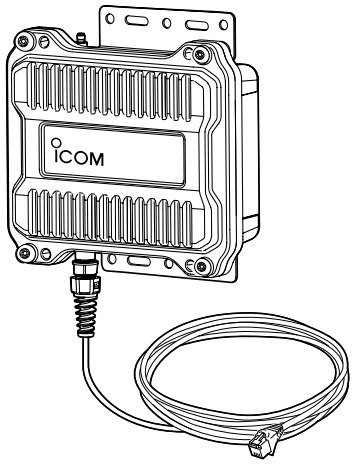
ICOM

取扱説明書

FWA BASESTATION

BS−900

FWA専用
[IEEE802.3af]規格PoE準拠



Icom Inc.

株式会社エクセリ　東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5　URL : https : //www.exseli.com/

はじめに

このたびは、本製品をお買い上げいただきまして、まことにありがとうございます。

本製品は、4.9GHz帯の加入者系固定無線アクセスシステム(FWA)の基地局として使用するFWA BASESTATIONです。

ご使用の前に、この取扱説明書をよくお読みいただき、本製品の性能を十分発揮していただくとともに、末長くご愛用くださいますようお願い申し上げます。

本書の表記について

本書は、次の表記規則にしたがって記述しています。

「 」表記：オペレーティングシステム(OS)の各ウィンドウ(画面)、ユーティリティー、設定画面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：タブ名、アイコン名、テキストボックス名、チェックボックス名、各設定画面の設定項目名を([ ])で囲んで表記します。

〈 〉表記：ダイアログボックスのコマンドボタンなどの名称を(〈〉)で囲んで表記します。

※Microsoft® Windows® 8.1、Microsoft® Windows® 8.1 Proは、Windows 8.1と表記します。
Microsoft® Windows® 7 Home Premium、Microsoft® Windows® 7 ProfessionalおよびMicrosoft® Windows® 7 Ultimateは、Windows 7と表記します。
Microsoft® Windows Vista® Home Basic、Microsoft® Windows Vista® Home Premium、Microsoft® Windows Vista® BusinessおよびMicrosoft® Windows Vista® Ultimateは、Windows Vistaと表記します。

※ 本書は、Ver. 1.03のファームウェアを使用して説明しています。

※ 本書では、Windows 7の画面を例に説明しています。

※ 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。

※ 本製品の仕様、外観、その他の内容については、改良のため予告なく変更されることがあり、本書の記載とは一部異なる場合があります。

登録商標/著作権について

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

はじめに

本製品の概要について

◎複数のアンテナを使用し、同時にデータを送受信することで、最大300Mbps(理論値)で通信できます。
※54Mbps(理論値)を超える通信速度は、暗号化方式を「なし」、または「AES」に設定している場合に有効です。
※最大300Mbps(理論値)を使用できるのは、帯域幅を「40MHz」に設定した場合だけです。

◎必要に応じて、ストリーム数(2ストリーム/1ストリーム)を変更できます。
※1ストリーム運用時、通信速度(理論値)は最大150Mbpsになります。

◎設置場所や通信障害を調査、診断の目安になるサイトサーベイ機能を搭載しています。
※スキャン実行中は、FWA無線LAN端末と通信できません。

◎[IEEE802.1Q]のVLAN規格に準拠した仮想AP機能を搭載していますので、本製品1台で最大8グループの無線ネットワークを構築できます。

◎ネットワーク認証は、「共有キー」、「オープンシステム」、「IEEE802.1X」、「WPA」、「WPA2」、「WPA-PSK」、「WPA2-PSK」に対応しています。

◎「IEEE802.1X」、「WPA」、「WPA2」を設定すると、認証にRADIUSサーバーを使用できます。

◎IP67(耐塵形と防浸形)の性能に対応できるように設計されています。

◎[IEEE802.3af]に準拠したPoE受電機能に対応していますので、弊社別売品の「イーサネット電源供給ユニット(SA-4)」、または[IEEE802.3af]規格対応のHUB(市販品)から電源を受電できます。

◎ネットワーク管理機能として、SNMPをサポートしています。

◎本製品のご使用は、無線局の登録および無線従事者の免許が必要です。

IP表記について

機器内への異物の侵入に対する保護性能を表すための表記です。
IPにつづけて保護等級を示す数字で記載され、1つ目の数字が防塵等級、2つ目が防水等級を意味します。
また、保護等級を定めない場合は、その等級の表記に該当する数字の部分を「X」で表記します。

【本書で記載する保護の程度について】
IP6X(耐塵形):試験用粉塵を1m^{3}あたり2kgの割合で浮遊させた中に8時間放置したのちに取り出して、無線機内部に粉塵の侵入がないこと
IPX7(防浸形):水深1mの静水(常温の水道水)に静かに沈め、30分間放置したのちに取り出して、無線機として機能すること

無線通信できるFWA機器について

2016年5月現在、本製品と無線通信★できるFWA機器は、SE-570FW、SE-570FWD、SE-900FWです。
★SE-570FW/SE-570FWDにはVer.2.03以降のファームウェアをご使用ください。
※FWA機器の接続互換については、8-15ページをご覧ください。

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

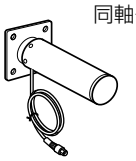
はじめに

別売品について

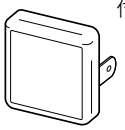
（2016年5月現在）

本製品に外部アンテナを2本接続するときは、同じ製品名のアンテナを接続してください。（AH-163を除く）

AH-159 指向性アンテナ
同軸ケーブル：約2m



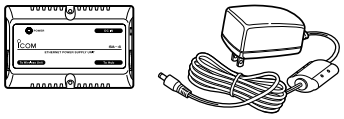
AH-160 平面アンテナ
付属同軸ケーブル:約2m



AH-161 無指向性アンテナ
同軸ケーブル:約2.5m

AH-163 無指向性アンテナ
同軸ケーブル:約2.5m

SA-4 イーサネット電源供給ユニット



【別売品についてのご注意】

弊社製別売品は、本製品の性能を十分に発揮できるように設計されていますので、必ず弊社指定の別売品をお使いください。

弊社指定以外の別売品とのご使用が原因で生じるネットワーク機器の破損、故障、または動作や性能については、保証対象外とさせていただきますので、あらかじめご了承ください。

通信距離について

無線通信距離は環境によって異なりますので、以下の表は目安としてご使用ください。

		SE-900FW		
		AH-159 AH-160 AH-161	SE-900FW 内部アンテナ	AH-163
BS-900	AH-159 AH-160 AH-161	約2500m	約2500m	約1000m
	AH-163	約1000m	約1000m	約1000m

※本書では、SE-900FW（FWA無線LAN端末）と通信した場合の距離を参考として記載しています。
　長距離通信モードを「有効」、パワーレベルを「高」（出荷時の設定）に設定した値です。
※対向する互いの設置場所が上記に示す距離を超えないように設置してください。

【通信実験するときの距離について】

通信実験をするときは、機器間の距離を5m以上はなしてください。
5m以下の距離で通信実験をすると、無線ユニットの通信特性により通信速度が遅くなることがあります。

株式会社エクセリ　東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5　URL : https : //www.exseli.com/

無線通信の最大通信速度について

BS-900とSE-900FWで通信した場合の速度

帯域幅	最大通信速度(理論値)	
	ストリーム数 2	ストリーム数 1★
40MHz	300Mbps	150Mbps
20MHz	144Mbps	72Mbps
10MHz	—	27Mbps

※ストリーム数の設定が異なる機器と通信するときは、少ない方のストリーム数で通信します。
※SE-570FW、SE-570FWDと通信する場合は、本製品の設定に関係なく、ストリーム数は「1」、最大通信速度は「54Mbps」になります。

無線LANの性能表示等の記載について

◎本製品の通信速度についての記載は、無線LAN規格による理論上の最大値であり、実際のデータ転送速度(実効値)を示すものではありません。
◎実際のデータ転送速度は、周囲の環境条件(通信距離、障害物、電子機器等の電波環境要素、使用するパソコンの性能、ネットワークの使用状況など)に影響します。

★ANT1側だけに外部アンテナを接続する場合は、アンテナ数を「1×1」、ストリーム数を「1」に設定してください。
周囲環境によっては、外部アンテナ2本接続時でも、ストリーム数「1」の方が通信が安定する場合もあります。

はじめに

無線通信の帯域幅について

帯域幅の組み合わせによる接続の可否と通信時の帯域幅

下表のように組み合わせにより、接続できる条件が異なりますのでご注意ください。

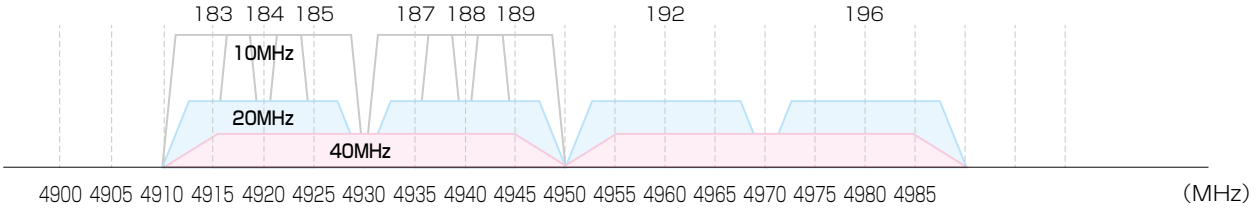
	帯域幅	BS-900		
		40MHz	20MHz	10MHz
SE-900FW	40MHz	○	△	×
	20MHz	△	○	×
	10MHz	×	×	○

○：設定した帯域幅で接続可　　△：20MHz 帯域幅で接続可　　×：接続不可

※SE-570FW、SE-570FWDとは、20MHz帯域幅でしか通信できません。

帯域幅と無線通信チャンネルについて

下表のように設定する帯域幅により、使用できるチャンネルが異なります。



はじめに

出荷時のおもな設定値

設定メニュー	設定画面	設定項目	設定名称	設定値
ネットワーク設定	LAN側IP	IPアドレス設定	IPアドレス	192.168.0.1
			サブネットマスク	255.255.255.0
	DHCPサーバー	DHCPサーバー設定	DHCPサーバー	無効
無線設定	無線LAN	無線LAN設定	無線UNIT	有効
			帯域幅	20MHz
			チャンネル	184CH(4920MHz)
			アンテナ数(Tx×Rx)	2×2
			長距離通信モード	無効
	仮想AP	仮想AP設定	インターフェース	ath0
			SSID	WIRELESSLAN-0
			ストリーム数	2
		暗号化設定	ネットワーク認証	オープンシステム/共有キー
			暗号化方式	なし
管理	管理者	管理者パスワードの変更	管理者ID	admin(変更不可)
			現在のパスワード	admin(半角小文字)

【不正アクセス防止のアドバイス】

本製品に設定するすべてのパスワードは、容易に推測されないものにしてください。

数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた複雑なものにし、さらに定期的にパスワードを変更されることをおすすめします。

はじめに

設定画面の名称と機能について

本製品の設定画面の名称と各画面に含まれる項目を説明します。
設定画面の構成について詳しくは、8-6ページをご覧ください。

設定画面選択メニュー

各設定画面を用途別に、メニューとしてまとめています。
メニュー名をクリックするごとに、各設定画面へのリンクを開け閉めできます。

設定画面表示エリア

設定画面選択メニューで選択されたタイトルの画面を表示します。
※上図は、「ネットワーク設定」メニューの「LAN側IP」をクリックしたときに表示される画面です。

ホームページのリンク

インターネットに接続できる環境で、アイコンをクリックすると、弊社のホームページを閲覧できます。

設定ボタン

設定した内容の登録や取り消しをします。
※〈登録〉をクリックして、「再起動が必要な項目が変更されています。」と表示されるときは、〈再起動〉をクリックします。
表示された画面にしたがって操作します。
再起動中は、下記を表示します。

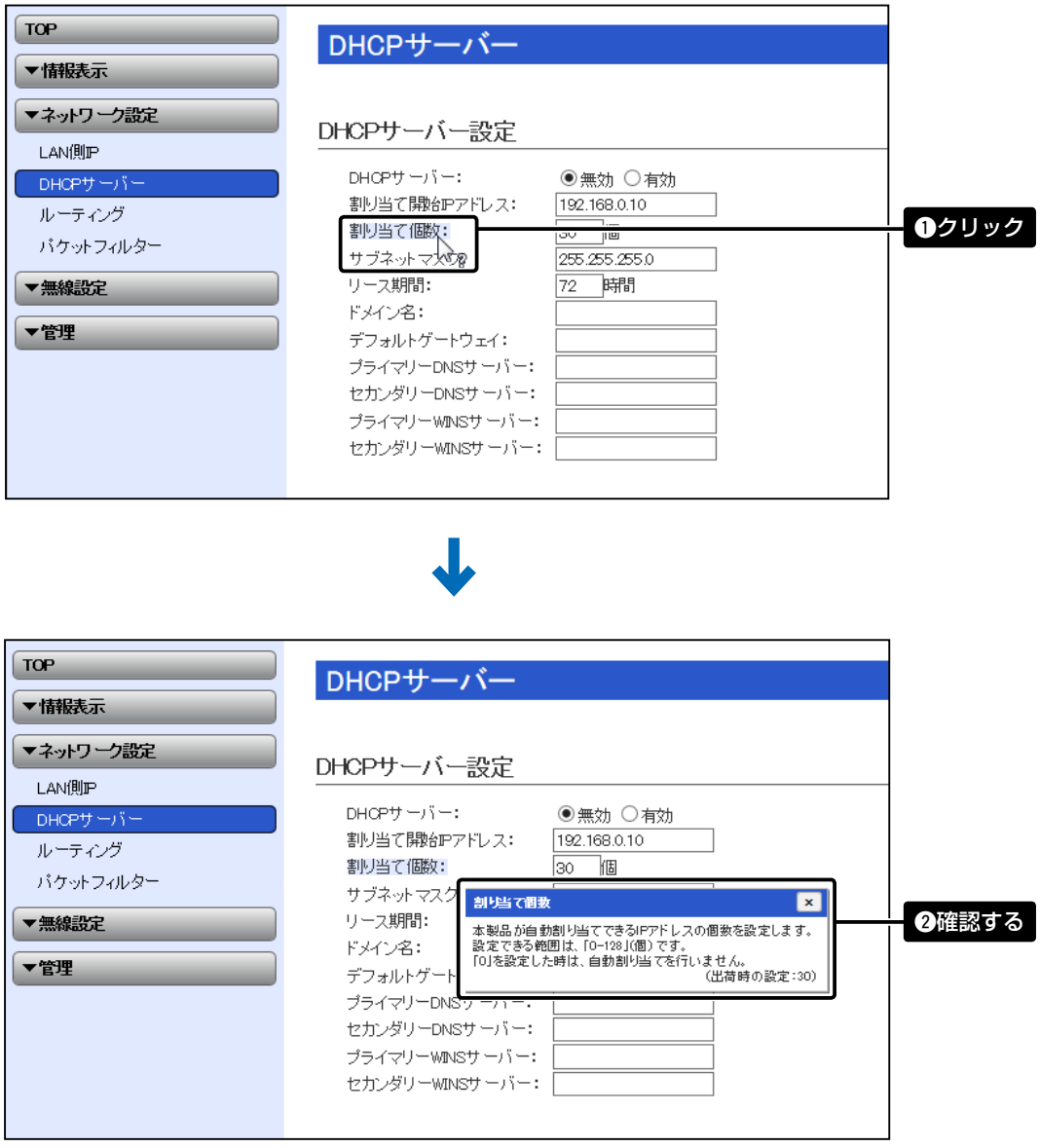
> **本体を再起動しています。**
> 本体の起動を確認後、[Back]をクリックしてください。

※再起動後に、設定した内容が有効となります。
※再起動が完了するまで、[Back]と表示された文字の上にマウスポインターを移動してクリックしても、設定画面に戻りません。
しばらくしてから再度操作してください。
※表示画面によって、表示されるボタンの種類や位置が異なります。

はじめに

オンラインヘルプについて

設定画面で表示される設定項目ごとに、設定できることや出荷時の設定などをオンラインヘルプで説明しています。
オンラインヘルプを確認するときは、下図のように設定項目の上にマウスポインターを移動して、「？」が表示されたら、クリックしてください。



はじめに

もくじ

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

第 1 章

「TOP」メニュー

この章では、
本製品の「TOP」メニューで表示される画面について説明しています。

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

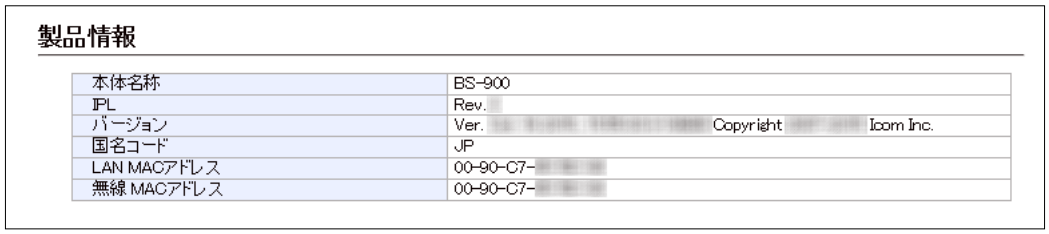
1 「TOP」メニュー

1.「TOP」画面について

TOP

■ 製品情報

ファームウェアのバージョン情報、本製品のMACアドレス(LAN/無線)を表示します。

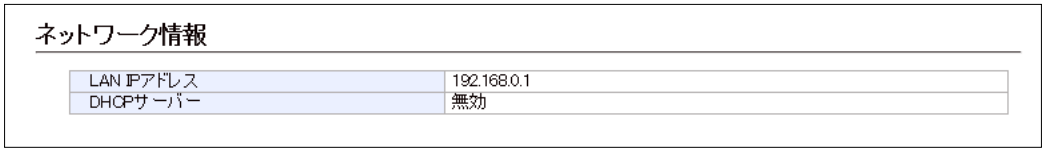


※MACアドレスは、本製品のようなネットワーク機器がそれぞれ独自に持っている機器固有の番号で、12桁(0090C7×××××)で表示されています。

TOP

■ ネットワーク情報

本製品のIPアドレスなど、ネットワーク情報を表示します。



「情報表示」メニュー

第 2 章

この章では、
本製品の「情報表示」メニューで表示される画面について説明しています。

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

2 「情報表示」メニュー

1.「ネットワーク情報」画面について

情報表示 > ネットワーク情報

■ インターフェースリスト

「ネットワーク設定」メニュー→「ルーティング」画面→[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。

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
lo0	127.0.0.1	255.255.255.255
mirror0	192.168.0.1	255.255.255.0

情報表示 > ネットワーク情報

■ Ethernetポート接続情報

本製品のポートについて、通信速度と通信モードを表示します。

Ethernetポート接続情報

インターフェース	MACアドレス	リンク状態
eth0	00-90-C7-	1000BASE-T full-duplex

※本製品の[LAN]ポート(eth0)は、接続モードが「自動(Auto)」となっています。
接続する機器側も「自動(Auto)」を設定することで、通信に最適な速度、モードを自動選択します。
※接続する機器を100Mbps、または10Mbpsで固定する場合、半二重(half-duplex)設定にしてください。
弊社製品に限らず、自動(Auto)と固定速度full-duplexとがネゴシエーションする場合、自動(Auto)側はhalf-duplexと認識されることがあり、パフォーマンスが著しく低下する原因になることがあります。
※通信速度に関係なく、接続するHUBを「full-duplex」固定に設定すると、[Ethernetポート接続情報]項目で「half-duplex」と表示されることがあります。

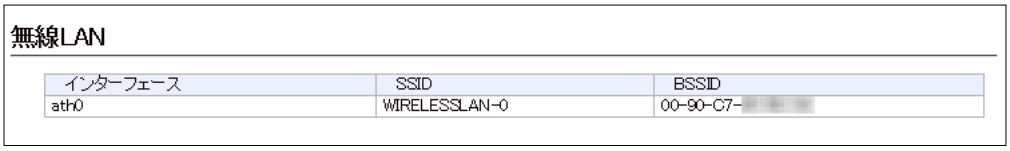
2 「情報表示」メニュー

1.「ネットワーク情報」画面について（つづき）

情報表示 > ネットワーク情報

■ 無線LAN

本製品で使用している仮想AP（ath0～ath7）を表示します。

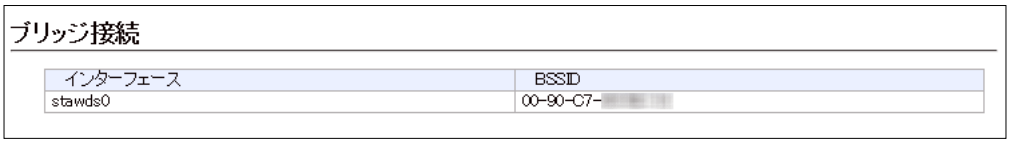


※「無線設定」メニュー→「無線LAN」画面→［無線LAN設定］項目にある［無線UNIT］欄で、「無効」に設定されている場合は、上記の一覧を表示しません。

情報表示 > ネットワーク情報

■ ブリッジ接続

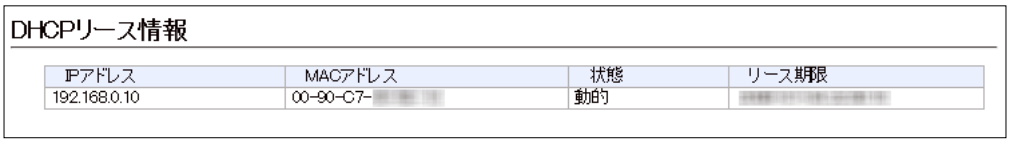
本製品で使用しているブリッジ接続設定（stawds0～stawds7）を表示します。



情報表示 > ネットワーク情報

■ DHCPリース情報

本製品のDHCPサーバー機能を使用している場合、本製品に接続する端末に割り当てされたIPアドレスの状態と有効期限を表示します。



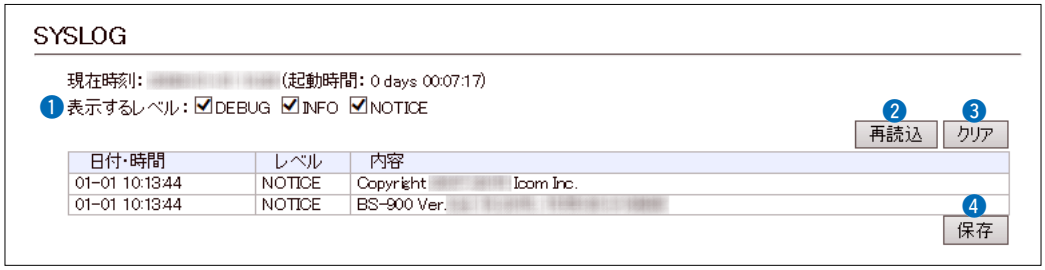
端末に割り当てされたIPアドレスの状態を、「動的」/「静的」/「解放済」で表示します。
◎**動的**　：IPアドレスが自動で割り当てされているとき
◎**静的**　：IPアドレスが固定で割り当てされているとき
◎**解放済**：IPアドレスを解放したとき
※リース期限は、［状態］欄が「動的」のときだけ、端末に割り当てされたIPアドレスの有効期限を表示します。

2. 「SYSLOG」画面について

情報表示 > SYSLOG

■ SYSLOG

本製品のログ情報は、「情報表示」メニューの「SYSLOG」画面で確認できます。
※表示されるのは、「管理」メニューの「SYSLOG」画面で、「有効」に設定されたレベルのログ情報だけです。



❶表示するレベル ……

非表示に設定するときは、非表示にするレベルのチェックボックスをクリックして、チェックマーク[✔]をはずします。
（出荷時の設定：☑DEBUG ☑INFO ☑NOTICE）
※「SYSLOG」画面のチェックボックス状態は、保存されません。
設定画面へのアクセスごとに、元の状態に戻ります。

❷〈再読込〉 ……

[表示するレベル]（❶）欄でチェックマーク[✔]のあるレベルについてのSYSLOG情報を最新の状態にするボタンです。
※最大511件のログ情報を記憶できます。
511件を超えると、古いログ情報から削除されます。

❸〈クリア〉 ……

表示されたログ情報を削除するボタンです。
※電源を切る、または設定の変更や初期化に伴う再起動でも、それまでのログ情報は削除されます。

❹〈保存〉 ……

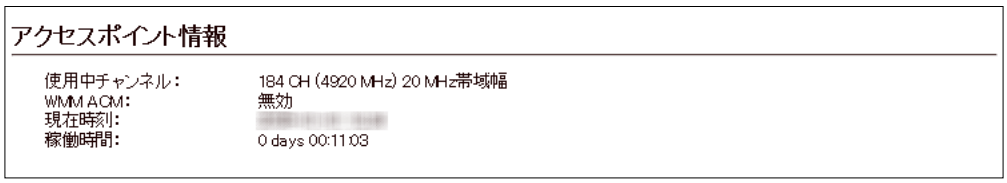
本製品の内部に蓄積されている最新のログ情報を保存するボタンです。
※クリックして、表示された画面にしたがって操作すると、ログ情報をテキスト形式（拡張子：txt）で保存できます。

3.「無線設定情報一覧 無線」画面について

情報表示 > 無線設定情報一覧 無線

■ アクセスポイント情報

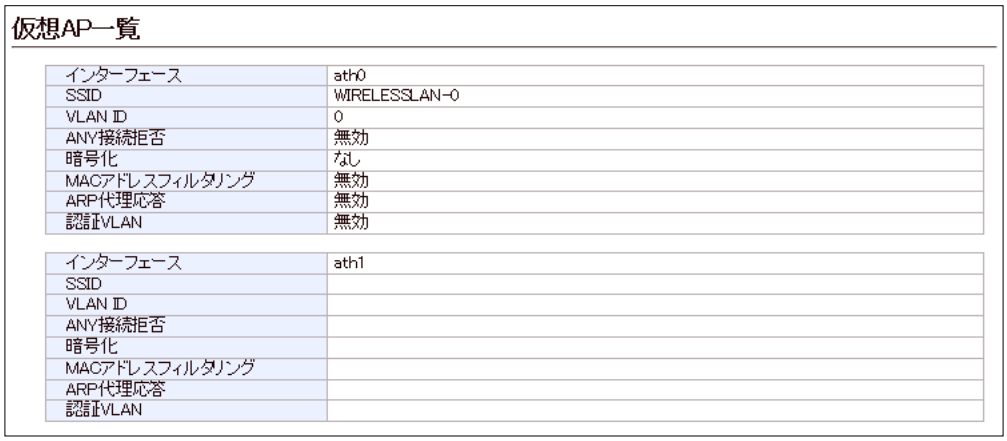
使用するチャンネル、帯域幅、稼働時間などを表示します。
※電源を切る、または設定の変更や初期化に伴う再起動で、それまでの稼働時間は初期化されます。



情報表示 > 無線設定情報一覧 無線

■ 仮想AP一覧

仮想APごとに、設定状況を一覧で表示します。
※使用していない仮想APの一覧は、[インターフェース]欄以外が空白になります。



4.「無線設定情報一覧 端末情報」画面について

情報表示 > 無線設定情報一覧 端末情報

■ 端末情報

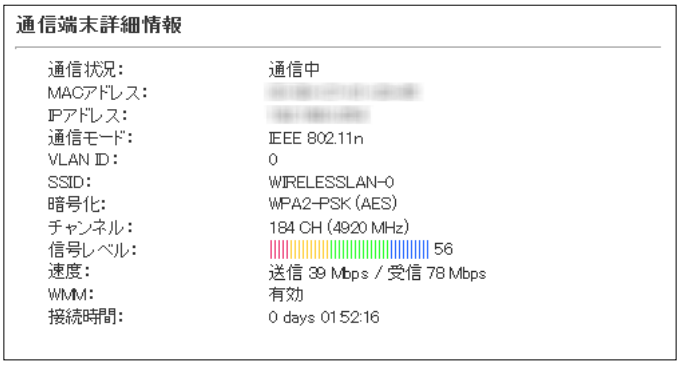
本製品と通信するFWA無線LAN端末があるとき、そのFWA無線LAN端末との通信情報を表示します。

※〈最新状態に更新〉をクリックすると、表示内容を最新の状態にします。
※〈詳細〉をクリックすると、通信中のFWA無線LAN端末について別画面(下図)で表示します。

情報表示 > 無線設定情報一覧 端末情報

■ 通信端末詳細情報

FWA無線LAN端末と通信中、「無線設定情報一覧 端末情報」画面の[端末情報]項目に表示された〈詳細〉をクリックすると表示します。



※[信号レベル]欄に、FWA無線LAN端末から受信した電波信号の強さを、メーターと数値で表示します。

表　示	[赤]	[黄]	[緑]	[青]
レベル	0～4	5～14	15～29	30以上

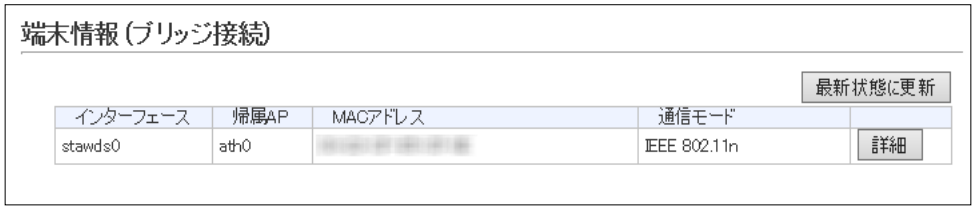
安定した通信の目安は、「緑(15)」以上のレベルです。(単位はありません)
ただし、信号レベルが高くても、同じ周波数帯域を使用するFWA機器が近くで稼働している場合やFWA機器の稼働状況などにより、通信が安定しないことがあります。
したがって、あくまでも通信の目安としてご利用ください。

4.「無線設定情報一覧 端末情報」画面について(つづき)

情報表示 > 無線設定情報一覧 端末情報

■ 端末情報(ブリッジ接続)

本製品とブリッジ接続するFWA無線LAN端末があるとき、そのFWA無線LAN端末との通信情報を表示します。

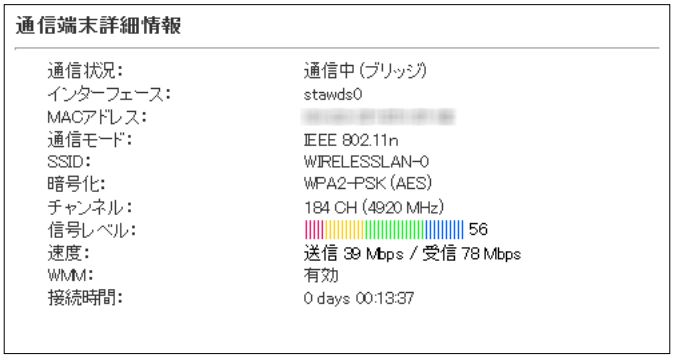


※〈最新状態に更新〉をクリックすると、表示内容を最新の状態にします。
※〈詳細〉をクリックすると、ブリッジ接続で通信中のFWA無線LAN端末について別画面(下図)で表示します。

情報表示 > 無線設定情報一覧 端末情報 > 通信端末詳細情報

■ 通信端末詳細情報(ブリッジ接続)

FWA無線LAN端末とブリッジ接続で通信中、「無線設定情報一覧 端末情報」画面の[端末情報(ブリッジ接続)]項目に表示された〈詳細〉をクリックすると表示します。



※[信号レベル]欄に、FWA無線LAN端末から受信した電波信号の強さを、メーターと数値で表示します。

表 示	[赤]	[黄]	[緑]	[青]
レベル	0～4	5～14	15～29	30以上

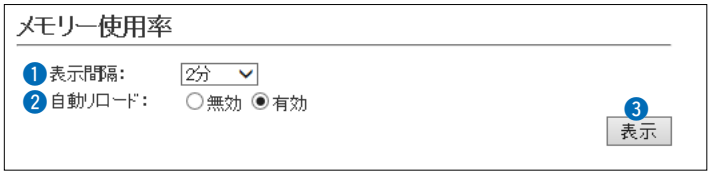
安定した通信の目安は、「緑(15)」以上のレベルです。(単位はありません)
ただし、信号レベルが高くても、同じ周波数帯域を使用するFWA機器が近くで稼働している場合やFWA機器の稼働状況などにより、通信が安定しないことがあります。
したがって、あくまでも通信の目安としてご利用ください。

5.「統計情報」画面について

情報表示 > 統計情報

■ メモリー使用率

本製品のメモリー使用率について、統計グラフを表示します。
※[メモリー使用率]項目の各設定内容は、設定画面へのアクセスごとに、出荷時の状態に戻ります。

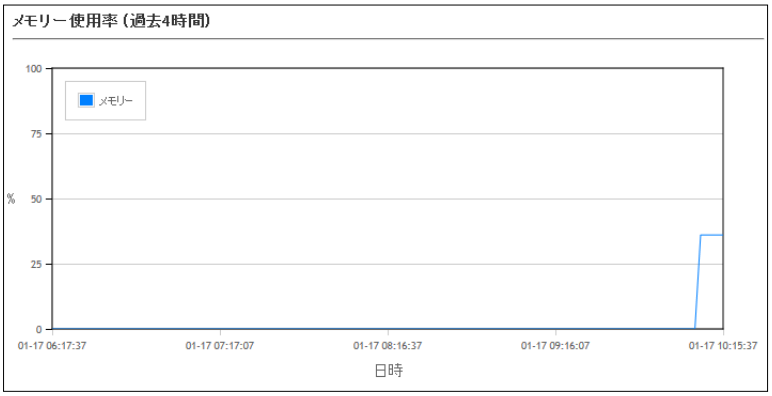


❶表示間隔 …… グラフに表示するサンプリング間隔を、「2分」、「1時間」から選択します。
（出荷時の設定：2分）

❷自動リロード …… 定期的にグラフを再描画するかどうかを設定します。（出荷時の設定：有効）
※再描画する間隔は、[表示間隔]（❶）欄で設定した時間になります。

❸〈表示〉 …… クリックすると、メモリー使用率グラフを別画面で表示します。

【メモリー使用率グラフについて】



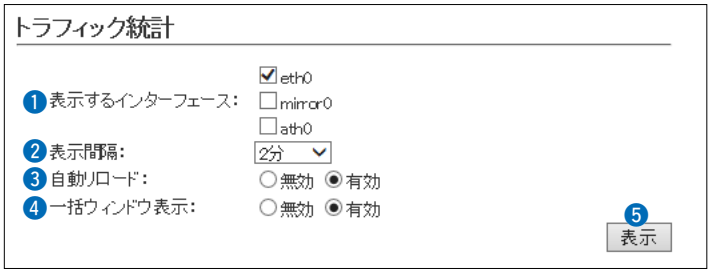
※上図は、表示例です。
※横軸は日時、縦軸はメモリー使用率を表示します。

5.「統計情報」画面について(つづき)

情報表示 > 統計情報

■ トラフィック統計

本製品のインターフェースごとに、トラフィックの統計グラフを表示します。
※[トラフィック統計]項目の各設定内容は、設定画面へのアクセスごとに、出荷時の状態に戻ります。



❶表示するインターフェース … インターフェースの各グラフについて、表示/非表示を選択します。
表示に設定するときは、インターフェースのチェックボックスをクリックして、チェックマーク[✔]を入れます。
(出荷時の設定：✔eth0 □ mirror0 □ ath0)

❷表示間隔 …… グラフに表示するサンプリング間隔を、「2分」、「1時間」から選択します。
(出荷時の設定：2分)

❸自動リロード …… 定期的にグラフを再描画するかどうかを設定します。(出荷時の設定：有効)
※再描画する間隔は、[表示間隔](❷)欄で設定した時間になります。

❹一括ウィンドウ表示 …… 選択したインターフェースのグラフについて、表示方法を設定します。
(出荷時の設定：有効)

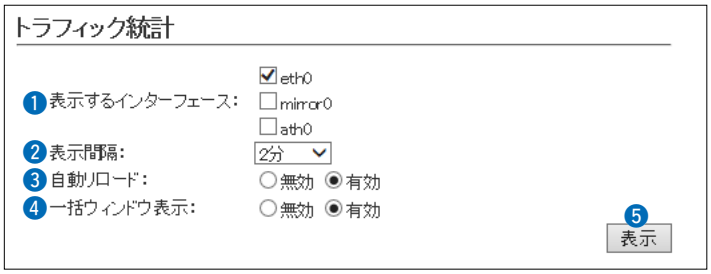
◎有効
選択したすべてのインターフェースを1つの画面内に並べて表示します。

◎無効
インターフェースごとに、別画面でグラフを表示します。
※ご使用の環境によっては、ポップアップに対する警告が表示されることがあります。
この場合、WWWブラウザーの設定でポップアップ表示の許可が必要です。

5.「統計情報」画面について

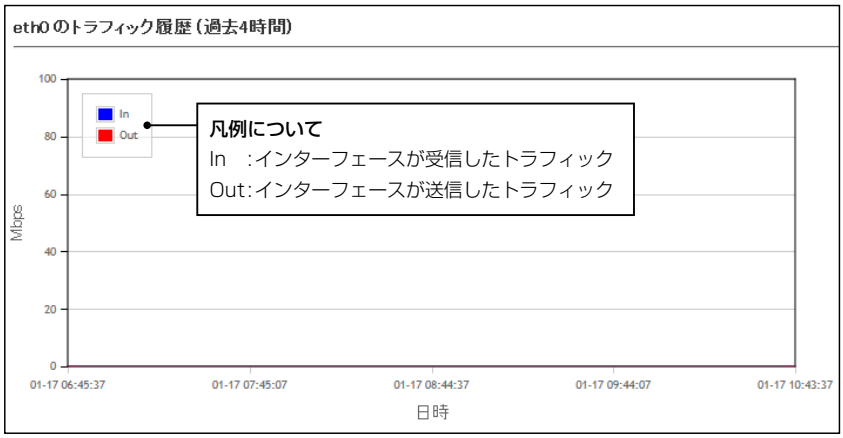
情報表示 > 統計情報

■ トラフィック統計（つづき）



5〈表示〉 …… クリックすると、トラフィック統計グラフを別画面で表示します。

【トラフィック統計グラフについて】



※上図は、表示例です。

※横軸は日時、縦軸はトラフィックの状態を表示します。

「ネットワーク設定」メニュー

第 3 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ています。

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

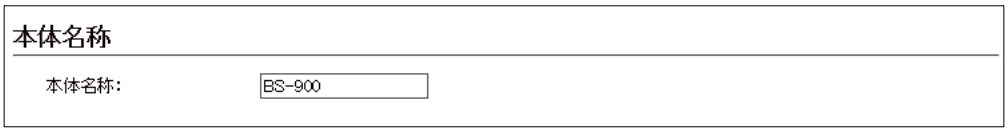
3 「ネットワーク設定」メニュー

1.「LAN側IP」画面について

ネットワーク設定 ＞ LAN側IP

■ 本体名称

本製品の名称を設定します。



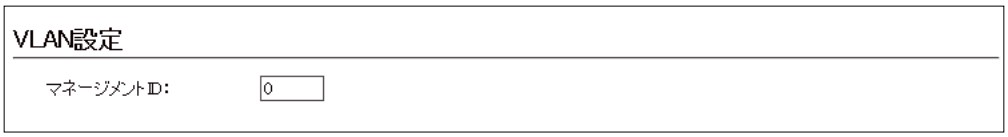
本体名称……

「Telnet」で本製品に接続したとき、ここで設定した本体名称を表示します。
（出荷時の設定：BS-900）
※半角英数字（a～ｚ、A～Z、0～9、－）を、任意の31文字以内で設定します。
なお、半角英数字以外の文字は、使用しないでください。
※「－（ハイフン）」を本体名称の先頭、または末尾に使用すると、登録できません。

ネットワーク設定 ＞ LAN側IP

■ VLAN設定

VLAN機能についての設定です。



マネージメントID ……

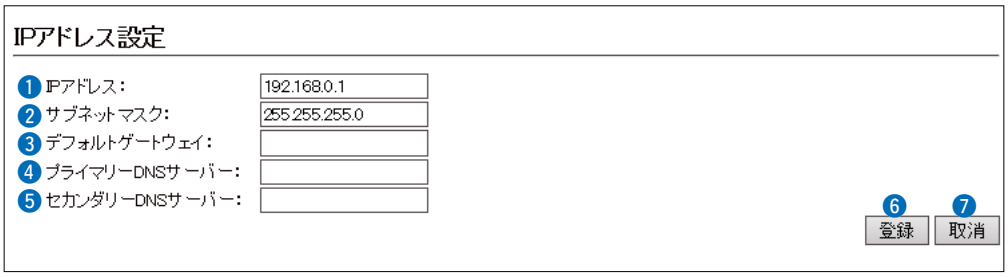
本製品に設定された同じID番号を持つネットワーク上の機器からのアクセスだけを許可できます。（出荷時の設定：0）
設定できる範囲は、「0～4094」です。
※VLAN IDを使用しないネッワークから本製品にアクセスするときは、「0」を設定します。
※不用意に設定すると、本製品の設定画面にアクセスできなくなりますのでご注意ください。

1.「LAN側IP」画面について(つづき)

ネットワーク設定 > LAN側IP

■ IPアドレス設定

本製品のLAN側IPアドレスを設定します。



❶IPアドレス ……

本製品のIPアドレスを設定します。
(出荷時の設定:192.168.0.1)
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LANに合わせたネットワークアドレスに変更してください。
※本製品のDHCPサーバー機能を使用する場合は、[DHCPサーバー設定]項目の[割り当て開始IPアドレス]欄(P.3-5)についてもネットワーク部を同じ設定にしてください。

❷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LANに合わせたサブネットマスクに変更してください。

例:サブネットマスクを「255.255.255.248」に設定すると、同じネットワークで使用するIPアドレスは、「192.168.0.0~192.168.0.7」の範囲になります。
この場合、「192.168.0.2~192.168.0.6」が端末に割り当てできるIPアドレスになります。
なお、端末に割り当てできないIPアドレスは次のようになります。
「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

❸デフォルトゲートウェイ ……

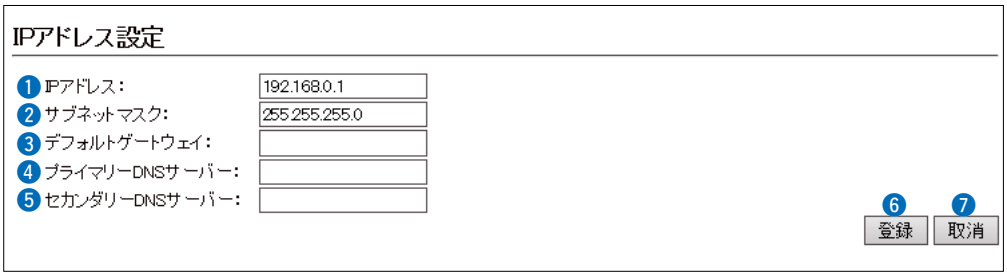
本製品とネットワーク部が異なる接続先と通信する場合、パケット転送先機器のIPアドレスを入力します。
※本製品と同じIPアドレスは登録できません。

