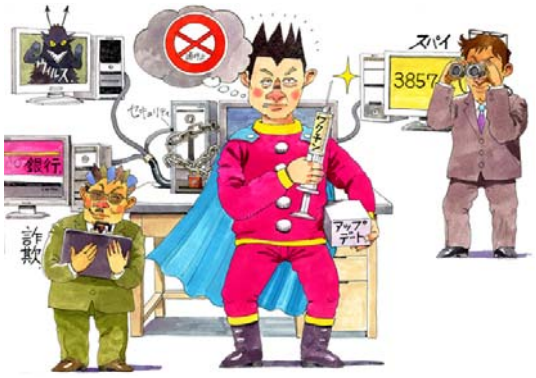
第５回　ブラウザの拡張機能　ブラウザとセキュリティ

インターネットの便利さは、目の前の PC が世界中のコンピュータと結ばれていることで実現しています。外の世界からは便利さとともに脅威も同時に送られてきます。迷惑メール、ウイルス、ボット、フィッシング詐欺、最近では被害にあうだけでなく、いつの間にか自分も加害者になっている場合もあります。こうした脅威から身を守るためブラウザやソフトの機能についてお話します。



【今回登場するキーワード】

「マルウェア」
「コンピュータウイルス」
「フィッシング詐欺」
「ワンクリック詐欺」
「SSL」
「不正アクセス」
「スパイウェア」

インターネットの便利さの裏面には危険もあります。メールや Web サイトから感染して PC やソフトを機能不全に陥れたり、データを消去したり、ネットワークに流出させたりする「マルウェア」、ワンクリック詐欺やフィッシング詐欺などの「ネットワーク犯罪」、知らぬ間に PC に入り込みキー操作を記録して盗み取る「不正アクセス」など、多くの脅威に囲まれています。これらの脅威から PC を守る方策をお話します。

■マルウェアから PC を守る

はじめに、ウイルスを含む悪意あるプログラムの総称「マルウェア」(Malware) のお話しです。不正な（悪質な・有害な・悪意ある）ソフトウェアの総称をマルウェアといいます。コンピュータウイルスはそのひとつです。マルウェアに感染した PC は、動作が不安定になる、起動しない、動作が遅い、勝手にメールを送る、異常終了などの障害が起こります。

マルウェアは、メールの添付ファイルとして迷惑メールで送られてきたり、ネットワーク経由で送信されてきたり、Web サイトから感染したファイルを知らずにダウンロードしてしまったり、というように外部から PC に侵入してきます。マルウェアの感染経路として最も危険なのが、インターネットなのです。

マルウェアから PC を守るためには、以下に示す IPA (独立行政法人 情報処理推進機構) の「パソコンユーザのためのウイルス対策 7 箇条」のように、基本的な事柄を地道に行う以外に対策はありません。

■パソコンユーザのためのウイルス対策 7 箇条

1. 最新のウイルス定義ファイルに更新しワクチンソフトを活用すること
2. メールの添付ファイルは、開く前にウイルス検査を行うこと
3. ダウンロードしたファイルは、使用する前にウイルス検査を行うこと
4. アプリケーションのセキュリティ機能を活用すること
5. セキュリティパッチをあてること
6. ウイルス感染の兆候を見逃さないこと
7. ウイルス感染被害からの復旧のためデータのバックアップを行うこと

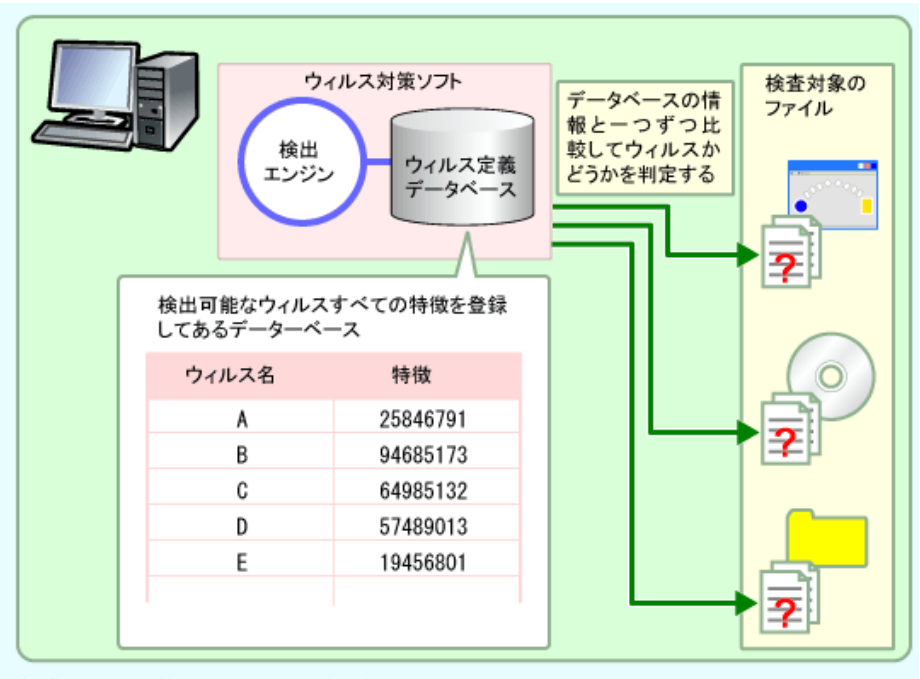
独立行政法人 情報処理推進機構（セキュリティセンター） IPA/SEC
http://www.ipa.go.jp/security/antivirus/7kajonew.html

