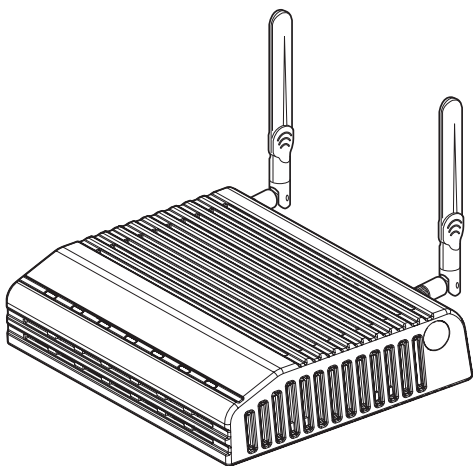


WIRELESS ACCESS POINT
AP-9000

IEEE802.11ac規格準拠
IEEE802.11n規格準拠
IEEE802.11a(W52/W53/W56)/g/b規格準拠
IEEE802.3af規格PoE準拠



Icom Inc.

はじめに

1 ご使用になる前に

2 導入ガイド

3 無線LAN接続[基本編]

4 無線LAN接続[活用編]

5 そのほかの機能について

6 保守について

7 情報表示について

8 ご参考に

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

はじめに

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

本製品は、IEEE802.11ac規格*、IEEE802.11n規格に準拠し、5.2/5.3/5.6GHz帯と2.4GHz帯の2波同時通信ができる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、無線2(5GHz帯)だけです。

本書の表記について

本書は、次の表記規則にしたがって記述しています。

[]表記：オペレーティングシステム(OS)の各ウィンドウ(画面)、ユーティリティ、設定画面の各メニューとそのメニューに属する設定画面の名称を([])で囲んで表記します。

[]表記：タブ名、アイコン名、テキストボックス名、チェックボックス名、各設定画面の設定項目名を([])で囲んで表記します。

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

※Microsoft® Windows® 8.1、Microsoft® Windows® 8.1 Proは、Windows 8.1と表記します。

Microsoft® Windows® 7 Home Premium、Microsoft® Windows® 7 ProfessionalおよびMicrosoft® Windows® 7 Ultimateは、Windows 7と表記します。

Microsoft® Windows Vista® Home Basic、Microsoft® Windows Vista® Home Premium、Microsoft® Windows Vista® BusinessおよびMicrosoft® Windows Vista® Ultimateは、Windows Vistaと表記します。

※本書は、Ver. 2.14のファームウェアを使用して説明しています。

※本書では、Windows 7の画面を例に説明しています。

※本書中の画面は、OSのバージョンや設定によって、お使いになるパソコンと多少異なる場合があります。

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

登録商標/著作権について

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

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

Wi-Fi、WPA、WMM、WPS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、各社の商標および登録商標です。

はじめに

無線LAN規格について

本製品が準拠する無線LAN規格と最大通信速度

周波数帯	無線LAN規格	帯域幅	最大通信速度(理論値)
5.2/5.3/5.6GHz	IEEE802.11ac (W52/W53/W56)	80MHz	867Mbps
		40MHz	400Mbps
		20MHz	173Mbps
	IEEE802.11n (W52/W53/W56)	40MHz	300Mbps
		20MHz	144Mbps
	IEEE802.11a (W52/W53/W56)		54Mbps
2.4GHz	IEEE802.11n	40MHz	300Mbps
			144Mbps
	IEEE802.11g	20MHz	54Mbps
			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、ネットワークの使用状況など)に影響します。

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	IEEE802.11ac (W52/W53/W56)	約30m	約100m
	IEEE802.11n (W52/W53/W56)		
	IEEE802.11a (W52/W53/W56)		
2.4GHz	IEEE802.11n	約30m	約100m
	IEEE802.11g		
	IEEE802.11b		

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

★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。

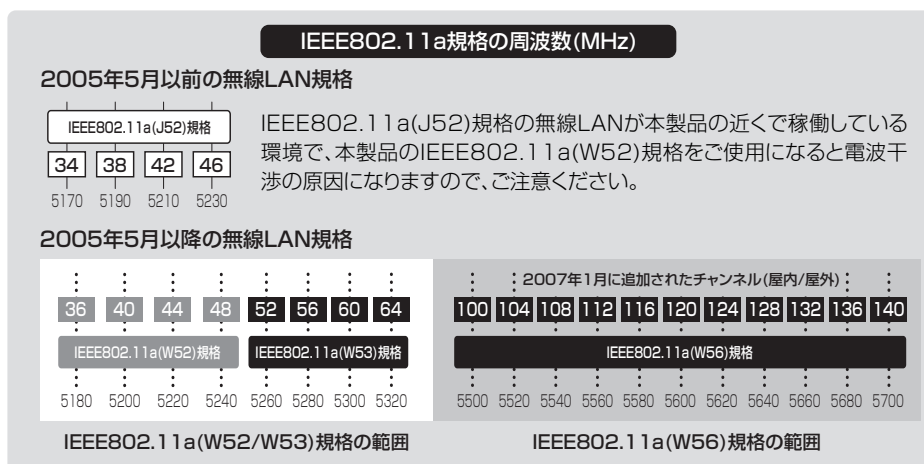
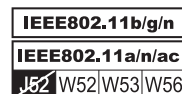
はじめに

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、2.4GHz帯用(無線1)、5GHz帯用(無線2)の無線LANユニットが内蔵されています。必要に応じて、チャンネルや帯域幅を変更してください。

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

※帯域幅を80MHzに設定できるのは、無線2(5GHz帯)だけです。

はじめに

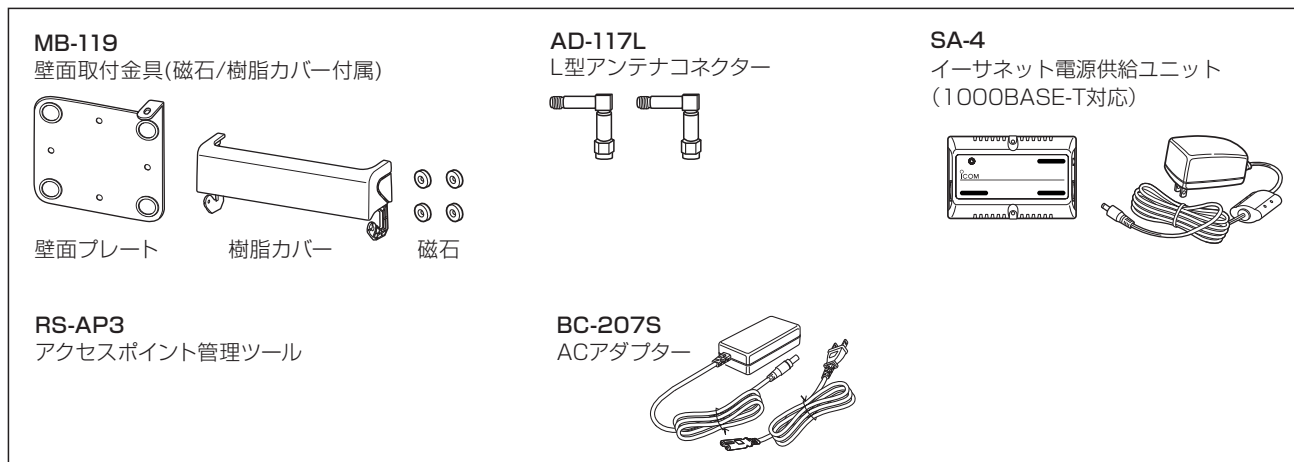
本製品の概要について

- ◎IEEE802.11ac規格、IEEE802.11n規格に準拠し、最大867Mbps(理論値)の速度で通信できます。
 - ※IEEE802.11ac規格を使用できるのは、5GHz帯(無線2)だけです。
 - さらに、最大867Mbps(理論値)で使用するには、帯域幅を「80MHz」に設定してください。
 - ※IEEE802.11ac規格、IEEE802.11n規格での通信は、暗号化方式を「なし」、または「AES」に設定している場合に有効です。
- ◎IEEE802.11a(W52/W53/W56)規格、IEEE802.11g/b規格に準拠し、5GHz帯と2.4GHz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端末とは通信できません。
- ◎異なる無線LAN規格の機器を同時に使用する環境において、速度低下を緩和するプロテクション機能を搭載しています。
- ◎DFS機能の搭載により、5.3/5.6GHz帯のチャンネルで通信しているときは、気象レーダーなどへの電波干渉を自動で回避します。
- ◎IEEE802.1QのVLAN規格に準拠した仮想AP機能を搭載していますので、本製品1台で最大16グループ(2.4GHz帯、5GHz帯ごとに最大8グループ)の無線ネットワークを構築できます。
 - ※ルーター機能とは併用できません。
- ◎ポートベースVLAN機能搭載により、本製品の[WAN/LAN]ポート、[LAN]ポートを論理的に2つのVLANグループに分割して、異なるVLANグループ間の通信を遮断することで、セキュリティの向上やネットワークの負荷を軽減できます。
 - ※ルーター機能とは併用できません。
- ◎本製品の[WAN/LAN]ポートは、トランキングポートとしても設定できます。
 - この場合、IEEE802.1QのVLAN規格に準拠したタグVLANとして使用できます。
 - VLAN対応スイッチと併用することで、複数のVLANグループを1本のLANケーブルで接続できます。
 - ※ルーター機能とは併用できません。
- ◎ネットワーク認証は、「共有キー」、「オープンシステム」、「IEEE802.1X」、「WPA」、「WPA2」、「WPA-PSK」、「WPA2-PSK」に対応しています。
- ◎「MAC認証」、「IEEE802.1X」、「WPA」、「WPA2」を設定すると、認証にRADIUSサーバーを使用できます。
- ◎ユーザー単位で端末を認証するWeb認証機能を搭載しています。
- ◎認証VLAN有効時、RADIUSサーバーを利用した認証結果(応答属性)に応じて、無線LAN端末の所属VLAN IDをグループ分けできます。
- ◎IEEE802.3afに準拠したPoE受電機能に対応していますので、弊社別売品の「イーサネット電源供給ユニット(SA-4)」、またはIEEE802.3af規格対応のHUB(市販品)から電源を受電できます。
- ◎「Wi-Fiアライアンス」が提唱するWPS(Wi-Fi Protected Setup)機能の搭載により、SSIDと暗号化(WPA-PSK/WPA2-PSK)を本製品(仮想AP)、およびWPS機能対応の無線LAN端末に自動設定できます。
 - ※2017年1月現在、本製品は、Wi-Fiアライアンスの認定を取得していません。
- ◎市販のUSBメモリーを本製品の[USB]ポートに差し込んでから電源を入れることで、本製品の設定を自動保存できます。
 - また、あらかじめ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たUSBメモリーを差し込んでから電源を接続することで、自動で設定の復元やファームウェアのバージョンアップができます。
 - ※使用するには、指定したファイル名で設定ファイル、およびファームウェアファイルを保存する必要があります。
- ◎本製品の設定画面からUSB認証キーを設定することで、本製品の[USB]ポートから設定ファイルが持ち出されることや意図しない設定の変更などを防止できます。
- ◎FTTH、ADSL、VDSL、CATV対応のルーター機能を搭載しています。
 - ※本製品の[WAN/LAN]ポートは、回線種別を変更(DHCPクライアント/固定IP/PPPoE)することで、WAN側接続用ポートに切り替わります。
- ◎ネットワーク管理機能として、SNMPをサポートしています。
- ◎本製品は、免許不要・資格不要です。

はじめに

別売品について

(2017年1月現在)



【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
無線設定	無線LAN	無線LAN設定	チャンネル	001CH(2412MHz)(無線1) 036CH(5180MHz)(無線2)
			帯域幅	20MHz
			仮想AP	仮想AP設定
			SSID	WIRELESSLAN-0
			暗号化設定	ネットワーク認証
			暗号化方式	なし
管理	管理者	管理者パスワードの変更	管理者ID	admin(変更不可)
			現在のパスワード	admin(半角小文字)

【不正アクセス防止のアドバイス】

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

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

はじめに

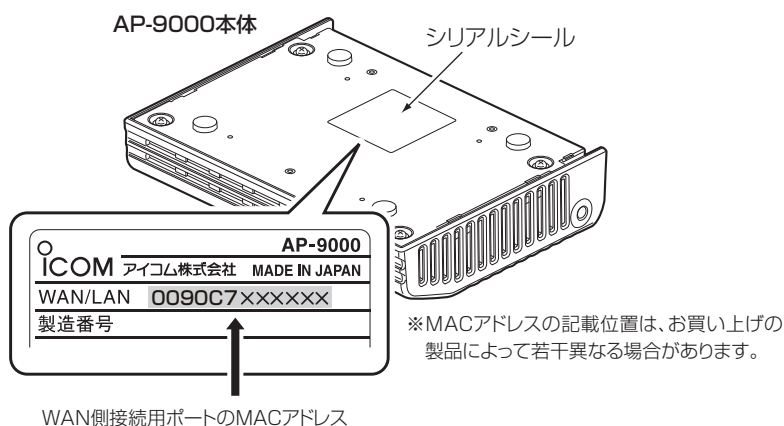
本体MACアドレスが必要なときは

本製品のシリアルシールに、WAN側接続用ポートのMACアドレス(機器固有の番号)が12桁で記載されています。

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

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

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



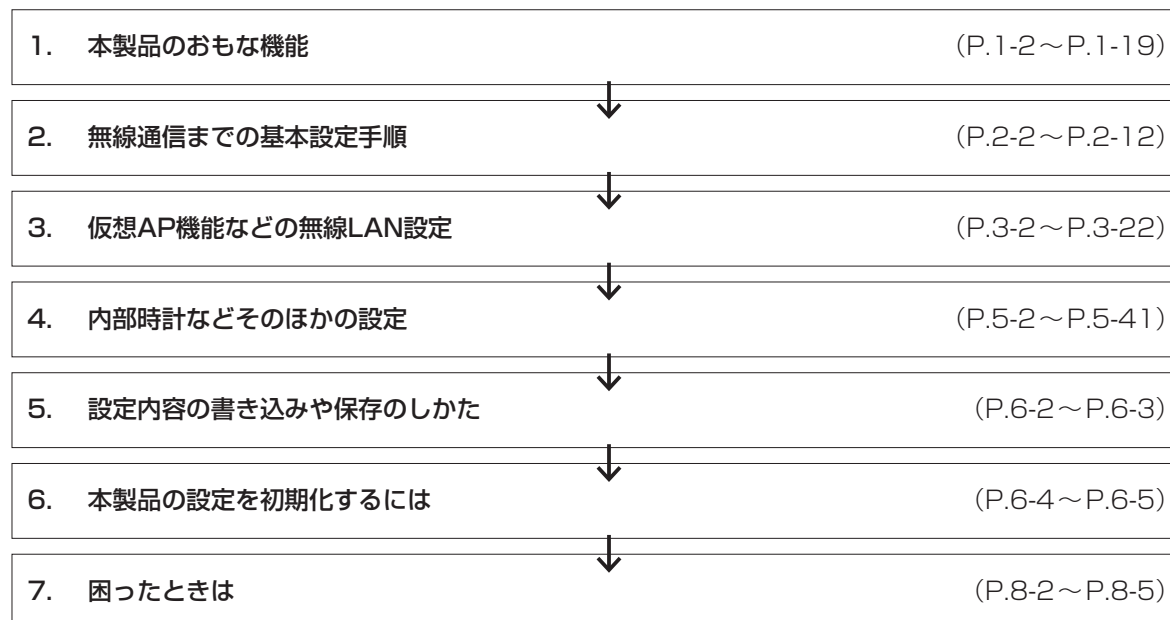
ご参考に

上記のMACアドレスやLAN側のMACアドレスは、本製品の設定画面(P.6-6)から確認できます。

はじめに

ご使用までの流れ

本製品を設定されるときは、次の手順にしたがってお読みください。



はじめに

オンラインヘルプについて

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

The image illustrates the process of accessing online help for the DHCP server configuration. It shows two states of the configuration page:

- Top Screenshot:** The 'DHCPサーバー設定' page is shown. The '割り当て個数' (Number of assignments) field is highlighted with a mouse cursor and a question mark icon. A callout box labeled '1 クリック' (Click) points to this field.
- Bottom Screenshot:** The 'DHCPサーバー設定' page is shown with the '割り当て個数' field set to '30'. A callout box labeled '2 確認する' (Check) points to the field. A dialog box titled '割り当て個数' (Number of assignments) is displayed, providing a warning: '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。設定できる範囲は、[0-128](個)です。[0]を設定した時は、自動割り当てを行いません。(出荷時の設定:30)'.

はじめに

もくじ

はじめに	i	7. WMM詳細について	4-13
本書の表記について	i	8. レート設定について	4-20
登録商標/著作権について	i	9. ARP代理応答について	4-26
無線LAN規格について	ii	10. IP Advance Radio Systemについて	4-27
無線通信チャンネルについて	iii	11. 本製品のPINコードについて	4-28
本製品の概要について	iv	5. そのほかの機能について	5-1
別売品について	v	1. 設定画面へのアクセスを制限するには	5-2
出荷時のおもな設定値	v	2. 内部時計を設定するには	5-3
本体MACアドレスが必要なときは	vi	3. 本製品のDHCPサーバー機能を使用するには	5-4
ご使用までの流れ	vii	4. 「ルーティング」画面について	5-6
オンラインヘルプについて	viii	5. パケットフィルターの使用例について	5-8
1. ご使用になる前に	1-1	6. Web認証機能を設定するには	5-13
1. 各部の名称と機能	1-2	7. 「管理」画面について	5-19
2. 本製品のおもな機能	1-8	8. 本製品のルーター機能を使用するには	5-29
2. 導入ガイド	2-1	9. ポートベースVLAN機能を設定するには	5-38
1. 設定に使うパソコンについて	2-2	10. POPCHAT@Cloud 連携機能を設定するときは	5-42
2. 設定用のパソコンに固定IPアドレスを設定する	2-3	6. 保守について	6-1
3. 設定に使うパソコンを接続する	2-4	1. 設定内容の確認または保存	6-2
4. 設定画面にアクセスするには	2-7	2. 保存された設定の書き込み(復元)	6-3
5. 本体IPアドレスを変更するときは	2-8	3. 設定を出荷時の状態に戻すには	6-4
6. 無線ネットワーク名と暗号化を手動で設定する	2-9	4. ファームウェアをバージョンアップする	6-6
7. WPS機能で自動設定したいSSIDと共有鍵(キー)を指定する	2-11	5. USBメモリーによる自動設定機能について	6-10
3. 無線LAN接続[基本編]	3-1	6. USBメモリーから自動で設定を復元するには	6-14
1. 無線通信を停止するには	3-2	7. USBメモリーからファームウェアをバージョンアップするには	6-17
2. IEEE802.11ac規格(5GHz帯)の通信をするには	3-3	8. USBメモリー用の認証キーを設定するには	6-19
3. [WEP RC4]暗号化を設定するには	3-4	7. 情報表示について	7-1
4. 無線ネットワーク名と暗号化を自動で設定するときは	3-9	1. 「TOP」画面について	7-2
5. 仮想APを設定するには	3-12	2. 「ネットワーク情報」画面について	7-3
6. 無線AP(アクセスポイント)間通信機能を設定するには	3-14	3. 「SYSLOG」画面について	7-6
7. MACアドレスフィルタリングを設定するには	3-22	4. 「無線設定情報一覧」画面について	7-7
4. 無線LAN接続[活用編]	4-1	8. ご参考に	8-1
1. チャンネルの自動設定について	4-2	1. 困ったときは	8-2
2. アカウンティング設定について	4-4	2. Telnetで接続するには	8-6
3. MAC認証サーバー(RADIUS)設定について	4-6	3. 設定画面の構成について	8-8
4. RADIUS設定について	4-8	4. 設定項目の初期値一覧	8-11
5. 認証VLANについて	4-10	5. 機能一覧	8-22
6. ネットワーク監視設定について	4-12	6. 設定項目で使用できる文字列について	8-23
		7. PoEによる電源供給について	8-24
		8. 弊社製無線アクセスポイントの機能対応表	8-25
		9. 定格について	8-26

この章では、
本製品のおもな機能などについて説明しています。

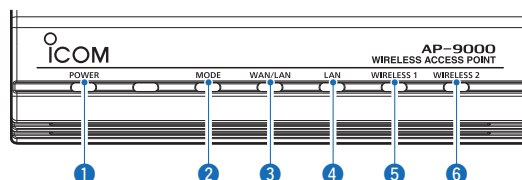
1. 各部の名称と機能	1-2
■ 上部部	1-2
■ 後面部	1-4
■ マスクシートの取り付け	1-6
■ フェライトコアの取り付け	1-6
■ クッションの取り付け	1-6
■ アンテナの取り付け	1-7
2. 本製品のおもな機能	1-8
■ アクセスポイント機能について	1-8
■ 無線ネットワーク名(SSID)について	1-8
■ 接続端末制限機能について	1-8
■ IEEE802.11ac 規格について	1-8
■ IEEE802.11n 規格について	1-8
■ 無線 LAN セキュリティーについて	1-9
■ ローミング機能について	1-10
■ 無線 AP (アクセスポイント)間通信機能について	1-11
■ 仮想 AP 機能について	1-13
■ DFS 機能とチャンネルの自動設定について	1-14
■ WPS 機能について	1-15
■ ルーター機能について	1-16
■ ポートベースVLAN 機能について	1-17
■ PoE 機能について	1-19

1 ご使用になる前に

1. 各部の名称と機能

■ 上面部

各ランプのおもな動作と状態について説明します。

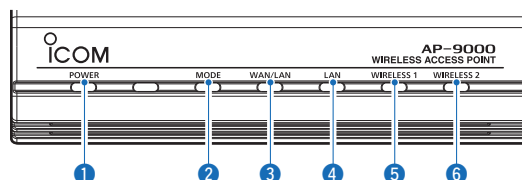


- 1 POWER***¹ 電源と起動時の状態を表示します。
- 緑点灯：電源ON
 - 赤点灯：USBロード失敗
 - ☀ 赤点滅：IPアドレス衝突(起動時のみ検知)
 - 橙点灯：USBロード時
 - ☀ 橙点滅：起動時
 - 消 灯：電源OFF
- 2 MODE** <WPS>ボタンと<INIT>ボタン操作時の状態を表示します。
- 緑点灯：WPS成功時
 - ☀ 緑点滅：<INIT>ボタン操作時
WPS実行中
 - ☀ 赤点滅：WPS失敗時
 - 橙点灯：オンライン更新ファームウェア検知時
- 3 WAN/LAN** [WAN/LAN]ポートの接続/通信状態を表示します。
- 緑点灯：リンク時 (1000BASE-T)
 - ☀ 緑点滅：データ通信中 (1000BASE-T)
 - 橙点灯：リンク時 (10BASE-T/100BASE-TX)
 - ☀ 橙点滅：データ通信中 (10BASE-T/100BASE-TX)
 - 消 灯：リンク未確立時
- 4 LAN** [LAN]ポートの接続/通信状態を表示します。
- 緑点灯：リンク時 (1000BASE-T)
 - ☀ 緑点滅：データ通信中 (1000BASE-T)
 - 橙点灯：リンク時 (10BASE-T/100BASE-TX)
 - ☀ 橙点滅：データ通信中 (10BASE-T/100BASE-TX)
 - 消 灯：リンク未確立時
- ★1 LED消灯モードが「有効」に設定されているときは明るさが暗くなります。(出荷時の設定：無効)
※「有効(完全消灯)」に設定されているときは、すべてのランプが消灯します。

1 ご使用になる前に

1. 各部の名称と機能

■ 上面部(つづき)



- 5 WIRELESS 1 無線1(2.4GHz帯)の状態を表示します。
- 緑点灯 : 端末が1台以上帰属時^{★2}
 - 橙点灯 : 2.4GHz帯側有効時 帰属端末なし
 - 消 灯 : 2.4GHz帯側無効時
- 6 WIRELESS 2 無線2(5GHz帯)の状態を表示します。
- 緑点灯 : 端末が1台以上帰属時^{★2}
 - 橙点灯 : 5GHz帯側有効時 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帯側無効時

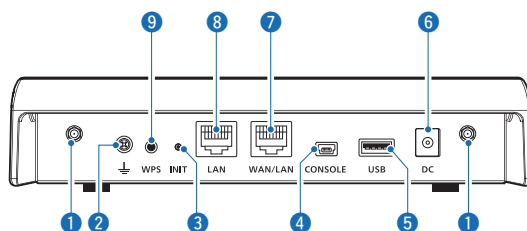
★2 無線LANユニット有効時、本製品と通信できる無線LAN端末が存在しない、または無線通信しない状態がつづく
と、橙点灯に変わります。なお、橙点灯に変わるまでの時間は、通信状態によって異なります。

1 ご使用になる前に

1. 各部の名称と機能(つづき)

■ 後面部

接続各部と各ボタンの名称について説明します。



- ① アンテナコネクタ 付属のアンテナを接続します。(P1-7)
※十分な性能でご使用いただくため、アンテナは、必ず2本とも接続してください。
- ② アース端子 アース線(市販品)を接続します。
- ③ <INIT>ボタン 設定を初期化するときを使用します。(P6-4)
※ペン先などを利用して押してください。
- ④ [CONSOLE]ポート
(USB2.0/1.1) 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。
※本製品とパソコンをUSBケーブルで接続し、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については、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(miniBタイプ)、ターミナルソフトウェアは、別途ご用意ください。
- ⑤ [USB]ポート
(USB2.0/1.1) 設定復元、ファームウェアのバージョンアップ用として使用するUSBメモリー(市販品)を差し込みます。
※ご使用になるときは、本製品のACアダプターを取りはずしてから、USBメモリーを[USB]ポートの奥まで挿入してください。
※すべてのUSBメモリーでの動作を保証するものではありません。
※USBメモリー以外のUSB機器などを接続しないでください。
使用条件については、本書6-9ページをご覧ください。

USBドライバーおよびインストールガイドのダウンロードについて

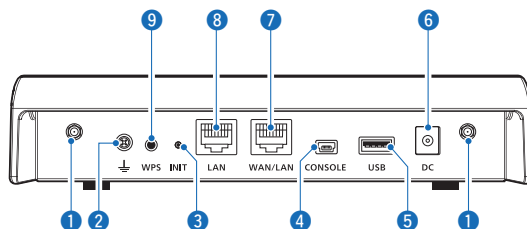
インターネットから、弊社ホームページ <http://www.icom.co.jp/> にアクセスしていただき、サポート情報(サポート情報→各種ダウンロード)よりダウンロードしてください。

※弊社ホームページからダウンロードする手順は、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

■ 後面部(つづき)



- 6 DCジャック**…………… 本製品に付属、または別売品の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。
- 7 [WAN/LAN]ポート (RJ-45型)**…………… 回線種別の設定によって、用途が異なります。(P.1-16、P.5-29)
※PoEから受電する場合は、回線種別の設定に関係なく使用できますので、SA-4 (別売品)の[To Wireless Unit]ポート、またはIEEE802.3af対応のHUBと接続してください。
- ◎[LANポートとして使用する](出荷時の設定)に設定時
[LAN]ポートに切り替わりますので、HUB(VLAN対応スイッチなど)やルータータイプモデムなどのネットワーク機器と接続します。
- ◎[DHCPクライアント]/[固定IP]/[PPPoE]に設定時
[WAN]ポートに切り替わりますので、ADSL、VDSL、CATVでお使いのブリッジタイプモデム、またはFTTHでお使いの回線終端装置と接続します。
- 8 [LAN]ポート (RJ-45型)**…………… HUBなどのネットワーク機器と接続します。
※PoEから受電する場合は、SA-4(別売品)の[To Wireless Unit]ポート、またはIEEE802.3af対応のHUBと接続してください。
- 9 (WPS)ボタン**…………… WPS機能を使用して、暗号化自動設定を開始するときに使用します。
※出荷時、または全設定を初期化したときは、WPS設定で使用するインターフェースを設定してからご使用ください。(P.2-11)

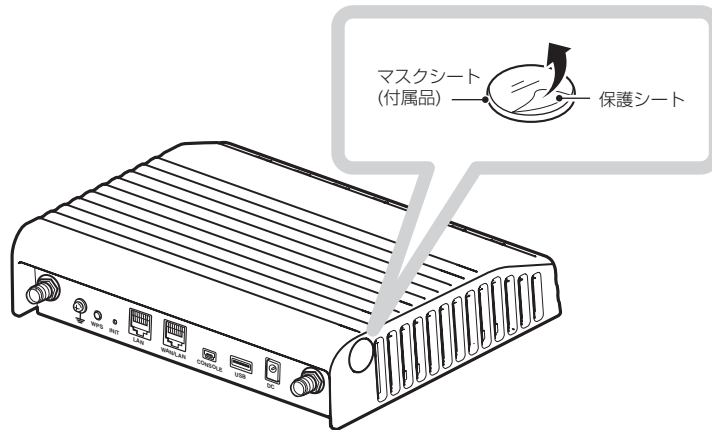
1 ご使用になる前に

1. 各部の名称と機能(つづき)

■ マスクシートの取り付け

保護シートをはがして、本製品の両側面にマスクシートを貼り付けます。

※別売品(MB-119)の樹脂カバーを本製品に取り付ける場合は、樹脂カバーをビスで固定するまで、マスクシートを貼り付けないでください。

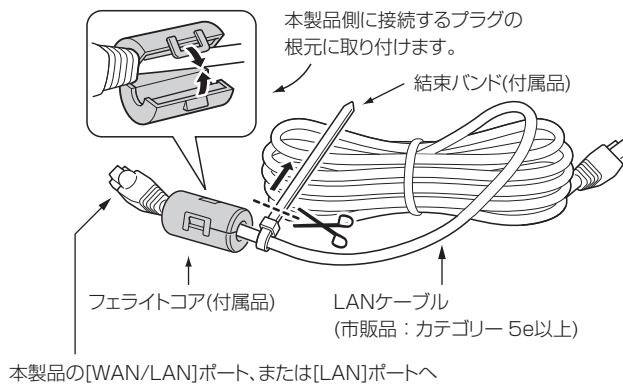


■ フェライトコアの取り付け

電波障害対策のため、下図の位置に必ず取り付けてください。

※図のように取り付けない場合、電波障害を引き起こす原因になります。

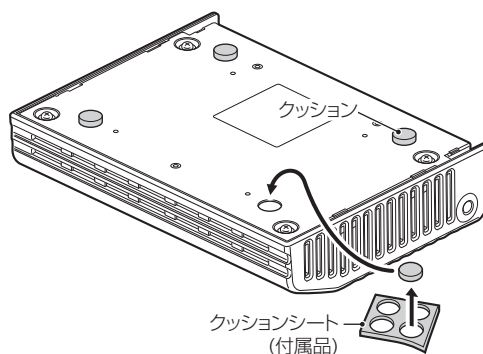
※本製品の[LAN]ポート、[WAN/LAN]ポートの両方をご使用になる場合は、[WAN/LAN]ポート側にフェライトコアを取り付けてください。



■ クッションの取り付け

クッションは、シートからはずして、下記のように本製品の底面部に貼り付けます。

※丸く型抜きされたクッションが4個、粘着面を保護するシートの上に付いています。



1 ご使用になる前に

1. 各部の名称と機能(つづき)

■ アンテナの取り付け

2本のアンテナは、ダイバーシティーやMIMOとして機能しますので、マルチパスに強く、安定した電波状態で通信できます。

取り付けるときは、アンテナの根元を右方向に手で締まる程度まで回します。

アンテナは、3段階の角度(0/45/90度)に折り曲げて使用できます。

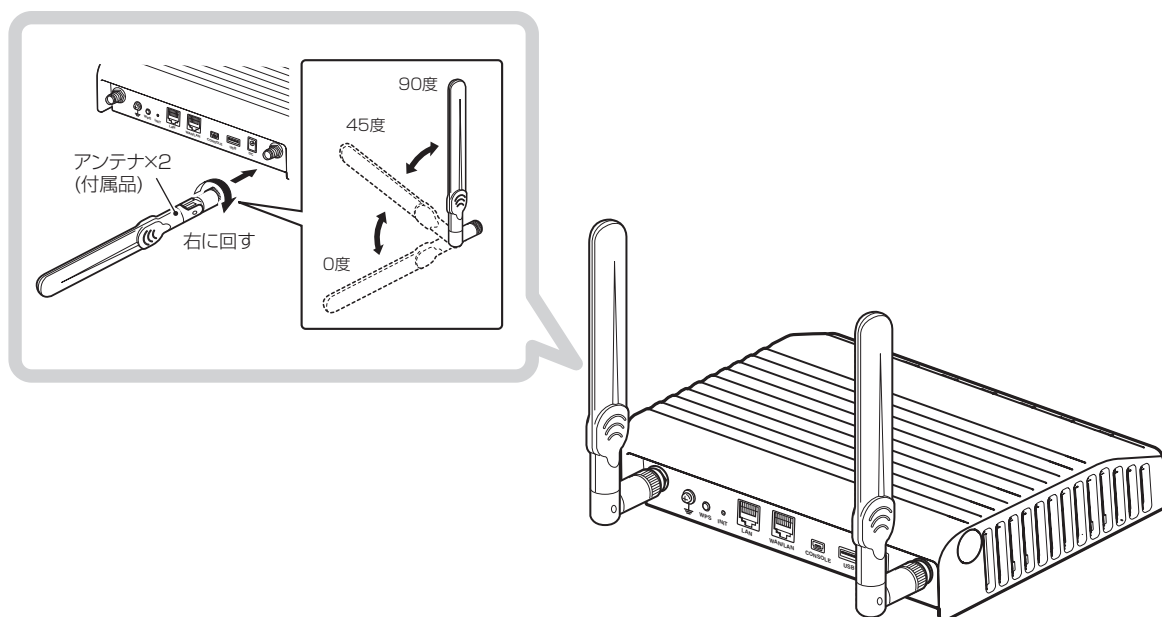
また、折り曲げた状態で、左右に回転できます。

取りはずすときは、アンテナの根元を持って左方向に回します。

※十分な性能でご使用いただくため、アンテナは、2本とも取り付けてください。

※電波状況が悪いと感じられたときは、アンテナの向き、または本製品の設置場所を変更してください。

※AD-117L(別売品)を本製品に取り付ける場合は、AD-117Lの取扱説明書にしたがってアンテナを接続してください。



△警告

本製品に取り付けたアンテナを持って本製品を振り回さないでください。
本人やほかの人に当たるなどして、けがや破損、および故障の原因になります。

ご注意

技術基準適合証明(工事設計認証)を受けていますので、付属のアンテナ以外は使用できません。

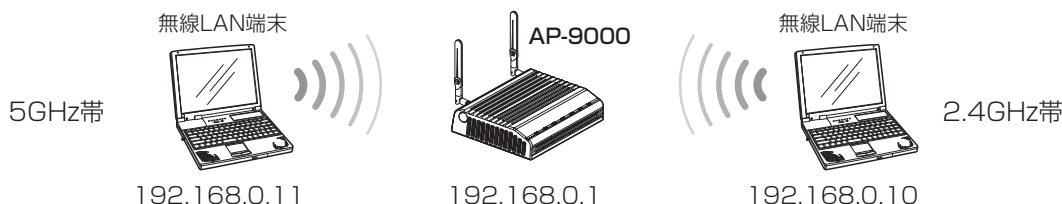
1 ご使用になる前に

2. 本製品のおもな機能

■ アクセスポイント機能について

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

※IEEE802.11規格(14CH)の無線LAN端末とは通信できません。



■ 無線ネットワーク名(SSID)について

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.2-9)

※異なるSSIDを設定している無線LAN端末は接続できません。

※本製品には2.4GHz帯用と5GHz帯用の無線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。

■ 接続端末制限機能について

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1(ath0~ath7)、無線2(ath8~ath15)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LANユニットで最大128台(無線AP間通信を含む)までです。

■ IEEE802.11ac規格について

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

★IEEE802.11ac規格での通信は、暗号化方式を「なし」、または「AES」に設定している場合に有効です。

IEEE802.11ac規格を利用できるのは、無線2(5GHz帯)だけです。

さらに、最大867Mbps(理論値)で使用するには、帯域幅を「80MHz」に設定してください。(P.3-3)

※IEEE802.11n/a規格と互換性があります。

■ IEEE802.11n規格について

最大2倍の周波数帯域幅(チャンネル)と複数のアンテナを使用してデータを送受信することで、最大300Mbps*(理論値)の速度で通信できます。

★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。

さらに、最大300Mbps(理論値)で使用するには、帯域幅を「40MHz」に設定してください。

※IEEE802.11a/g/b規格と互換性があります。

1 ご使用になる前に

2. 本製品のおもな機能(つづき)

■ 無線LANセキュリティについて

本製品は、無線LAN通信に必要な次のセキュリティを搭載しています。

※無線LAN端末側の搭載機能については、ご使用になる端末の取扱説明書でご確認ください。

◎MACアドレスフィルタリング

あらかじめ本製品の各仮想AP(ath0～ath15)に登録されたMACアドレスを持つ無線LAN端末だけにアクセスを許可、または拒否するときに使用します。

◎WEP RC4^{*1}

暗号鍵(キー)が一致した場合に、無線LAN端末と接続できる暗号化方式です。

※「WEP RC4」暗号化方式しか対応していない無線LAN端末と接続するときに使用します。

◎TKIP^{*2}

暗号鍵(キー)を一定間隔で自動更新しますので、「WEP RC4」より強力です。

◎AES^{*2}

無線LAN通信で標準的に使われている強力な暗号化方式です。

◎WPA/WPA2

RADIUSサーバーで「IEEE802.1X」認証します。

◎WPA-PSK/WPA2-PSK

RADIUSサーバーを使用しない簡易的な認証方式で、共有鍵(キー)を使用します。

◎IEEE802.1X^{*3}

RADIUSサーバーを使用して、無線LAN端末からのアクセスに認証を設ける機能です。

◎MAC認証

RADIUSサーバーを使用して、無線LAN端末のMACアドレスを認証します。

※1 通信相手と暗号化方式や鍵(キー)の設定が異なるときは、通信できません。

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

※2 IEEE802.11n規格、IEEE802.11ac規格での通信は、暗号化方式を「なし」、または「AES」に設定している場合に有効です。

無線1(2.4GHz帯)での無線AP間通信では、必ず暗号化設定が必要で、「AES」で暗号化されます。(P.3-16)

※3 WEP RC4以外の暗号化方式では使用できません。

ネットワーク認証と暗号化方式の対応について

	オープンシステム	共有キー	オープンシステム/ 共有キー	WPA/WPA2	WPA-PSK/WPA2-PSK	IEEE802.1X
なし	○	×	○	×	×	×
WEP RC4	○	○	○	×	×	○
TKIP	×	×	×	○	○	×
AES	×	×	×	○	○	×

不正アクセス防止のアドバイス

本製品に設定する暗号鍵(WEPキー)/共有鍵(Pre-Shared Key)は、容易に推測されないものにしてください。

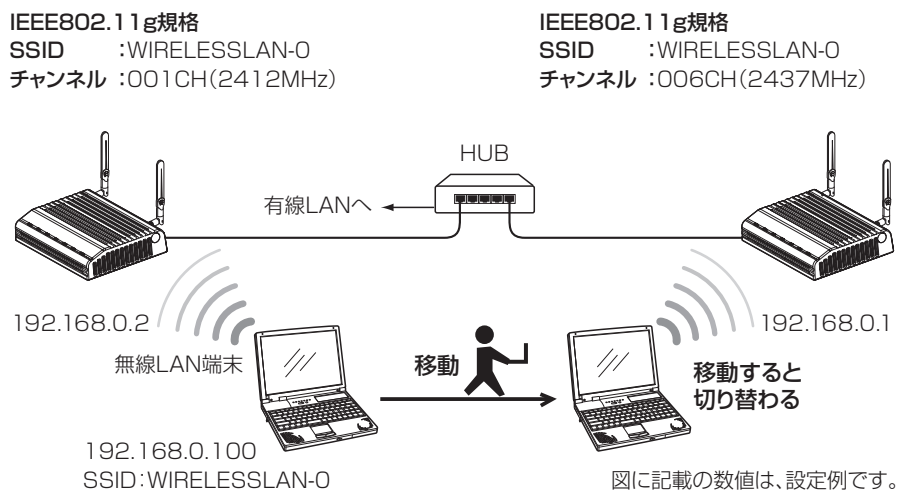
数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた複雑なものにし、さらに定期的に暗号鍵を変更されることをおすすめします。

1 ご使用になる前に

2. 本製品のおもな機能(つづき)

■ ローミング機能について

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



ローミング機能を使用するには

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

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

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

※ローミングのしきい値は、無線LAN端末側に依存します。

1 ご使用になる前に

2. 本製品のおもな機能(つづき)

■ 無線AP(アクセスポイント)間通信機能について

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。

※無線AP間通信機能の設定例については、本書3-15ページ～3-21ページをご覧ください。

無線AP間通信機能を使用するには

本製品に内蔵された無線LANユニットにより、通信できる相手側の無線アクセスポイント(弊社製)と使用方法が異なりますのでご注意ください。

無線LANユニット		AP-80	AP-80HR	AP-80M	AP-80MR	AP-800	AP-8000	AP-90M	AP-90MR	AP-900	AP-9000	SE-900 (アクセスポイントモード時)
無線1 (WDS)	2.4GHz帯	○	○	○	○	○	○	○	○	○	○	×
無線2 (WBR)	5GHz帯	×	×	×	×	×	×	○	○	○	○	○

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

※2017年1月現在、上記以外の製品では、無線AP間通信できません。

なお、SE-900は、2.4GHz/5GHzの2波同時通信には対応していません。

※5GHz帯で無線AP間通信が利用できるのは、5.2GHz帯だけです。

無線1(2.4GHz帯)で使用する場合(WDS)(P.3-15)

◎チャンネルを「自動」に設定した場合(P.4-2)、無線AP間通信機能は動作しません。

◎無線アクセスポイントに内蔵された無線LANユニットのBSSID★¹を互いに登録し合う必要があります。

◎最大8台分の相手を登録して、1対8の通信ができます。

★¹ 本製品のBSSIDは、「AP間通信 (WDS)」画面で確認できます。(P.3-15)

下図の例では、[B]側のBSSIDを[A]側に、[A]側のBSSIDを[B]側に登録します。

本製品と同じチャンネルで稼働するAP-80、AP-80HR、AP-80M、AP-80MR、AP-800、AP-8000、AP-90M、AP-90MR、AP-900、AP-9000(本製品)のBSSIDだけを自動検出するため、BSSIDを容易に登録できます。

