ICOM®

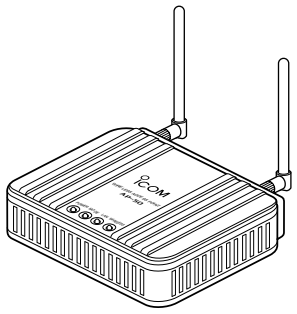
取扱説明書[活用編]

WAVEMASTER®

WIRELESS ACCESS POINT

AP-50

IEEE802.3af規格PoE対応



Icom Inc.

各章について

各メニューの設定画面について説明しています。
設定画面は、用途別に下記の各メニューに分類されています。

はじめに

本書は、本製品で設定できるさまざまな機能について、各メニューの設定画面について詳しく説明しています。
取扱説明書[導入編]に記載されていない詳細な機能を設定するときなど、本書と併せてご覧ください。

表記について

本書は、次の規則にしたがって表記しています。

「　」表記：本製品の各メニューと、そのメニューに属する設定画面の名称を(「」)で囲んで表記します。
[　] 表記：各設定画面の設定項目名を([])で囲んで表記します。
〈　〉表記：設定画面上に設けられたコマンドボタンの名称を(〈〉)で囲んで表記します。

※Microsoft® Windows® XP Professional、Microsoft® Windows® XP Home Editionは、Windows XPと表記します。
Microsoft® Windows® 2000 Professionalは、Windows 2000と表記します。
Microsoft® Windows® Millennium Editionは、Windows Meと表記します。
Microsoft® Windows® 98 Second Editionは、Windows 98 SEと表記します。
※本書は、Ver1.17のファームウェアを使用して説明しています。
※本書中の画面は、OSのバージョンや設定によって、お使いになるパソコンと多少異なる場合があります。

登録商標について

「ネットワーク設定」メニュー

第1章

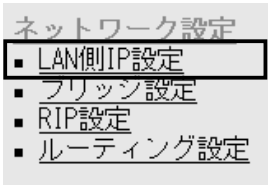
この章では、
「ネットワーク設定」メニューで表示される設定画面について説明します。

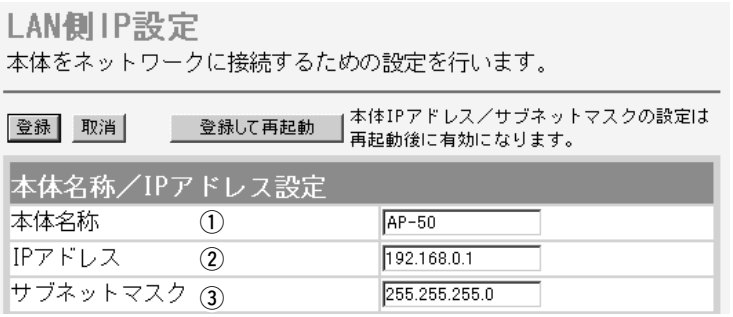
1 「ネットワーク設定」メニュー

1-1.「LAN側IP設定」画面

■本体名称/IPアドレス設定

本製品の名称とLAN側IPアドレスを設定します。





〈登録〉ボタン …… [IPアドレス]欄と[サブネットマスク]欄以外の設定内容が有効になります。

※[IPアドレス]欄と[サブネットマスク]欄、[DHCPサーバ設定]項目、[静的DHCPサーバ設定]の変更内容は、画面上で確定されるだけですので、〈登録して再起動〉をクリックするまで有効になりません。

〈取消〉ボタン …… 「LAN側IP設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

〈登録して再起動〉ボタン …… 本製品を再起動して、「LAN側IP設定」画面で変更したすべての設定内容が有効になります。

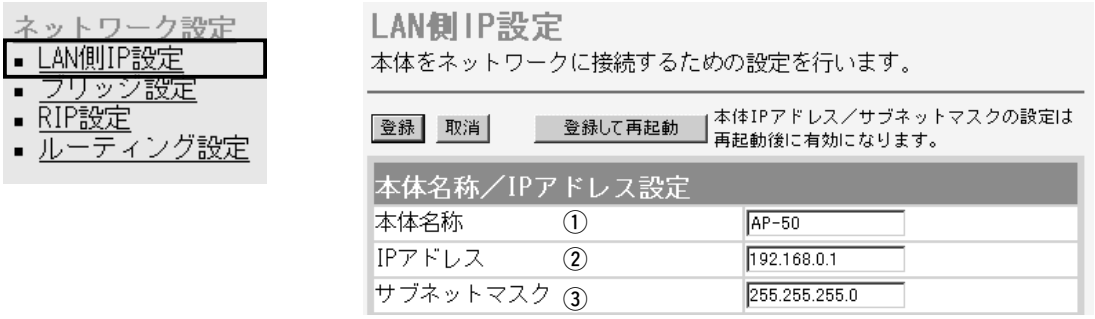
①本体名称 …… 名前や名称を、任意の英数字や記号[半角31(全角15)文字以内]で入力します。
設定した名称は、Telnet(☞5章)でログインしたときのログインメッセージに使用されます。 (出荷時の設定：AP-50)

②IPアドレス …… 本製品のIPアドレスを入力します。
(出荷時の設定：192.168.0.1)
本製品を稼働中のネットワークに接続するときなど、そのLANに合わせたネットワークIPアドレスに変更してください。

※本製品のDHCPサーバ機能を使用する場合は、[DHCPサーバ設定]項目の[割り当て開始IPアドレス]欄についてもネットワーク部を同じ設定にしてください。

1-1.「LAN側IP設定」画面

■本体名称/IPアドレス設定(つづき)



③サブネットマスク ……

本製品のサブネットマスク(同じネットワークで使用するIPアドレスの範囲)を設定します。　(出荷時の設定：255.255.255.0)
本製品を現在稼働中のネットワークに接続するときなど、そのネットワークに合わせたサブネットマスクに変更してください。

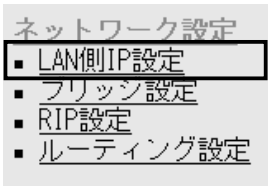
[例：固定IPアドレスを8個取得している場合]
(192.168.0.0 ～192.168.0.7)

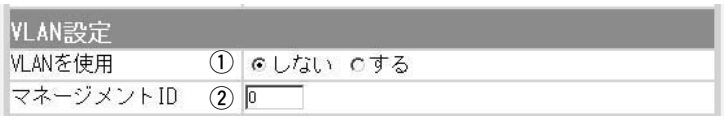
サブネットマスクを「255.255.255.248」と設定する場合、「192.168.0.2～192.168.0.6」が同じネットワークとしてパソコンに割り当てできます。
この場合、下記のIPアドレスはパソコンに割り当てできません。
「192.168.0.0」：ネットワークアドレス
「192.168.0.1」：本製品のLAN側IPアドレス
「192.168.0.7」：ブロードキャストアドレス

1 「ネットワーク設定」メニュー

1-1.「LAN側IP設定」画面(つづき)

■VLAN設定　　**VLAN機能についての設定です。**





①VLANを使用 ……　VLAN(Virtual LAN)機能を使用して、本製品の無線ネットワークと同じ[VLAN ID]が設定された有線ネットワークとだけ通信できるようにするか、しないかを設定します。

(出荷時の設定：しない)

※VLAN機能を「する」に設定するとき、[マネージメントID]欄(②)を「1～4094」に設定してください。
「0」(出荷時の設定)の場合は、設定できません。

※無線ネットワークの[VLAN ID]は、「無線LAN設定」メニューの「無線LAN設定」画面にある[VLANID]欄(☞P21)と「暗号化設定」画面にある[キー値]項目の[デフォルトキー]欄(☞P31)、[仮想BSS設定]項目(☞P32)で設定します。

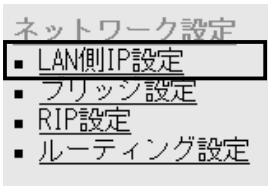
②マネージメントID ……　本製品へのアクセスを許可するIDを設定します。

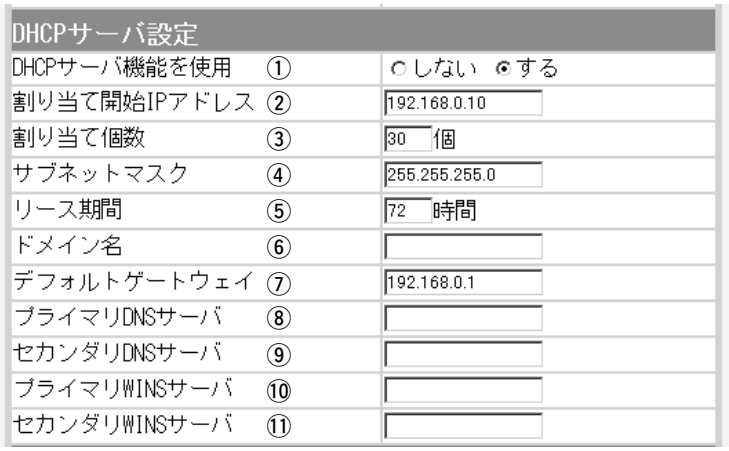
(出荷時の設定：1)

設定できる範囲は、「1～4094」です。
本製品に設定されたマネージメントIDを持つ機器からのアクセスだけを許可できます。

1-1.「LAN側IP設定」画面(つづき)

■DHCPサーバ設定　　**DHCPサーバ機能についての設定です。**





DHCPサーバ設定		
DHCPサーバ機能を使用	①	○しない ◉する
割り当て開始IPアドレス	②	192.168.0.10
割り当て個数	③	30 個
サブネットマスク	④	255.255.255.0
リース期間	⑤	72 時間
ドメイン名	⑥	
デフォルトゲートウェイ	⑦	192.168.0.1
プライマリDNSサーバ	⑧	
セカンダリDNSサーバ	⑨	
プライマリWINSサーバ	⑩	
セカンダリWINSサーバ	⑪	

①DHCPサーバ機能を使用 …　本製品をDHCPサーバとして使用「する」か「しない」かの設定です。本製品に有線および無線で接続しているパソコンのTCP/IP設定を、「IPアドレスを自動的に取得する」と設定している場合、本製品のDHCPクライアントになります。
この機能によって、動的にDHCPサーバである本製品からIPアドレス/サブネットマスクが与えられます。　(出荷時の設定：する)

②割り当て開始IPアドレス …　本製品に有線および無線で直接接続するパソコンへ、IPアドレスを自動で割り当てるときの開始アドレスを設定します。
(出荷時の設定：192.168.0.10)

③割り当て個数 ……　[割り当て開始IPアドレス]欄に設定されたIPアドレスから連続で自動割り当て可能なアドレスの最大個数は、0～128(無線LANで接続するパソコンを含む)までです。　(出荷時の設定：30)
※128個を超える分については、設定できませんので手動でクライアントに割り当ててください。
※「0」を設定したときは、自動割り当てをしません。

④サブネットマスク ……　[割り当て開始IPアドレス]欄に設定されたIPアドレスに対するサブネットマスクです。　(出荷時の設定：255.255.255.0)

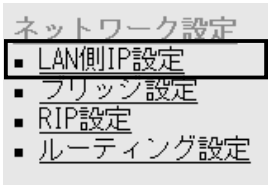
⑤リース期間 ……　DHCPサーバがローカルIPアドレスを定期的に自動でパソコンに割り当てなおす期限を時間で指定します。
設定できる範囲は、「1～9999」です。　(出荷時の設定：72)

⑥ドメイン名 ……　指定のドメイン名を設定する必要があるときは、DHCPサーバが有線で接続するパソコンに通知するネットワークアドレスのドメイン名を127文字(半角英数字)以内で入力します。

1 「ネットワーク設定」メニュー

1-1.「LAN側IP設定」画面

■DHCPサーバ設定(つづき)



DHCPサーバ設定		
DHCPサーバ機能を使用	①	○しない ◉する
割り当て開始IPアドレス	②	192.168.0.10
割り当て個数	③	30 個
サブネットマスク	④	255.255.255.0
リース期間	⑤	72 時間
ドメイン名	⑥	
デフォルトゲートウェイ	⑦	192.168.0.1
プライマリDNSサーバ	⑧	
セカンダリDNSサーバ	⑨	
プライマリWINSサーバ	⑩	
セカンダリWINSサーバ	⑪	

⑦ デフォルトゲートウェイ … ネットワーク管理者から指定されたときなど、必要に応じて、有線(LAN)側に通知するゲートウェイを入力します。
(出荷時の設定：192.168.0.1)

⑧ プライマリDNSサーバ …… 本製品のDHCPサーバ機能を使用する場合に有効な機能で、必要に応じて使い分けたいDNSサーバのアドレスが2つある場合は、優先したい方のアドレスを入力します。
入力すると、本製品のIPアドレスの代わりに設定したDNSサーバアドレスをDHCPクライアントに通知します。

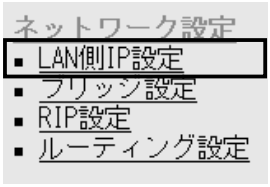
⑨ セカンダリDNSサーバ …… [プライマリDNSサーバ]欄と同様に、使い分けたいDNSサーバアドレスのもう一方を入力します。

⑩ プライマリWINSサーバ … Microsoftネットワークを使ってWINSサーバを利用する場合は、WINSサーバアドレスを入力します。
WINSサーバのアドレスが2つある場合は、優先したい方のアドレスを入力します。

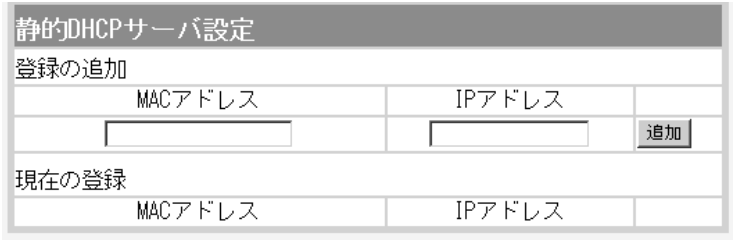
⑪ セカンダリWINSサーバ … 「プライマリWINSサーバ」と同様、WINSサーバのアドレスが2つある場合は、残りの一方を入力します。

1-1.「LAN側IP設定」画面(つづき)

