

ワイヤレスアクセスポイント
AP-9600

IEEE802.11ax規格準拠
IEEE802.11ac規格準拠
IEEE802.11n規格準拠
IEEE802.11a/g/b規格準拠

はじめに

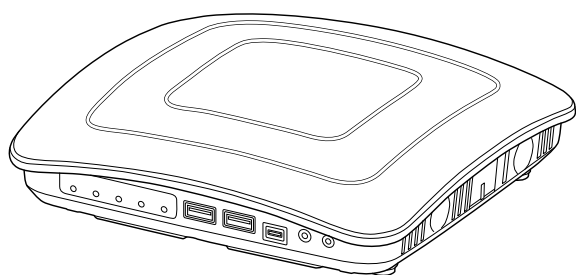
1 ご使用になる前に

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



Icom Inc.

- ◎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、IEEE802.11ax規格、IEEE802.11ac規格*に準拠し、2.4GHz帯と5GHz帯の2波同時通信ができる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。

★IEEE802.11ac規格を使用できるのは、5GHz帯だけです。

登録商標/著作権について

アイコム、ICOM、ICOMロゴは、アイコム株式会社の登録商標です。

Microsoft、Windowsは、マイクロソフト企業グループの商標です。

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. 1.01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

- ◎IEEE802.11ax規格に準拠し、最大2402Mbps(理論値)の速度で通信できます。
 - ※2402Mbps(理論値)は、5GHz帯で帯域幅を「80MHz」に設定したときの速度です。
 - ※IEEE802.11ax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。
- ◎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。
- ◎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」、「WPA3」、「WPA3-SAE」に対応しています。
- ◎「IEEE802.1X」、「WPA」、「WPA2」、「WPA3」を設定すると、認証にRADIUSサーバーを使用できます。
- ◎IEEE802.3bt規格に準拠したPoE受電機能に対応しています。
 - ※本製品の性能を十分に発揮するために、PoEから受電する場合は、IEEE802.3bt規格対応のHUBまたはインジェクター製品(市販品)と接続してください。
- ◎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、多台数接続時の通信速度を改善できます。
- ◎USBメモリー(市販品)を本製品のUSBポートに接続することで、ファームウェアの更新、設定の保存/復元ができます。
- ◎PPPoE、DHCP、固定IPなど、各種接続方式に対応したブロードバンドルーター機能を搭載しています。
- ◎インターネットを利用して、専用線のような通信回線を構築できるVPNルーター機能を搭載しています。
- ◎ネットワーク管理機能として、SNMPに対応しています。
- ◎IPフィルター機能を搭載していますので、アクセス制限ができます。
- ◎本製品は、免許不要・資格不要です。

はじめに

別売品について

(2023年4月現在)

RS-AP3 (近日対応予定)
アクセスポイント管理ツール

RC-AP10 (近日対応予定)
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	LAN側IP	IPアドレス設定	IPアドレス	192.168.0.1
			サブネットマスク	255.255.255.0
	DHCPサーバー	DHCPサーバー設定	DHCPサーバー	無効
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	無線UNIT	無効
			チャンネル	036CH (5180MHz) (無線LAN1) 001CH (2412MHz) (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
			暗号化設定	ネットワーク認証 オープンシステム
			暗号化方式	なし
管理	管理者	管理者パスワードの変更	管理者ID	admin (変更不可)
			現在のパスワード	—

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	IEEE802.11ax (W52/W53/W56)	80MHz	2402Mbps
		40MHz	1147Mbps
		20MHz	574Mbps
	IEEE802.11ac (W52/W53/W56)	80MHz	1733Mbps
		40MHz	800Mbps
		20MHz	347Mbps
	IEEE802.11n (W52/W53/W56)	40MHz	600Mbps
		20MHz	289Mbps
	IEEE802.11a (W52/W53/W56)	20MHz	54Mbps
2.4GHz	IEEE802.11ax	40MHz	1147Mbps
		20MHz	574Mbps
	IEEE802.11n	40MHz	600Mbps
		20MHz	289Mbps
	IEEE802.11g	20MHz	54Mbps
	IEEE802.11b	20MHz	11Mbps

【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*
5.2/5.3/5.6GHz	IEEE802.11ax (W52/W53/W56)	約30m	約100m
	IEEE802.11ac (W52/W53/W56)		
	IEEE802.11n (W52/W53/W56)		
	IEEE802.11a (W52/W53/W56)		
2.4GHz	IEEE802.11ax	約30m	約100m
	IEEE802.11n		
	IEEE802.11g		
	IEEE802.11b		

※本書では、AP-9600同士で通信した場合の距離を参考として記載しています。

★ 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。

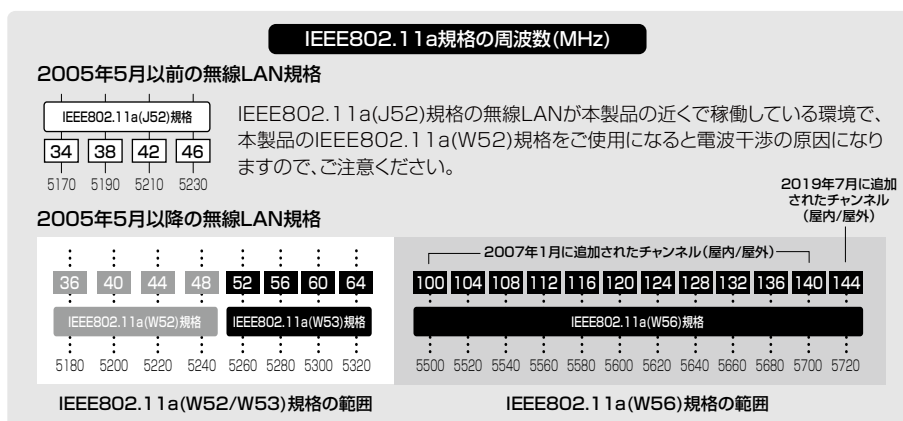
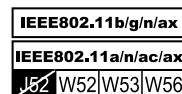
はじめに

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。



帯域幅と無線通信チャンネルについて

本製品には、5GHz帯用(無線LAN1)、2.4GHz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。

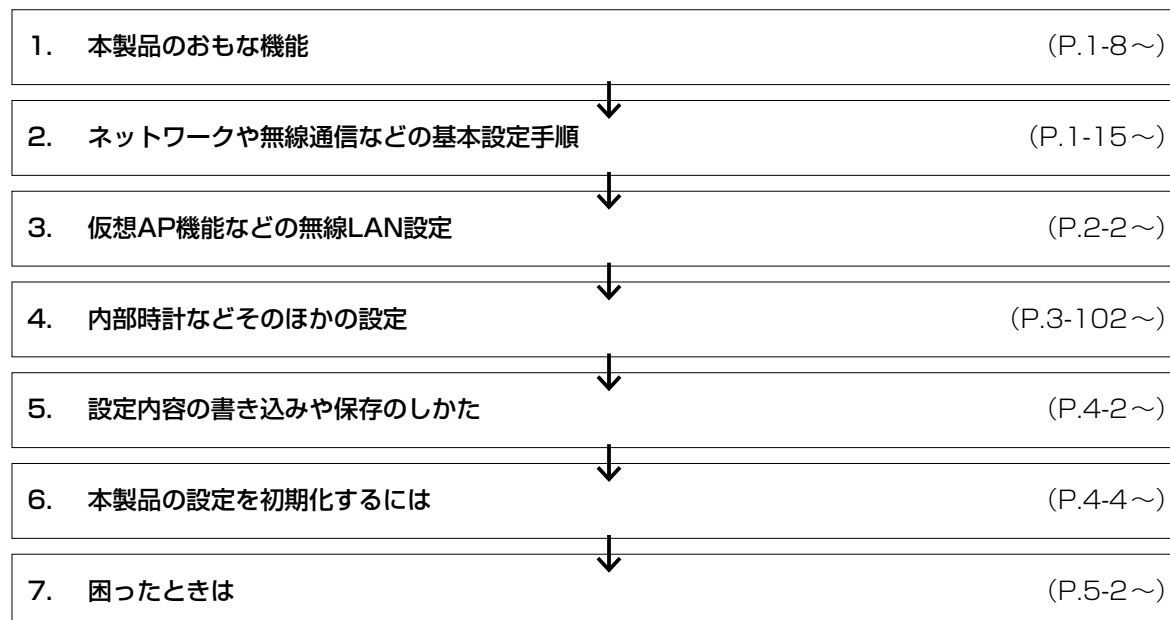
周波数帯	帯域幅	使用できるチャンネル
5GHz	80MHz	36、40、44、48、52、56、60、64、100、104、108、112、116、120、124、128、132、136、140、144
	40MHz	36、44、52、60、100、108、116、124、132、140
	20MHz	36、40、44、48、52、56、60、64、100、104、108、112、116、120、124、128、132、136、140、144、自動
2.4GHz	40MHz	1、2、3、4、5、6、7、8、9
	20MHz	1、2、3、4、5、6、7、8、9、10、11、12、13、自動

※帯域幅を80MHzに設定できるのは、無線LAN1(5GHz帯)だけです。

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。



はじめに

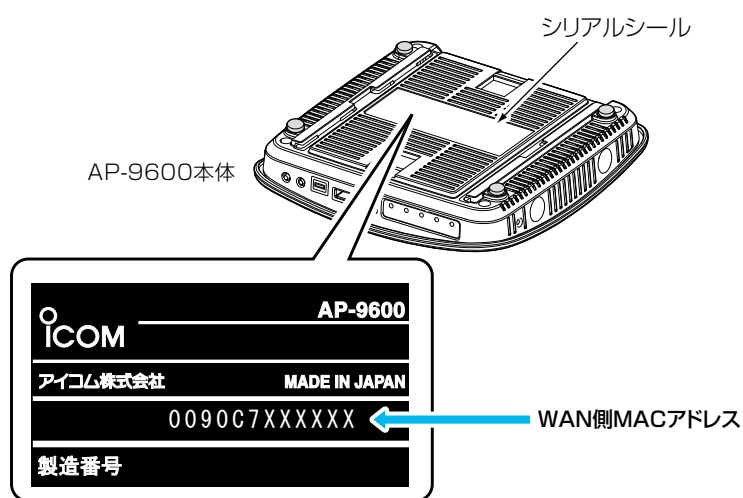
本体MACアドレスが必要なときは

本体MACアドレス(機器固有の番号)は、本製品のシリアルシール(下図)に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、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WAN側MACアドレス(機器固有の番号)を、ご契約の接続業者、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。

※無線LANやLAN側のMACアドレスではありませんのでご注意ください。



※MACアドレスの記載位置は、お買い上げの製品によって若干異なる場合があります。

ご参考

上記のMACアドレスは、設定画面でも確認できます。(P.3-5)

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
■ 外観図	1-2
■ LANポート側	1-3
■ ランプ表示側	1-4
■ <MODE>ボタン側/セキュリティースロット側	1-7
2. おもな機能について	1-8
■ アクセスポイント機能	1-8
■ 無線ネットワーク名(SSID)	1-8
■ 接続端末制限機能	1-8
■ IEEE802.11ax規格	1-8
■ ビームフォーミング機能/MU-MIMO機能	1-8
■ ローミング機能について	1-9
■ 無線AP間通信機能(WBR)について	1-10
■ 仮想AP機能について	1-11
■ DFS機能とチャンネルの自動設定	1-12
■ ルーター機能	1-13
■ VPN機能	1-13
3. 接続や設置について	1-14
■ 本製品を壁面に固定するときは	1-14
4. 設定のしかた	1-15
■ 設定用のパソコンに固定IPアドレスを設定する	1-15
■ 設定に使うパソコンを接続する	1-16
■ 設定画面へのアクセスと初期設定について	1-17
■ 設定画面の名称と機能について	1-18
■ 設定画面の表示について	1-19
■ 本体IPアドレスを変更するときは	1-21

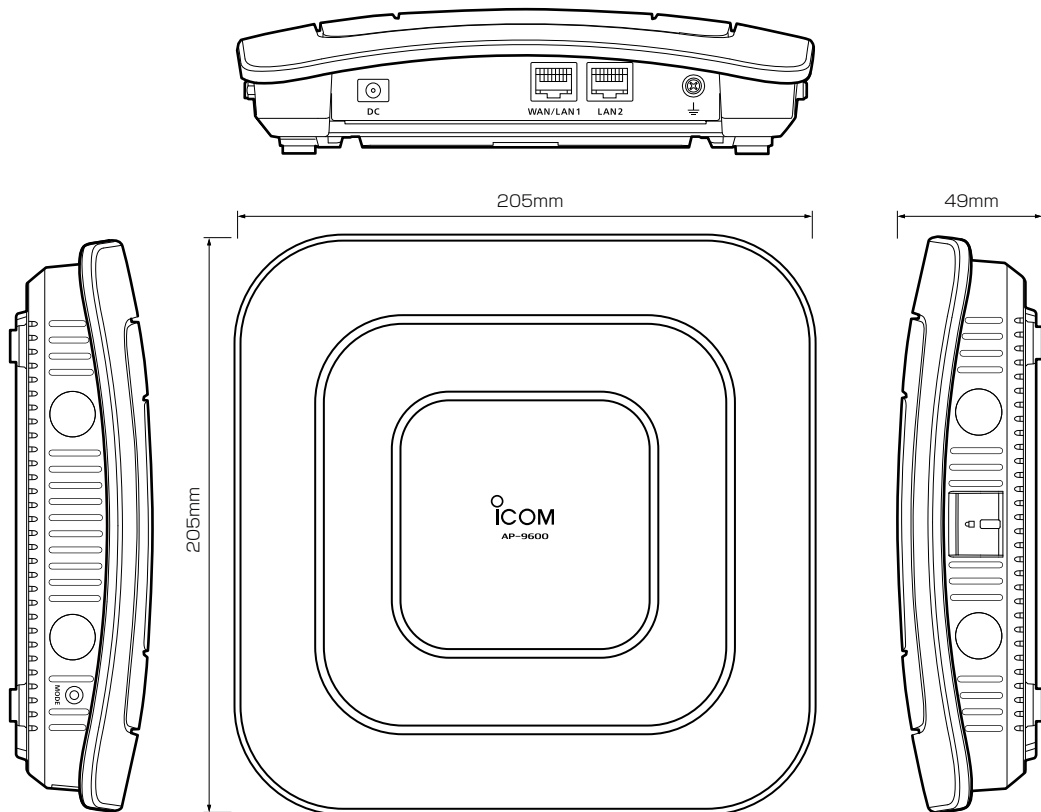
1 ご使用になる前に

1. 各部の名称と機能

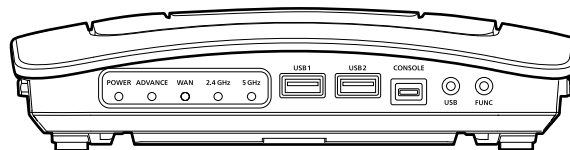
■ 外観図

各面の詳細については、参照ページをご覧ください。

LANポート側(P.1-3)



〈MODE〉ボタン側(P.1-7)



セキュリティーロット側
(P.1-7)

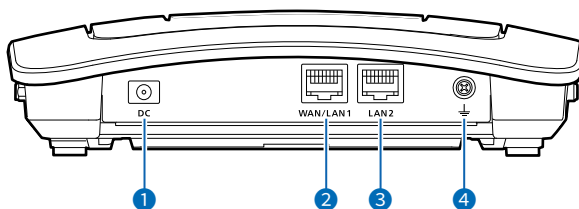
ランプ表示側(P.1-4)

1 ご使用になる前に

1. 各部の名称と機能

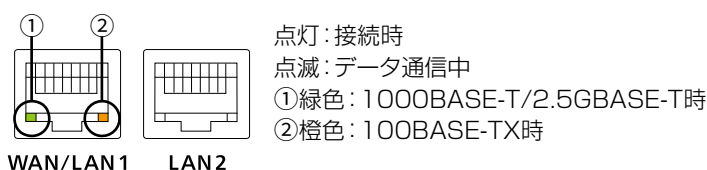
■ LANポート側

LANポートやランプの動作について説明します。



- ① 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。
- ② [WAN/LAN1]ポート …………… 回線種別の設定によって、用途が異なります。(P.1-13)
(RJ-45型×1) ※PoEから受電する場合は、回線種別設定に関係なく使用できますので、IEEE802.3bt規格対応のHUBまたはインジェクター製品(市販品)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。
- ③ [LAN2]ポート …………… HUBなどのネットワーク機器と接続します。
(RJ-45型×1) ※PoEから受電する場合は、IEEE802.3bt規格対応のHUBまたはインジェクター製品(市販品)と接続してください。

ランプ表示



- ④ アース端子 …………… 市販のアース線を接続します。

ご注意

IEEE802.3at規格のPoEから受電する場合は、次のように制限されます。

- ・無線LAN(1/2)が2ストリームに制限されます。
- ・[USB1]ポートの最大出力電流が500mAに制限されます。
- ・[USB2]ポートは使用できません。

※IEEE802.3af規格の場合は、動作保証外です。

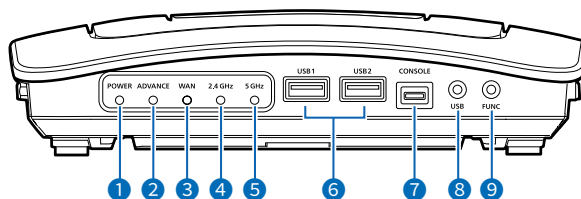
1 ご使用になる前に

1. 各部の名称と機能

■ ランプ表示側

ランプの動作やUSBポートについて説明します。

※すべてのランプ(①～⑤)が赤点滅のときは、機器の異常を検出していますので、弊社サポートセンターにお問い合わせください。

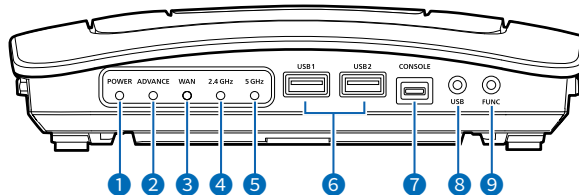


- ① [POWER]ランプ ……………
- 青点灯：電源ON時
 - ☀️ 青点滅：ファームウェアロード時
 - 橙点灯：オンライン更新(ファームウェア更新あり)
 - ☀️ 橙点滅：〈MODE〉ボタン操作時
 - 消 灯：電源OFF時
- ※電源投入時、すべてのランプが点滅(赤→緑→青→白)します。
※起動中、[POWER]ランプは白点灯→青点滅→青点灯の順で遷移します。
※LED消灯モードが「有効」のときは、[POWER]ランプの明るさが暗くなり、「有効(完全消灯)」のときは消灯します。(出荷時の設定：無効)
- ② [ADVANCE]ランプ ……………
- 青点灯：USBメモリー接続時
 - ☀️ 青点滅：USBロード時
 - 赤点灯：USBロード失敗時
 - 消 灯：USBメモリー未接続
- ③ [WAN]ランプ ……………
- 青点灯：リンク時(2.5GBASE-T)
 - ☀️ 青点滅：データ通信中(2.5GBASE-T)
 - 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(100BASE-TX)
 - ☀️ 橙点滅：データ通信中(100BASE-TX)
 - 消 灯：リンク未確立時
- ④ [2.4GHz]ランプ ……………
- 青点灯：端末が1台以上帰属時
 - 橙点灯：2.4GHz帯有効時(帰属端末なし)
 - 消 灯：2.4GHz帯無効時

1 ご使用になる前に

1. 各部の名称と機能

■ ランプ表示側

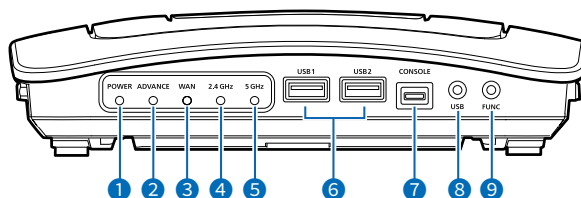


- 5 [5GHz]ランプ ……………
- 青点灯： 端末が1台以上帰属時
 - 橙点灯： 5GHz帯有効時(帰属端末なし)
 - ☀ 橙点滅： DFS動作による無線動作待機中
 - 消 灯： 5GHz帯無効時
- 6 [USB](1/2)ポート …………… (USB3.0)
- 設定復元、ファームウェアの更新で使用するUSBメモリー(市販品)を接続します。
- ご使用になるときは、USBポートの奥まで挿入してください。
- ※使用するUSBデバイスについては、4-10ページでご確認ください。
- ※最大出力電流が「オフ」に設定されているUSBポートは、USBデバイスを接続しても使用できません。(P.1-3、P.3-96)
- ※すべてのUSBデバイスでの動作を保証するものではありません。

1 ご使用になる前に

1. 各部の名称と機能

■ ランプ表示側



- ⑦ [CONSOLE]ポート …………… 本製品の設定にターミナルソフトウェアを使用するとき、USBケーブル(市販品)を接続します。
(USB Type-C)
※ご使用していただくために必要なUSBドライバー、およびインストールガイドは、弊社ホームページ(下記参照)からダウンロードできます。
※USBケーブル(Type-C)、ターミナルソフトウェアは、別途ご用意ください。
- ⑧ <USB>ボタン …………… USBメモリー接続時、[ADVANCE]ランプ(②)が点灯(青)から消灯に切り替わるまでボタンを長く押しと、USBメモリーを取りはずせます。
※設定復元、ファームウェアの更新で使用するUSBメモリー(市販品)を差し込んだときは、[ADVANCE]ランプ(②)が点灯(青)してからボタンを短く押ししてください。(P.4-9)
- ⑨ <FUNC>ボタン …………… 本製品の設定画面で割り当てた機能进行操作するときを使用します。
※2023年4月現在、近日常対応予定です。

USBドライバーのダウンロードについて

本製品の[CONSOLE]ポートは、弊社ネットワーク機器用のUSBドライバーで動作します。

弊社ホームページのサポート情報(サポート情報→法人のお客様→ダウンロード)から、USBドライバーをダウンロードできます。

アイコム株式会社 サポート情報

<https://www.icom.co.jp/support/business/>

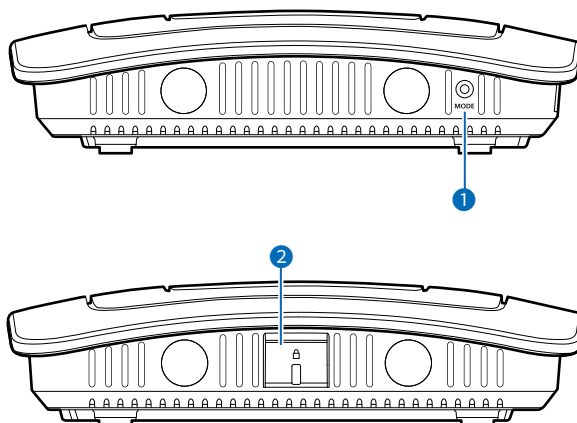
※弊社ホームページからのダウンロード手順については、予告なく変更する場合がありますのであらかじめご了承ください。

1 ご使用になる前に

1. 各部の名称と機能

■ 〈MODE〉ボタン側/セキュリティー slots 側

接続部やボタン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 セキュリティー slots 市販のセキュリティーワイヤーで本製品を固定するときに使用します。
机の脚や支柱などにセキュリティーワイヤーを固定してから、本製品のセキュリティー slots 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ーワイヤーの取扱説明書をご覧ください。
※セキュリティーワイヤーには、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ー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、IEEE802.11ax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。

※ 出荷時、本製品の無線UNITは「無効」に設定されています。

※ 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.2-3)

※ 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5GHz帯用(無線LAN1)と2.4GHz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。

■ IEEE802.11ax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2402Mbps★(理論値)の速度で通信できます。

★ IEEE802.11ax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。

最大2402Mbps(理論値)で使用するには、無線LAN1で帯域幅を「80MHz」に設定してください。(P.2-8)
(無線LAN2で帯域幅を「40MHz」に設定すると最大1147Mbps)

※ IEEE802.11ac/n/a/g/b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。

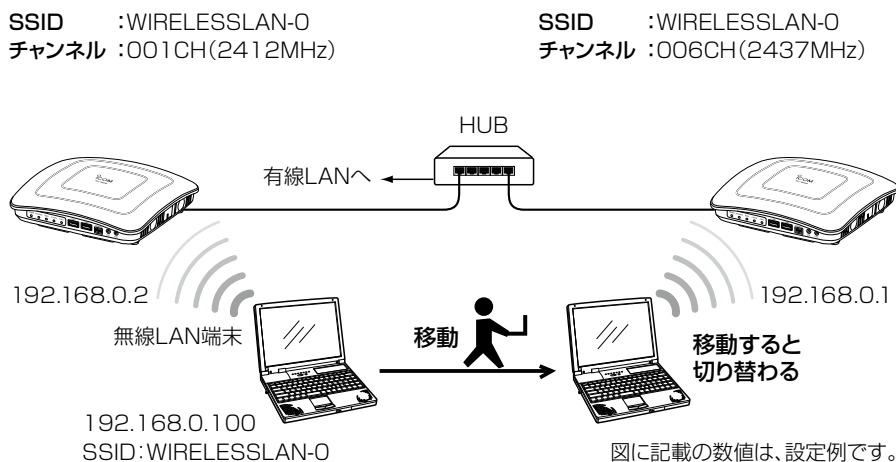
さらに、電波干渉を避けて、複数の端末へ並行送信できるMU-MIMO機能も備え、多台数接続時の通信速度を改善できます。

1 ご使用になる前に

2. おもな機能について

■ 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。

上記の例にある2.4GHz帯で無線LANを使用する場合は、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。

※5GHz帯で無線AP間通信が利用できるのは、5.2GHz帯だけです。

※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。(P.5-20)

無線AP間通信機能(WBR)を使用する場合

◎ 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.2-6)、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。(2023年4月現在)

「ath0」: AP-95M(無線LAN1(2.4GHz帯))、AP-9500/AP-9600(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/AP-9600(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 :036 CH (5180 MHz)
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。

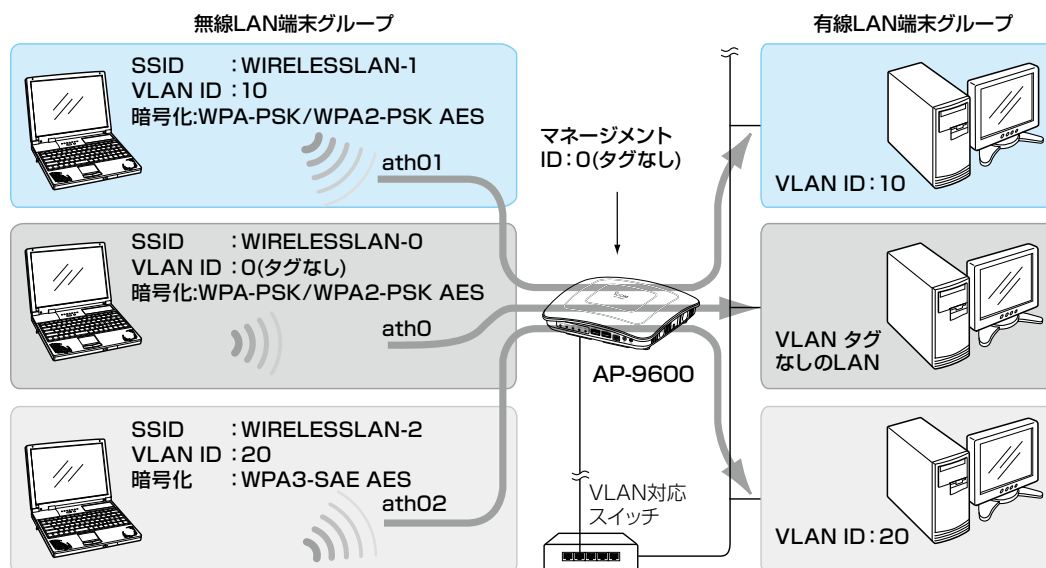
※電波強度が変化しても、接続が切れない限りローミングしません。

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。
※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

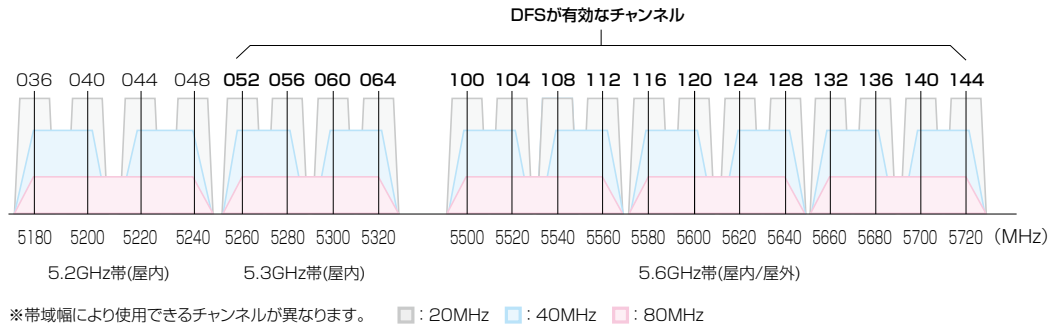
- ◎仮想APを使用して、最大16グループの無線ネットワークを構築できます。
- ◎複数の仮想AP機能を使用する場合、1つのユニットに対して、同じSSIDを設定できません。
- ◎各仮想APの無線LAN端末グループに、VLAN ID(0~4094)を設定できます。
- ◎出荷時、本製品の[管理ID]が「0」(タグなし)に設定されていますので、VLAN IDが設定されたネットワークからは、本製品の設定画面にアクセスできません。

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(052～144)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[●]橙点滅して、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(100～144)でレーダー波を検出した場合は、[5GHz]ランプが[●]橙点滅すると同時に、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(052～144)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。

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

本製品のルーター機能を使用すると、本製品に接続したパソコンや機器からインターネットに接続できます。

※ 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[WAN/LAN1]ポートに接続します。

※ 出荷時や全設定初期化時、本製品のルーター機能(回線種別)は、「無効(LANポートとして使用する)」に設定されています。(P.3-41)

ご契約の回線接続業者との契約内容にしたがって、回線種別(DHCPクライアント/PPPoE/固定IP)を設定してください。

■ VPN機能

VPN(Virtual Private Network)機能を使用すると、インターネット上の2地点を暗号化通信で接続して、仮想的なネットワークを構成できます。

※ VPN機能を使用する場合は、本製品の[WAN/LAN1]ポートにWAN回線を接続し、ルーター機能(回線種別)の設定が必要です。

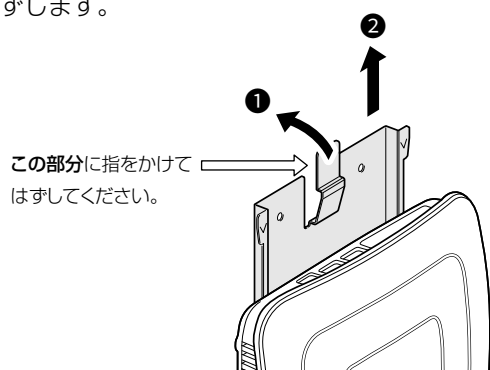
※接続先に合わせて、IPsecトンネルを登録してください。(P.3-60)

1 ご使用になる前に

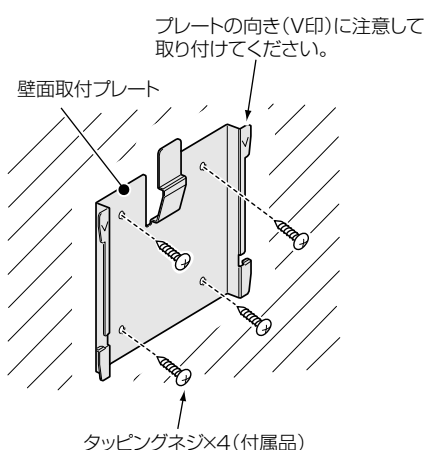
3. 接続や設置について

■ 本製品を壁面に固定するときは

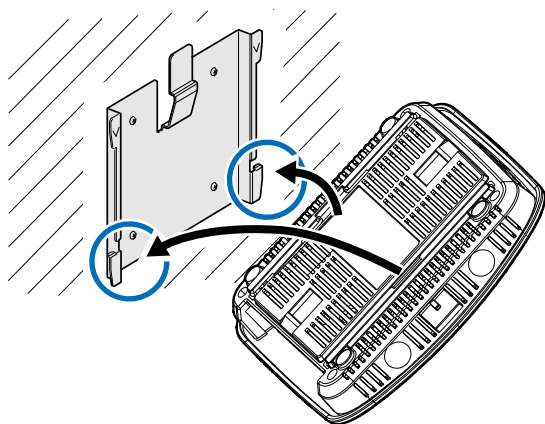
- 1 出荷時、本製品に壁面取付プレートが装着されていますので、図のように壁面取付プレートを取りはずします。



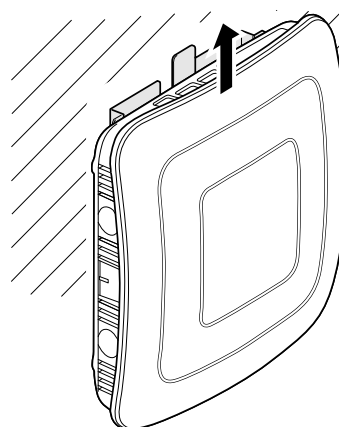
- 2 壁面取付プレートを壁面に取り付けます。



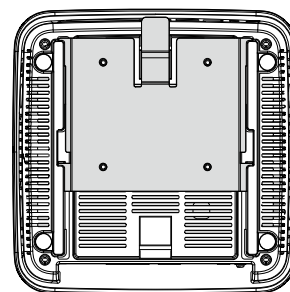
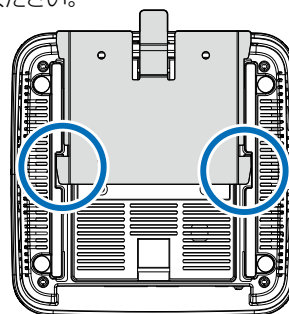
- 3 壁面取付プレートの下部を本製品の溝(右図参照)に差し込みます。



- 4 本製品をスライドして固定します。(下図参照)



○の部分にプレートを差し込むように取り付けたと、本製品をスライドしてください。



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には、接続するパソコンに固定IPアドレスの設定が必要です。

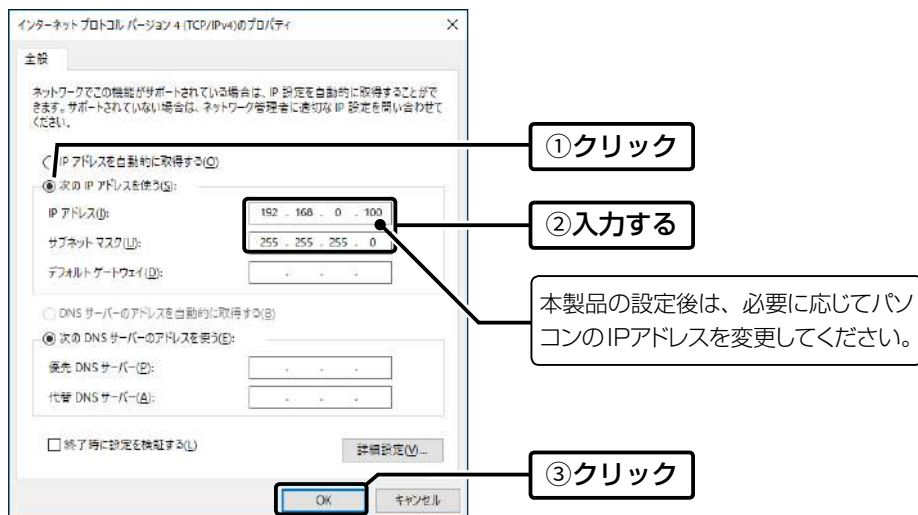
■ 設定用のパソコンに固定IPアドレスを設定する

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

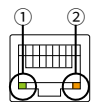
4. 設定のしかた

■ 設定に使うパソコンを接続する

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ポートにある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。



WAN/LAN 1



LAN 2

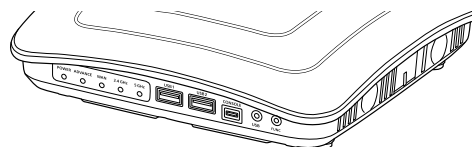
ランプ表示について

点灯：接続時

点滅：データ通信中

① 緑色：1000BASE-T/2.5GBASE-T時

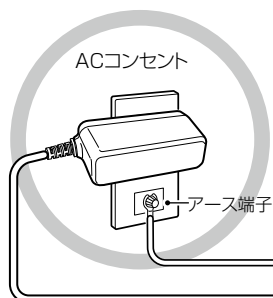
② 橙色：100BASE-TX時



[POWER]ランプなどは、LANポートの反対側にあります。

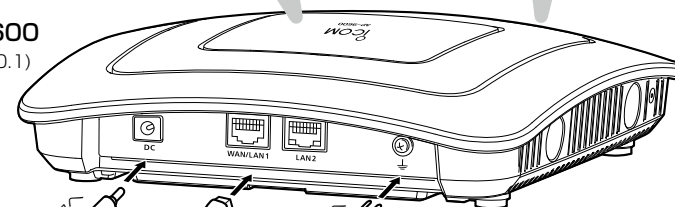
② 電源を接続する

本製品の[POWER]ランプが点灯します。



AP-9600

(出荷時の設定: 192.168.0.1)



設定用パソコン

(設定例: 192.168.0.100)

① 各ケーブルを接続する

LANケーブル
(市販品: カテゴリー5e以上)

③ パソコンを起動する

⚠ 警告

◎本製品のアース端子を、ガス管や水道管には絶対に接続しないでください。

◎落雷したときの電氣的ショックの緩和、感電やノイズの回り込みを防止するため、本製品のアース端子は、市販のアース線を使用して、コンセントのアース端子、または地中に埋めたアース棒(市販品)に必ず接続してください。

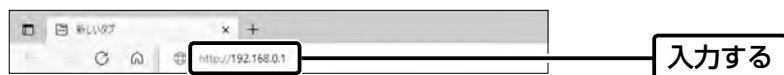
1 ご使用になる前に

4. 設定のしかた

■ 設定画面へのアクセスと初期設定について

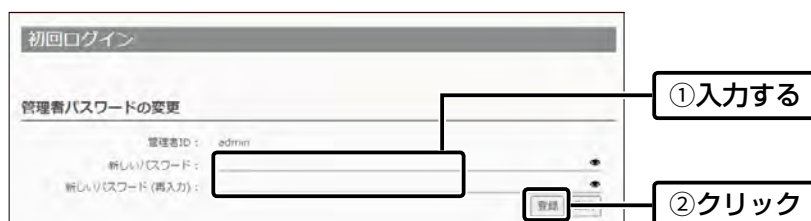
はじめて本製品をご使用になるときは、管理者パスワードの設定が必要です。
下記の手順で設定画面にアクセスして、設定してください。

- 1 WWWブラウザのアドレスバーに「http://192.168.0.1」を入力し、[Enter]キーを押します。
初回ログイン画面が表示されます。



※上図は、出荷時のIPアドレス(192.168.0.1)を入力した場合です。

- 2 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)で各項目を入力して、〈登録〉をクリックします。
※目のアイコン(右端)をクリックすると、入力したパスワードを確認できます。



- 3 サインイン画面が表示されたら、[ユーザー名]欄に「admin」、[パスワード]欄に手順2で設定したパスワードを入力し、〈サインイン〉をクリックします。
通常の設定画面に切り替わります。



※次回以降のアクセスでは、ユーザー名(admin)と設定したパスワードを入力してください。
※管理者パスワードを忘れた場合は、工場出荷時(初期値)の状態に戻す必要があります。

WWWブラウザについて

動作確認済のWWWブラウザは、Microsoft Edge(Chromiumベース)です。
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。

保存場所について

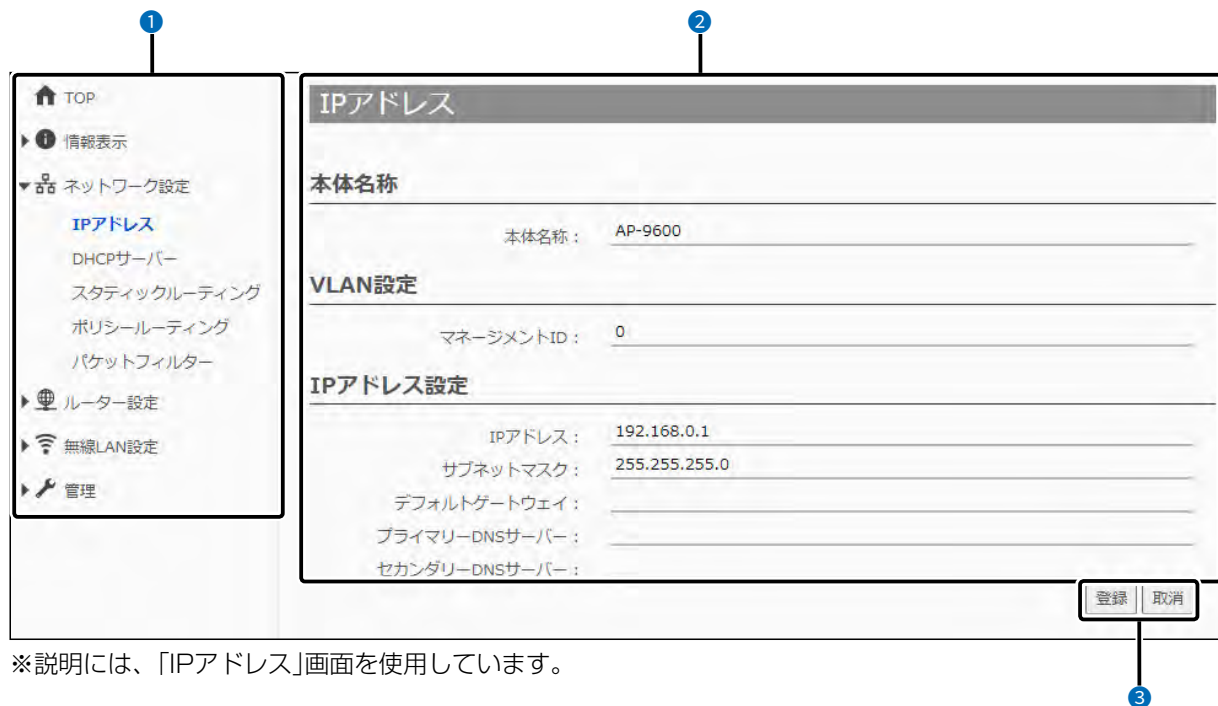
設定内容を保存すると、Microsoft Edge (Chromiumベース)の場合、デフォルトの設定では、「ダウンロード」フォルダーにファイルが保存されます。
必要に応じて、WWWブラウザの設定で、デスクトップなど任意の場所に変更してください。

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、5-7ページをご覧ください。



※説明には、「IPアドレス」画面を使用しています。

- 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

ICOM AP-9600

TOP
情報表示
ネットワーク設定
IPアドレス
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
IPsecトンネル

IPアドレス

本体名称
本体名称 : AP-9600

VLAN設定
マネージメントID : 0

設定画面：中

ICOM AP-9600

IPアドレス

本体名称
本体名称 : AP-9600

VLAN設定
マネージメントID : 0

IPアドレス設定

設定画面：小

ICOM AP-9600

IPアドレス

本体名称
本体名称 : AP-9600

VLAN設定
マネージメントID : 0

IPアドレス設定

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

「≡」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。

本体名称
本体名称: AP-9500

VLAN設定
マネージメントID: 0

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:
プライマリDNSサーバー:
セカンダリDNSサーバー:

登録

※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.1-17)
※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」(サブネットマスク「255.255.255.0」)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
■ 無線通信機能を有効にするには	2-2
■ 無線ネットワーク名を手動で設定する	2-3
■ 暗号化を手動で設定する	2-4
■ MACアドレスフィルタリングを設定するには	2-5
■ 自動チャンネルを設定するときは	2-6
■ 80MHz帯域幅通信をするときは	2-8
2. 無線LAN接続[活用編]	2-9
■ 仮想APを設定するには	2-9
■ 無線AP間通信機能(WBR)を使用する場合	2-10
■ アカウンティング設定について	2-14
■ RADIUS設定について	2-15

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 > 無線LAN

■ 無線通信機能を有効にするには

無線LAN1 (5GHz帯) を例に無線通信機能を有効にする手順を説明します。

※出荷時や全設定初期化時、本製品の無線UNITは「無効」に設定されています。

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 [無線UNIT] 欄で「有効」を選択します。 (出荷時の設定：無効)

無線LAN	
無線UNIT :	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
帯域幅 :	20 MHz
チャンネル :	036 CH (5180 MHz)
パワーレベル :	高
DTIM間隔 :	1

登録 取消

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

■ 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 (5GHz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

アカウントティング : 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

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、出荷時の設定で使用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

■ 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 (5GHz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 : WPA2-PSK/WPA3-SAE
暗号化方式 : AES
PSK (Pre-Shared Key) : wirelessmaster

- 1 [ネットワーク認証]欄で「WPA2-PSK/WPA3-SAE」、[暗号化方式]欄で「AES」を選択し、[PSK (Pre-Shared Key)]欄で「wirelessmaster」(半角)を入力します。

※目のアイコン(右端)をクリックすると、入力したパスワードを確認できます。

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

アカウントिंग : 無効 有効

暗号化設定

ネットワーク認証 : WPA2-PSK/WPA3-SAE

暗号化方式 : AES

PSK (Pre-Shared Key) : wirelessmaster

WPAキー更新間隔 : 120 分

登録 取消

① 選択する

② 入力する

※目のアイコン(右端)をクリックすると、入力した内容を確認できます。

- 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]

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

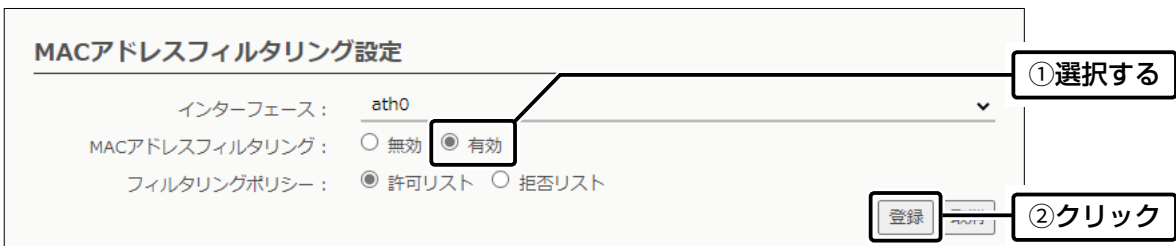
仮想APごとに、本製品への接続を許可する、または拒否する無線LAN端末を登録できます。

※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 (5GHz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。



- 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(052～144)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。

5GHz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：036CH (5180MHz))

The image shows two screenshots of the wireless LAN settings interface. The top screenshot shows the '無線LAN' (Wireless LAN) settings page with the following options: 無線UNIT: 無効 (radio button), 有効 (radio button, selected); 帯域幅: 20 MHz; チャンネル: 自動; パワーレベル: 高; DTIM間隔: 1. A blue box highlights the '20 MHz' band width, with an arrow pointing to it and the text '出荷時の設定であることを確認します。' (Confirm that this is the factory setting). A box labeled '① 選択する' (Select) points to the '自動' channel dropdown. A box labeled '② クリック' (Click) points to the '登録' (Register) button.