◎無線AP間通信するには、チャンネル、および無線AP間通信専用の共有鍵(PSK: Pre-Shared Key)★²★³を相手側と同じ設定にします。

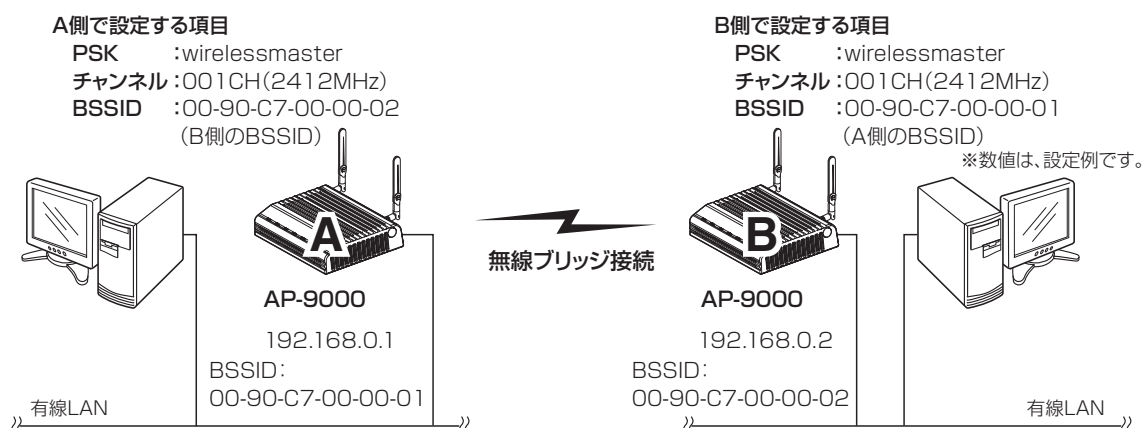
★² 「AES」方式の暗号化を本製品の「AP間通信 (WDS)」画面で設定します。(P.3-16)

★³ 各仮想AP(ath0～ath7)のSSIDや暗号化の設定は、本製品と無線LAN端末の接続だけに使用しますので、無線AP間通信には関係ありません。

◎無線AP間通信する相手側のBSSIDだけを登録してご使用ください。

必要でないBSSIDが複数登録されている場合は、通信速度低下の原因になります。

◎VLAN IDの有無に関係なく、すべてのパケットが透過されます。



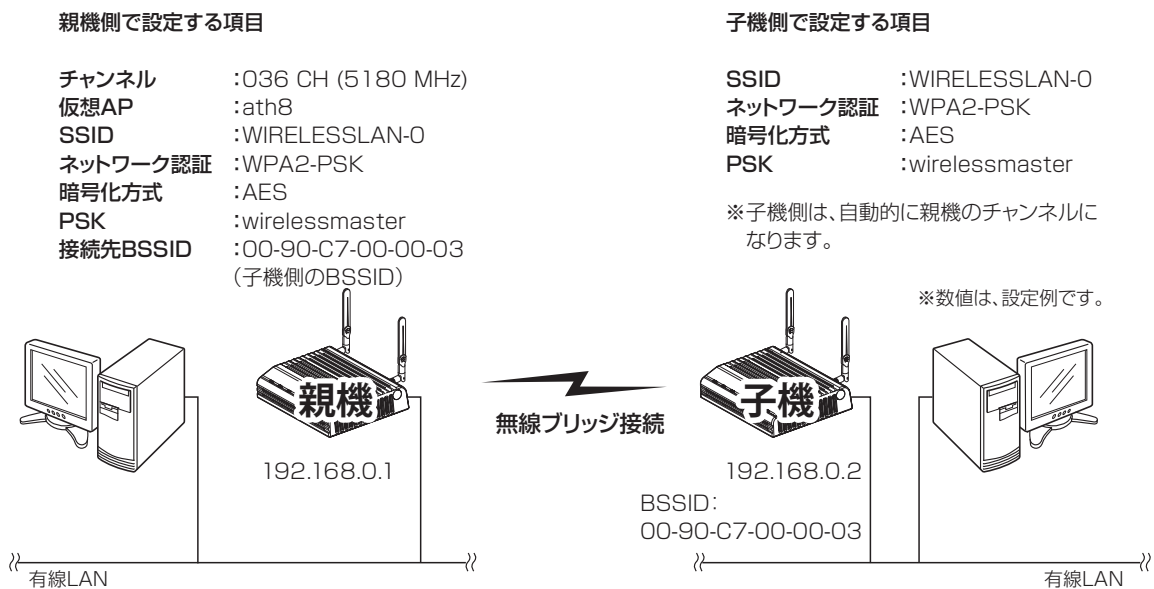
1 ご使用になる前に

2. 本製品のおもな機能

■ 無線AP(アクセスポイント)間通信機能について(つづき)

無線2(5GHz帯)で使用する場合(WBR)(P.3-17)

- ◎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、チャンネル詳細設定で5.3/5.6GHz帯のチャンネルを選択した場合(P.4-3)、無線AP間通信機能は動作しません。
- ◎親機側の仮想AP「ath8」*の設定内容で無線AP間通信(WBR)して、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。(2017年1月現在)
 - 「ath0」：アクセスポイントモードのSE-900
 - 「ath4」：AP-90M、AP-90MR
 - 「ath8」：AP-900、AP-9000



- ◎子機側は、SSIDと暗号化が一致する親機をスキャンします。
 - ※子機側の「AP間通信」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、無線2(5GHz帯)の仮想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. 本製品のおもな機能(つづき)

■ 仮想AP機能について

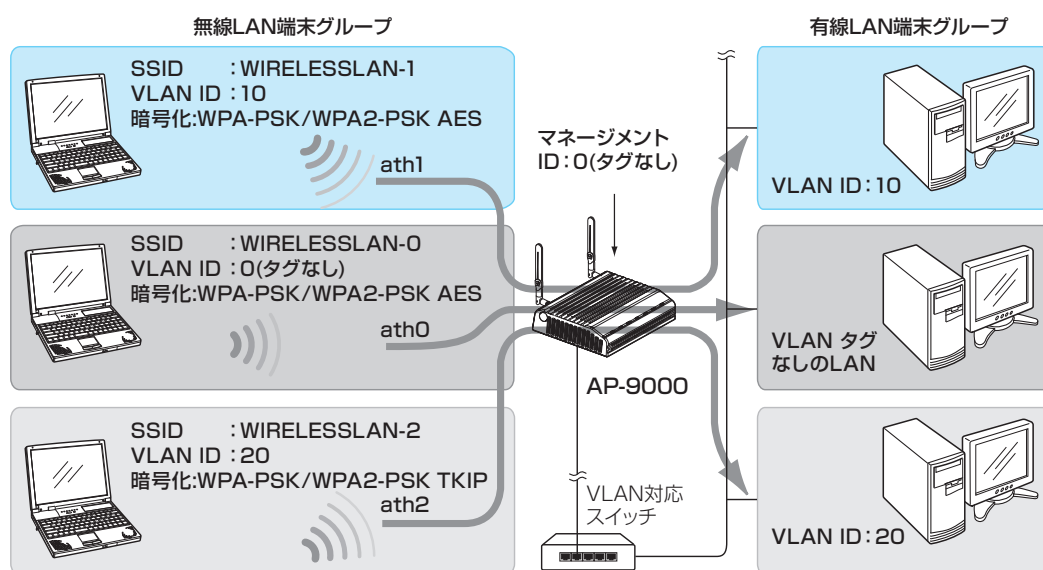
本製品1台で、条件(SSID/暗号化方式/VLAN ID)の異なる無線LAN端末グループを複数構成できます。

※各仮想APのVLAN機能とルーター機能は併用できません。

※下記の図は、「ath0」～「ath2」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。

設定例については、本書3-12ページ～3-13ページをご覧ください。

※通信速度低下を防止するため、無線1、無線2、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(ath0～ath15)*を使用して、最大16グループの無線ネットワークを構築できます。

★IEEE802.11ac規格の無線ネットワークを構築する場合は、無線2(5GHz帯)の「仮想AP」画面で仮想AP(ath8～ath15)を設定します。

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

◎各仮想AP(ath0～ath15)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[Management ID]が「0」(タグなし)に設定されていますので、VLAN IDが設定されたネットワークからは、本製品の設定画面にアクセスできません。

◎各仮想AP(ath0～ath15)の通信レートを、「レート」画面で設定できます。

ベーシックレートを設定した場合、無線LAN端末側が、その速度を使用できることが条件となります。

たとえば、ベーシックレートを設定したレートで通信できない無線LAN端末は、本製品に接続できません。

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

1 ご使用になる前に

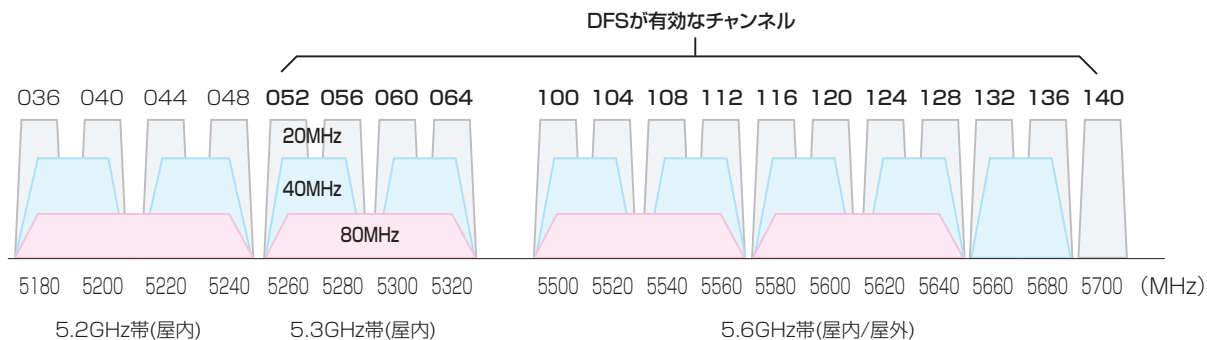
2. 本製品のおもな機能(つづき)

■ DFS機能とチャンネルの自動設定について

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。

※DFS機能が有効なチャンネルが選択されているとき、無線AP間通信機能は動作しません。

チャンネルの自動設定など詳細については、本書4-3ページをご覧ください。



◎本製品の設定画面で5.3/5.6GHz帯(052～140)のチャンネルを選択して、再起動すると、電源投入直後の1分間はレーダー波を検出します。

レーダー波検出中は、本製品の[WIRELESS 2]ランプが \odot 橙点滅して、本製品へのアクセスをすべて停止します。本製品の起動中、または運用中にレーダー波を検出したときは、自動的に電波干渉しないチャンネルに変更されます。

※レーダー波を検出したチャンネルは、検出してから30分間利用できません。

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

◎5.6GHz帯の全チャンネル(100～140)でレーダー波を検出した場合は、[WIRELESS 2]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、上図のようにチャンネルを束ねて使用します。

※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。

◎本製品の設定画面でチャンネルを「自動」に設定すると、本製品の起動時にほかの無線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。

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

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

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

1 ご使用になる前に

2. 本製品のおもな機能(つづき)

■ WPS機能について

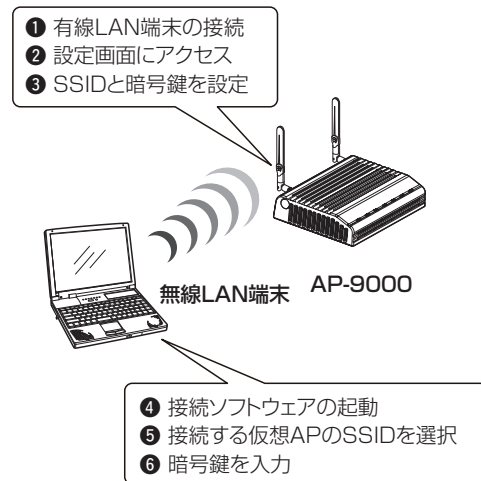
「Wi-Fiアライアンス」が提唱する機能で、SSIDと暗号化(WPA-PSK/WPA2-PSK)を本製品とWPS機能対応無線LAN端末に自動設定できます。

※自動設定の方法は、本製品の後面部(P.1-5)にある〈WPS〉ボタンを使用する「プッシュボタン(Push Button Configuration)方式」と自動設定する相手のPINコードを使用する「PIN(Personal Identification Number)方式」を選択できます。

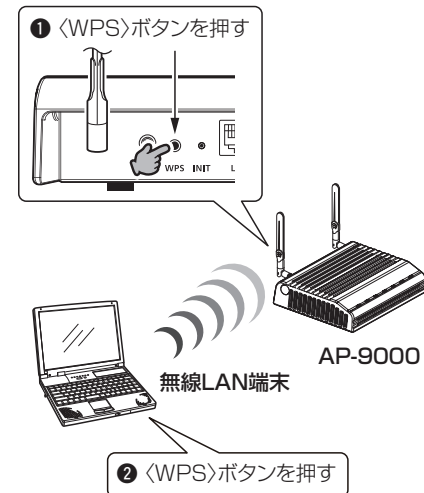
WPS機能で無線LAN端末に自動設定したいSSIDと共有鍵(キー)を指定する場合の操作例については、本書2章(P.2-12)をご覧ください。

WPS機能による自動設定の例については、本書3章(P.3-9)をご覧ください。

【WPS機能を使用しない場合】



【WPS機能を使用する場合】



WPS機能を使用するには

◎WPS機能対応の無線LAN端末を準備してください。

◎無線LAN端末が〈WPS〉ボタンを装備していない場合は、WPS対応アプリケーション、またはWindows標準のワイヤレスネットワーク接続(Windows 7以降)を使用してください。

◎本製品のWPS機能で自動設定する仮想AP(ath0~ath15)を、「仮想AP」画面で有効にしてから、「WPS」画面の「使用するインターフェース」欄で選択してください。(P.2-11)

「使用するインターフェース」欄で無効な仮想APや「なし」(出荷時の設定)を設定している場合、本製品の後面部にある〈WPS〉ボタンを使用できません。(P.1-5)

また、本製品の設定画面にも〈開始〉ボタンが表示されません。

1 ご使用になる前に

2. 本製品のおもな機能(つづき)

■ ルーター機能について

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

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

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

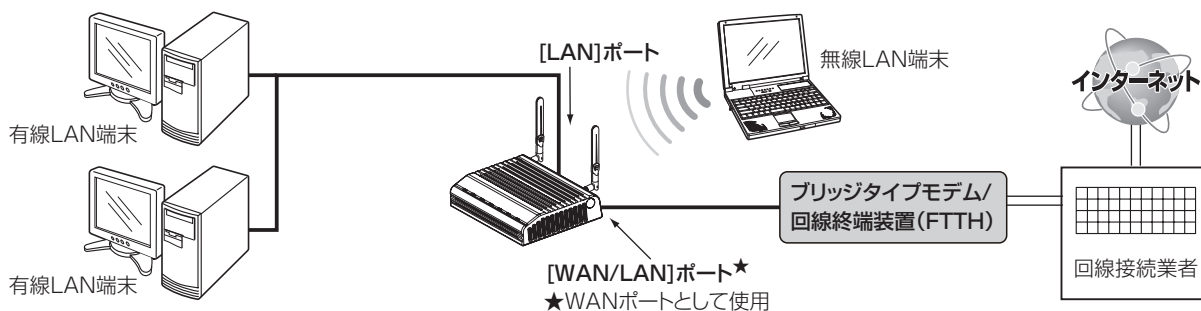
※ルーター機能を使用するときは、「ルーター設定」メニュー→「WAN接続先」画面→「回線種別設定」項目→「回線種別」欄で、「DHCPクライアント」、「PPPoE」、「固定IP」に変更してください。(P.5-29)

※回線種別が不明な場合は、ご契約の回線接続業者との契約内容をご確認ください。

ブリッジタイプモデムとの接続

下図を参考に、本製品の[WAN/LAN]ポートとブリッジタイプモデムを接続します。

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

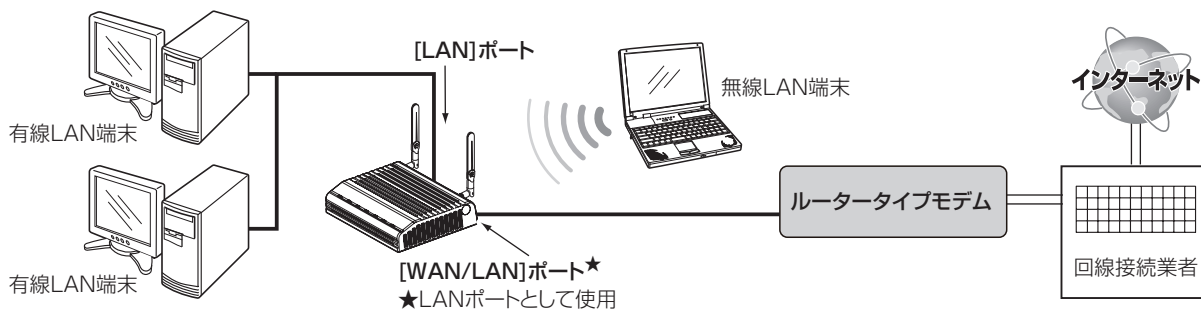


ルータータイプモデムとの接続

下図を参考に、本製品の[WAN/LAN]ポートとルータータイプモデムを接続します。

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

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



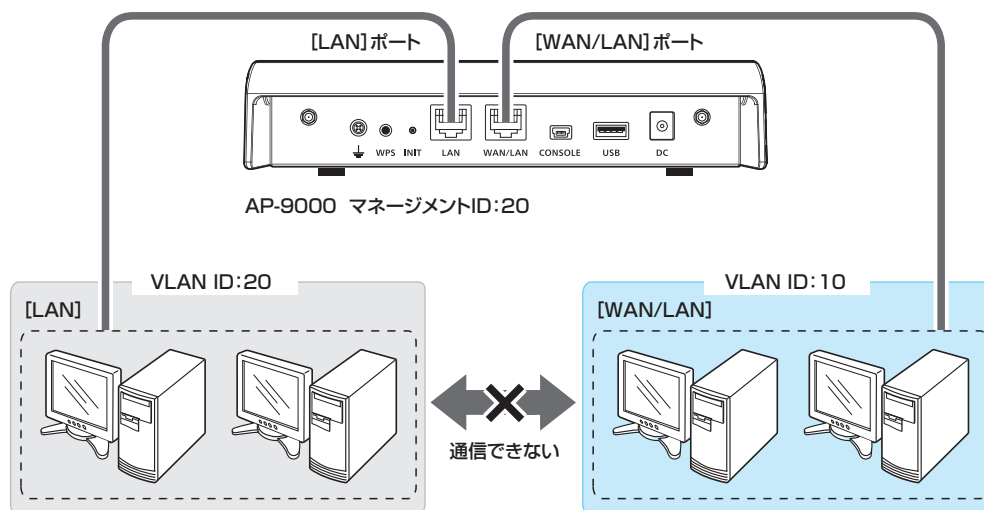
1 ご使用になる前に

2. 本製品のおもな機能(つづき)

■ ポートベースVLAN機能について

本製品の[WAN/LAN]ポート、[LAN]ポートを論理的に2つのVLANグループに分割して、異なるVLANグループ間の通信を遮断することで、セキュリティの向上やネットワークの負荷を軽減できます。

※本製品の回線種別を「LANポートとして使用する」(出荷時の設定)に設定しているときだけ使用できる機能です。



上図は、本製品のポートごとに設定されたVLAN IDによって、本製品と接続された有線LAN端末を「VLAN ID：10」と「VLAN ID：20」のグループに分割した例です。

この場合、本製品の管理IDと同じID(例：20)が設定された[LAN]ポートに接続するパソコンだけが本製品の設定画面にアクセスできます。

※設定例については、本書5-38ページ～5-39ページをご覧ください。

無線LAN端末を有線LAN端末と同じグループに設定する場合

「無線設定」メニュー→「仮想AP」画面→「仮想AP設定」項目→「VLAN ID」欄で有線LAN端末のグループと同じVLAN IDに設定してください。

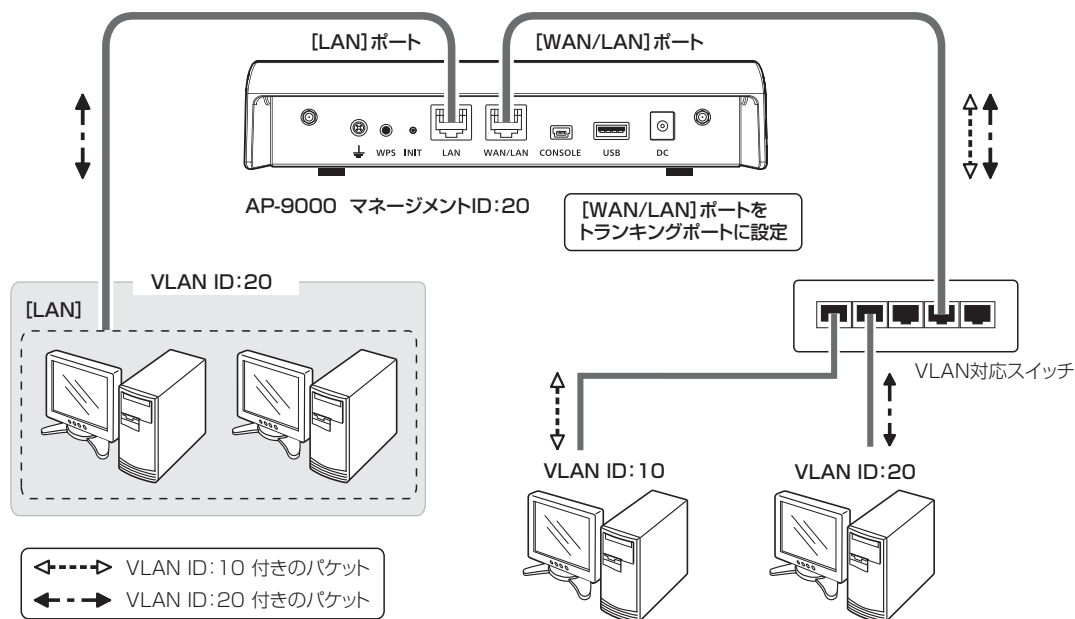
1 ご使用になる前に

2. 本製品のおもな機能

■ ポートベースVLAN機能について(つづき)

トランキングポートについて

VLANグループを構成する場合、HUB間で複数のポートが必要ですが、本製品の[WAN/LAN]ポートをトランキングポートに設定することで、タグVLANとして動作しますので、1つのポートで構成できます。



上図は、[LAN]ポートを「VLAN ID：20」のグループにして、[WAN/LAN]ポートをトランキングポートに設定した場合の例です。

※設定例については、本書5-40ページ～5-41ページをご覧ください。

1 ご使用になる前に

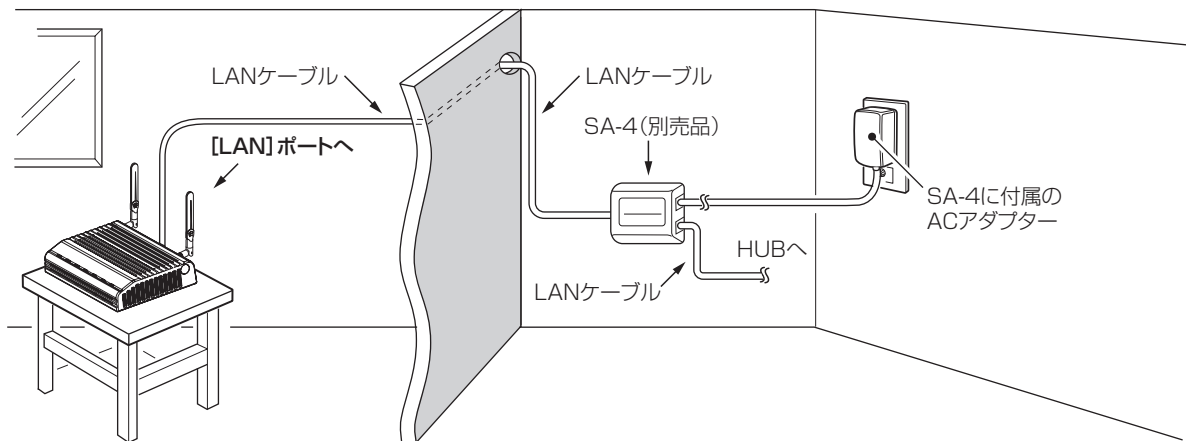
2. 本製品のおもな機能(つづき)

■ PoE機能について

本製品の設置場所付近にコンセントやIEEE802.3af規格対応のHUBがない場合に備えて、別売品のイーサネット電源供給ユニット(SA-4)をご用意しています。

SA-4をお使いいただくことで、本製品の[LAN]ポート、または[WAN/LAN]ポートから電源を受電できます。

※本製品との接続方法について詳しくは、「7. PoEによる電源供給について」(P.8-24)をご覧ください。



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. 設定に使うパソコンについて	2-2
■ 有線LAN端末と接続して設定する場合	2-2
■ 無線LAN端末と接続して設定する場合	2-2
2. 設定用のパソコンに固定IPアドレスを設定する	2-3
3. 設定に使うパソコンを接続する	2-4
■ 有線LAN端末を使用する場合	2-4
■ 無線LAN端末を使用する場合	2-5
4. 設定画面にアクセスするには	2-7
5. 本体IPアドレスを変更するときは	2-8
6. 無線ネットワーク名と暗号化を手動で設定する	2-9
■ 無線ネットワーク名を手動で設定する	2-9
■ 暗号化を手動で設定する	2-10
7. WPS機能で自動設定したいSSIDと共有鍵(キー)を指定する	2-11
■ WPS機能を有効にする	2-11
■ WPS機能で無線LAN端末を自動設定する	2-12

2 導入ガイド

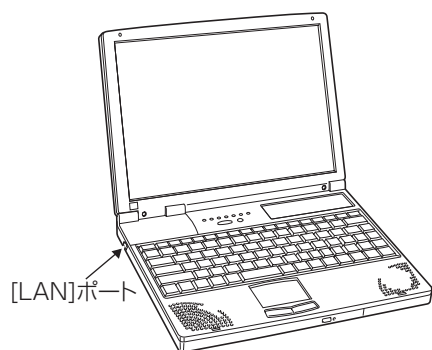
1. 設定に使うパソコンについて

出荷時、本製品のIPアドレスは「192.168.0.1」、DHCPサーバー機能は「無効」に設定されています。
本製品の設定画面にアクセスするときは、接続するパソコンに固定IPアドレスの設定が必要です。(P.2-3)

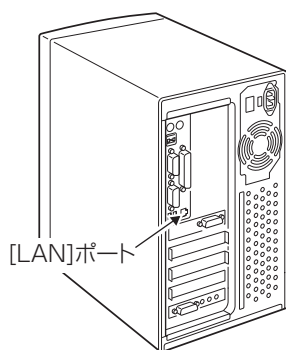
■ 有線LAN端末と接続して設定する場合

本製品の設定には、LANケーブルを接続できるパソコンをご用意ください。

ノートブック型パソコン



デスクトップ型パソコン



※[LAN]ポートの位置は、ご使用のパソコンによって異なりますので、LANケーブルを接続するときは、パソコンの取扱説明書などでご確認ください。

※すでに有線LANでご使用のパソコンを本製品の設定に使用する場合は、そのパソコンを既存の有線LANから切りはなしてください。

■ 無線LAN端末と接続して設定する場合

無線LAN機能搭載のパソコンをご用意ください。

本製品は、IEEE802.11ac/n/a (W52/W53/W56)/g/b規格に準拠しています。

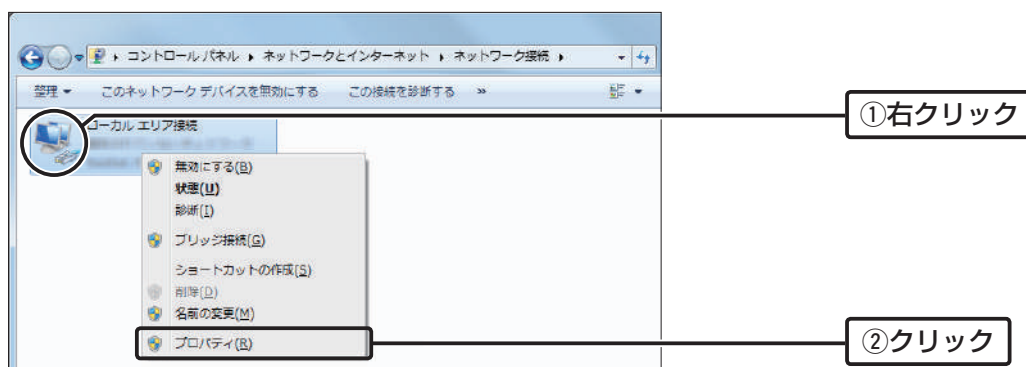
2 導入ガイド

2. 設定用のパソコンに固定IPアドレスを設定する

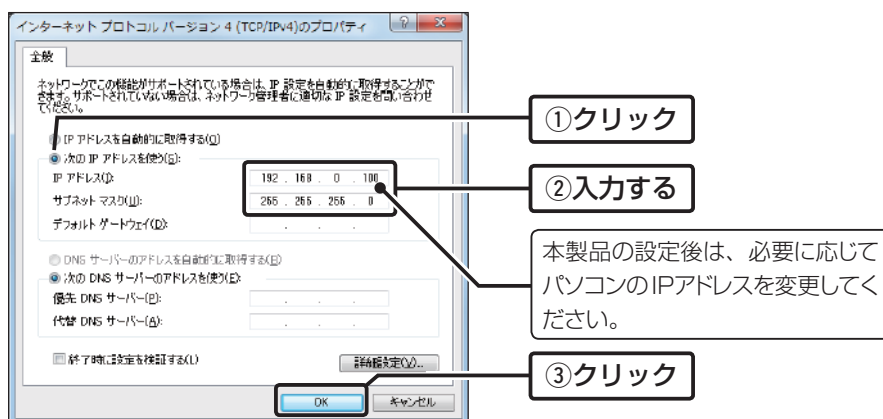
本製品の設定に使用するパソコンに固定IPアドレス(例：192.168.0.100)を設定する手順について、Windows 7を例に説明します。

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。

- 1 マウスを<スタート>(ロゴボタン)→[コントロールパネル]の順に操作します。
- 2 コントロールパネルで、[ネットワークとインターネット]をクリックし、表示された画面で[ネットワークと共有センター]をクリックします。
- 3 タスク欄の[アダプターの設定の変更]をクリックします。
- 4 [ローカルエリア接続](有線LAN端末で設定する場合)、または[ワイヤレスネットワーク接続](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。



- 5 [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。
- 6 「ローカル エリア接続のプロパティ」画面(有線LAN端末で設定する場合)、または「ワイヤレスネットワーク接続のプロパティ」画面(無線LAN端末で設定する場合)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。
- 7 [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。



※上図は、設定例です。

- 8 <閉じる>をクリックします。

2 導入ガイド

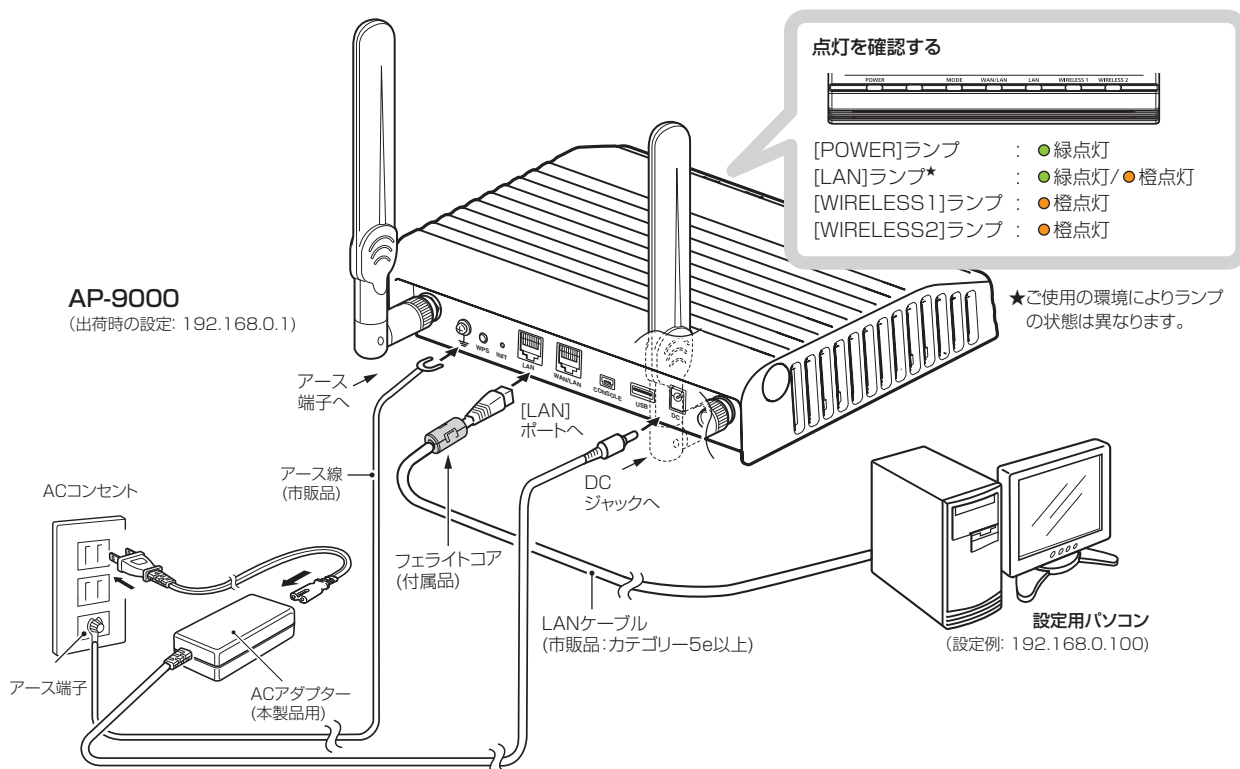
3. 設定に使うパソコンを接続する

出荷時の状態で接続するときは、本製品に接続するパソコンを既存のネットワークから切りはなしてください。

■ 有線LAN端末を使用する場合

本製品とパソコン(有線LAN端末)の電源を入れます。

※接続するときは、本製品、および接続する機器の電源を切ってください。



△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。
- ◎本製品に取り付けた外部アンテナを持って本製品を振り回さないでください。
本人や他人に当たるなどして、けがや破損、および故障の原因になります。

(次ページにつづく)

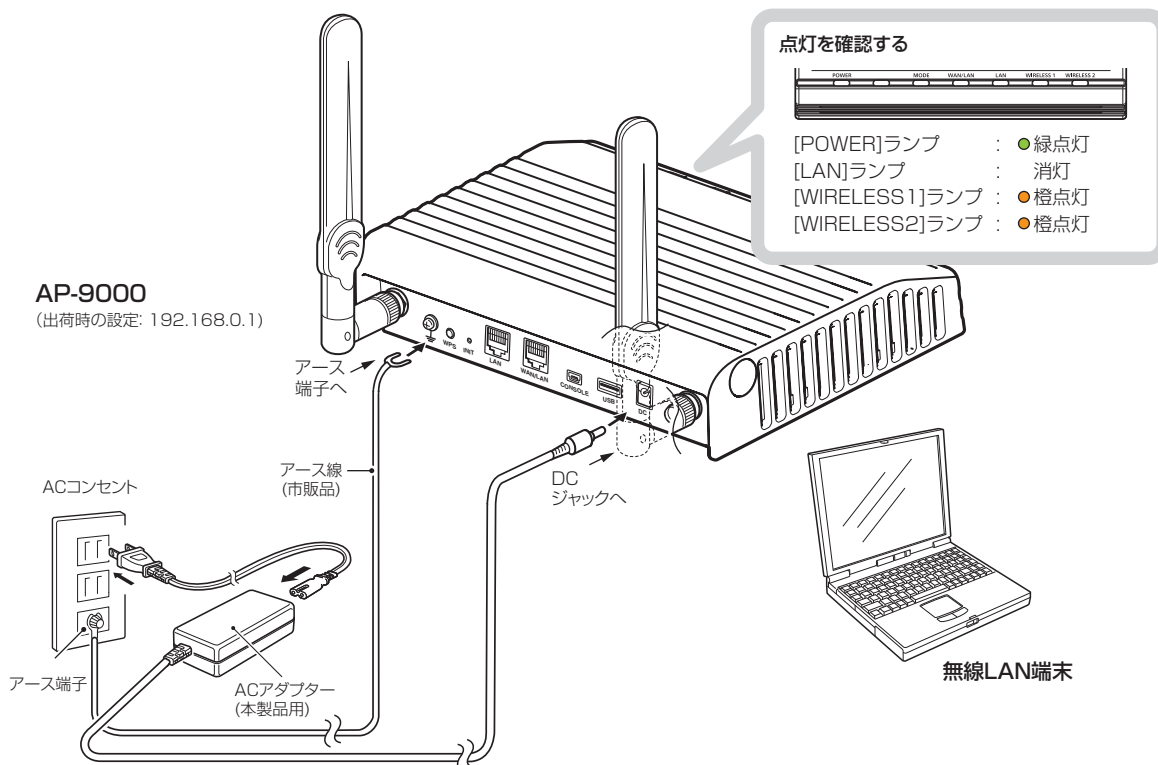
2 導入ガイド

3. 設定に使うパソコンを接続する(つづき)

■ 無線LAN端末を使用する場合

※接続するときは、本製品、および接続する機器の電源を切ってください。

- 1 本製品の電源を入れ、無線LANに対応するパソコン(無線LAN端末)の電源を入れます。

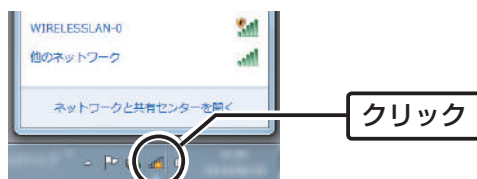


△ 警告

- ◎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。
- ◎本製品に取り付けた外部アンテナを持って本製品を振り回さないでください。本人や他人に当たるなどして、けがや破損、および故障の原因になります。

- 2 [ワイヤレスネットワーク接続アイコン]をクリックします。

※アイコンが表示されるまで数分かかることがあります。



(次ページにつづく)

2 導入ガイド

3. 設定に使うパソコンを接続する

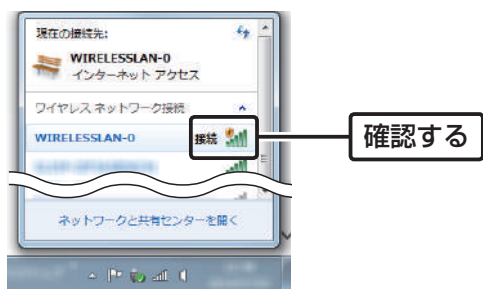
■ 無線LAN端末を使用する場合(つづき)

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

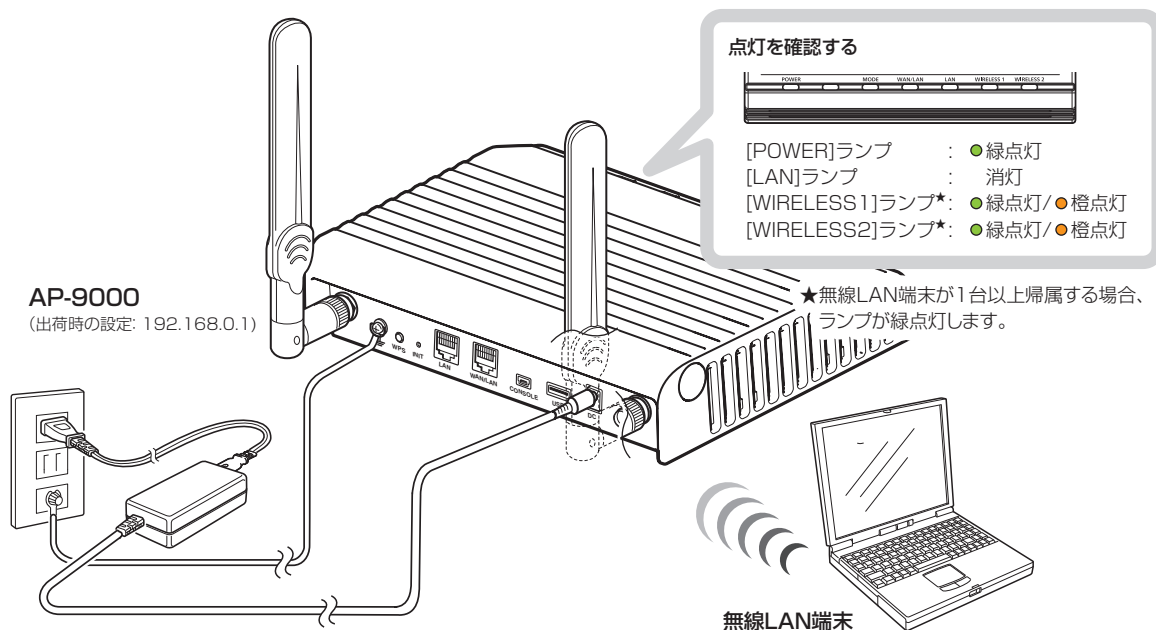


- ※ 本製品に暗号鍵(キー)を設定した場合は、「ネットワークに接続」画面が表示されますので、画面にしたがって暗号鍵(キー)を入力してください。
※ 不正アクセス防止のため、必ず暗号化を設定してください。暗号鍵(WEPキー)/共有鍵(Pre-Shared Key)は、容易に推測されないものにしてください。
数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた複雑なものにし、さらに定期的に暗号鍵/共有鍵を変更されることをおすすめします。

