

無線 LAN
JRL-710 / 720 シリーズ
ユーザーズマニュアル

第 4.1 版：2007 年 12 月



日本無線株式会社

<http://www.jrc.co.jp>

はじめに



このたびは、無線 LAN アダプタ「JRL-710/720 シリーズ」をお買いあげいただきまして誠にありがとうございます。

本書では、JRL-710/720 シリーズの設定方法について説明します。





ご使用のまえに

絵表示について

本書では、製品を安全に正しくお使いいただき、お使いになる人や他の人への危害や財産への損害を未然に防止するために、色々な絵表示をしています。その表示と意味は次のようになっています。内容をよく理解してから本文をお読みください。

 警告	この表示を無視して誤った取扱いをすると、人が死亡または重傷を負う可能性が想定される内容を示しています。
 注意	この表示を無視して誤った取扱いをすると、人が傷害を負う可能性が想定される内容および物的損害の発生が想定される内容を示しています。

絵表示の例

 	記号⊘は、禁止の行為であることを告げるものです。 図の中や近傍に具体的な禁止内容(左図の場合は分解禁止)が描かれています。
 	記号❗は、行為を強制したり指示する内容を告げるものです。 図の中に具体的な指示内容(左の場合は電源プラグをコンセントから抜け)が描かれています。

商標について

記載されている会社名及び商品名は、それぞれ各社の商標及び登録商標です。

無線 LAN 製品ご使用時におけるセキュリティに関するご注意
(お客様の権利(プライバシー保護)に関する重要な事項です！)

無線 LAN では、LAN ケーブルを使用する代わりに、電波を利用してパソコン等と無線アクセスポイント間で情報をやり取りするため、電波の届く範囲であれば自由に LAN 接続が可能であるという利点があります。

その反面、電波はある範囲内であれば障害物(壁等)を越えてすべての場所に届くため、セキュリティを設定しない場合、以下のような問題が発生する可能性があります。

- 通信内容を盗み見られる
悪意ある第三者が、電波を故意に傍受し、
ID やパスワード又はクレジットカード番号等の個人情報
メールの内容
等の通信内容を盗み見られる可能性があります。
- 不正に侵入される
悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、
個人情報や機密情報を取り出す(情報漏洩)
特定の人物になりすまして通信し、不正な情報を流す(なりすまし)
傍受した通信内容を書き換えて発信する(改ざん)
パソコンウィルスなどを流しデータやシステムを破壊する(破壊)

本来、無線 LAN カードや無線アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線 LAN 製品のセキュリティを設定して製品を使用することで、その問題が発生する可能性は少なくなります。

無線 LAN は、購入直後の状態においては、セキュリティに関する設定が施されていない場合があります。

したがって、お客様がセキュリティ問題発生の可能性を少なくするためには、無線 LAN カードや無線 LAN アクセスポイントをご使用になる前に、マニュアルにしたがって無線 LAN のセキュリティを設定してください。

無線 LAN の仕様上、特殊な方法によりセキュリティ設定が破られることもあり得ますので、ご理解の上、ご使用ください。

セキュリティの設定などについて、お客様ご自分で対処できない場合には、販売店までお問い合わせください。

当社では、お客様がセキュリティを設定しないで使用した場合の問題を充分理解した上で、お客様自身の判断と責任においてセキュリティを設定し、製品を使用することをお奨めします。

本装置は GPL のソフトウェアを使用しています。お客様は、このソフトウェアのソースコードを入手・改変・再配布する権利があることをお知らせします。ソースコードの配布については、電子メールでお問い合わせください。

wlan-support@jrc.co.jp

[注 1] 配布時に発生する費用は、お客様のご負担となります。

[注 2] 本装置を使用する時に、ソースコードを入手する必要はありません。

[注 3] 配布したソースコードについて、保証・サポートはしません。

目 次

1 設定の前に.....	1
1.1 設定の必要性.....	1
1.2 ネットワークの構成と役割の確認.....	1
1.3 IP アドレスの付与	2
1.4 設定手順	2
2 設定の準備.....	3
2.1 設定機材の準備	3
2.2 ログイン	4
2.3 ユーザアカウント	5
2.4 トップ画面.....	5
2.5 ログアウト.....	6
3 簡単設定	7
3.1 想定システム.....	7
3.2 最小限の設定項目	7
3.3 AP の設定	7
3.4 ST の設定.....	10
3.5 動作の確認.....	12
4 詳細設定	14
4.1 メニュー画面の説明	14
4.2 設定画面の説明.....	15
4.3 ネットワーク設定[Network].....	16
4.4 認証設定[Authentication]	20
4.5 暗号化設定[Encryption].....	22
4.6 無線[Wireless].....	28
4.7 SNMP の設定[SNMP].....	40
4.8 VLAN の設定[VLAN]	41
4.9 IAPP 設定[IAPP]	42
4.10 Filter MAC 設定[Filter MAC]	43
4.11 サービス機能停止[Host Name].....	44
4.12 接続制御設定[Access Control]	45
4.13 フィルタパケットの設定[Filter Packet].....	47
4.14 セントレックス機能の設定[Centrex].....	47
4.15 アカウント設定[Login/Password].....	50
4.16 再起動[Restart]	50
4.17 設定復旧[Restore]	51
4.18 バージョンアップ[Version Up].....	51
4.19 初期化モード起動[Start Init]	51
4.20 設定概要表示[Setup Summary]	52

4.21 認証概要表示[Authentication Summary]	52
4.22 ログ表示[Logging]	53
5 診断機能	54
5.1 機材の準備と接続	54
5.2 ログインとログアウト	55
5.3 diag アカウントで使用できるコマンド	57
5.4 mti コマンド(AP/ST 共通)	57
5.5 scan コマンド	57
5.6 stscan コマンド	60
5.7 rssi コマンド(ST で動作している場合のみ有効)	61
5.8 wti コマンド	62
5.9 diag コマンド	62
5.10 stlist コマンド(AP で動作している場合のみ有効)	64
5.11 pclist コマンド(AP で動作している場合のみ有効)	64
5.12 eti コマンド	65
5.13 set コマンド	66
5.14 get コマンド	67
5.15 save コマンド	67
5.16 load コマンド	68
5.17 acladd コマンド	68
5.18 aclclr コマンド	68
5.19 reset コマンド	69
6 工場出荷時設定	70
7 無線 LAN 関連用語集	78
付録 1 パソコンの IP アドレスの変更	83
付録 2 パソコンの IP アドレスの確認	84
付録 3 接続の確認(PING コマンド)	85
付録 4 1 台のパソコンで、連続して無線 LAN を設定する	86
付録 5 専用シリアルケーブル配線図	87
付録 6 セキュリティの設定	88
付録 7 WEP キー設定のヒント	89
付録 8 MAC アドレスフィルタの設定	90
付録 9 AP が無線送信する条件	91
付録 10 WEB ブラウザの一時ファイル(キャッシュ)設定	92
付録 11 WEB ブラウザのプロキシ設定の変更	94
付録 12 パケットフィルタの設定手順	96
付録 13 有線 MAC アドレスと無線 MAC アドレス	98
付録 14 設定した IP アドレスを忘れてしまったら	99
付録 15 MIB	100
付録 16 無線 LAN の簡易回線設計	101

付録 17 グローバル IP アドレスとローカル IP アドレス.....	103
付録 18 14 チャンネル対応機種について.....	104
付録 19 5.2G 帯対応機種について.....	106
付録 20 4.9G 帯対応機種について.....	108
付録 21 SET/GET コマンドで利用できる設定パラメータ	110
付録 22 設定ファイルの使用方法.....	115

1 設定の前に

1.1 設定の必要性

無線 LAN は通信のための多くの機能を有しており、通信システムの要求に応じて動作条件を設定する必要があります。工場出荷時には、できるだけ設定変更をしなくても動作できるような初期値(デフォルト)を設定していますが、最小限の設定変更が必要です。また、複雑なシステム構成や高度な運用をする場合はそれに応じた設定が必要です。

本書では、とりあえず通信動作ができるまでの「3 簡単設定」と、高度システムにも対応可能な「4 詳細設定」に章立てを分けて記載していますので、状況に合わせてご利用ください。さらに、回線状態の調査や動作速度の確認のために「5 診断機能」を解説していますので、システム設計や保守にご利用ください。

1.2 ネットワークの構成と役割の確認

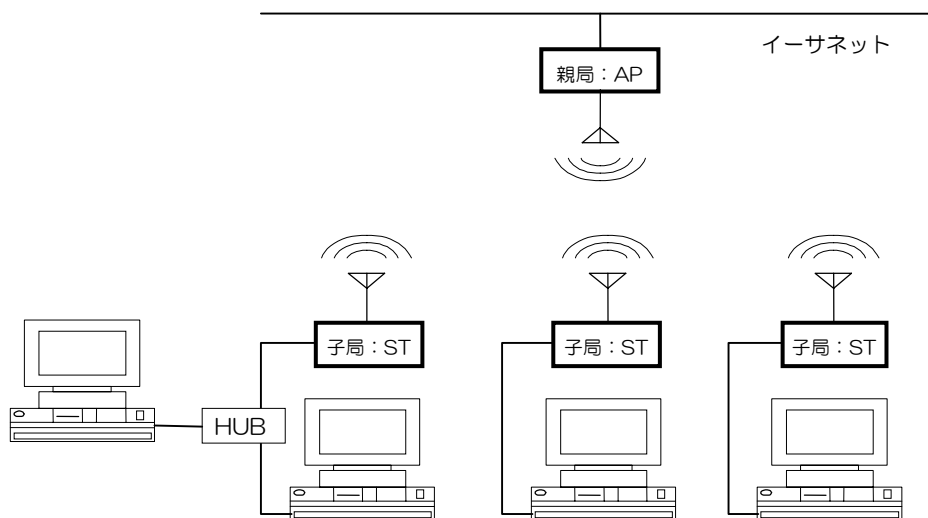
無線 LAN で構成するネットワークは、Infrastructure Network(基幹接続ネットワーク)といいます。この構成の概略図を下図に示します。

この図のネットワーク構成において、これから設定しようとする無線 LAN が「親局(AP: Access Point)」に相当するのか、「子局(ST: Station)」に相当するかを決めてください。

無線 LAN は、「AP」と「ST」の間で通信します。*

したがって、1:1 の通信(Point to Point 通信)でも、片側を「AP」、もう一方を「ST」に設定します。

※: ST どうして通信するときも AP を経由して通信します。



[備考]

- AP(複数設置可)は有線回線と無線回線を接続するアクセスポイントです。
- ST は端末や HUB と接続し、端末や HUB に接続された機器を無線接続します。
- 無線通信するのは同一の SSID が設定された AP と ST の間だけです。
- (複数の)AP 相互は無線通信しません。
- ST どうしは AP を介して無線通信します。

1.3 IP アドレスの付与

無線 LAN には、装置の設定/保守管理のために IP アドレスを付与する必要があります。

装置の工場出荷時状態(デフォルト)では、無線 LAN の IP アドレスは「192.168.1.1」に設定されています。したがって、装置を最初に設定するときは、設定用パソコンの IP アドレスを同一セグメント内の IP アドレス(192.168.1.2~254)に設定しなければなりません。また、装置を運用するときには、運用するネットワーク内の IP アドレスが重複しないよう、ユニークな IP アドレスを必ず設定してください。

使用可能な IP アドレスの値は、ネットワーク管理者やインターネット接続サービス業者にお問い合わせの上、取得してください。

無線 LAN の IP アドレスは必ずしもグローバルアドレスである必要はなく、企業などに割り当てられたローカル IP アドレスを使用できます。閉じられた(インターネットに接続されていない)ネットワークであれば、工場出荷時の IP アドレス(192.168.1.*)の*を重複しないように設定するだけでも運用可能です。

1.4 設定手順

- ① 設定用パソコン(Personal Computer)を用意し、無線 LAN と通信できるように、設定用パソコンの IP アドレスを無線 LAN の IP アドレス(同一セグメント)に合わせます。
- ② 無線 LAN にログインします。
- ③ ログイン後、AP/ST の種別、IP アドレス、周波数チャネルおよび SSID 等を設定します。
- ④ 無線 LAN を再起動します。再起動後に設定が有効になります。
- ⑤ 設定用パソコンの IP アドレスを元の設定に戻します。

注意

- 本書の中で伝送速度に関する数値を記載していますが、この数値は無線 LAN 規格の理論上の最大値であり、実際のデータ転送速度を示すものではありません。
- 設定用パソコンの OS は Windows 2000, XP のいずれか、WEB ブラウザは Internet Explorer 6.0 を推奨します。
- ネットワーク構成の説明でパソコンを例にとっていますが、イーサネットインターフェースを有する装置であればワークステーションや組込用コンピュータなど、どのような機種でも接続可能です。

2 設定の準備

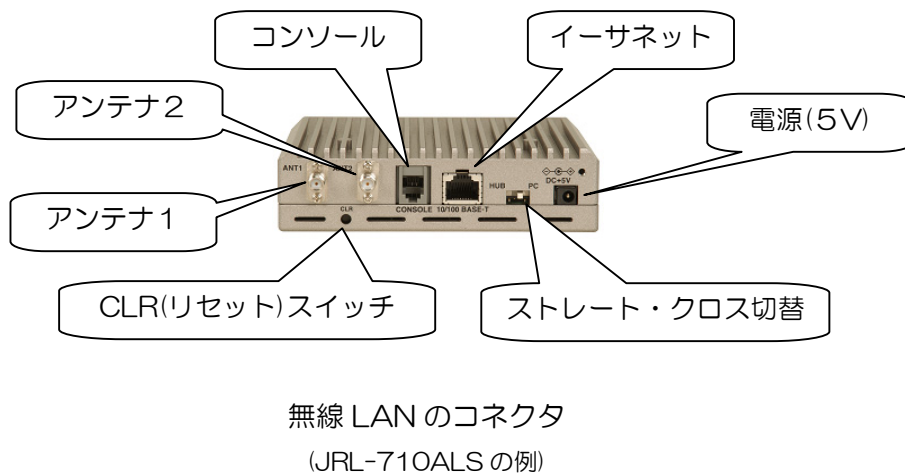
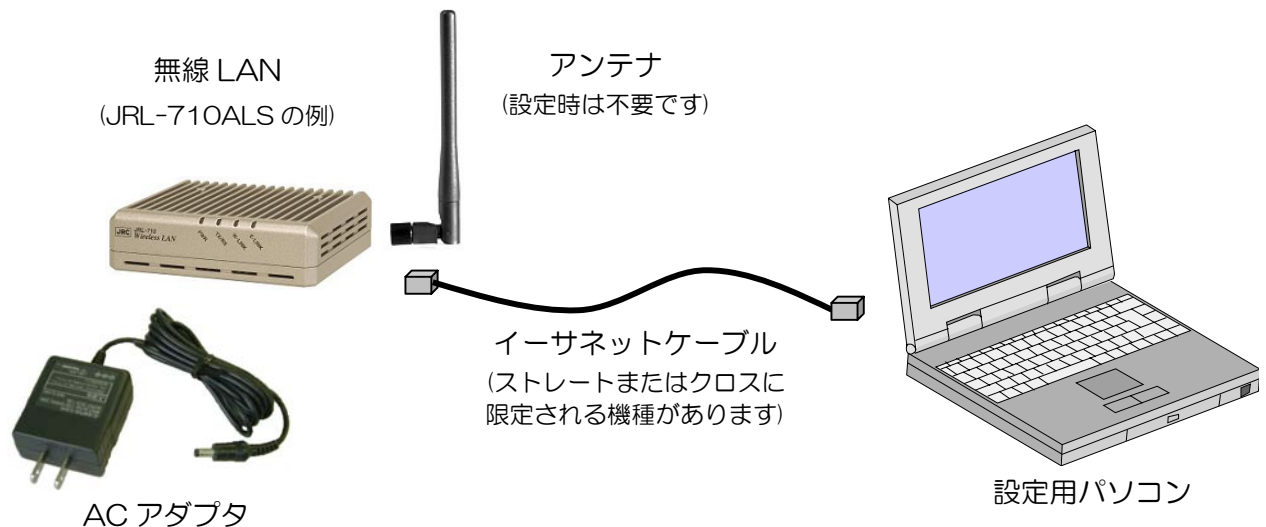
2.1 設定機材の準備

設定用パソコンと接続用イーサネットケーブルを用意します。

設定用パソコンの IP アドレスを無線 LAN の IP アドレス(同一セグメント)にあわせませす。

無線 LAN のデフォルト IP アドレスは「192.168.1.1」ですので、「192.168.1.X」に変更します。ただし「X」の値は、1 以外(2~254)の数値を入力します。たとえば、「192.168.1.101」とします。

パソコンの IP アドレス設定が完了したら、パソコンと無線 LAN とをイーサネットケーブルで接続します。パソコンと正常に接続されると「E-LINK」の LED が点灯します。



⚠ 注意

- 無線 LAN の設定を完了するまでは、無線 LAN をネットワーク(LAN)に接続しないでください。

[備考]

- パソコンの IP アドレス変更方法は「付録 1 パソコンの IP アドレスの変更」を参照ください。
- パソコンの IP アドレスは Windows コマンドプロンプトの“winipcfg”や“ipconfig”コマンドで確認できます。「付録 2 パソコンの IP アドレスの確認」を参照してください。
- 複数の無線 LAN を連続設定する場合、2 台目以降の無線 LAN にログインできないことがあります。

ます。この場合「付録 4 1 台のパソコンで、連続して無線 LAN を設定する」を参照ください。

- プロキシサーバが存在するネットワーク環境で使用しているパソコンを無線 LAN アダプタに使用するときには、「付録 11 WEB ブラウザのプロキシ設定の変更」を参照してください。
- 上記のパソコンの IP アドレスは無線 LAN を初めて設定する場合のものです。それぞれの環境に合わせた IP アドレスに読みかえてください。
- Ethernet ケーブルにはストレートタイプとクロスタイプがあります。無線 LAN の機種によって適合ケーブルが異なります。

適合ケーブル

無線 LAN 機種	パソコンと接続		HUB 経由で接続		備考
	ストレート	クロス	ストレート	クロス	
JRL-710ALS	○	○	○	○	MDI/MDI-X 手動切替
JRL-710APS	○	○	○	○	
JRL-710SU	○	—	—	○	
JRL-720E	—	○	○	—	
JRL-720E2	○	○	○	○	MDI/MDI-X 自動切替 *
JRL-710AL2	○	○	○	○	
JRL-710AP2	○	○	○	○	
JRL-710SU2	○	○	○	○	
JRL-710AF	○	○	○	○	
JRL-710749E	○	○	○	○	
JRL-710749SU	○	○	○	○	

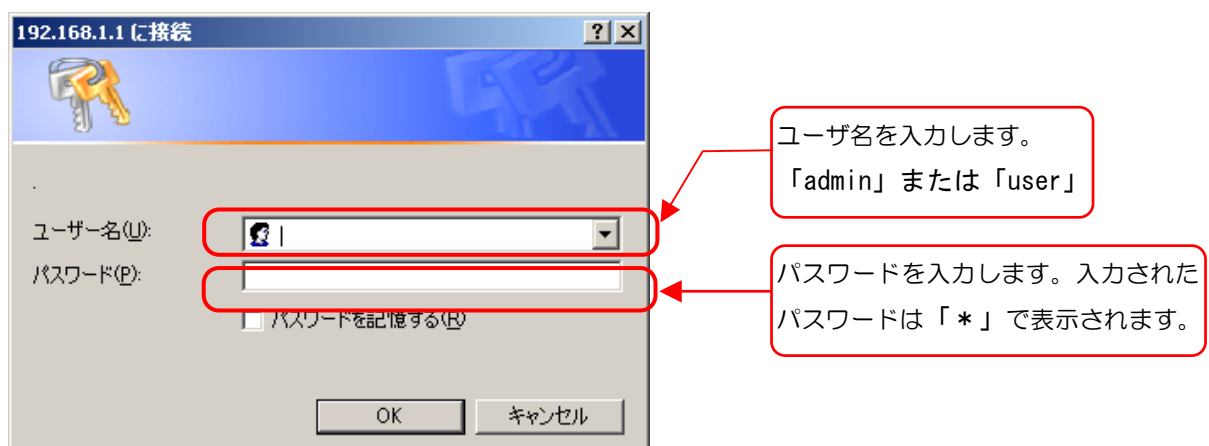
* : イーサネット速度を [Auto] に設定した場合。[Auto] 以外は MDI-X に固定。

2.2 ログイン

WEB ブラウザを立ち上げて無線 LAN にアクセスします。無線 LAN の IP アドレスが「192.168.1.1」の場合、WEB ブラウザのアドレス入力欄に「http://192.168.1.1」と入力すると、無線 LAN と接続されてログインウィンドウが開きます。

WEB ブラウザに一時ファイルが残っている場合は、2 回目以降のログイン時にログインウィンドウを表示せずに次の段階に進むことがあります。これを避けるには WEB ブラウザの一時ファイルを消去します。消去手順については「付録 10 WEB ブラウザの一時ファイル(キャッシュ)設定」を参照下さい。

ログインウィンドウ



[備考]

- WEB ブラウザは、Internet Explorer 6.0 にて動作を確認しています。他の WEB ブラウザでは表示および動作が異なる場合があります。

2.3 ユーザアカウント

無線 LAN へアクセスするために 3 種類(管理者用, 一般利用者用, 特殊操作用)のユーザアカウントが用意されており, ログイン後のコマンド実行権限に差があります。

管理者用ユーザ名は「admin」で, すべてのコマンドが実行できます。一般利用者用ユーザ名は「user」で実行可能なコマンドが制限され, 設定の参照のみ利用可能です。また, 「diag」は設置時や保守時の診断機能など特殊なコマンド操作を実行するユーザ名で, パスワードは「admin」アカウントと同一になり, 「admin」アカウントのパスワードを変更すると「diag」アカウントのパスワードも変更されます。

工場出荷時の状態では, 以下のユーザ(アカウント)名とパスワードが設定されています。

設定情報保護のため, ご購入後, 必ず最初のログイン時にパスワードを変更し, 変更した内容は忘れないようにしてください。

ユーザ名	パスワード(デフォルト)	権 限
admin	admin	設定変更・設定表示
user	user	設定変更(パスワードのみ)・設定表示
diag	admin	診断機能の実行, 詳細は「5 診断機能」参照

[備考]

- ユーザ名とパスワードは全て半角英数文字で入力してください。
- ユーザ名とパスワードは大文字と小文字を区別します。

IP アドレスやパスワードがわからなくなりログインできなくなった場合には, 本装置の「CLR」ボタンを押しながら電源を投入することで, 全ての設定をリセットする(工場出荷時の状態: デフォルトに戻す)ことができます。「CLR」ボタンは電源投入後も約 40 秒間(リセット動作が終了するまで)押し続けてください。

屋外設置用(JRL-7**SU タイプ)など一部の機種には「CLR」ボタンがありません。

⚠ 注意

- 「CLR」ボタンによるリセットは, 全ての設定がリセットされますのでご注意ください。

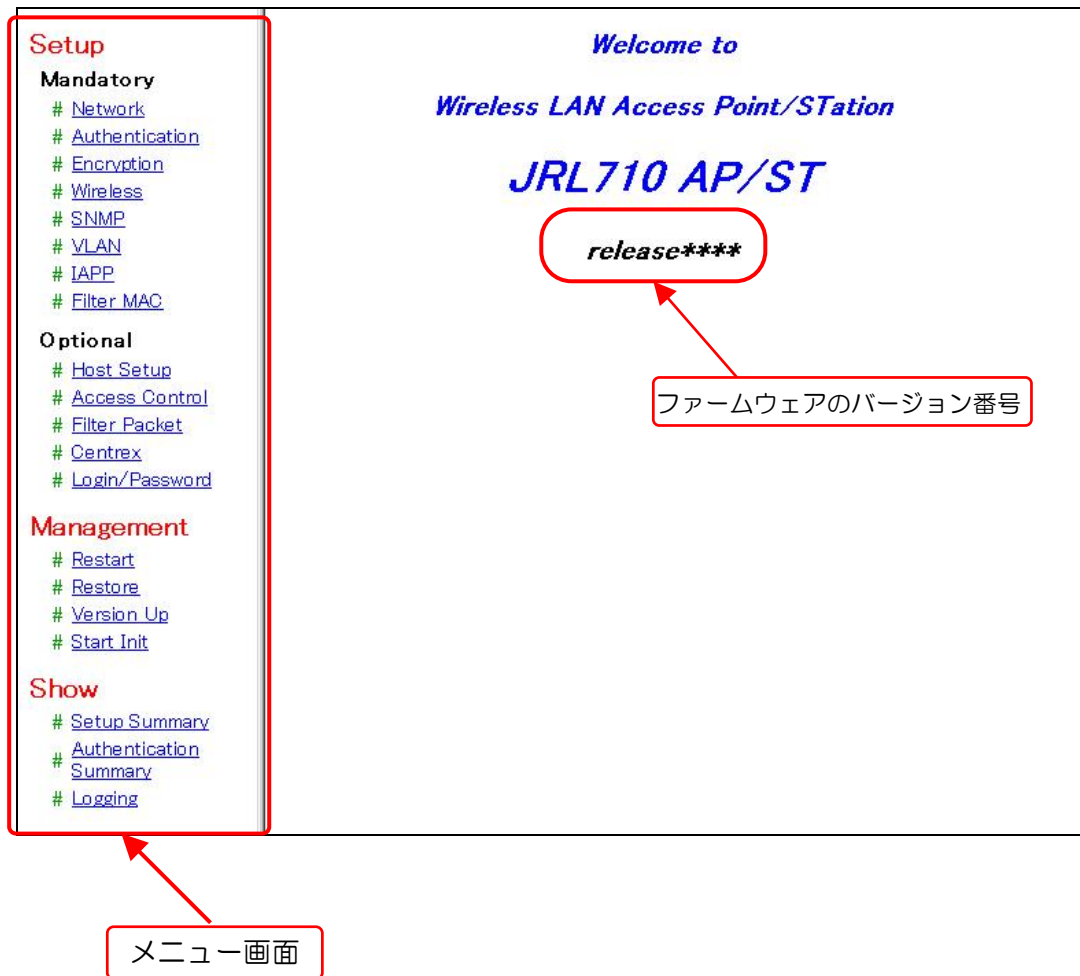
2.4 トップ画面

ログインすると, トップ画面が表示されます。

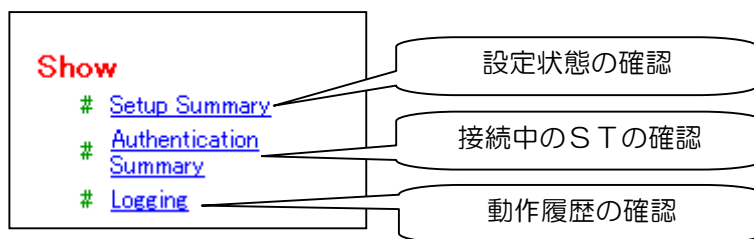
アカウント名によってメニュー画面の表示が異なります。

動作モードが AP に設定されているときと ST に設定されているときで, メニュー画面の表示が異なります。デフォルトは AP に設定されています。

トップ画面には, 無線 LAN のファームウェアバージョン番号が表示されます。



ユーザ名を”user”でログインした場合は下記のメニューだけが表示され、ここに表示されている項目だけが利用可能です。



無線 LAN の設定を変更しようとする、確認を求めるウィンドウがポップアップ表示されます。このときパソコン上でセキュリティソフトウェア等の「ポップアップブロック」機能が動作していると、確認用のウィンドウを開くことができず、設定変更ができません。
設定変更はパソコンのポップアップブロックが解除されている状態で実行してください。

2.5 ログアウト

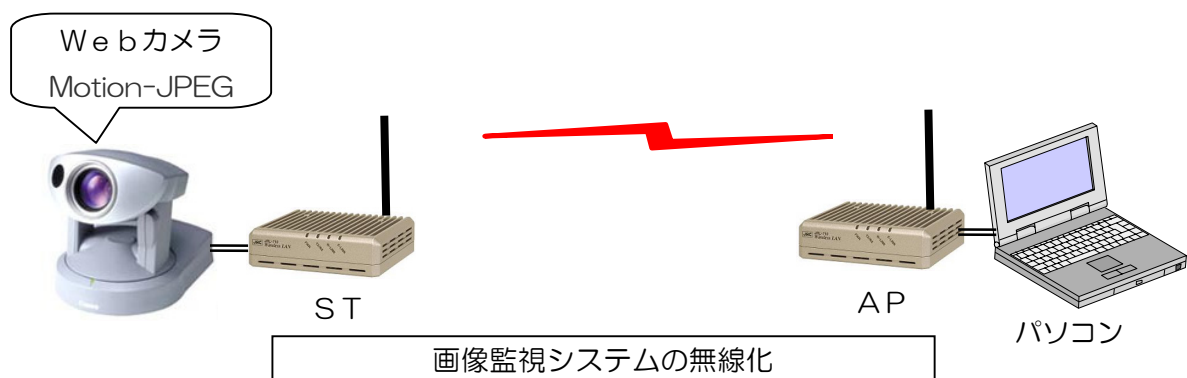
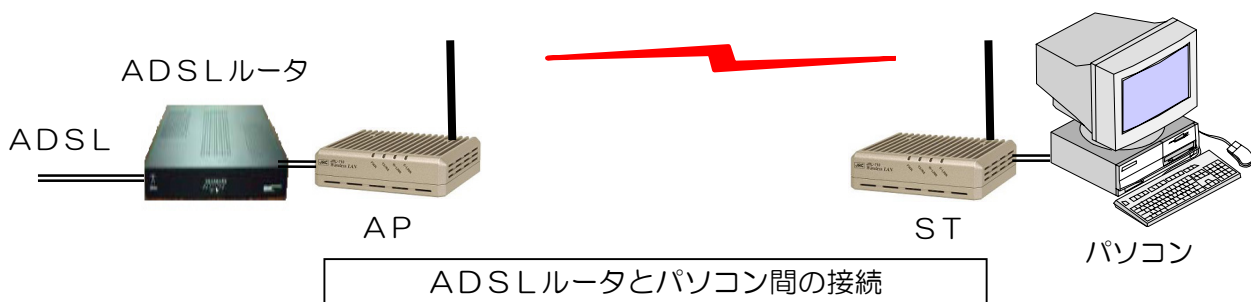
ブラウザ画面の「ファイル」→「閉じる」または  ボタンでブラウザを閉じてください。

3 簡単設定

単純な通信システムであれば無線 LAN の設定も簡単なもので済みます。つまり、工場出荷時の設定を大きく変更せずに運用することが可能です。まずは無線 LAN を動作させてみましょう。

3.1 想定システム

下図のようなシステムを想定します。いずれもイーサネットケーブルで接続したときに正常に動作しているものとしてします。



P-P回線(1:1回線)で動画をマルチキャストで伝送する場合は、送り側の無線 LAN を ST に設定した方が安定した伝送が可能です。

これは、イーサネット側から ST に入力されたマルチキャストパケットは無線回線上はユニキャストパケットとして扱うので、回線上の通信エラーが ARQ(自動再送)機能によって救われるからです。一方、AP に入力されたマルチキャストパケットは、ARQ が機能しないので、回線上の通信エラーを修復できず、画像の抜けやフリーズとなってしまいます。

3.2 最小限の設定項目

以下の項目を設定(あるいは変更)する必要があります。

- (1) AP/STの種別
- (2) IPアドレス
- (3) 暗号化

3.3 AP の設定

まず、1 台目を AP に設定します。

3.3.1 AP/ST の種別と IP アドレスの変更

デフォルトは AP 設定なので、「admin」アカウントでログインした後のメニュー画面は AP の設定メニューになっています。IP アドレスはデフォルトで「192.168.1.1」になっているので、そのまま使用します。

3.3.2 AP の WEP の設定

Setup

Mandatory

- # [Network](#)
- # [Authentication](#)
- # [Encryption](#)
- # [Wireless](#)
- # [SNMP](#)
- # [VLAN](#)
- # [IAPP](#)
- # [Filter MAC](#)

Optional

- # [Host Setup](#)
- # [Access Control](#)
- # [Filter Packet](#)
- # [Centrex](#)
- # [Login/Password](#)

Management

- # [Restart](#)
- # [Restore](#)
- # [Version Up](#)
- # [Start Init](#)

Show

- # [Setup Summary](#)
- # [Authentication Summary](#)
- # [Logging](#)

①メニュー画面の [Encryption] をクリックすると暗号化設定画面になります。

②暗号化モード選択のため、プルダウンメニューから [WEP] をクリックします。

Encryption Configuration

Encryption Mode: none, none, **WEP**, WPA-PSK, 802.11i

Apply Cancel Default

③ [WEP] が選択されると暗号キー設定画面になります。

Encryption Configuration

Encryption Mode: WEP

WEP Key

Use WEP Key No. WEP1

No.	Length	Key
WEP Key 1	128bit	0123456789abcdef0123456789ABCDEF
WEP Key 2	none	
WEP Key 3	40bit	
WEP Key 4	104bit	
	128bit	

④WEP キー1 の長さ選択のため、プルダウンメニューから [128bit] をクリックします。

⑤WEP キー1 を入力します。128bit を選択したので、半角 16 進数(0~9, a~f)で、32 文字を入力します。英字部分は大文字も使えます。

⑥ [Apply] (適用) ボタンを押すと確認画面が出てきます。後述の確定作業を行います。

3.3.3 AP 設定の確定

画面上で設定を変更しただけでは内部メモリに反映しないので、設定を確定する操作が必要です。

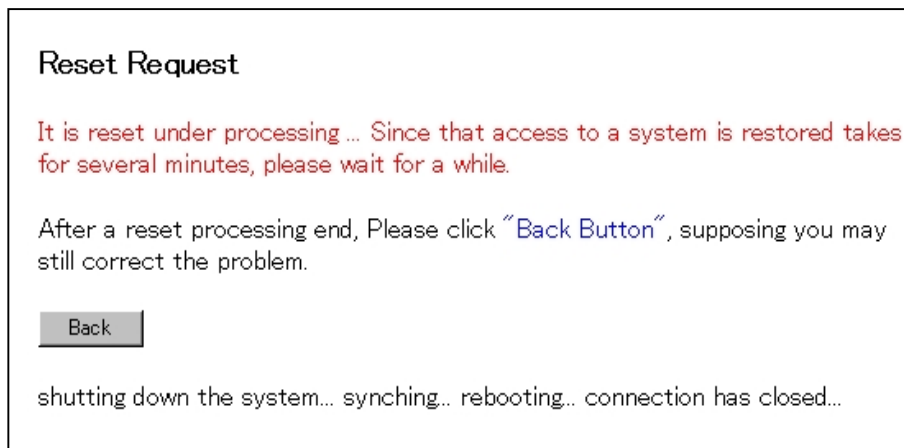
をクリックすると確認画面が出てくるので、 をクリックします。

次にリセット確認画面が出てきます。



さらに をクリックすると、無線LANはリセット動作(40秒程度かかります)に入ります。リセット後に設定が機能します。

＜リセット中の画面＞



これで AP の設定は終了です。ブラウザ画面の [ファイル] → [閉じる] または ボタンでブラウザを閉じてください。

⚠ 注意

- 同じ IP アドレスを持つ機器が同一ネットワーク内に存在するとネットワーク機能が阻害されます。ここでは単純なシステムの無線化を前提にしているので、AP の IP アドレスはデフォルトのまま使用しています。つまりデフォルトの IP アドレスを持つ他の機器が存在しないという前提で設定しています。
- もし IP アドレスが重複する場合は、ネットワーク管理者に使用できる IP アドレスを確認してください。

3.4 STの設定

2台目をSTに設定します。

3.4.1 AP/STの種別変更

「admin」アカウントでログインします。ログイン直後のメニュー画面はAPの設定メニューになっています。次の手順でSTに変更します。

Setup

Mandatory

- # [Network](#)
- # [Authentication](#)
- # [Encryption](#)
- # [Wireless](#)
- # [SNMP](#)
- # [VLAN](#)
- # [IAPP](#)
- # [Filter MAC](#)

Optional

- # [Host Setup](#)
- # [Access Control](#)
- # [Filter Packet](#)
- # [Centrex](#)
- # [Login/Password](#)

Management

- # [Restart](#)
- # [Restore](#)
- # [Version Up](#)
- # [Start Init](#)

Show

- # [Setup Summary](#)
- # [Authentication Summary](#)
- # [Logging](#)

①メニュー画面の [Wireless] をクリックすると無線設定画面になります。

②無線動作モード選択のため、プルダウンメニューから「ST」を選択します。

③ ST 設定画面に切り替わります。

④ [Apply] (適用) ボタンを押すと確認画面が出てきます。後述の確定作業を行います。

Wireless Configuration

Operating Type: AP (selected) / ST (available)