3 「ネットワーク設定」メニュー

1.「LAN側IP」画面について

ネットワーク設定 > LAN側IP

■ IPアドレス設定(つづき)



❹プライマリーDNSサーバー … 本製品がアクセスするDNSサーバーのアドレスを入力します。
※使い分けたいアドレスが2つある場合は、優先したい方のアドレスを入力してください。

❺セカンダリーDNSサーバー … [プライマリーDNSサーバー](❹)欄と同様に、本製品がアクセスするDNSサーバーのアドレスを入力します。
※必要に応じて、使い分けたいDNSサーバーアドレスのもう一方を入力します。

❻〈登録〉 …… 「LAN側IP」画面で設定した内容を登録するボタンです。

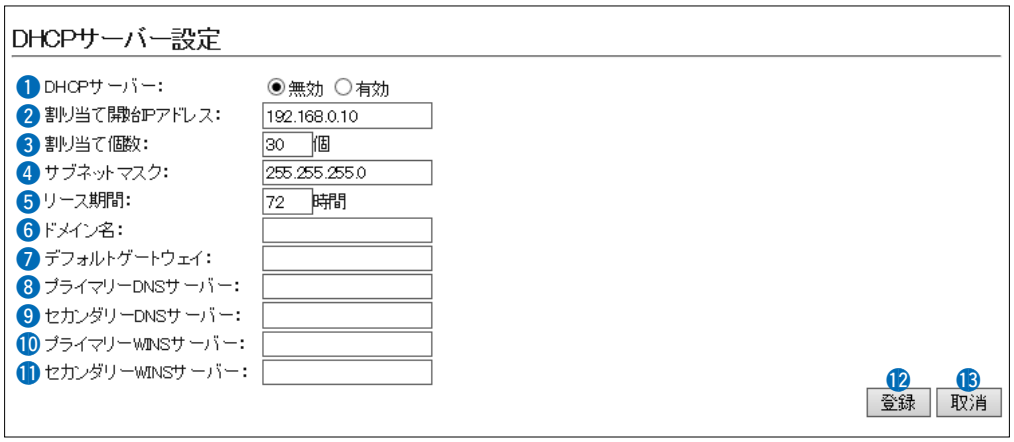
❼〈取消〉 …… 「LAN側IP」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

2.「DHCPサーバー」画面について

ネットワーク設定 > DHCPサーバー

■ DHCPサーバー設定

DHCPサーバー機能についての設定です。



❶DHCPサーバー …… 本製品のDHCPサーバー機能を設定します。（出荷時の設定：無効）
「有効」に設定すると、[DHCPサーバー設定]項目の❷～⓫に設定された内容にしたがって、DHCPサーバーとして動作します。

❷割り当て開始IPアドレス …… 本製品に接続する端末へ、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）

❸割り当て個数 …… 本製品が自動割り当てできるIPアドレスの個数を設定します。
（出荷時の設定：30）
[割り当て開始IPアドレス](❷)欄に設定されたIPアドレスから連続で自動割り当てできるIPアドレスの最大個数は、「0～128」(個)までです。
※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。

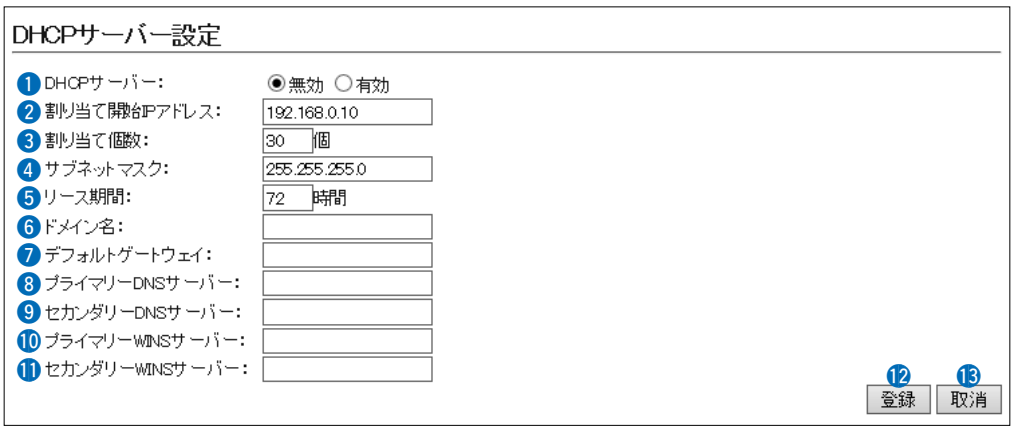
❹サブネットマスク …… [割り当て開始IPアドレス](❷)欄に設定されたIPアドレスに対するサブネットマスクです。（出荷時の設定：255.255.255.0）

❺リース期間 …… DHCPサーバーが割り当てるIPアドレスの有効期間を時間で指定します。
設定できる範囲は、「1～9999」(時間)です。（出荷時の設定：72）

2.「DHCPサーバー」画面について

ネットワーク設定 > DHCPサーバー

■ DHCPサーバー設定(つづき)



❻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サーバーが端末に通知するネットワークのドメイン名を127文字(半角英数字)以内で入力します。

❼デフォルトゲートウェイ …… 本製品のDHCPサーバー機能を使用するときに、[割り当て開始IPアドレス](❷)欄のIPアドレスとネットワーク部が異なる接続先と通信する場合、パケット転送先機器のIPアドレスを入力します。
※本製品のIPアドレスと重複しないように設定してください。

❽プライマリーDNSサーバー … DNSサーバーを利用する場合は、DNSサーバーアドレスを入力します。
DNSサーバーのアドレスが2つある場合は、優先したい方のアドレスを入力します。

❾セカンダリーDNSサーバー … [プライマリーDNSサーバー](❽)欄と同様、DNSサーバーのアドレスが2つある場合は、残りの一方を入力します。

❿プライマリーWINSサーバー WINSサーバーを利用する場合は、WINSサーバーアドレスを入力します。
WINSサーバーのアドレスが2つある場合は、優先したい方のアドレスを入力します。

⓫セカンダリーWINSサーバー [プライマリーWINSサーバー](❿)欄と同様、WINSサーバーのアドレスが2つある場合は、残りの一方を入力します。

⓬〈登録〉 …… [DHCPサーバー設定]項目で設定した内容を登録するボタンです。

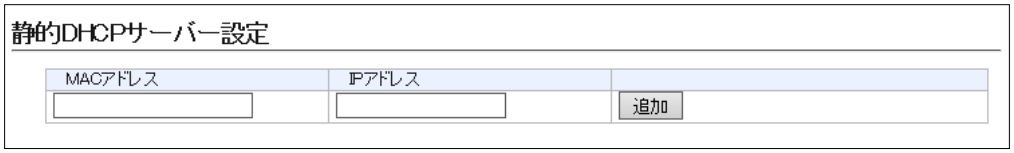
⓭〈取消〉 …… [DHCPサーバー設定]項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

2.「DHCPサーバー」画面について（つづき）

ネットワーク設定 > DHCPサーバー

■ 静的DHCPサーバー設定

固定IPアドレスを特定の端末に割り当てる設定です。

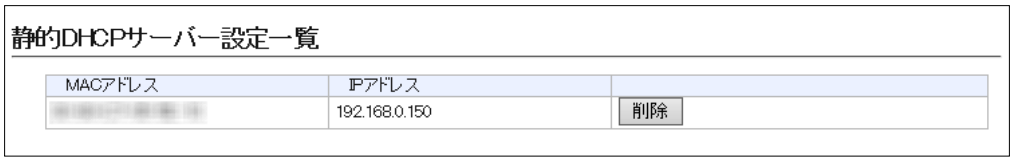


静的DHCPサーバー設定 …… 端末のMACアドレスとIPアドレスの組み合わせを登録します。
※本製品のDHCPサーバー機能を使用する場合に有効です。（P.3-5）
※入力後は、〈追加〉をクリックしてください。
※最大32個の組み合わせまで登録できます。
※DHCPサーバー機能により自動で割り当てられるIPアドレスの範囲外でIPアドレスを設定してください。
例：[DHCPサーバー設定]項目で、[割り当て開始IPアドレス]欄と[割り当て個数]欄が出荷時の設定の場合は、192.168.0.40以降のIPアドレスを設定してください。
※本製品のIPアドレスと重複しないように設定してください。

ネットワーク設定 > DHCPサーバー

■ 静的DHCPサーバー設定一覧

[静的DHCPサーバー設定]項目で登録した内容を表示します。
※画面の値は、登録例です。



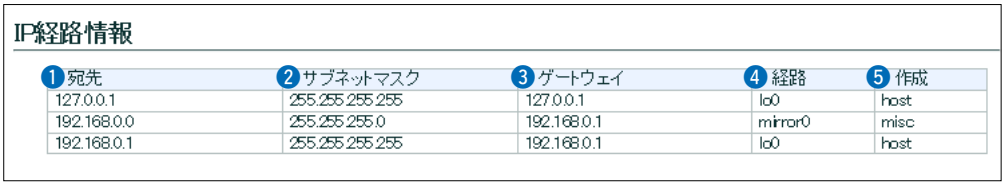
〈削除〉…… 登録した内容を取り消すときは、該当する欄の〈削除〉をクリックします。

3.「ルーティング」画面について

ネットワーク設定 > ルーティング

■ IP経路情報

パケットの送信において、そのパケットをどのルーター、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、現在有効な経路だけを表示します。


IP経路情報

❶宛先	❷サブネットマスク	❸ゲートウェイ	❹経路	❺作成
127.0.0.1	255.255.255.255	127.0.0.1	lo0	host
192.168.0.0	255.255.255.0	192.168.0.1	mirror0	misc
192.168.0.1	255.255.255.255	192.168.0.1	lo0	host

❶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。

❷サブネットマスク …… 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。

❸ゲートウェイ… …… 宛先IPアドレスに対するゲートウェイを表示します。

❹経路 …… 宛先IPアドレスに対する転送先インターフェースを表示します。
◎**lo0** ：ループバックアドレスを意味するインターフェース
◎**mirror0** ：LANインターフェース

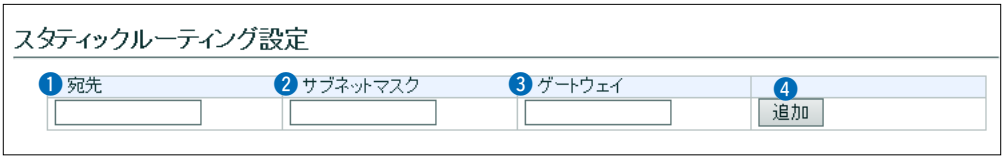
❺作成 …… どのように経路情報が作成されたかを表示します。
◎**static** ：スタティック(定義された)ルートにより作成
◎**misc** ：ブロードキャストに関係するフレーム処理で作成
◎**host** ：ホストルートにより作成

3.「ルーティング」画面について（つづき）

ネットワーク設定 > ルーティング

■ スタティックルーティング設定

パケットの中継経路を最大32件まで登録できます。



❶宛先 …… 対象となる相手先のIPアドレスを入力します。

❷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。

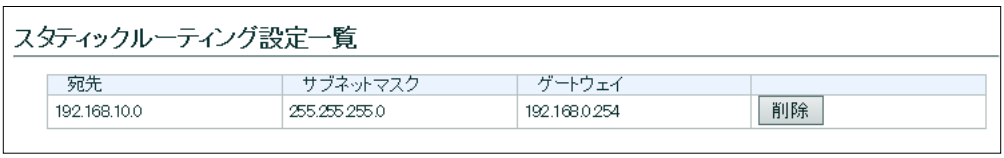
❸ゲートウェイ …… パケット転送先ルーターのIPアドレスを入力します。

❹〈追加〉 … …… クリックすると、入力内容が登録されます。
［スタティックルーティング設定一覧］項目で登録した内容を確認できます。

ネットワーク設定 > ルーティング

■ スタティックルーティング設定一覧

［スタティックルーティング設定］項目で登録した内容を表示します。
※画面の値は、入力例です。



〈削除〉…… 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。

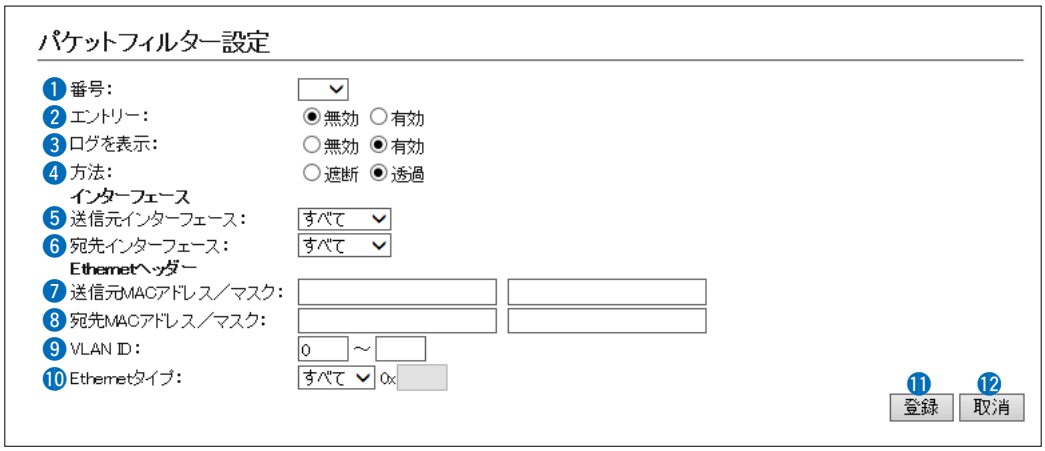
株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

4.「パケットフィルター」画面について

ネットワーク設定 > パケットフィルター

■ パケットフィルター設定

登録したエントリーに該当するパケットを通過させたり、遮断したりするフィルターの設定です。



❶番号 ……

フィルターが比較する順位を指定します。
設定できる範囲は、「1～64」です。
本製品が受信、または送信するパケットと[現在の登録]項目に表示されたフィルターと比較します。
※フィルタリングの条件は、1つ以上指定してください。
※番号が指定されていないときは、登録できません。
※IPv6のパケットには対応していません。

順位と比較について

フィルターを複数設定しているときは、番号の小さい順番に比較を開始します。
フィルタリングの条件に一致した中から、番号が最小のエントリーで処理をします。
※フィルタリングの条件に一致した時点で、それ以降の番号のエントリーは比較しません。

❷エントリー ……

登録するフィルターの使用について設定します。　（出荷時の設定：無効）
登録だけして使用しないときは、「無効」を選択します。

❸ログを表示 ……

「情報表示」メニューの「SYSLOG」画面へのログ表示について設定します。
（出荷時の設定：有効）

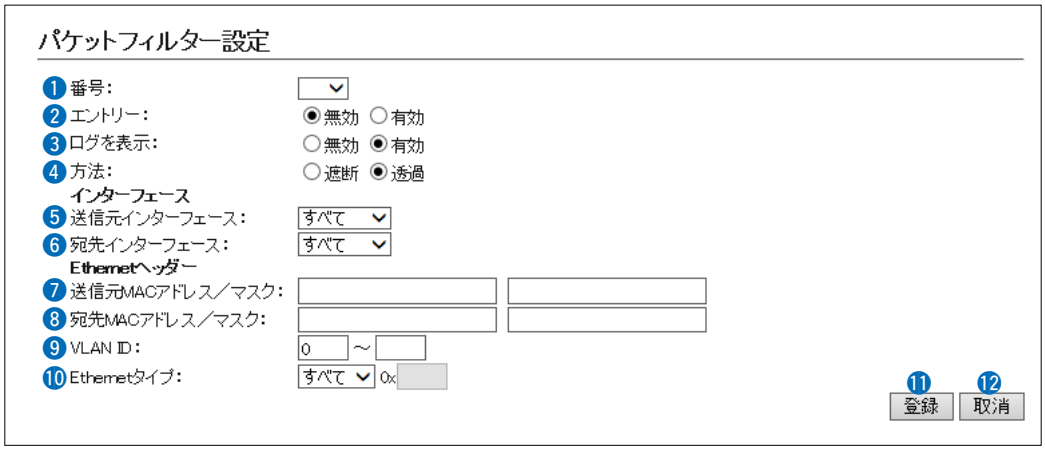
❹方法 ……

フィルタリング方法を選択します。　（出荷時の設定：透過）
◎**遮断**：すべてのフィルタリング条件に一致した場合、そのパケットを破棄します。
◎**透過**：すべてのフィルタリング条件に一致した場合、そのパケットを通過します。

4.「パケットフィルター」画面について

ネットワーク設定 > パケットフィルター

■ パケットフィルター設定(つづき)



❺送信元インターフェース ……

フィルタリングの対象となる送信元インターフェースを選択します。
(出荷時の設定:すべて)

◎mirror0 :インターフェースが本製品自身の場合
◎eth0 :インターフェースが有線LANの場合
◎ath0~ath7 :インターフェースが本製品の無線LAN(仮想AP)の場合
◎stawds0~stawds7 :インターフェースがブリッジ接続の場合

※「すべて」を選択すると、「mirror0」、「eth0」、「ath0~ath7」、「stawds0~stawds7」が送信元インターフェースの対象になります。
※無線ブリッジ接続している端末は、ath0を指定しても条件に一致しません。stawds0~stawds7で指定してください。

❻宛先インターフェース ……

フィルタリングの対象となる宛先インターフェースを選択します。
(出荷時の設定:すべて)

◎mirror0 :インターフェースが本製品自身の場合
◎eth0 :インターフェースが有線LANの場合
◎ath0~ath7 :インターフェースが本製品の無線LAN(仮想AP)の場合
◎stawds0~stawds7 :インターフェースがブリッジ接続の場合

※「すべて」を選択すると、「mirror0」、「eth0」、「ath0~ath7」、「stawds0~stawds7」が宛先インターフェースの対象になります。
※無線ブリッジ接続している端末は、ath0を指定しても条件に一致しません。stawds0~stawds7で指定してください。

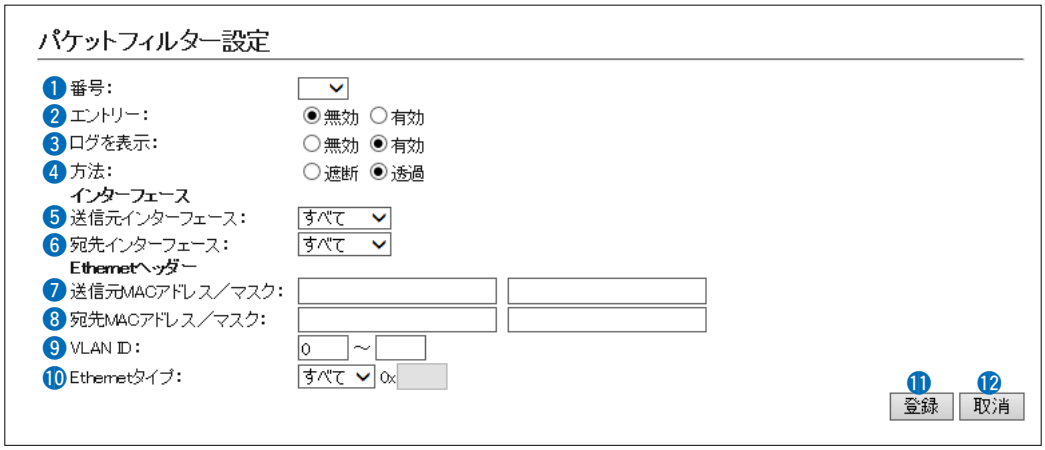
❼送信元MACアドレス/マスク ……

フィルタリングの対象となるEthernetヘッダー内において、送信元MACアドレスの有効範囲を設定します。
フィルタリングの条件として、これらを2進数で表現したときの論理積(AND)が[パケットフィルター設定一覧]項目に表示されます。(P.3-20)
※登録例については、[宛先MACアドレス/マスク](❽)欄で説明しています。

4.「パケットフィルター」画面について

ネットワーク設定 > パケットフィルター

■ パケットフィルター設定(つづき)



❽宛先MACアドレス／マスク … フィルタリングの対象となるEthernetヘッダー内において、宛先MACアドレスの有効範囲を設定します。
フィルタリングの条件として、これらを2進数で表現したときの論理積(AND)が[パケットフィルター設定一覧]項目に表示されます。(P.3-20)

MACアドレスとマスク値の登録例

[送信元MACアドレス／マスク](❼)欄についても、下記の例を参考にしてください。

※小文字で入力しても、登録結果は、登録例(例1～例3)のように大文字になります。

例1)宛先MACアドレス／マスク
00-90-C7-3C-00-64／(空白)
[パケットフィルター設定一覧]項目には、下記の内容で表示します。
00-90-C7-3C-00-64／FF-FF-FF-FF-FF-FF
※マスクを指定しないときは、「FF-FF-FF-FF-FF-FF」として登録されます。
※00-90-C7-3C-00-64に一致するMACアドレスがフィルタリングの対象になります。

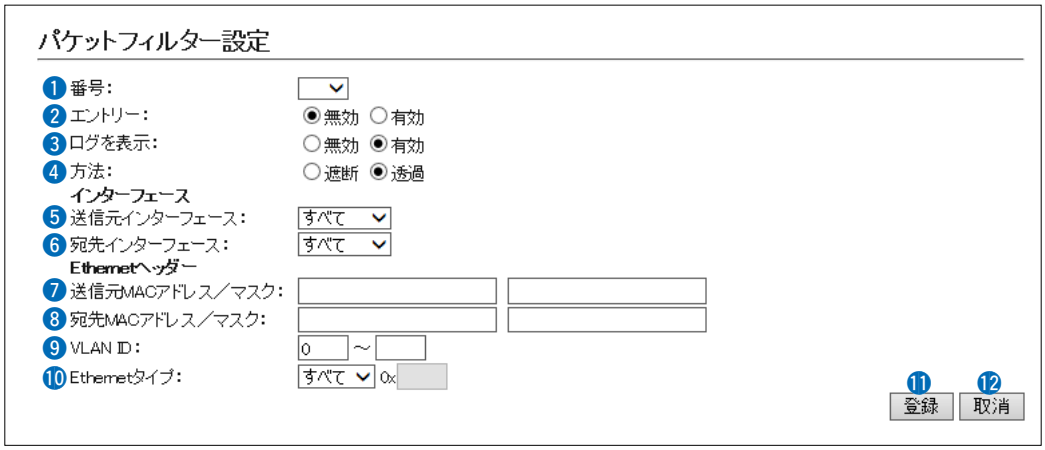
例2)宛先MACアドレス／マスク
00-90-C7-3C-00-64／FF-FF-FF-00-00-00
[パケットフィルター設定一覧]項目には、下記の内容で表示します。
00-90-C7-00-00-00／FF-FF-FF-00-00-00
※マスク値「0」との論理積は、「0」になるため、「00-90-C7」部分が一致するMACアドレスがフィルタリング対象になります。

例3)宛先MACアドレス／マスク
00-90-C7-3C-00-64／FF-FF-FF-00-00-FF
[パケットフィルター設定一覧]項目には、下記の内容で表示します。
00-90-C7-00-00-64／FF-FF-FF-00-00-FF
※00-90-C7-00-00-64 ～ 00-90-C7-FF-FF-64までが有効範囲になります。
例2と同様、マスク「00」の部分は、どんな値のMACアドレスでもフィルタリングの条件に一致する対象になります。

4.「パケットフィルター」画面について

ネットワーク設定 > パケットフィルター

■ パケットフィルター設定(つづき)



❾VLAN ID ……

フィルタリングの対象となる[VLAN ID]を指定(開始値～終端値)します。
入力できる範囲は、「0～4094」です。
「0」を開始値に指定したときは、範囲指定できません。
※開始値だけを設定したときは、一致するパケットが対象です。
※「0」は、VLANタグのないパケット、およびVLAN IDが「0」のパケットが対象です。
「0」以外は、指定のVLANタグ付きパケットが対象です。

❿Ethernetタイプ ……

フィルタリングの対象となるEthernetタイプ名称(ARP/IP)、または16進数(0000～FFFF(4桁))で指定します。 (出荷時の設定:すべて)
※16進数で指定するとき、小文字(例:ffff)で入力しても、登録結果は大文字(例:FFFF)になります。

⓫〈登録〉 ……

クリックすると、「パケットフィルター設定」画面で設定した内容が登録されます。

⓬〈取消〉 ……

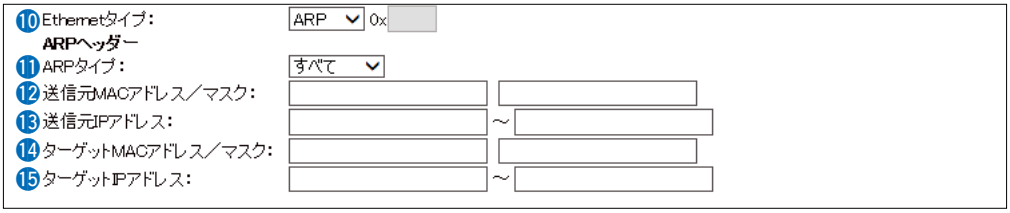
「パケットフィルター設定」画面で設定した内容を取消、出荷時の設定に戻すボタンです。
なお、〈登録〉をクリックすると、変更前の状態には戻りません。

4.「パケットフィルター」画面について

ネットワーク設定 > パケットフィルター

■ パケットフィルター設定(つづき)

[Ethernetタイプ](⑩)欄で、「ARP」を選択したときは、下記の画面になります。



⑪ARPタイプ ……

フィルタリングの対象となるARPタイプを選択します。
(出荷時の設定:すべて)
「すべて」、「request」、「reply」、「rrequest」、「rreply」の中から選択できます。
※「すべて」を選択すると、すべてのARPタイプに該当します。

⑫送信元MACアドレス/マスク ……

フィルターの対象となるARPヘッダー内において、送信元MACアドレスの有効範囲を設定します。
フィルタリングの条件として、これらを2進数で表現したときの論理積(AND)が[パケットフィルター設定一覧]項目に表示されます。(P.3-20)
※登録例については、[宛先MACアドレス/マスク](⑧)欄で説明しています。

⑬送信元IPアドレス ……

フィルターの対象となるARPヘッダー内において、送信元IPアドレスの有効範囲(開始値~終端値)を設定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。

⑭ターゲットMACアドレス/マスク ……

フィルターの対象となるARPヘッダー内において、ターゲットMACアドレスの有効範囲を設定します。
フィルタリングの条件として、これらを2進数で表現したときの論理積(AND)が[パケットフィルター設定一覧]項目に表示されます。(P.3-20)
※登録例については、[宛先MACアドレス/マスク](⑧)欄で説明しています。

⑮ターゲットIPアドレス ……

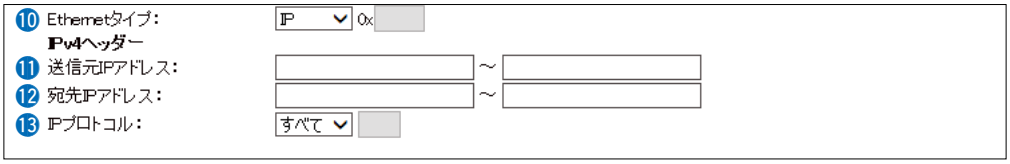
フィルターの対象となるARPヘッダー内において、ターゲットIPアドレスの有効範囲(開始値~終端値)を設定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。

4.「パケットフィルター」画面について

ネットワーク設定 > パケットフィルター

■ パケットフィルター設定(つづき)

[Ethernetタイプ](⑩)欄で「IP」、[IPプロトコル](⑬)欄で「すべて」/[指定]を選択したときは、下記の画面になります。



⑪送信元IPアドレス ……

フィルターの対象となるIPヘッダー内において、送信元IPアドレスの有効範囲(開始値～終端値)を設定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。

⑫宛先IPアドレス ……

フィルターの対象となるIPヘッダー内において、宛先IPアドレスの有効範囲(開始値～終端値)を設定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。

⑬IPプロトコル ……

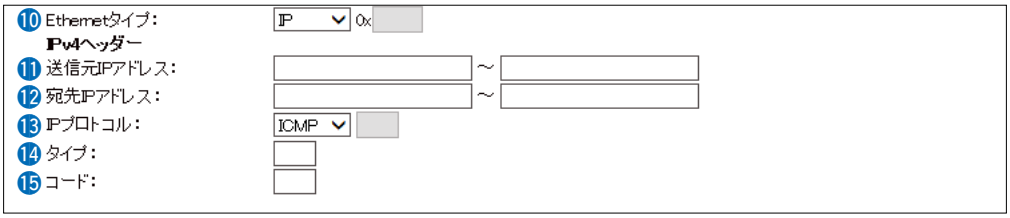
フィルターの対象となるIPヘッダー内において、パケットのトランスポート層プロトコルを選択します。
◎**すべて**：すべてのプロトコルに一致します。
◎**ICMP**：ICMPだけに一致します。
◎**IGMP**：IGMPだけに一致します。
◎**TCP**：TCPだけに一致します。
◎**UDP**：UDPだけに一致します。
◎**指定**：右のテキストボックスに、IPヘッダーに含まれるパケットのトランスポート層プロトコル番号を入力します。
プロトコル番号は、10進数で0～255までの半角数字を入力します。

4.「パケットフィルター」画面について

ネットワーク設定 > パケットフィルター

■ パケットフィルター設定(つづき)

[Ethernetタイプ](⑩)欄で「IP」、[IPプロトコル](⑬)欄で「ICMP」を選択したときは、下記の画面になります。



⑭タイプ …… フィルタリングの対象となるICMPヘッダー内のタイプを番号(0～255)で指定します。
※指定しないときは、すべてがフィルタリングの対象になります。

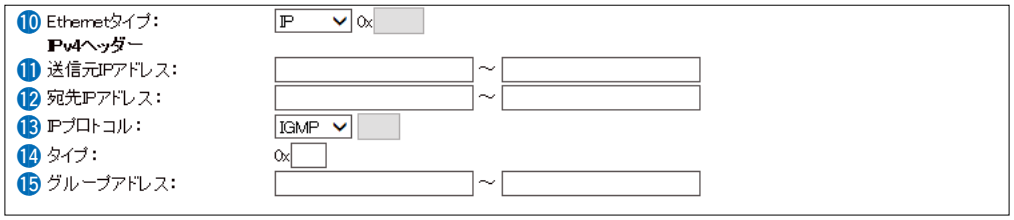
⑮コード …… フィルタリングの対象となるICMPヘッダー内のコードを番号(0～255)で指定します。
※指定しないときは、すべてがフィルタリングの対象になります。

4.「パケットフィルター」画面について

ネットワーク設定 > パケットフィルター

■ パケットフィルター設定(つづき)

[Ethernetタイプ](⑩)欄で「IP」、[IPプロトコル](⑬)欄で「IGMP」を選択したときは、下記の画面になります。



⑭タイプ ……

フィルタリングの対象となるIGMPヘッダー内のタイプを16進数(00～FF(2桁))で指定します。
※指定しないときは、すべてがフィルタリングの対象になります。
※16進数で指定するときは、小文字(例：ff)で入力しても、登録結果は大文字(例：FF)になります。

⑮グループアドレス ……

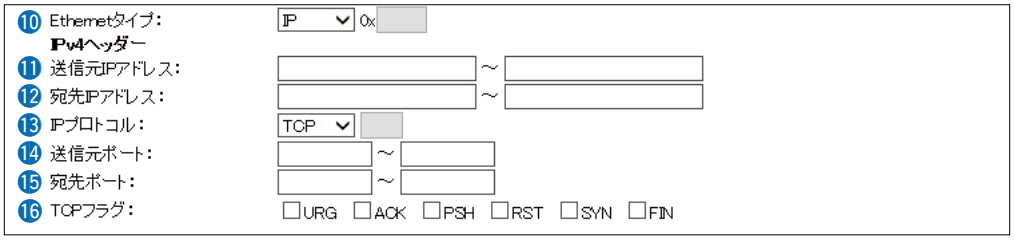
フィルタリングの対象となるIGMPヘッダー内のマルチキャストグループアドレスの有効範囲(開始値～終端値)を設定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。
※IPv6には対応していません。

4.「パケットフィルター」画面について

ネットワーク設定 > パケットフィルター

■ パケットフィルター設定(つづき)

[Ethernetタイプ](⑩)欄で「IP」、[IPプロトコル](⑬)欄で「TCP」を選択したときは、下記の画面になります。



⑭送信元ポート ……

フィルタリングの対象となる送信元TCPポート番号(1～65535)の有効範囲(開始値～終端値)を指定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「1」から終端値までの範囲をフィルタリングします。
◎送信元ポートを指定しないときは、すべてのTCPポート番号がフィルタリングの対象になります。
※TCPヘッダー内のSource Portと比較します。

⑮宛先ポート ……

フィルタリングの対象となる宛先TCPポート番号(1～65535)の有効範囲(開始値～終端値)を指定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「1」から終端値までの範囲をフィルタリングします。
◎宛先ポートを指定しないときは、すべてのTCPポート番号がフィルタリングの対象になります。
※TCPヘッダー内のDestination Portと比較します。

⑯TCPフラグ ……

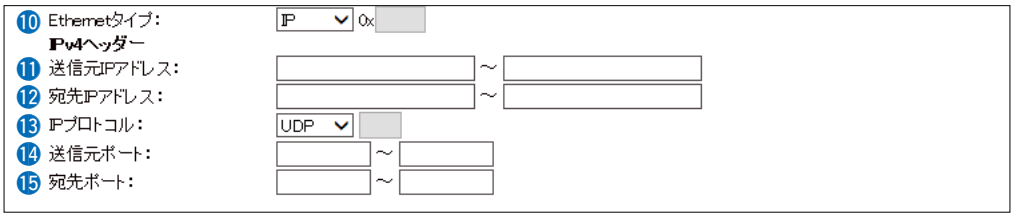
フィルタリングの対象となるTCPフラグを指定します。
※本製品で指定できるフラグは、URG、ACK、PSH、RST、SYN、FINです。
※TCPヘッダー内のTCPフラグと比較します。
※選択したフラグは、[パケットフィルター設定一覧]項目に表示されます。
※何も指定しない場合は、TCPフラグの状態に関係なくフィルタリングの対象になります。
※複数のフラグを選択した場合は、複数のフラグが同時に立っているパケットをフィルタリングの対象とします。

4.「パケットフィルター」画面について

ネットワーク設定 > パケットフィルター

■ パケットフィルター設定(つづき)

[Ethernetタイプ](⑩)欄で「IP」、[IPプロトコル](⑬)欄で「UDP」を選択したときは、下記の画面になります。



⑭送信元ポート ……

フィルタリングの対象となる送信元UDPポート番号(1～65535)の有効範囲(開始値～終端値)を指定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「1」から終端値までの範囲をフィルタリングします。
◎送信元ポートを指定しないときは、すべてのUDPポート番号がフィルタリングの対象になります。
※UDPヘッダー内のSource Portと比較します。

⑮宛先ポート ……

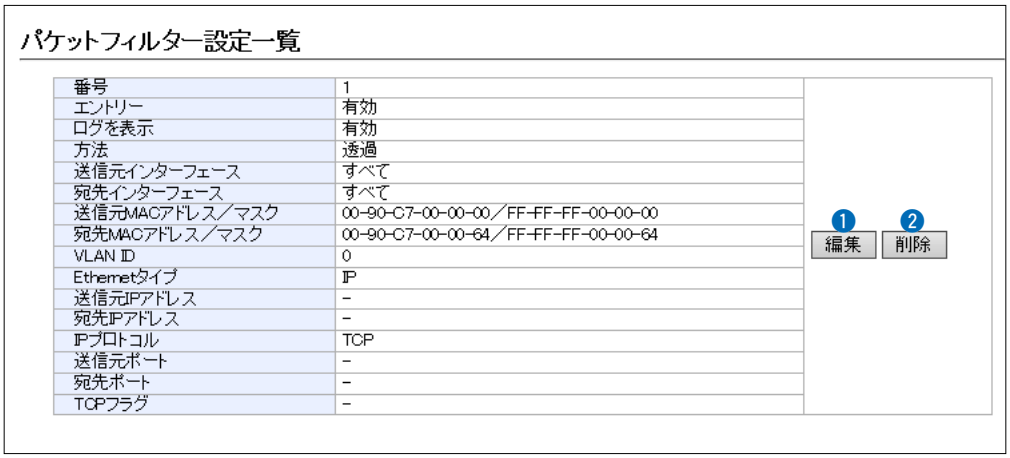
フィルタリングの対象となる宛先UDPポート番号(1～65535)の有効範囲(開始値～終端値)を指定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「1」から終端値までの範囲をフィルタリングします。
◎宛先ポートを指定しないときは、すべてのUDPポート番号がフィルタリングの対象になります。
※UDPヘッダー内のDestination Portと比較します。

4.「パケットフィルター」画面について（つづき）

ネットワーク設定 > パケットフィルター

■ パケットフィルター設定一覧

[パケットフィルター設定]項目から登録した現在の各エントリーの内容を表示します。



❶〈編集〉 …… 左の欄に表示されるエントリーを編集するボタンです。
クリックすると、その左の欄に表示された内容を[パケットフィルター設定]項目の各欄に表示します。（P.3-10）

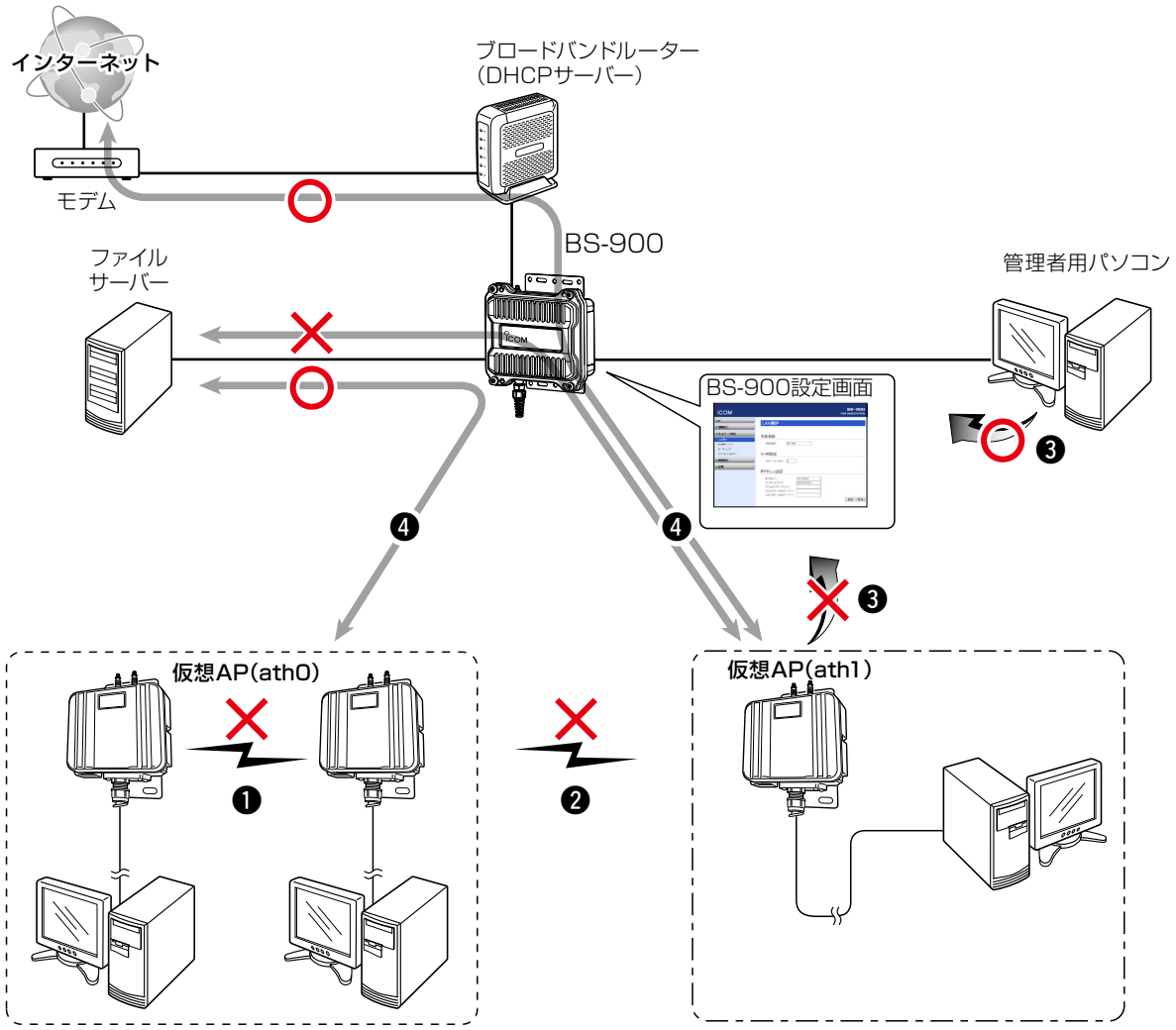
❷〈削除〉 …… 左の欄に表示されたエントリーを削除するボタンです。
〈削除〉をクリックすると、削除されます。

4.「パケットフィルター」画面について（つづき）

ネットワーク設定 > パケットフィルター

■ パケットフィルターの使用例

下図とその説明（❶～❹）に示すような使用例について、パケットフィルターの登録方法を説明します。



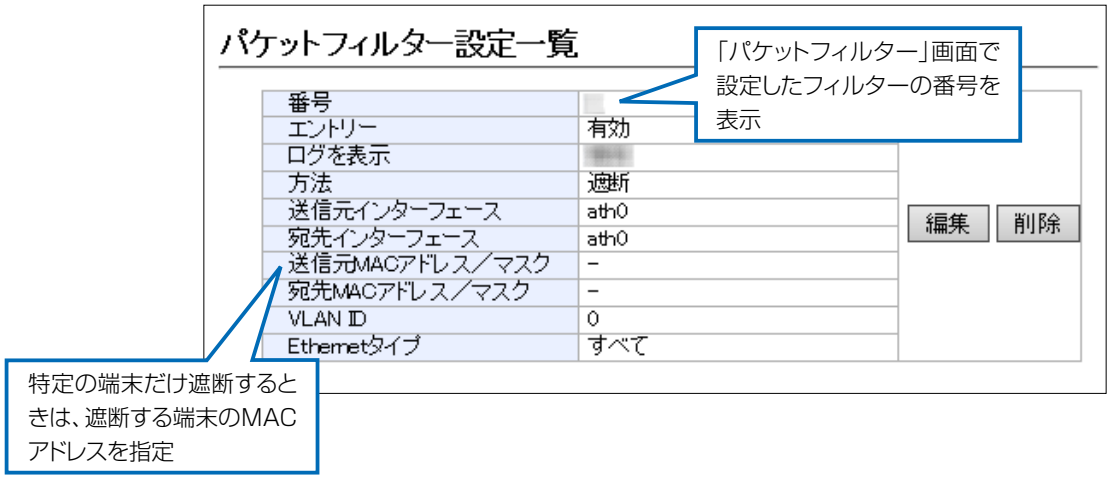
無線LANのパケットについて
通常端末の場合、送信元や宛先インターフェースは、ath0～ath7を指定します。
※無線ブリッジ接続している端末は、stawds0～stawds7を指定してください。（ath0を指定しても条件に一致しません。）

