標準ソフト+フリーウェアを使って
最短ステップで実現！

WindowsXPで作る スマート自宅サーバー

橋本情報戦略企画 橋本和則【著】

- リモートコントロール
- ストリーミングサーバー
- FTPサーバー
- HTTPサーバー
- メールサーバー

技術評論社

本PDFデータは、書籍『Windows XPで作るスマート自宅サーバー』を基に、
2011年4月4日に技術評論社が作成したものです。

◆本書をお読みになる前に

本書に記載された内容は、情報の提供のみを目的としています。したがって、本書を用いた運用は、必ずお客様自身の責任と判断によって行ってください。これらの情報の運用の結果について、技術評論社および著者はいかなる責任も負いません。

本書記載の情報は、2005年11月現在のものを掲載しています。ソフトウェアのバージョンアップやWebページの更新などにより、本書での説明とは機能内容や画面図などが異なってしまうこともあり得ます。

以上の注意事項をご承諾いただいた上で、本書をご利用願います。これらの注意事項をお読みいただかずに、お問い合わせいただいても、技術評論社および著者は対処しかねます。あらかじめ、ご承知おきください。

はじめに

自宅サーバーの活用は無限大だ。

筆者の事務所内には現在5台のパソコンが存在するが、ディスプレイは4台しかない。

しかも3台はメインマシン用で、1台はテレビ録画専用マシンだ。では、残りの3台はどのように管理しているかといえば「リモートコントロール」でメインマシンから管理するようにしている。つまりディスプレイレスでコスト削減、そして置き場所を選ばなくなるので（クーリングの問題さえクリアすれば押入れの中でもよいのだ）、結果省スペース化しているのだ。

サブマシンうち1台は、FTPサーバー＆Webサーバー化して、技術評論社との原稿ファイルの受け渡しやWebチェックに役立てている。テレビ録画用マシンでは、地方出張時にFTPサーバーを起動し、遠隔地から録画した番組をダウンロードして見られるようにしている。もう一方のサブマシンには「Webカメラ」をぶら下げている。このWebカメラは「マンションの玄関」に装着するようにして（エアコンの配管をうまく伝うようにしている）、インターネット上に公開し、外出時でも人の出入りをチェックできるようにしている。これらすべてが、「自宅サーバーテクニック」だ。

自宅サーバーの特徴として、まず、ブロードバンド回線さえ所有していればコスト0円で構築できるというメリットがある。また、利用方法は上の例に挙げたものだけではなく、会社から自宅のパソコンをコントロールする、知人やクライアントのサポートに利用する、巨大なファイルの交換、CGIのテスト、ペットや作業者の監視など、とにかくさまざまな「便利な活用方法」があるのだ。

本書では自宅サーバーを最大限に活用できる、「リモートコントロール」、「ビデオ映像配信」、「FTPサーバー」、「HTTPサーバー」、「メールサーバー」の5大テクニックを余すことなくお伝えする。ネットワークを120%活用したいという人は、本書のテクニックをぜひ自分のものにしてほしい。

最後に、本書の作成にあたって企画＆編集を担当していただいた、技術評論社の青木さんに深く感謝したい。

2005年11月
橋本情報戦略企画　橋本和則

目次

Chapter 01

自宅サーバーでできること

「自宅サーバー」などというと、ずいぶん難しい、上級者のテクニックのように思えるかもしれないが、そんなことはない。むしろ、自宅と会社を行き来する人、ペットや作業を監視したい人、大きなファイルの受け渡しをしたい人など「これをしたい」という用途がある一般ユーザーこそが活用できるテクニックなのだ。この章では、まずは「自宅サーバーでできることと、活用方法」を紹介しよう。

自宅サーバーはすべて「無料」で実現できる!!

本書では自宅サーバーテクニックとして、リモートコントロール、ビデオ配信、FTPサーバー、HTTPサーバー、メールサーバーを説明する。これらは、Windows XPが動作するパソコンとインターネット接続環境さえあれば、すべて「無料」で実現できる。

各テクニックについては次項からの説明を参照してほしいが、自宅でパソコンを複数台所有している人、あるいは会社と自宅などで結果的に2台以上のパソコンを利用する人にぜひ活用してほしいのが「自宅サーバー」テクニックだ。

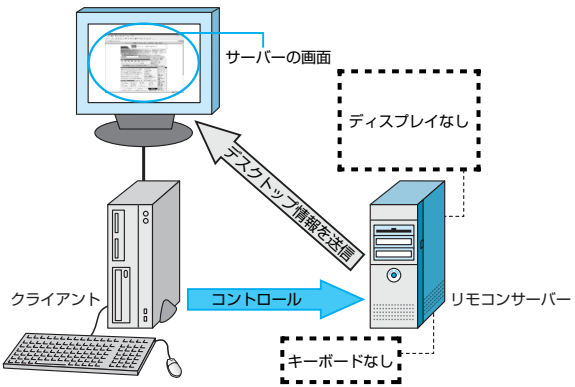
「リモートコントロールサーバー」でパソコンをリモートコントロール

パソコンをパソコンでコントロール――と書くと難しく感じるかもしれないが、ネットワーク知識をきちんと身につければ、意外に簡単に実現できる。

リモートコントロール環境を実現すれば、クライアントからサーバーパソコンを自由に操作できるため、サーバーパソコンをキーボードレス・モニターレスにすることも可能になる。また、**「会社から自宅のパソコンを操作する」**という便利な環境を実現できる。

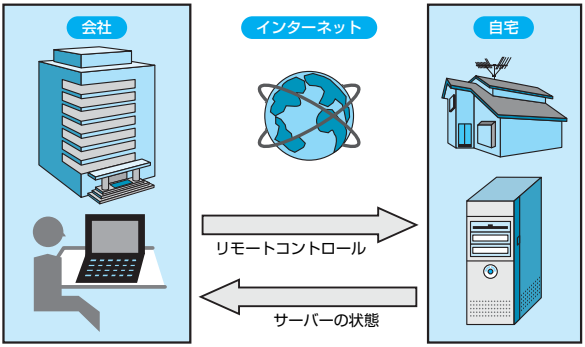
リモートコントロールは基本的に直接操作と全く違いがないので、遠隔地から、アプリケーションのインストールやパソコンの再起動、ルーターの設定などのコアな操作も行うことができる。「リモートコントロール」の活用方法は無限大なのだ。

▼モニターもキーボードも必要なくなる「リモートコントロール」



リモートコントロールをセットアップすれば、サーバーパソコンはモニターやキーボードを接続しなくとも外部から操作可能になる。これを応用して、他人が触れることができない「隠しパソコン」を構築することもできる。

▼遠隔リモートコントロール



リモートコントロールソフト＋自宅サーバーの組み合わせで、遠隔リモートコントロールが実現する。会社にいながら自宅のパソコンのデータを閲覧したり、メール送信やダウンロード指示などを実行できる。

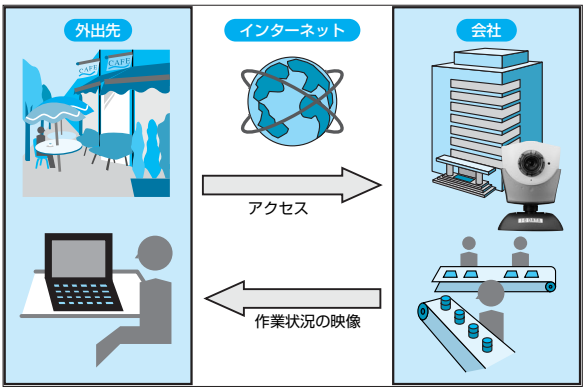
「ビデオ配信」で遠隔監視＆既存動画閲覧

ビデオ配信とは、サーバーに置いたビデオファイル（動画ファイル）をダウンロードさせることではなく、**Webカメラに映る「生の映像」を遠隔地に配信するシステムだ。**

このビデオ配信テクニックも活用方法はさまざまだ。会社の責任者なら作業員の遠隔監視を行うことができ、ペットを飼っている人ならペットの様子を確認することができる。バンド活動をしていたり、ネットアイドルをしていたりという「メディアに露出したい人」であれば、「自分自身」を情報として配信してもよいだろう。

また、ビデオ配信する映像はサーバーに「保存」しておくこともできる。

▼遠隔ビデオ配信（遠隔監視）の活用



遠隔ビデオ配信テクニックを利用すれば、外出先から自宅の様子を見たり、会社の状況を確認したりすることができる。遠隔地からジェスチャー付きで部下に指示を出したり、ビデオ会議に参加したりと、仕事に活用することもできる。

Webカメラ：アイ・オー・データ機器「USB-CAM30MS」

「自宅FTPサーバー」でファイル交換

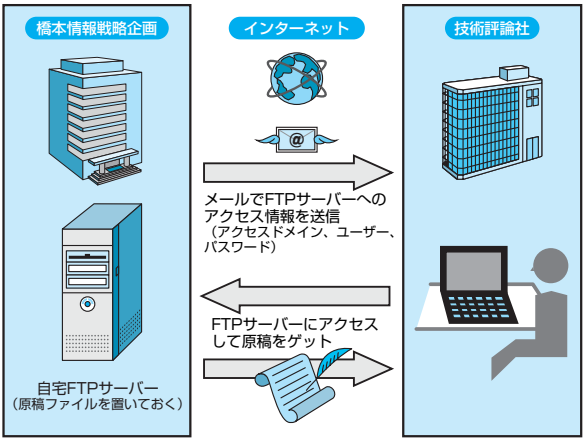
数百MBもの作業データを至急クライアントに渡したい…といった場合、以前であれば、MOディスクなどに書き込んでバイク便を飛ばしたものだが、現在のようなブロードバンド環境が整備された時代ではそんな必要はない。「FTPサーバー」を利用してデータを受け渡せばよいのだ。

ところがこれが「数GB単位」になってくると、プロバイダやネットストレージサービスから割り当てられた個人用のサーバースペースに保存することが難しくなってくる。

そこで登場するのが「自宅FTPサーバー」だ。**自宅のパソコンをFTPサーバーにすれば、事実上無限の容量を利用できるため、数GBのファイルの受け渡しも容易に実現できる。**また、ユーザー単位でファイルの読み込みや書き込みの制限、アクセスフォルダの制限が行えるため、個人用に留まらず、さまざまな場面で活用することができる。

「アノニマス（Anonymous）」ユーザーを作成しておけば、不特定のユーザーにファイルを渡したり、あるいは書き込んでもらうなどの「お楽しみ」も可能だ。

▼原稿の送信



筆者は、実際に「自宅FTPサーバー」を利用して、技術評論社編集部に原稿を渡している。メールで送れるような容量ではなく、またメディアに書き込んで郵送する経費がもったいないからだ。自宅FTPサーバーを立ち上げ、原稿担当者にアクセス情報を送信、そしてダウンロードしてもらえば、時間的・金銭的コストを大幅に節約できる。

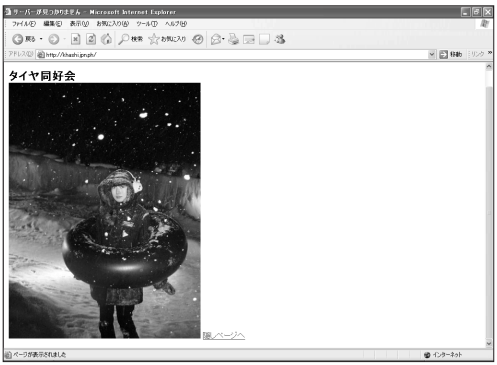
CGI対応「自宅HTTPサーバー」でフリーWebエリアを実現

「自宅HTTPサーバー」とは、いわゆるWebサーバーを自宅パソコンに設置したものだ。

自宅HTTPサーバーの場合、プロバイダから割り当てられるWebサーバー用スペースに比べ、**「容量が無制限」「CGIを自由に配置できる」「パスワード認証ページも簡単に作れる」などのメリットがある。**

インターネットへの個人ページの公開はもちろん、イントラネットやWebページの動作テストなどにも役立てることができる。

▼自宅HTTPサーバーの活用



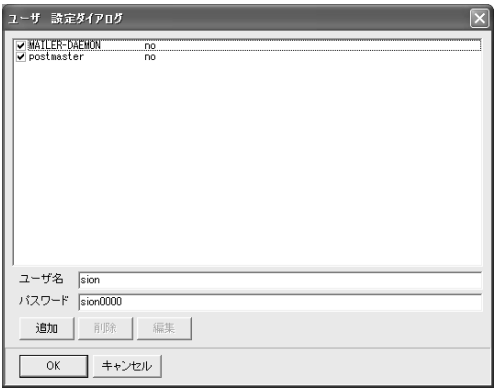
オリジナルWebページを作成。CGIも自分の好きなように設置できる。

「自宅メールサーバー」でオリジナルメールアカウントを無数に作成

自宅メールサーバーでは、SMTPサーバーやPOP3サーバーという、通常ならプロバイダが管理すべきサーバーを個人で管理する。そうすることで、自分がプロバイダになったかのように、「メールアカウント（メールアドレス）」を好きなだけ作成して管理することができる。

自宅メールサーバーで作成したメールアカウントは、その特性上、メインメールアドレスに使用すべきではない。ただし、匿名性が高いことを利用して、サブメールアドレスとしてメールマガジンの購読や、懸賞サイトなどの「使い分け用途」で大いに役立つだろう。

▼自宅メールサーバーの活用



「自宅メールサーバー」を作れば、自分がメールサーバー管理者になって、メールアドレスを好きなだけ作成することができる。

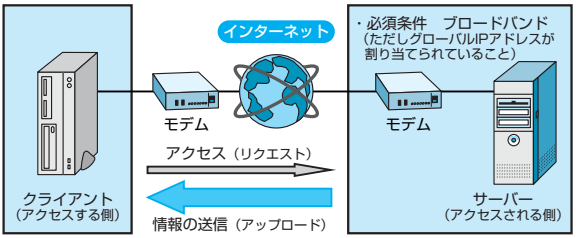
自宅サーバー構築の条件

自宅サーバーを構築するための条件は、「サーバー側の回線（たとえば会社から自宅にアクセスするのであれば自宅側）が“ブロードバンド”であること」、たったこれだけだ。

さらに細かい条件を言うと、回線に「グローバルIPアドレス」が割り当てられている必要があるのだが、現在の一般的なプロバイダはグローバルIPアドレスを割り当てているので特に気にすることはないだろう（グローバルIPアドレスについてはP.021参照）。

ただ、「理想」を言えば、サーバー側の回線は速いに越したことはない。この速さに関しては「ダウンロード側」（プロバイダから自宅に向かう側）よりも「アップロード側」（自宅からプロバイダに向かう側）のスピードが求められる。その点で、アップロード側の速度が遅いADSL回線より、FTTH回線（光回線）のほうが自宅サーバー運営に向いているだろう。

▼自宅サーバーに必要な条件



自宅サーバーに必要なのは「アクセスされる側（つまりサーバー）」が「ブロードバンドでかつグローバルIPアドレスが割り当てられている」ことだけだ。なお、サーバーから送信する情報量を考えると「アップロードスピード」が速いに越したことはない。

▼ADSLサービス

ADSLのサービスプラン。アップロードスピードはたいてい1MBであり、3MBのプランを選択しても、実測では1MBとそれほど変わらなかったりする。

本書が想定する環境

自宅サーバー構築の設定において、最も大きな差になるのが「ルーターの有無」である。

簡単に言うと、ルーターがなければ自宅サーバー構築はかなりシンプルになり、ルーターがあるとかなり詳しくネットワークの理論を学ぶ必要に迫られる。

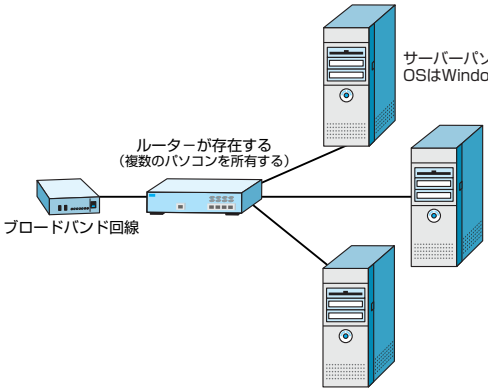
これについて詳しくは10章で述べるが、本書の読者の場合は「ルーターが存在する環境が普通」だと考えられるので、本書ではルーターが存在することを前提に説明していく。

また、自宅サーバーのOSはWindows XPを前提として説明する。紹介するソフトのほとんどはWindows XP以外のWindowsでも駆動可能だが、動作保障はしない。

まとめると、以下のようになる（すべてサーバー側の環境）。

- 回線はブロードバンド（グローバルIPアドレスが割り当てられている）
- ルーターが存在する（ローカルレベルのネットワーク環境がある）
- OSはWindows XP SP2（ファイアウォールはSP2の「Windowsファイアウォール」を利用）

▼本書が想定する環境



本書はサーバー環境において「一般回線のブロードバンド」を利用し、パソコンに「Windows XP SP2」を、そしてルーターを利用していることを想定して説明する。

本書の解説順序

本書では、自宅サーバーを活用したリモートコントロールやFTPサーバー環境の構築を最終的な目標として解説していくが、この環境を実現するには、ざっと以下のようなセットアップが必要になる。

- サーバーアプリケーションのセットアップ
- クライアントアプリケーションのセットアップ
- LAN（ローカルエリアネットワーク）のセットアップ
- ファイアウォールのセットアップ
- ルーターのセットアップ
- ダイナミックDNSのセットアップ

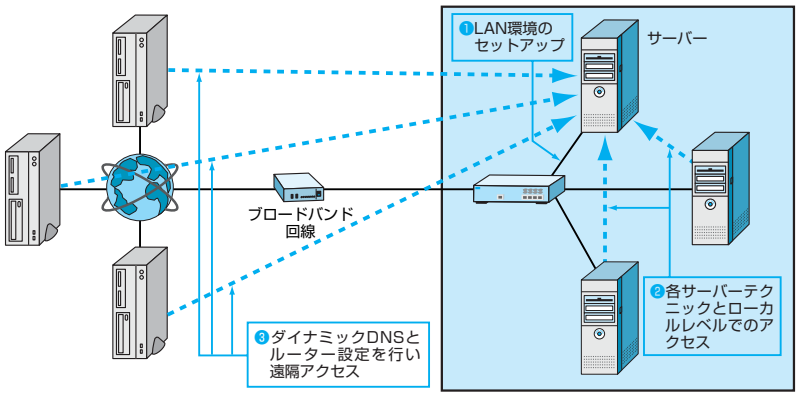
自宅サーバーを実現するには、このようにさまざまなセットアップが必要であり、どれが欠けてもうまくいかない（動かない）。この点が、「自宅サーバーが難しい」といわれる理由である。

そこで本書では、まずローカルエリアネットワーク、つまりインターネットを介さないネットワークに限定した上で、リモートコントロールやビデオ配信、FTPサーバー、HTTPサーバーを実現し、各機能の「動作確認」を行う。

そのあとに、「ダイナミックDNS」などのインターネットを介した遠隔接続に必要な設定を行い、「自宅サーバー」を完成させるものとする。

具体的には、以下のような説明順序になる。

▼本書の説明順序



❶ LAN環境のセットアップ（各サーバー共通）
ネットワーク環境の用語や確認方法を知る

↓

❷ 各サーバーの構築とローカルレベルでのアクセス
各サーバーをLAN内で実現して、動作確認する

↓

❸ ダイナミックDNSとルーター設定を行い遠隔アクセス
インターネットを介した遠隔地からのアクセスを実現する

ネットワーク用語と本書の表記

ネットワーク用語の大きな問題点は、「使用する場面で用語の意味が異なる」こと、そして「用語が適用される範囲が明確ではない」ことだ。

この問題は自宅サーバー構築時には大きな弊害になる。各アプリケーションごとに用語の表記が異なったり、意図する意味が不明瞭であったりするからだ。特に本書は「リモートコントロールサーバー」「動画サーバー、クライアント」「FTPサーバー、クライアント」「HTTPサーバー」「メールサーバー、メールソフト」など、多岐に渡るサーバーやクライアントの設定、テクニックを説明するため、この用語統一が取れていない状態では混乱を起こす可能性がある。

よって本書では、最初に各ネットワーク用語についての明確な定義づけを行い、その意味を説明することにした。各ネットワーク用語の詳しい意味や構造については、次章を参照の上、理解を深めてほしい。また、各サーバーテクニックの実践中に用語の意味があいまいになってきた場合は、付録P.235を参照してほしい。

Chapter 02

自宅サーバーに必要なネットワークの基礎知識

「自宅サーバー」はネットワークを活用した総合テクニックなので、ネットワークの基本的な知識や用語、構造を知っておく必要がある。ネットワークの基礎知識は自宅サーバーを構築するときにはもちろん、運用時のトラブルシュートにも役立つので、きちんと頭に入れておこう。

ネットワークの基礎知識

ネットワークの理論自体は特に難しいものではないが、各サーバーを構築する際には「プライベートIPアドレスとグローバルIPアドレスの違い」「ポート番号を指定してデータはやり取りされる」など、普段はあまり意識しない「ネットワークの理論」をきちんと理解しておかなければならない。

ネットワークの基礎知識を理解している者であれば、この章は読み飛ばしてもよい。いち早く各サーバー機能を実現したいなら次章から読み進め、あいまいな知識や用語があったら本章で確認するとよいだろう。

グローバルIPアドレスとプライベートIPアドレス

IPアドレスの役割、及び「グローバルIPアドレス」と「プライベートIPアドレス」の違いを知ることこそ、自宅サーバー構築の最重要ポイントといってよい。

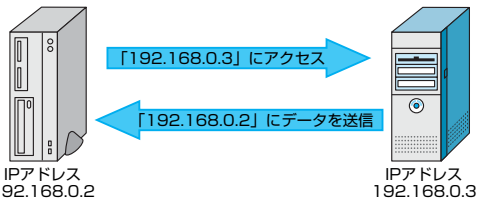
●IPアドレスとは

IPアドレスを一言で表現すると、ネットワークにおける「住所」である。

インターネットの世界では、住所として「競合しない（つまり固有の）」IPアドレスが割り当てられており、現在ではほとんどのネットワークでこの「IPアドレス」を指定して通信している。これは、LAN内のパソコン同士はもちろん、WANにおけるパソコン同士の通信や、インターネット上のWebページを閲覧するときでも変わらない。

「いや、Webを見るときには『http://www.gihyo.co.jp』等、文字列で相手を指定しているじゃないか？」と思うかもしれないが、実はこれもIPアドレスの見せ方を変えているに過ぎない（P.025参照）。

▼IPアドレスはネットワークの「住所」



パソコン同士の通信は相手を特定する手段（住所）として「IPアドレス」利用する。これは、LAN内のパソコン同士はもちろん、WANにおける通信やWebページを閲覧するときでも変わらない。

●グローバルIPアドレスとプライベートIPアドレス

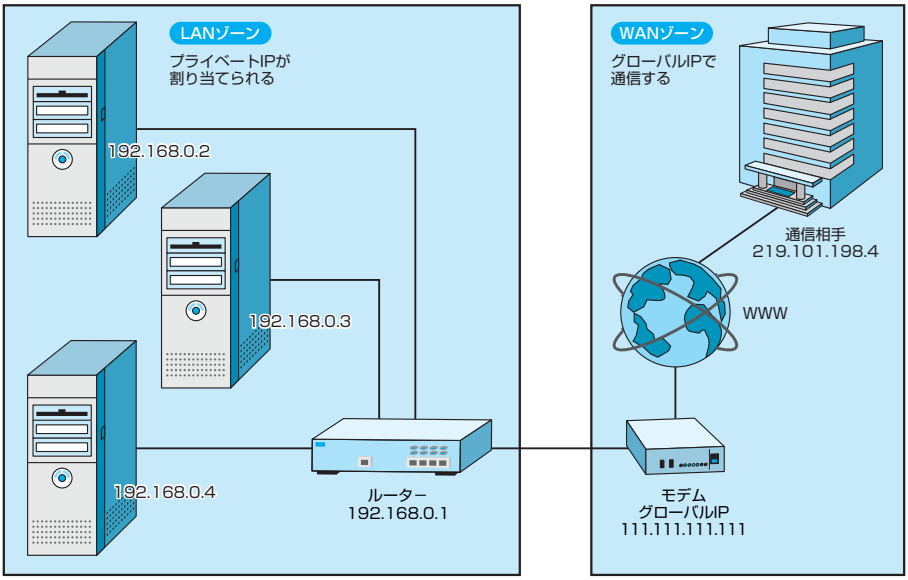
IPアドレスには「グローバルIPアドレス」と「プライベートIPアドレス」がある。

グローバルIPアドレスは「世界」と通信できるIPアドレスのことだ。インターネット通信を行う際は、回線ごとに必ずこのグローバルIPアドレスが割り当てられている（一部のプロバイダでは例外あり。マンション備え付けの回線や、CATVなど）。一方、「プライベートIPアドレス」は閉じたIPアドレスであり、自分のLAN（ローカルエリアネットワーク）内の通信のみで有効なIPアドレスだ。

まとめると、**「グローバルIPアドレス」は、インターネットを介してアクセスできる（される）IPアドレス。**そして、**「プライベートIPアドレス」は、自分のLAN（ローカルエリアネットワーク）内の通信のみで有効なIPアドレスだ。**

なお、「グローバルIPアドレス」「プライベートIPアドレス」とも、「＊＊＊.＊＊＊.＊＊＊.＊＊＊」（＊に数字が入る）という形でアドレスが示されるが、「プライベートIPアドレス」はこの割り当て番号の範囲が決まっているという特徴がある。

▼グローバルIPアドレスとプライベートIPアドレスのゾーン



グローバルIPアドレスがインターネット世界との通信に使われるのに対し、プライベートIPアドレスはその枝葉としてLAN内でのみ使用される。なお、WAN（会社と自宅の間など）で相手先アドレスとして指定できるのは、「グローバルIPアドレス」だけだ。

ポート番号

ネットワークにおける通信は、IPアドレスと共に必ず「ポート番号」を指定して行われる。

IPアドレスが住所だとすると、ポート番号は「出入り口の場所」を示す情報だ。以前のWindowsでは、通信を行いやすくするためにすべてのポートが「常に開けっ放し」の状態になっていたが、最近では逆に「必要なポート以外は閉じる」ように変わってきている（Windows XP SP2など）。

ポートには0～65535までの番号が存在し、各サーバー・クライアントアプリケーションは、この中のいずれかのポート番号を指定して互いに通信している。

ちなみに、FTPサーバー、HTTPサーバー、メールサーバーは、使用するポート番号が決められている。**FTPサーバーは20番と21番、HTTPサーバーは80番、メールサーバーは「SMTPサーバー」に25番、「POP3サーバー」に110番を使用する。**

このような通信用途（プロトコル）が決められているポートのことを**「ウェルノウン（well known）ポート」**という。

一方、リモートコントロールサーバーやビデオ配信サーバーでは、特に利用するポートが決められていないので、「自分で自由に決めた」ポート番号をサーバーとクライアントに設定して、アクセスする必要がある。

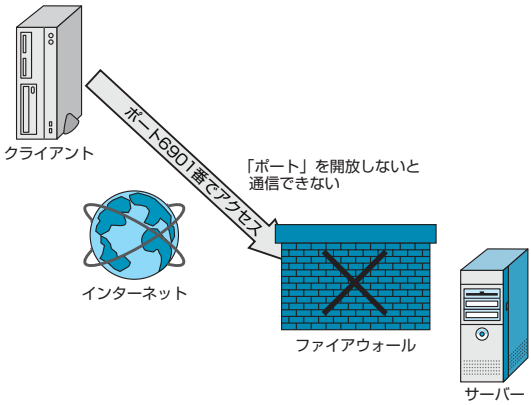
ファイアウォールの役割

「ファイアウォール」とは、ネットワークを使って通信しようとするアプリケーション（ネットワークアプリケーション）のデータをブロックする機能だ。ファイアウォールにはさまざまな種類や役割があるが、自宅サーバーを作る上では、シンプルに「ポートをふさぐ機能」だと考えてよいだろう。

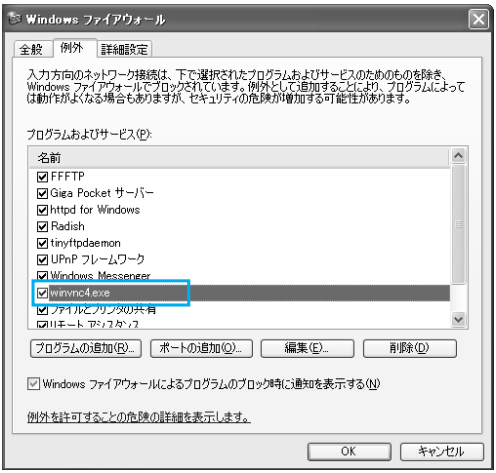
ファイアウォールでは、必要最小限のポート以外をすべてふさいで、不要な通信を遮断している。つまり、ポートをふさぐことによって、外部からの不正アクセスに対する安全性を確保しているのだ。しかし、これは通信の種類を限定しているということにほかならいため、新規にサーバーアプリケーションを導入する際には、しばしば「通信できない」という問題を引き起こしてしまう。

この問題は、ファイアウォールの設定でポートを開放することによって解決する。Windows XP SP2の場合は、「Windowsファイアウォール」で「ポートの開放設定」を行うか、「ネットワークアプリケーションの許可」を行う。

▼ポートを利用した通信



新たにサーバーアプリケーションを導入しようとしても、Windows XP SP2では標準でポートをふさいでいるため、アクセスできない状態に陥る。アクセスしたければ「ポート」を開放してやる必要がある。



通信を許可するためには、サーバーが利用するポート番号を指定してそのポートを開放するか、サーバーアプリケーション自体の通信を許可する設定を行う。本書では基本的に後者の「サーバーアプリケーションを許可する」設定方法で説明する（画面ではリモートコントロールサーバーを許可している）。

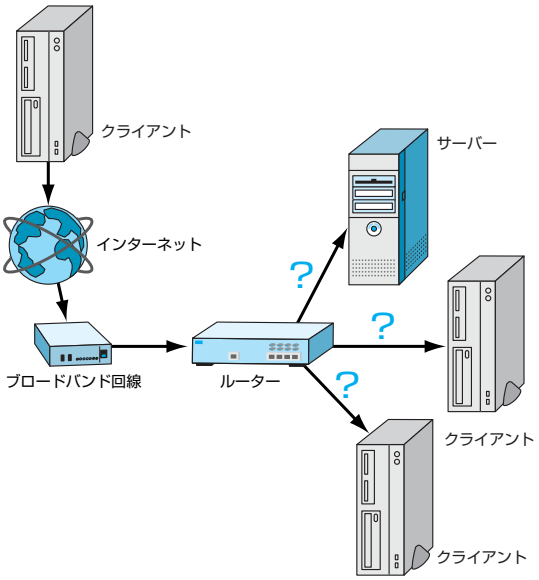
ルーターのしくみと役割

サーバーを設置するネットワーク環境にルーターを導入しているのであれば、ルーターの動作と役割を知っておく必要がある。

ルーターとは、NAT（Network Address Translation）機能を使って、1つのインターネット回線を複数台のパソコンで利用するための機器だ。この機能は自動的に処理されるため、インターネットを利用する側（Webサイトなどにアクセスするユーザー）は、特にルーターの存在を意識しなくてもよい。

しかし、ルーターに接続したパソコンをサーバーとして使う場合、問題が生じる。外部のクライアントが指定できるのはインターネット上で通用する住所「グローバルIPアドレス」までであるため、ルーターに複数のパソコンがぶら下がっている場合、クライアントから来る通信をどのパソコンに送ればよいか、ルーターが判断できなくなるのだ。

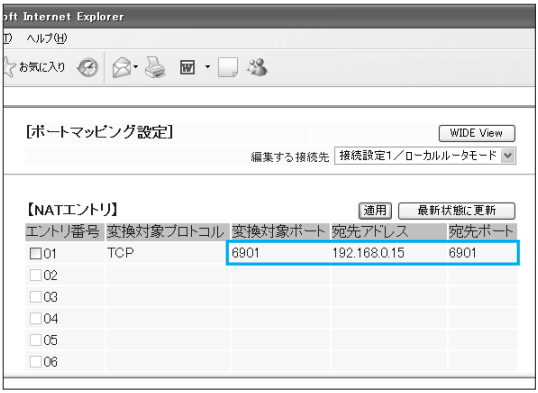
▼ルーターの通信の流れ



ルーターが存在すると送信先（パソコン）が複数あるため、相手から来た通信をどこに送信してよいかわからない。つまり、結果的に「ポートをふさいでいる」状態になる。

「クライアントからの通信をどのパソコンに送ればよいのかわからない」という状態を解決するには、ルーターに「ポート＊＊番に来たデータはパソコン＊＊へ送信せよ」という指令を設定し、通信データをサーバーに誘導する必要がある。この機能は「ポートマッピング」と呼ばれる。

▼ポートマッピング



ルーターに「ポート6901番に届いた信号をプライベートIPアドレス「192.168.0.15」のパソコンに送信せよ」という命令を設定することで、外部クライアントからの通信をサーバーに送ることができる。これが「ポートマッピング」だ。

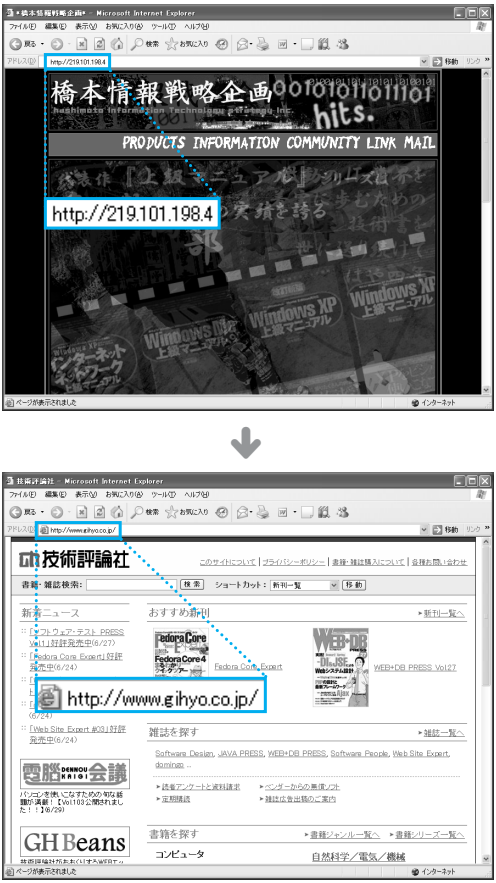
ドメイン名

インターネットを介した通信は「グローバルIPアドレス」という12桁の数字でやり取りされることは先に述べたが、実際の通信で、このグローバルIPアドレス「＊＊＊.＊＊＊.＊＊＊.＊＊＊」をいちいち入力するのは非常に面倒くさい。そのため、インターネットの世界では一般的に、IPアドレスの代わりに「ドメイン名」という文字列が使用されている。

たとえばWebサイトを閲覧する際、普通はWebブラウザに「http://www.gihyo.co.jp」などと英数字で入力するが、実はこの文字列は「グローバルIPアドレス」の代用品に過ぎない。ドメイン名として「www.gihyo.co.jp＝219.101.198.4」と登録されているからアクセスできるのであり、技術評論社のWebサイトのアドレスの実体はあくまでグローバルIPアドレス「http://219.101.198.4」である。

これを確認したければ、Webブラウザのアドレス欄に「http://219.101.198.4」と入力してみればよい。「http://www.gihyo.co.jp」と入力したときと同じ結果を表示できるだろう。

▼グローバルIPアドレスでのWebサイト表示



アドレスバーに「http://219.101.198.4」と入力してアクセスした場合でも、結果的に技術評論社のサイトが表示される。

ドメイン名には名前の付け方や登録方法など、さまざまな国際規定が設けられているが、本書の解説では「IPアドレスを文字列に置き換えたもの」とだけ覚えておけばよいだろう。ただし、**この「ドメイン」という用語は場面によって意味が大きく異なり、混乱を招くため、本書では極力利用しないことにする。**

Chapter 03

ネットワーク情報を確認&設定せよ

ネットワークの通信が「IPアドレスを住所」として行われるのは前章で述べたが、このような事情から、サーバーにするパソコンのIPアドレスやMACアドレスはしっかり確認しておかなければならない。また、ファイアウォールの設定もサーバーアプリケーション導入時には必須となる。本章ではこれらの設定と確認方法を紹介しよう。

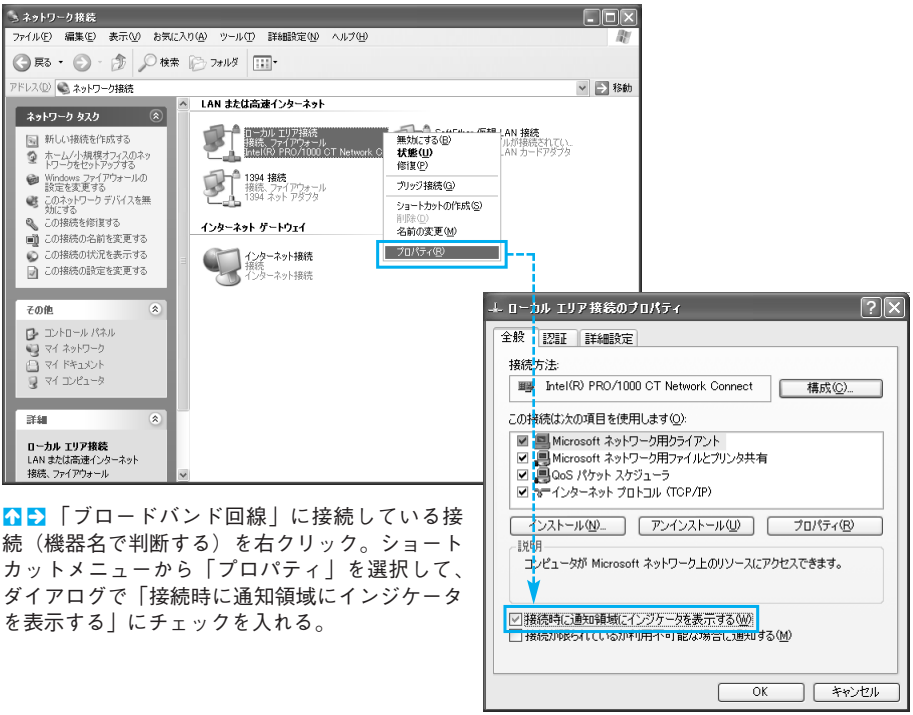
ネットワークアイコンの表示

自宅サーバーを構築するには、さまざまなネットワーク情報を確認しながら設定を行わなければならない。「ネットワーク情報の確認」にはいくつかの方法があるが、タスクバーにネットワークアイコンを表示することで、確認作業を簡略化することができる。

ネットワークアイコンを表示するには、「コントロールパネル」から「ネットワーク接続」を選択して設定する。LAN（あるいは回線）に接続しているネットワークのアイコン（通常は「ローカルエリア接続」）を右クリックして、ショートカットメニューから「プロパティ」を選択。「接続のプロパティ」ダイアログが表示されたら、「接続時に通知領域にインジケータを表示する」にチェックを入れる。

これで、タスクバーの通知領域にネットワークアイコンが表示されるようになる。このネットワークアイコンは、データ通信が行われていることをチカチカ光ることで通知してくれるほか、アイコンをダブルクリックすることでさまざまな情報を確認できる。

▼ネットワークアイコンの表示



「ブロードバンド回線」に接続している接続（機器名で判断する）を右クリック。ショートカットメニューから「プロパティ」を選択して、ダイアログで「接続時に通知領域にインジケータを表示する」にチェックを入れる。

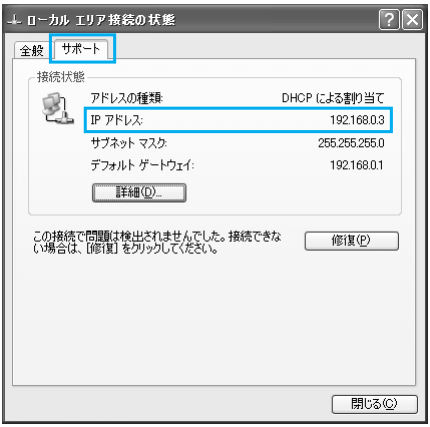
▼ネットワークアイコン

通知領域にネットワークアイコンを表示すると、回線の使用状況を確認できるほか、各ネットワーク情報の確認が手早く行える。

パソコンのIPアドレスの確認

ネットワーク上のパソコンには、必ず固有のIPアドレスが割り当てられている。パソコンに割り当てられているIPアドレスは、先ほど設定した通知領域のネットワークアイコンをダブルクリックすると確認できる。「～接続の状態」ダイアログが表示されたら、「サポート」タブをクリックすれば、「IPアドレス」欄が表示される。

▼IPアドレスの確認



各パソコンに割り当てられたIPアドレスは、通信を行ううえで重要な「住所」になる。どんなネットワークサービスも、基本的にこのIPアドレスを指定して通信を行う。

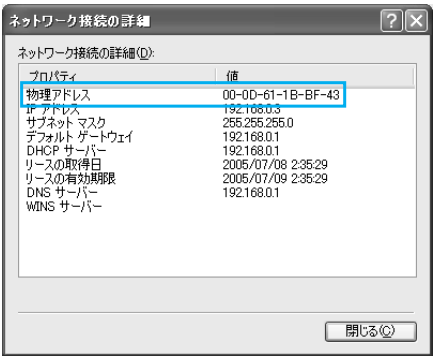
パソコンのMACアドレスの確認

MACアドレスとは、LANアダプタが持つ固有の番号のことで、「XX-XX-XX-XX-XX-XX」のような形になっている。各XXは、00～FFの数値（16進数）で示される。

MACアドレスは基本的に世界にたった1つしかない番号であるため（ただし、最近のルーターやLANアダプタにはMACアドレスを書き換えられる機種もある）、ネットワークで相手を識別するときに使用されている。ルーターは、この番号を基に、各パソコンにプライベートIPアドレスを割り当てている。

MACアドレスは、パソコンのIPアドレスと同じ方法で確認できる。通知領域のネットワークアイコンをダブルクリックし、ダイアログが表示されたら、さらに「サポート」タブにある「詳細」ボタンをクリックする。「物理アドレス」欄の文字列がMACアドレスだ。

▼MACアドレスの確認



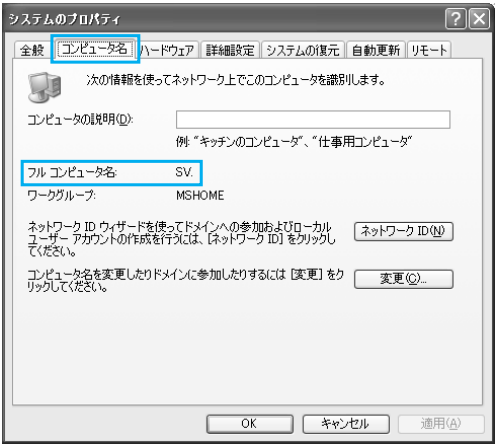
ルーターはLANアダプタの「MACアドレス」を参照し、各パソコンにIPアドレスを割り当てる。また、ルーターのアクセス制限の設定などでも、MACアドレスが使われる。

コンピュータ名の確認

ここで言うコンピュータ名とは、Windowsをインストールしたとき（または初回起動時）に入力する、パソコンの名称のことだ。コンピュータ名は、LAN内で各パソコンを識別するための情報で、ファイルの共有などさまざまな場面で利用できる。

コンピュータ名の確認は、コントロールパネルから「システム」を選択し、「システムのプロパティ」ダイアログの「コンピュータ名」タブをクリックすると知ることができる。また、ここで「変更」ボタンをクリックすることで、コンピュータ名を変更することも可能だ。

▼コンピュータ名の確認



コンピュータ名はローカルエリアネットワーク（LAN）でファイル共有やリモートコントロールなどを行う際に必須の情報になる。各パソコンのコンピュータ名は、なるべくわかりやすく簡潔な名前に整理しておこう。

コマンドプロンプトでネットワーク情報を確認する

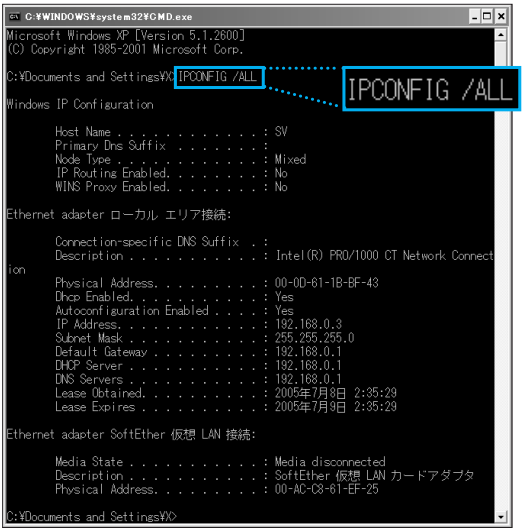
ネットワークアイコンからパソコンのIPアドレスやMACアドレスを確認することができるが、コマンドプロンプトからこれらの情報を確認する方法もある。

まず、スタートメニューから「すべてのプログラム」－「アクセサリ」－「コマンドプロンプト」と選択して、コマンドプロンプトを起動する（「ファイル名を指定して実行」から「CMD」で起動してもよい）。

コマンドプロンプトウィンドウが表示されたら、「IPCONFIG　/ALL」とコマンド入力すればよい。表示される情報の意味は、P.033の表を参照のこと。

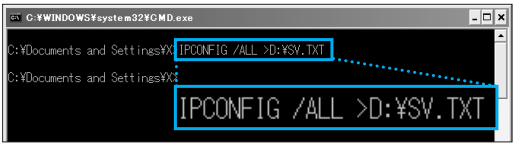
なお、この表示をテキストに出力しておきたいという場合には、リダイレクトを使用す

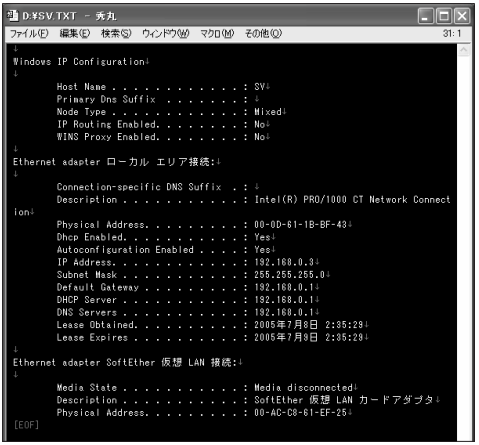
▼「IPCONFIG /ALL」で表示される画面



「IPCONFIG /ALL」でネットワークの情報を一覧表示できる。

▼テキストファイルへの保存





「IPCONFIG /ALL > [ファイル名]」と入力すると、テキストファイルにネットワーク情報を保存することもできる。

▼「IPCONFIG /ALL」で表示される情報（自宅サーバーで使うもの）

Host Name	コンピュータ名	リモートコントロールなどでの通信先の指定に使用する。
Description	ネットワークアダプタ名	アダプタを複数搭載するパソコンの場合は、この名前でどの通信に利用しているアダプタかを判別する必要がある。
Physical Address	MACアドレス	ルーターによるポートマッピング設定などで必要になる場合がある。
IP Address	コンピュータのIPアドレス	通信ターゲットの指定に使用される重要なアドレス。
Default Gateway	デフォルトゲートウェイ	ルーターを使用したLAN環境の場合、たいていこの値がルーターのIPアドレスと同一になる。

ファイアウォールの設定

ファイアウォールは、ネットワークにおいて機器間の通信を遮断する「壁」になる機能だ。各サーバーテクニックにとって、この「壁」は非常に邪魔であり、実際に、クライアントからサーバーへのアクセスが遮断されるという弊害が起こることもある。

その一方で、ファイアウォールは、外部からの不正なアクセスを防いだり、不正なプログラムによる情報漏えいを防いだりする、非常に重要な機能でもある。

そのため、ファイアウォールそのものの機能をオフにすることなく、クライアントとサーバーアプリケーションの通信だけを「許可」する設定が必要になる。

なお、本書はファイアウォールとして「Windows XP SP2の『Windowsファイアウォール』」を使用して説明する。もし、ほかのファイアウォールソフトを利用している場合は、各設定項目をそのファイアウォールのメニューに読み替えて設定してほしい。

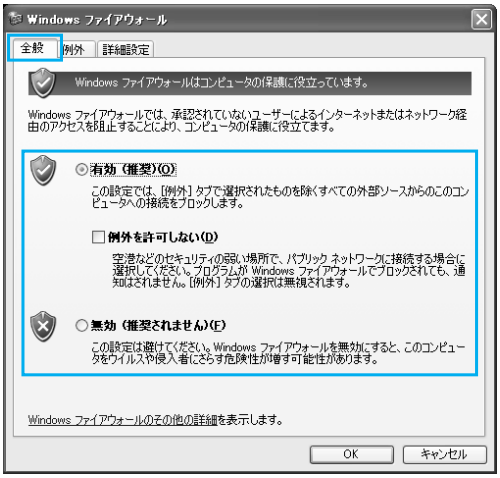
●ファイアウォールの状態確認

現在のファイアウォール設定の確認は、コントロールパネルから「Windowsファイアウォール」を選択して行う。

「Windowsファイアウォール」ダイアログの「全般」タブでは、Windowsファイアウォールがオンかオフかを確認できる。また「例外」タブでは「プログラムとサービス」欄で「通信を許可しているアイテム」を確認できる。

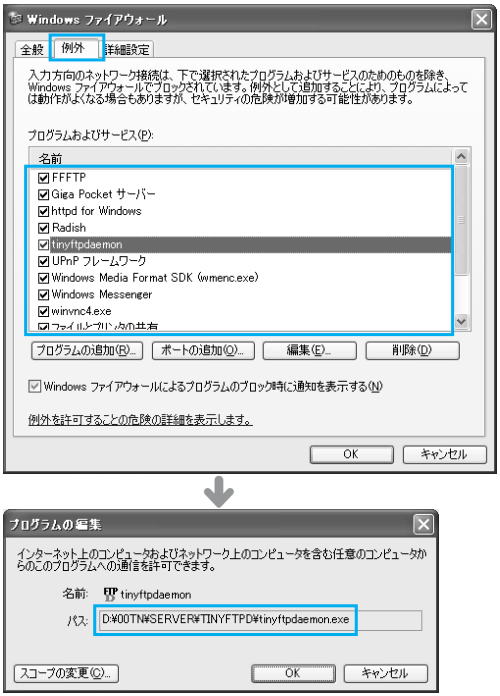
各アイテムの詳細は、アイテムをダブルクリックすることで確認できる。アイテムが「アプリケーションの許可」である場合は、許可しているアプリケーション名と実行ファイルのフルパスが、「ポート番号の開放」である場合は、開放しているポート番号が表示される。

▼Windowsファイアウォール（「全般」タブ）



「全般」タブでは「Windowsファイアウォール」設定がオンかオフか（有効か無効か）を確認できる。

▼Windowsファイアウォール（「例外」タブ）



「例外」タブでは、通信を許可しているアプリケーション（サービス）の名称を確認できる。詳細は項目をダブルクリックすると表示される。許可しているアプリケーションの実行ファイル名、あるいは許可しているポート番号を確認できる。

●アプリケーションの通信許可設定

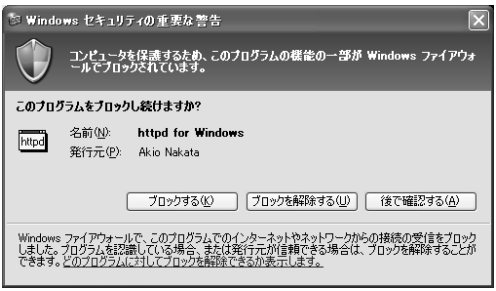
任意のアプリケーションの通信を許可する方法には、主に3つのバリエーションがある。この通信許可設定は次章以降でも解説するが、ここでは、それぞれの設定方法を簡単に説明しよう。

