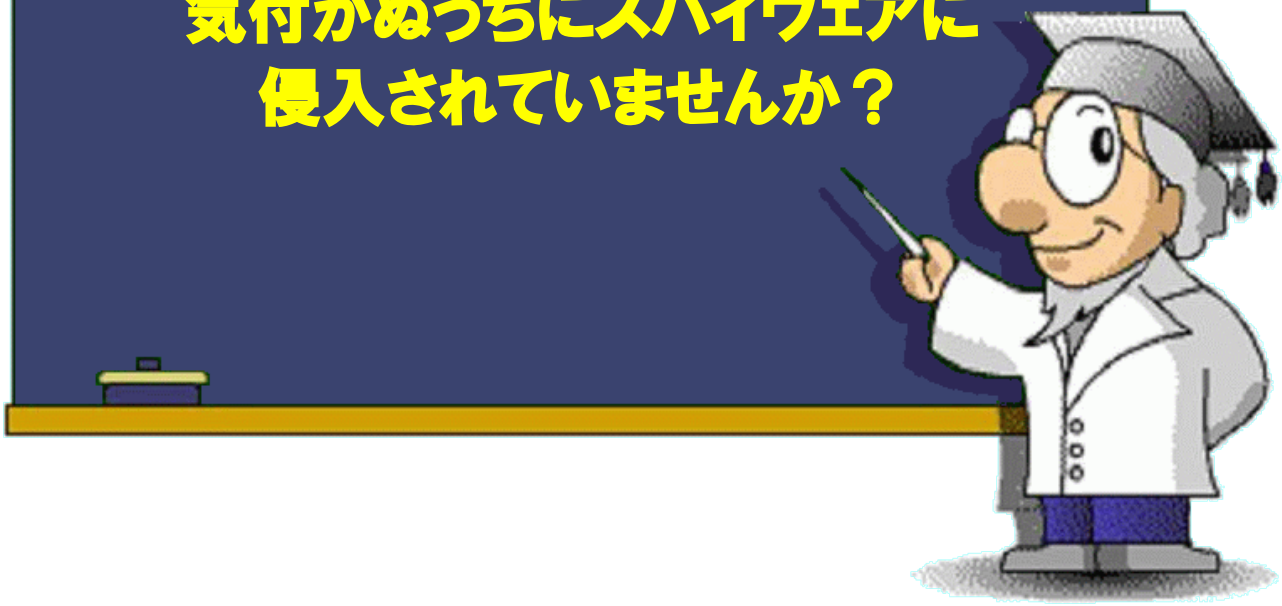
IPA 対策のしおり シリーズ (2)

