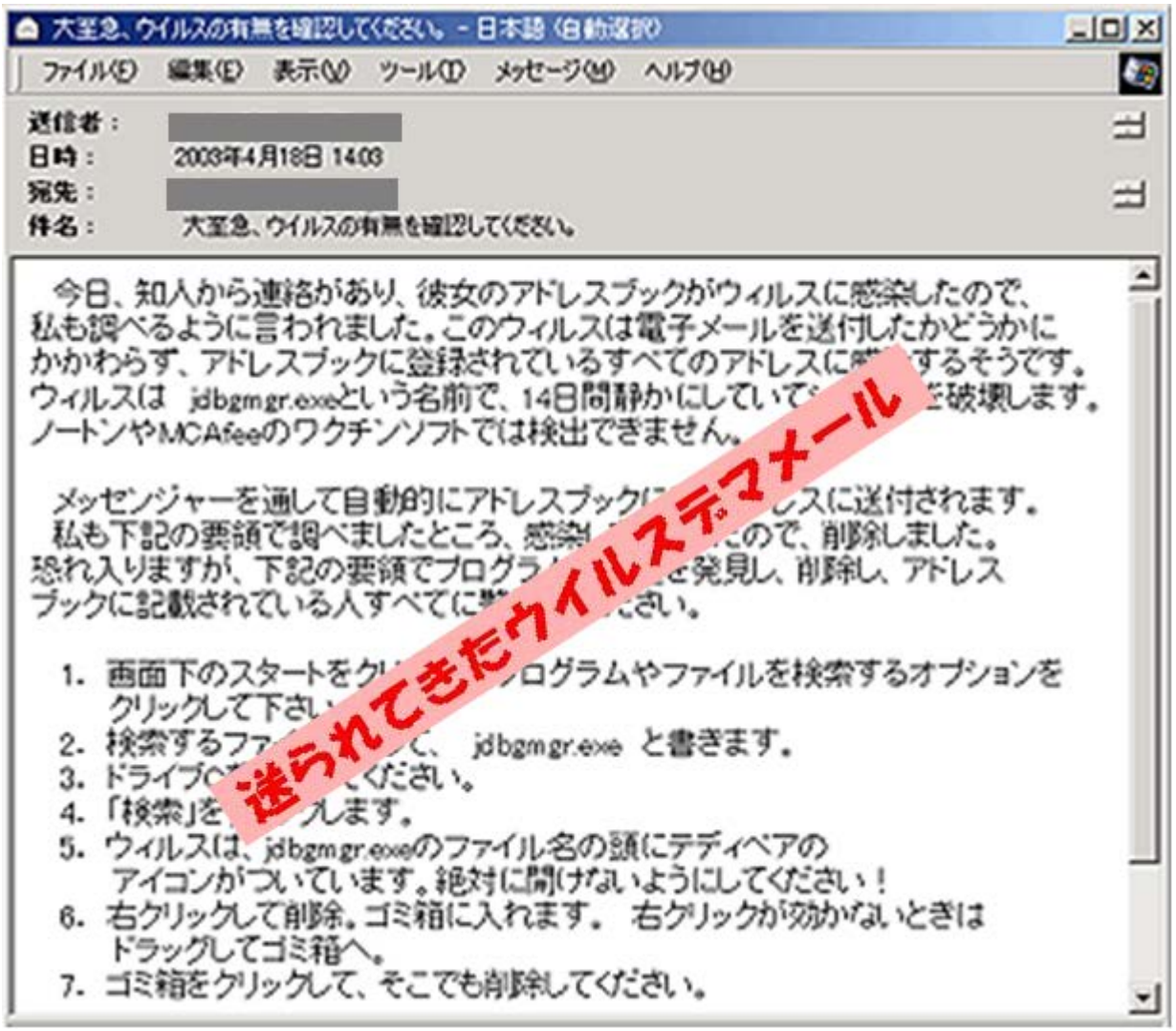
例えば、ウイルスデマメールのように、あたかもウイルスが蔓延しているような情報を送りつけ、利用者が指示にしたがって指定されたファイルを削除すると、実はそのファイルは正規のファイルであったりします。



【悪意のあるポップアップメッセージの例】

最近では、「戦争が始まった」とか「アメリカの大統領が死んだ」とかをメールの件名に記載し、利用者の興味を引かせ、添付ファイルを開かせるようなウイルスもありましたし、いわゆるワンクリック詐欺で使用されるメールもデマメールの一種と考えられます。

少し古い例ですが、ウイルスデマメールの例を以下に示します。



このようなメールを受け取っても慌てないで下さい。『jdbgmgr.exe というファイルはウイルスなので、削除しなさい』という内容ですが、このファイル名は、マイクロソフト社の正規の Java デバッグ用のプログラムの名称であり、必ずしもウイルスに感染しているファイルではありません。 ウイルス対策ソフトでウイルスが検出されない場合は、削除しないで下さい。

対策としては、

- **何となくおかしいなと感じたら、自分自身で真偽を確かめるために、メールに記載されたキーワード（例で言えば『jdbgmgr.exe』）でインターネット検索してみる**
- **「他の人にも転送して下さい」は危ないキーワード、チェーンメールにならないように、他の人に転送しない**
- **ウイルスに感染している可能性については、自身が利用しているウイルス対策ソフトでウイルス検査を実施する**
- **ウイルス対策ソフトをお持ちでないならば、ウイルス対策ベンダーが提供している無償のオンラインウイルススキャンを実施してみる**

などが挙げられます。

デマメールに関する情報は以下に示すサイトでもご覧になれます。参考にして下さい。

■ VirusHoaxes(偽ウイルス)のデマメールに関する情報
http://www.ipa.go.jp/security/topics/virus_hoax.html

