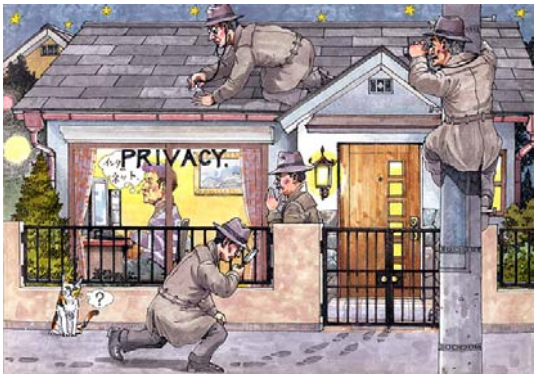
第 6 回 ブラウザとプライバシー



居ながらにして世界とつながるインターネット。ショッピングも自宅でじっくり品定めして、クリックするだけの便利さ。ところが一度ショッピングしたサイトを開くと、ログインしていないのに自分の名前が…。便利さの反面、少し怖いところもあります。Web サーバとの通信を保つ Cookie、PC の中に保存されているキャッシュ、閲覧履歴などは設定次第で要注意機能にもなります。今回は、ブラウザの設定で、自分のプライバシーを守る方法を解説します。

【今回登場するキーワード】

「Cookie（クッキー）」
「セッション」
「プライバシーポリシー 」
「キャッシュ（インターネット一時ファイル） 」
「履歴」

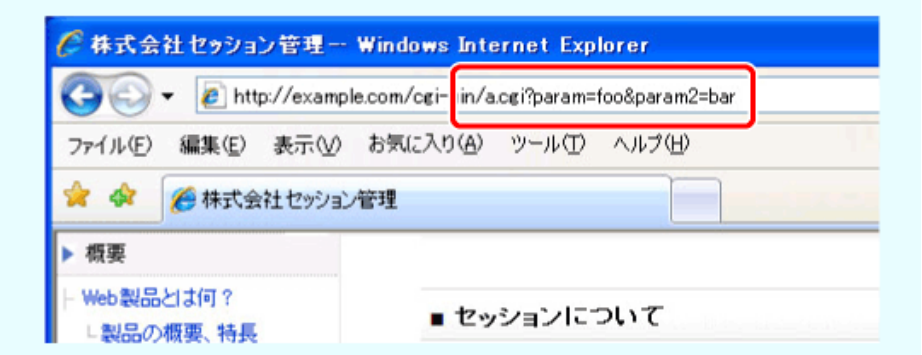
CD や書籍の販売で世界一のネットショップ Amazon.com にアクセスすると、以前そこで買い物をした経験があれば「こんにちは、〇〇さん。おすすめの商品があります。」と自分の名前とともにおすすめ商品が表示されます。Amazon.com に何らかの自分のデータが残っていることが想像できます。しかしどうして私が〇〇と分かったのでしょうか。

■どうして名前が分かるのか

Web サーバとブラウザはページ情報だけをやり取りしているわけではありません。まず、Web サーバがブラウザを見分ける仕組みから見てみましょう。

・ブラウザを見分ける

Web サーバとブラウザの間はデータの「要求」に「応答」するという単純なやりとりで成り立っています。ブラウザからのトップページのデータを送信してくださいという要求に対して、Web サーバは、トップページの HTML や画像などを含んだデータを送信します。この両者のやりとりをセッションといいます。ページを閲覧していくうちに、次の図のように URL の後に暗号のような文字が続くことがあります。



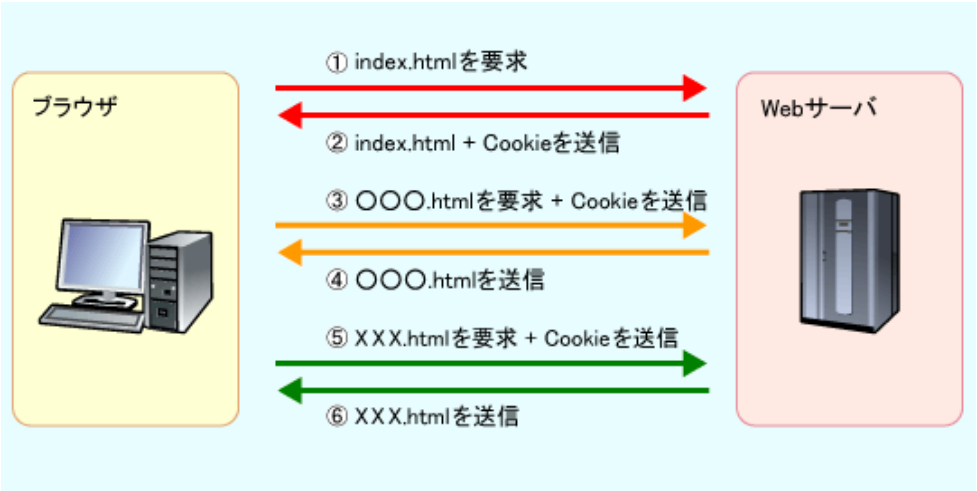
この URL の「？」から右の文字列をセッション ID といいます。Web サーバがブラウザを特定するための符号です。Web サーバからブラウザに送信され、これを受け取ったブラウザは、Web サーバにデータを要求するときにこのセッション ID を一緒に送信します。こうすることで、Web サーバは、すでにログイン済みのブラウザであるから認証を省略する、このブラウザからの要求によって特別な処理を行うといった、特定のブラウザ向けの動作をすることができるのです。

ネットショップのように、ログインした後で同じショップの他のページに移動しても、セッションが継続されている限り、ID やパスワードの入力を省略できるのも、この仕組みがあるからです。

こうしたセッション ID の送受信は、上図のようにブラウザの URL 欄を使う方法以外に、HTML の中に画面に表示されない属性を付けてやり取りしたり、Cookie と呼ばれるテキストファイルに保存してやり取りしたりしています。この中では、Cookie による方法が最も多く使われています。

・ブラウザと Web サーバをつなぐ合い言葉“Cookie（クッキー）”

Amazon.com などでショッピングをしたり、会員登録をしたサイトを訪問すると、ログインしていないのにユーザー名を表示するのは、この Cookie によるものです。Cookie は、Web サーバがブラウザに対して情報を残す仕組みです。Web サーバは送信するデータに Set-Cookie というヘッダーを付けて送信します。これを受けたブラウザは、その Web サーバ専用の Cookie を生成します。そして、2 回目以降、その Web サーバにデータを要求するときには Cookie を同時に送信します。Web サーバは送られてきた Cookie で、Web サイト内のデータベースの記録を調べてユーザー名を表示したり、認証を省略したりします。

