Future X Communications

AE1021/AE1021PE Management Guide

2016 年 8 月 Ver 2.5

FXC株式会社

本マニュアルについて

■ 本マニュアルでは、AE1021/AE1021PE の各種設定手順について説明します。
本製品の設定は、LAN ポートに設定用の端末（PC）を接続して Web ブラウザで行います。

この度は、お買い上げいただきましてありがとうございます。製品を安全にお使いいただくため、
必ず最初にお読みください。

・下記事項は、安全のために必ずお守りください。

●安全のための注意事項を守る
注意事項をよくお読みください。製品全般の注意事項が記載されています。

●故障したら使わない
すぐに販売店まで修理をご依頼ください。

●万一異常が起きたら
- 煙が出たら
- 異常な音、においがしたら
- 内部に水・異物が入ったら
- 製品を高所から落としたり、破損したとき

① 電源を切る
② 接続ケーブルを抜く
③ 販売店に修理を依頼する

- 下記の注意事項を守らないと、火災・感電などにより死亡や大けがの原因となります。

●電源ケーブルや接続ケーブルを傷つけない
- 電源ケーブルを傷つけると火災や感電の原因となります。
- 重いものをのせたり、引っ張ったりしない。
- 加工したり、傷つけたりしない。
- 熱器具の近くに配線したり、加熱したりしない。

●内部に水や異物を入れない
- 火災や感電の原因となります。
- 万一、水や異物が入ったときは、すぐに電源を切り、販売店に点検・修理をご依頼ください。

●内部をむやみに開けない
・ 本体をむやみに開けたり改造したりすると、火災や感電の原因なります。

●落雷が発生したらさわらない
・ 落雷の恐れがあるときは、本製品や接続ケーブルに触らないでください。
感電の原因になります。

●油煙、湯気、湿気、ほこりの多い場所には設置しない
・ 火災や感電の原因となります。

- 下記の注意事項を守らないとけがをしたり周辺の物品に損害を与える原因となります。

●ぬれた手で触らない
・ 感電の原因となります。

●電源ケーブルは必ずΦ1.6mmまたはΦ2.0mmの単線ケーブル（VVFなど）を使用する（AE1021）
・ 規定のケーブルを使わないと、火災や感電の原因となります。

●指定の電圧で使う
・ AE1021の電源はAC100V（50/60Hz）で使用してください。

●コンセントや配線器具の定格を超えるような接続はしない
・ 発熱による火災の原因となります。

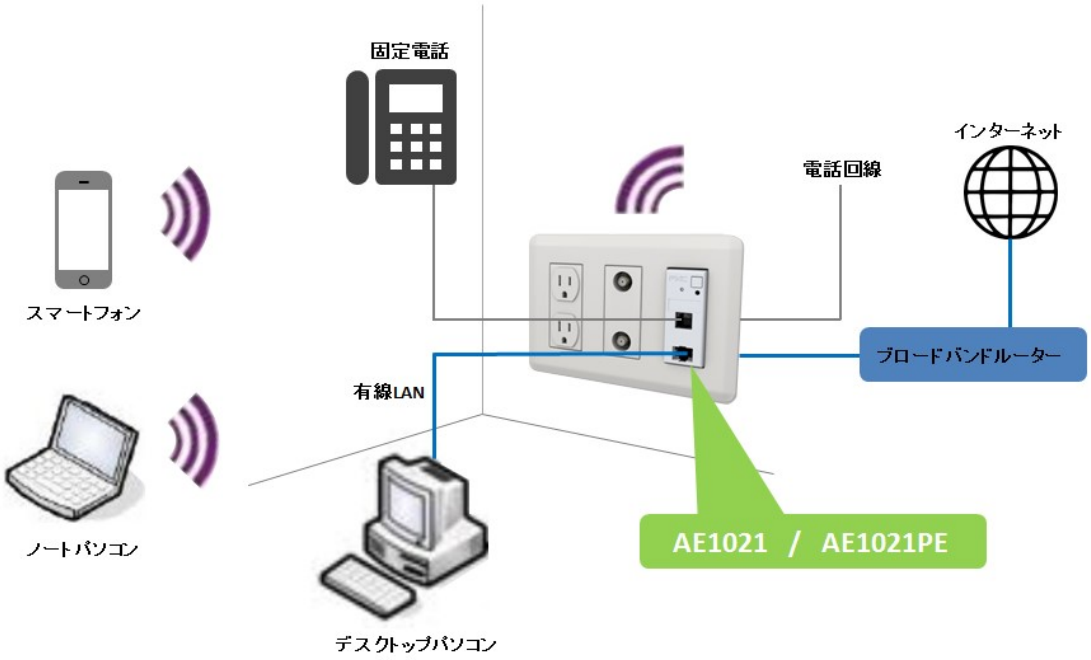
●通風孔をふさがない
- 通風孔をふさいでしまうと、内部に熱がこもり、火災や故障の原因となります。

●RJ45ポートには電話線コネクタを差し込まない
- RJ45ポートが損傷する場合があります。

目次

はじめに

AE1021/AE1021PEは、住宅・オフィス・会議室・病室・公共施設等の標準の情報コンセント内に埋込み、インテリア的にもすっきりとした、省スペースで快適な無線LAN環境を実現可能な小型無線アクセスポイントです。本体前面部には有線LANのRJ45インターフェースと電話回線に接続するRJ11のインターフェースも装備されています。また、給電方法として、AE1021がAC電源ケーブルによるAC100V給電タイプ、AE1021PEが上面RJ45 LAN(WAN)ポートへのPoE給電タイプとなっております。



- 本製品の特長 -

- 多彩なインタフェースを搭載
  RJ45インターフェース及びRJ11 のインタフェースを搭載し、無線 LAN 環境だけでなく、有線LAN による ネットワーク接続と固定電話の利用が可能。

- 高速ギガビットイーサネットに対応
  有線LAN の接続は、ギガビットイーサネット(1000BASE-T/100BASE-TX) 対応で高速で大容量通信が 可能。

- 柔軟な設置形態
  JIS規格のコンセントであればメーカを問わず設置可能。又、AC100V給電またはPoE給電に対応し、用途に合わせ機器を選択して設置可能。

ご使用になる前に

本製品を設置する上での注意点

- 本製品の設置方法については、本製品に同梱のインストレーションガイドをご覧ください。

- 本製品の設置にあたっては、必ず電気工事士の有資格者が行ってください。無資格者の設置作業によって発生した損害につきましては、当社は一切その責任を負いかねます。

最適な無線環境でお使いになるには、以下の点を考慮してください。

- 無線機器の動作距離については、本体を配置する上でそれらの環境の障害により影響をうけるため事前に定義することはできません。障害の原因としては、本製品間の信号を通過する壁および床の数、位置、厚さ、の他の障害が考えられます。

- RF ノイズを生成する他の電気製品および電化製品からの干渉を受ける場合があります。
  代表的なものとして、電子レンジおよびコードレス電話等が挙げられます。
  RF ノイズを発生する機器は本製品から 90cm 以上離してください。

おことわり

- 本製品の故障や不具合または停電や落雷などの外的要因で生じた通信機会損失による損害につきましては、当社は一切その責任を負いかねます。

- 本製品の仕様、機能については、ファームウェアのアップデートなどにより将来予告なく変更される場合があります。

1 章 PC の設定方法

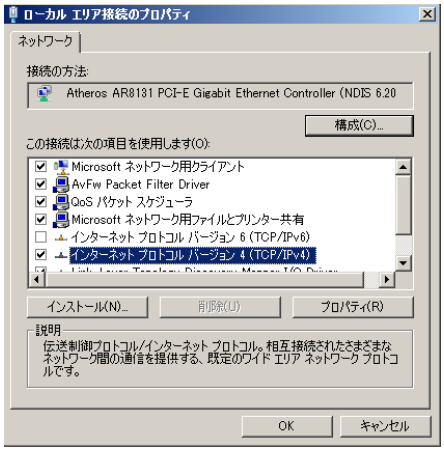
本機の設定を行う場合、お持ちの PC と本機の LAN ポート(上面 LAN(WAN)ポートまたは前面 LAN ポート)を LAN ケーブルで接続してください。
お使いの PC のネットワーク設定を下記の手順に従って行ってください。

IPアドレスを固定設定する場合:

下記の手順に従って PC の IP アドレスを設定してください。

1. 画面下の「ネットワークと共有センターを開く」を選択するか、「コントロールパネル」→「ネットワークと共有センター」をクリックして、「アダプタの設定の変更(画面左)→「ローカルエリア接続」を右クリックします。

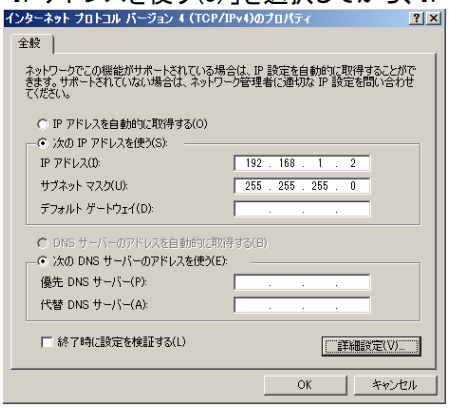
2. 「ローカルエリア接続のプロパティ」が表示されるためその中から「インターネット プロトコル バージョン 4 (TCP/IPv4)をクリックするとグレー表示され、右下の「プロパティ」がクリック可能になります。



画面 1:

4. <プロパティ(R)>ボタンをクリックすると下記の画面が表示されるため、それぞれ値を入力します。

【注記】:
デフォルト設定では、「IP アドレスを自動的に取得する(O)」が選択されているため、下記の画面のように「次の IP アドレスを使う(S)」を選択してから、IP アドレスとサブネットマスクの値を入力してください。



画面 2:

5. IP アドレスおよびサブネットマスクを入力して、<OK>ボタンをクリックします。

【注記】:
IP アドレスおよびサブネットマスクは同じサブネットの値に設定してください。
また、必要に応じてデフォルトゲートウェイの値を入力してください。

例:
お使いの PC の IP アドレス : 192.168.1.2 - 192.168.1.254
お使いの PC のサブネットマスク : 255.255.255.0

※但し、AE1021 本体の工場出荷時の設定は 192.168.1.253 です。
PC ではこのアドレスを使用しないでください。

6. 値を入力後、<OK>ボタンをクリックします。

2 章 Web 設定方法

ここでは、Web 設定画面による本体の設定方法について説明します。

お使いの PC のイーサネットポート、または無線 LAN アダプタと本製品を接続してください。

デフォルト設定値 ：

IPアドレス	**192.168.1.253**
ユーザ名/パスワード	**admin/admin**
オペレーションモード	**Bridge**
SSID名	**SSID1** **SSID2**

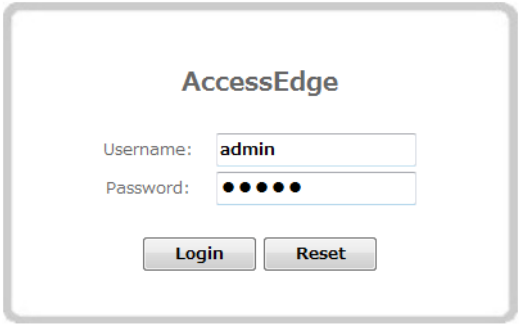
2.1 Web設定方法

1. Web ブラウザ(Internet Explorer/Firefox/Safari)を開いて、「IP アドレス:192.168.1.253」を入力します。

【注記】:
本体の初期設定の IP アドレスを変更する場合は、変更後の IP アドレスを入力してください。

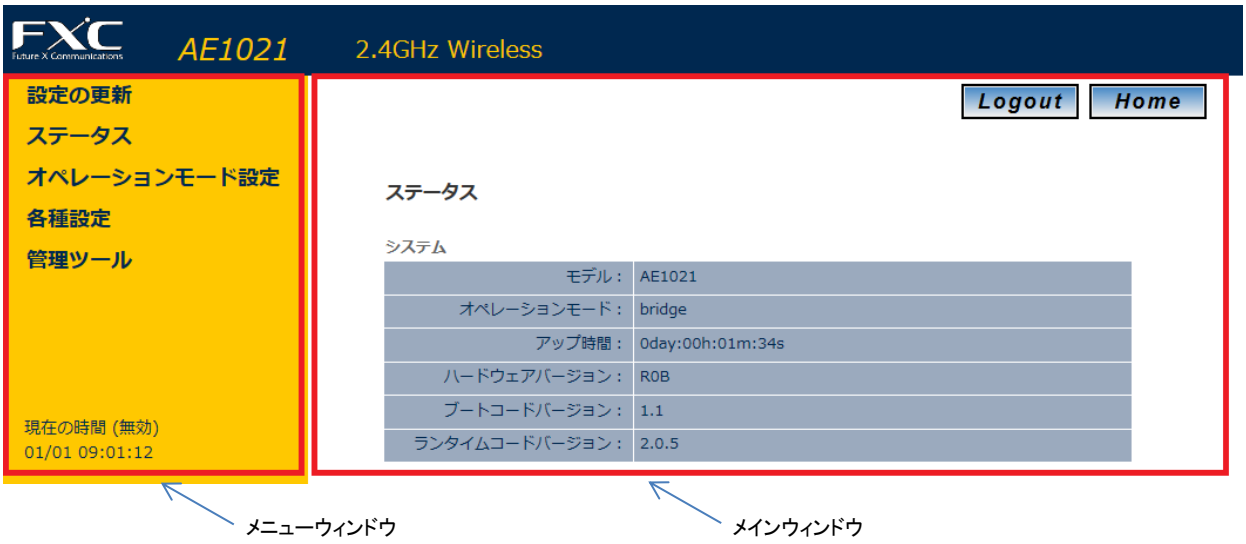
画面 3:

2. ユーザ名とパスワードを入力後に<login>ボタンをクリックすると、以下の画面が表示されますので、ユーザ名とパスワードをそれぞれ入力してください。
初期設定のパスワードは「admin」です。



画面 4:

4. ログインが正常に行われると、以下のメインメニューが表示されます。



メニューウィンドウ
メニューウィンドウでは、本製品でサポートされる各メニューがツリー状に表示されます。

メインウィンドウ
メニューウインドウで選択したメニューの設定項目、及びステータス情報を表示します。

Windows 7 をお使いの場合：

クライアントを接続する場合は、下記の手順に従ってください。

1. 画面下の「ネットワークと共有センターを開く」を選択するか、「スタート」→「コントロールパネル」をクリックして設定を行ってください。

「コントロールパネル」→「ネットワークと共有センター」をクリックしても設定可能です。

【注記】:
表示方法が「カテゴリ」表示でなく、「アイコン」表示になっている場合は、【ネットワークと共有センター】
 をクリックしてください。

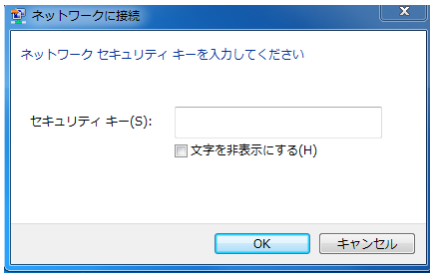
2. 「ネットワークに接続」をクリックします。
「現在の接続先」リストで近くにあるアクセスポイントが表示されます。

画面5:

3. リストからお使いの本体の無線接続を選択すると、以下の画面が表示されるため、リストからお使いの「ネットワーク名(SSID)」をダブルクリックしてください。

画面 6:

4. お使いの接続先の<接続(C)>ボタンをクリックすると、以下の「ネットワークに接続」が表示されます。

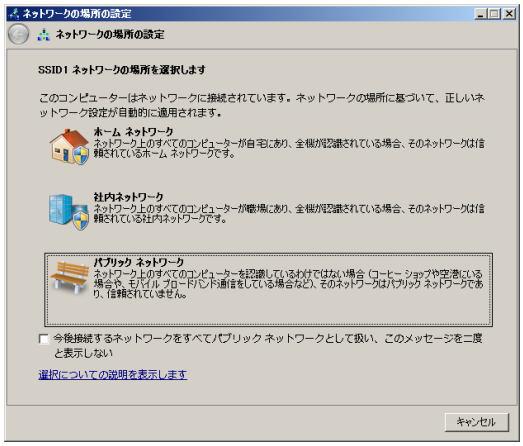


画面 7:

5. 「セキュリティキー」に値を入力し、[OK]をクリックします。

【注記】
セキュリティキーの値については、本機に設定したセキュリティキーを入力してください。
詳細については、「セキュリティ設定」の項を参照してください。

6. 「ネットワークの場所の設定」が表示されたら、「ホームネットワーク」をクリックします。



画面 8:

7. 正しく接続されているかどうかの確認をしてください。

【注記】: 画面右下の通知領域のアイコンをクリックし、「接続」になっていることを確認してください。

画面 9:

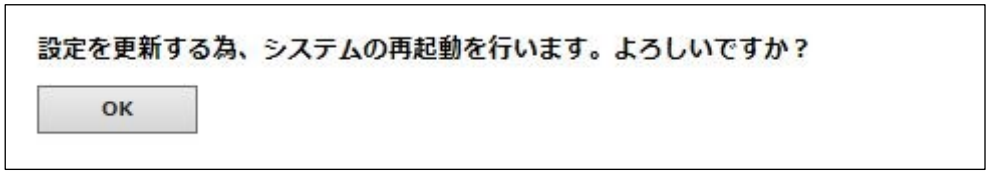
8. これで設定は完了です。

3 章　本機の設定方法

ここでは、本機の設定方法について説明します。

3.1 設定の更新

メニューウィンドウ左上の"設定の更新"タブをクリックすると、以下の画面が表示されます。
設定の変更を反映するためには、必ずこの画面で<OK>ボタンをクリックして、AP を再起動してください。