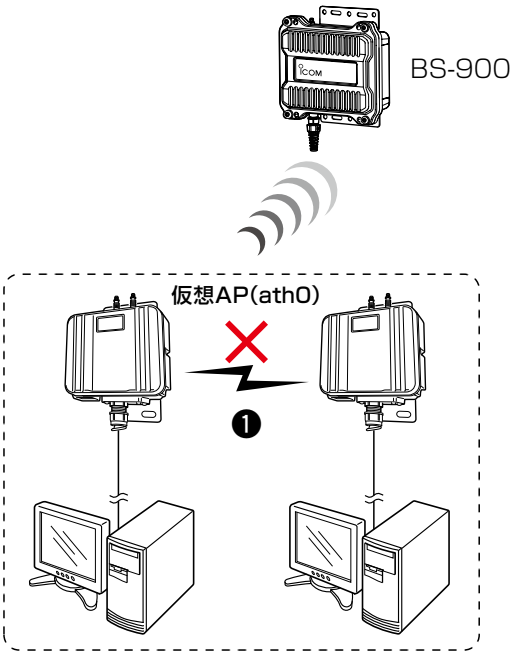
4.「パケットフィルター」画面について（つづき）

ネットワーク設定 > パケットフィルター

❶仮想AP内のFWA無線LAN端末同士の通信を禁止するには

送信元インターフェース、宛先インターフェースともにath0を設定することによりath0に接続した無線端末間通信禁止ができます。
※特定の端末だけ遮断するときは、MACアドレスを指定します。
※MACアドレスを指定しない場合、ath0に接続するすべての無線端末同士を遮断します。





4.「パケットフィルター」画面について（つづき）

ネットワーク設定 > パケットフィルター

❷仮想AP間のFWA無線LAN端末同士の通信を禁止するには

下記の2つ（❶と❷）のフィルターの登録が必要です。

❶ 仮想AP（ath0）→仮想AP（ath1）方向の通信を遮断

❷ 仮想AP（ath1）→仮想AP（ath0）方向の通信を遮断

パケットフィルター設定一覧

「パケットフィルター」画面で設定したフィルターの番号を表示

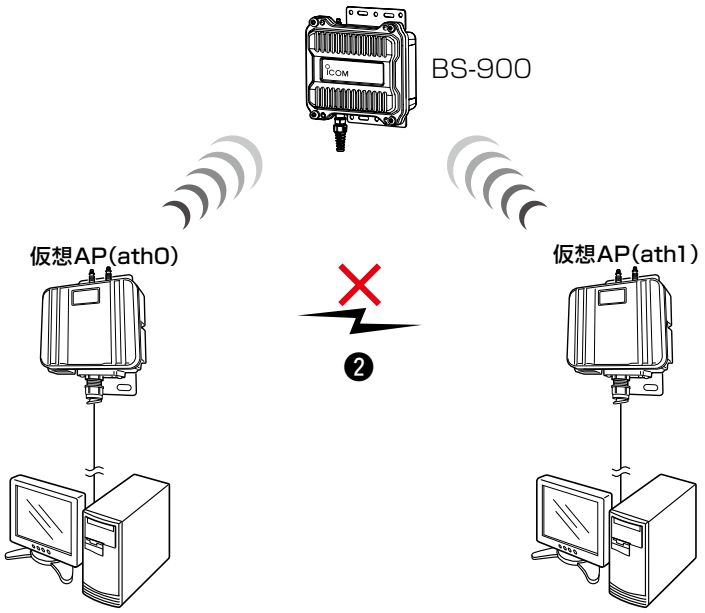
番号	[redacted]
エントリー	有効
ログを表示	[redacted]
方法	遮断
送信元インターフェース	ath0
宛先インターフェース	ath1
送信元MACアドレス／マスク	-
宛先MACアドレス／マスク	-
VLAN ID	0
Ethernetタイプ	すべて

編集 削除

上記のフィルターで登録した番号と異なる番号を表示

番号	[redacted]
エントリー	有効
ログを表示	[redacted]
方法	遮断
送信元インターフェース	ath1
宛先インターフェース	ath0
送信元MACアドレス／マスク	-
宛先MACアドレス／マスク	-
VLAN ID	0
Ethernetタイプ	すべて

編集 削除



4.「パケットフィルター」画面について（つづき）

ネットワーク設定 > パケットフィルター

❸BS-900の設定画面へのアクセスを管理者用端末に制限するには

下記の2つ（❶と❷）のフィルターの登録が必要です。

※ マネージメントID（VLAN設定）を「0」に設定した場合を例に説明しています。

※ 設定に使用する端末からのWEB画面へのアクセスを妨げないようエントリー追加・削除の順番は、注意してください。エントリーを追加するときは、透過エントリー→遮断エントリーの順に、エントリーの削除は、遮断エントリー→透過エントリーの順に操作してください。

❶ 管理用端末からのWEBアクセスを透過

❷ 管理用端末以外からのWEBアクセスを遮断

パケットフィルター設定一覧

「パケットフィルター」画面で設定したフィルターの番号を表示

管理者用のパソコンに設定されたIPアドレス

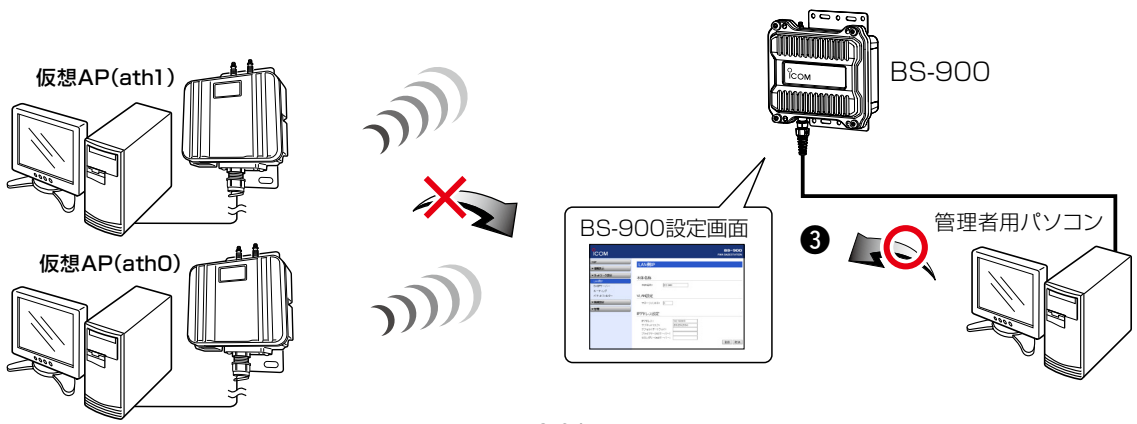
登録した上記のフィルターより大きな番号を表示

番号	[redacted]
エントリー	有効
ログを表示	[redacted]
方法	透過
送信元インターフェース	すべて
宛先インターフェース	mirror0
送信元MACアドレス／マスク	-
宛先MACアドレス／マスク	-
VLAN ID	0
Ethernetタイプ	IP
送信元IPアドレス	192.168.0.[redacted]
宛先IPアドレス	-
IPプロトコル	TCP
送信元ポート	-
宛先ポート	80
TCPフラグ	-

編集 削除

番号	[redacted]
エントリー	有効
ログを表示	[redacted]
方法	遮断
送信元インターフェース	すべて
宛先インターフェース	mirror0
送信元MACアドレス／マスク	-
宛先MACアドレス／マスク	-
VLAN ID	0
Ethernetタイプ	IP
送信元IPアドレス	-
宛先IPアドレス	-
IPプロトコル	TCP
送信元ポート	-
宛先ポート	80
TCPフラグ	-

編集 削除



4.「パケットフィルター」画面について（つづき）

ネットワーク設定 > パケットフィルター

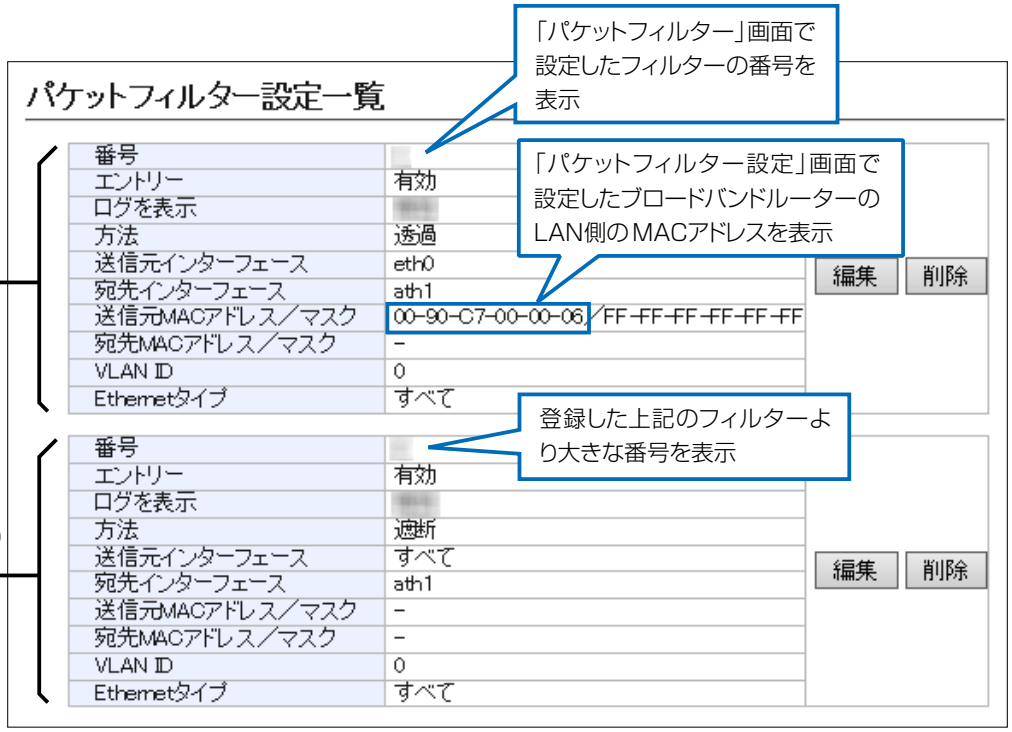
❹仮想APからインターネットへの接続を許可し、それ以外の有線LANとの通信を遮断するには

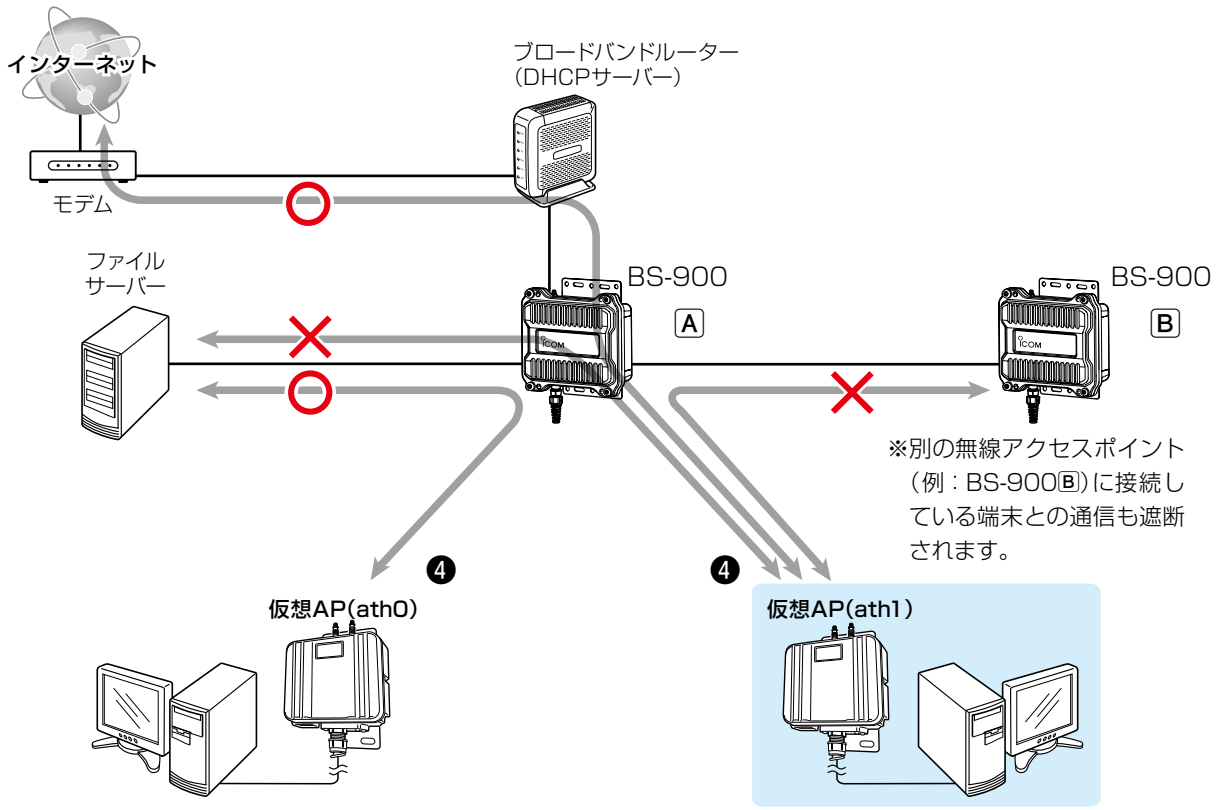
下記の2つ（❶と❷）のフィルターの登録が必要です。

※ブロードバンドルーター以外のDHCPサーバーを使用する場合は、対応する透過エントリーを追加してください。

❶ブロードバンドルーターから仮想AP（ath1）への通信を透過

❷ブロードバンドルーター以外から仮想AP（ath1）への通信を遮断





「無線設定」メニュー

第 4 章

この章では、
「無線設定」メニューで表示される設定画面について説明しています。

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

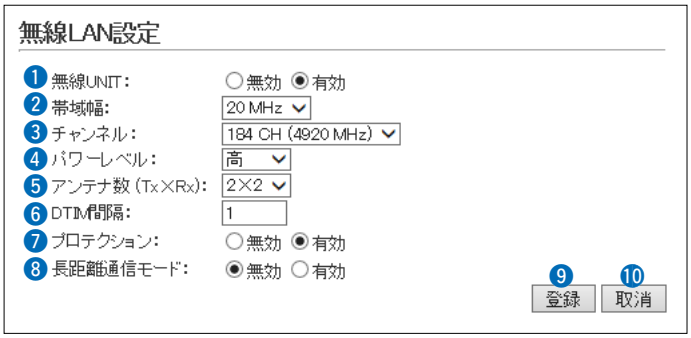
4 「無線設定」メニュー

1.「無線LAN」画面について

無線設定 > 無線LAN

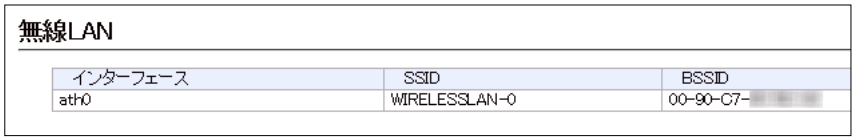
■ 無線LAN設定

本製品に内蔵された無線LANユニットに対する設定です。



❶無線UNIT ……

無線通信機能の使用を設定します。　（出荷時の設定：有効）
「無効」に設定すると、本製品の無線通信機能を停止します。
また、「有効」に設定されているときだけ、「情報表示」メニューにある「ネットワーク情報」画面の［無線LAN］項目（参照下図）に表示します。



❷帯域幅 ……

本製品で使用する周波数帯域幅を設定します。　（出荷時の設定：20MHz）
20MHz、または40MHz帯域幅を選択した場合だけ、「仮想AP」画面でストリーム数を設定できます。
※10MHz帯域幅選択時、「仮想AP」画面の［ストリーム数］欄（P.4-8）は表示されません。
※万一、本製品から、ほかの無線局に対して有害な電波干渉の事例が発生した場合には、帯域幅を変更してください。
※帯域幅について詳しくは、vページをご覧ください。

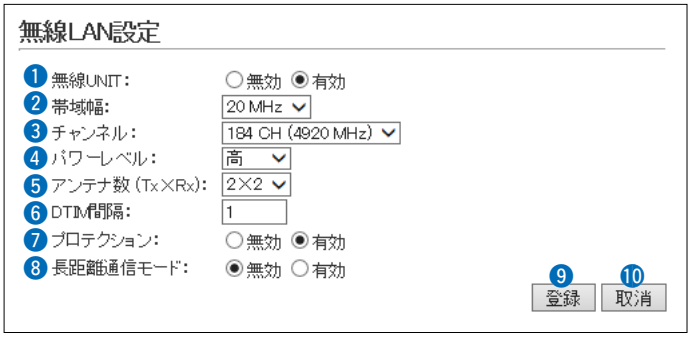
❸チャンネル ……

本製品の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：184CH（4920MHz））
※FWA無線LAN端末は、本製品のチャンネルを自動的に検知して通信します。
※設定する帯域幅（❷）により、使用できるチャンネルが異なりますので、vページをご覧ください。

1.「無線LAN」画面について

無線設定 > 無線LAN

■ 無線LAN設定(つづき)



❹パワーレベル ……

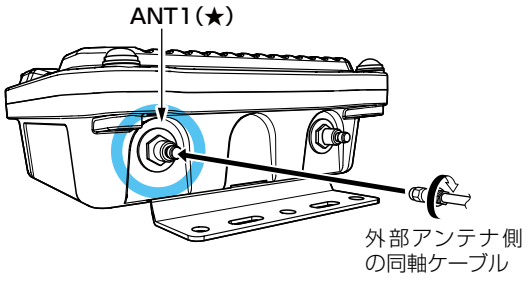
本製品に内蔵する無線LANカードの送信出力を、高/中/低/最低(4段階)の中から選択します。 (出荷時の設定：高)
本製品の最大伝送距離は、パワーレベルが「高」の場合です。
パワーレベルを低くすると、伝送距離も短くなります。

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広範囲に届く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FWA基地局が設置された環境で、近くの無線LAN機器との電波干渉をなくして、通信速度の低下などを軽減したいとき無線通信機能の使用を設定します。

❺アンテナ数(Tx×Rx) ……

無線通信時に使用するアンテナの本数を設定します。(出荷時の設定：2×2)
ANT1側(★)だけに外部アンテナを接続する場合は、「1×1」に設定してください。



※[アンテナ数(Tx×Rx)]は、間違った設定をすると十分な性能が得られません。
取り扱いについては、十分にご注意ください。

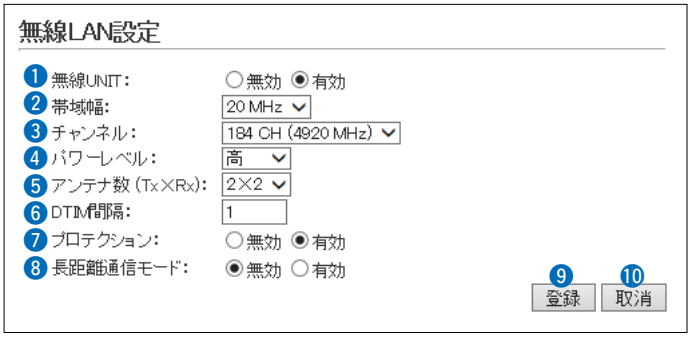
株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

4　「無線設定」メニュー

1.「無線LAN」画面について

無線設定 ＞ 無線LAN

■ 無線LAN設定（つづき）



❻DTIM間隔 ……

DTIM（Delivery Traffic Indication Message）をビーコンに挿入する間隔を設定します。（出荷時の設定：1）
設定できる範囲は、「1～50」です。
DTIMとは、パワーセーブしている端末に対して、ブロードキャスト・マルチキャストパケット配送を伝えるメッセージのことです。
※設定を変更すると、正常に通信できないことがありますので、特に必要がない場合は、工場出荷時の状態でご使用ください。

❼プロテクション ……

異なる無線LAN規格の混在による電波干渉をなくして、無線LANの通信速度低下を軽減したいとき有効な設定です。（出荷時の設定：有効）
※「有効」に設定すると、通信速度の低下を防止するのに効果があります。

❽長距離通信モード ……

相手との通信距離が600m以上の直線距離がある場合は、「有効」に設定します。（出荷時の設定：無効）
※「有効」に設定するときは、FWA無線LAN端末も「有効」にしてください
※通信相手との距離が600m未満で長距離通信モードを使用すると、通信速度低下の原因になりますので、出荷時の設定でご使用ください。
※長距離通信をする場合、直線の見通し距離だけでなく、電波の反射や干渉の影響、およびフレネルゾーンなどを考慮して、アンテナを設置する必要があります。
長距離通信モードを設定しても改善されない場合は、これらも原因と考えられます。
※「フレネルゾーンについて」や「地球の影響について」は、別紙の「設定ガイド」をご覧ください。

❾〈登録〉 ……

「無線LAN」画面で設定した内容を登録するボタンです。

❿〈取消〉 ……

「無線LAN」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。

株式会社エクセリ　東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5　URL : https : //www.exseli.com/

2.「仮想AP」画面について

無線設定 > 仮想AP

■ 仮想AP設定

本製品1台で複数の仮想無線アクセスポイントとして使用するための設定です。
[アカウンティング](❽)欄で「有効」、[MAC認証](❾)欄で「有効」を選択したときに、下記の画面になります。

❶インターフェース ……

設定する仮想APを選択します。 (出荷時の設定：ath0)
仮想APごとに、[仮想AP設定]項目(❷～❿)と[暗号化設定]項目の設定内容を変更できます。
※「ath1～ath7」を使用するときは、[仮想AP](❷)欄を「有効」にしてください。
※仮想APごとの設定状況は、「情報表示」メニューの「無線設定情報一覧 無線」にある「仮想AP一覧」(ath0～ath7)に表示します。(P.2-5)
※ご使用のWWWブラウザーでJavaScript®が「無効」に設定されていると、仮想APを選択したとき、[仮想AP設定]項目と[暗号化設定]項目の設定内容が更新されません。
更新されないときは、ご使用のWWWブラウザーでJavaScript®の設定が「有効」に設定されていることを確認してください。

❷仮想AP ……

[インターフェース](❶)欄で選択した仮想APの使用について設定します。
(出荷時の設定：有効(ath0)、無効(ath1～ath7))
※「ath0」は「無効」にできません。
※通信速度低下を防止するため、使用する無線インターフェースだけを「有効」に設定してください。

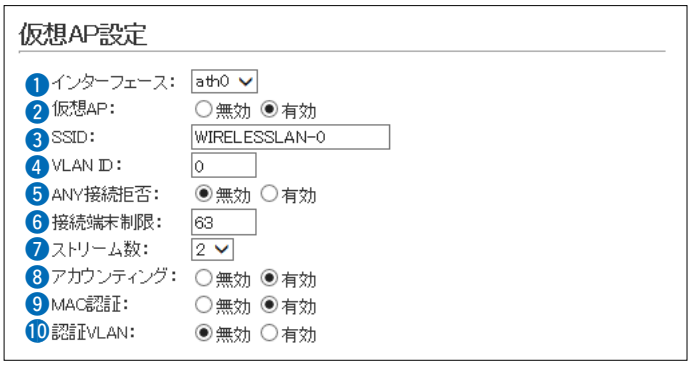
株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

2.「仮想AP」画面について

無線設定 > 仮想AP

■ 仮想AP設定(つづき)

[アカウンティング](❽)欄で「有効」、[MAC認証](❾)欄で「有効」を選択したときに、下記の画面になります。



❸SSID ……

[インターフェース](❶)欄で選択した仮想APの使用について設定します。
大文字/小文字の区別に注意して、任意の半角英数字32文字以内で入力します。 (出荷時の設定：WIRELESSLAN-0(ath0)
WIRELESSLAN-1(ath1)
WIRELESSLAN-2(ath2)
WIRELESSLAN-3(ath3)
WIRELESSLAN-4(ath4)
WIRELESSLAN-5(ath5)
WIRELESSLAN-6(ath6)
WIRELESSLAN-7(ath7))

※[SSID]は、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。
[SSID]の異なるFWA無線LAN端末とは接続できません。
※FWA基地局が無線伝送エリア内に複数存在しているような場合、個々のネットワークグループを[SSID(無線ネットワーク名)]で識別できます。
※複数の仮想APを使用する場合、同じSSIDを設定できません。
※[SSID]と[ESSID]は、同じ意味で使用しています。
本製品以外の機器では、[ESSID]と表記されている場合があります。

❹VLAN ID ……

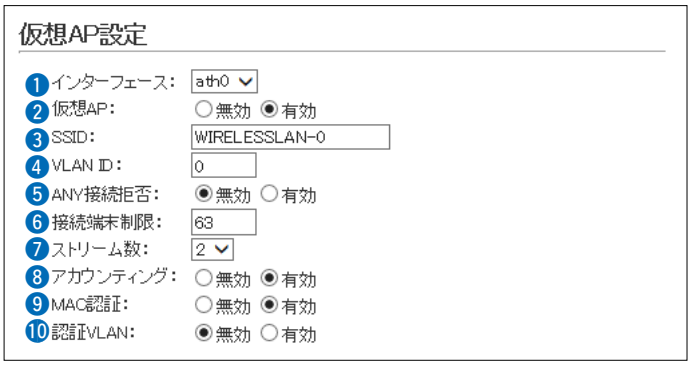
[インターフェース](❶)欄で選択した仮想APが所属する無線グループのID番号を設定します。 (出荷時の設定：0)
設定できる範囲は、「0～4094」です。
※[VLAN ID]を付けないときは、「0」に設定します。
※異なるID番号のネットワークとは通信できません。

2.「仮想AP」画面について

無線設定 > 仮想AP

■ 仮想AP設定(つづき)

[アカウンティング](❽)欄で「有効」、[MAC認証](❾)欄で「有効」を選択したときに、下記の画面になります。



❺ANY接続拒否 ……

[インターフェース](❶)欄で選択した仮想APと「ANY」モード(アクセスポイント自動検索接続機能)で通信するFWA無線LAN端末からの検索や接続の拒否についての設定します。 (出荷時の設定:無効)

※一部のFWA無線LAN端末と接続できないことや動作が不安定になることがありますので、特に必要がない場合は、出荷時の設定で使用されることをおすすめします。

❻接続端末制限 ……

[インターフェース](❶)欄で選択した仮想APに同時接続可能なFWA無線LAN端末の台数を設定します。 (出荷時の設定:63)

設定できる範囲は、「1～128」です。

接続できる台数を制限すると、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。

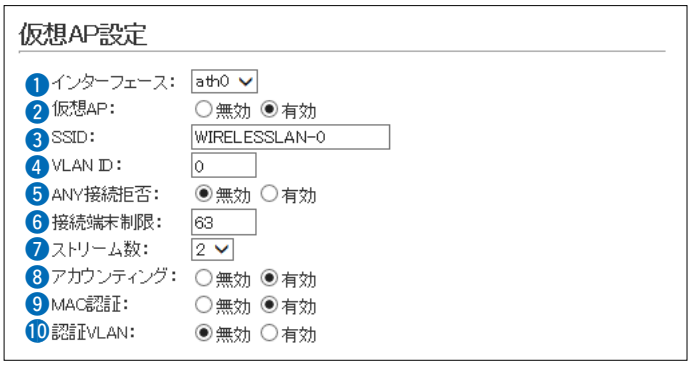
※仮想APごとに最大128台まで設定できますが、実際に通信できるのは、全仮想APの合計(無線ユニット全体)で最大128台(ブリッジ通信を含む)までになります。

2.「仮想AP」画面について

無線設定 > 仮想AP

■ 仮想AP設定(つづき)

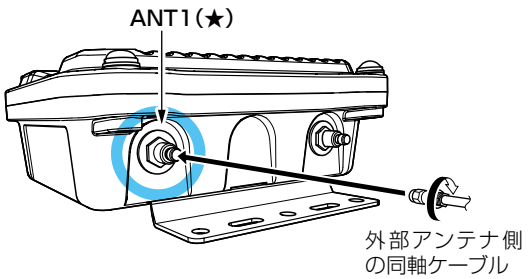
[アカウンティング](❽)欄で「有効」、[MAC認証](❾)欄で「有効」を選択したときに、下記の画面になります。



❼ストリーム数 ……

[インターフェース](❶)欄で選択した仮想APで使用するストリーム数を設定します。 (出荷時の設定：2)

※ANT1側(★)だけに外部アンテナを接続し、20MHz、または40MHz帯域幅で通信する場合は、「1」に設定してください。



※本製品の最大通信速度について詳しくは、ivページをご覧ください。

※[ストリーム数]は、間違った設定をすると十分な性能が得られません。取り扱いについては、十分にご注意ください。

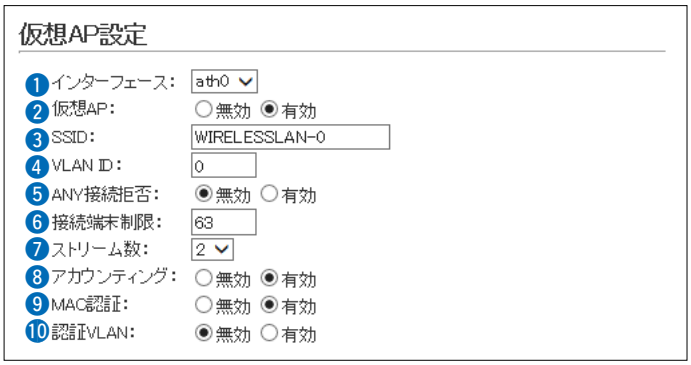
※通信が安定しない場合、ストリーム数「1」に切り替えたほうがよい場合があります。

2.「仮想AP」画面について

無線設定 > 仮想AP

■ 仮想AP設定(つづき)

[アカウンティング](❽)欄で「有効」、[MAC認証](❾)欄で「有効」を選択したときに、下記の画面になります。



❽アカウンティング ……

[インターフェース](❶)欄で選択した仮想APと通信するFWA無線LAN端末のネットワーク利用状況(接続、切断、MACアドレスなど)を収集してアカウンティングサーバーに送信するときに設定します。

(出荷時の設定:無効)

「有効」を選択したときは、アカウンティングサーバーの設定が必要です。

※仮想APごとに個別の設定を使用するか、またはすべての仮想APで共通設定を使用するかは、[アカウンティング設定]項目で選択できます。(P.4-20)

※共通設定を使用するときは、「認証サーバー」画面でアカウンティングサーバーを設定します。

❾MAC認証 ……

[インターフェース](❶)欄で選択した仮想APと通信するFWA無線LAN端末のMACアドレスをRADIUSサーバーで認証します。(出荷時の設定:無効)

「有効」を選択したときは、RADIUSサーバーの設定が必要です。

※仮想APごとに個別の設定をするか、またはすべての仮想APで共通設定を使用するかは、[MAC認証サーバー(RADIUS)設定]項目で選択できます。(P.4-11)

※共通設定を使用するときは、「認証サーバー」画面でRADIUSサーバーを設定します。

※MAC認証機能では、任意のネットワーク認証と暗号化方式を組み合わせて使用できます。

※FWA無線LAN端末のMACアドレスは、事前にRADIUSサーバーに登録する必要があります。

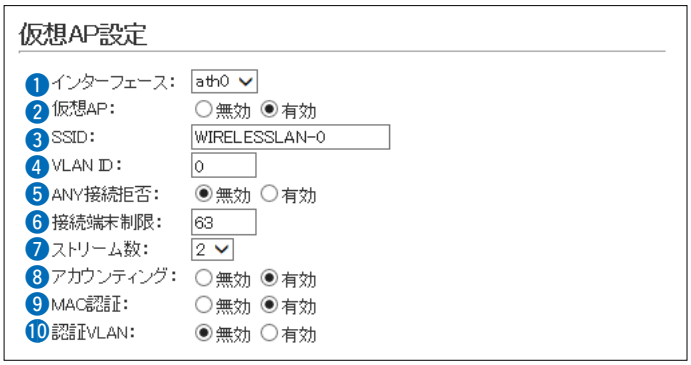
MACアドレスが「00-AB-12-CD-34-EF」の場合は、ユーザー名/パスワードは「00ab12cd34ef」(半角英数字(小文字))になります。

2.「仮想AP」画面について

無線設定 > 仮想AP

■ 仮想AP設定(つづき)

[アカウンティング](❽)欄で「有効」、[MAC認証](❾)欄で「有効」を選択したときに、下記の画面になります。



❾認証VLAN ……

[インターフェース](❶)欄で選択した仮想APと通信するFWA無線LAN端末の所属VLAN IDを、RADIUSサーバーを利用した認証結果(応答属性)に応じて、グループ分けできる機能です。 (出荷時の設定:無効)
「有効」を選択したときは、RADIUSサーバーの設定が必要です。
※「仮想AP」画面の[仮想AP設定]項目(P.4-9)でMAC認証を有効にする、または[暗号化設定]項目(P.4-12)でネットワーク認証(WPA、WPA2、WPA/WPA2、IEEE802.1X)を選択すると、認証VLANが設定できるようになります。

◎MAC認証が有効の場合

[MAC認証サーバー(RADIUS)設定]項目(P.4-11)で、仮想APごとに個別の設定するか、すべての仮想APで共通設定を使用するかを選択します。

◎ネットワーク認証でWPA、WPA2、WPA/WPA2、IEEE802.1Xを選択した場合

[RADIUS設定]項目(P.4-19)で、仮想APごとに個別の設定するか、すべての仮想APで共通設定を使用するかを選択します。

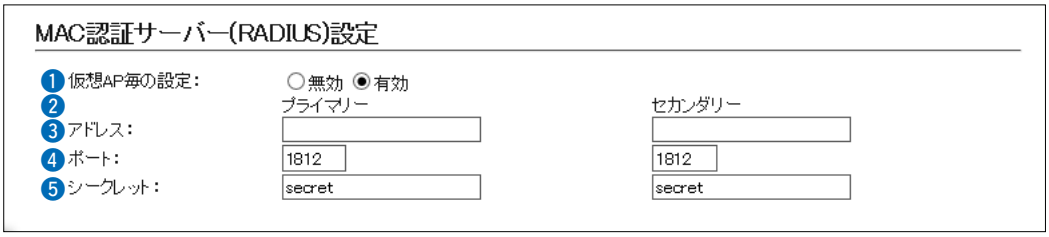
※共通設定を使用するときは、「認証サーバー」画面でRADIUSサーバーを設定します。(P.4-21)
※仮想APにネットワーク認証とMAC認証の両方を設定し、両方の応答属性からVLAN ID情報を取得した場合、ネットワーク認証のVLAN IDが優先されます。
応答属性が通知されない場合や値が正しくない場合、仮想APに設定したVLAN IDに所属します。

2.「仮想AP」画面について（つづき）

無線設定 ＞ 仮想AP

■ MAC認証サーバー（RADIUS）設定

FWA無線LAN端末のMACアドレスをRADIUSサーバーで認証するときに設定します。
[仮想AP設定]項目の[MAC認証]欄で「有効」、[仮想AP毎の設定]（❶）欄で「有効」を選択したときに、下記の画面になります。



❶仮想AP毎の設定 ……

仮想APごとに、異なる設定でRADIUSサーバーによる認証をするかしないかを設定します。（出荷時の設定：無効）
仮想APごとに個別設定するときは、[仮想AP設定]項目の[インターフェース]欄で仮想APを指定し、この欄で「有効」を設定します。
※「無効」の場合は、[認証サーバー]画面の設定内容でRADIUSサーバーによる認証をします。

❷プライマリー/セカンダリー …

[プライマリー]列に設定したRADIUSサーバーからの応答がない場合、その次のアクセスさせるRADIUSサーバーがあるときだけ、[セカンダリー]列にそのRADIUSサーバーアドレスを設定します。

❸アドレス ……

対象となるRADIUSサーバーのIPアドレスを入力します。

❹ポート ……

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

❺シークレット ……

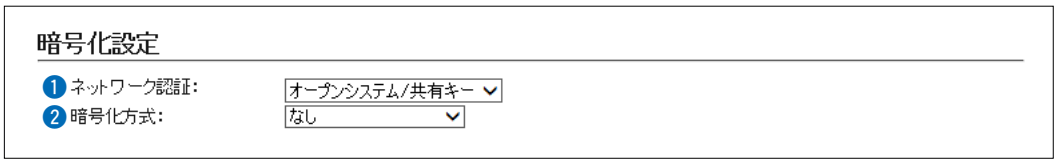
本製品とRADIUSサーバーの通信に使用するキーを設定します。
（出荷時の設定：secret）
RADIUSサーバーに設定された値と同じ設定にします。
半角64文字以内の英数字で入力します。

2.「仮想AP」画面について（つづき）

無線設定 ＞ 仮想AP

■ 暗号化設定

無線LANの通信データを保護するために暗号化を設定します。
※選択する設定内容（❶、❷）に応じて、下記以外の設定（❸～❼）を表示します。（P.4-15～P.4-18）



❶ネットワーク認証 ……

FWA無線LAN端末からのアクセスに対する認証方式を選択します。
（出荷時の設定：オープンシステム/共有キー）
※異なる認証方式の相手とは互換性がありませんので、通信をする相手間で同じ設定にしてください。
※「IEE802.1X」、「WPA」、「WPA2」、「WPA/WPA2」を選択したときは、RADIUSサーバーによる認証設定が必要です。

認証方式について

◎オープンシステム/共有キー
「WEP RC4」暗号化方式によるアクセスに対して、認証方式（オープンシステム/共有キー）を自動認識します。

◎オープンシステム
「WEP RC4」暗号化方式によるアクセスに対して、暗号鍵（キー）の認証をしません。

◎共有キー
「WEP RC4」暗号化方式によるアクセスに対して、本製品と同じ暗号鍵（キー）かどうかを認証します。

◎IEEE802.1X
「WEP RC4」暗号化方式を使用し、RADIUSサーバーによるIEEE802.1X認証するときの設定です。
※RADIUSサーバーによる認証設定が必要です。

◎WPA（Wi-Fi Protected Access）
「TKIP/AES」暗号化方式を使用し、RADIUSサーバー認証するときの設定です。
※［IEEE802.1X］認証より強力で、「TKIP」暗号化方式の使用を標準規格とする認証方式です。
※RADIUSサーバーによる認証設定が必要です。

◎WPA2
ネットワーク認証方式にWPA2を使用します。
※「WPA」認証より強力な「AES」暗号化方式の使用を標準規格とする認証方式で、「PMKIDキャッシュ」により、再接続による認証が不要です。
※「WPA2」認証に対応したクライアントが必要です。
※RADIUSサーバーによる認証設定が必要です。

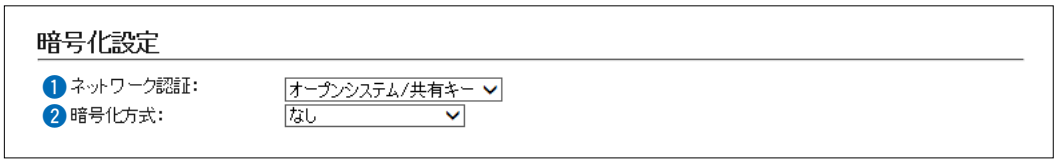
◎WPA/WPA2
「WPA」認証と「WPA2」認証を自動認識します。

2.「仮想AP」画面について

無線設定 > 仮想AP

■ 暗号化設定(つづき)

※選択する設定内容(❶、❷)に応じて、下記以外の設定(❸～❼)を表示します。(P.4-15～P.4-18)



❶ネットワーク認証(つづき) …

◎**WPA-PSK(Pre-Shared Key)**
共有鍵(キー)で認証します。
RADIUSサーバーを利用しない簡易的な「TKIP/AES」暗号化の認証方式で、通信相手と共通の鍵を持っているかどうかの認証をします。

◎**WPA-PSK/WPA2-PSK**
ネットワーク認証(WPA-PSK/WPA2-PSK)を自動認識します。

❷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]/[TKIP]/[AES]です。
異なる暗号化方式とは互換性がありませんので、暗号化方式とビット数は、通信をする相手間で同じ設定にしてください。
※暗号化方式を「なし」、または「AES」に設定している場合だけ、54Mbps(理論値)を超える速度で通信できます。

暗号化方式について

◎**なし**
データを暗号化しないで通信します。
※[ネットワーク認証](❶)欄で、「オープンシステム/共有キー」、または「オープンシステム」を選択したとき使用できます。
※暗号化を設定されることをおすすめします。

◎**WEP RC4**
暗号鍵(キー)が一致した場合に、通信できる暗号化方式です。
※暗号鍵(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。
※[ネットワーク認証](❶)欄で、「オープンシステム/共有キー」、または「オープンシステム」、「共有キー」、「IEEE802.1X」を選択したとき使用できます。

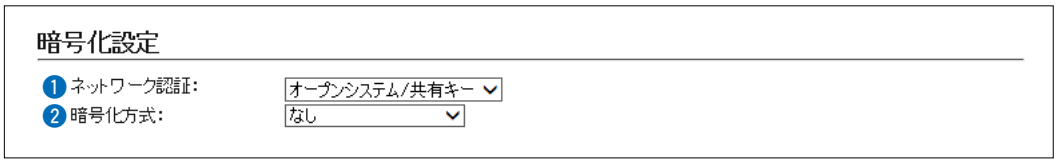
◎**TKIP(Temporal Key Integrity Protocol)**
暗号鍵(キー)を一定間隔で自動更新しますので、「WEP RC4」より強力です。
※[ネットワーク認証](❶)欄で、「WPA」や「WPA2」、または「WPA-PSK」、「WPA2-PSK」を選択したとき使用できます。

2.「仮想AP」画面について

無線設定 > 仮想AP

■ 暗号化設定（つづき）

※選択する設定内容（❶、❷）に応じて、下記以外の設定（❸～❼）を表示します。（P.4-15～P.4-18）



❷暗号化方式（つづき） ……

◎AES（Advanced Encryption Standard）

暗号化の強化、および暗号鍵（キー）を一定間隔で自動更新しますので、「TKIP」より強力な暗号化方式です。

※［ネットワーク認証］（❶）欄で、「WPA」や「WPA2」、または「WPA-PSK」、「WPA2-PSK」を選択したとき使用できます。

◎TKIP/AES

FWA基地局の暗号化方式（TKIP/AES）を自動認識します。

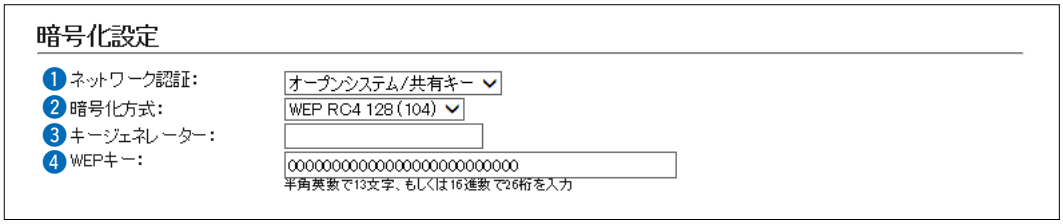
※「AES」が認識されたときだけ、54Mbps（理論値）を超える速度で通信できます。