The bottom screenshot shows the same settings page after the '登録' button is clicked. The 'チャンネル' dropdown now shows '自動' and '使用中チャンネル: 100 CH (5500 MHz)'. A box labeled '③ 確認する' (Confirm) points to the '自動' channel dropdown. The '登録' button is now disabled, and a '取消' (Cancel) button is visible.

ご注意

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(100～144)に設定してご使用ください。

※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。

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

2.4GHz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：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

登録

① 選択する

② クリック



無線LAN

無線UNIT : 無効 有効

帯域幅 : 20 MHz

チャンネル : 自動

使用中チャンネル: 006 CH (2437 MHz)

パワーレベル : 高

DTIM間隔 : 1

登録 取消

③ 確認する

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LAN

■ 80MHz帯域幅通信をするときは

IEEE802.11ax規格を使用できるのは、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2402Mbps（理論値）で使用するには、無線LAN1（5GHz帯）で帯域幅を「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LAN1」、「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)

The screenshot shows the '無線LAN' (Wireless LAN) settings page. The '無線UNIT' (Wireless Unit) is set to '有効' (Enabled). The '帯域幅' (Channel Width) is set to '80 MHz', which is highlighted with a box and a '選択する' (Select) button. Other settings include 'チャンネル' (Channel) at '036 CH (5180 MHz)', 'パワーレベル' (Power Level) at '高' (High), and 'DTIM間隔' (DTIM Interval) at '1'. There are '登録' (Register) and '取消' (Cancel) buttons at the bottom right.

3 「登録」をクリックします。

40/80MHz帯域幅通信をする時の手引き

◎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

2. 無線LAN接続 [活用編]

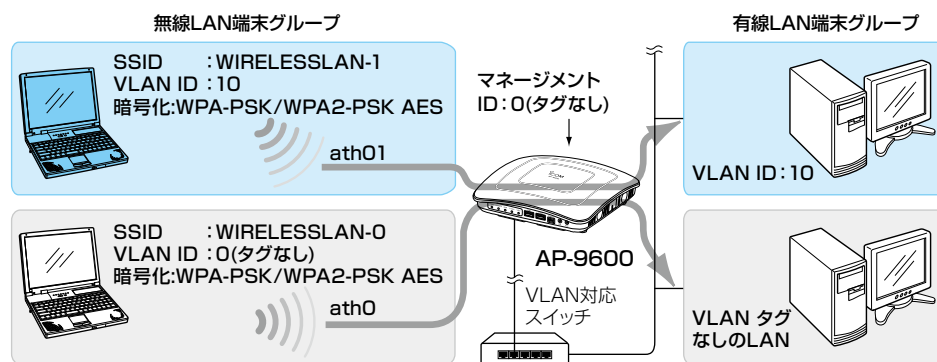
無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ 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.1-11)

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。

① 選択する

② クリック

③ 入力する

④ 選択する

⑤ 入力する

⑥ クリック

※目のアイコン(右端)をクリックすると、入力した内容を確認できます。

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)

■ 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.1-10)

※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.2-6)、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、「036 CH (5180 MHz)」(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ときは」で設定されているものとします。(P.1-21)

親機(P.2-12)

[無線LAN設定]項目	チャンネル	: 「036 CH (5180 MHz)」(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.2-13)

[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。

親機側の設定	子機側の設定
チャンネル : 036 CH (5180 MHz)	SSID : WIRELESSLAN-0
仮想AP : ath0	ネットワーク認証 : WPA2-PSK
SSID : WIRELESSLAN-0	暗号化方式 : AES
ネットワーク認証 : WPA2-PSK	PSK : wirelessmaster
暗号化方式 : AES	
PSK : wirelessmaster	
接続先BSSID : 1E-90-C7-00-00-03(子機のBSSID)	

※数値は、設定例です。



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 > AP間通信 (WBR)

■ 無線AP間通信機能(WBR)を使用する場合

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

アカウントिंग: 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): ●●●●●●●●

WPAキー更新間隔: 120 分

登録 取消

AP-9600の無線AP間通信で使用できる親機側の仮想AP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

※目のアイコン(右端)をクリックすると、入力した内容を確認できます。

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 取消

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

子機のBSSIDを親機側に登録します。

(次ページにつづく)

2 導入ガイド

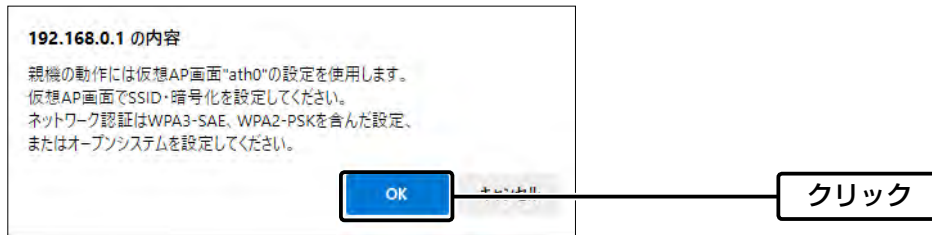
2. 無線LAN接続[活用編]

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

親機を設定する

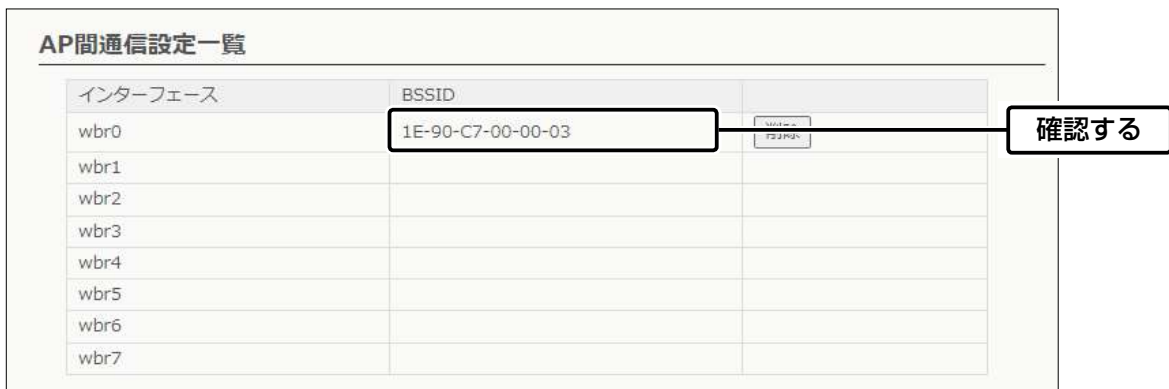
5 <OK>をクリックします。



※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。



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

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: []

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): []

登録 取消

※目のアイコン(右端)をクリックすると、入力した内容を確認できます。

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。

192.168.0.1 の内容

子機に設定すると仮想AP"ath07"は使用できなくなります。
設定してもよろしいですか?

OK キャンセル

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

■ 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 (5GHz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

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

アドレス:

ポート: 1813 1813

シークレット:

① 設定する

※目のアイコン(右端)をクリックすると、入力した内容を確認できます。

登録 取消

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/WPA3/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(5GHz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

アカウントティング: 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:

登録 取消

① 設定する

② クリック

※目のアイコン(右端)をクリックすると、入力した内容を確認できます。

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	3-17
■ 静的DHCPサーバー設定一覧	3-17
「スタティックルーティング」画面	3-18
■ IP経路情報	3-18
■ スタティックルーティング設定	3-19
■ スタティックルーティング設定一覧	3-19
「ポリシールーティング」画面	3-20
■ 送信元ルーティング設定	3-20
■ 送信元ルーティング設定一覧	3-20
「パケットフィルタ」画面	3-21
■ パケットフィルタ設定	3-21
■ パケットフィルタ設定一覧	3-33
パケットフィルタの使用例について	3-34
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	3-35
② AP-9600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	3-36
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	3-37

3 設定画面について

下記は、前ページからの「つづき」です。

ルーター設定

「WAN接続先」画面	3-38
■ 回線状態表示 [DHCPクライアント設定時]	3-38
■ 回線状態表示 [固定IP設定時]	3-39
■ 回線状態表示 [PPPoE設定時]	3-40
■ 回線種別設定	3-41
■ 回線設定 [DHCPクライアント設定時]	3-42
■ 回線設定 [固定IP設定時]	3-43
■ 回線設定 [PPPoE設定時]	3-44
■ 回線設定一覧 [PPPoE設定時]	3-46
「アドレス変換」画面	3-47
■ アドレス変換設定	3-47
■ DMZホスト設定	3-47
■ 静的マスカレードテーブル設定	3-48
■ 静的マスカレードテーブル設定一覧	3-49
「IPフィルター」画面	3-50
■ 一般設定	3-50
■ IPフィルター設定	3-51
■ IPフィルター設定一覧	3-57
「簡易DNS」画面	3-58
■ 簡易DNSサーバー設定	3-58
■ 簡易DNSサーバー設定一覧	3-58
「VPN」画面	3-59
■ IPsec設定	3-59
■ IPsecトンネル設定	3-60
■ IPsecトンネル設定一覧	3-62
■ IPsecトンネル設定例(1)	3-63
■ IPsecトンネル設定例(2)	3-64

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	3-65
■ 無線LAN	3-65
「仮想AP」画面	3-67
■ 仮想AP設定	3-67
■ 暗号化設定	3-70
■ RADIUS設定	3-77
■ アカウンティング設定	3-78
「MACアドレスフィルタリング」画面	3-79
■ MACアドレスフィルタリング設定	3-79
■ 端末MACアドレスリスト	3-80
■ MACアドレスフィルタリング設定一覧	3-81
「AP間通信 (WBR)」画面	3-82
■ AP間通信設定	3-82
■ 親機設定	3-83
■ AP間通信設定一覧	3-84
■ 子機設定	3-85
「WMM詳細」画面	3-88
■ WMM詳細設定	3-88
■ WMMパワーセーブ設定	3-92
「ARP代理応答」画面	3-93
■ ARP代理応答設定	3-93
■ ARPキャッシュ情報	3-94

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	3-95
■ 管理者パスワードの変更	3-95
「管理ツール」画面	3-96
■ USB設定	3-96
■ HTTP/HTTPS設定	3-98
■ HTTP/HTTPS設定後、設定画面にアクセスできなくなったときは	3-99
■ Telnet/SSH設定	3-100
「時計」画面	3-102
■ 時刻設定	3-102
■ 自動時計設定	3-103
「SYSLOG」画面	3-104
■ SYSLOG設定	3-104
「SNMP」画面	3-105
■ SNMP設定	3-105
■ SNMPv3設定	3-106
「LED」画面	3-107
■ LED消灯モード	3-107
「ネットワークテスト」画面	3-108
■ PINGテスト	3-108
■ 経路テスト	3-109
「再起動」画面	3-110
■ 再起動	3-110
「設定の保存/復元」画面	3-111
■ 設定の保存	3-111
■ 設定の復元	3-111
■ 設定内容一覧	3-112
「初期化」画面	3-113
■ 初期化	3-113
「ファームウェアの更新」画面	3-114
■ ファームウェア情報	3-114
■ オンライン更新	3-115
■ 自動更新	3-116
■ 手動更新	3-117

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、時刻、稼働時間、メモリー使用量、PoEステータスが表示されます。

システム情報	
本体名称	AP-9600
バージョン	
国名コード	JP
現在時刻	
稼働時間	
メモリー使用量	296528 kB / 821908 kB (36% 使用中)
PoEステータス	ACアダプター

※上図は、ACアダプターを接続している場合の表示例です。

PoEから受電している場合は、そのPoE規格(IEEE 802.3af、IEEE 802.3at、IEEE 802.3bt)が表示されます。

TOP

■ MACアドレス

本製品のMACアドレス(WAN/LAN/無線)が表示されます。

MACアドレス	
WAN/LAN1	00-90-C7-XXXXXX
LAN2	00-90-C7-XXXXXX
無線LAN1	00-90-C7-XXXXXX
無線LAN2	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

本製品の各ポートについて、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
WAN/LAN1	00-90-C7- <small>XXXXXXXXXX</small>	1000BASE-T full-duplex
LAN2	00-90-C7- <small>XXXXXXXXXX</small>	リンクダウン

※本製品の[WAN/LAN1]ポート、[LAN2]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-.....
ath1	WIRELESSLAN-0	00-90-C7-.....

※[無線LAN]項目の[無線UNIT]欄(P.3-65)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.3-67)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	接続先BSSID
wbr0

※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.3-83)

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られた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
.....	192.168.0.30
.....	192.168.0.11

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。

日付・時間	レベル	内容
01-21 20:47:28	INFO	soc0: IEEE 802.11axg: detected a roaming STA CA-EE-F5-16-19-0E

- ① 表示するレベル** 非表示に設定するとき、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)で絞りこんだ内容を保存します。
※クリックして、表示された画面にしたがって操作すると、ログ情報をテキスト形式(拡張子：txt)で保存できます。
- 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LAN1 36 CH (5180 MHz)	ath0	00-90-C7-██████	WIRELESSLAN-0	WPA2-PSK (AES)
無線LAN2 1 CH (2412 MHz)	ath1	00-90-C7-██████	WIRELESSLAN-0	WPA-PSK/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	██████████	192.168.0.27	53	173.3 Mbps	6.0 Mbps	<input type="button" value="詳細"/>

※仮想APのARP代理応答機能(P.3-93)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:	ath0
MACアドレス:	
IPアドレス:	192.168.0.27
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:	 50
速度:	送信 6.0 Mbps / 受信 173.3 Mbps
WMMパワーセーブ:	無効
接続時間:	0 day 00:00:41

※ [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	接続先BSSID	RSSI	受信速度	送信速度	
wbr8	00-90-C7- 	28	34.4 Mbps	229.4 Mbps	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「wbr8」(無線LAN2))



※ 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：	1E-90-C7- 
通信モード：	IEEE 802.11ax
SSID：	WIRELESSLAN-0
暗号化：	WPA2-PSK (AES)
チャンネル：	1 CH (2412 MHz)
信号レベル：	 28
レート：	送信 34.4 Mbps / 受信 172.1 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 : <input type="text" value="AP-9600"/>

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-9600)
※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 : <input type="text" value="0"/>

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。
※WAN側などのデフォルトゲートウェイが有効になった場合、この欄で設定した経路は無効になります。
- 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。

※ 9、10は [DNS代理応答] 欄を「無効」に設定した場合に表示されません。

DHCPサーバー設定

DHCPサーバー : 1 無効 有効

割り当て開始IPアドレス : 2 _____

割り当て個数 : 3 30 _____ 個

サブネットマスク : 4 _____

リース期間 : 5 72 _____ 時間

ドメイン名 : 6 _____

デフォルトゲートウェイ : 7 _____

DNS代理応答 : 8 無効 有効

プライマリーDNSサーバー : 9 _____

セカンダリーDNSサーバー : 10 _____

プライマリーWINSサーバー : 11 _____

セカンダリーWINSサーバー : 12 _____

13 14
登録 取消

- 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] 欄と [割り当て個数] 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] 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] 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。

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

※⑨、⑩は[DNS代理応答]欄を「無効」に設定した場合に表示されます。

DHCPサーバー設定

DHCPサーバー：① 無効 有効

割り当て開始IPアドレス：② _____

割り当て個数：③ 30 _____ 個

サブネットマスク：④ _____

リース期間：⑤ 72 _____ 時間

ドメイン名：⑥ _____

デフォルトゲートウェイ：⑦ _____

DNS代理応答：⑧ 無効 有効

プライマリDNSサーバー：⑨ _____

セカンダリDNSサーバー：⑩ _____

プライマリWINSサーバー：⑪ _____

セカンダリWINSサーバー：⑫ _____

⑬ 登録 ⑭ 取消

- 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。
- 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。
※[DNS代理応答]欄を「有効」に設定している場合は、この欄と[セカンダリDNSサーバー]欄は表示されず、本製品がプライマリDNSサーバーとして通知されます。
- ⑩ セカンダリDNSサーバー …… [プライマリDNSサーバー]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。

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

※⑨、⑩は[DNS代理応答]欄を「無効」に設定した場合に表示されます。

DHCPサーバー設定

DHCPサーバー：① 無効 有効

割り当て開始IPアドレス：② _____

割り当て個数：③ 30 _____ 個

サブネットマスク：④ _____

リース期間：⑤ 72 _____ 時間

ドメイン名：⑥ _____

デフォルトゲートウェイ：⑦ _____

DNS代理応答：⑧ 無効 有効

プライマリDNSサーバー：⑨ _____

セカンダリDNSサーバー：⑩ _____

プライマリWINSサーバー：⑪ _____

セカンダリWINSサーバー：⑫ _____

⑬ 登録 ⑭ 取消

- ⑪ **プライマリ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WINSサーバー** … [プライマリWINSサーバー]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	
<input type="text"/>	<input type="text"/>	<input type="button" value="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	
<input type="text"/>	192.168.0.50	<input type="button" value="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LANの場合
◎eth0 : インターフェースがWAN側の場合
◎ppp0～ppp7 : インターフェースがWAN側PPPoEの場合
◎vti0～vti31 : インターフェースがIPsec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64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 [経路] 欄で「ゲートウェイを設定」を選択した場合に、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)」、「vti0～vti31」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	
192.168.10.0	255.255.255.0	192.168.0.254		① 編集 ② 削除
127.0.0.0	255.0.0.0	127.0.0.1		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.3-41)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... [経路]欄で「ゲートウェイを設定」を選択した場合に、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 対象となる送信元IPアドレスから送られてきたパケットの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)」、「vti0～vti31」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が表示されます。
※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。

パケットフィルター設定

番号 : ①

エントリー : 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

宛先インターフェース : ⑥

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

⑩ 登録 ⑪ 取消

- 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

パケットフィルター設定

番号 : ① ▼

エントリー : 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 ▼

宛先インターフェース : ⑥ ▼

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 ▼

⑩ 登録 ⑪ 取消

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 : 本製品自身の場合
 - ◎eth0 : 有線LAN(WAN/LAN1)の場合
※「WAN接続先」画面の回線種別(P.3-41)を「LANポートとして使用する」に設定しているときだけ、フィルタリング条件に一致します。
 - ◎eth1 : 有線LAN(LAN2)の場合
 - ◎ath0、ath01～ath07 : 本製品の無線LAN1(5GHz帯仮想AP)の場合
 - ◎ath1、ath11～ath17 : 本製品の無線LAN2(2.4GHz帯仮想AP)の場合
 - ◎wbr0～wbr17 : AP間通信(WBR)の場合
- ※「すべて」を選択すると、「br-lan」、「eth0」、「eth1」、「ath0、ath01～ath07」、「ath1、ath11～ath17」、「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 : 本製品自身の場合
 - ◎eth0 : 有線LAN(WAN/LAN1)の場合
※「WAN接続先」画面の回線種別(P.3-41)を「LANポートとして使用する」に設定しているときだけ、フィルタリング条件に一致します。
 - ◎eth1 : 有線LAN(LAN2)の場合
 - ◎ath0、ath01～ath07 : 本製品の無線LAN1(5GHz帯仮想AP)の場合
 - ◎ath1、ath11～ath17 : 本製品の無線LAN2(2.4GHz帯仮想AP)の場合
 - ◎wbr0～wbr17 : AP間通信(WBR)の場合
- ※「すべて」を選択すると、「br-lan」、「eth0」、「eth1」、「ath0、ath01～ath07」、「ath1、ath11～ath17」、「wbr0～wbr17」が宛先インターフェースの対象になります。

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

パケットフィルター設定

番号: ①

エントリー: 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

宛先インターフェース: ⑥

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

⑩ 登録 ⑪ 取消

- 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]欄(⑧)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。

- 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.3-33)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.3-33)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。

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

8 宛先MACアドレス/マスク(つづき)

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.3-33)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。

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 : 3-25ページ～3-29ページ

◎ARP : 3-30ページ

◎IPv4 : 3-31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

[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パケットについて、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 : 3-26ページ
◎IPv4 : 3-27ページ～3-29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

[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、「0～65535」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、ターゲット 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、ターゲット 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

[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

[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

[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送信元の 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

[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、「0～65535」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、ターゲット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、ターゲット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

[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

[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送信元の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。

番号	項目	詳細	
1	エントリー	無効	① 編集 ② 削除
	ログ出力	有効	
	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	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.3-21)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

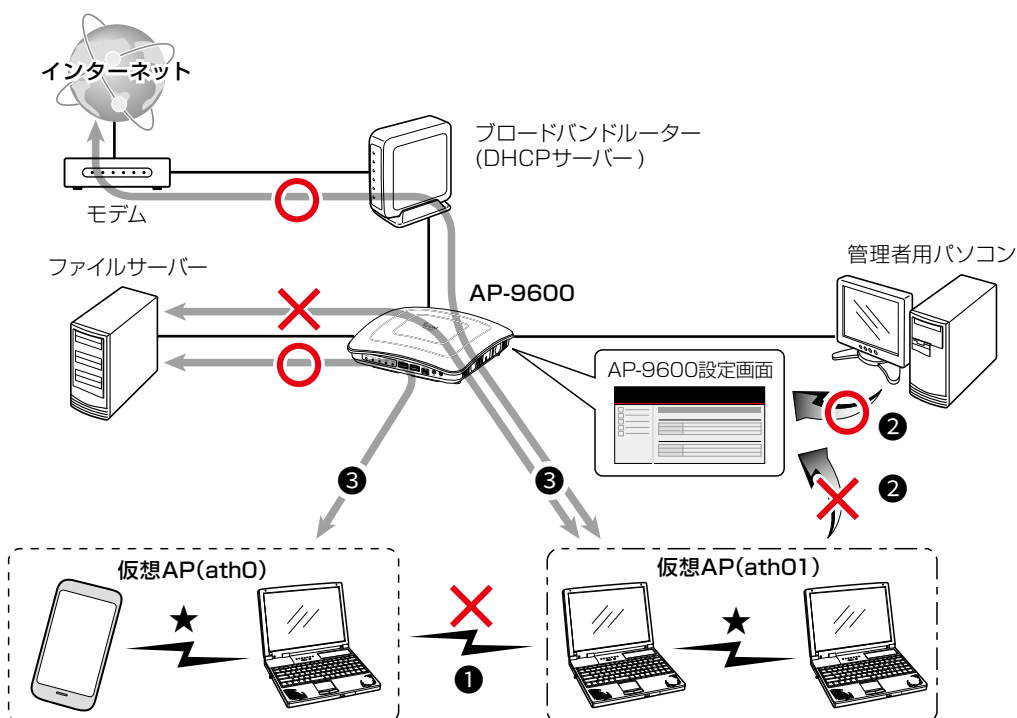
ネットワーク設定 > パケットフィルター

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.3-35)
- ② AP-9600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.3-36)
- 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.3-37)

※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.3-69)

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.3-69)

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」画面で設定したフィルターの番号を表示

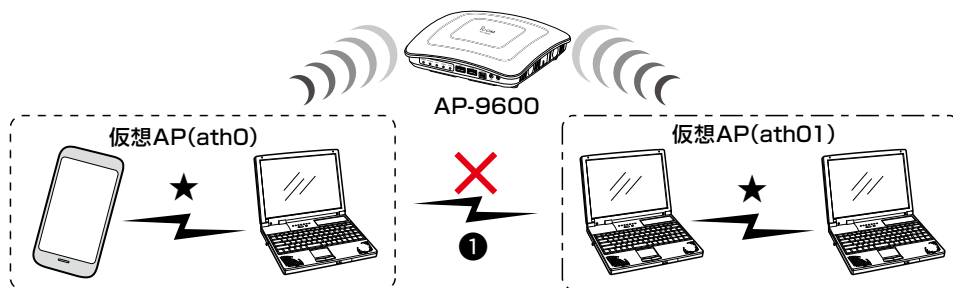
上記のフィルターで登録した番号と異なる番号を表示

番号	項目	詳細	
★	エントリー	有効	
	ログ出力	無効	編集
	フィルター方法	遮断	削除
	送信元インターフェース	ath0	
	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 仮想AP(ath0)→仮想AP(ath01)方向の通信を遮断

番号	項目	詳細	
★	エントリー	有効	
	ログ出力	無効	編集
	フィルター方法	遮断	削除
	送信元インターフェース	ath01	
	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	

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-9600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設定一覧

番号	項目	詳細	
1	エントリー	有効	<div style="display: flex; flex-direction: column; align-items: center;"> <div style="margin-bottom: 10px;">編集</div> <div>削除</div> </div>
	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. /	
	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	

番号	項目	詳細	
2	エントリー	有効	<div style="display: flex; flex-direction: column; align-items: center;"> <div style="margin-bottom: 10px;">編集</div> <div>削除</div> </div>
	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	

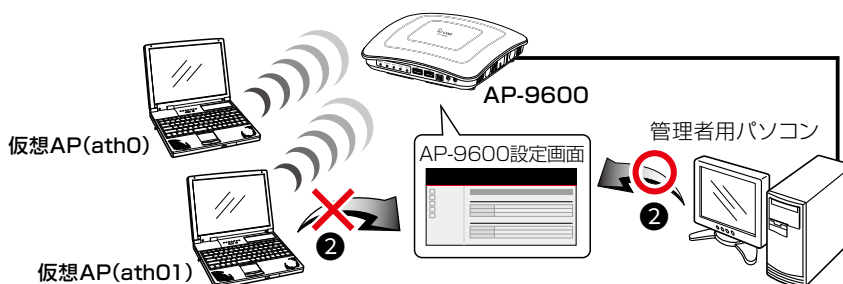
「パケットフィルター」画面で設定したフィルターの番号を表示

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 管理用端末以外からのWEBアクセスを遮断



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

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。

※下記の図は、ブロードバンドルーターを[LAN2]ポートに接続した場合の例です。

[WAN/LAN1]ポートに接続する場合は、送信元インターフェースに「eth0」を指定してください。

パケットフィルター設定一覧

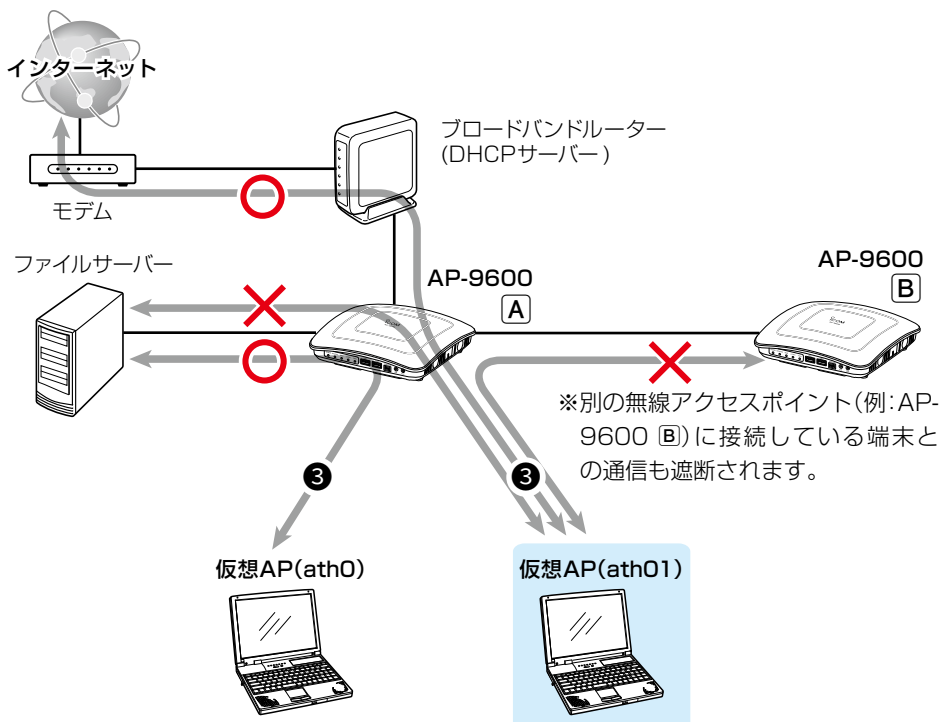
番号	項目	詳細		
1	エントリー	有効	編集 削除	
	ログ出力			
	フィルター方法	透過		
	送信元インターフェース	eth1		
	宛先インターフェース	ath01		
	送信元 MAC アドレス / マスク	-00-00-06 / FF-FF-FF-FF-FF-FF		
	宛先 MAC アドレス / マスク	すべて		
	Ethernet タイプ	すべて		
	エントリー	有効		編集 削除
	ログ出力			
	フィルター方法	遮断		
	送信元インターフェース	すべて		
	宛先インターフェース	ath01		
	送信元 MAC アドレス / マスク	すべて		
	宛先 MAC アドレス / マスク	すべて		
	Ethernet タイプ	すべて		

「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

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

「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.3-41)、[回線設定]項目(P.3-42)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、表示例です。

1 接続状態	接続中
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アドレスを表示します。
- 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
ず。

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.3-41)、[回線設定]項目(P.3-43)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、表示例です。

1 接続状態	接続中
2 回線種別	固定IP
3 本体側のIPアドレス	192.168.1.1
4 相手先のIPアドレス	192.168.1.1
5 DNSサーバー	192.168.1.1

- 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.3-41)、[回線設定]項目(P.3-44)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、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 ▼ 切断	なし ▼ 接続
2 接続状態	接続中	
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.3-44)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

1 回線種別 : 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[WAN/LAN1]ポートをWANポートとして使用できます。
- ◎回線を本製品のWAN側ポートに接続しない場合
LANポートとして使用する
LANポートに切り替わり、HUBやルーターなどのネットワーク機器と接続できます。
- ◎回線を本製品のWAN側ポートに接続する場合
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できます。
- 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.3-41)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

接続先名 : ① _____

プライマリーDNSサーバー : ② _____

セカンダリーDNSサーバー : ③ _____

④ 登録 ⑤ 取消

- 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。
- ③ セカンダリーDNSサーバー [プライマリーDNSサーバー]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、[プライマリーDNSサーバー]欄、[セカンダリー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.3-38)

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.3-41)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

接続先名 : ① _____

IPアドレス : ② _____

サブネットマスク : ③ _____

デフォルトゲートウェイ : ④ _____

プライマリーDNSサーバー : ⑤ _____

セカンダリーDNSサーバー : ⑥ _____

⑦ 登録 ⑧ 取消

- | | |
|-----------------|--|
| 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]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.3-41)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DNSサーバー : ⑦ []

セカンダリ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。
※目のアイコン(右端)をクリックすると、入力したパスワードを確認できます。
- 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.3-40)
※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.3-40)
- 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 [REDACTED]

パスワード : ④ [REDACTED] [目隠しアイコン]

接続方法 : ⑤ 常時 ▼

IPアドレス : ⑥

プライマリDNSサーバー : ⑦

セカンダリ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] [12]

[登録] [取消]

- ⑦ **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。
- ⑧ **セカンダリDNSサーバー** …… [プライマリDNSサーバー]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」(出荷時の設定)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。

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 [REDACTED]

パスワード : ④ [REDACTED] 👁

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

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。

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.3-44)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)	[REDACTED]	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。

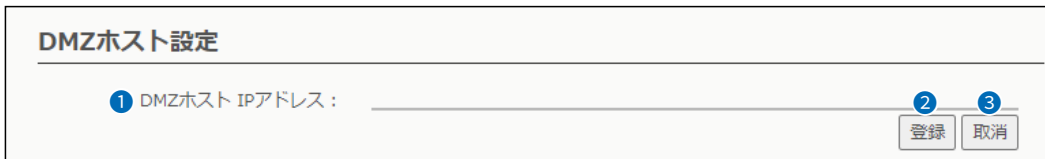


アドレス変換…………… 本製品のアドレス変換機能を設定します。 (出荷時の設定：有効)
「有効」に設定すると、本製品のIPマスカレード機能を使用して、WAN側グローバルアドレスをプライベートアドレスに変換します。

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。



- 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パケットを、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	
<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP ▼	追加 ⑤

- ① WAN側ポート 選択したプロトコル(④)に対するWAN側ポート番号を入力します。
- 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側ポート番号を入力します。
- 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。

3 設定画面について

「アドレス変換」画面

ルーター設定 > アドレス変更

■ 静的マスカレードテーブル設定一覧

[静的マスカレードテーブル設定]項目で登録した内容を表示します。

※画面の内容は、設定例です。

WAN側ポート	LAN側IP	LAN側ポート	プロトコル	①	②
11	192.168.0.10	4011	TCP	編集	削除
22	192.168.0.10	8022	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 <取消> 「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。

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：無効)
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	* (*)	無効	編集	削除
	IN		* (*)			

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 1

エントリー: ② 無効 有効

フィルター方法: ③ 遮断 透過

フィルター方向: ④ IN OUT

送信元IPアドレス: ⑤ _____ マスク: 32

宛先IPアドレス: ⑥ _____ マスク: 32

プロトコル: ⑦ TCP 指定時: _____

送信元ポート番号: ⑧ _____ ~ _____

宛先ポート番号: ⑨ _____ ~ _____

SYSLOGに出力: ⑩ 無効 有効

⑪ 登録 ⑫ 取消

- 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。
- 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。

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 1

エントリー: ② 無効 有効

フィルター方法: ③ 遮断 透過

フィルター方向: ④ IN OUT

送信元IPアドレス: ⑤ _____ マスク: 32

宛先IPアドレス: ⑥ _____ マスク: 32

プロトコル: ⑦ TCP

送信元ポート番号: ⑧ _____ ~ _____

宛先ポート番号: ⑨ _____ ~ _____

SYSLOGに出力: ⑩ 無効 有効

⑪ 登録 ⑫ 取消

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。

IPフィルター設定

番号: ① 1

エントリー: ② 無効 有効

フィルター方法: ③ 遮断 透過

フィルター方向: ④ IN OUT

送信元IPアドレス: ⑤ _____ マスク: 32

宛先IPアドレス: ⑥ _____ マスク: 32

プロトコル: ⑦ TCP

送信元ポート番号: ⑧ _____ ~ _____

宛先ポート番号: ⑨ _____ ~ _____

SYSLOGに出力: ⑩ 無効 有効

登録 取消

⑦ プロトコル(つづき) 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。

プロトコル: ICMP

タイプ: _____

コード: _____

指定時: _____

[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送信元のTCP/UDPポート番号を指定する項目です。
(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。

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。
(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。

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 1

エントリー: ② 無効 有効

フィルター方法: ③ 遮断 透過

フィルター方向: ④ IN OUT

送信元IPアドレス: ⑤ _____ マスク: 32

宛先IPアドレス: ⑥ _____ マスク: 32

プロトコル: ⑦ TCP

送信元ポート番号: ⑧ _____ ~ _____

宛先ポート番号: ⑨ _____ ~ _____

SYSLOGに出力: ⑩ 無効 有効

⑪ 登録 ⑫ 取消

- ⑩ **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。
- ⑪ **〈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。
- ⑫ **〈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.3-51～P.3-56)から登録した現在の各エントリーの内容を表示します。

番号	フィルター方法 フィルター方向	プロトコル	送信元IPアドレス (送信元ポート番号) 宛先IPアドレス (宛先ポート番号)	SYSLOGに出力	① 編集	② 削除
59	遮断	TCP/UDP	* (135)	無効	編集	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	* (*)	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、表示された内容を[IPフィルター設定]項目の各欄に表示します。
- 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
<input type="text"/>	<input type="text"/>
<input type="button" value="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」を登録しておくこと、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サーバー設定一覧

[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	<input type="text"/>
<input type="button" value="削除"/>	

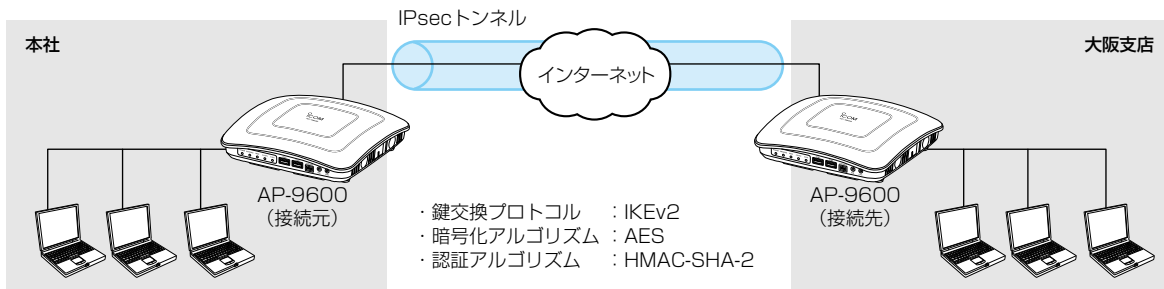
登録した内容を取り消すときは、該当する欄の〈削除〉をクリックします。

3 設定画面について

「VPN」画面

VPN(Virtual Private Network)機能を使用すると、インターネット上の2地点を暗号化通信で接続して、仮想的なネットワークを構成できます。

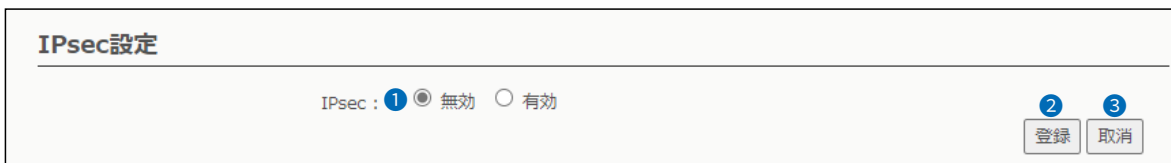
※本製品のVPN機能は、AP-9500、SR-7100VN、SR-8000V、VE-PG4と互換性があります。(2023年4月現在)
※接続先に合わせて、IPsecトンネルを登録してください。(P.3-63、P.3-64)



ルーター設定 > VPN

■ IPsec設定

IPsecによる仮想プライベートネットワーク(VPN)接続を使用するための設定です。

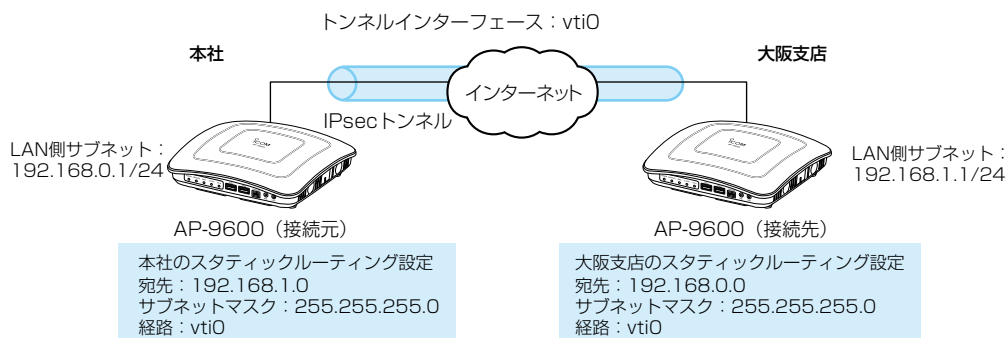


- ① IPsec..... 本製品のIPsec機能を設定します。 (出荷時の設定：無効)
「有効」に設定すると、IPsecトンネルを使用したVPN接続を利用できます。
- ② <登録> 「IPsec設定」項目で設定した内容を登録するボタンです。
- ③ <取消> 「IPsec設定」項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお、<登録>をクリックすると、変更前の状態には戻りません。

ご参考

VPN機能を使用する場合は、本製品の[WAN/LAN1]ポートにWAN回線を接続し、ルーター機能(回線種別)、スタティックルーティングの設定(P.3-19)が必要です。