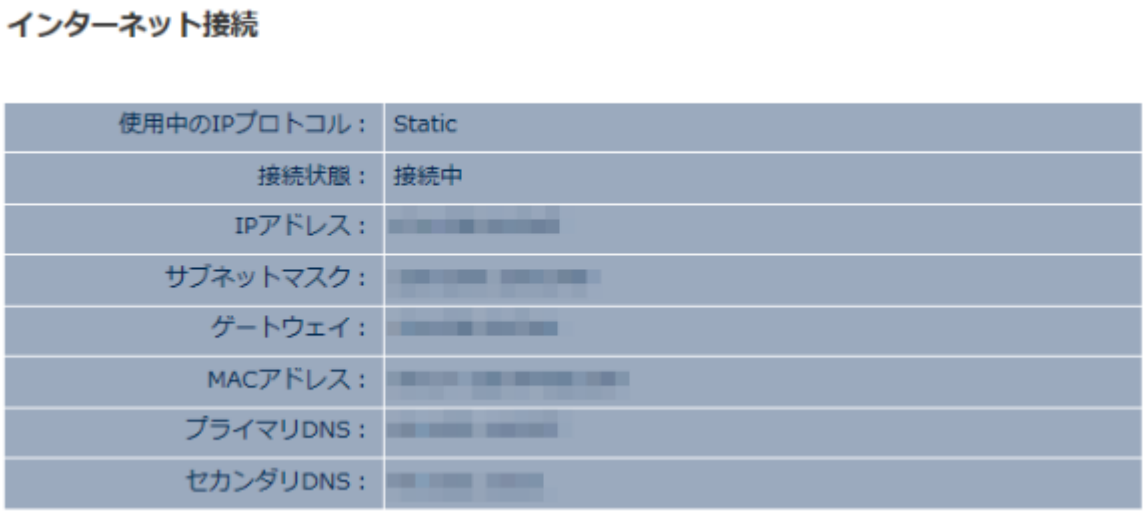


3.2 ステータス情報

「ステータス」情報メニューでは、現在のシステム設定、無線 LAN（WLAN）、LAN インタフェース、ステーションステータス、システムログの情報が表示されます。

3.2.1 インターネット接続

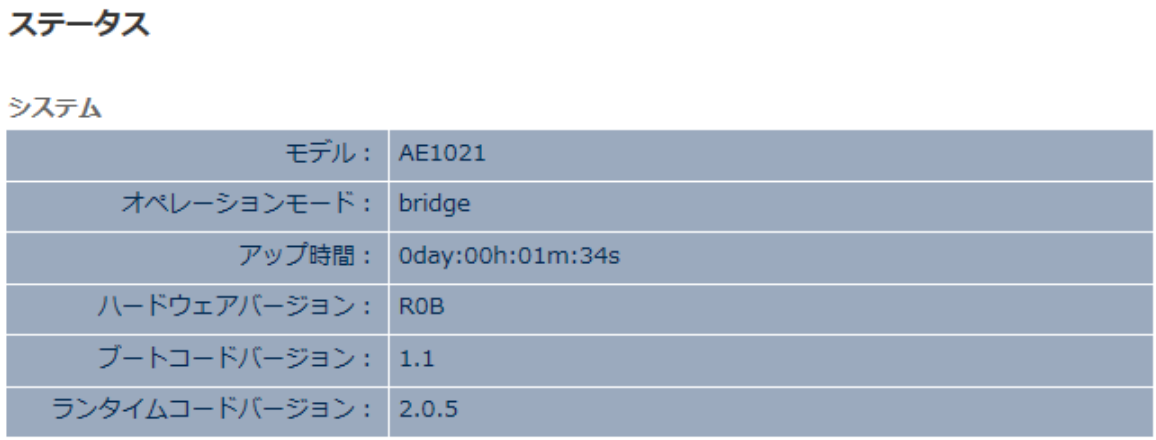
現在のインターネットの接続ステータスを表示します。



インターネット接続	
使用中のIPプロトコル:	Dynamic: DNSサーバは自動的に割り当てられます。 Static:DNSサーバは手動で割り当てられます。
IPアドレス:	WAN側のIPアドレスを表示します。
サブネットマスク:	WAN側のサブネットマスクを表示します。
ゲートウェイ:	WAN側のゲートウェイアドレスを表示します。
MACアドレス:	APのMACアドレスを表示します。
プライマリDNS:	プライマリドメインネームサーバのIPアドレスを表示します。
セカンダリDNS:	セカンダリドメインネームサーバのIPアドレスを表示します。

システム情報

「ステータス」画面では、AP のハードウェアおよびソフトウェアのバージョン番号、本体のモデル番号が表示されます。



システム	
モデル:	本体のモデル名
オペレーションモード	Bridge：本体がアクセスポイントモードで動作していることを示します。 Router：本体がRouterモードで動作していることを示します。
アップ時間:	再起動後の本体の稼働時間を表示します。
ハードウェアバージョン:	本体のハードウェアのバージョン番号を表示します。
ブートコードバージョン:	本体のブートコードのバージョン番号を表示します。
ランタイムコードバージョン:	現在のシステムのバージョン番号を表示します。

3.2.2 機器のステータス

「機器のステータス」画面では、AP の無線および LAN インタフェースの設定値が表示されます。

機器のステータス

無線設定

モード：		Access Point
無線機能：		有効
チャンネル：		自動 - (Current Channel is 6)
SSID1	ESSID：	SSID1
	機能：	有効
	セキュリティ：	WPA2PSK(mixed)
SSID2	ESSID：	SSID2
	機能：	有効
	セキュリティ：	WEP
SSID3	ESSID：	
	機能：	無効
	セキュリティ：	無効
SSID4	ESSID：	
	機能：	無効
	セキュリティ：	無効

LAN 設定

IPアドレス：	192.168.14.1
サブネットマスク：	255.255.255.0
DHCPサーバ：	有効
MACアドレス：	00:17:2E:9A:EE:BD

無線設定	
モード:	本体がアクセスポイントモードで動作していることを示します。
無線機能：	無線の状態（有効/無効）を表示します。
チャンネル:	無線クライアントと通信する際に使用される、AP用の無線チャンネル。「自動」に設定すると、APは使用されていない無線チャンネルを自動選択します。
SSID:	APに設定されているSSIDを表示します。お使いのデバイスをネットワーク接続する場合には、ここで表示されているSSIDと同じものを選択してください
機能:	無線の状態（有効/無効）を表示します。
セキュリティ:	SSIDの現在の無線セキュリティの設定が表示されます。
LAN 設定	
IPアドレス:	APのIPアドレスを表示します。
サブネットマスク:	IPアドレスのサブネットマスクを表示します。
DHCPサーバ:	APのDHCPサーバのステータスを表示します。
MACアドレス:	APのMACアドレスを表示します。

3.2.3 システムログ

AE1021/AE1021PE はログ処理を行い、内蔵メモリにメッセージを保存します。記録されたメッセージはデバイスやネットワークの障害を解析する上で大切な役割を果たします。
システムログ画面では、最新のメッセージが古い履歴から順に表示されます。

本体のメモリに保存されたログメッセージは、デバイスの再起動時に消去されます。

3.2.4 セキュリティログ

「セキュリティログ」画面では、最新のセキュリティメッセージが古い履歴から順に表示されます。本体のメモリに保存されたログメッセージは、デバイスの再起動時に消去されます。

3.2.5 無線アクセスログ

「無線アクセスログ」画面では、AP への無線アクセス履歴が古い順に表示されます。本体のメモリに保存されたログメッセージは、デバイスの再起動時に消去されます。

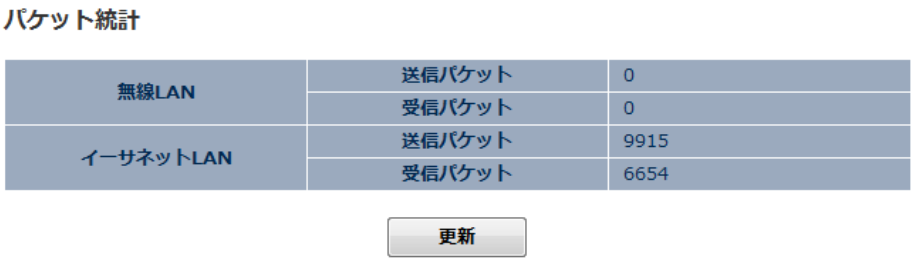
3.2.6 接続中のDHCPクライアント

「接続中の DHCP クライアント」画面では、本機に接続されているデバイスの MAC アドレスを確認したり、DHCP サーバにより IP アドレスが割り当てられているデバイスの MAC アドレスを確認したりすることができます。

接続先のDHCPクライアント	
IPアドレス	クライアントに割り当てられているIPアドレスを表示します。
MACアドレス	クライアントのMACアドレスを表示します。
制限時間（秒）	クライアントに割り当てられたIPアドレスの使用可能な時間(秒単位)

3.2.7 パケット統計

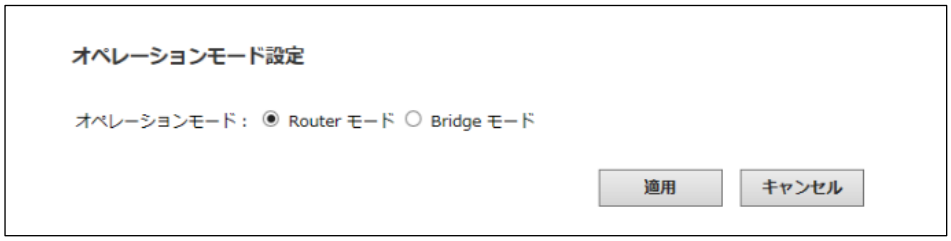
「パケット統計」画面では、WLAN および LAN インタフェースのネットワークトラフィックの統計情報が表示されます。



パケット統計	
無線LAN/送信パケット:	APの再起動後に無線LANインタフェースで送信されたパケット数を表示します。
無線LAN/受信パケット:	APの再起動後に無線LANインタフェースで受信したパケット数を表示します。
イーサネットLAN/送信パケット:	APの再起動後にLANインタフェースで送信されたパケット数を表示します。
イーサネットLAN/受信パケット:	APの再起動後にLANインタフェースで受信したパケット数を表示します。

3.3 オペレーションモード

この画面では、お使いのネットワーク環境に合うモードに設定します。



オペレーションモードの設定	
Routerモード	ケーブル、またはDSLモデムなど、インターネットアクセス装置に接続する無線LANおよび無線クライアントの接続モードを設定します。
Bridgeモード（アクセスポイントモード）	有線LANを無線クライアントに拡張するためのアクセスポイントモードを設定します。 工場出荷時では、「Bridgeモード」に設定されています。 【注記】: 「Bridge」モードを設定すると、有線/無線の設定は有効ですが、ルータ機能は無効となります。

上記のモードのいずれかを選択したら、<適用>ボタンをクリックしてください。

3.4 各種設定

「基本設定」メニューでは、システム設定、LAN 設定および無線 LAN の設定を行うことができます。

3.4.1 システム

「システム設定」メニューでは、タイムゾーンの設定、パスワードの設定、その他の管理の設定を行います。

1) タイムゾーン

AE1021/AE1021PE では、SNTP を使用してタイムゾーンを設定することができます。SNTP では、英国のグリニッジを通る地球の本初子午線（経度 0）を基準とする協定世界時が使用されます（協定世界時は、UTC と呼ばれるものであり、正式名称はグリニッジ標準時間（GMT））。デバイスの正確な時間を保持することにより、システムログはイベントエントリの日時を正確に記録します。

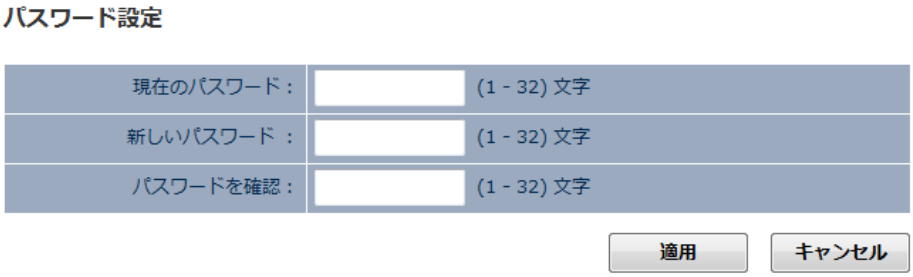
ローカルタイムに応じて現在の時刻を表示するには、お使いのタイムゾーンの設定を行ってください。

タイムゾーン	
タイムゾーン:	タイムゾーンを設定します。（デフォルト：GMT+09:00 Tokyo） タイムゾーンの設定を有効にするためには、タイムサーバアドレスを実在のサーバに設定する必要があります。
タイムサーバアドレス:	本体の時間設定を更新するためのタイムサーバアドレスを設定します。
夏時間設定:	夏時間設定の有効/無効を設定します。 「有効」にチェックを入れ、期間を設定すると、その期間の間本体の時間設定が1時間進んだ設定となります。夏時間設定を有効にする場合には、タイムサーバアドレスを実在のサーバに設定する必要があります。

2) パスワードの設定

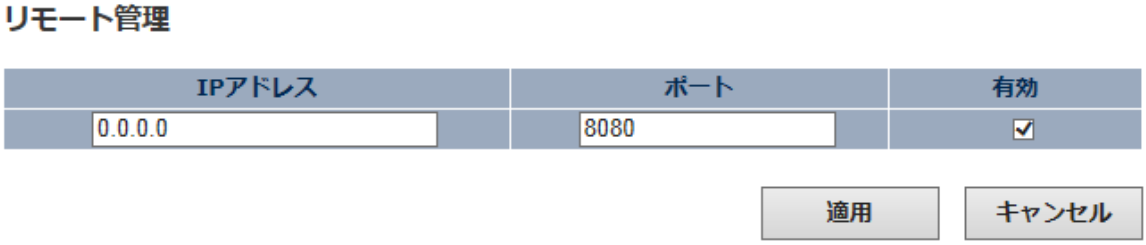
「パスワードの設定」画面では、AP の WEB ユーザインタフェースへの管理アクセスのパスワードの変更を行うことが可能です。

【注記】: パスワードに使用可能な文字は、大文字/小文字の英数字及び、アンダーバー "_"のみです。



パスワードの設定	
現在のパスワード:	現在の管理者用パスワードを入力します(デフォルト設定: admin)。
新しいパスワード:	新しい管理者用パスワードを入力します(有効範囲: 1-32文字)
パスワード確認:	確認用に新しいパスワードを入力します(有効範囲: 1-32文字)

3) リモート管理

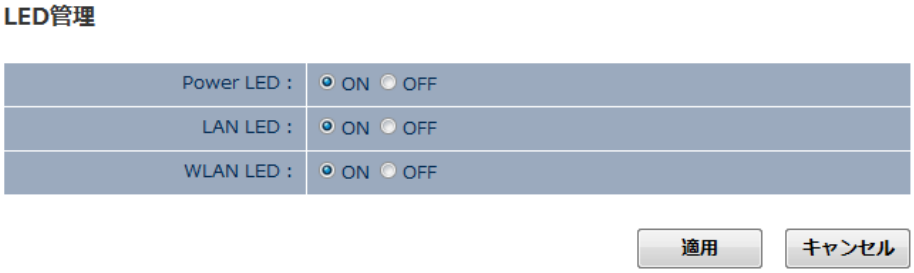


リモート管理	
IPアドレス:	リモートアクセスする端末のIPアドレスを設定します。 【注記】: リモートアクセス側の「グローバルIPアドレス」を設定してください。NATを越えたローカルIPアドレスを入力しても動作しません。 APに設定したLAN側IPアドレスと同じサブネットに属するIPアドレスは設定できません。
ポート:	WEBブラウザは、標準のHTTPサービスの「port 80」を使用します。AE1021/AE1021PEのデフォルトのリモート管理用のWEBポート番号は「8080」です。セキュリティを確保するために、リモート管理用のポート番号をボックスに入力することにより変更することが可能です。共通のサービスポートの番号を除く、「1～65534」までの番号を選択してください。
有効:	ここに、☑をいれると、リモート管理アクセス用のIPアドレスを有効にします。

【注記】:　AE1021/AE1021PE へのアクセスを行うには、お使いのブラウザのアドレスバーに AE1021/AE1021PE の WAN 側 IP アドレスを入力して、続けて、コロンとカスタムポート番号を入力して下さい。
例えば、AE1021 の WAN 側 IP アドレスに「202.96.12.9」、ポート番号に「8080」を使用する場合は、"http://202.96.12.9:8080"と入力します。AE1021 のパスワードが必要な場合は、AE1021/AE1021PE のユーザインタフェース用のユーザ名とパスワードを入力します。

4) LED 管理

「LED 管理」画面では、AP の LED の ON/OFF の切り替えを行います。



LED管理	
Power LED :	APのPower LEDを有効/無効にします。
LAN LED :	APのLANポートのLEDを有効/無効にします。
WLAN LED :	APのWLANポートのLEDを有効/無効にします。