これらの対策は、ウイルス対策ソフトの導入、ブラウザやメールソフトのセキュリティの設定と Windows やアプリケーションを常に最新の状態にしておくことでほとんど実現することができます。

・ウイルス対策ソフト

ウイルス対策ソフトの導入は、マルウェア対策の基本中の基本です。ウイルス対策ソフトは、マルウェアが外部から侵入するのを防いだり、定期的に PC 内部を検査して感染しているファイルやデータがないかどうかを調べたりします。

ウイルス対策ソフトは、プログラム本体とウイルスのコードのパターンを定義した定義ファイル（パターンファイルともいいます）のデータベースで構成されます。ウイルス対策ソフトはパターンマッチングと呼ばれる方法で、定義ファイルのデータベースを使って、検査対象のファイルにウイルスと同じパターンのコードが含まれていないかどうかをチェックします。



【図】ウィルス対策ソフトのウィルス検出方法

ウイルスの種類は日々増え続けていますので、それに対応する定義ファイルも日々新しいものが作られます。この定義ファイルは、ウイルス対策ソフトメーカーの Web サイトからダウンロードして、自分のウイルス対策ソフトのデータベースを更新します。

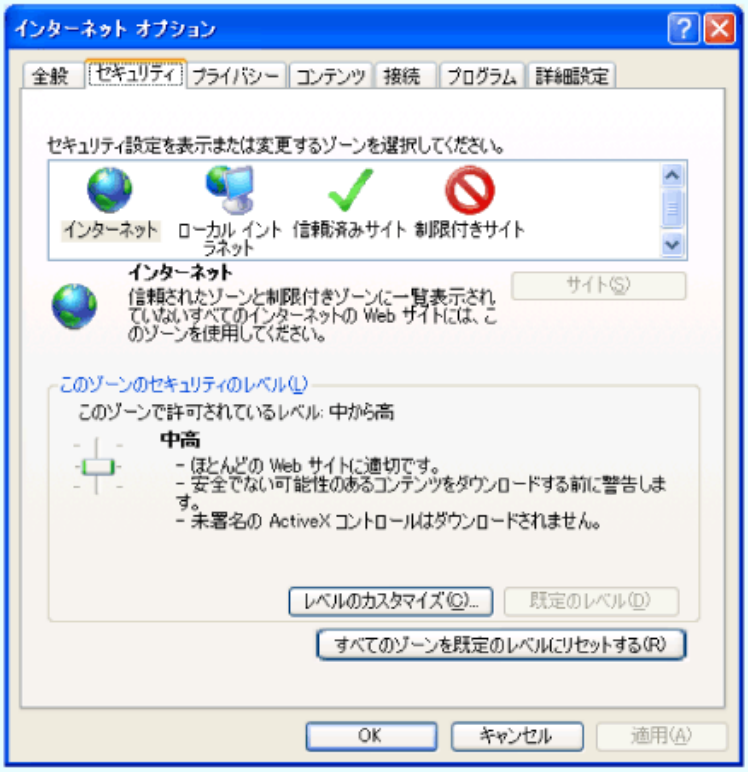
ウイルス対策ソフトは、データベースを自動的に更新する機能、データやファイルにウイルスが含まれていないかを常に監視する機能、自動的に PC 内部を検査する機能を備えています。

データベースの自動更新機能で、常に定義ファイルを最新の状態にして新しいウイルスを検出できるようにしておくことができます。ウイルスの監視機能を常時起動させておくことで、受信メールやその添付ファイル、ネットワークから送られてくるファイル、メディアに記録されたファイル、ダウンロードしたファイル等にウイルスが含まれていないかどうか監視し、リアルタイムにマルウェアを検出し、駆除することができます。さらに、定期的に PC 内部を検査することで、内部に入り込んだウイルスを検出し、駆除することができるようになっています。

・ブラウザのセキュリティの設定

ブラウザのセキュリティ設定を変更することでセキュリティを強化することができます。Internet Explorer 7.0（以降、IE と表記します。）を例にブラウザセキュリティ設定を具体的に説明します。

IE のセキュリティ設定は、「ツール」メニューの「インターネットオプション」で行います。次の画面は「インターネットオプション」で「セキュリティ」タブを選んだ状態です。



