パソコンのセキュリティについて

１．はじめに

インターネットは、私たちの社会生活を便利にしてくれる、欠かせないものになっています。しかし、世界中のコンピュータが接続されたネットワークであるため、ウイルスの感染やコンピュータへの不正侵入などの危険にさらされています。例えば、ウイルスに感染すると、コンピュータの中にある家族の写真や、友人との電子メールが流出するなど、自分だけでなく、他の人にも被害が及ぶことがあります。

情報セキュリティ対策については、インターネットサービスを提供する会社やウイルス対策会社などから、様々なサービスやソフトウェアなどが提供されています。しかし、より重要なのは、利用者一人一人が情報セキュリティ対策の必要性を十分認識し、対応することです。

情報セキュリティ対策には様々な方法がありますが、まずは、「ソフトウェアの更新」、「ウイルス対策サービス・ソフトの導入」、「パーソナルファイアウォールの利用」の３つを基本とし、対策をしっかり行っていただきますようお願いします。

２．OSのアップデートの実施（Windows）

２．１．Windows Updateについて

Windows上での最も基本的なセキュリティ対策は、Windowsを最新の状態に保つことです。アップデートにより不具合の解消も行われます。初期状態では、更新プログラムを自動的にインストールするよう設定されています。

Windows Vista以降では標準で自動的に更新されるように設定されていますが、Windows XPでは、インストールできるプログラムがあるとき、以下のような通知が表示されます。これに従い、表示をクリックしてインストールを行いましょう。

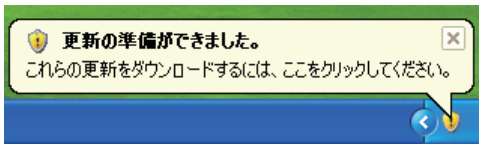

図１．Windows Updateの更新通知（Windows XPでの例）

また、以下のようにWindows Updateを呼び出すことで、アップデートに関する設定や、手動でのアップデートなどが行えます。

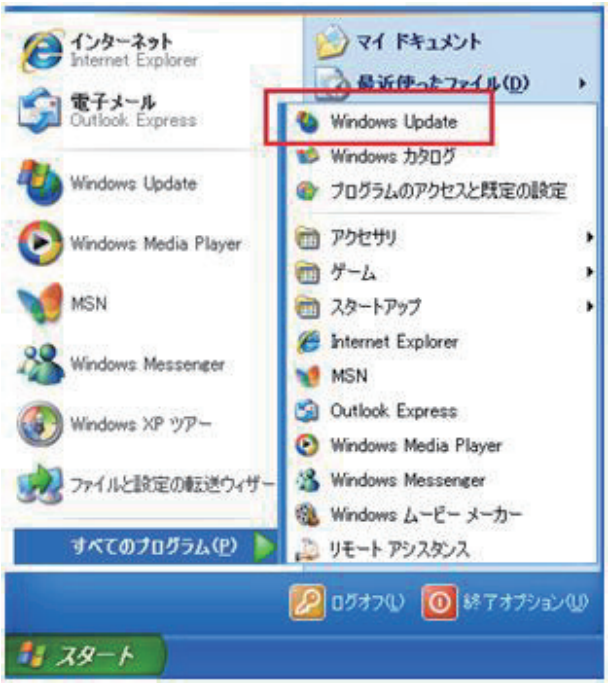

図 2. Windows Updateの呼び出し（Windows XP での例）

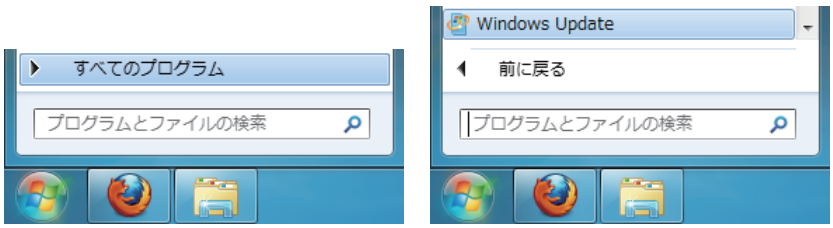

図 3. Windows Updateの呼び出し（Windows 7 での例）

２．２．Windowsのサポート終了時期

サポートが終了すると、セキュリティプログラムが更新されなくなります。サポートの終了したOSを使用することは、セキュリティ上好ましくありません。新しいOSにアップグレードすることをおすすめします。各Windowsのサポート終了時期は以下の通りです。