- 4 「接続」と表示されたことを確認します。



- 5 本製品の[WIRELESS] (1/2)ランプが●緑点灯したことを確認します。

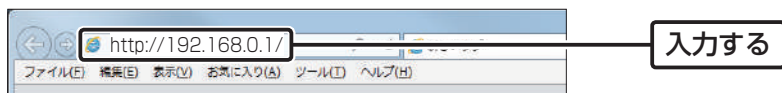


2 導入ガイド

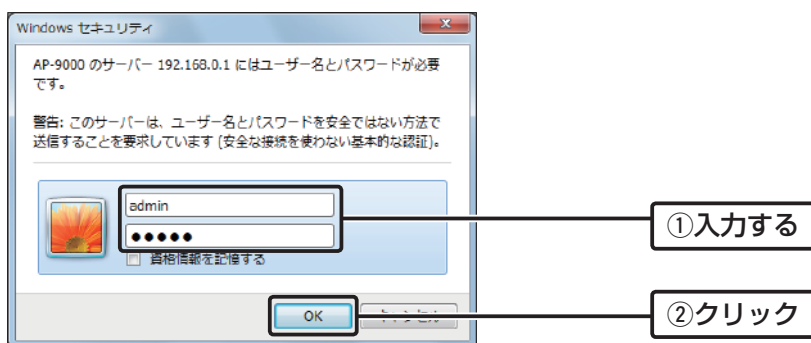
4. 設定画面にアクセスするには

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

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



- 3 [Enter]キーを押します。
[ユーザー名]と[パスワード]を求め画面が表示されます。
- 4 [ユーザー名]欄に「admin」、[パスワード]欄に「admin」(出荷時の設定)を入力し、〈OK〉をクリックすると、設定画面が表示されます。



WWWブラウザについて

Microsoft® Internet Explorer® 11で動作確認しています。
設定画面が正しく表示できるように、WWWブラウザのJavaScript®機能、およびCookieは有効にしてください。
※Microsoft® Internet Explorer® 8以前をご使用の場合は、正しく表示できないことがあります。

2 導入ガイド

5. 本体IPアドレスを変更するときは

ネットワーク設定 > LAN側IP > IPアドレス設定

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、「LAN側IP」の順にクリックします。

2 「LAN側IP」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-9000

VLAN設定
管理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

①入力する

②クリック

※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 「再起動」をクリックします。

再起動 再起動が必要な項目が変更されています。

本体名称

クリック

※表示される画面にしたがって、本製品を再起動します。

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

「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.2-7)

※IPアドレスの「ネットワーク部(例: 192.168.0)」を変更したときは、設定に使用するパソコンの「ネットワーク部」についても本製品と同じに変更します。

IPアドレスの割り当てかた

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

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

「ネットワーク部」が同じIPアドレスを持つネットワーク機器(パソコンなど)は、同じネットワーク上にあると認識されます。

さらに「ホスト部」によって同じネットワーク上にある各ネットワーク機器を識別しています。

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

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

2 導入ガイド

6. 無線ネットワーク名と暗号化を手動で設定する

無線設定 > 無線1/無線2 > 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1(2.4GHz帯)の「ath0」で通信する場合を例に説明しています。 (出荷時の設定：WIRELESSLAN-0)

※本製品の無線ネットワーク名(SSID)と暗号化を自動で設定する場合は、本書3-9ページをご覧ください。

1 「無線設定」メニューの「無線1」、「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

アカウントिंग: 無効 有効

MAC認証: 無効 有効

暗号化設定

ネットワーク認証: オープンシステム/共有キー

暗号化方式: なし

登録 取消

入力する

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)
※WPS機能と併用できませんので、ご注意ください。

3 <登録>をクリックします。
「再起動が必要な項目が変更されています。」が表示されます。

(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

6. 無線ネットワーク名と暗号化を手動で設定する(つづき)

無線設定 > 無線1/無線2 > 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1(2.4GHz帯)の「ath0」で通信する場合を例に説明しています。

ネットワーク認証 : WPA-PSK/WPA2-PSK

暗号化方式 : TKIP/AES

PSK (Pre-Shared Key) : wirelessmaster

※設定例以外の暗号化設定については、本書3-4ページ～3-8ページをご覧ください。

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

※[PSK (Pre-Shared Key)]欄に入力した文字数によって、入力モード(ASCII:半角で8文字～63文字入力/
16進数:64桁入力)を自動判別します。

仮想AP設定

インターフェース: ath0

仮想AP: 無効 有効

SSID: ICOM

VLAN ID: 0

ANY接続拒否: 無効 有効

接続端末制限: 63

アカウントing: 無効 有効

MAC認証: 無効 有効

暗号化設定

ネットワーク認証: WPA-PSK/WPA2-PSK

暗号化方式: TKIP/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

- 2 <登録>をクリックします。

- 3 <再起動>をクリックします。

再起動 再起動が必要な項目が変更されています。

仮想AP設定

クリック

※表示される画面にしたがって、本製品を再起動します。

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

7. WPS機能で自動設定したいSSIDと共有鍵(キー)を指定する

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

※ネットワーク名(SSID)と暗号化の設定については、本書2-9ページをご覧ください。

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

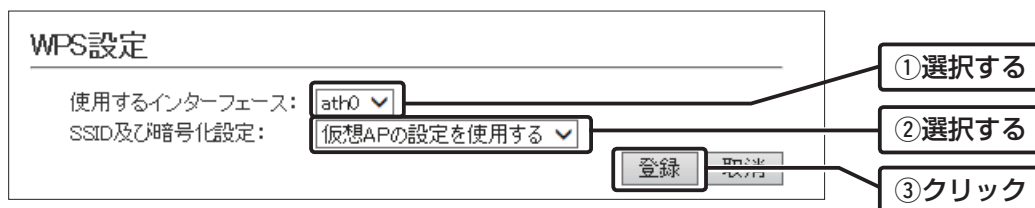
無線設定 > WPS

■ WPS機能を有効にする

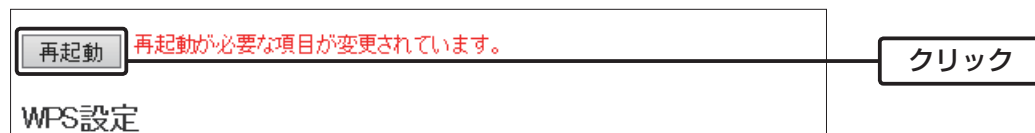
「プッシュボタン方式」を例に説明します。(P.1-15)

※WPS機能を有効にすると、本製品の後面部にある〈WPS〉ボタンの操作が有効になります。

- 1 「無線設定」メニュー、「WPS」の順にクリックします。
- 2 WPS機能を使用する仮想AP(例：ath0)を選択し、〈登録〉をクリックします。(出荷時の設定：なし)



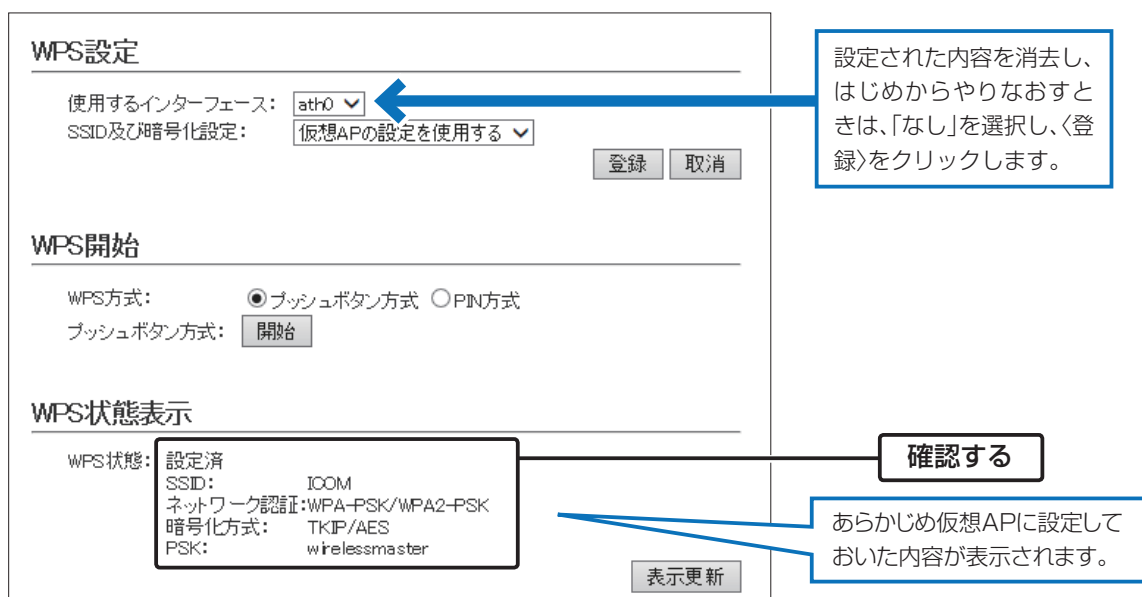
- 3 〈再起動〉をクリックします。



※表示される画面にしたがって、本製品を再起動します。

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

- 5 「WPS」画面の[WPS状態]欄を確認します。



(次ページにつづく)

2 導入ガイド

7. WPS機能で自動設定したいSSIDと共有鍵(キー)を指定する(つづき)

〈WPS〉ボタンを使用した自動設定の操作手順について説明します。
本製品のSSIDと共有鍵(キー)の内容を無線LAN端末に自動設定します。

無線設定 > WPS

■ WPS機能で無線LAN端末を自動設定する

無線LAN端末は、WPS対応のものをご用意ください。

本書では、Windows 7標準のワイヤレスネットワーク接続を例に、WPS機能で無線LAN端末を自動設定する手順を説明します。

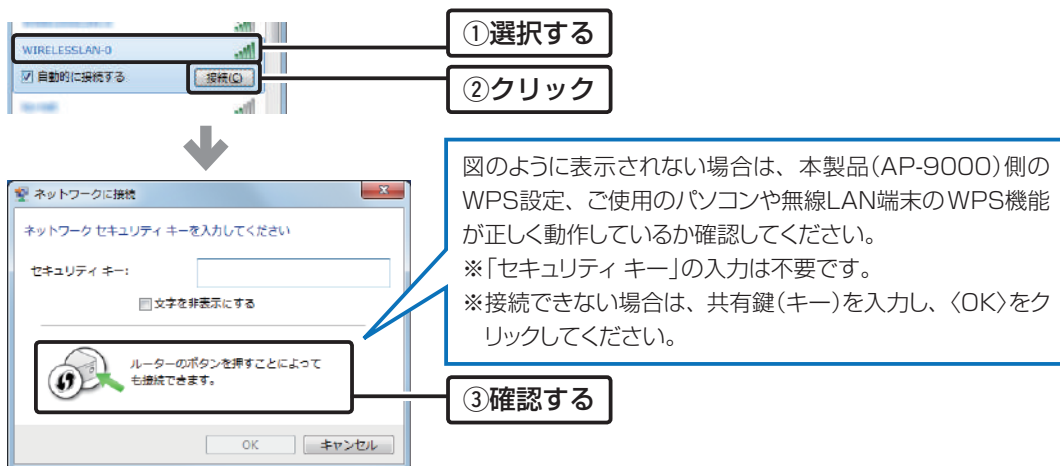
※ 無線LAN端末側の操作について詳しくは、お使いになる端末の取扱説明書をご覧ください。

※ [MODE]ランプが ● 赤点滅し、設定できない場合は、[使用するインターフェース]欄を「なし」(P.2-11)に戻してから、手動で設定してください。(P.2-9)

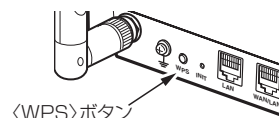
- 1 無線LAN端末側で、[ワイヤレスネットワーク接続アイコン]をクリックします。
※アイコンが表示されるまで数分かかることがあります。



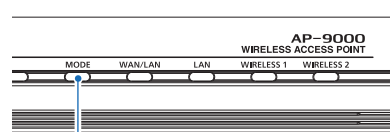
- 2 本製品に設定されたSSID (例：WIRELESSLAN-0)を選択し、〈接続(C)〉をクリックします。
「ネットワークに接続」画面が表示されます。



- 3 本製品の〈WPS〉ボタンを押します。
[MODE]ランプがゆっくり ● 緑点滅します。



- 4 [MODE]ランプが ● 緑点灯になると、設定完了です。



- 緑点灯 : WPS成功時
- 緑点滅 : WPS実行時
- 赤点滅 : WPS失敗時(約20秒後消灯)

この章では、

本製品の無線LANを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. 無線通信を停止するには	3-2
■ 無線UNITを無効にする	3-2
2. IEEE802.11ac規格(5GHz帯)の通信をするには	3-3
■ 80MHz帯域幅通信をするときは	3-3
3. [WEP RC4]暗号化を設定するには	3-4
■ 暗号鍵(キー)の入力について	3-4
■ ASCII文字→16進数変換表	3-4
■ 16進数で暗号鍵(キー)を入力するには	3-5
■ ASCII文字で暗号鍵(キー)を入力するには	3-6
■ 暗号鍵(キー)を生成するには	3-7
■ 暗号鍵(キー)値の設定例	3-8
4. 無線ネットワーク名と暗号化を自動で設定するときは	3-9
■ WPS機能を有効にする	3-9
■ 〈WPS〉ボタンで自動設定を開始する	3-10
5. 仮想APを設定するには	3-12
6. 無線AP(アクセスポイント)間通信機能を設定するには	3-14
■ 無線1(2.4GHz帯)で使用する場合(WDS)	3-15
■ 無線2(5GHz帯)で使用する場合(WBR)	3-17
■ 親機を設定する	3-18
■ 子機を設定する	3-20
■ 無線AP間通信で使用する本製品をRS-AP3で管理するときは	3-21
7. MACアドレスフィルタリングを設定するには	3-22

3 無線LAN接続[基本編]

1. 無線通信を停止するには

出荷時や全設定初期化時、本製品の無線LANユニットは無線1(2.4GHz帯)、無線2(5GHz帯)ともに、「有効」に設定されています。

無線設定 > 無線1/無線2 > 無線LAN

■ 無線UNITを無効にする

無線2(5GHz帯)を例に無線通信を停止する手順を説明します。

1 「無線設定」メニューの「無線2」、「無線LAN」の順にクリックします。

2 「無線UNIT」欄で「無効」を選択します。 (出荷時の設定：有効)

無線LAN設定

無線UNIT: 無効 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

プロテクション: 無効 有効

登録 取消

選択する

3 「登録」をクリックします。

4 「再起動」をクリックします。

再起動 再起動が必要な項目が変更されています。

無線LAN設定

クリック

※表示される画面にしたがって、本製品を再起動します。

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

3 無線LAN接続[基本編]

2. IEEE802.11ac規格(5GHz帯)の通信をするには

IEEE802.11ac規格を使用できるのは、無線2(5GHz帯)で暗号化設定を「なし」、または「AES」を設定したときだけです。

※暗号化設定が「WEP RC4」、または「TKIP」の場合は、使用する無線LANユニット(2.4GHz/5GHz帯)に応じてIEEE802.11a/b/g規格で通信します。

無線設定 > 無線2 > 無線LAN

■ 80MHz帯域幅通信をするときは

次の手順で帯域幅を変更してください。

1 「無線設定」メニューの「無線2」、「無線LAN」の順にクリックします。

2 [帯域幅]欄で「80MHz」を選択します。

(出荷時の設定：20MHz)

無線LAN設定

無線UNIT: 無効 有効

帯域幅: 80 MHz

チャンネル: 036 CH (5180 MHz)

パワーレベル: 高

DTIM間隔: 1

プロテクション: 無効 有効

登録 取消

選択する

3 <登録>をクリックします。

4 <再起動>をクリックします。

再起動 再起動が必要な項目が変更されています。

無線LAN設定

クリック

※表示される画面にしたがって、本製品を再起動します。

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

40/80MHz帯域幅通信をするときの手引き

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

◎万一、本製品から、ほかの無線局に対して有害な電波干渉の事例が発生した場合には、[帯域幅]欄を「20MHz」(出荷時の設定)でご使用ください。

3. [WEP RC4]暗号化を設定するには

[WEP RC4]暗号化設定は、次の3とおりです。

- ◎16進数で暗号鍵(キー)を直接入力する(P.3-5)
- ◎ASCII文字で暗号鍵(キー)を直接入力する(P.3-6)
- ◎[キージェネレーター]に入力した文字列から暗号鍵(キー)を生成する(P.3-7)

※出荷時や全設定初期化時、暗号化は設定されていません。

※[WEP RC4]暗号化を設定できないときは、使用する仮想AP(ath0~ath15)にWPS機能が設定されていないことを確認してください。(P.2-11)

※[WPA-PSK(TKIP)/(AES)]暗号化設定例については、本書2-10ページをご覧ください。

■ 暗号鍵(キー)の入力について

[暗号化方式]の設定によって、入力する暗号鍵(キー)の文字数や桁数が異なります。

また、入力された文字数、および桁数によって、入力モード(16進数/ASCII文字)を自動判別します。

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

※入力できる桁数、および文字数は、()内のビット数に対する値です。

■ ASCII文字→16進数変換表

相手が指定する[入力モード]で暗号鍵(キー)を設定できない場合は、下記の変換表を参考に指示された暗号鍵(キー)に対応する記号や英数字で入力してください。

たとえば、16進数入力で「4153434949」(10桁)を設定している場合、ASCII文字では、「ASCII」(5文字)になります。

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

不正アクセス防止のアドバイス

本製品に設定する暗号鍵(WEPキー)は、容易に推測されないものにしてください。

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

3 無線LAN接続[基本編]

3. [WEP RC4]暗号化を設定するには(つづき)

無線設定 > 無線1/無線2 > 仮想AP

■ 16進数で暗号鍵(キー)を入力するには

無線1(2.4GHz帯)の「ath0」を設定する場合を例に説明します。

ネットワーク認証 : 「オープンシステム/共有キー」(出荷時の設定)

暗号化方式 : 「WEP RC4 128(104)」ビット

WEPキー : 「0~9」、および「a~f(またはA~F)」を使用して26桁を入力

- 1 「無線設定」メニューの「無線1」、「仮想AP」の順にクリックします。
- 2 [暗号化方式]欄で「WEP RC4 128(104)」を選択し、26桁の暗号鍵(キー)を[WEPキー]欄に入力します。

仮想AP設定

インターフェース: ath0 ▼
仮想AP: 無効 有効
SSID: WIRELESSLAN-0
VLAN ID: 0
ANY接続拒否: 無効 有効
接続端末制限: 63
アカウントिंग: 無効 有効
MAC認証: 無効 有効

暗号化設定

ネットワーク認証: オープンシステム/共有キー ▼
暗号化方式: WEP RC4 128 (104) ▼
キージェネレーター:
WEPキー:
半角英数で13文字、もしくは16進数で26桁を入力

登録 取消

出荷時の設定であることを確認します。

① 選択する

② 入力する

- 3 <登録>をクリックします。

- 4 <再起動>をクリックします。

再起動 再起動が必要な項目が変更されています。

仮想AP設定

クリック

※表示される画面にしたがって、本製品を再起動します。

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

3 無線LAN接続[基本編]

3. [WEP RC4]暗号化を設定するには(つづき)

無線設定 > 無線1/無線2 > 仮想AP

■ ASCII文字で暗号鍵(キー)を入力するには

無線1(2.4GHz帯)の「ath0」を設定する場合を例に説明します。

ネットワーク認証 : 「オープンシステム/共有キー」(出荷時の設定)

暗号化方式 : 「WEP RC4 128(104)」ビット

WEPキー : 13文字を入力(例: RETSAMEVAWNAL)

- 1 「無線設定」メニューの「無線1」、「仮想AP」の順にクリックします。
- 2 [暗号化方式]欄で「WEP RC4 128(104)」を選択し、13文字の暗号鍵(キー)を[WEPキー]欄に入力します。

仮想AP設定

インターフェース: ath0 ▼
仮想AP: 無効 有効
SSID: WIRELESSLAN-0
VLAN ID: 0
ANY接続拒否: 無効 有効
接続端末制限: 63
アカウントिंग: 無効 有効
MAC認証: 無効 有効

出荷時の設定であることを確認します。

暗号化設定

ネットワーク認証: オープンシステム/共有キー ▼
暗号化方式: WEP RC4 128 (104) ▼
キージェネレーター:
WEPキー: RETSAMEVAWNAL
半角英数字13文字、もしくは16進数で26桁を入力

登録 取消

① 選択する
② 入力する

- 3 <登録>をクリックします。
- 4 <再起動>をクリックします。

再起動 再起動が必要な項目が変更されています。

仮想AP設定

クリック

※表示される画面にしたがって、本製品を再起動します。

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

3 無線LAN接続[基本編]

3. [WEP RC4]暗号化を設定するには(つづき)

無線設定 > 無線1/無線2 > 仮想AP

■ 暗号鍵(キー)を生成するには

無線1(2.4GHz帯)の「ath0」を設定する場合を例に説明します。

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

- 1 「無線設定」メニューの「無線1」、「仮想AP」の順にクリックします。
- 2 [暗号化方式]欄で「WEP RC4 128(104)」を選択し、任意の文字列を[キージェネレーター]欄に入力します。(例: ICOM)

仮想AP設定

インターフェース: ath0

仮想AP: 無効 有効

SSID: WIRELESSLAN-0

VLAN ID: 0

ANY接続拒否: 無効 有効

接続端末制限: 63

アカウントing: 無効 有効

MAC認証: 無効 有効

暗号化設定

ネットワーク認証: オープンシステム/共有キー

暗号化方式: WEP RC4 128 (104)

キージェネレーター: ICOM

WEPキー: 半角英数で13文字、もしくは16進数で26桁を入力

薄い文字で生成内容が表示されます。

登録 取消

出荷時の設定であることを確認します。

① 選択する

② 入力する

- 3 <登録>をクリックします。
- 4 <再起動>をクリックします。

再起動 再起動が必要な項目が変更されています。

仮想AP設定

クリック

※表示される画面にしたがって、本製品を再起動します。

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

キージェネレーターについて

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

3 無線LAN接続[基本編]

3. [WEP RC4]暗号化を設定するには(つづき)

無線設定 > 無線1/無線2 > 仮想AP

■ 暗号鍵(キー)値の設定例

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

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

AP-9000側	弊社製無線LAN端末側
暗号化設定 ネットワーク認証: <input type="text" value="オープンシステム/共有キー"/> 暗号化方式: <input type="text" value="WEP RC4 128 (104)"/> キージェネレーター: <input type="text"/> WEPキー: <input type="text" value="486F7473706F744C6363657373"/> <small>半角英数で13文字、もしくは16進数で26桁を入力</small>	キーインデックス: <input type="text" value="1"/> WEPキー: <input checked="" type="radio"/> 16進数入力 <input type="radio"/> ASCII文字入力 キー1: <input type="text" value="48-6F-74-73-70-6F-74-4C-63-63-65-73-73"/>

キーインデックス「1」のWEPキー(値)が本製品と同じため通信できます。

※キー1の暗号鍵(キー)がデータの送信と受信に使用されます。

キーインデックスについて

本製品には、キーインデックスの設定はありませんが、「1」に相当します。

※無線LAN端末側で、[キーインデックス]の設定を「1」以外で使用している場合は、[キーインデックス]を「1」に変更して、そのテキストボックスに本製品と同じ暗号鍵(キー)を設定してください。

不正アクセス防止のアドバイス

本製品に設定する暗号鍵(WEPキー)は、容易に推測されないものにしてください。

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

3 無線LAN接続[基本編]

4. 無線ネットワーク名と暗号化を自動で設定するときは

WPS(Wi-Fi Protected Setup)機能により、自動生成されるネットワーク名(SSID)と共有鍵(キー)を本製品と無線LAN端末(WPS対応)に自動設定します。

※WPS機能を使用せず、本製品に手動でネットワーク名(SSID)と暗号化を設定する場合は、本書2-9ページをご覧ください。

無線設定 > WPS

■ WPS機能を有効にする

「プッシュボタン方式」を例に説明します。(P.1-15)

※WPS機能を有効にすると、本製品の後面部にある〈WPS〉ボタンの操作が有効になります。

なお、「仮想AP」画面(例：ath0)のSSIDと暗号化設定は変更できなくなります。

1 「無線設定」メニュー、「WPS」の順にクリックします。

2 WPS機能を使用する仮想AP(例：ath0)を選択します。 (出荷時の設定：なし)

WPS設定

使用するインターフェース: ath0 ▼

SSID及び暗号化設定: 仮想APの設定を使用する ▼

登録 取消

選択する

3 [SSID及び暗号化設定]欄で「WPSで設定を生成する」を選択して、「登録」をクリックします。

「再起動が必要な項目が変更されています。」が表示されます。

※本製品に手動で設定したネットワーク名(SSID)と共有鍵(キー)を使用するときは、「仮想APの設定を使用する」(出荷時の設定)を選択してください。

WPS設定

使用するインターフェース: ath0 ▼

SSID及び暗号化設定: WPSで設定を生成する ▼

WPAキー更新間隔: 120 分

登録 取消

① 選択する

② クリック

4 〈再起動〉をクリックします。

再起動 再起動が必要な項目が変更されています。

WPS設定

クリック

※表示される画面にしたがって、本製品を再起動します。

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

3 無線LAN接続[基本編]

4. 無線ネットワーク名と暗号化を自動で設定するときは(つづき)

〈WPS〉ボタンを使用した自動設定の操作手順について説明します。

本製品が自動生成するSSIDと暗号化(WPA-PSK/WPA2-PSK)の内容を無線LAN端末に自動設定します。

無線設定 > WPS

■ 〈WPS〉ボタンで自動設定を開始する

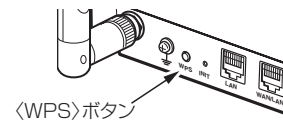
本書では、SE-90Mの操作を例に無線LAN端末側の操作を説明します。

※ 無線LAN端末が〈WPS〉ボタンを装備していない場合は、WPS対応のアプリケーションをご用意ください。

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

※ 設定できない場合は、[使用するインターフェース]欄を「なし」(P.3-9)に戻してから、手動で設定してください。
(P.2-9)

1 本製品の〈WPS〉ボタンを押します。

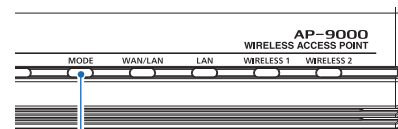


2 本製品の[MODE]ランプがゆっくり緑点滅していることを確認します。

※ 無線LAN端末側の操作は、本製品の操作から120秒以内に開始してください。

本製品の場合、120秒以上経過すると設定に失敗します。

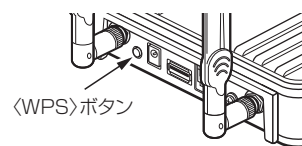
この場合、[MODE]ランプが赤点滅に切り替わり、約20秒後に消灯しますので、はじめから操作をやりなおしてください。



[MODE]ランプ

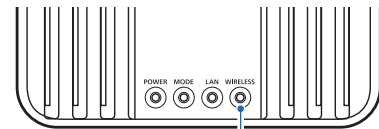
- 緑点灯 : WPS成功時
- 緑点滅 : WPS実行時
- 赤点滅 : WPS失敗時(約20秒後消灯)

3 SE-90Mの〈WPS〉ボタンを、[WIRELESS]ランプが緑点滅するまで押します。



4 SE-90Mの[WIRELESS]ランプがゆっくり緑点滅していることを確認します。

※ SE-90Mの場合、設定に失敗すると[WIRELESS]ランプが赤点滅に切り替わり、約20秒後に● 橙点灯しますので、はじめから操作をやりなおしてください。



[WIRELESS]ランプの状態表示

- 緑点灯 : 無線通信確立時 / WPS 成功時(約 5 分通知)
- 緑点滅 : WPS 実行時
- 赤点滅 : WPS 失敗時(約 20 秒通知)
- 橙点灯 : 無線機能動作時(通信中の無線アクセスポイントが存在しないとき)
- 消 灯 : 無線機能停止時

(次ページにつづく)

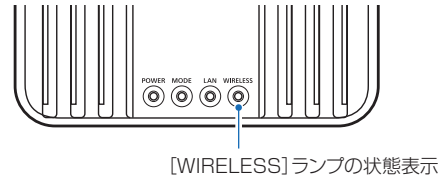
3 無線LAN接続[基本編]

4. 無線ネットワーク名と暗号化を自動で設定するときは

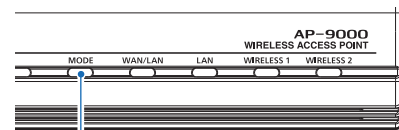
無線設定 > WPS

■ 〈WPS〉ボタンで自動設定を開始する(つづき)

- 5 SE-90Mの[WIRELESS]ランプが●緑点灯していることを確認します。



- 6 本製品の[MODE]ランプが●緑点灯していることを確認します。



- 緑点灯 : WPS成功時
- 緑点滅 : WPS実行時
- 赤点滅 : WPS失敗時(約20秒後消灯)

- 7 本製品の「WPS」画面で〈表示更新〉をクリックします。
本製品に自動設定された内容を「WPS状態表示」に表示します。

※2台目以降の無線LAN端末に自動設定するときは、別の無線LAN端末を使用して、「〈WPS〉ボタンで自動設定を開始する」の手順1(P.3-10)から操作してください。

WPS設定

使用するインターフェース: ath0
SSID及び暗号化設定: WPSで設定を生成する
WPAキー更新間隔: 120分

登録 取消

WPS開始

WPS方式: プッシュボタン方式 PIN方式
プッシュボタン方式: 開始

本製品の後面部にある〈WPS〉ボタン(P.3-10)と同じ動作をします。

WPS状態表示

WPS状態: 設定済 初期化して再起動

SSID: WIRELESSLAN-
ネットワーク認証: WPA-PSK/WPA2-PSK
暗号化方式: TKIP/AES
PSK: _____

表示更新 クリック

本製品に自動設定された内容を消去して、〈WPS〉ボタンで自動設定を開始する操作をはじめからやりなおすときクリックします。(P.3-10)

3 無線LAN接続[基本編]

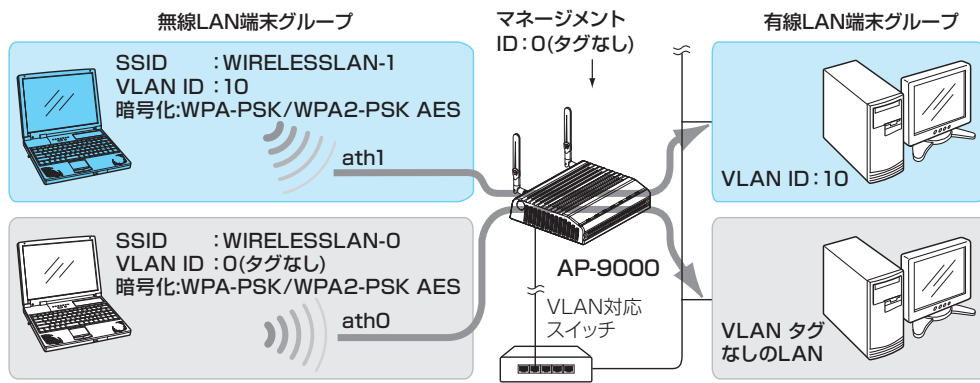
5. 仮想APを設定するには

無線設定 > 無線1/無線2 > 仮想AP

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

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



※仮想AP「ath0」は、設定されているものとします。

※使用条件については、「仮想AP機能について」をご覧ください。(P.1-13)

- 1 「無線設定」メニューの「無線1」、「仮想AP」の順にクリックします。
- 2 [インターフェース]欄で「ath1」を選択し、上記の設定例にしたがって設定します。

仮想AP設定

インターフェース: ath1

仮想AP: 無効 有効

SSID: WIRELESSLAN-1

VLAN ID: 10

ANY接続拒否: 無効 有効

接続端末制限: 63

アカウントिंग: 無効 有効

MAC認証: 無効 有効

暗号化設定

ネットワーク認証: WPA-PSK/WPA2-PSK

暗号化方式: AES

PSK (Pre-Shared Key): RETSAMEVAWNAL

WPAキー更新間隔: 120 分

登録

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

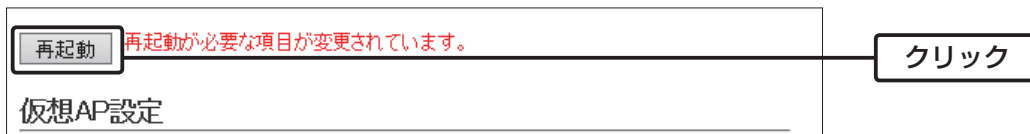
(次ページにつづく)

3 無線LAN接続[基本編]

5. 仮想APを設定するには(つづき)

無線設定 > 無線1/無線2 > 仮想AP

3 <再起動>をクリックします。



※表示される画面にしたがって、本製品を再起動します。

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

3 無線LAN接続[基本編]

6. 無線AP(アクセスポイント)間通信機能を設定するには

本製品に内蔵された無線LANユニットにより、通信できる相手側の無線アクセスポイント(弊社製)や使用方法が異なりますのでご注意ください。

無線LANユニット		AP-80	AP-80HR	AP-80M	AP-80MR	AP-800	AP-8000	AP-90M	AP-90MR	AP-900	AP-9000	SE-900 (アクセスポイントモード時)
無線1 (WDS)	2.4GHz帯	○	○	○	○	○	○	○	○	○	○	×
無線2 (WBR)	5GHz帯	×	×	×	×	×	×	○	○	○	○	○

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

※2017年1月現在、上記以外の製品では、無線AP間通信できません。

なお、SE-900は、2.4GHz/5GHzの2波同時通信には対応していません。

無線1で使用する場合(WDS)(P.3-15)

- ◎無線アクセスポイントに内蔵された無線LANユニットのBSSIDを互いに登録し合う必要があります。
- ◎チャンネル、および無線AP間通信専用の共有鍵(キー)を相手側と同じ設定にします。

無線2で使用する場合(WBR)(P.3-17)

- ◎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。
- ◎親機側の仮想AP★に設定されたSSID、暗号化を子機側に設定する必要があります。

★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。(2017年1月現在)

「ath0」：アクセスポイントモードのSE-900

「ath4」：AP-90M、AP-90MR

「ath8」：AP-900、AP-9000

RS-AP3で本製品を管理するときは(P.3-21)

無線AP間通信をする本製品をRS-AP3(弊社製アクセスポイント管理ツール)で管理するときは、本製品側の設定画面(無線1、または無線2)で無線AP間通信機能を設定して、あらかじめ通信できる状態にしておいてください。

※2017年1月現在、RS-AP3を使用して管理できる無線アクセスポイントは、AP-90M、AP-90MR、AP-900、AP-9000、アクセスポイントモードのSE-900です。

(次ページにつづく)

3 無線LAN接続[基本編]

6. 無線AP(アクセスポイント)間通信機能を設定するには(つづき)

無線設定 > 無線1 > AP間通信 (WDS)

■ 無線1 (2.4GHz帯)で使用する場合(WDS)

次の条件で、2台の本製品(図：AとB)を設定する場合を例に説明します。

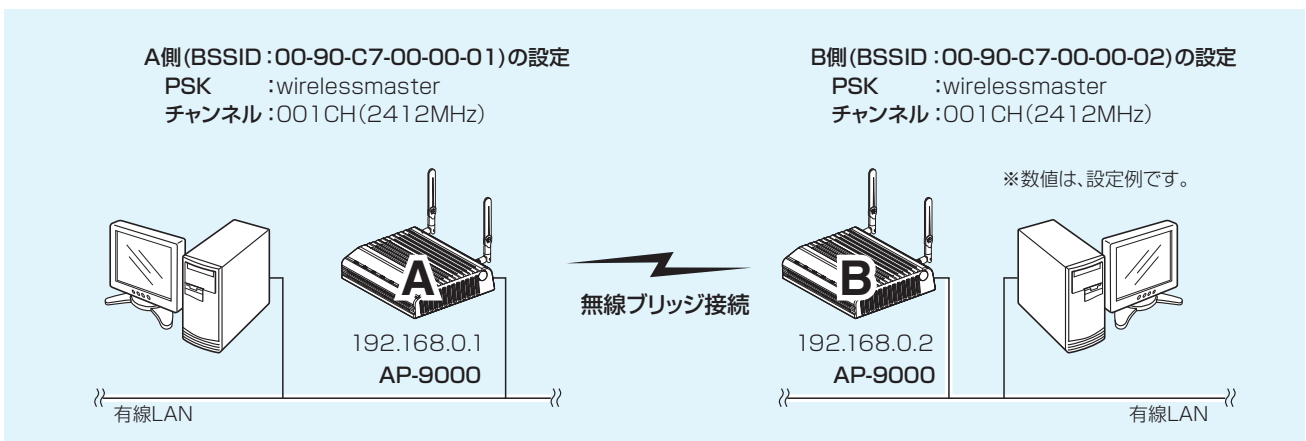
※使用条件については、「無線AP(アクセスポイント)間通信機能について」をご覧ください。(P.1-11)

※最初に、相手側の無線アクセスポイントと同じチャンネル(例：001CH(2412MHz))に設定してください。

※チャンネルを「自動」に設定した場合、無線AP間通信機能は動作しません。

※本製品のIPアドレスは、「本体IPアドレスを変更する」(P.2-8)で設定されているものとします。

[AP間通信設定]項目 インターフェース : [wds0]
接続先BSSID : [00-90-C7-00-00-02]をA側に登録する
: [00-90-C7-00-00-01]をB側に登録する
PSK(Pre-Shared Key) : [wirelessmaster](同じ共有鍵をA側とB側に設定する)

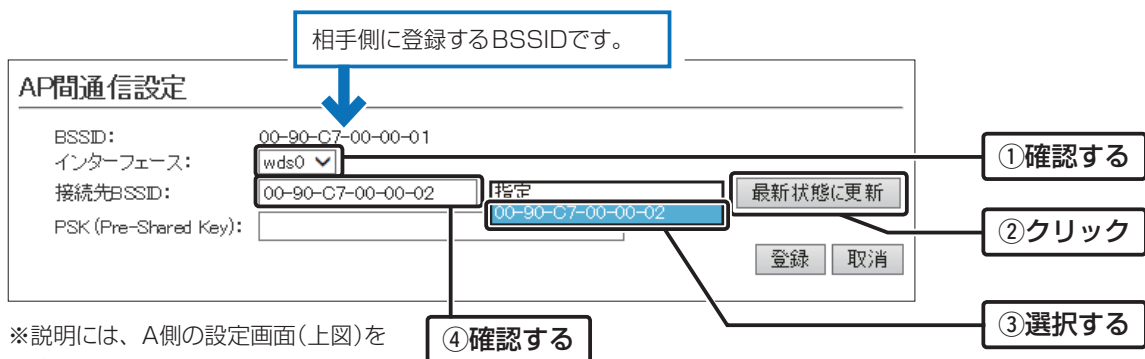


1 「無線設定」メニューの「無線1」、「AP間通信 (WDS)」の順にクリックします。

2 設定条件にしたがって、自動検出された対向する相手側のBSSIDを下記のように登録します。

※B側のBSSID(例：00-90-C7-00-00-02)をA側に登録、A側のBSSID(例：00-90-C7-00-00-01)をB側に登録します。

※自動検出されないときは、相手のBSSIDを[接続先BSSID]欄に直接入力します。



(次ページにつづく)

3 無線LAN接続[基本編]

6. 無線AP(アクセスポイント)間通信機能を設定するには

無線設定 > 無線1 > AP間通信 (WDS)

■ 無線1 (2.4GHz帯)で使用する場合(WDS)(つづき)

3 無線AP間通信専用の共有鍵を[PSK(Pre-Shared Key)]欄に入力します。

※双方に同じ共有鍵(例: wirelessmaster)を設定します。

AP間通信設定

BSSID: 00-90-C7-00-00-01
インターフェース: wds0
接続先BSSID: 00-90-C7-00-00-02 指定 最新状態に更新
PSK (Pre-Shared Key): wirelessmaster

登録 取消

①入力する

②クリック

AP間通信設定一覧

インターフェース	BSSID	PSK	編集	削除
wds0	00-90-C7-00-00-02	wirelessmaster		
wds1				
wds2				
wds3				
wds4				
wds5				
wds6				
wds7				

③確認する

4 <再起動>をクリックします。

再起動 再起動が必要な項目が変更されています。

再起動

AP間通信設定

クリック

※表示される画面にしたがって、本製品を再起動します。

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

3 無線LAN接続[基本編]

6. 無線AP(アクセスポイント)間通信機能を設定するには(つづき)

無線設定 > 無線2 > AP間通信 (WBR)

■ 無線2(5GHz帯)で使用する場合(WBR)

次の条件で、2台の本製品(図：親機の仮想AP「ath8」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(アクセスポイント)間通信機能について」をご覧ください。(P.1-12)

※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、チャンネル詳細設定で5.3/5.6GHz帯のチャンネルを選択した場合(P.4-3)、無線AP間通信機能は動作しません。

※子機は自動的に親機のチャンネルになります。

本書では、出荷時の設定「036 CH (5180 MHz)」(無線2)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「ath15」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」(P.2-8)で設定されているものとします。

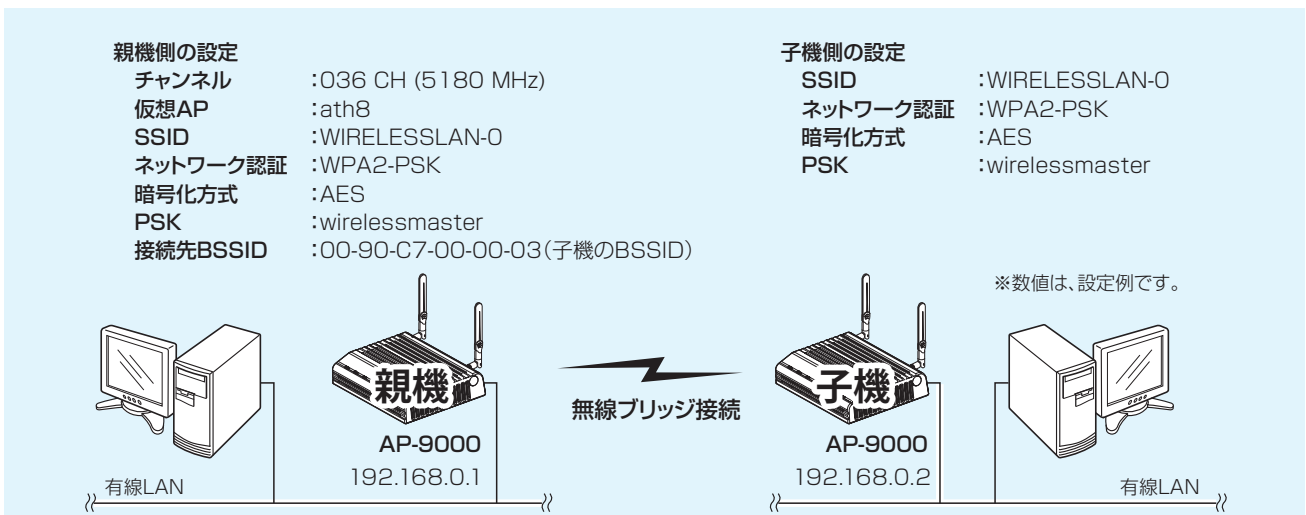
親機(P.3-18)