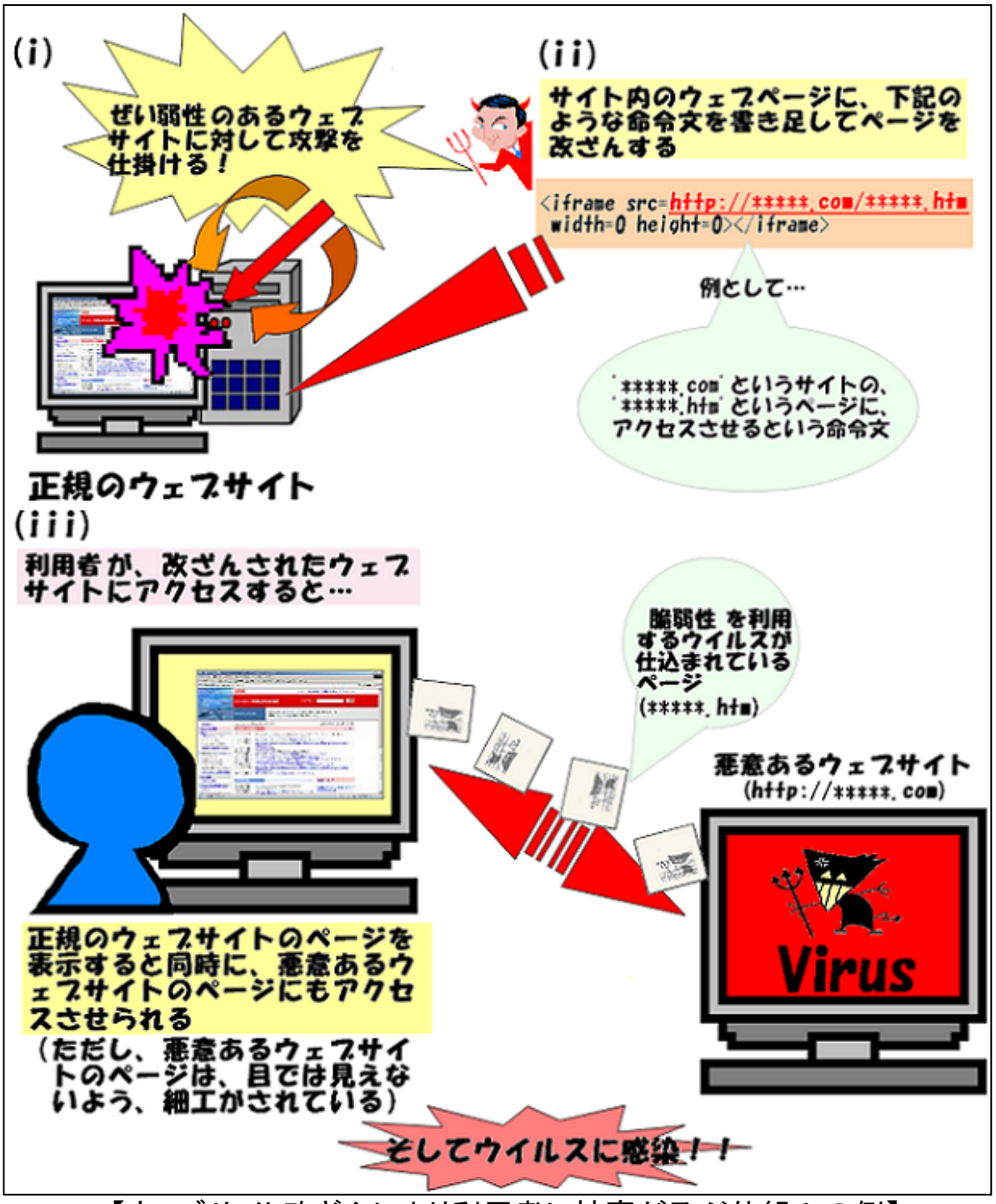
■ 「jdbgmgr.exe」に関するデマメール情報
http://www.ipa.go.jp/security/topics/alert140515.html

■ ウィルスデマ情報（トレンドマイクロ）
https://imperia.trendmicro-europe.com/jp/threat/threats-knowledge/non-virus/

5. ウェブサイトを介した悪意

(1) 改ざんされたウェブサイトへの訪問で…

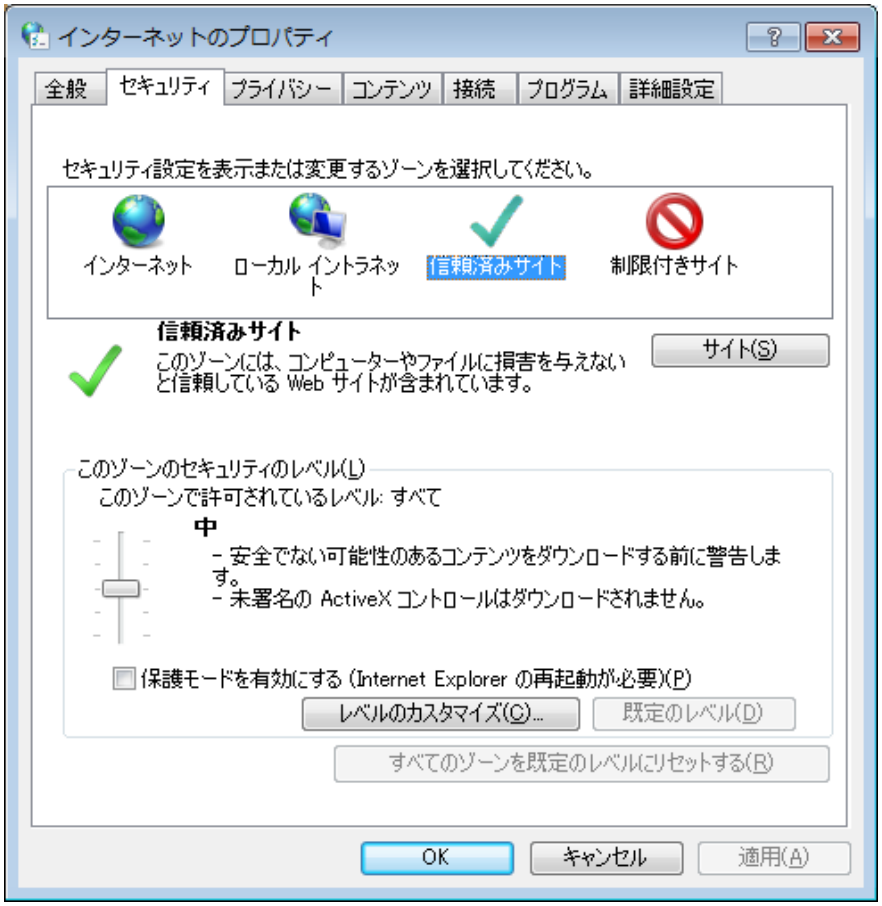
2007 年後半になってから、不正アクセスにより改ざんされるウェブサイトが急増しています。これらのウェブサイトの見かけは変わっていませんが、見えないところに仕掛けられたコードにより、利用者を悪意のあるウェブサイトに誘導し、結果的に、利用者のパソコンに不正なプログラム(ウイルス等)がインストールされる危険性があります。



【ウェブサイト改ざんにより利用者に被害が及ぶ仕組みの例】

いままでは、ウェブサイトを閲覧する際にはブラウザのセキュリティ設定を強化し、信頼できないサイトと信頼できるサイトを区別してアクセスすることが推奨されていましたが、近頃は信頼していたサイトも危ない状況になっています。

たとえば、MicrosoftのIE（Internet　Explorer）では、セキュリティゾーン*17の考え方により、インターネット、イントラネット、信頼済みサイト、制限付きサイトに分けて、それぞれのセキュリティ設定ができるようになっています。