RTS Threshold: 2346 (0-2346)

Fragmentation Threshold: 2346 (256-2346)

Hard Retry: 7 (0-15)

Soft Retry: 0 (0-15)

Allow ALL Inter-Client Communication: ☒ enable ☐ disable

ACK Timeout: short

TX Power: full

Wireless Mode: 11g

AP Channel: 1 (2.412GHz)

Beacon Interval (msec): 100 (20-1000)

ERP Information Element: ☒ enable ☐ disable

Diversity Antenna: ☐ enable ☒ disable

Short Preamble: ☒ enable ☐ disable

Rate Configuration

Apply Cancel Default

Wireless Configuration

Operating Type: ST (selected)

RTS Threshold: 2346 (0-2346)

Fragmentation Threshold: 2346 (256-2346)

Hard Retry: 7 (0-15)

Soft Retry: 0 (0-15)

ACK Timeout: short

TX Power: full

Wireless Mode: 11g

Diversity Antenna: ☐ enable ☒ disable

Short Preamble: ☒ enable ☐ disable

Pseudo Mode: ☐ enable ☒ disable

Pseudo MAC: 00:00:27:3E:****

Rate Configuration

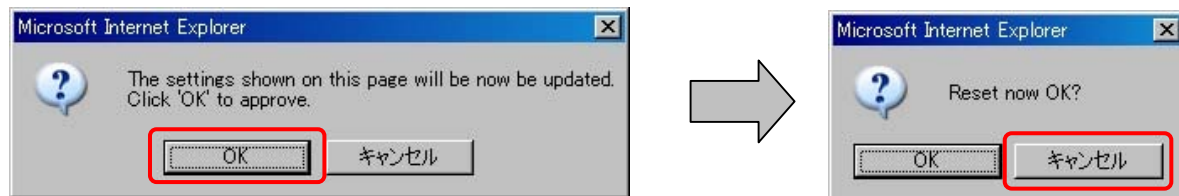
Wireless Configuration for ST

Apply Cancel Default

3.4.2 ST設定の確定

Apply をクリックすると確認画面が出てくるので、**OK** をクリックします。

次にリセット確認画面が出てきます。まだ、設定することがあるので、ここでは **キャンセル** を押して、メニューの **[Network]** をクリックします。



3.4.3 STのIPアドレスの変更

Setup

Mandatory

- # **Network**
- # Authentication
- # Encryption
- # Wireless
- # SNMP
- # VLAN
- # Filter MAC

Optional

- # Host Setup
- # Access Control
- # Filter Packet
- # Centrex
- # Login/Password

Management

- # Restart
- # Restore
- # Version Up
- # Start Init

Show

- # Setup Summary
- # Authentication Summary
- # Logging

①メニュー画面の **[Network]** をクリックするとネットワーク設定画面になります。
(このメニューはST用です)

②デフォルトの「192.168.1.1」を消し、「192.168.1.2」を入力します。

③ **[Apply]** (適用) ボタンを押すと確認画面が出てきます。
後述の確定作業を行います。

リリース O4**以前のファームウェアをお使いの場合、IP アドレスを変更後 **[Apply]** を押すと、即座に IP アドレス変更が実動作に反映されます。この場合パソコンと無線 LAN 装置との間の LAN 接続が切断されるため、改めてブラウザから変更後の IP アドレスを指定して再接続する必要があります。なおリリース O4**からは IP アドレスを設定変更しても再起動するまでは実動作に反映されません。ここでの説明はリリース O4**以降の動作に基づいています。

3.4.4 IP アドレスの確定

をクリックすると確認画面が出てくるので、 をクリックします。

次にリセット確認画面が出てきます。まだ設定することがあるので、ここでは を押してメニューの [Encryption] をクリックします。



3.4.5 STのWEPの設定

メニュー画面の [Encryption] をクリックすると暗号化設定画面になります。AP と同じ要領で暗号方式を設定し、暗号キーを入力します。暗号キーは AP と同一にしてください。

3.4.6 ST設定の確定

暗号化設定画面の をクリックすると確認画面が出てきます。 をクリックするとリセット確認画面が出てきます。



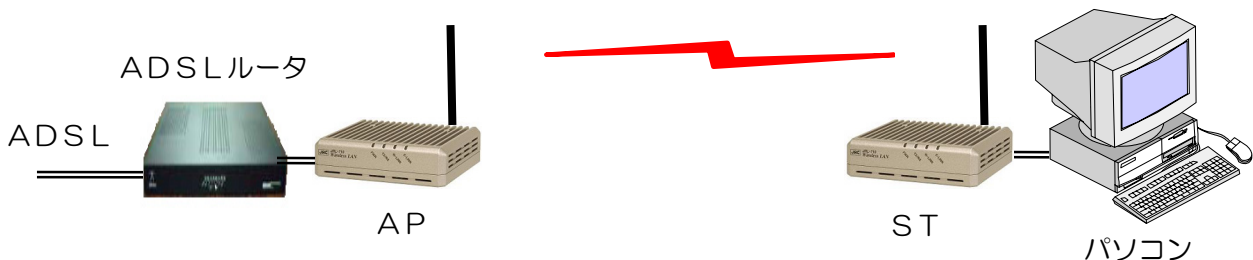
さらに をクリックすると、無線 LAN はリセット動作 (40 秒程度かかります) に入ります。リセット後に設定が機能します。

これで ST の設定は終了です。ブラウザ画面の [ファイル] → [閉じる] または ボタンでブラウザを閉じてください。

3.5 動作の確認

設定した無線 LAN をシステムに組み込みます。それまでイーサネットケーブルで接続されていたときと変わらぬ性能が得られるはずです。

インターネットに接続できる環境であれば、適当な速度測定サイトに接続してスループット (回線速度) を測定してみてください。ADSL などのインターネット接続回線の速度が十分早い場合は 10～20Mbps 程度の数値が得られます。もちろん、接続回線の速度より速くなることはありません。



[備考]

- AP-ST 間を見通せる位置に設置してください。
- 一般的な大きさ(1 辺が 30m以下)の同一室内であれば、置き場所をあまり気にせずに通信できます。
- AP-ST 間が極端に近い場合(1 m以下)は、受信電力が大きくなりすぎてスループットが低下することがあります。なお、利得の高い(指向性)アンテナを使用したときは、AP-ST 間をさらに離さないとスループットが低下することがあります。
- 近隣で他の無線 LAN や電子レンジ、医療機器などが動作しているとスループットが低下します。

簡単設定はとりあえず無線 LAN を使ってみるための設定です。セキュリティ機能は暗号化(WEP)だけですので万全とはいえませんが、無線 LAN の有用性を実感していただければと思います。

「4 詳細設定」をお読みの上、高度な機能を使いこなしていただければ幸いです。

4 詳細設定

4.1 メニュー画面の説明

WEB ブラウザで設定する場合、画面の左側に常に以下のリンクメニューの一覧が表示されており、いつでも設定(Setup)・管理(Management)・表示(Show)画面へと移動することが可能です。また、AP・ST 設定時の各使用可能メニュー項目は下記のとおりです。

【AP 設定時】



【ST 設定時】



通信するために
必要最低限の設定項目

AP/ST 設定

AP/ST 設定

高度・拡張的な設定項目

システム管理項目画面

設定項目や機器情報の確認



メニュー画面は AP/ST 設定によって異なり、各項目内も AP/ST で設定内容が異なります。デフォルトは AP 設定になっていますので、ST として設定するときには最初にメニューの [Wireless] で ST に変更してください。




4.2 設定画面の説明




画面左側のリンクメニューの項目を選択(クリック)すると、画面に設定画面(各設定・管理・表示画面)が表示されます。

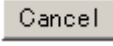

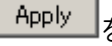
設定内容を変更する場合、表示させた設定画面上で変更する項目を選択または入力します。

以下は選択方法の例です。

表示	名称	選択方法
<input checked="" type="radio"/> enable <input type="radio"/> disable	ラジオボタン	いずれか一つだけを選択できます。 <input checked="" type="radio"/> が選択された状態です。
	プルダウンメニュー	 をクリックすると項目の一覧が表示されます。その中から一つを選択します。
<input checked="" type="checkbox"/> Wireless <input type="checkbox"/> IAPP	チェックボックス	<input checked="" type="checkbox"/> が選択されている状態です。再び <input checked="" type="checkbox"/> をクリックすると、表示が <input type="checkbox"/> になり、非選択になります。


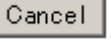
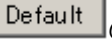
画面下部に    の3つのボタンが並んでいる設定画面では、次の操作で変更結果を保存または破棄できます。

ボタン	機能
	現在表示中の内容を設定として保存します。
	現在表示中の内容を破棄し、表示を現在の設定内容に復元します。
	現在表示中の内容を破棄し、表示を工場出荷時の設定内容に復元します。

 あるいは  は表示のみを復元します。したがって、表示内容を設定として保存する場合は、 をクリックする必要があります。

また、この操作の影響が及ぶ範囲は、現在表示中の内容についてのみであり、表示されていない内容への影響はありません。

画面によっては、操作内容に合わせて上記ボタンが表示されないものがあります。

   のボタンが表示されない画面の操作については、その画面の説明を参照ください。

4.3 ネットワーク設定[Network]

メニュー画面の [Network] をクリックすると、ネットワークの設定を行う画面になります。ここではグローバル IP アドレス、DNS サーバ、ローカル IP アドレス、イーサネット環境などを設定します。

AP で動作している場合

IP(Global)	
Obtain IP Information by DHCP ?	<input type="radio"/> enable <input checked="" type="radio"/> disable
IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text"/>
DNS(Global)	
Obtain DNS Information by DHCP ?	<input type="radio"/> enable <input checked="" type="radio"/> disable
DNS Server IP Address 1	<input type="text"/>
DNS Server IP Address 2	<input type="text"/>
IP Address (Local)	
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Ethernet Configuration	
Speed	<input type="text" value="Auto"/>
RADIUS Server	
RADIUS Server IP Address 1	<input type="text"/>
RADIUS Server Port 1	<input type="text" value="1812"/> (0-65535)
RADIUS Server Key 1	<input type="text" value="*****"/>
RADIUS Server IP Address 2	<input type="text"/>
RADIUS Server Port 2	<input type="text" value="1812"/> (0-65535)
RADIUS Server Key 2	<input type="text" value="*****"/>
* Current/Default RADIUS Server Key 1/2 is not displayed. Input 1 - 32 ASCII chars to change.	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Default"/>	

設定可能なグローバル IP アドレス、DNS サーバ、ローカル IP アドレス、デフォルトゲートウェイ IP アドレスの取得については、ネットワーク管理者やインターネット接続サービス業者にお問い合わせください。

ST で動作している場合

IP(Global)	
Obtain IP Information by DHCP ?	<input type="radio"/> enable <input checked="" type="radio"/> disable
IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text"/>
DNS(Global)	
Obtain DNS Information by DHCP ?	<input type="radio"/> enable <input checked="" type="radio"/> disable
DNS Server IP Address 1	<input type="text"/>
DNS Server IP Address 2	<input type="text"/>
IP Address (Local)	
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Ethernet Configuration	
Speed	<input type="text" value="Auto"/> ▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Default"/>	

4.3.1 グローバル IP アドレス設定[IP(Global)]

IP(Global)	
Obtain IP Information by DHCP ?	<input type="radio"/> enable <input checked="" type="radio"/> disable
IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text"/>

Obtain IP Information by DHCP ? / DHCP

DHCP クライアントを使用する/しないを決定します。

enable 使用する
 disable 使用しない ← デフォルト

⚠ 注意

- DHCP 機能は現在のところ未対応です。必ず[disable]でお使いください。

IP Address / IP アドレス

DHCP を使用しない場合、割り当てるグローバル IP アドレスを設定します。

192.168.1.1 : デフォルトの IP アドレスです。

Subnet Mask / サブネットマスク

グローバル IP アドレスのサブネットマスクを設定します。

255. 255. 255. 0：デフォルトのサブネットマスクです。

Default Gateway／デフォルトゲートウェイ

デフォルトゲートウェイの IP アドレスを設定します。

192. 168. 1. 254：デフォルトの IP アドレスです。

4.3.2 グローバル DNS 設定[DNS(Global)]

DNS (Global)	
Obtain DNS Information by DHCP ?	<input type="radio"/> enable <input checked="" type="radio"/> disable
DNS Server IP Address 1	<input type="text"/> Primary
DNS Server IP Address 2	<input type="text"/> Secondary

Obtain IP Information by DHCP ?／DHCP

DHCP クライアントを使用する/しないを設定します。

enable 使用する
 disable 使用しない ← デフォルト

⚠ 注意

- DHCP 機能は現在のところ未対応です。必ず [disable] でお使いください。

DNS Server IP Address 1／DNSサーバ(Primary)

プライマリ DNS サーバの IP アドレスを設定します。デフォルトは空欄です。

DNS Server IP Address 2／DNSサーバ(Secondary)

セカンダリ DNS サーバの IP アドレスを設定します。デフォルトは空欄です。

4.3.3 ローカル IP アドレス[IP Address(Local)]

グローバル IP アドレス以外にもう一つのアドレスをオプション指定できます。不要であれば空欄のままにします。ローカル IP アドレスの使用例については「付録 17 グローバル IP アドレスとローカル IP アドレス」を参照ください。

IP Address (Local)	
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>

IP Address／ローカル IP アドレス

割り当てるローカル IP アドレスを設定します。デフォルトは空欄です。

Subnet Mask／ローカルサブネットマスク

ローカル IP アドレスのサブネットマスクを設定します。デフォルトは空欄です。

⚠ 注意

- ローカル IP アドレスは、グローバル IP アドレスと同じ値に設定できません。

4.3.4 LAN(有線)ポートの設定[Ethernet Configuration]

Ethernet Configuration	
Speed	Auto

Speed／イーサネット速度

イーサネットポートの速度を設定します。

Auto	オートネゴシエーション ◀ デフォルト
100Mbps/Full-Duplex	100Mbps 全二重
100Mbps/Half-Duplex	100Mbps 半二重
10Mbps/Full-Duplex	10Mbps 全二重
10Mbps/Half-Duplex	10Mbps 半二重

一般にはオートネゴシエーションに設定します。HUB などの接続先によっては固定にした方がよい場合があります。

⚠ 注意

- 接続機器によっては、オートネゴシエーションでリンクが確立しないことがあります。その場合は、相手機器がサポートする速度に合わせて、本装置の内容を変更してください。
- 有線 LAN 機器同士の相互接続性については、検証を行う機関・組織が存在せず、各メーカーが独自判断に基づいて機器を製造しているのが現状です。このため全ての他社製有線 LAN 機器とのネゴシエーションについて保証することができません。接続性に問題がある場合は別途用意したハブを中継させて接続する等の回避策が必要になる場合があります。ご了承ください。

4.3.5 認証サーバの設定[RADIUS Server]

認証サーバを使用する場合の設定です。設定内容はネットワーク管理者にお尋ねください。

認証サーバを使用しないときは設定する必要はありません。

RADIUS Server	
RADIUS Server IP Address 1	<input type="text"/>
RADIUS Server Port 1	<input type="text" value="1812"/> (0-65535)
RADIUS Server Key 1	<input type="text" value="*****"/>
RADIUS Server IP Address 2	<input type="text"/>
RADIUS Server Port 2	<input type="text" value="1812"/> (0-65535)
RADIUS Server Key 2	<input type="text" value="*****"/>
<small>* Current/Default RADIUS Server Key 1/2 is not displayed. Input 1 - 32 ASCII chars to change.</small>	

RADIUS Server IP Address 1

プライマリ RADIUS サーバの IP アドレスを設定します。デフォルトは空欄です。

RADIUS Server Port 1

プライマリ RADIUS サーバのポート番号を 0～65535 で設定します。デフォルトは 1812 です。

RADIUS Server Key 1

プライマリ RADIUS サーバの RADIUS シークレットを 1 文字以上 32 文字以下の半角文字(英数

およびハイフン)で設定します。設定済の内容は「****」のように秘匿表示されます。

RADIUS Server IP Address 2

セカンダリ RADIUS サーバの IP アドレスを設定します。デフォルトは空欄です。

RADIUS Server Port 2

セカンダリ RADIUS サーバのポート番号を[0～65535]で設定します。デフォルトは[1812]です。

RADIUS Server Key 2

セカンダリ RADIUS サーバの RADIUS シークレットを 1 文字以上 32 文字以下の半角文字(英数およびハイフン)で設定します。設定済の内容は「****」のように秘匿表示されます。

4.4 認証設定[Authentication]

メニュー画面の [Authentication] をクリックすると、認証設定を行う画面になります。

より高度な認証方式(802.11i)を利用する場合は、別途 [Encryption] 画面で設定してください。

AP で動作している場合

Authentication Configuration	
Open	<input checked="" type="radio"/> enable <input type="radio"/> disable
Shared	<input checked="" type="radio"/> enable <input type="radio"/> disable
SSID	
SSID	<input type="text" value="JRL-710"/>
Suppress SSID on Beacon	<input type="radio"/> enable <input checked="" type="radio"/> disable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Default"/>	

ST で動作している場合

Authentication Configuration	
Type	<input type="text" value="auto"/>
SSID	
SSID (1)	<input type="text" value="JRL-710"/>
SSID (2)	<input type="text"/>
SSID (3)	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Default"/>	

4.4.1 認証詳細設定[Authentication Configuration]

AP で動作している場合

Authentication Configuration	
Open	<input checked="" type="radio"/> enable <input type="radio"/> disable
Shared	<input checked="" type="radio"/> enable <input type="radio"/> disable

open/オープン認証

オープン認証を許可/不許可に設定します。

enable 許可 ◀ デフォルト

disable 不許可

shared／シェアード認証

シェアード認証を許可/不許可に設定します。

enable 許可 ◀ デフォルト

disable 不許可

他メーカーの無線 LAN カードと接続するときは両方とも[enable]にした方がつながりやすくなります。

ST で動作している場合

Authentication Configuration	
Type	auto ▼

Type／認証方式

認証方式を選択します。

open オープン認証

shared シェアード認証

auto オープン/シェアード認証両方対応 ◀ デフォルト

4.4.2 SSID 設定[SSID]

AP で動作している場合

SSID	
SSID	JRL-710
Suppress SSID on Beacon	<input type="radio"/> enable <input checked="" type="radio"/> disable

SSID

SSID を 1 文字以上 32 文字以下の半角文字(英数およびハイフン)で設定します。

JRL-710 : デフォルトの SSID です。

第三者が類推しにくく、かつ管理に便利な SSID を書き込むのが原則です。システム名、場所名、管理者名などをローマ字表記で織り込む例が多いようです。

Suppress SSID on Beacon／ANY拒否

AP のビーコン信号に SSID 情報を含ませるかどうかを設定します。同時に、ANY 接続の拒否／許可が設定されます。

enable ビーコンに SSID を含まない、ANY 接続拒否

disable ビーコンに SSID を含む、ANY 接続許可 ◀ デフォルト

ANY 接続を許可すると SSID を「ANY」と設定した無線 LAN を接続できるようになります。つまり、SSID を知らない第三者の無線 LAN がネットワークに接続する危険性があります。

デフォルトは接続のしやすさを優先して [disable] になっています。通常運用中は [enable] にしてください。

ST で動作している場合

SSID	
SSID (1)	JRL-710
SSID (2)	
SSID (3)	

SSID (1) ~ (3)

SSID を 1 文字以上 32 文字以下の半角文字(英数およびハイフン)で設定します。

必ず AP の SSID に一致させてください。

JRL-710 : デフォルトの SSID です。

SSID の異なる複数の AP と接続したい場合は、ST に最大 3 つまでの SSID を設定することができます。ST の通信範囲に SSID の一致する複数の AP が存在するときは、もっとも受信電力の大きい AP を自動選択して接続します

⚠ 注意

- AP で動作しているときは、必ず SSID を設定する必要があります。
- ST で動作しているときに、[SSID (1) ~ (3)] がいずれも未入力の場合は ANY 接続 (SSID なし) の設定となります。
- ST で動作しているときに SSID (1) を「ANY」にしたままだと、AP 動作に変更できません。

4.5 暗号化設定[Encryption]

メニュー画面の [Encryption] をクリックすると、暗号化設定を行う画面になります。

画面上のプルダウンメニューから暗号モードを選択すると、各暗号モードに応じた設定画面に切り替わります。

デフォルトは暗号化無しになっていますが、限られた用途(その場限りの実験システムやデモンストレーションなど)を除き、暗号化することを推奨します。

Encryption Configuration	
Encryption Mode	none ▼
<div> <div>Apply</div> <div>Cancel</div> <div>Default</div> </div>	

Encryption Mode / 暗号化モード

暗号モードを 暗号化なし(none)/WEP/WPA-PSK/802.11i の中から選択します。

none	暗号化無し ← デフォルト	<div style="display: inline-block; vertical-align: middle;"> <div style="text-align: center;">弱</div> <div style="text-align: center;">↑</div> <div style="text-align: center;">↓</div> <div style="text-align: center;">強</div> </div> <div style="display: inline-block; vertical-align: middle; margin-left: 10px;">暗号強度</div>
WEP	WEP を選択	
WPA-PSK	WPA-PSK を選択	
802.11i	802.11i を選択	

4.5.1 WEP モード使用時

Encryption Configuration		
Encryption Mode	WEP	
WEP Key		
Use WEP Key No.	WEP1	
No.	Length	Key
WEP Key 1	none	
WEP Key 2	none	
WEP Key 3	none	
WEP Key 4	none	
* Input as hexadecimal(0-9,a-f or A-F) value. [40bit->10digits, 104bit->26digits, 128bit->32digit]		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Default"/>		

Use WEP Key No. / WEP キー選択

使用する WEP キーを選択します。

- | | | |
|------|---------------|---------|
| WEP1 | WEP Key 1 を使用 | ◀ デフォルト |
| WEP2 | WEP Key 2 を使用 | |
| WEP3 | WEP Key 3 を使用 | |
| WEP4 | WEP Key 4 を使用 | |

WEP key N length / キー長選択 (Nはキー番号 1~4 に該当します。)

WEP キーの長さを設定します。

- | | |
|----------------------------|------------------------|
| 40bit : キー長 40 (64) bit | ※WEP キーの内容は 10 文字入力する。 |
| 104bit : キー長 104 (128) bit | ※WEP キーの内容は 26 文字入力する。 |
| 128bit : キー長 128 (152) bit | ※WEP キーの内容は 32 文字入力する。 |
| none : 使用しない | ◀ デフォルト |

()内の数値はイニシャルベクター(暗号コードを生成するための乱数)24 ビットを含んだ数値です。
たとえばキー長 104 ビットのとき、この 24 ビットを足して WEP128 ビットということがあります。

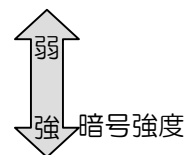
WEP key N / キー入力 (Nはキー番号 1~4 に該当します。)

WEP キーの内容を入力します。最大4つまで登録できます。

使用できる文字列は、半角英文字(a~f, A~F)および半角数字(0~9)です。

設定済の内容はキー長に応じて「****」のように秘匿表示されます。

- 例) 40 bit を選択した場合 Key : abcdef7890(10 文字)
- 104 bit を選択した場合 Key : abcdef78901234567890123456(26 文字)
- 128 bit を選択した場合 Key : abcdef78901234567890123456789012(32 文字)



暗号化してもスループットの低下はわずかです(5%以下)。

4.5.2 WPA-PSK モード使用時

AP で動作している場合

Encryption Configuration	
Encryption Mode	WPA-PSK ▼
RSN setting	
Cipher type	AES ▼
EAPoL Message Encryption	<input checked="" type="radio"/> enable <input type="radio"/> disable
Group Key Update	<input checked="" type="radio"/> on <input type="radio"/> off
Group Key Update Interval (sec)	86400 (30-86400)
PSK	
WPA-PSK Passphrase	*****
* Current/Default passphrase is not displayed. Input 8 - 63 ASCII chars to change.	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Default"/>	

ST で動作している場合

Encryption Configuration	
Encryption Mode	WPA-PSK ▼
RSN setting	
Cipher type	AES ▼
EAPoL Message Encryption	<input checked="" type="radio"/> enable <input type="radio"/> disable
PSK	
WPA-PSK Passphrase	*****
* Current/Default passphrase is not displayed. Input 8 - 63 ASCII chars to change.	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Default"/>	

Cipher Type／暗号モード

無線通信フレームの暗号アルゴリズムを設定します。

AES(Advanced Encryption Standard)は、米国商務省標準技術局(NIST)によって選定された次世代標準暗号化方式で、RC4 より暗号強度が高くなっています。

TKIP(Temporary Key Integrity Protocol)は、WEP と同じ暗号方式(RC4)で、暗号キーを無線リンクごとに変更することによって暗号強度を高めたものです。

AES 無線通信フレームを AES で暗号化 ◀ デフォルト

TKIP 無線通信フレームを TKIP で暗号化

Group Key Update／キー更新

Group key 更新の ON/OFF を設定します。Group key 更新を行うと、定期的に Multicast フレームの暗号鍵を自動更新するため、盗聴などに対するセキュリティが向上します。

※Unicast フレームの暗号鍵も自動更新する場合は、RADIUS サーバで設定します。

ON Group key を自動更新 ◀ デフォルト

OFF Group key の自動更新無し

Group Key Update Interval (30~86400 sec)／キー更新間隔

Group key の更新間隔を設定します。デフォルトは[86, 400]秒(24 時間)です。

WPA-PSK passphrase／パスフレーズ

WPA-PSK パスフレーズを8文字以上63文字以下の半角文字(英数およびハイフン)で設定します。
設定済の内容は「****」のように秘匿表示されます。

4.5.3 802.11iモード使用時

AP で動作している場合

Encryption Configuration	
Encryption Mode	802.11i ▼
RSN setting	
Cipher type	AES ▼
EAPoL Message Encryption	<input checked="" type="radio"/> enable <input type="radio"/> disable
Group Key Update	<input checked="" type="radio"/> on <input type="radio"/> off
Group Key Update Interval (sec)	86400 (30-86400)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Default"/>	

ST で動作している場合

<TLS 認証使用時>

Encryption Configuration			
Encryption Mode		802.11i ▼	
RSN setting			
Cipher type		AES ▼	
EAPoL Message Encryption		<input checked="" type="radio"/> enable <input type="radio"/> disable	
PMKSA Cache		<input checked="" type="radio"/> enable <input type="radio"/> disable	
EAP			
Extensible Authentication Protocols		TLS ▼	
Identity string for EAP		Identity string for EAP	
Certificate			
CA Certificate			
No	issuer	subject	dates
1			
2			
3			
4			
5			
6			
7			
8			
Client Certificate			
No	issuer	subject	dates
1			
<input type="button" value="IMPORT Certificate"/>			
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Default"/>			

<PEAP 認証使用時>

Encryption Configuration			
Encryption Mode	802.11i		
RSN setting			
Cipher type	AES		
EAPoL Message Encryption	<input checked="" type="radio"/> enable <input type="radio"/> disable		
PMKSA Cache	<input checked="" type="radio"/> enable <input type="radio"/> disable		
EAP			
Extensible Authentication Protocols	PEAP		
PEAP/TLS Inner Authentication Protocols	MS-CHAPv2		
Identity string for EAP	Identity string for EAP		
Password string for EAP	*****		
* Current/Default password is not displayed. Input 8 - 63 ASCII chars to change.			
Certificate			
CA Certificate			
No	issuer	subject	dates
1			
2			
3			
4			
5			
6			
7			
8			
Client Certificate			
No	issuer	subject	dates
1			
IMPORT Certificate			
Apply Cancel Default			

Cipher Type／暗号モード

無線通信フレームの暗号アルゴリズムを設定します。


AES 無線通信フレームを AES で暗号化  デフォルト

TKIP 無線通信フレームを TKIP で暗号化

Group Key Update／キー更新

Group key 更新の ON/OFF を設定します。

Group key 更新を行うと、定期的に Multicast フレームの暗号鍵を自動更新するため、盗聴などに対するセキュリティが向上します。

on Group key を自動更新  デフォルト

off Group key の自動更新無し

※Unicast フレームの暗号鍵も自動更新する場合は、RADIUS サーバで設定します。

Group Key Update Interval (30..86400 sec)／キー更新間隔

Group key の更新間隔を設定します。デフォルトは [86400] 秒(24 時間)です。

Extensible Authentication Protocols／認証モード

EAP(Extensible Authentication Protocol) 認証タイプを設定します。

EAP-TLS(EAP - Transport Layer Security)とは、サーバ／クライアントの双方で電子証明書を利用する方式で、次の PEAP よりセキュリティが強化されます。

PEAP(Protected Extensible Authentication Protocol)とは、クライアント側ではユーザーIDとパスワードによる認証、認証サーバ側では電子証明書による認証が行われる方式です。

EAP-TLS EAP-TLS で認証
PEAP PEAP で認証

PEAP/TLS Inner Authentication Protocols／内部認証モード

PEAP で使用する内部認証タイプを設定します。PEAP 時のみ有効な設定です。

MS-CHAPv2 MS-CHAP version2 で内部認証
EAP-TLS EAP-TLS で内部認証

Identity string for EAP／ユーザID

EAP 認証で使用するユーザID を設定します。

1 文字以上 32 文字以下の半角文字(英数およびハイフン)で設定します。

Password string for EAP／パスワード

EAP 認証で使用するユーザパスワードを設定します。

PEAP 内部認証が MS-CHAP version2 時のみ有効な設定です。

8 文字以上 63 文字以下の半角文字(英数およびハイフン)で設定します。

設定済のパスワードは「****」のように秘匿表示されます。

認証ファイル設定[Certificate]

Certificate			
CA Certificate			
No	issuer	subject	dates
1			
2			
3			
4			
5			
6			
7			
8			
Client Certificate			
No	issuer	subject	dates
1			
IMPORT Certificate			

CA Certificate／ルート証明書


本装置にインポートされているルート CA 証明書を表示します。(最大8個)



Client Certificate／クライアント証明書

本装置にインポートされているクライアント証明書を表示します。

証明書が8個を越えてしまった場合は、画面メッセージに従って不要なものに上書きしてください。

4.5.4 電子証明書インポート[Import Certificate Setting]

 ボタンをクリックすると、本装置に電子証明書をインポートする画面が表示されます。

Import Certificate Setting	
Import File	<input type="text"/> 
	

Import File／ファイルインポート

本装置にインポートする電子証明書ファイル名を入力、もしくは **参照...** ボタンで表示されるダイアログからファイルを選択してください。

Import ボタンをクリックすると、証明書のインポートが行われます。

4.6 無線[Wireless]

メニュー画面の [Wireless] をクリックすると、無線通信設定を行う画面になります。

AP で動作している場合

AP/ST の設定

Wireless Configuration	
Operating Type	AP ▼
RTS Threshold	2346 (0-2346)
Fragmentation Threshold	2346 (256-2346)
Hard Retry	7 (0-15)
Soft Retry	0 (0-15)
Allow ALL Inter-Client Communication	<input checked="" type="radio"/> enable <input type="radio"/> disable
ACK Timeout	short ▼
TX Power	full ▼
<hr/>	
Wireless Mode	11g ▼
AP Channel	1(2.412GHz) ▼
<hr/>	
Beacon Interval (msec)	100 (20-1000)
ERP Information Element	<input checked="" type="radio"/> enable <input type="radio"/> disable
Diversity Antenna	<input type="radio"/> enable <input checked="" type="radio"/> disable
Short Preamble	<input checked="" type="radio"/> enable <input type="radio"/> disable
<hr/>	
Rate Configuration	
<hr/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Default"/>	

デフォルトは AP 設定になっていますので、ST として設定するときは最初に ST に変更してください。

ST で動作している場合

Wireless Configuration		
Operating Type	ST	
RTS Threshold	2346	(0-2346)
Fragmentation Threshold	2346	(256-2346)
Hard Retry	7	(0-15)
Soft Retry	0	(0-15)
ACK Timeout	short	
TX Power	full	
<hr/>		
Wireless Mode	11g	
<hr/>		
Diversity Antenna	<input type="radio"/> enable <input checked="" type="radio"/> disable	
Short Preamble	<input checked="" type="radio"/> enable <input type="radio"/> disable	
<hr/>		
Pseudo Mode	<input type="radio"/> enable <input checked="" type="radio"/> disable	
Pseudo MAC	00:00:27:3E:***	
<hr/>		
Rate Configuration		
<hr/>		
Wireless Configuration for ST		
<hr/>		
Apply	Cancel	Default

Operating Type／無線局動作モード

動作モードを設定します。

- AP AP として動作 ◀ デフォルト
- ST ST として動作

RTS Threshold／RTSしきい値

RTS/CTS 機能のしきい値を [0～2346 Byte] で設定します。

この値よりも大きなデータサイズを持つフレームは RTS/CTS 交換を用いて配信します。逆にこの値以下のデータサイズを持つフレームは RTS/CTS 交換なしで配信されます。

デフォルトは [2346 Byte] です。

複数の ST を含むシステムで、ST どうしが隠れ端末状態になっていると送信競合が起きスループットが低下します。このようなときに RTS/CTS 機能を動作させると送信競合を低減できます。

一般にイーサネットのフレーム長は 1,518Byte 以下なので、それ以上の数値を設定すると RTS/CTS 機能は働きません。

Fragmentation Threshold／フラグメントしきい値

フラグメントのしきい値を設定します。無線送信しようとするデータのサイズが、このしきい値以上の場合に、そのデータを分割(フラグメント)して無線送信します。[256～2346 Byte] の間で設定してください。

デフォルトは [2346 Byte] です。

無線回線の状態が悪い(通信エラーが多い)ときでも、無線送信フレーム長を短くすれば通信が成功しやすくなります。一般にイーサネットのフレーム長は 1,518Byte 以下なので、それ以上の数値を設定するとフラグメント機能は働きません。

Hard Retry／リトライ回数(ハードウェア)

ハードウェア制御のリトライ回数を [0～15] で設定します。

デフォルトは [7] です。

リトライ回数(再送回数)を増やせば無線回線で通信エラーを生じても受信しやすくなります。無線回線の状態が非常によいときはリトライ回数を減らすとわずかですがスループットが向上します。

Soft Retry／リトライ回数(ソフトウェア)

ソフトウェア制御のリトライ回数を [0～15] で設定します。

デフォルトは [0] です。

ハードリトライ回数の上限でもパケットを正常受信できなかったときに、最初からリトライを繰り返す機能です。たとえば、ハードリトライ回数を7回、ソフトリトライ回数を3回と設定すると、同じパケットの送信を最大 32 回繰り返します。

(最初の1回+ハードリトライ7回)×(最初の1回+ソフトリトライ3回)=32回

Allow ALL Inter-Client Communication／ST間通信

AP が、ST 間通信(子機間通信)を許可するかどうかを設定します。

enable	ST 間通信を許可	◀ デフォルト
disable	ST 間通信を禁止	

無線 ISP(Internet Services Provider)などで、ST ごとにユーザが異なる場合は ST 間通信を不許可にします。また、マルチキャストで画像データを伝送する場合は必ず [disable] にしてください。

ACK Timeout／ACK待ち時間

長距離通信時の ACK の応答待ち時間を設定します。最大通信距離に応じて [short], [medium], [long] のいずれかを選択します。

short	最大通信距離 2km まで	◀ デフォルト
medium	最大通信距離 5km まで	
long	最大通信距離 30km まで	

ACK Timeout を長くするとわずかですがスループットが低下しますので、必要最小値を選択することが望ましいといえます。電波の伝搬時間を元に通信距離を計算していますが、約 2 倍の余裕を見た計算値ですので、実際の通信距離が表の距離より多少長くなっても通信可能です。

TX Power／送信電力制御


送信電力の最大値を設定します。周辺機器への干渉が問題になる場合、[full] 以外を選択して送信電力を下げてください。ここでいう最大出力は、無線 LAN の機種ごとにあらかじめ申請された送信電力を表します。

full	最大出力	◀ デフォルト
half	最大出力 -3dB(1 / 2)	
quarter	最大出力 -6dB(1 / 4)	
eighth	最大出力 -9dB(1 / 8)	
min	最小	

低下量は概略値です。

Wireless Mode／無線通信方式

無線通信方式を設定します。

- 11g IEEE802.11g モードを使用  デフォルト
- 11b IEEE802.11b モードを使用
- 11b+g IEEE802.11b+g モードを使用

一般には高速で耐マルチパス特性のよい 11g モードで使います。通信相手が 11b モードしか対応していないときは 11b モード、両モードが混在しているときは 11b+g モードにします。

- 11g モード：OFDM 方式 6～54Mbps
- 11b モード：DSSS 方式 1～11Mbps
- 11b+g モード：11g, 11b の両モードに対応