[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	: 「ath8」 ※親機側の仮想AP「ath8」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	: 「wbr8」
	接続先BSSID	: 「00-90-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せん。

子機(P.3-20)

[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、「wbr17」から変更できません。



3 無線LAN接続[基本編]

6. 無線AP(アクセスポイント)間通信機能を設定するには(つづき)

無線設定 > 無線2 > AP間通信 (WBR)

■ 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 「無線設定」メニューの「無線2」、「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「ath8」を設定します。

仮想AP設定

インターフェース: ath8
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
アカウントing: 無効 有効
MAC認証: 無効 有効

暗号化設定

ネットワーク認証: WPA2-PSK
暗号化方式: AES
PSK (Pre-Shared Key): wirelessmaster
WPAキー更新間隔: 120 分

登録

① 選択する
② 入力する
③ クリック

無線AP間通信で利用できる親機側の仮想APは「ath8」だけです。
出荷時の設定であることを確認します。

- 3 「無線設定」メニューの「無線2」、「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: wbr8
接続先BSSID: 00-90-C7-00-00-03

登録

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)

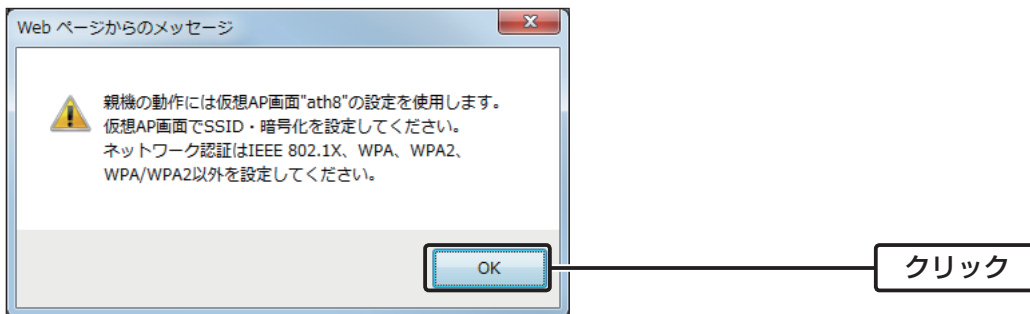
3 無線LAN接続[基本編]

6. 無線AP(アクセスポイント)間通信機能を設定するには

無線設定 > 無線2 > AP間通信 (WBR)

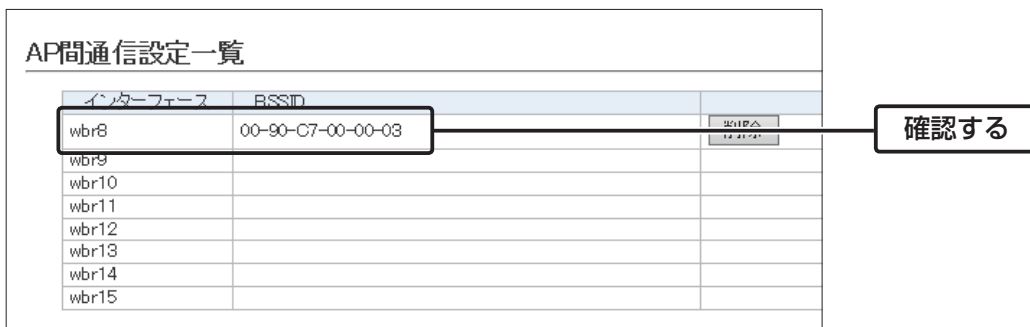
■ 親機を設定する(つづき)

5 <OK>をクリックします。

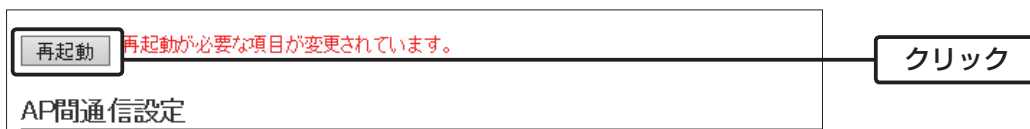


※無線2では、親機側の仮想AP「ath8」に設定されたSSIDと暗号化を使用して、無線AP間通信をします。
※子機側は、SSIDと暗号化が一致する親機をスキャンします。

6 [AP間通信設定一覧]項目の登録内容を確認します。



7 <再起動>をクリックします。



※表示される画面にしたがって、本製品を再起動します。

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

3 無線LAN接続[基本編]

6. 無線AP(アクセスポイント)間通信機能を設定するには(つづき)

無線設定 > 無線2 > AP間通信 (WBR)

■ 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。

※無線2では、親機側の仮想AP「ath8」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2(5GHz帯)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「ath15」は使用できなくなります。

1 「無線設定」メニューの「無線2」、「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:

子機設定

BSSID: 00-90-C7-00-00-03

インターフェース: wbr17

SSID: WIRELESSLAN-0

ネットワーク認証: WPA2-PSK

暗号化方式: AES

PSK (Pre-Shared Key): wirelessmaster

登録

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。

Web ページからのメッセージ

子機に設定すると仮想AP"ath15"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

4 <再起動>をクリックします。

再起動

再起動が必要な項目が変更されています。
AP間通信の子機として動作するときは、チャンネル設定は無効です。
AP間通信の子機として動作するときは、WMM詳細設定は無効です。

AP間通信設定

クリック

※表示される画面にしたがって、本製品を再起動します。

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

3 無線LAN接続[基本編]

6. 無線AP(アクセスポイント)間通信機能を設定するには(つづき)

無線設定 > 無線1 > AP間通信 (WDS)

無線設定 > 無線2 > AP間通信 (WBR)

管理 > 管理ツール

■ 無線AP間通信で使用する本製品をRS-AP3で管理するときは

- ① AP-9000側の設定画面(無線1、または無線2)で無線AP間通信機能を設定して、あらかじめ通信できる状態にしておいてください。
- ② AP-9000側の設定画面で、管理ツール設定を「有効」にします。
- ③ RS-AP3で管理を開始する前に、AP-9000側の設定した内容を、「個別設定」画面[★]で設定してください。
★無線2(5GHz帯)で無線AP間通信機能をご使用になる場合は、「共通設定」画面の仮想APで親機のSSIDと暗号化を設定してください。

無線2：親機の「個別設定」画面

AP間通信(WBR)	
AP間通信	有効
動作モード	親機
接続先BSSID (wbr8)	00-90-C7-00-00-03
接続先BSSID (wbr9)	
接続先BSSID (wbr...)	
接続先BSSID (wbr...)	
接続先BSSID (wbr...)	
接続先BSSID (wbr...)	
接続先BSSID (wbr...)	
接続先BSSID (wbr...)	

無線2：子機の「個別設定」画面

AP間通信(WBR)	
AP間通信	有効
動作モード	子機
インターフェース wbr17	
SSID	WIRELESSLAN-0
ネットワーク認証	WPA2-PSK
暗号化方式	AES
PSK (Pre-Share...)	wirelessmaster
SNMP設定	
場所	共通設定を使用
連絡先	共通設定を使用

無線2：「共通設定」画面

仮想AP	
インターフェース ath8	
仮想AP	有効
SSID	WIRELESSLAN-0
VLAN ID	0
ANY接続拒否	無効
接続端末制限	63
アカウントing	無効
MAC認証	無効
暗号化設定	
ネットワーク認証	WPA2-PSK
暗号化方式	AES
PSK (Pre-Shared Key)	wirelessmaster
WPAキー更新間隔(分)	120

RS-AP3で管理するときの注意

- ◎AP-9000のポートベースVLAN機能をご使用になるときは、RS-AP3と通信できる状態にしておいてください。
- ◎管理を終了するまで、AP-9000のWAN側(ルーター設定)を変更できません。
- ◎ルーター機能使用時、AP-9000のWAN側から管理する場合には、回線種別を「固定IP」に設定し、管理を開始する前に、WAN側IPアドレスに固定IPアドレスを設定してください。
※回線種別を「DHCPクライアント」に設定してご使用になる場合は、DHCPサーバー側で静的DHCPサーバー機能などを利用し、常に同じIPアドレスが付与されるようにネットワーク環境を構築してください。
※回線種別が「PPPoE」に設定されているときは、AP-9000のWAN側から管理できません。

7. MACアドレスフィルタリングを設定するには

無線設定 > 無線1/無線2 > MACアドレスフィルタリング

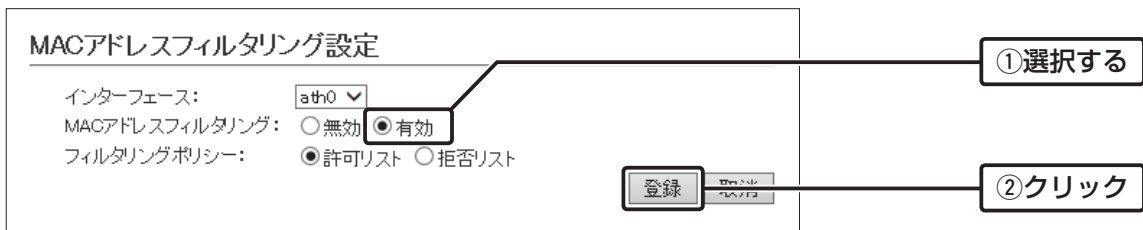
仮想AP(ath0～ath15)ごとに、本製品への接続を許可する、または拒否する無線LAN端末を登録できます。

※仮想APごとに、最大1024台分のMACアドレスを登録できます。

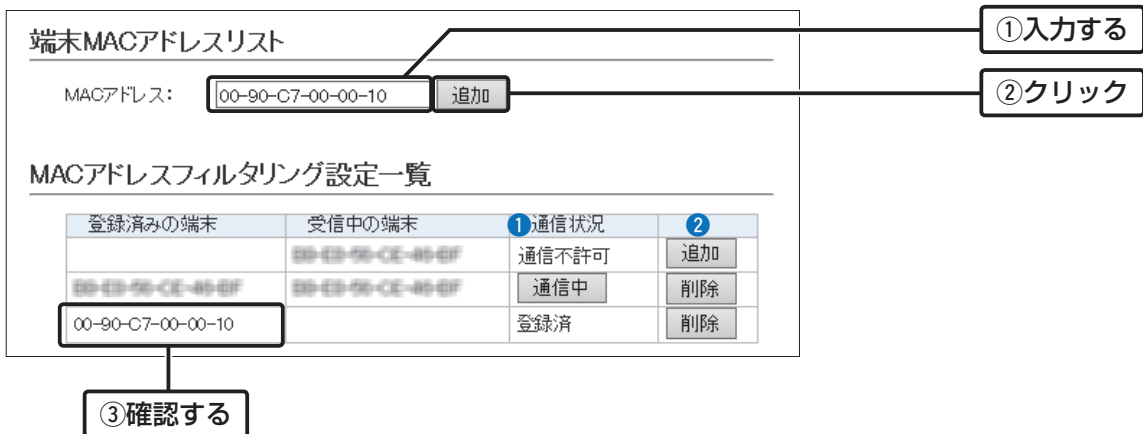
※無線1(2.4GHz帯)の仮想AP(例: ath0)を例に、接続を許可する無線LAN端末の登録を説明します。

1 「無線設定」メニューの「無線1」、「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)で表示します。
- 〔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。

この章では、
無線LANの詳細な機能を設定する手順について説明します。

1. チャンネルの自動設定について	4-2
■ 2.4GHz帯で自動チャンネルを設定するときは	4-2
■ 5GHz帯で自動チャンネルを設定するときは	4-3
2. アカウンティング設定について	4-4
■ 仮想APごとに個別設定するときは	4-4
■ 共通設定するときは	4-5
3. MAC認証サーバー (RADIUS)設定について	4-6
■ 仮想APごとに個別設定するときは	4-6
■ 共通設定するときは	4-7
4. RADIUS設定について	4-8
■ 仮想APごとに個別設定するときは	4-8
■ 共通設定するときは	4-9
5. 認証VLANについて	4-10
■ MAC認証を利用するときは	4-11
■ ネットワーク認証 (WPA/WPA2/IEEE802.1X)を利用するときは	4-11
6. ネットワーク監視設定について	4-12
7. WMM詳細について	4-13
■ WMM詳細設定	4-13
■ WMMパワーセーブ設定	4-18
■ CAC設定	4-19
8. レート設定について	4-20
■ プリセットされた設定を使用するときは	4-20
■ プリセットされた各レート設定	4-21
■ 通信レートの各設定について	4-23
■ MCS値ごとの通信レートについて	4-24
■ 仮想AP共通設定をするときは	4-25
9. ARP代理応答について	4-26
10. IP Advance Radio Systemについて	4-27
11. 本製品のPINコードについて	4-28
■ PINコードを確認してWPSを開始するときは	4-28
■ PINコードを再生成するには	4-28

4 無線LAN接続[活用編]

1. チャンネルの自動設定について

本製品の設定画面でチャンネルを「自動」に設定すると、本製品の起動時にほかの無線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。

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

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

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

無線設定 > 無線1 > 無線LAN

■ 2.4GHz帯で自動チャンネルを設定するときは

下記のように無線1(2.4GHz帯)を設定します。

1 「無線設定」メニューの「無線1」、「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(2412MHz))

無線LAN設定

無線UNIT: 無効 有効

帯域幅: 20 MHz

チャンネル: 自動

パワーレベル: 高

DTIM間隔: 1

プロテクション: 無効 有効

登録

① 選択する

② クリック

3 〈再起動〉をクリックします。

再起動

再起動が必要な項目が変更されています。
無線LANの暗号化機能が設定されていない仮想APがあります。
安心してご利用いただくため、設定されることを強くおすすめします。

無線LAN設定

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: 001 CH (2412 MHz)

パワーレベル: 高

DTIM間隔: 1

プロテクション: 無効 有効

チャンネル詳細設定

本製品が検索するチャンネルを変更するときに使用します。

<input checked="" type="checkbox"/> 001 CH (2412 MHz)	<input checked="" type="checkbox"/> 002 CH (2417 MHz)	<input checked="" type="checkbox"/> 003 CH (2422 MHz)	<input checked="" type="checkbox"/> 004 CH (2427 MHz)
<input checked="" type="checkbox"/> 005 CH (2432 MHz)	<input checked="" type="checkbox"/> 006 CH (2437 MHz)	<input checked="" type="checkbox"/> 007 CH (2442 MHz)	<input checked="" type="checkbox"/> 008 CH (2447 MHz)
<input checked="" type="checkbox"/> 009 CH (2452 MHz)	<input checked="" type="checkbox"/> 010 CH (2457 MHz)	<input checked="" type="checkbox"/> 011 CH (2462 MHz)	<input checked="" type="checkbox"/> 012 CH (2467 MHz)
<input checked="" type="checkbox"/> 013 CH (2472 MHz)			

登録 取消

登録 取消

クリック

※表示される画面にしたがって、本製品を再起動します。

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

4 無線LAN接続[活用編]

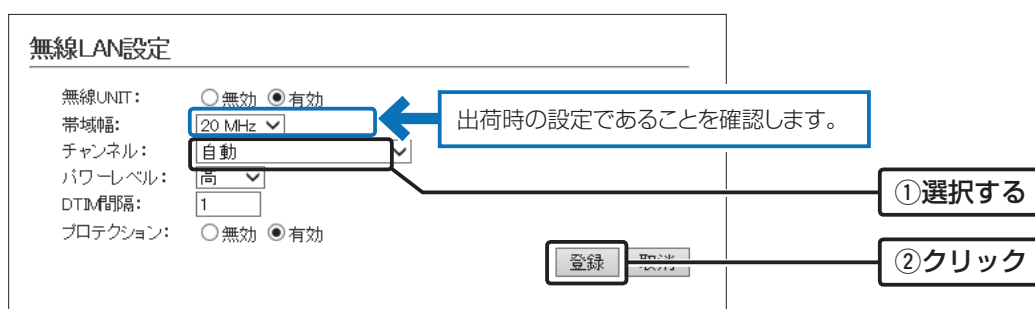
1. チャンネルの自動設定について(つづき)

無線設定 > 無線2 > 無線LAN

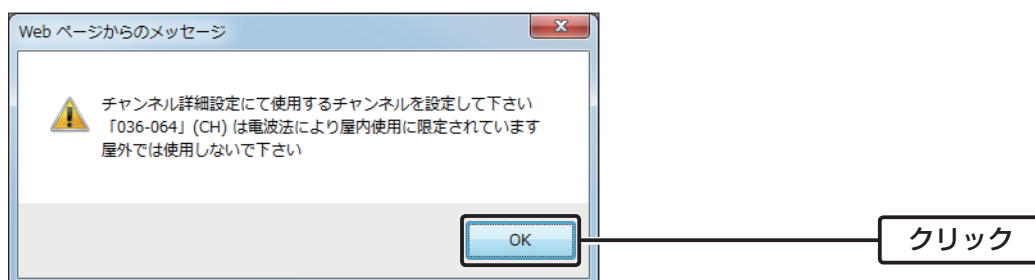
■ 5GHz帯で自動チャンネルを設定するときは

下記のように無線2(5GHz帯)を設定します。

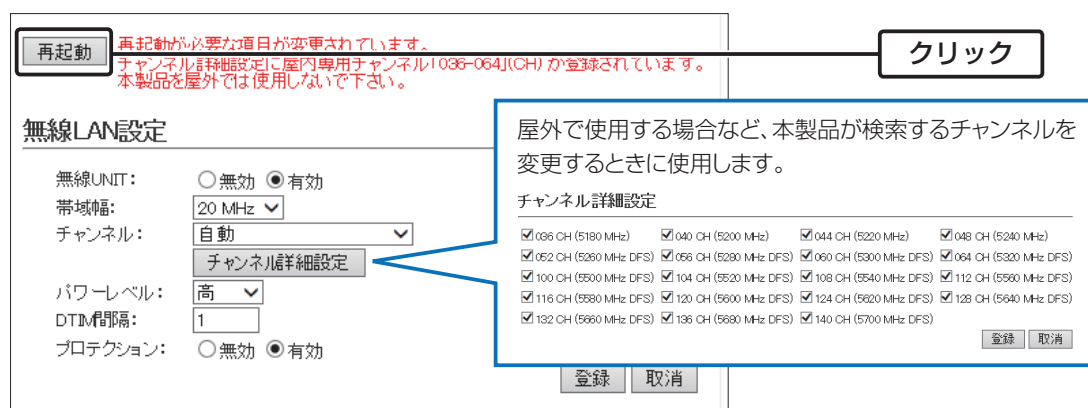
- 1 「無線設定」メニューの「無線2」、「無線LAN」の順にクリックします。
- 2 [チャンネル]欄で「自動」を選択し、〈登録〉をクリックします。 (出荷時の設定：036CH (5180MHz))



- 3 〈OK〉をクリックします。



- 4 〈再起動〉をクリックします。



※表示される画面にしたがって、本製品を再起動します。

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

屋外で使用する時のご注意

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

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

4 無線LAN接続[活用編]

2. 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、アカウンティングサーバーの設定が必要です。

※仮想APごとに個別の設定を使用するか、またはすべての仮想APで共通設定を使用するかは、「仮想AP」画面で選択できます。

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

無線設定 > 無線1/無線2 > 仮想AP

■ 仮想APごとに個別設定するときは

無線1(2.4GHz帯)の仮想AP「ath3」で個別設定する場合を例に説明します。

- 1 「無線設定」メニューの「無線1」、「仮想AP」の順にクリックします。
- 2 個別設定をする仮想APの「アカウンティング」欄で「有効」を選択します。(出荷時の設定：無効)

仮想AP設定

インターフェース: ath3

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

アカウンティング: 無効 有効

MAC認証: 無効 有効

① 選択する

② 選択する

- 3 [仮想AP毎の設定]欄で「有効」を選択し、対象となるアカウンティングサーバーについて設定します。
※ご使用になるシステムによっては、出荷時の設定値とポート番号が異なることがありますのでご確認ください。
※[シークレット]欄は、アカウンティングサーバーに設定された値と同じ設定にします。

アカウンティング設定

仮想AP毎の設定: 無効 有効

アドレス:

ポート: 1813 1813

シークレット: secret secret

登録

① 選択する

② 設定する

③ クリック

- 4 <再起動>をクリックします。

再起動 再起動が必要な項目が変更されています。

仮想AP設定

クリック

※表示される画面にしたがって、本製品を再起動します。

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

4 無線LAN接続[活用編]

2. アカウンティング設定について(つづき)

無線設定 > 無線1/無線2 > 認証サーバー

無線設定 > 無線1/無線2 > 仮想AP

■ 共通設定するとき

無線1(2.4GHz帯)で共通設定する場合を例に説明します。

- 1 「無線設定」メニューの「無線1」、「認証サーバー」の順にクリックします。
- 2 対象となるアカウンティングサーバーについて設定します。
※ご使用になるシステムによっては、出荷時の設定値とポート番号が異なることがありますのでご確認ください。
※[シークレット]欄は、アカウンティングサーバーに設定された値と同じ設定にします。

アカウンティング設定

	プライマリー	セカンダリー
アドレス:		
ポート:	1813	1813
シークレット:	secret	secret

登録

① 設定する

② クリック

- 3 「無線設定」メニューの「無線1」、「仮想AP」の順にクリックします。
- 4 共通設定をする仮想APの[アカウンティング]欄で「有効」を選択し、〈登録〉をクリックします。
(出荷時の設定：無効)

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

アカウンティング: 無効 有効

MAC認証: 無効 有効

アカウンティング設定

仮想AP毎の設定: 無効 有効

登録

① 選択する

② 選択する

③ 確認する

④ クリック

- 5 〈再起動〉をクリックします。

再起動 再起動が必要な項目が変更されています。

再起動

仮想AP設定

クリック

※表示される画面にしたがって、本製品を再起動します。

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

4 無線LAN接続[活用編]

3. MAC認証サーバー (RADIUS)設定について

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

※使用するためには、RADIUSサーバーの設定が必要です。

※仮想APごとに個別の設定を使用するか、またはすべての仮想APで共通設定を使用するかは、「仮想AP」画面で選択できます。

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

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

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

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

無線設定 > 無線1/無線2 > 仮想AP

■ 仮想APごとに個別設定するときは

無線1 (2.4GHz帯)の仮想AP「ath3」で個別設定する場合を例に説明します。

- 1 「無線設定」メニューの「無線1」、「仮想AP」の順にクリックします。
- 2 個別設定をする仮想APの[MAC認証]欄で「有効」を選択します。(出荷時の設定：無効)

仮想AP設定

インターフェース: ath3

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

アカウントing: 無効 有効

MAC認証: 無効 有効

① 選択する

② 選択する

- 3 [仮想AP毎の設定]欄で「有効」を選択し、対象となるRADIUSサーバーについて設定します。
※ご利用になるシステムによっては、出荷時の設定値とポート番号が異なることがありますのでご確認ください。
※[シークレット]欄は、RADIUSサーバーに設定された値と同じ設定にします。

MAC認証サーバー(RADIUS)設定

仮想AP毎の設定: 無効 有効

アドレス: [] []

ポート: 1812 1812

シークレット: secret secret

① 選択する

② 設定する

③ クリック

- 4 <再起動>をクリックします。

再起動 再起動が必要な項目が変更されています。

仮想AP設定

再起動

クリック

※表示される画面にしたがって、本製品を再起動します。

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

4 無線LAN接続[活用編]

3. MAC認証サーバー (RADIUS)設定について(つづき)

無線設定 > 無線1/無線2 > 仮想AP

無線設定 > 無線1/無線2 > 認証サーバー

■ 共通設定するとき

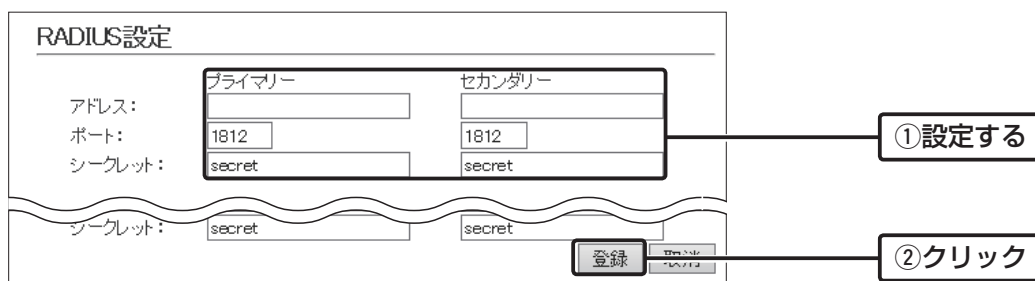
無線1(2.4GHz帯)で共通設定する場合を例に説明します。

1 「無線設定」メニューの「無線1」、「認証サーバー」の順にクリックします。

2 対象となるRADIUSサーバーについて設定します。

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

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



RADIUS設定

	プライマリー	セカンダリー
アドレス:	<input type="text"/>	<input type="text"/>
ポート:	<input type="text" value="1812"/>	<input type="text" value="1812"/>
シークレット:	<input type="text" value="secret"/>	<input type="text" value="secret"/>

シークレット:

登録

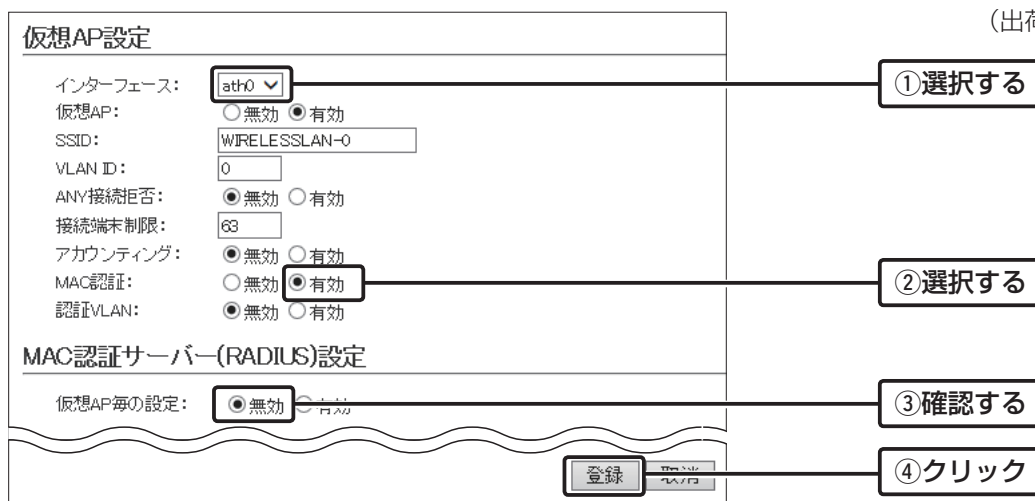
①設定する

②クリック

3 「無線設定」メニューの「無線1」、「仮想AP」の順にクリックします。

4 共通設定をする仮想APの[MAC認証]欄で「有効」を選択し、〈登録〉をクリックします。

(出荷時の設定: 無効)



仮想AP設定

インターフェース:

仮想AP: 無効 有効

SSID:

VLAN ID:

ANY接続拒否: 無効 有効

接続端末制限:

アカウントing: 無効 有効

MAC認証: 無効 有効

認証VLAN: 無効 有効

MAC認証サーバー(RADIUS)設定

仮想AP毎の設定: 無効 有効

登録

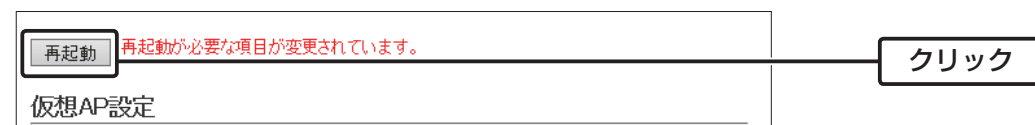
①選択する

②選択する

③確認する

④クリック

5 〈再起動〉をクリックします。



再起動 再起動が必要な項目が変更されています。

仮想AP設定

クリック

※表示される画面にしたがって、本製品を再起動します。

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

4 無線LAN接続[活用編]

4. RADIUS設定について

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

※使用するためには、RADIUSサーバーの設定が必要です。

※仮想APごとに個別の設定を使用するか、またはすべての仮想APで共通設定を使用するかは、「仮想AP」画面で選択できます。

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

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

無線設定 > 無線1/無線2 > 仮想AP

■ 仮想APごとに個別設定するときは

無線1(2.4GHz帯)の仮想AP「ath3」で個別設定する場合を例に説明します。

1 「無線設定」メニューの「無線1」、「仮想AP」の順にクリックします。

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

仮想AP設定

インターフェース: ath3

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

3 [仮想AP毎の設定]欄で「有効」を選択し、対象となるRADIUSサーバーについて設定します。
※ご使用になるシステムによっては、出荷時の設定値とポート番号が異なることがありますのでご確認ください。
※[シークレット]欄は、RADIUSサーバーに設定された値と同じ設定にします。

RADIUS設定

仮想AP毎の設定: 無効 有効

アドレス:

ポート: 1812 1812

シークレット: secret secret

登録 取消

4 <再起動>をクリックします。

再起動 再起動が必要な項目が変更されています。

仮想AP設定

※表示される画面にしたがって、本製品を再起動します。

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

4 無線LAN接続[活用編]

4. RADIUS設定について(つづき)

無線設定 > 無線1/無線2 > 仮想AP

無線設定 > 無線1/無線2 > 認証サーバー

■ 共通設定するとき

無線1(2.4GHz帯)で共通設定する場合を例に説明します。

1 「無線設定」メニューの「無線1」、「認証サーバー」の順にクリックします。

2 対象となるRADIUSサーバーについて設定します。

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

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

RADIUS設定

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

シークレット: secret secret

登録 戻る

①設定する

②クリック

3 「無線設定」メニューの「無線1」、「仮想AP」の順にクリックします。

4 共通設定をする仮想APでネットワーク認証と暗号化方式を設定し、〈登録〉をクリックします。

(例: WPA2認証)

仮想AP設定

インターフェース: ath0

仮想AP: 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

RADIUS設定

仮想AP毎の設定: 無効 有効

登録 戻る

①選択する

②設定する

③確認する

④クリック

5 〈再起動〉をクリックします。

再起動 再起動が必要な項目が変更されています。

仮想AP設定

クリック

※表示される画面にしたがって、本製品を再起動します。

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

4 無線LAN接続[活用編]

5. 認証VLANについて

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

※使用するためには、RADIUSサーバーの設定が必要です。

※仮想APごとに個別の設定を使用するか、またはすべての仮想APで共通設定を使用するかは、「仮想AP」画面で選択できます。

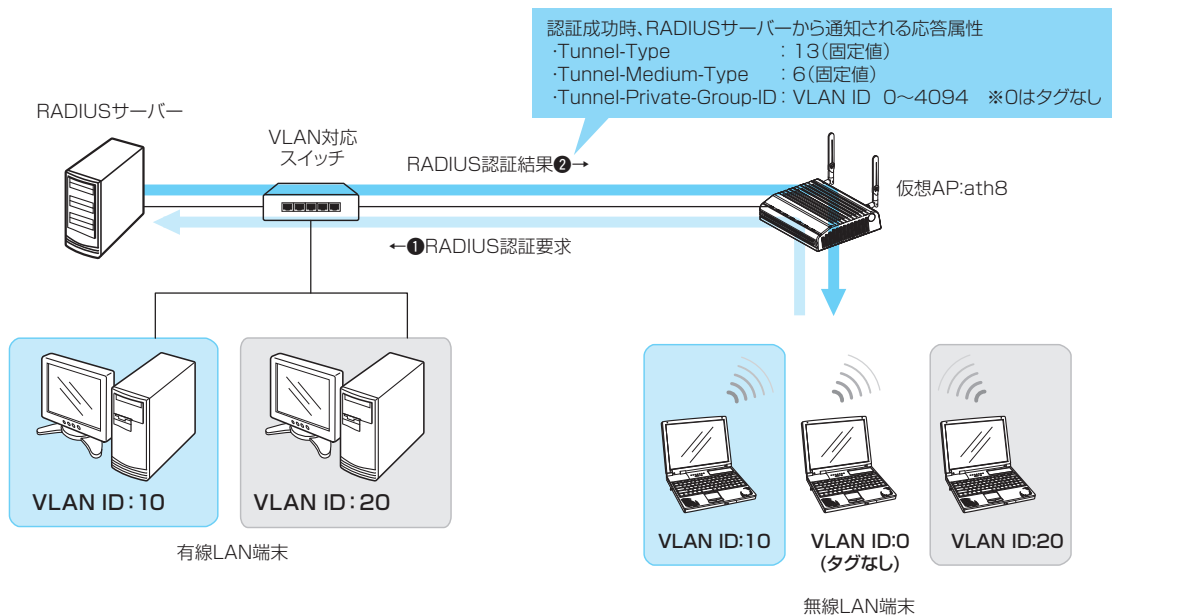
※共通設定を使用するときは、「認証サーバー」画面でRADIUSサーバーを設定します。

※「仮想AP」画面の[仮想AP設定]項目でMAC認証を有効にする、または[暗号化方式]項目でネットワーク認証(WPA/WPA2/IEEE802.1X)を選択すると、認証VLANが設定できるようになります。(P.4-11)

※仮想APにネットワーク認証とMAC認証の両方を設定し、両方の応答属性からVLAN ID情報を取得した場合、ネットワーク認証のVLAN IDが優先されます。

応答属性が通知されない場合や値が正しくない場合、仮想APに設定したVLAN IDに所属します。

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



※説明に使用している各端末のVLAN IDや仮想APは設定例です。

※認証VLAN機能利用時、同一仮想AP内(例:ath8)における同報系通信は、所属VLANグループに関係なく通知されます。

ご参考に

各無線LAN端末の所属VLAN IDは、下記のように「情報表示」メニューの「端末情報」画面で確認できます。(P.7-8)

端末情報					
現在時刻: 2023/08/15 15:24 (稼働時間: 0 days 00:15:24)					
最新状態に更新					
帰属AP	MACアドレス	IPアドレス	VLAN ID	通信モード	詳細
ath8	XXXXXXXXXX	XXXXXXXXXX	0	IEEE 802.11ac	詳細
ath8	XXXXXXXXXX	XXXXXXXXXX	10	IEEE 802.11ac	詳細
ath8	XXXXXXXXXX	XXXXXXXXXX	20	IEEE 802.11ac	詳細

※上図は、同じ仮想APに接続し、VLAN IDが異なる場合の表示例です。

4 無線LAN接続[活用編]

5. 認証VLANについて(つづき)

無線設定 > 無線1/無線2 > 仮想AP

■ MAC認証を利用するときは

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

仮想AP設定	
インターフェース:	ath0
仮想AP:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
SSID:	WIRELESSLAN-0
VLAN ID:	0
ANY接続拒否:	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
接続端末制限:	63
アカウンティング:	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
MAC認証:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
認証VLAN:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

※MAC認証するときのRADIUSサーバー設定は、本書4-6ページ～4-7ページをご覧ください。

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

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

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

無線設定 > 無線1/無線2 > 仮想AP

■ ネットワーク認証(WPA/WPA2/IEEE802.1X)を利用するときは

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

仮想AP設定	
インターフェース:	ath0
仮想AP:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
SSID:	WIRELESSLAN-0
VLAN ID:	0
ANY接続拒否:	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
接続端末制限:	63
アカウンティング:	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
MAC認証:	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
認証VLAN:	<input type="radio"/> 無効 <input checked="" type="radio"/> 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

※ネットワーク認証するときのRADIUSサーバー設定は、本書4-8ページ～4-9ページをご覧ください。

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

6. ネットワーク監視設定について

無線設定 > 無線1/無線2 > ネットワーク監視設定

本製品と指定ホストとの通信障害を検出したとき、自動的に仮想APを停止させるための設定です。

※存在しないホスト、またはセキュリティー設定などにより、PINGに 응답しないホストを設定すると、誤検出の原因になりますので、事前に正常時、障害時を含めた動作確認をしてください。

ネットワーク監視設定	
① インターフェース:	ath0 ▼
② 監視対象ホスト1:	<input type="text"/>
監視対象ホスト2:	<input type="text"/>
② 監視対象ホスト3:	<input type="text"/>
監視対象ホスト4:	<input type="text"/>
③ 監視間隔:	10 秒
④ タイムアウト時間:	1 秒
⑤ 失敗回数:	3 回
⑥ 条件:	ひとつ以上のホストが応答なし ▼

- ① **インターフェース** …………… 設定する仮想APを選択します。
- ② **監視対象ホスト1～4** …………… 監視の対象となるホストのIPアドレスを入力します。
※設定した監視対象ホストに対して、[監視間隔] (③) 欄に設定された間隔でPingを送出します。
※すべてが空欄(出荷時の設定)の場合は、死活監視をしません。
- ③ **監視間隔** …………… 指定ホストにPingを送出する間隔を設定します。
設定できる範囲は、「1～120」(秒)です。 (出荷時の設定：10)
- ④ **タイムアウト時間** …………… Pingに対する指定ホストからの応答を待つ時間を設定します。
設定できる範囲は、「1～10」(秒)です。 (出荷時の設定：1)
※設定時間を超えると、応答失敗と判断されます。
- ⑤ **失敗回数** …………… 本製品の仮想APを停止するまでのPingの応答失敗回数を設定します。
設定できる範囲は、「1～10」(回)です。 (出荷時の設定：3)
- ⑥ **条件** …………… 本製品の仮想APを停止させる条件を設定します。
(出荷時の設定：ひとつ以上のホストが応答なし)
- ◎ひとつ以上のホストが応答なし：
設定したホストのうち、1つでもホストから応答がない場合、仮想APを停止します。
 - ◎すべてのホストが応答なし：
設定したすべてのホストから応答がない場合、仮想APを停止します。

7. WMM詳細について

無線設定 > 無線1/無線2 > 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。

※パラメーターは、無線LANユニットごとに設定します。

WMM詳細設定

周波数帯: 2.4 GHz

To Station

1 AC Name	2 CWin min	2 CWin max	3 AIFSN (1-15)	5 TXOP (0-255)	6 No Ack
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

1 AC Name	2 CWin min	2 CWin max	4 AIFSN (2-15)	5 TXOP (0-255)	7 ACM
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(2~5)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。

7. WMM詳細について

無線設定 > 無線1/無線2 > WMM詳細

■ WMM詳細設定(つづき)

WMM詳細設定

周波数帯: 2.4 GHz

To Station

1 AC Name	2 CWin min	2 CWin max	3 AIFSN (1-15)	5 TXOP (0-255)	6 No Ack
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

1 AC Name	2 CWin min	2 CWin max	4 AIFSN (2-15)	5 TXOP (0-255)	7 ACM
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からランダムで選択することで、IEEE802.11規格でのフレーム衝突を回避します。

設定値が小さいほど優先順位が上がり、設定値が大きいくほど優先順位が下がります。

(出荷時の設定 : [To Station] / [From Station])

CWin min→ AC_BK(15)
AC_BE(15)
AC_VI(7)
AC_VO(3)

[To Station]

CWin max→AC_BK(1023)
AC_BE(63)
AC_VI(15)
AC_VO(7)

[From Station]

CWin max→AC_BK(1023)
AC_BE(1023)
AC_VI(15)
AC_VO(7)

7. WMM詳細について

無線設定 > 無線1/無線2 > WMM詳細

■ WMM詳細設定(つづき)

WMM詳細設定

周波数帯: 2.4 GHz

To Station

① AC Name	② CWin min	② CWin max	③ AIFSN (1-15)	⑤ TXOP (0-255)	⑥ No Ack
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

① AC Name	② CWin min	② CWin max	④ AIFSN (2-15)	⑤ TXOP (0-255)	⑦ ACM
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))

7. WMM詳細について

無線設定 > 無線1/無線2 > WMM詳細

■ WMM詳細設定(つづき)

WMM詳細設定

周波数帯: 2.4 GHz

To Station

1 AC Name	2 CWin min	2 CWin max	3 AIFSN (1-15)	5 TXOP (0-255)	6 No Ack
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

1 AC Name	2 CWin min	2 CWin max	4 AIFSN (2-15)	5 TXOP (0-255)	7 ACM
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]→ AC_BK(0)
 AC_BE(0)
 AC_VI(94)
 AC_VO(47)
 [From Station]→ AC_BK(0)
 AC_BE(0)
 AC_VI(94)
 AC_VO(47))

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. WMM詳細について

無線設定 > 無線1/無線2 > WMM詳細

■ WMM詳細設定(つづき)

WMM詳細設定

周波数帯: 2.4 GHz

To Station

① AC Name	② CWin min	② CWin max	③ AIFSN (1-15)	⑤ TXOP (0-255)	⑥ No Ack
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

① AC Name	② CWin min	② CWin max	④ AIFSN (2-15)	⑤ TXOP (0-255)	⑦ ACM
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"/>

⑦ ACM

ACM(Admission Control Mandatory)を設定します。

ACMで保護されたカテゴリーで通信するときは、チェックボックスにチェックマーク[✓]を入れます。

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

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

4 無線LAN接続[活用編]

7. WMM詳細について(つづき)

無線設定 > 無線1/無線2 > 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: <input type="radio"/> 無効 <input checked="" type="radio"/> 有効

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：有効)
「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。

4 無線LAN接続[活用編]

7. WMM詳細について(つづき)

無線設定 > 無線1/無線2 > WMM詳細

■ CAC設定

コール・アドミッション・コントロール機能によるIP電話の通話数を制限して、音声通信の品質を確保するとき設定します。

※CAC設定を使用するには、[WMM詳細設定]項目にある[ACM]欄の[AC_VO]にチェックマーク[✓]を入れてください。
[ACM]欄の[AC_VI]は、必要に応じてチェックマーク[✓]を入れてください。(4-17ページ)

CAC設定	
①通話制限台数:	<input type="text" value="6"/>
②未使用の帯域	100.00%

①通話制限台数 …………… IP電話の最大通話数を設定します。
設定できる範囲は、「1～63」です。 (出荷時の設定：6)

②未使用の帯域 …………… 全使用帯域に対する未使用帯域の割合を表示します。
制限台数倍率の目安：IEEE802.11g規格の場合

CODEC 通信速度	G711 (20ms)	G711 (40ms)	G729a (20ms)	G723.1 (30ms)	G729a (40ms)
1Mbps	1.00	1.17	2.00	2.83	3.50
2Mbps	1.67	2.17	2.83	4.17	5.33
5.5Mbps	3.00	4.50	4.17	6.00	7.83
11Mbps	3.83	6.33	4.67	6.83	9.00
6Mbps	6.00	7.50	12.50	17.83	21.67
9Mbps	8.00	10.50	15.33	21.83	27.17
12Mbps	10.33	13.83	18.83	27.33	34.00
18Mbps	13.50	18.67	22.00	31.67	40.33
24Mbps	16.17	23.17	25.00	36.33	46.33
36Mbps	19.67	29.83	27.50	40.00	51.83
48Mbps	22.00	34.83	29.00	42.17	55.17
54Mbps	22.83	36.83	29.33	42.67	56.50