【Microsoft　IE8 のセキュリティ設定オプション】

このような設定が有効となる背景には、信頼できるサイトは「改ざんなど受けない」ことが前提となっているわけで、利用者の預かり知らないところで問題が発生する危険があることが、最近のウェブサイトの脅威と言えます。

なんとも厄介な状況です。この状況での一般利用者の対策は2つあります。

- **パソコンの OS やアプリケーションのぜい弱性を解消する(最新の状態にする)**
  - 使用中のパソコンの OS が Windows の場合は、Windows Update あるいは Microsoft Update の実施
  - 使用中の Web ブラウザを最新版に（さらに更新状況を確認）
- **Web を参照するためのブラウザのセキュリティ設定を強化する**
  - セキュリティ設定の強化された最新のブラウザを選択
  - ActiveX、JavaScript の動作抑止

と言うことになります。

当然、前述した信頼済みのサイトでも同様にセキュリティ設定を強化したブラウザで訪問することを推奨します。いろいろな便利な機能の利用や、情報の利用ができなくなる問題は残りますが…

利用者が企業(組織)の中にいる場合は、企業(組織)としてイントラネット-インターネットの出入り口(ゲートウェイ)にプロキシサーバ*18を設置することで、改ざんされたウェブサイトに埋め込まれた不正なコード(特に不正なウェブサイトへ誘導するコード)を無効にする(事前に登録したウェブサイト以外は、利用者によるアクセス許可を必要とする等)方法も効果があるようです。最近では、不正と認定されたウェブサイトの情報を広く共有しWeb(URL)フィルタリング*19を行うことのできるサービスも提供され始めています。

一般の利用者の場合は、上記のような仕組みを構築することが困難なため、一部のセキュリティ対策ベンダーが提供する統合セキュリティソフトを利用したり、セキュリティ機能が強化されたブラウザを利用したりすることで、不正と認定されたウェブサイトをフィルタリングすることができます。

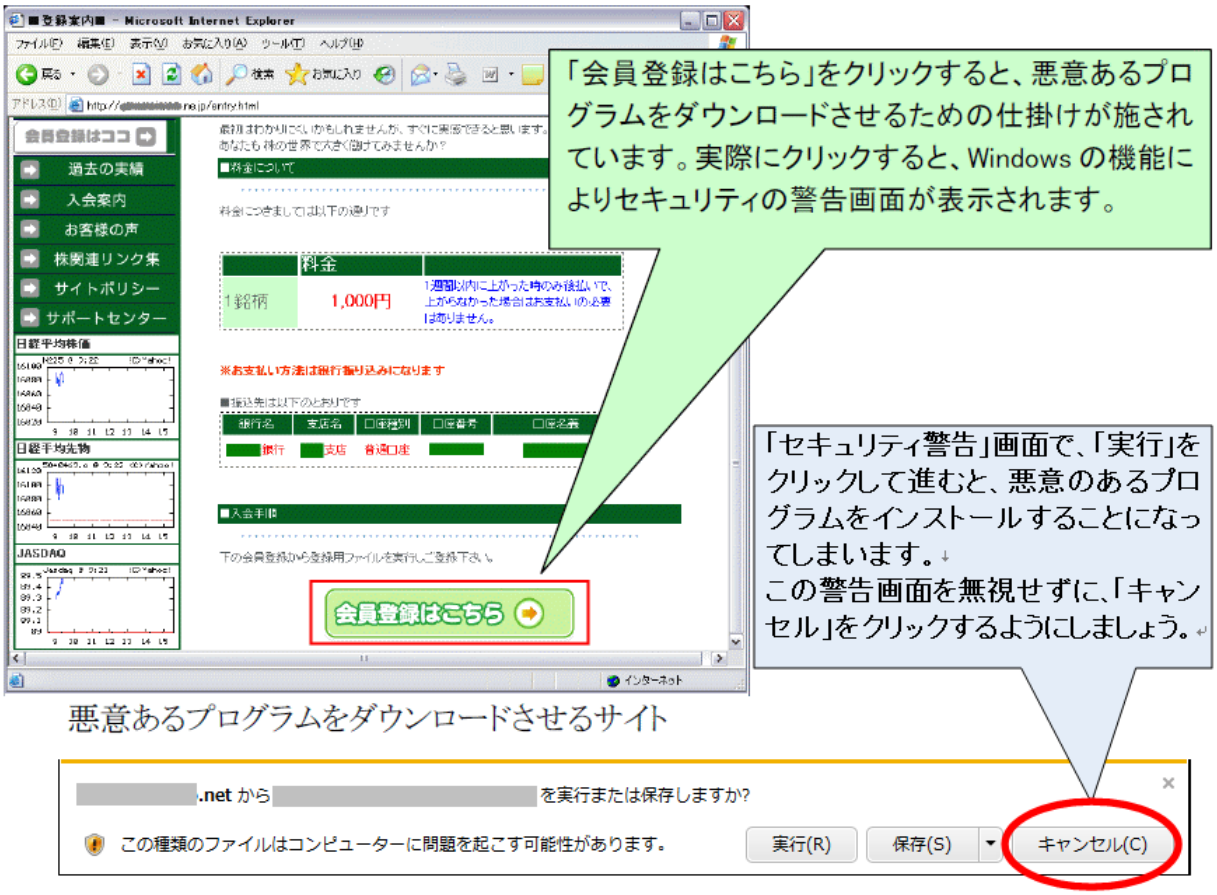
ブラウザ Firefox＋アドオン NoScript で、NoScript のオプション<IFRAME>禁止 の設定を行うのが、現状ではセキュリティ上 Best？
ただし、Microsoft IE でないと正しく表示されない(機能しない)ウェブサイトもあるようなので注意が必要です。サイトによってブラウザを使い分けるか、Firefox＋IE エンジンが使えるアドオンを利用する方法があります。
いずれにしても、訪問したサイトが安全かどうかの判断(スクリプトを許すかどうか)は利用者が行う必要があります。ご注意下さい。

広く一般の利用者へ情報発信するウェブサイトの管理者には、このような問題が発生しないように、ウェブサイトが改ざんされることのないようウェブサイトのぜい弱性の解消やセキュアな運用を期待します。

(2) 利用者を騙すウェブサイト

不正アクセスにより改ざんされたウェブサイト以外にも、悪意のあるウェブサイトは存在します。ワンクリック詐欺(不正請求)サイトやフィッシング詐欺サイト、偽セキュリティ対策ソフトを提供するサイト、利用者の興味を引き付けて不正なサイトに誘い込む迷惑ブログサイト等々、不正な利用料の請求をしたり、個人情報を詐取したり、役にも立たないソフトウェアを売りつけたり…悪意のウェブサイトは出現しては消え、同じような手口で利用者を騙し続けています。