●アプリケーション起動時に表示されるダイアログで設定する

Windowsファイアウォールを有効にしていると、ネットワークアプリケーションが起動した際（あるいは通信を開始しようとした際）、それを検知して「Windowsセキュリティの重要な警告」ダイアログが表示される。

このダイアログで、対象アプリケーションの通信許可を設定できる。許可するのであれば「ブロックを解除する」ボタンをクリックすればよい。

▼Windowsセキュリティの重要な警告



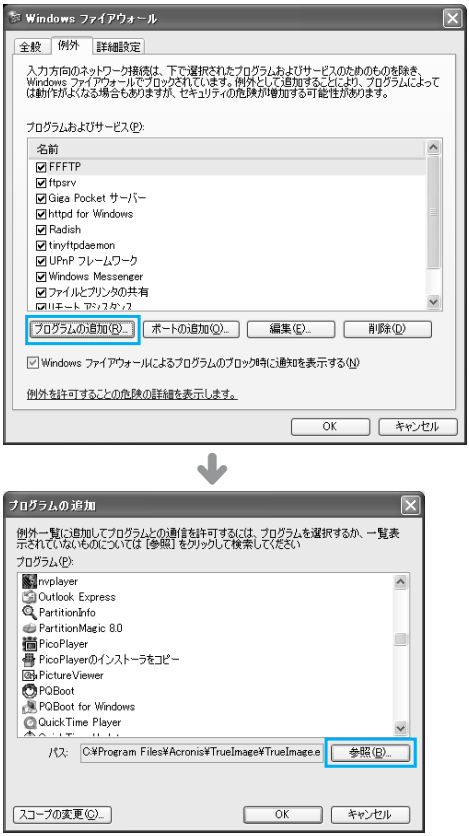
ネットワークアプリケーションが起動した際に表示されるダイアログ。このダイアログでファイアウォールの設定が行える。

●手動で任意のアプリケーションの通信を許可する

先の「Windowsセキュリティの重要な警告」ダイアログは、基本的にスタートメニューやアイコンからアプリケーションを起動したときに表示されるダイアログであり、サーバーアプリケーションが「サービス」として起動している場合には表示されない。サービスとして起動しているネットワークアプリケーションの場合は、「Windowsファイアウォール」ダイアログで許可設定を行う必要がある。

❶コントロールパネルから「Windowsファイアウォール」を選択する。
❷「Windowsファイアウォール」ダイアログの「例外」タブをクリックする。
❸「プログラムの追加」ボタンをクリックする。
❹「プログラムの追加」ダイアログの「参照」ボタンをクリックし、サーバーアプリケーションに該当する実行ファイルを指定する。

▼サーバープログラムの許可



サービスとして起動するサーバープログラムは、「Windowsファイアウォール」ダイアログの「例外」タブから「プログラムの追加」ボタンをクリックして、実行ファイルを指定する必要がある。

●手動で「任意ポート番号」を開放する

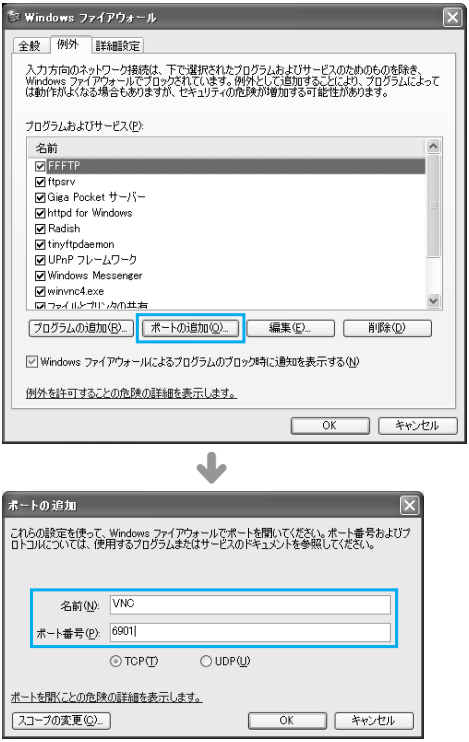
通信許可設定の3つ目のバリエーションとして、「ポートの開放」がある。

具体的には、「Windowsファイアウォール」ダイアログを表示して「例外」タブから「プログラムの追加」ボタンをクリックし、さらに「ポートの追加」ボタンをクリックして、ネットワーク通信に使用する任意のポートを開放する方法だ。

「任意アプリケーションの許可」を行う方法に対し、こちらはアプリケーションに依存せず、通信に必要なポート番号の開放のみを行う。この方法を使うと、同じポート番号を使う複数のネットワークアプリケーションの通信をまとめて許可することができる。

なお、本書では先の「任意アプリケーション」の設定で説明していくので、この設定方法は特に利用しない。

▼ポートの開放



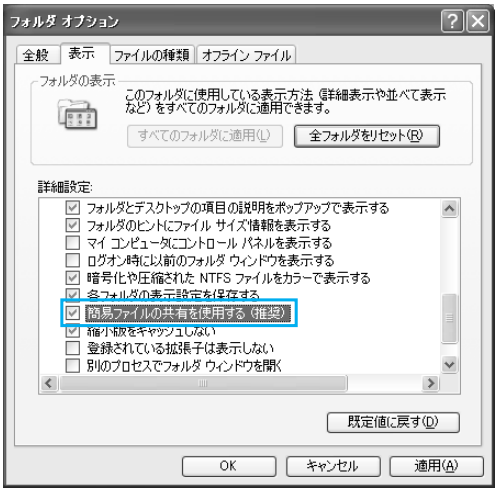
「Windowsファイアウォール」で任意のポート番号を開放する。利用するポート番号がわかっている場合に有効な設定だ。

ファイルの共有設定

自宅サーバーの構築においてファイル共有の設定は必須ではないが、サーバー環境やクライアント環境を構築する際に、ローカルエリアでファイルをやり取りする場面も多く発生する。ファイル共有（フォルダ共有）の設定をしておくに越したことはないので、ここで説明しよう。

なお、ここでは説明をわかりやすくするために、ファイル共有を提供する側の名称として、「サーバー」ではなく「ホスト」という用語を使って説明する。

▼「簡易ファイル共有」設定



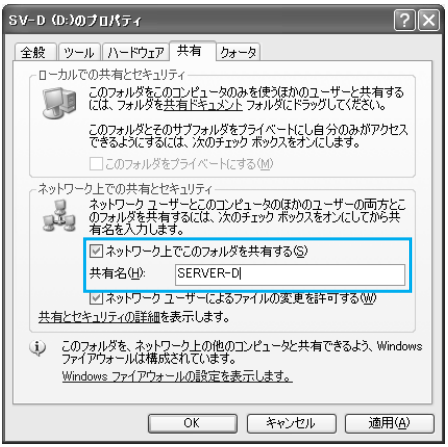
Windows XP Professionalの場合、「簡易ファイル共有」設定をオン／オフできるが、ここでは「オン」の状態でのファイル共有方法を説明する。なお、Home Editionにはこの設定はない（常に「簡易ファイル共有」が有効）。

●ファイルの共有設定　＜ホスト側＞

ネットワーク間でフォルダ共有を行うには、まず共有される側（ホスト）で、共有したいフォルダやドライブに対して「共有しますよ」と宣言する必要がある。

❶共有したいフォルダ（あるいは共有したいドライブ）を右クリックし、ショートカットメニューから「共有とセキュリティ」を選択する。
❷フォルダのプロパティで「ネットワーク上でこのフォルダを共有する」にチェックして、共有名に任意の文字列を入れる。この文字列がネットワーク上の共有名になる。
❸フォルダの閲覧だけでなく、フォルダ内部のファイル／フォルダの変更まで許可する場合は、「ネットワークユーザーによるファイルの変更を許可する」にもチェックを入れ、「OK」をクリックする。

▼ファイルの共有設定



共有したいフォルダを右クリックして、ショートカットメニューから「共有とセキュリティ」を選択、「ネットワーク上でこのフォルダを共有する」にチェックを入れて任意の共有名を設定する。

●共有フォルダに接続する　＜クライアント側＞

ホスト側で共有設定したフォルダにクライアントからアクセスするには、「マイネットワーク」を利用する。エクスプローラを起動し、フォルダツリーから「マイネットワーク」を選択すると、接続可能な共有フォルダが表示される。共有フォルダをダブルクリックすれば、内容にアクセスできる。

なお、コントロールパネルの「フォルダオプション」設定で「ネットワークのフォルダとプリンタを自動的に検索する」がオフになっている場合、共有フォルダは表示されない。

▼共有フォルダへの接続

マイネットワークを開くと、共有できるフォルダやドライブが表示される。

●共有フォルダにドライブ名を割り当てる　＜クライアント側＞

共有フォルダは、クライアント側でドライブ名を割り当てて利用することも可能だ。

ドライブ名を割り当てると、共有フォルダをローカルドライブと同じように扱うことができるため、アプリケーションのセットアップファイル等も、ローカルドライブにコピーすることなく実行することができる。

共有フォルダにドライブ名を割り当てるには、エクスプローラのメニューバーから「ツール」－「ネットワークドライブの割り当て」を選択する。「ネットワークドライブの割り当て」ダイアログが表示されるので、割り当てたいドライブ名を選択し、フォルダ欄にUNCと呼ばれる方式でネットワークのパスを入力する。UNCとは「Universal Naming Convention」の略であり、以下のような構文になる。

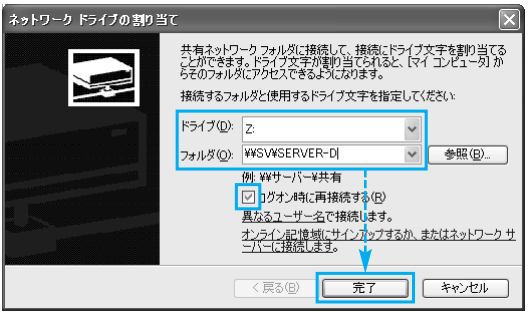
▼UNCによるネットワークパスの入力方法

¥¥[コンピュータ名]¥[共有名]

たとえば、コンピュータ名が「SV」で、共有名が「SERVER-D」の場合、パスに「¥¥SV¥SERVER-D」と入力すればよい。

この際、「ログオン時に再接続する」のチェックをオンにすると、以後パソコンを起動する度に、このドライブ名で同じ共有フォルダにアクセスできるようになる。常に使いたい共有フォルダがある場合に設定しておくと便利だ。

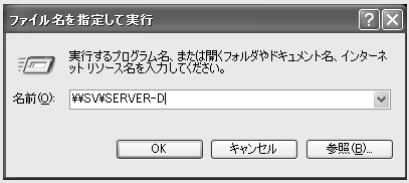
▼ネットワークドライブの割り当て



ドライブ名を選択してUNCを入力し、「完了」ボタンをクリックすれば、指定したドライブ名に共有フォルダが割り当てられる。

COLUMN 共有フォルダをすばやく開くには

共有フォルダをすばやく開きたいときは、「ファイル名を指定して実行」を利用すると便利だ。WIN+Rキーを押すと「ファイル名を指定して実行」ダイアログが表示されるので、続いてUNCを直接入力してEnterキーを押せば、共有フォルダをすぐに開くことができる。なお、一度入力したUNCはリストボックスに保存されるので、次回からはUNCを入力せずに開くことができる。



「ファイル名を指定して実行」ダイアログで、UNCを入力してEnterキーを押す。するとすぐに共有フォルダが開かれる。

Chapter 04

パソコンをリモートコントロールせよ

ここではローカルエリアに限定した「リモートコントロール」を解説しよう。パソコンからパソコンを動かすという、複数のパソコンを所有する者にとっては非常に便利なテクニックであり、ディスプレイレスマシンの構築や無線LANを利用した別の部屋のパソコンの操作、あるいは家族に内緒の「隠しマシン」を作るなど、活用方法は無限大だ。

リモートコントロールとは

自分のパソコンを他のパソコンから操作する…と書くと、さも難しいことのように思えるかもしれないが、実は技術的にはそれほど難しくない。

リモートコントロールクライアントとサーバー間での実際の通信を考えてみよう。

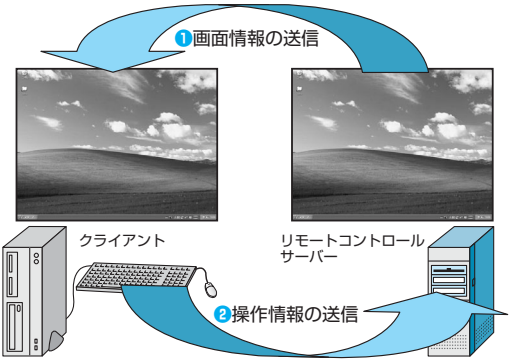
クライアントは最初に接続したとき、まずサーバー側の「デスクトップのキャプチャー画面」を送ってもらう。クライアントは以後、その画面上で操作（キーボードやマウスによる入力）を行い、その操作情報がサーバーに送られる。

サーバーは、その操作情報に基づいて実際の操作を行う。操作の結果、デスクトップ画面に差異が生じた場合、再び画面情報をクライアントに送る。

この繰り返しが「リモートコントロール」である。

このようなやりとりは、現在のLAN環境（100Base-T以上）ならば十分実用性がある。また、**インターネットを経由した場合でも、「ブロードバンド回線」であればそれほどストレスなく動かすことができるのだ。**

▼リモートコントロールのしくみ



リモートコントロールの通信では、クライアントから操作情報を送信し、サーバーから画面情報を送信しているだけだ。ネットワークへの負荷も少ないため、LANやブロードバンド回線経由であれば快適に動作する。

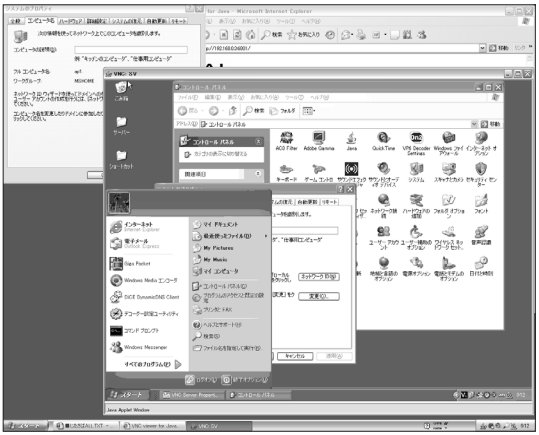
リモートコントロールソフト

リモートコントロールを実現するソフトには、無償で利用できるソフト、市販ソフト、Windows XP標準機能「リモートデスクトップ（利用するにはProfessionalが必要）」の3種類がある。無償のソフトとしては「VNC」、市販ソフトでは「Desktop On-Call」が有名だ。ここでは、無償で利用できる「VNC」をチョイスすることにしよう。

VNCは「Virtual Network Computing」の略で、Windows版以外に、Linux版やMac OS版などが用意されている。以前のバージョンに比べアルゴリズムが改善されたため、リモコンソフトとして快適に動作する。

なお、クライアントとして、「専用クライアント（VNCビューワ）」とWebブラウザの双方を利用することができる。Webブラウザを利用する場合、クライアント側に専用ソフトは必要ないため、外出先で他人のパソコンをちょっとだけ借りて遠隔操作するようなこともできる。

▼VNCの画面

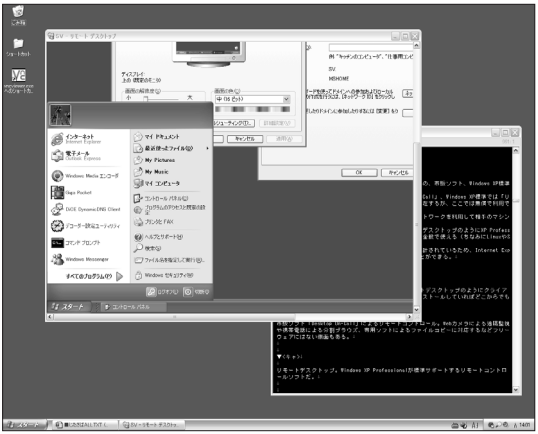


VNCは一般的なWebブラウザでコントロールできる。つまり、Windowsのリモートデスクトップのようにクライアントソフトをインストールする必要はなく、Java実行環境がインストールされていればどこからでもアクセスできる。

▼Desktop On-Callの画面

市販ソフト「Desktop On-Call」によるリモートコントロール画面。Webカメラによる遠隔監視や携帯電話によるブラウズ、専用ソフトによるファイルコピーなど、フリーウェアにはない豊富な機能を持つ（製品情報はhttp://www.ifour.co.jp/product/doc55/）。

▼リモートデスクトップの画面



リモートデスクトップ。サーバー側のOSがWindows XP Professionalでないと利用できない。また、リモコンの操作方法もかなり特殊だ。

「リモートコントロール」セットアップの流れ

リモートコントロールのセットアップは、まず「サーバー側」から設定を行う。また、サーバーアプリケーションであるVNCの設定と併せて、「ファイアウォールの設定」も必要になる。

▼「リモートコントロールサーバー」の設定ステップ

サーバーパソコンのIPアドレス（あるいはコンピュータ名）を知る（P.029参照）

↓

VNCのインストール

↓

VNCの設定（ポート番号、パスワード）

↓

ファイアウォールの設定

一方、VNCサーバーにアクセスするための方法には、2つの選択肢がある。専用ソフト（VNCビューワ）で接続するか、Webブラウザで接続するかだ。

VNC付属のクライアントソフト「VNCビューワ」を利用するのであれば、サーバー側にセットアップしたVNCと同じバージョンのパッケージでインストールを行う。Webブラウザ（Internet Explorerなど）を利用する場合はソフトウェアのセットアップは必要ないが、Javaの実行環境が必須だ。そのため、利用するパソコンによっては、Javaの入手とインストールを行う必要がある。

▼クライアントで**「VNCビューワ」**を使用する場合の設定ステップ

VNCのインストール（サーバーオプションなしでのインストール）
↓
「VNCビューワ」でVNCサーバーにアクセス

▼クライアントで**「Webブラウザ」**を使用する場合の設定ステップ

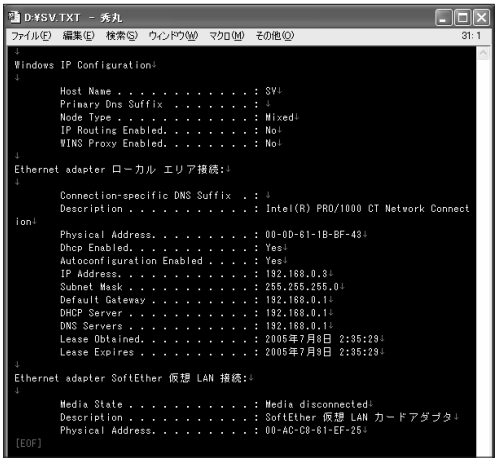
「Java」のインストール
↓
「Webブラウザ」でVNCサーバーにアクセス

サーバー

VNCサーバーのセットアップ

まず、サーバー側のパソコン（VNCをインストールするパソコン）のIPアドレスを調べておく必要がある。サーバーのIPアドレスは、すべての自宅サーバーテクニック（ビデオ配信、FTPサーバー、HTTPサーバー、メールサーバー）において必須の情報だ。IPアドレスの調べ方は、P.029参照してほしい。

▼IPアドレス

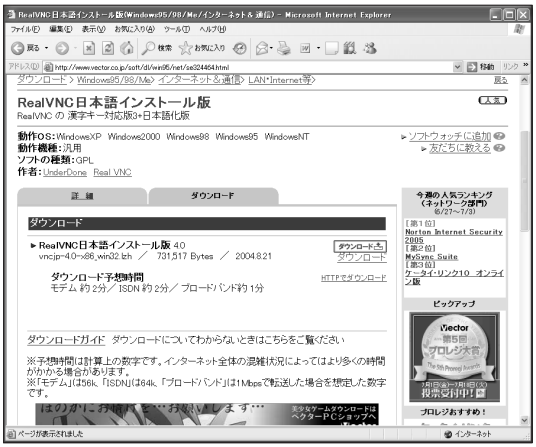


サーバー側のIPアドレス等の情報を事前に調べておく。ローカルエリア内でサーバー・クライアント接続を行う場合は、サーバー側の「プライベートIPアドレス」が必須になる。

●VNCのインストール

VNCをダウンロードし、インストールを行う。VNCにはさまざまな配布形態があるが、使いやすいのは日本語にローカライズされているバージョンだ。日本語版VNCは、「ベクター」などのダウンロードサービスで入手できる。

▼RealVNC日本語インストール版 4.0



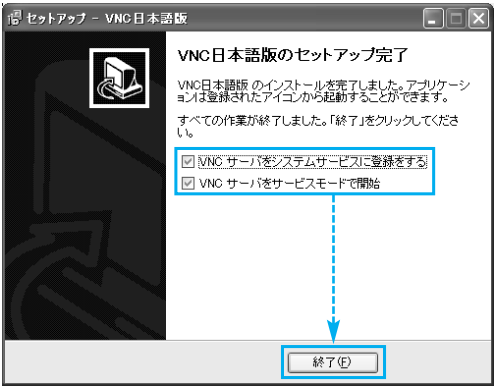
http://www.vector.co.jp/soft/win95/net/se324464.html

ダウンロードしたファイルを解凍し、セットアップファイルをダブルクリックして実行すると、セットアップダイアログが起動するので、画面に従ってインストール先などの設定を行う。最後に、「VNCサーバーを～」という項目が2つ表示されるので、サーバー側のパソコンでは双方にチェックを入れた状態で「終了」ボタンをクリックする。

なお、VNCをサーバーモードでインストールすると、VNCのプログラムが「サービス」として自動的に起動するようになる（常に起動した状態になる）。

※ダウンロードしたファイルを解凍するには、「Lhaplus」「Lhaca」などのLZH形式に対応したアーカイブソフトが必要。

▼VNCのセットアップ



セットアップの最後に「VNCサーバーを～」のチェックボックスを両方チェックして「終了」ボタンをクリックする。

●VNCサーバーの設定

VNCサーバーのインストールが完了すると、タスクバーの通知領域に「VNCアイコン」が表示される。アイコンをダブルクリックすると「VNC Server Properties」ダイアログが現れ、各種設定を行うことができる。設定が必要なのは、「接続」タブと「認証」タブの2ヵ所だ。

▼VNCアイコン

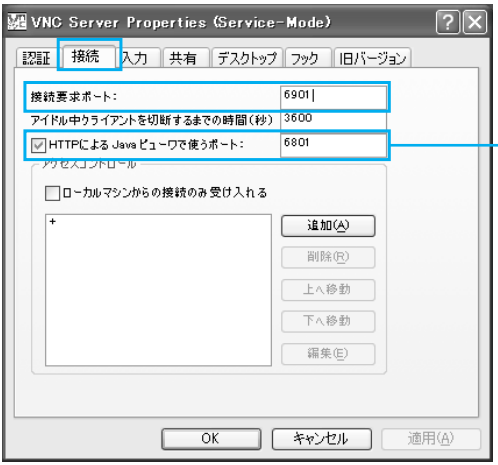
通知領域の「VNCアイコン」をダブルクリックすれば、設定が行える。

「接続」タブでは、VNCサーバーのポート番号設定を行う。この設定がVNCサーバーにおける最重要設定項目と言ってよい。中でも「接続要求ポート」は、クライアントからアクセスして、VNCサーバーを動かすために必須のポート番号だ。

このポート番号はデフォルトのまま（5900番）でもよいが、**インターネット経由での遠隔操作を視野に入れた場合、セキュリティ面を考えるなら変更しておいたほうがよい**（詳しくはP.143参照）。

また、「HTTPによるJavaビューワで使うポート」も、クライアント側からWebブラウザでアクセスする場合には必要な設定だ。Webブラウザでアクセスする可能性がある場合は、チェックしてポート番号を指定しておくこと。

▼VNCサーバーのポート番号設定

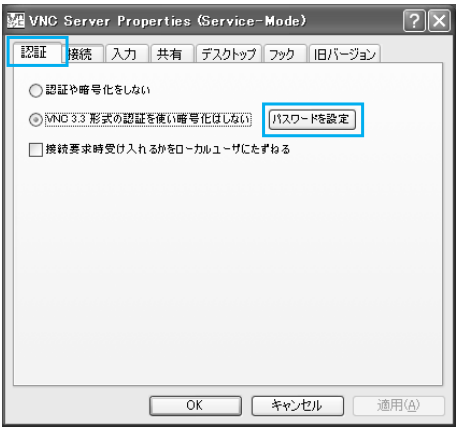


Javaアクセスを利用する場合はチェックして入力

通知領域のVNCアイコンをダブルクリックしてサーバーの設定を行う。最も重要な設定は「接続要求ポート」のポート番号だ（ここでは6901番を指定）。

「認証」タブでは、パスワード設定を行う。「パスワードを設定」ボタンをクリックして、任意の文字列をパスワードとして入力する。

▼VNCサーバーのパスワード設定



「パスワードを設定」ボタンをクリックして、任意のパスワードを入力する。

04

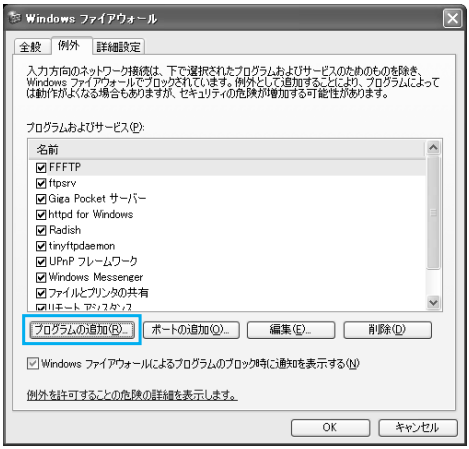
●ファイアウォールの設定

Windows XP SP2など、「ファイアウォール」が存在する環境でVNCサーバーを利用する場合は、ファイアウォールの設定を変更して「VNCサーバー」の利用を許可する必要がある。

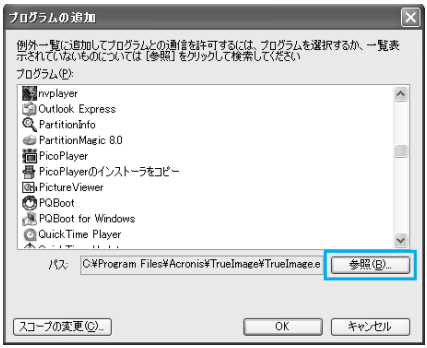
後述するFTPサーバーやHTTPサーバーの場合は、自らがネットワークアプリケーションを起動する際に「セキュリティ警告」ダイアログが自動的に表示されるので、その段階で設定を行えばよい。しかし、VNCサーバーの場合は「サービス」で起動するため、この警告が表示されない。そのため、事前にコントロールパネルで以下のように設定する。

❶コントロールパネルから「Windowsファイアウォール」を選択し、「Windowsファイアウォール」ダイアログを表示する。
❷「例外」タブをクリックし、利用許可されているアプリケーション（またはポート番号）一覧を表示する。
❸「プログラムの追加」ボタンをクリックし、「プログラムの追加」ダイアログを表示する。
❹「参照」ボタンをクリックし、VNCサーバーの実行ファイル（標準設定のままであれば「C:¥Program Files¥RealVNC¥VNC4¥winvnc4.exe」）を指定して、「OK」ボタンをクリックする。

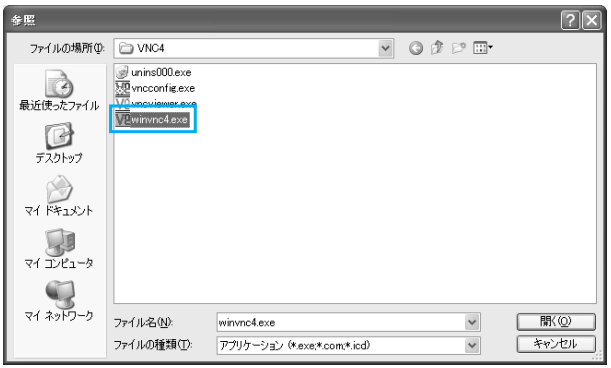
▼Windowsファイアウォール

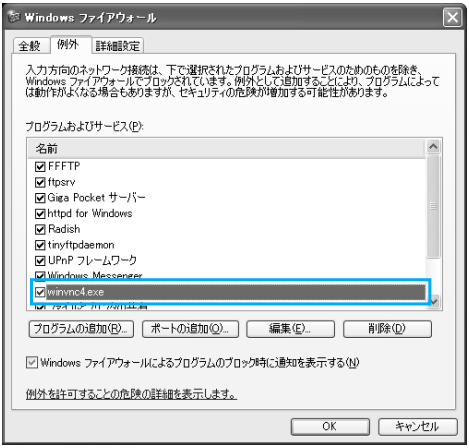


「Windowsファイアウォール」の「例外」タブ。ここの一覧においてアプリケーションが許可されていない場合には、「プログラムの追加」ボタンをクリック。



「プログラムの追加」ダイアログが表示されるので、さらに「参照」ボタンをクリックして、VNCサーバーの実行ファイルを指定する。





「例外」タブの一覧にVNCサーバーの指定が追加された。これで、クライアントからVNCサーバーへのアクセスが許可された（ファイアウォールに穴が開いた）。

クライアント

VNCクライアントのセットアップ

前述したように、クライアントからVNCサーバーにアクセスしてリモートコントロールを行う方法には、「VNCクライアントソフト（VNCビューワ）」を利用する方法と、「Webブラウザ（要Java）」を利用する方法の2通りある。ここでは双方のセットアップ手順を説明しよう。

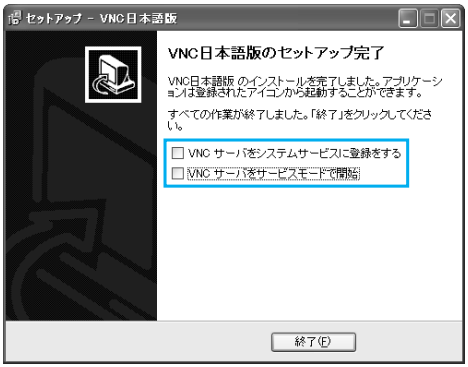
●「VNCビューワ」のセットアップ

VNCビューワを利用して接続する場合は、クライアント側のパソコンにも「VNCパッケージ」をインストールする。

クライアント側に必要なのは「VNCビューワ」だけなので、セットアップダイアログの最終画面で「VNCサーバーを～」のチェックボックスを2つともチェックオフにして、「終了」ボタンをクリックする。

インストール後、スタートメニューから「プログラム」－「RealVNC」－「VNC ビューワ 4」－「VNCビューワの起動」と選択すれば、VNCビューワが起動する。

▼VNCビューワのセットアップ



VNCビューワのみをインストールする場合は、セットアップの最後で2つのチェックボックスをチェックオフにする。なお、このようにセットアップした場合でもサーバーはインストールされる。単に、サービスとして起動しなくなるだけだ。

●「Webブラウザ」のセットアップ

WebブラウザからVNCサーバーをリモートコントロールする場合は、**「Java」が必須になる。**

Javaの実行環境は、Windowsのバージョンによってバンドル状況が異なる（コラム参照）。現在販売されている最新のWindows（Windows XP SP2）にはJavaがインストールされていないため、以下のサイトから「Java Runtime Environment（Java実行環境）」をダウンロードしてセットアップする必要がある。なお、初めからJavaを利用できるWindowsを使っている場合でも、互換性や安全性を重視するなら、このJava実行環境をセットアップしておくべきだろう。

▼Java Runtime Environmentのダウンロードサイト

http://Java.com/ja/download/manual.jsp

COLUMN Javaのバンドル状況

WindowsにおけるJavaの実行環境は「古いOSにはバンドルされているが新しいOSにはバンドルされていない」という不思議な状況になっている（これはマイクロソフトとSunの裁判による結果だ）。具体的には、Windows XP SP1まではマイクロソフト版のJava実行環境（Microsoft Java Virtual Machine）がバンドルされており、それ以降のWindows（SP1aから）では一切バンドルされていない。
なお、Windowsをアップグレードインストールした場合はこの限りではない。たとえばOS初期インストール時のOSがJavaを搭載したバージョンであれば、アップグレード後も継続してJavaを利用できる。

▼Windows XPにおけるJava実行環境のバンドル状況

Windows XP(初期)	Windows XP SP1	Windows XP SP1a	Windows XP SP2
MS-Java	MS-Java	×	×

▼Microsoft Java Virtual Machine（MSJVM）のサポート情報

http://www.microsoft.com/japan/Java/default.mspx

04

クライアント

クライアントからVNCサーバーにアクセスする

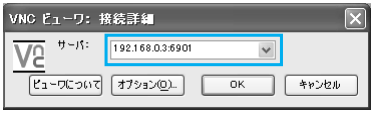
ここでは、クライアントからVNCサーバーにアクセスする手順を、「VNCビューワを使った方法」と「Webブラウザを使った方法」の2通り解説しよう。

●「VNCビューワ」によるVNCサーバーへの接続

クライアントで「VNCビューワ」を起動し、アドレス入力欄で次のように入力して「OK」ボタンをクリックする。

[サーバーのIPアドレス]:[ポート番号]
([ポート番号]は、VNCサーバー設定ダイアログの「接続」タブで指定したもの)

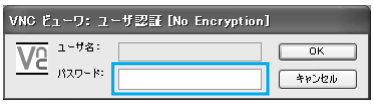
▼VNCサーバーのアドレス指定



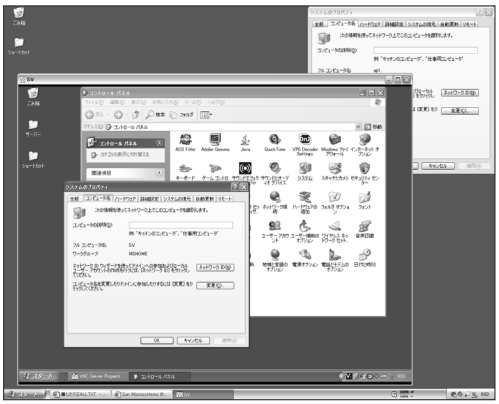
「[サーバーのIPアドレス]:[ポート番号]」という形でアクセスアドレスを指定。

次にパスワード入力画面になるので、「認証」タブで設定したパスワードを入力して「OK」ボタンをクリックすると、VNCサーバーのあるパソコンをリモートコントロールできるようになる。リモートコントロールの操作方法は、通常のデスクトップ操作と同様だ。

▼VNCサーバーのパスワード指定



正常にアクセスできればパスワード入力画面になる。パスワードを入力すれば、リモートコントロールが可能になる。

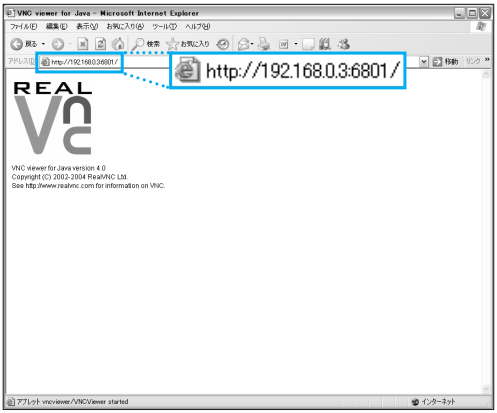


●「Webブラウザ」によるVNCサーバーへの接続

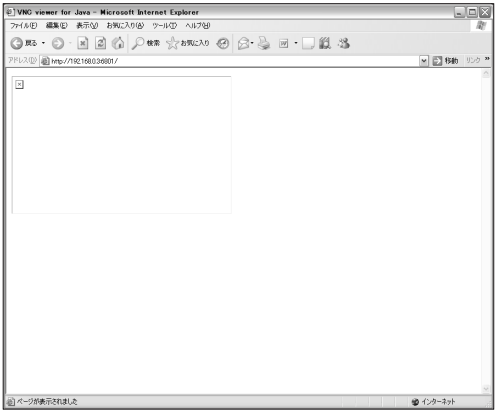
Webブラウザ(Internet Explorer等)を起動し、アドレスバーで以下のように入力し、「移動」ボタンをクリックしてアクセスする。

http://[サーバーのIPアドレス]:[Javaポート番号]
([Javaポート番号]は、VNCサーバー設定ダイアログにおける「接続」タブ内「HTTPによるJavaビューワで使うポート」で指定した番号)

▼VNCサーバーのアドレス指定



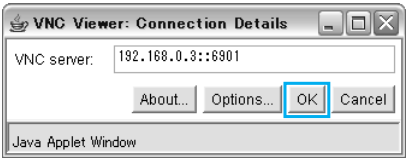
Webブラウザのアドレスバーに「http://［サーバーのIPアドレス］:［Javaポート番号］」と入力してアクセス。

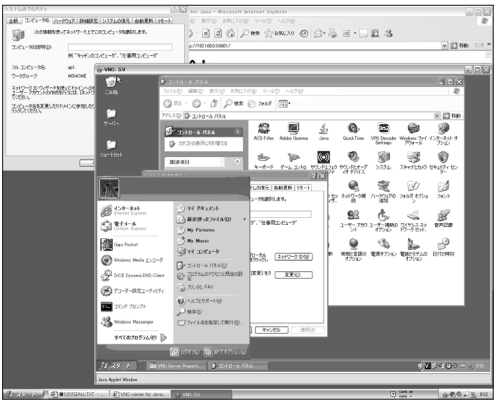


Javaがインストールされていないと、この画面が出てストップしてしまう。このような場合はJavaをインストールしてから再実行すること。

VNCサーバーに正常にアクセスできると「VNC Viewer: Connection Details」ダイアログが表示されるので、「OK」ボタンをクリックする。あとはパスワードを入力すれば、リモートコントロールを実行できる。

▼Webブラウザによる接続





Webブラウザによるリモートコントロールの実行例。外出先で他人のパソコンからアクセスしたいときなどに役立つ。

COLUMN　共有フォルダをすばやく開くには

VNCビューワでVNCサーバーに接続する際、いちいちVNCビューワを起動して、IPアドレスとポート番号を入力するのは非常に面倒だ。そこで活用したいのが、ショートカットだ。

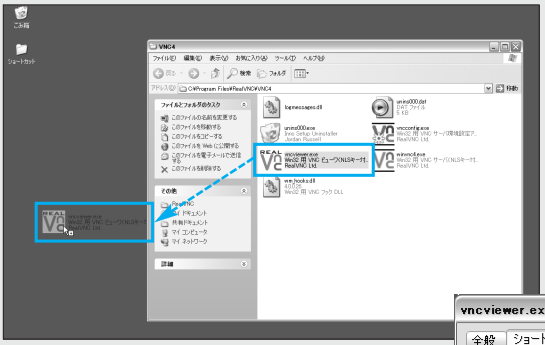
VNCビューワの本体は「vncviewer.exe（標準のインストールパスは「C:¥Program Files¥RealVNC¥VNC4¥」）」という実行ファイルなので、まずこのファイルのショートカットを作成する（ファイルを右クリックして「ショートカットの作成」をクリックする、などの方法で作成）。

次に、そのショートカットのプロパティを表示し、「リンク先」欄の「～¥vncviewer.exe"」のあとに半角スペースを入力、続けて「[サーバーのIPアドレス]:[ポート番号]」と入力する（[サーバーのIPアドレス]の代わりに[サーバーのコンピュータ名]を入力してもよい）。入力後、「OK」ボタンをクリックすれば完成だ。

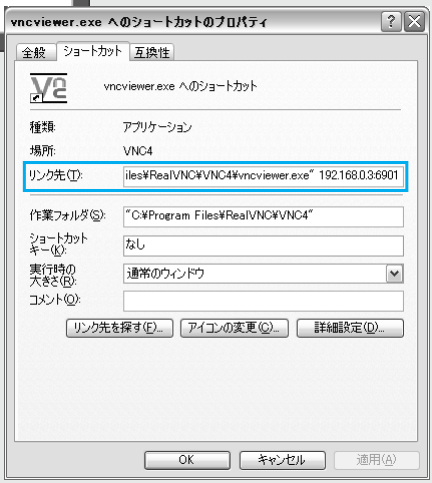
このショートカットをダブルクリックすれば、アドレスを入力せずにサーバーにアクセスできるようになる。

▼「リンク先」欄に入力する文字列（インストールフォルダが標準の場合）

"C:¥Program Files¥RealVNC¥VNC4¥vncviewer.exe" [サーバーのIPアドレス]:[ポート番号]



「vncviewer.exe」のショートカットを作成して、プロパティを開く。



プロパティの「リンク先」で「～¥vncviewer.exe"に続けて［サーバーのIPアドレス］:［ポート番号］」という形で指定する。このショートカットを作れば、簡単にVNCサーバーにアクセスできるようになる。

Chapter 05

ビデオ映像をストリーム配信せよ

ブロードバンドの普及により、動画ニュースや定点カメラ映像を配信しているWebサイトも多く見かけるようになったが、実は技術的には難しくなく、マイクロソフトが無償供給する「Windows Mediaエンコーダ」を利用すれば個人でも簡単に実現できる。この「ビデオ映像のストリーム配信」の設定とともに、動画の基礎知識についても解説しよう。

ストリーム配信とは

「ストリーム配信」と言われてもピンとこない方もいるかもしれないので、まずストリーム配信とは何か、そして何ができるのかを説明しよう。

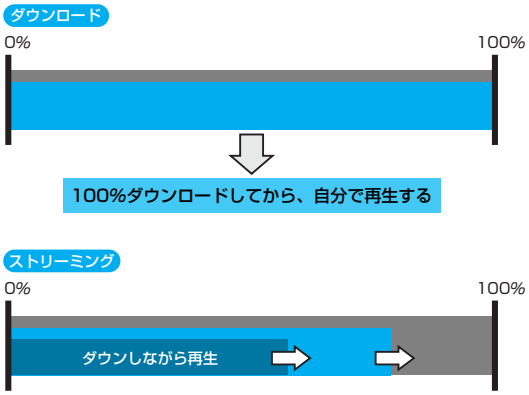
ストリーム配信とは、サーバーにある「映像や音声」をクライアントに送ることだ。ただしその際、「映像や音声」のデータはファイルの形で送られるのではなく、「ストリーミング」という方式で配信される。

たとえば、Webサイトを利用してフリーウェアなどのファイルを渡す場合、Webサイトにアップロードしたファイルをクライアント側でダウンロードしてもらう。その際、時間をかけて完全にダウンロードしないと、そのファイルを利用することはできない（映像コンテンツをこの形で置いているWebサイトも存在するが、それはストリーム配信ではない）。

一方、**「ストリーミング」を利用した配信では、ダウンロードが完了するまで待たなくても、ダウンロードしたデータを順次再生することができる。**この方式を使えば、映像ファイルを送るだけでなく、現在カメラに映っている映像やマイクで話している音声を「ファイル化しないで」配信することも可能だ。つまり、ストリーム配信とは、インターネット上で「テレビ局」を運営するようなものなのだ。

なお、ストリーミング方式でリアルタイム映像や動画ファイルを配信することは、特に「ビデオ配信」と呼ばれる。

▼ファイルのダウンロードとストリーミングの違い



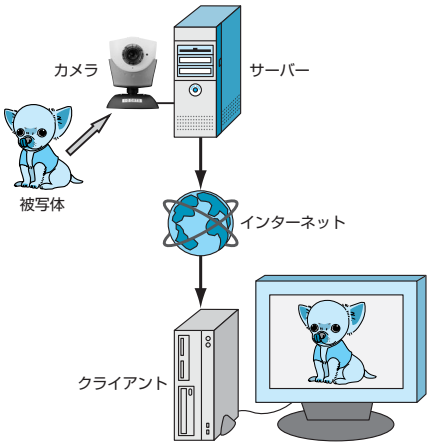
ファイルサーバーではファイルを完全にダウンロードして初めて再生可能になるが、ストリーミングサーバーでは、バッファーにたまったデータを順次再生できる。

灰　色：ファイル全体
オレンジ：ダウンロードが終了したデータ
茶　色：再生状況

▼「ストリーム配信」でできること

- ライブ映像の配信
- ライブ音声の配信
- あらかじめ作成しておいた動画の配信
- あらかじめ作成しておいた音声の配信

▼ライブ映像のストリーム配信



ストリーム配信を利用すると、サーバー側のライブ映像をリアルタイムでクライアントに配信することができる。

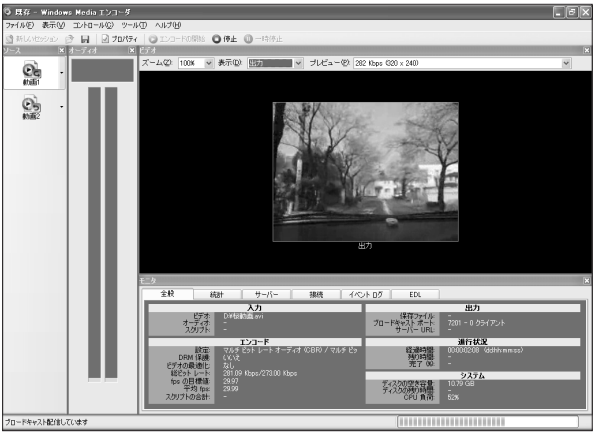
Webカメラ：アイ・オー・データ機器「USB-CAM30MS」

ビデオ配信ソフト

ビデオ配信ソフトには、「Real System Server」や「ライブカメラ Ninja for Windows」などがあるが、本書ではマイクロソフトが提供している「Windows Media エンコーダ」を紹介しよう。

「Windows Mediaエンコーダ」では、Webカメラやマイクから入力される「今の映像」や「今の音声」を配信したり、保存しておいたデジカメムービーなどを配信することができる。マイクロソフト提供ということで、Windows上での信頼性が高いのも見逃せない。

▼Windows Mediaエンコーダ



「Windows Mediaエンコーダ」。無償ながら、インターフェース、機能ともに優れている。

「ビデオ配信」セットアップの流れ

「ビデオ配信」サーバーのセットアップでは、「何を配信するか」によって用意するものが異なってくる。

自宅のライブ映像（自己アピールやペット監視など）を配信したいのであれば、その対象物を映し出すWebカメラが必要になる。デジタルカメラやデジタルビデオカメラであらかじめ撮影しておいた映像（風景や議事録など）を配信したいのであれば、その映像をキャプチャーした録画ファイルを用意しておく必要がある。

▼ライブ映像の配信

サーバーパソコンのIPアドレス（あるいはコンピュータ名）を知る（P.029参照）

↓

Webカメラのセットアップ

↓

マイクのセットアップ（音声も配信する場合）

↓

Windows Mediaエンコーダのインストール

↓

Windows Mediaエンコーダの設定（デバイス設定、ポート番号、ビットレート）

↓

ファイアウォールの確認（基本的に設定の必要なし）

↓

配信の実行

▼動画ファイルの配信

サーバーパソコンのIPアドレス（あるいはコンピュータ名）を知る（P.029参照）

↓

動画ファイルの用意（キャプチャー＋編集＋エンコード）

↓

Windows Mediaエンコーダのインストール

↓

Windows Mediaエンコーダの設定（ファイル指定、ポート番号、ビットレート）

↓

ファイアウォールの確認（基本的に設定の必要なし）

↓

配信の実行

なお、クライアント側はWindows標準プレイヤーの「Windows Media Player」で閲覧するので、特に準備が必要なものはないが、Windows XP SP2に付属しているものより新しいWindows Media Player（現時点の最新版はバージョン10）が公開されているので、インストールしておくとよいだろう。

▼Windows Media Player 最新版の入手先

http://www.microsoft.com/japan/windows/windowsmedia/download/default.aspx

▼Windows Media Player 10

Windows Media Player 10。Windows XP SP2付属のもの（バージョン9）より進化している。

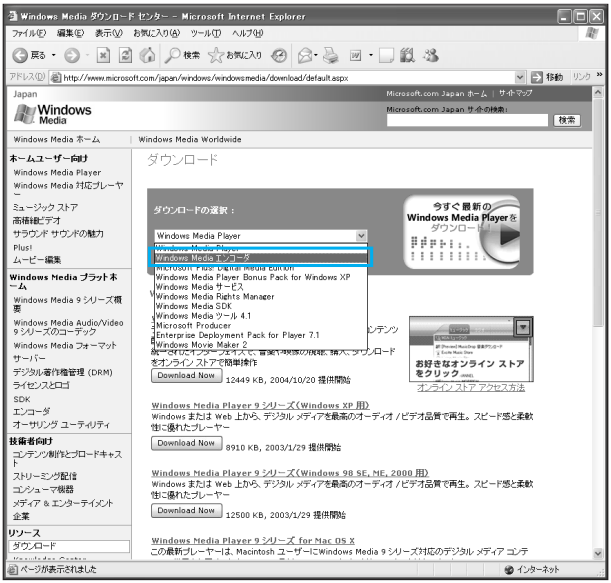
サーバー

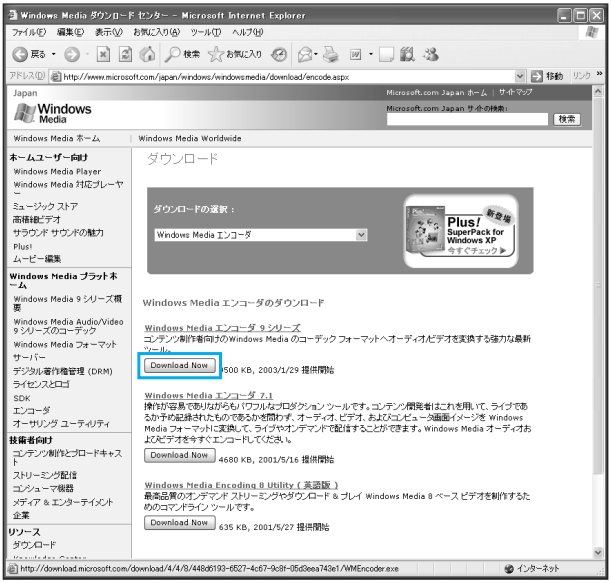
「Windows Mediaエンコーダ」のセットアップ

まずは、「Windows Mediaエンコーダ」のパッケージを以下のサイトからダウンロードし、インストールする。なお、以下のページの初期状態では「Windows Mediaエンコーダ」は表示されていない。ドロップダウンリストから「Windows Mediaエンコーダ」を選択してから、「Windows Mediaエンコーダ 9シリーズ」の下の「Download Now」ボタンをクリックしてダウンロードしよう。

● Windows Mediaエンコーダ
http://www.microsoft.com/japan/windows/windowsmedia/download/default.aspx

▼Windows Mediaエンコーダのダウンロード

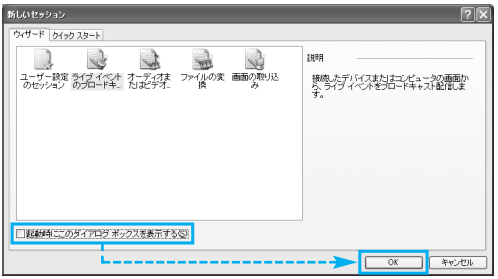




ドロップダウンから「Windows Mediaエンコーダ」を選択してから「Download Now」ボタンをクリック。

Windows Mediaエンコーダのインストール後、最初に起動すると、まず「新しいセッション」ダイアログが起動する。ただし、本書ではこのウィザードを利用しないので、「起動時にこのダイアログボックスを表示する」のチェックをはずし、「キャンセル」ボタンをクリックする。

▼「新しいセッション」ダイアログ



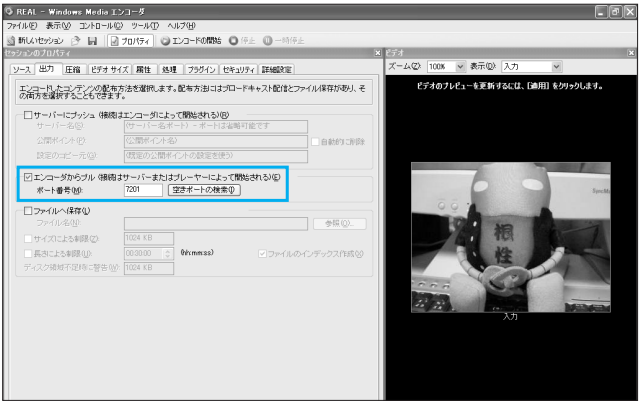
ウィザードを利用しないでも「セッションのプロパティ」ダイアログで各種設定できるので、キャンセルする。