通信速度を「1Mbps」、CODEC規格を「G711(20ms)」とした基準を「1」として、無線LAN端末の通信速度を変化させたときの通話制限台数に対する倍率の目安です。

【例】通話制限台数が「6」(出荷時の設定)の場合、1Mbps端末では6台に制限されますが、5.5Mbpsでは18台まで収容できます。(表中：倍率3.00)
なお、通信条件などによって多少異なる場合がありますのでご注意ください。

8. レート設定について

無線設定 > 無線1/無線2 > レート

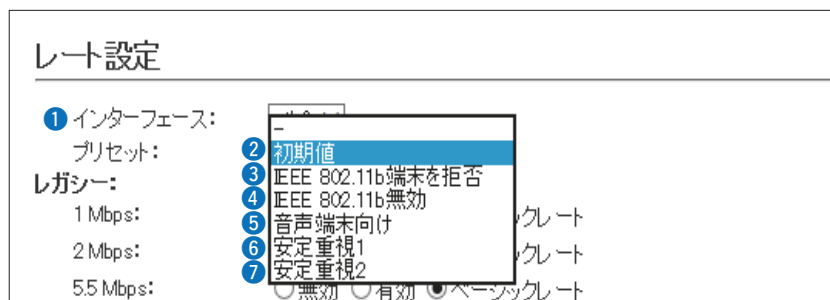
■ プリセットされた設定を使用するときは

本製品と接続できる無線LAN端末を制限するとき、またはマルチキャストパケット伝送時の速度を指定するときに、「レート」画面で仮想AP(ath0～ath15)ごとにレートを設定できます。

プリセットされた設定を使用する場合は、「初期値」、「IEEE 802.11b端末を拒否」*、「IEEE 802.11b無効」*、「音声端末向け」、「安定重視1」、「安定重視2」から選択します。

★無線2では表示されない項目です。

※プリセットされた設定内容(P.4-21)を変更したときは、[プリセット]欄に「-」が表示されます。



- ① **インターフェース** …………… 設定する仮想APを選択します。
- ② **初期値** …………… レート設定を出荷時の状態に戻すときに使用します。
- ③ **IEEE802.11b端末を拒否*** …… 6Mbps、12Mbps、24Mbpsのレートをベーシックレートに設定することで、IEEE802.11b規格だけで動作する端末からの接続を拒否するときに使用します。IEEE802.11b規格のレートは有効のため、IEEE802.11g規格対応の端末に対して、IEEE802.11b規格のレートで通信できます。
- ④ **IEEE802.11b無効*** …………… IEEE802.11b規格のレートを無効化することで、IEEE802.11b規格での通信を無効化します。IEEE802.11b規格のレートを使用することによる通信品位の低下を改善したい場合に使用します。
- ⑤ **音声端末向け** …………… 音声端末向けにIEEE802.11b規格のレートを無効化し、さらに中間のレートを無効化することで、通話品位悪化時のパケット再送回数を低減し、通話を安定させます。
- ⑥ **安定重視1** …………… 無線アクセスポイントと無線LAN端末の通信において、速度重視ではなく、安定性を重視したい場合に使用します。IEEE802.11ac規格、IEEE802.11n規格の高いレートを無効化することで、電波状況が悪い場合にパケット再送回数を低減し、通信を安定させます。
- ⑦ **安定重視2** …………… 「安定重視1」で通信の安定性が改善しない場合に選択します。「安定重視1」よりもさらに多くのレートを無効化して、通信を安定させます。

4 無線LAN接続[活用編]

8. レート設定について

無線設定 > 無線1/無線2 > レート

■ プリセットされた各レート設定

初期値	IEEE802.11b端末を拒否	IEEE802.11b無効
1Mbps ベーシックレート (2.4GHz時) 非表示(5GHz時)	1Mbps 有効 2Mbps 有効 5.5Mbps 有効	1Mbps 無効 2Mbps 無効 5.5Mbps 無効
2Mbps ベーシックレート (2.4GHz時) 非表示(5GHz時)	6Mbps ベーシックレート 9Mbps 有効 11Mbps 有効	6Mbps ベーシックレート 9Mbps 有効 11Mbps 無効
5.5Mbps ベーシックレート (2.4GHz時) 非表示(5GHz時)	12Mbps ベーシックレート 18Mbps 有効 24Mbps ベーシックレート	12Mbps ベーシックレート 18Mbps 有効 24Mbps ベーシックレート
6Mbps 有効(2.4GHz時) ベーシックレート(5GHz時)	36Mbps 有効 48Mbps 有効 54Mbps 有効	36Mbps 有効 48Mbps 有効 54Mbps 有効
9Mbps 有効	MCS0 有効 MCS1 有効 MCS2 有効 MCS3 有効 MCS4 有効 MCS5 有効 MCS6 有効 MCS7 有効 MCS8 有効 MCS9 有効 MCS10 有効 MCS11 有効 MCS12 有効 MCS13 有効 MCS14 有効 MCS15 有効	MCS0 有効 MCS1 有効 MCS2 有効 MCS3 有効 MCS4 有効 MCS5 有効 MCS6 有効 MCS7 有効 MCS8 有効 MCS9 有効 MCS10 有効 MCS11 有効 MCS12 有効 MCS13 有効 MCS14 有効 MCS15 有効
11Mbps ベーシックレート (2.4GHz時) 非表示(5GHz時)		
12Mbps 有効(2.4GHz時) ベーシックレート(5GHz時)		
18Mbps 有効		
24Mbps 有効(2.4GHz時) ベーシックレート(5GHz時)		
36Mbps 有効		
48Mbps 有効		
54Mbps 有効		
MCS0 有効		
MCS1 有効		
MCS2 有効		
MCS3 有効		
MCS4 有効		
MCS5 有効		
MCS6 有効		
MCS7 有効		
MCS8 有効		
MCS9 有効		
MCS10 有効		
MCS11 有効		
MCS12 有効		
MCS13 有効		
MCS14 有効		
MCS15 有効		
VHT-MCS 1ストリーム MCS0-9(IEEE802.11ac 対応時のみ表示)		
VHT-MCS 2ストリーム MCS0-9(IEEE802.11ac 対応時のみ表示)		
マルチキャストレート 1Mbps(2.4GHz時) 6Mbps(5GHz時)	マルチキャストレート 1Mbps	マルチキャストレート 6Mbps

4 無線LAN接続[活用編]

8. レート設定について

無線設定 > 無線1/無線2 > レート

■ プリセットされた各レート設定(つづき)

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

4 無線LAN接続[活用編]

8. レート設定について(つづき)

無線設定 > 無線1/無線2 > レート

■ 通信レートの各設定について

本製品と接続できる無線LAN端末を制限するとき、またはマルチキャストパケット伝送時の速度を指定するときは、「レート」画面で各仮想AP(ath0～ath15)のレートを設定します。

ベーシックレートを設定した場合、無線LAN端末側が、その速度やMCS値を使用できることが条件となります。たとえば、ベーシックレートを設定したレートで通信できない無線LAN端末は、本製品に接続できません。

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

[レガシー]欄は、IEEE802.11a/g/b規格での通信速度ごとに設定します。

- 無効：選択した速度では通信しない
- 有効：選択した速度で通信する
- ベーシックレート
：無線LAN端末が選択した速度で通信できない場合は接続を許可しない

レート設定

インターフェース: ath0 ▼ 初期値

プリセット: 初期値

レガシー:

1 Mbps:	<input type="radio"/> 無効	<input type="radio"/> 有効	<input checked="" type="radio"/> ベーシックレート
2 Mbps:	<input type="radio"/> 無効	<input type="radio"/> 有効	<input checked="" type="radio"/> ベーシックレート
5.5 Mbps:	<input type="radio"/> 無効	<input type="radio"/> 有効	<input checked="" type="radio"/> ベーシックレート
6 Mbps:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
9 Mbps:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
11 Mbps:	<input type="radio"/> 無効	<input type="radio"/> 有効	<input checked="" type="radio"/> ベーシックレート
12 Mbps:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
18 Mbps:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
24 Mbps:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
36 Mbps:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
48 Mbps:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
54 Mbps:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート

HT-MCS:

MCS 0:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
MCS 1:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
MCS 2:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
MCS 3:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
MCS 4:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
MCS 5:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
MCS 6:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
MCS 7:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
MCS 8:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
MCS 9:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
MCS 10:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
MCS 11:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
MCS 12:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
MCS 13:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
MCS 14:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート
MCS 15:	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="radio"/> ベーシックレート

マルチキャスト送信レート:
マルチキャストレート: 1 Mbps ▼

[HT-MCS]欄は、IEEE802.11n規格以降での変調方式、ストリーム数、通信レートなどを対応付けしたMCS値(P.4-24)ごとに設定します。

- 無効：選択したMCS値では通信しない
- 有効：選択したMCS値で通信する
- ベーシックレート
：無線LAN端末が選択したMCS値で通信できない場合は接続を許可しない

※無線2(5GHz帯)の「レート」画面には、[VHT-MCS]欄も表示されますので、ストリーム数ごとに、対応するMCS値(P.4-24)を設定します。

VHT-MCS:

1ストリーム:	<input type="radio"/> MCS 0-7	<input type="radio"/> MCS 0-8	<input checked="" type="radio"/> MCS 0-9
2ストリーム:	<input type="radio"/> MCS 0-7	<input type="radio"/> MCS 0-8	<input checked="" type="radio"/> MCS 0-9

マルチキャスト送信レートの設定について

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

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

4-23

株式会社エクセリ(代理店届出番号C1909977) 東京都墨田区菊川3 17 2 アドン菊川ビル4F / 大阪府大阪市中央区久太郎町1 9 5 URL : <https://www.exseli.com/>

4 無線LAN接続[活用編]

8. レート設定について(つづき)

無線設定 > 無線1/無線2 > レート

■ MCS値ごとの通信レートについて

下表を目安に、「レート」画面で[HT-MCS]欄や[VHT-MCS]欄を設定してください。

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

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

8. レート設定について(つづき)

無線設定 > 無線1/無線2 > レート

■ 仮想AP共通設定をするときは

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

仮想AP共通設定

①最低レートの再送制限: 無効 有効

②キックアウト: 弱

- ①最低レートの再送制限 …………… 最低レートでの再送を制限することで、ほかの端末に対する悪影響を抑止します。
(出荷時の設定：無効)
通信品位の悪い端末の存在がほかの端末に対して悪影響をおよぼす場合に設定すると、全体の通信品位の悪化を低減できます。
※無線1だけに表示される項目です。
- ②キックアウト …………… 通信品位の低い端末を早期に追い出すことで、ほかの端末に対する悪影響を抑止します。
(出荷時の設定：弱)
通信品位の悪い端末の存在がほかの端末に対して悪影響をおよぼす場合に設定すると、全体の通信品位の悪化を低減できます。
設定するときは、「無効」、「弱」、「中」、「強」から選択します。
「強」にするほど、通信品位の低い端末を追い出しやすくなるため、通信品位の低い端末は切断されやすくなります。

9. ARP代理応答について

無線設定 > 無線1/無線2 > ARP代理応答

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	
① インターフェース:	ath0 ▼
② ARP代理応答:	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
③ 不明なARPの透過:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
④ ARPエージング時間:	0 分

- ① インターフェース …………… 設定する仮想APを選択します。
- ② ARP代理応答 …………… [インターフェース] (①) 欄で選択した仮想APで、ARP代理応答の機能を使用するかしないかを設定します。 (出荷時の設定：無効)
- ③ 不明なARPの透過 …………… [インターフェース] (①) 欄で選択した仮想APと通信している無線LAN端末すべてのARP情報がわかっていて、不明なARPが来たとき、透過するかしないかを設定します。 (出荷時の設定：有効)
- ARPリクエストを受信したとき、本製品に接続している無線LAN端末のIPアドレス学習状況によって、下記のような処理をします。
- ◎ IPアドレス学習済みの無線LAN端末だけが存在する場合
ARPリクエストのTargetIPが学習したIPアドレスと一致する場合は、本製品が代理応答します。
一致しない場合、[不明なARPの透過] (③) 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] (③) 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。
※「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、時間設定に関わらずARP情報が削除されます。

ARPキャッシュ情報について

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

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

10. IP Advance Radio Systemについて

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

本製品をIP1000Cの近隣呼出機能(特定のエリアに限定して運用する機能)と連動させて利用するときには設定します。
[通知]欄を「有効」に設定して名前を登録しておくこと、IP1000C側の「近隣呼出接続」画面で、無線アクセスポイントを自動検索することで、BSSIDと名前の検索や登録ができます。

※下記のように、設定する仮想APを選択すると、テナント番号ごとに無効、有効が選択できます。
※名前(例：1Fフロア)を設定するときは、半角31(全角15)文字以内で入力します。

近隣呼出設定

インターフェース: ath0 ▼

BSSID: XXXXXXXXXX

テナント番号	通知	名前
1	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効	1Fフロア
2	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効	
3	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効	
4	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効	
5	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効	
6	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効	
7	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効	
8	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効	
9	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効	
10	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効	

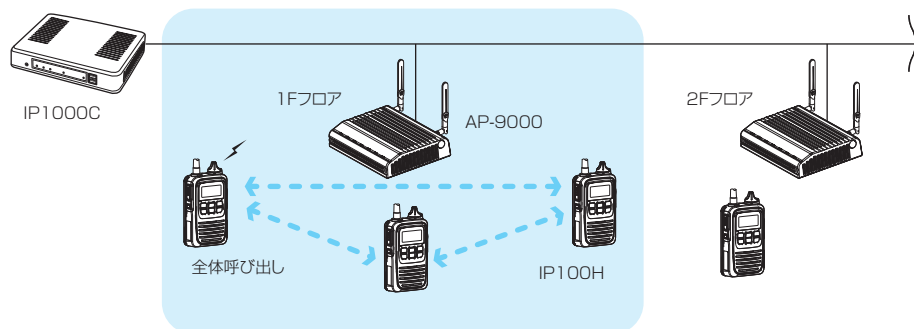
登録

近隣呼出機能について

特定のエリア(例:1Fフロア)に限定して、IP1000Hを運用するとき使用する機能です。

※IP1000C側で、近隣呼出機能を使用するエリア(無線アクセスポイント)の登録が必要です。

【IP1000Hから近隣呼出機能で全体呼び出しをした場合】



4 無線LAN接続[活用編]

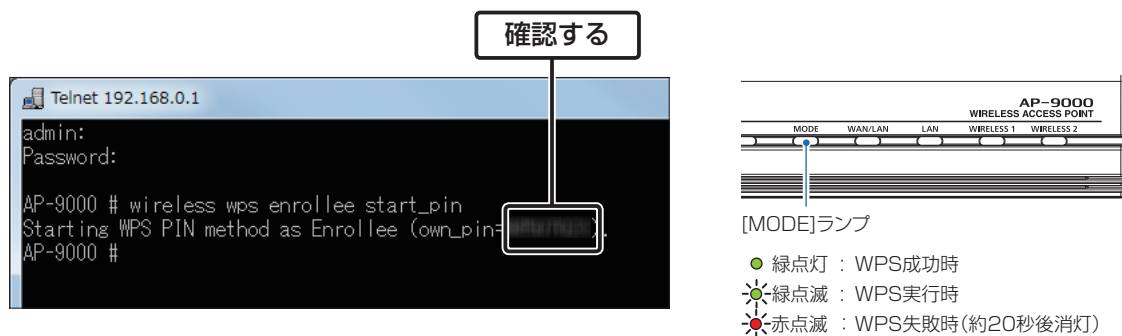
11. 本製品のPINコードについて

無線設定 > WPS

本製品のPINコード(8桁の半角数字)は、WPS対応の無線LAN端末で生成したSSIDと暗号化方式をPIN方式で本製品に自動設定をするときに必要になります。

■ PINコードを確認してWPSを開始するときは

- ① WPS機能[★]を使用する本製品の仮想APを設定してから、Telnetや[CONSOLE]ポート(P.8-6)を使用して本製品(例：192.198.0.1)にアクセスします。
★「WPS」画面で、「SSID及び暗号化設定」欄を「WPSで設定を生成する」に設定し、「WPS状態」欄が「未設定」(初期状態)になっていることを確認してください。
- ② [AP-9000 #]につづいて、「**wireless wps enrollee start_pin**」を入力後、[Enter]キーを押します。
PINコードが表示されると同時に、本製品の[MODE]ランプがゆっくり[☼]緑点滅します。
- ③ 無線LAN端末側に本製品のPINコードを入力し、WPSを開始してください。



■ PINコードを再生成するには

- ① WPS機能を使用する本製品の仮想APを設定してから、Telnetや[CONSOLE]ポート(P.8-6)を使用して本製品(例：192.198.0.1)にアクセスします。
- ② [AP-9000 #]につづけて、「**wireless wps generate_pin**」を入力後、[Enter]キーを押します。
- ③ 保存のため[AP-9000 #]につづけて、「**save**」を入力後、[Enter]キーを押します。

```
Telnet 192.168.0.1
login: admin
Password:
AP-9000 # wireless wps generate_pin
AP-9000 # save
AP-9000 #
```

※[AP-9000 #]につづいて、「**wireless wps enrollee start_pin**」を入力後、[Enter]キーを押すと、再生成したPINコードが表示されると同時に、本製品の[MODE]ランプがゆっくり[☼]緑点滅します。

この章では、
設定の追加や変更が必要と思われる項目などについて説明します。

1. 設定画面へのアクセスを制限するには	5-2
2. 内部時計を設定するには	5-3
3. 本製品のDHCPサーバー機能を使用するには	5-4
■ DHCPサーバー設定	5-4
■ 静的DHCPサーバー設定	5-5
4. 「ルーティング」画面について	5-6
■ IP経路情報	5-6
■ スタティックルーティング設定	5-7
5. パケットフィルターの使用例について	5-8
① 仮想AP内の無線LAN端末同士の通信を禁止するには	5-9
② 仮想AP間の無線LAN端末同士の通信を禁止するには	5-10
③ AP-9000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	5-11
④ 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	5-12
6. Web認証機能を設定するには	5-13
■ Web認証ページを設定するときは	5-13
■ カスタムページの作成について	5-15
7. 「管理」画面について	5-19
■ HTTP/HTTPS設定	5-19
■ HTTP/HTTPS設定後、設定画面にアクセスできなくなったときは	5-20
■ Telnet/SSH設定	5-21
■ SSH公開鍵管理	5-23
■ SYSLOG設定	5-24
■ SNMP設定	5-25
■ LED消灯モード	5-26
■ PINGテスト	5-27
■ 経路テスト	5-28
8. 本製品のルーター機能を使用するには	5-29
■ ご契約回線への接続方法を確認する	5-29
■ WAN側(有線LAN)を設定するときは	5-29
■ DHCP方式での接続を指定された場合(DHCPクライアント)	5-30
■ 固定IPアドレスでの接続を指定された場合(固定IP)	5-31
■ PPPoE方式での接続を指定された場合(PPPoE)	5-32
■ アドレス変換設定	5-34
■ 静的マスカレードテーブル設定	5-35
■ 静的マスカレードテーブル設定一覧	5-36
■ IPフィルターについて	5-37
9. ポートベースVLAN機能を設定するには	5-38
■ ポートベースVLANを設定するときは	5-38
■ トランキングポートを設定するには	5-40
10. POPCHAT@Cloud連携機能を設定するときは	5-42
■ POPCHAT@Cloud連携機能を設定するときは	5-43

5 そのほかの機能について

1. 設定画面へのアクセスを制限するには

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

管理 > 管理者

- 1 「管理」メニュー、「管理者」の順にクリックします。
「管理者」画面が表示されます。
- 2 [現在のパスワード]、[新しいパスワード]、[新しいパスワード再入力]欄に、大文字/小文字の区別に注意して、任意の英数字/記号(半角31文字以内)で入力します。
[新しいパスワード]、[新しいパスワード再入力]欄に入力した文字は、すべて*(アスタリスク)、または●(黒丸)で表示されます。

管理者パスワードの変更

管理者ID: admin

現在のパスワード: ●●●●

新しいパスワード: ●●●●●●●●

新しいパスワード再入力: ●●●●●●●●

登録 取消

入力する

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

不正アクセス防止のアドバイス

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

数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた長く複雑なものにし、さらに定期的にパスワードを変更すると効果があります。

ご注意

管理者パスワードを忘れた場合、設定画面を確認するには、工場出荷時(初期化)の状態に戻す必要があります。

※初期化するときは、本書6-4ページの手順にしたがって、本製品の<INIT>ボタンを操作してください。

5 そのほかの機能について

2. 内部時計を設定するには

本製品の内部時計を正確に表示させるため、設定されることをおすすめします。

※本製品の自動時計設定機能を使用する場合についても記載していますので、併せてご覧ください。

管理 > 時計

- 1 「管理」メニュー、「時計」の順にクリックします。
「時計」画面が表示されます。
- 2 パソコンから自動取得した時刻が、[時刻設定]項目に表示されていることを確認して、〈設定〉をクリックします。
内部時計に設定された時刻が、[本体の現在時刻]欄に表示されます。
※[設定する時刻]欄に表示されている時刻がパソコンと異なるときは、はじめからやりなおすと正確な時刻を取得できません。
※「時計」画面の〈登録〉では、時刻を設定できません。

時刻設定

本体の現在時刻: 2008年01月01日 12時08分 (Asia/Tokyo)
設定する時刻: 2017年01月12日 14時10分 **設定**

自動時計設定

自動時計設定: 無効 有効
NTPサーバー1: 210.173.160.27
NTPサーバー2: 210.173.160.57
アクセス時間間隔: 1 日
前回アクセス日時: -
次回アクセス日時: -

登録 取消

①確認する
②クリック

「有効」に設定されているときは、インターネットに接続すると、下記のNTPサーバーにアクセスして、自動で時刻を設定できます。

※初期に参照しているNTPサーバーは、インターネットマルチフィード株式会社のもので、
<http://www.jst.mfeed.ad.jp/>

自動時計設定機能について

自動時計設定機能で「有効」を選択して〈登録〉を押した直後、NTPサーバーに日時の問い合わせをして、内部時計を自動設定します。

また、自動時計設定機能を「有効」に設定すると、本体起動時にNTPサーバーに日時の問い合わせをします。それ以降は、設定されたアクセス時間間隔で、内部時計を自動設定します。

ご注意

自動時計設定機能は、NTPサーバーへの問い合わせ先(経路)を設定する必要があります。

経路を設定しないときは、問い合わせできませんので、自動時計設定機能をお使いいただけません。

「ネットワーク設定」メニュー→「LAN側IP」画面→「IPアドレス設定」項目にある「デフォルトゲートウェイ」欄、または「ルーティング」画面の「スタティックルーティング設定」項目で、ルーティングテーブルを設定するか、「ルーター設定」メニューからルーター機能を設定してください。

5 そのほかの機能について

3. 本製品のDHCPサーバー機能を使用するには

本製品のDHCPサーバー機能を使用するときは、下記の手順でDHCPサーバー機能と自動割り当て開始IPアドレスを設定してください。

※出荷時や全設定初期化時、本製品のDHCPサーバー機能は、「無効」に設定されています。

※本製品を接続するネットワーク上に、ほかのDHCPサーバーがすでに存在する状態で使用すると、IPアドレスの競合など、ネットワーク障害の原因になりますのでご注意ください。

ネットワーク設定 > DHCPサーバー

■ DHCPサーバー設定

- 1 「ネットワーク設定」メニュー、「DHCPサーバー」の順にクリックします。
「DHCPサーバー」画面が表示されます。
- 2 [DHCPサーバー設定]項目で、[DHCPサーバー]欄の「有効」を選択し、必要に応じて[割り当て開始IPアドレス]などを変更します。

The screenshot shows the 'DHCPサーバー設定' (DHCP Server Settings) page. The 'DHCPサーバー' (DHCP Server) status is set to '有効' (Enabled). The '割り当て開始IPアドレス' (Assigned start IP address) is 192.168.0.10, '割り当て個数' (Assigned number) is 30, and 'サブネットマスク' (Subnet mask) is 255.255.255.0. The 'リース期間' (Lease time) is 72 hours. The '登録' (Register) button is highlighted with a callout box containing the text: '自動割り当て開始IPアドレスの[ネットワーク部(例：192.168.0)]が、本製品のIPアドレスのネットワーク部と同じになるように設定してください。' (Please set the network part of the automatically assigned start IP address, such as [192.168.0], to be the same as the network part of the product's IP address.)

Annotations:

- ① 選択する (Select)
- ② 変更する (Change)
- ③ クリック (Click)

- 3 <再起動>をクリックします。

The screenshot shows the '再起動' (Restart) button highlighted with a callout box containing the text: '再起動' (Restart). Below the button, the 'DHCPサーバー設定' (DHCP Server Settings) page is visible, showing the 'DHCPサーバー' (DHCP Server) status set to '有効' (Enabled).

Annotation:

- クリック (Click)

※表示される画面にしたがって、本製品を再起動します。

自動割り当て個数について

本製品で設定できる自動割り当て可能なIPアドレスの個数は、0個～128個までです。

出荷時の割り当て開始IPアドレスとサブネットマスクの設定値の場合、理論上割り当て可能なIPアドレスの個数は、最大253個までですが、128個を超える分については、手動でクライアントに割り当ててください。

5 そのほかの機能について

3. 本製品の DHCP サーバー機能を使用するには(つづき)

ネットワーク設定 > DHCPサーバー

■ 静的DHCPサーバー設定

固定IPアドレスを特定の端末に割り当てる設定です。

静的DHCPサーバー設定

MACアドレス	IPアドレス	
<input type="text"/>	<input type="text"/>	<input type="button" value="追加"/>

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"/>

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。

※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。

※本製品のDHCPサーバー機能を使用する場合に有効です。

※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、[開始IPアドレス]欄と[割り当て個数]欄が出荷時の設定の場合は、
192.168.0.40以降のIPアドレスを設定してください。

※本製品のIPアドレスと重複しないように設定してください。

※登録した内容を削除するときは、[静的DHCPサーバー設定一覧]項目で該当する欄の〈削除〉をクリックします。

5 そのほかの機能について

4. 「ルーティング」画面について

通信経路(ルート)についての設定画面です。

ネットワーク設定 > ルーティング

■ IP経路情報

パケットの送信において、そのパケットをどのルーター、またはどの端末に配送すべきかの情報を表示します。
※この項目には、現在有効な経路だけを表示します。

①宛先	②サブネットマスク	③ゲートウェイ	④経路	⑤作成
127.0.0.1	255.255.255.255	127.0.0.1	lo0	host
192.168.0.0	255.255.255.0	192.168.0.1	mirror0	misc
192.168.0.1	255.255.255.255	192.168.0.1	lo0	host
192.168.10.0	255.255.255.0	192.168.0.254	mirror0	static

- ①宛先 ルーティングの対象となるパケットの宛先IPアドレスを表示します。
- ②サブネットマスク 宛先IPアドレスに対するサブネットマスクを表示します。
- ③ゲートウェイ 宛先IPアドレスに対するゲートウェイを表示します。
- ④経路 宛先IPアドレスに対する転送先インターフェースを表示します。
◎lo0 : ループバックアドレスを意味するインターフェース
◎mirror0 : LANインターフェース
- ⑤作成 どのように経路情報が作成されたかを表示します。
◎static : スタティック(定義された)ルートにより作成
◎misc : ブロードキャストに関するフレーム処理で作成
◎host : ホストルートにより作成

5 そのほかの機能について

4. 「ルーティング」画面について(つづき)

ネットワーク設定 > ルーティング

■ スタティックルーティング設定

パケットの中継経路を最大32件まで登録できます。

※画面の値は、登録例です。

スタティックルーティング設定

①宛先	②サブネットマスク	③ゲートウェイ	④追加
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="追加"/>

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	
192.168.10.0	255.255.255.0	192.168.0.254	<input type="button" value="削除"/>

- ①宛先 対象となる相手先のIPアドレスを入力します。
- ②サブネットマスク 対象となる宛先のIPアドレスに対するサブネットマスクを入力します。
- ③ゲートウェイ パケット転送先ルーターのIPアドレスを入力します。
- ④〈追加〉 クリックすると、[スタティックルーティング設定一覧]項目に入力内容が表示されます。
※登録した内容を削除するときは、[スタティックルーティング設定一覧]項目で該当する欄の〈削除〉をクリックします。

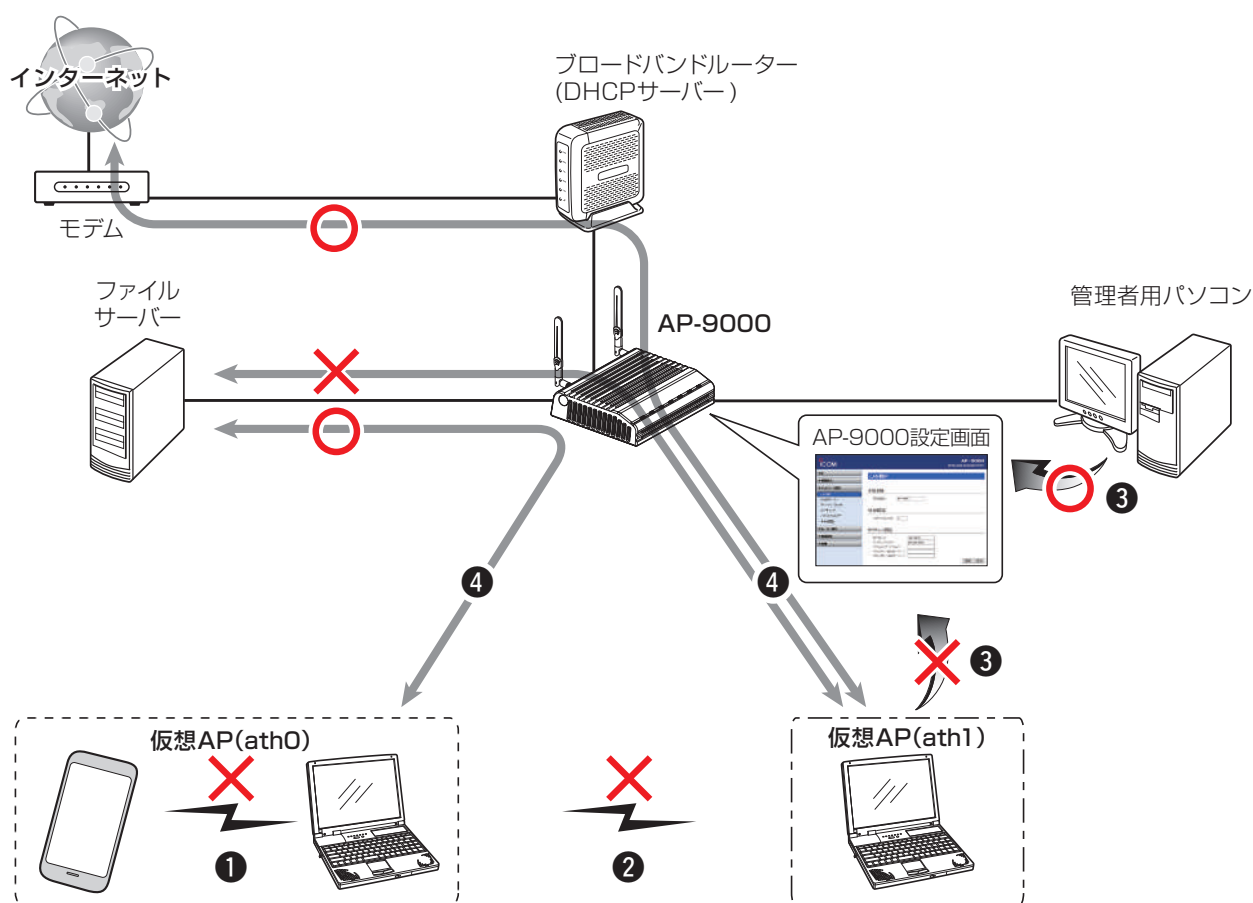
5 そのほかの機能について

5. 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(①～④)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 仮想AP内の無線LAN端末同士の通信を禁止するには (P.5-9)
- ② 仮想AP間の無線LAN端末同士の通信を禁止するには (P.5-10)
- ③ AP-9000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.5-11)
- ④ 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.5-12)



5 そのほかの機能について

5. パケットフィルターの使用例について(つづき)

ネットワーク設定 > パケットフィルター

① 仮想AP内の無線LAN端末同士の通信を禁止するには

送信元インターフェース、宛先インターフェースともにath0を設定することによりath0に接続した無線端末間通信禁止ができます。

※特定の端末だけ遮断するときは、MACアドレスを指定します。

※MACアドレスを指定しない場合、ath0に接続するすべての無線端末同士を遮断します。

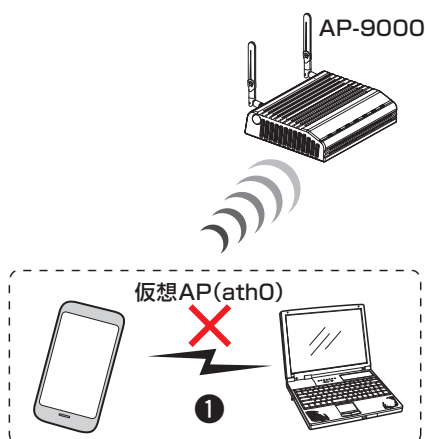
パケットフィルター設定一覧

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

「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

特定の端末だけ遮断するときは、遮断する端末のMACアドレスを指定

編集 削除



5 そのほかの機能について

5. パケットフィルターの使用例について(つづき)

ネットワーク設定 > パケットフィルター

② 仮想AP間の無線LAN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。

① 仮想AP(ath0)→仮想AP(ath1)方向の通信を遮断

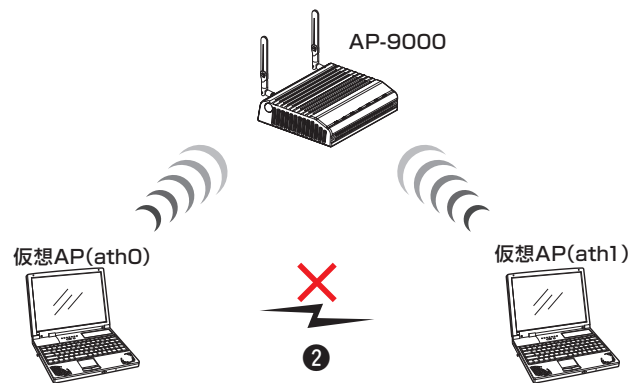
② 仮想AP(ath1)→仮想AP(ath0)方向の通信を遮断

「パケットフィルター」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	1	有効	
エントリー		ログを表示	
方法		遮断	
送信元インターフェース		ath0	編集 削除
宛先インターフェース		ath1	
送信元MACアドレス/マスク		-	
宛先MACアドレス/マスク		-	
VLAN ID		0	
Ethernetタイプ		すべて	

番号	2	有効	
エントリー		ログを表示	
方法		遮断	
送信元インターフェース		ath1	編集 削除
宛先インターフェース		ath0	
送信元MACアドレス/マスク		-	
宛先MACアドレス/マスク		-	
VLAN ID		0	
Ethernetタイプ		すべて	



5 そのほかの機能について

5. パケットフィルターの使用例について(つづき)

ネットワーク設定 > パケットフィルター

③ AP-9000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		
エントリー	有効	
ログを表示		
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	mirrar0	
送信元MACアドレス/マスク	-	
宛先MACアドレス/マスク	-	
VLAN ID	0	編集 削除
Ethernetタイプ	IP	
送信元IPアドレス	192.168.0	
宛先IPアドレス	-	
IPプロトコル	TCP	
送信元ポート	-	
宛先ポート	80	
TCPフラグ	-	
番号		
エントリー	有効	
ログを表示		
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	mirrar0	
送信元MACアドレス/マスク	-	
宛先MACアドレス/マスク	-	
VLAN ID	0	編集 削除
Ethernetタイプ	IP	
送信元IPアドレス	-	
宛先IPアドレス	-	
IPプロトコル	TCP	
送信元ポート	-	
宛先ポート	80	
TCPフラグ	-	

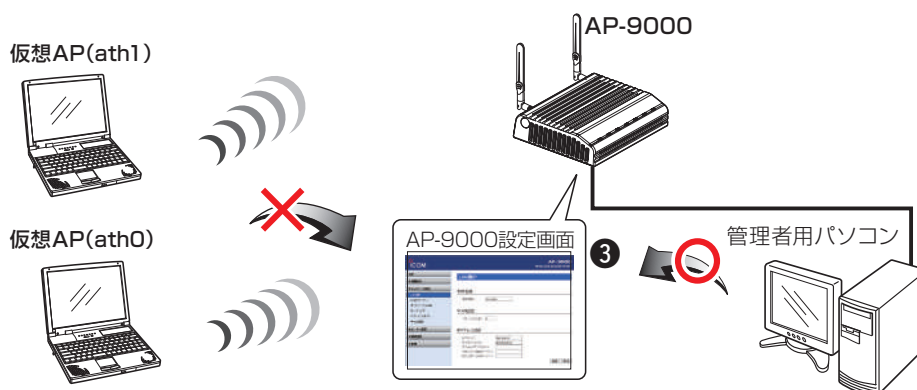
① 管理用端末からのWEBアクセスを透過

② 管理用端末以外からのWEBアクセスを遮断

「パケットフィルター」画面で設定したフィルターの番号を表示

管理者用のパソコンに設定されたIPアドレス

登録した上記のフィルターより大きな番号を表示



5 そのほかの機能について

5. パケットフィルターの使用例について(つづき)

ネットワーク設定 > パケットフィルター

④ 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を追加してください。

「パケットフィルター」画面で設定したフィルターの番号を表示

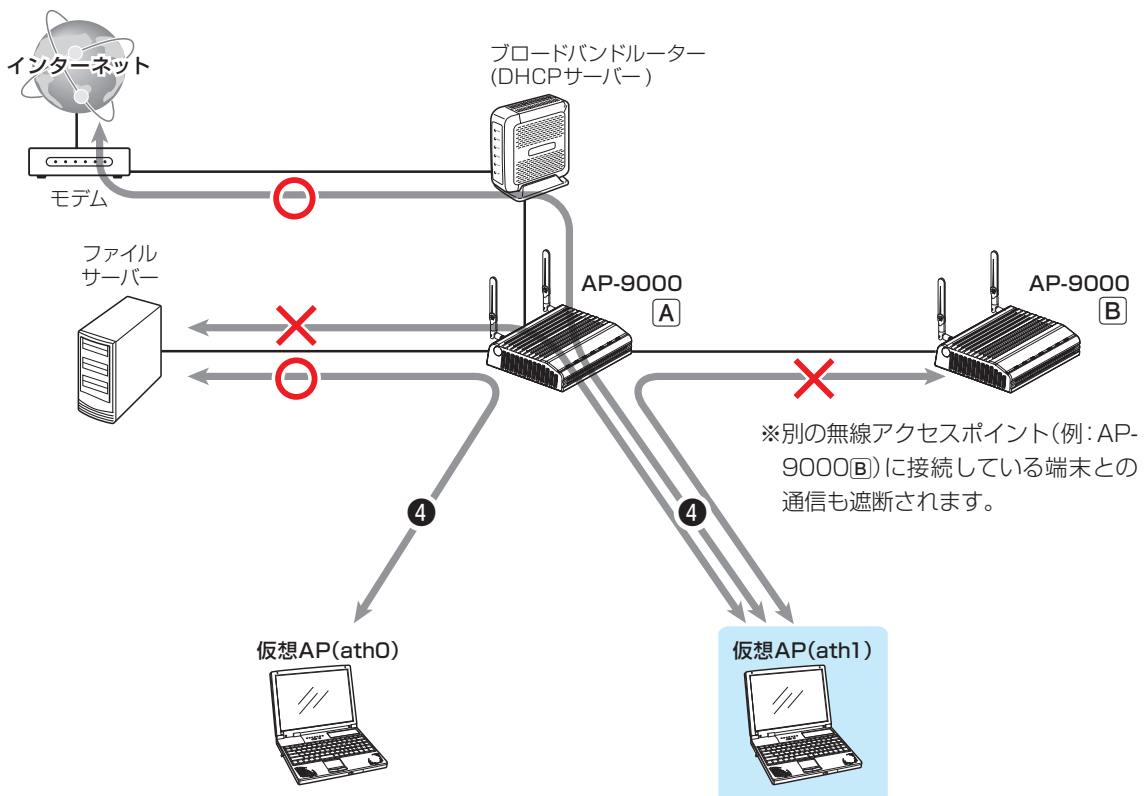
「パケットフィルター」画面で設定したブロードバンドルーターのLAN側のMACアドレスを表示

登録した上記のフィルターより大きな番号を表示

番号									
エントリ	有効								
ログを表示									
方法	透過								
送信元インターフェース	eth0								
宛先インターフェース	ath1								
送信元MACアドレス/マスク	00-90-C7-00-00-06	/FF-FF-FF-FF-FF-FF							
宛先MACアドレス/マスク	-								
VLAN ID	0								
Ethernetタイプ	すべて								
								編集	削除
番号									
エントリ	有効								
ログを表示									
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	ath1								
送信元MACアドレス/マスク	-								
宛先MACアドレス/マスク	-								
VLAN ID	0								
Ethernetタイプ	すべて								
								編集	削除

① ブロードバンドルーターから仮想AP(ath1)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(ath1)への通信を遮断



5 そのほかの機能について

6. Web認証機能を設定するには

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

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

※「基本」画面、「詳細」画面と併せて設定してください。

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

ネットワーク設定 > Web認証 > 基本

ネットワーク設定 > Web認証 > 詳細

■ Web認証ページを設定するときは

次の手順でWeb認証を有効にして、認証ページ、認証方法(例：RADIUSを優先)を設定します。

※無線1(2.4GHz帯)の仮想AP(例：ath0)を例に、説明しています。

- 1 「ネットワーク設定」メニューの「Web認証」、「基本」の順にクリックします。
- 2 [Web認証] 欄で「有効」を選択し、認証成功時に表示するページを設定します。

Web認証

インターフェース: ath0

Web認証: 無効 有効

ページタイトル: Set your page title.