5) スケジュール機能

「スケジュール機能」画面では、無線インタフェースの有効な時間を設定します。また、リセット時間を設定することも可能です。

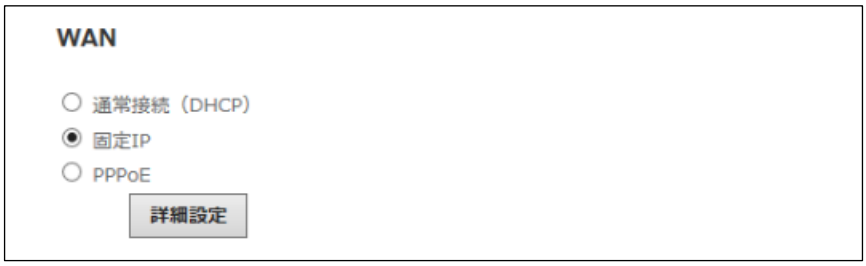
スケジュール機能	
Schedule Description :	スケジュールの種類について表示しています。 Wireless Active : 無線通信機能のスケジュール設定 Restart : 再起動のスケジュール設定
Service:	無線通信またはリセット時間のスケジュール設定を有効にします。
Days:	スケジュール機能が有効となる曜日を設定します。
Time of Day:	無線通信機能の場合は、APに接続可能な時間の範囲を設定します。 設定した場合、有効時間外にAPに無線接続をすることが出来なくなります。 リセットサービスの場合は、設定した時間にAPのリセットが行われるようになります。

3.4.2 WAN

ここでは、本機の WAN 接続について説明します。WAN 画面では、DHCP、固定 IP、PPPoE、DDNS および MAC アドレスのクローンなど、標準の WAN サービスの設定に使用します。

インターネットサービスプロバイダによって提供されている WAN 接続タイプ（通常タイプ（DHCP）、固定 IP、PPPoE）のいずれかを選択して、〈詳細の設定〉ボタンをクリックします。

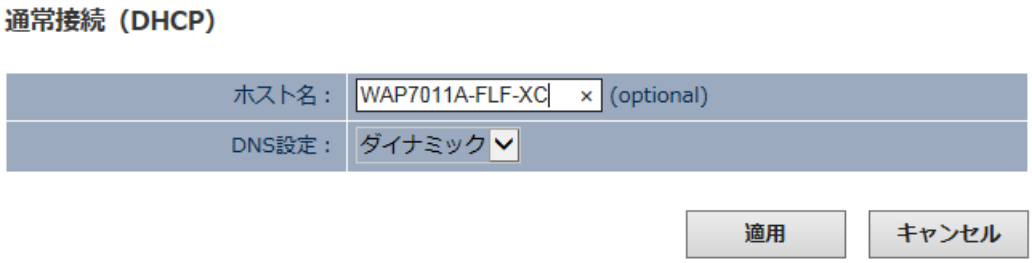
〈詳細設定〉ボタンをクリックすることで、選択した接続タイプの詳細設定画面へと遷移されます。



WAN接続タイプ	
通常接続（DHCP）:	WANポートのDHCPを有効にします。
固定IP:	WANポートの固定IPアドレスを設定します。
PPPoE:	WANポートのIPアドレスは、PPPoE(Point-to-Point Protocol over Ethernet)を使ってインターネットプロバイダによって割り当てられます。

1) 通常接続(DHCP)

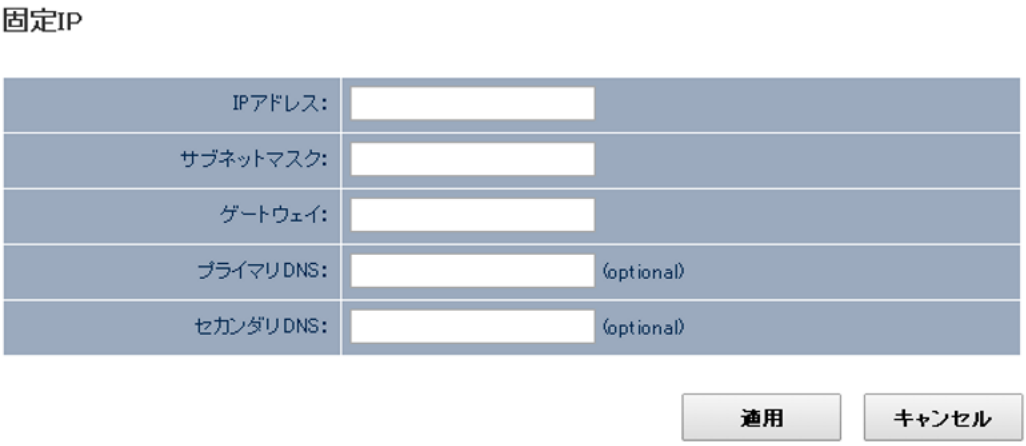
WAN ポートの DHCP 機能を有効にします。この設定により、AP は ISP で動作する DHCP サーバから IP アドレスを入手することが可能です。



DHCP接続	
ホスト名:	DHCPクライアントのホスト名。ホスト名はオプションですが、使用するISPによってはホスト名が必要になる場合があります。
DNS設定:	Dynamic：DNSサーバにより自動的に割り当てられます。 Static　：DNSサーバアドレスを手動で設定します。
プライマリDNS:	プライマリドメインネームサーバのIPアドレスを入力します。DNSは、数値で表すIPアドレスをドメイン名にマッピングし、IPアドレス以外の覚えやすい名前を使ってネットワークホストを識別するために使用します。DNSサーバを指定する場合は、テキストボックス内にIPアドレスを入力してください。それ以外は空欄のままにしてください。
セカンダリDNS:	セカンダリドメインネームサーバのIPアドレスを入力します。

2) 固定 IP

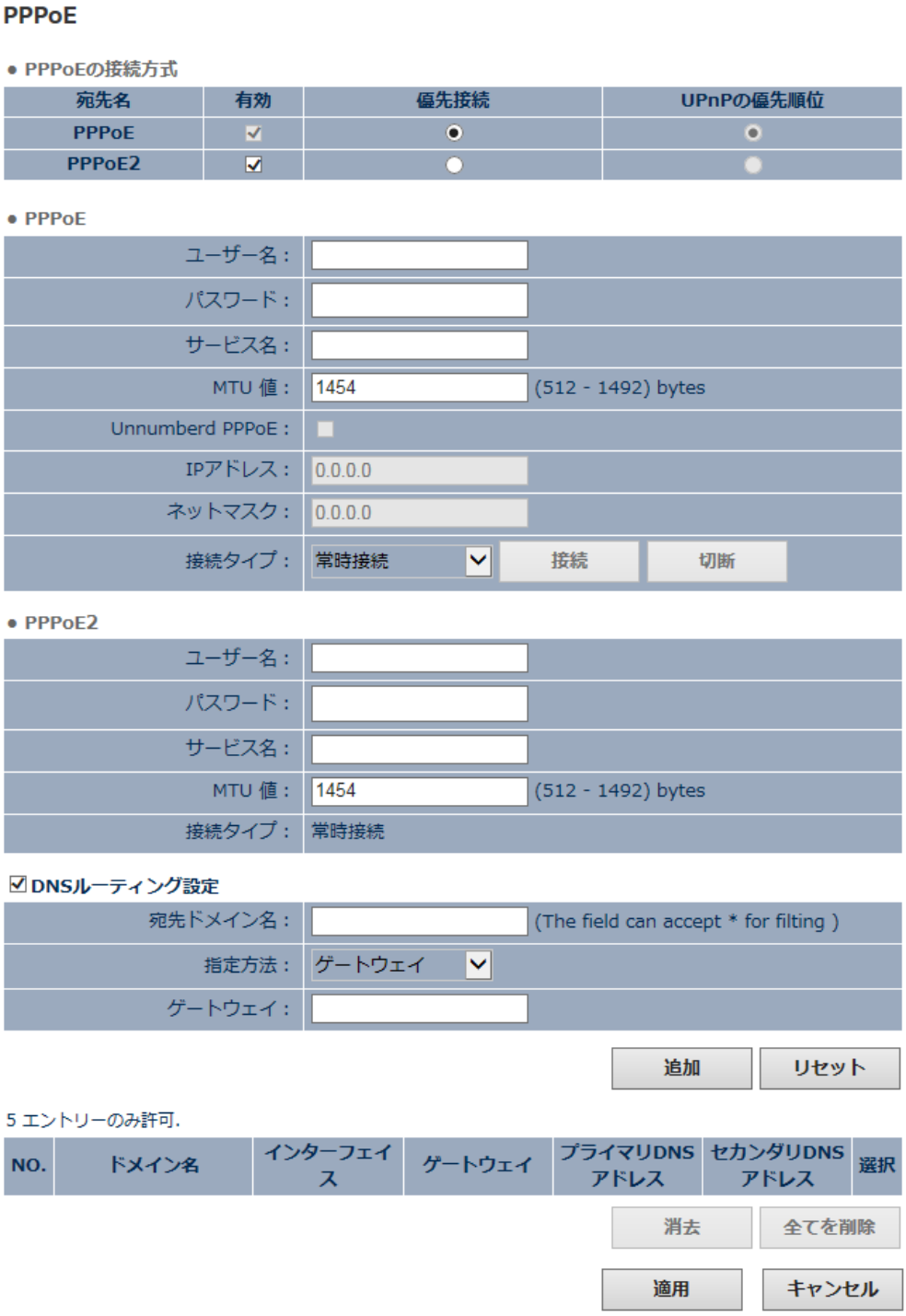
インターネットサービスプロバイダにより固定の IP アドレスを割り当てる場合は、本機に指定された IP アドレスおよびサブネットマスクを入力した後、お使いの ISP のゲートウェイアドレスを入力してください。



固定IP	
IPアドレス:	WAN側のIPアドレスを設定します。
サブネットマスク:	WAN側のサブネットマスクを設定します。
ゲートウェイ:	WAN側のゲートウェイアドレスを設定します。
プライマリDNS:	プライマリドメインネームサーバのIPアドレスを設定します。DNSは、数値で表すIPアドレスをドメイン名にマッピングし、IPアドレス以外の覚えやすい名前を使ってネットワークホストを識別するために使用します。DNSサーバを指定する場合は、テキストボックス内にIPアドレスを入力してください。それ以外は空欄のままにしてください。
セカンダリDNS:	セカンダリドメインネームサーバのIPアドレスを設定します。

3) PPPoE

WAN ポートの IP アドレスは、PPPoE を介して ISP により割り当てられます。
プライマリ/セカンダリ PPPoE インタフェースは両方とも設定することが可能です。

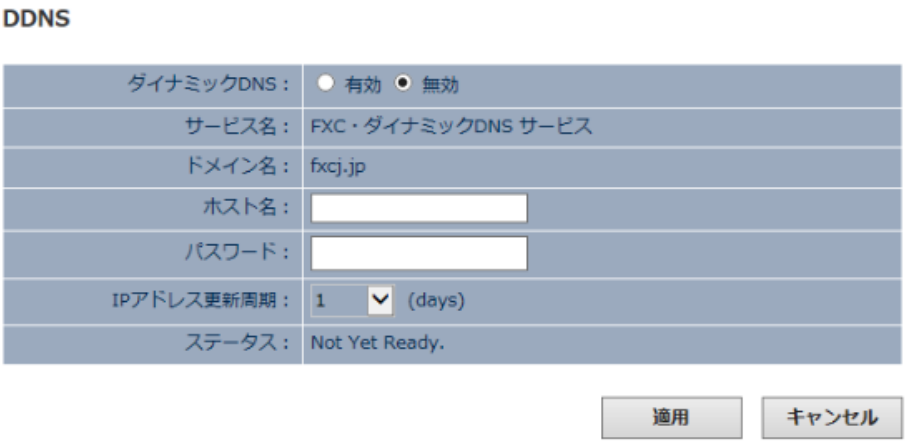


PPPoE	
PPPoE接続方式	
宛先名	PPPoE1インタフェースとPPPoE2インタフェースを表示しております。
有効	PPPoE1は、永続的に有効です。PPPoE2インタフェースは、有効/無効の切り替えができます。
優先接続	PPPoEインタフェースを設定して、プライマリ接続を行います。別のPPPoEインタフェースが有効な場合は、バックアップ接続として使用します。
UPnPの優先順位	UPnPを介して、アドバタイズ対象のPPPoEインタフェースを設定します。
PPPoE	
PPPoE	PPPoE1インタフェースの設定ができます。
ユーザ名:	WANポートのPPPoE1のユーザ名を設定します。
パスワード:	WANポートのPPPoE1のパスワードを設定します。
サービス名:	サービス名は通常オプションですが、サービスプロバイダによっては必要になる場合があります。サービス名により属性を設定し、ダイナミックPPPoEインタフェースを開始します。
MTU値:	ネットワークプロトコルにより送信可能な最大パケットのMTU(Maximum Transmission Unit)のサイズを設定します。
Unnumbered PPPoE:	一度に割り当てられるIPアドレスの範囲をリクエストします。固有のローカルアドレスが提供されていないpoint-to-pointインタフェースを指定します。例えば、ISPによりIPアドレスのブロックを割り当てる場合は、"Unnumbered PPPoE"を選択して、PPPoEインタフェースに対してLANに割り当てられた範囲と同じ値の中からIPアドレスを設定します。
IPアドレス:	PPPoE1インタフェースのIPアドレスを入力します。アドレスが固有のアドレスでない場合は、LANと同じネットワークの範囲内のアドレスを使用します。 通常、IPインタフェース間のルーティングを行う場合、異なるネットワーク番号をもつ必要があります。ただし、PPPoEのリンクの遠端が認識できるため、固有のIPアドレスは必要ありません。
ネットマスク:	PPPoE1インタフェースのサブネットマスクを設定します。
接続タイプ:	PPPoE1の接続モードを選択します。 ・常時接続: アクティビティに関係なく、インターネット接続を継続します。 ・オンデマンド接続 指定した非アクティブ(アイドルタイム)の経過後にインターネット接続を中断し、インターネットに再度アクセスする際に再度確立します。 ・手動接続: <接続>ボタン、および<切断>ボタンをクリックすると、直ちに接続/接続解除します。
Idle Time	操作が行われていない状態で、自動的にインターネット接続が切断されるまでの時間を分単位で設定します(有効範囲: 1 – 1000分)。
PPPoE2	
PPPoE2:	PPPoE2インタフェースの設定ができます。
ユーザ名:	WANポートのPPPoE2のユーザ名を設定します。
パスワード:	WANポートのPPPoE2のパスワードを設定します。
サービス名:	サービス名は通常オプションですが、サービスプロバイダによっては必要になる場合があります。サービス名により属性を設定し、ダイナミックPPPoEインタフェースを開始します。
MTU値:	ネットワークプロトコルにより送信可能な最大パケットのMTU(Maximum Transmission Unit)のサイズを設定します。
接続タイプ:	PPPoE2の接続モードは"常時接続"固定となっております。

Idle Time	操作が行われていない状態で、自動的にインターネット接続が切断されるまでの時間を分単位で設定します(有効範囲: 1 – 1000 分)。
DNSルーティング設定	
DNSルーティング設定	DNSルーティング機能は、DNSルーティングテーブルの該当エントリを参照することにより、DNSルーティングテーブル内のLANクライアントのDNSクエリを宛先に転送します。DNSクエリがルーティングテーブル内のエントリと一致しない場合は、デフォルトのルーティングの宛先に転送します。テーブル内の転送可能なエントリは最大5つまでです。
宛先ドメイン名:	ルーティングテーブルに追加するドメイン名の宛先を表示します。名前には、ワイルドカードの文字を使用できます。
指定方法:	宛先ドメインと一致するDNSクエリについては、クエリの伝送方式を指定します。 ■ インターフェース: 指定の PPPoE インタフェースを介して、プライマリ/セカンダリ DNS サーバに LAN クライアントの DNS クエリを伝送します。 ■ ゲートウェイ: 指定のゲートウェイ IP アドレスに LAN クライアントの DNS クエリを伝送します。
テーブルエントリ	
ドメイン名	ルーティングと一致する宛先ドメイン名を表示します。
インターフェイス	一致するDNSクエリのルーティングに使用するPPPoEインタフェースを表示します。
ゲートウェイ	一致するDNSクエリのルーティングに使用するゲートウェイのIPアドレスを表示します。
プライマリDNS	指定したPPPoE インタフェースのプライマリDNSサーバのIPアドレスを表示します。
セカンダリDNS	指定したPoE インタフェースのセカンダリDNSサーバのIPアドレスを表示します。
選択	エントリを選択する場合は、☑を入れて下さい。

4) DDNS

Dynamic DNS (DDNS)は、動的(ダイナミック)に割り当てられたユーザーのグローバル IP アドレスに対して、固定のドメイン名でつないでくれるサービスのことです。
DDNS により、IP アドレスを変更すると、DNS の記録は更新され、お使いのドメイン名の IP アドレスを自動的に対応します。この機能は、固定のドメイン名をもつウェブサイト、FTP サーバ(e-mail サーバ)へのホスティングを行う際に有用です。
ダイナミック DNS クライアントサービスには、登録されている「ホスト名」と「パスワード」が必要です。

