B5FY-7021-01 Z2

取扱説明書

ワイヤレス LAN ステーション FMWT-56AG

FUJITSU

はじめに

このたびは、弊社の FMV シリーズ用ワイヤレス LAN ステーション（FMWT-56AG）をお買い上げいただき、まことにありがとうございます。
本書は、ワイヤレス LAN ステーション（以降、本製品または無線 LAN アクセスポイント）の基本的な取り扱い方法、設置方法、および設定方法について説明しています。ご使用になる前に本書をよくお読みになり、正しい取り扱いをされますようお願いいたします。

2006 年 7 月

安全にお使いいただくために

このマニュアルには、本製品を安全に正しくお使いいただくための重要な情報が記載されています。
本製品をお使いになる前に、このマニュアルを熟読してください。特に、「安全上のご注意」（→ P.5）をよくお読みになり、理解されたうえで本製品をお使いください。
また、このマニュアルは、本製品の使用中にいつでもご覧になれるよう大切に保管してください。

注意

本製品は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス B 情報技術装置です。本製品は、家庭環境で使用することを目的としていますが、本製品がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。本製品は、マニュアルに従って正しい取り扱いをしてください。

本製品のハイセイフティ用途での使用について

本製品は、一般事務用、パーソナル用、家庭用、通常の産業用などの一般的用途を想定したものであり、ハイセイフティ用途での使用を想定して設計・製造されたものではありません。お客様は、当該ハイセイフティ用途に要する安全性を確保する措置を施すことなく、本製品を使用しないでください。ハイセイフティ用途とは、以下の例のような、極めて高度な安全性が要求され、仮に当該安全性が確保されない場合、直接生命・身体に対する重大な危険性を伴う用途をいいます。

- 原子力施設における核反応制御、航空機自動飛行制御、航空交通管制、大量輸送システムにおける運行制御、生命維持のための医療用機器、兵器システムにおけるミサイル発射制御など

本製品には、有寿命部品が含まれています。

- 有寿命部品の交換時期の目安は、使用頻度や条件により異なりますが、約 5 年です。
  なお、この期間はあくまでも目安であり、故障しないことや無料修理をお約束するものではありません。ご使用状態によっては早期に部品交換が必要となる場合があります。
- 製品に使用しているアルミ電解コンデンサは、寿命が尽きた状態で使用し続けると、電解液の漏れや枯渇が生じ、異臭の発生や発煙の原因となる場合がありますので、早期の交換をお勧めします。
- 部品の交換は、当社の定める補修用性能部品単位での修理による交換となります。

- 本製品は、落雷等による電源の瞬時電圧低下に対して不都合が生じることがあります。電源の瞬時電圧低下対策としては、交流無停電電源装置等を使用されることをお薦めします。
- 漏洩電流について、この装置は、社団法人 日本電子工業振興協会のパソコン業界基準（PC-11-1988）に適合しております。

保守部品供給期間について

本製品の保守部品の供給期間は、販売完了後 5 年間とさせていただきます。

このマニュアルの表記について

■本文中の記号

表：本文中の記号

重要	お使いになるときに注意していただきたいことや、してはいけないことを記述しています。必ずお読みください。
POINT	操作に関連することを記述しています。必要に応じてお読みください。

■画面例およびイラスト

表記されている画面およびイラストは一例です。お使いの機種や状況によって、画面およびイラストが若干異なることがあります。

■クリック操作について

このマニュアルは、マウスのクリック操作をシングルクリックで記述しています。設定によっては、ダブルクリックに読み替えてください。

■用語について

このマニュアルでは、ネットワークへの接続方法や、本製品を使って通信を行うパソコンを、次のように表記しています。

表：本文中の用語

本書の表記	意味
無線 LAN	LAN ケーブルを使わず無線を使用する LAN
有線 LAN	LAN ケーブルを使用する LAN
無線 LAN 端末	本製品に無線 LAN で接続するパソコン
有線 LAN 端末	本製品に有線 LAN で接続するパソコン
端末	無線 LAN 端末、または有線 LAN 端末、または、無線 LAN 端末と有線 LAN 端末
管理者用パソコン	本製品の設定を行うパソコン

■製品などの呼び方について

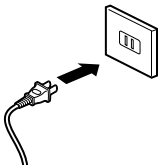
本文中の製品名称を、次のように略して表記する場合があります。

表：製品名称などの表記

<table>
<tr><th>製品名称</th><th colspan="2">本書での表記</th></tr>
<tr><td>ワイヤレス LAN ステーション FMWT-56AG</td><td colspan="2">FMWT-56AG</td><td>本製品、または無線 LAN アクセスポイント</td></tr>
<tr><td>Microsoft® Windows® XP Professional</td><td colspan="2" rowspan="6">Windows XP</td><td rowspan="14">Windows</td></tr>
<tr><td>Microsoft® Windows® XP Home Edition</td></tr>
<tr><td>Microsoft® Windows® XP Media Center Edition 2004</td></tr>
<tr><td>Microsoft® Windows® XP Media Center Edition 2005</td></tr>
<tr><td>Microsoft® Windows® XP Tablet PC Edition</td></tr>
<tr><td>Microsoft® Windows® XP Tablet PC Edition 2005</td></tr>
<tr><td>Microsoft® Windows® XP Professional 日本語版 Service Pack1</td><td colspan="2" rowspan="2">Windows XP、または Windows XP SP1</td></tr>
<tr><td>Microsoft® Windows® XP Home Edition 日本語版 Service Pack1</td></tr>
<tr><td>Microsoft® Windows® XP Professional 日本語版 Service Pack2 セキュリティ強化機能搭載</td><td colspan="2" rowspan="2">Windows XP、または Windows XP SP2</td></tr>
<tr><td>Microsoft® Windows® XP Home Edition 日本語版 Service Pack2 セキュリティ強化機能搭載</td></tr>
<tr><td>Microsoft® Windows® 2000 Professional</td><td colspan="2">Windows 2000</td></tr>
<tr><td>Microsoft® Windows® Millennium Edition</td><td colspan="2">Windows Me</td></tr>
<tr><td>Microsoft® Windows® 98 Operating System SECOND EDITION</td><td colspan="2">Windows 98</td></tr>
<tr><td>Microsoft® Windows Server™ 2003 Standard Edition</td><td colspan="2">Windows Server 2003</td></tr>
<tr><td>Microsoft® Internet Explorer 6.0</td><td>Internet Explorer 6</td><td rowspan="2">Internet Explorer 5.0 以降、または Internet Explorer</td><td rowspan="2">Web ブラウザ</td></tr>
<tr><td>Microsoft® Internet Explorer 5.5、
Microsoft® Internet Explorer 5.01、
および Microsoft® Internet Explorer 5.0</td><td>Internet Explorer 5</td></tr>
</table>

■電源プラグとコンセントの形状について

本製品に添付されている電源ケーブル（2 ピン）の電源プラグは「平行 2 極プラグ」です。このマニュアルでは「電源プラグ」と表記しています。接続先のコンセントには「平行 2 極プラグ（125V15A）用コンセント」をご利用ください。このマニュアルでは「コンセント」と表記しています。



■商標について

Atheros、the Atheros logo、Super A、Super G は、Atheros Communications, Inc. の商標または登録商標であり、弊社は同社の許可に基づき当該商標を使用しています。

Bluetooth は、Bluetooth SIG の登録商標であり、弊社へライセンスされています。
JavaScript は、米国およびその他の国における米国 Sun Microsystems, Inc. の商標または登録商標です。
Microsoft、Windows、MS、MS-DOS は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。
Wi-Fi および Wi-Fi ロゴは、Wi-Fi Alliance の登録商標です。
その他の各製品名は、各社の商標または登録商標です。
その他の各製品は、各社の著作物です。

安全上のご注意

■安全にお使いいただくための絵記号について

本書では、いろいろな絵表示を使っています。これは本製品を安全に正しくお使いいただき、あなたや他の人々に加えられるおそれのある危害や損害を、未然に防止するための目印となるものです。その表示と意味は次のようになっています。内容をよくご理解のうえ、お読みください。

表：安全にお使いいただくための絵記号

⚠警告	この表示を無視して、誤った取り扱いをすると、人が死亡する可能性または重傷を負う可能性があることを示しています。
⚠注意	この表示を無視して、誤った取り扱いをすると、人が傷害を負う可能性が想定される内容、および物的損害のみの発生が想定される内容を示しています。

また、危害や損害の内容がどのようなものかを示すために、上記の絵表示と同時に次の記号を使っています。

表：危害や損害の内容を示す記号

⚠	△で示した記号は、警告・注意を促す内容であることを告げるものです。記号の中やその脇には、具体的な警告内容が示されています。
🚫	🚫で示した記号は、してはいけない行為（禁止行為）であることを告げるものです。記号の中やその脇には、具体的な禁止内容が示されています。
❗	●で示した記号は、必ず従っていただく内容であることを告げるものです。記号の中やその脇には、具体的な指示内容が示されています。

⚠警告

- 本製品は主電源コンセントの近くに設置し、電源プラグへ容易に手が届くようにしてください。万一、本製品から発熱や煙、異臭や異音がするなどの異常が発生したときは、ただちに本製品の AC アダプタの電源プラグをコンセントから抜いてください。
  その後、異常な現象がなくなるのを確認して、またはご購入元にご連絡ください。お客様自身による修理は危険ですから絶対におやめください。
  異常状態のまま使用すると、感電・火災の原因となります。
- 本製品の内部に水などの液体や金属片などの異物が入った場合は、すぐに AC アダプタの電源プラグをコンセントから抜いてください。
  その後、「お問い合わせ先」（→ P.199）、またはご購入元にご連絡ください。そのまま使用すると、感電・火災の原因となります。
  特にお子様のいるご家庭ではご注意ください。
- 本製品を落としたり、カバーなどを破損したときは、電源プラグをコンセントから抜いてください。
  その後、「お問い合わせ先」（→ P.199）、またはご購入元にご連絡ください。そのまま使用すると、感電・火災の原因となります。
- 電源プラグは、家庭用電源（AC100V）に接続してください。
  また、タコ足配線をしないでください。
  感電・火災の原因となります。
- 添付の AC アダプタ、電源ケーブル（2 ピン）以外は使用しないでください。また、添付の AC アダプタ、電源ケーブル（2 ピン）を他の製品に使用しないでください。
  感電や故障の原因となります。
- AC アダプタや電源プラグは、コンセントの奥まで確実に差し込み、不完全な接続状態で使用しないでください。
  火災・故障の原因となることがあります。
- 濡れた手で電源プラグを抜き差ししないでください。
  感電・火災の原因となります。
- AC アダプタの電源プラグにドライバーなどの金属を近づけないでください。
  感電・火災の原因となります。
- AC アダプタや電源プラグはコンセントから定期的に抜いて、コンセントとの接続部分のほこりやゴミを乾いた布でよく拭いてください。
  ほこりがたまったままの状態で使用すると、火災の原因となります。
- 電源ケーブルや電源プラグが傷んだり、コンセントの差し込み口がゆるいときは使用しないでください。
  そのまま使用すると、感電・火災の原因となります。
- 電源ケーブルを傷つけたり、加工したりしないでください。重いものを乗せたり、引っ張ったり、無理に曲げたり、ねじったり、加熱したりすると電源ケーブルを傷め、感電・火災の原因となります。
  修理は、「お問い合わせ先」（→ P.199）、またはご購入元にご連絡ください。
- 本製品をお客様ご自身で改造しないでください。またマニュアル等で指示がある場合を除いて分解しないでください。
  感電・火災の原因となります。
  修理や点検が必要な場合は、「お問い合わせ先」（→ P.199）、またはご購入元にご連絡ください。

・本製品を風通しの悪い場所、火気のある場所、引火性ガスの発生する場所で使用したり、置いたりしないでください。
火災の原因となります。

・本製品を風呂場やシャワー室など、水のかかるおそれのある場所で本製品を使用したり置いたりしないでください。
感電・火災の原因になります。

・振動している場所や傾いたところなどの不安定な場所に置かないでください。
本製品が倒れたり、落下したりして、けがの原因となります。

・本製品の上や周りに花びん・コップなどの液体の入ったものを置かないでください。
水などの液体が本製品の内部に入って、感電・火災の原因となります。
また、本製品の上に重いものを置かないでください。故障・けがの原因となります。

・病院内や医療用電気機器のある場所では、本製品を使用しないでください。特に手術室、集中治療室、CCU（冠状動脈疾患監視病室）などには持ち込まないでください。
本製品からの電波が医療用電気機器に影響を及ぼすことがあり、誤動作による事故の原因になります。

・本製品を使用したり持ち運んだりする場合は、心臓ペースメーカーの装着部位から 22cm 以上離してください。もしくは本製品の電源を切ってください。
電波によりペースメーカーの動作に影響を及ぼす原因となります。

・航空機内など無線通信機能の使用を禁止されている場所や、自動ドア・火災報知器等の自動制御機器の近くでは、本製品を使用しないでください。
誤動作による事故の原因になります。

・梱包に使用している袋等はお子様の手の届くところに置かないでください。
口に入れたり、頭にかぶったりすると、窒息の原因となります。

・近くで落雷のおそれがある場合は、本製品の電源ケーブルをコンセントから抜き、その後 LAN ケーブルをコネクタから抜いてください。
そのまま使用すると、落雷による感電・火災の原因となります。

⚠注意

・電源プラグを抜くときは電源ケーブルを引っ張らず、必ず電源プラグを持って抜いてください。
電源ケーブルを引っ張ると、電源ケーブルの芯線が露出したり断線したりして、感電・火災の原因となることがあります。

・本製品を調理台や加湿器のそば、ほこりの多い場所などで使用したり置いたりしないでください。
感電・火災の原因となることがあります。

・本製品を直射日光があたる場所、閉めきった自動車内、ストーブのような暖房器具のそばで使用したり、置いたりしないでください。
感電・火災の原因となることがあります。また、破損や故障の原因となることがあります。

・使用中の本製品や AC アダプタなどを、布などでおおったり、包んだりしないでください。また、排気孔などの開口部をふさがないでください。
内部に熱がこもり、火災の原因となることがあります。

・本製品を移動する場合は、必ず電源プラグをコンセントから抜いてください。また、接続ケーブルなども外してください。作業は足元に十分注意して行ってください。
電源ケーブルが傷つき、感電・火災の原因となったり、本製品が落下したり倒れたりして、けがの原因となることがあります。

・LAN の差し込み口（モジュラージャックコネクタ）に指などを入れないでください。
感電の原因となることがあります。

・CD-ROM をセットするとき、および取り出すときには、トレーに指などを入れないでください。
けがの原因となることがあります。

本製品の IEEE802.11a について

本製品は、2005 年 5 月 16 日に総務省より発表された「電波法施行規則の一部を改正する省令」による、5GHz 帯無線 LAN（IEEE802.11a 規格）の変更後の周波数帯に対応しています。この省令については、富士通パソコン情報ページ FMWORLD.NET をご覧ください。

本製品の IEEE802.11a について

・ 本製品の IEEE802.11a は、以下の 8 つのチャンネルを使用できます。
  ・ W52：36(5,180MHz)/40(5,200MHz)/44(5,220MHz)/48(5,240MHz)
  ・ W53：52(5,260MHz)/56(5,280MHz)/60(5,300MHz)/64(5,320MHz)

IEEE802.11a を使用する場合は、上記チャンネルを利用できる無線 LAN 製品とのみ通信が可能です。

電波に関するご注意

■ワイヤレス・インタオペラビリティ

本製品は、DS-SS 方式および OFDM 方式を基礎とする無線 LAN 製品との相互通信システムの協調を実現するように設計されています。また、無線 LAN 製品の相互接続性を検証する「Wi-Fi Alliance」が定義する、無線 LAN 標準の「Wi-Fi®」に準拠しております。

■電波放射の環境への影響

・本製品は、他の高周波デバイス同様に、高周波エネルギーを放出していますが、本製品が放出するエネルギーのレベルは、例えば携帯電話のような無線デバイスが放出する電磁エネルギーよりはるかに低く抑えられています。
・本製品は、高周波安全基準および勧告のガイドライン内で動作するため、本製品の使用者に対し、安全性を確信しています。本基準および勧告は、科学界の統一見解を反映しており、研究班の審議および広範な研究文献を継続的に調査し解釈する科学者たちの委員会を根本としています。
・ある状況や環境において、本製品の使用は、建物の所有者や団体の責任ある代表者により制限されることがあります。例えば、下記に挙げる場合です。
  - 飛行機内での本製品の使用
  - 他のデバイスやサービスに対し干渉の危険がある環境での使用
・特定の団体や環境（例えば空港）で無線デバイスの使用に適用される方針が明確に分からない場合は、機器の電源を入れる前に本製品の使用許可について問い合わせをしてください。

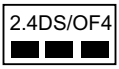
■電波放射の人体への影響

本製品から放射される出力パワーは、FCC 電波放射限界よりはるかに低くなっています。それでも、本製品は、通常の動作中に人間の接触に対し電位が最小限にとどめられるように使用されなくてはなりません。使用中は本製品に極力触れないでください。

■干渉に関する注意事項

・本製品は、高周波エネルギーを発生させ、使用し、また放射します。
・このマニュアルに従わずに設定したり使用したりすると、無線通信に有害な干渉を生じることがあります。
・本製品がラジオ、テレビの受信機に有害な干渉を与える原因となっている場合は（本製品の電源を入／切する事で原因となっているかどうかを判別できます）、次の方法で干渉を取り除くようにしてください。
  - 本製品と受信機の距離を離す
  - 受信機を接続しているコンセントと別系統回路のコンセントに本製品を接続する
  - 経験のあるラジオ／テレビ技術者に相談する
・本製品、および付属品の不正な改造、指定された以外の代替品等の接続は行わないでください。
・本製品、および付属品の不正な改造や、指定された以外の代替品等の接続により発生した、ラジオやテレビへの干渉についての責任を負いません。
・近くに他のチャンネルを使用している無線 LAN 機器がある場合、干渉により本来の性能が出ない場合があります。この場合、他のチャンネルを使用している無線 LAN 機器と使用しているチャンネルの間隔をあけるように変更して干渉の影響が最小となるチャンネルでお使いください。それでも解決しない場合は、他のチャンネルを使用している無線 LAN 機器から 3m 以上離して干渉の影響が最小となる場所でお使いください。
・IEEE802.11a の旧チャンネル J52 を使用する無線 LAN アクセスポイントとの混在環境においては、それぞれの無線 LAN アクセスポイントで設定されているチャンネルが 2 つしか離れていない場合（例えば、34(J52) と 36(W52) など）、電波干渉が発生するため IEEE802.11a 本来の性能が出ない場合があります。IEEE802.11a 本来の性能が必要な場合は、J52 と W52 を別の無線 LAN ネットワークにし、使用しているチャンネルの間隔を 6 チャンネル以上あけてお使いください。
・IEEE802.11g と IEEE802.11b の混在環境においては、IEEE802.11g は IEEE802.11b との互換性をとるため IEEE802.11g 本来の性能が出ない場合があります。IEEE802.11g 本来の性能が必要な場合は、IEEE802.11g と IEEE802.11b を別の無線 LAN ネットワークにし、使用しているチャンネルの間隔を 5 チャンネル以上あけてお使いください。
・本製品の 2.4GHz 帯は、チャンネル 1 ～ 14 まで使用することができますが、他の無線機器も同じ周波数帯を使っていることがあります。他の無線機器との電波干渉を防止するため、下記事項に注意してお使いください。

この機器の使用上の注意



上記表示のある無線機器は 2.4GHz 帯を使用しています。変調方式として DS-SS 変調方式および OFDM 変調方式を採用し、与干渉距離は 40m です。
この機器の使用周波数は 2.4GHz 帯です。この周波数帯では、電子レンジ等の産業・科学・医療用機器のほか、他の同種無線局、工場の製造ライン等で使用される免許を要する移動体識別用構内無線局、免許を要しない特定小電力無線局、アマチュア無線局等（以下「他の無線局」と略す）が運用されています。
・ この機器を使用する前に、近くに医療機関や工場がないことを確認してください。
・ 万一、この機器と「他の無線局」との間に電波干渉が発生した場合には、速やかにこの機器の使用チャンネルを変更するか、使用場所を変えるか、または機器の運用を停止してください。
・ 不明な点、その他お困りのことが起きたときは、お買い求めの販売店または富士通パーソナル製品に関するお問合せ窓口までお申しつけください。

■海外での使用について

本製品は、日本国内での無線規格に準拠し、認定を取得しています。日本国内でのみお使いいただけます。また、海外でご使用になると罰せられることがあります。

■屋外での使用について

IEEE802.11a 準拠（5GHz 帯）の無線 LAN の屋外使用は、電波法により禁じられています。本製品を屋外で使用する場合は、IEEE802.11a インターフェースの「無線スイッチ」を「オフ」に設定してください。

■無線機器との通信について

Bluetooth® 機器とは通信規格が異なるため通信できません。

■航空機内での使用について

航空機内では使用しないでください。罰せられる場合があります。

無線 LAN 製品ご使用時におけるセキュリティに関するご注意

重要

・お客様の権利（プライバシー保護）に関する重要な事項です。

無線 LAN では、LAN ケーブルを使用する代わりに、電波を利用してパソコンなどと無線 LAN アクセスポイント（ワイヤレス LAN ステーション、ワイヤレスブロードバンドルータ、ファミリーネットワークステーションなど）間で情報のやり取りを行うため、電波の届く範囲であれば自由に LAN 接続が可能であるという利点があります。

その反面、電波はある範囲内であれば障害物（壁など）を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

・通信内容を盗み見られる
悪意ある第三者が、電波を故意に傍受し、
- ID やパスワード又はクレジットカード番号などの個人情報
- メールの内容

などの通信内容を盗み見られる可能性があります。

・不正に侵入される
悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、
- 個人情報や機密情報を取り出す（情報漏洩）
- 特定の人物になりすまして通信し、不正な情報を流す（なりすまし）
- 傍受した通信内容を書き換えて発信する（改ざん）
- コンピュータウィルスなどを流しデータやシステムを破壊する（破壊）

などの行為をされてしまう可能性があります。

本来、無線 LAN カードや無線 LAN アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線 LAN 製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。
無線 LAN 製品は、購入直後の状態においては、セキュリティに関する設定が施されていない場合があります。
したがって、お客様がセキュリティ問題発生の可能性を少なくするためには、無線 LAN カードや無線 LAN アクセスポイントをご使用になる前に、必ず無線 LAN 製品のセキュリティに関するすべての設定を取扱説明書に従って行ってください。
なお、無線 LAN の仕様上、特殊な方法によりセキュリティ設定が破られることもあり得ますので、ご理解のうえ、ご使用ください。
セキュリティの設定などについて、お客様ご自身で対処できない場合には、「富士通パーソナル製品に関するお問合せ窓口」までお問い合わせください。
当社では、お客様がセキュリティの設定を行わないで使用した場合の問題を充分理解したうえで、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお奨めします。
セキュリティ対策を施さず、あるいは、無線 LAN の仕様上やむを得ない事情によりセキュリティの問題が発生した場合、当社は、これによって生じた損害に対する責任を負いかねます。

目次

1

第 1 章

お使いになる前に

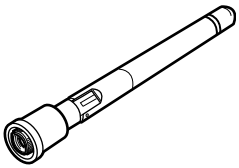
本製品をお使いになる前に必ずお読みください。

1 梱包物の確認

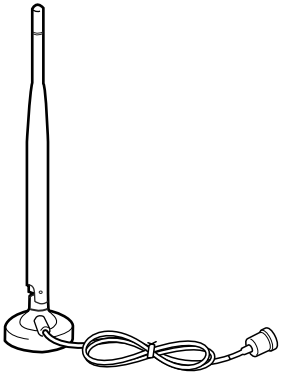
箱の中に次の品物がそろっているか確認してください。もし足りない部品などがあった場合は、できるだけ早く、ご購入元にご連絡ください。

・ワイヤレス LAN ステーション本体

・外部アンテナ



・延長アンテナ



・AC アダプタ

・電源ケーブル（2 ピン）

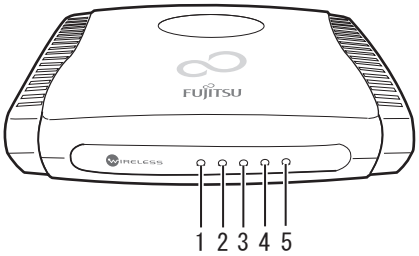
・壁かけ用のネジ類
（ネジ ×2、プラスチックプラグ ×2）
・壁かけ用ネジ位置決めテンプレート
・延長アンテナ壁取り付け用付属品一式
（プレート ×1、プレート用ネジ ×3、壁取り付け用ネジ ×3、プラスチックプラグ ×3）
・取り付けユニット一式（本体用／ AC アダプタ用）
- 本体用取り付けユニット
ユニット類（本体取り付けユニット ×1、固定ユニット ×1）
添付品（ユニット取り付け用ネジ ×4、ワッシャ ×4、固定用小ネジ ×1、プラスチックプラグ ×4）
- AC アダプタ用取り付けユニット
ユニット類（AC アダプタ取り付けユニット 1×1、AC アダプタ取り付けユニット 2×1、AC アダプタ固定プレート ×1、固定プレート用小ネジ× 2）
添付品（ユニット取り付け用ネジ ×2、ワッシャ ×2、固定用小ネジ ×1、プラスチックプラグ ×2）

取り付けユニットについて詳しくは、「設置（取り付けユニットを使用する場合）」（→ P.43）をご覧ください。
・CD-ROM
・『はじめにお読みください』
・『この機器の使用上の注意』（ARIB ラベル）
・保証書

2 各部の名称と働き

本製品の各部の名称と働きを説明します。

■前面



1 11g ランプ
2 11a ランプ
3 LAN ランプ
4 STATUS ランプ
5 PWR ランプ

□ ランプの動作

各ランプは、本製品の状態によって次のように動作します。表内で「-」になっているランプの動作は、状況により異なります。

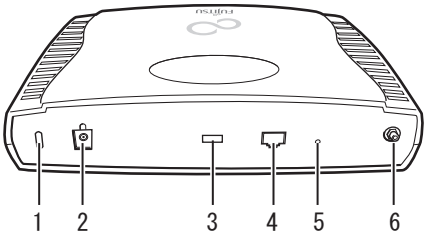
表：ランプの動作

本製品の状態	ランプの状態				
	11g ランプ	11a ランプ	LAN ランプ	STATUS ランプ	PWR ランプ
電源が切れている状態	消灯	消灯	消灯	消灯	消灯
起動中／再起動中／初期化中	-	-	-	点滅	点灯
LAN コネクタ接続中	-	-	点灯	-	点灯
LAN コネクタ未接続	-	-	消灯	-	点灯
LAN コネクタ通信中	-	-	点滅	点灯	点灯
IEEE802.11a 動作中	-	点灯	-	点灯	点灯
IEEE802.11a 通信中	-	点滅	-	点灯	点灯
IEEE802.11a 無線スイッチ OFF	-	消灯	-	点灯	点灯
IEEE802.11b/IEEE802.11g 動作中	点灯	-	-	点灯	点灯

表：ランプの動作

本製品の状態	ランプの状態				
	11g ランプ	11a ランプ	LAN ランプ	STATUS ランプ	PWR ランプ
IEEE802.11b/IEEE802.11g 通信中	点滅	-	-	点灯	点灯
IEEE802.11b/IEEE802.11g 無線スイッチ OFF	消灯	-	-	点灯	点灯
IEEE802.11a 不具合発生中	-	消灯	-	消灯	点灯
IEEE802.11b/IEEE802.11g 不具合発生中	消灯	-	-	消灯	点灯
経路異常発生中	消灯	消灯	-	点灯	点灯
初期診断失敗	-	-	-	消灯	点灯
ファームウェア書き換え中	点滅	点滅	-	点滅	点灯
設定ファイル読み込み中	-	-	-	点滅	点灯

■背面



1 盗難防止用ロック取り付け穴

市販の盗難防止用ケーブルを接続することができます。

2 DC コネクタ

添付の AC アダプタを接続します。

3 PoE 切替スイッチ

Power over Ethernet を利用して LAN ケーブルから電源を供給する場合、使用する電源供給ユニットによって PoE 切替スイッチを切り替えます。電源供給ユニットは、弊社指定の製品をお使いください。

背面に向かって左が「802.3af」側（ご購入時の設定）、右が「PE11」側です。通常は、「802.3af」側から変更する必要はありません。電源供給ユニット FMWT-PE11 をお使いになる場合のみ、「PE11」側へスイッチを設定してください。

重要

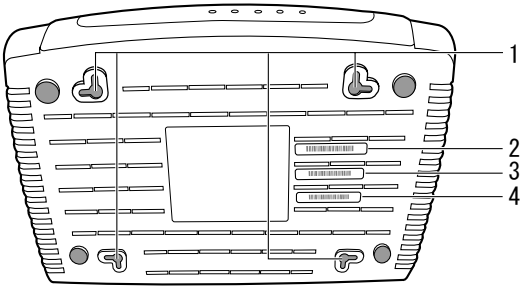
- PoE 切替スイッチを切り替えるときは、必ず LAN コネクタと AC アダプタを取り外し、電源が入っていないことを確認してから行ってください。
- 弊社指定の電源供給ユニットについては、富士通パソコン情報ページ FMWORLD.NET の http://www.fmworld.net/biz/ でご確認ください。

4 LAN コネクタ
LAN ケーブル（ストレートタイプ、クロスタイプのどちらでも可）を接続します。

5 LOAD DEFAULT ボタン
本製品の設定内容をご購入時の状態に戻すときに使います。

6 アンテナ接続部
添付の外部アンテナ、または延長アンテナを接続します。

■底面



1 壁かけ用穴
本製品を壁に掛けて使う場合に使用します。

2 有線 LAN の MAC アドレスラベル

3 無線 LAN（IEEE802.11a）の MAC アドレスラベル

4 無線 LAN（IEEE802.11b/IEEE802.11g）の MAC アドレスラベル

3 本製品の概要

本製品の特長と機能の概要について説明します。

特長

本製品の主な特長は次のとおりです。本製品の仕様については、「仕様」（→ P.202）でご確認ください。

POINT

本製品に関する情報について

本製品に関する情報を、富士通パソコン情報ページ FMWORLD.NET の、次の URL で公開しています。

URL：http://www.fmworld.net/biz/

■高速無線 LAN 通信対応

・IEEE802.11a（W52/W53）／IEEE802.11b／IEEE802.11g に準拠し、無線上で規格値 54Mbps［注 1］の通信に対応しています。

［注 1］ 表示の数値は、無線 LAN 規格の理論上の最大値であり、実際のデータ転送速度を示すものではありません。

・無線 LAN インターフェースは、無線 LAN 標準の Wi-Fi® および WPA に準拠し、Wi-Fi ロゴを取得しています。

・無線 LAN の高速化技術である、Super A および Super G 機能を搭載しています。

■最新の無線 LAN セキュリティ機能対応

・WEP キーの長さは、64 ビット、128 ビット、152 ビットに対応しています。
WEP キーによる暗号化は上記ビット数で行いますが、設定可能なビット数は固定長 24 ビットを引いた 40 ビット、104 ビット、128 ビットです。

・クライアント認証規格 IEEE802.1X（EAP-TLS、EAP-MD5、EAP-TTLS、PEAP）に対応しています。

・WPA のユーザー認証規格、および暗号化方式（TKIP、AES）に対応しています。

・IEEE802.11i (WPA2) のユーザー認証規格、および暗号化方式（TKIP、AES）に対応しています。

・無線 LAN 端末の接続、切断のログをアカウンティングサーバーに送出する「RADIUS アカウンティング」に対応しています。

・複数の SSID を設定している場合に、許可されていない SSID に無線 LAN 端末が接続することを防ぐ「SSID 認証機能」を搭載しています。

■さまざまな環境に対応したネットワークの構築をサポートする機能

・指定した有線 LAN 側経路を監視し、異常を検知したときに強制的に無線 LAN 端末をローミングさせるリンクインテグリティ機能を搭載しています。
・VLAN（タグ VLAN）機能に対応しています。
・認証 VLAN（RFC 準拠）に対応しています。
・無線 LAN の QoS 規格 WMM（IEEE802.11e EDCA）に対応しています。
・Proxy ARP に対応しています。
・LAN ケーブルからの電源の供給が可能な Power over Ethernet に対応しています。
別途、オプションの電源供給ユニットが必要です。
・無線LANインターフェースごとに、無線LAN端末の接続台数を制限することができます。

■設定／管理機能

・SNMP、拡張 MIB、トラップによる管理機能を搭載しています。
・Web ブラウザを使った設定／管理機能を採用しています。
・無線 LAN 端末からの本製品の設定画面へのログインや SNMP アクセスを拒否する、アクセス制限機能を搭載しています。また、ポート番号指定による設定画面へのログイン制限機能を搭載しています。
・周辺無線 LAN アクセスポイント検出機能を搭載し、不正な無線 LAN アクセスポイントの設置などを検出することができます。
・複数台の本製品を一括設定できる無線 LAN アクセスポイント管理ツール「Dr.WLAPPer」を標準添付しています。
Dr.WLAPPer の機能について詳しくは、「Dr.WLAPPer の機能について」（→ P.148）をご覧ください。

本製品がサポートする機能の概要

本製品がサポートする主な機能の概要を説明します。

■外部アンテナと延長アンテナ

本製品は内蔵アンテナの他に、外部アンテナと延長アンテナの 2 種類のアンテナを標準添付しています。アンテナは 2 種類のうち、どちらか 1 つを本製品に取り付けて使用します。

標準では外部アンテナを使用しますが、本製品と無線 LAN 端末の距離が離れていたり、間に障害物があったりすると、本製品の電波が無線 LAN 端末に届くまでに弱くなり、通信速度が低下するなどの現象が発生します。

このような場合には、延長アンテナに変更してアンテナを適切な場所に設置すると、電波強度が改善され、通信距離を延ばすことができます。

■Power over Ethernet（オプション）

無線 LAN アクセスポイントの設置場所は、壁や天井など高くて障害物の少ない場所が適していますが、一般的にこのような場所の近くにはコンセントがなく、電源ケーブルを接続するのが困難です。このような場合に便利なのが、Power over Ethernet 機能です。

Power over Ethernet は、LAN ケーブル（カテゴリー 5 のツイストペアケーブル）を経由して、無線 LAN アクセスポイントに電源を供給する機能です。この機能を利用することにより、電源ケーブルが不要となり、新たにコンセントを作るなどの電源工事が不要となります。

本製品で Power over Ethernet 機能を利用する場合には、別途、弊社指定の Power over Ethernet 用の電源供給ユニットが必要です。弊社指定の電源供給ユニットは、富士通パソコン情報ページ FMWORLD.NET の次の URL でご確認いただけます。

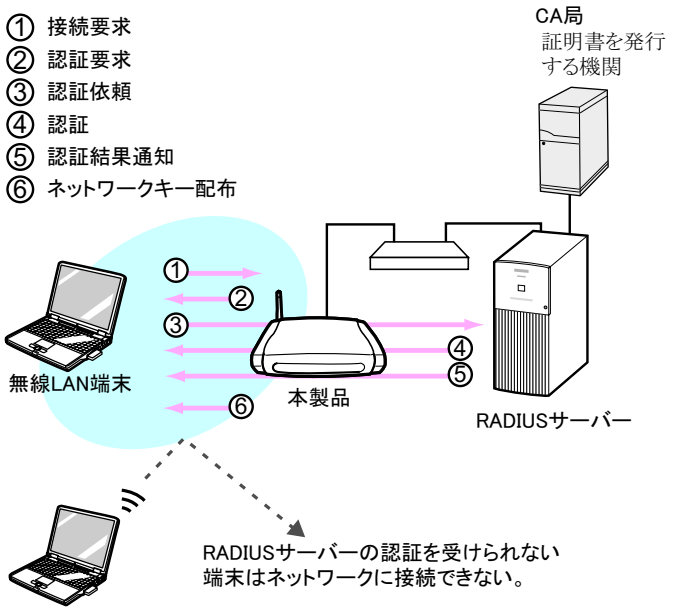
URL：http://www.fmworld.net/biz/

■IEEE802.1X ／ WPA ／ IEEE802.11i (WPA2)

IEEE802.1X、WPA、または IEEE802.11i (WPA2) 機能を利用すると、通常無線 LAN アクセスポイントで行っている無線 LAN 端末の管理を、RADIUS サーバーと呼ばれる認証用のサーバーで行います。本機能を利用すると、次のことが行えます。

・電子証明書および ID ／パスワードを使用したクライアント認証（EAP+RADIUS）を行います。
　無線 LAN 端末は、RADIUS サーバーとの認証が成功しない限りネットワークにアクセスすることはできません。これにより、認証されていない無線 LAN 端末からの通信をすべて拒否し、認証された無線 LAN 端末のみ通信できるようにします。
・無線 LAN アクセスポイントを複数台設置しているネットワーク環境では、各無線 LAN アクセスポイントに接続している無線 LAN 端末のアクセスを、RADIUS サーバーで一元管理できます。
・認証プロトコルに、EAP-TLS、EAP-TTLS、PEAP を使用すると、ネットワークキーを自動生成し、定期的に変更、配布するため、ネットワークキーの解読を困難にし、セキュリティレベルを高めることができます。
・WPA、または IEEE802.11i (WPA2) 機能を使用すると、セキュリティレベルの高い暗号化方式、TKIP または AES を使用することができます。

次の図は、無線 LAN 端末と RADIUS サーバー間で行われる認証の流れのイメージです。



□ SSID 認証

SSID 認証機能を使う場合は、各無線 LAN 端末が接続するべき SSID を RADIUS サーバーで管理します。無線 LAN 端末が本製品を介して RADIUS サーバーとの認証に成功すると、この端末の本来接続するべき SSID が、RADIUS サーバーから本製品に通知されます。本製品は、通知された SSID と実際に端末が使用している SSID を比較し、同じであった場合のみこの端末からの接続を許可します。本製品の VLAN 機能を有効にして複数の SSID（ネットワークプロファイル）を設定している場合に、1 台の無線 LAN 端末が複数の SSID を利用して想定外の VLAN に接続するなどの不正ネットワーク利用を防ぐことができます。

「IEEE802.1X ／ WPA ／ IEEE802.11i (WPA2)」（→ P.26）の図を例にすると、RADIUS サーバーから通知される「認証結果通知」に、端末が接続するべき SSID が付加情報として本製品に通知されます。本製品はこのとき、通知された SSID と実際に端末が使用している SSID を比較し、同じであれば認証成功の通知を端末に送信して端末の接続を許可します。RADIUS サーバーからの認証結果が成功だったとしても、比較した SSID が異なる場合には本製品から端末に対して認証不可の通知を送信し、接続を許可しません。

■RADIUS アカウンティング

RADIUS アカウンティング機能を利用すると、無線 LAN のアクセスログを管理することができます。アクセスログの管理はアカウンティングサーバーと呼ばれるアカウンティング用のサーバーが行います。本機能を利用すると、次のことが行えます。

- 無線 LAN 端末の接続時および切断時にアカウンティングサーバーへアクセスログを送信するため、どのユーザーが、いつ、どのくらいアクセスしたかなどの情報をアカウンティングサーバーに蓄積できます。
- 無線 LAN アクセスポイントを複数台設置しているネットワーク環境では、各無線 LAN アクセスポイントに接続している無線 LAN 端末のアクセスログを、アカウンティングサーバーで一元管理できます。

■ VLAN

VLAN は、企業内のネットワークにおいて物理的なネットワーク接続とは別に、仮想的なネットワークグループ（VLAN グループ）を形成する機能です。同じネットワークセグメント内の端末やネットワーク資源であっても、VLAN グループが異なると通信ができません。

ネットワークを VLAN でグループ分けすると、次のような利点があります。

・不必要なパケットが異なる VLAN グループへは送信されないため、ネットワークトラフィックを抑制し、コリジョンの発生を抑えることができます。
・ネットワークをグループ化することにより、不要な端末やネットワーク資源へのアクセスを制限し、セキュリティを確保することができます。

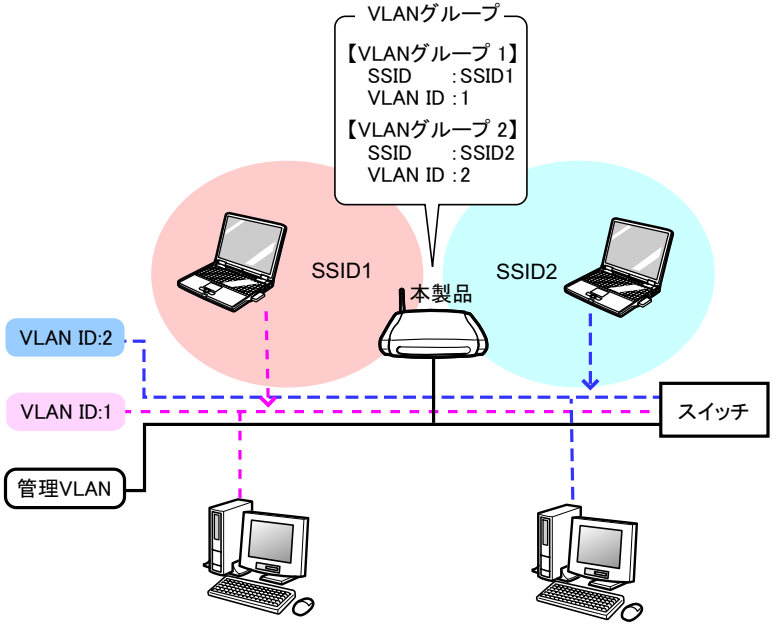
VLAN を構築するためには、別途、VLAN に対応したスイッチやルータが必要です。

本製品では、通常 VLAN と認証 VLAN をサポートしています。

□ 通常 VLAN

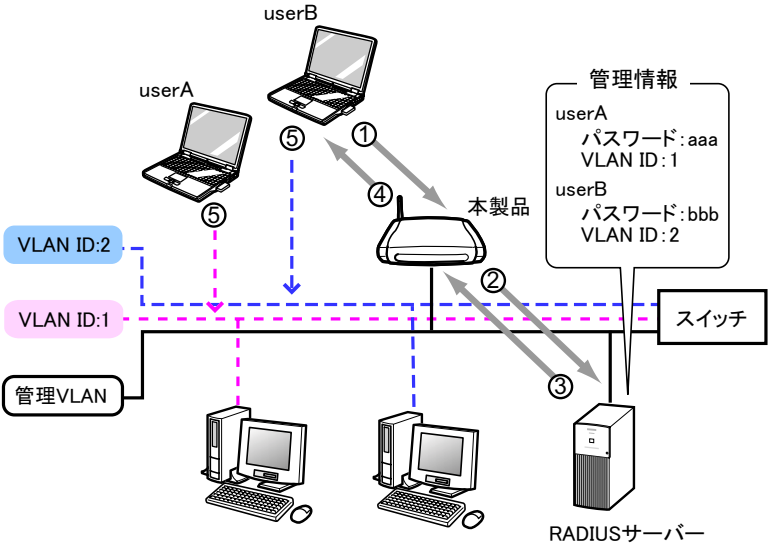
本製品は、無線 LAN の SSID と有線 LAN の VLAN ID を関連付けることで、無線 LAN 端末を SSID ごとに異なる VLAN グループに所属させることができます。これを通常 VLAN といいます。

次の図では、VLAN ID の「1」と「SSID1」を関連付けて VLAN グループ 1 を形成し、VLAN ID の「2」と「SSID2」を関連付けて VLAN グループ 2 を形成しています。同じ VLAN グループ内のコンピュータどうしは通信できますが、異なる VLAN グループのコンピュータとは通信できません。



□ 認証 VLAN

認証 VLAN では、RADIUS サーバーがユーザー情報とともに VLAN ID を管理しています。無線 LAN 端末は、ネットワーク接続時に本製品を介して RADIUS サーバーとの認証を行います。認証に成功した無線 LAN 端末のみが RADIUS サーバーから接続可能な VLAN ID を割り当てられて、その VLAN グループのネットワークに接続できるようになります。RADIUS サーバーが VLAN ID の管理／割り当てを行うため、SSID やセキュリティなどの無線 LAN の設定に関係なく端末ごとに VLAN ID を設定できます。物理的な場所などの制約を受けず、より柔軟な VLAN ネットワークを構築することができます。



