IPA 対策のしおり シリーズ (4)

不正アクセス対策のしおり

大丈夫ですか、
あなたのパソコン？
（パソコン利用者向け）

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6版

不正アクセスとは･･･

不正アクセスとは、2012 年 5 月 1 日に改正施行された、不正アクセス禁止法(不正アクセス行為の禁止等に関する法律)(*1)に定義された不正アクセス行為および不正アクセスを助長する行為のことを言います。具体的には、以下に示す行為のことです。

- コンピュータのOSやアプリケーションあるいはハードウェアに存在するぜい弱性(セキュリティホール)(*2)を利用して、コンピュータのアクセス制御(*3)機能を迂回し、コンピュータ内に侵入する行為(侵入行為)
- 他の人に与えられた、利用者IDおよびパスワード(*4)を、その持ち主の許可を得ずに利用して、持ち主に提供されるべきサービスを受ける行為(『なりすまし』行為)
- 持ち主の許可を得ずに、その持ち主の利用者 ID およびパスワードを第三者に提供する行為

本しおりは、パソコンの利用者向けのものです。企業(組織)内のネットワークに対する不正アクセスの対策には十分ではない(あるいは不適切な場合もある)ことに、ご注意下さい。

例えば、こんな話･･･

・パスワードの落とし穴

A さんは、インターネットオークションの常連で、野球カードの売買を頻繁に行っていました。A さんは、オークションにログインするための利用者 ID およびパスワードを忘れないように、自分の名前をパスワードにしていました。

ある日、いつものようにオークションにログインしようとしたら、「パスワードが違います！」というメッセージが表示され、何度試してもログインできません。パスワードを変更した覚えはないので、管理会社に問い合わせると、「パスワードが変更されています。」と言われました。

安易なパスワードを設定していた結果、簡単に推測されてしまい、オークションのパスワードを盗まれてしまったのでした。

・常時接続の落とし穴

B さんは、CATV（ケーブルテレビ）を利用してインターネットを利用していました。接続時間に関わらず料金が一定のため、常時インターネットに接続したままでした。

B さんはセキュリティには無頓着で、セキュリティホール（ぜい弱性）を修正する作業（Microsoft Update 等）は一切行っていませんでした。

ある日、情報セキュリティ対策機関から「B さんのパソコンから某政府機関を攻撃しているので、直ちにアクセスを停止し、必要な対処をして下さい。」と連絡がありました。B さんは慌ててパソコンをインターネットから切断しました。

無防備な状態でインターネットに常時接続をしていた結果、いつの間にか侵入され、B さんのパソコンを踏み台にして攻撃に使用されていたのでした。

・無線 LAN の落とし穴

C さん一家は、家族で複数のパソコンを利用しています。家族が自分たちの部屋毎にパソコンを使いたいので、家中を LAN ケーブルでつながなくて済む無線 LAN を導入することにしました。無線 LAN の機器を、説明書もよく読まずに、つなげたらすぐに使えたので、そのまま利用していました。

何週間かして、オンラインゲームを利用していると、なんだかパソコンの反応が遅くなったように感じられ、アクセスもしていないのにハードディスクのアクセスランプが激しく点滅することも多くなりました。

ある日、クレジット会社から、家族の誰もが身に覚えのない請求書が届きました。調べてみると、オンラインショッピングで買い物があったようです。

後日、分かったことには、C さん一家では、家族でオンラインショッピングができるように、クレジットカードの番号を記録したファイルを、ファイル共有していたため、そのファイルがセキュリティ対策を施していない無線 LAN を通じて不正アクセスされ、なりすましでショッピングが行われていたことが判明しました。

このように、「安易なパスワードを設定していた」、「セキュリティホールを修正していなかった」、「アクセス制御があまかった」といった原因で、不正アクセスの被害を受ける危険性があります。これらは他人事ではなく、インターネットユーザであれば、誰にでも起こりうる事例です。これから紹介する最低限のセキュリティ対策を実施し、快適にインターネットをお使い下さい。

1. 修正プログラム(パッチ)を適用しよう（侵入対策）

Windows や Macintosh、Linux などの OS（Operating System）、Internet Explorer や Firefox などのブラウザ、その他あらゆるソフトウェアには、セキュリティ上の問題となる欠陥(ぜい弱性)が発見されることがあります。

このような**安全上の欠陥のことをセキュリティホール(ぜい弱性)**といいます。セキュリティホールが存在する OS やアプリケーションを使用していると、ウイルス感染や不正アクセスの侵入口となり、パソコン内のデータが削除されてしまったり、個人情報を盗み見られたりする危険性があります。

これらの危険を回避するためには、セキュリティホールを解消するための修正プログラム（パッチ）を適用するといった作業が重要になります。修正プログラムとは、ソフトウェアの開発元が提供するもので、欠陥を塞ぐためのプログラムのことです。

Windows 利用者は、Microsoft Update を定期的に実施するか、自動更新設定を行って下さい。Microsoft 社が提供している OS に用意されたパッチ、および Internet Explorer や Office 製品等に用意されたパッチが適用できます。