【図】インターネットオプションのセキュリティ画面

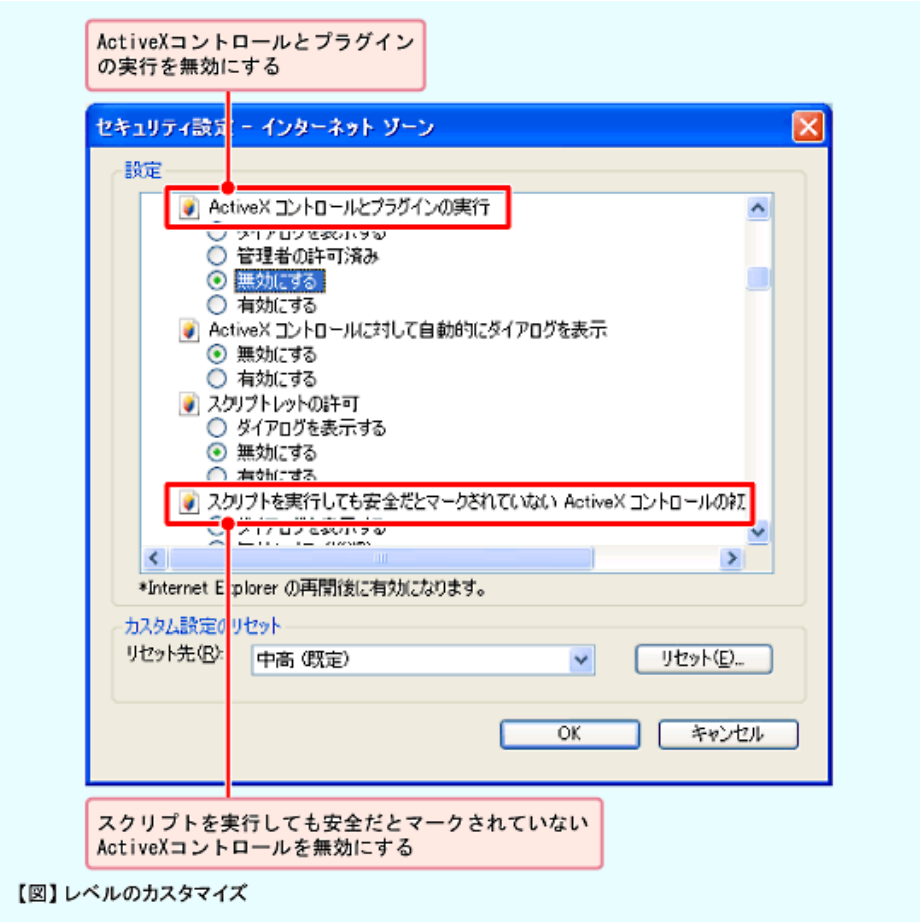
各部分を簡単に説明していきましょう。

最初に Web コンテンツのゾーンごとのセキュリティレベルを設定します。

Icon	ゾーン名称	説明
	インターネット	通常のインターネットで参照するサイト。下記の 3 つのゾーンのサイト以外の全てのサイトが該当する
	イントラネット	イントラネット内にあるサーバを指定する。通常、個人レベルで設定することはない
	信頼済みサイト	Windows Update やウイルス対策ソフトなど信頼できるサイトで、動作に制限があると支障が出る場合に指定する。指定されたサイトはセキュリティによる制限が緩和された状態で表示される
	制限付きサイト	危険なサイト、信頼できないサイトを指定する。ここで指定されたサイトは最も厳しいセキュリティレベルで表示される

表：コンテンツのゾーン

「レベルのカスタマイズ」で、ActiveX とスクリプトの設定を行います。
ボタンをクリックすると次の画面が表示されます。



【図】レベルのカスタマイズ

ActiveX（ActiveX control、アクティブ・エックス・コントロール）は、以前 OLE コントロール、OCX、OLE カスタムコントロールなどと呼ばれていたアプリケーションの機能を拡張するためのプログラムです。ブラウザの場合、動きのある Web ページの実現や、動画・音声の再生、

バナー広告などに広く利用されています。この ActiveX の動作を無条件に許可しておくと、悪意ある Web サイトから PC にマルウェアを取り込むのに利用されてしまうことがあります。

スクリプトは簡易なプログラムです。Web サイトやメールの HTML コードの中に埋め込まれることがあります。ブラウザが HTML の中のスクリプトを見つけると、自動的にそれを解釈して実行します。JavaScript はその代表的な例で、動きのある Web ページ、計算機能やスムーズな表示を実現するために多くの Web サイトで利用されています。ブラウザが自動的に実行してしまうので、無条件にスクリプトの実行を許可しておくと、Web サイトに埋め込まれた悪意あるスクリプトを実行し、マルウェアをダウンロードしてしまう恐れがあります。

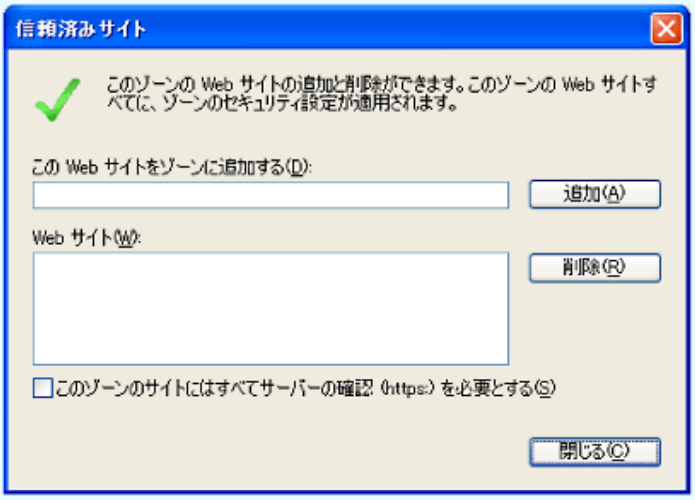
次表のような設定をお勧めします。

設定項目	設定値
ActiveX コントロールとプラグインの実行	無効 インストール済み ActiveX やプラグインの動作を指定する。推奨設定は無効だが、Flash が動作しないなど不自由になることがある
スクリプトを実行しても安全だとマークされていない ActiveX コントロール	無効 安全マークがついていない ActiveX コントロールの起動の許可を設定する。有効にすると安全マークの確認を行わない
スクリプトを実行しても安全だとマークされている ActiveX コントロールの実行	有効 安全マークが含まれているので、有効でかまわない
バイナリビヘイビアと スクリプトビヘイビア	無効 ActiveX がスクリプトによってイベントが発生することがスクリプトビヘイビア。スクリプトをバイナリで ActiveX に埋め込んだものを動作させてイベントが発生することがバイナリビヘイビア
署名済み ActiveX コントロールのダウンロード	ダイアログを表示 ActiveX コントロールには Microsoft が発行した独自のナンバーが割り当てられ、インストール時に確認される。署名済みのものにはチェックが入っているので、ある程度安全が確保されている。署名が偽造されることもあるので注意が必要
未署名の ActiveX コントロールのダウンロード	無効 未署名ということはチェックが入っていないので危険