スタティックルーティングの設定例



3 設定画面について

「VPN」画面

ルーター設定 > VPN

■ IPsecトンネル設定

IPsecによる仮想プライベートネットワーク(VPN)接続を使用するための設定です。

IPsecトンネル設定

トンネルインターフェース: ① vti0

トンネル: ② 無効 有効

トンネル名: ③

インターフェース: ④ eth0

認証鍵 (Pre-Shared Key): ⑤

リモートアドレス: ⑥

リモートID: ⑦ IPアドレス

ローカルID: ⑧ IPアドレス

登録 取消

- ① **トンネルインターフェース** …… IPsecトンネルを登録するインターフェースを指定します。
(出荷時の設定：vti0)
選択できる範囲は「vti0～vti31」です。
- ② **トンネル** …… 登録するIPsecトンネル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。
- ③ **トンネル名** …… IPsecトンネルを識別する名称を半角31(全角31)文字以内で入力します。
- ④ **インターフェース** …… 接続先と通信するインターフェースを選択します。(出荷時の設定：eth0)
◎eth0
「WAN接続先」画面の回線種別(P.3-41)を「固定IP」、または「DHCPクライアント」に設定しているときに選択します。
◎ppp0(WAN1)～ppp7(WAN8)
「WAN接続先」画面の回線種別(P.3-41)を「PPPoE」に設定しているときに選択します。
- ⑤ **認証鍵(Pre-Shared Key)** …… 接続先との認証に使用します。
接続先の機器と同じ文字列を半角128文字以内の英数字で入力します。
※目のアイコン(右端)をクリックすると、入力した内容を確認できます。
- ⑥ **リモートアドレス** …… 接続先のWAN側IPアドレス、またはホスト名を入力します。
※接続先からのIPsec接続を待ち受ける場合は、[リモートアドレス]欄を空白のままにして登録します。
双方の機器に割り当てられたWAN側IPアドレスが動的の場合、どちらか一方がダイナミックDNSサービスに登録し、ホスト名を取得している必要があります。

3 設定画面について

「VPN」画面

ルーター設定 > VPN

■ IPsecトンネル設定

IPsecトンネル設定

トンネルインターフェース: ① vti0

トンネル: ② 無効 有効

トンネル名: ③

インターフェース: ④ eth0

認証鍵 (Pre-Shared Key): ⑤

リモートアドレス: ⑥

リモートID: ⑦ IPアドレス

ローカルID: ⑧ IPアドレス

⑨ 登録 ⑩ 取消

- ⑦ リモートID** 接続先の機器を識別するIDを設定します。
IDは、「IPアドレス」、「KEYID」、「FQDN」、「USER-FQDN」からタイプを選択します。
(出荷時の設定：IPアドレス)
 - ◎IPアドレス : IPアドレス形式
 - ◎KEYID : 半角256文字以内の英数字
 - ◎FQDN : 半角253文字以内のドメイン名
 - ◎USER-FQDN : 半角254文字以内のメールアドレス形式
入力例：user@xxxx.yyyy.zzzz
① 64文字以内
② 「xxxx」、「yyyy」、「zzzz」は、それぞれ63文字以内
- ⑧ ローカルID** 接続先の機器に提示するIDを設定します。
IDは、「IPアドレス」、「KEYID」、「FQDN」、「USER-FQDN」からタイプを選択します。
(出荷時の設定：IPアドレス)
 - ◎IPアドレス : IPアドレス形式
 - ◎KEYID : 半角256文字以内の英数字
 - ◎FQDN : 半角253文字以内のドメイン名
 - ◎USER-FQDN : 半角254文字以内のメールアドレス形式
入力例：user@xxxx.yyyy.zzzz
① 64文字以内
② 「xxxx」、「yyyy」、「zzzz」は、それぞれ63文字以内
- ⑨ <登録>** 「IPsecトンネル設定」項目で設定した内容を登録するボタンです。
- ⑩ <取消>** 「IPsecトンネル設定」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

「VPN」画面

ルーター設定 > VPN

■ IPsecトンネル設定一覧

IPsecによる仮想プライベートネットワーク(VPN)接続を使用するための設定です。

1 トンネルインターフェース	2 インターフェース	3 状態	4 リモートアドレス	5 リモートID	6 ローカルID	7	8
vti0	eth0	IPsec無効		IPアドレス	IPアドレス	編集	削除

- ① トンネルインターフェース …… インターフェース名(トンネル名)が表示されます。
- ② インターフェース …………… トンネル送信元のインターフェース名が表示されます。
- ③ 状態 …………… IPsec接続の状態が表示されます。
 - 接続中
IPsecトンネルが接続されている状態です。
 - 接続待機中
トンネルの接続先からのIPsec接続試行を待っている状態です。
 - 接続試行中
トンネルの接続先に対してIPsec接続試行を実行中です。
 - IPsec無効
IPsec設定のIPsecが無効化されている状態です。
 - 無効
IPsecトンネルが無効化されている状態です。
- ④ リモートアドレス …………… 接続先に設定されている相手先IPアドレス、またはホスト名が表示されます。設定されていない場合は「-」が表示されます。接続中は相手先IPアドレスが表示されます。
- ⑤ リモートID …………… IPsec接続に使用するID(相手側)が表示されます。
- ⑥ ローカルID …………… IPsec接続に使用するID(自分側)が表示されます。
- ⑦ 〈編集〉 …………… ボタンの左側に表示されたIPsecトンネルを編集するボタンです。〈編集〉をクリックすると、表示された内容を含むIPsecトンネルの設定が、[IPsecトンネル設定]項目の各欄に表示されます。
- ⑧ 〈削除〉 …………… ボタンの左側に表示されたIPsecトンネルを削除するボタンです。

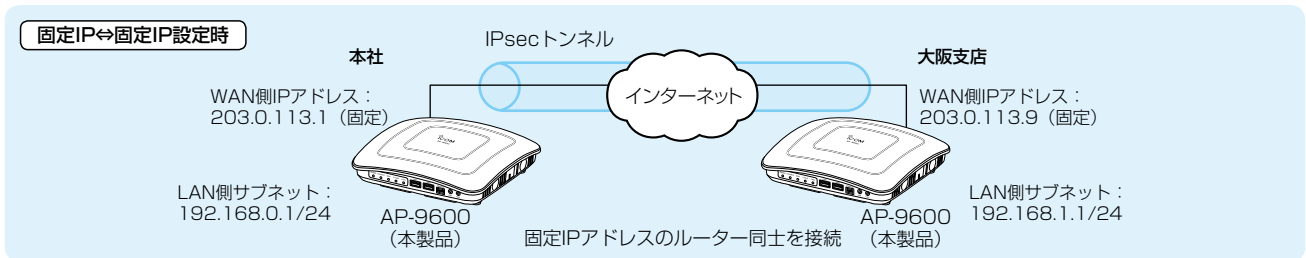
3 設定画面について

「VPN」画面

ルーター設定 > VPN

■ IPsecトンネル設定例(1)

本製品、接続先ともに、WAN側IPアドレスが固定で割り当てられ、回線種別がPPPoEの場合



※IPsecトンネルへの経路設定(スタティックルーティング)も必要です。(P.3-19、P.3-59)

本社側

IPsec設定

IPsec : 無効 有効

登録 取消

IPsecトンネル設定

トンネルインターフェース : vti0

トンネル : 無効 有効

トンネル名 : 大阪支店

インターフェース : ppp0 (WAN01)

認証鍵 (Pre-Shared Key) : ●●●●

リモートアドレス :

リモートID : KEYID ▼ osaka

ローカルID : KEYID ▼ honsha

登録 取消

認証鍵 (Pre-Shared Key) は、接続する機器同士で同じ文字列を入力します。

リモートIDには、接続先(大阪支店)のローカルIDを入力します。

「WAN接続先」画面で設定した接続先(PPPoE)を選択します。

リモートアドレスには、接続先(大阪支店)のWAN側IPアドレスを入力します。

大阪支店側

IPsec設定

IPsec : 無効 有効

登録 取消

IPsecトンネル設定

トンネルインターフェース : vti0

トンネル : 無効 有効

トンネル名 : 本社

インターフェース : ppp0 (WAN01)

認証鍵 (Pre-Shared Key) : ●●●●

リモートアドレス : 203.0.113.1

リモートID : KEYID ▼ honsha

ローカルID : KEYID ▼ osaka

登録 取消

リモートIDには、接続先(本社)のローカルIDを入力します。

リモートアドレスには、接続先(本社)のWAN側IPアドレスを入力します。

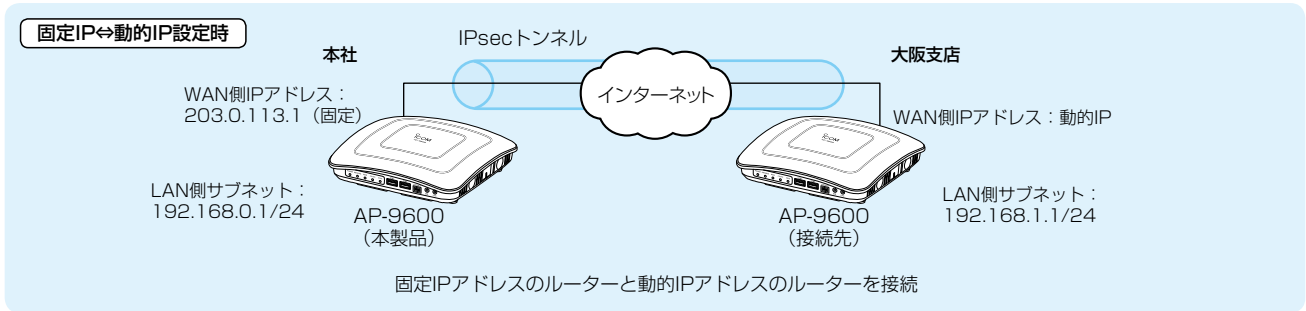
3 設定画面について

「VPN」画面

ルーター設定 > VPN

■ IPsecトンネル設定例(2)

本製品のWAN側IPアドレスが固定、接続先のWAN側IPアドレスが動的で割り当てられ、回線種別は本製品、接続先ともにPPPoEの場合



※IPsecトンネルへの経路設定(スタティックルーティング)も必要です。(P.3-19、P.3-59)

本社側

IPsec設定

IPsec : 無効 有効

登録 取消

IPsecトンネル設定

トンネルインターフェース : vti0

トンネル : 無効 有効

トンネル名 : 大阪支店

インターフェース : ppp0 (WAN01)

認証鍵 (Pre-Shared Key) : ●●●●

リモートアドレス : ●●●●

リモートID : KEYID ▼ osaka

ローカルID : KEYID ▼ honsha

登録 取消

「WAN接続先」画面で設定した接続先(PPPoE)を選択します。

接続先(大阪支店)のリモートアドレスを省略した場合、接続先からIPsec接続を開始する必要があります。 ※空欄にすると待機状態になり、自らIPsec接続を開始しません。

認証鍵 (Pre-Shared Key) は、接続する機器同士で同じ文字列を入力します。

リモートIDには、接続先(大阪支店)のローカルIDを入力します。

大阪支店側

IPsec設定

IPsec : 無効 有効

登録 取消

IPsecトンネル設定

トンネルインターフェース : vti0

トンネル : 無効 有効

トンネル名 : 本社

インターフェース : ppp0 (WAN01)

認証鍵 (Pre-Shared Key) : ●●●●

リモートアドレス : 203.0.113.1

リモートID : KEYID ▼ honsha

ローカルID : KEYID ▼ osaka

登録 取消

接続先(本社)のWAN側IPアドレスを、リモートアドレスに入力します。

リモートIDには、接続先(本社)のローカルIDを入力します。

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LAN1：5GHz帯

◎無線LAN2：2.4GHz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 : ③ 036 CH (5180 MHz)

パワーレベル : ④ 高

DTIM間隔 : ⑤ 1

登録 取消

⑥ ⑦

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：無効)
「有効」に設定すると、本製品の無線LAN機能を使用できます。(P.2-2)

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」、「80MHz」から選択できます。
◎無線LAN2：「20MHz」、「40MHz」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→036CH (5180MHz)
無線LAN2→001CH (2412MHz))
※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、5-3ページをご覧ください。
※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。
※5.3/5.6GHz帯のチャンネル選択時のDFS機能については、1-12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

※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 : ③ 036 CH (5180 MHz)

パワーレベル : ④ 高

DTIM間隔 : ⑤ 1

登録 取消

⑥ ⑦

- 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 **〈登録〉** …………… 「無線LAN」画面で設定した内容を登録するボタンです。
- ⑦ **〈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LAN1：5GHz帯

◎無線LAN2：2.4GHz帯

※本書では、「無線LAN1」の画面で説明しています。

※説明のため、[アカウントング](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。

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

アカウントング：⑧ 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。
※「ath0」～「ath07」、「ath11」～「ath17」を使用するときは、[仮想AP]欄を「有効」にしてください。
※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]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。
※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

※本書では、「無線LAN1」の画面で説明しています。

※説明のため、[アカウントング] (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。

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

アカウントング: ⑧ 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))

※[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

※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。

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

アカウントिंग: ⑧ 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、出荷時の設定で使用される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.3-21)で設定できます。
- ⑧ アカウントिंग [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トिंग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、アカウントिंगサーバーの設定が必要です。 (P.3-78)

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.3-73～P.3-75)

暗号化設定	
ネットワーク認証 : ①	オープンシステム ▼
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)

※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」、「WPA2」、「WPA3」、「WPA3 192-bit」、「WPA/WPA2」、「WPA2/WPA3」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

WPA/WPA2/WPA3-Enterprise

◎WPA3 192-bit

ネットワーク認証方式にWPA3 192-bitを使用します。

※「WPA3」認証より強力なCNSA準拠の暗号化方式を使用する認証方式です。

※「WPA3 192-bit」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。

◎WPA3

ネットワーク認証方式にWPA3を使用します。

無線LAN通信の管理フレームを暗号化して盗聴やなりすましを防止します。

※「WPA3」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。

◎WPA2/WPA3

「WPA2」認証と「WPA3」認証を自動認識します。

◎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.3-73～P.3-75)

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

① ネットワーク認証(つづき) ……

WPA/WPA2/WPA3-Personal

◎WPA3-SAE

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「AES」暗号化の認証方式で、SAEのハンドシェイクを利用して、通信相手と暗号鍵(キー)を交換し、認証をします。

◎WPA2-PSK/WPA3-SAE

ネットワーク認証(WPA2-PSK/WPA3-SAE)を自動認識します。

◎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「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。

その他

◎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。

◎オープンシステム

ネットワーク認証をしません。

◎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。

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.3-73～P.3-75)

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

- 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ありませんので、暗号化方式とビット数は、
通信をする相手間で同じ設定にしてください。
※IEEE802.11ax規格、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

◎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、その他(IEEE802.1X、オープンシステム、
オープンシステム/共有キー)以外を選択したとき使用できます。

◎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/WPA2」、または「WPA-PSK/
WPA2-PSK」を選択したとき使用できます。

◎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)ビットの中から選択でき
ます。

※[ネットワーク認証](①)欄で、その他(IEEE802.1X、オープンシステム、
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。

◎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、その他(オープンシステム、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。

※暗号化を設定されることをおすすめします。

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(⑤～⑦)が表示されます。(P.3-75～P.3-76)

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

③ キージェネレーター

[暗号化方式](②)欄(P.3-72)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」、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)」を選択します。
 - [キージェネレーター]欄と[WEPキー](④)欄(P.3-74)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ありませんので、ご注意ください。

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

※[WEPキー]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。

※目のアイコン(右端)をクリックすると、生成された内容を確認できます。

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(⑤～⑦)が表示されます。(P.3-75～P.3-76)

暗号化設定	
ネットワーク認証 : ①	オープンシステム ▼
暗号化方式 : ②	WEP RC4 64 (40) ▼
キージェネレーター : ③	👁
WEPキー : ④	●●●●●● ●●●●●● 👁
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桁の入力例：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。
 - ※ 目のアイコン(右端)をクリックすると、入力内容を確認できます。

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、④、⑦)が表示されます。(P.3-73～P.3-76)

暗号化設定	
ネットワーク認証 : ①	WPA2-PSK/WPA3-SAE ▼
暗号化方式 : ②	AES ▼
PSK (Pre-Shared Key) : ⑤	●●●●●●●● ●
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/WPA2/WPA3-Personal(WPA3-SAE、WPA2-PSK/WPA3-SAE、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。

※ WPA3-SAEの場合は8～64文字、WPA2-PSK/WPA3-SAEの場合は8～63文字を入力してください。

※ WPA2-PSKとWPA-PSK/WPA2-PSKの場合は、16進数で設定するときは64桁、ASCII文字で設定するときは、8～63文字を入力してください。

※ 目のアイコン(右端)をクリックすると、入力内容を確認できます。

⑥ WPAキー更新間隔 ……………

[ネットワーク認証](①)欄で、その他(IEEE802.1X、オープンシステム、オープンシステム/共有キー)以外を選択したとき、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

※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.3-73～P.3-75)

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、ネットワーク認証を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、「WPA3 192-bit」、「WPA3」、「WPA2/WPA3」、「WPA2」、「WPA/WPA2」、「IEEE802.1X」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	
① プライマリー	セカンダリー
アドレス : ②	_____
ポート : ③	1812
シークレット : ④	●●●●● ●●●●●

- 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。
※目のアイコン(右端)をクリックすると、入力内容を確認できます。

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

■ 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。

- 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。
※目のアイコン(右端)をクリックすると、入力内容を確認できます。
- 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。

- 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。

※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、[MACアドレスフィルタリング設定]項目と[MACアドレスフィルタリング設定一覧]項目に登録された内容が更新されません。

更新されないときは、ご使用のWWWブラウザで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 **MACアドレスフィルタリング** …… [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]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 :	<input type="text"/> <input type="button" value="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

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

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


「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] (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。



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。 (出荷時の設定：無効)
「有効」に設定すると、本製品のAP間通信を使用できます。
- 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。

※「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。

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)
※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。

インターフェース	接続先BSSID	
wbr0		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。

※選択する設定内容(④、⑤)に応じて、下記以外の設定(⑥)が表示されません。(P.3-87)

- 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。
※「無線LAN」項目の[無線UNIT]欄(P.3-65)を「無効」に設定しているときは、[BSSID]が表示されません。
- 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 [仮想AP設定]項目で設定したSSIDが表示されます。
- 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)

認証方式について

◎ WPA3-SAE

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「AES」暗号化の認証方式で、SAEのハンドシェイクを利用して、通信相手と暗号鍵(キー)を交換し、認証をします。

◎ WPA2-PSK/WPA3-SAE

ネットワーク認証(WPA2-PSK/WPA3-SAE)を自動認識します。

◎ 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「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。

◎ オープンシステム

ネットワーク認証をしません。

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)

■ 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)が表示されます。(P.3-87)

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

暗号化方式 : ⑤ なし

登録 取消

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、「AES」です。

暗号化方式について

◎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、「オープンシステム」以外を選択したとき使用できます。

◎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」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。

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

子機設定

BSSID : ① [REDACTED]

インターフェース : ② wbr16

SSID : ③ WIRELESSLAN-0

ネットワーク認証 : ④ WPA3-SAE

暗号化方式 : ⑤ AES

PSK (Pre-Shared Key) : ⑥ [REDACTED]

⑦ 登録 ⑧ 取消

- ⑥ 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、「オープンシステム」以外を選択したとき、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。
※ WPA3-SAEの場合は8～64文字、WPA2-PSK/WPA3-SAEの場合は8～63文字を入力してください。
※ WPA2-PSKの場合は、16進数で設定するときは64桁、ASCII文字で設定するときは、8～63文字を入力してください。
※ 目のアイコン(右端)をクリックすると、入力内容を確認できます。
- ⑦ <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。
- ⑧ <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。

WMM詳細設定

周波数帯： 5 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	<input type="checkbox"/>
AC_BE	15	63	3	0	<input type="checkbox"/>
AC_VI	7	15	1	94	<input type="checkbox"/>
AC_VO	3	7	1	47	<input type="checkbox"/>

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	<input type="checkbox"/>
AC_VO	3	7	2	47	<input type="checkbox"/>

- 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

WMM詳細設定

周波数帯： 5 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	<input type="checkbox"/>
AC_BE	15	63	3	0	<input type="checkbox"/>
AC_VI	7	15	1	94	<input type="checkbox"/>
AC_VO	3	7	1	47	<input type="checkbox"/>

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	<input type="checkbox"/>
AC_VO	3	7	2	47	<input type="checkbox"/>

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

WMM詳細設定

周波数帯： 5 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	<input type="checkbox"/>
AC_BE	15	63	3	0	<input type="checkbox"/>
AC_VI	7	15	1	94	<input type="checkbox"/>
AC_VO	3	7	1	47	<input type="checkbox"/>

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	<input type="checkbox"/>
AC_VO	3	7	2	47	<input type="checkbox"/>

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

WMM詳細設定

周波数帯： 5 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	<input type="checkbox"/>
AC_BE	15	63	3	0	<input type="checkbox"/>
AC_VI	7	15	1	94	<input type="checkbox"/>
AC_VO	3	7	1	47	<input type="checkbox"/>

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	<input type="checkbox"/>
AC_VO	3	7	2	47	<input type="checkbox"/>

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。 (出荷時の設定：無効)
「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。 |
| 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

「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。

ARP代理応答設定

インターフェース : ① ath0

ARP代理応答 : ② 無効 有効

不明なARPの透過 : ③ 無効 有効

ARPエージング時間 : ④ 0 分

⑤ 登録 ⑥ 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)
- ② ARP代理応答 [インターフェース]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]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。
- 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。

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

ARP代理応答設定

インターフェース：① ath0

ARP代理応答：② 無効 有効

不明なARPの透過：③ 無効 有効

ARPエージング時間：④ 0 分

⑤ 登録 ⑥ 取消

- 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。

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

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

「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。
※目のアイコン(右端)をクリックすると、入力したパスワードを確認できます。
- 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。
- ⑤ <登録> 「管理者パスワードの変更」項目で設定した内容を登録するボタンです。
- ⑥ <取消> 「管理者パスワードの変更」項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお、<登録>をクリックすると、変更前の状態には戻りません。

不正アクセス防止のアドバイス

本製品に設定するすべてのパスワードは、容易に推測されないものにしてください。
数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた長く複雑なものに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

■ USB設定

市販のUSBデバイス(USBメモリー)を本製品のUSBポートに差し込んだときの動作を設定します。

※[最大出力電流(USB1)]/[最大出力電流(USB2)](①)欄の両方を「オフ」に設定すると、②～⑤は表示されません。

USB設定

最大出力電流 (USB1) : ① オフ 500 mA 900 mA

最大出力電流 (USB2) : オフ 500 mA 900 mA

USBメモリー : ② 無効 有効

USBアクセス許可 : ③ ファームウェアの更新
 設定の保存/復元

USB認証キー : ④ _____

USB認証キーの書き込み : ⑤

① 最大出力電流(USB1)/(USB2)

.....

USBポートの最大出力電流を設定します。

(出荷時の設定：500mA(USB1)/500mA(USB2))

※「オフ」に設定されていると、USBデバイスを差し込んでも使用できません。

※電源供給がIEEE802.3at規格の場合、[USB1]ポートの最大出力電流が500mAに制限され、[USB2]ポートは使用できなくなります。

② USBメモリー

.....

USBメモリーを本製品のUSBポートに差し込んだときの動作について設定します。
(出荷時の設定：有効)

※「無効」に設定されていると、本製品のファームウェアファイルや設定ファイルなどを保存したUSBメモリーを差し込んでも、ファイルを読み込みません。

③ USBアクセス許可

.....

本製品に接続されたUSBメモリーから読み込むファイルを選択します。

(出荷時の設定： ファームウェアの更新

設定の保存/復元)

※チェックマーク[]をはずすと、ファイルを保存したUSBメモリーを差し込んだ状態で<USB>ボタンを短く押しても、該当ファイルを読み込みません。

◎ファームウェアの更新(P.4-15)

本製品のファームウェアファイル(拡張子：dat)を保存したUSBメモリーを差し込んで<USB>ボタンを短く押すと、ファームウェアを更新します。

◎設定の保存/復元(P.4-13)

本製品の設定ファイルをUSBメモリーに保存後、設定が異なる本製品にUSBメモリーを差し込んで<USB>ボタンを短く押すと、自動で設定を復元します。

3 設定画面について

「管理ツール」画面

管理 > 管理ツール

■ USB設定

USB設定

最大出力電流 (USB1) : オフ 500 mA 900 mA

最大出力電流 (USB2) : オフ 500 mA 900 mA

USBメモリー : 無効 有効

USBアクセス許可 : ファームウェアの更新
 設定の保存/復元

USB認証キー :

USB認証キーの書き込み:

④ **USB認証キー** …………… 本製品のUSBポートに差し込んだUSBメモリーへのファイルの読み込みと書き出しに対するUSB認証キーを設定します。
大文字/小文字の区別に注意して、64文字以内(任意の半角英数字/記号)で入力します。
※入力後、「管理ツール」画面の〈登録〉をクリックすると、本製品にUSB認証キーが設定されます。
※本製品にUSB認証キーを設定すると、本製品からUSBメモリーに書き込んだUSB認証キーと同じかどうかを認証します。

⑤ **USB認証キーの書き込み** ……… 本製品に設定されているUSB認証キーを本製品のUSBポートに差し込んだUSBメモリーへ書き込むボタンです。
〈書き込み〉をクリックして、表示される画面にしたがって操作してください。

USB認証キーを保存したUSBメモリーを差し込んでいる場合は、「既に認証キーが書き込まれています。上書きする場合は「進む」ボタンをクリックしてください。」が表示されます。

USB認証キーの書き込み

USBメモリーに認証キーを書き込みます。
USBメモリーを本体に装着し、準備ができたなら「進む」ボタンをクリックしてください。



USB認証キーの書き込み

認証キーの書き込みが完了しました。

※下記の画面が表示されたときは、〈OK〉をクリックして画面を閉じ、「管理ツール」画面の〈登録〉をクリックしてください。

192.168.0.1 の内容

USB認証キーが変更されています。
変更を登録してから、書き込みを行なってください。

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

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

HTTPS : ③ 無効 有効

HTTPSポート番号 : ④

- 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

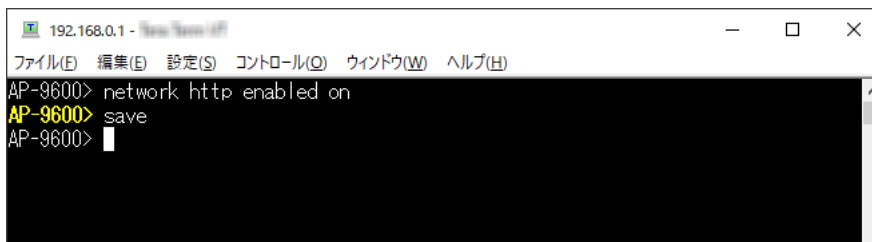
管理 > 管理ツール

■ 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-9600>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.3-100)

- ① AP-9600> **network http enabled on** と入力し[Enter]キーを押します。
- ② AP-9600> **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。



```
192.168.0.1 - New Term 0/0
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)
AP-9600> network http enabled on
AP-9600> save
AP-9600> 
```

※本製品の[CONSOLE]ポートとパソコンの[USB]ポートを市販のUSBケーブル(Type-C)で接続すると、上記と同様にターミナルソフトウェアから設定できます。(P.5-6)

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。

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

- 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]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

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 2023/1/23 21:23

設定する時刻 : ② 2023 年 03 月 31 日 13 時 20 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] 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

⑤ 登録 ⑥ 取消

- 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サーバーに日時の間い合わせをして、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]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。
- ⑤ <登録> [自動時計設定]項目で設定した内容を登録するボタンです。
- ⑥ <取消> [自動時計設定]項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお、<登録>をクリックすると、変更前の状態には戻りません。

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サーバーに日時の間い合わせをして、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サーバーに日時の間い合わせをします。

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、WAN側をインターネットに接続する、またはNTPサーバーへの間い合わせ先(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、間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

「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。

- 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。 (出荷時の設定：有効)
「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。
- 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。

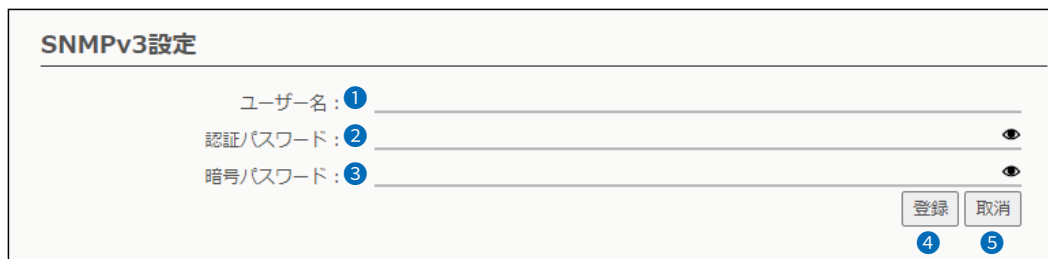
3 設定画面について

「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時の設定です。



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。
※目のアイコン(右端)をクリックすると、入力したパスワードを確認できます。
- 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。
※目のアイコン(右端)をクリックすると、入力したパスワードを確認できます。
- 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。

- 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 : LED消灯モードを使用して、[POWER]ランプを減灯するとき
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、[POWER]ランプの明るさが暗くなります。
同時に、[POWER]以外のランプは、本製品の使用中でも消灯状態になります。
- 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。
- ※USBメモリー(市販品)を差し込んだ状態では、LED消灯モードは動作しません。
- ※〈MODE〉ボタン、〈FUNC〉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」、「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。

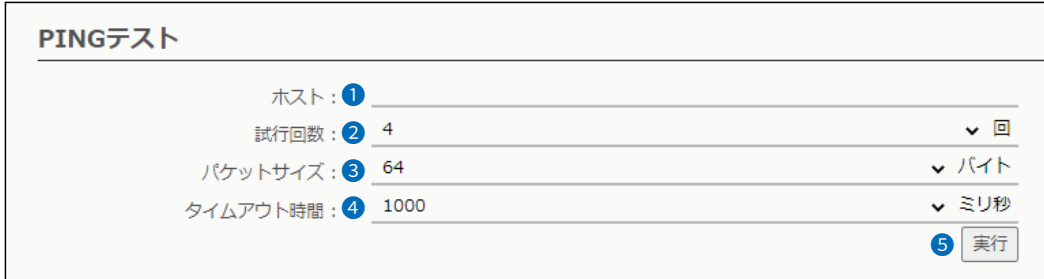
3 設定画面について

「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

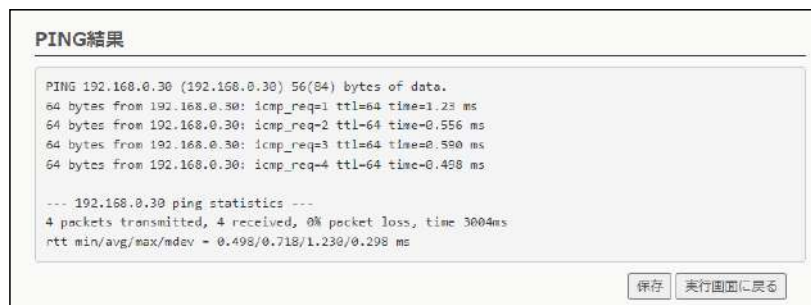
パケットサイズ : ③ 64 ▼ バイト

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。
クリックして、表示される画面にしたがって操作すると、「PING結果」表示に切り替わり、テスト結果を表示します。

PING結果について



PING結果

```
PING 192.168.0.30 (192.168.0.30) 56(64) bytes of data:
64 bytes from 192.168.0.30: icmp_req=1 ttl=64 time=1.23 ms
64 bytes from 192.168.0.30: icmp_req=2 ttl=64 time=0.556 ms
64 bytes from 192.168.0.30: icmp_req=3 ttl=64 time=0.590 ms
64 bytes from 192.168.0.30: icmp_req=4 ttl=64 time=0.498 ms

--- 192.168.0.30 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.498/0.718/1.230/0.298 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 ▼ 秒

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。
クリックして、表示される画面にしたがって操作すると、「経路テスト結果」表示に切り替わり、テスト結果を表示します。

経路テスト結果について

経路テスト結果

```
tracerroute to 192.168.0.30 (192.168.0.30), 16 hops max, 46 byte packets
1 192.168.0.30 (192.168.0.30) 1.287 ms 0.699 ms 0.618 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。

<p>再起動</p> <hr/> <p>再起動: <input type="button" value="実行"/></p>

3 設定画面について

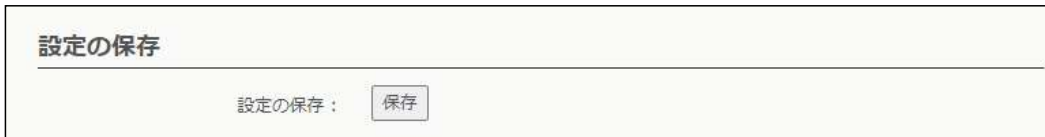
「設定の保存/復元」画面

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。

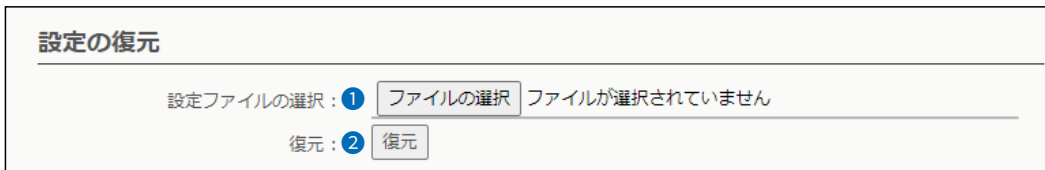
保存したファイルは、[設定の復元]項目の操作で、本製品に書き込みできます。

管理 > 設定の保存/復元

■ 設定の復元

保存した設定ファイルの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、〈ファイルの選択〉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

