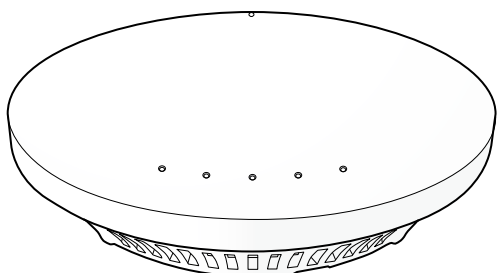


WIRELESS ACCESS POINT
AP-95M

IEEE802.11ac Wave 2規格準拠



Icom Inc.

はじめに

1 ご使用になる前に

2 導入ガイド

3 設定画面について

4 保守について

5 ご参考に

- ◎ 5.2GHz帯無線LANの使用は、電波法により、5.2GHz帯高出力データ通信システムの基地局、または陸上移動中継局と通信する場合を除き、屋内に限定されます。
- ◎ 5.3GHz帯無線LANの使用は、電波法により、屋内に限定されます。

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、IEEE802.11ac Wave2規格に準拠し、5GHz帯と2.4GHz帯の同時通信に対応したワイヤレスアクセスポイントです。

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。

登録商標/著作権

アイコム株式会社、アイコム、Icom Inc.、アイコムロゴは、アイコム株式会社の登録商標です。

Microsoft、Windowsは、米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。

Wi-Fi、WPA、WMMは、Wi-Fi Allianceの商標または登録商標です。

その他、本書に記載されている会社名、製品名は、各社の商標または登録商標です。

なお、本文中ではTM、®などのマークを省略しています。

本書の内容の一部、または全部を無断で複製/転用することは、禁止されています。

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：本製品の各メニューと、そのメニューに属する設定画面の名称を(「 」)で囲んで表記します。

[]表記：各設定画面の設定項目名を([])で囲んで表記します。

< >表記：設定画面上に設けられたコマンドボタンの名称を(< >)で囲んで表記します。

※ 本書は、Ver. 2.24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 10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。

はじめに

本製品の概要について

- ◎IEEE802.11ac Wave2規格に準拠し、最大867Mbps(理論値)の速度で通信できます。
 - ※IEEE802.11ac規格を使用できるのは、5GHz帯だけです。
 - さらに、最大867Mbps(理論値)で使用するには、帯域幅を「80MHz」に設定してください。
 - ※IEEE802.11ac規格、IEEE802.11n規格での通信は、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。
- ◎IEEE802.11a(W52/W53/W56)規格、IEEE802.11b/g規格に準拠し、2.4GHz帯と5GHz帯の2波同時通信に対応しています。
 - ※IEEE802.11a(J52)規格の無線LAN製品とは通信できません。
- ◎異なる無線LAN規格の機器を同時に使用する環境において、速度低下を緩和するプロテクション機能を搭載しています。
- ◎DFS機能の搭載により、5.3/5.6GHz帯のチャンネルで通信しているときは、気象レーダーなどへの電波干渉を自動で回避します。
- ◎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16グループ(2.4GHz帯、5GHz帯ごとに最大8グループ)の無線ネットワークを構築できます。
 - ※各仮想APのVLAN機能とルーター機能は併用できません。
- ◎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。
- ◎「MAC認証」、「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。
- ◎認証VLAN有効時、RADIUSサーバーを利用した認証結果(応答属性)に応じて、無線LAN端末の所属VLAN IDをグループ分けできます。
- ◎ユーザー単位で端末を認証するWeb認証機能を搭載しています。
- ◎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-5)」、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。
- ◎Wi-Fiアライアンスが提唱するWPS(Wi-Fi Protected Setup)機能の搭載により、SSIDと暗号化(WPA-PSK/WPA2-PSK)をWPS機能対応の無線LAN端末に自動設定できます。
 - ※2021年6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。
- ◎端末のある方向に向けて電波を送るビームフォーミング機能を搭載しています。
 - さらに、電波干渉を避けて、複数の端末へ並行送信できるMU-MIMO機能も備えています。
- ◎災害時統一SSIDを利用した公衆無線LANサービス「00000JAPAN」に対応しています。
- ◎ネットワーク管理機能として、SNMPに対応しています。
- ◎本製品は、免許不要・資格不要です。
- ◎FTTH、ADSL、VDSL、CATV対応のルーター機能を搭載しています。(Ver. 2.07以降)
 - ※本製品の[LAN]ポートは、回線種別を変更(DHCPクライアント/固定IP/PPPoE)することで、WAN側接続用ポートに切り替わります。
 - 設定変更後は、無線LAN端末から本製品の設定画面にアクセスしてください。

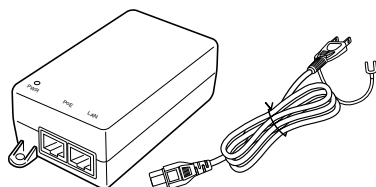
はじめに

別売品について

(2021年6月現在)

SA-5

イーサネット電源供給ユニット
(IEEE802.3at/IEEE802.3af規格準拠)



RS-AP3

アクセスポイント管理ツール

RC-AP10

無線LANコントローラー

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。

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	IPアドレス	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
ルーター設定	WAN接続先	回線種別設定	回線種別	LANポートとして使用する
無線LAN設定	無線LAN	無線LAN	チャンネル	001CH (2412MHz) (無線LAN1) 036CH (5180MHz) (無線LAN2)
			帯域幅	20MHz
			インターフェース	ath0 (無線LAN1) ath1 (無線LAN2)
	仮想AP	仮想AP設定	SSID	WIRELESSLAN-0
			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
		暗号化設定		
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長く複雑なものにされることをおすすめします。

はじめに

無線LAN規格について

本製品が準拠する無線LAN規格と最大通信速度

周波数帯	無線LAN規格	帯域幅	最大通信速度(理論値)
5.2/5.3/5.6GHz	IEEE802.11ac (W52/W53/W56)	80MHz	867Mbps
		40MHz	400Mbps
		20MHz	192Mbps
	IEEE802.11n (W52/W53/W56)	40MHz	300Mbps
		20MHz	144Mbps
	IEEE802.11a (W52/W53/W56)		54Mbps
2.4GHz	IEEE802.11n	40MHz	400Mbps ^{★1}
			192Mbps ^{★1}
	IEEE802.11g	20MHz	54Mbps
	IEEE802.11b		11Mbps

★1 無線LAN端末側がデジタル変調方式の256QAMに対応している必要があります。

【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、IEEE802.11の無線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、電子レンジ等の電波環境要素、使用するパソコンの性能、通信する相手側の性能や設定、ネットワークの使用状況など)に影響されます。

本製品が準拠する無線LAN規格と通信距離

無線通信距離は、設置場所や通信周波数によって異なります。

以下の表は目安としてご覧ください。

周波数帯	無線LAN規格	室内見通し	オープンスペース ^{★2}
5.2/5.3/5.6GHz	IEEE802.11ac (W52/W53/W56)	約30m	約100m
	IEEE802.11n (W52/W53/W56)		
	IEEE802.11a (W52/W53/W56)		
2.4GHz	IEEE802.11n	約30m	約100m
	IEEE802.11g		
	IEEE802.11b		

※本書では、弊社製SE-90Mと通信した場合の距離を参考として記載しています。

★2 5.2/5.3GHz帯無線LANの使用は、電波法により、屋内に限定されます。

はじめに

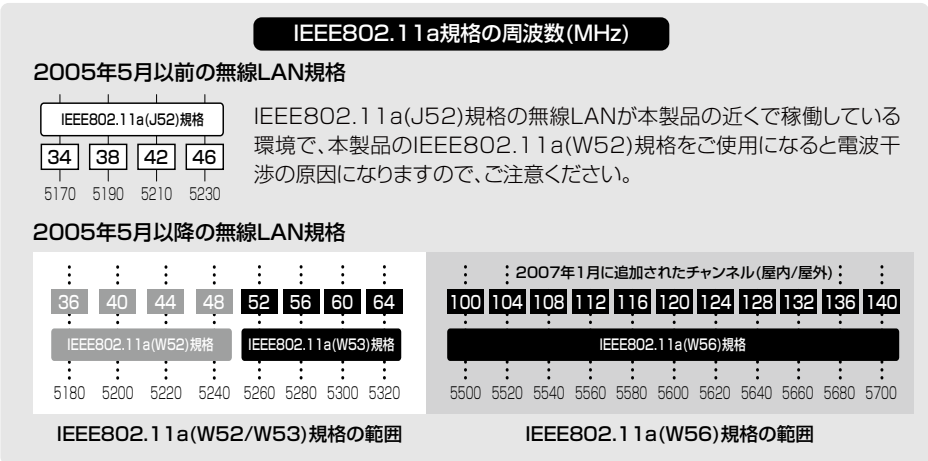
無線通信チャンネルについて

IEEE802.11a(W52/W53/W56)規格の無線通信チャンネルについて

右に記載する表示がある製品は、IEEE802.11a(W52/W53/W56)規格で採用された無線通信チャンネルに対応した製品を意味します。

無線LAN端末についても、右に記載する表示がある製品でご使用いただくことをおすすめします。

IEEE802.11b/g/n
IEEE802.11a/n/ac
J62 W52 W53 W56



帯域幅と無線通信チャンネルについて

本製品には、2.4GHz帯用(無線LAN1)、5GHz帯用(無線LAN2)の無線LANユニットが内蔵されています。

必要に応じて、チャンネルや帯域幅を変更してください。

周波数帯	帯域幅	使用できるチャンネル
5GHz	80MHz	36、40、44、48、52、56、60、64、100、104、108、112、116、120、124、128
	40MHz	36、44、52、60、100、108、116、124、132
	20MHz	36、40、44、48、52、56、60、64、100、104、108、112、116、120、124、128、132、136、140、自動
2.4GHz	40MHz	1、2、3、4、5、6、7、8、9
	20MHz	1、2、3、4、5、6、7、8、9、10、11、12、13、自動

※帯域幅を80MHzに設定できるのは、無線LAN2(5GHz帯)だけです。

はじめに

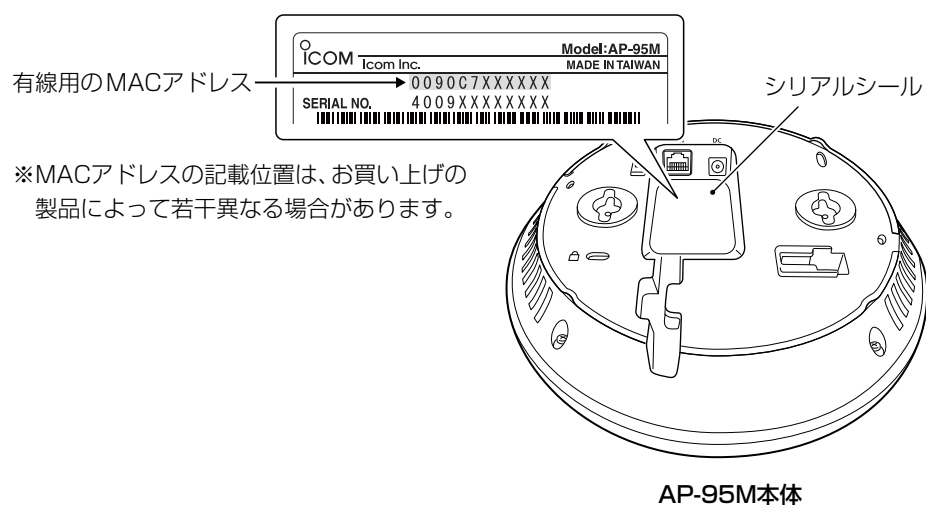
本体MACアドレスが必要なときは

本製品のシリアルシールに、有線用のMACアドレス(機器固有の番号)が12桁で記載されています。

本製品をインターネットに接続してご使用になる場合、回線種別を変更(DHCPクライアント/固定IP/PPPoE)して、本製品の[LAN]ポートをWAN側接続用ポートに切り替えます。

ご契約の接続業者、またはプロバイダーや提供を受けるサービスによっては、モデムに直接接続するネットワーク機器(本製品)がそれぞれ独自に持っているMACアドレス(下図参照)を、接続業者、またはプロバイダーに対して事前申請を必要とする場合があります。

そのような場合、申請、および登録が完了するまで、本製品を利用してインターネットに接続できません。



ご参考に

上記のMACアドレスや無線用のMACアドレスは、本製品の設定画面(P.3-5)からでも確認できます。

はじめに

ご使用までの流れ

本製品を設定されるときは、次の手順にしたがってお読みください。

1. 本製品のおもな機能	(P.1-4～)
↓	
2. ネットワークや無線通信などの基本設定手順	(P.1-14～)
↓	
3. 仮想AP機能などの無線LAN設定	(P.2-15～)
↓	
4. 内部時計などその他の設定	(P.3-123～)
↓	
5. 設定内容の書き込みや保存のしかた	(P.4-2～)
↓	
6. 本製品の設定を初期化するには	(P.4-4～)
↓	
7. 困ったときは	(P.5-2～)

ご使用になる前に

第 1 章

この章では、
本製品の基本操作やおもな機能などを説明しています。

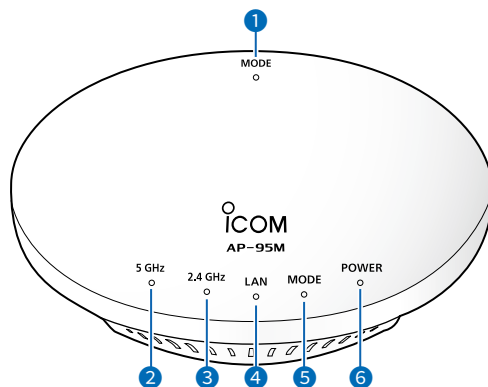
1. 各部の名称と機能	1-2
■ 上部部	1-2
■ 底面部	1-3
2. おもな機能について	1-4
■ アクセスポイント機能	1-4
■ 無線ネットワーク名(SSID)	1-4
■ 接続端末制限機能	1-4
■ 同一仮想AP内の端末間通信禁止機能	1-4
■ IEEE802.11ac規格	1-4
■ IEEE802.11n規格	1-5
■ ビームフォーミング機能/MU-MIMO機能	1-5
■ ローミング機能について	1-5
■ 無線AP間通信機能(WBR)について	1-6
■ 仮想AP機能について	1-7
■ ルーター機能について	1-8
■ DFS機能とチャンネルの自動設定	1-9
■ WPS機能について	1-10
3. 設置について	1-11
■ ブラケットを使用して固定するときは	1-11
■ ブラケットと金属プレートを使用して固定するときは	1-12
■ レール用クリップを使用して固定するときは	1-13
4. 設定のしかた	1-14
■ 設定用のパソコンに固定IPアドレスを設定する	1-14
■ 設定に使うパソコンを接続する	1-15
■ 設定画面にアクセスするには	1-18
■ 設定画面の名称と機能について	1-19
■ 設定画面の表示について	1-20
■ 本体IPアドレスを変更するときは	1-22

1 ご使用になる前に

1. 各部の名称と機能

■ 上面部

各ランプのおもな動作と状態について説明します。



- | | |
|----------------------|---|
| ① 〈MODE〉ボタン | 設定を初期化するときに使用します。(P.4-4)
※ペン先などを利用して押してください。 |
| ② [5GHz] ランプ | ● 緑点灯： 端末(5GHz帯)が1台以上帰属時★/WPS成功時
☀ 緑点滅： DFS動作による無線動作待機中
消 灯： 上記以外 |
| ③ [2.4GHz] ランプ | ● 緑点灯： 端末(2.4GHz帯)が1台以上帰属時★/WPS成功時
消 灯： 上記以外 |
| ④ [LAN] ランプ | ● 緑点灯： リンク時(1000BASE-T)
☀ 緑点滅： データ通信中(1000BASE-T)
● 橙点灯： リンク時(10BASE-T/100BASE-TX)
☀ 橙点滅： データ通信中(10BASE-T/100BASE-TX)
消 灯： 上記以外 |
| ⑤ [MODE] ランプ | ● 緑点灯： 〈MODE〉ボタン操作時
☀ 緑点滅： WPS実行時
● 橙点灯： オンライン更新(ファームウェア更新あり)
☀ 橙点滅： WPS失敗時(約30秒後消灯)
消 灯： 上記以外 |
| ⑥ [POWER] ランプ | ● 緑点灯： 電源ON時
☀ 緑点滅： ファームウェアロード時
消 灯： 上記以外
※電源投入時、すべてのランプが点滅します。
※起動中、[POWER] ランプは、緑点灯→緑点滅→緑点灯の順で遷移します。 |

※LED消灯モードが「有効(完全消灯)」のときは、すべてのランプが消灯します。(出荷時の設定：無効)

★無線LANユニット有効時、本製品と通信できる無線LAN端末が存在しない、または無線通信しない状態がつづくと、[5GHz] ランプ、[2.4GHz] ランプは、消灯に変わります。

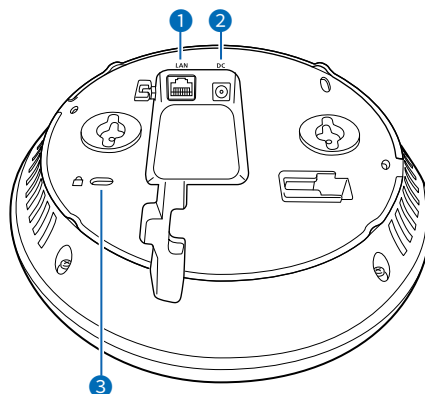
なお、消灯に変わるまでの時間は、通信状態によって異なります。

1 ご使用になる前に

1. 各部の名称と機能

■ 底面部

接続各部について説明します。



① [LAN]ポート (RJ-45型×1)

回線種別の設定によって、用途が異なります。(P.3-51)

※PoEから受電する場合は、回線種別の設定に関係なく使用できますので、SA-5(別売品)、またはIEEE802.3af対応のHUBと接続してください。

◎「[LAN]ポートとして使用する」(出荷時の設定)に設定時

[LAN]ポートに切り替わりますので、HUB(VLAN対応スイッチなど)やルータータイプモデムなどのネットワーク機器と接続します。

◎「[DHCPクライアント]/[固定IP]/[PPPoE]に設定時

[WAN]ポートに切り替わりますので、ADSL、VDSL、CATVでお使いのブリッジタイプモデム、またはFTTHでお使いの回線終端装置と接続します。

② DCジャック

本製品に付属のACアダプターを接続します。

※PoEから受電する場合は、接続する必要はありません。

③ セキュリティースロット

市販のセキュリティワイヤーで本製品を固定するときに使用します。

セキュリティワイヤーを固定してから、本製品のセキュリティースロットに取り付けてください。

※取り付け方法については、ご使用になるセキュリティワイヤーの取扱説明書をご覧ください。

※セキュリティワイヤーには、シリンダーヘッド部の横からワイヤーが出るものと、上から出るものがあります。

ご利用の環境に応じたセキュリティワイヤーをご用意ください。

1 ご使用になる前に

2. おもな機能について

■ アクセスポイント機能

本製品は、IEEE802.11ac規格、IEEE802.11n規格に準拠し、5.2/5.3/5.6GHz帯と2.4GHz帯の2波同時通信ができる無線アクセスポイントです。

※ IEEE802.11規格(14CH)の無線LAN端末とは通信できません。

■ 無線ネットワーク名(SSID)

本製品と無線LAN端末には、接続先を識別するための無線ネットワーク名として、SSID(またはESS ID)が設定されています。(P.2-2)

※ 異なるSSIDを設定している無線LAN端末は接続できません。

※ 本製品には、2.4GHz帯用(無線LAN1)と5GHz帯用(無線LAN2)の無線LANユニットが内蔵されています。

複数の仮想AP機能を使用する場合、1つのユニットに対して、同じSSIDを設定できません。

■ 接続端末制限機能

本製品の仮想APごとに同時接続できる無線LAN端末の台数を制限して、接続が集中するときに起こる通信速度の低下を防止する機能です。

出荷時、仮想APごとに最大63台に設定されていますが、無線LAN1(ath0、ath01～ath07)、無線LAN2(ath1、ath11～ath17)それぞれで10台を超えないように運用されることをおすすめします。

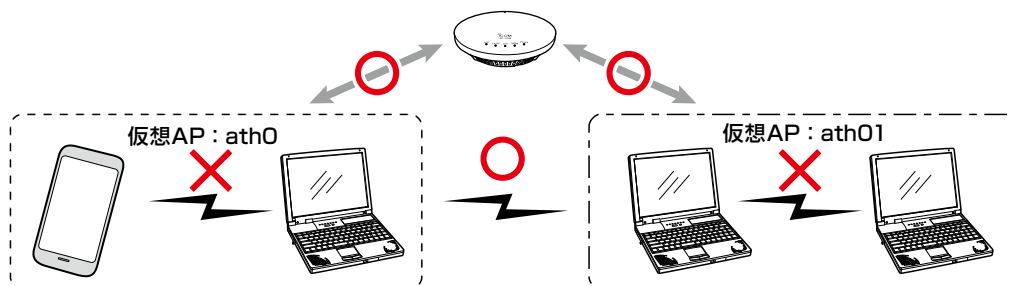
※ 仮想APごとに最大128台まで設定できますが、実際に通信できるのは、1つの無線ユニットで最大128台までです。

■ 同一仮想AP内の端末間通信禁止機能

本製品の同じ仮想APに帰属する無線LAN端末同士の通信を遮断する機能です。

※この機能を有効(P.3-72)にしたときは、同じ仮想APに帰属するすべての無線LAN端末が対象になります。

※異なる仮想AP(例：ath0とath01)に帰属する無線LAN端末同士の通信を禁止する場合は、パケットフィルターで設定できます。(P.3-20)



■ IEEE802.11ac規格

最大4倍の周波数帯域幅(チャンネル)と複数のアンテナを使用してデータを送受信することで、最大867Mbps[★](理論値)の速度で通信できます。

★ IEEE802.11ac規格での通信は、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。

IEEE802.11ac規格を利用できるのは、無線LAN2(5GHz帯)だけです。

さらに、最大867Mbps(理論値)で使用するには、帯域幅を「80MHz」に設定してください。(P.2-12)

※ IEEE802.11n/a規格と互換性があります。

1 ご使用になる前に

2. おもな機能について

■ IEEE802.11n規格

最大2倍の周波数帯域幅(チャンネル)と複数のアンテナを使用してデータを送受信することで、最大400Mbps^{★1★2}(理論値)の速度で通信できます。

★1 IEEE802.11n規格での通信は、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。

★2 最大400Mbps(理論値)で使用するには、帯域幅を「40MHz」に設定してください。

さらに、無線LAN端末側がデジタル変調方式の256QAMに対応している必要があります。

※ IEEE802.11a/b/g規格と互換性があります。

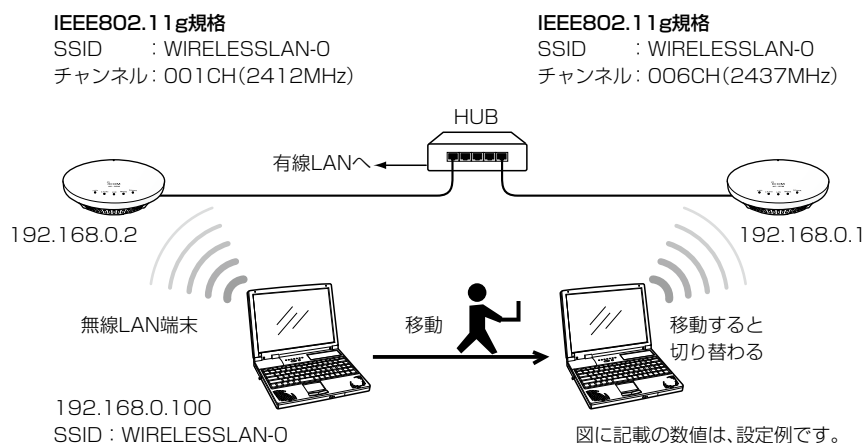
■ ビームフォーミング機能/MU-MIMO機能

端末のある方向に向けて電波を送るビームフォーミング機能を搭載しています。

さらに、電波干渉を避けて、複数の端末へ並行送信できるMU-MIMO機能も備えています。

■ ローミング機能について

無線LAN端末が移動しても、自動的に電波状況のよい無線アクセスポイントに切り替えること(ハンドオーバー)によって、工場など広い場所で無線LANが利用できる機能です。



ローミング機能を使用するには

◎本製品と無線LAN端末は、無線ネットワーク名(SSID)や暗号化をすべて同じ設定にしてください。

◎本製品の近くに複数の無線LAN機器が存在する環境でご使用になる場合は、電波干渉が発生しないチャンネル、または「自動」を設定してください。

上記の例で使用する無線LAN規格(IEEE802.11g)では、隣接する無線アクセスポイントと4チャンネル以上空けて設定してください。

※ローミングのしきい値は、無線LAN端末側に依存します。

1 ご使用になる前に

2. おもな機能について

■ 無線AP間通信機能(WBR)について

対応する弊社製無線アクセスポイント同士を無線ブリッジで接続できる機能です。

下記のように、通信できる相手側の無線アクセスポイント(弊社製)が異なります。(2021年6月現在)

無線LANユニット	周波数帯	AP-90M	AP-90MR	AP-95M	AP-900	AP-9000	AP-9500	SE-900 (アクセスポイント モード時)	SB-900
無線LAN1 (WBR)	2.4GHz帯	○	○	○	×	×	○	○	○
無線LAN2 (WBR)	5GHz帯	○	○	○	○	○	○	○	×

※必要に応じて、AP-90M、AP-90MR側の無線動作モード(2.4GHz/5GHz)を入れ替えるか、片方の動作を無効にしてください。(同じ無線動作モードを設定すると、無線が動作しなくなります。)

※5GHz帯で無線AP間通信が利用できるのは、5.2GHz帯だけです。

無線AP間通信機能(WBR)を使用するには

◎ 親機側でDFS機能が有効なチャンネルが選択されているとき、または「自動」を設定した場合(P.2-11)、無線AP間通信機能は動作しません。

◎ 親機側の仮想AP*「ath0」(無線LAN1)、または「ath1」(無線LAN2)の設定内容で無線AP間通信し、最大8台の子機とスター型のネットワークを構築できます。

※子機が接続できる親機は1台です。

◎ 子機側の「AP間通信 (WBR)」画面で「BSSID」を確認し、親機側の「接続先BSSID」に登録してください。

※親機側には、最大8台分の子機を登録できます。

※親機側★のSSIDと暗号化は、「仮想AP」画面で設定します。

★親機により、SSID、暗号化を確認する仮想APが異なりますのでご注意ください。(2021年6月現在)

「ath0」: AP-95M(無線LAN1 (2.4GHz帯))、AP-9500(無線LAN1 (5GHz帯))、SE-900(アクセスポイントモード時)、SB-900(無線1 (2.4GHz帯))

「ath1」: AP-95M(無線LAN2 (5GHz帯))、AP-9500(無線LAN2 (2.4GHz帯))

「ath4」: AP-90M、AP-90MR

「ath8」: AP-900、AP-9000

親機側で設定する項目

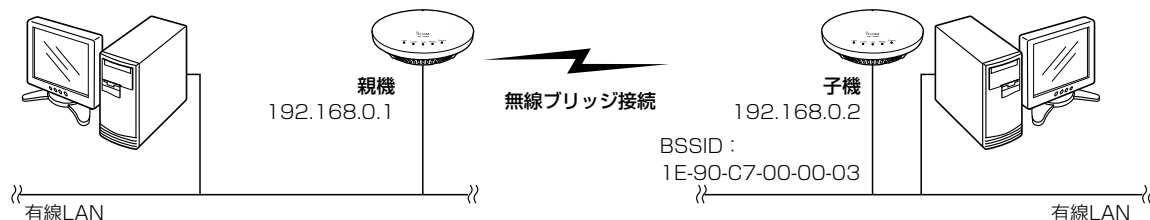
チャンネル : 001CH(2412MHz)
仮想AP : ath0
SSID : WIRELESSLAN-0
ネットワーク認証 : WPA2-PSK
暗号化方式 : AES
PSK : wirelessmaster
接続先BSSID : 1E-90-C7-00-00-03
(子機側のBSSID)

子機側で設定する項目

SSID : WIRELESSLAN-0
ネットワーク認証 : WPA2-PSK
暗号化方式 : AES
PSK : wirelessmaster

※子機側は、自動的に親機のチャンネルになります。

※数値は、設定例です。



◎ 子機側がスキャンして、SSIDと暗号化が一致した親機と接続します。

※子機側の「AP間通信 (WBR)」画面で、親機側のSSIDと暗号化を設定します。

※スキャン中の子機では、仮想APすべてが一時的に無効になります。

※子機側は自動的に親機側のチャンネルになります。

※子機として動作するとき、子機側のチャンネル設定、WMM詳細設定が無効になります。

※複数の親機が存在する場合は、電波強度により接続する親機が確定します。

※電波強度が変化しても、接続が切れない限りローミングしません。

1 ご使用になる前に

2. おもな機能について

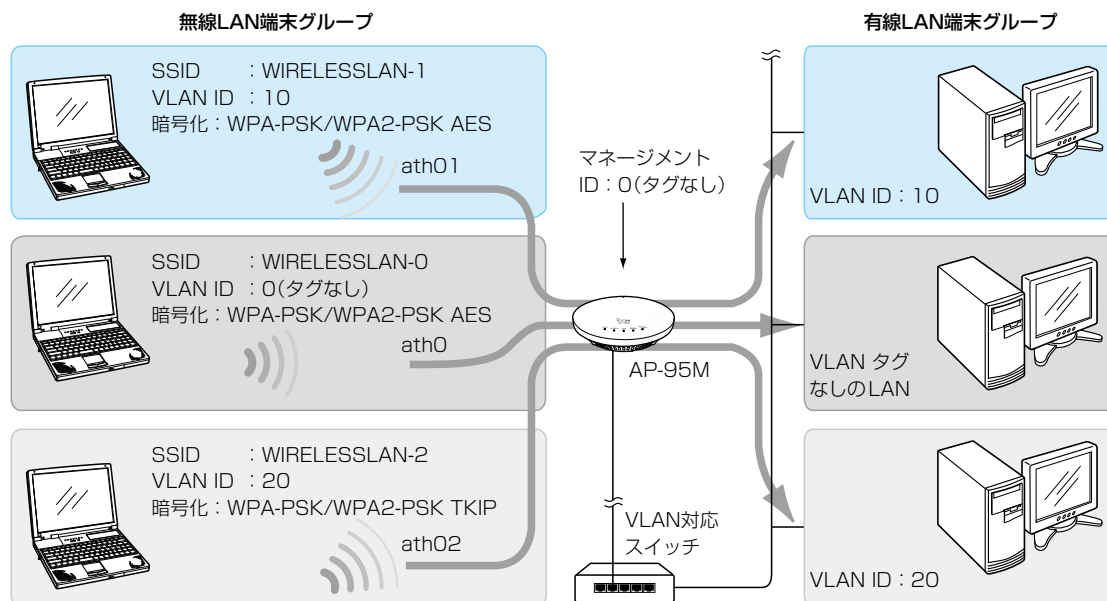
■ 仮想AP機能について

本製品1台で、条件(SSID/暗号化方式/VLAN ID)の異なる無線LAN端末グループを複数構成できます。

※各仮想APのVLAN機能とルーター機能は併用できません。

※下記の図は、「ath0」、「ath01」、「ath02」を異なる無線LAN端末グループの仮想APとして使用する例です。

※通信速度低下を防止するため、無線LAN1、無線LAN2、それぞれ仮想AP4台以下でお使いになることをおすすめします。



仮想AP機能を使用するには

◎仮想AP★を使用して、最大16グループの無線ネットワークを構築できます。

★IEEE802.11ac規格の無線ネットワークを構築する場合は、無線LAN2(5GHz帯)の「仮想AP」画面で仮想AP (ath1、ath11～ath17)を設定します。

◎複数の仮想AP機能を使用する場合、1つのユニットに対して、同じSSIDを設定できません。

◎各仮想APの無線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[管理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、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。

1 ご使用になる前に

2. おもな機能について

■ ルーター機能について

ADSL、VDSL、CATVでお使いのブリッジタイプモデム、またはFTTHでお使いの回線終端装置を本製品の[LAN]ポートと接続することで、本製品に無線LANで接続するパソコンからインターネット回線に接続できます。

※出荷時や全設定初期化時、本製品の回線種別は、「LANポートとして使用する」に設定されています。

お使いのモデムがルータータイプモデムの場合は、本製品のルーター機能を使用しませんので、本製品の回線種別は、「LANポートとして使用する」(出荷時の設定)に設定すると接続できます。

※ルーター機能を使用するときは、「ルーター設定」メニュー→「WAN接続先」画面→「回線種別設定」項目→「回線種別」欄で、「DHCPクライアント」、「PPPoE」、「固定IP」に変更してください。(P.3-51)

設定変更後は、無線LAN端末から本製品の設定画面にアクセスしてください。

※回線種別が不明な場合は、ご契約の回線接続業者との契約内容をご確認ください

ブリッジタイプモデムとの接続

下図を参考に、本製品の[LAN]ポートとブリッジタイプモデムを接続します。

※接続の前に、ご契約の回線接続業者との契約内容にしたがって、本製品の回線種別を「DHCPクライアント」、「PPPoE」、「固定IP」に変更すると、本製品の[LAN]ポートがWAN側接続用ポートに切り替わります。

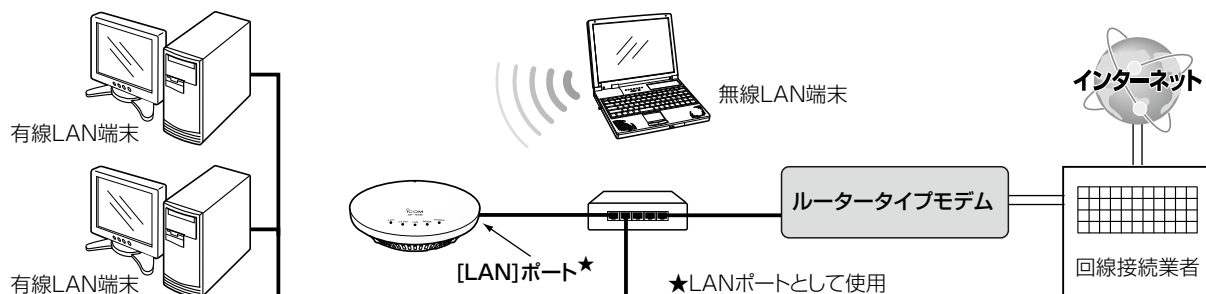


ルータータイプモデムとの接続

下図を参考に、本製品の[LAN]ポートとルータータイプモデムを接続します。

※本製品の回線種別は、出荷時の設定(LANポートとして使用する)で接続できます。

※出荷時や全設定初期化時、本製品の[LAN]ポートは、LAN側接続用ポートとして使用できます。

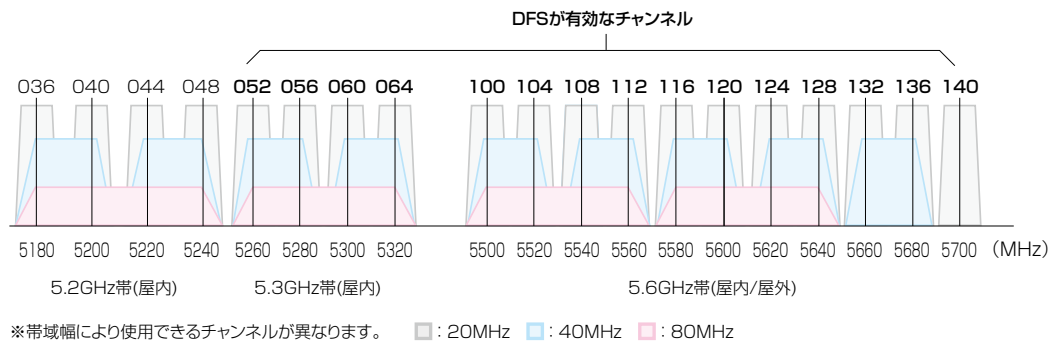


1 ご使用になる前に

2. おもな機能について

■ DFS機能とチャンネルの自動設定

DFS機能は、5.3/5.6GHz帯のチャンネルを設定したときだけ有効になり、気象レーダーなどへの電波干渉を自動で回避します。



◎ 本製品の設定画面で5.3/5.6GHz帯(052～140)のチャンネルを選択して登録すると、気象レーダーなどへの電波干渉を回避するため、1分間レーダー波を検出します。

レーダー波検出中は、本製品の[5GHz]ランプが $\star$ 緑点滅して、無線通信できなくなります。

本製品の起動中、または運用中にレーダー波を検出したときは、自動的に電波干渉しないチャンネルに変更されます。

※レーダー波を検出したチャンネルは、検出してから30分間利用できません。

◎ 5.3GHz帯(052～064)のチャンネルでレーダー波を検出して、DFS機能が無効なチャンネルが選択された場合は、別のチャンネルに変更されることはありません。

◎ 5.6GHz帯の全チャンネル(100～140)でレーダー波を検出した場合は、[5GHz]ランプが $\star$ 緑点滅すると同時に、本製品の「無線LAN」画面に「使用中チャンネル：スキャン中」が表示され、無線通信できなくなります。

このような場合は、30分間放置することで、検出チャンネルリストが初期化され、再度使用できます。

※無線通信できなくなってから30分経過しない状態で、電源を再投入する、または設定内容の変更などで再起動すると、その時点から30分間無線通信できませんのでご注意ください。

その場合、5.6GHz帯以外のチャンネルを使用できます。

◎ 40/80MHz帯域幅を設定した場合、上図のように、40MHz帯域幅では2つ、80MHz帯域幅では4つのチャンネルを束ねて使用します。

※本製品で設定した帯域幅に通信相手側が対応していない場合は、通信相手の帯域幅にしたがい、本製品で選択したチャンネルで通信します。

※レーダー波を検出した場合、40MHz帯域幅では2つ、80MHz帯域幅では4つのチャンネルが30分間利用できなくなります。

◎ 本製品の起動時に、DFS機能が無効なチャンネルが選択された場合は、そのあと、運用中に別のチャンネルに変更されることはありません。

ただし、DFS機能が有効な5.3/5.6GHz帯のチャンネル(052～140)が選択された場合は、運用中でもレーダー波を検出すると、さらにチャンネルが変更されることがあります。

◎ 本製品の設定画面でチャンネルを「自動」に設定すると、ほかの無線LAN機器からの電波干渉が少ないチャンネルに自動で設定します。

※「自動」が選択できるのは、20MHz帯域幅だけです。

※「自動」に設定した場合、設定画面上で使用中のチャンネルを確認できます。

「無線LAN設定」メニューの設定内容を変更し、〈登録〉をクリックすると、再度使用するチャンネルをスキャンします。

※チャンネル自動設定と、RS-AP3(弊社製無線アクセスポイント管理ツール)やRC-AP10(弊社製無線LANコントローラー)は併用できません。

1 ご使用になる前に

2. おもな機能について

■ WPS機能について

「Wi-Fiアライアンス」が提唱する機能で、SSIDと暗号化(WPA-PSK/WPA2-PSK)をWPS機能対応無線LAN端末に自動設定できます。

※自動設定の方法は、設定画面に表示された〈開始〉をクリックする「プッシュボタン(Push Button Configuration)方式」と自動設定する相手のPINコードを使用する「PIN(Personal Identification Number)方式」を選択できます。操作例については、2-13ページをご覧ください。

WPS機能を使用しない場合

- ① 有線LAN端末の接続
- ② 設定画面にアクセス
- ③ SSIDと暗号鍵を設定



- ④ 接続ソフトウェアの起動
- ⑤ 接続する仮想APのSSIDを選択
- ⑥ 暗号鍵を入力

WPS機能を使用する場合

あらかじめ、本製品側で仮想APの設定とWPSを使用する仮想APの割り当てが必要です。

- ① 有線LAN端末の接続
- ② 設定画面にアクセス
- ③ 「WPS」画面の〈開始〉をクリック



- ④ 〈WPS〉ボタンを押す

WPS機能を使用するには

- ◎WPS機能対応の無線LAN端末を準備してください。
- ◎無線LAN端末が〈WPS〉ボタンを装備していない場合は、WPS対応アプリケーション、またはWindows標準のワイヤレスネットワーク接続を使用してください。
- ◎本製品のWPS機能で自動設定する仮想APを「仮想AP」画面(P.3-70)で有効にし、SSIDや暗号設定などを設定してから、「WPS」画面の[使用するインターフェース]欄で選択してください。
[使用するインターフェース]欄で無効な仮想APや「なし」(出荷時の設定)を設定している場合、本製品の設定画面に〈開始〉が表示されません。