■ **静的DHCPサーバ設定**



特定のパソコンに割り当てるIPアドレスを固定するときの設定です。



DHCPサーバ機能を使用して、自動的に割り当てるIPアドレスを特定のパソコンに固定するとき、パソコンのMACアドレスとIPアドレスの組み合わせを登録する欄です。

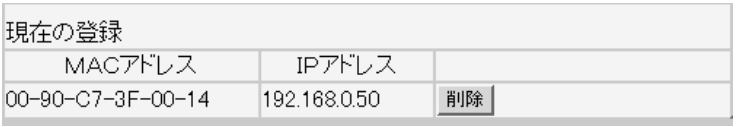
※入力後は、〈追加〉をクリックしてください。

※最大16個の組み合わせまで登録できます。

登録するパソコンのIPアドレスは、DHCPサーバ機能による割り当て範囲および本製品のIPアドレスと重複しないように指定してください。

【登録例】

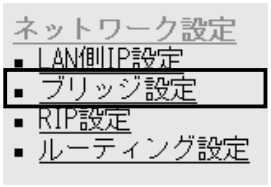
登録した内容を取り消すときは、該当する欄の〈削除〉をクリックします。



1-2.「ブリッジ設定」画面

■ ブリッジ設定

ブリッジ接続でスパニングツリー機能を設定するとき使用します。



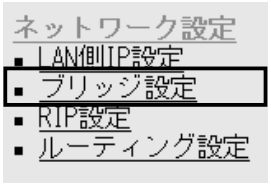
〈登録〉ボタン …… [ブリッジ設定]項目で変更した内容を画面上で確定するボタンです。
※〈登録して再起動〉をクリックするまで有効になりません。

〈取消〉ボタン …… [ブリッジ設定]項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

〈登録して再起動〉ボタン …… 本製品を再起動して、[ブリッジ設定]項目で変更したすべての設定内容を有効にします。

① スパニングツリー機能を使用 …… 経路のループを検出し、パケットが無限に循環するのを回避して、最適な経路を作成する機能を使用するかしないかを設定します。
(出荷時の設定：しない)
スパニングツリー機能を設定すると、経路障害のないときは、冗長リンクを検出して重複する経路のうち優先度の低い方を遮断します。
ブリッジ間で経路障害が起こったときは、正常時に遮断されていた経路を使用してネットワークの正常な稼働を保証します。

1-2.「ブリッジ設定」画面
■ブリッジ設定(つづき)



②ブリッジ優先度 ……
※出荷時の設定でご使用されることを推奨します。

ブリッジで通信する本製品の優先度を決定する値で、設定値が小さいほど、優先度が高くなります。
設定できる範囲は「0～65535」で、一番優先度が高いAP-50が、そのネットワークのルートブリッジになります。
(出荷時の設定：32768)
※同じ値が設定された機器がある場合は、MACアドレスの小さい機器の優先度が高くなります。

③エージングタイム ……
※出荷時の設定でご使用されることを推奨します。

本製品が自動学習したMACアドレスをアドレステーブルに記憶しておく時間を指定します。　(出荷時の設定：300)
設定できる範囲は、「15～1000000(秒)」です。
データが流れない状態が、この欄に設定された時間つづくと、アドレステーブルから削除されます。

④マックスエイジ ……
※出荷時の設定でご使用されることを推奨します。

BPDU(Bridge Protocol Data Unit)を指定します。
設定できる範囲は、「6～40(秒)」です。　(出荷時の設定：20)

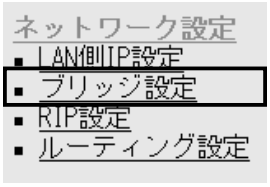
⑤ハロータイム ……
※出荷時の設定でご使用されることを推奨します。

本製品がルートブリッジとして動作するとき、本製品からBPDU情報を送出する間隔を設定します。
設定できる範囲は、「1～10(秒)」です。　(出荷時の設定：2)

⑥転送遅延 ……
※出荷時の設定でご使用されることを推奨します。

ネットワークの再編成中に学習したMACアドレスの有効期限を指定します。
設定できる範囲は、「4～30(秒)」です。　(出荷時の設定：15)

1-2.「ブリッジ設定」画面
■ブリッジ設定(つづき)



⑦パスコスト ……
※出荷時の設定でご使用されることを推奨します。

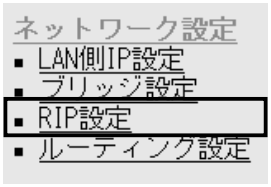
ネットワーク全体のブリッジとルートブリッジ間の優先データパスの決定に利用される値で、各ポートからルートブリッジまでの経路コストが小さいブリッジが優先されます。
設定できる範囲は、「1～65536」です。
(出荷時の設定：有線LAN：100/無線LAN：200)

⑧ポート優先度 ……
※出荷時の設定でご使用されることを推奨します。

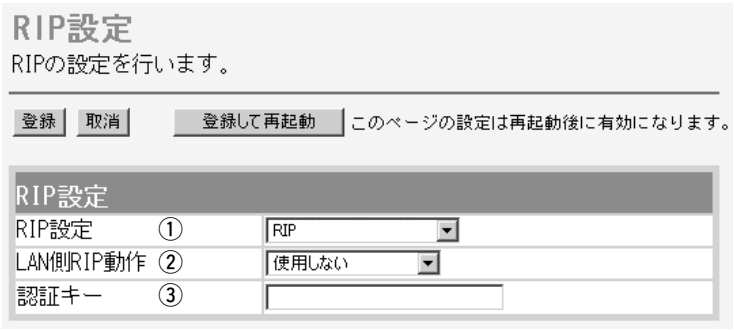
ブリッジで通信する本製品のポートごとに優先度を決定する値で、設定値が小さいほど、ポート優先度が高くなります。
設定できる範囲は、「0～255」です。
(出荷時の設定：有線LAN：128/無線LAN：128)
※各ポートで同じ値が設定されている場合は、物理的なポート番号の小さい順に優先度が高くなります。

1-3.「RIP設定」画面

■RIP設定



隣接ルータやアクセスポイントと経路情報を交換して、経路を動的に作成するときに使用します。



〈登録〉ボタン …… 「RIP設定」画面で変更した内容を画面上で確定するボタンです。
※〈登録して再起動〉をクリックするまで有効になりません。

〈取消〉ボタン …… 「RIP設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

〈登録して再起動〉ボタン …… 本製品を再起動して、「RIP設定」画面で変更したすべての設定内容を有効にします。

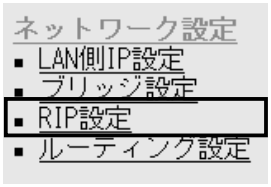
①RIP設定 …… RIPの種類を選択します。　(出荷時の設定：RIP)
◎RIP：　RIPの「Version1」を使用します。
◎RIP2(マルチキャスト)：
RIPの「Version2」を使用して、マルチキャストアドレスにパケットを送信します。
◎RIP2(ブロードキャスト)：
RIPの「Version2」を使用して、ブロードキャストアドレスにパケットを送信します。

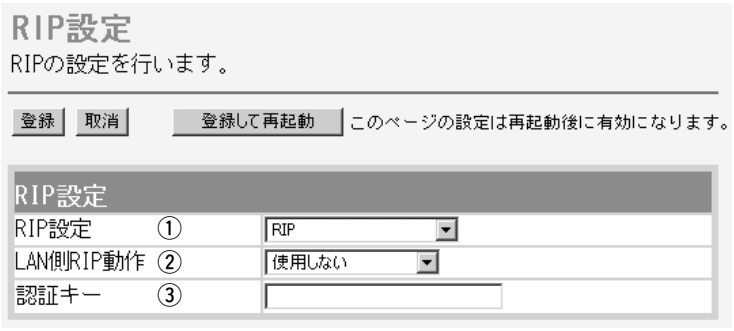
【RIP2について】
RIP2は、可変長サブネットマスクに対応していますので、イントラネット環境でも利用できます。
受信については、ブロードキャスト/マルチキャストの区別なく受け入れます。

②LAN側RIP動作 …… [RIP設定]欄で選択したLAN側のRIP動作について、「使用しない」、「受信のみ」、「受信も送信も行う」から選択します。
(出荷時の設定：使用しない)

1-3.「RIP設定」画面

■RIP設定(つづき)





③認証キー ……

[RIP設定](①)欄で、「RIP2(マルチキャスト)」または「RIP2(ブロードキャスト)」を設定する場合、そのRIP動作を認証するためのキーを入力します。

入力は、大文字/小文字の区別に注意して、半角15文字以内で入力します。

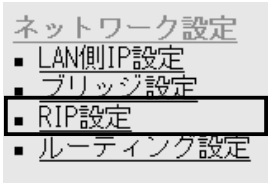
また、他のルータやアクセスポイントに設定されている認証キーと同じ設定にします。

認証キーを設定すると、「RIP」を設定しているゲートウェイと、異なる認証キーを設定している「RIP2」、および認証キーを設定していない「RIP2」ゲートウェイからのRIPパケットを破棄します。

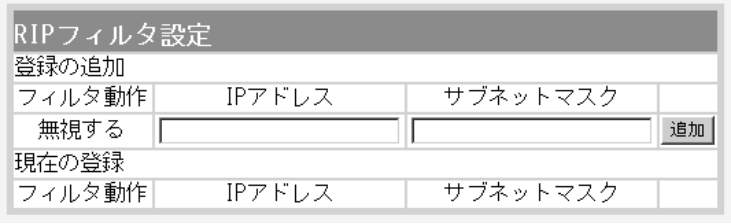
※[LAN側RIP動作](②)欄で「使用しない」を設定、または[RIP設定](①)欄で「RIP」を設定する場合は、空白にします。

1-3.「RIP設定」画面(つづき)

■RIPフィルタ設定



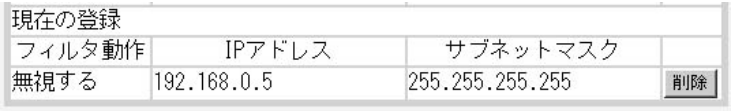
RIPフィルターについての設定です。



同一サブネットで使う複数のアクセスポイントやルータにおいて、特定のアクセスポイントやルータが出力するRIPパケットを受信しないように、そのパケットを出力するアクセスポイントやルータのIPアドレスとサブネットマスクを入力します。
最大16件の登録が可能です。
※入力後は、〈追加〉をクリックしてください。

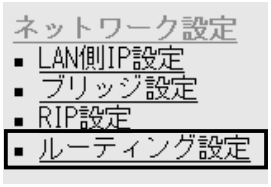
【登録例】

登録した内容を取り消すときは、該当する欄の〈削除〉をクリックします。



1-4.「ルーティング設定」画面

■ IP経路情報



ルータがパケットの送信において、そのパケットをどのルータ、またはどの端末に配送すべきかの情報を表示します。
この項目には、[スタティックルーティング設定]項目で追加した経路も表示されます。

IP経①情報

② 宛先	③ サブネットマスク	④ ゲートウェイ	⑤ 経路	⑥ 作成	メトリック
192.168.0.0	255.255.255.0	192.168.0.1	local	static	0
192.168.0.0	255.255.255.255	255.255.255.255	local	misc	0
192.168.0.1	255.255.255.255	192.168.0.1	local	static	0
192.168.0.255	255.255.255.255	255.255.255.255	local	misc	0

① 宛先 …… ルーティングの対象となるパケットの宛先IPアドレスを表示します。

② サブネットマスク …… ルーティングの対象となるパケットの宛先IPアドレスに対するサブネットマスクを表示します。

③ ゲートウェイ …… ルーティングの対象となるパケットの宛先IPアドレスに対するゲートウェイを表示します。

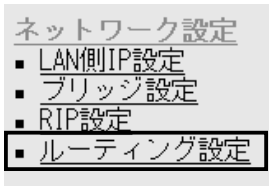
④ 経路 …… ルーティングの対象となるパケットの宛先IPアドレスに対する転送先インターフェイスを表示します。
◎ local：インターフェイスがLAN側(本製品)の場合です。
インターフェイスの詳細は、「情報表示」メニューの「ネットワーク情報」画面にある[ネットワーク インターフェイス リスト]項目に表示します。

⑤ 作成 …… どのように経路情報が作成されたかを表示します。
◎static：スタティック(定義された)ルートにより作成
◎rip　　：ダイナミック(自動生成された)ルートにより作成
◎misc　：ブロードキャストに関係するフレーム処理で作成

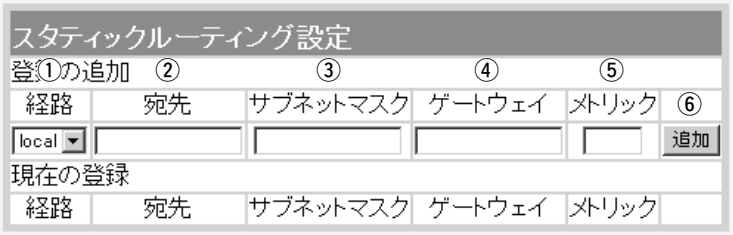
⑥ メトリック …… [スタティックルーティング設定]項目の[メトリック]欄で設定された値やダイナミックルーティングで作成された経路のコストを表示します。

1-4.「ルーティング設定」画面(つづき)

■ **スタティックルーティング設定**



パケットの中継経路を、意図的に定義するルーティングテーブルです。
登録できるのは、最大32件までです。



①経路 …… 回路の経路を指定します。
◎ local：登録する経路情報がLAN側(本製品)の場合です。

②宛先 …… 経路にLAN側を選択したときは、対象となる相手先のIPアドレスを入力します。
経路にWAN側を選択したときは、対象となる相手先のネットワークIPアドレスを入力します。
※IPアドレスは、ゲートウェイのネットワーク部と同じ設定にします。

③サブネットマスク …… 対象となる宛先のIPアドレスに対するサブネットマスクを入力します。

④ゲートウェイ …… ルーティングの対象となるパケット転送先ルータのゲートウェイを入力します。
※入力は、[経路]欄で入力したIPアドレスのネットワーク部と同じ設定にします。

⑤メトリック …… 宛先までのコストを表す数値を入力します。
数値が小さければ転送能力の高い回線と見なされ、数値が大きければ転送能力が低い回線と見なされます。
0(空白)～15まで入力できます。

⑥〈追加〉 …… 設定した内容で[IP経路情報]項目に登録します。
※操作後は、[現在の登録]欄に登録されたことを確認してください。
登録されると、その内容は[IP経路情報]項目に表示されます。

「無線LAN設定」メニュー

第2章

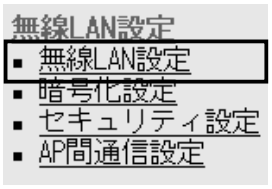
MACアドレスセキュリティー、無線端末間通信禁止機能、無線ネットワーク名、RADIUS認証、暗号化セキュリティー、無線AP間通信機能の設定を行います。

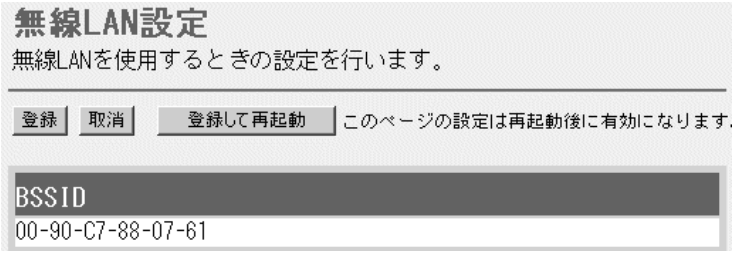
2 「無線LAN設定」メニュー

2-1.「無線LAN設定」画面

■BSSID

本製品に内蔵された無線LANカードの[BSSID]を表示します。





〈登録〉ボタン …… [無線LAN設定]項目で変更したすべての設定内容が有効になります。

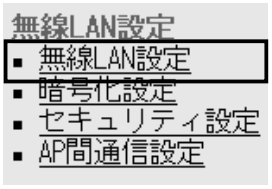
〈取消〉ボタン …… [無線LAN設定]項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

