

アマチュア無線のためのサーバー構築

2004年8月17日

SuperControlJapan

J11FGX

上野浩一

東京都青梅市河辺町10-2-1-213

<http://www.supercontrol.de/>

<http://www3.ocn.ne.jp/~pcc/>

Copyright©2004

西東京パソコンクリニック

<p>このドキュメントへの実費200円の御協力をお願いします みずほ銀行 青梅市河辺町支店 1618430 ウエノコウイチ</p>

サーバーをインターネットに公開すること

それは全世界に対して自分で情報の管理が出来ると宣言することです

インターネット上の多くのサービス(サーバー)はその歴史上UNIXというOSで構築されてきました。現在はLinuxやFreeBSD等といったOSでインターネットが構成されていると言っても過言ではないでしょう。

インターネット上のサービス
TELNET、SSH
FTPサーバー
Sendmail(メール配信)
WEB(HTTPD)サーバー

アマチュア無線の世界にもインターネットを使ったさまざまなプログラムが登場してきました。特徴はその多くがWindowsの上で動くものであり、UNIXサーバーで培われてきたセキュリティーとは異なるノウハウが必要となります。

アマチュア無線のためのプログラム
eQSO
EchoLink
STANDARD WIRES-II
KENWOOD TS-480 ARCP-480
SuperControl

この説明書はこれらのプログラムをユーザーとして使うのではなく、サーバーとして動かすために必要な事柄をまとめています。

サーバーに使うマシンとOSを選ぶ

インターネット上のサーバーはUNIXというOSが定番です。しかし、私たちが使うサーバープログラムの多くがWindowsの上で動くことから選べるOSの選択肢は少なくなってきます。

一番のお勧めはWindows2000です。24時間稼働するサーバーとしてはこれしが最適です。次にWindowsXPとなりますが、その信頼性はWindows2000から比べると落ちます。これはWindowsXPが劣っているということではなく、設計上の違いからくるものです。

WindowsME,Windows9xに至っては、サーバー管理者としては次章で述べるセキュリティーの観点からも選択すべきではありません。もし信頼性の高いサーバーを構築したいのであればWindows2000かWindows2003を選ぶべきです。

マシンは、省エネ省スペースの観点からノートパソコンがお勧めです。バッテリーが内蔵されているので停電によって起こるトラブルに対しても好都合です。ノートパソコンがない場合はデスクトップパソコンでもOKですが、発熱や騒音、電気代の問題をクリアさせる必要があります。

管理者の責任・セキュリティ

サーバーとして動かすからにはセキュリティを最高レベルに高めておかなければなりません。セキュリティホールを抱えたまま運用すると、外部からの攻撃を受けるばかりか、第三者への攻撃の足場にされて貴方が加害者になることもあります。

1. もし、貴方が使おうとしているサーバーマシンのOSが今まで無防備な状態で稼動していた、またはメール受信やブラウジングを沢山行っていたマシンであるならば、まずOSの入れ替え（リカバリー）から行ってください。
2. 安全が確保できたOSが用意できたら、そのマシンをルーターの後ろにつないでください。けて ADSL モデムや CATV などのグローバルアドレスのネットワークには繋がらないこと。その瞬間に貴方のサーバーは外部からの攻撃を受けることになります
3. 次に WindowsUpdate を最後まで行ってください
4. ウイルスチェックプログラムを導入します
ウイルスチェックプログラムを導入するときにはインターネットセキュリティや FireWall、PCGATEWAY と名前がつくものは選択しないでください。のちのちトラブルの元になります。あくまでもウイルスチェックプログラムのみを選択し、FireWall に関しては別の専用マシンを用意します。今、市販されているインターネットセキュリティ系のプログラム多くは貴方のマシンを完全に守るには中途半端であり、操作が難しすぎます。
5. ウイルスチェックプログラムは感染してからインストールしても正常に動かない事を肝に銘じてください。またウイルスチェックプログラムの更新手続きは忘れない。
6. 貴方が提供しようとするサービス以外のプログラムは入れない、動かさない
インターネットインフォメーションサービス(IIS)に統合されている TELNET,FTP,HTTP と言ったサービスはすべて停止させます。もちろん今まで使っていたメールプログラムやブラウザも例外ではありません。貴方がサービスを提供しようとしているマシンで OutlookExpress でメールの送受信や InternetExplorer でネットサーフィンなどは言語道断です。ファイルのダウンロードが必要であれば他のマシンでダウンロード後にウイルスチェックを行った後に CD やメモリースティックなどでファイルを移動する慎重さが必要です。