1 ご使用になる前に

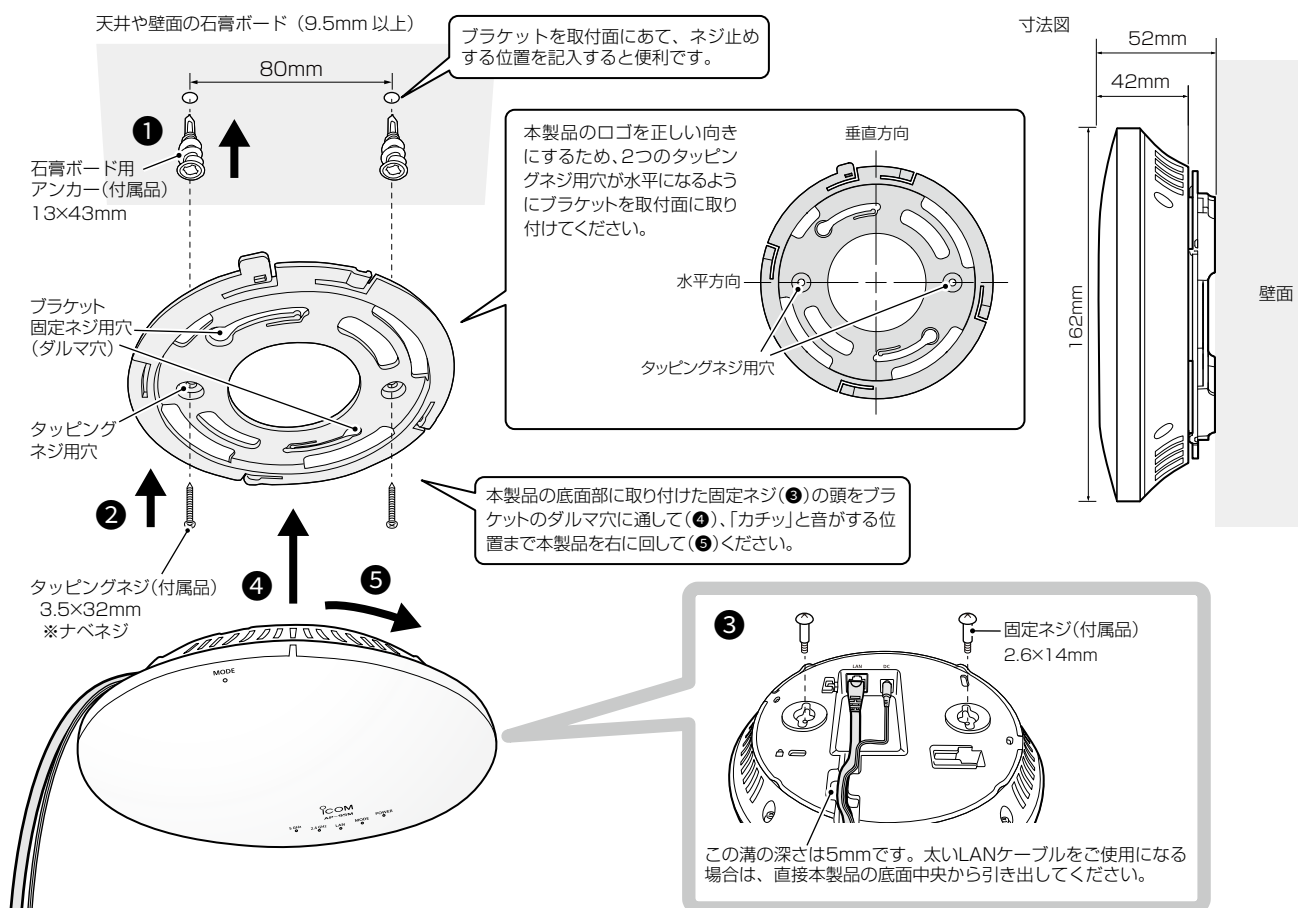
3. 設置について

本製品は前面方向に広がる電波の指向性を持つため、設置場所は壁面や天井をおすすめします。

※金属プレートも使用する場合は1-12ページ、本製品をレールに固定する場合は1-13ページをご覧ください。

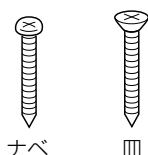
■ ブラケットを使用して固定するときは

次の手順(①～⑤)で、付属のブラケットを使用して、本製品を壁や天井に固定できます。



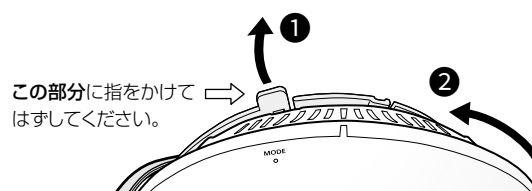
取り付けネジについて

本製品には、ナベネジと皿ネジが付属されています。ブラケットだけを取り付ける場合は、ナベネジを使用してください。



取りはずすときは

指や爪を痛めないように注意して、図のようにブラケットを取りはずしてください。

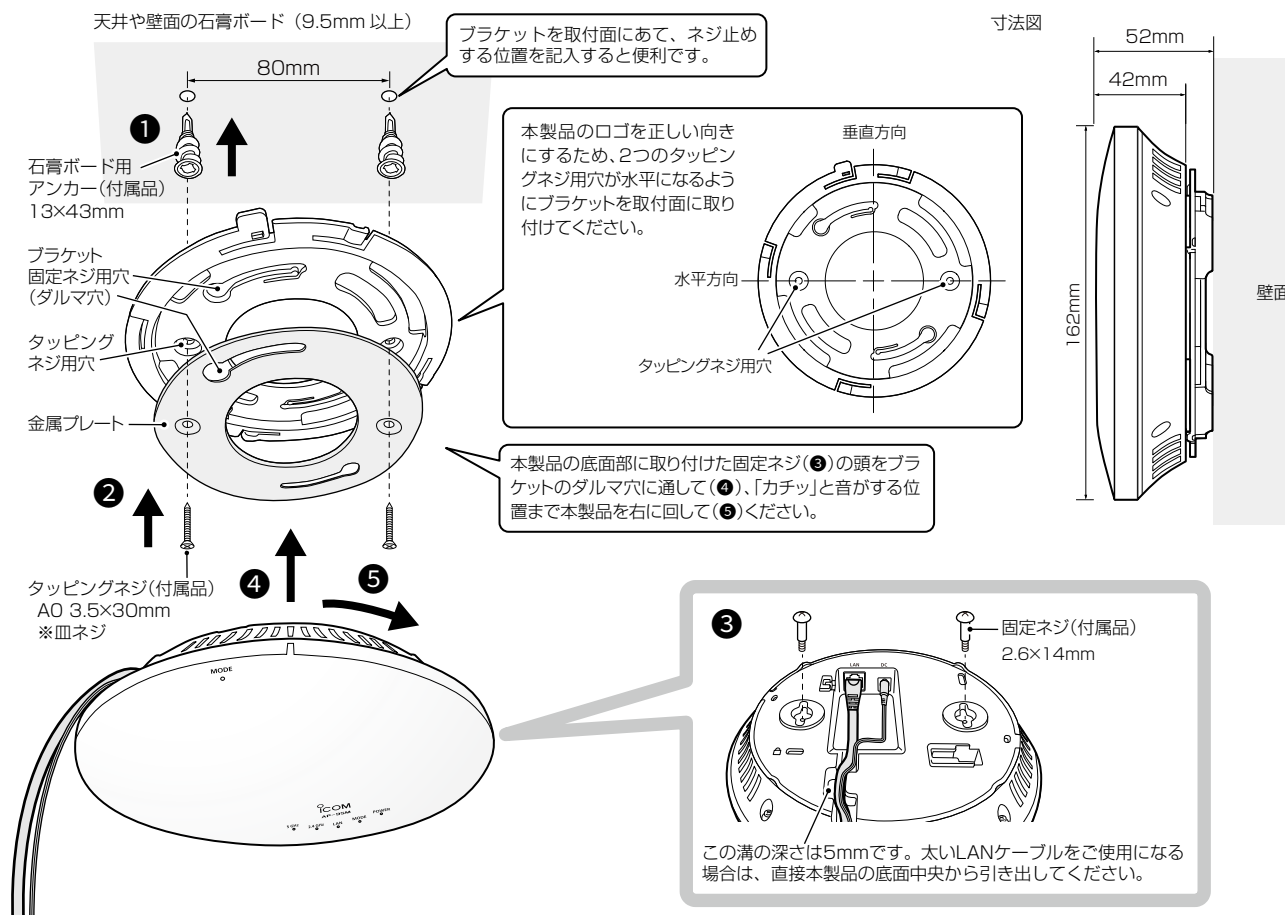


1 ご使用になる前に

3. 設置について

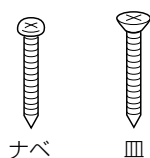
■ ブラケットと金属プレートを使用して固定するときは

下記のように付属の金属プレートを使用すると、ブラケットを補強できます。



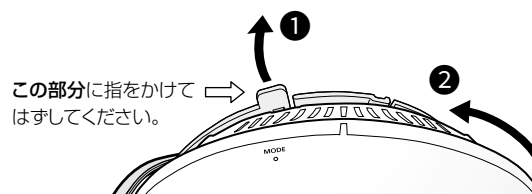
取り付けネジについて

本製品には、ナベネジと皿ネジが付属されています。ブラケットと金属プレートを取り付ける場合は、皿ネジを使用してください。



取りはずすときは

指や爪を痛めないように注意して、図のようにブラケットを取りはずしてください。



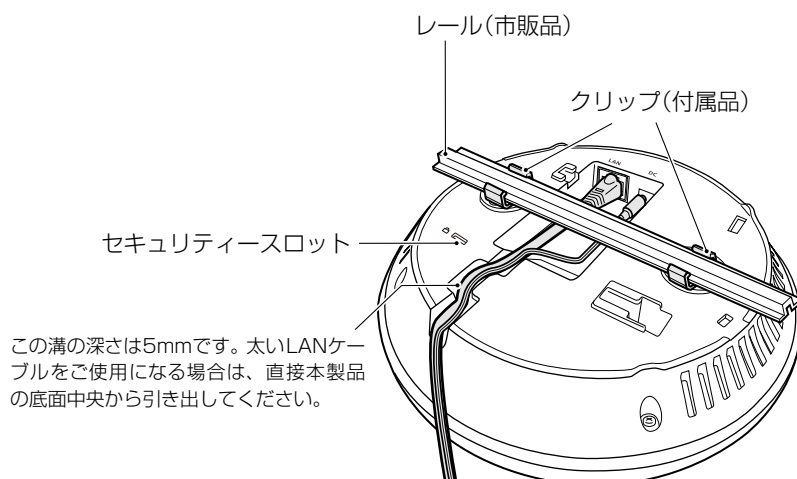
1 ご使用になる前に

3. 設置について

■ レール用クリップを使用して固定するときは

付属のレール用クリップを本製品に取り付け、「カチッ」と音がするまでレールに押し込みます。

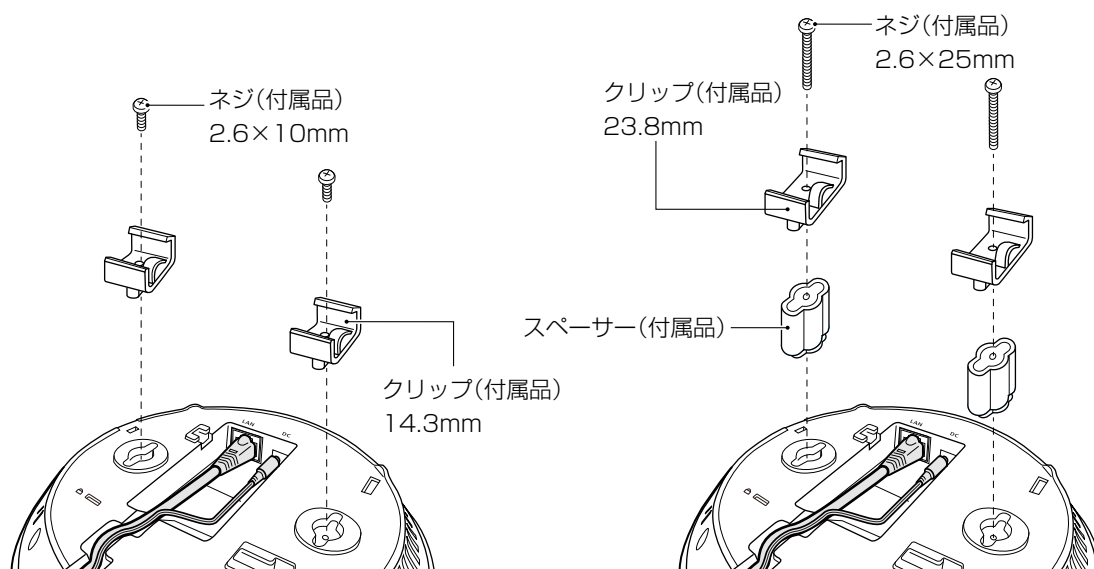
※市販のセキュリティワイヤーで本製品を固定するときは、支柱などにセキュリティワイヤーを固定してから、本製品のセキュリティスロットに取り付けてください。



クリップの取り付けについて

本製品には、2種類のクリップが付属されていますので、取り付けるレールにあわせてご使用ください。

※スペースが必要な場合は、付属のスペーサーと長いネジ(2.6×25mm)をご使用ください。



1 ご使用になる前に

4. 設定のしかた

出荷時、本製品のIPアドレスは「192.168.0.1」、DHCPサーバー機能は「無効」に設定されています。
本製品の設定画面にアクセスするときは、接続するパソコンに固定IPアドレスの設定が必要です。

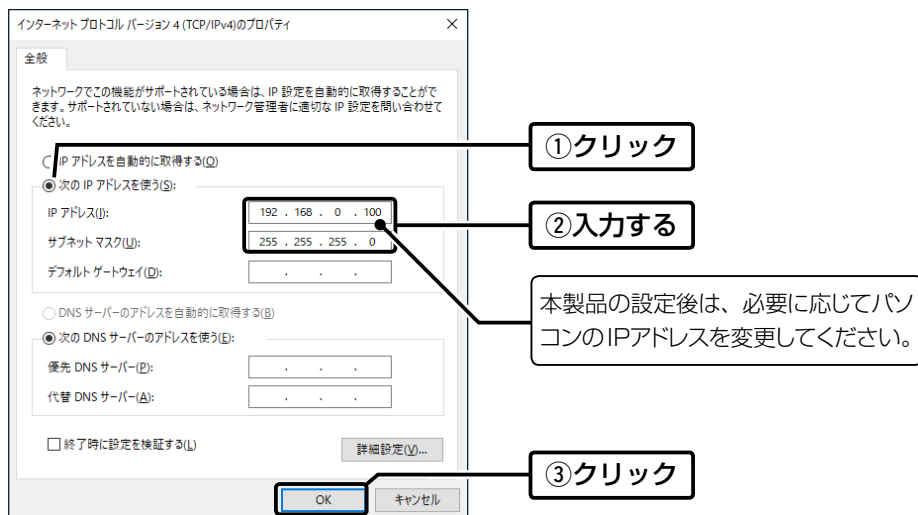
■ 設定用のパソコンに固定IPアドレスを設定する

Windows 10を例に、固定IPアドレス(例：192.168.0.100)をパソコンに設定する手順について説明します。

- 1 <スタート>(ロゴボタン)で右クリックし、表示されたメニューで[ネットワーク接続(W)]をクリックします。
- 2 [アダプターのオプションを変更する]をクリックします。
- 3 [イーサネット](有線LAN端末で設定する場合)、または[Wi-Fi](無線LAN端末で設定する場合)を右クリックし、表示されたメニューで[プロパティ(R)]をクリックします。



- 4 [ユーザーアカウント制御]のメッセージが表示された場合は、<続行(C)>をクリックします。
- 5 表示された画面で、[インターネットプロトコル バージョン4(TCP/IPv4)]を選択し、<プロパティ(R)>をクリックします。
「インターネット プロトコル バージョン 4 (TCP/IPv4)のプロパティ」画面(別画面)を表示します。
- 6 [次のIPアドレスを使う(S)]をクリックし、[IPアドレス(I)](例：192.168.0.100)と[サブネットマスク(U)](例：255.255.255.0)を入力して、<OK>をクリックします。



- 7 <OK>をクリックします。

1 ご使用になる前に

4. 設定のしかた

■ 設定に使うパソコンを接続する

有線LAN端末を使用する場合

本製品の電源を入れ、ランプの点灯を確認します。

④ ランプの点灯を確認する

本製品の[LAN]ランプが点灯しないときは、LANケーブルの接続をご確認ください。

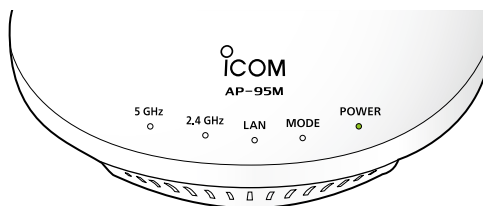
ランプ表示について

点灯：LAN接続時

点滅：LANデータ通信中

緑色：1000BASE-T時

橙色：10BASE-T/100BASE-TX時



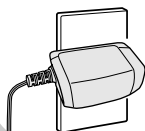
AP-95M
(出荷時の設定：192.168.0.1)

この溝の深さは5mmです。太いLANケーブルをご使用になる場合は、直接本製品の底面中央から引き出してください。

② 電源を接続する

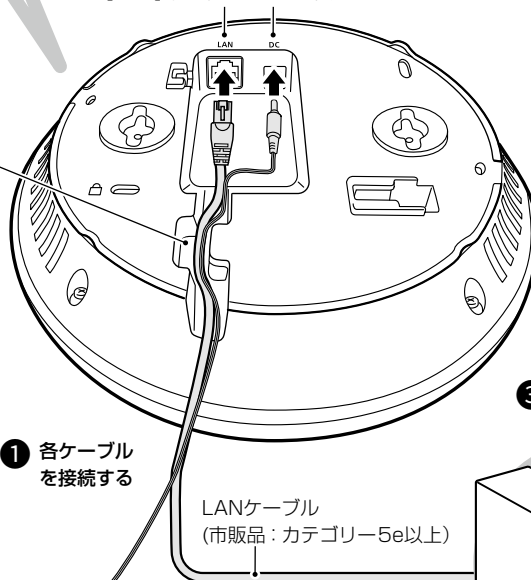
起動が完了すると、本製品の[POWER]ランプが点灯します。

ACコンセント



① 各ケーブルを接続する

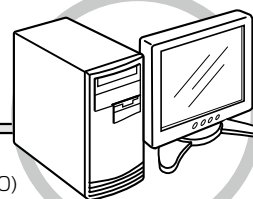
[LAN]ポートへ DCジャックへ



LANケーブル
(市販品：カテゴリ5e以上)

設定用パソコン
(設定例：192.168.0.100)

③ パソコンを起動する



1 ご使用になる前に

4. 設定のしかた

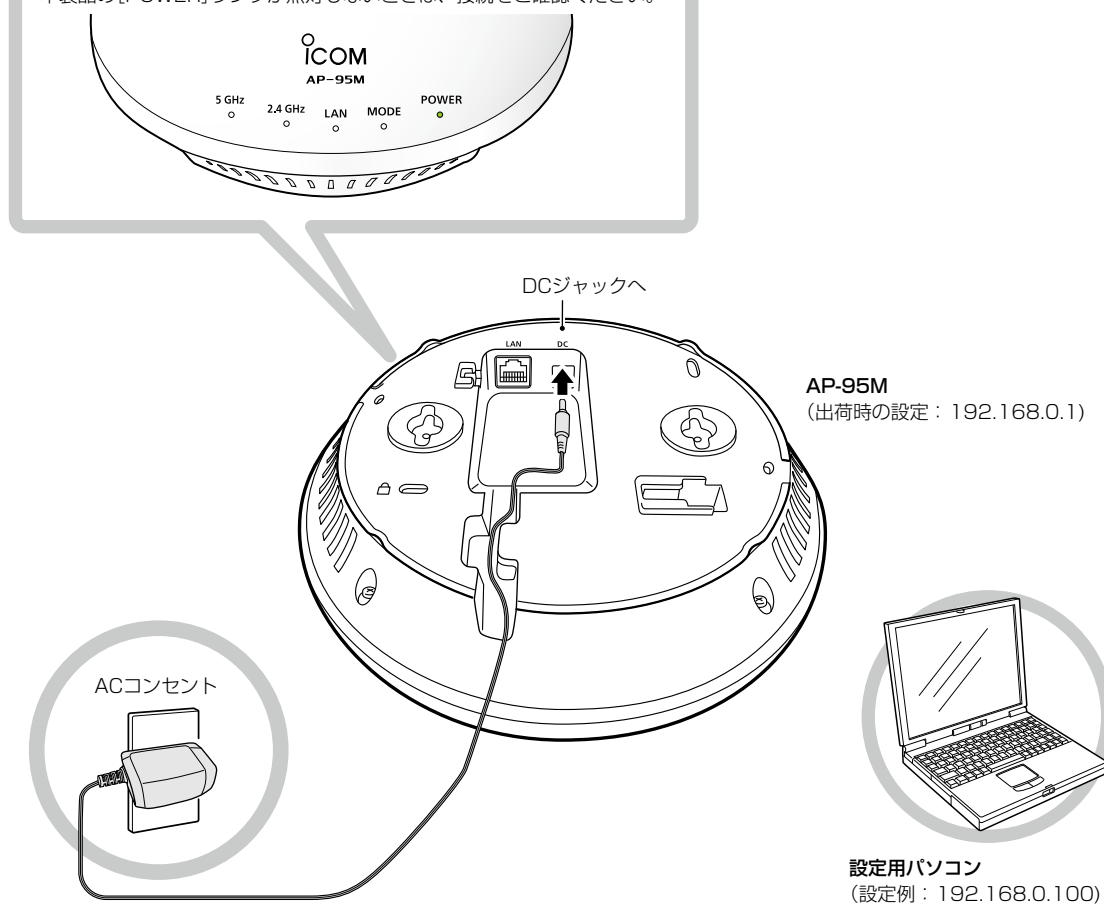
■ 設定に使うパソコンを接続する(つづき)

無線LAN端末を使用する場合

- 1 本製品の電源を入れ、ランプの点灯を確認します。

ランプの点灯を確認する

本製品の[POWER]ランプが点灯しないときは、接続をご確認ください。



- 2 [ネットワークアイコン]をクリックします。



(次ページにつづく)

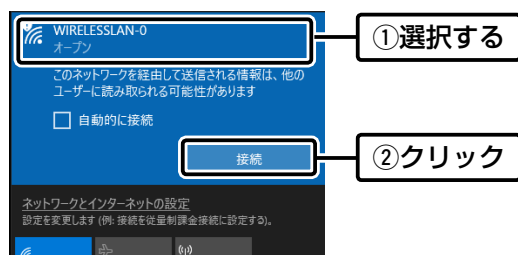
1 ご使用になる前に

4. 設定のしかた

■ 設定に使うパソコンを接続する(つづき)

無線LAN端末を使用する場合

- 3** 本製品に設定されたSSIDを選択し、〈接続〉をクリックして、表示される画面にしたがって操作します。
※出荷時、本製品のSSIDは、「WIRELESSLAN-0」に設定されています。

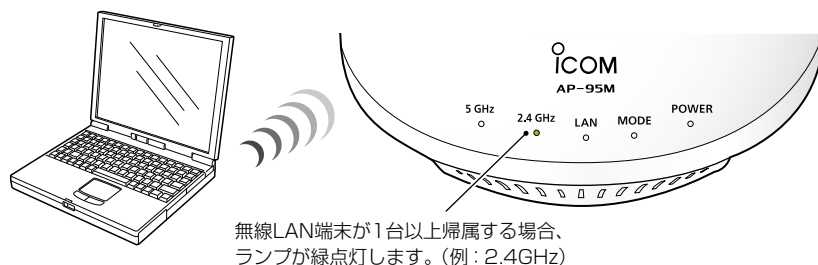


※本製品に暗号鍵(キー)を設定した場合は、「ネットワークに接続」画面が表示されますので、画面にしたがって暗号鍵(キー)を入力してください。

※不正アクセス防止のため、必ず暗号化を設定してください。暗号鍵(WEPキー)/共有鍵(Pre-Shared Key)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、さらに定期的に暗号鍵/共有鍵を変更されることをおすすめします。

- 4** 本製品の[2.4GHz]ランプ、または[5GHz]ランプが●緑点灯したことを確認します。



1 ご使用になる前に

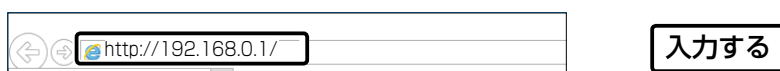
4. 設定のしかた

■ 設定画面にアクセスするには

本製品に接続したパソコンのWWWブラウザから、本製品の設定画面にアクセスする手順について説明します。

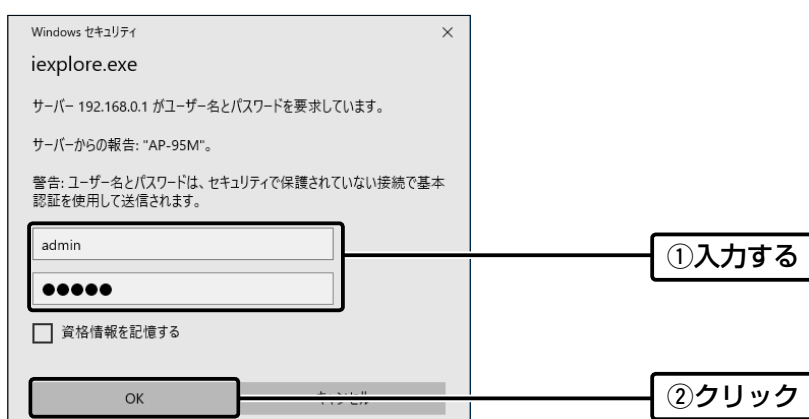
1 WWWブラウザを起動します。

2 本製品に設定されたIPアドレスをWWWブラウザのアドレスバーに入力します。
出荷時、本製品のIPアドレスは「192.168.0.1」に設定されています。



3 [Enter]キーを押します。
[ユーザー名]と[パスワード]を求める画面が表示されます。

4 [ユーザー名]欄に「admin」、[パスワード]欄に「admin」(出荷時の設定)を入力し、〈OK〉をクリックすると、設定画面が表示されます。



WWWブラウザについて

Microsoft Internet Explorer 11で動作確認しています。

設定画面が正しく表示できるように、WWWブラウザのJavaScript機能、およびCookieは有効にしてください。

1 ご使用になる前に

4. 設定のしかた

■ 設定画面の名称と機能について

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、5-6ページをご覧ください。



- | | |
|--------------------|--|
| ① 設定画面選択メニュー | 各メニューのタイトル上にマウスポインターを合わせてクリックすると、そのメニューに含まれる画面名が表示されます。 |
| ② 設定画面表示エリア | [設定画面選択メニュー]で選択したメニューに含まれる画面名(例：ネットワーク設定/IPアドレス)をクリックしたとき、その内容が表示されます。 |
| ③ 設定ボタン | 設定した内容の登録や取り消しをします。
※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。 |

1 ご使用になる前に

4. 設定のしかた

■ 設定画面の表示について

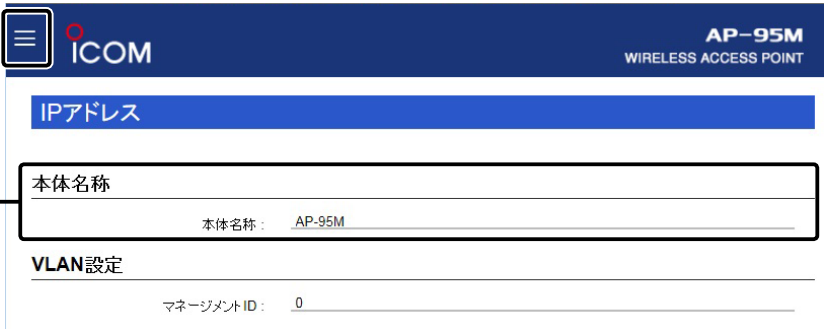
WWWブラウザのウィンドウサイズによって表示方法が異なります。
ウィンドウの幅を狭くすると、メニューが折りたたまれ「≡」が表示されます。
さらに狭くすると項目がすべて縦に表示されます。
ご使用になるパソコンの画面サイズに合わせて調整してください。

設定画面：大



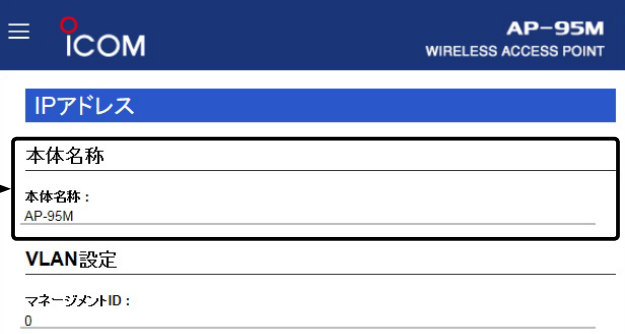
The large screen interface shows a full-width menu on the left with options: TOP, 情報表示, ネットワーク設定, IPアドレス (selected), DHCPサーバー, スタティックルーティング, ポリシールーティング, and パケットフィルター. The main content area has a header 'IPアドレス' and two sections: '本体名称' with a value of 'AP-95M' and 'VLAN設定' with a value of '0'.

設定画面：中



The medium screen interface shows a collapsed menu icon '≡' on the left. The main content area has a header 'IPアドレス' and two sections: '本体名称' with a value of 'AP-95M' and 'VLAN設定' with a value of '0'.

設定画面：小



The small screen interface shows a collapsed menu icon '≡' on the left. The main content area has a header 'IPアドレス' and two sections: '本体名称' with a value of 'AP-95M' and 'VLAN設定' with a value of '0'.

1 ご使用になる前に

4. 設定のしかた

■ 設定画面の表示について(つづき)

「≡」をクリックすると、折りたたまれたメニューが表示されます。



1 ご使用になる前に

4. 設定のしかた

ネットワーク設定 > IPアドレス > IPアドレス設定

■ 本体IPアドレスを変更するときは

本製品のIPアドレスを変更するときは、既存のネットワークと重複しないように設定します。

- 1 「ネットワーク設定」メニュー、「IPアドレス」の順にクリックします。
- 2 「IPアドレス」画面で、「IPアドレス設定」項目の設定を変更し、〈登録〉をクリックします。

※本製品のルーター機能をご使用になるとき、WAN側にデフォルトゲートウェイが設定された場合は、そのデフォルトゲートウェイを使用します。

- 3 設定変更後、「設定画面に戻る」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。
[ユーザー名]と[パスワード]を求める画面が表示されます。(P.1-18)
※IPアドレスの「ネットワーク部(例: 192.168.0)」を変更したときは、設定に使用するパソコンの「ネットワーク部」についても本製品と同じに変更します。

IPアドレスの割り当てかた

IPアドレスは、「ネットワーク部」と「ホスト部」の2つの要素から成り立っています。

出荷時の本製品のIPアドレス「192.168.0.1」(クラスC)を例とすると、最初の「192.168.0」までが「ネットワーク部」で、残りの「1」を「ホスト部」といいます。

「ネットワーク部」が同じIPアドレスを持つネットワーク機器(パソコンなど)は、同じネットワーク上にあると認識されます。さらに「ホスト部」によって同じネットワーク上にある各ネットワーク機器を識別しています。

以上のことから、IPアドレスを割り当てるときは、次のことに注意してください。

- 同じネットワークに含めたいネットワーク機器に対しては、「ネットワーク部」をすべて同じにする
- 同じネットワーク上の機器に対して、「ホスト部」を重複させない
- ネットワークアドレス(ホスト部の先頭、および「0」)を割り当てない
- ブロードキャストアドレス(ホスト部の末尾、および「255」)を割り当てない

この章では、
本製品を無線LANでご使用いただくために必要な基本設定の手順を説明しています。

1. 無線LAN接続[基本編]	2-2
■ 無線ネットワーク名を手動で設定する	2-2
■ 暗号化を手動で設定する	2-3
■ [WEP RC4]暗号化を設定するには	2-4
■ MACアドレスフィルタリングを設定するには	2-9
■ 自動チャンネルを設定するときは	2-10
■ 80MHz帯域幅通信をするときは	2-12
■ WPS機能で自動設定したいSSIDと共有鍵(キー)を指定する	2-13
2. 無線LAN接続[活用編]	2-15
■ 仮想APを設定するには	2-15
■ 無線AP間通信機能(WBR)を使用する場合	2-16
■ 無線AP間通信で使用する本製品をRS-AP3やRC-AP10で管理するときは	2-20
■ アカウンティング設定について	2-21
■ MAC認証サーバー(RADIUS)設定について	2-22
■ RADIUS設定について	2-23
■ 認証VLANについて	2-24

ご注意

「無線LAN設定」メニューの設定内容を変更して〈登録〉をクリックすると、本製品に接続するすべての無線通信が切断されます。

2 導入ガイド

1. 無線LAN接続[基本編]

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ 無線ネットワーク名を手動で設定する

無線LAN端末との識別に必要なSSIDを設定します。

※無線LAN1(2.4GHz帯)の「ath0」で通信する場合を例に説明しています。

(出荷時の設定: WIRELESSLAN-0)

1 「無線LAN設定」メニューの「無線LAN1」、「仮想AP」の順にクリックします。

2 [仮想AP設定]項目の[SSID]欄に、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。(入力例: ICOM)

仮想AP設定

インターフェース: ath0

仮想AP: ☐ 無効 ☒ 有効

SSID: ICOM

VLAN ID: 0

ANY接続拒否: ☒ 無効 ☐ 有効

接続端末制限: 63

同一仮想AP内の端末間通信禁止: ☒ 無効 ☐ 有効

アカウントing: ☒ 無効 ☐ 有効

MAC認証: ☒ 無効 ☐ 有効

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

暗号化方式: なし

登録 取消

3 <登録>をクリックします。

(次ページにつづく)

ANY接続拒否について

ANYモード(アクセスポイント自動検索接続機能)で通信する無線LAN端末からの検索、接続を拒否するときに設定します。

※ANY接続拒否を「有効」にすると、Windows標準のワイヤレスネットワーク接続画面にSSIDが表示されなくなります。

※一部の無線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 사용되는ことをおすすめします。

2 導入ガイド

1. 無線LAN接続[基本編]

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ 暗号化を手動で設定する

通信する相手の無線LAN端末にも同じ設定をしてください。

※無線LAN1(2.4GHz帯)の「ath0」で通信する場合を例に説明しています。

ネットワーク認証 : WPA-PSK/WPA2-PSK

暗号化方式 : TKIP/AES

PSK (Pre-Shared Key) : wirelessmaster

※設定例以外の暗号化設定については、2-4ページをご覧ください。

- 1 [ネットワーク認証]欄で「WPA-PSK/WPA2-PSK」、[暗号化方式]欄で「TKIP/AES」を選択し、[PSK (Pre-Shared Key)]欄で「wirelessmaster」(半角)を入力します。
※[PSK (Pre-Shared Key)]欄に入力した文字数によって、入力モード(ASCII:半角で8文字～63文字入力/
16進数:64桁入力)を自動判別します。

仮想AP設定

インターフェース : ath0

仮想AP : ☐ 無効 ☒ 有効

SSID : ICOM

VLAN ID : 0

ANY接続拒否 : ☒ 無効 ☐ 有効

接続端末制限 : 63

同一仮想AP内の端末間通信禁止 : ☒ 無効 ☐ 有効

アカウンティング : ☒ 無効 ☐ 有効

MAC認証 : ☒ 無効 ☐ 有効

暗号化設定

ネットワーク認証 : WPA-PSK/WPA2-PSK

暗号化方式 : TKIP/AES

PSK (Pre-Shared Key) : wirelessmaster

WPAキー更新間隔 : 120

① 選択する

② 入力する

登録

取消

- 2 <登録>をクリックします。

2 導入ガイド

1. 無線LAN接続[基本編]

■ [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.2-5)

◎ASCII文字で暗号鍵(キー)を直接入力する

◎[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.2-7)

※出荷時や全設定初期化時、暗号化は設定されていません。

※ [WEP RC4] 暗号化を設定できないときは、使用する仮想APIにWPS機能が設定されていないことを確認してください。
(P.2-13)

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なしてください。

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、さらに定期的に暗号鍵を変更されることをおすすめします。

2 導入ガイド

1. 無線LAN接続[基本編]

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ [WEP RC4]暗号化を設定するには(つづき)

16進数で暗号鍵(キー)を入力するには

無線LAN1 (2.4GHz帯)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 : 「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LAN設定」メニューの「無線LAN1」、「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。

仮想AP設定

インターフェース: ath0

仮想AP: ☐ 無効 ☒ 有効

SSID: WIRELESSLAN-0

VLAN ID: 0

ANY接続拒否: ☒ 無効 ☐ 有効

接続端末制限: 63

同一仮想AP内の端末間通信禁止: ☒ 無効 ☐ 有効

アカウントing: ☒ 無効 ☐ 有効

MAC認証: ☒ 無効

出荷時の設定であることを確認します。

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: WEP RC4 128 (104)

キージェネレーター:

WEPキー: 半角英数で13文字、もしくは16進数で26桁を入力

登録 取消

① 選択する

② 入力する

3 <登録>をクリックします。

2 導入ガイド

1. 無線LAN接続[基本編]

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ [WEP RC4]暗号化を設定するには(つづき)

ASCII文字で暗号鍵(キー)を入力するには

無線LAN1 (2.4GHz帯)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LAN設定」メニューの「無線LAN1」、「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。

仮想AP設定

インターフェース: ath0

仮想AP: ☐ 無効 ☒ 有効

SSID: WIRELESSLAN-0

VLAN ID: 0

ANY接続拒否: ☒ 無効 ☐ 有効

接続端末制限: 63

同一仮想AP内の端末間通信禁止: ☒ 無効 ☐ 有効

アカウントिंग: ☒ 無効 ☐ 有効

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

暗号化方式: WEP RC4 128 (104)

キージェネレーター: RETSAMEVAWNAL

WEPキー: RETSAMEVAWNAL

半角英数で13文字、もしくは16進数で26桁を入力

登録 取消

① 選択する

② 入力する

3 <登録>をクリックします。

2 導入ガイド

1. 無線LAN接続[基本編]

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ [WEP RC4]暗号化を設定するには(つづき)

暗号鍵(キー)を生成するには

無線LAN1 (2.4GHz帯)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LAN設定」メニューの「無線LAN1」、「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)

仮想AP設定

インターフェース: ath0

仮想AP: ☐ 無効 ☒ 有効

SSID: WIRELESSLAN-0

VLAN ID: 0

ANY接続拒否: ☒ 無効 ☐ 有効

接続端末制限: 63

同一仮想AP内の端末間通信禁止: ☒ 無効 ☐ 有効

アカウントिंग: ☒ 無効 ☐ 有効

MAC認証: ☒ 無効 ☐ 有効

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

暗号化方式: WEP RC4 128 (104)

キージェネレーター: ICOM

WEPキー:

半角英数字で13文字、もしくは16進数で26桁を入力

登録 取消

3 「登録」をクリックします。

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。

2 導入ガイド

1. 無線LAN接続[基本編]

■ [WEP RC4]暗号化を設定するには(つづき)

暗号鍵(キー)値の設定例

弊社製ワイヤレスLANユニットなどに付属の設定ユーティリティで本製品に接続する場合は、下記の設定例を参考にしてください。

※「WEP RC4 128(104)」ビットの暗号化方式を使用して、「486F7473706F744C6363657373」(16進数(26桁))の暗号鍵(キー)で本製品と無線LAN端末の両方に直接入力する場合を例に説明します。

本製品と無線LAN端末で暗号鍵(キー)値が異なる場合は、通信できません。

AP-95M側	弊社製無線LAN端末側
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: WEP RC4 128 (104) キージェネレーター: WEPキー: 486F7473706F744C6363657373 半角英数で13文字、もしくは16進数で26桁を入力	キーインデックス: 1 WEPキー: ☒ 16進数入力 ☐ ASCII文字入力 キー1: 48-6F-74-73-70-6F-74-4C-63-63-65-73-73

キーインデックス「1」のWEPキー(値)が本製品と同じため通信できます。

※キー1の暗号鍵(キー)がデータの送信と受信に使用されます。

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。

※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。

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)や記号などを長く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。

2 導入ガイド

1. 無線LAN接続[基本編]

無線LAN設定 > 無線LAN1/無線LAN2 > MACアドレスフィルタリング

■ MACアドレスフィルタリングを設定するには

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。

※無線LAN1(2.4GHz帯)の仮想AP(例: ath0)を例に、接続を許可する無線LAN端末の登録を説明します。

1 「無線LAN設定」メニューの「無線LAN1」、「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。

登録済みの端末	受信中の端末	通信状況	
		通信不許可	② 追加
		通信中	削除
00-90-C7-00-00-10		登録済	削除

① 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)が表示されます。

「通信不許可」: MACアドレスフィルタリング設定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。

② 〈追加〉/〈削除〉

表示されている無線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。

2 導入ガイド

1. 無線LAN接続[基本編]

無線LAN設定 > 無線LAN1/無線LAN2 > 無線LAN

■ 自動チャンネルを設定するときは

本製品の設定画面でチャンネルを「自動」に設定すると、ほかの無線LAN機器からの電波干渉が少ないチャンネルに自動で設定します。

※「自動」が選択できるのは、20MHz帯域幅だけです。

※「自動」に設定した場合、設定画面上で使用中のチャンネルを確認できます。

「無線LAN設定」メニューの設定内容を変更し、〈登録〉をクリックすると、再度使用するチャンネルをスキャンします。

※ 本製品の起動時に、DFS機能が無効なチャンネルが選択された場合は、その後、運用中に別のチャンネルに変更されることはありません。

ただし、DFS機能が有効な5.3/5.6GHz帯のチャンネル(052～140)が選択された場合は、運用中でもレーダーを検出すると、さらにチャンネルが変更されることがあります。

※ チャンネル自動設定と、RS-AP3(弊社製無線アクセスポイント管理ツール)やRC-AP10(弊社製無線LANコントローラー)は併用できません。

2.4GHz帯の場合

1 「無線LAN設定」メニューの「無線LAN1」、「無線LAN」の順にクリックします。

2 [チャンネル]欄で「自動」を選択し、〈登録〉をクリックします。 (出荷時の設定：001CH (2412 MHz))

無線LAN

無線UNIT: ☐ 無効 ☒ 有効

帯域幅: 20 MHz

チャンネル: 自動

パワーレベル: 高

DTIM間隔: 1

プロテクション: ☐ 無効 ☒ 有効

登録

①選択する

②クリック

③確認する

使用中チャンネル: 006 CH (2437 MHz)

登録 取消

2 導入ガイド

1. 無線LAN接続[基本編]

無線LAN設定 > 無線LAN1/無線LAN2 > 無線LAN

■ 自動チャンネルを設定するときは(つづき)

5GHz帯の場合

- 1 「無線LAN設定」メニューの「無線LAN2」、「無線LAN」の順にクリックします。
- 2 [チャンネル]欄で「自動」を選択し、〈登録〉をクリックします。 (出荷時の設定：036CH (5180MHz))

The image shows two screenshots of the '無線LAN' (Wireless LAN) settings page. The top screenshot shows the initial state with '無線UNIT' set to '有効' (Enabled), '帯域幅' (Channel Width) set to '20 MHz', 'チャンネル' (Channel) set to '自動' (Auto), 'パワーレベル' (Power Level) set to '高' (High), 'DTIM間隔' (DTIM Interval) set to '1', and 'プロテクション' (Protection) set to '有効' (Enabled). A blue box highlights the 'チャンネル' dropdown menu, and a blue arrow points to it with the text '出荷時の設定であることを確認します。' (Confirm the factory setting). A label '① 選択する' (1 Select) points to the 'チャンネル' dropdown. A label '② クリック' (2 Click) points to the '登録' (Register) button. The bottom screenshot shows the same page after the 'チャンネル' dropdown has been opened and '自動' (Auto) has been selected. A label '③ 確認する' (3 Confirm) points to the '自動' option. The '使用中チャンネル: 100 CH (5500 MHz)' is displayed below the '自動' option. The '登録' (Register) and '取消' (Cancel) buttons are visible at the bottom right.