〈登録して再起動〉ボタン …… 本製品を再起動して、「無線LAN設定」画面で変更したすべての設定内容が有効になります。

BSSID …… 本製品では、「情報表示」メニューの「ネットワーク情報」画面に表示される[本体MACアドレス]と同じものを表示します。

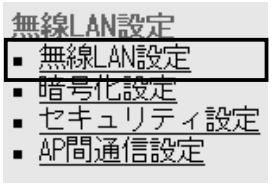
■無線LAN設定

本製品に内蔵された無線LANカードに対する設定です。



①SSID…… 無線ネットワークのグループ分けをするために使用します。
無線ルータや無線アクセスポイントが無線伝送エリア内に複数存在しているような場合、個々の無線ネットワークグループを[SSID(無線ネットワーク名)]で識別したり、異なる無線ネットワーク名で通信するグループからの混信を防止できます。
この[SSID]が異なると本製品と無線で通信できません。
大文字/小文字の区別に注意して、任意の英数字、半角31文字以内で入力します。 (出荷時の設定：LG)
※[SSID]と[ESS ID]は、同じ意味で使用しています。
本製品以外の無線LAN機器では、[ESS ID]と表記されている場合があります。

2-1.「無線LAN設定」画面
■無線LAN設定(つづき)



無線LAN設定		
SSID	①	LG
ANYを拒否	②	◉しない ○する
VLAN ID	③	
チャンネル	④	11 (2462MHz)
Rts/Ctsスレッシュホールド	⑤	無し
11g保護機能	⑥	無効
パワーレベル	⑦	高
接続端末制限	⑧	255
Super A/Gを使用	⑨	しない

②ANYを拒否 ……

「ANY」モード(アクセスポイント自動検索接続機能)で動作している無線パソコンからの検索や接続を拒否するかしないかを設定します。　(出荷時の設定：しない)
出荷時の設定では、弊社製無線LANカード(SL-11やSL-110を除く)を装着するパソコンとの接続が容易になるように、これらの無線パソコンからの検索や接続を許可しています。
この設定を「する」にした場合、「ANY」モードで通信する無線パソコンが使用する「Windows XP標準のワイヤレスネットワーク接続」や「無線ネット表示に対応する弊社製無線LANカードに付属の設定ユーティリティー」に検索されません。
※ご使用のパソコンにSL-50(ドライバーのVer.1.34以降)やSL-5000、SL-5000XG、SL-5100、SL-5200をインストールしたときは、出荷時から「ANY」モードで動作しています。

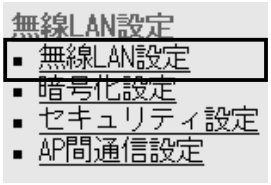
③VLAN ID ……

[SSID]の無線グループに[VLAN ID]を設定して、有線ネットワークとのあいだで仮想ネットワークを構成するとき使用します。
「無線LAN設定」画面に設定された[SSID](出荷時の設定：LG)に所属する無線グループのID番号を設定します。
設定できる範囲は、「1～4094」です。
※この画面に設定したID番号は、「ネットワーク設定」メニューの「LAN側IP設定」画面にある[VLAN ID設定]項目で、[VLANを使用]欄を「する」に設定すると有効になります。(☞P6)
※次ページの図に示すように、同じID番号が設定された有線ネットワークと無線ネットワークだけが、本製品を介して通信できます。
異なるID番号のネットワークとは通信できません。
[VLAN ID]が「20」の有線ネットワークと通信できる無線グループを追加して、本製品を複数の無線グループで使用する場合は、[仮想BSS設定]項目で、異なる[SSID]とID番号を登録することで、本書32ページの図に示すようなネットワーク構成で使用できます。

2 「無線LAN設定」メニュー

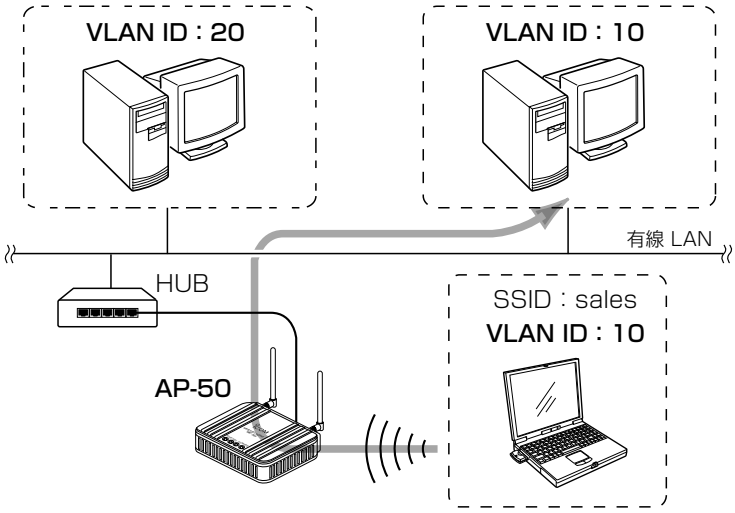
2-1.「無線LAN設定」画面

■無線LAN設定(つづき)



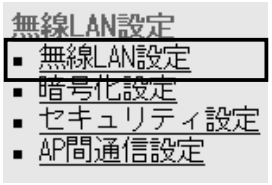
無線LAN設定		
SSID	①	LG
ANYを拒否	②	◉しない ○する
VLAN ID	③	
チャンネル	④	11 (2462MHz)
Rts/Ctsスレッシュホールド	⑤	無し
11g保護機能	⑥	無効
パワーレベル	⑦	高
接続端末制限	⑧	255
Super A/Gを使用	⑨	しない

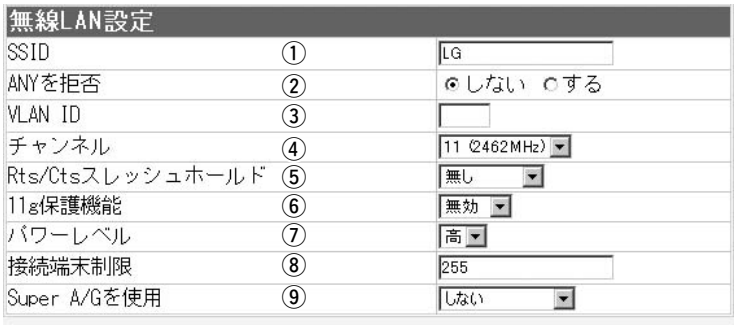
③VLAN ID(つづき) ……



2-1.「無線LAN設定」画面

■無線LAN設定(つづき)





無線LAN設定		
SSID	①	LG
ANYを拒否	②	◉しない ○する
VLAN ID	③	
チャンネル	④	11 (2462MHz)
Rts/Ctsスレッシュホールド	⑤	無し
11g保護機能	⑥	無効
パワーレベル	⑦	高
接続端末制限	⑧	255
Super A/Gを使用	⑨	しない

④チャンネル ……

本製品が無線通信に使用するチャンネルを設定します。

(出荷時の設定：11(2462MHz))

◎2.4GHz帯(IEEE802.11b/g規格)で通信するときは、「1～13」チャンネルを選択します。

◎5.2GHz帯(IEEE802.11a規格)で通信するときは、「34、38、42、46」チャンネルの中から選択します。

※無線パソコン側は、本製品のチャンネルを自動的に検知して通信します。

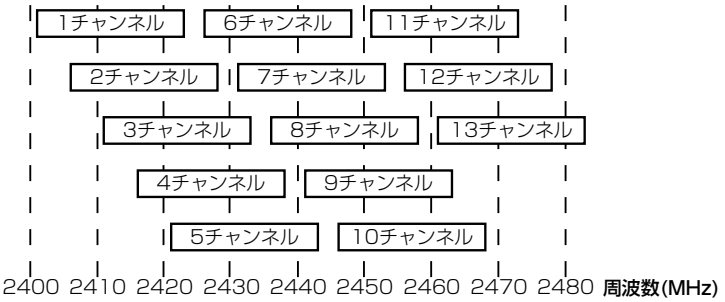
※本製品どうしを無線AP間通信(☞2-4章)するときは、相手の無線アクセスポイントと同じチャンネルに設定してください。

☞次ページにつづく近くに2.4GHz帯(IEEE802.11b/g)の無線アクセスポイント機能で通信する別の無線ネットワークグループが存在するときは、電波干渉を避けるため、本製品の「チャンネル」は、別の無線ネットワークグループと4チャンネル以上空けて設定してください。

それ以下のときは、図に示すように帯域の1部が重複するため混信する可能性があります。

例えば、お互いの設定が、1-6-11チャンネルに設定すると混信しません。

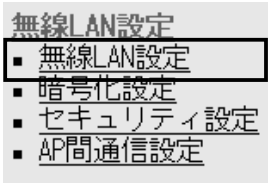
※5.2GHz帯(EEE802.11a)で通信する場合は、お互いを異なるチャンネルに設定すれば、チャンネル間の電波干渉に配慮する必要はありません。



2 「無線LAN設定」メニュー

2-1.「無線LAN設定」画面

■無線LAN設定(つづき)



無線LAN設定		
SSID	①	LG
ANYを拒否	②	◉しない ○する
VLAN ID	③	
チャンネル	④	11 (2462MHz)
Rts/Ctsスレッシュホールド	⑤	無し
11g保護機能	⑥	無効
パワーレベル	⑦	高
接続端末制限	⑧	255
Super A/Gを使用	⑨	しない

⑤Rts/Ctsスレッシュホールド ……

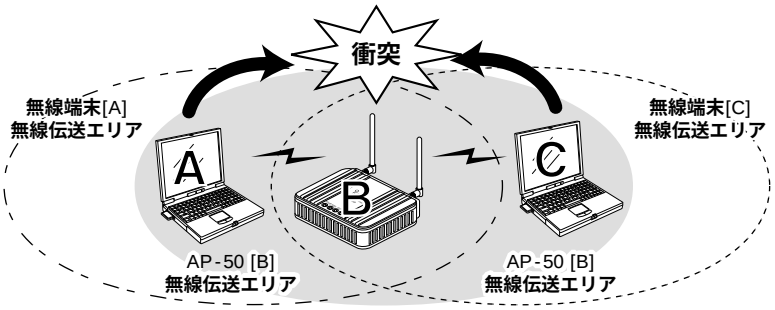
ネゴシエーションするために送るパケットのデータサイズを、「500バイト」または「1000バイト」から選択します。

(出荷時の設定：無し)

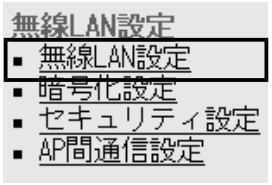
Rts/Cts(Request to Send/Clear to Send)スレッシュホールドを設定すると、隠れ端末の影響による通信速度の低下を防止できます。

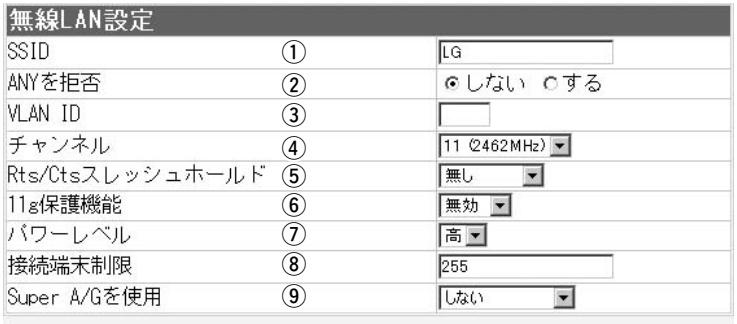
隠れ端末とは、下図のように、それぞれが本製品[B]と無線通信できても、互いが直接通信できない無線端末[A]-[C]同士([A]に対して[C]、[C]に対して[A])のことを呼びます。

通信の衝突を防止するには、無線端末[A]から送信要求(Rts)信号を受信した本製品[B]が、無線伝送エリア内にある無線端末[A]および[C]に送信可能(Cts)信号を送り返すことで、Rts信号を送信していない無線端末[C]に本製品[B]が隠れ端末と通信中であることを認識させます。これにより、Rts信号を送信していない無線端末[C]は、無線ルータ[B]から受信完了通知(ACK)を受信するまで本製品[B]へのアクセスを自制して、通信の衝突を防止できます。



2-1.「無線LAN設定」画面
■無線LAN設定(つづき)





⑥ 11g保護機能 ……

アクセスしてくる無線パソコンの無線LANの規格を認識して、接続を制限できます。　(出荷時の設定：無効)
接続制限することで、[IEEE802.11b(11Mbps)]規格の通信を制限して、[IEEE802.11g(54Mbps)]規格の通信に影響されないように保護します。

◎「無効」：[IEEE802.11g]規格または[IEEE802.11b]規格の無線パソコンと通信できます。
◎「有効」：[IEEE802.11b]規格と混在するネットワーク環境で、[IEEE802.11g]規格の通信速度が極端に遅い場合に設定します。
「有効」に設定すると、[IEEE802.11g]規格の無線パソコンとの通信を優先させます。
優先させることで、[IEEE802.11g]規格の通信速度が低下することを防止できます。
◎「g専用」：[IEEE802.11g]規格の無線パソコンとだけ通信できます。

⑦ パワーレベル ……

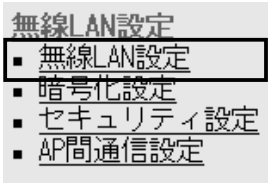
本製品に内蔵された無線LANカードの送信出力を設定します。
高/中/低(3段階)の中から選択できます。　(出荷時の設定：高)
本製品の最大伝送距離は、パワーレベルが「高」の場合です。
パワーレベルを低くすると、それに比例して伝送距離も短くなります。

【パワーレベルを低くする目的について】

◎本製品から送信される電波が部屋の外に漏れるのを軽減したいとき
◎通信エリアを制限してセキュリティーを高めたいとき
◎比較的狭いエリアに複数台の無線アクセスポイントが設置された環境で、近くの無線クライアントや無線アクセスポイントとの電波干渉を無くして、通信速度の低下などを軽減したいとき

2 「無線LAN設定」メニュー

2-1.「無線LAN設定」画面
■無線LAN設定(つづき)



無線LAN設定		
SSID	①	LG
ANYを拒否	②	◉しない ○する
VLAN ID	③	
チャンネル	④	11 (2462MHz)
Rts/Ctsスレッシュホールド	⑤	無し
11g保護機能	⑥	無効
パワーレベル	⑦	高
接続端末制限	⑧	255
Super A/Gを使用	⑨	しない