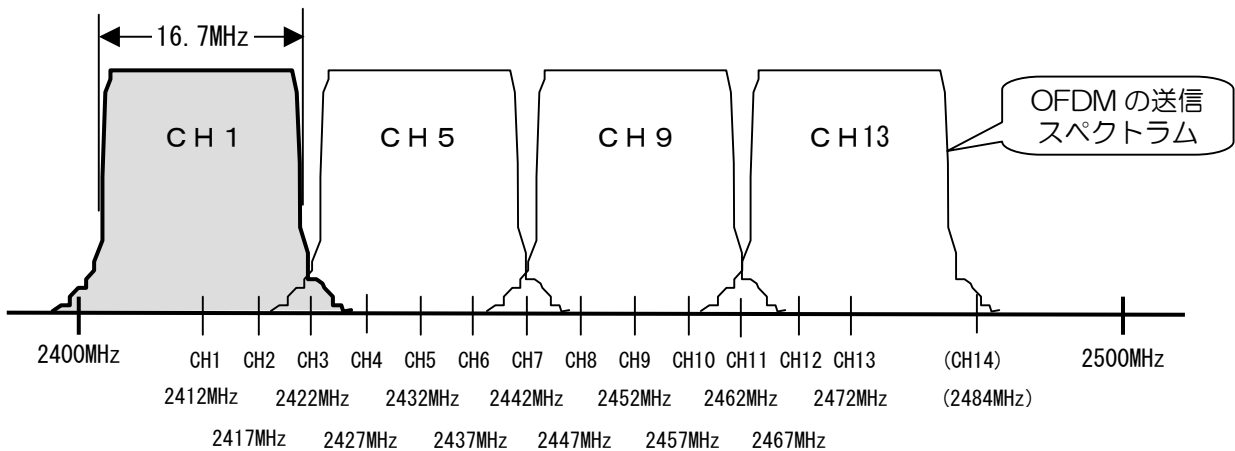
AP Channel／周波数チャネル(AP で動作している場合)

AP 動作時の使用チャネルを設定します。デフォルトはチャネル 1 です。

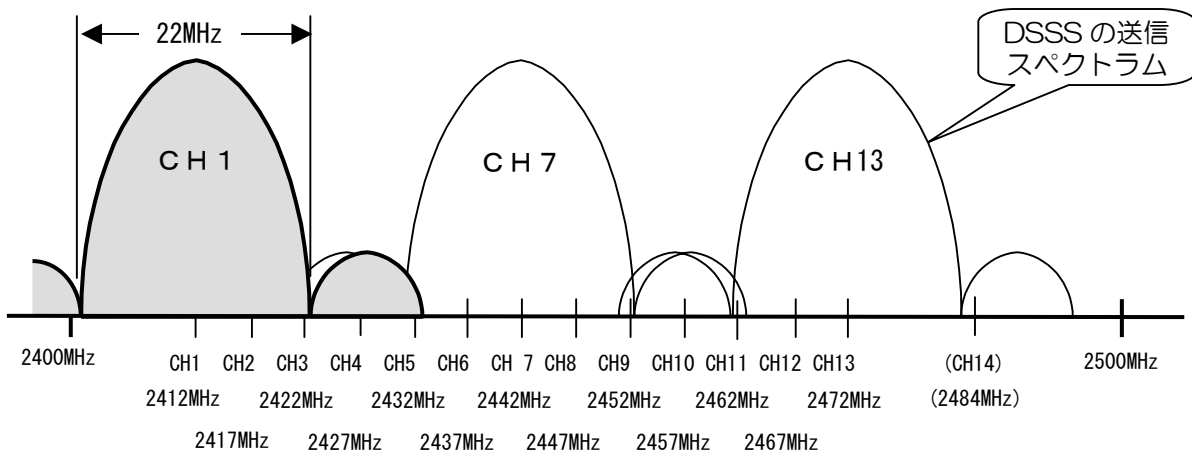
使用時に周辺の電波状態に応じチャネル 1～13 のいずれかを設定してください。

近隣に同じ周波数チャネルを使用している無線 LAN があると、CSMA 機能によって周波数を共用するためにスループットが低下します。また、無線 LAN の電波のスペクトラムは 17～22MHz に広がっているのに対してチャネル間隔は 5MHz しかありません。そのため、近隣に複数の AP を設置するときは、20MHz(OFDM：11g のとき)あるいは 25MHz(DSSS：11b のとき)以上離れた周波数チャネルを設定する必要があります。

<11g 使用時の周波数チャネル設定例>



<11b, 11b/g 使用時の周波数チャネル設定例>



Beacon Interval／ビーコン間隔 (AP で動作している場合)

ビーコン信号の送出間隔を 20～1000 msec で設定します。


デフォルトは 100 msec です。

ビーコン間隔を長くすると、ST が AP に接続するまでの時間が長くなります。また、極端にみじかくすると、わずかですがスループットが低下します。

ERP Information Element／ERP 情報

ERP Information とは、802.11g 規格に準拠した無線フレームに含まれる情報です。

他社製無線 LAN 装置と接続する際に、ERP 情報が原因で無線リンクできない場合にのみ本設定を変更してください。AP、ST とともに JRL-710/720 シリーズをご使用の場合は、デフォルト値から変更する必要はありません。


enable ERP 情報をサポート  デフォルト

disable ERP 情報のサポートなし

Diversity Antenna／ダイバーシティ

アンテナダイバーシティ機能を設定します。アンテナダイバーシティとは1台の無線LANに2本のアンテナを接続し、受信条件のよいアンテナを自動的に選択して通信する機能です。マルチパスフェージングなどで受信電力が低下する場合に有効です。

enable ダイバーシティ機能有効


disable ダイバーシティ機能無効  デフォルト。

注意

- アンテナダイバーシティに対応していない機種は、必ず [disable] でお使いください。
- アンテナダイバーシティに対応している機種で本機能を有効にした場合、ANT1、ANT2 の両端子にアンテナを接続してください。
- 技術基準適合証明を取得したアンテナを使用してください(適合アンテナは取扱説明書やカタログ等を参照してください)。

Short Preamble／ショートプリアンプル

ショートプリアンプルのサポートを設定します。

enable ショートプリアンプルを選択  デフォルト

disable ロングプリアンプルを選択

回線が劣悪で通信エラーが多いときに、ロングプリアンプルにすると改善する場合があります。通常はショートプリアンプルで使います。この機能は DSSS 方式のときに有効です。

Pseudo Mode／代理送受信モード (ST で動作している場合)

ST 動作時、有線 LAN 接続された外部機器の MAC アドレスを名乗って無線送受します。このため AP 側から見ると、対象の外部機器があたかも無線 LAN インタフェースを備えた装置であるかのように見えます。代理送受信する対象の外部機器は登録した 1 台のみ可能です。

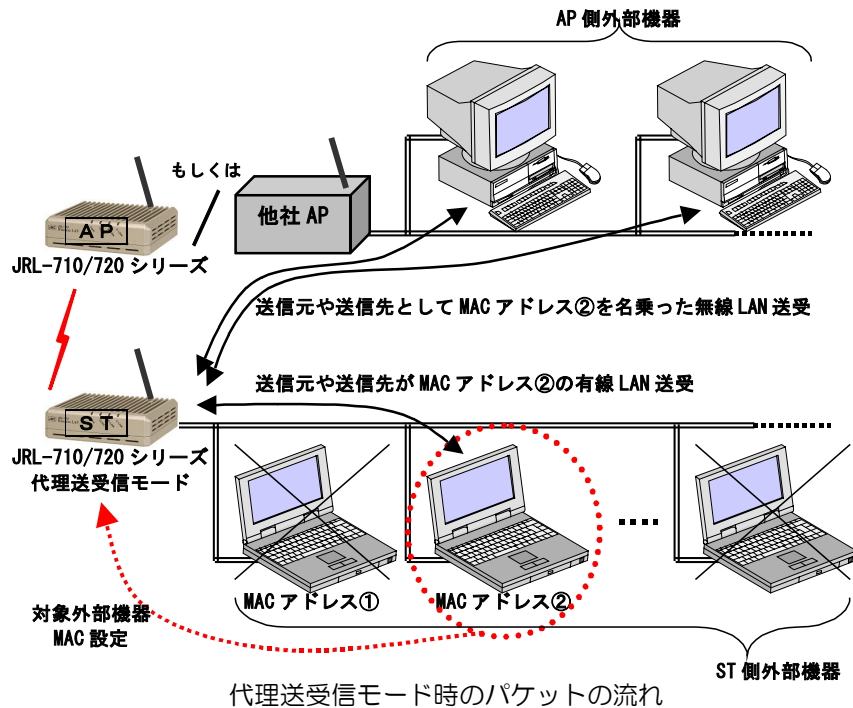
代理送受信モード設定時は、無線側から届いたパケットは無条件に外部機器に転送されます。

(無線パケットに含まれる宛先 MAC アドレスが外部機器のため)

従って代理送受信モード時は、ST に対する無線通信が不可能となります。

デフォルトは無効です。

enable 有効
 disable 無効 ◀ デフォルト



送信元 \ 送信先	ST 側外部機器	代理送受信設定 ST	AP	AP 側外部機器
ST 側外部機器		○(有線 LAN 接続)	○	○
代理送受信設定 ST	○(有線 LAN 接続)		○	○
AP	○	×		○(有線 LAN 接続)
AP 側外部機器	○	×	○(有線 LAN 接続)	

各機器間での通信の可否

代理送受信モード時は、無線区間を越えての ST へのアクセスは不可能になります。従って AP 側に有線 LAN 接続した機器からの ST の設定変更・diag コマンド実行はできません。代理送受信モード時の ST 設定変更・diag 実行は必ず ST に有線 LAN 接続した機器から行ってください。

JRL-710/720 シリーズは、AP 側・ST 側それぞれに有線 LAN 接続された複数の機器同士が通信し合える他社にない長所を持っています。代理送受信モードは、ST 設定した JRL-710/720 シリーズの無線 LAN 装置を市販の一般的な民生用 AP に無線接続させるためのモードであり、本シリーズのこの長所を制限した使用方法です。ST を代理送受信モードに設定すると、ST に有線接続した機器のうちの 1 台しか AP 側と通信できません。

JRL-710/720 シリーズを AP・ST 両方で使用される場合は、本シリーズの長所を生かした使用方法である「代理送受信モード」無効の設定を選択してください。

Pseudo MAC／代理送受信 MAC(ST で動作している場合)

代理送受信する対象の外部機器 MAC アドレスを設定します。

「**:**:**:**:**」のフォーマットで MAC アドレスを指定します。

代理送受信モードが無効の場合、このパラメータは参照されません。
デフォルトは、本無線 LAN 装置の無線 MAC アドレスです。

4.6.1 無線レート設定[Wireless Rate Configuration]

無線送信レートに関する設定画面です。

Wireless Configuration

Operating Type: AP

RTS Threshold: 2346 (0-2346)

Fragmentation Threshold: 2346 (256-2346)

Hard Retry: 7 (0-15)

Soft Retry: 0 (0-15)

Allow ALL Inter-Client Communication: ☒ enable ☐ disable

ACK Timeout: short

TX Power: full

Wireless Mode: 11g

AP Channel: 1(2.412GHz)

Beacon Interval (msec): 100 (20-1000)

ERP Information Element: ☒ enable ☐ disable

Diversity Antenna: ☐ enable ☒ disable

Short Preamble: ☒ enable ☐ disable

Rate Configuration

Apply Cancel Default

このボタンをクリックします

Rate Configuration

ボタンをクリックすると、[Rate Configuration] 画面に切り替わります。

<11g 使用時>：デフォルト

Rate Configuration

Wireless Mode: 11g

11g-protect: ☐ enable ☒ disable

11g Rate Set

	Supported	Basic	Mgmt	Multicast	Data(Unicast)
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
5.5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
11	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
12	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
18	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
24	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
36	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
48	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
54	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>

Ok

<11b 使用時>

Rate Configuration					
Wireless Mode					11b
11b Rate Set					
	Supported	Basic	Mgmt	Multicast	Data(Unicast)
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
5.5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Ok					

<11b+g 使用時>

Rate Configuration						
Wireless Mode					11b+g	
11g-protect					<input type="radio"/> enable <input checked="" type="radio"/> disable	
11b/11g Rate Set						
	Supported	Basic	Mgmt	Multicast	Data(Unicast)	
					11b	11g
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5.5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>		<input checked="" type="checkbox"/>
9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>		<input checked="" type="checkbox"/>
11	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>		<input checked="" type="checkbox"/>
18	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>		<input checked="" type="checkbox"/>
24	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>		<input checked="" type="checkbox"/>
36	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>		<input checked="" type="checkbox"/>
48	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>		<input checked="" type="checkbox"/>
54	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>		<input checked="" type="checkbox"/>
Ok						

[Rate Configuration]画面に切り替える前に、あらかじめWireless Modeを希望のモード(11g, 11b, 11b+g から選択)に設定しておいて下さい。

11g-protect/11g プロテクト

11g プロテクト機能の有効/無効を設定します。

11g 動作時、本機能を有効にすることで、周辺の第三者の 11b 端末との通信干渉を低減することができます。反面、プロテクト機能の処理時間分、無線送信が遅延するため、無線通信のスループットが多少低下する場合があります。

enable 11g プロテクト機能が有効

disable 11g プロテクト機能が無効 ◀ デフォルト

Supported Rate 1~54Mbps/サポートレート

サポートレートを設定します。

サポートレートとは、対応可能な伝送速度のことです。AP および ST が互いに報知し合うレー

ト情報の一つでもあり、これを受信することで無線接続相手の通信能力を把握します。

他社製無線 LAN 装置と接続する際に、サポートレートが原因で無線リンクできない場合は本設定を変更してください。

enable 当該レートをサポートレートに設定

disable 当該レートをサポートレートから除外

デフォルトは、全てのレートが [enable] です。

Basic Rate 1～54Mbps／ベーシックレート

ベーシックレートを設定します。ベーシックレートとは AP でのみ設定するパラメータで、AP が ST に対して報知するレート情報の一つです。

これを受信した ST は自身のサポートレートと比較し、無線リンクするかしないかの判断に使用します。なお、AP は ST が通知するサポートレートに、AP の報知するベーシックレートがひとつでも欠けている場合、無線リンクを拒否します。

他社製無線 LAN カードと接続する際、ベーシックレートが原因で無線リンクできない場合は本設定を変更してください。

サポートレート設定で enable にしたレートの中から、ベーシックレートを選択できます。

enable 当該レートをベーシックレートに設定する

disable 当該レートをベーシックレートに設定しない

デフォルトは、6, 12, 24Mbps が [enable] です。

Management／制御フレームレート

マネジメントフレームの送信レートを設定します。

マネジメントフレームとは、無線リンクの確立などに使用される制御フレームで、データ通信に使用されるフレームではありません。

設定値は、サポートレート設定で [enable] にしたレートの中から一つだけ選択できます。

デフォルトは 6Mbps です。

制御フレームは無線回線を動作させる上で重要なパケットです。そのため、エラーレートが低くなるように低いレートを設定します。なお、マルチパス環境下で動作させるときは、DSSS 方式の最低レート (1Mbps) より、OFDM 方式の最低レート (6Mbps) の方が有利な場合があります。

Multicast／マルチキャストレート

無線マルチキャストデータの送信レートを設定します。

AP でのみ設定するパラメータです。ST はイーサネット上のマルチキャストフレームも無線ユニキャストフレームで送信します。

設定値は、サポートレート設定で [enable] にしたレートの中から選択できます。デフォルトは 11g モードのとき 1Mbps, 11b あるいは 11b+g モードのとき 6Mbps です。11g モードでもここでの設定が優先されますので、11b から 11g にモード変更したは注意してください。

マルチキャストは ARQ (再送制御) がないので、エラーレートが低くなるように低い送信レートを設定します。なお、マルチパス環境下で動作させるときは、OFDM 方式の最低レート (6Mbps) のほうが有利な場合があります。

11g Data Rate 1～54Mbps (11b Data Rate 1～11Mbps)／ユニキャストレート

無線ユニキャストデータの送信レートを設定します。

複数のレートを [enable] とした場合は、その範囲でオートレート制御します。

固定レートで通信する場合は、所望のレートのみ [enable] としてください。

enable 当該レートを無線ユニキャストデータの送信に使用する

disable 当該レートを無線ユニキャストデータの送信に使用しない

デフォルトは全レートが [enable] です。

複数のユニキャストレートを [enable] にしておくと、その範囲内で回線の状態に応じてレートを自動可変します。具体的には通信エラーが多くなると1段レートを下げ、通信エラーが無くなるとレートを1段上げます。

固定回線などで回線状態の変化が少ない場合は、必要な伝送速度だけをサポートするようにしておくと、安定した通信状態を得られます。たとえば、24Mbps だけを [enable] にしておけば、常にそのレートで動作します。

逆に、回線状態が悪いとき(たとえば 12Mbps 以下でしか通信できないようなとき)に高いレートまで可変できる設定にすると、レート自動可変動作に多くの時間をとられスループットが低下することがあるので注意してください。

レート設定の数値はモード設定より優先します。たとえば、11g モードで制御フレームレート・マルチキャストレート・ユニキャストレートに対しそれぞれ 1Mbps だけを設定したとき、OFDM 方式は使われず、11b モードで 1Mbps に固定した場合と等価になります。

4.6.2 無線(ST 専用)設定[Wireless Configuration for ST]

ST として動作している場合の無線通信に関する設定画面です。

The image shows a screenshot of the 'Wireless Configuration' window. The title bar is 'Wireless Configuration'. The window contains several settings:

- Operating Type: ST (dropdown)
- RTS Threshold: 2346 (text input, range 0-2346)
- Fragmentation Threshold: 2346 (text input, range 256-2346)
- Hard Retry: 7 (text input, range 0-15)
- Soft Retry: 0 (text input, range 0-15)
- ACK Timeout: short (dropdown)
- TX Power: full (dropdown)
- Wireless Mode: 11g (dropdown)
- Diversity Antenna: ☐ enable ☒ disable
- Short Preamble: ☒ enable ☐ disable
- Pseudo Mode: ☐ enable ☒ disable
- Pseudo MAC: 00:00:27:3E:*** (text input)
- Rate Configuration: (button)
- Wireless Configuration for ST: (button, highlighted with a red box)
- Apply, Cancel, Default: (buttons)

このボタンをクリックします

Wireless Configuration for ST ボタンをクリックすると、[Wireless Configuration for ST] 画面に切り替わります。

Wireless Configuration for ST	
Wireless Mode	11g
Scan Mode	Active
Roaming Enable	<input type="radio"/> enable <input checked="" type="radio"/> disable
Scan Channel 1 (2.412GHz)	<input checked="" type="radio"/> enable <input type="radio"/> disable
Scan Channel 2 (2.417GHz)	<input checked="" type="radio"/> enable <input type="radio"/> disable
Scan Channel 3 (2.422GHz)	<input checked="" type="radio"/> enable <input type="radio"/> disable
Scan Channel 4 (2.427GHz)	<input checked="" type="radio"/> enable <input type="radio"/> disable
Scan Channel 5 (2.432GHz)	<input checked="" type="radio"/> enable <input type="radio"/> disable
Scan Channel 6 (2.437GHz)	<input checked="" type="radio"/> enable <input type="radio"/> disable
Scan Channel 7 (2.442GHz)	<input checked="" type="radio"/> enable <input type="radio"/> disable
Scan Channel 8 (2.447GHz)	<input checked="" type="radio"/> enable <input type="radio"/> disable
Scan Channel 9 (2.452GHz)	<input checked="" type="radio"/> enable <input type="radio"/> disable
Scan Channel 10 (2.457GHz)	<input checked="" type="radio"/> enable <input type="radio"/> disable
Scan Channel 11 (2.462GHz)	<input checked="" type="radio"/> enable <input type="radio"/> disable
Scan Channel 12 (2.467GHz)	<input checked="" type="radio"/> enable <input type="radio"/> disable
Scan Channel 13 (2.472GHz)	<input checked="" type="radio"/> enable <input type="radio"/> disable
11g RSSI To Scan (dBm)	-80 (-120 - 0)
11g Rate To Scan (Mbps)	6 (6-54)
Ok	

変更後は **Ok** ボタンをクリックすると [Wireless Configuration] の画面に戻るので、**Apply** ボタンをクリックして反映させてください。

[Rate Configuration]画面に切り替える前に、あらかじめ Wireless Mode を希望のモード (11g, 11b, 11b+g から選択) に設定しておいて下さい。

Scan Mode / スキャンモード

スキャンモードを設定します。

- | | |
|---------|---------------------|
| active | Active スキャン ◀ デフォルト |
| passive | Passive スキャン |
| any | 自動: [active]と同じ |


Active スキャンとは、接続できる AP をさがすときにプローブと呼ばれるパケットを ST が送信する方式です。

Passive スキャンとは、AP が定期的送信するビーコンを受信して接続できる AP を探す方式です。Active スキャンの方が AP に接続するまでの時間が多少早くなります。一方、Passive スキャンは ST 側で送信しないため、電波の使用時間を少なくでき、消費電力も削減できます。

any は周波数チャンネルによって Active スキャンか Passive スキャンかを自動的に選択する機能ですが、日本国の電波法ではどのチャンネルでも Active スキャンを禁止されていないので、any と設定しても Active スキャンになります。

Roaming Enable／ローミング

ローミングの設定をします。

- | | |
|---------|---|
| enable | ローミングをサポートする |
| disable | ローミングをサポートしない  デフォルト |

ローミングが「disable」でも、ST が AP の通信範囲を超えて移動すると、別の AP に接続する動作を開始します。移動先に同じ SSID の AP があれば、その AP に接続しますので、実質的にはローミング動作をします。

ローミング [enable] と [disable] の違いは、ローミング開始のきっかけが、前者は受信電力および伝送速度の変化、後者は回線断ということです。結果的にローミング [enable] の方が [disable] に比べて切替時間が早くなりますが、その差はわずか(数秒)です。

Scan Channel N／スキャンチャンネル(Nはチャンネル番号 1～13 に該当します)

チャンネル 1～13 のスキャンを設定します。

- | | |
|---------|-----------------|
| enable | 当該チャンネルをスキャンする |
| disable | 当該チャンネルをスキャンしない |

デフォルトは全チャンネルが [enable] です。

AP との接続が切断されたとき、あるいはローミング動作を開始したときは、ST は周波数チャンネルを変えながら接続できる AP を探し始めます。

デフォルトは全チャンネル(1～13)をスキャンする設定になっていますが、AP が使用している周波数チャンネルは限定されています。そのため、スキャンチャンネルを限定した方が接続するまでの時間が短くなります。ちなみに標準的なスキャン時間は 1 チャンネル当たり 100ms 程度です。

たとえば、4 台の AP がそれぞれチャンネル 1, 5, 9, 13 に設定されているときは、スキャンチャンネルはチャンネル 1, 5, 9, 13 だけを「enable」にした方がよいといえます。すべての AP の周波数チャンネルをチャンネル 1 にし、ST のスキャンチャンネルをチャンネル 1 だけに限定すれば、接続時間がもっとも短くなります。ただし、全 AP を同一チャンネルにすると、複数の ST で無線伝送帯域を分割利用することになるためスループットが低下する場合があります。

移動体通信におけるローミング動作は次の AP に接続するまでの時間は短い方がよいので、できるだけスキャンチャンネルを少なくなるようにしてください。

ST のビーコン受信レベル(RSSI)がしきい値以下になったとき、あるいは伝送速度が設定値未満になったときに、ローミング動作を開始(スキャンを開始)します。ローミング動作を開始条件は 11b(DSSS)モード、11g(OFDM)モードでそれぞれ別個に設定できます。

11b RSSI To Scan／スキャン開始レベル

11b モードでスキャンを開始する RSSI レベルのしきい値を -120～0 dBm で設定します。

デフォルトは -80 dBm です。

11b Rate To Scan／スキャン開始レート

11b モードでスキャンを開始するレートのしきい値を 1～11 Mbps で設定します。

デフォルトは 1 Mbps です。

11g RSSI To Scan／スキャン開始レベル

11g モードでスキャンを開始する RSSI レベルのしきい値を -120～0 dBm で設定します。

デフォルトは -80 dBm です。

11g Rate To Scan／スキャン開始レート

11g モードでスキャンを開始するレートのしきい値を 6～54 Mbps で設定します。

デフォルトは 6 Mbps です。

RSSI レベルのしきい値は受信感度以上で、かつ想定通信エリア内の受信レベル以下に設定します。原則としてデータ(ユニキャスト)レート設定の最小値のときの受信感度が下限になります。受信感度は伝送速度によって変化します。伝送レートに対する受信感度は付録 16 無線 LAN の簡易回線設計を参照ください。

スキャン開始レートのしきい値は、データ(ユニキャスト)レート設定の最大値から最小値の間に設定します。たとえば、データレート設定が6, 12, 24Mbps で通常は 24Mbps で動作しているシステムにおいて、スキャン開始レートのしきい値を 12Mbps に設定したとします。ST が接続している AP から遠ざかって自動レート可変機能によって 6Mbps にレートダウンしたときに、スキャン動作を開始することになります。

⚠ 注意

- スキャン開始レートのしきい値をデータ(ユニキャスト)レートの最低値以下にしたときは、レートダウンによるスキャンを開始しません。
- スキャン開始レートのしきい値をデータ(ユニキャスト)レート設定の最高値を越えて設定すると、常にスキャンを繰り返して通信動作ができなくなりますので注意してください。

4.7 SNMP の設定[SNMP]

メニュー画面の [SNMP] をクリックすると、SNMP 設定を行う画面になります。

SNMP Configuration	
Network	
Manager Address	<input type="text" value="192.168.1.0"/>
Manager Address Mask	<input type="text" value="255.255.255.0"/>
Agent Own Port	<input type="text" value="161"/>
Community Name	<input type="text" value="public"/>
Access Control	<input checked="" type="radio"/> read-only <input type="radio"/> read-write
Trap	
Sending Trap	<input type="radio"/> enable <input checked="" type="radio"/> disable
Trap Destination	<input type="text" value="192.168.1.254"/>
Trap Destination Port	<input type="text" value="162"/>
Trap Community Name	<input type="text" value="public"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Default"/>	

Manager Address

本機にアクセス可能な SNMP マネージャを指定するための設定です。以降の Manager Address Mask とともに使用します。画面例では 192.168.1.0~192.168.1.254 までの IP アドレスを持つ SNMP マネージャがアクセス可能となります。

Manager Address Mask で 0 に指定する部分は、ここでのアドレス設定も必ず 0 となるように指定してください。デフォルトは [192.168.1.0] です。

Manager Address Mask

本機にアクセス可能な SNMP マネージャを指定するための設定です。上記の Manager Address とともに使用します。255.255.255.255 を指定した場合、ただ一つの Manager Address を許可します。このときは Manager Address の値が、許可する SNMP マネージャの IP と一致した設定である必要があります。デフォルトは [255.255.255.0] です。

Agent Own Port

本機の SNMP エージェントが SNMP マネージャからの要求を待ち受けるポート番号の設定です。0～65535 の間で設定してください。

デフォルトは [161] です。

Community Name

SNMP マネージャと通信する際に使用するコミュニティ名を指定します。

デフォルトは [public] です。

Access Control

SNMP マネージャからの GET/SET 要求に対しアクセスを制限する機能の設定です。

read-only	GET のみ(読み出しのみ)可能	◀ デフォルト
read-write	GET および SET 可能	

Sending Trap

TRAP 送信をするかしないかを設定します。

enable	指定された宛先に TRAP を送信する
disable	TRAP を送信しない ◀ デフォルト

TRAP Destination

TRAP を送信する際の宛先 IP アドレスを指定します。

デフォルトは [192.168.1.254] です。

TRAP Destination Port

TRAP を送信する際の宛先ポート番号を指定します。0～65535 の間で設定してください。

デフォルトは [162] です。

TRAP Community Name

TRAP を送信する際に使用するコミュニティ名を指定します。

デフォルトは [public] です。

4.8 VLAN の設定[VLAN]

メニュー画面の [VLAN] をクリックすると、VLAN 設定を行う画面になります。

Filter

有線側から受信した 802.1q タグ付き VLAN パケットをフィルタリングおよびタグ削除すると

ともに、有線側への送信時にタグ(プライオリティ+ID)を付与する機能を動作させる設定です。

enable VLAN フィルタリング有効
disable VLAN フィルタリング無効 ◀ デフォルト

Priority

プライオリティを指定します。ここで指定されたプライオリティ値が、タグに付与されます。送信時の優先制御機能はありません。

0～7の間で設定してください。デフォルトは [0] です。

Tag ID

タグ ID を指定します。有線からパケットを受信した際、ここで指定された ID のパケットのみ通過させます。

タグを付与する設定の場合は、ここで指定した ID を有線に送信するパケットに付与します。0～4095の間で設定してください。デフォルトは [0] です。

Convert Tag

指定したタグ付き VLAN パケットを有線から受信した際のタグ削除、および有線送信する際のタグ付与を選択する設定です。この設定を [enable] にすると、有線受信したパケットのタグを削除し、また有線送信するパケットに指定されたプライオリティと ID のタグを付与します。(タグのスタックには対応しません)

enable 有線受信タグ削除および有線送信タグ付与 有効
disable 有線受信タグ削除および有線送信タグ付与 無効 ◀ デフォルト

Pass untagged to the Host

指定した ID のタグ付きパケットのみ通過させる設定であっても、タグ付でなく、かつ無線装置宛てのパケットであれば通過させる設定です。

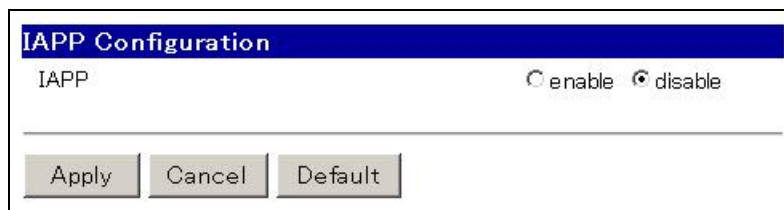
enable タグなし自装置宛パケットの通過 有効
disable タグなし自装置宛パケットの通過 無効 ◀ デフォルト

4.9 IAPP 設定[IAPP]

メニュー画面の [IAPP] をクリックすると、IAPP 設定を行う画面になります。

AP として動作している場合のみ有効な設定です。ST がローミングした場合、接続している ST 情報を有線 LAN 経由で送信あるいは受信します。

4.9.1 IAPP 設定[IAPP Configuration]



IAPP

IAPP 動作を有効にするか無効にするか設定します。

enable IAPP 動作有効
disable IAPP 動作無効 ◀ デフォルト

ST が AP 間でローミングする場合、各 AP の IAPP 機能を有効にしておくと AP 間でローミング情報の交換が行われ、動作がスムーズになる場合があります。

有効にする場合には対象となるすべての AP で [enable] を選択してください。

※ IAPP は、UDP 2313 ポートを使用します。

4.10 Filter MAC 設定[Filter MAC]

メニュー画面の [Filter MAC] をクリックすると、MAC アドレスのフィルタ設定を行う画面になります。

4.10.1 ACL Mode の設定[ACL Mode]

Mode

ACL (Access Control List) モードを有効/無効に設定します。

- enable MAC フィルタリングモード有効
- disable MAC フィルタリングモード無効 ◀ デフォルト

4.10.2 ACL リストの追加[Add ACL List]

ACL Type

登録する MAC アドレスを許可するかしないかを設定します。

- allow 許可する ◀ デフォルト
- deny 許可しない

ACL MAC

登録する MAC アドレスを設定します。使用できる文字列は、半角 16 進数字 (0~9, a~f) です。英字は大文字 (A~F) でも同じです。デフォルトは空欄です。

ACL Bitmask

ビットマスクを設定します。使用できる文字列は、半角 16 進数字 (0~9, a~f) です。英字は大文字 (A~F) でも同じです。デフォルトは空欄です。

4.10.3 ACL リストの削除[Clear ACL List]

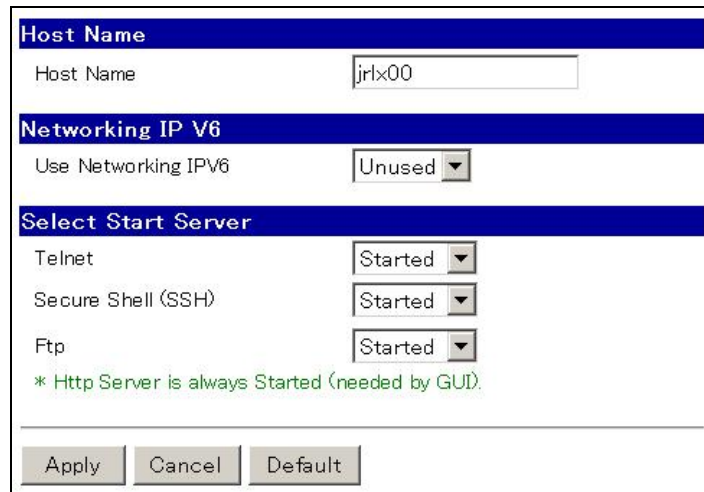

 A dialog box titled "Clear ACL List" with a blue header bar. Below the header is a white area with a "Clear" button in the bottom right corner.

Clear


をクリックすると、MAC アドレスフィルタのリストが全て削除されます。

4.11 サービス機能停止[Host Name]

メニュー画面の [Filter MAC] をクリックすると、ホスト設定を行う画面になります。

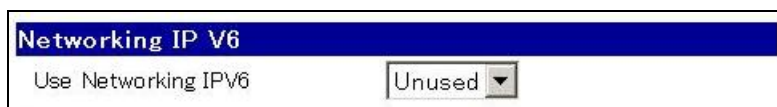

 A configuration dialog box titled "Host Name" with a blue header bar. It contains three sections: "Host Name" with a text field containing "jrlx00"; "Networking IP V6" with a dropdown menu set to "Unused"; and "Select Start Server" with three dropdown menus for "Telnet", "Secure Shell (SSH)", and "Ftp", all set to "Started". A green note below states "* Http Server is always Started (needed by GUI)". At the bottom are "Apply", "Cancel", and "Default" buttons.

4.11.1 ホストネームの設定[Host Name]


 A configuration dialog box titled "Host Name" with a blue header bar. It contains a "Host Name" section with a text field containing "jrlx00".
Host Name／ホスト名

ホスト名を 1 文字以上 64 文字以下の半角文字(英数字およびハイフン)で設定します。
デフォルトは jrlx00 です。

4.11.2 IPv6 ネットワークへの接続設定[Networking IP V6]


 A configuration dialog box titled "Networking IP V6" with a blue header bar. It contains a "Use Networking IPV6" section with a dropdown menu set to "Unused".
Use Networking IPv6／I P v 6 対応

IPv6 ネットワークへの対応を設定します。

Used	IPv6 で動作
Unused	IPv4 で動作 ← デフォルト

注意

本機能は現在のところ未対応です。必ず [Unused] でお使いください。

4.11.3 サービス機能設定[Select Start Server]

Select Start Server	
Telnet	Started ▼
Secure Shell (SSH)	Started ▼
Ftp	Started ▼
* Http Server is always Started (needed by GUI).	

Telnet

Telnet サーバを設定します。

Started	telnet サーバを開始	◀ デフォルト
Stopped	telnet サーバを停止	

Secure Shell (SSH)

SSH (Secure SHell) サーバを設定します。

Started	SSH サーバを開始	◀ デフォルト
Stopped	SSH サーバを停止	

FTP

FTP (File Transfer Protocol) サーバを設定します。

Started	FTP サーバを開始	◀ デフォルト
Stopped	FTP サーバを停止	

Telnet・SSH・FTP サーバ機能はネットワークを通して無線 LAN の制御や動作確認をするのに便利な機能です。反面、第三者からネットワークを通して設定などを変更される危険性もあります。そのため、固定的な運用(設定変更やバージョンアップがない)で、かつ高度なセキュリティを要求される場合は、これらのサービスを停止(Stopped)した方が望ましいといえます。

しかし、これらのサービスを停止すると設定変更やバージョンアップ時に利便性を損なう場合があります。サービスの開始/停止は無線側、有線側で個別に設定できますので、傍受されやすい無線回線側だけをサービス停止しておくのも一つの方法です。

HTTP サーバ機能は GUI を用いた設定を行う場合に必要になります。GUI 設定が必須となるリリース 04**からは HTTP サーバ機能を常に開始しておく必要があるため、HTTP サーバ機能の設定項目が存在しません。またリリース 04**以前のリリースをお使いの場合でも、HTTP サーバ機能を停止するとそれ以降の GUI を用いた設定変更ができなくなります。この場合は旧来の CLI を用いて設定変更を行うことになりますのでご注意ください。

4.12 接続制御設定[Access Control]

メニュー画面の [Access Control] をクリックすると、接続制御設定を行う画面になります。ネットワークからの接続に対して有効/無効を設定します。

Access Control

Ethernet-Side

Telnet ☒ enable ☐ disable

FTP ☒ enable ☐ disable

SSH ☒ enable ☐ disable

* Ethernet-Side Http Server is always enabled (needed by GUI).