表：ActiveXとスクリプトの設定

※「安全マーク」とは、ディスク入出力、メモリおよびレジスタへの直接アクセスをしないActiveXコントロールに付けることができるマーク。マークをつけるのは作者自身なので100%信頼できるわけではありません。

上記のように設定して、ActiveX の制限を厳しくすると、実は Windows Update さえ利用できなくなります。そこで、通常のサイトは設定した制限を保ったままで、特定のサイトだけ ActiveX の制限を緩和するために、「信頼済みサイト」への登録を行います。逆に絶対に信頼しないサイトには、ActiveX の制限を強化して「制限付きサイト」に登録します。



※「このゾーンのサイトには全てサーバの確認(https:)を必要とする」にチェックを付けるとhttps:のサイト以外は「信頼済みサイト」として利用できなくなります。通常、チェックは付けません。

【図】信頼済みサイト、制限付きサイト

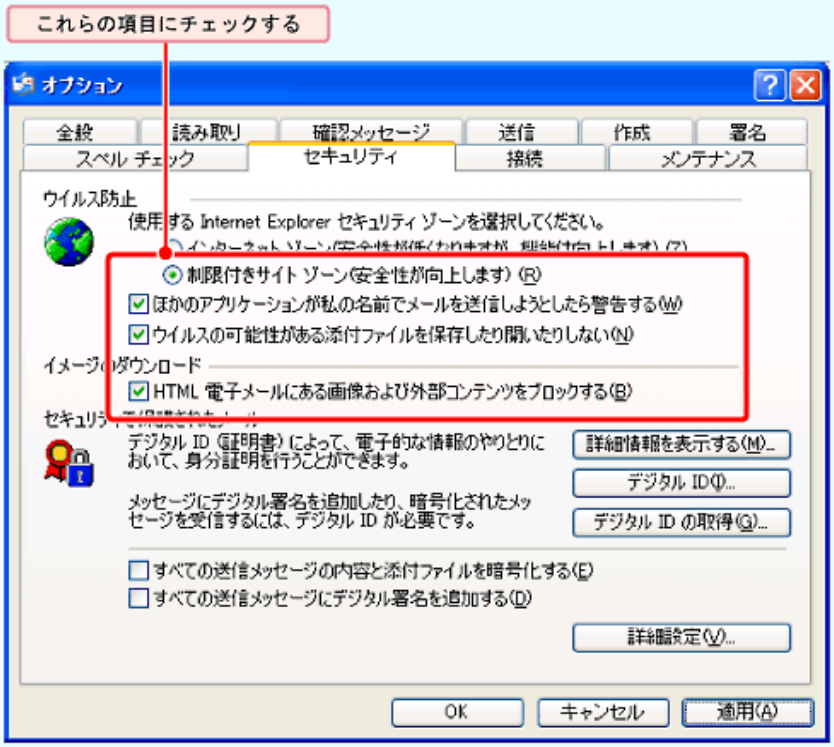
ブラウザのセキュリティを丁寧に設定するだけで、かなり強力なマルウェア対策となります。ActiveX やスクリプトを無効に設定すると Web サイトの閲覧はかなり制限されてしまいますが、信頼できるサイト、そうでないサイトをこまめに登録していくことで安全を確保しながら、閲覧の自由度を上げていくことができます。

・メールソフトのセキュリティの設定

メールソフトも設定を変更してセキュリティをより強化することができます。Outlook Express 7.0（以降、OE と表記します。）を例にメールソフトのキュリティに関する設定を説明します。