- **Microsoft Update**
  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。

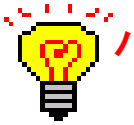
- **コンピュータの更新（マイクロソフト株式会社）**
  http://windows.microsoft.com/ja-jp/windows7/Updating-your-computer

2. たかがパスワード、されどパスワード（なりすまし対策）

利用者IDおよびパスワードの組み合わせは、情報システム(サービス)が個人（あなた）を特定するために用いるものです。利用者IDは、情報システムで利用者毎に一意に割り振られる場合がありますが、**パスワードはあなたが設定(変更)すべきものです**。利用者IDおよびパスワードが漏えいしたり、盗まれたりした場合、他人があなたになりすまして、情報システムにアクセスすることができてしまいます。

これにより、オンラインバンクにアクセスされ、預金を引き出されてしまったり、インターネットオークションにアクセスされ、高額な商品を落札されたりといった被害が発生してしまいます。

利用者 ID およびパスワードの組み合わせは、情報システムがあなたを特定するための唯一の情報であると考え、安易な設定をしない、他人に教えたりしない、定期的にパスワードを変更する、といった対策をとるようにしましょう。



パスワードの設定例：

(1) 大文字・小文字・数字・記号の組み合わせ
　　記号(!、#等)、数字、英字を適当に織り交ぜる

(2) 長いパスワード
　　最低 8 文字以上

(3) 推測しづらく自分が忘れないパスワード
　　無作為で意味を持たない文字列であること

パスワード盗難対策：

(1) 定期的にパスワードを変更する
(2) 紙に書き留めたまま放置しない（付箋は NG）
(3) パソコンに保存しない
(4) 人に教えない

3. インターネット接続時の注意（侵入対策）

家庭や出先でパソコンをインターネットにつなぐ場合は、その接続方法により、不正アクセス(侵入行為)を受け易い状態になる場合があります。

公衆回線(携帯電話の回線も含む電話回線)とモデムを利用した接続の場合、パソコンがインターネットと直接接続されることにより、インターネット側から不正アクセスを直接受ける可能性が高くなります。この場合は、後述するパソコン側で不正アクセスに対処するための設定やセキュリティ対策ソフトを利用されることをお勧めします。

ADSL 回線と ADSL モデムを利用した接続の場合、最近の ADSL モデムはルータ機能を内蔵している場合が多いため、このルータ機能により、インターネット側からの不正アクセスを直接受ける危険性は低くなっていますが、ルータ機能の設定を誤ると、やはり、インターネット側から不正アクセスを直接受ける可能性が高くなります。このような設定を意図的に行う場合は、後述するパソコン側で不正アクセスに対処するための設定やセキュリティ対策ソフトを利用されることをお勧めします。

CATV 回線とケーブルモデムを利用した接続や光ファイバー回線と VDSL モデムを利用した接続の場合、他の機器を介さないで、パソコンをインターネットに直接接続すると、インターネット側から不正アクセスを直接受ける可能性が高くなります。この場合は、ルータやファイアウォール機器の使用をお勧めします。ただし、使用する回線にあった機器でないと役に立ちませし、ルータやファイアウォール機器の設定を誤ると、やはり、インターネット側から不正アクセスを直接受ける可能性が高くなります。このような設定を意図的に行う場合は、後述するパソコン側で不正アクセスに対処するための設定やセキュリティ対策ソフトを利用されることをお勧めします。

公衆の無線 LAN ホットスポットや、ビジネスホテル等での LAN 接続等、不特定多数の利用者が同一 LAN 上に接続する可能性のある環境で、インターネットに接続する場合は、同一 LAN 上の他の利用者から不正アクセスを受ける可能性があります。このような環境では、後述するパソコン側で不正アクセスに対処するための設定やセキュリティ対策ソフトを利用されることをお勧めします。