- Windows 2000 ： 2010 年 7 月 13 日
- Windows XP ： 2014 年 4 月 8 日
- Windows Vista ： 2017 年 4 月 11 日
- Windows 7 ： 2020 年 1 月 14 日

３．ウイルス対策ソフトの導入

３．１．定義ファイルの更新について

ウイルス対策ソフトの導入は、安全にコンピュータを利用するためには必須といえます。常に新しい定義ファイルへと更新することで、ウイルスに感染しづらくなります。また、ウイルスを検出・駆除するため、定期的にスキャンを行って下さい。

３．２．各種ウイルス対策ソフト

代表的なウイルス対策ソフトを挙げます。

- ノートン インターネットセキュリティ
- ウイルスバスター
- マカフィー・インターネットセキュリティ
- ウイルスセキュリティ ZERO（Windows のサポート終了時期までアップデート更新が無料で行えます。サポート終了時期は 2.2 を参照下さい）

４．ウェブブラウザのセキュリティ

４．１．パスワードの管理について

インターネットに接続しているユーザのほとんどは、ウェブブラウザを利用してウェブサイトを閲覧したことがあるかと思います。近年のウェブブラウザはより多機能で便利なものとなっていますが、利用にはユーザのセキュリティ意識が必要であることに変わりありません。

パスワードの管理は、インターネット上のサービスを使用する上で避けては通れません。パスワードは通常、他人に推測されにくく、英数字からなる、指定された以上の文字数のものである必要があります。また、セキュリティの観点から、複数のウェブサイトで同じパスワードを使用することは推奨されません。

とはいえ、ウェブサイトごとに異なる英数字を全て記憶することは現実的ではないので、以下にパスワード管理のための方法をいくつか紹介したいと思います。

４．１．１．マスターパスワードの使用

マスターパスワードとは、キーボックスに鍵をかけるように、複数の ID とパスワードを保護するパスワードのことです。主要なウェブブラウザのうち、Firefox では標準機能として利用できます。

Firefox では、以下のようにオプションのセキュリティタブからマスターパスワードを利用することができます。ここで設定するパスワードは必ず、自分にとって憶えやすく、他人には推測されにくいものにしてください。

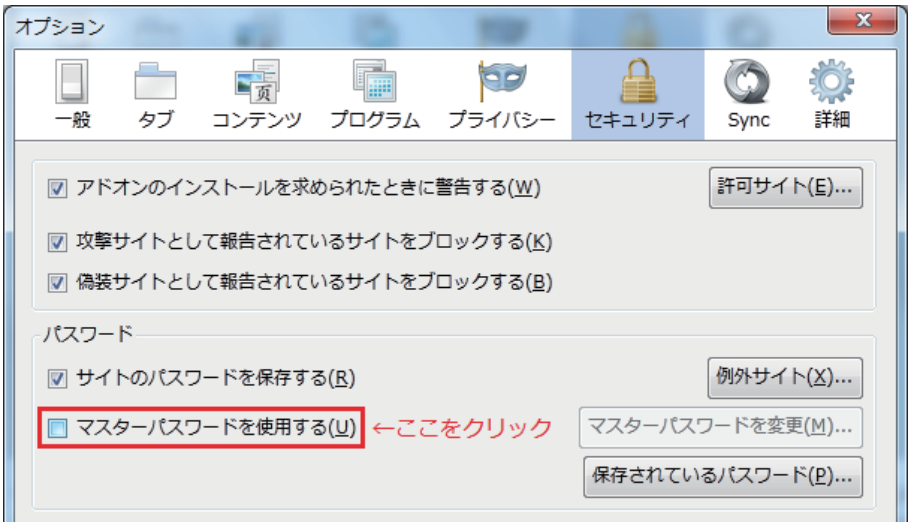

図 4. マスターパスワードの利用方法

4.1.2. パスワード管理ツールの使用

パスワード管理ツールは、マスターパスワードのようにIDとパスワードの一括管理が行えるだけでなく、パスワードの暗号化や自動生成などの機能が備わっているものもあります。有償・無償問わず様々なツールがあるので、導入を検討されることをおすすめします。

4.1.3. 重要度別のパスワード管理

重要な個人情報を登録しておらず、万が一パスワードが流出しても問題のないウェブサービスを利用する場合、新たにパスワードを用意せずに、他の同様なウェブサービスで使用しているパスワードと重複利用してもかまいません。パスワードは重要度に応じて適宜使い分けましょう。