スパイウェア対策のしおり

気付かぬうちにスパイウェアに侵入されていませんか？



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

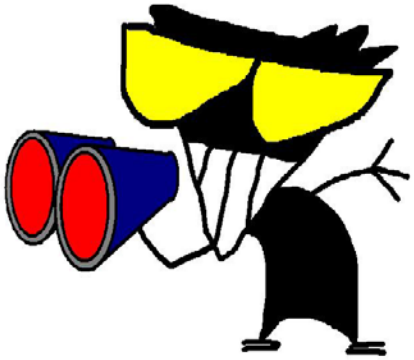
http://www.ipa.go.jp/security/

2012年6月8日 第10版

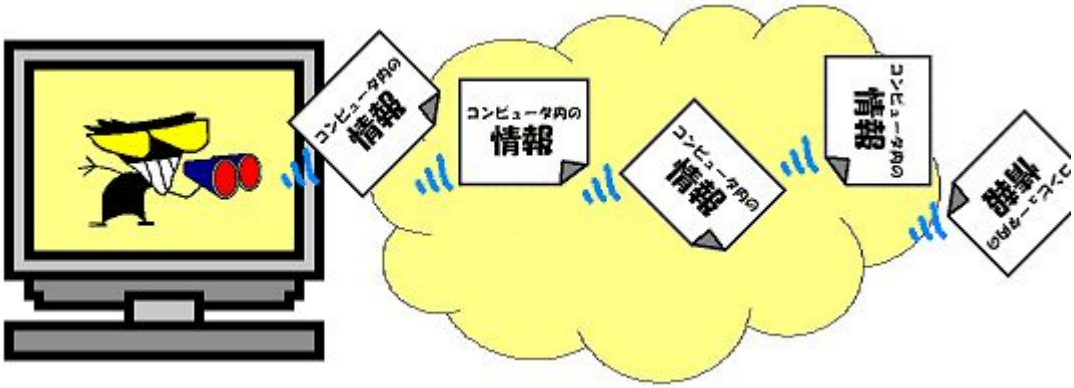
1. スパイウェアとは

スパイウェアの定義

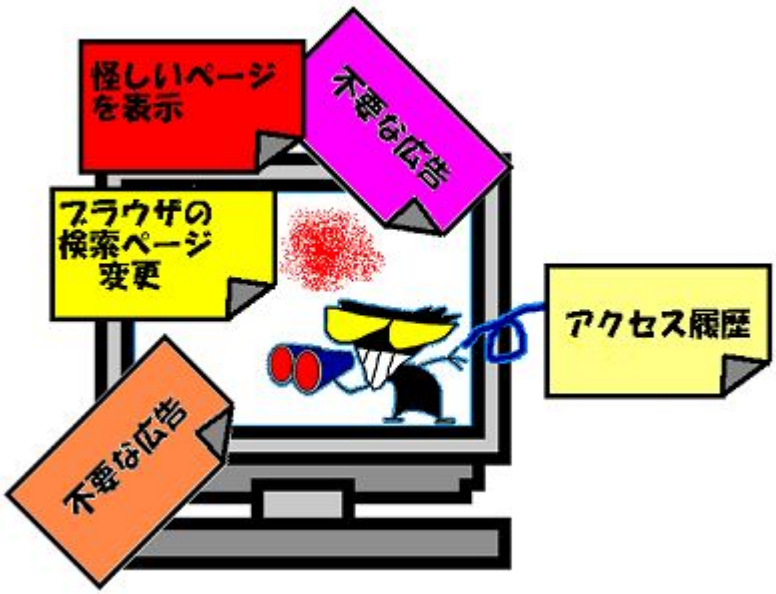
スパイウェアは、『利用者や管理者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラム等。』と定義されます。
[情報処理推進機構(IPA)と日本ネットワークセキュリティ協会(JNSA)スパイウェア対策啓発 WG による共同の定義]



現在、出回っているスパイウェアは、収集した情報をファイルに保存したり、外部へ(利用者以外のものに)自動的に送信したりするなどの機能を併せ持つものが多く見られます。また、ファイル交換ソフトを操り情報を漏えいする W32/Antinny ウイルスもスパイウェアに該当します。



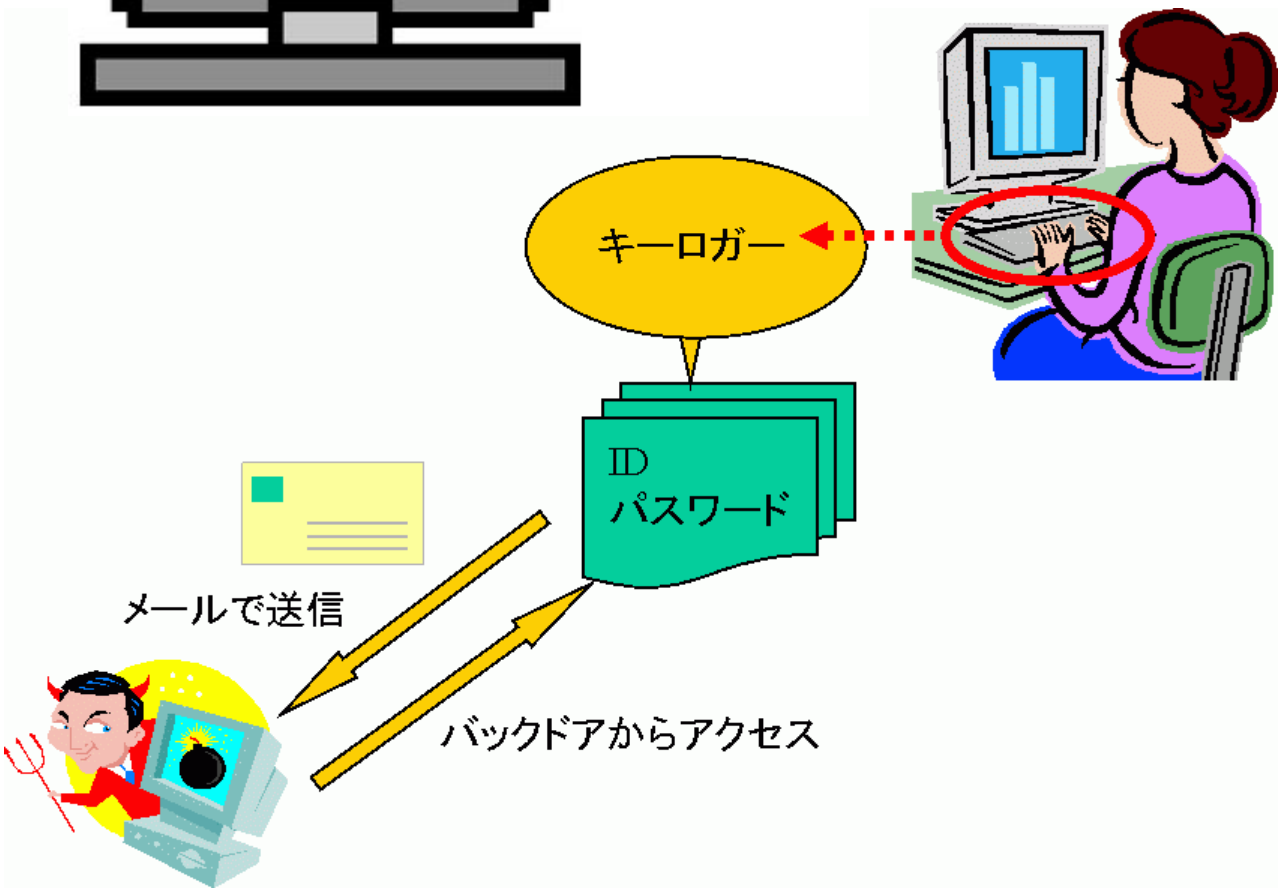
その他、ブラウザを乗っ取って、利用者の意図しない悪意のあるサイトに誘引したり、意図しない検索結果を表示したりするプログラムである「ハイジャッカー」は、情報を収集し、収集した情報を使ってこれらの動作を行っていますので、スパイウェアの範疇に入るものと言えます。