⑧接続端末制限 ……

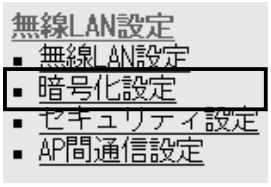
本製品に同時接続可能な無線パソコンの台数を設定します。
設定できる範囲は、「1～255」です。　(出荷時の設定：255)
接続制限を設定すると、本製品1台だけに接続が集中するのを防止(本製品の負荷を分散)できますので、接続集中による通信速度低下を防止できます。

⑨Super A/Gを使用……

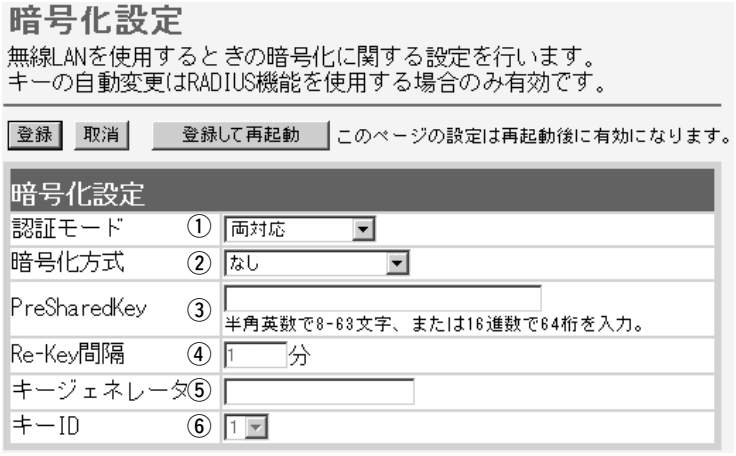
米国Atheros Communications社が開発した、独自の無線LAN高速化技術です。　(出荷時の設定：しない)
「しない」、「する(圧縮なし)」、「する(圧縮あり)」から選択できます。
「する(圧縮あり)」を選択すると、通信速度がさらに向上します。
※すでに圧縮されているデータを取り扱う機会が多い場合、「する(圧縮あり)」を使用すると、圧縮されたデータを転送しているあいだは、速度が低下する原因となります。
このような場合は、「する(圧縮なし)」に設定してご使用ください。
※[Super A/G]の設定を「する(圧縮あり)」に設定して、無線AP間通信機能と暗号化[WEP(RC4)、OCB AES]機能を併せて使用する場合は、[キーID](☞P30)の設定を無線AP間通信する相手と同じ設定にしてください。
通信相手と異なる[キーID]を設定すると、通信できなくなります。
※無線パソコンに装着された無線LANカードが、Super A/Gに対応していない場合は、[Super A/G]を使用しないときと同じ状態になります。
※「SuperA」と「SuperG」は、別々に設定できません。

2-2.「暗号化設定」画面

■暗号化設定



無線LANで通信するデータを保護するために、暗号化するための設定です。



〈登録〉ボタン ……　「暗号化」画面で変更した内容を画面上で確定するボタンです。
変更した内容は、〈登録して再起動〉をクリックするまで有効になりません。

〈取消〉ボタン ……　「暗号化」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉や〈登録して再起動〉をクリックすると、変更前の状態には戻りません。

〈登録して再起動〉ボタン ……　本製品を再起動して、「暗号化」画面で変更したすべての設定内容を有効にします。

① 認証モード ……　[暗号化方式](②)欄で、「WEP RC4 64(40)」、「WEP RC4 128(104)」、「WEP RC4 152(128)」、「OCB AES 128(128)」を選択したとき、その暗号化を使用する無線LANからのアクセスに対する認証方式を設定します。

(出荷時の設定：両対応)

※通信相手と認証モードが異なると通信できません。

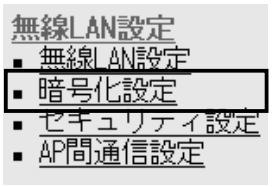
◎両対応　：無線LANのアクセスに対して、「オープンシステム」と「シェアードキー」を自動認識しますので、通信相手間で暗号化鍵(キー)が同じであれば通信可能です。

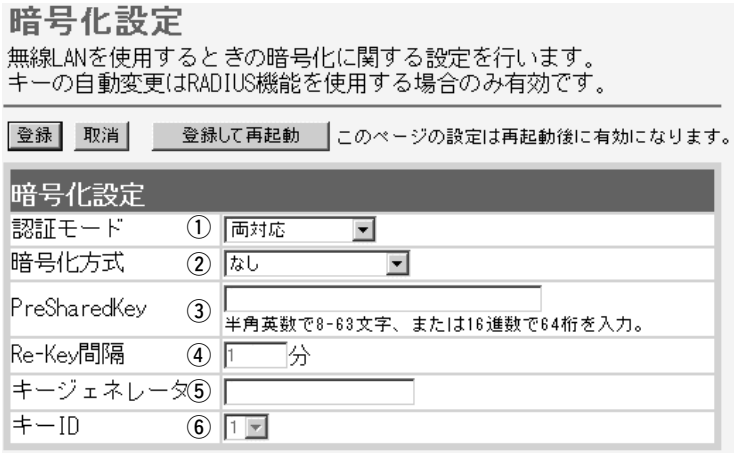
◎オープンシステム：無線LANのアクセスに対して認証を行いません。

◎シェアードキー　：無線LANのアクセスに対して通信相手と同じ暗号化鍵(キー)かどうかを認証します。

2-2.「暗号化設定」画面

■暗号化設定(つづき)





② 暗号化方式 …… 無線伝送データを暗号化する方式を選択します。

(出荷時の設定：なし)

対応する暗号化方式は、「WEP RC4」、「OCB AES」、「WPA-PSK(TKIP/AES)」です。

異なる暗号化方式の相手とは互換性がありませんので、暗号化方式とビット数は、通信を行う相手間で、同じ設定にしてください。

※Windows XP標準のワイヤレスネットワーク接続で対応していない暗号化[WEP RC4 152(128)/(OCB AES)]方式での接続は、弊社製無線LANカードに付属の設定ユーティリティーをご使用ください。

◎WEP RC4：

無線通信で一般によく使用されるセキュリティーです。

暗号化方式は、WEP RC4(Rivest's Cipher 4)アルゴリズムをベースに構成されています。

暗号化するデータのブロック長が8ビットで、暗号化鍵(キー)の長さを選択できます。

※暗号化鍵(キー)の長さは、64(40)/128(104)/152(128)ビットの中から選択できます。

※「WEP RC4 152(128)」方式は、Windows XP標準のワイヤレスネットワーク接続を使用して本製品に接続できません。

◎OCB AES：

[WEP RC4]より強力で、標準化が推進されている次世代の暗号化方式です。

※Windows XP標準のワイヤレスネットワーク接続を使用して本製品に接続できません。

◎WPA-PSK(TKIP/AES)：

「WPA-PSK」は、Windows XP(Service Pack1)に修正プログラムが適用されたパソコンで使用できる共有鍵認証方式です。

暗号化方式は、「TKIP」と「AES」に対応しています。

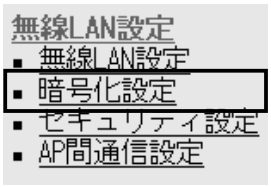
※無線AP間通信機能を利用する場合、併せて使用できませんので、「WEP(RC4)/OCB AES」方式でご使用ください。

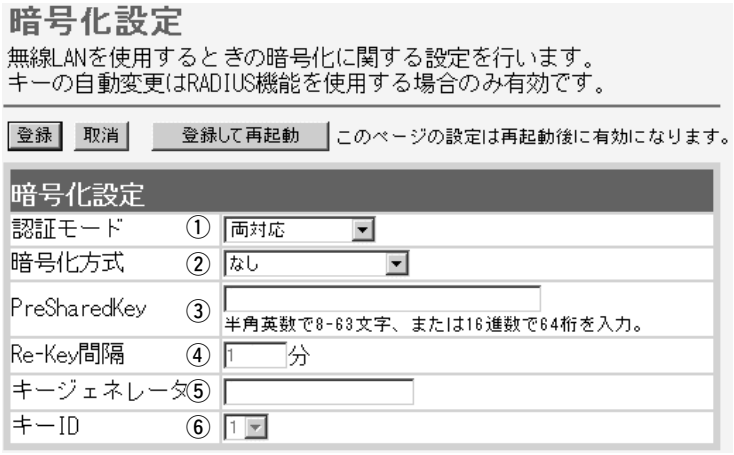
※SL-5200(弊社製無線LANカード)が装着されたWindows XP搭載のパソコンをご使用いただくと、Windows XP標準のワイヤレスネットワーク接続から本製品に接続できます。

※「TKIP」と「AES」は、互換性がありません。

※「WEP(RC4)/OCB AES」とは、互換性がありません。

2-2.「暗号化設定」画面
■暗号化設定(つづき)





③PreSharedKey……　[暗号化方式](②)欄で、「WPA-PSK(TKIP)」、または「WPA-PSK(AES)」を選択したとき、暗号化鍵(キー)を半角英数字で入力します。
※同じ暗号化方式を使用する相手と同じ暗号化鍵(キー)を設定してください。
※16進数で設定するときは、64桁を入力してください。
※ASCII文字で設定するときは、8～63文字を入力してください。

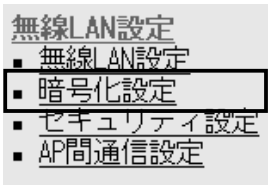
④Re-Key間隔　……　「WPA-PSK(TKIP)」、または「WPA-PSK(AES)」方式の暗号化を設定する場合、暗号化鍵(キー)の更新間隔を分単位で指定します。　(出荷時の設定：1分)
設定できる範囲は、「0～1440」です。
※「0」を設定した場合は、更新されません。

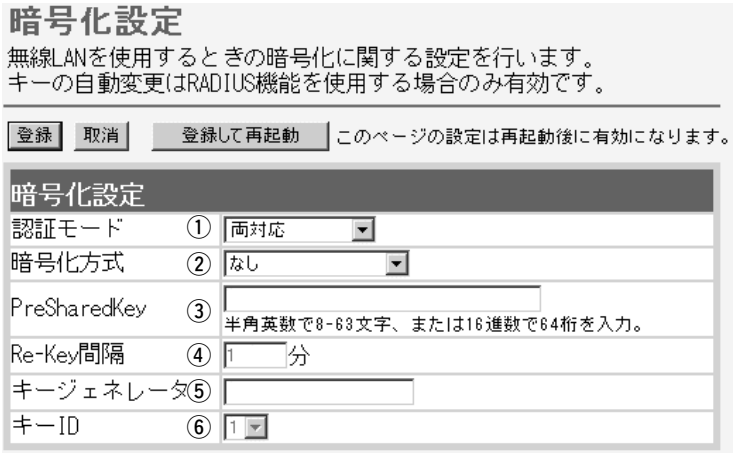
⑤キージェネレータ　……　[暗号化方式](②)欄で、「WEP RC4 64(40)」、「WEP RC4 128(104)」、「WEP RC4 152(128)」、「OCB AES 128(128)」を選択したとき、暗号化および復号に使う暗号化鍵(キー)を生成するための文字列を設定します。
通信を行う相手間で同じ文字列(大文字/小文字の区別に注意して、任意の半角英数字/記号)を31文字以内で設定します。
なお、入力した文字はすべて「＊」で表示します。　(表示例：＊＊)
「暗号化方式」を選択して、〈登録〉をクリックすると、[キージェネレータ]欄に入力した文字列より生成された鍵(キー)を[キー値]項目のテキストボックスに表示します。
[キー値]項目の各キー番号のテキストボックスに生成される桁数および文字数は、選択する「暗号化方式」によって異なります。
(取扱説明書[導入編]☞3-6章を参照)

☞次ページにつづく

2-2.「暗号化設定」画面

■暗号化設定(つづき)





⑤キージェネレータ(つづき)

※「WEP RC4」の場合、先頭の24ビットは、一定時間ごとに内容を自動更新して設定されますので、「キー値」項目のテキストボックスには表示されません。

※[キー値]項目の[入力モード]が「ASCII文字」に設定されている場合は、キージェネレータを使用できません。

※[暗号化方式]欄で「なし」が選択されていると、[キー値]項目の各キー番号のテキストボックスに鍵(キー)が生成されません。

※通信相手間で文字列が異なる場合、暗号化されたデータを復号できません。

※[キー値]項目から直接設定するときは、[キージェネレータ]欄には何も表示されません。

⑥キーID ……

[暗号化方式](②)欄で、「WEP RC4 64(40)」、「WEP RC4 128(104)」、「WEP RC4 152(128)」、「OCB AES 128(128)」を選択したとき、[キー値]項目の「1」～「4」に設定された暗号化鍵(キー)のうち送信データの暗号化に使用する鍵(キー)を、テキストボックスの番号で指定します。

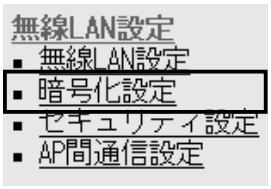
(出荷時の設定：1)

「1」～「4」に設定された暗号化鍵(キー)の内容が通信相手と同じであれば、通信する相手間で異なる番号を指定しても通信できます。

※本製品に無線LANで接続するパソコンの[キーID]を設定するとき、Windows XP(Service Pack1を除く)標準のワイヤレスネットワーク接続を使用する場合は、[キーID]の選択範囲が「0」～「3」で、本製品とは異なりますので注意してください。
本製品で「1」を選択した場合は、Windows XPの[キーインデックス(詳細)(X)]で「0」を設定するのと同じ意味になります。

2-2.「暗号化設定」画面(つづき)

■ **キー値**



「WEP RC4」、または「OCB AES」方式の暗号化で使用する暗号化鍵(キー)の設定です。

① 入力モード …… 暗号化鍵(キー)の入力のしかたを選びます。

(出荷時の設定：16進数)

※入力モードを変更したときは、「暗号化設定」画面の〈登録〉ボタンをクリックしてから、暗号化鍵(キー)を入力してください。

※ASCII文字が設定されているときは、[暗号化設定]項目の[キージェネレータ]を使用できません。

② 鍵(キー)入力用ボックス … キージェネレータを使用しない場合やASCII文字で入力するときは、暗号化および復号化に使用する鍵(キー)を、[入力モード](①)欄で設定された方法で、直接入力します。

(出荷時の設定：00-00-00-00-00)

※16進数以外のアルファベットは、入力しても無効です。

※暗号化鍵(キー)は、通信する相手間で、すべての[キーID(1～4)]値に対して同じ内容に設定することをお勧めします。
異なる設定の場合、通信相手間で[キーID]値の設定が異なると、通信できないことがあります。