●Windows Mediaエンコーダの「ポート番号」設定

Windows Mediaエンコーダのツールバーから「プロパティ」をクリックすると、「セッションのプロパティ」ダイアログが表示される。ここでは最低限、Windows Mediaエンコーダが利用するポート番号を指定する必要がある。

「出力」タブをクリックし、「ポート番号」欄に任意のポート番号を入力する。このとき、他のサーバーアプリケーション（デーモン）が使っている番号や「ウェルノウンポート番号（P.022参照）**」とバッティングしないよう気をつけよう。**

▼ポート番号設定



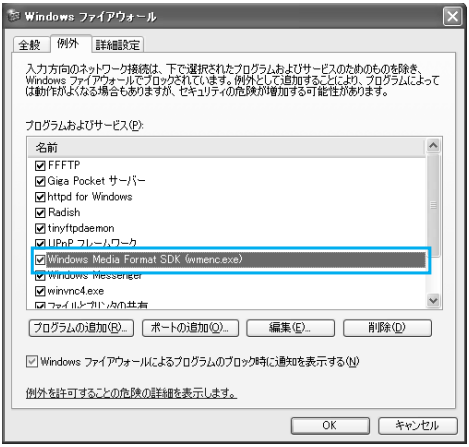
Windows Mediaエンコーダのポート番号設定。デフォルトの8080番はよく利用される番号なので、他のサーバーとバッティングしない任意のポート番号に変更する。

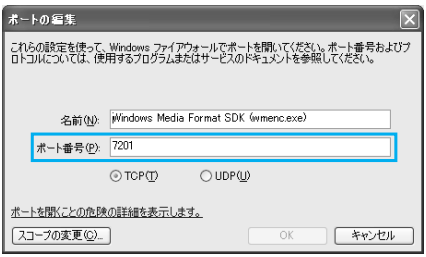
●ファイアウォールの確認

Windows Mediaエンコーダは、マイクロソフトのアプリケーションだけあって、「ポート番号の設定」を行うと、自動的にWindowsファイアウォールの設定を最適に変更してくれる。そのため、他のサーバーアプリケーションのように、手動でファイアウォールの設定を行う必要はない。

念のため、コントロールパネルの「Windowsファイアウォール」を開いて、「例外」タブ内「プログラムとサービス」欄に「Windows Mediaエンコーダ」の通信許可設定が追加されていることを確認しておこう。

▼Windowsファイアウォール





Windows Mediaエンコーダのポート番号設定は、自動的にWindowsファイアウォールに追加される（Windows Media Format SDK）。本書で解説するその他のサーバーアプリケーションの設定と異なり、「ポート番号」を解放していることがわかる。

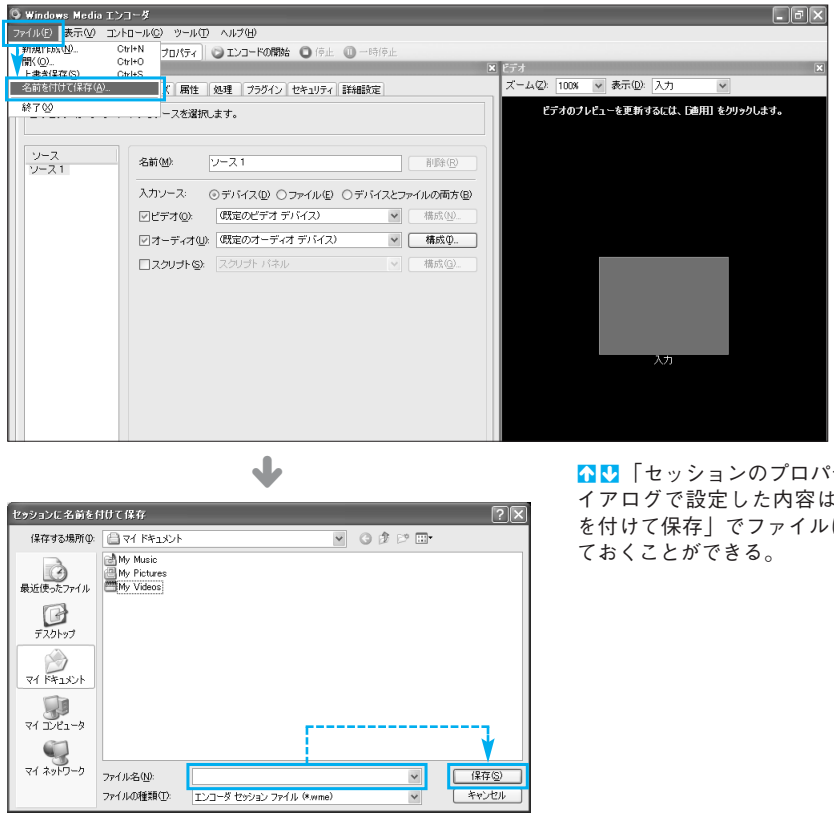
●設定をファイルに保存する

ポート番号を設定したあとは、「ライブ映像配信」か「動画ファイル配信」のいずれかのセットアップを行うのだが、その前に、この時点での設定をファイルに保存しておこう。

Windows Mediaエンコーダは他のサーバーアプリケーションと異なり、ポート番号などの設定をアプリケーション本体で保存できない。そのため、設定を変更するたびにファイルに保存する必要があるのだ。もちろん、ライブ配信や動画ファイル配信の設定・テストが終了したあとも、その設定をファイルに保存するようにしよう。

Windows Mediaエンコーダの設定をファイルに保存するには、メニューバーから「ファイル」－「名前を付けて保存」を選択し、任意のファイル名を付けて「保存」ボタンをクリックする。

▼設定をファイルに保存



↑↓「セッションのプロパティ」ダイアログで設定した内容は、「名前を付けて保存」でファイルに保存しておくことができる。

サーバー

「ライブ映像配信」のセットアップ

ライブ映像の配信を行う場合は、現在の映像をキャプチャーする「カメラ」が必要になる。DVカメラなどの本格的な製品を使うこともできるが、ストリーム配信の場合、それほど高い解像度は必要ないので、「Webカメラ」ないしは「Webカメラモードを持つデジタルカメラ」を用意するとよい。

▼Webカメラ

USB接続Webカメラ。数千円程度で購入でき、ストリーム配信用途ならば十分な解像度を持つ。

Webカメラ：アイ・オー・データ機器「USB-CAM30MS」

▼デジカメ

最近のデジカメにはWebカメラ機能を搭載しているものもあるので、これを利用してもよい。

デジタルカメラ：三洋電機「DSC-J4」

さらに、音声も配信するのであれば「マイク」が必要になる。マイクを新たに購入する際は、コネクタの形状に注意しよう。カラオケなどで使う「ボーカルマイク」のコネクタはそのままではパソコンにつながらないため、別途変換コネクタを用意する必要がある。

なお、環境にもよるが、パソコンのスピーカーを利用したままマイクを使うと、ハウリング（共鳴）を起こすことが多い。音質にこだわるのであればスピーカーをオフにし、音声をヘッドフォンで聞くとよいだろう。マイクとヘッドホンが一体化した「ヘッドセット」を利用する手もある。

▼ヘッドセット

ハウリングなどの問題を考えると、マイクを使うより「ヘッドセット」のほうが便利だ。最近のパソコンでは、ヘッドフォンは「緑」、マイクは「ピンク」と端子の色が統一されているため、その色のサウンドポートに差せばよい。

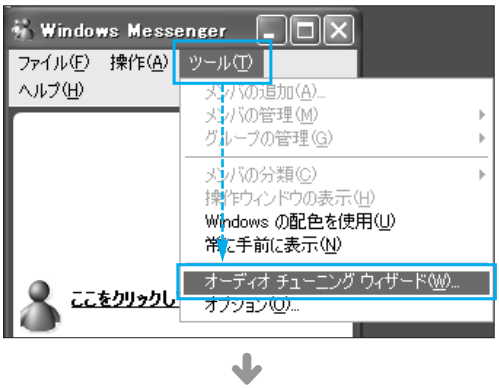
ヘッドセット：エレコム「MS-HS58V」

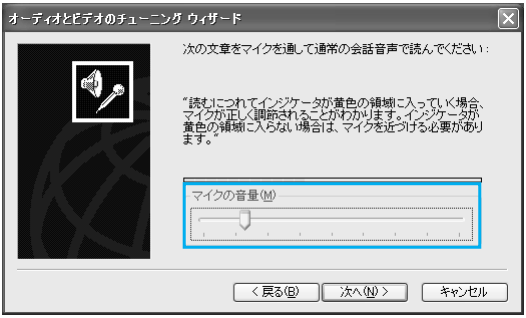
05

●マイクとスピーカーの音量調整

マイクとスピーカーの音量バランスの調整は手動で設定することもできるが、「Windows Messenger」を利用すると非常に簡単に設定できる。Windows Messengerを起動し、メニューバーから「ツール」－「オーディオ チューニング ウィザード」を選択すると、音量調整のウィザードを実行できる。

▼Windows Messengerを使った音量調整





Windows Messengerの「オーディオ チューニング ウィザード」を利用した音量調整。増幅器がついたマイクは、何も設定せずに使うと周囲を驚かすような音量が出てしまうため、このウィザードで調整するとよい。

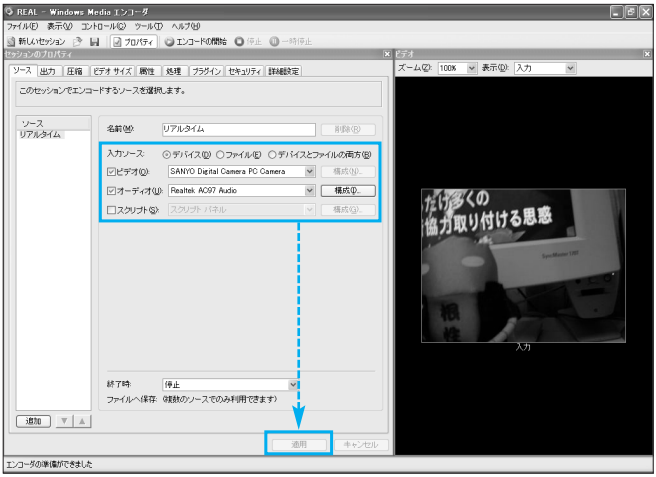
●ライブ映像（音声）の配信設定

ライブ映像（音声）の配信設定は、Windows Mediaエンコーダのツールバーから「プロパティ」をクリックし、「セッションのプロパティ」ダイアログの「ソース」タブをクリックして行う。

「名前」欄には任意の文字列を入力し、「入力ソース」欄で「デバイス」をチェックして、「ビデオ」「オーディオ」欄で利用するデバイスを選択する（デバイスが1つしかない場合は「規定」のままでよい）。設定が終わったら「適用」ボタンをクリックする。

「ビデオ」ウィンドウに現在のカメラ映像が表示されればOKだ。

▼ライブ映像（音声）の配信設定



ライブ映像（Webカメラの映像）を配信する設定。どのデバイスを利用するかを選択するだけで設定完了だ。

サーバー

「動画ファイル配信」のセットアップ

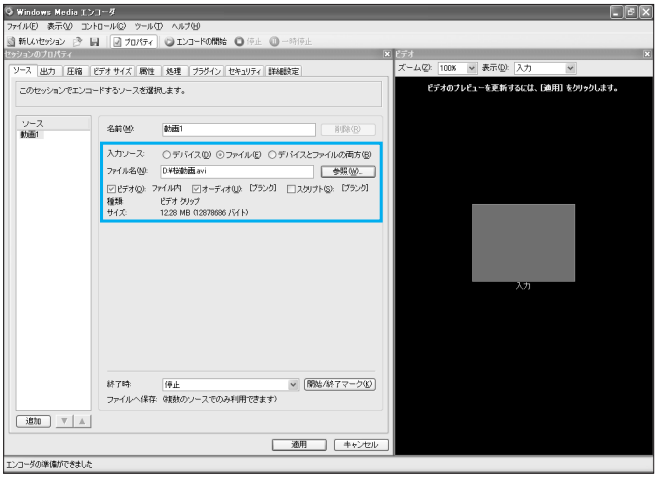
動画ファイルを配信するには、まずストリーム配信用の動画ファイルを用意しておく必要がある。

この動画ファイルはユーザーが独自に用意することになるが、このとき、**サーバーが動いているパソコンにその動画ファイルを再生できる環境、つまり動画ファイルに対応した「コーデック」がインストールされている必要がある**（コーデックについてはP.082参照）。

サーバーパソコンで再生できる動画ファイルを用意したら、Windows Mediaエンコーダのツールバーから「プロパティ」をクリックし、「セッションのプロパティ」ダイアログの「ソース」タブをクリックして各種設定を行う。

「名前」欄には任意の文字列を入力し、「入力ソース」で「ファイル」をチェック。「ファイル名」欄では「参照」ボタンをクリックして、準備した動画ファイルを指定する。

▼動画ファイルを配信する設定

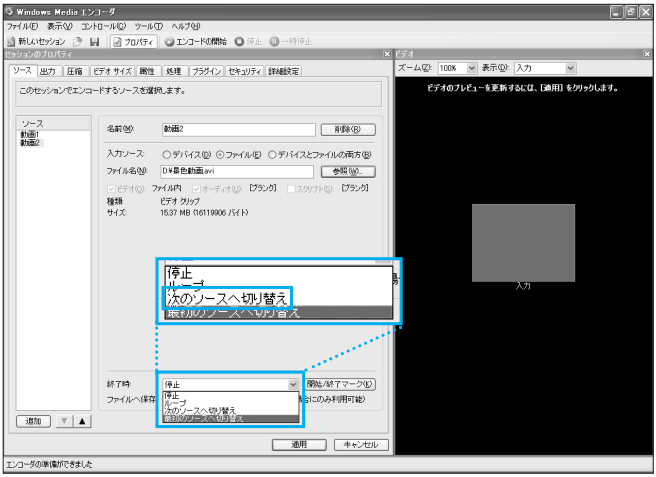


動画ファイルを配信する設定。なお、この動画ファイルはそのまま配信されるわけではなく、Windows Mediaエンコーダによって指定したビットレートに変換されたデータ（ストリームデータ）が配信される（P.080参照）。

なお、この「ソース」設定を複数登録すると、複数の動画ファイルを連続再生することも可能になる（ソースを「デバイス」にした場合でも追加は可能）。

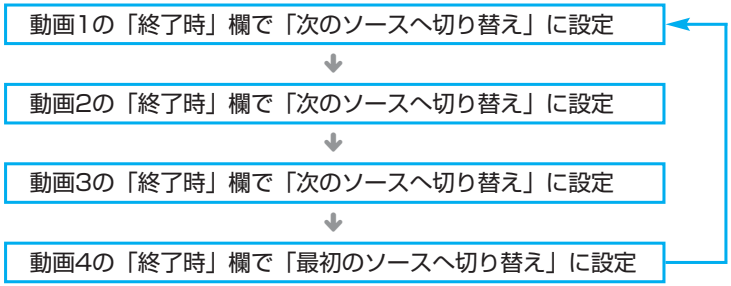
「ソース」の追加は、ダイアログ左下にある「追加」ボタンをクリックして行う。複数の動画ファイルを次々と再生したい場合は、各ソースの「終了時」欄で「次のソースへ切り替え」を選択する。さらに、一番最後に登録したソースで「最初のソースへ切り替え」を選択すると、すべての動画ファイルをループ再生することもできる。

▼複数の動画ファイルを連続再生



「ソース」を追加することで、動画ファイルを複数指定することができる。さらに「終了時」欄を変更することで、複数の動画を連続再生することもできる。

▼動画の連続再生



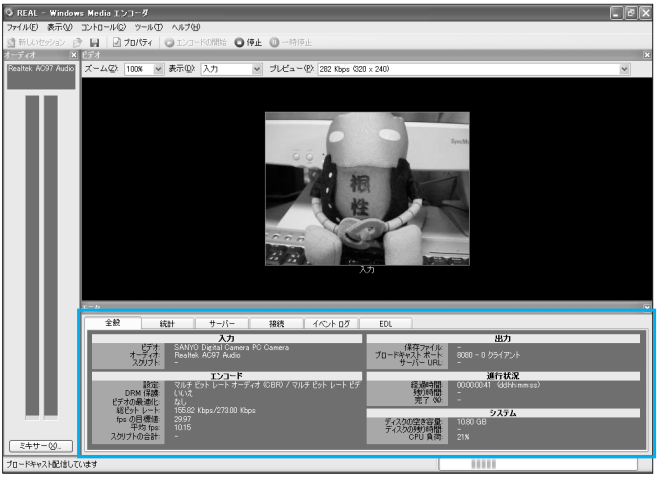
サーバー

ビデオ配信の実行

一般のサーバーの場合、サーバーアプリケーションを立ち上げておくだけでサーバーとして機能するが、Windows Mediaエンコーダによるビデオ配信では「エンコード」を実行しないとサーバー機能が開始されない。

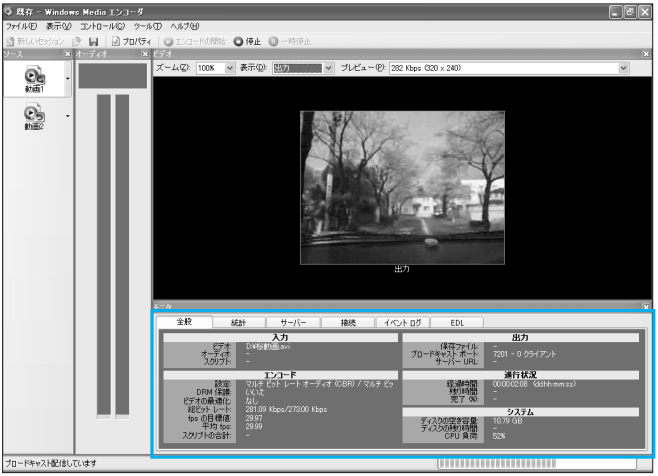
Windows Mediaエンコーダのツールバーにある「エンコードの開始」をクリックすることで、あらかじめ設定しておいたソースのストリーム配信が開始され、クライアント側で映像を閲覧できるようになる。

▼ライブ映像の配信



ライブ映像の配信設定をした場合のストリーム配信例。

▼既存動画ファイルの配信

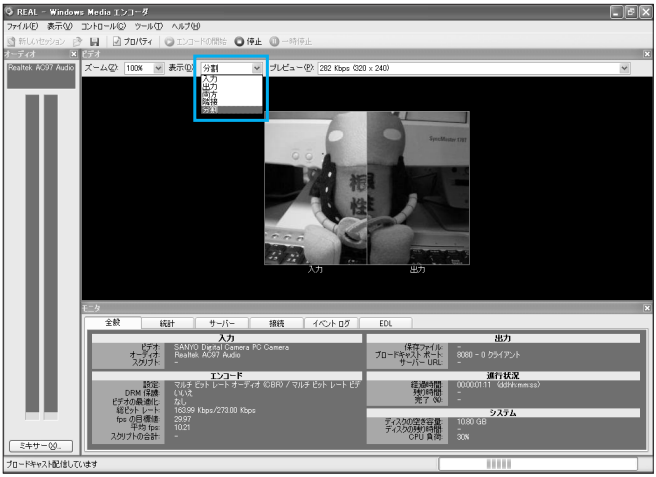


既存動画ファイルの配信設定をした場合のストリーム配信例。

サーバー機能（エンコード）の実行中は、「ビデオ」ウィンドウで再生中の映像をチェックできる。「表示」ドロップダウンボックスでは入力映像と出力映像を切り替えることができるが、「分割」を選ぶと、元映像と配信映像を同時に表示することも可能だ。

また、ソースを複数指定した場合は左側に「ソース」タブが表示され、再生ファイルを任意に切り替えることができる。

▼配信映像の表示切り替え



「表示」を切り替えることで、配信状態の確認や元動画との比較が行える。ソースを複数設定した場合は、再生するソースを切り替えることも可能だ。

05

クライアント

クライアントからビデオ配信サーバーにアクセスする

クライアント側のパソコンからビデオ配信サーバーの映像を鑑賞するには、Windows Media Playerを利用する。

Windows Media Playerのメニューバーから「ファイル」－「URLを開く」を選択すると、「URLを開く」ダイアログが表示されるので、「開く」欄に以下のURLを入力して「OK」ボタンをクリックする。

▼アクセスアドレス

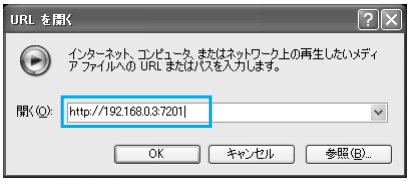
http://[サーバーのIPアドレス]:[ポート番号]

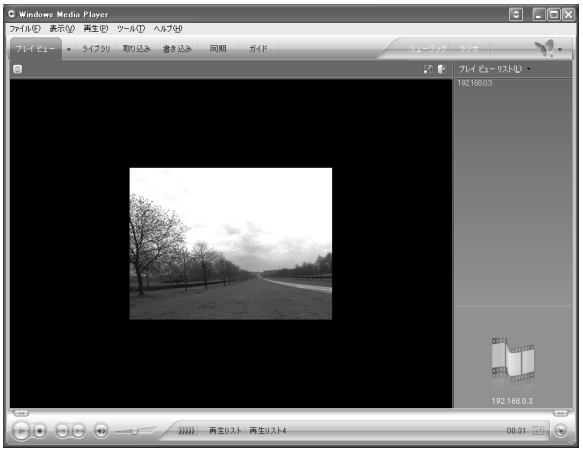
（「[サーバーのIPアドレス]」は「[サーバーのコンピュータ名]」に置き換えてもよい）

これで、サーバーが配信している映像を閲覧することができる。

なお、スキンモードなどでメニューバーが隠れているときは、右クリックのショートカットメニューやCtrl＋Uキーでも入力ダイアログを表示できる。

▼URLの入力





「URLを開く」ダイアログで、「http://［サーバーのIPアドレス］:［ポート番号］」と入力。

サーバー

Windows Mediaエンコーダの応用操作・設定

先に説明した基本的な使い方のほかにも、Windows Mediaエンコーダには便利な機能や詳細な設定項目が用意されている。ここではそれらの機能・設定を紹介しよう。

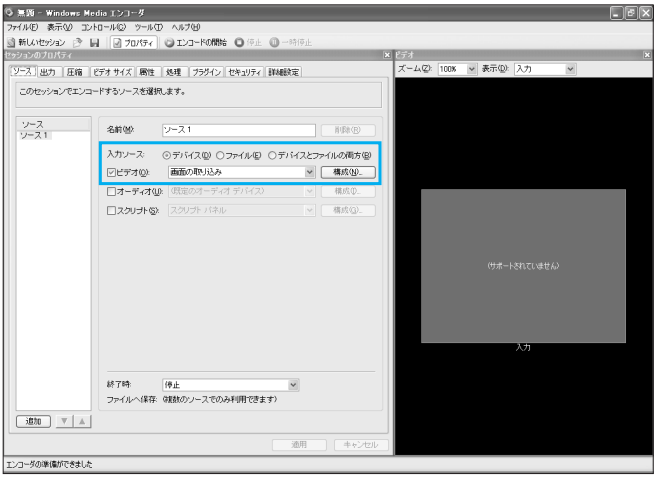
●「デスクトップ画面」の配信

Windows Mediaエンコーダでは、ライブ映像や動画ファイルだけでなく、「サーバーのデスクトップ映像」を配信することもできる。

「セッションのプロパティ」ダイアログの「ソース」タブで、「入力ソース」を「デバイス」にし、「ビデオ」欄で「画面の取り込み」を選択すればよい。この設定を行ってからツールバーの「エンコードの開始」をクリックすると、Windows Mediaエンコーダのウィンドウが最小化し、デスクトップ画面の配信が開始される。

もっとも、本書で解説している「リモートコントロール」を利用している場合は、この機能をあえて使う意味はあまりないだろう。

▼デスクトップ画面の配信



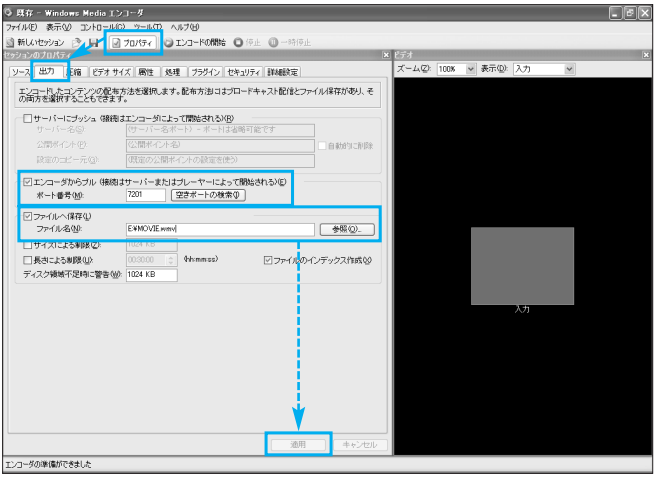
サーバーのデスクトップ画面を配信できる。パソコン画面を監視したい場合などに活用できる。

●配信映像をファイルに保存（エンコード）する

Windows Mediaエンコーダは、配信しているライブ映像をファイルに録画することもできる。ライブ映像を配信しながら、その映像を記録しておきたいときに便利な機能だ。

設定は、「セッションのプロパティ」ダイアログの「出力」タブで行う。「ファイルへ保存」のチェックボックスをチェックして、保存するファイル名を設定すればOKだ。なお、ストリーム配信を行わず、単に今のカメラ映像を動画ファイルとして保存（動画キャプチャー）したい場合は、「エンコーダからプル」のチェックボックスを外せばよい。

▼配信映像をファイルに保存



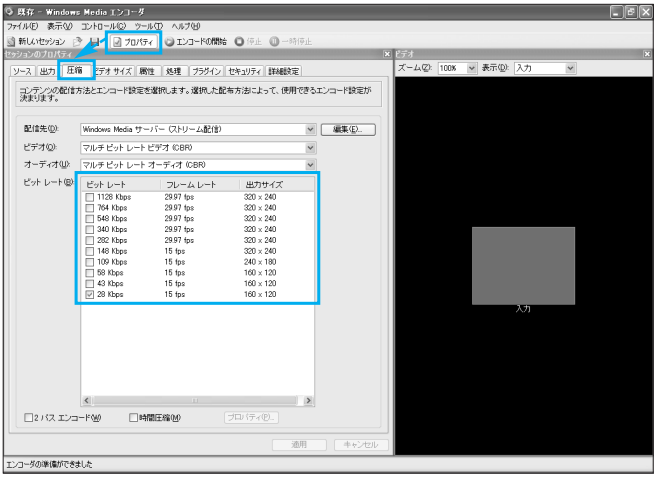
ストリーム配信している映像をファイルに保存できる。映像の録画だけを行う場合は、「エンコーダからプル」のチェックボックスを外して「エンコードの開始」をクリックする。

●配信ビットレートの最適化

ストリーム配信は、動画という「重い」データをリアルタイムに配信するので、インターネット回線にかなりの負担がかかる。**貧弱な回線では十分なデータを送れないため、映像がコマ落ちして満足に再生できなくなることもある。**このような負担を軽減するためには、配信する映像のビットレート（転送データの量）を下げる必要がある。

配信ビットレートの設定は、「セッションのプロパティ」ダイアログの「圧縮」タブで行うことができる。なお、ビットレートを低くすればするほど回線への負荷は減るが、その分動画のクオリティが落ちてしまう。使用しているインターネット回線の速度に合わせて、最適なビットレートを設定しよう。

▼ビットレートの設定



ビットレートは、画質が許容できる範囲内でなるべく下げておく。さもないと、「重すぎて」クライアント側でスムーズに再生できなくなる。

動画ファイルの基礎知識

ストリーム配信は回線に負担がかかるため、「できる限りビットレートを小さくして」送信することが重要である。また、単に小さくするだけではなく「目的に適した映像のクオリティ」も求めなければならない。この要件に対応するには、動画ファイルに対するある程度の理解が必要だ。ここでは、ストリーム配信に関係のあるものに絞って、動画ファイルの基礎知識を説明しよう。

●エンコード（Encode）とデコード（Decode）

動画に関わった際必ず出てくる言葉だが、簡単に言えば、エンコードとは「データ圧縮」、デコードは「データ解凍」である。動画をそのままファイルにすると非常に巨大なファイルサイズになってしまうため、ファイル化の際には必ず何らかの方式で小さなサイズに圧縮（エンコード）される。ファイルを再生する際には、解凍（デコード）という処理で元の動画データに戻され、画面に表示される。

このエンコードとデコードの処理は、「コーデック」というプログラムが担っている。

●コーデック（CODEC）

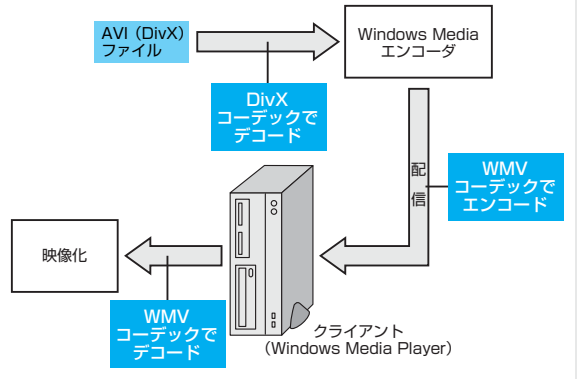
動画ファイルの再生には、「コーデック」というプログラムが必要だ。動画ファイルの種類としては、「MPEG-2」や「MPEG-4」「DivX」が有名だが、それらの動画ファイルを作成（エンコード）するときに使用したコーデックがパソコンに存在しないと、その動画を鑑賞することはできない。

たとえば、DivXで作成した動画ファイルをWindows Mediaエンコーダで配信したいのであれば、サーバーをインストールしたパソコンに「DivXのコーデック」をインストールしておく必要がある。

COLUMN　クライアント側にも動画ファイルのコーデックは必要？

「DivXで作成した動画ファイルを配信するにはサーバー側にDivXをインストールする必要がある」と説明したが、「じゃあ、クライアント側でもDivXが必要になるのでは？」と思う方もいるかもしれない。
その答えは「必要ない」だ。なぜなら、Windows Mediaエンコーダは、動画ファイルを読み込んだあと、Windows標準の「WMV（Microsoft Windows Media Video）」形式の動画ファイルに変換してクライアントに配信しているからである。
もちろん、WMV形式を再生するのにもコーデックは必要だが、「Windows Media Player」と一緒にWMVのコーデックもインストールされる（つまり、Windows XPには最初から入っている）ため、ユーザーがコーデックを意識する必要はないのだ。

▼クライアント側でコーデックが必要ないわけ



サーバー側ではWindows Mediaエンコーダで動画ファイルを読み込むために「コーデック」が必要だが、送信する際にWMV形式にエンコードしているため、クライアント側ではWindows Media Playerさえあればok。

●ビットレート（Bit Rate／bps）

ビットレートとは、1秒間に送信するデータの量のこと。単位は「bps（Bit Per Second）」で、ファイルサイズなどに使われる「Byte」ではないことに注意したい。8ビットで1バイトと同じデータ量になる。

一般的に、ビットレートの値が大きいほど（データ量が大きいほど）、配信される映像のクオリティがよくなり、ビットレートが小さいほど（データ量が小さいほど）映像クオリティは悪くなる。

ストリーム配信のような「受信と同時に再生」という方式の場合、安定した再生を実現するためには、この値が「回線速度より小さいこと」が非常に重要になる。自宅サーバー環境として一般的に利用されているADSL回線では、表記上のスペックでもアップロードは1Mbps～3Mbpsであり、実測値はこれに満たないことを考えると、ストリーム配信のビットレートは100Kbps前後を目安に調整すべきだろう。

●解像度（resolution）

解像度（動画の画面サイズ）も、動画において重要なファクターだ。

たとえば、640×480ドットの動画と320×240ドットの動画を同じビットレートで配信して「どちらがきれいか」を観察すると、320×240ドットのほうがきれいに表示されることがある。これは、前者のほうがファイルサイズが大きいため、無理にエンコード（圧縮）しすぎて画像が劣化したのが原因だ。

Windows Media Playerの場合、小さいサイズの画面も比較的きれいに拡大表示できるので、ストリーミングする映像もなるべく解像度を小さくして、劣化の少ない動画を作ることを心がけよう。

●フレームレート（frame rate／fps）

フレームレートとは、動画の再生中、1秒間に何回（何コマ）画面が更新されるかを表した値だ。通常のテレビ映像では、1秒間に30コマ（30フレーム）の映像が採用されており、映画やアニメの場合は24フレームであることが多い。

一般に、フレーム数が多い動画ほど、自然に近いなめらかな（カクカクしない）映像になるため、映像配信における理想のフレームレートも「30フレーム」だが、フレームレートが多いほど動画のデータ量も大きくなってしまう。つまり、同じビットレートでビデオ配信する場合、フレームレートと画質はトレードオフの関係になるのだ。

「ビットレート」を下げるため、あるいは映像のクオリティを維持するために、自宅サーバーのストリーム配信では「15fps」前後のフレームレートを設定するとよいだろう。

Chapter 06

FTPサーバーを構築せよ

「大きなファイルの受け渡しをしたい…」デジタルカメラで高解像度の撮影が可能になり、ビデオキャプチャーも当たり前になった今、当然起こりうる要望だ。しかし、このような「大容量ファイル」の遠距離間での受け渡しは意外と難しい。数百MBを超えるファイルはメールでは添付できず、プロバイダから割り当てられたWebエリアでも難しいからだ。そこで登場するのが「自宅FTPサーバー」だ。

FTPサーバーの活用

大容量ファイルを離れた場所にいる人にすぐに受け渡したいとき、どうしているだろうか？

昔はMOやCD-Rにファイルを書き込んでバイク便を飛ばしたものだが、今はそんなことは必要ない。ブロードバンドの普及で十分実用に耐えるようになった「FTPサーバー」を利用すればよいからだ。しかしながら、数十MB程度のデータならプロバイダのWebエリアなどをうまく利用すればよいが、1GBを超えるようなデータではサーバーの容量制限に引っかかるため、有料サーバーですら難しくなる。

そんなときは「自宅FTPサーバー」の出番だ。自宅サーバーなら、ファイル容量の制限は「自分が所有するハードディスク容量」であり、ユーザーごとにアクセスフォルダを分けることも可能になる。

もちろん、FTPサーバーを設置すれば、ファイルをダウンロードしてもらうだけではなく、アップロードしてもらうこともできる。ビジネスやホビーでのファイル交換にもってこいのサーバーが「自宅FTPサーバー」だ。

FTPサーバーアプリケーション（FTPデーモン）

FTPサーバーを実現するソフトは「FTPデーモン」とも呼称されるが、本書ではFTPサーバーアプリケーションと呼ぶことにする。Windows用のFTPサーバーアプリケーションには、「NekosogiFtpd（http://nekosogi.sytes.net/wiki/）」などがあるが、本書では「Tiny FTP Daemon」を利用したFTPサーバーの構築方法を説明しよう。

▼Tiny FTP Daemon

「Tiny FTP Daemon」。数年前に作成されたソフトだが、FTPサーバーアプリケーションとして十分な機能を持つ。

「FTPサーバー」セットアップの流れ

FTPサーバーのセットアップは、FTPサーバーアプリケーション自体の設定と、ユーザー設定の2つに分けることができる。

特に「ユーザー設定」は、今まで説明した「リモートコントロール」や「ビデオ配信」とは異なり、「複数ユーザーの管理」が重要なファクターになる。サーバーを誰にどこまで公開するのかをきちんと考えて設定する必要がある。

▼FTPサーバーの設定

サーバーパソコンのIPアドレス（あるいはコンピュータ名）を知る（P.029参照）
↓
Tiny FTP Daemonのインストール
↓
ファイアウォールの設定（Tiny FTP Daemonの起動）
↓
Tiny FTP Daemonのシステム設定（ポート番号や最大ユーザー数の設定）
↓
公開フォルダの用意（任意の空フォルダ）
↓
Tiny FTP Daemonのユーザー設定（ユーザーの作成、各種設定）

なお、クライアント側のアプリケーションは、基本的な機能だけならInternet Explorerでもよいが、現実的なFTPサーバーへのアクセスを考えると「FTPクライアントソフト」の導入が必要になる。本書では、「FFFTP」をクライアントソフトとして導入する方法を説明する。

▼FTPクライアントの設定

FFFTPのインストール
↓
FFFTPでホスト（アクセス先）を作成（設定）
↓
任意ホストでサーバーにアクセスしてファイルをダウンロード・アップロード

サーバー

Tiny FTP Daemonのセットアップ

まずサーバー側では、「Tiny FTP Daemon」のパッケージをダウンロードして、インストールする。ダウンロードしたファイルは実行ファイルなので、ダブルクリックして起動し、ウィザードに従えばセットアップできる。

● Tiny FTP Daemon

http://hp.vector.co.jp/authors/VA002682/tftpd_frame.htm

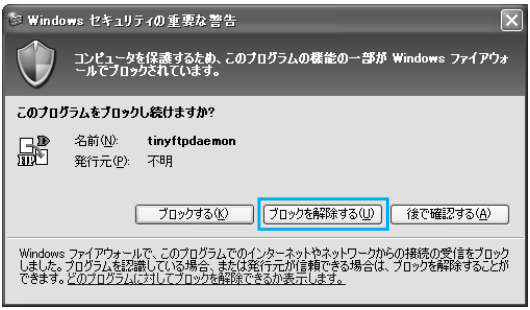
▼Tiny FTP Daemonのwebページ

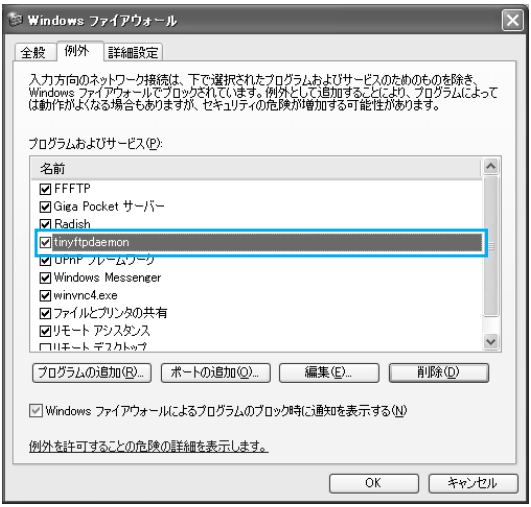
一瞬「大丈夫か？！」と思わせるWebサイトだが、ソフトの完成度は非常に高い。

●Tiny FTP Daemonの起動とファイアウォールの設定

「Tiny FTP Daemon」を最初に起動すると、「Windowsファイアウォール」が有効になっている環境ではセキュリティ警告が表示される。その場合は、「ブロックを解除する」ボタンをクリックして、通信を行えるようにしよう。このとき念のため、コントロールパネルにある「Windowsファイアウォール」の設定を開いて、「Tiny FTP Daemon」の通信が許可されているか確認しておこう。

▼Windowsファイアウォールの設定





「ブロックを解除する」ボタンをクリックして、ファイアウォールを解除する。

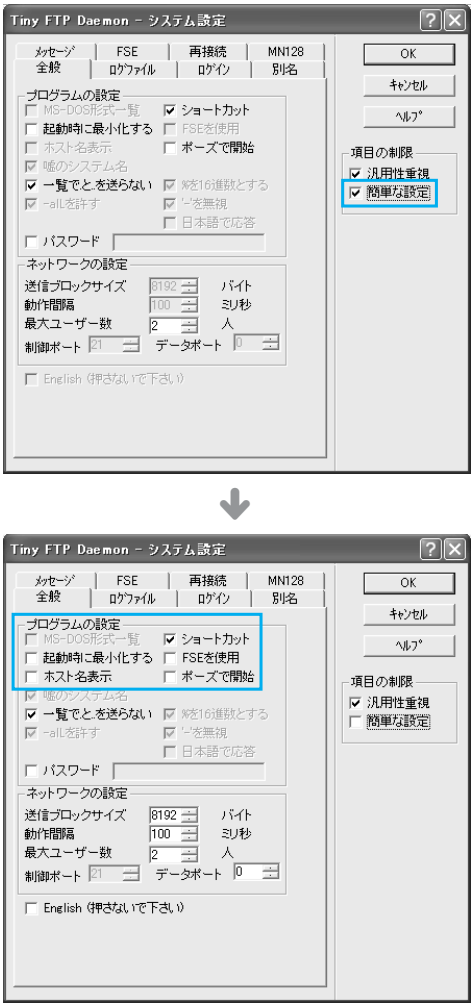
Windowsファイアウォールに例外設定があることを確認する。

●システム設定（ポート番号等）

Tiny FTP Daemonの標準設定では、絶対に必要な設定以外は設定項目がマスク（グレーアウト）されているため、まずはそれを解除する必要がある。

設定は、メニューバーから「設定」－「システム設定」を選択して行う。「システム設定」ダイアログが表示されたら「全般」タブを選択し、各設定項目を設定可能にするために、「項目の制限」欄の「簡単な設定」のチェックを外す。

▼各項目を設定可能にする

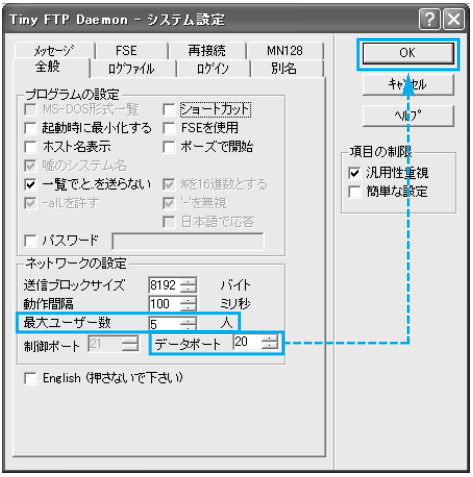


「項目の制限」欄の「簡単な設定」のチェックを外すと、グレーアウトされていた項目が設定可能になる。

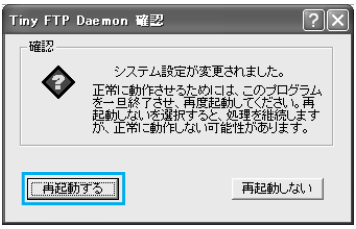
詳細設定での重要な項目は、「ポート番号」と「最大ユーザー数」だ。基本的に、**FTP通信でのデータポートは「20番」を利用することになっているので、「データポート」に「20」を入力する。**「最大ユーザー数」のほうは、デフォルトの数値では少々少ないので、ここでは「5」ぐらいを目安に入力する（各自の利用環境に応じて変更すること）。

それ以外の設定は任意だ。設定後、「OK」ボタンをクリックすると、Tiny FTP Daemonの再起動が促され、再起動すると設定が反映される。

▼ポート番号と最大ユーザー数の設定



「データポート」及び「最大ユーザー数（接続を許可する人数）」を設定。「データポート」は20番に設定するのが基本だ。



各種設定が終わると再起動が促される。この際起動はもちろん「ソフト」の再起動で、システムの再起動ではない。

06

サーバー

Tiny FTP Daemonのユーザー設定の準備

Tiny FTP Daemonに限らず、FTPサーバーのユーザー（サーバーがアクセスを許可するユーザー）は、ユーザー名とパスワード入力を求められる「認証型ユーザー」と、ユーザー認証を必要としない「アノニマスユーザー（Anonymous User）」の2つに分けられる。ここでは、このユーザー作成の際の前準備を説明しよう。

●公開用フォルダの作成

まず、これから作成するユーザーに対して公開する「フォルダ」を用意しておく。このフォルダは新規に作成してもよいし、既存のフォルダ（ダウンロードフォルダ等）をユーザー設定で「公開」に指定してもよい。

ここでは説明をわかりやすくするために、公開用に「ftpserver」というフォルダを新規作成し、この下にユーザー名と同じ名前のフォルダを作成して、各ユーザーにこのフォルダを公開することにする。

なお、「ユーザー名」と同じ文字列の「フォルダ名」は、Tiny FTP Daemonのユーザー設定でフォルダを指定する際に作成することも可能だ。

▼本書での公開用フォルダ設定

```
D:¥ftpserver
    ├anonymous
    ├[ユーザー名A]
    ├[ユーザー名B]
    ├[ユーザー名C]
    ・
    ・
    ・
```

●処理対象から除くドライブ名の指定

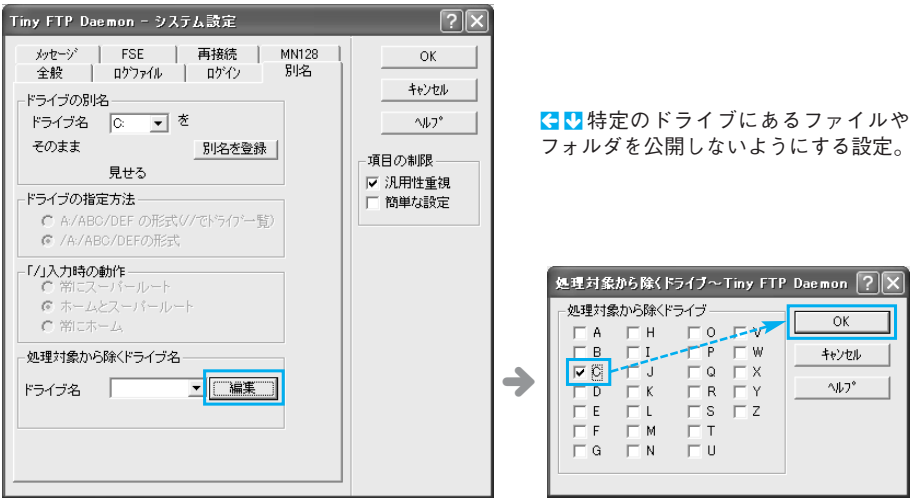
必須ではないが、「処理対象から除くドライブ名」をあらかじめ指定しておいたほうがよい。

Tiny FTP Daemonでは各ユーザーごとに公開するフォルダ（ユーザー設定時における「ホームディレクトリ」）を指定するのだが、このロケーション（場所）を指定する際、「処理対象から除くドライブ名」に指定したドライブにあるフォルダは選択できなくなる。

たとえば、本書の例のように公開用フォルダをDドライブに作成した場合は、システムドライブであるCドライブを間違えて公開しないように、Cドライブを処理対象から除くドライブ名に指定するとよいだろう。

Tiny FTP Daemonのメニューバーから「設定」－「システム設定」を選択し、「システム設定」ダイアログで「別名」タブを選択して「処理対象から除くドライブ名」欄の「編集」ボタンをクリックすると、「処理対象から除くドライブ」ダイアログが表示される。ここで公開する予定がないドライブ名にチェックを入れて「OK」ボタンをクリックすれば設定完了だ。

▼処理対象から除くドライブ名の指定



特定のドライブにあるファイルやフォルダを公開しないようにする設定。

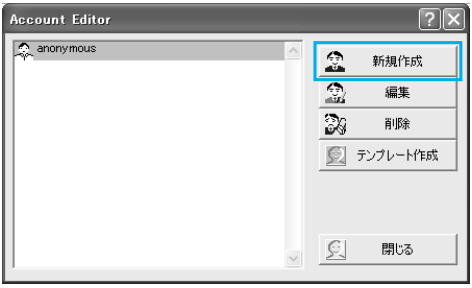
サーバー

認証型ユーザーの作成

クライアントからアクセスされた際、ユーザー名とパスワードの入力を求めるようにするには、新規ユーザーを作成して、ユーザー名とパスワードを設定する。

「Tiny FTP Daemon」のメニューバーから「設定」－「ユーザー設定」を選択し、「Account Editor」ダイアログの「新規作成」ボタンをクリックする。「ユーザー編集」ダイアログが表示されるので、ここで各種設定を行う。

▼認証型ユーザーの作成

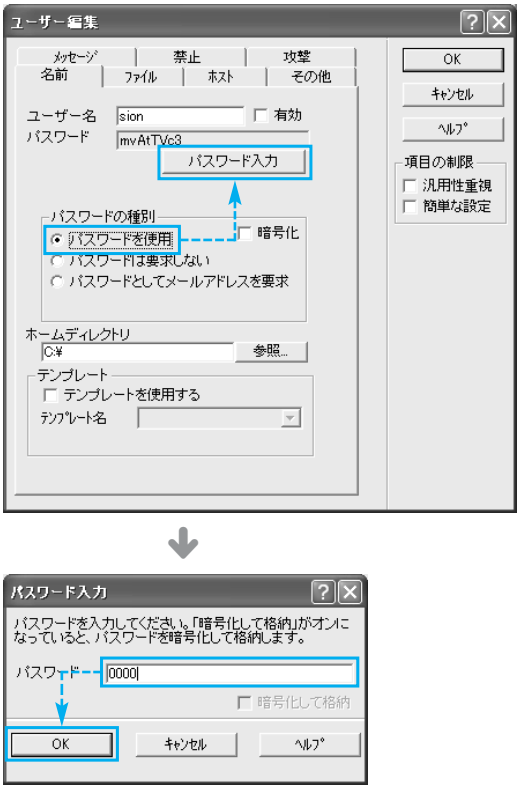


「Account Editor」ダイアログで「新規作成」ボタンをクリックすると認証型ユーザーを作成できる。

●ユーザー名、ホームディレクトリの設定

「名前」タブでは、基本設定を行う。「ユーザー名」には任意の名前を入力し、パスワードは、「パスワードの種別」欄の「パスワードを使用」にチェックを入れてから、「パスワード入力」ボタンをクリックして文字列を入力する。

▼パスワードの設定

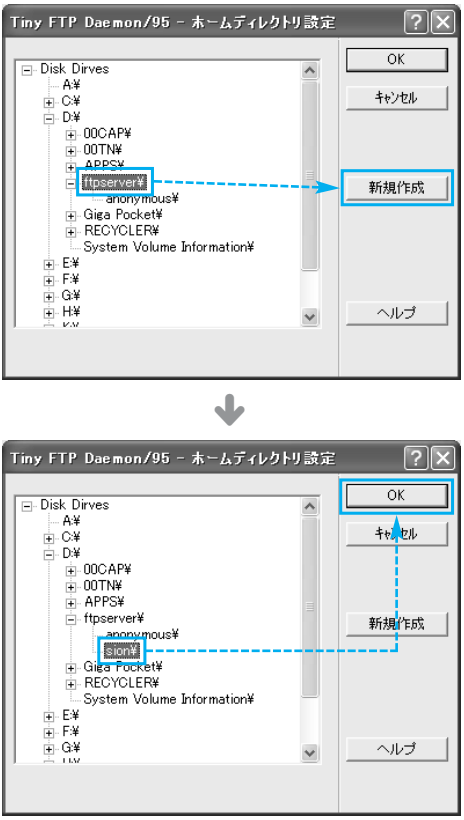


パスワードを設定するには、「パスワードの種別」欄から「パスワードを使用」にチェックを入れて、「パスワード入力」ボタンをクリックして設定する。

次に、該当ユーザーに公開するフォルダの設定を行う。

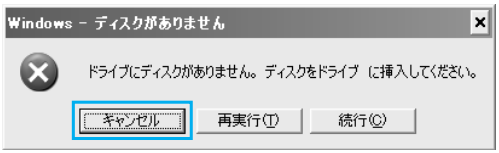
「ホームディレクトリ」欄で「参照」ボタンをクリックし、「ホームディレクトリ設定」ダイアログで公開するフォルダを指定する。ここで「新規作成」ボタンをクリックすれば、選択しているフォルダの下に「ユーザー名と同じ名前のフォルダ」を作成することができる。本書の例の場合は、「D:¥ftpserver¥」を選択して「新規作成」をクリックすればよい。