屋外で使用する時のご注意

5.2/5.3GHz帯無線LANの使用は、電波法により、屋内に限定されています。

屋外で5GHz帯をご利用になる場合は、手動で5.6GHz帯のチャンネル(100～140)に設定してご使用ください。

2 導入ガイド

1. 無線LAN接続 [基本編]

無線LAN設定 > 無線LAN2 > 無線LAN

■ 80MHz帯域幅通信をするときは

IEEE802.11ac規格を使用できるのは、無線LAN2(5GHz帯)で暗号化設定を「なし」、または「AES」に設定したときだけです。さらに、最大867bps (理論値)で使用するには、帯域幅を「80MHz」に設定してください。

※暗号化設定が「WEP RC4」、または「TKIP」の場合は、IEEE802.11a規格で通信します。

1 「無線LAN設定」メニューの「無線LAN2」、「無線LAN」の順にクリックします。

2 「帯域幅」欄で「80MHz」を選択します。 (出荷時の設定：20MHz)

無線LAN

無線UNIT: ☐ 無効 ☒ 有効

帯域幅: 80 MHz

チャンネル: 036 CH (5180 MHz)

パワーレベル: 高

DTIM間隔: 1

プロテクション: ☐ 無効 ☒ 有効

登録 取消

選択する

3 「登録」をクリックします。

40/80MHz帯域幅通信をするときの手引き

◎無線LAN通信で40MHz、または80MHz帯域幅をご使用になる場合、周囲の電波環境を事前に確認して、ほかの無線局に電波干渉を与えないようにしてください。

◎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」欄を「20MHz」(出荷時の設定)でご使用ください。

2 導入ガイド

1. 無線LAN接続 [基本編]

無線LAN設定 > WPS

■ WPS機能で自動設定したいSSIDと共有鍵(キー)を指定する

あらかじめ本製品で使用する仮想APIに設定したSSIDと共有鍵(キー)を、WPS機能でWPS機能対応無線LAN端末に自動設定する手順を説明します。

※ネットワーク名(SSID)と暗号化の設定については、2-2ページをご覧ください。

※WPS機能で利用できるネットワーク認証は、「WPA-PSK」、「WPA2-PSK」です。

WPS機能を有効にする

「プッシュボタン方式」を例に説明します。(P.3-114)

※WPS機能を有効にすると、「WPS」画面に「開始」が表示されます。

1 「無線LAN設定」メニュー、「WPS」の順にクリックします。

2 WPS機能を使用する仮想AP (例: ath0)を選択し、「登録」をクリックします。 (出荷時の設定: なし)

WPS設定

使用するインターフェース: ath0

登録 取消

① 選択する

② クリック

3 「WPS」画面の[WPS状態]欄を確認します。

WPS設定

使用するインターフェース: ath0

登録 取消

WPS開始

WPS方式: ☒ プッシュボタン方式 ☐ PIN方式

プッシュボタン方式: 開始

WPS状態表示

WPS状態表示: 設定済

SSID: ICOM

ネットワーク認証: WPA-PSK/WPA2-PSK

暗号化方式: AES

PSK: wirelessmaster

確認する

あらかじめ仮想APIに設定しておいた内容が表示されます。

(次ページにつづく)

2 導入ガイド

1. 無線LAN接続 [基本編]

無線LAN設定 > WPS

■ WPS機能で自動設定したいSSIDと共有鍵(キー)を指定する(つづき)

WPS機能で無線LAN端末を自動設定する

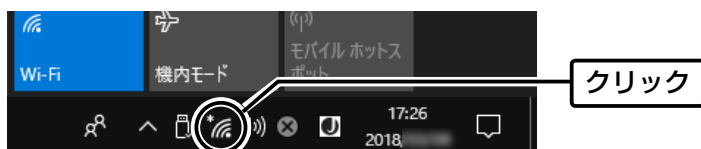
無線LAN端末は、WPS対応のものをご用意ください。

本書では、Windows 10での接続を例に、WPS機能で無線LAN端末を自動設定する手順を説明します。

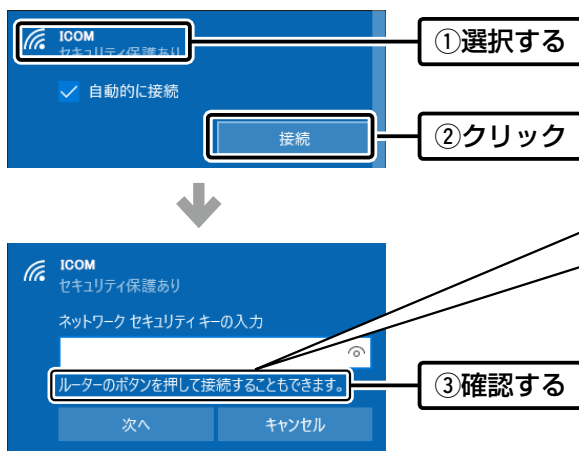
※ 無線LAN端末側の操作について詳しくは、お使いになる端末の取扱説明書をご覧ください。

※ [MODE]ランプが $\odot$ 緑点滅し、設定できない場合は、[使用するインターフェース]欄を「なし」に戻してから、手動で設定してください。(P.2-13)

- 1 無線LAN端末側で、通知領域(タスクトレイ)に表示されているネットワークアイコンをクリックします。

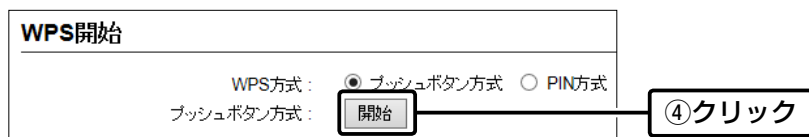


- 2 本製品に設定されたSSID (例：ICOM)を選択し、〈接続〉をクリックします。
「ネットワーク セキュリティ キーの入力」画面が表示されます。

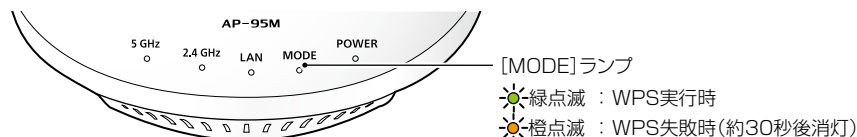


「ルーターのボタンを押して接続することもできます。」と表示されない場合は、本製品側のWPS設定、ご使用のパソコンや無線LAN端末のWPS機能が正しく動作しているか確認してください。
※この画面では、何も入力せずに、手順3に進みます。
※手順3の操作で接続できない場合は、手順2で「ネットワーク セキュリティ キー」を入力し、〈次へ〉をクリックしてください。

- 3 「WPS」画面の〈開始〉をクリックします。
[MODE]ランプがゆっくり $\odot$ 緑点滅します。



- 4 [2.4GHz]ランプ、または[5GHz]ランプが $\bullet$ 緑点灯になると、設定完了です。



2 導入ガイド

2. 無線LAN接続[活用編]

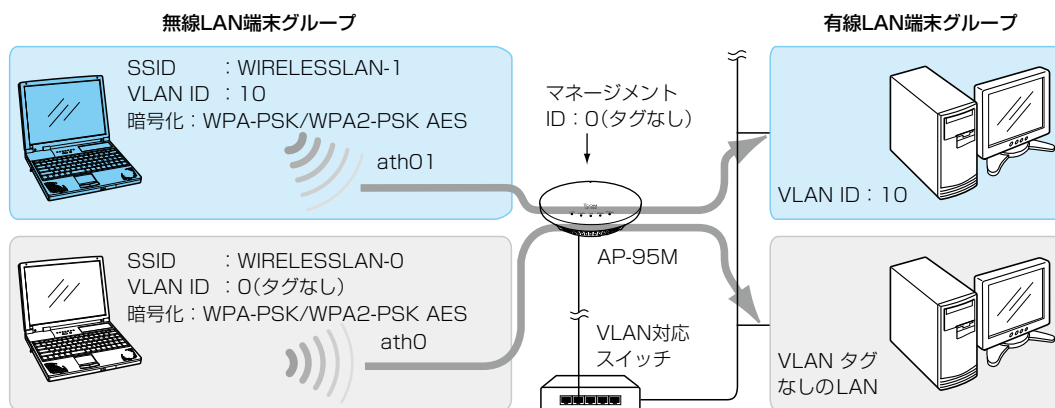
無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ 仮想APを設定するには

次の条件で、図の ■ 色で示す仮想AP (ath01) を設定する場合を例に説明します。

※各仮想APのVLAN機能とルーター機能は併用できません。

[仮想AP設定] 項目	インターフェース	: 「ath01」
	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機能について」をご覧ください。(P.1-7)

1 「無線LAN設定」メニューの「無線LAN1」、「仮想AP」の順にクリックします。

2 [インターフェース] 欄で「ath01」を選択し、上記の設定例にしたがって設定します。

The screenshot shows the configuration interface. The '仮想AP設定' (Virtual AP Settings) section includes: 'インターフェース' (Interface) set to 'ath01' (callout 1: ① 選択する); '仮想AP' (Virtual AP) set to '有効' (Enabled) (callout 2: ② クリック); 'SSID' set to 'WIRELESSLAN-1' (callout 3: ③ 入力する, with a note '出荷時の設定であることを確認します。'); 'VLAN ID' set to '10'; 'ANY接続拒否' (ANY connection refusal) set to '無効' (Disabled); '接続端末制限' (Connection terminal limit) set to '63'; '同一仮想AP内の端末間通信禁止' (Prohibit communication between terminals in the same virtual AP) set to '無効' (Disabled); 'アカウントing' (Accounting) set to '無効' (Disabled); and 'MAC認証' (MAC authentication) set to '無効' (Disabled). The '暗号化設定' (Encryption Settings) section includes: 'ネットワーク認証' (Network authentication) set to 'WPA-PSK/WPA2-PSK' (callout 4: ④ 選択する); '暗号化方式' (Encryption method) set to 'AES' (callout 5: ⑤ 入力する); 'PSK (Pre-Shared Key)' set to 'RETSAMEVAWNAL' (callout 6: ⑥ クリック); and 'WPAキー更新間隔' (WPA key update interval) set to '120' minutes. There are '登録' (Register) and 'キャンセル' (Cancel) buttons at the bottom right.

2 導入ガイド

2. 無線LAN接続[活用編]

無線LAN設定 > 無線LAN1/無線LAN2 > AP間通信 (WBR)

■ 無線AP間通信機能(WBR)を使用する場合

次の条件で、2台の本製品(図：親機の仮想AP「ath0」と子機)を設定する場合を例に説明します。

※使用条件については、「無線AP間通信機能(WBR)について」をご覧ください。(P.1-6)

※親機側でDFS機能が有効なチャンネルが選択されているとき、または「自動」を設定した場合(P.2-10)、無線AP間通信機能は動作しません。(5GHz帯で無線AP間通信が利用できるのは5.2GHz帯のみ)

※子機は自動的に親機のチャンネルになります。

本書では、「001CH (2412MHz)」(無線LAN1)で使用する場合を例にしています。

※無線AP間通信機能を設定すると、子機の仮想AP「ath07」(無線LAN1)、「ath17」(無線LAN2)は使用できなくなります。

※本製品のIPアドレスは、「本体IPアドレスを変更する」で設定されているものとします。(P.1-22)

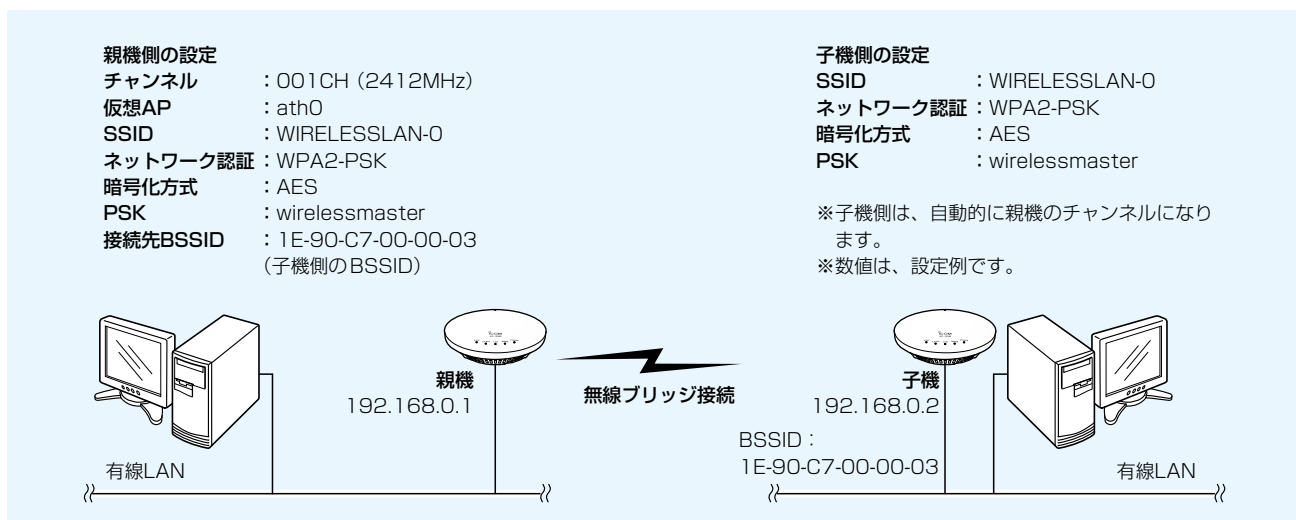
親機(P.2-17)

[無線LAN設定]項目	チャンネル	: 「001CH (2412MHz)」(出荷時の設定)
[仮想AP設定]項目	インターフェース	: 「ath0」 ※親機側の仮想AP「ath0」(無線LAN1)、「ath1」(無線LAN2)に設定されたSSIDと暗号化を使用して、無線AP間通信をします。
	仮想AP	: 「有効」(出荷時の設定)
	SSID	: 「WIRELESSLAN-0」(出荷時の設定)
[暗号化設定]項目	ネットワーク認証	: 「WPA2-PSK」
	暗号化方式:	: 「AES」
	PSK (Pre-Shared Key)	: 「wirelessmaster」
[AP間通信設定]項目	AP間通信	: 「有効」
	動作モード	: 「親機」
	インターフェース	: 「wbr0」
	接続先BSSID	: 「1E-90-C7-00-00-03」(子機のBSSID) ※子機側の「AP間通信 (WBR)」画面でAP間通信を「有効」にすると確認できます。

子機(P.2-19)

[AP間通信設定]項目	AP間通信	: 「有効」
	動作モード	: 「子機」
[子機設定]項目	SSID	: 「WIRELESSLAN-0」(出荷時の設定)
	ネットワーク認証	: 「WPA2-PSK」
	暗号化方式:	: 「AES」
	PSK (Pre-Shared Key)	: 「wirelessmaster」

※子機のインターフェースは、「wbr16」(無線LAN1)、「wbr17」(無線LAN2)から変更できません。



2 導入ガイド

2. 無線LAN接続[活用編]

無線LAN設定 > 無線LAN1/無線LAN2 > AP間通信 (WBR)

■ 無線AP間通信機能(WBR)を使用する場合(つづき)

親機を設定する

無線AP間通信で使用する親機側を、次の手順で設定します。

1 「無線LAN設定」メニューの「無線LAN1」、「仮想AP」の順にクリックします。

2 設定条件にしたがって、親機側の仮想AP「ath0」を設定します。

仮想AP設定

インターフェース: ath0

仮想AP: ☐ 無効 ☒ 有効

SSID: WIRELESSLAN-0

VLAN ID: 0

ANY接続拒否: ☒ 無効 ☐ 有効

接続端末制限: 63

同一仮想AP内の端末間通信禁止: ☒ 無効 ☐ 有効

アカウントティング: ☒ 無効 ☐ 有効

MAC認証: ☒ 無効 ☐ 有効

暗号化設定

ネットワーク認証: WPA2-PSK

暗号化方式: AES

PSK (Pre-Shared Key): wirelessmaster

WPAキー更新間隔: 120 分

登録

AP-95Mの無線AP間通信で利用できる親機側の仮想APIは「ath0」(無線LAN1)、「ath1」(無線LAN2)だけです。

出荷時の設定であることを確認します。

① 選択する

② 入力する

③ クリック

3 「無線LAN設定」メニューの「無線LAN1」、「AP間通信 (WBR)」の順にクリックします。

4 設定条件にしたがって、親機側のAP間通信を設定します。

AP間通信設定

AP間通信: ☐ 無効 ☒ 有効

動作モード: 親機

親機設定

インターフェース: wbr0

接続先BSSID: 1E-90-C7-00-00-03

登録

子機のBSSIDを親機側に登録します。

① クリック

② 選択する

③ 確認する

④ 入力する

⑤ クリック

(次ページにつづく)

2 導入ガイド

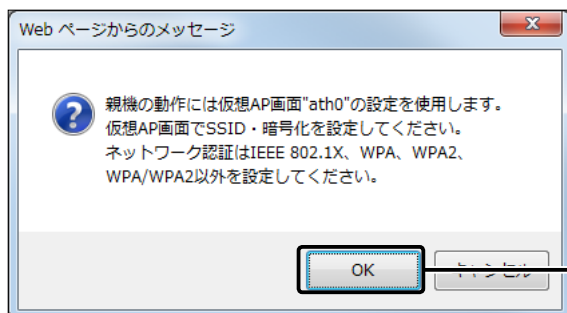
2. 無線LAN接続[活用編]

無線LAN設定 > 無線LAN1/無線LAN2 > AP間通信 (WBR)

■ 無線AP間通信機能(WBR)を使用する場合(つづき)

親機を設定する

5 <OK>をクリックします。



※無線LAN1では、親機側の仮想AP「ath0」に設定されたSSIDと暗号化を使用して、無線AP間通信をします。
※子機側は、SSIDと暗号化が一致する親機をスキャンします。

6 [AP間通信設定一覧] 項目の登録内容を確認します。

AP間通信設定一覧		
インターフェース	BSSID	
wbr0	1E-90-C7-00-00-03	削除
wbr1		
wbr2		
wbr3		
wbr4		
wbr5		
wbr6		
wbr7		

確認する

2 導入ガイド

2. 無線LAN接続[活用編]

無線LAN設定 > 無線LAN1/無線LAN2 > AP間通信 (WBR)

■ 無線AP間通信機能(WBR)を使用する場合(つづき)

子機を設定する

無線AP間通信で使用する子機側を、次の手順で設定します。

※ 親機側の仮想AP「ath0」(無線LAN1)、「ath1」(無線LAN2)に設定されたSSIDと暗号化を使用して、無線AP間通信をします。

※ 子機側は、SSIDと暗号化が一致する親機をスキャンします。

スキャン中の子機では、無線AP間通信で使用する無線LAN1ユニットの仮想APすべてが一時的に無効になります。

※ 無線AP間通信機能を設定すると、子機の仮想AP「ath07」(無線LAN1)、「ath17」(無線LAN2)は使用できなくなります。

1 「無線LAN設定」メニューの「無線LAN1」、「AP間通信 (WBR)」の順にクリックします。

2 設定条件にしたがって、子機側の暗号化を設定します。

AP間通信設定

AP間通信: ☐ 無効 ☒ 有効

動作モード: 子機

子機設定

BSSID: 1E-90-C7-00-00-03

インターフェース: wbr16

SSID: WIRELESSLAN-0

ネットワーク認証: WPA2-PSK

暗号化方式: AES

PSK (Pre-Shared Key): wirelessmaster

登録 取消

①クリック

②選択する

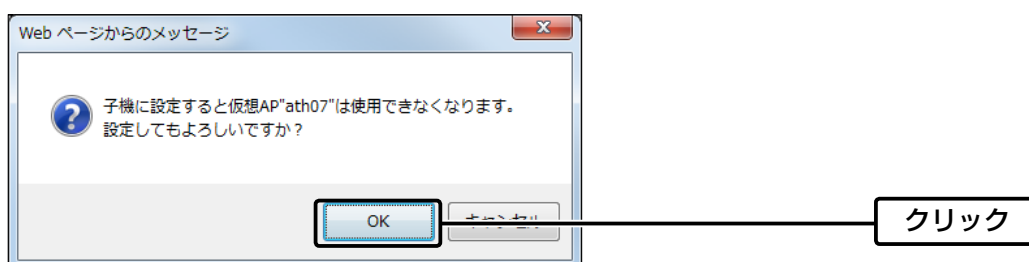
③確認する

④選択する

⑤入力する

⑥クリック

3 <OK>をクリックします。



2 導入ガイド

2. 無線LAN接続[活用編]

無線LAN設定 > 無線LAN1/無線LAN2 > AP間通信 (WBR)

管理 > 管理ツール

■ 無線AP間通信で使用する本製品をRS-AP3やRC-AP10で管理するときは

- ① 本製品の設定画面(無線LAN1、または無線LAN2)で無線AP間通信機能を設定して、あらかじめ通信できる状態にしておいてください。
- ② 本製品の設定画面で、管理ツール設定を「有効」にします。
- ③ 管理を開始する前に、本製品で設定した内容を、RS-AP3やRC-AP10の「個別設定」画面、「共通設定」画面★に設定してください。
★「共通設定」画面の仮想APで、無線AP間通信機能で使用する親機のSSIDと暗号化を設定してください。

例：RS-AP3

親機の「個別設定」画面

□ AP間通信(WBR)	
AP間通信	有効
動作モード	親機
接続先BSSID (wbr0)	1E-90-C7-00-00-03
接続先BSSID (wbr1)	
接続先BSSID (wbr2)	
接続先BSSID (wbr3)	
接続先BSSID (wbr4)	
接続先BSSID (wbr5)	
接続先BSSID (wbr6)	
接続先BSSID (wbr7)	

子機の「個別設定」画面

□ AP間通信(WBR)	
AP間通信	有効
動作モード	子機
□ インターフェイス wbr16	
SSID	WIRELESSLAN-0
ネットワーク認証	WPA2-PSK
暗号化方式	AES
PSK (Pre-Shared Key)	wirelessmaster
□ 無線 2	
無線UNIT	共通設定を使用
無線動作モード	共通設定を使用

「共通設定」画面

□ 仮想AP	
□ インターフェイス ath0	
仮想AP	有効
SSID	WIRELESSLAN-0
VLAN ID	0
ANY接続拒否	無効
接続端末制限	63
アカウントing	無効
MAC認証	無効
□ 暗号化設定	
ネットワーク認証	WPA2-PSK
暗号化方式	AES
PSK (Pre-Shared Key)	wirelessmaster
WPAキー更新間隔(分)	120

RS-AP3やRC-AP10で管理するときの注意

- ◎管理を終了するまで、本製品のWAN側(ルーター設定)を変更できません。
- ◎ルーター機能をご使用になる場合は、回線種別を「固定IP」に設定し、あらかじめWAN側IPアドレスに固定IPアドレスを設定してください。
- ※回線種別を「DHCPクライアント」に設定してご使用になる場合は、DHCPサーバー側で静的DHCPサーバー機能などを利用し、常に同じIPアドレスが付与されるようにネットワーク環境を構築してください。
- ※回線種別が「PPPoE」に設定されているときは、RS-AP3やRC-AP10で本製品を管理できません。
- ◎RS-AP3とRC-AP10は、設定を同期できません。

2 導入ガイド

2. 無線LAN接続[活用編]

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ アカウンティング設定について

通信する無線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、仮想APごとにアカウンティングサーバーの設定が必要です。

無線LAN1 (2.4GHz帯)の仮想AP「ath03」で個別設定する場合を例に説明します。

1 「無線LAN設定」メニューの「無線LAN1」、「仮想AP」の順にクリックします。

2 設定する仮想APを選択し、「アカウンティング」欄を「有効」にします。 (出荷時の設定：無効)

仮想AP設定

インターフェース: ath03

仮想AP: ☐ 無効 ☒ 有効

SSID: WIRELESSLAN-3

VLAN ID: 0

ANY接続拒否: ☒ 無効 ☐ 有効

接続端末制限: 63

同一仮想AP内の端末間通信禁止: ☒ 無効 ☐ 有効

アカウンティング: ☐ 無効 ☒ 有効

MAC認証: ☒ 無効 ☐ 有効

① 選択する

② 選択する

③ 選択する

3 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。

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:

ポート: 1813 1813

シークレット: secret secret

登録 キャンセル

① 設定する

② クリック

2 導入ガイド

2. 無線LAN接続[活用編]

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ MAC認証サーバー(RADIUS)設定について

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、仮想APごとにRADIUSサーバーの設定が必要です。

※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で使用できます。

※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、ユーザー名とパスワードは、「00ab12cd34ef」(半角英数字(小文字))になります。

無線LAN1(2.4GHz帯)の仮想AP「ath03」で個別設定する場合を例に説明します。

1 「無線LAN設定」メニューの「無線LAN1」、「仮想AP」の順にクリックします。

2 設定する仮想APを選択し、[MAC認証]欄を「有効」にします。(出荷時の設定：無効)

仮想AP設定

インターフェース: ath03

仮想AP: ☐ 無効 ☒ 有効

SSID: WIRELESSLAN-3

VLAN ID: 0

ANY接続拒否: ☒ 無効 ☐ 有効

接続端末制限: 63

同一仮想AP内の端末間通信禁止: ☒ 無効 ☐ 有効

アカウントিং: ☒ 無効 ☐ 有効

MAC認証: ☐ 無効 ☒ 有効

認証VLAN: ☒ 無効 ☐ 有効

①選択する

②選択する

③選択する

3 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。

MAC認証サーバー (RADIUS) 設定

プライマリー セカンダリー

アドレス:

ポート: 1812 1812

シークレット: secret secret

①設定する

暗号化方式: none

登録

②クリック

2 導入ガイド

2. 無線LAN接続[活用編]

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ 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、仮想APごとにRADIUSサーバーの設定が必要です。

※EAP認証の対応については、ご使用になるRADIUSサーバーや無線LAN端末の説明書をご覧ください。

無線LAN1(2.4GHz帯)の仮想AP「ath03」で個別設定する場合を例に説明します。

- 1 「無線LAN設定」メニューの「無線LAN1」、「仮想AP」の順にクリックします。
- 2 設定する仮想APを選択し、ネットワーク認証と暗号化方式を設定します。(例：WPA2認証)

仮想AP設定

インターフェース: ath03

仮想AP: ☐ 無効 ☒ 有効

SSID: WIRELESSLAN-3

VLAN ID: 0

ANY接続拒否: ☒ 無効 ☐ 有効

接続端末制限: 63

同一仮想AP内の端末間通信禁止: ☒ 無効 ☐ 有効

アカウンティング: ☒ 無効 ☐ 有効

MAC認証: ☒ 無効 ☐ 有効

認証VLAN: ☒ 無効 ☐ 有効

暗号化設定

ネットワーク認証: WPA2

暗号化方式: AES

WPAキー更新間隔: 120 分

① 選択する

② 選択する

③ 選択する

- 3 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。

RADIUS設定

	プライマリー	セカンダリー
アドレス:		
ポート:	1812	1812
シークレット:	secret	secret

登録 削除

① 設定する

② クリック

2. 無線LAN接続[活用編]

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ 認証VLANについて

認証VLAN有効時、RADIUSサーバーを利用した認証結果(応答属性)に応じて、無線LAN端末の所属VLAN IDをグループ分けできます。

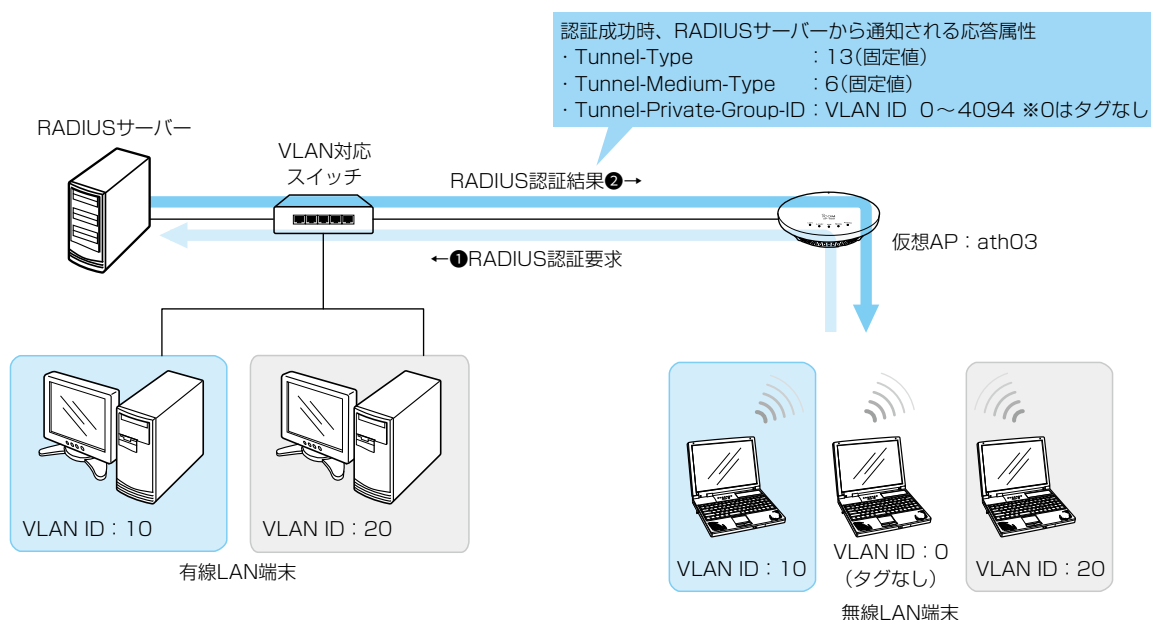
※使用するためには、仮想APごとにRADIUSサーバーの設定が必要です。

※「仮想AP」画面の[仮想AP設定]項目でMAC認証を有効にする、または[暗号化方式]項目でネットワーク認証(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。(P.2-25)

※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。

※RS-AP3やRC-AP10のMAC認証サーバー(簡易RADIUS)では、本機能は使用できません。(応答属性非対応のため)



※説明に使用している各端末のVLAN IDや仮想APは設定例です。

※認証VLAN機能利用時、同一仮想AP内(例: ath03)における同報系通信は、所属VLANグループに関係なく通知されます。

ご参考に

無線LAN端末の所属VLAN IDは、「無線LAN情報」画面の[端末情報]項目の〈詳細〉をクリックすると、確認できます。(P.3-9)

2 導入ガイド

2. 無線LAN接続[活用編]

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ 認証VLANについて(つづき)

MAC認証を利用するときは

「仮想AP」画面の「仮想AP設定」項目で、MAC認証と認証VLANを有効にします。

仮想AP設定

インターフェース:	ath03
仮想AP:	☐ 無効 ☒ 有効
SSID:	WIRELESSLAN-3
VLAN ID:	0
ANY接続拒否:	☒ 無効 ☐ 有効
接続端末制限:	63
同一仮想AP内の端末間通信禁止:	☒ 無効 ☐ 有効
アカウンティング:	☒ 無効 ☐ 有効
MAC認証:	☐ 無効 ☒ 有効
認証VLAN:	☐ 無効 ☒ 有効

① 選択する

② 選択する

※MAC認証をするときのRADIUSサーバー設定は、2-22ページをご覧ください。

※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で使用できます。

※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、ユーザー名とパスワードは、「00ab12cd34ef」(半角英数字(小文字))になります。

ネットワーク認証(WPA/WPA2/IEEE802.1X)を利用するときは

「仮想AP」画面の「暗号化設定」項目でネットワーク認証と暗号化方式を設定し、「仮想AP設定」項目で認証VLANを有効にします。
(例：WPA2認証)

仮想AP設定

インターフェース:	ath03
仮想AP:	☐ 無効 ☒ 有効
SSID:	WIRELESSLAN-3
VLAN ID:	0
ANY接続拒否:	☒ 無効 ☐ 有効
接続端末制限:	63
同一仮想AP内の端末間通信禁止:	☒ 無効 ☐ 有効
アカウンティング:	☒ 無効 ☐ 有効
MAC認証:	☒ 無効 ☐ 有効
認証VLAN:	☐ 無効 ☒ 有効

② 確認する

暗号化設定

ネットワーク認証:	WPA2
暗号化方式:	AES
WPAキー更新間隔:	120 分

① 設定する

※ネットワーク認証をするときのRADIUSサーバー設定は、2-23ページをご覧ください。

※EAP認証の対応については、ご使用になるRADIUSサーバーや無線LAN端末の説明書をご覧ください。

設定画面について

第 3 章

この章では、
各メニューで表示される設定画面について説明します。

「TOP」画面	3-5
■ システム情報	3-5
■ MACアドレス	3-5
■ WANステータス	3-5

情報表示

「ネットワーク情報」画面	3-6
■ インターフェース	3-6
■ Ethernetポート接続情報	3-6
■ 無線LAN	3-7
■ AP間通信 (WBR)	3-7
■ DHCPリース情報	3-7
「SYSLOG」画面	3-8
■ SYSLOG	3-8
「無線LAN情報」画面	3-9
■ アクセスポイント情報	3-9
■ 端末情報	3-9
■ 通信端末詳細情報	3-10
■ AP間通信情報	3-11
■ AP間通信詳細情報	3-11

ネットワーク設定

「IPアドレス」画面	3-12
■ 本体名称	3-12
■ VLAN設定	3-12
■ IPアドレス設定	3-13
「DHCPサーバー」画面	3-14
■ DHCPサーバー設定	3-14
■ 静的DHCPサーバー設定	3-16
■ 静的DHCPサーバー設定一覧	3-16
「スタティックルーティング」画面	3-17
■ IP経路情報	3-17
■ スタティックルーティング設定	3-18
■ スタティックルーティング設定一覧	3-18
「ポリシールーティング」画面	3-19
■ 送信元ルーティング設定	3-19
■ 送信元ルーティング設定一覧	3-19
「パケットフィルタ」画面	3-20
■ パケットフィルタ設定	3-20
■ パケットフィルタ設定一覧	3-32
パケットフィルタの使用例について	3-33
① 異なる仮想AP(例:ath0/ath01)の端末同士の通信を禁止するには	3-34
② AP-95M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	3-35
③ 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	3-36

3 設定画面について

下記は、前ページからの「つづき」です。

「Web認証 基本」画面	3-37
■ Web認証	3-37
■ カスタムページの作成について	3-39
「Web認証 詳細」画面	3-43
■ Web認証方法	3-43
■ RADIUS設定	3-44
■ ローカルリスト	3-45
■ 現在の登録	3-45
「POPCHAT@Cloud」画面	3-46
■ アカウント設定	3-46
■ インターフェース設定	3-47

ルーター設定

「WAN接続先」画面	3-48
■ 回線状態表示 (DHCPクライアント設定時)	3-48
■ 回線状態表示 (固定IP設定時)	3-49
■ 回線状態表示 (PPPoE設定時)	3-50
■ 回線種別設定	3-51
■ 回線設定 (DHCPクライアント設定時)	3-52
■ 回線設定 (固定IP設定時)	3-53
■ 回線設定 (PPPoE設定時)	3-54
■ 回線設定一覧 (PPPoE設定時)	3-56
「アドレス変換」画面	3-57
■ アドレス変換設定	3-57
■ DMZホスト設定	3-57
■ 静的マスカレードテーブル設定	3-58
■ 静的マスカレードテーブル設定	3-58
「IPフィルター」画面	3-59
■ 一般設定	3-59
■ IPフィルター設定	3-60
■ IPフィルター設定一覧	3-66
「簡易DNS」画面	3-67
■ 簡易DNSサーバー設定	3-67
■ 簡易DNSサーバー設定	3-67

3 設定画面について

下記は、前ページからの「つづき」です。

無線LAN設定

「無線LAN設定」画面	3-68
■ 無線LAN	3-68
「仮想AP」画面	3-70
■ 仮想AP設定	3-70
■ MAC認証サーバー(RADIUS)設定	3-75
■ 暗号化設定	3-76
■ RADIUS設定	3-83
■ アカウンティング設定	3-84
「MACアドレスフィルタリング」画面	3-85
■ MACアドレスフィルタリング設定	3-85
■ 端末MACアドレスリスト	3-86
■ MACアドレスフィルタリング設定一覧	3-87
「ネットワーク監視」画面	3-88
■ ネットワーク監視設定	3-88
「AP間通信 (WBR)」画面	3-90
■ AP間通信設定	3-90
■ 親機設定	3-91
■ AP間通信設定一覧	3-92
■ 子機設定	3-93
「WMM詳細」画面	3-97
■ WMM詳細設定	3-97
■ WMMパワーセーブ設定	3-101
「レート」画面	3-102
■ レート設定	3-102
■ プリセットされた各レート設定	3-104
■ 通信レートの各設定について	3-106
■ MCS値ごとの通信レートについて	3-107
■ 仮想AP共通設定	3-108
「ARP代理応答」画面	3-109
■ ARP代理応答設定	3-109
■ ARPキャッシュ情報	3-111
IP Advanced Radio Systemについて	3-112
「WPS」画面	3-113
■ WPS設定	3-113
■ WPS開始	3-114
■ WPS状態表示	3-115
「災害用仮想AP」画面	3-116
■ 災害用仮想AP	3-116

3 設定画面について

下記は、前ページからの「つづき」です。

管理

「管理者」画面	3-117
■ 管理者パスワードの変更	3-117
「管理ツール」画面	3-118
■ 無線アクセスポイント管理ツール設定	3-118
■ HTTP/HTTPS設定	3-119
■ HTTP/HTTPS設定後、設定画面にアクセスできなくなったときは	3-120
■ Telnet/SSH設定	3-121
「時計」画面	3-123
■ 時刻設定	3-123
■ 自動時計設定	3-124
■ SNTPサーバー設定	3-125
「SYSLOG」画面	3-126
■ SYSLOG設定	3-126
「SNMP」画面	3-127
■ SNMP設定	3-127
■ SNMPv3設定	3-128
「LED」画面	3-129
■ LED消灯モード	3-129
「ネットワークテスト」画面	3-130
■ PINGテスト	3-130
■ 経路テスト	3-131
「再起動」画面	3-132
■ 再起動	3-132
「設定の保存/復元」画面	3-133
■ 設定の保存	3-133
■ 設定の復元	3-133
■ 設定内容一覧	3-134
「初期化」画面	3-135
■ 初期化	3-135
「ファームウェアの更新」画面	3-136
■ ファームウェア情報	3-136
■ オンライン更新	3-137
■ 自動更新	3-138
■ 手動更新	3-139

3 設定画面について

「TOP」画面

TOP

■ システム情報

ファームウェアのバージョン情報、国名コード、時刻、稼働時間、メモリー使用量が表示されます。

システム情報	
本体名称	XXXXXXXXXX
バージョン	XXXXXXXXXX
国名コード	JP
現在時刻	20 年 月 日 6:04:18
稼働時間	0 day 06:05:03
メモリー使用量	144200 kB / 236180 kB (61% 使用中)

TOP

■ MACアドレス

本製品のMACアドレス(LAN/無線)が表示されます。

MACアドレス	
LAN	00-90-C7-XXXXXX
無線1	00-90-C7-XXXXXX
無線2	00-90-C7-XXXXXX

※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(00-90-C7-XX-XX-XX)で表示されています。

TOP

■ WANステータス

「ルーター設定」メニューの「WAN接続先」画面で設定したWAN側回線への接続状態が表示されます。

※下図は、出荷時の状態です。

WANステータス	
回線種別	LANポートとして使用する
接続先名	
接続状態	
IPアドレス	
デフォルトゲートウェイ	
DNSサーバー	

3 設定画面について

「ネットワーク情報」画面

情報表示 > ネットワーク情報

■ インターフェース

「ネットワーク設定」メニュー→「スタティックルーティング」画面→[IP経路情報]項目に表示された[経路]について、その詳細が表示されます。

インターフェース		
インターフェース	IPアドレス	サブネットマスク
br-lan	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が表示されます。

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
LAN	00-90-C7-XXXXXX	100BASE-TX full-duplex

※本製品の[LAN]ポートは、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)」に設定することで、通信に最適な速度、モードが自動選択されます。