OE のセキュリティ設定は、「ツール」メニューの「オプション」で行います。

次の画面は「オプション」の「セキュリティ」タブを選んだ状態です。



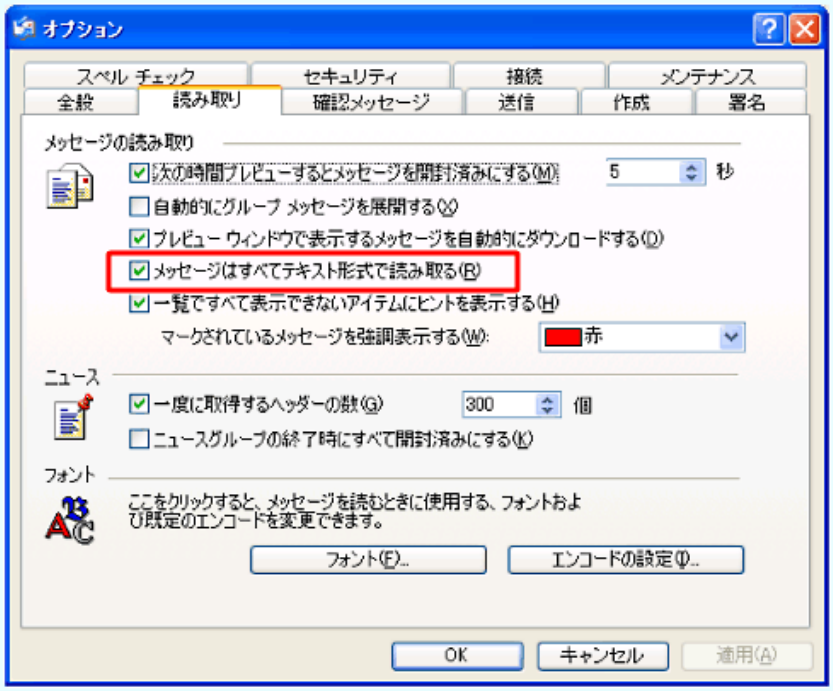
【図】メールのセキュリティタブ

受信メールの重要な設定は、上記の赤い枠の中です。

設定項目	説　明
使用する Internet Explorer セキュリティゾーン	[制限付きサイトゾーン] 特に理由がない限り上記に設定しておく
ほかのアプリケーションが私の名前でメールを送信しようとしたら警告する	有効 PC 内部に侵入したウイルスなど他のプログラムによりメールが送信されることを防ぐ
ウイルスの可能性がある添付ファイルを保存したり開いたりしない	有効 Windows XP SP1 以前は、Office の安全なドキュメントがブロックされていたが、SP2 以降、そうしたことがなくなり、潜在的な危険性があるタイプの添付ファイルのみブロックされる
HTML 電子メールにある画像および外部コンテンツをブロックする	有効 HTML メールに含まれる画像を表示すると、受信者のメールアドレスは有効というメッセージが送信者に伝えられる。これを悪用すると、迷惑メールの宛先が実在することを送信者に知らせることになる。

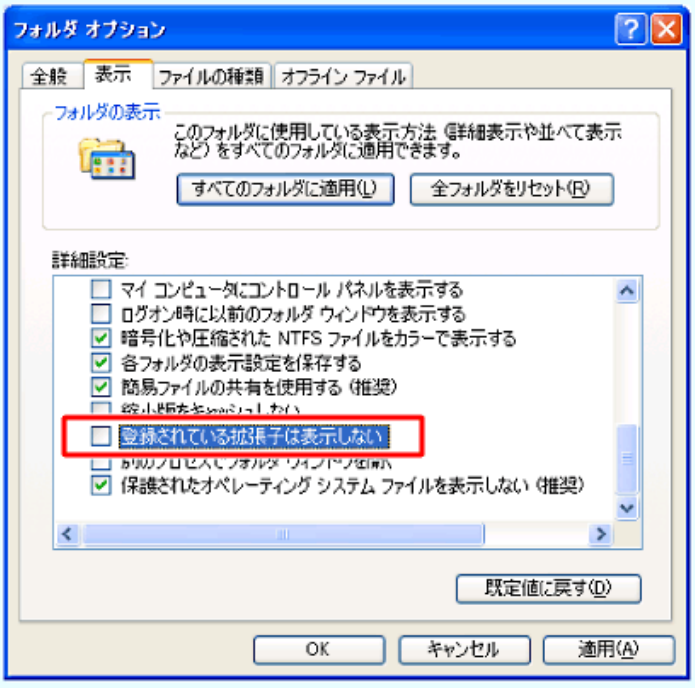
OE ではさらにお勧めしたいのが、受信した HTML メールをテキスト形式で表示する設定です。HTML メールがそのまま表示されると、埋め込まれたスクリプトが実行される可能性が高くなり

ます。さらに、後述するフィッシング詐欺サイトへのリンクのように、画面に表示されたリンク先と実際のリンク先が異なっていても気づきにくいなどの問題があります。テキスト形式で表示すれば、スクリプトやリンク先の問題は解決されます。



【図】テキスト形式で読み取る

また不用意にメールの添付ファイルを開かないようにするために、Windows のエクスプローラで、「ツール」メニューの「フォルダオプション」で、ファイルの拡張子をすべて表示するように設定します。次の画面は「フォルダオプション」の「表示」タブの画面です。



【図】すべての拡張子を表示する

［登録されている拡張子は表示しない］を無効にします。

こうすると、すべてのファイルの拡張子が表示されます。アイコンを偽装したり、拡張子をわかりづらくしたりするために紛らわしいファイル名を付けたマルウェアを誤って実行してしまうのを避けるためです。フォルダアイコンやテキストファイルのアイコンを偽装し、受信者がダブルクリックすると、実は実行ファイル（拡張子が、.exe や.vbs などのプログラムやスクリプト）で、その瞬間にマルウェアに感染するといったものが少なくありません。変わった形のアイコンや.exe などの実行ファイルであれば、開く際に注意する人もフォルダやテキストファイルのアイコンになっていると油断しがちです。

■ネットワーク犯罪から PC を守る

Web サイトでボタンをクリックしただけで「会費」を請求されたり、偽装された Web サイトでパスワードやクレジットカード番号を盗み取られたりする詐欺事件が後を絶ちません。こうしたネットワーク犯罪から PC を守るためのブラウザの機能と、暗号化でセキュリティを確保する SSL の仕組みについてお話しします。