(a) ワンクリック詐欺(不正請求)サイト



【ワンクリック詐欺(不正請求)サイトの例】

～　危ないサイトはアダルトサイトだけではない　～

ワンクリック詐欺(不正請求)の被害は、主にアダルトサイトで発生しています。サイト上で映像表示ボタン等をクリックすると、映像の代わりに不正な請求書が表示されました(ワンクリウェア*20と呼ばれるウイルスをインストールして、不正な請求書をパソコンの画面上に常に表示させる事例もあります)。

ところが、アダルトサイト以外のサイトでも同様の手口が確認されています。上記例のサイト(投資関係)では、確実に利益をあげられる株式情報を提供するという案内を記載し、会員登録をするように促しています。この会員登録という項目をクリックすると、ウイルスなどの悪意のあるプログラムをダウンロードさせる仕組みになっています。

これらの被害に遭わないよう、信頼できないサイトにはアクセスしない、アクセスしてしまっても、安易なダウンロードは避けることを心掛けて下さい。例に示すWindows によるセキュリティの警告画面が表示された場合は、決して「実行」をクリックすることなく、**「キャンセル」をクリック**して先に進まないように…

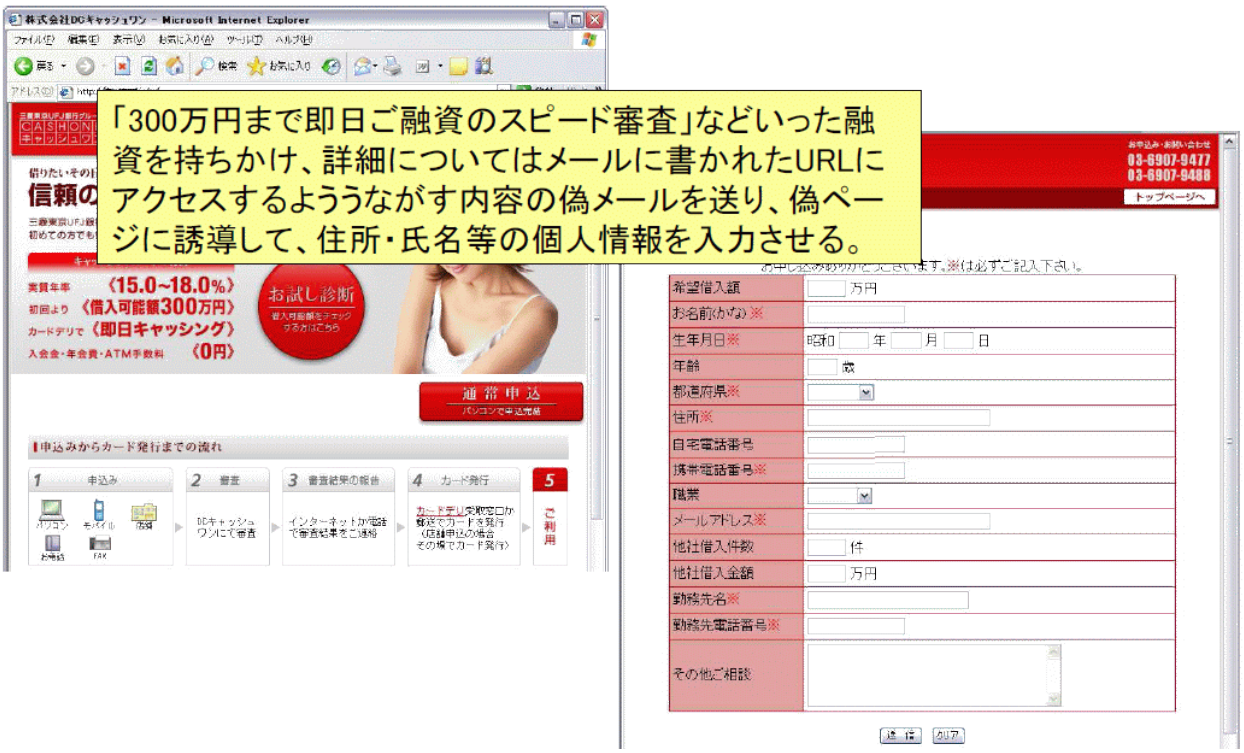
ワンクリック詐欺(不正請求)についてもっと詳細に知りたい方は、以下のサイト

の参照をお勧めします。

■ 身に覚えのない不正請求などの防止

http://www.ipa.go.jp/security/personal/protect/oneclick.html

(b) フィッシングサイト



【フィッシングサイトの例：2007 年 3 月】

フィッシングメールから誘導されたサイトでは、利用者を騙して個人情報等を入力させます。ここで入力した情報は、フィッシングサイト運営者に筒抜けになるわけです。

個人情報を知られてしまうと、その情報を基に更なるフィッシング目的の攻撃が行われる危険性もあります。

紹介した事例以外にも、各種のインターネットサービス(銀行やインターネットサービスプロバイダ等)に見せかけたフィッシングサイトを用意して、利用者 ID やパスワードを入力させるものもあります。利用者 ID やパスワードが詐取されると、本来の利用者が状況を確認できないように、パスワードを含む契約変更が行われ、場合によっては取り返しのつかない状況になります。

最近では、インターネット接続のためのブラウザを最新のものに変更すると、フィッシングサイトをある程度判断して利用者に警告を発する機能が搭載されていますが、基本的には、甘い誘いのメールの内容は警戒し、メール中のリンクを安易にクリックしないことが大切です。

