JPCERT-ED-2008-0002

JPCERT/CC

技術メモ － 安全な Web ブラウザの使い方

初版：2008-11-04 (Ver. 1.0)

発行日：2008-11-04 (Ver. 1.0)

執筆者：石田 康明、戸田 洋三

本文書の掲載 URL：http://www.jpcert.or.jp/ed/2008/ed080002.pdf

本文章は Web ブラウザを利用して Web ページを閲覧する際に注意すべき事項をまとめたものです。
個々のソフトウェアの情報に関しては常に最新のドキュメントを参照して下さい。

目次

図表目次

I. Web 環境を取り巻く脅威

情報の発信や収集において、インターネットは今や欠かせないインフラであり、多くの人が利用しています。その中でも Web (ウェブ)は企業や商品等の様々な情報の広報や、個人による自分の趣味や動向の発信に使われるなど、重要な情報インフラの一つとなっています。

しかし現在の Web を取り巻く環境に潜む脅威は、過去に比べて量的に増しているばかりでなく、質的にも、ウイルスやワームなどに、フィッシングなどの新しいタイプの脅威も加わって多様性を増してきています。またブラウザの多機能化やコンテンツの多様化に伴い、攻撃手法や攻撃対象も進化しています。さらに Web で提供される情報サービスが増えてきた結果、データの破壊などのいわゆるコンピュータ上での被害にとどまらず、個人・企業情報の盗難や流出、金銭被害や信用の毀損といった大きなダメージを伴う事故も増加の一途をたどっています。

インターネット利用者を狙った大規模な攻撃・感染は、以前は E-mail (メール)等を利用した直接的な攻撃を通じて行われていましたが、現在ではユーザ側による様々な対策が施されてきたことに伴い、多くの人が利用している Web ブラウザを狙った、Web ページに悪意のあるコードを仕掛ける等の手法による、受動的な攻撃・感染が主流となっています。

しかし Web の利用によるメリットは、コスト削減と時間的な効率化の両面で非常に大きく、また携帯電話やネット家電などにも組み込まれていることから、Web ブラウザを全く使わないで済ますことは不可能と言ってもよいでしょう。

本技術メモでは PC で Web ブラウザを用いる場合に、安全に、そして手軽に使うために利用者が守るべき注意点を解説します。

II. Web ブラウザ

Web ページを閲覧するためには一般的に Web ブラウザ と呼ばれる閲覧ソフトウェアが必要です。このソフトウェアは主に HTTP と呼ばれる通信プロトコルを利用して、サーバ側とデータを送受信します。Web ページは HTML などの形式に従って記述されており、Web ブラウザ側ではそれを解釈し、人間が閲覧できるようにレイアウトして画面上に表示します。

送受信されるデータの中にはパスワードやクレジットカード番号といった個人情報が含まれる場合もあり、これらの第三者に盗み見られたくないデータを送受信する場合は、安全にやりとりするためにデータ暗号化や認証を行う SSL が用いられます。

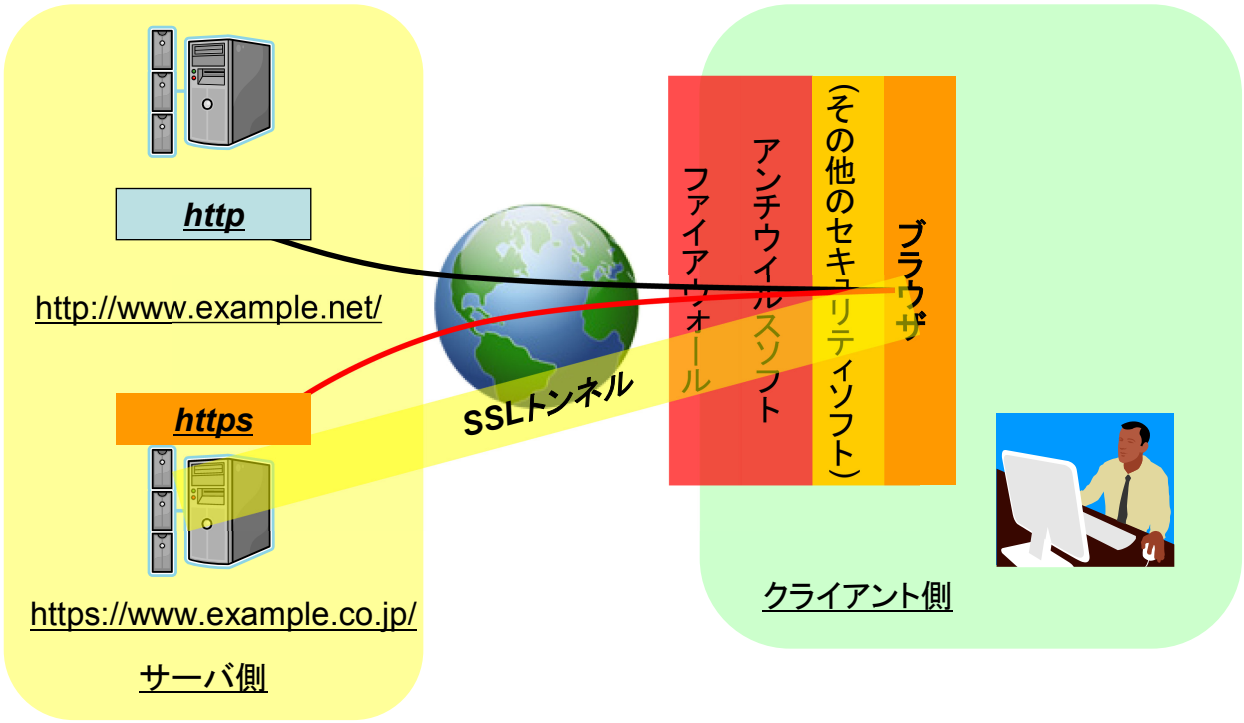

図 1 Web ブラウザを取り巻く環境

Web 技術は急速に進化しており、各ブラウザは競争の結果、多くの機能を標準搭載するようになってきました。また Web ブラウザが標準では表示・再生できないファイルを利用できるようにしたり、すでに存在する機能を拡張・補充したりするために 利用者によって「プラグイン」や「拡張機能」と呼ばれる機能追加のためのソフトウェア(ここでは総称してアドオンと呼びます)が Web ブラウザに組み込まれて利用されることもあります。