ポータルサイト: http://www.example.com/

移動待ち時間: 5 秒

有効期限: 24時間

登録

① 選択する

② 設定する

③ クリック

端末が本製品に接続しているときの、Web認証の有効期限です。
有効期限を経過すると次のアクセスは制限され、再度認証する必要があります。
有効期限は、「5分/10分/15分/30分/1時間/2時間/4時間/8時間/12時間/24時間」から選択します。
(出荷時の設定：24時間)

- 3 「Web認証」の「詳細」をクリックします。
- 4 設定する仮想APの認証方法を選択し、対象となるRADIUSサーバーについて設定します。
※ご使用になるシステムによっては、出荷時の設定値とポート番号が異なることがありますのでご確認ください。
※[シークレット]欄は、RADIUSサーバーに設定された値と同じ設定にします。

Web認証方法

インターフェース: ath0

認証方法: RADIUSを優先

RADIUS設定

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

登録

① 選択する

② 設定する

③ クリック

(次ページにつづく)

5 そのほかの機能について

6. Web認証機能を設定するには

ネットワーク設定 > Web認証 > 基本

ネットワーク設定 > Web認証 > 詳細

■ Web認証ページを設定するときは(つづき)

5 Web認証にローカルリストを使用する場合のユーザー名とパスワードを128文字以内(任意の半角英数字/記号)で入力し、〈追加〉をクリックします。

※最大32件まで登録できます。

ローカルリスト	
ユーザー名	パスワード
<input type="text"/>	<input type="text"/>

6 〈再起動〉をクリックします。

再起動が必要な項目が変更されています。

Web認証方法

※表示される画面にしたがって、本製品を再起動します。

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

5 そのほかの機能について

6. Web認証機能を設定するには(つづき)

ネットワーク設定 > Web認証 > 基本

■ カスタムページの作成について

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

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

※カスタムページの上限は、8192バイト(8Kバイト)です。

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

カスタムページ			
ログインページ:	<input type="text"/>	<input type="button" value="参照..."/>	<input type="button" value="登録"/> <input type="button" value="プレビュー"/>
認証成功ページ:	<input type="text"/>	<input type="button" value="参照..."/>	<input type="button" value="登録"/> <input type="button" value="プレビュー"/>

【登録の手順】

1. <参照 ...>をクリックして、カスタムページ(拡張子: fmt)の保存先を指定します。

2. <登録>をクリックします。

<プレビュー>をクリックすると、登録したページを表示します。

※出荷時の状態にするときは、<初期状態に戻す>をクリックします。

【ご参考】

出荷時のWeb認証ページについて

◎ログインページの場合

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

◎認証成功ページの場合

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

5 そのほかの機能について

6. Web認証機能を設定するには

ネットワーク設定 > Web認証 > 基本

■ カスタムページの作成について(つづき)

下記サンプルページのソースを参考にカスタムページを作成してください。

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

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

◎ログインページの場合

@TITLE@	
@NOTICE@	
ユーザー名とパスワードを入力してください。	
ユーザー名	<input type="text"/>
パスワード	<input type="password"/>
<input type="button" value="ログイン"/>	<input type="button" value="取り消し"/>

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<!--
カスタムページの文字コードは必ずShift_JISで保存してください。Shift_JIS以外の文字コードには対応していません。
「@」は識別子として利用されるため、「@」そのものを表示したい場合は「@@」と2つつづけて記述してください。
-->
<meta http-equiv="Content-Type" content="text/html; charset=Shift_JIS">
<meta http-equiv="Content-Style-Type" content="text/css">
<meta http-equiv="Pragma" content="no-cache">
<style type="text/css">
<!--
body {
    text-align:    center;
}
table {
    margin-right:  auto;
    margin-left:  auto;
    padding:      8px;
    border:       1px solid;
    border-color: black;
    width:       auto;
}
td {
    vertical-align: top;
    white-space:  nowrap;
    border:       0px;
}
.main {
    text-align:   left;
}
.title {
    text-align:  center;
    margin:      8px;
}
.notice {
    text-align:  center;
```

(次ページにつづく)

5 そのほかの機能について

6. Web認証機能を設定するには

ネットワーク設定 > Web認証 > 基本

■ カスタムページの作成について

◎ログインページの場合(つづき)

```
margin:      8px;
color:      red;
}
.info {
text-align: center;
margin:      8px;
}
.center {
text-align: center;
}
.input {
width:      16em;
}
-->
</style>
<!-- @TITLE@の部分は設定画面にある「ページタイトル」に設定された内容に置き換わります。 -->
<title>@TITLE@</title>
</head>
<body>
<!-- フォームのactionやmethod必ず以下のフォーマットにしてください -->
<form action="@CGI_NAME@" target="_self" method="POST">
<div class="main">
<h1 class="title">@TITLE@</h1>
<div class="notice">
<!-- @NOTICE@の部分はログイン失敗時に表示するエラーメッセージに置き換わります -->
@NOTICE@
</div>
<div class="info">
ユーザー名とパスワードを入力してください。
</div>
<table>
<tr>
<td>ユーザー名</td>
<td>
<!-- ユーザー名は必ず以下のフォーマットにしてください -->
<input class="input" type="text" maxlength="31" name="user">
</td>
</tr>
<tr>
<td>パスワード</td>
<td>
<!-- パスワードは必ず以下のフォーマットにしてください -->
<input class="input" type="password" maxlength="31" name="pass">
</td>
</tr>
<tr>
<td></td>
<td>
<input type="submit" value="ログイン">
<input type="reset" value="取り消し">
</td>
</tr>
</table>
</div>
</form>
</body>
</html>
```

5 そのほかの機能について

6. Web認証機能を設定するには

ネットワーク設定 > Web認証 > 基本

■ カスタムページの作成について(つづき)

◎認証成功ページの場合

@TITLE@

認証に成功しました。
@WAIT_TIME@秒後にポータルサイトに移動します。
自動で移動しない場合は[こちら](#)をクリックしてください。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<!--
カスタムページの文字コードは必ずShift_JISで保存してください。Shift_JIS以外の文字コードには対応していません。
「@」は識別子として利用されるため、「@」そのものを表示したい場合は「@@」と2つづけて記述してください。
-->
<meta http-equiv="Content-Type" content="text/html; charset=Shift_JIS">
<meta http-equiv="Content-Style-Type" content="text/css">
<meta http-equiv="Pragma" content="no-cache">
<!--
@WAIT_TIME@, @PORTAL_SITE@の部分は設定画面にある次の設定項目に設定された内容に置き換わります。
@WAIT_TIME@ 移動待ち時間
@PORTAL_SITE@ ポータルサイト
-->
<meta http-equiv="Refresh" content="@WAIT_TIME@;URL=@PORTAL_SITE@">
<style type="text/css">
<!--
body {
text-align: center;
}
.main {
text-align: left;
}
.title {
text-align: center;
margin: 8px;
}
.info {
text-align: center;
margin: 8px;
}
-->
</style>
<!-- @TITLE@の部分は設定画面にある「ページタイトル」に設定された内容に置き換わります。 -->
<title>@TITLE@</title>
</head>
<body>
<div class="main">
<h1 class="title">@TITLE@</h1>
<div class="info">
認証に成功しました。<br>
@WAIT_TIME@秒後にポータルサイトに移動します。<br>
<br>
自動で移動しない場合は<a href="@PORTAL_SITE@">こちら</a>をクリックしてください。
</div>
</div>
</body>
</html>
```

5 そのほかの機能について

7. 「管理」画面について

管理 > 管理ツール

■ HTTP/HTTPS設定

HTTPとHTTPSは、WWWブラウザ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:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
HTTPポート番号:	<input type="text" value="80"/>
HTTPS:	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
HTTPSポート番号:	<input type="text" value="443"/>

① HTTP 本製品へのHTTPプロトコルによるアクセスの許可を設定します。
(出荷時の設定：有効)

② HTTPポート番号 本製品へのHTTPプロトコルによるアクセスのポート番号を設定します。
(出荷時の設定：80)

設定できる範囲は、「80」と「1024～65535」です。

そのほか、本製品が使用する一部のポートで利用できないものがあります。

※HTTPS、Telnet、SSHを使用時、これらに設定されたポート番号と重複しないように設定してください。

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。

5 そのほかの機能について

7. 「管理」画面について(つづき)

管理 > 管理ツール

■ HTTP/HTTPS設定後、設定画面にアクセスできなくなったときは

Telnet(P.8-6)で本製品(例：192.198.0.1)にアクセスして、AP-9000 #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。

- ① AP-9000 # **network http on** と入力し[Enter]キーを押します。
- ② AP-9000 # **save** と入力し[Enter]キーを押す。
- ③ AP-9000 # **restart** と入力し[Enter]キーを押す。
- ④ 本製品の再起動が完了したら、本製品の設定画面へのアクセスを確認します。



```
Telnet 192.168.0.1
admin:
Password:
AP-9000 # network http on
AP-9000 # save
AP-9000 # restart
```

5 そのほかの機能について

7. 「管理」画面について(つづき)

管理 > 管理ツール

■ Telnet/SSH設定

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

Telnet/SSH設定	
① Telnet:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
② Telnetポート番号:	<input type="text" value="23"/>
③ SSH:	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
④ SSHバージョン:	<input type="text" value="自動"/>
⑤ SSH認証方式:	<input type="text" value="自動"/>
⑥ SSHポート番号:	<input type="text" value="22"/>

- 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：有効)
- 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：無効)
※「有効」を選択して、[SSH認証方式] (⑤) 欄で、「自動」/「公開鍵認証」を選択すると、[SSH公開鍵管理] 項目と [SSH公開鍵登録状況] 項目を表示します。
※SSHを使用すると、Telnetクライアントプログラムを使用して設定する内容を暗号化して通信できます。
※SSHを使用するには、別途SSHクライアントをご用意ください。
- ④ **SSHバージョン** [SSH] (③) 欄で「有効」を設定したとき、本製品で使用するSSH機能のバージョンを設定します。
(出荷時の設定：自動)
◎1 : バージョン1を使用します。
◎2 : バージョン2を使用します。
◎自動 : 「バージョン1」と「バージョン2」を自動認識します。
- ⑤ **SSH認証方式** [SSH] (③) 欄で「有効」を設定したとき、本製品へのアクセスに対する認証方式を設定します。
(出荷時の設定：自動)
◎パスワード認証 : パスワードを使用して認証するときに設定します。
◎公開鍵認証 : 公開鍵を使用して認証するときに設定します。
◎自動 : 「パスワード認証」と「公開鍵認証」を自動認識します。

5 そのほかの機能について

7. 「管理」画面について

管理 > 管理ツール

■ Telnet/SSH設定(つづき)

Telnet/SSH設定	
① Telnet:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
② Telnetポート番号:	<input type="text" value="23"/>
③ SSH:	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
④ SSHバージョン:	<input type="text" value="自動"/> ▼
⑤ SSH認証方式:	<input type="text" value="自動"/> ▼
⑥ SSHポート番号:	<input type="text" value="22"/>

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

5 そのほかの機能について

7. 「管理」画面について(つづき)

管理 > 管理ツール

■ SSH公開鍵管理

SSHでアクセスするときに使用する公開鍵を登録します。

※[Telnet/SSH設定]項目の[SSH]欄を「有効」、[SSH認証方式]欄を「自動」/「公開鍵認証」に設定したとき表示される項目です。

※画面は、登録例です。

SSH公開鍵管理

公開鍵ファイル:
既存の公開鍵は上書きされます

SSH公開鍵登録状況

<pre>----- BEGIN SSH2 PUBLIC KEY ----- Comment: AAAAE3NzaC1yc2EAAAABJQAAAIBzCXkODIZUlaXyfmPR7KJEB2v2jcvpd/yJ6sDZ5 ----- END SSH2 PUBLIC KEY -----</pre>	<input type="button" value="削除"/> SSHv2 RFC4716 形式
--	---

公開鍵ファイル…………… 登録できる鍵は、1種類だけです。

【登録の手順】

1. <参照…>をクリックして、公開鍵ファイルの保存先を指定します。
2. <登録>をクリックします。

● [SSH公開鍵登録状況]項目に公開鍵の内容を表示します。

※公開鍵ファイルの登録を取り消すときは、[SSH公開鍵登録状況]項目の<削除>をクリックします。

5 そのほかの機能について

7. 「管理」画面について(つづき)

管理 > SYSLOG

■ SYSLOG設定

指定したホストにログ情報などを出力するための設定です。

SYSLOG設定

① DEBUG:	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
② INFO:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
③ NOTICE:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
④ ホストアドレス:	<input type="text"/>

- ① **DEBUG**…………… 各種デバッグ情報を出力する設定です。 (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 そのほかの機能について

7. 「管理」画面について(つづき)

管理 > SNMP

■ SNMP設定

TCP/IPネットワークにおいて、ネットワーク上の各ホストから本製品の情報を自動的に収集して、ネットワーク管理をするときの設定です。

SNMP設定

① SNMP: 無効 有効

② コミュニティID(GET): public

③ 場所:

④ 連絡先:

- 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、本製品の設定情報をSNMP管理ツール側で管理できません。
- 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。

5 そのほかの機能について

7. 「管理」画面について(つづき)

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)を差し込んで電源を接続したときは、USBメモリーとのアクセス(設定保存/設定復元/ファームウェアのバージョンアップ)が完了後、LED消灯モードになります。

※〈INIT〉ボタン、〈WSP〉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。

5 そのほかの機能について

7. 「管理」画面について(つづき)

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。

The screenshot shows a form titled "PINGテスト" with the following fields and a button:

- ① ホスト: [Empty text input field]
- ② 試行回数: [4] 回 (dropdown menu)
- ③ パケットサイズ: [64] バイト (dropdown menu)
- ④ タイムアウト時間: [1000] ミリ秒 (dropdown menu)
- ⑤ 実行 (Execute button)

- ① **ホスト** PINGを送出する対象ホストのアドレスを入力します。
- 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】

The screenshot shows the "PING結果" screen with the following text and buttons:

```
Pinging 192.168.0.103 (192.168.0.103) with 64 bytes of data:
Reply from 192.168.0.103 bytes=64 ttl=64 seq=0 time=5ms
Reply from 192.168.0.103 bytes=64 ttl=64 seq=1 time=5ms
Reply from 192.168.0.103 bytes=64 ttl=64 seq=2 time=5ms
Reply from 192.168.0.103 bytes=64 ttl=64 seq=3 time=5ms

--- 192.168.0.103 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005 ms
rtt min/avg/max = 5/5/5 ms
```

Buttons: 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。

5 そのほかの機能について

7. 「管理」画面について(つづき)

管理 > ネットワークテスト

■ 経路テスト

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

経路テスト

① ノード:

② 最大ホップ数:

③ タイムアウト時間: 秒

④ DNS名前解決: 無効 有効

⑤

- ① ノード 経路テストをする対象ノード(機器)のアドレスを入力します。
- 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

```
tracert to 192.168.100.1 (192.168.100.1) from 192.168.0.1, 16 hops max
 1:  5 ms  0 ms  0 ms  192.168.0.254
 2:  0 ms  5 ms  0 ms  192.168.68.1
 3:  5 ms  5 ms  0 ms
 4:  0 ms  5 ms  5 ms
 5:  5 ms  0 ms  0 ms  192.168.53.4
 6: 10 ms 10 ms 10 ms  192.168.100.3
 7: 10 ms  5 ms 10 ms  192.168.100.1
```

※上図は、表示例です。

◎〈保存〉をクリックすると、テスト結果をファイル(拡張子：txt)に保存します。

※ファイル名は、「tracert_[対象ノードのアドレス].txt」で保存されます。

◎〈実行画面に戻る〉をクリックすると、画面が「経路テスト」表示に戻ります。

8. 本製品のルーター機能を使用するには

本製品のルーター機能を使用するときは、ご契約の回線接続業者などから指定された回線種別を選択し、本製品の[WAN/LAN]ポートの用途を変更します。

※出荷時、本製品の[WAN/LAN]ポートは、LAN側接続用ポートとして、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を接続できるように設定されています。

ルーター設定 > WAN接続先

■ ご契約回線への接続方法を確認する

ご契約の接続業者またはプロバイダーからインターネットへの接続方法と設定内容が指定されます。

ご契約内容と併せてご覧になり、該当する接続方法と設定項目を確認してください。

DHCP方式での接続を指定された場合(P.5-30)

本製品のWAN側に設定するIPアドレスをプロバイダーから自動取得します。

固定IPアドレスでの接続を指定された場合(P.5-31)

本製品のWAN側に設定するIPアドレスがプロバイダーから指定されます。

PPPoE方式での接続を指定された場合(P.5-32)

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。

ルータータイプモデムを提供された場合

お使いのモデムがルータータイプモデムの場合は、本製品のルーター機能を使用しません。

本製品の回線種別を「LANポートとして使用する」(出荷時の設定)に設定すると、お使いのモデムと接続できます。

※LAN側IPアドレスなどの設定について、あらかじめモデムに付属する取扱説明書でご確認ください。

■ WAN側(有線LAN)を設定するときは

[回線種別]欄で「DHCPクライアント」、「PPPoE」を設定した場合、再起動後は、DHCPサーバーやPPPoEサーバーから本製品のWAN(有線LAN)側IPアドレスを取得するようになりますので、設定用パソコンを本製品のWAN(有線LAN)側に接続しても設定画面にアクセスできません。

※各仮想APのVLAN機能とルーター機能は併用できません。

ルーター機能をご使用になる AP-9000をRS-AP3で管理するときのご注意

◎管理を終了するまで、AP-9000のWAN側(ルーター設定)を変更できません。

◎ルーター機能使用時、AP-9000のWAN側から管理する場合には、回線種別を「固定IP」に設定し、管理を開始する前に、WAN側IPアドレスに固定IPアドレスを設定してください。

※回線種別を「DHCPクライアント」に設定してご使用になる場合は、DHCPサーバー側で静的DHCPサーバー機能などを利用し、常に同じIPアドレスが付与されるようにネットワーク環境を構築してください。

※回線種別が「PPPoE」に設定されているときは、AP-9000のWAN側から管理できません。

5 そのほかの機能について

8. 本製品のルーター機能を使用するには(つづき)

ルーター設定 > WAN接続先

■ DHCP方式での接続を指定された場合(DHCPクライアント)

回線を本製品のWAN側に接続し、ご契約の回線接続業者から本製品のWAN側IPアドレスを「DHCP」方式で取得する場合の設定です。

- 1 「ルーター」メニュー、「WAN接続先」の順にクリックします。
「WAN接続先」画面が表示されます。
- 2 [回線種別設定]項目で「DHCPクライアント」を選択し、〈登録〉をクリックします。
※出荷時や全設定初期化時、「LANポートとして使用する」に設定されています。

回線種別設定

回線種別:

① 選択する

回線設定

接続先名:

プライマリーDNSサーバー:

セカンダリーDNSサーバー:

登録

② クリック

- 3 〈再起動〉をクリックします。

再起動 再起動が必要な項目が変更されています。

クリック

回線状態表示

※表示される画面にしたがって、本製品を再起動します。

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

- 5 [接続状態]欄に、「接続中」と表示されたことを確認します。
※〈接続状態の更新〉をクリックしても「接続中」と表示されない場合は、設定や接続などをご確認ください。

回線状態表示

接続状態	接続中
回線種別	DHCPクライアント
DNSサーバー	
本体側のIPアドレス	
相手先のIPアドレス	
接続時間	0 days 00:00:55

確認する

回線種別設定

回線種別:

5 そのほかの機能について

8. 本製品のルーター機能を使用するには(つづき)

ルーター設定 > WAN接続先

■ 固定IPアドレスでの接続を指定された場合(固定IP)

回線を本製品のWAN側に接続し、ご契約の回線接続業者から本製品のWAN側に設定するIPアドレスが指定された場合の設定です。

- 1 「ルーター」メニュー、「WAN接続先」の順にクリックします。
「WAN接続先」画面が表示されます。
- 2 [回線種別設定]項目で「固定IP」を選択し、[回線設定]項目に指定された内容を設定して、〈登録〉をクリックします。
※出荷時や全設定初期化時、「LANポートとして使用する」に設定されています。

回線種別設定

回線種別: 固定IP

① 選択する

回線設定

接続先名:
IPアドレス:
サブネットマスク:
デフォルトゲートウェイ:
プライマリーDNSサーバー:
セカンダリーDNSサーバー:

登録

② 設定する

③ クリック

- 3 〈再起動〉をクリックします。

再起動 再起動が必要な項目が変更されています。

④ クリック

回線状態表示

※表示される画面にしたがって、本製品を再起動します。

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

- 5 [接続状態]欄に、「接続中」と表示されたことを確認します。
※「接続中」と表示されない場合は、設定や接続などをご確認ください。

回線状態表示

接続状態	接続中
回線種別	固定IP
DNSサーバー	
本体側のIPアドレス	
相手先のIPアドレス	
接続時間	0 days 00:08:15

⑤ 確認する

回線種別設定

回線種別: 固定IP

5 そのほかの機能について

8. 本製品のルーター機能を使用するには(つづき)

ルーター設定 > WAN接続先

■ PPPoE方式での接続を指定された場合(PPPoE)

回線を本製品のWAN側に接続し、ご契約の回線接続業者から本製品のWAN側IPアドレスを「PPPoE」方式で取得する場合の設定です。

- 1 「ルーター」メニュー、「WAN接続先」の順にクリックします。
「WAN接続先」画面が表示されます。
- 2 [回線種別設定]項目で「PPPoE」を選択し、[回線設定]項目に指定された内容を設定して、〈登録〉をクリックします。
※出荷時や全設定初期化時、「LANポートとして使用する」に設定されています。

回線種別設定

回線種別:

① 選択する

回線設定

接続先の選択:

接続先名:

ユーザーID:

パスワード:

接続方法:

IPアドレス:

プライマリーDNSサーバー:

セカンダリーDNSサーバー:

詳細設定

認証プロトコル:

MSS制限値:

ACネーム:

サービスネーム:

② 設定する

登録

③ クリック

接続先を追加するときは、〈▼〉をクリックして、「WAN01～WAN08」(最大8件まで設定可能)から選択します。(出荷時の設定: WAN01)
※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。

- 3 〈再起動〉をクリックします。

再起動 再起動が必要な項目が変更されています。

クリック

回線状態表示

※表示される画面にしたがって、本製品を再起動します。

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

(次ページにつづく)

5 そのほかの機能について

8. 本製品のルーター機能を使用するには

ルーター設定 > WAN接続先

■ PPPoE方式での接続を指定された場合(PPPoE)(つづき)

- 5 再起動後、接続先を選択して、〈接続〉をクリックします。
※回線接続中は、選択できません。

回線状態表示

接続先の選択	WAN01	接続
接続状態	未接続	
回線種別	PPPoE	
DNSサーバー		
本体側のIPアドレス		
相手先のIPアドレス		
接続時間		

① 選択する

② クリック

回線種別設定

回線種別: PPPoE

- 6 [接続状態]欄に、「接続中」と表示されたことを確認します。
※〈接続状態の更新〉をクリックしても「接続中」と表示されない場合は、設定や接続などをご確認ください。

回線状態表示

接続先の選択	WAN01	接続	接続状態の更新
接続状態	接続中		
回線種別	PPPoE		
DNSサーバー			
本体側のIPアドレス			
相手先のIPアドレス			
接続時間	0 days 00:03:15		

確認する

回線種別設定

回線種別: PPPoE

回線設定一覧について

本製品に追加されたPPPoE接続先を削除するときは、[回線設定一覧]項目の〈削除〉をクリックします。

回線設定一覧

接続先名	ユーザーID	接続方法	
WAN01		常時	削除

5 そのほかの機能について

8. 本製品のルーター機能を使用するには(つづき)

ルーター設定 > アドレス変換

■ アドレス変換設定

本製品のアドレス変換機能を設定します。

※[回線種別]を「DHCPクライアント」、「固定IP」、「PPPoE」に設定(P.5-29)したときに、有効になります。

アドレス変換設定

① アドレス変換: 無効 有効

DMZホスト設定

② DMZホスト IPアドレス:

① 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、本製品の静的マスカレード機能を使用して、指定した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。

② 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)側から発信されたすべてのIPフレームを、LAN側に存在する特定IPアドレスへ転送できます。
転送することにより、本製品のLAN側に存在する端末でWWWサーバーを運用したり、ネットワーク対戦ゲームなどができたりしますが、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ーが低下しますので、ご使用には十分ご注意ください。
※DMZホスト機能を静的マスカレードテーブルと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。
※セキュリティー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。

5 そのほかの機能について

8. 本製品のルーター機能を使用するには(つづき)

ルーター設定 > アドレス変換

■ 静的マスカレードテーブル設定

静的にIPマスカレード変換をするための設定です。

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

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

- ① WAN側ポート 選択したプロトコル(④)に対するWAN側ポートを数字で指定するときは、「指定」を選択します。
数字で指定しない場合は、ニーモニック(DNS、Finger、FTP、Gopher、NEWS、POP3、SMTP、TELNET、Web、Whois)から選択します。
- ② LAN側IP 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WAN側ポートを数字で指定するときは、「指定」を選択します。
数字で指定しない場合は、ニーモニック(DNS、Finger、FTP、Gopher、NEWS、POP3、SMTP、TELNET、Web、Whois)から選択します。
- ④ プロトコル TCP、UDP、TCP/UDP、GRE、ESPから選択します。
- ⑤ 〈追加〉 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。
※ [現在の登録]項目で、〈編集〉をクリックしたときは、〈更新〉を表示します。

5 そのほかの機能について

8. 本製品のルーター機能を使用するには(つづき)

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。

WAN側ポート	LAN側IP	LAN側ポート	プロトコル	①	②
Web	192.168.0.10	Web	TCP	編集	削除
22	192.168.0.10	8022	TCP	編集	削除

※画面の値は、登録例です。

- 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]項目に表示します。
- 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。

5 そのほかの機能について

8. 本製品のルーター機能を使用するには(つづき)

ルーター設定 > IPフィルター

■ IPフィルターについて

「IPフィルター」画面の「IPフィルター設定一覧」項目で、登録されているIPフィルターを確認できます。
 ※登録しても使用しないときは、「IPフィルター設定」項目の「エントリー」欄で「無効」を選択してください。

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

- ◎1番 : 受信するパケットをすべて遮断する
- ◎2番 : 送信するパケット、およびそれに対する応答パケットをすべて通過する
- ◎58番 : FTPを通過させる
- ◎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、またはファイル共有機能による外部への情報漏えいを防止

※「*」は、各欄で設定できる「すべて」を対象としています。

※2番以外は、「無効」に設定されています。

番号	フィルター方法	インターフェース	送信元IPアドレス (送信元ポート番号)	SPI	
	フィルター方向	プロトコル	宛先IPアドレス (宛先ポート番号)	フィルター合致時 SYSLOGに出力	
1	遮断	すべて	* (*)	無効	編集 削除
	IN	すべて	* (*)	検索を継続 無効	
2	透過	すべて	* (*)	有効	編集 削除
	OUT	すべて	* (*)	検索を継続 無効	
58	透過	すべて	* (20)	無効	編集 削除
	IN	TCP (フラグ指定なし)	* (*)	検索を継続 無効	
59	遮断	すべて	* (135)	無効	編集 削除
	OUT	TCP/UDP	* (*)	検索を継続 無効	
60	遮断	すべて	* (*)	無効	編集 削除
				検索を継続	
63	遮断	すべて	* (*)	無効	編集 削除
	OUT	TCP (フラグ指定なし)	* (137-139)	検索を継続 無効	
64	遮断	すべて	* (137-139)	無効	編集 削除
	OUT	UDP	* (137-139)	検索を継続 無効	

9. ポートベースVLAN機能を設定するには

ネットワーク設定 > LAN側IP

ネットワーク設定 > ポートベースVLAN

■ ポートベースVLANを設定するときは

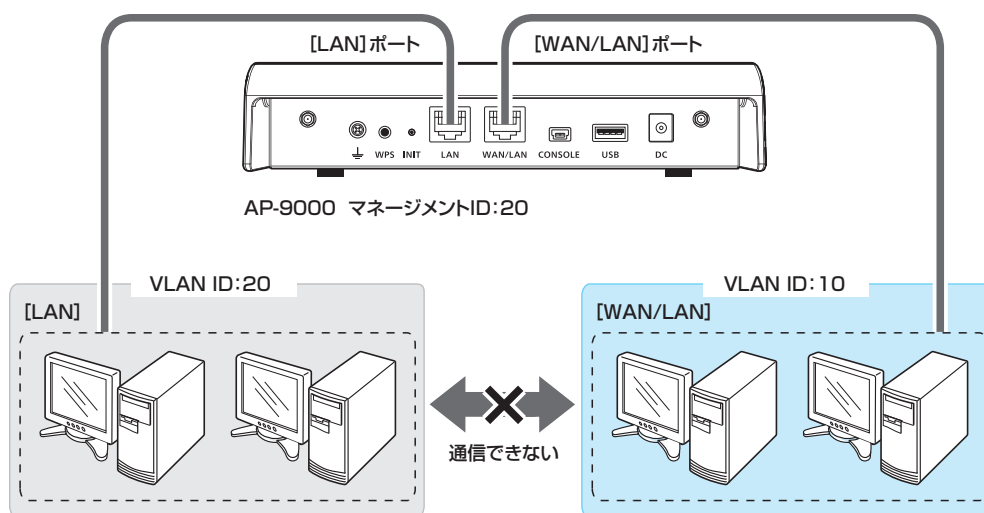
ポートベースVLAN機能を設定すると、本製品の[WAN/LAN]ポート、[LAN]ポートを論理的に複数のVLANグループに分割できます。

異なるVLANグループ間の通信を遮断できますので、セキュリティの向上やネットワークの負荷を軽減できます。

※使用条件については、「ポートベースVLAN機能について」(P.1-17)をご覧ください。

[WAN/LAN]ポートをトランキングポートとして使用する場合は、本書5-40ページをご覧ください。

※本製品の回線種別を「LANポートとして使用する」(出荷時の設定)を設定しているときだけ使用できる機能です。



本製品のポートごとに設定されたVLAN IDによって、本製品と接続された有線LAN端末を「VLAN ID：10」と「VLAN ID：20」のグループに分割した場合(上図)を例に説明します。

※操作手順は、次ページで説明しています。

設定例) 「LAN側IP」画面→「VLAN設定」項目

「管理ID」欄：「20」(設定変更後、本製品の設定画面へのアクセス用)

「ポートベースVLAN」画面→「ポートベースVLAN設定」項目

「ポートベースVLAN機能」欄：「有効」

「ポートベースVLAN」画面→「ポート個別設定」項目

[VLAN ID]欄 [eth0]([LAN]ポート) : 「20」

[eth1]([WAN/LAN]ポート) : 「10」

(次ページにつづく)

5 そのほかの機能について

9. ポートベースVLAN機能を設定するには(つづき)

ネットワーク設定 > LAN側IP

ネットワーク設定 > ポートベースVLAN

■ ポートベースVLANを設定するときは(つづき)

- 1 「ネットワーク」メニュー、「LAN側IP」の順にクリックします。
「LAN側IP」画面が表示されます。

- 2 [VLAN設定]項目で、マネージメントIDを設定し、〈登録〉をクリックします。

本体名称
本体名称: AP-9000

VLAN設定
マネージメントID: 20

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

- 3 「ネットワーク」メニューの「ポートベースVLAN」の順にクリックします。
「ポートベースVLAN」画面が表示されます。

- 4 [ポートベースVLAN機能]欄で「有効」を選択し、下記のようにポートごとのVLAN IDを設定します。

ポートベースVLAN設定
ポートベースVLAN機能: 無効 有効

ポート個別設定

LANポート	トランキングポート	VLAN ID
eth0		20
eth1	<input type="checkbox"/>	10

eth0は[LAN]ポート、eth1は[WAN/LAN]ポートを示しています。

登録

- 5 〈再起動〉をクリックします。

再起動 再起動が必要な項目が変更されています。

再起動

ポートベースVLAN設定

※表示される画面にしたがって、本製品を再起動します。

※再起動完了後、本製品の設定画面へのアクセスできるのは、マネージメントID(例：20)と同じVLAN ID(例：20)が設定された[LAN]ポートに接続するパソコンだけになります。

5 そのほかの機能について

9. ポートベースVLAN機能を設定するには(つづき)

ネットワーク設定 > LAN側IP

ネットワーク設定 > ポートベースVLAN

■ トランキングポートを設定するには

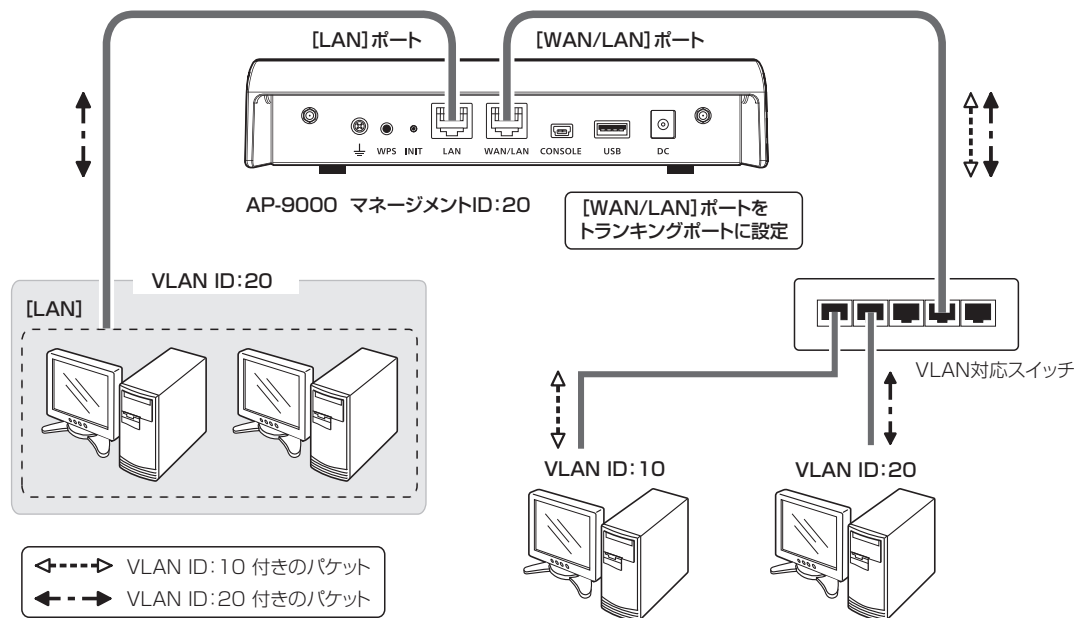
本製品の[WAN/LAN]ポートをトランキングポートに設定するための手順を説明します。

※使用条件については、「ポートベースVLAN機能について」(P.1-17)をご覧ください。

[WAN/LAN]ポート、[LAN]ポートを論理的に2つのVLANグループに分割する場合の設定手順は、本書5-38ページをご覧ください。

※設定すると、IEEE802.1QのVLAN規格に準拠したタギングポートとなります。

※本製品の回線種別を「LANポートとして使用する」(出荷時の設定)以外に設定している場合は、使用できません。



本製品のポートベースVLAN機能により、[WAN/LAN]ポートからのVLANタグ付きのパケットを分割した場合(上図)を例に説明します。

※操作手順は、次ページで説明しています。

設定例) 「LAN側IP」画面→「VLAN設定」項目

「マネージメントID」欄 : 「20」(設定変更後、本製品の設定画面へのアクセス用)

「ポートベースVLAN」画面→「ポートベースVLAN設定」項目

「ポートベースVLAN機能」欄 : 「有効」

「ポートベースVLAN」画面→「ポート個別設定」項目

「VLAN ID」欄 [eth0] ([LAN]ポート) : 「20」

「トランキングポート」欄 [eth1] ([WAN/LAN]ポート) : (チェックマークを入れる)

(次ページにつづく)

5 そのほかの機能について

9. ポートベースVLAN機能を設定するには(つづき)

ネットワーク設定 > LAN側IP

ネットワーク設定 > ポートベースVLAN

■ トランキングポートを設定するには(つづき)

- 1 「ネットワーク」メニュー、「LAN側IP」の順にクリックします。
「LAN側IP」画面が表示されます。

- 2 [VLAN設定]項目で、マネージメントIDを設定し、〈登録〉をクリックします。

本体名称
本体名称: AP-9000

VLAN設定
マネージメントID: 20

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

- 3 「ネットワーク」メニューの「ポートベースVLAN」の順にクリックします。
「ポートベースVLAN」画面が表示されます。

- 4 [ポートベースVLAN機能]欄で「有効」を選択し、下記のようにトランキングポート(eth1)とVLAN ID(eth0)を設定します。

ポートベースVLAN設定
ポートベースVLAN機能: 無効 有効

ポート個別設定

LANポート	トランキングポート	VLAN ID
eth0	<input type="checkbox"/>	20
eth1	<input checked="" type="checkbox"/>	

eth0は[LAN]ポート、eth1は[WAN/LAN]ポートを示しています。

登録 取消

- 5 〈再起動〉をクリックします。

再起動 再起動が必要な項目が変更されています。

再起動

※表示される画面にしたがって、本製品を再起動します。

※再起動完了後、本製品の設定画面へのアクセスできるのは、マネージメントID(例:20)と同じVLAN ID(例:20)が設定されたポートに接続するパソコンだけになります。

10. POPCHAT@Cloud連携機能を設定するときは

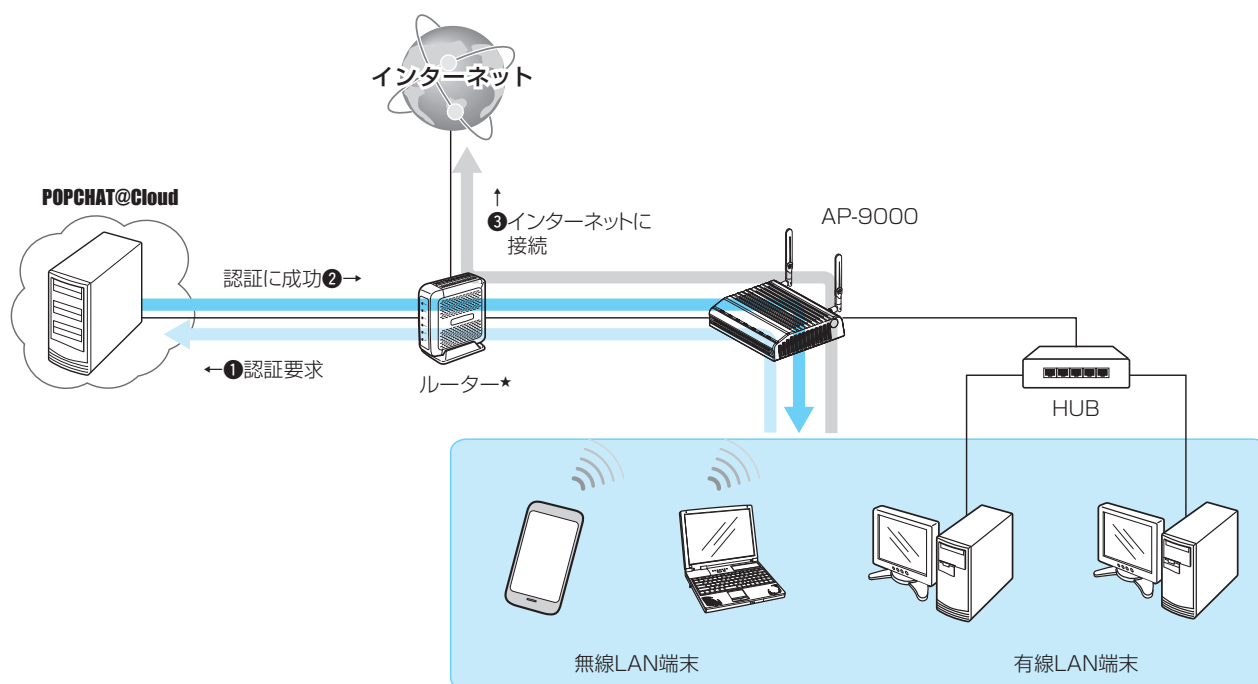
POPCHAT@Cloudのアカウント情報などを本製品に設定すると、端末が本製品に接続し、WWWブラウザで任意のサイトにアクセスしたとき、Wi-Fi認証@クラウドの認証ページが表示されます。

表示されたページにしたがって必要事項を入力し、認証されると無線LAN端末がインターネットにアクセスできます。
※本機能を設定する前に契約が必要です。

詳しくは、弊社営業窓口にお問い合わせください。

※POPCHAT@Cloud連携機能はインターフェース(eth0、ath0～ath15)ごとに設定できます。

※本機能を使用するには、インターネットへの接続環境と本製品へのDNS設定、デフォルトゲートウェイの設定が必要です。



★本製品のルーター機能を使用する場合、ルーターは不要です。

5 そのほかの機能について

10. POPCHAT@Cloud連携機能を設定するときは(つづき)

ネットワーク設定 > POPCHAT@Cloud

■ POPCHAT@Cloud連携機能を設定するときは

次の手順でPOPCHAT@Cloudのアカウント情報を入力し、使用するインターフェースを設定します。

※無線1(2.4GHz帯)の仮想AP(例: ath0)を例に、説明しています。

1 「ネットワーク設定」メニュー、「POPCHAT@Cloud」の順にクリックします。

2 [アカウント設定]項目に指定された内容を入力します。
※アカウント設定は、すべてのインターフェース間で共通の設定です。

アカウント設定

アプリケーションID:

秘密鍵:

認証サーバーURL:

入力する

3 使用するインターフェースを選択し、Wi-Fi認証@クラウドを「有効」に設定します。
※出荷時、[ゲートウェイID]欄は「本体MACアドレスを使用」に設定されています。
ゲートウェイIDが指定された場合は、「指定」を選択し、指定されたゲートウェイIDを右の欄に入力してください。