4. 不正アクセス対策の設定

① ファイル共有設定を無効化する

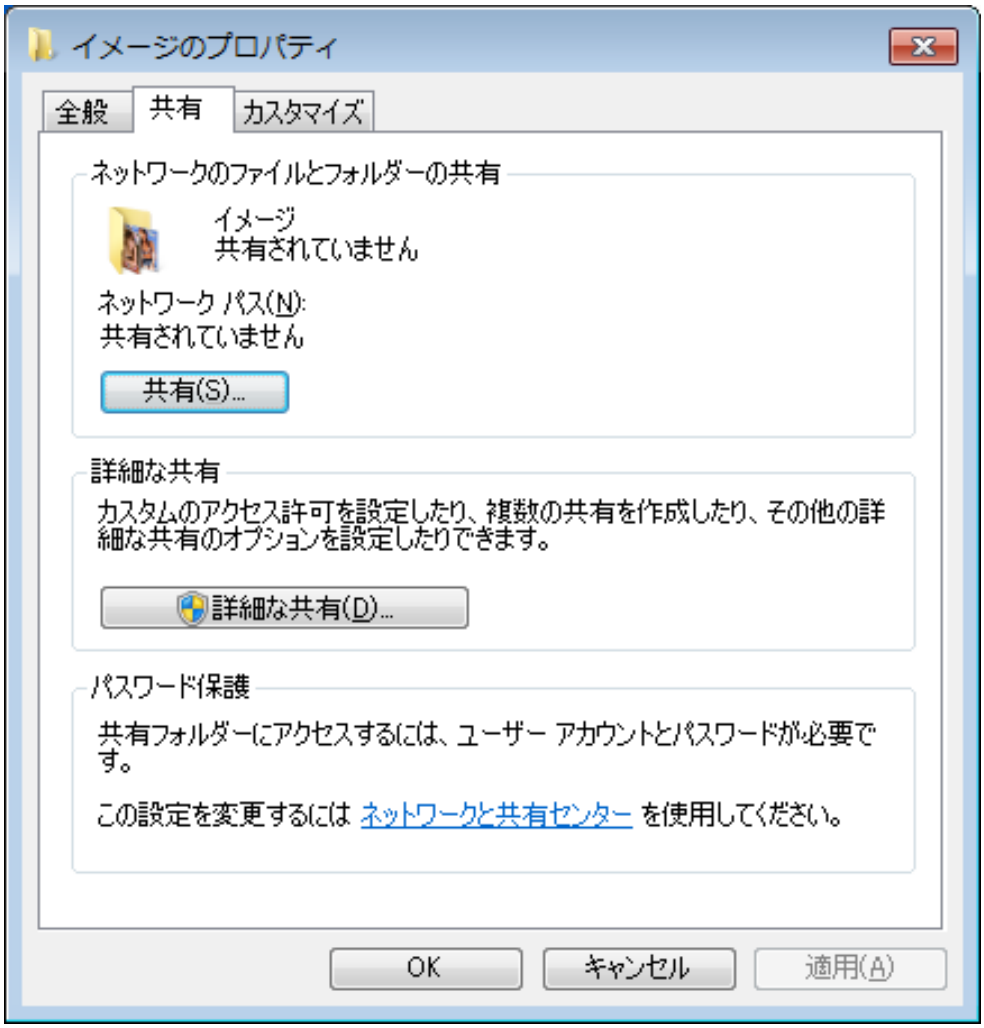
ビジネスホテルの LAN に、パソコンを接続して、マイネットワークからネットワーク全体を見てみると、他人のパソコンのフォルダが見える場合があります。これは、フォルダの共有設定を行ったまま、LAN に接続している利用者がいるからです。