また、Web ブラウザの機能(エンジン)は OS や他のアプリケーションと連携して動作する場合があります。例えば、メールクライアントの中には HTML メールを表示する際に、ブラウザエンジンを利用するものもあります。

以下に、主なブラウザと OS、アドオン等の概念図を示します。

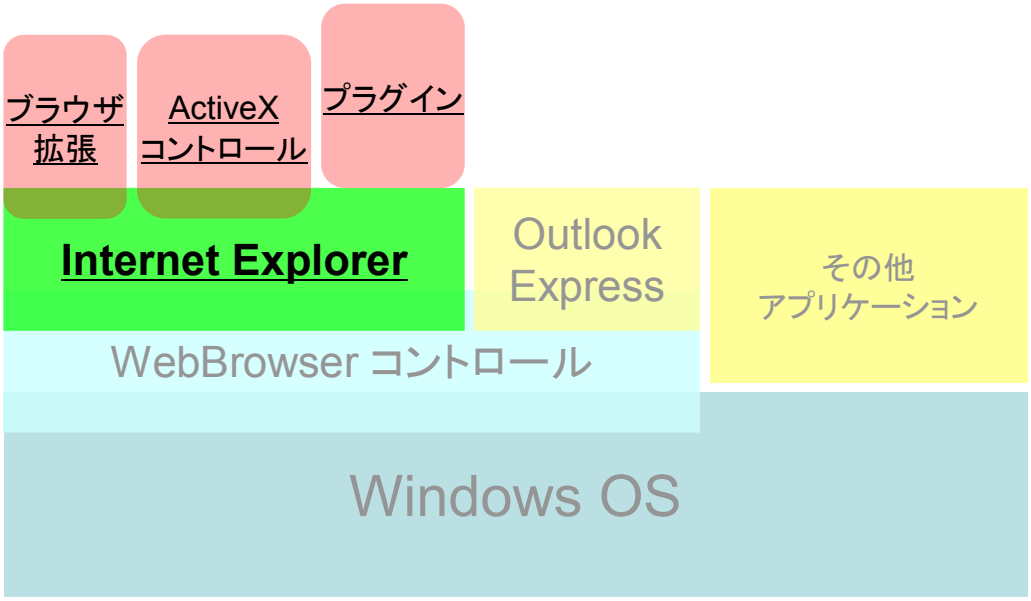

図 2 Internet Explorer と アドオン等

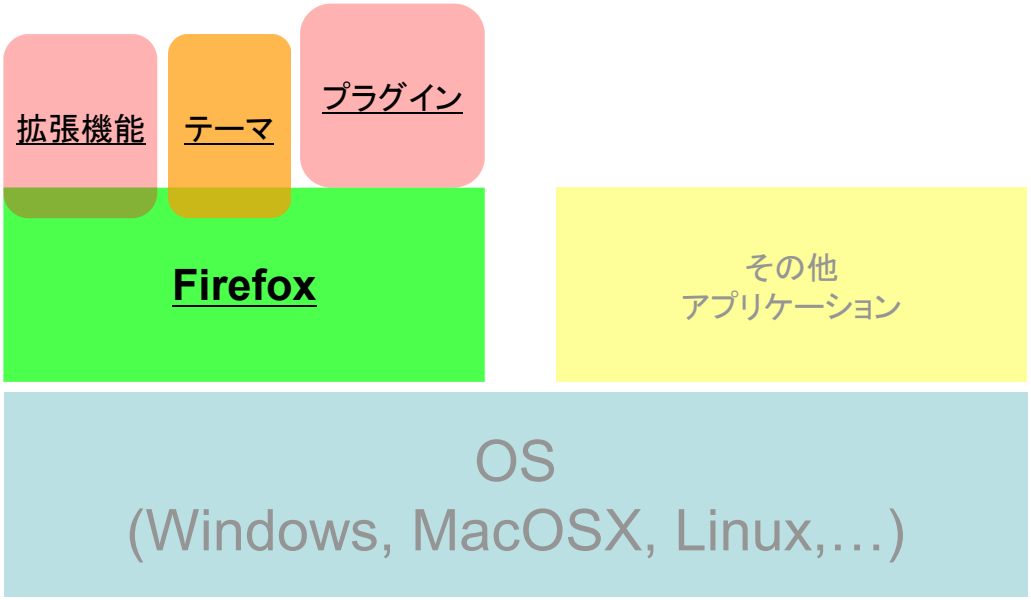

図 3 Firefox とアドオン等

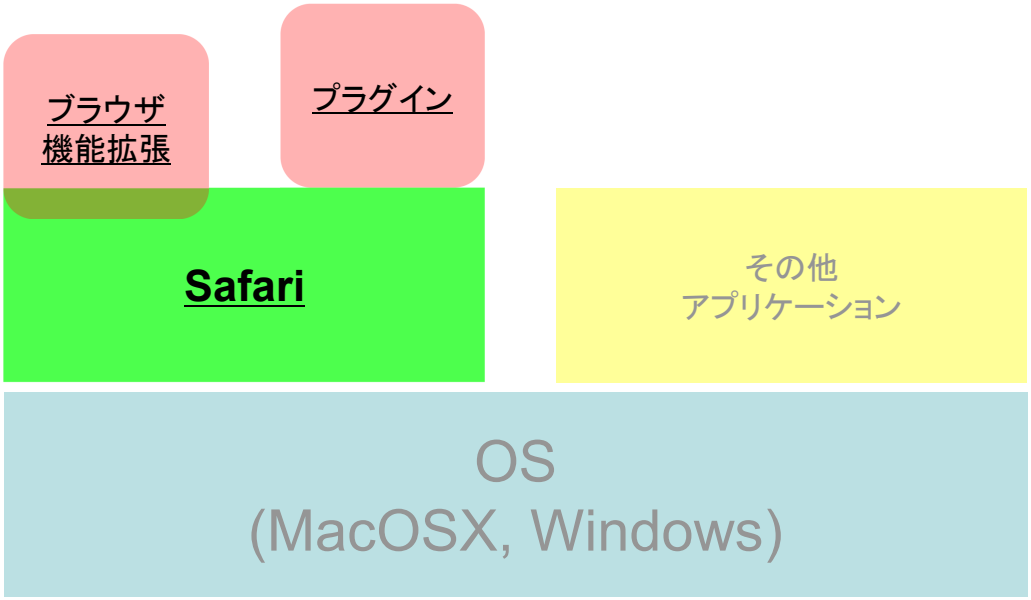

図 4 Safari とアドオン等

しかし便利さの反面で、システム的に複雑になってきたこともあり Web の閲覧時に注意すべき事項も増えてきました。

III. Web を閲覧する前に確認しておくべき事項

Web ブラウザを利用して閲覧する前にあらかじめ以下の点を確認しておきましょう。

1. OS や Web ブラウザは最新の状態に保つ

これが守られていれば多くの脅威から PC を守ることができる、一番重要な事項です。

OS に関しては最新の状態を保つためのプログラムが実装されています。Windows では「Windows Update (Microsoft Update)」、Mac OS X では「ソフトウェアアップデート」がこれに相当します。

Web ブラウザについても OS と同様に最新の状態を保つための機能が実装されています。Internet Explorer は Windows Update、Firefox では「ヘルプ」→「ソフトウェアの更新を確認」、Safari に関しては Mac OS X 版ではソフトウェアアップデートで、Windows 版では「Apple Software Update」を利用することで最新の状態を保つことができます。

サポートが終了した OS や Web ブラウザ、アドオンは、通常、脆弱性やバグが発見された場合でも修正が行われず、そのようなブラウザを使い続けることは攻撃者に対して付け入る隙を与えることになるため、利用すべきではありません。

自分が利用している OS、ソフトウェアのサポートが終了していないかどうかを今一度確認してみて下さい。

2. セキュリティソフトを導入、実行する

セキュリティソフトとは、いわゆるウイルス対策ソフトや(パーソナル)ファイアウォールなどを指し、ウイルスの侵入や外部の攻撃から PC を守るために利用されます。

Web を利用した攻撃の中に、一見しただけではわからない形で攻撃用の不正なコードを Web ページに仕掛け、利用しているユーザに気づかれないように個人情報を盗むものがあります。また、有名な Web ページや利用者が多い Web ページが狙って改竄され、不正なコードが仕掛けられていることもあります。

このような場合には、細心の注意を払っていたとしても人間の眼で発見することは容易ではありません。セキュリティソフトを利用することでこれらの攻撃や不正なコードを検出し、未然に防ぐことができるようにしておきましょう。

IV. 各 Web ブラウザに共通する設定上の注意事項