しかしながら情報収集機能を有するプログラムすべてがスパイウェアというわけではありません。

例えば、システムの動作テストや自動実行のためにキー入力情報を記録するプログラムである「キーロガー」は、利用者が正当に利用する限りにおいては、有益なものと考えられます。しかし、このプログラムに、収集したデータを送信する機能やバックドアあるいはリモートアクセス機能が組み合わされ、他人に利用されると、スパイウェアになってしまいます。

特に不特定多数の利用者がいるネットカフェ等のコンピュータにスパイウェアが仕掛けられた場合は、他の利用者に記録を参照される可能性があります。実際に、サイバー犯罪事件として報道されています。



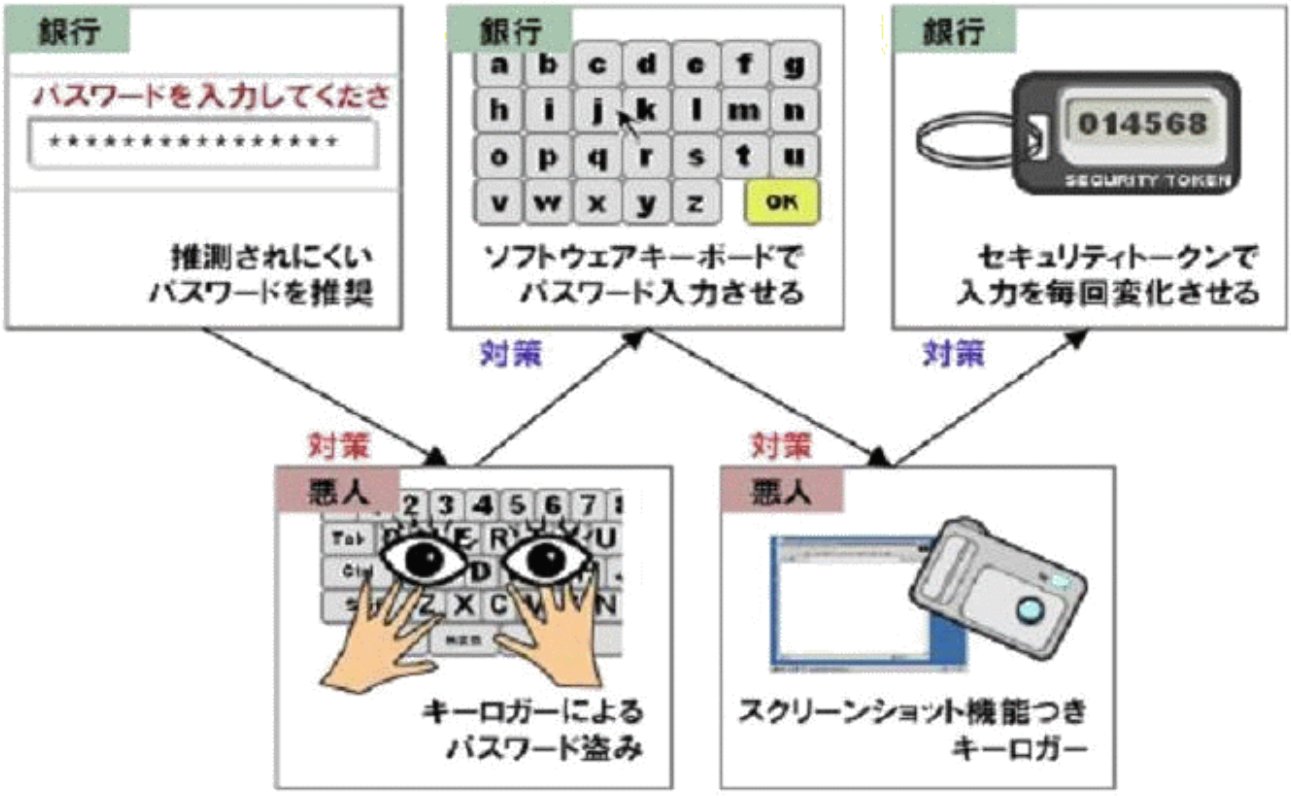
スパイウェア対策ソフトによって検知される一部のプログラムは、企業などで使われるシステム管理用ソフトの部品である場合もあります。