① 接続要求 ② 認証要求 ③ 認証 / VLAN ID通知 ④ VLAN IDの割り当て ⑤ VLAN接続

□ マルチプル SSID

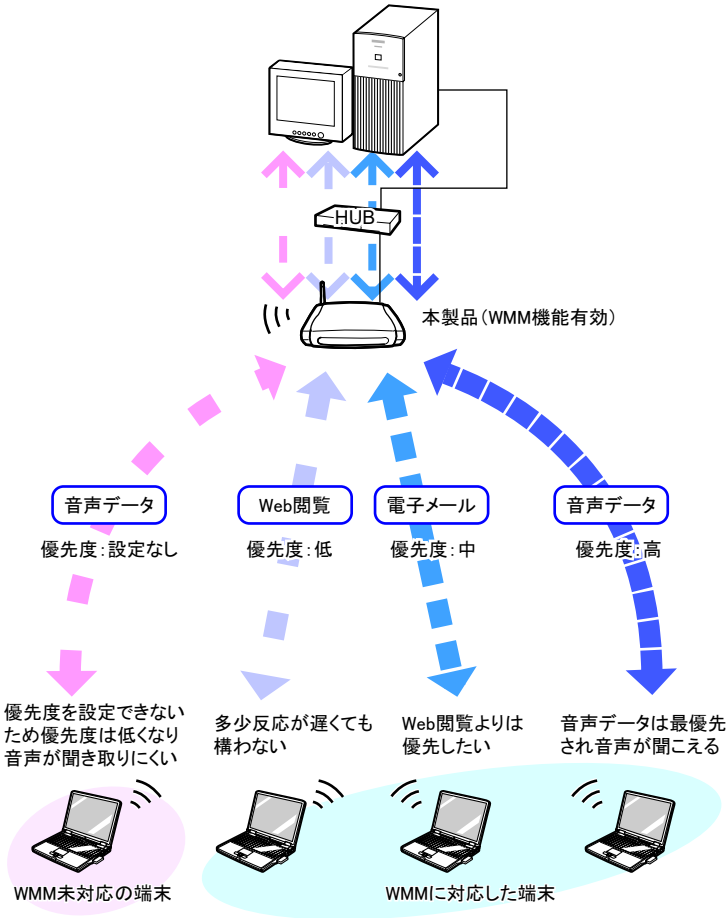
VLAN を有効に設定すると、IEEE802.11b/IEEE802.11g インターフェースと IEEE802.11a インターフェースにそれぞれ複数の異なる SSID を作成することができるようになります。本製品 1 台で、異なる無線 LAN ネットワークを最大 16 個まで同時に構築することができます。

□ マルチプルセキュリティポリシー

VLAN を有効に設定すると最大 16 個のセキュリティポリシーを作成することができ、SSID ごとに異なるセキュリティポリシーを使い分けることができます。
この機能により、WEP のみサポートしている無線 LAN 端末と WPA をサポートしている無線 LAN 端末が共存する場合に、WPA をサポートしている無線 LAN 端末のセキュリティレベルを下げることなく共存させることが可能となります。

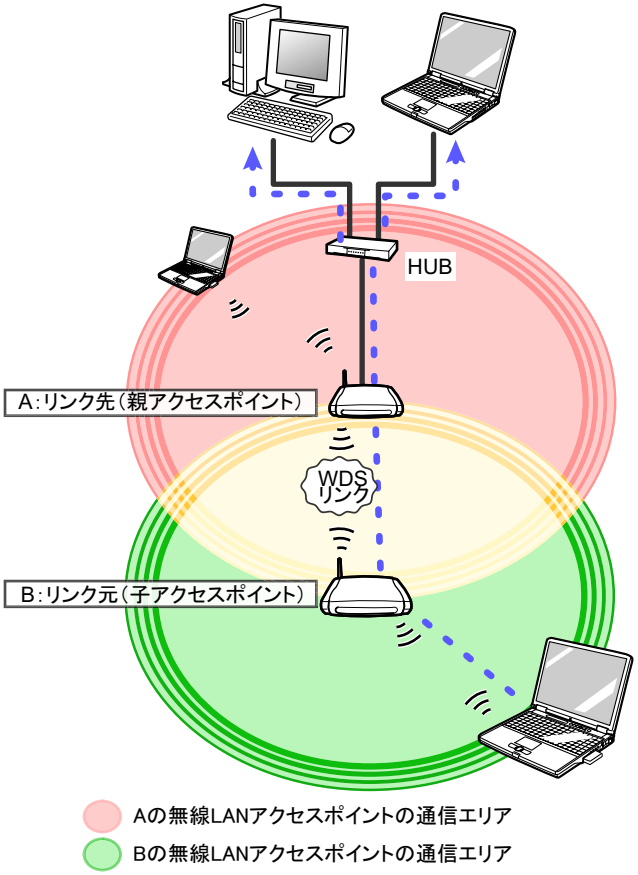
■WMM

WMM は、無線 LAN 上で、音声や映像などを扱うリアルタイムコンテンツの通信品質を保証するための技術で、IEEE802.11e で策定されている QoS 規格のひとつです。
無線 LAN を利用して、音声や映像などのマルチメディアデータを扱う場合、通信帯域不足やパケット遅延、パケットの損失などが原因で、音声や映像が途切れてしまったりすることがあります。このような問題を解決するために、WMM ではデータの種類によってアクセスカテゴリと呼ばれる 4 種類のカテゴリに分類し、カテゴリごとに優先順位をつけて通信を制御します。音声や動画などのマルチメディアデータを、テキストなどのデータより優先的に制御することで、無線 LAN 上で、品質のよいリアルタイムコンテンツを実現します。
なお、WMM 機能を使用する場合は、無線 LAN 端末が WMM に対応している必要があります。また、無線 LAN 端末に QoS に対応したアプリケーションソフトが必要です。



■WDS（アクセスポイント間通信）

無線 LAN アクセスポイントどうしを無線通信でリンクさせる機能で、アクセスポイント間通信、リピータ機能などと呼ばれる場合もあります。WDS 機能を使ってリンクさせる 2 台の無線 LAN アクセスポイントのうち、リンク先となるものを親アクセスポイント、リンク元となるものを子アクセスポイントと呼びます。なお、WDS リンクで数珠つなぎ接続することはできません。



本製品の WDS 機能を利用して、次のような使い方ができます。

・有線 LAN に接続している本製品に別の本製品を WDS リンクさせて、通信距離を延長したり電波の届かない場所へ電波を中継したりする。
無線 LAN 端末から有線 LAN ネットワークに通信するためには、端末の通信エリアに、有線 LAN に接続している無線 LAN アクセスポイントを設置する必要がありますが、建物の構造上の理由などにより、有線 LAN を引くことができない場所や、電波の死角となる場所ができてしまう場合があります。このような場合に、有線 LAN ネットワークに接続している本製品の通信エリアに、電波の中継役となる別の本製品を子アクセスポイントとして設置して WDS リンクさせます。こうして、有線 LAN に接続している本製品の通信範囲を拡張して、今まで無線 LAN で通信できなかったエリアからでも無線 LAN 端末から有線 LAN ネットワークに通信できるようになります。
・異なるネットワークにそれぞれ接続されている無線LANアクセスポイントどうしをWDS リンクさせて、双方のネットワーク間の通信を可能にする。
本製品を使った 2 つの異なるネットワークがあるとき、それぞれのネットワークの本製品どうしを WDS リンクさせることによって、それぞれのネットワークに接続している端末やサーバー間で通信を行えるようにすることができます。このようなことを行う場合、従来は LAN ケーブルやハブを使って無線 LAN アクセスポイントどうしを接続する必要がありましたが、WDS 機能を利用すれば、配線の心配をする必要がありません。

WDS リンクを行う親アクセスポイント、子アクセスポイントの設定に関する注意事項については、次の項目をご覧ください。

・IEEE802.11b/IEEE802.11g インターフェースで WDS 機能をお使いになる場合は、「WDS 機能を利用する場合の注意事項」（→ P.75）をご覧ください。
・IEEE802.11a インターフェースで WDS 機能をお使いになる場合は、「WDS 機能を利用する場合の注意事項」（→ P.85）をご覧ください。

■ Proxy ARP

ネットワークからの ARP 要求を無線 LAN ネットワークへ転送せずに、無線 LAN アクセスポイントが代理で ARP 要求に応答する機能です。

ARP とは、通信相手となるホストの IP アドレスを元に MAC アドレスを取得するためのプロトコルです。通信相手の IP アドレスを指定した ARP 要求に対して、その IP アドレスを持つホストが自身の MAC アドレスを返信することで、アドレス解決をします。ARP の要求パケットは、ネットワーク上にブロードキャストされるため、ネットワーク全体に負荷がかかります。

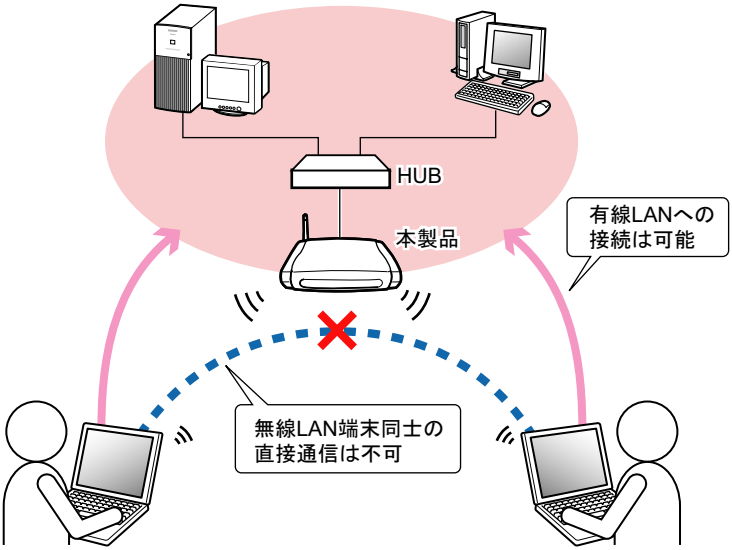
Proxy ARP 機能が無効な場合は、ブロードキャストパケットである ARP 要求パケットを無線 LAN に転送する必要があるため、無線 LAN のトラフィックに負荷がかかります。

Proxy ARP 機能を有効にすると、本製品は、接続している無線 LAN 端末の IP アドレスとホスト名との対応情報を保持するテーブル（ARP テーブル）に情報を登録し、このテーブルに登録されている無線 LAN 端末への ARP 要求のパケットを転送しません。[注 1] ARP 要求に指定された IP アドレスが、接続中の無線 LAN 端末のアドレスである場合には、本製品が ARP 要求に対して、該当する無線 LAN 端末の MAC アドレスを返信します。こうすることで、無線 LAN のトラフィックを軽減します。

[注 1] 本製品に接続してからまったく通信をしていない無線 LAN 端末の場合は、アドレス情報が ARP テーブルに登録されていないため、この端末に対する ARP 要求は無線 LAN に転送されます。
また、無通信切断タイマー機能で切断された無線 LAN 端末は本製品の ARP テーブルの登録から削除されます。

■プライバシープロテクション

本製品の初期状態では、同じ無線 LAN アクセスポイントに接続している無線 LAN 端末はお互いに通信できますが、プライバシープロテクション機能を利用すると、無線 LAN 端末間の通信を不可にすることができます。他の無線 LAN 端末からの個人情報の盗み見や、共有フォルダへのアクセスを防御できます。これにより、無線 LAN スポットサービスなど不特定多数の利用者が存在する環境で、各利用者のプライバシーを保護することができます。次の図は、プライバシープロテクション機能のイメージです。



■ローミング

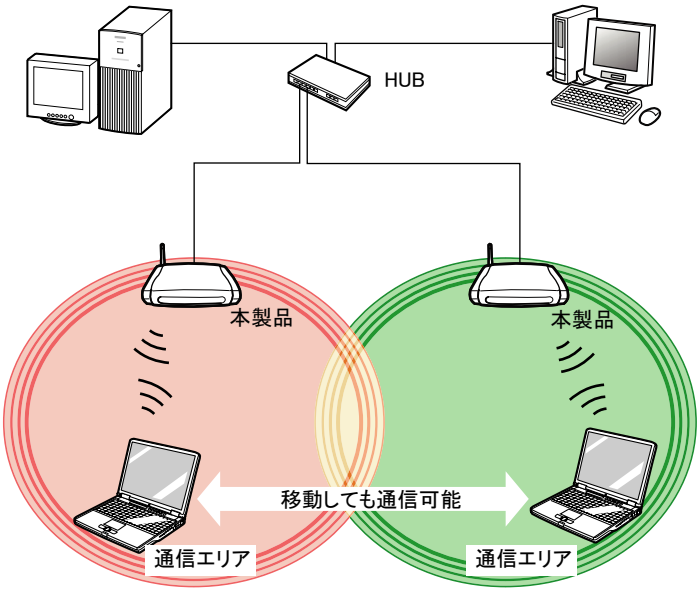
ローミングとは、無線 LAN 端末が、複数の無線 LAN アクセスポイント間を移動できるようにする機能です。ローミングの目的は、大きく分けて次の 2 つがあります。

・広い範囲で無線 LAN 端末の接続を維持する
無線 LAN 端末が無線 LAN アクセスポイントの通信エリア外に移動しても、同一 LAN 上の別の無線 LAN アクセスポイントに自動的に切り替えて、接続を維持できるようにします。例えば、ビルの各フロアに無線 LAN アクセスポイントを設置しておくことで、無線 LAN 端末がフロア間を移動しても、設定の変更などを意識する必要なく、ネットワークにアクセスできるようにします。

・ネットワーク機器や経路で障害が発生した場合の通信経路を確保する
通信経路上のネットワーク機器や経路に障害が発生した場合に、別の経路へ移行できるように、無線 LAN アクセスポイントを複数設置して通信経路を二重化しておきます。通信中の経路で異常が発生した場合に、無線 LAN アクセスポイントが自動的に切り替わって別の経路へ移行できるので、無線 LAN 端末の通信は途切れません。ネットワークの無停止運用が可能となり、システムの信頼性が向上します。

［注］　ご使用になる環境によっては、接続先のアクセスポイントが切り替わる際に通信が一時的に途切れることがあります。

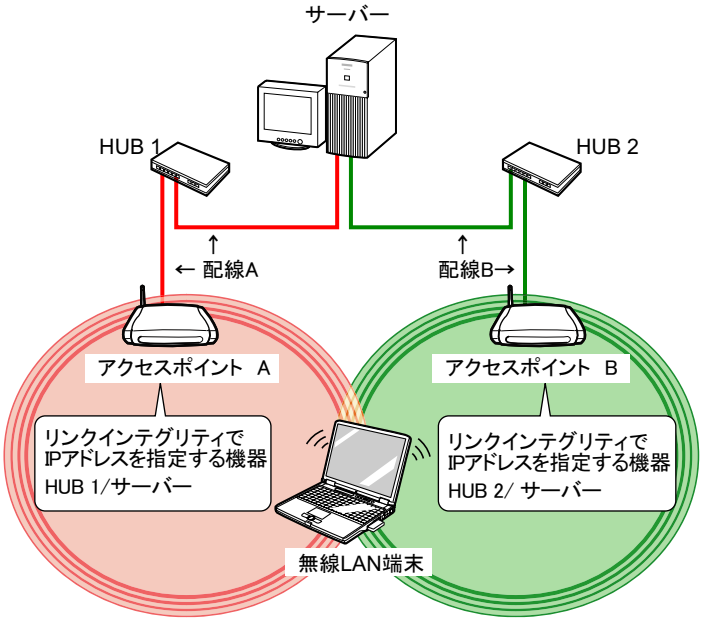
次の図は、ローミングのイメージです。



□ リンクインテグリティ

リンクインテグリティは、ローミング機能を使用しているネットワークで利用できる機能です。本機能を利用して、本製品は指定した有線 LAN 側経路（本製品、本製品に接続している有線経路、HUB）を常時監視します。そして、経路の異常を検知すると本製品の無線電波を停止して、強制的に無線 LAN 端末をローミングさせます。こうして、無線 LAN 端末がネットワークから切断されるのを防ぎます。

次の図の場合、アクセスポイント A はリンクインテグリティ機能により HUB1、およびサーバーまでの配線 A で異常が発生した場合にそれを検出し、自動的に電波を停止します。その結果、アクセスポイント A 経由で通信を行っていた無線 LAN 端末はアクセスポイント B にローミングし、配線 B の経路を使ってネットワークへの接続を維持できるようになっています。



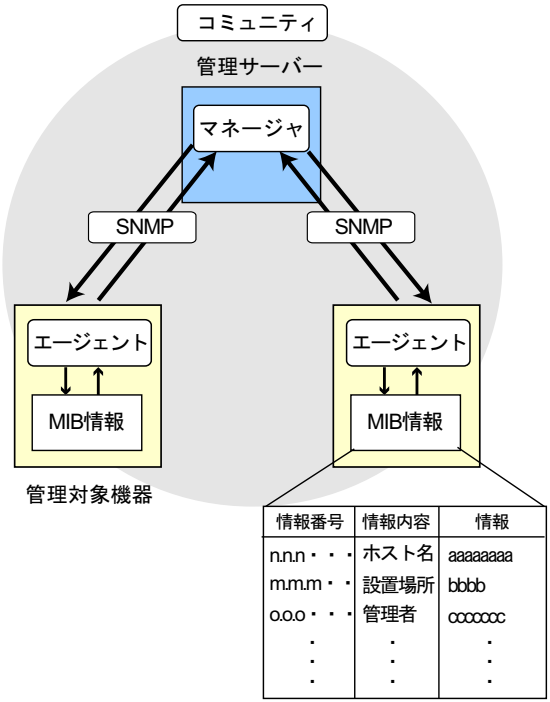
■SNMP ／ MIB 対応

ブラウザ設定画面やツールを使用する他に、SNMP を使用して本製品の監視、および設定を行うことができます。

SNMP を使用するときは、本製品を管理するサーバーに SNMP マネージャプログラムを用意し、1 つ、または複数の管理情報データベース（MIB）を SNMP マネージャプログラムのデータベースで管理します。

SNMP エージェントとなる本製品は MIB を操作して、マネージャからの要求に対し本製品のステータス返信や設定の変更を行います。また、本製品に特別なステータス変化が発生した場合は、トラップをマネージャに通知します。したがって、SNMP によるネットワーク監視を行うと障害の早期発見に役立ち、ネットワーク障害にすぐに対応できます。

次の図は、SNMP を利用してマネージャとエージェント間で情報をやり取りするイメージです。



マネージャとエージェントの間では、次の 3 種類のやり取りによって機器の管理を行います。

・マネージャからの情報要求に対する応答（Get）
マネージャから本製品のステータスや統計情報を要求された場合、本製品の MIB 情報を取得して応答します。
・マネージャからの MIB 情報の変更要求に対する応答（Set）
マネージャから MIB 情報の変更を要求された場合、本製品の MIB 情報の設定を変更します。
・ステータス変化の通知（Trap）
本製品に特別な状態の変化が発生した場合、エージェントからマネージャに自発的に通知します。これをトラップ（Trap）といいます。

■ syslog

syslog とは、システムで発生したイベントや情報のログを、メッセージとしてネットワーク上に転送したり、ファイルに記録したりする機能です。
本製品では、ログを syslog サーバーに通知することができます。ログを通知することにより、syslog サーバー上で本製品の監視を行うことができます。障害の早期発見と解決に役立ちます。

■簡易ロードバランス（接続台数制限）

あらかじめ本製品の無線インターフェースごとに接続可能な無線LAN端末の数を設定しておき、接続数が設定した制限台数に達した場合はそれ以上の無線 LAN 端末が本製品に接続できないようにします。1 つの無線 LAN インターフェースの制限台数を 1 ～ 30 台の範囲で設定でき、両方の無線 LAN インターフェースの合計が 40 台を超えないように設定します。接続数を制限することで、本製品の通信品質を維持し、安定したネットワーク運用を可能にします。例えば次のようなネットワークで利用すると効果的です。

・無線 LAN を利用して音声や映像などのマルチメディアデータを扱う場合
　1 台の無線 LAN アクセスポイントに接続できる端末数を制限することで通信品質を維持し、端末で音声や映像が途切れてしまうのを防ぎます。

・ローミング環境
　無線 LAN 端末のアクセスが集中する場所などには、本製品を複数台設置して、それぞれの本製品に接続できる端末数を制限しておきます。こうすることで、設定した数を超える端末は別の本製品に接続するようになり、1 台の無線 LAN アクセスポイントにアクセスが集中して処理速度が低下するのを防ぎます。

2

第 2 章

準備

本製品の設定を行う前に、設置と設定方法、およびネットワークへ導入するまでの手順を説明します。

1 設置方法

設置場所に関する注意事項と設置方法について説明します。

設置場所について

本製品の設置場所について次のことをご確認いただき、良好に動作する場所を実際にお試しいただいたうえでお使いください。

・本製品は、他の電気機器から離して使用してください。本製品と電源が入った電気機器を近づけていると、正常に通信できなかったり、電気機器の障害になったりすることがあります。正常に通信できない場合は、使用するチャンネルや使用場所を変更してください。
・放送局や無線機などが近く、正常に通信できないときは、本製品の設置場所を変えてみてください。周囲の電波が強すぎると、正常に通信できないことがあります。
・本製品の上または下に他の機器を重ねて設置しないでください（段積みの禁止）。
・風通しの良い場所に設置してください。

■IEEE802.11a 準拠（5GHz 帯）をお使いになる場合

・通信距離は見通し半径 15m 以内（無線 LAN 通信の推奨値）となります。ただし、無線 LAN の特性上、ご利用になる建物の構造・材質／障害物／ソフトウェア／設置状況／電波状況などの使用環境により通信距離は異なります。また、通信速度の低下や通信不能となる場合もありますのであらかじめご了承ください。
・本製品は、電波法の定めにより屋外では使用できません。屋内でのみご使用ください。
・W53 がサポートする周波数帯（52 ～ 64ch）を使用して運用している際に航空管制レーダーや気象レーダーなどで使用されるレーダー波を検出すると、本製品は、IEEE 802.11a インターフェースで使用するチャンネルを変更するために、ただちに再起動します。再起動中は IEEE 802.11a、および IEEE 802.11b/g のすべての無線 LAN 端末の通信が切断されますが、再起動後、引き続き通信が可能になります。IEEE 802.11a インターフェースのチャンネルは、再起動後は 36 チャンネルに変更されます。

■IEEE802.11b 準拠／ IEEE802.11g 準拠（2.4GHz 帯）をお使いになる場合

・通信距離は見通し半径 25m 以内（無線 LAN 通信の推奨値）となります。ただし、無線 LAN の特性上、ご利用になる建物の構造・材質／障害物／ソフトウェア／設置状況／電波状況などの使用環境により通信距離は異なります。また、通信速度の低下や通信不能となる場合もありますのであらかじめご了承ください。
・Bluetooth® 機器との電波干渉について
無線 LAN と Bluetooth® 機器は、同一周波数帯（2.4GHz）を使用するため、Bluetooth® 機器を搭載したコンピュータの近辺で本製品を使用すると、電波干渉が発生し、通信速度の低下や接続不能になる場合があります。この場合、次の対策を行ってください。
- Bluetooth® 機器を搭載したコンピュータからは、10m 以上離れた場所で使用してください。

- 10m 以内で使用する場合は、本製品の電波を停止するか Bluetooth® 機器の電源を切ってください。

設置と接続

本製品の組み立て、設置、および他の機器との接続方法を説明します。

■アンテナの接続

添付の外部アンテナ、または延長アンテナを本製品に接続します。
外部アンテナと延長アンテナの使い分けについては、「外部アンテナと延長アンテナ」（→P.25）をご覧ください。

重要

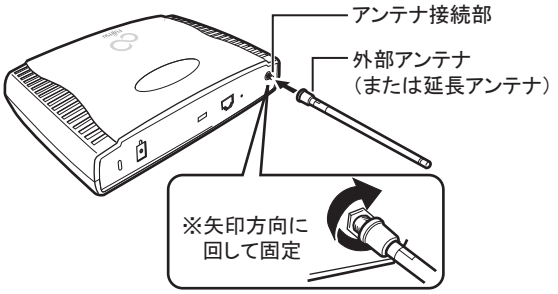
外部アンテナ、または延長アンテナは必ず接続してください

外部アンテナ、または延長アンテナは必ず接続してください。外部アンテナ、または延長アンテナを接続しないと、本来の通信性能が得られません。

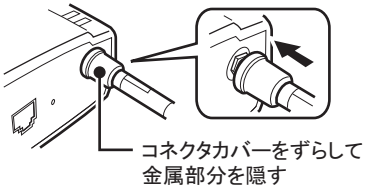
延長アンテナをお使いになる場合

延長アンテナをお使いになる場合は、本体設置後に接続してください。

1 本製品背面のアンテナ接続部に、添付の外部アンテナ、または延長アンテナを、次の図のように接続します。



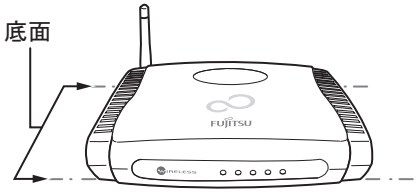
2 アンテナに付属しているコネクタカバーで、アンテナ接続部の金属部分を隠します。



延長アンテナの場合は、机などに置くか、または壁などにネジで取り付けてお使いください。壁に取り付ける場合は、延長アンテナに添付の壁取り付け用付属品一式をお使いください。

■設置（横置きの場合）

次の図のように、本製品の底面が下になるように設置します。



■設置（壁かけの場合）

次のように設置します。

重要

- 設置後、壁への充分な取り付け強度があることをご確認ください。落下によるけがや本製品破損の原因になります。
- 取り付けを行う壁の種類によっては、設置に必要な条件が変わりますので、添付品（ネジ・プラスチックプラグ）をお使いいただけない場合があります。

1 **本製品を壁にかける向きを決めます。**

本製品の壁かけ用穴は 4 つありますが、壁かけの向きによって、そのうちの 2 つをネジにかけます。

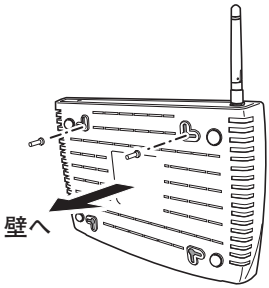
2 **本製品に添付の壁かけ用ネジ位置決めテンプレートをセロハンテープなどで貼って、壁にネジ位置の印を付けます。**

3 **壁かけ用ネジ位置決めテンプレートを取り外します。**

4 **印を付けた位置に、壁かけ用のネジを取り付けます。**

ネジの頭と壁の間が 5mm 程度離れるように取り付けます。

5 **本製品底面の壁かけ用穴を、壁かけ用のネジに次の図のようにかけます。**



■設置（取り付けユニットを使用する場合）

取り付けユニットを使用して、本製品および本製品の AC アダプタを壁に設置することができます。

重要

・天井に設置する場合は、設置事業者へご依頼ください。

POINT

壁に設置する場合

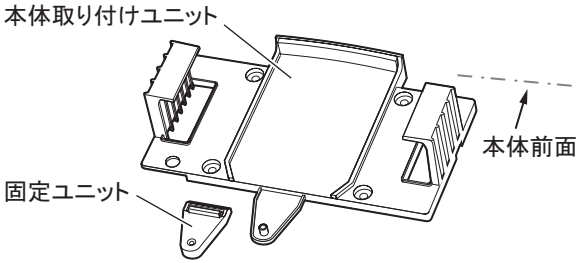
本製品の前面が下向きになるように本体取り付けユニットを取り付けてください。
AC アダプタ用取り付けユニットを使用する場合は、AC アダプタのケーブルや電源ケーブルが上方向に出るように取り付けてください。

□ 取り付けユニット一式の内容

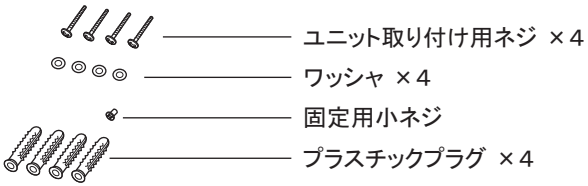
取り付けユニットには、次のものが含まれます。

本体用取り付けユニット一式

【ユニット類】

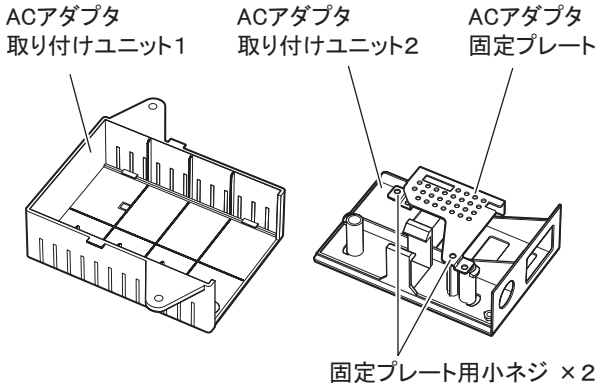


【添付品】

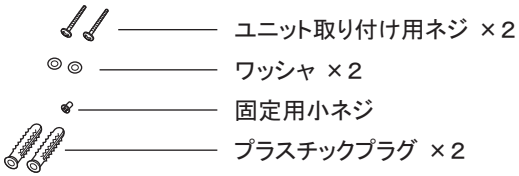


AC アダプタ用取り付けユニット一式

【ユニット類】



【添付品】



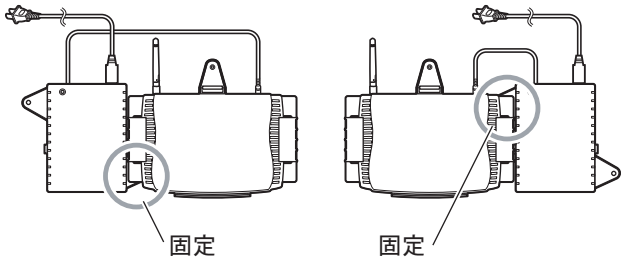
重要

・取り付けを行う壁の種類によっては、設置に必要な条件が変わりますので、添付品（ネジ・プラスチックプラグ）をお使いいただけない場合があります。

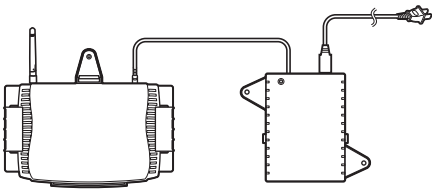
□ 設置パターン

次の 3 つの設置パターンがあります。

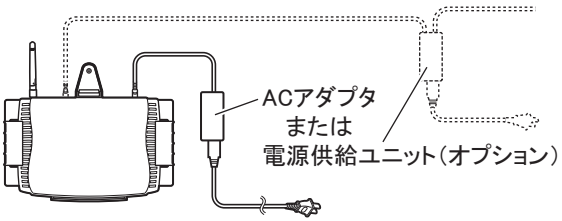
・設置パターン 1：AC アダプタ用取り付けユニットを本体用取り付けユニットに固定して設置
AC アダプタ用取り付けユニットは、本体用取り付けユニットの左右どちらでも固定することができます。



・設置パターン 2 : AC アダプタ用取り付けユニットを本体用取り付けユニットに固定せず離して設置
本製品の DC コネクタに、AC アダプタのケーブルが届くことを確認して、本体用取り付けユニットと AC アダプタ用取り付けユニットを取り付ける位置を決定してください。



・設置パターン 3 ：本体用取り付けユニットのみを設置



□ 設置手順

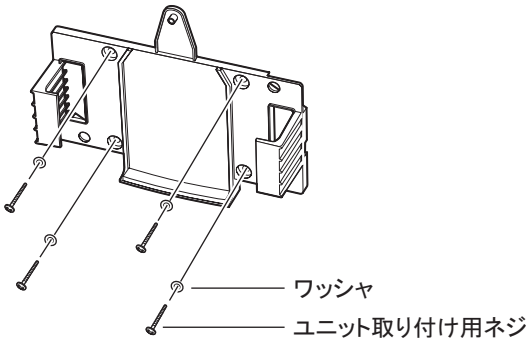
次のように設置します。

重要

・設置後、壁への充分な取り付け強度があることをご確認ください。落下によるけがや本製品破損の原因になります。

1 本体取り付けユニットを取り付けます。

図の 4 箇所を、ユニット取り付け用ネジでネジ止めします。ネジ止めの際はワッシャを使用してください。

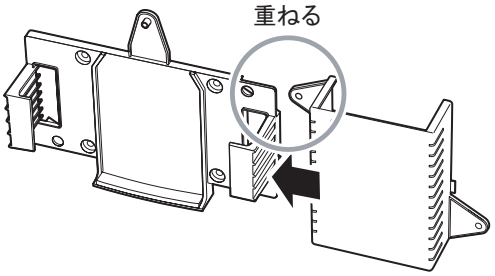


AC アダプタを設置しない場合（設置パターン 3）は、次に手順 3 に進みます。

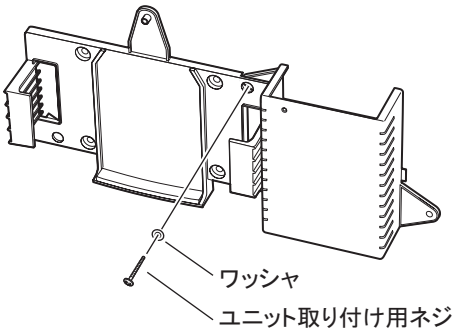
2 AC アダプタを設置する場合（設置パターン 1 または 2）は、AC アダプタ取り付けユニット 1 を取り付けます。

■ 本体取り付け用ユニットに固定する場合（設置パターン 1）

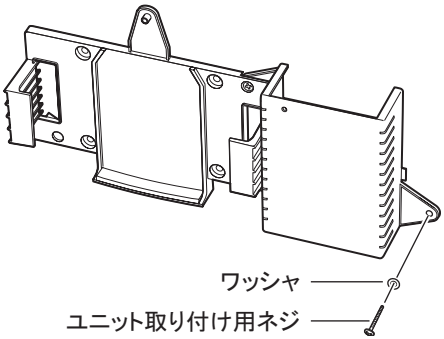
1. AC アダプタ取り付けユニット 1 の突起部のネジ穴を本体取り付けユニットの AC アダプタ取り付けユニット接続用のネジ穴に重なるようにスライドさせます。



2. ユニット取り付け用ネジでネジ止めします。ネジ止めの際はワッシャを使用してください。

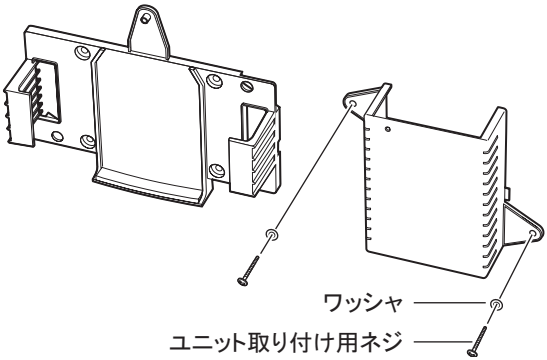


3. もう一方の突起部のネジ穴をネジ止めします。

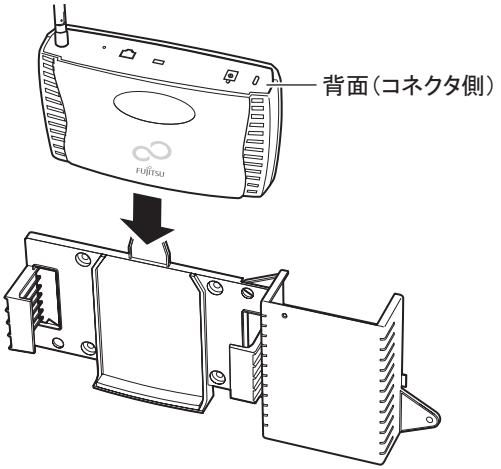


■ 本体取り付け用ユニットに固定しない場合（設置パターン 2）

1. AC アダプタ取り付けユニット 1 を、AC アダプタを設置する場所に取り付けます。
   両側の突起部のネジ穴を、ユニット取り付け用ネジでネジ止めします。ネジ止めの際はワッシャを使用してください。



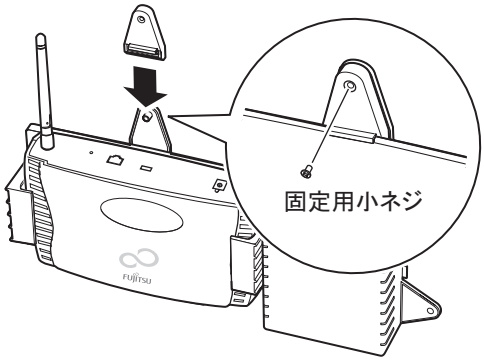
3 本製品を、本体取り付けユニットに図のように差し込みます。



重要

・本製品を固定するまでは、落ちないように手でしっかりと押さえてください。落下によるけがや本製品破損の原因になります。

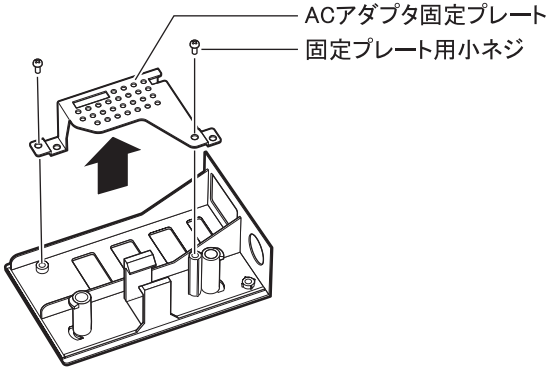
4 **本製品を固定するように本体取り付けユニット背面の突起部に固定ユニットを差し込み、固定用小ネジでネジ止めします。**



AC アダプタを設置しない場合（設置パターン 3）は、これで設置完了です。「各機器との接続」（→ P.50）にお進みください。

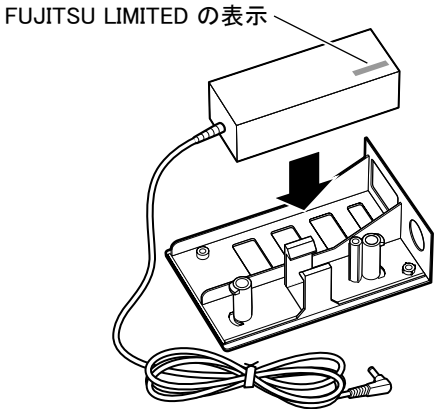
5 **AC アダプタを設置する場合（設置パターン 1 または 2）は、AC アダプタ取り付けユニット 2 から AC アダプタ固定プレートを取り外します。**

固定プレート用小ネジ（2 本）を外して取り外します。

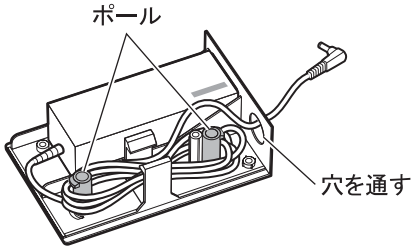


6 **AC アダプタ取り付けユニット 2 に、AC アダプタをセットします。**

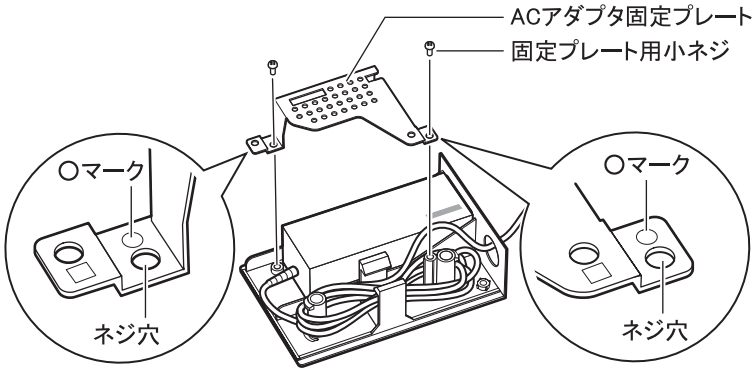
AC アダプタの「FUJITSU LIMITED」と表示されている面を上にしてセットします。



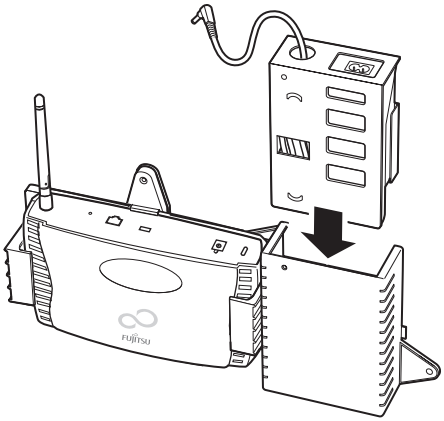
7 **AC アダプタのケーブルを AC アダプタ取り付けユニット 2 のポールに巻きつけて長さを調整し、ケーブルを丸い穴から外に出します。**



8 **図のように、AC アダプタ固定プレートの○マークのネジ穴 2 箇所が、AC アダプタ取り付けユニット 2 のネジ穴 2 箇所に重なるようにかぶせて、固定プレート用小ネジでネジ止めします。**



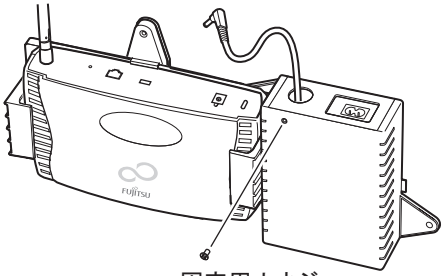
9 **AC アダプタをセットした AC アダプタ取り付けユニット 2 を、図のように AC アダプタ取り付けユニット 1 に差し込みます。**



重要

・AC アダプタ取り付けユニット 2 を固定するまでは、落ちないように手でしっかりと押さえてください。落下によるけがや本製品破損の原因になります。

10 **AC アダプタ取り付けユニット 1 と AC アダプタ取り付けユニット 2 を、取り付けユニット固定用小ネジでネジ止めします。**



固定用小ネジ

■各機器との接続

重要

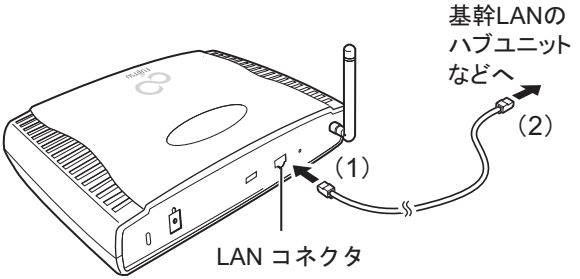
LAN ケーブルの取り付け／取り外し

LAN ケーブルの取り付け／取り外しを行うときは、本製品の電源が入っていないことを確認してください。その後、LAN ケーブルの取り付け／取り外しを行ってください。

□ AC アダプタを使用する場合

本製品のネットワークへの接続と、電源を入れる方法は次のとおりです。

1 （1）LAN ケーブルの一方を本製品背面の LAN コネクタに、（2）もう一方を基幹 LAN のハブユニットなどに接続します。



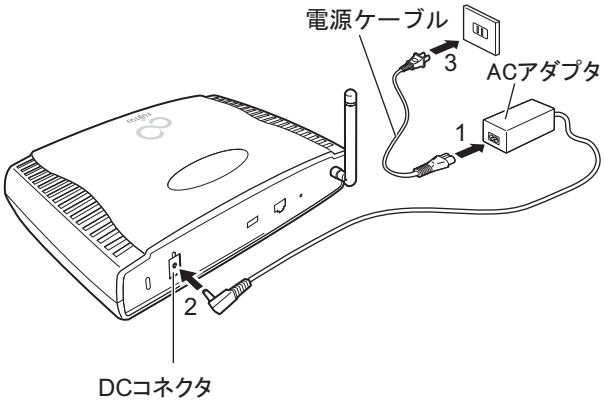
POINT

本製品の初期設定を行う場合

初期設定は、本製品と管理者用パソコンが 1 対 1 の状態で行います。
LAN ケーブルの一方を本製品背面の LAN コネクタに、もう一方を管理者用パソコンに接続します。

2 次のように本製品の電源を入れます。

1. 添付の電源ケーブル（2 ピン）と AC アダプタを接続します。
2. AC アダプタを本製品背面の DC コネクタに接続します。
3. 電源プラグをコンセントに接続します。



本製品の電源が入り、PWR ランプが点灯します。

POINT

電源を切る場合

本製品の電源を切る場合は、本製品を利用した通信を行っている端末がないことを確認してください。その後、電源プラグをコンセントから抜いてください。

□ 電源供給ユニットを使用する場合

重要

- 電源供給ユニットを接続する前に本製品背面の PoE 切替スイッチを確認してください。通常は、「802.3af」側に設定してください。電源供給ユニット FMWT-PE11 をお使いになる場合のみ、「PE11」側にスイッチを設定してください。
- PoE 切替スイッチを切り替えるときは、必ず LAN コネクタと AC アダプタを取り外し、電源が入っていないことを確認してから行ってください。

電源供給ユニットをお使いになる場合の接続と電源の入れ方については、お使いの電源供給ユニットに添付のマニュアルをご覧ください。

電源供給ユニット FMWT-PE11 をお使いになる場合、電源ケーブルは、ワイヤレス LAN ステーション FMWT-52/53 シリーズまたはワイヤレス LAN ステーション FMWT-54AG に添付の電源ケーブル（3 ピン）をお使いください。