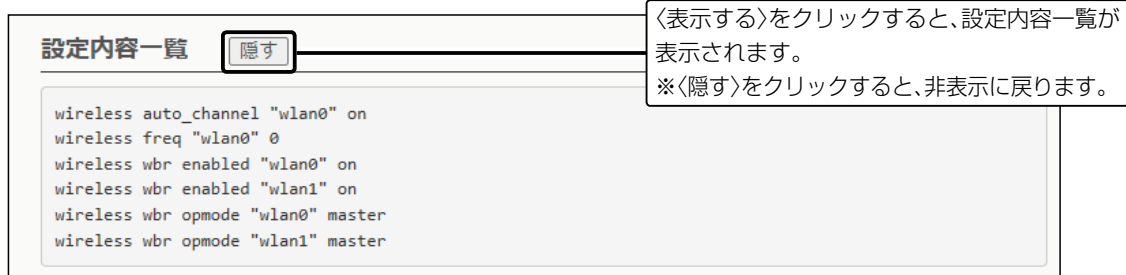
「設定の保存/復元」画面

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。

※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
```

〈表示する〉をクリックすると、設定内容一覧が表示されます。
※〈隠す〉をクリックすると、非表示に戻ります。

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

- 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(数分間)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-9600 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

登録 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
[POWER]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.4-8)
※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 ファイルが選択されていません

ファームウェアの更新 : ②

- ① ファームウェアの選択** …………… <ファイルの選択>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。
選択したファイルが、[ファームウェアの選択]項目に表示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]項目に表示された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
5. USBメモリーによる自動設定機能について	4-9
■ USBメモリー使用時のご注意	4-10
■ 対応するUSBメモリーの規格	4-10
■ 自動設定に使用するファイル名の付けかた	4-11
■ 自動バックアップされる設定ファイルについて	4-11
■ 複数台分の設定ファイルを1つのUSBメモリーで管理するには	4-12
6. USBメモリーから自動で設定を復元するには	4-13
■ 設定ファイルを保存して復元するまでの手順	4-13
7. USBメモリーからファームウェアを更新するには	4-15
■ 更新するまでの手順	4-15
8. USBメモリー用の認証キーを設定するには	4-17
■ 設定のしかた	4-17

4 保守について

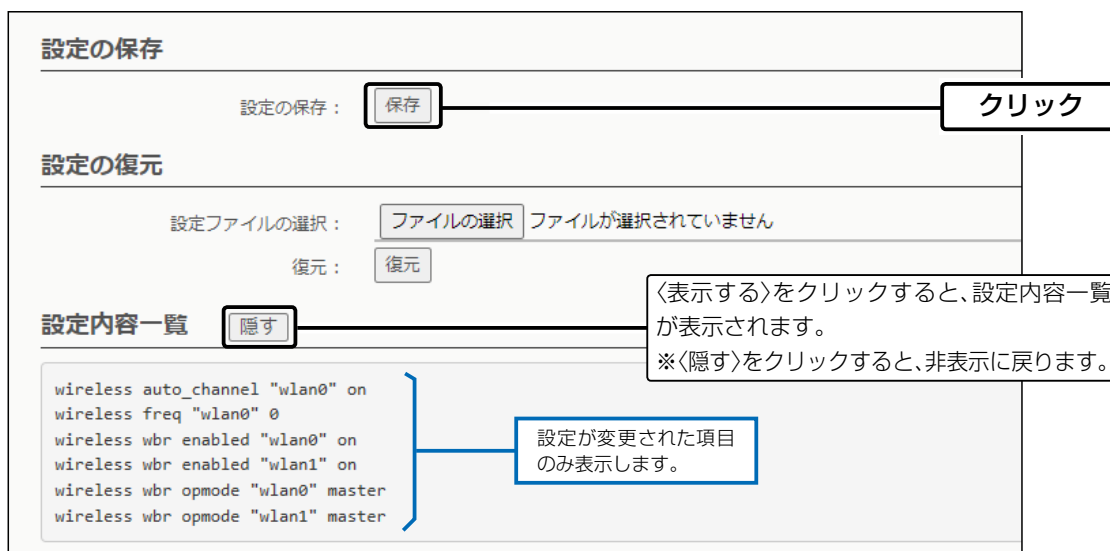
1. 設定内容の確認または保存

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で、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。
設定ファイルが保存されます。(P.1-17)



4 保守について

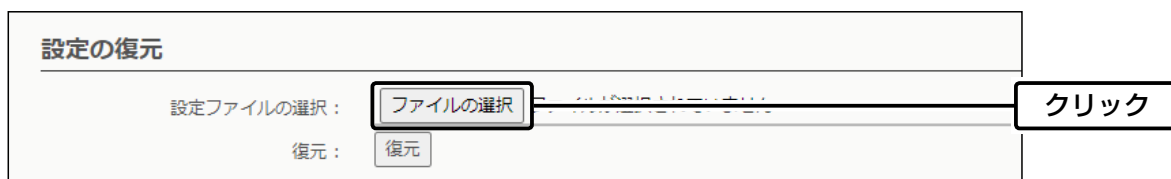
2. 保存された設定の書き込み(復元)

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。

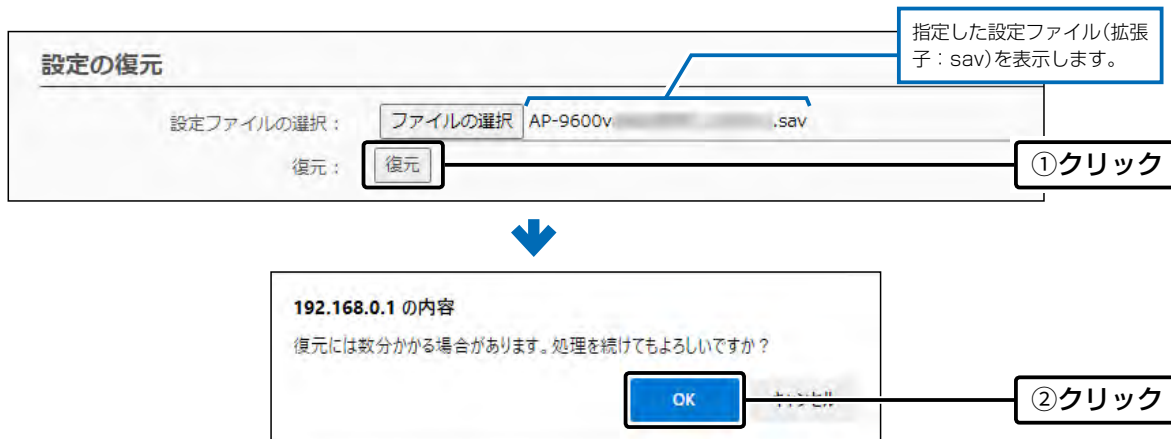
- 1 「管理」メニュー、「設定の保存/復元」の順にクリックします。
「設定の保存/復元」画面が表示されます。

- 2 「設定の復元」項目の〈ファイルの選択〉をクリックします。
「開く」画面(別画面)が表示されます。



- 3 「開く」画面(別画面)で、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、復元するために本製品が再起動します。



- 5 再起動後、[Back]と表示された文字の上にマウスポインタ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、復元中ですので、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。)

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、変更による障害、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

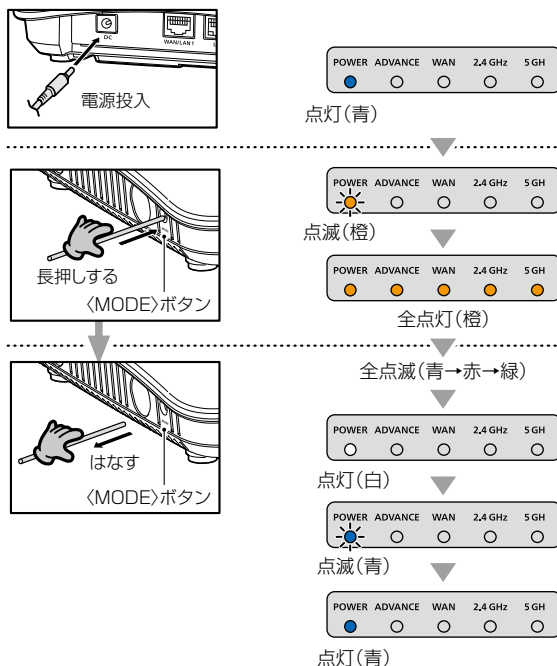
3. 設定を出荷時の状態に戻すには

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。
- 2 すべてのランプが●橙点灯するまで、〈MODE〉ボタンを押す
- 3 すべてのランプが●橙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●青点灯すると、初期化完了です。



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

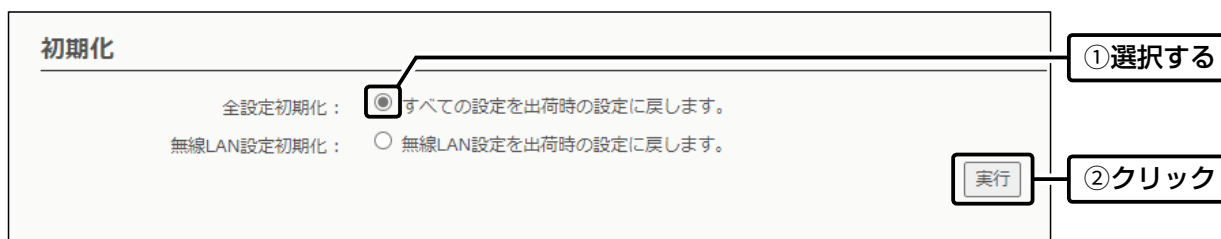
本製品に設定されたIPアドレスと管理者パスワードがわかっていて、そのIPアドレスで設定画面にアクセスできるときは、本製品の設定画面から、すべての設定を出荷時の状態に戻せます。

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。

Ⓐ 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。

Ⓑ 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ーに書き込まれているプログラムです。

このプログラムは、機能の拡張や改良のため、バージョンアップ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	AP-9600
バージョン	<input type="text"/> バージョン情報
国名コード	JP
現在時刻	20 / / 13:08:45
稼働時間	
メモリー使用量	285580 kB / 821908 kB (34% 使用中)
PoEステータス	ACアダプター

■ 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

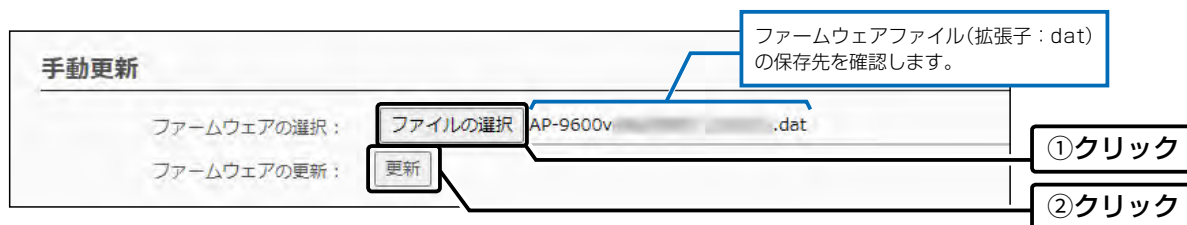
A ファイルを指定して更新する

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)

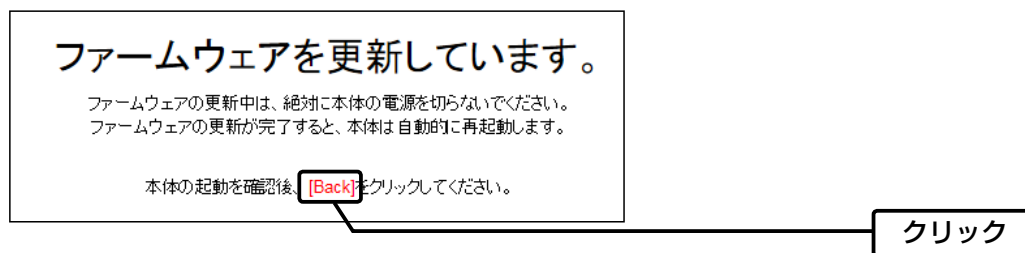
※ 更新後、既存の設定内容が初期化されるファームウェアファイルがありますので、ダウンロードするときは、弊社ホームページに記載の内容をご確認ください。

※ 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.3-95)

- 1 「管理」メニュー、「ファームウェアの更新」の順にクリックします。
「ファームウェアの更新」画面が表示されます。
- 2 下記のように、弊社ホームページよりダウンロードして解凍したファームウェアファイル(拡張子 : dat)の保存先を指定して、更新します。



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



ご注意

[Back]の操作(手順3)で設定画面に戻るようになるまで、ご使用のパソコンや本製品の電源を絶対に切らないでください。
途中で電源を切ると、データの消失や誤動作の原因になります。

※ 出荷時の設定内容に戻るような注意書きがあるバージョンアップ用ファームウェアの場合は、上図の[Back]をクリックしても設定画面に戻れないことがあります。

その場合は、接続するパソコンのIPアドレスを「例:192.168.0.100」に設定してから、本製品の設定画面「192.168.0.1」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

④ 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、[POWER]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。

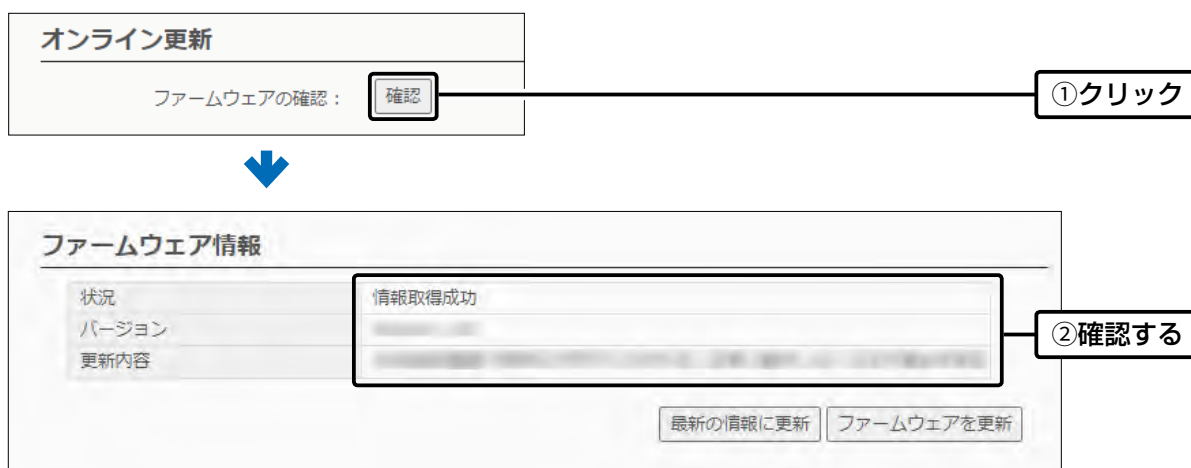
※ 自動更新機能が「有効」に設定されているときに、オンラインで新しいファームウェアを検知します。(P.3-116)

※ 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、[POWER]ランプが青点灯のときは、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、そのまま数分程度お待ちください。
弊社のアップデート管理サーバーに接続すると、ファームウェアのダウンロードを開始し、更新後は、自動的に再起動します。

ファームウェアを更新しています。

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。

4 保守について

5. USBメモリーによる自動設定機能について

本製品のUSBポートにUSBメモリー(市販品)を接続し、〈USB〉ボタンを短く押すと、あらかじめUSBメモリーに保存されたファームウェアファイルや設定ファイル(本製品の設定が保存されたファイル)を本製品に自動で読み込みます。また、本製品の「LAN2」のMACアドレスをフォルダー名とするフォルダーを作成することで、1つのUSBメモリーを使用して、複数台(本製品)の設定復元やファームウェアの更新ができます。

※操作方法については、4-13ページ～4-16ページをご覧ください。

◎ファームウェアの更新

本製品のファームウェアファイル(拡張子: dat)をUSBメモリーに保存後、本製品にUSBメモリーを差し込んで、ファームウェアを更新します。

◎設定の保存/復元

本製品の設定ファイルをUSBメモリーに保存後、本製品にUSBメモリーを差し込んで、自動で設定を復元します。

ご参考

「管理」メニューの「管理ツール」画面で、「最大出力電流」欄を「オフ」以外の設定にし、「USBメモリー」欄が「有効」に設定されているとき、USBメモリーが差し込まれると、USBメモリーへのアクセスが開始されます。

The screenshot shows the 'USB設定' (USB Settings) menu. It includes the following options:

- 最大出力電流 (USB1): Radio buttons for オフ (Off), 500 mA (selected), and 900 mA.
- 最大出力電流 (USB2): Radio buttons for オフ (Off), 500 mA (selected), and 900 mA.
- USBメモリー: Radio buttons for 無効 (Invalid) and 有効 (Valid) (selected).
- USBアクセス許可: Checkboxes for ファームウェアの更新 (Firmware Update) and 設定の保存/復元 (Save/Restore Settings).
- USB認証キー: A text input field with a toggle icon on the right.
- USB認証キーの書き込み: A button labeled '書き込み' (Write).

(※画面の内容は、出荷時の設定です。)

4 保守について

5. USBメモリーによる自動設定機能について

■ USBメモリー使用時のご注意

- ◎ 指紋認証型、アプリケーション認証(パスワード認証)型など、セキュリティ対応型のUSBメモリーは使用できません。
- ◎ ご使用になる前に、あらかじめ、USBメモリー内のデータをバックアップしてください。
- ◎ データ保護のため、必ず[ADVANCE]ランプが消灯してから、USBメモリーの接続や取りはずしをしてください。
設定保存/復元、ファームウェアの更新で使用する場合など、USBメモリーを接続中([ADVANCE]ランプ ● 青点灯中)は、絶対にUSBメモリーを取りはずさないでください。
ファイルの消失や故障の原因になります。
- ◎ USBメモリーは、どちらか一方のUSBポートにだけ接続してください。
2つのUSBポートを同時には使用できません。
- ◎ USBメモリーを差し込むときは、形状と差し込み方向に注意して、奥まで確実に差し込んでください。
- ◎ USBメモリーを接続中は、[ADVANCE]ランプが ● 青点灯します。
設定復元中やファームウェアの更新中は、[POWER]ランプが青色で点滅します。
- ◎ 本製品の設定画面でUSB認証キーが設定(P.4-17)されている場合、差し込まれたUSBメモリー側の認証キーと一致しないときは、自動設定機能は動作しません。
- ◎ 設定を復元する直前の設定値は、設定ファイル(bakdata.sav)として、本製品に接続したUSBメモリーにバックアップされます。
- ◎ USBメモリーに保存された設定ファイルやファームウェアファイルが、本製品に適用されているものと同じ場合や、破損していたり、本製品以外のものであったりするときは、自動設定、またはファームウェアの更新をしません。
※本製品で動作中のものと異なる設定ファイルやファームウェアファイルが、USBメモリーに保存されている場合は、その内容で自動設定されます。
- ◎ 設定ファイルとファームウェアファイルの両方がUSBメモリーに保存されている場合は、設定復元、ファームウェアの更新の順に自動設定を実行します。

■ 対応するUSBメモリーの規格

インターフェース : USB3.0/2.0/1.1

デバイス : USB 大容量デバイス(USB Mass Storage Class)

フォーマット : FAT16/FAT32(exFATやNTFSなど、ほかのフォーマットには対応していません。)

※すべてのUSB対応周辺機器で動作を保証するものではありません。

4 保守について

5. USBメモリーによる自動設定機能について

■ 自動設定に使用するファイル名の付けかた

設定ファイル名は、「savedata」(拡張子：sav)でUSBメモリーに保存してください。

※自動設定に使用する設定ファイルは、「管理」メニュー→「設定の保存/復元」画面→「設定の保存」項目(P.4-2)で保存したものと、自動バックアップされる設定ファイル以外は、使用できません。

ファームウェアファイル名は、「firmware」(拡張子：dat)でUSBメモリーに保存してください。

※ファームウェアの更新に使用するファームウェアファイルは、弊社ホームページからダウンロードし、解凍してから、ファームウェアファイル名を変更してください。

■ 自動バックアップされる設定ファイルについて

バックアップは、下記のファイル名で、最大10世代前まで自動バックアップされます。

最新のバックアップ設定ファイルは、bakdata.savで自動バックアップされます。

例：1世代前のファイル名 bakdata_1.sav

2世代前のファイル名 bakdata_2.sav

3世代前のファイル名 bakdata_3.sav

～ 中略 ～

10世代前のファイル名 bakdata_10.sav

※10世代を超えると、最も古いバックアップ設定ファイル(bakdata_10.sav)が削除されます。

また、削除と同時に、ファイル名の数字が1世代後退します。(例：bakdata_9.sav→bakdata_10.sav)

※ファームウェアファイルは、バックアップされません。

※本製品の設定内容を変更した場合に、設定ファイル(bakdata.sav)が自動バックアップされます。

4 保守について

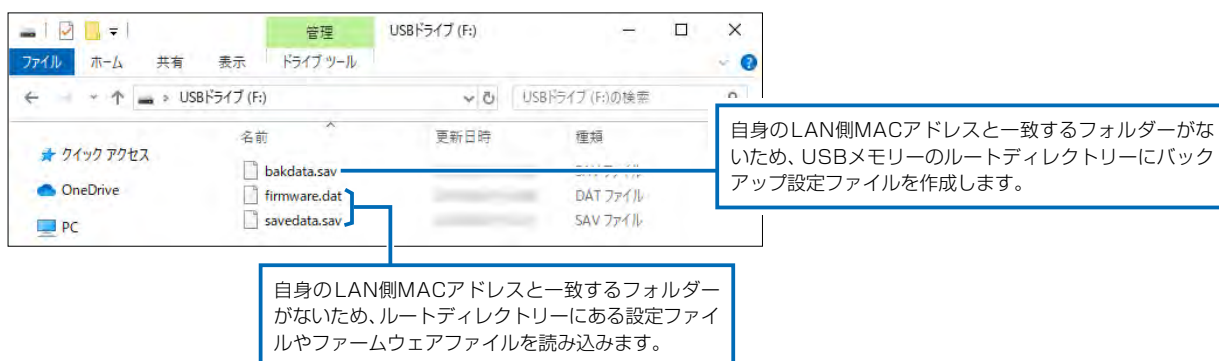
5. USBメモリーによる自動設定機能について

■ 複数台分の設定ファイルを1つのUSBメモリーで管理するには

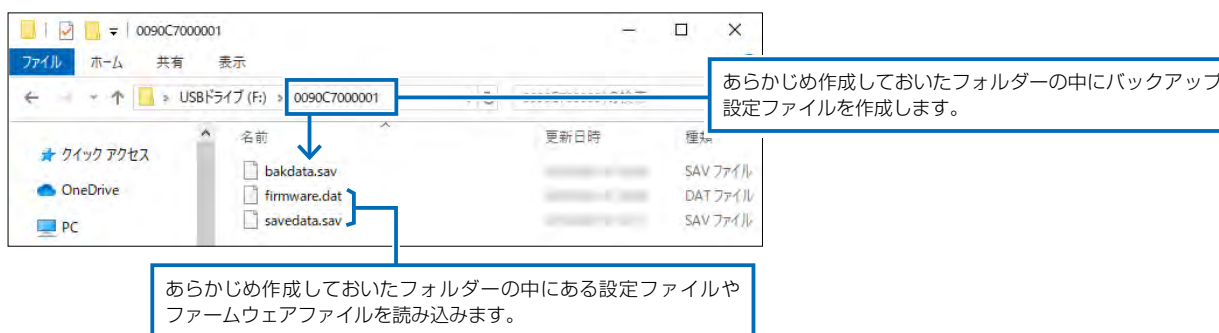
1つのUSBメモリーを使用して、本製品(複数台分)の設定復元やファームウェアの更新をするときは、あらかじめ、「TOP」画面に表示されている「LAN2」のMACアドレス(P.3-5)をフォルダー名★とするフォルダーを作成し、そのフォルダーに本製品の設定ファイルやファームウェアファイルを保存しておく必要があります。

★全角のフォルダー名は使用できません。

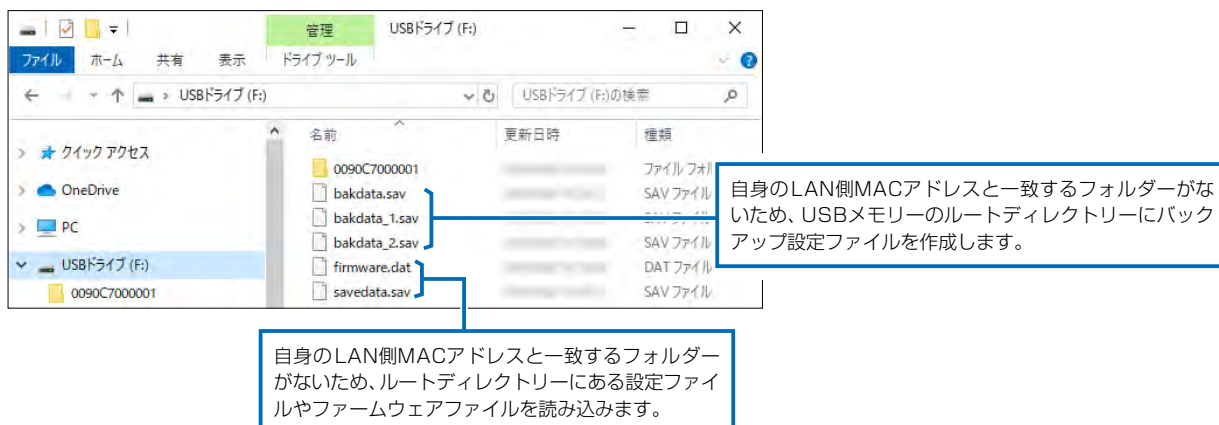
ルートディレクトリーにフォルダーがないとき



自身のLAN側MACアドレス(例：0090C7000001)と一致するフォルダーがあるとき



自身のLAN側MACアドレス(例：0090C7000002)と一致するフォルダーがないとき



4 保守について

6. USBメモリーから自動で設定を復元するには

管理 > 設定の保存/復元

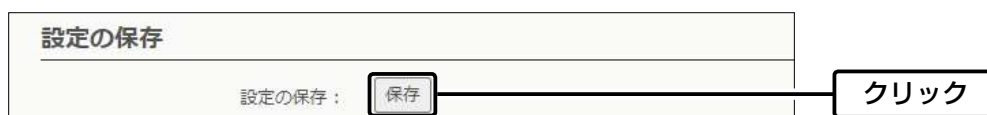
本製品の設定ファイルをUSBメモリー(市販品)に保存後、設定が異なる本製品にUSBメモリーを差し込んで、自動で設定を復元するまでの手順について説明します。

※ 使用条件については、「USBメモリーによる自動設定機能について」(P.4-9)をご覧ください。

※ Microsoft Edge (Chromiumベース)で「ダウンロード時の動作を毎回確認する」を有効にしている場合を例にしています。

■ 設定ファイルを保存して復元するまでの手順

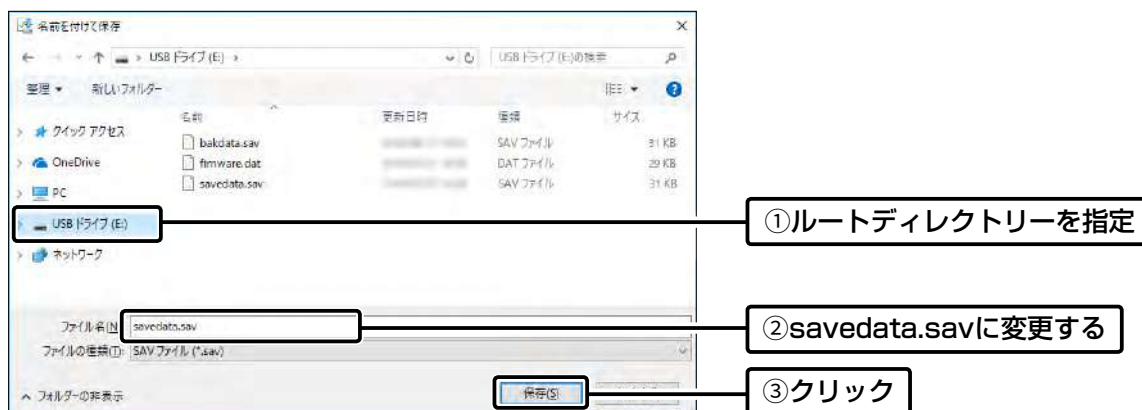
- 1 USBメモリーをパソコンに差し込みます。
- 2 本製品の設定画面にアクセスします。(P.1-17)
- 3 「管理」メニュー、「設定の保存/復元」の順にクリックします。
「設定の保存/復元」画面が表示されます。
- 4 「設定の保存」欄の「保存」をクリックします。



- 5 「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。



- 6 設定ファイルの保存先にUSBメモリーのルートディレクトリーを指定し、
ファイル名を「savedata.sav」に変更してから、「保存(S)」をクリックします。
※ ファイル名は、必ず「savedata.sav」に変更してください。
「savedata.sav」以外のファイル名では、USBメモリーからの復元に使用できません。



(次ページにつづく)

4 保守について

6. USBメモリーから自動で設定を復元するには

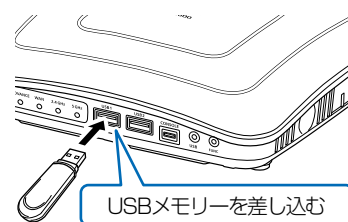
管理 > 設定の保存/復元

■ 設定ファイルを保存して復元するまでの手順

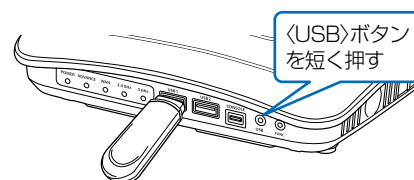
7 USBメモリーをパソコンから取りはずします。
※USBメモリーの取りはずしかたは、各周辺機器に付属する取扱説明書の記載内容にしたがってください。

8 設定を復元する本製品を用意します。

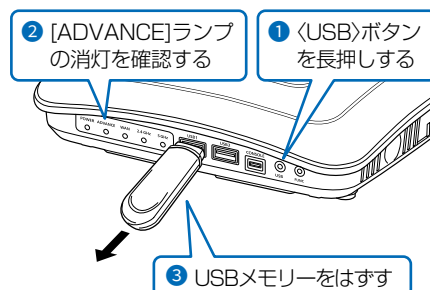
9 savedata.savが保存されたUSBメモリーを本製品のUSBポートに差し込みます。
USBメモリーが接続されると、[ADVANCE]ランプが●青点灯します。



10 〈USB〉ボタンを短く押します。
設定を復元するため、本製品が再起動します。



11 [POWER]ランプが●青点灯に切り替わったことを確認してから、[ADVANCE]ランプが消灯するまで、〈USB〉ボタンを押しつづけます。
[ADVANCE]ランプ消灯後、本製品からUSBメモリーを取りはずします。
※USBメモリーには、復元前の設定内容を保存した設定ファイルが自動でバックアップファイル(bakdata.sav)として保存されています。



ご注意

- ◎設定復元が完了するまで、絶対にUSBメモリーを取りはずしたり、電源を切ったりしないでください。
途中で、USBメモリーを取りはずしたり、電源を切ったりすると、設定ファイルの消失や故障の原因になります。
また、設定復元が完了するまで、本製品の設定画面にアクセスしないでください。
- ◎データ保護のため、必ず[ADVANCE]ランプが消灯してから、USBメモリーを取りはずしてください。

ご参考

「管理」メニューの「管理ツール」画面で、[最大出力電流]欄を「オフ」以外の設定にし、[USBメモリー]欄(P.3-96)が「有効」(出荷時の設定)に設定されているとき、USBメモリーが差し込まれた本製品の電源を入れると、USBメモリーへのアクセスが開始されます。

4 保守について

7. USBメモリーからファームウェアを更新するには

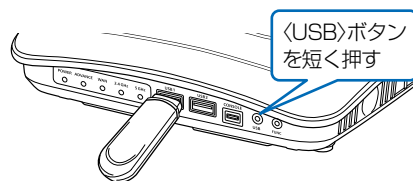
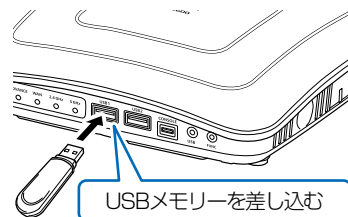
弊社ホームページよりダウンロードした本製品のファームウェアファイル(拡張子:dat)をUSBメモリー(市販品)に保存して、本製品のファームウェアを更新するまでの手順について説明します。

※使用条件については、「USBメモリーによる自動設定機能について」(P.4-9)をご覧ください。

※更新を実行する前に、「ファームウェアの更新についてのご注意」(P.4-6)をご覧ください。

■ 更新するまでの手順

- 1 本製品のファームウェアファイルを弊社ホームページよりダウンロードして、解凍します。
- 2 ファームウェアファイルのファイル名をfirmware.datに変更します。
※ファイル名は、必ず「firmware.dat」に変更してください。
「firmware.dat」以外のファイル名は、USBメモリーからの更新には使用できません。
- 3 USBメモリーをパソコンに差し込みます。
- 4 firmware.datをUSBメモリーのルートディレクトリーに保存します。
- 5 USBメモリーをパソコンから取りはずします。
※USBメモリーの取りはずしかたは、各周辺機器に付属する取扱説明書の記載内容にしたがってください。
- 6 ファームウェアを更新する本製品を用意します。
- 7 firmware.datが保存されたUSBメモリーを本製品のUSBポートに差し込みます。
USBメモリーが接続されると、[ADVANCE]ランプが●青点灯します。
- 8 〈USB〉ボタンを短く押します。
ファームウェアを更新するため、本製品が再起動します。



ご注意

ファームウェアの更新が完了するまで、絶対にUSBメモリーを取りはずしたり、電源を切ったりしないでください。
更新中に、USBメモリーを取りはずしたり、電源を切ったりすると、故障の原因になります。

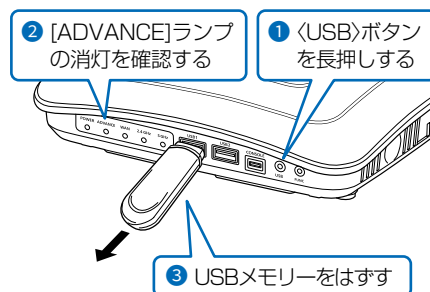
(次ページにつづく)

4 保守について

7. USBメモリーからファームウェアを更新するには

■ 更新するまでの手順

- 9 [POWER] ランプが ● 青点灯に切り替わったことを確認してから、[ADVANCE] ランプが消灯するまで、〈USB〉ボタンを押しつづけます。
[ADVANCE] ランプ消灯後、本製品からUSBメモリーを取りはずします。



ご注意

データ保護のため、必ず[ADVANCE]ランプが消灯してから、USBメモリーを取りはずしてください。

更新後は、本製品の設定画面にアクセスして、ファームウェアバージョンを確認してください。

USBメモリーに保存された設定ファイルやファームウェアファイルが本製品に適用されているものと同じとき、破損や本製品以外のものである場合は、自動設定、またはファームウェアの更新をしません。

4 保守について

8. USBメモリー用の認証キーを設定するには

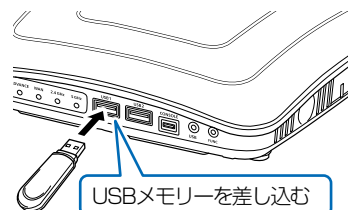
管理 > 管理ツール

本製品にUSB認証キーを設定することで、認証キーが一致するUSBメモリーを使用したときだけ、設定ファイルの自動バックアップ、設定の復元、ファームウェアの更新ができます。

■ 設定のしかた

- 1 USB認証キーの書き込みに使用するUSBメモリーを本製品の[USB]ポートに差し込みます。

※あらかじめ、USBメモリーに保存されたUSB認証キー(ファイル名: usbkey.dat)を変更する場合も、そのUSBメモリーを差し込みます。



- 2 本製品の設定画面にアクセスします。(P.1-17)

- 3 「管理」メニュー、「管理ツール」の順にクリックします。
「管理ツール」画面を表示します。

- 4 [USB設定]項目の[USB認証キー]欄に、大文字/小文字の区別に注意して、任意の半角英数字64文字以内で入力して、〈登録〉をクリックします。

※USB認証キーを変更する場合は、テキストボックスの内容を削除してから入力してください。

USB設定

最大出力電流 (USB1): オフ 500 mA 900 mA

最大出力電流 (USB2): オフ 500 mA 900 mA

USBメモリー: 無効 有効

USBアクセス許可: ファームウェアの更新

設定の保存/復元

USB認証キー:

USB認証キーの書き込み:

登録

- 5 〈書き込み〉をクリックします。

USB設定

最大出力電流 (USB1): オフ 500 mA 900 mA

最大出力電流 (USB2): オフ 500 mA 900 mA

USBメモリー: 無効 有効

USBアクセス許可: ファームウェアの更新

設定の保存/復元

USB認証キー:

USB認証キーの書き込み:

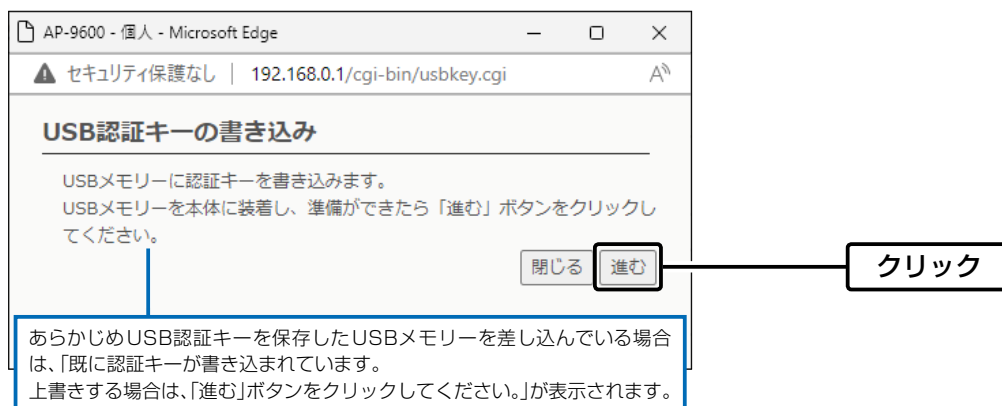
4 保守について

8. USBメモリー用の認証キーを設定するには

管理 > 管理ツール

■ 設定のしかた

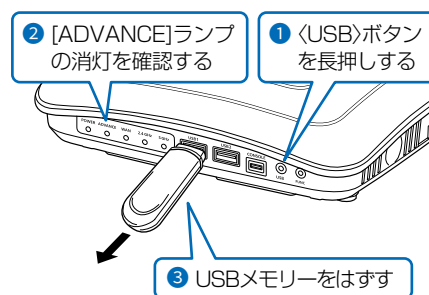
- 6 「USB認証キーの書き込み」(別画面)が表示されたら、〈進む〉をクリックします。
※書き込みを中止する場合は、〈閉じる〉をクリックします。



- 7 「認証キーの書き込みが完了しました。」が表示されたら、〈閉じる〉をクリックします。



- 8 本製品からUSBメモリーを取りはずします。



ご注意

データ保護のため、必ず[ADVANCE]ランプが消灯してから、USBメモリーを取りはずしてください。

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
■ [CONSOLE]ポートを使用する	5-6
3. 設定画面の構成について	5-7
4. 初期値一覧	5-10
■ ネットワーク設定	5-10
■ ルーター設定	5-11
■ 無線LAN設定	5-12
■ 管理	5-16
5. 機能一覧	5-18
■ 無線LAN機能	5-18
■ ネットワーク管理機能	5-18
■ ルーター機能	5-18
■ その他	5-18
6. 設定項目で使用できる文字列について	5-19
■ ネットワーク設定	5-19
■ 無線LAN設定	5-19
■ 管理	5-19
7. 弊社製無線アクセスポイントの機能対応表	5-20
8. 定格について	5-21
■ 一般仕様	5-21
■ 有線部	5-21
■ 無線部	5-21

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]ランプが点灯しない

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

[2.4GHz]ランプ/[5GHz]ランプが青点灯しない

- 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]ランプが青点灯しているが通信できない

- 暗号化セキュリティーの設定が異なっている
→ 本製品と接続先の暗号化セキュリティーの設定を確認する

5 ご参考に

1. 困ったときは

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。(2023年4月現在)

「ath0」: AP-95M(無線LAN1(2.4GHz帯))、AP-9500/AP-9600(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/AP-9600(無線LAN2(2.4GHz帯))

「ath4」: AP-90M、AP-90MR

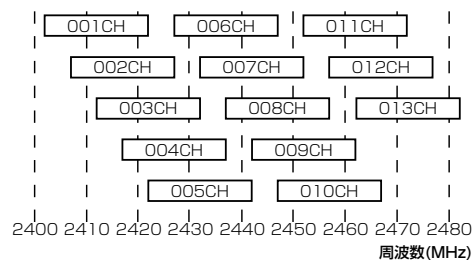
「ath8」: AP-900、AP-9000

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

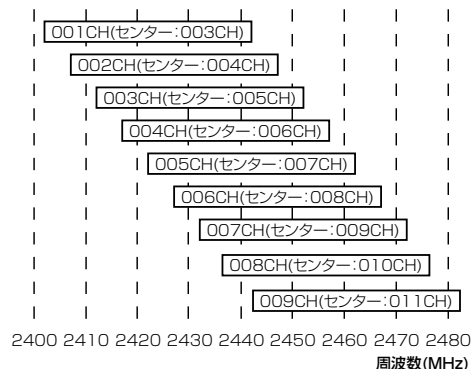
【帯域幅が20MHzの場合】(帯域の1部が重複)

- 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。



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

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
→ (スタート)(ロゴボタン)→[設定]→[ネットワークとインターネット]にある[プロキシ]で、設定を確認する

インターネットに接続できない

- 回線接続業者に契約をしたが、工事完了、または使用開始の通知がない
→ 契約、または工事の完了日をご契約の回線接続業者に確認する
- 使用する機器の MAC アドレスを登録していない
→ 登録が必要な回線接続業者の場合は、本製品の本体 MAC アドレス (WAN 側 MAC アドレス) を登録する (P.vii、P.3-5)
- ブリッジタイプモデム、または回線終端装置 (FTTH) をご使用の場合で、ご契約の回線接続業者への接続方法を間違えている
→ 該当する回線種別 (DHCP クライアント、固定 IP、PPPoE) を、ご契約の回線接続業者に確認する
- ブロードバンドモデム、または回線終端装置 (FTTH) が本製品と正しく接続されていない
→ ブリッジタイプモデム、または回線終端装置 (FTTH) の場合は、本製品の回線種別の設定をご契約の回線接続業者との契約内容にしたがって変更 (DHCP クライアント、固定 IP、PPPoE) してから [WAN/LAN1] ポートと接続する
ルータータイプモデムの場合は、本製品の回線種別を出荷時の設定 (使用しない) で、[LAN] ポートと接続する
- WAN (回線接続業者) 側から IP アドレスが取得できていない
→ 本製品とブリッジタイプモデム、または回線終端装置 (FTTH) の接続を確認する
WAN 側から取得した IP アドレスを確認するときは、「ルーター設定」メニューにある「WAN 接続先」画面の [回線状態表示] に表示される内容を確認する
- DNS サーバーの IP アドレスが正しく指定されていない
→ 「ネットワーク設定」メニュー、または「ルーター設定」メニューで DNS サーバーの設定を確認する

ルーター機能設定時に [WAN/LAN1] ポート (WAN 側) から本製品にアクセスできない

- 出荷時に登録されている IP フィルターの設定により、WAN 側から本製品へのアクセスを遮断しているため
→ △注意 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。

USB メモリーにアクセスできない

- 本製品の USB メモリー機能を無効に設定している
→ 本製品の USB メモリー機能を有効に設定する
- 使用する USB ポートの最大出力電流をオフに設定している
→ 最大出力電流をオフ以外に設定している USB ポートを使用する
→ 使用する USB ポートの最大出力電流をオフ以外に設定する (P.1-3、P.3-96)
※電源供給が IEEE802.3at 規格の場合、[USB1] ポートの最大出力電流が 500mA に制限され、[USB2] ポートは使用できません。

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.3-100)

※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` : 「管理者」画面で設定したパスワードを入力します。(P.3-95)

② ログインに成功すると、プロンプト AP-9600> 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。

※コマンド入力での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-9600> 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) e[Tab]→exit 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

2. Telnet/SSHで接続するには

■ [CONSOLE]ポートを使用する

本製品の[CONSOLE]ポートとパソコンの[USB]ポートを、市販のUSBケーブル(Type-C)で接続すると、ターミナルソフトウェアから設定できます。

※ご使用していただくためには、USBドライバーが必要です。

※弊社ホームページから、USBドライバーとインストールガイドをダウンロードしていただき、手順にしたがってインストールしてください。

※USBドライバーをインストールしたあと、ターミナルソフトウェアのCOMポートを下記の値に設定します。

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

※設定後、何も入力せずに[Enter]キーを押すと、「AP-9600 login:」と表示されます。

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
		AP間通信(WBR)
		DHCPリース情報
		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
		本体名称
		VLAN設定
ネットワーク設定	IPアドレス	IPアドレス設定
		DHCPサーバー
		DHCPサーバー設定
	スタティックルーティング	静的DHCPサーバー設定
		静的DHCPサーバー設定一覧
		IP経路情報
	ポリシールーティング	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
		送信元ルーティング設定
	パケットフィルター	送信元ルーティング設定一覧
		パケットフィルター設定
		パケットフィルター設定一覧
	ルーター設定	WAN接続先
回線種別設定		
アドレス変換		
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
VPN		IPsec設定
	IPsecトンネル設定	
	IPsecトンネル設定一覧	

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
		仮想AP設定
	無線LAN1 仮想AP	暗号化設定
		無線LAN1 MACアドレスフィルタリング
		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 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 ARP代理応答	ARP代理応答設定
		ARPキャッシュ情報
	無線LAN2 無線LAN	無線LAN
		仮想AP設定
	無線LAN2 仮想AP	暗号化設定
		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
		MACアドレスフィルタリング設定一覧
	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 ARP代理応答	ARP代理応答設定	
	ARPキャッシュ情報	

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
	管理ツール	USB設定
		HTTP/HTTPS設定
		Telnet/SSH設定
	時計	時刻設定
		自動時計設定
	SYSLOG	SYSLOG設定
	SNMP	SNMP設定
		SNMPv3設定
	LED	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-9600 ※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)
	DNS代理応答：無効
	プライマリーDNSサーバー：空白(設定なし)
	セカンダリーDNSサーバー：空白(設定なし)
	プライマリーWINSサーバー：空白(設定なし)
セカンダリーWINSサーバー：空白(設定なし)	
静的DHCPサーバー	MACアドレス：空白(設定なし) ※最大登録数：32
	IPアドレス：空白(設定なし)
「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：64
	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)
スタティックルーティング設定一覧	設定なし
「ポリシールーティング」画面	
送信元ルーティング設定	送信元：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)
送信元ルーティング設定一覧	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

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	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			
「VPN」画面				
IPsec設定	IPsec：無効			
IPsecトンネル設定	トンネルインターフェース：vti0 ※設定範囲「vti0～vti31」			
	トンネル：有効			
	トンネル名：空白(設定なし)			
	インターフェース：eth0			
	認証鍵(Pre-Shared Key)：空白(設定なし) ※半角英数字128文字以内			
	リモートアドレス：空白(設定なし)			
リモートID：IPアドレス				
ローカルID：IPアドレス				
IPsecトンネル設定一覧	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LAN] 無線LAN]画面	
無線LAN設定	無線UNIT：無効 帯域幅：20MHz チャンネル：036CH (5180MHz) パワーレベル：高 DTIM間隔：1
[無線LAN] 仮想AP]画面	
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～ath7) 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)
暗号化設定	ネットワーク認証： オープンシステム(ath0、ath01～ath07) 暗号化方式：なし(ath0、ath01～ath07)
[無線LAN] MACアドレスフィルタリング]画面	
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
MACアドレスフィルタリング設定一覧	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 AP間通信(WBR)」画面	
AP間通信設定	AP間通信：無効
「無線LAN1 WMM詳細」画面	
WMM詳細	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 <input type="checkbox"/> 、AC_BE <input type="checkbox"/> 、AC_VI <input type="checkbox"/> 、AC_VO <input type="checkbox"/> [From Station] ACM：AC_VI <input type="checkbox"/> 、AC_VO <input type="checkbox"/>
WMMパワーセーブ設定	WMMパワーセーブ：無効

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 ARP代理応答」画面(ath0～ath7)	
ARP代理応答	インターフェース：ath0 ARP代理応答：無効 不明なARPの透過：有効 ARPエージング時間：0(分) ※設定範囲「0～1440」(分)
ARPキャッシュ情報	設定なし
「無線LAN2 無線LAN」画面	
無線LAN設定	無線UNIT：無効 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」
「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) アカウントリング：無効(ath1、ath11～ath17)
暗号化設定	ネットワーク認証： オープンシステム(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	
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
MACアドレスフィルタリング設定一覧	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：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 <input type="checkbox"/> 、AC_BE <input type="checkbox"/> 、AC_VI <input type="checkbox"/> 、AC_VO <input type="checkbox"/>
	[From Station]
	ACM：AC_VI <input type="checkbox"/> 、AC_VO <input type="checkbox"/>
WMMパワーセーブ設定	WMMパワーセーブ：無効
「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エイジング時間：0(分) ※設定範囲「0～1440」(分)

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：空白(設定なし) 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	
USB設定	最大出力電流(USB1)：500mA 最大出力電流(USB2)：500mA USBメモリー：有効 USBアクセス許可： <input checked="" type="checkbox"/> ファームウェアの更新 <input checked="" type="checkbox"/> 設定の保存/復元 USB認証キー：空白(設定なし) ※半角64文字以内
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
「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 コミュニティー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)

5 ご参考に

4. 初期値一覧

■ 管理

設定画面/項目	初期値
「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

- IEEE802.11ax規格準拠
- 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(WEPC4、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、WPA3、WPA3-SAE)
- SSID(Service Set Identifier)
- アクセスポイント機能
- ローミング機能
- ANY接続拒否機能
- 仮想AP機能
- MACアドレスフィルタリング機能
- パワーレベル設定
- 接続端末制限機能
- 同一仮想AP内の端末間通信禁止機能
- WMM★²(Wi-Fi Multimedia)機能
- ARP代理応答
- WMMパワーセーブ
- 認証サーバー(RADIUS/アカウントリング)
- 自動チャンネル機能

■ ネットワーク管理機能

- SYSLOG
- SNMP(MIB-II)

■ ルーター機能

- 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
- VPN

■ その他

- タグVLAN機能
- 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
- PoE機能
- ファームウェアの更新(WEB/USB)
- 設定保存/復元(WEB/USB)
- WWWメンテナンス(HTTP/HTTPS)
- TELNETメンテナンス(TELNET/SSH)
- コンソールメンテナンス(USB)
- LAN2ポートHUB

★¹ 本製品のIEEE802.11ax規格、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。(2023年4月現在)

5 ご参考に

6. 設定項目で使用できる文字列について

下表のように、入力できる文字列が設定項目により異なります。

■ 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

■ 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	3-74ページ参照
		PSK (Pre-Shared Key)	ASCII*2、または16進数	3-75ページ参照
AP間通信(WBR)	子機設定	PSK (Pre-Shared Key)	ASCII*2、または16進数	3-87ページ参照

■ 管理

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

5 ご参考に

7. 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	AP-9600	SE-900
ルーター	ルーター機能	×	○	○	×	○	○	○	×
	WANポート	×	○* ¹	○* ¹	×	○* ¹	○	○* ¹	×
ネットワーク	ポートベースVLAN	×	×	×	×	○	×	×	×
	パケットフィルタ	○	○	○	○	○	○	○	○
無線	無線UNIT数	2	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* ³	○	○	×	×	×	×	×	○
	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* ⁶	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	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)	○ (MODE)
	屋外対応	×	×	×	○	×	×	×	○

- ★1 AP-90MR、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の場合は[WAN/LAN]ポート、AP-9600の場合は[WAN/LAN1]ポートを設定で切り替えて使用します。
- ★2 SE-900で、アクセスポイントモードとクライアントモードを切り替える機能です。
- ★3 無線UNITで使用する周波数帯(2.4GHz帯/5GHz帯)を切り替える機能です。
AP-9000やAP-900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、AP-9600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、AP-9500、AP-9600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ケーブルを[CONSOLE]ポートに接続します。
使用するUSBケーブルや設定方法など、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。

8. 定格について

■ 一般仕様

- 電 源** : DC12V±10% [DCプラグ極性 : ⊖⊕]
- ※ACアダプター(付属品)は、AC100V±10%
- ※PoEは、IEEE802.3bt準拠
- 最大40W(付属のACアダプター使用時)
- 最大48W(PoE使用時)
- 使 用 環 境** : 温度-10~+50℃ (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205(W)×49(H)×205(D)mm(突起物を除く)
- 重 量** : 約1.0kg(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(POWER、ADVANCE、WAN、2.4GHz、5GHz)
- ボタン(USB、FUNC、MODE)
- [USB]ポート×2 : USB Type-A(USB3.0)
- [CONSOLE]ポート×1 : USB Type-C(USB2.0)

■ 有線部

- インターフェース** : [WAN/LAN1]ポート(RJ-45型)×1(Auto MDI/MDI-X)
- IEEE802.3u/100BASE-TX準拠
 - IEEE802.3ab/1000BASE-T準拠
 - IEEE802.3bz/2.5GBASE-T準拠
 - IEEE802.3bt規格準拠
- [LAN2]ポート(RJ-45型)×1(Auto MDI/MDI-X)
- IEEE802.3u/100BASE-TX準拠
 - IEEE802.3ab/1000BASE-T準拠
 - IEEE802.3bz/2.5GBASE-T準拠
 - IEEE802.3bt規格準拠
- 通 信 速 度** : [WAN/LAN1]部 100/1000/2500Mbps(自動切り替え/全二重)
- [LAN2]部 100/1000/2500Mbps(自動切り替え/全二重)

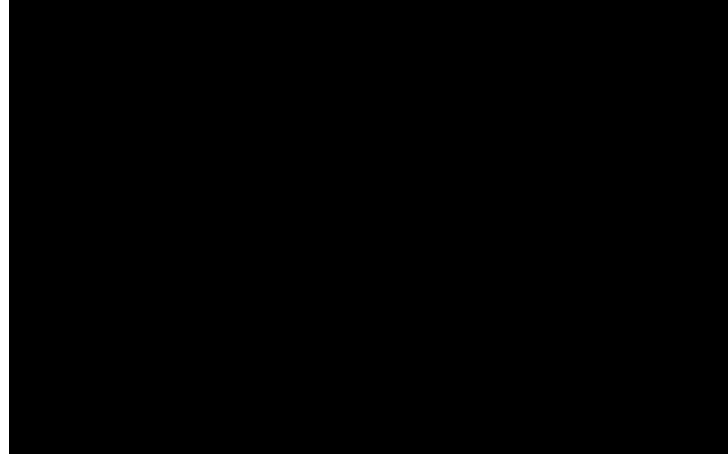
■ 無線部

- 国 際 規 格** : IEEE802.11ax準拠、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** : 5180~5720MHz
- 2412~2472MHz

定格・仕様・外觀等は、改良のため予告なく変更する場合があります。

How the World Communicates

～コミュニケーションで世界をつなぐ～



ワイヤレスアクセスポイント AP-9600

IEEE802.11ax規格準拠
IEEE802.11ac規格準拠
IEEE802.11n規格準拠
IEEE802.11a/g/b規格準拠

はじめに

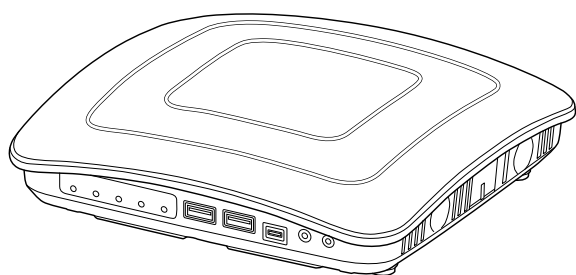
1 ご使用になる前に

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



Icom Inc.

- ◎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、IEEE802.11ax規格、IEEE802.11ac規格*に準拠し、2.4GHz帯と5GHz帯の2波同時通信ができる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。

★IEEE802.11ac規格を使用できるのは、5GHz帯だけです。

登録商標/著作権について

アイコム、ICOM、ICOMロゴは、アイコム株式会社の登録商標です。

Microsoft、Windowsは、マイクロソフト企業グループの商標です。

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写/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. 1.01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

- ◎IEEE802.11ax規格に準拠し、最大2402Mbps(理論値)の速度で通信できます。
 - ※2402Mbps(理論値)は、5GHz帯で帯域幅を「80MHz」に設定したときの速度です。
 - ※IEEE802.11ax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。
- ◎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。
- ◎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」、「WPA3」、「WPA3-SAE」に対応しています。
- ◎「IEEE802.1X」、「WPA」、「WPA2」、「WPA3」を設定すると、認証にRADIUSサーバーを使用できます。
- ◎IEEE802.3bt規格に準拠したPoE受電機能に対応しています。
 - ※本製品の性能を十分に発揮するために、PoEから受電する場合は、IEEE802.3bt規格対応のHUBまたはインジェクター製品(市販品)と接続してください。
- ◎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、多台数接続時の通信速度を改善できます。
- ◎USBメモリー(市販品)を本製品のUSBポートに接続することで、ファームウェアの更新、設定の保存/復元ができます。
- ◎PPPoE、DHCP、固定IPなど、各種接続方式に対応したブロードバンドルーター機能を搭載しています。
- ◎インターネットを利用して、専用線のような通信回線を構築できるVPNルーター機能を搭載しています。
- ◎ネットワーク管理機能として、SNMPに対応しています。
- ◎IPフィルター機能を搭載していますので、アクセス制限ができます。
- ◎本製品は、免許不要・資格不要です。

はじめに

別売品について

(2023年4月現在)

RS-AP3 (近日対応予定)
アクセスポイント管理ツール

RC-AP10 (近日対応予定)
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	LAN側IP	IPアドレス設定	IPアドレス	192.168.0.1
			サブネットマスク	255.255.255.0
	DHCPサーバー	DHCPサーバー設定	DHCPサーバー	無効
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	無線UNIT	無効
			チャンネル	036CH (5180MHz) (無線LAN1) 001CH (2412MHz) (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
			暗号化設定	ネットワーク認証 オープンシステム
			暗号化方式	なし
管理	管理者	管理者パスワードの変更	管理者ID	admin (変更不可)
			現在のパスワード	—

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	IEEE802.11ax (W52/W53/W56)	80MHz	2402Mbps
		40MHz	1147Mbps
		20MHz	574Mbps
	IEEE802.11ac (W52/W53/W56)	80MHz	1733Mbps
		40MHz	800Mbps
		20MHz	347Mbps
	IEEE802.11n (W52/W53/W56)	40MHz	600Mbps
		20MHz	289Mbps
	IEEE802.11a (W52/W53/W56)	20MHz	54Mbps
2.4GHz	IEEE802.11ax	40MHz	1147Mbps
		20MHz	574Mbps
	IEEE802.11n	40MHz	600Mbps
		20MHz	289Mbps
	IEEE802.11g	20MHz	54Mbps
	IEEE802.11b	20MHz	11Mbps

【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*
5.2/5.3/5.6GHz	IEEE802.11ax (W52/W53/W56)	約30m	約100m
	IEEE802.11ac (W52/W53/W56)		
	IEEE802.11n (W52/W53/W56)		
	IEEE802.11a (W52/W53/W56)		
2.4GHz	IEEE802.11ax	約30m	約100m
	IEEE802.11n		
	IEEE802.11g		
	IEEE802.11b		

※本書では、AP-9600同士で通信した場合の距離を参考として記載しています。

★ 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。

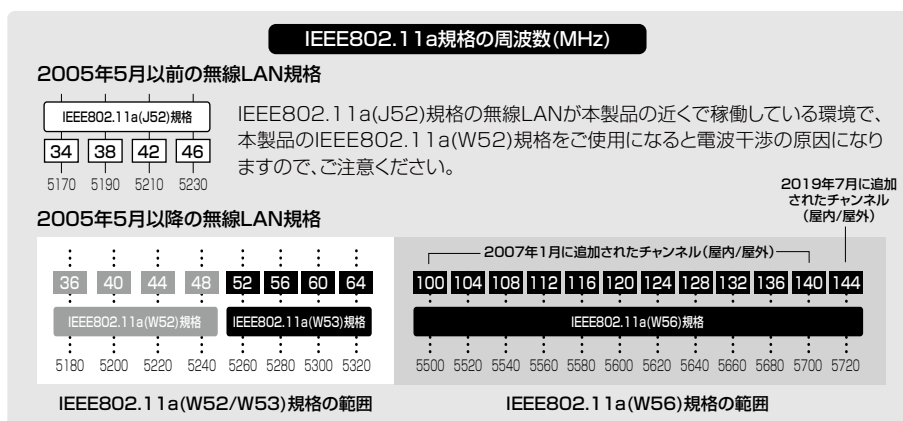
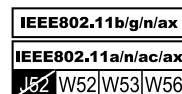
はじめに

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。



帯域幅と無線通信チャンネルについて

本製品には、5GHz帯用(無線LAN1)、2.4GHz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。

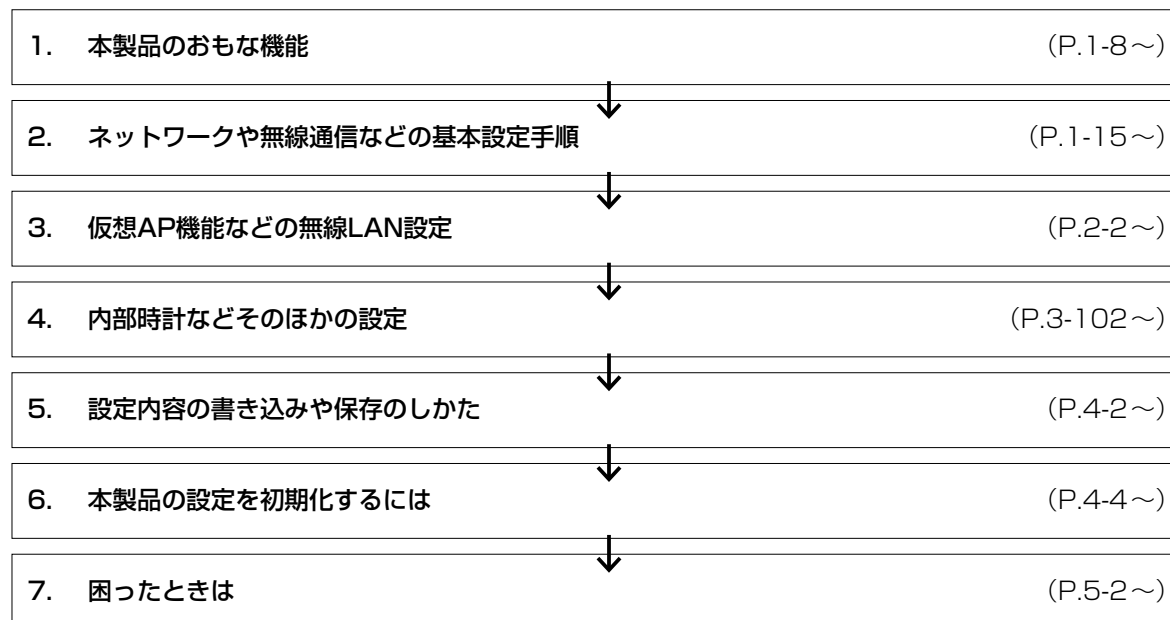
周波数帯	帯域幅	使用できるチャンネル
5GHz	80MHz	36、40、44、48、52、56、60、64、100、104、108、112、116、120、124、128、132、136、140、144
	40MHz	36、44、52、60、100、108、116、124、132、140
	20MHz	36、40、44、48、52、56、60、64、100、104、108、112、116、120、124、128、132、136、140、144、自動
2.4GHz	40MHz	1、2、3、4、5、6、7、8、9
	20MHz	1、2、3、4、5、6、7、8、9、10、11、12、13、自動

※帯域幅を80MHzに設定できるのは、無線LAN1(5GHz帯)だけです。

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。



はじめに

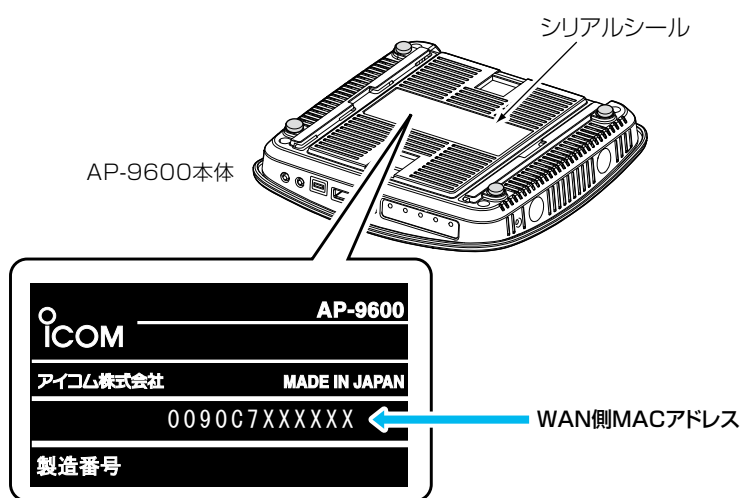
本体MACアドレスが必要なときは

本体MACアドレス(機器固有の番号)は、本製品のシリアルシール(下図)に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、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WAN側MACアドレス(機器固有の番号)を、ご契約の接続業者、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。

※無線LANやLAN側のMACアドレスではありませんのでご注意ください。



※MACアドレスの記載位置は、お買い上げの製品によって若干異なる場合があります。

ご参考

上記のMACアドレスは、設定画面でも確認できます。(P.3-5)

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
■ 外観図	1-2
■ LANポート側	1-3
■ ランプ表示側	1-4
■ <MODE>ボタン側/セキュリティースロット側	1-7
2. おもな機能について	1-8
■ アクセスポイント機能	1-8
■ 無線ネットワーク名(SSID)	1-8
■ 接続端末制限機能	1-8
■ IEEE802.11ax規格	1-8
■ ビームフォーミング機能/MU-MIMO機能	1-8
■ ローミング機能について	1-9
■ 無線AP間通信機能(WBR)について	1-10
■ 仮想AP機能について	1-11
■ DFS機能とチャンネルの自動設定	1-12
■ ルーター機能	1-13
■ VPN機能	1-13
3. 接続や設置について	1-14
■ 本製品を壁面に固定するときは	1-14
4. 設定のしかた	1-15
■ 設定用のパソコンに固定IPアドレスを設定する	1-15
■ 設定に使うパソコンを接続する	1-16
■ 設定画面へのアクセスと初期設定について	1-17
■ 設定画面の名称と機能について	1-18
■ 設定画面の表示について	1-19
■ 本体IPアドレスを変更するときは	1-21

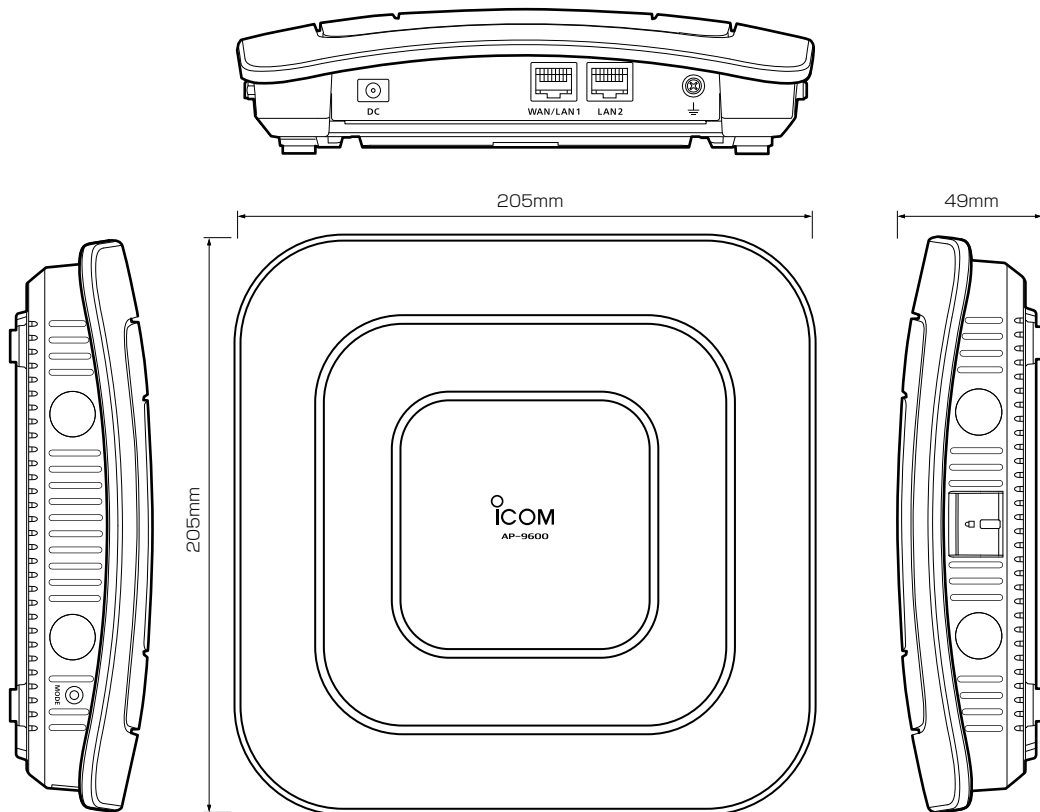
1 ご使用になる前に

1. 各部の名称と機能

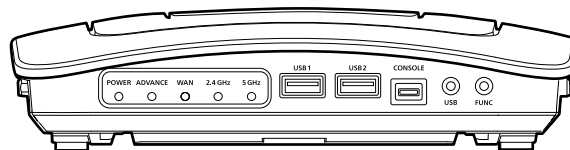
■ 外観図

各面の詳細については、参照ページをご覧ください。

LANポート側(P.1-3)



〈MODE〉ボタン側(P.1-7)



セキュリティーロット側
(P.1-7)

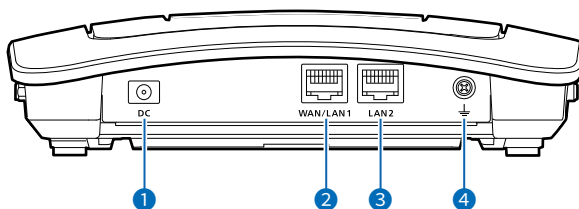
ランプ表示側(P.1-4)

1 ご使用になる前に

1. 各部の名称と機能

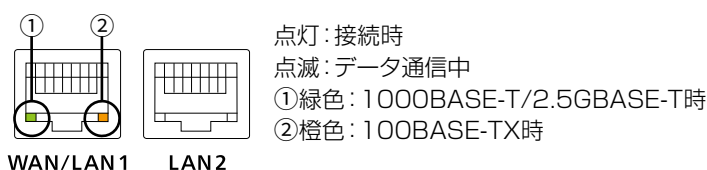
■ LANポート側

LANポートやランプの動作について説明します。



- ① 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。
- ② [WAN/LAN1]ポート …………… 回線種別の設定によって、用途が異なります。(P.1-13)
(RJ-45型×1) ※PoEから受電する場合は、回線種別設定に関係なく使用できますので、IEEE802.3bt規格対応のHUBまたはインジェクター製品(市販品)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。
- ③ [LAN2]ポート …………… HUBなどのネットワーク機器と接続します。
(RJ-45型×1) ※PoEから受電する場合は、IEEE802.3bt規格対応のHUBまたはインジェクター製品(市販品)と接続してください。

ランプ表示



- ④ アース端子 …………… 市販のアース線を接続します。

ご注意

IEEE802.3at規格のPoEから受電する場合は、次のように制限されます。

- ・無線LAN(1/2)が2ストリームに制限されます。
- ・[USB1]ポートの最大出力電流が500mAに制限されます。
- ・[USB2]ポートは使用できません。

※IEEE802.3af規格の場合は、動作保証外です。

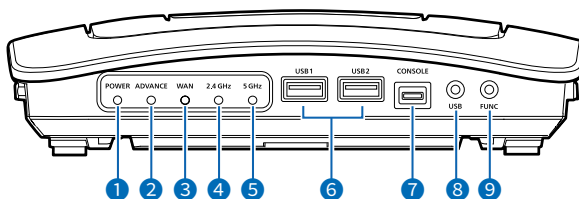
1 ご使用になる前に

1. 各部の名称と機能

■ ランプ表示側

ランプの動作やUSBポートについて説明します。

※すべてのランプ(①～⑤)が赤点滅のときは、機器の異常を検出していますので、弊社サポートセンターにお問い合わせください。



- ① [POWER]ランプ
 - 青点灯：電源ON時
 - ☀青点滅：ファームウェアロード時
 - 橙点灯：オンライン更新(ファームウェア更新あり)
 - ☀橙点滅：〈MODE〉ボタン操作時
 - 消 灯：電源OFF時
 - ※電源投入時、すべてのランプが点滅(赤→緑→青→白)します。
 - ※起動中、[POWER]ランプは白点灯→青点滅→青点灯の順で遷移します。
 - ※LED消灯モードが「有効」のときは、[POWER]ランプの明るさが暗くなり、「有効(完全消灯)」のときは消灯します。(出荷時の設定：無効)

- ② [ADVANCE]ランプ
 - 青点灯：USBメモリー接続時
 - ☀青点滅：USBロード時
 - 赤点灯：USBロード失敗時
 - 消 灯：USBメモリー未接続

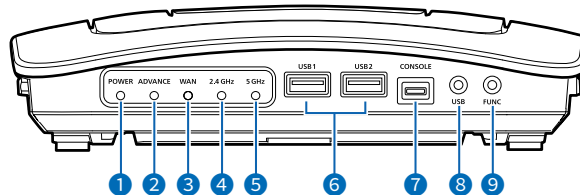
- ③ [WAN]ランプ
 - 青点灯：リンク時 (2.5GBASE-T)
 - ☀青点滅：データ通信中 (2.5GBASE-T)
 - 緑点灯：リンク時 (1000BASE-T)
 - ☀緑点滅：データ通信中 (1000BASE-T)
 - 橙点灯：リンク時 (100BASE-TX)
 - ☀橙点滅：データ通信中 (100BASE-TX)
 - 消 灯：リンク未確立時

- ④ [2.4GHz]ランプ
 - 青点灯：端末が1台以上帰属時
 - 橙点灯：2.4GHz帯有効時(帰属端末なし)
 - 消 灯：2.4GHz帯無効時

1 ご使用になる前に

1. 各部の名称と機能

■ ランプ表示側



5 [5GHz]ランプ

- 青点灯：端末が1台以上帰属時
- 橙点灯：5GHz帯有効時(帰属端末なし)
- ☀ 橙点滅：DFS動作による無線動作待機中
- 消 灯：5GHz帯無効時

6 [USB](1/2)ポート (USB3.0)

設定復元、ファームウェアの更新で使用するUSBメモリー(市販品)を接続します。

ご使用になるときは、USBポートの奥まで挿入してください。

※使用するUSBデバイスについては、4-10ページでご確認ください。

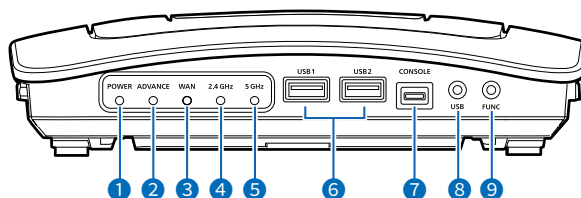
※最大出力電流が「オフ」に設定されているUSBポートは、USBデバイスを接続しても使用できません。(P.1-3、P.3-96)

※すべてのUSBデバイスでの動作を保証するものではありません。

1 ご使用になる前に

1. 各部の名称と機能

■ ランプ表示側



- 7 [CONSOLE]ポート** …………… 本製品の設定にターミナルソフトウェアを使用するとき、USBケーブル(市販品)を接続します。
(USB Type-C)
※ご使用していただくために必要なUSBドライバー、およびインストールガイドは、弊社ホームページ(下記参照)からダウンロードできます。
※USBケーブル(Type-C)、ターミナルソフトウェアは、別途ご用意ください。

- 8 <USB>ボタン** …………… USBメモリー接続時、[ADVANCE]ランプ(2)が点灯(青)から消灯に切り替わるまでボタンを長く押しと、USBメモリーを取りはずせます。
※設定復元、ファームウェアの更新で使用するUSBメモリー(市販品)を差し込んだときは、[ADVANCE]ランプ(2)が点灯(青)してからボタンを短く押ししてください。(P.4-9)

- 9 <FUNC>ボタン** …………… 本製品の設定画面で割り当てた機能进行操作するときを使用します。
※2023年4月現在、近日常対応予定です。

USBドライバーのダウンロードについて

本製品の[CONSOLE]ポートは、弊社ネットワーク機器用のUSBドライバーで動作します。

弊社ホームページのサポート情報(サポート情報→法人のお客様→ダウンロード)から、USBドライバーをダウンロードできます。

アイコム株式会社 サポート情報

<https://www.icom.co.jp/support/business/>

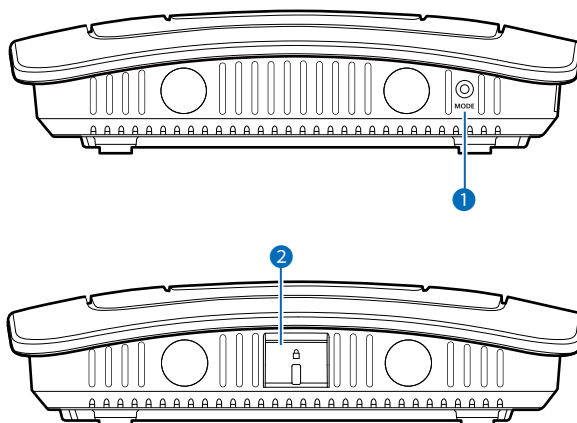
※弊社ホームページからのダウンロード手順については、予告なく変更する場合がありますのであらかじめご了承ください。

1 ご使用になる前に

1. 各部の名称と機能

■ 〈MODE〉ボタン側/セキュリティーロット側

接続部やボタン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 セキュリティーロット …………… 市販のセキュリティーワイヤーで本製品を固定するときに使用します。
机の脚や支柱などにセキュリティーワイヤーを固定してから、本製品のセキュリティー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ーワイヤーの取扱説明書をご覧ください。
※セキュリティーワイヤーには、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ー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、IEEE802.11ax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。

※ 出荷時、本製品の無線UNITは「無効」に設定されています。

※ 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.2-3)

※ 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5GHz帯用(無線LAN1)と2.4GHz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。

■ IEEE802.11ax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2402Mbps★(理論値)の速度で通信できます。

★ IEEE802.11ax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。

最大2402Mbps(理論値)で使用するには、無線LAN1で帯域幅を「80MHz」に設定してください。(P.2-8)
(無線LAN2で帯域幅を「40MHz」に設定すると最大1147Mbps)

※ IEEE802.11ac/n/a/g/b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。

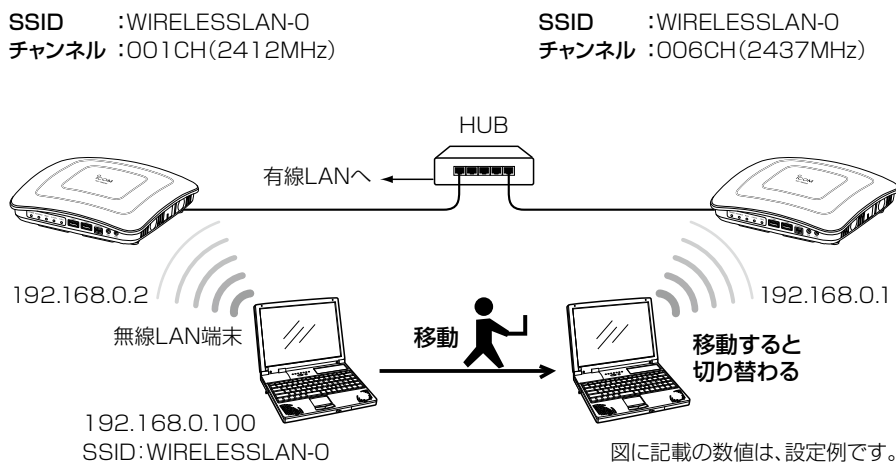
さらに、電波干渉を避けて、複数の端末へ並行送信できるMU-MIMO機能も備え、多台数接続時の通信速度を改善できます。

1 ご使用になる前に

2. おもな機能について

■ 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。

上記の例にある2.4GHz帯で無線LANを使用する場合は、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。

※5GHz帯で無線AP間通信が利用できるのは、5.2GHz帯だけです。

※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。(P.5-20)

無線AP間通信機能(WBR)を使用する場合

◎ 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.2-6)、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。(2023年4月現在)

「ath0」: AP-95M(無線LAN1 (2.4GHz帯))、AP-9500/AP-9600(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/AP-9600(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 : 036 CH (5180 MHz)
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。

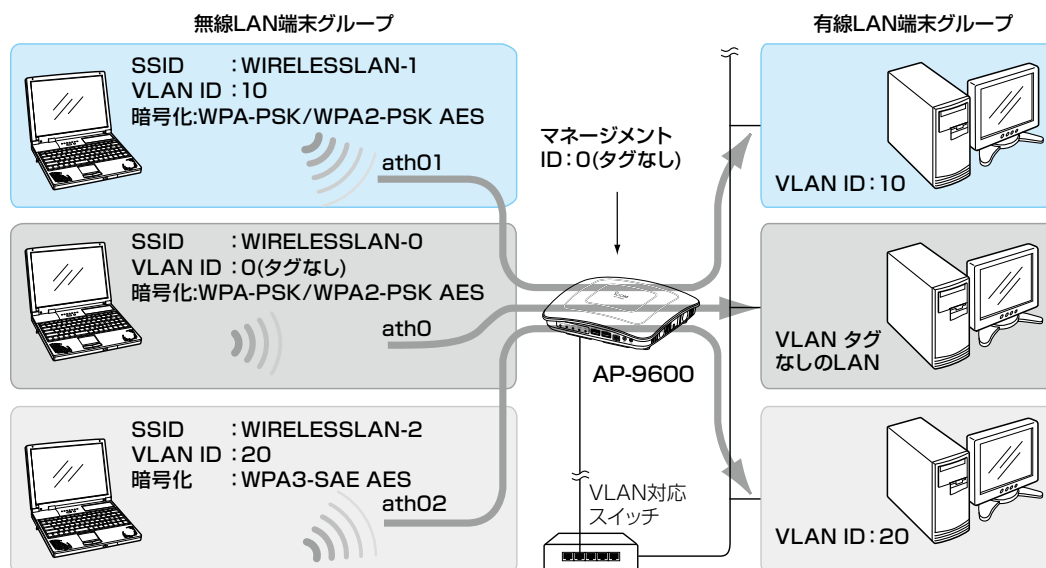
※電波強度が変化しても、接続が切れない限りローミングしません。

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。
※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

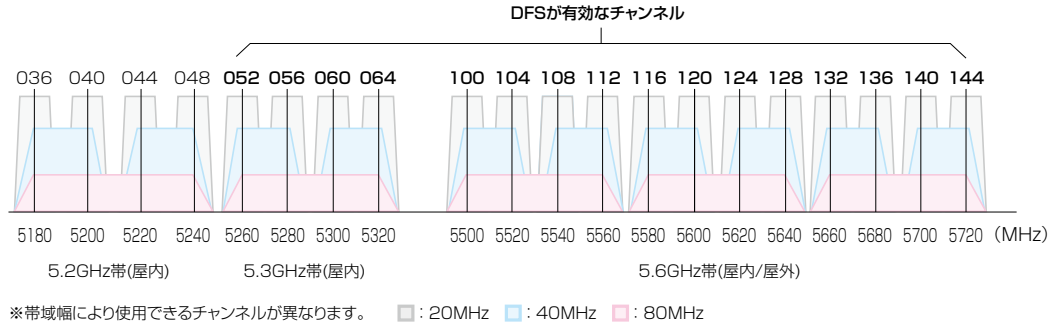
- ◎仮想APを使用して、最大16グループの無線ネットワークを構築できます。
- ◎複数の仮想AP機能を使用する場合、1つのユニットに対して、同じSSIDを設定できません。
- ◎各仮想APの無線LAN端末グループに、VLAN ID(0~4094)を設定できます。
- ◎出荷時、本製品の[管理ID]が「0」(タグなし)に設定されていますので、VLAN IDが設定されたネットワークからは、本製品の設定画面にアクセスできません。

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(052～144)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 \odot 橙点滅して、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(100～144)でレーダー波を検出した場合は、[5GHz]ランプが \odot 橙点滅すると同時に、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(052～144)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。

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

本製品のルーター機能を使用すると、本製品に接続したパソコンや機器からインターネットに接続できます。

※ 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[WAN/LAN1]ポートに接続します。

※ 出荷時や全設定初期化時、本製品のルーター機能(回線種別)は、「無効(LANポートとして使用する)」に設定されています。(P.3-41)

ご契約の回線接続業者との契約内容にしたがって、回線種別(DHCPクライアント/PPPoE/固定IP)を設定してください。

■ VPN機能

VPN(Virtual Private Network)機能を使用すると、インターネット上の2地点を暗号化通信で接続して、仮想的なネットワークを構成できます。

※ VPN機能を使用する場合は、本製品の[WAN/LAN1]ポートにWAN回線を接続し、ルーター機能(回線種別)の設定が必要です。

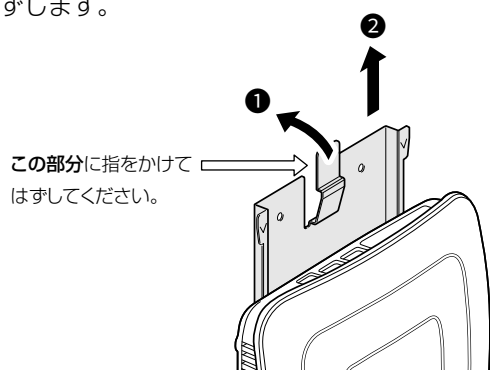
※接続先に合わせて、IPsecトンネルを登録してください。(P.3-60)

1 ご使用になる前に

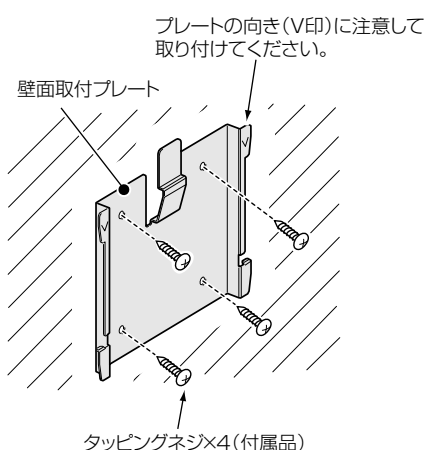
3. 接続や設置について

■ 本製品を壁面に固定するときは

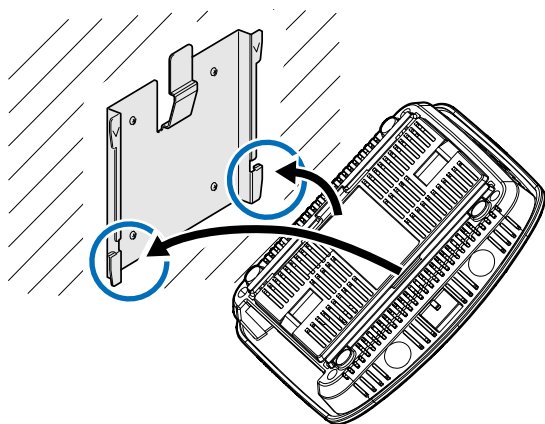
- 1 出荷時、本製品に壁面取付プレートが装着されていますので、図のように壁面取付プレートを取りはずします。



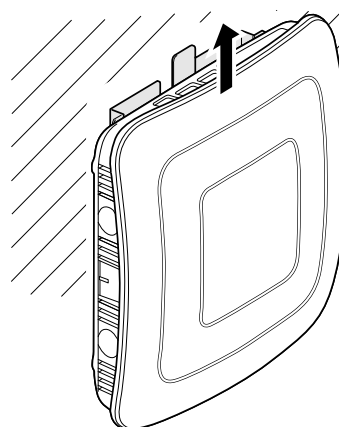
- 2 壁面取付プレートを壁面に取り付けます。



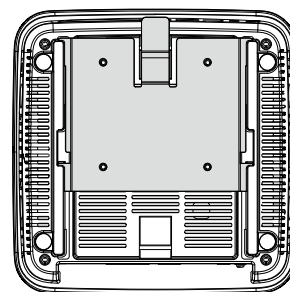
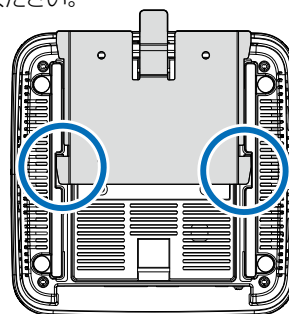
- 3 壁面取付プレートの下部を本製品の溝(右図参照)に差し込みます。



- 4 本製品をスライドして固定します。(下図参照)



○の部分にプレートを差し込むように取り付けたと、本製品をスライドしてください。



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には、接続するパソコンに固定IPアドレスの設定が必要です。

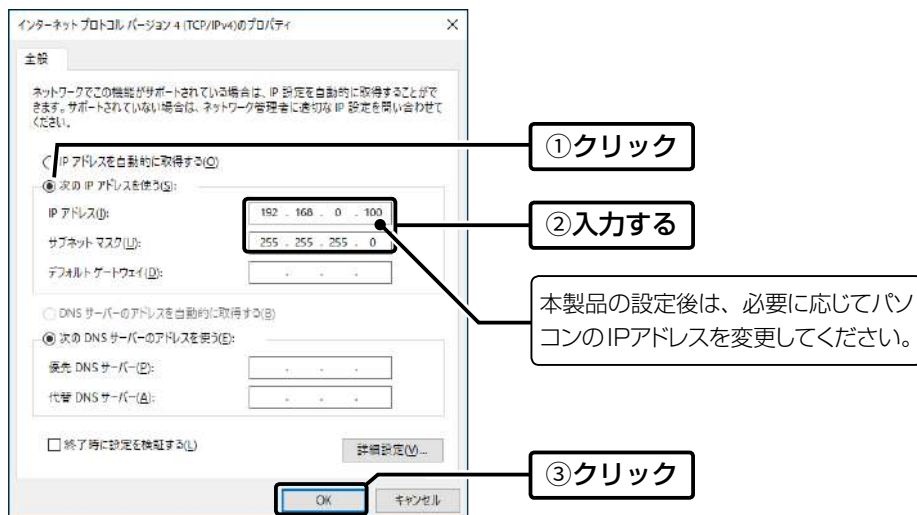
■ 設定用のパソコンに固定IPアドレスを設定する

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

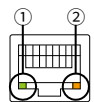
4. 設定のしかた

■ 設定に使うパソコンを接続する

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ポートにある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。



WAN/LAN 1



LAN 2

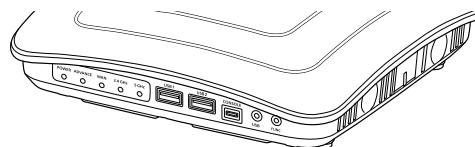
ランプ表示について

点灯：接続時

点滅：データ通信中

① 緑色：1000BASE-T/2.5GBASE-T時

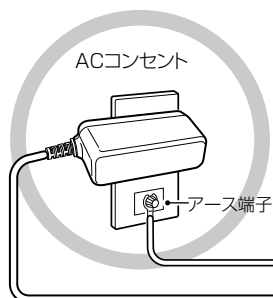
② 橙色：100BASE-TX時



[POWER]ランプなどは、LANポートの反対側にあります。

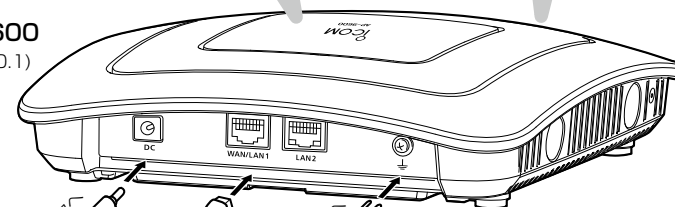
② 電源を接続する

本製品の[POWER]ランプが点灯します。



AP-9600

(出荷時の設定: 192.168.0.1)



① 各ケーブルを接続する

設定用パソコン
(設定例: 192.168.0.100)

③ パソコンを起動する

△ 警告

◎本製品のアース端子を、ガス管や水道管には絶対に接続しないでください。

◎落雷したときの電氣的ショックの緩和、感電やノイズの回り込みを防止するため、本製品のアース端子は、市販のアース線を使用して、コンセントのアース端子、または地中に埋めたアース棒(市販品)に必ず接続してください。

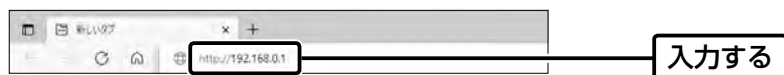
1 ご使用になる前に

4. 設定のしかた

■ 設定画面へのアクセスと初期設定について

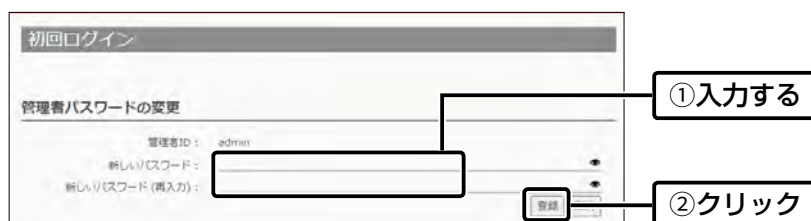
はじめて本製品をご使用になるときは、管理者パスワードの設定が必要です。
下記の手順で設定画面にアクセスして、設定してください。

- 1 WWWブラウザのアドレスバーに「http://192.168.0.1」を入力し、[Enter]キーを押します。
初回ログイン画面が表示されます。



※上図は、出荷時のIPアドレス(192.168.0.1)を入力した場合です。

- 2 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)で各項目を入力して、〈登録〉をクリックします。
※目のアイコン(右端)をクリックすると、入力したパスワードを確認できます。



- 3 サインイン画面が表示されたら、[ユーザー名]欄に「admin」、[パスワード]欄に手順2で設定したパスワードを入力し、〈サインイン〉をクリックします。
通常の設定画面に切り替わります。



※次回以降のアクセスでは、ユーザー名(admin)と設定したパスワードを入力してください。
※管理者パスワードを忘れた場合は、工場出荷時(初期値)の状態に戻す必要があります。

WWWブラウザについて

動作確認済のWWWブラウザは、Microsoft Edge(Chromiumベース)です。
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。

保存場所について

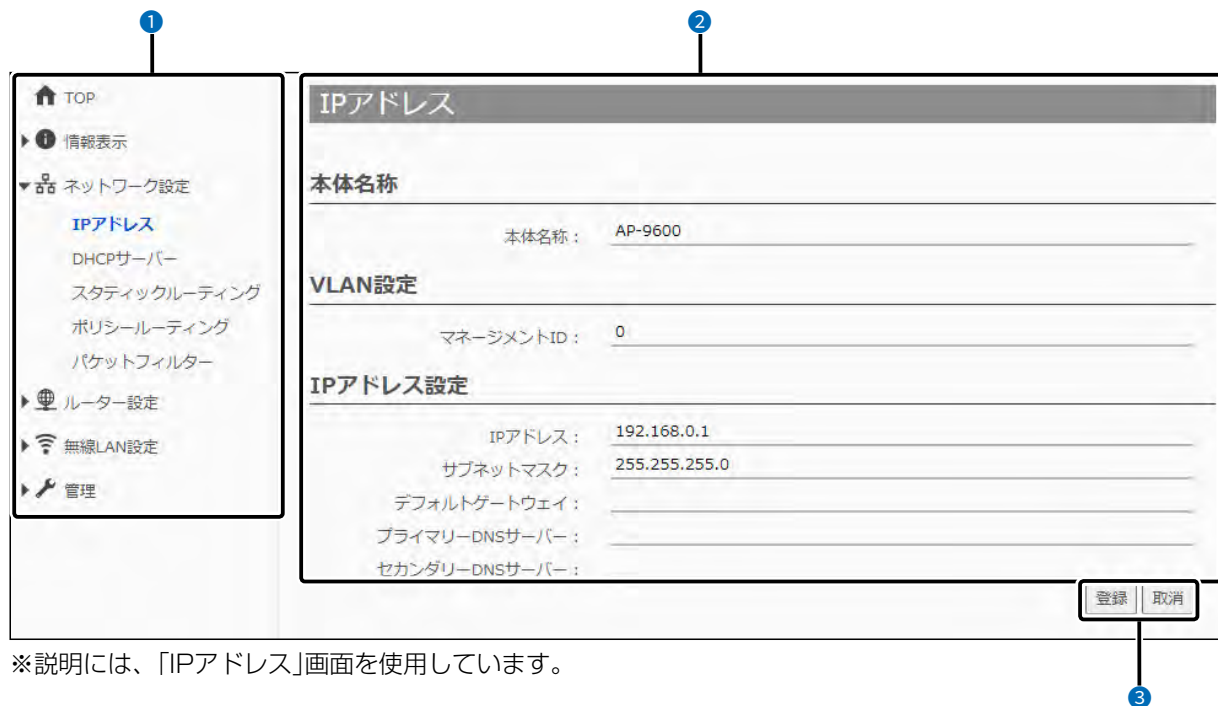
設定内容を保存すると、Microsoft Edge (Chromiumベース)の場合、デフォルトの設定では、「ダウンロード」フォルダーにファイルが保存されます。
必要に応じて、WWWブラウザの設定で、デスクトップなど任意の場所に変更してください。

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、5-7ページをご覧ください。



※説明には、「IPアドレス」画面を使用しています。

- 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

ICOM AP-9600

TOP

情報表示

ネットワーク設定

IPアドレス

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

IPsecトンネル

IPアドレス

本体名称

本体名称： AP-9600

VLAN設定

マネージメントID： 0

設定画面：中

ICOM AP-9600

IPアドレス

本体名称

本体名称： AP-9600

VLAN設定

マネージメントID： 0

IPアドレス設定

設定画面：小

ICOM AP-9600

IPアドレス

本体名称

本体名称： AP-9600

VLAN設定

マネージメントID： 0

IPアドレス設定

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

「≡」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。

本体名称
本体名称: AP-9500

VLAN設定
マネージメントID: 0

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:
プライマリDNSサーバー:
セカンダリDNSサーバー:

登録

※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.1-17)
※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」(サブネットマスク「255.255.255.0」)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
■ 無線通信機能を有効にするには	2-2
■ 無線ネットワーク名を手動で設定する	2-3
■ 暗号化を手動で設定する	2-4
■ MACアドレスフィルタリングを設定するには	2-5
■ 自動チャンネルを設定するときは	2-6
■ 80MHz帯域幅通信をするときは	2-8
2. 無線LAN接続[活用編]	2-9
■ 仮想APを設定するには	2-9
■ 無線AP間通信機能(WBR)を使用する場合	2-10
■ アカウンティング設定について	2-14
■ RADIUS設定について	2-15

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 > 無線LAN

■ 無線通信機能を有効にするには

無線LAN1 (5GHz帯) を例に無線通信機能を有効にする手順を説明します。

※出荷時や全設定初期化時、本製品の無線UNITは「無効」に設定されています。

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 [無線UNIT] 欄で「有効」を選択します。 (出荷時の設定：無効)

無線LAN	
無線UNIT :	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
帯域幅 :	20 MHz
チャンネル :	036 CH (5180 MHz)
パワーレベル :	高
DTIM間隔 :	1

登録 取消

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

■ 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 (5GHz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 入力する

VLAN ID : 0

ANY接続拒否 : 無効 有効 ANYによるアクセスを防止するときは、「有効」をクリックします。(出荷時の設定 : 無効)

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

暗号化設定

ネットワーク認証 : オープンシステム

暗号化方式 : なし

- 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、出荷時の設定で使用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

■ 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 (5GHz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 : WPA2-PSK/WPA3-SAE
暗号化方式 : AES
PSK (Pre-Shared Key) : wirelessmaster

- 1 [ネットワーク認証]欄で「WPA2-PSK/WPA3-SAE」、[暗号化方式]欄で「AES」を選択し、[PSK (Pre-Shared Key)]欄で「wirelessmaster」(半角)を入力します。

※目のアイコン(右端)をクリックすると、入力したパスワードを確認できます。

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

アカウントिंग : 無効 有効

暗号化設定

ネットワーク認証 : WPA2-PSK/WPA3-SAE

暗号化方式 : AES

PSK (Pre-Shared Key) : wirelessmaster

WPAキー更新間隔 : 120 分

登録 取消

① 選択する

② 入力する

※目のアイコン(右端)をクリックすると、入力した内容を確認できます。

- 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]

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

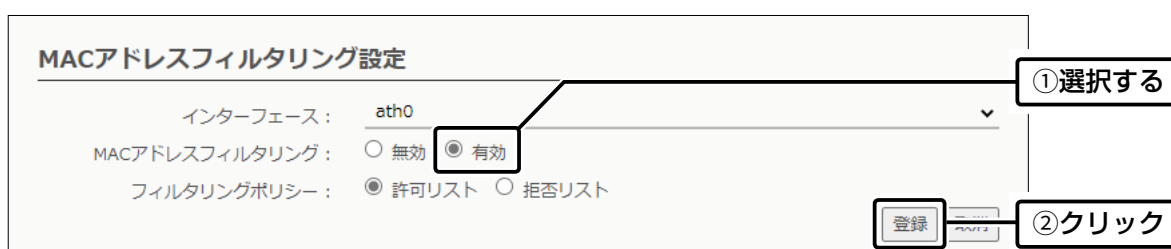
仮想APごとに、本製品への接続を許可する、または拒否する無線LAN端末を登録できます。

※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(5GHz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。



- 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(052～144)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。

5GHz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：036CH (5180MHz))

The image shows two screenshots of the wireless LAN settings interface. The top screenshot shows the '無線LAN' (Wireless LAN) settings page with the following options: 無線UNIT: 無効 (radio button), 有効 (radio button, selected); 帯域幅: 20 MHz; チャンネル: 自動; パワーレベル: 高; DTIM間隔: 1. A blue box highlights the '20 MHz' band width, with an arrow pointing to it and the text '出荷時の設定であることを確認します。' (Confirm that it is the factory setting). A box labeled '① 選択する' (Select) points to the '自動' channel dropdown. A box labeled '② クリック' (Click) points to the '登録' (Register) button.

The bottom screenshot shows the same settings page after the '登録' button is pressed. The 'チャンネル' dropdown now shows '自動' and '使用中チャンネル: 100 CH (5500 MHz)'. A box labeled '③ 確認する' (Confirm) points to the '自動' channel dropdown. The '登録' button is now disabled, and a '取消' (Cancel) button is visible.

ご注意

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(100～144)に設定してご使用ください。

※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。

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

2.4GHz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：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

登録

① 選択する

② クリック



無線LAN

無線UNIT : 無効 有効

帯域幅 : 20 MHz

チャンネル : 自動

使用中チャンネル: 006 CH (2437 MHz)

パワーレベル : 高

DTIM間隔 : 1

登録 取消

③ 確認する

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LAN

■ 80MHz帯域幅通信をするときは

IEEE802.11ax規格を使用できるのは、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2402Mbps（理論値）で使用するには、無線LAN1（5GHz帯）で帯域幅を「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LAN1」、「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)

The screenshot shows the '無線LAN' (Wireless LAN) settings page. The '無線UNIT' (Wireless Unit) is set to '有効' (Enabled). The '帯域幅' (Channel Width) is set to '80 MHz', which is highlighted with a box and a '選択する' (Select) button. The 'チャンネル' (Channel) is '036 CH (5180 MHz)', 'パワーレベル' (Power Level) is '高' (High), and 'DTIM間隔' (DTIM Interval) is '1'. There are '登録' (Register) and '取消' (Cancel) buttons at the bottom right.

3 「登録」をクリックします。

40/80MHz帯域幅通信をする時の手引き

◎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

2. 無線LAN接続 [活用編]

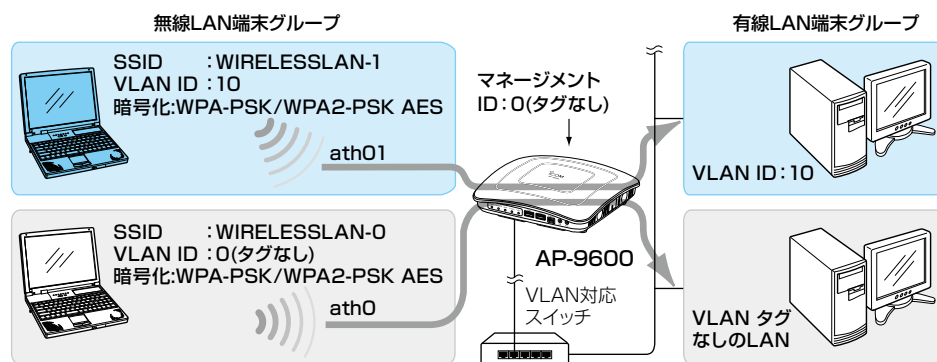
無線LAN設定 > 無線LAN1/無線LAN2 > 仮想AP

■ 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.1-11)

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。

① 選択する

② クリック

③ 入力する

④ 選択する

⑤ 入力する

⑥ クリック

※目のアイコン(右端)をクリックすると、入力した内容を確認できます。