③ デフォルトキー ……

※[無線LAN設定]項目の[Super A/Gを使用]欄で、「する(圧縮あり)」を設定している場合は、この設定を仮想BSSの通信に使用できません。

「ネットワーク設定」メニューの「LAN側IP設定」画面にある[VLAN ID設定]項目で、[VLANを使用]欄を「する」に設定し、仮想BSSで無線ネットワークグループを構成する場合、「無線LAN」画面にある[無線LAN設定]項目の[SSID]欄に設定した無線ネットワークグループが使用する仮想BSSで使用する暗号キーを設定します。
入力のしかたは、[鍵(キー)入力用ボックス](②)と同じです。

※無線パソコン(例：Sales☞P24)で使用する弊社製設定ユーティリティーの[キーID]欄は、「1」(出荷時の設定)に設定し、[キーID：1]の暗号化鍵(キー)を入力するテキストボックスには、[デフォルトキー](③)欄と同じ暗号化鍵(キー)を設定してください。

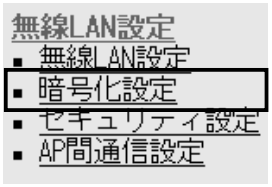
※本製品の「暗号化設定」画面の[キー値]項目にある[2]～[4]の暗号化鍵(キー)は、無線パソコンで使用する弊社製設定ユーティリティーの暗号化鍵(キー)を入力するテキストボックス[2]～[4]と同じ内容にしてください。

※16進数またはASCII文字で入力できます。

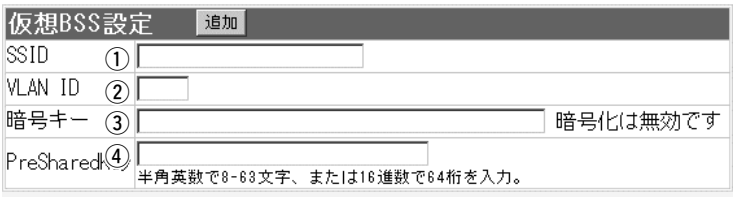
※キージェネレータには対応していません。

2-2.「暗号化設定」画面(つづき)

■仮想BSS設定

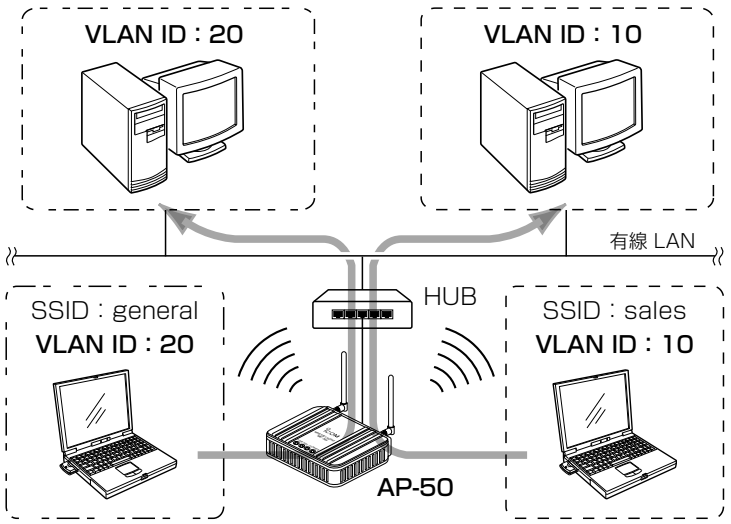


本製品1台で、異なる[SSID]の無線グループを複数構成するとき使用します。



※〈追加〉ボタンをクリックすると、設定した内容が[現在の登録]項目(☞P35)に表示され、最大16グループまで登録できます。

※有線ネットワーク側の[VLAN ID]は、VLAN機能搭載のHUBで設定しているものとします。



①SSID……

仮想BSSで使用する無線ネットワークのグループ分けをするために使用します。 (設定例：general)

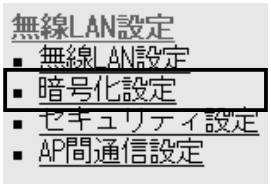
この[SSID]が異なると本製品と仮想無線BSSで通信できません。

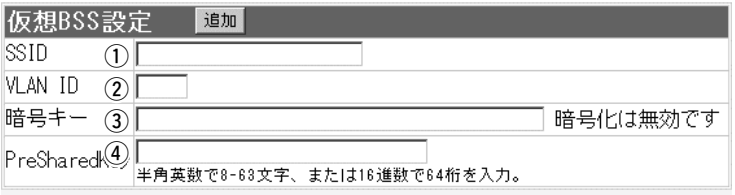
大文字/小文字の区別に注意して、任意の英数字、半角31文字以内で入力します。

※「無線LAN設定」画面で設定されている[SSID](☞P20)と同じものは、登録できません。

※「無線LAN設定」画面で設定されている[SSID](☞P20)も、既存の無線グループ(例：sales)として使用できます。

2-2.「暗号化設定」画面
■仮想BSS設定(つづき)





②VLAN ID ……

※[VLAN ID]だけを使用しない場合は、仮想BSSとして使用できます。

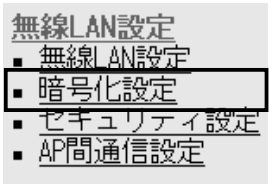
[仮想BSS設定]項目で設定した[SSID](①)に所属する無線グループにID番号を設定します。
設定できる範囲は、「0～4094」です。
同じID番号のネットワークだけが、仮想BSSで通信できます。
※「0」を設定したときは、VLANタグを付けずに送出します。
※異なるID番号のネットワークとは通信できません。
※1つの[SSID]に対して、複数のID番号は登録できません。
※同じ番号の[VLAN ID]を複数の異なる[SSID]に登録できます。
※設定したID番号は、「ネットワーク設定」メニューの「LAN側IP設定」画面にある[VLAN ID設定]項目で、[VLANを使用]欄を「する」に設定すると有効になります。(☞P6)

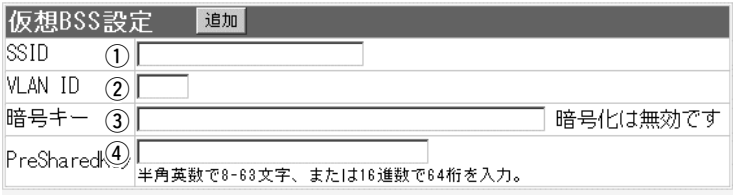
③暗号キー ……

上記画面で設定した[SSID]の無線グループで、「WEP RC4」、または「OCB AES」方式の暗号化で使用する暗号化鍵(キー)を設定します。
※仮想BSS設定で、暗号化を使用する場合は、「暗号化設定」画面の[暗号化設定]項目にある[キーID]欄を「1」(出荷時の設定)以外に変更しないと通信できません。
※無線パソコン(例：General☞P35)で使用する弊社製無線LANカード(例：SL-5200)に付属の設定ユーティリティーで、[キーID]欄は、「1」(出荷時の設定)に設定し、[キーID：1]の暗号化鍵(キー)を入力するテキストボックスには、[暗号キー](③)欄と同じ暗号化鍵(キー)を設定してください。
※本製品の「暗号化設定」画面の[キー値]項目にある[2]～[4]の暗号化鍵(キー)は、無線パソコンで使用する弊社製設定ユーティリティーの暗号化鍵(キー)を入力するテキストボックス[2]～[4]と同じ内容にしてください。
※無線パソコンとして、Windows XP標準のワイヤレスネットワーク接続をご使用の場合は、[PreSharedKey](④)欄をご使用ください。
※[無線LAN設定]項目の[Super A/Gを使用]欄で、「する(圧縮あり)」を設定している場合は、この設定を仮想BSSの通信に使用できません。

2-2.「暗号化設定」画面

■仮想BSS設定(つづき)





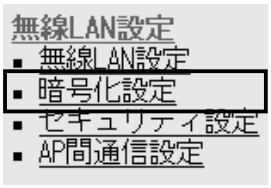
④PreSharedKey…… 上記画面で設定した[SSID]の無線グループで、「WPA-PSK(TKIP)」、または「WPA-PSK(AES)」方式の暗号化で使用する暗号化鍵(キー)を半角英数字で入力します。

※無線パソコンからの接続には、Windows XP標準のワイヤレスネットワーク接続を使用します。

※無線パソコンに弊社製無線LANカード(例：SL-5200)に付属の設定ユーティリティーをご使用の場合は、[暗号キー](③)欄をご使用ください。

2-2.「暗号化設定」画面(つづき)

■現在の登録　　**[仮想BSS設定]項目で登録した内容を表示します。**



現在の登録		③	④	⑤	⑥
①	②	SSID	VLAN ID	暗号キー	PreSharedKey
編集	削除	5100	30	5B-1E-7E-9D-78	
編集	削除	general	20	00-00-00-00-00	wavemaster

①〈編集〉ボタン …… [仮想BSS設定]項目で設定した登録(ボタンの右側に表示されている)内容を編集します。
クリックすると、登録内容が、[仮想BSS設定]項目の各設定欄に移行します。
※再登録するときは、暗号化方式の設定を確認してください。

②〈取消〉ボタン …… [仮想BSS設定]項目で設定した登録(ボタンの右側に表示されている)内容を削除します。

③SSID …… [仮想BSS設定]項目の[SSID]欄で設定した内容を表示します。

④VLAN ID …… [仮想BSS設定]項目の[VLAN ID]欄で設定した内容を表示します。
設定されていないときは、「–」を表示します。

⑤暗号キー …… [仮想BSS設定]項目の[暗号キー]欄で設定した内容を表示します。
設定されていないときは、「00-00-00-00-00」(入力モードが16進数の場合)を表示します。
「暗号化設定」画面の[暗号化設定]項目にある[暗号化方式]欄で、暗号化方式や暗号化ビット数を変更すると、変更前に登録した無線端末の暗号化キーも併せて初期化(表示例：00-00-00-00-00)されますので、再登録が必要になります。

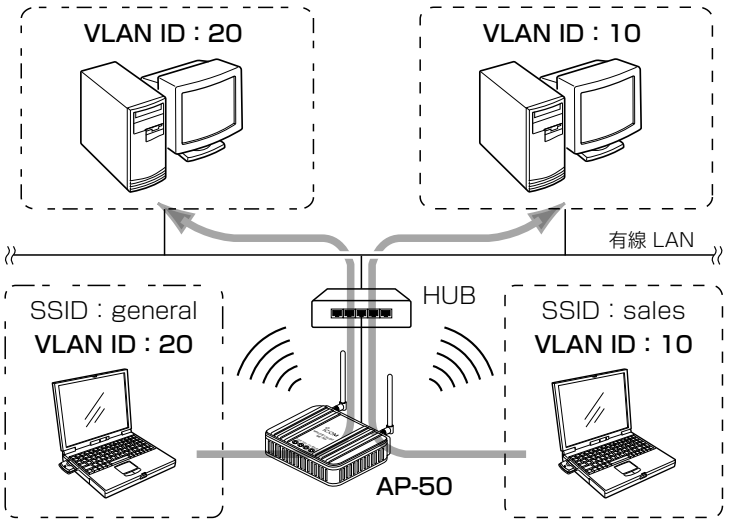
⑥PreSharedKey…… [仮想BSS設定]項目の[PreSharedkey]欄で設定した内容を表示します。

2-2.「暗号化設定」画面(つづき)

■設定例について

無線VLAN設定と仮想BSS設定を併せて使用する場合の登録例を下記の図を例に説明します。

※有線ネットワーク側の[VLAN ID]は、VLAN機能搭載のHUBで設定しているものとします。



【設定条件】

◎[IEEE802.11g]規格の無線LANを使用します。

◎[SSID]が「sales」の無線グループは、〈無線VLAN設定〉(☞P37～38)の手順で設定します。

◎[SSID]が「general」の無線グループは、〈仮想BSS設定〉(☞P39)の手順で設定します。

[WPA-PSK(TKIP/AES)]暗号化を使用する場合について、37～38ページで併せて説明しています。

【暗号化鍵の設定例】

本製品と各無線通信するグループとの暗号化鍵(キー)などの設定は、下記の条件で設定します。

◎[暗号化方式]：「WEP RC4 64(40)」

◎[入力方式]　：「16進数」

◎[キーID]　　：「2」(AP-50側)

※仮想BSSで使用する場合、本製品の[キーID]は、「1」以外(例：2)に設定します。

[キーID]　　：「1」(無線クライアント：「sales」/「general」側)

※無線クライアントの[キーID]は、「1」を設定します。

◎[キーID]が「2」～「4」に対する暗号化鍵(キー)は、本製品と無線クライアント側ですべて同じに設定してください。

〈AP-50側〉

キーID	鍵(キー)
1	00-00-00-00-00
②	0E-C4-7B-1A-EA
3	00-00-00-00-00
4	00-00-00-00-00

デフォルトキー：C0-1E-63-FF-FF

仮想BBSの暗号キー：06-67-93-34-56

〈無線クライアント側〉

〈sales〉

キーID	鍵(キー)
①	C0-1E-63-FF-FF
2	0E-C4-7B-1A-EA
3	00-00-00-00-00
4	00-00-00-00-00

〈general〉

キーID	鍵(キー)
①	06-67-93-34-56
2	0E-C4-7B-1A-EA
3	00-00-00-00-00
4	00-00-00-00-00

無線クライアント側は、弊社製無線LANカードに付属の設定ユーティリティーで、[キーID]、「2」～「4」のテキストボックスのどれか1つ(例：2)に、本製品の[キーID](例：2)のテキストボックスに設定した鍵(キー)と同じものを入力します。

2-2.「暗号化設定」画面

■設定例について(つづき)

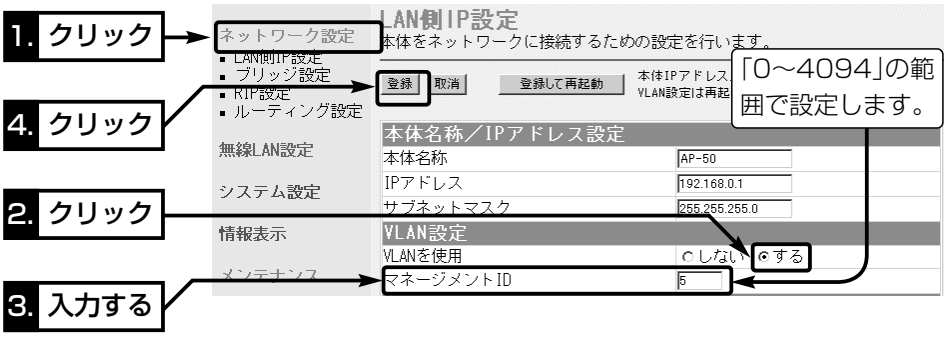
〈無線VLANの設定〉

無線VLANを使用する無線グループに対する設定です。

①「LAN側IP設定」画面の[VLAN設定]項目にある[VLANを使用]欄を「する」に設定します。

※[マネージメントID]欄は、「0～4094」(入力例：5)の範囲でIDを設定します。(「0」を設定すると、タグは付きません。)