※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。

3 設定画面について

「ネットワーク情報」画面

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が表示されます。

無線LAN		
インターフェース	SSID	BSSID
ath0	WIRELESSLAN-0	00-90-C7-08-F6-0A
ath1	WIRELESSLAN-0	00-90-C7-08-F6-0B

※[無線LAN]項目の[無線UNIT]欄(P.3-68)が「無効」に設定されている無線LANユニット、[仮想AP設定]項目の[仮想AP]欄(P.3-70)が「無効」に設定されているインターフェースは表示されません。

情報表示 > ネットワーク情報

■ AP間通信 (WBR)

本製品と無線AP間通信する無線アクセスポイントごとの詳細情報が表示されます。

AP間通信 (WBR)	
インターフェース	BSSID
wbr0	00-90-C7-08-F6-0A

※無線AP間通信に使用している本製品のインターフェースの名称と、無線AP間通信している相手側のBSSIDが表示されます。(P.3-93)

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(P.3-14)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が表示されます。

DHCPリース情報			
ホスト名	MACアドレス	IPアドレス	リース期限
DESKTOP	00-11-1A-00-00-00	192.168.0.30	2023/03/03 12:00:00
iPhone11	00-11-1A-00-00-01	192.168.0.11	2023/03/03 12:00:00

3 設定画面について

「SYSLOG」画面

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。

SYSLOG

現在時刻： 年 月 日 (稼働時間: 0 day 04:50:45)

表示するレベル： ① ☒ DEBUG ☒ INFO ☒ NOTICE

表示フィルター： ②

を含む ▼

③ 最新の情報に更新 ④ 保存 ⑤ クリア

日付・時間	レベル	内容
09-15 06:41:10	INFO	kernel: [wifi0] FWLOG: [17821207] WAL channel change freq=5600, mode=0 flags=0 rx_ok=1 tx_ok=1

- ① 表示するレベル …………… 非表示に設定するときには、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。
※「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。
- ② 表示フィルター …………… 表示内容を絞り込むときに使用するフィルターです。
フィルターとして使用するテキスト(例：dhcp)を入力し、「を含む」/「含まない」を選択します。
- ③ <最新の情報に更新> …………… [表示するレベル](①)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1000件のログ情報を記憶できます。
1000件を超えると、古いログ情報から削除されます。
- ④ <保存> …………… 表示するレベル(①)に応じた内容を保存するボタンです。
※表示フィルター(②)での絞りこみには関与しません。
※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。
- ⑤ <クリア> …………… すべてのログ情報を削除するボタンです。

3 設定画面について

「無線LAN情報」画面

情報表示 > 無線LAN情報

■ アクセスポイント情報

本製品の無線LAN機能で使用しているチャンネルと仮想APごとの設定内容が表示されます。

アクセスポイント情報				
デバイス	インターフェース	BSSID	SSID	暗号化
無線 1 1 CH (2412 MHz)	ath0	00-90-C7-XXXXXX	WIRELESSLAN-0	WPA-PSK/WPA2-PSK (AES)
無線 2 36 CH (5180 MHz)	ath1	00-90-C7-XXXXXX	WIRELESSLAN-0	WPA2-PSK (AES)

情報表示 > 無線LAN情報

■ 端末情報

本製品の仮想APと通信する無線LAN端末があるとき、その無線LAN端末との通信情報が表示されます。

端末情報						
所属AP	MACアドレス	IPアドレス	RSSI	受信速度	送信速度	
ath0	00:0A:00:00:00:00	192.168.0.11	16	54.0 Mbps	108.0 Mbps	詳細
ath1	00:0A:00:00:00:00	192.168.0.30	23	234.0 Mbps	260.0 Mbps	詳細

※仮想APのARP代理応答機能(P.3-109)が「有効」に設定され、本製品が学習した無線LAN端末のIPアドレス、または本製品のDHCPサーバー機能より割り当てられた無線LAN端末のIPアドレスが表示されます。

両方の条件に一致せず、本製品がIPアドレスを学習できていない場合、「－」が表示されます。

※〈詳細〉をクリックすると、通信中の無線LAN端末について別画面が表示されます。(P.3-10)

3 設定画面について

「無線LAN情報」画面

情報表示 > 無線LAN情報 > 端末情報

■ 通信端末詳細情報

無線LAN端末と通信中、「無線LAN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されます。

通信端末詳細情報	
通信状況：	通信中
インターフェース：	ath1
MACアドレス：	88:39:3A:00:00:14
IPアドレス：	192.168.0.11
通信モード：	IEEE 802.11ac
VLAN ID：	0
SSID：	WIRELESSLAN-0
暗号化：	WPA2-PSK (AES)
チャンネル：	36 CH (5180 MHz)
信号レベル：	 25
速度：	送信 260.0 Mbps / 受信 234.0 Mbps
WMMパワーセーブ：	無効
接続時間：	0 day 00:00:48

※ [信号レベル] 欄に、無線LAN端末から受信した電波信号の強さがメーターと数値で表示されます。

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無線LAN機器が近くで稼働している場合や無線LAN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。

3 設定画面について

「無線LAN情報」画面

情報表示 > 無線LAN情報

■ AP間通信情報

本製品と無線AP間通信する無線アクセスポイントがあるとき、その機器との通信情報が表示されます。

AP間通信情報					
インターフェース	BSSID	RSSI	受信速度	送信速度	
wbr0	1E-90-C7- 	24	86.0 Mbps	86.0 Mbps	詳細
wbr8	1E-90-C7- 				詳細

※ 無線AP間通信に使用している本製品のインターフェースと無線AP間通信している相手側のBSSIDが表示されます。
(表示例：親機)

※ 子機として通信しているときは、インターフェースに「wbr16」(無線LAN1)、「wbr17」(無線LAN2)が表示されます。

※ <詳細>をクリックすると、通信中の無線アクセスポイントについて別画面(下図)で表示します。

情報表示 > 無線LAN情報 > AP間通信情報

■ AP間通信詳細情報

無線AP間通信中、「無線LAN情報」画面の[AP間通信情報]項目に表示された<詳細>をクリックすると表示されます。

AP間通信詳細情報	
通信状況：	通信中
インターフェース：	wbr8
接続先BSSID：	
通信モード：	IEEE 802.11ac
SSID：	WIRELESSLAN-0
暗号化：	WPA2-PSK (AES)
チャンネル：	36 CH (5180 MHz)
信号レベル：	 58
レート：	送信 144.0 Mbps / 受信 52.0 Mbps

※ [信号レベル] 欄に、無線LAN端末から受信した電波信号の強さがメーターと数値で表示されます。

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無線LAN機器が近くで稼働している場合や無線LAN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。

3 設定画面について

「IPアドレス」画面

ネットワーク設定 > IPアドレス

■ 本体名称

本製品の名称を設定します。

本体名称
本体名称: <u>AP-95M</u>

本体名称.....

Telnet/SSHで本製品に接続したとき、ここで設定した本体名称が表示されます。
(出荷時の設定: AP-95M)

※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 > IPアドレス

■ VLAN設定

VLAN機能についての設定です。

VLAN設定
マネージメントID: <u>0</u>

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を使用しないネット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。

3 設定画面について

「IPアドレス」画面

ネットワーク設定 > IPアドレス

■ IPアドレス設定

本製品のIPアドレスを設定します。

IPアドレス設定

IPアドレス : ① 192.168.0.1

サブネットマスク : ② 255.255.255.0

デフォルトゲートウェイ : ③

プライマリーDNSサーバー : ④

セカンダリーDNSサーバー : ⑤

⑥ 登録

⑦ 取消

- | | |
|-----------------------|--|
| ① IPアドレス | 本製品のIPアドレスを入力します。 (出荷時の設定：192.168.0.1)
本製品を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、[割り当て開始IPアドレス]欄(P.3-14)についてもネットワーク部を同じに設定してください。 |
| ② 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。 |
| ③ デフォルトゲートウェイ | 本製品の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。
※本製品と同じIPアドレスは登録できません。 |
| ④ 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。 |
| ⑤ セカンダリーDNSサーバー | [プライマリーDNSサーバー] (④)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。 |
| ⑥ <登録> | 「IPアドレス」画面で設定した内容を登録するボタンです。 |
| ⑦ <取消> | 「IPアドレス」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。 |

3 設定画面について

「DHCPサーバー」画面

ネットワーク設定 > DHCPサーバー

■ DHCPサーバー設定

本製品のDHCPサーバー機能を設定します。

DHCPサーバー設定

DHCPサーバー：☒ 無効 ☐ 有効

割り当て開始IPアドレス：

割り当て個数： 個

サブネットマスク：

リース期間： 時間

ドメイン名：

デフォルトゲートウェイ：

DNS代理応答：☒ 無効 ☐ 有効

プライマリーDNSサーバー：

セカンダリーDNSサーバー：

プライマリーWINSサーバー：

セカンダリーWINSサーバー：

- ① DHCP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、「割り当て開始IPアドレス」(②)欄と「割り当て個数」(③)欄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。
- ② 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)
- ③ 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」(②)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。
- ④ サブネットマスク 「割り当て開始IPアドレス」(②)欄に設定されたIPアドレスに対するサブネットマスクを設定します。 (出荷時の設定：255.255.255.0)
- ⑤ 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。 (出荷時の設定：72)
設定できる範囲は、「1～9999」(時間)です。
- ⑥ ドメイン名 指定のドメイン名を設定する必要があるときは、DHCPサーバーが有線で接続する端末に通知するネットワークアドレスのドメイン名を253文字(半角英数字)以内で入力します。
- ⑦ 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、クライアントに通知するデフォルトゲートウェイアドレスを入力します。
※空白にした場合は、通知されません。

3 設定画面について

「DHCPサーバー」画面

ネットワーク設定 > DHCPサーバー

■ DHCPサーバー設定(つづき)

DHCPサーバー設定

DHCPサーバー：☒ 無効 ☐ 有効

割り当て開始IPアドレス：

割り当て個数： 個

サブネットマスク：

リース期間： 時間

ドメイン名：

デフォルトゲートウェイ：

DNS代理応答：☒ 無効 ☐ 有効

プライマリーDNSサーバー：

セカンダリーDNSサーバー：

プライマリーWINSサーバー：

セカンダリーWINSサーバー：

登録

取消

- ⑧ DNS代理応答 本製品のDNS代理応答機能を設定します。 (出荷時の設定：無効)
DNS代理応答機能とは、端末からのDNS要求をプロバイダー側のDNSサーバーへ転送する機能です。
「有効」に設定すると、本製品のアドレスをネットワーク上の端末にDNSサーバーとして設定している場合、本製品が接続する先のDNSサーバーのアドレスが変更になったときでも、端末側の設定を変更する必要がありません。
- ⑨ プライマリーDNSサーバー 本製品のDHCPサーバー機能を利用するときに、クライアントに通知する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。
※入力すると、設定したDNSサーバーアドレスをDHCPクライアントに通知します。
- ⑩ セカンダリーDNSサーバー [プライマリーDNSサーバー] (⑨) 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。
- ⑪ プライマリーWINSサーバー ... 本製品のDHCPサーバー機能を利用するときに、クライアントに通知する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。
- ⑫ セカンダリーWINSサーバー ... [プライマリーWINSサーバー] (⑪) 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。
- ⑬ <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。
- ⑭ <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。

3 設定画面について

「DHCPサーバー」画面

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		
MACアドレス	IPアドレス	
		追加

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.3-14)

※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]欄が初期値の場合は、
192.168.0.41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が表示されます。

静的DHCPサーバー設定一覧		
MACアドレス	IPアドレス	
00:00:00:00:00:00	192.168.0.50	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 設定画面について

「スタティックルーティング」画面

ネットワーク設定 > スタティックルーティング

■ 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が表示されます。
※この項目では、現在有効な経路だけが表示されます。

IP経路情報			
宛先 ①	サブネットマスク ②	ゲートウェイ ③	経路 ④
192.168.0.0	255.255.255.0		br-lan
192.168.10.0	255.255.255.0	192.168.0.254	br-lan

- ① 宛先 ルーティングの対象となるパケットの宛先IPアドレスが表示されます。
- ② 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が表示されます。
- ③ ゲートウェイ 宛先IPアドレスに対するゲートウェイが表示されます。
- ④ 経路 宛先IPアドレスに対する転送先インターフェースが表示されます。
br-lan：インターフェースが本製品自身の場合

3 設定画面について

「スタティックルーティング」画面

ネットワーク設定 > スタティックルーティング

■ 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。

スタティックルーティング設定				
宛先 ①	サブネットマスク ②	ゲートウェイ ③	経路 ④	⑤
192.168.10.0	255.255.255.0	192.168.0.254	ゲートウェイを設定▼	追加

- ① 宛先 対象となる相手先のIPアドレスを入力します。
- ② 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。
- ③ 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。
- ④ 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、「ゲートウェイを設定」、「ppp0(WAN01)～ppp7(WAN08)」から選択します。
- ⑤ 〈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 > スタティックルーティング

■ 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が表示されます。

※画面の値は、入力例です。

スタティックルーティング設定一覧					
宛先	サブネットマスク	ゲートウェイ	経路	①	②
127.0.0.0	255.0.0.0	127.0.0.1		編集	削除
192.168.10.0	255.255.255.0	192.168.0.254		編集	削除

- ① 〈編集〉 登録した内容を編集するときは、該当する欄の〈編集〉をクリックします。
- ② 〈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 設定画面について

「ポリシールーティング」画面

ネットワーク設定 > ポリシールーティング

■ 送信元ルーティング設定

送信元の端末(パソコンなど)を特定して、パケットの中継経路を最大32件まで登録できます。

※ルーター機能が有効(P.3-51)のときに使用する設定です。

送信元ルーティング設定				
送信元 ①	サブネットマスク ②	ゲートウェイ ③	経路 ④	⑤
192.168.0.20	255.255.255.255		ppp1 (WAN02) ▼	追加

- ① 送信元 送信元のIPアドレスを入力します。
- ② サブネットマスク 対象となる送信元のIPアドレスに対するサブネットマスクを入力します。
- ③ 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。
- ④ 経路 パケット転送先インターフェースを、「ゲートウェイを設定」、「ppp0 (WAN01)～ppp7 (WAN08)」から選択します。
- ⑤ 〈追加〉 クリックすると、入力内容が登録されます。
[送信元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 > ポリシールーティング

■ 送信元ルーティング設定一覧

[送信元ルーティング設定]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。

送信元ルーティング設定一覧					
送信元	サブネットマスク	ゲートウェイ	経路	①	②
192.168.0.20	255.255.255.255		ppp1 (WAN02)	編集	削除

- ① 〈編集〉 登録した内容を編集するときは、該当する欄の〈編集〉をクリックします。
- ② 〈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 設定画面について

「パケットフィルター」画面

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の通過と遮断の設定です。

- ① 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、送信、または転送するパケットと[現在の登録]項目に表示されたフィルターと比較します。
※番号が指定されていないときは、登録できません。
※IPv6のフィルタリング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。
- ② 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。
- ③ ログ出力 「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：無効)
※大量のログを処理すると、システム処理速度に影響します。
- ④ フィルター方法 フィルタリングの方法を選択します。 (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。

3 設定画面について

「パケットフィルター」画面

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)

⑤ 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)

- ◎br-lan : インターフェースが本製品自身の場合
- ◎eth1 : インターフェースが有線LANの場合
- ◎ath0, ath01～ath08: インターフェースが本製品の無線LAN1
(2.4GHz帯仮想AP)の場合
- ◎ath1, ath11～ath18: インターフェースが本製品の無線LAN2
(5GHz帯仮想AP)の場合
- ◎wbr0～wbr17 : インターフェースがAP間通信(WBR)の場合
- ※「すべて」を選択すると、「br-lan」、「eth1」、「ath0, ath01～ath08」、
「ath1, ath11～ath18」、「wbr0～wbr17」が送信元インターフェース
の対象になります。

⑥ 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)

- ◎br-lan : インターフェースが本製品自身の場合
- ◎eth1 : インターフェースが有線LANの場合
- ◎ath0, ath01～ath08: インターフェースが本製品の無線LAN1
(2.4GHz帯仮想AP)の場合
- ◎ath1, ath11～ath18: インターフェースが本製品の無線LAN2
(5GHz帯仮想AP)の場合
- ◎wbr0～wbr17 : インターフェースがAP間通信(WBR)の場合
- ※「すべて」を選択すると、「br-lan」、「eth1」、「ath0, ath01～ath08」、
「ath1, ath11～ath18」、「wbr0～wbr17」が宛先インターフェースの
対象になります。

⑦ 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アドレスの範囲を設定します。
※MACアドレスは、半角英数字12桁(16進数)で入力します。
※登録例は、「宛先MACアドレス/マスク:」(⑧)欄で説明しています。
※空白の場合は、すべてのMACアドレスがフィルタリング対象になります。

3 設定画面について

「パケットフィルター」画面

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)

⑧ 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。

※MACアドレスは、半角英数字12桁(16進数)で入力します。

※空白の場合は、すべてのMACアドレスがフィルタリング対象になります。

【MACアドレスとマスク値の登録例】

登録結果は、小文字で入力しても、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(P.3-32)には、下記の内容が表示されます。

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(P.3-32)には、下記の内容が表示されます。

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(P.3-32)には、下記の内容が表示されます。

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。

3 設定画面について

「パケットフィルター」画面

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)

パケットフィルター設定

番号: ① ▼

エントリ: ② ☒ 無効 ☐ 有効

ログ出力: ③ ☒ 無効 ☐ 有効

フィルター方法: ④ ☐ 遮断 ☒ 透過

インターフェース

送信元インターフェース: ⑤ すべて ▼

宛先インターフェース: ⑥ すべて ▼

Ethernet ヘッダー

送信元 MAC アドレス / マスク: ⑦ /

宛先 MAC アドレス / マスク: ⑧ /

Ethernet タイプ: ⑨ すべて ▼

⑩ 登録 ⑪ 取消

- ⑨ Ethernetタイプ フィルタリングの対象となるEthernetタイプ名称(VLAN/ARP/IPv4/指定)を選択します。(出荷時の設定: すべて)
※「指定」を選択したとき表示されるテキストボックスに設定できる範囲は、「0600～FFFF」(16進数)です。
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。
※選択したタイプで表示される設定は、下記のページで説明しています。
◎VLAN: 3-24ページ～3-28ページ
◎ARP: 3-29ページ
◎IPv4: 3-30ページ
- ⑩ <登録> [パケットフィルター設定]項目で設定した内容を登録するボタンです。
- ⑪ <取消> [パケットフィルター設定]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。

3 設定画面について

「パケットフィルター」画面

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] (⑨) 欄で「VLAN」を選択、[Ethernetタイプ] (⑬) 欄で「すべて」を選択すると、下記の画面が表示されます。

Ethernet ヘッダー	
送信元 MAC アドレス / マスク:	_____ / _____
宛先 MAC アドレス / マスク:	_____ / _____
Ethernet タイプ: ⑨	VLAN ▼
VLAN ID: ⑫	_____
Ethernet タイプ: ⑬	すべて ▼

⑫ VLAN ID

フィルタリングの対象となる[VLAN ID]を指定します。

入力できる範囲は、「1～4094」です。 (出荷時の設定：すべて)

※入力しない(空白)ときは、すべてのVLAN IDの packets が対象です。

[パケットフィルター設定一覧]項目には、「すべて」と表示されます。

⑬ Ethernetタイプ

[VLAN ID] (⑫) 欄で指定したVLAN IDでカプセル化された packets について、フィルタリングの対象となるEthernetタイプ名称(ARP/IPv4/指定)を選択します。 (出荷時の設定：すべて)

※「指定」を選択したとき表示されるテキストボックスに設定できる範囲は、「0600～FFFF」(16進数)です。

※選択したタイプで表示される設定は、下記のページで説明しています。

◎ARP : 3-25ページ

◎IPv4 : 3-26ページ～3-28ページ

3 設定画面について

「パケットフィルター」画面

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] (9) 欄で「VLAN」を選択、[Ethernetタイプ] (13) 欄で「ARP」を選択すると、下記の画面が表示されます。

Ethernet ヘッダー	
送信元 MAC アドレス / マスク :	_____ / _____
宛先 MAC アドレス / マスク :	_____ / _____
Ethernet タイプ :	(9) VLAN ▼
VLAN ID :	(12) _____
Ethernet タイプ :	(13) ARP ▼
ARP ヘッダー	
オペレーションコード :	(14) すべて ▼
送信元 MAC アドレス / マスク :	(15) _____ / _____
送信元 IP アドレス / マスク :	(16) _____ / _____
ターゲット MAC アドレス / マスク :	(17) _____ / _____
ターゲット IP アドレス / マスク :	(18) _____ / _____

14 オペレーションコード ……………

[VLAN ID] (12) 欄で指定した VLAN ID でカプセル化されたパケットについて、フィルタリングの対象となる ARP 動作の種類を表すためのコードを選択します。
(出荷時の設定：すべて)

「すべて」、「request」、「reply」、「指定」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。

※「指定」を選択したとき表示されるテキストボックスに設定できる範囲は、「00000～65535」です。

15 送信元MACアドレス/マスク …

[VLAN ID] (12) 欄で指定した VLAN ID でカプセル化されたパケットについて、フィルタリングの対象となる 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。

※MACアドレスは、半角英数字12桁(16進数)で入力します。

16 送信元IPアドレス/マスク ………

[VLAN ID] (12) 欄で指定した VLAN ID でカプセル化されたパケットについて、フィルタリングの対象となる ARP ヘッダー内において、送信元 IP アドレスの有効範囲を設定します。

17 ターゲットMACアドレス/マスク …

[VLAN ID] (12) 欄で指定した VLAN ID でカプセル化されたパケットについて、フィルタリングの対象となる ARP 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。

※MACアドレスは、半角英数字12桁(16進数)で入力します。

18 ターゲットIPアドレス/マスク …

[VLAN ID] (12) 欄で指定した VLAN ID でカプセル化されたパケットについて、フィルタリングの対象となる ARP ヘッダー内において、宛先 IP アドレスの有効範囲を設定します。

3 設定画面について

「パケットフィルター」画面

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](9)欄で「VLAN」を選択、[Ethernetタイプ](13)欄で「IPv4」、[IPプロトコル](22)欄で「すべて」、[ICMP]、[IGMP]を選択すると、下記の画面が表示されます。

Ethernet ヘッダー

送信元 MAC アドレス / マスク: _____ / _____

宛先 MAC アドレス / マスク: _____ / _____

Ethernet タイプ: (9) VLAN ▼

VLAN ID: (12) _____

Ethernet タイプ: (13) IPv4 ▼

IPv4 ヘッダー

送信元 IP アドレス / マスク: (19) _____ / _____

宛先 IP アドレス / マスク: (20) _____ / _____

TOS: (21) 0x _____

IP プロトコル: (22) すべて ▼

(19) 送信元IPアドレス/マスク ………

[VLAN ID](12)欄で指定したVLAN IDでカプセル化されたパケットについて、フィルターの対象となるIPv4ヘッダー内において、送信元IPアドレスの有効範囲を設定します。

範囲は、マスク(サブネットマスク)で指定します。

◎マスクを設定しない場合は、IPアドレスと完全に一致したときフィルタリングします。

◎マスクを設定する場合は、例えば192.168.0.0/255.255.255.0と設定する場合は、192.168.0.0～192.168.0.255に一致したときフィルタリングします。

(20) 宛先IPアドレス/マスク ………

[VLAN ID](12)欄で指定したVLAN IDでカプセル化されたパケットについて、フィルターの対象となるIPv4ヘッダー内において、宛先IPアドレスの有効範囲を設定します。

範囲は、マスク(サブネットマスク)で指定します。

◎マスクを設定しない場合は、IPアドレスと完全に一致したときフィルタリングします。

◎マスクを設定する場合は、例えば192.168.0.0/255.255.255.0と設定する場合は、192.168.0.0～192.168.0.255に一致したときフィルタリングします。

(21) TOS ………

[VLAN ID](12)欄で指定したVLAN IDでカプセル化されたパケットについて、フィルタリングの対象となるIPv4ヘッダー内のTOS(Type Of Service)フィールドの値を設定します。

※設定できる範囲は、「00～FF」(16進数)です。

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。

3 設定画面について

「パケットフィルター」画面

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](9)欄で「VLAN」を選択、[Ethernetタイプ](13)欄で「IPv4」、[IPプロトコル](22)欄で「すべて」、[ICMP]、[IGMP]を選択すると、下記の画面が表示されます。

Ethernet ヘッダー	
送信元 MAC アドレス / マスク:	_____ / _____
宛先 MAC アドレス / マスク:	_____ / _____
Ethernet タイプ:	(9) VLAN ▼
VLAN ID:	(12) _____
Ethernet タイプ:	(13) IPv4 ▼
IPv4 ヘッダー	
送信元 IP アドレス / マスク:	(19) _____ / _____
宛先 IP アドレス / マスク:	(20) _____ / _____
TOS:	(21) 0x _____
IP プロトコル:	(22) すべて ▼

(22) IPプロトコル

[VLAN ID](12)欄で指定したVLAN IDでカプセル化されたパケットについて、フィルターの対象となるIPv4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。
(出荷時の設定：すべて)

◎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：選択したとき表示されるテキストボックスに、IPv4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。

※設定できる範囲は、「0～255」(10進数)です。

3 設定画面について

「パケットフィルター」画面

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] (9) 欄で「VLAN」を選択、[Ethernetタイプ] (13) 欄で「IPv4」、[IPプロトコル] (22) 欄で「TCP」、「UDP」を選択すると、下記の画面が表示されます。

Ethernet ヘッダー
送信元 MAC アドレス / マスク: _____ / _____
宛先 MAC アドレス / マスク: _____ / _____
Ethernet タイプ (9): VLAN ▼
VLAN ID (12): _____
Ethernet タイプ (13): IPv4 ▼
IPv4 ヘッダー
送信元 IP アドレス / マスク (19): _____ / _____
宛先 IP アドレス / マスク (20): _____ / _____
TOS (21): 0x _____
IP プロトコル (22): TCP ▼
送信元ポート番号 (23): _____ ~ _____
宛先ポート番号 (24): _____ ~ _____

23 送信元ポート番号

[VLAN ID] (12) 欄で指定した VLAN ID でカプセル化されたパケットについて、フィルタリングの対象となる発信元の TCP ポート、または UDP ポートの番号(始点と終点)をテキストボックスに入力します。
特定のポートだけを指定するときは、始点だけ、または始点/終点に同一の番号を入力してください。
※入力できる範囲は、10進数で「0～65535」までの半角数字です。

24 宛先ポート番号

[VLAN ID] (12) 欄で指定した VLAN ID でカプセル化されたパケットについて、フィルタリングの対象となる宛先の TCP ポート、または UDP ポートの番号(始点と終点)をテキストボックスに入力します。
特定のポートだけを指定するときは、始点だけ、または始点/終点に同一の番号を入力してください。
※入力できる範囲は、10進数で「0～65535」までの半角数字です。

3 設定画面について

「パケットフィルター」画面

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] (9)欄で「ARP」を選択すると、下記の画面が表示されます。

Ethernet ヘッダー	
送信元 MAC アドレス / マスク:	_____ / _____
宛先 MAC アドレス / マスク:	_____ / _____
Ethernet タイプ:	9 ARP ▼
ARP ヘッダー	
オペレーションコード:	25 すべて ▼
送信元 MAC アドレス / マスク:	26 _____ / _____
送信元 IP アドレス / マスク:	27 _____ / _____
ターゲット MAC アドレス / マスク:	28 _____ / _____
ターゲット IP アドレス / マスク:	29 _____ / _____

- 25 オペレーションコード フィルタリングの対象となるARP動作の種類を表すためのコードを選択します。
(出荷時の設定：すべて)
「すべて」、「request」、「reply」、「指定」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。
※「指定」を選択したとき表示されるテキストボックスに設定できる範囲は、「00000～65535」です。
- 26 送信元MACアドレス/マスク ... フィルタリングの対象となる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。
※MACアドレスは、半角英数字12桁(16進数)で入力します。
- 27 送信元IPアドレス/マスク フィルタリングの対象となるARPヘッダー内において、送信元IPアドレスの有効範囲を設定します。
- 28 ターゲットMACアドレス/マスク ... フィルタリングの対象となるARP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。
※MACアドレスは、半角英数字12桁(16進数)で入力します。
- 29 ターゲットIPアドレス/マスク ... フィルタリングの対象となるARPヘッダー内において、宛先IPアドレスの有効範囲を設定します。

3 設定画面について

「パケットフィルター」画面

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](9)欄で「IPv4」を選択、[IPプロトコル](33)欄で「すべて」、「ICMP」、「IGMP」を選択すると、下記の画面が表示されます。

Ethernet ヘッダー
送信元 MAC アドレス / マスク: _____ / _____
宛先 MAC アドレス / マスク: _____ / _____
Ethernet タイプ: 9 IPv4 ▼
IPv4 ヘッダー
送信元 IP アドレス / マスク: 30 _____ / _____
宛先 IP アドレス / マスク: 31 _____ / _____
TOS: 32 0x _____
IP プロトコル: 33 すべて ▼

- 30 送信元IPアドレス/マスク ……… フィルターの対象となるIPv4ヘッダー内において、送信元IPアドレスの有効範囲を設定します。
範囲は、マスク(サブネットマスク)で指定します。
◎マスクを設定しない場合は、IPアドレスと完全に一致したときフィルタリングします。
◎マスクを設定する場合は、例えば192.168.0.0/255.255.255.0と設定する場合は、192.168.0.0～192.168.0.255に一致したときフィルタリングします。
- 31 宛先IPアドレス/マスク ……… フィルターの対象となるIPv4ヘッダー内において、宛先IPアドレスの有効範囲を設定します。
範囲は、マスク(サブネットマスク)で指定します。
◎マスクを設定しない場合は、IPアドレスと完全に一致したときフィルタリングします。
◎マスクを設定する場合は、例えば192.168.0.0/255.255.255.0と設定する場合は、192.168.0.0～192.168.0.255に一致したときフィルタリングします。
- 32 TOS …………… フィルタリングの対象となるIPv4ヘッダー内のTOS(Type Of Service)フィールドの値を設定します。
※設定できる範囲は、「00～FF」(16進数)です。
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。
- 33 IPプロトコル …………… フィルターの対象となるIPv4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。(出荷時の設定：すべて)
◎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：選択したとき表示されるテキストボックスに、IPv4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。
※設定できる範囲は、「0～255」(10進数)です。

3 設定画面について

「パケットフィルター」画面

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](9)欄で「IPv4」を選択、[IPプロトコル](33)欄で「TCP」、「UDP」を選択すると、下記の画面が表示されます。

Ethernet ヘッダー	
送信元 MAC アドレス / マスク :	_____ / _____
宛先 MAC アドレス / マスク :	_____ / _____
Ethernet タイプ :	(9) IPv4 ▼
IPv4 ヘッダー	
送信元 IP アドレス / マスク :	(30) _____ / _____
宛先 IP アドレス / マスク :	(31) _____ / _____
TOS :	(32) 0x _____
IP プロトコル :	(33) TCP ▼
送信元ポート番号 :	(34) _____ ~ _____
宛先ポート番号 :	(35) _____ ~ _____

- (34) 送信元ポート番号 フィルタリングの対象となる発信元のTCPポート、またはUDPポートの番号(始点と終点)をテキストボックスに入力します。
特定のポートだけを指定するときは、始点だけ、または始点/終点に同一の番号を入力してください。
※入力できる範囲は、10進数で「0～65535」までの半角数字です。
- (35) 宛先ポート番号 フィルタリングの対象となる宛先のTCPポート、またはUDPポートの番号(始点と終点)をテキストボックスに入力します。
特定のポートだけを指定するときは、始点だけ、または始点/終点に同一の番号を入力してください。
※入力できる範囲は、10進数で「0～65535」までの半角数字です。

3 設定画面について

「パケットフィルター」画面

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。

パケットフィルター設定一覧			
番号	項目	詳細	
1	エントリー	無効	
	ログ出力	有効	① 編集
	フィルター方法	透過	
	送信元インターフェース	すべて	② 削除
	宛先インターフェース	すべて	
	送信元 MAC アドレス / マスク	すべて	
	宛先 MAC アドレス / マスク	すべて	
	Ethernet タイプ	すべて	

- ①〈編集〉 登録したパケットフィルターを編集するボタンです。
※〈編集〉をクリックすると、[パケットフィルター設定]項目(P.3-20)で編集できます。
- ②〈削除〉 登録したパケットフィルターを削除するボタンです。

3 設定画面について

パケットフィルターの使用例について

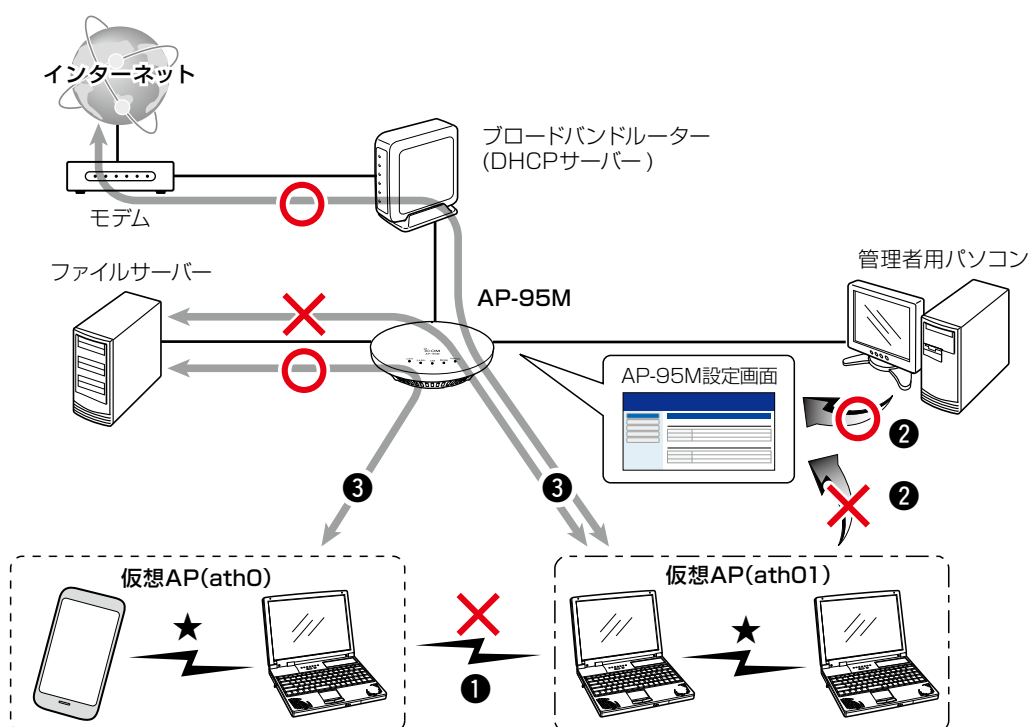
ネットワーク設定 > パケットフィルター

下図とその説明(①～③)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。

- ① 異なる仮想AP(例: ath0/ath01)の端末同士の通信を禁止するには (P.3-34)
- ② AP-95M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 (P.3-35)
- ③ 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への接続を禁止するには (P.3-36)

※下図の★印(仮想AP内の無線LAN端末同士の通信の禁止)を設定するときは、仮想AP(例: ath0、ath01)の設定画面で、「同一仮想AP内の端末間通信禁止」を「有効」に設定してください。(P.3-72)

パケットフィルターの設定では、下図の★印の通信を禁止できません。



3 設定画面について

パケットフィルターの使用例について

ネットワーク設定 > パケットフィルター

①異なる仮想AP(例: ath0/ath01)の端末同士の通信を禁止するには

下記の2つ(①と②)のフィルターの登録が必要です。

※下図の★印(仮想AP内の無線LAN端末同士の通信の禁止)を設定するときは、仮想AP(例: ath0、ath01)の設定画面で、「同一仮想AP内の端末間通信禁止」を「有効」に設定してください。(P.3-72)

パケットフィルターの設定では、下図の★印の通信を禁止できません。

パケットフィルター設定一覧

番号	項目	詳細	
1	エントリー	有効	
	ログ出力	無効	編集
	フィルター方法	遮断	
	送信元インターフェース	ath0	削除
	宛先インターフェース	ath01	
	送信元 MAC アドレス / マスク	すべて	
	宛先 MAC アドレス / マスク	すべて	
	Ethernet タイプ	すべて	

「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	項目	詳細	
2	エントリー	有効	
	ログ出力	無効	編集
	フィルター方法	遮断	
	送信元インターフェース	ath01	削除
	宛先インターフェース	ath0	
	送信元 MAC アドレス / マスク	すべて	
	宛先 MAC アドレス / マスク	すべて	
	Ethernet タイプ	すべて	

上記のフィルターで登録した番号と異なる番号を表示

① 仮想AP(ath0) → 仮想AP(ath01)方向の通信を遮断

② 仮想AP(ath01) → 仮想AP(ath0)方向の通信を遮断

3 設定画面について

パケットフィルターの使用例について

ネットワーク設定 > パケットフィルター

② AP-95M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(①と②)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。

「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

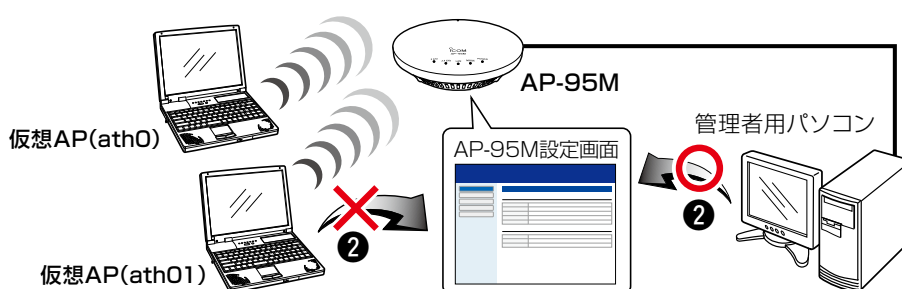
上記のフィルターで登録した番号より大きな番号を表示

管理者用のパソコンに設定されたIPアドレス

① 管理用端末からのWEBアクセスを透過

② 管理用端末以外のWEBアクセスを遮断

番号	項目	詳細
1	エントリー	有効
	ログ出力	無効
	フィルター方法	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	br-lan
	送信元 MAC アドレス / マスク	すべて
	宛先 MAC アドレス / マスク	すべて
	Ethernet タイプ	IPv4
	送信元 IP アドレス / マスク	192.168.0.0 / 255.255.255.0
	宛先 IP アドレス / マスク	すべて
	TOS	すべて
	IP プロトコル	TCP
	送信元ポート番号	すべて
	宛先ポート番号	80 ~ 80
2	エントリー	有効
	ログ出力	無効
	フィルター方法	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	br-lan
	送信元 MAC アドレス / マスク	すべて
	宛先 MAC アドレス / マスク	すべて
	Ethernet タイプ	IPv4
	送信元 IP アドレス / マスク	すべて
	宛先 IP アドレス / マスク	すべて
	TOS	すべて
	IP プロトコル	TCP
	送信元ポート番号	すべて
	宛先ポート番号	80 ~ 80



3 設定画面について

パケットフィルターの使用例について

ネットワーク設定 > パケットフィルター

③ 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(①と②)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。

「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

「パケットフィルター」画面で設定したブロードバンドルーターのLAN側のMACアドレスを表示

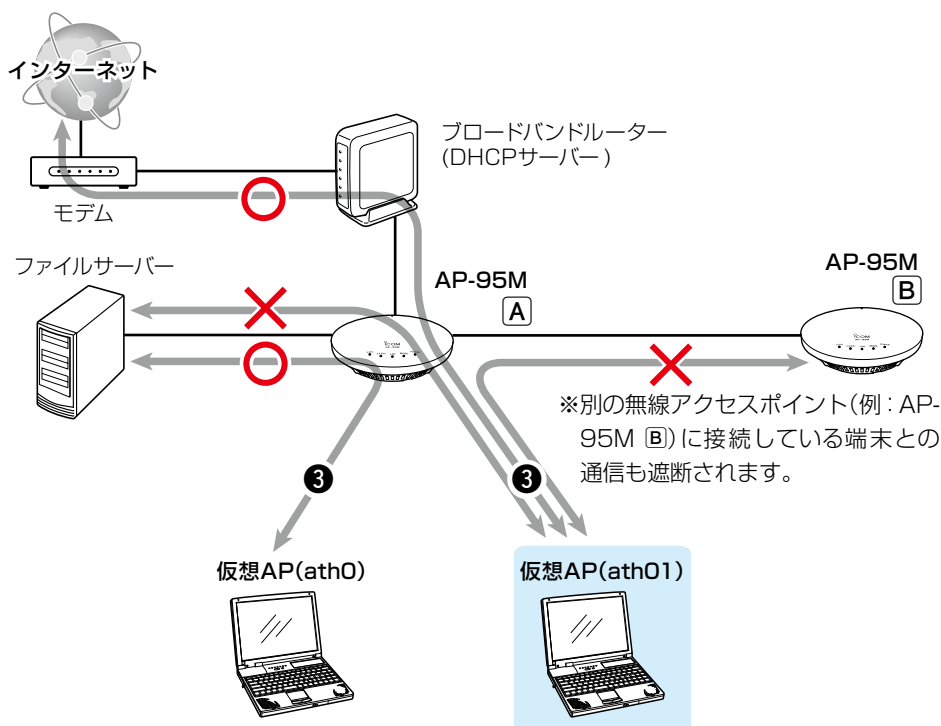
番号	項目	詳細	編集	削除
1	エントリー	有効		
	ログ出力			
	フィルター方法	透過		
	送信元インターフェース	eth1		
	宛先インターフェース	ath0		
	送信元 MAC アドレス / マスク	00-00-06-FF-FF-FF-FF-FF-FF		
	宛先 MAC アドレス / マスク	すべて		
	Ethernet タイプ	すべて		

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	項目	詳細	編集	削除
2	エントリー	有効		
	ログ出力			
	フィルター方法	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	ath01		
	送信元 MAC アドレス / マスク	すべて		
	宛先 MAC アドレス / マスク	すべて		
	Ethernet タイプ	すべて		

① ブロードバンドルーターから仮想AP(ath01)への通信を透過

② ブロードバンドルーター以外から仮想AP(ath01)への通信を遮断



3 設定画面について

「Web認証 基本」画面

ネットワーク設定 > Web認証 > 基本

■ Web認証

Web認証機能を設定すると、端末が本製品に接続し、WWWブラウザで任意のサイトにアクセスしたとき、Web認証ページが表示されます。

ユーザー名とパスワードを入力し、認証されると、端末がネットワークにアクセスできます。

※「基本」画面、「詳細」画面と併せて設定してください。

※「https://」ではじまるサイトにアクセスした場合、認証ページは表示されません。

Web認証

インターフェース : ① ath0

Web認証 : ② ☒ 無効 ☐ 有効

ページタイトル : ③ Set your page title.