本章では、安全な Web アクセスのためのブラウザ設定の注意事項について一般的な考え方を解説します。個々の Web ブラウザにおける具体的な設定方法については 次章を参照してください。

1. スクリプト等の実行を制限する

JavaScript 等のスクリプトや ActiveX コントロールなどは、 Web ブラウザ上で表示を変えて動きのある動的なコンテンツを生成・表示するための技術です。

静的なコンテンツをダウンロードすることによって表示を更新していた従来の方式に比べて、これらの技術を利用すれば、ローカルマシン上で Web アプリケーションの処理を可能となり、Ajax に代表されるインタラクティブなインターフェースが実現できるなど、高い利便性が得られます。反面、PC 上の重要なファイルを削除・変更するなど、悪意を持った処理が行われる可能性もあります。従って無制限にスクリプト等を実行できるようにしておくのはセキュリティ上好ましくありません。

これらの機能は原則無効とした上で、信頼できる Web サイトでのみ限定的に有効とする等、一定の制限を加えた上で実行できるようにすべきです。通常、ブラウザにはスクリプト等を制限するための機能が標準的に備わっており、またアドオンではより詳細な設定を行えるものもあります。適切な設定を行い、上手に活用しましょう。

2. ポップアップウィンドウを制限する

Web ページ上のリンクをクリックした際に、閲覧している Web ブラウザのウィンドウとは別にウィンドウが開くことがあります。これはポップアップウィンドウと呼ばれ、広告目的などで、注目させたい内容を特別に目立たせるために利用されることがあります。

しかし、こういったポップアップウィンドウの中に攻撃者による不正なコード等が仕掛けられていたり、ウィンドウを消すと新たなウィンドウが立ち上がるように設定されていることがあり、PC が予期せぬ状態に陥ってしまう可能性があります。

ポップアップウィンドウは自分が信頼できる Web ページのみ許可するようにしましょう。

3. SSL 2.0 を無効化する

SSL 2.0 には実装上の脆弱性があります。SSL 2.0 のみでしか利用できない Web ページはほとんど存在せず、またサポートしている暗号のアルゴリズムも古いため、ブラウザの設定で無効化して使わないようにすべきです。すでに SSL 2.0 をサポートしていない Web ブラウザもありますが、IE6 は初期状態では SSL 2.0 が有効になっているため、あらかじめ無効化しておく注意が必要です。

V. 個々の Web ブラウザの注意事項

この章では、前章で述べた注意事項に対応する、個々の Web ブラウザでの具体的な設定方法を、主な Web ブラウザについて説明していきます。

1. Internet Explorer 6 (IE6)

※ 本文では Windows XP SP3 + IE6 SP3 での利用を前提としています。
公式 Web ページ: http://www.microsoft.com/japan/windows/ie/ie6/default.mspx

IE6 は Windows XP に標準搭載されており、Windows 2000 でも Windows Update 等で別途インストールすることで利用できます。