②〈登録〉ボタンをクリックします。



③[IEEE802.11g]規格側の「無線LAN設定」画面で、[SSID]欄を「sales」に設定します。

④この画面で設定した[SSID](例：sales)で使用する[VLAN ID]を「10」に設定します。

⑤〈登録〉ボタンをクリックします。

2-2.「暗号化設定」画面

■設定例について〈無線VLANの設定〉(つづき)

⑥[IEEE802.11g]規格側の「暗号化設定」画面にある[暗号化設定]項目で、[暗号化方式]欄を「WEP RC4 64(40)」に設定します。

⑦[キーID]欄を「2」に設定します。

※仮想BSSIDを使用しますので、「1」を[キーID]に設定しないでください。

※無線クライアント側の[キーID]には、「1」を設定します。

⑧〈登録〉ボタンをクリックします。

- [キー値]項目にある「1」～「4」と「デフォルトキー」のテキストボックスに「00-00-00-00-00」と表示されます。

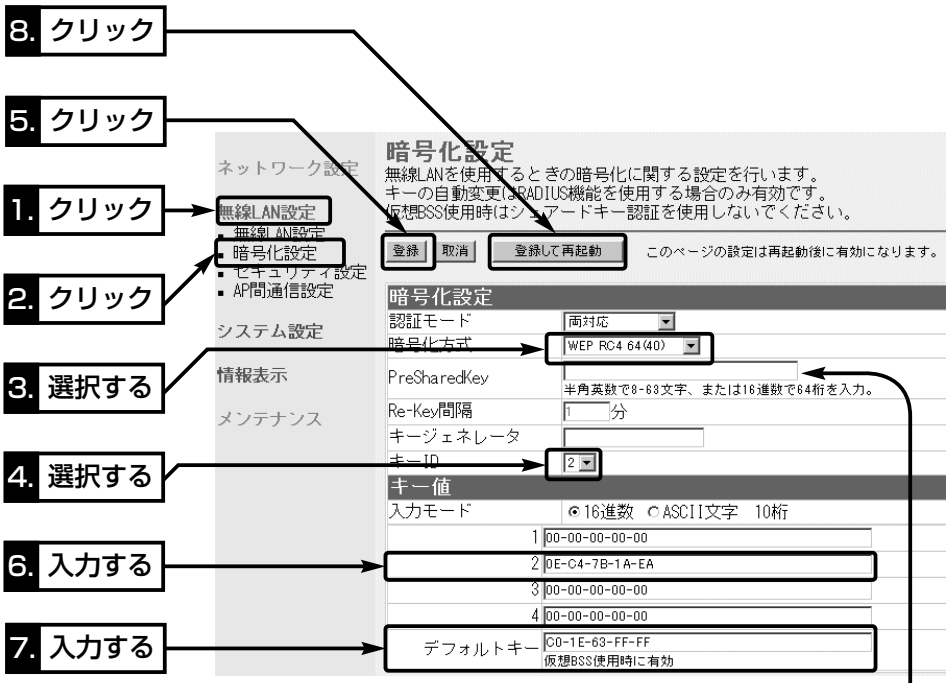
⑨暗号化鍵(キー)を[キー値]項目にある「2」のテキストボックスに入力します。

※無線クライアント側の[キーID]が「2」のテキストボックスにも同じ暗号化鍵(キー)を設定します。

⑩無線VLANで使用する暗号化鍵(キー)を[キー値]項目にある「デフォルトキー」のテキストボックスに入力します。

※無線クライアント(Sales)側の[キーID]が「1」のテキストボックスにも同じ暗号化鍵(キー)を設定します。

⑪〈登録して再起動〉ボタンをクリックします。



[WPA-PSK(TKIP/AES)]暗号化を使用する場合

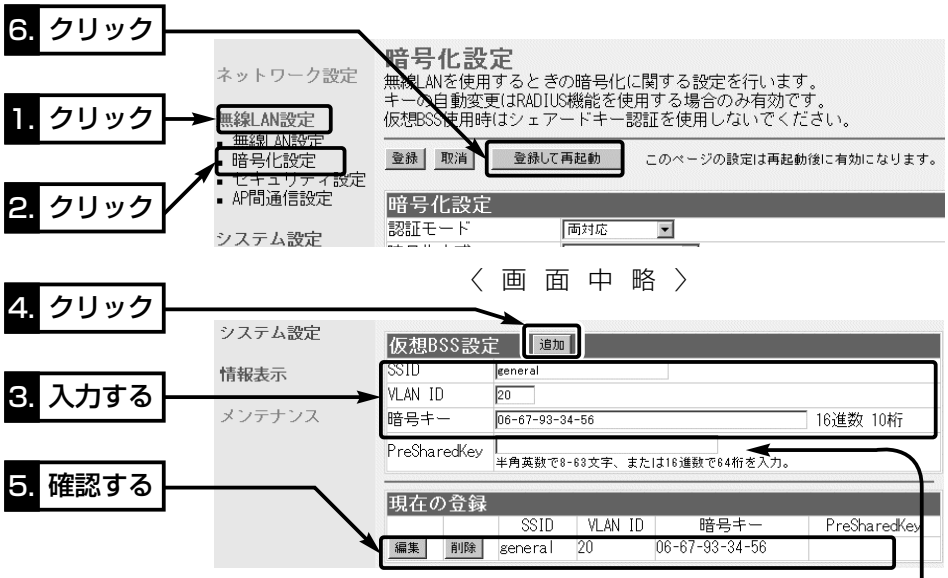
[WPA-PSK(TKIP/AES)]暗号化方式の場合は、[暗号化設定]項目の[PreSharedKey]欄に、無線クライアント側(例：sales)と同じ[PreSharedKey]を入力します。
この場合、[キーID]欄と[キー値]項目の設定は不要です。

2-2.「暗号化設定」画面
■設定例について(つづき)

〈仮想BSSの設定〉

仮想BSSで[VLAN ID]を使用する無線グループに対する設定です。

①[IEEE802.11g]規格側の「暗号化設定」画面にある[仮想BSS設定]項目で、[SSID]欄を「general」と入力します。
②[VLAN ID]欄を「20」に設定します。
③仮想BSSで使用する暗号化鍵(キー)を[暗号キー]欄のテキストボックスに入力します。
※無線クライアント(general)側の[キーID]が「1」のテキストボックスにも同じ暗号化鍵(キー)を設定します。
④〈追加〉ボタンをクリックします。
●登録した内容は、[現在の登録]項目に表示します。
⑤〈登録して再起動〉ボタンをクリックします。
※[キーID：2]のテキストボックスに入力された暗号化鍵(キー)と同じものが、無線クライアント側の[キーID：2～4]のどれか1つのテキストボックス(例：「2」☞P36)に設定されていることを確認します。

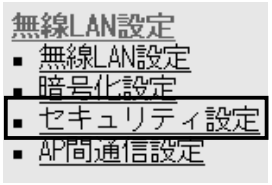


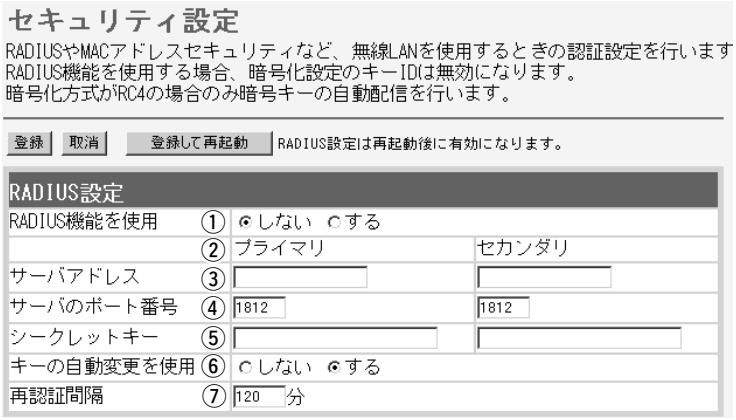
[WPA-PSK(TKIP/AES)]暗号化を使用する場合

[WPA-PSK(TKIP/AES)]暗号化方式の場合は、[仮想BSS設定]項目の[PreSharedKey]欄に、無線クライアント側(例：general)と同じ[PreSharedKey]を入力します。
この場合、[暗号キー]欄の設定は不要です。

2-3.「セキュリティ設定」画面

■RADIUS設定　　RADIUSサーバを利用したIEEE802.1x認証についての設定です。





〈登録〉ボタン …… 「セキュリティ設定」画面の[MACアドレスセキュリティ設定]項目、および[無線端末間通信設定]項目の設定内容が有効になります。

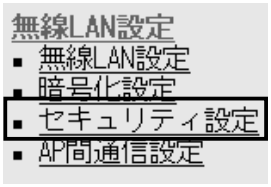
※[RADIUS設定]項目の変更内容は、画面上で確定されるだけですので、〈登録して再起動〉をクリックするまで有効になりません。

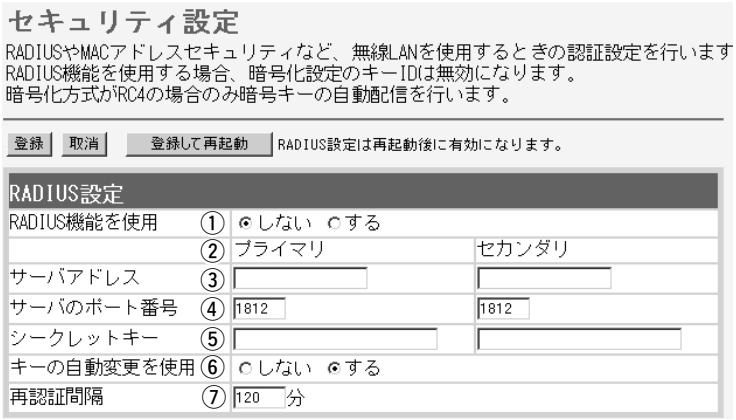
〈取消〉ボタン …… 「セキュリティ設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

〈登録して再起動〉ボタン …… 本製品を再起動して、「セキュリティ設定」画面で変更したすべての設定内容を有効にします。

①RADIUS機能を使用 …… RADIUSサーバを利用して、IEEE802.1x認証を「する」か「しない」かを選択します。　(出荷時の設定：しない)
本製品は、EAP-MD5とEAP-TLSに対応しています。
「RADIUS機能を使用する」に設定している場合は、「暗号化設定」画面の[キーID]欄の設定は無効になります。
また、RADIUSサーバとの鍵交換は、「暗号化設定」画面にある[暗号化方式]欄で「WEP RC4」を設定するとき有効で、無線パソコン側では、Windows XP標準のワイヤレスネットワーク接続の設定で、「キーは自動的に提供される(H)」にチェックマークが入っている状態に該当します。
「暗号化設定」画面にある[暗号化方式]欄で「OCB AES」を設定するときは、RADIUS認証だけを行います。
このときは、RADIUSサーバと鍵交換は行いません。

2-3.「セキュリティ設定」画面
■RADIUS設定(つづき)





② プライマリ/セカンダリ …… [プライマリ]列に設定したサーバから応答がないとき、その次にアクセスさせるRADIUSサーバがあるときは、[セカンダリ]列にそのRADIUSサーバアドレスを設定します。

③ サーバアドレス …… 対象となるRADIUSサーバのIPアドレスを入力します。

④ サーバのポート番号 …… 対象となるRADIUSサーバの認証ポートを設定します。
設定できる範囲は、「1～65535」です。 (出荷時の設定：1812)
※ご使用になるシステムによっては、出荷時の設定値と異なることがありますのでご確認ください。

⑤ シークレットキー …… この欄に設定されたキーを使用して本製品とRADIUSサーバ間の通信パケットを暗号化します。
RADIUSサーバに設定された値と同じ値を入力します。
入力は、半角31文字以内の英数字で入力します。

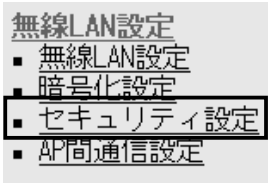
⑥ キーの自動変更を使用 …… 本製品のRADIUS機能を使用するとき有効な機能で、Windows 2000(Service Pack4)やWindows XPを使って本製品にIEEE802.1x認証でアクセスする無線パソコンに対して、RADIUSサーバから定期的に異なるキーをその無線パソコンに自動で割り当てる機能を使用して認証させるとき設定します。
(出荷時の設定：する)
※弊社製無線LANカードに付属の設定ユーティリティーは、この機能に対応していませんので、この設定ユーティリティーをWindowsＸＰにインストールして使用している無線パソコンに対しては、機能しません。

⑦ 再認証間隔 …… RADIUSサーバに再度認証を要求する間隔を分で設定します。
設定できる範囲は、「30～9999」です。 (出荷時の設定：120)

2-3.「セキュリティ設定」画面(つづき)

■無線端末間通信設定

無線パソコンどうしが本製品を介して通信するのを禁止するとき設定します。

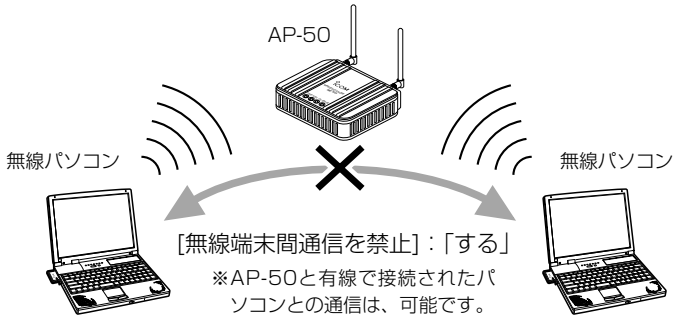


無線端末間通信設定	
無線端末間通信を禁止	◉しない ○する

無線端末間通信を禁止 ……

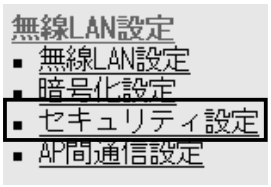
本製品を無線ホットスポット接続に利用するときなどは、設定を変更すると本製品を介して無線パソコンどうしが通信することを禁止できます。 (出荷時の設定：しない)

※この機能は、本製品で設定している無線チャンネルに該当する無線LAN規格の無線パソコンについて有効です。

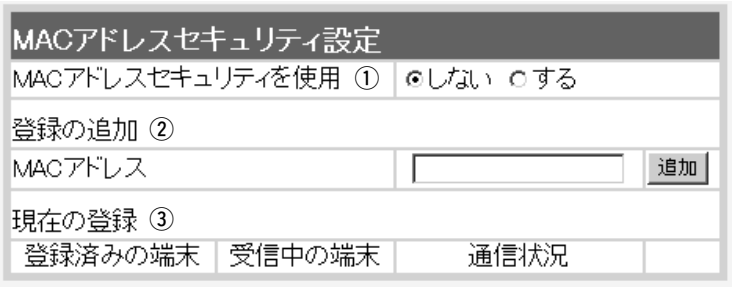


2-3.「セキュリティ設定」画面(つづき)