ポータルサイト : ④ http://www.example.com/

移動待ち時間 : ⑤ 5 秒

有効期限 : ⑥ 24時間

⑦ 登録 ⑧ 取消

- ① 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)
※無線LAN1はath0、ath01～ath07、無線LAN2はath1、ath11～ath17から選択します。
※災害用仮想AP(ath08、ath18)には設定できません。(P.3-116)
※インターフェースごとに、下記の設定内容を変更できます。
◎[Web認証]項目
◎[カスタムページ]項目(P.3-39)
◎「Web認証 詳細」画面の各項目(P.3-43)
- ② Web認証 [インターフェース](①)欄で選択したインターフェースについて、Web認証を使用するときは、「有効」に設定します。 (出荷時の設定 : 無効)
※Web認証を使用できる仮想APは、「仮想AP」画面の[仮想AP]欄が「有効」に設定されたものだけです。
※ご使用のWWWブラウザでJavaScriptが「無効」に設定されていると、仮想APの名称を選択したとき、[Web認証]項目と[カスタムページ]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。
- ③ ページタイトル 無線LAN端末からアクセスするWeb認証ページのタイトルを、任意の255文字以内で入力します。 (出荷時の設定 : Set your page title.)
- ④ ポータルサイト Web認証成功後にアクセスするポータルサイトのURLを、「http://」も含めて半角255文字以内で入力します。
(出荷時の設定 : http://www.example.com/)

3 設定画面について

「Web認証 基本」画面

ネットワーク設定 > Web認証 > 基本

■ Web認証(つづき)

※「基本」画面、「詳細」画面と併せて設定してください。

※「https://」ではじまるサイトにアクセスした場合、認証ページは表示されません。

- ⑤ 移動待ち時間 Web認証成功後、Web認証用ページからポータルサイトに移動するまでの時間(秒)を設定します。
設定できる範囲は、「0～60」(秒)です。
(出荷時の設定：5)
- ⑥ 有効期限 端末が本製品に接続しているときのWeb認証の有効期限を設定します。
(出荷時の設定：24時間)
有効期限を経過すると次のアクセスは制限され、再度認証する必要があります。
有効期限は、「5分/10分/15分/30分/1時間/2時間/4時間/8時間/12時間/24時間」から選択します。
- ⑦ 〈登録〉 [Web認証] 項目で設定した内容を登録するボタンです。
- ⑧ 〈取消〉 [Web認証] 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。

「Web認証」画面で設定を変更するときのご注意

別のインターフェースと併せて設定するときは、〈登録〉を操作してから、別のインターフェースを選択してください。
〈登録〉の操作をしないで別のインターフェースを選択したときは、変更する前の設定内容に戻ります。

3 設定画面について

「Web認証 基本」画面

ネットワーク設定 > Web認証 > 基本

■ カスタムページの作成について

Web認証ページに表示される内容を出荷時の状態から変更するときは、カスタムページ(拡張子: tmpl)を作成して登録します。

※カスタムページの上限は、32Kバイトです。

※登録するカスタムページの作成方法は、3-40ページをご覧ください。

カスタムページ	
ログインページ:	参照...
	登録 プレビュー
認証成功ページ:	参照...
	登録 プレビュー

【登録の手順】

1. 〈参照...〉をクリックして、カスタムページ(拡張子: tmpl)の保存先を指定します。
2. 〈登録〉をクリックします。
〈プレビュー〉をクリックすると、登録したページを表示します。
※出荷時の状態にするときは、〈初期状態に戻す〉をクリックします。

【ご参考】

出荷時のWeb認証ページについて

◎ログインページの場合

Set your page title. ログイン失敗時はここにメッセージが表示されます ユーザー名とパスワードを入力してください。 <table border="1"><tr><td>ユーザー名</td><td> </td></tr><tr><td>パスワード</td><td> </td></tr><tr><td colspan="2">ログイン 取り消し</td></tr></table>	ユーザー名		パスワード		ログイン 取り消し	
ユーザー名						
パスワード						
ログイン 取り消し						

◎認証成功ページの場合

Set your page title. 認証に成功しました。 5秒後にポータルサイトに移動します。 自動で移動しない場合はこちらをクリックしてください。

3 設定画面について

「Web認証 基本」画面

ネットワーク設定 > Web認証 > 基本

■ カスタムページの作成について(つづき)

下記サンプルページのソースを参考にカスタムページを作成してください。

※UTF-8以外の文字コードには対応していませんので、カスタムページの文字コードは、必ずUTF-8で保存してください。

※カスタムページには、画像やほかのサイトへのリンクを作成できませんのでご注意ください。

◎ ログインページの場合

Set your page title.
ログイン失敗時はここにメッセージが表示されます
ユーザー名とパスワードを入力してください。

ユーザー名	
パスワード	
ログイン 取り消し	

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
  <head>
<!--
カスタムページの文字コードは必ずUTF-8で保存してください。UTF-8以外の文字コードには対応していません。
-->
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <meta http-equiv="Content-Style-Type" content="text/css">
    <meta http-equiv="Pragma" content="no-cache">
    <style type="text/css">
<!--
    body {
        text-align: center;
    }
    table {
        margin-right: auto;
        margin-left: auto;
        padding: 8px;
        border: 1px solid;
            border-color: black;
        width: auto;
    }
    td {
        vertical-align: top;
        white-space: nowrap;
        border: 0px;
    }
    .main {
        text-align: left;
    }
    .title {
        text-align: center;
        margin: 8px;
    }
    .notice {
        text-align: center;
        margin: 8px;
        color: red;
    }
-->
```

3 設定画面について

「Web認証 基本」画面

ネットワーク設定 > Web認証 > 基本

■ カスタムページの作成について(つづき)

◎ ログインページの場合

```
.info {
    text-align: center;
    margin: 8px;
}
.center {
    text-align: center;
}
.input {
    width: 16em;
}
-->
</style>
<!-- {{TITLE}}の部分は設定画面にある「ページタイトル」に設定された内容に置き換わります。-->
<title>{{TITLE}}</title>
</head>
<body>
<!-- フォームのmethodは必ず以下のフォーマットにしてください -->
<form target="_self" method="POST">
    <div class="main">
        <h1 class="title">{{TITLE}}</h1>
        <div class="notice">
            <!-- {{NOTICE}}の部分はログイン失敗時に表示するエラーメッセージに置き換わります -->
            {{NOTICE}}
        </div>
        <div class="info">
            ユーザー名とパスワードを入力してください。
        </div>
        <table>
            <tr>
                <td>ユーザー名</td>
                <td>
                    <!-- ユーザー名は必ず以下のフォーマットにしてください -->
                    <input class="input" type="text" maxlength="128" name="user">
                </td>
            </tr>
            <tr>
                <td>パスワード</td>
                <td>
                    <!-- パスワードは必ず以下のフォーマットにしてください -->
                    <input class="input" type="password" maxlength="128" name="pass">
                </td>
            </tr>
            <tr>
                <td></td>
                <td>
                    <input type="submit" value="ログイン">
                    <input type="reset" value="取り消し">
                </td>
            </tr>
        </table>
    </div>
</form>
</body>
</html>
```


3 設定画面について

「Web認証 基本」画面

ネットワーク設定 > Web認証 > 基本

■ カスタムページの作成について(つづき)

◎ 認証成功ページの場合

Set your page title.

認証に成功しました。
5秒後にポータルサイトに移動します。

自動で移動しない場合は[こちら](#)をクリックしてください。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
  <head>
<!--
カスタムページの文字コードは必ずUTF-8で保存してください。UTF-8以外の文字コードには対応していません。
-->
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <meta http-equiv="Content-Style-Type" content="text/css">
    <meta http-equiv="Pragma" content="no-cache">
<!--
{{WAIT_TIME}}, {{PORTAL_SITE}}の部分は設定画面にある次の設定項目に設定された内容に置き換わります。
{{WAIT_TIME}} 移動待ち時間
{{PORTAL_SITE}} ポータルサイト
-->
    <meta http-equiv="Refresh" content="{{WAIT_TIME}};URL={{PORTAL_SITE}}">
    <style type="text/css">
<!--
body {
  text-align: center;
}
.main {
  text-align: left;
}
.title {
  text-align: center;
  margin: 8px;
}
.info {
  text-align: center;
  margin: 8px;
}
-->
</style>
<!-- {{TITLE}}の部分は設定画面にある「ページタイトル」に設定された内容に置き換わります。 -->
<title>{{TITLE}}</title>
</head>
<body>
  <div class="main">
    <h1 class="title">{{TITLE}}</h1>
    <div class="info">
      認証に成功しました。<br>
      {{WAIT_TIME}}秒後にポータルサイトに移動します。<br>
      <br>
      自動で移動しない場合は<a href="{{PORTAL_SITE}}">こちら</a>をクリックしてください。
    </div>
  </div>
</body>
</html>
```

「Web認証 詳細」画面

ネットワーク設定 > Web認証 > 詳細

■ Web認証方法

仮想APごとにWeb認証方法を設定します。

Web認証方法	
インターフェース : ①	ath0
認証方法 : ②	RADIUSのみ使用

- ① 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、[認証方法] (②) 欄でWeb認証方法の設定を変更できます。
※無線LAN1はath0、ath01～ath07、無線LAN2はath1、ath11～ath17から選択します。
※災害用仮想AP(ath08、ath18)には設定できません。(P.3-116)
※「Web認証」－「基本」画面にある[Web認証] 欄(P.3-37)を「無効」にしたインターフェースの場合、「詳細」画面の設定は動作しません。
- ② 認証方法 [インターフェース] (①) 欄で選択したインターフェースについて、Web認証の認証方法を選択します。 (出荷時の設定：RADIUSのみ使用)
- ◎RADIUSのみ使用
RADIUSサーバーだけをWeb認証に使用します。
※RADIUSサーバーの指定が必要です。(P.3-44)
- ◎ローカルリストのみ使用
RADIUSサーバーを使用せず、[現在の登録] 項目に表示されたユーザー情報をWeb認証に使用します。(P.3-45)
※ローカルリストの設定が必要です。
- ◎ローカルリストを優先
[現在の登録] 項目に表示されたユーザー情報を優先してWeb認証に使用します。
ユーザー情報が検索できなかったときは、[RADIUS設定] 項目で指定されたRADIUSサーバーをWeb認証に使用します。
※RADIUSサーバーの指定と、ローカルリストの設定が必要です。
(P.3-44、P.3-45)
- ◎RADIUSを優先
RADIUSサーバーを優先してWeb認証に使用します。
RADIUSサーバーからの応答がない場合は、[現在の登録] 項目に表示されたユーザー情報をWeb認証に使用します。
※RADIUSサーバーの指定と、ローカルリストの設定が必要です。
(P.3-44、P.3-45)
※ご使用のWWWブラウザでJavaScriptが「無効」に設定されていると、仮想APの名称を選択したとき、[Web認証方法] 項目の[認証方法] 欄と[RADIUS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。

3 設定画面について

「Web認証 詳細」画面

ネットワーク設定 > Web認証 > 詳細

■ RADIUS設定

仮想APごとにWeb認証方法を設定します。

※ [Web認証方法] 項目の [認証方法] 欄で、「ローカルリストのみ使用」が選択されているときは表示されません。
(P.3-43)

RADIUS設定	
① プライマリー	セカンダリー
アドレス: ②	
ポート: ③ 1812	1812
シークレット: ④ secret	secret
	⑤ 登録 ⑥ 取消

- ① 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サーバーを設定します。(②～④)
- ② 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。
- ③ 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。
設定できる範囲は、「1～65535」です。(出荷時の設定：1812)
※ご使用になるシステムによっては、初期値と異なることがありますのでご確認ください。
- ④ 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。
大文字/小文字の区別に注意して、半角64文字以内の英数字で入力します。
- ⑤ <登録> …………… 「Web認証方法」項目や「RADIUS設定」項目で設定した内容を登録するボタンです。
- ⑥ <取消> …………… 「Web認証方法」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。

3 設定画面について

「Web認証 詳細」画面

ネットワーク設定 > Web認証 > 詳細

■ ローカルリスト

Web認証に使用するユーザー名とパスワードを登録します。

最大32件まで登録できます。

※ [Web認証方法] 項目の [認証方法] 欄で、「RADIUSのみ使用」が選択されているときは表示されません。(P.3-43)

ローカルリスト		
① ユーザー名	② パスワード	③
		追加

① ユーザー名 Web認証に使用するユーザー名を128文字以内(任意の半角英数字/記号)で入力します。
※空白(設定なし)は、登録できません。

② パスワード Web認証に使用するパスワードを128文字以内(任意の半角英数字/記号)で入力します。
※空白(設定なし)は、登録できません。

③ 〈追加〉 入力した内容(①～②)を[現在の登録]項目の各欄に登録するボタンです。

ネットワーク設定 > Web認証 > 詳細

■ 現在の登録

[ローカルリスト]項目で登録した内容が表示されます。

※画面の値は、登録例です。

現在の登録		
ユーザー名	パスワード	
icom		削除

〈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 設定画面について

「POPCHAT@Cloud」画面

ネットワーク設定 > POPCHAT@Cloud

■ アカウント設定

POPCHAT@Cloudのアカウント情報などを本製品に設定すると、端末が本製品に接続し、WWWブラウザで任意のサイトにアクセスしたとき、Wi-Fi認証@クラウドの認証ページが表示されます。

表示されたページにしたがって必要事項を入力し、認証されると端末がインターネットにアクセスできます。

※本機能を設定する前にご契約が必要です。弊社営業窓口にお問い合わせください。

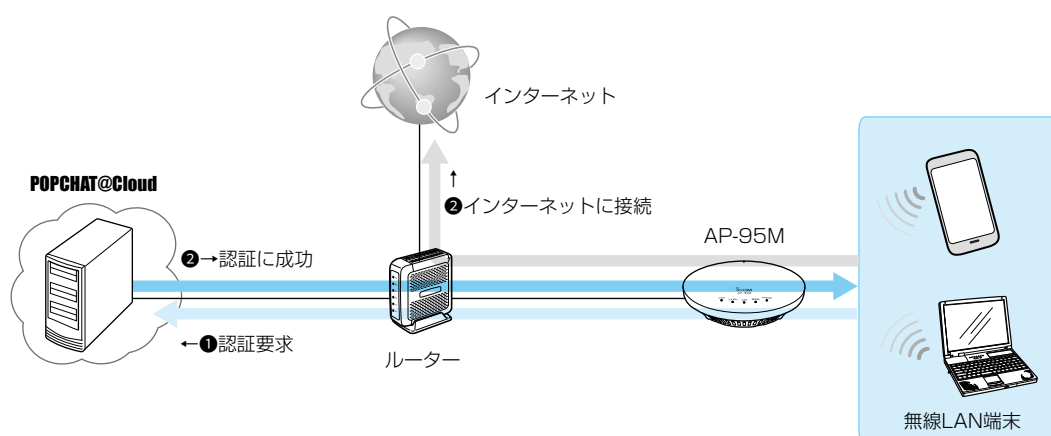
※POPCHAT@Cloud連携機能は、インターフェースごとに設定できます。(P.3-47)

※本機能を使用するには、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、本体の時刻設定(手動設定またはNTPによる自動設定)が必要です。

アカウント設定

アクティベートキー: _____

アクティベートキー…………… 指定されたアクティベートキーを半角64文字以内で入力します。
(出荷時の設定：空白(なし))



3 設定画面について

「POPCHAT@Cloud」画面

ネットワーク設定 > POPCHAT@Cloud

■ インターフェース設定

POPCHAT@Cloud連携機能で使用する仮想APを設定します。

- ① インターフェース POPCHAT@Cloud連携機能で使用する仮想APを選択します。
(出荷時の設定：ath0)
仮想APごとに、Wi-Fi認証@クラウド(②)を設定できます。
※無線LAN1はath0、ath01～ath07、無線LAN2はath1、ath11～ath17から選択します。
※災害用仮想AP(ath08、ath18)には設定できません。(P.3-116)
- ② Wi-Fi認証@クラウド [インターフェース](①)欄で選択したインターフェースについて、Wi-Fi認証@クラウドを使用するときは、「有効」に設定します。(出荷時の設定：無効)
※Wi-Fi認証@クラウドを使用できる仮想APは、「仮想AP」画面の[仮想AP]欄が「有効」に設定されたものだけです。
※ご使用のWWWブラウザでJavaScriptが無効に設定されていると、仮想APの名称を選択したとき、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。
- ③ 〈登録〉 「POPCHAT@Cloud」画面で設定した内容を登録するボタンです。
- ④ 〈取消〉 「POPCHAT@Cloud」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。

3 設定画面について

「WAN接続先」画面

ルーター設定 > WAN接続先

■ 回線状態表示 (DHCPクライアント設定時)

[回線種別設定]項目(P.3-51)、[回線設定]項目(P.3-52)で設定したWAN側回線への接続状態が表示されます。
※画面の値は、表示例です。

回線状態表示	
① 接続状態	ケーブル未接続
② 回線種別	DHCPクライアント
③ 本体側のIPアドレス	
④ 相手先のIPアドレス	
⑤ DNSサーバー	

- ① 接続状態 WAN側回線への接続状態が「ケーブル未接続」/「接続試行中」/「接続中」で表示されます。
- ② 回線種別 本製品に設定されている回線への接続方式が表示されます。
- ③ 本体側のIPアドレス 本製品のWAN側に自動取得したIPアドレスが表示されます。
- ④ 相手先のIPアドレス DHCPで自動取得したデフォルトゲートウェイが表示されます。
- ⑤ DNSサーバー 手動設定、またはDHCPで自動取得したDNSサーバーアドレスが表示されます。

3 設定画面について

「WAN接続先」画面

ルーター設定 > WAN接続先

■ 回線状態表示 (固定IP設定時)

[回線種別設定] 項目 (P.3-51)、[回線設定] 項目 (P.3-53) で設定した WAN 側回線への接続状態が表示されます。
※画面の値は、表示例です。

回線状態表示	
① 接続状態	ケーブル未接続
② 回線種別	固定IP
③ 本体側のIPアドレス	
④ 相手先のIPアドレス	
⑤ DNSサーバー	

- ① 接続状態 WAN側回線への接続状態が「ケーブル未接続」/「接続試行中」/「接続中」で表示されます。
- ② 回線種別 本製品に設定されている回線への接続方式が表示されます。
- ③ 本体側のIPアドレス 本製品のWAN側に設定したIPアドレスが表示されます。
- ④ 相手先のIPアドレス 手動設定したデフォルトゲートウェイが表示されます。
- ⑤ DNSサーバー 手動設定したDNSサーバーアドレスが表示されます。

3 設定画面について

「WAN接続先」画面

ルーター設定 > WAN接続先

■ 回線状態表示 (PPPoE設定時)

[回線種別設定]項目(P.3-51)、[回線設定]項目(P.3-54)で設定したWAN側回線への接続状態が表示されます。
※画面の値は、表示例です。

回線状態表示		
PPPoEセッション	第1セッション	第2セッション
① 接続先の選択	WAN01 ▼ 接続	なし ▼ 接続
② 接続状態		
③ 回線種別	PPPoE	PPPoE
④ 本体側のIPアドレス		
⑤ 相手先のIPアドレス		
⑥ DNSサーバー		
⑦ 接続時間		

- ① 接続先の選択 [回線設定]項目(P.3-54)で登録したWAN側回線への接続先から選択します。
※回線接続中は、選択できません。
- <接続>
 「未接続」のセッションに接続するとき、クリックします。
- <切断>
 現在接続しているセッションを切断するとき、クリックします。
- ② 接続状態 WAN側回線への接続状態が「ケーブル未接続」/「未接続」/「接続試行中」/「接続中」で表示されます。
- ③ 回線種別 本製品に設定されている回線への接続方式が表示されます。
- ④ 本体側のIPアドレス 本製品のWAN側に設定したIPアドレス、または接続先より割り当てられたIPアドレスが表示されます。
- ⑤ 相手先のIPアドレス ご契約の回線接続業者のIPアドレスが表示されます。
- ⑥ DNSサーバー ご契約の回線接続業者のDNSサーバーアドレスが表示されます。
- ⑦ 接続時間 ご契約の回線接続業者に接続してから、この画面にアクセスした時点までの時間が表示されます。

3 設定画面について

「WAN接続先」画面

ルーター設定 > WAN接続先

■ 回線種別設定

本製品の回線種別についての設定です。

回線種別設定

回線種別: ① LANポートとして使用する

② ③ ✓

登録 取消

- ① **回線種別** ご契約の回線接続業者から指定された回線種別を選択します。
(出荷時の設定: LANポートとして使用する)
「DHCPクライアント」、「固定IP」、「PPPoE」を設定したときは、ルーター機能が有効になり、本製品の[LAN]ポートをWANポートとして使用できます。
※ルーター機能が有効のときは、本製品のWAN側IPアドレスが有線LAN側の設定になり、WAN側(有線LAN)と無線LAN間は、ルーティングされます。
- LANポートとして使用する**
[LAN]ポートに切り替わりますので、HUBやルーターなどのネットワーク機器と接続します。
- DHCPクライアント**
ルーター機能を使用する場合で、本製品のWAN側IPアドレスを、ご契約の回線接続業者から「DHCP」方式で取得します。
- 固定IP**
ルーター機能を使用する場合で、本製品のWAN側IPアドレスを、ご契約の回線接続業者から指定された固定のIPアドレスを割り当てて使用します。
- PPPoE**
本製品のWAN側IPアドレスを、ご契約の回線接続業者から「PPPoE」方式で取得します。
- ② **〈登録〉** 「回線種別設定」項目で設定した内容を登録するボタンです。
- ③ **〈取消〉** 「回線種別設定」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。

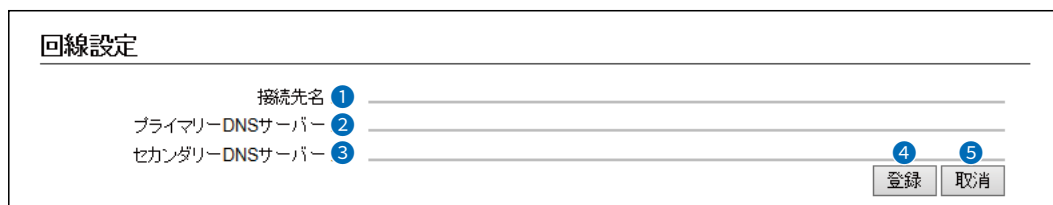
3 設定画面について

「WAN接続先」画面

ルーター設定 > WAN接続先

■ 回線設定 (DHCPクライアント設定時)

[回線種別設定]項目(P.3-51)で選択した本製品のWAN側回線について設定します。



- | | |
|----------------------|--|
| ① 接続先名 | ご契約の回線接続業者の名前を任意の英数字31文字以内で入力します。 |
| ② プライマリDNSサーバー | ご契約の回線接続業者から指定された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。 |
| ③ セカンダリDNSサーバー | [プライマリDNSサーバー](②)欄と同様、DNSサーバーのアドレスが2つある場合は、DNSサーバーアドレスのもう一方を入力します。 |
| ④ <登録> | 「回線設定」項目で設定した内容を登録するボタンです。 |
| ⑤ <取消> | 「回線設定」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。 |

DHCPによる自動取得について

DHCPクライアント設定時、[プライマリDNSサーバー]欄、[セカンダリDNSサーバー]欄が共に空白の場合、DHCPによる自動取得を開始します。

自動取得に成功すると、[回線状態表示]項目の[DNSサーバー]欄にIPアドレスが表示されます。(P.3-48)

3 設定画面について

「WAN接続先」画面

ルーター設定 > WAN接続先

■ 回線設定 (固定IP設定時)

[回線種別設定] 項目(P.3-51)で選択した本製品のWAN側回線について設定します。

- | | |
|-----------------------|--|
| ① 接続先名 | ご契約の回線接続業者の名前を任意の英数字31文字以内で入力します。 |
| ② IPアドレス | ご契約の回線接続業者から指定された本製品のWAN側IPアドレスを入力します。 |
| ③ サブネットマスク | ご契約の回線接続業者から指定された本製品のWAN側のサブネットマスクを入力します。 |
| ④ デフォルトゲートウェイ | ご契約の回線接続業者から指定された本製品のデフォルトゲートウェイを入力します。 |
| ⑤ プライマリーDNSサーバー | ご契約の回線接続業者から指定された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。 |
| ⑥ セカンダリーDNSサーバー | [プライマリーDNSサーバー] (⑤)欄と同様、DNSサーバーのアドレスが2つある場合は、DNSサーバーアドレスのもう一方を入力します。 |
| ⑦ <登録> | 「回線設定」項目で設定した内容を登録するボタンです。 |
| ⑧ <取消> | 「回線設定」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。 |

3 設定画面について

「WAN接続先」画面

ルーター設定 > WAN接続先

■ 回線設定 (PPPoE設定時)

[回線種別設定]項目(P.3-51)で選択した本製品のWAN側回線について設定します。

回線設定

接続先の選択 ①

WAN01 (ppp0)

▼

接続先名 ②

WAN01

ユーザーID ③

パスワード ④

接続方法 ⑤

常時

▼

IPアドレス ⑥

プライマリーDNSサーバー ⑦

セカンダリーDNSサーバー ⑧

認証プロトコル ⑨

接続先に合わせる

▼

MSS制限値 ⑩

1322

⑪ 登録

⑫ 取消

- ① 接続先の選択 接続先を追加するときは、「WAN01 (ppp0)」～「WAN08 (ppp7)」(最大8件まで設定可能)から選択します。(出荷時の設定：WAN01 (ppp0))
登録されている接続先の内容を変更するときは、編集する接続先名を選択します。
- ② 接続先名 ご契約の回線接続業者の名前を任意の英数字31文字以内で入力します。
- ③ ユーザーID ご契約の回線接続業者から指定されたログインユーザー名、またはアカウント名を大文字/小文字の表記に注意して入力します。
- ④ パスワード ご契約の回線接続業者から指定されたログインパスワードを大文字/小文字の表記に注意して入力します。
入力中の文字は、すべて* (アスタリスク)、または●(黒丸)で表示されます。
- ⑤ 接続方法 「PPPoE」回線への接続方法を選択します。(出荷時の設定：常時)
- ◎手動
[回線状態表示]項目の<接続>/<切断>をクリックして、回線を手動で接続、または切断できます。(P.3-50)
※本製品を起動したときは、切断された状態です。
- ◎常時
常時接続します。
[接続先の選択](①)欄で指定した接続先と常に接続状態を保持します。
※本製品を起動したときは、接続された状態です。
※[回線状態表示]項目の<接続>/<切断>をクリックすると、手動で操作できます。(P.3-50)
- ⑥ IPアドレス ご契約の回線接続業者から指定されたときに限り、本製品のWAN側IPアドレスを入力します。

3 設定画面について

「WAN接続先」画面

ルーター設定 > WAN接続先

■ 回線設定 (PPPoE設定時)

回線設定

接続先の選択

1

WAN01 (ppp0)

▼

接続先名

2

WAN01

ユーザーID

3

パスワード

4

接続方法

5

常時

▼

IPアドレス

6

プライマリーDNSサーバー

7

セカンダリーDNSサーバー

8

認証プロトコル

9

接続先に合わせる

▼

MSS制限値

10

1322

11

登録

12

取消

- ⑦ **プライマリーDNSサーバー** …… ご契約の回線接続業者から指定された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。
- ⑧ **セカンダリーDNSサーバー** …… [プライマリーDNSサーバー] (⑦) 欄と同様、DNSサーバーのアドレスが2つある場合は、DNSサーバーアドレスのもう一方を入力します。
- ⑨ **認証プロトコル** …………… ご契約の回線接続業者から指定された、認証プロトコルを設定します。
(出荷時の設定：接続先に合わせる)
指定のない場合は、「接続先に合わせる」でご使用ください。
- ◎PAP
パスワードによってユーザーを識別します。
パスワードが暗号化されないなどの弱点があります。
- ◎CHAP
認証情報のやり取りが暗号化されるため、PAPよりも安全性が高い認証プロトコルです。
- ⑩ **MSS制限値** …………… ご契約の回線接続業者から指定されている場合に限り、WAN側回線への最大有効データ長を数字で指定します。(出荷時の設定：1322)
設定できる範囲は、「536～1452(バイト)」です。
MSS値とは、受信できるTCP最大セグメントサイズのことです。
一般に、MSS値はフラグメントが発生しない範囲で大きいほどよいとされています。
しかし、[PPPoE]回線のMTUは、通常のEthernetのMTU(1500バイト)より小さいため、MSS値が大きくなりすぎると、パケットがインターネット上を通過しないことがありますのでご注意ください。
- ⑪ **〈登録〉** …………… 「回線設定」項目で設定した内容を登録するボタンです。
- ⑫ **〈取消〉** …………… 「回線設定」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。

3 設定画面について

「WAN接続先」画面

ルーター設定 > WAN接続先

■ 回線設定一覧 (PPPoE設定時)

[回線設定] 項目 (P.3-54) で登録した接続先の一覧です。

回線設定一覧			
接続先名	ユーザーID	接続方法	
WAN01(ppp0)		常時	削除

〈削除〉…………… ボタンの左欄に表示された内容を削除するとき、クリックします。

3 設定画面について

「アドレス変換」画面

ルーター設定 > アドレス変換

■ アドレス変換設定

本製品のアドレス変換機能を設定します。

※回線種別を「DHCPクライアント」、「固定IP」、「PPPoE」に設定(P.3-51)したときに、有効になります。

アドレス変換設定 アドレス変換: ☐ 無効 ☒ 有効

アドレス変換…………… 本製品のアドレス変換機能を設定します。 (出荷時の設定：有効)
「有効」に設定すると、本製品のIPマスカレード機能を使用して、WAN側グローバルアドレスをプライベートアドレスに変換します。

ルーター設定 > アドレス変換

■ DMZホスト設定

本製品のDMZホスト機能を設定します。

DMZホスト設定 DMZホスト IPアドレス: ① ② 登録 ③ 取消

- ① DMZホスト IPアドレス** …… DMZホスト機能(非武装セグメント)の対象となるパソコン(ホスト)のIPアドレスを入力します。
DMZホスト機能を使用すると、WAN(インターネット)側から受信した転送先不明のIPフレームを、LAN側に存在する特定IPアドレスへ転送できます。これにより、本製品のLAN側に存在する端末で各種サーバーを運用したり、ネットワーク対戦ゲームをしたりできますが、転送先に設定した端末のIPアドレスに対してセキュリティが低下しますので、ご使用には十分ご注意ください。
※DMZホスト機能と静的マスカレードテーブルを同時に使用した場合は、静的マスカレードテーブルの設定が優先されます。
※セキュリティの低下で生じる結果については、弊社で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。
- ② 〈登録〉** …………… 「アドレス変換設定」項目や「DMZホスト設定」項目で設定した内容を登録するボタンです。
- ③ 〈取消〉** …………… 「アドレス変換設定」項目や「DMZホスト設定」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。

3 設定画面について

「アドレス変換」画面

ルーター設定 > アドレス変換

■ 静的マスカレードテーブル設定

静的にIPマスカレード変換をするための設定です。

テーブルに追加すると、マスカレードIP(ルーターグローバルIP)に対して、アクセスしてきたパケットをプロトコルにより判定し、ここで指定したプライベートIPアドレスを割り当てたローカル端末へアドレス変換します。

静的マスカレードテーブル設定				
WAN側ポート ①	LAN側IP ②	LAN側ポート ③	プロトコル ④	⑤
指定 ▼		指定 ▼	TCP ▼	追加

- ① WAN側ポート 選択したプロトコル(④)に対するWAN側ポートを数字で指定するときは、「指定」を選択します。
数字で指定しない場合は、ニーモニック(DNS、Finger、FTP、Gopher、NEWS、POP3、SMTP、Telnet、Web、Whois)から選択します。
- ② LAN側IP 該当するパケットを転送するLAN側プライベートIPアドレスを入力します。
- ③ LAN側ポート 選択したプロトコル(④)に対するLAN側ポートを数字で指定するときは、「指定」を選択します。
数字で指定しない場合は、ニーモニック(DNS、Finger、FTP、Gopher、NEWS、POP3、SMTP、Telnet、Web、Whois)から選択します。
- ④ プロトコル TCP、UDP、TCP/UDP、GRE、ESPから選択します。
- ⑤ 〈追加〉 静的マスカレードテーブルを本製品に登録するとき、クリックします。
※最大32個のマスカレードテーブルを登録できます。

ルーター設定 > アドレス変換

■ 静的マスカレードテーブル設定

[静的マスカレードテーブル設定]項目で登録した内容が表示されます。

※画面の値は、設定例です。

静的マスカレードテーブル設定一覧					
WAN側ポート	LAN側IP	LAN側ポート	プロトコル	①	②
22	192.168.0.10	8022	TCP	編集	削除
Web	192.168.0.10	Web	TCP	編集	削除

- ① 〈編集〉 登録した内容を編集するときは、該当する欄の〈編集〉をクリックします。
※登録されている内容は、[静的マスカレードテーブル設定]項目に表示されます。
- ② 〈削除〉 登録した内容を削除するときは、該当する欄の〈削除〉をクリックします。

3 設定画面について

「IPフィルター」画面

ルーター設定 > IPフィルター

■ 一般設定

本製品で使用するIPフィルターの共通設定です。

一般設定

遮断時の動作：① ☒ 破棄 ☐ 拒絶

IPフィルター不一致時のSYSLOG：② ☒ 無効 ☐ 有効

③ 登録 ④ 取消

- ① 遮断時の動作 パケットを遮断するときの動作を選択します。 (出荷時の設定：破棄)
◎破棄：パケットを破棄し、相手に何も返しません。
◎拒絶：受け取らないという拒否パケットを相手に返します。
- ② IPフィルター不一致時の
SYSLOG WAN側から開始し、どのIPフィルターにも一致しないパケットの場合、遮断
します。このとき、ログに記録するかどうかを設定します。
(出荷時の設定：無効)
※大量のログを処理すると、システム処理速度に影響します。
- ③ 〈登録〉 [一般設定]項目で設定した内容を登録するボタンです。
- ④ 〈遮断〉 [一般設定]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。

3 設定画面について

「IPフィルター」画面

ルーター設定 > IPフィルター

■ IPフィルター設定

登録した条件に該当するパケットの通過と阻止についての設定です。

※IPフィルターの変更によるセキュリティの低下で生じる結果については、弊社で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。

※説明のため、[プロトコル] (7) 欄を「TCP」に設定したときに表示される画面を使用しています。

IPフィルター設定

番号: 1

エントリー: ☐ 無効 ☒ 有効

フィルター方法: ☐ 遮断 ☒ 透過

フィルター方向: ☒ IN ☐ OUT

送信元IPアドレス: マスク: 32

宛先IPアドレス: マスク: 32

プロトコル: TCP 指定時:

送信元ポート番号: すべて 指定時: ~

宛先ポート番号: すべて 指定時: ~

TCPフラグ: ☐ URG ☐ ACK ☐ PSH ☐ RST ☐ SYN ☐ FIN

SYSLOGに出力: ☒ 無効 ☐ 有効

登録 取消

① 番号 IPフィルターが比較する順位を指定します。
選択できる範囲は、「1」～「64」です。
IPフィルター機能を使用時、本製品が受信、送信、または転送するパケットと
[IPフィルター設定一覧] 項目の内容を比較します。
一致した場合、設定に応じた処理を実行して比較を終了します。

② 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: 有効)
登録しても使用しないときは、「無効」を選択します。
「無効」で登録すると、下記の画面のように、[IPフィルター設定一覧] 項目の
[番号] 欄に「(off)」が表示されます。

1 (off)	透過	TCP (フラグ指定なし)	* (*)	無効	編集	削除
	IN		* (*)			

③ フィルター方法 フィルタリングの方法は、次の2とおりから選択します。
(出荷時の設定: 透過)
◎遮断: フィルタリングの条件に一致した場合、そのパケットをすべて破棄
します。
◎透過: フィルタリングの条件に一致した場合、そのパケットをすべて通過
させます。

3 設定画面について

「IPフィルター」画面

ルーター設定 > IPフィルター

■ IPフィルター設定

※説明のため、[プロトコル](7)欄を「TCP」に設定したときに表示される画面を使用しています。

- 4 フィルター方向 フィルターの対象となるパケットの通信方向を設定します。
(出荷時の設定：IN)
◎IN : WAN側から受信するパケットに対してフィルタリング処理をします。
◎OUT : WAN側へ送信するパケットに対してフィルタリング処理をします。
- 5 送信元IPアドレス 送信元ホストのIPアドレス、サブネットマスク(ビット数)を設定することにより、特定のホストからのパケットをフィルタリング処理します。
何も設定しない場合は、すべてのアドレスを対象とします。
マスク(ビット数)の選択できる範囲は、「1」～「32」です。
- 6 宛先IPアドレス 宛先ホストのIPアドレス、サブネットマスク(ビット数)を設定することにより、特定のホストからのパケットをフィルタリング処理します。
何も設定しない場合は、すべてのアドレスを対象とします。
マスク(ビット数)の選択できる範囲は、「1」～「32」です。
- 7 プロトコル フィルタリングの対象となるパケットのトランスポート層プロトコルを選択する項目です。
(出荷時の設定：すべて)
◎すべて : すべてのプロトコルに一致します。
◎TCP : TCPだけに一致します。
「TCP」を選択すると、[送信元ポート番号](8)欄、[宛先ポート番号](9)欄、[TCPフラグ](10)欄が表示されます。
◎UDP : UDPだけに一致します。
「UDP」を選択すると、[送信元ポート番号](8)欄、[宛先ポート番号](9)欄が表示されます。
◎TCP/UDP : TCPとUDPに一致します。
「TCP/UDP」を選択すると、[送信元ポート番号](8)欄、[宛先ポート番号](9)欄が表示されます。

3 設定画面について

「IPフィルター」画面

ルーター設定 > IPフィルター

■ IPフィルター設定

※説明のため、[プロトコル](7)欄を「TCP」に設定したときに表示される画面を使用しています。

7 プロトコル

◎ICMP

: ICMPだけに一致します。

「ICMP」を選択すると、[タイプ] 欄、[コード] 欄(下図)が表示されます。

[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。

[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。

◎IGMP

: IGMPだけに一致します。

◎指定

: 右のテキストボックスに、IP層ヘッダーに含まれる上位層プロトコル番号を入力します。

プロトコル番号は、「0 ~ 255」までの半角数字を入力します。

3 設定画面について

「IPフィルター」画面

ルーター設定 > IPフィルター

■ IPフィルター設定

※説明のため、[プロトコル](7)欄を「TCP」に設定したときに表示される画面を使用しています。

8 送信元ポート番号

フィルタリングの対象となる発信元のTCP/UDPポート番号を指定する項目です。
(出荷時の設定：すべて)

指定には、2とおりの方法があります。

◎数字で指定するとき

1. 「指定」を選択します。
2. 「指定時：(始点)～(終点)」欄のテキストボックスに番号を入力します。
特定のポートだけを指定するときは、始点だけ、または始点/終点に同一の番号を入力してください。
入力できる範囲は、「1～65535」までの半角数字です。

◎ニーモニックで指定するとき

「すべて」、「指定」以外の項目を選択します。
本製品で指定できるニーモニックは、「DNS」、「Finger」、「FTP」、「Gopher」、「NEWS」、「POP3」、「SMTP」、「Telnet」、「Web」、「Whois」です。
※「すべて」を選択した場合は、すべてのポート番号を対象とします。

3 設定画面について

「IPフィルター」画面

ルーター設定 > IPフィルター

■ IPフィルター設定

※説明のため、[プロトコル](7)欄を「TCP」に設定したときに表示される画面を使用しています。

9 宛先ポート番号

フィルタリングの対象となる宛先のTCP/UDPポート番号を指定する項目です。
(出荷時の設定：すべて)

指定には、2とおりの方法があります。

◎数字で指定するとき

1. 「指定」を選択します。
2. 「指定時：(始点)～(終点)」欄のテキストボックスに番号を入力します。
特定のポートだけを指定するときは、始点だけ、または始点/終点に同一の番号を入力してください。
入力できる範囲は、「1～65535」までの半角数字です。

◎ニーマモニックで指定するとき

「すべて」、「指定」以外の項目を選択します。
本製品で指定できるニーマモニックは、「DNS」、「Finger」、「FTP」、「Gopher」、「NEWS」、「POP3」、「SMTP」、「Telnet」、「Web」、「Whois」です。
※「すべて」を選択した場合は、すべてのポート番号を対象とします。