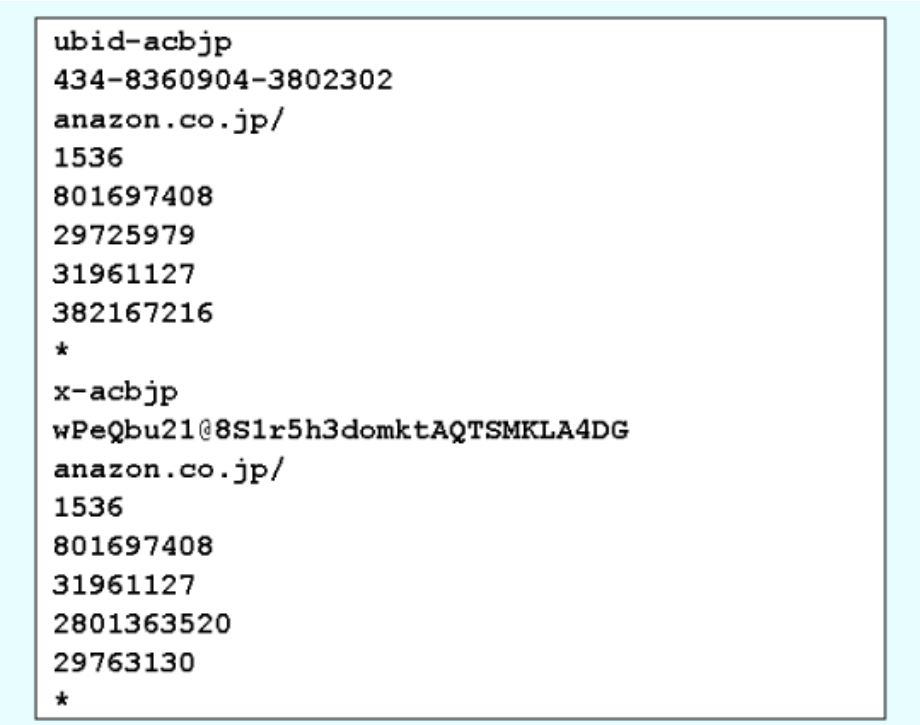


Cookie 自体に個人情報は含まれてはいませんが、ブラウザに名前を表示させたくない場合があるかもしれません。

ブラウザは Cookie を受け取るように初期設定されていることが多いため、ユーザーの多くは知らずに Cookie を受け取っていますが、ブラウザ側で Cookie の受け取りを拒否したり、制限したりすることができます。ただし、Cookie の受け取りを全面的に拒否すると、ブラウザは Cookie を受け取るかどうか確認する画面を頻繁に表示するようになり、Web の利用が実用的でなくなります。というのは、Web ページの Cookie は 1 ページに 1 個だけとは限らないからです。Web ページ上のバナー広告や文字だけの広告も、クリックして広告掲載者の Web ページを表示したか、そこで買い物をしたかなどを調べるために、Cookie が埋め込まれています。そのため、Cookie をすべて拒否すると、ブラウザからの確認メッセージが多くなってしまうのです。

・Cookie とはどんなもの

Cookie の実体は次のようなテキストファイルです。



【 図 】Cookieの実体

上記の Cookie の実体からは簡単には読み取ることはできませんが、ID やパスワードなどのユーザー情報や、ドメイン名、最後にサイトを訪れた日時、訪問回数などが記録されています。さらに、Cookie には有効期間があり、ブラウザを閉じると消滅する一時的なものから、数時間、さらには 30 日間といった長期間保存されるものもあります。

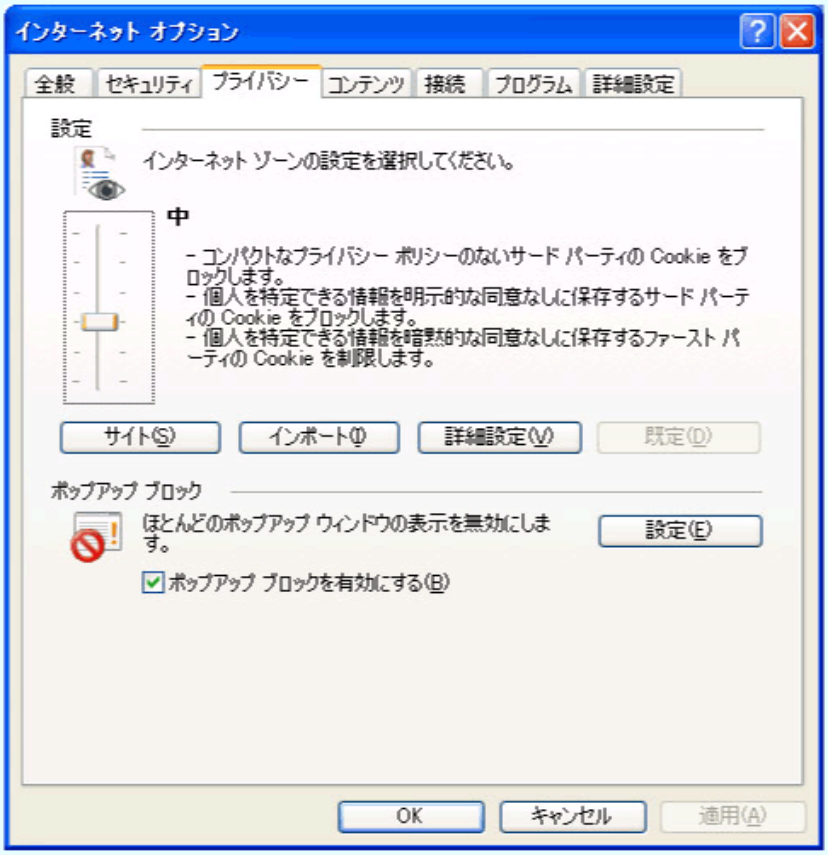
Cookie は、それをセットした Web サイトだけが利用できる情報です。ある Web サイトが作成した Cookie を他の Web サイトが利用することはできません。W3C(The World Wide Web Consortium)が Web サイトのプライバシーポリシーを記述するための標準フォーマットとして