自分のパソコンの中を見て下さいと言っているようなものです。不特定の人が利用する LAN に接続するのであれば、フォルダの共有設定の無効化を行って下さい。

フォルダが共有設定されている場合は、フォルダのアイコンが、左に示すアイコンのように表示されます。

フォルダ共有の設定画面は、当該フォルダの上でマウス「右クリック」→「プロパティ」→「共有」で表示されます。

お使いの OS が Windows 7 の場合は左に示す画面が表示されます。

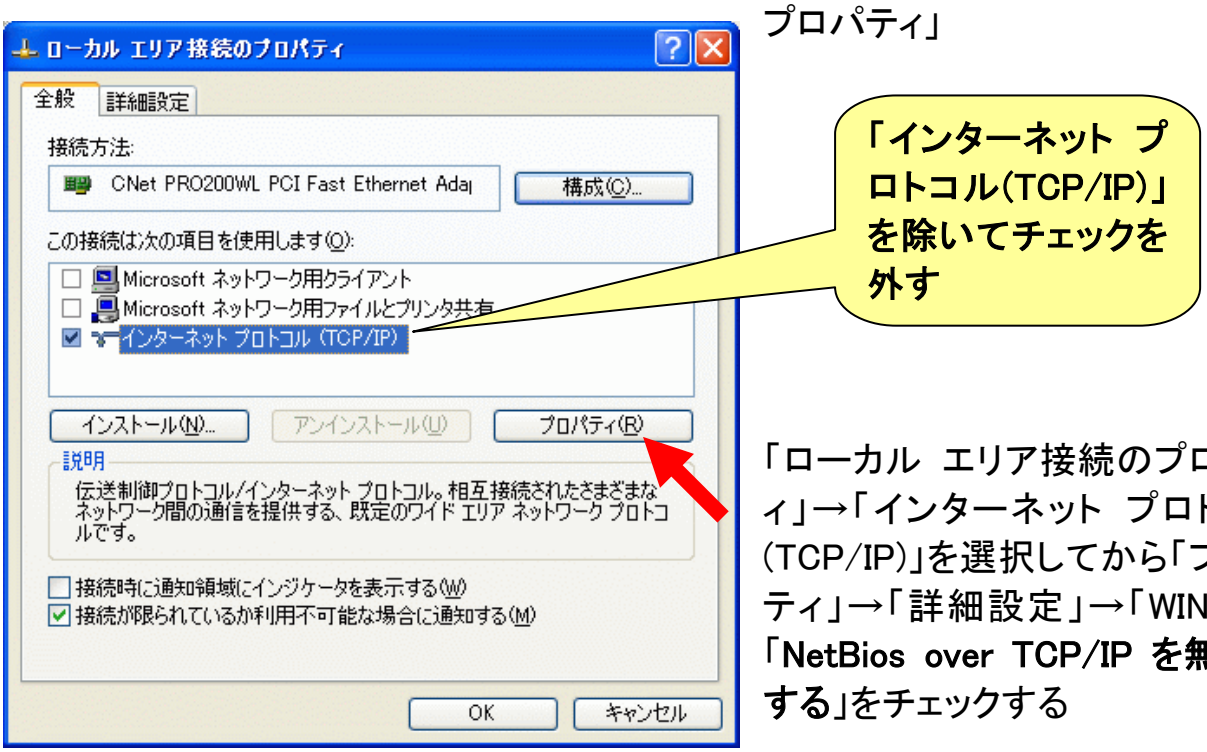


② ローカル エリア接続の設定を変更する

さらに、ローカルエリア接続の設定を変更し、**あなたのパソコンが Microsoft Windows Network 上で見えないようにする**ことを、お勧めします。

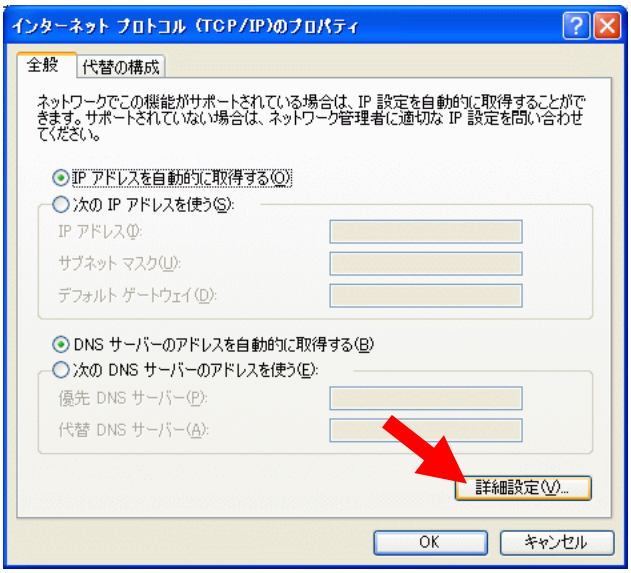
操作手順(Windows XP):

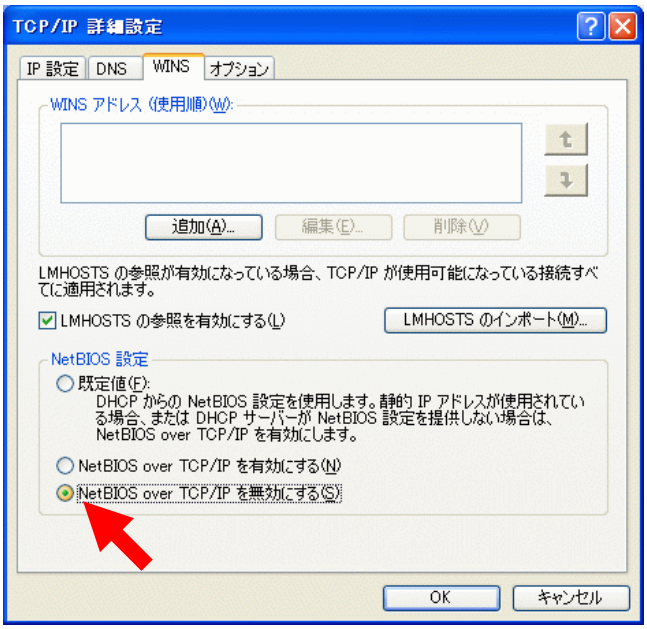
「スタート」→「設定」→「コントロールパネル」→「ネットワーク接続」→「ローカル エリア接続」の右クリック→「プロパティ」→「ローカル エリア接続のプロパティ」



「インターネット プロトコル(TCP/IP)」を除いてチェックを外す

「ローカル エリア接続のプロパティ」→「インターネット プロトコル(TCP/IP)」を選択してから「プロパティ」→「詳細設定」→「WINS」→**「NetBios over TCP/IP を無効にする」**をチェックする





Windows 7 の場合も基本的に同じです。

操作手順(Windows 7):
「コントロールパネル」→「ネットワークと共有センター」→「ローカルエリア接続」→「プロパティ」

(注意事項)

あなたが普段使っている、通常のネットワーク環境で利用する場合に、元の設定に戻すことを忘れずに・・・ここで示した設定を行うと、ネットワークプリンタやネットワーク上でのファイル共有ができなくなります。