▼ホームディレクトリの設定



フォルダ指定ダイアログでフォルダを指定して「新規作成」ボタンをクリックすれば、「ユーザー名」と同じ名前のフォルダを作成できる。

▼ホームディレクトリ作成時のエラーメッセージ



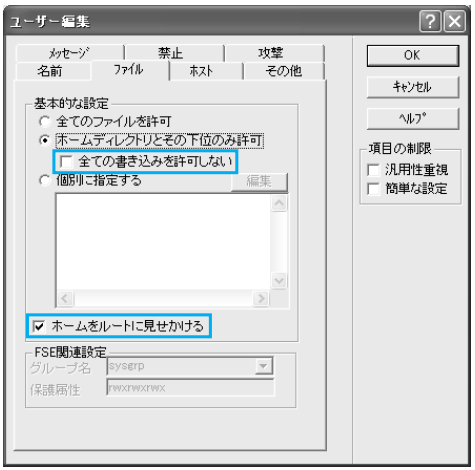
ホームディレクトリの「参照」ボタンをクリックすると、環境によってはエラーダイアログが表示されるが、「キャンセル」をクリックすれば以後正常に設定できる。

●書き込み制限などの設定

「ファイル」タブでは、指定ユーザーがログオンした際のディレクトリ表示の方法や、書き込みを許可するかどうかなどの設定ができる。

基本的に「ホームをルートに見せかける」はチェックして、「ホームディレクトリ」で指定したフォルダがログオンユーザーから「ルート」に見えるようにしよう。また、**フォルダへの書き込みを許可する場合には「全ての書き込みを許可しない」のチェックを外そう**（ダウンロードのみ許可する場合はチェックしたままにする）。

▼書き込み制限等の設定

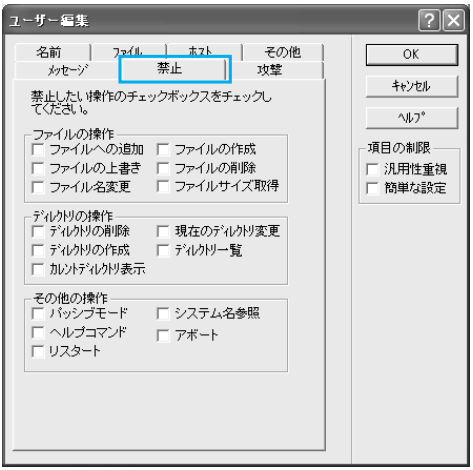


「全ての書き込みを許可しない」のチェックを外せば、クライアント側からフォルダにファイルを書き込むことも可能になる。クライアントから「ファイルを受け取りたい」ときに便利だ。なお、「全ての書き込みを許可しない」のチェックを外した上で「禁止」タブをクリックすると、「書き込み」に関する細かい設定を行うことができる。

▼書き込みの設定

- 書き込みを許可する場合
  「全ての書き込みを許可しない」のチェックを外す
- 書き込みを許可しない場合
  「全ての書き込みを許可しない」のチェックを入れる

▼禁止操作の設定



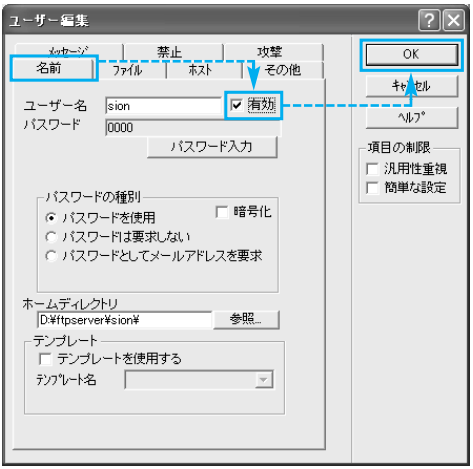
「禁止」タブでは、ユーザーの禁止操作を設定できる。「新しいファイルはアップロードしてほしいが、すでにあるファイルは改変してほしくない」といった細かい設定が可能だ。

●ユーザーの有効化

ユーザー名、パスワード、ホームディレクトリ、ファイルの書き込み許可等の設定をすべて行ったら、「名前」タブをクリックし、ユーザー名欄の横にある「有効」にチェックを入れて「OK」ボタンをクリックする。

これで、このユーザーによるサーバーへのアクセスが可能になる。

▼ユーザーの有効化



各種設定を確認して間違いなければ、「有効」にチェックを入れてユーザーを有効化する。「有効」にチェックを入れないと、このユーザーではログオンできない。

サーバー

「アノニマスユーザー」の設定

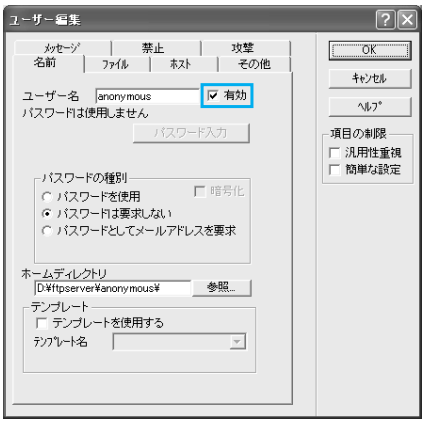
アノニマスユーザーとは、「ユーザー認証を必要としない」ユーザーのことだ。つまり、アノニマスユーザーに対しては、Webサイトにダウンロードファイルを置くようなイメージでFTPサーバーを公開することができる。**FTPサーバーにアクセスしてきた誰もが自由にダウンロードでき、そして設定によってはアップロードできるように設定することもできる。**

当然ながら「重要なファイル」や「特定の人だけに渡したいファイル」はアノニマスユーザーに公開できないので、アノニマスユーザー用のフォルダを別に作成して、そのフォルダのみにアクセス許可を与える必要がある。

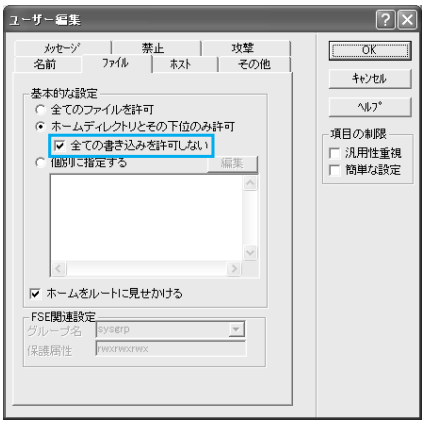
アノニマスユーザーのアクセスを許可するには、メニューバーから「設定」－「ユーザー設定」を選択する。「Account Editor」ダイアログが表示されたら、「anonymous」を選択し、「編集」ボタンをクリックして設定を行う。

「ユーザー編集」ダイアログの「名前」タブを選択して「有効」にチェックを入れ、「ホームディレクトリ」には誰にでも公開できるフォルダを指定する。ファイル書き込み制限などの設定は、先に解説した「認証型ユーザー」と同様だ。

▼「アノニマスユーザー」の設定



「anonymous」はあらかじめ用意されているが、有効にはなっていない。使用する場合は「名前」タブの「有効」にチェックすればよい。ただし、自宅サーバーでアノニマスユーザーを利用する場面はあまりないだろう。



アノニマスユーザーの設定では、特にファイルの書き込み制限や公開フォルダの指定に注意したい。

クライアント

クライアントからFTPサーバーにアクセスする

クライアント側のパソコンからFTPサーバーにアクセスする際には、複数FTPサーバーの利用やダウンロード時の利便性などを考え、専用のFTPクライアントソフトを導入したほうがよい。ここでは「FFFTP」の導入と利用方法を説明する。

● FFFTP

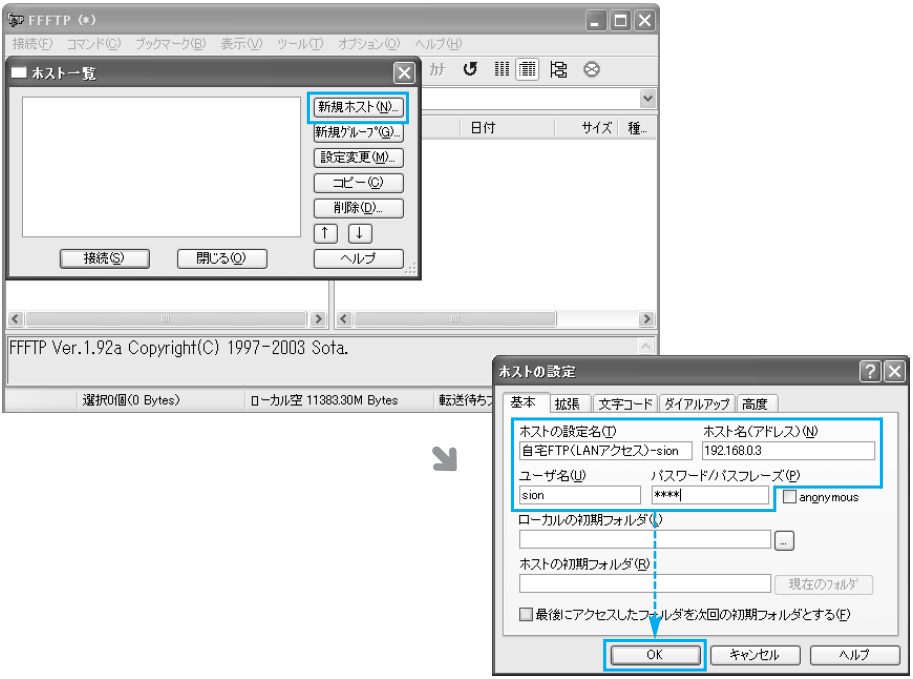
http://www2.biglobe.ne.jp/~sota/ffftp.html

FFFTPのパッケージは実行ファイルなので、ダウンロードしたファイルをダブルクリックして起動し、ウィザードに従って操作するだけでセットアップできる。

FFFTPを起動するとメイン画面と共に「ホスト一覧」が表示されるので、まずここでホスト設定（サーバーへのアクセス設定）を行う。「新規ホスト」ボタンをクリックし、「ホストの設定」ダイアログの「基本」タブでは、以下の設定を行う。

ホストの設定名	任意の名前を入力する。「ホスト一覧」に表示される名前なので「[サーバー名]-[ユーザー名]」などのわかりやすい名前をつけること
ホスト名（アドレス）	アクセス先のアドレスを入力する。LAN内のFTPサーバーにアクセスする場合は「サーバーのIPアドレス」を指定する
ユーザー名／パスワード	サーバー側で作成し、アクセスを許可した「ユーザー名」と「パスワード」を入力する

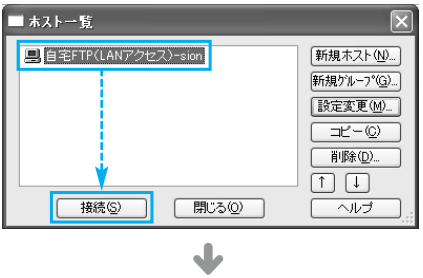
▼ホストの設定



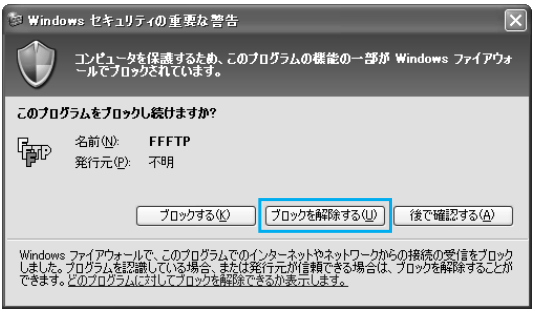
設定が終了すると「ホスト一覧」に項目が表示されるので、選択して「接続」ボタンをクリックする。設定を間違えていなければFTPサーバーに接続されるだろう。

ユーザーにアップロードを許可しているのであればファイルをアップロード、許可していないのなら公開フォルダにあるファイルをダウンロードするなどして、正常に通信できるか確認しよう。

▼通信の確認



サーバー側で作成したユーザー名でサーバーにアクセス。



クライアント側がWindows XP SP2の場合、FFFTPで最初に接続する際にファイアウォールの警告ダイアログが表示されるので、「ブロックを解除する」ボタンをクリックして通信を許可しよう(P.035参照)。

サーバー側のユーザー設定でアップロードを許可していない場合、アップロードしようとするとエラーが表示される。

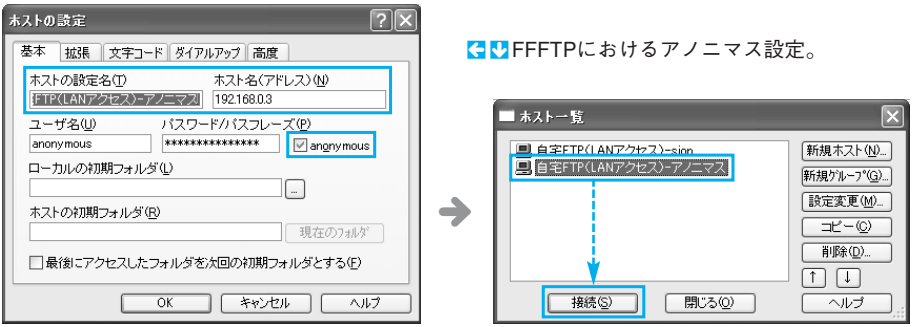
●「アノニマスユーザー」でのアクセス

サーバー側でアノニマスを有効にしている場合は、FFFTPでアノニマスユーザーを登録すれば、アノニマス接続も可能だ。

「ホスト一覧」ダイアログから「新規ホスト」ボタンをクリックし、「ホストの設定」ダイアログの「基本」タブで設定を行う。「ホストの設定名」に任意の名前(「[サーバー名]-アノニマス」など)、「ホスト名」にアクセス先のアドレスを入力し、「anonymous」のチェックボックスにチェックを入れれば登録完了だ。なお、サーバー側で「anonymous」にパスワードを設定した場合は、パスワードも入力する。

作成が終わったら、アノニマスユーザーを選択して、「接続」ボタンをクリックする。

▼「アノニマスユーザー」の設定



FFFTPにおけるアノニマス設定。

COLUMN Internet ExplorerでFTPを利用する

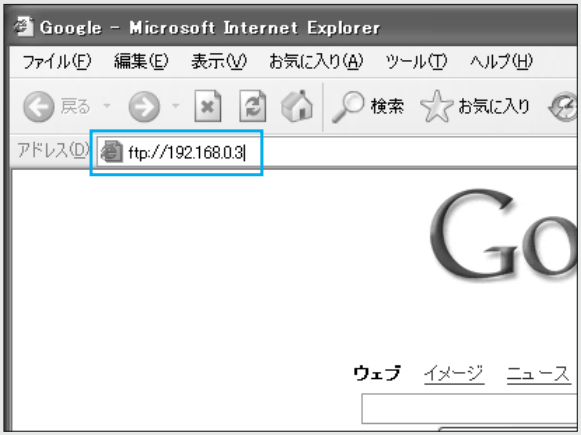
FTPサーバーを利用するときは専用のFTPクライアントソフトを利用するのが当たり前、という認識があるが、実はInternet ExplorerもFTPクライアントとして立派に動作する。

操作は簡単で、FTPサーバーのアドレスをアドレスバーに入力するだけだ。ただし、FTPサーバーであることを自動認識してくれないので、アドレスバーには以下のように入力する必要がある。

▼アドレスの入力方法

ftp://[サーバーのIPアドレス]

▼アドレスの入力

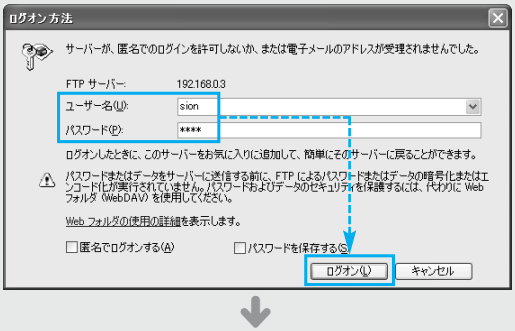


アドレスバーには、「ftp://」に続いてサーバーのIPアドレスを入力する。

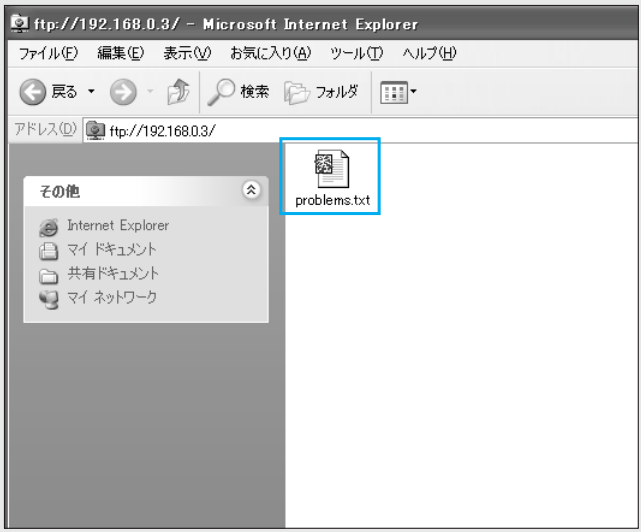
FTPサーバーにアクセスするとユーザー名とパスワードの入力が促されるので、入力して「ログオン」ボタンをクリックすればよい（アノニマスユーザーでログオンする場合は「匿名でログオンする」にチェックを入れる）。

他人のパソコンなど、FTPクライアントソフトを利用できない環境では、Internet Explorerを試してみるとよいだろう。

▼Internet ExplorerによるFTPサーバーへのアクセス



Internet ExplorerによるFTPサーバーへのアクセス例。外出先で人のパソコンを借りてアクセスする場合などで役立つだろう。



サーバー

Tiny FTP Daemonの応用操作・設定

Tiny FTP Daemonでは、クライアントが接続しているときの操作やユーザー設定など、先に紹介した以外にもさまざまな活用法が用意されている。ここでは、それらの一部を紹介しよう。

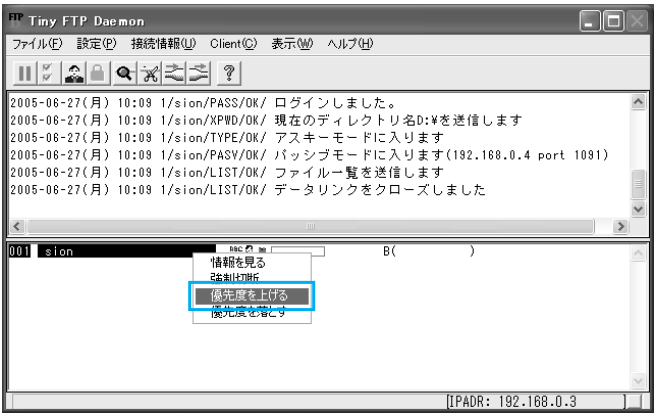
●アクセス中にクライアントとの接続スピードを上げる

サーバーとクライアントの接続速度をアップしたければ「優先度」を上げればよい。

アクセス中のクライアントの優先度をアップするには、サーバー側（Tiny FTP Daemon）で接続ユーザーを右クリックし、ショートカットメニューから「優先度を上げる」を選択する。

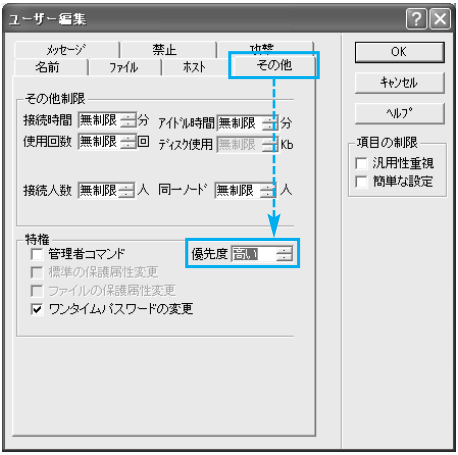
なお、Tiny FTP Daemonの「ユーザー編集」であらかじめクライアントの「優先度」を高くしておくこともできる。

▼優先度の設定



「優先度を上げる」で、クライアントとの接続スピードをアップできる。ただし、回線速度の限界を超えることはできない。

▼特定ユーザーの優先度設定



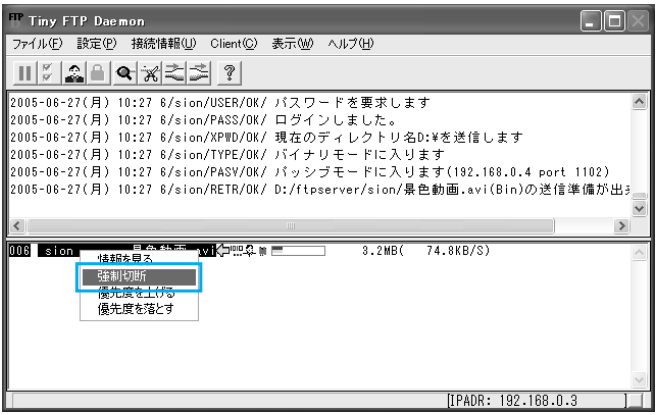
特定ユーザーの「優先度」を常に高くしておきたいときは、「ユーザー編集」の「その他」タブの「優先度」で指定する。

●ユーザーの強制切断

現在サーバーに接続しているユーザーの接続を強制切断したい場合は、接続ユーザーを右クリックしてショートカットメニューから「強制切断」を選択する。

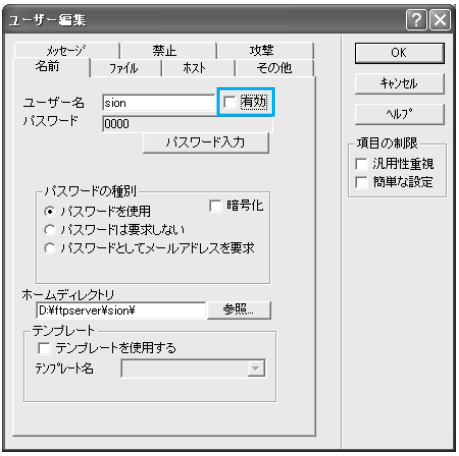
このとき、クライアントからの要求でサーバー上のファイルをクライアントに送信（クライアントから見た場合の「ダウンロード」）しているときに強制切断を行った場合、ダウンロード途中の不完全なファイルがクライアントに残される。

▼ユーザーの強制切断



「強制切断」で現在接続中のユーザーを強制的に切断できる。

▼ユーザーごとのログオン許可設定



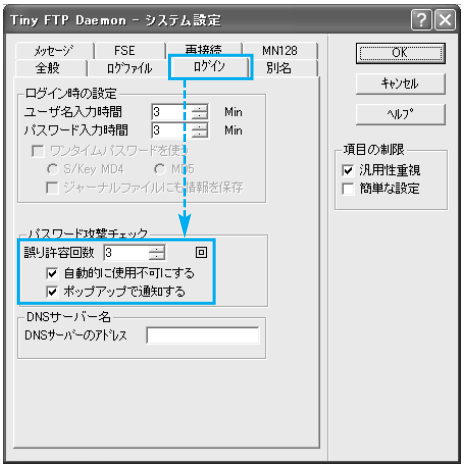
以後そのユーザーのログオンを許さない場合は、ユーザー編集で「有効」のチェックを外せばよい。

●パスワードの誤り許容回数の設定

悪意を持った第三者の侵入を防ぐため、ユーザーのログオン時に「＊回パスワードを間違えたらログオンできなくなる」設定を行うことも可能だ。この設定は「システム側（全ユーザー共通）」と「ユーザーごと」で個別に指定することができるが、通常はシステム側で一括して設定してしまったほうが便利だろう。

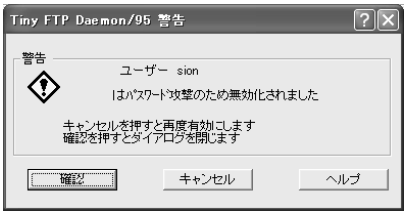
メニューバーから「設定」－「システム設定」を選択し、「システム設定」ダイアログの「ログオン」タブをクリック。「パスワード攻撃チェック」欄の「誤り許容回数」に回数を設定（通常は3〜6回）し、許容回数を超えた場合の動作を指定する。「自動的に使用不可にする」にチェックしておけば、**ログイン時に許容回数を超えてパスワードを間違えたユーザーは強制的に無効になる。**

▼パスワードの誤り許容回数の設定



誤り許容回数の設定。パスワードをランダムに生成するアタックプログラムへの対策だ。

▼パスワード使用不可の警告



「ポップアップで通知する」をチェックしておけば、誤り許容回数を超えたときに警告ダイアログが表示される。

Chapter 07

HTTPサーバーを構築せよ

HTTPサーバーとは、いわゆる「Webサーバー」のこと。無料Webスペースやプロバイダ供給のエリアが存在する以上、自宅サーバーでHTTPサーバーを立ち上げることは無意味なように思えるかもしれないが、容量が事実上無制限で、好きなようにCGIを作成できるというメリットがある。本章ではCGIを利用できる、HTTPサーバーのセットアップ方法を紹介しよう。

HTTPサーバーのしくみと活用

HTTPサーバー（Webサーバー）とは、作成したWebページを自分のパソコンの中に置いて、これをインターネット上の誰からも閲覧できるようにする環境のことだ。

このHTTPサーバーが他のサーバーと大きく異なるのが、「個人利用の場面を考えにくい」ということだ。リモートコントロールであれば会社－自宅間などのプライベートな操作、FTPサーバーであれば自宅パソコンの個人的なファイルを外部からダウンロード、などの場面が考えられる。しかし、Webページの場合は基本的に「他人に見せる」ために作成するものであるため、「立ち上げっぱなしのサーバー」が必要になる（他のサーバーは利用するときだけ起動していればよい）。

はっきり言ってしまえば、いろいろな人に見てもらいたいWebページを公開するのであれば、プロバイダから割り当てられたWebページエリアにWebページをアップロードしたほうがよいだろう。常時パソコンを起動しておく必要もないし、FTPを利用すればどんなパソコンでも管理できるからだ。

あえて「自宅HTTPサーバー」を利用するメリットを考えると、まず「容量が事実上無限」であることが挙げられる。プロバイダから割り当てられる個人Webスペースは多くても数GB程度だが、自宅HTTPサーバーであればハードディスクの空き容量がそのまま利用できる容量になるので、事実上無限のエリアがある。高解像度写真や長時間映像などの巨大なデータをコンテンツにしたい場合には大いに役立つだろう。

また、「CGI」の制限がないというメリットもある。プロバイダによっては、CGIに大きな制限（利用する数や重さ）を設けていることが多いが、自分のパソコンで動かすのであれば何を動かすのも自由というわけだ。

その他のメリットとして、「ローカルネットワークで動作テストできる」という点もあるだろう。自作のWebページをアップロードする前にCGI動作を含めて動作を確認できるというのは大きなメリットだ。

▼自宅HTTPサーバーのメリットとデメリット

	自宅サーバー	プロバイダーのWebスペース
容量	事実上無限	有限（多くても数GB）
CGI	どんなCGIも利用可能	制限有り
管理のしやすさ	自宅サーバーを常に稼動させる必要がある	どこからでも管理できる
作動テスト	LANでテスト可能	アップロードしないとテストできない

HTTPサーバーアプリケーション（HTTPデーモン）

HTTPサーバーを実現するソフトは、「HTTPデーモン」とも呼ばれるが、本書ではHTTPサーバーアプリケーションと呼称することにする。

HTTPサーバーアプリケーションでは「Apache（http://www.apache.org/）」が有名だが、本書では最初からWindows用として開発されており、使いやすい「AN HTTPD」を使用することとする。なお、HTTPサーバーはサーバーを動かしっぱなしにするため、**他のサーバーアプリケーション以上に「セキュリティ」に神経質になる必要がある。そういう意味でも常に「最新版」のアプリケーションを利用するようにしたい。**

さらに、CGI（Perl）を利用するのであれば別途Perlをセットアップする必要があるが、本書では「ActivePerl」を選択するものとする。

▼AN HTTPD

「AN HTTPD」はHTTPサーバーアプリケーション。認証Webページなども設定可能だ。

▼ActivePerlのインストール

自宅HTTPサーバー環境でCGIを利用したいなら、「Perl」をインストールする必要がある。

「HTTPサーバー」セットアップの流れ

HTTPサーバーの場合、ポート番号や最初に開くファイル名などのルールが決まっているので、「AN HTTPD」のインストール後に必ず変更しなければならない項目はない。

しかし、初期設定では作成Webページを「AN HTTPD」本体フォルダに配置するようになっているので、これは別のフォルダに変更したほうがよい。また、CGIを利用するのであれば、別ソフトのインストールを行う必要がある。そしてもちろん、Webページを表示するために「HTMLで記述したテキストファイル（HTMLファイル）」を用意する必要がある。

▼HTTPサーバーの設定

サーバーパソコンのIPアドレス（あるいはコンピュータ名）を知る（P.029参照）
↓
AN HTTPDのインストール
↓
ファイアウォールの設定（AN HTTPDの起動）
↓
作成Webページを置くフォルダの指定（ドキュメントルート）
↓
ユーザー認証の設定（ユーザー任意、設定しなくてもよい）
↓
作成Webページをドキュメントルートに配置

▼CGIを利用する場合

ActivePerlのインストール
↓
AN HTTPDでCGIを置くロケーションの設定
↓
CGIファイルの用意
↓
CGIファイルの改変（Perlの指定）
↓
所定位置にCGIファイルを置く
↓
作成したWebページ（HTMLファイル）でCGIを指定

サーバー

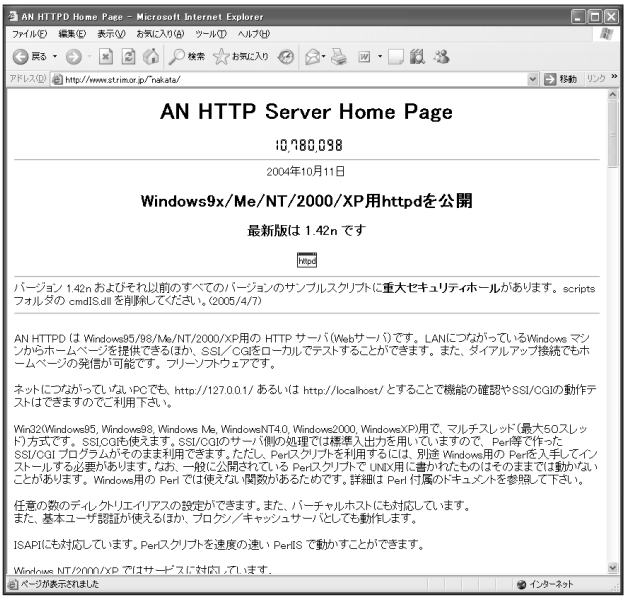
AN HTTPDのセットアップ

まず、「AN HTTPD」をダウンロード、インストールする。

「AN HTTPD」はさまざまなWebサイトでダウンロードできるが、最新版を利用したほうがよいので、公式ホームページからダウンロードしよう。

なお、ダウンロードパッケージにはZIP形式とEXE形式の2種類あるが、EXE形式ファイルの場合、実行時に指定したフォルダに直接AN HTTPDの構成ファイルが解凍される。そのため、あらかじめAN HTTPDを解凍するフォルダを、管理しやすい場所に作成しておくとよいだろう。

▼AN HTTPD

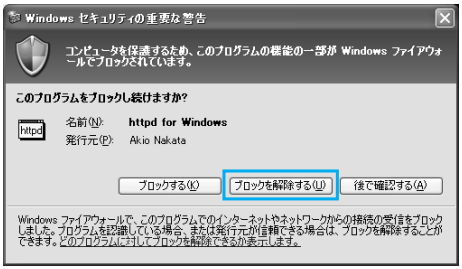


http://www.st.rim.or.jp/~nakata/

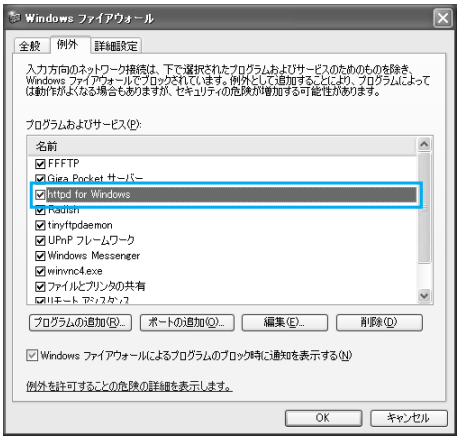
●AN HTTPDの起動とファイアウォールの設定

パッケージを解凍したフォルダを開くと、AN HTTPDの本体ファイル「httpd.exe」があるので、これを実行する。このとき、Windows XP SP2ではWindowsファイアウォールのセキュリティ警告が表示されるので、「ブロックを解除する」ボタンをクリックして通信を許可する。

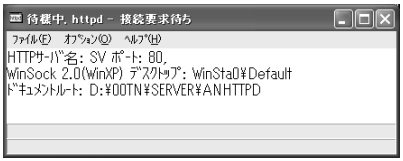
▼Windowsファイアウォールの設定



「AN HTTPD」を最初に起動するとセキュリティ警告が表示されるので、「ブロックを解除する」ボタンをクリックする。その後、実行ファイルのあるフォルダを基準に設定ファイルが自動生成される。



ファイアウォール設定の確認。「AN HTTPD」がネットワークアプリケーションとして許可されていることを確認する。



通知領域の「AN HTTPD」のアイコンをクリックすると表示される「AN HTTPD」のメインウィンドウ。設定ダイアログ等の表示は「通知領域」のアイコンからも行えるので、このウィンドウを表示しておく必要はない。

●作成Webページを置くフォルダの設定

AN HTTPDのデフォルト設定では「作成したWebページ」を置く場所が「AN HTTPDの本体ファイルがあるフォルダ」になっているが、これは管理上好ましくない。そこで、「Webページを置くフォルダ」を新規に作成したフォルダに変更する。

通知領域の「AN HTTPD」アイコンを右クリックし、ショートカットメニューから「オプション／一般」を選択すると「オプション／一般」ダイアログが表示される。ここで「一般」タブをクリックし、「ドキュメントルート」欄でWebページを置くフォルダを変更しよう。

この「一般」タブ内では、ポート番号やデフォルトインデックス（Webページを開いた際に最初に開かれるファイル）の指定もできるが、**通常は「80」「index.html」のままでよい。**

なお、本書で作成するような単一のURLでアクセスできるWebページや画像等の集合を「Webサイト」と呼ぶが、これはクライアント側から見た場合の呼称だ。HTTPサーバー（Webサーバー）自体と意味を混同してしまう可能性もあるため、本書では、HTTPサーバーで公開するWebサイトのことを「作成Webページ」と呼ぶことにする。

▼ドキュメントルートの設定

「ドキュメントルート」はWebページを置くフォルダのこと。その他の設定は基本的にデフォルトのままでよい。

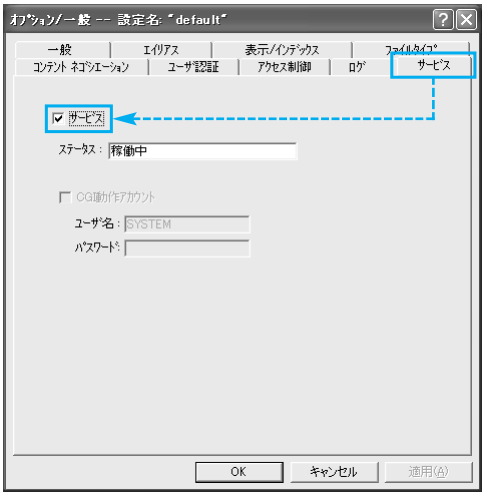
「OK」ボタンをクリックして設定を有効にすると、自動的に再起動し、設定が終了する。

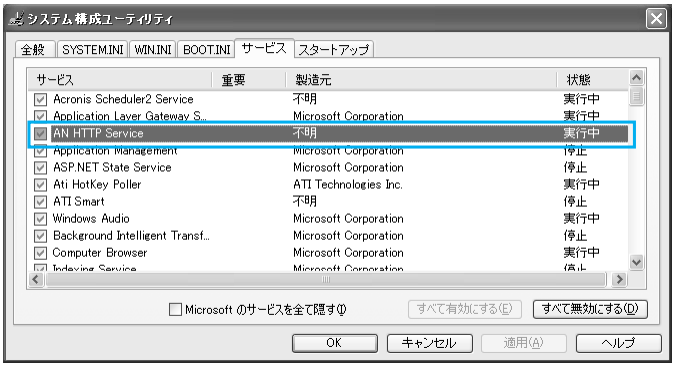
●AN HTTPDをサービスとして起動する設定

AN HTTPDを常時起動しておきたい、パソコンを起動した直後から起動しておきたいといった場合は、AN HTTPDを「サービス」として起動するように設定しよう。

「オプション／一般」ダイアログを表示し、「サービス」タブをクリックして、「サービス」にチェックを入れれば設定完了だ。

▼サービスとして起動する設定





「オプション／一般」ダイアログの「サービス」タブにある「サービス」にチェックを入れれば、以後AN HTTPDは「サービス」として起動する。

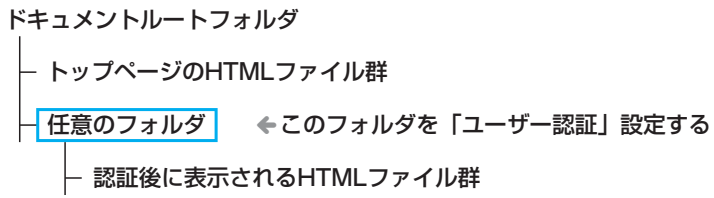
サーバー

ユーザー認証ページの設定

AN HTTPDでは、「ユーザー認証」ページも簡単に設定できる。

認証は「特定のフォルダ以下にあるファイル」にだけ適用できる。つまり、ドキュメントルート以下に任意のフォルダを作成し、その中にユーザー認証したいHTMLファイルを置いてから、そのフォルダを「認証設定」すればよい。

▼ユーザー認証ページの配置方法

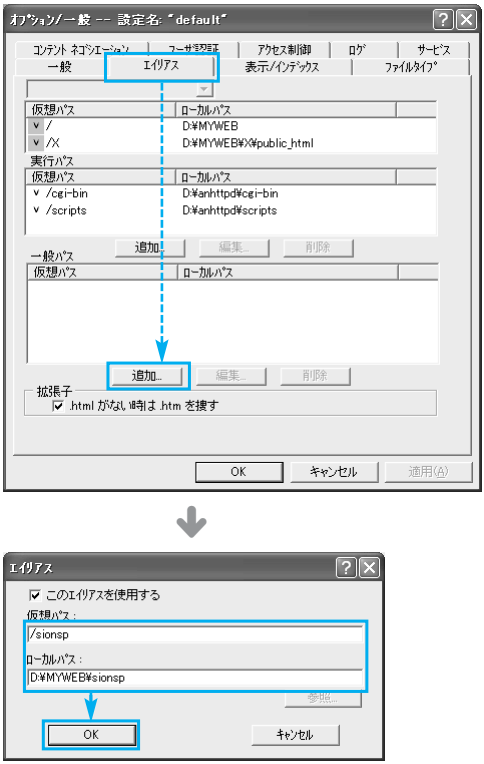


●フォルダの設定

まず、ドキュメントルートフォルダ以下に任意の名前で新規フォルダ（ここでは「sionsp」とした）を作成し、ユーザー認証を行いたいHTMLファイルを収納する。次に、URLでフォルダを指定するために必要な「仮想パス」を割り当てる。

通知領域の「AN HTTPD」アイコンを右クリックして「オプション／一般」を選択すると「オプション／一般」ダイアログが表示されるので、「エイリアス」タブをクリック。「一般パス」欄の下にある「追加」ボタンをクリックすると表示される「エイリアス」画面で、「ローカルパス」欄に作成したフォルダ名のフルパスを、「仮想パス」欄にURLで利用するパス名を“/”に続けて入力する。「OK」ボタンをクリックすれば設定完了だ。

▼ユーザー認証用のフォルダの設定



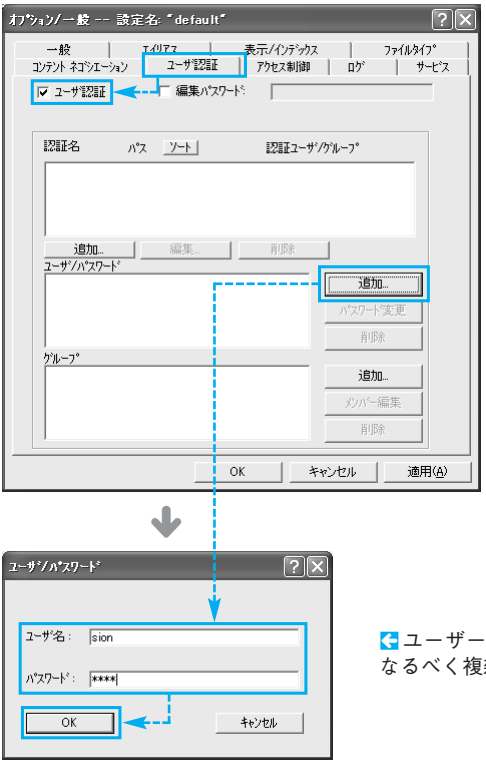
ここでは「D:¥MYWEB」以下に「sionsp」フォルダを作成し、仮想パスも「sionsp」という名前にした。

●ユーザーの設定

作成したフォルダに対する認証設定は「オプション／一般」ダイアログで行う。「ユーザ認証」タブをクリックし、まず「ユーザ認証」のチェックボックスにチェックを入れる。

次に、認証を行う場面で利用する、ユーザーとパスワードを設定する。「ユーザ/パスワード」欄にある「追加」ボタンをクリックすると「ユーザ/パスワード」ダイアログが現れるので、任意の文字列を設定する。

▼ユーザーの設定



ユーザー名とパスワードの任意設定。パスワードにはなるべく複雑な文字列を使うこと。

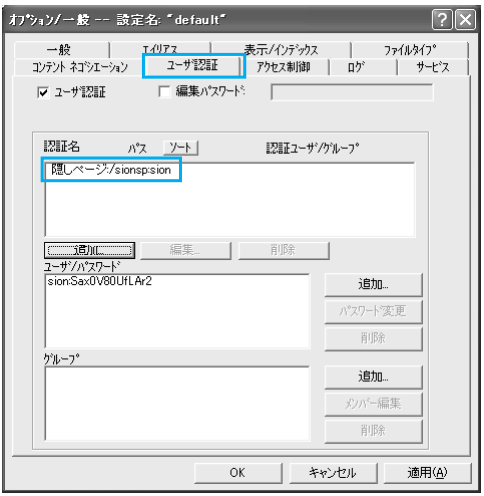
●認証フォルダの指定

続いて「認証が必要なフォルダ」を指定する。この設定を行ったフォルダ内にあるHTMLは、先に設定したユーザーとパスワードを入力しないと閲覧できないようになる。

「認証名」にある「追加」ボタンをクリックすると「認証情報」ダイアログが現れるので、認証名として任意の文字列を入力しする。「パス」欄には、認証したいフォルダのパスを入力する。そして、「認証ユーザ/グループ」欄に先に作成したユーザー名を入力して「OK」ボタンをクリックすればよい。

▼認証フォルダの指定

「認証情報」ダイアログで、ユーザー認証するフォルダとユーザー名を指定する。



設定終了後のダイアログ。「/sionsp」以下のHTMLを表示するにはユーザー名「sion」で認証が必要、という設定だ。

実際の認証場面。ダイアログの表示はこのようになる。

サーバー

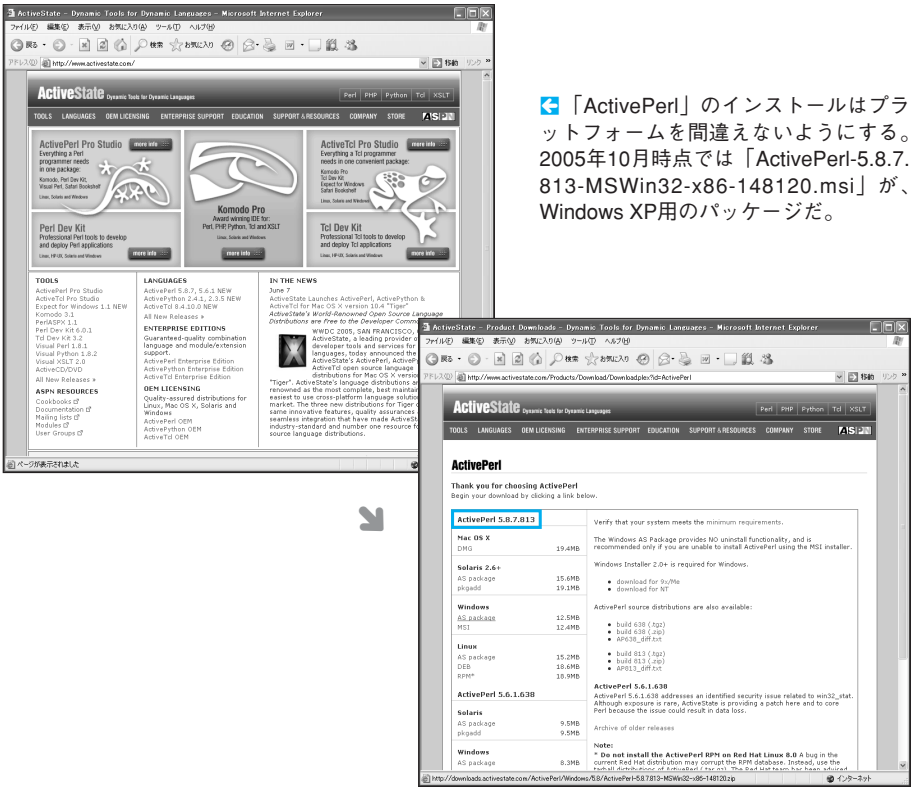
CGIを利用する

Webページ上のカウンタや入力フォームなどで利用されている「CGI」とは、「プログラムをサーバー側で処理するしくみ」のことで、クライアント側に負荷を掛けずにさまざまな情報を提供するために利用される。この「サーバー側でプログラムを処理する」ためには、**サーバー側に「Perl」などのプログラムを実行する環境が必要になる。**

ここではサーバーパソコンに「ActivePerl」をインストールして利用しよう。以下のサイトから、Windows用のパッケージをダウンロードして実行する。

- **ActivePerl**
  http://www.activestate.com/

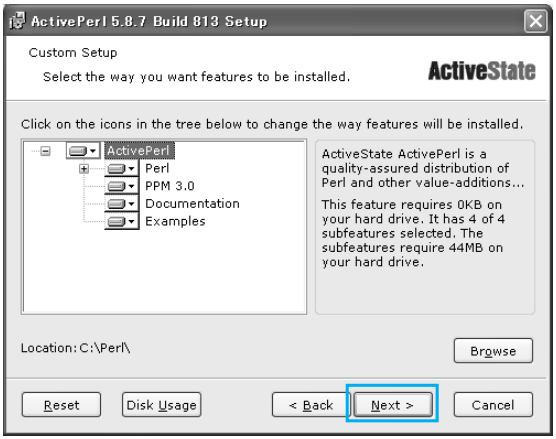
▼ActivePerlのダウンロード

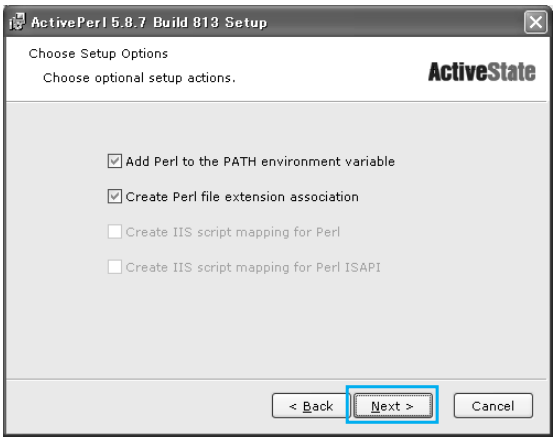


「ActivePerl」のインストールはプラットフォームを間違えないようにする。2005年10月時点では「ActivePerl-5.8.7.813-MSWin32-x86-148120.msi」が、Windows XP用のパッケージだ。

インストールは、セットアップウィザードのダイアログに従えばよい。なお、デフォルト設定でインストールすると、ActivePerlのインストールフォルダは「C:¥Perl」になる。

▼ActivePerlのインストール





「ActivePerl」をインストール。設定はダイアログのデフォルト設定のままでよい。

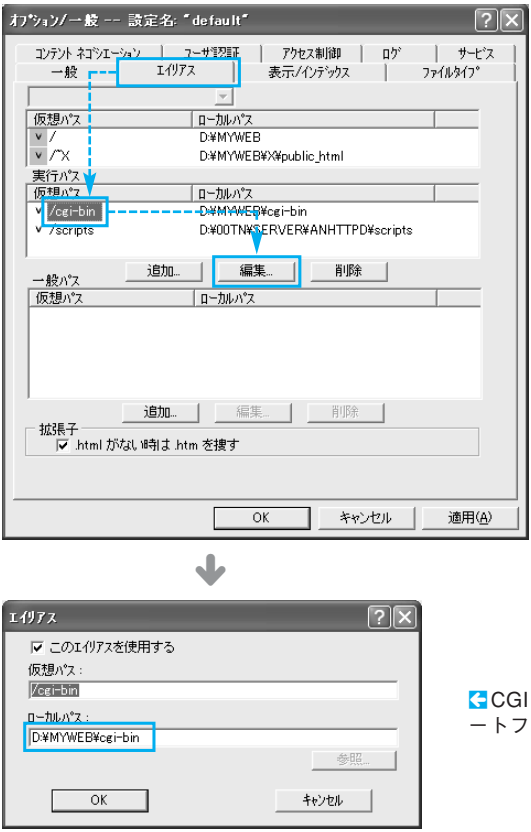
●AN HTTPDでCGIを置くロケーションの設定

次に、AN HTTPDを起動して、「どこにCGIを置くか」のロケーション設定を行う。

「オプション／一般」ダイアログの「エイリアス」タブをクリックし、「仮想パス」欄の「/cgi-bin」を選択して「編集」ボタンをクリックする。「エイリアス」画面が表示されるので、「ローカルパス」欄にCGIファイルを置くフォルダを指定する（通常は標準設定のフォルダで構わない）。

以後すべてのCGIファイルは、ここで設定したフォルダに置くようにする。

▼CGIファイルを置く場所の設定



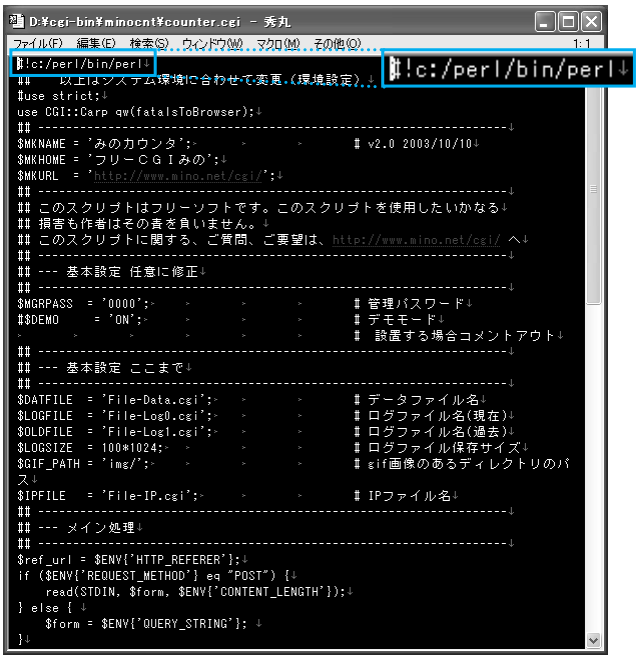
CGIファイルを置く場所の設定。ここではルートフォルダ配下に設定した。

●CGIファイルの改変

フリーで公開されているCGIファイルを利用する場合、入手したCGIファイルを編集して、まず「Perl」の位置を指定しなければならない。

先の「ActivePerl」を利用した場合、Perlのロケーションはインストールしたフォルダの配下「/bin/perl」になるので、デフォルト設定でインストールした場合は「c:/perl/bin/perl」を指定すればよい。