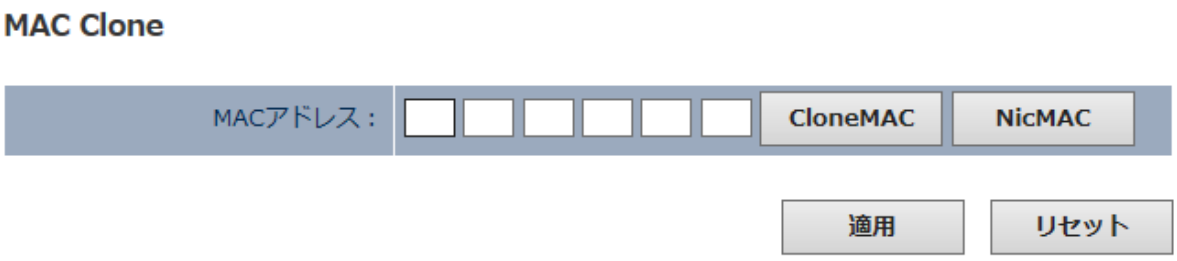


DDNS	
ダイナミックDNS:	DDNS機能を有効/無効にします。
サービス名:	DDNSサービス名は、“FXC · ダイナミックDNSサービス“と表示されます。
ドメイン名:	DDNSドメイン名は、 “fxcj.jp”と表示されます。
ホスト名:	DDNSクライアントサービスのアカウントユーザ名を入力します。
パスワード:	DDNSクライアントサービスのアカウントのパスワードを入力します。
IPアドレス更新時間:	ダイナミックIPアドレスをアップデートする頻度(日単位)を選択します(有効範囲: 1-30日)。
ステータス:	DDNSサービス接続の現在のステータスを表示します。

5) MAC Clone

CATV 回線など、ISP によっては MAC アドレス登録が必要な場合があります。
その場合、ISP に登録されている MAC アドレスと一致するように本機の WAN ポートの MAC アドレスを変更することができます。
ISP に登録している MAC アドレスを手動で入力する場合は、MAC アドレス欄に直接入力して<適用>ボタンをクリックします。また、本機に接続されているクライアント PC の MAC アドレスが既に登録済みの場合は、<CloneMAC>ボタンをクリックすることにより、その MAC アドレスを本機の WAN ポートの MAC アドレスとして設定することができます。
<NicMAC>ボタンをクリックすると、本機の元の MAC アドレスに戻ります。
何れも変更適用後に、メニューウィンドウ左上の「設定の更新」タブをクリックして、設定の更新を行ってください。

【注記】:
MAC Clone 機能については、お客様が契約されている ISP からの特別な指示が無い限り、通常は未設定としてください。



3.4.3 LAN側の設定

AE1021/AE1021PE は WEB ブラウザを使用して、設定の管理を行うため有効な IP アドレスを備えています。本体のデフォルトの IP アドレスは、「192.168.1.253」です。デフォルトの IP アドレスを使用するか、既存のローカルネットワークで使用可能な別のアドレスを割り当てることができます。ユニットは、DHCP(Dynamic Host Configuration Protocol)としても有効です。

AP には DHCP サーバが含まれ、このサーバによりサービスを要する接続先のホストに対して IP アドレスを一時的に割り当て可能となります。ユニット上に設定された共通のアドレスプールからのアドレスをクライアントに割り当てます。
アドレスのプールの範囲は、IP アドレスの最初と最後を指定することにより設定してください。
本体の IP アドレスについては、アドレスプールの範囲内に設定しないよう注意してください。

LAN側設定

● DHCPクライアント

IPアドレス：	192.168.1.253
サブネットマスク：	255.255.255.0

● DHCPサーバ

DHCPサーバ：	有効
リース時間：	48 days
開始IPアドレス：	192.168.1.100
終了IPアドレス：	192.168.1.200
デフォルトゲートウェイ：	◉ APのIPアドレスをデバイスに通知する ○ 指定のアドレスをデバイスに通知する ○ アドレスをデバイスに通知しない
DNSアドレス：	◉ APのIPアドレスをデバイスに通知する ○ 指定のアドレスをデバイスに通知する プライマリDNSアドレス： セカンダリDNSアドレス： ○ アドレスをデバイスに通知しない
ドメイン名：	○ 指定のアドレスをデバイスに通知する ○ アドレスをデバイスに通知しない
WINSサーバアドレス：	○ 指定のアドレスをデバイスに通知する プライマリWINSサーバアドレス： セカンダリWINSサーバアドレス： ◉ アドレスをデバイスに通知しない

● ポートセパレート

Separate(LAN with WiFi)：	☐ 有効

● 固定DHCPリーステーブル

16エントリーのみ許可.

NO.	MACアドレス	IPアドレス	選択
	None	----	

消去　全てを削除

☐ 固定DHCPリースを有効

MACアドレス	IPアドレス	
		追加　リセット

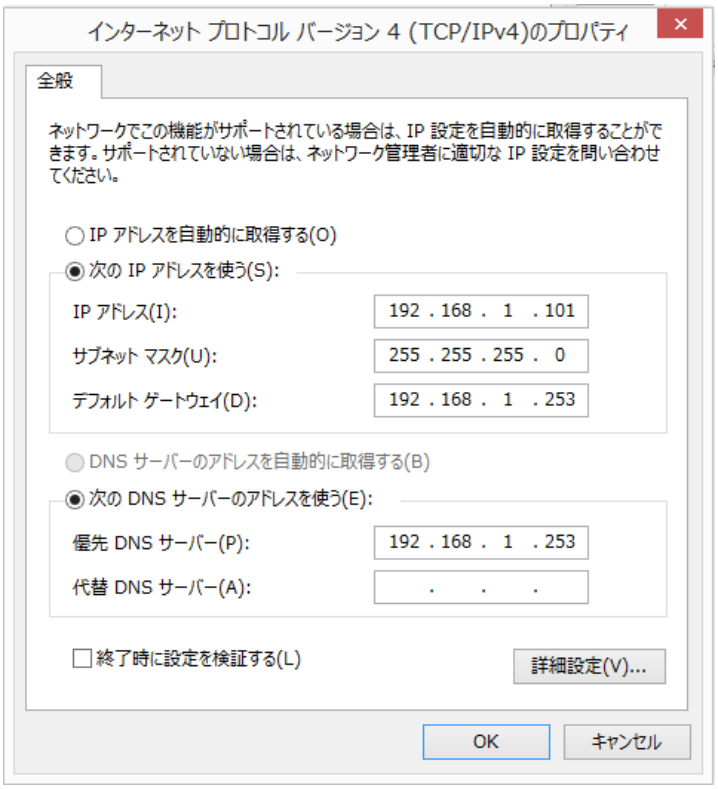
適用　キャンセル

LAN側設定	
DHCPクライアント	
IPアドレス:	APのIPアドレスを表示します。有効なIPアドレスは、0～255までのピリオドで区切られた4桁の10進数の値から構成されます。デフォルトの設定値は、「192.168.1.253」です。
サブネットマスク:	ローカルのIPサブネットマスクが表示されます。 デフォルトの設定値は、「255.255.255.0」です。
DHCPサーバ	
DHCPサーバ:	DHCPサーバを有効にします。有効に設定する場合は、アドレスプールおよびリースタイムを設定してください。
リース時間:	本装置全体のデフォルトリース時間（DHCPクライアントへのIPアドレスのリース時間）を指定します。
開始/終了IP Address	DHCPサーバによりDHCPクライアントに割り当て可能な範囲内の最初と最後のIPアドレスを設定します。アドレスプールの範囲は、本体のIP設定と同じサブネット内にあります。本体でサポート可能なクライアント数の上限値は「253」です。
デフォルトゲートウェイ:	コンピュータや通信機器などのネットワーク設定の一つで、送信相手までの経路がわからない場合にデータを送信する中継機器のIPアドレスです。指定のアドレスをデバイスに通知する場合には、空欄にIPアドレスを入力してください。
DNSアドレス:	ネットワーク上のDNS(Domain Name Server)のIPアドレスです。指定のIPアドレスをデバイスに通知する場合は、通知先のプライマリDNSアドレス、セカンダリDNSアドレスをそれぞれ設定してください。
ドメイン名:	DNS(Domain Name Server)により、IPアドレスをドメイン名にマッピングし、IPアドレス以外の名前でネットワークホストを識別することができます。ローカルネットワーク上にDNSサーバがある場合は、空欄にIPアドレスを入力してください。
WINSサーバアドレス:	Windowsインターネット ネーム サービス (**WINS**) **サーバー**は、コンピュータ名 (NetBIOS名) に動的にIPアドレスをマッピングします。これにより、ユーザーはIPアドレスではなくコンピュータ名でリソースにアクセスできるようになります。 指定のアドレスをデバイスに通知する場合は、プライマリWINSサーバアドレス/セカンダリWINSサーバアドレスをそれぞれ入力してください。
ポートセパレート	
Separate(LAN with WiFi):	チェックを入れることで、AP本体前面のLANポートの通信と、無線の通信が分離され、相互に通信が出来なくなります。 【注記】:LANポートの通信速度が最大200Mbpsに制限されます。
固定DHCPリーステーブル	
固定DHCPリーステーブル:	DHCPアドレスプールからのスタティックIPアドレスをDHCPクライアントのMACアドレスにマッピングします。最大16エントリまで登録可能です。
NO.:	テーブルのインデックス番号を表示します。
MACアドレス:	DHCPクライアントのMACアドレスを表示します。
IPアドレス:	特定のMACアドレスに割り当てるDHCPアドレスプールからのIPアドレスを表示します。
選択:	個々に選択したDHCPスタティックアドレステーブルのエントリを有効にします。<消去>ボタンをクリックすると、テーブルから選択したエントリを削除します。
□固定DHCPリースを有効	
固定DHCPリースを有効:	このフィールドに☑を入れて、スタティックのDHCPリースを有効にします。
MACアドレス:	DHCPクライアントのMACアドレスを入力します。文字列の中は、空白のままにしたり、特殊な文字を使用しないでください。

IPアドレス:	DHCPアドレスプールの中からIPアドレスを入力して、該当のMACアドレスに割り当てます。

【注記】:　AP の DHCP サーバの機能を使用するには、すべてのパソコンの IP 設定を「自動的に取得する」モードに設定してください。

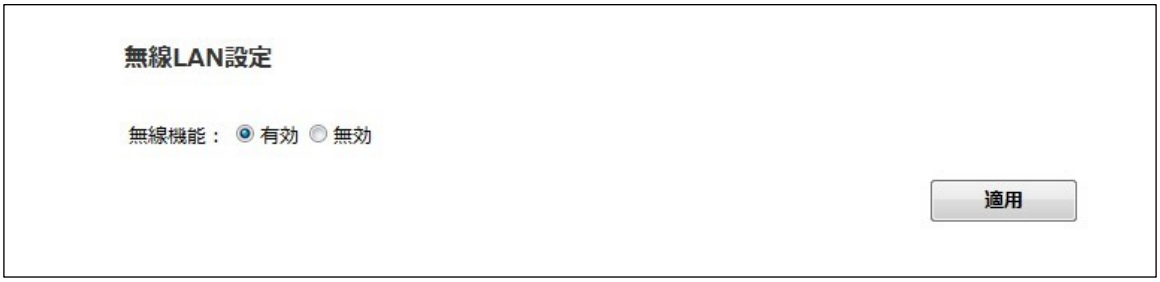
【注記】:　パソコンの IP アドレスを固定で使用する場合は、下図を参照し「優先 DNS サーバ(P):」に AP の管理 IP アドレスを入力してください。



3.4.4　無線LAN設定

このメニューでは、AP の無線インタフェースを有効にします。

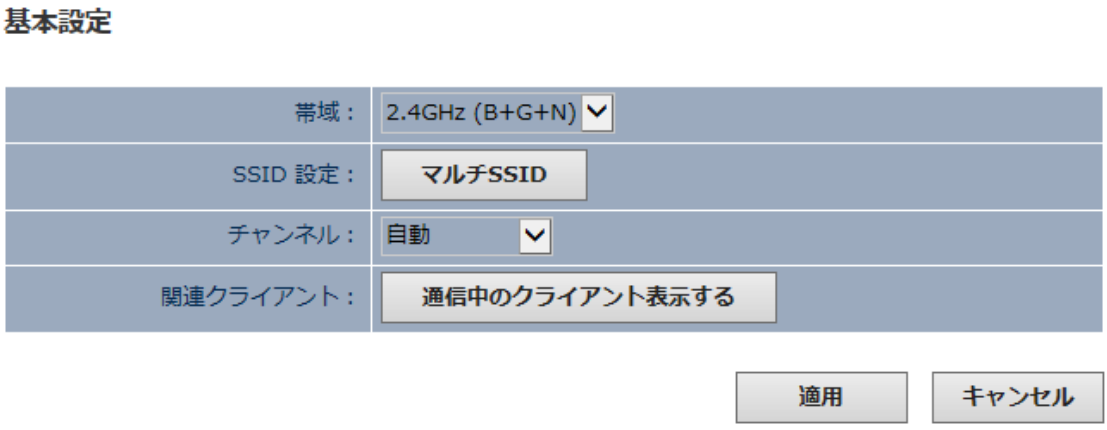
AE1021/AE1021PE には、ローカルの Wi-Fi 通信用の 2.4GHz の IEEE 802.11n の無線インタフェースが含まれます。「無線 LAN 設定」画面では、無線通信やセキュリティに関して設定することができます。



1) 基本設定

ここでは、「基本設定」メニューをクリックして、本体の Wi-Fi 無線インタフェース用の基本設定を行うことが可能です。本体の無線は、「802.11b only」、「802.11g only」、「802.11n only」、「802.11b/g mixed」、「802.11b/g/n mixed」の 5 つのモードから選択できます。

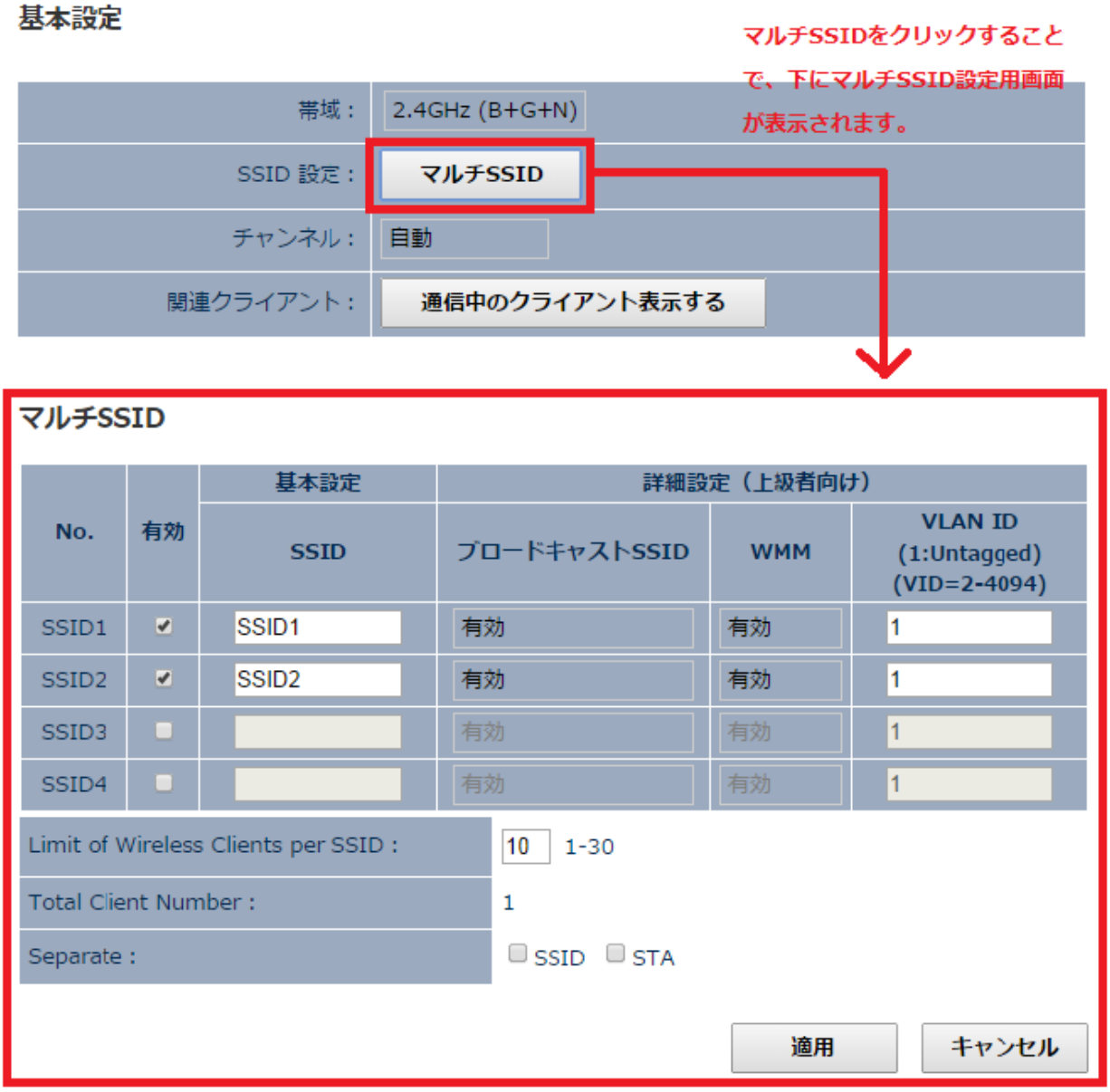
【注記】:「802.11g」は 802.11b、「802.11n」は 802.11b/g とそれぞれ低速のデータ転送率で上位互換性があります。