■MACアドレスセキュリティ設定



通信を許可する無線端末のMACアドレスを登録することで、通信制限するとき必要な設定です。



①MACアドレス
セキュリティを使用 ……

本製品に登録されたMACアドレスを持つ無線LANのパソコンだけが、本製品にワイヤレス接続できるように「する」か「しない」かを選択します。　(出荷時の設定：しない)
「する」を選択すると、[現在の登録]欄に登録されていないMACアドレスを持つ無線LANのパソコンからのアクセスを防止します。

② 登録の追加 ……

この欄に対象となる無線LANカードのMACアドレスを入力して〈追加〉をクリックすると、[登録済みの端末]欄に登録されます。
MACアドレスセキュリティーが有効なとき、[登録済みの端末]欄に表示されたMACアドレスをもつ無線LANカードとだけ通信できます。
※最大256台分のMACアドレスを登録できます。
※入力は半角英数字で12桁(16進数)を入力します。
※入力後は〈追加〉をクリックして、[現在の登録]欄に登録されたことを確認してください。
※2つの入力例は、同じMACアドレスになります。
(入力例：00-90-c7-4B-00-32、0090c74B0032)

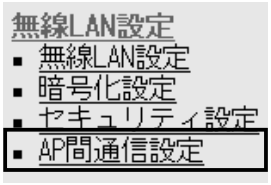
③ 現在の登録 ……

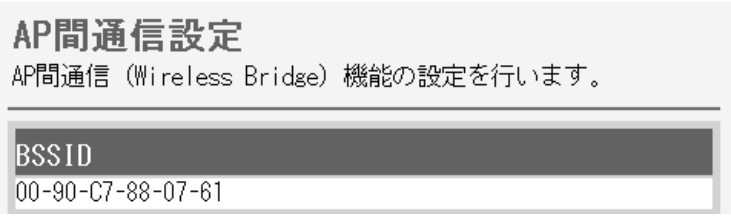
本製品と無線で通信している端末の状況や登録済みの無線端末のMACアドレスを表示します。
登録されているMACアドレスは、〈削除〉で登録の削除ができます。
受信中の端末欄に表示されているMACアドレスで登録されていないものは、〈追加〉ボタンが表示されますので、それをクリックすると、その端末のMACアドレスが登録できます。

2-4.「AP間通信設定」画面

■BSSID

本製品に内蔵する無線LANカードの[BSSID]を表示します。

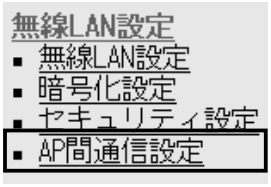


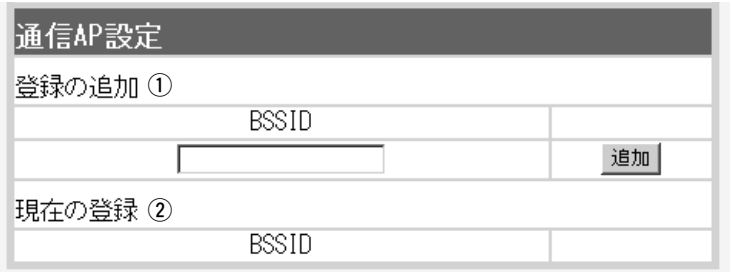


AP間通信を使用するときは、画面に表示された[BSSID]を相手側のAP-50に登録します。
また、本製品には相手側の[BSSID]を「ステーションリスト」に登録します。

■通信AP設定

AP間通信する相手のBSSIDを登録します。





① 登録の追加 ……

AP間通信する相手側(AP-50、AP-50R、SR-5200VoIP、SR-5000VoIP、AP-5100、AP-5100Aなど)の[BSSID]を入力します。
※〈追加〉をクリックすると、入力した[BSSID]が有効になります。
※最大6台分の[BSSID]が登録できます。
※[BSSID]の入力は、半角英数字で12桁(16進数)を入力します。
※[BSSID]を次のように入力すると、同じ[BSSID]として処理します。(入力例：00-90-C7-88-00-65、0090C7880065)

② 現在の登録 ……

本製品に登録されている[BSSID]を表示します。
この欄に登録されている[BSSID]を持つ無線ルータや無線アクセスポイントと本製品のあいだでAP間通信できます。
【登録例】
登録した内容を取り消すときは、該当する欄の〈削除〉をクリックします。

「システム設定」メニュー

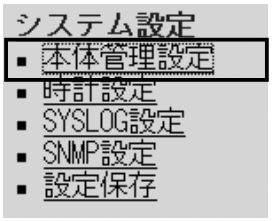
第3章

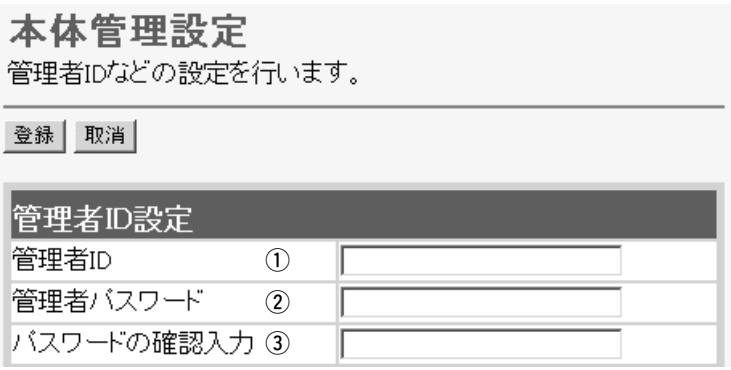
この章では、
「システム設定」メニューで表示される設定画面について説明します。

3-1.「本体管理設定」画面

■管理者ID設定

本製品の設定画面へのアクセス制限を設定します。





⚠ご注意
管理者パスワードを忘れた場合、設定を確認できなくなりますのでご注意ください。
この場合、設定を工場出荷時に戻していただくことになります。

〈登録〉ボタン …… 「本体管理設定」画面で変更したすべての設定内容が有効になります。

〈取消〉ボタン …… 「本体管理設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

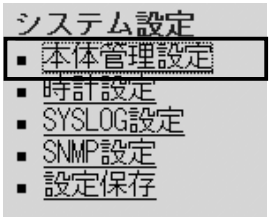
①管理者ID …… 本製品の設定画面へのアクセスを制限する場合に、管理者としての名前を、大文字/小文字の区別に注意して、任意の英数字、半角31文字以内で入力します。 (入力例：AP50)
[管理者ID]を設定すると、次回のアクセスからユーザー名の入力を求められますので、そこに[管理者ID]を入力します。

②管理者パスワード …… [管理者ID]に対するパスワードを設定する場合、大文字/小文字の区別に注意して、任意の英数字、半角31文字以内で入力します。
入力した文字は、すべて「＊(アスタリスク)」で表示されます。
(表示例：＊＊＊＊)
[管理者パスワード]を設定すると、次回のアクセスからパスワードの入力を求められますので、そこに[管理者パスワード]を入力します。

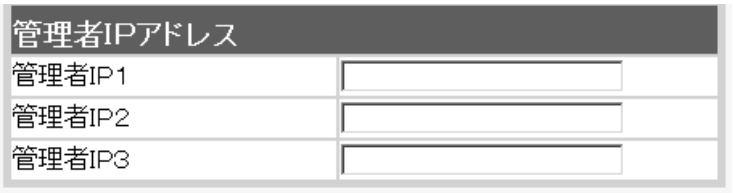
③パスワードの確認入力 …… 確認のために、パスワードを再入力します。 (表示例：＊＊＊＊)

3-1.「本体管理設定」画面(つづき)

■ 管理者IPアドレス



本製品の設定画面へのアクセスをIPアドレスで制限するときの設定です。

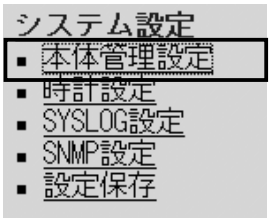


本製品の設定画面へのアクセスを制限する場合に、管理者が本製品に有線または無線でアクセスするパソコンのIPアドレスを3台まで登録できます。　(入力例：192.168.0.5)

※[管理者IPアドレス]を設定すると、IPアドレスが登録されたパソコン以外は、次回のアクセスから本製品の設定画面にアクセスできなくなります。

※空白の場合は、本製品に接続するすべてのパソコンが設定画面にアクセスできます。

■ 設定初期化



本製品の設定内容をすべて出荷時の状態に戻します。

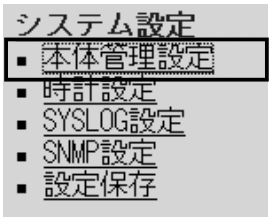
本製品の設定内容をすべて出荷時の状態に戻します。
[初期化する]欄のチェックボックスをクリックしてチェックマークを入れてから、〈実行〉ボタンをクリックします。

● 次の画面を表示後、出荷時の状態になります。

再起動しています。しばらくお待ちください。

3-1.「本体管理設定」画面(つづき)

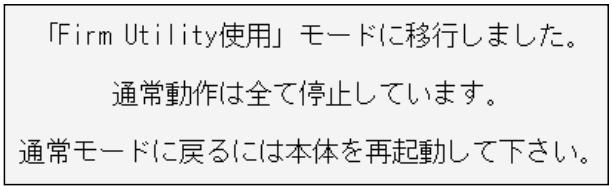
■「Firm Utility使用」モード



本製品に付属の「Firm Utility」を使用して、本製品を出荷時の状態に戻したり、ファームウェアをバージョンアップするとき使用します。

「Firm Utility使用」モードにするときは、[移行する]欄のチェックボックスをクリックしてチェックマークを入れてから、〈実行〉ボタンをクリックします。

●次の画面を表示して、「Firm Utility使用」モードに移行します。

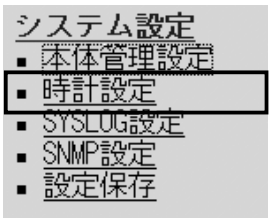


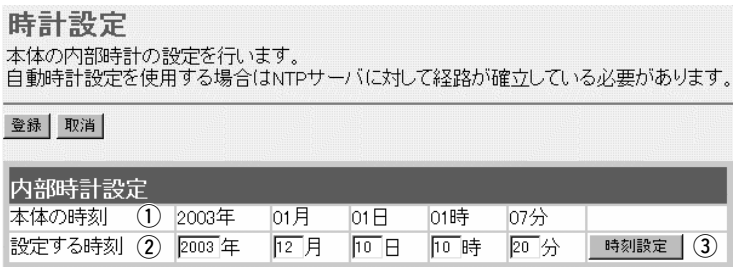
※「Firm Utility使用」モードに移行後も、本製品に設定された内容で動作します。

※「Firm Utility使用」モードに移行しないと、「Firm Utility」と本製品が通信できません。

3-2.「時計設定」画面

■ 内部時計設定　　**本製品の内部時計を設定します。**





〈登録〉ボタン …… [自動時計設定]項目で変更したすべての設定内容が有効になります。

〈取消〉ボタン …… 「時計設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお、〈登録〉をクリックすると、変更前の状態には戻りません。

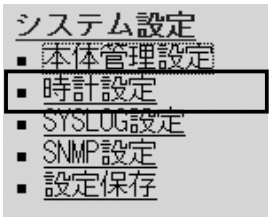
① 本体の時刻 …… 本製品に設定されている時刻を表示します。

② 設定する時刻 …… 本製品の設定画面にアクセスしたときの時刻を、最初に表示します。
※〈取消〉ボタンをクリックすると、空白になります。
　WWWブラウザの〈更新〉ボタンをクリックすると、パソコンの時計設定を取得して表示します。

③〈時刻設定〉ボタン …… [設定する時刻](②)欄に表示された時刻を本製品に設定するボタンです。
時刻を正確に設定するときは、本製品の設定画面に再度アクセスしなおすか、WWWブラウザの〈更新〉ボタンをクリックしてから、〈時刻設定〉ボタンをクリックしてください。

3-2.「時計設定」画面(つづき)

■ **自動時計設定**



本製品の内部時計を自動設定するとき、アクセスするタイムサーバの設定です。

自動時計設定		
自動時計設定を使用	①	○しない ◉する
NTPサーバ1 IPアドレス	②	133.100.9.2
NTPサーバ2 IPアドレス	③	
アクセス時間間隔	④	1 日
前回アクセス日時	⑤	----/--/-- --:--
次回アクセス日時	⑥	2003/01/02 00:00

※自動時計設定機能は、NTPサーバへの問い合わせ先(経路)を「ルーティング設定」画面で設定することで使用できます。
ルーティングテーブルを設定しないときは、問い合わせできません。

① 自動時計設定を使用 …… インターネット上に存在するタイムサーバに日時の問い合わせを行い、内部時計を自動設定します。 (出荷時の設定：する)

②NTPサーバ1 IPアドレス … 最初にアクセスさせたいタイムサーバのIPアドレスを入力します。
(出荷時の設定：133.100.9.2)

③NTPサーバ2 IPアドレス … [NTPサーバ1 IPアドレス]の次にアクセスさせるタイムサーバがあるときは、そのIPアドレスを入力します。
返答がないときは、再度[NTPサーバ1 IPアドレス]で設定したタイムサーバにアクセスします。

④ アクセス時間間隔 …… タイムサーバにアクセスさせる間隔を日で設定します。
設定できる範囲は、「0～99」です。 (出荷時の設定：1)
「0」を設定したときは、タイムサーバにアクセスを行いません。
「PPPoE」による手動接続では、前回アクセスした日から設定した日数が経過している場合は、接続時にアクセスします。
常時接続では、設定した日数にしたがってアクセスします。

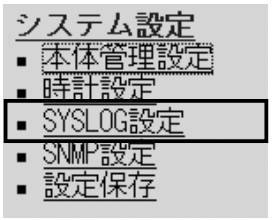
⑤ 前回アクセス日時 …… タイムサーバにアクセスした日時を表示します。

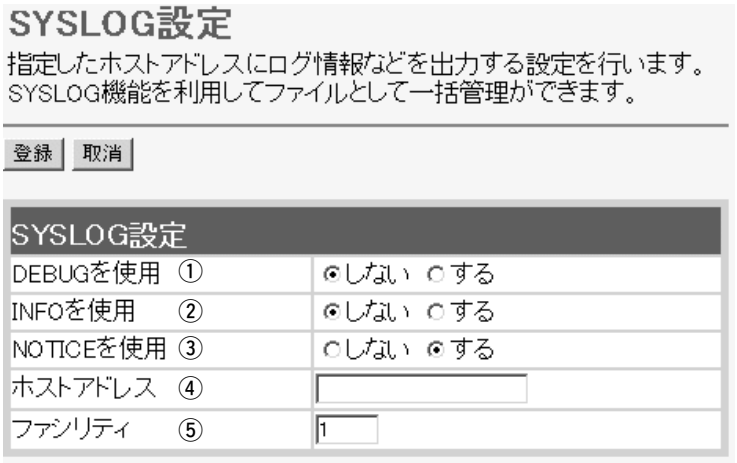
⑥ 次回アクセス日時 …… タイムサーバにアクセスする予定日時を、[前回アクセス日時]欄と[アクセス時間間隔]欄で設定された日数より算出して表示します。