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)

■ 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.1-10)

※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.2-6)、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、「036 CH (5180 MHz)」(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ときは」で設定されているものとします。(P.1-21)

親機(P.2-12)

[無線LAN設定]項目	チャンネル	: 「036 CH (5180 MHz)」(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.2-13)

[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。

親機側の設定	子機側の設定
チャンネル : 036 CH (5180 MHz)	SSID : WIRELESSLAN-0
仮想AP : ath0	ネットワーク認証 : WPA2-PSK
SSID : WIRELESSLAN-0	暗号化方式 : AES
ネットワーク認証 : WPA2-PSK	PSK : wirelessmaster
暗号化方式 : AES	
PSK : wirelessmaster	
接続先BSSID : 1E-90-C7-00-00-03(子機のBSSID)	

※数値は、設定例です。



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 > AP間通信 (WBR)

■ 無線AP間通信機能(WBR)を使用する場合

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

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)： ●●●●●●●●

WPAキー更新間隔： 120 分

登録 取消

AP-9600の無線AP間通信で使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

※目のアイコン(右端)をクリックすると、入力した内容を確認できます。

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 取消

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

子機のBSSIDを親機側に登録します。

(次ページにつづく)

2 導入ガイド

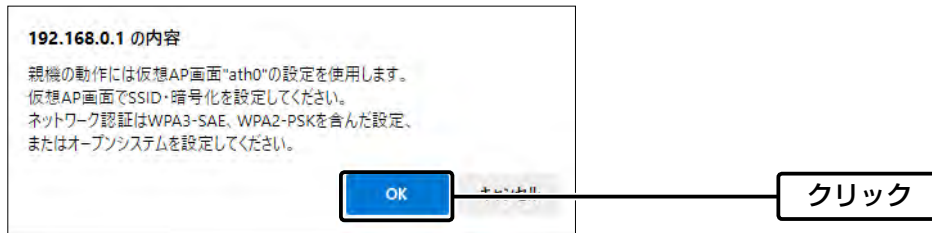
2. 無線LAN接続[活用編]

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

親機を設定する

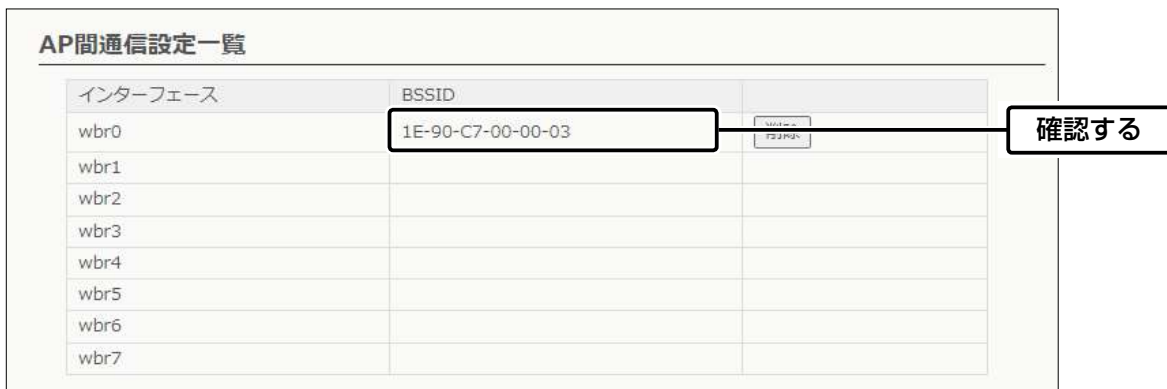
5 <OK>をクリックします。



※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。



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

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: []

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): []

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

※目のアイコン(右端)をクリックすると、入力した内容を確認できます。

親機側に登録するBSSIDです。

3 <OK>をクリックします。

192.168.0.1 の内容

子機に設定すると仮想AP"ath07"は使用できなくなります。
設定してもよろしいですか?

OK キャンセル

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

■ 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 (5GHz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

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

アドレス:

ポート: 1813 1813

シークレット:

登録 取消

① 設定する

② クリック

※目のアイコン(右端)をクリックすると、入力した内容を確認できます。

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 > 仮想AP

■ RADIUS設定について

ネットワーク認証(WPA/WPA2/WPA3/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 (5GHz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

アカウントリング: 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:

登録 取消

① 設定する

② クリック

※目のアイコン(右端)をクリックすると、入力した内容を確認できます。

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	3-17
■ 静的DHCPサーバー設定一覧	3-17
「スタティックルーティング」画面	3-18
■ IP経路情報	3-18
■ スタティックルーティング設定	3-19
■ スタティックルーティング設定一覧	3-19
「ポリシールーティング」画面	3-20
■ 送信元ルーティング設定	3-20
■ 送信元ルーティング設定一覧	3-20
「パケットフィルタ」画面	3-21
■ パケットフィルタ設定	3-21
■ パケットフィルタ設定一覧	3-33
パケットフィルタの使用例について	3-34
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	3-35
② AP-9600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	3-36
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	3-37

3 設定画面について

下記は、前ページからの「つづき」です。

ルーター設定

「WAN接続先」画面	3-38
■ 回線状態表示 [DHCPクライアント設定時]	3-38
■ 回線状態表示 [固定IP設定時]	3-39
■ 回線状態表示 [PPPoE設定時]	3-40
■ 回線種別設定	3-41
■ 回線設定 [DHCPクライアント設定時]	3-42
■ 回線設定 [固定IP設定時]	3-43
■ 回線設定 [PPPoE設定時]	3-44
■ 回線設定一覧 [PPPoE設定時]	3-46
「アドレス変換」画面	3-47
■ アドレス変換設定	3-47
■ DMZホスト設定	3-47
■ 静的マスカレードテーブル設定	3-48
■ 静的マスカレードテーブル設定一覧	3-49
「IPフィルター」画面	3-50
■ 一般設定	3-50
■ IPフィルター設定	3-51
■ IPフィルター設定一覧	3-57
「簡易DNS」画面	3-58
■ 簡易DNSサーバー設定	3-58
■ 簡易DNSサーバー設定一覧	3-58
「VPN」画面	3-59
■ IPsec設定	3-59
■ IPsecトンネル設定	3-60
■ IPsecトンネル設定一覧	3-62
■ IPsecトンネル設定例(1)	3-63
■ IPsecトンネル設定例(2)	3-64

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	3-65
■ 無線LAN	3-65
「仮想AP」画面	3-67
■ 仮想AP設定	3-67
■ 暗号化設定	3-70
■ RADIUS設定	3-77
■ アカウンティング設定	3-78
「MACアドレスフィルタリング」画面	3-79
■ MACアドレスフィルタリング設定	3-79
■ 端末MACアドレスリスト	3-80
■ MACアドレスフィルタリング設定一覧	3-81
「AP間通信 (WBR)」画面	3-82
■ AP間通信設定	3-82
■ 親機設定	3-83
■ AP間通信設定一覧	3-84
■ 子機設定	3-85
「WMM詳細」画面	3-88
■ WMM詳細設定	3-88
■ WMMパワーセーブ設定	3-92
「ARP代理応答」画面	3-93
■ ARP代理応答設定	3-93
■ ARPキャッシュ情報	3-94

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	3-95
■ 管理者パスワードの変更	3-95
「管理ツール」画面	3-96
■ USB設定	3-96
■ HTTP/HTTPS設定	3-98
■ HTTP/HTTPS設定後、設定画面にアクセスできなくなったときは	3-99
■ Telnet/SSH設定	3-100
「時計」画面	3-102
■ 時刻設定	3-102
■ 自動時計設定	3-103
「SYSLOG」画面	3-104
■ SYSLOG設定	3-104
「SNMP」画面	3-105
■ SNMP設定	3-105
■ SNMPv3設定	3-106
「LED」画面	3-107
■ LED消灯モード	3-107
「ネットワークテスト」画面	3-108
■ PINGテスト	3-108
■ 経路テスト	3-109
「再起動」画面	3-110
■ 再起動	3-110
「設定の保存/復元」画面	3-111
■ 設定の保存	3-111
■ 設定の復元	3-111
■ 設定内容一覧	3-112
「初期化」画面	3-113
■ 初期化	3-113
「ファームウェアの更新」画面	3-114
■ ファームウェア情報	3-114
■ オンライン更新	3-115
■ 自動更新	3-116
■ 手動更新	3-117

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、時刻、稼働時間、メモリー使用量、PoEステータスが表示されます。

システム情報	
本体名称	AP-9600
バージョン	
国名コード	JP
現在時刻	
稼働時間	
メモリー使用量	296528 kB / 821908 kB (36% 使用中)
PoEステータス	ACアダプター

※上図は、ACアダプターを接続している場合の表示例です。

PoEから受電している場合は、そのPoE規格(IEEE 802.3af、IEEE 802.3at、IEEE 802.3bt)が表示されます。

TOP

■ MACアドレス

本製品のMACアドレス(WAN/LAN/無線)が表示されます。

MACアドレス	
WAN/LAN1	00-90-C7-XXXXXX
LAN2	00-90-C7-XXXXXX
無線LAN1	00-90-C7-XXXXXX
無線LAN2	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

本製品の各ポートについて、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
WAN/LAN1	00-90-C7- <small>XXXXXXXXXX</small>	1000BASE-T full-duplex
LAN2	00-90-C7- <small>XXXXXXXXXX</small>	リンクダウン

※本製品の[WAN/LAN1]ポート、[LAN2]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-.....
ath1	WIRELESSLAN-0	00-90-C7-.....

※[無線LAN]項目の[無線UNIT]欄(P.3-65)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.3-67)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	接続先BSSID
wbr0

※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.3-83)

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られた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
.....	192.168.0.30
.....	192.168.0.11

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。

日付・時間	レベル	内容
01-21 20:47:28	INFO	soc0: IEEE 802.11axg: detected a roaming STA CA-EE-F5-16-19-0E

- 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)で絞りこんだ内容を保存します。
※クリックして、表示された画面にしたがって操作すると、ログ情報をテキスト形式(拡張子：txt)で保存できます。
- 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LAN1 36 CH (5180 MHz)	ath0	00-90-C7- [マスキング]	WIRELESSLAN-0	WPA2-PSK (AES)
無線LAN2 1 CH (2412 MHz)	ath1	00-90-C7- [マスキング]	WIRELESSLAN-0	WPA-PSK/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	[マスキング]	192.168.0.27	53	173.3 Mbps	6.0 Mbps	<input type="button" value="詳細"/>

※仮想APのARP代理応答機能(P.3-93)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:	ath0
MACアドレス:	
IPアドレス:	192.168.0.27
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:	 50
速度:	送信 6.0 Mbps / 受信 173.3 Mbps
WMMパワーセーブ:	無効
接続時間:	0 day 00:00:41

※ [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	接続先BSSID	RSSI	受信速度	送信速度	
wbr8	00-90-C7- 	28	34.4 Mbps	229.4 Mbps	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「wbr8」(無線LAN2))



※ 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：	1E-90-C7- 
通信モード：	IEEE 802.11ax
SSID：	WIRELESSLAN-0
暗号化：	WPA2-PSK (AES)
チャンネル：	1 CH (2412 MHz)
信号レベル：	 28
レート：	送信 34.4 Mbps / 受信 172.1 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 : <input type="text" value="AP-9600"/>

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-9600)
※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 : <input type="text" value="0"/>

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。
※WAN側などのデフォルトゲートウェイが有効になった場合、この欄で設定した経路は無効になります。
- 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。

※ 9、10は [DNS代理応答] 欄を「無効」に設定した場合に表示されません。

DHCPサーバー設定

DHCPサーバー： 1 無効 有効

割り当て開始IPアドレス： 2 _____

割り当て個数： 3 30 _____ 個

サブネットマスク： 4 _____

リース期間： 5 72 _____ 時間

ドメイン名： 6 _____

デフォルトゲートウェイ： 7 _____

DNS代理応答： 8 無効 有効

プライマリーDNSサーバー： 9 _____

セカンダリーDNSサーバー： 10 _____

プライマリーWINSサーバー： 11 _____

セカンダリーWINSサーバー： 12 _____

13 14
登録 取消

- 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] 欄と [割り当て個数] 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] 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] 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。

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

※9、10は[DNS代理応答]欄を「無効」に設定した場合に表示されます。

DHCPサーバー設定

DHCPサーバー：1 無効 有効

割り当て開始IPアドレス：2 _____

割り当て個数：3 30 _____ 個

サブネットマスク：4 _____

リース期間：5 72 _____ 時間

ドメイン名：6 _____

デフォルトゲートウェイ：7 _____

DNS代理応答：8 無効 有効

プライマリDNSサーバー：9 _____

セカンダリDNSサーバー：10 _____

プライマリWINSサーバー：11 _____

セカンダリWINSサーバー：12 _____

13 14
登録 取消

- 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。
- 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。
※[DNS代理応答]欄を「有効」に設定している場合は、この欄と[セカンダリDNSサーバー]欄は表示されず、本製品がプライマリDNSサーバーとして通知されます。
- 10 セカンダリDNSサーバー …… [プライマリDNSサーバー]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。

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

※⑨、⑩は[DNS代理応答]欄を「無効」に設定した場合に表示されます。

DHCPサーバー設定

DHCPサーバー：① 無効 有効

割り当て開始IPアドレス：② _____

割り当て個数：③ 30 _____ 個

サブネットマスク：④ _____

リース期間：⑤ 72 _____ 時間

ドメイン名：⑥ _____

デフォルトゲートウェイ：⑦ _____

DNS代理応答：⑧ 無効 有効

プライマリDNSサーバー：⑨ _____

セカンダリDNSサーバー：⑩ _____

プライマリWINSサーバー：⑪ _____

セカンダリWINSサーバー：⑫ _____

⑬ 登録 ⑭ 取消

- ⑪ **プライマリ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WINSサーバー** … [プライマリWINSサーバー]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	
<input type="text"/>	<input type="text"/>	<input type="button" value="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	
<input type="text"/>	192.168.0.50	<input type="button" value="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LANの場合
◎eth0 : インターフェースがWAN側の場合
◎ppp0～ppp7 : インターフェースがWAN側PPPoEの場合
◎vti0～vti31 : インターフェースがIPsec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64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 [経路] 欄で「ゲートウェイを設定」を選択した場合に、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)」、「vti0～vti31」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	
192.168.10.0	255.255.255.0	192.168.0.254		① 編集 ② 削除
127.0.0.0	255.0.0.0	127.0.0.1		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.3-41)のときに使用する設定です。

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..... [経路]欄で「ゲートウェイを設定」を選択した場合に、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 対象となる送信元IPアドレスから送られてきたパケットの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)」、「vti0~vti31」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が表示されます。
※画面の値は、入力例です。

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。

パケットフィルター設定

番号 : ① _____ ▼

エントリー : 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

- 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

パケットフィルター設定

番号 : ①

エントリー : 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

宛先インターフェース : ⑥

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

⑩ 登録 ⑪ 取消

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 : 本製品自身の場合
 - ◎eth0 : 有線LAN(WAN/LAN1)の場合
※「WAN接続先」画面の回線種別(P.3-41)を「LANポートとして使用する」に設定しているときだけ、フィルタリング条件に一致します。
 - ◎eth1 : 有線LAN(LAN2)の場合
 - ◎ath0、ath01～ath07 : 本製品の無線LAN1(5GHz帯仮想AP)の場合
 - ◎ath1、ath11～ath17 : 本製品の無線LAN2(2.4GHz帯仮想AP)の場合
 - ◎wbr0～wbr17 : AP間通信(WBR)の場合
- ※「すべて」を選択すると、「br-lan」、「eth0」、「eth1」、「ath0、ath01～ath07」、「ath1、ath11～ath17」、「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 : 本製品自身の場合
 - ◎eth0 : 有線LAN(WAN/LAN1)の場合
※「WAN接続先」画面の回線種別(P.3-41)を「LANポートとして使用する」に設定しているときだけ、フィルタリング条件に一致します。
 - ◎eth1 : 有線LAN(LAN2)の場合
 - ◎ath0、ath01～ath07 : 本製品の無線LAN1(5GHz帯仮想AP)の場合
 - ◎ath1、ath11～ath17 : 本製品の無線LAN2(2.4GHz帯仮想AP)の場合
 - ◎wbr0～wbr17 : AP間通信(WBR)の場合
- ※「すべて」を選択すると、「br-lan」、「eth0」、「eth1」、「ath0、ath01～ath07」、「ath1、ath11～ath17」、「wbr0～wbr17」が宛先インターフェースの対象になります。

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

パケットフィルター設定

番号: ①

エントリー: 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

宛先インターフェース: ⑥

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

⑩ 登録 ⑪ 取消

- 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]欄(⑧)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。

- 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.3-33)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.3-33)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。

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

パケットフィルター設定

番号: ①

エントリー: 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

宛先インターフェース: ⑥

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

⑩ 登録 ⑪ 取消

⑧ 宛先MACアドレス/マスク(つづき)

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.3-33)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。

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 : 3-25ページ～3-29ページ

◎ARP : 3-30ページ

◎IPv4 : 3-31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

[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パケットについて、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 : 3-26ページ
◎IPv4 : 3-27ページ～3-29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

[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、「0～65535」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、ターゲット 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、ターゲット 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

[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。

The screenshot shows the configuration interface for a packet filter. It is organized into three main sections:

- 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

[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

[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送信元の 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

[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、「0～65535」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、ターゲット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、ターゲット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

[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

[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送信元の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。

番号	項目	詳細	
1	エントリー	無効	① 編集
	ログ出力	有効	
	フィルター方法	透過	② 削除
	送信元インターフェース	すべて	
	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.3-21)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

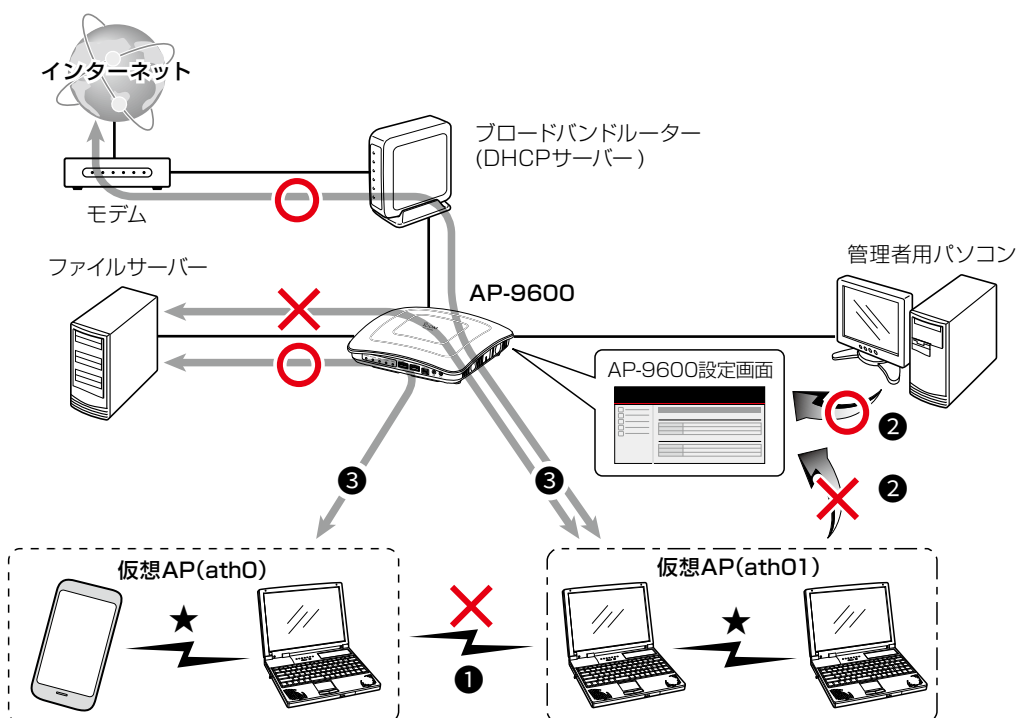
ネットワーク設定 > パケットフィルター

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.3-35)
- ② AP-9600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.3-36)
- 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.3-37)

※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.3-69)

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.3-69)

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」画面で設定したフィルターの番号を表示

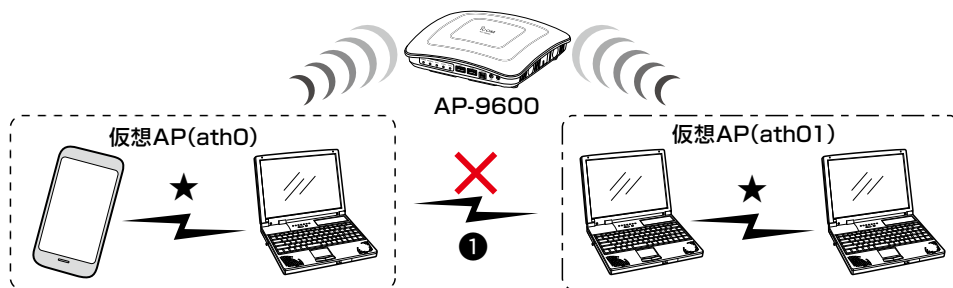
上記のフィルターで登録した番号と異なる番号を表示

番号	項目	詳細	
★	エントリー	有効	編集
	ログ出力	無効	
	フィルター方法	遮断	削除
	送信元インターフェース	ath0	
	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 仮想AP(ath0)→仮想AP(ath01)方向の通信を遮断

番号	項目	詳細	
★	エントリー	有効	編集
	ログ出力	無効	
	フィルター方法	遮断	削除
	送信元インターフェース	ath01	
	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	

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-9600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設定一覧

番号	項目	詳細	
1	エントリー	有効	<div style="display: flex; flex-direction: column; align-items: center;"> <div style="margin-bottom: 10px;">編集</div> <div>削除</div> </div>
	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. /	
	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	

番号	項目	詳細	
2	エントリー	有効	<div style="display: flex; flex-direction: column; align-items: center;"> <div style="margin-bottom: 10px;">編集</div> <div>削除</div> </div>
	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	

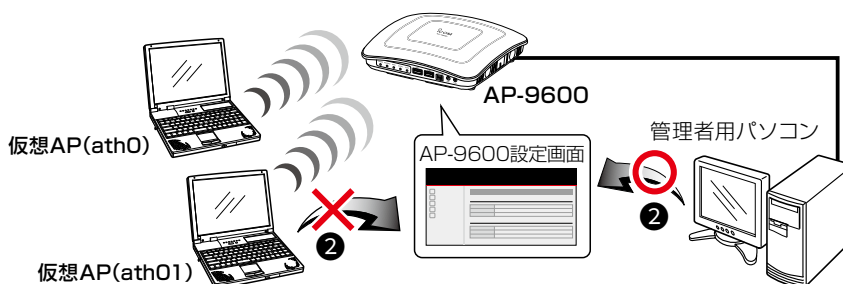
「パケットフィルター」画面で設定したフィルターの番号を表示

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 管理用端末以外からのWEBアクセスを遮断



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

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。

※下記の図は、ブロードバンドルーターを[LAN2]ポートに接続した場合の例です。

[WAN/LAN1]ポートに接続する場合は、送信元インターフェースに「eth0」を指定してください。

パケットフィルター設定一覧

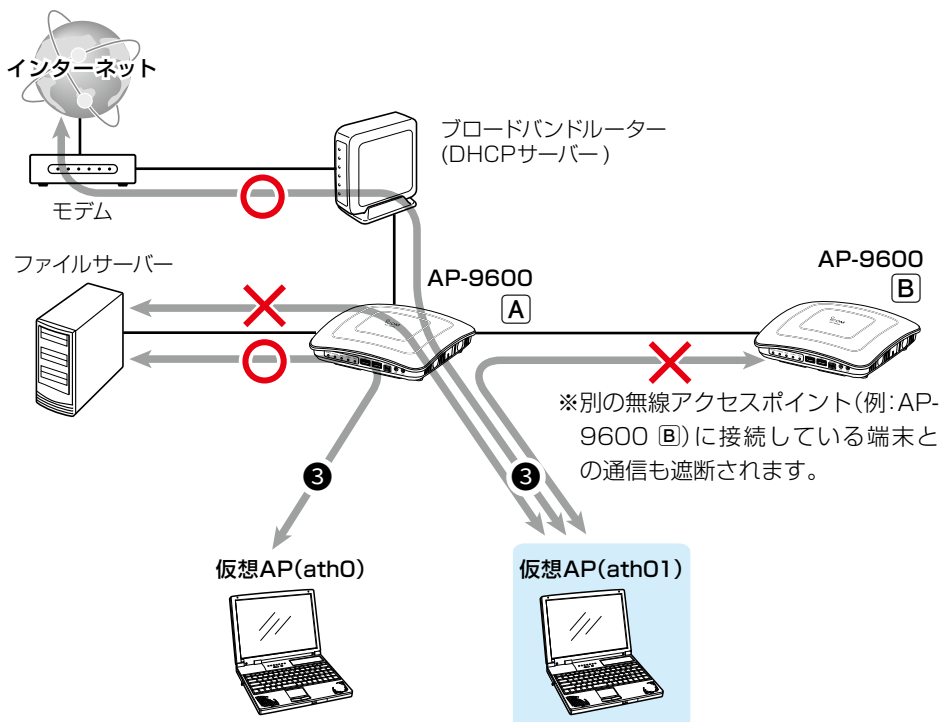
番号	項目	詳細		
1	エントリー	有効	編集 削除	
	ログ出力			
	フィルター方法	透過		
	送信元インターフェース	eth1		
	宛先インターフェース	ath01		
	送信元 MAC アドレス / マスク	00-00-06 / FF-FF-FF-FF-FF-FF		
	宛先 MAC アドレス / マスク	すべて		
	Ethernet タイプ	すべて		
	エントリー	有効		編集 削除
	ログ出力			
	フィルター方法	遮断		
	送信元インターフェース	すべて		
	宛先インターフェース	ath01		
	送信元 MAC アドレス / マスク	すべて		
	宛先 MAC アドレス / マスク	すべて		
	Ethernet タイプ	すべて		

「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

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

「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.3-41)、[回線設定]項目(P.3-42)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、表示例です。

1 接続状態	接続中
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アドレスを表示します。
- 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
ず。

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.3-41)、[回線設定]項目(P.3-43)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、表示例です。

1 接続状態	接続中
2 回線種別	固定IP
3 本体側のIPアドレス	XXXXXXXXXX
4 相手先のIPアドレス	XXXXXXXXXX
5 DNSサーバー	XXXXXXXXXX

- 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.3-41)、[回線設定]項目(P.3-44)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、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 ▼ 切断	なし ▼ 接続
2 接続状態	接続中	
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.3-44)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。

- 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[WAN/LAN1]ポートをWANポートとして使用できます。
- ◎回線を本製品のWAN側ポートに接続しない場合
LANポートとして使用する
LANポートに切り替わり、HUBやルーターなどのネットワーク機器と接続できます。
- ◎回線を本製品のWAN側ポートに接続する場合
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できます。
- 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.3-41)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

接続先名 : ① _____

プライマリDNSサーバー : ② _____

セカンダリDNSサーバー : ③ _____

④ 登録 ⑤ 取消

- 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]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.3-38)

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.3-41)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

接続先名 : ① _____

IPアドレス : ② _____

サブネットマスク : ③ _____

デフォルトゲートウェイ : ④ _____

プライマリーDNSサーバー : ⑤ _____

セカンダリーDNSサーバー : ⑥ _____

⑦ 登録 ⑧ 取消

- | | |
|-----------------|--|
| 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]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]

回線設定

接続先の選択 : ① WAN01 (ppp0) ▼

接続先名 : ② WAN01

ユーザーID : ③ [REDACTED]

パスワード : ④ [REDACTED] 👁

接続方法 : ⑤ 常時 ▼

IPアドレス : ⑥

プライマリDNSサーバー : ⑦

セカンダリ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DNSサーバー** …… [プライマリDNSサーバー]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」(出荷時の設定)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。

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 [REDACTED]

パスワード : ④ [REDACTED] 👁

接続方法 : ⑤ 常時 ▼

IPアドレス : ⑥

プライマリDNSサーバー : ⑦

セカンダリ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

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。

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.3-44)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)	[REDACTED]	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。

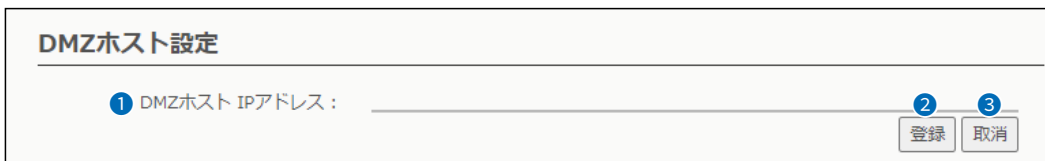


アドレス変換…………… 本製品のアドレス変換機能を設定します。 (出荷時の設定：有効)
「有効」に設定すると、本製品のIPマスカレード機能を使用して、WAN側グローバルアドレスをプライベートアドレスに変換します。

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。



- 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パケットを、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	
<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP ▼	追加 ⑤

- ① WAN側ポート 選択したプロトコル(④)に対するWAN側ポート番号を入力します。
- 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側ポート番号を入力します。
- 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。

3 設定画面について

「アドレス変換」画面

ルーター設定 > アドレス変更

■ 静的マスカレードテーブル設定一覧

[静的マスカレードテーブル設定]項目で登録した内容を表示します。

※画面の内容は、設定例です。

WAN側ポート	LAN側IP	LAN側ポート	プロトコル	①	②
11	192.168.0.10	4011	TCP	編集	削除
22	192.168.0.10	8022	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 <取消> 「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。

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：無効)
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	* (*)	無効	編集	削除
	IN		* (*)			

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 1

エントリー: ② 無効 有効

フィルター方法: ③ 遮断 透過

フィルター方向: ④ IN OUT

送信元IPアドレス: ⑤ _____ マスク: 32

宛先IPアドレス: ⑥ _____ マスク: 32

プロトコル: ⑦ TCP 指定時: _____

送信元ポート番号: ⑧ _____ ~ _____

宛先ポート番号: ⑨ _____ ~ _____

SYSLOGに出力: ⑩ 無効 有効

⑪ 登録 ⑫ 取消

- 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。
- 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。

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 1

エントリー: ② 無効 有効

フィルター方法: ③ 遮断 透過

フィルター方向: ④ IN OUT

送信元IPアドレス: ⑤ _____ マスク: 32

宛先IPアドレス: ⑥ _____ マスク: 32

プロトコル: ⑦ TCP

指定時: _____

送信元ポート番号: ⑧ _____ ~ _____

宛先ポート番号: ⑨ _____ ~ _____

SYSLOGに出力: ⑩ 無効 有効

⑪ 登録 ⑫ 取消

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(つづき) ◎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送信元のTCP/UDPポート番号を指定する項目です。
(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。

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。
(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。

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 1

エントリー: ② 無効 有効

フィルター方法: ③ 遮断 透過

フィルター方向: ④ IN OUT

送信元IPアドレス: ⑤ _____ マスク: 32

宛先IPアドレス: ⑥ _____ マスク: 32

プロトコル: ⑦ TCP

送信元ポート番号: ⑧ _____ ~ _____

宛先ポート番号: ⑨ _____ ~ _____

SYSLOGに出力: ⑩ 無効 有効

⑪ 登録 ⑫ 取消

- ⑩ **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。
- ⑪ **〈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。
- ⑫ **〈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.3-51～P.3-56)から登録した現在の各エントリーの内容を表示します。

番号	フィルター方法 フィルター方向	プロトコル	送信元IPアドレス (送信元ポート番号) 宛先IPアドレス (宛先ポート番号)	SYSLOGに出力	① 編集	② 削除
59	遮断	TCP/UDP	* (135)	無効	編集	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	* (*)	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、表示された内容を[IPフィルター設定]項目の各欄に表示します。
- 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
<input type="text"/>	<input type="text"/>
<input type="button" value="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」を登録しておくこと、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サーバー設定一覧

[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	<input type="text"/>
<input type="button" value="削除"/>	

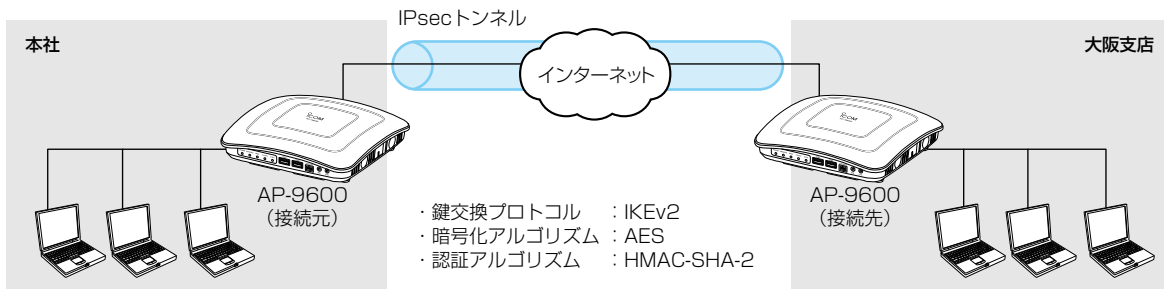
登録した内容を取り消すときは、該当する欄の「削除」をクリックします。

3 設定画面について

「VPN」画面

VPN(Virtual Private Network)機能を使用すると、インターネット上の2地点を暗号化通信で接続して、仮想的なネットワークを構成できます。

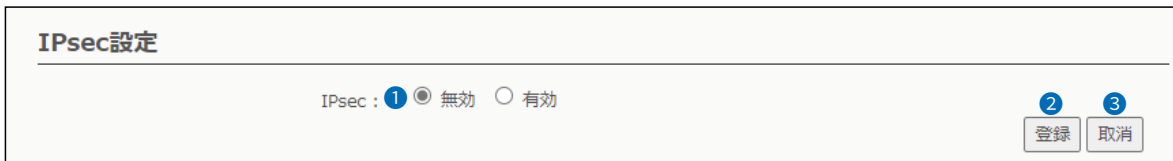
※本製品のVPN機能は、AP-9500、SR-7100VN、SR-8000V、VE-PG4と互換性があります。(2023年4月現在)
※接続先に合わせて、IPsecトンネルを登録してください。(P.3-63、P.3-64)



ルーター設定 > VPN

■ IPsec設定

IPsecによる仮想プライベートネットワーク(VPN)接続を使用するための設定です。

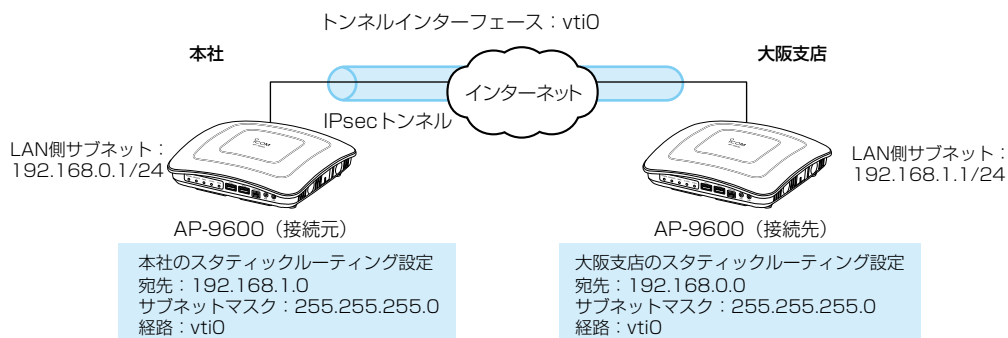


- ① IPsec..... 本製品のIPsec機能を設定します。 (出荷時の設定：無効)
「有効」に設定すると、IPsecトンネルを使用したVPN接続を利用できます。
- ② <登録> 「IPsec設定」項目で設定した内容を登録するボタンです。
- ③ <取消> 「IPsec設定」項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお、<登録>をクリックすると、変更前の状態には戻りません。

ご参考

VPN機能を使用する場合は、本製品の[WAN/LAN1]ポートにWAN回線を接続し、ルーター機能(回線種別)、スタティックルーティングの設定(P.3-19)が必要です。

スタティックルーティングの設定例



3 設定画面について

「VPN」画面

ルーター設定 > VPN

■ IPsecトンネル設定

IPsecによる仮想プライベートネットワーク(VPN)接続を使用するための設定です。

- ① **トンネルインターフェース** …… IPsecトンネルを登録するインターフェースを指定します。
(出荷時の設定：vti0)
選択できる範囲は「vti0～vti31」です。
- ② **トンネル** …… 登録するIPsecトンネル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。
- ③ **トンネル名** …… IPsecトンネルを識別する名称を半角31(全角31)文字以内で入力します。
- ④ **インターフェース** …… 接続先と通信するインターフェースを選択します。(出荷時の設定：eth0)
◎eth0
「WAN接続先」画面の回線種別(P.3-41)を「固定IP」、または「DHCPクライアント」に設定しているときに選択します。
◎ppp0(WAN1)～ppp7(WAN8)
「WAN接続先」画面の回線種別(P.3-41)を「PPPoE」に設定しているときに選択します。
- ⑤ **認証鍵(Pre-Shared Key)** …… 接続先との認証に使用します。
接続先の機器と同じ文字列を半角128文字以内の英数字で入力します。
※目のアイコン(右端)をクリックすると、入力した内容を確認できます。
- ⑥ **リモートアドレス** …… 接続先のWAN側IPアドレス、またはホスト名を入力します。
※接続先からのIPsec接続を待ち受ける場合は、[リモートアドレス]欄を空白のままにして登録します。
双方の機器に割り当てられたWAN側IPアドレスが動的の場合、どちらか一方がダイナミックDNSサービスに登録し、ホスト名を取得している必要があります。

3 設定画面について

「VPN」画面

ルーター設定 > VPN

■ IPsecトンネル設定

IPsecトンネル設定

トンネルインターフェース: ① vti0

トンネル: ② 無効 有効

トンネル名: ③

インターフェース: ④ eth0

認証鍵 (Pre-Shared Key): ⑤

リモートアドレス: ⑥

リモートID: ⑦ IPアドレス

ローカルID: ⑧ IPアドレス

⑨ 登録 ⑩ 取消

- ⑦ リモートID** 接続先の機器を識別するIDを設定します。
IDは、「IPアドレス」、「KEYID」、「FQDN」、「USER-FQDN」からタイプを選択します。 (出荷時の設定：IPアドレス)
 - ◎IPアドレス : IPアドレス形式
 - ◎KEYID : 半角256文字以内の英数字
 - ◎FQDN : 半角253文字以内のドメイン名
 - ◎USER-FQDN : 半角254文字以内のメールアドレス形式
入力例: user@xxxx.yyyy.zzzz
① 64文字以内
② 「xxxx」、「yyyy」、「zzzz」は、それぞれ63文字以内
- ⑧ ローカルID** 接続先の機器に提示するIDを設定します。
IDは、「IPアドレス」、「KEYID」、「FQDN」、「USER-FQDN」からタイプを選択します。 (出荷時の設定：IPアドレス)
 - ◎IPアドレス : IPアドレス形式
 - ◎KEYID : 半角256文字以内の英数字
 - ◎FQDN : 半角253文字以内のドメイン名
 - ◎USER-FQDN : 半角254文字以内のメールアドレス形式
入力例: user@xxxx.yyyy.zzzz
① 64文字以内
② 「xxxx」、「yyyy」、「zzzz」は、それぞれ63文字以内
- ⑨ <登録>** 「IPsecトンネル設定」項目で設定した内容を登録するボタンです。
- ⑩ <取消>** 「IPsecトンネル設定」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

「VPN」画面

ルーター設定 > VPN

■ IPsecトンネル設定一覧

IPsecによる仮想プライベートネットワーク(VPN)接続を使用するための設定です。

1 トンネルインターフェース	2 インターフェース	3 状態	4 リモートアドレス	5 リモートID	6 ローカルID	7 編集	8 削除
vti0	eth0	IPsec無効		IPアドレス	IPアドレス		

- 1 **トンネルインターフェース** …… インターフェース名(トンネル名)が表示されます。
- 2 **インターフェース** …………… トンネル送信元のインターフェース名が表示されます。
- 3 **状態** …………… IPsec接続の状態が表示されます。
 - 接続中**
IPsecトンネルが接続されている状態です。
 - 接続待機中**
トンネルの接続先からのIPsec接続試行を待っている状態です。
 - 接続試行中**
トンネルの接続先に対してIPsec接続試行を実行中です。
 - IPsec無効**
IPsec設定のIPsecが無効化されている状態です。
 - 無効**
IPsecトンネルが無効化されている状態です。
- 4 **リモートアドレス** …………… 接続先に設定されている相手先IPアドレス、またはホスト名が表示されます。
設定されていない場合は「-」が表示されます。
接続中は相手先IPアドレスが表示されます。
- 5 **リモートID** …………… IPsec接続に使用するID(相手側)が表示されます。
- 6 **ローカルID** …………… IPsec接続に使用するID(自分側)が表示されます。
- 7 **〈編集〉** …………… ボタンの左側に表示されたIPsecトンネルを編集するボタンです。
〈編集〉をクリックすると、表示された内容を含むIPsecトンネルの設定が、[IPsecトンネル設定]項目の各欄に表示されます。
- 8 **〈削除〉** …………… ボタンの左側に表示されたIPsecトンネルを削除するボタンです。

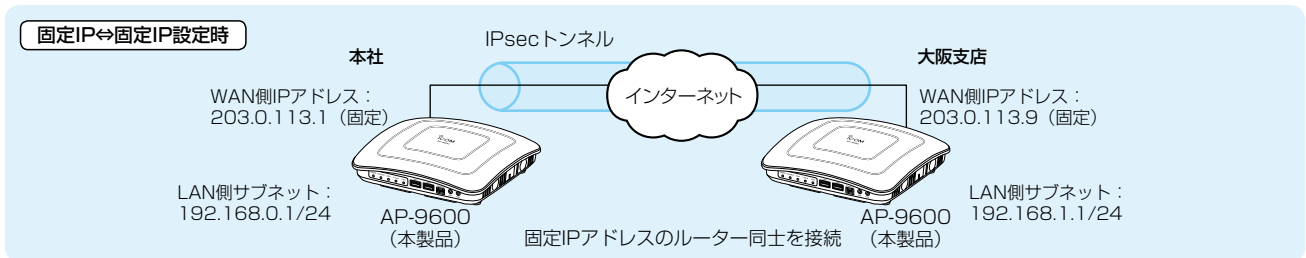
3 設定画面について

「VPN」画面

ルーター設定 > VPN

■ IPsecトンネル設定例(1)

本製品、接続先ともに、WAN側IPアドレスが固定で割り当てられ、回線種別がPPPoEの場合



※IPsecトンネルへの経路設定(スタティックルーティング)も必要です。(P.3-19、P.3-59)

本社側

IPsec設定

IPsec : 無効 有効

登録 取消

IPsecトンネル設定

トンネルインターフェース : vti0

トンネル : 無効 有効

トンネル名 : 大阪支店

インターフェース : ppp0 (WAN01)

認証鍵 (Pre-Shared Key) : ●●●●

リモートアドレス :

リモートID : KEYID ▼ osaka

ローカルID : KEYID ▼ honsha

登録 取消

認証鍵 (Pre-Shared Key) は、接続する機器同士で同じ文字列を入力します。

リモートIDには、接続先(大阪支店)のローカルIDを入力します。

「WAN接続先」画面で設定した接続先(PPPoE)を選択します。

リモートアドレスには、接続先(大阪支店)のWAN側IPアドレスを入力します。

大阪支店側

IPsec設定

IPsec : 無効 有効

登録 取消

IPsecトンネル設定

トンネルインターフェース : vti0

トンネル : 無効 有効

トンネル名 : 本社

インターフェース : ppp0 (WAN01)

認証鍵 (Pre-Shared Key) : ●●●●

リモートアドレス : 203.0.113.1

リモートID : KEYID ▼ honsha

ローカルID : KEYID ▼ osaka

登録 取消

リモートIDには、接続先(本社)のローカルIDを入力します。

リモートアドレスには、接続先(本社)のWAN側IPアドレスを入力します。

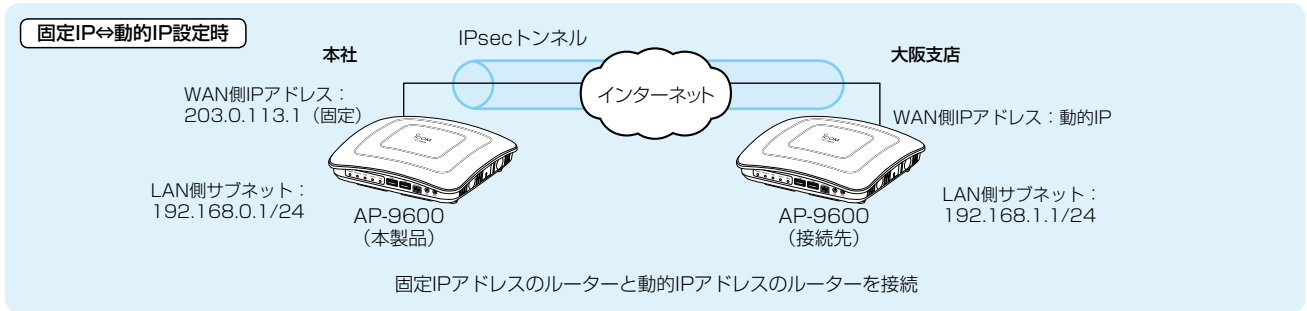
3 設定画面について

「VPN」画面

ルーター設定 > VPN

■ IPsecトンネル設定例(2)

本製品のWAN側IPアドレスが固定、接続先のWAN側IPアドレスが動的で割り当てられ、回線種別は本製品、接続先ともにPPPoEの場合



※IPsecトンネルへの経路設定(スタティックルーティング)も必要です。(P.3-19、P.3-59)

本社側

IPsec設定

IPsec : 無効 有効 登録 取消

IPsecトンネル設定

トンネルインターフェース : vti0

トンネル : 無効 有効

トンネル名 : 大阪支店

インターフェース : ppp0 (WAN01)

認証鍵 (Pre-Shared Key) : ●●●●

リモートアドレス : ●●●●

リモートID : KEYID ▼ osaka

ローカルID : KEYID ▼ honsha

登録 取消

「WAN接続先」画面で設定した接続先(PPPoE)を選択します。

接続先(大阪支店)のリモートアドレスを省略した場合、接続先からIPsec接続を開始する必要があります。 ※空欄にすると待機状態になり、自らIPsec接続を開始しません。

認証鍵 (Pre-Shared Key) は、接続する機器同士で同じ文字列を入力します。

リモートIDには、接続先(大阪支店)のローカルIDを入力します。

大阪支店側

IPsec設定

IPsec : 無効 有効 登録 取消

IPsecトンネル設定

トンネルインターフェース : vti0

トンネル : 無効 有効

トンネル名 : 本社

インターフェース : ppp0 (WAN01)

認証鍵 (Pre-Shared Key) : ●●●●

リモートアドレス : 203.0.113.1

リモートID : KEYID ▼ honsha

ローカルID : KEYID ▼ osaka

登録 取消

接続先(本社)のWAN側IPアドレスを、リモートアドレスに入力します。

リモートIDには、接続先(本社)のローカルIDを入力します。

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LAN1：5GHz帯

◎無線LAN2：2.4GHz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 : ③ 036 CH (5180 MHz)

パワーレベル : ④ 高

DTIM間隔 : ⑤ 1

登録 取消

⑥ ⑦

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：無効)
「有効」に設定すると、本製品の無線LAN機能を使用できます。(P.2-2)

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」、「80MHz」から選択できます。
◎無線LAN2：「20MHz」、「40MHz」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→036CH (5180MHz)
無線LAN2→001CH (2412MHz))
※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、5-3ページをご覧ください。
※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。
※5.3/5.6GHz帯のチャンネル選択時のDFS機能については、1-12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

※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 : ③ 036 CH (5180 MHz)

パワーレベル : ④ 高

DTIM間隔 : ⑤ 1

登録 取消

⑥ ⑦

- 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 **〈登録〉** …………… 「無線LAN」画面で設定した内容を登録するボタンです。
- ⑦ **〈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LAN1：5GHz帯

◎無線LAN2：2.4GHz帯

※本書では、「無線LAN1」の画面で説明しています。

※説明のため、[アカウントング](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。

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

アカウントング：⑧ 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。
※「ath0」～「ath07」、「ath11」～「ath17」を使用するときは、[仮想AP]欄を「有効」にしてください。
※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]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。
※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

※本書では、「無線LAN1」の画面で説明しています。

※説明のため、[アカウントング] (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。

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

アカウントング: ⑧ 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))

※[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

※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。

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

アカウントिंग: ⑧ 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、出荷時の設定で使用される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.3-21)で設定できます。
- ⑧ アカウントिंग [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トिंग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、アカウントिंगサーバーの設定が必要です。 (P.3-78)

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.3-73～P.3-75)

暗号化設定	
ネットワーク認証 : ①	オープンシステム ▼
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)

※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」、「WPA2」、「WPA3」、「WPA3 192-bit」、「WPA/WPA2」、「WPA2/WPA3」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

WPA/WPA2/WPA3-Enterprise

◎WPA3 192-bit

ネットワーク認証方式にWPA3 192-bitを使用します。

※「WPA3」認証より強力なCNSA準拠の暗号化方式を使用する認証方式です。

※「WPA3 192-bit」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。

◎WPA3

ネットワーク認証方式にWPA3を使用します。

無線LAN通信の管理フレームを暗号化して盗聴やなりすましを防止します。

※「WPA3」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。

◎WPA2/WPA3

「WPA2」認証と「WPA3」認証を自動認識します。

◎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.3-73～P.3-75)

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

① ネットワーク認証(つづき) ……

WPA/WPA2/WPA3-Personal

◎WPA3-SAE

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「AES」暗号化の認証方式で、SAEのハンドシェイクを利用して、通信相手と暗号鍵(キー)を交換し、認証をします。

◎WPA2-PSK/WPA3-SAE

ネットワーク認証(WPA2-PSK/WPA3-SAE)を自動認識します。

◎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「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。

その他

◎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。

◎オープンシステム

ネットワーク認証をしません。

◎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。

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.3-73～P.3-75)

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

- 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ので、暗号化方式とビット数は、
通信をする相手間で同じ設定にしてください。
※IEEE802.11ax規格、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

◎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、その他(IEEE802.1X、オープンシステム、
オープンシステム/共有キー)以外を選択したとき使用できます。

◎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/WPA2」、または「WPA-PSK/
WPA2-PSK」を選択したとき使用できます。

◎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)ビットの中から選択でき
ます。

※[ネットワーク認証](①)欄で、その他(IEEE802.1X、オープンシステム、
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。

◎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、その他(オープンシステム、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。

※暗号化を設定されることをおすすめします。

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(⑤～⑦)が表示されます。(P.3-75～P.3-76)

暗号化設定	
ネットワーク認証 : ①	オープンシステム ▼
暗号化方式 : ②	WEP RC4 64 (40) ▼
キージェネレーター : ③	👁
WEPキー : ④	●●●●●● ●●●●●● 👁
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桁の入力例：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。
 - ※ 目のアイコン(右端)をクリックすると、入力内容を確認できます。

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、④、⑦)が表示されます。(P.3-73～P.3-76)

暗号化設定	
ネットワーク認証 : ①	WPA2-PSK/WPA3-SAE ▼
暗号化方式 : ②	AES ▼
PSK (Pre-Shared Key) : ⑤	●●●●●●●● ●
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/WPA2/WPA3-Personal (WPA3-SAE、WPA2-PSK/WPA3-SAE、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。

※ WPA3-SAE の場合は8～64文字、WPA2-PSK/WPA3-SAE の場合は8～63文字を入力してください。

※ WPA2-PSK と WPA-PSK/WPA2-PSK の場合は、16進数で設定するときは64桁、ASCII文字で設定するときは、8～63文字を入力してください。

※ 目のアイコン(右端)をクリックすると、入力内容を確認できます。

⑥ WPAキー更新間隔 ……………

[ネットワーク認証] (①) 欄で、その他(IEEE802.1X、オープンシステム、オープンシステム/共有キー)以外を選択したとき、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

※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.3-73～P.3-75)

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、ネットワーク認証を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、「WPA3 192-bit」、「WPA3」、「WPA2/WPA3」、「WPA2」、「WPA/WPA2」、「IEEE802.1X」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	
① プライマリー	セカンダリー
アドレス : ②	_____
ポート : ③	1812
シークレット : ④	●●●●● ●●●●●

- 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。
※目のアイコン(右端)をクリックすると、入力内容を確認できます。

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

■ 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。

- 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。
※目のアイコン(右端)をクリックすると、入力内容を確認できます。
- 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。

- 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。
※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、[MACアドレスフィルタリング設定]項目と[MACアドレスフィルタリング設定一覧]項目に登録された内容が更新されません。
更新されないときは、ご使用のWWWブラウザで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 MACアドレスフィルタリング...** [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]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。
※使用するときには、「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 :	<input type="text"/> <input type="button" value="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

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

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

「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] (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。

- ① AP間通信 無線AP間通信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、本製品のAP間通信を使用できます。

- 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。

※「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。

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)
※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。

インターフェース	接続先BSSID	
wbr0		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。

※選択する設定内容(④、⑤)に応じて、下記以外の設定(⑥)が表示されません。(P.3-87)

- 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。
※「無線LAN」項目の[無線UNIT]欄(P.3-65)を「無効」に設定しているときは、[BSSID]が表示されません。
- 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 [仮想AP設定]項目で設定したSSIDが表示されます。
- 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)

認証方式について

◎WPA3-SAE

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「AES」暗号化の認証方式で、SAEのハンドシェイクを利用して、通信相手と暗号鍵(キー)を交換し、認証をします。

◎WPA2-PSK/WPA3-SAE

ネットワーク認証(WPA2-PSK/WPA3-SAE)を自動認識します。

◎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「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。

◎オープンシステム

ネットワーク認証をしません。

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)

■ 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)が表示されます。(P.3-87)

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

暗号化方式 : ⑤ なし

登録 取消

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、「AES」です。

暗号化方式について

◎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、「オープンシステム」以外を選択したとき使用できます。

◎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」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。

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

子機設定

BSSID : ① [REDACTED]

インターフェース : ② wbr16

SSID : ③ WIRELESSLAN-0

ネットワーク認証 : ④ WPA3-SAE

暗号化方式 : ⑤ AES

PSK (Pre-Shared Key) : ⑥ [REDACTED]

登録 取消

- ⑥ 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、「オープンシステム」以外を選択したとき、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。
※ WPA3-SAEの場合は8～64文字、WPA2-PSK/WPA3-SAEの場合は8～63文字を入力してください。
※ WPA2-PSKの場合は、16進数で設定するときは64桁、ASCII文字で設定するときは、8～63文字を入力してください。
※ 目のアイコン(右端)をクリックすると、入力内容を確認できます。
- ⑦ <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。
- ⑧ <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。

WMM詳細設定

周波数帯： 5 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	<input type="checkbox"/>
AC_BE	15	63	3	0	<input type="checkbox"/>
AC_VI	7	15	1	94	<input type="checkbox"/>
AC_VO	3	7	1	47	<input type="checkbox"/>

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	<input type="checkbox"/>
AC_VO	3	7	2	47	<input type="checkbox"/>

- 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

WMM詳細設定

周波数帯 : 5 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	<input type="checkbox"/>
AC_BE	15	63	3	0	<input type="checkbox"/>
AC_VI	7	15	1	94	<input type="checkbox"/>
AC_VO	3	7	1	47	<input type="checkbox"/>

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	<input type="checkbox"/>
AC_VO	3	7	2	47	<input type="checkbox"/>

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

WMM詳細設定

周波数帯： 5 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	<input type="checkbox"/>
AC_BE	15	63	3	0	<input type="checkbox"/>
AC_VI	7	15	1	94	<input type="checkbox"/>
AC_VO	3	7	1	47	<input type="checkbox"/>

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	<input type="checkbox"/>
AC_VO	3	7	2	47	<input type="checkbox"/>

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

WMM詳細設定

周波数帯： 5 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	<input type="checkbox"/>
AC_BE	15	63	3	0	<input type="checkbox"/>
AC_VI	7	15	1	94	<input type="checkbox"/>
AC_VO	3	7	1	47	<input type="checkbox"/>

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	<input type="checkbox"/>
AC_VO	3	7	2	47	<input type="checkbox"/>

- 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。 (出荷時の設定：無効)
「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。 |
| 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

「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。

ARP代理応答設定

インターフェース : ① ath0

ARP代理応答 : ② 無効 有効

不明なARPの透過 : ③ 無効 有効

ARPエージング時間 : ④ 0 分

⑤ 登録 ⑥ 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)
- ② ARP代理応答 [インターフェース]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]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。
- 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。

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

ARP代理応答設定

インターフェース：① ath0

ARP代理応答：② 無効 有効

不明なARPの透過：③ 無効 有効

ARPエージング時間：④ 0 分

⑤ 登録 ⑥ 取消

- 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。

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

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

「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。

- 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求められるので、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。
※目のアイコン(右端)をクリックすると、入力したパスワードを確認できます。
- 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。
- 5 <登録>** 「管理者パスワードの変更」項目で設定した内容を登録するボタンです。
- 6 <取消>** 「管理者パスワードの変更」項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお、<登録>をクリックすると、変更前の状態には戻りません。

不正アクセス防止のアドバイス

本製品に設定するすべてのパスワードは、容易に推測されないものにしてください。
数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた長く複雑なものに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

■ USB設定

市販のUSBデバイス(USBメモリー)を本製品のUSBポートに差し込んだときの動作を設定します。

※[最大出力電流(USB1)]/[最大出力電流(USB2)](①)欄の両方を「オフ」に設定すると、②～⑤は表示されません。

USB設定

最大出力電流 (USB1) : ① オフ 500 mA 900 mA

最大出力電流 (USB2) : オフ 500 mA 900 mA

USBメモリー : ② 無効 有効

USBアクセス許可 : ③ ファームウェアの更新
 設定の保存/復元

USB認証キー : ④ _____

USB認証キーの書き込み : ⑤

① 最大出力電流(USB1)/(USB2)

.....

USBポートの最大出力電流を設定します。

(出荷時の設定：500mA(USB1)/500mA(USB2))

※「オフ」に設定されていると、USBデバイスを差し込んでも使用できません。

※電源供給がIEEE802.3at規格の場合、[USB1]ポートの最大出力電流が500mAに制限され、[USB2]ポートは使用できなくなります。

② USBメモリー

.....

USBメモリーを本製品のUSBポートに差し込んだときの動作について設定します。

(出荷時の設定：有効)

※「無効」に設定されていると、本製品のファームウェアファイルや設定ファイルなどを保存したUSBメモリーを差し込んでも、ファイルを読み込みません。

③ USBアクセス許可

.....

本製品に接続されたUSBメモリーから読み込むファイルを選択します。

(出荷時の設定： ファームウェアの更新

設定の保存/復元)

※チェックマーク[]をはずすと、ファイルを保存したUSBメモリーを差し込んだ状態で<USB>ボタンを短く押しても、該当ファイルを読み込みません。

◎ファームウェアの更新(P.4-15)

本製品のファームウェアファイル(拡張子：dat)を保存したUSBメモリーを差し込んで<USB>ボタンを短く押すと、ファームウェアを更新します。

◎設定の保存/復元(P.4-13)

本製品の設定ファイルをUSBメモリーに保存後、設定が異なる本製品にUSBメモリーを差し込んで<USB>ボタンを短く押すと、自動で設定を復元します。

3 設定画面について

「管理ツール」画面

管理 > 管理ツール

■ USB設定

USB設定

最大出力電流 (USB1) : オフ 500 mA 900 mA

最大出力電流 (USB2) : オフ 500 mA 900 mA

USBメモリー : 無効 有効

USBアクセス許可 : ファームウェアの更新
 設定の保存/復元

USB認証キー :

USB認証キーの書き込み:

- ④ **USB認証キー** …………… 本製品のUSBポートに差し込んだUSBメモリーへのファイルの読み込みと書き出しに対するUSB認証キーを設定します。
大文字/小文字の区別に注意して、64文字以内(任意の半角英数字/記号)で入力します。
※入力後、「管理ツール」画面の〈登録〉をクリックすると、本製品にUSB認証キーが設定されます。
※本製品にUSB認証キーを設定すると、本製品からUSBメモリーに書き込んだUSB認証キーと同じかどうかを認証します。

- ⑤ **USB認証キーの書き込み** ……… 本製品に設定されているUSB認証キーを本製品のUSBポートに差し込んだUSBメモリーへ書き込むボタンです。
〈書き込み〉をクリックして、表示される画面にしたがって操作してください。

USB認証キーを保存したUSBメモリーを差し込んでいる場合は、「既に認証キーが書き込まれています。上書きする場合は「進む」ボタンをクリックしてください。」が表示されます。

USB認証キーの書き込み

USBメモリーに認証キーを書き込みます。
USBメモリーを本体に装着し、準備ができたなら「進む」ボタンをクリックしてください。



USB認証キーの書き込み

認証キーの書き込みが完了しました。

- ※下記の画面が表示されたときは、〈OK〉をクリックして画面を閉じ、「管理ツール」画面の〈登録〉をクリックしてください。

192.168.0.1 の内容

USB認証キーが変更されています。
変更を登録してから、書き込みを行なってください。

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

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

HTTPS : ③ 無効 有効

HTTPSポート番号 : ④

- 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

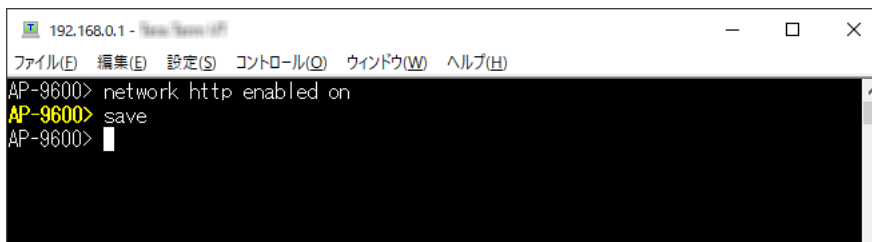
管理 > 管理ツール

■ 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-9600>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.3-100)

- ① AP-9600> **network http enabled on** と入力し[Enter]キーを押します。
- ② AP-9600> **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。