WLAN基本設定	
帯域:	無線の動作モードを設定します。 ■11b only: 802.11b, 802.11g および 802.11n クライアントはすべて、Wi-Fi 無線との通信が可能ですが、 802.11g および 802.11n クライアントは 802.11b プロトコルおよびデータ通信速度 (11 Mbps まで)に制限されます。 ■11g only: 802.11g および 802.11n クライアントは共に Wi-Fi 無線との通信が可能ですが、802.11n クライアントは 802.11g プロトコルおよびデータ通信速度 (最大 54Mbps まで)に制限されます。どの 802.11b クライアントも Wi-Fi 無線との通信は不可能です。 ■11n only: 802.11n クライアントのみ Wi-Fi 無線との通信が可能です(最大 150Mbps まで)。 ■11b/g mixed: 802.11b および 802.11g クライアントは、両方とも Wi-Fi 無線との通信は可能ですが、802.11g についてはデータ通信速度が低速になる場合があります。 ■11b/g/n Mixed: 802.11b/g/n クライアントはすべて Wi-Fi 無線との通信が可能(最大 150 Mbps まで)ですが、802.11b/g についてはデータ通信速度が低速になる場合があります。
SSID設定:	ボタンをクリックすると、SSIDインタフェースを設定します(以下参照ください)。
チャンネル:	APの無線チャンネルを、1～13から選択します。 "自動"を選択すると、APは使用されていない無線チャンネルを自動で選択します。
関連クライアント:	<通信中のクライアント表示する>ボタンをクリックすると、現在APに接続されている端末の情報を確認することが出来ます。

SSID 設定

AE1021/AE1021PE は、最大 4 つの SSID インタフェースをサポートしています。それぞれの SSID は異なるアクセスポイントとして機能し、それぞれ個別に SSID およびセキュリティを設定可能です。ただし、ほとんどの無線機能の設定はすべての SSID インタフェースに共通して適用されます。指定した SSID での通信を、他の SSID での通信から隔離することが可能です。物理的に異なるアクセスポイントをもつ場合は、クライアントは同じ方法で各 SSID に接続されます。AE1021/AE1021PE は、SSID インタフェースごとにサポート可能な無線クライアントは、最大「30」までです。

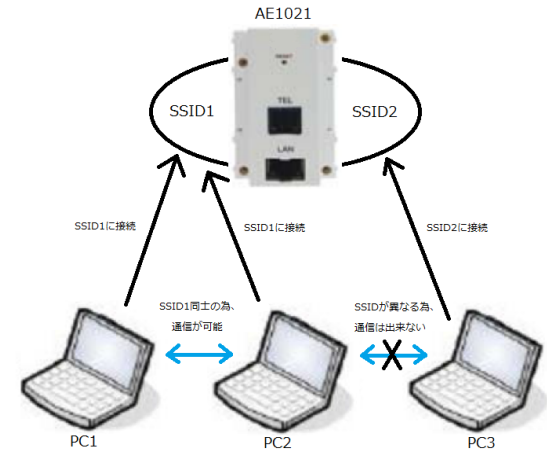


マルチSSID	
No.	SSIDインタフェース番号
有効	☑をクリックして、SSIDインタフェースを有効にします。
SSID	SSID名を設定します（有効範囲: 1-32 文字）。 SSID名については、1-32文字の範囲内で英数字を入力して設定します。 変更完了後、<適用>ボタンをクリックした後<設定の更新>ボタンをクリックして設定を確定してください。

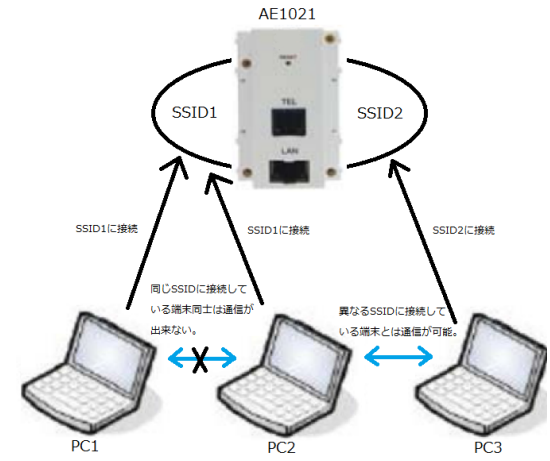
ブロードキャストSSID	SSIDのブロードキャストの有効/無効を設定します(デフォルト:有効)。 SSIDブロードキャストを無効にすると、無線クライアントは接続する前にSSIDを認識する必要があるため、ネットワークのセキュリティが高くなります。
WMM	WMM機能の有効/無効を設定します(デフォルト:有効)。この機能を有効にすることで、APはトラフィックに優先度付けを行い、通信のパフォーマンスを最適化します。 SSIDインタフェースでは、この機能を有効にすることをお勧めします。
VLAN ID	VLAN ID 1はタグなしVLANとなります。 2-4094を設定すると、WANポート側では自動的に2-4094に対応したTagをつけて送出します。 この際、WANポート側では設定する項目はありません。 SSIDにVLAN IDを設定するだけで、自動的にWANポート側でのTag通信が可能となります。 ※APがルーターモードの状態では、VLAN IDを設定することはできません。
Limit of Wireless Clients per SSID:	各SSIDに接続できるクライアントの上限数を設定します。SSIDにつき上限値は「30」となります(有効範囲: 1 - 30;デフォルト10)。
Total Client Number:	APに接続されているクライアントの合計数を表示します。
Separate:	この機能は、SSIDおよびクライアントのトラフィックを相互に分離します。この機能はデフォルトの状態では無効となっております。 ■ SSID: 「Separate SSID」が有効の場合、同じ SSID に接続されているクライアント同時の通信は可能ですが、異なる SSID に接続されているクライアントとの通信が出来なくなります。 ■ STA: 「Separate STA」が有効の場合、同じ SSID に接続されているクライアント同士の通信が出来なくなります。

■Separate SSID/STA を設定した場合の動作の例を以下に示します。

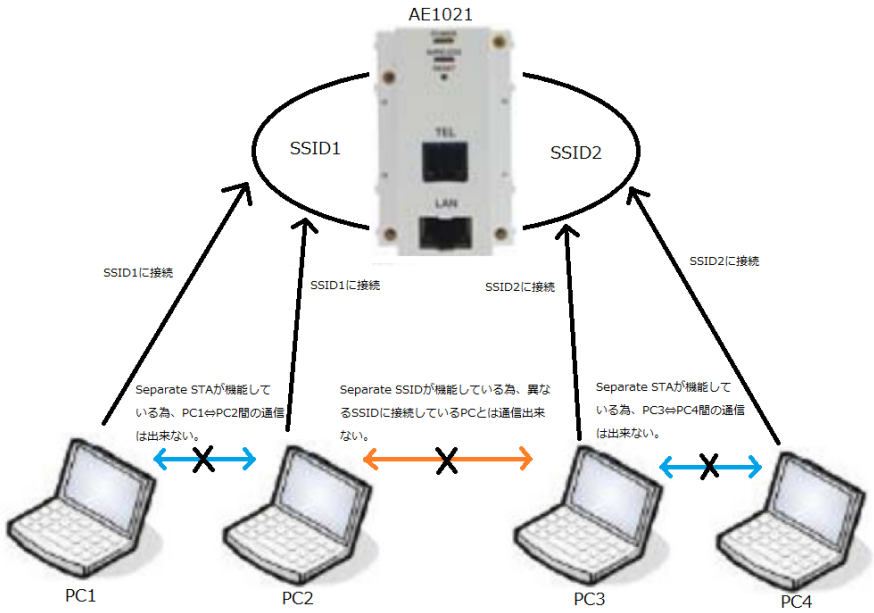
●Separate SSIDを設定している状態での通信



●Separate STAを設定している状態での通信



●Separate SSID及びSeparate STAが両方機能している状態での通信



■無線－前面LANポート間のセパレート機能については、LAN側設定メニューにてポートセパレートの有効/無効を設定いただけます。本書28～29ページを御参照ください。

2) 通信中の無線クライアントテーブル

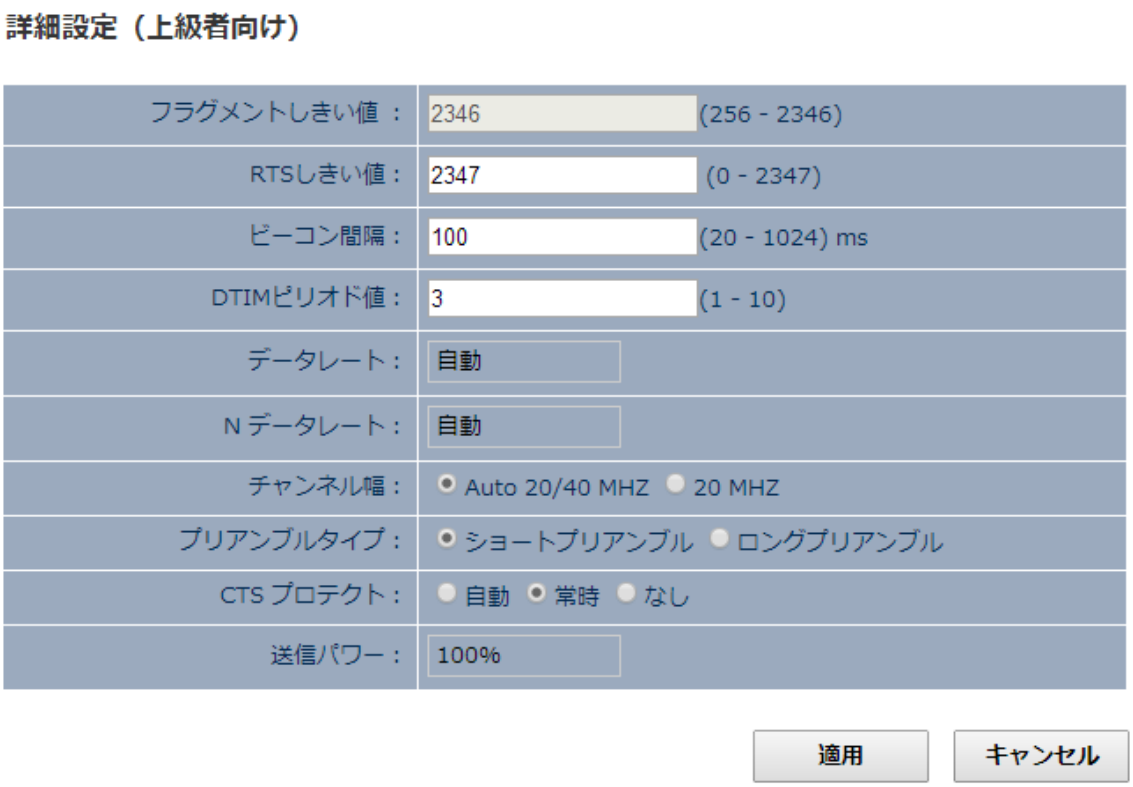
無線LAN設定の「基本設定」画面から、<通信中の無線クライアントテーブル>メニューをクリックすると、APに現在接続されているクライアントの情報が表示されます。

通信中の無線クライアントテーブル	
MACアドレス	APに接続されているクライアントのMACアドレスを表示します。
802.11 Phyモード	クライアントによりサポートされている「802.11b」、「11g」、「11n」モードを表示します。
Tx Packet	クライアントのパケット送信数の合計を表示します。
Rx Packet	クライアントのパケット受信数の合計を表示します。
Tx Rate (Mbps)	クライアントの現在の送信データの通信速度を表示します。
Expired Time (s)	クライアントがAPに接続してからの経過時間を表示します。

3) 詳細設定(上級者向け)

無線 LAN の「詳細設定(上級者向け)」画面では、AE1021/AE1021PE の無線インタフェースの詳細な設定を行うことが可能です。

この設定は、上級者向けです。パラメータの変更等の詳細について習熟していない場合は、デフォルト値のままでお使いになることをお勧めします。

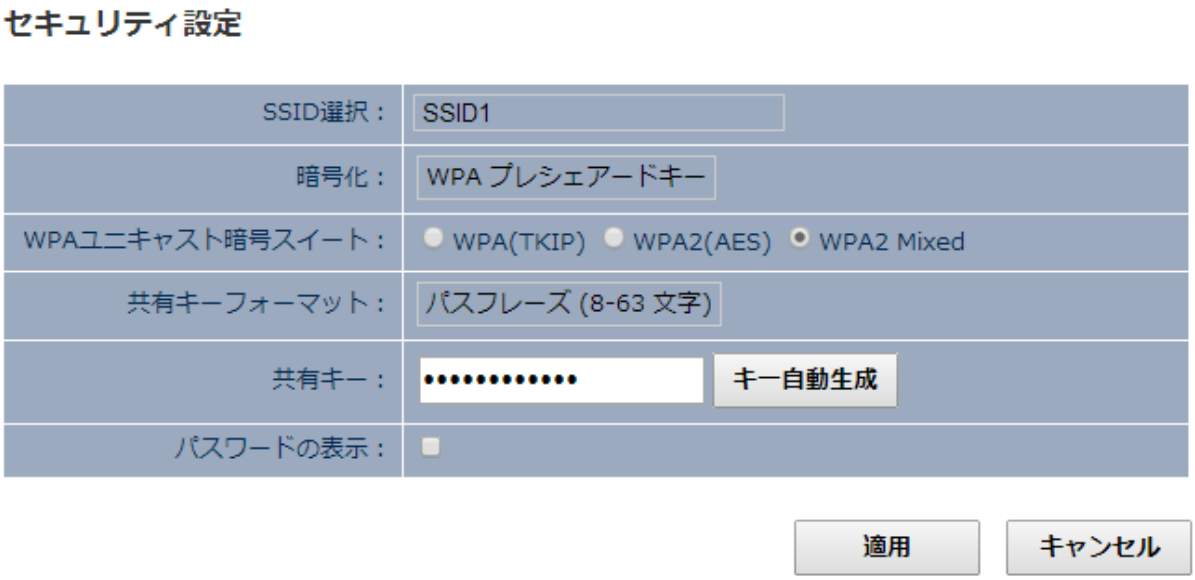


詳細設定(上級者向け)	
フラグメントしきい値:	AE1021/AE1021PEを通過時の分割可能なパケットサイズの下限値を設定します。PDFのフラグメント化は、フレームサイズを小さく分割することによりデータ伝送がよりスムーズに行われるため、通信の信頼性を高めることが可能です。 強力な干渉を受けた場合やネットワークの高使用率によるコリジョンが生じた場合は、分割するサイズを設定して、より小さく分割して送信します。これにより、より小さいフレームの再送信時間の速度が上がりますが、複数のフレームの送信により多くの負荷がかかるため、通常の場合(強力な干渉等がない場合)は分割サイズを大きい値に設定してください(有効範囲: 256-3.246 bytes; デフォルト:2346 bytes)。
RTS しきい値:	送信側への通信を開始する前に、受信側にRTS信号を送る際のパケットサイズの閾値を設定します。 AE1021/AE1021PEは、RTSフレームを受信側に送信して、データフレームの送信を行います。ステーション側はRTSフレームを受信後、CTS(clear to send)フレームを送信して、データ送信が開始可能な状態にあることを送信側に通知します。 RTSの閾値を「0」に設定すると、AE1021/AE1021PEはRTS信号を送信します。閾値を「2347」に設定すると、AE1021/AE1021PEはRTS信号を送信しません。その他の値に設定し、かつパケットサイズがRTS閾値以上超えると、RTS/CTS (Request to Send / Clear to Send)方式が有効となります。 AE1021/AE1021PEは相互に干渉を行いません。RTS/ CTS 方式では“Hidden Node Problem(隠れ端末問題)”を解決することが可能です(有効範囲: 0-2347bytes:、デフォルト: 2347 bytes)。
ビーコン間隔:	AE1021/AE1021PEからのビーコン信号の送信速度。ビーコン信号により、無線クライアントはAE1021/AE1021PEとの通信を継続し、また電源管理情報を伝送します(有効範囲: 20-1024ms、デフォルト:100ms)。