▼CGIファイルの編集



Perlを利用したCGIファイルを利用する場合は、メモ帳などで編集して、「Perl」の位置指定を「c:/perl

サーバー

Webページを作成する際の注意

作成するWebページの構成や内容はユーザーが任意に決めてよいが、本書で記述した通りにセットアップした「AN HTTPD」と「ActivePerl」の組み合わせで利用する場合、以下の事項を守る必要がある。

- 「ドキュメントルート」に設定したフォルダにHTMLファイルを置く
- 作成Webページにおけるトップページのファイル名は「index.html（またはデフォルトインデックスとして指定したファイル名）」にする
- CGIファイルは、Perlで記述したものを利用する
- CGIファイルは、「オプション／一般」ダイアログ「エイリアス」タブの仮想パス「/cgi-bin」で指定したフォルダに配置する
- CGIファイルに記述するPerlのパス指定は、「c:/perl/bin/perl」にする
- 認証ページを置く場合は、「ドキュメントルート」内に任意のフォルダを作成し、そのフォルダ以下に認証後に表示するHTMLファイルを配置する

サーバー

サンプルWebページを作る

HTTPサーバー動作確認（認証、CGI含む）用にサンプルWebページを作りたいが、自分で書き起こすのは面倒という場合は、以下の例に従って簡単なWebページを作成するとよい。

●トップページ

AN HTTPDの「オプション／一般」ダイアログの「一般」タブにある「デフォルトインデックス」欄で設定した名称でHTMLファイルを作成する（通常はindex.html）。

なお、以下のサンプルでは認証ページへのリンクを配置している（<A href=〜>〜</A>）。

▼サンプルWebページ（index.html）

```
<HTML>
<TITLE>[任意Webページ名]</TITLE>
</HEAD>
<BODY>
<P><B><FONT size="5">[任意Webページ名]</FONT></B><BR>
<IMG src="[任意画像ファイル01]">
<A href="sionsp/kakusi.html">隠しページへ</A>
</BODY>
</HTML>
```

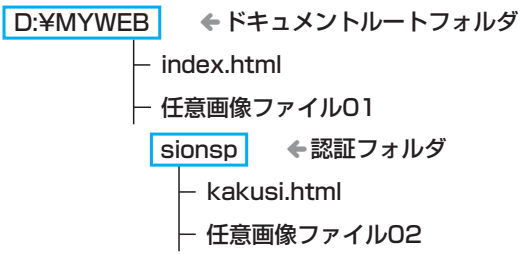
●認証ページ

基本的にどんな内容でもよいが、必ず、「認証情報」ダイアログで設定した仮想パスに該当するフォルダに配置すること。

▼ユーザー認証用の隠しページ（/sionsp/kakusi.html）

```
<HTML>
<HEAD>
<TITLE>[任意隠しページ名]</TITLE>
</HEAD>
<BODY>
<P><FONT size="5"><B>[任意隠しページ名]</B></FONT><BR>
<IMG src="[任意画像ファイル02]"></P>
</BODY>
</HTML>
```


▼サンプルファイルの配置例



●CGIファイル

ここでは、フリーCGIである「みのカウンタ」を利用したサンプルを示す。

CGIの利用方法は下記Webサイトか添付ファイルを参照してほしいが、簡単に設定の流れをまとめておこう。

▼フリーCGIみの（みのカウンタ）

http://www.mino.net/cgi/

▼みのカウンタの利用ステップ

CGIファイルの配置
AN HTTPDの「オプション／一般」ダイアログ「エイリアス」タブの仮想パス「/cgi-bin」で指定したロケーションにCGIファイル（みのカウンタ）をコピーする。

↓

「counter.cgi」の改変
メモ帳などのエディタで開き、「Perlのパス指定」と各種設定を行う。

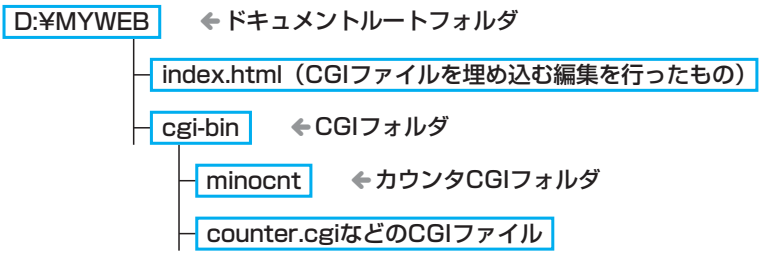
↓

カウンタの作成
Webブラウザで管理画面を開き、「カウンタ」を作成する（カウンタのIDを発行する）。

↓

HTMLの改変
カウンタをWebページに配置するためにトップページのHTMLファイルを編集する。

▼サンプルファイルの配置例



●「counter.cgi」の改変

「counter.cgi」の編集は、「みのカウンタ」のマニュアルに従い、「Perlのパス指定」「管理者のパスワードの指定」「デモモード指定のコメントアウト」を行う。

「Perlのパス指定」は「ActivePerl」のインストールパス「c:/perl/bin/perl」にして、$MGRPASSに管理者のパスワードを入力し、「デモモード」を解除するために「$DEMO～」の行頭に“#”を追加してコメントアウトする。

なお、カウンタとして実際利用するには、管理画面を表示してカウンタの新規登録を行う必要がある（次項参照）。

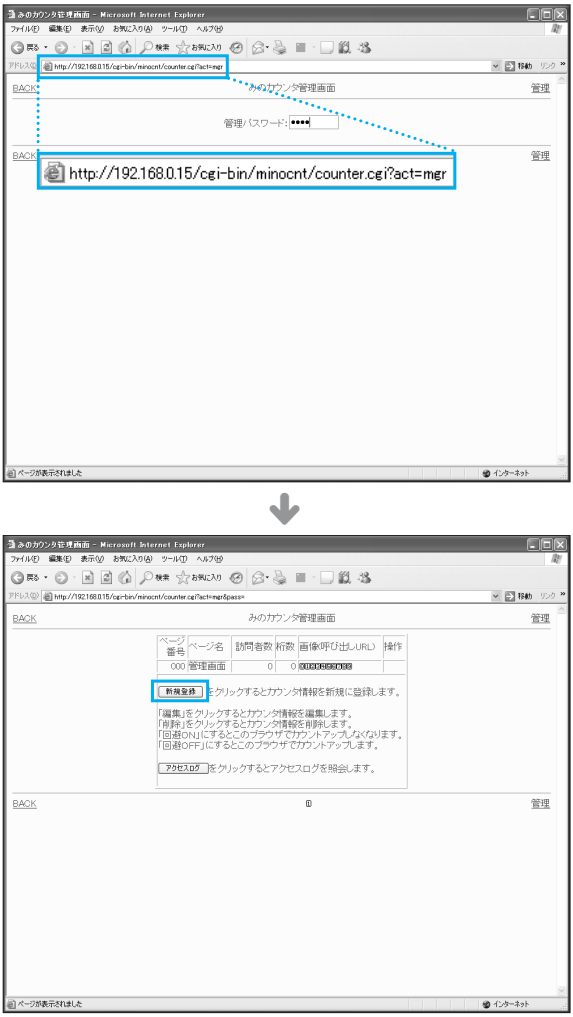
▼「¥cgi-bin¥minocnt¥counter.cgi」の改変

```
#!c:/perl/bin/perl
$MGRPASS    = '0000';                    # 管理パスワード
#$DEMO      = 'ON';                      # デモモード
```

●カウンタの作成

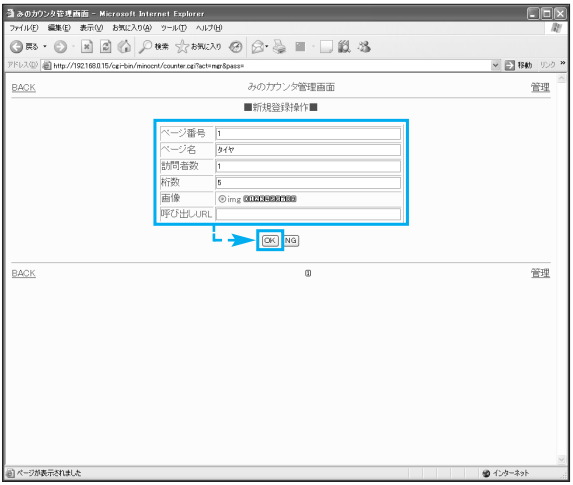
カウンタを利用するには、管理画面で新規カウンタを作成する必要がある。サーバー側のパソコンでWebブラウザ（Internet Explorerなど）を起動し、アドレスバーで「http://127.0.0.1/cgi-bin/minocnt/counter.cgi?act=mgr」と入力すると管理画面が表示されるので、任意のカウンタを作成する（サンプルに従うなら、作成時のページ番号には「1」を指定する）。

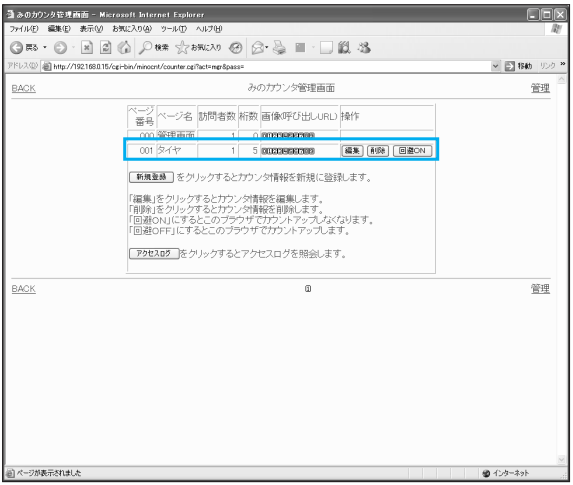
▼カウンタの作成



カウンタの作成画面。ログオン後「新規登録」ボタンをクリックすると登録完了。なお、クライアント側からアクセスする場合は「http://[サーバーのIPアドレス]/cgi-bin/minocnt/counter.cgi?act=mgr」と入力する。

▼カウンタの新規登録





「ID=1」のカウンタを作成。ページ番号以外は任意に設定してよい。

●「index.html」の改変

「index.html」には、以下の2行を加える。なお、2行目の「id=」の指定は、先に作成したカウンタのページ番号と同じ番号にする。

▼サンプルWebページ（index.html）に以下の2行を追加

```
<a href="cgi-bin/minocnt/counter.cgi?act=log">
<img src=cgi-bin/minocnt/counter.cgi?id=1 alt="訪問者数" border=0></a><HEAD>
```

クライアント

クライアントからWebを見る

作成したWebページをクライアント側からWebブラウザで確認してみよう。

通常、Webページを閲覧する際は「http://www.gihyo.co.jp」などのドメイン名を指定するが、現時点ではまだドメインを取得していないので、サーバーのIPアドレスを直接指定する。具体的には、アドレスバーに以下のように入力する。

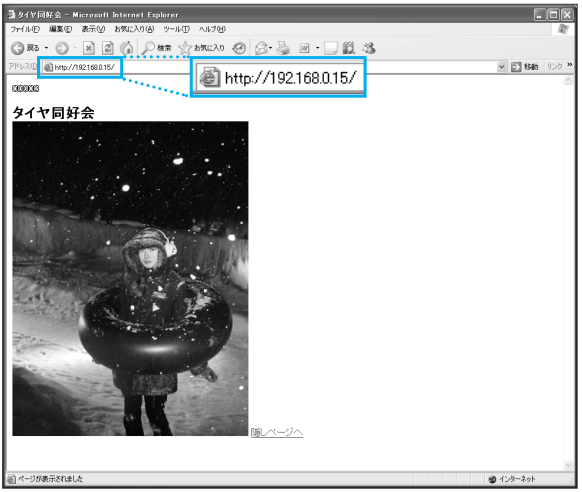
▼アクセスアドレス

```
http://[サーバーのIPアドレス]
```

なお、通常はWebサーバーのポート番号は「80番」なのでポート番号を省略して表記したが、「AN HTTPD」の設定でポート番号を80番以外に設定した場合は、「http://[サーバーのIPアドレス]:[ポート番号]」という形で入力する必要がある。

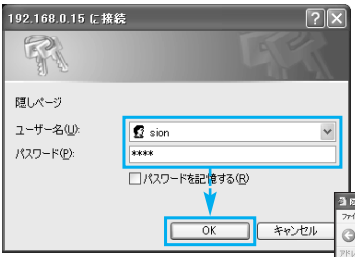
トップページが表示されたら、CGIの動作やユーザー認証を確認するとよいだろう。

▼Webページの閲覧



Webブラウザのアドレスバーに「http://[サーバーのIPアドレス]」と入力すると、作成したWebページを閲覧できる。

▼認証が必要なWebページの閲覧



隠しページへログオン。設定したユーザー名とパスワードを入力すれば閲覧できる。

Chapter 08

遠隔接続に必要な手順と準備

ローカルレベルでのリモートコントロール、ビデオ映像配信、FTP/HTTPサーバーの設定はわかった。あとは遠隔接続を設定すれば自宅サーバーは完成する。遠隔接続には、いくつかのテクニックと設定が必要になるほか、ローカルレベルとは若干異なるセキュリティ意識が必要になる。本章では、これらの設定についての総合情報を説明しよう。

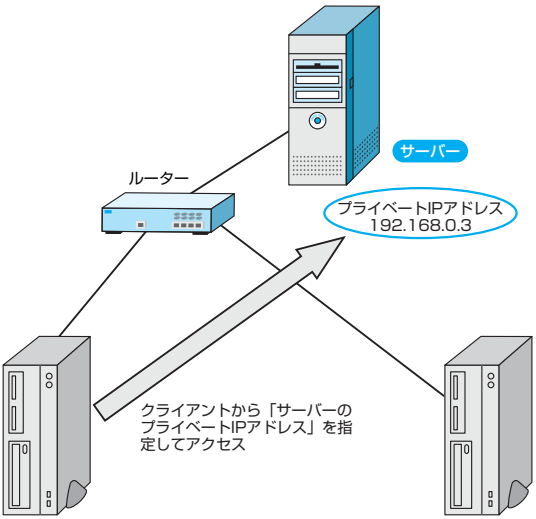
「LAN」と「WAN」の違いから考える自宅サーバーの理論

本書をここまで読み進めたユーザーであれば、「ローカルレベル」での各サーバーの設定は終了しているはずだ。つまり、後は「遠隔接続」を実現するための設定を行えば、インターネットを介した「WAN接続」を実現することができる。ここでは「リモートコントロール」を例に、実際のWAN接続の実現に必要な手順を考えてみよう。

●LANにおけるアクセスのおさらい

LAN環境でリモートコントロールを行う場合、クライアントからサーバーにアクセスするときに指定するアクセスアドレスは「サーバーパソコンのIPアドレス」、いわゆる「プライベートIPアドレス」だった。

▼LANにおけるリモートコントロール



LAN環境でのリモートコントロールでは「固定されたサーバーのIPアドレス（プライベートIPアドレス）」を指定してアクセスする。

●WAN接続に置き換えた場合の構成

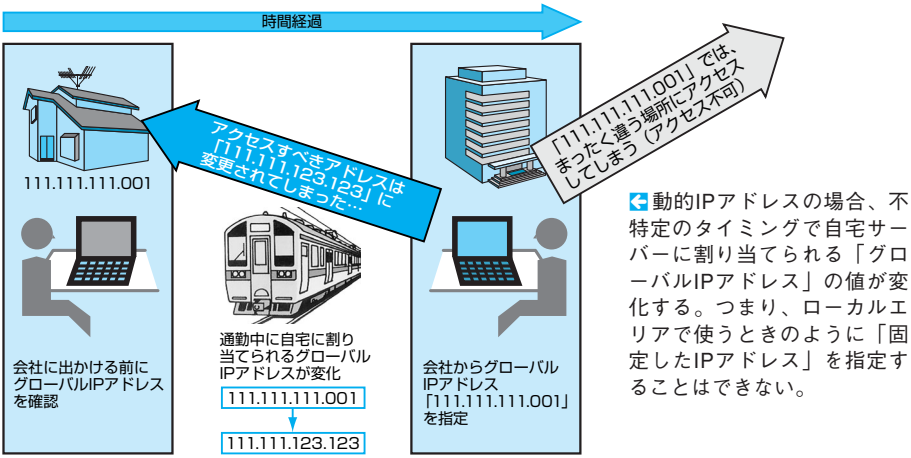
LAN環境における接続手順を単純にWAN環境に当てはめると、プライベートIPアドレスの部分を「グローバルIPアドレス」に置き換えればよいことになる。

しかしここで問題になってくることが2点ある。

まず1つが、「一般的なプロバイダから割り当てられるグローバルIPアドレス」は固定されておらず、周期的にアドレスが変化するという問題だ。このようなIPアドレスを**「動的IPアドレス」**と呼ぶが、プロバイダの都合でIPアドレスが変化するため、サーバー用に割り当てるIPアドレスとして利用することは難しい。たとえば、会社に出かける前にグローバルIPアドレスを確認しても、通勤中にアドレスが変化してしまった場合は会社からそのアドレスでアクセスできなくなってしまう。

このグローバルIPアドレスの変化に対応するためには、「ダイナミックDNS」を利用する必要がある（次項参照）。

▼動的IPアドレスの問題点



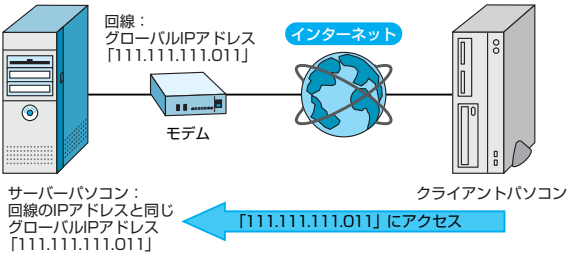
動的IPアドレスの場合、不特定のタイミングで自宅サーバーに割り当てられる「グローバルIPアドレス」の値が変化する。つまり、ローカルエリアで使うときのように「固定したIPアドレス」を指定することはできない。

そしてもう1つが、ルーターの存在によってクライアントが通信先を特定できなくなるという弊害だ。

グローバルIPアドレスで場所を特定できるのは、あくまで「回線（モデム）」までであるため、その先に**ルーターが存在している場合、クライアント側ではLANに接続しているどのパソコンにアクセスしてよいかわからなくなってしまう。**

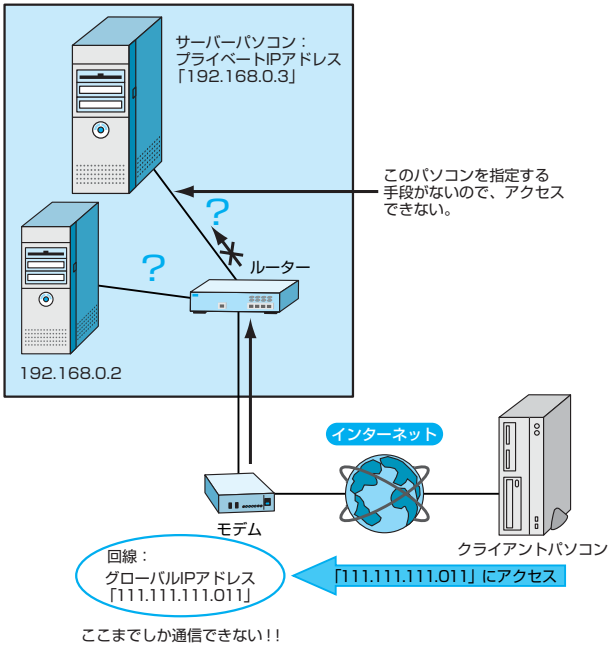
このアクセス先を特定できない問題は、**ルーター自身の設定である「ポートマッピング」を利用**しないと解決できない。

▼ルーターが存在しない場合



ルーターが存在しなければ、回線のアドレスとサーバーパソコンのアドレスはイコールなので、現在の「グローバルIPアドレス」を指定して通信するだけでよい。

▼ルーターが存在する場合



ルーターが存在する場合は、現在の「グローバルIPアドレス」を指定しても、回線（モデム）の先にある通信先（サーバー）のアドレスは特定できない。

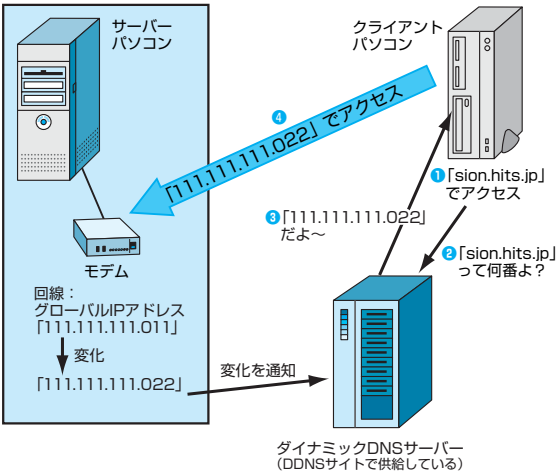
動的IPアドレスを「ダイナミックDNS」で解消（9章で解説）

一般回線に割り当てられるIPアドレスは「動的IPアドレス」であり、IPアドレスが周期的に変化する。インターネット経由でクライアントからサーバーにアクセスする際、「グローバルIPアドレス」を指定してアクセスすることは述べたが、「グローバルIPアドレスが知らない値に変化」した場合は、アクセスする手段がなくなってしまう。

そこで登場するのが「ダイナミックDNS」だ。詳しい解説や設定方法は9章で述べるが、簡単に言えば**「動的IPアドレスを文字列（アクセスドメイン名）に置き換える」ことでアドレスを固定**し、**動的IPアドレスが変化した際には「アクセスドメインのIPアドレス情報を自動更新する」ことで動的IPアドレスの問題を解消する**、というしくみになっている。

ダイナミックDNSを実現するには「ダイナミックDNSサイトへの登録」及び「IPアドレス更新ソフトのセットアップ」が必要になるが、これらの手順については9章で詳しく説明する。

▼「ダイナミックDNS」の構造



「ダイナミックDNS」を利用すれば、固有の文字列（アクセスドメイン名）でサーバーにアクセスできるようになる。この「文字列を現在のグローバルIPアドレスに置き換える」作業は、「ダイナミックDNSサービスを供給するサーバー」が自動的に行ってくれる。

ルーターの壁を「ポートマッピング」で解消（10章で解説）

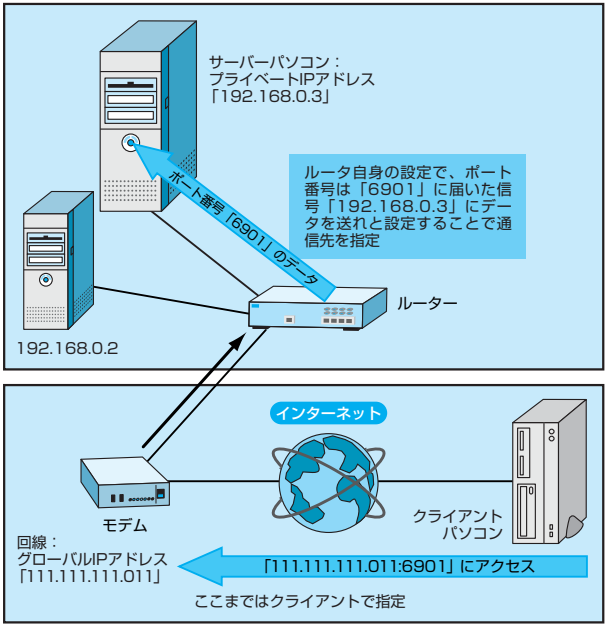
ルーターを利用すると、複数のパソコンから同時にインターネットにアクセスできるというメリットがあるが、WAN環境、つまり「外部から接続される環境」では面倒な問題が発生する。

インターネットの先のクライアントは「グローバルIPアドレス」と「通信ポート」しか情報を持っていないため、ルーターから先のパソコンを特定することはできない。そのため、ルーターに届いた通信をどのパソコンに割り振るかは「ルーター自身」で設定する必要があるのだ。

ルーターに届いた通信を、ポート番号を利用して特定のパソコンに割り振るしくみを「ポートマッピング」と言う。ルーターはこの機能を利用して、「ポート＊＊番に届いた通信は、ローカルパソコン＊＊に送れ」というように「ポート番号」ごとに通信先を指定しているのだ。

ルーターのポートマッピング設定については10章で詳しく説明する。

▼ポートマッピングとは



外部クライアントからルーターの先にある自宅サーバーへの通信は、「ルーターに」どのパソコンにデータを送るかという設定を行うことで実現する。

WAN環境での自宅サーバー構築のステップ

さて、本書の最終目標である「自宅サーバー構築」までのステップ、つまりはWAN接続によるリモートコントロール、Webカメラ、FTPサーバー、HTTPサーバーを実現するまでのステップを説明しよう。

これまでの解説で、すでに各サーバーをローカルレベルで実現しているので、あとは「WANレベル」での設定を追加すればよい。基本的には、以下のようなステップで環境構築すれば、WAN環境での「自宅サーバー」が完成する。

▼自宅サーバー構築までのステップ

各サーバーアプリケーションのセットアップ（4章～7章）
↓
ダイナミックDNSのセットアップ（9章）
↓
ルーターのポートマッピング設定（10章）
↓
WANアクセスの設定（自宅サーバーの完成）（11章）

詳しい説明は各章で解説するが、1つだけ環境構築における注意点を述べるなら、「ルーターの個体差」が「ルーターのポートマッピング設定」及び「開通テスト」の操作手順に大きな差になって現れるということだ。これは、**ルーターの仕様がメーカーにごとに大きく異なることに起因する。**このような事情から、設定を行うときは常にルーターのマニュアルを手元に置き、時間が許すならざっと通読しておくとよいだろう。

自宅サーバーのセキュリティ

「自宅サーバーのセキュリティ」と言っても、最近のブロードバンドの普及により通常の利用方法でも「パソコンがサーバー扱い」になっていることが多いため、行うべきことはブロードバンド環境における一般のセキュリティ対策とほとんど変わらない。

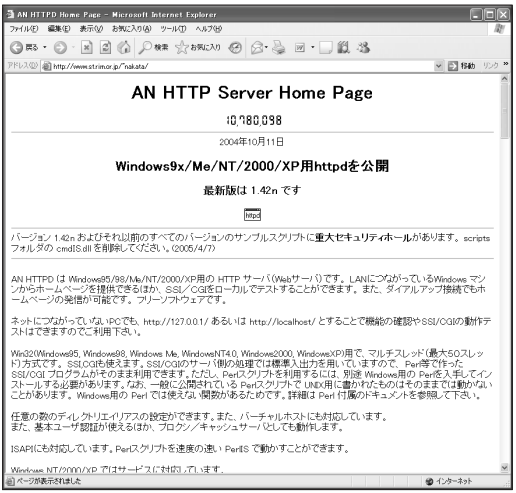
ただし、アクセスすることが主な一般環境と、アクセスされることが主な自宅サーバー環境では、気をつけるべきセキュリティ項目の優先度が異なる。ここでは、「自宅サーバー環境」に必要なセキュリティのポイントを述べよう。

●サーバーアプリケーションのアップデート

クライアント側のネットワークアプリケーションは、あくまで「アクセスすること」を主にするのに対し、**自宅サーバーで使われるサーバーアプリケーションは、常にサーバーパソコンの「ポート」を開放し、「アクセスを口をあけて待っている」状態になっている。**つまり、もしサーバーアプリケーションにセキュリティホールや脆弱性等が存在すると、サーバーアプリケーションの運営に問題が発生するのはもちろん、サーバーパソコンそのものに危険が及ぶことになる。

「サーバーアプリケーション」のセキュリティ対策がOSのそれ以上に重要になるため、各アプリケーションのアップデート状況には常に気をつけてほしい。公式Webサイトを定期的に確認して、こまめに最新版にアップデートするように心がけたい。

▼サーバーアプリケーション「AN HTTP」のWebページ

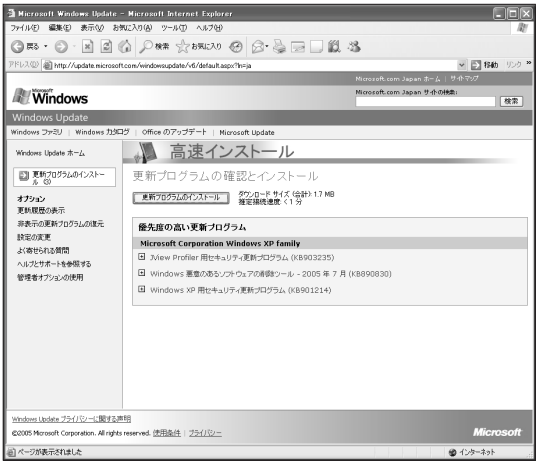


サーバーアプリケーションは、外部と通信をやり取りする「一番重要な部位」である。ここに脆弱性が存在した場合、最悪パソコンごと乗っ取られる可能性があるのだ。

●OSのアップデート

サーバーアプリケーションのアップデートが重要であるように、サーバーアプリケーションが稼働するインフラである「OSのセキュリティ対策」が重要なのは言うまでもない。自動更新やWindows Updateなどで、常にOSを最新状態に保つようにしたい。

▼Windows Update



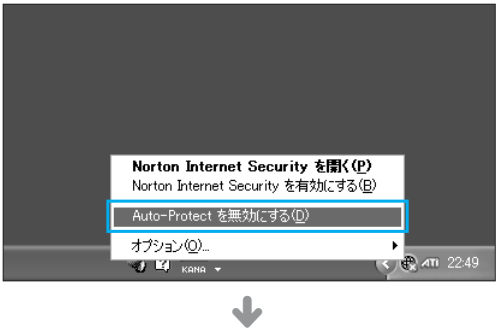
Windows Updateは、スタートメニューから「すべてのプログラム」ー「Windows Update」で実行できる。このWindows Updateでは、Windows XP自身のセキュリティアップデートを行うことができる。

●アンチウイルスソフトの導入

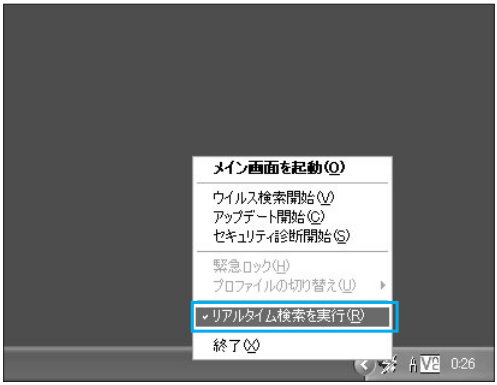
Windows XP SP2では、セキュリティセンターによってアンチウイルスソフトを導入、稼働しておくことが促されるようになっているが、サーバーパソコンにおいても「アンチウイルスソフト」を必ず導入しておこう。

アンチウイルスソフトを導入する際に注意したいのは、ソフト自身を常に最新版に保つことと、**ファイル監視機能（ノートン・アンチウイルスにおける「Auto-Protect」、ウイルスバスターにおける「リアルタイム検索」）を常にオンにしておくことだ。**また、アンチウイルスソフトのアップデートの隙間をぬって最新ウイルスが侵入することもあるため、定期的に手動でウイルススキャンを行うべきだろう。

▼ファイル監視機能



「ファイル監視機能」は各メーカーごとに名称は異なるが、たいてい通知領域からコントロールできる。



▼ウイルススキャン

ノートン・アンチウイルスでパソコン全体をウイルススキャン。任意に実行できるほか、スケジューリングで定期的に自動実行させることもできる。

●ルーターのファームウェアアップデート

通信の門となる、ルーターのセキュリティにも注意したい。

最近のルーターはほぼ「ファームウェアアップデート」に対応しており、**アップデートを行うことでルーター機能の不具合が解消されるほか、既知の攻撃方法に対するセキュリティが高められる。**

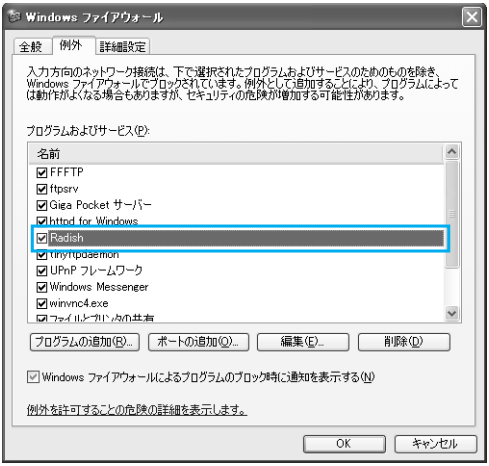
なお、比較的古めのルーターはそもそも本体が「脆弱性」を抱えているものもあるため、なるべく「サポートが継続されており、ファームウェアアップデートができる」ルーターを利用するようにしたい。

●不要なポートは開けない

サーバーアプリケーションを稼働させるためには、ファイアウォール設定でポートを開放（アプリケーションの使用許可）しなければならないが、この際、必要最小限のポートだけに通信許可を与え、不要なポートを開放しないようにする必要がある。つまり、使いもしないアプリケーションに通信許可を与えたり、使わないポート番号を開放したりすることは厳禁ということだ。

ルーターにおけるポートマッピングの設定も同様で、基本的に必要最小限のポート以外は「ポートマッピング」しないようにする。

▼Windows ファイアウォール



ファイアウォールにおけるアプリケーションの許可設定は「必要なもののみ」にとどめること。

●パスワードを複雑にして定期的に変更する

いくら厳重にセキュリティ対策を行っていても、悪意を持つユーザーにパスワードがバレてしまっては意味がない。

たとえば、リモートコントロールサーバーのパスワードが見破られてしまった場合、リモートコントロールによりOSのすべての操作が可能になるため、ファイルや各サーバーアプリケーションの設定を好きなように書き換えられてしまう。

そのため、**パスワードを乱数などの「類推しにくい」ものにすることはもちろん、万が一漏洩したときに備えて、定期的にパスワードを変更するようにしよう。**

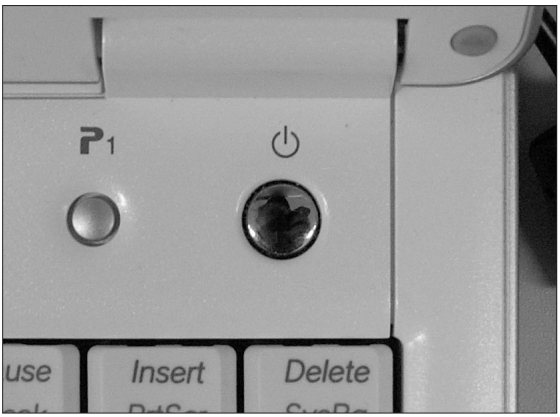
▼パスワード設定

自宅サーバーの場合、「アクセスドメイン」は類推しやすい。アクセスされることは比較的容易なので、砦となるのは「パスワード」のみである。

●電源を切る・ネットをオフにする

コロンブスの卵的な発想だが、サーバーパソコンの電源を切ってしまえば、アクセスされることも無ければクラックを受けることもない。サーバーを利用しない時間は「パソコンの電源を切って」おこう。

▼パソコンの電源



OSやアプリケーションに脆弱性があれば、パソコンに電源を入れているだけでクラッキングされる恐れがある。使用しないときは電源を切っておくよう心がけたい。

●余計なアプリケーションを入れない・使用しない

基本的にパソコンというものは、アプリケーションを入れれば入れるほど、セキュリティリスクが高まる。そのため、サーバーパソコンには、OS、サーバーアプリケーション、セキュリティソフトなど、最低限のアプリケーションだけをインストールするようにして、それ以外のアプリケーションはなるべくインストールしないようにしたい。

また、アングラ系のWebサイトにアクセスすることや、余計なスクリプトの実行を許可することなど、サーバーの運用に関係のない操作・設定も避けること。

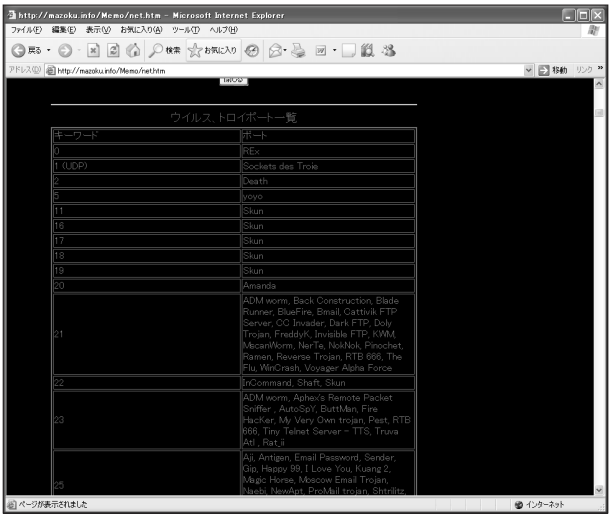
●ポート番号の変更

ポート番号を変更する利点は、主に2つある。

1つは「トロイ」と呼ばれる攻撃プログラムが利用するポート番号を使わないようにすることで、システムのセキュリティレベルを上げることができる点だ。

これは、**「トロイに利用されるポート番号」を避けて各サーバーアプリケーションのポート設定**を行うことで実現できる。トロイに利用されるポート番号はひんぱんに変わるため、ここでは具体的な番号を挙げないが、トロイに利用されるポート番号を知りたければ「Web検索」を利用するとよいだろう。たとえば、Googleなどで「トロイ ポート」などのキーワードで検索すれば、トロイが利用するポート番号を一覧にしているサイトが見つかるので、それらを参考に設定するとよい。

▼トロイに利用されるポート番号



危険なポート番号をWebで確認して、そのポート番号を避けて設定するようにする。

もう1つの利点は、「他人がアクセスしにくくなる」という点である。

たとえば、リモートコントロールソフトである「VNC」はデフォルトで「5900番」のポート番号が設定されているが、このポート番号を利用した場合は、クライアントからサーバーにアクセスする際にポート番号を入力する必要がなくなる。つまり、クライアントからアクセスする際に、「アクセスドメイン」だけでアクセスできてしまうのだ。

「ダイナミックDNSサービス」に実際に登録してみればわかるが、自宅サーバーのアクセスドメインは、ダイナミックDNSサービスを利用したことがあるものなら「容易に予想」することができる。**そのため、わざとポート番号を変更して、リモートコントロールサーバーなどの「絶対に他人に使わせてはいけないサーバー」をアクセスしにくくするテクニックが非常に有効なのだ。**

▼ポート番号設定が5900番の場合

「アクセスドメイン」だけでリモートコントロール可能な状態（ポート番号の指定は不要）

↓

ほかのサーバー（FTPサーバーなど）を他人に公開している場合、
「アクセスドメイン」は簡単にわかってしまう

↓

VNCビューワで「アクセスドメイン」を入力するだけでアクセスできる

↓

「パスワード」が破られれば侵入されてしまう

※FTPサーバーやHTTPサーバーを他人に公開している場合、アクセスドメインだけでアクセスできる「リモートコントロールサーバー」は危険すぎる。

▼ポート番号設定が5900番以外の場合

「[アクセスドメイン]:[ポート番号]」でアクセスできる状態になる
（ポート番号の指定が必要）

↓

ほかのサーバー（FTPサーバーなど）を他人に公開している場合、
「アクセスドメイン」は簡単にわかってしまう

↓

VNCビューワで「[アクセスドメイン]:[ポート番号]」を入力する必要があり、
他人はポート番号を類推しなければアクセスできない
（パスワードを含めると二重パスワードになる）

※ポート番号を変更すれば、本来のパスワードと合わせて結果的に二重パスワードになる。

Chapter 09

ダイナミックDNSを確立せよ

遠隔接続においてキモになる設定が「ダイナミックDNS」だ。ダイナミックDNSは一般回線レベルにおける各種問題を解決することができ、また「自分固有のドメイン」でサーバーにアクセスすることが可能になる。「ダイナミックDNS」の構築は少し難しいかもしれないが、本章をじっくり読めばわかるはずだ。

ダイナミックDNSのしくみと活用

「ダイナミックDNS」とは、本来インターネット経由でアクセスする際に直接指定する必要のあるサーバーの「動的IPアドレス」を、「固有の文字列（アクセスドメイン）」に変換する機能だ。

ダイナミックDNSは、一般回線における動的IPアドレスの定期的な変化を解決するための手段になる。この機能を利用するには、まずダイナミックDNSを提供しているインターネットサービスと契約し、サーバーに「グローバルIPアドレスの変化を通知するソフト」をインストールして、アクセスドメインとIPアドレスの対比情報を常に更新するようにする。

▼一般回線のグローバルIPアドレス

	アクセスアドレス
昨日	111.111.111.011
↓	
本日	111.111.111.022

※一般回線（ADSLや光等）に割り当てられるIPアドレスは「定期的に変化する」という特性を持つため、常に同じIPアドレスを指定してアクセスすることは不可能だ。

▼ダイナミックDNSの役割

	アクセスドメイン		アクセスアドレス
昨日	sion.hits.jp	=	111.111.111.011
↓	↓常に一緒		↓定期的に変化
本日	sion.hits.jp	=	111.111.111.022

※ダイナミックDNSサービスで固有のドメイン名を取得すれば、IPアドレスが変化しても、固定の「アクセスドメイン」を使ってアクセスできる。

ダイナミックDNSの利点をまとめると、以下のようになる。

- **IPアドレスではなく「固有のドメイン名」を利用できる**
- **動的IPアドレスの定期的な変化に対応できる**

また、この「ダイナミックDNS」を実現するには、以下の作業が必要になる。

- **ダイナミックDNSサービスへの登録**
- **IPアドレス更新ソフトのセットアップと常駐**

COLUMN　ダイナミックDNSにおける用語の定義

ダイナミックDNS関連の設定では、ネットワーク用語における「表記のゆれ」、あるいは「意味の範囲のゆれ」が随所に見られ、非常にわかりにくい。多くの書籍や雑誌が「なんとなく表現」している傾向にある。
これは、ソフトやサイトごとに表記が違う現状では致し方ないといえるが、本書ではIPアドレスを更新するためのソフト「DiCE」での表記を基に、混乱を起こさないための「用語定義」を行うことにする。なお、この定義は「ダイナミックDNS」に関してのみ有効とする。

- **ダイナミックDNSサービス**
  「ダイナミックDNS」機能を提供しているサイト。「ドメイン」を取得できるサービスのこと。
- **IPアドレス更新ソフト**
  ダイナミックDNSサービスで取得した「ドメイン」に対してサーバーのIPアドレスを送信し、「変換情報を更新」するソフトのこと。WindowsではIPアドレス更新ソフト＝「DiCE」と考えてよい。
- **ダイナミックDNS**
  「ダイナミックDNSサービス」＋「IPアドレス更新ソフト」を組み合わせて実現する最終的な「ダイナミックDNS」機能のこと。
- **アクセスドメイン**
  IPアドレスを文字列に置き換えたものを「ドメイン名」というが、自宅サーバー構築における「ドメイン」は、各サーバーアプリケーションごとに意味する「範囲」が異なるという問題がある。たとえば「sion.hits.jp」というドメイン名の場合、この全体を「ドメイン」とすることもあれば、「hits.jp」の部分だけを「ドメイン」と称したりもする。これでは非常にわかりにくいので、本書ではアクセス時に指定するドメイン名（先の例では「sion.hits.jp」）のことを「アクセスドメイン」と称して説明する。なお、ダイナミックDNSサービスの申請時、たいていの場合は前半部は任意の文字列を指定可能で、後半は複数候補からの選択方式になる。

▼「アクセスドメイン」の定義

アクセスドメイン＝[ホスト名].[ドメイン名]

- **ホスト名**
  本来はドメイン内のサーバーを文字列に置き換えたものを示すが、「ダイナミックDNS」設定時においては「アクセスドメイン」の前半部とする。
  「sion.hits.jp」であれば「sion」の部分。
- **ドメイン名**
  本来はIPアドレスを固有の文字列に置き換えたものを示すが、「ダイナミックDNS」設定時においては「アクセスドメイン」の後半部とする。ダイナミックDNSサービスにおいて、この部分は選択式だ。

「ダイナミックDNS」セットアップの流れ

「ダイナミックDNS」を実現するまでのプロセスは、「ダイナミックDNSサービスへの登録」と「IPアドレス更新ソフトの設定」の2つに分けることができる。

まず「ダイナミックDNSサービスへの登録」だが、これはユーザーが任意にサービスを選択して登録を行うことになる。この登録手順はサイトごとに多少異なるが、たいていは以下のような手順になるので参考にしてほしい（具体的な手順についてはP.154参照）。

▼ダイナミックDNSサービスへの登録（順序はサイトごとに多少異なる）

サービスWebサイトの表示（サービス概要や利用規定を確認）
↓
基本情報の入力（ユーザー名とメールアドレス）
↓
ドメイン名の選択（サービスによっては本登録後）
↓
確認メールの受信と本登録
（たいていはメール内のURLをクリックするか、メール記述のパスワードでログオンする。中には確認だけのものもある）
↓
ダイナミックDNSサービスへログオン
↓
詳細設定を行い、本登録完了

「IPアドレス更新ソフト」については、Windows環境では「DiCE」をデファクトスタンダードと考えてよいので、これを用いて説明する。DiCEの設定では「ダイナミックDNSサービス」で登録した情報を入力する。

▼IPアドレス更新ソフトの設定

「DiCE」パッケージのインストール
↓
登録したダイナミックDNSサービス用の「DiCE」プラグインの入手
（ただし、ほとんどのサービスは最初から登録されている）
↓
サービスに登録した情報を「DiCE」に設定
↓
ダイナミックDNSサービスに対してIPアドレスを更新

ダイナミックDNSサービスの選び方

ダイナミックDNSサービスを提供しているサイトは30社以上存在するが、そのサービス形態はさまざまである。ダイナミックDNSサービス選択のポイントは大きく2つあるので、ここではそれを解説しよう。

●有料か無料かで選ぶ

各ダイナミックDNSサービスを分類する際、「有料か無料か」が1つの線引きになる。

ダイナミックDNSサービスに「スピード」という概念はないと考えてよいので（IPアドレスを通知するだけのシステムなので速さ関係ない。P.135参照）、「有料か無料かなら『無料』のほうが…」と考えるのが普通だ。しかし、筆者はこの「無料のダイナミックDNSサービス」を数年間使い続けているが、ほぼ1年ごとに新しい無料ダイナミックDNSサービスへの乗り換えを迫られている。なぜなら、さまざまな事情で無料サービスは継続が難しいからである。**つまり、「有料か無料か」というファクターは同時に「継続性が高いか低いか」という要素も含んでいるのである。それを踏まえた上で、どちらかを選択する必要がある。**

なお、もし自宅サーバーを「たまに（年に数回ほど）しか利用しない」、あるいは「よく利用するものの、数ヶ月間利用しないこともある」場合には、問答無用で「有料サービス」をお勧めする。無料サービスの場合、長期間ログオンしないといつの間にか登録が抹消されてしまうことが多いからだ。

▼有料サービスと無料サービスの違い

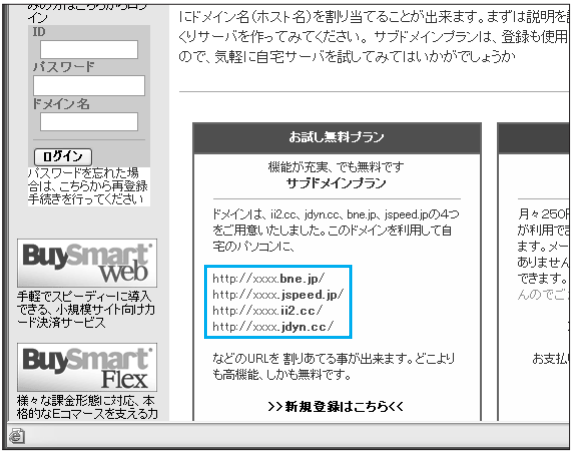
	メリット	デメリット
有料サービス	高い継続性と付加サービス	有償である
無料サービス	無償である	サービス停止や有料サービスへの移行の可能性有り

●ドメイン名の好みで選ぶ

もう1つの選択ポイントになるのが「ドメイン名」の文字列の好みである（ここで言うドメイン名はアクセスドメインの後半部のこと）。

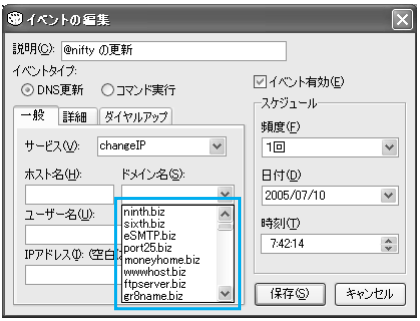
実際に登録処理してみるとわかるが、ダイナミックDNSサービスの「ドメイン名」は選択式であり、バリエーションに限りがある。この文字列にこだわりたいときは、各ダイナミックDNSサービスを見比べて（あるいはDiCEで各サービス設定を覗いて）、気に入った文字列があるサービスを選択する必要がある。

▼ダイナミックDNSサービスのドメイン名



かっこいい文字列がよい、短い文字列がよいなどのこだわりがあるなら、各ダイナミックDNSサービスを見比べて、ドメイン名の文字列を比較するとよい。

▼「DiCE」でドメイン名を確認



まず「DiCE」を導入して、各サービスが提供するドメイン名を確認するとよいだろう（DiCEのセットアップはP.160参照）。

●主なダイナミックDNSサービス関連サイト

●無料ダイナミックDNSサービス

CJB.NET
http://www.cjb.net/

DDNS instat.ne.jp（日本語サイト）
http://www.instat.ne.jp/ddns/index.html

DDNS.nu
http://www.ddns.nu/

DION ダイナミックDNS
（日本語サイト・DION会員限定）
http://www.dion.ne.jp/ddns/

DNIP.NET
http://www.dnip.net/

Dynamic DO!
（日本語サイト、有料サービスも有り）
http://ddo.jp/

Dynamx
http://www.dynam.ac/

DynDNS
http://www.dyndns.org/

DynDSL.com
http://www.dyndsl.com/

DYNSERV
http://www.dyn.ee/

Dynu
http://www.dynu.com/

DYNUP.net
http://www.dynup.net/

Earth Dynamic DNS
（日本語サイト、有料サービスも有り）
http://mydns.to/

EveryDNS.net
http://www.everydns.net/

HN.ORG
http://hn.org/

JPN.ch（日本語サイト）
http://jpn.ch/

JSpeed（日本語サイト）
http://ddns.j-speed.net/

Microtech
http://www.mtgsy.net/

miniDNS
http://www.minidns.net/

MyIP
http://myip.us/

myserver.org（有料サービスも有り）
http://www.myserver.org/

No-IP.com（有料サービスも有り）
http://www.no-ip.com/

RegisterFly.com
http://registerfly.com/

SelfHost
http://www.selfhost.com/

UNICC
http://www.uni.cc/

Yi
http://www.yi.org/

YSNI Dynamic Network（日本語サイト）
http://www.ysdn.org/

ZENNO.com（日本語サイト）
http://zenno.com/doc/ddns.php

zoneedit
http://www.zoneedit.com/

家サーバー・プロジェクト（日本語サイト）
http://www.ieserver.net/

私的ダイナミックDNS（日本語サイト）
http://www.mydns.jp/

大分インターネットレンタルサーバー
（日本語サイト、有料サービスも有り）
http://www.usa.ne.jp/

●有料ダイナミックDNSサービス（ドメインサービス含む）

3domain（日本語サイト）
http://www.3domain.hk/

BIGLOBEダイナミックDNSサービス
（日本語サイト）
http://ddns.biglobe.ne.jp/

changeIP.com
http://www.changeip.com/

deerfield.com
http://dns2go.deerfield.com/

DHS International
http://www.dhs.org/

DNSART.com
http://www.dnsart.com/Home/

DtDNS
http://www.dtdns.com/

livedoorドメイン（日本語サイト）
http://domain.livedoor.com/

Now!Network
http://www.now.nu/

ODN ダイナミックDSN（日本語サイト）
http://odn.onamae.com/html/

ODS
http://www.ods.org/

ZiVE（日本語サイト）
http://www.zive.org/

お名前.com（日本語サイト）
http://www.onamae.com/ddns/

バリュードメイン（日本語サイト）
http://www.value-domain.com/

マイドメイン（日本語サイト）
http://my-domain.jp/

@niftyダイナミックDNS
（日本語サイト、@nifty会員限定）
http://www.nifty.com/ddns/

●IPアドレス更新ソフト

DiCE
http://www.hi-ho.ne.jp/yoshihiro_e/dice/

GnuDIP
http://gnudip2.sourceforge.net/

ダイナミックDNSサービスへの登録

基本的に、選択したダイナミックDNSサービスへの登録作業はWebサイトの表示に従って行えばよいが、各登録情報は必ず一度「エディタなり手書きメモなり」に書き写しておいてほしい。特に日本語サイト以外で登録申請を行った場合は、登録時点で覚えていたとしても、後に再設定が必要になったときに忘れてしまうと一大事になる（サイトごとに項目名の揺れが激しいことも一因だ）ので、必ず項目名とともにメモしておこう。また、サービスによっては「ユーザーID」「登録名」「ホスト名」が同じ文字列になる（1つの設定がすべての項目に適用される）ものがあるので、このあたりでも混乱しないようにしたい。

