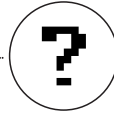


Frequently Asked Question



いまさら聞けない



いまだから聞きたい

このコーナーでは読者の皆さんのインターネットに関する疑問や質問にお答えします。「?」と感じたことはどのようなことでも構いませんので、以下のメールアドレスまでご質問ください。なお、ご質問へのメールでの回答はできませんのでご了承ください。

ご質問はこちらまで
im-welove@impress.co.jp

今月のポイント

1 「ブリッジ型」と「ルーター型」の違い 2 無線LAN導入時の注意点



11月号のADSLモデムに関する質問で、「ルータータイプがおすすめ」ということはわかりましたが、ブリッジ型とルーター型のADSLモデムの違いが今ひとつよくわかりませんでした。詳しく教えてください。よろしくお願いします。(M・Aさん)



ADSLモデムには「ルーター型」「ブリッジ型」「USB型」の3タイプがあります。なかでもルーター型とブリッジ型は、ともにイーサネットで接続するために外見上は違いがわかりにくいかも知れません。今回は、ルーター型とブリッジ型のモデムの違いを説明していきましょう。

まずルーター型のADSLモデムですが、これはその名のとおりに「ルーター」として機能します。では、ルーターとはどのような働きをするのでしょうか？ここではルーター機能についておさらいしておきましょう。ルーターとは、異なるネットワーク同士を接続するネットワーク機器です。OSI参照モデルのネットワーク層以上で動くため、その動作はTCP/IPなどのネットワークプロトコルに依存します。ADSLモデムの場合、WAN側(ADSLモデムより外側)とLAN側(ADSLモデムより内側の家庭やオフィスにあるPCやネットワーク)を相互に接続しているわけです。つまりネットワー

ク的に見ると、自宅のPCは外部のネットワークと「別のネットワーク」になっているのがルーター型の大きな特徴です。ISPなどから割り振られるIPアドレスはルーターが持ち、ルーターに接続してあるPCにはルーターが「DHCP」という機能を使って内部ネットワーク用のプライベートアドレスを割り当てます。通常はWAN(インターネット)側からプライベートアドレスを見ることはできないので、ルーターを導入したネットワークは外からはルーターまでしか見られません。そのためルーターを導入することはセキュリティ面でも効果的です。次はブリッジ型です。ブリッジはLANに

おけるセグメント間を接続する機器で、受け取ったパケットを目的の端末へと効率よく中継するための機器です。一言でいうとブリッジとは、ネットワーク機器の橋渡しを行うものです。ルーターと異なり、OSI参照モデルのデータリンク層で動作しているのもブリッジの特徴です。ブリッジ型のADSLモデムを導入した場合、ISPから割り振られるIPアドレスはPC自身が持つので、WAN側からPCが丸見えになります。不正アクセスなどの危険を避けるため、別途ルーターを購入するといいいでしょう。

一見似ているADSLモデムが、ネットワーク的には大きく異なるのです。(編集部)

ルーター型は「転送」機能、
ブリッジ型は「橋渡し」機能



Q

無線LANを導入しました！非常に快適に使っているのですが、知人から「無線LANはセキュリティーを正しく設定しないと危険が多い」と聞き、なんだか不安になりました。どのような危険性がある、私は何をしなければいけないのか教えてください。(東京都 西野 勤さん)

A

有線LANと違って、無線LANでは電波を利用するので、その電波の到達範囲内であれば、無線LANが利用できるわけです。要するに、オフィスや自宅に設置した無線LANアクセスポイントに対して、屋外の道端から誰かがアクセスしてくることもあり得るのです。無線LANは当然ながらファイアーウォール内に設置するので、そこに第三者が直接アクセスしてくることは、セキュリティもあつたものではありません。というわけで、無線LANではセキュリティの確保が最重要課題です。

セキュリティの第1歩は、通信するデータの暗号化です。これは「WEPキー」と呼ばれる暗号化キーの設定で行います。できれば128ビット長のWEPキーを利用し、普段使っているパスワードなどのように容易に推測できない文字列を使って設定してください。

また、無線LANのアクセスポイントの設定では、「ESS-ID」という、いわゆるアクセスポイントの名前が設定できます。基本的にはこのESS-IDを知らないとアクセスポイントの利用はできないので、セキュリティ確保の1つの方法と言えます。しかし、ウィンドウズXPなどはESS-IDを自動で探す機能を持っているので、ESS-IDだけでは不十分です。なお、ウィンドウズXP上でその存在を見えなくする機能を持ったものもあります。

無線LANでは、アクセスポイントに接続してくるPCカードを、個別に制限することができます。通常のイーサネットと同様に、無線LAN装置それぞれに「MACアドレス」

無線LANを使うなら、これだけは設定しないと危険！

と呼ばれる48ビット長の固有のアドレスが割り振られています。アクセスポイントでこのMACアドレスに基づく制限をかければ、不要なアクセスを避けられます。

最後に、無線LANのセキュリティーに直接の関係はありませんが、アクセスポイントを設定するときの管理者認証のパスワード設定も、忘れずに設定しておきましょう。

無線LANのセキュリティーを設定するのは、機種ごとに方法が異なり、簡単なよう

で面倒です。無線LANの初心者の場合、それらをまとめて面倒見てくれるソフトウェアを使うのも1つの方法と言えます。ソースネクストの「鉄壁 無線LAN」もその1つで、WEPキーやMACアドレスでの制限などの設定が簡単にできます。

無線LANを利用する場合は、以上のようなことを十分理解し、セキュリティーを確保することが重要です。

(本誌アドバイザー 井上尚司)

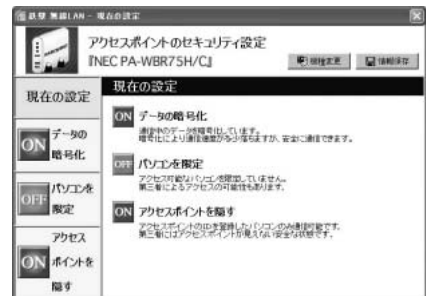
無線LAN、これだけは守るべし



- 1 暗号化キーを設定し、データを暗号化しよう
- 2 ESS-IDを設定しよう
- 3 MACアドレス制限を使って、アクセスを制限しよう
- 4 アクセスポイントの設定パスワードも忘れずに
- 5 自信がなければセキュリティー設定の専用ソフトを



MACアドレスはPCカードの裏などに書いてある。



無線LANのユーティリティソフト「鉄壁 無線LAN」の画面。 www.sourcenext.com



[インターネットマガジン バックナンバーアーカイブ] ご利用上の注意

このPDFファイルは、株式会社インプレスR&D(株式会社インプレスから分割)が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

<http://i.impressRD.jp/bn>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真の撮影者、イラストの作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元(株式会社インプレス R&D)、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D(当時は株式会社インプレス)と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接のおよび間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先

株式会社インプレスR&D

All-in-One INTERNET magazine 編集部

im-info@impress.co.jp