3-3.「SYSLOG設定」画面

■SYSLOG設定

指定したホストアドレスにログ情報などを出力する設定です。





〈登録〉ボタン …… 「SYSLOG設定」画面で変更したすべての設定内容が有効になります。

〈取消〉ボタン …… 「SYSLOG設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

①DEBUGを使用 …… 各種デバッグ情報をSYSLOGに出力「する」か「しない」かを選択します。　(出荷時の設定：しない)

②INFOを使用 …… INFOタイプのメッセージをSYSLOGに出力「する」か「しない」かを選択します。　(出荷時の設定：しない)

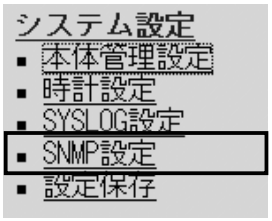
③NOTICEを使用 …… NOTICEタイプのメッセージをSYSLOGに出力「する」か「しない」かを選択します。　(出荷時の設定：する)

④ホストアドレス …… SYSLOG機能を使用する場合、SYSLOGを受けるホストのアドレスを入力します。
ホストはSYSLOGサーバ機能に対応している必要があります。

⑤ファシリティ …… SYSLOGのファシリティを入力します。
設定できる範囲は、「0～23」です。　(出荷時の設定：1)
通常「1」を使用します。

3-4.「SNMP設定」画面

■SNMP設定



TCP/IPネットワークにおいて、ネットワーク上の各ホストから自動的に情報を収集してネットワーク管理するときの設定です。

〈登録〉ボタン …… 「SNMP設定」画面で変更したすべての設定内容が有効になります。

〈取消〉ボタン …… 「SNMP設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

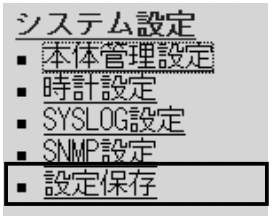
①SNMPを使用 …… SNMP機能を使用「する」か「しない」かを選択します。
(出荷時の設定：する)

②コミュニティID(GET) …… 本製品の設定情報をSNMP管理ツール側から読み出すことを許可するIDを設定します。 (出荷時の設定：public)
入力は、半角31文字以内の英数字で入力します。

③コミュニティID(SET) …… 本製品の設定情報をSNMP管理ツール側から変更することを許可するIDを設定します。 (出荷時の設定：private)
入力は、半角31文字以内の英数字で入力します。

3-5.「設定保存」画面

■設定の保存と書き込み

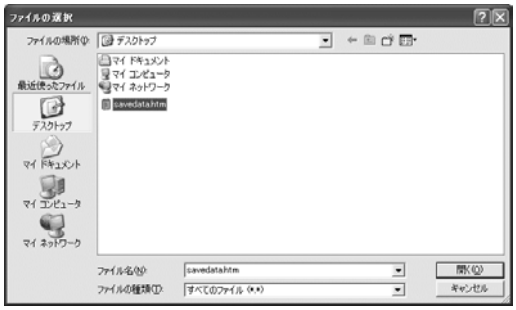


本製品の設定内容を保存したり、保存した設定ファイルを本製品に書き込んだりします。

① 保存したファイルを書き込む ……

[ファイルに保存する](②)欄の操作で保存した設定ファイル(拡張子：.sav)内容を本製品に書き込むとき使用します。

設定ファイルの保存先をテキストボックスに直接入力するか、〈参照...〉ボタンをクリックします。



右上の画面から目的の設定ファイルをクリックして、〈開く(O)〉をクリックします。

テキストボックスに保存先を指定後、〈書き込み〉ボタンをクリックすると、本製品にその設定内容を書き込みます。

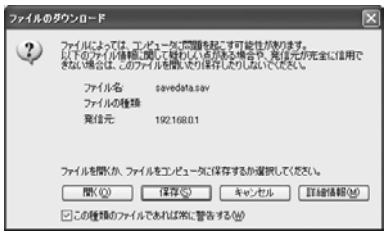
書き込む前の設定内容は、消去されますのでご注意ください。

※市販のソフトウェアなどで編集したものは、誤動作の原因になりますので、本製品に登録しないでください。

② ファイルに保存する ……

本製品すべての設定内容をパソコンに保存することで、本製品の設定をバックアップすることができます。

[設定の保存と書き込み]項目で[ファイルに保存]をクリックすると表示される右の画面から〈保存(S)〉をクリックすると、設定ファイルを保存できます。

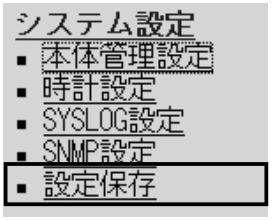


設定ファイルのファイル形式(拡張子)は、「.sav」です。

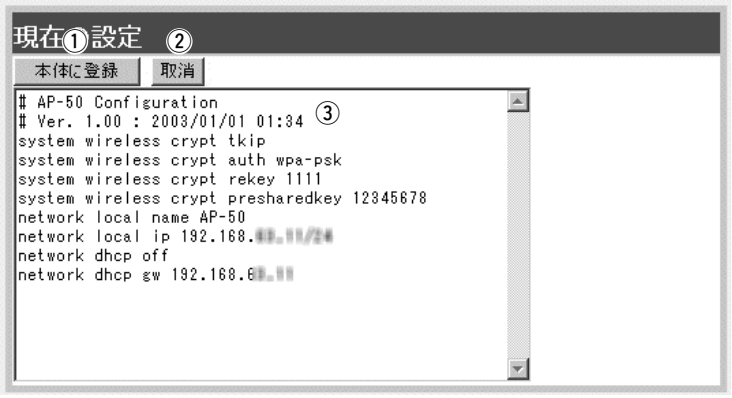
保存したファイルは、[保存したファイルを書き込む](①)欄の操作で、本製品自身や本製品を使用する別の相手に書き込みできます。

3-5.「設定保存」画面(つづき)

■ 現在の設定



本製品の設定変更内容を確認したり、設定した内容を設定ファイルとして保存します。



① 〈本体に登録〉ボタン …… 「内容表示」(③)部に表示された内容を、本製品に書き込みます。
※[設定の保存と書き込み]項目(☞P53)の「ファイルに保存」をクリックして保存した設定ファイル(拡張子：.sav)は、このボタンを使用して書き込みできません。

② 〈取消〉ボタン …… 「内容表示」(③)部に表示された内容を変更したとき、変更を取り消して、このファイルを最初に開いたときの内容に戻します。

③「内容表示」画面 …… 基本的な設定と初期値から変更された設定を表示します。
この画面内容をパソコンに保存するときは、[設定の保存と書き込み]項目(☞P53)を使用してください。
※各画面で設定されたSSID、パスワード、キージェネレータ(暗号化鍵の生成元文字列)の内容は、暗号化されて表示されます。そのため、保存された設定ファイルよりこれらの情報が外部に漏れることはありません。

「情報表示」メニュー

第4章

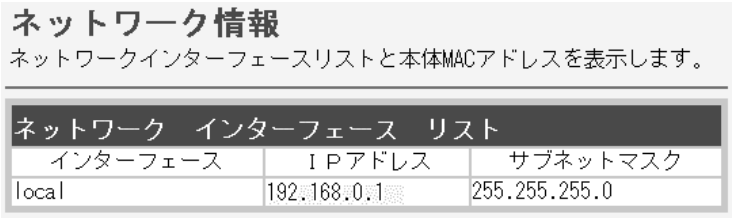
この章では、
「情報表示」メニューで表示される設定画面について説明します。

4 「情報表示」メニュー

4-1.「ネットワーク情報」画面

■ネットワーク インターフェイス リスト

「ネットワーク設定」メニューの「ルーティング設定」画面にある[IP経路情報]項目に表示された[経路]について、その詳細を表示します。

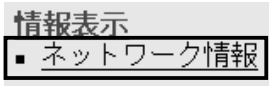


ネットワーク情報

ネットワークインターフェースリストと本体MACアドレスを表示します。

ネットワーク　インターフェース　リスト		
インターフェース	ＩＰアドレス	サブネットマスク
local	192.168.0.1	255.255.255.0

■ブリッジポート情報



本製品の使用ポートについて、ブリッジ通信の状況とパケットの数を表示します。

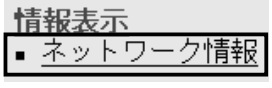
ブリッジポート情報		
ポート	通信情報	
Ethernet ①	状況	通信中
	送信パケット数	149
	受信パケット数	11103
Wireless ②	状況	通信中
	送信パケット数	10955
	受信パケット数	0
Wireless Bridge ③ 00-90-C7-88-00-65	状況	通信中
	送信パケット数	10955
	受信パケット数	0

① **Ethernet**…… 有線LAN]ポートの通信状況と、そのときの送信と受信のパケット数を表示します。

② **Wireless**…… 無線アクセスポイント接続の通信状況と、そのときの送信と受信のパケット数を表示します。

③ **Wireless Bridge** …… 無線ブリッジ接続の通信状況と、そのときの送信と受信のパケット数を表示します。
また、本製品に内蔵された無線LANカードの[BSSID]を表示します。

■本体MAC アドレス



本製品のMACアドレスを表示します。
※このMACアドレスは、本製品の底面パネルに貼られているシリアルシールにも12桁で記載されています。

本体MACアドレス
00-90-C7-85-00-D1

ご参考に

第5章

この章では、
Telnetや[CONSOLE]ポートを使用した接続とオンラインヘルプの見かたについて説明します。

5 ご参考に

5-1.Telnetによる接続

Telnetでの接続について説明します。
ご使用のOSやTelnetクライアントが異なるときは、それぞれの使用方法をご確認ください。

■ Windows 2000/Windows XPの場合

①Windowsを起動します。
②[スタート]メニューから[ファイル名を指定して実行]を選択します。名前欄に「Telnet.exe」と入力し、<OK>をクリックします。
③Telnetクライアントが起動しますので、下記のように指定します。
Microsoft Telnet>open 本製品のIPアドレス
(工場出荷時の設定：192.168.0.1)
④[User]と[Password]が要求されます。
設定したユーザ名とパスワードを入力してログインしてください。
※初期値では[User]、[Password]ともに設定されていません。
何も入力せずに[Enter]キーを押してください。
⑤ログインメッセージ(Welcome to AP-50!)が表示されます。

■ Windows 98/98 SE/Meの場合

①Windowsを起動します。
②[スタート]メニューから[ファイル名を指定して実行]を選択します。
名前欄に「Telnet.exe」と入力し、<OK>をクリックします。
③Telnetクライアントが起動しますので、メニューバーから[接続]→[リモートシステム]を選択します。
④[接続]ダイアログボックスが表示されます。
ホスト名、ポート、ターミナルの種類を下記のように選択して、<接続(C)>ボタンをクリックします。
ホスト名：本製品のIPアドレス(出荷時の設定：192.168.0.1)
ポート　：telnet(23)
ターミナルの種類：vt100
⑤[User]と[Password]が要求されます。
設定したユーザ名とパスワードを入力してログインしてください。
※初期値では[User]、[Password]ともに設定されていません。
何も入力せずに[Enter]キーを押してください。
⑥ログインメッセージ(Welcome to AP-50!)が表示されます。

5-2.[CONSOLE]ポートを使用する

本製品の[CONSOLE]ポートとパソコンの[COM]ポートを弊社別売品のケーブル(OPC-1402)で接続すると、ターミナルソフトから設定できます。
パソコンの[COM]ポートは、下記の値に設定すると使用できます。

[接続方法]の選択：OPC-1402を接続している[COM]ポートの番号を指定します。
通信速度　：115200(ビット/秒)
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

※設定後、何も入力せずに[Enter]キーを押すと、「AP-50 #」と表示されます。

5-3.オンラインヘルプ

Telnet、または[CONSOLE]ポートを使用したターミナルソフトの接続では、オンラインで、コマンドリファレンスを参照できます。

◎コマンド一覧 ……

[Tab]キーを押すと、使用できるコマンドの一覧が表示されます。
コマンド名の入力に続いて[Tab]キーを押すと、サブコマンドの一覧が表示されます。

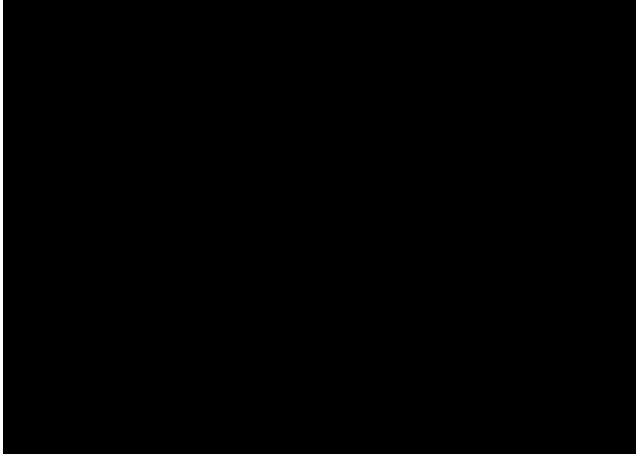
◎コマンドヘルプ ……

コマンドの意味を知りたい時は、コマンド名の入力に続いて[?]キーを押すとコマンドのヘルプが表示されます。

◎コマンド名の補完 ……

コマンド名を先頭から数文字入力し[Tab]キーを押すと、コマンド名が補完されます。
入力した文字に続くコマンドが一つしか無いときは、コマンド名を最後まで補完します。
　例) cl[Tab]→clear
複数のコマンドがあるときは、同じ文字列の所までを補完します。
さらに[Tab]キーを押すと、コマンドの候補を表示します。
　例) r[Tab]→re
　　re[Tab]→restart　remote
　　res[Tab]→restart

高品質がテーマです。



アイコム株式会社

本　　社	547-0003	大阪市平野区加美南1-1-32	
北海道営業所	003-0806	札幌市白石区菊水6条2-2-7	TEL 011-820-3888
仙台営業所	983-0857	仙台市宮城野区東十番丁54-1	TEL 022-298-6211
東京営業所	108-0022	東京都港区海岸3-3-18	TEL 03-3455-0331
名古屋営業所	468-0066	名古屋市天白区元八事3-249	TEL 052-832-2525
大阪営業所	547-0004	大阪市平野区加美鞍作1-6-19	TEL 06-6793-0331
広島営業所	733-0842	広島市西区井口3-1-1	TEL 082-501-4321
四国営業所	760-0071	高松市藤塚町3-19-43	TEL 087-835-3723
九州営業所	815-0032	福岡市南区塩原4-5-48	TEL 092-541-0211

● サービスについてのお問い合わせは各営業所サービス係宛にお願いします。

A-6363 I-2J-① © 2004 Icom Inc.