2 設定について

本製品の設定方法と設定を行うときの注意事項について説明します。

設定方法と動作環境

本製品の設定は、管理者用パソコンからネットワーク経由で行います。管理者用パソコンに有線 LAN 機能を搭載している必要があります。
設定方法には、Web ブラウザを使用する方法と、ツールを使用する方法があります。

■ブラウザ設定画面

本製品は、Web ブラウザを使用した管理用インターフェースを標準で備えています。ブラウザ設定画面を使用するパソコンの動作条件は次のとおりです。

□ 対応ブラウザ

・Internet Explorer 5.0 以降

ブラウザ設定画面の使用方法は、次の章をご覧ください。

・基本的な使い方
「ブラウザ設定画面の使い方」（→ P.59）
・設定の詳細
「設定の詳細（ネットワークの設定）」（→ P.65）
「設定の詳細（管理／メンテナンス機能）」（→ P.119）

■Dr.WLAPPer（ドクターラッパー）

無線 LAN アクセスポイント管理ツール「Dr.WLAPPer」は、管理者用パソコンにインストールして使用します。動作環境は次のとおりです。

□ 対応 OS

・Microsoft® Windows® XP Professional Service pack 1 以降
・Microsoft® Windows® XP Home Edition Service pack 1 以降
・Microsoft® Windows® 2000 Professional Service pack 3 以降
Microsoft® XML Parser (MSXML) 3.0 以降がインストールされている必要があります。
Microsoft® XML Parser (MSXML) については、Microsoft のホームページをご覧ください。
・Microsoft® Windows Server™ 2003 Standard Edition

Dr.WLAPPer のインストール方法および使用方法については、「Dr.WLAPPer（ドクターラッパー）の使い方」（→ P.147）をご覧ください。

設定時のご注意

本製品の設定を行う場合は、必ず次の注意事項を守ってください。

・本製品と管理者用パソコンは、有線 LAN で接続してください。
・本製品をネットワークに接続する前に、必ず IP アドレスの設定を行ってください。
・複数のパソコンから、ブラウザ設定画面に管理者権限でログインしないでください。
・複数の Web ブラウザから、ブラウザ設定画面に管理者権限でログインしないでください。
・ブラウザ設定画面と Dr.WLAPPer で同時に管理者権限でログインしないでください。
・複数のパソコンで同時に Dr.WLAPPer を起動しないでください。
・スパニングツリー機能付きの HUB と接続していると、設定を変更した後、本製品の情報の取得に失敗する場合があります。
この場合、ブラウザ設定画面では再読み込み、Dr.WLAPPer では「最新の情報に更新」を行い、情報を取得し直してください。

3 初期設定から導入までの流れ

本製品をネットワークへ導入するまでの流れは次のようになります。

1 管理者用パソコンの初期設定を行います。

1. 管理者用パソコンの Web ブラウザのプロキシサーバーと JavaScript の設定を確認します。
   確認方法は、「Web ブラウザの設定確認」（→ P.57）をご覧ください。
2. 管理者用パソコンの有線 LAN の IP アドレスを、本製品の初期値に合わせて変更します。
   本製品の初期値は、IP　アドレスが「192.168.2.2」、サブネットマスクが「255.255.255.0」、DHCP サーバー機能が「無効」です。
   パソコンの IP アドレスの設定方法については、「パソコンの IP アドレスの設定方法」（→ P.179）をご覧ください。
3. 本製品と管理者用パソコンを LAN ケーブルで接続します。
   接続方法については、「各機器との接続」（→ P.50）をご覧ください。
4. 管理者用パソコンから本製品に対して、PING コマンドで接続確認をします。
   接続確認方法については、「パソコンからの接続確認」（→ P.184）をご覧ください。

2 本製品の初期設定を行います。

重要

・本製品と管理者用パソコンが 1 対 1 の状態で行ってください。

1. 管理者用パソコンからブラウザ設定画面にログインします。
   ログイン方法については、「開始／終了」（→ P.60）をご覧ください。
2. ブラウザ設定画面の「管理機能」メニューをクリックします。
3. 管理者情報を設定します。
   「アカウント設定」カテゴリの、「管理者ユーザー名」、「管理者パスワード」、「管理者パスワード（再入力）」を入力します。
4. 「設定」ボタンをクリックします。
5. 「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」というメッセージの画面で「キャンセル」をクリックします。
6. ブラウザ設定画面の「有線 LAN」メニューをクリックします。
7. 本製品の IP アドレスを設定します。
   「手動設定」カテゴリの「IP アドレス」に、設定する IP アドレスを入力します。
8. 「設定」ボタンをクリックします。
9. 「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」というメッセージの画面で「OK」をクリックします。
   本製品の IP アドレスを変更すると、管理者用パソコンから本製品にアクセスできなくなり、設定画面にログインできなくなる場合があります。
   必要に応じて、管理者用パソコンの IP アドレスの設定を変更してください。

10. 管理者用パソコンのブラウザ設定画面を終了します。
終了方法については、「開始／終了」（→ P.60）をご覧ください。

3 本製品を基幹 LAN に接続します。

接続方法については、「各機器との接続」（→ P.50）をご覧ください。

4 管理者用パソコンを基幹 LAN に接続します。

5 各設定を行います。

重要

・設定する内容によっては、本製品を基幹 LAN から外して、管理者用パソコンと 1 対 1 で行わなければならない場合があります。
設定する内容による注意事項については、設定項目の説明のページをご覧ください。

・ブラウザ設定画面で設定する場合
ネットワークの設定については、「設定の詳細（ネットワークの設定）」（→ P.65）をご覧ください。
管理機能の設定については、「設定の詳細（管理／メンテナンス機能）」（→ P.119）をご覧ください。
・ツールで設定する場合
Dr.WLAPPer の使用方法については、「Dr.WLAPPer（ドクターラッパー）の使い方」（→ P.147）をご覧ください。

6 無線 LAN 端末の設定を行います。

無線 LAN 端末の設定方法については、次のマニュアルをご覧になるか、お使いの機器のメーカーにお問い合わせください。
・無線 LAN 機能が標準搭載されているパソコンの場合は、パソコンのマニュアルをご覧ください。
・無線LANカードを増設した場合は、無線LANカードのマニュアルをご覧ください。

Web ブラウザの設定確認

管理者用パソコンの Web ブラウザの設定を確認します。

■プロキシサーバーの設定確認

LAN にプロキシサーバーを使用する設定になっている場合は、本製品との接続にはプロキシサーバーを使用しない設定にします。次の手順で確認、設定を行ってください。

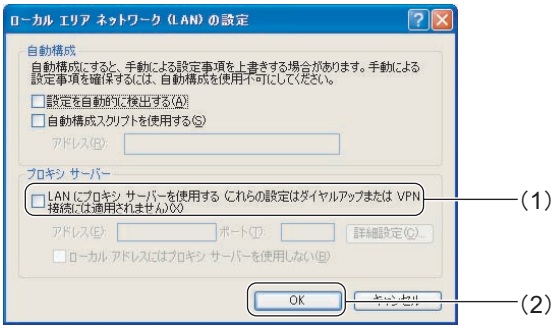
1 **Internet Explorer を起動します。**

2 **「ツール」メニュー→「インターネット オプション」の順にクリックします。**

3 **「接続」タブをクリックします。**

4 **「LAN の設定」をクリックします。**

5 **(1)「LAN にプロキシサーバーを使用する」(Internet Explorer 5 の場合:「プロキシサーバーを使用する」)が☐になっていることを確認し、(2)「OK」をクリックします。**



POINT

「LAN にプロキシサーバーを使用する」(Internet Explorer 5 の場合:「プロキシサーバーを使用する」)が☑になっている場合

次のように設定します。

1. 「詳細設定」をクリックします。
2. 「例外」に本製品の IP アドレスを入力して、「OK」をクリックします。
   本製品の IP アドレスはご購入時、「192.168.2.2」に設定されています。
   IP アドレスを変更した場合は、「例外」に入力した IP アドレスを、変更後と同じアドレスに修正してください。
   「ローカルエリアネットワーク (LAN) の設定」ウィンドウに戻ります。
3. 「OK」をクリックします。

6 **「インターネット オプション」ウィンドウで、「OK」をクリックします。**

■Web ブラウザの JavaScript 設定の確認

本製品の設定画面を使用する場合は、Web ブラウザの JavaScript が有効になっている必要があります。次の手順で確認、設定を行ってください。

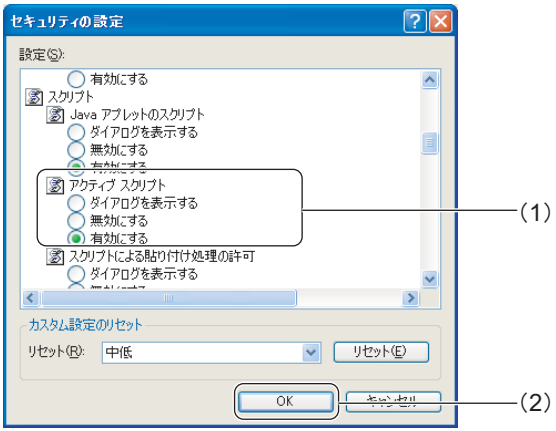
1 **Internet Explorer を起動します。**

2 **「ツール」メニュー→「インターネット オプション」をクリックします。**

3 **「セキュリティ」タブをクリックします。**

4 **「インターネット」を選択して、「レベルのカスタマイズ」をクリックします。**

5 **(1)「スクリプト」の中の「アクティブスクリプト」で、「有効にする」が◉になっていることを確認します。**
「有効にする」が◉になっていない場合はクリックして◉にし、(2)「OK」をクリックします。



Internet Explorer の JavaScript が有効になります。

3

第 3 章
ブラウザ設定画面の使い方

ブラウザ設定画面の使い方を説明します。

1 開始／終了

ブラウザ設定画面の開始と終了方法を説明します。

POINT

Internet Explorer 5 をお使いの場合

ブラウザ設定画面が正しく表示されず、正常に操作できないことがあります。
このような場合には、Internet Explorer 6 にアップデートするか、または添付の管理ツール「Dr.WLAPPer」で設定を行ってください。Dr.WLAPPer を使用した設定方法については、「Dr.WLAPPer（ドクターラッパー）の使い方」（→ P.147）をご覧ください。

■開始

POINT

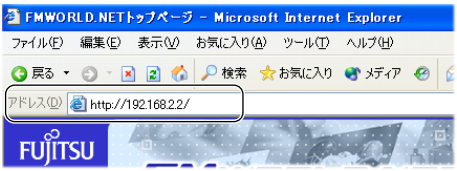
・前回ログイン時に画面上で設定変更を行った後、再起動により本製品への設定の反映を行っていない場合、その設定はログイン時に破棄されます。

1 管理者用パソコンの Web ブラウザを起動します。

2 Web ブラウザのアドレス欄に次のように入力し、【Enter】キーを押します。

http://[本製品の IP アドレス]/

本製品 IP アドレスの初期値は、192.168.2.2 です。初期値の場合は「http://192.168.2.2/」と入力します。



POINT

「管理機能」画面で、「ポート番号」を初期値から変更した場合

本製品のブラウザ設定画面を開始するときに、ポート番号の指定が必要になります。
Web ブラウザのアドレス入力欄に、次のように本製品の IP アドレスとポート番号を半角コロン（:）で区切って指定します。
http://[本製品の IP アドレス]:[ポート番号]/
本製品の IP アドレスが「192.168.2.2」、ポート番号が「88」の場合は、「http://192.168.2.2:88/」と入力します。

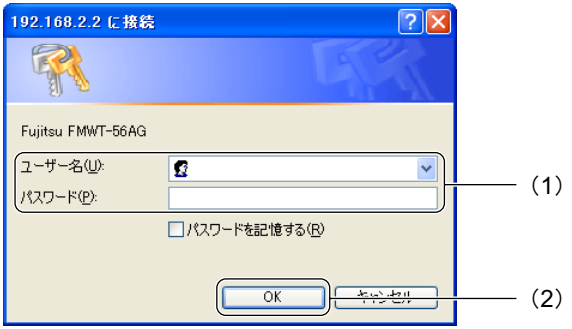
ログインウィンドウが表示されます。

3 **(1) ユーザー名とパスワードを入力し、(2)「OK」をクリックします。**

管理者権限でログインする場合は、本製品の「管理者ユーザー名」、「管理者パスワード」を入力します。初期値はどちらも「admin」です。

一般ユーザー権限でログインする場合は、「一般ユーザー名」、「一般パスワード」を入力します。初期値はどちらも「public」です。

管理者権限と一般ユーザー権限については、「「アカウント設定」カテゴリ」(→ P.122)をご覧ください。



ブラウザ設定画面が表示されます。

画面の構成については、「画面構成」(→ P.62)をご覧ください。

■終了

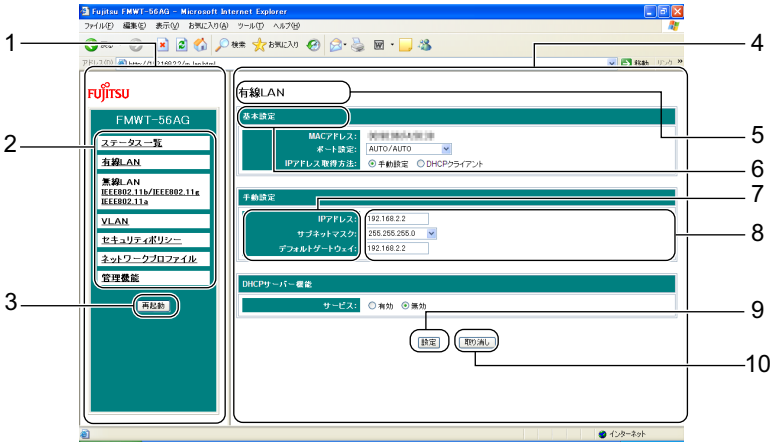
設定終了後は、Web ブラウザの をクリックして、Web ブラウザを閉じます。

2 ブラウザ設定画面

ブラウザ設定画面の画面構成と、基本的な設定手順を説明します。

画面構成

ブラウザ設定画面の画面構成について説明します。



1 メニューフレーム

メニュー用のフレームです。

2 メニュー

メニューをクリックすると、メインフレームに各メニュー画面が表示されます。

3 「再起動」ボタン

クリックすると本製品が再起動されます。また、設定内容を変更した場合は、クリックすると設定内容が本製品に反映されます。

画面上で設定を変更しても、本製品に反映されていない情報があると、ボタンの周りが黄色になります。この状態で Web ブラウザを終了すると、変更した内容は、次回ログイン時に破棄されます。

4 メインフレーム

選択したメニューのメニュー画面が表示されます。

5 画面名

現在開いている画面の画面名です。

6 カテゴリ

各設定項目をまとめたカテゴリ名です。

7 項目

設定項目です。

8 選択肢／詳細項目
各項目に対する選択肢や、詳細設定の項目が表示されます。

9 「設定」ボタン
現在開いているメニュー画面の設定内容を保存します。クリックすると、「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」と表示されます。「OK」をクリックすると、本製品が再起動され、変更した内容が本製品に反映されます。「キャンセル」をクリックすると、画面上には変更した内容が保存されますが、本製品には反映されず、メニューフレームの「再起動」ボタンの周りが黄色になります。

10 「取り消し」ボタン
クリックすると、現在開いているメニュー画面で変更した項目を、変更前の状態に戻します。ただし、「設定」ボタンをクリックして保存された内容は、変更前の状態に戻すことはできません。

ブラウザ設定画面の基本手順

ブラウザ設定画面を使った基本的な設定手順を説明します。

1 管理者権限で、ブラウザ設定画面にログインします。
ログイン方法については、「開始」（→ P.60）をご覧ください。

2 設定する内容によって、メニューを選択します。

3 必要な設定を行います。
各メニュー画面の設定の詳細は、それぞれ次の参照先をご覧ください。
- 「ステータス一覧」メニュー
  「ステータスの確認」（→ P.135）
- 「有線 LAN」メニュー
  「有線 LAN の設定」（→ P.66）
- 「無線 LAN」メニュー
  「無線 LAN インターフェースの設定」（→ P.75）
- 「VLAN」メニュー
  「VLAN の設定」（→ P.93）
- 「セキュリティポリシー」メニュー
  「セキュリティポリシーの設定」（→ P.97）
- 「ネットワークプロファイル」メニュー
  「ネットワークプロファイルの設定」（→ P.115）
- 「管理機能」メニュー
  「管理機能の設定」（→ P.120）
  「システムのメンテナンス」（→ P.139）

4 1 つのメニュー画面での設定が終了したら、メニュー画面内の「設定」ボタンをクリックします。
「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」と表示されます。

5 次のように操作します。

・別メニューの設定を行う場合
「キャンセル」をクリックして、手順 2 から手順 5 までを繰り返します。

POINT

キャンセルをクリックした場合

本製品に反映されていない情報があると、「再起動」ボタンの周りが黄色になります。その状態で再起動ボタンをクリックすると、本製品が再起動され、設定が反映されます。

・別メニューの設定を行わない場合
「OK」をクリックします。
本製品が再起動され、「設定を保存しています。」という画面が表示されます。
「設定を保存しています。」という画面が終了すると再起動が終了し、各メニュー画面で設定した内容が本製品に反映されます。

POINT

・再起動が完了するまでは、画面に表示された時間がかかります。
・再起動が開始されると、管理者用パソコンは本製品から切断されます。
再起動後、自動的に再接続しない場合は、しばらくしてから Web ブラウザを起動し直し、もう一度本製品にログインしてください。

6 ブラウザ設定画面を終了します。

終了方法については、「終了」（→ P.61）をご覧ください。

4

第 4 章

設定の詳細（ネットワークの設定）

ネットワークに関する設定の詳細について説明します。

1 有線 LAN の設定

ネットワークに関する設定を行います。

ネットワークに関する設定を行う場合は、「有線 LAN」メニューをクリックします。メインフレームに「有線 LAN」画面が表示されます。

POINT

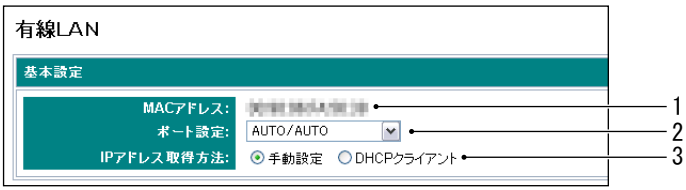
「有線 LAN」画面での設定が終了したら、次のように操作してください

1. 「有線 LAN」画面の「設定」ボタンをクリックします。
   「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」というメッセージが表示されます。
2. 次のように操作します。
   別メニューの設定を行わない場合
   「OK」をクリックします。
   別メニューの設定を行う場合
   「キャンセル」をクリックして、別メニュー画面の設定を行います。

「有線 LAN」画面の項目について、カテゴリごとに説明します。

■「基本設定」カテゴリ

ネットワークに接続するための基本的な設定を行うカテゴリです。各項目について説明します。



1 MAC アドレス

本製品の LAN ポートの MAC アドレスが表示されます。

2 ポート設定 （初期値：AUTO/AUTO）

をクリックして、本製品の LAN ポートの通信速度とデュプレックス（Duplex）を選択します。
通常は「AUTO/AUTO」を選択します。本製品とハブユニットとの通信が正常に行えない場合に、ハブユニットと同じリンクスピードとデュプレックスを選択します。

- AUTO/AUTO
  接続先の機器と通信を行い、本製品がリンクスピードとデュプレックスを自動的に決定します。
- 100Mbps/Full Duplex
  100Mbps の通信速度で、送信、受信それぞれに専用のラインを使用して同時に通信を行います。

・100Mbps/Half Duplex
100Mbps の通信速度で、送信、受信を 1 つのラインで交互に行います。
・10Mbps/Full Duplex
10Mbps の通信速度で、送信、受信それぞれに専用のラインを使用して同時に通信を行います。
・10Mbps/Half Duplex
10Mbps の通信速度で、送信、受信を 1 つのラインで交互に行います。

3 IP アドレス取得方法 （初期値：手動設定）
本製品の IP アドレスの取得方法を選択します。
・手動設定
固定 IP アドレスを指定します。
・DHCP クライアント
DHCP サーバーより IP アドレスを自動取得します。

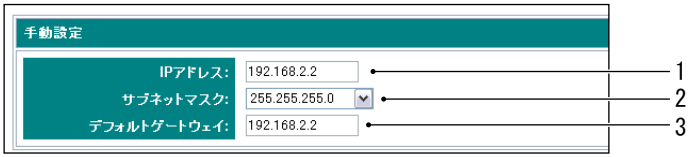
重要

「DHCP クライアント」に設定する場合は次の点にご注意ください
「DHCP クライアント」に設定すると、本製品の IP アドレスが毎回変わる場合があります。IP アドレスがわからないと、本製品の設定画面にログインできなくなります。IP アドレスがわからず、本製品にログインできなくなった場合は、「IP アドレス、ユーザー名、パスワードを忘れてログインできない」（→ P.187）をご覧ください。

「DHCP クライアント」から「手動設定」に変更した場合
IP アドレスは直前に DHCP サーバーから割り当てられていた IP アドレスになります。

■「手動設定」カテゴリ

「基本設定」カテゴリの「IP アドレス取得方法」が「手動設定」の場合に表示されるカテゴリです。本製品のIPアドレスの値などを設定するカテゴリです。各項目について説明します。



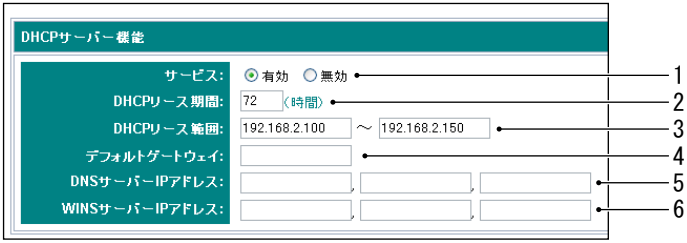
1 IP アドレス （初期値：192.168.2.2）
本製品の IP アドレスを指定します。

2 サブネットマスク （初期値：255.255.255.0）
をクリックしてサブネットマスクを選択します。

3 デフォルトゲートウェイ （初期値：192.168.2.2）
基幹 LAN に接続する場合、ネットワークに合わせたデフォルトゲートウェイを必要に応じて指定します。
何も設定しないと、「IP アドレス」と同じ値が設定されます。

■「DHCP サーバー機能」カテゴリ

「DHCP サーバー機能」カテゴリで設定できる項目について説明します。



1 サービス （初期値：無効）

DHCP サーバー機能を使用するかどうかを選択します。

・有効

DHCP サーバー機能を使用する場合は、「有効」をクリックして◉にし、次の 2 ～ 6 の設定を行います。

・無効

DHCP サーバー機能を使用しない場合は、「無効」をクリックして◉にします。

2 DHCP リース期間 （初期値：72）

DHCP クライアントに割り当てる DHCP アドレスのリース期間を 0 ～ 99999 (時間) の範囲で指定します。ただし、DHCP クライアントが本製品に接続している間は、ここで設定した期限が切れる前に、再度同じ IP アドレスを自動的に割り当てます。

無期限に設定する場合は、「0」を入力します。

3 DHCP リース範囲 （初期値：192.168.2.100 ～ 192.168.2.150）

DHCP クライアントに割り当てる IP アドレスを、開始 IP アドレスから終了 IP アドレスで範囲指定します。

4 デフォルトゲートウェイ （初期値：なし）

必要に応じて指定します。

5 DNS サーバー IP アドレス （初期値：なし）

必要に応じて指定します。3 つまで指定できます。

6 WINS サーバー IP アドレス （初期値：なし）

必要に応じて指定します。3 つまで指定できます。

2 無線 LAN の設定手順について

無線 LAN の設定は、「無線 LAN」、「VLAN」、「セキュリティポリシー」、「ネットワークプロファイル」の各メニューに分かれています。必要に応じて「無線 LAN」、「VLAN」、「セキュリティポリシー」の設定を行い、最終的に各メニューで設定した内容を、「ネットワークプロファイル」メニューで組み合わせます。
次の手順を参考にして設定を行ってください。

■無線 LAN の設定手順

各メニュー画面を、次の手順で設定します。

1 「無線 LAN」メニューの「IEEE802.11b/IEEE802.11g」または「IEEE802.11a」をクリックします。

2 「基本設定」カテゴリの設定を行います。
設定の詳細については、「無線 LAN インターフェースの設定」（→ P.75）をご覧ください。

3 「設定」ボタンをクリックします。

4 「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」というメッセージの画面で「キャンセル」をクリックします。

POINT

「IEEE802.11b/IEEE802.11g」と「IEEE802.11a」の両方の無線 LAN インターフェースを設定する場合
「IEEE802.11b/IEEE802.11g」画面と「IEEE802.11a」画面の両方で手順 2 ～手順 4 を行います。

5 VLAN の設定を行う場合は、「VLAN」メニューをクリックして、VLAN の設定を行います。
設定手順については、「VLAN の設定を行う場合」（→ P.71）をご覧ください。

POINT

認証 VLAN を使用する場合
VLAN の設定を行う前に、手順 8 の RADIUS サーバーの設定を行う必要があります。設定の詳細は、「「RADIUS 機能」カテゴリ」（→ P.107）をご覧ください。

6 「セキュリティポリシー」メニューをクリックして、無線 LAN のセキュリティの設定を行います。
セキュリティの方法によって設定手順が異なります。

・WEP キーを使用する場合は、「セキュリティポリシーの設定手順（WEP の場合）」（→ P.71）をご覧ください。
・IEEE802.1X を使用する場合は、「セキュリティポリシーの設定手順（IEEE802.1X の場合）」（→ P.72）をご覧ください。
・WPA、または IEEE802.11i(WPA2) を使用する場合は、「セキュリティポリシーの設定手順（WPA または IEEE802.11i (WPA2) の場合）」（→ P.72）をご覧ください。
・WPA-PSK、または IEEE802.11i (WPA2)-PSK を使用する場合は、「セキュリティポリシーの設定手順（WPA-PSK または IEEE802.11i (WPA2)-PSK の場合）」（→ P.73）をご覧ください。

7 MAC アドレスフィルタリングの設定を行う場合は、「MAC アドレスフィルタリング」カテゴリの設定を行います。

設定手順については、「MAC アドレスフィルタリングの設定を行う場合」（→ P.73）をご覧ください。

8 RADIUS サーバーの設定を行う場合は、「RADIUS 機能」カテゴリの設定を行います。

セキュリティの方法が IEEE802.1X、WPA、または IEEE802.11i (WPA2) の場合は、必ず設定を行ってください。
セキュリティの方法が WEP キー、WPA-PSK、または IEEE802.11i (WPA2)-PSK の場合は、RADIUS アカウンティングの設定を行う場合のみ設定を行ってください。
設定の詳細については、「「RADIUS 機能」カテゴリ」（→ P.107）をご覧ください。

9 「ネットワークプロファイル」メニューをクリックして、プロファイルの設定を行います。

「ネットワークプロファイル」メニューの設定の詳細については、「ネットワークプロファイルの設定」（→ P.115）をご覧ください。

10 「設定」ボタンをクリックします。

11 「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」という画面が表示されます。

12 次のように操作します。

・別メニューの設定を行わない場合
「OK」をクリックします。
・別メニューの設定を行う場合
「キャンセル」をクリックして、別メニュー画面の設定を行います。

■VLAN の設定を行う場合

「VLAN」画面で次のように設定します。
「VLAN」メニューの設定の詳細については、「VLAN の設定」（→ P.93）をご覧ください。

1 **「VLAN　機能」の「通常　VLAN」または「認証　VLAN」をクリックして◉にします。**

2 **VLAN 機能の設定により、次のように操作します。**

■ 通常 VLAN の場合

1. 「VLAN 名」、「VLAN ID」、「サービスクラス」を指定して、VLAN グループを作成します。
2. 「設定」ボタンをクリックします。
3. 「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」というメッセージの画面で「キャンセル」をクリックします。
4. 「管理 VLAN」を設定します。

■ 認証 VLAN の場合

1. 「管理 VLAN」の VLAN ID とサービスクラスを設定します。

3 **「設定」ボタンをクリックします。**

4 **「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」というメッセージの画面で「キャンセル」をクリックします。**

「無線 LAN の設定手順」（→ P.69）の手順 6（→ P.69）に戻ります。

■セキュリティポリシーの設定手順（WEP の場合）

「セキュリティポリシー」画面で次のように設定します。

1 **「ポリシー」カテゴリの設定を行います。**

設定の詳細については、「「ポリシー」カテゴリ」（→ P.99）をご覧ください。

2 **「セキュリティ」カテゴリの「モード」で、「ベーシック」をクリックして◉にします。**

3 **「802.1X 機能」カテゴリの「802.1X」で、「未使用」をクリックして◉にします。**

4 **「WEP キー」カテゴリで WEP キーの詳細を設定します。**

「WEP キー」カテゴリの設定の詳細については、「「WEP キー」カテゴリ」（→ P.102）をご覧ください。

5 **「設定」ボタンをクリックします。**

6 **「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」というメッセージの画面で「キャンセル」をクリックします。**

「無線 LAN の設定手順」（→ P.69）の手順 7（→ P.70）に戻ります。

■セキュリティポリシーの設定手順（IEEE802.1X の場合）

「セキュリティポリシー」画面で次のように設定します。

1 **「ポリシー」カテゴリの設定を行います。**
設定の詳細については、「「ポリシー」カテゴリ」（→ P.99）をご覧ください。

2 **「セキュリティ」カテゴリの「モード」で、「ベーシック」をクリックして◉にします。**

3 **「802.1X 機能」カテゴリの「802.1X」で、「使用」をクリックして◉にします。**
設定の詳細については、「「802.1X 機能」カテゴリ」（→ P.101）をご覧ください。

4 **認証プロトコルによって設定する項目が異なります。**

■ EAP-TLS、EAP-TTLS、PEAP の場合

1. 「802.1X」カテゴリの「キーの配信」で、「有効」をクリックして◉にします。
2. 「802.1X」カテゴリのその他の設定を行います。

■ EAP-MD5 の場合

1. 「802.1X」カテゴリの「キーの配信」で、「無効」をクリックして◉にします。
2. 「WEP キー」カテゴリの設定を行います。
   設定の詳細については、「「WEP キー」カテゴリ」（→ P.102）をご覧ください。

5 **「設定」ボタンをクリックします。**

6 **「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」というメッセージの画面で「キャンセル」をクリックします。**

「無線 LAN の設定手順」（→ P.69）の手順 7（→ P.70）に戻ります。

■セキュリティポリシーの設定手順（WPA または IEEE802.11i (WPA2) の場合）

「セキュリティポリシー」画面で次のように設定します。

1 **「ポリシー」カテゴリの設定を行います。**
設定の詳細については、「「ポリシー」カテゴリ」（→ P.99）をご覧ください。

2 **「セキュリティ」カテゴリの「モード」で、「アドバンスド」をクリックして◉にします。**

3 **「WPA/802.11i (WPA2)」カテゴリの設定を行います。**

1. 「認証モード」を設定します。

   WPA のみ使用する場合、▼をクリックして「WPA」を選択します。

   IEEE802.11i (WPA2) のみ使用する場合、▼をクリックして「802.11i (WPA2)」を選択します。

   WPA と IEEE802.11i (WPA2) の両方を使用する場合、▼をクリックして「WPA/802.11i (WPA2)」を選択します。

2.「WPA/802.11i (WPA2)」カテゴリのその他の設定を行います。
設定の詳細については、「「WPA/802.11i (WPA2)」カテゴリ」(→P.104)をご覧ください。

4 「設定」ボタンをクリックします。

5 「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」というメッセージの画面で「キャンセル」をクリックします。

「無線 LAN の設定手順」（→ P.69）の手順 7（→ P.70）に戻ります。

■セキュリティポリシーの設定手順（WPA-PSK または IEEE802.11i (WPA2)-PSK の場合）

「セキュリティポリシー」画面で次のように設定します。

1 「ポリシー」カテゴリの設定を行います。
設定の詳細については、「「ポリシー」カテゴリ」（→ P.99）をご覧ください。

2 「セキュリティ」カテゴリの「モード」で、「アドバンスド」をクリックして◉にします。

3 「WPA/802.11i (WPA2)」カテゴリの設定を行います。

1.「認証モード」を設定します。

WPA-PSK のみ使用する場合、をクリックして「WPA-PSK」を選択します。

IEEE802.11i (WPA2)-PSK のみ使用する場合、をクリックして「802.11i (WPA2)-PSK」を選択します。

WPA-PSK と IEEE802.11i (WPA2)-PSK の両方を使用する場合、をクリックして「WPA-PSK/802.11i (WPA2)-PSK」を選択します。

2.「WPA/802.11i (WPA2)」カテゴリのその他の設定を行います。
設定の詳細については、「「WPA/802.11i (WPA2)」カテゴリ」(→P.104)をご覧ください。

4 「設定」ボタンをクリックします。

5 「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」というメッセージの画面で「キャンセル」をクリックします。

「無線 LAN の設定手順」（→ P.69）の手順 7（→ P.70）に戻ります。

■MAC アドレスフィルタリングの設定を行う場合

1 「セキュリティポリシー」画面で「MAC アドレスフィルタリングの設定」ボタンをクリックします。
「MAC アドレスフィルタリングの設定」画面が表示されます。

2 対象となる無線 LAN 端末を登録します。
設定の詳細については、「「MAC アドレスフィルタリングの設定」画面」（→ P.108）をご覧ください。

3 **無線 LAN 端末の登録が終了したら、「戻る」ボタンをクリックします。**
「セキュリティポリシー」画面に戻ります。

4 **「アドレス制御」の設定を行います。**
設定の詳細については、「「MAC アドレスフィルタリング」カテゴリ」（→ P.106）をご覧ください。

5 **「設定」ボタンをクリックします。**

6 **「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」というメッセージの画面で「キャンセル」をクリックします。**

「無線 LAN の設定手順」（→ P.69）の手順 8（→ P.70）に戻ります。

3 無線 LAN インターフェースの設定

「無線 LAN」メニューでは、無線 LAN 通信を行うための基本的な設定を行います。

本製品は、次の無線 LAN 規格をサポートしています。

・IEEE802.11a

5GHz の周波数帯を使用します。通信速度は規格値 54Mbps［注 1］です。また無線 LAN 高速化技術 Super A に対応し、より高速な通信を可能にしています。

・IEEE802.11b

2.4GHz の周波数帯を使用します。通信速度は規格値 11Mbps［注 1］です。

・IEEE802.11g

IEEE802.11b と同じ周波数帯（2.4GHz）を使用しますが、通信速度が規格値 54Mbps［注 1］に高速化されています。また無線 LAN 高速化技術 Super G に対応し、より高速な通信を可能にしています。

［注 1］ 表示の数値は、無線 LAN 規格の理論上の最大値であり、実際のデータ転送速度を示すものではありません。

「IEEE802.11b/IEEE802.11g」画面

IEEE802.11b/IEEE802.11g インターフェースに関する設定を行う場合は、「無線 LAN」メニューの「IEEE802.11b/IEEE802.11g」をクリックします。メインフレームに「IEEE802.11b/IEEE802.11g」画面が表示されます。

POINT

「IEEE802.11b/IEEE802.11g」画面での設定が終了したら、次のように操作してください

1. 「IEEE802.11b/IEEE802.11g」画面の「設定」ボタンをクリックします。
   「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」というメッセージが表示されます。
2. 次のように操作します。
   別メニューの設定を行わない場合
   「OK」をクリックします。
   別メニューの設定を行う場合
   「キャンセル」をクリックして、別メニュー画面の設定を行います。

■設定に関するご注意

□ WDS 機能を利用する場合の注意事項

WDS 機能を使用する場合、親アクセスポイントと子アクセスポイントの設定について以下の点に注意してください。

WDS 機能の概要については、「WDS（アクセスポイント間通信）」（→ P.31）をご覧ください。

・WDS リンクを行う親アクセスポイントの設定について
- 「WDS」を無効にしてください。
- Super G 機能は使用できません。「Super G」を無効にしてください。
- VLAN 機能は使用できません。VLAN 機能を無効にしてください。
- セキュリティポリシーを WEP キーで設定してください。WEP キーで設定する手順については、「セキュリティポリシーの設定手順（WEP の場合）」（→ P.71）をご覧ください。IEEE802.1X、WPA、WPA-PSK、IEEE802.11i (WPA2)、IEEE802.11i (WPA2)-PSK は使用できません。

・WDS リンクを行う子アクセスポイントの設定について
- 「WDS」を有効にしてください。
- 「モード」を親アクセスポイントと同じ設定にしてください。
  例えば、親アクセスポイントのモードの設定が「11b & 11g」の場合は、「11b & 11g」に設定してください。
- 「チャンネル」を設定する必要はありません。
  チャンネルの設定は無視され、自動的に親アクセスポイントのチャンネルとなります。
- 「Super G」を無効にしてください。
- IEEE802.11a インターフェースの「無線スイッチ」を「オフ」に設定してください。
- VLAN 機能を無効にしてください。
- セキュリティポリシーを親アクセスポイントと同じ設定にしてください。
- 「SSID」を親アクセスポイントと同じ設定にしてください。
  なお、親アクセスポイントと同じ SSID が設定されている別の無線 LAN アクセスポイントが電波の届く範囲にあると、その無線 LAN アクセスポイントと接続してしまう可能性がありますので、十分注意してください。

WDS 機能を利用する場合は、運用時に次のことをご注意ください。

・子アクセスポイントは、IEEE802.11b/IEEE802.11g インターフェースのみ通信が可能です。親アクセスポイントは、IEEE802.11b/IEEE802.11g および IEEE802.11a の両方のインターフェースで通信が可能です。

・親アクセスポイントの再起動や、電波状況などの影響により WDS リンクが切断された場合、子アクセスポイントは自動的に再起動します。この場合、子アクセスポイントに接続している無線 LAN 端末の接続は切断されます。

・WDS を有効にした後、WDS リンクが確立されるまで、無線 LAN 端末は子アクセスポイントに 接続できません。端末が長時間接続できない場合は、親と子それぞれのアクセスポイントの WDS に関する設定が正しいかどうか確認してください。

・子アクセスポイントが複数ある場合は、子アクセスポイントどうしが接続しないように、MAC アドレスフィルタリングの設定を行ってください。

・WDS リンクが確立されると、「ステータス一覧」画面の「接続中の無線 LAN 端末」に、親アクセスポイントには子アクセスポイントの、子アクセスポイントには親アクセスポイントの MAC アドレスが登録されます。詳しくは「ステータスの確認」（→ P.135）の「「無線 LAN ネットワーク情報」カテゴリ」（→ P.137）をご覧ください。

■ 無線 LAN 端末の仕様確認

次の設定項目については、本製品に接続する無線 LAN 端末の仕様を考慮して設定する必要があります。事前に、無線 LAN 端末の仕様をご確認ください。

無線 LAN 端末の仕様については、次のマニュアルをご覧になるか、お使いの機器のメーカーにお問い合わせください。

・無線 LAN 機能が標準搭載されているパソコンの場合は、パソコンに添付のマニュアルをご覧ください。
・無線 LAN カードを増設した場合は、無線 LAN カードのマニュアルをご覧ください。

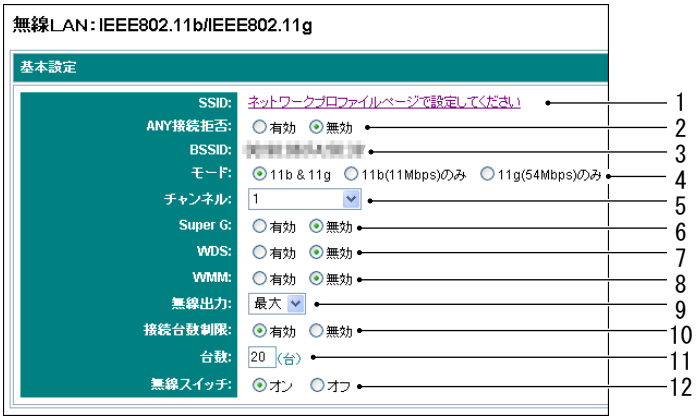
表：IEEE802.11b/IEEE802.11g の設定を行う前に確認しておくこと

設定項目名	選択肢		注意事項
モード	・11b & 11g ・11b（11Mbps）のみ ・11g（54Mbps）のみ		無線LANのインターフェースを設定します。 「11b & 11g」を選択した場合、無線 LAN 端末が IEEE802.11b、または IEEE802.11g に対応している必要があります。 「11b（11Mbps）のみ」を選択した場合、無線LAN端末がIEEE802.11bに対応している必要があります。 「11g（54Mbps）のみ」を選択した場合、無線LAN端末がIEEE802.11gに対応している必要があります。
チャンネル	「モード」が「11b & 11g」または「11g（54Mbps）のみ」の場合	・1 ～ 13 の範囲で固定値を設定 ・Auto（1 ～ 11ch） ・Auto（1 ～ 13ch）	無線LANの通信に使用するチャンネルを設定します。 無線LAN端末が対応しているチャンネルの範囲が、1 ～ 11 チャンネルの場合があります。
	「モード」が「11b（11Mbps）のみ」の場合	・1 ～ 14 の範囲で固定値を設定 ・Auto（1 ～ 11ch） ・Auto（1 ～ 14ch）	
Super G	・有効 ・無効		IEEE802.11g の無線 LAN 通信で、Super G 機能を使用するかどうかを選択します。Super G 機能を使用する場合は、無線LAN端末がSuper Gに対応している必要があります。Super G に対応していない無線 LAN 端末は、通信速度が低下する場合があります。
WMM	・有効 ・無効		IEEE802.11b/IEEE802.11g の無線 LAN 通信で、WMM 機能を使用するかどうかを選択します。WMM 機能を使用する場合は、無線 LAN 端末が WMM に対応している必要があります。WMM に対応していない無線 LAN 端末は、通信速度が低下する場合があります。

「IEEE802.11b/IEEE802.11g」画面の項目について、カテゴリごとに説明します。

■「基本設定」カテゴリ

IEEE802.11b/IEEE802.11g の無線 LAN 通信に関する設定を行うカテゴリです。各項目について説明します。



1 SSID

SSID と無線 LAN インターフェースとの組み合わせは、「ネットワークプロファイル」メニューで設定します。このメニュー画面では SSID は設定しません。

2 ANY 接続拒否 （初期値：無効）

ANY 接続拒否機能を有効にするかどうか設定します。

・有効

SSID を設定していない無線 LAN 端末から本製品への接続を不可能にする場合は、「有効」をクリックして◉にします。

・無効

SSID を設定していない無線 LAN 端末から本製品への接続を可能にする場合は、「無効」をクリックして◉にします。

POINT

ANY 接続拒否を「有効」にした場合

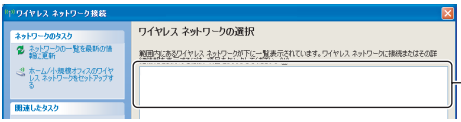
SSID の隠蔽も有効になり、Windows XP の機能などを利用しても本製品の SSID を取得できなくなります。

例えば、Windows XP SP2 の端末で、「ワイヤレスネットワーク接続」ウィンドウの「ワイヤレスネットワークの選択」に本製品の SSID が表示されなくなります。

【ANY接続拒否が「無効」の場合】

本製品のSSIDが表示されます。

【ANY接続拒否が「有効」の場合】



本製品のSSIDが表示されません。

3 BSSID

通常は、本製品の無線 LAN ポート（IEEE802.11b/IEEE802.11g）の MAC アドレスが表示されます。

「無線スイッチ」を「オフ」に設定している場合は、「11b/11g 停止中」と表示されます。リンクインテグリティ機能により無線電波を停止している場合は、「経路異常発生中」と表示されます。

4 モード （初期値：11b & 11g）

本製品の動作モードを選択します。

・11b & 11g
IEEE802.11b と IEEE802.11g モードの無線 LAN 端末からの接続を可能にする場合は、「11b & 11g」をクリックして◉にします。

・11b（11Mbps）のみ
IEEE802.11b モードの無線 LAN 端末のみからの接続を可能にする場合は、「11b（11Mbps）のみ」をクリックして◉にします。

・11g（54Mbps）のみ
IEEE802.11g モードの無線 LAN 端末のみからの接続を可能にする場合は、「11g（54Mbps）のみ」をクリックして◉にします。

5 チャンネル （初期値：1）

▾をクリックして、無線 LAN 通信を行う際に使用する周波数帯（1 ～ 14 チャンネル）を選択します。

POINT

同一フロア内など、近くで他の無線 LAN(IEEE802.11b/IEEE802.11g 準拠) を運用している場合

電波の干渉を防ぐため、チャンネルの値を 5 つ以上離してください。例えば、チャンネル 1、6、11 のように設定してください。また、「モード」が「11b（11Mbps）のみ」の場合、14 チャンネルは 11 チャンネルと値が 5 つ離れていませんが、使用周波数が少し離れているため、11 チャンネルのネットワークとの共存が可能です。