DTIMピリオド値:	ビーコン間隔に対して、どの程度の割合でDTIMを送信するかを設定します。DTIM(Delivery Traffic Indication Map)間隔とは、MACレイヤのブロードキャスト/マルチキャストトラフィックの転送速度を示します。パワーセーブモードを使用しているステーションを起動させる必要があります。デフォルトの「3」は、BSS(Basic Service Set)のブロードキャスト/マルチキャストフレームをすべて保存し、3ビーコン間隔で転送することを示します。 DTIM間隔を短くすると、ブロードキャスト/マルチキャストフレームを等間隔で送信させることにより、パワーセーブモードのステーションは頻繁に起動を行ったり、、より早く電流を排出したりします。DTIMの値を高くすると、パワーセーブモードのステーションで使用する電流を軽減しますが、ブロードキャスト/マルチキャストフレームの送信に遅延が生じます(有効範囲: 1-10ビーコン; デフォルト: 3ビーコン)。
データレート:	無線インタフェース上でAE1021/AE1021PEのパケット転送用の802.11b、または802.11gのデータ通信速度の最小値(オプション: 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54 Mbps, または自動; デフォルト: 自動)。
Nデータレート:	無線インタフェース上でAE1021/AE1021PEのパケット転送用の802.11nシングルストリームデータ通信速度の最小値。MCS(Modulation and Coding Scheme)は、モジュレーション、コーディング、使用するチャンネル数を決定します (有効範囲: MCS0-MCS7、または自動 ; デフォルト:自動)。
チャンネル幅:	Wi-Fi無線では、デフォルト設定では20 MHzのチャンネルの帯域幅を保持し、802.11bデバイスを低速で上位互換性を確保します。 「Auto 20/40 MHz」に設定すると、ネットワークのクライアントに応じて「20MHz」または「40 MHz」のいずれかを選択します(オプション: Auto 20/40 MHz、または20 MHz; デフォルト: 20 MHz)。
プリアンブルタイプ:	プリアンブルは、無線通信の最初の部分です。これにより、受信側はデータを送信前にトランスミッタとの同期を取ることが可能になります。802.11プリアンブルは、「ロング」または「ショート」に設定します。ショートプリアンブルの場合はパフォーマンス全体が高くなります。無線装置をネットワークで使用する場合はロングプリアンブルに設定する必要があります。
CTSプロテクト:	802.11bクライアントの上位互換性の保護機能を設定します。保護機能が有効な場合は、802.11g/nクライアントのスループットは約50%下がります。 ここでは、以下のように3つのモードが設定可能です(デフォルト設定: 常時)。 ■ **自動**: 802.11b クライアントがネットワーク上で検出されると、保護方法が有効になります。802.11b クライアントが検出されない場合は、保護方法は無効になります。 ■ **常時**: 802.11b クライアントの保護方法は常に有効です。 ■ **なし**: 802.11b クライアントの保護機能を強制的に無効にします。
送信パワー:	AE1021/AE1021PEから送信された無線信号の出力を調整します。 出力を設定して、無線信号が対象のサービスエリア外に広がらないよう出力を設定します。 設定範囲は: 5%, 10%, 25%, 50%, 100% (デフォルト: 100%)から選択します。

セキュリティ設定

AE1021/AE1021PE は各種のセキュリティ機能をサポートしています。このセキュリティ機能には、ネットワークの要件に応じて各レベルごとに認証および暗号化を行います。AE1021/AE1021PE にはそれぞれ異なるアクセスポイントとして機能する 4 つの SSID インタフェースを備え、それぞれ異なるセキュリティを設定することが可能です。



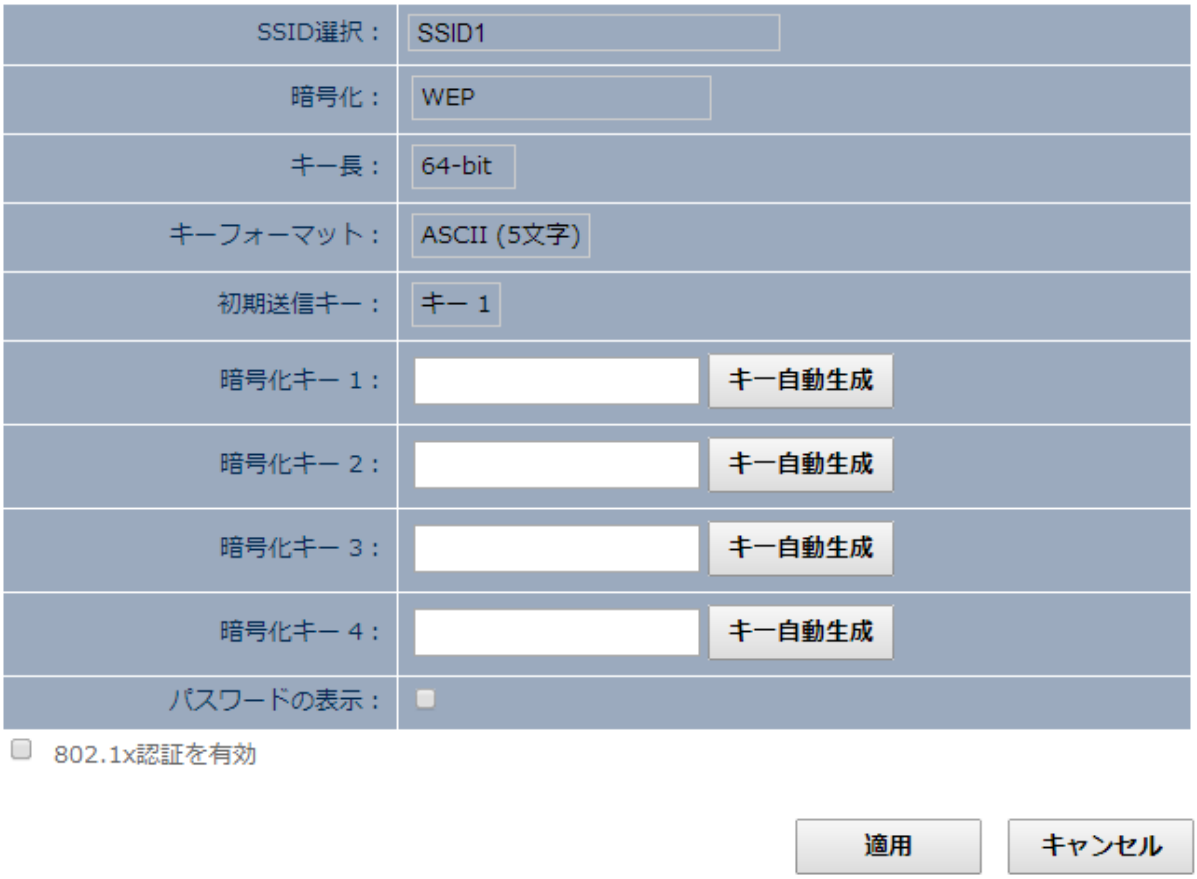
SSID インタフェースを選択する場合は、以下のセキュリティを設定することが可能です。

- Disabled　：　選択した SSID インタフェースにはセキュリティがありません。
- WEP　　：　WEP(Wired Equivalent Privacy)および 802.1X ダイナミック WEP セキュリティを設定します。詳細については、「WEP(Wired Equivalent Privacy)」の項を参照して下さい。
- WPA プレシェアードキー:
  詳細については、「WPA プレシェアードキー」の項を参照してください。 .
- WPA RADIUS　:
  詳細については、「WPA RADIUS」の項を参照してください。

「WEP(Wired Equivalent Privacy)」

WEP はセキュリティの基本レベルであり、非認証のネットワークへのアクセスを回避し、無線クライアント/AE1021 間で送信されたデータの暗号化を行います。WEP は、スタティックの共用キー(固定長の 16 進数、または英数文字)を使用し、ネットワークを使用したいクライアントに対して手動で伝達されます。

セキュリティ設定



WEPセキュリティ設定	
SSID選択:	セキュリティ設定用のSSIDを選択します。
暗号化:	WEPを選択して、基本のWEPセキュリティの設定値を表示します。
キー長:	キーの長さ(64ビット、または128ビット)を選択します。無線クライアントで使用する暗号キーのサイズはすべて同じでなければなりません(デフォルト設定: 64ビット)。
キーフォーマット:	WEP暗号キーの入力方法(Hex、またはASCII)のいずれかを選択します(デフォルト設定: Hex)。
初期送信キー:	暗号キーの番号を選択します。クライアントが使用する4つのWEPキーが同じ値に設定されている場合は、クライアントキーをアップデートせずに、暗号キーを任意の値に変更することができます(デフォルト設定:キー1)。
暗号化キー 1-4:	SSIDに対してWEP暗号キーを4つまで入力します。 ■ Hex : 64ビットキーの場合は、10つの16進数文字、128ビットキーの場合は、26個の16進数文字を入力します(0-9 および A-F)。 ■ ASCII : 64ビットキーの場合は5文字の英数字、128ビットキーの場合は、13文字の英数字を入力します。
キー自動生成	このボタンを押すことによって、ランダムな共有キーが自動的に作成されます。
パスワードの表示:	チェックを入れると、暗号化キー1～4の内容が表示されます。
□802.1x認証を有効:	RADIUSサーバからWEPキーを動的に伝達可能にします。 詳細については、次の項を参照してください。

【注記】: WEP キーインデックス、タイプ、長さは、クライアントに設定されている値と一致しなければなりません。

IEEE 802.1X は、ユーザ認証用の RADIUS サーバを用いてネットワークのアクセス制御を行う標準のフレームワークです。 この制御機能は、802.1X クライアントアプリケーションによりユーザ認証用の資格証明書の有無を確認することによって、ネットワークへの非認証アクセスを防ぎます。802.1X 規格は EAP(Extensible Authentication Protocol)を用いて、クライアントからのユーザの資格証明書(デジタル証明書、ユーザ名およびパスワード、その他)を RADIUS サーバに渡します。次に、クライアントによるネットワークへのアクセスが行われる前に、RADIUS サーバ上でクライアント認証が行われます。

【注記】:　ここでは、AE1021 対応の RADIUS サーバが実装されていることが前提です。 RADIUS サーバソフトウェアの使用方法についての詳細はご使用される RADIUS サーバ付属のドキュメントを参照してください。

WEPによる802.1X 認証を可能にすると、WEP 認証キーは RADIUS サーバにより自動的に設定され、接続先のクライアントすべてに伝達されます。

ダイナミックWEPセキュリティ設定	
SSID選択:	セキュリティ設定用のSSIDを選択します。
暗号化:	WEPを選択して、セキュリティの設定を表示します。
802.1x認証を有効:	RADIUSサーバからWEPキーを自動的に伝達可能にします。
RADIUSサーバIPアドレス:	RADIUSサーバのIPアドレスを指定します。
RADIUSサーバポート:	認証メッセージ用のRADIUSサーバが使用するUDP(User Datagram Protocol) ポート(有効範囲: 1024-65535; デフォルト: 1812)
RADIUSサーバパスワード:	AE1021/RADIUSサーバ間のメッセージ暗号化用の共用のテキスト文字列。RADIUSサーバで指定されてる文字列と同じ文字列であることを確認してください。文字列の間にスペースを入れないでください(範囲:1-64 文字)。
パスワードの表示:	チェックを入れると、RADIUSサーバのパスワードの内容が表示されます。

WPA プレシェアードキー

WPA(Wi-Fi Protected Access)は、WEP の脆弱性に対して一時的な解決策として導入され、さらに強力な無線セキュリティを向上させたものです。WPA2 には、完全な無線セキュリティ規格に対応しており、WPA との上位互換性を備えています。WPA および WPA2 は、「enterprise」および 「personal」モードで設定されます。

セキュリティ設定	
SSID選択:	セキュリティ設定用のSSIDを選択します。
暗号化:	WPAのプレシェアードキーを選択して、セキュリティ設定値を表示します。
WPAユニキャスト暗号スイート:	クライアント用のユニキャストデータ暗号タイプを選択します(デフォルト設定: WPA2 Mixed)。 ■ **WPA (TKIP)**: TKIP (Temporal Key Integrity Protocol)キーを暗号化に使用します。WPA は TKIP を WEP に代わるデータ暗号化方式として指定します。TKIP はデータ暗号化キーを動的に変更することにより、WEP スタティックキーの問題を回避します。 ■ **WPA2 (AES)**: AES(Advanced Encryption Standard)キーを暗号化に使用します。WPA2 は通信メッセージの完全性を保つために CBC-MAC(Cipher Block Chaining Message Authentication Code)をもつ「AES Counter-Mode 暗号化」を使用します。AES-CCMP 暗号化の使用は、WPA2 の標準要求事項に指定されています。ただし、ネットワークに WPA2 を実装する前に、クライアントデバイスを WPA2 対応のハードウェアにアップグレードしてください。 ■ **WPA2 Mixed**: Uses either TKIP、または AES キーを暗号化に使用します。「WPA and WPA2 mixed」モードでは、WPA および WPA2 クライアントの両方を共通の SSID に関連付けることが可能です。「mixed」モードでは、それぞれのクライアントごとに、ユニキャストの暗号タイプ(TKIP、または AES)が設定されます。
共有キーフォーマット:	WPAプレシェアードキーは、ASCII文字列、または64文字の16進数文字で入力します。
共有キー:	パスフレーズキーを「8～63文字以内」のASCII文字、または64文字の16進数文字で入力します。
キー自動生成	このボタンを押すことによって、ランダムな共有キーが自動的に作成されます。
パスワードの表示:	チェックを入れると、共有キーの内容が表示されます。

WPA RADIUS

エンタープライズ向けには、WPA および WPA2 はユーザ認証用に IEEE 802.1X を使用し、無線ネットワークに RADIUS 認証サーバを設定する必要があります。データ暗号化キーは自動的に設定され、ネットワーク接続先のクライアントすべてに伝達されます。

ダイナミックWEPセキュリティ設定	
SSID選択:	セキュリティ設定用のSSIDを選択します。
暗号化:	WPAのRADIUSを選択して、セキュリティ設定値を表示します。
WPAユニキャスト暗号スイート:	クライアント用のユニキャストデータ暗号タイプを選択します(デフォルト設定: WPA2 Mixed)。 ■ **WPA (TKIP)**: TKIP (Temporal Key Integrity Protocol)キーを暗号化に使用します。WPA は TKIP を WEP に代わるデータ暗号化方式として指定します。TKIP はデータ暗号化キーを動的に変更することにより、WEP スタティックキーの問題を回避します。 ■ **WPA2 (AES)**: AES（Advanced Encryption Standard）キーを暗号化に使用します。 WPA2 は通信メッセージの完全性を保つために CBC-MAC(Cipher Block Chaining Message Authentication Code)をもつ AES Counter-Mode 暗号化を使用します。AES-CCMP 暗号化の使用は、WPA2 の標準要求事項に指定されています。ただし、ネットワークに WPA2 を実装する前に、クライアントデバイスを WPA2 対応のハードウェアにアップグレードしてください。 ■ **WPA2 Mixed**: TKIP、または AES キーを暗号化に使用します。「WPA and WPA2 mixed」モードでは、WPA および WPA2 クライアントの両方を共通の SSID に関連付けることが可能です。「mixed」モードでは、それぞれのクライアントごとに、ユニキャストの暗号タイプ（TKIP、または AES)が設定されます。
RADIUSサーバIPアドレス:	RADIUSサーバのIPアドレスを指定します。
RADIUSサーバポート:	RADIUSサーバが認証メッセージ用に使用するUDP (User Datagram Protocol)ポート番号。（有効範囲: 1024-65535; デフォルト: 1812）
RADIUSサーバパスワード:	AE1021/RADIUS間のメッセージ暗号化用の共用のテキスト文字列。RADIUS サーバで指定されてる文字列と同じ文字列であることを確認してください。文字列の間にスペースを入れないでください(範囲:1-64 文字)。
パスワードの表示:	チェックを入れると、RADIUSサーバのパスワードが表示されます。

アクセスコントロール

無線クライアントは、AE1021 上に設定されたローカルのデータベースの MAC アドレスをチェックすることにより、ネットワークアクセスを認証することが可能です。無線クライアントの MAC アドレスをフィルタリングテーブルに 20 個まで設定できます。

アクセスコントロール	
MACアドレスフィルタリングテーブル	現在MACアドレスフィルタリングテーブルに登録されているMACアドレスおよびコメントを表示します。アクセスコントロールが有効の場合、このテーブルに登録されているクライアントのみ、APに無線接続できます。
MACアドレス	クライアントの物理アドレス。16進数の6ペアの文字列を入力します(″xxxxxxxxxxxx″ 12桁　ハイフン無し)。
コメント	登録したMACアドレスに関してのコメントを入力します。
選択	フィルタリングテーブルのエントリは、個々に選択可能です。<消去>ボタンをクリックすると、テーブルから選択したMACアドレスがすべて削除されます。
□　アクセスコントロールを有効にする	設定したエントリに応じて無線クライアントのアクセスコントロールを有効にします。
追加	MACアドレスおよびコメントを入力して、フィルタリングテーブルに新しいエントリを追加します。
消去	既に設定されているMACアドレスを削除する場合は、削除したいMACアドレスを選択して、<消去>ボタンをクリックしてください。

<全てを削除>ボタンをクリックすると、テーブル内に登録されているエントリはすべて削除されます。

3.4.5 QoS

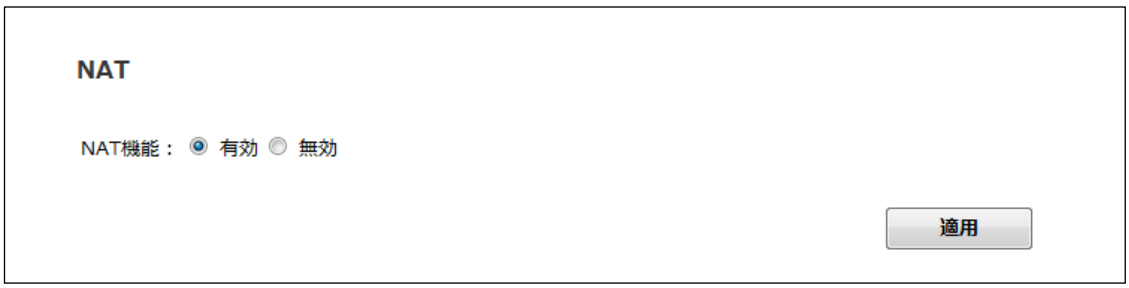
LAN/WAN 間の帯域幅の相違点は、時間的制約のあるアプリケーションによってはパフォーマンスを非常に低下されることです。QoS(Quality of Service)機能により、ユーザはアプリケーションのトラフィックを分類したり、安定した帯域幅を確保することが可能です。QoS 画面では、WAN ポートのアップロード/ダウンロードの帯域幅を設定可能です。
音声および動画などのプライオリティの高いトラフィックの場合は、他のトラフィックタイプより帯域幅の割り当てを高くすることができます。