インターフェース設定

インターフェース: ath0

Wi-Fi認証@クラウド: 無効 有効

ゲートウェイID: 本体MACアドレスを使用

登録 取消

① 選択する

② 選択する

③ 設定する

④ クリック

4 <再起動>をクリックします。

再起動 再起動が必要な項目が変更されています。

アカウント設定

クリック

※表示される画面にしたがって、本製品を再起動します。

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

この章では、

本製品の設定内容保存や初期化、ファームウェアのバージョンアップをする手順について説明しています。

1. 設定内容の確認または保存	6-2
2. 保存された設定の書き込み(復元)	6-3
3. 設定を出荷時の状態に戻すには	6-4
A) <INIT>ボタンを使用する	6-4
B) 設定画面を使用する	6-5
4. ファームウェアをバージョンアップする	6-6
■ ファームウェアについて	6-6
■ バージョンアップについてのご注意	6-6
A) ファイルを指定して更新する	6-7
B) オンラインバージョンアップ	6-8
5. USBメモリーによる自動設定機能について	6-10
■ USBメモリー使用時のご注意	6-11
■ 対応するUSBメモリーの規格	6-11
■ 自動設定に使用するファイル名の付けかた	6-12
■ 自動バックアップされる設定ファイルについて	6-12
■ 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	6-13
6. USBメモリーから自動で設定を復元するには	6-14
■ 設定ファイルを保存して復元するまでの手順	6-14
7. USBメモリーからファームウェアをバージョンアップするには	6-17
■ バージョンアップするまでの手順	6-17
8. USBメモリー用の認証キーを設定するには	6-19
■ 設定のしかた	6-19

6 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、またはUSBメモリーに保存できます。

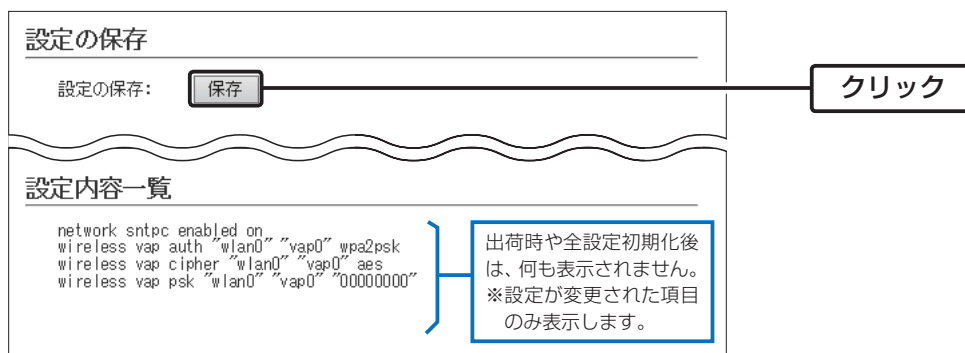
※保存した設定ファイル(拡張子:sav)は、本製品以外の製品では使用できません。

※設定を保存しておく、と、誤って設定内容が失われたときなどに利用できます。

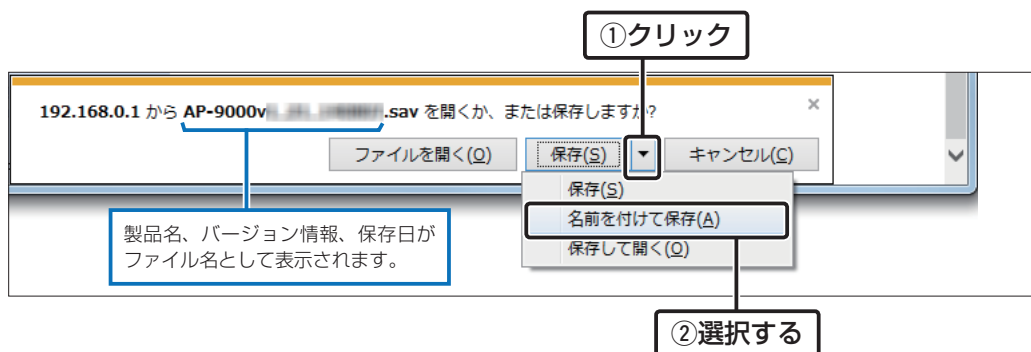
※設定ファイルをUSBメモリー(市販品)に保存して、本製品に書き込むこともできます。(P.6-14)

- 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」欄の〈保存〉をクリックします。
ファイルの確認画面(別画面)が表示されます。



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



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

6 保守について

2. 保存された設定の書き込み(復元)

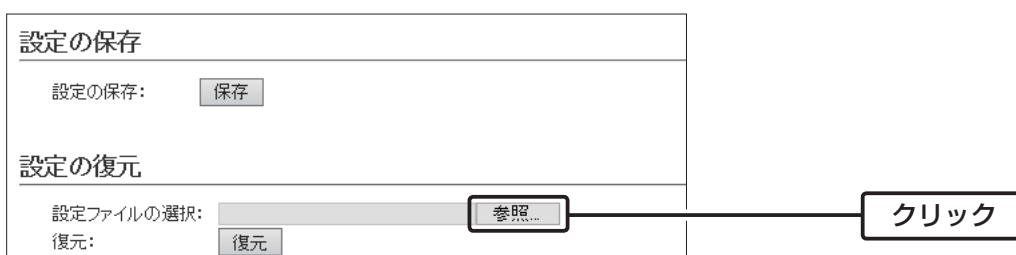
管理 > 設定の保存/復元

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.6-2)を本製品に書き込む手順を説明します。

※設定ファイルをUSBメモリー(市販品)に保存して、本製品に書き込むこともできます。(P.6-14)

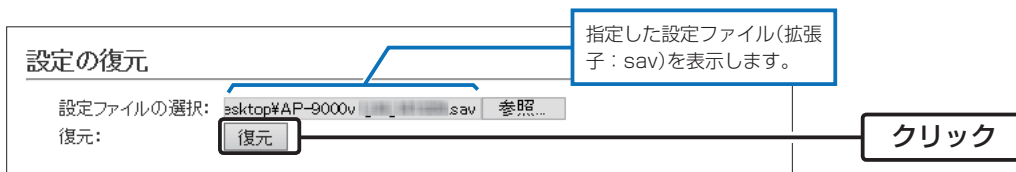
- 1 「管理」メニュー、「設定の保存/復元」の順にクリックします。
「設定の保存/復元」画面が表示されます。

- 2 設定ファイルを指定するため、〈参照...〉をクリックします。
「アップロードするファイルの選択」画面(別画面)が表示されます。



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

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



設定ファイルについてのご注意

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

6 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。

A) <INIT>ボタンを使用する

本製品に設定されたIPアドレスと管理者パスワードが不明な場合など、設定画面にアクセスできないとき

B) 設定画面を使用する(P.6-5)

A) <INIT>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、電源を入れます。

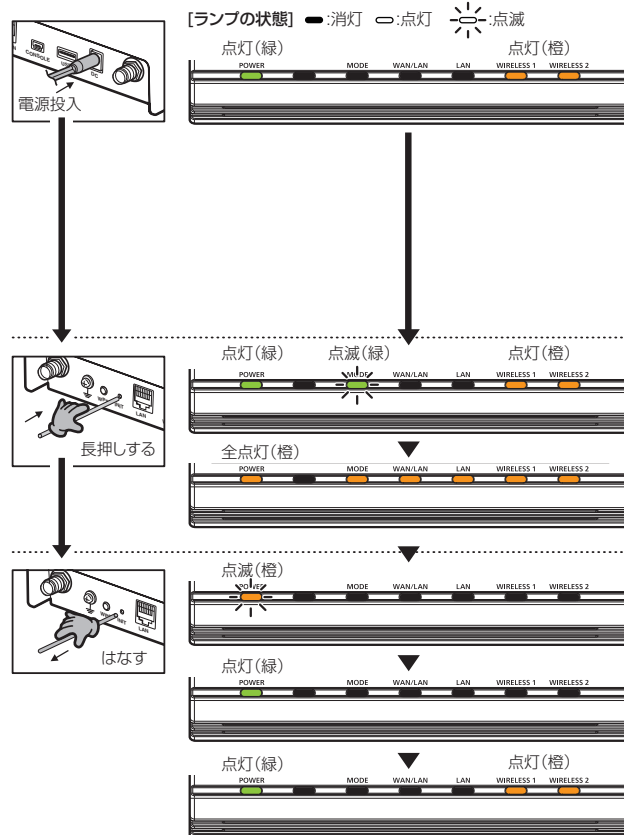
※[POWER]ランプと[WIRELESS](1/2)ランプの点灯を確認してから、手順2の操作を開始してください。

※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、<INIT>ボタンを押します。

3 すべてのランプが●橙点灯したら、<INIT>ボタンから手をはなします。

※[WIRELESS](1/2)ランプが●橙点灯すると、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。

6 保守について

3. 設定を出荷時の状態に戻すには(つづき)

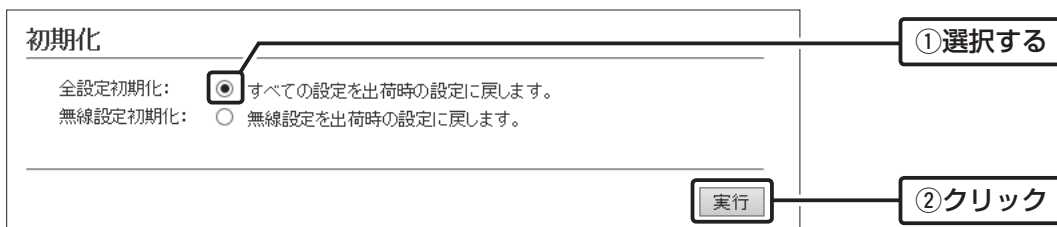
管理 > 初期化

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。

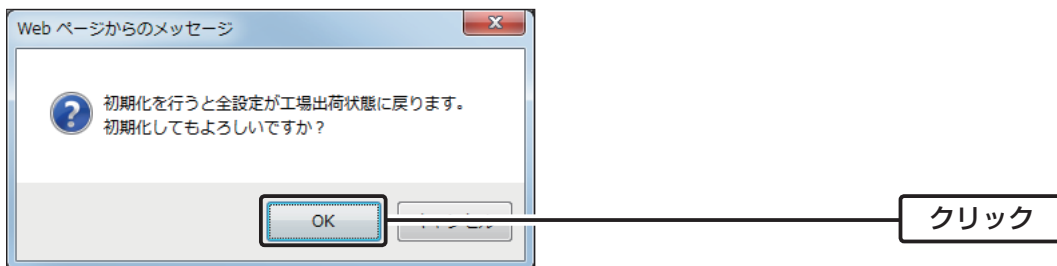
IPアドレスと管理者パスワードが不明な場合などの初期化については、本書6-4ページをご覧ください。

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

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

「無線設定」メニューで設定した内容だけを出荷時の状態に戻します。

初期化すると、本製品のSSIDは「WIRELESSLAN-0」、暗号化設定は「なし」(出荷時の設定)になります。

初期化実行後、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、「無線設定」メニュー、および無線LAN端末の設定を変更してください。

6 保守について

4. ファームウェアをバージョンアップする

本製品の設定画面からファームウェアをバージョンアップできます。

A ファイルを指定して更新する

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

B オンラインバージョンアップ(P.6-8)

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。

※ ファームウェアファイルをUSBメモリー(市販品)に保存して、本製品をバージョンアップすることもできます。(P.6-17)

TOP

■ ファームウェアについて

ファームウェアは、本製品を動作させるために、出荷時から本製品のフラッシュメモリーに書き込まれているプログラムです。

このプログラムは、機能の拡張や改良のため、バージョンアップをすることがあります。

バージョンアップの作業をする前に、本製品の設定画面にアクセスして、「TOP」画面に表示されるバージョン情報を確認してください。

バージョンアップをすると、機能の追加など、本製品を最良の状態にできます。

製品情報	
本体名称	AP-9000
IPL	Rev. 1
バージョン	Ver. 1.00 Copyright © 2008 Icom Inc.
国名コード	JP
WAN/LAN MACアドレス	00-90-C7-■■■■■■■■
LAN MACアドレス	00-90-C7-■■■■■■■■
無線1 MACアドレス	00-90-C7-■■■■■■■■
無線2 MACアドレス	00-90-C7-■■■■■■■■

バージョン情報

■ バージョンアップについてのご注意

◎ ファームウェアの更新中は、絶対に本製品の電源を切らないでください。

更新中に電源を切ると、データの消失や故障の原因になります。

◎ ご使用のパソコンでファイアウォール機能が動作していると、バージョンアップできないことがあります。

バージョンアップできない場合は、ファイアウォール機能を無効にしてください。

◆ バージョンアップの結果については、自己責任の範囲となります。

次に示す内容をよくお読みになってから、弊社ホームページ <http://www.icom.co.jp/> より提供される本製品のアップデート用ファームウェアファイルをご使用ください。

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

6 保守について

4. ファームウェアをバージョンアップする(つづき)

管理 > ファームウェアの更新

A ファイルを指定して更新する

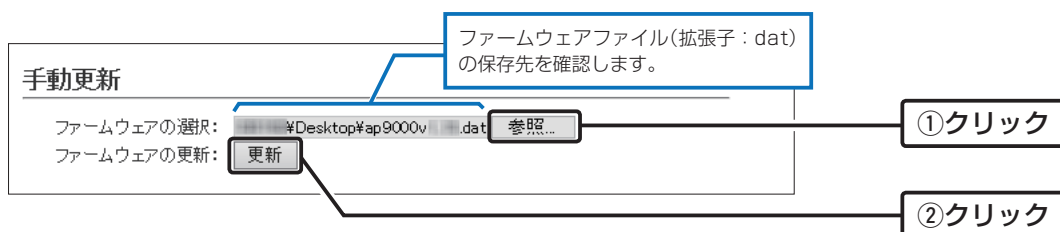
バージョンアップの前に、現在の設定内容を保存されることをおすすめします。(P.6-2)

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

※日常、管理者以外の端末からバージョンアップできないように、設定画面へのアクセス制限の設定(P.5-2)をおすすめします。

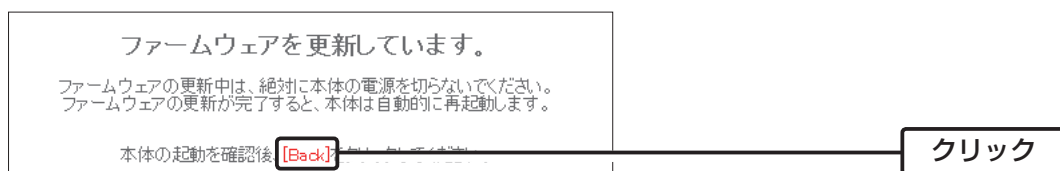
1 「管理」メニュー、「ファームウェアの更新」の順にクリックします。
「ファームウェアの更新」画面が表示されます。

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



3 更新完了後、[Back]と表示された文字の上にマウスポインターを移動してクリックすると、設定画面に戻ります。

設定画面に戻らないときは、ファームウェアの更新中ですので、しばらくしてから再度クリックしてください。
(接続するパソコンや本製品の電源は、絶対に切らないでください。)



ご注意

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

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

その場合は、接続するパソコンのIPアドレスを「例: 192.168.0.100」に設定してから、本製品の設定画面「192.168.0.1」にアクセスしなおしてください。

6 保守について

4. ファームウェアをバージョンアップする(つづき)

管理 > ファームウェアの更新

㊦ オンラインバージョンアップ

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

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

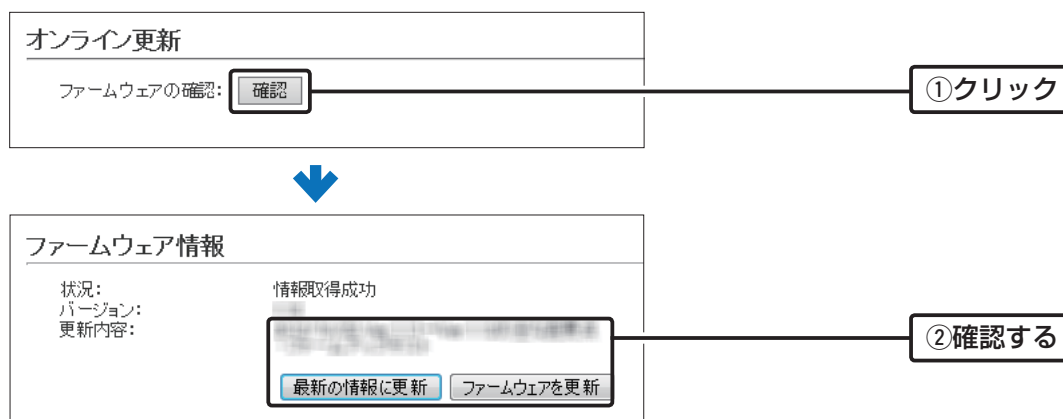
※ バージョンアップの前に、現在の設定内容を保存されることをおすすめします。(P.6-2)

1 「管理」メニュー、「ファームウェアの更新」の順にクリックします。

「ファームウェアの更新」画面が表示されます。

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

※「新しいファームウェアはありません。」が表示され、[MODE]ランプが● 橙点灯していないときは、バージョンアップは必要ありません。



3 <ファームウェアを更新>をクリックします。

弊社のアップデート管理サーバーにアクセスを開始します。

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

4 更新が完了するまで、そのまま数分程度お待ちください。

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

ファームウェア更新中は絶対に本体の電源を切らないでください。
ファームウェア更新中はブラウザを閉じず、そのままお待ちください。
ファームウェアの更新が完了すると、本体は自動で再起動します。

6 保守について

4. ファームウェアをバージョンアップする

管理 > ファームウェアの更新

⑧ オンラインバージョンアップ(つづき)

自動更新機能有効時の通知機能について

本製品の自動更新機能が「有効」に設定されている場合は、オンラインで新しいファームウェアを検知したときに、[MODE]ランプが● 橙点灯します。ご都合のよいときに、6-8ページの手順でファームウェアの更新をしてください。

※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」(出荷時の設定：有効)に設定してください。

自動更新

自動更新: 無効 有効

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)を接続して電源を入れると、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「WAN/LAN MACアドレス」(P.vi、P.6-6)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バージョンアップができます。※操作方法については、本書6-14ページ～6-20ページをご覧ください。

ご参考に

「管理」メニューの「管理ツール」画面で、[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。

◎ 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、ファームウェアをバージョンアップします。

◎ 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。

USB設定

USBメモリー:	<input type="radio"/> 無効 <input checked="" type="radio"/> 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:	<input style="width: 100%;" type="text"/>	
USB認証キーの書き込み:	<input type="button" value="書き込み"/>	

(※画面の内容は、出荷時の設定です。)

(次ページにつづく)

6 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(つづき)

■ 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、セキュリティー対応型の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、必ず本製品の電源を切ってから、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、ファームウェアのバージョンアップを使用する場合など、USBメモリーにアクセス中([POWER]ランプ ● 橙点灯中)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メモリーにアクセス中は、[POWER]ランプが ● 橙点灯します。
設定復元が完了すると、[POWER]ランプが ● 緑点灯に切り替わります。
ファームウェアのバージョンアップ中は、すべてのランプが橙色で点灯します。
- ◎ 本製品の設定画面でUSB認証キーが設定(P.6-20)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より古い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、ファームウェアのバージョンアップ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 : USB2.0/1.1 (USB3.0接続時は、USB2.0で動作します。)

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。

(次ページにつづく)

6 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(つづき)

■ 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.6-2)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。

※ファームウェアの自動バージョンアップ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。

(次ページにつづく)

6 保守について

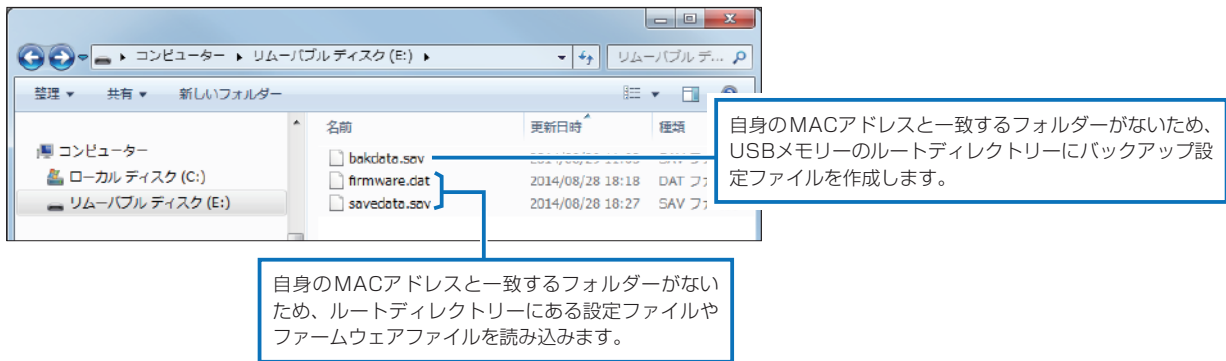
5. USBメモリーによる自動設定機能について(つづき)

■ 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

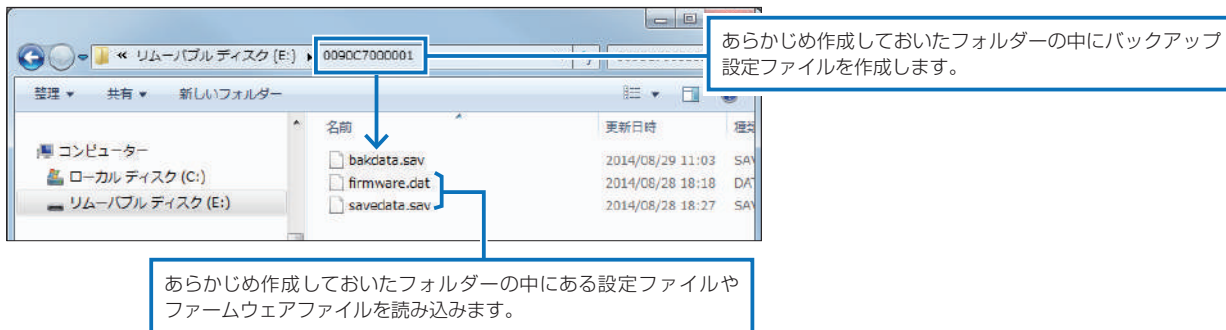
1つのUSBメモリーを使用して、本製品(複数台分)の設定復元やファームウェアのバージョンアップをするときは、あらかじめ、「TOP」画面に表示されている「WAN/LAN MACアドレス」(P.6-6)をフォルダー名[★]とするフォルダーを作成し、そのフォルダーに本製品の設定ファイルやファームウェアファイルを保存しておく必要があります。

★全角のフォルダー名は使用できません。

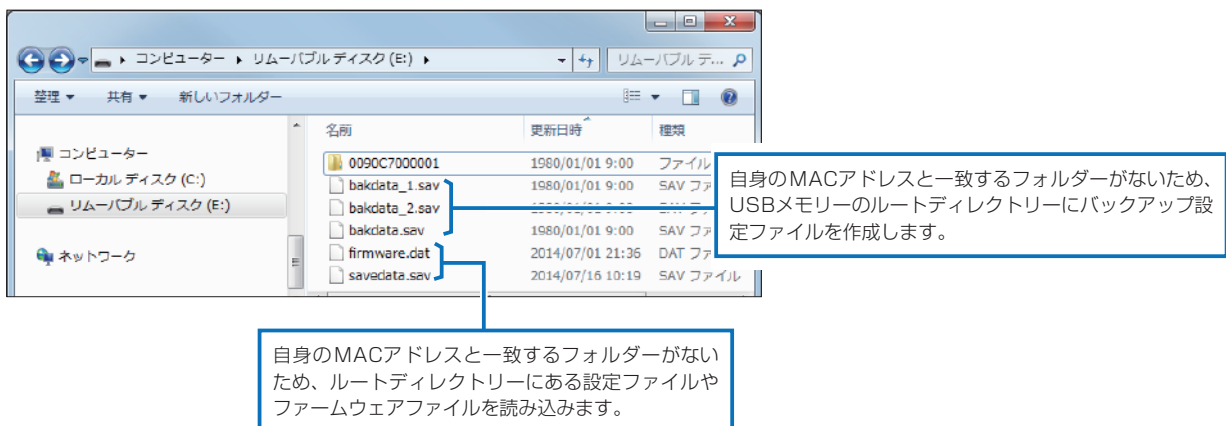
ルートディレクトリーにフォルダーがないとき



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



(次ページにつづく)

6 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

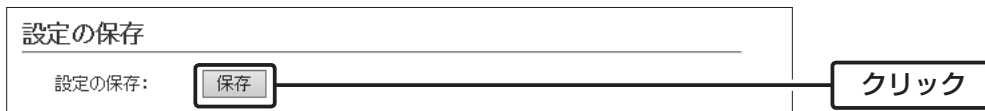
管理 > 設定の保存/復元

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。

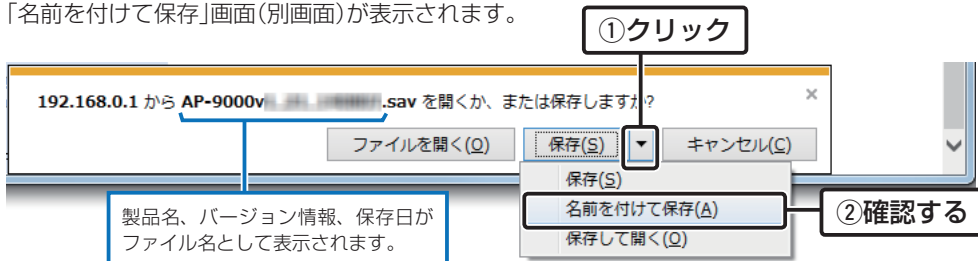
※ 使用条件については、「USBメモリーによる自動設定機能について」(P.6-12)をご覧ください。

■ 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.2-7)
- 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。
ファイルの確認画面(別画面)が表示されます。



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



- 6 「名前を付けて保存」(別画面)画面で、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)

6 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

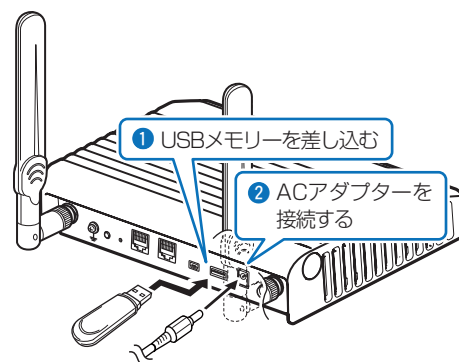
■ 設定ファイルを保存して復元するまでの手順(つづき)

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。

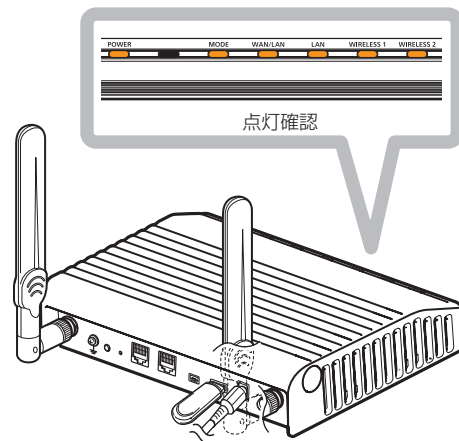
9 本製品の電源を切ります。

10 savedata.savが保存されたUSBメモリーを本製品の
[USB]ポートに差し込んでから、本製品の電源を入れます。



11 [POWER]ランプが●緑点灯後、約10秒経過すると、USBメモリーへのアクセスを開始します。
アクセス(設定の復元)中は、すべてのランプが●橙点灯します。

【ご注意】 設定復元(アクセス)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。



(次ページにつづく)

6 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

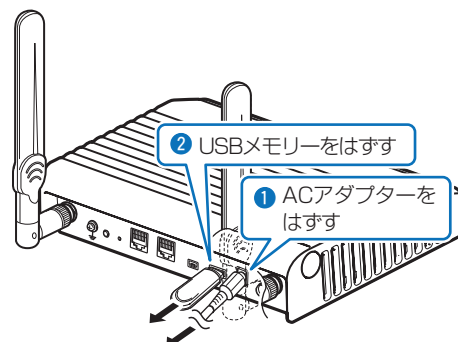
管理 > 設定の保存/復元

■ 設定ファイルを保存して復元するまでの手順(つづき)

12 すべてのランプが消灯し、本製品が再起動します。
起動中、[POWER]ランプが \odot 橙点滅から \bullet 緑点灯に切り替わったことを確認してから本製品の電源を切ります。
最後に、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】 データ保護のため、必ず本製品の電源を切ってから、USBメモリーを取りはずしてください。



ご参考に

「管理」メニューの「管理ツール」画面で、[USBメモリー]欄(P.6-10)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。

6 保守について

7. USBメモリーからファームウェアをバージョンアップするには

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バージョンアップ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.6-11)をご覧ください。

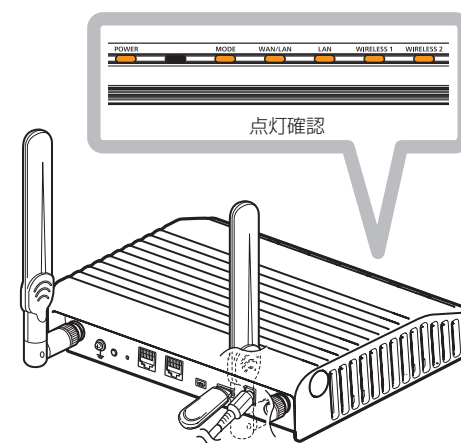
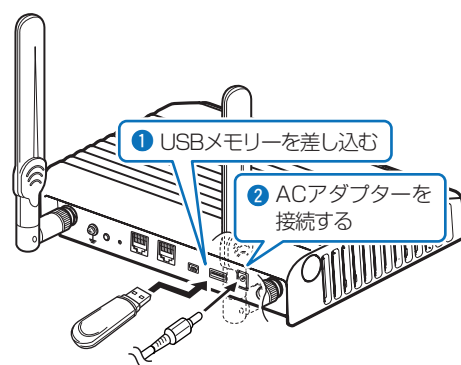
※バージョンアップの前に、「バージョンアップについてのご注意」(P.6-6)をご覧ください。

■ バージョンアップするまでの手順

- 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メモリーからのバージョンアップに使用できません。
- 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 バージョンアップする本製品を用意します。
- 7 本製品の電源を切り、本製品に接続するすべての機器を取りはずします。
- 8 firmware.datが保存されたUSBメモリーを本製品の[USB]ポートに差し込んでから、本製品の電源を入れます。

- 9 [POWER]ランプが●緑点灯後、約10秒経過すると、USBメモリーへのアクセスが開始されます。
アクセス中は、[POWER]ランプが●橙点灯します。
※ファームウェアのバージョンアップ中は、すべてのランプが●橙点灯します。



【ご注意】 ファームウェアのバージョンアップが完了するまで、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。
バージョンアップ中に、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。



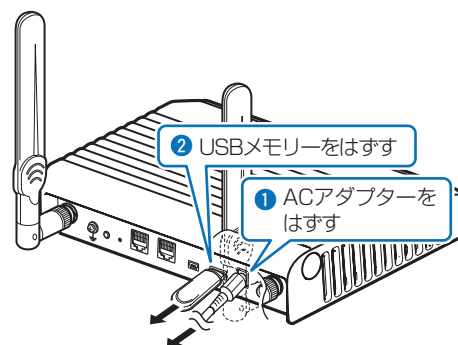
6 保守について

7. USBメモリーからファームウェアをバージョンアップするには

■ バージョンアップするまでの手順(つづき)

- 10 すべてのランプが消灯し、本製品が再起動します。
起動中、[POWER]ランプが  橙点滅から  緑点灯に切り替わったことを確認してから本製品の電源を切ります。
最後に、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、必ず本製品の電源を切ってから、
USBメモリーを取りはずしてください。



バージョンアップ操作後は、本製品の管理者用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一とき、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。

6 保守について

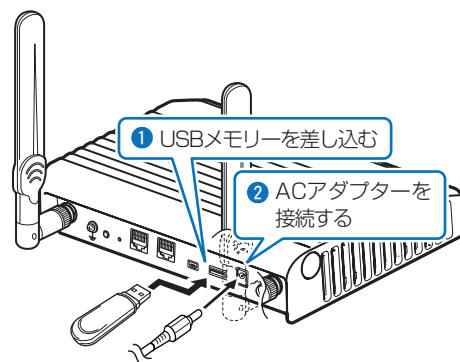
8. USBメモリー用の認証キーを設定するには

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、ファームウェアのバージョンアップができます。

■ 設定のしかた

- 1 本製品の電源を切ります。
- 2 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]ポートに差し込んでから、本製品の電源を入れます。
※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。
- 3 本製品の設定画面にアクセスします。(P.2-7)
- 4 「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。
- 5 [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	
USBメモリー:	<input type="radio"/> 無効 <input checked="" type="radio"/> 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:	<input type="text" value="●●●●●●"/>
USB認証キーの書き込み:	<input type="button" value="書き込み"/>
SSH認証方式:	<input checked="" type="checkbox"/> 自動
SSHポート番号:	<input type="text" value="22"/>
	<input type="button" value="登録"/>

①入力する

②クリック

- 6 〈書き込み〉をクリックします。

USB設定	
USBメモリー:	<input type="radio"/> 無効 <input checked="" type="radio"/> 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:	<input type="text" value="●●●●●●"/>
USB認証キーの書き込み:	<input type="button" value="書き込み"/>

クリック

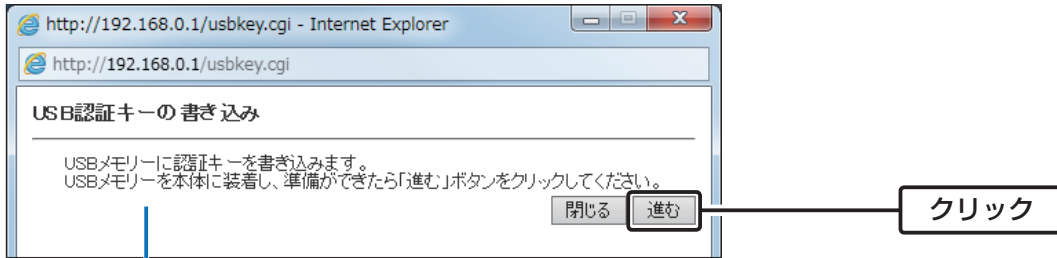
6 保守について

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

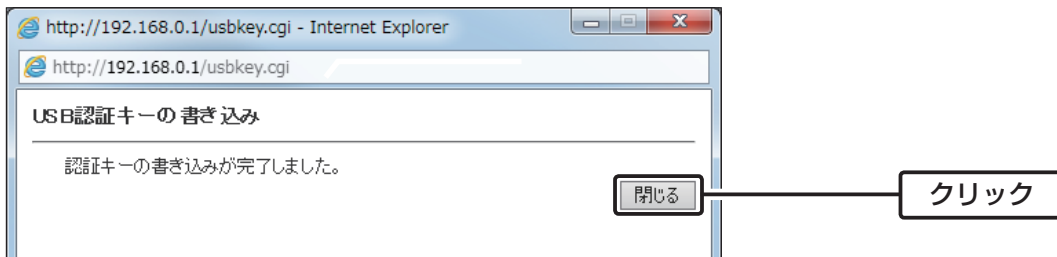
■ 設定のしかた(つづき)

- 7 「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。

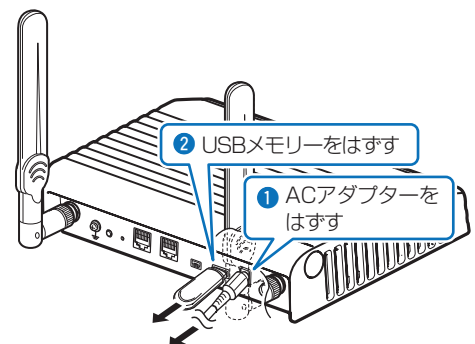


あらかじめUSB認証キーを保存したUSBメモリーを差し込んでいる場合は、「既に認証キーが書き込まれています。上書きする場合は「進む」ボタンをクリックしてください。」が表示されます。

- 8 「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。



- 9 本製品の電源を切り、USBメモリーを取りはずします。
【ご注意】 データ保護のため、必ず本製品の電源を切ってから、USBメモリーを取りはずしてください。



この章では、
本製品や無線LAN端末の情報が表示される画面について説明します。

1. 「TOP」画面について	7-2
■ 製品情報	7-2
■ ネットワーク情報	7-2
2. 「ネットワーク情報」画面について	7-3
■ インターフェースリスト	7-3
■ Ethernetポート接続情報	7-3
■ 無線LAN	7-4
■ AP間通信 (WDS)	7-4
■ AP間通信 (WBR)	7-4
■ DHCPリース情報	7-5
3. 「SYSLOG」画面について	7-6
4. 「無線設定情報一覧」画面について	7-7
■ アクセスポイント情報	7-7
■ 仮想AP一覧	7-7
■ 端末情報	7-8
■ 通信端末詳細情報	7-8
■ AP間通信情報	7-9
■ AP間通信詳細情報	7-9

7 情報表示について

2. 「ネットワーク情報」画面について

情報表示 > ネットワーク情報

■ インターフェースリスト

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

インターフェース	IPアドレス	サブネットマスク
lo0	127.0.0.1	255.255.255.255
mirror0	192.168.0.1	255.255.255.0

※「インターフェース」欄の表示内容は、「WAN接続先」画面にある「回線種別設定」項目の「回線種別」欄の設定で異なります。

「LANポートとして使用」(出荷時の設定)に設定したときは、「mirror0」、「lo0」を表示します。

「DHCPクライアント」、「固定IP」に設定したときは、「mirror0」、「lo0」、「ag0」を表示します。

「PPPoE」に設定したときは、「mirror0」、「lo0」、「pppoe0」を表示します。

「lo0」は、インターフェースが本製品自身の場合を意味します。

情報表示 > ネットワーク情報

■ Ethernetポート接続情報

本製品のポートごとに、通信速度と通信モードを表示します。

インターフェース	MACアドレス	リンク状態
eth0	00-90-C7-■■■■■■■■	100BASE-TX full-duplex
eth1	00-90-C7-■■■■■■■■	未接続

※本製品の「LAN」ポート(eth0)、「WAN/LAN」ポート(eth1)は、接続モードが「自動(Auto)」となっています。

接続する機器側も「自動(Auto)」を設定することで、通信に最適な速度、モードを自動選択します。

※接続する機器を100Mbps、または10Mbpsで固定する場合、半二重(half-duplex)設定にしてください。

弊社製品に限らず、自動(Auto)と固定速度full-duplexとがネゴシエーションする場合、自動(Auto)側はhalf-duplexと認識されることがあり、パフォーマンスが著しく低下する原因になることがあります。

※通信速度に関係なく、接続するHUBを「full-duplex」固定に設定すると、「Ethernetポート接続情報」項目で「half-duplex」と表示されることがあります。

7 情報表示について

2. 「ネットワーク情報」画面について(つづき)

情報表示 > ネットワーク情報

■ 無線LAN

本製品で使用している仮想AP(ath0～ath15)を表示します。

無線LAN		
インターフェース	SSID	BSSID
ath0	WIRELESSLAN-0	00-90-C7-██████
ath1	WIRELESSLAN-1	02-90-C7-██████
インターフェース	SSID	BSSID
ath8	WIRELESSLAN-0	00-90-C7-██████

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

情報表示 > ネットワーク情報

■ AP間通信 (WDS)

本製品の無線1(2.4GHz帯)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を表示します。

AP間通信 (WDS)	
インターフェース	BSSID
wds0	00-90-C7-██████

※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(wds0～wds7)と、無線AP間通信している相手側のBSSIDが表示されます。

情報表示 > ネットワーク情報

■ AP間通信 (WBR)

本製品の無線2(5GHz帯)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を表示します。

AP間通信 (WBR)	
インターフェース	BSSID
wbr17	00-90-C7-██████

※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(wbr8～wbr15、wbr17)と、無線AP間通信している相手側のBSSIDが表示されます。

※インターフェースに「wbr17」が表示されているときは、無線AP間通信の子機として動作しています。

7 情報表示について

2. 「ネットワーク情報」画面について(つづき)

情報表示 > ネットワーク情報

■ DHCPリース情報

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

IPアドレス	MACアドレス	状態	リース期限
192.168.0.10	08:00:27:00:00:00	動的	2023/10/27 10:00:00

端末に割り当てされたIPアドレスの状態を、「動的」/「静的」/「解放済」で表示します。

◎動的 : IPアドレスが自動で割り当てされているとき

◎静的 : IPアドレスが固定で割り当てされているとき

◎解放済 : IPアドレスを解放したとき

※リース期限は、[状態]欄が「動的」のときだけ、端末に割り当てされたIPアドレスの有効期限を表示します。

3. 「SYSLOG」画面について

情報表示 > SYSLOG

本製品のログ情報は、「情報表示」メニューの「SYSLOG」画面で確認できます。

※表示されるのは、「管理」メニューの「SYSLOG」画面で、「有効」に設定されたレベルのログ情報だけです。

日付・時間	レベル	内容
01-01 09:20:15	INFO	IEEE 802.11ng: association complete (VLAN=0:WIRELESSLAN-0)
01-01 09:00:31	NOTICE	Copyright Icom Inc.
01-01 09:00:31	NOTICE	AP-9000 Ver.