2.「仮想AP」画面について

無線設定 > 仮想AP

■ 暗号化設定(つづき)

※選択する設定内容(❶、❷)に応じて、下記以外の設定(❺、❻、❼)を表示します。(P.4-17～P.4-18)



❸キージェネレーター ……

[暗号化方式](❷)欄(P.4-13)で「WEP RC4」の暗号化方式を選択したとき、暗号化および復号に使用する16進数の暗号鍵(キー)を生成するための文字列を設定します。 (出荷時の設定:空白(なし))

次の順番に操作すると、設定できます。

1.[ネットワーク認証](❶)欄で、「オープンシステム/共有キー」、または「オープンシステム」、「共有キー」を選択します。

2.[暗号化方式](❷)欄で、「WEP RC4 64(40)」、「WEP RC4 128(104)」、「WEP RC4 152(128)」を選択します。

- [キージェネレーター]欄と[WEPキー](❹)欄(P.4-16)が表示されます。

3.大文字/小文字の区別に注意して、文字列を[キージェネレーター]欄に31文字以内(任意の半角英数字/記号)で入力します。

- 入力した文字列より生成された16進数の暗号鍵(キー)が[WEPキー](❹)欄に表示されます。

※暗号鍵(キー)を直接入力する場合は、キージェネレーターに文字列が残っていると、[WEPキー](❹)欄に直接入力できませんので、削除してください。

※入力する文字列は、通信する相手(弊社製機器)側のキージェネレーターと同じ文字列を設定してください。
他社製の機器とは互換性がありませんので、ご注意ください。

※キージェネレーターから生成された暗号鍵(キー)が通信相手間で異なる場合、暗号化されたデータを復号できません。

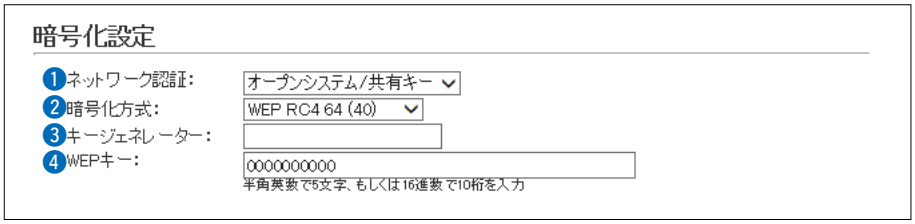
※[WEPキー](❹)欄に表示される暗号鍵(キー)の桁数、および文字数は、[暗号化方式](❷)欄の設定によって異なります。

2.「仮想AP」画面について

無線設定 > 仮想AP

■ 暗号化設定(つづき)

※選択する設定内容(❶、❷)に応じて、下記以外の設定(❺、❻、❼)を表示します。(P.4-17～P.4-18)



❹WEPキー ……

[キージェネレーター](❸)欄を使用しないで、暗号鍵(キー)を直接設定するとき入力します。

※16進数で設定するときは、「0～9」および「a～f(またはA～F)」の半角文字を入力してください。

※ASCII文字で設定するときは、大文字/小文字の区別に注意して、任意の半角英数字を入力してください。

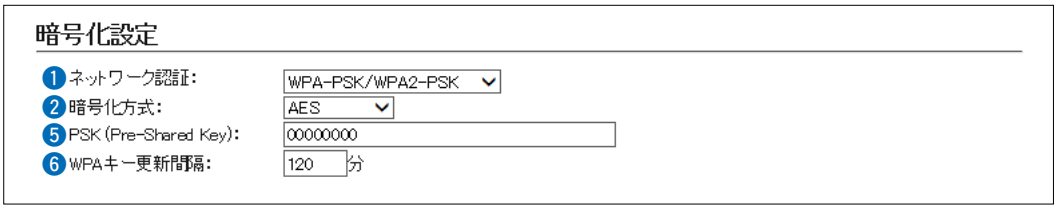
※入力する暗号鍵(キー)の桁数は、[暗号化方式](❷)欄を設定したとき表示される桁数(10桁の表示例:0000000000)と同じに設定してください。ASCII文字で入力する場合は、16進数の半分(例:5文字)で入力してください。

2.「仮想AP」画面について

無線設定 > 仮想AP

■ 暗号化設定(つづき)

※選択する設定内容(❶、❷)に応じて、下記以外の設定(❸、❹、❼)を表示します。(P.4-15～P.4-16、P.4-18)



❺PSK(Pre-Shared Key) …… 共通鍵(キー)を半角英数字で入力します。
※[ネットワーク認証](❶)欄で、「WPA-PSK」、「WPA2-PSK」、「WPA-PSK/WPA2-PSK」を選択したとき、設定できます。
※同じ暗号化方式を使用するFWA無線LAN端末と、同じ共有鍵(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、大文字/小文字の区別に注意して、8～63文字を入力してください。

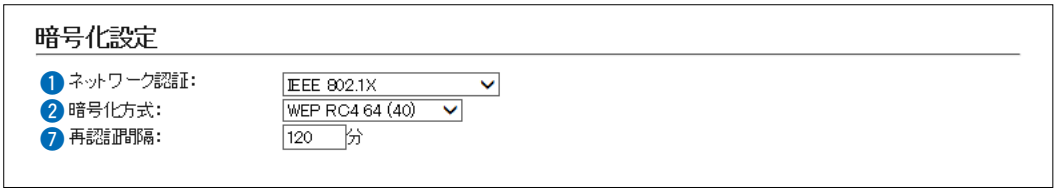
❻WPAキー更新間隔 …… [ネットワーク認証](❶)欄で、「WPA」、「WPA2」、「WPA/WPA2」、「WPA-PSK」、「WPA2-PSK」、「WPA-PSK/WPA2-PSK」を選択したとき、暗号鍵(キー)の更新間隔を分で設定します。 (出荷時の設定：120)
設定できる範囲は、「0～1440」(分)です。
※「0」を設定すると、更新しません。

2.「仮想AP」画面について

無線設定 > 仮想AP

■ 暗号化設定(つづき)

※選択する設定内容(❶、❷)に応じて、下記以外の設定(❸、❹、❺、❻)を表示します。(P.4-15～P.4-17)



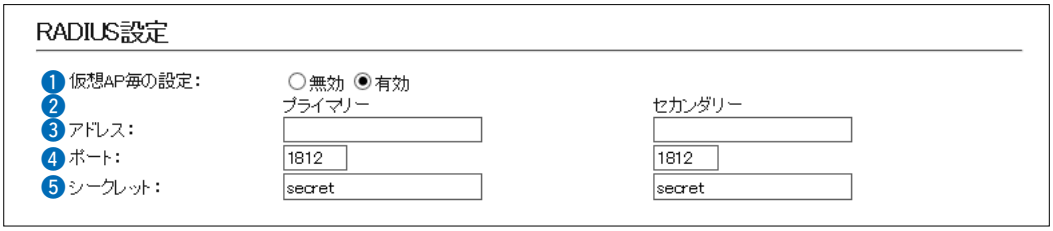
❼再認証間隔 …… [ネットワーク認証](❶)欄で、「IEEE802.1X」を選択したとき、RADIUSサーバーに再度認証を要求する間隔を分で設定します。
設定できる範囲は、「0～9999」(分)です。 (出荷時の設定：120)
※「0」を設定したときは、再認証しません。

2.「仮想AP」画面について（つづき）

無線設定 ＞ 仮想AP

■ RADIUS設定

RADIUSサーバーを使用して、WPA認証、WPA2認証、IEEE802.1X認証するときの設定です。
[暗号化設定]項目の[ネットワーク認証]欄で「IEEE802.1X」、「WPA」、「WPA2」、「WPA/WPA2」、[仮想AP毎の設定]（❶）欄で「有効」を選択したときに、下記の画面になります。
※EAP認証の対応については、ご使用になるRADIUSサーバーやFWA無線LAN端末の説明書をご覧ください。



❶仮想AP毎の設定 ……

仮想APごとに、異なる設定でRADIUSサーバーによる認証をするかしないかを設定します。（出荷時の設定：無効）
仮想APごとに個別設定するときは、[仮想AP設定]項目の[インターフェース]欄で仮想APを指定し、この欄で「有効」を設定します。
※「無効」の場合は、「認証サーバー」画面の設定内容でRADIUSサーバーによる認証をします。

❷プライマリー/セカンダリー …

[プライマリー]列に設定したRADIUSサーバーから応答がない場合、その次にアクセスさせるRADIUSサーバーがあるときだけ、[セカンダリー]列にそのRADIUSサーバーアドレスを設定します。

❸アドレス ……

対象となるRADIUSサーバーのIPアドレスを入力します。

❹ポート ……

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

❺シークレット ……

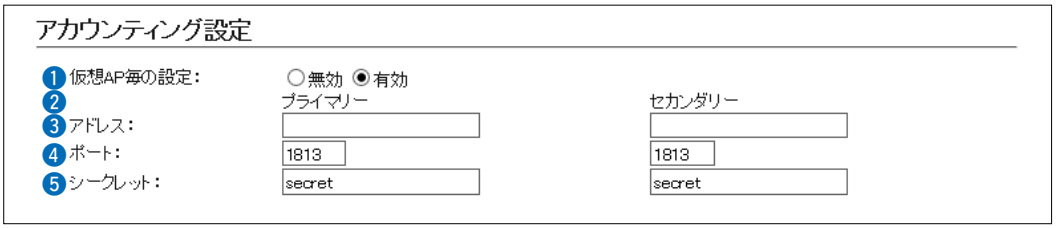
本製品とRADIUSサーバーの通信に使用するキーを設定します。
（出荷時の設定：secret）
RADIUSサーバーに設定された値と同じ設定にします。
半角64文字以内の英数字で入力します。

2.「仮想AP」画面について（つづき）

無線設定 ＞ 仮想AP

■ アカウンティング設定

セッション中に使用されたリソースの量（接続、切断、MACアドレスなど）をアカウンティングサーバーに送信する設定です。
［仮想AP設定］項目の［アカウンティング］欄で「有効」、［仮想AP毎の設定］（❶）欄で「有効」を選択したときに、下記の画面になります。



❶仮想AP毎の設定 ……

仮想APごとに、異なるアカウンティング設定をするかしないかを設定します。
（出荷時の設定：無効）
仮想APごとに個別設定するときは、［仮想AP設定］項目の［インターフェース］欄で仮想APを指定し、この欄で「有効」を設定します。
※「無効」の場合は、「認証サーバー」画面の設定内容でアカウンティングサーバーへ情報を送信します。

❷プライマリー/セカンダリー …

［プライマリー］列に設定したアカウンティングサーバーから応答がない場合、その次にアクセスさせるアカウンティングサーバーがあるときだけ、［セカンダリー］列にそのアカウンティングサーバーアドレスを設定します。

❸アドレス ……

対象となるアカウンティングサーバーのIPアドレスを入力します。

❹ポート ……

対象となるアカウンティングサーバーのポートを設定します。
（出荷時の設定：1813）
設定できる範囲は、「1～65535」です。
※ご使用のシステムによっては、出荷時の設定と異なることがありますのでご確認ください。

❺シークレット ……

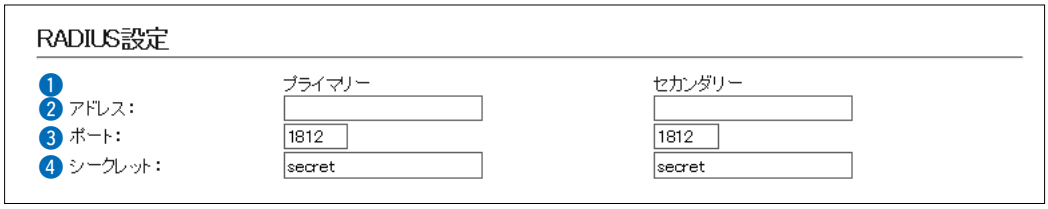
この欄に設定されたキーを使用して、本製品とサーバー間の通信をします。
（出荷時の設定：secret）
アカウンティングサーバーに設定された値と同じ設定にします。
半角64文字以内の英数字で入力します。

3.「認証サーバー」画面について

無線設定 > 認証サーバー

■ RADIUS設定

RADIUSサーバーを使用して、MAC認証、WPA認証、WPA2認証、IEEE802.1X認証するときの設定です。
※「仮想AP」画面の[MAC認証サーバー(RADIUS)設定]項目、[RADIUS設定]項目の[仮想AP毎の設定]欄を「無効」に設定したすべての仮想APで共用する設定です。
※「仮想AP」画面の[仮想AP設定]項目でMAC認証、または[暗号化設定]項目でネットワーク認証の設定が必要です。
※EAP認証の対応については、ご使用になるRADIUSサーバーやFWA無線LAN端末の説明書をご覧ください。



❶プライマリー/セカンダリー … [プライマリー]列に設定したRADIUSサーバーから応答がない場合、その次にアクセスさせるRADIUSサーバーがあるときだけ、[セカンダリー]列にそのRADIUSサーバーアドレスを設定します。

❷アドレス …… 対象となるRADIUSサーバーのIPアドレスを入力します。

❸ポート …… 対象となるRADIUSサーバーのポートを設定します。
(出荷時の設定：1812)
設定できる範囲は、「1～65535」です。
※ご使用のシステムによっては、出荷時の設定と異なることがありますのでご確認ください。

❹シークレット …… 本製品とRADIUSサーバーの通信に使用するキーを設定します。
(出荷時の設定：secret)
RADIUSサーバーに設定された値と同じ設定にします。
半角64文字以内の英数字で入力します。

3.「認証サーバー」画面について(つづき)

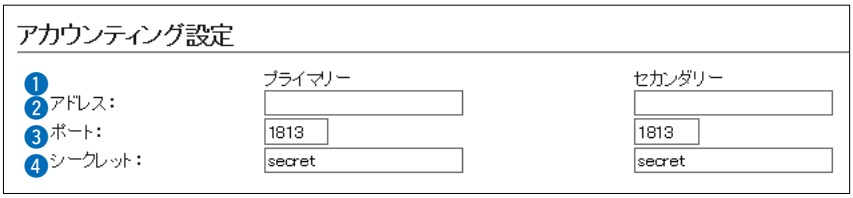
無線設定 > 認証サーバー

■ アカウンティング設定

セッション中に使用されたリソースの量(接続、切断、MACアドレスなど)をアカウンティングサーバーに送信する設定です。

※「仮想AP」画面の[アカウンティング設定]項目の[仮想AP毎の設定]欄を「無効」に設定したすべての仮想APで共用する設定です。

※「仮想AP」画面の[仮想AP設定]項目でアカウンティングの設定が必要です。



❶プライマリー/セカンダリー … [プライマリー]列に設定したアカウンティングサーバーから応答がない場合、その次にアクセスさせるアカウンティングサーバーがあるときだけ、[セカンダリー]列にそのアカウンティングサーバーアドレスを設定します。

❷アドレス …… 対象となるアカウンティングサーバーのIPアドレスを入力します。

❸ポート …… 対象となるアカウンティングサーバーのポートを設定します。
(出荷時の設定:1813)
設定できる範囲は、「1~65535」です。
※ご使用のシステムによっては、出荷時の設定と異なることがありますのでご確認ください。

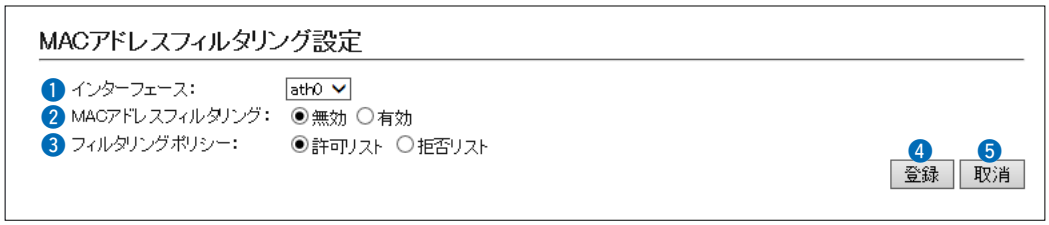
❹シークレット …… この欄に設定されたキーを使用して、本製品とサーバー間の通信をします。
(出荷時の設定:secret)
アカウンティングサーバーに設定された値と同じ設定にします。
半角64文字以内の英数字で入力します。

4.「MACアドレスフィルタリング」画面について

無線設定 > MACアドレスフィルタリング

■ MACアドレスフィリタリング設定

仮想APに接続できるFWA無線LAN端末を制限する設定です。
※仮想APごとに、最大1024台分のMACアドレスを登録できます。



❶インターフェース ……

設定する仮想APを選択します。 （出荷時の設定：ath0）
仮想APごとに、本製品への接続を許可する、または拒否するFWA無線LAN端末を登録できます。
※ご使用のWWWブラウザーでJavaScript®が「無効」に設定されていると、仮想APを選択したとき[MACアドレスフィルタリング設定]項目と[MACアドレスフィルタリング設定一覧]項目に登録された内容が更新されません。
更新されないときは、ご使用のWWWブラウザーでJavaScript®の設定が「有効」に設定されていることを確認してください。

❷MACアドレスフィルタリング

[インターフェース]（❶）欄で選択した仮想APについて、MACアドレスファイルタリング機能の使用を設定します。 （出荷時の設定：無効）
※「有効」に設定すると、[フィルタリングポリシー]（❸）欄の設定、および[MACアドレスフィルタリング設定一覧]項目に登録された内容が有効になります。
※使用するときは、「仮想AP」画面で該当する仮想APを選択し、[仮想AP]欄を「有効」に設定しておきます。

❸ファイルタリングポリシー …

[MACアドレスフィルタリング設定一覧]項目に登録されたFWA無線LAN端末との無線通信を許可するか拒否するかを設定します。
（出荷時の設定：許可リスト）

許可リスト ：MACアドレスが登録されたFWA無線LAN端末だけが、本製品と無線通信できます。
※通信を拒否する対象は、MACアドレスを登録していないすべてのFWA無線LAN端末です。

拒否リスト ：MACアドレスが登録されたFWA無線LAN端末だけが、本製品と無線通信できません。
※通信を許可する対象は、MACアドレスを登録していないすべてのFWA無線LAN端末です。

❹〈登録〉 ……

「MACアドレスフィルタリング設定」項目で設定した内容を登録するボタンです。

❺〈取消〉 ……

「MACアドレスフィルタリング設定」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。

4.「MACアドレスフィルタリング」画面について（つづき）

無線設定 > MACアドレスフィルタリング

■ 端末MACアドレスリスト

各仮想APについて、MACアドレスフィルタリングの対象となるFWA無線LAN端末のMACアドレスを登録します。

MACアドレス ……

MACアドレスフィルタリングの対象となるFWA無線LAN端末のMACアドレスを入力します。
入力後は、〈追加〉をクリックすると、[MACアドレスフィルタリング設定一覧]項目に表示します。
※対象となるFWA無線LAN端末のMACアドレスが[MACアドレスフィルタリング設定一覧]項目から登録できないときに使用します。
※1つの仮想APにつき、最大1024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。
※2つの入力例は、同じMACアドレスになります。
（入力例：00-90-c7-00-00-10、0090c7000010）
※[MACアドレスフィルタリング設定]項目の[インターフェース]欄で選択した仮想APについて、MACアドレスフィルタリングが有効なとき、[MACアドレスフィルタリング設定一覧]項目に登録されたFWA無線LAN端末との通信を[フィルタリングポリシー]欄の設定にしたがって制御します。

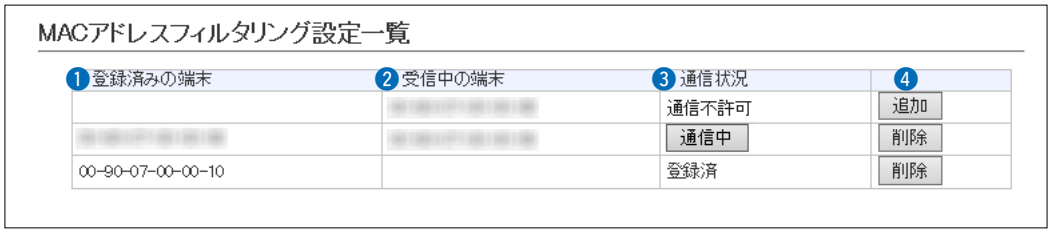
4.「MACアドレスフィルタリング」画面について（つづき）

無線設定 ＞ MACアドレスフィルタリング

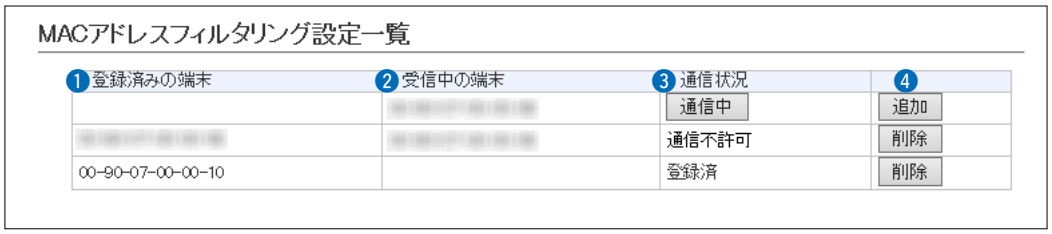
■ MACアドレスフィルタリング設定一覧

各仮想APについて、MACアドレスフィルタリングの対象となるFWA無線LAN端末の登録と通信状態を表示する画面です。

［フィルタリングポリシー］を「許可リスト」で使用した場合



［フィルタリングポリシー］を「拒否リスト」で使用した場合



❶登録済み端末 …… 登録されているFWA無線LAN端末のMACアドレスを表示します。

❷受信中の端末 …… 本製品の無線伝送領域内で通信しているFWA無線LAN端末のMACアドレスを表示します。

❸通信状況 …… 本製品との無線通信状況を表示します。

通信中 ：本製品と無線通信中のとき、〈通信中〉とボタンで表示します。
※〈通信中〉をクリックすると、無線通信状態（別画面）を表示します。

通信不許可 ：本製品により無線通信が拒否されているときの表示です。

登録済 ：MACアドレスが登録済みで、無線通信をしていないときの表示です。

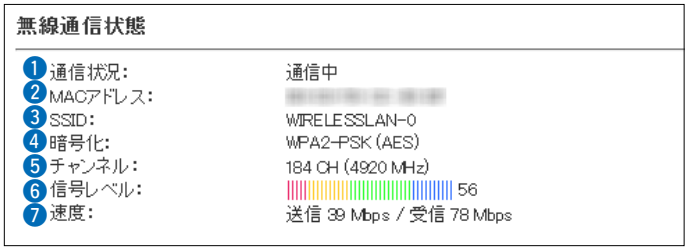
❹〈追加〉／〈削除〉 …… 表示されているFWA無線LAN端末のMACアドレスをリストに追加、またはリストから削除するボタンです。

4.「MACアドレスフィルタリング」画面について（つづき）

無線設定 ＞ MACアドレスフィルタリング

■ 無線通信状態

FWA無線LAN端末との通信状況をモニターします。
※[MACアドレスフィルタリング設定一覧]項目に〈通信中〉が表示されている場合に確認できる画面です。



❶通信状況 ……

「未接続」、「通信中」、「認証中」、「認証失敗」など、接続状況を表示します。
※「通信不可」を表示する場合は、お買い上げの販売店、または弊社サポートセンターにお問い合わせください。
※FWA無線LAN端末と無線ブリッジ接続しているときは、「通信中(ブリッジ)」が表示されます。

❷MACアドレス ……

FWA無線LAN端末のMACアドレスを表示します。

❸SSID ……

FWA無線LAN端末の[SSID]を表示します。

❹暗号化 ……

FWA無線LAN端末との通信に使用している認証モード、暗号化方式を表示します。

❺チャンネル ……

FWA無線LAN端末との通信に使用しているチャンネルを表示します。

❻信号レベル ……

FWA無線LAN端末から受信した電波信号の強さを、メーターと数値で表示します。

表　示	[赤]	[黄]	[緑]	[青]
レベル	0～4	5～14	15～29	30以上

安定した通信の目安は、「緑(15)」以上のレベルです。(単位はありません)
ただし、信号レベルが高くても、同じ周波数帯域を使用するFWA機器が近くで稼働している場合やFWA機器の稼働状況などにより、通信が安定しないことがあります。
したがって、あくまでも通信の目安としてご利用ください。

❼速度 ……

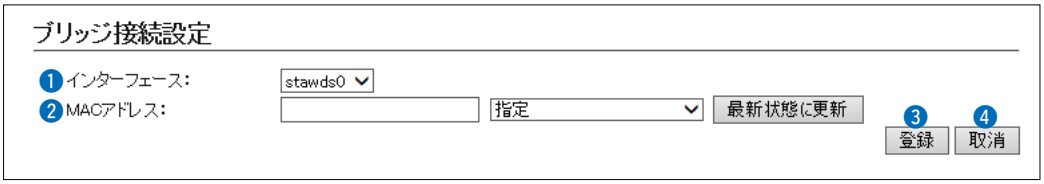
本製品の通信速度を理論値(Mbps)で表示します。

5.「ブリッジ接続」画面について

無線設定 > ブリッジ接続

■ ブリッジ接続設定

ブリッジ接続するFWA無線LAN端末を登録します。



❶インターフェース …… 登録、または編集するブリッジ接続のインターフェースを選択します。
（出荷時の設定：stawds0）
※最大8台分の相手を登録できます。
※登録した内容は、［ブリッジ接続設定一覧］項目に表示されます。
※インターフェースの名称（stawds0～stawds7）は、変更できません。

❷MACアドレス …… ブリッジ接続するFWA無線LAN端末のMACアドレスを、12桁（16進数）の半角英数字で入力、または自動検出されたMACアドレスの中から選択します。
※「指定」を選択しているときは、MACアドレスをテキストボックスに直接入力できます。
次の2つの入力例は、同じ結果になります。
「00-90-C7-77-00-77」、「0090C7770077」
※自動検出できるのは、下記条件をすべて満たすものだけです。
◎本製品の仮想AP「ath0」に接続している
◎ブリッジ接続機能が「有効」になっている
※SE-570FWやSE-570FWDの場合は、接続端末MACアドレスを自動に設定するとブリッジ接続機能が有効になります。
◎MACアドレスが登録されていない
※自動検出されたMACアドレスは、選択候補として表示されます。
「指定」以外の選択ができないときは、検出できるFWA無線LAN端末が存在しないときです。
※〈最新状態の更新〉をクリックすると、最新の検出結果から選択できます。

❸〈登録〉 …… 「ブリッジ接続設定」項目で設定した内容を登録するボタンです。

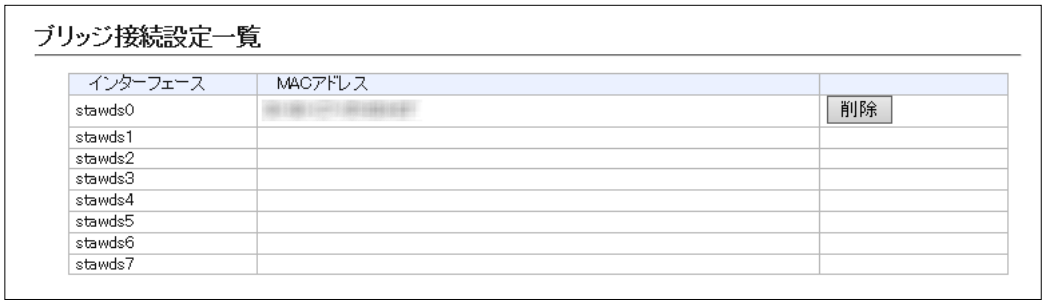
❹〈取消〉 …… 「ブリッジ接続設定」項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお、〈登録〉をクリックすると、変更前の状態には戻りません。

5.「ブリッジ接続」画面について(つづき)

無線設定 > ブリッジ接続

■ ブリッジ接続設定一覧

[ブリッジ接続設定]項目で設定した内容を表示します。



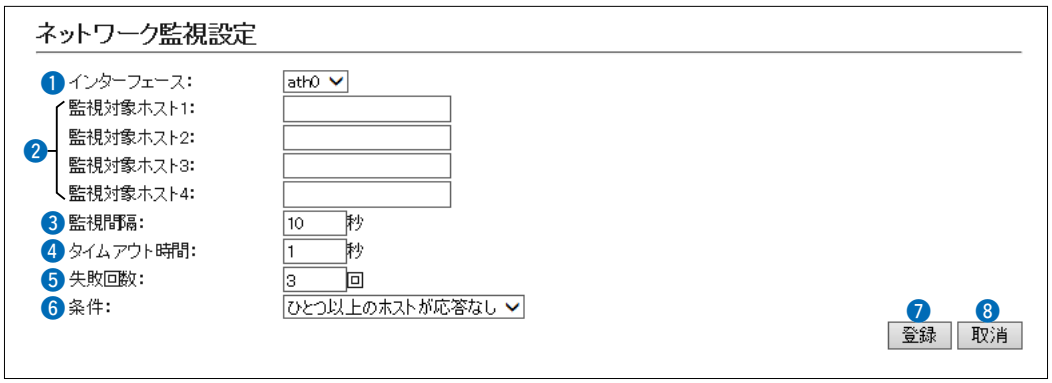
〈削除〉…… 登録した内容を取り消すときは、該当する欄の〈削除〉をクリックします。

6.「ネットワーク監視」画面について

無線設定 ＞ ネットワーク監視

■ ネットワーク監視設定

本製品と指定ホストとの通信障害を検出したとき、自動的に仮想APを停止させるための設定です。
※存在しないホスト、またはセキュリティー設定などにより、PINGに応答しないホストを設定すると、誤検出の原因になりますので、事前に正常時、障害時を含めた動作確認をしてください。



❶インターフェース …… 設定する仮想APを選択します。（出荷時の設定：ath0）

❷監視対象ホスト1～4 …… 監視対象となるホストのIPアドレスを入力します。
※設定した監視対象ホストに対して、[監視間隔]（❸）欄に設定された間隔でPingを送出します。
※すべてが空欄（出荷時の設定）の場合は、死活監視をしません。

❸監視間隔 …… 指定ホストにPingを送出する間隔を設定します。（出荷時の設定：10）
設定できる範囲は、「1～120」（秒）です。

❹タイムアウト時間 …… Pingに対する指定ホストからの応答を待つ時間を設定します。（出荷時の設定：1）
設定できる範囲は、「1～10」（秒）です
※設定時間を超えると、応答失敗と判断されます。

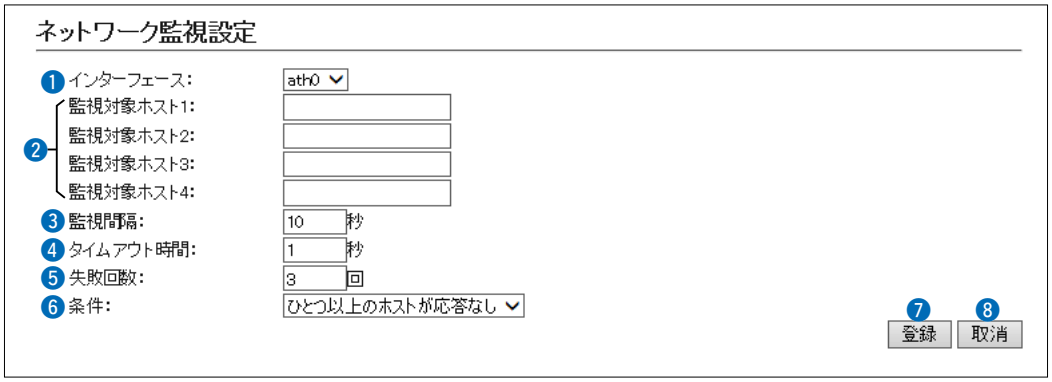
❺失敗回数 …… 本製品の仮想APを停止するまでのPingの応答失敗回数を設定します。（出荷時の設定：3）
設定できる範囲は、「1～10」（回）です

❻条件 …… 本製品の仮想APを停止させる条件を設定します。（出荷時の設定：ひとつ以上のホストが応答なし）
◎**ひとつ以上のホストが応答なし：**
設定したホストのうち、1つでもホストから応答がない場合、仮想APを停止します。
◎**すべてのホストが応答なし：**
設定したすべてのホストから応答がない場合、仮想APを停止します。

6.「ネットワーク監視」画面について

無線設定 > ネットワーク監視

■ ネットワーク監視設定（つづき）



7〈登録〉 …… 「ネットワーク監視設定」項目で設定した内容を登録するボタンです。

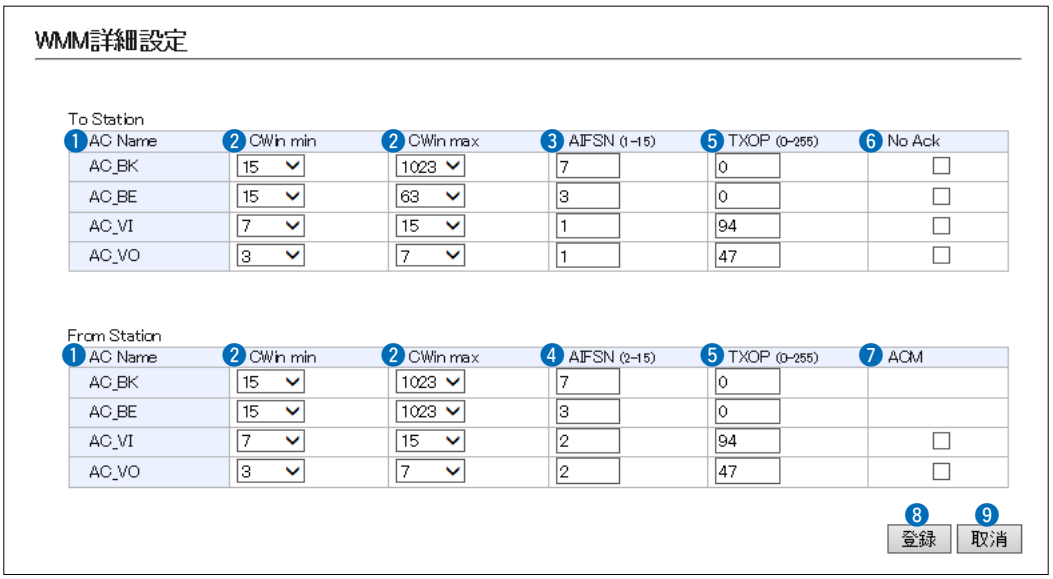
8〈取消〉 …… 「ネットワーク監視設定」項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお、〈登録〉をクリックすると、変更前の状態には戻りません。

7.「WMM詳細」画面について

無線設定 > WMM詳細

■ WMM詳細設定

本製品のWMM機能を使用した無線LAN通信において、[To Station]は、本製品から各FWA無線LAN端末へのデータに対する優先度を設定するEDCA(Enhanced Distributed Channel Access)パラメーターの設定です。
[From Station]は、各FWA無線LAN端末から本製品へのデータに対する優先度を設定するEDCA(Enhanced Distributed Channel Access)パラメーターの設定です。



❶AC Name ……

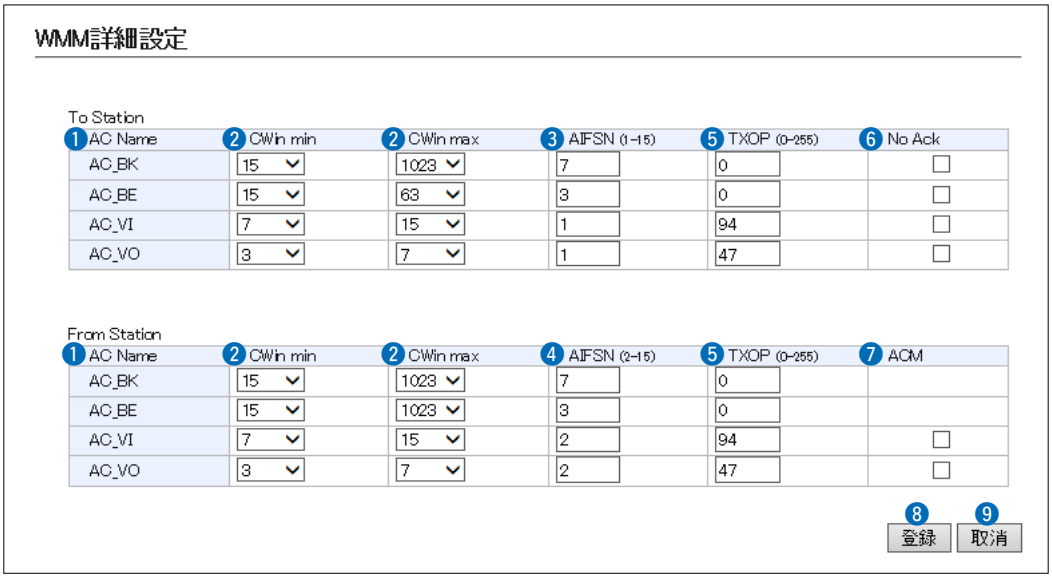
WMM(Wi-Fi Multimedia)で規定されるAC(Access Category)の名称で、アクセスカテゴリー(AC_BK、AC_BE、AC_VI、AC_VO)ごとに、EDCAパラメーター(❷～❺)を設定できます。
EDCAパラメーター(❷～❺)の各値は、Wi-Fiアライアンスで定められたアクセスカテゴリーの優先順位[AC_BK(低い)、AC_BE(通常)、AC_VI(優先)、AC_VO(最優先)]となるよう設定されています。

ご注意
EDCAパラメーター(❷～❺)の各値は、一般的な使用で変更する必要はありません。
なお、変更が必要な場合でも、原則としてWi-Fiアライアンスで定められたアクセスカテゴリーの優先順位を保つように設定してください。
優先順位を変更した場合、ACM(❼)などの制御が正しく動作しない場合があります。

7.「WMM詳細」画面について

無線設定 > WMM詳細

■ WMM詳細設定(つづき)



❷CWin min/CWin max ……

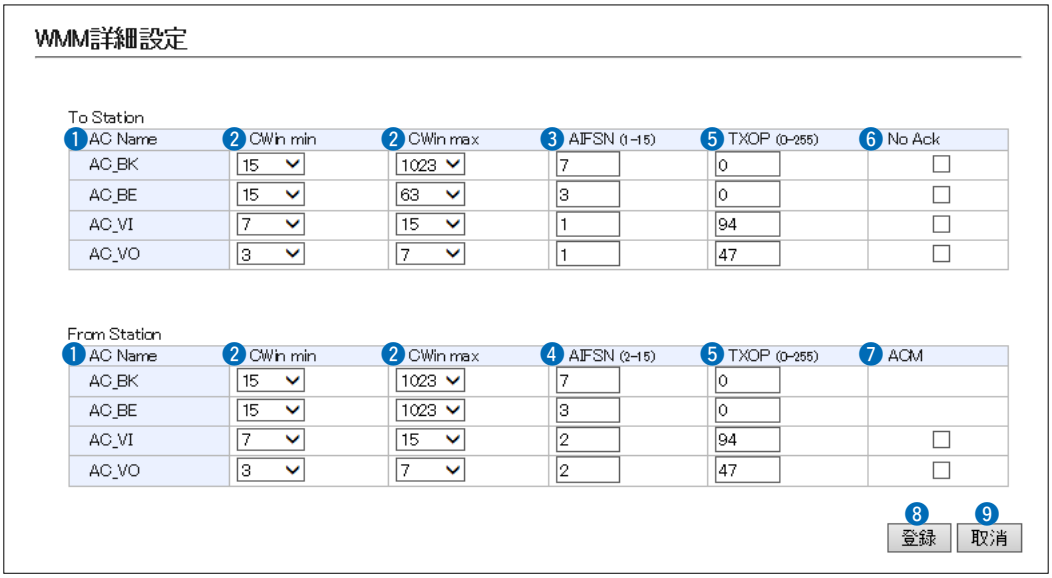
CWin(Contention Window)の最小値(min)/最大値(max)を設定します。チャンネルが一定期間未使用になったあとの送信タイミングをContention Windowから乱数で選択することで、[IEEE802.11]規格でのフレーム衝突を回避します。
設定値が小さいほど優先順位が上がり、設定値が大きいほど優先順位が下がります。　(出荷時の設定：[To Station]/[From Station]

CWin min→ AC_BK(15)
AC_BE(15)
AC_VI(7)
AC_VO(3)
[To Station]
CWin max→ AC_BK(1023)
AC_BE(63)
AC_VI(15)
AC_VO(7)
[From Station]
CWin max→ AC_BK(1023)
AC_BE(1023)
AC_VI(15)
AC_VO(7))

7.「WMM詳細」画面について

無線設定 > WMM詳細

■ WMM詳細設定(つづき)



❸AIFSN(1-15)……

Arbitration Interframe Space Number(フレーム送信間隔)を設定します。
設定値が小さいほど、バックオフ制御を開始する時間が早くなるため優先度が高くなります。
設定できる範囲は、「1～15」です。

(出荷時の設定:[To Station]→ AC_BK(7)
AC_BE(3)
AC_VI(1)
AC_VO(1))

❹AIFSN(2-15)……

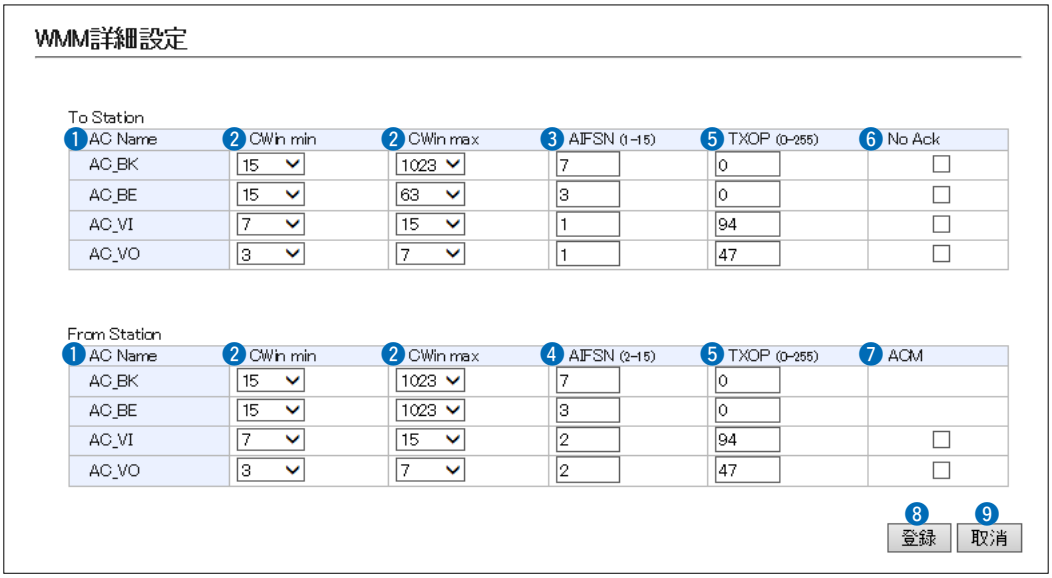
Arbitration Interframe Space Number(フレーム送信間隔)を設定します。
設定値が小さいほど、バックオフ制御を開始する時間が早くなるため優先度が高くなります。
設定できる範囲は、「2～15」です。