・「モード」が「11b & 11g」または「11g（54Mbps）のみ」の場合
1 ～ 13 チャンネルの範囲で指定します。
「Auto（1 ～ 11ch)」または「Auto（1 ～ 13ch)」を選択すると、() 内の範囲で通信状態が良好なチャンネルを本製品が自動的に検索して設定します。
・「モード」が「11b（11Mbps）のみ」の場合
1 ～ 14 チャンネルの範囲で指定します。
「Auto（1 ～ 11ch)」または「Auto（1 ～ 14ch)」を選択すると、() 内の範囲で通信状態が良好なチャンネルを本製品が自動的に検索して設定します。

6 Super G （初期値：無効）

「モード」が「11b & 11g」または「11g（54Mbps）のみ」の場合、Super G 機能を使用するかどうかを選択します。

・有効
Super G 機能を使用する場合は、「有効」をクリックして◉にします。
・無効
Super G 機能を使用しない場合は、「無効」をクリックして◉にします。

7 WDS （初期値：無効）

WDS 機能を使用するかどうかを選択します。

・有効
WDS 機能を使用する場合は、「有効」をクリックして◉にします。
・無効
WDS 機能を使用しない場合は、「無効」をクリックして◉にします。

8 WMM （初期値：無効）

WMM 機能を使用するかどうかを選択します。
WMM 機能の概要については、「WMM」（→ P.30）をご覧ください。

・有効
WMM 機能を使用する場合は、「有効」をクリックして◉にします。
・無効
WMM 機能を使用しない場合は、「無効」をクリックして◉にします。

9 無線出力 （初期値：最大）

▼をクリックして「最大」、「大」、「中」、「小」、「最小」のいずれかを選択します。それぞれの出力値は次のとおりです。

・最大 ：18dBm
・大 ：16.5dBm
・中 ：13.5dBm
・小 ：10.5dBm
・最小 ：0dBm

10 接続台数制限 （初期値：無効）

本製品に IEEE802.11b/IEEE802.11g で接続する端末数を制限するかどうかを選択します。

接続台数制限機能の概要については、「簡易ロードバランス（接続台数制限）」（→ P.37）をご覧ください。

・有効

本製品に IEEE802.11b/IEEE802.11g で接続する端末数を制限する場合は、「有効」をクリックして◉にし、「台数」を設定します。

・無効

本製品に IEEE802.11b/IEEE802.11g で接続する端末数を制限しない場合は、「無効」をクリックして◉にします。

11 台数 （初期値：20 台）

「接続台数制限」が有効のとき、本製品に IEEE802.11b/IEEE802.11g で接続できる端末の最大数を 1 ～ 30（台）の範囲で指定します。

POINT

・「IEEE802.11a」画面の「接続台数制限」が有効のとき、「IEEE802.11a」画面の接続台数制限の台数と、「IEEE802.11b/IEEE802.11g」画面の接続台数制限の台数の合計が 40 台を超えないように設定してください。

・本製品が WDS の親アクセスポイントに設定されている場合、子アクセスポイントも台数に含まれます。

12 無線スイッチ （初期値：オン）

IEEE802.11b/IEEE802.11g の無線電波の発信／停止を選択します。

・オン

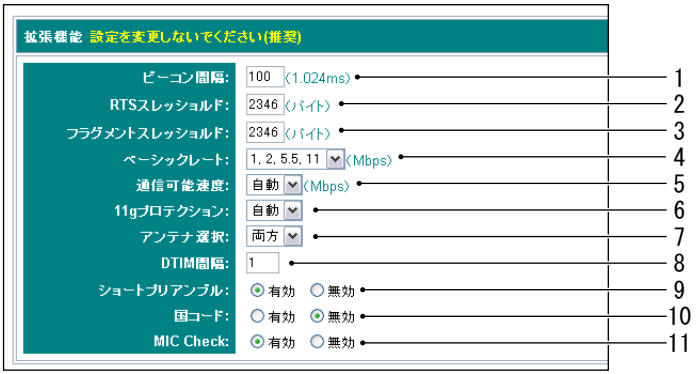
IEEE802.11b/IEEE802.11g で通信を行う場合は、「オン」をクリックして◉にします。「オン」にすると、IEEE802.11b/IEEE802.11g の電波が発信されます。

・オフ

IEEE802.11b/IEEE802.11g の通信を停止する場合は、「オフ」をクリックして◉にします。「オフ」にすると、IEEE802.11b/IEEE802.11g の電波が停止されます。

■「拡張機能」カテゴリ

拡張機能の各設定項目の値は、通常は変更しないでください。無線 LAN 端末が正常に通信できない場合のみ、必要に応じて設定を変更してください。
各項目について説明します。



1 ビーコン間隔 （初期値：100）

ビーコンの送出間隔を 20 ～ 1000（1.024ms）の範囲で指定します。

2 RTS スレッショルド （初期値：2346）

RTS パケットを送信するデータサイズのしきい値を 1 ～ 2346（バイト）の範囲で指定します。データフレーム長がこのサイズを超える場合、RTS/CTS を使用します。

3 フラグメントスレッショルド （初期値：2346）

パケットを断片化するデータサイズを256～2346(バイト)の範囲の偶数で指定します。

4 ベーシックレート （初期値：1, 2, 5.5, 11）

をクリックしてベーシックレート（Mbps）を選択します。

初期値、および選択肢については「動作モードによるベーシックレート／通信可能速度の設定値について」（→ P.84）をご覧ください。

5 通信可能速度 （初期値：自動）

をクリックして通信可能速度（Mbps）を選択します。

初期値、および選択肢については「動作モードによるベーシックレート／通信可能速度の設定値について」（→ P.84）をご覧ください。

6 11g プロテクション （初期値：自動）

をクリックして 11g プロテクションを選択します。

・自動
11g プロテクションの有効、無効を自動的に切り替えます。IEEE802.11b 無線 LAN 端末が存在する環境で、11g プロテクションが有効になります。

・オフ
11g プロテクション機能を使用しません。「基本設定」カテゴリの「モード」が「11b(11Mbps) のみ」の場合は、「オフ」の設定のみとなります。

7 アンテナ選択 （初期値：両方）

をクリックして「両方」、「1」、「2」のいずれかを選択します。

・両方
外部アンテナまたは延長アンテナと、内蔵アンテナを使用する場合は、「両方」を選択します。

・1
外部アンテナまたは延長アンテナを使用し、内蔵アンテナを使用しない場合は、「1」を選択します。

・2
内蔵アンテナを使用し、外部アンテナまたは延長アンテナは使用しない場合は、「2」を選択します。

8 DTIM 間隔 （初期値：1）

ビーコンに DTIM を付加する間隔を 1 ～ 255 の範囲で指定します。

9 ショートプリアンブル （初期値：有効）

ショートプリアンブルを「有効」、「無効」から選択します。「無効」に設定した場合、ショートプリアンブルの無線 LAN 端末から本製品への接続が不可能になります。

10 国コード （初期値：無効）

ビーコンに国コードを付加するかどうかを設定します。「有効」に設定した場合、日本の国コードを付加したビーコンを送出します。

11 MIC Check （初期値：有効）

WPA、または IEEE802.11i (WPA2) の暗号化方式に TKIP を使用して通信するとき、メッセージの改ざんを防止するために MIC エラーを検出するかどうかを選択します。

・有効
MIC エラーを検出する場合は、「有効」をクリックしてにします。

・無効
MIC エラーを検出しない場合は、「無効」をクリックしてにします。

□ 動作モードによるベーシックレート／通信可能速度の設定値について

「ベーシックレート」および「通信可能速度」の選択肢と初期値は、「基本設定」カテゴリの「モード」の設定によって次の表のようになります。

表：モードによるベーシックレート／通信可能速度の設定値

「基本設定」カテゴリー「モード」の設定	「拡張機能」カテゴリー「ベーシックレート」の選択肢と初期値	「拡張機能」カテゴリー「通信可能速度」の選択肢と初期値
11b & 11g	・1, 2, 5.5, 11 Mbps（初期値） ・1, 2 Mbps	・自動（初期値） ・1 Mbps ・2 Mbps ・5.5 Mbps ・6 Mbps ・9 Mbps ・11 Mbps ・12 Mbps ・18 Mbps ・24 Mbps ・36 Mbps ・48 Mbps ・54Mbps
11g（54Mbps）のみ	・1, 2, 5.5, 6, 11, 12, 24 Mbps（初期値） ・6, 12, 24 Mbps	
11b（11Mbps）のみ	・1, 2, 5.5, 11 Mbps（初期値） ・1, 2 Mbps	・自動（初期値） ・1 Mbps ・2 Mbps ・5.5 Mbps ・11 Mbps

「IEEE802.11a」画面

IEEE802.11a インターフェースに関する設定を行う場合は、「無線 LAN」メニューの「IEEE802.11a」をクリックします。メインフレームに「IEEE802.11a」画面が表示されます。

POINT

「IEEE802.11a」画面での設定が終了したら、次のように操作してください

1. 「IEEE802.11a」画面の「設定」ボタンをクリックします。
   「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」というメッセージが表示されます。
2. 次のように操作します。
   別メニューの設定を行わない場合
   「OK」をクリックします。
   別メニューの設定を行う場合
   「キャンセル」をクリックして、別メニュー画面の設定を行います。

■設定に関するご注意

□ WDS 機能を利用する場合の注意事項

WDS 機能を使用する場合、親アクセスポイントと子アクセスポイントの設定について以下の点に注意してください。

WDS 機能の概要については、「WDS（アクセスポイント間通信）」（→ P.31）をご覧ください。

・WDS リンクを行う親アクセスポイントの設定について
  - 「WDS」を無効にしてください。
  - Super A 機能は使用できません。「Super A」を無効にしてください。
  - VLAN 機能は使用できません。VLAN 機能を無効にしてください。
  - セキュリティポリシーを WEP キーで設定してください。WEP キーで設定する手順については、「セキュリティポリシーの設定手順（WEP の場合）」（→ P.71）をご覧ください。
    IEEE802.1X、WPA、WPA-PSK、802.11i (WPA2)、802.11i (WPA2)-PSK は使用できません。

・WDS リンクを行う子アクセスポイントの設定について
  - 「WDS」を有効にしてください。
  - 「チャンネル」を設定する必要はありません。
    チャンネルの設定は無視され、自動的に親アクセスポイントのチャンネルとなります。
  - 「Super A」を無効にしてください。
  - IEEE802.11b/IEEE802.11g インターフェースの「無線スイッチ」を「オフ」に設定してください。
  - VLAN 機能を無効にしてください。
  - セキュリティポリシーを親アクセスポイントと同じ設定にしてください。
  - 「SSID」を親アクセスポイントと同じ設定にしてください。
    なお、親アクセスポイントと同じ SSID が設定されている別の無線 LAN アクセスポイントが電波の届く範囲にあると、その無線 LAN アクセスポイントと接続してしまう可能性がありますので、十分注意してください。

WDS 機能を利用する場合は、運用時に次のことをご注意ください。

・子アクセスポイントは、IEEE802.11a インターフェースのみ通信が可能です。親アクセスポイントは、IEEE802.11b/IEEE802.11g および IEEE802.11a の両方のインターフェースで通信が可能です。

・親アクセスポイントの再起動や、電波状況などの影響により WDS リンクが切断された場合、子アクセスポイントは自動的に再起動します。この場合、子アクセスポイントに接続している無線 LAN 端末の接続は切断されます。

・WDS を有効にした後、WDS リンクが確立されるまで、無線 LAN 端末は子アクセスポイントに 接続できません。端末が長時間接続できない場合は、親と子それぞれのアクセスポイントの WDS に関する設定が正しいかどうか確認してください。

・WDS 機能を使用する際、親アクセスポイントと子アクセスポイントは同じチャンネルを利用するため、親アクセスポイントと子アクセスポイントで IEEE802.11a の使用できるチャンネルが異なると正常に動作しません。
  例えば親アクセスポイントに本製品（IEEE802.11a（W52/W53）対応）を使用して、子アクセスポイントにワイヤレス LAN ステーション FMWT-54AG（IEEE802.11a（J52）対応）を使用することはできません。

・子アクセスポイントが複数ある場合は、子アクセスポイントどうしが接続しないように、MAC アドレスフィルタリングの設定を行ってください。

・WDS リンクが確立されると、「ステータス一覧」画面の「接続中の無線 LAN 端末」に、親アクセスポイントには子アクセスポイントの、子アクセスポイントには親アクセスポイントの MAC アドレスが登録されます。詳しくは「ステータスの確認」（→ P.135）の「「無線 LAN ネットワーク情報」カテゴリ」（→ P.137）をご覧ください。

■無線 LAN 端末の仕様確認

次の設定項目については、本製品に接続する無線 LAN 端末の仕様を考慮して設定する必要があります。事前に、無線 LAN 端末の仕様をご確認ください。

無線 LAN 端末の仕様については、次のマニュアルをご覧になるか、お使いの機器のメーカーにお問い合わせください。

・無線 LAN 機能が標準搭載されているパソコンの場合は、パソコンに添付のマニュアルをご覧ください。

・無線 LAN カードを増設した場合は、無線 LAN カードのマニュアルをご覧ください。

表：IEEE802.11a の設定を行う前に確認しておくこと

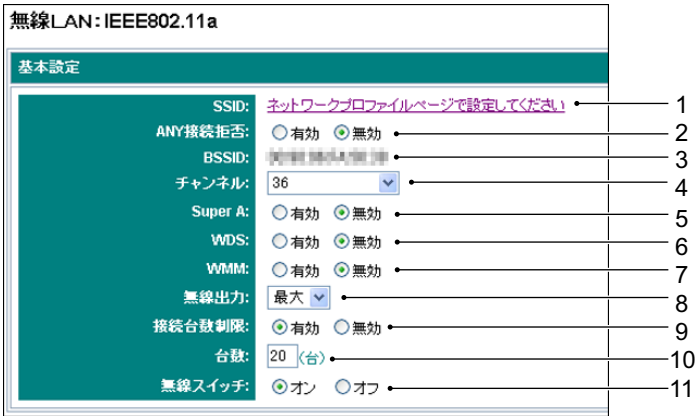
設定項目名	選択肢	注意事項
Super A	・有効 ・無効	IEEE802.11a の無線 LAN 通信で、Super A 機能を使用するかどうかを選択します。Super A 機能を使用する場合は、無線 LAN 端末が Super A に対応している必要があります。Super A に対応していない一部の無線 LAN 端末では、通信速度が低下する場合があります。
WMM	・有効 ・無効	IEEE802.11a の無線 LAN 通信で、WMM 機能を使用するかどうかを選択します。WMM 機能を使用する場合は、無線 LAN 端末が WMM に対応している必要があります。WMM に対応していない無線 LAN 端末は、通信速度が低下する場合があります。
チャンネル	・36、40、44、48、52、56、60、64、Auto［注 1］	IEEE802.11a で本製品に接続する無線 LAN 端末が、本製品の使用できるチャンネルに対応していない場合は、IEEE802.11a での通信はできません。

［注 1］ Auto の場合は、本製品が対応しているチャンネルの中で通信状態が良好なチャンネルを使用します。

「IEEE802.11a」画面の項目について、カテゴリごとに説明します。

■「基本設定」カテゴリ

IEEE802.11aの無線LAN通信に関する設定を行うカテゴリです。各項目について説明します。



1 SSID

SSID と無線 LAN インターフェースとの組み合わせは、「ネットワークプロファイル」メニューで設定します。このメニュー画面では SSID は設定しません。

2 ANY 接続拒否 （初期値：無効）

ANY 接続拒否機能を使用するかどうかを選択します。

・ 有効

SSID を設定していない無線 LAN 端末から本製品への接続を不可能にする場合は、「有効」をクリックして◉にします。

・ 無効

SSID を設定していない無線 LAN 端末から本製品への接続を可能にする場合は、「無効」をクリックして◉にします。

POINT

ANY 接続拒否を「有効」にした場合

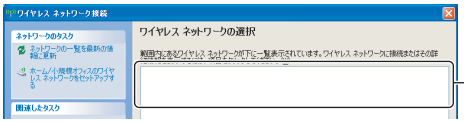
SSID の隠蔽も有効になり、Windows XP の機能などを利用しても本製品の SSID を取得できなくなります。

例えば、Windows XP SP2 の端末で、「ワイヤレスネットワーク接続」ウィンドウの「ワイヤレスネットワークの選択」に本製品の SSID が表示されなくなります。

【ANY接続拒否が「無効」の場合】

本製品のSSIDが表示されます。

【ANY接続拒否が「有効」の場合】



本製品のSSIDが表示されません。

3 BSSID

通常は、本製品の無線 LAN ポート（IEEE802.11a）の MAC アドレスが表示されます。「無線スイッチ」を「オフ」に設定している場合は、「11a 停止中」と表示されます。リンクインテグリティ機能により無線電波を停止している場合は、「経路異常発生中」と表示されます。

4 チャンネル （初期値：36）

をクリックして、無線 LAN 通信を行う際に使用する周波数帯を選択します。

36、40、44、48、52、56、60、64、Auto のいずれかを選択します。

Auto を選択すると、上記チャンネルの中で通信状態が良好なチャンネルを本製品が自動的に検索して設定します。

POINT

- 同一フロア内など、近くで他の無線 LAN（IEEE802.11a 準拠）を運用している場合、電波の干渉を防ぐため、異なるチャンネルの値を設定してください。
- 同一フロア内など、近くで J52 と W52 の無線 LAN（IEEE802.11a 準拠）を運用している場合、電波の干渉を防ぐため、チャンネルの値を 6 つ以上離してください。例えば、チャンネル 34（J52）、40（W52）、46（J52）のように設定してください。

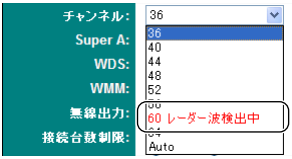
重要

本製品の DFS 機能について

・W53 がサポートする周波数帯（52 ～ 64ch）では、航空管制レーダーや気象レーダーなどで使用されるレーダー波を検出した場合、本製品はただちに再起動し、IEEE802.11a インターフェースのチャンネルを 36 チャンネルに変更します。このとき、IEEE802.11b/g インターフェースも含め本製品に接続していたすべての無線 LAN 端末は切断されますが、再起動後、引き続き通信が可能になります。レーダー波を検出したチャンネルは再起動 30 分後に設定が可能となりますので、再起動前のチャンネルを使用する場合は、再度チャンネルの設定を行ってください。

・52、56、60、64、Auto に設定した場合、本製品の起動後、電波の送出を開始する前に DFS によるレーダー波の検出を 1 分間行います。レーダー波の検出中は IEEE802.11a と IEEE802.11b/g の両方のインターフェースでの通信はできません。

・52、56、60、64 チャンネルのいずれかでレーダー波を検出した場合、「レーダー波検出中」と表示されます。



この場合、30 分間はそのチャンネルを使用できなくなりますので、「レーダー波検出中」と表示されているチャンネルは設定しないでください。
なお、30 分経過後にレーダー波が検出されず、「IEEE802.11a」画面を再読み込みした場合は、「レーダー波検出中」と表示されなくなり、そのチャンネルを使用できるようになります。

5 Super A （初期値：無効）

Super A 機能を使用するかどうかを選択します。

・有効

Super A 機能を使用する場合は、「有効」をクリックして◉にします。

・無効

Super A 機能を使用しない場合は、「無効」をクリックして◉にします。

6 WDS （初期値：無効）

WDS 機能を使用するかどうかを選択します。

・有効

WDS 機能を使用する場合は、「有効」をクリックして◉にします。

・無効

WDS 機能を使用しない場合は、「無効」をクリックして◉にします。

7 WMM （初期値：無効）

WMM 機能を使用するかどうかを選択します。

WMM 機能の概要については、「WMM」（→ P.30）をご覧ください。

・有効

WMM 機能を使用する場合は、「有効」をクリックして◉にします。

・無効

WMM 機能を使用しない場合は、「無効」をクリックして◉にします。

8 無線出力 （初期値：最大）

をクリックして「最大」、「大」、「中」、「小」、「最小」のいずれかを選択します。それぞれの出力値は次のとおりです。

POINT

出力値について

チャンネルに 52、56、60、64、Auto のいずれかが設定されている場合、TPC 機能によって、出力値が自動的に 3dB 低くなる場合があります。

・最大 ：18dBm
・大 ：15dBm
・中 ：12dBm
・小 ：9dBm
・最小 ：0dBm

9 接続台数制限 （初期値：無効）

本製品に IEEE802.11a で接続する端末数を制限するかどうかを選択します。
接続台数制限機能の概要については、「簡易ロードバランス（接続台数制限）」（→ P.37）をご覧ください。

・有効
本製品に IEEE802.11a で接続する端末数を制限する場合は、「有効」をクリックしてにし、「台数」を設定します。

・無効
本製品に IEEE802.11a で接続する端末数を制限しない場合は、「無効」をクリックしてにします。

10 台数 （初期値：20 台）

「接続台数制限」が有効のとき、本製品に IEEE802.11a で接続できる端末の最大数を 1 ～ 30（台）の範囲で指定します。

POINT

・「IEEE802.11b/IEEE802.11g」画面の「接続台数制限」が有効のとき、「IEEE802.11b/IEEE802.11g」画面の接続台数制限の台数と、「IEEE802.11a」画面の接続台数制限の台数の合計が 40 台を超えないように設定してください。
・本製品が WDS の親アクセスポイントに設定されている場合、子アクセスポイントも台数に含まれます。

11 無線スイッチ （初期値：オン）

IEEE802.11a の無線電波の発信／停止を選択します。

重要

・IEEE802.11a 準拠（5GHz 帯）の無線 LAN の屋外使用は、電波法により禁じられています。本製品を屋外で使用する場合は、「オフ」を選択してください。

・オン
IEEE802.11a で通信を行う場合は、「オン」をクリックしてにします。「オン」にすると、IEEE802.11a の電波が発信されます。

・オフ
IEEE802.11a の通信を停止する場合は、「オフ」をクリックして◉にします。「オフ」にすると、IEEE802.11a の電波が停止されます。

■「拡張機能」カテゴリ

拡張機能の各設定項目の値は、通常は変更しないでください。無線 LAN 端末が正常に通信できない場合のみ、必要に応じて設定を変更してください。
各項目について説明します。

1 ビーコン間隔 （初期値：100）
ビーコンの送出間隔を 20 ～ 1000（1.024ms）の範囲で指定します。

2 RTS スレッショルド （初期値：2346）
RTS パケットを送信するデータサイズのしきい値を 1 ～ 2346（バイト）の範囲で指定します。データフレーム長がこのサイズを超える場合、RTS/CTS を使用します。

3 フラグメントスレッショルド （初期値：2346）
パケットを断片化するデータサイズを256～2346(バイト)の範囲の偶数で指定します。

4 通信可能速度 （初期値：自動）
をクリックして通信可能速度（Mbps）を、「自動」、または 6 ～ 54 の範囲から選択します。

5 アンテナ選択 （初期値：両方）
をクリックして「両方」、「1」、「2」のいずれかを選択します。
・両方
外部アンテナまたは延長アンテナと、内蔵アンテナを使用する場合は、「両方」を選択します。
・1
外部アンテナまたは延長アンテナを使用し、内蔵アンテナを使用しない場合は、「1」を選択します。
・2
内蔵アンテナを使用し、外部アンテナまたは延長アンテナは使用しない場合は、「2」を選択します。

6 DTIM 間隔 （初期値：1）
ビーコンに DTIM を付加する間隔を 1 ～ 255 の範囲で指定します。

7 MIC Check （初期値：有効）

WPA、または IEEE802.11i (WPA2) の暗号化方式に TKIP を使用して通信するとき、メッセージの改ざんを防止するために MIC エラーを検出するかどうかを選択します。

・有効

MIC エラーを検出する場合は、「有効」をクリックして◉にします。

・無効

MIC エラーを検出しない場合は、「無効」をクリックして◉にします。

4 VLAN の設定

VLAN に関する設定を行います。本製品では、通常 VLAN と認証 VLAN をサポートしており、それぞれ設定方法が異なります。VLAN 機能の概要については、「VLAN」（→ P.28）をご覧ください。

・通常 VLAN
VLAN ID（タグ）によるグループを手動で作成します。作成できるグループ数は、最大 16 個です。「ネットワークプロファイル」メニューで、作成した VLAN グループを SSID と組み合わせるので、同じ VLAN グループに属する端末は、同じネットワークプロファイルを使用します。
・認証 VLAN
端末が RADIUS サーバーとの認証に成功した場合に RADIUS サーバーから VLAN ID が通知され、本製品が自動で割り当てます。RADIUS サーバーで端末ごとにユーザー情報と VLAN ID を管理しているので、本製品で VLAN グループを作成する必要はなく、VLAN グループと SSID の組み合わせも行いません。

VLAN の設定を行う場合は、「VLAN」メニューをクリックします。メインフレームに「VLAN」画面が表示されます。

POINT

本製品の VLAN 機能を有効にする場合

・VLAN 機能を有効にすると、異なる VLAN グループに属する端末間の通信が不可となります。十分注意して設定してください。
・VLAN 機能を有効にする場合は、次の手順で本製品をネットワークへ導入してください。
1. 本製品の設定を、本製品と管理者用パソコンが 1 対 1 の状態で行います。
2. 別途、VLAN 対応のスイッチまたはルータの設定を行います。
3. VLAN 機能が有効になった本製品を、VLAN 対応のスイッチまたはルータに接続します。
4. 管理者用パソコンやSNMPの管理サーバーとなるパソコンを、本設定の「管理VLAN」で設定したグループに属するように接続します。

「VLAN」画面での設定が終了したら、次のように操作してください

1. 「VLAN」画面の「設定」ボタンをクリックします。
「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」というメッセージが表示されます。
2. 次のように操作します。
別メニューの設定を行わない場合
「OK」をクリックします。
別メニューの設定を行う場合
「キャンセル」をクリックして、別メニュー画面の設定を行います。

■VLAN 機能の設定に関するご注意

VLAN 機能の設定を行う場合は、次の点にご注意ください。

・VLAN 機能と WDS 機能の同時使用はできません。
VLAN 機能を有効にした場合、無線 LAN メニューの「IEEE802.11b/IEEE802.11g」画面、および「IEEE802.11a」画面の WDS 機能は自動的に無効になります。

・認証 VLAN を使用する場合は、事前に RADIUS サーバーの設定を行う必要があります。RADIUS サーバーの設定については、「「RADIUS 機能」カテゴリ」（→ P.107）をご覧ください。

・VLAN が有効の場合は、本製品自体が送信元および送信先となる通信は、「管理 VLAN」に指定された VLAN グループ内でのみ可能となります。よって、次の機能は「管理 VLAN」に指定した VLAN グループ内でのみ適応可能です。
- 設定画面へのログイン
- DHCP クライアント
- DHCP サーバー
- Proxy ARP
- RADIUS
- NTP 時刻設定
- syslog
- SNMP
- リンクインテグリティ
- PING テスト

・VLAN 機能の通常 VLAN ／認証 VLAN ／無効を切り替えた場合は、「セキュリティポリシー」画面の設定および「ネットワークプロファイル」画面の設定が、予期した設定になっているかどうか確認してください。予期した設定と異なる場合は、これらを再度設定し直してください。

・無線 LAN 側に送出されるブロードキャストパケット、マルチキャストパケットは VLAN の設定に関係なく、すべての無線 LAN 端末で受信されます。これは IEEE802.11 の仕様によるもので、異常な動作ではありません。

・「ANY 接続拒否」機能が無効のとき、本製品から発信するビーコンパケットに含まれる SSID は、IEEE802.11b/IEEE802.11g と IEEE802.11a それぞれのインターフェースで、一番数字の小さい番号のプロファイルに設定された SSID となります。

「VLAN」画面の項目について説明します。

■「VLAN 機能」カテゴリ

VLAN 機能に関する設定を行うカテゴリです。各項目について説明します。

【通常VLANを選択したときの画面】

【認証VLANを選択したときの画面】

1 VLAN 機能 （初期値：無効）

VLAN 機能を使用するかどうかを選択します。VLAN 機能を有効にする場合は、通常 VLAN と認証 VLAN のどちらを使用するか選択します。

・通常 VLAN

通常 VLAN を使用する場合は、「通常 VLAN」をクリックして◉にし、管理 VLAN、および VLAN グループの設定を行います。

・認証 VLAN

認証 VLAN を使用する場合は、「認証 VLAN」をクリックして◉にし、管理 VLAN の設定を行います。

・無効

VLAN 機能を使用しない場合は、「無効」をクリックして◉にします。

2 管理 VLAN

VLAN 機能を有効にしたとき、表示される項目です。

・通常 VLAN の場合

▼をクリックして、本製品の設定や管理が可能な VLAN グループの VLAN 名と VLAN ID を指定します。

・認証 VLAN の場合
VLAN ID とサービスクラスを設定します。

表：管理 VLAN の設定項目と説明

詳細項目	説明
VLAN ID（初期値：1）	VLAN ID を 0 ～ 4094 の範囲で設定します。
サービスクラス（初期値：1）	をクリックして、優先情報を 1 ～ 8 の範囲で選択します。優先度は「1」が一番高く、番号が大きくなるほど低くなっていきます。

3 1 ～ 16

VLAN 機能で「通常 VLAN」を選択したとき、表示される項目です。VLAN グループを作成します。

・VLAN 名 （「1」の初期値：VLAN1、「2」～「16」の初期値：なし）
VLAN の設定を行う VLAN グループの識別子を設定します。ここで設定する VLAN 名はネットワークプロファイルページで SSID およびポリシー名と関連付けする際に利用します。
任意の文字列を、16 文字以内で入力します。
複数の VLAN グループを作成する場合、それぞれ異なる VLAN 名を設定してください。同じ VLAN 名は設定できません。

重要

・syslog、SNMP 機能を使用して本製品を管理する場合は、全角文字、半角カタカナを使用しないでください。

・VLAN ID （初期値：1）
VLAN ID を 0 ～ 4094 の範囲で設定します。VLAN ID によって端末をグループ分けすることができます。
複数の VLAN グループを作成する場合、それぞれ異なる VLAN ID を設定してください。同じ VLAN ID は設定できません。

・サービスクラス （初期値：1）
をクリックして、各 VLAN の優先情報を 1 ～ 8 の範囲で選択します。優先度は「1」が一番高く、番号が大きくなるほど低くなっていきます。

POINT

VLAN の削除

設定済みの VLAN を削除する場合は、削除する VLAN の VLAN 名を削除します。
・「1」の VLAN 名は削除できません。
・ネットワークプロファイルで使用されている VLAN は削除できません。

5 セキュリティポリシーの設定

無線 LAN のセキュリティに関する設定を行います。セキュリティの設定をセキュリティポリシーとして保存し、「ネットワークプロファイル」メニューで SSID と組み合わせます。
VLAN が無効の場合と有効の場合で、マルチプルセキュリティポリシー機能の無効と有効が自動的に切り替わるため、設定可能なセキュリティポリシーの数が異なります。

・VLAN が無効の場合
マルチプルセキュリティポリシー機能は無効です。IEEE802.11b/IEEE802.11g インターフェースと IEEE802.11a インターフェースのそれぞれに 1 つずつ、セキュリティポリシーを作成できます。
・VLAN が有効の場合
マルチプルセキュリティポリシー機能が有効になります。SSID ごとにセキュリティポリシーを使い分けることができます。最大 16 パターンのセキュリティポリシーを作成することができます。

「セキュリティポリシー」画面

無線 LAN のセキュリティに関する設定を行う場合は、「セキュリティポリシー」メニューをクリックします。メインフレームに「セキュリティポリシー」画面が表示されます。

POINT

「セキュリティポリシー」画面での設定が終了したら、次のように操作してください

1. 「セキュリティポリシー」画面の「設定」ボタンをクリックします。
「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」というメッセージが表示されます。
2. 次のように操作します。
別メニューの設定を行わない場合
「OK」をクリックします。
別メニューの設定を行う場合
「キャンセル」をクリックして、別メニュー画面の設定を行います。

■セキュリティポリシーの設定に関するご注意

セキュリティポリシーの設定について、次の点にご注意ください。
・WDS 機能と、WPA、WPA-PSK、IEEE802.11i(WPA2)、IEEE802.11i (WPA2)-PSK、または IEEE802.1X の同時使用はできません。「セキュリティ」カテゴリの「モード」を「アドバンスド」に設定する場合、または「802.1X 機能」カテゴリの「802.1X」を「使用」に設定する場合は、WDS を無効にしてください。

- 上記のセキュリティポリシーを IEEE802.11b/IEEE802.11g で使用する場合
「IEEE802.11b/IEEE802.11g」画面の「基本設定」カテゴリー「WDS」を無効に設定してください。
- 上記のセキュリティポリシーを IEEE802.11a で使用する場合
「IEEE802.11a」画面の「基本設定」カテゴリー「WDS」を無効に設定してください。

・VLAN 有効時、WPA、802.11i (WPA2)、WPA-PSK、802.11i (WPA2)-PSK のグループキー更新間隔はすべてのセキュリティポリシーで共通の値となり、1 つのセキュリティポリシーに設定されたグループキー更新間隔の値が他のセキュリティポリシーにも反映されます。

■無線 LAN 端末の仕様確認

次の設定項目については、本製品に接続する無線 LAN 端末の仕様を考慮して設定する必要があります。事前に、無線 LAN 端末の仕様をご確認ください。

無線 LAN 端末の仕様については、次のマニュアルをご覧になるか、お使いの機器のメーカーにお問い合わせください。

・無線 LAN 機能が標準搭載されているパソコンの場合は、パソコンに添付のマニュアルをご覧ください。
・無線 LAN カードを増設した場合は、無線 LAN カードのマニュアルをご覧ください。

表：無線 LAN のセキュリティの設定を行う前に確認しておくこと

設定項目名	選択肢	注意事項
「セキュリティ」カテゴリ		
モード	・ベーシック ・アドバンスド	ベーシックを選択すると、無線 LAN のセキュリティを WEP キーまたは、IEEE802.1X で設定します。アドバンスドを選択すると、無線 LAN のセキュリティを WPA、WPA-PSK、IEEE802.11i (WPA2)、IEEE802.11i (WPA2)-PSK で設定します。 無線 LAN 端末によっては、「アドバンスド」は使用できない場合があります。
「802.1X 機能」カテゴリ		
802.1X	・使用 ・未使用	IEEE802.1X機能を使用するかどうかを選択します。 無線 LAN 端末によっては、IEEE802.1X 機能を使用できない場合があります。
「WEP キー」カテゴリ		
キーの長さ	・40 ビット ・104 ビット ・128 ビット	ネットワークキーの長さを設定します。 無線 LAN 端末によっては、104 ビット、128 ビットを使用できない場合があります。
ネットワーク認証	・オープンシステム ・共有キー	無線 LAN の認証方式を設定します。 無線 LAN 端末によっては、オープンシステムまたは共有キーを使用できない場合があります。
キーの形式	・ASCII 文字 ・16 進数	ネットワークキーの入力形式を設定します。 無線 LAN 端末によっては、ASCII 文字、16 進数どちらかの設定しか行えない場合があります。

表：無線 LAN のセキュリティの設定を行う前に確認しておくこと

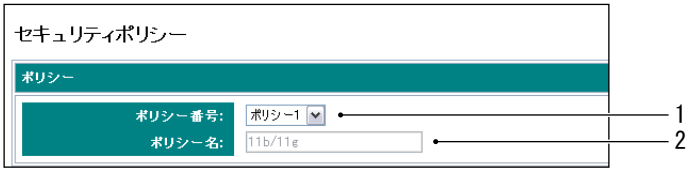
設定項目名	選択肢	注意事項
キーインデックス	・VLAN が無効の場合 「キー 1」～「キー 4」 ・VLAN が有効の場合 「キー 1」のみ	次のように設定してください。 ・キーインデックスを 1 ～ 4 で設定する無線 LAN 端末の場合は、本製品と同じインデックス番号のネットワークキーを同じ値で設定してください。 ・キーインデックスを 0 ～ 3 で設定する無線 LAN 端末の場合は、次のように対応するインデックス番号のネットワークキーを同じ値で設定してください。 ・本製品のキーインデックス 1 と無線 LAN 端末のキーインデックス 0 ・本製品のキーインデックス 2 と無線 LAN 端末のキーインデックス 1 ・本製品のキーインデックス 3 と無線 LAN 端末のキーインデックス 2 ・本製品のキーインデックス 4 と無線 LAN 端末のキーインデックス 3
「WPA/802.11i(WPA2)」カテゴリ		
暗号化方式	・TKIP ・AES ・自動	WPA の暗号化方式を選択します。 無線 LAN 端末によっては、AES を使用できない場合があります。

「セキュリティポリシー」画面の項目について、カテゴリごとに説明します。

■「ポリシー」カテゴリ

ひとつひとつのセキュリティポリシーを識別するための設定を行うカテゴリです。VLAN が無効の場合と有効の場合で設定方法が異なります。

□ VLAN が無効の場合



1 ポリシー番号 （初期値：ポリシー 1）

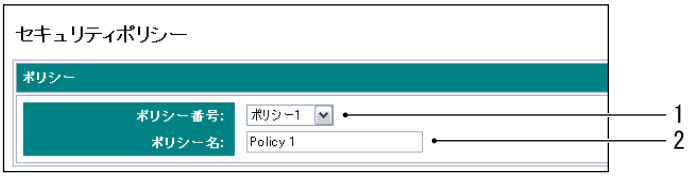
をクリックして「ポリシー 1」または「ポリシー 2」を選択します。

・ポリシー 1
IEEE802.11b/IEEE802.11g 用のセキュリティポリシーを設定する場合は、「ポリシー 1」を選択します。

・ポリシー 2
IEEE802.11a 用のセキュリティポリシーを設定する場合は、「ポリシー 2」を選択します。

2 ポリシー名
ポリシー 1 のポリシー名は「11b/11g」固定です。ポリシー 2 のポリシー名は「11a」固定です。

□ 通常 VLAN または認証 VLAN が有効の場合



1 ポリシー番号 （初期値：ポリシー 1）
をクリックして、「ポリシー 1」～「ポリシー 16」の範囲で選択します。設定を行うポリシーが 1 つの場合は、「ポリシー 1」を選択します。

2 ポリシー名 （初期値：Policy 1）
選択したポリシー番号の識別子を 1 ～ 30 文字の範囲で入力します。異なるポリシー番号に対して同じポリシー名を指定することはできません。
ポリシー名は必ず設定してください。ポリシー名が設定されていないセキュリティポリシーは使用できません。

重要

・syslog、SNMP 機能を使用して本製品を管理する場合は、全角文字、半角カタカナを使用しないでください。

POINT

セキュリティポリシーの削除

設定済みのセキュリティポリシーを削除する場合は、削除するセキュリティポリシーの「ポリシー番号」を選択して、「ポリシー名」を削除します。
・「ポリシー 1」のポリシー名は削除できません。
・ネットワークプロファイルで使用されているポリシーは削除できません。

■「セキュリティ」カテゴリ

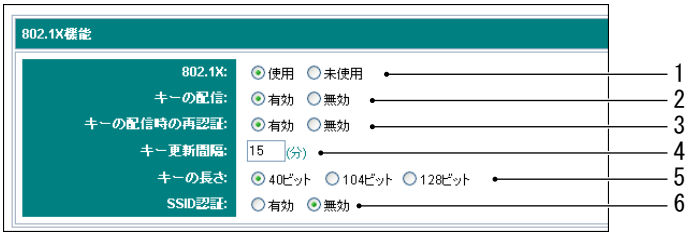
使用するセキュリティに合わせてセキュリティモードを選択するカテゴリです。各項目について説明します。

1 モード
セキュリティモードを選択します。

・ベーシック
無線 LAN のセキュリティを WEP キーまたは、IEEE802.1X で設定する場合は、「ベーシック」をクリックして◉にします。
・アドバンスド
無線 LAN のセキュリティを WPA、WPA-PSK、IEEE802.11i(WPA2)、または IEEE802.11i (WPA2)-PSK で設定する場合は、「アドバンスド」をクリックして◉にします。

■「802.1X 機能」カテゴリ

「セキュリティ」カテゴリの「モード」が「ベーシック」の場合に表示されます。IEEE802.1X に関する設定を行うカテゴリです。各項目について説明します。



1 802.1X （初期値：未使用）

802.1X 機能の「使用」、「未使用」を選択します。

認証 VLAN を有効にした場合は、初期値が「使用」になり、「未使用」は選択できません。

・使用
無線 LAN のセキュリティを IEEE802.1X で設定する場合は、「使用」をクリックして◉にします。

・未使用
無線 LAN のセキュリティを WEP キーで設定する場合は、「未使用」をクリックして◉にします。

2 キーの配信 （初期値：有効）

「802.1X」が「有効」のとき、ネットワークキー配信を行うかどうかを選択します。

・有効
無線 LAN 端末が使用するネットワークキーを自動的に割り当てる場合は、「有効」をクリックして◉にします。RADIUS サーバーの認証プロトコルが EAP-TLS、EAP-TTLS、PEAP の場合は、「有効」を選択してください。

・無効
無線 LAN 端末が使用するネットワークキーを手動で設定する場合は、「無効」をクリックして◉にします。「無効」に設定した場合は「WEP キー」カテゴリでネットワークキーを設定します。RADIUS サーバーの認証プロトコルが EAP-MD5 の場合は、「無効」を選択してください。

3 キーの配信時の再認証 （初期値：有効）

「キーの配信」が「有効」のとき、一定間隔で再認証を行うかどうかを設定します。

・有効
「キー更新間隔」で指定した時間が経過したとき、再認証を行うようにする場合は、「有効」をクリックして◉にします。
・無効
再認証を行わないようにする場合は、「無効」をクリックして◉にします。

4 キー更新間隔 （初期値：15）
「キーの配信時の再認証」が「有効」のとき、ネットワークキーの更新間隔を 15 ～ 1440（分）の範囲で指定します。

5 キーの長さ （初期値：40 ビット）
「キーの配信」が「有効」のとき、使用するネットワークキーを「40 ビット」、「104 ビット」、「128 ビット」のいずれかから選択します。

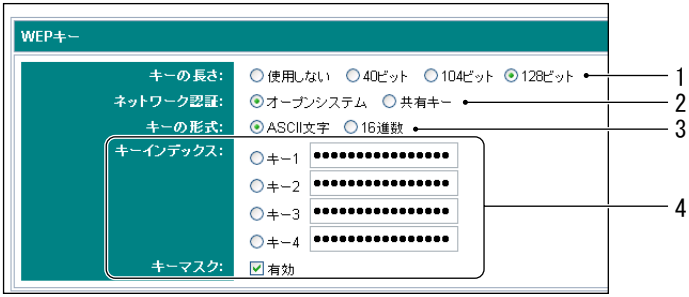
重要

・「キーの長さ」が長いほど、ネットワークキーは解読されにくくなります。ご利用になる無線 LAN 端末の仕様に合わせて、できるだけ長い「キーの長さ」を選択することをお勧めします。

6 SSID 認証 （初期値：無効）
「802.1X」が「有効」のとき、SSID 認証を行うかどうかを選択します。SSID 認証の概要については、「SSID 認証」（→ P.27）をご覧ください。
・有効
SSID 認証を使用する場合は、「有効」をクリックして◉にします。
・無効
SSID 認証を使用しない場合は、「無効」をクリックして◉にします。

■「WEP キー」カテゴリ

「WEP キー」の詳細を設定するカテゴリで、次の場合に表示されます。
・「セキュリティ」カテゴリの「モード」が「ベーシック」、「802.1X 機能」カテゴリの「802.1X」が「未使用」の場合
・「セキュリティ」カテゴリの「モード」が「ベーシック」、「802.1X 機能」カテゴリの「802.1X」が「使用」、「キーの配信」が「無効」の場合
各項目について説明します。



1 キーの長さ （初期値：使用しない）

使用するネットワークキーの長さに合わせて、「40 ビット」、「104 ビット」、「128 ビット」のいずれかをクリックして◉にします。

重要

- **「キーの長さ」は必ず「使用しない」以外を選択して、ネットワークキーを設定してください。ネットワークキーを設定しないと、無線 LAN 機能を搭載したすべてのコンピュータから、本製品に接続できます。したがって、本製品に不正にアクセスされたり、本製品に接続している無線 LAN 端末のデータを、盗まれたり、破壊されたりする危険性があります。**
- **「キーの長さ」が長いほど、ネットワークキーは解読されにくくなります。ご利用になる無線 LAN 端末の仕様に合わせて、できるだけ長い「キーの長さ」を選択することをお勧めします。**