QoS設定	
基本設定	
アップロード帯域幅:	トラフィックすべてのアップロード帯域幅の上限を指定します(Kbps単位)。
ダウンロード帯域幅:	トラフィックすべてのダウンロード帯域幅の下限を指定します(Kbps単位)。
現在のQoSテーブル	
現在のQoSテーブル:	設定されたQoSルールのテーブルはWANポートのトラフィックに適用されます。テーブルに登録可能なルールは「16個」までです。
□QoSを有効にする	
ルール名:	トラフィックのマッピングルールを識別するためのテキスト名を表示します。
帯域幅:	QoSルールに応じて識別されるアップロード/ダウンロードのトラフィックの帯域幅を「Maximum」、または「Guarantee」のいずれかに設定します。
ローカルIPアドレス:	LANのIPアドレス、またはアドレスの範囲を設定します。
ローカルポート範囲:	LANのトラフィックの特定ポート、またはポート範囲を設定します。
リモートIPアドレス:	トラフィックの外部IPアドレス、またはアドレスの範囲を設定します。
リモートポート範囲:	外部トラフィックの特定ポート、あるいはポートの範囲を設定します。
優先度:	指定したプライオリティタグの値をもつトラフィックを設定します。
トラフィック形式:	ドロップダウンリストからの優先度の高いサービスのトラフィックを設定します。
プロトコル:	トラフィックのプロトコルを「TCP」、または「UDP」のいずれかに設定します。

3.4.6 NAT

NAT(Network Address Translation)は、ネットワーク全体で複数の内部 IP アドレスから1つの外部 IP アドレスにマッピングするための標準的な方法です。

AP については、内部(ローカル)IP アドレスは、DHCP サーバによりローカルのパソコンに割り当てられる IP アドレス、外部 IP アドレスは、指定した WAN インタフェースに割り当てられた IP アドレスです。



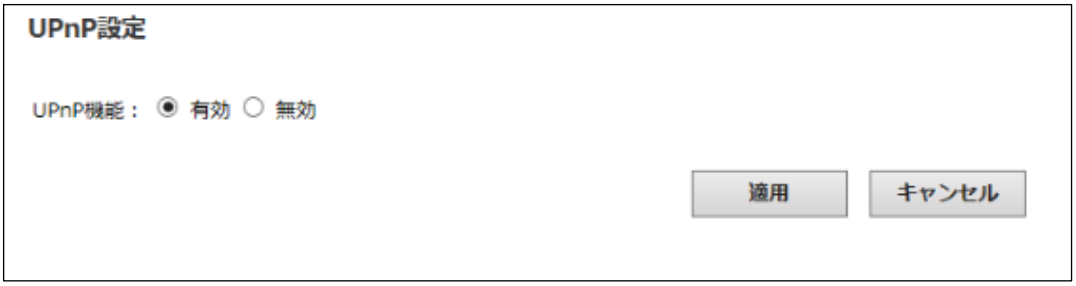
1) ポート転送

ポート転送は、内部(ローカル LAN)ネットワーク上の適切なパソコンに、WEB サーバなどの特定サービスの外部(内部)トラフィックを転送する方法です。この機能により、外部ユーザは、NAT 対応の AP を介して外部からローカル IP アドレスのポートでアクセスが可能になります(エントリは「最大 20 個」まで有効)。

ポート転送設定	
ローカルIP	外部ユーザ向けの特定サービスのホスティングを行うローカルパソコンのIPアドレスを表示します。
タイプ	サービスで使用するポートのプロトコル(TCP、UDP、あるいは両方)を設定します。
ポート範囲	ローカルコンピュータへのトラフィックの転送用のパブリックポート、あるいはポートレンジ(インターネットユーザにより使用)が表示されます。
コメント	ポート転送用の設定を識別するために有用なコメントを入力します。
選択	テーブル内のエントリを選択します。

2) UPnP 設定

UPnP(Universal Plug and Play)では、同じ規格でサポートされているデバイス間の内部接続を行います。
UPnPは、TCP/IP、UDP、HTTPなどの標準インタネットプロトコルに基づいています。UPnPプロトコルを有効にするには、「有効」を選択して、<適用>ボタンをクリックします。



3) ALG 設定

ALG(Application-Layer Gateway)機能は、特定のプロトコルのトラフィックをブロックせずに AP に通過させることが可能です。ALG 機能は、AP の NAT 機能と共に、選択したプロトコルセッションの制御およびモニタリングしたり、ローカルネットワーク上のインターネット上のデバイスとローカルネットワーク上のクライアント間で必要なポートを動的にオープンします。

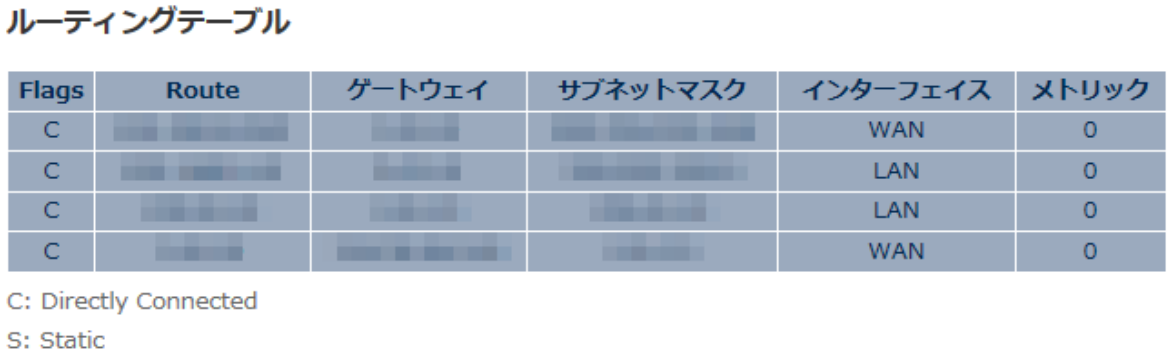
【注記】: 6 つの指定プロトコルタイプ(FTP、H323、IPSec、PPTP, L2TP および SIP)のみ、AP に対して ALG を設定可能です。

3.4.7 ルーティング

ルーティング設定では、手動によるネットワーク間のルート設定を行います。ユーザは、ルーティングテーブルに直接入力することによりスタティックルートを設定可能です。スタティックルーティングの設定は容易に行うことができます。

ルーティングテーブル

ここでは、宛先への最適なパスに沿って、パケットの転送に必要な情報を表示します。各パケットには、元の情報と宛先情報が含まれます。パケットを受信する際、ネットワークデバイスはパケットを調べてルーティングテーブルのエントリに一致すると、宛先への一番適したルートを提供します。次に、テーブルは、デバイスにネットワーク間のルート上でネクストホップにパケットを送信するよう指示を出します。



ルーティングテーブル	
Flags	ルーティングのタイプは、以下のとおりです。 ■ C: AP に直接接続されているネットワーク ■ S: AP に手動で入力したルート ■ R: IP プロトコルを介して動的に学習されたルート ■ I: ICMP リダイレクトメッセージから設定されたルート
Route	パケットを転送可能な宛先ネットワークが表示されます。
ゲートウェイ	一致するフレームの転送先のネクストホップのルータのIPアドレスが表示されます。
サブネットマスク	宛先に関連のあるサブネットワークが表示されます。
インターフェイス	ルートのパケットの送信先のインタフェースを表示します。
メトリック	ルートコストを表示するための値。同じ宛先への可能な複数のルーティング間で、最適なルートを選択可能です。

静的ルーティング設定

静的ルーティングにより、特定の宛先ネットワーク、サブネットワーク、あるいはホスト間のルーティングを手動で設定します。静的ルーティングは、サブネットへの特定のルーティングを手動で設定する必要があります。

静的ルーティングでは、ネットワークトポロジーに変更が生じても、自動的に変更されないため、小規模の安定したルーティングにのみお使いになることをお勧めします。

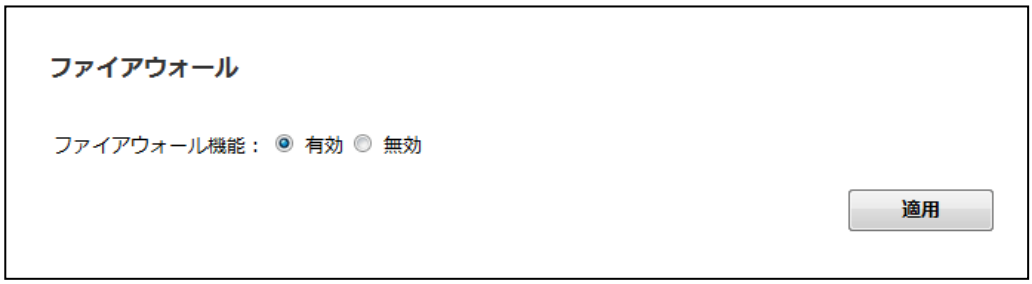
静的ルーティング設定	
宛先IPアドレス	パケットのルーティングを行う宛先ネットワークを表示します。
サブネットマスク	宛先に関連のあるサブネットマスクを表示します。
ゲートウェイ	一致したフレームの転送先のネクストホップのルータのIPアドレスを表示します。
メトリック	ルートコストを表示するための値。同じ宛先への可能な複数のルーティング間で、最適なルートを選択可能です(有効範囲: 2-15)。
インターフェイス	ルートのパケットの送信先にインタフェースを表示します。

3.4.8 ファイアウォール機能設定

AP は、ネットワークへの外部から侵入されるのを防いだり、共通のハッカーによる攻撃に対する防御を行うための、包括的なファイアウォールの保護を行います。

IP アドレスおよび TCP/UDP ポート番号、特定の MAC アドレスを設定することにより、ローカルネットワークのクライアントからのインターネットへのアクセスをブロックすることも可能です。

ファイアウォールの機能を有効にするには、「有効」を選択して、〈適用〉ボタンをクリックしてください。



1) MAC アドレスフィルタリング

MAC アドレスに応じてローカルネットワーク上のクライアントからのインターネットへのアクセスをブロックすることが可能です。AP 上の MAC アドレスのフィルタリングは、「最大 20 個」まで設定可能です。

MACアドレスフィルタリング	
クライアントPC MACアドレス	ローカルパソコンのブロックするMACアドレスを設定します(″xxxxxxxxxxx″ 12桁　ハイフン無し)。
コメント	テーブルエントリを識別するテキスト文字列を表示します。.
選択	テーブルエントリを選択します。

2) IP アドレスフィルタリング

IP アドレスフィルタリング機能により、プロトコルタイプ、IP アドレス、TCP/UDP ポート番号に応じてトラフィックを制限することが可能です。

IPアドレスフィルタリング	
クライアントPC情報:	フィルタテーブルのエントリのクライアントPC情報を表示します。
クライアントPC IPアドレス:	フィルタリングに一致するIPアドレス、またはアドレスの範囲を表示します。
サービス名:	テーブルエントリの中でブロックしたいサービスのリストを表示します。
プロトコル:	ブロックするプロトコルタイプ(TCP, UDP、あるいはその両方)を表示します。
ポート範囲:	ブロックするポート、またはポート範囲を指定します。
選択	テーブルエントリを選択します。

□IPフィルタリングを有効にする(拒否)

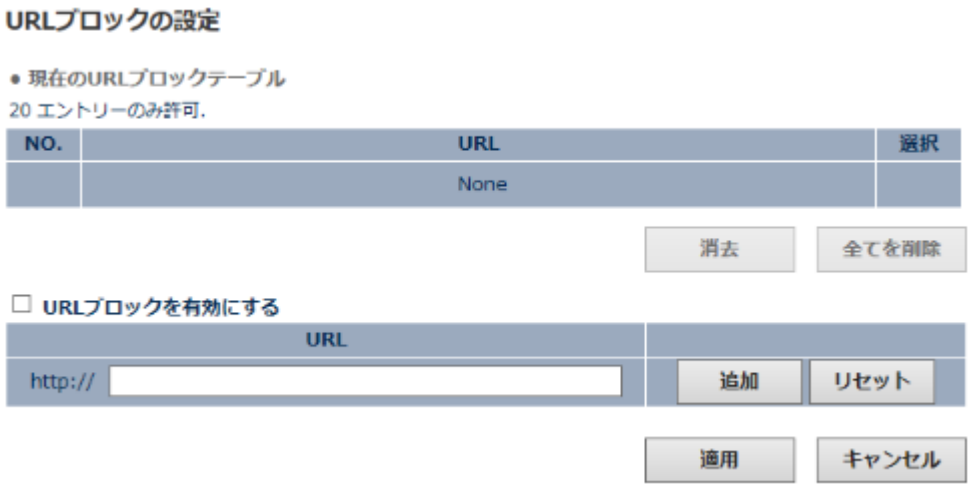
IPアドレスのフィルタリングを行う場合、以下の手順に従ってください。

1. 「クライアント PC 情報」フィールドにフィルタを識別する名前を入力します。
2. 「Client PC IP」フィールドにクライアントの IP アドレス(単体、または IP アドレスの範囲)を指定します。
3. 「プロトコルタイプ」フィールドから、必要なプロトコルタイプを選択してから、TCP/UDP ポート番号を入力するか、リストの中からサービスを選択します。
4. 画面右下の<追加>ボタンをクリックして、現在のフィルタリングテーブルにエントリを追加します。
   【注記】: IP フィルタリングは最大 10 個まで設定可能です。
5. 「IP フィルタリングを有効にする(拒否)」フィールドにチェックを入れ、<適用>ボタンをクリックしてください。

3) URL ブロックの設定

AP は、URL ドメインに応じてインターネットへのアクセスをブロックします。

ネットワークからの URL アクセスをフィルタリングすることにより、ユーザは指定したオンラインのコンテンツへのアクセスを禁止することが可能です。



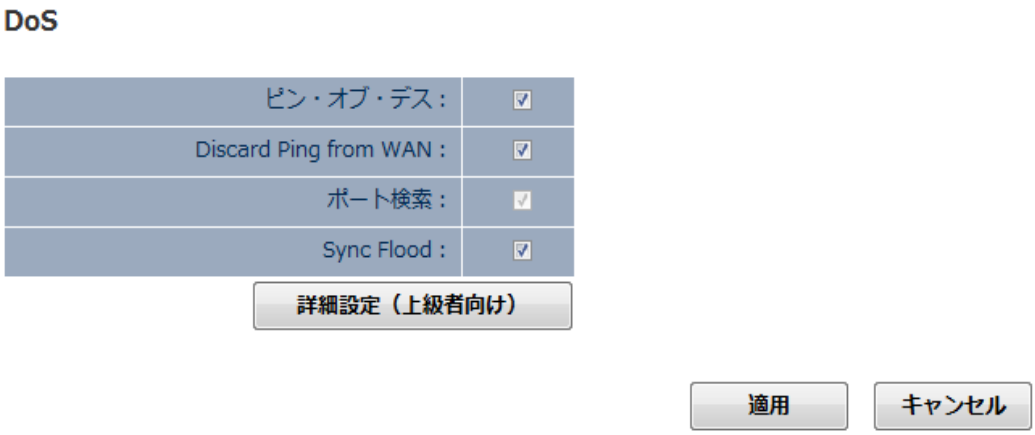
URL ブロックを有効にするには、以下の手順に従ってください。

1. ブロックする先のドメインの URL を入力してから<追加>ボタンをクリックすると、「現在のフィルタリングテーブル」にエントリが追加されます。
   【注記】:URL フィルタは 20 個まで設定可能です。
2. 「URL ブロックを有効にする」にチェックを入れ、<適用>ボタンをクリックしてください。

<全てを削除>ボタンをクリックすると、テーブル内に登録されているエントリはすべて削除されます。

4) DoS

AP のファイアウォールにより、共有の DoS(Denial of Service)およびハッカーによる攻撃からお使いのネットワークを保護します。設定したい DoS 攻撃のタイプを選択して、<適用>ボタンをクリックしてください。



(1) <詳細設定(上級者向け)>ボタンをクリックすると、以下の画面が表示されます。

DoS設定	
ピン・オブ・デス:	本体で処理不可能なオーバーサイズのpingパケットの受信を回避します。 通常のpingパケットは、56バイト、あるいはIPヘッダをもつ84バイトです。 最大値65,535バイトより大きいIPパケットサイズを「ピン・オブ・デス」として検知します。
Discard Ping from WAN:	WANポートからのICMPのPingを破棄して、応答しないように設定します。 この機能により、お使いのネットワークセキュリティのレベルを強化します。
ポート検索:	このオプションを有効にすると、アクティブなネットワークのタイプを識別し、送信元IPアドレスからトラフィックをブロックします。
Sync Flood:	3ウェイTCPハンドシェイクのプロセスを遮ったり、偽ったIPアドレスに受信した応答を送信したりするSYN(synchronized)攻撃から防御します。