また、提供する側と提供を受ける側での考え方の相違により、インターネットの利便性を向上させる目的で作成されたソフトウェアについても、提供を受ける側では、スパイウェアであると位置付けられる場合もあります。この問題の多くは、アドウェア(*1)と呼ばれる広告などを勝手に表示するソフトウェアとスパイウェアの区分け部分で取り沙汰されています。

このように、スパイウェアとは、あいまいな部分もあることを忘れてはいけません。たとえスパイウェア対策ソフトでたくさんのスパイウェアが検出されても、慌てる必要はありません。すべてが、情報漏えいを引き起こしているとは限らないからです。自分が望まないものは駆除すると言う考え方で対処することをお勧めします。

参考までに・・・

スパイウェア(キーロガー)は進化する・・・銀行と悪人の対決

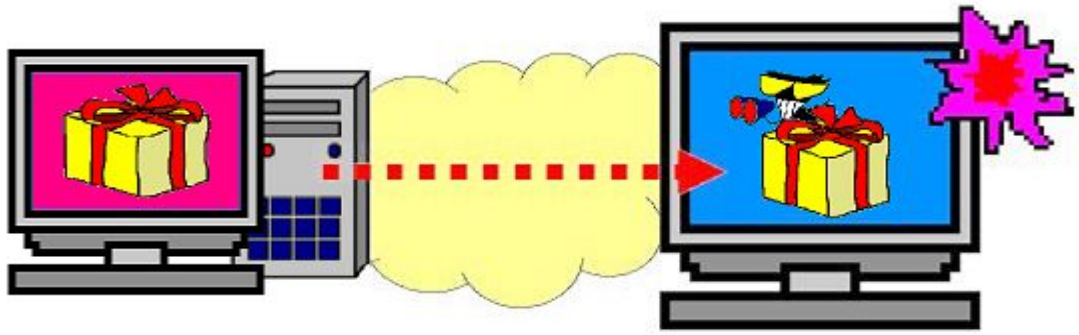


出典:情報セキュリティ白書 2006 年版
http://www.ipa.go.jp/security/vuln/20060322_ISwhitepaper.html

2. どのようにして侵入されるのか

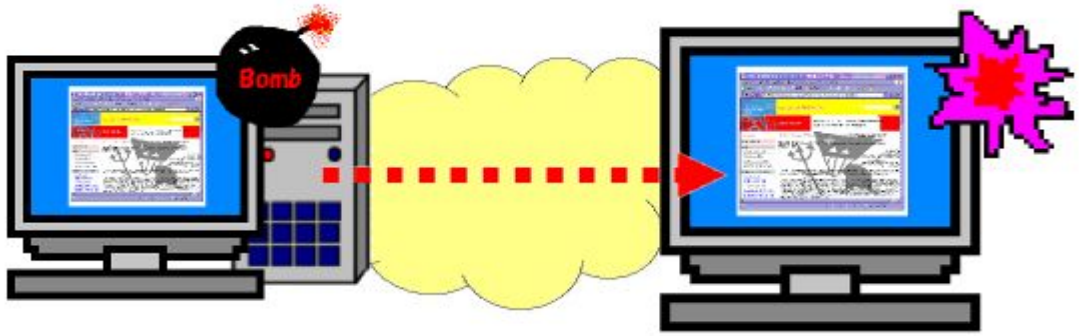
スパイウェアの侵入は、主に利用者自身が誤って(知らないうちに)インストールすることで起こります。さらに、ウイルスやワームの一部として侵入される場合もあります。