P3P(Platform for Privacy Preferences)を定めており、Cookie の保存方法は厳しく制限されています。個人情報が送受信されることはないようになっていますが、Web サイトのデータベースと連動して、ユーザー名を表示したり、おすすめ商品を表示したりすることがあり、PC を共有する場合には不都合も生じます。そうした場合に、Cookie の受け取りを制限したり、サイトごとに対応方法を分けたりすることができます。

・Cookie を受け取る、受け取らないを設定する

Cookie に関する設定方法を紹介しておきましょう。

画面は、Internet Explorer 7（以降、IE7 と表記します。なお特に断りのない限り IE6 でも機能・操作方法は同じです）の例です。「ツール」メニュー、「インターネットオプション」を選択し、「プライバシー」タブの画面を表示させます。



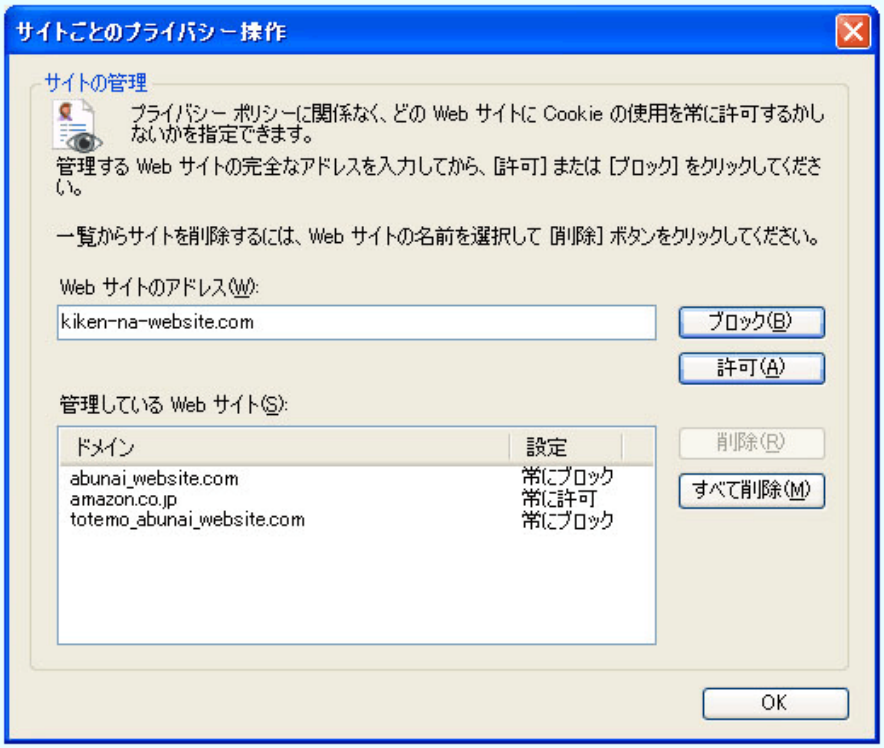
【図】プライバシータブ画面

Firefox では「ツール」メニュー「オプション」の「プライバシー」画面で同等の設定が可能です。
Opera では「ツール」メニュー「設定」の「プライバシー」画面で同等の設定が可能です。

画面の上半分で Cookie の設定を行います。インターネットゾーンの設定のスライダーを上に動かして、最上部にすると全ての Cookie がブロック（受け取りを拒否）されます。逆に、最下部にすると、全ての Cookie を受け取ります。実際には「サイト」または「詳細設定」ボタンで細かく設定を行うことをお勧めします。

サイト

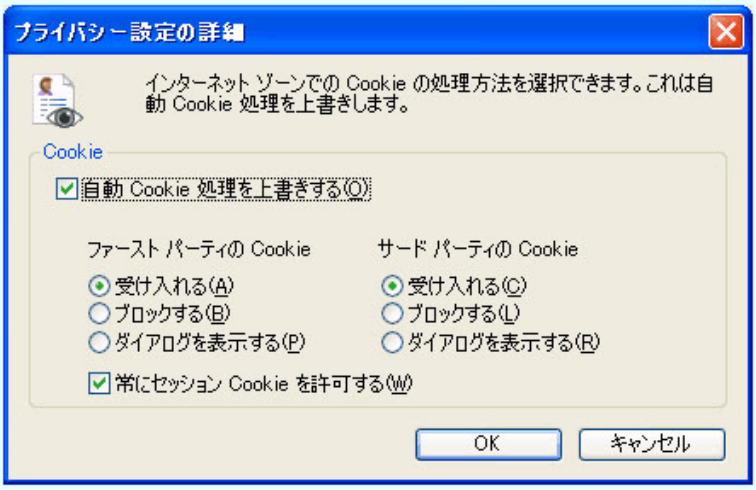
Web サイトごとに Cookie を受け取る、受け取らないを設定します。常にブロックする、または常に許可する Web サイトを個別に設定します。ここで指定した Web サイト以外からの Cookie は、「プライバシー」タブ画面のインターネットゾーンの設定に従います。



【 図 】サイトごとのプライバシー操作画面

詳細設定

インターネットゾーンの設定での処理方法を選択します。



【 図 】プライバシー設定の詳細画面（自動Cookie上書きをチェック）

「ファーストパーティの Cookie」とは表示される Web サイトの Cookie です。「サードパーティの Cookie」とは、その Web ページに貼り付けられた広告バナーなどの Cookie です。「ダイアログを表示する」を選択すると、Cookie のセットが求められるたびに、受け取るかどうか問い合わせる画面が表示されるようになります。安全性は高くなりますが、実際に Web サイトを閲覧するとこのダイアログが頻繁に表示され大変使いにくくなります。

「セッション Cookie」とはブラウザを閉じた時点で消滅する一時的な Cookie のことです。

詳細設定を行うと、「プライバシー」タブの画面でインターネットゾーンの設定は「カスタム」となります。

インポート

このボタンを最後に説明するのは、現時点で手軽に利用する方法がないからです。通常、インポート機能があればどこかにその逆、つまりエクスポート機能があるはずですが、IE7 にはありません（IE6 にも）。Microsoft 社の Web サイトでは、「カスタマイズしたプライバシーインポートファイルを作成する方法」（http://www.microsoft.com/japan/msdn/workshop/security/privacy/overview/privacyimportxml.aspx）が案内されていますが、XML(Extensible Markup Language)で作成したプライバシー設定のスクリプトをインポートするもので簡単な機能ではありません。