以下に書き込み用のサンプルを示すので、これを参考に書き込んでほしい。

▼ダイナミックDNSサービス登録表

ダイナミックDNS サービス名	
ダイナミックDNS サービスURL	
ユーザーID (ID)	
パスワード (Password)	
登録名 (Name)	
登録メールアドレス (Email Address)	
ホスト名 (Hostname)	
ドメイン名 (Domain)	
アクセスドメイン (通常は[ホスト名].[ドメイン名])	

ダイナミックDNSサービス登録手順の具体例

ここでは、ダイナミックDNSサービス登録手順の具体例として、日本の代表的なサービスである「家サーバー・プロジェクト」のダイナミックDNSサービスを取り上げて紹介しよう。

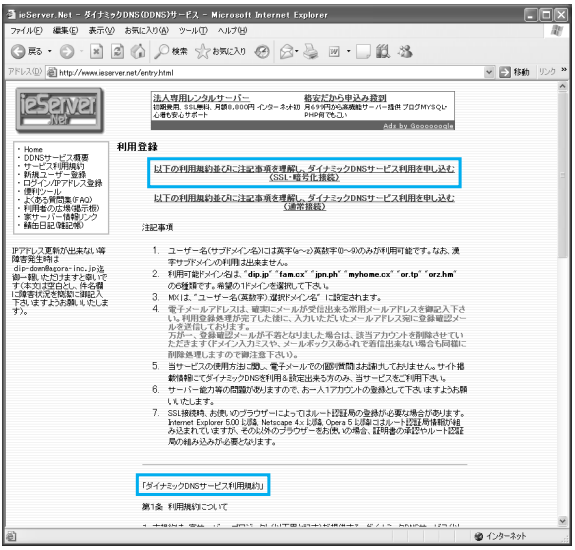
●**家サーバー・プロジェクト ダイナミックDNSサービス**
http://www.ieserver.net/

●「新規ユーザー登録」の開始

メイン画面の「新規ユーザー登録」をクリックして、ユーザー登録を開始する。

なおこの際、「利用規約」が表示されるが、重要な情報なのできちんと読んで同意（申し込み）すること。

▼ユーザー登録

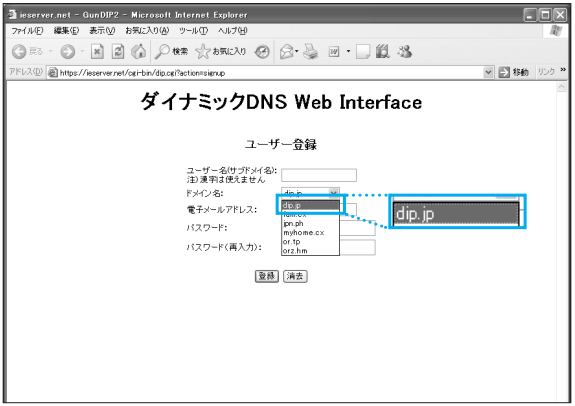


ダイナミックDNSサービスの申請を開始。必ず「利用規約」を読み、内容を理解してから同意するようにする。

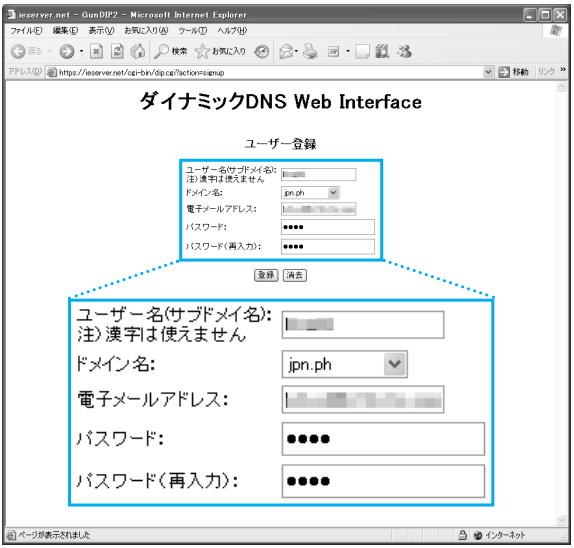
●登録情報の入力

まず、「ドメイン名」から自分が利用したいものを選択する。続いて、「ユーザー名」、「メールアドレス」、「パスワード」をそれぞれ入力する。「家サーバー・プロジェクト」においての「ユーザー名」は、本書における（DiCE設定における）「ホスト名」にあたり、アクセスドメイン名の前半部になるものなので、適当に命名しないように注意する。

▼登録情報の入力



まず「ドメイン名」を選択。好きなものを選択するようにする。



「ユーザー名」、「メールアドレス」、「パスワード」各情報を入力。なお、この「ユーザー名」は「ホスト名」でもあり、すなわちアクセスアドレスは「[ユーザー名].[ドメイン名]」ということになる。

▼「家サーバー・プロジェクト」におけるアクセスドメイン

アクセスドメイン　＝　[ホスト名].[ドメイン名]

↑

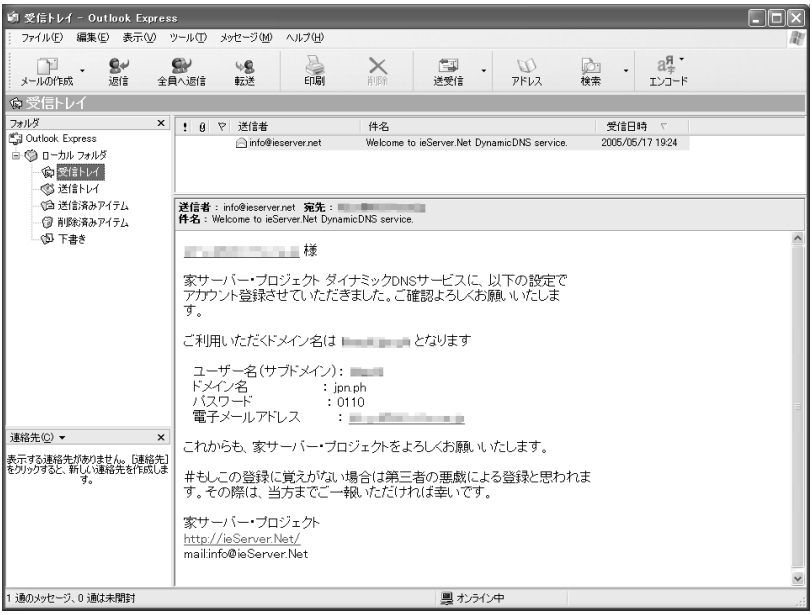
ホスト名として「ユーザー名」が割り当てられる

※「家サーバー・プロジェクト」の場合、「ユーザー名」がアクセスドメイン名の前半部である「ホスト名」になる。

●登録完了

登録情報の入力で各種情報を入力して「登録」ボタンをクリックすると、「登録が完了しました」が表示される。この際、登録したメールアドレスに登録情報の確認が送信されているので、メールソフトを起動して内容を確認する。

▼登録完了のメッセージ

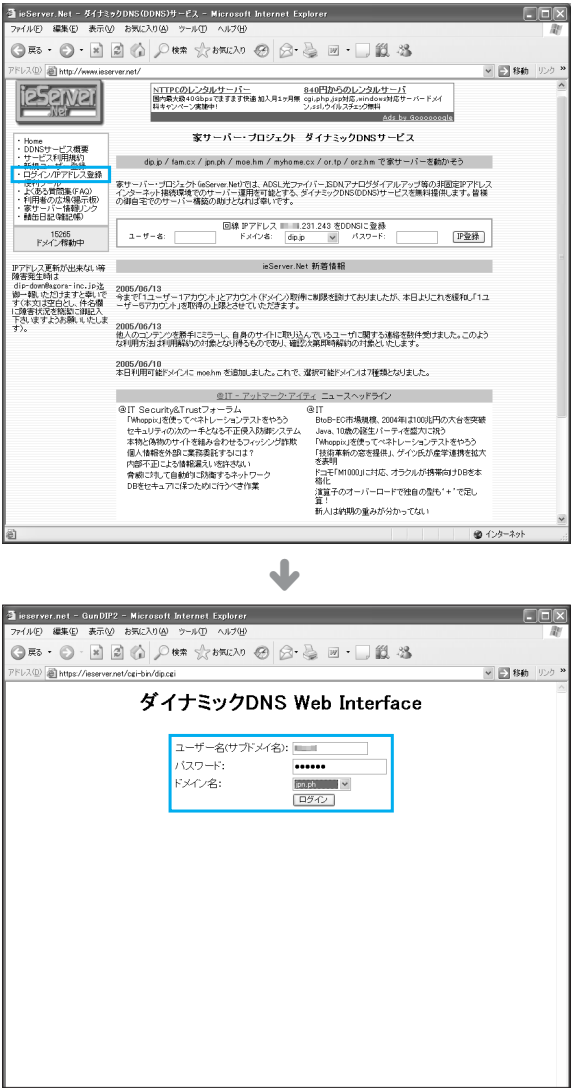


ダイナミックDNSの登録が完了すると、登録メールアドレスに詳細（サービスによっては認証用のパスワード）が送信されてくる。

●設定画面へのログオン

「家サーバー・プロジェクト」のホームに移動し、「ログオン/IPアドレス登録」をクリックするとログオン画面になる。先に登録した「ユーザー名」「パスワード」を入力し、登録時に選択した「ドメイン名」を選択して「ログオン」ボタンをクリックする。

▼設定画面へのログオン

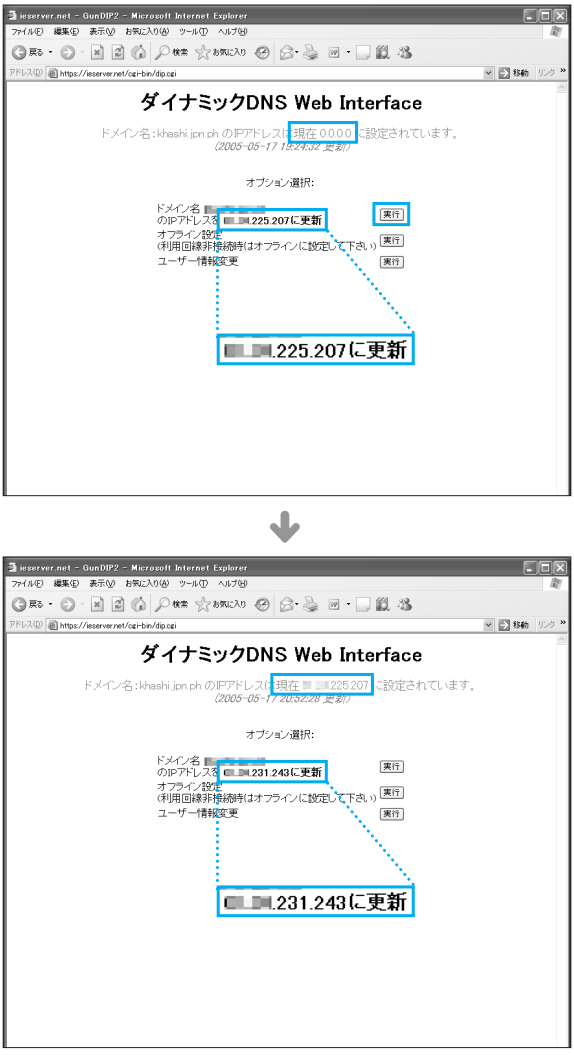


「ログオン/IPアドレス登録」では、設定の確認変更とダイナミックDNSを利用する「IPアドレスの登録」を行うことができる。

●設定の確認

ログオン時の入力項目に間違いがなければ、登録情報が表示される。なお、この時点でアクセスドメイン（画面表記上のドメイン名）を使用するサーバーのIPアドレスを登録・更新することもできるが、あとでDiCEで設定するので、ここでは特に更新しなくてもよい。

▼設定の確認



登録直後の画面。まだIPアドレスは「0.0.0.0」で登録されている。ドメイン名表記の横にある「実行」ボタンをクリックすれば、IPアドレスの更新を行うことができる。

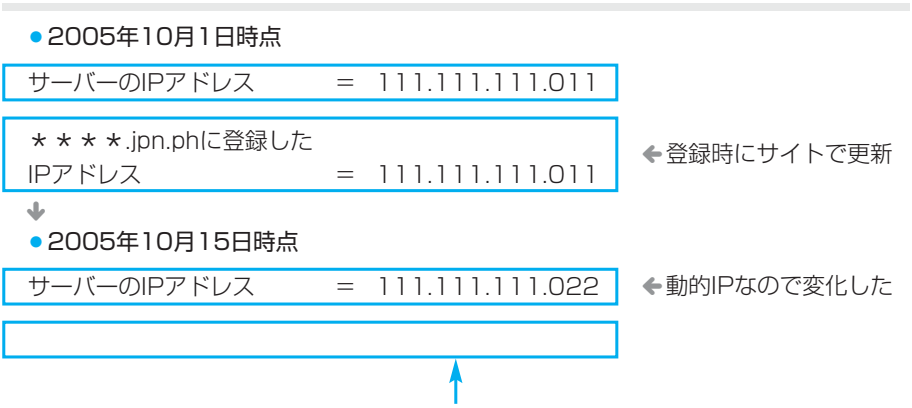
1ヶ月後にログオンした画面。以前のIPアドレスと現在のIPアドレスが異なることがわかる。この「動的IPアドレス」の問題を解決してくれるのが「ダイナミックDNSサービス」だ。

サーバー

IPアドレス更新ソフト「DiCE」のセットアップ

「ダイナミックDNSサービス」に登録すれば「アクセスドメイン」を利用できるようになるが、その場合でも最も重要なのは「現在のグローバルIPアドレス」である。「ダイナミックDNSサービス」に登録し、その時点でサーバーのIPアドレスを更新しても、このままでは将来のアクセスは保障されないからだ。

▼一般回線のグローバルIPアドレス



※＊＊＊＊.jpn.phに登録したIPアドレスが「111.111.111.011」のままなので、アクセスドメインを使ってアクセスできなくなる

上記の説明では「10月15日」にIPアドレスが変化しているが、実際はいつIPアドレスが変化するかわからない。知らないうちにIPアドレスが更新されるので、「アクセスドメイン」によるサーバーアクセスは保障されないのである。

そのため、**このような「IPアドレス」の変化を感知し、ダイナミックDNSサービスに対して「サーバーのアクセスドメインは『＊＊＊.＊＊＊.＊＊＊.＊＊＊』に更新された！！」と通知、更新するソフト（本書では「DiCE」）を利用する必要があるのだ。**

「DiCE」は、次の公式サイトからインストールパッケージ（MSIファイル）をダウンロードし、ダブルクリックすることでセットアップできる。なお、当たり前だが、必ずサーバーアプリケーションをインストールしているパソコンにセットアップすること。

▼DiCE

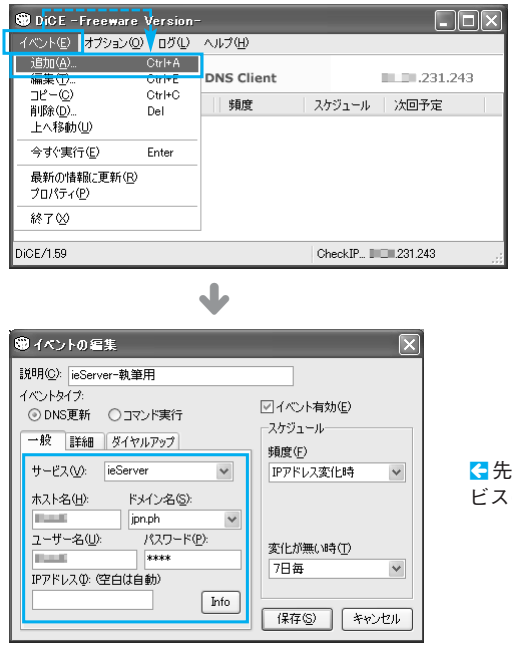
http://www.hi-ho.ne.jp/yoshihiro_e/dice/

●DiCEの設定

DiCEを起動し、「イベント」－「追加」を選択すると、「イベントの編集」ダイアログが表示される。ここで「DNS更新」にチェックを入れて、以下の項目を入力して「保存」ボタンをクリックする。

説明	任意の文字列を入力する。この項目は設定そのものには関係ないが、わかりやすいように「ダイナミックDNSサービス名＋利用用途」などにするとよい
サービス	登録を行ったダイナミックDNSサービス名を選択。一覧にない場合にはP.163参照
ホスト名	登録したホスト名を入力する
ドメイン名	登録時に選んだドメイン名をドロップダウンボックスから選択する
ユーザー名	「ダイナミックDNSサービス」にログオンするためのユーザー名を入力する
パスワード	「ダイナミックDNSサービス」にログオンするためのパスワードを入力する
スケジュール	設定は任意だが、「頻度」欄は「IPアドレス変化時」、「変化がない時」欄は「7日毎」程度にするとよい

▼DiCEの設定



ダイナミックDNSへIPアドレスの変化を通知、更新するために、メニューバーから「イベント」ー「追加」を選択。

先にユーザー登録したダイナミックDNSサービスの登録情報を入力する。

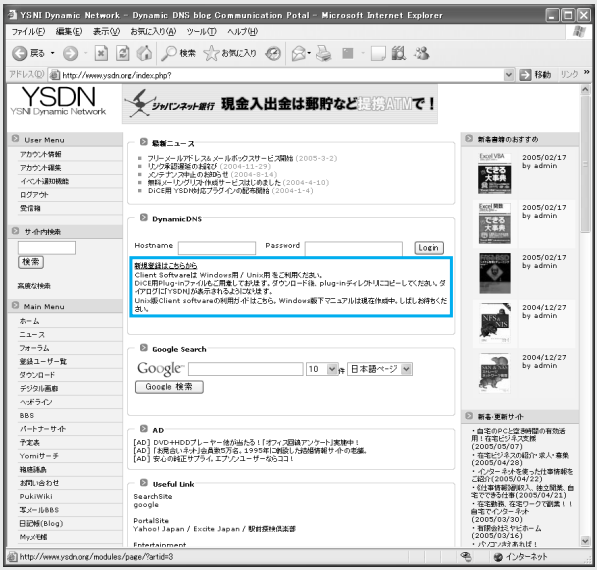
設定を終了してメイン画面に戻ったら、設定した項目（イベント名）にチェックがついていることを確認する。以上で設定は終了だ。

▼DiCEの設定確認

登録したイベント名にチェックがついていれば、以後は設定に従ってIPアドレスの通知、更新作業が自動的に行われる。

COLUMN 「イベントの編集」ダイアログに登録したサービスがない場合

「イベントの編集」ダイアログの「サービス」欄に自分の登録したダイナミックDNSサービスが存在しない場合は、もう一度ダイナミックDNSサービスの登録サイトを閲覧してみよう。国内のダイナミックDNSサービスであれば、「DiCE」用のプラグインがダウンロードできるようになっているので、それを導入すれば選択できるようになる。



登録サイトからプラグインをダウンロード。もしくは、DiCEの最新版を確認してみよう。最新版ではサービスの項目が増えている場合もある。

サーバー

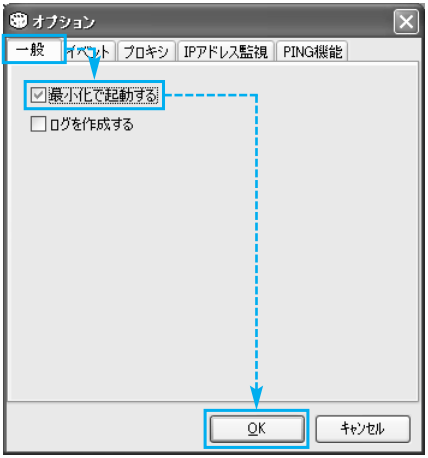
「ダイナミックDNS」の活用（IPアドレスの更新）

「ダイナミックDNSサービス」に登録し、DiCEの設定を行ったあとは、「ただDiCEを起動しっぱなし」にしておけばよい。DiCEが設定に従って、自動的にIPアドレスを更新してくれる。逆に言えば、IPアドレスが変化したときにDiCEが起動していないと「DiCE」の存在価値はないので、サーバーが駆動中には常に「DiCE」が起動しているよう、スタートメニューの「スタートアップ」に登録しておこう。

●DiCEのウィンドウを非表示にする

Windows起動時に表示されるDiCEのウィンドウが邪魔に感じるなら、メニューバーから「オプション」－「環境設定」を選択し、「オプション」ダイアログ「一般」タブにある「最小化で起動する」にチェックを入れる。これでウィンドウが表示されなくなる。

▼DiCEを起動時に最小化する設定



起動時に最小化する設定。ダイナミックDNSサービスの設定後はウィンドウを表示しておく必要はないので、この設定にしておくとよい。

●IPアドレスの手動更新

ダイナミックDNSサービスに対するIPアドレスの更新を手動で行うには、メイン画面でイベント名を右クリックし、ショートカットメニューから「今すぐ実行」を選択する。メイン画面の右下に「Successful［サーバーIPアドレス］」と表示されれば更新終了だ。**サーバーを長期に渡って利用していなかったときなどは、この「手動更新」を実行するとよいだろう。**

▼IPアドレスの手動更新

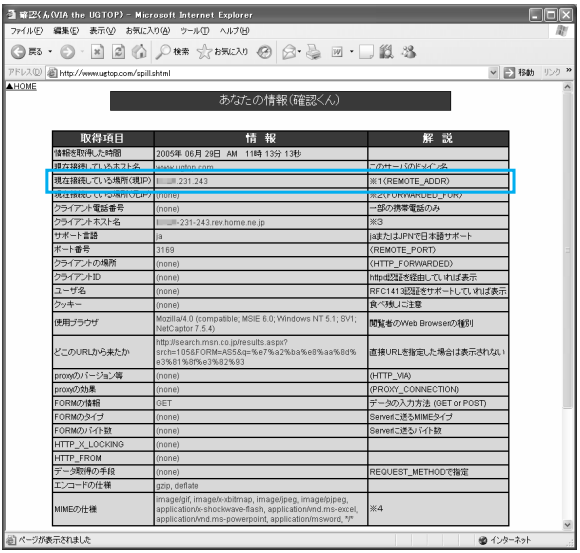
IPアドレスの手動更新。なお、この更新作業はダイナミックDNSサービスのサーバーに負荷をかけるため、連続して実行しないこと。

●ダイナミックDNSの動作確認

ダイナミックDNSサービスを登録し、「DiCE」でIPアドレスの更新が行われていれば、常に「アクセスドメイン＝サーバーのIPアドレス（回線のグローバルIPアドレス）」になっているはずだ。この動作が正常かどうかを判断するには、次のようにする。

まず、サーバーのIPアドレス（グローバルIPアドレス）は、確認サイト「確認くん」で表示できる。

▼確認くん



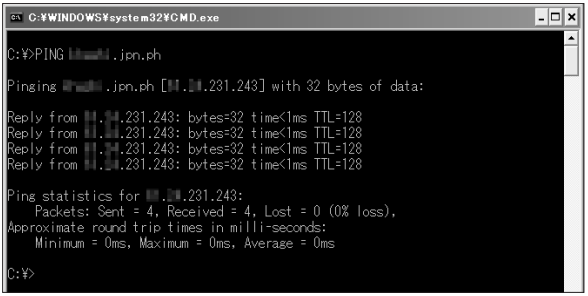
http://www.ugtop.com/spill.shtml

次に、アクセスドメインのIPアドレスを「PING」コマンドを利用して確認する。スタートメニューから「すべてのプログラム」−「アクセサリ」−「コマンドプロンプト」と選択。コマンドプロンプトが表示されたら、

PING [アクセスドメイン]

と入力して Enter キーを押す。現在の回線のグローバルIPアドレスが表示されればOKだ。ここで過去のIPアドレスが表示された場合は、DiCEで手動更新作業を行ってからもう一度「PING」コマンドで確認しよう。

▼「PING」コマンドでIPアドレスを確認



「PING」コマンドでアクセスドメインのIPアドレスを確認。確認くんで表示されたIPアドレスが表示されればOKだ。

Chapter 10

ルーターの設定とポートマッピング

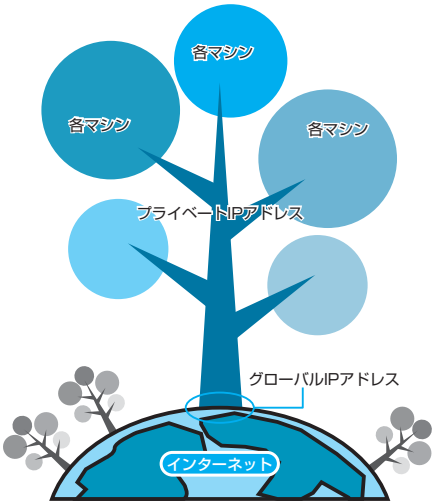
ルーターを設置すると「ひとつの回線で複数パソコンでのインターネットが可能になる」が、自分がアクセスされる側になる「自宅サーバー」では、「外部からアクセスするパソコンがわからない」という問題が起こる。そのアクセス対象のパソコンを指定する設定が「ポートマッピング」だ。なお、サーバー回線側にルーターが存在しない場合には、この章を読み飛ばしてかまわない。

ルーターのしくみと「ポートマッピング設定」の必然性

数年前まで「ルーター」はかなり高価なもので、一般家庭で利用している方は少なかった。しかし最近では、「ブロードバンド」や「無線LAN」の普及により、ユーザー自身が意識していなくてもルーターを利用していることが多い（プロバイダが提供するモデムにルーター機能が付いている）。**ルーターを簡単に説明すると「インターネット回線をローカルネットワーク上の各パソコンで同時利用するためのデバイス」である。**これは、NAT（Network Address Translation）という機能で実現されている。

ルーターの主な仕事は、回線に1つだけ割り当てられている「グローバルIPアドレス」と、LAN上の各パソコンに割り当てられた「プライベートIPアドレス」を相互変換することだ。たとえば、ローカルネットワークを「木」とイメージすると、回線に割り当てられたグローバルIPアドレスが「幹」、プライベートIPアドレスが「枝」に相当する。

▼ルーターとIPアドレス

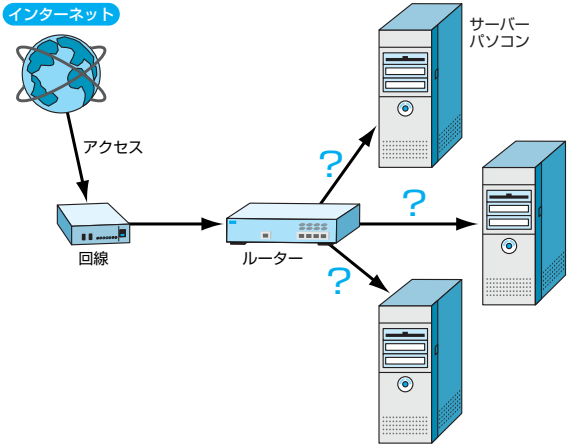


インターネットを「地球（世界間のグローバル通信）」とし、グローバルIPアドレスを「幹」、プライベートIPアドレスを「枝」と考えるとわかりやすい。

インターネットの世界で通信を行うには「グローバルIPアドレス」を使う必要があることは前述した通りだが、回線にパソコンが1台しか存在しない状態なら、グローバルIPアドレスを独占できるため全く問題は生じない。**しかし、「ルーター」を利用して各パソコンにプライベートIPアドレスを割り当てている状態のときに、外部からのアクセスが来ると、それがどのパソコンをターゲットにしたものかわからなくなってしまう。**

自宅サーバーは「外部から」のアクセス（リクエスト）を受けて、リクエストに応じた動作を行うものなので、ルーターがサーバーの動いているパソコンにリクエストを通知できなければ、自宅サーバーなど成り立たなくなってしまうのだ。

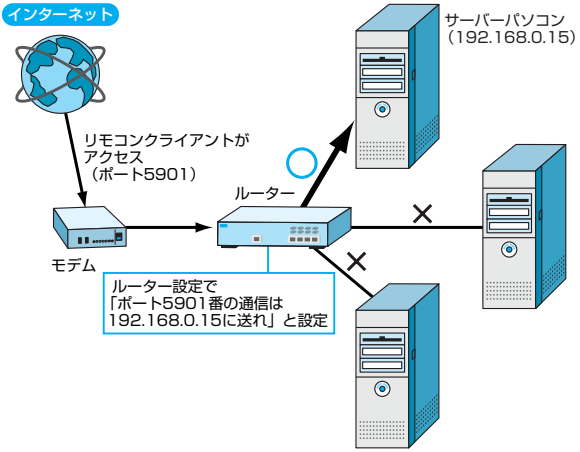
▼ルーターが存在することによる自宅サーバーの問題



ルーターを使って複数のパソコンをインターネットに接続している場合、LAN上のパソコンからのリクエストは問題なく送信できるが、外部からアクセスがあった場合、どのパソコンへ送信するか決定できなくなる。

この「外部からのアクセスをサーバーに送信できない」という問題は、あらかじめルーターに対して「ポート＊＊に届いたデータは、＊＊パソコンに送る」と指示することで解決する。**この指示設定のことを「ポートマッピング」と言う。**

▼ポートマッピング



「ポートマッピング」とは、外部から来たデータを「ポート番号」を指標にして各パソコンに割り振るための設定だ。

「ポートマッピング」設定の流れ

ルーターのポートマッピング設定は、ルーターの機種によって異なる。

単に画面や用語の表記が異なるばかりでなく、設定方法までメーカーや機種ごとにさまざまだ。ルーターを発売しているメーカーは有名なものでも10社近くあり、そのほかにプロバイダが配布する専用ルーターもあるので、ここですべてのルーターの設定方法を説明することはできない。そのため本書では、設定の手順ではなく、「設定の理論」について説明する。理論さえきちんと理解すれば、マニュアルを読まなくても設定できるようになるだろう。

▼ルーターのポートマッピングの流れ

サーバーパソコンのIPアドレスとMACアドレスを知る（またはIPアドレスを固定する）
↓
ルーターの設定画面にログオンする
↓
ポートマッピングを設定する
↓
設定を有効にする（ルーターの再起動）

サーバー

サーバーパソコンの情報を知る

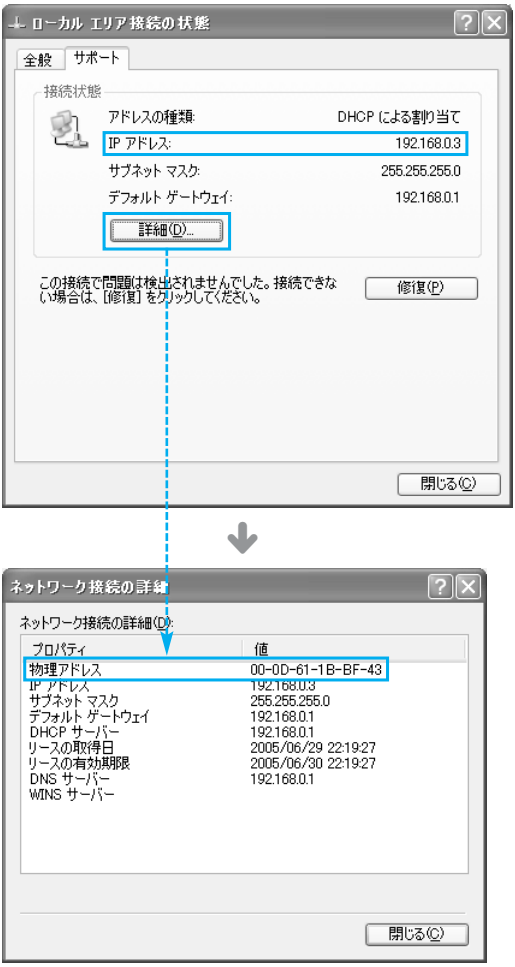
ポートマッピングの設定では「ポート＊＊番に届いた通信は、パソコン＊＊に送れ」といった記述を行うのだが、この「パソコン」はどのようにして特定するのだろうか？

実はルーターのメーカーによって「特定」の方法は異なる。あるメーカーでは「パソコンのIPアドレス」を利用し、またあるメーカーではパソコンに装着されたLANポートの「MACアドレス」を利用して特定する。どちらのケースにも対応できるよう、サーバーパソコンの「IPアドレス」と「MACアドレス」を両方確認しておき、ポートマッピングの設定に備えるとよいだろう。

●サーバーパソコンの情報の確認

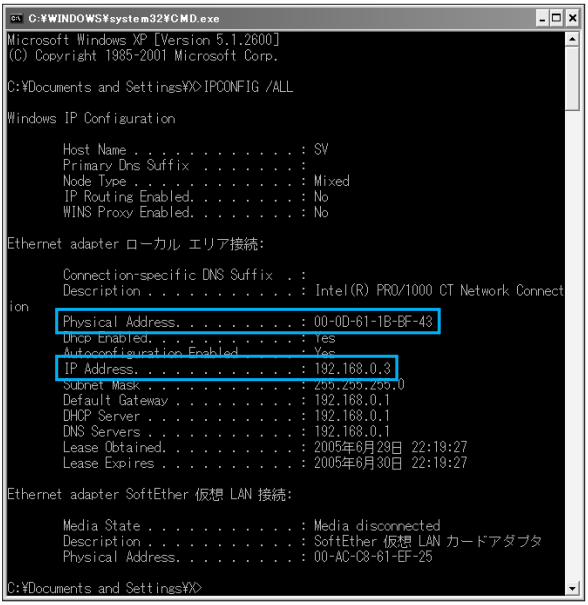
「IPアドレス」と「MACアドレス」の確認は、P.028で紹介した通り、通知領域のネットワークアイコンか、コマンドプロンプトにおける「IPCONFIG /ALL」コマンドを利用して行う。

▼「IPアドレス」と「MACアドレス」の確認



サーバーパソコンの通知領域にあるネットワークアイコンをダブルクリック。「サポート」タブでIPアドレスを確認できる。また、「詳細」ボタンでMACアドレス（物理アドレス）を確認できる。

▼「IPCONFIG /ALL」コマンド



コマンドプロンプトによる確認。「IP Address」がIPアドレス、「Physical Address」がMACアドレスだ。

●サーバーパソコンのIPアドレスの固定

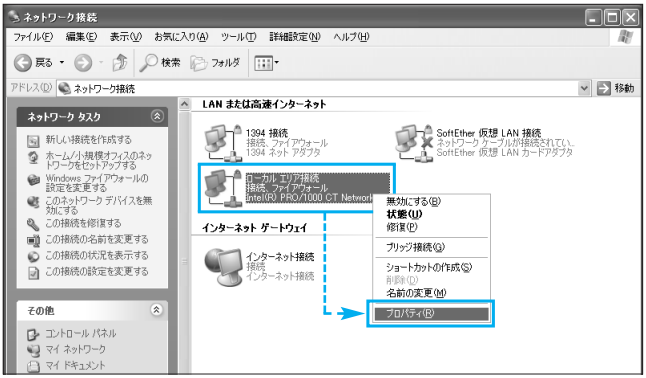
一般的なルーター環境では、各パソコンのIPアドレスは「DHCP」機能によって自動的に割り振られている。その場合、「プライベートIPアドレス」はパソコンが起動するたびに再割り当てされるため、特定のIPアドレスを使い続けることはできない（ただし、最近のルーターは一度割り当てた値を覚えているので基本的に変化しない）。

「IPアドレス」を利用してポートマッピングを設定する場合、サーバーパソコンに割り当てられるプライベートIPアドレスが変化してしまっては困るので、サーバーパソコンのIPアドレスだけは固定しておいたほうがよい。

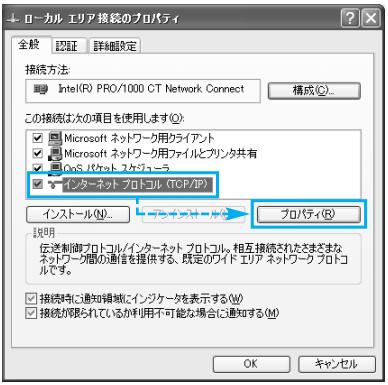
パソコンのIPアドレスを固定するには、「コントロールパネル」から「ネットワーク接続」を選択してプロパティ画面を開き、ルーターにつながっているネットワークアイコン（たいてい「ローカルエリア接続」）を右クリックして、ショートカットメニューから「プロパティ」をクリックする。

続いて、ダイアログの「インターネットプロトコル（TCP/IP）」を選択して「プロパティ」ボタンをクリックすると「インターネットプロトコル（TCP/IP）のプロパティ」ダイアログが表示されるので、「次のIPアドレスを使う」にチェックを入れて各項目を入力する。

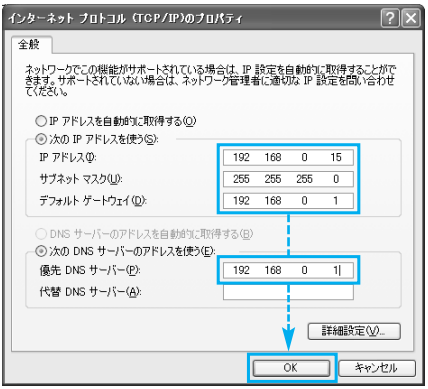
▼IPアドレスの固定方法



ルーターと接続しているネットワークアイコンを右クリックして、ショートカットメニューから「プロパティ」を選択。



「インターネットプロトコル（TCP/IP）」を選択して「プロパティ」ボタンをクリックする。

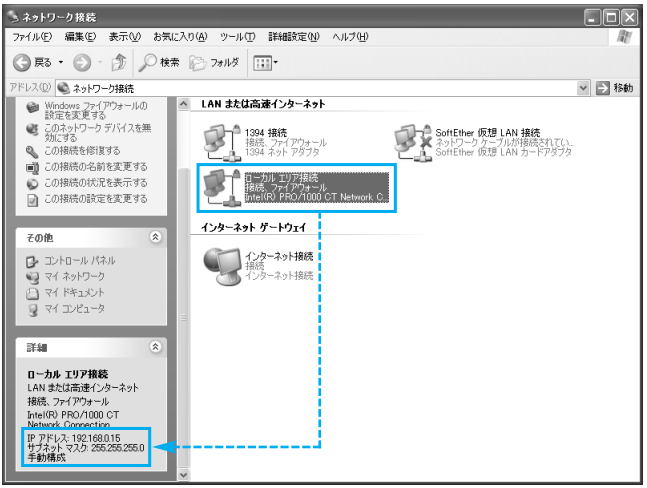


「IPアドレス」「サブネットマスク」「デフォルトゲートウェイ」「優先DNSサーバー」に入力して「OK」ボタンをクリックする。

IPアドレス	固定するプライベートIPアドレスを入力する。上位3つはルーターのIPアドレス（デフォルトゲートウェイ）と同じ数字を入力し、下位1つだけ任意の数字にする。ただし、DHCPで割り当てられるパソコンとIPアドレスがバッティングしないよう、所有パソコンの数＋5ぐらいを目安に入力すること。
サブネットマスク	通常は自動で入力される数値のままでよい。
デフォルトゲートウェイ	サーバーパソコンのIPアドレスを確認した際に同時に表示される「デフォルトゲートウェイ」のアドレスを入力する。ルーターのIPアドレスと同じだ。
優先DNSサーバー	ルーターによって数値は異なるが、基本的にルーターのIPアドレスを入力すればよい。
代替DNSサーバー	通常は空白のままでよい。

設定後はInternet ExplorerなどでWebブラウズして、きちんとルーターが動作しているかを確認しよう。なお、この設定を行ったあと通信できなくなる場合は、DHCPに任せる初期設定に戻して、その状態でポートマッピングを設定してもよいだろう。ほとんどのルーターは一度パソコンに割り当てたIPアドレスを覚えていて、同じアドレスを割り当て続けるため、大幅にネットワーク環境を変更しない限りIPアドレスは変更されないからだ。

▼IPアドレスの確認



設定後の状態はタスクペインで確認できる。

▼通信テスト

念のため、Internet Explorerなどを利用して通信テストを行うこと。

ルーターの設定画面にログオン

ルーターの設定の詳細はルーターのマニュアルを参照してほしいが、ほとんどのルーターは、Webブラウザのアドレス欄に「デフォルトゲートウェイ」アドレスを入力することで設定画面にログオンできる（ただし、一部のプロバイダが提供するルーター内蔵モデムでは、特定のIPアドレスを指定する必要がある。詳しくはルーターのマニュアルを参照のこと）。この際、ユーザー名とパスワードを聞かれるが（パスワードのみの場合もある）、たいていの場合、初期設定はユーザー名が「admin」（またはadministrator）、パスワードは空だ。

▼ルーターの設定画面にログオン

Webブラウザでルーターの IPアドレスにアクセスし、ダイアログ上でユーザー名とパスワードを入力する。

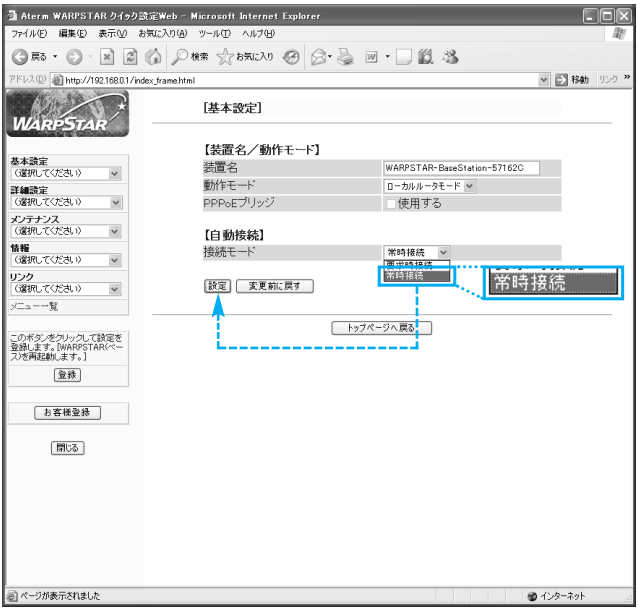
10

●回線接続の設定

ほとんどのルーターはデフォルトで「常時接続」モードになっているので問題ないが、中には「要求時接続」モード、つまりLAN内のパソコンからインターネットアクセスのリクエストがないとWANに接続しない（インターネット接続を確立しない）モードをデフォルトにしている製品もある。

この接続モードは、インターネットブラウズなど通常の利用法では問題がないが、**自宅サーバーのように「待ち受け」が必要な場合は、「常時接続」モードにして、LAN内のパソコンの状態にかかわらず「通信を常に行える」状態にしておかなければならない。**接続モードは、ルーター設定画面の「接続モード」や「自動接続」など、接続関連の項目で確認、設定できる。

▼回線接続の設定



NEC「AtermWR7600H」での例。必ず「常時接続」モードにする。

ポートマッピングの設定

ポートマッピング設定は、メーカーによって設定方法が異なるばかりか、「ポートマッピング」の名称そのものが違う場合もある。筆者が知りうる限りでも「NATテーブル編集」、「仮想サーバー設定」、「NATアドレス変換」、「バーチャルサーバー」、「アドレス変換」など、これでもかというバリエーションがある。

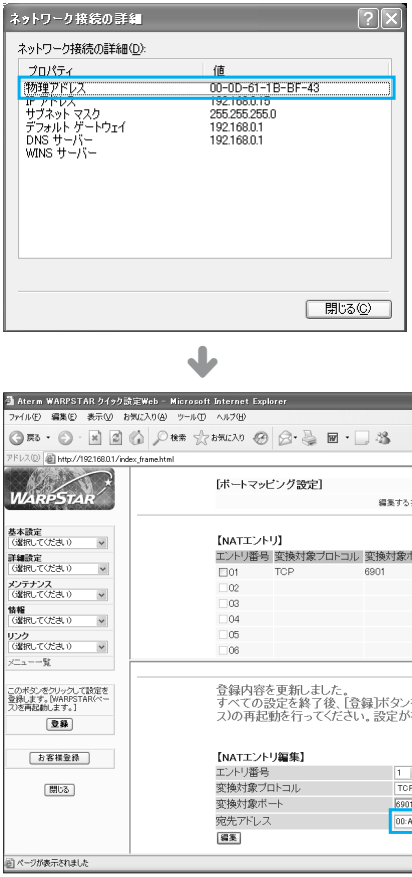
ポートマッピングの設定は、実際に自分の所有するルーターの設定画面にログオンし、以下の2タイプ（「IPアドレス指定」と「MACアドレス指定」）の設定方法のうち、当てはまるほうの設定を行えばよい。ここでは、NECのルーター「AtermWR7600H」を例に説明しよう。なお、「ポート番号」の指定は、どのサーバーアプリケーションを利用するかで異なる。具体的な番号はP.022を参照してほしい。

●MACアドレスで指定するタイプ

LANアダプタが持つ「MACアドレス」を指定してパソコンを特定するタイプのルーターでは、IPアドレスを気にせず設定することができる。たとえばNECのルーター「AtermWR7600H」の場合、「変換対象ポート」にポート番号を入力し、「宛先アドレス」に指定ポート番号に、送信先のパソコン（のLANアダプタ）が持つ「MACアドレス」を入力する（なお、このルーターでは「IPアドレス」による指定も可能）。

MACアドレスを指定するタイプのメリットは、サーバーパソコンのIPアドレスを固定する必要がないということだ。

▼ポートマッピングをMACアドレスで指定

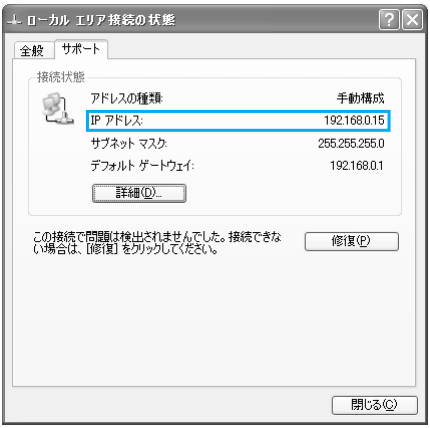


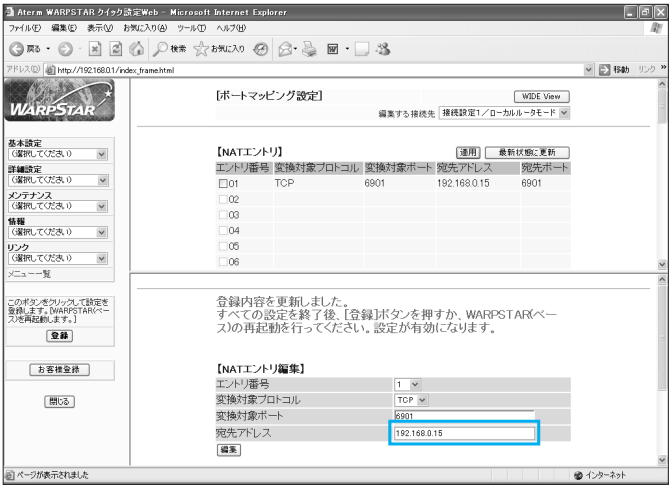
ポートマッピングを「MACアドレス」で指定する例。設定の前にあらかじめMACアドレス（物理アドレス）を調べておこう。

●IPアドレスで指定するタイプ

パソコンに割り当てているプライベートIPアドレスを指定する場合、「変換対象ポート」にポート番号を入力し、「宛先アドレス」にそのポート番号に届いたデータの送信先のパソコンに割り当てたIPアドレスを入力する。

▼ポートマッピングをIPアドレスで指定

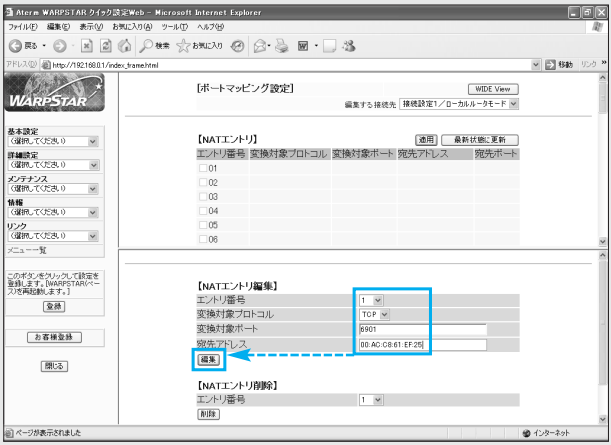




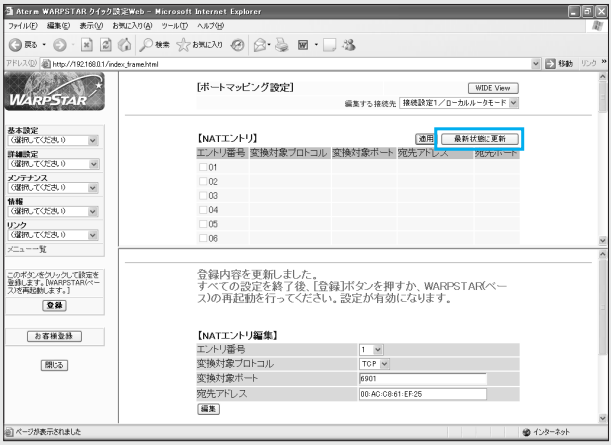
IPアドレス指定によるポートマッピングの設定。サーバーパソコンに割り当てられているIPアドレスを指定する。

COLUMN　ルーターごとのポートマッピング設定の違い

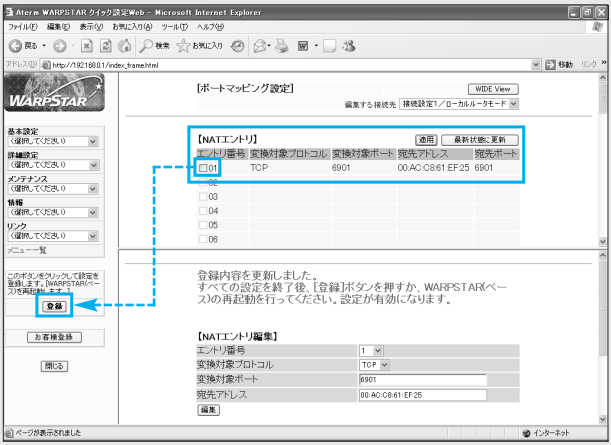
本書ではNECのルーター「AtermWR7600H」を例に説明したが、異なるメーカーのルーターでは、設定方法や設定項目が全く異なる場合もある。「AtermWR7600H」では、ポート番号とパソコン情報を設定したあと、「編集」ボタンをクリックして登録し、その後、上段の「最新状態に更新」ボタンをクリックして、エントリテーブルに反映させる。エントリテーブルに反映したら、エントリ番号のチェックボックスにチェックを入れ、有効化する…という、結構面倒くさい手順だ。