(出荷時の設定:[From Station]→ AC_BK(7)
AC_BE(3)
AC_VI(2)
AC_VO(2))

7.「WMM詳細」画面について

無線設定 > WMM詳細

■ WMM詳細設定(つづき)



❺TXOP(0-255) ……

チャンネルアクセス権を獲得したあと、排他的にチャンネルの使用を認める期間(Transmission Opportunity Limit)を設定します。
「0」が設定されている場合は、アクセス権獲得後に送信できるフレームは1つになります。

(出荷時の設定：[To Station]→ AC_BK(0)
AC_BE(0)
AC_VI(94)
AC_VO(47)
[From Station]→ AC_BK(0)
AC_BE(0)
AC_VI(94)
AC_VO(47))

❻No Ack……

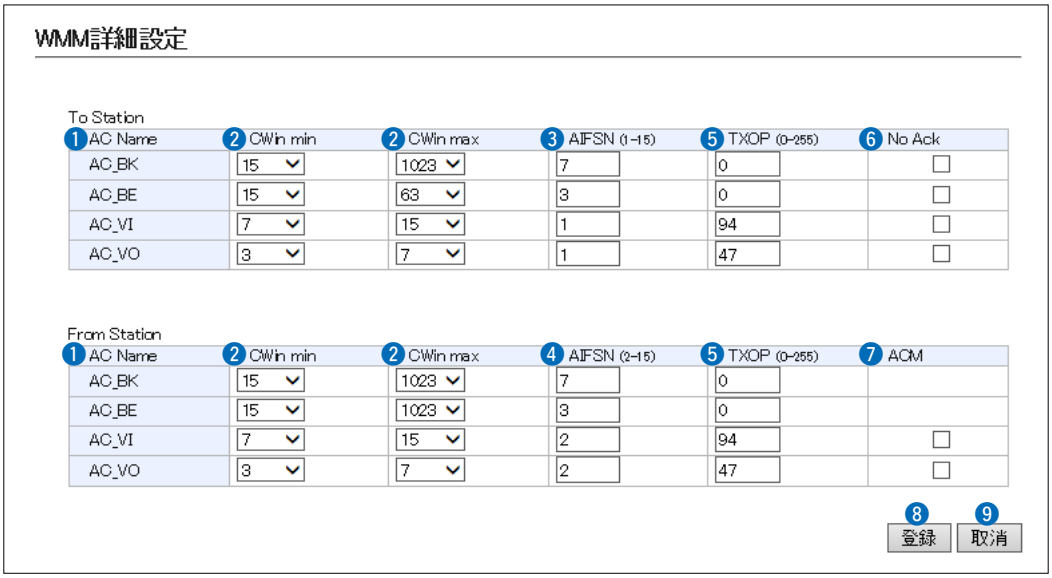
ACK(受信完了通知)による再送信制御についての設定です。
再送信制御をしないときは、チェックボックスにチェックマーク[✔]を入れます。

(出荷時の設定：[To Station]→ AC_BK ☐
AC_BE ☐
AC_VI ☐
AC_VO ☐)

7.「WMM詳細」画面について

無線設定 > WMM詳細

■ WMM詳細設定(つづき)



❼ACM ……

ACM(Admission Control Mandatory)を設定します。
ACMで保護されたカテゴリーで通信するときは、チェックボックスにチェックマーク[✔]を入れます。

(出荷時の設定：[From Station]→ AC_VI □ AC_VO □)

※ACMで保護されたカテゴリーで通信するには、この機能に対応したFWA無線LAN端末の設定が必要です。

❽〈登録〉 ……

「WMM詳細設定」項目で設定した内容を登録するボタンです。

❾〈取消〉 ……

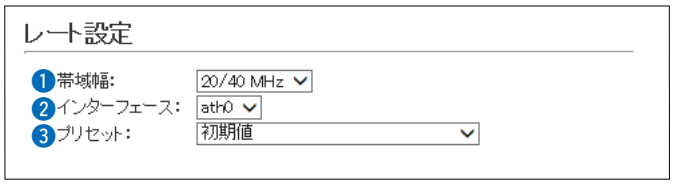
「WMM詳細設定」項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお、〈登録〉をクリックすると、変更前の状態には戻りません。

8.「レート」画面について

無線設定 > レート

■ レート設定

本製品と接続できるFWA無線LAN端末を制限するとき、またはマルチキャストパケット伝送時の速度を指定するときに、「レート」画面で仮想APごとにレートを設定できます。仮想AP(ath0～ath7)ごとにレートを設定できます。



❶帯域幅 …… 周波数帯域幅ごとにレート設定を変更できます。
(出荷時の設定：20/40MHz)
※10MHz帯域幅を選択すると、[HT-MCS]欄は設定できません。

❷インターフェース …… 設定する仮想APを選択します。 (出荷時の設定：ath0)
仮想APごとに、[レガシー]欄と[HT-MCS]欄の設定内容を変更できます。

❸プリセット …… プリセットされた設定を使用する場合に、「初期値」、「長距離通信 (64-QAM無効)」、「長距離通信(16/64-QAM 無効)」から選択します。
(出荷時の設定：初期値)
※設定したレートにより、接続が不安定になることがありますので、特に問題がない場合は、出荷時の設定でご使用ください。
「初期値」で通信が安定しない場合は、ほかのプリセットを試してください。
切り替えた方がよいときは、そのプリセットでご使用ください。
※プリセットされた設定内容を変更したときは、[プリセット]欄に「ー」が表示されます。

8.「レート」画面について(つづき)

無線設定 > レート

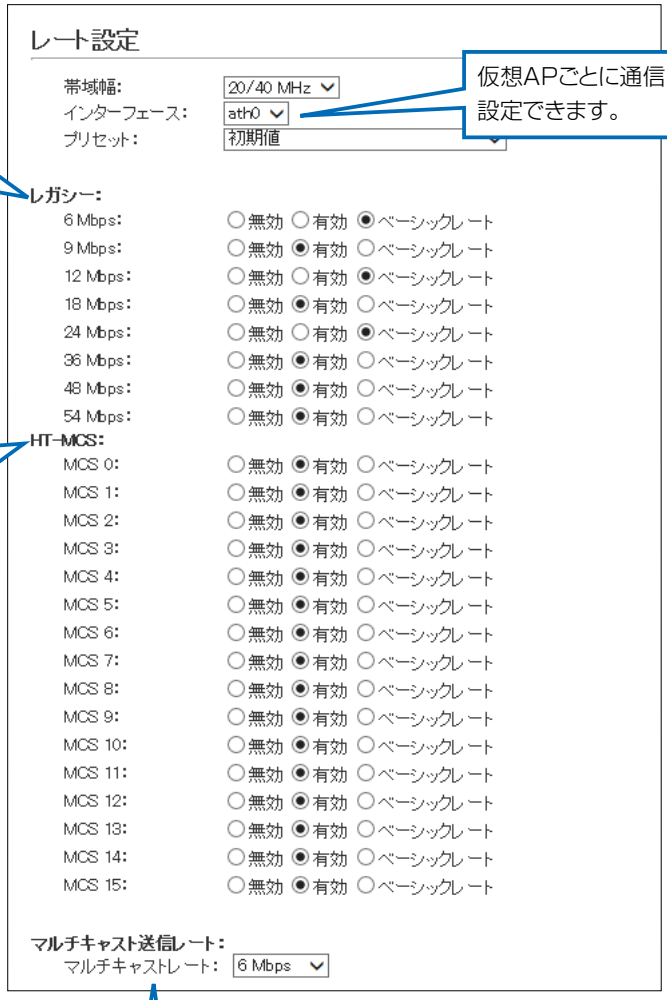
■ 通信レートの各設定について

本製品と接続できるFWA無線LAN端末を制限するとき、またはマルチキャストパケット伝送時の速度を指定するときは、「レート」画面で各仮想AP(ath0～ath7)のレートを設定します。
ベーシックレートを設定した場合、FWA無線LAN端末側が、その速度やMCS値を使用できることが条件となります。
たとえば、ベーシックレートを設定したレートで通信できないFWA無線LAN端末は、本製品に接続できません。

※設定したレートにより、接続が不安定になることがありますので、特に問題がない場合は、出荷時の設定でご使用ください。

[レガシー]欄は通信速度ごとに設定します。
◎無効 : 選択した速度では通信しない
◎有効 : 選択した速度で通信する
◎ベーシックレート
: FWA無線LAN端末が選択した速度で通信できない場合は接続を許可しない

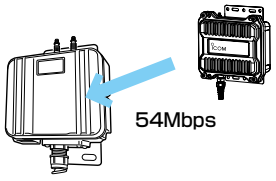
[HT-MCS]欄は、HT(High Throughput)の速度で使用する変調方式、ストリーム数、通信レートなどを対応付けしたMCS値(P.4-38)ごとに設定します。
◎無効 : 選択したMCS値では通信しない
◎有効 : 選択したMCS値で通信する
◎ベーシックレート
: FWA無線LAN端末が選択したMCS値で通信できない場合は接続を許可しない



マルチキャスト送信レートの設定について

接続した複数のFWA無線LAN端末の受信状態が異なるため、マルチキャストパケット伝送時、どの端末も受信できる最低速度で通信しています。(通信速度を優先させたくても変更できない状態)

エリアや端末の受信状況により、マルチキャストパケット伝送時の通信速度を選択すると、動画配信にも対応できるようになります。



※出荷時、マルチキャスト送信レートは、無線LAN規格の最低レートに設定されています。

8.「レート」画面について（つづき）

無線設定 > レート

■ MCS値ごとの通信レートについて

下表を目安に、「レート」画面で設定してください。

HT-MCS	ストリーム数	変調方式	通信レート（Mbps）			
			帯域幅 20MHz(HT20)		帯域幅 40MHz(HT40)	
			800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	6.5	7.2	13.5	15
1		QPSK	13	14.4	27	30
2		QPSK	19.5	21.7	40.5	45
3		16-QAM	26	28.9	54	60
4		16-QAM	39	43.3	81	90
5		64-QAM	52	57.8	108	120
6		64-QAM	58.5	65	121.5	135
7		64-QAM	65	72.2	135	150
8	2	BPSK	13	14.4	27	30
9		QPSK	26	28.9	54	60
10		QPSK	39	43.3	81	90
11		16-QAM	52	57.8	108	120
12		16-QAM	78	86.7	162	180
13		64-QAM	104	115.6	216	240
14		64-QAM	117	130	243	270
15		64-QAM	130	144.4	270	300

レガシー

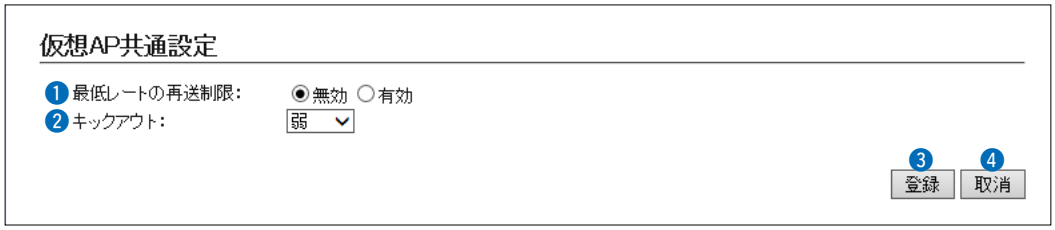
変調方式	通信レート（Mbps）	
	帯域幅 10MHz	帯域幅 20MHz
BPSK	3	6
BPSK	4.5	9
QPSK	6	12
QPSK	9	18
16-QAM	12	24
16-QAM	18	36
64-QAM	24	48
64-QAM	27	54

8.「レート」画面について（つづき）

無線設定 > レート

■ 仮想AP共通設定

無線ユニットごとに、本製品と通信するFWA無線LAN端末を制限して、通信状態を改善するときに設定します。



❶最低レートの再送制限 ……

最低レートでの再送を制限することで、ほかの端末に対する悪影響を抑止します。（出荷時の設定：無効）
通信品位の悪い端末の存在がほかの端末に対して悪影響をおよぼす場合に設定すると、全体の通信品位の悪化を低減できます。

❷キックアウト ……

通信品位の低い端末を早期に追い出すことで、ほかの端末に対する悪影響を抑止します。（出荷時の設定：弱）
通信品位の悪い端末の存在がほかの端末に対して悪影響をおよぼす場合に設定すると、全体の通信品位の悪化を低減できます。
設定するときは、「無効」、「弱」、「中」、「強」から選択します。
「強」にするほど、通信品位の低い端末を追い出しやすくなるため、通信品位の低い端末は切断されやすくなります。

❸〈登録〉 ……

「レート」画面で設定した内容を登録するボタンです。

❹〈取消〉 ……

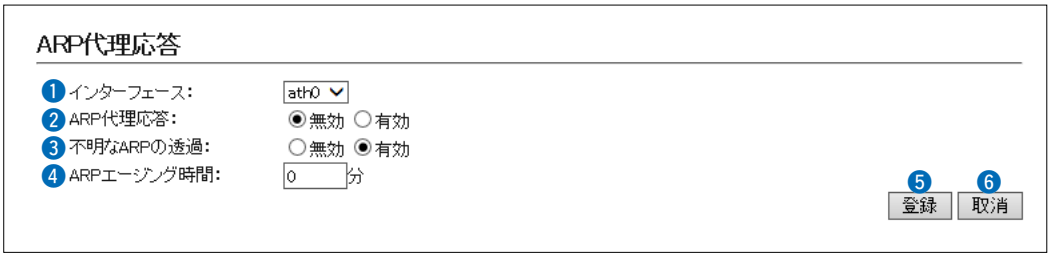
「レート」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお、〈登録〉をクリックすると、変更前の状態には戻りません。

9.「ARP代理応答」画面について

無線設定 ＞ ARP代理応答

■ ARP代理応答

FWA無線LAN端末へのARPリクエストに対する応答を代理することで、FWA無線LAN端末の省電力制御をする機能の設定です。



❶インターフェース …… 設定する仮想APを選択します。（出荷時の設定：ath0）

❷ARP代理応答 …… [インターフェース]（❶）欄で選択した仮想APで、ARP代理応答の機能を使用するかしないかを設定します。（出荷時の設定：無効）

❸不明なARPの透過 …… [インターフェース]（❶）欄で選択した仮想APと通信しているFWA無線LAN端末すべてのARP情報がわかっていて、不明なARPが来たとき、透過するかしないかを設定します。（出荷時の設定：有効）
ARPリクエストを受信したとき、FWA基地局（本製品）に接続しているFWA無線LAN端末のIPアドレス学習状況によって、下記のような処理をします。

◎IPアドレス学習済みのFWA無線LAN端末だけが存在する場合
ARPリクエストのTargetIPが学習したIPアドレスと一致する場合は、アクセスポイントが代理応答します。
一致しない場合、[不明なARPの透過]（❸）欄の設定が「有効」の場合は透過、「無効」の場合は破棄します。

◎IPアドレスを学習していないFWA無線LAN端末が1台でもいる場合
ARPリクエストのTargetIPが学習したIPアドレスと一致する場合は、アクセスポイントが代理応答します。
一致しない場合、[不明なARPの透過]（❸）欄の設定に関係なく、ARPリクエストを透過します。

❹ARPエージング時間 …… 学習したARP情報を削除するまでの時間を設定します。
設定できる範囲は、「0～1440（分）」です。（出荷時の設定：0）
※ARP情報を学習後、設定した時間が経過すると、該当するARP情報が削除されます。
※「0」（出荷時の設定）のときは、削除されません。
※FWA無線LAN端末がFWA基地局（本製品）から離脱した場合は、時間設定に関わらずARP情報が削除されます

❺〈登録〉 …… [ARP代理応答]項目で設定した内容を登録するボタンです。

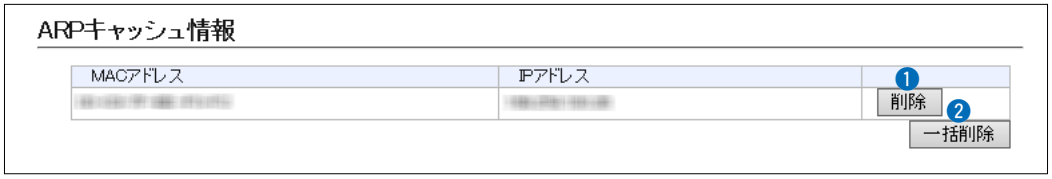
❻〈取消〉 …… [ARP代理応答]項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお、〈登録〉をクリックすると、変更前の状態には戻りません。

9.「ARP代理応答」画面について（つづき）

無線設定 ＞ ARP代理応答

■ ARPキャッシュ情報

学習したARP情報がMACアドレスとIPアドレスの組み合わせで表示されますので、必要に応じて削除してください。



❶〈削除〉 …… [ARP代理応答]項目の[インターフェース]欄で選択したインターフェースが学習したARPキャッシュ情報を削除するボタンです。

❷〈一括削除〉 …… [ARP代理応答]項目の[インターフェース]欄で選択したインターフェースが学習したARPキャッシュ情報を一括して削除するボタンです。

「管理」メニューについて

第 5 章

この章では、
「管理」メニューで表示される設定画面について説明します。

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

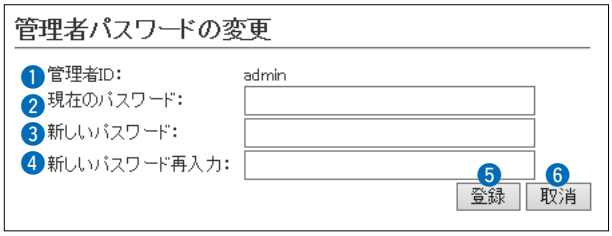
5 「管理」メニューについて

1.「管理者」画面について

管理 > 管理者

■ 管理者パスワードの変更

本製品の設定画面にアクセスするためのパスワードを変更します。



❶管理者ID ……

本製品の設定画面へのアクセスを許可する管理者IDを表示します。
※本製品の設定画面にアクセスすると、ユーザー名として入力を求められますので、本製品の管理者ID(admin)を入力します。
※本製品の[管理者ID]は、変更できません。

❷現在のパスワード ……

新しいパスワードに変更するとき、現在のパスワードを大文字/小文字の区別に注意して入力します。 (出荷時の設定：admin)
※入力中の文字は、すべて＊(アスタリスク)、または●(黒丸)で表示します。

❸新しいパスワード ……

新しいパスワードを入力します。
大文字/小文字の区別に注意して、任意の英数字/記号(半角31文字以内)で入力します。
※新しいパスワードを登録後は、設定内容がマスクされ、すぐにパスワードの入力を求める画面を表示しますので、そこに新しいパスワードを入力します。

❹新しいパスワード再入力 ……

確認のために、新しいパスワードを再入力します。

❺〈登録〉 ……

[管理者パスワードの変更]項目で設定した内容を登録するボタンです。

❻〈取消〉 ……

[管理者パスワードの変更]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。

不正アクセス防止のアドバイス
本製品に設定するすべてのパスワードは、容易に推測されないものにしてください。
数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた長く複雑なものにし、さらに定期的にパスワードを変更されることをおすすめします。

ご注意
パスワードをお忘れの場合、本製品の全設定を初期化する以外に方法がありません。
初期化の方法は、お買い上げの販売店、または弊社サポートセンターにお問い合わせください。

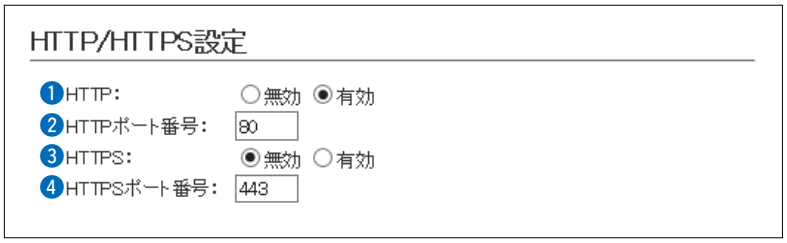
株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

2.「管理ツール」画面について

管理 > 管理ツール

■ HTTP/HTTPS設定

HTTPとHTTPSは、WWWブラウザーから設定画面にアクセスするためのプロトコルです。
※両方を「無効」に設定すると、WWWブラウザーを使用して、本製品の設定画面にアクセスできなくなりますのでご注意ください。



❶HTTP ……

本製品へのHTTPプロトコルによるアクセスの許可を設定します。
（出荷時の設定：有効）

❷HTTPポート番号 ……

本製品へのHTTPプロトコルによるアクセスのポート番号を設定します。
（出荷時の設定：80）
設定できる範囲は、「80」と「1024～65535」です。
そのほか、本製品が使用する一部のポートで利用できないものがあります。
※HTTPS、Telnet、SSHを使用時、これらに設定されたポート番号と重複しないように設定してください。

❸HTTPS ……

本製品へのHTTPSプロトコルによるアクセスの許可を設定します。
（出荷時の設定：無効）
※HTTPSを使用すると、パスワードやデータが暗号化されるため、TelnetやHTTPでのアクセスより安全性が向上します。

❹HTTPSポート番号 ……

本製品へのHTTPSプロトコルによるアクセスのポート番号を設定します。
（出荷時の設定：443）
設定できる範囲は、「443」と「1024～65535」です。
そのほか、本製品が使用する一部のポートで利用できないものがあります。
※HTTP、Telnet、SSHを使用時、これらに設定されたポート番号と重複しないように設定してください。

2.「管理ツール」画面について(つづき)

管理 > 管理ツール

■ HTTP/HTTPS設定後、設定画面にアクセスできなくなったときは

Telnet(P.7-4)で本製品(例：192.198.0.1)にアクセスして、BS-900 #につづけて、下記の太字部分のように入力後、[Enter]キーを押してください。

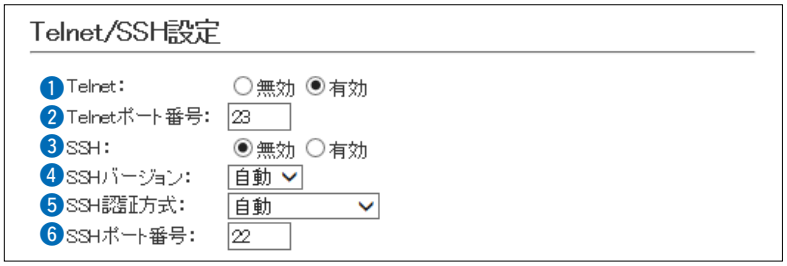
①BS-900 # **network http on**　と入力し[Enter]キーを押します。
②BS-900 # **save**　と入力し[Enter]キーを押す。
③BS-900 # **restart**　と入力し[Enter]キーを押す。
④本製品の再起動が完了したら、本製品の設定画面へのアクセスを確認します。

2.「管理ツール」画面について（つづき）

管理 > 管理ツール

■ Telnet/SSH設定

TelnetクライアントやSSHクライアントからアクセスするためのプロトコルについて設定します。



❶Telnet ……

本製品へのTelnetプロトコルによるアクセスの許可を設定します。
（出荷時の設定：有効）

❷Telnetポート番号 ……

本製品へのTelnetプロトコルによるアクセスのポート番号を設定します。
（出荷時の設定：23）
設定できる範囲は、「23」と「1024～65535」です。
そのほか、本製品が使用する一部のポートで利用できないものがあります。
※HTTP、HTTPS、SSHを使用時、これらに設定されたポート番号と重複しないように設定してください。

❸SSH ……

本製品へのSSHプロトコルによるアクセスの許可を設定します。
（出荷時の設定：無効）
※「有効」を選択して、[SSH認証方式]（❺）欄で、「自動」/「公開鍵認証」を選択すると、[SSH公開鍵管理]項目と[SSH公開鍵登録状況]項目を表示します。
※SSHを使用すると、Telnetクライアントプログラムを使用して設定する内容を暗号化して通信できます。
※SSHを使用するには、別途SSHクライアントをご用意ください。

❹SSHバージョン ……

[SSH]（❸）欄で「有効」を設定したとき、本製品で使用するSSH機能のバージョンを設定します。（出荷時の設定：自動）
◎**1**　：バージョン1を使用します。
◎**2**　：バージョン2を使用します。
◎**自動**：「バージョン1」と「バージョン2」を自動認識します。

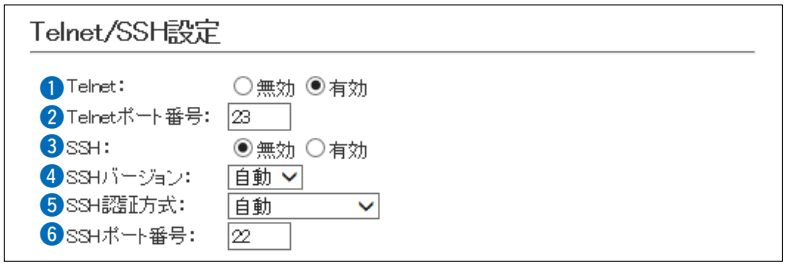
❺SSH認証方式 ……

[SSH]（❸）欄で「有効」を設定したとき、本製品へ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：自動）
◎**パスワード認証**：パスワードを使用して認証するときに設定します。
◎**公開鍵認証**　：公開鍵を使用して認証するときに設定します。
◎**自動**　：「パスワード認証」と「公開鍵認証」を自動認識します。

2.「管理ツール」画面について

管理 > 管理ツール

■ Telnet/SSH設定（つづき）



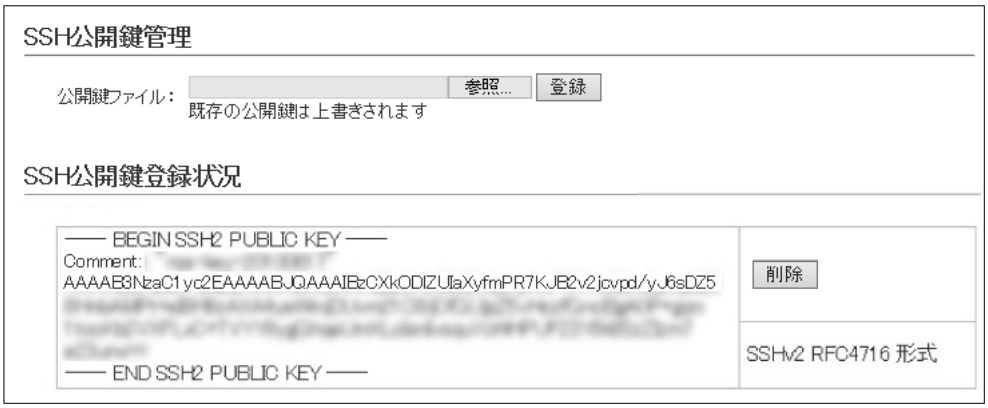
6 SSHポート番号 …… 本製品へのSSHプロトコルによるアクセスのポート番号を設定します。
（出荷時の設定：22）
設定できる範囲は、「22」と「1024～65535」です。
そのほか、本製品が使用する一部のポートで利用できないものがあります。
※HTTP、Telnet、HTTPSを使用時、これらに設定されたポート番号と重複しないように設定してください。

2.「管理ツール」画面について(つづき)

管理 > 管理ツール

■ SSH公開鍵管理

SSHでアクセスするときに使用する公開鍵を登録します。
※[Telnet/SSH設定]項目の[SSH]欄を「有効」、[SSH認証方式]欄を「自動」/「公開鍵認証」に設定したとき表示される項目です。
※画面は、登録例です。



公開鍵ファイル……

登録できる鍵は、1種類だけです。

【登録の手順】

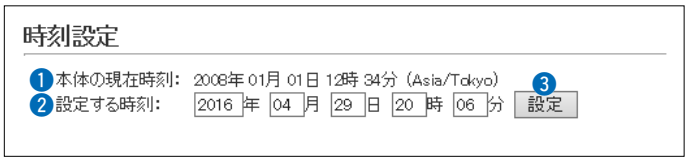
1.〈参照...〉をクリックして、公開鍵ファイルの保存先を指定します。
2.〈登録〉をクリックします。
●[SSH公開鍵登録状況]項目に公開鍵の内容を表示します。
※公開鍵ファイルの登録を取り消すときは、[SSH公開鍵登録状況]項目の〈削除〉をクリックします。

3.「時計」画面について

管理 > 時計

■ 時刻設定

本製品の内部時計を手動で設定します。



❶本体の現在時刻 …… 本製品に設定されている時刻を表示します。
※自動時計設定時、インターネット上に存在するNTPサーバーに日時の問い合わせをしているときは、「NTPサーバーへアクセスしています...」を表示します。

❷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表示します。
※お使いのWWWブラウザーで表示画面を更新すると、パソコンの時計設定を取得して表示します。

❸〈設定〉 …… [設定する時刻](❷)欄に表示された時刻を本製品に手動で設定するボタンです。
※時刻を手動で設定するときは、本製品の設定画面に再度アクセスするか、お使いのWWWブラウザーで表示画面を更新してから、〈設定〉をクリックしてください。

3.「時計」画面について（つづき）

管理 > 時計

■ 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ーの設定です。

❶自動時計設定 ……

本製品の自動時計設定機能を設定します。（出荷時の設定：無効）
「有効」に設定すると、インターネット上に存在するNTPサーバーに日時の問い合わせをして、内部時計を自動設定します。

❷NTPサーバー１ ……

アクセスするNTPサーバーのIPアドレスを入力します。
（出荷時の設定：210.173.160.27）
応答がないときは、[NTPサーバー2]（❸）欄で設定したNTPサーバーにアクセスします。
※初期に参照しているNTPサーバーアドレスは、インターネットマルチフィード株式会社 http://www.jst.mfeed.ad.jp/ のものです。

❸NTPサーバー２ ……

[NTPサーバー1]の次にアクセスさせるNTPサーバーがあるときは、そのIPアドレスを入力します。（出荷時の設定：210.173.160.57）

❹アクセス時間間隔 ……

NTPサーバーにアクセスする間隔を設定します。（出荷時の設定：1）
設定できる範囲は、「1～99」（日）です。
※設定した日数でアクセスできなかったときは、次の間隔までアクセスしません。

❺前回アクセス日時 ……

NTPサーバーにアクセスした日時を表示します。

自動時計設定機能について
自動時計設定機能で「有効」を選択して〈登録〉を押した直後、NTPサーバーに日時の問い合わせをして、内部時計を自動設定します。
また、自動時計設定機能を「有効」に設定すると、本体起動時にNTPサーバーに日時の問い合わせをします。
それ以降は、設定されたアクセス時間間隔で、内部時計を自動設定します。

ご注意
自動時計設定機能は、NTPサーバーへの問い合わせ先（経路）を設定する必要があります。
経路を設定しないときは、問い合わせできませんので、自動時計設定機能をお使いいただけません。
「ネットワーク設定」メニュー→「LAN側IP」画面→[IPアドレス設定]項目にある[デフォルトゲートウェイ]欄、または「ルーティング」画面の[スタティックルーティング設定]項目で、ルーティングテーブルを設定してください。

3.「時計」画面について

管理 > 時計

■ 自動時計設定(つづき)

❻次回アクセス日時 …… NTPサーバーにアクセスする予定日時を、[前回アクセス日時](❺)欄と[アクセス時間間隔](❹)欄で設定された日数より算出して表示します。

❼〈登録〉 …… [自動時計設定]項目で設定した内容を登録するボタンです。

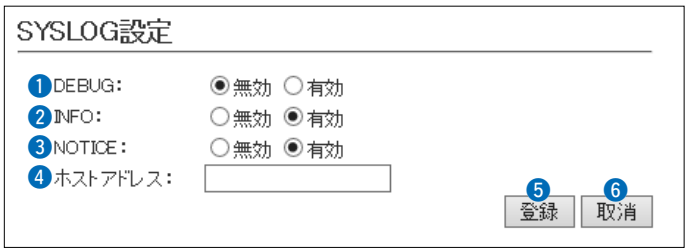
❽〈取消〉 …… [自動時計設定]項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

4.「SYSLOG」画面について

管理 > SYSLOG

■ SYSLOG設定

指定したホストにログ情報などを出力するための設定です。



❶DEBUG…… 各種デバッグ情報をSYSLOGに出力する設定です。（出荷時の設定：無効）

❷INFO…… INFOタイプのメッセージをSYSLOGに出力する設定です。
（出荷時の設定：有効）

❸NOTICE …… NOTICEタイプのメッセージをSYSLOGに出力する設定です。
（出荷時の設定：有効）

❹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サーバー機能に対応している必要があります。

❺〈登録〉 …… [SYSLOG設定]項目で設定した内容を登録するボタンです。

❻〈取消〉 …… [SYSLOG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。

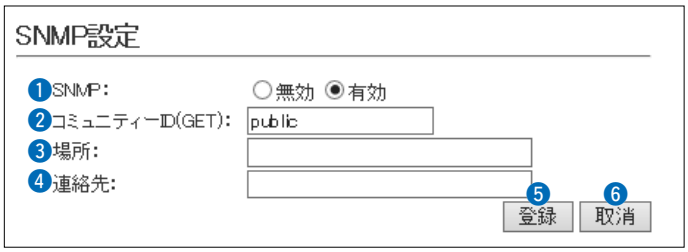
株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

5.「SNMP」画面について

管理 > SNMP

■ 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本製品の情報を自動的に収集して、ネットワーク管理をするときの設定です。



❶SNMP …… 本製品のSNMP機能を設定します。（出荷時の設定：有効）
「有効」に設定すると、本製品の設定情報をSNMP管理ツール側で管理できます。

❷コミュニティー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、半角31文字以内の英数字で入力します。（出荷時の設定：public）

❸場所 …… MIB-II(RFC1213)に対応するSNMP管理ツール側で表示される場所を、半角127文字以内の英数字で入力します。

❹連絡先 …… MIB-II(RFC1213)に対応するSNMP管理ツール側で表示される連絡先を、半角127文字以内の英数字で入力します。

❺〈登録〉 …… [SNMP設定]項目で設定した内容を登録するボタンです。

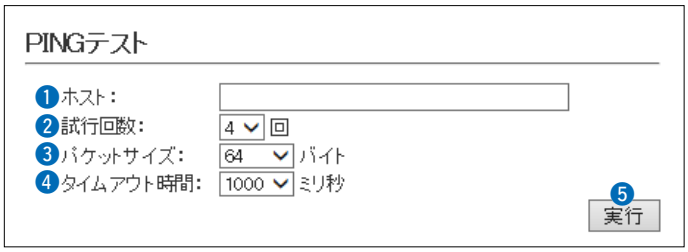
❻〈取消〉 …… [SNMP設定]項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

6.「ネットワークテスト」画面について

管理 > ネットワークテスト

■ PINGテスト

本製品からPINGを送出し、ネットワークの疎通確認テストをします。



❶ホスト …… PINGを送出する対象ホストのIPアドレス、またはドメイン名を半角64文字以内で入力します。

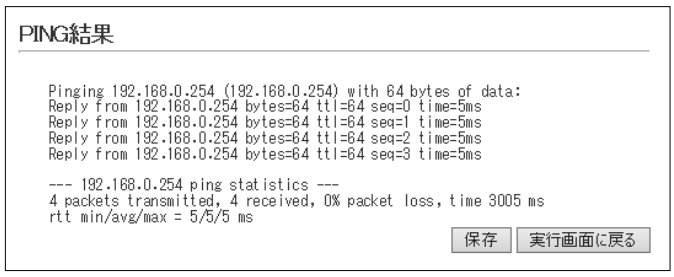
❷試行回数 …… PINGを送出する回数を、「1」、「2」、「4」、「8」から選択します。
（出荷時の設定：4）

❸パケットサイズ …… 送信するパケットのデータ部分のサイズを設定します。（出荷時の設定：64）
設定できるサイズは、「32」、「64」、「128」、「256」、「512」、「1024」、「1448」、「1500」、「2048」（バイト）です。

❹タイムアウト時間 …… PING送出後、応答を待つ時間を、「500」、「1000」、「5000」（ミリ秒）から選択します。（出荷時の設定：1000）
設定した時間以内に応答がないときは、タイムアウトになります。

❺〈実行〉 …… PINGテストを実行するボタンです。
クリックして、表示される画面にしたがって操作すると、「PING結果」表示に切り替わり、テスト結果を表示します。

【PING結果について】



※上図は、表示例です。

◎〈保存〉をクリックすると、テスト結果をファイル（拡張子：txt）に保存します。
※ファイル名は、「ping_［対象ホストのアドレス］.txt」で保存されます。
◎〈実行画面に戻る〉をクリックすると、画面が「PINGテスト」表示に戻ります。

6.「ネットワークテスト」画面について(つづき)

管理 > ネットワークテスト

■ 経路テスト

本製品から特定のノードに対しての経路テスト(tracert/traceroute)をします。

❶ノード …… 経路テストをする対象ノード(機器)のアドレスを入力します。

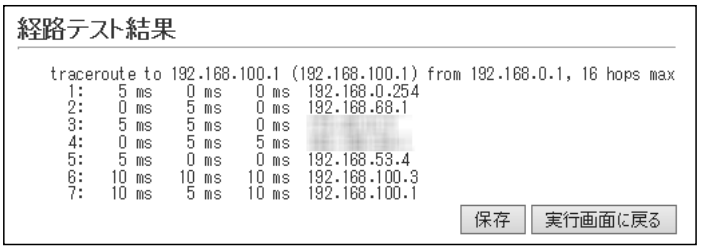
❷最大ホップ数 …… 経由するホップ数(中継設備数)の最大値を、「4」、「8」、「16」、「32」から選択します。(出荷時の設定:16)

❸タイムアウト時間 …… テスト開始後、応答を待つ時間を、「1」、「3」、「5」(秒)から選択します。(出荷時の設定:3)
設定した時間以内に応答がないときは、タイムアウトになります。

❹DNS名前解決 …… テスト結果に表示するIPアドレスを、ホスト名に変換するかどうか設定します。(出荷時の設定:有効)
「有効」に設定すると、中継設備や対象ノードのアドレスに対して、DNS名前解決をします。

❺〈実行〉 …… 経路テストを実行するボタンです。
クリックして、表示される画面にしたがって操作すると、「経路テスト結果」表示に切り替わり、テスト結果を表示します。

【経路テスト結果について】



※上図は、表示例です。

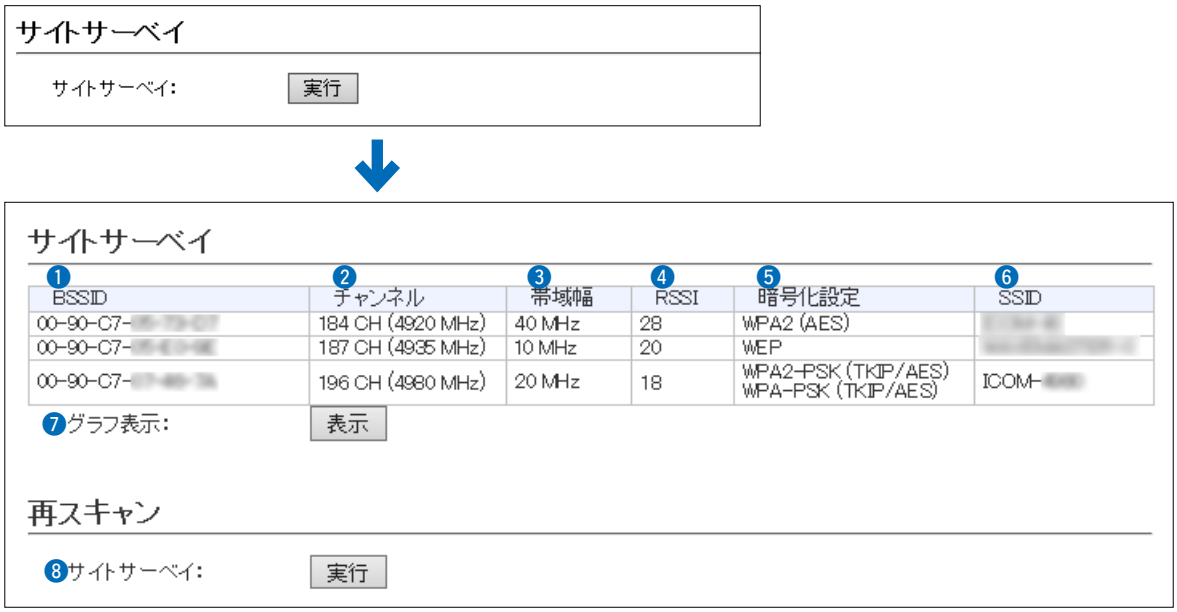
◎〈保存〉をクリックすると、テスト結果をファイル(拡張子:txt)に保存します。
※ファイル名は、「tracert_[対象ノードのアドレス] .txt」で保存されます。
◎〈実行画面に戻る〉をクリックすると、画面が「経路テスト」表示に戻ります。

7.「サイトサーベイ」画面について

管理 > サイトサーベイ

■ サイトサーベイ

〈実行〉をクリックして、表示される画面にしたがって操作すると、本製品の設置場所でのサイトサーベイ(電波環境調査)実施し、結果を一覧で表示します。
※本製品の無線伝送エリア内で稼働するFWA基地局の情報を一覧で表示します。(最大表示件数：255件)
　FWA基地局が検出されないときは、項目名だけを表示します。
※スキャン実行中は、FWA無線LAN端末と通信できません。



❶**BSSID** …… 検出されたFWA基地局(本製品を除く)のBSSIDを表示します。

❷**チャンネル** …… 検出されたFWA基地局(本製品を除く)の無線チャンネルを表示します。

❸**帯域幅** …… 検出されたFWA基地局(本製品を除く)の帯域幅を表示します。

❹**RSSI** …… 検出されたFWA基地局(本製品を除く)から受信した電波の強さを表示します。
※数値が大きいほど、電波強度が強いことを示しています。

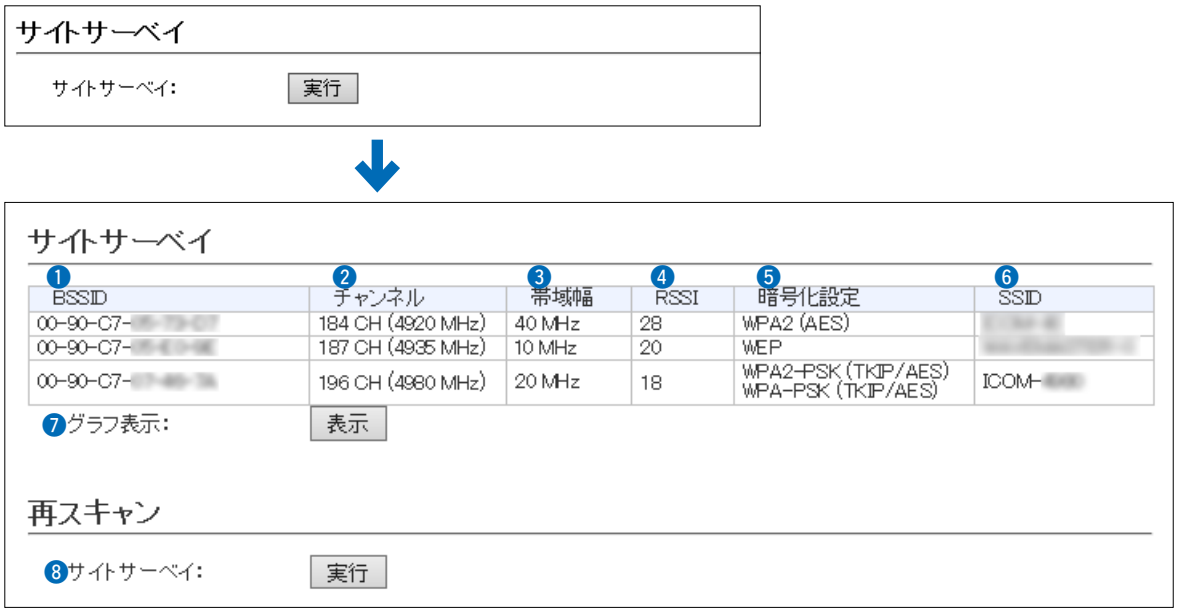
❺**暗号化設定** …… 検出されたFWA基地局(本製品を除く)が通信で使用する暗号化方式を表示します。
※「WEP RC4」、または「OCB AES」のときは、「WEP」と表示します。