■Web サイトをたどった足跡を消す

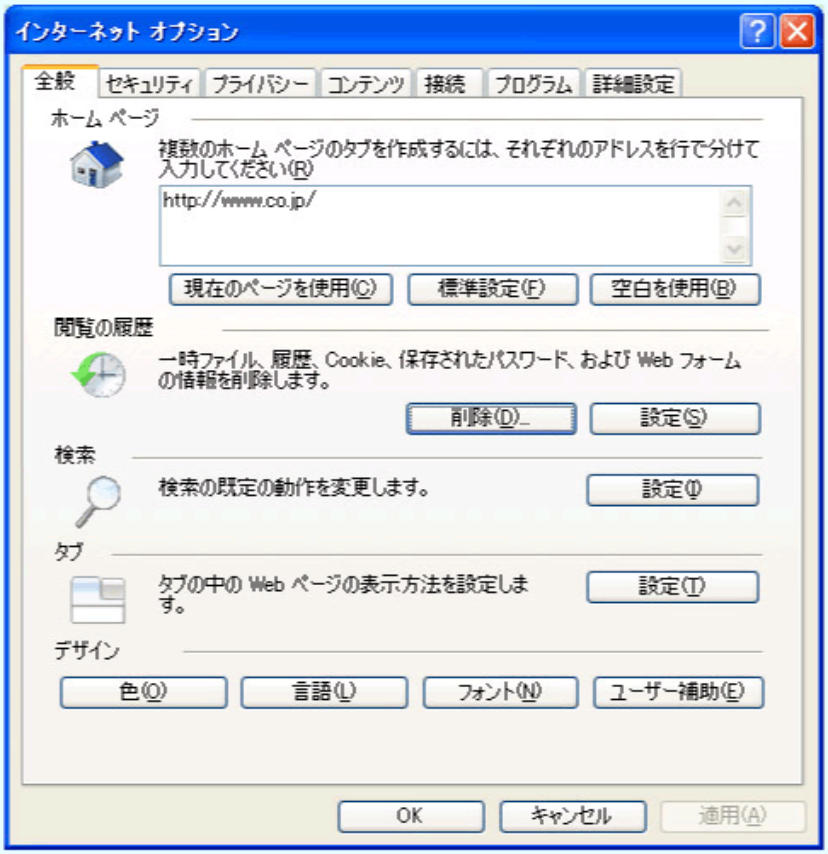
ブラウザの履歴表示で、これまでに表示した Web ページを見ることができます。自分だけが使用する PC であれば問題ありませんが、PC を共有している場合や他の人が使用したときに、この機能で訪問先の Web サイトが見られてしまうかもしれません。また、一時的に他の人の PC を借用したときに自分が閲覧したサイトの記録が残ってしまいます。

Web サイト訪問の足跡を消すには、表示履歴のファイルを消去する方法と、PC に保存されているインターネット一時ファイルを削除する方法があります。履歴の中で残したいものと消したいものが混在する場合には、手作業で履歴を削除します。履歴とキャッシュ（インターネット一時ファイル）を削除する方法を説明します。

・Web サイトの訪問履歴を消す

履歴ボタンで、閲覧した日時ごとに表示した Web サイトの URL を参照することができます。便利な機能ですが、検索サイトでの検索語まで残りますので、PC を共有している場合には注意したい機能です。

IE では履歴やインターネット一時ファイルなどの訪問履歴をまとめて削除することができるようになっています。「ツール」メニュー、「インターネットオプション」を選択し、「全般」タブの画面を表示させます。



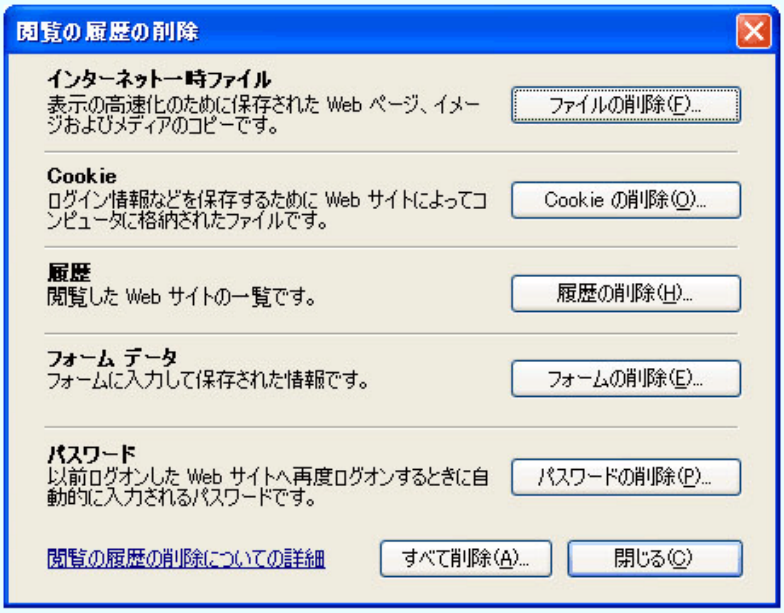
【図】インターネットオプション全般タブ

Firefox では「ツール」メニュー「オプション」の「プライバシー」画面で同等の設定が可能です。
Opera では「ツール」メニュー「設定」の「履歴とキャッシュ」画面で同等の設定が可能です。

閲覧の履歴を削除するときは、閲覧の履歴の「削除」、キャッシュと履歴を設定するときは「設定」を選びます。

・閲覧の履歴を削除する

「全般」タブの閲覧の履歴の「削除」を選択すると次の画面が表示されます。なお、Internet Explorer 6 では全般タブの画面で削除することができますが、フォームとパスワードだけを削除する機能はありません。