・増加するネットワーク犯罪

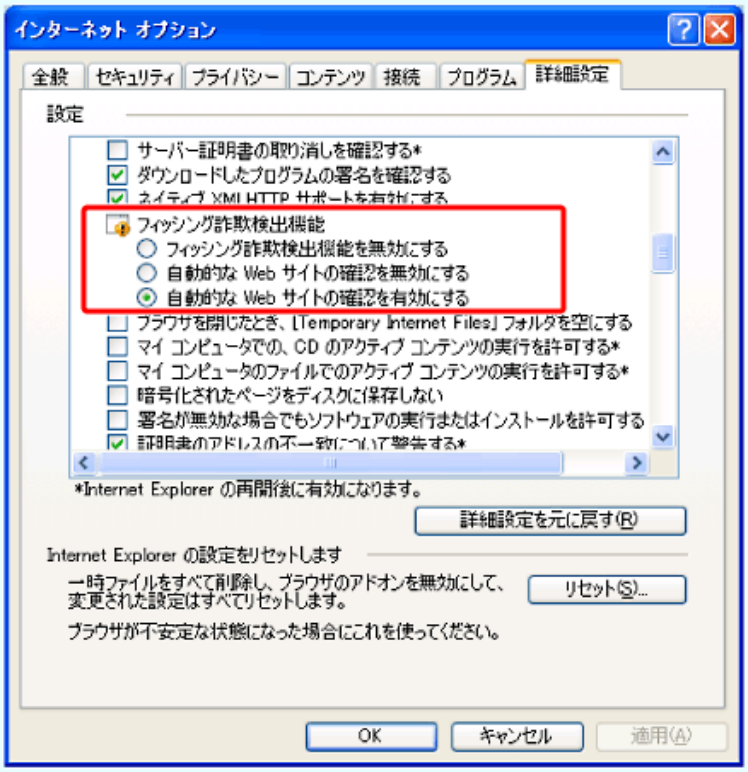
被害が拡大しているワンクリック詐欺は、迷惑メールや掲示板、アダルトサイトのリンクなどで、ユーザーを Web サイトに誘導し、サイト内のボタンやリンクをクリックさせて、「入会手続きが完了いたしました」などと表示して会費を不当に請求する詐欺です。画面には、有料の会員登録が完了した旨、プロバイダ名や IP アドレス、場合によってはメールアドレスも表示し、ユーザーに個人情報を知られたと思いこませて会費を振り込むように要求します。

海外で大きな被害が発生しているフィッシング詐欺は、銀行やショッピングサイトなど実物に似せて作ったサイトに迷惑メールなどで誘導し、登録情報の更新などと偽ってクレジットカード番号、ID、暗証番号などを入力させて、情報を盗み出す詐欺です。盗み出した番号でカードを偽造して預金を引き出したり、ショッピングの決済をしたりして高額な被害を生じます。

この他に、オークションで商品を受け取って代金を払い込まない、または代金を受け取って商品を送らないオークション詐欺、次点落札者を狙う次点詐欺、ほとんど効果のないウイルス対策ソフトを販売するために、突然、本物によく似た警告画面を表示してユーザーをだます偽ソフトなど、数多くのネットワーク犯罪が報告されています。IPA は、2007 年 10 月の「ワンクリック不正請求」に関する相談件数が 369 件に達し、過去最高であった 2007 年 8 月の 330 件を超えたと報告しており、ネットワーク犯罪は増加傾向にあります。

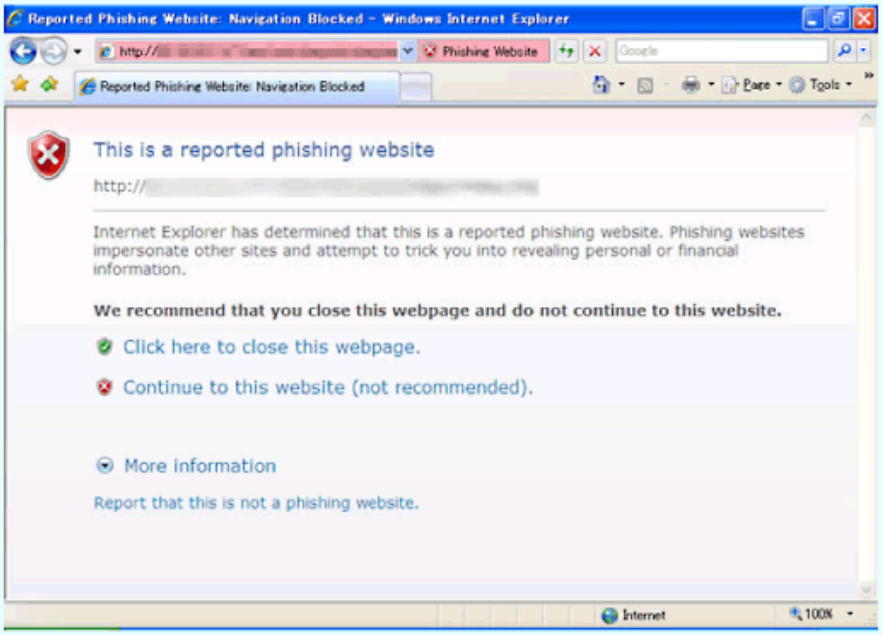
・ブラウザのフィッシング防止機能

ネットワーク犯罪の増加に対し、ブラウザも犯罪防止のための機能を搭載し始めました。IE や Firefox 2.0、Opera など最新のブラウザにはフィッシング詐欺サイト検出機能が装備されています。例えば、IE のフィッシング詐欺検出機能は、Microsoft のフィッシングサイトデータベースと照合して、怪しいサイトかどうかを警告するシステムです。



【図】フィッシング検出機能の設定

検出機能を有効にして、フィッシングサイトと思われるサイトにアクセスしようとすると、アドレスバーが赤く表示され、警告が出るようになります。



【図】フィッシング検出機能の設定

・ユーザーを守る証明書と SSL

犯罪から守り、正常なネット上の取引を行うために、安全を確保して通信を行う仕組みが SSL（Secure Socket Layer）です。オンラインショッピングの決済時にクレジットカードの番号を入