Wireless-Side

Telnet ☒ enable ☐ disable

FTP ☒ enable ☐ disable

Web/HTTP ☒ enable ☐ disable

SSH ☒ enable ☐ disable

Apply Cancel Default

Ethernet-side／イーサネット(有線)側

Telnet

Telnet のアクセス制御(イーサネット側)を設定します。

- | | | |
|---------|-----------------|---------|
| enable | イーサネット側からアクセス可 | ◀ デフォルト |
| disable | イーサネット側からアクセス不可 | |

FTP

FTP のアクセス制御(イーサネット側)を設定します。

- | | | |
|---------|-----------------|---------|
| enable | イーサネット側からアクセス可 | ◀ デフォルト |
| disable | イーサネット側からアクセス不可 | |

SSH

SSH のアクセス制御(イーサネット側)を設定します。

- | | | |
|---------|-----------------|---------|
| enable | イーサネット側からアクセス可 | ◀ デフォルト |
| disable | イーサネット側からアクセス不可 | |

Wireless-side／無線側

Telnet

Telnet のアクセス制御(ワイヤレス側)を設定します。

- | | | |
|---------|----------------|---------|
| enable | ワイヤレス側からアクセス可 | ◀ デフォルト |
| disable | ワイヤレス側からアクセス不可 | |

FTP

FTP のアクセス制御(ワイヤレス側)を設定します。

- | | | |
|---------|----------------|---------|
| enable | ワイヤレス側からアクセス可 | ◀ デフォルト |
| disable | ワイヤレス側からアクセス不可 | |

Web/HTTP

HTTP のアクセス制御(ワイヤレス側)を設定します。

- | | | |
|---------|----------------|---------|
| enable | ワイヤレス側からアクセス可 | ◀ デフォルト |
| disable | ワイヤレス側からアクセス不可 | |

SSH

SSH のアクセス制御(ワイヤレス側)を設定します。

- | | | |
|--------|---------------|---------|
| enable | ワイヤレス側からアクセス可 | ◀ デフォルト |
|--------|---------------|---------|

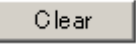
disable ワイヤレス側からアクセス不可

イーサネット側からの HTTP アクセスは GUI を用いた設定を行うとき必要になります。GUI 設定が必須となるリリース 04**からはイーサネット側から常にアクセス可にしておく必要があります。設定項目が存在しません。なおワイヤレス側からの HTTP アクセスについては、第三者からの無線 LAN 設定変更を防ぐ観点から必要に応じてアクセス可・不可を選択可能です。

4.13 フィルタパケットの設定[Filter Packet]



メニュー画面の [Filter Packet] をクリックすると、パケットフィルタを設定する画面になります。

4.13.1 フィルタパケットリスト消去[Clear All Filter Setting]

 をクリックすると、パケットフィルタのリストを全て削除されます。

4.13.2 パケットフィルタアップデート[Upload All Filter Setting]

[Filter Packet] 画面で [Upload All Filter Setting] の文字をクリックすることで [Upload All Filter Setting] 画面に切り替わります。

 ボタンをクリックしてパケットフィルタ用のファイルを選択し、 ボタンをクリックするとファイルからパケットフィルタ設定が読み込まれます。

[備考]

- パケットフィルタアップデートに必要な設定ファイルの作成については「付録 12 パケットフィルタの設定手順」を参照してください。

4.14 セントレックス機能の設定[Centrex]

メニュー画面の [Centrex] をクリックすると、セントレックス設定を行う画面になります。

セントレックス機能は AP モード時のみ機能します。AC(無線コントローラ)からの要求に応じて、AP に対し無線リンクしようとする ST を一時的にリンク制限します。

AC は最大 2 台(AC#1 および AC#2)まで設定可能です。

デフォルトではセントレックス機能は無効となっています。

セントレックス機能は特殊用途向け機能であり、通常無線 LAN を使用される上では不要な機能です。
特に断りのない限り、無効設定のままでご使用下さい。

AP Configuration

Centrex Mode ☐ enable ☒ disable

Apply Cancel Default

Centrex Mode

セントレックス機能の有効・無効を設定します。

enable 有効

disable 無効 ◀ デフォルト

メニュー画面の [Centrex Mode] を有効にすると、セントレックス機能詳細設定および無線コントローラ AC#1, AC#2 の設定画面が表示されます。

AP Configuration

Centrex Mode ☒ enable ☐ disable

Vender ID hex(0-9,a-f or A-F) 16digits.

Protocol Version hex(0-9,a-f or A-F) 4digits.

Receive Port Number (49152-65535)

Reject-Request Enable ☒ enable ☐ disable

AC#1 Configuration

AC#1 Send Enable ☐ enable ☒ disable

AC#2 Configuration

AC#2 Send Enable ☐ enable ☒ disable

Apply Cancel Default

Vender ID

AP のベンダ ID を 16 文字の半角英文字(a~f, A~F)および半角数字(0~9)で設定します。

通常設定変更する必要はありません。

デフォルトは [0000270000000000] です。

Protocol Version

AC・AP 間制御用プロトコルのバージョン番号を 4 文字の半角英文字(a~f, A~F)および半角数字(0~9)で設定します。

デフォルトは [0001] です。

Receive Port Number

AC から制御用プロトコルを受信する際のポート番号を 49152~65535 の範囲で指定します。

デフォルトは [50002] です。

Reject-Request Enable

AC#1・AC#2 から送信される接続解除要求受付の許可・不許可を設定します。

セントレックス機能無効時、接続解除要求はこのパラメータに関係なく不許可になります。

enable 許可 ◀ デフォルト

disable 不許可

AC#1 Send Enable

無線コントローラ AC#1 への通知メッセージ送信の有効・無効を設定します。

enable 有効
 disable 無効 ◀ デフォルト

AC#2 Send Enable

無線コントローラ AC#2 への通知メッセージ送信の有効・無効を設定します。

enable 有効
 disable 無効 ◀ デフォルト

メニュー画面の [AC#1 Send Enable] あるいは [AC#2 Send Enable] を有効にすると、無線コントローラ AC#1・AC#2 の詳細設定画面が表示されます。

AP Configuration	
Centrex Mode	<input checked="" type="radio"/> enable <input type="radio"/> disable
Vender ID	<input type="text" value="0000270000000000"/> hex(0-9,a-f or A-F) 16digits.
Protocol Version	<input type="text" value="0001"/> hex(0-9,a-f or A-F) 4digits.
Receive Port Number	<input type="text" value="50002"/> (49152-65535)
Reject-Request Enable	<input checked="" type="radio"/> enable <input type="radio"/> disable
AC#1 Configuration	
AC#1 Send Enable	<input checked="" type="radio"/> enable <input type="radio"/> disable
AC#1 IP Address	<input type="text" value="192.168.1.200"/>
AC#1 Send Port Number	<input type="text" value="50000"/> (49152-65535)
AC#2 Configuration	
AC#2 Send Enable	<input checked="" type="radio"/> enable <input type="radio"/> disable
AC#2 IP Address	<input type="text" value="192.168.1.201"/>
AC#2 Send Port Number	<input type="text" value="50000"/> (49152-65535)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Default"/>	

AC#1 IP Address

AC#1 の IP アドレスを指定します。

デフォルトの IP アドレスは 192.168.1.200 です。

AC#1 IP Address

AP から AC#1 に通知メッセージを送信する際の AC#1 ポート番号を指定します。

設定可能な範囲は 49152～65535 です。

既出の AP Configuration メニュー上の Receive Port Number 設定値と重複しないように数値を指定する必要があります。

デフォルトの AC#1 ポート番号は 50000 です。

AC#2 IP Address

AC#2 の IP アドレスを指定します。

デフォルトの IP アドレスは 192.168.1.201 です。

AC#2 IP Address

AP から AC#2 に通知メッセージを送信する際の #2 ポート番号を指定します。

設定可能な範囲は 49152～65535 です。

既出の AP Configuration メニュー上の Receive Port Number 設定値と重複しないように数値を指定する必要があります。

デフォルトの AC#2 ポート番号は 50000 です。

4.15 アカウント設定[Login/Password]

メニュー画面の [Login/Password] をクリックすると、ログインパスワード設定を行う画面になります。「admin」および「user」アカウントのパスワードを設定します。

Password／パスワード

パスワードを設定します。

Password(confirm)／パスワード確認

パスワード確認のため再度設定します。

⚠ 注意

- パスワードを変更する場合は、忘れないようメモをとってください。
- 「admin」アカウントでログインしてパスワードを変更した場合、「diag」アカウントのパスワードも変更されます。
- もしパスワードを忘れた場合は、本装置の「CLR」ボタンを押しながら電源を投入することで、パスワードも含めて全ての設定をリセットする(工場出荷時の状態：デフォルトに戻す)ことができます。「CLR」ボタンは電源投入後も約 40 秒間(リセット動作が終了するまで)押し続けてください。
- 屋外設置用(JRL-7**SU タイプ)など一部の機種には「CLR」ボタンがありません。

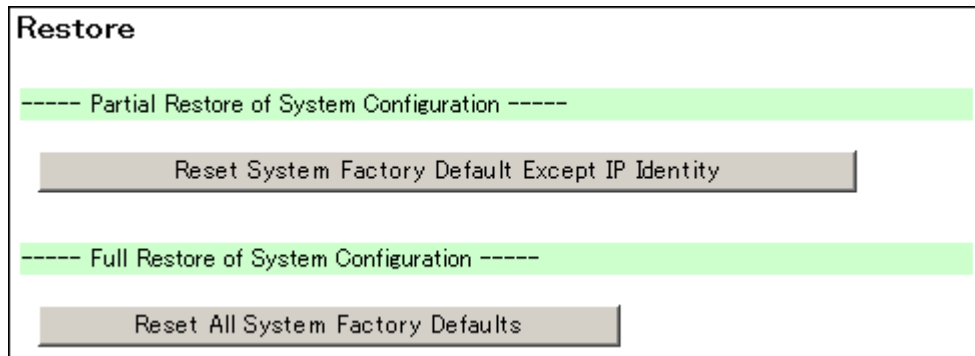
4.16 再起動[Restart]

メニュー画面の [Restart] をクリックすると、装置の再起動を行う画面になります。

Restart をクリックすると、無線 LAN が再起動します。

4.17 設定復旧[Restore]

メニュー画面の [Restore] をクリックすると、設定復旧を行う画面になります。設定をデフォルトに戻します。



Reset System Factory Default Except IP Identity : IP アドレス以外の設定情報をデフォルトに戻します。

Reset All System Factory Defaults : 全設定情報をデフォルトに戻します。

⚠ 注意

- 再起動あるいは設定復旧すると、ST で動作している場合でも動作モードは AP に戻ります。起動後、ログインし動作モードを変更してください。再起動あるいは全設定情報をデフォルトにしたときは、IP アドレスもデフォルトになるので、ログインの際には忘れずにパソコンの IP アドレスを無線 LAN と通信できるよう変更してください。

4.18 バージョンアップ[Version Up]

本装置の初期化モード機能をバージョンアップします。

初期化モード機能は、本装置のファームウェア(組込ソフトウェア)バージョンアップで使用する機能です。

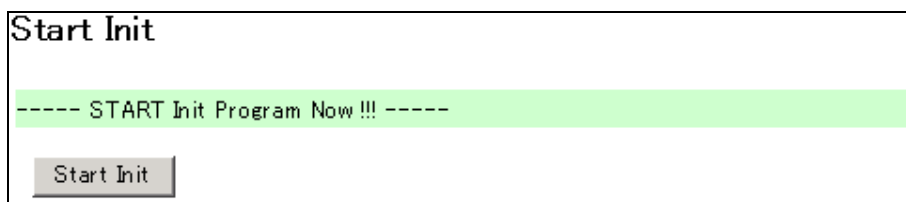
初期化モード機能およびファームウェアのバージョンアップ方法に関しては別紙『無線 LAN JRL-710/720 シリーズ ファームウェアバージョンアップマニュアル』を参照してください。

4.19 初期化モード起動[Start Init]

本装置を初期化モードで起動します。

初期化モードとは、本装置のファームウェアをバージョンアップするための特殊な動作モードです。このモードで動作中は、「W-LINK」LED が 1 秒間隔で点滅します。

メニュー画面の [Start Init] をクリックすると、装置を初期化モードで起動する画面になります。



Start Init をクリックすると、装置が初期化モードで起動します。

初期化モードを起動させた後でバージョンアップを中止したいときは、本装置の電源をいったん切り、再投入してください。

4.20 設定概要表示[Setup Summary]

メニュー画面の [Setup Summary] をクリックすると、設定項目の確認を行う画面になります。設定概要画面で表示する項目を選択します。選択された項目(☑になっている項目)の概要が表示されます。

AP で動作している場合

ST で動作している場合

以下から項目を選択し、**Display** ボタンをクリックしてください。

<u>Network</u>	ネットワーク設定情報を表示します。
<u>Authentication</u>	認証設定情報を表示します。
<u>Encyption</u>	暗号化設定情報を表示します。
<u>Wireless</u>	無線通信設定情報を表示します。
<u>SNMP</u>	SNMP 設定情報を表示します。
<u>VLAN</u>	VLAN 設定情報を表示します。
<u>IAPP</u>	(AP で動作している場合)IAPP 設定情報を表示します。
<u>Filter MAC</u>	フィルタリングされた MAC アドレス情報を表示します。
<u>Time</u>	時刻情報を表示します。
<u>Host</u>	ホスト設定情報を表示します。
<u>Access</u>	接続制御設定情報を表示します。
<u>Centrex</u>	(AP で動作している場合)セントレックス設定情報を表示します。

4.21 認証概要表示[Authentication Summary]

AP で動作している場合。メニュー画面の [Authentication Summary] をクリックすると、現在接続している ST の確認を行う画面になります。

Connection - Authentication Status	
Number of Connected the Station(s)	1
Station 1	
MAC Address	"*****"
Authentication Status	WpaAuthenticated
Authentication Type	WPA-PSK

無線MACアドレス

Number of Connected the Station(s)

無線接続している ST の数が表示されます。

MAC Address

無線接続している ST の MAC アドレスが表示されます。

Authentication Status

認証状態が表示されます。

Authentication Type

接続に使用された認証タイプが表示されます。

4.22 ログ表示[Logging]

メニュー画面の [Logging] をクリックすると、システム履歴を表示する画面になります。システムの履歴として下記に示す各履歴情報より選択表示します。

Logging	
<input checked="" type="radio"/> System Log	<input type="radio"/> APL Log
<pre> Jan 1 09:00:09 (JRLx00) JRLxx0 start... Jan 1 09:00:10 (none) syslogd 1.3-3: restart. Jan 1 09:00:10 (none) crontab[47]: (root) REPLACE (root) Jan 1 09:00:10 (none) /sbin/cron[48]: (CRON) INFO (pidfile fd = 3) Jan 1 09:00:11 (none) /sbin/cron[49]: (CRON) STARTUP (fork ok) Jan 1 09:00:11 (none) /sbin/cron[49]: (CRON) INFO (Running @reboot jobs) Jan 1 00:00:13 (none) init: Re-reading inittab Jan 1 09:00:14 (none) mini_httpd[85]: socket :: - Address family not supported by protocol Jan 1 09:00:14 (none) mini_httpd[88]: started as root without requesting chroot(), warning only Jan 1 09:00:14 (none) mini_httpd[88]: starting on (none), port 80 Jan 1 09:00:14 (none) sshd[83]: Server listening on 0.0.0.0 port 22. Jan 1 09:00:22 (JRLx00) JRLAP started !!! Jan 1 09:00:22 (JRLx00) gateway device is "br0" Jan 1 09:00:23 (JRLx00) DNS1 does not set Jan 1 09:00:23 (JRLx00) DNS2 does not set Jan 1 09:00:26 (none) syslogd 1.3-3: restart. Jan 1 00:00:26 (none) init: Entering runlevel: 2 </pre>	

System Log

システム履歴を表示します。

APL Log

アプリケーション履歴を表示します。

5 診断機能

無線回線を通してデータ通信を行うためには、十分な受信電力を確保しなければなりません。また、他の無線局やノイズ発生源から電波干渉を受けると正常な通信ができなくなります。そのため、無線 LAN 構築時や運用中には電波環境の調査や無線動作状態の確認が必要です。

JRL-710/720 シリーズ無線 LAN には診断機能が組み込まれており、パソコンを接続して電波環境や無線動作状態を監視することができます。

診断機能はコマンドライン上で動作しますので、お客様ご自身でマクロ(特定の操作手順のプログラム)を組めば、自動データ収集などの高度な使い方も可能です。

5.1 機材の準備と接続

診断用パソコンと接続用ケーブルを用意します。診断用無線 LAN は、新たに用意する方法と、すでにシステムに組み込まれている無線 LAN を使用する方法があります。

無線 LAN との接続方法として、①イーサネットケーブルを通して telnet からログインする方法と、②診断用パソコンをコンソールとして専用シリアルケーブルで接続する方法を用意しています。

5.1.1 IP アドレスの設定

設定用パソコンが無線 LAN と通信できるように、パソコンの IP アドレス(セグメント)を無線 LAN の IP アドレス(同一セグメント)にあわせます。

診断用無線 LAN を新たに用意した場合、工場出荷時の無線 LAN の IP アドレスは「192.168.1.1」ですので、「192.168.1.X」に変更します。ただし「X」の値は、1 以外(2~254)の数値を入力します。たとえば、「192.168.1.101」とします。

すでにネットワークとして動作している無線 LAN の場合は、その無線 LAN に設定されている IP アドレスと同一セグメントで、ネットワーク内の他の機器と重複しない IP アドレスを設定します。

使用できる IP アドレスはネットワーク管理者に確認してください。

5.1.2 イーサネットで接続

イーサネットケーブルを通して telnet からログインする方法です。当該無線 LAN がネットワークに組み込まれている場合は、ネットワークに接続されているパソコンから操作することもできます。

5.1.3 CONSOLE ポートで接続

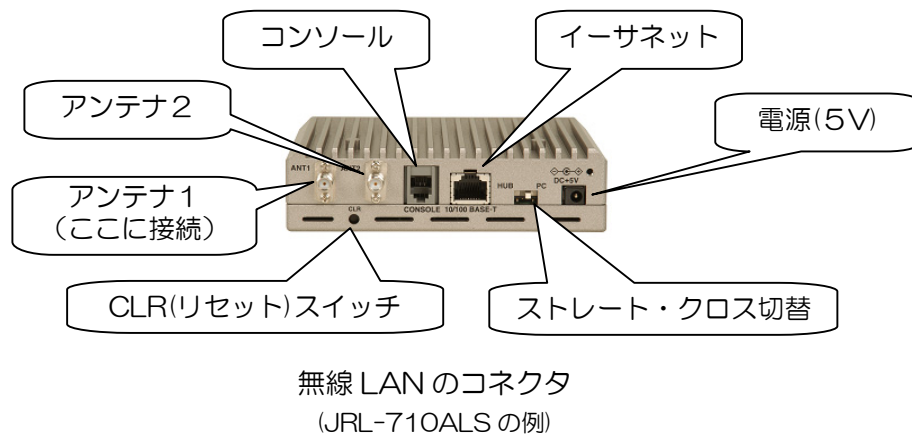
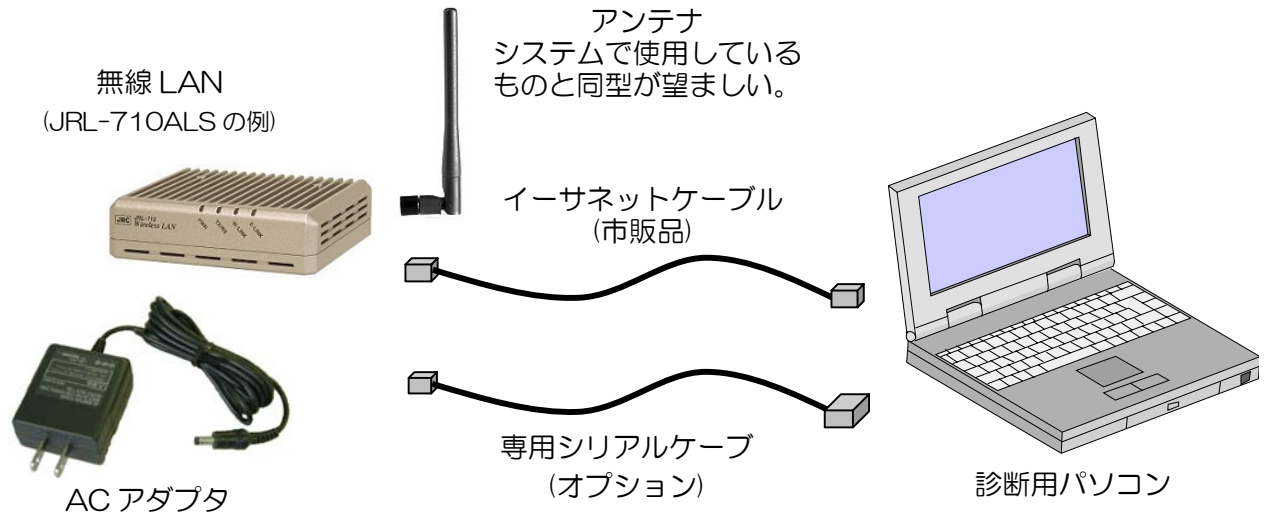
専用シリアルケーブル(オプション)を用いて、パソコンの COM ポートと無線 LAN の「CONSOLE」ポートを接続してください。独立したコネクタを使いますので、当該無線 LAN がネットワークに組み込まれている場合でも、ネットワーク側の動作を止めることなく接続ができます。

診断用パソコンの COM ポートを設定します。ハイパーターミナル等のターミナルソフトを用いてログインできます。

[備考]

- 専用シリアルケーブル(オプション)の配線については「付録 5 専用シリアルケーブル配線図」を参照ください。
- ハイパーターミナルのインストール・使用方法は、Windows のヘルプを参照してください。

- ターミナルの設定が「VT-100/漢字」の場合、正しく設定できない場合があります。「VT-100」や「VT-100/ANSI」を利用してください。
- Windows の [ping] コマンドを利用して、正しく接続したかどうかを確認できます。「付録3 接続の確認(ping コマンド)」を参照してください。
- 一部の機種には「CONSOLE」ポートがありません。



5.2 ログインとログアウト

5.2.1 ログイン

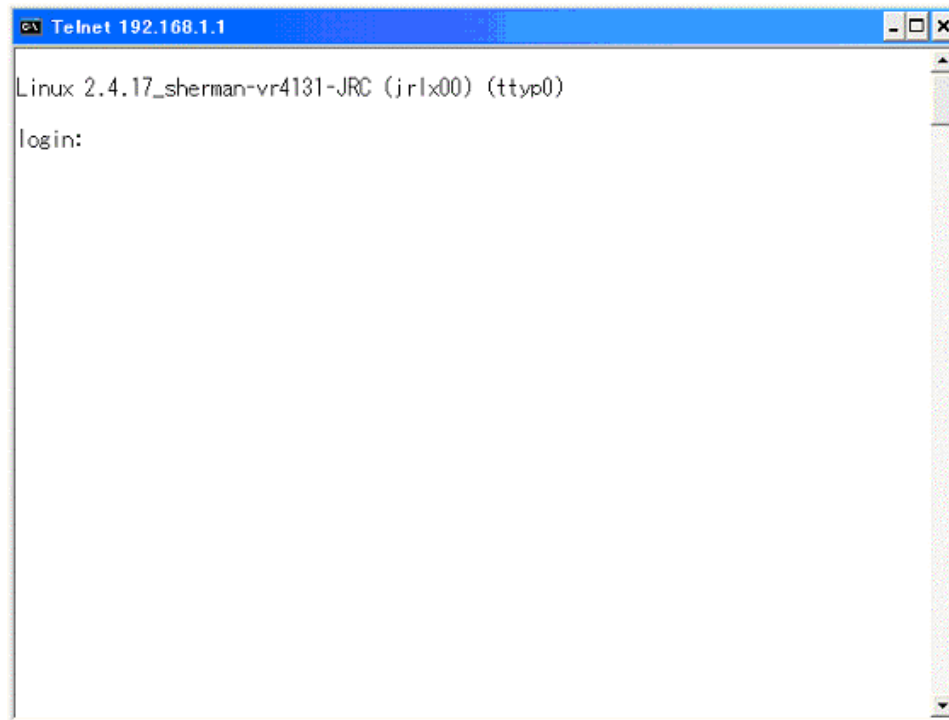
Telnet クライアントから無線 LAN にアクセスすると次の図のように表示されます。

WindowsXP/2000 では、コマンドプロンプトから「telnet 192.168.1.1」と入力すると(無線 LAN の IP アドレスが 192.168.1.1 の場合)、ログイン画面が表示されます。

ログイン画面で、ユーザ名「diag」を入力すると、パスワードの入力を要求されます。

パスワード「admin」(工場出荷時のパスワード)を入力するとログインできます。

ログインするとメニュー画面が表示されます。



⚠ 注意

- セキュリティ保護のため、入力したパスワードは表示されません。
- ユーザ名、パスワードの入力を間違えると、「Login incorrect」のメッセージが表示され、再度ユーザ名を入力する画面が表示されます。連続して3回間違えた場合およびユーザ名、パスワードの入力が60秒間なかった場合は、無線LANへの接続が切断されます。WindowsXP/2000では、「ホストとの接続が切断されました。」のメッセージが表示され、コマンドラインに戻ります。

5.2.2 ログアウト

コマンドラインから [exit] と入力するとログアウトします。

Telnet クライアントを強制的に終了させると、再ログインできなくなることがあります。この場合、無線LANの電源を入れ直す（一旦電源を切る）か、5分以上経過してからアクセスし直してください。

なお、Telnet で接続したまま5分間キーボード入力が無いと自動的にログアウトしてしまうので注意してください。

5.3 diag アカウントで使用できるコマンド

「diag」アカウントでログイン時、実行可能なコマンド一覧表を示します。

コマンド	機 能	AP	ST	備 考
?	コマンドの一覧を表示します。	○	○	
help	コマンドの一覧を表示します。	○	○	
exit	ログアウトします。	○	○	
mti	自局のアドレス情報を表示します。	○	○	
scan	スキャンを実行し、結果を一覧表示します。	○	○	
rssi	受信電力を計測・表示します。	×	○	STのみ
wti	接続している相手局を表示します。	○	○	
diag	無線回線の診断を実行します。	○	○	
stlist	接続しているSTを一覧表示します。	○	×	APのみ
pclist	接続しているSTおよびST下のパソコン等のMACアドレスを一覧表示します。	○	×	APのみ
eti	ブリッジテーブルを表示します。	○	○	
set	動作パラメータの一覧表示や設定値を変更します。	○	○	
get	指定した動作パラメータを表示します。	○	○	
save	変更した動作パラメータを装置に保存します。	○	○	
load	設定ファイルで動作パラメータを一括変更します。	○	○	
acladd	MAC アドレスフィルタリストに追加します。	○	○	
aclclr	MAC アドレスフィルタリストを削除します。	○	○	
reset	装置を簡易的にリブートします。	○	○	

コマンドの使用方法を以下に説明します。

5.4 mti コマンド(AP/ST 共通)

ログインしている装置の設定情報を表示します。

(1) コマンド書式

mti

(2) 表示例

--My Terminal Information--		
Mode	= Infrastructure	ネットワーク構成
My Type	= AP	AP/ST
MAC Address(wired)	= 00:00:27:3E:0x:xx	有線MACアドレス
MAC Address(wireless)	= 00:00:27:3E:1x:xx	無線MACアドレス
IP Address	= 192.168.1.1	IPアドレス
Subnet Mask	= 255.255.255.0	サブネットマスク
Broadcast	= 192.168.1.255	ブロードキャストアドレス
Gateway	=	デフォルト・ゲートウェイアドレス
AP channel	= 1	通信チャンネル
SSID	= [JRL-710]	SSID [] 内がSSIDです。
Wireless mode	= 11g	無線通信モード

5.5 scan コマンド

周波数チャンネルを順次変えながら各チャンネルの受信電力を測定する機能で、周辺の電波状況の調査に便利です。

AP で動作している場合、スキャンしたチャンネル、ノイズレベル(平均、ピーク)、アクティビティ(IEEE802.11 規格での動作)を表示します。

ST で動作している場合、スキャンしたチャンネル、AP の BSSID (MAC アドレス)、チャンネル、受信レベル、11b/11g モードの区別、SSID、暗号化の有無を表示します。

scan コマンドは IEEE802.11b/g で規定された無線 LAN の電波の強度を測定するものです。したがって、DSSS あるいは OFDM 以外の変調方式を用いた通信装置 (移動体識別装置、アマチュア無線など) や ISM 機器 (電子レンジ、医療器など) の電波の強度は測定できません。

DSSS あるいは OFDM 以外の電波でも極めて大きな入力があると数値として表示される場合がありますが、正確なレベルを表示できませんので注意してください。

(1) コマンド書式

scan COUNT <例> scan 100

COUNT : 測定回数を 1~2, 147, 483, 647 の範囲で指定できます。省略した場合、10 回測定し、結果を表示します。

実行中 [Ctrl] + [C] キーを押せば測定を中止できます。

(2) 表示例

AP で動作している場合

```
diag> scan 100
scan: 100 times
Scan channels are:
#MHz CHAN  MODE
2412   1  G, OFDM, 2.4G
2417   2  G, OFDM, 2.4G
2422   3  G, OFDM, 2.4G
2427   4  G, OFDM, 2.4G
2432   5  G, OFDM, 2.4G
2437   6  G, OFDM, 2.4G
2442   7  G, OFDM, 2.4G
2447   8  G, OFDM, 2.4G
2452   9  G, OFDM, 2.4G
2457  10  G, OFDM, 2.4G
2462  11  G, OFDM, 2.4G
2467  12  G, OFDM, 2.4G
2472  13  G, OFDM, 2.4G
*
```

Now scanning... (CTRL+C to stop)

```
#CHAN ANL PNL ACT
1 -87 -85 [802.11]
2 -82 -82 [802.11]
3 -84 -83 [802.11]
4
5
6 -71 -71
7
8
9
10
11 -87 -86 [802.11]
12
13
*
```

scan コマンド実行
scan を行う回数

MHz : 周波数
CHAN : チャンネル (1~13)
MODE : 無線通信モード

CHAN : チャンネル (1~13)
ANL : 平均ノイズレベル [dBm]
PNL : ピークノイズレベル [dBm]
ACT : アクティビティ (標準規格を表示)

[備考]

- 上記チャンネルのリストは、[Scan Channel] を [enable] に設定している内容に該当します。無線レート設定 [Wireless Rate Configuration] で [disable] に設定したチャンネルは表示されません。
- 上記リストのモード表示は、[Wireless Mode] で [11g] を選択した場合です。Wireless Mode で [11b] を選択した場合は、[G, OFDM, 2.4G] の部分が [B, CCK, 2.4G] になります。
- ANL は受信した複数の(受信できた)パケットの平均レベル、PNL は同最大レベルの表示です。
- ANL と PNL の数値が同じあるいは差が小さいときは、そのチャンネルを使用している無線局が1局だけの可能性が高いといえます。逆に差が大きいときは、そのチャンネルを使用している無線局が複数あり、それぞれ距離が異なる可能性が高いといえます。
- [802.11]と表示されない項目は、無線 LAN と認識できなかった信号(ISM機器やアマチュア無線など)のレベルを意味します。この場合の ANL, PNL は正確なレベルを表示できません(実際のノイズレベルに比べて小さなレベルを表示します)。

ST で動作している場合

diag> scan 100

scan: 100 times

Scan channels are:

#MHz	CHAN	MODE
2412	1	G, OFDM, 2.4G
2417	2	G, OFDM, 2.4G
2422	3	G, OFDM, 2.4G
2427	4	G, OFDM, 2.4G
2432	5	G, OFDM, 2.4G
2437	6	G, OFDM, 2.4G
2442	7	G, OFDM, 2.4G
2447	8	G, OFDM, 2.4G
2452	9	G, OFDM, 2.4G
2457	10	G, OFDM, 2.4G
2462	11	G, OFDM, 2.4G
2467	12	G, OFDM, 2.4G
2472	13	G, OFDM, 2.4G

*

Now scanning... (CTRL+C to stop)

#MAC	CHAN	RSSI	TYPE	MODE	SSID	ENC
00:00:27:3E:10:01	1	-81	AP	11g	'JRL-710'	
00:00:27:3E:10:02	6	-70	AP	11g	'JRL-710'	ENC
00:00:27:0E:00:01	11	-86	AP	11b	' '	ENC
00:00:27:1E:00:03	2	-78	AP	11g	' '	

*

scan コマンド実行

scan を行う回数

MHz：周波数

CHAN：チャンネル(1～13)

MODE：無線通信モード

MAC ADDR：MAC アドレス

CHAN：チャンネル

RSSI：受信電界強度 [dBm]

TYPE：AP or IBSS (アドホックモードの局)

SSID

ENC：暗号化の有無

ENC：有／空欄：無

[備考]

- ビーコンを受信できた AP の情報を表示します。同じチャンネルを AP 以外(ST や ISM 機器など)が使用していても表示できません。
- 上記チャンネルのリストは、[Scan Channel] を [enable] に設定している内容に該当します。無線レート設定 [Wireless Rate Configuration] で [disable] に設定したチャンネルは表示されません。
- 上記リストのモードは、[Wireless Mode] で [11g] を選択した場合です。[Wireless Mode] で [11b] を選択した場合は、[G, OFDM, 2.4G] の部分が [B, CCK, 2.4G] になります。
- 同一チャンネルで複数の SSID が存在する場合は、測定時のいずれか一つが表示されます。複数回数測定を繰り返しますので、その度に異なる SSID が表示されることがありますが、異常ではありません。

(3) 判断

できるだけ他局が使用していないチャンネルを選択します。

チャンネル間隔は 5MHz ですが、無線 LAN の電波はスペクトラムの広がり (OFDM で約 16MHz, DSSS で約 22MHz) を持っていますので、チャンネル間隔は 20~25MHz 離す必要があります。たとえば、1 チャンネルを他局が使用しているときは5あるいは6チャンネル以上を使用することになります。

実際に測定してみると、10MHz 間隔の 1, 5, 9, 13 チャンネルがすべて使われている場合もあり得ます。しかし、他局のレベルよりも自局の通信相手の信号のレベルが十分高い (たとえば 20dB 以上) ときは、大きな影響を受けずに (スループットがそれほど低下せずに) 使用できます。

5.6 stscan コマンド

周波数チャンネルを順次変えながら各チャンネルの無線 LAN 機器を探索する機能です。ST で動作させる scan コマンドと同じ結果を得られます。また、実行時のパラメータを指定することにより、スキャン実行時間の短縮や、逆にスキャン時間を増やして、受信しにくい環境にある AP の情報を探索しやすくすることが可能です。AP で動作している場合も ST で動作している場合も実行可能となっており、同じ結果が得られます。

(1) コマンド書式

```
stscan COUNT [-i interval(ms)] [-a 11a channel mask] [-b 11b/g channel mask]
```

必須

COUNT : 測定回数を 1~2, 147, 483, 647 で指定できます。省略した場合、10 回測定し、結果を表示します。実行中に [Ctrl] + [C] キーを押せば測定を中止できます。

オプション(以下省略可能)

-i intervals : スキャンするチャンネルの時間幅を変更できます。単位は ms です。指定しない場合、200ms となります。

-a 11a channel mask : スキャンするチャンネル (11a モード) を指定するときに使用します。指定できる値は 16 進数で 00~0f です。省略した場合は 0f となります。以下に対応するチャンネルとビットを示します。なお、実行する無線装置の機種により 11a モード機能が対応していない場合、本設定は無効となります。

36ch : bit0

40ch : bit1

44ch : bit2

48ch : bit3

設定例) 36ch のみスキャン : 値 = 01

40ch, 48ch のみスキャン : 値 = 0a

-b 11b/g channel mask : スキャンする 11b/g モードのチャンネルを指定するときに使用します。指定できる値は 16 進数で 0~3fff です。省略した場合は 3fff となります。上記 11a に同じく、最下位ビットが最初のチャンネル (1ch) に対応します。なお、実行する無線装置の機種により 11b 専用のチャンネル (14ch) が対応していない場合や 11g モード (1~13ch が対応していない場合は、対応するビットの値は無効となります。