4.2. セキュリティの設定について

アドオン（プラグイン）の導入時またはウェブサイト閲覧時に、ウェブブラウザがユーザの許可を求める場合がありますが、これら全てに無条件に許可を与えることは危険です。信頼できないソフトウェアや怪しいウェブサイトには不必要に許可を与えないで下さい。

4.3. ウェブサイトのセキュリティ表示

ウェブサイトには、セキュリティで保護された接続（SSL）を使用しているものがあります。SSLは、例えばショッピングサイトで入力するクレジットカード番号等の個人情報を暗号化し、安全に送受信するために使われています。SSLを使用しているかどうかを確認するには、ウェブブラウザのアドレスバーをご覧下さい。アドレスの先頭が "https://" であるウェブサイトは、SSLを使用しています。

また、SSLを使用しているサイトが正規のものであるかどうかは、SSLサーバ証明書を確認して下さい。以下にFirefox 8での例を示します。

図 5. SSL サーバ証明書の確認（日本ベリサイン株式会社 Web サイト）

4．4．各種ウェブブラウザ

以下に代表的なウェブブラウザを挙げます。

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera

※ウェブサイトによっては、古いウェブブラウザのサポートを終了していることがあります。代わりに各ウェブブラウザの最新バージョンをご使用下さい。

5．メール利用のセキュリティ

5．1．スパムメール

インターネットで様々なサービスへの登録や掲示板、ホームページでメールアドレスを公開すると、必ずと言っていいほど迷惑なメールや広告が送られてきます。一般にスパム（spam）と呼ばれるこのインターネット版ダイレクトメールは一方的に送られてくるため、防ぐのが困難なのが現状です。以下に代表的なスパムメール対策を挙げます。

- スパムメールに返事をしない
- HTML 形式のスパムメールは開かない
- インターネットで公開するメールアドレスにはフリーメールを使用する
- フィルターを使用する

5．2．添付ファイル

メールの添付ファイルは、つい開いてしまいがちです。しかし、ウイルスが潜んでいることがありますので注意が必要です。以下はメールの添付ファイルの取扱いに関する注意事項です。

- 見知らぬ相手先から届いた添付ファイル付きのメールは無条件に削除する
- 添付ファイルの見た目（拡張子）に惑わされない
- 知り合いから届いたメールであっても、添付ファイルの開封には注意する
- メールの本文でまかなえるようなものをテキスト形式等のファイルで添付しない
- 各メーラー特有の添付ファイルの取扱いに注意する

6．ファイアウォールの利用

6．1．ファイアウォールの概要

ファイアウォールは、「信頼できるネットワーク（イントラネット）」と「信頼できないネットワーク（インターネット）」の２つのネットワーク間のアクセスを制御するために使われます。ファイアウォールを導入すれば、外部の攻撃から社内ネットワークを守り、セキュリティを大幅に高めることができます。ファイアウォールには、主に以下のような機能が備えられています。

- アクセス制限
- アドレス変換
- ユーザ認証
- ログ収集／解析
- コンテンツフィルタリング
- ルーティング

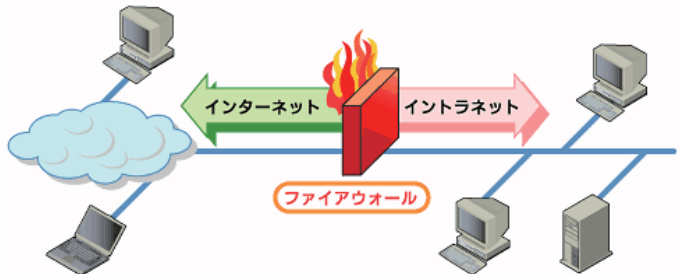

図 6.　もっともシンプルなファイアウォールの設置例

6.2. ファイアウォールの種類

ファイアウォールは、設置場所によって大まかに2つに分類できます。

- ゲートウェイ型（ルータに設置）
- ノード型（個々のコンピュータに設置）

ゲートウェイ型は、外部（WAN）と内部（LAN）の間に設置するため、外部からの不正アクセスをまとめてブロックできますが、内部からの不正アクセスには対応できません。一方、ノード型は、コンピュータごとに設定できるので柔軟性があり、他のネットワーク利用時にも対応できますが、コンピュータへ負荷がかかります。

ノード型のファイアウォールは、OSに標準で搭載されているものや、ウイルス対策ソフトの機能として提供されているものがあります。これらをまとめて「パーソナルファイアウォール」と呼びます。