10 TCPフラグ

[プロトコル](7)欄で「TCP」を選択したとき、フィルタリングの対象となるTCPの通信フラグを選択する項目です。
(出荷時の設定：指定なし)
本製品で指定できるTCPフラグは、URG、ACK、PSH、RST、SYN、FINです。
※下記の画面のように選択したTCPフラグ(例：RST)を略して、[現在の登録]項目の[プロトコル(TCPフラグ)]欄に表示します。

3	透過	TCP (R)	* (*)	無効	編集	削除
	IN		* (*)			

※指定なし(チェックボックスすべてチェックなし)の場合は、TCPのフラグオプションをフィルターの条件にしません。

3 設定画面について

「IPフィルター」画面

ルーター設定 > IPフィルター

■ IPフィルター設定

※説明のため、[プロトコル](7)欄を「TCP」に設定したときに表示される画面を使用しています。

IPフィルター設定

番号: 1

エントリー: ☐ 無効 ☒ 有効

フィルター方法: ☐ 遮断 ☒ 透過

フィルター方向: ☒ IN ☐ OUT

送信元IPアドレス: マスク: 32

宛先IPアドレス: マスク: 32

プロトコル: TCP

送信元ポート番号: すべて 指定時: ~

宛先ポート番号: すべて 指定時: ~

TCPフラグ: ☐URG ☐ACK ☐PSH ☐RST ☐SYN ☐FIN

SYSLOGに出力: ☒ 無効 ☐ 有効

登録 取消

- 11 SYSLOGに出力 IPフィルター登録時、このオプションを「有効」に設定すると、フィルタリング処理をしたとき、SYSLOGを出力します。（出荷時の設定：無効）
※大量のログを処理すると、システム処理速度に影響します。
- 12 〈登録〉 [IPフィルター設定] 項目で設定した内容を登録するボタンです。
- 13 〈取消〉 [IPフィルター設定] 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。

3 設定画面について

「IPフィルター」画面

ルーター設定 > IPフィルター

■ IPフィルター設定一覧

[IPフィルター設定]項目(P.3-60～P.3-65)から登録した現在の各エントリーの内容が表示されます。

IPフィルター設定一覧					
番号	フィルター方法	プロトコル (TCPフラグ)	送信元IPアドレス (送信元ポート番号)	SYSLOGに出力	
	フィルター方向		宛先IPアドレス (宛先ポート番号)		
59	遮断	TCP/UDP	* (135)	無効	① 編集 ② 削除
	OUT		* (*)		
60	遮断	TCP/UDP	* (*)	無効	編集 削除
	OUT		* (135)		
61	遮断	TCP/UDP	* (445)	無効	編集 削除
	OUT		* (*)		
62	遮断	TCP/UDP	* (*)	無効	編集 削除
	OUT		* (445)		
63	遮断	TCP (フラグ指定なし)	* (*)	無効	編集 削除
	OUT		* (137-139)		
64	遮断	UDP	* (137-139)	無効	編集 削除
	OUT		* (137-139)		

出荷時、または全設定を初期化したときから登録されているIPフィルターについて

◎59～64番：Windowsのアプリケーションを外部からリモートコントロールされる危険性、およびファイル共有機能による外部への情報漏えいを防止する

※「*」は、各欄で設定できる「すべて」を対象としています。

①〈編集〉…………… ボタンの左側に表示されたIPフィルターを編集するボタンです。
〈編集〉をクリックすると、表示された内容が[IPフィルター設定]項目の各欄
に表示されます。

②〈削除〉…………… ボタンの左側に表示されたIPフィルターを削除するボタンです。

3 設定画面について

「簡易DNS」画面

ルーター設定 > 簡易DNS

■ 簡易DNSサーバー設定

本製品を簡易DNSサーバーとして使用するとき設定します。

※「DHCPサーバー」画面の「DNS代理応答」欄(P.3-15)を「有効」に設定しておく必要があります。

簡易DNSサーバー設定		
※DHCPサーバーのDNS代理応答を有効にしておく必要があります。		
IPアドレス	ホスト名	
		追加

端末のホスト名と対応するIPアドレスの組み合わせを入力して、〈追加〉をクリックします。

登録すると、ドメイン名からIPアドレスを検索するDNS要求と、IPアドレスからドメイン名を検索するDNS逆引き要求に応答します。

※最大32個の組み合わせまで登録できます。

※本製品のDNS代理応答機能を使用する場合に有効です。

※ローカルIPアドレスとそのホスト名を登録するときは、静的DHCPサーバーを利用してMACアドレスとIPアドレスの組み合わせを固定しておくことをおすすめします。

※ホスト名として「ホスト名.ドメイン名」を登録しておく、ホスト名のみ一致する場合でも応答します。

ルーター設定 > 簡易DNS

■ 簡易DNSサーバー設定

「簡易DNSサーバー設定」項目で登録した内容が表示されます。

簡易DNSサーバー設定一覧		
IPアドレス	ホスト名	
192.168.1.50	example.local	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 設定画面について

「無線LAN設定」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 無線LAN

■ 無線LAN

本製品に内蔵された無線LANユニットに対する設定です。

◎無線LAN1：2.4GHz帯

◎無線LAN2：5GHz帯

※本書では、「無線LAN1」の画面で説明しています。

無線LAN	
無線UNIT:	① ○ 無効 ● 有効
帯域幅:	② 20 MHz ▼
チャンネル:	③ 001 CH (2412 MHz) ▼
パワーレベル:	④ 高 ▼
DTIM間隔:	⑤ 1 ▼
プロテクション:	⑥ ○ 無効 ● 有効
⑦ 登録 ⑧ 取消	

① 無線UNIT 無線LANユニットの使用を設定します。 (出荷時の設定：有効)
「有効」に設定すると、本製品の無線LAN機能を使用できます。

② 帯域幅 本製品の無線LAN機能で使用する周波数帯域幅を設定します。
(出荷時の設定：20MHz)
◎無線LAN1：「20MHz」、「40MHz」から選択できます。
◎無線LAN2：「20MHz」、「40MHz」、「80MHz」から選択できます。
※無線LAN通信で40MHz、または80MHz帯域幅をご使用になる場合、周囲の電波環境を事前に確認して、ほかの無線局に電波干渉を与えないようにしてください。
※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]欄を「20MHz」でご使用ください。
※本製品で設定した帯域幅に通信相手側が対応していない場合は、通信相手の帯域幅にしたがい、本製品で選択したチャンネル(③)で通信します。

③ チャンネル 本製品の無線LAN機能で使用するチャンネルを設定します。
(出荷時の設定：無線LAN1→001CH (2412MHz)
無線LAN2→036CH (5180MHz))
※設定した帯域幅(②)により、選択できるチャンネルが異なります。(P.v)
※2.4GHz帯使用時の電波干渉については、5-4ページをご覧ください。
※5.2/5.3GHz帯無線LANの使用は、電波法により、屋内に限定されます。
※5.3/5.6GHz帯のチャンネル選択時のDFS機能については、1-9ページをご覧ください。

3 設定画面について

「無線LAN設定」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 無線LAN

■ 無線LAN(つづき)

※本書では、「無線LAN1」の画面で説明しています。

- ④ **パワーレベル** 本製品に内蔵する無線LANユニットの送信出力を、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を高めたいとき
◎比較的狭いエリアに複数台の無線アクセスポイントが設置された環境で、近くの無線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
- ⑤ **DTIM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、初期値でご使用ください。
- ⑥ **プロテクション** 異なる無線LAN規格の混在による無線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)
- ⑦ **〈登録〉** 「無線LAN」画面で設定した内容を登録するボタンです。
- ⑧ **〈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。

3 設定画面について

「仮想AP」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 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。

◎無線LAN1：2.4GHz帯

◎無線LAN2：5GHz帯

※本書では、「無線LAN1」の画面で説明しています。

※説明のため、[アカウンティング] (8) 欄、および [MAC認証] (9) 欄を「有効」に設定したときに表示される画面を使用しています。

※災害用仮想APを選択時、下記の設定 (5 ～ 6、8 ～ 10) は表示されません。

仮想AP設定

インターフェース : ① ath0

仮想AP : ② ☒ 無効 ☐ 有効

SSID : ③ WIRELESSLAN-0

VLAN ID : ④ 0

ANY接続拒否 : ⑤ ☒ 無効 ☐ 有効

接続端末制限 : ⑥ 63

同一仮想AP内の端末間通信禁止 : ⑦ ☒ 無効 ☐ 有効

アカウンティング : ⑧ ☐ 無効 ☒ 有効

MAC認証 : ⑨ ☐ 無効 ☒ 有効

認証VLAN : ⑩ ☒ 無効 ☐ 有効

- ① 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：無線LAN1→ath0
無線LAN2→ath1)
仮想APごとに、[仮想AP設定] 項目 (② ～ ⑦) と [暗号化設定] 項目の設定内容を変更できます。
※無線LAN1はath0、ath01～ath08、無線LAN2はath1、ath11～ath18から選択します。
※「ath01～ath07」、「ath11～ath17」を使用するときは、[仮想AP] (②) 欄を「有効」にしてください。
※災害モード(P.3-116)を設定すると、インターフェースに「ath08」と「ath18」が追加されます。
※ご使用のWWWブラウザで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。
- ② 仮想AP [インターフェース] (①) 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：無線LAN1→有効(ath0)、無効(ath01～ath07)
無線LAN2→有効(ath1)、無効(ath11～ath17))
※「ath0」、「ath1」は、「無効」にできません。
※ここでは、「ath08」、「ath18」を「無効」にできません。
「無効」にするには、3-116ページをご覧ください。
※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。

3 設定画面について

「仮想AP」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ 仮想AP設定(つづき)

※本書では、「無線LAN1」の画面で説明しています。

※説明のため、[アカウントिंग](8)欄、および[MAC認証](9)欄を「有効」に設定したときに表示される画面を使用しています。

※災害用仮想APを選択時、下記の設定(5～6、8～10)は表示されません。

仮想AP設定
インターフェース: ① ath0
仮想AP: ② ☒ 無効 ☐ 有効
SSID: ③ WIRELESSLAN-0
VLAN ID: ④ 0
ANY接続拒否: ⑤ ☒ 無効 ☐ 有効
接続端末制限: ⑥ 63
同一仮想AP内の端末間通信禁止: ⑦ ☒ 無効 ☐ 有効
アカウントING: ⑧ ☐ 無効 ☒ 有効
MAC認証: ⑨ ☐ 無効 ☒ 有効
認証VLAN: ⑩ ☒ 無効 ☐ 有効

③ SSID

[インターフェース](①)欄で選択した仮想APのSSIDを設定します。

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、ath1))

WIRELESSLAN-1(ath01、ath11)
WIRELESSLAN-2(ath02、ath12)
WIRELESSLAN-3(ath03、ath13)
WIRELESSLAN-4(ath04、ath14)
WIRELESSLAN-5(ath05、ath15)
WIRELESSLAN-6(ath06、ath16)
WIRELESSLAN-7(ath07、ath17))

※災害用仮想APのSSID(00000JAPAN)は、変更できません。

※[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]の異なる無線LAN端末とは接続できません。

※無線アクセスポイントが無線伝送エリア内に複数存在しているような場合、個々の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。

④ VLAN ID

[インターフェース](①)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。

3 設定画面について

「仮想AP」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ 仮想AP設定(つづき)

※本書では、「無線LAN1」の画面で説明しています。

※説明のため、[アカウントिंग](8)欄、および[MAC認証](9)欄を「有効」に設定したときに表示される画面を使用しています。

※災害用仮想APを選択時、下記の設定(5～6、8～10)は表示されません。

仮想AP設定

インターフェース : ① ath0

仮想AP : ② ☒ 無効 ☐ 有効

SSID : ③ WIRELESSLAN-0

VLAN ID : ④ 0

ANY接続拒否 : ⑤ ☒ 無効 ☐ 有効

接続端末制限 : ⑥ 63

同一仮想AP内の端末間通信禁止 : ⑦ ☒ 無効 ☐ 有効

アカウントING : ⑧ ☐ 無効 ☒ 有効

MAC認証 : ⑨ ☐ 無効 ☒ 有効

認証VLAN : ⑩ ☒ 無効 ☐ 有効

⑤ ANY接続拒否

[インターフェース](①)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)で通信する無線LAN端末からの検索や接続の拒否について設定をします。(出荷時の設定：無効)

※一部の無線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 사용되는ことをおすすめします。

⑥ 接続端末制限

[インターフェース](①)欄で選択した仮想APに同時接続可能な無線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LANユニット全体)で最大128台までになります。

⑦ 同一仮想AP内の端末間通信禁止 ...

[インターフェース](①)欄に表示された仮想APに帰属する無線LAN端末同士の通信について設定をします。(出荷時の設定：無効)

※「有効」に設定すると、同じ仮想AP(例：ath0)に帰属する無線LAN端末間の通信を遮断します。

※異なる仮想AP(例：ath0とath01)に帰属する無線LAN端末同士の通信を禁止する場合は、パケットフィルター(P.3-20)で設定できます。

3 設定画面について

「仮想AP」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ 仮想AP設定(つづき)

※本書では、「無線LAN1」の画面で説明しています。

※説明のため、[アカウントिंग](8)欄、および[MAC認証](9)欄を「有効」に設定したときに表示される画面を使用しています。

※災害用仮想APを選択時、下記の設定(5～6、8～10)は表示されません。

仮想AP設定
インターフェース : ① ath0
仮想AP : ② ☒ 無効 ☐ 有効
SSID : ③ WIRELESSLAN-0
VLAN ID : ④ 0
ANY接続拒否 : ⑤ ☒ 無効 ☐ 有効
接続端末制限 : ⑥ 63
同一仮想AP内の端末間通信禁止 : ⑦ ☒ 無効 ☐ 有効
アカウントING : ⑧ ☐ 無効 ☒ 有効
MAC認証 : ⑨ ☐ 無効 ☒ 有効
認証VLAN : ⑩ ☒ 無効 ☐ 有効

⑧ アカウNテイング

[インターフェース](①)欄で選択した仮想APと通信する無線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トING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、アカウントINGサーバーの設定が必要です。
(P.3-84)

⑨ MAC認証

[インターフェース](①)欄で選択した仮想APと通信する無線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。

※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で使用できます。

※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、ユーザー名とパスワードは「00ab12cd34ef」(半角英数字(小文字))になります。

3 設定画面について

「仮想AP」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ 仮想AP設定(つづき)

※本書では、「無線LAN1」の画面で説明しています。

※説明のため、[アカウントिंग](8)欄、および[MAC認証](9)欄を「有効」に設定したときに表示される画面を使用しています。

※災害用仮想APを選択時、下記の設定(5～6、8～10)は表示されません。

仮想AP設定
インターフェース: ① ath0
仮想AP: ② ☒ 無効 ☐ 有効
SSID: ③ WIRELESSLAN-0
VLAN ID: ④ 0
ANY接続拒否: ⑤ ☒ 無効 ☐ 有効
接続端末制限: ⑥ 63
同一仮想AP内の端末間通信禁止: ⑦ ☒ 無効 ☐ 有効
アカウントING: ⑧ ☐ 無効 ☒ 有効
MAC認証: ⑨ ☐ 無効 ☒ 有効
認証VLAN: ⑩ ☒ 無効 ☐ 有効

⑩ 認証VLAN

[インターフェース](①)欄で選択した仮想APと通信する無線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。

※必要な応答属性については、2-24ページをご覧ください。

※[MAC認証](⑨)欄を「有効」に設定する、または[暗号化設定]項目の[ネットワーク認証]欄(P.3-76)でネットワーク認証(IEEE802.1X、WPA2、WPA/WPA2、WPA)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]項目で、RADIUSサーバーの設定をします。(P.3-75)

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

[RADIUS設定]項目で、RADIUSサーバーの設定をします。(P.3-83)

※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。

※RS-AP3やRC-AP10のMAC認証サーバー(簡易RADIUS)では、本機能は使用できません。(応答属性非対応のため)

3 設定画面について

「仮想AP」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ MAC認証サーバー(RADIUS)設定

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。

※説明のため、[仮想AP設定]項目の[MAC認証]欄(P.3-73)を「有効」に設定したときに表示される画面を使用しています。

MAC認証サーバー(RADIUS)設定	
	① プライマリー セカンダリー
アドレス: ②	
ポート: ③ 1812	1812
シークレット: ④ secret	secret

- ① 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。
- ② 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。
- ③ 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。
※で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。
- ④ 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 設定画面について

「仮想AP」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 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(①、②)に応じて、下記以外の設定(③～⑥)が表示されます。(P.3-79～P.3-81)

暗号化設定	
ネットワーク認証:	① オープンシステム/共有キー
暗号化方式:	② なし

① ネットワーク認証

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ないため、通信をする相手間で同じ設定にしてください。

※「IEEE802.1X」、「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」認証より強力な「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。

3 設定画面について

「仮想AP」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ 暗号化設定

※選択する設定内容(①、②)に応じて、下記以外の設定(③～⑥)が表示されます。(P.3-79～P.3-81)

暗号化設定	
ネットワーク認証: ①	オープンシステム/共有キー ▼
暗号化方式: ②	なし ▼

① 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。

◎WPA2-PSK

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。

② 暗号化方式 ……………

無線伝送データを暗号化する方式を選択します。(出荷時の設定: なし)
対応する暗号化方式は、[WEP RC4]/[TKIP]/[AES]です。

異なる暗号化方式とは互換性がないため、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。

※IEEE802.11ac規格、IEEE802.11n規格での通信は、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。

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](①)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](①)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。

◎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](①)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。

3 設定画面について

「仮想AP」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ 暗号化設定

※選択する設定内容(①、②)に応じて、下記以外の設定(③～⑥)が表示されます。(P.3-79～P.3-81)

暗号化設定	
ネットワーク認証: ①	オープンシステム/共有キー ▼
暗号化方式: ②	なし ▼

② 暗号化方式(つづき)

◎TKIP/AES

無線LAN端末からのアクセスに対して暗号化方式(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。

※[ネットワーク認証](①)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(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](①)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。

3 設定画面について

「仮想AP」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ 暗号化設定(つづき)

※選択する設定内容(①、②)に応じて、下記以外の設定(⑤～⑦)が表示されます。(P.3-81～P.3-82)

暗号化設定	
ネットワーク認証: ①	オープンシステム/共有キー
暗号化方式: ②	WEP RC4 64 (40)
キージェネレーター: ③	
WEPキー: ④	0000000000 半角英数字で5文字、もしくは16進数で10桁を入力

③ キージェネレーター ……………

[暗号化方式](②)欄(P.3-77)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](①)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]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](④)欄(P.3-80)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]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]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ないので、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]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]欄の設定によって異なります。

3 設定画面について

「仮想AP」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ 暗号化設定(つづき)

※選択する設定内容(①、②)に応じて、下記以外の設定(⑤～⑦)が表示されます。(P.3-81～P.3-82)

暗号化設定	
ネットワーク認証: ①	オープンシステム/共有キー
暗号化方式: ②	WEP RC4 64 (40)
キージェネレーター: ③	
WEPキー: ④	0000000000 半角英数字で5文字、もしくは16進数で10桁を入力

④ WEPキー

[キージェネレーター](③)欄を使用しないで、暗号鍵(キー)を直接設定するときに入力します。

※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](②)欄を設定したときに表示される桁数(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。

3 設定画面について

「仮想AP」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ 暗号化設定(つづき)

※選択する設定内容(①、②)に応じて、下記以外の設定(③、④、⑦)が表示されます。(P.3-79～P.3-82)

暗号化設定	
ネットワーク認証: ①	WPA-PSK/WPA2-PSK ▼
暗号化方式: ②	AES ▼
PSK (Pre-Shared Key): ⑤	00000000
WPAキー更新間隔: ⑥	120 分

⑤ PSK(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] (①) 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。

⑥ WPAキー更新間隔 ……………

[ネットワーク認証] (①) 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。

3 設定画面について

「仮想AP」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ 暗号化設定(つづき)

※選択する設定内容(①、②)に応じて、下記以外の設定(③～⑥)が表示されます。(P.3-79～P.3-81)

暗号化設定		
ネットワーク認証:	① IEEE 802.1X	▼
暗号化方式:	② WEP RC4 64 (40)	▼
再認証間隔:	⑦ 120	分

- ⑦ 再認証間隔 [ネットワーク認証](①)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。

3 設定画面について

「仮想AP」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 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」を選択したときに、下記の画面が表示されます。

※EAP認証の対応については、ご使用になるRADIUSサーバーや無線LAN端末の説明書をご覧ください。

RADIUS設定		
	プライマリー	セカンダリー
アドレス:		
ポート:	1812	1812
シークレット:	secret	secret

- ① 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[セカンダリー]列に設定したRADIUSサーバーでアクセスを試みます。
- ② 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。
- ③ 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。
設定できる範囲は、「1～65535」です。 (出荷時の設定：1812)
※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。
- ④ 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 設定画面について

「仮想AP」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 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」を選択したときに、下記の画面が表示されます。

アカウンティング設定	
① プライマリー	セカンダリー
アドレス: ②	
ポート: ③ 1813	1813
シークレット: ④ secret	secret
	⑤ 登録 ⑥ 取消

- | | |
|-----------------------|--|
| ① 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[セカンダリー]列に設定したアカウンティングサーバーでアクセスを試みます。 |
| ② 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。 |
| ③ 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。
設定できる範囲は、「1～65535」です。 (出荷時の設定: 1813)
※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。 |
| ④ シークレット | 本製品とアカウンティング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)
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。 |
| ⑤ 〈登録〉 | [仮想AP]項目で設定した内容を登録するボタンです。 |
| ⑥ 〈取消〉 | [仮想AP]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。 |

3 設定画面について

「MACアドレスフィルタリング」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 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

各仮想APに接続できる無線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。

※ご使用のWWWブラウザでJavaScriptが「無効」に設定されていると、[MACアドレスフィルタリング設定]項目でインターフェースを選択したとき、「MACアドレスフィルタリング」画面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。

- | | |
|----------------------------|---|
| ① 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(無線LAN1)
ath1(無線LAN2))
選択するインターフェースごとに、本製品への接続を許可する、または拒否する無線LAN端末を登録できます。
※無線LAN1はath0、ath01～ath07、無線LAN2はath1、ath11～ath17から選択します。
※災害用仮想AP(ath08、ath18)には設定できません。(P.3-116) |
| ② MACアドレスフィルタリング … | [インターフェース](①)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](③)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」画面で該当するインターフェースを選択し、[仮想AP]欄を「有効」に設定しておきます。 |
| ③ フィ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無線LAN端末だけが、本製品と無線通信できます。
※MACアドレスを登録していない無線LAN端末は、本製品と無線通信できません。
拒否リスト ：MACアドレスが登録された無線LAN端末だけが、本製品と無線通信できません。
※MACアドレスを登録していない無線LAN端末は、本製品と無線通信できます。 |
| ④ <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。 |
| ⑤ <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。 |

3 設定画面について

「MACアドレスフィルタリング」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 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無線LAN端末のMACアドレスを登録します。

端末MACアドレスリスト	
MACアドレス :	追加

MACアドレス

MACアドレスフィルタリングの対象となる無線LAN端末のMACアドレスを入力します。入力後、〈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]項目に表示されます。

※対象となる無線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。

3 設定画面について

「MACアドレスフィルタリング」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 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

MACアドレスフィルタリング設定一覧			
登録済みの端末 ①	受信中の端末 ②	通信状況 ③	④
		通信不許可	追加
		通信中	削除
		登録済	削除

[フィルタリングポリシー]を「拒否リスト」で使用した場合

MACアドレスフィルタリング設定一覧			
登録済みの端末 ①	受信中の端末 ②	通信状況 ③	④
		通信中	追加
		通信不許可	削除
		登録済	削除

- ① 登録済みの端末 登録されている無線LAN端末のMACアドレスが表示されます。
- ② 受信中の端末 本製品の無線伝送領域内で通信している無線LAN端末のMACアドレスが表示されます。
- ③ 通信状況 本製品との無線通信状況が表示されます。
〈通信中〉 : 本製品と無線通信中のとき、〈通信中〉とボタンで表示されます。
※〈通信中〉をクリックすると、無線通信状態(別画面)が表示されます。
「通信不許可」: MACアドレスフィルタリング設定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。
- ④ 〈追加〉/〈削除〉 表示されている無線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。

3 設定画面について

「ネットワーク監視」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 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。

※本書では、「無線LAN1」の画面で説明しています。

※存在しないホスト、またはセキュリティ設定などにより、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。

- | | |
|-------------------|---|
| ① 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：無線LAN1→ath0
無線LAN2→ath1)
※無線LAN1はath0、ath01～ath08、無線LAN2はath1、ath11～ath18から選択します。 |
| ② 監視対象ホスト1～4..... | 監視の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](③)欄に設定された間隔でPINGを送出します。
※すべてが空欄(初期値)の場合は、監視動作をしません。 |
| ③ 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。 |
| ④ 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。 |
| ⑤ 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。
設定できる範囲は、「1～10」(回)です。 (出荷時の設定：3) |

3 設定画面について

「ネットワーク監視」画面

無線LAN設定 > 無線LAN1/無線LAN2 > ネットワーク監視

■ ネットワーク監視設定(つづき)

※本書では、「無線LAN1」の画面で説明しています。

ネットワーク監視設定

インターフェース : ① ath0

監視対象ホスト1 :
監視対象ホスト2 :
監視対象ホスト3 :
監視対象ホスト4 : ②

監視間隔 : ③ 10 秒

タイムアウト時間 : ④ 1 秒

失敗回数 : ⑤ 3 回

条件 : ⑥ ひとつ以上のホストが応答なし ⑦ ⑧ ✓

登録 取消

- ⑥ 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。
- 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。

3 設定画面について

「AP間通信 (WBR)」画面

無線LAN設定 > 無線LAN1/無線LAN2 > AP間通信 (WBR)

■ AP間通信設定

無線AP間通信を使用するための設定です。

※説明のため、[AP間通信] (8) 欄を「有効」に設定したときに表示される画面を使用しています。

AP間通信設定

1 AP間通信:

☐ 無効 ☒ 有効

2 動作モード:

親機

- | | | |
|---------------|---|-------------|
| 1 AP間通信 | 無線AP間通信の使用を設定します。
「有効」に設定すると、本製品のAP間通信を使用できます。 | (出荷時の設定：無効) |
| 2 動作モード | 無線AP間通信を使用するときの動作モードを、「親機」、「子機」から選択します。
※親機側の仮想AP「ath0」(無線LAN1)、「ath1」(無線LAN2)に設定されたSSIDと暗号化を使用して、無線AP間通信をします。 | |

3 設定画面について

「AP間通信 (WBR)」画面

無線LAN設定 > 無線LAN1/無線LAN2 > AP間通信 (WBR)

■ 親機設定

親機として無線AP間通信をするための設定です。

※本書では、「無線LAN1」の画面で説明しています。

※「AP間通信設定」項目の「動作モード」で「親機」を選択したときに表示される項目です。

「子機」を選択したときに表示される項目は、3-93ページで説明しています。

親機設定

① インターフェース : wbr0

② 接続先BSSID :

③ 登録

④ 取消

- | | |
|------------------|--|
| ① インターフェース | 無線AP間通信の名称を選択します。（出荷時の設定：無線LAN1→wbr0
無線LAN2→wbr8）
※無線LAN1はwbr0～wbr7、無線LAN2はwbr8～wbr15から選択します。
※最大8台分の子機を登録できます。
※登録した内容は、[AP間通信設定一覧]項目に表示されます。
※インターフェースの名称は、変更できません。 |
| ② 接続先BSSID | 無線AP間通信する子機側(接続先)の[BSSID]を12桁(16進数)の半角英数字で入力します。 |
| ③ 〈登録〉 | [親機設定]項目で設定した内容を登録するボタンです。 |
| ④ 〈取消〉 | [親機設定]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。 |

3 設定画面について

「AP間通信 (WBR)」画面

無線LAN設定 > 無線LAN1/無線LAN2 > AP間通信 (WBR)

■ AP間通信設定一覧

[親機設定] 項目で登録した設定内容が表示されます。

※本書では、「無線LAN1」の画面で説明しています。

AP間通信設定一覧		
インターフェース	BSSID	
wbr0	無線LAN1 (親機)	削除
wbr1		
wbr2		
wbr3		
wbr4		
wbr5		
wbr6		
wbr7		

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 設定画面について

「AP間通信 (WBR)」画面

無線LAN設定 > 無線LAN1/無線LAN2 > AP間通信 (WBR)

■ 子機設定

子機として無線AP間通信をするための設定です。

※「AP間通信設定」項目の「動作モード」で「子機」を選択したときに表示される項目です。

「親機」を選択したときに表示される項目は、3-91ページで説明しています。

※選択する設定内容(④、⑤)に応じて、下記以外の設定(⑥、⑦、⑧)が表示されます。(P.3-95～P.3-96)

子機設定

BSSID : ①

インターフェース : ② wbr16

SSID : ③ WIRELESSLAN-0

ネットワーク認証 : ④ オープンシステム/共有キー

暗号化方式 : ⑤ なし

登録 取消

- ① BSSID 親機に登録する[BSSID]が表示されます。
※表示された[BSSID]を無線AP間通信する親機側の機器に登録します。
- ② インターフェース 無線AP間通信の名称が表示されます。
※インターフェースの名称は、変更できません。
(出荷時の設定：無線LAN1→wbr16
無線LAN2→wbr17)
- ③ SSID 親機側で設定されたSSIDを入力します。(出荷時の設定：WIRELESSLAN-0)
- ④ ネットワーク認証 親機側に設定された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)

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。

◎WPA2-PSK

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。

3 設定画面について

「AP間通信 (WBR)」画面

無線LAN設定 > 無線LAN1/無線LAN2 > AP間通信 (WBR)

■ 子機設定

※選択する設定内容(④、⑤)に応じて、下記以外の設定(⑥、⑦、⑧)が表示されます。(P.3-93～P.3-96)

子機設定

BSSID: ①

インターフェース: ② wbr16

SSID: ③ WIRELESSLAN-0

ネットワーク認証: ④ オープンシステム/共有キー

暗号化方式: ⑤ なし

⑨ 登録

⑩ 取消

④ 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。

⑤ 暗号化方式 ……………

親機側に設定された暗号化方式を選択します。(出荷時の設定：なし)
対応する暗号化方式は、[WEP RC4]/[TKIP]/[AES]です。

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](④)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](④)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」を選択したとき使用できます。

◎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](④)欄で、「WPA-PSK」、または「WPA2-PSK」を選択したとき使用できます。

3 設定画面について

「AP間通信 (WBR)」画面

無線LAN設定 > 無線LAN1/無線LAN2 > AP間通信 (WBR)

■ 子機設定

※選択する設定内容(④、⑤)に応じて、下記以外の設定(⑧)が表示されます。(P.3-96)

子機設定

BSSID : ①

インターフェース : ② wbr16

SSID : ③ WIRELESSLAN-0

ネットワーク認証 : ④ オープンシステム/共有キー

暗号化方式 : ⑤ WEP RC4 64 (40)

キージェネレーター : ⑥

WEPキー : ⑦ 0000000000

⑧

⑩

⑤ 暗号化方式(つづき).....

◎TKIP/AES

無線LAN端末からのアクセスに対して暗号化方式(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。

※「ネットワーク認証」(④)欄で、「WPA-PSK」、または「WPA2-PSK」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」欄で、「WPA-PSK」、または「WPA2-PSK」を選択したとき使用できます。

⑥ キージェネレーター

「暗号化方式」(⑤)欄(P.3-94)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))

※入力方法の詳細については、3-79ページをご覧ください。

⑦ WEPキー

「キージェネレーター」(⑥)欄を使用しないで、暗号鍵(キー)を直接設定するときに入力します。(出荷時の設定：0000000000)

※「0～9」、および「a～f(またはA～F)」の16進数、またはASCII文字で、半角入力してください。

3 設定画面について

「AP間通信 (WBR)」画面

無線LAN設定 > 無線LAN1/無線LAN2 > AP間通信 (WBR)

■ 子機設定(つづき)

※選択する設定内容(④、⑤)に応じて、下記以外の設定(⑥、⑦)が表示されます。(P.3-95)

子機設定

BSSID : ①

インターフェース : ② wbr16

SSID : ③ WIRELESSLAN-0

ネットワーク認証 : ④ WPA-PSK/WPA2-PSK

暗号化方式 : ⑤ AES

PSK (Pre-Shared Key) : ⑧ 00000000

⑨ 登録

⑩ 取消

- ⑧ PSK (Pre-Shared Key) 共通鍵(キー)を半角英数字で入力します。(出荷時の設定: 00000000)
※ [ネットワーク認証] (④)欄で、「WPA-PSK」、「WPA2-PSK」、「WPA-PSK/WPA2-PSK」を選択したとき、設定できます。
※ 親機側と同じ共有鍵(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。
- ⑨ <登録> [子機設定]項目で設定した内容を登録するボタンです。
- ⑩ <取消> [子機設定]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。

3 設定画面について

「WMM詳細」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 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。

※本書では、「無線LAN1」の画面で説明しています。

WMM詳細設定
周波数帯： 2.4 GHz
To Station

AC Name ①	CWin min ②	CWin max ②	AIFSN (1-15) ③	TXOP (0-255) ⑤	No Ack ⑥
AC_BK	15	1023	7	0	☐
AC_BE	15	63	3	0	☐
AC_VI	7	15	1	94	☐
AC_VO	3	7	1	47	☐

From Station

AC Name ①	CWin min ②	CWin max ②	AIFSN (2-15) ④	TXOP (0-255) ⑤	ACM ⑦
AC_BK	15	1023	7	0	
AC_BE	15	1023	3	0	
AC_VI	7	15	2	94	☐
AC_VO	3	7	2	47	☐

① AC 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(②～⑤)を設定できます。

EDCAパラメーターの各値は、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(②～⑤)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(⑦)などの制御が正しく動作しない場合があります。

3 設定画面について

「WMM詳細」画面

無線LAN設定 > 無線LAN1/無線LAN2 > WMM詳細

■ WMM詳細設定(つづき)

※本書では、「無線LAN1」の画面で説明しています。

WMM詳細設定

周波数帯 : 2.4 GHz

To Station

AC Name ①	CWin min ②	CWin max ②	AIFSN (1-15) ③	TXOP (0-255) ⑤	No Ack ⑥
AC_BK	15	1023	7	0	☐
AC_BE	15	63	3	0	☐
AC_VI	7	15	1	94	☐
AC_VO	3	7	1	47	☐

From Station

AC Name ①	CWin min ②	CWin max ②	AIFSN (2-15) ④	TXOP (0-255) ⑤	ACM ⑦
AC_BK	15	1023	7	0	
AC_BE	15	1023	3	0	
AC_VI	7	15	2	94	☐
AC_VO	3	7	2	47	☐

② CWin 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からランダムに選択することで、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))

3 設定画面について

「WMM詳細」画面

無線LAN設定 > 無線LAN1/無線LAN2 > WMM詳細

■ WMM詳細設定(つづき)

※本書では、「無線LAN1」の画面で説明しています。

WMM詳細設定

周波数帯： 2.4 GHz

To Station

AC Name ①	CWin min ②	CWin max ②	AIFSN (1-15) ③	TXOP (0-255) ⑤	No Ack ⑥
AC_BK	15	1023	7	0	☐
AC_BE	15	63	3	0	☐
AC_VI	7	15	1	94	☐
AC_VO	3	7	1	47	☐

From Station

AC Name ①	CWin min ②	CWin max ②	AIFSN (2-15) ④	TXOP (0-255) ⑤	ACM ⑦
AC_BK	15	1023	7	0	
AC_BE	15	1023	3	0	
AC_VI	7	15	2	94	☐
AC_VO	3	7	2	47	☐

- ③ AIFSN(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))

- ④ AIFSN(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))

3 設定画面について

「WMM詳細」画面

無線LAN設定 > 無線LAN1/無線LAN2 > WMM詳細

■ WMM詳細設定(つづき)

※本書では、「無線LAN1」の画面で説明しています。

WMM詳細設定

周波数帯： 2.4 GHz

To Station

AC Name ①	CWin min ②	CWin max ②	AIFSN (1-15) ③	TXOP (0-255) ⑤	No Ack ⑥
AC_BK	15	1023	7	0	☐
AC_BE	15	63	3	0	☐
AC_VI	7	15	1	94	☐
AC_VO	3	7	1	47	☐

From Station

AC Name ①	CWin min ②	CWin max ②	AIFSN (2-15) ④	TXOP (0-255) ⑤	ACM ⑦
AC_BK	15	1023	7	0	
AC_BE	15	1023	3	0	
AC_VI	7	15	2	94	☐
AC_VO	3	7	2	47	☐

⑤ TXOP(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]/[From Station]

AC_BK(0)
AC_BE(0)
AC_VI(94)
AC_VO(47))

⑥ No 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 ACM 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無線LAN端末の設定が必要です。

3 設定画面について

「WMM詳細」画面

無線LAN設定 > 無線LAN1/無線LAN2 > WMM詳細

■ WMMパワーセーブ設定

IEEE802.11e U-APSD(Unscheduled Automatic Power Save Delivery)機能対応の端末を省電力制御するときの設定です。

WMMパワーセーブ設定

WMMパワーセーブ: ① ☐ 無効 ☒ 有効

② 登録

③ 取消

- | | |
|-------------------|--|
| ① WMMパワーセーブ | WMMパワーセーブ機能を設定します。
「有効」に設定すると、WMMパワーセーブ機能が設定された無線LAN端末側で、省電力制御が必要と判断したときに動作します。
(出荷時の設定: 有効) |
| ② <登録> | [WMMパワーセーブ設定]項目で設定した内容を登録するボタンです。 |
| ③ <取消> | [WMMパワーセーブ設定]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。 |

3 設定画面について

「レート」画面

無線LAN設定 > 無線LAN1/無線LAN2 > レート

■ レート設定

本製品と接続できる無線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。

※本書では、「無線LAN1」の画面で説明しています。

レート設定	
インターフェース :	① ath0
プリセット :	② 初期値

- ① 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：無線LAN1→ath0
無線LAN2→ath1)
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。
※無線LAN1はath0、ath01～ath07、無線LAN2はath1、ath11～ath17から選択します。
※災害用仮想AP(ath08、ath18)には設定できません。(P.3-116)
- ② 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」、「IEEE 802.11b端末を拒否★」、「IEEE 802.11b無効★」、「音声端末向け」、「安定重視1」、「安定重視2」から選択します。 (出荷時の設定：初期値)
★無線LAN2(5GHz帯)では表示されない項目です。
※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「一」が表示されます。
- ◎IEEE802.11b端末を拒否★
6Mbps、12Mbps、24Mbpsのレートをベーシックレートに設定することで、IEEE802.11b規格だけで動作する端末からの接続を拒否します。
IEEE802.11b規格のレートは有効のため、IEEE802.11g規格対応の端末に対して、IEEE802.11b規格のレートで通信できます。
- ◎IEEE802.11b無効★
IEEE802.11b規格のレートを無効化することで、IEEE802.11b規格での通信を無効化します。
IEEE802.11b規格のレートを使用することによる通信品位の低下を改善したい場合に使用します。

3 設定画面について

「レート」画面

無線LAN設定 > 無線LAN1/無線LAN2 > レート

■ レート設定

※本書では、「無線LAN1」の画面で説明しています。

レート設定	
インターフェース :	① ath0
プリセット :	② 初期値

② プリセット(つづき)……………

◎音声端末向け

音声端末向けにIEEE802.11b規格のレートを無効化し、さらに中間のレートを無効化することで、通話品位悪化時のパケット再送回数を低減し、通話を安定させます。

◎安定重視1

無線アクセスポイントと無線LAN端末の通信において、速度重視ではなく、安定性を重視したい場合に使用します。

IEEE802.11ac規格、IEEE802.11n規格の高いレートを無効化することで、電波状況が悪い場合にパケット再送回数を低減し、通信を安定させます。

◎安定重視2

「安定重視1」で通信の安定性が改善しない場合に選択します。

「安定重視1」よりもさらに多くのレートを無効化して、通信を安定させます。

3 設定画面について

「レート」画面

無線LAN設定 > 無線LAN1/無線LAN2 > レート

■ プリセットされた各レート設定

初期値		IEEE802.11b端末を拒否		IEEE802.11b無効	
1Mbps	ベーシックレート (2.4GHz時)	1Mbps	有効	1Mbps	無効
	非表示 (5GHz時)	2Mbps	有効	2Mbps	無効
2Mbps	ベーシックレート (2.4GHz時)	5.5Mbps	有効	5.5Mbps	無効
	非表示 (5GHz時)	6Mbps	ベーシックレート	6Mbps	ベーシックレート
5.5Mbps	ベーシックレート (2.4GHz時)	9Mbps	有効	9Mbps	有効
	非表示 (5GHz時)	11Mbps	有効	11Mbps	無効
6Mbps	ベーシックレート (2.4GHz時)	12Mbps	ベーシックレート	12Mbps	ベーシックレート
	非表示 (5GHz時)	18Mbps	有効	18Mbps	有効
9Mbps	有効(2.4GHz時)	24Mbps	ベーシックレート	24Mbps	ベーシックレート
11Mbps	ベーシックレート(5GHz時)	36Mbps	有効	36Mbps	有効
	非表示 (5GHz時)	48Mbps	有効	48Mbps	有効
12Mbps	有効(2.4GHz時)	54Mbps	有効	54Mbps	有効
	ベーシックレート(5GHz時)	MCS0~MCS15		MCS0~MCS15	
18Mbps	有効		有効		有効
24Mbps	有効(2.4GHz時)	マルチキャストレート	1Mbps	マルチキャストレート	6Mbps
	ベーシックレート(5GHz時)				
36Mbps	有効				
48Mbps	有効				
54Mbps	有効				
MCS0~MCS15					
	有効				
VHT-MCS 1~2ストリーム					
	(IEEE802.11ac対応時のみ 表示)				
	MCS0-9				
マルチキャストレート					
	1Mbps(2.4GHz時)				
	6Mbps(5GHz時)				