【NATエントリ編集】で任意の番号にエントリ（ポートマッピング値を入力）する。「編集」ボタンをクリック。

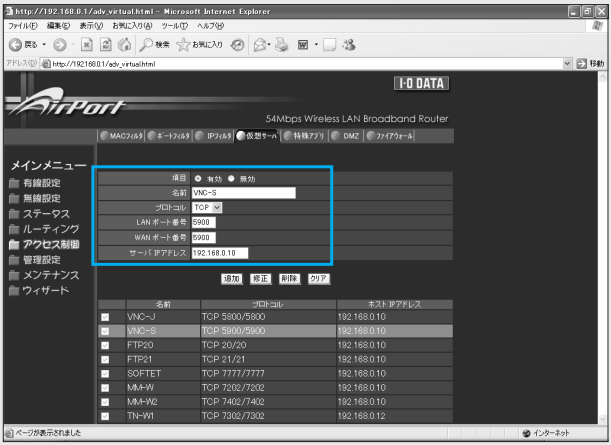


「最新状態に更新」ボタンをクリック。



「NATエントリ」（上のテーブル部分）に設定が反映される。有効化するには、さらに「エントリ番号」にチェックを入れてルーターを「再起動」しなければならない。

一方、アイ・オー・データ機器の「WN-AG/BBR-S」では、各ポートマッピングに任意の名称を付けられるほか、入力ポート（WANポート）と出力ポート（LANポート）を別々に設定できる（基本的には同じ番号でよいが）。また、登録した時点で有効化できるなど、NECのルーターより利便性が高い。ただし、サーバーパソコンの指定は「IPアドレス」でしか行うことができない。



アイ・オー・データ機器のルーター「WN-AG/BBR-S」では、入力ポートと出力ポートを別々に設定できるほか、設定ごとに名前を付けたり、登録した時点で有効無効を設定したりすることができる。

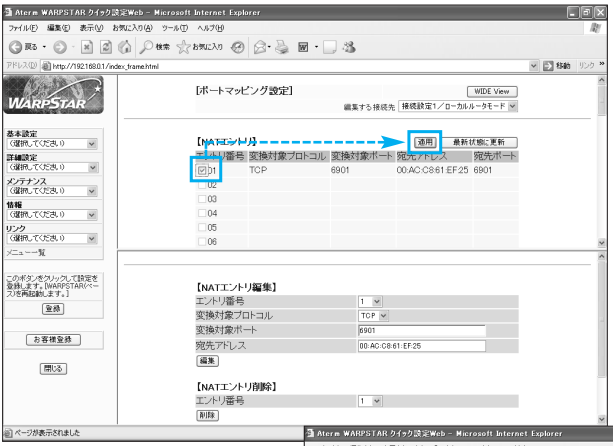
●ポートマッピングの設定の有効化

ポートマッピングの設定を有効化する方法もルーターによって異なるが、たいていの場合、以下のどちらか、あるいは両方を実行することで有効になる。

- **設定項目の「有効」にチェックを入れる**
- **ルーターを再起動する**

ほとんどのルーターは設定後に再起動を促すので、その指示に従えば有効化できる。「AtermWR7600H」では、「ポートマッピング設定」エントリテーブル内の「エントリ番号」にチェックを入れて「適用」をクリックし、再起動することで設定が反映される。

▼ポートマッピングの設定の有効化



エントリ番号にチェックを入れてから「適用」ボタンをクリック。

「登録」ボタンをクリックするとダイアログが表示されるので、「OK」ボタンを2回クリックしてルーターの再起動を待つ。「AtermWR7600H」はポートマッピングの設定にかなりのステップを要する。

Chapter 11

各サーバーをWANで実現遠隔接続を実行せよ

4章～7章で説明したリモートコントロール、ビデオ映像配信、FTPサーバー、HTTPサーバーを「遠隔接続」、つまり自宅サーバー化する方法を説明しよう。今まで説明したテクニックを組み合わせて設定を行っているので、つまづいたときはもう一度各章に戻って参照してみよう。本章で「自宅サーバー」が完成する。

1 自宅サーバーの実行の流れ

サーバー

「ダイナミックDNSの設定」と「ルーターのポートマッピング」がセットアップできていれば、あとは各サーバーアプリケーションとリンクさせれば「自宅サーバー」の完成だ。ここでは、今まで設定したサーバーの動作確認と共に、総合的なセットアップの流れを説明しよう。

なお、本章では、ローカルレベルのアクセスとWAN経由のアクセスで説明を分けるために、以下のような用語の使い分けを行うことにする。

▼WANアクセス（遠隔地アクセス）の際の用語の定義

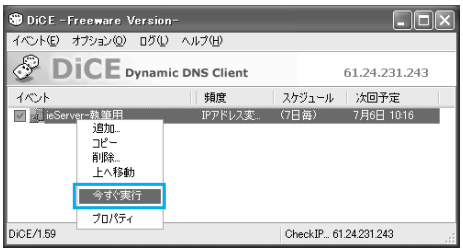
LAN接続環境の場合	WAN接続環境の場合
リモートコントロール	**遠隔リモートコントロール**
ビデオ配信	**遠隔ビデオ配信**
FTPサーバー	**自宅FTPサーバー**
HTTPサーバー	**自宅HTTPサーバー**

「DiCE」の起動とダイナミックDNSの動作の確認

サーバーパソコンでは、動的IPアドレスに対応するため、IPアドレスをDNSサーバーに知らせるソフト「DiCE」を常に起動しておく必要がある。

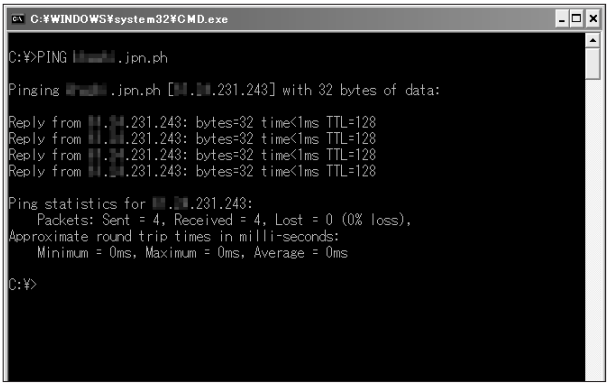
各サーバーの実行前には、「IPアドレスの手動更新（P.165参照）」を行い、さらに「ダイナミックDNSの動作の確認（P.165参照）」を行って、ダイナミックDNSが正常に機能していることを確認しておくこと。

▼IPアドレスの手動更新



「DiCE」でIPアドレスを手動更新。基本的に自動更新に任せるのが普通だが、自宅サーバーを最初に駆動するときは実行しておいたほうがよいだろう。

▼グローバルIPアドレスの確認

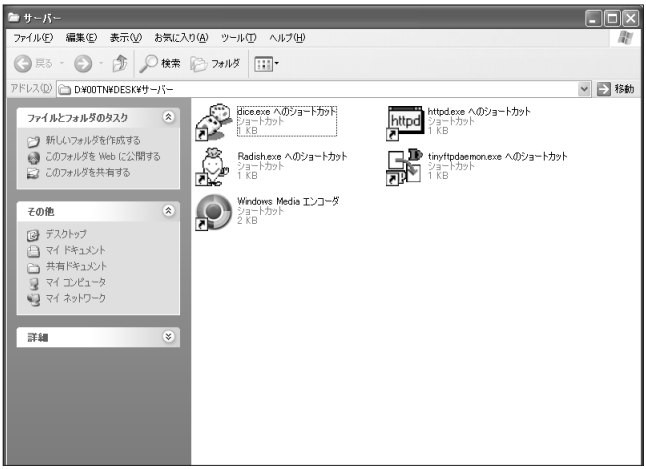


PING [アクセスドメイン]で、自分の取得したダイナミックDNSにきちんと自分の回線のグローバルIPアドレスが割り当てられているかを確認。

各サーバーアプリケーションの起動

次に、各サーバーアプリケーションの起動準備をしておこう。すべてのアプリケーション（HTTPサーバー、FTPサーバー、リモートコントロール、ビデオ配信）を同時に起動しておいても構わないが、動作確認を行う場合は、1つだけを起動してチェックしたほうがよいだろう。

▼ショートカットの利用

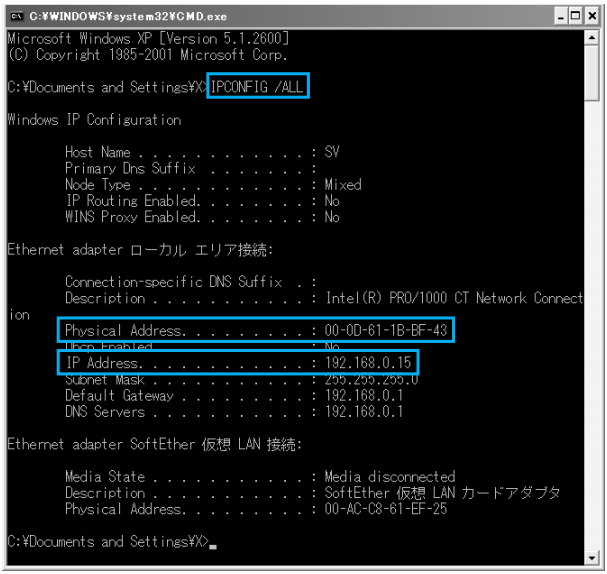


ショートカットアイコンを作成して、サーバーアプリケーションの起動をしやすくしておくとよい。

サーバーパソコンのプライベートIPアドレス&MACアドレスの確認

サーバーパソコンのプライベートIPアドレスとMACアドレスも確認しておくこと。
この情報はWAN接続を設定する際の「ルーターのポートマッピング」で必要になる。

▼IPアドレスとMACアドレスの確認



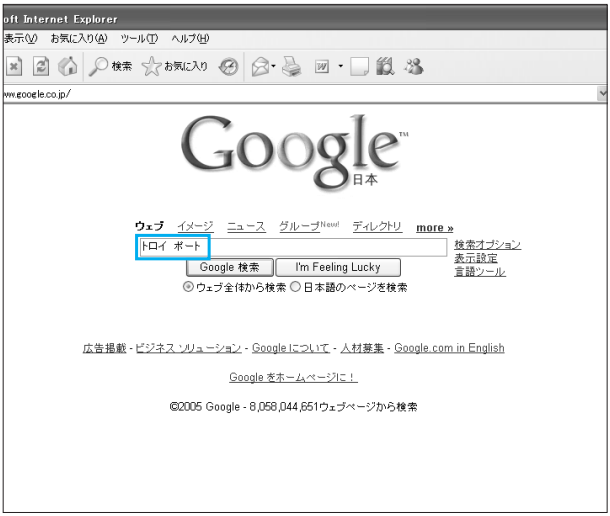
サーバーパソコンのプライベートIPアドレスとMACアドレスを確認。所有ルーターによるが、このどちらかの情報が「ポートマッピング設定」に必要になる。

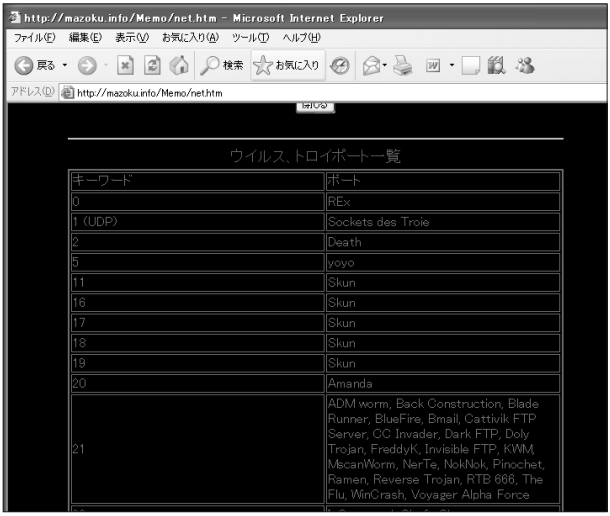
「トロイに使用されないポート番号」の確認

自宅HTTPサーバー、自宅FTPサーバーのポート番号指定は、一般的な番号の割り当てに従ったほうがよいが、遠隔リモートコントロールと遠隔ビデオ配信におけるポート番号は任意に決めてよい。ただし、**番号を決める際、「ウェルノウンポート（自宅HTTPサーバー、自宅FTPサーバー、メールサーバーなどで使用される既知のポート）」と「トロイで利用されるポート番号」は避けなければならない。**

ウェルノウンポートとのバッティングを避けるために、ポート番号には基本的に「1000番以上」の数字を指定するようにし、また「トロイで利用されるポート番号」を避けるために、Webサイトでトロイが使用する番号の情報を入手し、遠隔リモートコントロール用と遠隔ビデオ配信用に番号を2つ用意しておこう。

▼「トロイに使用されないポート番号」の確認





「トロイに使用されないポート番号」を検索サイトで確認。この一覧にあるポート番号を避けたうえで、任意の番号を2つ用意しておく。

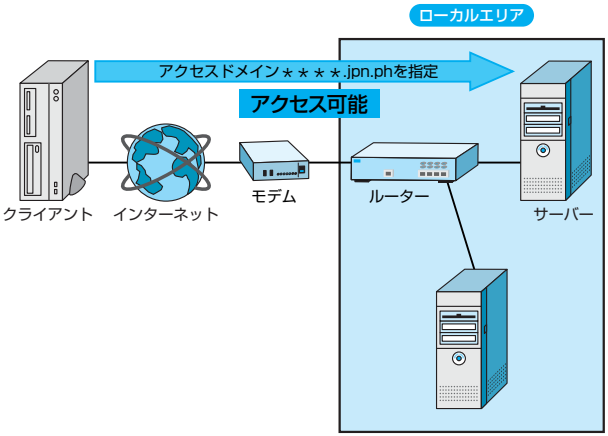
ローカルエリアからサーバーへのWANアクセスは「できない」

これから説明する、遠隔リモートコントロール、遠隔ビデオ配信、自宅FTPサーバー、自宅HTTPサーバー環境を実現したあと、接続テストを行うことになるが、このテストを行う際に注意点がひとつある。

ほとんどのルーターはセキュリティ対策のため、標準設定では「ローカルエリアからの自宅サーバーへのアクセス」を許さないようになっている。つまり、LAN内のパソコンからでは、アクセスドメインを指定した接続テストはできないのだ。

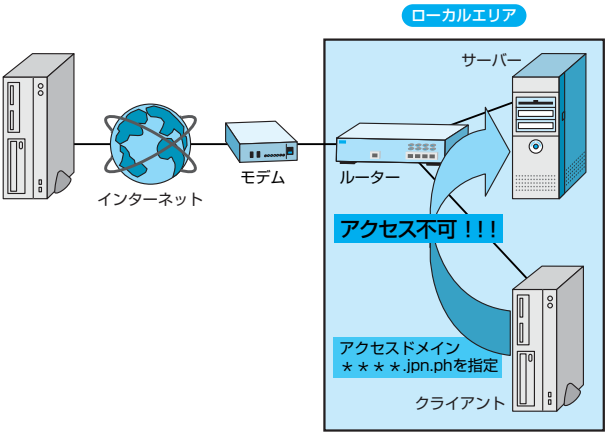
なお、いくつかのメーカーでは**「ローカルエリアからの自宅サーバーのアクセス」を許可しているものもあるが、本書では許可していない状況を前提に説明する。**

▼自宅サーバーにおいて「許される」アクセス



自宅サーバーおける一般的なアクセス。自宅サーバーは「外部回線からのアクセス」を基本としている。

▼自宅サーバーにおいて「許されない」アクセス



「アクセスドメイン（＊＊＊＊.jpn.ph等）」を指定して、ローカルエリア内のパソコンからサーバーパソコンにアクセスすることはできない。これは、ルーターのセキュリティ機能に引っかかるためだ（一部のルーターでは可能な場合もある）。

テストアクセス環境の準備

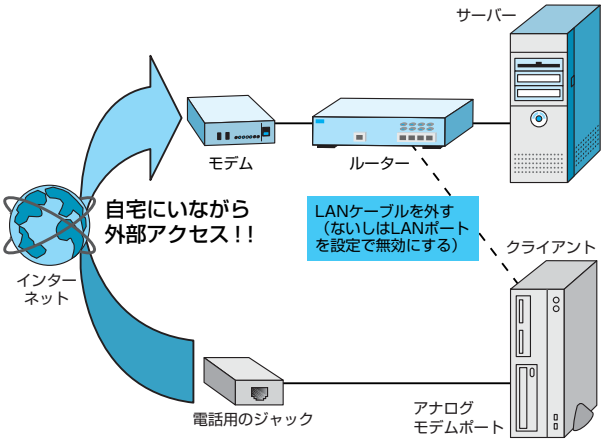
基本的にルーターはローカルエリアから自宅サーバーへの「アクセスドメイン」を指定したアクセスを許さないため、実際に環境構築が終了しても「本当に動作するか」の確認作業を行うのに困却することになる。もちろん、自宅サーバーを「自宅」に設置にしたのであれば、会社や友達の家からアクセスすればよいことのだが、これでは「設定にミス」があったときにすぐに修正できない。

そこで、自宅にいながら自宅サーバーにアクセスする手段として、以下の方法を提案したい。

●アナログモデム＋ダイヤルアップ

ノートパソコンやメーカー製のデスクトップパソコンには、「アナログモデムポート」を備えている製品もある。また、たいていのプロバイダは現在使用しているブロードバンド回線と共に「ダイヤルアップ」による接続も許可しているので、サーバー側は今のブロードバンド回線を利用し、クライアントは電話回線を使ってアクセスすれば、自宅に居ながら外部アクセスをテストできる。ただし、当然ながら「電話代」がかかることになるので、あまり長時間接続しないこと。

▼自宅にいながらの外部アクセス

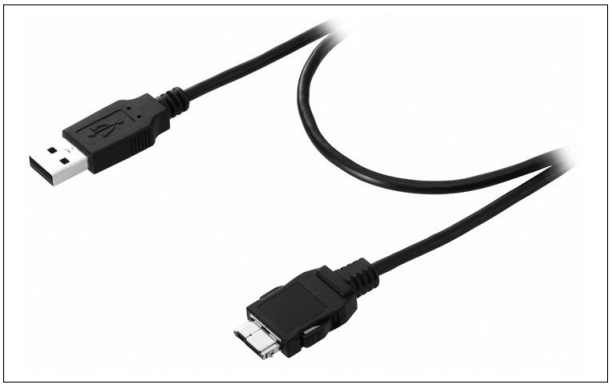


ブロードバンド回線はサーバーに割り振り、クライアントはローカルエリアのネットワークを遮断した上で、「モデム」でダイヤルアップして接続確認する。

●携帯電話＋ダイヤルアップ

これも理論としては「アナログモデム＋ダイヤルアップ」と同様で、クライアントパソコンをブロードバンド回線から切断し、携帯電話を利用して接続するというものだ。携帯電話とパソコンの接続には専用のUSB接続ケーブルが必要になるが、自宅サーバーを活用する際にモバイルアクセスする場面も考えられるので、この機会に所有しておいても損はないだろう。

▼携帯電話用USB接続ケーブル



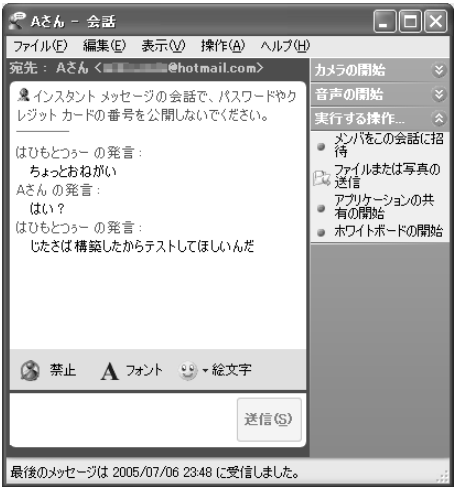
携帯電話用USB接続ケーブル。なお、このケーブルによる接続は、ノートパソコンはもちろん、デスクトップでも可能だ。

携帯電話用USB接続ケーブル：
アイ・オー・データ機器「USB-3GF」

●友達や知人にチャットやメールで連絡

信頼できる友達や知人にインターネットユーザーがいるのであれば、自宅HTTPサーバーのアドレス（アクセスドメイン）や遠隔ビデオ配信サーバーのアドレスを教えて、閲覧可能かどうかを確認してもらうとよい。その際、Windows Messengerなどで「チャットをしながら」テストしてもらえばベストだろう。なお、「遠隔リモートコントロール」は、セキュリティ上、アクセス方法を他人に教えるのはオススメしない。また、自宅FTPサーバーにはアクセス時に相性があるので（P.212参照）、接続確認するだけなら自宅HTTPサーバーか遠隔ビデオ配信で試すとよいだろう。

▼Windows Messengerでチャットしながらテスト



友人に「自宅サーバー接続確認」の連絡をするという手もある。ただし、セキュリティのことを考えると「遠隔リモートコントロール」の接続テストを他人に頼むのは控えたほうがよい。

2 遠隔リモートコントロール①

サーバー VNC　クライアント VNC専用ビューワ

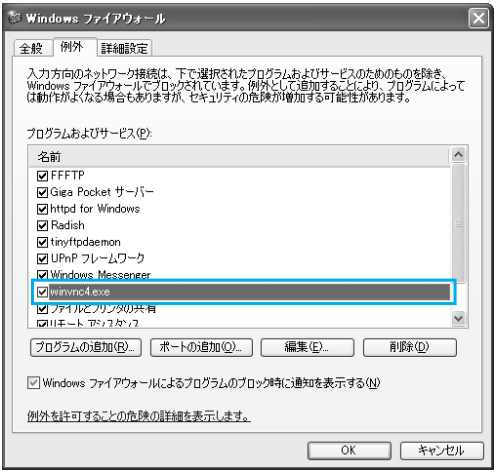
ここでは、VNCサーバー＋VNCクライアント（VNC専用ビューワ）による、遠隔接続の方法を説明しよう（Webブラウザで接続する方法は次節参照）。この遠隔リモートコントロールの設定では、「ポート番号の選択」と「ポートマッピング」がポイントになる。

サーバー

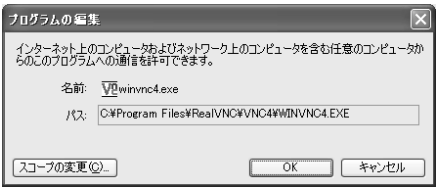
通信許可の確認

VNCのサーバーはインストール時に「サービス起動」設定が行われるため、手動で起動する必要がないが、ファイアウォールの設定は手動で行わなければならない。設定方法についてはP.051で説明したが、自宅サーバーを実現する前にもう一度確認しておこう。コントロールパネルから「Windowsファイアウォール」を選択し、「例外」タブをクリックして「プログラムとサービス」欄で確認できる。

▼VNCの通信許可の確認



ファイアウォールでVNCの通信許可がきちんと行われているかを確認。



サーバー

VNCのポート設定の確認

VNCが利用するポート番号を確認する。通知領域の「VNCアイコン」をダブルクリックして表示される「VNC Server Properties」ダイアログの「接続要求ポート」に使用中のポート番号が表示される。

ローカルエリア接続の場合は、セキュリティの脅威がないため何番でもよかったが、WAN接続では「トロイが使用するポート番号（P.186参照）」を利用しないように気をつけよう。特に、クライアントからポート番号なしでアクセスできてしまうので、デフォルトのポート番号は使わないようにしよう（P.143参照）。

▼VNCのポート設定の確認

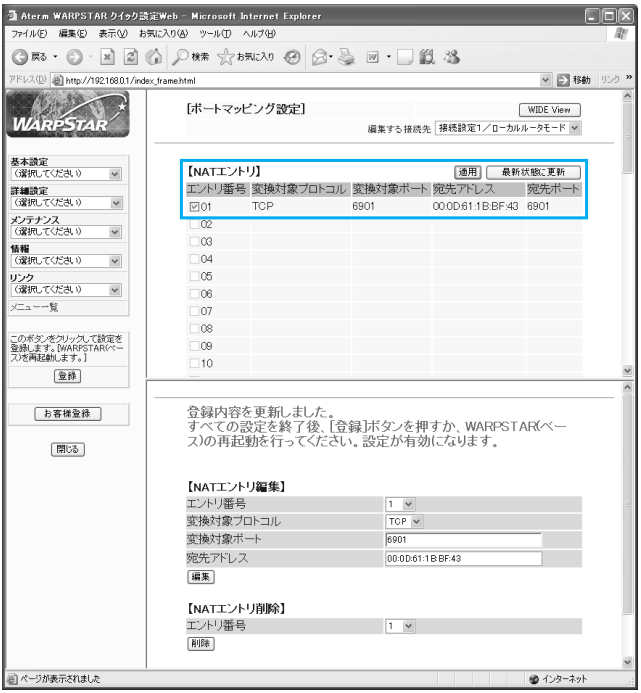
「接続要求ポート」でVNCのポート番号を設定。ここでは「6901番」を指定している。

サーバー

ルーターのポートマッピングの設定

WAN接続で利用するには、ルーターのポートマッピングを行って、指定したポート番号に届いた信号をVNCが起動しているサーバーパソコンに送るよう設定する必要がある。先に確認しておいたVNCのポート番号（接続要求ポート）と、サーバーのアドレス（IPアドレスかMACアドレス）を指定する。

▼ルーターのポートマッピング設定



ルーターのポートマッピング設定。ポート番号は「VNCの設定で指定したポート番号」に合わせる。ルーターのポートマッピングの方法については10章参照のこと。

クライアント

遠隔リモートコントロール

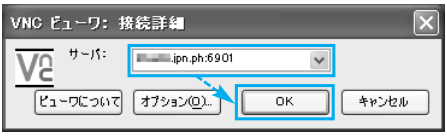
クライアントの「VNCビューワ」を起動して、サーバーを以下のように指定する。

▼アクセスアドレス

[アクセスドメイン]:[ポート番号]

たとえば、アクセスドメインが「＊＊＊＊.jpn.ph」、VNCの指定ポートが「6901」なら「＊＊＊＊.jpn.ph:6901」と指定すればよい。アクセスしたあとは、VNCサーバーで設定したパスワードを入力すれば、遠隔リモートコントロールできるようになる。

▼遠隔リモートコントロール



「[アクセスドメイン]:[ポート番号]」と指定。

パスワードを入力すれば、遠隔リモートコントロールが実現する。

COLUMN　「遠隔リモートコントロール」さえ起動しておけば…

この「遠隔リモートコントロール」さえ実現してしまえば、実はこれ以後に説明する「遠隔ビデオ配信」、「自宅FTPサーバー」、「自宅HTTPサーバー」の各種設定はすべて遠隔地のパソコンから実行できる。そういう意味もあって、本書では「遠隔リモートコントロール」を最初のサーバーテクニックとして説明した。

遠隔リモートコントロールできるということは、アプリケーションのインストールや各種設定が行え、またWindowsの再起動やルーターのポートマッピング設定など、パソコンのすべての機能を操作できることを意味する。逆に言えば、第三者にどんな不正行為も許してしまうのが遠隔リモートコントロールなので、アクセスアドレスとパスワードはとりわけ厳重に管理する必要がある。

3 遠隔リモートコントロール②

サーバー VNC　クライアント Webブラウザ

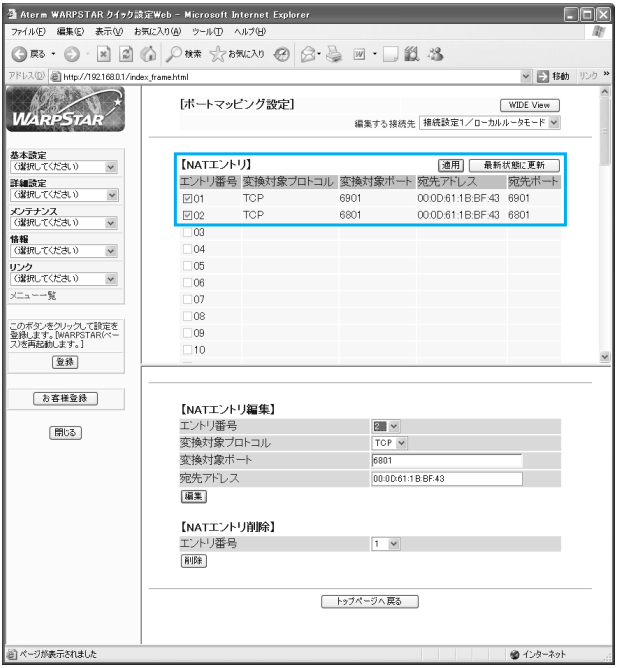
VNCサーバーにクライアントからWebブラウザを利用して接続するための、設定、操作手順を紹介しよう。「通信許可の確認」「VNCのポート設定の確認」は、11-02で説明したクライアントに「VNCビューワ」を選択した場合と同様なので省略するが、サーバー側の「Javaポート番号の設定」と、クライアント側の「Javaのインストールの確認」を行う必要がある。

サーバー

ルーターのポートマッピングの設定

Webブラウザでリモートコントロール接続を行う場合、**先に説明した「接続要求ポート」に加えて「Java用のポート」もポートマッピングする必要がある。**Java用のポート番号は「VNC Server Properties」ダイアログの設定に合わせる。

▼ルーターのポートマッピング設定



ルーターのポートマッピング設定。ルーターのポートマッピングの方法については10章参照のこと。

クライアント

遠隔リモートコントロール

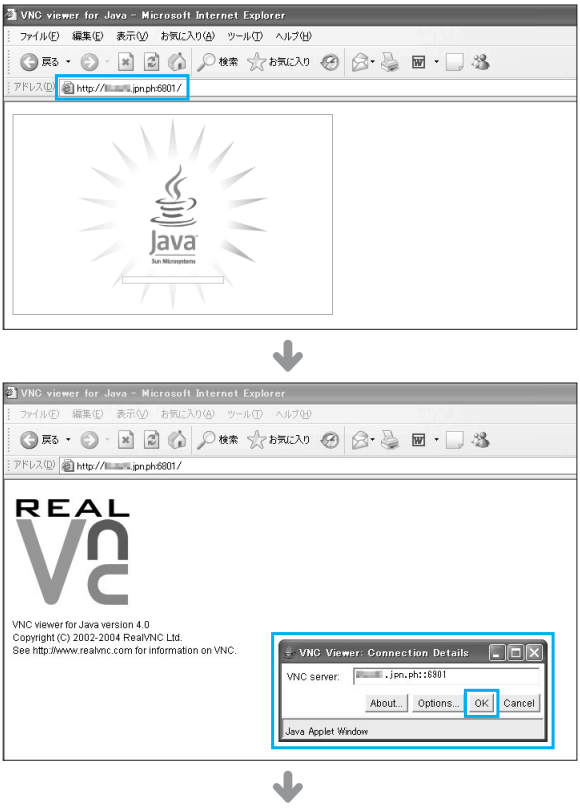
WebブラウザでVNCサーバーにアクセスする場合の必須条件は、「Javaがインストールされている」ことである。うまくアクセスできないときは、P.054を参考にJavaをインストールしよう。

Javaがインストールされていれば、Webブラウザ（Internet Explorer）を起動し、アドレス指定で「アクセスアドレス」を入力すれば遠隔リモートコントロールが実現する。アクセスアドレスは以下のように入力しよう。

▼アクセスアドレス

http://[アクセスドメイン]:[Javaポート番号]

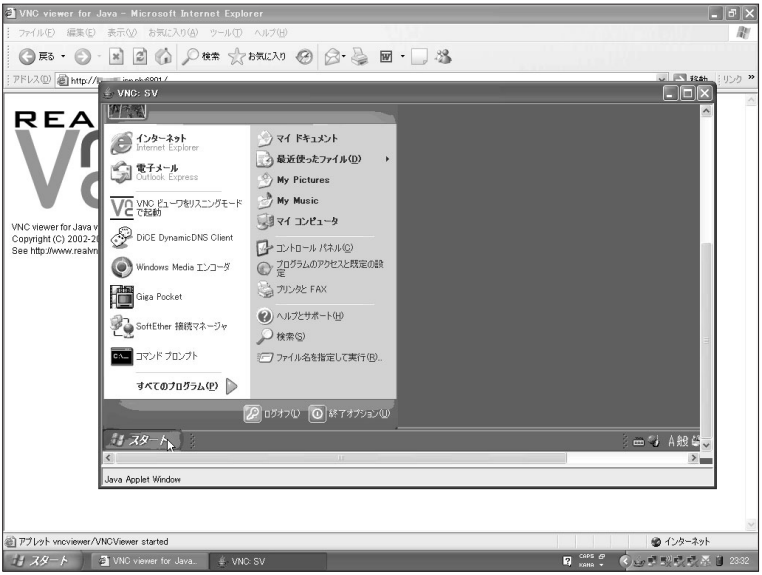
▼遠隔リモートコントロール



アクセスアドレスに「http://[アクセスドメイン]:[Javaポート番号]」を指定。

ダイアログが表示されるので「OK」ボタンをクリック。

パスワード入力を行えば、VNCサーバーにアクセスできる。



4 遠隔ビデオ配信

サーバー Windows Mediaエンコーダ
クライアント Windows Media Player

遠隔ライブ映像配信の設定は、2つの点に注意する。1つは、遠隔リモートコントロールと同様、ポート番号の選択。そしてもう1つが、配信する映像の品質調整だ。遠隔接続の場合、外部からの接続に利用する回線の太さに違いがあるため、貧弱な回線では重すぎで再生できなくなるなどの問題が発生することがある。その場合は、配信する映像のビットレート調整が必要になる。

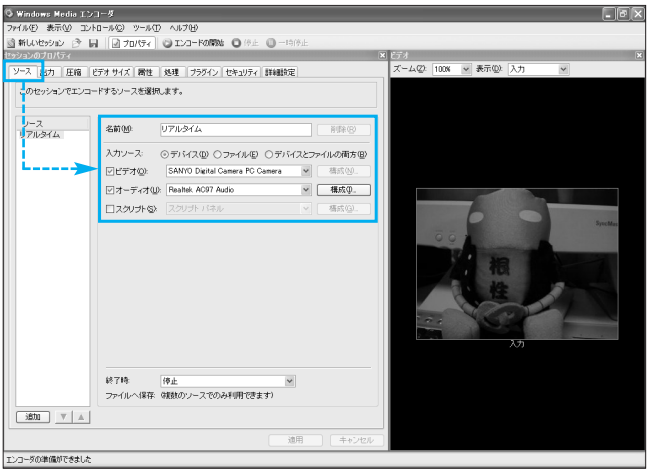
サーバー

Windows Mediaエンコーダの前準備

5章で作成した設定ファイルを保存しているのであれば、Windows Mediaエンコーダを起動して、設定ファイルを読み込もう。

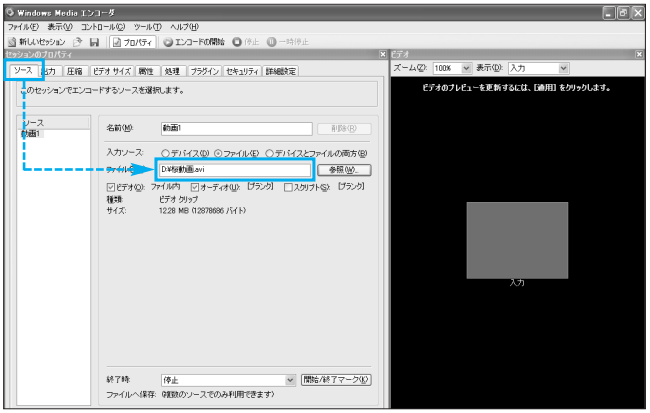
さらに、ライブ映像配信を実行する場合は、入力ソースとなるデバイス（ビデオとオーディオ）がきちんと動作しているかを確認し、動画ファイルを配信する場合は、動画ファイルのパス指定に間違いがないかを確認する。

▼ライブ映像配信の設定



Webカメラやデジタルカメラを利用したライブ映像配信の設定。各デバイスがきちんと指定されているか、正常に動作しているかを確認する。

▼動画ファイルの配信設定



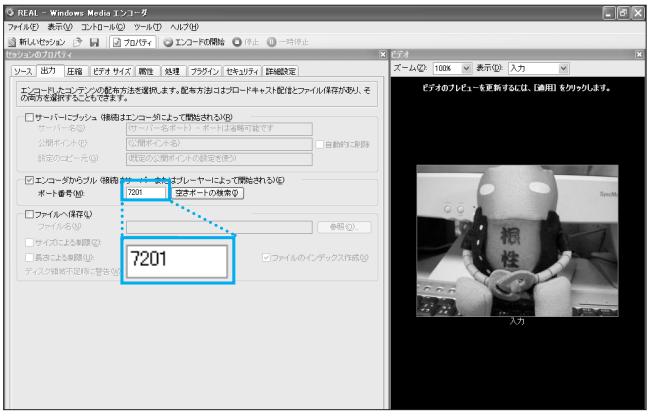
動画ファイルの配信であれば、動画ファイルの設定に誤りがないか確認する。

サーバー

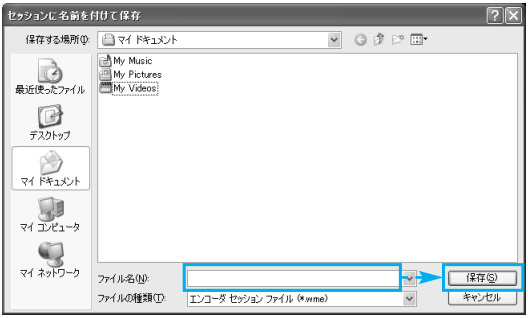
Windows Mediaエンコーダのポート設定の確認

WAN接続の場合、セキュリティを考えて「トロイが使用するポートではないもの」をポート番号としてセレクトする。なお、Windows Mediaエンコーダは再起動するごとにこのポート番号設定をリセットしてしまうため、ポート設定したあとは、次回配信時でも同じポートを利用するように「設定保存」を行う必要がある。

▼ポート番号の設定

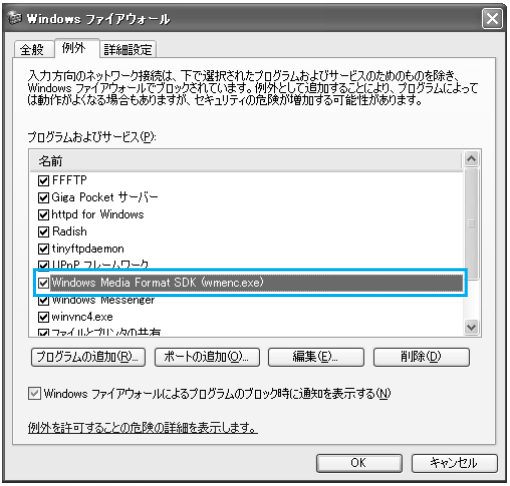


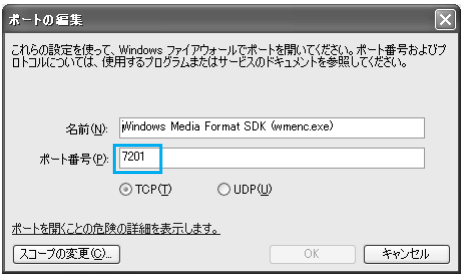
ポート番号の設定。ここでは「7201」番を指定した。指定後に「設定保存」を行い、以後はその設定を読み込むようにする。



任意の名前を付けて設定ファイルを保存する。

▼Windowsファイアウォール





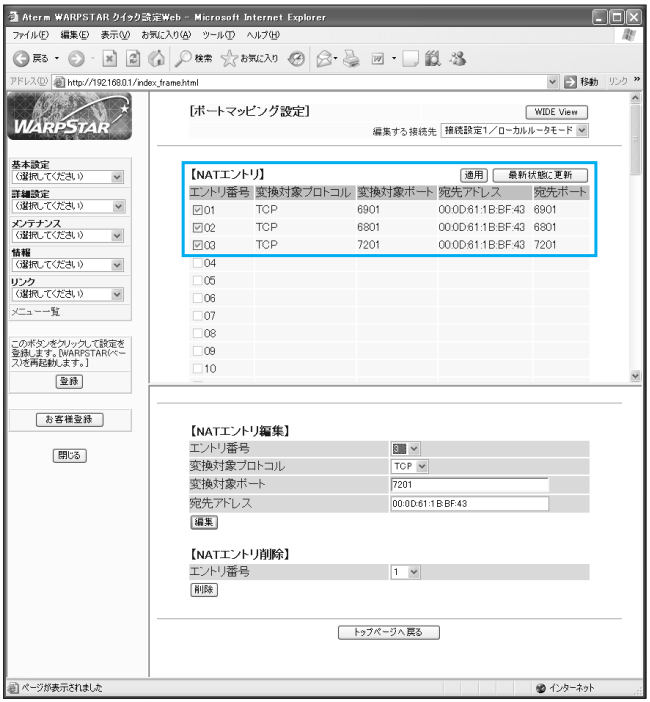
Windows Mediaエンコーダの場合、「Windowsファイアウォール」の設定は自動的に行われる。

サーバー

ルーターのポートマッピング設定

Windows Mediaエンコーダのポート設定に従って、ルーターのポートマッピング設定を行う。

▼ルーターのポートマッピング設定



ルーターのポートマッピング設定。ルーターのポートマッピングの方法については10章参照のこと。

サーバー

エンコードの開始

ほかのサーバーアプリケーションは「起動するだけで」サーバーが機能したが、Windows Mediaエンコーダで映像配信する場合、エンコードを実行しないとサーバーとして動作しない。配信を行う際は「エンコードの開始」ボタンをクリックする。

▼エンコードの開始

「エンコードの開始」ボタンをクリックして、配信を開始する。

クライアント

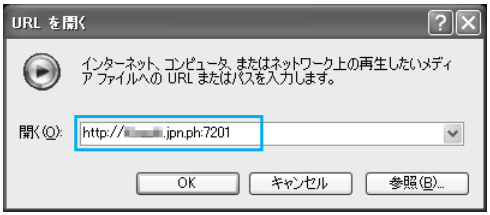
遠隔ビデオ配信の閲覧

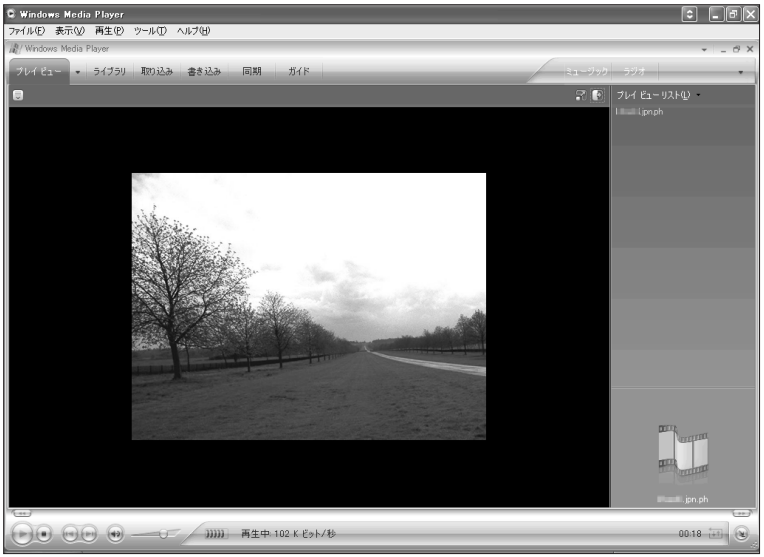
遠隔ビデオ配信を閲覧するには、クライアント側でWindows Media Playerを起動し、メニューバーから「ファイル」－「URLを開く」を選択する。「URLを開く」ダイアログが表示されたら、「開く」欄に以下のように入力する。

▼アクセスアドレス

```
http://[アクセスドメイン]:[ポート番号]
```

▼遠隔クライアントからのアクセス





遠隔クライアントからのアクセスは、アドレス指定で「http://[アクセスドメイン]:[ポート番号]」と指定する。これでWindows Mediaエンコーダが送信する映像を閲覧できる。

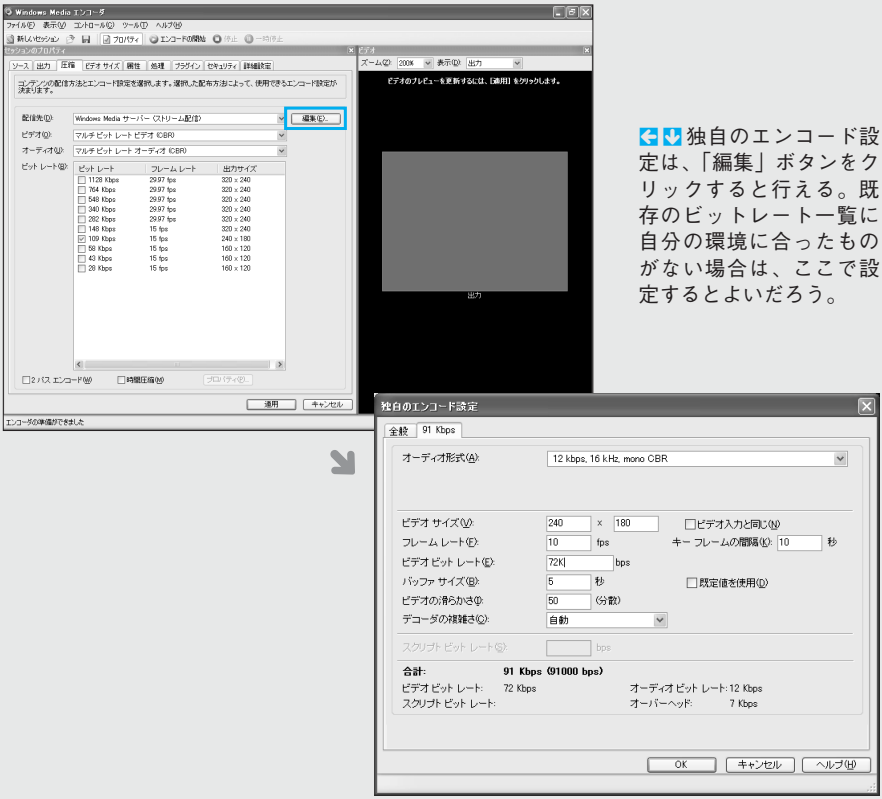
COLUMN　回線に応じてビットレートを下げる

サーバー回線のアップロードスピード、そして遠隔地のクライアント回線のダウンロードスピードが、「遠隔ビデオ配信」設定のキモになる。利用する回線のスピードに合わせて、最も適切な映像品質、ビットレートを設定する必要がある。回線スピードは当然ながら利用環境ごとに異なるので、クライアントから接続テストを行って、再生が重すぎるようなら調整を行おう。

送信ビットレートの調整は、ツールバーの「プロパティ」をクリックして、「セッションのプロパティ」ダイアログの「圧縮」タブで設定することができる。クライアントの待ち時間が多すぎたり、映像がスムーズに再生されなかったりする場合は、ビットレートを下げてみよう（詳しくはP.080参照）。

なお、映像のビットレートは、「圧縮」タブ内のビットレート設定一覧から選択する以外に、「編集」ボタンをクリックしてより詳細に設定することもできる。動画ファイルのエンコードについて理解しているなら難しくないので、エンコード設定のカスタマイズにチャレンジしてもよいだろう。

▼エンコード設定のカスタマイズ



独自のエンコード設定は、「編集」ボタンをクリックすると行える。既存のビットレート一覧に自分の環境に合ったものがない場合は、ここで設定するとよいだろう。

5 自宅FTPサーバー

サーバー Tiny FTP Daemon　クライアント FFFTP

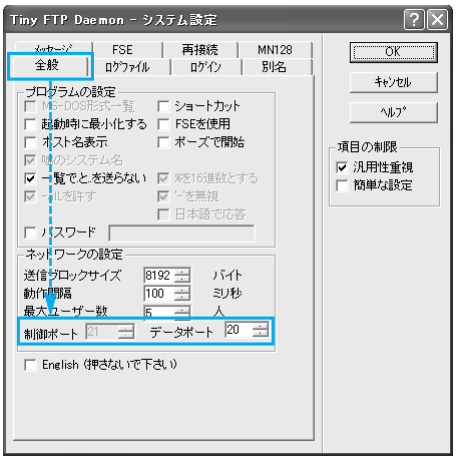
FTP自体はクライアントとしてホームページの作成などでよく利用していると思うが、自分がサーバー（ホスト）を運営する場合は、運営方針やルールをしっかり決めておかなければならない。たとえば、他人に公開するのであれば、誰にどこまでのアクセスを許すかをしっかりと定義しておく必要がある。そういう意味では、一番難しいのはFTPサーバーの設定ではなく、「ユーザーの管理」であろう。

サーバー

Tiny FTP Daemonのポート設定の確認

自宅FTPサーバーでは「制御用」と「データ転送用」の2つのポート番号が必要で、**「制御用」としてポート21番、「データ転送用」として20番**を利用するのが標準になっている。この設定を確認する場合は、メニューバーから「設定」－「システム設定」を選択。「システム設定」ダイアログの「全般」タブをクリックして「ネットワーク設定」欄を表示する。

▼Tiny FTP Daemonのポート設定の確認

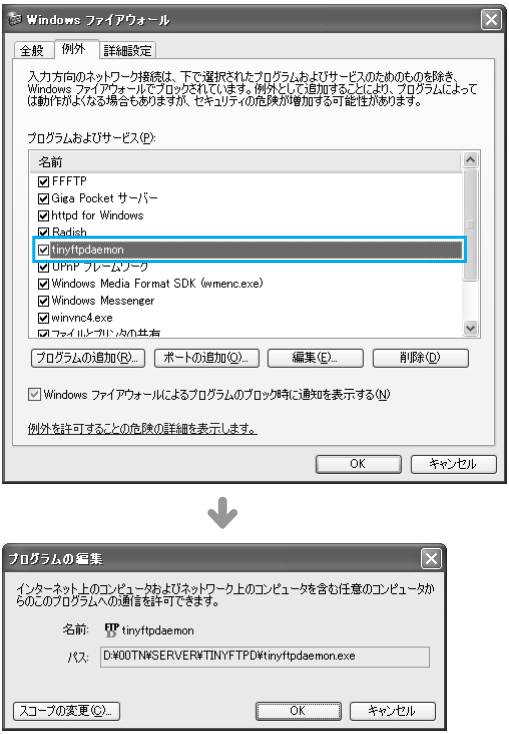


「制御ポート」が21番、「データポート」が20番であることを確認する。なお、これらの設定を変更する場合は、「項目の設定」欄のチェックボックスを外す必要がある。

通信許可の確認（ファイアウォール）

「Tiny FTP Daemon」の通信許可を行っているかどうか確認する。コントロールパネルから「Windowsファイアウォール」を選択し、「例外」タブをクリックすると表示される「プログラムとサービス」欄で確認できる。