6.3. パーソナルファイアウォールの利用

OSやウイルス対策ソフトごとに設定方法は異なりますが、まずはファイアウォールが有効になっているかどうかの確認を行って下さい。ファイアウォールが無効になっている場合は有効にして下さい。Windows XP, Vista, 7には、ファイアウォールが標準で搭載されています。

Windows XPの場合、［スタート］-［コントロールパネル］-［Windowsファイアウォール］の順にクリックして呼び出します。以下の図は、ファイアウォールが有効になっている場合の例です。

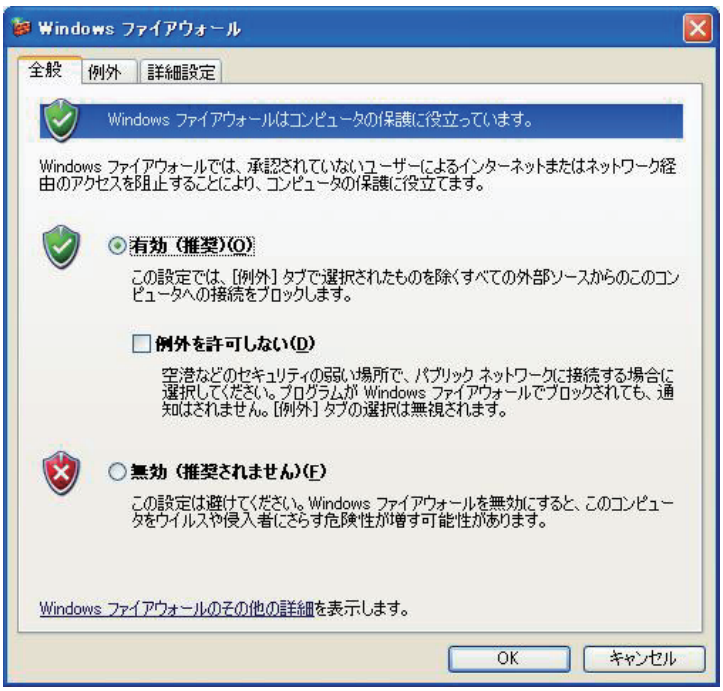

図 7. ファイアウォールの確認（Windows XP での例）

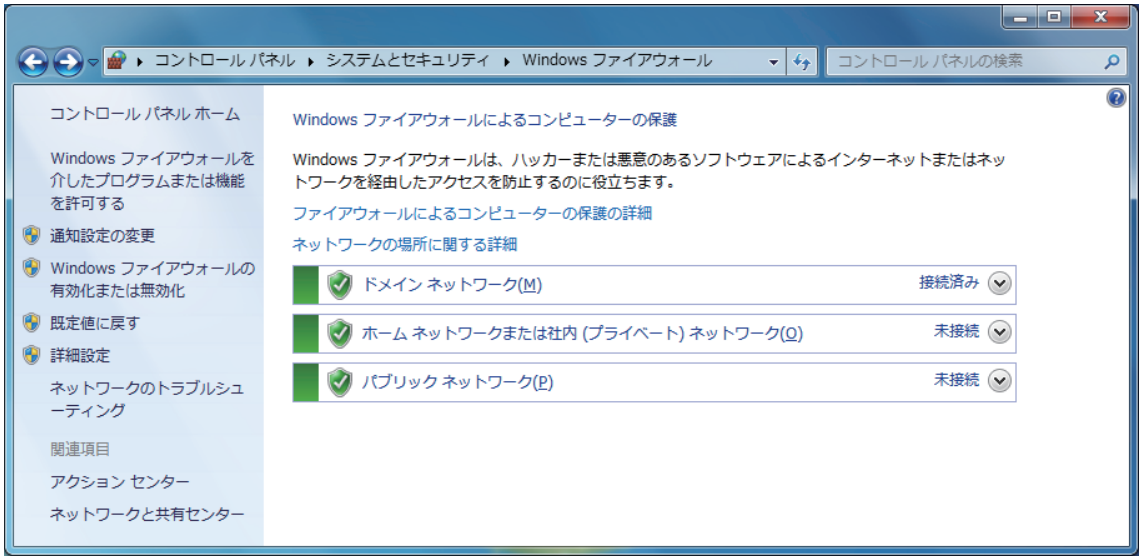

図 8. ファイアウォールの確認（Windows 7 での例）