ネットワークプリンタもファイル共有もお使いでなければ、この設定のままでも問題はありません。

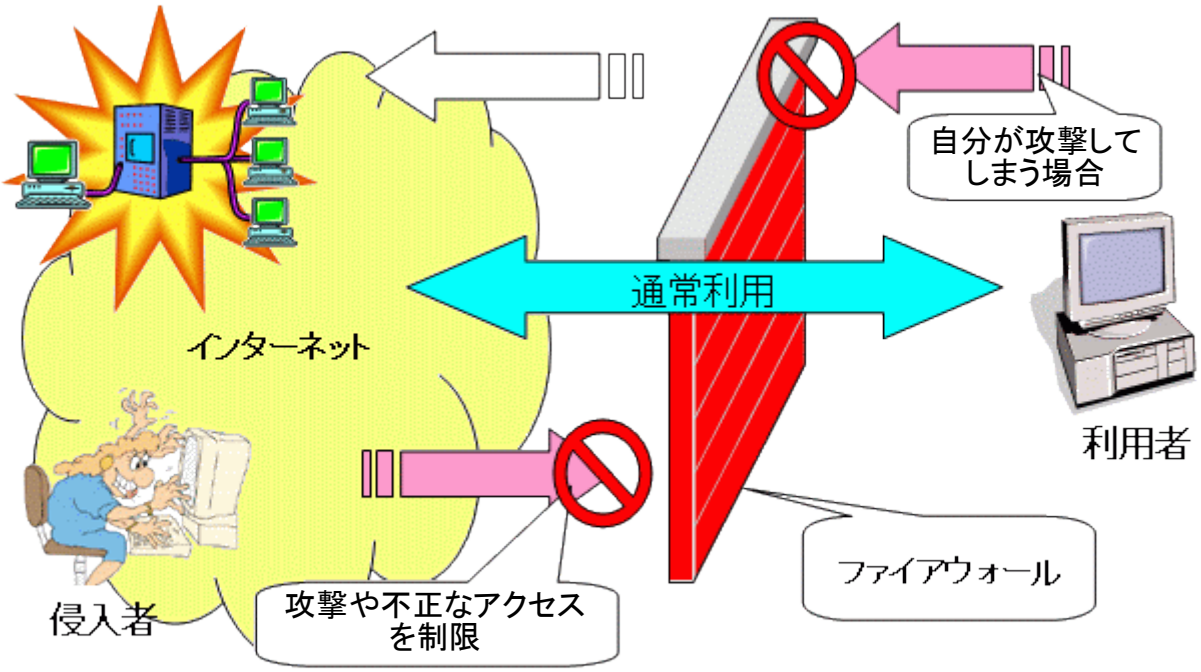
5. ファイアウォールソフト(統合セキュリティ対策ソフト)の活用の勧め

不正アクセス対策の重要ツールとして、ファイアウォール(防火壁)というものがあります。

ウイルス対策やスパイウェア対策だけでなく、ファイアウォール機能を持つ統合セキュリティ対策ソフトの活用あるいはパーソナルファイアウォールソフトの活用をお勧めします。

ファイアウォール機能は、インターネットとお使いのパソコンのデータのやり取りを監視することにより、悪影響を与えると思われる通信に対して、警告を表示し、侵入をブロックしてくれます。

また、スパイウェアのように、侵入したパソコンから外部にパソコン内の個人情報などを送信しようとした場合にも、警告を表示してくれるため、被害を未然に防ぐことが可能です。



特にモバイル環境で利用する場合は、ルータもファイアウォールも使われないため、利用するパソコンにパーソナルファイアウォールソフトまたはファイアウォール機能を持つ統合セキュリティ対策ソフトをインストールし、活用することを、お勧めします。

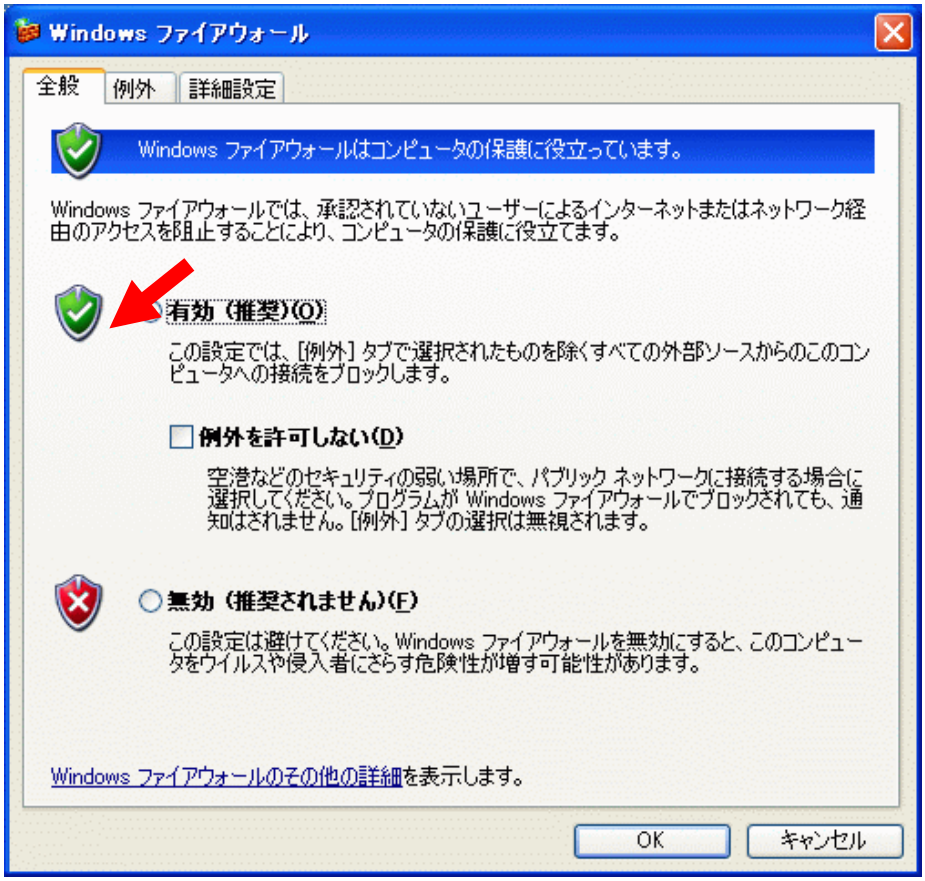
Windows XP 以降の OS を利用しているならば、OS に内蔵された Windows ファイアウォールの利用も、お勧めします。