よりセキュアにするための設定には次のようなものがあります。

① スクリプト等の実行を制限する

- Internet Explorer 6 上で

  [ツール]→[インターネットオプション]→[セキュリティ]
  →[Web コンテンツのゾーン *を選択してセキュリティのレベルを設定する]
  →[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]を選択
  →[既定のレベル]を選択する、もしくは[レベルのカスタマイズ]で各種スクリプトごとにゾーンごとの信頼度に応じて有効/無効/確認を求める等を選択する
  →場合によって[信頼済みサイト]/ [制限サイト]のそれぞれのゾーンごとに、Web サイトの信頼度に応じて、URL を[追加]/[削除]する

② ポップアップウィンドウを制限する

- Internet Explorer 6 上で

  [ツール]→[インターネットオプション]→[プライバシー]→[ポップアップ ブロック]
  →[ポップアップをブロックする]にチェック

  例外的にポップアップウィンドウを許可する場合は、右にある[設定]ボタンより
  [例外]→[許可する Web サイトのアドレス]にアドレスを追加する

* 「ゾーン」とはこの場合セキュリティゾーンとも呼ばれ、Internet Explorer では様々な Web サイトを登録することで、適切なセキュリティレベルを適用することができます。[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]の 4 ゾーンがあり、特に設定しない限りインターネットゾーンが適用されます。

③　SSL 2.0 を無効化する

- Internet Explorer 6 上で

  [ツール]→[インターネットオプション]→[詳細設定]→[セキュリティ]
  →[SSL 2.0 を使用する]のチェックをはずす

④　アドオンを有効/無効化する

- Internet Explorer 6 上で

  [ツール]→[インターネットオプション]→[プログラム]→[アドオンの管理]
  →[現在 Internet Explorer で読み込まれているアドオン]
  →有効化/無効化したいアドオンを選択し、[設定]より有効/無効を選択する

2. Internet Explorer 7 (IE7)

※ 本文では Windows Vista SP1 + IE7 SP1 での利用を前提としています。
公式 Web ページ:
http://www.microsoft.com/japan/windows/products/winfamily/ie/default.mspx

IE7 は Windows Vista に標準搭載されており、Windows XP でも Windows Update 等で別途インストールすることで利用できます。
よりセキュアにするための設定には次のようなものがあります。

① スクリプト等の実行を制限する

- Internet Explorer 7 上で

[ツール]→[インターネットオプション]→[セキュリティ]
→[セキュリティ設定を表示または変更するゾーンを選択して下さい。]
→[インターネット] / [ローカルイントラネット]/ [信頼済みサイト]/ [制限付きサイト]を選択
→[既定のレベル]を選択する、もしくは[レベルのカスタマイズ]で各種スクリプトごとにゾーン
ごとの信頼度に応じて有効/無効/確認を求める等を選択する
→場合によって[信頼済みサイト]/ [制限サイト]のそれぞれのゾーンごとに、Web サイト信頼度に応じて、URL を[追加]/[削除]する

② ポップアップウィンドウを制限する

- Internet Explorer 7 上で

[ツール]→[ポップアップ ブロック]→[ポップアップ ブロックを有効にする]を選択

例外的にポップアップウィンドウを許可する場合は、[ポップアップ ブロックの設定]より
[許可する Web サイトのアドレス]にアドレスを追加する

③ アドオンを有効/無効化する

- Internet Explorer 7 上で

[ツール]→[アドオンの管理]→[アドオンを有効または無効にする]
→有効化/無効化したいアドオンを選択し、[設定]より有効/無効を選択する

④　フィッシング詐欺検出機能を有効化する

- Internet Explorer 7 上で

  [ツール]→[フィッシング詐欺検出機能]→[自動的な Web サイトの確認を有効にする]を選択

⑤　プライバシー情報の消去

- Internet Explorer 7 上で

  [ツール]→[インターネットオプション]→[閲覧の履歴]
  →[削除]をクリック
  →[すべて削除]もしくは[インターネット一時ファイル]、[Cookie]、[履歴]、[フォーム データ]、[パスワード]の中からプライバシー情報を消去したいものを選んでクリック

3. Firefox 2.0

※ 本文では Windows XP SP3 + Firefox 2.0.0.17 での利用を前提としています。
公式 Web ページ: http://mozilla.jp/firefox/all-older

Firefox 2.0 は Mozilla Foundation がリリースしている Web ブラウザで、Windows シリーズや Mac OS X、Linux 等の多くの OS でリリースされています。多くの開発者により作成された、様々な機能を持つアドオンが提供されており、ユーザが任意に追加することが可能です。

なお、すでに後継となる Firefox 3.0 がリリースされているため、2008 年 12 月中旬をもってセキュリティ修正を含めた全ての更新が停止する予定となっています。

① スクリプト等の実行を制限する

- Firefox 2.0 上で

  [ツール]→[オプション]→[コンテンツ]
  →[JavaScript を有効にする]のチェックボックスを外す
  →[Java を有効にする]のチェックボックスを外す

  しかしこの場合一切実行できなくなるため、一部のサイトでは有効にしたい、という場合は拡張機能の一つ「NoScript」が便利です。

- NoScript: https://addons.mozilla.org/ja/firefox/addon/722

  この拡張機能は JavaScript や Java のみではなく、Adobe Flash Player などのプラグインの制御も行えます。スクリプト等を実行したいサイトでは、設定することで一時的に、もしくは恒久的に実行を許可することができます。なお安全に利用することを考慮し、通常は原則スクリプト等の実行は無効にした上で、実行する必要があるサイトでのみ一時的に許可することが望ましいでしょう。