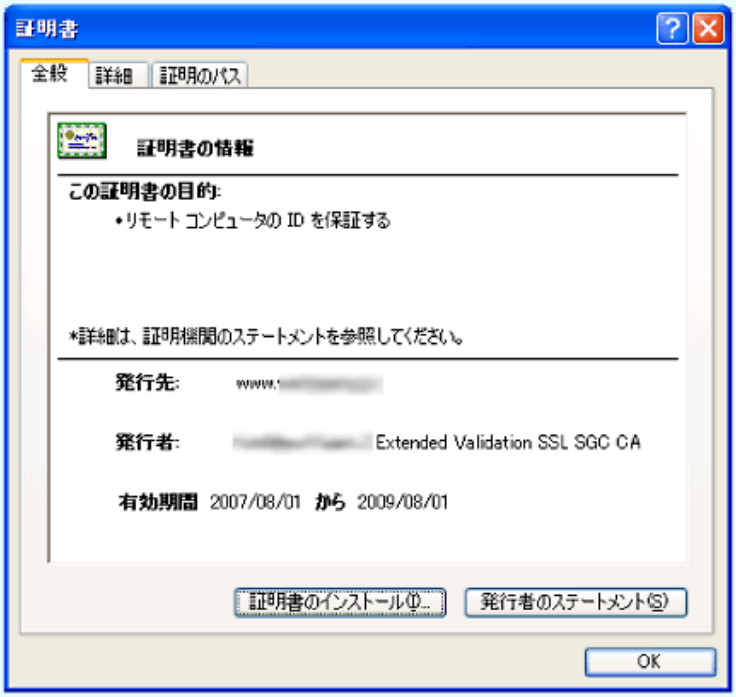
力するときなど、通常の HTTP プロトコルでの通信では、第三者に傍受される可能性があります。そこで、利用されるのが、ブラウザと Web サーバを暗号化して通信する SSL というプロトコルです。

SSL での通信中は、ブラウザに鍵のアイコンが表示されます。またアドレス欄には、「http://×××…」の変わりに、「https://×××…」と「ｓ」が付きます。これが、SSL でサーバと通信しているときの URL の表示です。

【図】SSL通信時のブラウザ（日本ベリサイン社 https://www.verisign.co.jp/）

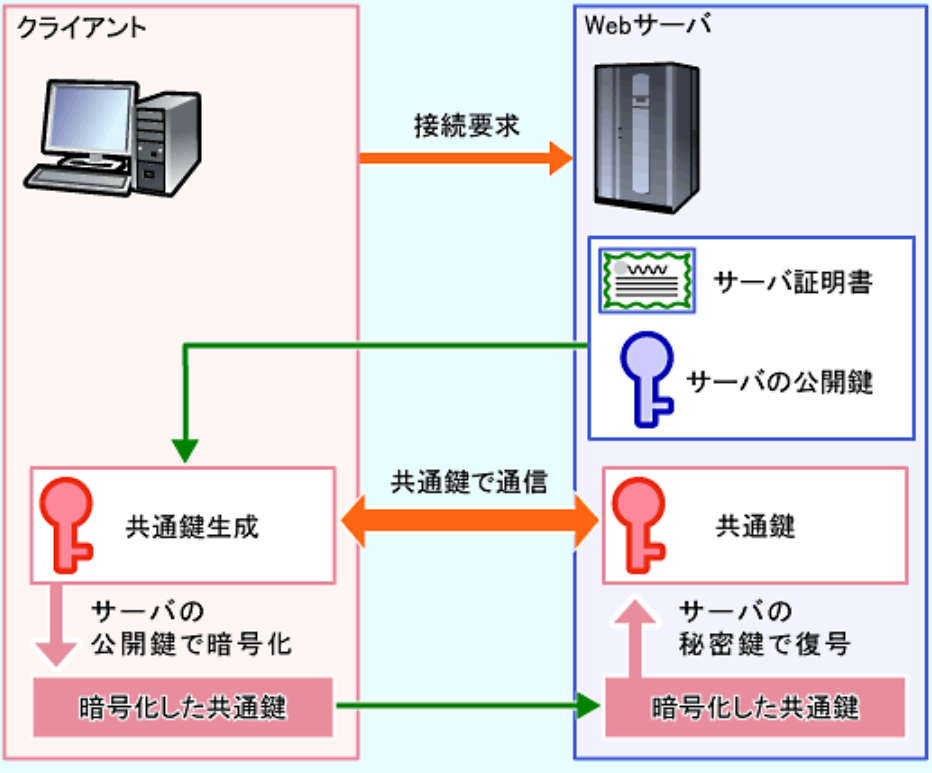
重要な情報を入力する際には、ブラウザの SSL の鍵アイコンとアドレス欄を確認します。個人情報や決済情報などの入力中に鍵アイコンが表示されない場合は、セキュリティに問題がありますので、入力を中止した方が良いでしょう。また、前述したフィッシング詐欺は、アドレス欄と鍵アイコンを確認すれば見破ることができます。偽サイトでは、ほとんどの場合、通信は暗号化されていません。またよく観察すると、アドレス欄がポップアップなどで偽装されていることが分かる場合があります。

さらに、表示されている鍵アイコンをダブルクリックすると、SSL で使われている電子証明書（実態は SSL サーバー証明書）の内容が表示され、今、アクセスしている URL が正しいかどうか確認することができます。



【図】SSLで使われる電子証明書

SSL で使われている電子証明書（SSL サーバー証明書）は、Web サイトの運営組織を独自の方法で確認し、その証しとして、確認した第三者機関が発行しています。つまり、SSL で使う電子証明書が発行されているということで Web サイトの運営者を確認できるのです。
SSL 通信の仕組みに触れておきましょう。



【図】SSLのしくみ

SSL では、ブラウザからの接続要求があると、サーバは「公開鍵」と「秘密鍵」のペアを作り、ブラウザに公開鍵を渡し、この公開鍵でデータを暗号化して送るように要求します。ブラウザは公開鍵を使ってデータを暗号化し、サーバにデータを送ります。