Windows XP では Windows ファイアウォールは、外部からの悪影響を与えると思われる通信をブロックしますが、内部からの不正な通信はブロックしませんが、Windows XP の後継 OS である Windows Vista 以降では両方向の不正な通信をブロックする仕様になっています。そのため、利用するパソコンにパーソナルファイアウォールソフトまたはファイアウォール機能を持つ統合セキュリティ対策ソフトを活用できない場合は、この機能を有効にすることを、お勧めします。

ただし、ファイアウォール機能を持つ統合セキュリティ対策ソフトを利用する場合は、この設定が対策ソフト側の管理となり、以下の設定はできなくなる場合があります。

操作手順(Windows XP):

「スタート」→「設定」→「コントロールパネル」→
「Windows セキュリティ センター」→「Windows ファイアウォール」



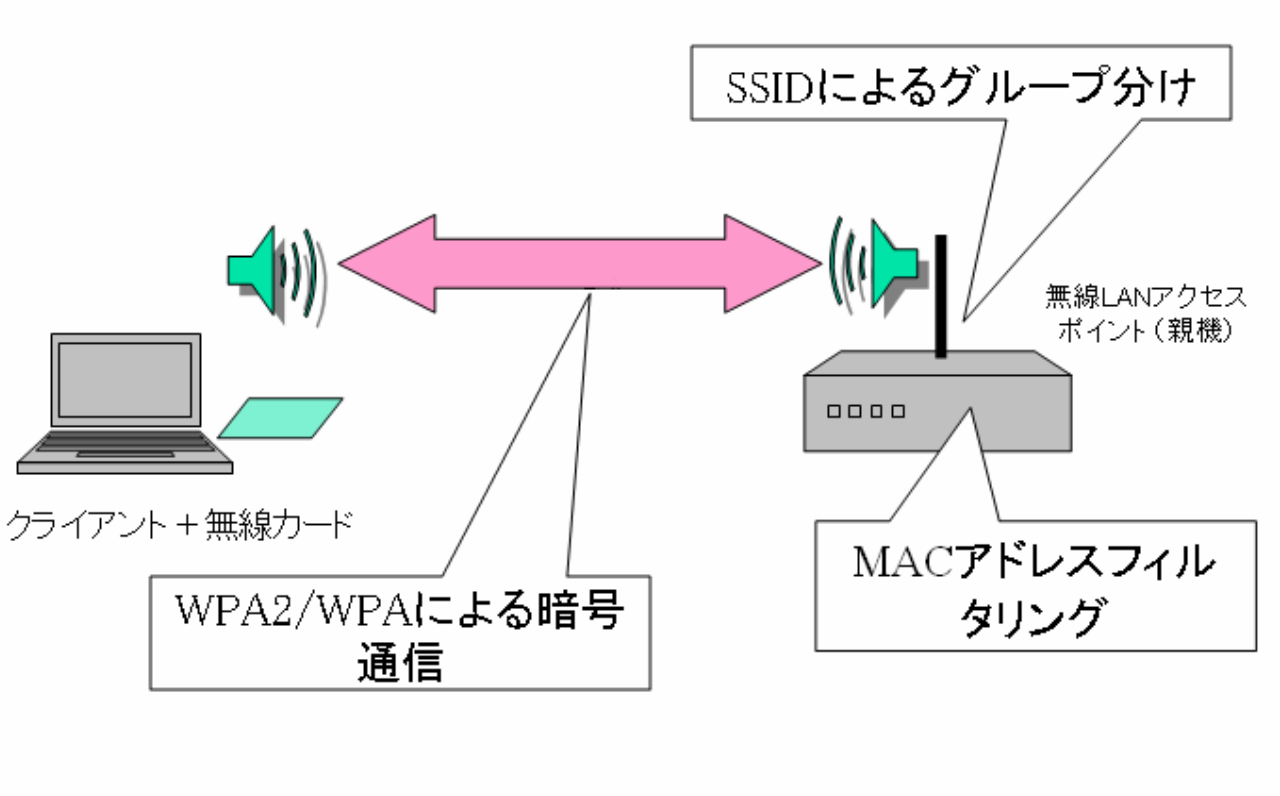
6. 無線 LAN の基本

無線 LAN は、ネットワークケーブルが不要で、電波が届く範囲であれば、家の中やオフィスでどこにいても利用できる、非常に便利な仕組みです。

ところが、セキュリティに関する設定を行っていないと、パソコン内の情報が盗まれてしまったり、無線 LAN を無断で利用されてしまったりといった危険があります。

最近の無線 LAN 機器には、必要最低限、実施しておくべきセキュリティ設定が用意されています。

以下に掲げるポイントは必ず実施するようにしましょう(**詳細は、無線 LAN 機器に添付された取扱説明書をご覧下さい**)。

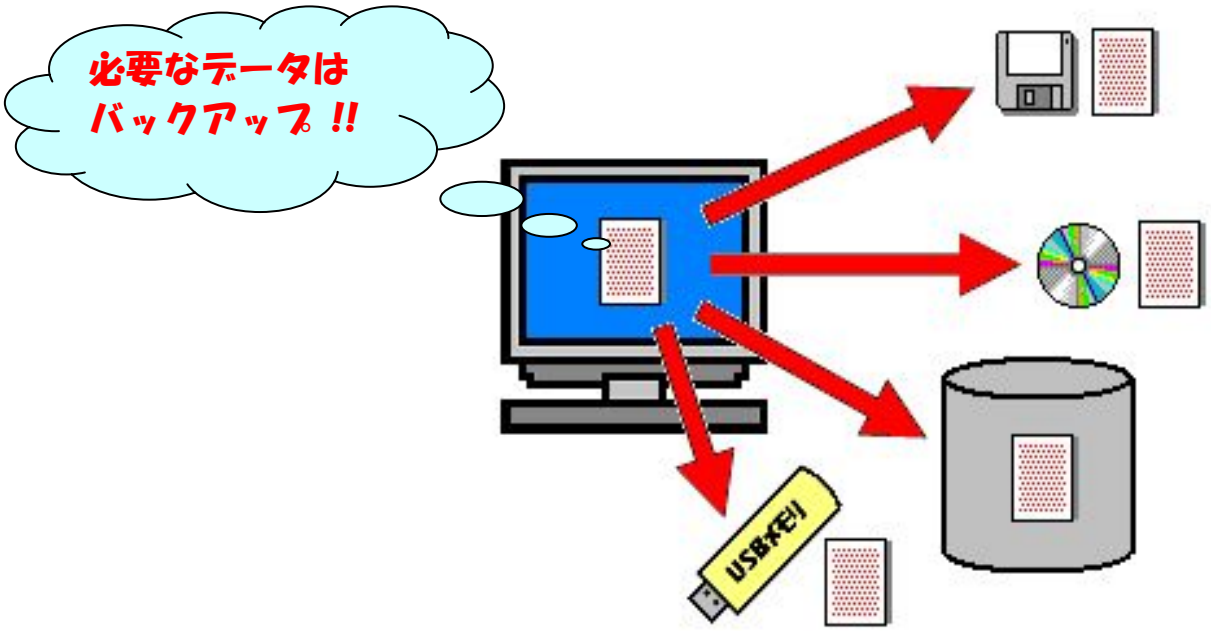


■ 無線 LAN アクセスポイント（親機）
- □ WPA2/WPA(*5)を設定する
  ※WEP(*6)にはぜい弱性が発見されているため、使用するべきではない
- □ SSID(*7)を設定する
- □ MACアドレス(*8)によるフィルタリングを設定する