▼「Tiny FTP Daemon」の通信許可の確認



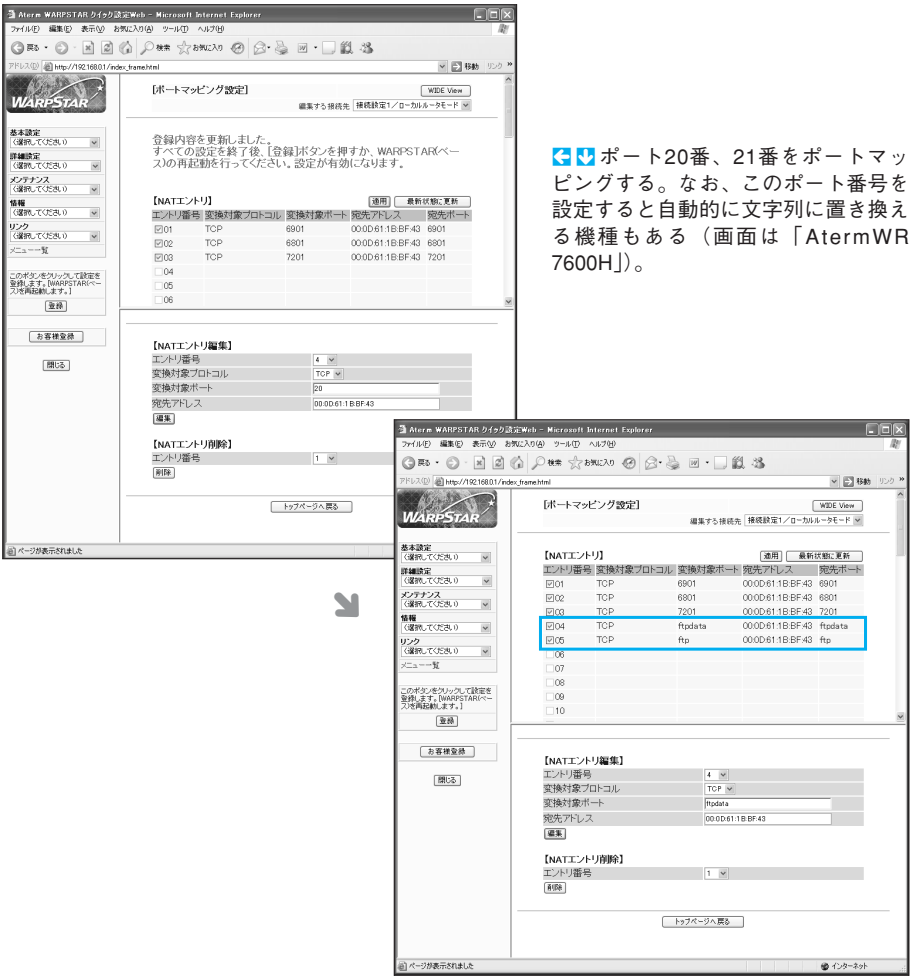
Windowsファイアウォールにおける「Tiny FTP Daemon」の通信許可設定。

サーバー

ルーターのポートマッピング設定

WAN接続で自宅FTPサーバーを利用できるよう、ルーターのポートマッピング設定を行う。自宅FTPサーバーの場合、20番、21番をポートマッピングする。なお、ポートマッピングの際、ルーターによっては20番を「ftpdata」、21番を「ftp」という表記に置き換えることがある。

▼ルーターのポートマッピング設定



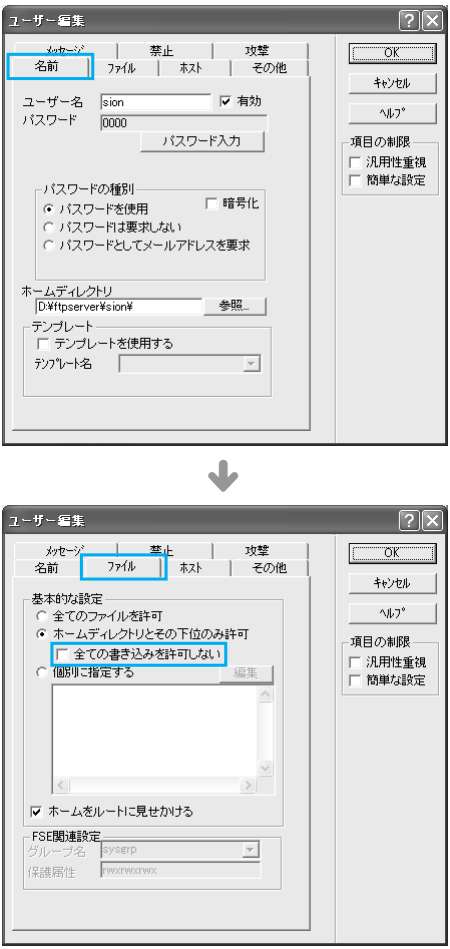
ポート20番、21番をポートマッピングする。なお、このポート番号を設定すると自動的に文字列に置き換える機種もある（画面は「AtermWR7600H」）。

サーバー

ユーザー設定の確認

6章で設定した、接続を許可するユーザーの設定を確認する。特にユーザー名とパスワードは、しっかり確認しておこう。**なお、接続テストを行う場合は、「書き込み」を許可したユーザーを作成し、そのユーザーでアクセスして、ダウンロードとアップロードの双方に問題がないことを確認するとよいだろう。**

▼ユーザー設定の確認



ユーザー設定の確認。「ファイル」タブの「全ての書き込みを許可しない」のチェックを外せば、書き込みも行えるユーザーになる。

クライアント

自宅FTPサーバーへのアクセス

FTPサーバーへのアクセスはどのFTPクライアントを利用してもよいが、ここでは本書で紹介している「FFFTP」を使って説明する。

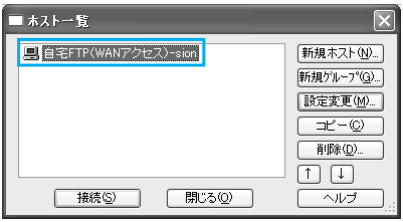
FFFTPを起動したら、「ホスト一覧」ダイアログから「新規ホスト」ボタンをクリックする。ホストの設定で、「ホスト名（アドレス）」として以下の要領でアクセスドメインを入力する。

▼FFFTPのホストの設定

ホストの設定名	任意の名前を入力。「ホスト一覧」に表示される文字なので「[ロケーション]-[アクセスドメイン]-[ユーザー名]」のようにわかりやすく命名する。
ホスト名（アドレス）	アクセス先のアドレスを入力。遠隔からのログオンであれば「アクセスドメイン名」を記入する。
ユーザー名／パスワード	サーバー側でアクセスを許可したユーザー名、パスワードを入力する。

設定が終了したら、作成したホストを選択して自宅FTPサーバーにアクセスし、ファイルのアップロードやダウンロードなどをテストしてみよう。

▼自宅FTPサーバーへのアクセス



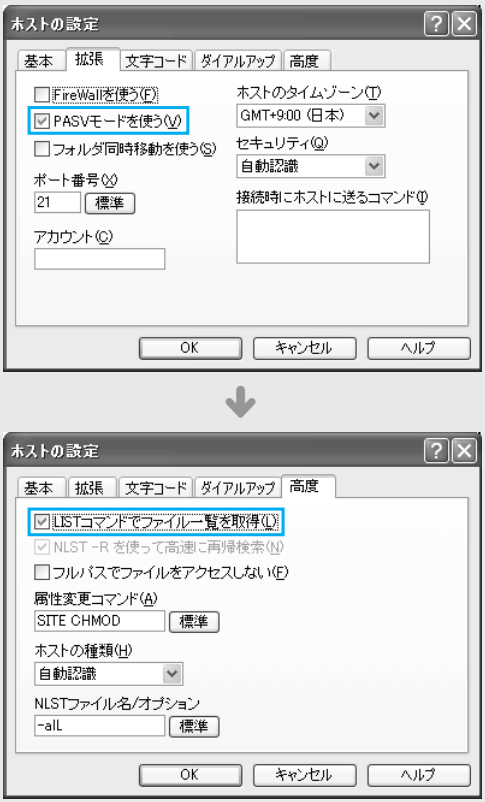
作成ホストで自宅FTPサーバーにアクセス。

アップロードやダウンロードなどを行い、動作を確認する。

COLUMN 自宅FTPサーバーに接続できないときは

自宅FTPサーバーでは、「回線」、「自宅FTPサーバー」、「FTPクライアント」の相性のために、デフォルトの設定では接続できない場合がある。
その際に着目すべき設定は、「PASVモード」と「LISTコマンド」だ。この2つの設定を変更することで、サーバーに接続できるようになる可能性がある。FFFTPの場合は「ホスト設定」画面の「拡張」タブと「高度」タブで設定変更できるので、FTPサーバーにアクセスできないときはオン／オフを切り替えてみるとよいだろう。

▼FFFTPの設定変更



FTPサーバーに接続できないときは、「ホスト設定」で「PASVモード」と「LISTコマンド」の有効／無効を変更する。なお、接続できる場合でも、この設定のオン／オフでログオン後のリスト表示の速さなどに差が出ることがある。

6 自宅HTTPサーバー

サーバー AN HTTPD　クライアント Internet Explorer

自宅HTTPサーバーの設定は難しいことはない。サーバーもクライアントもルールが明確なため、「ポートマッピング設定」さえきちんと設定していれば、難なくアクセスすることができる。

サーバー

AN HTTPDの起動と設定確認

自宅HTTPサーバーアプリケーションである「AN HTTPD」を起動して設定を確認する。もちろん、サービスモードで起動する設定になっていれば自分で起動する必要はない。「AN HTTPD」が起動しているかどうかは、通知領域で確認できる。

「AN HTTPD」はほかのサーバーアプリケーションと異なり、メインウィンドウの「閉じる」ボタン☒をクリックすると終了してしまう。不用意に終了してしまわないように注意しよう。

▼AN HTTPDの起動

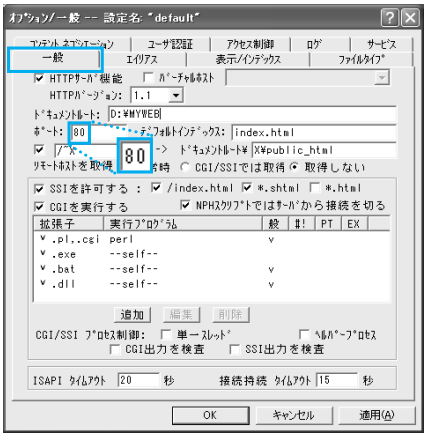
「AN HTTPD」のメインウィンドウ。何の問い合わせも無く終了してしまうので、アプリケーションを閉じる「クセ」のある人は注意する必要がある。

サーバー

AN HTTPDポート設定確認

自宅HTTPサーバーにおける通信は、標準化されているポート80番を利用する。AN HTTPDの「オプション／一般」ダイアログを開いて、「一般」タブで「80番」に設定されているかを確認しておこう。また、「ドキュメントルート」や「CGIロケーション設定」が正しく設定されているかも再度確認するとよいだろう（P.113/P.121参照）。

▼AN HTTPDポート設定確認

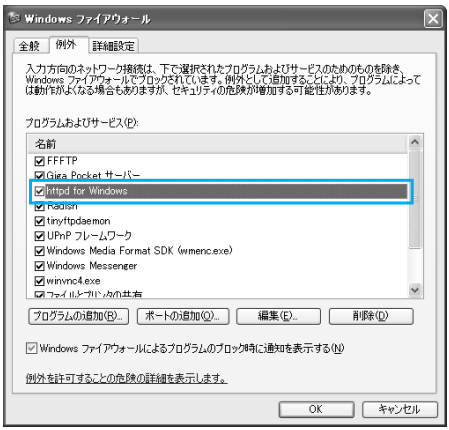


ポート番号設定が「80番」であることを確認する。なお、諸事情で「80番以外」を設定する場合は、ポートマッピング設定をその番号に置き換え、ブラウズ時にもポート番号を指定する必要がある。

通信許可の確認（ファイアウォール）

「AN HTTPD」の通信許可がきちんと行われているかを確認する。コントロールパネルから「Windowsファイアウォール」を選択。「例外」タブをクリックして「プログラムとサービス」欄で確認できる。

▼「AN HTTPD」の通信許可の確認



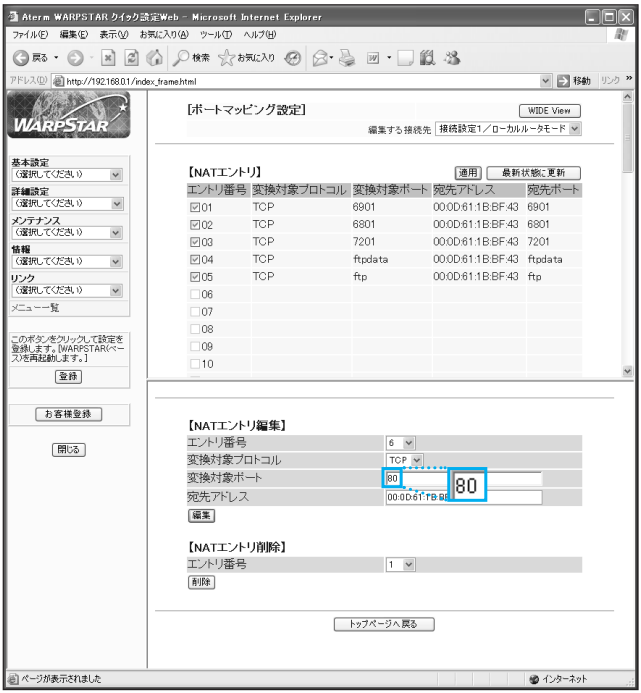
「AN HTTPD」の通信許可が行われていることを確認。

サーバー

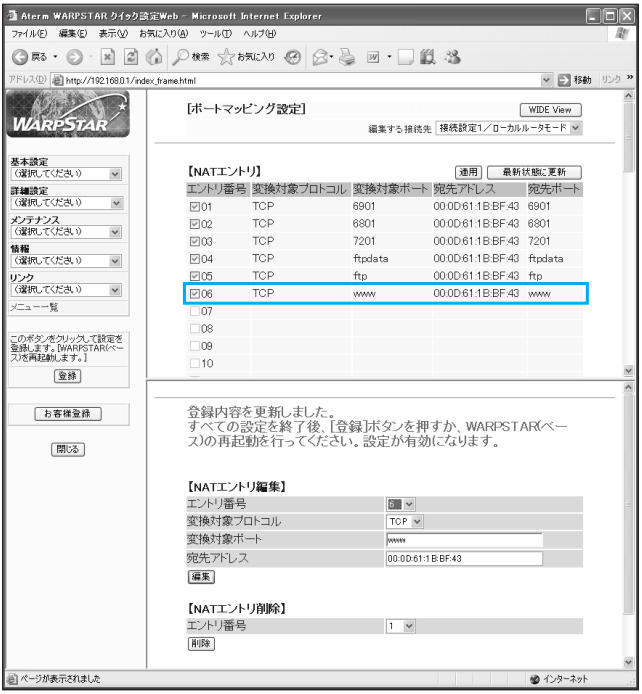
ルーターのポートマッピング設定

自宅HTTPサーバーのために、ポート80番のポートマッピング設定をルーター設定画面で行う。なお、ルーターによっては、ポートマッピングの際に80番を「www」や「http」などの文字に置き換えることがある。

▼ルーターのポートマッピング設定



ポート80番をポートマッピングする。なお、このポート番号を設定すると自動的に「www」などの文字に置き換える機種もある（画面は「AtermWR7600H」）。



クライアント

遠隔Web閲覧

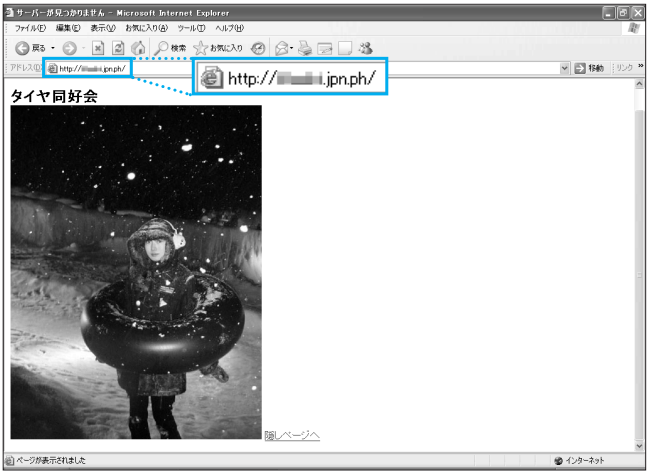
自宅HTTPサーバーのWebページを遠隔地のクライアントから閲覧するには、Internet Explorer（ほかのWebブラウザでも可）を起動し、アドレス欄に以下のように入力する。

▼アクセスアドレス

http://[アクセスドメイン]

なお、接続確認を行う場合、あらかじめWebブラウザの「キャッシュ（インターネット一時ファイル）」を消去しておいたほうがよいだろう。Internet Explorerの場合は、メニューから「ツール」－「インターネットオプション」を選択し、「全般」タブの「ファイルの削除」ボタンをクリックする。

▼自宅HTTPサーバーのWebページの閲覧



Internet Explorerのアドレスバーに「http://[アクセスドメイン]」と入力すると、HTTPサーバーに作成したWebサイトを閲覧できる。

COLUMN　自宅HTTPサーバーの活用法

自分のWebページをインターネット上で公開する場合、普通に考えれば「プロバイダに割り当てられたWebサーバー領域」にHTMLをアップロードしたほうがよい。自分の回線負荷をかけることもなく、またクラッキングなどの心配もないからだ。あえて自宅HTTPサーバーを有効利用できるケースを挙げるなら、まず「会社などのローカルエリア内限定のサイト」が考えられる。ブラウザを起動する際に表示されるページ（ホームページ）をこのHTTPサーバーのサイトにしておけば、内部の業務連絡などに活用することができる。

もう1つの利用法は、「ファイルの容量や種類に制限がない」という点を生かし、ファイルサーバー的に使うことだ。このとき、プロバイダに割り当てられたWebスペースにトップページを置き、そこから自宅HTTPサーバーに置いたコンテンツにリンクを張るようにするとよいだろう。

Chapter 12

メールサーバー& メールアカウントを構築せよ

本章では、「自宅メールサーバー」の構築方法を説明しよう。自宅メールサーバーは「ダイナミックDNSサービス」に大きく依存したテクニックであり、これまでのサーバーとは設定の手順が異なるので、理論や留意点を理解してから実践してほしい。なお、自宅メールサーバーは利用の際に「モラル」が求められる。悪用は厳禁だ。

メールサーバーの構築とは

本書では、「各サーバーのテクニック（リモートコントロール、ビデオ配信、FTPサーバー、HTTPサーバー）」を先に解説したあと「WAN接続テクニック」を紹介するという流れで、自宅サーバー構築のテクニックを解説してきた。しかし、「メールサーバー」の設定についてのみ、この流れを破って最終章で説明することにする。

その理由は2つある。

1つは、各サーバー機能の中で「メールサーバー」だけは「ダイナミックDNS」を設定しないと実現できない、という根本的な理由である。自宅メールサーバーにおけるメールアドレスは「[任意の文字列]@[アクセスドメイン]」という形になるため、ダイナミックDNSでアクセスドメインの取得は必須なのだ。

そしてもう1つが、「積極的に導入する理由が希薄である」という理由だ。

メールサーバーの特性上、運用するためには基本的にサーバーを「立ち上げっぱなし」にする必要がある（立ち上げていないとメールが送信元にリターンされてしまうため）。加えて、通信回線の信頼性や利用用途を考えると、自宅メールを利用するぐらいなら「フリーメール（ホットメールなど）」を利用するほうが便利なケースが多い。

また、無料であることが多い「ダイナミックDNSサービス」は恒久的な利用が保障されていないため、**ある日いきなりサービスが終了してメールアドレスが使えなくなる可能性もある。**ある日突然利用できなくなるのでは、「アドレス」としては使い物にならない。

もちろん、自宅メールサーバーにもメリットはある。フリーメールのほとんどがWebメールであるのに対して「POP3サーバーを利用できる（メールソフトを利用できる）」ことや、メールアドレスを事実上無限に作成できることなどだ。

▼自宅メールサーバーのメリットとデメリット

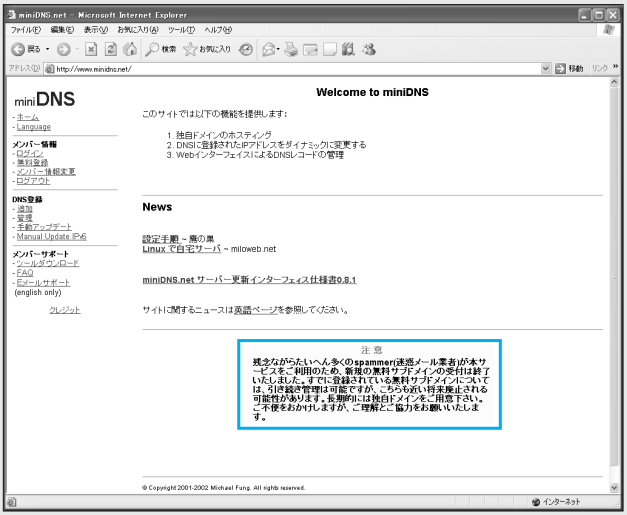
	自宅サーバー	フリーメール
容量	事実上無限	有限
恒久性	低い	高い
利便性	高い（メールソフト利用可）	低い（ブラウザ上のみ）
利用できるアドレス	無限	サービスごとに1つだけ

COLUMN　メールアドレスの悪用

非常に残念な話だが、自宅メールサーバーを「スパムメール」の配布に利用している業者がたくさんいる。プロバイダメールに比べ、「無数のメールアドレスを作れる」「プロバイダに使用を制限されない（面が割れない）」という特性を生かした悪質な使い方だ。そして、このような使い方をする悪者のために、数々の良心的な「ダイナミックDNSサービス」が閉鎖に追い込まれており、その結果、私たちのような一般のユーザーが迷惑をこうむっているのだ。

また、明らかなスパムメールに限らず、自宅メールサーバーを利用してイタズラメールを送ったり、匿名で抗議メールを投書したりするようなことも、受け取る相手の迷惑になる。くれぐれも、自宅メールサーバーを悪用しないよう、気をつけてほしい。

▼「無料アクセスドメイン」サービスのサイト



スパムメールを送るユーザーのせいで「無料アクセスドメイン」サービスを終了したサイト。

メールサーバーを実現するソフトとセットアップの流れ

メールサーバーを実現するソフトにはさまざまな種類があるが、ここでは使いやすく国産のソフトでもある「Radish」の使い方を紹介しよう。なお、「Radish」による自宅メールサーバーの構築は、以下のようなステップで行う。これまでのサーバーアプリケーションと比べて大きく異なるのは、あらかじめ「ダイナミックDNSの確立」が必要になることだ。

▼「自宅メールサーバー」の設定ステップ

ダイナミックDNSの確立（8～10章）
↓
Radishのインストールと起動
↓
Radishの設定
↓
ユーザーの作成
↓
ルーターのポートマッピング

また、クライアント側（メールソフト）の設定では、**「ローカルレベル」と「WANレベル（リモートアクセス）」で異なる設定を用意する必要がある。**

さらに、リモートコントロールであればリモートコントロール、FTPであればダウンロード&アップロードが済めば設定を破棄できる（使い切りできる）のに対し、メールソフトの場合は送受信したメールデータを同期しておく必要がある。そのため、たとえばノートパソコンを使って外出先と自宅内の両方でメールを送受信したいときは、使用環境に合わせて、いちいちアカウントの設定を書き換えて使わなければならない。

▼メールソフトの設定

メールソフトの選定（本書はOutlook Expressで説明）
↓
アカウント設定（「ローカルレベル」と「WANレベル」で設定が異なる）
↓
メールの送受信

サーバー

Radishのセットアップ

Radishのセットアップを順を追って解説しよう。
まず、「Radish3」の「実行ファイル」を以下のサイトでダウンロードしよう。

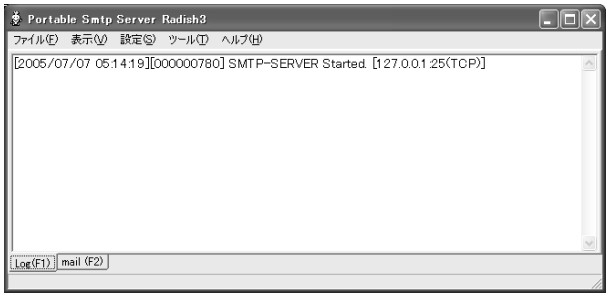
● Radish3
http://homepage2.nifty.com/spw/

※ダウンロードしたファイルを解凍するには、「Lhaplus」「Lhaca」などのLZH形式に対応したアーカイブソフトが必要。

●Radishの起動とファイアウォールの設定

ダウンロードしたファイルを任意の名前を付けたフォルダに解凍する。次に「Radish.exe」という実行ファイルをダブルクリックすると「Radish」が起動する。通知領域に「Radish」アイコンが表示されるので、これをダブルクリックすればメインウィンドウが表示される。

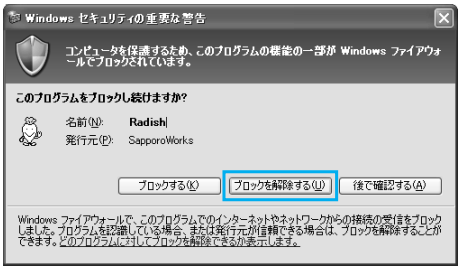
▼Radishの画面

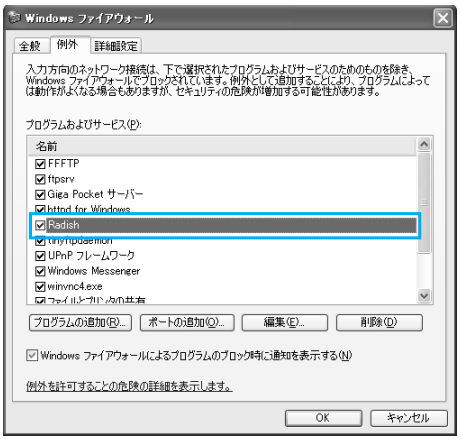


「Radish」を最初に起動したときの画面。なお、この時点では通信が確立されていないので、Windowsファイアウォールの問い合わせは表示されない。

なお、Radishでは各種設定後に再起動を行わなければならないが、この再起動の際、ファイアウォールのセキュリティ警告が表示される（Windows XP SP2のWindowsファイアウォールの場合）。ここで「ブロックを解除する」ボタンをクリックして通信許可を行えば、以後は警告画面が表示されなくなる。通信許可したあと、Windowsファイアウォールできちんと設定されているかを確認するとよいだろう。

▼Radishを通信許可





ネットワーク設定後にRadishを再起動するとファイアウォールの警告が表示されるので、「ブロックを解除する」ボタンをクリックする。

コントロールパネルからWindowsファイアウォールを開いて、設定が追加されていることを確認しよう。

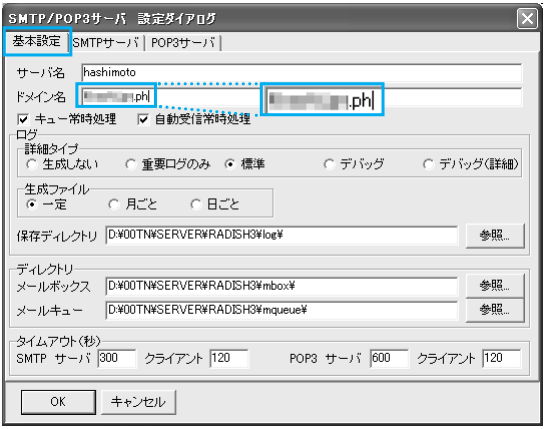
●Radishの設定

メインウィンドウのメニューバーから「設定」－「SMTP/POP3サーバー」を選択すると「SMTP/POP3サーバー設定ダイアログ」が表示されるので、各タブをクリックして設定を行う。以下の各種設定が終了したあと、「Radish」を終了して再起動すると、設定が有効になる。

●「基本設定」タブ

「サーバー名」にはメールサーバーの名前（任意の文字列）、「ドメイン名」には「アクセスドメイン」（P.147参照）を入力する。

▼Radishの基本設定



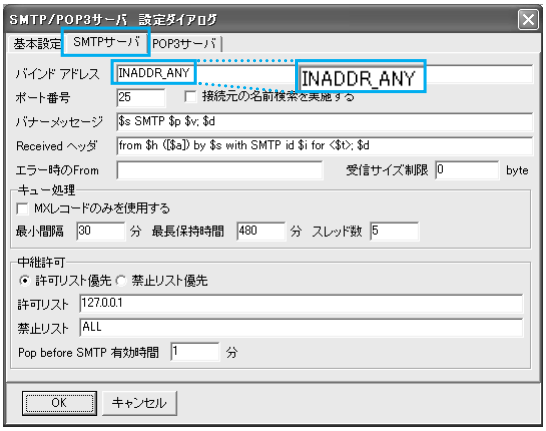
「基本設定」タブでは、「ドメイン名」にダイナミックDNSサービスで取得した「アクセスドメイン」を入力する。

●「SMTPサーバー」タブ

「バインドアドレス」に、公開サーバー用の設定「INADDR_ANY」と入力する。また、**「Pop before SMTP」には、POP認証後に何分SMTPの中継をするかを入力する。**基本的には1～5分程度の時間を設定するが、初めのうちは多めに設定しておいたほうがよいだろう。

ポート番号やその他の設定は、基本的にデフォルトのままでよい。

▼RadishのSMTPサーバー



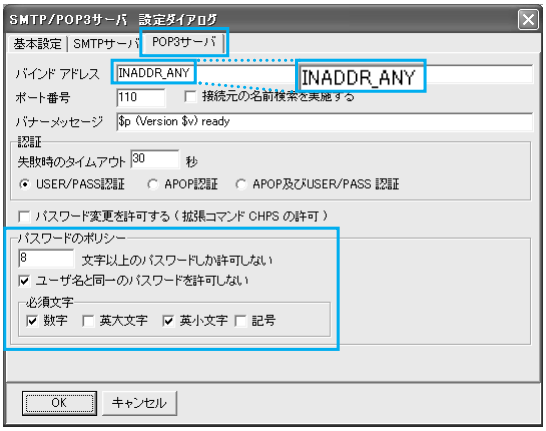
「SMTPサーバ」タブでは、「バインドアドレス」に「INADDR_ANY」と入力。「Pop before SMTP」の設定はデフォルトより長めに設定してもよい。

- **「POP3サーバー」タブ**

「バインドアドレス」には「SMTPサーバー」と同様に「INADDR_ANY」を入力する。

「パスワードポリシー」欄はユーザーパスワードに利用できる文字を制限する設定だ。パスワードに必ず「記号」や「英大文字」を入れるのはかなり面倒なので、制限を外してしまってもよいだろう。

▼RadishのPOP3サーバー設定



「POP3サーバ」タブでは、「バインドアドレス」に「INADDR_ANY」を入力。「パスワードポリシー」でパスワードとして使える文字を制限できるが、あまりきつくする必要はないだろう。

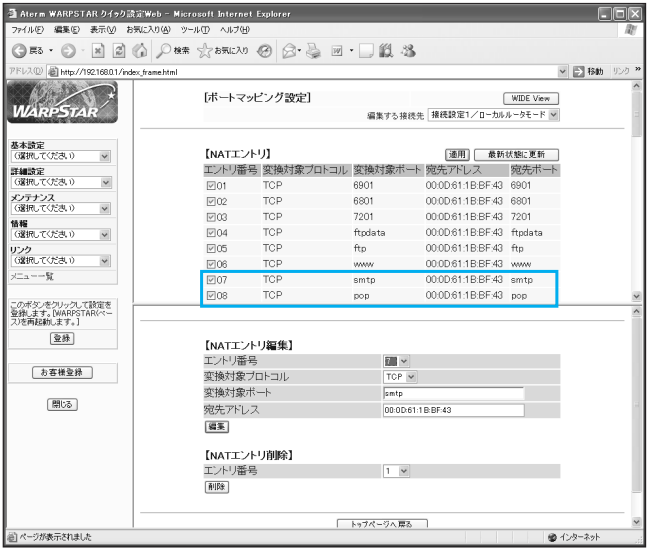
●ルーターのポートマッピング設定

続いて、ルーターのポートマッピング設定を行う。

メールサーバーの場合、**SMTPサーバーは25番、POPサーバーは110番**を利用するのが標準であり、「Radish」のデフォルト設定もそれに従ったものになっている。よって、ルーターのポートマッピング設定でも25番と110番をマッピングする。ポートマッピング設定の詳細は10章を参照してほしい。

なお、ポートマッピングの際、ルーターによっては25番を「smtp」、110番を「pop」という形に表記を置き換えるものもある。

▼ルーターのポートマッピング設定



ルーターのポートマッピング設定。ルーターによっては25番を「smtp」、110番を「pop」と表記を置き換える（画面は「AtermWR7600H」）。

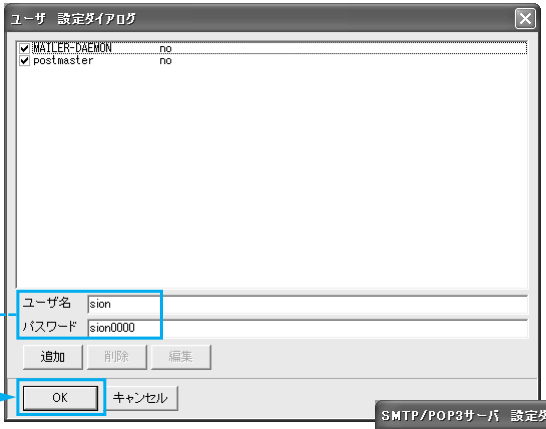
サーバー

メールアカウントの作成

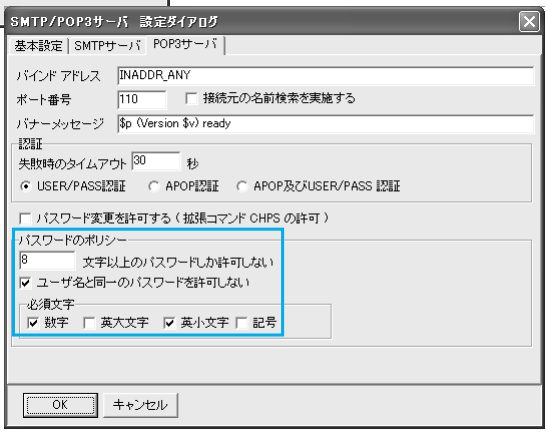
メールアカウントの作成は、メインウィンドウのメニューバーから「設定」－「ユーザー」を選択し、「ユーザー設定ダイアログ」ダイアログで行う。「ユーザー名」にはメールアドレスに使いたい好きな名前を入力し、「パスワード」には任意の文字列を入力する。ただし、パスワードの文字は「SMTP/POP3サーバー設定ダイアログ」ダイアログの「POP3サーバー」タブで設定する「パスワードポリシー」に沿ったものでなければならない。

この設定を行うと、**「[ユーザー名]@[アクセスドメイン]」**というメールアドレスを作成したことになる。

▼メールアカウントの作成



「ユーザ設定ダイアログ」ではメールアカウントの作成を行うことができる。



パスワードは「SMTP/POP3サーバー設定ダイアログ」の「POP3サーバー」タブで設定できる「パスワードポリシー」に沿ったものしか設定できない。

クライアント

クライアントのメール設定

ここでは、クライアント側の設定として、Windows XPの標準メールソフトであるOutlook Expressの設定方法を説明しよう。

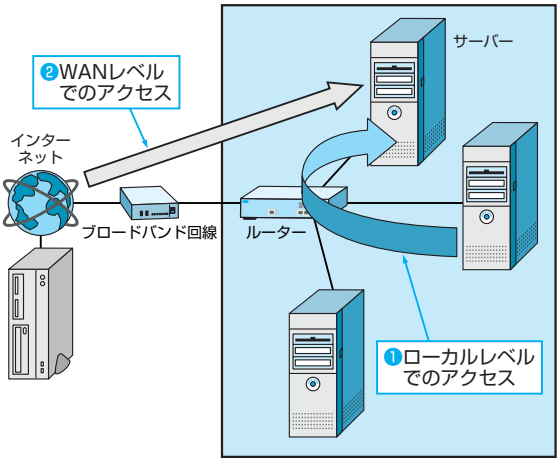
Outlook Expressメニューバーから「ツール」－「アカウント」を選択し、「インターネットアカウント」ダイアログが表示されたら「追加ボタン」をクリック。ショートカットメニューから「メール」を選択する。「インターネット接続ウィザード」が表示されるので、指示に従って必要事項を入力する。

なお、**前述したように「ダイナミックDNSはローカルエリア内からのアクセスを許可しない」という事実があるため、クライアント側のメールアカウントの設定は、ローカルエリア内からの接続とWAN経由の接続でそれぞれ異なる設定が必要になる。**

▼クライアントのメール設定

おなじみのウィザードによるメールアカウントの設定。しかし、自宅サーバーの場合はローカルエリアとWANで設定を変えなければならない。

▼ネットワークゾーンごとの設定の違い

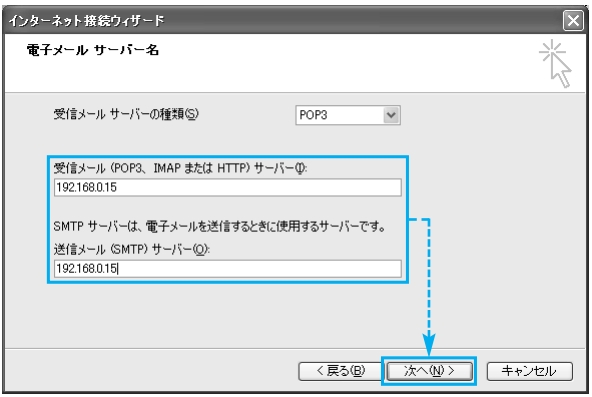


❶ゾーンでは受信メールサーバー（POP3サーバー）と送信メールサーバー（SMTPサーバー）に「サーバーのプライベートIPアドレス」を指定し、❷ゾーンでは「アクセスドメイン」を指定する必要がある。

●ローカルエリア内のパソコンにおけるメール設定（図の❶ゾーン）

「インターネット接続ウィザード」で「電子メールサーバー名」が表示されたら、受信メールサーバー、送信メールサーバーの各欄にRadishをセットアップしたパソコンの「プライベートIPアドレス」を指定する。

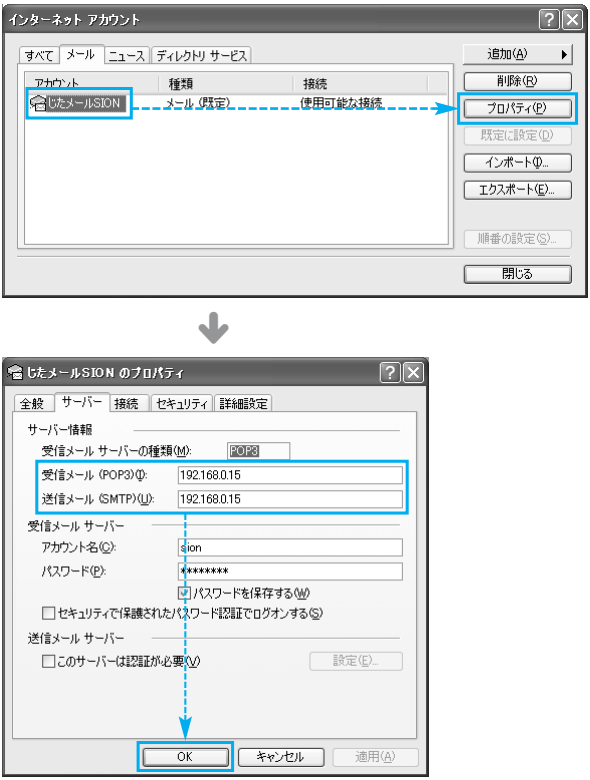
▼ローカルエリア内のパソコンでのメール設定



ローカルエリア内のパソコンでのメール設定。各サーバーに「プライベートIPアドレス」を指定する。

一度作成したアカウントの設定を変更する場合は、「ツール」－「アカウント」を選択して表示される「インターネットアカウント」ダイアログの「メール」タブをクリックし、任意アカウントを選択して「プロパティ」ボタンをクリックする。「サーバー」タブをクリックして、受信メール、送信メールのそれぞれの項目に「サーバーのプライベートIPアドレス」を指定して「OK」ボタンをクリックする。

▼既存のアカウントを変更

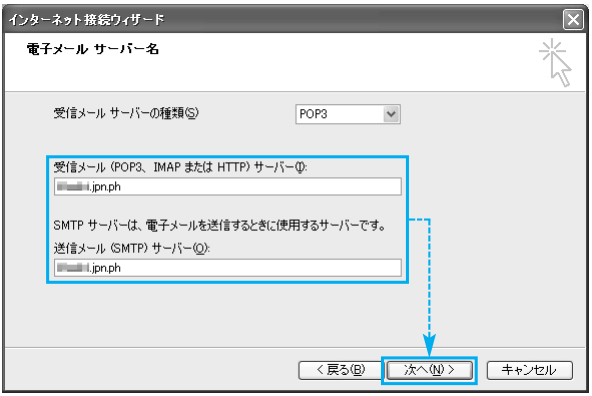


既存のアカウントを変更する場合は、「プロパティ」ボタンをクリックして、「サーバー」タブ内の受信メール、送信メールのそれぞれの項目を「サーバーのプライベートIPアドレス」に改変する。

●WANアクセスするパソコンのメール設定（図の❷ゾーン）

「インターネット接続ウィザード」で「電子メールサーバー名」の設定が表示されたら、受信メールサーバー、送信メールサーバーとしてダイナミックDNSの「アクセスドメイン」を指定する。

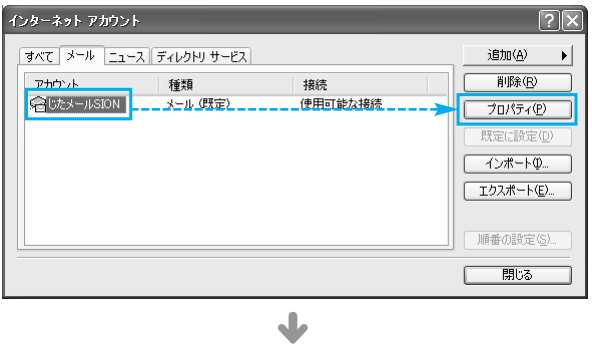
▼WAN経由でアクセスするパソコンでのメール設定



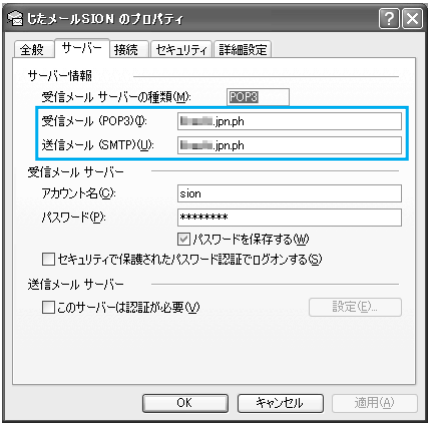
WAN経由でアクセスするパソコンでのメール設定。通常のプロバイダメールと同様に、メールアドレスから“@”より前の文字列を抜いた「ドメイン名」を入力すればよい。

一度作成したアカウントの設定を変更する場合は、「ツール」－「アカウント」を選択して表示される「インターネットアカウント」ダイアログの「メール」タブをクリックし、任意アカウントを選択して「プロパティ」ボタンをクリックする。「サーバー」タブをクリックして、受信メール、送信メールのそれぞれの項目を「アクセスドメイン」に改変して「OK」ボタンをクリックする。

▼既存のアカウントの変更



既存のアカウントを変更する場合は、「プロパティ」ボタンをクリックして、「サーバー」タブ内の受信メール、送信メールのそれぞれの項目を「アクセスアドレス」に改変する。



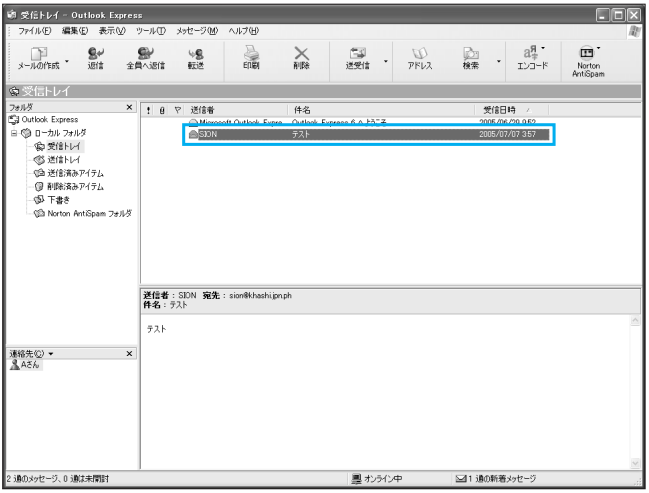
●メールの送受信の実行

Outlook Expressの設定が終了したら、作成したアドレスでメールの送受信をテストする。

まず「送受信」ボタンをクリックして、問題なくサーバーと通信できることを確認する。その後の操作は任意だが、まずは作成したメールアドレス（自分自身）にメールを送信し、受信できるかを確認するとよい。問題なく受信できたら、今度はいつも利用しているメールアカウントから作成したメールアドレスに送信し、そのメールを受信→返信できることを確認しよう。

▼メールの送受信テスト

メール設定の確認の基本は「自分宛メール」だ。このメールのやり取りが正常にできることを確認してから、別のメールアドレスとの送受信テストに移行すること。


受信トレイ - Outlook Express
ファイル(F) 編集(E) 表示(V) ツール(T) メッセージ(M) ヘルプ(H)
メールの作成
返信
全員へ返信
転送
印刷
削除
送受信
アドレス
検索
エンコード
Norton AntiSpam
受信トレイ
フォルダ
Outlook Express
ローカル フォルダ
受信トレイ
送信トレイ
送信済みアイテム
削除済みアイテム
下書き
Norton AntiSpam フォルダ
送信者
件名
受信日時
SION
テスト
2005/07/07 3:57
送信者：SION 宛先：sion@kkhashi.jpn.ph
件名：テスト
テスト
連絡先(C)
Aさん
2 通のメッセージ、0 通は未開封
オンライン中
1 通の新着メッセージ

本書で扱う主なネットワーク用語

●LAN

LANはネットワーク環境そのものを示す用語として「誤用」されることがあるが、本来の意味は「Local Area Network」で、「家庭内」や「事務所内」といった「狭い空間」におけるネットワークのことだ。ルーターによってプライベートIPアドレスが割り当てられたネットワークを示すのが一般的だ。本書では、1台のルーターにつながった「ローカルエリア」のネットワークを示す用語として利用する。

●WAN

WANは「Wide Area Network」の略で、日本語では「広域通信網」と訳される。本書では、「自宅➡会社」間や「モバイル➡自宅サーバー」間などの「インターネット通信網を介したネットワーク」を示す言葉として使用する。また、「遠隔地のパソコン➡インターネット➡自宅サーバー」という遠隔アクセスのことを「WAN接続」と呼ぶ。

●IPアドレス

インターネットでは、パソコンや回線の「住所」を「IPアドレス」で記述する。アドレスは、「＊＊＊.＊＊＊.＊＊＊.＊＊＊」という数字で表記される。一般的なブロードバンド環境では、ブロードバンド回線に「グローバルIPアドレス」が、ローカルエリア内の各パソコンに「プライベートIPアドレス」が割り当てられている。

●プライベートIPアドレス

プライベートIPアドレスとは、インターネット上に流出しない、ローカルエリア限定の「閉じた」IPアドレスのことで、「ローカルIPアドレス」とも言う。グローバルIPアドレスがインターネットでの直接通信に使われるのに対し、プライベートIPアドレスは事務所や家庭などのLAN内のパソコンを特定するために利用される。プライベートIPアドレスとして利用できるアドレスの範囲は決められていて、必ず以下のいずれかの範囲のアドレスが使用される。

▼プライベートIPアドレスに利用できるアドレス範囲

10.0.0.0～10.255.255.255
172.16.0.0～172.31.255.255
192.168.0.0～192.168.255.255

●グローバルIPアドレス

インターネット上で使われる、相手を特定するためのIPアドレス。ブロードバンド回線ごとに世界でたった1つのグローバルIPアドレスが割り振られており、インターネットにおける「住所」としての役割を果たしている。本書の11章でWAN経由のサーバー接続を実現する際は、外部から「グローバルIPアドレス」をターゲットに通信することになる。

●動的IPアドレス

一般のブロードバンド回線に割り当てられるグローバルIPアドレスは、周期的に番号が変化する。つまり、昨日までのサーバー回線のIPアドレスと、今日のサーバー回線のIPアドレスは異なることがあるのだ。このように突然番号が変化してしまうIPアドレスのことを「動的IPアドレス」と言う。

●ルーター

ルーターは、1つの回線を複数のパソコンで同時に使えるようにするための機器だ。その機能を簡単に言うと、「インターネット」と「パソコン」の仲介役のようなものだ。ルーターのWANポートには回線のグローバルIPアドレスが割り当てられ、各パソコンにプライベートIPアドレスを割り当てることによって、同時に回線を利用できるよう仲立ちをしてくれるのだ。ただし、複数のパソコンで1つの回線を共有でき、外部からの不正アクセスに強いなど「いいこと尽くめ」のルーターだが、自宅サーバーを構築する際は、複数のパソコンで共有しているために「外部から受け取った信号をどのパソコンに送信するかわからなくなる」という問題が起こる。この問題を解決するためには、ルーター自身の「ポートマッピング」設定を行う必要がある。

●ポートマッピング

ルーターで設定できる「ポート＊＊番に届いた信号はパソコン＊＊に送信する」という指示のこと。この設定により、LAN内で複数のパソコンを利用している場合でも外部からのアクセスを目的のパソコンに届けることが可能になる。なお、メーカーによって呼び名が異なり、「NATテーブル変換」や「仮想サーバー設定」などと記述される場合もある。

●ポート番号

IPアドレスに続けて補足的に付けられるアドレスをポート番号と呼ぶ。普段はあまり意識しなくてよいが、自宅サーバー構築の際には重要な要素になる。遠隔地からルーター内のサーバーにアクセスする際、住所であるグローバルIPアドレスだけではサーバーを特定できないが、IPアドレスと共に「ポート番号」を指定することにより、ターゲットとなるサーバー（およびパソコン）を特定することが可能になる。

●サーバー

「サーバー」という用語はさまざまな意味を持つが、本書では、ネットワーク通信における「アクセスされる側」、つまり「アクセス先」という意味で用いる。ソフトウェアによっては、サーバーのことを「ホスト」と称する。また、このようなサーバーを実現するソフトのこと「デーモン」とも呼ぶ。本書では、一般に「ホスト」と称されるものも基本的に「サーバー」という言葉で説明する。

●クライアント

サーバーやホストに「アクセスする」側のソフトやパソコンのこと。リモートコントロールの場合であればコントロールを行う側、FTPの場合はFTPサーバーを利用する側のこと。

●ダイナミックDNS

一般的なブロードバンド回線は動的IPアドレスであるが、サーバー側のアドレスが動的IPアドレスではクライアント側で固定したアドレスを利用できないため、非常に使いづらい。この動的IPアドレスを「固定文字列（ドメイン名）」に置き換え、動的IPアドレスの状態を更新することで、固有のドメイン名でアクセスできるようにするしくみのことを「ダイナミックDNS」と言う。また、このシステムを提供する団体を「ダイナミックDNSサービス」と呼ぶ。

●アクセスアドレス

本書では、サーバーにアクセスする際に利用するグローバルIPアドレス、あるいはドメイン名のことを指す。

索引

英数字

ア行

カ行

サ行

タ行

ナ行

ハ行

マ行

ヤ行

ラ行

●著者略歴
橋本情報戦略企画　橋本和則
1971年生まれ、34歳。『橋本情報戦略企画（Hashimoto IT Strategy）』（http://seifer-almasy.cool.ne.jp/hits/）を主宰。書籍執筆のほか企画業務、企業コンサル、プレゼンプランニング＆コンサル、人材教育など多彩に展開。著書には「上級マニュアル」シリーズ、「甦れ!ベタついたWindows XP」「P2Pファイルの達人」（技術評論社）のほか、「Windows XP 再インストール完全バイブル」（日経BPソフトプレス）「PowerPointマル勝プレゼンテーション術」（翔泳社）、月刊「Windows Server World」連載記事（IDG）などがある。

●カバー　花本　浩一
●カバーイラスト　日野　譲
●本文レイアウト　チーム・エムツー
●本文デザイン・イラスト　チーム・エムツー
●担当　青木　宏治

Windows XPで作るスマート自宅サーバー

平成17年12月25日　初版　第1刷発行

著　者　橋本　和則
発行者　片岡　巖
発行所　株式会社技術評論社
東京都品川区上大崎3-1-1
電話 03-5745-7800 販売促進部
03-5745-7830 書籍編集部
印刷／製本　株式会社加藤文明社

定価はカバーに表示してあります。

ISBN4-7741-2603-9　C3055
Printed in Japan