❻**SSID** …… 検出されたFWA基地局(本製品を除く)のSSIDを表示します。

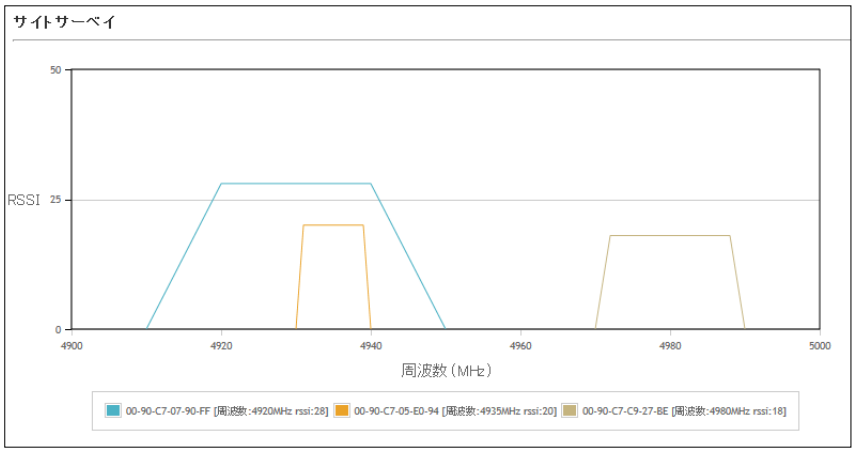
7.「サイトサーベイ」画面について

管理 > サイトサーベイ

■ サイトサーベイ（つづき）



❼グラフ表示 …… 〈表示〉をクリックすると、サイトサーベイ（電波環境調査）の結果をグラフで表示します。



※上図は、表示例です。

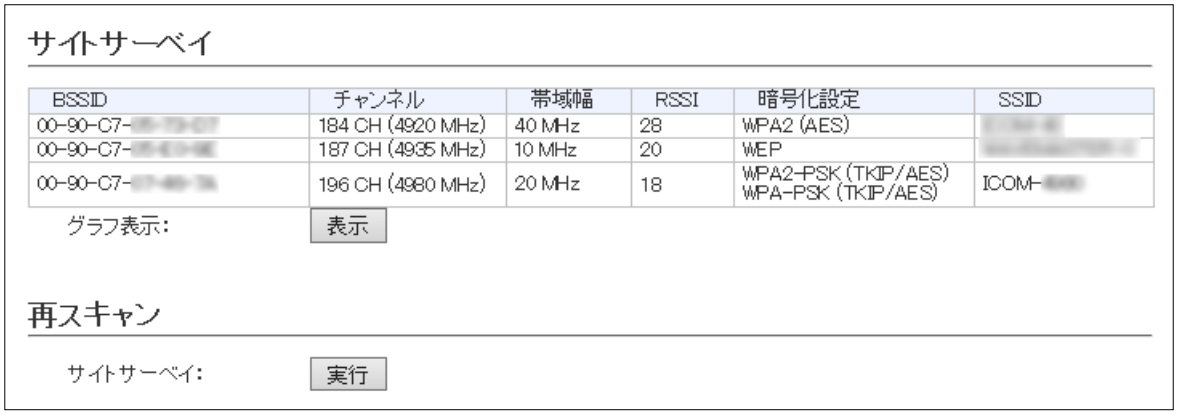
❽サイトサーベイ …… 〈実行〉をクリックすると、再度サイトサーベイを実行します。

7.「サイトサーベイ」画面について(つづき)

管理 > サイトサーベイ

■ サイトサーベイの調査例について

下記の画面は、本製品の設置場所でサイトサーベイ(電波環境調査)を実行した例です。



上記画面の調査例では、本製品以外に3台のFWA基地局が、本製品の設置場所周辺で稼働していることを示しています。電波干渉を回避するためには、本製品のチャンネルを「192CH」、帯域幅を「20MHz」に設定すればよいという目安になります。

※電波法上、無線局の登録申請で許可されたチャンネル以外を使用することはできませんので、ご注意ください。

※実際に本製品を設置する場所で調査してください。

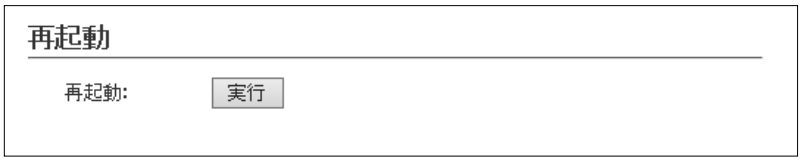
※電波状況は、時間帯によって変化することがありますので、設置前と設置後に、ある程度間隔をおきながら数回ずつ調査することをおすすめします。

8.「再起動」画面について

管理 > 再起動

■ 再起動

〈実行〉をクリックすると、本製品は再起動します。

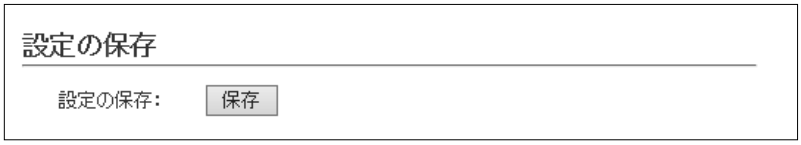


9.「設定の保存/復元」画面について

管理 > 設定の保存/復元

■ 設定の保存

本製品の設定内容を保存します。
※保存した設定ファイル(拡張子：sav)は、本製品以外の製品では使用できません。



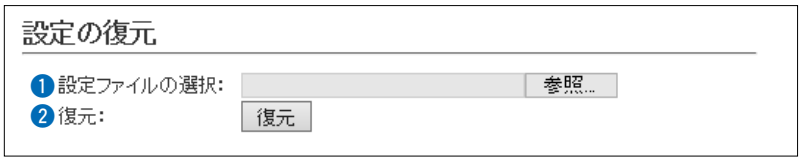
設定の保存……

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できます。
〈保存〉をクリックして、表示された画面にしたがって操作すると、設定ファイル(拡張子：sav)を保存できます。
保存したファイルは、[設定の復元]項目の操作で、本製品に書き込みできます。

管理 > 設定の保存/復元

■ 設定の復元

保存した設定ファイルを本製品に書き込みます。
※書き込みには数分かかる場合があります。



❶設定ファイルの選択 ……

[設定の保存]項目の操作で保存した設定ファイル(拡張子：sav)の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指定するため、〈参照...〉をクリックします。
表示された画面から目的の設定ファイルをクリックして、〈開く(O)〉をクリックすると、選択した設定ファイルの参照先が表示されます。

❷復元 ……

[設定ファイルの選択](❶)欄のテキストボックスに保存先を指定後、〈復元〉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。
※書き込みを完了すると、本製品は自動的に再起動します。
※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。

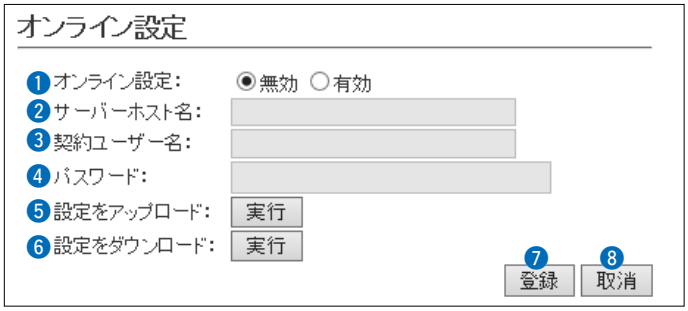
設定ファイルについてのご注意
本製品以外の機器へ書き込み、改変による障害、および書き込みに伴う本製品の故障、誤動作、不具合、破損、データの消失、または停電などの外部要因により通信、通話などの機会を失ったために生じる損害や逸失利益、または第三者からのいかなる請求についても当社は一切その責任を負いかねますのであらかじめご了承ください。

9.「設定の保存/復元」画面について（つづき）

管理 > 設定の保存/復元

■ オンライン設定

本製品の設定内容を暗号化された通信経路を利用して転送でき、遠隔地から保守できます。
※オンライン設定を使用するには、別途SFTPサーバーが必要です。



❶オンライン設定 …… オンライン設定を使用するとき、「有効」にします。（出荷時の設定：無効）
※SFTPサーバーの設備がない場合は、「有効」に設定しても、使用できません。

❷サーバーホスト名…… SFTPサーバーホスト名のIPアドレス、またはFQDN(Fully Qualified Domain Name)を128文字(半角)以内で入力します。

❸契約ユーザー名 …… SFTPサーバー契約ユーザー名を、128文字(半角英数字/記号)以内で入力します。

❹パスワード…… SFTPサーバーパスワードを、128文字(半角英数字/記号)以内で入力します。

❺設定をアップロード …… 〈実行〉をクリックすると、本製品から設定内容を読み出して、自動でSFTPサーバーへ転送します。

❻設定をダウンロード…… 〈実行〉をクリックすると、SFTPサーバーから本製品の設定内容を読み出して、本製品に自動で書き込みます。
※設定内容の書き込みが完了すると、本製品が自動的に再起動され、設定が有効になります。

❼〈登録〉 …… [オンライン設定]項目で設定した内容を登録するボタンです。

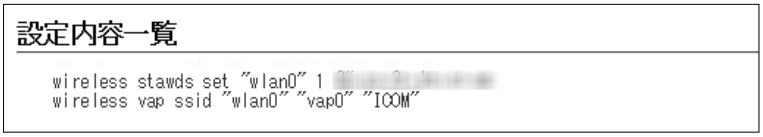
❽〈取消〉 …… [オンライン設定]項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

9.「設定の保存/復元」画面について（つづき）

管理 > 設定の保存/復元

■ 設定内容一覧

出荷時の設定から変更された内容を表示します。
※出荷時や全設定初期化後は、何も表示されません。
※画面の内容は、表示例です。

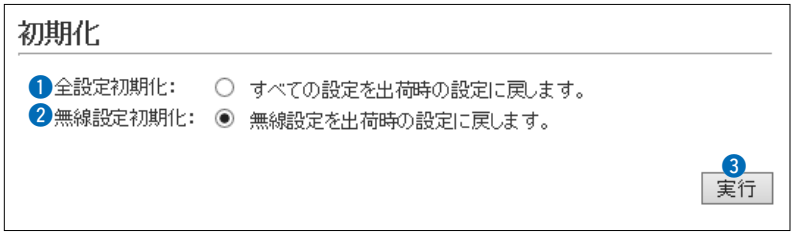


10.「初期化」画面について

管理 > 初期化

■ 初期化

選択した初期化条件で、本製品の設定内容を初期化します。
※IPアドレスと管理者用のパスワードが不明な場合などの初期化については、7-4ページをご覧ください。



1 全設定初期化 …… 本製品に設定されたすべての内容を出荷時の状態に戻します。(P.7-4)
※初期化によって、本製品にアクセスできなくなった場合は、パソコンのIPアドレスを変更してください。

2 無線設定初期化 …… 「無線設定」メニューの設定内容を出荷時の状態に戻します。

3 〈実行〉 …… 選択された初期化条件にしたがって、初期化します。

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

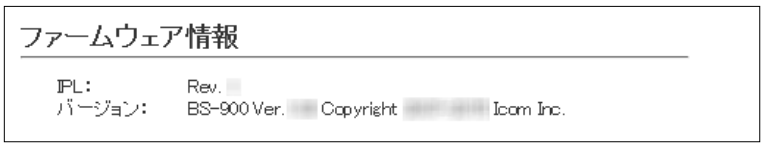
11.「ファームウェアの更新」画面について

バージョンアップについてのご注意
故障の原因になるため、ファームウェアの更新が完了するまで、本製品の電源を切らないでください。
※バージョンアップによって追加や変更になる機能、注意事項については、あらかじめ弊社ホームページでご確認ください。

管理 > ファームウェアの更新

■ ファームウェア情報

本製品のファームウェアについて、バージョン情報を表示します。

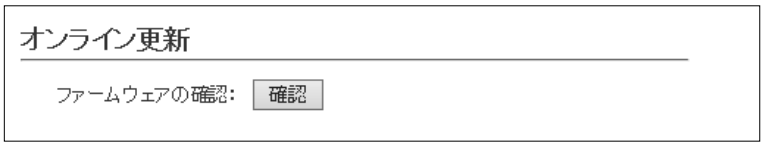


11.「ファームウェアの更新」画面について(つづき)

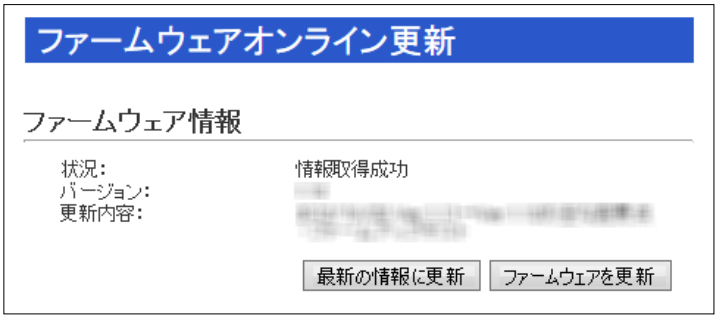
管理 > ファームウェアの更新

■ オンライン更新

ファームウェアをオンラインでバージョンアップします。
※ファームウェアの確認には、インターネットへの接続環境と本製品へのDNS設定、デフォルトゲートウェイ(P.3-3)の設定が必要です。



ファームウェアの確認……　〈確認〉をクリックすると、アップデート管理サーバーに接続します。
接続に成功すると、最新のファームウェア情報(下図)を表示します。



【ファームウェア情報について】

◎「新しいファームウェアはありません」が表示されるときは、現在のファームウェアが最新ですので、ファームウェアの更新は必要ありません。
◎「情報取得成功」と更新内容が表示されたときは、〈ファームウェアを更新〉をクリックすると最新のファームウェアをアップデート管理サーバーからオンラインで更新できます。(P.7-8)
◎「接続失敗」や「サーバーからエラーが返されました」が表示されるときは、下記を参考に、本製品からアップデート管理サーバーへ接続できる環境であることをご確認ください。

デフォルトゲートウェイとDNSサーバーアドレスを本製品に設定していますか?
→「ネットワーク設定」メニューの「LAN側IP」画面で設定を確認する
本製品からWeb通信することを、ファイアウォールなどで遮断していませんか?
→ネットワーク管理者に確認する

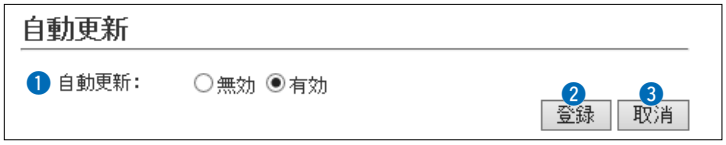
バージョンアップについてのご注意
故障の原因になるため、ファームウェアの更新が完了するまで、本製品の電源を切らないでください。
※バージョンアップによって追加や変更になる機能、注意事項については、あらかじめ弊社ホームページでご確認ください。

11.「ファームウェアの更新」画面について(つづき)

管理 > ファームウェアの更新

■ 自動更新

ファームウェアの自動更新機能を使用するときに設定します。



❶自動更新 …… ファームウェアの自動更新機能を設定します。 (出荷時の設定:有効)

◎ファームウェアに重要な更新が含まれる場合

自動更新機能が動作し、アップデート管理サーバーから本製品のファームウェアを更新します。

※運用中にファームウェアを更新して本製品が再起動しますので、自動更新を望まない場合は「無効」に設定してください。

◎ファームウェアに重要な更新が含まれていない場合

[MODE]ランプが橙点灯します。

※オンラインファーム検知時、ファームウェアは自動的に更新されません。

※ご都合のよいときに、ファームウェアを手動で更新してください。

(P.7-8)

❷〈登録〉 …… [自動更新]項目で設定した内容を登録するボタンです。

❸〈取消〉 …… [自動更新]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。

11.「ファームウェアの更新」画面について(つづき)

管理 > ファームウェアの更新

■ 手動更新

パソコンに保存しているファイルを指定してファームウェアをバージョンアップします。

❶ファームウェアの選択 …… 〈参照...〉をクリックして、表示された画面から、パソコンに保存している本製品のファームウェアファイル(拡張子：dat)を選択して、〈開く(O)〉をクリックします。
選択したファイルとその階層が、[ファームウェアの選択]項目のテキストボックスに自動入力されたことを確認します。

❷ファームウェアの更新 …… 〈更新〉をクリックすると、[ファームウェアの選択]項目のテキストボックスに表示された保存先のファームウェアファイル(拡張子：dat)を本製品に書き込みます。
更新を開始すると、「ファームウェアを更新しています。」と表示されます。

バージョンアップについてのご注意
故障の原因になるため、ファームウェアの更新が完了するまで、本製品の電源を切らないでください。
※バージョンアップによって追加や変更になる機能、注意事項については、あらかじめ弊社ホームページでご確認ください。

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

おもな機能の設定について

第 6 章

この章では、
本製品のおもな機能の設定について説明しています。

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

1. [WEP RC4]暗号化を設定するには

[WEP RC4]暗号化設定は、次の3とおりです。

◎16進数で暗号鍵(キー)を直接入力する(P.6-3)
◎ASCII文字で暗号鍵(キー)を直接入力する(P.6-4)
◎[キージェネレーター]に入力した文字列から暗号鍵(キー)を生成する(P.6-5)

※出荷時や全設定初期化時、暗号化は設定されていません。

■ 暗号鍵(キー)の入力について

[暗号化方式]の設定によって、入力する暗号鍵(キー)の文字数や桁数が異なります。
また、入力された文字数、および桁数によって、入力モード(16進数/ASCII文字)を自動判別します。

ネットワーク認証		暗号化方式	入力モード	
オープンシステム	共有キー		16進数(HEX)	ASCII文字
○	×	なし(出荷時の設定)	―	―
○	○	WEP RC4 64(40)ビット	10桁	5文字(半角)
○	○	WEP RC4 128(104)ビット	26桁	13文字(半角)
○	○	WEP RC4 152(128)ビット	32桁	16文字(半角)

※入力できる桁数、および文字数は、( )内のビット数に対する値です。

■ ASCII文字→16進数変換表

相手が指定する[入力モード]で暗号鍵(キー)を設定できない場合は、下記の変換表を参考に指示された暗号鍵(キー)に対応する記号や英数字で入力してください。
たとえば、16進数入力で「4153434949」(10桁)を設定している場合、ASCII文字では、「ASCII」(5文字)になります。

ASCII文字		!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
16進数	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f
ASCII文字	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
16進数	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f
ASCII文字	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16進数	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f
ASCII文字	P	Q	R	S	T	U	V	W	X	Y	Z	[	¥	]	^	_
16進数	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f
ASCII文字	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
16進数	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f
ASCII文字	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	
16進数	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	

不正アクセス防止のアドバイス
本製品に設定する暗号鍵(WEPキー)は、容易に推測されないものにしてください。
数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた複雑なものにし、さらに定期的に暗号鍵を変更されることをおすすめします。

キーインデックスについて
本製品には、キーインデックスの設定はありませんが、「1」に相当します。
※FWA無線LAN端末側で、[キーインデックス]の設定を「1」以外で使用している場合は、[キーインデックス]を「1」に変更して、そのテキストボックスに本製品と同じ暗号鍵(キー)を設定してください。

1. [WEP RC4]暗号化を設定するには(つづき)

無線設定 > 仮想AP

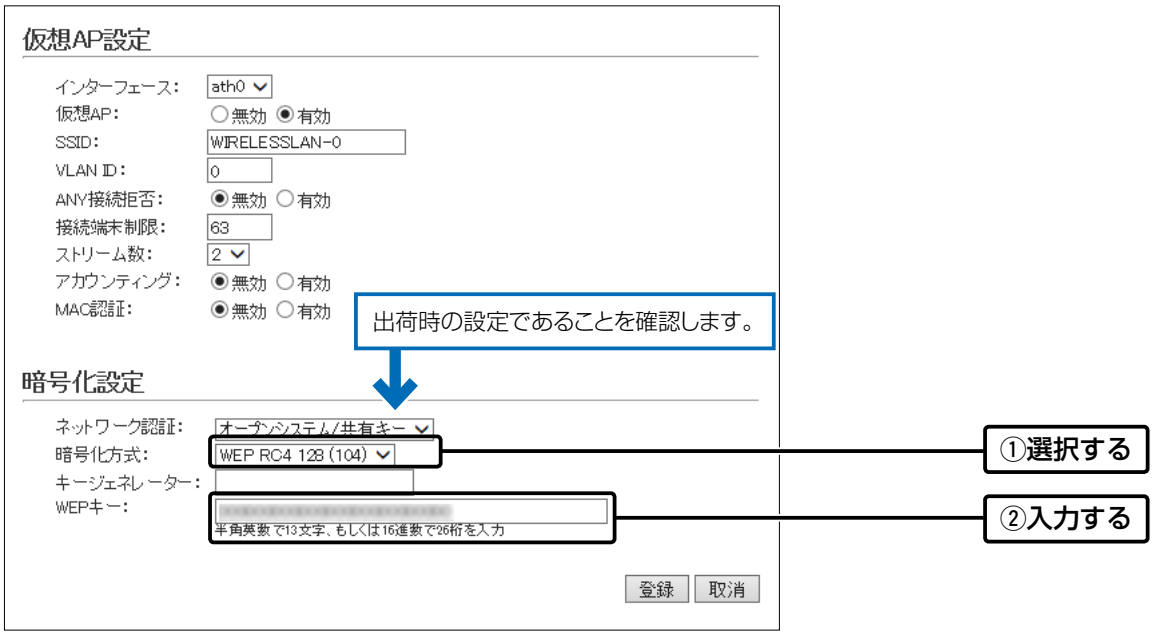
■ 16進数で暗号鍵(キー)を入力するには

仮想AP「ath0」を設定する場合を例に説明します。

ネットワーク認証 :「オープンシステム/共有キー」(出荷時の設定)
暗号化方式 :「WEP RC4 128(104)」ビット
WEPキー :「0~9」、および「a ~f(またはA ~F)」を使用して26桁を入力

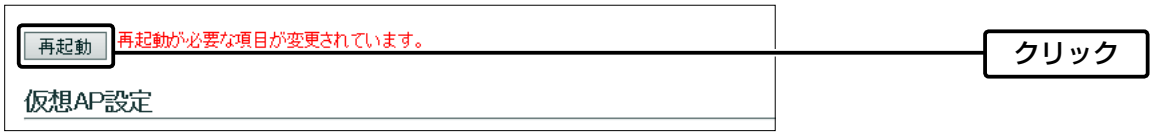
1 「無線設定」メニュー、「仮想AP」の順にクリックします。

2 [暗号化方式]欄で「WEP RC4 128(104)」を選択し、26桁の暗号鍵(キー)を[WEPキー]欄に入力します。



3 〈登録〉をクリックします。

4 〈再起動〉をクリックします。



※表示される画面にしたがって、本製品を再起動します。

5 再起動完了後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

1. [WEP RC4]暗号化を設定するには(つづき)

無線設定 > 仮想AP

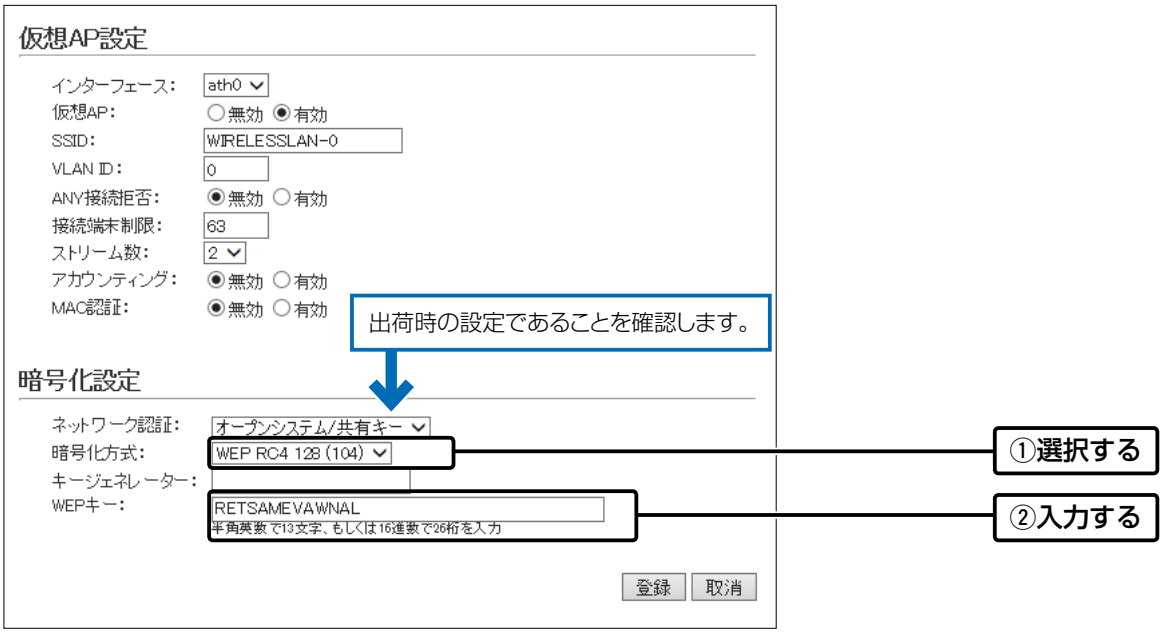
■ ASCII文字で暗号鍵(キー)を入力するには

仮想APの「ath0」を設定する場合を例に説明します。

ネットワーク認証 :「オープンシステム/共有キー」(出荷時の設定)
暗号化方式 :「WEP RC4 128(104)」ビット
WEPキー : 13文字を入力(例:RETSAMEVAWNAL)

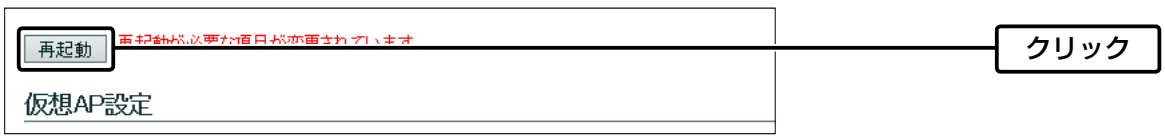
1 「無線設定」メニュー、「仮想AP」の順にクリックします。

2 [暗号化方式]欄で「WEP RC4 128(104)」を選択し、13文字の暗号鍵(キー)を[WEPキー]欄に入力します。



3 〈登録〉をクリックします。

4 〈再起動〉をクリックします。



※表示される画面にしたがって、本製品を再起動します。

5 再起動完了後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

1. [WEP RC4]暗号化を設定するには(つづき)

無線設定 > 仮想AP

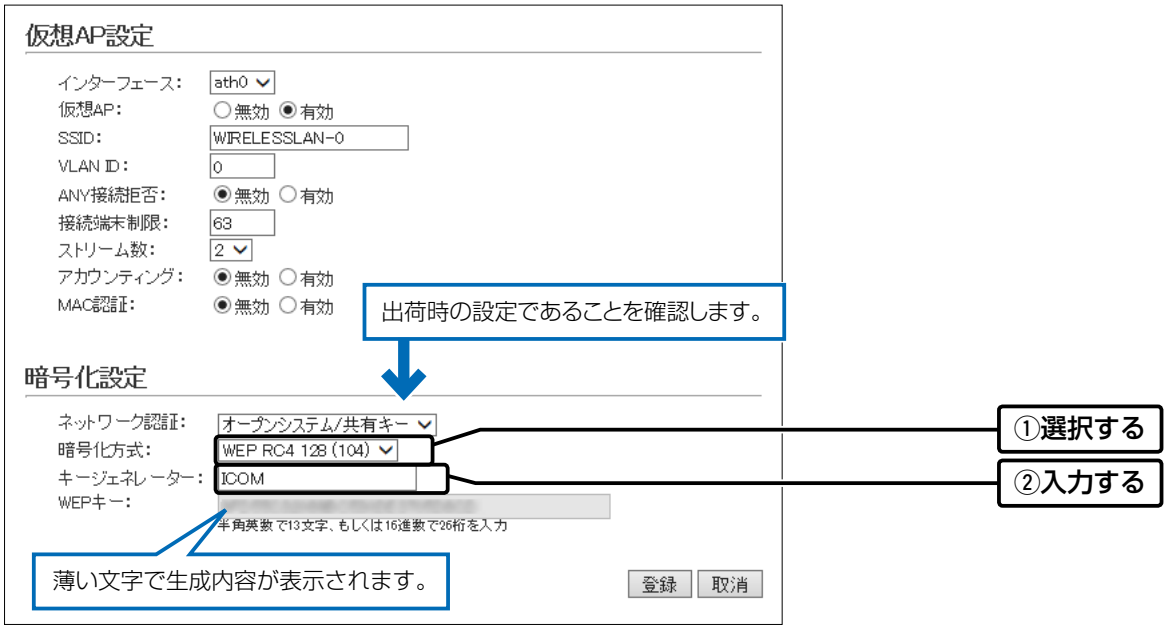
■ 暗号鍵(キー)を生成するには

仮想APの「ath0」を設定する場合を例に説明します。

ネットワーク認証　：「オープンシステム/共有キー」(出荷時の設定)
暗号化方式　　：「WEP RC4 128(104)」ビット
キージェネレーター：任意の文字列(半角英数字31文字以内)を入力(例:ICOM)

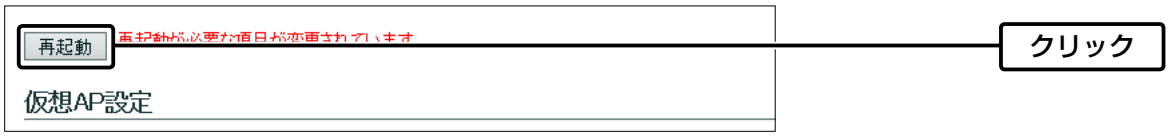
1 「無線設定」メニュー、「仮想AP」の順にクリックします。

2 [暗号化方式]欄で「WEP RC4 128(104)」を選択し、任意の文字列を[キージェネレーター]欄に入力します。(例：ICOM)



3 〈登録〉をクリックします。

4 〈再起動〉をクリックします。



※表示される画面にしたがって、本製品を再起動します。

5 再起動完了後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

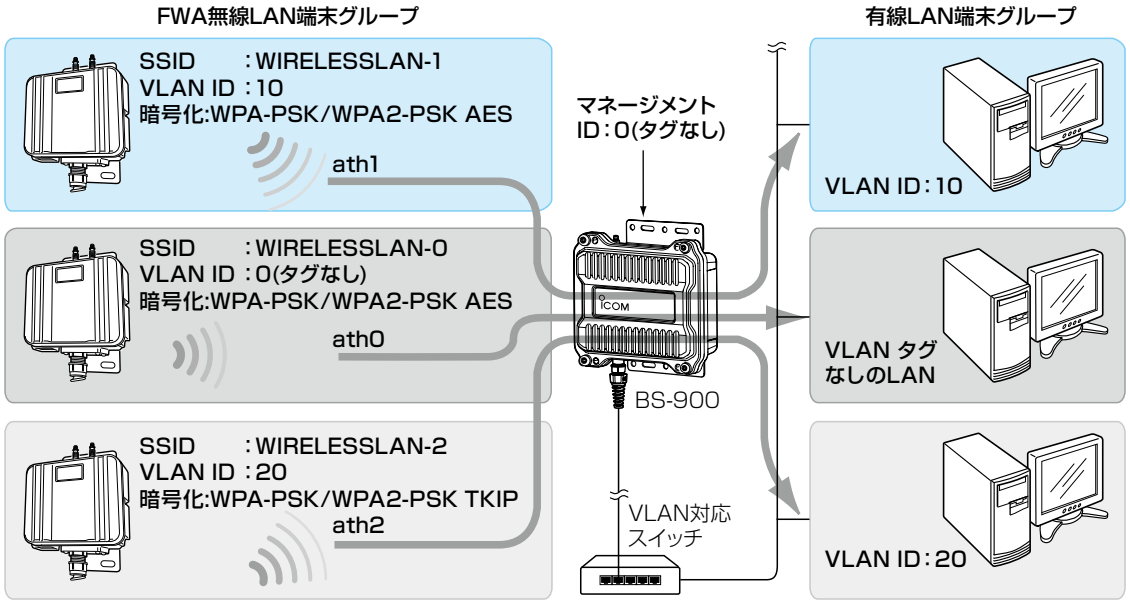
キージェネレーターについて
◎[キージェネレーター]は、弊社以外の機器と互換性はありません。
◎任意の文字列を入力すると、暗号鍵(キー)をテキストボックスに自動生成できます。
◎生成される桁数、および文字数は、選択する[暗号化方式]によって異なります。

株式会社エクセリ　東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5　URL : https : //www.exseli.com/

2. 仮想AP機能を使用するには

■ 仮想AP機能について

本製品1台で、条件(SSID/暗号化方式/VLAN ID)の異なるFWA無線LAN端末グループを複数構成できます。
※下記の図は、「ath0」～「ath2」を異なるFWA無線LAN端末グループの仮想APとして使用する例です。
設定例については、6-7ページ～6-8ページをご覧ください。



※図では、本製品のアンテナを省略しています。

◎仮想APを使用して、最大8グループの無線ネットワークを構築できます。
◎複数の仮想AP機能を使用する場合、同じ[SSID]を設定できません。
◎各仮想APのFWA無線LAN端末グループに、VLAN ID(0～4094)を設定できます。
◎出荷時、本製品の[マネージメントID]が「0」(タグなし)に設定されていますので、VLAN IDが設定されたネットワークからは、本製品の設定画面にアクセスできません。
◎各仮想APの通信レートを、「レート」画面で設定できます。
ベーシックレートを設定した場合、FWA無線LAN端末側が、その速度を使用できることが条件となります。
たとえば、ベーシックレートを設定したレートで通信できないFWA無線LAN端末は、本製品に接続できません。
※設定したレートにより、接続が不安定になることがありますので、特に問題がない場合は、出荷時の設定でご使用ください。

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

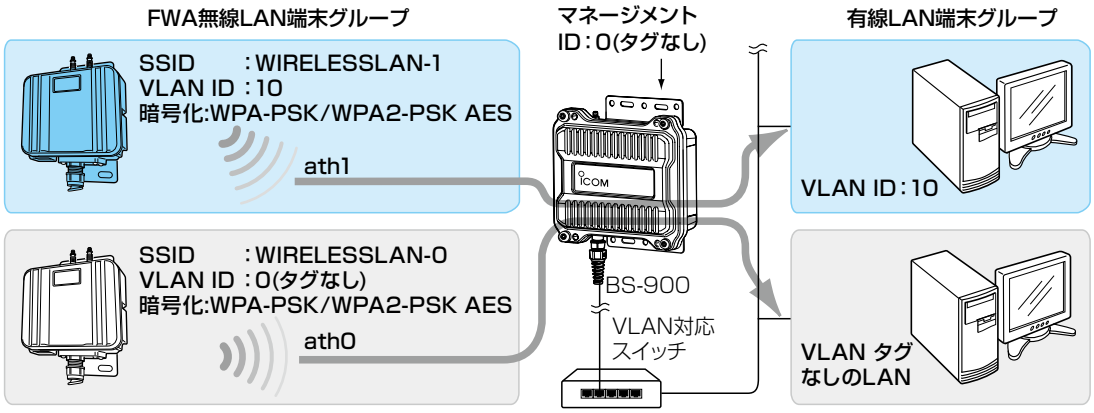
2. 仮想AP機能を使用するには(つづき)

無線設定 > 仮想AP

■ 仮想AP機能を設定するには

次の条件で、図の■色で示す仮想AP(ath1)を設定する場合を例に説明します。

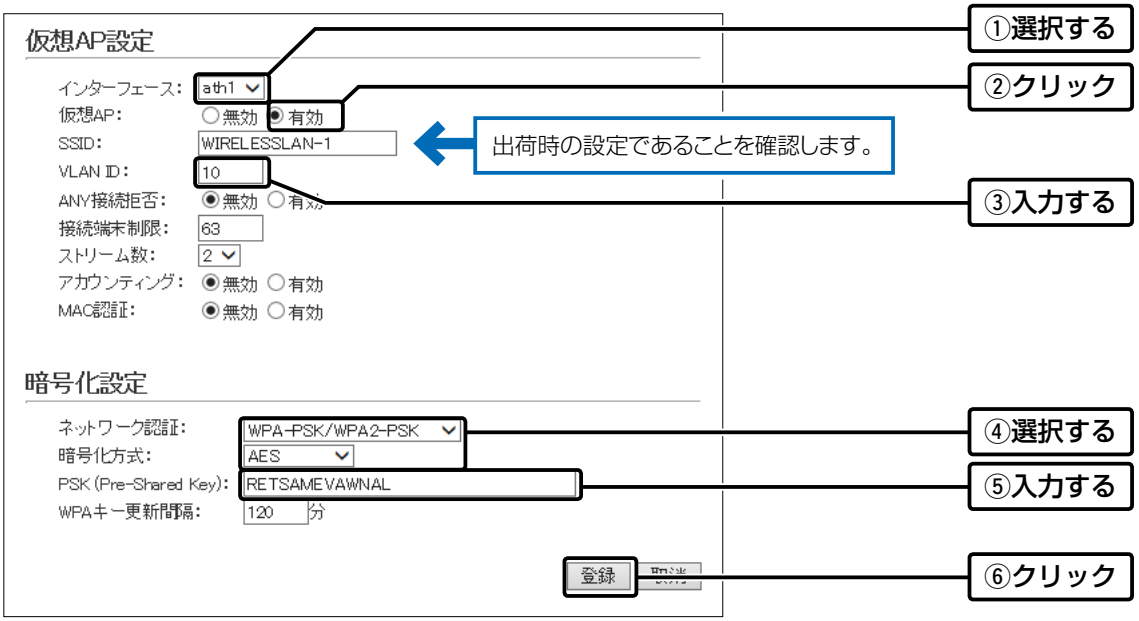
[仮想AP設定]項目	インターフェース	:「ath1」
	仮想AP	:「有効」
	SSID	:「WIRELESSLAN-1」(出荷時の設定)
	VLAN ID	:「10」
[暗号化設定]項目	ネットワーク認証	:「WPA-PSK/WPA2-PSK」
	暗号化方式	:「AES」
	PSK(Pre-Shared Key)	:「RETSAMEVAWNAL」



※仮想AP「ath0」は、設定されているものとします。
※使用条件については、「仮想AP機能を使用するには」をご覧ください。(P.6-6)

1 「無線設定」メニュー、「仮想AP」の順にクリックします。

2 [インターフェース]欄で「ath1」を選択し、上記の設定例にしたがって設定します。



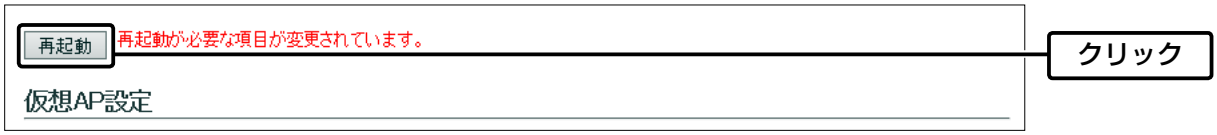
(次ページにつづく)

2. 仮想AP機能を使用するには

無線設定 > 仮想AP

■ 仮想AP機能を設定するには(つづき)

3 〈再起動〉をクリックします。



※表示される画面にしたがって、本製品を再起動します。

4 再起動完了後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

3. MACアドレスフィルタリングを設定するには

無線設定 > MACアドレスフィルタリング

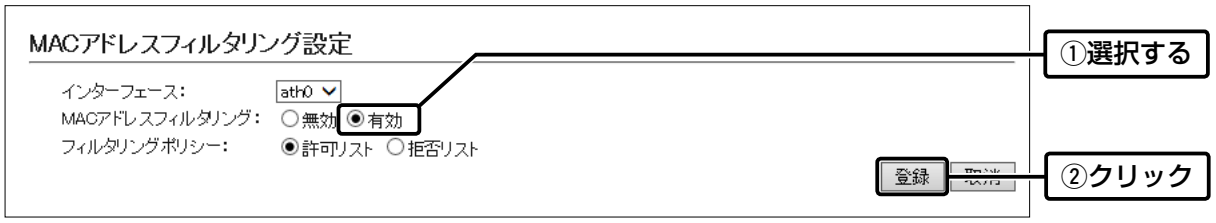
仮想AP(ath0～ath7)ごとに、本製品への接続を許可する、または拒否するFWA無線LAN端末を登録できます。

※仮想APごとに、最大1024台分のMACアドレスを登録できます。

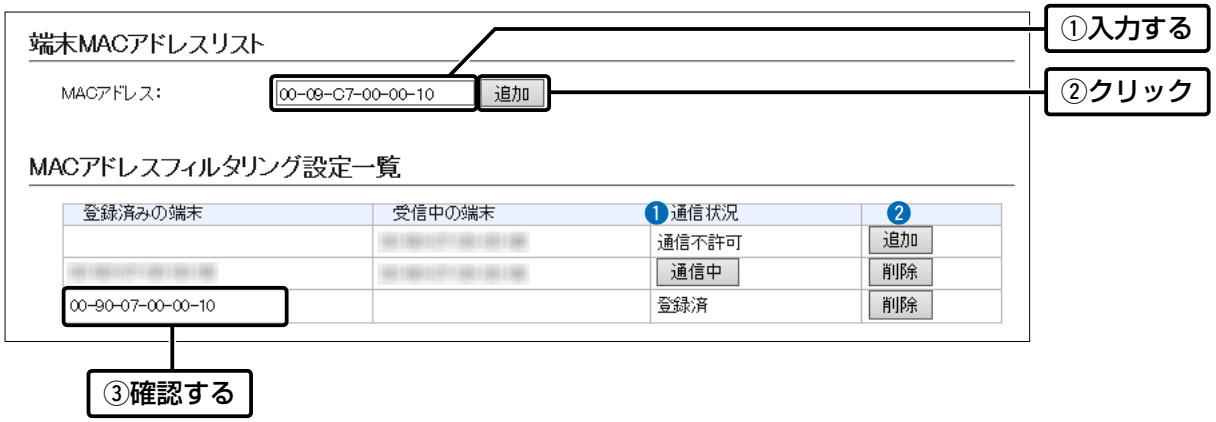
※仮想AP(例:ath0)を例に、接続を許可するFWA無線LAN端末の登録を説明します。