フィッシングについてもっと詳細に知りたい方は、以下のサイトの参照をお勧

めします。

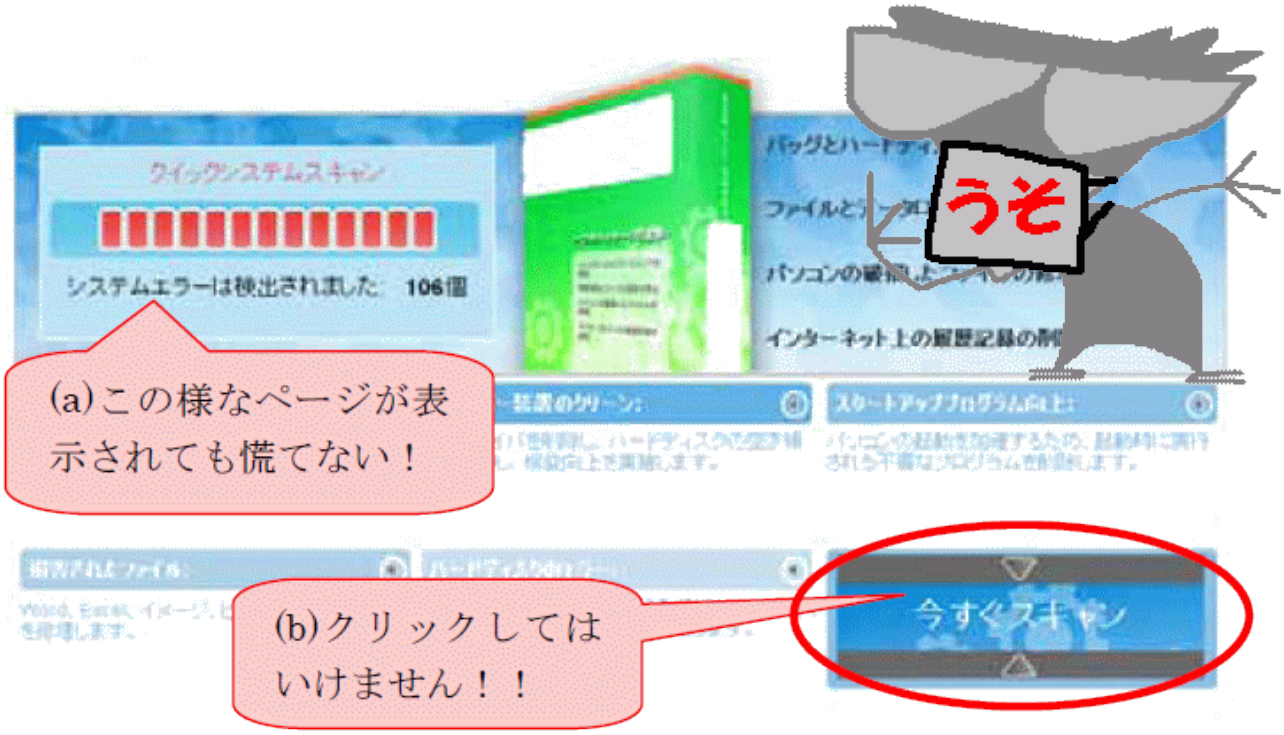
■ フィッシング（Phishing)対策

http://www.ipa.go.jp/security/personal/protect/phishing.html

■ AntiPhishingJapan フィッシング対策協議会

http://www.antiphishing.jp/

(c) 偽セキュリティ対策ソフトを提供するサイト



【偽セキュリティ対策ソフトの例：ウェブサイト上の広告画像（バナー広告）】

インターネットを利用していて突然、**「あなたのパソコンからウイルスが発見されました」**、**「あなたのパソコンにはエラーが発生しています」**といった内容のメッセージ画面が表示されて、それらの問題を解消するためには画面に表示されている「セキュリティ対策ソフト」の購入をするように勧められます。実際には、ほとんどの場合、メッセージを偽って表示して、問題が無くても問題があるように見せかけて、セキュリティ対策ソフトの代金を支払わせようとする悪質な行為です。代金を支払っても、そもそも問題がないわけですから、何の解決にもなりません。

場合によっては、インストールしたソフトがウイルスであり、パソコンにさまざまな悪意の仕掛けを埋め込まれる危険性もあります。

最近では、この類のソフトウェアをスケアウェア(脅迫ソフトウェア)と呼ぶ人たちもいますが、根拠のないことで利用者を脅し、金銭を巻き上げる行為はワンクリック詐欺(不正請求)と同じ問題と言えます。

(d) 迷惑ブログサイトあるいは迷惑ブログコメント/トラックバック

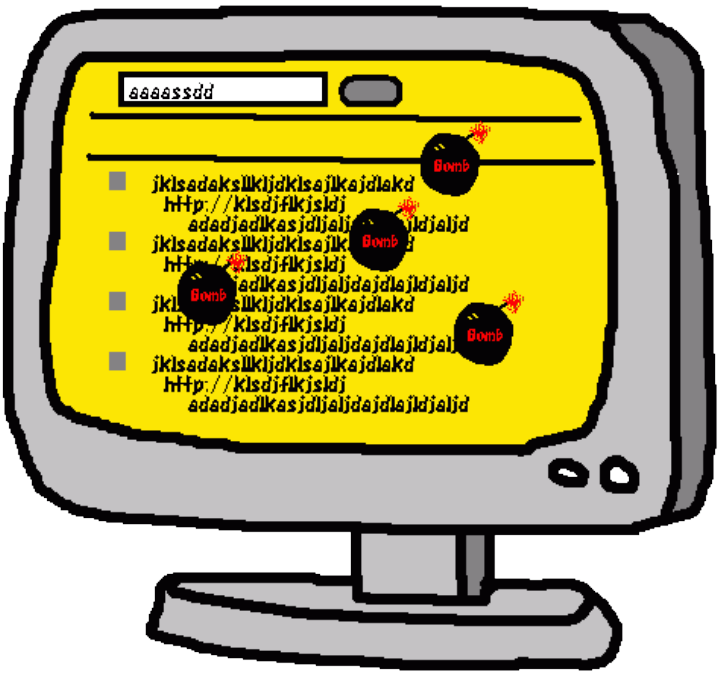
利用者が興味を引きそうな情報を提供するように見せかけて、不正なサイトへ誘導するリンクをクリックさせる迷惑ブログサイト(有名人の情報/重大事件の情報等)、あるいは、一般のブログサイトへの迷惑コメントや迷惑トラックバックの書き込みにより、利用者を不正なサイトへ誘導するような行為も見受けられます。

迷惑(スパム)メールのような能動的なものではありませんが、罠を仕掛けて獲物を待つような悪意にも注意が必要です。

このような情報に悪意があるか否かを判別することはとても難しいので、(1)で挙げた利用者の対策をしっかり実施しておきましょう。

(3) SEO ポイズニング

SEO(Search Engine Optimization:検索エンジン最適化)ポイズニングとは、検索エンジンに用意された検索エンジン最適化機能を悪用して、悪意のあるサイトを検索結果の上位に表示させる行為です。この手口により、Google や Yahoo 等の検索エンジンを使い、人気の高い検索キーワードに対して、悪意のあるウェブサイトに利用者を誘いこむ事例が、数多く、検索エンジン提供元に報告されています。