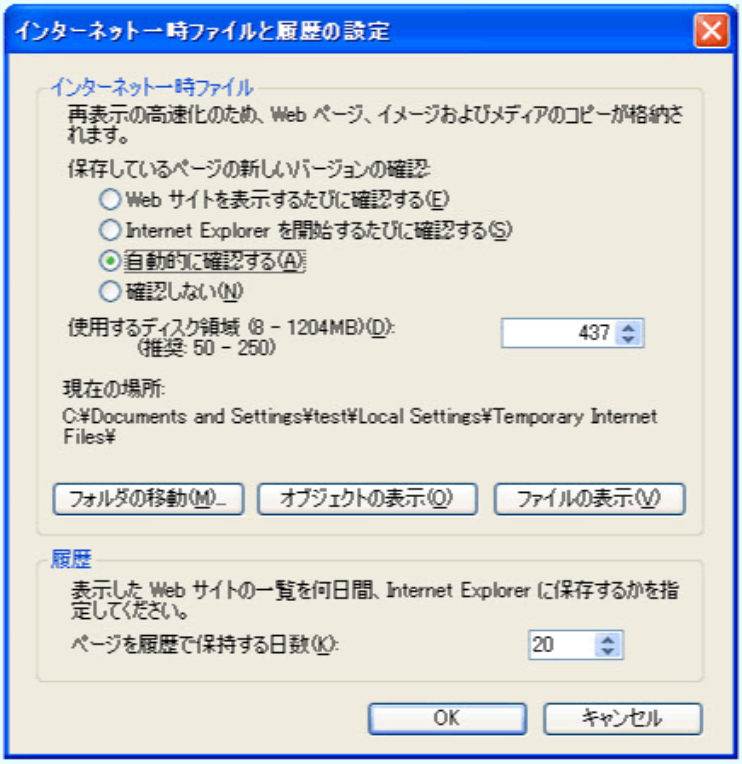
【 図 】閲覧の履歴の削除

インターネット一時ファイル	Web ページの HTML や画像データは「インターネット一時ファイル」として HDD に保存されています。次回以降同じページを表示するときに、この中から読み出して表示することで、通信回線を経由するよりも高速に表示するためのものです。IE の「戻る」ボタンや「履歴」、「オフライン表示」はこのファイルを参照しています。本稿では、「インターネット一時ファイル」をキャッシュと表記しています。
Cookie	PC の中にすでに保存されている Cookie を消去します。Cookie については前項をご覧ください。
フォームデータ	ログイン画面や登録画面など Web サイトの入力フォームで入力したデータも履歴として保存されています。このデータを削除します。
パスワード	ログイン画面で入力の際に保存したパスワードを削除します。
すべて削除	上記の全てを削除します。公共の施設などの共用 PC の使用終了時には、必ずこの操作を行って、Web サイトへのアクセスの痕跡をすべて消しておくようにしましょう。なお、すべて削除しても、Cookie がメモリに残っている場合がありますので、この操作を行った後、必ずブラウザを終了させてください。

■Web サイト訪問の足跡の残し方を設定する

プライバシーは大切ですが、Web サイトの訪問履歴やキャッシュは、残し方を工夫すれば、オフラインでの使用や再訪問に便利な機能です。削除だけでなく、残すための設定方法も紹介しておきましょう。

「全般」タブの閲覧の履歴の「設定」を選択すると「インターネット一時ファイルと履歴の設定」画面が表示されます。



【 図 】インターネット一時ファイルと履歴の設定

この画面でキャッシュと履歴の保存方法や期限を設定します。

・インターネット一時ファイル（キャッシュ）

キャッシュをどのように利用するかを設定します。ブラウザはページを表示するときに、その Web ページのデータがキャッシュに保存されているかどうか調べます。保存されていれば、更新日付を比較し、新しい方のデータを表示します。ここで設定するのは、更新日付を比較するかどうか、する場合には常に比較するのかどうか、を設定します。

ページを表示するごとに確認する	常に最新のページを表示します。Web ページを表示するたびにサーバにアクセスし、更新されていれば最新の情報を読み込みます。
Internet Explorer を起動するごとに確認する	IE を起動後アクセスした Web ページは最新の情報が表示され、同じページへの 2 回目以降のアクセスではキャッシュが表示されます。
自動的に確認する	ページの更新頻度をもとに最新の情報を表示するか、キャッシュを表示するかを IE が自動的に判断します。
確認しない	常にキャッシュが表示されます。サーバへはアクセスしないため、表示速度は最も速くなります。

上へいくほど情報の新しさ優先、下へいくほどブラウザの表示速度優先の設定です。IE のデフォルト設定は「自動的に確認する」となっています。高速回線を使用している場合は「ページを表示するごとに確認する」か「Internet Explorer を起動するたびに確認する」をお勧めします。低速回線の場合は、「自動的に確認する」をお勧めします。

使用するディスク領域

インターネット一時ファイル用として使うディスク容量を指定します。MB（メガバイト）単位の数字で指定します。

IE では、システムディスクの 3%がキャッシュのデフォルト値として設定されます（バージョンアップした場合は前の設定値を引き継ぐ)。40GB の HDD の場合には 1.2GB にもなります。キャッシュは大きすぎると、更新日付を比較する際の PC の負荷が高くなりますが、画面表示の体感上の差はありません。ただ、ファイル数は数万（記事作成用の PC の例では 384MB で約 55000 ファイル）となり、HDD のメンテナンス時のスキャンディスクやウィルススキャンなどでは動作に要する時間が長くなります。128MB～256MB の範囲で十分と推測されます。

現在の場所

キャッシュが保存されているフォルダ名が表示されます。保存フォルダの変更は、「フォルダの移動」ボタンで行います。

「フォルダの移動」	キャッシュの保存場所を変更します。「使用するディスク領域」の設定値以上の空き容量を持つ HDD を指定してください。
「オブジェクトの表示」	既にダウンロードされている ActiveX コントロールなどを表示します。
「ファイルの表示」	保存されているキャッシュの一覧を表示します。

履歴

履歴として PC に URL とアクセスした日時を保存しておく日数を指定します。この日数を過ぎた履歴は削除されます。

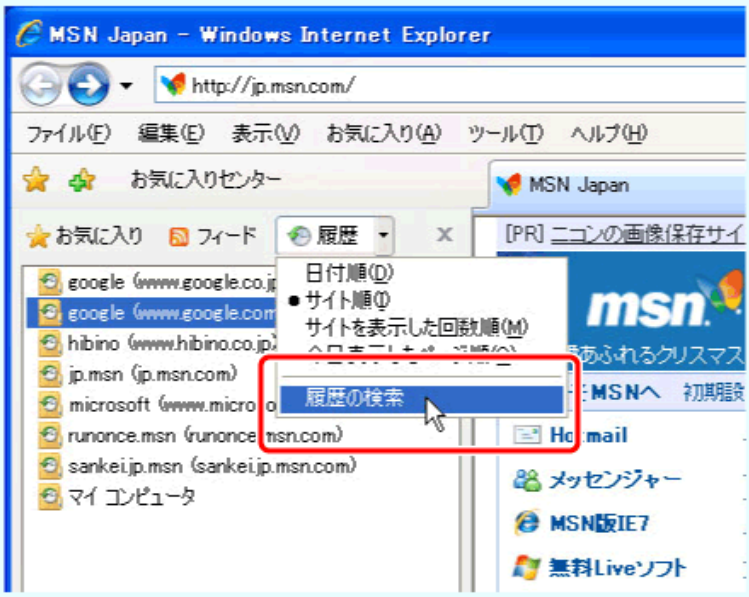
・残しておきたくない履歴だけを削除する

共有の PC や一時的に他の人の PC を利用した場合に、フォームへの入力やログイン時の情報を保持する Web サイトなどの訪問履歴は残しておきたくありません。かとってすべての履歴を削