```
192.168.0.1 - New Term 0/0
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)
AP-9600> network http enabled on
AP-9600> save
AP-9600> 
```

※本製品の[CONSOLE]ポートとパソコンの[USB]ポートを市販のUSBケーブル(Type-C)で接続すると、上記と同様にターミナルソフトウェアから設定できます。(P.5-6)

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。

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

- 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]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

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 2023/1/23 21:23

設定する時刻 : ② 2023 年 03 月 31 日 13 時 20 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] 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

⑤ 登録 ⑥ 取消

- 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]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。
- ⑤ <登録> [自動時計設定]項目で設定した内容を登録するボタンです。
- ⑥ <取消> [自動時計設定]項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお、<登録>をクリックすると、変更前の状態には戻りません。

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、WAN側を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

「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。

- 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。 (出荷時の設定：有効)
「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。

- 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。

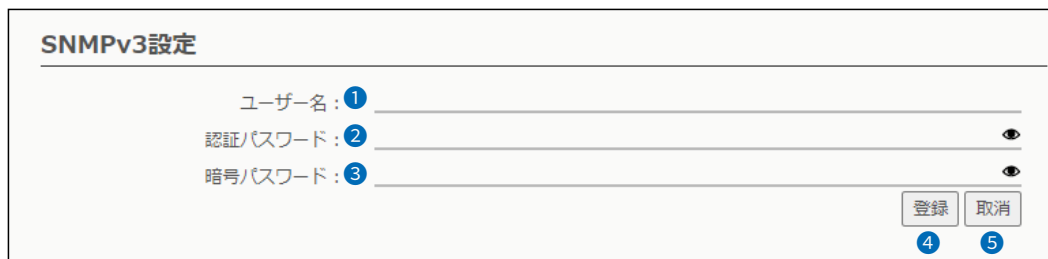
3 設定画面について

「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時の設定です。



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。
※目のアイコン(右端)をクリックすると、入力したパスワードを確認できます。
- 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。
※目のアイコン(右端)をクリックすると、入力したパスワードを確認できます。
- 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。

- 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 : LED消灯モードを使用して、[POWER]ランプを減灯するとき
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、[POWER]ランプの明るさが暗くなります。
同時に、[POWER]以外のランプは、本製品の使用中でも消灯状態になります。
- 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。
- ※USBメモリー(市販品)を差し込んだ状態では、LED消灯モードは動作しません。
- ※〈MODE〉ボタン、〈FUNC〉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」、「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。

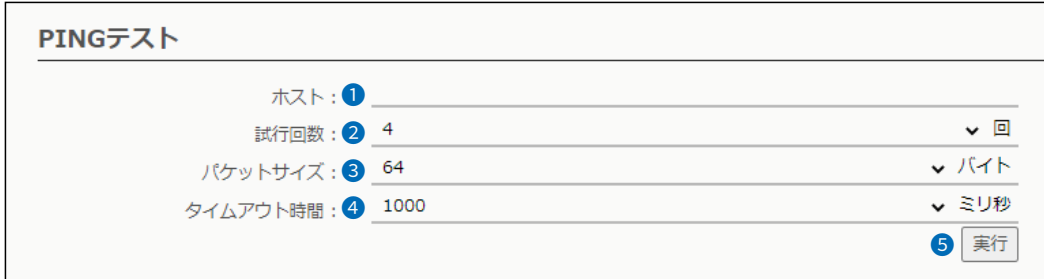
3 設定画面について

「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

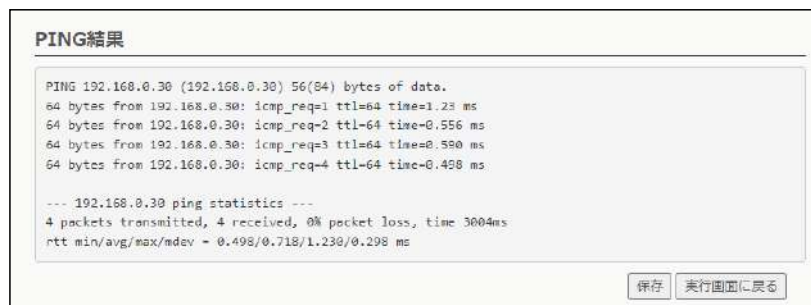
パケットサイズ : ③ 64 ▼ バイト

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。
クリックして、表示される画面にしたがって操作すると、「PING結果」表示に切り替わり、テスト結果を表示します。

PING結果について



PING結果