利用者によっては、検索エンジンによる検索結果の上位に表示された情報を信用する場合が多いようですが、検索結果が必ずしも信用できるサイトである保証はありません。

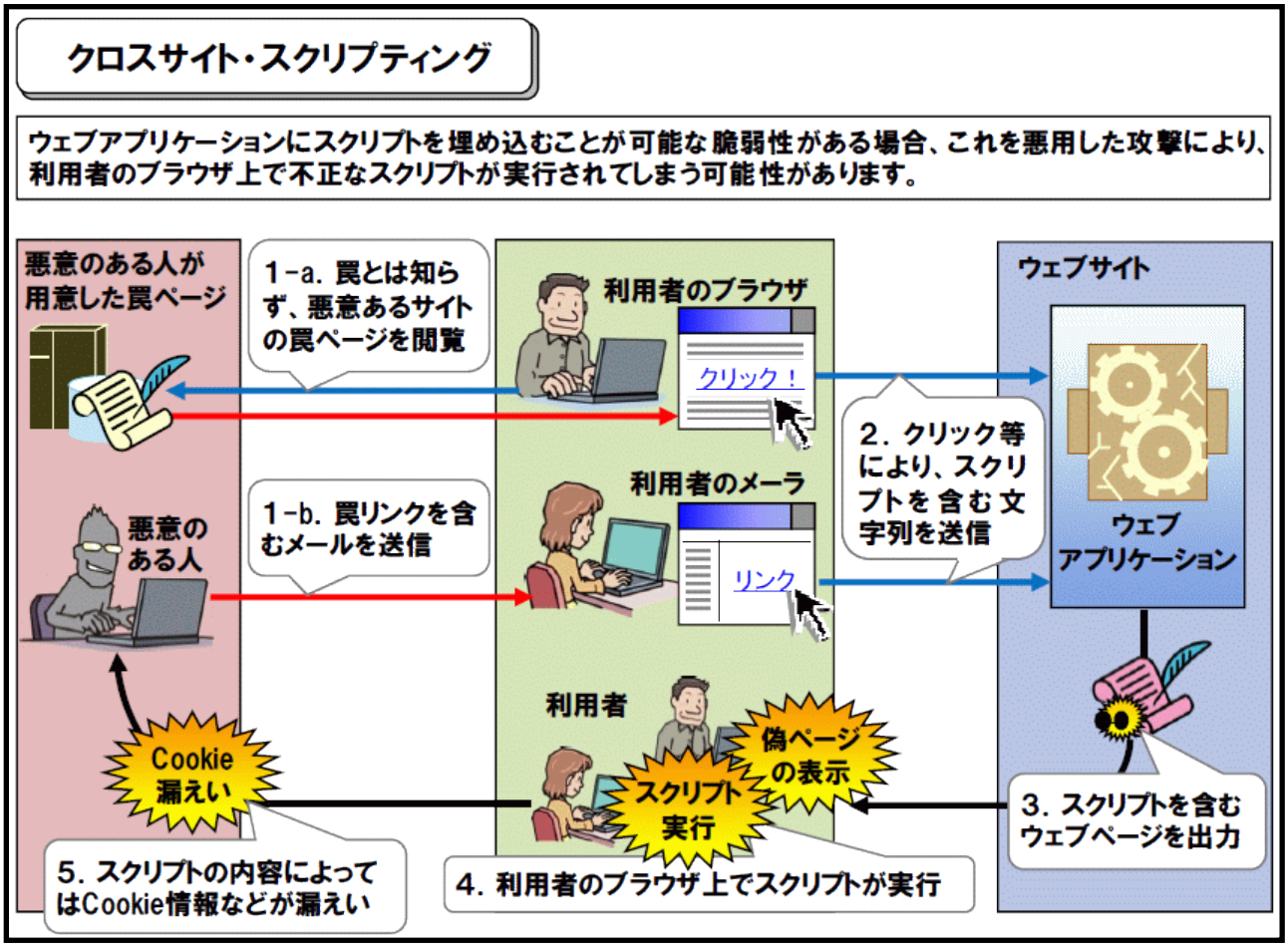
最悪の場合は、スパイウェアやボットと呼ばれるコンピュータウイルスを強制的にダウンロードさせるサイトが上位に表示される場合もありますので、**ブラウザのセキュリティ設定の強化や各種のセキュリティ対策ソフトの利用が推奨されます。さらに利用者のパソコンのぜい弱性が利用される場合もありますので、利用しているパソコンのセキュリティ更新を忘れずに実施して下さい。**

(4) ぜい弱性を持つウェブサイト

クロスサイト・スクリプティング(XSS)に代表されるぜい弱性を持つ利用者の脅威となるウェブサイトが多数存在します。これらのサイトは利用者の書き込みが多く行われる掲示板サイト、会員登録のあるサイト、ショッピングサイトなどに多く見受けられるようです。

悪意のある攻撃者が、利用者をフィッシング等の手口で不正なウェブサイトに誘導し、ぜい弱性のあるウェブサイトを模倣した入力域からの利用者の入力値に悪意のスクリプトを紛れ込ませ、さらにぜい弱性のあるウェブサイトへ利用者を誘い込めば、利用者のブラウザ上で悪意のスクリプトを実行させることができます。

最悪の場合は、ブラウザが完全に乗っ取られ、偽情報の表示、個人情報の流出、セッションハイジャックや不正なコードのダウンロード等も行われる危険性があります。(1)で示した改ざんされたウェブサイトと違い、そのウェブサイトの管理者も気が付かない場合は、とても危険な(野放しの)存在と言えます。ウェブサイトの管理者には、このような問題が発生しないように、ウェブサイトのぜい弱性について理解し、それらの問題の解消やセキュアな運用を期待します。



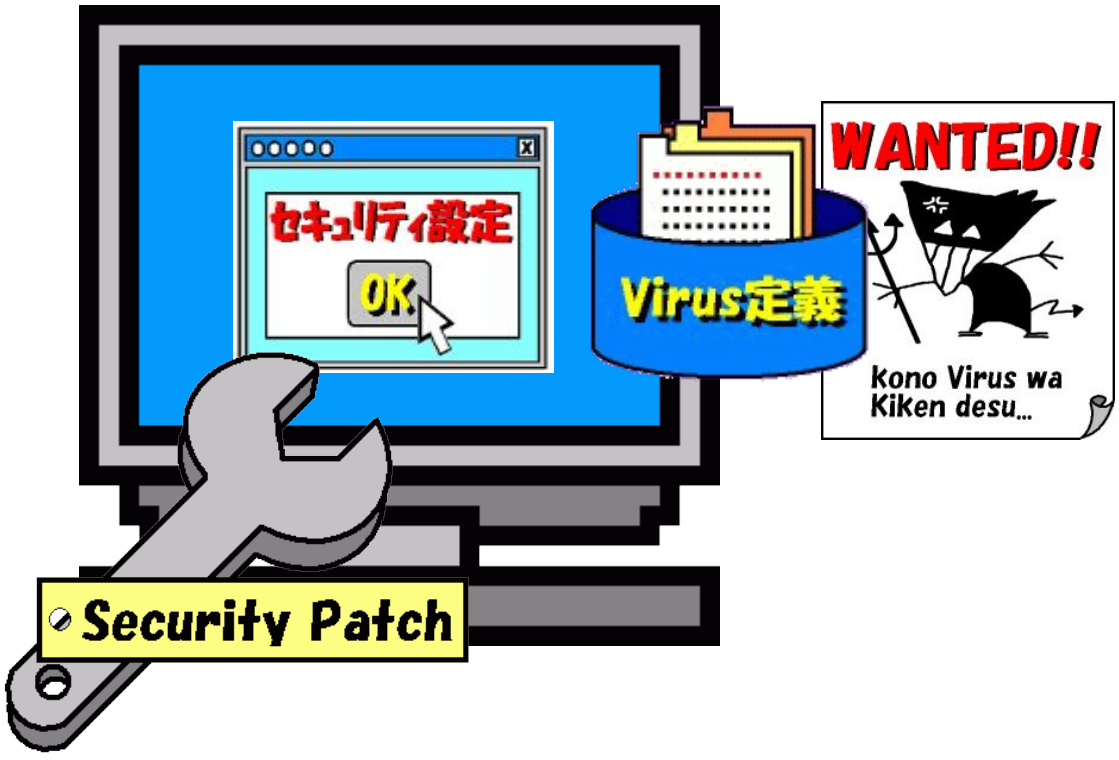
【クロスサイト・スクリプティング(XSS)『安全なウェブサイトの作り方』から引用】