設定例) 1ch, 5ch, 9ch, 13ch のみスキャン : 値 = 1111

(2) 表示例

<pre>diag> stscan 1 scan: 1 times Scan channels are: #MHz CHAN MODE 2412 1 G, OFDM, 2.4G 2417 2 G, OFDM, 2.4G 2422 3 G, OFDM, 2.4G 2427 4 G, OFDM, 2.4G 2432 5 G, OFDM, 2.4G 2437 6 G, OFDM, 2.4G 2442 7 G, OFDM, 2.4G 2447 8 G, OFDM, 2.4G 2452 9 G, OFDM, 2.4G 2457 10 G, OFDM, 2.4G 2462 11 G, OFDM, 2.4G 2467 12 G, OFDM, 2.4G 2472 13 G, OFDM, 2.4G * Now scanning... (CTRL+C to stop) #MAC CHAN RSSI TYPE MODE SSID ENC 00:00:27:3E:10:01 1 -81 AP 11g 'JRL-710' ENC 00:00:27:3E:10:02 6 -70 AP 11g 'JRL-710' ENC 00:00:27:0E:00:01 11 -86 AP 11b '' ENC 00:00:27:1E:00:03 2 -78 AP 11g '' ENC *</pre>	<p>scan コマンド実行 scan を行う回数</p> <p>MHz：周波数 CHAN：チャンネル(1~13) MODE：無線通信モード</p> <p>MAC ADDR：MAC アドレス CHAN：チャンネル RSSI：受信電界強度 [dBm] TYPE：AP or IBSS(アドホックモードの局) SSID ENC：暗号化の有無 ENC：有／空欄：無</p>
--	--

(3) 結果の判断

前項の scan コマンドと同様，AP に設定する通信チャンネルを選択する際の参考としてください。

5.7 rssi コマンド(ST で動作している場合のみ有効)

AP からのビーコン信号の受信電力(1 秒平均)を指定回数測定し，結果を表示します。AP に接続していない状態では，[! Not connected.] が表示されます。

AP からの受信信号の強度(受信電力)を直読できます。無線回線の適否の判断の他，アンテナ設置時の方向調整に便利です。

(1) コマンド書式

rssi COUNT <例> count 100

COUNT：測定回数を 1~2, 147, 483, 647 で指定できます。省略した場合，10 回(10 秒間)測定し，結果を表示します。

実行中に [Ctrl] + [C] キーを押せば測定を中止できます。

(2) 表示例

10 回(10 秒間)測定したときの表示例です。ほぼ一定した数値が得られていますので安定した回線と判断できます。

<pre>diag> rssi 10 rssi: count=10 (CTRL+C to stop) rssi: -70 rssi: -70 rssi: -71 rssi: -70 rssi: -70 rssi: -71 rssi: -71 rssi: -70</pre>	<p>10 回を指定した例</p> <p>単位は dBm</p>
---	----------------------------------

```

rssi: -71
rssi: -70

```

(3) 結果の判断

安定な通信動作のためには必要十分な受信電力が不可欠です。受信電力は少なくとも受信感度以上でなければなりません。また、回線設計で計算した受信電力と異なる場合(±6dB 以上)は、電波伝搬障害物やアンテナ方向の異常などを調査する必要があります。

5.8 wti コマンド

無線通信の接続状況を表示します。

AP で動作している場合、接続している ST の MAC アドレス(無線側)を最大 128 個、ST の下に存在する PC の MAC アドレスを最大 64 個表示します。64 個以上の場合、64 個までのリストと個数が表示されます。

ST で動作している場合、接続している AP の BSSID(=無線側 MAC アドレス)を表示します。

(1) コマンド書式

wti

(2) 表示例

AP で動作している場合

```

=== AP mode ===
#No  ST                No  PC
1    00:00:27:3E:1x:xx    1  xx:xx:xx:xx:xx:xx
*

```

接続中の ST の MAC アドレス
接続中のパソコンなどの MAC アドレス

ST で動作している場合

```

=== ST mode ===
ApAddr=00:00:27:3E:1x:xx

```

接続中の AP の MAC アドレス

5.9 diag コマンド

当社独自の無線回線診断用コマンドです。診断フレームを送出し、その結果を表示します。無線回線の評価の目安としてご利用ください。

(1) コマンド書式

diag [-b] [-c COUNT] [-s SIZE] SECOND DEST-MAC

<例>diag -b -c 30 -s 1000 10 3Exxxx

必須

SECOND : 1 回の診断時間(秒)を設定します。

DEST-MAC : 接続相手(ST)の MAC アドレス(全 12 桁のうち下 6 桁のみ)を設定します。

※ ST で実行する場合は [DEST-MAC] (=接続中の AP の MAC アドレス)を省略可能です。

オプション(以下省略可能)

-b : 診断フレームの双方向伝送を指定できます。省略した場合、片方向(自局→相手局)伝送になります。

-c COUNT : 回線診断回数を 1~60 で指定できます。省略した場合は 1 回です。

-s SIZE : 診断フレームの長さを 32~1,518 Byte で指定できます。省略した場合は 1,518 Byte になります。

diag -? 上記ヘルプを表示します。

(2) 表示例

APで動作している場合(双方向伝送, 診断回数 1 回, パケットサイズ 1,500Byte, 指定時間 3 秒, 接続相手指定)

diag> diag -b -c 1 -s 1500 3 3Exxxx						接続先MACアドレス
Target: 00:00:27:3E:xx:xx						パケットサイズ [Bytes]
Size: 1500						診断時間 [秒]
Second: 3						診断回数
Count: 1						双方向伝送
Option: Bidirectional						
DIAG running... (CTRL+C to stop)						
#	TOTAL	MIN	AVG	MAX		
TxTotal	2033	-	-	-		診断時間内の全送信 (AP→ST) パケット数
TxOk	2033	-	-	-	100.0 (% , vs TxTotal)	送信 (AP→ST) 成功パケット数
TxStraightOk	1993	-	-	-	98.0 (% , vs TxOk)	再送なしで送信 (AP→ST) 成功したパケット数
TxFailed:RetryOver	0	-	-	-	0.0 (% , vs TxTotal)	送信 (AP→ST) 失敗パケット数
						(再送回数を越えたもの)
TxFailed:NoMem	0	-	-	-		送信 (AP→ST) 失敗パケット数 (送信キューバ
						ッファフルによる)
TxFailed:Other	0	-	-	-		送信 (AP→ST) 失敗パケット数 (その他の理由
						による)
TxRetry	42	1	1.0	2		再送パケット数
TxRate (Mbps)	-	24	24.0	24		(AP→ST) 送信レート [Mbps]
TxAckRssi	-	-45	-42.9	-40		相手局 (ST) からの送信ACKのRSSI値
						[dBm]
RxOk	2033	-	-	-	100.0 (% , vs TxOk)	受信 (ST→AP) 成功パケット数
RxStraightOk	2033	-	-	-	100.0 (% , vs RxOk)	再送なしで受信 (ST→AP) 成功したパケット数
RxRate (Mbps)	-	24	24.0	24		(ST→AP) 受信レート [Mbps]
RxRssi	-	-45	-42.8	-40		受信 (ST→AP) パケットRSSI値 [dBm]
PeerRxRssi	-	-42	-39.6	-37		相手局 (ST) でパケットを受信したときのRSSI値 [dBm]
Elapse (msec)	3000	-	-	-		診断時間 [ms]
ActRate (kbps)	16318	-	-	-		実際の転送速度 [kbps]
*						

STで動作している場合(診断回数 1 回, パケットサイズ 1,450Byte, 診断時間 3 秒)

diag> diag -c 1 -s 1450 3						接続しているAP
Target: AP						パケットサイズ [Bytes]
Size: 1450						診断時間 [s]
Second: 3						診断回数
Count: 1						
Option: Delay=0						
DIAG running... (CTRL+C to stop)						
#	TOTAL	MIN	AVG	MAX		
TxTotal	4417	-	-	-		全送信 (ST→AP) パケット数
TxOk	4417	-	-	-	100.0 (% , vs TxTotal)	送信 (ST→AP) 成功パケット数
TxStraightOk	4384	-	-	-	99.2 (% , vs TxOk)	再送なしで送信 (ST→AP) 成功したパケット数
TxFailed:RetryOver	0	-	-	-	0.0 (% , vs TxTotal)	送信 (ST→AP) 失敗パケット数 (再送回数を
						越えたもの)
TxFailed:NoMem	0	-	-	-		送信 (ST→AP) 失敗パケット数 (送信キュー
						バッファフルによる)
TxFailed:Other	0	-	-	-		送信 (ST→AP) 失敗パケット数 (その他の理
						由による)
TxRetry	33	1	1.0	1		再送パケット数
TxRate (Mbps)	-	24	24.0	24		(ST→AP) 送信レート
TxAckRssi	-	-40	-38.0	-36		相手局 (AP) からのACKのRSSI [dBm]

Elapse(msec)	3000	-	-	-	診断時間 [ms]
ActRate(kbps)	17137	-	-	-	転送速度 [kbps]
*					

(3) 主要判断基準

項目	意味	判断基準
TxOk	送信成功パケット数。通常は 100%	100%であれば良好。 99%以上であれば実用可。
TxStraightOk	再送なしで送信成功したパケット数。 回線状態が良好であれば 100%	99%以上であれば良好。 90%以上であれば実用可。
TxRetry	再送パケット数。 回線状態が良好であればトータル0	全送信パケット数の1%以下であれば良好。 10%以下であれば実用可。
TxAckRssi	相手局からの ACK の RSSI [dBm]	受信感度に対して十分大きいこと。 設計値に対し6~10dB 以上。
ActRate (kbps)	転送速度 [kbps]	想定値に対して大きな差がないこと。

転送速度(スループット)は送信レートによって変化します。受信入力が高くて電波干渉がない場合は設定した送信レートの1/2程度のスループットが得られます。たとえば、送信レートを 24Mbps に設定したときに、スループット 12Mbps 程度を得られれば良好な回線と判断できます。

無線回線の適否は、RSSI コマンドや diag コマンドで受信電力を測定し、受信感度に対してマージンが取れていることで判断します。しかし、受信電力の測定には誤差があり、受信感度の公称値は最悪値なので、計算上のマージンは必ずしも絶対とはいえません。

そこで、次のような方法で実用的なマージンを確認する方法があります。

- (1) スループットが70%に低下するまで無線LANとアンテナの間にアッテネータを入れてみる。
- (2) スループットが70%に低下するまでアンテナ方向をずらしてみる(指向性アンテナの場合)。

いずれの場合も、正常状態の受信電力と、スループットが70%に低下したときの受信電力を比較すれば、実用的なマージンを知ることができます。

5.10 stlist コマンド (AP で動作している場合のみ有効)

接続している ST の MAC アドレスを表示します。

(1) コマンド書式

stlist

(2) 表示例

AP で動作している場合

```
diag> stlist
#   MAC
1   00:00:27:3E:1x:xx
*
```

接続中の ST の MAC アドレス

ST で動作している場合 (ST で stlist コマンドを実行すると次のエラーメッセージが出ます)

```
diag> stlist
stlist: wlan0: device not found or not AP mode.
```

5.11 pclist コマンド (AP で動作している場合のみ有効)

当該 AP に接続している ST と、その ST に接続しているパソコン等の MAC アドレスをリスト表示します。

(1) コマンド書式

pctllist

(2) 表示例

AP で動作している場合

```
diag> pctl list
#No ST No PC
1 00:00:27:3E:1x:xx 1 xx:xx:xx:xx:xx:xx
*
```

接続中のSTのMACアドレス
パソコン等のMACアドレス

ST で動作している場合(ST で pctl list コマンドを実行すると次のエラーメッセージが出ます)

```
diag> pctl list
stlist: wlan0: device not found or not AP mode.
```

5.12 eti コマンド

ブリッジテーブルに登録されている MAC アドレスを有線側・無線側を区別してリスト表示します。表示は最大 64 個です。64 個以上の場合、個数のみ表示されます。ブリッジテーブルのエイジングタイムは 1,800 秒(30 分)です。

(1) コマンド書式

eti

(2) 表示例

AP で動作している場合

```
diag> eti
port no mac addr is local? ageing timer
1 00:00:27:3e:0x:xx yes 0.00
2 00:00:27:3e:1x:xx yes 0.00
2 00:00:27:3e:1x:xx yes 0.00
2 00:00:27:3e:0x:xx no 420.90
2 xx:xx:xx:xx:xx:xx no 224.86
1 xx:xx:xx:xx:xx:xx no 261.64
```

ST で動作している場合

```
diag> eti
port no mac addr is local? ageing timer
2 00:00:27:3e:0x:xx no 106.10
1 00:00:27:3e:0x:xx yes 0.00
2 00:00:27:3e:1x:xx yes 0.00
1 xx:xx:xx:xx:xx:xx no 1751.70
1 xx:xx:xx:xx:xx:xx no 0.03
```

port no

1：有線側テーブルの MAC アドレス

2：無線側テーブルの MAC アドレス

Is local?

Yes：自局(当該無線 LAN)の MAC アドレス

No：他局の MAC アドレス

ageing timer：テーブルに登録されてからの経過時間 [秒]

ageing timer はブリッジテーブルに登録されてからの経過時間を示し、当該 MAC アドレスでパケットの送受信動作が生じると 0 にクリアされます。ageing timer の数値が所定のエイジングタイム(1,800 秒：30 分)に達すると、当該 MAC アドレスはテーブルから抹消されます。

自局の MAC アドレステーブルに対してはエイジングタイマが動作しないので、常に 0 秒です。

5.13 set コマンド

無線 LAN 装置の動作パラメータを変更する際に、WEB ブラウザを使用せずコマンドラインから変更するためのコマンドです。

(1) コマンド書式

<u>set</u>	: 動作パラメータを一覧表示します
<u>set</u> [パラメータ名] [設定値]	: 指定した動作パラメータを変更します
<u>set --help</u>	: 各動作パラメータの解説を表示します（英語）

指定できる動作パラメータと設定できる値については付録 21 を参照してください。

set コマンドで一覧表示される動作パラメータには、暗号化設定の一部（WEP キー 1～4, WPA-PSK パスフレーズ, 802.11i 関連パラメータ）と、装置へのログインパスワードは含まれません。get コマンドによる参照でも同じ動作となります。WEP キー 1～4 と WPA-PSK パスフレーズ、ログインパスワードはセキュリティ保護のため表示しませんが設定・変更は可能です。その際使用するパラメータ名については付録 21 を参照してください。

(2) 表示例

動作パラメータの一覧表示

```
diag> set
IPADDR      = 10. 32. 54. 132      NETMASK      = 255. 255. 255. 0
GATEWAY      =                     ELINK          = auto
AUTHEN       = 0                   SSID         = JRL-710
SSID1        = JRL-710            SSID2        =
SSID3        =                   STEALTH         = 0
ENCMODE      = 0                  KEY_LEN1     = 0
KEY_LEN2     = 0                  KEY_LEN3     = 0
KEY_LEN4     = 0                  WEPKEYID     = 1
CIPHER       = 0                  GKEY_UPD     = 1
GKEY_INT     = 86400              TYPE         = 1
RTSCTS       = 2346               FRAGMENT     = 2346
RETRY_HW     = 7                  RETRY_SW     = 0
.
.
```

暗号化設定（WEP, WPA パスフレーズ）およびログインパスワードは表示されません

動作パラメータの変更

```
diag> set SSID musen01
diag>
```

⚠ 注意

- set コマンドによる 802.11i 関連パラメータの表示・設定・変更機能には対応していません。

⚠ 注意

- set コマンドによる動作パラメータの変更だけでは、無線 LAN 装置のメモリに変更が反映されず、動作にも反映されません。set コマンドにより必要な変更を加えた際は、必ず save コマンド（後述）を実行し変更内容を装置のメモリに反映（保存）させてください。その後、装置は再起動することにより、変更したパラメータで動作を開始します。

5.14 get コマンド

無線 LAN 装置の動作パラメータを参照する際、WEB ブラウザを使用せずコマンドラインから参照するためのコマンドです。

(1) コマンド書式

get : 動作パラメータを一覧表示します
get [パラメータ名] : 指定した動作パラメータの設定値を表示します

(2) 表示例

動作パラメータの一覧表示

```
diag> get
IPADDR      = 10. 32. 54. 132      NETMASK      = 255. 255. 255. 0
GATEWAY      =                    ELINK          = auto
AUTHEN       = 0                  SSID          = JRL-710
SSID1        = JRL-710            SSID2         =
SSID3        =                   STEALTH         = 0
ENCMODE      = 0                  KEY_LEN1      = 0
KEY_LEN2     = 0                  KEY_LEN3      = 0
KEY_LEN4     = 0                  WEPKEYID      = 1
CIPHER       = 0                  GKEY_UPD      = 1
GKEY_INT     = 86400              TYPE          = 1
RTSCTS       = 2346              FRAGMENT      = 2346
RETRY_HW     = 7                  RETRY_SW      = 0
.
.
```

暗号化設定 (WEP, WPA パスフレーズ) およ
 びログインパスワードは表示されません

動作パラメータの変更

```
diag> get SSID
JRL-710
diag>
```

5.15 save コマンド

set コマンドによる無線 LAN 装置の動作パラメータ変更後に、装置内のフラッシュメモリーに動作パラメータを保存するためのコマンドです。なお、save コマンドで作成される設定ファイルには、暗号化設定の一部 (WEP キー1~4, WPA-PSK パスフレーズ, 802.11i 関連パラメータ) と、装置へのログインパスワードは含まれません。load コマンドで他の装置に書き込む場合には、テキストエディタなどを使用し、取得した設定ファイルに必要な暗号化設定を追加して使用ください。

(1) コマンド書式

save : 動作パラメータを装置に書き込みます
 装置内に以下の設定ファイルを作成します
 「setup.txt」
 「setup_<MACアドレス下位3バイト>.txt」
save [設定ファイル名] : 動作パラメータを装置に書き込み、同時に、装置内に指定した名称の設定ファイルを作成します
 (設定ファイルの詳細は付録 22を参照してください)

5.16 load コマンド

save コマンドにより作成して装置からダウンロード取得した設定ファイルを使用して、装置の動作パラメータを変更するためのコマンドです。

(2) コマンド書式

load : 設定ファイル「setup.txt」で動作パラメータを変更します
load [設定ファイル名] : 指定した設定ファイルで動作パラメータを変更します

(設定ファイルの詳細は付録 22を参照してください)

⚠ 注意

- set コマンドと同じく、load による動作パラメータの変更だけでは、無線 LAN 装置のメモリに変更が反映されず、動作にも反映されません。load コマンドにより必要な変更を加えた際は、必ず save コマンドを実行し変更内容を装置のメモリに反映（保存）させてください。その後、装置は再起動することにより、変更したパラメータで動作を開始します。

5.17 acladd コマンド

装置の MAC アドレスフィルタ機能に必要となる、フィルタアドレスを設定するコマンドです。

本コマンドを使用し、装置内で保存・管理しているリストファイルにフィルタアドレスを追加します。本コマンドにより、すでにリストに登録されているフィルタアドレスの属性を変更することも可能です。

acladd および aclclr コマンド（次項）は set や load コマンドと異なり save による装置への保存は不要です。

(1) コマンド書式

acladd : 装置に登録済みのフィルタリストを表示します
acladd [MAC アドレス] [アドレスマスク] [タイプ]
 : フィルタアドレス（マスク含む）をリストに追加します
 : タイプには 1（接続可）または 2（接続不可）を指定します

(2) 表示例

diag> acladd	フィルタリストの表示
MAC MASK type	
0000273E0000 FFFFFFF000000 1	フィルタアドレス 1
001122ABCDEF FFFFFFF000000 1	フィルタアドレス 2
diag>	
diag> acladd 00AABBCCDDEE FFFFFFFF00 1	フィルタアドレスの追加
diag>	

5.18 aclclr コマンド

装置の MAC アドレスフィルタ機能に使用するリストファイルから、登録したフィルタアドレスを削除します。パラメータを指定しない場合、リストファイルに登録されたアドレスを全て削除します。

(1) コマンド書式

aclclr : フィルタリストに登録されたアドレスを全て削除します
aclclr [MAC アドレス] [アドレスマスク]
 : フィルタアドレス（マスク含む）をリストから削除します

(2) 表示例

diag> acldlr 0000273E0000 FFFFFFF000000	フィルタアドレスの削除
diag>	
diag> acldlr	全フィルタアドレスの削除
diag>	

5.19 reset コマンド

装置をリブートします。※通常運用時は GUI の restart 機能をお使い下さい

(1) コマンド書式

reset [-y]

<例>reset -y

オプション(省略可能)

-y：確認メッセージ表示を行わず，コマンド受付と同時にリセットを実行します。

(2) 表示例

diag> reset proceed (Y/N) ? y	確認応答要求，「y」をキー入力する
----------------------------------	-------------------

6 工場出荷時設定

本装置は、下記のいずれかの操作により工場出荷時設定(デフォルト)に戻すことができます。

- トップメニューから、Management 欄の[Restore]をクリックします。
- 「CLR」ボタン※を押したまま無線 LAN の電源を投入します。「CLR」ボタンはリセット動作が終了するまで(40 秒程度)押し続けます。

※一部の機種には、「CLR」ボタンがありません。

本装置の設定項目および工場出荷時の設定を以下に示します。

⚠ 注意

- 工場出荷時設定の値は、他の設定パラメータとの整合性維持・あるは改良目的のためにファームウェアによって異なる場合があります。ご了承ください。

動作モード		設定項目名	機能	工場出荷時設定
Network				
共通	共通	IP (Global)		
		Obtain IP Information by DHCP	DHCP クライアント機能での IP アドレス取得設定 ※使用不可	disable
		IP Address (Global)	グローバル IP アドレス設定	192.168.1.1
		Subnet Mask (Global)	グローバル IP アドレスのサブネットマスク設定	255.255.255.0
		Default Gateway (Global)	デフォルトゲートウェイ IP アドレス設定	(空欄)
		DNS		
		Obtain DNS Information by DHCP	DHCP クライアント機能での DNS アドレス取得設定 ※使用不可	disable
		DNS Server IP Address (Primary)	プライマリ DNS の IP アドレス設定	(空欄)
		DNS Server IP Address (Secondary)	セカンダリ DNS の IP アドレス設定	(空欄)
		IP (Local)		
		IP Address (Local)	ローカル IP アドレス設定	(空欄)
		Subnet Mask (Local)	ローカル IP アドレスのサブネットマスク設定	(空欄)
		Ethernet Configuration		
		Ethernet Speed	イーサネットポート設定	Auto
AP	共通	RADIUS		
		RADIUS Server IP Address 1	プライマリ RADIUS の IP アドレス設定	(空欄)
		RADIUS Server Port 1	プライマリ RADIUS のポート番号設定	1812
		RADIUS Server Key 1	プライマリ RADIUS の RADIUS シークレット設定	*****
		RADIUS Server IP Address 2	セカンダリ RADIUS の IP アドレス設定	(空欄)
		RADIUS Server Port 2	セカンダリ RADIUS のポート番号設定	1812
		RADIUS Server Key 2	セカンダリ RADIUS の RADIUS シークレット設定	*****
Authentication				
AP	共通	Authentication Type		
		Authentication Type Open	オープン認証使用通信設定	enable
		Authentication Type Shared	シェアード認証使用通信設定	enable
		SSID		
		SSID (#1)	SSID1 設定	JRL-710
		Suppress SSID on Beacon	SSID の隠蔽 および ANY 接続拒否設定	disable
ST	共通	Authentication Type		
		Authentication Type	オープン/シェアード認証タイプ設定	auto
		SSID		
		SSID (#1) AnySSID	SSID1 設定	JRL-710
		SSID (#2) AnySSID	SSID2 設定	(空欄)
		SSID (#3) AnySSID	SSID3 設定	(空欄)

第 6 章 工場出荷時設定

動作モード	設定項目名	機能	工場出荷時設定
Encryption			
AP	共通	Encryption Mode	
		Encryption Mode	暗号モードの選択設定
		WEK Key	
		Use WEK key	WEK キー番号設定
		WEK key 1 length	WEK キー 1 の長さ設定
		WEK key 1	WEK キー 1 設定
		WEK key 2 length	WEK キー 2 の長さ設定
		WEK key 2	WEK キー 2 設定
		WEK key 3 length	WEK キー 3 の長さ設定
		WEK key 3	WEK キー 3 設定
		WEK key 4 length	WEK キー 4 の長さ設定
		WEK key 4	WEK キー 4 設定
		RSN Setting	
		Cipher Type	WPA-PSK/802.11i 時の暗号アルゴリズム
		EAPoL Message Encryption	EAPoL フレームの暗号化設定
		Group Key Update	グループキーの更新設定
		Group Key Update Interval	グループキーの更新間隔 [s]
		PSK Passphrase	
		WPA-PSK Passphrase	WPA-PSK 暗号化機能使用時の使用パスワード
ST	共通	Encryption Mode	
		Encryption Mode	暗号モードの選択設定
		WEK Key	
		Use WEK key	WEK キー番号設定
		WEK key 1 length	WEK キー 1 の長さ設定
		WEK key 1	WEK キー 1 設定
		WEK key 2 length	WEK キー 2 の長さ設定
		WEK key 2	WEK キー 2 設定
		WEK key 3 length	WEK キー 3 の長さ設定
		WEK key 3	WEK キー 3 設定
		WEK key 4 length	WEK キー 4 の長さ設定
		WEK key 4	WEK キー 4 設定
		RSN Setting	
		Cipher Type	WPA-PSK/802.11i 時の暗号アルゴリズム
		EAPoL Message Encryption	EAPoL フレームの暗号有効/無効設定
		PMKSA Cache	PMKSA キャッシュ有効/無効設定
		PSK Passphrase	
		WPA-PSK Passphrase	WPA-PSK 暗号化機能使用時の使用パスワード
		EAP Setting	
		EAP-TLS	
		EAP Type	EAP 認証タイプ設定
		Identity string for EAP	EAP 認証で使用するユーザ ID 設定
		PEAP	
		EAP Type	EAP 認証タイプ設定
		PEAP Inner Authentication Type	PEAP で使用する内部認証タイプ設定
		Identity string for EAP	EAP 認証で使用するユーザ ID 設定
		Password string for EAP	EAP 認証で使用するユーザパスワード設定
		Certificate	
		Certificate	本体保存認証ファイルの読み込みおよび設定

第 6 章 工場出荷時設定

動作モード		設定項目名	機能	工場出荷時設定
Wireless				
AP	共通	Wireless Configuration		
		Operating Type	AP/ST の設定	AP
		RTS Threshold	RTS しきい値設定	2346
		Fragmentation Threshold	送信パケットのフラグメント(分割) しきい値設定	2346
		Hard Retry	ハードウェア制御 1 パケット毎のリトライ最大回数設定	7
		Soft Retry	ソフトウェア制御 1 パケット毎のリトライ最大回数設定	0
		Allow ALL Inter-Client Communication	S T 間通信機能 有効/無効設定	enable
		ACK Timeout	Ack 待ち時間設定	short
		TX Power	送信パワー設定	full
		Wireless Mode	無線 LAN 通信モードの選択設定	11b
				11g
				11b+g
		AP Channel	AP 無線チャネル設定	1
		Beacon Interval	ビーコン送信間隔[ms]設定	100
		ERP Information Element	ERP 情報のサポート	enable
		Diversity Antenna	ダイバーシティ機能有効/無効設定	disable
		Short Preamble	ショートプリアンプルのサポート	enable
	11b 11b+g 11g 11b+g	Wireless Rate Configuration		
		Wireless Mode		
		11g-protect	11g プロテクト機能設定	disable
				disable
		Supported Rate Set		
		Supported Rate 1Mbps	802.11b 通信時のサポートレート設定	enable
		Supported Rate 2Mbps		enable
		Supported Rate 5.5Mbps		enable
		Supported Rate 11Mbps		enable
		Supported Rate 1Mbps	802.11g 通信時のサポートレート設定	enable
		Supported Rate 2Mbps		enable
		Supported Rate 5.5Mbps		enable
		Supported Rate 6Mbps		enable
		Supported Rate 9Mbps		enable
		Supported Rate 11Mbps		enable
		Supported Rate 12Mbps		enable
		Supported Rate 18Mbps		enable
		Supported Rate 24Mbps		enable
		Supported Rate 36Mbps		enable
		Supported Rate 48Mbps		enable
		Supported Rate 1Mbps	802.11b+g 通信時のサポートレート設定	enable
		Supported Rate 2Mbps		enable
		Supported Rate 5.5Mbps		enable
		Supported Rate 6Mbps		enable
		Supported Rate 9Mbps		enable
		Supported Rate 11Mbps		enable
		Supported Rate 12Mbps		enable
		Supported Rate 18Mbps		enable
		Supported Rate 24Mbps		enable
		Supported Rate 36Mbps		enable
		Supported Rate 48Mbps		enable
		Supported Rate 54Mbps		enable

第 6 章 工場出荷時設定

動作モード		設定項目名	機能	工場出荷時設定
Wireless				
AP	11b	Basic Rate Set		
		Basic Rate 1Mbps	802.11b 通信時のベーシックレート設定	enable
		Basic Rate 2Mbps		enable
		Basic Rate 5.5Mbps		enable
		Basic Rate 11Mbps		enable
	11g	Basic Rate 1Mbps	802.11g 通信時のベーシックレート設定	disable
		Basic Rate 2Mbps		disable
		Basic Rate 5.5Mbps		disable
		Basic Rate 6Mbps		enable
		Basic Rate 9Mbps		disable
		Basic Rate 11Mbps		disable
		Basic Rate 12Mbps		enable
		Basic Rate 18Mbps		disable
		Basic Rate 24Mbps		enable
		Basic Rate 36Mbps		disable
		Basic Rate 48Mbps		disable
		Basic Rate 54Mbps		disable
	11b+g	Basic Rate 1Mbps	802.11b+g 通信時のベーシックレート設定	disable
		Basic Rate 2Mbps		disable
		Basic Rate 5.5Mbps		disable
		Basic Rate 6Mbps		(disable) *
		Basic Rate 9Mbps		(disable) *
		Basic Rate 11Mbps		disable
		Basic Rate 12Mbps		(disable) *
		Basic Rate 18Mbps		(disable) *
		Basic Rate 24Mbps		(disable) *
		Basic Rate 36Mbps		(disable) *
		Basic Rate 48Mbps		(disable) *
		Basic Rate 54Mbps		(disable) *
	11b	Transmit Rate Set		
		Management Rate	マネジメントフレームの送信レート	1 [Mbps]
		Multicast Rate	マルチキャストデータの送信レート	1 [Mbps]
		11b Data Rate 1Mbps	802.11b 通信時のユニキャストデータ送信レート設定	enable
		11b Data Rate 2Mbps		enable
		11b Data Rate 5.5Mbps		enable
		11b Data Rate 11Mbps		enable
	11g	Management Rate	マネジメントフレームの送信レート	6 [Mbps]
		Multicast Rate	マルチキャストデータの送信レート	6 [Mbps]
		11g Data Rate 1Mbps	802.11g 通信時のユニキャストデータ送信レート設定	enable
		11g Data Rate 2Mbps		enable
		11g Data Rate 5.5Mbps		enable
		11g Data Rate 6Mbps		enable
		11g Data Rate 9Mbps		enable
		11g Data Rate 11Mbps		enable
		11g Data Rate 12Mbps		enable
		11g Data Rate 18Mbps		enable
		11g Data Rate 24Mbps		enable
		11g Data Rate 36Mbps		enable
		11g Data Rate 48Mbps		enable
		11g Data Rate 54Mbps		enable

注 *印は [disable] に固定されており， [enable] にできません。

第 6 章 工場出荷時設定

動作モード		設定項目名	機能	工場出荷時設定
Wireless				
AP	11b+g	Transmit Rate Set		
		Management Rate	マネジメントフレームの送信レート	1 [Mbps]
		Multicast Rate	マルチキャストデータの送信レート	1 [Mbps]
		11b Data Rate 1Mbps	802.11b+g 通信時のユニキャストデータ送信レート設定	enable
		11b Data Rate 2Mbps		enable
		11b Data Rate 5.5Mbps		enable
		11b Data Rate 11Mbps		enable
		11g Data Rate 1Mbps		enable
		11g Data Rate 2Mbps		enable
		11g Data Rate 5.5Mbps		enable
		11g Data Rate 6Mbps		enable
		11g Data Rate 9Mbps		enable
		11g Data Rate 11Mbps		enable
		11g Data Rate 12Mbps		enable
		11g Data Rate 18Mbps		enable
		11g Data Rate 24Mbps		enable
		11g Data Rate 36Mbps		enable
		11g Data Rate 48Mbps		enable
		11g Data Rate 54Mbps		enable
		ST		共通
Operating Type	AP/ST の設定		ST	
RTS Threshold	RTS しきい値		2346	
Fragmentation Threshold	送信パケットのフラグメント(分割)しきい値設定		2346	
Hard Retry	ハードウェア制御 1 パケット毎のリトライ最大回数設定		7	
Soft Retry	ソフトウェア制御 1 パケット毎のリトライ最大回数設定		0	
ACK Timeout	Ack 待ち時間		short	
TX Power	送信パワー設定		full	
Wireless Mode	無線 LAN 通信モードの選択設定		11b	
			11g	
			11b+g	
Diversity Antenna	ダイバーシティ 機能 有効/無効設定		disable	
Short Preamble	ショートプリアンプルのサポート		enable	
共通	Wireless Configuration for ST			
	Scan Mode		ST スキャンモードの設定	Active
	Keep Alive Probe Interval		Keep Alive フレームの送信間隔設定	0 [ms]
	Roaming Enable		ローミング機能 有効/無効設定	disable
	Scan Channel 1		チャンネル 1 スキャン設定	enable
	Scan Channel 2		チャンネル 2 スキャン設定	enable
	Scan Channel 3		チャンネル 3 スキャン設定	enable
	Scan Channel 4		チャンネル 4 スキャン設定	enable
	Scan Channel 5		チャンネル 5 スキャン設定	enable
	Scan Channel 6		チャンネル 6 スキャン設定	enable
	Scan Channel 7		チャンネル 7 スキャン設定	enable
	Scan Channel 8		チャンネル 8 スキャン設定	enable
	Scan Channel 9		チャンネル 9 スキャン設定	enable
	Scan Channel 10		チャンネル 10 スキャン設定	enable
	Scan Channel 11		チャンネル 11 スキャン設定	enable
	Scan Channel 12		チャンネル 12 スキャン設定	enable
	Scan Channel 13		チャンネル 13 スキャン設定	enable
	11b 11b+g		11b RSSI To Scan	802.11b 接続時のローミングしきい値設定(受信電界強度[dBm])
11b Rate To Scan			802.11b 接続時のローミングしきい値設定(送信レート[Mbps])	1
11g 11b+g	11g RSSI To Scan		802.11g 接続時のローミングしきい値設定(受信電界強度[dBm])	-80
	11g Rate To Scan		802.11g 接続時のローミングしきい値設定(送信レート[Mbps])	6

第 6 章 工場出荷時設定

動作モード		設定項目名	機能	工場出荷時設定
Wireless				
ST		Wireless Rate Configuration		
		Wireless Mode		
	11g	11g-protect	11g プロテクト機能設定	disable
	11b+g			disable
	11b	Supported Rate Set		
		Supported Rate 1Mbps	802.11b 通信時のサポートレート設定	enable
		Supported Rate 2Mbps		enable
		Supported Rate 5.5Mbps		enable
		Supported Rate 11Mbps		enable
	11g	Supported Rate 1Mbps	802.11g 通信時のサポートレート設定	enable
		Supported Rate 2Mbps		enable
		Supported Rate 5.5Mbps		enable
		Supported Rate 6Mbps		enable
		Supported Rate 9Mbps		enable
		Supported Rate 11Mbps		enable
		Supported Rate 12Mbps		enable
		Supported Rate 18Mbps		enable
		Supported Rate 24Mbps		enable
		Supported Rate 36Mbps		enable
		Supported Rate 48Mbps		enable
		Supported Rate 54Mbps		enable
	11b+g	Supported Rate 1Mbps	802.11b+g 通信時のサポートレート設定	enable
		Supported Rate 2Mbps		enable
		Supported Rate 5.5Mbps		enable
		Supported Rate 6Mbps		enable
		Supported Rate 9Mbps		enable
		Supported Rate 11Mbps		enable
		Supported Rate 12Mbps		enable
		Supported Rate 18Mbps		enable
		Supported Rate 24Mbps		enable
		Supported Rate 36Mbps		enable
		Supported Rate 48Mbps		enable
		Supported Rate 54Mbps		enable
	11b	Transmit Rate Set		
		Management Rate	マネジメントフレームの送信レート	1 [Mbps]
		11b Data Rate 1Mbps	802.11b 通信時のユニキャストデータ送信レート設定	enable
		11b Data Rate 2Mbps		enable
		11b Data Rate 5.5Mbps		enable
		11b Data Rate 11Mbps		enable
	11g	Management Rate	マネジメントフレームの送信レート	6 [Mbps]
		11g Data Rate 1Mbps	802.11g 通信時のユニキャストデータ送信レート設定	enable
		11g Data Rate 2Mbps		enable
		11g Data Rate 5.5Mbps		enable
		11g Data Rate 6Mbps		enable
		11g Data Rate 9Mbps		enable
		11g Data Rate 11Mbps		enable
		11g Data Rate 12Mbps		enable
		11g Data Rate 18Mbps		enable
		11g Data Rate 24Mbps		enable
		11g Data Rate 36Mbps		enable
		11g Data Rate 48Mbps		enable
		11g Data Rate 54Mbps		enable