② ポップアップウィンドウを制限する

- Firefox 2.0 上で

  [ツール]→[オプション]→[コンテンツ]
  →[ポップアップウィンドウをブロックする]にチェック

  例外的にポップアップウィンドウを許可する場合は、右にある[許可サイト]ボタンよりサイトのアドレスを入力し、[許可]ボタンを押します。

③　拡張機能を有効/無効化する

- Firefox 2.0 上で

  [ツール]→[アドオン]→[拡張機能]
  →有効化/無効化したい拡張機能を選択し、[有効]/[無効]ボタンを押す

④　拡張機能やテーマの更新を確認する

拡張機能やテーマを導入していくと、どのアドオンが更新されたかの確認に手間がかかるようになります。セキュリティ上の問題が修正される場合もあり、更新されたアドオンを自動的に確認できることが望ましいです。

この確認を補助する手段として Firefox 2.0 では標準で更新確認のための機能を備えています。

- Firefox 2.0 上で

  [ツール]→[アドオン]→[拡張機能]→[更新を確認]ボタンを押す
  [ツール]→[アドオン]→[テーマ]→[更新を確認]ボタンを押す

  また拡張機能でも更新の確認を補助するものとして、「Update Notifier」があります。

- Update Notifier: https://addons.mozilla.org/ja/firefox/addon/2098

  この拡張機能は Firefox 2.0 にインストールされているアドオンをチェックし、更新されているものがあればアラートをあげてユーザに対応を促します。これによりアドオンの更新に気づかず対応を忘れてしまい、脆弱なまま放置されてしまう可能性が少なくなります。

⑤　プライバシー情報の消去

- Firefox 2.0 上で

  [ツール]→[オプション]→[プライバシー]→[プライバシー情報]
  →[Firefox の終了時にプライバシー情報を消去する]にチェック
  →[設定]から細かい設定が可能

4. Firefox 3.0

※ 本文では Windows XP SP3 + Firefox 3.0.3 での利用を前提としています。
公式 Web ページ: http://mozilla.jp/firefox/

Firefox 3.0 は Mozilla Foundation がリリースしている Web ブラウザで、Windows シリーズや Mac OS X、Linux 等の多くの OS でリリースされています。多くの開発者により作成された、様々な機能を持つアドオンが提供されており、ユーザが任意に追加することが可能です。

① スクリプト等の実行を制限する

- Firefox 3.0 上で

  [ツール]→[オプション]→[コンテンツ]
  →[JavaScript を有効にする]のチェックボックスを外す
  →[Java を有効にする]のチェックボックスを外す

  しかしこの場合一切実行できなくなるため、一部のサイトでは有効にしたい、という場合は拡張機能の一つ「NoScript」が便利です。

- NoScript: https://addons.mozilla.org/ja/firefox/addon/722

  この拡張機能は JavaScript や Java のみではなく、Adobe Flash Player などのプラグインの制御も行えます。スクリプト等を実行したいサイトでは、設定することで一時的に、もしくは恒久的に実行を許可することができます。なお安全に利用することを考慮し、通常は原則スクリプト等の実行は無効にした上で、実行する必要があるサイトでのみ一時的に許可することが望ましいでしょう。

② ポップアップウィンドウを制限する

- Firefox 3.0 上で

  [ツール]→[オプション]→[コンテンツ]
  →[ポップアップウィンドウをブロックする]にチェック

  例外的にポップアップウィンドウを許可する場合は、右にある[許可サイト]ボタンよりサイトのアドレスを入力し、[許可]ボタンを押します。

③　拡張機能を有効/無効化する

- Firefox 3.0 上で

  [ツール]→[アドオン]→[拡張機能]
  →有効化/無効化したい拡張機能を選択し、[有効]/[無効]ボタンを押す

④　拡張機能やテーマの更新を確認する

拡張機能やテーマを導入していくと、どのアドオンが更新されたかの確認に手間がかかるようになります。セキュリティ上の問題が修正される場合もあり、更新されたアドオンを自動的に確認できることが望ましいです。

この確認を補助する手段として Firefox 3.0 では標準で更新確認のための機能を備えています。

- Firefox 3.0 上で

  [ツール]→[アドオン]→[拡張機能]→[更新を確認]ボタンを押す
  [ツール]→[アドオン]→[テーマ]→[更新を確認]ボタンを押す

  また拡張機能でも更新の確認を補助するものとして、「Update Notifier」があります。

- Update Notifier: https://addons.mozilla.org/ja/firefox/addon/2098

  この拡張機能は Firefox 3.0 にインストールされているアドオンをチェックし、更新されているものがあればアラートをあげてユーザに対応を促します。これによりアドオンの更新に気づかず対応を忘れてしまい、脆弱なまま放置されてしまう可能性が少なくなります。

⑤　プラグインを有効/無効化する・プラグインのバージョンを確認する

Firefox 3.0 では新たにプラグインに関する管理をアドオンから行うことができるようになりました。プラグインの有効/無効化およびバージョンの確認を行うことができます。しかし、拡張機能やテーマとは異なり、更新の確認やアップデートは行うことができませんので、注意して下さい。

- Firefox 3.0 上で

  [ツール]→[アドオン]→[プラグイン]
  →有効化/無効化したいプラグインを選択し、[有効]/[無効]ボタンを押す
  →プラグイン名の下に書かれているバージョンを確認する(書かれていないものもあります)

⑥　プライバシー情報の消去

- Firefox 3.0 上で

  [ツール]→[オプション]→[プライバシー]→[プライバシー情報]
  →[Firefox の終了時にプライバシー情報を消去する]にチェック
  →[設定]から細かい設定が可能

5. Safari 3

※ 本文では Mac OS X 10.5 + Safari 3.1.2 での利用を前提としています。
公式 Web ページ: http://www.apple.com/jp/macosx/features/safari.html

Safari は Apple がリリースしている Web ブラウザで、Mac OS X シリーズには標準搭載されています。Windows OS でも別途ダウンロード等で入手し、インストールすることで利用可能になります。

① スクリプト等の実行を制限する

- Safari 3 上で

  [Safari]→[環境設定]→[セキュリティ]
  →[JavaScript を有効にする]のチェックボックスを外す
  →[Java を有効にする]のチェックボックスを外す