1)Web(または外部媒体)からの安易なフリーソフトウェア(無償プログラム)やシェアウェア(有償プログラム)あるいは便利なツールであることを謳うプレゼントのダウンロード(*2)やインストール(*3)により、それらのプログラムについてくるスパイウェアが侵入



Web サイトからダウンロードしたファイルがスパイウェアであるケースがあります。Web サイトを検索したときに表示されるダウンロード許諾や、フリーソフトウェア等をインストールするときに表示される利用許諾を良く読み、必要のないものはインストール又はダウンロードしないようにしましょう。必要ならば、ダウンロードしたファイルはウイルス検査を行ってから、インストールするようにしましょう。

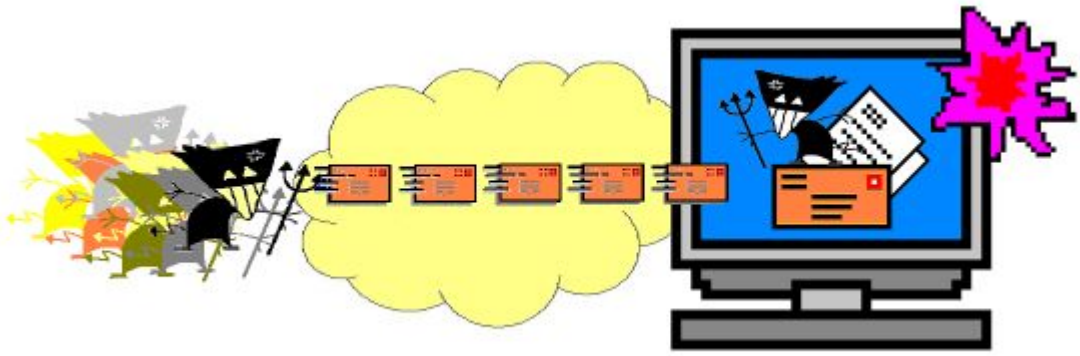
2)不正な(コードの埋め込まれた)Web ページの閲覧による侵入
3)スパムメールに示されたリンク(URL)のクリックにより不正なサイトに導かれて侵入



メールの本文に記述されているリンク先や掲示板などに貼り付けてあるリンク先にアクセスすることにより、スパイウェアを仕掛けられている Web サイトに導かれ、スパイウェアを取り込まされるケース等もありますので、リンクをクリックする場合は、必要なものに限りアクセスするようにしましょう。

2)、3)の手法は、ぜい弱性（およびセキュリティ設定の弱さ）を突いた侵入ですので、特に注意が必要です。このケースでは、不正な(怪しげな)Web ページに近づかないとともに、Windows Update などによりぜい弱性を解消しておき、ブラウザ等のセキュリティを強化しておくことが、対策(後述)として必須となります。

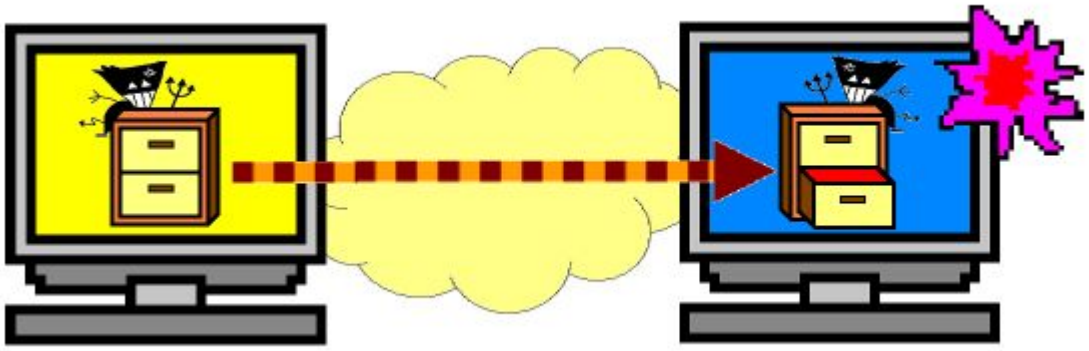
4)ウイルスメールの添付ファイルの実行による侵入



5)ファイル交換(P2P)ソフトの利用による侵入

ファイル交換ソフトによりダウンロードしたファイルにウイルスやスパイウェアが付いているケースがあります。ダウンロードしたファイルは必ずウイルス検査を行いましょう。

ただし、Winny によるファイル交換で感染する W32/Antinny ウイルスのように、国内（あるいはアジア圏）でのみ拡散しているものは、海外のフリーのウイルス対策ソフトなどでは検知できない場合があるので注意が必要です。