2 ネットワーク認証 （初期値：オープンシステム）

ネットワーク認証を選択します。

・オープンシステム

無線 LAN 端末の接続時にネットワークキーが一致するかどうかを本製品に確認させない場合は、「オープンシステム」をクリックして◉にします。

ただし、本製品とネットワークキーが一致していない無線 LAN 端末は、本製品経由の通信を行うことはできません。ネットワークキーを使用しない場合は、「オープンシステム」のみ選択可能です。

・共有キー

無線 LAN 端末の接続時にネットワークキーが一致するかどうかを本製品に確認させる場合は、「共有キー」をクリックして◉にします。

ネットワークキーを使用していない無線 LAN 端末、およびネットワークキーが一致しない無線 LAN 端末は接続できません。

3 キーの形式 （初期値：ASCII 文字）

キーの形式を選択します。

・ASCII 文字

キー 1 ～キー 4 にネットワークキーを ASCII 文字で入力する場合は、「ASCII 文字」をクリックして◉にします。ネットワークキーに使用できる文字は半角英数字、半角記号です。アルファベットの大文字、小文字を区別します。

ネットワークキーを 40 ビットで設定する場合は、5 文字で入力します。

ネットワークキーを 104 ビットで設定する場合は、13 文字で入力します。

ネットワークキーを 128 ビットで設定する場合は、16 文字で入力します。

・16 進数

キー 1 ～ 4 にネットワークキーを 16 進数のキャラクターコードで入力する場合は、「16 進数」をクリックして◉にします。ネットワークキーに使用できる文字は半角の 0 ～ 9、A ～ F、a ～ f です。アルファベットの大文字、小文字を区別しません。

ネットワークキーを 40 ビットで設定する場合は、10 桁で入力します。

ネットワークキーを 104 ビットで設定する場合は、26 桁で入力します。

ネットワークキーを 128 ビットで設定する場合は、32 桁で入力します。

4 キーインデックス （初期値：キー 1）

・VLAN が無効の場合

必要に応じて、ネットワークキーを 4 つまで設定できます。通常は「キー 1」をクリックして◉にし、ネットワークキーを入力します。

・VLAN が有効の場合

「キー 1」にネットワークキーを入力します。

VLAN が有効の場合は、本製品のマルチプル SSID 機能が有効になります。マルチプル SSID 機能が有効の状態では、使用可能なキーインデックスは「キー 1」のみとなります。

POINT

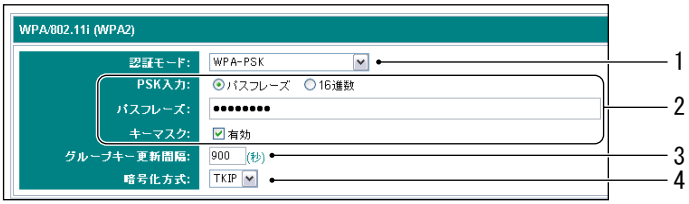
ネットワークキーを確認する場合

ネットワークキーは常にマスク表示されています。ネットワークキーの値を確認する場合は、「キーマスク」の有効をクリックして☐にすると、マスク表示が無効になります。ただし「設定」ボタンをクリックすると、「キーマスク」は自動的に有効になります。

■「WPA/802.11i (WPA2)」カテゴリ

WPA の詳細を設定するカテゴリで、「セキュリティ」カテゴリの「モード」が「アドバンスド」のときに表示されます。各項目について説明します。

【WPA-PSKを選択したときの画面】



【WPAを選択したときの画面】

1 認証モード （初期値：WPA-PSK）

WPA ／ IEEE802.11i (WPA2) の認証モードを選択します。

認証 VLAN を有効にした場合は、初期値が WPA になり、WPA-PSK、802.11i (WPA2)-PSK、WPA-PSK/802.11i (WPA2)-PSK は選択できません。

・WPA-PSK

無線 LAN のセキュリティを WPA-PSK で設定します。

・WPA

無線 LAN のセキュリティを WPA で設定します。

・802.11i (WPA2)-PSK
無線 LAN のセキュリティを IEEE802.11i (WPA2)-PSK で設定します。
・802.11i (WPA2)
無線 LAN のセキュリティを IEEE802.11i (WPA2) で設定します。
・WPA-PSK/802.11i (WPA2)-PSK
無線 LAN 端末の認証モードを WPA-PSK と IEEE802.11i (WPA2)-PSK のいずれかで自動判別し、認証を行います。
・WPA/802.11i (WPA2)
無線 LAN 端末のセキュリティを WPA と IEEE802.11i (WPA2) のいずれかで自動判別し、認証を行います。

2 PSK 入力 （初期値：パスフレーズ）

「認証モード」が「WPA-PSK」、「802.11i (WPA2)-PSK」、または「WPA-PSK/802.11i (WPA2)-PSK」のとき、PSK の入力方法を選択して PSK を入力します。

POINT

PSK を確認する場合

PSK は常にマスク表示されています。PSK の値を確認する場合は、「キーマスク」の有効をクリックして☐にすると、マスク表示が無効になります。ただし「設定」ボタンをクリックすると、「キーマスク」は自動的に有効になります。

・パスフレーズ
「パスフレーズ」をクリックして◉にすると、「パスフレーズ」項目が表示されます。「パスフレーズ」に PSK を ASCII 文字 8 ～ 63 文字の範囲で入力します。使用できる文字は、半角英数字、半角記号です。アルファベットの大文字、小文字を区別します。
「パスフレーズ」項目の初期値は「12345678」です。

重要

・文字数が長いほどパスフレーズは解読されにくくなります。パスフレーズは 21 文字以上で設定することをお勧めします。

・16 進数
16 進数をクリックして◉にすると、「PSK」項目が表示されます。「PSK」に PSK を 16 進数 64 文字で入力します。使用できる文字は、0 ～ 9、A ～ F、a ～ f です。アルファベットの大文字、小文字を区別しません。
「PSK」項目の初期値はありません。

3 グループキー更新間隔 （初期値：900）

グループキーの更新間隔を 900 ～ 86400(秒) の範囲で指定します。

4 暗号化方式 （初期値：TKIP）

暗号化方式を選択します。▼をクリックして「TKIP」、「AES」、「自動」のいずれかを選択します。
・TKIP
TKIP で暗号化を行う場合は「TKIP」を選択します。無線 LAN 端末の暗号化方式を TKIP に設定している必要があります。

・AES
AES で暗号化を行う場合は「AES」を選択します。無線 LAN 端末の暗号化方式を AES に設定している必要があります。
・自動
無線 LAN 端末の暗号化方式を自動判別し、TKIP、または AES で暗号化を行う場合は「自動」を選択します。

5 SSID 認証 （初期値：無効）

「認証モード」が「WPA」、「802.11i(WPA2)」、または「WPA/802.11i(WPA2)」のとき、SSID 認証を行うかどうかを選択します。SSID 認証の概要については、「SSID 認証」（→ P.27）をご覧ください。

・有効
SSID 認証を使用する場合は、「有効」をクリックして◉にします。
・無効
SSID 認証を使用しない場合は、「無効」をクリックして◉にします。

■「MAC アドレスフィルタリング」カテゴリ

無線 LAN 端末の接続を MAC アドレスによって制御するための設定を行うカテゴリです。

重要

・「MAC アドレスフィルタング」カテゴリの設定を行う前に、必ず「セキュリティポリシー」画面の「設定」ボタンをクリックしてください。
「セキュリティポリシー」画面の「設定」ボタンをクリックせずに MAC アドレスフィルタリングの設定を行うと、「セキュリティポリシー」画面で変更した内容が反映されません。

各項目について説明します。

1 アドレス制御 （初期値：無効）

登録した無線 LAN 端末の制御方法を選択します。

POINT

・無線 LAN 端末を登録していない状態で、「拒否」または「許可」を選択して「設定」ボタンをクリックすると、「拒否」の場合は、すべての無線 LAN 端末からの接続を許可し、「許可」の場合はすべての無線 LAN 端末からの接続を拒否するように設定されます。

・許可
登録した無線 LAN 端末のみ、本製品と接続できるようにする場合は、「許可」をクリックして◉にします。登録していない無線LAN端末は、本製品と接続できません。本製品と接続できるようにする無線 LAN 端末は、「MAC アドレスフィルタリングの設定」ボタンをクリックして表示される画面で登録します。

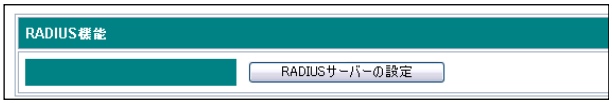
・拒否
登録した無線 LAN 端末は、本製品と接続できないようにする場合は、「拒否」をクリックして◉にします。登録していない無線 LAN 端末は、本製品と接続できます。本製品に接続できないようにする無線 LAN 端末は、「MAC アドレスフィルタリングの設定」ボタンをクリックして表示される画面で登録します。
・無効
MAC アドレスによる無線 LAN 端末の接続の制御を行わない場合は、「無効」をクリックして◉にします。

2 「MAC アドレスフィルタリングの設定」ボタン

クリックすると、「MAC アドレスフィルタリングの設定」画面が表示されます。無線 LAN 端末を登録するとき、および無線 LAN 端末の接続状況を確認するときにクリックします。
「MAC アドレスフィルタリングの設定」画面については、「「MAC アドレスフィルタリングの設定」画面」（→ P.108）をご覧ください。

■「RADIUS 機能」カテゴリ

RADIUS 認証サーバーおよびアカウンティングサーバーを設定するためのカテゴリです。
RADIUS アカウンティング機能については、「RADIUS アカウンティング」（→ P.27）をご覧ください。
RADIUS 機能を設定する場合は、RADIUS サーバーとして設定したパソコンが 1 台以上必要です。
RADIUS サーバーの設定を行う場合は、「RADIUS 機能」カテゴリの「RADIUS サーバーの設定」ボタンをクリックします。「RADIUS サーバーの設定」ボタンをクリックすると、「RADIUS サーバーの設定」画面が表示されます。



重要

**・「RADIUS サーバーの設定」ボタンをクリックする前に、必ず「セキュリティポリシー」画面の「設定」ボタンをクリックしてください。
「セキュリティポリシー」画面の「設定」ボタンをクリックせずに「RADIUS サーバーの設定」ボタンをクリックすると、「セキュリティポリシー」画面で変更した内容が反映されません。**

「RADIUS サーバーの設定」画面については、「「RADIUS サーバーの設定」画面」（→ P.110）をご覧ください。

「MAC アドレスフィルタリングの設定」画面

「MAC アドレスフィルタリングの設定」画面では、無線 LAN 端末の接続状況の確認を行ったり、フィルタリングの対象となる無線 LAN 端末の登録を行ったりします。

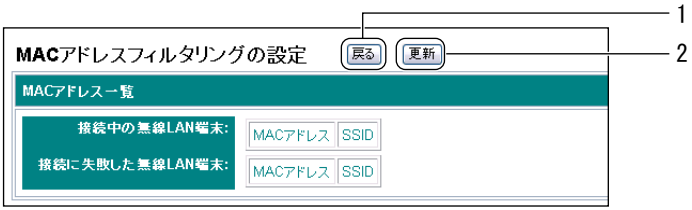
POINT

「MAC アドレスフィルタリングの設定」画面での設定が終了したら、次のように操作してください

1. 「MAC アドレスフィルタリングの設定」画面の「戻る」ボタンをクリックします。
   「セキュリティポリシー」画面に戻ります。
2. 「MAC アドレスフィルタリング」カテゴリの「アドレス制御」の設定を行います。
3. 必要に応じて「セキュリティポリシー」画面の設定を行います。

「MAC アドレスフィルタリングの設定」画面の項目について、カテゴリごとに説明します。

■画面上部のボタン

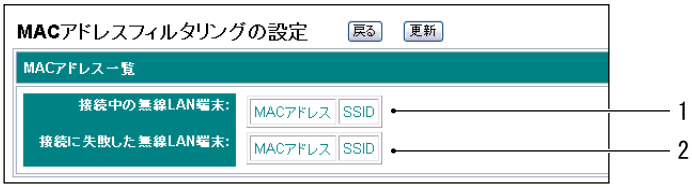


1 「戻る」ボタン
クリックすると、「セキュリティポリシー」画面に戻ります。

2 「更新」ボタン
クリックすると「MAC アドレス一覧」カテゴリの内容を更新して、現在の接続状況を表示します。

■「MAC アドレス一覧」カテゴリ

無線 LAN 端末の接続状況の確認を行うカテゴリです。各項目について説明します。



1 接続中の無線 LAN 端末

本製品に接続中の無線 LAN 端末の MAC アドレス一覧が表示されます。

無通信切断タイマー機能により本製品から接続を切断された無線 LAN 端末は、表示から削除されます。

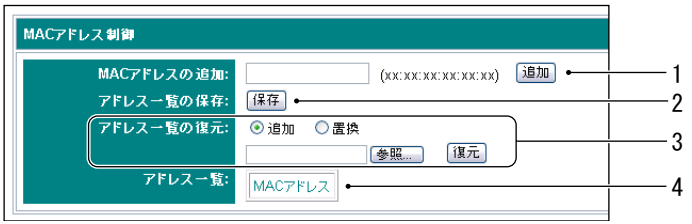
「無通信切断タイマー」については、「無通信切断タイマー設定」（→ P.128）をご覧ください。

2 接続に失敗した無線 LAN 端末

MAC アドレスフィルタリングにより、本製品に接続できなかった無線 LAN 端末の MAC アドレス一覧が表示されます。

■「MAC アドレス制御」カテゴリ

無線 LAN 端末の登録などを行うカテゴリです。各項目について説明します。



1 MAC アドレスの追加

本製品へのアクセスを制御する無線 LAN 端末を登録します。128 個まで登録できます。

無線 LAN 端末の MAC アドレスを、次の例のように 2 桁ずつコロン（:）で区切って入力し、「追加」ボタンをクリックします。

例）00:11:22:33:44:55 （MAC アドレスが「001122334455」の場合）

追加された MAC アドレスは、「アドレス一覧」に表示されます。

2 アドレス一覧の保存

「保存」ボタンをクリックすると、「アドレス一覧」に設定された MAC アドレス一覧を CSV 形式のファイルに保存します。

実際に画面に表示されるメッセージなどを確認して、ファイルを保存してください。

POINT

- ここで保存したファイルは、アドレス一覧を復元するときに使用します。わかりやすい名前、場所で保存してください。
- ファイルの種類は「.csv」になります。変更しないでください。

3 アドレス一覧の復元

「アドレス一覧の保存」で保存した CSV 形式のファイルを使用して、アドレス一覧を復元します。次の手順で復元します。

1. **アドレス一覧の復元方法を選択します。**
   - 追加（初期値）
     現在のアドレス一覧に、ファイルに登録されているアドレス一覧を追加登録する場合は、「追加」をクリックして◉にします。
   - 置換
     現在のアドレス一覧を消去し、ファイルに登録されているアドレス一覧を登録する場合は、「置換」をクリックして◉にします。
2. **「参照」ボタンをクリックします。**
   「参照」ボタンをクリックした後は、実際に画面に表示されるメッセージなどを確認して、ファイルを選択してください。
   選択したファイル名がテキストボックスに表示されます。
3. **「復元」ボタンをクリックします。**

POINT

エラーメッセージが表示された場合

- 選択したファイルの種類が「.csv」ではないか、または正しいファイルではありません。アドレス一覧を登録した、正しい「（ファイル名）.csv」ファイルを選択してください。
- 登録できるアドレスは 128 個までです。
  追加／置換した結果、アドレスの登録数が 129 個以上になる場合はエラーメッセージが表示され、129 個目以降の MAC アドレスは破棄されます。

4 アドレス一覧

登録した無線 LAN 端末の MAC アドレス一覧が表示されます。

「RADIUS サーバーの設定」画面

「RADIUS サーバーの設定」画面では、認証用やアカウンティング用の RADIUS サーバーに関する設定を行います。

POINT

「RADIUS サーバーの設定」画面での設定が終了したら、次のように操作してください

1. 「RADIUS サーバーの設定」画面の「設定」ボタンをクリックします。
   「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」というメッセージが表示されます。
2. 次のように操作します。
   別メニューの設定を行わない場合
   「OK」をクリックします。
   別メニューの設定を行う場合
   「キャンセル」をクリックして、別メニュー画面の設定を行います。

■RADIUS の設定に関するご注意

RADIUS の設定について、次の点にご注意ください。

・RADIUS サーバーの設定は、すべてのセキュリティポリシーで共通です。セキュリティポリシーごとに異なる設定を使い分けることはできません。

・認証 VLAN 機能、または SSID 認証機能を使用する場合は、「RADIUS サーバー 1」と「RADIUS サーバー 2」の少なくともどちらか一方を「使用」にして、各項目を設定してください。認証 VLAN 機能、または SSID 認証機能を有効にしている場合、「RADIUS サーバー 1」と「RADIUS サーバー 2」の両方を「未使用」に設定することはできません。

「RADIUS サーバーの設定」画面の項目について説明します。

■「RADIUS 機能」カテゴリ

各項目について説明します。

1 RADIUS サーバー 1 （初期値：未使用）

RADIUS サーバー 1 を次のように設定します。

・使用

RADIUS サーバーの設定をする場合、使用をクリックして◉にし、次の表にある詳細項目の設定を行います。

表：「RADIUS サーバー」の設定項目と説明

詳細項目	説明
IP アドレス	RADIUS サーバーの IP アドレスを指定します。

表：「RADIUS サーバー」の設定項目と説明

詳細項目	説明
ポート （初期値：1812）	RADIUS 認証で使用するポート番号を 1 ～ 65535 の範囲で指定します。通常は変更する必要はありません。
共有シークレット	RADIUS 認証サーバーで指定されている共有シークレットを半角英数字、および半角記号 64 文字以内で入力します。アルファベットの大文字、小文字を区別します。全角文字や、半角カタカナは使用できません。
アカウンティング用ポート （初期値：1813）	「RADIUS アカウンティング」項目の設定が「認証サーバーを使用」のときに設定可能な詳細項目です。 RADIUS アカウンティングで使用するポート番号を 1 ～ 65535 の範囲で指定します。通常は変更する必要はありません。

・未使用
RADIUS サーバーを使用しない場合、「未使用」をクリックして◉にします。

2 RADIUS サーバー 2

・使用
RADIUS サーバー 1 以外の RADIUS サーバーがある場合は、「使用」をクリックして◉にし、RADIUS サーバー 1 と同様に設定します。

・未使用
RADIUS サーバー 1 以外の RADIUS サーバーがない場合は「未使用」をクリックして◉にします。

3 アカウンティングサーバー

「RADIUS アカウンティング」項目の設定が「個別指定」のときに表示される項目です。

表：「アカウンティングサーバー」の設定項目と説明

詳細項目	説明
IP アドレス	アカウンティングサーバーの IP アドレスを指定します。
ポート （初期値：1813）	RADIUS アカウンティングで使用するポート番号を 1 ～ 65535 の範囲で指定します。通常は変更する必要はありません。
共有シークレット	アカウンティングサーバーで指定されている共有シークレットを半角英数字、および半角記号 64 文字以内で入力します。アルファベットの大文字、小文字を区別します。全角文字や、半角カタカナは使用できません。

POINT

RADIUS サーバー 1、RADIUS サーバー 2、アカウンティングサーバーの共有シークレットを確認する場合

共有シークレットは常にマスク表示されています。共有シークレットの値を確認する場合は、「キーマスク」の有効をクリックして☐にすると、マスク表示が無効になります。ただし「設定」ボタンをクリックすると、「キーマスク」は自動的に有効になります。

4 アクセス方法 （初期値：プライマリ / セカンダリ）

「RADIUS サーバー 1」と「RADIUS サーバー 2」の両方が「使用」のときに表示される項目です。「RADIUS サーバー 1」と「RADIUS サーバー 2」の使い方を設定します。

・プライマリ / セカンダリ

「RADIUS サーバー 1」を優先サーバー、「RADIUS サーバー 2」をバックアップサーバーとして使用する場合は、「プライマリ / セカンダリ」をクリックして◉にします。再認証時には、必ず「RADIUS サーバー 1」にアクセスし、「RADIUS サーバー 1」からの応答がない場合、「RADIUS サーバー 2」にアクセス先を切り替えます。

・同等

「RADIUS サーバー 1」と「RADIUS サーバー 2」を同じ優先度で使用する場合は、「同等」をクリックして◉にします。再認証時には、前回の認証に成功したサーバーにアクセスします。RADIUS サーバーからの応答がない場合、アクセス先を切り替えます。

5 RADIUS アカウンティング

RADIUS アカウンティングを使用するかどうか、また使用する場合は、アカウンティングサーバーの指定方法を選択します。

POINT

・WEP、WPA-PSK、または IEEE802.11i(WPA2)-PSK で設定したセキュリティポリシーがある場合は、「個別指定」を選択してください。

・認証サーバーを使用

RADIUS アカウンティングを使用し、RADIUS サーバー 1（および RADIUS サーバー 2）を、アカウンティングサーバーとして併用する場合は、「認証サーバーを使用」をクリックして◉にします。

「RADIUS サーバー 1」（および「RADIUS サーバー 2」）の詳細項目で「アカウンティング用ポート」を設定する必要があります。

・個別指定

RADIUS アカウンティングを使用し、アカウンティングサーバーを、RADIUS 認証サーバーとは別に指定する場合は、「個別指定」をクリックして◉にします。

「アカウンティングサーバー」項目を設定する必要があります。

・未使用

RADIUS アカウンティングを使用しない場合は、「未使用」をクリックして◉にします。

6 リトライ間隔 （初期値：5）

RADIUS サーバーに認証要求をリトライするときの間隔を 1 ～ 60（秒）の範囲で指定します。通常は変更する必要はありません。

7 リトライ回数 / サーバー （初期値：5）

サイクルごとに何回リトライを行うかを、1 ～ 10（回）の範囲で指定します。通常は変更する必要はありません。

8 サイクル数 （初期値：3）

それぞれのサーバーに対して、「リトライ回数 / サーバー」で指定した回数のリトライを行うことを 1 サイクルといいます。何サイクル試行したら認証要求を停止するかを、1 ～ 5（回）の範囲で指定します。通常は変更する必要はありません。

6 ネットワークプロファイルの設定

SSID を設定し、SSID と無線 LAN インターフェース、VLAN グループ（通常 VLAN が有効の場合のみ）、セキュリティポリシーを組み合わせます。その組み合わせをネットワークプロファイルとして保存します。
VLAN が無効の場合と有効の場合で、マルチプル SSID 機能の無効と有効が自動的に切り替わるため、設定可能なネットワークプロファイルの数が異なります。

・VLAN が無効の場合
マルチプル SSID 機能は無効です。IEEE802.11b/IEEE802.11g インターフェースと IEEE802.11a インターフェースのそれぞれに 1 つの SSID を設定します。同じ SSID を設定することもできます。
・VLAN が有効の場合
マルチプル SSID 機能が有効となります。IEEE802.11b/IEEE802.11g インターフェースと IEEE802.11a インターフェースのそれぞれで、複数のネットワークプロファイルを作成できます。最大 16 パターンのネットワークプロファイルを作成することができます。

POINT

・ただし、「ANY 接続拒否」が無効の場合でも、それぞれのインターフェースで一番数字の小さい番号のプロファイルに設定された SSID 以外は隠蔽されます。

ネットワークプロファイルの設定を行う場合は、「ネットワークプロファイル」メニューをクリックします。メインフレームに「ネットワークプロファイル」画面が表示されます。

POINT

「ネットワークプロファイル」画面での設定が終了したら、次のように操作してください

1. 「ネットワークプロファイル」画面の「設定」ボタンをクリックします。
「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」というメッセージが表示されます。
2. 次のように操作します。
別メニューの設定を行わない場合
「OK」をクリックします。
別メニューの設定を行う場合
「キャンセル」をクリックして、別メニュー画面の設定を行います。

「ネットワークプロファイル」画面の項目について説明します。

■「プロファイル」カテゴリ

ネットワークプロファイルを作成するカテゴリです。VLAN が無効の場合と有効の場合で、設定方法が異なります。

□ VLAN が無効の場合

1 1

IEEE802.11b/IEEE802.11g 用のネットワークプロファイルを作成します。

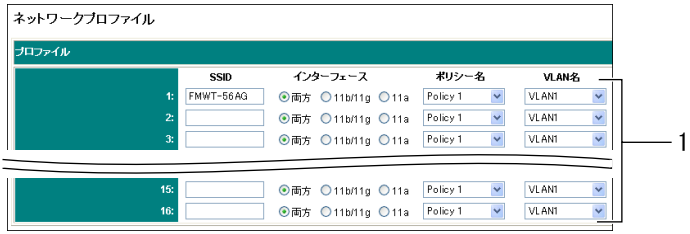
・SSID （初期値：FMWT-56AG）
SSID を半角英数および半角記号で 1 ～ 32 文字の範囲で入力します。アルファベットの大文字、小文字を区別します。
・インターフェースは「11b/11g」固定です。
・ポリシー名は「11b/11g」固定です。

2 2

IEEE802.11a 用のネットワークプロファイルを作成します。

・SSID （初期値：FMWT-56AG）
SSID を半角英数および半角記号で 1 ～ 32 文字の範囲で入力します。アルファベットの大文字、小文字を区別します。
・インターフェースは「11a」固定です。
・ポリシー名は「11a」固定です。

□ 通常 VLAN または認証 VLAN が有効の場合



1 1 ～ 16

プロファイルを次のように設定します。

・SSID （「1」の初期値：FMWT-56AG、「2」～「16」の初期値：なし）
SSID を半角英数および半角記号で 1 ～ 32 文字の範囲で入力します。アルファベットの大文字、小文字を区別します。最大 16 個の SSID を使用して、無線 LAN 端末を VLAN ID によりグループ分けすることができます。
複数のネットワークプロファイルを作成する場合、それぞれ異なる SSID を設定してください。同じ SSID は設定できません。
SSID は必ず設定してください。SSID が設定されていないネットワークプロファイルは使用できません。

・インターフェース （初期値：両方）
無線 LAN インターフェースを選択します。
  ・両方
  IEEE802.11b/IEEE802.11g、IEEE802.11a の両方でプロファイルの設定を使用する場合は、「両方」をクリックして◉にします。
  ・11b/11g
  IEEE802.11b/IEEE802.11g のみでプロファイルの設定を使用する場合は、「11b/11g」をクリックして◉にします。
  ・11a
  IEEE802.11a のみでプロファイルの設定を使用する場合は、「11a」をクリックして◉にします。

・ポリシー名 （初期値：ポリシー 1）
▼をクリックしてポリシー名を選択します。

・VLAN 名 （初期値：VLAN1）
VLAN 機能が「通常 VLAN」の場合は、SSID と VLAN 名の組み合わせを設定します。「認証 VLAN」の場合、この項目は表示されません。
▼をクリックして VLAN 名を選択します。複数のネットワークプロファイルを作成する場合、それぞれ異なる VLAN 名を選択してください。異なるネットワークプロファイルで同じ VLAN 名は設定できません。

POINT

有効なプロファイルの無線 LAN インターフェースがすべて同一の場合

・有効なプロファイルの「インターフェース」の設定がすべて「11b/11g」の場合

「どのプロファイルにも 11a が割り当てられていませんので、このインターフェースの無線スイッチをオフにします。よろしいですか？」という確認画面が表示されます。
・「OK」をクリックすると、自動的に「IEEE802.11a」画面の「基本設定」カテゴリー「無線スイッチ」がオフに設定されます。
・「キャンセル」をクリックすると、「IEEE802.11a」画面の「基本設定」カテゴリー「ANY 接続拒否」が「有効」に設定されます。

・有効なプロファイルの「インターフェース」の設定がすべて「11a」の場合
「どのプロファイルにも 11b/11g が割り当てられていませんので、このインターフェースの無線スイッチをオフにします。よろしいですか？」という確認画面が表示されます。
・「OK」をクリックすると、自動的に「IEEE802.11b/IEEE802.11g」画面の「基本設定」カテゴリー「無線スイッチ」が「オフ」に設定されます。
・「キャンセル」をクリックすると、「IEEE802.11b/IEEE802.11g」画面の「基本設定」カテゴリー「ANY 接続拒否」が「有効」に設定されます。

使用していなかった無線 LAN インターフェースを使用するプロファイルを作成した場合は、「IEEE802.11b/IEEE802.11g」画面および「IEEE802.11a」画面の「基本設定」カテゴリー「ANY 接続拒否」項目と「無線スイッチ」項目の設定が、予期した設定になっているかどうか確認してください。予期した設定と異なる場合は、これらの項目のみ、再度設定し直してください。

POINT

ネットワークプロファイルの削除

設定済みのネットワークプロファイルを削除する場合は、削除するネットワークプロファイルの SSID を削除します。
・VLAN が無効の場合、ネットワークプロファイルは削除できません。
・VLAN が有効の場合、「1」のネットワークプロファイルは削除できません。

5

第 5 章

設定の詳細（管理／メンテナンス機能）

管理機能およびメンテナンス機能の詳細について説明します。

1 管理機能の設定

本製品を管理するための基本的な設定や、システム設定を行う場合は、「管理機能」メニューをクリックします。メインフレームに「管理機能」画面が表示されます。

POINT

「管理機能」画面での設定が終了したら、次のように操作してください

1. 「管理機能」画面の「設定」ボタンをクリックします。
   「設定の変更を反映させるには再起動が必要です。今すぐ再起動しますか？」というメッセージが表示されます。
2. 次のように操作します。
   別メニューの設定を行わない場合
   「OK」をクリックします。
   別メニューの設定を行う場合
   「キャンセル」をクリックして、別メニュー画面の設定を行います。

「管理機能」画面の「システム時刻」カテゴリ、「アカウント設定」カテゴリ、「システム設定」カテゴリ、「監視機能」カテゴリの項目について説明します。
その他のカテゴリについては、「システムのメンテナンス」（→ P.139）をご覧ください。

■管理機能の設定に関するご注意

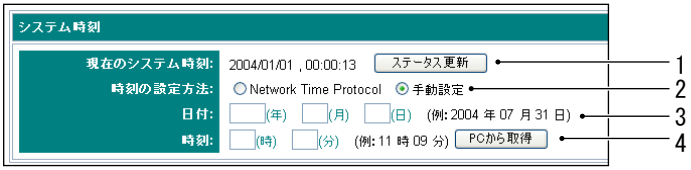
管理機能の設定について、次の点にご注意ください。

・時刻の設定方法が「手動設定」の場合は、本製品の電源を入れ直した場合および本製品を再起動した場合は、システム時刻の設定が初期値に戻ります。
本製品の電源を入れ直したあと、および再起動した後は、再度、時刻の設定を行ってください。

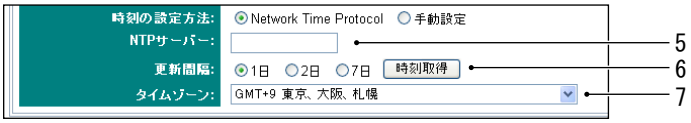
■「システム時刻」カテゴリ

本製品のシステム時刻を設定するカテゴリです。
各項目について説明します。

【時刻の設定方法が「手動設定」のときの画面】



【時刻の設定方法が「Network Time Protocol」のときの画面】



1 現在のシステム時刻

「管理機能」画面を開いたときの本製品のシステム時刻が表示されます。
「ステータス更新」ボタンをクリックすると、「現在のシステム時刻」の表示が更新されます。

2 時刻の設定方法 （初期値：手動設定）

本製品のシステム時刻の設定方法を選択します。

・Network Time Protocol

システム時刻を NTP サーバーから自動取得する場合は、「Network Time Protocol」をクリックして◉にします。NTP サーバーとして設定したパソコンが 1 台必要です。

・手動設定

システム時刻を手動で設定する場合は、「手動設定」をクリックして◉にします。

3 日付

「時刻の設定方法」が「手動設定」のとき、現在の日付を入力します。「年」「月」「日」をすべて入力します。

表：「日付」の各詳細項目の説明

詳細項目	説明
年（初期値：2004）	2000 ～ 2037 の範囲で入力します。
月 （初期値：01）	01 ～ 12 の範囲で入力します。1 桁の月（1 月～ 9 月）の場合は、最初に 0 を付けて「01」のように入力します。
日 （初期値：01）	年や月によって、入力範囲は次のようになります。1 桁の日（1 日～ 9 日）の場合は、最初に 0 を付けて「01」のように入力します。 ・「月」が 01、03、05、07、08、10、12 のとき 01 ～ 31 ・「月」が 04、06、09、11 のとき 01 ～ 30 ・「月」が 02 のとき 01 ～ 28 01 ～ 29（うるう年の場合）

4 時刻

「時刻の設定方法」が「手動設定」のとき、現在の時刻を入力します。「時」「分」の両方を入力します。

POINT

・「PC から取得」ボタンをクリックすると、管理者用パソコンの日付と時刻を取得して本製品の「日付」と「時刻」を設定します。

表：「時刻」の各詳細項目の説明

詳細項目	説明
時 （初期値：00）	00 ～ 23 の範囲で設定します。1 桁（0 時～ 9 時）の場合は、最初に 0 を付けて「01」のように入力します。
分 （初期値：00）	00 ～ 59 の範囲で設定します。1 桁（0 分～ 9 分）の場合は、最初に 0 を付けて「01」のように入力します。

5 NTP サーバー （初期値：なし）

「時刻の設定方法」が「Network Time Protocol」のとき、NTP サーバーの IP アドレスを設定します。

6 更新間隔 （初期値：1 日）

「時刻の設定方法」が「Network Time Protocol」のとき設定します。本製品が自動的に NTP サーバーと時刻の同期を行う間隔を「1 日」、「2 日」、「7 日」のいずれかから選択し、クリックして◉にします。

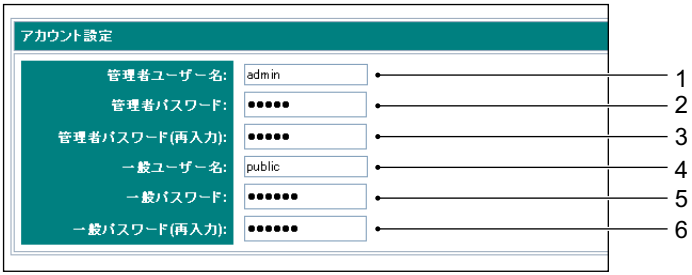
「時刻取得」ボタンをクリックすると、即時に NTP サーバーと時刻の同期を行い、「現在のシステム時刻」の表示が更新されます。

7 タイムゾーン （初期値：GMT ＋ 9 東京、大阪、札幌）

「時刻の設定方法」が「Network Time Protocol」のとき設定します。「GMT ＋ 9 東京、大阪、札幌」を選択します。

■「アカウント設定」カテゴリ

本製品の設定画面にログインするアカウントの設定を行うカテゴリです。各項目について説明します。



1 管理者ユーザー名 （初期値：admin）

本製品の設定を変更したり、ステータスの確認を行ったりする管理者権限のユーザー名を指定します。半角 1 ～ 32 文字の範囲で入力します。使用できる文字は、半角英数字、および半角記号（ただし半角のコロン「:」は除く）で、アルファベットの大文字、小文字を区別します。全角文字や、半角カタカナは使用できません。

管理者ユーザー名でログインすると、ブラウザ設定画面のすべてのメニュー画面で読み書きができます。Dr.WLAPPer を使用する場合も、「管理者ユーザー名」でログインします。

2 管理者パスワード （初期値：admin）

「管理者ユーザー名」でログインするときに使用するパスワードを指定します。半角英数字、および半角記号で、1 ～ 32 文字の範囲で入力します。アルファベットの大文字、小文字を区別します。全角文字や、半角カタカナは使用できません。

3 管理者パスワード（再入力）（初期値：admin）

確認のために「管理者パスワード」と同じ値を入力します。

4 一般ユーザー名 （初期値：public）

本製品のステータス確認のみを行うことができる、一般権限のユーザー名を指定します。半角 1 ～ 32 文字の範囲で入力します。使用できる文字は、半角英数字、および半角記号（ただし半角のコロン「:」は除く）で、アルファベットの大文字、小文字を区別します。全角文字や、半角カタカナは使用できません。また、「管理者ユーザー名」と同じ名前は指定できません。

一般ユーザー名でログインすると、ブラウザ設定画面の「ステータス一覧」画面のみ見ることができます。別のメニューを選択すると、ログイン画面が表示されます。別のメニュー画面にアクセスする場合は、管理者ユーザー名でログインし直す必要があります。

5 一般パスワード （初期値：public）

「一般ユーザー名」でログインするときに使用するパスワードを指定します。半角英数字、および半角記号で、1 ～ 32 文字の範囲で入力します。アルファベットの大文字、小文字を区別します。全角文字や、半角カタカナは使用できません。

6 一般パスワード（再入力）（初期値：public）

確認のために「一般パスワード」と同じ値を入力します。

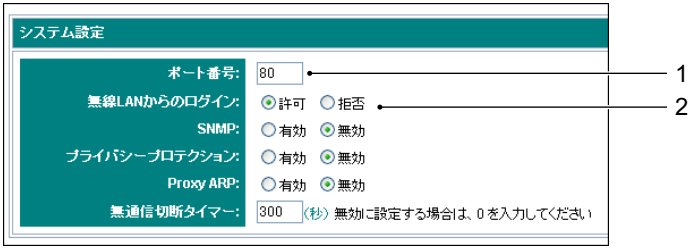
■「システム設定」カテゴリ

「システム設定」カテゴリでは、次の機能に関する設定が行えます。

・「設定画面へのログイン制限設定」（→ P.124）
・「SNMP 設定」（→ P.125）
・「プライバシープロテクション設定」（→ P.127）
・「Proxy ARP 設定」（→ P.128）
・「無通信切断タイマー設定」（→ P.128）

□ 設定画面へのログイン制限設定

本製品の設定画面へのログインを制限するための設定に関する項目について説明します。



1 ポート番号 （初期値：80）

本製品にログインするためのポート番号を 1 ～ 65535 の範囲で指定します。通常は変更する必要はありません。

なお、次の番号は指定できません。

・67（DHCP サーバー）
・68（DHCP クライアント）
・123（NTP）
・161（SNMP）
・syslog 機能を有効に設定している場合は、「管理機能」画面の「syslog サーバー 1」、「syslog サーバー 2」の「ポート」に指定している番号
（「syslog 設定」（→ P.131）参照）

POINT

ポート番号を「80」以外に設定した場合

本製品のブラウザ設定画面を開始するときに、ポート番号の指定が必要になります。Web ブラウザのアドレス入力欄に、次のように本製品の IP アドレスとポート番号を半角コロン（:）で区切って指定します。

http://[本製品の IP アドレス]:[ポート番号]/

本製品の IP アドレスが「192.168.2.2」、ポート番号が「88」の場合は、「http://192.168.2.2:88/」と入力します。

2 無線 LAN からのログイン （初期値：許可）

本製品のブラウザ設定画面に、無線 LAN 端末からログインできるようにするかどうかを設定します。

・許可
無線 LAN 端末からログインできるようにする場合は、「許可」をクリックして◉にします。

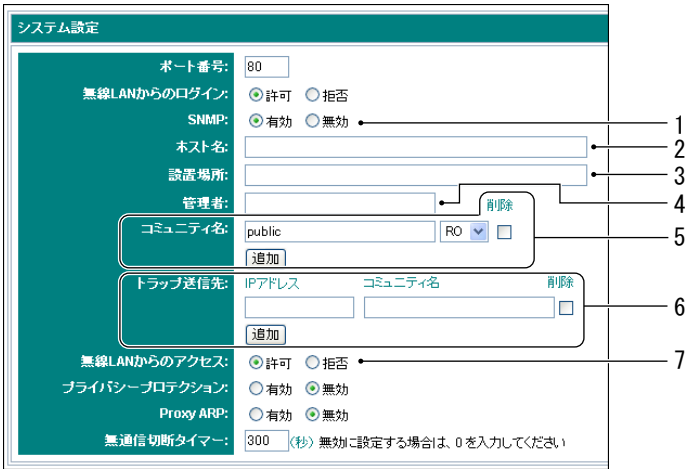
・拒否
無線 LAN 端末からログインできないようにする場合は、「拒否」をクリックして◉にします。

□ SNMP 設定

SNMP エージェント機能に関する項目について説明します。
SNMP 機能の概要については、「SNMP ／ MIB 対応」（→ P.35）をご覧ください。
本製品がサポートする MIB 情報とトラップの内容については、「MIB 情報一覧」（→ P.206）をご覧ください。

POINT

・本製品の SNMP エージェント機能を利用して本製品の MIB 情報を取得するためには、管理サーバーとなるパソコンに SNMP マネージャと呼ばれるソフトウェアをインストールする必要があります。



1 SNMP （初期値：無効）

SNMP エージェント機能を使用するかどうかを選択します。

・有効
SNMP エージェント機能を使用する場合は、「有効」をクリックして◉にし、次の 2 ～ 7 の設定を行います。

・無効
SNMP エージェント機能を使用しない場合は、「無効」をクリックして◉にします。

2 ホスト名 （初期値：なし）

ホスト名（オブジェクト名：sysName）を設定します。
任意の文字列を、半角英数字、および半角記号 64 文字以内で入力します。全角文字や、半角カタカナは使用できません。通常、FQDN（Fully-Qualified Domain Name）を記述します。

3 設置場所 （初期値：なし）

設置場所（オブジェクト名：sysLocation）を設定します。

任意の文字列を、半角英数字、および半角記号 64 文字以内で入力します。全角文字や、半角カタカナは使用できません。

4 管理者 （初期値：なし）

管理者名（オブジェクト名：sysContact）を設定します。

任意の文字列を、半角英数字、および半角記号 32 文字以内で入力します。全角文字や、半角カタカナは使用できません。

5 コミュニティ名 （初期値：public）

POINT

・同じコミュニティ名を複数設定した場合、一番下に設定されたものが有効になります。

表：「コミュニティ名」の詳細項目と説明

詳細項目	説明
テキストボックス	コミュニティ名を入力します。コミュニティ名は、SNMP が管理するネットワークの名前です。管理する側のマネージャと同じ名前を設定します。半角英数字、および半角記号（ただし半角のシャープ「#」、およびスペースは除く）32 文字以内で入力します。アルファベットの大文字・小文字を区別します。全角文字や、半角カタカナは使用できません。
RO ／ RW	をクリックしてMIB情報に対するアクセス権の種類を選択します。 「RO」（Read-Only）を選択すると、コミュニティ内のマネージャから MIB 情報の取得を行うことができます。 「RW」（Read-Write）を選択すると、コミュニティ内のマネージャから MIB 情報の取得と変更を行うことができます。
削除	登録済みのコミュニティ名を削除する場合は、「削除」をクリックして にします。
「追加」ボタン	複数のコミュニティを登録する場合、「追加」ボタンをクリックします。新しいテキストボックスが追加されるので、必要な項目を入力します。最大 8 件まで登録できます。

6 トラップ送信先

トラップを設定する場合、次のように設定します。

POINT

・トラップ送信先に同じ IP アドレスを複数設定した場合、一番下に設定されたものが有効になります。

表：トラップ送信先の詳細項目と説明

詳細項目	説明
IP アドレス	トラップを送信する SNMP マネージャの IP アドレスを指定します。
コミュニティ名	トラップ送信先のコミュニティ名を入力します。任意の文字列を、半角英数字、および半角記号（ただし半角のシャープ「#」、およびスペースは除く）32 文字以内で入力します。アルファベットの大文字、小文字を区別します。全角文字や、半角カタカナは使用できません。初期値は設定されていません。
削除	登録済みのトラップ送信先を削除する場合は、「削除」をクリックして☑にします。
「追加」ボタン	複数のトラップ送信先を登録する場合、「追加」ボタンをクリックします。新しいテキストボックスが追加されるので、必要な項目を入力します。最大 8 件まで登録できます。