- 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。
(出荷時の設定：[✓]DEBUG [✓]INFO [✓]NOTICE)
※「SYSLOG」画面のチェックボックス状態は、保存されません。
設定画面へのアクセスごとに、元の状態に戻ります。
- ②<再読込>** …………… [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511件のログ情報を記憶できます。
511件を超えると、古いログ情報から削除されます。
- ③<クリア>** …………… 表示されたログ情報を削除するボタンです。
※電源を切る、または設定の変更や初期化に伴う再起動でも、それまでのログ情報は削除されます。
- ④<保存>** …………… 本製品の内部に蓄積されている最新のログ情報を保存するボタンです。
※クリックして、表示された画面にしたがって操作すると、ログ情報をテキスト形式(拡張子:txt)で保存できます。

7 情報表示について

4. 「無線設定情報一覧」画面について

情報表示 > 無線設定情報一覧 > 無線1

情報表示 > 無線設定情報一覧 > 無線2

■ アクセスポイント情報

無線LANユニットごとに、使用するチャンネル、帯域幅、稼働時間などを表示します。

アクセスポイント情報	
使用中チャンネル:	1 CH (2412 MHz) 20 MHz帯域幅
WMM ACM:	無効
WMM PowerSave:	有効
現在時刻:	2017/08/04 00:13:39
稼働時間:	0 days 00:13:39

※電源を切る、または設定の変更や初期化に伴う再起動で、それまでの稼働時間は初期化されます。

情報表示 > 無線設定情報一覧 > 無線1

情報表示 > 無線設定情報一覧 > 無線2

■ 仮想AP一覧

仮想APごとに、設定状況を一覧で表示します。

仮想AP一覧	
インターフェース	ath0
SSID	WIRELESSLAN-0
VLAN ID	0
ANY接続拒否	無効
暗号化	なし
MACアドレスフィルタリング	無効
ARP代理応答	無効
Web認証	無効
認証VLAN	無効
WiFi認証@クラウド	無効
インターフェース	ath1
SSID	
VLAN ID	
ANY接続拒否	
暗号化	

※使用していない仮想APの一覧は、[インターフェース]欄以外が空白になります。

7 情報表示について

4. 「無線設定情報一覧」画面について(つづき)

情報表示 > 無線設定情報一覧 > 端末情報

■ 端末情報

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端末との通信情報を表示します。

端末情報				
現在時刻: [時刻] (稼働時間: 0 days 01:17:27)				
最新状態に更新				
所属AP	MACアドレス	IPアドレス	VLAN ID	通信モード
ath8	[MAC]	192.168.0.10	0	IEEE 802.11n
詳細				


※<最新状態に更新>をクリックすると、表示内容を最新の状態にします。

※<詳細>をクリックすると、通信中の無線LAN端末について別画面(下図)で表示します。

情報表示 > 無線設定情報一覧 > 端末情報 > 通信端末詳細情報

■ 通信端末詳細情報

無線LAN端末と通信中、「端末情報」画面の[端末情報]項目に表示された<詳細>をクリックすると表示します。

通信端末詳細情報	
通信状況:	通信中
MACアドレス:	[MAC]
IPアドレス:	192.168.0.10
通信モード:	IEEE 802.11n
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:	 56
速度:	送信 39 Mbps / 受信 78 Mbps
WMM:	有効
WMMパワーセーブ:	無効
WMM CAC使用率:	0.00%
Web認証:	
接続時間:	0 days 00:00:13

※[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を、メーターと数値で表示します。

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

安定した通信の目安は、「緑(15)」以上のレベルです。(単位はありません)

ただし、信号レベルが高くて、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。

※[Web認証]欄に、Web認証を設定したときの認証状況を表示します。

「認証済」はWeb認証が完了しているとき、「未認証」はWeb認証が完了していない、またはWeb認証に失敗して無線LAN端末が再接続したときに表示されます。

Web認証を設定していないときは、何も表示されません。

7 情報表示について

4. 「無線設定情報一覧」画面について(つづき)

情報表示 > 無線設定情報一覧 > 端末情報

■ 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ごとの詳細情報を表示します。

AP間通信情報			
インターフェース	BSSID	通信モード	
wbr8	無線LANアクセスポイント	IEEE 802.11ac	最新状態に更新 詳細


※「最新状態に更新」をクリックすると、表示内容を最新の状態にします。

※「詳細」をクリックすると、通信中の無線AP間通信について別画面(下図)で表示します。

情報表示 > 無線設定情報一覧 > 端末情報 > 端末情報

■ AP間通信詳細情報

無線アクセスポイントと無線AP間通信中、「端末情報」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します。

AP間通信詳細情報	
通信状況:	通信中
インターフェース:	wbr8
MACアドレス:	無線LANアクセスポイント
通信モード:	IEEE 802.11ac
SSID:	WIRELESSLAN-0
暗号化:	WPA2-PSK (AES)
チャンネル:	36 CH (5180 MHz)
信号レベル:	 43
速度:	送信 173.3Mbps / 受信 173.3Mbps

※[信号レベル]欄に、無線アクセスポイントから受信した電波信号の強さを、メーターと数値で表示します。

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

安定した通信の目安は、「緑(15)」以上のレベルです。(単位はありません)

ただし、信号レベルが高くて、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。

※[MACアドレス]欄に表示されるのは、無線AP間通信している相手側のBSSIDです。

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	8-2
2. Telnet で接続するには	8-6
■ Windows 7 の場合	8-6
■ [CONSOLE] ポートを使用する	8-6
■ Telnet コマンドについて	8-7
3. 設定画面の構成について	8-8
4. 設定項目の初期値一覧	8-11
■ ネットワーク設定	8-11
■ ルーター設定	8-13
■ 無線設定	8-14
■ 管理	8-20
5. 機能一覧	8-22
■ 無線 LAN 機能	8-22
■ ネットワーク管理機能	8-22
■ ルーター機能	8-22
■ その他	8-22
6. 設定項目で使用できる文字列について	8-23
■ ネットワーク設定	8-23
■ 無線設定	8-23
■ 管理	8-23
7. PoE による電源供給について	8-24
8. 弊社製無線アクセスポイントの機能対応表	8-25
9. 定格について	8-26
■ 一般仕様	8-26
■ 有線部	8-26
■ 無線部	8-26

8 ご参考に

1. 困ったときは

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

[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]ランプや [WAN/LAN]ランプが点灯しない

- LANケーブルが本製品と正しく接続されていない
→ 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

[WIRELESS] (1/2)ランプが緑点灯しない

- パソコンの無線LANが機能していない
→ ご使用のパソコン、または無線LANアダプターに付属の取扱説明書を確認する
- 無線LAN端末と本製品の無線LAN規格が異なっている
→ ご使用になる無線LAN端末が準拠している無線LAN規格を確認する
- 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
- 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

[WIRELESS] (1/2)ランプが緑点灯しているが通信できない

暗号化セキュリティーの設定が異なっている

→ 本製品と無線LAN端末の暗号化セキュリティーの設定を確認する

<WPS>ボタンが機能しない(無線LANを自動設定できない)

- 本製品のWPS機能を無効に設定している
→ WPS機能を使用するインターフェース(ath0~ath15)が未設定か、インターフェースの番号を間違えて設定している(P.2-11)
- 無線LAN端末が無線LANの自動設定に対応していない
→ WPS対応の弊社製無線LAN端末(例：SU-81、SU-80、SE-80M、SE-90Mなど)を用意する
- ほかの無線LAN端末と自動設定中である
→ ほかの無線LAN端末との自動設定が完了するまで待つ
- 本製品と無線LAN端末の自動設定操作を2分以内に開始できなかった
→ 自動設定操作を2分以内に開始する
- 何度繰り返しても、自動設定できない
→ WPS機能を無効に変更して、手動で設定する

8 ご参考に

1. 困ったときは(つづき)

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

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

本製品の設定画面が正しく表示されない

- WWWブラウザのJavaScript®機能、およびCookieを無効に設定している
→ JavaScript®機能、およびCookieを有効に設定する
- Microsoft® Internet Explorer® 8.0以前を使用している
→ Microsoft® Internet Explorer® 9.0以降を使用する

本製品の設定画面にアクセスできない

- パソコンのIPアドレスを設定していない
→ 本製品の出荷時や全設定初期化時は、パソコンのIPアドレスを固定IPアドレスに設定する(P.2-3)
- 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(P.2-8)
- 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ブラウザにプロキシサーバーが設定されている
→ Internet Explorer®の「ツール(T)」メニューから「インターネットオプション(O)」、[接続]タブ、〈LANの設定(L)〉の順に操作して、[設定を自動的に検出する(A)]や[LANにプロキシサーバーを使用する(X)]にチェックマークが入っていないことを確認する

本製品の設定画面で設定を変更できない

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

RS-AP3から本製品を管理できない

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

無線1(2.4GHz帯)で無線AP間通信できない(WDS)

- チャンネルを「自動」に設定している
→ 使用されているチャンネルを確認する
- 共有鍵(PSK : Pre-Shared Key)が相手側と異なっている
→ 相手側の共有鍵を確認する
- 無線AP間通信する相手側のBSSIDが正しく登録されていない
→ 相手側のBSSIDを確認する

8 ご参考に

1. 困ったときは(つづき)

無線2(5GHz帯)で無線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」のチャンネル詳細設定で5.3/5.6GHz帯のチャンネルが選択されている
→ 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。(2017年1月現在)

「ath0」：アクセスポイントモードのSE-900

「ath4」：AP-90M、AP-90MR

「ath8」：AP-900、AP-9000

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「WAN/LAN MACアドレス」(WAN側接続用ポートのMACアドレス)を登録する(P.vi、P.6-6)
- 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/LAN」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(LANポートとして使用する)で、「WAN/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
- 「切断」で、回線を強制的に切断している
→ 「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「接続」をクリックして、回線を強制的に接続する
- 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/LAN」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。

8 ご参考に

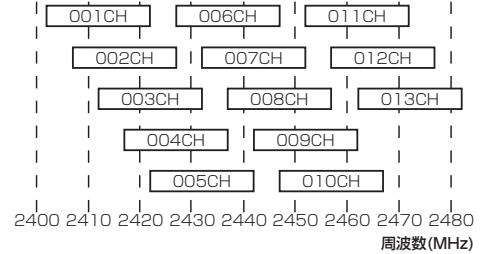
1. 困ったときは(つづき)

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

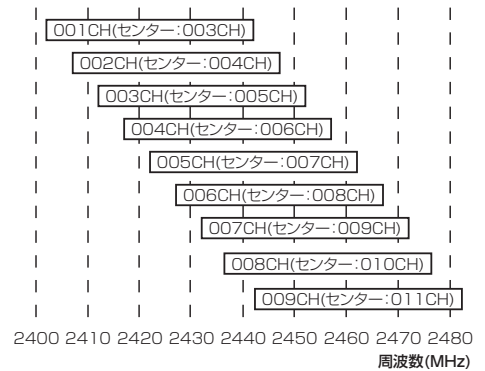
【帯域幅が20MHzの場合】(帯域の一部が重複)

- 本製品の設置場所を変更する
- 本製品のチャンネルを「自動」に設定する
- 近くに存在する無線LAN端末や無線アクセスポイントなどと、4チャンネル以上空けて、本製品のチャンネルを変更する
 - ※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】(帯域の一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
- 本製品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。



8 ご参考に

2. Telnetで接続するには

Telnetでの接続について説明します。

ご使用のOSやTelnetクライアントが異なるときは、それぞれの使用方法をご確認ください。

■ Windows 7の場合

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

【設定のしかた】

- ① Windowsを起動します。
- ② [スタート] (ロゴボタン) から [プログラムとファイルの検索] を選択します。
名前欄に「telnet.exe」と入力し、[Enter] キーを押します。
※ Windows Vistaをご使用の場合は、[スタート] (ロゴボタン) から [検索の開始] を選択します。
※ Windows 8.1の場合は、[スタート] (ロゴボタン) から [ファイル名を指定して実行] を選択します。
- ③ Telnetクライアントが起動しますので、下記のように入力します。
Microsoft Telnet>open 本製品のIPアドレス(入力例：open 192.168.0.1)
- ④ 下記を入力して[Enter] キーを押すと、ログインできます。
login : admin
password : admin
※出荷時や全設定初期化時のpasswordは、adminです。(P.5-2)
- ⑤ ログインメッセージ(AP-9000 #)が表示されます。

■ [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(miniBタイプ)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、パソコンの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-9000 #」と表示されます。

2. Telnetで接続するには(つづき)

■ Telnetコマンドについて

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

コマンド一覧……………	[Tab]キーを押すと、使用できるコマンドの一覧が表示されます。 コマンド名の入力につづいて[Tab]キーを押すと、サブコマンドの一覧が表示されます。
コマンドヘルプ……………	コマンドの意味を知りたいときは、ヘルプコマンドにつづいて、コマンド名を入力するとコマンドのヘルプが表示されます。 例) help save (saveコマンドのヘルプを表示する場合)
コマンド名の補完……………	コマンド名を先頭から数文字入力し[Tab]キーを押すと、コマンド名が補完されます。 入力した文字につづくコマンドが1つしかないときは、コマンド名を最後まで補完します。 例) v[Tab]→ver 複数のコマンドがあるときは、コマンドの候補を表示します。 例) res[Tab]→reset restart

8 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	製品情報 ネットワーク情報		
情報表示	ネットワーク情報	インターフェースリスト		
		Ethernetポート接続情報		
		無線LAN		
		DHCPリース情報		
		SYSLOG		
		無線設定情報一覧 無線1	アクセスポイント情報	
		無線設定情報一覧 無線2	仮想AP一覧	
		無線設定情報一覧 無線2	アクセスポイント情報	
		無線設定情報一覧 端末情報	仮想AP一覧	
		無線設定情報一覧 端末情報	端末情報	
ネットワーク設定	LAN側IP	AP間通信情報		
		統計情報		
		メモリ使用率		
		トラフィック統計		
		本体名称		
		VLAN設定		
		IPアドレス設定		
		DHCPサーバー	DHCPサーバー設定	
		DHCPサーバー	静的DHCPサーバー設定	
		DHCPサーバー	静的DHCPサーバー設定一覧	
ネットワーク設定	ポートベースVLAN	ポートベースVLAN設定		
		ポート個別設定		
		ルーティング	IP経路情報	
		ルーティング	スタティックルーティング設定	
		ルーティング	スタティックルーティング設定一覧	
		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
				パケットフィルター設定一覧
		ネットワーク設定	Web認証 基本	Web認証
				カスタムページ
		ネットワーク設定	Web認証 詳細	Web認証方法
RADIUS設定				
ルーター設定	POPCHAT@Cloud	アカウント設定		
		POPCHAT@Cloud	アカウント設定	
		POPCHAT@Cloud	インターフェース設定	
		ルーター設定	WAN接続先	回線状態表示
				回線種別設定
		ルーター設定	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
				静的マスカレードテーブル設定一覧
ルーター設定	IPフィルター	IPフィルター設定		
		IPフィルター設定一覧		

(次ページにつづく)

3. 設定画面の構成について(つづき)

設定メニュー	設定画面	設定項目
無線設定	無線1 無線LAN	無線LAN設定
	無線1 仮想AP	仮想AP設定 暗号化設定
	無線1 認証サーバー	RADIUS設定 アカウント設定
	無線1 MACアドレスフィルタリング	MACアドレスフィルタリング設定 端末MACアドレスリスト MACアドレスフィルタリング設定一覧
	無線1 ネットワーク監視	ネットワーク監視設定
	無線1 AP間通信 (WDS)	AP間通信設定 AP間通信設定一覧
	無線1 WMM詳細	WMM詳細設定 WMMパワーセーブ設定 CAC設定
	無線1 レート	レート設定
	無線1 ARP代理応答	ARP代理応答 ARPキャッシュ情報
	無線1 IP Advanced Radio System	近隣呼出設定
	無線2 無線LAN	無線LAN設定
	無線2 仮想AP	仮想AP設定 暗号化設定
	無線2 認証サーバー	RADIUS設定 アカウント設定
	無線2 MACアドレスフィルタリング	MACアドレスフィルタリング設定 端末MACアドレスリスト MACアドレスフィルタリング設定一覧
	無線2 ネットワーク監視	ネットワーク監視設定
	無線2 AP間通信 (WBR)	AP間通信設定
	無線2 WMM詳細	WMM詳細設定 WMMパワーセーブ設定 CAC設定
	無線2 レート	レート設定
	無線2 ARP代理応答	ARP代理応答 ARPキャッシュ情報
	無線2 IP Advanced Radio System	近隣呼出設定
	WPS	WPS設定 WPS開始 WPS状態表示

(次ページにつづく)

3. 設定画面の構成について(つづき)

設定メニュー	設定画面	設定項目
管理	管理者	管理者パスワードの変更
	管理ツール	無線アクセスポイント管理ツール設定
		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
	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
		オンライン設定
		設定内容一覧
	初期化	初期化
	ファームウェアの更新	ファームウェア情報
		オンライン更新
		自動更新
		手動更新

8 ご参考に

4. 設定項目の初期値一覧

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

■ネットワーク設定

設定画面/項目	初期値	設定範囲/最大登録数	
「LAN側IP」画面			
本体名称	本体名称：AP-9000	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)		
	静的DHCPサーバー	MACアドレス：空白(設定なし) IPアドレス：空白(設定なし)	最大登録数：32
「ポートベースVLAN」画面			
ポートベースVLAN設定	ポートベースVLAN機能：無効		
ポート個別設定	LANポート	トラッキングポート	
	eth0	<input type="checkbox"/>	0
	eth1	<input type="checkbox"/>	0
「ルーティング」画面			
スタティックルーティング設定	宛先：空白(設定なし)	最大登録数：32	
	サブネットマスク：空白(設定なし)		
	ゲートウェイ：空白(設定なし)		
「パケットフィルター」画面			
パケットフィルター設定一覧	(設定なし)	最大登録数：64	
「Web認証 基本」画面 (eth0、ath0～ath15)			
Web認証	インターフェース：eth0		
	Web認証：無効		
	ページタイトル：Set your page title.	任意の半角255 (全角127) 文字以内	
	ポータルサイト：http://www.example.com/	「http://」も含めて半角255文字以内	
	移動待ち時間：5(秒)	設定範囲「0～60」(秒)	
	有効期限：24時間		

8 ご参考に

4. 設定項目の初期値一覧

■ ネットワーク設定(つづき)

設定画面/項目	初期値	設定範囲/最大登録数
「Web認証 詳細」画面 (eth0、ath0～ath15)		
Web認証方法	インターフェース：eth0 認証方法：RADIUSのみ使用	
RADIUS設定 (プライマリー/セカンダリー)		
	アドレス：空白(設定なし)	
	ポート：1812	設定範囲「1～65535」
	シークレット：secret	半角64文字以内
「POPCHAT@Cloud」画面		
アカウント設定	アプリケーションID：空白(設定なし) 秘密鍵：空白(設定なし) 認証サーバーURL：空白(設定なし)	半角36文字以内 半角36文字以内 半角64文字以内
インターフェース設定 (eth0、ath0～ath15)		
	インターフェース：eth0	
	Wi-Fi認証@クラウド：無効	

8 ご参考に

4. 設定項目の初期値一覧(つづき)

■ ルーター設定

設定画面 / 項目	初期値	設定範囲 / 最大登録数		
「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	静的マスカレードテーブル(設定なし)	最大登録数：32		
「IP フィルター」画面				
IP フィルター設定		最大登録数：64		
番号	フィルター方法	インターフェース	送信元IPアドレス(送信元ポート番号)	SPI
	フィルター方向	プロトコル	宛先IPアドレス(宛先ポート番号)	フィルター合致時 SYSLOGに出力
1	遮断	すべて	*(*)	無効
	IN	すべて	*(*)	検索を継続 無効
2	透過	すべて	*(*)	有効
	OUT	すべて	*(*)	検索を継続 無効
58	透過	すべて	*(20)	無効
	IN	TCP(フラグ指定なし)	*(*)	検索を継続 無効
59	遮断	すべて	*(135)	無効
	OUT	TCP/UDP	*(*)	検索を継続 無効
60	遮断	すべて	*(*)	無効
	OUT	TCP/UDP	*(135)	検索を継続 無効
61	遮断	すべて	*(445)	無効
	OUT	TCP/UDP	*(*)	検索を継続 無効
62	遮断	すべて	*(*)	無効
	OUT	TCP/UDP	*(445)	検索を継続 無効
63	遮断	すべて	*(*)	無効
	OUT	TCP(フラグ指定なし)	*(137-139)	検索を継続 無効
64	遮断	すべて	*(137-139)	無効
	OUT	UDP	*(137-139)	検索を継続 無効

4. 設定項目の初期値一覧(つづき)

■ 無線設定

設定画面/項目	初期値	設定範囲/最大登録数
「無線1 無線LAN」画面		
無線LAN設定	無線UNIT：有効 帯域幅：20MHz チャンネル：001CH (2412MHz) パワーレベル：高 DTIM間隔：1 プロテクション機能：有効	設定範囲「1～50」
「無線1 仮想AP」画面(ath0～ath7)		
仮想AP設定	インターフェース：ath0 仮想AP：有効(ath0) 無効(ath1～ath7)	
	SSID：WIRELESSLAN-0(ath0) WIRELESSLAN-1(ath1) WIRELESSLAN-2(ath2) WIRELESSLAN-3(ath3) WIRELESSLAN-4(ath4) WIRELESSLAN-5(ath5) WIRELESSLAN-6(ath6) WIRELESSLAN-7(ath7)	半角英数字32文字以内
	VLAN ID：0(ath0～ath7)	設定範囲「0～4094」
	ANY接続拒否：無効(ath0～ath7)	
	接続端末制限：63(ath0～ath7)	設定範囲「1～128」
	アカウントिंग：無効(ath0～ath7)	
	MAC認証：無効	
暗号化設定	ネットワーク認証：オープンシステム/共有キー (ath0～ath7) 暗号化方式：なし(ath0～ath7)	
「無線1 認証サーバー」画面		
RADIUS設定(プライマリー/セカンダリー)		
	アドレス：空白(設定なし)	
	ポート：1812	設定範囲「1～65535」
	シークレット：secret	半角64文字以内
アカウントिंग設定(プライマリー/セカンダリー)		
	アドレス：空白(設定なし)	
	ポート：1813	設定範囲「1～65535」
	シークレット：secret	半角64文字以内

8 ご参考に

4. 設定項目の初期値一覧

■ 無線設定(つづき)

設定画面/項目	初期値	設定範囲/最大登録数
「無線1 MACアドレスフィルタリング」画面(ath0~ath7)		
MACアドレスフィルタリング設定	インターフェース：ath0 MACアドレスフィルタリング：無効 フィルタリングポリシー：許可リスト	
端末MACアドレスリスト	MACアドレス：空白(設定なし)	最大登録数：1024(※仮想APごとの数)
「無線1 ネットワーク監視」画面(ath0~ath7)		
ネットワーク監視設定	インターフェース：ath0 監視対象ホスト1：空白(設定なし) 監視対象ホスト2：空白(設定なし) 監視対象ホスト3：空白(設定なし) 監視対象ホスト4：空白(設定なし) 監視間隔：10(秒) タイムアウト時間：1(秒) 失敗回数：3(回) 条件：ひとつ以上のホストが応答なし	設定範囲「1~120」(秒) 設定範囲「1~10」(秒) 設定範囲「1~10」(回)
「無線1 AP間通信WDS」画面		
AP間通信設定(設定なし)		
「無線1 WMM詳細」画面		
WMM詳細設定	[To Station]/[From Station] CWin min：AC_BK(15)、AC_BE(15)、 AC_VI(7)、AC_VO(3) [To Station] CWin max：AC_BK(1023)、AC_BE(63)、 AC_VI(15)、AC_VO(7) [From Station] CWin max：AC_BK(1023)、AC_BE(1023)、 AC_VI(15)、AC_VO(7)	
	[To Station] AIFSN(1-15)：AC_BK(7)、AC_BE(3)、 AC_VI(1)、AC_VO(1)	設定範囲「1~15」
	[From Station] AIFSN(2-15)：AC_BK(7)、AC_BE(3)、 AC_VI(2)、AC_VO(2)	設定範囲「2~15」
	[To Station]/[From Station] TXOP(0-255)：AC_BK(0)、AC_BE(0)、 AC_VI(94)、AC_VO(47)	設定範囲「0~255」
	[To Station] 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：有効	
CAC設定	通話制限台数：6	設定範囲「1~63」

8 ご参考に

4. 設定項目の初期値一覧

■ 無線設定(つづき)

設定画面/項目	初期値	設定範囲/最大登録数
「無線1 レート」画面(ath0~ath7)		
レート設定	インターフェース：ath0 プリセット：初期値 レガシー： 1Mbps：ベーシックレート 2Mbps：ベーシックレート 5.5Mbps：ベーシックレート 6Mbps：有効 9Mbps：有効 11Mbps：ベーシックレート 12Mbps：有効 18Mbps：有効 24Mbps：有効 36Mbps：有効 48Mbps：有効 54Mbps：有効 HT-MCS： MCS 0：有効 MCS 1：有効 MCS 2：有効 MCS 3：有効 MCS 4：有効 MCS 5：有効 MCS 6：有効 MCS 7：有効 MCS 8：有効 MCS 9：有効 MCS 10：有効 MCS 11：有効 MCS 12：有効 MCS 13：有効 MCS 14：有効 MCS 15：有効 マルチキャスト送信レート： マルチキャスト：1Mbps	
仮想AP共通設定	最低レートの再送制限：無効 キックアウト：弱	

8 ご参考に

4. 設定項目の初期値一覧

■ 無線設定(つづき)

設定画面/項目	初期値	設定範囲/最大登録数
「無線1 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)
「無線1 IP Advanced Radio System」画面(ath0～ath7)		
近隣呼出設定	インターフェース：ath0 テナント番号 通知 名前	名前は半角31 (全角15) 文字以内
	1 有効 空白 (設定なし)	
	2 有効 空白 (設定なし)	
	3 有効 空白 (設定なし)	
	4 有効 空白 (設定なし)	
	5 有効 空白 (設定なし)	
	6 有効 空白 (設定なし)	
	7 有効 空白 (設定なし)	
	8 有効 空白 (設定なし)	
	9 有効 空白 (設定なし)	
	10 有効 空白 (設定なし)	
「無線2 無線LAN」画面		
無線LAN設定	無線UNIT：有効 帯域幅：20MHz チャンネル：036CH (5180MHz) パワーレベル：高 DTIM間隔：1 プロテクション機能：有効	設定範囲「1～50」
「無線2 仮想AP」画面(ath8～ath15)		
仮想AP設定	インターフェース：ath8 仮想AP：有効(ath8) 無効(ath9～ath15) SSID：WIRELESSLAN-0(ath8) WIRELESSLAN-1(ath9) WIRELESSLAN-2(ath10) WIRELESSLAN-3(ath11) WIRELESSLAN-4(ath12) WIRELESSLAN-5(ath13) WIRELESSLAN-6(ath14) WIRELESSLAN-7(ath15) VLAN ID：0(ath8～ath15) ANY接続拒否：無効(ath8～ath15) 接続端末制限：63(ath8～ath15) アカウントング：無効(ath8～ath15) MAC認証：無効	半角英数字32文字以内 設定範囲「0～4094」 設定範囲「1～128」

8 ご参考に

4. 設定項目の初期値一覧

■ 無線設定(つづき)

設定画面/項目	初期値	設定範囲/最大登録数
「無線2 仮想AP」画面(ath8～ath15)		
暗号化設定	ネットワーク認証：オープンシステム/共有キー (ath8～ath15) 暗号化方式：なし(ath8～ath15)	
「無線2 認証サーバー」画面		
RADIUS設定(プライマリー/セカンダリー)		
	アドレス：空白(設定なし)	
	ポート：1812	設定範囲「1～65535」
	シークレット：secret	半角64文字以内
アカウント設定(プライマリー/セカンダリー)		
	アドレス：空白(設定なし)	
	ポート：1813	設定範囲「1～65535」
	シークレット：secret	半角64文字以内
「無線2 MACアドレスフィルタリング」画面(ath8～ath15)		
MACアドレスフィルタリング設定		
	インターフェース：ath8	
	MACアドレスフィルタリング：無効	
	フィルタリングポリシー：許可リスト	
端末MACアドレスリスト	MACアドレス：空白(設定なし)	最大登録数：1024 (※仮想APごとの数)
「無線2 ネットワーク監視」画面(ath8～ath15)		
ネットワーク監視設定		
	インターフェース：ath8	
	監視対象ホスト1：空白(設定なし)	
	監視対象ホスト2：空白(設定なし)	
	監視対象ホスト3：空白(設定なし)	
	監視対象ホスト4：空白(設定なし)	
	監視間隔：10(秒)	設定範囲「1～120」(秒)
	タイムアウト時間：1(秒)	設定範囲「1～10」(秒)
	失敗回数：3(回)	設定範囲「1～10」(回)
	条件：ひとつ以上のホストが応答なし	
「無線2 AP間通信(WBR)」画面		
AP間通信設定	AP間通信：無効	
「無線2 WMM詳細」画面		
WMM詳細設定		
	[To Station]/[From Station] CWin min：AC_BK(15)、AC_BE(15)、 AC_VI(7)、AC_VO(3)	
	[To Station] CWin max：AC_BK(1023)、AC_BE(63)、 AC_VI(15)、AC_VO(7)	
	[From Station] CWin max：AC_BK(1023)、AC_BE(1023)、 AC_VI(15)、AC_VO(7)	
	[To Station] AIFSN(1-15)：AC_BK(7)、AC_BE(3)、 AC_VI(1)、AC_VO(1)	設定範囲「1～15」
	[From Station] AIFSN(2-15)：AC_BK(7)、AC_BE(3)、 AC_VI(2)、AC_VO(2)	設定範囲「2～15」
	[To Station]/[From Station] TXOP(0-255)：AC_BK(0)、AC_BE(0)、 AC_VI(94)、AC_VO(47)	設定範囲「0～255」

8 ご参考に

4. 設定項目の初期値一覧

■ 無線設定(つづき)

設定画面/項目	初期値	設定範囲/最大登録数
「無線2 WMM詳細」画面		
WMM詳細設定	[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：有効	
CAC設定	通話制限台数：6	設定範囲「1～63」
「無線2 レート」画面(ath8～ath15)		
レート設定	インターフェース：ath8 プリセット：初期値 レガシー： 6Mbps：ベーシックレート 9Mbps：有効 12Mbps：ベーシックレート 18Mbps：有効 24Mbps：ベーシックレート 36Mbps：有効 48Mbps：有効 54Mbps：有効 HT-MCS： MCS 0：有効 MCS 1：有効 MCS 2：有効 MCS 3：有効 MCS 4：有効 MCS 5：有効 MCS 6：有効 MCS 7：有効 MCS 8：有効 MCS 9：有効 MCS 10：有効 MCS 11：有効 MCS 12：有効 MCS 13：有効 MCS 14：有効 MCS 15：有効 VHT-MCS： 1ストリーム：MCS 0-9 2ストリーム：MCS 0-9 マルチキャスト送信レート： マルチキャスト：6Mbps	
仮想AP共通設定	キックアウト：弱	
「無線2 ARP代理応答」画面(ath8～ath15)		
ARP代理応答	インターフェース：ath8 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)

8 ご参考に

4. 設定項目の初期値一覧

■ 無線設定(つづき)

設定画面/項目	初期値	設定範囲/最大登録数
「無線2 IP Advanced Radio System」画面(ath8~ath15)		
近隣呼出設定	インターフェース：ath8	
	テナント番号	通知
	名前	名前は半角31 (全角15) 文字以内
	1	有効 空白 (設定なし)
	2	有効 空白 (設定なし)
	3	有効 空白 (設定なし)
	4	有効 空白 (設定なし)
	5	有効 空白 (設定なし)
	6	有効 空白 (設定なし)
	7	有効 空白 (設定なし)
	8	有効 空白 (設定なし)
	9	有効 空白 (設定なし)
	10	有効 空白 (設定なし)
「WPS」画面(ath0~ath15)		
WPS設定	使用するインターフェース：なし	

■ 管理

設定画面/項目	初期値	設定範囲/最大登録数
「管理者」画面		
管理者パスワードの変更	管理者ID：admin(変更不可) 現在のパスワード：admin(非表示) 新しいパスワード：空白(設定なし) 新しいパスワード再入力：空白(設定なし)	英数字/記号 (半角31文字以内)
「管理ツール」画面		
無線アクセスポイント管理ツール設定	RS-AP3：無効	
USB設定	USBメモリー：有効 USBアクセス許可： ファームウェアの更新 <input type="checkbox"/> (あり(ON)) 設定の保存/復元 <input checked="" type="checkbox"/> (あり(ON))	
	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：有効 Telnetポート番号：23 SSH：無効 SSHバージョン：自動 SSH認証方式：自動 SSHポート番号：22	

8 ご参考に

4. 設定項目の初期値一覧

■ 管理(つづき)

設定画面/項目	初期値	設定範囲/最大登録数
「時計」画面		
時計設定	設定する時刻：パソコンから取得した時刻	
自動時計設定	自動時計設定：無効 NTPサーバー1：210.173.160.27 NTPサーバー2：210.173.160.57 アクセス時間間隔：1(日)	設定範囲「1～99」(日)
「SYSLOG」画面		
SYSLOG設定	DEBUG：無効 INFO：有効 NOTICE：有効 ホストアドレス：空白(設定なし)	
「SNMP」画面		
SNMP設定	SNMP：有効 コミュニティID(GET)：public 場所：空白(設定なし) 連絡先：空白(設定なし)	
「LED」画面		
LED 消灯モード	LED 消灯モード：無効 LED 消灯モードに入るまでの時間：30 秒	設定範囲「0～3600」(秒)
「ネットワークテスト」画面		
PINGテスト	ホスト：空白(設定なし) 試行回数：4(回) パケットサイズ：64(バイト) タイムアウト時間：1000(ミリ秒)	
経路テスト	ノード：空白(設定なし) 最大ホップ数：16 タイムアウト時間：3(秒) DNS名前解決：有効	
「設定の保存/復元」画面		
オンライン設定	オンライン設定：無効 サーバーホスト名：空白(設定なし) 契約ユーザー名：空白(設定なし) パスワード：空白(設定なし)	
「ファームウェアの更新」画面		
自動更新	自動更新：有効	

5. 機能一覧

■ 無線LAN機能

- IEEE802.11ac規格★¹
- IEEE802.11n規格★¹
- IEEE802.11a(W52/W53/W56)/g/b規格
- 暗号化セキュリティ(WEP RC4、TKIP、AES)
- ネットワーク認証
(オープンシステム、共有キー、IEEE802.1X、WPA、WPA2、WPA-PSK、WPA2-PSK)
- MAC認証(RADIUS)
- SSID(Service Set Identifier)
- アクセスポイント機能
- ローミング機能
- ANY接続拒否機能
- 仮想AP機能
- MACアドレスフィルタリング機能
- プロテクション機能
- パワーレベル調整機能
- 接続端末制限機能
- WMM★²(Wi-Fi Multimedia)機能
- WPS機能★²
- ARP代理応答
- WMMIパワーセーブ
- 無線AP間通信機能
- 認証サーバー(RADIUS/アカウンティング)
- ネットワーク監視機能
- 自動チャンネル機能

■ ネットワーク管理機能

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

■ ルーター機能

- 接続方式(DHCPクライアント、固定IP、PPPoE)
- スタティックルーティング機能
- DNS代理応答機能
- IPフィルター機能
- アドレス変換(IPマスカレード)
- 静的IPマスカレード
- DMZホストアドレス

■ その他

- DHCPサーバー機能
- 静的DHCPサーバー機能
- タグVLAN機能
- ポートベースVLAN機能
- 認証VLAN
- パケットフィルター機能
- 接続制限機能(管理者ID/パスワード)
- 内部時計設定
- Web認証(RADIUS/ローカルリスト)
- POPCHAT@Cloud連携機能
- PoE機能
- ファームウェアのバージョンアップ
- WWWメンテナンス(HTTP/HTTPS)
- TELNETメンテナンス(TELNET/SSH)

★¹ 本製品のIEEE802.11ac規格、IEEE802.11n規格での通信は、暗号化方式を「なし」、または「AES」に設定している場合に有効です。

★² 2017年1月現在、本製品は、Wi-Fiアライアンスの認定を取得していません。

8 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。

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

■ ネットワーク設定

設定画面	設定項目	設定欄	入力できる文字列	入力できる文字数
LAN側IP	本体名称	本体名称	半角英数字 ^{★1} /「-」 ※先頭と末尾は半角英数字のみ	31文字以内
DHCPサーバー	DHCPサーバー設定	ドメイン名	半角英数字 ^{★1} /「.」/「-」 ※先頭と末尾は半角英数字のみ	127文字以内
Web認証 詳細	ローカルリスト	ユーザー名	ASCII ^{★2}	128文字以内
		パスワード	ASCII ^{★2}	128文字以内

■ 無線設定

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	3-4ページ参照
		PSK (Pre-Shared Key)	ASCII ^{★2} 、または16進数	2-10ページ参照
AP間通信 (WDS)	AP間通信設定	PSK (Pre-Shared Key)	ASCII ^{★2} 、または16進数	3-16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	3-20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
設定の保存/復元	オンライン設定	サーバーホスト名	半角英数字 ^{★1} /「.」/「-」 ※先頭と末尾は半角英数字のみ	128文字以内
		契約ユーザー名	半角英数字/記号	128文字以内
		パスワード	半角英数字/記号	128文字以内

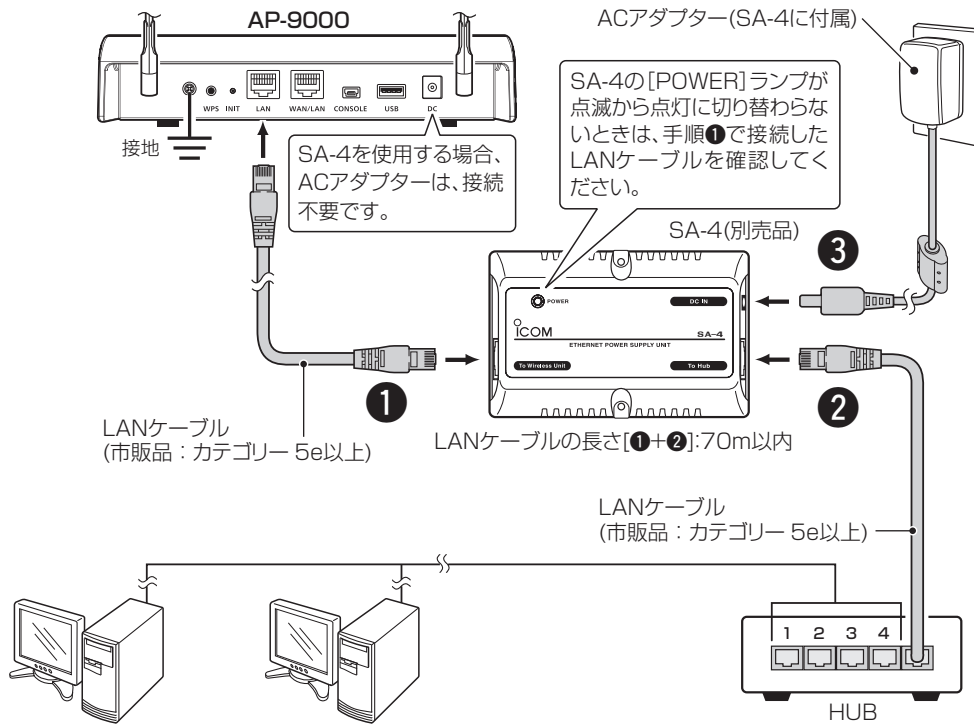
★1 半角英数字は、半角英字と半角数字です。

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

7. PoEによる電源供給について

本製品の[LAN]ポート、または[WAN/LAN]ポートに接続されたLANケーブルとSA-4(別売品)を接続して、本製品に電源を供給する接続方法について説明します。

※下記の図に示す番号の順に接続後、SA-4の[POWER]ランプが点滅から点灯状態に切り替わらないときは、手順①で接続したLANケーブルを確認してください。



設置と接続のご注意

- ◎ 1台のSA-4で電源供給できるのは、本製品1台だけです。
- ◎ 本製品用のACアダプターは必要ありません。
- ◎ SA-4には、電源が必要ですので、コンセントから近い場所に設置してください。
- ◎ SA-4には、HUBなどのネットワーク機器に搭載のリピーター機能は、搭載していません。
したがって、使用するLANケーブルは、HUB(HUBを使用しない場合は、パソコン)からSA-4を介して接続された本製品までの総延長距離が70m以内の場所に設置してください。
※ご使用のLANケーブルによっては、Ethernet規格の最大長制限より短くなる場合があります。
- ◎ SA-4は、防水構造ではありませんので、雨水などでぬれやすい場所には設置できません。
- ◎ 1000BASE-T規格でご使用になる場合、カテゴリ5e以上のLANケーブルをご使用ください。
- ◎ LANケーブルを接続後、SA-4のACアダプターを接続してから、SA-4の[POWER]ランプが点灯に切り替わる(給電する)まで、10秒~15秒かかることがあります。

8 ご参考に

8. 弊社製無線アクセスポイントの機能対応表

		AP-90M	AP-90MR	AP-9000	AP-900	SE-900 (アクセスポイントモード時)
ルーター	ルーター機能	×	○	○	×	×
	WAN ポート	×	○ ^{★1}	○ ^{★1}	×	×
ネットワーク	ポートベース VLAN	×	×	○	×	×
無線	無線 UNIT 数	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}	× ^{★3}	○
	ストリーム数	×	×	×	○	○
	無線 UNIT ごとの 仮想 AP 数	4	4	8	8	8
	AP 間通信(WDS)	無線 1	無線 1	無線 1	無線 1	×
	AP 間通信(WBR)	無線 2	無線 2	無線 2	無線 2	○
	WPS	○	○	○	×	×
管理	USB 設定	○	○	○	×	×
	LED 消灯モード	○	○	○	×	×
その他	CONSOLE ^{★4★5}	×	×	○	○	×
	初期化ボタン	○ (MODE)	○ (MODE)	○ (INIT)	×	○ (MODE)
	屋外対応	×	×	×	○	○

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

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

★2 クライアントモードに切り替えることで無線LAN端末として動作します。

★3 無線動作モードの設定がない機種では、無線1が2.4GHz帯、無線2が5GHz帯に固定されています。

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

使用方法など、詳しくは「[CONSOLE]ポートを使用する」(P.8-6)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。

9. 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(本製品用)は、AC100V±10%
※PoEは、IEEE802.3af準拠
最大12W(本製品のACアダプター使用時)
最大12W(PoE使用時)
- 使用環境** : 温度-10～+55℃(0℃以下では常時通電時)*、湿度5～95%(結露状態を除く)
★-10℃～0℃の環境では、電源投入して1時間以上経過してから、本製品をリセット(再起動)して通信を開始してください。
- 外形寸法** : 約190(W)×40(H)×140(D)mm(突起物を除く)
- 重量** : 約0.6kg(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、MODE、WAN/LAN、LAN、WIRELESS1、WIRELESS2)
ボタン(INIT、WPS)
[USB]ポート : USB Aタイプ(USB2.0/1.1)
[CONSOLE]ポート : USB miniBタイプ(USB2.0/1.1)

■ 有線部

- 通信速度** : 10/100/1000Mbps(自動切り替え/全二重)
- インターフェース** : [LAN]ポート(RJ-45型)×1(Auto MDI/MDI-X)
[WAN/LAN]ポート(RJ-45型)×1(Auto MDI/MDI-X)
●IEEE802.3/10BASE-T準拠
●IEEE802.3u/100BASE-TX準拠
●IEEE802.3ab/1000BASE-T準拠
●IEEE802.3af準拠

■ 無線部

- 国際規格** : IEEE802.11ac準拠、IEEE802.11n準拠
IEEE802.11a準拠、IEEE802.11g/b準拠
- 国内規格** : ARIB STD-T71/ARIB STD-T66
- 使用周波数範囲** : 5180～5700MHz
2412～2472MHz

※定格・仕様・外観等は改良のため予告なく変更する場合があります。

高品質がテーマです。