除するわけにもいきません。そうした場合には、残したくない訪問履歴だけを選んで手動で削除する方法があります。

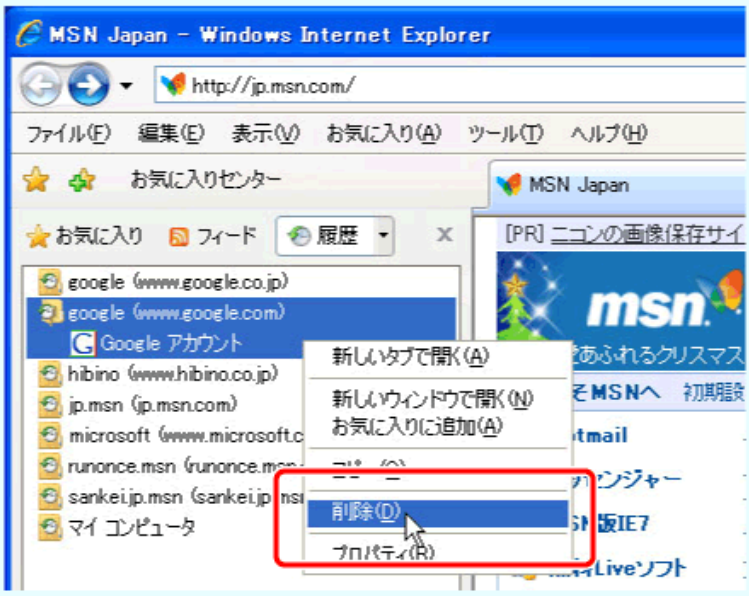
ブラウザの「ツール」メニューの「ツールバー」から「履歴」を選択します。

訪問履歴が表示されますので、履歴の検索や並べ替え機能を使って、履歴の一覧から残したくない Web サイトの URL を探します。



【 図 】履歴の検索

残したくない URL を選択し、右クリックして表示されるメニューから「削除」をクリックします。

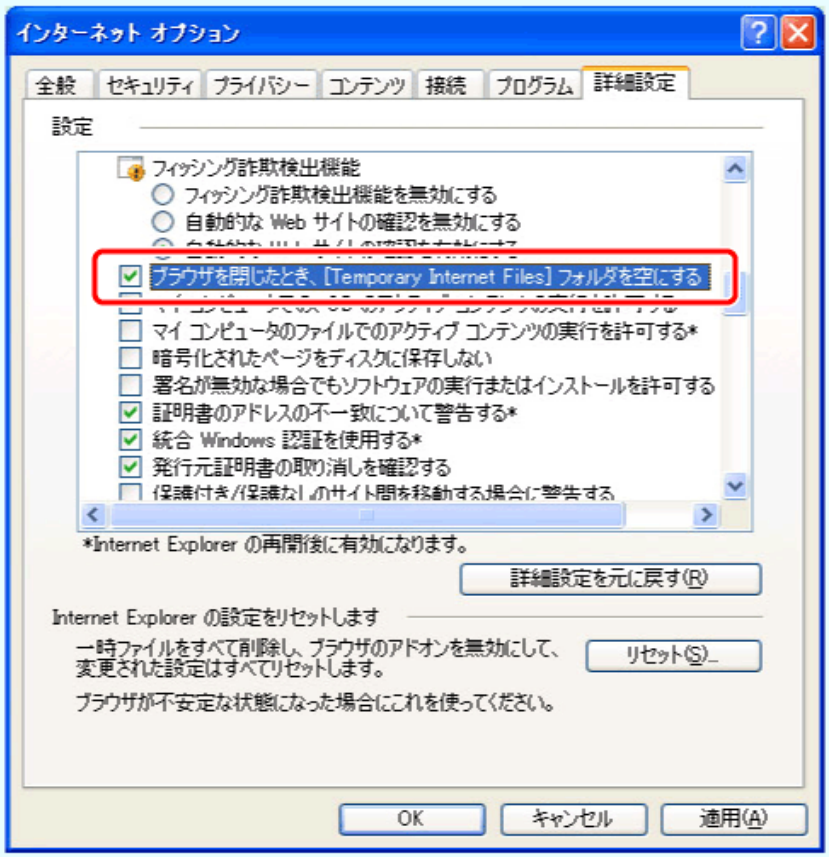


【 図 】手作業で履歴を削除する

・ブラウザを閉じたときにインターネット一時ファイルを削除する

フォームの入力画面などを扱うことが多い業務用 PC では、キャッシュを一切残さないようにするのも有効です。悪意ある第三者によるのぞき見や万一の PC 本体の盗難に対して最低限の機密が保持されます。そのために、ブラウザを閉じたときに、キャッシュ用のフォルダを空にする設定があります。

「ツール」メニュー、「インターネットオプション」を選択し、「詳細設定」タブの画面を表示させ、「ブラウザを閉じたとき、[Temporary Internet Files]フォルダを空にする」をチェックして「OK」ボタンをクリックします。



【 画面 】ブラウザを閉じたときキャッシュをクリアする

上記の設定でキャッシュ用のフォルダは空になります。通信環境によっては、起動時のブラウザの Web ページ表示は遅くなりますが、インターネット一時ファイルの設定を「Internet Explorer を起動するごとに確認する」としておくことで、ブラウザを閉じるまではキャッシュが利用できますので、速度低下の心配はないと思われます。

■Web サーバが取得するブラウザの情報

Web サーバはブラウザとの通信時に、相手のブラウザの情報を取得しています。前回、ワンクリック詐欺サイトでは、あたかも個人情報を取得したかのように表示するとお話ししましたが、表示される情報の基になっているのが、この Web サーバが取得するブラウザの情報です。

Web サーバはアクセスしたユーザーの情報をどこまで取得できるのでしょうか。インターネットには、Web サイトにアクセスすることで、サーバ側が得ることのできるブラウザ情報を表示するサイトがいくつかあります。