7 無線 LAN からのアクセス （初期値：許可）

無線 LAN 端末から、本製品に SNMP アクセスをできるようにするかどうかを設定します。

・許可

無線 LAN 端末から本製品に SNMP アクセスできるようにする場合は、「許可」をクリックして◉にします。

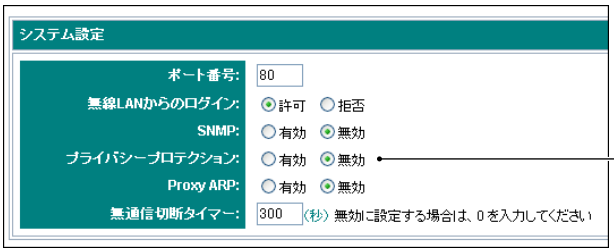
・拒否

無線 LAN 端末から本製品に SNMP アクセスできないようにする場合は、「拒否」をクリックして◉にします。

□ プライバシープロテクション設定

本製品に接続する無線 LAN 端末どうしの通信を許可するかどうかを設定します。

プライバシープロテクション機能の概要については、「プライバシープロテクション」（→ P.33）をご覧ください。



1 プライバシープロテクション （初期値：無効）

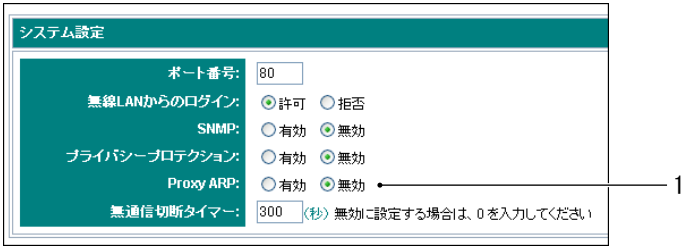
・有効

本製品を介した無線 LAN 端末間の通信を不可にする場合は、クリックして◉にします。

・無効
本製品を介した無線 LAN 端末間の通信を可能にする場合は、クリックして◉にします。

☐ Proxy ARP 設定

Proxy ARP 機能を使用するかどうかを設定します。
Proxy ARP 機能の概要については、「Proxy ARP」（→ P.32）をご覧ください。



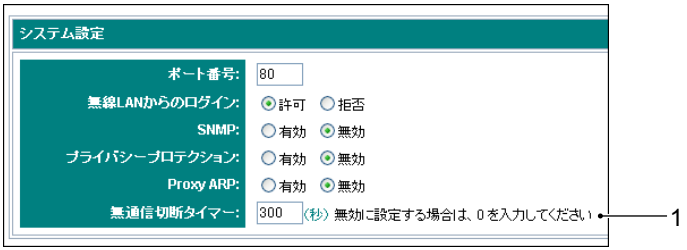
1 Proxy ARP （初期値：無効）

・有効
Proxy ARP 機能を使用する場合は、「有効」をクリックして◉にします。

・無効
Proxy ARP 機能を使用しない場合は、「無効」をクリックして◉にします。

☐ 無通信切断タイマー設定

本製品に接続している無線 LAN 端末が通信を行わない状態が続いた場合は、本製品からの接続を切断します。接続を切断するまでの時間を設定します。



1 無通信切断タイマー （初期値：300）

接続中の無線 LAN 端末が通信を行わなくなってから、接続を切断するまでの時間を、0、または 30 ～ 86400（秒）の範囲で指定します。通常は変更する必要はありません。「0」を設定すると、接続中の無線 LAN 端末が通信を行わなくても本製品から接続を切断しません。長時間、連続運用する場合や、接続する無線 LAN 端末が多い場合は、「0」を設定しないでください。

■「監視機能」カテゴリ

「監視機能」カテゴリでは、次の機能に関する設定が行えます。

・「AP 検出設定」（→ P.129）
・「syslog 設定」（→ P.131）
・「リンクインテグリティ設定」（→ P.134）

□ AP 検出設定

AP 検出機能では、無線電波をスキャンし、周辺の無線 LAN アクセスポイント情報を取得します。不正な無線 LAN アクセスポイントの設置などを検出することができます。
ただし、IEEE802.11a で J52（34、38、42、46 チャンネル）を使用している無線 LAN アクセスポイントは検出できません。

POINT

Dr.WLAPPer の監視機能

Dr.WLAPPer では AP 検出機能を利用して、本製品の稼動状態を監視します。Dr.WLAPPer の監視機能については、「Dr.WLAPPer の機能について」（→ P.148）をご覧ください。

AP 検出機能に関する項目について説明します。

1 AP 検出

「スキャン結果の表示」ボタンをクリックすると「スキャン結果」画面が表示されます。スキャン結果画面については、「スキャン結果画面」（→ P.130）をご覧ください。

2 定期スキャン （初期値：無効）

定期的にスキャンを実行させるかどうかを選択します。定期スキャンを有効にすると、「スキャン間隔」で設定した時間内に全チャンネルのスキャンを 1 チャンネルずつ行い、全チャンネルのスキャン終了後にスキャン結果画面を自動的に更新します。

・有効
定期的にスキャンを実行させる場合は、「有効」をクリックして◉にし、「スキャン間隔」の設定を行います。

・無効
定期的にスキャンを実行させない場合は、「無効」をクリックして◉にします。

重要

・定期スキャン機能を有効に設定すると、すべての無線 LAN 端末は本製品に接続できなくなります。

3 スキャン間隔 （初期値：900）

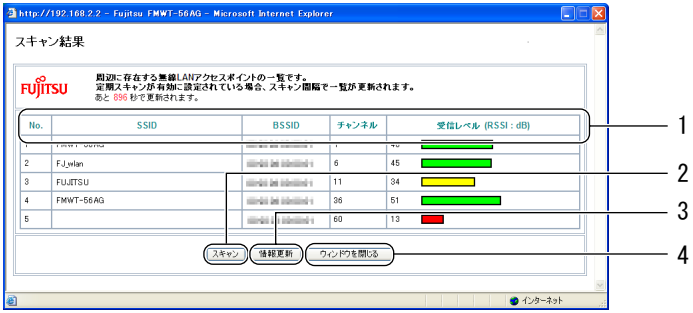
定期スキャンを実行させる間隔を、60 ～ 86400（秒）の範囲で指定します。通常は変更する必要はありません。

定期スキャンの結果は、「スキャン結果の表示」ボタンをクリックして表示されるスキャン結果画面で確認することができます。

スキャン結果画面

「定期スキャン」が有効の場合は、定期スキャンの際に検出した無線 LAN アクセスポイントの情報が表示されます。

また、スキャン結果画面で「スキャン」ボタンをクリックすると、その時点で行ったスキャンの結果が表示されます。



1 SSID ／ BSSID ／チャンネル／受信レベル（RSSI : dB）

スキャンを行った際に検出した無線 LAN アクセスポイントの SSID ／ BSSID ／チャンネル／受信レベル（RSSI : dB）の情報が表示されます。スキャンを行う本製品自体の情報は表示されません。

POINT

受信レベル（RSSI : dB）について

検出した無線 LAN アクセスポイントの受信レベル（RSSI）を、数値とバーの長さで示します。数値が大きい（バーが長い）無線 LAN アクセスポイントほど、受信レベルが高いことを意味しています。

バーの色は受信レベルの値により、0 ～ 20（dB）は赤、21 ～ 40（dB）は黄、41 ～ 100（dB）は緑で表示されます。

SSID の表示について

検出した無線 LAN アクセスポイントが SSID の隠蔽を有効にしている場合、SSID は表示されません。

2「スキャン」ボタン

「スキャン」ボタンをクリックすると全チャンネルのスキャンを行い、スキャン結果画面を更新します。

POINT

・無線 LAN 通信中に「スキャン」ボタンをクリックすると、本製品が全チャンネルのスキャンを行うため、少しの間通信できなくなります。

3 「情報更新」ボタン

「情報更新」ボタンをクリックすると、定期スキャンの最新の情報を表示します。スキャンは行いません。

4 「ウィンドウを閉じる」ボタン

「ウィンドウを閉じる」ボタンをクリックすると、スキャン結果画面を終了します。

□ syslog 設定

syslog 機能に関する項目について説明します。

syslog 機能の概要については、「syslog」（→ P.36）をご覧ください。

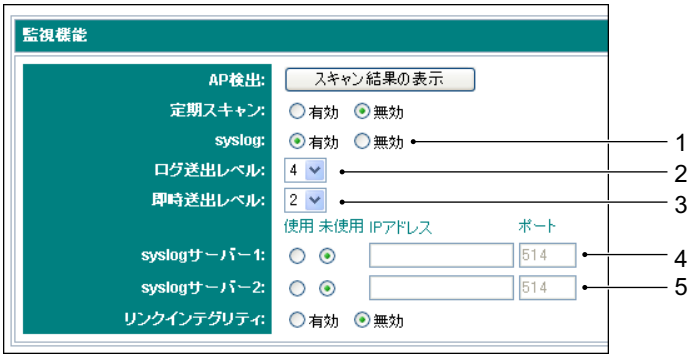
本製品の syslog のメッセージ一覧は、「syslog メッセージ一覧」（→ P.225）をご覧ください。

POINT

syslog の確認について

本製品で取得した syslog のログ情報は、syslog サーバー機能に対応したパソコンに送信して確認することができます。このため、ログ情報を確認するためには、syslog サーバー機能に対応したパソコンが必要になります。

パソコンを syslog 機能に対応させるには、syslog サーバーソフトウェアが必要です。



1 syslog （初期値：無効）

本製品の動作状態を監視してログを記録する syslog 機能を使用するかどうかを選択します。

・有効

syslog 機能を使用する場合は、「有効」をクリックして◉にし、次の 2 ～ 5 の設定を行います。

・無効

syslog 機能を使用しない場合は、「無効」をクリックして◉にします。

2 ログ送出レベル （初期値：4）

「syslog」の設定が有効のとき、表示される項目です。 をクリックして、syslog サーバーに通知するログのレベルを 0 ～ 7 の範囲で指定します。

「ログ送出レベル」が「4」、「即時送出レベル」が「2」の場合、送出レベルが 3 ～ 4 のログは本製品に 10 個蓄積された時点で通知します。ただし、10 個蓄積される前に送出レベル 0 ～ 2 のログが記録された場合には、そのログと同時に、その時点までに蓄積されたログを通知します。

3 即時送出レベル （初期値：2）

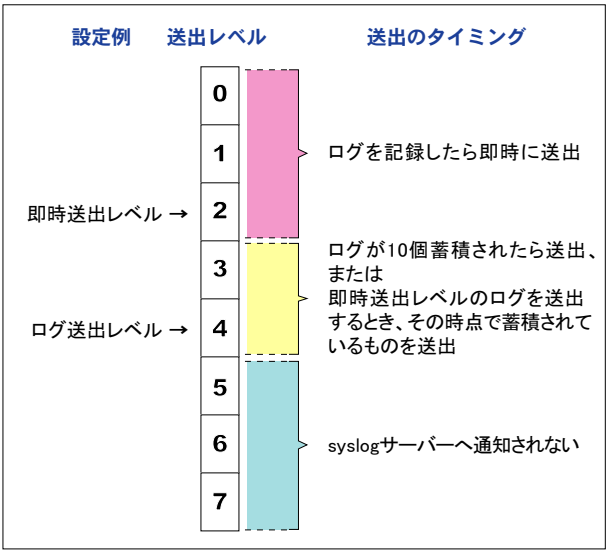
「syslog」の設定が有効のとき、表示される項目です。 をクリックして、syslog サーバーに即時に通知するログのレベルを 0 ～ 7 の範囲で指定します。

「即時送出レベル」が「2」の場合、送出レベル 0 ～ 2 のログが記録されると、即時に syslog サーバーに通知します。

POINT

「ログ送出レベル」と「即時送出レベル」の設定によるログの送出タイミングについて

「ログ送出レベル」を 4、「即時送出レベル」を 2 に設定した場合の、各レベルのログの送出タイミングを図で表すと、次のようになります。



4 syslog サーバー 1 （初期値：未使用）

本製品のログ情報を送信する syslog サーバーを設定します。

・使用

本製品のログ情報を指定するパソコンに送信する場合は、「使用」をクリックして◉にします。次の詳細項目を設定します。

表：「syslog サーバー」の詳細項目と説明

詳細項目	説明
IP アドレス	本製品のログ情報を送信するパソコンの IP アドレスを指定します。
ポート （初期値：514）	syslog で使用するポート番号を 1 ～ 65535 の範囲で指定します。 通常は変更する必要はありません。 なお、次のポート番号は使用できません。 ・67（DHCP サーバー） ・68（DHCP クライアント） ・123（NTP） ・161（SNMP） ・「管理機能」画面の「ポート番号」に指定している番号 （「設定画面へのログイン制限設定」（→ P.124）参照）

・未使用

本製品のログ情報をパソコンに送信しない場合は、「未使用」をクリックして◉にします。

5 syslog サーバー 2 （初期値：未使用）

・使用

syslog サーバー 1 以外の syslog サーバーがある場合は、「使用」をクリックして◉にし、「syslog サーバー 1」と同様に詳細項目を設定します。

・未使用

syslog サーバー 1 以外の syslog サーバーがない場合は、「未使用」をクリックして◉にします。

□ リンクインテグリティ設定

リンクインテグリティ機能に関する項目について説明します。
リンクインテグリティ機能の概要については、「リンクインテグリティ」（→ P.35）をご覧ください。

POINT

本機能により経路に異常が検知された場合の現象と対策

本機能により経路に異常が検知されると、本製品の無線電波が停止し、11g ランプと 11a ランプ（「各部の名称と働き」（→ P.20）参照）が消灯します。本製品の無線電波が停止した場合、経路の異常から回復すると、「診断間隔」に設定した時間の経過後に無線電波を再開します。

LAN ケーブルが接続されていない場合

リンクインテグリティ機能を有効にした場合、本製品の LAN コネクタに LAN ケーブルが接続されていないと、「診断時間」や「リトライ回数」の設定に関係なく、すぐに無線電波が停止します。

1 リンクインテグリティ （初期値：無効）

リンクインテグリティ機能を使用するかどうかを選択します。

・有効
リンクインテグリティ機能を使用する場合は、「有効」をクリックして◉にし、次の 2 ～ 4 の設定を行います。

・無効
リンクインテグリティ機能を使用しない場合は、「無効」をクリックして◉にします。

2 IP アドレス （初期値：なし）

監視する経路上にある機器の IP アドレスを入力します。3 つまで設定できます。

・「IP アドレス」に誤ったアドレスを設定すると、本製品の無線 LAN 通信が行えなくなります。十分注意して設定してください。

3 診断間隔 （初期値：60）

▼をクリックして、指定した有線 LAN 側経路を診断する間隔を 1 ～ 600（秒）の範囲で選択します。

4 リトライ回数 （初期値：2）

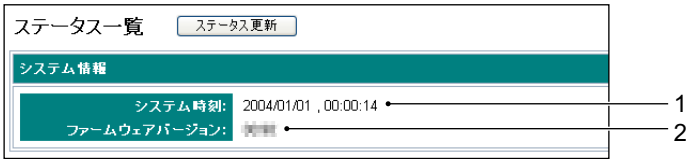
▼をクリックして、経路の異常を検知した場合に何回リトライを行うかを 0 ～ 5（回）の範囲で選択します。

2 ステータスの確認

本製品の状態や、無線 LAN 端末の接続状況などの確認について説明します。

本製品の設定内容や、無線 LAN 端末の接続状況などを確認する場合は、「ステータス一覧」メニューをクリックします。メインフレームに「ステータス一覧」画面が表示されます。「ステータス一覧」画面で確認できる項目について、カテゴリごとに説明します。

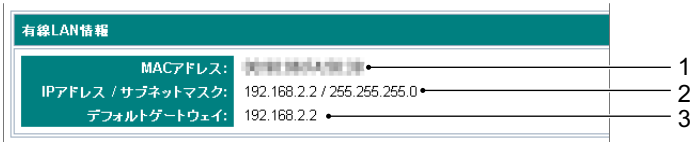
■「システム情報」カテゴリ



1 システム時刻
現在の時刻です。時刻の設定を行っていない場合は、正しい日付／時刻が表示されません。

2 ファームウェアバージョン
現在のファームウェアバージョンです。

■「有線 LAN 情報」カテゴリ



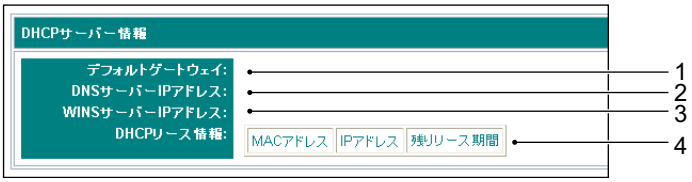
1 MAC アドレス
有線 LAN ポートの MAC アドレスです。

2 IP アドレス／サブネットマスク
有線 LAN ポートの IP アドレスとサブネットマスクです。

3 デフォルトゲートウェイ
有線 LAN ポートのデフォルトゲートウェイです。

■「DHCP サーバー情報」カテゴリ

「有線 LAN」画面の「DHCP サーバー機能」カテゴリー「サービス」が「有効」のときに表示されるカテゴリです。



1 デフォルトゲートウェイ

DHCP サーバー機能で使用するデフォルトゲートウェイです。

2 DNS サーバー IP アドレス

DHCP サーバー機能で使用する DNS サーバーの IP アドレスです。

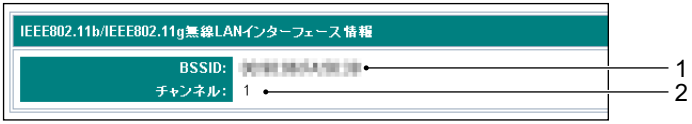
3 WINS サーバー IP アドレス

DHCP サーバー機能で使用する WINS サーバーの IP アドレスです。

4 DHCP リース情報

本製品に接続しているすべての DHCP クライアントの MAC アドレス、IP アドレスおよび残りリース期間が表示されます。

■「IEEE802.11b/IEEE802.11g 無線 LAN インターフェース情報」カテゴリ



1 BSSID

IEEE802.11b/IEEE802.11g無線LANインターフェースのMACアドレスが表示されます。

「11b/11g 停止中」と表示されている場合は、無線スイッチがオフに設定されている状態です。

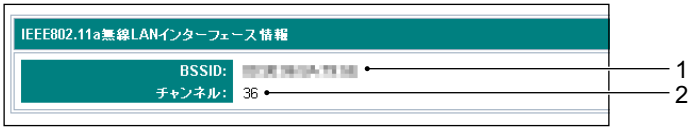
「経路異常発生中」と表示されている場合は、リンクインテグリティ機能により、無線電波を停止している状態です。

2 チャンネル

IEEE802.11b/IEEE802.11g 無線 LAN インターフェースが使用しているチャンネルが表示されます。

何も表示されていない場合は、無線スイッチがオフに設定されているか、またはリンクインテグリティ機能により無線電波を停止している状態です。

■「IEEE802.11a 無線 LAN インターフェース情報」カテゴリ



1 BSSID

IEEE802.11a 無線 LAN インターフェースの MAC アドレスが表示されます。

「11a 停止中」と表示されている場合は、無線スイッチがオフに設定されている状態です。

「経路異常発生中」と表示されている場合は、リンクインテグリティ機能により、無線電波を停止している状態です。

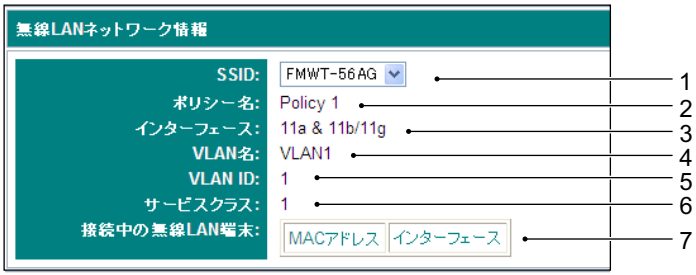
2 チャンネル

IEEE802.11a 無線 LAN インターフェースが使用しているチャンネルが表示されます。

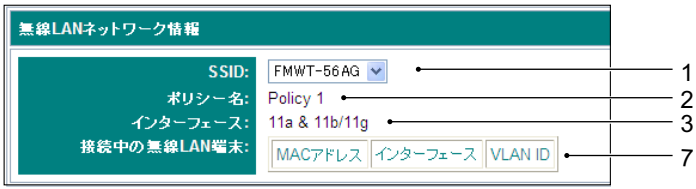
何も表示されていない場合は、無線スイッチをオフに設定しているか、またはリンクインテグリティ機能により無線電波を停止している状態です。

■「無線 LAN ネットワーク情報」カテゴリ

【通常VLANを選択しているときの画面】



【認証VLANを選択しているときの画面】



1 SSID

をクリックして、「無線 LAN ネットワーク情報」カテゴリに、どの SSID のステータスを表示するか選択します。

2 ポリシー名

選択した SSID のネットワークプロファイルに関連付けされているポリシー名が表示されます。

3 インターフェース

選択した SSID のネットワークプロファイルに関連付けされているインターフェースが以下の形式で表示されます。

・インターフェースで「両方」を指定している場合
11a & 11b/11g

・インターフェースで 11b/11g を指定している場合
11g/11b

・インターフェースで 11a を指定している場合
11a

4 VLAN 名

通常 VLAN を選択している場合に、選択した SSID のネットワークプロファイルに関連付けされている VLAN 名が表示されます。認証 VLAN を選択している場合、この項目は表示されません。

5 VLAN ID

通常 VLAN を選択している場合に、選択した SSID のネットワークプロファイルに関連付けされている VLAN 名に指定されている VLAN ID が表示されます。認証 VLAN を選択している場合、この項目は表示されません。

6 サービスクラス

通常 VLAN を選択している場合に、選択した SSID のネットワークプロファイルに関連付けされている VLAN 名に指定されているサービスクラスが表示されます。認証 VLAN を選択している場合、この項目は表示されません。

7 接続中の無線 LAN 端末

選択した SSID に接続中の無線 LAN 端末の MAC アドレスと、無線 LAN インターフェースが表示されます。無線 LAN インターフェースは、次のように表示されます。

・無線 LAN 端末が IEEE802.11b で接続している場合：11b
・無線 LAN 端末が IEEE802.11g で接続している場合：11g
・無線 LAN 端末が IEEE802.11a で接続している場合：11a

認証 VLAN を選択している場合は、インターフェースの横に VLAN ID が表示されます。無通信切断タイマー機能により本製品から接続を切断された無線 LAN 端末は、表示から削除されます。

POINT

本製品で WDS 機能をご利用の場合

本製品が WDS の親アクセスポイントに設定されている場合は、子アクセスポイントの BSSID が表示されます。

本製品が WDS の子アクセスポイントに設定されている場合は、親アクセスポイントの BSSID が表示されます。

3 システムのメンテナンス

本製品のメンテナンス機能について説明します。

再起動

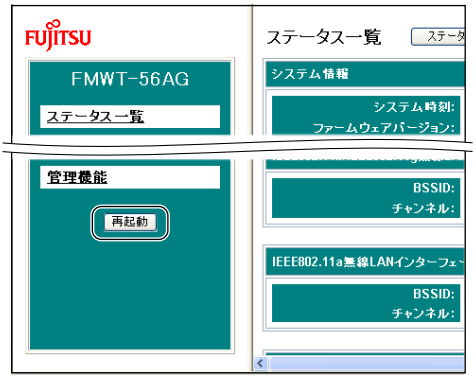
本製品に接続している端末で、正常にネットワーク通信が行えないなどの現象が発生した場合、本製品の動作が不安定になっている可能性があります。その場合は、本製品を再起動します。

POINT

・再起動が開始されると、管理者用パソコンは、本製品から切断されます。
再起動後、自動的に再接続しない場合は、しばらくしてから Web ブラウザを起動し直し、もう一度本製品にログインしてください。

本製品を再起動する手順は次のとおりです。

1 メニューフレームの「再起動」ボタンをクリックします。



再起動が開始され、「設定を保存しています。」という画面が表示されます。

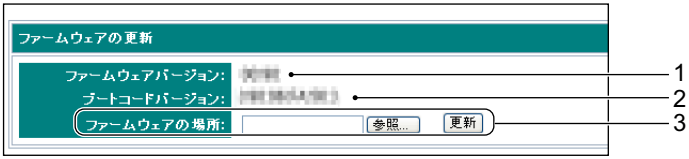
重要

・「設定を保存しています。」という画面の表示中は、絶対に本製品の電源を切らないでください。

Web ブラウザで「設定を保存しています。」という画面が終了すると、再起動が完了します。

ファームウェアの更新

本製品の機能を向上させるため、バージョンアップ用のファームウェアが提供される場合があります。ファームウェアの更新は、「管理機能」メニューの「ファームウェアの更新」カテゴリで行います。
「ファームウェアの更新」カテゴリには、次の項目があります。



1 ファームウェアバージョン
現在のファームウェアバージョンが表示されます。

2 ブートコードバージョン
現在のブートコードバージョンが表示されます。

3 ファームウェアの場所
バージョンアップ用のファームウェアファイルへのパスを指定して、ファームウェアを更新します。ファームウェアの更新手順や注意事項については、「ファームウェアの更新手順」（→ P.140）をご覧ください。

■ファームウェアの更新手順

□ ファームウェアの更新について

・ファームウェアの最新版は、富士通パソコン情報サイト FMWORLD.NET の次の URL でご提供する予定です。
URL：http://www.fmworld.net/biz/
現在、本製品で使用しているファームウェアより新しいバージョンであることを確認して、ダウンロードしてください。ダウンロードの方法は、ダウンロードのサイトでご確認ください。
・本製品のファームウェアをダウンロードするときに、Readme.txt などが添付されている場合は、ファームウェアの更新を行う前に必ずお読みください。
・ファームウェアを更新しても、本製品の設定内容は保存されます。ただし、機能変更があると設定が消去されてしまう可能性もありますので、更新を行う前にファームウェアに添付の Readme.txt などで必ず確認してください。

□ ファームウェアの更新手順

POINT

・ファームウェアの更新が開始されると、管理者用パソコンは本製品から切断されます。ファームウェアの更新完了後、自動的に再接続しない場合は、しばらくしてから Web ブラウザを起動し直し、もう一度本製品にログインしてください。

1 **本製品の DC コネクタから AC アダプタを抜いて電源を切り、再度 AC アダプタを接続して電源を入れます。**

2 **Web ブラウザを起動し、本製品の設定画面にログインします。**
ログインの方法は、「開始」（→ P.60）をご覧ください。

3 **メニューフレームの「管理機能」メニューをクリックします。**
メインフレームに「管理機能」画面が表示されます。

4 **「ファームウェアの場所」の「参照」ボタンをクリックします。**

「参照」ボタンをクリックした後は、次の手順を参考にして、実際に画面に表示されるメッセージなどを確認して、ファームウェアファイルを選択してください。

5 **「ファイルの選択」ウィンドウで、ダウンロードしたファームウェアファイルへのパスを選択して、「開く」をクリックします。**

POINT

・ファームウェアのファイルの種類は「.bin」です。

「ファームウェアの場所」に、選択したファームウェアのファイルへのパスが表示されます。

6 **「更新」ボタンをクリックします。**

POINT

エラーメッセージが表示された場合
選択したファイルの種類が、ファームウェアのファイルと異なります。ダウンロードしたファームウェアのファイルを選択してください。

7 **確認のメッセージが表示されたら、「OK」をクリックします。**
ファームウェアの更新が開始されます。

重要

更新中は次の点に十分ご注意ください
確認のメッセージの画面で「OK」をクリックすると、「ファームウェアを更新しています」という画面が表示されます。「ファームウェアを更新しています」という画面が終了するまで、絶対に本製品の電源を切ったり、パソコンの操作を行ったりしないでください。本製品が動作しなくなる場合があります。

ブラウザ設定画面で「ファームウェアを更新しています」という画面が終了すると、ファームウェアの更新が完了します。

8 **ファームウェアの更新が完了したら、Web ブラウザの ✕ をクリックして Web ブラウザを閉じます。**

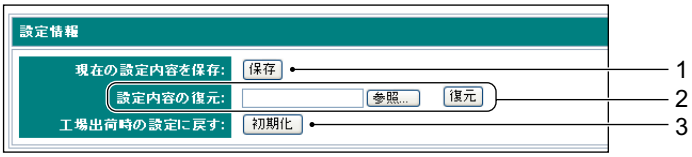
9 **再度 Web ブラウザを起動し、本製品の設定画面にログインします。**
ログインの方法は、「開始」（→ P.60）をご覧ください。

10 **メニューフレームの「管理機能」メニューをクリックします。**
メインフレームに「管理機能」画面が表示されます。

11 **「ファームウェアバージョン」に表示されているバージョンが、更新したファームウェアのバージョンになっていることを確認します。**

設定情報（保存／復元／初期化）

本製品は、設定情報を保存、復元したり、設定内容をご購入時の設定に戻したりすることができます。設定情報に関する設定は、「管理機能」メニューの「設定情報」カテゴリで行います。
「設定情報」カテゴリには、次の項目があります。



1 **現在の設定内容を保存**
現在の設定内容を保存します。設定内容の保存の手順については、「設定内容の保存」（→ P.142）をご覧ください。

2 **設定内容の復元**
保存した設定内容を復元します。設定内容の復元の手順については、「設定内容の復元」（→ P.143）をご覧ください。

3 **工場出荷時の設定に戻す**
設定内容を、すべてご購入時の設定に戻します。ご購入時の設定に戻す手順については、「初期化」（→ P.145）をご覧ください。

■設定内容の保存

POINT

設定内容を複数台の本製品にコピーしたい場合
Dr.WLAPPer をお使いになると、1 台の本製品の設定内容を、グループ単位で複数台の本製品に設定することができます。詳しくは、「Dr.WLAPPer を利用した設定」（→ P.160）をご覧ください。

1 **保存する設定内容を確認します。**

次の項目は、設定内容を復元するときに必要です。わからなくなると、ここで保存した設定内容を復元するときに、本製品にログインできなくなります。必ず確認し、設定を保存するときのファイル名と一緒にメモしておいてください。

・「管理機能」画面の「アカウント設定」カテゴリー「管理者ユーザー名」
・「管理機能」画面の「アカウント設定」カテゴリー「管理者パスワード」
・「管理機能」画面の「システム設定」カテゴリー「ポート番号」

2 **メニューフレームの「管理機能」メニューをクリックします。**

メインフレームに「管理機能」画面が表示されます。

3 **「設定情報」カテゴリー「現在の設定内容を保存」の「保存」ボタンをクリックします。**

「保存」ボタンをクリックした後は、以降の手順を参考に、実際に画面に表示されるメッセージなどを確認して、ファイルを保存してください。

4 **「ファイルのダウンロード」ウィンドウで、「保存」をクリックします。**

画面の指示に従って、設定内容を保存するファイル名と保存場所を指定し、ファイルを保存します。

POINT

・ここで保存したファイルは、設定内容を復元するときに使用します。わかりやすい名前、場所で保存してください。また、手順 1 で確認した、ユーザー名、パスワード、ポート番号と一緒に必ずメモしておいてください。
・ファイルの種類は「.conf」になります。変更しないでください。

■設定内容の復元

重要

・設定内容を復元すると、IP アドレスなどネットワークに関する設定も復元する設定ファイルの内容に従って設定されるため、復元後に本製品にアクセスできなくなる場合があります。設定内容の復元後、必要に応じて IP アドレスなどの設定を修正してください。

□ 設定内容の復元手順

1 **本製品を再起動します。**

再起動の手順については、「再起動」（→ P.139）をご覧ください。

2 **メニューフレームの「管理機能」メニューをクリックします。**
メインフレームに「管理機能」画面が表示されます。

3 **「設定情報」カテゴリー「設定内容の復元」の「参照」ボタンをクリックします。**

「参照」ボタンをクリックした後は、次の手順を参考にして、実際に画面に表示されるメッセージなどを確認して、ファイルを選択してください。

4 **「ファイルの選択」ウィンドウで、「設定内容の保存」（→ P.142）で保存したファイルを選択して、「開く」をクリックします。**

POINT

・設定内容のファイルの種類は「.conf」です。

「設定内容の復元」に、選択した設定内容のファイルへのパスが表示されます。

5 **「復元」ボタンをクリックします。**
確認のメッセージが表示されたら、「OK」をクリックします。

POINT

エラーメッセージが表示された場合
選択したファイルの種類が、設定内容を保存したファイルと異なります。「設定内容の保存」（→ P.142）で保存した、「（ファイル名）.conf」ファイルを選択してください。

「設定内容の復元に成功しました。」という画面が表示されます。

6 **画面の内容を確認します。**
表示されている内容は、本製品の設定画面にログインするときに必要な情報です。わからなくなると本製品にログインできなくなるため、必ず確認してください。

7 **「戻る」ボタンをクリックします。**
復元した内容が設定画面に反映されます。
この状態では、本体に設定内容は反映されていません。続けて次の手順を行います。

8 **本製品を再起動します。**
再起動の手順については、「再起動」（→ P.139）をご覧ください。
「設定を保存しています。」という画面が終了すると、復元した設定内容が反映されます。

POINT

・「設定を保存しています。」という画面の表示中に、ログイン画面が表示された場合は、復元する設定内容のユーザー名／パスワードを入力してください。

復元する設定内容のユーザー名／パスワードを忘れた場合、設定内容を復元できません。ログイン画面で「キャンセル」をクリックしてください。
その後、本製品の設定内容をご購入時の状態に戻します。詳しくは「IP アドレス、ユーザー名、パスワードを忘れてログインできない」（→ P.187）をご覧ください。

■初期化

1 「設定情報」カテゴリー－「工場出荷時の設定に戻す」の「初期化」ボタンをクリックします。

2 確認のメッセージが表示されたら、「OK」をクリックします。
「設定を保存しています。」という画面が表示されます。

重要

- 「設定を保存しています。」という画面の表示中は、絶対に本製品の電源を切らないでください。

「設定を保存しています。」という画面が終了すると、本製品の設定内容がご購入時の状態に戻ります。

パスワードの忘却などにより設定画面にログインできない場合は、LOAD DEFAULT ボタンを使用して本製品の設定をご購入時の状態に戻します。詳しくは、「初期化（LOAD DEFAULT ボタン）」（→ P.176）をご覧ください。

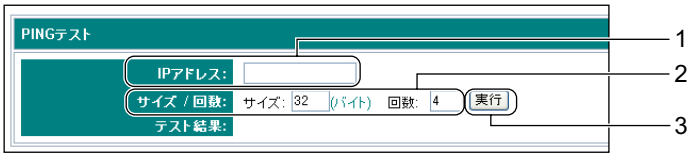
PING テスト

本製品から、パソコンやネットワーク上の機器に対して接続確認を行うことができます。本製品からの接続確認は、「管理機能」メニューの「PING テスト」カテゴリで行います。

POINT

- パソコンから本製品に対して接続確認を行う方法については、「パソコンからの接続確認」（→ P.184）をご覧ください。

1 次のように操作します。



1. 「PING テスト」カテゴリの「IP アドレス」に、接続確認相手の IP アドレスを入力します。
2. 「サイズ / 回数」に、接続確認用のパケットサイズと回数を入力します。
   通常は変更する必要はありません。変更する場合は、次の範囲で入力します。
   ・サイズ （初期値：32）
   PING パケットのデータサイズを、8 ～ 6400（バイト）の範囲で入力します。
   ・回数 （初期値：4）
   PING テストを実行する回数を、1 ～ 999（回）の範囲で入力します。
3. 「実行」ボタンをクリックします。

2 **確認の画面が表示されたら、「OK」をクリックします。**
PING テストが完了すると、「テスト結果」に結果が表示されます。

3 **PING テストの結果を確認します。**
「テストの結果」に表示される結果と意味は、次のとおりです。

表：PING テストの結果と意味

	テスト結果の表示例	結果の意味
例 1	4 packets transmitted, 4 received, 0% loss, time ・・・	接続確認は成功です。
例 2	192.168.2.10 is alive	接続確認は成功です（192.168.2.10 は接続確認相手の IP アドレスです）。
例 3	no answer from ・・・	接続確認は失敗です。

6

第 6 章

Dr.WLAPPer（ドクターラッパー）の使い方

Dr.WLAPPer は無線 LAN アクセスポイントの管理ツールで、一括管理機能などをサポートします。Dr.WLAPPer の使い方を説明します。

1 Dr.WLAPPer をお使いになる前に

Dr.WLAPPer をお使いになるために知っておいていただきたい内容を説明します。

POINT

・Dr.WLAPPer の最新版は、富士通パソコン情報サイト FMWORLD.NET の次の URL でご提供する予定です。
URL：http://www.fmworld.net/biz/

Dr.WLAPPer の機能について

Dr.WLAPPer は、無線 LAN アクセスポイントの一括管理／監視を行うことができるツールです。次の無線 LAN アクセスポイントを管理することができます。

・ワイヤレス LAN ステーション FMWT-56AG（本製品）
・ワイヤレス LAN ステーション FMWT-55AG
・ワイヤレス LAN ステーション FMWT-54AG

Dr.WLAPPer の機能について説明します。

□ 管理機能

・グループ化／メンテナンス
複数のグループを作成することにより、グループごとに無線 LAN アクセスポイントを管理することができるようになります。企業などのネットワークで、部署ごと、ビルのフロアごとなど、共通の設定を使用する単位でグループを作成しておくと、設定やメンテナンスを効率よく行えます。
グループ化について詳しくは、「登録」（→ P.157）をご覧ください。
メンテナンスについて詳しくは、「Dr.WLAPPer を利用したメンテナンス」（→ P.163）をご覧ください。

・稼動状況の確認
メイン画面で、無線 LAN アクセスポイントの稼動状況をグループごとに一覧したり（「稼動情報ビュー」）、無線 LAN 端末の接続状況を確認したり（「詳細ビュー」）できます。
詳しくは、「Dr.WLAPPer メイン画面の見方」（→ P.151）をご覧ください。

・設定
ネットワーク上にある無線 LAN アクセスポイントから設定内容を読み込み、グループ単位で一括して設定をコピーできます。また用途に合わせて変更した内容で、一括設定することもできます。一括設定を行うことにより、同一部署内の複数の無線 LAN アクセスポイントに設定する場合などに、設定もれなどの心配がありません。
またスケジューリング機能により、任意の時間（2 日後まで）に設定の反映を行うことができます。無線 LAN 端末が通信を行っていない時間帯を指定しておけば、業務に支障がないよう設定作業を行うことができます。
詳しくは、「Dr.WLAPPer を利用した設定」（→ P.160）をご覧ください。

POINT

複数台の管理に関するご注意

・ファームウェアバージョンが異なる無線 LAN アクセスポイントが混在している場合に行える一括処理は、次のとおりです。
  ・「表示」メニューの「最新の情報に更新」
  ・「管理」メニューの「再起動」
  ・「管理」メニューの「ファームウェア更新」
・ファームウェアバージョンが異なる無線 LAN アクセスポイントを複数選択した場合、設定の一括変更を行うことはできません。また、同一グループ内にファームウェアバージョンが異なる無線 LAN アクセスポイントが混在している場合に、そのグループを選択して設定の一括変更を行うこともできません。
  一括設定を行う場合は、対象となる無線 LAN アクセスポイントのファームウェアのバージョンをすべて同じにしてください。
  ファームウェアのバージョンをすべて同じにできない場合は、個々に設定を行ってください。
・古いバージョンのファームウェアを搭載した無線 LAN アクセスポイントを選択した場合、新しいバージョンのファームウェアで追加された項目は、「設定の変更」ウィンドウでグレイアウト表示になります。

□ 監視機能

・不正無線 LAN アクセスポイント検出／監視
  周辺無線 LAN アクセスポイント検出機能を利用して、Dr.WLAPPer が管理している無線 LAN アクセスポイント以外の無線機器を、不正な無線 LAN アクセスポイントとして検出／監視することができます。
・無線 LAN アクセスポイントの無線部状態監視
  管理対象の無線 LAN アクセスポイントが 3 台以上設置されている環境では、Dr.WLAPPer は周辺無線 LAN アクセスポイント検出機能を利用して、お互いの無線状態を監視し合うことで、無線が正しく動作しているかどうかを監視することができます。

監視機能の使用方法については、「Dr.WLAPPer の監視機能」（→ P.166）をご覧ください。

インストールと開始／終了

Dr.WLAPPer のインストール方法、および開始と終了方法について説明します。

POINT

・Dr.WLAPPer のインストール、および開始を行うには、OS に管理者権限でログインしている必要があります。

■ Dr.WLAPPer のインストール

Dr.WLAPPer は、管理者用パソコンにインストールして使用します。インストール方法を説明します。

1 本製品に添付の CD-ROM を、パソコンにセットします。

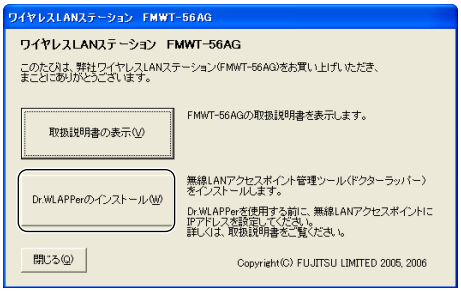
「ワイヤレス LAN ステーション FMWT-56AG」ウィンドウが表示されます。

POINT

「ワイヤレス LAN ステーション FMWT-56AG」ウィンドウが表示されない場合

エクスプローラを起動して、CD-ROM 内の「Autorun」をクリックします。

2 「Dr.WLAPPer のインストール」をクリックします。



画面の指示に従ってインストールを行ってください。
インストール終了後、画面の指示に従ってパソコンを再起動してください。

POINT

- Dr.WLAPPer をインストールすると、Dr.WLAPPer Monitor サービスにより syslog のポート（UDP ポート 514）が常に使用される状態になります。
  Dr.WLAPPer をインストールする管理者用パソコンで syslog サーバーソフトウェアを併用しているなど、他のプログラムでポート番号 514 を使用する場合は、Dr.WLAPPer の監視機能の設定で「syslog サーバー 1」の「ポート」の設定を変更する必要があります。監視機能の設定について詳しくは、「監視の設定」（→ P.166）をご覧ください。
- Dr.WLAPPer インストール後、パソコンを再起動すると、画面右下の通知領域に Dr.WLAPPer 監視ツールのアイコン（ ）が表示されます。このアイコンから Dr.WLAPPer を起動することはできません。Dr.WLAPPer 監視ツールについては、「Dr.WLAPPer の監視機能」（→ P.166）をご覧ください。

■開始

次の手順で、「Dr.WLAPPer」を開始します。

POINT

- Dr.WLAPPer を使用する場合の注意事項については、「設定時のご注意」（→ P.54）をご覧ください。
- 本バージョンの Dr.WLAPPer をインストール後、最初の起動時にメッセージ画面が表示されますので内容を確認して「OK」をクリックしてください。
  旧バージョンの Dr.WLAPPer をアップデートした場合は、最初の起動時にすべての無線 LAN アクセスポイントの情報を取得し直す必要があります。すべてのグループに対して、「表示」メニュー→「最新の情報に更新」を行ってください。

1 **「スタート」ボタン→「すべてのプログラム」（または「プログラム」）→「FUJITSU」→「Dr.WLAPPer」→「Dr.WLAPPer」の順にクリックします。**

Dr.WLAPPer メイン画面が表示されます。

画面の見方については、「Dr.WLAPPer メイン画面の見方」（→ P.151）をご覧ください。

■終了

次のいずれかの手順で Dr.WLAPPer メイン画面を終了します。

・Dr.WLAPPer メイン画面の をクリックします。

・「ファイル」メニュー→「終了」の順にクリックします。

POINT

Dr.WLAPPer 監視ツールを起動している場合

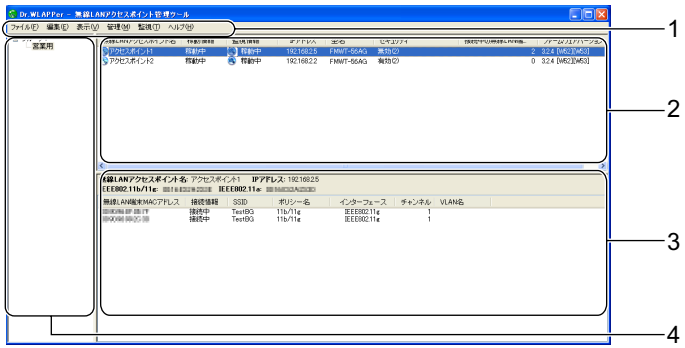
Dr.WLAPPer のメイン画面を終了しても、監視ツールは終了しません。監視ツールの終了については、「終了」（→ P.168）をご覧ください。

Dr.WLAPPer メイン画面の見方

Dr.WLAPPer メイン画面の画面構成と、表示される項目などについて説明します。

■Dr.WLAPPer メイン画面

Dr.WLAPPer のメイン画面です。



1 メニュー

「ファイル」メニュー、「編集」メニュー、「表示」メニュー、「管理」メニュー、「監視」メニュー、「ヘルプ」メニューがあります。詳しくは、「メニュー詳細」（→ P.152）をご覧ください。