ネットワーク接続のための ADSL モデム

現在使用している ADSL モデムが以下のものをならばルータを内蔵していないタイプです。
これらのモデムをお使いの方はルーターの設置へ読み進めてください



以下のタイプのモデムはルーターを内蔵しています。
パネルに PPP というランプがあることで判ります。

NTT ADSL モデム NV	NTT ADSL モデム NV-2(実売 16590 円)
	
アッカで使用されている NT-ME MN7300	住友電工 MegaBit Gear
	

これらのモデムはルーターとしてもモデム（ブリッジ）としても利用できます。
次章では NV-2 をルーターとして設定するときの方法について解説します

NV-2 をルーターとして設定する

フレッツ ADSL を使用し、IP 電話（VoIP）を利用する時はこの設定を行います
もし IP 電話を使用せず別途ルーターを設置できるのであれば、**ルーターの設置**へ読み進めてください

【設定ウィザード】

設定ウィザードでは、接続に必要な最低限の設定を行います。

ADSLモデム内蔵ルーターとして利用する場合

接続先の設定として、プロバイダから提供された情報を入力してください。

- 例) ・複数のパソコンからインターネットを利用する場合
- ・IP 電話サービスを利用する場合

ADSLモデムとして利用する場合

フレッツ接続ツールやブロードバンドルーターで接続先の設定を行ってください。

- 例) ・パソコンでフレッツ接続ツール等を利用する場合
- ・ブロードバンドルーターを接続して利用する場合

【利用タイプの選択】

利用タイプ	<input checked="" type="radio"/> ADSLモデム内蔵ルーター
	<input type="radio"/> ADSLモデム


【接続先の設定】

接続先名	接続設定1
接続先ユーザー名	xxxxxx@ipcon.ocn.ne.jp
接続パスワード	*****

※[接続先ユーザー名]の例: xxxxx@xxxxx.ne.jp

利用タイプで **ADSL モデム内蔵ルーター** を選び、接続先の設定にプロバイダーからの接続 ID とパスワードを入力します。モデムを再起動すると ADSL ランプと PPP ランプが点灯し通信が開始されます

サーバーは 192.168.1.11 固定 IP、使用するサーバープログラムは SuperControl とします



詳細設定の中の静的 IP マスカレード設定を選択します
このなかにインターネットに提供したいサービスを登録していきます

基本設定
(選択してください)

電話設定
(選択してください)

詳細設定
(選択してください)

- (選択してください)
- LAN側設定
- DHCP手動設定
- パケットフィルタ設定
- 静的IPマスカレード設定**
- 静的NAT設定
- 静的ルーティング設定
- 高度な設定

このボタンをクリックして設定を登録します。[本商品を再起動します。]

登録

3000 SuperControl の制御ポート (任意に設定できます)

11500 SuperControl で利用する VoIP ポート (固定)

その他のポート

5900 サーバー監視用 VNC ポート

1503 T.120 (TCP)

1720 H.323 コール セットアップ (TCP)

NetMeeting、KENWOOD ARCP-480 を使用するには
ポート 522、389、1503、1720、1731 の全ての設定が必要

500、10024 eQSO で使用

50000 KENWOOD ARCP-480/ARHP-10 で使用

[静的IPマスカレード設定]

WIDE View

編集する接続先 接続設定1 / UPnP 優先

[NATエントリ]

適用
最新状態に更新

エントリ番号	変換対象プロトコル	変換対象ポート	宛先アドレス	宛先ポート
<input type="checkbox"/> 01	TCP	3000	192.168.1.11	3000
<input type="checkbox"/> 02	TCP	11500	192.168.1.11	11500
<input type="checkbox"/> 03	TCP	5900	192.168.1.11	5900
<input type="checkbox"/> 04	TCP	1503	192.168.1.11	1503
<input type="checkbox"/> 05	TCP	1720	192.168.1.11	1720
<input type="checkbox"/> 06				