第 6 章 工場出荷時設定

動作モード		設定項目名	機能	工場出荷時設定
Wireless				
ST	11b+g	Transmit Rate Set		
		Management Rate	マネジメントフレームの送信レート	1 [Mbps]
		11b Data Rate 1Mbps	802.11b+g 通信時のユニキャストデータ送信レート設定	enable
		11b Data Rate 2Mbps		enable
		11b Data Rate 5.5Mbps		enable
		11b Data Rate 11Mbps		enable
		11g Data Rate 1Mbps		enable
		11g Data Rate 2Mbps		enable
		11g Data Rate 5.5Mbps		enable
		11g Data Rate 6Mbps		enable
		11g Data Rate 9Mbps		enable
		11g Data Rate 11Mbps		enable
		11g Data Rate 12Mbps		enable
		11g Data Rate 18Mbps		enable
		11g Data Rate 24Mbps		enable
		11g Data Rate 36Mbps		enable
		11g Data Rate 48Mbps		enable
		11g Data Rate 54Mbps		enable
IAPP				
AP	共通	IAPP Configuration		
		IAPP	IAPP 設定	disable
ST	共通	L2Update Interval	L2UPDATE の送信間隔[s]設定	0
Centrex				
AP	共通	AP Configuration		
		Centrex Mode	Centrex 機能設定	disable
		Vender ID	ベンダ ID	0000270000000000
		Protocol Version	プロトコルバージョン番号	0001
		Receive Port Number	制御用プロトコル受信ポート番号	50002
		Reject-Request Enable	接続解除要求受付設定	enable
		AC#1 Configuration		
		AC#1 Send Enable	AC#1 通知メッセージ送信設定	disable
		AC#1 IP Address	AC#1 IP アドレス	192.168.1.200
		AC#1 Send Port Number	AC#1 ポート番号	50000
		AC#2 Configuration		
		AC#2 Send Enable	AC#2 通知メッセージ送信設定	disable
		AC#2 IP Address	AC#2 IP アドレス	192.168.1.201
		AC#2 Send Port Number	AC#2 ポート番号	50000
Time Setup				
共通	共通	DateTime Configuration		
		Current DateTime	システム時計時刻(RTC なし)	JAN 0109:00:00 1970
		UpTime	システム起動時間	0.00

第6章 工場出荷時設定

動作モード		設定項目名	機能	工場出荷時設定
Host Setup				
共通	共通	Host Configuration		
		Host Name	ホスト名設定	jrlx00
		Use Networking IPv6	IPv6 機能使用設定 ※使用不可	Unused
		Select Start Server (Telnet)	Telnet サーバ機能 開始/停止設定	Started
		Select Start Server (SSH)	SSH サーバ機能 開始/停止設定	Started
		Select Start Server (HTTP)	HTTP サーバ機能 開始/停止設定	Started
		Select Start Server (FTP)	FTP サーバ機能 開始/停止設定	Started
Access Control				
共通	共通	Access Control		
		Ethernet Side - Telnet	Telnet のアクセス制御設定(イーサネット側)	enable
		Ethernet Side - FTP	FTP のアクセス制御設定(イーサネット側)	enable
		Ethernet Side - Web/HTTP	HTTP のアクセス制御設定(イーサネット側)	enable
		Ethernet Side - SSH	SSH のアクセス制御設定(イーサネット側)	enable
		Wireless Side - Telnet	Telnet のアクセス制御設定(無線側)	enable
		Wireless Side - FTP	FTP のアクセス制御設定(無線側)	enable
		Wireless Side - Web/HTTP	HTTP のアクセス制御設定(無線側)	enable
Wireless Side - SSH	SSH のアクセス制御設定(無線側)	enable		
Filter MAC				
共通	共通	ACL Mode		
		ACL Mode	MAC アドレスフィルタ機能の有効/無効設定	disable
		ACL List		
		Add	フィルタアドレスリストへの追加設定	-
		ACL Type	フィルタアドレスリストへの追加種別(許可/拒否)設定	-
		ACL MAC	フィルタアドレスリストへの追加アドレス設定	-
		ACL Bitmask	フィルタアドレスリストへの追加アドレスの評価ビットマスク設定	-
Filter Packet				
共通	共通	Clear All Filter Setting		
		Clear All Filter Setting	フィルタパケットの設定情報を初期化する	-
SNMP				
共通	共通	SNMP Configuration		
		Manager IP Address	SNMP マネージャ IP アドレス設定	192.168.1.0
		Manager Subnet Mask	SNMP マネージャ サブネットマスク設定	255.255.255.0
		Agent Own Port	SNMP エージェント使用ポート設定	161
		Community Name	SNMP コミュニティ名設定	public
		Access Control	SNMP アクセス制御	read-only
		TRAP Level	SNMP トラップ設定	disable
		TRAP Destination IP Address	SNMP トラップ先 IP アドレス設定	192.168.1.254
		TRAP Destination Port	SNMP トラップ先ポート番号設定	162
TRAP Community Name	SNMP コミュニティ名	public		
VLAN				
共通	共通	VLAN Configuration		
		Filter	VLAN フィルタ機能の有効/無効設定	disable
		Priority	プライオリティ	0
		Tag ID	タグ ID	0
		Convert Tag	タグ削除・付与の有効/無効設定	disable
		Pass untagged to the Host	タグなし自局宛パケットのフィルタリング設定	disable
Login/Password				
共通	共通	Change Login Password	ユーザ名設定	-

7 無線 LAN 関連用語集

- 2.4GHz 帯：一般的には 2.4～2.5GHz の ISM 帯を指しますが，無線 LAN の場合は①2.4～2.497GHz または②2.4～2.4835GHz を指します。①は最初に開放された日本独自の周波数帯であり，②は欧米にあわせて追加開放された周波数帯です。①②とも無線 LAN に使用されていますが，使用できる変調方式や最大 EIRP など一部の規格が異なるので注意が必要です。なお，JRL-710/720 シリーズは②2.4～2.4835GHz の帯域を使用します。
- 802.11i：米国電気電子学会 IEEE で規格化された無線 LAN のためのセキュリティ規格。
- AES：Advanced Encryption Standard の略。米国政府内での情報処理用に採用された次世代標準暗号化方式のこと。規定の基準(暗号強度，処理速度等)を満足しており，その仕様も公開されていることから広い分野で利用されています。
- ANY 接続拒否：SSID を「ANY」にセットした無線 LAN からの接続を拒否する機能。
- AP：Access Point の略。Infrastructure ネットワーク(基幹接続ネットワーク)における親局。
- CA：Certification Authority の略。電子証明書を発行する機関であり，認証局と呼ばれることもあります。
- CA Certificate：(ルート)CA 証明書。EAP-TLS や PEAP 認証において，ST が接続しようとしているネットワークが信頼できるかを確認するために使用されます。必要に応じて，ST にインポートすることで使用されます。
- Certificate：直訳すると証明書ですが，本書では特に EAP-TLS や PEAP 認証で使用する電子証明書のことを指します。
- Client Certificate：クライアント証明書。EAP-TLS 認証において，クライアントの正当性を証明(本人確認)するために使用されます。必要に応じて，無線 LAN ステーションにインポートすることで使用されます。
- CSMA：Carrier Sense Multiple Access。他の無線 LAN が送信していることを検知すると，自局は送信せず，衝突を回避する仕組み。
- Data Rate：無線区間の伝送速度。
- DHCP サーバ：ダイアルアップなどでネットワークに接続してきた機器に対して，IP アドレスを割り当てたり，ゲートウェイ・DNS サーバの IP アドレスを通知する機能を有したサーバ。
- DNS サーバ：ネットワークにおいてドメイン名を IP アドレスに変換する機能を有したサーバ。

- EAP：802.11iで使用される拡張可能な認証方式。本装置では、EAP 認証方式として、EAP-TLS と PEAP が利用可能です。
- EAP-TLS：802.11iで使用される EAP 認証方式の一つです。
無線 LAN ステーションおよび RADIUS のそれぞれが電子証明書を持つことで互いに本人確認を行います。無線 LAN ステーションには、クライアント証明書とルート CA 証明書を設定する必要があります。セキュリティ的には最も安全な EAP 認証方式ですが、証明書のメンテナンス作業が負担となります。
- FTP：ネットワークでファイルを転送するためのプロトコル。Windows のコマンドプロンプトや FTP ソフトで使用できます。
- Group Key：WPA-PSK や 802.11i の時に使用されるマルチキャストフレームを暗号化するための暗号鍵。設定により定期的に Group Key を更新することで、無線 LAN 通信のセキュリティが向上します。
- HTML：文書の論理構造や見栄えを記述するために使用される言語。この言語で記述された文書はパソコンのブラウザを用いて閲覧します。HTML はホームページの記述の他、通信機器等の設定インタフェース記述用としても用いられます。
- IAPP：Inter Access Point Protocol。同じネットワークに存在する AP 間で ST のモビリティをサポートするプロトコルです。
- Inter-Client Communication：ST 間通信。Infrastructure Mode において ST 間は、AP を経由して無線通信します。AP で Allow Inter-Client Communication を disable に選択することで、ST 間の無線通信を制限できます。設定は AP でのみ有効です。
- JavaScript：インタープリタ型のプログラム言語です。GUI 記述に用いられる HTML 言語は静的な情報しか表示できませんが、JavaScript を使用することで動的な情報を表示したり制御したりすることができます。無線 LAN 装置はモードによって動作内容が異なるため、動的に表示内容を変化させるために JavaScript を使用しています。
- MDI/MDI-X (Medium Dependent Interface/MDI-Crossover)：イーサネットポートの端子配列の種類。前者は、端子 1・2 に送信、3・6 に受信が割り当てられ、後者は端子 1・2 に受信、3・6 に送信が割り当てられています。同じ配列どうしの接続にはクロスケーブルが必要です。
- Mode：Infrastructure (基幹接続ネットワーク) と Ad Hoc Mode (アドホックネットワーク) があります。前者では有線 LAN と端末や HUB の間を無線化できます。後者は簡易的なネットワークで、無線 LAN 一台に付き一台の端末しか接続できません。無線 LAN (JRL-710/720 シリーズ) では Infrastructure のみに対応しています。
- MS-CHAPv2：802.11i で PEAP を選択した場合に使用されるクライアントのパスワード認証方式です。

- PEAP : 802.11i で使用される EAP 認証方式の一つです。
EAP-TLS 同様、無線 LAN ステーションと RADIUS が相互に認証を行います。無線 LAN ステーションはクライアント証明書かわりにパスワードを使用します。証明書のメンテナンス作業が軽減できることが特徴です。
- RADIUS : Remote Authentication Dial In User Service の略。ダイヤルアップ接続のための認証システム。802.11i では、この認証システムを無線アクセス制御のために利用しています。
- Roaming : ローミング。複数の AP が設置された環境で、ST が通信する AP を切り替えること。ST で設定します。
- RSN : Robust Security Network の略。無線 LAN のセキュリティ規格です
802.11i が提供するセキュリティ的に強固なネットワークのことです。
- RSSI : Received Signal Strength Indication の略。受信信号強度。
- RTS/CTS : Request To Send/Clear To Send。隠れ端末どうしの送信パケット衝突を軽減させる機能。設定値以上のパケット長で機能します。
- SSH : ネットワーク経由で他のパソコンにログインし通信するためのソフトウェアで、ネットワーク上でやりとりするデータを暗号化していることが特長。
- SSID : 無線 LAN に設定する ID。SSID が異なると通信しません。ASCII 文字で 1~32 文字を設定します。
- ST : STation の略。Infrastructure ネットワーク(基幹接続ネットワーク)における子局。同一 SSID の AP(親局)と無線通信します。
- TKIP : Temporal Key Integrity Protocol の略。WEP と同じく暗号アルゴリズムに RC4 を用いた暗号方式。IV(Initial Vector : 暗号コードを生成するための乱数)を 24bit から 48bit に拡張し、さらにフレーム送信ごとに生成する RC4 鍵の生成アルゴリズムを改善することで、WEP よりも暗号強度が増しています。
- VLAN : Virtual LAN。IEEE 802.1Q 準拠の標準プロトコルです。1つの物理上のネットワークを最大 4096 個の VLAN と呼ばれる仮想上のネットワークグループに分ける仕組みです。互いの VLAN を区別するために、各パケットには VLAN タグと呼ばれる特別なフィールドが設けられます。VLAN タグの付加・削除は、通常この機能を持ったスイッチングハブを用いて行います。異なる VLAN 間ではパケットの相互流入がないため、ネットワークの権限分けなどに利用されます。逆に意図的に VLAN 間でパケットをやりとりするためには、スイッチングハブを用いてルーティングさせる設定が必要になります。
- WEP : Wired Equivalent Privacy。無線区間におけるセキュリティ機能。WEP Key はデータの

暗号化に利用する暗号鍵で、長さは 40[bit]、104[bit]、128[bit]から選択できます。

- WPA-PSK：WPA は Wi-Fi Protected Access の意。PSK は PresharedKey の意。WEP に代わる新しいセキュリティ機能。JRL-710/720 シリーズでは AP と ST 双方で事前共有鍵 (Preshared Key) を設定する PSK 方式に対応しています。
- オープン認証：WEP を使用したときに認証方式の一つで、共通暗号キーを確認せずに認証する方式。暗号キーにかかわらず認証してしまうので、シェアード認証方式に比べてセキュリティ面で劣ります。
- 親局：Infrastructure ネットワーク(基幹接続ネットワーク)における AP (Access Point)。
- 隠れ端末：無線端末が互いに CSMA できない状態。
- グローバルアドレス(global address)：インターネットに接続された機器に一意に割り当てられた IP アドレス。ICANN(Internet Corporation for Assigned Names and Numbers：非営利法人)が一元的に管理しています。
- 子局：Infrastructure ネットワーク(基幹接続ネットワーク)における ST (STation)。
- シェアード認証：WEP を使用したときに認証方式の一つで、AP から乱数(チャレンジ)を送り、ST からその乱数を暗号化して返送(チャレンジレスポンス)する方式。AP でチャレンジレスポンスを復号できれば共通の暗号キーを保有していることがわかります。
- ダイバーシティ(アンテナダイバーシティ)：アンテナの受信レベルが低下した場合に対応するため、複数のアンテナを用いて受信レベルの高いアンテナを選択し、通信の品質を向上させる技術。
- 端末テーブル：AP が管理する MAC アドレスのテーブル。ST に有線接続しているパソコン等の MAC アドレスが登録されます。
- デフォルト(default)：初期値、既定値。本書では工場出荷時の設定値の意味で使用しています。
- ビーコン：通信に必要な様々な情報を通知するための制御信号。AP から定期的に送信されます。
- フラグメンテーション：送信パケットのサイズが大きい場合に、パケットを分割して送信する方法。
- プリアンブル：無線パケットの先頭部分で、同期をとるための信号。
- ブリッジテーブル：パケットの送り先を決めるために AP が管理する MAC アドレスのテーブル。無線側の無線 ST テーブルと有線側の端末テーブルで構成されます。
- ブロードキャストパケット：ネットワーク全体を意味する特殊なアドレスを指定し、不特定多数の相手に向かって送信するパケット。

- マルチキャストパケット：特定のグループを意味する特殊なアドレスを指定し、特定多数の相手に向かって送信するパケット。
- 無線 ST テーブル：AP が管理する MAC アドレスのテーブル。接続している無線 ST の MAC アドレスが登録されます。
- ユニキャストパケット：単一のアドレスを指定し、特定の相手に向かって送信するパケット。
- ローカルアドレス(local address, private address と同意)：組織内のネットワークに接続された機器に一意に割り当てられた IP アドレス。組織内で自由に割り当てることができますが、インターネット上での一意性は保証されないため、そのままではインターネットを通じて通信できません。
- ログインアカウント：無線 LAN(JRL-710/720 シリーズ)の設定を確認・変更する時の認証に使用する ID。JRL-710/720 シリーズでは「admin」、「user」および「diag」の 3 つの ID が用意されています。

付録1 パソコンの IP アドレスの変更

Windows パソコンで IP アドレスを変更する場合、次のように設定します。なお詳細な設定方法については、Windows またはお使いの NIC (Network Interface Card) の取扱説明書を参照してください。

ここでは Windows XP Home Edition を搭載したパソコンに IP アドレス「192.168.1.100」を設定する例を示しています。無線 LAN 装置の IP アドレスと重複せず、かつ同一のネットワークセグメントに属する値を設定する必要があります。なお工場出荷時状態の無線 LAN 装置の IP アドレスは「192.168.1.1」となっています。

[スタートメニュー] → [設定] → [コントロールパネル] を開き、[ネットワーク接続] アイコンをダブルクリックします。

- ① [ローカルエリア接続] (ご利用のパソコンによって、名称が異なることがあります。) アイコンをダブルクリックします。
- ② 「ローカルエリア接続」「全般タブ」の [プロパティ] をクリックします。次の画面の前端タブの「インターネットプロトコル(TCP/IP)」を選択(クリック)し、[プロパティ] をクリックします。
- ③ 「全般」タブの中で、「次の IP アドレスを使う(S)」を選択し、IP アドレス、サブネットマスクの各欄に値を入力します。
(IP アドレスに「192.168.1.100」、サブネットマスクに「255.255.255.0」を入力し、[OK] をクリックします。)
※ 無線 LAN の設定時には、WINS やゲートウェイ等の設定は必要ありません。
- ④ 最後に、「インターネットプロトコル(TCP/IP)」のプロパティ画面を閉じ、「ローカルエリア接続」のプロパティ画面も [OK] をクリックし閉じます。
※ 設定の反映に時間がかかることがあります。
- ⑤ 「ローカルエリア接続」のプロパティ画面の [OK] をクリックすると設定した IP アドレスが有効になります。

【備考】

- Windows 98SE/ME では、IP アドレスを変更するとパソコンの再起動を要求されます。表示されるメッセージに従って、パソコンを再起動してください。
- 「付録2 パソコンの IP アドレスの確認」に従って正しく IP アドレスが設定変更されたことを確認してください。

付録2 パソコンの IP アドレスの確認

パソコンの IP アドレスは、Windows の “ipconfig” コマンドや “winipcfg” コマンドで確認できます。

- Windows NT/2000/XP の場合

【スタートメニュー】 から 【プログラム】 → 【アクセサリ】 → 【コマンドプロンプト】 を選択し、コマンドプロンプト画面で、“ipconfig” と入力します。

```
C:\>ipconfig
Windows IP Configuration

Ethernet adapter ローカル エリア接続:
    Connection-specific DNS Suffix . : 
    IP Address . . . . . : 192.168.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

上記例では、ローカルエリア 接続に、IP アドレス＝「192.168.1.100」、サブネットマスク＝「255.255.255.0」が設定されていることを示しています。

【備考】

WindowsXP の場合、パソコンが LAN ケーブルで正しく接続されていないと、上記値は表示されず、「Media State : Media Disconnected」と表示されます。

- Windows 98SE/ME の場合

【スタートメニュー】 から 【プログラム】 → 【アクセサリ】 → 【MS-DOS プロンプト】 を選択し、MS-DOS プロンプト画面で、“winipcfg” と入力します。

```
C:\>winipcfg
```

下記ウィンドウが開き、使用しているネットワークアダプタを選択すると IP アドレスが確認できます。適切に設定できていない場合は、再度設定してください。



付録3 接続の確認(ping コマンド)

無線 LAN 装置は有線・無線 LAN からの ping 要求パケットに対し応答を返します。これを利用して設定用パソコンから“ping”コマンドを発行することで設定用パソコンと無線 LAN 装置間の LAN 接続が正常かどうか確認することができます。“ping”コマンドを発行するには、[スタートメニュー] から [プログラム(P)] → [アクセサリ] → [コマンドプロンプト] を選択し、コマンドプロンプト画面で“ping 192.168.1.1”を実行します。

[備考]

「192.168.1.1」は無線 LAN 装置のデフォルト IP アドレスです。IP アドレスを変更している場合は、適宜読みかえてください。

正しく LAN 接続されていると次のように無線 LAN 装置からの応答が得られます。

```
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=10ms TTL=64
Reply from 192.168.1.1: bytes=32 time<10ms TTL=64
Reply from 192.168.1.1: bytes=32 time<10ms TTL=64
Reply from 192.168.1.1: bytes=32 time<10ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

無線 LAN 装置からの応答が得られない場合、次のように表示されます。このような場合には無線 LAN 装置の「E-LINK」が点灯していることや、パソコンの IP アドレスの確認等を行って接続し直します。

```
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

“ping”コマンドへの応答があった場合、コマンドプロンプトで“arp -a”を実行すると無線 LAN 装置の MAC アドレスが確認できます。

```
C:\>arp -a

Interface: 192.168.1.100 on Interface1:
Internet Address      Physical Address      Type
192.168.1.1           00-00-27-3e-00-01     dynamic
```

“ping”の応答がなかった場合には次のような表示になります。

```
C:\>arp -a

No ARP Entries Found
```

付録4 1 台のパソコンで、連続して無線 LAN を設定する

1 台のパソコンで連続して無線 LAN 装置を設定しようとする時、2 台目以降の無線 LAN 装置にログインできなくなることがあります。これは設定に使用するパソコンが IP アドレスに対応する機器の MAC アドレスを ARP テーブルと呼ばれる形式で記憶しているためです。この場合パソコンの ARP テーブルを削除することで記憶が初期化され、次の無線 LAN 装置にログインできるようになります。

機器	IP アドレス	MAC アドレス
無線 LAN1	192.168.1.1	00:00:27:3e:00:01
無線 LAN2	192.168.1.1	00:00:27:3e:00:02

IP アドレスと対応する MAC の例

上記のような工場出荷時状態の 2 台の無線 LAN 装置を続けて設定する場合、無線 LAN1 を設定した直後のパソコンの ARP テーブルは次のようになっています (ARP テーブルを確認するにはコマンドプロンプトから “arp -a” と入力します)。

C:\>arp -a		
Interface: 192.168.1.254 on Interface 1		
Internet Address	Physical Address	Type
192.168.1.1	00-00-27-3e-00-01	dynamic

この状態では 2 台目の無線 LAN 装置にアクセスできません。これはパソコンが「192.168.1.1」の機器の MAC アドレスを「00:00:27:3e:00:01」であると記憶しているためです。この記憶を ARP テーブルから削除します (ARP テーブルを削除するには「arp -d IP アドレス」と入力します)。

```
C:\>arp -d 192.168.1.1
```

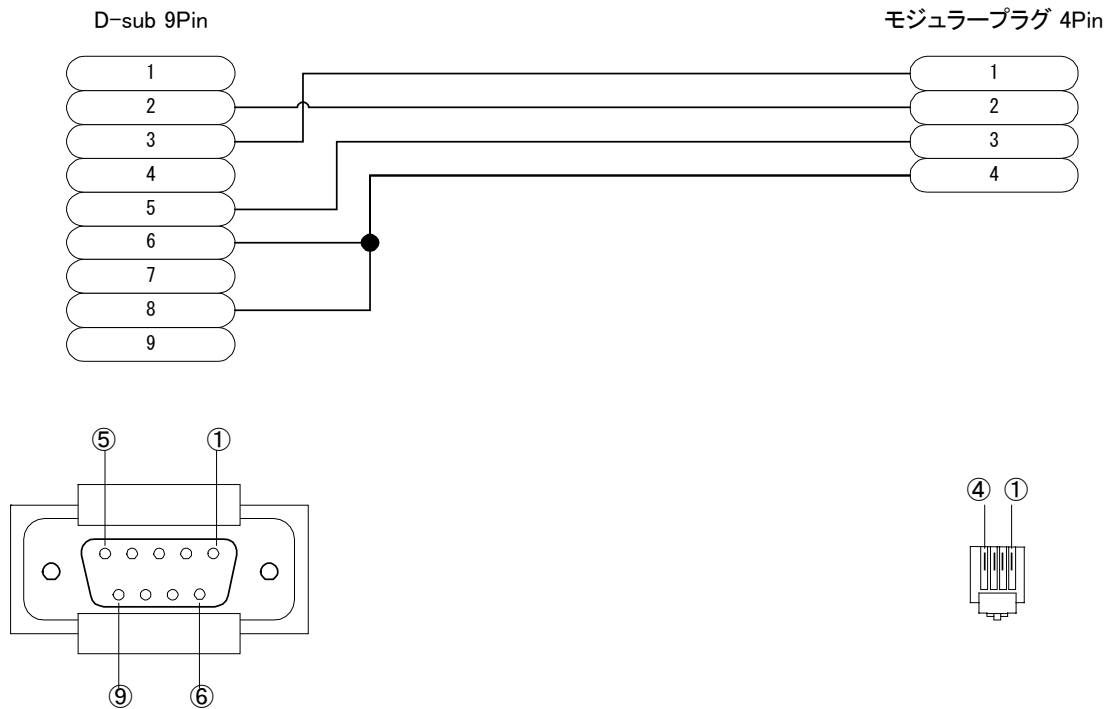
全ての ARP テーブルが削除されると「No ARP Entries Found」と表示されます。