```
PING 192.168.0.30 (192.168.0.30) 56(64) bytes of data:
64 bytes from 192.168.0.30: icmp_req=1 ttl=64 time=1.23 ms
64 bytes from 192.168.0.30: icmp_req=2 ttl=64 time=0.556 ms
64 bytes from 192.168.0.30: icmp_req=3 ttl=64 time=0.590 ms
64 bytes from 192.168.0.30: icmp_req=4 ttl=64 time=0.498 ms

--- 192.168.0.30 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.498/0.718/1.230/0.298 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 ▼ 秒

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。
クリックして、表示される画面にしたがって操作すると、「経路テスト結果」表示に切り替わり、テスト結果を表示します。

経路テスト結果について

経路テスト結果

```
tracerroute to 192.168.0.30 (192.168.0.30), 16 hops max, 46 byte packets
 1 192.168.0.30 (192.168.0.30) 1.287 ms 0.699 ms 0.618 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

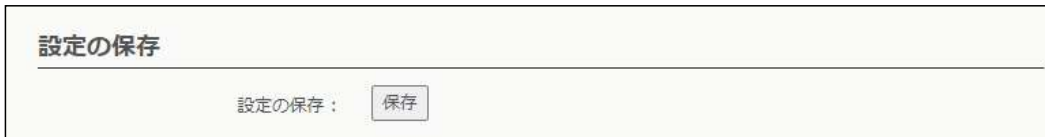
「設定の保存/復元」画面

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。

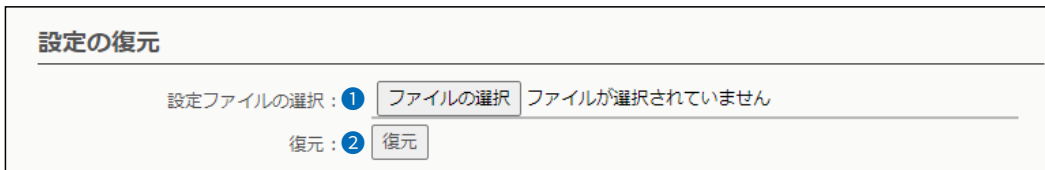
保存したファイルは、[設定の復元]項目の操作で、本製品に書き込みできます。

管理 > 設定の保存/復元

■ 設定の復元

保存した設定ファイルの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、〈ファイルの選択〉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

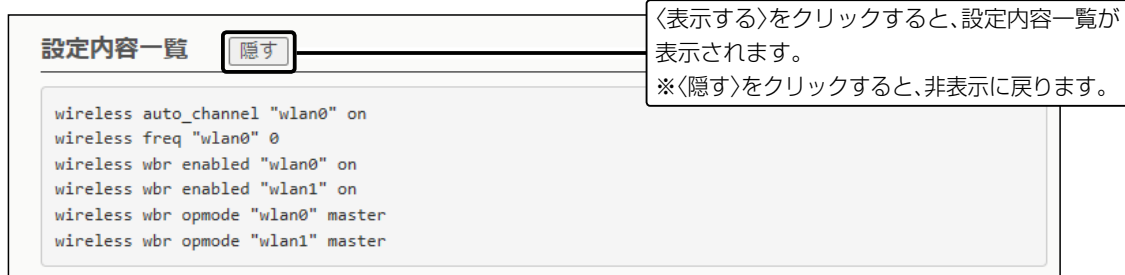
「設定の保存/復元」画面

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。

※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
```

〈表示する〉をクリックすると、設定内容一覧が表示されます。
※〈隠す〉をクリックすると、非表示に戻ります。

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

- 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(数分間)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-9600 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
[POWER]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.4-8)
※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 ファイルが選択されていません

ファームウェアの更新 : ②

- ① ファームウェアの選択** …………… <ファイルの選択>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。
選択したファイルが、[ファームウェアの選択]項目に表示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]項目に表示された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
5. USBメモリーによる自動設定機能について	4-9
■ USBメモリー使用時のご注意	4-10
■ 対応するUSBメモリーの規格	4-10
■ 自動設定に使用するファイル名の付けかた	4-11
■ 自動バックアップされる設定ファイルについて	4-11
■ 複数台分の設定ファイルを1つのUSBメモリーで管理するには	4-12
6. USBメモリーから自動で設定を復元するには	4-13
■ 設定ファイルを保存して復元するまでの手順	4-13
7. USBメモリーからファームウェアを更新するには	4-15
■ 更新するまでの手順	4-15
8. USBメモリー用の認証キーを設定するには	4-17
■ 設定のしかた	4-17

4 保守について

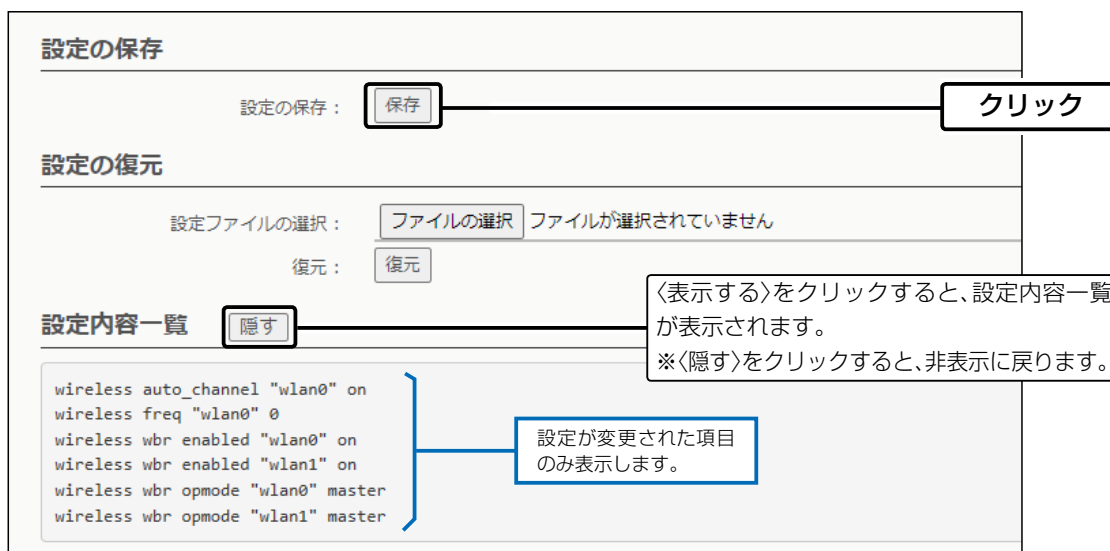
1. 設定内容の確認または保存

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、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。
設定ファイルが保存されます。(P.1-17)



4 保守について

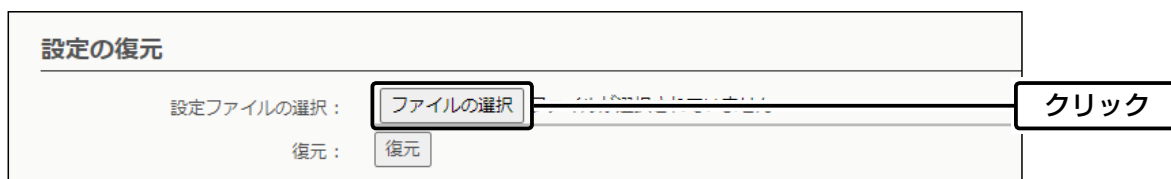
2. 保存された設定の書き込み(復元)

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。

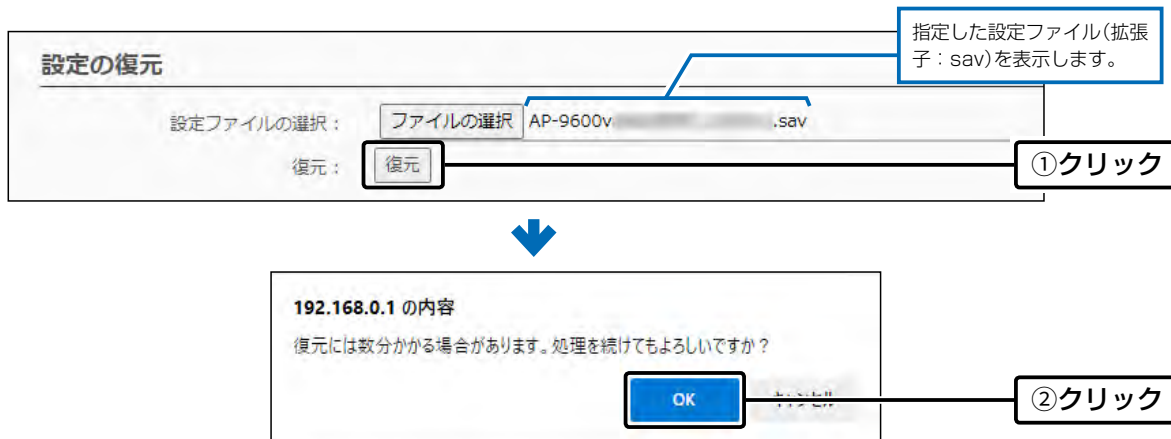
- 1 「管理」メニュー、「設定の保存/復元」の順にクリックします。
「設定の保存/復元」画面が表示されます。

- 2 「設定の復元」項目の〈ファイルの選択〉をクリックします。
「開く」画面(別画面)が表示されます。



- 3 「開く」画面(別画面)で、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、復元するために本製品が再起動します。



- 5 再起動後、[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、復元中ですので、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。)

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、変更による障害、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

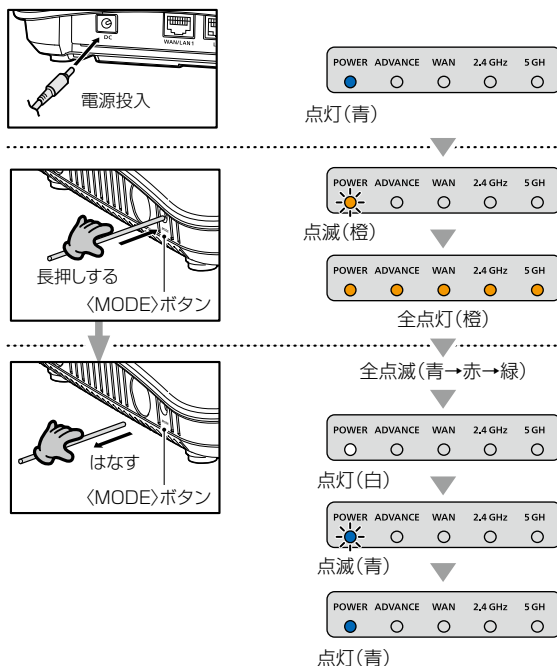
3. 設定を出荷時の状態に戻すには

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。
- 2 すべてのランプが● 橙点灯するまで、〈MODE〉ボタンを押す
- 3 すべてのランプが● 橙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● 青点灯すると、初期化完了です。



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

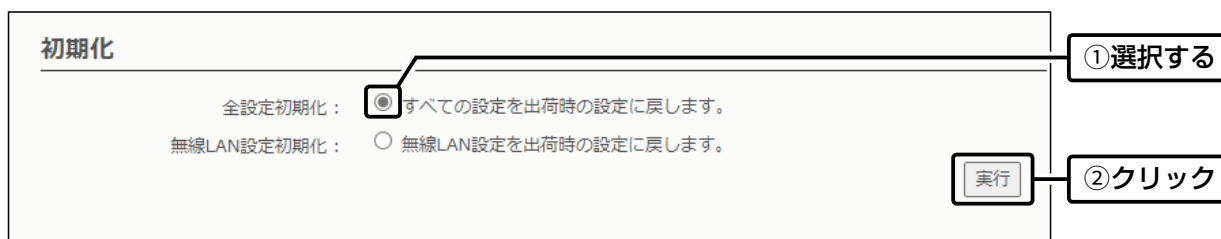
本製品に設定されたIPアドレスと管理者パスワードがわかっていて、そのIPアドレスで設定画面にアクセスできるときは、本製品の設定画面から、すべての設定を出荷時の状態に戻せます。