- □ 空白又は ANY 端末からの接続を拒否する

■ アクセスポイントの設定に合わせてパソコンを設定する

7. 万一のためにデータは必ずバックアップしておく

不正アクセス(侵入行為)を受けてしまったパソコンは、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ことが多いため、復旧のためにはパソコン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、不正アクセスによりハードディスクの内容が破壊された場合には、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。



【システム復元機能】

Windows XP にはシステムを復元する機能があります。この機能を利用すると、システムを以前の状態に戻すことができます。

例えば、不正アクセス(侵入行為)によりシステムが変更されてしまった場合、復元機能を利用することで、変更される前の状態に戻せることがあります。何らかのファイルを開いて、動作がおかしくなってしまったときなど、この機能を試してみることをお勧めします。詳しい手順については、以下のサイトをご覧下さい。

システムの復元を使用して Windows XP を復元する方法(マイクロソフト社)
http://support.microsoft.com/default.aspx?scid=kb;ja;306084

8. 万一、被害に遭ってしまったら･･･

不正アクセス(侵入行為)により、パソコンに何か不正なプログラムを仕掛けられたようであれば、まず、ウイルス定義ファイルを最新の状態にしたセキュリティ対策ソフト(ウイルス対策ソフトあるいはスパイウェア対策ソフト)により、パソコンの検査を実施して下さい。不正なプログラムは特定できたが、不正プログラムの駆除や隔離ができない場合は、使用したセキュリティ対策ソフトの Web サイトで、検出された不正プログラムの情報を探し、そこに記述されている対策（処置）を実施して下さい。