  しかしこの場合一切実行できなくなるため、利用の際には注意が必要です。

② ポップアップウィンドウを制限する

- Safari 3 上で

  [Safari]→[ポップアップウィンドウを開かない]にチェック

③ プラグインを有効/無効化する

- Safari 3 上で

  [Safari]→[環境設定]→[セキュリティ]
  →[プラグインを有効にする]のチェックボックスで有効/無効化する

VI. Web ブラウザの操作上での注意事項

Web ブラウザを使用して Web を閲覧する際に注意すべき事項のうち、ソフトウェアの更新や設定等で防ぐことのできるものについては前章までに解説しました。しかし、安全な Web アクセスのためには、それだけでは十分ではありません。

例えば、正規の組織やサービスのページのように見せかけた不正なページが存在します。このようなページは攻撃者が仕掛けた悪意のあるページであることが多く、金融機関や特定のサービスのアカウントやパスワードを盗み取る目的(フィッシング *)で設置されています。他にもクロスサイトスクリプティング †、クロスサイトリクエストフォージェリ ‡といった攻撃者が仕掛けた罠が、不正な Web ページには設置されています。

こうした落とし穴を作りこんで待ち受けていて、ユーザが操作を行って初めて被害が発生するタイプの攻撃を「受動型攻撃」と呼びます。

受動型攻撃の被害を避けるためには悪意のある Web サイトを訪れないことに尽きますが、攻撃者は様々な手段を用いて巧みに利用者を悪意のある Web サイトに誘導します。

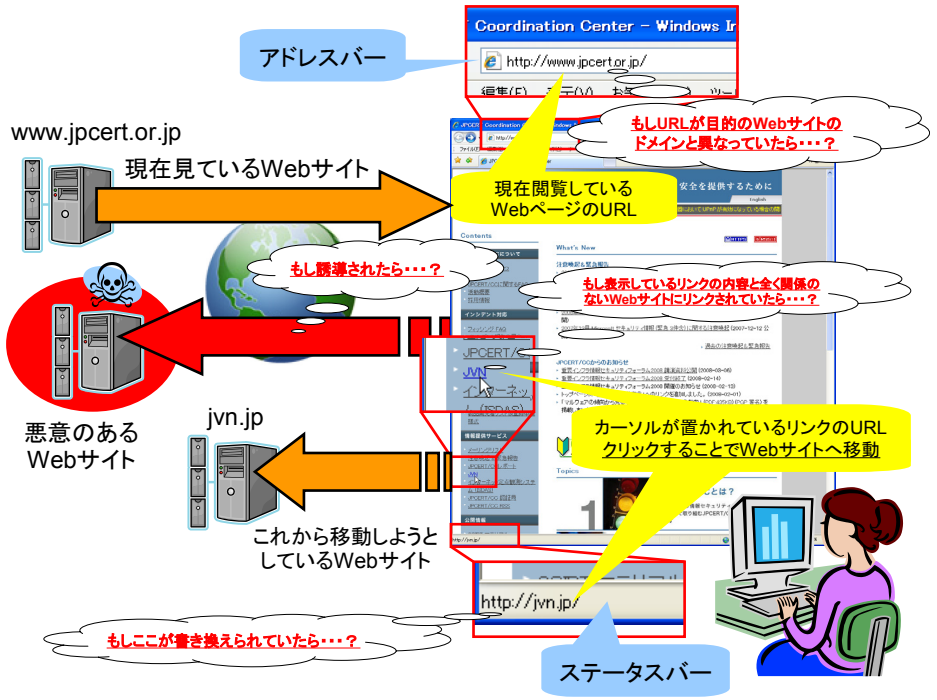

図 5 Web ブラウザ利用時に注意するポイント

---

* 銀行やオークションなどのオンラインサービスを装った Web サイトへ誘導し、ユーザの口座番号、暗証番号、個人情報などの重要な情報を盗み取ろうとする行為。

† 脆弱な Web サイトを介してユーザのブラウザ上で悪意のあるスクリプトを実行させる攻撃。結果として個人情報が漏洩したり、意図しない商取引が行われたりする等の被害が発生する。

‡ ログイン状態が保持された Web サイトに対し、外部のサイトを利用した悪意のあるリクエストがブラウザ経由で送り込まれる攻撃。結果としてユーザの意図しない処理、例えばパスワードの不正変更や意図しない商取引などが行われてしまう。

1. 悪意のある Web サイトへと導く手口

悪意のある Web サイトに利用者をアクセスさせる手口としては、例えば以下のようなものがあります。

① 迷惑メール・フィッシングメール

一般的に迷惑メールとは、受信する側の同意を得ずに広告などを送りつけるメールを指します。その一部は、悪意のある Web サイトへ誘導する目的で発信されています。例えば、「今だけ 9 割引！」とか、「あなたにだけお知らせするお得な情報！」、あるいは興味を引きそうな架空のニュースの見出し等、閲覧意欲をあおるようなキーワードとともに悪意のある Web ページへのリンクを記載し、誘導しようとします。特に、フィッシングメールの場合は金銭的な被害に結びつく可能性もあります。

② 掲示板・ブログ等の書込み

掲示板は多くの場合、不特定多数のユーザによって書込みが行われ、様々な情報が交錯しています。多様な情報の中には、有用なページへのリンクのように見せかけて悪意のある Web サイトへのリンクを載せたものが混在している可能性もあります。

掲示板と同様にブログのコメント欄やトラックバックなどでも悪意のある Web サイトへのリンクが書き込まれている場合があります。

③ リンクの偽装

悪意のあるページへのリンクを問題のないページへのリンクのように見せかけることをリンクの偽装と言います。巧妙に偽装がなされている場合には、多くのユーザが悪意あるページであることに気づくことなくリンクをクリックしてしまいます。

④ サーチエンジンの利用

サーチエンジンの検索結果は一般的に、キーワードとのマッチングの程度が高いページほど、また、多くのユーザが訪れたページほど最初に表示されます。

このためユーザは最初の部分に出てくるページについては深く考えずに訪れる傾向があります。攻撃者はユーザのこのような行動パターンを想定し、関連するキーワードをページ中に多用するなどの手法を使って、本来アクセスすべきページよりも悪意のあるページが検索結果の上位に来るように細工をして、多くのユーザに有用なサイトであると誤認させてアクセスさせます。