3. パソコンユーザのためのスパイウェア対策 5 箇条

スパイウェア対策も、今までのウイルス対策と同じような対策が必要です。ウイルス対策でも論じられるように、ひとつの対策をしておけば大丈夫と考えるのは危険です。不正アクセス対策で言うところの多重防御が必要となりますので、ここに示す５箇条(および補足)を実施することをお勧めします。

(1) スパイウェア対策ソフトを利用し、定期的な定義ファイルの更新およびスパイウェア検査を行う
(2)コンピュータを常に最新の状態にしておく
(3)怪しいサイトや不審なメールに注意
(4)コンピュータのセキュリティを強化する
(5)万が一のために、必要なファイルのバックアップを取る

補足)
自分で管理できないコンピュータでは、重要な個人情報の入力を行わない

(1) スパイウェア対策ソフトを利用し、定期的な定義ファイルの更新及びスパイウェア検査を行う

スパイウェア対策ソフト（あるいはウイルス対策ソフト）を利用することで、スパイウェアの侵入や実行を抑止することができます。ただし、対策ソフト本体や定義ファイルを常に最新の状態にしておくことが大切です。

また、利用者が意図的にインストールしたソフトウェアがスパイウェアとして検知される場合(スパイウェアと検知される部品プログラムを含んでいるような場合)は、該当ソフトウェア(プログラム)の検知を除外する設定が必要です。つまり、利用者の責任において使用しなければならないと言うことになります。

最近のウイルス対策ソフトは、スパイウェアを検知できるものが増えてきました。しかしながら、これらのウイルス対策ソフトやスパイウェア専用の対策ソフトでも、スパイウェアをすべて検知し、駆除することは難しい場合があります。対策ソフトベンダでは、新しい検知方法などを考案し、未知のスパイウェア（ウイルス）でも検知するように、ソフトを進化させていますが、完全と言うことはないので、これさえあれば

と言う過信は禁物です。

(2) コンピュータを常に最新の状態にしておく

コンピュータにあるぜい弱性(セキュリティホール)を利用して侵入するスパイウェアの存在が確認されています。ぜい弱性を解消するために、コンピュータを常に最新の状態にしておくことが重要です。

セキュリティホールは基本ソフト(OS)だけでなく、利用されている各種のソフトウェアにも存在する場合があります。

Windows ユーザの場合は、Microsoft Update を定期的に実行することをお勧めします。それ以外の OS やソフトウェアをご利用のかたは、ベンダや各種の公開されたセキュリティ情報を参照し、ぜい弱性が公開された場合はすぐに対処して下さい。

■ Microsoft Update （マイクロソフト株式会社）
http://www.update.microsoft.com/microsoftupdate/v6/

Microsoft Update の使い方については、以下の Web サイトが参考になります。

■ **コンピュータの更新（マイクロソフト株式会社）**
http://windows.microsoft.com/ja-jp/windows7/Updating-your-computer

(3) 怪しいサイトや不審なメールに注意

●Web サイトの閲覧

悪意のある Web サイトでは、サイトを閲覧しただけでスパイウェア等をインストールされる場合があります。

検索エンジンで検索された怪しげなサイト、スパムメールやポップアップメッセージに記載された怪しいと思われるサイトには近づかない方が賢明です。必要ならば、後述するブラウザのセキュリティ設定を強化してから閲覧して下さい。

●便利なツールのダウンロード

シェアウェアやフリーソフトウェアを Web サイトからダウンロードする場合は、信頼できるサイトのみから行いましょう。同様な意味で、ファイル交換(P2P)から取得したソフトウェアについても注意が必要です。これらのファイルを利用(インストール)する前に、スパイウェア対策ソフトやウイルス対策ソフトで検査することを忘れないようにして下さい。

●不審なメール

ウイルスメールと同様に、不審なメールに添付されたファイルを開くことで、スパイウェアがインストールされたり、メール本文に記載された怪しげなサイトを訪問すると、スパイウェアをインストールされたりする場合があります。

以下に示すことを心掛けて下さい。

・不審なメールに付いた添付ファイルは開かない
・不審なメールに記述されたリンクは開かない

注:スパイウェア等の不正プログラムの拡張子(ファイル名の末尾にある 3 文字程度のアルファベット)には、.exe .pif .scr 等が使われることがあります。添付ファイルがこのような拡張子の場合は、特に危険ですので、必ずウイルス検査を行うようにしましょう。

●理解できないポップアップ画面や確認メッセージ

理解できないポップアップ画面や確認メッセージ(プロンプト)は、画面上のボタンを操作することで、内蔵された不正な処理が動作する場合があります。おかしいなと思ったら、×ボタン(強制終了ボタン:ALT+F4 と同じ)で終了しましょう。