セキュリティ対策ソフトを使用していない方で、ネットワークに接続できるのであれば、セキュリティ対策ベンダーが提供している、無償のオンラインスキャン(オンラインでの不正プログラム検査サービス)を利用することで、不正プログラム名を特定できる可能性があります。不正プログラム名が特定できたならば、オンラインスキャンと同じ Web サイトで、検出された不正プログラムの情報を探し、そこに記述されている対策方法についてお試し下さい。

それでも、よく分からないとおっしゃる方は、マルウェアおよび不正アクセスに関する総合的な相談窓口として、**情報セキュリティ安心相談窓口**を開設しておりますので、こちらへお問い合わせ下さい。

■情報セキュリティ安心相談窓口

「情報セキュリティ安心相談窓口」の受付電話番号は
下記の URL をご参照ください。

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

※多くの方からご相談をいただく内容については、
上記の「情報セキュリティ安心相談窓口」ページに
「よくある相談と回答(FAQ)」の情報を掲載していますので、
まずはそちらをご覧くださいますようお願いいたします。

その他、情報セキュリティに関して困った場合は、
電子メールでもご相談を受け付けております。

E-mail ： **anshin@ipa.go.jp**

なりすまし行為の被害にあった場合は、サービスを提供している事業者あるいは都道府県警察本部のサイバー犯罪相談窓口に、お問い合わせ下さい。また、クレジットカード関連などの被害の場合は、全国の消費生活センター(国民生活センター)や各クレジットカード会社の相談窓口に、お問い合わせ下さい。

9. 参考情報

対策を含めて、以下の資料を参照下さい。

- 不正アクセス行為は処罰されます！
  http://www.npa.go.jp/cyber/legislation/gaiyou/main.htm
- 不正アクセス対策
  http://www.ipa.go.jp/security/fusei/ciadr.html
- コンピュータ不正アクセス関連 FAQ
  http://www.ipa.go.jp/security/ciadr/faq01.html
- セーフティとセキュリティ センター（マイクロソフト株式会社）
  http://www.microsoft.com/ja-jp/security/default.aspx

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

10.用語の説明

(*1)不正アクセス禁止法(不正アクセス行為の禁止等に関する法律)

「不正アクセス行為の禁止等に関する法律(いわゆる不正アクセス禁止法)」は、1999 年 8 月 6 日に参院本会議で可決、成立しました。一部を除き、2000 年 2 月 13 日から施行されました。また、2000 年 7 月 1 日からは、残りの項目である援助規程(第6条)も施行され、新しくは、2012 年 5 月 1 日に改正不正アクセス禁止法が施行されました。

実際の条文に関しては、以下の警察庁のサイトをご参照下さい。

http://www.npa.go.jp/cyber/legislation/gaiyou/houann.htm
http://www.npa.go.jp/cyber/legislation/gaiyou/gaiyou.htm
http://www.npa.go.jp/cyber/legislation/gaiyou/main.htm

国家公安委員会による「不正アクセス行為の再発を防止するための都道府県公安委員会による援助に関する規則」は、下記にあります。

http://www.npa.go.jp/cyber/legislation/kitei/enjyo_kitei.htm

その他に、不正アクセス行為によりコンピュータに障害が発生した場合や、データの破壊が行われたような場合には、威力業務妨害等の罪に該当する場合があります。

(*2)ぜい弱性 (vulnerability)

情報セキュリティ分野において、通常、ぜい弱性とは、システム、ネットワーク、アプリケーション、または関連するプロトコルのセキュリティを損なうような、予定外の望まないイベントにつながる可能性がある弱点の存在、設計もしくは実装のエラーのことを言います。オペレーティングシステムのぜい弱性である場合もあれば、アプリケーションシステムのぜい弱性である可能性もあります。また 、ソフトウェアのぜい弱性以外に、セキュリティ上の設定が不備な状態においても、ぜい弱性があるといわれることがあります。俗に、セキュリティホール(security hole)と呼ばれることもあります。

(*3)アクセス制御 (access control)

コンピュータセキュリティにおいて、ユーザがコンピュータシステムの資源にアクセスすることができる権限・認可をコントロールすることを言います。

(*4)利用者 ID およびパスワード

不正アクセス禁止法では、識別符号と記述されているものです。いわゆる、本人を特定することのできる符号、指紋、署名、音声や影像などですが、ここでは単純に利用者 ID およびパスワードと表現します。

(*5)WPA2/WPA (Wi-Fi Protected Access)

WEP に替わる暗号化方式として無線 LAN の業界団体 Wi-Fi Alliance が発表した規格のことを言い、WEP の弱点を補強し、セキュリティ強度を向上したものです。WPA2 は WPA をさらにバージョンアップしたもので、より強力なアルゴリズムである AES(Advanced Encryption Standard)を採用しています。

(*6)WEP (Wired Equivalent Privacy)

RC4 アルゴリズムをベースにした秘密鍵暗号方式で、IEEE によって標準化されています。しかし、WEP には様々なぜい弱性が発見・報告されています。

(*7)SSID (Service Set IDentifier)

アクセスポイント(AP)を識別するための ID のことを言います。ESSID と呼ぶこともあります。

(*8)MAC アドレス

ここでは、無線 LAN アダプタ(子機)に設定されている固有の ID のことを言います。

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