サーチエンジンを利用する際は、検索結果の最初に来ていたとしても悪意のある Web ページである可能性があることを念頭に置く必要があります。

⑤　URL の打ち間違い等を狙った、正規のドメインに似せたドメイン

Web ブラウザのアドレスバーに直接 URL を入力して、Web ページへアクセスする際に、ユーザが犯す URL の打ち間違いを狙って、攻撃者が正規のドメインに似せたドメインを取得し、そこに悪意のある Web ページを作成していることがあります。この攻撃の多くは有名な組織のドメインを狙います。例えば、北京オリンピックの公式サイトに似たドメインが取得され、フィッシング詐欺サイトが設けられた事例がありました。この詐欺サイトではオリンピックの観戦チケットを安く売るように見せかけ、ユーザのクレジットカード情報を騙し取っていました。

2. 誘導されないための対策

悪意のある Web サイトであることを事前に察知しアクセスしないようにするためには、まず閲覧している、および閲覧しようとしている Web サイトおよび Web コンテンツをどのような人が作成し確認したのかを正しく見極める必要があります。前節で取り上げた項目に即して、それぞれの対策を考えてみましょう。

① 迷惑メール・フィッシングメール

フィッシングメールの場合、本来訪問すべきなのは金融機関などが運用する個人情報等を取り扱う Web サイトです。そうした重要なWebサイトへのアクセスにあたっては、**当該組織から送られてきた書類などに記載されている URL を手動で入力した上であらかじめブックマークしておき、アクセスする際はブックマークのみを利用**し、**フィッシングメールの可能性を否定できないメール中のリンクをクリックしない**ようにして下さい。

また、迷惑メール・フィッシングメールをインターネットプロバイダ等のサービスやメールソフトの機能、あるいは専用のソフトウェア等を用いて積極的に削除するよう努めましょう。

さらに、偶発的なクリックによる被害を避けるため、可能ならばメールソフトの設定で HTML メールを標準では開かないようにした方が良いでしょう。

② 掲示板・ブログ等の書込み

不特定多数によって書き込みが行われる掲示板・ブログ等の Web サイトでは、極力リンクをクリックしない方がよいでしょう。どうしてもリンク先にアクセスしたい場合は、**リンクをクリックする前に、カーソルをリンクの上に移動し、ステータスバーなどでアクセスしようとしている URL を確認**し、**信頼できるドメインかどうかを十分に吟味した上でクリック**して下さい。

③ リンクの偽装

表示と参照先URLが異なる、単純な HTML 上の表示の偽装への対策は、上記②の対策で紹介したステータスバーなどによる確認が良いでしょう。しかし、一部 Web サイトでは JavaScript 等によってステータスバーに表示される URL を置き換えている場合があります。これを防ぐには**スクリプトの実行を一旦制限した上で URL を確認する**必要があります。

④ サーチエンジンの利用

最近では、サーチエンジンの検索結果に、リンク先の URL や内容の一部が表示されることが多く、これらの情報を参考に危険なページである可能性を吟味しましょう。また、**日常的に訪れる Web サイトは、サーチエンジンを利用したアクセスを避け、ブックマークを利用する**ようにしましょう。

⑤　URL の打ち間違い等を狙った、正規のドメインに似せたドメイン

URL を入力する際は、特にトップレベルドメイン（.jp, .com, .org, .net 等）や属性ドメイン（.co.jp, .or.jp, .go.jp 等）にも注意を払い、曖昧な記憶に頼らないようにしましょう。また、発音が似た別の綴りや、同じ文字が多く並ぶドメインの打ち間違いにも注意しましょう。

また、最近では日本語もドメインに利用できるようになり、半角と全角との打ち間違いによっても、別のサイトにアクセスする可能性があることにも注意しましょう。

3. 誘導されてしまった際の被害を抑える対策

うっかり悪意のある Web ページを閲覧してしまった場合に備えて、以下のような対策を行うことで被害を最小限に抑えられる可能性があります。

① 認証を要求されるサイトを利用している間はログアウトするまで他のサイトにアクセスしない

クロスサイトリクエストフォージェリが仕掛けられたページを閲覧した場合、攻撃者が標的としている Web ページに対し偽造(forgery)リクエストが送られます。この時、標的となる Web ページにログインした状態にあると、偽造リクエストが処理されてしまいます。このような攻撃を防ぐために、**認証を要求されるサイトを利用している間は他のサイトへのアクセスを行わず、ログアウトしてから他のサイトへアクセス**するとよいでしょう。さらに、可能であれば一旦 Web ブラウザ を終了してから、再起動して他のサイトへアクセスしましょう。

② 信頼できる Web サイトであると確認できるまではスクリプト等を停止しておく

どのような Web サイトであっても信頼できる Web サイトであると確認できるまではスクリプト等を動作させないほうがよいでしょう。スクリプト等を停止しておくことで悪意のあるコードや偽造リクエストの実行を防げるため効果があります。

③ SSL サーバ証明書が正規の証明書であるかどうかを確認する

HTTPS による暗号化通信が行われている Web ページでは、SSL サーバ証明書に問題がないことを確認することが重要です。Web ブラウザは証明書の検証を自動で行い、失敗した場合には警告を表示します。警告が表示された場合には、速やかにその Web ページの閲覧を中止してください。

また、フィッシングサイトなどでは形式的には正当とされる証明書を利用していることがあるため、アドレスバーに表示された URL が意図した正規の URL であることを確認してください。

VII.その他のソフトウェアや機能

Web ブラウザを利用して Web ページを閲覧する際に注意すべき事項・設定について説明してきましたが、今までに説明してきたもの以外にも安全に Web ページを閲覧する上で併用するとよいソフトウェアや機能があります。