5) DMZ

DMZ 機能を有効にすると、プライベート LAN 上で指定したパソコンから公共向けの WAN からのトラフィックはすべて AP のファイアウォールを通過できるようになります。
複数のパブリック IP アドレスをお使いの ISP から使用する場合、DMZ ホストを「最大 9 個」まで設定可能です。

パソコンを DMZ に設定する場合は、クライアント PC の IP アドレスフィールドに LAN の IP アドレスを入力します。
DMZ パソコンにインターネットから公共の IP アドレスフィールドにアクセスするには、スタティック IP アドレスを入力してください。お使いの ISP で DHCP を介して WAN ポートの IP アドレスを設定する場合は、オプションの中から選択してください（パブリックの IP アドレスは“0.0.0.0.”と表示されます）。

3.4.9 その他の機能

3.4.9.1 IPv6 設定

1） Routerモードでお使いの場合:

IPv6 のパケットの扱いを「IPv6 Bridge」と「PPPoE パススルー」のメニュー項目でお使いの環境に応じて設定を行うことができます。

1-1) IPv6 Bridge 機能　有効/無効

IPv6 ブリッジ機能は、ISP によってサポートされている IPv6 サービスをそのまま透過する機能です。
IPv6 ブリッジの機能を有効にするには、「有効」を選択して〈適用〉ボタンをクリックしてください。

IPv6　Bridge機能	
有効/無効	IPv6ブリッジ機能を有効/無効にします。 【注記】: 本モードを有効にしたまま、IPV6マルチキャストストリーミングパケットが大量に流れる「ひかりTV」などを利用すると、無線LANの通信が不可となる可能性があります。
無線のみ無効	無線 LAN 側の IPv6 ブリッジ機能のみ無効にします。 【注記】: 有線側にて「ひかりTV」などのIPv6マルチキャストのストリーミングを受信させながら、 無線にてIPv4でのインターネット通信を行うことを想定したモードです。 通常は本設定をチェックすることをお勧めします。

1-2) PPPoE パススルー機能　有効/無効

PPPoE パススルー機能は、ローカル LAN 上のパソコンで有効にすると、AP を介して ISP に対して独自に PPPoE 接続を行います。この機能は、ISP により複数の PPPoE セッションを介して接続されていることが前提です。
PPPoE パススルー機能はデフォルト設定では無効です。
この機能を有効にするには、「有効」を選択して〈適用〉ボタンをクリックしてください。

PPPoEパススルー機能	
有効/無効	PPPoEによる通信パケットを透過させるモードです。 無線でPPPoEによる通信が必要な際に有効にしてください。

2)　Bridgeモードでお使いの場合：

IPv6 のパケットの扱いを「IPv6 設定」のメニュー項目でお使いの環境に応じて設定を行うことができます。

IPv6設定	
IPv6パススルー	有線/無線の両方へLAN内のIPv6通信のパケットを透過させるモードです。 無線でIPv6通信が必要な際に設定してください。 【注記】: 本モードは、IPV6マルチキャストストリーミングパケットが大量に流れる「ひかりTV」などを利用している際に設定すると、無線LANの通信が不可となる可能性があります。
IPv6有線のみ パススルー	有線のみにLAN内のIPv6通信のパケットを透過させる機能です。 【注記】: 有線側にて「ひかりTV」などのIPv6マルチキャストのストリーミングを受信させながら、 無線にてIPv4でのインターネット通信を行うことを想定したモードです。 通常は本モードに設定することをお勧めします。

【注記】:

この設定は、上級者向けです。パラメータの変更等の詳細について習熟していない場合は、デフォルト値のままでお使いになることをお勧めします。

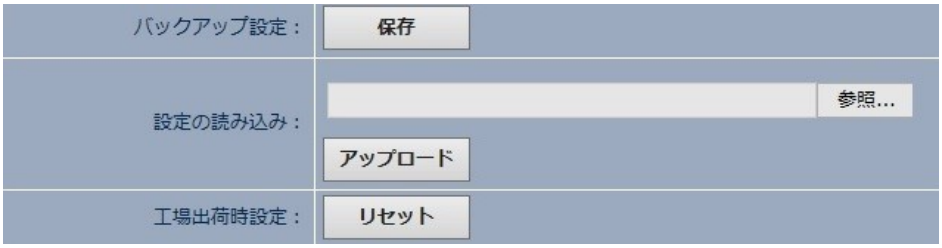
上記のモードのいずれかを選択したら、<適用>ボタンをクリックしてください。

3.5 管理ツール

AE1021/AE1021PE の「設定ツール」メニューでは、本体の管理機能(config ファイルの保存/復元、システムソフトウェアのアップグレード、AE1021/AE1021PE のリセットなど)を設定することが可能です。

3.5.1 設定ツール

「設定ツール」画面では、管理用 PC 上のファイルに AE1021/AE1021PE の設定値のバックアップを行います。
「バックアップ設定」メニューの〈保存〉ボタンをクリックして、お使いのパソコンのディレクトリを指定し、ファイル名を“xxx.cpt”形式で保存します。
ローカルパソコンに保存されている cofig ファイルから AE1021/AE1021PE の設定値を復元するには、〈参照〉ボタンを使って、お使いのパソコン上で config ファイルを選択した後、〈アップロード〉ボタンをクリックします。



設定ツール	
バックアップ設定:	管理用パソコンのファイルに現在のAPの設定を保存します。
設定の読み込み:	<参照>ボタンをクリックして、“xxx.cpt”形式で保存されている設定ファイルを選択します。その後<アップロード>ボタンをクリックして、アップロードします。
工場出荷時設定:	APの設定を工場設定時に戻します。

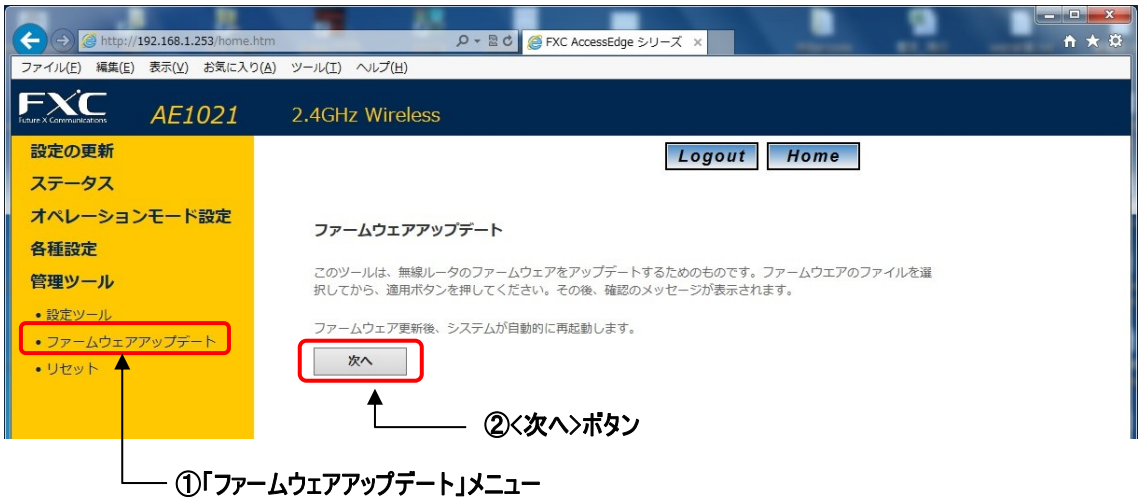
3.5.2 ファームウェアアップデート

AE1021/AE1021PE をアップグレードするには、あらかじめ管理用パソコンのローカルに保存した新しいファームウェアを使用してください。新しいファームウェアは今後、拡張機能を追加したり、問題を解決するために定期的に提供します。
当社ホームページよりダウンロードし、ローカルに保存してください。

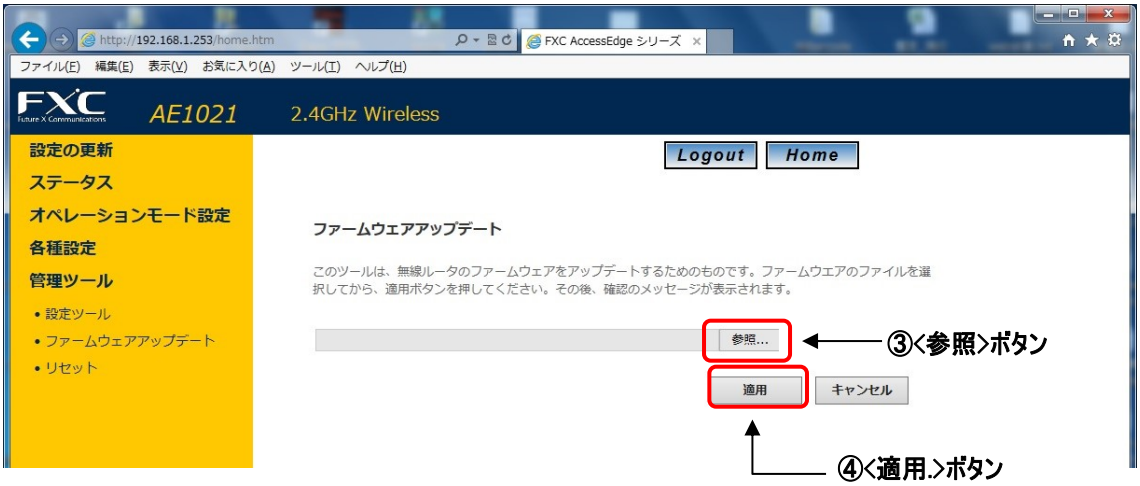
－ アップデート手順 －

1. まず、左メニューから管理ツール＞①「ファームウェアアップデート」メニューをクリックします。

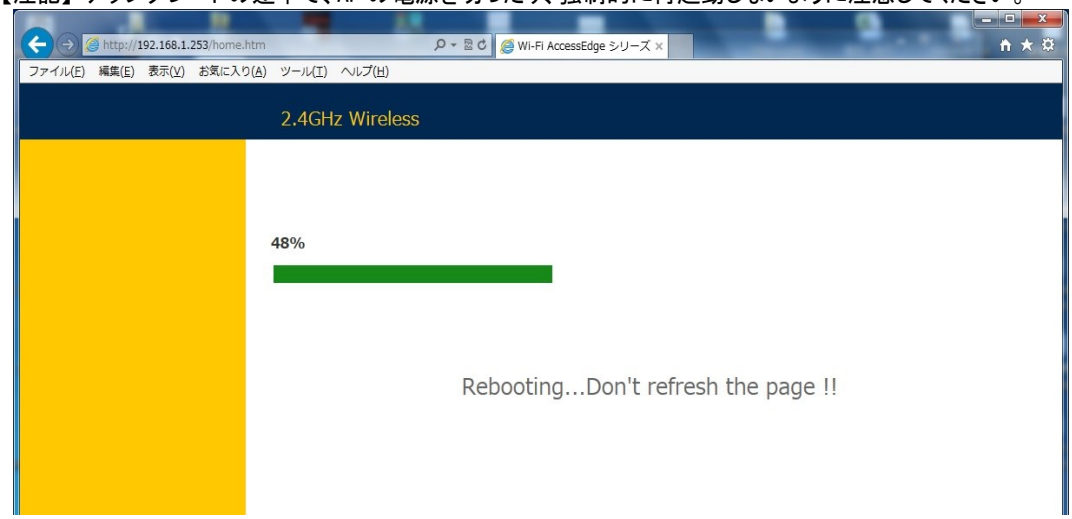
2. 次に、「ファームウェアアップデート」画面の②＜次へ＞ボタンをクリックします。



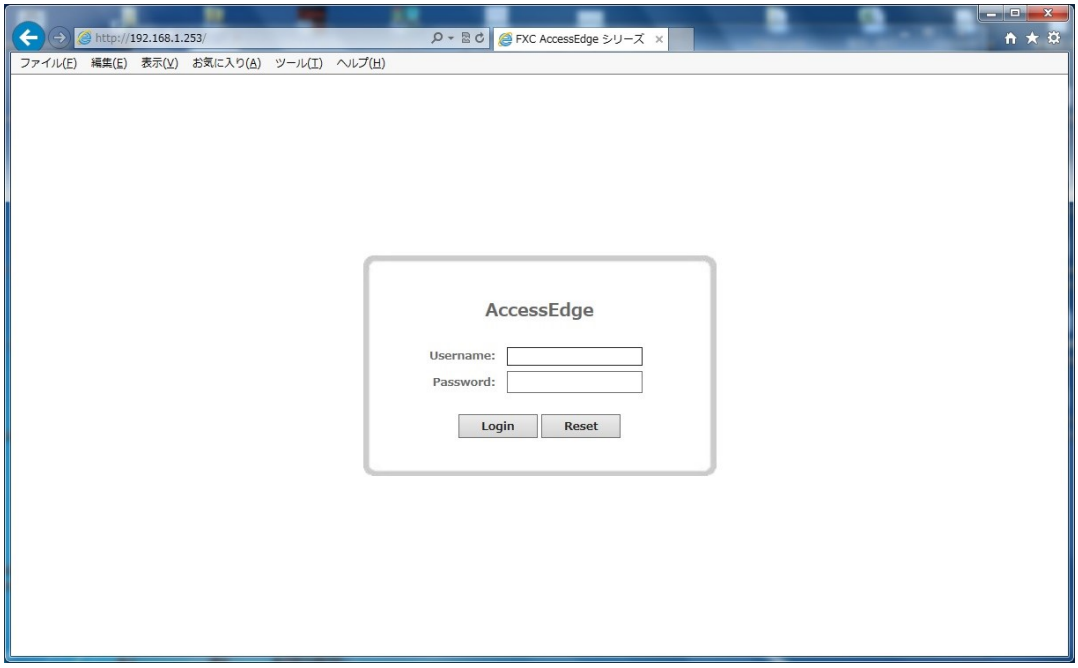
3. 「ファームウェアアップデート」画面より、③<参照>ボタンをクリックして、ローカルに保存されたファームウェアのファイルを選択し、④<適用>ボタンをクリックしてください。
※ファームウェアファイルの拡張子は. img です。(例:FXC_AE1021_AE1021PE_FW_2.0.6. img)



4. ファームウェアの更新が開始され、完了すると自動的に再起動しログイン画面が出ますので、それまでしばらくお待ちください。
【注記】:アップグレードの途中で、AP の電源を切ったり、強制的に再起動しないように注意してください。



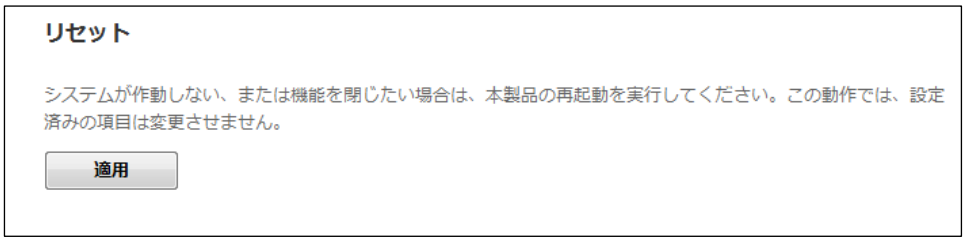
5. ログイン画面が表示されますので、ユーザ名およびパスワードを入力してください。



3.5.3 リセット

ここでは、本機のソフトウェアをリセットすることができます。本機が正しく動作しなくなったり、動作を中断したい場合は、再起動を行ってください。

【注記】:　リセットしても、現在保存されている設定内容は変わりませんが、「3.5.1管理ツールメニュー」→「設定ツール」にある〈リセット〉ボタンをクリックすると、工場出荷時の設定に戻りますのでご注意ください。



4 章 トラブルシューティング

●無線 LAN 接続ができない。

□ ルータおよび無線 LAN クライアントに本機と同じ SSID が設定されていることを確認してください。
本機の SSID 初期値は SSID1 及び SSID2 です。

□ 本機と無線 LAN クライアントのセキュリティ設定が合致しているか再度確認してください。

□ 本機と無線 LAN クライアントの電源をオフにして、再度、本機＞無線 LAN クライアントの順に電源を入れてみてください。

●無線接続が途切れる。

□ 他の無線機器との干渉により、通信品質が低下する場合があります。このような場合は、本機及び、ご使用の無線 LAN アダプタなどのチャンネルを変えて、干渉を回避してください。

□ 電子レンジやモニタなどの RF ノイズを発生する機器は本製品から 90cm 以上離してください。

AE1021/AE1021PE Management Guide (FXC14-DC-200007-R2.5）

初版	2014 年　7 月
第 2 版	2014 年 11 月
第 3 版	2014 年 12 月
第 4 版	2015 年　1 月
第 5 版	2015 年　3 月
第 6 版	2015 年 12 月
第 7 版	2016 年　8 月

Management Guide
AE1021/AE1021PE
Management Guide
AE1021/AE1021PE
Management Guide
AE1021/AE1021PE
Management Guide
AE1021/AE1021PE
Management Guide
AE1021/AE1021PE
Management Guide
AE1021/AE1021PE
Management Guide
AE1021/AE1021PE
Management Guide
AE1021/AE1021PE4
Management Guide
AE1021/AE1021PE
Management Guide
AE1021/AE1021PE
Management Guide
AE1021/AE1021PE
Management Guide
AE1021/AE1021PE
Management Guide
AE1021/AE1021PE
Management Guide
AE1021/AE1021PE
Management Guide

FXC株式会社