6. 現状での利用者の対策

最新のブラウザには、悪意のあるサイトを表示する際に、利用者の不利益になるスクリプトの実行やサイトの表示に対して警告を発信する機能が実装され始めています。これらの機能は、ある程度の脅威を利用者に警告してくれるものですが、完全に防御してくれるわけではありません。利用者が脅威を理解し、自分自身で脅威から身を守る必要があることを忘れてはなりません。

常日頃から、以下に示す最低限の対策を実施して下さい。

- ❖ パソコンの OS やアプリケーション（ブラウザやメーラーを含む）のぜい弱性を解消し（最新の状態にする）、セキュリティ設定を強化（ActiveX、JavaScript の動作抑止）する
- ❖ ウイルス対策ソフトで定期的にウイルス検査を実施する
- ❖ 見知らぬ人からのメールや添付ファイルは安易に開かない
- ❖ 銀行や信販会社からのメールを安易に信用しない
- ❖ OS が表示する警告メッセージが出たら、慌てずに、自分の意思でないダウンロード要求はキャンセルする



7. 用語の説明

(*1) ウイルスメール

コンピュータウイルスが添付ファイル等に付けられたメール。安易に添付ファイルを開くとウイルスに感染します。

(*2) スパムメール

商用目的かどうかによらず、個人的、宗教的なものも含めて宣伝や嫌がらせなどの目的で不特定多数に大量に送信されるメールのこと。一般に、迷惑メールとも呼ばれています。

(*3) フィッシング

金融機関（銀行やクレジットカード会社）などを装ったメールを送り、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を詐取する行為。

(*4) ボット

コンピュータウイルスの一種でコンピュータに感染し、ネットワーク(インターネット)を通じて外部から操ることを目的として作成されたプログラム。感染すると、外部からの指示を待ち、与えられた指示に従って処理を実行する。この動作が「ロボット」に似ていることから、ボットと呼ばれています。

(*5) ワーム

通常のウイルスは感染対象のプログラムを必要とするが、ワームは、感染対象となるプログラムがなく、自分自身の複製をコピーして増殖する。ネットワーク内を這い回る虫のように見えることから、この名称が付けられました。

(*6) ウイルス対策ソフト

コンピュータウイルスを検知･駆除するソフトウェア。ウイルスに破壊されたデータは復元することができないので注意して下さい。

(*7) クラッカー

不正アクセス等の悪意のある行為により、他人のコンピュータに侵入し、データの盗聴や改ざんを行う人。

(*8) ウイルス作成ツール

悪意のある不正なプログラムを簡単に作るためのツール。

(*9) ルートキット

不正な行為を行うためのプログラムを取りまとめたパッケージ。不正アクセスのために利用され、侵入されたコンピュータに仕掛けられる。不正なプログラムの動きを見えないように隠したりします。

(*10) インスタントメッセージサービス(IM)

インターネットに接続したパソコン同士で、チャットやファイルのやりとりができるソフトウェア。同じソフトを利用している仲間がインターネットに接続しているかどうかがわかり、リアルタイムにメッセージを送ることができます。AOL Instant Messaging や MSN Messenger が有名。

(*11) メーラー

メールの作成や送信･受信を行い、受信したメールの保存･管理も行なうソフトウェア。

(*12) シグネチャ

一般的には署名の意味であるが、ここではウイルスの特徴（パターン）を示すデータのことである。シグネチャを用いた検知手法のことを、シグネチャベースの検知とかパターンマッチングによる検知という。ちなみに、このシグネチャを取りまとめたファイルがウイルス定義ファイルである。

(*13) ウイルス定義ファイル

ウイルス対策ソフトがウイルスを検知するために利用するウイルスの特徴（パターン）を記録したファイル。いわゆるウイルスの手配書をまとめたもの。

(*14) メールフィルタリングサービス

メールサーバ（家庭での一般利用者の場合はサービスプロバイダ）が提供する迷惑メールやスパムメールを除去するサービス。

(*15) スパイウェア

利用者や管理者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラム等。

(*16) 暗号通信(SSL)

インターネット上でやりとりする情報を暗号化して送受信するプロトコル(通信規約)。個人情報やクレジットカード番号などを安全に送受信することができ、オンラインバンキングなどのサイトで利用されています。

(*17) セキュリティゾーン

以下に示すマイクロソフトのサイトに詳しい説明があります。

■ セキュリティゾーンの設定

http://www.microsoft.com/japan/windows/ie/using/howto/security/setup.mspx

(*18) プロキシサーバ

インターネットとイントラネットの境界に置かれ、ネット間の通信を中継するサーバ。代理サーバとも呼ばれ、メールサーバ用のウイルス対策やWeb（コンテンツ）フィルタリング等のセキュリティ対策を行うことができます。

(*19) Web(URL)フィルタリング

特定の URL アドレスを持つウェブサイトとのアクセスを制限（抑止）すること。よく知られたフィッシングサイトやウイルスを配布するような不正なウェブサイトの URL アドレス情報を共有し、そのようなサイトとのアクセスを制限するサービスです。

(*20) ワンクリウェア

ワンクリック詐欺を行う目的のウェブサイトに仕掛けられており、画像や映像に見せかけて利用者を騙し、ダウンロードさせ、パソコンに感染すると、デスクトップに請求書を表示したりするプログラムです。簡単に削除できない場合が多いです。