1 「無線設定」メニュー、「MACアドレスフィルタリング」の順にクリックします。

2 [MACアドレスフィルタリング]欄で「有効」を選択し、〈登録〉をクリックします。



3 接続を許可するFWA無線LAN端末のMACアドレスを入力し、〈追加〉をクリックします。



❶通信状況 …… 本製品との無線通信状況を表示します。

〈通信中〉 ：本製品と無線通信中のとき、〈通信中〉とボタンで表示します。

※〈通信中〉をクリックすると、無線通信状態(別画面)で表示します。

「通信不許可」：本製品により無線通信が拒否されているときの表示です。

「登録済」 ：MACアドレスが登録済みで、無線通信をしていないときの表示です。

❷〈追加〉/〈削除〉 …… 表示されているFWA無線LAN端末のMACアドレスをリストに追加、またはリストから削除するボタンです。

4. アカウンティング設定について

通信するFWA無線LAN端末のネットワーク利用状況(接続、切断、MACアドレスなど)を収集してアカウンティングサーバーに送信するときに設定します。

※使用するためには、アカウンティングサーバーの設定が必要です。
※仮想APごとに個別の設定を使用するか、またはすべての仮想APで共通設定を使用するかは、「仮想AP」画面で選択できます。
※共通設定を使用するときは、「認証サーバー」画面でアカウンティングサーバーを設定します。

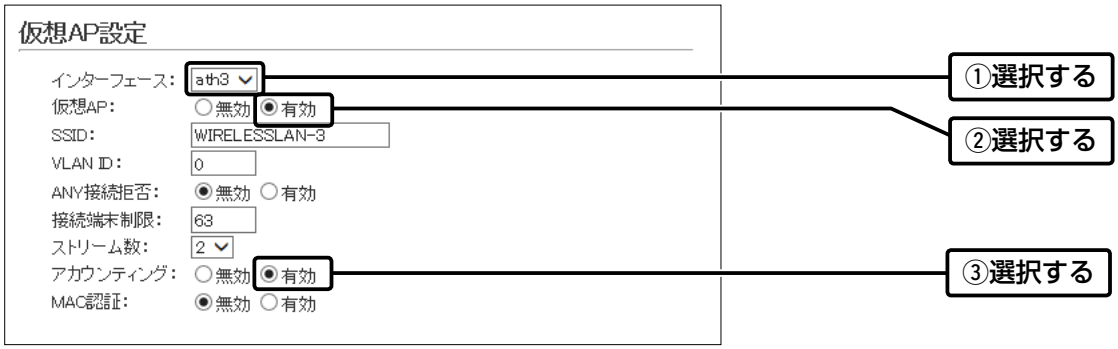
無線設定 > 仮想AP

■ 仮想APごとに個別設定するときは

仮想AP「ath3」で個別設定する場合を例に説明します。

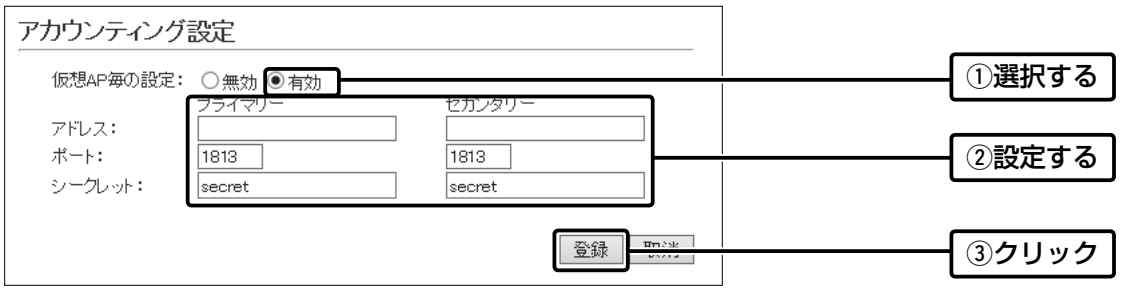
1 「無線設定」メニュー、「仮想AP」の順にクリックします。

2 個別設定をする仮想APの[アカウンティング]欄で「有効」を選択します。(出荷時の設定：無効)

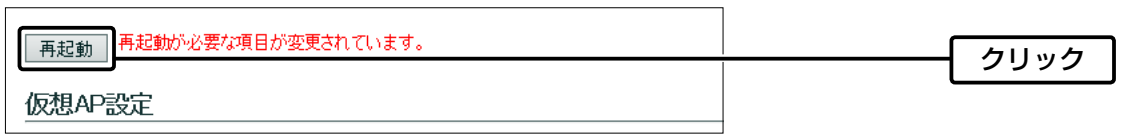


3 [仮想AP毎の設定]欄で「有効」を選択し、対象となるアカウンティングサーバーについて設定します。

※ご使用になるシステムによっては、出荷時の設定値とポート番号が異なることがありますのでご確認ください。
※[シークレット]欄は、アカウンティングサーバーに設定された値と同じ設定にします。



4 〈再起動〉をクリックします。



※表示される画面にしたがって、本製品を再起動します。

5 再起動完了後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

4. アカウンティング設定について(つづき)

無線設定 > 認証サーバー

無線設定 > 仮想AP

■ 共通設定するときは

共通設定する場合を例に説明します。

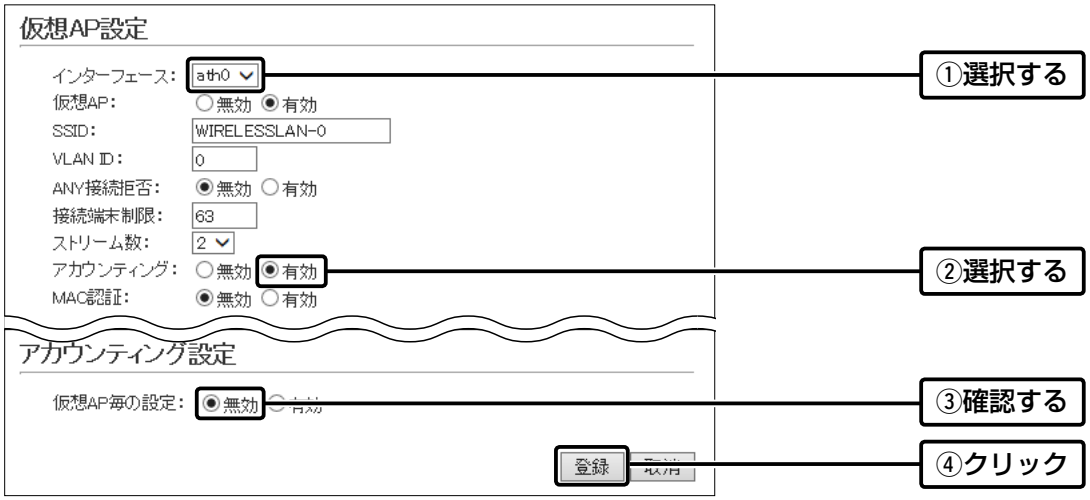
1 「無線設定」メニュー、「認証サーバー」の順にクリックします。

2 対象となるアカウンティングサーバーについて設定します。

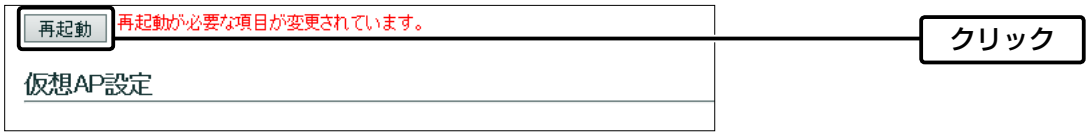
※ご使用になるシステムによっては、出荷時の設定値とポート番号が異なることがありますのでご確認ください。
※[シークレット]欄は、アカウンティングサーバーに設定された値と同じ設定にします。

3 「無線設定」メニュー、「仮想AP」の順にクリックします。

4 共通設定をする仮想APの[アカウンティング]欄で「有効」を選択します。(出荷時の設定:無効)



5 〈再起動〉をクリックします。



※表示される画面にしたがって、本製品を再起動します。

6 再起動完了後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

5. MAC認証サーバー(RADIUS)設定について

FWA無線LAN端末のMACアドレスをRADIUSサーバーで認証するときに設定します。

※使用するためには、RADIUSサーバーの設定が必要です。
※仮想APごとに個別の設定を使用するか、またはすべての仮想APで共通設定を使用するかは、「仮想AP」画面で選択できます。
※共通設定を使用するときは、「認証サーバー」画面でRADIUSサーバーを設定します。
※MAC認証機能では、任意のネットワーク認証と暗号化方式を組み合わせて使用できます。
※FWA無線LAN端末のMACアドレスは、事前にRADIUSサーバーに登録する必要があります。
MACアドレスが「00-AB-12-CD-34-EF」の場合は、ユーザー名/パスワードは「00ab12cd34ef」(半角英数字(小文字))になります。

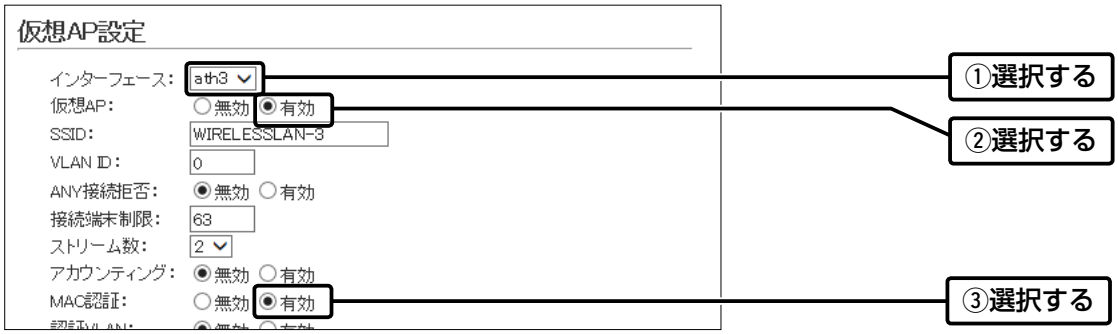
無線設定 > 仮想AP

■ 仮想APごとに個別設定するときは

仮想AP「ath3」で個別設定する場合を例に説明します。

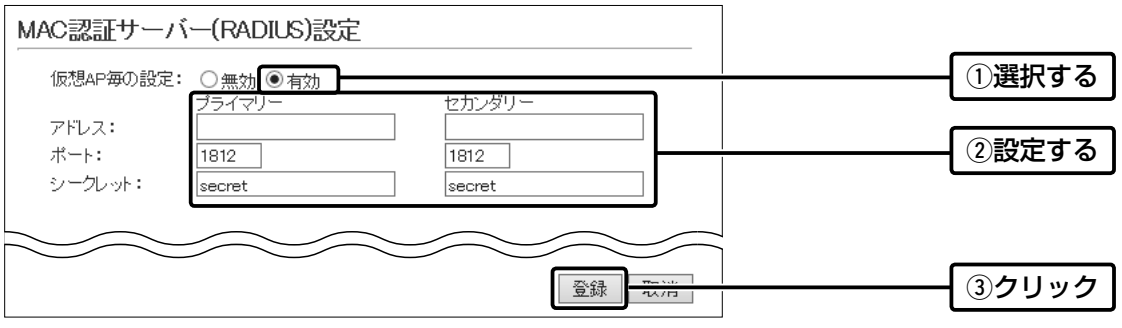
1 「無線設定」メニュー、「仮想AP」の順にクリックします。

2 個別設定をする仮想APの[MAC認証]欄で「有効」を選択します。(出荷時の設定:無効)

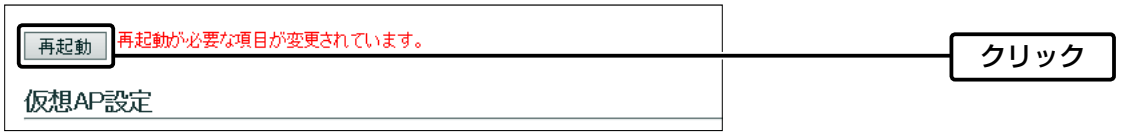


3 [仮想AP毎の設定]欄で「有効」を選択し、対象となるRADIUSサーバーについて設定します。

※ご使用になるシステムによっては、出荷時の設定値とポート番号が異なることがありますのでご確認ください。
※[シークレット]欄は、RADIUSサーバーに設定された値と同じ設定にします。



4 〈再起動〉をクリックします。



※表示される画面にしたがって、本製品を再起動します。

5 再起動完了後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

5. MAC認証サーバー(RADIUS)設定について(つづき)

無線設定 > 認証サーバー

無線設定 > 仮想AP

■ 共通設定するときは

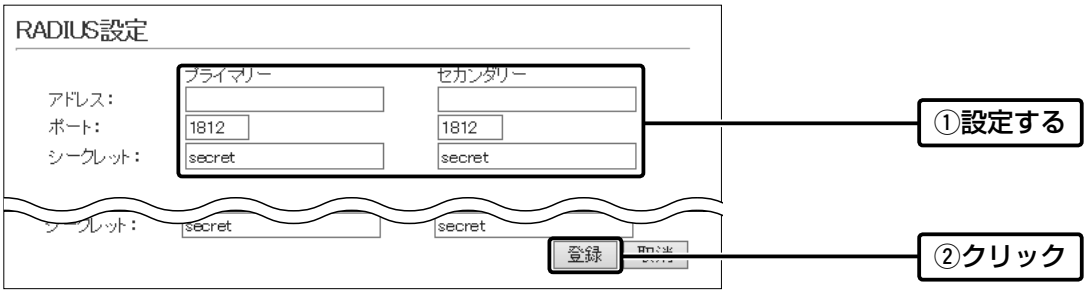
共通設定する場合を例に説明します。

1 「無線設定」メニュー、「認証サーバー」の順にクリックします。

2 対象となるRADIUSサーバーについて設定します。

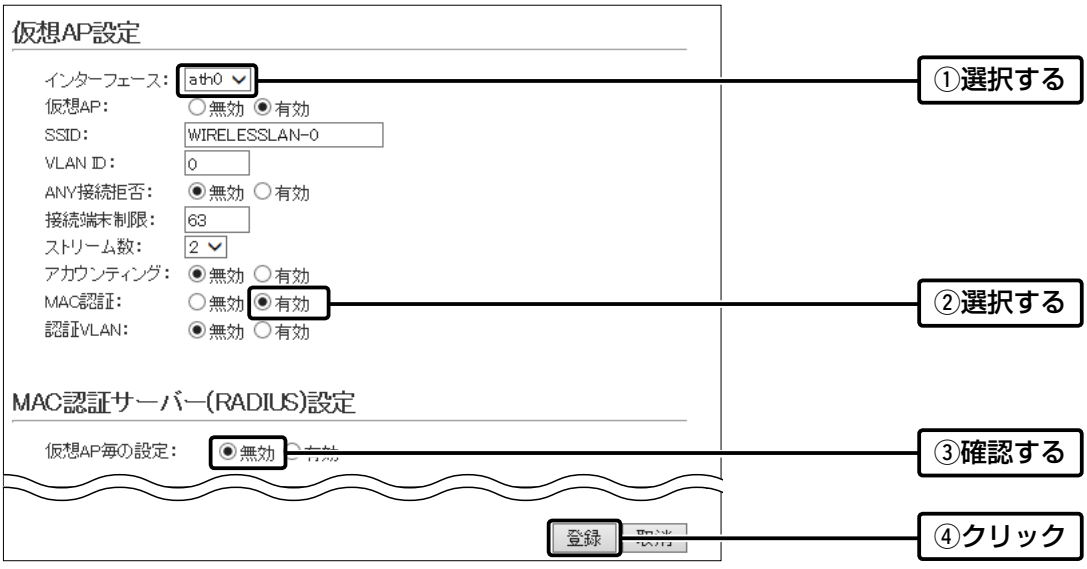
※ご使用になるシステムによっては、出荷時の設定値とポート番号が異なることがありますのでご確認ください。

※[シークレット]欄は、RADIUSサーバーに設定された値と同じ設定にします。

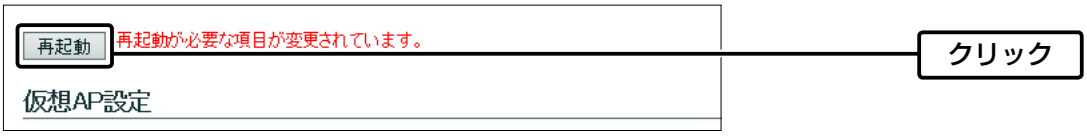


3 「無線設定」メニュー、「仮想AP」の順にクリックします。

4 共通設定をする仮想APの[MAC認証]欄で「有効」を選択します。(出荷時の設定：無効)



5 〈再起動〉をクリックします。



※表示される画面にしたがって、本製品を再起動します。

6 再起動完了後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

6. RADIUS設定について

ネットワーク認証(WPA/WPA2/IEEE802.1X)を利用して、RADIUSサーバーを使用するときに設定します。

※使用するためには、RADIUSサーバーの設定が必要です。
※仮想APごとに個別の設定を使用するか、またはすべての仮想APで共通設定を使用するかは、「仮想AP」画面で選択できます。
※共通設定を使用するときは、「認証サーバー」画面でRADIUSサーバーを設定します。
※EAP認証の対応については、ご使用になるRADIUSサーバーやFWA無線LAN端末の説明書をご覧ください。

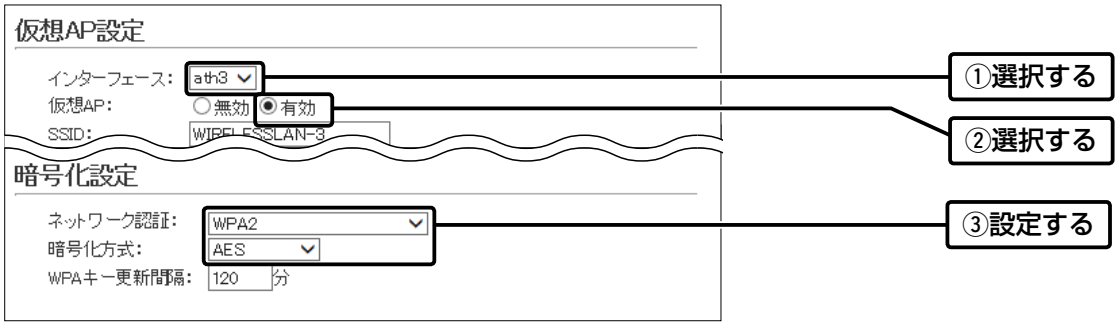
無線設定 > 仮想AP

■ 仮想APごとに個別設定するときは

仮想AP「ath3」で個別設定する場合を例に説明します。

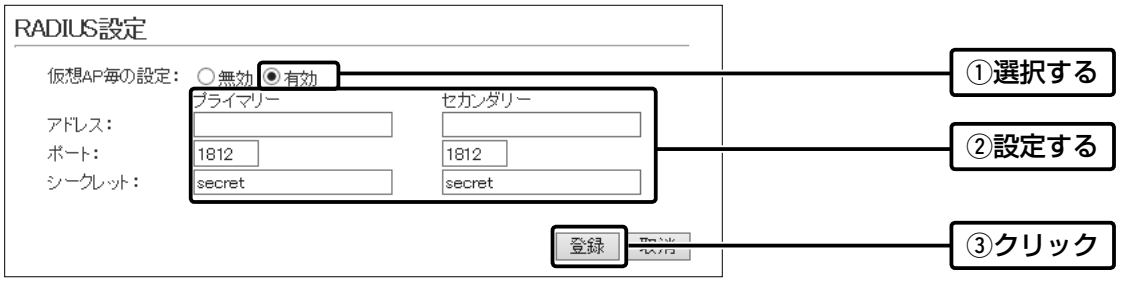
1 「無線設定」メニュー、「仮想AP」の順にクリックします。

2 個別設定をする仮想APでネットワーク認証と暗号化方式を設定します。(例：WPA2認証)

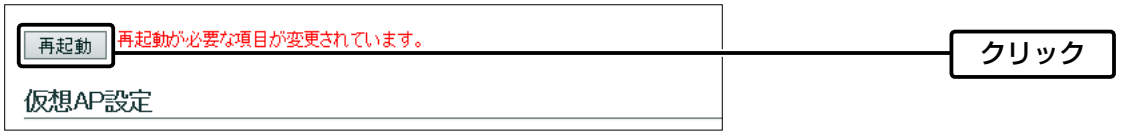


3 [仮想AP毎の設定]欄で「有効」を選択し、対象となるRADIUSサーバーについて設定します。

※ご使用になるシステムによっては、出荷時の設定値とポート番号が異なることがありますのでご確認ください。
※[シークレット]欄は、RADIUSサーバーに設定された値と同じ設定にします。



4 〈再起動〉をクリックします。



※表示される画面にしたがって、本製品を再起動します。

5 再起動完了後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

6. RADIUS設定について(つづき)

無線設定 > 認証サーバー

無線設定 > 仮想AP

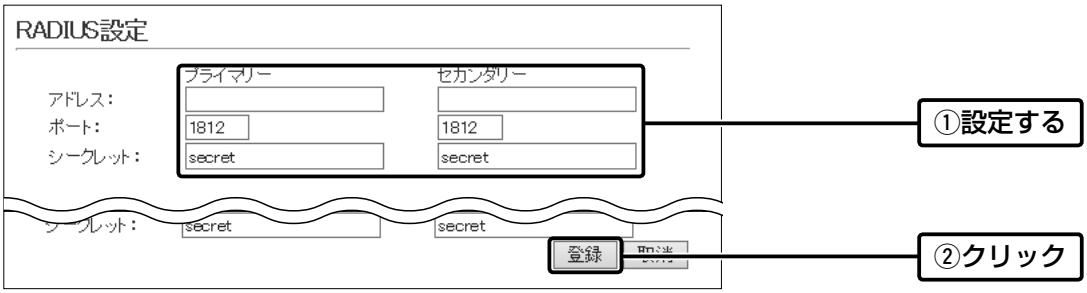
■ 共通設定するときは

共通設定する場合を例に説明します。

1 「無線設定」メニュー、「認証サーバー」の順にクリックします。

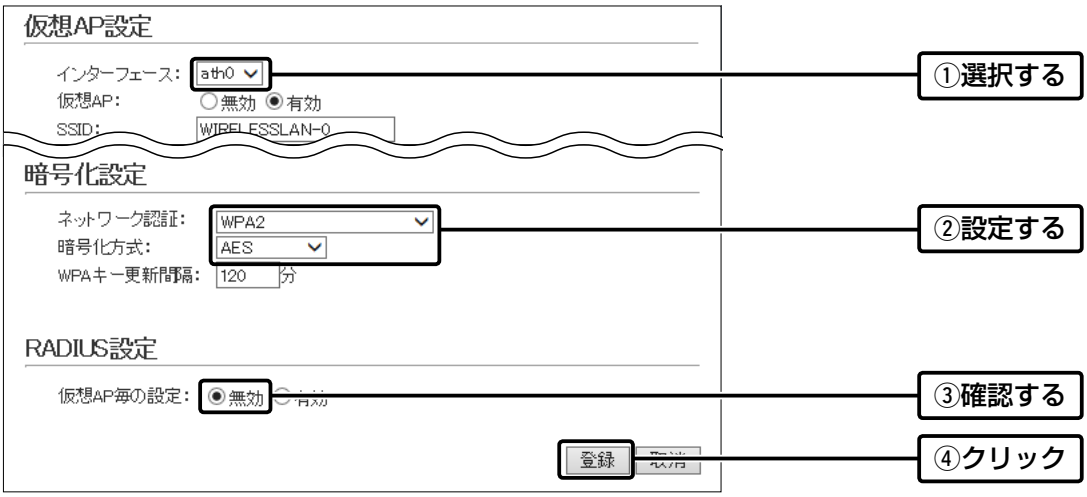
2 対象となるRADIUSサーバーについて設定します。

※ご使用になるシステムによっては、出荷時の設定値とポート番号が異なることがありますのでご確認ください。
※[シークレット]欄は、RADIUSサーバーに設定された値と同じ設定にします。

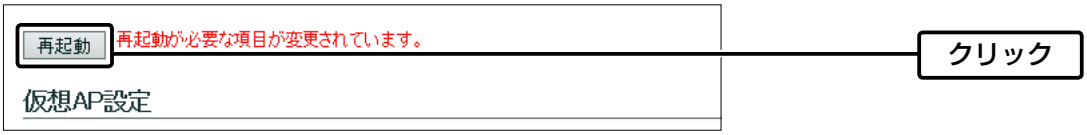


3 「無線設定」メニュー、「仮想AP」の順にクリックします。

4 共通設定をする仮想APでネットワーク認証と暗号化方式を設定します。(例:WPA2認証)



5 〈再起動〉をクリックします。



※表示される画面にしたがって、本製品を再起動します。

6 再起動完了後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

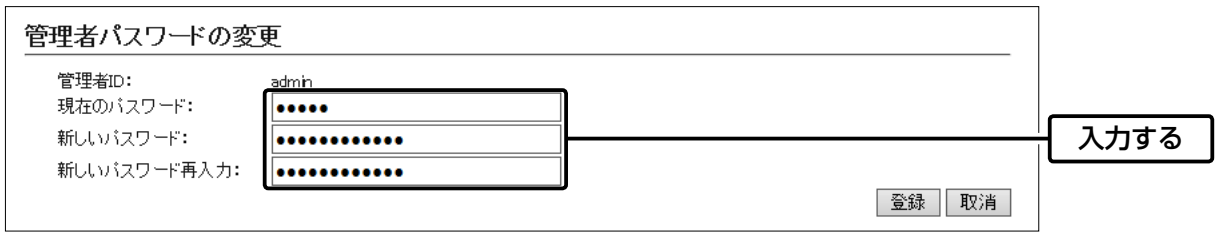
7. 設定画面へのアクセスを制限するには

出荷時、本製品の設定画面には、[管理者ID(admin)]と[パスワード(admin)]でアクセスできます。
パスワードを設定することで、管理者以外がWWWブラウザーから本製品の設定を変更できないようにします。

管理 > 管理者

1 「管理」メニュー、「管理者」の順にクリックします。
「管理者」画面が表示されます。

2 [現在のパスワード]、[新しいパスワード]、[新しいパスワード再入力]欄に、大文字/小文字の区別に注意して、任意の英数字/記号(半角31文字以内)で入力します。
[新しいパスワード]、[新しいパスワード再入力]欄に入力した文字は、すべて＊(アスタリスク)、または●(黒丸)で表示されます。



3 〈登録〉をクリックします。
※[ユーザー名]と[パスワード]を求める画面が表示されたときに、変更した新しい管理者パスワードを入力します。

不正アクセス防止のアドバイス
本製品に設定するすべてのパスワードは、容易に推測されないものにしてください。
数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた長く複雑なものにし、さらに定期的にパスワードを変更されることをおすすめします。

ご注意
パスワードをお忘れの場合、本製品の全設定を初期化する以外に方法がありません。
初期化の方法は、お買い上げの販売店、または弊社サポートセンターにお問い合わせください。

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

8. 無線ブリッジ接続をするときは

■ 無線ブリッジ接続機能を使用するには

SE-900FW(FWA無線LAN端末)のブリッジ接続機能を有効に設定して、SE-900FWのMACアドレスを本製品に登録すると、無線ブリッジ接続に切り替わります。

※接続するFWA無線LAN端末により、接続条件が異なります。
SE-570FW、SE-570FWDの場合は、端末側の接続端末MACアドレスを自動に設定し、端末のMACアドレスを本製品に登録すると、無線ブリッジ接続に切り替わります。

無線ブリッジ接続について

◎本製品の「ath0」に接続した端末だけ、無線ブリッジ接続できます。

◎SE-900FWの画面でブリッジ接続機能を有効にしていても、本製品の「ブリッジ接続」画面で、端末のMACアドレスが登録されていない場合は、通常の接続になります。
※SE-570FW、SE-570FWDは、接続端末MACアドレスを自動以外に設定するとブリッジ接続が無効になります。

◎無線ブリッジ接続の端末に対して、MACアドレスフィルタリング、端末台数制限機能は適用されます。

◎無線ブリッジ接続の端末に対して、VLANを透過します。
※仮想APのVLAN機能は適用しません。

◎無線ブリッジ接続の端末に対して、認証VLAN機能、ARP代理応答機能は動作しません。

8. 無線ブリッジ接続をするときは(つづき)

無線設定 > ブリッジ接続 (BS-900側)

無線設定 > 接続 (SE-900FW側)

■ FWA無線LAN端末と無線ブリッジ接続する

次の条件で、SE-900FWと無線ブリッジ接続する場合を例に説明します。

※使用条件については、「無線ブリッジ接続について」をご覧ください。(P.6-17)

※無線接続するためのSSIDや暗号化設定などの設定は完了しているものとします。

BS-900側(FWA基地局)の設定

帯域幅	:20MHz
チャンネル	:184CH(4920MHz)
インターフェース	:ath0
SSID	:WIRELESSLAN-0
ネットワーク認証	:WPA-PSK/WPA2-PSK
暗号化方式	:TKIP/AES
PSK(Pre-Shared Key)	:wirelessmaster
MACアドレス	:00-90-C7-00-00-02 (端末側のMACアドレス)

SE-900FW側(FWA無線LAN端末)の設定

SSID	:WIRELESSLAN-0
接続端末MACアドレス	:00-90-C7-00-00-02
帯域幅	:20MHz
ブリッジ接続	:有効
ネットワーク認証	:WPA-PSK/WPA2-PSK
暗号化方式	:TKIP/AES
PSK(Pre-Shared Key)	:wirelessmaster

※図では、外部アンテナを省略しています。

※数値は、設定例です。

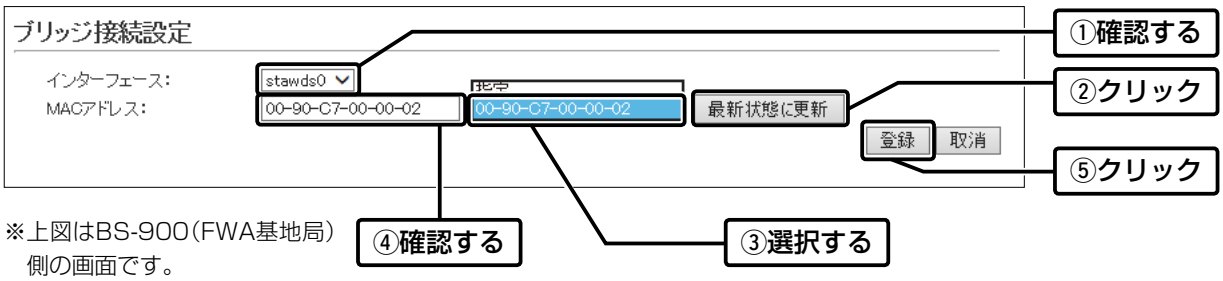
①BS-900(FWA基地局)側に端末のMACアドレスを登録する

1 BS-900(FWA基地局)側の設定画面にアクセスします。

2 「無線設定」メニュー、「ブリッジ接続」の順にクリックします。

3 設定条件にしたがって、下記のように自動検出された対向するSE-900FW(FWA無線LAN端末)側のMACアドレス(例:00-90-C7-00-00-02)を登録します。

※自動検出されないときは、相手の[接続端末MACアドレス]を[MACアドレス]欄に直接入力します。



※上図はBS-900(FWA基地局)側の画面です。

8. 無線ブリッジ接続をするときは

無線設定 > ブリッジ接続（BS-900側）

無線設定 > 接続（SE-900FW側）

■ FWA基地局と無線ブリッジ接続する

①BS-900（FWA基地局）側に端末のMACアドレスを登録する（つづき）

4 [ブリッジ接続設定一覧]欄の内容を確認して、〈再起動〉をクリックします。

※表示される画面にしたがって、再起動します。

8. 無線ブリッジ接続をするときは

無線設定 > ブリッジ接続（BS-900側）

無線設定 > 接続（SE-900FW側）

■ FWA基地局と無線ブリッジ接続する（つづき）

②SE-900FW（FWA無線LAN端末）側で無線ブリッジ接続を確認する

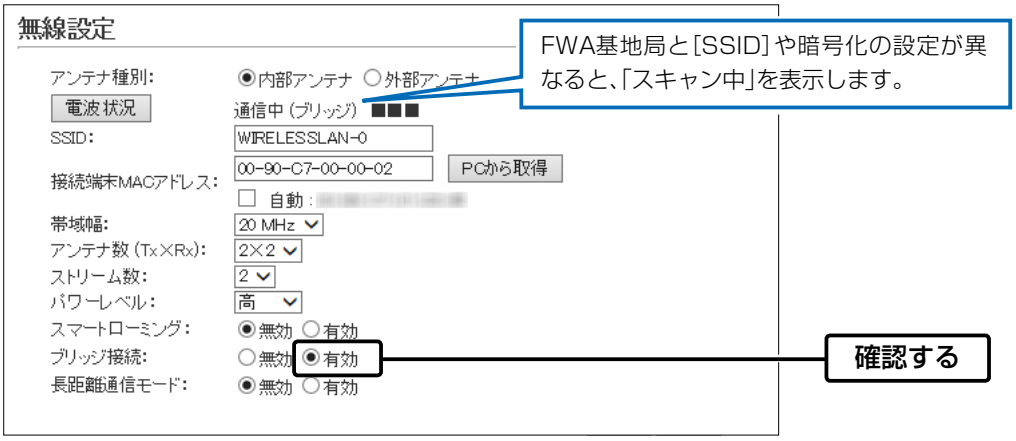
1 SE-900FW（FWA無線LAN端末）側の設定画面にアクセスします。

2 「無線設定」メニュー、「接続」の順にクリックします。

3 [ブリッジ接続]が「有効」に設定されていることを確認します。

「通信中（ブリッジ）■■■」が画面に表示されます。

※設定変更後など、WWWブラウザーの表示を更新するまで、「スキャン中」と表示される場合があります。

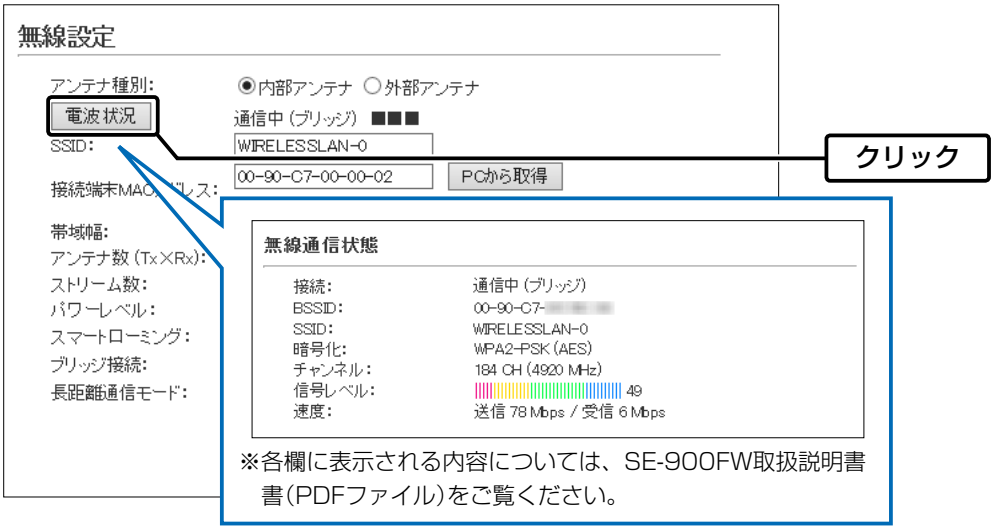


4 〈電波状況〉をクリックします。

[無線通信状態]項目（別画面）を表示します。

※別画面に表示される内容は約2秒ごとに更新されます。

連続でモニターすると、ネットワークに負荷がかかりますので、確認が完了したら、別画面は閉じてください。



保守について

第 7 章

この章では、
本製品の設定内容の保存、ファームウェアのバージョンアップをする手順について説明しています。

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

7 保守について

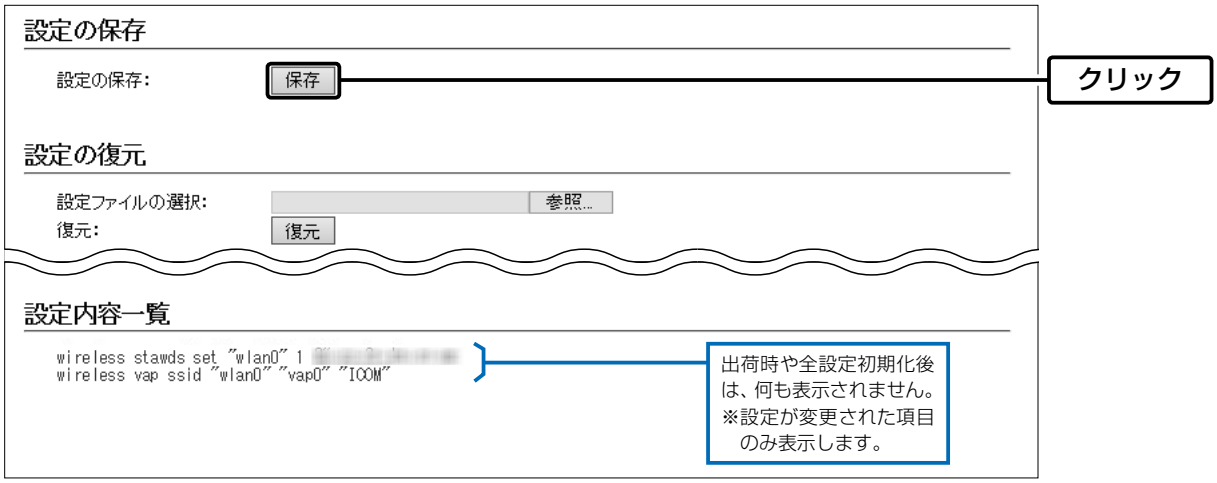
1. 設定内容の確認または保存

管理 > 設定の保存/復元

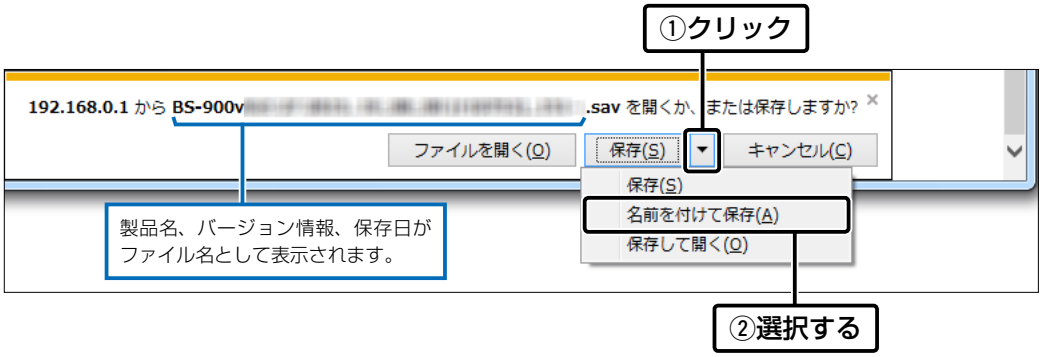
本製品の設定画面で変更された内容を確認して、その内容を設定ファイル(拡張子:sav)としてパソコンに保存できます。
※保存した設定ファイル(拡張子:sav)は、本製品以外の製品では使用できません。
※設定を保存しておくと、誤って設定内容が失われたときなどに利用できます。

1 「管理」メニュー、「設定の保存/復元」の順にクリックします。
「設定の保存/復元」画面が表示されます。

2 [設定の保存]項目の〈保存〉をクリックします。
ファイルの確認画面(別画面)が表示されます。



3 〈保存(S)〉の「▼」をクリックして、「名前を付けて保存(A)」を選択します。
「名前を付けて保存」画面(別画面)が表示されます。



4 保存する場所を選択して、〈保存(S)〉をクリックします。
選択した場所に設定ファイル(拡張子:sav)が保存されます。

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

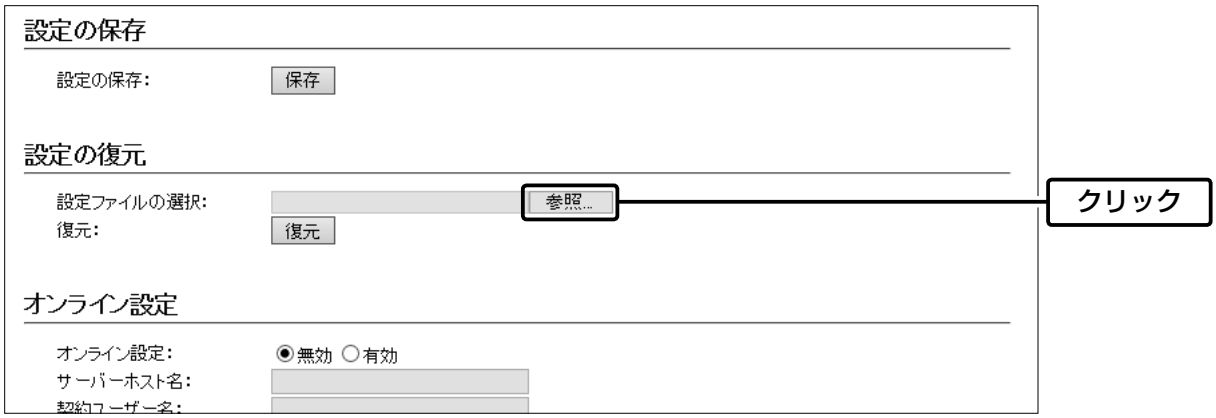
2. 保存された設定の書き込み(復元)

管理 > 設定の保存/復元

本製品の設定画面からパソコンに保存した設定ファイル(P.7-2)を本製品に書き込む手順を説明します。

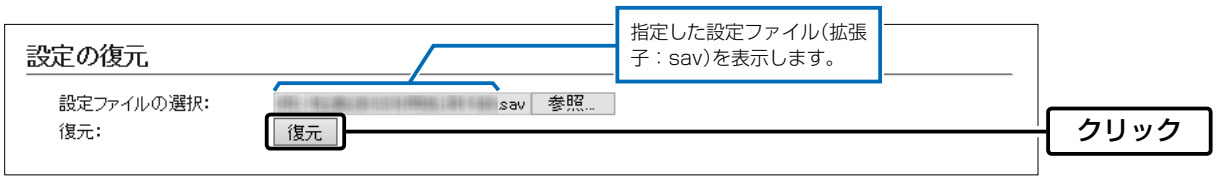
1 「管理」メニュー、「設定の保存/復元」の順にクリックします。
「設定の保存/復元」画面が表示されます。