例：
Web ブラウザが公開する情報 ： 架空請求事業者データベース
Fictitious claim swindle data base (http://www.yumenara.com/kaku/env/)
Environment Variables Checker (http://www.cybersyndrome.net/evc.html)

サーバは、アクセスしてきたブラウザから次のような情報を取得しています。上記のサイトで確認してみてください。

項目:値（値は説明用に変更しています）	解　説
ブラウザ&OS Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)	利用中のブラウザと OS、画面の解像度です。最適な画面表示のためには欠かすことができない情報です。
IP アドレス: 58.1.xxx.xxx	インターネットの利用には必須のアドレスです。
ホストネーム: fnttkyoxxx.tkyo.fnt.ftth.ppp.xxxxx.ne.jp	IP アドレスの別名です。利用しているプロバイダや大まかな地域は特定できることがあります。
使用ポート: 4671	1024 番から 65535 番までの中からランダムに選ばれ、アクセスするたびに変わります。
アクセスした日時: 2007 年 12 月 14 日 02 時 51 分 40 秒	この日時はサーバの時計の日時です。
UNIX 時間: 1197568300	アクセスした日時を、UNIX 時間に変換したものです。単位は秒です。
レファラ （表示はされません）	どのサイトを経由してきたか、検索エンジン、キーワードなどがわかります。

サーバは以上のような情報を取得していることを覚えておきましょう。どれもサーバがブラウザに最適なデータを提供するために必要な情報です。この中で個人情報を特定できるのは、強いてあげれば IP アドレスですが、地域や団体などをある程度までの範囲で絞り込むことはできるかもしれませんが、完全に個人を特定できるものではありません。ワンクリック詐欺サイトではこれらの情報の一部を表示して個人情報を得たように装います。画面表示をよく確認しましょう。

エラーメッセージや警告を偽装してクリックさせるものもありますので、最後に Web サーバからのメッセージについて触れておきます。

■Web サーバからのメッセージ

Web サーバはブラウザとのやりとりに問題が生じたときに、ブラウザにエラーメッセージを送信します。「404 Not Found エラー」はどなたも一度はご覧になったことがあるでしょう。リンク先のページが存在しないというエラーです。先頭の「404」をステータスコードと言います。ステータスコードは次のように分類されています。

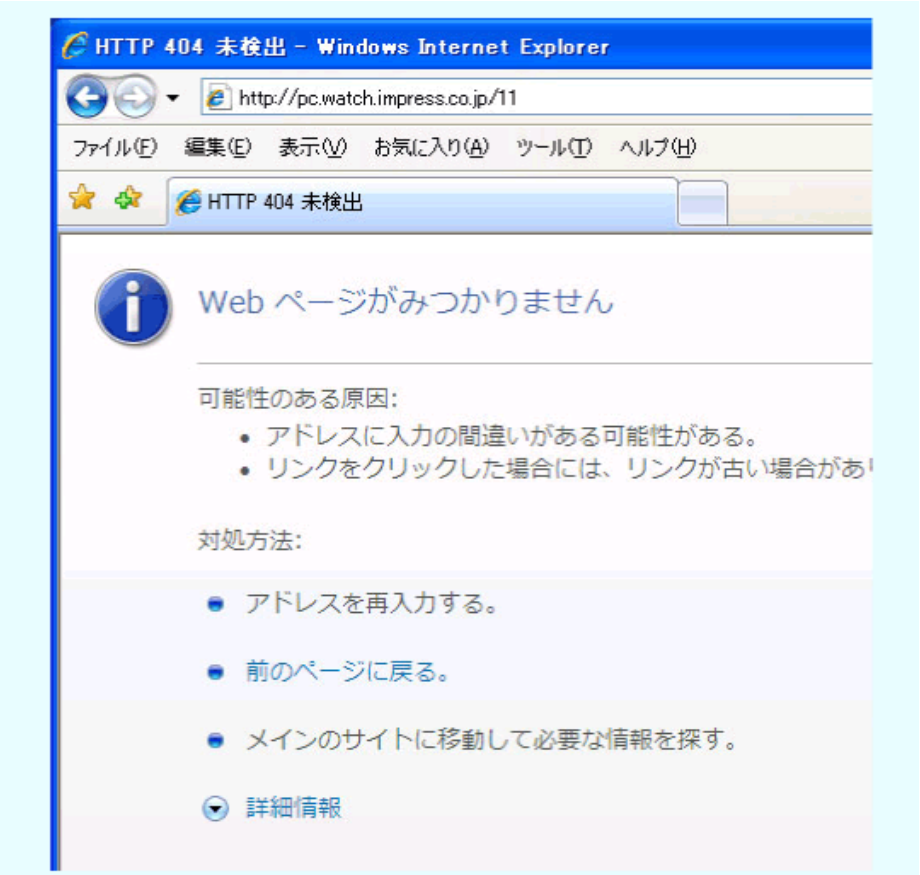
ステータスコード	意　味
100 番台	案内（インフォメーション）
200 番台	正常処理
300 番台	移転通知
400 番台	（クライアントにおける）処理失敗
500 番台	サーバーエラー

表：Web サーバのステータスコード

ブラウザではエラーとして 300 番～500 番台のコードまたはメッセージが表示されます。エラーの代表的なものとユーザー側での対処方法を紹介しておきます。ブラウザによっては、独自のメッセージを表示する場合があり、必ずしも以下のようなメッセージとは限りません（後述）。