・ポップアップされたメッセージは×ボタンで終了する
・理解できない確認メッセージ(プロンプト)は×ボタンで終了する

●偽装アンチスパイウェア

最近増加しているスパイウェアの被害に、”偽装アンチスパイウェア”ソフトウェアを使った方法があります。これらは、一見正統なスパイウェア対策ソフトウェアのように振る舞いますが、それ自身にアドウェアや、トロイの木馬を含んでいて、コンピュータがスパイウェアに感染していると警告を表示し、除去するには製品を購入するように強要するものです。

さらに、利用者の承諾なしに、コンピュータをスキャンする(あるいはスキャンした)スパイウェア対策ソフトは、”偽装アンチスパイウェア”ソフトである可能性が高いようです。疑わしい警告メッセージなどを鵜呑みにしない心掛けが必要です。

後述の参考情報に記載した、対策ソフトベンダーでは、無料でスパイウェア(ウイルス)を検査(あるいは駆除)するサービスを行っています。必要ならば、検査(あるいは駆除)を実施して下さい。

(4) コンピュータのセキュリティを強化する

●パーソナルファイアウォールを使う

外部からのコンピュータへの不正アクセスによりスパイウェアをインストールされる可能性があります。正しく設定すれば、ファイアウォールは不正なアクセスを抑止します。また、既にインストールされてしまったスパイウェアからのデータ送信を抑止することができる場合もあります(セキュリティ対策ソフトのファイアウォール機能や Windows Vista に付属している Windows ファイアウォール機能等)。
注:ルータの機能や Windows XP に付属している Windows ファイアウォール機能では、スパイウェアが内部から外部へ通信することを防ぐことができません。

●ブラウザのセキュリティ設定を行う

インターネットサーフィンを行う場合、ブラウザのセキュリティ設定を行うことをお勧めします。先にも述べた、怪しげなサイトを訪問する場合、セキュリティ設定を高い状態にしておくことが重要です。利用者の意図とは関係なしに、悪意のある ActiveX やスクリプトによって、スパイウェア等をインストールされる可能性があります。

Windows ユーザで Internet Explorer 6 を使用している場合は、インターネットのプロパティのセキュリティ設定で必ず『中』以上を設定し、Internet Explorer 7 を使用している場合は、必ず『中高』以上を設定しましょう。

さらに、スパイウェアを論じる場合に良く取り沙汰されるクッキー(*4)については、インターネットのプロパティのプライバシー設定で必ず『中』以上の設定をしましょう。

■Internet Explorer でセキュリティを確保する(マイクロソフト株式会社)
http://www.microsoft.com/japan/windows/ie/using/howto/security/settings.mspx