2 稼動情報ビュー

ツリービューで選択したグループの無線LANアクセスポイントの稼動情報を表示します。

稼動情報ビューの詳細は、「稼動情報ビュー」（→ P.153）をご覧ください。

3 詳細ビュー

稼動情報ビューで選択した無線 LAN アクセスポイントの詳細情報と、無線 LAN 端末の接続状況が表示されます。

詳細ビューの詳細は、「詳細ビュー」（→ P.155）をご覧ください。

4 ツリービュー

登録したグループがツリー状で表示されます。グループについては「グループの作成／グループ名の変更」（→ P.157）をご覧ください。

□ メニュー詳細

「ファイル」メニュー

「ファイル」メニューでは、「無線 LAN アクセスポイント登録」、「グループ作成」、「終了」が選択できます。

・無線 LAN アクセスポイント登録
無線 LAN アクセスポイントを新規に登録します。詳しくは「登録」（→ P.157）をご覧ください。

・グループ作成
グループを新規に作成します。詳しくは「登録」（→ P.157）をご覧ください。

・終了
Dr.WLAPPer を終了します。詳しくは「インストールと開始／終了」（→ P.149）をご覧ください。

「編集」メニュー

「編集」メニューでは、「設定の変更」、「削除」、「グループ名の変更」、「登録情報の変更」が選択できます。

・設定の変更
選択した無線 LAN アクセスポイントの設定を変更します。詳しくは「Dr.WLAPPer を利用した設定」（→ P.160）をご覧ください。

・削除
選択した無線 LAN アクセスポイントまたは、選択したグループおよびその配下のすべて（グループ、無線 LAN アクセスポイント）を削除します。

・グループ名の変更
選択したグループのグループ名を変更します。詳しくは「登録」（→ P.157）をご覧ください。

・登録情報の変更
「無線 LAN アクセスポイントの登録」で登録した情報の変更を行います。詳しくは「登録」（→ P.157）をご覧ください。

「表示」メニュー

「表示」メニューでは、「最新の情報に更新」が選択できます。

・最新の情報に更新
稼動情報ビュー、詳細ビューに表示されている無線 LAN アクセスポイントの内容を最新の情報に更新します。

「管理」メニュー

「管理」メニューでは、「再起動」、「ファームウェア更新」が選択できます。

・再起動
選択した無線 LAN アクセスポイントを再起動します。詳しくは「Dr.WLAPPer を利用したメンテナンス」（→ P.163）をご覧ください。

・ファームウェア更新
選択した無線 LAN アクセスポイントのファームウェア更新を行います。詳しくは「Dr.WLAPPer を利用したメンテナンス」（→ P.163）をご覧ください。

「監視」メニュー

「監視」メニューでは、「監視一括設定」、「監視ツールの表示」が選択できます。

・監視一括設定
選択したグループに登録されている無線LANアクセスポイントに対して監視設定を行います。詳しくは「監視の設定」（→ P.166）をご覧ください。

・監視ツールの表示
Dr.WLAPPer 監視ツールを表示します。Dr.WLAPPer 監視ツールの使い方については、「Dr.WLAPPer 監視ツールの使い方」（→ P.169）をご覧ください。

「ヘルプ」メニュー

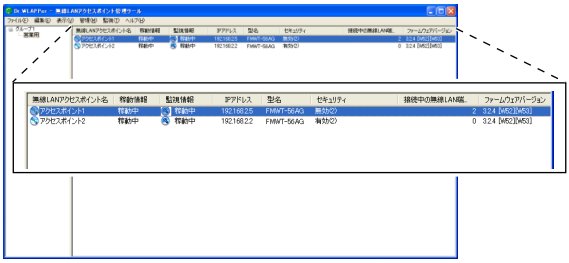
「ヘルプ」メニューでは、「マニュアル」、「バージョン情報」が選択できます。

・マニュアル
ワイヤレス LAN ステーションの取扱説明書が表示されます。

・バージョン情報
Dr.WLAPPer のバージョン情報が表示されます。

■稼動情報ビュー

稼動情報ビューには、ツリービューで選択したグループに登録されている本製品について、次の情報が表示されます。



・無線 LAN アクセスポイント名
登録時に設定した無線 LAN アクセスポイント名と、稼動情報アイコンが表示されます。

・稼動情報
無線 LAN アクセスポイントの稼動状況が表示されます。それぞれ次の状態を示します。

- 稼動中
  正常に動作しています。
- 未稼動
  動作していないか、または応答がありません。

POINT

稼動中の無線 LAN アクセスポイントが「未稼動」と表示される場合

稼動中の無線 LAN アクセスポイントが「未稼動」と表示される場合は、その無線 LAN アクセスポイントを選択して、「表示」メニュー→「最新の情報に更新」の順にクリックしてください。
次のような場合に「未稼動」と表示されることがあります。
・ネットワーク負荷が高いなどの原因で、パケットの取りこぼしが発生したとき
・無線 LAN アクセスポイントの設定を変更したとき（変更した項目により、再起動に時間がかかる場合があります。）

- 取得不可
  次のいずれかの理由で情報を取得できません。
  ・無線 LAN アクセスポイントのファームウェアが Dr.WLAPPer で未対応のバージョン
  ・ログインに失敗
  ・対象外の無線 LAN アクセスポイント
- 情報取得中
  情報取得処理中
- 情報未取得
  まだ情報を取得していません。

・監視情報
監視機能を使用している場合、本製品の無線部の稼動状況が表示されます。
- 稼動中
  正常に動作しています。
- 故障の疑い
  故障の可能性があります。一時的に監視情報が取得できなかった可能性もあります。
- 故障
  故障しています。
- 未稼動
  監視をしていないか、まだ監視情報を取得していません。

・IP アドレス
無線 LAN アクセスポイントの IP アドレスが表示されます。

・型名
無線 LAN アクセスポイントの型名が表示されます。

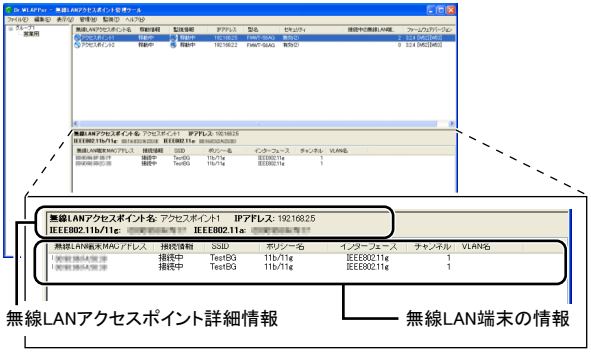
・セキュリティ
セキュリティの設定について、有効か無効かが表示されます。ネットワークプロファイルが複数設定されている場合は、「有効（x)、無効（x)」などと表示されます。

・接続中の無線 LAN 端末数
接続している無線 LAN 端末の数が表示されます。複数のネットワークプロファイルが設定されている場合は、すべてのプロファイルで接続している無線 LAN 端末の合計です。

・ファームウェアバージョン
無線 LAN アクセスポイントのファームウェアのバージョンと、対応している周波数帯が表示されます。

■詳細ビュー

詳細ビューには、稼動情報ビューで選択した無線 LAN アクセスポイントの詳細情報と無線 LAN 端末の接続状況について、次の情報が表示されます。



□ 無線 LAN アクセスポイント詳細情報

・無線 LAN アクセスポイント名
・IP アドレス
・IEEE802.11b/11g（[BSSID]）
IEEE802.11b/IEEE802.11g の BSSID（MAC アドレス）が表示されます。
無線スイッチが「オフ」の場合は、「停止中」と表示されます。
リンクインテグリティ機能によって電波が停止している場合は、「経路異常発生中」と表示されます。
・IEEE802.11a（[BSSID]）
IEEE802.11a の BSSID（MAC アドレス）が表示されます。
無線スイッチが「オフ」の場合は、「停止中」と表示されます。
リンクインテグリティ機能によって電波が停止している場合は、「経路異常発生中」と表示されます。

□ 無線 LAN 端末の情報

・無線 LAN 端末 MAC アドレス
無線 LAN 端末の MAC アドレスが表示されます。
・接続情報
接続中の無線 LAN 端末は「接続中」、接続に失敗した無線 LAN 端末は「接続に失敗」と表示されます。
・SSID
無線 LAN 端末の SSID が表示されます。
・ポリシー名
セキュリティポリシーの名前が表示されます。
・インターフェース
無線 LAN 端末の無線 LAN インターフェースが「IEEE802.11b/11g」または「IEEE802.11a」と表示されます。
・チャンネル
チャンネル番号が表示されます。

・VLAN 名
通常 VLAN 機能を使用している場合は、VLAN 名が表示されます。認証 VLAN を使用している場合および VLAN が無効の場合は、何も表示されません。

2 Dr.WLAPPer の管理機能

Dr.WLAPPer で、無線 LAN アクセスポイントの管理を行う方法を説明します。

登録

Dr.WLAPPer で管理するためには、対象となる無線 LAN アクセスポイントを登録する必要があります。

■グループの作成／グループ名の変更

Dr.WLAPPer は、グループごとに無線 LAN アクセスポイントを管理できます。グループは 5 階層まで作成することができます。第 1 階層にはグループを 1 つだけ登録できます。第 2 階層から第 5 階層までは、各階層に複数のグループを登録することができます。
初期状態では第 1 階層の「グループ 1」が登録されています。

POINT

グループ名について

グループ名は、任意の文字列を 64 バイト（半角文字で 64 文字、全角文字で 32 文字）以内で設定します。また、1 つのグループに複数のサブグループを作成する場合は、サブグループのグループ名が、グループ内で一意の名前となるようにしてください。アルファベットの大文字と小文字は区別されませんので、ご注意ください。

□ グループの作成

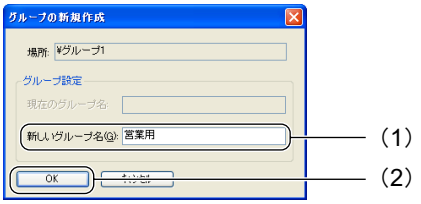
次の手順でグループを作成します。

1 メイン画面のツリービューで、作成するグループの親となるグループを選択します。

2 「ファイル」メニュー→「グループ作成」をクリックします。
「グループの新規作成」ウィンドウが表示されます。

3 (1)「新しいグループ名」に作成するグループ名を入力して、(2)「OK」をクリックします。

「場所」に表示されているのは、作成するグループの親グループです。



グループが登録されます。

□ グループ名の変更

次の手順でグループ名を変更します。

1 メイン画面のツリービューで、グループ名を変更するグループを選択します。

2 「編集」メニュー→「グループ名の変更」をクリックします。

「グループ名の変更」ウィンドウが表示されます。

「現在のグループ名」に、変更前のグループ名が表示されています。

3 「新しいグループ名」に変更後のグループ名を入力して、「OK」をクリックします。

グループ名が変更されます。

POINT

グループの削除

ツリービューで、削除するグループを選択して、「編集」メニュー→「削除」の順にクリックします。

選択したグループと、そのグループの配下に登録されているグループをすべて削除します。ただし、第 1 階層のグループを削除することはできません。

■無線 LAN アクセスポイントの登録／登録情報の変更

無線 LAN アクセスポイントの登録および登録情報の変更について説明します。

□ 無線 LAN アクセスポイントの登録

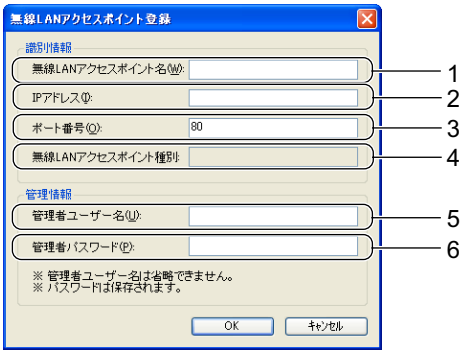
次の手順で登録します。

1 メイン画面のツリービューで、登録先のグループを選択します。

2 「ファイル」メニュー→「無線 LAN アクセスポイント登録」の順にクリックします。

「無線 LAN アクセスポイント登録」ウィンドウが表示されます。

3 Dr.WLAPPer に登録する無線 LAN アクセスポイントの情報を入力して、「OK」をクリックします。



1. **無線 LAN アクセスポイント名**
   Dr.WLAPPer 上に表示する無線 LAN アクセスポイント名です。任意の文字列を 32 バイト（半角文字で 32 文字、全角文字で 16 文字）以内で設定してください。また、1 つのグループに複数台の無線 LAN アクセスポイントを登録する場合は、グループ内で一意の名前となるようにしてください。
2. **IP アドレス**
   管理する無線 LAN アクセスポイントにアクセスするための IP アドレスです。
3. **ポート番号**
   管理する無線 LAN アクセスポイントにアクセスするための http ポート番号です。
4. **無線 LAN アクセスポイント種別**
   無線 LAN アクセスポイントの型名です。
5. **管理者ユーザー名**
   管理する無線LANアクセスポイントにアクセスするための管理者ユーザー名です。
6. **管理者パスワード**
   管理する無線LANアクセスポイントにアクセスするための管理者パスワードです。

POINT

- **ポート番号、管理者ユーザー名、管理者パスワードは、無線 LAN アクセスポイントに対してアクセスするための値です。登録する無線 LAN アクセスポイントに設定されている値を入力してください。**

メイン画面の稼動情報ビューに、登録した無線 LAN アクセスポイントの稼動状態が表示されます。
登録が完了し、Dr.WLAPPer で管理ができるようになります。

□ 登録情報の変更

次の手順で登録情報を変更します。

1 メイン画面の稼動情報ビューで、登録情報を変更する無線 LAN アクセスポイントを選択します。

2 「編集」メニュー→「登録情報の変更」の順にクリックします。

「無線 LAN アクセスポイント登録情報の変更」ウィンドウが表示されます。

3 変更する情報を入力して、「OK」をクリックします。

登録情報の各項目については、「無線 LAN アクセスポイントの登録」（→ P.158）をご覧ください。

POINT

・IP アドレス、ポート番号、管理者ユーザー名、管理者パスワードは、無線 LAN アクセスポイントに対してアクセスするための値です。この画面で値を変えても無線 LAN アクセスポイントには反映されません。今まで接続できていた場合、この値を変えると接続できなくなりますのでご注意ください。

POINT

無線 LAN アクセスポイント名の削除

稼動情報ビューで、Dr.WLAPPer から登録を削除する無線 LAN アクセスポイントを選択して、「編集」メニュー→「削除」の順にクリックします。

Dr.WLAPPer を利用した設定

Dr.WLAPPer を使用して設定を行う方法を説明します。

POINT

複数の無線 LAN アクセスポイントの設定を一括で行う場合

一括設定するすべての無線LANアクセスポイントのファームウェアバージョンが同じになっている必要があります。異なるファームウェアバージョンの無線 LAN アクセスポイントが混在していると、設定の変更を一括で行うことはできません。

1 設定を変更する無線 LAN アクセスポイント、またはグループを選択します。

・1 台のみ設定の変更を行う場合
メイン画面の稼動情報ビューで、設定の変更を行う無線 LAN アクセスポイントを 1 台選択します。

・グループ内のすべての無線 LAN アクセスポイントの設定を一括で変更する場合
メイン画面のツリービューでグループを選択します。

POINT

・選択したグループの直下に登録されている無線LANアクセスポイントが対象となります。サブグループに登録されている無線 LAN アクセスポイントは対象となりません。
・「稼動情報」が、「未稼動」または「取得不可」の無線 LAN アクセスポイントは、設定変更ができません。

・グループ内で複数の無線 LAN アクセスポイントを選択して設定を変更する場合
メイン画面のツリービューからグループを選択し、稼動情報ビューで設定の変更を行う無線 LAN アクセスポイントを複数選択します。

POINT

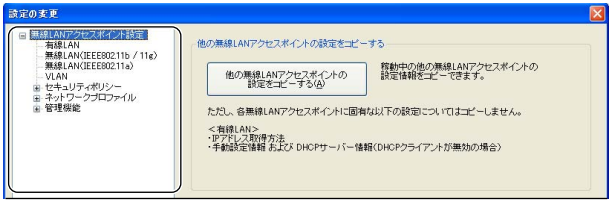
複数の無線 LAN アクセスポイントを選択した場合

・「設定の変更」ウィンドウでグレイアウト表示になっている項目以外は、すべて同じ内容で設定されます。「設定の変更」ウィンドウでグレイアウト表示になっている項目は、現在の設定内容が保持されます。
・無線 LAN アクセスポイントごとに異なる値が設定されている項目は、「設定の変更」ウィンドウの項目名が青色で表示され、値は表示されません。項目名が青色で表示されているものについては、必ず値を指定してください。指定した値が、選択したすべての無線 LAN アクセスポイントに設定されます。

2 「編集」メニュー→「設定の変更」をクリックします。

「設定の変更」ウィンドウが表示されます。

3 「設定の変更」ウィンドウの「無線　LAN　アクセスポイント設定」のメニューから変更する項目を選択して、設定を変更します。



メニューや設定する項目は、本製品のブラウザ設定画面とほぼ同じです。設定の詳細については、それぞれ次の章をご覧ください。

・ネットワークの設定については、「設定の詳細（ネットワークの設定）」（→ P.65）をご覧ください。
・管理機能の設定については、「設定の詳細（管理／メンテナンス機能）」（→ P.119）をご覧ください。

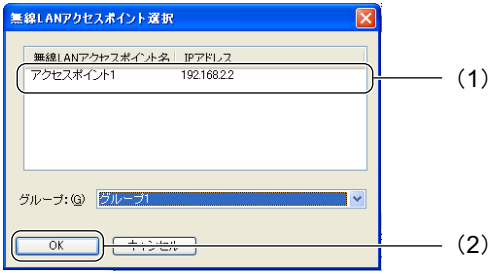
ただし、次の設定項目には対応していません。

・「IEEE802.11b/IEEE802.11g」画面の「拡張機能」カテゴリのすべての項目
・「IEEE802.11a」画面の「拡張機能」カテゴリのすべての項目
・「MAC アドレスフィルタリングの設定」画面の「アドレス一覧の保存」および「アドレス一覧の復元」

POINT

他の無線 LAN アクセスポイントの設定をコピーする場合

・稼動中の別の無線 LAN アクセスポイントから設定内容をコピーする場合は、「設定の変更」ウィンドウで「他の無線 LAN アクセスポイントの設定をコピーする」をクリックすると、「無線 LAN アクセスポイント選択」ウィンドウが表示されます。(1) コピー元の無線 LAN アクセスポイントを選択して (2)「OK」をクリックします。異なるグループの無線 LAN アクセスポイントを選択する場合は、「グループ」の をクリックしてグループを選択してから、コピー元の無線 LAN アクセスポイントを選択してください。



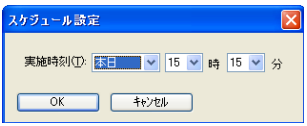
「設定の変更」ウィンドウに、コピーした内容が表示されます。

・ファームウェアバージョンの異なる無線 LAN アクセスポイント間では、設定をコピーする機能はご利用できません。ファームウェアバージョンの異なる無線 LAN アクセスポイントは、「無線LANアクセスポイント選択」ウィンドウに表示されません。

値を変更した項目は、項目名が赤色の文字で表示されます。
選択した値などによって、サブメニューが表示される場合があります。サブメニューが表示された場合は、サブメニューをクリックして設定を行います。

4 必要な設定が終了したら、「設定の変更」ウィンドウの「直ちに実行」または「スケジュールして実行」をクリックします。

・「直ちに実行」をクリックすると、即時に設定を反映します。
・「スケジュールして実行」をクリックすると、「スケジュール設定」ウィンドウが表示されます。



実施時刻を指定して「OK」をクリックすると、指定した日時に設定の反映を行います。2 日後まで指定可能です。
夜中や休日など、端末が通信を行っていない時間を指定しておくことができます。

POINT

次の場合には登録したスケジュールが破棄されます

・スケジュールが実行される前に、Dr.WLAPPer で別の設定の変更を行った場合
・スケジュールが実行される前に、Dr.WLAPPer を終了した場合
・スケジュールした時刻に本製品が「稼動」状態でない場合
・「編集」メニュー→「スケジュールの取り消し」で、スケジュールを取り消した場合

・「キャンセル」をクリックすると、変更した内容は保持されず、「設定の変更」ウィンドウが閉じます。

「設定の変更」ウィンドウが終了します。

Dr.WLAPPer を利用したメンテナンス

Dr.WLAPPer を使用してメンテナンスを行う方法を説明します。

Dr.WLAPPer でサポートしているメンテナンス機能は、再起動およびファームウェアの更新です。設定情報の保存、復元、初期化、および PING テストの機能はサポートしておりませんので、ご了承ください。

■再起動

再起動を行う場合は、次の手順で行います。

1 再起動を行う無線 LAN アクセスポイント、またはグループを選択します。

・1 台のみ再起動を行う場合

稼動情報ビューで再起動を行う無線 LAN アクセスポイントを 1 台選択します。

・グループ内のすべての無線 LAN アクセスポイントを一括で再起動する場合

ツリービューでグループを選択します。

POINT

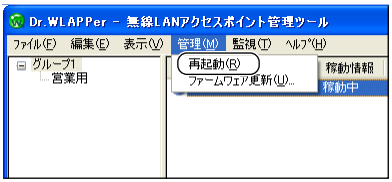
・選択したグループの直下に登録されている無線LANアクセスポイントが対象となります。サブグループに登録されている無線 LAN アクセスポイントは対象となりません。

・「未稼動」および「取得不可」の無線 LAN アクセスポイントは、再起動できません。

・グループ内で複数の無線 LAN アクセスポイントを選択して再起動する場合

稼動情報ビューで再起動を行う無線 LAN アクセスポイントを複数選択します。

2 「管理」メニュー→「再起動」をクリックします。



確認のメッセージが表示されます。

3 「OK」をクリックします。

選択した無線 LAN アクセスポイントが再起動されます。

処理が終了すると、「処理結果」が表示されます。

4 内容を確認して、「OK」をクリックします。

■ファームウェアの更新

ファームウェアの更新に関する注意事項などについては「ファームウェアの更新」(→ P.140)をご覧ください。
ファームウェアの更新を行う場合は、次の手順で行います。

1 ファームウェアの更新を行う無線 LAN アクセスポイント、またはグループを選択します。

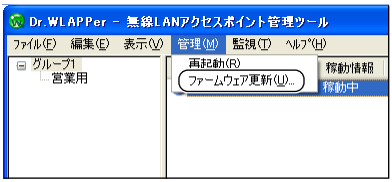
・1 台のみファームウェアの更新を行う場合
稼動情報ビューでファームウェアの更新を行う無線LANアクセスポイントを1台選択します。
・グループ内のすべての無線LANアクセスポイントのファームウェアを一括で更新する場合
ツリービューでグループを選択します。

POINT

- 選択したグループの直下に登録されている無線LANアクセスポイントが対象となります。サブグループに登録されている無線 LAN アクセスポイントは対象となりません。
- 「未稼動」および「取得不可」の無線 LAN アクセスポイントは、ファームウェアの更新ができません。

・グループ内で複数の無線LANアクセスポイントを選択してファームウェアの更新を行う場合
稼動情報ビューでファームウェアの更新を行う無線LANアクセスポイントを複数選択します。

2 「管理」メニュー→「ファームウェア更新」をクリックします。



ファームウェアのファイルを選択する画面が表示されます。

3 ファームウェアのファイルを選択します。

確認のメッセージが表示されます。

4 「OK」をクリックします。

「ファームウェア更新処理中」という画面が表示されます。

重要

- 「ファームウェア更新処理中」という画面が終了するまで、絶対に無線 LAN アクセスポイントの電源を切ったり、パソコンの操作を行ったりしないでください（ただし「ファームウェア更新中」画面の「中断」を除く）。無線 LAN アクセスポイントが動作しなくなる場合があります。

POINT

「中断」について

複数の無線LANアクセスポイントのファームウェアを更新する場合は、「ファームウェア更新処理中」の画面で中断ができます。「中断」をクリックすると、処理中のファームウェア更新が終了した時点で処理を中断し、未処理の無線 LAN アクセスポイントのファームウェアを更新しません。

処理が終了すると、「処理結果」が表示されます。

5 内容を確認して、「OK」をクリックします。

6 稼動情報ビューで、選択した無線 LAN アクセスポイントのファームウェアバージョンが、更新したバージョンになっていることを確認します。

3 Dr.WLAPPer の監視機能

Dr.WLAPPerを使用して無線LANアクセスポイントの無線監視を行う方法を説明します。

監視の設定

監視機能を利用するための設定について説明します。

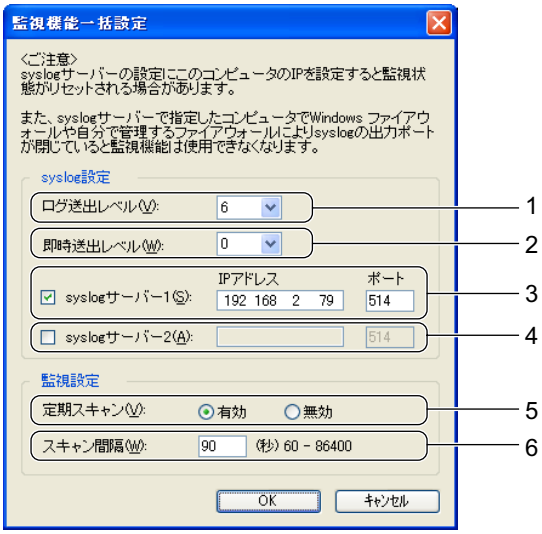
POINT

- 監視機能を使用する場合は必ず「監視一括設定」で　syslog　の設定をしてください。また、syslog の設定を変更する場合も「監視一括設定」で設定を変更してください。
  Dr.WLAPPer の「編集」メニュー→「設定の変更」や、ブラウザ設定画面の「管理機能」メニューで syslog の設定を行っても、監視機能は正常に動作しません。
- 無線 LAN インターフェースの設定で、「無線スイッチ」をオフにしている無線 LAN アクセスポイントは監視機能を利用できません。

1 Dr.WLAPPer メイン画面のツリービューから、一括監視設定するグループを選択します。

2 「監視」メニュー→「監視一括設定」をクリックします。
「監視機能一括設定」画面が表示されます。

3 監視機能に関する設定をします。



1. **ログ送出レベル**
   syslog サーバーに通知するログのレベルです。6 または 7 を設定します。
2. **即時送出レベル**
   syslog サーバーに即時に通知するログのレベルです。0 ～ 5 を指定すると、監視機能で使用するログが 10 個たまるまで送出されない場合があります。
3. **syslog サーバー 1**
   Dr.WLAPPer をインストールしている管理者用パソコンの IP アドレス、および利用する syslog ポートを設定します。syslog ポートを変更した場合、無線 LAN アクセスポイントの設定の変更と共に、管理者用パソコンが Dr.WLAPPer で syslog メッセージを受信するためのポートの設定も同時に行います。
4. **syslog サーバー 2**
   Dr.WLAPPer をインストールしている管理者パソコン以外に syslog を送出したい場合に設定します。
5. **定期スキャン**
   無線 LAN アクセスポイントが定期的に周辺無線 LAN アクセスポイント検出機能を行うかどうかを指定します。監視機能を利用する場合は、「有効」を選択してください。
6. **スキャン間隔**
   定期スキャンの時間間隔を指定します。グループ毎に異なる値を設定することはできません。すべてのグループで同じ値を設定してください。

POINT

「syslog サーバー 1」の「ポート」について

・「ポート」の値は、通常変更する必要はありません。ただし、Dr.WLAPPer をインストールしている管理者用パソコンで syslog サーバーソフトウェアを併用しているなど、他のプログラムがポート番号 514 を使用している場合は、他のプログラムで使用されていない番号を設定してください。
・syslog サーバーに指定したコンピュータで、OS のファイアウォールや自分で管理するファイアウォールにより「ポート」に指定したポート番号が閉じていると、監視機能は使用できなくなります。
Windows XP や Windows Server 2003 で監視ツールが使用できない場合は、Windows ファイアウォールの詳細設定で、本製品から送信される syslog メッセージを通過させるように設定を行ってください。通過させるサービスの内容は次のとおりです。
  ・サービスの説明 ：syslog
  ・TCP または UDP ：UDP
  ・ポート番号：514（「syslog サーバー1」の「ポート」に「514」が設定されている場合）
・グループごとに異なるポート番号を設定することはできません。すべてのグループで同じポート番号を設定してください。

重要

「定期スキャン」について

・「定期スキャン」を有効に設定すると、すべての無線 LAN 端末は本製品に接続できなくなります。

4 **「OK」をクリックします。**

選択したグループ内の無線 LAN アクセスポイントが再起動されます。
処理が終了すると、「処理結果」が表示されます。

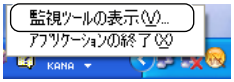
5 **内容を確認して、「OK」をクリックします。**

監視ツールの開始／終了

■開始

Dr.WLAPPer インストール後、パソコンを再起動すると、画面右下の通知領域に Dr.WLAPPer 監視ツールのアイコン（ ）が表示されます。アイコンが表示されているときは、アイコンから監視ツールを開くことができます。

1 **画面右下の通知領域に表示されている Dr.WLAPPer 監視ツールのアイコン（ ）を右クリックして、表示されるメニューから「監視ツールの表示」をクリックします。**



Dr.WLAPPer 監視ツール画面が表示されます。

POINT

アイコンが表示されていない場合

Dr.WLAPPer インストール直後や、「Dr.WLAPPer 監視ツールの終了」（→ P.169）で監視ツールを終了して、画面右下の通知領域に監視ツールのアイコンが表示されていない場合は、次の方法で起動することができます。

・Dr.WLAPPer から起動する
Dr.WLAPPer メイン画面の「監視」メニュー→「監視ツールの表示」の順にクリックします。
Dr.WLAPPer 監視ツール画面が表示されます。画面右下の通知領域に Dr.WLAPPer 監視ツールのアイコン（ ）が表示されます。

■終了

□ Dr.WLAPPer 監視ツール画面の終了

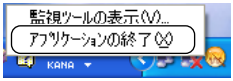
Dr.WLAPPer 監視ツール画面のみを終了します。画面を閉じても、画面右下の通知領域に Dr.WLAPPer 監視ツールのアイコンが表示されている間は、監視ツールは動作中です。

1 **Dr.WLAPPer 監視ツール画面の「ファイル」メニュー→「終了」をクリックします。**

□ Dr.WLAPPer 監視ツールの終了

Dr.WLAPPer 監視ツールを終了します。画面右下の通知領域からアイコンが消えます。

1 **画面右下の通知領域から Dr.WLAPPer 監視ツールのアイコン（ ）を右クリックし、表示されるメニューから「アプリケーションの終了」をクリックします。**



Dr.WLAPPer 監視ツールの使い方

■監視ツールのメニュー

Dr.WLAPPer 監視ツールのメニューには「ファイル」メニュー、「表示」メニュー、「ヘルプ」メニューがあります。

「ファイル」メニュー

「ファイル」メニューでは、「ログの消去」、「ログの設定」、「終了」が選択できます。

・ログの消去
今までの検出されたログをすべて消去します。詳しくは「ログの消去」（→ P.174）をご覧ください。

・ログの設定
保存するログの設定を行います。詳しくは「ログの設定」（→ P.170）をご覧ください。

・終了
Dr.WLAPPer 監視ツールを終了します。詳しくは「監視ツールの開始／終了」（→ P.168）をご覧ください。

「表示」メニュー

「表示」メニューでは、「すべてのログを表示」、「情報の再取得」が選択できます。

・すべてのログを表示
すべてのログを表示するか、ツリービューで選択したグループ配下または無線 LAN アクセスポイントのみのログを表示するか切り替えられます。詳しくは「ログ表示モードの切り替え」（→ P.173）をご覧ください。

・情報の再取得
　監視情報を最新の情報にします。

「ヘルプ」メニュー

「ヘルプ」メニューでは、「マニュアル」、「バージョン情報」が選択できます。

・マニュアル
　ワイヤレス LAN ステーションの取扱説明書が表示されます。
・バージョン情報
　Dr.WLAPPer 監視ツールのバージョン情報が表示されます。

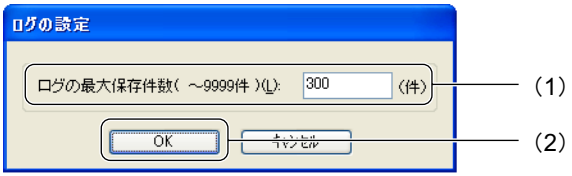
■ログの設定

表示するログの数を設定します。ログの数が設定した数を上回ると、古いログから消去されます。

1　Dr.WLAPPer　監視ツール画面で、「ファイル」メニュー→「ログの設定」の順にクリックします。

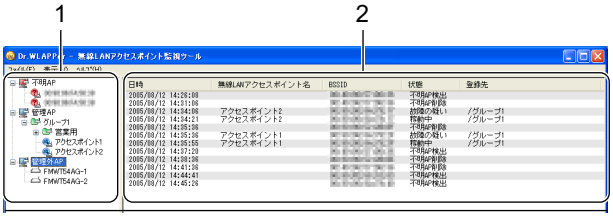
「ログの設定」画面が表示されます。

2　(1) 表示させるログの最大数を入力して、(2)「OK」をクリックします。



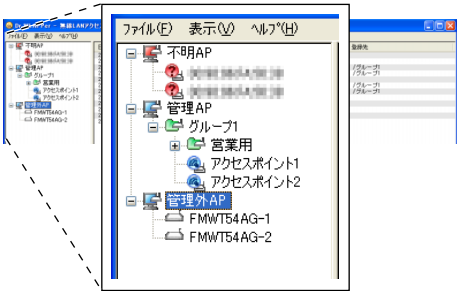
■ログの見方

Dr.WLAPPer 監視ツール画面の見方について説明します。



1 ツリービュー

Dr.WLAPPer 監視ツールでは、ツールで検知した無線 LAN アクセスポイントを次のように分類して、ツリービューに表示します。



・不明 AP

Dr.WLAPPer に登録されていない無線 LAN アクセスポイントを検出したときに、不明 AP として表示されます。不明 AP は、監視の対象となります。使用場所や使用目的がはっきりしていて管理する必要がない不明 AP は、ドラッグして「管理外 AP」へ移動することができます。右クリックして表示されるメニューから「管理外 AP に追加する」をクリックしても移動できます。

・管理 AP

Dr.WLAPPer に登録されている無線 LAN アクセスポイントです。管理 AP は、監視の対象となります。稼動状態をアイコンで示します。

表：管理 AP の稼動状況アイコン一覧

アイコンの状態	説明
	稼動中です。
	故障の疑いがあります。
	故障しています。
	電波が検出されていません。

・管理外 AP

不明 AP に検出された無線 LAN アクセスポイントのうち、使用している場所などが明らかで、監視する必要がないものを管理外 AP として登録します。管理外 AP は、監視の対象となりません。

POINT

管理外 AP の登録名を変更する

管理外 AP に登録した無線 LAN アクセスポイントは、ツリービューに表示する名前を変更することができます。

1. ツリービューで、登録名を変更する管理外 AP 内の無線 LAN アクセスポイントを右クリックして表示されるメニューから「登録名を変更する」をクリックします。
2. 「登録名の変更」画面で、新しい登録名を 32 文字以内で入力し、「OK」をクリックします。
   登録名が変更されます。

管理外 AP から削除する

管理外 AP に登録していた無線 LAN アクセスポイントを、管理外 AP の登録から削除することができます。試験運用中などの理由で管理外 AP に登録していた無線 LAN アクセスポイントを、試験運用終了時に管理外 AP から削除する場合などに使用します。

1. ツリービューで、管理外 AP から登録を削除する無線 LAN アクセスポイントを右クリックして表示されるメニューから「管理外 AP から削除する」をクリックします。
   管理外 AP から削除されます。

2 ログビュー

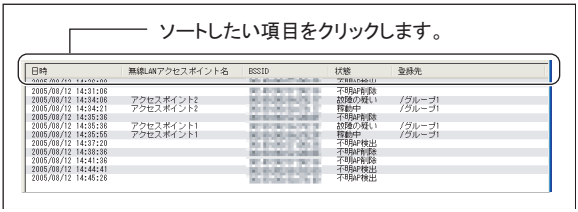
ログビューには、無線の状態に変化が検出された場合の記録が表示されます。

- 日時
  状態を検出した日時が表示されます。
- 無線 LAN アクセスポイント名
  Dr.WLAPPer に登録されている無線 LAN アクセスポイントの場合は、無線 LAN アクセスポイント名が表示されます。登録されていない無線 LAN アクセスポイントの場合は、何も表示されません。
- BSSID
  状態を検出した無線 LAN アクセスポイントの BSSID が表示されます。
- 状態
  検出した状態が表示されます。
- 登録先
  Dr.WLAPPer に登録されている無線 LAN アクセスポイントの場合は、登録先グループのパスが表示されます。登録されていない無線 LAN アクセスポイントの場合は、何も表示されません。

POINT

ログのソート

ログビューの各項目をクリックすると、クリックした項目でログ情報をソートして表示します。項目をクリックするたびにソートの昇順と降順が切り替わります。



POINT

情報の更新について

Dr.WLAPPer 監視ツール画面の情報は、「監視の設定」（→ P.166）の「スキャン間隔」に設定した間隔で更新されます。不明 AP を検出したときや管理 AP の状態が変わったときは即時更新されます。

Dr.WLAPPer で登録情報の変更を行った後など、監視ツールですぐに最新の情報を確認したい場合は、Dr.WLAPPer 監視ツール画面の「表示」メニュー→「情報の再取得」の順にクリックすると、最新の情報に更新されます。

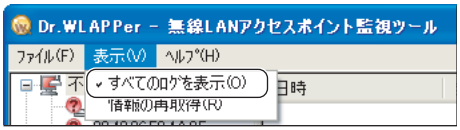
■ログ表示モードの切り替え

ログの表示には、「すべてのログを表示」と「絞り込んで表示」のふたつのモードがあります。表示モードの確認と切り替えをする場合は、次の手順で行います。

1 「表示」メニューをクリックします。

- 「すべてのログを表示」に ✔ が付いているときは、管理 AP、不明 AP のすべての無線 LAN アクセスポイントのログが表示されます。
- 「すべてのログを表示」に ✔ が付いていない場合は、「絞り込んで表示」モードになります。ツリービューで選択したグループまたは無線 LAN アクセスポイントのログのみが表示されます。ただし、ツリービューで管理外 AP が選択されている場合は、ログビューには何も表示されません。

2 ログの表示モードを切り替える場合は、「すべてのログを表示」をクリックします。



「すべてのログを表示」の ✔ の有無が切り替わり、表示モードが切り替わります。

POINT

・ツリービューで不明 AP または管理 AP のグループまたは無線 LAN アクセスポイントを右クリックして表示されるメニューから「すべてのログを表示」をクリックしても、ログの表示モードを切り替えることができます。

■プロパティの確認

個々の無線 LAN アクセスポイントの情報を確認することができます。

1 **Dr.WLAPPer　監視ツール画面のツリービューから、情報を確認する無線 LAN アクセスポイントを選択します。**

2 **右クリックして表示されるメニューから「プロパティ」をクリックします。**
「アクセスポイントのプロパティ」画面が表示されます。

3 **確認したら「OK」をクリックします。**

■ログの消去

1 **「ファイル」メニュー→「ログの消去」をクリックします。**

すべてのログが消去されます。

7

第 7 章
こんなときは

困ったときの対処方法などを説明します。

1 その他の使い方

本製品のその他の使い方を説明します。

初期化（LOAD DEFAULT ボタン）

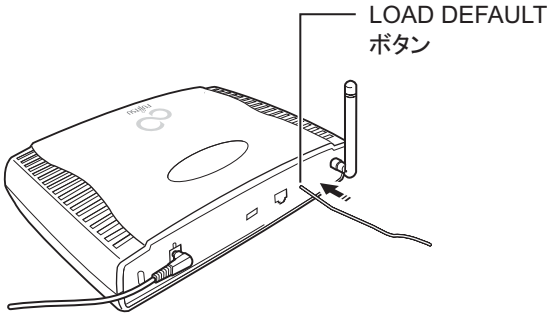
パスワードの忘却や設定の誤りによって本製品の設定画面にログインできなくなった場合などは、本製品の設定内容をご購入時の状態に戻します。
LOAD DEFAULT ボタンを使用して、本製品の設定内容をご購入時の設定に戻す方法について説明します。

POINT

設定画面にログインできる場合

ブラウザ設定画面から、本製品の設定をご購入時の状態に戻すこともできます。詳しくは、「設定情報（保存／復元／初期化）」（→ P.142）をご覧ください。

1 LOAD DEFAULT ボタンを、細長い針金のようなもので 5 秒間押し続けます。



2 STATUS ランプが点滅し始めたら、ボタンを押すのをやめます。

重要

・STATUS ランプの点滅中は絶対に本製品の電源を切らないでください。

STATUS ランプの点滅が終了すると、本製品の設定内容がご購入時の状態に戻ります。

ローミング機能の利用

本製品のローミング機能をご利用になる場合のご注意などについて説明します。
ローミング機能の概要については、「ローミング」（→ P.34）をご覧ください。
またローミング機能をご利用になる場合は、リンクインテグリティ機能が使用できます。リンクインテグリティ機能については、「リンクインテグリティ設定」（→ P.134）をご覧ください。

■検証済み無線 LAN アクセスポイント

次の無線 LAN アクセスポイントとローミングの検証を行っています。

・ワイヤレス LAN ステーション FMWT-56AG（本製品）
・ワイヤレス LAN ステーション FMWT-55AG
・ワイヤレス LAN ステーション FMWT-54AG
・ワイヤレス LAN ステーション FMWT-53A
・ワイヤレス LAN ステーション FMWT-53G
・ワイヤレス LAN ステーション FMWT-52A
・ワイヤレス LAN ステーション FMWT-52B
・ワイヤレス LAN ステーション FMWT-52AB
・ワイヤレス LAN ステーション FMWT-52BB
・ワイヤレスブロードバンドルータ FMWBR-201
・ワイヤレスブロードバンドルータ FMWBR-102

■ローミング機能使用時の設定例

ローミング機能を使用する場合は、次の例を参考に各アクセスポイントの設定を行ってください。

□ 有線 LAN の設定

・IP アドレス
　192.168.2.2 と 192.168.2.3 のように、各無線 LAN アクセスポイントに異なる IP アドレスを設定します。
・サブネットマスク
　各無線 LAN アクセスポイントに同じ値（255.255.255.0 など）を設定します。

有線 LAN の設定について詳しくは、「有線 LAN の設定」（→ P.66）をご覧ください。

□ 無線 LAN インターフェースの設定

チャンネルの設定に注意してください。

・IEEE802.11b/IEEE802.11g の場合
　無線 LAN アクセスポイントどうしで値を 5 つ以上離して（1 と 6、6 と 11 など）設定します。IEEE802.11b/IEEE802.11g インターフェースの設定については、「「IEEE802.11b/IEEE802.11g」画面」（→ P.75）をご覧ください。
・IEEE802.11a の場合
　無線 LAN アクセスポイントどうしで異なる値（36 と 40 など）を設定します。IEEE802.11a インターフェースの設定については、「「IEEE802.11a」画面」（→ P.84）をご覧ください。

□ セキュリティポリシーの設定

無線 LAN のセキュリティを、すべて同じように設定したセキュリティポリシーを、各無線 LAN アクセスポイントに作成します。セキュリティポリシーの設定について詳しくは、「セキュリティポリシーの設定」（→ P.97）をご覧ください。

□ ネットワークプロファイルの設定

同じ SSID で、同一の設定内容の組み合わせのプロファイルを、各無線 LAN アクセスポイントに作成します。ネットワークプロファイルの設定について詳しくは、「ネットワークプロファイルの設定」（→ P.115）をご覧ください。

2 Q&A

正常に動作しない場合は、Q&A の内容を確認してください。また、本製品以外の原因も考えられますので、システムとして組み合わされている他の機器も合わせてお調べください。どうしても原因がわからないときは「お問い合わせ先」（→P.199）に連絡してください。

Q パソコンの IP アドレスの設定方法

A 次のようにして IP アドレスを設定します

パソコンの IP アドレスは、次のように操作して表示される画面で設定します。

1 次のように操作します。

Windows XP の場合

1. 「スタート」ボタン→「コントロールパネル」の順にクリックします。
2. 「ネットワークとインターネット接続」をクリックします。
   「ネットワークとインターネット接続」が表示されない場合は、そのまま手順 3 へお進みください。
3. 「ネットワーク接続」をクリックします。
4. 「ネットワーク接続」ウィンドウで、「ローカルエリア接続」（無線 LAN 端末の場合は「ワイヤレスネットワーク接続」）を右クリックして表示されるメニューから、「プロパティ」をクリックします。
5. 「ローカルエリア接続のプロパティ」（無線 LAN 端末の場合は「ワイヤレスネットワーク接続のプロパティ」）ウィンドウで、「全般」タブをクリックします。
   「インターネットプロトコル（TCP/IP）」をクリックして反転表示させ、「プロパティ」をクリックします。
   「インターネットプロトコル（TCP/IP）のプロパティ」ウィンドウが表示されます。

Windows 2000 の場合

1. 「スタート」ボタン→「設定」→「コントロールパネル」の順にクリックします。
2. 「コントロールパネル」ウィンドウで、「ネットワークとダイヤルアップ接続」をクリックします。
3. 「ネットワークとダイヤルアップ接続」ウィンドウで、「ローカルエリア接続」を右クリックして表示されるメニューから、「プロパティ」をクリックします。
4. 「インターネットプロトコル（TCP/IP）をクリックして反転表示させ、「プロパティ」をクリックします。
   「インターネットプロトコル（TCP/IP）のプロパティ」ウィンドウが表示されます。