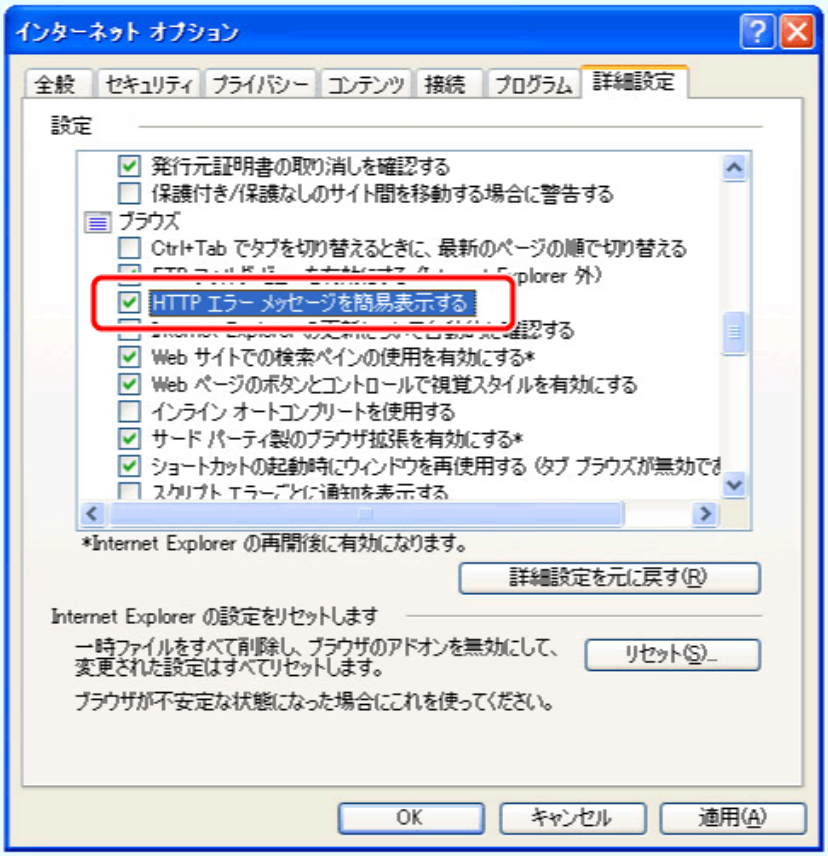
エラーメッセージと意味	説　明
401 Authorization Required 「認証に失敗しました」	パスワードや ID が間違っていて認証ができないので閲覧を許可できない、というエラーです。問題なく閲覧できていたサイトでこのエラーが表示された場合、Cookie が削除されたか、期限切れになっているため、あらためて認証が必要になっていることが考えられます。
403 Forbidden 「接続が禁止されています」	接続するためには権限が必要です。閲覧が禁止されているページですので、「再読込」して結果が同じであれば、ユーザー側では対処のしようはありません。
404 Not Found 「ファイルが見つかりませんでした」	ページが移動していたり、ファイルが削除されていたりしています。入力された URL のタイプミスでも発生します。リンク元を「再読込」して再度リンクをクリックしても結果が同じであれば、サーバ側の問題である可能性が高く、ユーザー側では対処できません。
500 Internal Server Error 「内部エラーが発生しています」	サーバの設定や CGI のプログラムの間違いなどが発生しています。サーバ側の問題なので、「再読込」して結果が同じであればユーザー側では対処のしようがありません。
503 Service Temporarily Unavailable 「一時的にサービスを提供することができません」	サーバは一時的にサービスの提供ができなくなっています。アクセスの集中などのため、混み合っているか、メンテナンス中などでページを閲覧できなくなっていますので、時間を置いてアクセスするか、アクセスが少ないと思われる時間帯にもう一度接続してみてください。

ほとんどの場合 Web サーバのエラーメッセージは、IE7 では次のように表示されます。これはブラウザ(IE7)が Web サーバからのメッセージを受け取って独自に表示している画面です。



【 画面 】404 Not Foundエラー画面（IE 7）

「ツール」メニュー、「インターネットオプション」の「詳細設定」で、サーバが送っているオリジナルのエラー表示に切り換えることができます。「HTTP エラーメッセージを簡易表示する」のチェックをはずします。



【 画面 】エラーメッセージの簡易表示

Web サーバのエラーメッセージもほとんどの場合カスタマイズされていますが、時には次のような画面が表示されることがあります。この画面は Apache という Web サーバソフトウェアが出力するエラーメッセージで、いわば素顔の Web サーバのエラーメッセージです。

通常は Web サーバのエラー表示は英文が多く、ブラウザの簡易表示の方が分かりやすくなっています。もちろん、エラーメッセージは見ないですませればそれに越したことはありませんが、万一エラーに遭遇したときは、表示を切り換えてみると表示中の Web サーバソフトウェアを知ることができるかもしれません。

Web サイト閲覧中に、上記以外のエラーメッセージや警告が表示された場合は、むやみに「OK」をクリックしたりせず、画面表示をよく確認してください。時には Windows が警告を表示している場合もあります。怪しいときには、次のような方法でブラウザを終了してください。

操作対象	操作方法
ブラウザ	閉じる（×）ボタン
キーボード	ALT キーと F4 キーの同時押し
タスクバー	右クリックして「閉じる」

表：怪しい警告やメッセージへの対処

■便利さとプライバシー

今日のブラウザにはインターネットを利用するための便利な機能が満載されています。例えば、履歴表示は、閲覧した日やキーワードによる検索で履歴の中から Web ページを探し出すことができる便利な機能です。しかし、この便利さが自分以外の人にとっても同じであることを忘れてしまいがちです。ブラウザの戻るボタンで閲覧した Web ページが表示されてしまったり、履歴に個人情報の入力フォームが残っていたり、Web サイトによっては、おすすめ商品が勝手に表示されたりすることがあります。

悪意の有無とは関係なく、第三者に個人的な情報や仕事関係の情報が見られてしまう可能性があります。キャッシュファイルから情報を得ることも可能です。インターネットに接続中はもとより、接続されていない状態でも注意が必要なのです。そのために、ブラウザにはプライバシーを守るための設定が用意されています。しかし、ブラウザの初期設定は、便利さ優先になっているのが実情です。そのため、多くの人がプライバシーに関する設定はデフォルト値のままでブラウザを利用していると思われます。

前回のセキュリティに関する設定に加えて、Cookie の受け取りやキャッシュ、履歴の設定など、わずかの手数で、安心してインターネットの便利さや楽しさを享受することができるようになります。これを機会に、ぜひご自分のブラウザの設定を見直してみてください。

■おさらい

Cookie はプライバシー設定で、受け取り・ブロックを設定できる。
Web サーバはブラウザから情報を取得する。
キャッシュや履歴の削除・設定の方法を覚えておく。
怪しいエラーメッセージや警告への対処方法を覚えておく。
次回は、知っておくと便利なブラウザの設定のお話し（仮）です。

・参考リンク

とことん Cookie 技術解説：日経パソコンオンライン
http://pc.nikkeibp.co.jp/article/NPC/20070322/265912/

Cookie の食べ方教えます：日経パソコンオンライン
http://pc.nikkeibp.co.jp/article/NPC/20070322/265949/

Internet Explorer での設定
http://www.odn.ne.jp/rescue/browser/ie/index.html

HTTP ステータスコード
http://www5.plala.or.jp/vaio0630/mail/st_code.htm

ITmedia News：怪しい「セキュリティ警告」への対処法、クリックする前も後も落ち着いて
http://www.itmedia.co.jp/news/articles/0610/19/news034.html