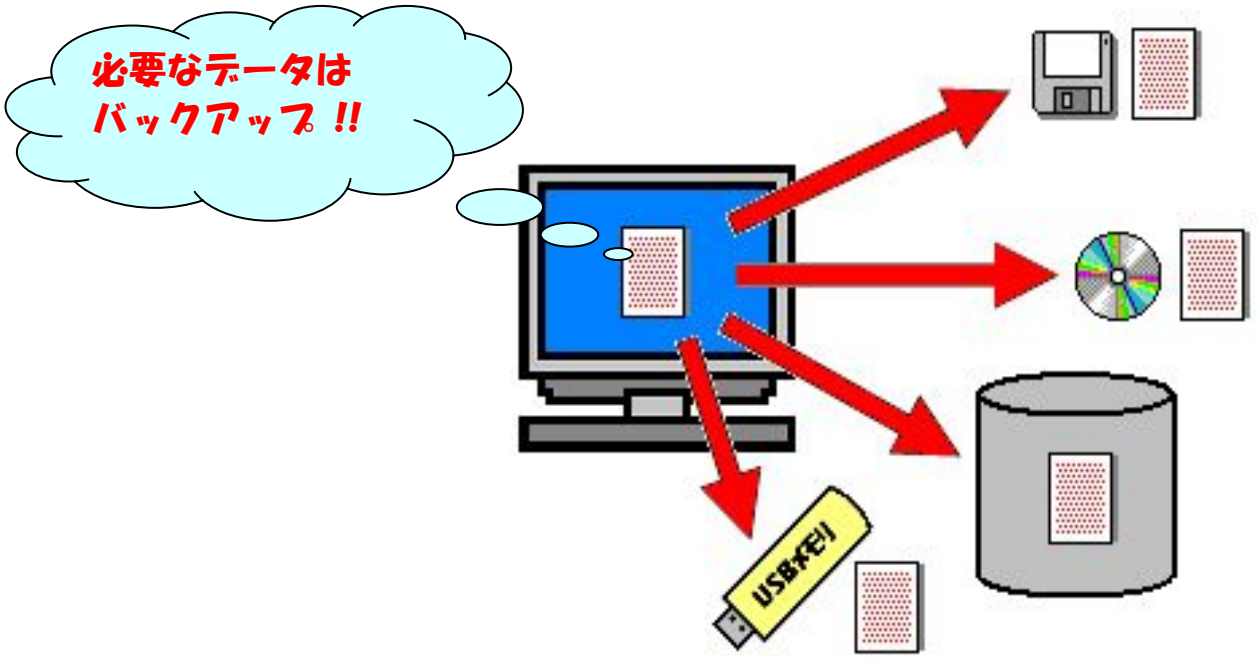
●必要な場合以外は管理者モード(*5)を使わない

管理者モードを使用している状態で、コンピュータで不正なプログラムが動作すると、コンピュータの制御を完全に乗っ取られる可能性があります。必要でない場合は、管理者モードで動作させないことが重要です。

(5)　万が一のために、必要なファイルのバックアップを取る

どんな場合でも、コンピュータの状態を安全な状態にするには、システム自体を初期化しなければなりません。この際、大切なファイル等は、事前にバックアップしておくことが重要です。

不正なプログラムを埋め込まれたりシステムを改変されたりしている場合、復旧のためにはコンピュータの初期化を余儀なくされることもあります。**日頃からデータのバックアップをとる習慣をつけておきましょう**。また、アプリケーションのオリジナル CD-ROM 等は大切に保存しておきましょう。万一、システムプログラムが改変された場合には、オリジナル CD-ROM 等から再インストールすることで復旧することができます。



(補足)自分で管理できないコンピュータでは、重要な個人情報の入力を行わない

不特定多数が利用するネットカフェ等、自分で管理できないコンピュータでは、銀行の口座番号やカード情報等の重要な個人情報の入力を行わないことが重要です。犯罪の被害者にならないためにも、心得て下さい。

用語の説明:

(*1)アドウェア(Adware)

広告を勝手に表示する機能を持つソフトウェア。利用者の画面に広告を表示する代わりに、利用者が無料で利用できる。なかには、利用者のコンピュータの環境やWebブラウザのアクセス履歴などの情報を外部に通知するものがあり、これがスパイウェアのはじまりと言われています。

(*2)ダウンロード

Web サイト等にあるデータをクライアントのパソコンに転送(移動)すること。

(*3)インストール

ソフトウェアをクライアントのパソコンに導入すること。これにより、ソフトウェアを利用することができるようになる。

(*4)クッキー(Cookie)

Web サーバーと Web ブラウザの間で、ユーザに関する情報やアクセス情報などをやりとりするための仕組み。

(*5)管理者モード

コンピュータの OS には、利用者の権限を設定することができる機能が付いています。管理者モードとは、いわゆる特権モードで、コンピュータに対して何でもできる(重要な設定も変更できる)モードです。これに対して、利用者モードも用意されており、コンピュータの動作に関して重要な設定変更はできませんが、通常の利用では、このモードで十分に作業を行うことができます。詳しくは、お使いのコンピュータの解説書をお読み下さい。

参考情報:

■スパイウェアによる被害の防止に向けた注意喚起
http://www.ipa.go.jp/security/topics/170720_spyware.html

■マルウェア対策を強化してコンピュータを保護する方法
http://www.microsoft.com/ja-jp/security/pc-security/protect-pc.aspx

■アダルトサイト被害対策の部屋
http://www.higaitaisaku.com/

■インターネットセキュリティナレッジ スパイウェア特集
（トレンドマイクロ株式会社）
http://is702.jp/special/403/

■株式会社シマンテック
http://www.symantec.com/ja/jp/

■マカフィー株式会社
http://www.mcafee.com/japan/

■スパイウェア リサーチセンター（株式会社アークン）
http://www.ahkun.jp/researchcenter/SpywareResearchCenter.html

■スパイウェアガイド（株式会社ネクステッジテクノロジー）
http://www.shareedge.com/spywareguide/

■Spyware Information Center
http://www.ca.com/us/spyware.aspx

■Panda Software Japan(パンダソフトウェア ジャパン)
http://www.ps-japan.co.jp/

■webroot(ウェブルート・ソフトウェア株式会社)
http://www.webroot.co.jp/Ja_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

本しおりを作成発行するにあたり、以下の団体の協力を得ています。

●日本ネットワークセキュリティ協会(JNSA)
スパイウェア対策啓発WG
http://www.jnsa.org/
http://www.jnsa.org/spyware/

●日本複合カフェ協会(JCCA)
http://www.jcca.ne.jp/

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