```
C:\>arp -a
No ARP Entries Found
```

記憶が消去された状態でパソコンから「192.168.1.1」にアクセスしようすると、パソコンは未知の IP アドレス「192.168.1.1」に対応する機器を改めて調査するので 2 台目の無線 LAN 装置にアクセス可能となります。

付録5 専用シリアルケーブル配線図

設定用シリアルケーブルの配線図を示します。パソコン側が「D-sub 9pin」、無線 LAN 側が「モジュラープラグ」になります。



パソコンの COM ポートは、下記内容に設定してください。

設定項目	設定値
速度[bps]	115,200
データビット	8
パリティ	なし
ストップビット	1
フロー制御	なし

【備考】

D-sub 9Pin コネクタは、ヒロセ電機 HDEB-9S 相当。

モジュラープラグは、ヒロセ電機 TM4P-44P 相当。

付録6 セキュリティの設定

無線 LAN 装置では、いくつかのセキュリティに関連する設定が可能です。以下に要点を記載しますので、システム運用上の必要性に応じて設定を変更してください。

- SSID の変更

第三者が類推しにくく、かつ管理に便利な SSID を書き込むのが原則です。システム名、場所名、管理者名などをローマ字表記で織り込む例が多いようです。

- 暗号化機能の使用

データの漏洩を防ぐため、暗号化機能を有効にして使用してください。

暗号方式 WEP, WPA-PSK, 802.11i のうち、どれか1つを選択します。

暗号方式には 3 種類ありますが、WEP < WPA-PSK < 802.11i の順に、後者になるほど強度が増します。但し 802.11i については RADIUS サーバの設置等、運用準備が別途必要になります。WPA-PSK と 802.11i については、さらに TKIP と AES のいずれかが選択可能です。TKIP よりも AES の方が暗号強度が高いと言われています。

AP と ST の暗号方式は同じものを選択する必要があります。

WPA-PSK を設定する場合、パスフレーズとして次のような設定を推奨します。

- ・なるべく辞書に載っている単語を使わない
- ・無意味な英数字と記号を適宜組み合わせる
- ・文字数を少なくとも 13 文字以上、できれば 20 文字以上とする

- Windows XP パソコンとの WEP 通信について

他社製無線 LAN カードを接続した Windows XP パソコンに「Wi-Fi Protected Access (WPA) アップデート (815485)」パッチを適用すると、WEP での動作に支障が出る不具合が Microsoft 社から報告されています（「Q815485」適用後 WEP キーを使用してアクセスポイントに接続できなくなる）。

WPA 対応パッチ適用後、AP との WEP 通信に支障が出る場合には、

- ・ WEP を使用しない。暗号化なし、あるいは WPA-PSK を使用する。
 - ・パッチ「Q815485」を Microsoft 社指示に従ってアンインストールし、WEP を使用する。
- のいずれかを選択願います。

- MAC アドレスフィルタリングの使用

ネットワークへの不正侵入を避けるため、特定の通信相手以外の接続を許可しない設定にしてください。

- パスワードの変更

ご購入後、直ちに變更してください。変更後の内容を忘れないよう、メモをとって管理してください。

- ホストへのアクセス制限

管理者以外のユーザからのアクセスを許可しないように設定してください。

- ST 間通信

必要に応じて設定してください。

- ビーコン信号の SSID 情報

システム運用上問題ない場合は、ビーコン信号に SSID 情報を含まないよう設定してください。

付録7 WEP キー設定のヒント

使用する WEP Key は、送信する無線 LAN に設定されている WEP Key No. で決定します。受信する無線 LAN の、該当する WEP Key が同じでないと受信しません。一般に、端末間の通信は双方向にパケットをやり取りするので、それぞれの WEP Key No. には同じ WEP Key を設定します。

WEP Key No. ごとに、同一の WEP Key を設定した場合

AP		ST	
Key No.	WEP Key	Key No.	WEP Key
1	◎	1	◎
2	△	2	△
3	□	3	□
4	◇	4	◇

上記のように WEP Key を設定した場合、AP でも ST でも任意の WEP Key No. を選択できます。

WEP Key No. ごとに、異なる WEP Key を設定した場合

AP		ST	
Key No.	WEP Key	Key No.	WEP Key
1	◎	1	◎
2	△	2	△
3	□	3	◇
4	◇	4	□

上記のように WEP Key を設定した場合、相互に通信する組み合わせは下記の通りです。

		ST の WEP Key No.			
		1	2	3	4
AP の Key No.	1	○	○	×	×
	2	○	○	×	×
	3	×	×	×	×
	4	×	×	×	×

WEP Key No. ごとに、異なる WEP Key を設定した場合

AP		ST1		ST2	
Key No.	WEP Key	Key No.	WEP Key	Key No.	WEP Key
1	◎	1	◎	1	◎
2	△	2	△	2	△
3	□	3	◇	3	▽
4	◇	4	□	4	◇

上記のように WEP Key を設定した場合、相互に通信する組み合わせは下記の通りです。

		ST1 の Key No.				ST2 の Key No.			
		1	2	3	4	1	2	3	4
AP の Key No.	1	○	○	×	×	○	○	×	○
	2	○	○	×	×	○	○	×	○
	3	×	×	×	×	×	×	×	×
	4	×	×	×	×	○	○	×	○

[備考]

ST1 と ST2 の間は AP を経由して通信するため、ST 間の WEP Key や WEP Key No. は考慮する必要はありません。

付録8 MAC アドレスフィルタの設定

MAC アドレスフィルタリング機能は、無線接続相手の MAC アドレスを登録することで接続の制限(フィルタリング)をかける機能です。

フィルタリングできる MAC アドレスは、実際の無線接続で使用される MAC アドレスです。フィルタしたい相手機器が MAC アドレスを2つ(有線 MAC と無線 MAC)持っている場合には、無線 MAC アドレスを登録してください。以下、設定の詳細を説明します。

下記例は MAC アドレスフィルタリング機能を有効(ACL Mode : enable)にした場合で、無線 LAN 「0000273e1xxx」, 「0000273e21xx」の接続を許可し、無線 LAN 「0000273e3xxx」および特定の MAC アドレス「34567890abcd」は接続を許可しない条件を登録しています。

ACL Mode: enable

リスト No.	許可(allow)／不許可(deny)	MAC アドレス	ビットマスク
1	allow (1)	0000273e1000	ffffffffff000
2	allow (1)	0000273e2100	ffffffffffff00
3	deny (2)	0000273e3000	ffffffffffff00
4	deny (2)	34567890abcd	ffffffffffffff

新規に接続相手が発生した場合、接続相手の MAC アドレスをリストの上から順番に評価し、該当する条件で接続の許可または不許可が実行されます。

MAC アドレスフィルタリング機能が無効の場合(ACL Mode : disable)、デフォルトで全ての接続が許可されます。それに対して MAC アドレスフィルタリング機能が有効の場合(ACL Mode : enable)、リストに存在しない MAC アドレスはデフォルトで拒否されます。

従って MAC アドレスフィルタリング機能有効時で新規の接続相手の MAC アドレスが「0123456789ab」の場合、リスト 1～4 のいずれにも該当せず、接続が拒否されます。

付録9 APが無線送信する条件

APは接続された端末のMACアドレスを管理しています。APに無線接続したSTは「無線STテーブル」に、無線STに有線接続された端末は「端末テーブル」に登録されます。

「無線STテーブル」に無線STのMACアドレスが登録されるのは、STがAPにアソシエートした時です。

「端末テーブル」にSTに有線接続された端末のMACアドレスが登録されるのは、端末が何らかの packets を送出し、APに届いた時です。

APは宛先が「端末テーブル」に登録されたパケットと、ブロードキャスト・マルチキャストを無線回線に送出します。宛先が「端末テーブル」に登録されていないユニキャストは無線送信しません。

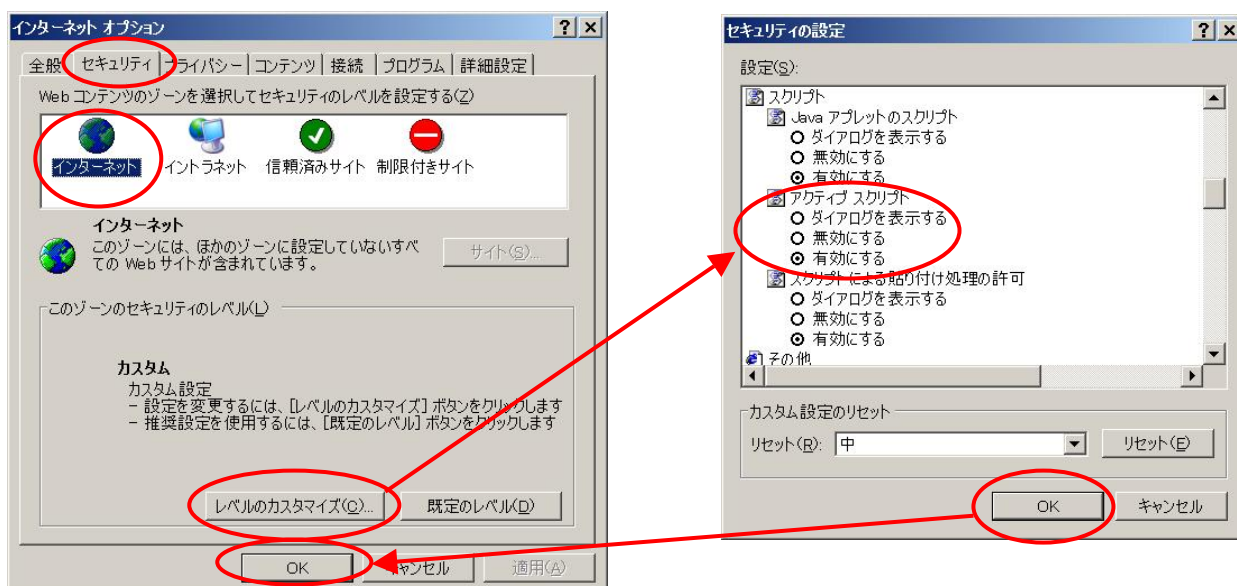
APを再起動したり、STが別のAPに接続した時(ローミングした時)は、一時的に通信が途切れることがあります。この場合は、ST側から何らかの packets を送出することで「端末テーブル」が更新され通信するようになります。

付録10 WEB ブラウザの一時ファイル(キャッシュ)設定

● ブラウザ JavaScript 設定の有効化

無線 LAN 装置の GUI(グラフィカル・ユーザ・インタフェース)機能は、動作モードに応じて設定画面を変化させるため、JavaScript と呼ばれるスクリプト言語を用いて記述してあります。これに合わせてパソコンの WEB ブラウザ設定でも JavaScript を有効にする設定を選択する必要があります。WEB ブラウザの JavaScript 設定はデフォルトで有効ですが、セキュリティレベル設定によっては無効が選択されていることがあります。

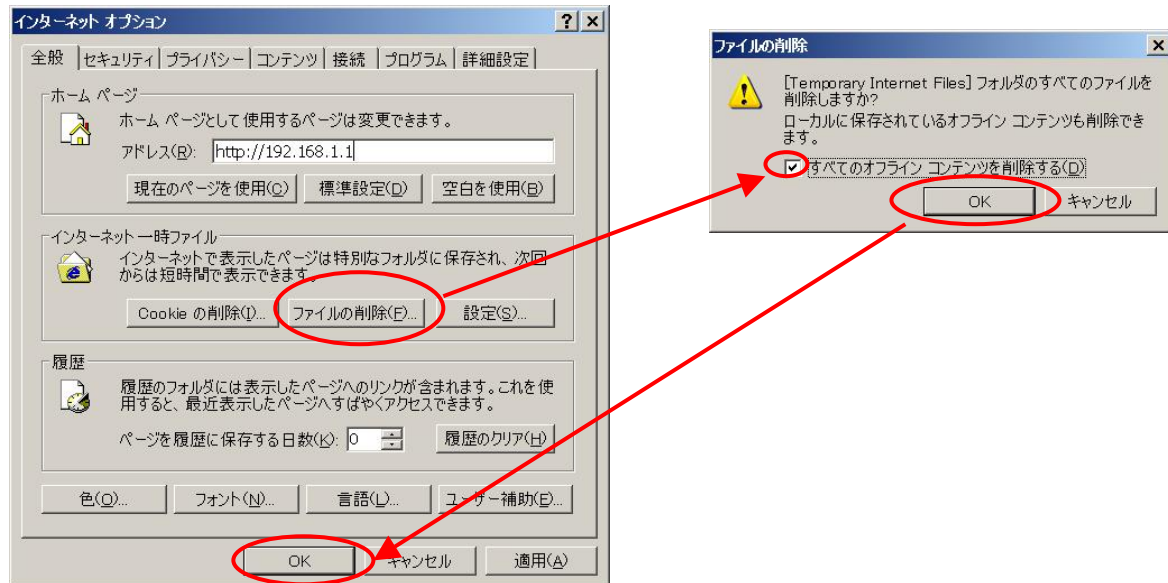
JavaScript を有効にするには次のように設定を行います。Microsoft 社 Internet Explorer 6.0 の場合、[ツール] ⇒ [インターネット オプション] ⇒ [セキュリティ] タブを選択した画面で[Web コンテンツのゾーン]から[インターネット]を選択し、[レベルのカスタマイズ]をクリックします。ここで現れる[セキュリティの設定]画面上で、[アクティブスクリプト]の項目を[有効にする]に選択した上で[OK]をクリックします。さらに[インターネットオプション]の画面でも「OK」をクリックします。



● インターネット一時ファイル(キャッシュ)の削除

無線 LAN 装置 GUI が用いる JavaScript 及び HTML 記述の内容は無線 LAN のソフトリリースによって異なります。これはリリース毎に機能が異なり、機能に合わせて GUI の表示内容・動作が異なるためです。このため一台のパソコンで異なるリリースの無線 LAN を連続して設定しようとする、WEB ブラウザの一時ファイル(キャッシュ)に以前用いたリリース用の JavaScript が残っていて期待した動作とならないことがあります。このような場合は、一時ファイル(キャッシュ)をクリアすることで正しく表示・設定されるようになります。

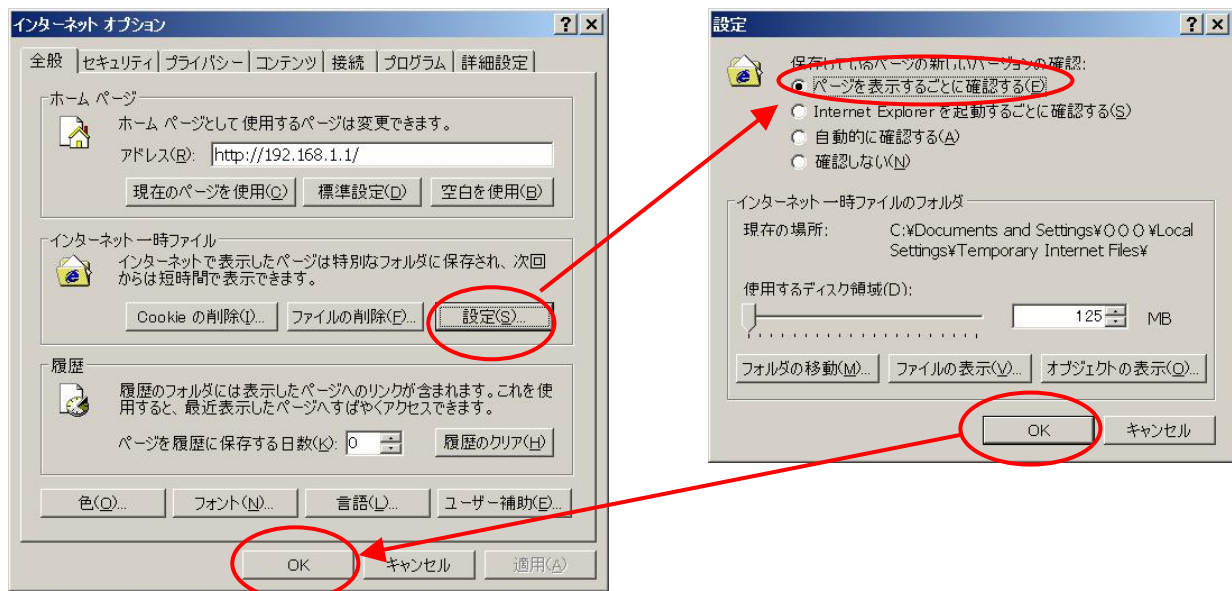
一時ファイル(キャッシュ)をクリアするには次のように設定します。Microsoft 社 Internet Explorer 6.0 の場合、[ツール] ⇒ [インターネットオプション] タブを選択した画面上で[インターネットの一時ファイル]の[ファイルの削除]をクリックし、[すべてのオフラインコンテンツを削除する]にチェックを入れた上で[OK]をクリックします。さらに[インターネットオプション]の画面でも[OK]をクリックします。この状態で再度無線 LAN にアクセスして画面を更新(再読み込み)してください。



- 一時ファイル(キャッシュ)を参照しないようにする

異なるリリースの無線 LAN 装置を設定しようとするたびに一時ファイル(キャッシュ)をクリアするのは煩雑です。このような場合、一時ファイルの扱い方を変更することで自動的に最新の内容が参照されるようになります。

保存したページを参照せず、常に新しいページを参照させるには次のように設定します。Microsoft 社 Internet Explorer 6.0 の場合、[ツール]⇒[インターネットオプション]タブを選択した画面上で、[インターネットの一時ファイル]の[設定]をクリックして設定画面を出し、[保存しているページの新しいバージョンの確認]を[ページを表示するごとに確認する]に選択した上で[OK]をクリックします。さらに[インターネットオプション]の画面でも[OK]をクリックします。



上記「ページを表示するごとに確認する」設定を行った場合、無線 LAN 装置以外の、例えばインターネット上の一部の WEB ページの表示が遅く感じられる場合があります。これは該当ページを表示するのに必要な全てのデータを、ブラウザの一時ファイルを用いなくて、全てインターネット上から取得しようとするためです。体感上の遅さを改善したい場合には「自動的に確認する」設定を選択した上で、前述の一時ファイル(キャッシュ)の削除手順を併用されるようお勧めします。

付録11 WEB ブラウザのプロキシ設定の変更

プロキシサーバが存在するネットワーク環境で使用しているパソコンを無線 LAN アダプタの設定に使用するとき、以下の設定をしてください。

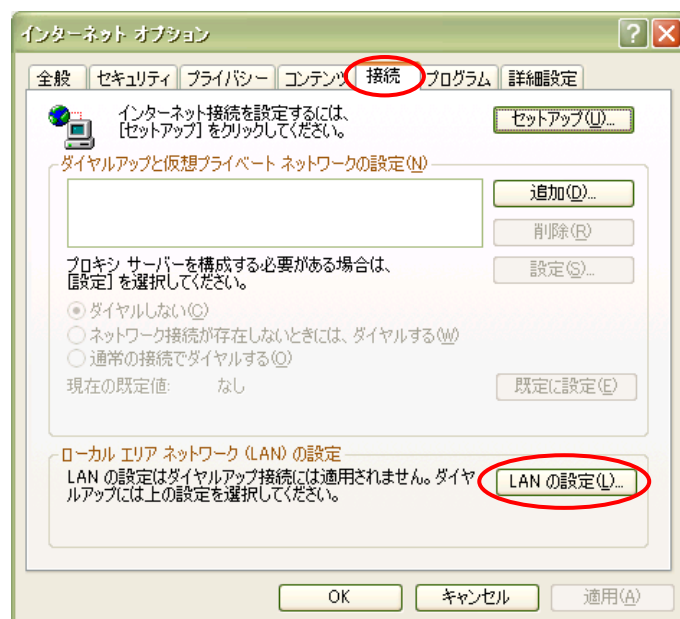
Internet Explorer 6.0 の場合

Internet Explorer を起動します。

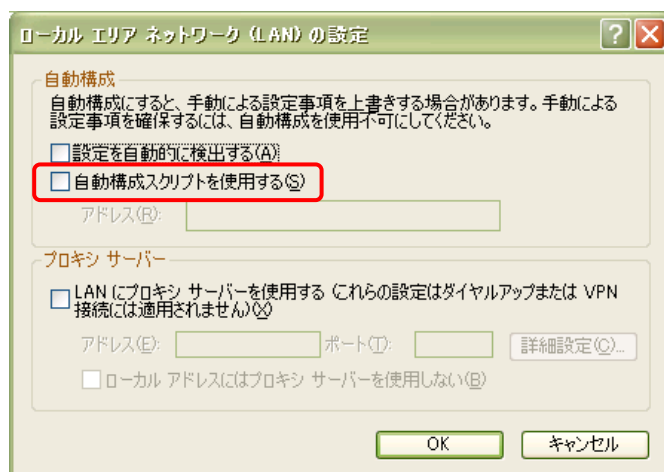
- ① ブラウザのメニューから [ツール(T)] → [インターネットオプション(O)] をクリックします。



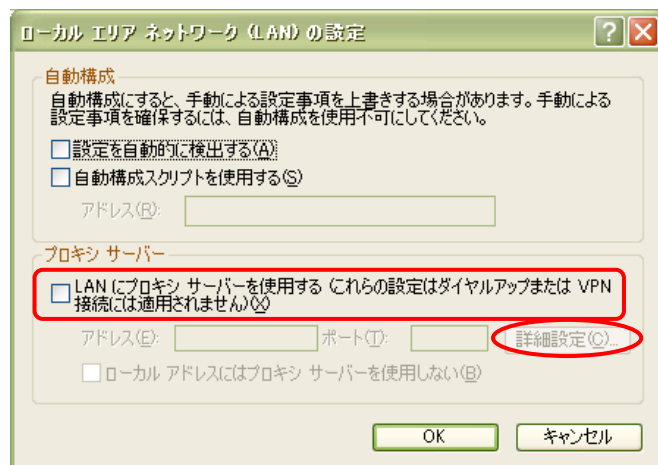
- ② インターネットオプション画面で、[接続] タブをクリックし、[LAN の設定(L)] をクリックします。



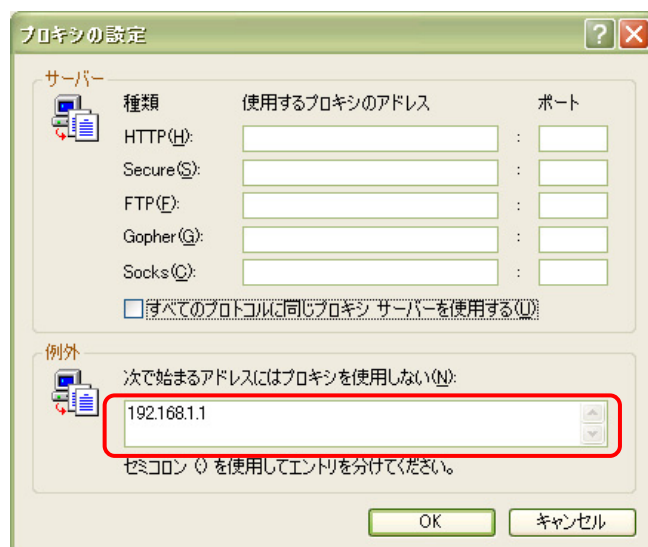
- ③ 「設定を自動的に検出する(A)」、「自動構成スクリプトを使用する(S)」がチェックされているときは、チェックをはずします。



- ④ 「設定を自動的に検出する(A)」がチェックがなく、「LANにプロキシサーバーを使用する(X)」がチェックされている時は、[詳細設定(C)] をクリックします。



- ⑤ 「次で始まるアドレスにはプロキシを使用しない(N)」の入力欄に、本装置の IP アドレス(工場出荷時は 192.168.1.1)を入力し、[OK] をクリックします。



付録12 パケットフィルタの設定手順

パケットフィルタは、ある特定種類のパケットを遮断するためのものです。無線 LAN 装置内で有線から無線に、あるいは無線から有線にパケットが転送される際、指定されたパケットを遮断します。パケット種類を指定するためには設定ファイルを用意する必要があります。設定ファイルの記述にあたっては linux に関する前提知識が必要になります。以下の手順で設定します。

(ア) 有線 LAN 接続する

無線 LAN 装置・パソコンの IP アドレスを確認した上で、両者を有線 LAN 接続します。E-Link の LED 等を用いて無線 LAN 装置とパソコンが正しく接続されていることを確認してください。接続にあたっては HUB 等が必要になる場合があります。

(イ) コマンドプロンプト(DOS 窓)を準備する

Windows パソコン上でコマンドプロンプトを起動します。

[スタートメニュー] → [すべてのプログラム] → [アクセサリ] → [コマンドプロンプト] をクリックするとコマンドプロンプトが表示されます。

上記手順でコマンドプロンプトが起動しない場合、次の手順を実行してみてください。

【Windows98SE/Me の場合】

[スタートメニュー] → [ファイル名を指定して実行] 画面から command コマンドを実行する。

【WindowsNT/2000/XP の場合】

[スタートメニュー] → [ファイル名を指定して実行] 画面から cmd コマンドを実行する。

① 設定ファイルを ftp 転送する

例えば次のようなフィルタ用設定ファイル iptables.conf を準備して ftp 転送します。

フィルタ設定の一例： 特定の MAC(00:00:27:11:22:33)宛のパケットを透過させない。

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A FORWARD -m dmac --mac-dest 00:00:27:11:22:33 -j DROP
COMMIT
```

- パケットフィルタは FORWARD (ブリッジング動作、つまり無線から有線へ、あるいは有線から無線へのパケット転送)動作に対してのみ適用可能です。INPUT, OUTPUT へのフィルタリングは内部予約であり、動作保証しておりません。
- FORWARD のデフォルトポリシーは ACCEPT で設定してください。
- 「iptables.conf」はファクトリリセットの対象外です。設定を元に戻す場合はパケットフィルタのクリア(「4.13.1 フィルタパケットリスト消去[Clear All Filter Setting]」参照)を実行してください。
- フィルタ設定記述は linux 標準の iptables コマンドに準拠しています。iptables 参照ファイルの記述フォーマットについては linux に関する各種解説書を参照ください。

設定ファイルをアスキーモードで ftp 転送します。コマンドプロンプトから実行します。

<pre> C:\> ftp 192.168.1.1 Connected to 192.168.1.1. 220 jrlx00 FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready. User (192.168.1.1:(none)): admin 331 Password required for admin. Password: 230 User admin logged in. Hash mark printing On ftp: (2048 bytes/hash mark) . ftp> ascii 200 Type set to A. ftp> put iptables.conf 150 Opening ASCII mode data connection for 'iptables.conf'. 226 Transfer complete. ftp: **bytes sent in **Seconds **Kbytes/sec. ftp > bye </pre>	<p>ftp [設定先 IP アドレス]</p> <p>ユーザ名「admin」と入力</p> <p>パスワードを入力</p> <p>“ascii”と入力</p> <p>“put iptables.conf”と入力</p> <p>ftp 接続を切断</p>
--	---

- ここでは転送する設定ファイルが C：ドライブ直下に置いてあるものとして説明しています。
- ここでは無線 LAN 装置の IP アドレスが 192.168.1.1 であるものとして説明しています。
- ここでアスキーモードで転送しているのは、改行コードの自動変換を機能させるためです。
- 設定ファイルのファイル名は iptables.conf と決められています。これ以外の名前のファイルを ftp 転送してもパケットフィルタは機能しません。

(ウ) 無線 LAN 装置をリブートさせる

設定を反映させるために無線 LAN 装置をリブート再起動します。

リブート再起動後、設定ファイルに記述した内容が実動作に反映されます。

付録13 有線 MAC アドレスと無線 MAC アドレス

本装置は無線側、有線側それぞれに別個の MAC アドレスを持っています。

本装置で診断機能を立ち上げ、“mti” コマンドを実行することで、それぞれの MAC アドレスを確認できます。

有線接続している PC から “arp” コマンド等でリンクしている機器を表示させた場合は、MAC アドレスとして有線 MAC アドレスが表示されます。

AP 動作している本装置で “stlist” コマンドを実行すると、無線リンクしている ST の無線 MAC アドレスが一覧表示されます。

MAC アドレスフィルタを設定する場合は、対向する JRL-710/720 シリーズの無線 MAC アドレスを登録します。

無線 MAC アドレスと有線 MAC アドレスは下記の規則で割り当てられています。

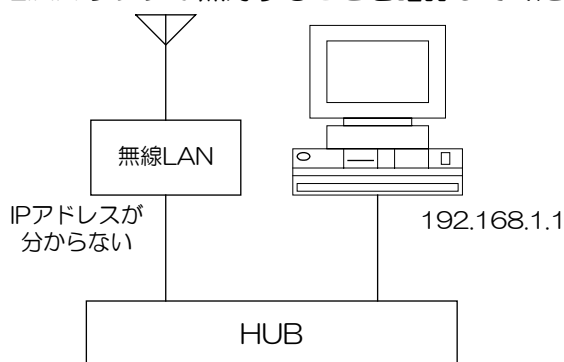
有線 MAC アドレス：00-00-27-3e-○?-?? 「○」は必ず偶数(0, 2, 4, 6, 8, a, c, e)

無線 MAC アドレス：00-00-27-3e-△?-?? 「△」は「○」に 1 を加えた数(1, 3, 5, 7, 9, b, d, f)

付録14 設定した IP アドレスを忘れてしまったら

無線 LAN に設定した IP アドレスは、無線 LAN にログインして mti コマンドを実行することで確認できます。IP アドレスを忘れてしまいログインできない場合は、下記の方法を試してください。

- ① パソコンの IP アドレスを「192.168.1.1」に設定し、図のように無線 LAN とパソコンを HUB に接続します。HUB の LINK ランプが点灯することを確認してください。



- ② 端末の ARP テーブルを確認します。コマンドプロンプトから “arp -a” と入力してください。

```

C:\>arp -a
Interface: 192.168.1.1 on Interface 1
Internet Address    Physical Address    Type
192.168.1.100      00-11-22-33-44-55   dynamic
192.168.1.200      00-66-77-88-99-00   dynamic
  
```

- ③ ARP テーブルがある場合は、全て削除してください。表示された全ての IP アドレスに対して “arp -d (IP アドレス)” と入力します。

```

C:\>arp -d 192.168.1.100
  
```

- ④ ARP テーブルが全て削除されたことを確認してください。「No ARP Entries Found」と表示されます。

```

C:\>arp -a
No ARP Entries Found
  
```

- ⑤ 無線 LAN の電源を切り、再び電源を投入します。

- ⑥ パソコンの ARP テーブルを確認すると、無線 LAN の IP アドレスが分かります。“arp -a” と入力します。

```

C:\>arp -a
Interface: 192.168.1.1 on Interface 1
Internet Address    Physical Address    Type
192.168.1.234      00-00-27-0e-dc-ba   dynamic
  
```

この例の場合、無線 LAN の IP アドレスは「192.168.1.234」と分かります。もし ARP テーブルに新規追加されていない場合、無線 LAN 自身が 192.168.1.1 の可能性があります。

付録15 MIB

本装置が対応する MIB (Management Information Base) を以下に示します。

<MIB-II> OID { . 1. 3. 6. 1. 2. 1. 2. 2. 1. *}

オブジェクト名称	OID	説明
ifIndex	1	各 I/F に 1 から順に割り振られた一意の値
ifDescr	2	各 I/F の説明
ifType	3	I/F の種類
ifMtu	4	MTU 値
ifSpeed	5	現在の帯域幅の見積 (ビット/秒)
ifPhysAddress	6	物理アドレス (MAC アドレス)
ifAdminStatus	7	I/F の要求状態 (up, down, testing)
ifOpenStatus	8	現在の I/F の操作状態 (up, down, testing)
ifInOctets	10	受信オクテット総数
ifInUcastPkts	11	上位層に渡したパケット数 (M, B-CAST 除く)
ifInErrors	14	エラーで破棄された入力パケット数
ifOutOctets	16	不明または非サポートで破棄された出力パケット
ifOutUcastPkts	17	上位層から渡されたパケット数 (M, B-CAST 除く)
ifOutDiscards	19	エラーではないのに破棄された出力パケット数
ifOutErrors	20	エラーで破棄された出力パケット数
ifOutQLen	21	出力パケットキューの長さ (パケット数単位)
ifSpecific	22	I/F に固有な MIB 定義への参照

<802.11> OID { . 1. 2. 840. 10036. *}

オブジェクト名称	OID	説明
dot11StationID	1. 1. 1. 1	監視装置の MAC アドレス
dot11DesiredSSID	1. 1. 1. 9	監視装置の ESSID
dot11RTSThreshold	2. 1. 1. 2	RTS/GTS 起動用しきい値
dot11ManufacturerName	2. 1. 1. 8	"Japan Radio Co., Ltd."
dot11ProductID	2. 1. 1. 9	監視装置の製造番号
dot11MulticastTransmittedFrameCount	2. 2. 1. 2	無線送信したマルチキャストフレーム数
dot11FailedCount	2. 2. 1. 3	無線送信で失敗したフレーム数
dot11RetryCount	2. 2. 1. 4	無線再送した回数
dot11ReceivedFrameCount	2. 2. 1. 10	無線受信した総フレーム数
dot11MulticastReceivedFrameCount	2. 2. 1. 11	無線受信したマルチキャストフレーム数
dot11FCSErrorCount	2. 2. 1. 12	無線受信時 FCS エラーフレーム数
dot11TransmittedFrameCount	2. 2. 1. 13	無線送信した総フレーム数
dot11ManufacturerProductName	3. 1. 2. 1. 3	"JRL-710"
dot11DiversitySupport	4. 2. 1. 2	アンテナダイバーシティ ON/OFF
dot11CurrentChannel	4. 5. 1. 1	使用中の周波数チャネル

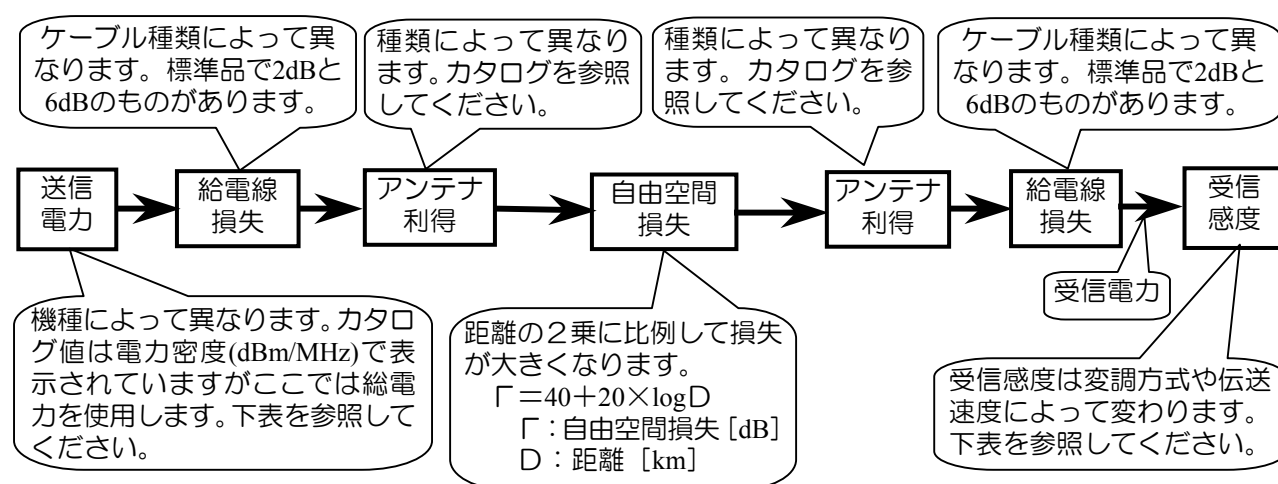
付録16 無線LANの簡易回線設計

無線 LAN を利用して屋外長距離通信システムを構築するときは回線設計が必要です。回線設計とはある2点間で通信するときに必要な無線諸元(送信出力やアンテナ利得など)を計算することです。設計する上では、電波伝搬損失(自由空間損失、遮蔽損失、媒体損失、回折損失など)や干渉波強度(他波干渉、自波干渉、雑音など)など多くの項目を考慮しなければなりません。

ここでは、伝搬損失は自由空間損失のみで干渉波がないものとした回線設計例を示しますので、通信距離の想定や現場で測定した RSSI の適否の判断に利用してください。

(1) 電波伝搬系統

まず、電波伝搬系統を想定し、送信機の出力がアンテナや空間を通して受信機に到達したときに、所要受信電力(受信感度+マージン)以上になるかを確認します。



(2) 受信電力の計算

受信電力は次の式で計算できます。

$$\text{受信電力} = \text{送信電力} - \text{給電線損失} + \text{アンテナ利得} - \text{自由空間損失} + \text{アンテナ利得} - \text{給電線損失}$$

(3) 適否の判断

計算した受信電力が受信感度より十分大きいことが要求されます。一般的には6~10dBのマージンを見ます。自由空間以外の損失や干渉波の存在が想定されるときはマージンをさらに大きくします。

無線LANの送信電力

変調方式	DSSS(11b)			OFDM(11g)		
電力密度	1mW/MHz	2mW/MHz	8mW/MHz	1mW/MHz	2mW/MHz	8mW/MHz
電力密度	0dBm/MHz	3dBm/MHz	9dBm/MHz	0dBm/MHz	3dBm/MHz	9dBm/MHz
総電力	10 dBm	13 dBm	19 dBm	12 dBm	15 dBm	21 dBm

無線LANの受信感度(PE R=10⁻²相当/パケット長 1,000Bytes)

変調方式	DSSS(11b)				OFDM(11g)								
伝送速度	Mbps	1	2	5.5	11	6	9	12	18	24	36	48	54
受信感度	dBm	-90	-87	-85	-82	-82	-81	-79	-77	-74	-70	-66	-65

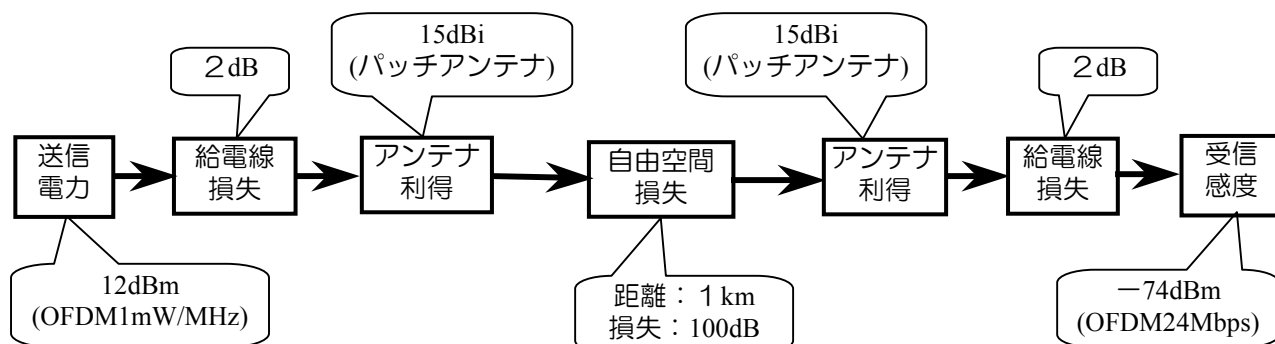
(4) 計算例

下図の諸元で計算します。

受信電力は

$$\begin{aligned} \text{受信電力} &= 12\text{dBm} - 2\text{dB} + 15\text{dBi} - 100\text{dB} + 15\text{dBi} - 2\text{dB} \\ &= -62\text{dBm} \end{aligned}$$

となり、OFDM24Mbps のときの受信感度 -74dBm に比べて 12dB のマージンがあるので、回線が成立することがわかります。



2.4GHz 帯の自由空間損失

通信距離 (m)	1	10	20	50	100	200	500	1k	2k	5k	10k	20k
自由空間損失 (dB)	40	60	66	74	80	86	94	100	106	114	120	126

【備考】

無線 LAN の出力は、電波法で 10mW/MHz ($=10\text{dBm/MHz}$) 以下と電力密度 (1MHz 当たりの電力) で規定されていますが、アンテナ利得と給電線損失を含めた EIRP (Equivalent Isotropic Radiated Power 等価等方放射電力) の規定もあります。EIRP はアンテナの指向角によって最大規定値が変化し、次の式で表されます。

$$\text{EIRP} \leq 12.14\text{dBm/MHz} + 10 \times \log A$$

A は $360^\circ \div$ 指向角で、10 を越えるときは 10 とする。

無指向性アンテナのときは $\text{EIRP} \leq 12.14\text{dBm/MHz}$ になり、指向角が 36° 以下のアンテナのときは $\text{EIRP} \leq 22.14\text{dBm/MHz}$ になります。

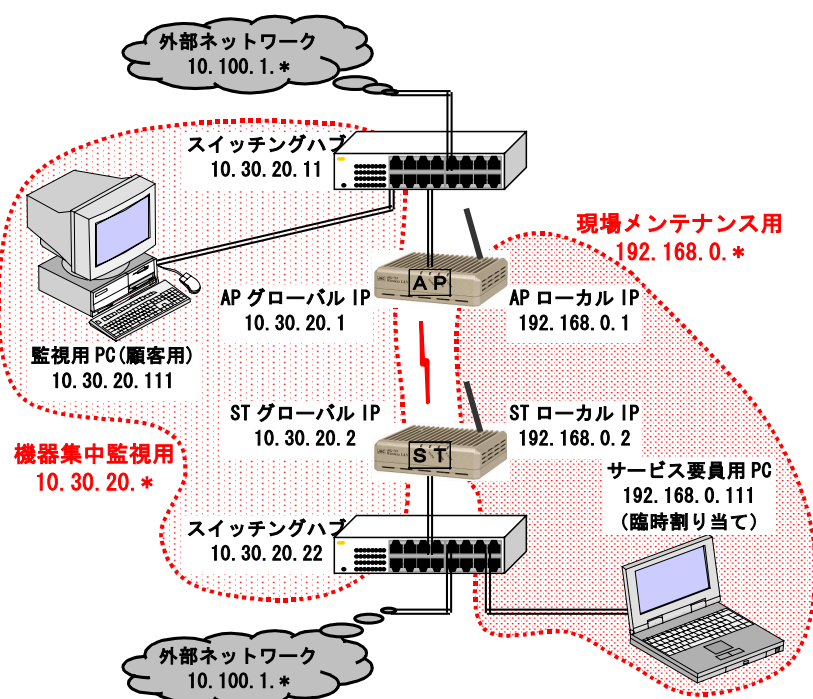
無線 LAN と組み合わせ可能なアンテナおよび給電線はカタログなどを参照してください。

付録17 グローバル IP アドレスとローカル IP アドレス

「4.3 ネットワーク設定[Network]」の章で述べたように、JRL-710/720 シリーズは 2 つの IP アドレスであるグローバル IP アドレス・ローカル IP アドレスを指定することができます。グローバル IP アドレスは無線 LAN 装置がパケット送受を行う上で必須の設定です。しかしローカル IP アドレスは無線 LAN 装置動作上必須ではありません。ローカル IP アドレスはお客様の用途に応じて別体系の IP アドレスで無線 LAN 装置にアクセスしたい場合に役に立つオプションです。

例えば下図のように通常運用時のネットワーク機器集中監視にはグローバル IP アドレスの体系を用い、現場メンテナンス時にはローカル IP アドレスの体系を使うといった用途が考えられます。

ローカル IP アドレスが設定してあればサービス要員用 PC への臨時 IP アドレス割り当て時に役立ちます。また IP アドレス体系がグローバル・ローカルと分離できていれば、スイッチングハブの VLAN 機能を用いて互いの IP アドレス体系を仮想的に別ネットワーク化できます。この場合、機器メンテナンス性を確保しながら機器を不正アクセスから保護するといったネットワーク設計が可能になります。



グローバル IP ・ ローカル IP 使い分け例

付録18 14 チャンネル対応機種について

JRL-710/720 シリーズの一部の機種では標準で使用可能な 2.4G 帯の 1～13 チャンネル(2.412～2.472GHz, 5MHz 間隔)に加えて, 総務省の技術基準適合証明を受けた上で 14 チャンネル(2.484GHz)に対応しています。14 チャンネルでの送受信は DSSS 変調方式のみ認可されています。従って 14 チャンネル対応機種で 14 チャンネルを選択する場合には「Wireless Mode」を「11b」に設定する必要があります。「4.6 無線[Wireless]」での「AP で動作している場合」GUI 画面から下記要領で設定します。

AP で動作している場合

The screenshot shows the 'Wireless Configuration' window. The 'Wireless Mode' dropdown is set to '11b' and the 'AP Channel' dropdown is set to '14(2.484GHz)'. Red boxes and arrows highlight these settings with the following annotations:

- ① 11b モードを選択します (Select 11b mode)
- ② 14 チャンネル対応機種の
場合, 14 チャンネルが
選択可能になります (In the case of 14-channel compatible equipment, 14 channels can be selected)

The GUI includes the following fields and options:

Wireless Configuration	
Operating Type	AP
RTS Threshold	2346 (0-2346)
Fragmentation Threshold	2346 (256-2346)
Hard Retry	7 (0-15)
Soft Retry	0 (0-15)
Allow ALL Inter-Client Communication	<input checked="" type="radio"/> enable <input type="radio"/> disable
ACK Timeout	short
TX Power	full
Wireless Mode	11b
AP Channel	14(2.484GHz)
Beacon Interval (msec)	100 (20-1000)
ERP Information Element	<input checked="" type="radio"/> enable <input type="radio"/> disable
Diversity Antenna	<input type="radio"/> enable <input checked="" type="radio"/> disable
Short Preamble	<input checked="" type="radio"/> enable <input type="radio"/> disable
Rate Configuration	
Apply Cancel Default	

「ST で動作している場合」については, デフォルトで 14 チャンネルがスキャン対象チャンネルに含まれます。スキャン対象チャンネルの編集を行う場合は下記要領で設定します。

ST で動作している場合

Wireless Configuration

Operating Type: ST

RTS Threshold: 2346 (0-2346)

Fragmentation Threshold: 2346 (256-2346)

Hard Retry: 7 (0-15)

Soft Retry: 0 (0-15)

ACK Timeout: short

TX Power: full

Wireless Mode: 11b

Diversity Antenna: ☐ enable ☒ disable

Short Preamble: ☒ enable ☐ disable

Pseudo Mode: ☐ enable ☒ disable

Pseudo MAC: 00:00:27:3E:***

Rate Configuration

Wireless Configuration for ST

Apply Cancel Default

① 11b モードを選択します

② スキャンチャンネル編集のため「Wireless Configuration for ST」をクリックします

ST で動作している場合 (ST 専用詳細設定)

Wireless Configuration for ST

Wireless Mode: 11b

Scan Mode: Active

Roaming Enable: ☐ enable ☒ disable

Scan Channel 1 (2.412GHz): ☒ enable ☐ disable

Scan Channel 2 (2.417GHz): ☒ enable ☐ disable

Scan Channel 3 (2.422GHz): ☒ enable ☐ disable

Scan Channel 4 (2.427GHz): ☒ enable ☐ disable

Scan Channel 5 (2.432GHz): ☒ enable ☐ disable

Scan Channel 6 (2.437GHz): ☒ enable ☐ disable

Scan Channel 7 (2.442GHz): ☒ enable ☐ disable

Scan Channel 8 (2.447GHz): ☒ enable ☐ disable

Scan Channel 9 (2.452GHz): ☒ enable ☐ disable

Scan Channel 10 (2.457GHz): ☒ enable ☐ disable

Scan Channel 11 (2.462GHz): ☒ enable ☐ disable

Scan Channel 12 (2.467GHz): ☒ enable ☐ disable

Scan Channel 13 (2.472GHz): ☒ enable ☐ disable

Scan Channel 14 (2.484GHz): ☒ enable ☐ disable

11b RSSI To Scan (dBm): -80 (-120 - 0)

11b Rate To Scan (Mbps): 1 (1-11)

Ok

③ 「11b」モードが選択されていることを確認します

④ 14 チャンネル対応機器の場合スキャンチャンネルの編集対象として 14 チャンネルが表示されます

11b 以外のモード, 例えば 11g や 11b+g モードを選択している場合には変調方式として OFDM が選択される場合があるため 14 チャンネルの設定・運用はできません。この場合 1~13 チャンネルの範囲で設定・運用が可能です。

技術基準適合証明は個別の装置毎に取得しています。

1~13 チャンネルで認証を受けた装置は, 例えファームウェア変更等を行ったとしても 14 チャンネルを実動作上でも法律上でも機能させることはできません。

付録19 5.2G 帯対応機種について

JRL-710/720 シリーズの一部の機種では、総務省の技術基準適合証明を受けた上で 5.2G 帯に対応しています。5.2G 帯対応機種で 5.2G を選択するためには「Wireless Mode」を、AP で動作している場合には「11a」に、ST で動作している場合には「11a」・「11a+b」・「11a+g」・「11a+b+g」のいずれかに設定する必要があります。

5.2G 帯対応機種でサポートされるチャンネルは次の通りです。

チャンネル番号	周波数(GHz)
36	5.180
40	5.200
44	5.220
48	5.240

⚠ 注意

- 5.2G 帯は屋内でのみ運用可能です。屋外での運用は認められていません。屋外で運用する場合は 11b あるいは 11b+g モードを使用してください。

「4.6 無線[Wireless]」での「AP で動作している場合」GUI 画面から下記要領で設定します。

AP で動作している場合

The screenshot shows the 'Wireless Configuration' window. The 'Operating Type' is set to 'AP'. The 'Wireless Mode' is set to '11a', and the 'AP Channel' is set to '36(5.180GHz)'. Red boxes and arrows highlight these settings, with callouts explaining the requirements for 5.2G band operation.