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。

Ⓐ 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。

Ⓑ 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ーに書き込まれているプログラムです。

このプログラムは、機能の拡張や改良のため、バージョンアップ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	AP-9600
バージョン	<input type="text"/> バージョン情報
国名コード	JP
現在時刻	20 / / 13:08:45
稼働時間	
メモリー使用量	285580 kB / 821908 kB (34% 使用中)
PoEステータス	ACアダプター

■ 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

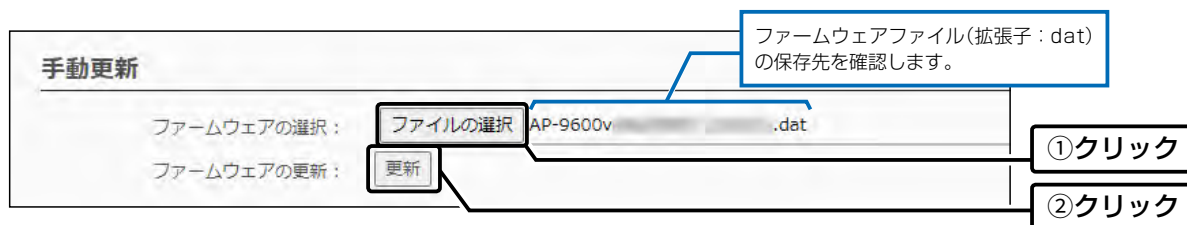
A ファイルを指定して更新する

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)

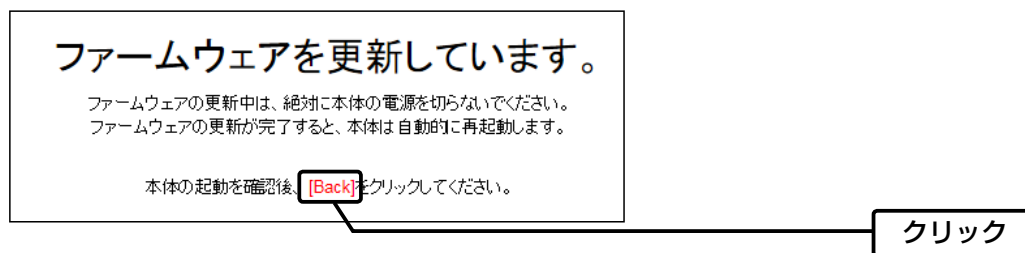
※ 更新後、既存の設定内容が初期化されるファームウェアファイルがありますので、ダウンロードするときは、弊社ホームページに記載の内容をご確認ください。

※ 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.3-95)

- 1 「管理」メニュー、「ファームウェアの更新」の順にクリックします。
「ファームウェアの更新」画面が表示されます。
- 2 下記のように、弊社ホームページよりダウンロードして解凍したファームウェアファイル(拡張子 : dat)の保存先を指定して、更新します。



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



ご注意

[Back]の操作(手順3)で設定画面に戻るようになるまで、ご使用のパソコンや本製品の電源を絶対に切らないでください。
途中で電源を切ると、データの消失や誤動作の原因になります。

※ 出荷時の設定内容に戻るような注意書きがあるバージョンアップ用ファームウェアの場合は、上図の[Back]をクリックしても設定画面に戻れないことがあります。

その場合は、接続するパソコンのIPアドレスを「例:192.168.0.100」に設定してから、本製品の設定画面「192.168.0.1」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

④ 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、[POWER]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。

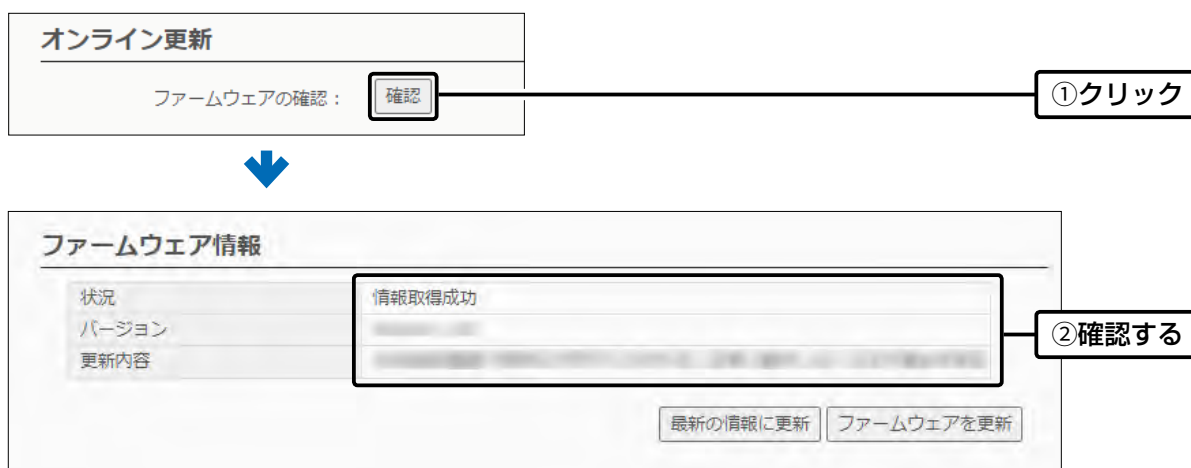
※ 自動更新機能が「有効」に設定されているときに、オンラインで新しいファームウェアを検知します。(P.3-116)

※ 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、[POWER]ランプが青点灯のときは、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、そのまま数分程度お待ちください。
弊社のアップデート管理サーバーに接続すると、ファームウェアのダウンロードを開始し、更新後は、自動的に再起動します。

ファームウェアを更新しています。

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。

4 保守について

5. USBメモリーによる自動設定機能について

本製品のUSBポートにUSBメモリー(市販品)を接続し、〈USB〉ボタンを短く押すと、あらかじめUSBメモリーに保存されたファームウェアファイルや設定ファイル(本製品の設定が保存されたファイル)を本製品に自動で読み込みます。また、本製品の「LAN2」のMACアドレスをフォルダー名とするフォルダーを作成することで、1つのUSBメモリーを使用して、複数台(本製品)の設定復元やファームウェアの更新ができます。

※操作方法については、4-13ページ～4-16ページをご覧ください。

◎ファームウェアの更新

本製品のファームウェアファイル(拡張子: dat)をUSBメモリーに保存後、本製品にUSBメモリーを差し込んで、ファームウェアを更新します。

◎設定の保存/復元

本製品の設定ファイルをUSBメモリーに保存後、本製品にUSBメモリーを差し込んで、自動で設定を復元します。

ご参考

「管理」メニューの「管理ツール」画面で、「最大出力電流」欄を「オフ」以外の設定にし、「USBメモリー」欄が「有効」に設定されているとき、USBメモリーが差し込まれると、USBメモリーへのアクセスが開始されます。

The screenshot shows the 'USB設定' (USB Settings) menu. It includes the following options:

- 最大出力電流 (USB1): オフ 500 mA 900 mA
- 最大出力電流 (USB2): オフ 500 mA 900 mA
- USBメモリー: 無効 有効
- USBアクセス許可: ファームウェアの更新, 設定の保存/復元
- USB認証キー: [Redacted]
- USB認証キーの書き込み: [書き込み]

(※画面の内容は、出荷時の設定です。)

4 保守について

5. USBメモリーによる自動設定機能について

■ USBメモリー使用時のご注意

- ◎ 指紋認証型、アプリケーション認証(パスワード認証)型など、セキュリティ対応型のUSBメモリーは使用できません。
- ◎ ご使用になる前に、あらかじめ、USBメモリー内のデータをバックアップしてください。
- ◎ データ保護のため、必ず[ADVANCE]ランプが消灯してから、USBメモリーの接続や取りはずしをしてください。
設定保存/復元、ファームウェアの更新で使用する場合など、USBメモリーを接続中([ADVANCE]ランプ ● 青点灯中)は、絶対にUSBメモリーを取りはずさないでください。
ファイルの消失や故障の原因になります。
- ◎ USBメモリーは、どちらか一方のUSBポートにだけ接続してください。
2つのUSBポートを同時には使用できません。
- ◎ USBメモリーを差し込むときは、形状と差し込み方向に注意して、奥まで確実に差し込んでください。
- ◎ USBメモリーを接続中は、[ADVANCE]ランプが ● 青点灯します。
設定復元中やファームウェアの更新中は、[POWER]ランプが青色で点滅します。
- ◎ 本製品の設定画面でUSB認証キーが設定(P.4-17)されている場合、差し込まれたUSBメモリー側の認証キーと一致しないときは、自動設定機能は動作しません。
- ◎ 設定を復元する直前の設定値は、設定ファイル(bakdata.sav)として、本製品に接続したUSBメモリーにバックアップされます。
- ◎ USBメモリーに保存された設定ファイルやファームウェアファイルが、本製品に適用されているものと同じ場合や、破損していたり、本製品以外のものであったりするときは、自動設定、またはファームウェアの更新をしません。
※本製品で動作中のものと異なる設定ファイルやファームウェアファイルが、USBメモリーに保存されている場合は、その内容で自動設定されます。
- ◎ 設定ファイルとファームウェアファイルの両方がUSBメモリーに保存されている場合は、設定復元、ファームウェアの更新の順に自動設定を実行します。

■ 対応するUSBメモリーの規格

インターフェース : USB3.0/2.0/1.1

デバイス : USB 大容量デバイス(USB Mass Storage Class)

フォーマット : FAT16/FAT32(exFATやNTFSなど、ほかのフォーマットには対応していません。)

※すべてのUSB対応周辺機器で動作を保証するものではありません。

4 保守について

5. USBメモリーによる自動設定機能について

■ 自動設定に使用するファイル名の付けかた

設定ファイル名は、「savedata」(拡張子：sav)でUSBメモリーに保存してください。

※自動設定に使用する設定ファイルは、「管理」メニュー→「設定の保存/復元」画面→「設定の保存」項目(P.4-2)で保存したものと、自動バックアップされる設定ファイル以外は、使用できません。

ファームウェアファイル名は、「firmware」(拡張子：dat)でUSBメモリーに保存してください。

※ファームウェアの更新に使用するファームウェアファイルは、弊社ホームページからダウンロードし、解凍してから、ファームウェアファイル名を変更してください。

■ 自動バックアップされる設定ファイルについて

バックアップは、下記のファイル名で、最大10世代前まで自動バックアップされます。

最新のバックアップ設定ファイルは、bakdata.savで自動バックアップされます。

例：1世代前のファイル名 bakdata_1.sav

2世代前のファイル名 bakdata_2.sav

3世代前のファイル名 bakdata_3.sav

～ 中略 ～

10世代前のファイル名 bakdata_10.sav

※10世代を超えると、最も古いバックアップ設定ファイル(bakdata_10.sav)が削除されます。

また、削除と同時に、ファイル名の数字が1世代後退します。(例：bakdata_9.sav→bakdata_10.sav)

※ファームウェアファイルは、バックアップされません。

※本製品の設定内容を変更した場合に、設定ファイル(bakdata.sav)が自動バックアップされます。

4 保守について

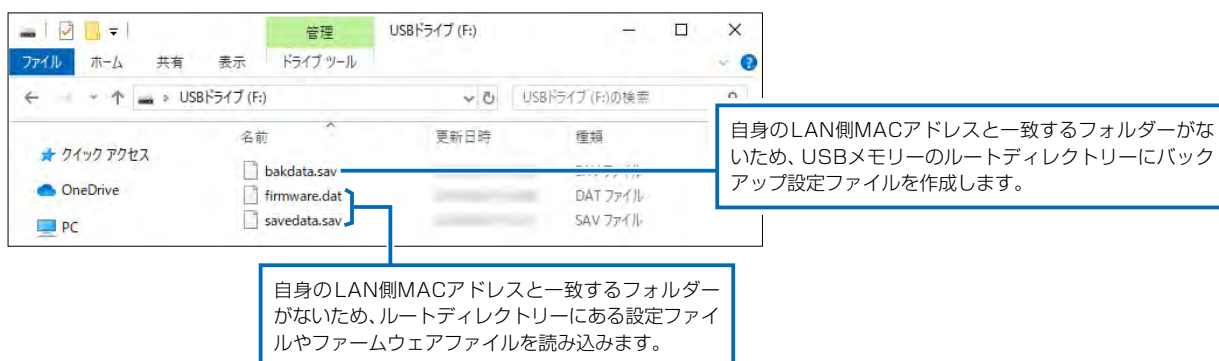
5. USBメモリーによる自動設定機能について

■ 複数台分の設定ファイルを1つのUSBメモリーで管理するには

1つのUSBメモリーを使用して、本製品(複数台分)の設定復元やファームウェアの更新をするときは、あらかじめ、「TOP」画面に表示されている「LAN2」のMACアドレス(P.3-5)をフォルダー名★とするフォルダーを作成し、そのフォルダーに本製品の設定ファイルやファームウェアファイルを保存しておく必要があります。

★全角のフォルダー名は使用できません。

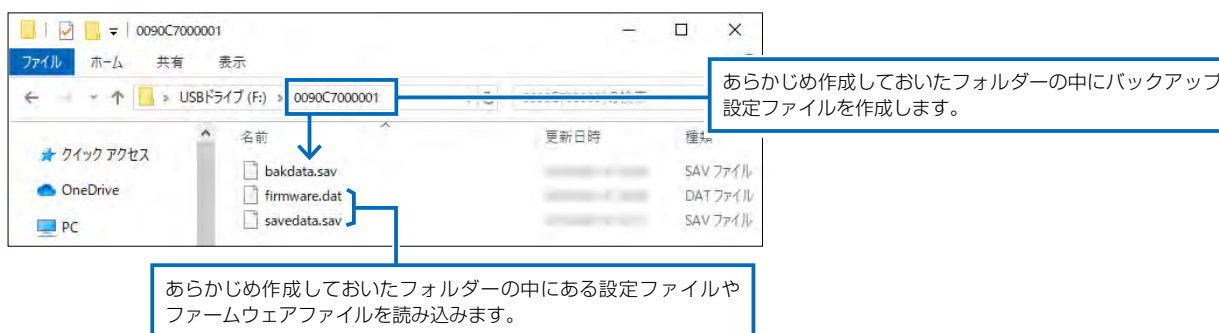
ルートディレクトリーにフォルダーがないとき



自身のLAN側MACアドレスと一致するフォルダーがないため、USBメモリーのルートディレクトリーにバックアップ設定ファイルを作成します。

自身のLAN側MACアドレスと一致するフォルダーがないため、ルートディレクトリーにある設定ファイルやファームウェアファイルを読み込みます。

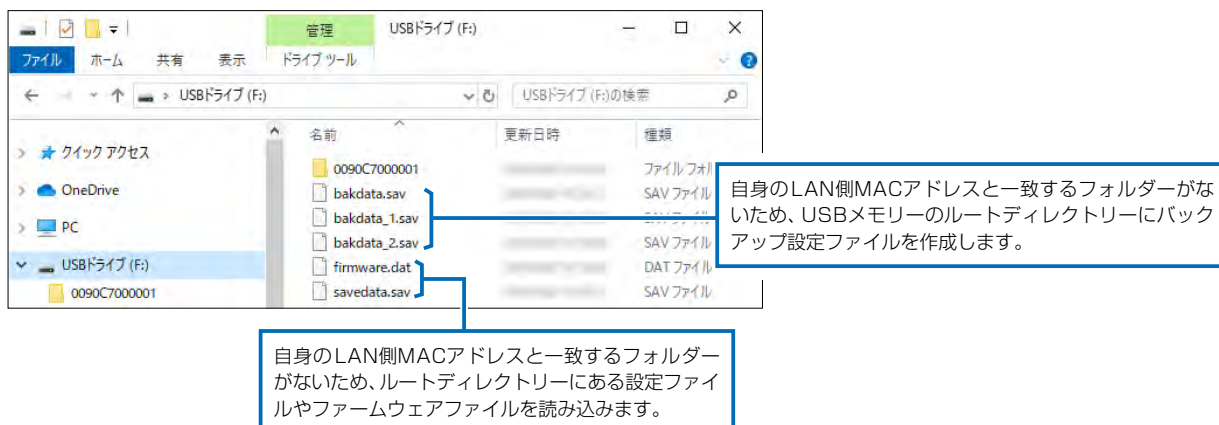
自身のLAN側MACアドレス(例：0090C7000001)と一致するフォルダーがあるとき



あらかじめ作成しておいたフォルダーの中にバックアップ設定ファイルを作成します。

あらかじめ作成しておいたフォルダーの中にある設定ファイルやファームウェアファイルを読み込みます。

自身のLAN側MACアドレス(例：0090C7000002)と一致するフォルダーがないとき



自身のLAN側MACアドレスと一致するフォルダーがないため、USBメモリーのルートディレクトリーにバックアップ設定ファイルを作成します。

自身のLAN側MACアドレスと一致するフォルダーがないため、ルートディレクトリーにある設定ファイルやファームウェアファイルを読み込みます。

4 保守について

6. USBメモリーから自動で設定を復元するには

管理 > 設定の保存/復元

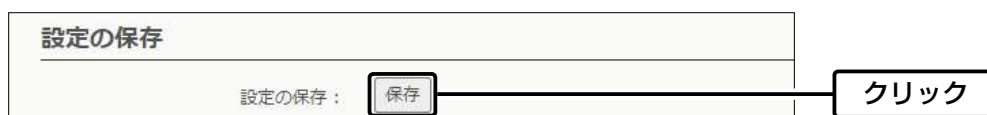
本製品の設定ファイルをUSBメモリー(市販品)に保存後、設定が異なる本製品にUSBメモリーを差し込んで、自動で設定を復元するまでの手順について説明します。

※ 使用条件については、「USBメモリーによる自動設定機能について」(P.4-9)をご覧ください。

※ Microsoft Edge (Chromiumベース)で「ダウンロード時の動作を毎回確認する」を有効にしている場合を例にしています。

■ 設定ファイルを保存して復元するまでの手順

- 1 USBメモリーをパソコンに差し込みます。
- 2 本製品の設定画面にアクセスします。(P.1-17)
- 3 「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。
- 4 「設定の保存」欄の「保存」をクリックします。



- 5 「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。



- 6 設定ファイルの保存先にUSBメモリーのルートディレクトリーを指定し、ファイル名を「savedata.sav」に変更してから、「保存(S)」をクリックします。
※ ファイル名は、必ず「savedata.sav」に変更してください。
「savedata.sav」以外のファイル名では、USBメモリーからの復元に使用できません。



(次ページにつづく)

4 保守について

6. USBメモリーから自動で設定を復元するには

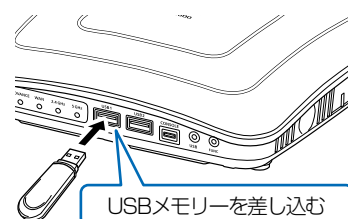
管理 > 設定の保存/復元

■ 設定ファイルを保存して復元するまでの手順

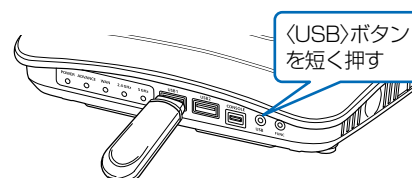
7 USBメモリーをパソコンから取りはずします。
※USBメモリーの取りはずしかたは、各周辺機器に付属する取扱説明書の記載内容にしたがってください。

8 設定を復元する本製品を用意します。

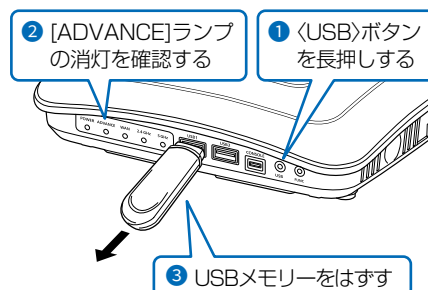
9 savedata.savが保存されたUSBメモリーを本製品のUSBポートに差し込みます。
USBメモリーが接続されると、[ADVANCE]ランプが●青点灯します。



10 〈USB〉ボタンを短く押します。
設定を復元するため、本製品が再起動します。



11 [POWER]ランプが●青点灯に切り替わったことを確認してから、[ADVANCE]ランプが消灯するまで、〈USB〉ボタンを押しつづけます。
[ADVANCE]ランプ消灯後、本製品からUSBメモリーを取りはずします。
※USBメモリーには、復元前の設定内容を保存した設定ファイルが自動でバックアップファイル(bakdata.sav)として保存されています。



ご注意

- ◎設定復元が完了するまで、絶対にUSBメモリーを取りはずしたり、電源を切ったりしないでください。
途中で、USBメモリーを取りはずしたり、電源を切ったりすると、設定ファイルの消失や故障の原因になります。
また、設定復元が完了するまで、本製品の設定画面にアクセスしないでください。
- ◎データ保護のため、必ず[ADVANCE]ランプが消灯してから、USBメモリーを取りはずしてください。

ご参考

「管理」メニューの「管理ツール」画面で、[最大出力電流]欄を「オフ」以外の設定にし、[USBメモリー]欄(P.3-96)が「有効」(出荷時の設定)に設定されているとき、USBメモリーが差し込まれた本製品の電源を入れると、USBメモリーへのアクセスが開始されます。

4 保守について

7. USBメモリーからファームウェアを更新するには

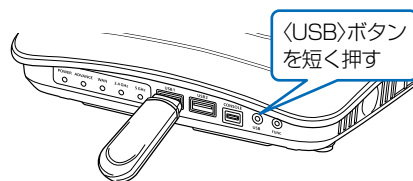
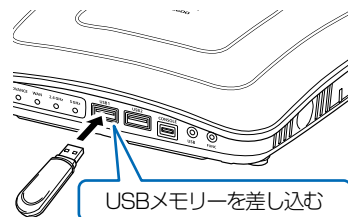
弊社ホームページよりダウンロードした本製品のファームウェアファイル(拡張子:dat)をUSBメモリー(市販品)に保存して、本製品のファームウェアを更新するまでの手順について説明します。

※使用条件については、「USBメモリーによる自動設定機能について」(P.4-9)をご覧ください。

※更新を実行する前に、「ファームウェアの更新についてのご注意」(P.4-6)をご覧ください。

■ 更新するまでの手順

- 1 本製品のファームウェアファイルを弊社ホームページよりダウンロードして、解凍します。
- 2 ファームウェアファイルのファイル名をfirmware.datに変更します。
※ファイル名は、必ず「firmware.dat」に変更してください。
「firmware.dat」以外のファイル名は、USBメモリーからの更新には使用できません。
- 3 USBメモリーをパソコンに差し込みます。
- 4 firmware.datをUSBメモリーのルートディレクトリーに保存します。
- 5 USBメモリーをパソコンから取りはずします。
※USBメモリーの取りはずしかたは、各周辺機器に付属する取扱説明書の記載内容にしたがってください。
- 6 ファームウェアを更新する本製品を用意します。
- 7 firmware.datが保存されたUSBメモリーを本製品のUSBポートに差し込みます。
USBメモリーが接続されると、[ADVANCE]ランプが●青点灯します。
- 8 〈USB〉ボタンを短く押します。
ファームウェアを更新するため、本製品が再起動します。



ご注意

ファームウェアの更新が完了するまで、絶対にUSBメモリーを取りはずしたり、電源を切ったりしないでください。
更新中に、USBメモリーを取りはずしたり、電源を切ったりすると、故障の原因になります。

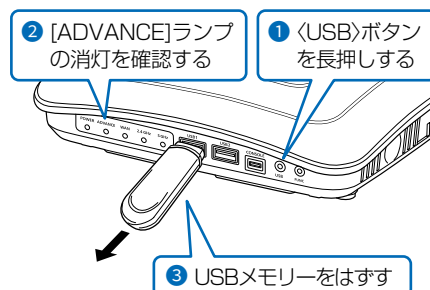
(次ページにつづく)

4 保守について

7. USBメモリーからファームウェアを更新するには

■ 更新するまでの手順

- 9 [POWER] ランプが ● 青点灯に切り替わったことを確認してから、[ADVANCE] ランプが消灯するまで、〈USB〉ボタンを押しつづけます。
[ADVANCE] ランプ消灯後、本製品からUSBメモリーを取りはずします。



ご注意

データ保護のため、必ず[ADVANCE]ランプが消灯してから、USBメモリーを取りはずしてください。

更新後は、本製品の設定画面にアクセスして、ファームウェアバージョンを確認してください。

USBメモリーに保存された設定ファイルやファームウェアファイルが本製品に適用されているものと同じとき、破損や本製品以外のものである場合は、自動設定、またはファームウェアの更新をしません。

4 保守について

8. USBメモリー用の認証キーを設定するには

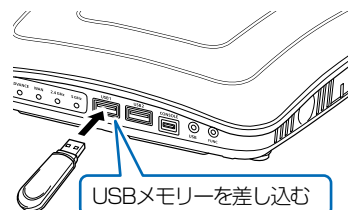
管理 > 管理ツール

本製品にUSB認証キーを設定することで、認証キーが一致するUSBメモリーを使用したときだけ、設定ファイルの自動バックアップ、設定の復元、ファームウェアの更新ができます。

■ 設定のしかた

- 1 USB認証キーの書き込みに使用するUSBメモリーを本製品の[USB]ポートに差し込みます。

※あらかじめ、USBメモリーに保存されたUSB認証キー(ファイル名: usbkey.dat)を変更する場合も、そのUSBメモリーを差し込みます。



- 2 本製品の設定画面にアクセスします。(P.1-17)

- 3 「管理」メニュー、「管理ツール」の順にクリックします。
「管理ツール」画面を表示します。

- 4 [USB設定]項目の[USB認証キー]欄に、大文字/小文字の区別に注意して、任意の半角英数字64文字以内で入力して、〈登録〉をクリックします。

※USB認証キーを変更する場合は、テキストボックスの内容を削除してから入力してください。

USB設定

最大出力電流 (USB1): オフ 500 mA 900 mA

最大出力電流 (USB2): オフ 500 mA 900 mA

USBメモリー: 無効 有効

USBアクセス許可: ファームウェアの更新
 設定の保存/復元

USB認証キー:

USB認証キーの書き込み:

登録

①入力する

※目のアイコン(右端)をクリックすると、入力した内容を確認できます。

②クリック

- 5 〈書き込み〉をクリックします。

USB設定

最大出力電流 (USB1): オフ 500 mA 900 mA

最大出力電流 (USB2): オフ 500 mA 900 mA

USBメモリー: 無効 有効

USBアクセス許可: ファームウェアの更新
 設定の保存/復元

USB認証キー:

USB認証キーの書き込み:

登録

クリック

4 保守について

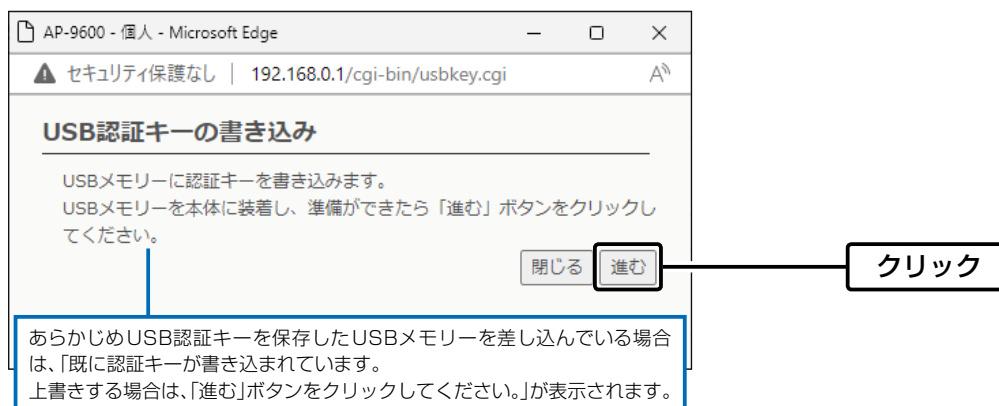
8. USBメモリー用の認証キーを設定するには

管理 > 管理ツール

■ 設定のしかた

6 「USB認証キーの書き込み」(別画面)が表示されたら、〈進む〉をクリックします。

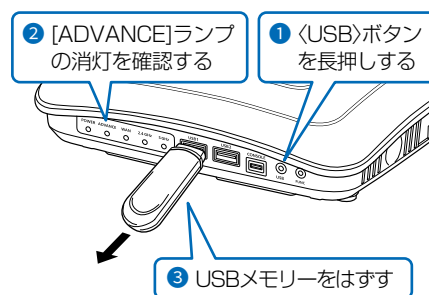
※書き込みを中止する場合は、〈閉じる〉をクリックします。



7 「認証キーの書き込みが完了しました。」が表示されたら、〈閉じる〉をクリックします。



8 本製品からUSBメモリーを取りはずします。



ご注意

データ保護のため、必ず[ADVANCE]ランプが消灯してから、USBメモリーを取りはずしてください。

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
■ [CONSOLE]ポートを使用する	5-6
3. 設定画面の構成について	5-7
4. 初期値一覧	5-10
■ ネットワーク設定	5-10
■ ルーター設定	5-11
■ 無線LAN設定	5-12
■ 管理	5-16
5. 機能一覧	5-18
■ 無線LAN機能	5-18
■ ネットワーク管理機能	5-18
■ ルーター機能	5-18
■ その他	5-18
6. 設定項目で使用できる文字列について	5-19
■ ネットワーク設定	5-19
■ 無線LAN設定	5-19
■ 管理	5-19
7. 弊社製無線アクセスポイントの機能対応表	5-20
8. 定格について	5-21
■ 一般仕様	5-21
■ 有線部	5-21
■ 無線部	5-21

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]ランプが点灯しない

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

[2.4GHz]ランプ/[5GHz]ランプが青点灯しない

- 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]ランプが青点灯しているが通信できない

- 暗号化セキュリティーの設定が異なっている
→ 本製品と接続先の暗号化セキュリティーの設定を確認する

5 ご参考に

1. 困ったときは

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。(2023年4月現在)

「ath0」: AP-95M(無線LAN1(2.4GHz帯))、AP-9500/AP-9600(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/AP-9600(無線LAN2(2.4GHz帯))

「ath4」: AP-90M、AP-90MR

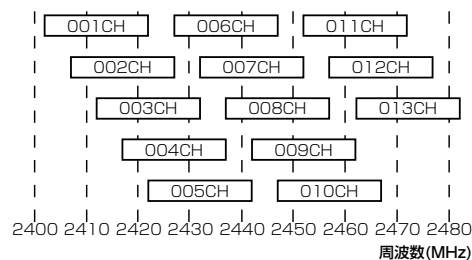
「ath8」: AP-900、AP-9000

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

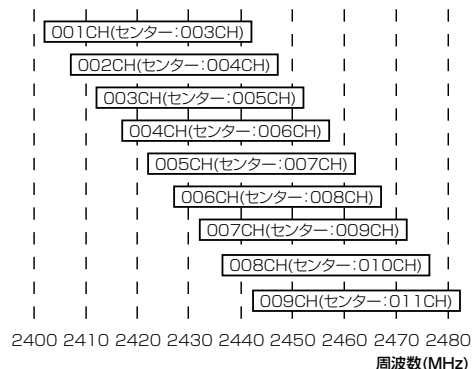
【帯域幅が20MHzの場合】(帯域の1部が重複)

- 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。



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

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
→ (スタート)(ロゴボタン)→[設定]→[ネットワークとインターネット]にある[プロキシ]で、設定を確認する

インターネットに接続できない

- 回線接続業者に契約をしたが、工事完了、または使用開始の通知がない
→ 契約、または工事の完了日をご契約の回線接続業者に確認する
- 使用する機器の MAC アドレスを登録していない
→ 登録が必要な回線接続業者の場合は、本製品の本体 MAC アドレス (WAN 側 MAC アドレス) を登録する (P.vii、P.3-5)
- ブリッジタイプモデム、または回線終端装置 (FTTH) をご使用の場合で、ご契約の回線接続業者への接続方法を間違えている
→ 該当する回線種別 (DHCP クライアント、固定 IP、PPPoE) を、ご契約の回線接続業者に確認する
- ブロードバンドモデム、または回線終端装置 (FTTH) が本製品と正しく接続されていない
→ ブリッジタイプモデム、または回線終端装置 (FTTH) の場合は、本製品の回線種別の設定をご契約の回線接続業者との契約内容にしたがって変更 (DHCP クライアント、固定 IP、PPPoE) してから [WAN/LAN1] ポートと接続する
ルータータイプモデムの場合は、本製品の回線種別を出荷時の設定 (使用しない) で、[LAN] ポートと接続する
- WAN (回線接続業者) 側から IP アドレスが取得できていない
→ 本製品とブリッジタイプモデム、または回線終端装置 (FTTH) の接続を確認する
WAN 側から取得した IP アドレスを確認するときは、「ルーター設定」メニューにある「WAN 接続先」画面の [回線状態表示] に表示される内容を確認する
- DNS サーバーの IP アドレスが正しく指定されていない
→ 「ネットワーク設定」メニュー、または「ルーター設定」メニューで DNS サーバーの設定を確認する

ルーター機能設定時に [WAN/LAN1] ポート (WAN 側) から本製品にアクセスできない

- 出荷時に登録されている IP フィルターの設定により、WAN 側から本製品へのアクセスを遮断しているため
→ △注意 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。

USB メモリーにアクセスできない

- 本製品の USB メモリー機能を無効に設定している
→ 本製品の USB メモリー機能を有効に設定する
- 使用する USB ポートの最大出力電流をオフに設定している
→ 最大出力電流をオフ以外に設定している USB ポートを使用する
→ 使用する USB ポートの最大出力電流をオフ以外に設定する (P.1-3、P.3-96)
※電源供給が IEEE802.3at 規格の場合、[USB1] ポートの最大出力電流が 500mA に制限され、[USB2] ポートは使用できません。

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.3-100)

※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` : 「管理者」画面で設定したパスワードを入力します。(P.3-95)

② ログインに成功すると、プロンプト AP-9600> 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。

※コマンド入力での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-9600> 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) e[Tab]→exit 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

2. Telnet/SSHで接続するには

■ [CONSOLE]ポートを使用する

本製品の[CONSOLE]ポートとパソコンの[USB]ポートを、市販のUSBケーブル(Type-C)で接続すると、ターミナルソフトウェアから設定できます。

※ご使用していただくためには、USBドライバーが必要です。

※弊社ホームページから、USBドライバーとインストールガイドをダウンロードしていただき、手順にしたがってインストールしてください。

※USBドライバーをインストールしたあと、ターミナルソフトウェアのCOMポートを下記の値に設定します。

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

※設定後、何も入力せずに[Enter]キーを押すと、「AP-9600 login:」と表示されます。

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
		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	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
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
	VPN	IPsec設定
		IPsecトンネル設定
IPsecトンネル設定一覧		

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
		仮想AP設定
	無線LAN1 仮想AP	暗号化設定
		MACアドレスフィルタリング設定
	無線LAN1 MACアドレスフィルタリング	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 AP間通信 (WBR)
	無線LAN1 WMM詳細	WMM詳細設定
		WMMパワーセーブ設定
	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LAN2 無線LAN	無線LAN
		仮想AP設定
	無線LAN2 仮想AP	暗号化設定
		MACアドレスフィルタリング設定
	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
		MACアドレスフィルタリング設定一覧
		無線LAN2 AP間通信 (WBR)
	無線LAN2 WMM詳細	WMM詳細設定
		WMMパワーセーブ設定
無線LAN2 ARP代理応答	ARP代理応答設定	
	ARPキャッシュ情報	

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
	管理ツール	USB設定
		HTTP/HTTPS設定
		Telnet/SSH設定
	時計	時刻設定
		自動時計設定
	SYSLOG	SYSLOG設定
	SNMP	SNMP設定
		SNMPv3設定
	LED	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-9600 ※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)
	DNS代理応答：無効
	プライマリーDNSサーバー：空白(設定なし)
	セカンダリーDNSサーバー：空白(設定なし)
	プライマリーWINSサーバー：空白(設定なし)
セカンダリーWINSサーバー：空白(設定なし)	
静的DHCPサーバー	MACアドレス：空白(設定なし) ※最大登録数：32 IPアドレス：空白(設定なし)
「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：64
	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)
スタティックルーティング設定一覧	設定なし
「ポリシールーティング」画面	
送信元ルーティング設定	送信元：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)
送信元ルーティング設定一覧	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

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	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			
「VPN」画面				
IPsec設定	IPsec：無効			
IPsecトンネル設定	トンネルインターフェース：vti0 ※設定範囲「vti0～vti31」			
	トンネル：有効			
	トンネル名：空白(設定なし)			
	インターフェース：eth0			
	認証鍵(Pre-Shared Key)：空白(設定なし) ※半角英数字128文字以内			
	リモートアドレス：空白(設定なし)			
リモートID：IPアドレス				
ローカルID：IPアドレス				
IPsecトンネル設定一覧	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LAN] 無線LAN]画面	
無線LAN設定	無線UNIT：無効 帯域幅：20MHz チャンネル：036CH (5180MHz) パワーレベル：高 DTIM間隔：1
[無線LAN] 仮想AP]画面	
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～ath7) 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)
暗号化設定	ネットワーク認証： オープンシステム(ath0、ath01～ath07) 暗号化方式：なし(ath0、ath01～ath07)
[無線LAN] MACアドレスフィルタリング]画面	
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
MACアドレスフィルタリング設定一覧	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 AP間通信(WBR)」画面	
AP間通信設定	AP間通信：無効
「無線LAN1 WMM詳細」画面	
WMM詳細	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 <input type="checkbox"/> 、AC_BE <input type="checkbox"/> 、AC_VI <input type="checkbox"/> 、AC_VO <input type="checkbox"/> [From Station] ACM：AC_VI <input type="checkbox"/> 、AC_VO <input type="checkbox"/>
WMMパワーセーブ設定	WMMパワーセーブ：無効

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 ARP代理応答」画面(ath0～ath7)	
ARP代理応答	インターフェース：ath0 ARP代理応答：無効 不明なARPの透過：有効 ARPエイジング時間：0(分) ※設定範囲「0～1440」(分)
ARPキャッシュ情報	設定なし
「無線LAN2 無線LAN」画面	
無線LAN設定	無線UNIT：無効 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」
「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) アカウントング：無効(ath1、ath11～ath17)
暗号化設定	ネットワーク認証： オープンシステム(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	
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
MACアドレスフィルタリング設定一覧	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：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 <input type="checkbox"/> 、AC_BE <input type="checkbox"/> 、AC_VI <input type="checkbox"/> 、AC_VO <input type="checkbox"/>
	[From Station]
	ACM：AC_VI <input type="checkbox"/> 、AC_VO <input type="checkbox"/>
WMMパワーセーブ設定	WMMパワーセーブ：無効
「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)

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：空白(設定なし) 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	
USB設定	最大出力電流(USB1)：500mA 最大出力電流(USB2)：500mA USBメモリー：有効 USBアクセス許可： <input checked="" type="checkbox"/> ファームウェアの更新 <input checked="" type="checkbox"/> 設定の保存/復元 USB認証キー：空白(設定なし) ※半角64文字以内
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
「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 コミュニティー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)

5 ご参考に

4. 初期値一覧

■ 管理

設定画面/項目	初期値
「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

- IEEE802.11ax規格準拠
- 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(WEPC4、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、WPA3、WPA3-SAE)
- SSID(Service Set Identifier)
- アクセスポイント機能
- ローミング機能
- ANY接続拒否機能
- 仮想AP機能
- MACアドレスフィルタリング機能
- パワーレベル設定
- 接続端末制限機能
- 同一仮想AP内の端末間通信禁止機能
- WMM★²(Wi-Fi Multimedia)機能
- ARP代理応答
- WMMパワーセーブ
- 認証サーバー(RADIUS/アカウントリング)
- 自動チャンネル機能

■ ネットワーク管理機能

- SYSLOG
- SNMP(MIB-II)

■ ルーター機能

- 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
- VPN

■ その他

- タグVLAN機能
- 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
- PoE機能
- ファームウェアの更新(WEB/USB)
- 設定保存/復元(WEB/USB)
- WWWメンテナンス(HTTP/HTTPS)
- TELNETメンテナンス(TELNET/SSH)
- コンソールメンテナンス(USB)
- LAN2ポートHUB

★¹ 本製品のIEEE802.11ax規格、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。(2023年4月現在)

5 ご参考に

6. 設定項目で使用できる文字列について

下表のように、入力できる文字列が設定項目により異なります。

■ 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

■ 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	3-74ページ参照
		PSK (Pre-Shared Key)	ASCII* ² 、または16進数	3-75ページ参照
AP間通信(WBR)	子機設定	PSK (Pre-Shared Key)	ASCII* ² 、または16進数	3-87ページ参照

■ 管理

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

5 ご参考に

7. 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	AP-9600	SE-900
ルーター	ルーター機能	×	○	○	×	○	○	○	×
	WANポート	×	○* ¹	○* ¹	×	○* ¹	○	○* ¹	×
ネットワーク	ポートベースVLAN	×	×	×	×	○	×	×	×
	パケットフィルタ	○	○	○	○	○	○	○	○
無線	無線UNIT数	2	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* ³	○	○	×	×	×	×	×	○
	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* ⁶	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	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)	○ (MODE)
	屋外対応	×	×	×	○	×	×	×	○

- ★1 AP-90MR、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の場合は[WAN/LAN]ポート、AP-9600の場合は[WAN/LAN1]ポートを設定で切り替えて使用します。
- ★2 SE-900で、アクセスポイントモードとクライアントモードを切り替える機能です。
- ★3 無線UNITで使用する周波数帯(2.4GHz帯/5GHz帯)を切り替える機能です。
AP-9000やAP-900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、AP-9600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、AP-9500、AP-9600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ケーブルを[CONSOLE]ポートに接続します。
使用するUSBケーブルや設定方法など、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。

8. 定格について

■ 一般仕様

電	源	: DC12V±10% [DCプラグ極性: ⊖—●—⊕] ※ACアダプター(付属品)は、AC100V±10% ※PoEは、IEEE802.3bt準拠 最大40W(付属のACアダプター使用時) 最大48W(PoE使用時)
使	用 環 境	: 温度-10~+50℃ (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205(W)×49(H)×205(D)mm(突起物を除く)
重	量	: 約1.0kg(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(POWER、ADVANCE、WAN、2.4GHz、5GHz) ボタン(USB、FUNC、MODE) [USB]ポート×2 : USB Type-A(USB3.0) [CONSOLE]ポート×1 : USB Type-C(USB2.0)

■ 有線部

インターフェース	: [WAN/LAN1]ポート(RJ-45型)×1(Auto MDI/MDI-X) <ul style="list-style-type: none">●IEEE802.3u/100BASE-TX準拠●IEEE802.3ab/1000BASE-T準拠●IEEE802.3bz/2.5GBASE-T準拠●IEEE802.3bt規格準拠 [LAN2]ポート(RJ-45型)×1(Auto MDI/MDI-X) <ul style="list-style-type: none">●IEEE802.3u/100BASE-TX準拠●IEEE802.3ab/1000BASE-T準拠●IEEE802.3bz/2.5GBASE-T準拠●IEEE802.3bt規格準拠
通 信 速 度	: [WAN/LAN1]部 100/1000/2500Mbps(自動切り替え/全二重) [LAN2]部 100/1000/2500Mbps(自動切り替え/全二重)

■ 無線部

国 際 規 格	: IEEE802.11ax準拠、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	: 5180~5720MHz 2412~2472MHz

定格・仕様・外觀等は、改良のため予告なく変更する場合があります。

How the World Communicates

～コミュニケーションで世界をつなぐ～