ルーターの設置

ADSL モデムでは内蔵ルーターを OFF にします

* ADSL 内蔵の VoIP 機能が使えなくなりますので御注意ください

【設定ウィザード】

設定ウィザードでは、接続に必要な最低限の設定を行います。

ADSLモデム内蔵ルータとして利用する場合

接続先の設定として、プロバイダから提供された情報を入力してください。

- 例) ・複数のパソコンからインターネットを利用する場合
- ・IP電話サービスを利用する場合

ADSLモデムとして利用する場合

フレッツ接続ツールやブロードバンドルータで接続先の設定を行ってください。

- 例) ・パソコンでフレッツ接続ツール等を利用する場合
- ・ブロードバンドルータを接続して利用する場合

【利用タイプの選択】

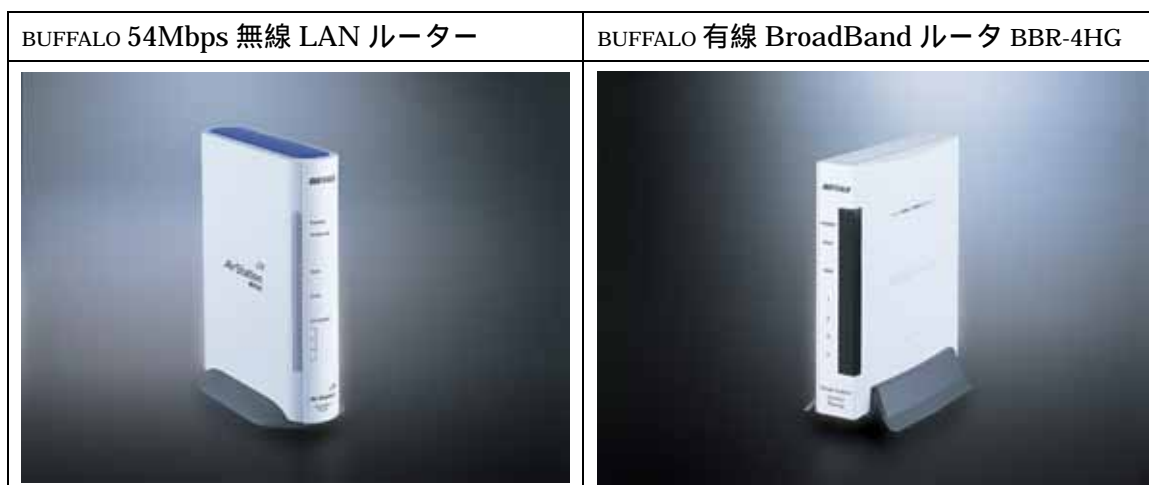
利用タイプ	<input type="radio"/> ADSLモデム内蔵ルータ
	<input checked="" type="radio"/> ADSLモデム

【接続先の設定】

接続先名	接続設定1
接続先ユーザー名	
接続パスワード	

※ [接続先ユーザー名]の例: xxxxx@xxxxx.ne.jp

ルーターには無線 LAN 内臓タイプと有線のみ の 2 種類があります
 ここでは BUFFALO 社製の無線ルーターを例に設定方法を解説します



サーバーは 192.168.11.66 固定 IP、使用するサーバープログラムは SuperControl とします
 基本的に ADSL モデム内臓ルーターに設定する内容と同じです。

ADSL モデム内臓ルーターで 1503、1720 ポートを設定しても音声を通らないときには ADSL モデムのルーター機能は OFF にしてこのルーターで設定で試してみてください。