2 [設定の復元]項目の〈参照...〉をクリックします。
「アップロードするファイルの選択」画面(別画面)が表示されます。



3 「アップロードするファイルの選択」画面(別画面)から、設定ファイル(拡張子:sav)を指定して、〈開く(O)〉をクリックします。
[設定ファイルの選択]欄のテキストボックスに、書き込む設定ファイルが表示されます。

4 〈復元〉をクリックします。
「設定データを復元しています。」が表示され、設定を復元するために本製品が再起動します。



設定ファイルについてのご注意
本製品以外の機器への書き込み、改変による障害、および書き込みに伴う本製品の故障、誤動作、不具合、破損、データの消失、あるいは停電などの外部要因により通信、通話などの機会を失ったために生じる損害や逸失利益、または第三者からのいかなる請求についても当社は一切その責任を負いかねますのであらかじめご了承ください。

3. 設定を出荷時の状態に戻すには

ネットワーク構成を変更するときなど、本製品の設定をはじめからやりなおすときや、既存の設定データをすべて消去したいときなど、設定内容を出荷時の状態に戻せます。
そのときの状況に応じて、次の3とおりの方法があります。

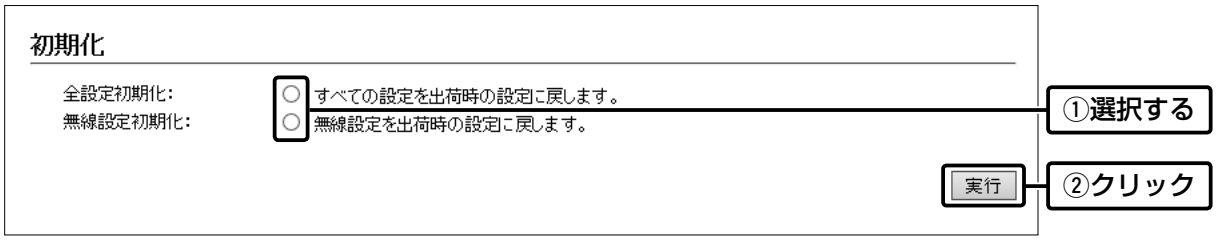
管理 > 初期化

■ 設定画面を使用する

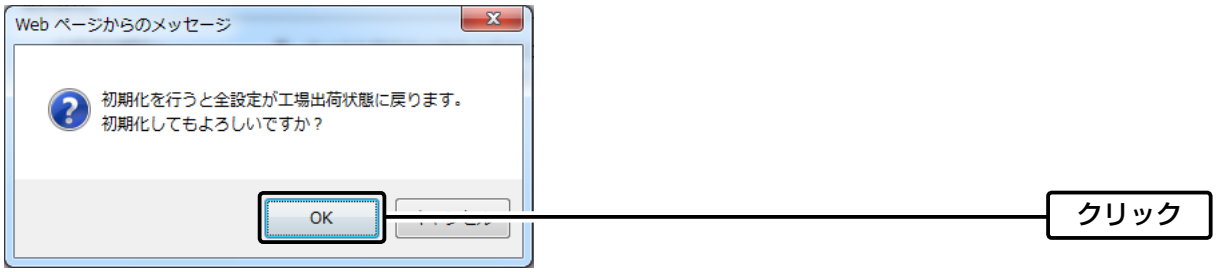
本製品に設定されたIPアドレスがわかっていて、そのIPアドレスで設定画面にアクセスできるときに使用します。

1 「管理」メニュー、「初期化」の順にクリックします。

2 初期化の条件を選択して、〈実行〉をクリックします。



3 〈OK〉をクリックします。
出荷時の状態に戻すために、本製品が再起動します。



4 再起動完了後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

■ Telnetを使用する

本製品に設定されたIPアドレスがわかっていて、Telnetで本製品に接続できるときに使用します。（P.8-4）
※Telnetから、init allコマンドを実行すると、すべての設定項目が出荷時の状態になります。

■ [CONSOLE]ポートを使用する

本製品に設定されたIPアドレスが不明な場合など、設定画面にアクセスできないときに使用します。
※[CONSOLE]ポートと接続したターミナルソフトウェアから、init allコマンドを実行すると、すべての設定項目が出荷時の状態になります。
※ターミナルソフトウェアを使用して接続する方法は、8-5ページ、または別紙のBS-900設定ガイドをご覧ください。

3. 設定を出荷時の状態に戻すには(つづき)

初期化の条件について

◎全設定初期化を選択した場合(init allコマンド)

本製品に設定されたすべての内容を出荷時の状態に戻します。
初期化すると、本製品のIPアドレスは「192.168.0.1」(出荷時の設定)になります。
初期化実行後、本製品にアクセスできなくなった場合は、パソコンのIPアドレスを変更してください。

◎無線設定初期化を選択した場合(init wlanコマンド)

「無線設定」メニューで設定した内容だけを出荷時の状態に戻します。
初期化すると、本製品の[SSID]は「WIRELESSLAN-0」、暗号化設定は「なし」(出荷時の設定)になります。
初期化実行後、FWA無線LAN端末に設定されたSSIDや暗号化設定が本製品と異なったときは、アクセスできなくなりますので、必要に応じて、「無線設定」メニュー、およびFWA無線LAN端末の設定を変更してください。

株式会社エクセリ　東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5　URL : https : //www.exseli.com/

4. ファームウェアをバージョンアップする

本製品の設定画面からファームウェアをバージョンアップできます。

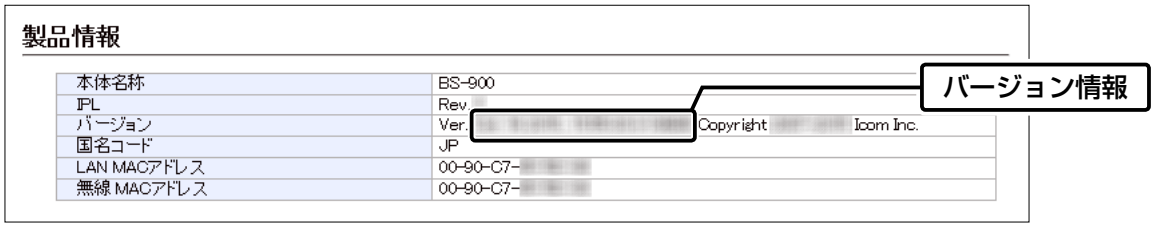
Ⓐ ファイルを指定して更新する(P.7-7)
オンラインバージョンアップできない環境では、あらかじめ弊社ホームページからダウンロードしたファームウェアを指定して、手動でバージョンアップできます。

Ⓑ オンラインバージョンアップ(P.7-8)
インターネットから本製品のファームウェアを最新の状態に自動更新できます。

TOP

■ ファームウェアについて

ファームウェアは、本製品を動作させるために、出荷時から本製品のフラッシュメモリーに書き込まれているプログラムです。
このプログラムは、機能の拡張や改良のため、バージョンアップをすることがあります。
バージョンアップの作業をする前に、本製品の設定画面にアクセスして、「TOP」画面に表示されるバージョン情報を確認してください。
バージョンアップをすると、機能の追加など、本製品を最良の状態にできます。



■ バージョンアップについてのご注意

◎ ファームウェアの更新中は、絶対に本製品の電源を切らないでください。
更新中に電源を切ると、データの消失や故障の原因になります。

◎ ご使用のパソコンでファイアウォール機能が動作していると、バージョンアップできないことがあります。
バージョンアップできない場合は、ファイアウォール機能を無効にしてください。

◆ バージョンアップの結果については、自己責任の範囲となります。
次に示す内容をよくお読みになってから、弊社ホームページ http://www.icom.co.jp/ より提供される本製品のアップデート用ファームウェアファイルをご使用ください。
本製品以外の機器への書き込み、改変による障害、および書き込みに伴う本製品の故障、誤動作、不具合、破損、データの消失、あるいは停電などの外部要因により通信、通話などの機会を失ったために生じる損害や逸失利益、または第三者からのいかなる請求についても当社は一切その責任を負いかねますのであらかじめご了承ください。

4. ファームウェアをバージョンアップする(つづき)

管理 > ファームウェアの更新

Ⓐ ファイルを指定して更新する

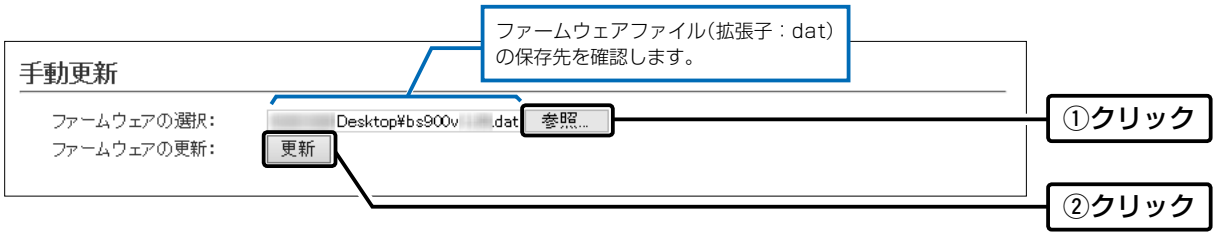
バージョンアップの前に、現在の設定内容を保存されることをおすすめします。(P.7-2)

※ バージョンアップ後、既存の設定内容が初期化されるファームウェアファイルがありますので、ダウンロードするときは、弊社ホームページに記載の内容をご確認ください。

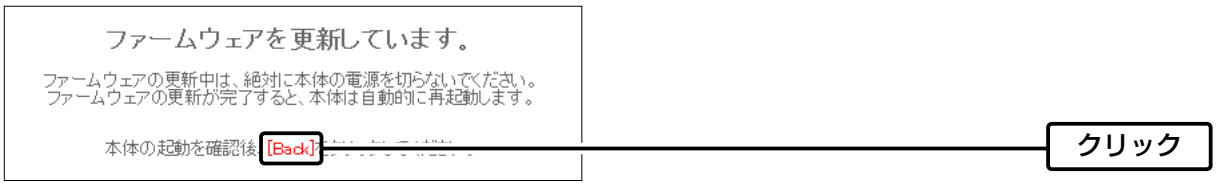
※ 日常、管理者以外の端末からバージョンアップできないように、設定画面へのアクセス制限の設定(P.6-16)をおすすめします。

1 「管理」メニュー、「ファームウェアの更新」の順にクリックします。
「ファームウェアの更新」画面が表示されます。

2 下記のように、弊社ホームページよりダウンロードして解凍したファームウェアファイル(拡張子：dat)の保存先を指定して、更新します。



3 更新完了後、[Back]と表示された文字の上にマウスポインターを移動してクリックすると、設定画面に戻ります。
設定画面に戻らないときは、ファームウェアの更新中ですので、しばらくしてから再度クリックしてください。
(接続するパソコンや本製品の電源は、絶対に切らないでください。)



ご注意
[Back]の操作(手順3)で設定画面に戻るようになるまで、ご使用のパソコンや本製品の電源を絶対に切らないでください。
途中で電源を切ると、データの消失や誤動作の原因になります。
※出荷時の設定内容に戻るような注意書きがあるバージョンアップ用ファームウェアの場合は、上図の[Back]をクリックしても設定画面に戻れないことがあります。
その場合は、接続するパソコンのIPアドレスを「例：192.168.0.100」に設定してから、本製品の設定画面「192.168.0.1」(出荷時の設定)にアクセスしなおしてください。

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

4. ファームウェアをバージョンアップする(つづき)

管理 > ファームウェアの更新

Ⓑ オンラインバージョンアップ

下記の手順で、最新のファームウェアを確認後、[MODE]ランプが●橙点灯しているときは、本製品のファームウェアをオンラインでバージョンアップできます。

※ ファームウェアの確認には、インターネットへの接続環境と本製品へのDNS設定、デフォルトゲートウェイの設定が必要です。

※ バージョンアップの前に、現在の設定内容を保存されることをおすすめします。(P.7-2)

1 「管理」メニュー、「ファームウェアの更新」の順にクリックします。

「ファームウェアの更新」画面が表示されます。

2 [ファームウェアの確認]欄の〈確認〉をクリックして、表示される更新内容を確認します。

※「新しいファームウェアはありません。」が表示され、[MODE]ランプが消灯のときは、バージョンアップは必要ありません。

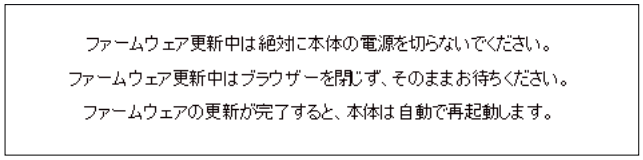
3 〈ファームウェアを更新〉をクリックします。

弊社のアップデート管理サーバーにアクセスを開始します。

※バージョンアップにより、既存の設定内容が初期化されるファームウェアファイルがありますので、バージョンアップする前に、表示される更新内容をご確認ください。

4 更新が完了するまで、そのまま数分程度お待ちください。

弊社のアップデート管理サーバーに接続すると、ファームウェアのダウンロードを開始し、更新後は、自動的に再起動します。



【ファームウェアの自動更新機能について】

◎ファームウェアに重要な更新が含まれる場合、自動更新機能が動作し、アップデート管理サーバーから本製品のファームウェアを更新します。運用中にファームウェアを更新して本製品が再起動しますので、自動更新を望まない場合は「無効」に設定してください。(P.5-25) (出荷時の設定:有効)

◎ファームウェアに重要な更新が含まれていない場合は、[MODE]ランプが橙点灯します。

※オンラインファーム検知時、ファームウェアは自動的に更新されません。

※ご都合のよいときに、ファームウェアを手動で更新してください。(上記参照)

ご参考に

第 8 章

この章では、
困ったときの対処法、仕様などを説明しています。

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

8 ご参考に

1. 困ったときは

下記のような現象は、故障ではありませんので、修理を依頼される前にもう一度お調べください。
それでも異常があるときは、弊社サポートセンターまでお問い合わせください。

[PWR]ランプ/[LAN]ランプが点灯しない

●LANケーブルが本製品と正しく接続されていない
→ SA-4(別売品)、または[IEEE802.3af]対応のHUBとの接続を確認する

●[IEEE802.3af]対応のHUB、またはSA-4(別売品)の電源が入っていない
→ 電源の接続を確認する

[📶]ランプが点灯しない

●本製品の無線LAN機能を無効に設定している
→ 本製品の無線LAN機能を有効に設定する

[📶]ランプが緑点灯しない

●FWA無線LAN端末と本製品の帯域幅が異なっている
→ ご使用になるFWA無線LAN端末の帯域幅を確認する

●通信終了後、無線通信しない状態が4分以上つづいた
→ 本製品に再度アクセスして点灯することを確認する

●[SSID](またはESSID)の設定が異なっている
→ 本製品とFWA無線LAN端末の[SSID]を確認する

●暗号化認証モードが異なるタイプである
→ FWA無線LAN端末、または本製品の認証モードを同じ設定にする

●MACアドレスフィルタリングを使用している
→ FWA無線LAN端末のMACアドレスを本製品に登録する

●本製品のANY接続拒否機能を有効に設定している
→ 本製品のANY接続拒否機能を無効に設定する

[📶]ランプが緑点灯しているが通信できない

暗号化セキュリティーの設定が異なっている
→ 本製品とFWA無線LAN端末の暗号化セキュリティーの設定を確認する

54Mbpsを超える速度で通信できない

●FWA無線LAN端末が対応していない
→ 対応しているFWA無線LAN端末を使用する

●「AES」以外の暗号化セキュリティーを使用している
→ 54Mbpsを超える速度で通信する場合は、暗号化設定を「なし」、または「AES」に設定する

本製品の設定画面が正しく表示されない

●WWWブラウザーのJavaScript機能、およびCookieを無効に設定している
→ JavaScript機能、およびCookieを有効に設定する

●Microsoft Internet Explorer8.0以前を使用している
→ Microsoft Internet Explorer9.0以降を使用する

1. 困ったときは(つづき)

本製品の設定画面にアクセスできない

●パソコンのIPアドレスを設定していない
→ 本製品の出荷時や全設定初期化時は、パソコンのIPアドレスを固定IPアドレスに設定する

●IPアドレスのネットワーク部が、本製品とパソコンで異なっている
→ パソコンに設定されたIPアドレスのネットワーク部を本製品と同じにする

●ご使用のWWWブラウザーにプロキシサーバーが設定されている
→ Internet Explorerの「ツール(T)」メニューから「インターネットオプション(O)」、[接続]タブ、〈LANの設定(L)〉の順に操作して、[設定を自動的に検出する(A)]や[LANにプロキシサーバーを使用する(X)]にチェックマークが入っていないことを確認する

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

2. Telnetで接続するには

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 7の場合

お使いいただくときは、「コントロールパネル」→「プログラム」→「Windows の機能の有効化または無効化」から、[Telnetクライアント]を有効にしてから、下記の手順で操作してください。

【設定のしかた】

① Windowsを起動します。
② [スタート](ロゴボタン)から[プログラムとファイルの検索]を選択します。
名前欄に「telnet.exe」と入力し、[Enter]キーを押します。
※Windows Vistaをご使用の場合は、[スタート](ロゴボタン)から[検索の開始]を選択します。
※Windows 8.1の場合は、[スタート](ロゴボタン)から[ファイル名を指定して実行]を選択します。
③ Telnetクライアントが起動しますので、下記のように入力します。
Microsoft Telnet>open 本製品のIPアドレス(入力例：open 192.168.0.1)
④ 下記を入力して[Enter]キーを押すと、ログインできます。
login ：admin
password：admin
※出荷時や全設定初期化時のpasswordは、adminです。(P.5-2)
⑤ ログインメッセージ(BS-900 #)が表示されます。

■ Telnetコマンドについて

使用できるTelnetコマンドの表示方法と、コマンド入力について説明します。

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つづいて[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ときは、ヘルプコマンドにつづいて、コマンド名を入力するとコマンドのヘルプが表示されます。
例) help save （saveコマンドのヘルプを表示する場合）

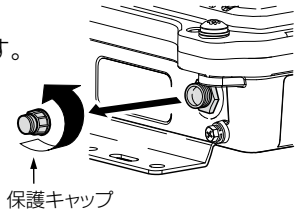
コマンド名の補完…… コマンド名を先頭から数文字入力し[Tab]キーを押すと、コマンド名が補完されます。
入力した文字につづくコマンドが1つしかないときは、コマンド名を最後まで補完します。
例) v[Tab]→ver
複数のコマンドがあるときは、コマンドの候補を表示します。
例) res[Tab]→reset restart

2. Telnetで接続するには(つづき)

■ [CONSOLE]ポートを使用するときは

本製品の[CONSOLE]ポートとパソコンのCOMポートを、設定用ケーブル(シリアル通信用)で接続すると、ターミナルソフトウェアから設定できます。
※設定用ケーブルは販売していませんので、必要な場合は、お買い上げの販売店にお問い合わせください。
※使用するときは、パソコンのCOMポートを下記の値に設定します。

① 電源供給に使用しているSA-4(別売品)、または[IEEE802.3af]対応のHUBの電源をはずします。
② [CONSOLE]ポートの保護キャップ(右図)をはずします。
③ 本製品の[CONSOLE]ポートとパソコンの[COM]ポートを設定用ケーブルで接続します。
④ 本製品に電源を供給し、パソコンからターミナルソフトウェアを起動します。
⑤ 下記を設定して、[ENTER]キーを押します。


保護キャップ

[接続方法]の選択 : 設定用ケーブルを接続しているCOMポートの番号を指定
通信速度 : 115200(ビット/秒)
データビット : 8
パリティー : なし
ストップビット : 1
フロー制御 : なし

⑥ BS-900 #と表示されたことを確認します。
※アクセス後に[Tab]キーを押すと、本製品で使用できるコマンドの一覧が表示されます。

3. 設定画面の構成について

本製品の全設定を初期化したとき、WWWブラウザーに表示される画面構成です。

設定メニュー	設定画面	設定項目
TOP	TOP	製品情報
		ネットワーク情報
情報表示	ネットワーク情報	インターフェースリスト
		Ethernetポート接続情報
		無線LAN
		ブリッジ接続
		DHCPリース情報
	SYSLOG	SYSLOG
	無線設定情報一覧　無線	アクセスポイント情報
		仮想AP一覧
	無線設定情報一覧　端末情報	端末情報
		端末情報(ブリッジ接続)
	統計情報	メモリー使用率
		トラフィック統計
ネットワーク設定	LAN側IP	本体名称
		VLAN設定
		IPアドレス設定
	DHCPサーバー	DHCPサーバー設定
		静的DHCPサーバー設定
		静的DHCPサーバー設定一覧
	ルーティング	IP経路情報
		スタティックルーティング設定
		スタティックルーティング設定一覧
	パケットフィルター	パケットフィルター設定
		パケットフィルター設定一覧
無線設定	無線LAN	無線LAN設定
	仮想AP	仮想AP設定
		暗号化設定
	認証サーバー	RADIUS設定
		アカウンティング設定
	MACアドレスフィルタリング	MACアドレスフィルタリング設定
		端末MACアドレスリスト
		MACアドレスフィルタリング設定一覧
	ブリッジ接続	ブリッジ接続設定
		ブリッジ接続設定一覧
	ネットワーク監視	ネットワーク監視設定
	WMM詳細	WMM詳細設定
	レート	レート設定
		仮想AP共通設定
	ARP代理応答	ARP代理応答
		ARPキャッシュ情報

株式会社エクセリ　東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5　URL : https : //www.exseli.com/

3. 設定画面の構成について(つづき)

設定メニュー	設定画面	設定項目
管理	管理者	管理者パスワードの変更
	管理ツール	HTTP/HTTPS設定
		Telnet/SSH設定
	時計	時刻設定
		自動時計設定
	SYSLOG	SYSLOG設定
	SNMP	SNMP設定
	ネットワークテスト	PINGテスト
		経路テスト
	サイトサーベイ	サイトサーベイ
	再起動	再起動
	設定の保存/復元	設定の保存
		設定の復元
		オンライン設定
		設定内容一覧
	初期化	初期化
	ファームウェアの更新	ファームウェア情報
		オンライン更新
		自動更新
		手動更新

4. 設定項目の初期値一覧

本製品の設定画面について、全設定を初期化したときに表示される各項目の初期値です。

■ ネットワーク設定

設定画面/項目	初期値	設定範囲/最大登録数
「LAN側IP」画面		
本体名称	本体名称：BS-900	半角英数字と「-」(31文字以内)
VLAN設定	マネージメントID：0	設定範囲「0～4094」
IPアドレス設定	IPアドレス：192.168.0.1	
	サブネットマスク：255.255.255.0	
	デフォルトゲートウェイ：空白(設定なし)	
	プライマリーDNSサーバー：空白(設定なし)	
	セカンダリーDNSサーバー：空白(設定なし)	
「DHCPサーバー」画面		
DHCPサーバー設定	DHCPサーバー：無効	
	割り当て開始IPアドレス：192.168.0.10	
	割り当て個数：30(個)	設定範囲「0～128」(個)
	サブネットマスク：255.255.255.0	
	リース期間：72(時間)	設定範囲「1～9999」(時間)
	ドメイン名:空白(設定なし)	
	デフォルトゲートウェイ：空白(設定なし)	
	プライマリーDNSサーバー：空白(設定なし)	
	セカンダリーDNSサーバー：空白(設定なし)	
	プライマリーWINSサーバー：空白(設定なし)	
	セカンダリーWINSサーバー：空白(設定なし)	
静的DHCPサーバー	MACアドレス：空白(設定なし)	最大登録数：32
	IPアドレス：空白(設定なし)	
「ルーティング」画面		
スタティックルーティング設定	宛先：空白(設定なし)	最大登録数：32
	サブネットマスク：空白(設定なし)	
	ゲートウェイ：空白(設定なし)	
「パケットフィルター」画面		
パケットフィルター設定	番号：空白(設定なし)	設定範囲「1～64」
	エントリー：無効	
	ログを表示：有効	
	方法：透過	
	インターフェース 送信元インターフェース：すべて	
	インターフェース 宛先インターフェース：すべて	
	Ethernetヘッダー 送信元MACアドレス／マスク：空白(設定なし)	
	Ethernetヘッダー 宛先MACアドレス／マスク：空白(設定なし)	
	Ethernetヘッダー VLAN ID：0～空白(設定なし)	
	Ethernetヘッダー Ethernetタイプ：すべて	

（次ページにつづく）

4. 設定項目の初期値一覧(つづき)

■ 無線設定

設定画面/項目	初期値	設定範囲/最大登録数
「無線LAN」画面		
無線LAN設定	無線UNIT：有効	
	帯域幅：20MHz	
	チャンネル：184CH (4920MHz)	
	パワーレベル：高	
	アンテナ数(Tx×Rx)：2×2	
	DTIM間隔：1	設定範囲「1～50」
	プロテクション：有効	
	長距離通信モード：無効	
「仮想AP」画面(ath0～ath7)		
仮想AP設定	インターフェース：ath0	
	仮想AP：有効(ath0)	
	無効(ath1～ath7)	
	SSID：WIRELESSLAN-0(ath0)	半角英数字32文字以内
	WIRELESSLAN-1(ath1)	
	WIRELESSLAN-2(ath2)	
	WIRELESSLAN-3(ath3)	
	WIRELESSLAN-4(ath4)	
	WIRELESSLAN-5(ath5)	
	WIRELESSLAN-6(ath6)	
	WIRELESSLAN-7(ath7)	
	VLAN ID：0(ath0～ath7)	設定範囲「0～4094」
	ANY接続拒否：無効(ath0～ath7)	
	接続端末制限：63(ath0～ath7)	設定範囲「1～128」
	ストリーム数：2	
	アカウンティング：無効(ath0～ath7)	
	MAC認証：無効	
暗号化設定	ネットワーク認証：オープンシステム/共有キー (ath0～ath7)	
	暗号化方式：なし(ath0～ath7)	
「認証サーバー」画面		
RADIUS設定(プライマリー／セカンダリー)		
	アドレス：空白(設定なし)	
	ポート：1812	設定範囲「1～65535」
	シークレット：secret	半角64文字以内
アカウンティング設定 (プライマリー／セカンダリー)		
	アドレス：空白(設定なし)	
	ポート：1813	設定範囲「1～65535」
	シークレット：secret	半角64文字以内
「MACアドレスフィルタリング」画面(ath0～ath7)		
MACアドレスフィルタリング設定	インターフェース：ath0	
	MACアドレスフィルタリング：無効	
	フィルタリングポリシー：許可リスト	
端末MACアドレスリスト	MACアドレス：空白(設定なし)	最大登録数：1024(※仮想APごとの数)
「ブリッジ接続」画面(stawds0 ～ stawds7)		
ブリッジ接続設定	(設定なし)	

(次ページにつづく)

4. 設定項目の初期値一覧

■ 無線設定(つづき)

設定画面/項目	初期値	設定範囲/最大登録数
「ネットワーク監視」画面(ath0～ath7)		
ネットワーク監視設定	インターフェース：ath0	
	監視対象ホスト1：空白(設定なし)	
	監視対象ホスト2：空白(設定なし)	
	監視対象ホスト3：空白(設定なし)	
	監視対象ホスト4：空白(設定なし)	
	監視間隔：10(秒)	設定範囲「1～120」(秒)
	タイムアウト時間：1(秒)	設定範囲「1～10」(秒)
	失敗回数：3(回)	設定範囲「1～10」(回)
	条件：ひとつ以上のホストが応答なし	
「WMM詳細」画面		
WMM詳細設定	[To Station]/[From Station] CWin min：AC_BK(15)、AC_BE(15)、AC_VI(7)、AC_VO(3)	
	[To Station] CWin max：AC_BK(1023)、AC_BE(63)、AC_VI(15)、AC_VO(7)	
	[From Station] CWin max：AC_BK(1023)、AC_BE(1023)、AC_VI(15)、AC_VO(7)	
	[To Station] AIFSN(1-15)：AC_BK(7)、AC_BE(3)、AC_VI(1)、AC_VO(1)	設定範囲「1～15」
	[From Station] AIFSN(2-15)：AC_BK(7)、AC_BE(3)、AC_VI(2)、AC_VO(2)	設定範囲「2～15」
	[To Station]/[From Station] TXOP(0-255)：AC_BK(0)、AC_BE(0)、AC_VI(94)、AC_VO(47)	設定範囲「0～255」
	[To Station]（✔なし(OFF)） No Ack：AC_BK □、AC_BE □、AC_VI □、AC_VO □	
	[From Station]（✔なし(OFF)） ACM：AC_VI □、AC_VO □	

（次ページにつづく）

4. 設定項目の初期値一覧

■ 無線設定(つづき)

設定画面/項目	初期値	設定範囲/最大登録数
「レート」画面(ath0～ath7)		
レート設定	帯域幅：20/40MHz	
	インターフェース：ath0	
	プリセット：初期値	
	レガシー：	
	6Mbps：ベーシックレート	
	9Mbps：有効	
	12Mbps：ベーシックレート	
	18Mbps：有効	
	24Mbps：ベーシックレート	
	36Mbps：有効	
	48Mbps：有効	
	54Mbps：有効	
	HT-MCS：	
	MCS 0：有効	
	MCS 1：有効	
	MCS 2：有効	
	MCS 3：有効	
	MCS 4：有効	
	MCS 5：有効	
	MCS 6：有効	
	MCS 7：有効	
	MCS 8：有効	
	MCS 9：有効	
	MCS 10：有効	
	MCS 11：有効	
	MCS 12：有効	
	MCS 13：有効	
	MCS 14：有効	
	MCS 15：有効	
	マルチキャスト送信レート	
	マルチキャストレート：6Mbps	
仮想AP共通設定	最低レートの再送制限：無効	
	キックアウト：弱	
「ARP代理応答」画面(ath0～ath7)		
ARP代理応答	インターフェース：ath0	
	ARP代理応答：無効	
	不明なARPの透過：有効	
	ARPエージング時間：0(分)	設定範囲「0～1440」(分)

4. 設定項目の初期値一覧(つづき)

■ 管理

設定画面/項目	初期値	設定範囲/最大登録数
「管理者」画面		
管理者パスワードの変更	管理者ID：admin(変更不可)	
	現在のパスワード：admin(非表示)	
	新しいパスワード：空白(設定なし)	英数字/記号（半角31文字以内）
	新しいパスワード再入力：空白(設定なし)	
「管理ツール」画面		
HTTP/HTTPS設定	HTTP：有効	
	HTTPポート番号：80	
	HTTPS：無効	
	HTTPSポート番号：443	
Telnet/SSH設定	Telnet：有効	
	Telnetポート番号：23	
	SSH：無効	
	SSHバージョン：自動	
	SSH認証方式：自動	
	SSHポート番号：22	
「時計」画面		
時計設定	設定する時刻：パソコンから取得した時刻	
自動時計設定	自動時計設定：無効	
	NTPサーバー1：210.173.160.27	
	NTPサーバー2：210.173.160.57	
	アクセス時間間隔：1(日)	設定範囲「1～99」(日)
「SYSLOG」画面		
SYSLOG設定	DEBUG：無効	
	INFO：有効	
	NOTICE：有効	
	ホストアドレス：空白(設定なし)	
「SNMP」画面		
SNMP設定	SNMP：有効	
	コミュニティーID(GET)：public	
	場所：空白(設定なし)	
	連絡先：空白(設定なし)	
「ネットワークテスト」画面		
PINGテスト	ホスト：空白(設定なし)	
	試行回数：4(回)	
	パケットサイズ：64(バイト)	
	タイムアウト時間：1000(ミリ秒)	
経路テスト	ノード：空白(設定なし)	
	最大ホップ数：16	
	タイムアウト時間：3(秒)	
	DNS名前解決：有効	
「設定の保存/復元」画面		
オンライン設定	オンライン設定：無効	
	サーバーホスト名：空白(設定なし)	
	契約ユーザー名：空白(設定なし)	
	パスワード：空白(設定なし)	
「ファームウェアの更新」画面		
自動更新	自動更新：有効	

5. 機能一覧

■ 無線LAN機能

- ●ブリッジ接続機能
- ●暗号化セキュリティー(WEP RC4、TKIP、AES)
- ●ネットワーク認証
  (オープンシステム、共有キー、IEEE802.1X、WPA、WPA2、WPA-PSK、WPA2-PSK)
- ●MAC認証(RADIUS)
- ●SSID(Service Set IDentifier)
- ●アクセスポイント機能
- ●ローミング機能
- ●ANY接続拒否機能
- ●仮想AP機能
- ●MACアドレスフィルタリング機能
- ●プロテクション機能
- ●パワーレベル調整機能
- ●接続端末制限機能
- ●WMM★(Wi-Fi Multimedia)機能
- ●ARP代理応答
- ●認証サーバー(RADIUS/アカウンティング)
- ●ネットワーク監視機能
- ●ストリーム数切替機能
- ●レート設定機能

■ ネットワーク管理機能

- ●SYSLOG
- ●SNMP(MIB-II)

■ その他

- ●DHCPサーバー機能
- ●静的DHCPサーバー機能
- ●タグVLAN機能
- ●認証VLAN機能
- ●パケットフィルター機能
- ●接続制限機能(管理者ID/パスワード)
- ●内部時計設定
- ●PoE機能
- ●ファームウェアのバージョンアップ
- ●WWWメンテナンス(HTTP/HTTPS)
- ●TELNETメンテナンス(TELNET/SSH)

★ 2016年5月現在、本製品は、Wi-Fiアライアンスの認定を取得していません。

株式会社エクセリ 東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5 URL : https : //www.exseli.com/

6. 設定項目で使用できる文字列について

下表のように、入力できる文字列が設定項目により異なります。

※設定画面のオンラインヘルプで設定項目を確認するときは、設定項目の上にマウスポインターを移動して、「?」が表示されたら、クリックしてください。

■ ネットワーク設定

設定画面	設定項目	設定欄	入力できる文字列	入力できる文字数
LAN側IP	本体名称	本体名称	半角英数字★1/「-」 ※先頭と末尾は半角英数字のみ	31文字以内
DHCPサーバー	DHCPサーバー設定	ドメイン名	半角英数字★1/「.」/「-」 ※先頭と末尾は半角英数字のみ	127文字以内

■ 無線設定

設定画面	設定項目	設定欄	入力できる文字列	入力できる文字数
仮想AP	暗号化設定	WEPキー	ASCII★2、または16進数	6-3ページ参照
		PSK（Pre-Shared Key）	ASCII★2、または16進数	4-17ページ参照

■ 管理

設定画面	設定項目	設定欄	入力できる文字列	入力できる文字数
管理者	管理者パスワードの変更	パスワード	半角英数字/記号	31文字以内
SNMP	SNMP設定	コミュニティーID(GET)	半角英数字/記号 ※「\」/「"」/「'」を除く	31文字以内
ネットワークテスト	PINGテスト	ホスト	半角英数字★1/「.」/「-」 ※先頭と末尾は半角英数字のみ	64文字以内
		ノード	半角英数字★1/「.」/「-」 ※先頭と末尾は半角英数字のみ	64文字以内
設定の保存/復元	オンライン設定	サーバーホスト名	半角英数字★1/「.」/「-」 ※先頭と末尾は半角英数字のみ	128文字以内
		契約ユーザー名	半角英数字/記号	128文字以内
		パスワード	半角英数字/記号	128文字以内

★1 半角英数字は、半角英字と半角数字です。

★2 ASCIIは、ASCII文字のうち表示できるものです。（半角英数字/記号/半角スペース）
大文字小文字の区別に注意して入力してください。

7. FWA機器の接続互換について

弊社製FWA機器は、下表のように組み合わせにより、接続できる条件が異なりますのでご注意ください。

■ 接続対応表

親機/子機	通信モード	SE-570FW Ver2.03	SE-570FWD Ver2.03	SE-900FW Ver1.01
BS-570 Ver2.05	インフラストラクチャー	◎	◎	○
	ブリッジ*	◎	◎	○
BS-900 Ver1.02	インフラストラクチャー	○	○	◎
	ブリッジ*	○	○	◎

◎：接続可能(暗号化機能も互換)　○：接続可能(一部の暗号化は互換なし)
★VLAN IDの有無に関係なく、すべてのパケットを透過するモードです。

■ 帯域幅

親機/子機	帯域幅	SE-570FW Ver2.03	SE-570FWD Ver2.03	SE-900FW Ver1.01		
		20MHz	20MHz	40MHz	20MHz	10MHz
BS-570 Ver2.05	20MHz	○	○	△	○	×
BS-900 Ver1.02	40MHz	△	△	○	△	×
	20MHz	○	○	△	○	×
	10MHz	×	×	×	×	○

○：設定した帯域幅で接続可　△：20MHz 帯域幅で接続可　×：接続不可

■ 暗号化セキュリティー

	WEP RC4	OCB AES	TKIP	AES	TKIP/AES
BS-570 SE-570FW/SE-570FWD	○	○	○	○	○
BS-900 SE-900FW	○	×	○	○	○

■ ネットワーク認証

	IEEE802.1X	WPA	WPA2	WPA-PSK	WPA2-PSK
BS-570 SE-570FW/SE-570FWD	○	○	×	○	×
BS-900 SE-900FW	○	○	○	○	○

7. FWA機器の接続互換について(つづき)

■ 無線ブリッジ接続について

本書では、BS-900とSE-900FWを例に無線ブリッジ接続を説明しています。(P.6-18)
★従来機種とは、下記のように条件が異なりますのでご注意ください。

親機(FWA基地局)

BS-900	Ver1.02以降	端末のMACアドレスを登録すると、無線ブリッジ接続に切り替わる
BS-570★	Ver2.05以降	無線通信を開始すると、自動的に無線ブリッジ接続に切り替わる

子機(FWA無線LAN端末)

SE-900FW	Ver1.01以降	ブリッジ接続を有効に設定
SE-570FW★	Ver2.03以降	接続端末MACアドレスを自動に設定
SE-570FWD★	Ver2.03以降	接続端末MACアドレスを自動に設定

BS-900やSE-900FWと従来機種の共通点(親機/子機)

◎BS-900やSE-900FWと従来機種(BS-570やSE-570FWなど)で接続、通信できる
◎無線ブリッジ接続の端末に対してはVLANを透過する
　※仮想APのVLAN機能(BS-570では仮想BSS)は適用しない
◎無線ブリッジ接続の端末に対して、MACアドレスフィルタリング、端末台数制限機能は適用する

BS-900と従来機種の異なる点(親機)

◎BS-900は、仮想AP「ath0」に接続した端末だけ無線ブリッジ接続できる
　※BS-570の場合は、「無線LAN」画面で設定したSSIDで接続した端末だけ無線ブリッジ接続できる
　※仮想BSSに接続する端末はブリッジ接続できない
◎BS-900に無線ブリッジ接続する端末のMACアドレスを事前登録する(P.6-18)
　※未登録の端末は通常端末として接続、通信する
　※BS-570の場合は、端末のMACアドレスの登録は不要
◎BS-900の場合、下記条件をすべて満たす端末を自動検出して、BS-900の「ブリッジ接続」画面に表示
　• BS-900の仮想AP「ath0」に現在接続中　• ブリッジ接続が有効　• MACアドレスが未登録
◎BS-900の場合は、ブリッジ接続stawds0-stawds7をパケットフィルターの条件にできる

SE-900FWと従来機種の異なる点(子機)

◎SE-900FWには、ブリッジ接続有効/無効の設定がある
　※SE-570FW、SE-570FWDは、接続端末MACアドレスを自動以外に設定するとブリッジ接続が無効になる
◎SE-900FWは、ブリッジ接続時にインターフェースstawds0を使用する
　(情報表示→ネットワーク情報→ブリッジ接続)

無線ブリッジ接続のとき対象外になる機能

　• 仮想APのVLAN機能　• 認証VLAN機能　• ARP代理応答機能

8. 定格について

■ 一般仕様

電　　源：PoE(IEEE802.3af準拠 最大12W)
使 用 環 境：温度−20～+55℃(0℃以下では常時通電時)★、湿度5～95%（結露状態を除く）
★−20℃～0℃の環境では、電源投入して1時間以上経過してから、本製品をリセット(再起動)して通信を開始してください。
外 形 寸 法：約215(W)×191(H)×77.5(D)mm(取り付け金具、突起物を除く)
重　　量：約3.5kg(本体接続LANケーブル/取り付け金具を含む)
適 合 規 格：クラスB情報技術装置(VCCI)
インターフェース：状態表示ランプ(PWR、MODE、LAN、)
防 水 関 係：IP67

■ 有線部

通 信 速 度：10/100/1000Mbps(自動切り替え/全二重)
インターフェース：[LAN]ポート(RJ-45型)×1(Auto MDI/MDI-X)
●IEEE802.3/10BASE-T準拠
●IEEE802.3u/100BASE-TX準拠
●IEEE802.3ab/1000BASE-T準拠
●IEEE802.3af準拠
[CONSOLE]ポート
●RS-232C準拠

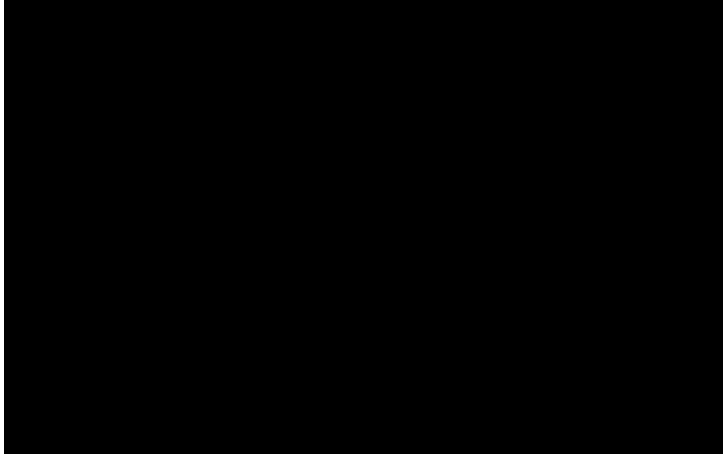
■ 無線部

無線設備区分：証明規則第二条第一項第十九号の五
使用周波数：40MHz帯域幅時 4920/4960MHz
20MHz帯域幅時 4920/4940/4960/4980MHz
10MHz帯域幅時 4915/4920/4925/4935/4940/4945MHz
インターフェース：アンテナコネクター(SMA-J型×2系統)

※定格・仕様・外観等は改良のため予告なく変更する場合があります。

株式会社エクセリ　東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5　URL : https : //www.exseli.com/

高品質がテーマです。



アイコム株式会社
547-0003 大阪市平野区加美南1-1-32

A-7261-3J-①

株式会社エクセリ　東京都中央区日本橋浜町2-30-1 / 大阪府大阪市中央区久太郎町1-9-5　URL : https : //www.exseli.com/