3 設定画面について

「レート」画面

無線LAN設定 > 無線LAN1/無線LAN2 > レート

■ プリセットされた各レート設定(つづき)

音声端末向け		安定重視1		安定重視2	
1Mbps	無効(2.4GHz時) 非表示(5GHz時)	1Mbps	ベーシックレート (2.4GHz時)	1Mbps	ベーシックレート (2.4GHz時)
2Mbps	無効(2.4GHz時) 非表示(5GHz時)	2Mbps	ベーシックレート (2.4GHz時)	2Mbps	ベーシックレート (2.4GHz時)
5.5Mbps	無効(2.4GHz時) 非表示(5GHz時)	5.5Mbps	ベーシックレート (2.4GHz時)	5.5Mbps	ベーシックレート (2.4GHz時)
6Mbps	ベーシックレート	6Mbps	有効(2.4GHz時)	6Mbps	有効(2.4GHz時)
9Mbps	無効	9Mbps	有効	9Mbps	有効
11Mbps	無効(2.4GHz時) 非表示(5GHz時)	11Mbps	ベーシックレート (2.4GHz時)	11Mbps	ベーシックレート (2.4GHz時)
12Mbps	ベーシックレート	12Mbps	有効(2.4GHz時)	12Mbps	有効(2.4GHz時)
18Mbps	無効	18Mbps	有効	18Mbps	有効
24Mbps	ベーシックレート	24Mbps	有効(2.4GHz時)	24Mbps	有効(2.4GHz時)
36Mbps	無効	36Mbps	有効	36Mbps	有効
48Mbps	無効	48Mbps	有効	48Mbps	有効
54Mbps	有効	54Mbps	有効	54Mbps	有効
MCS0	有効	MCS0~MCS11	有効	MCS0~MCS7	有効
MCS1	無効	MCS12~MCS15	無効	MCS8~MCS15	無効
MCS2	無効	VHT-MCS 1~2ストリーム	(IEEE802.11ac対応時のみ 表示)	VHT-MCS 1~2ストリーム	(IEEE802.11ac対応時のみ 表示)
MCS3	無効	MCS0-8		MCS0-7	
MCS4	有効	マルチキャストレート		マルチキャストレート	
MCS5	無効	1Mbps(2.4GHz時)		1Mbps(2.4GHz時)	
MCS6	無効	6Mbps(5GHz時)		6Mbps(5GHz時)	
MCS7	有効				
MCS8	有効				
MCS9	無効				
MCS10	無効				
MCS11	無効				
MCS12	有効				
MCS13	無効				
MCS14	無効				
MCS15	有効				
VHT-MCS 1~2ストリーム	(IEEE802.11ac対応時のみ 表示)				
MCS0-9					
マルチキャストレート					
6Mbps					

3 設定画面について

「レート」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 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は、「レート」画面で各仮想AP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、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
： 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、通信レートなどを対応付けしたMCS値ごとに設定します。(P.3-107)

- 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
： 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

無線LAN2 (5GHz) の場合、「レート」画面に [VHT-MCS] 欄も表示されますので、ストリーム数ごとに、対応するMCS値を設定します。(P.3-107)

レート設定

インターフェース: ath1
プリセット: 初期値

仮想APごとに通信レートを設定できます。

レガシー:

6 Mbps:	☐ 無効	☐ 有効	☒ ベーシックレート
9 Mbps:	☐ 無効	☒ 有効	☐ ベーシックレート
12 Mbps:	☐ 無効	☐ 有効	☒ ベーシックレート
18 Mbps:	☐ 無効	☒ 有効	☐ ベーシックレート
24 Mbps:	☐ 無効	☐ 有効	☒ ベーシックレート
36 Mbps:	☐ 無効	☒ 有効	☐ ベーシックレート
48 Mbps:	☐ 無効	☒ 有効	☐ ベーシックレート
54 Mbps:	☐ 無効	☒ 有効	☐ ベーシックレート

HT-MCS:

MCS 0:	☐ 無効	☒ 有効	☐ ベーシックレート
MCS 1:	☐ 無効	☒ 有効	☐ ベーシックレート
MCS 2:	☐ 無効	☒ 有効	☐ ベーシックレート
MCS 3:	☐ 無効	☒ 有効	☐ ベーシックレート
MCS 4:	☐ 無効	☒ 有効	☐ ベーシックレート
MCS 5:	☐ 無効	☒ 有効	☐ ベーシックレート
MCS 6:	☐ 無効	☒ 有効	☐ ベーシックレート
MCS 7:	☐ 無効	☒ 有効	☐ ベーシックレート
MCS 8:	☐ 無効	☒ 有効	☐ ベーシックレート
MCS 9:	☐ 無効	☒ 有効	☐ ベーシックレート
MCS 10:	☐ 無効	☒ 有効	☐ ベーシックレート
MCS 11:	☐ 無効	☒ 有効	☐ ベーシックレート
MCS 12:	☐ 無効	☒ 有効	☐ ベーシックレート
MCS 13:	☐ 無効	☒ 有効	☐ ベーシックレート
MCS 14:	☐ 無効	☒ 有効	☐ ベーシックレート
MCS 15:	☐ 無効	☒ 有効	☐ ベーシックレート

VHT-MCS:

1 ストリーム:	☐ MCS 0-7	☐ MCS 0-8	☒ MCS 0-9
2 ストリーム:	☐ MCS 0-7	☐ MCS 0-8	☒ MCS 0-9

マルチキャスト送信レート:

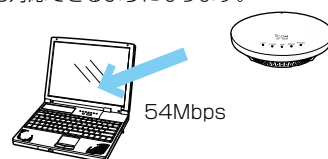
マルチキャストレート: 6 Mbps

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。



3 設定画面について

「レート」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 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[HT-MCS]欄を設定してください。

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

VHT-MCS	ストリーム数	通信レート (Mbps)					
		帯域幅 20MHz(VHT20)		帯域幅 40MHz(VHT40)		帯域幅 80MHz(VHT80)	
		800ns GI	400ns GI	800ns GI	400ns GI	800ns GI	400ns GI
0	1	6.5	7.2	13.5	15	29.3	32.5
1		13	14.4	27	30	58.5	65
2		19.5	21.7	40.5	45	87.8	97.5
3		26	28.9	54	60	117	130
4		39	43.3	81	90	175.5	195
5		52	57.8	108	120	234	260
6		58.5	65	121.5	135	263.3	292.5
7		65	72.2	135	150	292.5	325
8		78	86.7	162	180	351	390
9		—	—	180	200	390	433.3
0	2	13	14.4	27	30	58.5	65
1		26	28.9	54	60	117	130
2		39	43.3	81	90	175.5	195
3		52	57.8	108	120	234	260
4		78	86.7	162	180	351	390
5		104	115.6	216	240	468	520
6		117	130	243	270	526.5	585
7		130	144.4	270	300	585	650
8		156	173.3	324	360	702	780
9		—	—	360	400	780	866.7

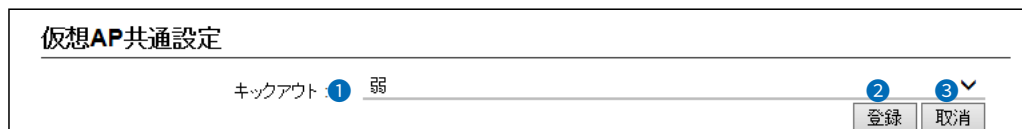
3 設定画面について

「レート」画面

無線LAN設定 > 無線LAN1/無線LAN2 > レート

■ 仮想AP共通設定

無線LANユニットごとに、本製品と通信する無線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。



- | | |
|----------------|---|
| ① 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。 |
| ② 〈登録〉 | 「レート」画面で設定した内容を登録するボタンです。 |
| ③ 〈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。 |

3 設定画面について

「ARP代理応答」画面

無線LAN設定 > 無線LAN1/無線LAN2 > ARP代理応答

■ ARP代理応答設定

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、無線LAN端末の省電力制御をする機能の設定です。
※本書では、「無線LAN1」の画面で説明しています。

- ① 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：無線LAN1→ath0、無線LAN2→ath1)
※無線LAN1はath0、ath01～ath07、無線LAN2はath1、ath11～ath17から選択します。
※災害用仮想AP(ath08、ath18)には設定できません。(P.3-116)
- ② ARP代理応答 [インターフェース](①)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)
- ③ 不明なARPの透過 [インターフェース](①)欄で選択した仮想APと通信している無線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、本製品に接続している無線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、本製品が代理応答します。
一致しない場合、[不明なARPの透過]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、本製品が代理応答します。
一致しない場合、[不明なARPの透過]欄の設定に関係なく、ARPリクエストを透過します。

3 設定画面について

「ARP代理応答」画面

無線LAN設定 > 無線LAN1/無線LAN2 > ARP代理応答

■ ARP代理応答設定(つづき)

※本書では、「無線LAN1」の画面で説明しています。

- ④ **ARP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。
※接続した無線LAN端末がDHCPクライアントであった場合、DHCPによるリース期間が優先されます。
※「0」(出荷時の設定)のときは、削除されません。
※無線LAN端末が本製品から離脱した場合は、時間設定に関係なく、ARP情報が削除されます。
- ⑤ **〈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。
- ⑥ **〈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。

3 設定画面について

「ARP代理応答」画面

無線LAN設定 > 無線LAN1/無線LAN2 > 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。

ARPキャッシュ情報		
MACアドレス	IPアドレス	
XXXXXXXXXX	XXXXXXXXXX	1 削除
		2 一括削除

- ① 〈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。
- ② 〈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。

3 設定画面について

IP Advanced Radio Systemについて

無線設定 > 無線1/無線2 > IP Advanced Radio System

本製品を弊社製コントローラーの近隣呼出機能(特定のエリアに限定して運用する機能)と連動させて利用するときに設定します。

[通知] 欄を「有効」に設定して名前を登録しておく、コントローラー側の「近隣呼出接続」画面で、無線アクセスポイントを自動検索することで、BSSIDと名前の検索や登録ができます。

※[インターフェース]欄で設定する仮想APを選択して、各テナントを設定します。

※無線LAN1はath0、ath01～ath07、無線LAN2はath1、ath11～ath17から選択します。

※災害用仮想AP(ath08、ath18)には設定できません。(P.3-116)

※名前(例: 1Fフロア)を設定するときは、任意の31文字以内で入力します。

※本書では、「無線LAN1」の画面で説明しています。

近隣呼出設定		
インターフェース: ath0 ▼		
BSSID: 00-90-C7-XXXX-XXXX		
テナント番号	通知	名前
1	☐ 無効 ☒ 有効	
2	☐ 無効 ☒ 有効	
3	☐ 無効 ☒ 有効	
4	☐ 無効 ☒ 有効	
5	☐ 無効 ☒ 有効	
6	☐ 無効 ☒ 有効	
7	☐ 無効 ☒ 有効	
8	☐ 無効 ☒ 有効	
9	☐ 無効 ☒ 有効	
10	☐ 無効 ☒ 有効	

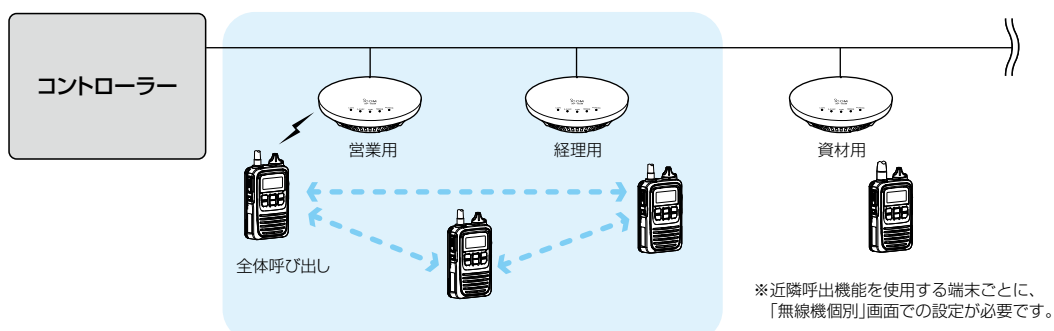
登録 取消

近隣呼出機能について

特定のエリア(例: 1Fフロア)に限定して、WLAN無線機を運用するときに使用する機能です。

※コントローラー側で、近隣呼出機能を使用するエリア内にある無線アクセスポイント(例: 営業用と経理用)の登録が必要です。

【近隣呼出機能で全体呼び出しをした場合】



3 設定画面について

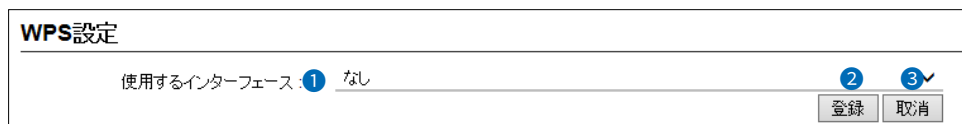
「WPS」画面

無線LAN設定 > WPS

■ WPS設定

WPS(Wi-Fi Protected Setup)機能の使用についての設定です。

※WPSとは、無線LANのSSIDと暗号化方式の設定を容易にするために、「Wi-Fiアライアンス」が提唱する機能です。



- | | |
|-------------------|---|
| ① 使用するインターフェース …… | WPS機能を使用する仮想APを選択します。 (出荷時の設定：なし)
※無線LAN1はath0、ath01～ath07、無線LAN2はath1、ath11～ath17から選択します。
※災害用仮想AP(ath08、ath18)には設定できません。(P.3-116)
※相手の無線LAN端末は、WPS機能対応の製品が必要です。
※ANY接続拒否(P.3-71)との併用は、できません。
※使用できるネットワーク認証は、「WPA-PSK」、「WPA2-PSK」です。
※使用できる暗号化方式は、「TKIP/AES」だけです。 |
| ② 〈登録〉 …… | [使用するインターフェース]項目で設定した内容を登録するボタンです。 |
| ③ 〈取消〉 …… | [使用するインターフェース]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。 |

3 設定画面について

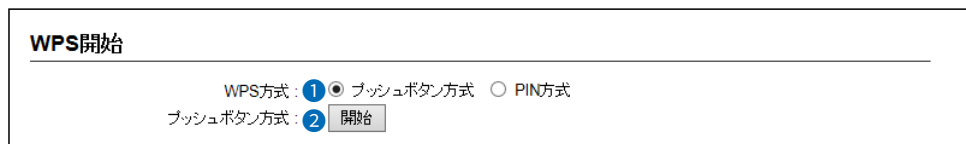
「WPS」画面

無線LAN設定 > WPS

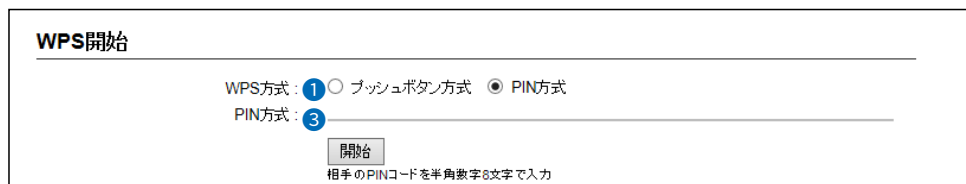
■ WPS開始

[SSID]と[暗号化方式]の自動設定を開始するための操作画面です。

プッシュボタン方式を選択した場合



PIN方式を選択した場合



① WPS方式

自動設定の方式を選択します。 (出荷時の設定：プッシュボタン方式)

◎プッシュボタン方式

本製品に設定した[SSID]と暗号化の設定を、無線LAN端末(WPS対応)のワンボタン操作で自動設定する方式です。

◎PIN方式

本製品に設定した[SSID]と暗号化の設定を、設定したPINコードの無線LAN端末(WPS対応)に自動設定する方式です。

② プッシュボタン方式

プッシュボタン方式で自動設定を開始するためのボタンです。

自動設定を開始するときは、表示された〈開始〉をクリックします。

※ボタンは、[WPS設定]項目の[使用するインターフェース]欄からインターフェース名を選択後、〈登録〉をクリックして処理が完了するまで表示されません。

※自動設定を開始すると、[MODE]ランプが~~点滅~~緑点滅します。

[2.4GHz]ランプ、または[5GHz]ランプが●緑点灯になると、設定完了です。

③ PIN方式

PIN方式で自動設定を開始するための[PINコード入力]欄とボタンです。

※PINコードが不明な場合は、ご使用になる無線LAN端末に付属する取扱説明書でご確認ください。

※自動設定を開始すると、[MODE]ランプが~~点滅~~緑点滅します。

[2.4GHz]ランプ、または[5GHz]ランプが●緑点灯になると、設定完了です。

3 設定画面について

「WPS」画面

無線LAN設定 > WPS

■ WPS状態表示

WPS機能で自動設定する内容の確認に使用します。

WPS状態表示

WPS状態表示:	設定済
SSID:	ICOM
ネットワーク認証:	WPA-PSK/WPA2-PSK
暗号化方式:	AES
PSK:	wirelessmaster

3 設定画面について

「災害用仮想AP」画面

無線LAN設定 > 災害用仮想AP

■ 災害用仮想AP

災害モード(災害用統一SSID★)「00000JAPAN」の設定です。

★大規模災害発生時に公衆無線LANの無料開放の目的で事業者等が共通で使用するSSIDです。

事業者共通で使用するSSID(00000JAPAN)のため、ユーザー認証や暗号化は設定できない仕様となっています。

※本製品は、無線LAN ビジネス推進連絡会「大規模災害時における公衆無線LANの無料開放に関するガイドライン」に準拠しています。

<http://www.wlan-business.org/customer/introduction/feature>

災害用仮想AP	
00000JAPAN 仮想AP : ① ☒ 無効 ☐ 有効	② 登録 ③ 取消

- ① 00000JAPAN仮想AP 災害モードを設定します。 (出荷時の設定：無効)
「有効」に設定すると、SSIDが「00000JAPAN」の設定された仮想APが、無線LAN1 (ath08)と無線LAN2 (ath18)に追加されます。
※ath08と ath18で使用できるのは、下記の機能です。
 ◎パケットフィルター ◎VLAN ID
 ◎同一仮想AP内の端末間通信禁止 ◎ネットワーク監視
- ② 〈登録〉 [災害用仮想AP]項目で設定した内容を登録するボタンです。
- ③ 〈取消〉 [災害用仮想AP]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。

3 設定画面について

「管理者」画面

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。

管理者パスワードの変更

管理者ID ① admin

現在のパスワード ②

新しいパスワード ③

新しいパスワード再入力 ④

登録

取消

- ① 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。
- ② 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。
- ③ 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、次のアクセスから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。
- ④ 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。

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されることをおすすめします。

ご注意

管理者パスワードを忘れた場合、設定画面にアクセスするには、工場出荷時(初期値)の状態に戻す必要があります。
※初期化するときは、4-4ページにしたがって、本製品の〈MODE〉ボタンを操作してください。

3 設定画面について

「管理ツール」画面

管理 > 管理ツール

■ 無線アクセスポイント管理ツール設定

本製品をRS-AP3やRC-AP10(別売品)で集中管理できるようにするための設定です。

※説明のため、[RS-AP3] (①)欄を「有効」に設定したときに表示される画面を使用しています。

無線アクセスポイント管理ツール設定	
RS-AP3 : ①	☐ 無効 ☒ 有効
RS-AP3接続ポートの開放 : ②	☒ 無効 ☐ 有効

- ① RS-AP3 RS-AP3(アクセスポイント集中管理ツール)やRC-AP10(無線LANコントローラー)から本製品を集中管理できるようにするとき設定します。
(出荷時の設定：無効)
※本製品が集中管理されているあいだは、本製品の設定画面から設定を変更できません。
- ② RS-AP3接続ポートの開放 本製品のルーター機能を使用しているときに、RS-AP3やRC-AP10から本製品のWAN側へアクセスできるようにするための設定です。
(出荷時の設定：無効)
「有効」に設定した場合は、RS-AP3やRC-AP10がWAN側からアクセスできるようにIPフィルターが自動的に追加されます。
※「無効」に設定した状態でRS-AP3やRC-AP10から本製品のWAN側へアクセスできるようにするときは、適切なIPフィルターの設定が必要になります。

3 設定画面について

「管理ツール」画面

管理 > 管理ツール

■ HTTP/HTTPS設定

HTTPとHTTPSは、WWWブラウザ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。

HTTP/HTTPS設定	
HTTP :	☒ ① 無効 ☒ 有効
HTTPポート番号 :	② 80
HTTPS :	☒ ③ 無効 ☐ 有効
HTTPSポート番号 :	④ 443

- | | |
|--------------------|--|
| ① HTTP | 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) |
| ② HTTP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。
設定できる範囲は、「80」と「1024～65535」です。(出荷時の設定：80)
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。 |
| ③ HTTPS | 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。 |
| ④ HTTPS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。 |

3 設定画面について

「管理ツール」画面

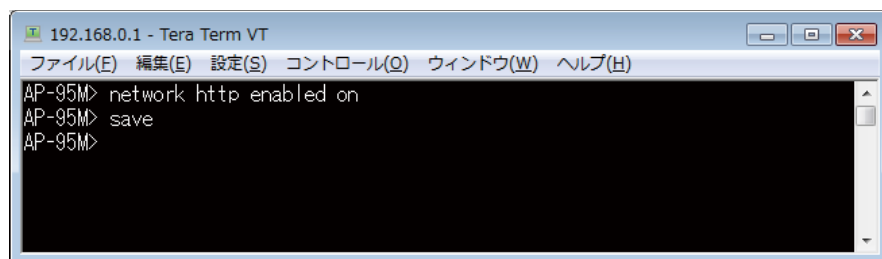
管理 > 管理ツール

■ 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やSSH(P.5-5)で本製品(例：192.168.0.1)にアクセスして、AP-95M>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。

※出荷時、「Telnet/SSH設定」項目の[Telnet]欄が「無効」に設定されているため、Telnetクライアントから本製品にアクセスできません。(P.3-121)

- ① AP-95M> **network http enabled on** と入力し[Enter]キーを押します。
- ② AP-95M> **save** と入力し[Enter]キーを押す。
- ③ プロンプト応答後、本製品の設定画面へのアクセスを確認します。



3 設定画面について

「管理ツール」画面

管理 > 管理ツール

■ Telnet/SSH設定

TelnetクライアントやSSHクライアントからのアクセスについて設定します。

- ① Telnet 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：無効)
- ② Telnet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。
- ③ SSH 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：有効)
※SSHを使用すると、SSH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。
※本製品が対応しているのは、SSHプロトコルのバージョン2だけです。
※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。
- ④ SSH認証方式 [SSH] (③)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。
- ⑤ 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。

3 設定画面について

「管理ツール」画面

管理 > 管理ツール

■ Telnet/SSH設定(つづき)

Telnet/SSH設定

Telnet : ① ☒ 無効 ☐ 有効

Telnetポート番号 : ② 23

SSH : ③ ☐ 無効 ☒ 有効

SSH認証方式 : ④ 自動 ▼

SSHポート番号 : ⑤ 22

SSH公開鍵 : ⑥

⑦ 登録 ⑧ 取消

- ⑥ SSH公開鍵 [SSH] (③)欄を「有効」、[SSH認証方式] (④)欄を「自動」/「公開鍵認証」に設定したとき、SSHでアクセスするときに使用する公開鍵を設定します。
設定するSSH公開鍵ファイルをテキストエディターなどで開き、その全文を本欄にペーストしてください。
- ⑦ 〈登録〉 「管理ツール」画面で設定した内容を登録するボタンです。
- ⑧ 〈取消〉 「管理ツール」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。

3 設定画面について

「時計」画面

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。

時刻設定

本体の現在時刻 : ① 2019年 月 日 11:05

設定する時刻 : ② 2019 年 月 日 09 時 25 分 ③ 設定

- | | |
|-----------------|--|
| ① 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。 |
| ② 設定する時刻 | 本製品の設定画面にアクセスしたときの時刻を表示します。
※お使いのWWWブラウザ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。 |
| ③ 〈設定〉 | [設定する時刻] (②) 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 設定画面について

「時計」画面

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。

自動時計設定	
自動時計設定 :	① ☒ 無効 ☐ 有効
NTPサーバー1 :	② 210.173.160.27
NTPサーバー2 :	③ 210.173.160.57
NTPステータス :	④ 同期していません

- ① 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。
- ② NTP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] (③) 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 <https://www.jst.mfeed.ad.jp/> のものです。
- ③ NTP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)
- ④ NTPステータス NTPサーバーとの同期の状態を表示します。
NTPサーバーと同期しているときは、「同期しました」が表示されます。

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、定期的に内部時計を自動設定します。

ご注意

自動時計設定機能は、インターネットに接続する、または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→「IPアドレス」画面→「IPアドレス」項目にある[デフォルトゲートウェイ]欄、または「スタティックルーティング」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 設定画面について

「時計」画面

管理 > 時計

■ SNTPサーバー設定

SNTPサーバー設定

SNTPサーバー機能: ① ☐ 無効 ☒ 有効
外部NTPサーバーへの経路が確保できない弊社RoIP機器用です。

② 登録

③ 取消

- ① SNTPサーバー機能 本製品を弊社製RoIP機器用のNTPサーバーとして使用するときの設定です。
(出荷時の設定：有効)
「有効」に設定すると、NTPサーバーとして動作する本製品に弊社製RoIP機器が日時の問い合わせをして、内部時計を自動設定します。
※この機能は、外部のNTPサーバーへの問い合わせ先(経路)が設定できない弊社製RoIP機器専用です。
※外部のNTPサーバーへの問い合わせ先(経路)が設定できない弊社製RoIP機器を本製品と併用している場合に、この機能を使用されることをおすすめします。
※この機能を使用するには、あらかじめ「時計」画面で、本製品本体の時計を設定してください。
- ② 〈登録〉 「時計」画面で設定した内容を登録するボタンです。
- ③ 〈取消〉 「時計」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。

3 設定画面について

「SYSLOG」画面

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。

SYSLOG設定

DEBUG: ① ☒ 無効 ☐ 有効

INFO: ② ☐ 無効 ☒ 有効

NOTICE: ③ ☐ 無効 ☒ 有効

ホストアドレス: ④ _____

⑤ 登録 ⑥ 取消

- | | |
|-----------------|--|
| ① DEBUG | 各種デバッグ情報を指定したホスト(④)に出力する設定です。
(出荷時の設定：無効) |
| ② INFO | INFOタイプのメッセージを指定したホスト(④)に出力する設定です。
(出荷時の設定：有効) |
| ③ NOTICE | NOTICEタイプのメッセージを指定したホスト(④)に出力する設定です。
(出荷時の設定：有効) |
| ④ ホストアドレス | SYSLOG機能を使用する場合、SYSLOGを受けるホストのアドレスを入力します。
※ホストは、SYSLOGサーバー機能に対応している必要があります。 |
| ⑤ 〈登録〉 | [SYSLOG設定]項目で設定した内容を登録するボタンです。 |
| ⑥ 〈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。 |

3 設定画面について

「SNMP」画面

管理 > SNMP

■ SNMP設定

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。

SNMP設定

SNMP: ① ☐ 無効 ☒ 有効

コミュニティID (GET): ② public

場所: ③

連絡先: ④

- | | |
|-----------------------|--|
| ① SNMP | 本製品のSNMP機能を設定します。
「有効」に設定すると、本製品の各種情報をSNMP管理ツール側で管理できま
す。
(出荷時の設定：有効) |
| ② コミュニティID(GET) | 本製品の設定情報をSNMP管理ツール側から読み出すことを許可するIDを、
半角31文字以内の英数字で入力します。
(出荷時の設定：public) |
| ③ 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。 |
| ④ 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。 |

3 設定画面について

「SNMP」画面

管理 > SNMP

■ SNMPv3設定

認証パスワードと暗号化パスワードを組み合わせ、セキュアな通信をするときの設定です。

SNMPv3設定

ユーザー名: ① _____
認証パスワード: ② _____
暗号パスワード: ③ _____

登録 取消
④ ⑤

- | | |
|-----------------|--|
| ① ユーザー名 | 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ユーザー名を、半角英数字31文字以内で入力します。 |
| ② 認証パスワード | 認証パスワードを、半角英数字8文字以上、63文字以内で入力します。 |
| ③ 暗号パスワード | 暗号パスワードを、半角英数字8文字以上、63文字以内で入力します。 |
| ④ 〈登録〉 | [SNMP]画面で設定した内容を登録するボタンです。 |
| ⑤ 〈取消〉 | [SNMP]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。 |

3 設定画面について

「LED」画面

管理 > LED

■ LED消灯モード

本製品を使用中、LEDランプを点灯させないようにする機能です。

LED消灯モード

LED消灯モード: ① ● 無効 ○ 有効 (完全消灯)

LED消灯モードに入るまでの時間: ② 30 秒

登録 取消

③ ④

- ① LED消灯モード 本製品のLED消灯モードを設定します。 (出荷時の設定：無効)
- 無効 : LED消灯モードを使用しないとき
- 有効(完全消灯) : LED消灯モードを使用して、すべてのランプを消灯するとき
- 本製品の起動後に、[LED消灯モードに入るまでの時間] (②) 欄に設定した時間(出荷時の設定：30秒)が経過すると、本製品の使用中でも、すべてのランプが消灯状態になります。
- ※〈MODE〉ボタンを操作したときは、[LED消灯モード] (①) 欄の設定に関係なく、点灯、または点滅します。
- ② LED消灯モードに入るまでの時間 [LED消灯モード] (①) 欄を「有効(完全消灯)」に設定したとき、LED消灯モードになるまでの時間を設定します。 (出荷時の設定：30秒)
- 設定できる範囲は、「0 ～ 3600」(秒)です。
- ③ 〈登録〉 [LED消灯モード] 項目で設定した内容を登録するボタンです。
- ④ 〈取消〉 [LED消灯モード] 項目の設定内容を変更したとき、変更前の状態に戻るボタンです。
- 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。

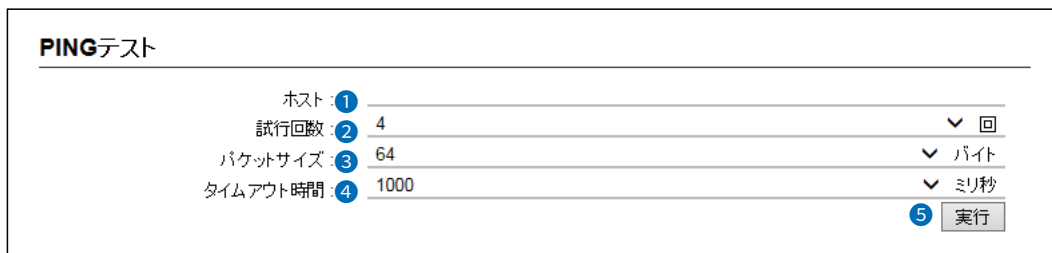
3 設定画面について

「ネットワークテスト」画面

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。



PINGテスト

ホスト: ① _____

試行回数: ② 4 [▼] [回]

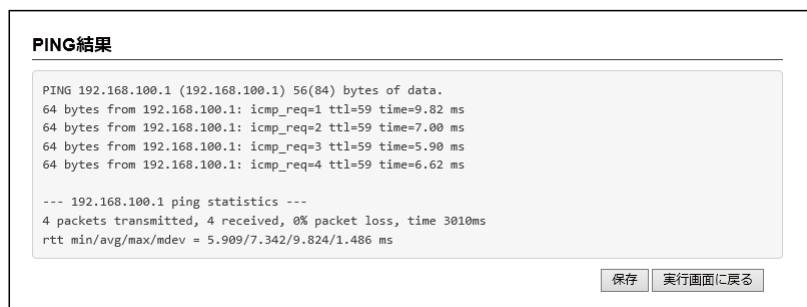
パケットサイズ: ③ 64 [▼] [バイト]

タイムアウト時間: ④ 1000 [▼] [ミリ秒]

⑤ [実行]

- ① **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。
- ② **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)
- ③ **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。
- ④ **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。
- ⑤ **〈実行〉** PINGテストを実行するボタンです。
クリックすると、「PING結果」表示に切り替わり、テスト結果が表示されます。

PING結果について



PING結果

```
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.  
64 bytes from 192.168.100.1: icmp_req=1 ttl=59 time=9.82 ms  
64 bytes from 192.168.100.1: icmp_req=2 ttl=59 time=7.00 ms  
64 bytes from 192.168.100.1: icmp_req=3 ttl=59 time=5.90 ms  
64 bytes from 192.168.100.1: icmp_req=4 ttl=59 time=6.62 ms  
  
--- 192.168.100.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3010ms  
rtt min/avg/max/mdev = 5.909/7.342/9.824/1.486 ms
```

[保存] [実行画面に戻る]

※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。

3 設定画面について

「ネットワークテスト」画面

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(traceroute)をします。

経路テスト

ノード: ①

最大ホップ数: ② 16

タイムアウト時間: ③ 3

DNS名前解決: ④ ☐ 無効 ☒ 有効

⑤ 実行

- ① ノード 経路テストをする対象ノード(機器)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。
- ② 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)
- ③ 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。
- ④ DNS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。
- ⑤ <実行> 経路テストを実行するボタンです。
クリックすると、「経路テスト結果」表示に切り替わり、テスト結果が表示されます。

経路テスト結果について

経路テスト結果

```
traceroute to 192.168.100.1 (192.168.100.1), 16 hops max, 38 byte packets
 1  1.885 ms  2.101 ms  2.248 ms
 2  20.590 ms  32.736 ms  5.745 ms
 3  192.168.54.1  17.774 ms  4.630 ms  4.497 ms
 4  192.168.53.4  5.841 ms  4.537 ms  7.152 ms
 5  192.168.100.3  10.446 ms  8.165 ms  8.240 ms
 6  192.168.100.1  10.473 ms  8.243 ms  8.037 ms
```

保存

実行画面に戻る

※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、「traceroute_[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。

3 設定画面について

「再起動」画面

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。

再起動

再起動:

3 設定画面について

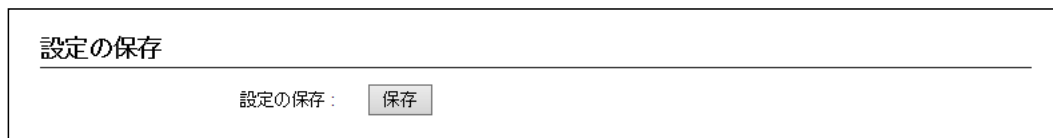
「設定の保存/復元」画面

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。

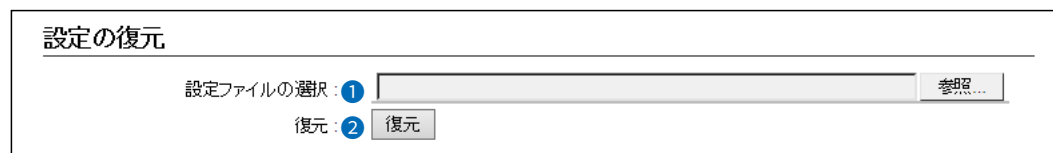
保存したファイルは、[設定の復元]項目の操作で、本製品に書き込みできます。

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。



① 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。

② 復元

[設定ファイルの選択] (①) 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。

3 設定画面について

「設定の保存/復元」画面

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。

設定内容一覧

```
wireless auto_channel "wlan0" on
wireless freq "wlan0" 0
wireless wbr enabled "wlan0" on
wireless wbr enabled "wlan1" on
wireless wbr opmode "wlan0" master
wireless wbr opmode "wlan1" master
```

3 設定画面について

「初期化」画面

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、4-4ページをご覧ください。

初期化	
全設定初期化:	☐ ① すべての設定を出荷時の設定に戻します。
無線LAN設定初期化:	☐ ② 無線LAN設定を出荷時の設定に戻します。
③ 実行	

- | | |
|--------------------|--|
| 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。
※初期化実行後、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LAN設定初期化 | 「無線LAN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。 |

3 設定画面について

「ファームウェアの更新」画面

ファームウェアの更新についてのご注意

- ◎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。
 - ◎更新中(約10分間)は、すべての接続が切断されます。
 - インターネットご利用中に更新が実行される場合がありますのでご注意ください。
 - ◎ネットワークやサーバーの状態によっては、更新に失敗することがあります。
- ※更新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。

ファームウェア情報

バージョン: AP-95M Ver. Copyright Icom Inc.

3 設定画面について

「ファームウェアの更新」画面

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更新します。

※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が必要です。

オンライン更新

ファームウェアの確認:

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。

ファームウェアオンライン更新

ファームウェア情報

状況	情報取得成功
バージョン	
更新内容	

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。
- ◎「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「IPアドレス」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

ファームウェアの更新についてのご注意

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。

※更新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。

3 設定画面について

「ファームウェアの更新」画面

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。

自動更新

自動更新 : ☒ ① 無効 ☐ 有効

② 登録

③ 取消

- ① 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)
自動更新機能有効時の通知機能について
[MODE]ランプが● 橙点灯した場合は、ご都合のよいときにファームウェアの更新をしてください。(P.4-6)
※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。
※更新内容によっては、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が自動更新されることがあります。
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。
- ② 〈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。
- ③ 〈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。

3 設定画面について

「ファームウェアの更新」画面

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更新します。

手動更新

ファームウェアの選択 : ①

参照...

ファームウェアの更新 : ②

更新

- ① **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。
- ② **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。

ファームウェアの更新についてのご注意

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。

※更新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。

この章では、

本製品の設定内容の保存、ファームウェアを更新する手順について説明しています。

1. 設定内容の確認または保存	4-2
2. 保存された設定の書き込み(復元)	4-3
3. 設定を出荷時の状態に戻すには	4-4
■ 〈MODE〉ボタンを使用する	4-4
■ 設定画面を使用する	4-5
4. ファームウェアを更新する	4-6
■ ファームウェアについて	4-6
■ ファームウェアの更新についてのご注意	4-6
A) ファイルを指定して更新する	4-7
B) オンライン更新	4-8

4 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。

設定の保存

設定の保存:

設定の復元

設定ファイルの選択:

復元:

設定内容一覧

```
wireless auto_channel "wlan0" on
wireless freq "wlan0" 0
wireless wbr enabled "wlan0" on
wireless wbr enabled "wlan1" on
wireless wbr opmode "wlan0" master
wireless wbr opmode "wlan1" master
```

出荷時や全設定初期化後は、何も表示されません。
※設定が変更された項目のみ表示します。

- 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。

192.168.0.1 から AP-95M .sav を開くか、または保存しますか?

ファイルを開く(O)

保存(S)
名前を付けて保存(A)
保存して開く(Q)

製品名、バージョン情報、保存日がファイル名として表示されます。

- 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。

4 保守について

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.4-2)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。

設定の保存

設定の保存:

設定の復元

設定ファイルの選択:

復元:

クリック

- 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。」が表示されます。
※設定を復元するために本製品が再起動します。

設定の復元

設定ファイルの選択: C:\Desktop\AP-95Mv sav

復元:

指定した設定ファイル(拡張子: sav)を表示します。

①クリック

Web ページからのメッセージ

復元には数分かかる場合があります。処理を続けてもよろしいですか?