Wireless Configuration

Operating Type: AP

RTS Threshold: 2346 (0-2346)

Fragmentation Threshold: 2346 (256-2346)

Hard Retry: 7 (0-15)

Soft Retry: 0 (0-15)

Allow ALL Inter-Client Communication: ☒ enable ☐ disable

ACK Timeout: short

TX Power: full

Wireless Mode: 11a

AP Channel: 36(5.180GHz)

Beacon Interval (msec): 100 (20-1000)

ERP Information Element: ☒ enable ☐ disable

Diversity Antenna: ☐ enable ☒ disable

Short Preamble: ☒ enable ☐ disable

Rate Configuration

Apply Cancel Default

① 5.2G 帯対応機種の
場合「11a」モード
を選択します

② 11a を選択した場合、
36/40/44/48
チャンネルが選択可能
になります

「ST で動作している場合」については、デフォルトで 36/40/44/48 チャンネルがスキャン対象チャンネルに含まれます。スキャン対象チャンネルの編集を行う場合は下記要領で設定します。

ST で動作している場合

Wireless Configuration

Operating Type: (0-2346)

RTS Threshold: (256-2346)

Fragmentation Threshold: (0-15)

Hard Retry: (0-15)

Soft Retry: (0-15)

ACK Timeout:

TX Power:

Wireless Mode:

Diversity Antenna: ☐ enable ☒ disable

Short Preamble: ☒ enable ☐ disable

Pseudo Mode: ☐ enable ☒ disable

Pseudo MAC:

Rate Configuration

Wireless Configuration for ST

Apply Cancel Default

① 5.2G 帯対応機種の場合
「11a」「11a+b」「11a+g」「11a+b+g」のいずれかのモードを選択します

② スキャンチャンネル編集のため
「Wireless Configuration for ST」をクリックします

ST で動作している場合 (ST 専用詳細設定)

Wireless Configuration for ST

Wireless Mode:

Scan Mode:

Roaming Enable: ☐ enable ☒ disable

Scan Channel 36 (5.180GHz): ☒ enable ☐ disable

Scan Channel 40 (5.200GHz): ☒ enable ☐ disable

Scan Channel 44 (5.220GHz): ☒ enable ☐ disable

Scan Channel 48 (5.240GHz): ☒ enable ☐ disable

11a RSSI To Scan (dBm): (-120 - 0)

11a Rate To Scan (Mbps): (6-54)

Ok

③ 「11a」「11a+b」「11a+g」「11a+b+g」のいずれかのモードが選択されていることを確認します

④ 5.2G 帯対応機器の場合
スキャンチャンネルの編集対象として 36/40/44/48 チャンネルが表示されます

710/720 シリーズの 5.2G 帯対応機種は、W52 と呼ばれる 36 / 40 / 44 / 48 チャンネル(5.18 / 5.20 / 5.22 / 5.24 GHz)に対応します。
W53 と呼ばれる 52 / 56 / 60 / 64 チャンネル(5.26 / 5.28 / 5.30 / 5.32 GHz)には対応していません。

技術基準適合証明は個別の装置毎に取得しています。
5.2G 帯で認証を受けていない装置は、例えファームウェア変更等を行ったとしても 5.2G 帯を実動作上でも法律上でも機能させることはできません。

付録20 4.9G 帯対応機種について

JRL-710/720 シリーズの一部の機種では、総務省の技術基準適合証明を受けた上で 4.9G 帯に対応しています。4.9G 帯対応機種で 4.9G を選択するためには「Wireless Mode」を「11j」に設定する必要があります。

4.9G 帯対応機種は特殊構成の無線部を持つため、他のバンドである 2.4G 帯(802.11b/g)や 5.2G 帯(802.11a)は使用できません。802.11j 専用機種となります。

4.9G 帯対応機種でサポートされるチャンネルは次の通りです。

チャンネル番号	周波数(GHz)
184	4.92
188	4.94
192	4.96
196	4.98

⚠ 注意

- 4.9G 帯は屋内・屋外で運用可能ですが、運用にあたっては届出制の免許を受ける必要があります。

「4.6 無線[Wireless]」での「AP で動作している場合」GUI 画面から下記要領で設定します。

AP で動作している場合

The screenshot shows the 'Wireless Configuration' window. The 'Wireless Mode' dropdown is set to '11j' and the 'AP Channel' dropdown is set to '184(4.920GHz)'. Red boxes and arrows highlight these settings, with callouts explaining that '11j' mode is required for 4.9G and that selecting '11j' enables the 184/188/192/196 channels.

①4.9G 帯対応機種の
場合「11j」モード
を選択します

②11j を選択した場合、
184/188/192/196
チャンネルが選択可能にな
ります

ST で動作している場合

Wireless Configuration

Operating Type: ST

RTS Threshold: 2346 (0-2346)

Fragmentation Threshold: 2346 (256-2346)

Hard Retry: 7 (0-15)

Soft Retry: 0 (0-15)

ACK Timeout: short

TX Power: full

Wireless Mode: 11j

Diversity Antenna: ☐ enable ☒ disable

Short Preamble: ☒ enable ☐ disable

Pseudo Mode: ☐ enable ☒ disable

Pseudo MAC: 00:00:27:3E:**:**

Rate Configuration

Wireless Configuration for ST

Apply Cancel Default

① 4.9G 帯対応機種の場合「11j」モードを選択します

② スキャンチャンネル編集のため「Wireless Configuration for ST」をクリックします

ST で動作している場合 (ST 専用詳細設定)

Wireless Configuration for ST

Wireless Mode: 11j

Scan Mode: Active

Roaming Enable: ☐ enable ☒ disable

Scan Channel 184 (4.920GHz): ☒ enable ☐ disable

Scan Channel 188 (4.940GHz): ☒ enable ☐ disable

Scan Channel 192 (4.960GHz): ☒ enable ☐ disable

Scan Channel 196 (4.980GHz): ☒ enable ☐ disable

11j RSSI To Scan (dBm): -80 (-120 - 0)

11j Rate To Scan (Mbps): 6 (6-54)

Ok

③ 「11j」が選択されていることを確認します

④ 4.9G 帯対応機器の場合スキャンチャンネルの編集対象として184/188/192/196チャンネルが表示されます

技術基準適合証明は個別の装置毎に取得しています。

4.9G 帯で認証を受けていない装置は、例えファームウェア変更等を行ったとしても 4.9G 帯を実動作上でも法律上でも機能させることはできません。

付録21 set/get コマンドで利用できる設定パラメータ

diag ユーザでログインして使用する set および get コマンドで変更可能な設定パラメータについて下表に示します。

パラメータ名	設定範囲	内容	注意事項
IPADDR	1.0.0.1～223.*.* (127.*.*除く)	本体の IP アドレス	
NETMASK	128.0.0.0～ 255.255.255.252	本体のサブネットマスク	
GATEWAY	1.0.0.1～223.*.* (127.*.*除く)	本体のデフォルトゲートウェイ	
ELINK	"auto": 自動認識 "10": 10M Half "10f": 10M Full "100": 100M Half "100f": 100M Full	LAN ポートの設定 (Auto/100M/10M/全 2 重/半 2 重)	MDI/MDI-X 固定には対応しません
AUTHEN	0: AUTO (ST) / Open&Shared (AP) 1: Open Only 2: Shared Only	認証方式 (ST は Auto/Open/Shared)	2: Shared Only には WEP Key 設定が必要です
SSID	0～32 文字 半角英数字, ハイフン	AP の SSID ST の SSID1 にもコピーされます	スペース(空白)は使用できません
SSID1		ST で使用する SSID の設定	SSID1 から優先順で使用されます SSID2 と SSID3 は, 空白の場合使用されません
SSID2			
SSID3			
STEALTH	0: ステルス機能 OFF 1: ステルス機能 ON	ビーコンに SSID 情報を載せない AnySSID 検索への応答拒否	
ENCMODE	0: none (暗号化なし) 1: WEP 2: WPA-PSK	暗号化モード none/WEP/WPA-PSK	1: WEP は WEPKEYID で指定した ID の WEP Key 設定が必要です 2: WPA-PSK は PSKPASS 設定が必要です
KEY_LEN1	40/104/128	WEP キーの長さ設定	
KEY_LEN2			
KEY_LEN3			
KEY_LEN4			
KEY_DEF1	HEX 5/13/16Byte	WEP キー設定	1 から 4 の対応する WEP キーの長さに合わせた設定が必要です
KEY_DEF2			
KEY_DEF3			
KEY_DEF4			
WEPKEYID	1～4	WEP 送信キー番号	対応する WEP キーの設定が必要です

付録

パラメータ名	設定範囲	内容	注意事項
CIPHER	0: AES 1: TKIP	WPA-PSK の暗号化方式選択	
PSKPASS	8～63 文字 半角英数字, ハイフン	WPA-PSK のパスフレーズ	
GKEY_UPD	0: OFF 1: ON	WPA-PSK のグループキー更新	
GKEY_INT	30～86400 [sec]	グループキー更新間隔	
TYPE	0: ST 1: AP	AP/ST 切替え	
RTSCTS	0～2346	RTS しきい値	
FRAGMENT	256～2346	フラグメントしきい値	
RETRY_HW	0～15	ハードウェア制御のリトライ回数	
RETRY_SW	0～15	ソフトウェア制御のリトライ回数	
BSS_COM	0: ST 間通信禁止 1: ST 間通信許可	子機間通信の許可または禁止	
ACKTMO	0: short 1: middle 2: long	ACK 受信待ち時間 0: 0-2km 1: 2-5km 2: 5-30km	
TPCLVL	0: full 1: half (1/2) 2: quarter (1/4) 3: eighth (1/8) 4: min	送信電力設定	
WMODE	1: 11b 2: 11g 3: 11b+g 4: 11a 5: 11a+b (ST のみ) 6: 11a+g (ST のみ) 7: 11a+b+g (ST のみ)	無線モード	TYPE 設定に対応した値を設定する必要があります 11a 設定は対応機種のみ有効です
CHANNEL	1～14 36, 40, 44, 48	AP に設定する通信チャンネル	WMODE 設定に対応した値を設定する必要があります
BC_INT	20～1000 [msec]	ビーコン送信周期	
ANTDIV	0: OFF 1: ON	アンテナダイバーシティ設定	OFF のとき ANT1 固定です
ANTBCDST	0～65535 (0: fix ANT1)	アンテナごとのビーコン送信周期	ANTDIV が ON のとき有効です
PREAMBLE	0: disable (long のみ) 1: enable (short)	プリアンブル長選択	
PSEUD_MODE	0: none 1: Pseud MAC mode	代理送受信モード設定	
PSEUD_ADDR	MAC address (HEX 12 文字)	代理送受信用 MAC アドレス指定	
PROTECT11G	0: プロテクト OFF 1: プロテクト ON	11g 通信の優先設定	11g, 11b+g 通信で有効です

付録

パラメータ名	設定範囲	内容	注意事項	
RATE_SUP1	0: Not Supported 1: Supported	サポートレート設定	11b, 11g 通信で有効です	
RATE_SUP2				
RATE_SUP5				
RATE_SUP11				
RATE_SUP6				
RATE_SUP9			11g, 11b+g, 11a 通信で有効です	
RATE_SUP12				
RATE_SUP18				
RATE_SUP24				
RATE_SUP36				
RATE_SUP48				
RATE_SUP54				
RATE_BAS1	0: Not Required 1: Required	ベーシックレート設定 (AP で有効)	対応するサポートレート設定を「1: Supported」とする必要があります 対応するレートをサポートしていない子機の接続を拒否します	
RATE_BAS2				
RATE_BAS5				
RATE_BAS11				
RATE_BAS6				
RATE_BAS9				
RATE_BAS12				
RATE_BAS18				
RATE_BAS24				
RATE_BAS36				
RATE_BAS48				
RATE_BAS54				
RATE_MGTB	1, 2, 5, 11	マネジメントレート設定 ビーコンなど管理用パケットの送信レート設定	対応するサポートレート設定を「1: Supported」とする必要があります	
RATE_MGTG	1, 2, 5, 11, 6, 9, 12, 18, 24, 36, 48, 54			
RATE_MGBG	1, 2, 5, 11			
RATE_MGTA	6, 9, 12, 18, 24, 36, 48, 54			
RATE_MULB	1, 2, 5, 11	マルチキャストレート設定 マルチキャスト(ブロードキャスト)の送信レート設定 (AP で有効)		11b/g/a の各通信モードに対応したパラメータが使用されます
RATE_MULG	1, 2, 5, 11, 6, 9, 12, 18, 24, 36, 48, 54			
RATE_MULA	6, 9, 12, 18, 24, 36, 48, 54			
RATE_MUBG	1, 2, 5, 11			
RATE_DB1	0: Not Use 1: Use	データレート設定 11b モードのデータ送信レート設定	対応するサポートレート設定を「1: Supported」とする必要があります AP の場合, 11b レートしかサポートしない子機への送信レートに使用します	
RATE_DB2				
RATE_DB5				
RATE_DB11				

パラメータ名	設定範囲	内容	注意事項
RATE_DG1	0: Not Use 1: Use	データレート設定 11b モードのデータ送信レート設定	対応するサポートレート設定を「1: Supported」とする 必要があります AP の場合, 11g レートをサ ポートする子機への送信レ ートに使用します
RATE_DG2			
RATE_DG5			
RATE_DG11			
RATE_DG6			
RATE_DG9			
RATE_DG12			
RATE_DG18			
RATE_DG24			
RATE_DG36			
RATE_DG48			
RATE_DG54			
RATE_DA6	0: Not Use 1: Use	データレート設定 11a モードのデータ送信レート設定	対応するサポートレート設 定を「1: Supported」とする 必要があります 11a モードで使用されます
RATE_DA9			
RATE_DA12			
RATE_DA18			
RATE_DA24			
RATE_DA36			
RATE_DA48			
RATE_DA54			
SCAN_MODE	0: active 1: passive 2: any	スキャン方式の設定	AP では設定に関わらず passive 動作となります
SCAN_CH1	0: Not Use 1: Use	スキャンするチャネルの設定	11b, 11g 通信で使用されま す
SCAN_CH2			
SCAN_CH3			
SCAN_CH4			
SCAN_CH5			
SCAN_CH6			
SCAN_CH7			
SCAN_CH8			
SCAN_CH9			
SCAN_CH10			
SCAN_CH11			
SCAN_CH12			
SCAN_CH13			
SCAN_CH14	0: Not Use 1: Use	スキャンするチャネルの設定	11b 通信で有効となります 14ch 対応機種で有効です
SCAN_CH36	0: Not Use 1: Use	スキャンするチャネルの設定	11a 通信で有効となります 36, 40, 44, 48ch (W52) 対 応機種のみ有効です
SCAN_CH40			
SCAN_CH44			
SCAN_CH48			

付録

パラメータ名	設定範囲	内容	注意事項
ROAM_MODE	0: disable 1: enable	ローミング機能の設定 (ST のみ)	
ROAM_RSSIB	-120~0	ローミング開始 RSSI しきい値設定 (ST のみ)	11b/g/a の各通信モードに対応したパラメータが使用されます
ROAM_RSSIG	-120~0		
ROAM_RSSIA	-120~0		
ROAM_RATEB	1, 2, 5, 11	ローミング開始レートしきい値設定 (ST のみ)	11b/g/a の各通信モードに対応したパラメータが使用されます
ROAM_RATEG	1, 2, 5, 11, 6, 9, 12, 18, 24, 36, 48, 54		
ROAM_RATEA	6, 9, 12, 18, 24, 36, 48, 54		
IAPP	0: disable 1: enable	IAPP 機能の設定 (AP のみ)	
ACL_MODE	0: disable 1: enable	MAC アドレスフィルタ機能の設定	
SV_TELNET	0: Not Start 1: Start Server	telnet による設定機能の有効または無効の設定	telnet/SSH/HTTP 全てが「0: Not Start」の場合、RS232C シリアルケーブルアクセスが必要となります
SV_SSH	0: Not Start 1: Start Server	SSH による設定機能の有効または無効の設定	
SV_HTTP	0: Not Start 1: Start Server	WEB ブラウザによる設定機能の有効または無効の設定	
SV_FTP	0: Not Start 1: Start Server	ftp による設定ファイルのアップロードとダウンロード機能の有効または無効の設定	
AC_W_TELNET	0: Not permit 1: Permit	無線ネットワークからの telnet アクセスを許可する設定	SV_TELNET が「1: Start Server」のときに有効です
AC_W_SSH		無線ネットワークからの SSH アクセスを許可する設定	SV_SSH が「1: Start Server」のときに有効です
AC_W_HTTP		無線ネットワークからの HTTP (WEB ブラウザによる設定) アクセスを許可する設定	SV_HTTP が「1: Start Server」のときに有効です
AC_W_FTP		無線ネットワークからの ftp アクセスを許可する設定	SV_FTP が「1: Start Server」のときに有効です
AC_E_TELNET	0: Not permit 1: Permit	有線ネットワークからの telnet アクセスを許可する設定	SV_TELNET が「1: Start Server」のときに有効です
AC_E_SSH		有線ネットワークからの SSH アクセスを許可する設定	SV_SSH が「1: Start Server」のときに有効です
AC_E_HTTP		有線ネットワークからの HTTP (WEB ブラウザによる設定) アクセスを許可する設定	SV_HTTP が「1: Start Server」のときに有効です
AC_E_FTP		有線ネットワークからの ftp アクセスを許可する設定	SV_FTP が「1: Start Server」のときに有効です
PASSWD_ADMIN	1~8 文字 半角英数字, ハイフン	Login/Password (admin/User)	再入力による確認機能はありません
PASSWD_USER			

付録22 設定ファイルの使用方法

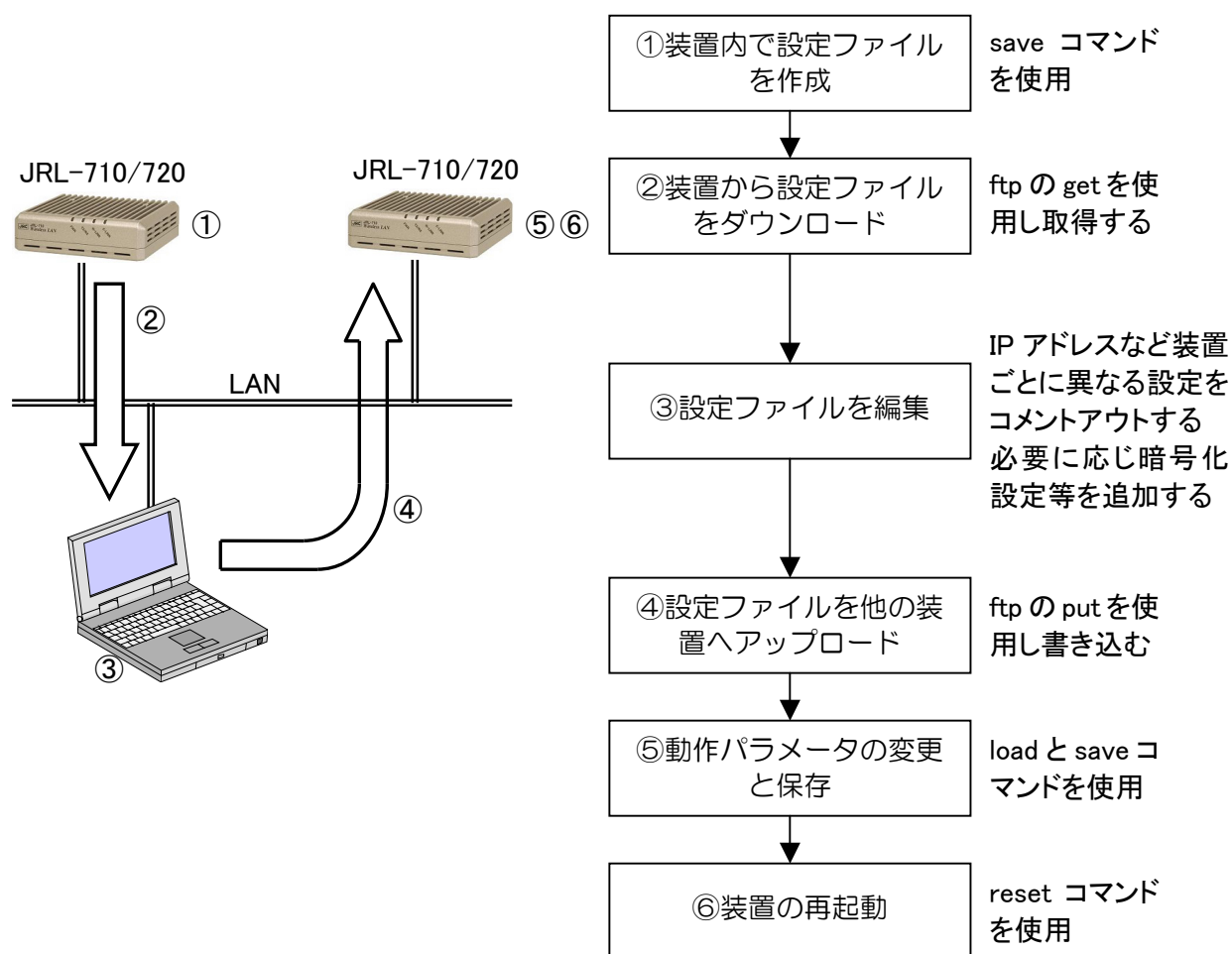
diag ユーザでログインして使用する save と load コマンドにより、装置の動作パラメータを管理する手順について以下に説明します。なお、本項では次のような用途で操作する場合を例にしています。

- ・ 現在動作中の装置の動作パラメータを取得し PC に保存・管理する
- ・ WEB ブラウザで詳細な設定変更をした内容を、複数の装置に効率よく反映させる

機器の保守で、交換前の装置の動作パラメータを交換後の装置に書き込む場合などにも有効です。

(1) 操作の流れ

設定ファイルを使用した動作パラメータの操作については、以下のような流れとなります。



(2) 設定ファイルの作成と装置からのダウンロード (①②)

以下に設定ファイルの作成手順と、ftp を使用したダウンロードについて説明します。

なお本機能を使用するには、装置に telnet または SSH で diag ユーザログイン可能であることと、あらかじめ装置の動作パラメータ設定で ftp によるアクセスが可能となっている環境が必要です。

(2-1) diag ユーザでのログイン

telnet または SSH を使用して、diag ユーザで装置にログインします。ログイン方法については本マニュアルの「5. 診断機能」を参照してください。

(2-2) save コマンドの実行

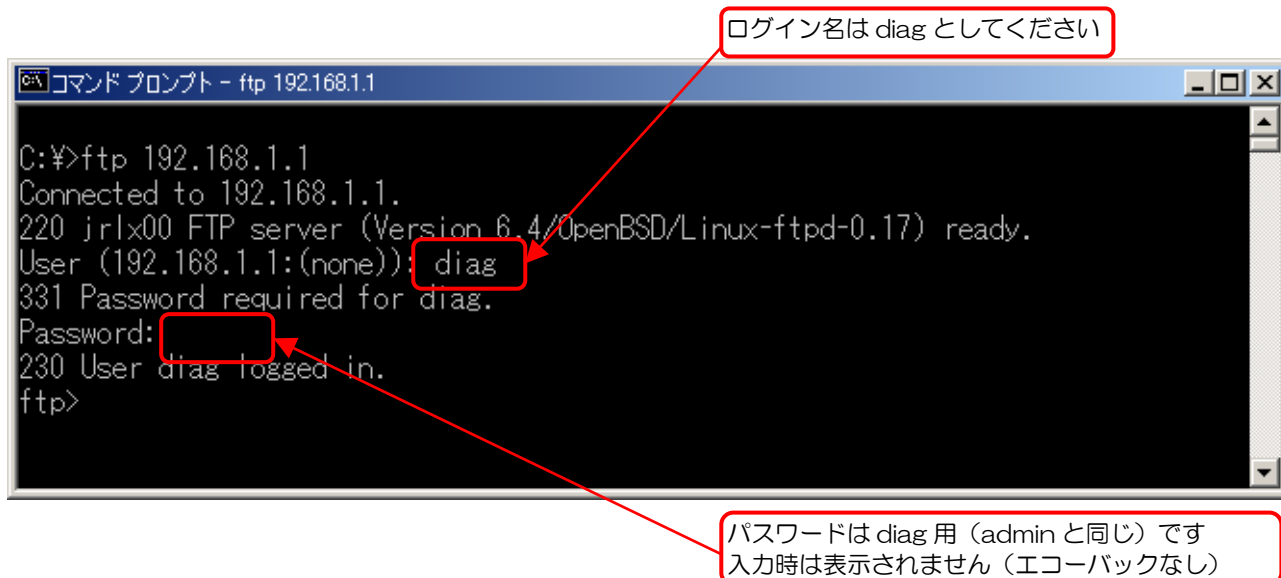
装置内で設定ファイルを作成します。ログインが完了している telnet または SSH の画面から以下の操作を実行してください。

```
diag > save
diag >
```

装置内のファイル管理領域に「setup.txt」と「setup_<MAC アドレス下位3バイト>.txt」の両設定ファイルが作成されます。

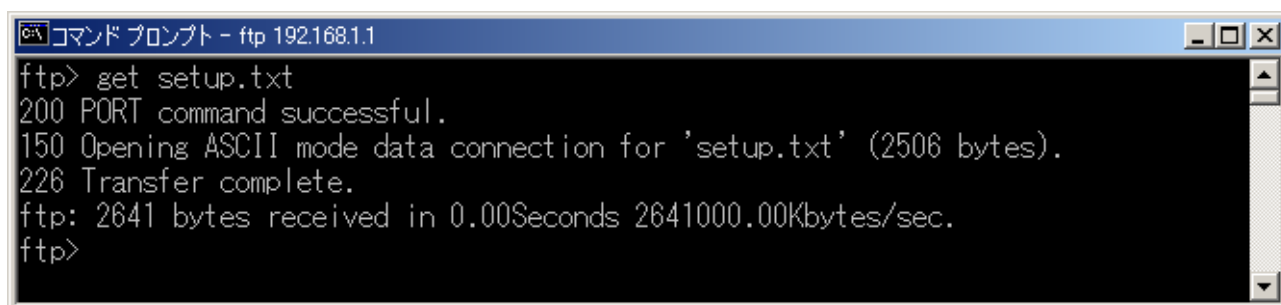
(2-3) ftp ログイン

作成された設定ファイルを装置からダウンロードします。ftp を使用しますので以下のように装置へのログインを実行してください。なお、以下の例は装置の IP アドレスが 192.168.1.1 の場合です。



(2-4) ftp コマンド (get) の実行

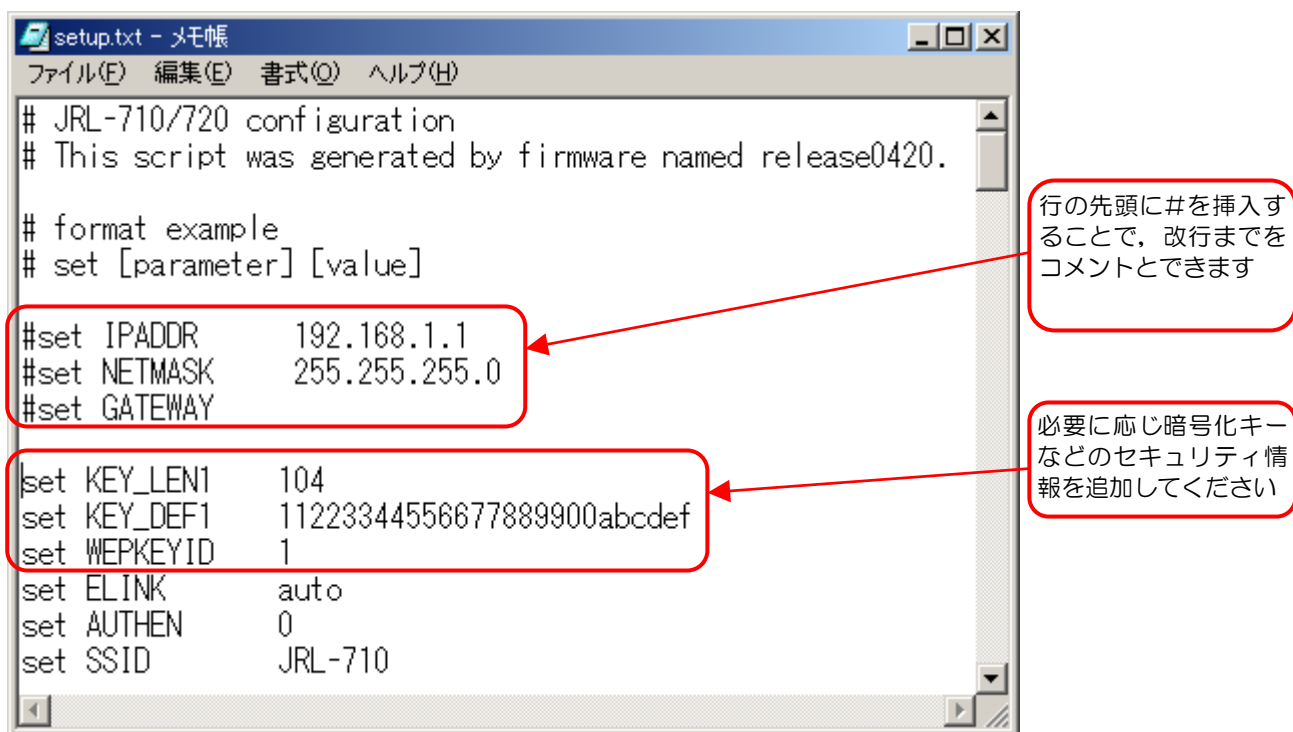
ftp の get コマンドを実行してダウンロードします。以下のように、ログインした ftp 画面で get コマンドを実行してください。なお、転送時のデータモードは ASCII またはバイナリのどちらでも構いませんが、バイナリモードの場合、設定ファイル内の各行末の改行コードに CR (ODh) が含まれず LF (0Ah) のみとなりますので、編集時の際 Windows の Notepad など、デフォルトでは LF による改行をサポートしないエディタを使用する場合には ftp デフォルトの ASCII モードを使用ください。



save コマンドにより作成される設定ファイルは、装置内の揮発性記憶領域で管理されており、装置を再起動すると自動的に削除されます。設定ファイルをダウンロードするときは、必ず直前に telnet または SSH の diag ログインを実行し、diag のコンソールから save コマンドを使って設定ファイルを作成してから ftp で取得してください。ダウンロード後も装置を再起動するまでは設定ファイルの繰り返し取得が可能です。

(3) 設定ファイルの編集 (③)

ダウンロードした設定ファイルを使用して他の装置へ設定を反映させたいとき、IP アドレスなどの変更させたくない動作パラメータについては、他の装置へアップロードする前に設定ファイルを編集する必要があります。この場合、以下のように“#”を挿入することで設定ファイル内のコメント情報とすることが可能です。また、暗号化キーなどのセキュリティ情報は、save コマンドにより作成される設定ファイルには含まれていませんので、必要に応じてテキストエディタにより追加する必要があります。



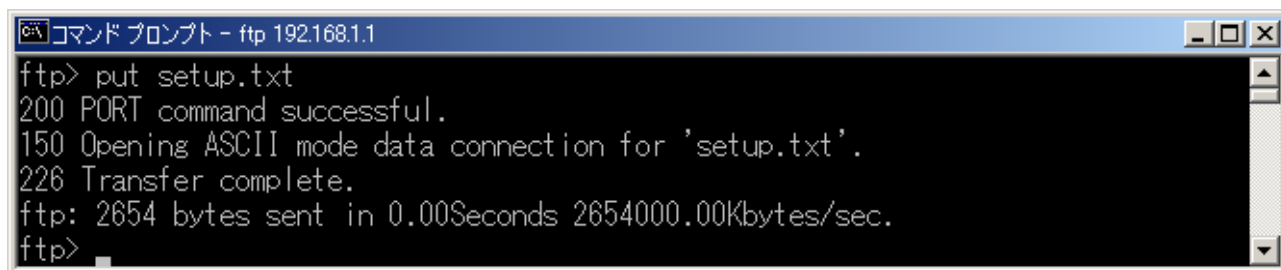
(4) 設定ファイルのアップロードと動作パラメータの変更 (④⑤)

(4-1) ftp ログイン

編集した設定ファイルを、装置にアップロードするために ftp を使用します。(2-3)にある ftp ログインを実行してください。

(4-2) ftp コマンド (put) の実行

ftp の put コマンドを実行してアップロードします。以下のように、ログインした ftp 画面で put コマンドを実行してください。以下の例は、設定ファイルを「setup.txt」とした場合です。



```
コマンドプロンプト - ftp 192.168.1.1
ftp> put setup.txt
200 PORT command successful.
150 Opening ASCII mode data connection for 'setup.txt'.
226 Transfer complete.
ftp: 2654 bytes sent in 0.00Seconds 2654000.00Kbytes/sec.
ftp>
```

(4-3) diag ユーザでのログイン

telnet または SSH を使用して、diag ユーザで装置にログインします。ログイン方法については本マニュアルの「5. 診断機能」を参照してください。

(4-4) load コマンドの実行

装置内で設定ファイルを使用して動作パラメータを変更します。ログインが完了している telnet または SSH の画面から以下の操作を実行してください。以下の例は、アップロードした設定ファイル名が「setup.txt」である場合です。なお、ファイル名が「setup.txt」である場合のみ、load コマンドだけ（パラメータなし）でも動作します。

```
diag > load setup.txt
diag >
```

(4-5) save コマンドの実行

変更した動作パラメータを装置のフラッシュメモリに保存します。(2-2)と同様にログインが完了している telnet または SSH の画面から以下の操作を実行してください。

```
diag > save
diag >
```

(5) 装置の再起動 (6)

変更・保存した動作パラメータで装置を動作させるには、装置内で動作しているソフトウェアを再起動する必要があります。ログインが完了している telnet または SSH の画面から以下の操作を実行してください。なお、「reset -y」と入力することで、reset コマンドの実行確認（「proceed (Y/N) ?」への「y」入力）を省略することができます。

```
diag > reset
diag > proceed (Y/N) ? y
```




<http://www.jrc.co.jp>

(無断複製・転載を禁ずる)

本書は森林資源保護のため、再生紙を使用しています。

第4版 2007年 7月

第4.1版 2007年 12月

編 者 日本無線株式会社

発行者 日本無線株式会社

〒181-8510 東京都三鷹市下連雀 5-1-1

通信機器事業本部カスタマーサービスグループ

E-mail : wlan-support@jrc.co.jp

TEL : 0422-45-9578 FAX : 0422-45-9104

DC4.1-JRL-710/720