1. URL フィルタリング

URL フィルタリングを利用すれば、ページの内容に応じたカテゴリ分けがなされ、ユーザは自分が望むカテゴリのみにアクセスを限定し、望まないカテゴリのページをフィルタリングすることができます。

組織で導入する場合には、管理者が業務に関係のないカテゴリをフィルタすることで、私用利用を防ぐことができるメリットもあります。またユーザが不用意に悪意のある Web サイトを閲覧してしまうことや、Web メール等による外部への情報の持ち出しを防ぐ効果も期待できます。

ただし、フィルタリングのカテゴリ分けの判断は提供ベンダによるため、フィルタされることを望んでいたページがフィルタされないことや、その逆の場合もあります。また新規に作成された Web ページの場合はそもそも提供ベンダのデータベースに登録されていないため、フィルタリングされないこともあります。

多くの製品にはホワイトリスト/ブラックリスト機能が標準で備わっており、これを利用すれば、フィルタリング対象をカスタマイズしておくことも可能です。

URL フィルタリング製品としては、アプライアンスボックスやサーバ上で動作するタイプ、クライアント上で稼動するアンチウイルスソフトに同梱されたタイプなどがあります。

また URL フィルタリングに類似した製品として、Web ページを解析した上で、ダウンロード用のリンク数やスクリプトの有無をチェックし、そのスコアに応じて Web ページの危険度の評価値を表示するものもあります。このカテゴリで無償で利用できるものに McAfee 社の SiteAdvisor があります。

- McAfee SiteAdvisor：http://www.siteadvisor.com/

SiteAdvisor は検索エンジンで検索した結果に基づいて初めて訪れる Web ページなどで危険な Web ページかどうかの評価値を得て、判断の参考とできるため、一定の効果があります。

2008 年 10 月現在、IE 用のプラグインと Firefox 用の拡張機能が提供されています。

2. 個人情報(プライバシー)保護

フィッシングやクロスサイトスクリプティングなど、様々な手法で攻撃者側はユーザの個人情報を狙っています。そのため、あらかじめ登録された個人情報(クレジットカード番号やアカウント、パスワードなど)が Web ブラウザ等を経由して外部に送信されようとした時にアラートをあげ、送信を止める機能を個人情報保護機能と呼びます。

個人情報保護機能は最近ではアンチウイルスソフトに同梱されることも多くなりましたが、個人情報保護機能のみを単体で提供するソフトウェアもあります。

VIII. 安全に利用するために

本文書では Web ブラウザに関して、あらかじめ行っておくべき設定や Web ページを閲覧する際に注意すべき事項や操作法について記載してきました。

その中で OS や Web ブラウザを最新の状態に保つことの重要性を指摘しました。新たなアップデートが出た場合には、アップデートを適用するだけではなく、一歩踏み込んでどのような脆弱性があり修正されたのかを把握しておくと、今後の PC の管理や万が一攻撃の被害に遭ってしまった場合に役立つでしょう。

しかし、利用している OS や Web ブラウザについてのアップデート情報は一般的に個々の製品毎に分散しており、場合によってはすぐに見つけることが難しいかもしれません。

こういったユーザや管理者を手助けするための Web サイトの一つとして、JVN (Japan Vulnerability Notes) があります。

- JVN：https://jvn.jp/

OS や Web ブラウザ以外のソフトウェアに関する情報も掲載されているため、アドオンの情報を収集する際にも便利です。

またユーザ側の対策が進むのに対抗して、攻撃者は次々と新たな攻撃方法を考案して襲い掛かってきます。ユーザはそうした新たな攻撃の動向について情報を収集するとともに、必要に応じて新たな対策を導入しなければいけません。一般的にはユーザや組織が独力で完全な対処を行うことはすでに難しくなっています。

このような新たな攻撃方法に関する動向や注意喚起等の情報は JPCERT/CC の Web サイトを通じて得ることもできます。

- JPCERT/CC：https://www.jpcert.or.jp/

またメーリングリストや RSS を利用すれば最新の情報をいち早く受け取ることができます。ぜひ活用を検討して下さい。

Web を利用する際は、本文書で述べた基本的な注意事項に留意し、また JVN や JPCERT/CC 等の Web サイトを利用して集めた最新情報を組み合わせることで、危険を避けつつ Web を活用しましょう。

万が一それでも攻撃による被害に遭ってしまった場合は、あわてずに組織のシステム管理者に連絡をとりましょう。システム管理者の方は被害の状況に応じて、あるいは同類の被害の拡大を防ぐために、以下に掲げたような関係機関・組織に連絡することを検討しましょう。

- 各金融機関やサービスプロバイダ等の問い合わせ窓口
- 警察
  - **最寄りの警察署に届け出る**
  - **全国警察サイバー犯罪相談窓口等一覧** ：http://www.npa.go.jp/cyber/soudan.htm
- IPA (情報処理推進機構)
  - **セキュリティセンター ： 届出について** ：http://www.ipa.go.jp/security/todoke/
- JPCERT/CC
  - **インシデント報告の届出** ：https://www.jpcert.or.jp/form/

IX. 参考資料

- Cyber Security Tips
http://www.us-cert.gov/cas/tips/

- 安全な Web サイト利用の鉄則
http://www.rcis.aist.go.jp/special/websafety2007/

- SPREAD セキュリティ対策推進協議会
http://www.spread-j.org/index.html

- JPCERT/CC： 注意喚起 & 緊急報告
https://www.jpcert.or.jp/at/

- JPCERT/CC： フィッシングに関する FAQ
https://www.jpcert.or.jp/ir/faq.html

- 情報処理推進機構 ： セキュリティセンター
http://www.ipa.go.jp/security/

- Japan Vulnerability Notes
https://jvn.jp/

- マイクロソフト セキュリティ ホーム
http://www.microsoft.com/japan/security/default.mspx

- Mozilla Japan： セキュリティセンター
http://www.mozilla-japan.org/security/

- アップル - サポート – Safari
http://www.apple.com/jp/support/safari/

※ 文中の会社名、製品名は各社の登録商標または商標です。