OK

②クリック

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。

4 保守について

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、既存の設定データをすべて消去して、設定をはじめからやりなおすときは、本製品の設定内容を出荷時の状態に戻せます。

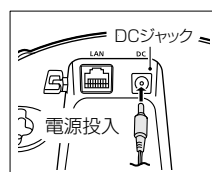
そのときの状況に応じて、次の2とおりの方法があります。

■ 〈MODE〉ボタンを使用する

- 1** 本製品からすべての機器を取りはずして、電源を入れる

[POWER] ランプの点灯を確認してから、手順2の操作を開始してください。

※ご使用の環境により、[POWER] ランプ以外の状態は異なります。



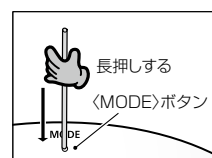
ランプ表示

5GHz	2.4GHz	LAN	MODE	POWER
○	○	○	○	●

点灯(緑)

- 2** すべてのランプが ● 緑点灯するまで、〈MODE〉ボタンを押す

※〈MODE〉ボタンを押すと、[MODE] ランプが点灯します。
そのまま押しつづけると、すべてのランプが点灯します。



5GHz	2.4GHz	LAN	MODE	POWER
○	○	○	●	●

点灯(緑) 点灯(緑)

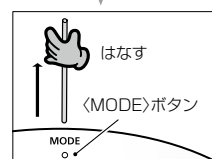
↓

5GHz	2.4GHz	LAN	MODE	POWER
●	●	●	●	●

全点灯(緑)

- 3** すべてのランプが ● 緑点灯したことを確認して、〈MODE〉ボタンから手をはなす

※[POWER] ランプが ● 緑点灯すると、初期化完了です。



5GHz	2.4GHz	LAN	MODE	POWER
○	○	○	○	●

点滅(緑)

↓

5GHz	2.4GHz	LAN	MODE	POWER
○	○	○	○	●

点灯(緑)

ご注意

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。

4 保守について

3. 設定を出荷時の状態に戻すには

管理 > 初期化

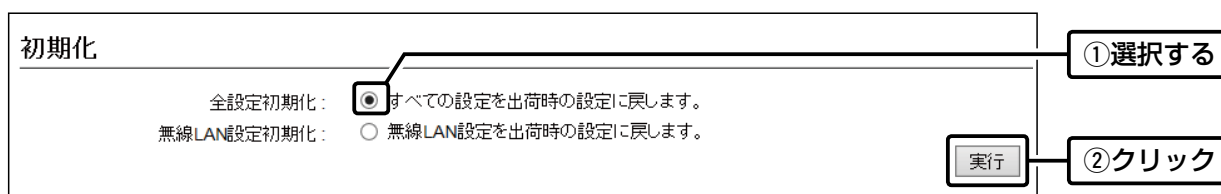
本製品に設定されたIPアドレスと管理者パスワードがわかっていて、そのIPアドレスで設定画面にアクセスできるときは、本製品の設定画面から、すべての設定を出荷時の状態に戻せます。

IPアドレスと管理者パスワードが不明な場合などの初期化については、4-4ページをご覧ください。

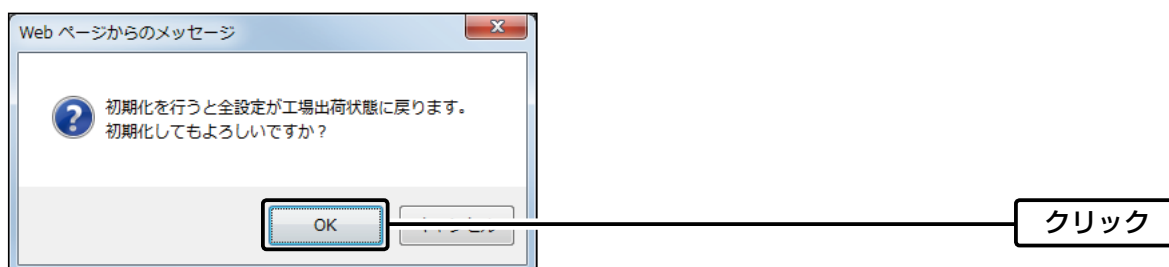
■ 設定画面を使用する

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

- 2 初期化したい条件(例:全設定初期化)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、「設定画面に戻る」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。

初期化の条件について

◎全設定初期化をクリックした場合

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。

◎無線設定初期化をクリックした場合

「無線LAN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。

初期化実行後、パソコンに設定された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LAN設定」メニューの設定を変更してください。

4 保守について

4. ファームウェアを更新する

本製品の設定画面からファームウェアを更新できます。

A ファイルを指定して更新する

オンライン更新できない環境では、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、手動で更新できます。

B オンライン更新(P.4-8)

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、バージョンアップすることがあります。

更新を実行する前に、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。ファームウェアを更新すると、機能の追加など、本製品を最良の状態にできます。

システム情報	
本体名称	
バージョン	
国名コード	JP
現在時刻	20 年 月 日 6:04:18
稼働時間	0 day 06:05:03
メモリー使用量	144200 kB / 236180 kB (61% 使用中)

バージョン情報

■ ファームウェアの更新についてのご注意

◎ ファームウェアの更新が完了するまで、約10分かかります。

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、更新できないことがあります。

更新できない場合は、ファイアウォール機能を無効にしてください。

◆ ファームウェアの更新結果については、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 <https://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 保守について

4. ファームウェアを更新する

管理 > ファームウェアの更新

A ファイルを指定して更新する

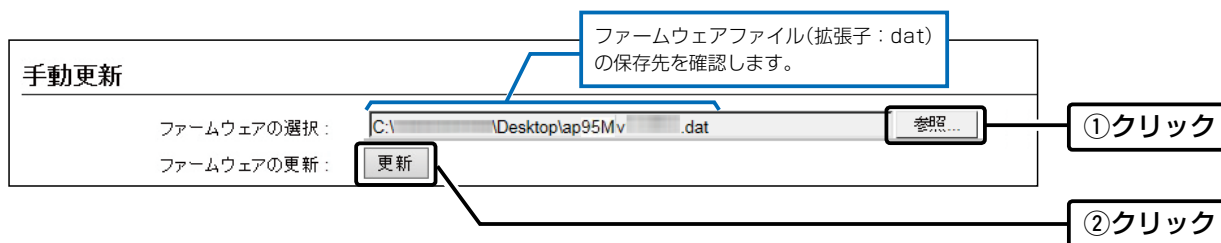
ファームウェアの更新を実行する前に、現在の設定内容を保存されることをおすすめします。(P.4-2)

※ 更新後、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。

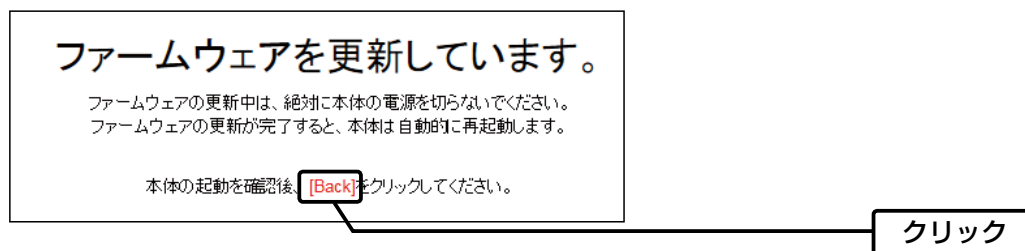
※ 日常、管理者以外の端末から更新できないように、設定画面へのアクセス制限の設定をおすすめします。(P.3-117)

- 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。)
※更新が完了するまで、約10分かかります。



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」にアクセスしなおしてください。

4 保守について

4. ファームウェアを更新する

管理 > ファームウェアの更新

⑧ オンライン更新

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更新できます。

※ 自動更新機能が「有効」に設定されているときに、オンラインで新しいファームウェアを検知します。(P.3-138)

※ 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。

※ 更新を実行する前に、現在の設定内容を保存されることをおすすめします。(P.4-2)

- 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、更新は必要ありません。

- 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。
※更新により、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、更新を実行する前に、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、そのまま約10分お待ちください。
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。

ファームウェアを更新しています。

ファームウェアの更新中は、絶対に本体の電源を切らないでください。
ファームウェアの更新が完了すると、本体は自動的に再起動します。

本体の起動を確認後、[Back]をクリックしてください。

この章では、
困ったときの対処法、設定画面の構成、仕様などを説明しています。

1. 困ったときは	5-2
2. Telnet/SSHで接続するには	5-5
■ Telnet/SSHコマンドについて	5-5
3. 設定画面の構成について	5-6
4. 初期値一覧	5-9
■ ネットワーク設定	5-9
■ ルーター設定	5-11
■ 無線LAN設定	5-12
■ 管理	5-18
5. 機能一覧	5-19
■ 無線LAN機能	5-19
■ ネットワーク管理機能	5-19
■ ルーター管理機能	5-19
■ その他	5-19
6. 設定項目で利用できる文字列について	5-20
■ ネットワーク設定	5-20
■ 無線LAN設定	5-20
■ 管理	5-20
7. PoEによる電源供給について	5-21
8. 弊社製無線アクセスポイントの機能対応表	5-22
9. 定格について	5-23
■ 一般仕様	5-23
■ 有線部	5-23
■ 無線部	5-23

5 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。

[POWER] ランプが点灯しない

- ACアダプターが本製品に接続されていない
→ 本製品のACアダプター、およびDCプラグの接続を確認する
- ACアダプターをパソコンなどの電源と連動したコンセントに接続している
→ 本製品のACアダプターを壁などのコンセントに直接接続する

[LAN] ポートの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
→ 本製品やパソコンの[LAN]ポート、またはLANケーブルを確認する
- パソコン、またはHUBの電源が入っていない
→ パソコンとHUBの電源が入っていることを確認する

[2.4GHz] ランプ/[5GHz] ランプが緑点灯しない

- パソコンの無線LANが機能していない
→ ご使用のパソコン、または無線LANアダプターに付属の取扱説明書を確認する
- 無線LAN端末と本製品の無線LAN規格が異なっている
→ ご使用になる無線LAN端末が準拠している無線LAN規格を確認する
- 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
- 無線LAN端末の通信モードが「アドホック」になっている
→ 無線通信モードを「インフラストラクチャー」に変更する
- SSID(またはESSID)の設定が異なっている
→ 本製品と無線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
→ 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で通信できる端末を制限している
→ 通信を許可する無線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

[2.4GHz] ランプ/[5GHz] 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の設定が異なっている

→ 本製品と接続先の暗号化セキュリティの設定を確認する

仮想APIにWeb認証機能やPOPCHAT@Cloud連携機能などの制限が設定され、認証前の状態になっている

→ 設定を解除する、または端末からWWWブラウザで認証画面にアクセスして認証情報を入力する

IEEE802.11n規格、またはIEEE802.11ac規格で通信できない

- 無線LAN端末がIEEE802.11n規格、またはIEEE802.11ac規格に準拠していない
→ IEEE802.11n規格、またはIEEE802.11ac規格に準拠した無線LAN端末を使用する
- 「AES」以外の暗号化セキュリティを使用している
→ IEEE802.11n規格、IEEE802.11ac規格で通信する場合は、暗号化設定を「なし」、または「AES」に設定する

5 ご参考に

1. 困ったときは

WPS機能が動作しない(無線LANを自動設定できない)

- 本製品のWPS機能を無効に設定している
→ WPS機能を使用するインターフェースが未設定か、インターフェースの番号を間違えて設定している(P.2-13)
- 無線LAN端末が無線LANの自動設定に対応していない
→ WPS対応の無線LAN端末を用意する
- ほかの無線LAN端末と自動設定中である
→ ほかの無線LAN端末との自動設定が完了するまで待つ
- 本製品と無線LAN端末の自動設定操作を2分以内に開始できなかった
→ 自動設定操作を2分以内に開始する
- 何度繰り返しても、自動設定できない
→ WPS機能を無効に変更して、手動で設定する

本製品の設定画面で設定を変更できない

- 管理ツール設定を「有効」に設定して、RS-AP3やRC-AP10で管理を開始している
→ RS-AP3やRC-AP10側で設定を変更する
→ RS-AP3やRC-AP10側で管理を終了して、本製品の設定画面で設定を変更する

RS-AP3やRC-AP10から本製品を管理できない

- 管理ツール設定が「無効」に設定されている
→ 管理ツール設定を「有効」に設定する
- 本製品のIPアドレスがRS-AP3やRC-AP10側に正しく設定されていない
→ 本製品のIPアドレスを確認して、設定しなおす
- LANケーブルが本製品と正しく接続されていない
→ 本製品やRC-AP10、HUBの[LAN]ポート、またはLANケーブルを確認する

無線AP間通信できない(WBR)

- 親機で、DFS機能が有効なチャンネルが選択されている、または「自動」を設定している
→ 使用されているチャンネルを確認する
- 子機の暗号化設定が親機の仮想AP*と異なっている
→ 親機の暗号化設定を確認する
- 子機のSSIDが親機の仮想AP*と異なっている
→ 親機のSSIDを確認する
- 無線AP間通信する子機のBSSIDが親機に正しく登録されていない
→ 子機のBSSIDを確認する

★親機により、SSID、暗号化を確認する仮想APが異なりますのでご注意ください。(2021年6月現在)

「ath0」: AP-95M(無線LAN1(2.4GHz帯))、AP-9500(無線LAN1(5GHz帯))、SE-900(アクセスポイントモード時)、SB-900(無線1(2.4GHz帯))

「ath1」: AP-95M(無線LAN2(5GHz帯))、AP-9500(無線LAN2(2.4GHz帯))

「ath4」: AP-90M、AP-90MR

「ath8」: AP-900、AP-9000

5 ご参考に

1. 困ったときは

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 Explorer 10 以前を使用している
→ Microsoft Internet Explorer 11 以降を使用する

本製品の設定画面にアクセスできない

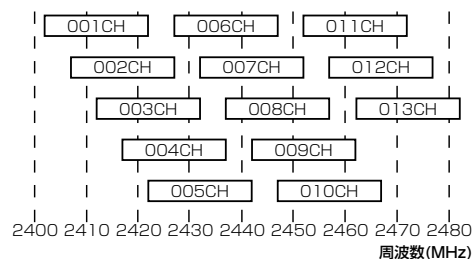
- パソコンの IP アドレスを設定していない
→ 本製品の出荷時や全設定初期化時は、DHCP サーバー機能が無効のため、パソコンの IP アドレスを固定 IP アドレスに設定する
- IP アドレスのネットワーク部が、本製品とパソコンで異なっている
→ パソコンに設定された IP アドレスのネットワーク部を本製品と同じにする
- 無線 LAN 設定が、本製品とパソコンで異なっている
→ パソコンに設定されたネットワーク認証や暗号鍵(キー)を本製品と同じにする
- ご使用の WWW ブラウザーにプロキシサーバーが設定されている
→ Internet Explorer の「ツール(T)」メニューから「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

2.4GHz 帯使用時に電波干渉が発生した

本製品の近くに 2.4GHz 帯の無線アクセスポイントやビル間通信機器が存在する

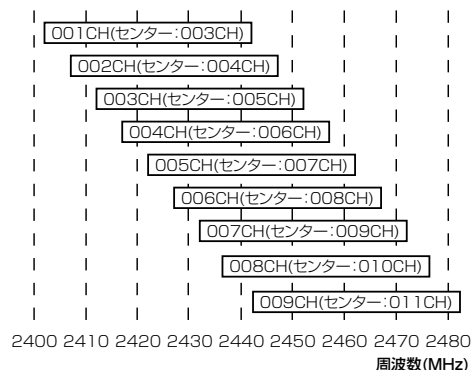
【帯域幅が 20MHz の場合】(帯域の 1 部が重複)

- 本製品の設置場所を変更する
- 無線アクセスポイント側のチャンネルを変更する
※ 近くに存在する無線 LAN 機器と 4 チャンネル以上空けて設定する
※ たとえば、お互いの設定を「001CH(2412MHz)」-「006CH(2437MHz)」-「011CH(2462MHz)」にすると電波干渉しません。



【帯域幅が 40MHz の場合】(帯域の 1 部がすべてのチャンネルで重複)

- 本製品の設置場所を変更する
- 本製品の帯域幅(20MHz)やパワーレベルを変更する
- 無線アクセスポイント側のチャンネルを変更する
※ たとえば、お互いの設定を「001CH(2412MHz)」-「009CH(2452MHz)」にすると電波干渉しません。
※ 通常(20MHz)の 2 倍の周波数帯域幅を使用するため、設定できるのは「001CH(2412MHz)~009CH(2452MHz)」だけです。



2. Telnet/SSHで接続するには

Telnet/SSHでの接続について説明します。

ご使用のOSやTelnet/SSH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。

※出荷時、「Telnet/SSH設定」項目の[Telnet]欄が「無効」に設定されているため、Telnetクライアントから本製品にアクセスできません。(P.3-121)

※本製品のTelnetで採用している文字コードは、UTF-8です。

Windows標準のTelnetクライアントでは対応できない場合がありますので、UTF-8に対応したターミナルソフトウェアをご使用ください。

【ログインについて】

① 下記を入力して、ログインします。

login : admin(固定)

password : admin

※「管理者」画面で設定したパスワードを入力します。(P.3-117)

出荷時や全設定初期化時のpasswordは、adminです。

② ログインに成功すると、プロンプト AP-95M> が表示されます。

【設定の保存について】

設定変更後、「save」を入力して[Enter]キーを押します。

※コマンド入力で保存をしていない場合、本体再起動後、設定の変更が失われます。

【ログアウトについて】

「quit」、「exit」、「logout」コマンドを実行すると、ログアウトします。

■ Telnet/SSHコマンドについて

使用できるTelnet/SSH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、コマンド名につづいて、「?」を入力するとコマンドのヘルプが表示されます。 例) AP-95M> save ? (saveコマンドのヘルプを表示する場合) ※「help」を入力して[Enter]キーを押すと、全ヘルプの一覧が表示されます。 ※Windows標準のTelnetクライアントでは文字化けする場合がありますので、UTF-8に対応したターミナルソフトウェアをご使用ください。
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) s[Tab]→save 複数のコマンドがあるときは、1回目の押下でビープ音コマンドを送出し、2回目以降の押下でコマンド候補を表示します。 例) res[Tab]→reset restart ※ビープ音は、お使いのターミナルソフトウェアやOSの設定により、音の有無、音色が異なります。

5 ご参考に

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	システム情報 MACアドレス WANステータス
情報表示	ネットワーク情報	インターフェース Ethernetポート接続情報 無線LAN AP間通信(WBR) DHCPリース情報
	SYSLOG	SYSLOG
	無線LAN情報	アクセスポイント情報 端末情報 AP間通信情報
ネットワーク設定	IPアドレス	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
	スタティックルーティング	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
	ポリシールーティング	送信元ルーティング設定 送信元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
	Web認証 基本	Web認証 カスタムページ
	Web認証 詳細	Web認証方法 RADIUS設定
	POPCHAT@Cloud	アカウント設定 インターフェース設定
ルーター設定	WAN接続先	回線状態表示 回線種別設定
	アドレス変換	アドレス変換設定 DMZホスト設定 静的マスカレードテーブル設定 静的マスカレードテーブル設定一覧
	IPフィルター	一般設定 IPフィルター設定 IPフィルター設定一覧
	簡易DNS	簡易DNSサーバー設定 簡易DNSサーバー設定一覧

5 ご参考に

3. 設定画面の構成について

設定メニュー	設定画面	設定項目
無線LAN設定	無線LAN1 無線LAN	無線LAN
	無線LAN1 仮想AP	仮想AP設定
		暗号化設定
	無線LAN1 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
	無線LAN1 ネットワーク監視	ネットワーク監視設定
	無線LAN1 AP間通信 (WBR)	AP間通信設定
	無線LAN1 WMM詳細	WMM詳細設定
		WMMパワーセーブ設定
	無線LAN1 レート	レート設定
	無線LAN1 ARP代理応答	ARP代理応答設定
		ARPキャッシュ情報
	無線LAN1 IP Advanced Radio System	近隣呼出設定
	無線LAN2 無線LAN	無線LAN
	無線LAN2 仮想AP	仮想AP設定
		暗号化設定
	無線LAN2 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
	無線LAN2 ネットワーク監視	ネットワーク監視設定
	無線LAN2 AP間通信 (WBR)	AP間通信設定
	無線LAN2 WMM詳細	WMM詳細設定
		WMMパワーセーブ設定
	無線LAN2 レート	レート設定
	無線LAN2 ARP代理応答	ARP代理応答設定
		ARPキャッシュ情報
	無線LAN2 IP Advanced Radio System	近隣呼出設定
	WPS	WPS設定
		WPS開始
		WPS状態表示
	災害用仮想AP	災害用仮想AP

5 ご参考に

3. 設定画面の構成について

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
		無線アクセスポイント管理ツール設定
	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
		SNTPサーバー設定
	SYSLOG	SYSLOG設定
	SNMP	SNMP設定
		SNMPv3設定
		LED消灯モード
	ネットワークテスト	PINGテスト
		経路テスト
	再起動	再起動
	設定の保存/復元	設定の保存
		設定の復元
		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

5 ご参考に

4. 初期値一覧

本製品の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
「IPアドレス」画面	
本体名称	本体名称：AP-95M ※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)
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)
「スタティックルーティング」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)
「ポリシールーティング」画面	
ポリシールーティング設定	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一覧	(設定なし) ※最大登録数：64
「Web認証 基本」画面(ath0、ath01～ath07、ath1、ath11～ath17)	
Web認証	インターフェース：ath0
	Web認証：無効
	ページタイトル：Set your page title. ※任意の255文字以内
	ポータルサイト：http://www.example.com/ ※「http://」も含めて半角255文字以内
	移動待ち時間：5(秒) ※設定範囲「0～60」(秒)
	有効期限：24時間

5 ご参考に

4. 初期値一覧

■ ネットワーク設定(つづき)

設定画面/項目	初期値
「Web認証 詳細」画面(ath0、ath01～ath07、ath1、ath11～ath17)	
Web認証方法	インターフェース：ath0 認証方法：RADIUSのみ使用
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
「POPCHAT@Cloud」画面	
アカウント設定	アクティベートキー：空白(設定なし) ※半角64文字以内
インターフェース設定(ath0、ath01～ath07、ath1、ath11～ath17)	
	インターフェース：ath0
	Wi-Fi認証@クラウド：無効

5 ご参考に

4. 初期値一覧

■ ルーター設定

設定画面/項目		初期値		
「WAN接続先」画面				
回線種別設定		回線種別：LANポートとして使用する		
「アドレス変換」画面				
アドレス変換設定		アドレス変換：有効		
DMZホスト設定		DMZホスト IPアドレス：空白(設定なし)		
静的マスカレードテーブル設定一覧		設定なし ※最大登録数：32		
「IPフィルター」画面				
一般設定		遮断時の動作：破棄		
		IPフィルター不一致時のSYSLOG：無効		
IPフィルター設定一覧				
番号	フィルター方法	TCPプロトコル (TCPフラグ)	送信元IPアドレス(送信元ポート番号)	SYSLOGに出力
	フィルター方向		宛先IPアドレス(宛先ポート番号)	
59	遮断	TCP/UDP	*(135)	無効
	OUT		*(*)	
60	遮断	TCP/UDP	*(*)	無効
	OUT		*(135)	
61	遮断	TCP/UDP	*(445)	無効
	OUT		*(*)	
62	遮断	TCP/UDP	*(*)	無効
	OUT		*(445)	
63	遮断	TCP (フラグ指定なし)	*(*)	無効
	OUT		*(137-139)	
64	遮断	UDP	*(137-139)	無効
	OUT		*(137-139)	
「簡易DNS」画面				
簡易DNSサーバー設定一覧		設定なし		

5 ご参考に

4. 初期値一覧

■ 無線LAN設定

設定画面/項目	初期値
「無線LAN1 無線LAN」画面	
無線LAN設定	無線UNIT：有効
	帯域幅：20MHz
	チャンネル：001CH (2412MHz)
	パワーレベル：高
	DTIM間隔：1 ※設定範囲「1～50」
	プロテクション：有効
「無線LAN1 仮想AP」画面(ath0、ath01～ath07)	
仮想AP設定	インターフェース：ath0
	仮想AP：有効(ath0)
	無効(ath01～ath07)
	SSID：WIRELESSLAN-0(ath0) ※半角英数字32文字以内
	WIRELESSLAN-1(ath01)
	WIRELESSLAN-2(ath02)
	WIRELESSLAN-3(ath03)
	WIRELESSLAN-4(ath04)
	WIRELESSLAN-5(ath05)
	WIRELESSLAN-6(ath06)
	WIRELESSLAN-7(ath07)
	VLAN ID：0(ath0、ath01～ath07)
	ANY接続拒否：無効(ath0、ath01～ath07)
	接続端末制限：63(ath0、ath01～ath07)
	同一仮想AP内の端末間通信禁止：無効(ath0、ath01～ath07)
	アカウントリング：無効(ath0、ath01～ath07)
	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、ath01～ath07)
	暗号化方式：なし(ath0、ath01～ath07)
「無線LAN1 MACアドレスフィルタリング」画面(ath0、ath01～ath07)	
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
「無線LAN1 ネットワーク監視」画面(ath0、ath01～ath07)	
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
無線LAN1 AP間通信(WBR)画面	
AP間通信設定	AP間通信：無効

5 ご参考に

4. 初期値一覧

■ 無線LAN設定(つづき)

設定画面/項目	初期値
「無線LAN1 WMM詳細」画面	
WMM詳細	周波数帯 : 2.4GHz
	[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]
	No Ack : AC_BK ☐ 、AC_BE ☐ 、AC_VI ☐ 、AC_VO ☐
	[From Station]
	ACM : AC_VI ☐ 、AC_VO ☐
WMM/パワーセーブ設定	WMM/パワーセーブ : 有効
「無線LAN1 レート」画面(ath0、ath01～ath07)	
レート設定	インターフェース : ath0
	プリセット : 初期値
	レガシー :
	1Mbps : ベーシックレート
	2Mbps : ベーシックレート
	5.5Mbps : ベーシックレート
	6Mbps : 有効
	9Mbps : 有効
	11Mbps : ベーシックレート
	12Mbps : 有効
	18Mbps : 有効
	24Mbps : 有効
	36Mbps : 有効
	48Mbps : 有効
	54Mbps : 有効

5 ご参考に

4. 初期値一覧

■ 無線LAN設定(つづき)

設定画面/項目	初期値
「無線LAN1 レート」画面(ath0、ath01～ath07)	
レート設定	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：1Mbps
仮想AP共通設定	キックアウト：弱
「無線LAN1 ARP代理応答」画面(ath0、ath01～ath07)	
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エイジング時間：0(分) ※設定範囲「0～1440」(分)
「無線1 IP Advanced Radio System」画面(ath0、ath01～ath07)	
近隣呼出設定	インターフェース：ath0
	テナント番号 通知 名前 名前は任意の31文字以内
	1 有効 空白(設定なし)
	2 有効 空白(設定なし)
	3 有効 空白(設定なし)
	4 有効 空白(設定なし)
	5 有効 空白(設定なし)
	6 有効 空白(設定なし)
	7 有効 空白(設定なし)
	8 有効 空白(設定なし)
	9 有効 空白(設定なし)
	10 有効 空白(設定なし)

5 ご参考に

4. 初期値一覧

■ 無線LAN設定(つづき)

設定画面/項目	初期値
「無線LAN2 無線LAN」画面	
無線LAN設定	無線UNIT：有効
	帯域幅：20MHz
	チャンネル：036CH (5180MHz)
	パワーレベル：高
	DTIM間隔：1 ※設定範囲「1～50」
	プロテクション：有効
「無線LAN2 仮想AP」画面(ath1、ath11～ath17)	
仮想AP設定	インターフェース：ath1
	仮想AP：有効(ath1)
	無効(ath11～ath17)
	SSID：WIRELESSLAN-0(ath1) ※半角英数字32文字以内
	WIRELESSLAN-1(ath11)
	WIRELESSLAN-2(ath12)
	WIRELESSLAN-3(ath13)
	WIRELESSLAN-4(ath14)
	WIRELESSLAN-5(ath15)
	WIRELESSLAN-6(ath16)
	WIRELESSLAN-7(ath17)
	VLAN ID：0(ath1、ath11～ath17)
	ANY接続拒否：無効(ath1、ath11～ath17)
	接続端末制限：63(ath1、ath11～ath17)
	同一仮想AP内の端末間通信禁止：無効(ath1、ath11～ath17)
	アカウンティング：無効(ath1、ath11～ath17)
	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(ath1、ath11～ath17)
	暗号化方式：なし(ath1、ath11～ath17)
「無線LAN2 MACアドレスフィルタリング」画面(ath1、ath11～ath17)	
MACアドレスフィルタリング設定	インターフェース：ath1
	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

5 ご参考に

4. 初期値一覧

■ 無線LAN設定(つづき)

設定画面/項目	初期値
「無線LAN2 ネットワーク監視」画面(ath1、ath11～ath17)	
ネットワーク監視設定	インターフェース：ath1
	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
「無線LAN2 AP間通信(WBR)」画面	
AP間通信設定	AP間通信：無効
「無線LAN2 WMM詳細」画面	
WMM詳細設定	周波数帯：5GHz
	[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]
	No Ack：AC_BK ☐ 、AC_BE ☐ 、AC_VI ☐ 、AC_VO ☐
	[From Station]
	ACM：AC_VI ☐ 、AC_VO ☐
WMM/パワーセーブ設定	WMM/パワーセーブ：有効
「無線LAN2 レート」画面(ath1、ath11～ath17)	
レート設定	インターフェース：ath1
	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

5 ご参考に

4. 初期値一覧

■ 無線LAN設定(つづき)

設定画面/項目	初期値			
「無線LAN2 レート」画面(ath1、ath11～ath17)				
レート設定	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			
	VHT-MCS：			
	1ストリーム：MCS 0-9			
	2ストリーム：MCS 0-9			
マルチキャスト送信レート：				
マルチキャスト：6Mbps				
仮想AP共通設定	キックアウト：弱			
「無線LAN2 ARP代理応答」画面(ath1、ath11～ath17)				
ARP代理応答	インターフェース：ath1			
	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)			
「無線 2 IP Advanced Radio System」画面(ath1、ath11～ath17)				
近隣呼出設定	インターフェース：ath1			
	テナント番号	通知	名前	名前は任意の31文字以内
	1	有効	空白（設定なし）	
	2	有効	空白（設定なし）	
	3	有効	空白（設定なし）	
	4	有効	空白（設定なし）	
	5	有効	空白（設定なし）	
	6	有効	空白（設定なし）	
	7	有効	空白（設定なし）	
	8	有効	空白（設定なし）	
	9	有効	空白（設定なし）	
	10	有効	空白（設定なし）	
「WPS」画面(なし、ath0、ath01～ath07、ath1、ath11～ath17)				
WPS設定	使用するインターフェース：なし			
「災害用仮想AP」画面				
災害用仮想AP	00000JAPAN 仮想AP：無効			

5 ご参考に

4. 初期値一覧

■ 管理

設定画面/項目	初期値
「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	
RS-AP3	RS-AP3：無効
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：無効 Telnetポート番号：23 SSH：有効 SSH認証方式：自動 SSHポート番号：22 SSH公開鍵：(空白)
「時計」画面	
時刻設定	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
SNTPサーバー設定	SNTPサーバー機能：有効
「SYSLOG」画面	
SYSLOG	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ID (GET)：public 場所：空白(設定なし) 連絡先：空白(設定なし)
SNMPv3設定	ユーザー名：空白(設定なし) 認証パスワード：空白(設定なし) 暗号パスワード：空白(設定なし)
「LED」画面	
LED消灯モード	LED消灯モード：無効 LED消灯モードに入るまでの時間：30秒 ※設定範囲「0～3600」(秒)
「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
「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

- IEEE802.11ac規格★¹
- IEEE802.11n規格★¹
- IEEE802.11a/g/b規格
- 暗号化セキュリティ(WEK 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
- 災害用仮想AP機能(00000JAPAN)
- 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
- 無線AP間通信機能(WBR)
- 同一仮想AP内の端末間通信禁止機能
- WMM★²(Wi-Fi Multimedia)機能
- WPS機能★²
- ARP代理応答
- WMMパワーセーブ
- 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
- 自動チャンネル機能

■ ネットワーク管理機能

- SYSLOG
- SNMP(MIB-II)
- RS-AP3

■ ルーター管理機能

- PPPoE接続(常時/手動)
- DHCPクライアント接続
- 固定IP接続
- DMZ
- IPマスカレード
- 静的マスカレード
- DHCPサーバー機能
- 静的DHCPサーバー機能
- スタティックルーティング
- ポリシールーティング
- IPフィルター機能
- DNS代理応答

■ その他

- タグVLAN機能
- 認証VLAN
- パケットフィルター
- 接続制限機能(管理者ID/パスワード)
- 内部時計設定
- Web認証(RADIUS/ローカルリスト)
- POPCHAT@Cloud連携機能
- PoE機能
- ファームウェアの更新
- 設定保存/復元
- WWWメンテナンス(HTTP/HTTPS)
- TELNETメンテナンス(TELNET/SSH)

★¹ 本製品のIEEE802.11ac規格、IEEE802.11n規格での通信は、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。

★² 本製品は、Wi-Fiアライアンスの認定を取得していません。(2021年6月現在)

6. 設定項目で利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。

■ 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
IPアドレス	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	253文字以内
Web認証 詳細	ローカルリスト	ユーザー名	ASCII ^{★2}	128文字以内
		パスワード	ASCII ^{★2}	128文字以内

■ 無線LAN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	2-4ページ参照
		PSK (Pre-Shared Key)	ASCII ^{★2} 、または16進数	2-3ページ参照
AP間通信(WBR) 子機設定		WEPキー	ASCII ^{★2} 、または16進数	2-4ページ参照
		PSK (Pre-Shared Key)	ASCII ^{★2} 、または16進数	2-3ページ参照

■ 管理

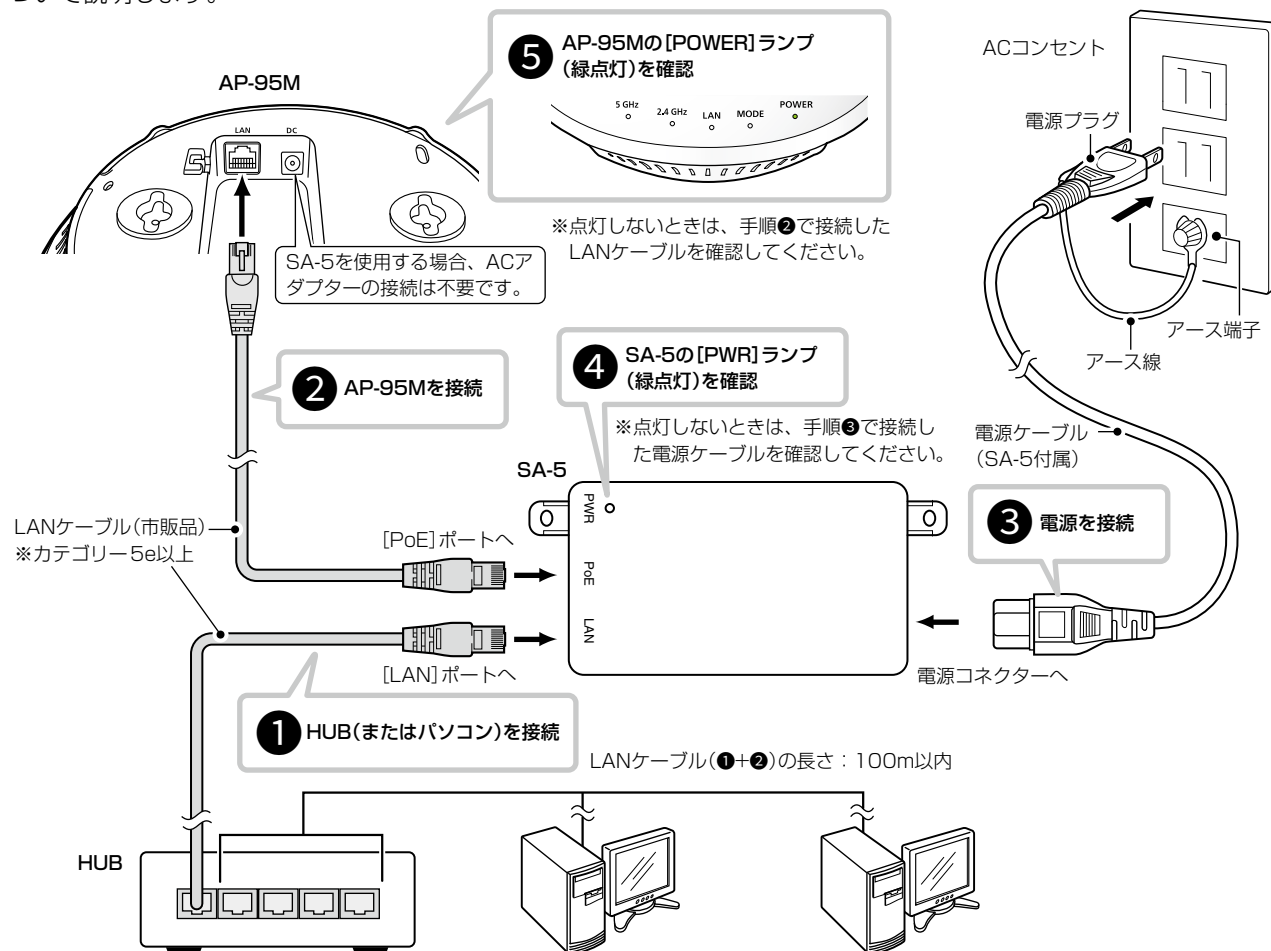
設定画面	設定項目	設定欄	入力できる文字列	入力できる文字数
管理者	管理者パスワードの変更	パスワード	半角英数字/記号	31文字以内
SNMP	SNMP設定	コミュニティID(GET)	半角英数字/記号 ※「\」/「*」/「 」を除く	31文字以内
ネットワークテスト	PINGテスト	ホスト	半角英数字 ^{★1} /「.」/「-」 ※先頭と末尾は半角英数字のみ	64文字以内
	経路テスト	ノード	半角英数字 ^{★1} /「.」/「-」 ※先頭と末尾は半角英数字のみ	64文字以内

★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. PoEによる電源供給について

本製品の[LAN]ポートに接続されたLANケーブルとSA-5(別売品)を接続して、本製品に電源を供給する接続方法について説明します。



- SA-5の[LAN]ポートとHUB(HUBを使用しない場合はパソコン)*をLANケーブルで接続します。
★SA-5は、MDI(ストレート)/MDI-X(クロス)を切り替えできません。
- SA-5の[PoE]ポートと本製品のLANポートを、LANケーブルで接続します。
- SA-5に付属の電源ケーブルを、SA-5の電源コネクタとACコンセントに接続します。
- SA-5の[PWR]ランプが緑点灯することを確認します。
※点灯しない場合は、手順③で接続した電源ケーブルを確認してください。

- 本製品の[POWER]ランプが緑点灯することを確認します。
※点灯しない場合は、手順②で接続したLANケーブルを確認してください。
※1000BASE-T規格、またはIEEE802.3af規格でご使用になる場合は、必ずカテゴリ5e以上のLANケーブルをご使用ください。
※カテゴリ5以下のLANケーブルを使用すると、1000BASE-T規格、またはIEEE802.3af規格では正常に動作しないことがあります。

設置と接続のご注意

- ◎1台のSA-5で電源供給できるのは、本製品1台だけです。
- ◎本製品用のACアダプターは必要ありません。
- ◎SA-5には、電源が必要ですので、コンセントから近い場所に設置してください。
- ◎SA-5は、HUBなどのネットワーク機器に搭載のリピーター機能を搭載していません。
使用するLANケーブルは、HUB(HUBを使用しない場合はパソコン)からSA-5を介して接続された本製品までの総延長距離が100m以内の場所に設置してください。
※ご使用になるLANケーブルの種類によっては、総延長距離が短くなることがあります。
- ◎SA-5は、防水構造ではありませんので、雨水などでぬれやすい場所には設置できません。

5 ご参考に

8. 弊社製無線アクセスポイントの機能対応表

		AP-90M	AP-90MR	AP-95M	AP-900	AP-9000	AP-9500	SE-900 (アクセスポイントモード時)
ルーター	ルーター機能	×	○	○	×	○	○	×
	WANポート	×	○★ ¹	○★ ¹	×	○★ ¹	○	×
ネットワーク	ポートベースVLAN	×	×	×	×	○	×	×
	パケットフィルター	○	○	○	○	○	×	○
無線	無線UNIT数	2	2	2	2	2	2	1
	動作モード	×	×	×	×	×	×	○★ ²
	アンテナ種別	×	×	×	×	×	○	○
	無線動作モード	○	○	×	×	×	×	○
	ストリーム数設定	×	×	×	○	×	×	○
	無線UNITごとの 仮想AP数	4	4	8★ ⁶	8	8	8	8
	AP間通信(WDS)	無線1	無線1	×	無線1	無線1	×	×
	AP間通信(WBR)	無線2	無線2	無線LAN1/2	無線2	無線2	無線LAN1/2	○
	WPS	○	○	○	×	○	○	×
管理	USB設定	○	○	×	×	○	○	×
	LED消灯モード	○	○	○★ ⁷	×	○	○	×
その他	CONSOLE★ ⁴ ★ ⁵	×	×	×	○	○	○	×
	初期化ボタン	○ (MODE)	○ (MODE)	○ (MODE)	×	○ (INIT)	○ (MODE)	○ (MODE)
	屋外対応	×	×	×	○	×	×	○

★1 AP-90MRやAP-95Mの場合、ルーター機能使用時は[LAN]ポートをWANポートとして使用します。

AP-9000の場合、[WAN/LAN]ポートを設定で切り替えて使用します。

★2 クライアントモードに切り替えることで無線LAN端末として動作します。

★3 AP-900やAP-9000では、無線1が2.4GHz帯、無線2が5GHz帯に固定されています。

AP-95Mでは、無線LAN1が2.4GHz帯、無線LAN2が5GHz帯に固定されています。

AP-9500では、無線LAN1が5GHz帯、無線LAN2が2.4GHz帯に固定されています。

★4 AP-9000やAP-9500の設定にターミナルソフトウェアを使用するときは、市販品のUSBケーブル(miniBタイプ)を[CONSOLE]ポートに接続します。

使用方法など、ご使用になる機器の取扱説明書をご覧ください。

★5 AP-900の設定にターミナルソフトウェアを使用するときは、設定用ケーブルを[CONSOLE]ポートに接続します。

設定用ケーブルは販売しておりませんので、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。

★6 災害用仮想APを除いた数です。

★7 「有効」([POWER]ランプ減灯)には設定できません。

9. 定格について

■ 一般仕様

電	源	源：DC12V±10% [DCプラグ極性：⊖—●—⊕] ※ACアダプター(付属品)は、AC100V±10% ※PoEは、IEEE802.3af準拠 最大9W(付属のACアダプター使用時) 最大9W(PoE使用時)
使 用 環 境		温度-10～+55℃(0℃以下では常時通電時)*、湿度5～95% (結露状態を除く) ★-10℃～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162(W)×42(H)×162(D)mm(突起物を除く)
重	量	約520g(付属品を除く)
適 合 規 格		クラスB情報技術装置(VCCI)
インターフェース		ランプ(5GHz、2.4GHz、LAN、MODE、POWER) ボタン(MODE)

■ 有線部

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規格準拠
通 信 速 度	：[LAN]部 10/100/1000Mbps(自動切り替え/全二重)

■ 無線部

国 際 規 格	：IEEE802.11ac準拠、IEEE802.11n準拠 IEEE802.11a準拠、IEEE802.11g/b準拠
国 内 規 格	：ARIB STD-T71/ARIB STD-T66
使用周波数範囲	：5180～5700MHz 2412～2472MHz

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。

高品質がテーマです。