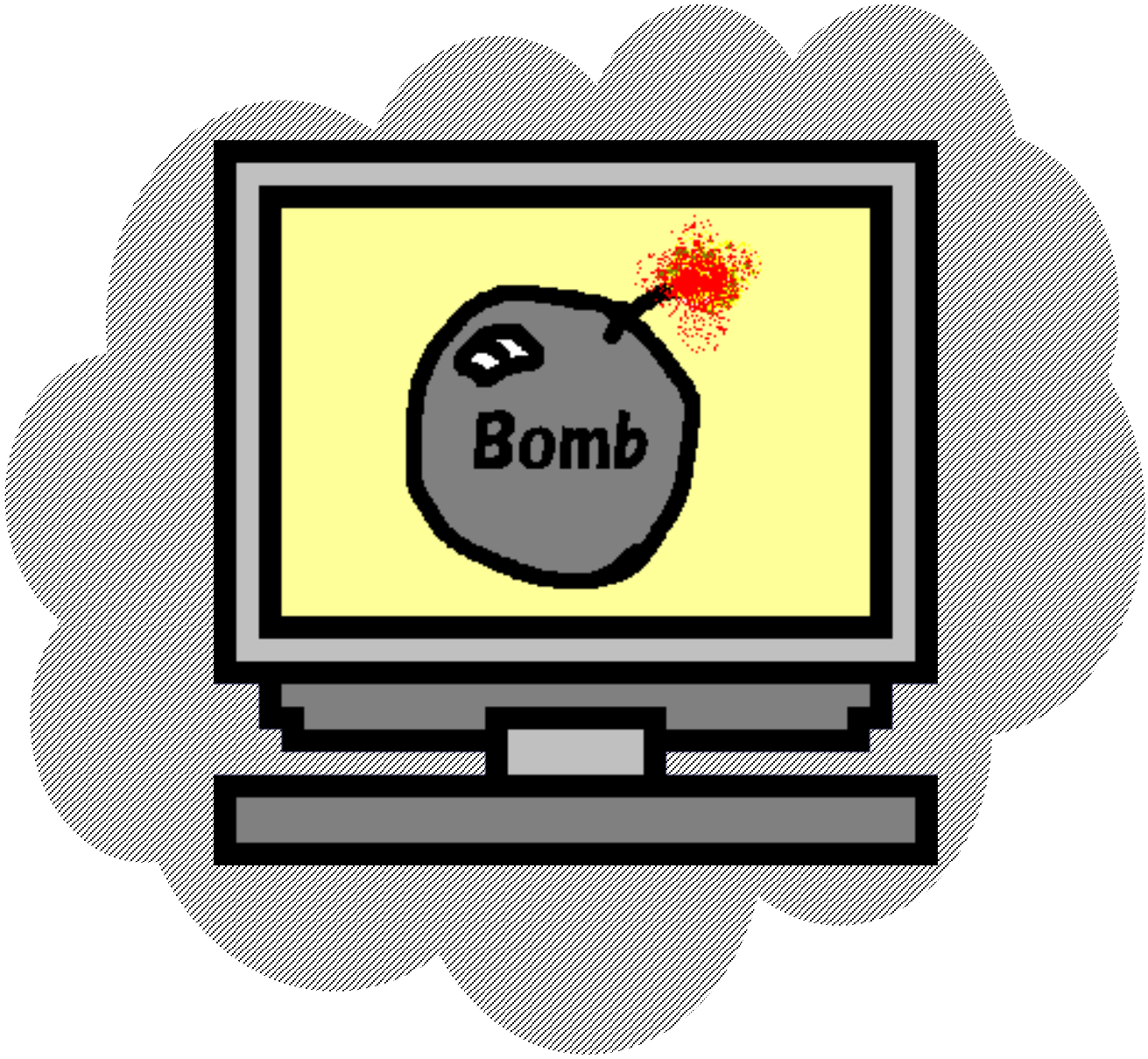
8. 参考情報

■ 情報セキュリティの脅威に対する意識調査 2011 年版
http://www.ipa.go.jp/security/fy23/reports/ishiki/
■ 情報セキュリティ白書 2011 年版
http://www.ipa.go.jp/security/publications/hakusyo/2011/hakusho2011.html
■ 今月の呼びかけ
http://www.ipa.go.jp/security/personal/yobikake/
■ 安全なウェブサイトの作り方
http://www.ipa.go.jp/security/vuln/websecurity.html
■ 警察庁 サイバー犯罪対策
http://www.npa.go.jp/cyber/
■ VirusHoaxes(偽ウイルス)のデマメールに関する情報
http://www.ipa.go.jp/security/topics/virus_hoax.html
■ 「jdbgmgr.exe」に関するデマメール情報
http://www.ipa.go.jp/security/topics/alert140515.html
■ ウィルスデマ情報(トレンドマイクロ)
https://imperia.trendmicro-europe.com/jp/threat/threats-knowledge/non-virus/
■ 身に覚えのない不正請求などの防止
http://www.ipa.go.jp/security/personal/protect/oneclick.html
■ フィッシング (Phishing)対策
http://www.ipa.go.jp/security/personal/protect/phishing.html
■ AntiPhishingJapan フィッシング対策協議会
http://www.antiphishing.jp/
■ ボット対策プロジェクト Cyber Clean Center サイバークリーンセンター
https://www.ccc.go.jp/

IPA 対策のしおり シリーズ

http://www.ipa.go.jp/security/antivirus/shiori.html

- IPA 対策のしおり シリーズ(1) ウイルス対策のしおり
- IPA 対策のしおり シリーズ(2) スパイウェア対策のしおり
- IPA 対策のしおり シリーズ(3) ボット対策のしおり
- IPA 対策のしおり シリーズ(4) 不正アクセス対策のしおり
- IPA 対策のしおり シリーズ(5) 情報漏えい対策のしおり
- IPA 対策のしおり シリーズ(6) インターネット利用時の危険対策のしおり
- IPA 対策のしおり シリーズ(7) 電子メール利用時の危険対策のしおり
- IPA 対策のしおり シリーズ(8) スマートフォンのセキュリティ対策のしおり
- IPA 対策のしおり シリーズ(9) 初めての情報セキュリティ 対策のしおり
- IPA 対策のしおり シリーズ(10) 標的型攻撃メール対策のしおり



IPA 独立行政法人情報処理推進機構
セキュリティセンター

〒113-6591 東京都文京区本駒込2丁目28番8号
（文京グリーンコートセンターオフィス16階）
URL http://www.ipa.go.jp/security/

【情報セキュリティ安心相談窓口】（コンピュータウイルスおよび不正アクセス）
URL http://www.ipa.go.jp/security/anshin/
E-mail anshin@ipa.go.jp