自分の公開鍵で暗号化されたデータを受け取ったサーバは、ペアとなっている秘密鍵で暗号を解読（復号）します。このとき、公開鍵で暗号化されたデータはペアになる秘密鍵でしか復号できない仕組みになっているので、公開鍵が漏れても解読されることはなく安心できるわけです。

■不正アクセスから PC を守る

インターネットなどを通じて、不正に他人の PC や Web サイトに侵入することを不正アクセスと言います。最も被害が大きいのが、スパイウェアによるものです。スパイウェアはその名の通り、PC の内部に入り込み、外部にユーザーの個人情報を送信したり、セキュリティのために閉じてあるポートを開放してウイルスを取り込んだりします。

・気が付きにくい不正アクセス

スパイウェアは、ウイルスのように他の PC に感染するということはありません。侵入した PC 内でのみ活動します。ユーザーの知らないうちに送り込まれるスパイウェアは、静かに PC 内部に潜んでおり、ウイルス対策ソフトでも検出は困難です。しかし、ひとたび活動を開始すると、PC 内部の個人情報を外部に送信したり、勝手にポップアップウィンドウを表示したり、お気に入りを書き換えたりします。キー操作を記録するキーロガーなどで ID やパスワードなどを盗み出すこともあります。

しかし、異常が発生しなければ、ユーザーはほとんど気が付きません。

万一、PC に次のような症状が現れたときには、スパイウェア侵入を疑ってみた方が良いかもしれません。

■メール
・覚えのない相手から、身に覚えのないメール(迷惑メール等)が届くようになった
■ Internet Explorer
・Internet Explorer の起動時のホームページが勝手に変わってしまう。戻せない ・「お気に入り」に覚えのない URL が追加されている ・ ポップアップウィンドウが表示されるようになった ・ Internet Explorer が起動しない
■ OS
・フリーズや異常終了など動作が不安定になった ・PC 起動時にインストールした覚えのないソフトが起動する ・PC の動作が遅くなり、場合によってはフリーズする ・PC を終了しようとしても、エラーで正常に終了できない

表：スパイウェア侵入の兆候

・不正アクセス対策ソフト

スパイウェア対策の基本もスパイウェア対策用のソフトの導入です。ウイルス対策ソフトに簡易なスパイウェア対策機能を持つものもありますが、ウイルスとは性格が異なりますので不十分なことが多いようです。専用のソフトウェアの導入をお勧めします。

代表的なスパイウェア対策ソフトとして、Microsoft 社の「Windows Defender」があります。日本語の正式版が公開されており、Windows Vista には標準で搭載されています。PC 内部に侵入したスパイウェアを検出し、削除します。手動での検査やあらかじめ設定したスケジュールによる定期的な検査によるスパイウェア検出のほか、リアルタイム保護機能によりスパイウェアがインストールされる前にブロックすることもできるようになっています。なお、Windows Defender は無償でダウンロードして使用することができます。

（http://www.microsoft.com/japan/athome/security/spyware/software/default.mspx）

■OS もアプリケーションも常に最新の状態で

PC のセキュリティを確保するためには、OS、ブラウザ、プラグイン、アプリケーションをこまめにアップデートして、常に最新の状態を保つようにしなくてはなりません。これは、ソフトウェアの脆弱性（セキュリティ上の欠点）を突いて、ウイルスやスパイウェアが送り込まれる可能性があるからです。ソフトウェアメーカーは発見された脆弱性を修正したセキュリティパッチと呼ばれるプログラムを公開しています。新しいウイルスに最新の定義ファイルで対応するように、新しく発見された脆弱性は最新のセキュリティパッチで修正され、これがアップデートプログラムとして提供されるのです。

特に、ウイルス対策ソフトの定義ファイルは必ず最新の状態にしておくことが必要です。

Windows やウイルス対策ソフトには自動更新機能が装備されており、この機能を有効にしておけば、日常意識することなく PC を最新の状態に保つことができます。積極的に活用したいものです。

PC のセキュリティは、悪意ある攻撃に対して対症療法的に対応しているのが現実です。新しいウイルスに対して新しい定義ファイル、新手の詐欺手法に対して対応策や対応プログラムというように、悪意ある攻撃の方が常に一歩先というのが現状なのです。こうした状況に対処するためには、ユーザー自身のセキュリティに対する意識が重要です。マルウェアの 95%以上がメールまたはメールの添付ファイルによって感染しています。不審な添付ファイルをダブルクリックしない、メールの表示はテキスト形式にするというだけで、ほとんどのマルウェアを防ぐことができるのです。この機会に、ブラウザやメールソフトの設定など目の前の PC について考えてみてください。

■おさらい

・ウイルス対策ソフトの定義ファイルは常に最新のものに更新しておく
・ウイルス対策の基本は、ウイルス対策ソフトの導入・ブラウザの設定・ソフトのアップデート
・SSL はオンラインショッピングなど安全な通信のための仕組み。URL の「https://～」の「s」とブラウザの鍵アイコンを確認する。
・不正アクセスには、スパイウェア対策ソフトを導入する。
・OS もアプリケーションも常に最新のものにアップデートしておく

次回はサーバの仕組みについてお話しします。

・参考リンク
IPA セキュリティセンター
http://www.ipa.go.jp/security/index.html
インターネットセキュリティナレッジ
http://is702.jp/
シマンテック
http://www.symantec.com/region/jp/index.html
トレンドマイクロ
http://www.trendmicro.co.jp/
マカフィー
http://www.mcafee.com/jp/