Wireless LAN Access Point

Air Station

WHR2-G54

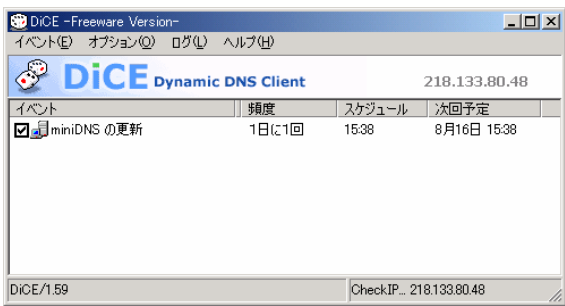

<ul style="list-style-type: none"> ▲TOPへ戻る ▶LAN設定 ▶WAN設定 ▼ネットワーク設定 <ul style="list-style-type: none"> 登録情報 アドレス変換 パケットフィルタ アタックブロック UPnP ▶管理 	<table border="1"> <thead> <tr> <th>グループ</th> <th>WAN側IPアドレス</th> <th>プロトコル</th> <th>LAN側IPアドレス</th> <th>LAN側ポート</th> </tr> </thead> <tbody> <tr> <td>VNC</td> <td>エアステーションのWAN側IPアドレス</td> <td>TCPポート:5900 <--></td> <td>192.168.11.66</td> <td>TCPポート:5900</td> </tr> <tr> <td rowspan="2">NetMeeting</td> <td>エアステーションのWAN側IPアドレス</td> <td>TCPポート:1503 <--></td> <td>192.168.11.66</td> <td>TCPポート:1503</td> </tr> <tr> <td>エアステーションのWAN側IPアドレス</td> <td>TCPポート:1720 <--></td> <td>192.168.11.66</td> <td>TCPポート:1720</td> </tr> <tr> <td rowspan="2">SuperControl</td> <td>エアステーションのWAN側IPアドレス</td> <td>TCPポート:3000 <--></td> <td>192.168.11.66</td> <td>TCPポート:3000</td> </tr> <tr> <td>エアステーションのWAN側IPアドレス</td> <td>TCPポート:11500 <--></td> <td>192.168.11.66</td> <td>TCPポート:11500</td> </tr> </tbody> </table>	グループ	WAN側IPアドレス	プロトコル	LAN側IPアドレス	LAN側ポート	VNC	エアステーションのWAN側IPアドレス	TCPポート:5900 <-->	192.168.11.66	TCPポート:5900	NetMeeting	エアステーションのWAN側IPアドレス	TCPポート:1503 <-->	192.168.11.66	TCPポート:1503	エアステーションのWAN側IPアドレス	TCPポート:1720 <-->	192.168.11.66	TCPポート:1720	SuperControl	エアステーションのWAN側IPアドレス	TCPポート:3000 <-->	192.168.11.66	TCPポート:3000	エアステーションのWAN側IPアドレス	TCPポート:11500 <-->	192.168.11.66	TCPポート:11500
グループ	WAN側IPアドレス	プロトコル	LAN側IPアドレス	LAN側ポート																									
VNC	エアステーションのWAN側IPアドレス	TCPポート:5900 <-->	192.168.11.66	TCPポート:5900																									
NetMeeting	エアステーションのWAN側IPアドレス	TCPポート:1503 <-->	192.168.11.66	TCPポート:1503																									
	エアステーションのWAN側IPアドレス	TCPポート:1720 <-->	192.168.11.66	TCPポート:1720																									
SuperControl	エアステーションのWAN側IPアドレス	TCPポート:3000 <-->	192.168.11.66	TCPポート:3000																									
	エアステーションのWAN側IPアドレス	TCPポート:11500 <-->	192.168.11.66	TCPポート:11500																									

ダイナミック DNS

ADSLなどの安価なインターネット接続サービスを利用するとグローバルIPアドレスがプロバイダー側の都合でそのつど変化します。電子メールアドレスなどと違って一旦ルーターに割り振られたIPアドレスも、いつの間にか違うアドレスになっていることもあるわけです。

これでは出先など外部から自分のサーバーにアクセス事が出来なくなってしまいます。しかし固定IPアドレスのサービスはまだ高価です。そこで自宅でサーバーを持ちたい人に強い見方なのがダイナミックDNSというシステムであり、以下のプログラムDiCEがFreewareとして配布されていますので誰でも自由に使えます。詳しくは以下のURLを参考にしてください。

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

DiCE の画面	DiCE 用に 1 台 Win2000 を用意している
	

以上で簡単ですが、インターネットサーバーの構築について概略を記させていただきました。

SuperControl のインストールについては CD-ROM の中に日本語の説明書を入れてあります
そちらをごらんください。

セキュリティは受身ではなく是非積極的な対策を取ってください。

また日々新しい脅威が発見されています。

<https://service1.symantec.co.jp/sarc/index.html> Symantec Security Response

<http://www.jpcert.or.jp/announce.html> JPCERT/CC

マイクロソフト セキュリティ情報

等を購読して情報収集を怠らないようにしましょう。

西東京パソコンクリニックではパソコンサポートやサーバー構築のお手伝いをしています。

<http://www3.ocn.ne.jp/~pcc/>

このドキュメントへの実費 200 円の御協力をお願いします
みずほ銀行 青梅市河辺町支店 1618430 ウエノコウイチ

全体の構成

ADSL モデム



DiCE クライアント



SuperControl サーバー