Windows Me ／ Windows 98 の場合

1. 「スタート」ボタン→「設定」→「コントロールパネル」の順にクリックします。
2. 「コントロールパネル」ウィンドウで、「ネットワーク」アイコンをクリックします。
3. 「ネットワーク」ウィンドウの「ネットワークの設定」タブの画面で、「TCP/IP」をクリックして反転表示させ、「プロパティ」をクリックします。
「TCP/IP のプロパティ」ウィンドウの「IP アドレス」タブの画面が表示されます。

2 表示された画面で、次のように操作します。

パソコンに固定 IP アドレスを設定する場合

・Windows XP ／ Windows 2000 の場合
「インターネットプロトコル（TCP/IP）のプロパティ」ウィンドウで、「次の IP アドレスを使う」をクリックして◉にして、「IP アドレス」、「サブネットマスク」などを入力します。
・Windows Me ／ Windows 98 の場合
「TCP/IP のプロパティ」ウィンドウの「IP アドレス」タブの画面で、「IP アドレスを指定」をクリックして◉にして、「IP アドレス」、「サブネットマスク」などを入力します。

パソコンの IP アドレスを自動的に取得する場合

・Windows XP ／ Windows 2000 の場合
「インターネットプロトコル（TCP/IP）のプロパティ」ウィンドウで、「IP アドレスを自動的に取得する」をクリックして◉にします。
・Windows Me ／ Windows 98 の場合
「TCP/IP のプロパティ」ウィンドウの「IP アドレス」タブの画面で、「IP アドレスを自動的に取得」をクリックして◉にします。

■固定 IP アドレスについて

IP アドレスは、1 から 255 までの 4 個の数値で表します。本製品と各パソコンに次のように設定します。() 内はサブネットマスクです。サブネットマスクは、本製品と、本製品に接続されたネットワーク内のパソコンで、同じ値を設定します。

・本製品の設定例
本製品：192.168.2.2（255.255.255.0）
本製品の IP アドレスを上記のように設定した場合、本製品に接続するパソコンの IP アドレスは次のように設定します。本製品を DHCP サーバーとして使用するときは、「DHCP リース範囲」も、次の範囲の中で指定します。

・パソコン側の設定例（「次のようにして IP アドレスを設定します」（→ P.179）の画面で設定します）

パソコン A：192.168.2.10 （255.255.255.0）
パソコン B：192.168.2.11 （255.255.255.0）
パソコン C：192.168.2.12 （255.255.255.0）
：
：
パソコン X：192.168.2.254 （255.255.255.0）

POINT

本製品を DHCP サーバーとして使用する場合のパソコンの固定 IP アドレスの指定範囲

「DHCP リース範囲」に指定した範囲のアドレスを、パソコンの固定 IP アドレスとして設定することはできません。パソコンの固定 IP アドレスの指定は、次の例を参考にして行ってください。

例）本製品の IP アドレスが「192.168.2.2」、DHCP リース範囲が「192.168.2.100 ～ 192.168.2.150」の場合

パソコンの固定 IP アドレスは、本製品の IP アドレスと「DHCP リース範囲」を除いた次の範囲の中で、他の機器に設定されていないアドレスを指定します。

・192.168.2.1
・192.168.2.3 ～ 192.168.2.99
・192.168.2.151 ～ 192.168.2.254

家庭内や組織内などの閉じたネットワークの中で、ローカル IP アドレスとして使用できる IP アドレス

・10.0.0.1 ～ 10.255.255.254
・172.16.0.1 ～ 172.31.255.254
・192.168.0.1 ～ 192.168.255.254

Q パソコンの IP アドレス／ MAC アドレスの確認方法

パソコンの IP アドレス／ MAC アドレスの確認方法を説明します。

A 次のようにして IP アドレスを確認します

1 次のように操作します。

Windows XP の場合

「スタート」ボタン→「すべてのプログラム」→「アクセサリ」→「コマンドプロンプト」の順にクリックします。

Windows 2000 の場合

「スタート」ボタン→「プログラム」→「アクセサリ」→「コマンドプロンプト」の順にクリックします。

Windows Me の場合

「スタート」ボタン→「プログラム」→「アクセサリ」→「MS-DOS プロンプト」の順にクリックします。

Windows 98 の場合

「スタート」ボタン→「プログラム」→「MS-DOS プロンプト」の順にクリックします。
「MS-DOSプロンプト」、または「コマンドプロンプト」ウィンドウが表示されます。

2 次のように入力し、【Enter】キーを押します。
ipconfig

3 IP アドレスが正常に表示されているか確認します。
Windows XP ／ Windows 2000 の場合の表示例（パソコンの IP アドレスが 192.168.2.100 の場合）

```
IP Address. . . . . .  192.168.2.100
Subnet Mask. . . . . .  255.255.255.0
Default Gateway. . . . . .  192.168.2.2
```

POINT

Windows XP または Windows 2000 で、2 つの LAN 機能を同時に運用している場合

・本製品との接続に使用している LAN アダプタの名称を確認し、そのアダプタの IP アドレスが正常に表示されているか確認してください。

Windows 98／Windows Meの場合の表示例（パソコンのIPアドレスが192.168.2.100の場合）

```
IP アドレス. . . . . .  192.168.2.100
サブネット マスク. . . . . .  255.255.255.0
デフォルト ゲートウェイ. . . . . .  192.168.2.2
```

POINT

パソコンで IP アドレスが正常に表示されない場合は、本製品のネットワークの設定を確認してください。また、次の内容を確認してください。

IP アドレスが 169.254.nnn.mmm または 0.0.0.0 と表示されたとき

DHCP サーバーから正常に IP アドレスを取得できていません。次の点を確認してください。

・無線 LAN 端末の場合は、セキュリティの設定が本製品と一致しているか確認してください。
・パソコンの TCP/IP の設定を確認してください。

Windows XP または Windows 2000 で、「IP Address」が表示されず、「Cable Disconnected」または「Media Disconnected」と表示されたとき
または、Windows Me で「IP アドレス」が 0.0.0.0 と表示され、「メディアの状態」に「切断」と表示されたとき
または、Windows 98 で「IP アドレス」が 169.254.nnn.mmm または 0.0.0.0 と表示されたとき

無線 LAN 端末の場合は、次の設定を確認してください。

・SSID（ネットワーク名）が本製品と一致しているか
・無線 LAN のセキュリティの設定が本製品と一致しているか
・本製品の使用チャンネルが、無線 LAN 端末で使用可能なチャンネルの範囲内で設定されているか

有線 LAN 端末の場合は、LAN ケーブルが正常に接続されているか確認してください。

4 次のように入力し、【Enter】キーを押します。
exit
「MS-DOS プロンプト」、または「コマンドプロンプト」ウィンドウが閉じます。

A 次のようにして MAC アドレスを確認します

1 次のように操作します。
Windows XP の場合
「スタート」ボタン→「すべてのプログラム」→「アクセサリ」→「コマンドプロンプト」の順にクリックします。
Windows 2000 の場合
「スタート」ボタン→「プログラム」→「アクセサリ」→「コマンドプロンプト」の順にクリックします。
Windows Me の場合
「スタート」ボタン→「プログラム」→「アクセサリ」→「MS-DOS プロンプト」の順にクリックします。
Windows 98 の場合
「スタート」ボタン→「プログラム」→「MS-DOS プロンプト」の順にクリックします。
「MS-DOSプロンプト」、または「コマンドプロンプト」ウィンドウが表示されます。

2 次のように入力し、【Enter】キーを押します。
ipconfig /all

3 MAC アドレスを確認します。
Windows XP ／ Windows 2000 の場合
「Physical Address」の値が MAC アドレスです。

POINT

Windows XP または Windows 2000 で、2 つの LAN 機能を同時に運用している場合
本製品との接続に使用している LAN アダプタの名称を確認し、そのアダプタの MAC アドレスを確認してください。

Windows Me ／ Windows 98 の場合
「物理アドレス」の値が MAC アドレスです。

4 次のように入力し、【Enter】キーを押します。
exit
「MS-DOS プロンプト」、または「コマンドプロンプト」ウィンドウが閉じます。

Q パソコンからの接続確認

POINT

・本製品側から接続確認する方法については、「PING テスト」（→ P.145）をご覧ください。

A PING コマンドで接続確認をします

1 パソコンで、IP アドレスが正常に取得できているか確認します。
確認方法は、「パソコンの IP アドレス／ MAC アドレスの確認方法」（→ P.181）をご覧ください。

2 次のように操作します。
Windows XP の場合
「スタート」ボタン→「すべてのプログラム」→「アクセサリ」→「コマンドプロンプト」の順にクリックします。
Windows 2000 の場合
「スタート」ボタン→「プログラム」→「アクセサリ」→「コマンドプロンプト」の順にクリックします。
Windows Me の場合
「スタート」ボタン→「プログラム」→「アクセサリ」→「MS-DOS プロンプト」の順にクリックします。
Windows 98 の場合
「スタート」ボタン→「プログラム」→「MS-DOS プロンプト」の順にクリックします。
「MS-DOSプロンプト」、または「コマンドプロンプト」ウィンドウが表示されます。

3 次のように入力し、【Enter】キーを押します（本製品のIPアドレスが「192.168.2.2」の場合）。
ping 192.168.2.2
本製品と正常に接続できている場合は、パソコンで次のように表示されます。

```
Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=13ms TTL=64
Reply from 192.168.2.2: bytes=32 time<1ms TTL=64
Reply from 192.168.2.2: bytes=32 time<1ms TTL=64
Reply from 192.168.2.2: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 3ms
```

POINT

「Request timed out」「Destination host unreachable」などと表示される場合
接続確認相手との通信が行えない状態です。次の確認を行ってください。
・パソコンで IP アドレスが正しく設定されているか確認してください。

パソコンの IP アドレスを確認する方法については、「パソコンの IP アドレス／MAC アドレスの確認方法」（→ P.181）をご覧ください。
・有線 LAN の場合は、LAN ケーブルが正しく接続されているか確認してください。
・無線 LAN の場合は、無線 LAN の各設定が本製品の設定と合っているか確認してください。

4 次のように入力し、【Enter】キーを押します。
exit
「MS-DOS プロンプト」、または「コマンドプロンプト」ウィンドウが閉じます。

Q 電源供給ユニットを使用して本製品の電源が入らない

A LAN ケーブルが正しく接続されているか確認してください

本製品の LAN コネクタに正しく LAN ケーブルが接続されているか、確認してください。また、電源供給ユニット側も確認してください。

A 電源供給ユニットの電源が入っているか確認してください

A PoE 切替スイッチの設定を確認してください

電源供給ユニット（FMWT-PE11）をお使いの場合、本製品の PoE 切替スイッチの設定を確認してください。PoE 切替スイッチが「802.3af」側に設定されている可能性があります。「電源供給ユニットを使用する場合」（→ P.52）をご覧になり、PoE 切替スイッチを「PE11」側に設定してください。

Q 設定画面へのログイン画面が表示されない

次の項目を確認する前に、パソコンが本製品と LAN 接続できていることを確認してください。接続確認の方法については、「パソコンからの接続確認」（→ P.184）をご覧ください。

A Web ブラウザに入力した IP アドレスが正しいか、確認してください

Web ブラウザのアドレス欄には「http://[本製品の IP アドレス]/」と入力します。[本製品の IP アドレス] の部分が、本製品の IP アドレスと合っているか確認してください。本製品の IP アドレスの初期値は「192.168.2.2」です。IP アドレスを変更した場合は、変更後の IP アドレスを入力します。
ログイン方法については、「開始」（→ P.60）をご覧ください。

A Web ブラウザのプロキシサーバーの設定を確認してください

LAN にプロキシサーバーを使用する設定になっている場合は、本製品との接続にはプロキシサーバーを使用しない設定にします。
確認、設定方法については、「Web ブラウザの設定確認」（→ P.57）をご覧ください。

A 設定画面へのログイン制限の設定を確認してください

「管理機能」画面で設定画面へのログイン制限に関する設定を行っている場合は、設定画面へのログインが次のように一部制限されます。

■「管理機能」画面の「ポート番号」を「80」以外の値に設定している場合

本製品のブラウザ設定画面を開始するときに、ポート番号の指定が必要になります。次のように、Web ブラウザのアドレス入力欄に、本製品の IP アドレスとポート番号を半角コロン（:）で区切って指定します。

http://[本製品の IP アドレス]:[ポート番号]

例えば、本製品の IP アドレスが「192.168.2.2」、ポート番号が「88」の場合は、「http://192.168.2.2:88/」と入力します。

ポート番号を忘れてしまった場合は、「IP アドレス、ユーザー名、パスワードを忘れてログインできない」（→ P.187）をご覧ください。

■「無線 LAN からのログイン」を「拒否」に設定している場合

「管理機能」画面で「無線 LAN からのログイン」を「拒否」に設定している場合、無線 LAN 端末から本製品の設定画面にログインすることはできません。有線 LAN 端末からのみ、ログインが可能です。

A VLAN が有効の場合は管理者用パソコンの属する VLAN グループを確認してください

VLAN を有効にしている場合、「VLAN」画面の「管理 VLAN」に設定した VLAN グループに属する端末からのみ、設定画面にログインできます。その他の VLAN グループに属している端末ではログイン画面が表示されません。

Q 設定画面へのログイン画面が再度表示される

A ユーザー名、パスワードが正しいか確認してください

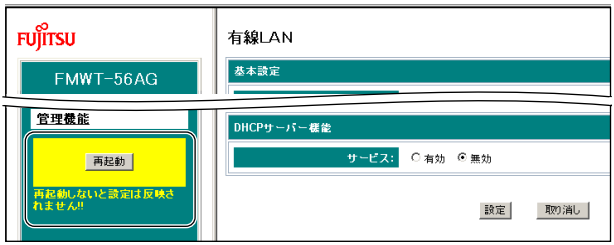
ログイン画面でユーザー名、パスワードを間違えて入力すると、再度ログイン画面が表示されます。正しい値を入力し直して、再度ログインを行ってください。

管理者権限でログインする場合は、「ユーザー名」、「パスワード」には、本製品の「管理者ユーザー名」「管理者パスワード」を入力します。

一般ユーザー権限でログインする場合は、「ユーザー名」、「パスワード」に「一般ユーザー名」、「一般パスワード」を入力します。

Q 再起動した後に「再起動」ボタンの周りが黄色の状態のまま残り、正常に設定が反映されない

ブラウザ設定画面で本製品の再起動を行い、「設定を保存しています。」という画面が終了しても、メニューフレームの「再起動」ボタンの周りが黄色のままになっていて正しく設定が反映されない場合があります。



A 本製品の電源を入れ直してください

このような場合は本製品の電源を切り、電源を入れ直してください。その後、再度設定し直してください。

Q IPアドレス、ユーザー名、パスワードを忘れてログインできない

A 本製品の設定内容をご購入時の状態に戻します

本製品の設定内容をご購入時の状態に戻した後、本製品の初期値でログインします。初期値は、それぞれ次のとおりです。

・IP アドレス：192.168.2.2
・管理者ユーザー名：admin
・管理者パスワード：admin

ご購入時の設定に戻す方法については、「初期化（LOAD DEFAULT ボタン）」（→ P.176）をご覧ください。

Q 通信ができない

本製品を使用した通信が正常にできない場合は、接続確認を行ってみてください。接続確認が成功する場合は、端末で使用しているアプリケーションや OS の仕様などの問題が考えられます。接続確認に失敗する場合は、本製品または本製品と接続している機器の設定の誤りやハードウェアの異常が考えられます。

接続確認の方法については、次の参照先をご覧ください。

・本製品からの接続確認
「PING テスト」（→ P.145）
・パソコンからの接続確認
「パソコンからの接続確認」（→ P.184）

A ランプの状態を確認してください

本製品の PWR ランプ、STATUS ランプ、LAN ランプの状態を確認してください。

■PWR ランプが点灯していない場合

電源が入っていません。

電源ケーブルや AC アダプタが正しく接続されているか確認してください。電源供給ユニットをお使いの場合は、電源供給ユニットが正しく接続されているか確認してください。

接続と電源の入れ方については、「各機器との接続」（→ P.50）をご覧ください。

■PWR ランプ：点灯、STATUS ランプ：消灯の場合

本製品の初期診断に失敗しています。

本製品の DC コネクタから AC アダプタを抜いて電源を切り、再度 AC アダプタを接続して電源を入れ直してください。

■PWR ランプ：点灯、LAN ランプ：消灯の場合

LAN ケーブルが正しく接続されていません。

LAN ケーブルの一方を本製品の LAN コネクタに、もう一方を接続する機器の LAN コネクタに正しく接続してください。本製品への LAN ケーブルの接続については、「各機器との接続」（→ P.50）をご覧ください。

上記の対策を行っても状態が変わらない場合は、本製品に何らかの異常が発生している可能性があります。「お問い合わせ先」（→ P.199）にご相談ください。

A 本製品を再起動してください

本製品が内部エラーなどにより、不安定な状態になっている可能性があります。本製品を再起動してください。再起動の方法は、「再起動」（→ P.139）をご覧ください。

A パソコンの設定などを確認してください

パソコンで次のような問題がないか確認します。

・IP アドレスが正しく設定されているか確認します。

確認方法は、「パソコンの IP アドレス／ MAC アドレスの確認方法」（→ P.181）を参考にしてください。

正しく設定されていない場合は、「パソコンの IP アドレスの設定方法」（→ P.179）を参考にして、IP アドレスを正しく設定してください。

・LAN カードや LAN ドライバの状態に問題がないか確認してください。

LAN カードを増設しているパソコンの場合は、LAN カードが正しくセットされているか確認してください。

また、LAN ドライバが正しくインストールされているか確認してください。

詳しくは、次のマニュアルをご覧ください。

・有線 LAN 機能、無線 LAN 機能が標準搭載されている場合は、パソコンのマニュアルをご覧ください。

・LAN カードを増設した場合は、LAN カードのマニュアルをご覧ください。

A 通信先のパソコンなどの仕様や設定を確認してください

通信相手のパソコンなどで、次のような問題がないか確認してください。

・接続先のネットワークにアクセスする権限があるかどうか確認します。

接続先となるパソコンの共有フォルダなどの設定によりアクセスが制限されている場合があります。この場合はネットワークに接続できても、共有フォルダなどのネットワーク資源にアクセスできなくなります。このような場合には接続先のパソコンなどの設定をご確認ください。

・接続先のパソコンの OS やアプリケーションの仕様を確認します。
接続先のパソコンの OS やアプリケーションによっては、同時に接続できる台数に制限がある場合があります。接続先の OS やアプリケーションの仕様をご確認ください。

Q 無線 LAN 通信ができない

「通信ができない」（→ P.187）の内容も確認してください。

A ランプの状態を確認してください

■IEEE802.11b/IEEE802.11g で通信ができない場合

本製品の IEEE802.11b/IEEE802.11g インターフェースが正常に動作中の場合、11g ランプ、STATUS ランプ、PWR ランプが点灯します。ランプの状態が次のような場合には、それぞれの対策を行ってください。

11g ランプ：消灯、STATUS ランプ：点灯、PWR ランプ：点灯の場合

IEEE802.11b/IEEE802.11g の無線スイッチが「オフ」に設定されています。
IEEE802.11b/IEEE802.11g 無線スイッチを「オン」にします。
設定方法については、「「IEEE802.11b/IEEE802.11g」画面」（→ P.75）をご覧ください。

11g ランプ：消灯、STATUS ランプ：消灯、PWR ランプ：点灯の場合

IEEE802.11b/IEEE802.11g インターフェースで不具合が発生しています。
本製品を再起動してください。再起動については、「再起動」（→ P.139）をご覧ください。再起動しても問題が解決しない場合は、「お問い合わせ先」（→ P.199）にご相談ください。

11a ランプ：消灯、11g ランプ：消灯、STATUS ランプ：点灯、PWR ランプ：点灯の場合

リンクインテグリティ機能で指定した機器との経路に不具合が発生しています。
本製品の LAN コネクタに、LAN ケーブルが正しく接続されているか確認してください。正しく接続されている場合は、リンクインテグリティ機能で IP アドレスを指定した機器が本製品と通信可能な状態かどうか確認してください。
「リンクインテグリティ」の設定については、「リンクインテグリティ設定」（→ P.134）をご覧ください。

■IEEE802.11a で通信ができない場合

本製品の IEEE802.11a インターフェースが動作中の場合、11a ランプ、STATUS ランプ、PWR ランプが点灯します。ランプの状態が次のような場合には、それぞれの対策を行ってください。

11a ランプ：消灯、STATUS ランプ：点灯、PWR ランプ：点灯の場合

IEEE802.11a の無線スイッチが「オフ」に設定されています。
IEEE802.11a 無線スイッチを「オン」にします。
設定方法については、「「IEEE802.11a」画面」（→ P.84）をご覧ください。

11a ランプ：消灯、STATUS ランプ：消灯、PWR ランプ：点灯の場合

IEEE802.11a インターフェースで不具合が発生しています。

本製品を再起動してください。再起動については、「再起動」（→ P.139）をご覧ください。再起動しても問題が解決しない場合は、「お問い合わせ先」（→ P.199）にご相談ください。

11a ランプ：消灯、11g ランプ：消灯、STATUS ランプ：点灯、PWR ランプ：点灯の場合

リンクインテグリティ機能で指定した機器との経路に不具合が発生しています。

本製品の LAN コネクタに、LAN ケーブルが正しく接続されているか確認してください。正しく接続されている場合は、リンクインテグリティ機能で IP アドレスを指定した機器が本製品と通信可能な状態かどうか確認してください。

「リンクインテグリティ」の設定については、「リンクインテグリティ設定」（→ P.134）をご覧ください。

A チャンネルの設定を確認してください

■IEEE802.11b/IEEE802.11g で通信ができない場合

次の点をご確認ください。

- 近くに他の無線 LAN ネットワークがある場合は、使用するチャンネルが重なると電波が干渉するため正常に通信が行えません。
  近くの無線 LAN ネットワークとは、チャンネルの値を 5 つ以上離して設定するようにしてください。
- 本製品のチャンネルの設定が 12 ～ 14 チャンネルで設定されていると、無線 LAN 端末の仕様によっては通信が行えない場合があります。
  無線 LAN 端末によっては、対応しているチャンネルの範囲が、1 ～ 11 チャンネルの場合があります。無線 LAN 端末側の仕様を確認して、このような場合には 1 ～ 11 チャンネルの範囲で固定のチャンネルを設定するようにしてください。

POINT

本製品のチャンネルの設定が「Auto（1～13ch）」または「Auto（1～14ch）」の場合

本製品が使用するチャンネルを自動的に設定するため、12 ～ 14 チャンネルに設定される可能性があります。無線 LAN 端末が 12 ～ 14 チャンネルを使用できない場合は、本製品のチャンネルを「Auto（1 ～ 13ch）」または「Auto（1 ～ 14ch）」に設定しないでください。

チャンネルの設定方法については、「「IEEE802.11b/IEEE802.11g」画面」（→ P.75）をご覧ください。

■IEEE802.11a で通信ができない場合

次の点をご確認ください。

- 近くに他の無線 LAN ネットワークがある場合は、使用するチャンネルが重なると電波が干渉するため正常に通信が行えません。
  近くの無線 LAN ネットワークとは、異なる値のチャンネルを設定するようにしてください。

チャンネルの設定方法については、「「IEEE802.11a」画面」（→ P.84）をご覧ください。

A IEEE802.11a の場合は使用できるチャンネルを確認してください

本製品で使用できる IEEE802.11a のチャンネルは、W52 ／ W53 の以下のチャンネルです。

・W52：36(5,180MHz)/40(5,200MHz)/44(5,220MHz)/48(5,240MHz)
・W53：52(5,260MHz)/56(5,280MHz)/60(5,300MHz)/64(5,320MHz)

IEEE802.11a で本製品に接続する無線 LAN 端末が、本製品で使用できるチャンネルに対応していない場合は、IEEE802.11a での通信はできません。

また、無線 LAN 端末が使用できるチャンネルの範囲が本製品と異なる場合は、無線 LAN 端末が使用できる範囲で固定のチャンネルを設定するようにしてください。「Auto」を選択すると、無線 LAN 端末が使用できないチャンネルで動作する可能性がありますので、ご注意ください。

A 本製品と無線 LAN 端末の設置場所を確認してください

本製品と無線 LAN 端末の距離を短くしたり、障害物をなくして見通しをよくしたりしてから、再度接続してください。

設置場所については、「設置場所について」（→ P.40）をご覧ください。

A 本製品とアンテナの接続を確認してください

本製品と外部アンテナ、または延長アンテナが正しく接続されているか確認してください。

アンテナの接続については、「アンテナの接続」（→ P.41）をご覧ください。

A SSID の設定を確認してください

SSID が、本製品と無線 LAN 端末で一致しているか確認してください。

本製品の設定の確認方法については、「ネットワークプロファイルの設定」（→ P.115）をご覧ください。

無線 LAN 端末側の設定の確認方法については、次のマニュアルをご覧ください。

・無線 LAN 機能が標準搭載されている場合は、パソコンのマニュアルをご覧ください。
・無線 LAN カードを増設した場合は、無線 LAN カードのマニュアルをご覧ください。

A MAC アドレスフィルタリングの設定を確認してください

MAC アドレスフィルタリングの設定で、「アドレス制御」が「許可」になっている場合、登録してある無線 LAN 端末のみ、本製品と接続できます。

また、「アドレス制御」が「拒否」になっている場合、登録してある無線 LAN 端末は、本製品と接続できません。

MAC アドレスフィルタリングの設定の確認方法は、「「MAC アドレス制御」カテゴリ」（→ P.109）をご覧ください。

A セキュリティを WEP で設定している場合は次の確認をしてください

無線 LAN 端末側で、電波状態や通信状態を確認して、本製品との接続状態によって次の項目を確認してください。

・「無線 LAN 端末と本製品が接続できていない場合」（→ P.192）
・「無線 LAN 端末と本製品が、接続はできるが通信はできない場合」（→ P.192）

無線 LAN 端末の電波状態の確認方法は、次のマニュアルをご覧ください。

・無線 LAN 機能が標準搭載されている場合は、パソコンのマニュアルをご覧ください。
・無線 LAN カードを増設した場合は、無線 LAN カードのマニュアルをご覧ください。

通信状態の確認方法は、「パソコンからの接続確認」（→ P.184）をご覧ください。

■無線 LAN 端末と本製品が接続できていない場合

ネットワーク認証とネットワークキーの設定が、本製品と無線 LAN 端末で一致しているか確認してください。

■無線 LAN 端末と本製品が、接続はできるが通信はできない場合

無線 LAN 端末の無線 LAN 接続状態を確認すると本製品と接続できているにもかかわらず、本製品との接続確認には失敗する場合は、ネットワークキーの値が一致しているか確認してください。

本製品のネットワーク認証とネットワークキーの設定については、「「WEP キー」カテゴリ」（→ P.102）をご覧ください。

無線 LAN 端末の仕様や設定の確認方法については、次のマニュアルをご覧になるか、お使いの機器のメーカーにお問い合わせください。

- 無線 LAN 機能が標準搭載されているパソコンの場合は、パソコンのマニュアルをご覧ください。
- 無線 LAN カードを増設した場合は、無線 LAN カードのマニュアルをご覧ください。

A セキュリティを WPA、または 802.11i (WPA2) で設定している場合は次の確認をしてください

WPA および 802.11i (WPA2) の設定については、「「WPA/802.11i (WPA2)」カテゴリ」（→ P.104）をご覧ください。

■認証モードによって次の確認をしてください

認証モードが「WPA-PSK」、「802.11i (WPA2)-PSK」、または「WPA-PSK/802.11i(WPA2)-PSK」の場合

PSK の設定が、本製品と無線 LAN 端末で一致しているかどうか確認してください。

- 「PSK 入力」で「パスフレーズ」を選択した場合
  「パスフレーズ」に設定したネットワークキーと、無線 LAN 端末のパスフレーズが一致しているか確認してください。
- 「PSK 入力」で「16 進数」を選択した場合
  「PSK」に設定したネットワークキーと無線 LAN 端末の 16 進数の値が一致しているか確認してください。

認証モードが「WPA」、「802.11i (WPA2)」、または「WPA/802.11i (WPA2)」の場合

「WPA/802.11i (WPA2)」に関する設定をご覧になり、設定が正しいかどうか確認してください。

■暗号化方式を確認してください

暗号化方式に「AES」を使用する場合は、無線 LAN 端末の機能が AES に対応している必要があります。無線 LAN 端末の仕様を確認して、AES に対応していない無線 LAN 端末がある場合には、暗号化方式を「自動」または「TKIP」に設定してください。

■本製品の暗号化方式の設定が「AES」または「自動」で、無線 LAN 端末の設定が「AES」の場合

無線 LAN 端末に次のパソコンをお使いになっている場合、無線 LAN ドライバのバージョンによっては本製品と通信できなくなる場合があります。

・弊社製無線 LAN 機能標準搭載モデルのパソコン
・ワイヤレス LAN カード FMV-JW481 を増設して使用しているパソコン
これらのパソコンお使いになっていて、このような現象が発生する場合は、無線 LAN ドライバを更新してください。無線 LAN ドライバの最新版は、富士通パソコン情報サイト FMWORLD.NET（http://www.fmworld.net/）でご提供しています。

■本製品の暗号化方式の設定が「自動」で、無線 LAN 端末の設定が「TKIP」の場合
無線 LAN 端末に、弊社製無線 LAN 機能標準搭載モデルのパソコンをお使いになっている場合、無線 LAN ドライバのバージョンによっては本製品と通信できなくなる場合があります。このような現象が発生する場合は、無線 LAN ドライバを更新してください。無線 LAN ドライバの最新版は、富士通パソコン情報サイト FMWORLD.NET（http://www.fmworld.net/）でご提供しています。

A AP 検出設定の定期スキャンの設定を確認してください

「管理機能」画面で「定期スキャン」を「有効」に設定している場合、すべての無線 LAN 端末は本製品に接続できません。有線 LAN 端末からのみ、接続が可能です。

Q IEEE802.11a で設定したチャンネルで動作しない

A DFS 機能によりチャンネルが自動的に変更されている可能性があります

IEEE802.11a で、W53 がサポートする周波数帯（52 ～ 64ch）を使用して運用している際に航空管制レーダーや気象レーダーなどで使用されるレーダー波を検出すると、本製品はただちに再起動し、IEEE802.11a インターフェースのチャンネルを 36 チャンネルに変更します。レーダー波を検出したチャンネルは再起動 30 分後に設定が可能となりますので、再起動前のチャンネルを使用する場合は、再度チャンネルの設定を行ってください。IEEE802.11a のチャンネル設定については、「「基本設定」カテゴリ」（→ P.87）をご覧ください。

Q IEEE802.1X で通信ができない

A 利用中のネットワーク名（SSID）を選択して、再接続してください

Windows XP SP2 のパソコンで、再接続を行う方法の一例を記載します。

1「スタート」ボタン→「コントロールパネル」の順にクリックします。

2「ネットワークとインターネット接続」をクリックします。

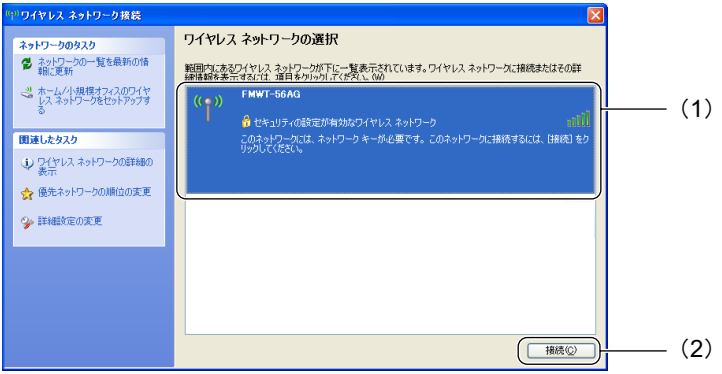
POINT

・「ネットワークとインターネット接続」が表示されていない場合は、そのまま手順 3 へお進みください。

3「ネットワーク接続」をクリックします。
「ネットワーク接続」ウィンドウに、現在インストールされているネットワークの一覧が表示されます。

4 一覧から「ワイヤレスネットワーク接続」を右クリックして、表示されるメニューから「利用できるワイヤレスネットワークの表示」をクリックします。
「ワイヤレスネットワーク接続」ウィンドウが表示されます。

5 (1)「ワイヤレスネットワークの選択」の一覧からご利用中のネットワーク名(SSID)をクリックして反転表示させ、(2)「接続」をクリックします。



Q SNMP エージェント機能が正常に動作しない

次の項目を確認する前に、SNMP マネージャと本製品が LAN 接続できていることを確認してから行ってください。接続確認の方法については、「パソコンからの接続確認」(→ P.184)をご覧ください。

A コミュニティ名を確認してください

SNMP の認証のために使用される「コミュニティ名」はエージェントとマネージャで一致している必要があります。本製品に設定されているコミュニティ名と SNMP マネージャに設定されているコミュニティ名が一致しているかどうか確認してください。

A MIB 情報を取得できない場合は SNMP の設定を確認してください

SNMP マネージャから本製品の MIB 情報を取得できない場合は、本製品の SNMP の設定を確認してください。

・「管理機能」画面の「システム設定」カテゴリー「SNMP」が「有効」になっていることを確認してください。

A MIB 情報を変更できない場合はコミュニティを「RW」にしてください

SNMP マネージャから本製品の MIB 情報を変更できない場合は、使用するコミュニティを「RW」に設定してください。

「管理機能」画面の「SNMP 設定」カテゴリー「コミュニティ名」が「RO」の場合、マネージャからの設定要求に応答しません。設定要求を許可する場合は、該当するコミュニティを「RW」に設定してください。

A トラップ送信先の設定を確認してください

本製品からのトラップを SNMP マネージャが受信できない場合は、トラップ送信先の設定を確認してください。

「管理機能」画面の「システム設定」カテゴリー「トラップ送信先」の「IP アドレス」に、SNMP マネージャがインストールされたパソコンの IP アドレスが設定されているか確認してください。
また、「管理機能」画面の「システム設定」カテゴリー「トラップ送信先」の「コミュニティ名」が SNMP マネージャと一致していることを確認してください。

A VLAN が有効な場合は SNMP マネージャの属する VLAN グループを確認してください

VLAN を有効にしている場合、SNMP マネージャとなるパソコンを「VLAN」画面の「管理 VLAN」に設定した VLAN グループに接続する必要があります。

A SNMP のアクセス制限の設定を確認してください

「管理機能」画面で「無線 LAN からのアクセス」を「拒否」に設定している場合、無線 LAN 端末から SNMP アクセスすることはできません。有線 LAN 端末からのみ、SNMP アクセスが可能です。

A SNMP マネージャとなるパソコンの OS が Windows XP の場合、パソコンのファイアウォールの設定を確認してください

Windows XP のファイアウォールが有効になっていると、本製品のトラップを SNMP マネージャが受信できない場合があります。この場合はパソコンのファイアウォールの詳細設定で、本製品から送信される SNMP のトラップを通過させるように設定を行ってください。
通過させるサービスの内容は次のとおりです。
・サービスの説明 ：snmptrap
・TCP または UDP ：UDP
・ポート番号 ：162
詳しくは、Windows XP のヘルプをご覧ください。

Q syslog サーバーにメッセージが通知されない

次の項目を確認する前に、本製品と syslog サーバーが LAN 接続できていることを確認してください。接続確認の方法については、「パソコンからの接続確認」（→ P.184）をご覧ください。

A 即時送出レベルの設定を確認してください

即時送出レベルの設定値未満の送出レベルのメッセージは、本製品の内部に保存されずに、すぐ送信されます。即時送出対象のメッセージは、起動中など本製品が通信出来ない状態では破棄されてしまいます。
各メッセージの送出レベルについては、「syslog メッセージ一覧」（→ P.225）をご覧ください。

A ログ送出レベルの設定を確認してください

送出されないメッセージの送出レベルがログ送出レベルに設定値より大きい場合、そのメッセージは送信されません。この場合はログ送出レベルの設定を、送信するメッセージの送出レベルに合わせて変更してください。
各メッセージの送出レベルについては、「syslog メッセージ一覧」（→ P.225）をご覧ください。

A syslog サーバーの設定を確認してください

本製品からのログを syslog サーバーが受信できない場合は、syslog サーバーの設定を確認してください。「管理機能」画面の「システム設定」カテゴリー「syslog サーバー 1」／「syslog サーバー 2」の「IP アドレス」に、syslog サーバーがインストールされたパソコンの IP アドレスが設定されているか確認してください。

A VLAN が有効の場合は syslog サーバーの属する VLAN グループを確認してください

VLAN を有効にしている場合、syslog サーバーとなるパソコンを「VLAN」画面の「管理 VLAN」に設定した VLAN グループに接続する必要があります。

A syslog サーバーとなるパソコンの OS が Windows XP の場合、パソコンのファイアウォールの設定を確認してください

Windows XP のファイアウォールが有効になっていると、本製品の syslog メッセージを syslog サーバーが受信できない場合があります。この場合はパソコンのファイアウォールの詳細設定で、本製品から送信される syslog メッセージを通過させるように設定を行ってください。

通過させるサービスの内容は次のとおりです。

・サービスの説明 ：syslog
・TCP または UDP ：UDP
・ポート番号 ：514 （「管理機能」画面の「システム設定」カテゴリー「syslog サーバー 1」／「syslog サーバー 2」の「ポート」に「514」が設定されている場合）

詳しくは、Windows XP のヘルプをご覧ください。

Q NTP サーバーからシステム時刻を自動取得できない

A 「管理機能」画面の「システム時刻」カテゴリの「NTP サーバー」の設定を確認してください

「管理機能」画面の「システム時刻」カテゴリの「NTP サーバー」に、NTP サーバーとなるパソコンの IP アドレスが正しく設定されているか確認してください。

A NTP サーバーとなるパソコンの OS が Windows XP の場合、パソコンのファイアウォールの設定を確認してください

Windows XP のファイアウォールが有効になっていると、本製品の NTP パケットを NTP サーバーが受信できない場合があります。この場合はパソコンのファイアウォールの詳細設定で、本製品から送信される NTP パケットを通過させるように設定を行ってください。

通過させるサービスの内容は次のとおりです。

・サービスの説明：Network Time Protocol
・TCP または UDP：UDP
・ポート番号：123

詳しくは、Windows XP のヘルプをご覧ください。

Q リンクインテグリティ機能により、本製品の無線電波が停止する

次の項目を確認する前に、有線 LAN 端末から本製品に対して、接続確認を行ってください。接続確認の方法については、「パソコンからの接続確認」（→ P.184）をご覧ください。

A 接続確認に失敗する場合は、指定した有線 LAN 側経路（本製品、本製品に接続している有線経路、HUB）に異常が発生しています

経路の異常から回復すると、「診断間隔」に設定した時間の経過後に本製品の無線電波が再開されます。

A 接続確認が成功する場合は、「管理機能」画面の「システム設定」カテゴリー「リンクインテグリティ」の「IP アドレス」の設定を確認してください

「管理機能」画面の「システム設定」カテゴリー「リンクインテグリティ」の「IP アドレス」に、監視する経路上にある機器の IP アドレスが正しく設定されているか確認してください。

A リンクインテグリティの「IP アドレス」に指定した機器が Windows XP のパソコンの場合、パソコンのファイアウォールの設定を確認してください

Windows XP のファイアウォールが有効になっていると、本製品のリンクインテグリティ機能が正しく動作しない場合があります。この場合は、パソコンのファイアウォールの詳細設定で、ICMP（Internet Control Message Protocol）のエコー要求の着信を許可するように設定を行う必要があります。
詳しくは、Windows XP のヘルプをご覧ください。

Q PING テストのテスト結果に「no answer from...」と表示される

A 「管理機能」画面の「PING テスト」カテゴリの「IP アドレス」の設定を確認してください

「管理機能」画面の「PING テスト」カテゴリの「IP アドレス」に、接続確認を行うパソコンの IP アドレスが正しく設定されているか確認してください。

A 接続確認を行うパソコンの OS が Windows XP の場合、パソコンのファイアウォールの設定を確認してください

Windows XP のファイアウォールが有効になっていると、本製品の PING テストが正常に行われない場合があります。この場合は、パソコンのファイアウォールの詳細設定で、ICMP（Internet Control Message Protocol）のエコー要求の着信を許可するように設定を行う必要があります。
詳しくは、Windows XP のヘルプをご覧ください。

Q Dr.WLAPPer をアンインストールしたい

Dr.WLAPPer のアンインストール方法について説明します。

POINT

・Dr.WLAPPer のアンインストールを行うには、OS に管理者権限でログインしている必要があります。

A Dr.WLAPPer をアンインストールする場合は次の手順で行ってください

1 画面右下の通知領域に表示されている Dr.WLAPPer 監視ツールのアイコン ( ) を右クリックし、表示されるメニューから「アプリケーションの終了」をクリックします。
通知領域から Dr.WLAPPer 監視ツールのアイコンが消えます。

2 次のように操作します。
Windows XP の場合
「スタート」ボタン→「コントロールパネル」の順にクリックし、「プログラムの追加と削除」をクリックします。
Windows 2000 の場合
「スタート」ボタン→「設定」→「コントロールパネル」の順にクリックし、「アプリケーションの追加と削除」をクリックします。
Windows Server 2003 の場合
「スタート」ボタン→「コントロールパネル」→「プログラムの追加と削除」の順にクリックします。
「プログラムの追加と削除」または「アプリケーションの追加と削除」ウィンドウが表示されます。

3 「現在インストールされているプログラム」で「Dr.WLAPPer」をクリックし、「削除」または「変更と削除」をクリックします。
「Dr.WLAPPer － 無線 LAN アクセスポイント管理ツール」ウィンドウが表示されます。

4 アンインストール確認のウィンドウで「はい」をクリックします。
Dr.WLAPPer が削除されます。

5 「アンインストール完了」が表示されたら、「完了」をクリックします。

6 すべてのウィンドウを閉じます。

7 パソコンを再起動します。

3 お問い合わせ先

本製品のご使用に際して何か困ったことが起きた場合は、ご購入元にご確認いただくか、以下それぞれのお問い合わせ先にご相談ください。

・おかけ間違いのないよう、ご注意ください。
・各窓口ともダイヤル後、音声ガイドに従い、ボタン操作を行ってください。
お客様の相談内容によって、各窓口へご案内いたします。
・システムメンテナンスのため、お問い合わせ時間であっても受け付けを休止させていただく場合があります。

■故障・修理に関するお問い合わせ先

□ 法人のお客様

「富士通ハードウェア修理相談センター」
・フリーダイヤル 0120-422-297
・お問い合わせ時間 9:00 ～ 17:00（土曜、日曜、祝日および年末年始を除く）

□ 個人のお客様

「富士通パーソナル製品に関するお問合せ窓口」
・フリーダイヤル 0120-950-222
・お問い合わせ時間 9:00 ～ 17:00

■技術的なご質問、ご相談のお問い合わせ先

「富士通パーソナル製品に関するお問合せ窓口」
・フリーダイヤル 0120-950-222
・お問い合わせ時間 9:00 ～ 17:00

8

第 8 章

付録

本製品をお使いになるうえで、またこのマニュアルをお読みになるうえで、参考となる内容を記述しています。

1 仕様

本製品の仕様です。

■製品名／型名

表：品名と型名

項目	仕様
品名	ワイヤレス LAN ステーション
型名	FMWT-56AG

■ハードウェア仕様

表：ハードウェア仕様

項目			仕様
無線 LAN インターフェース			・IEEE802.11a （5.2GHz 54Mbps 無線 LAN 標準プロトコル）準拠（W52/W53） ・IEEE802.11b （2.4GHz 11Mbps 無線 LAN 標準プロトコル）準拠 ・IEEE802.11g （2.4GHz 54Mbps 無線 LAN 標準プロトコル）準拠
	伝送方式		・OFDM 方式 ・DS-SS 方式
	転送レート		・DS-SS：11/5.5/2/1Mbps （自動／手動切り替え） ・OFDM：54/48/36/24/18/12/9/6Mbps （自動／手動切り替え）
	周波数範囲	IEEE802.11a（W52/W53）	5,160 ～ 5,360MHz
		IEEE802.11b	2,400 ～ 2,497MHz
		IEEE802.11g	2,400 ～ 2,484MHz
	チャンネル数	IEEE802.11a（W52/W53）	8 （36,40,44,48,52,56,60,64 のうち 1 つを使用）
		IEEE802.11b	14 （1 ～ 14 のうち 1 つを使用）
		IEEE802.11g	13 （1 ～ 13 のうち 1 つを使用）
	送信電力	IEEE802.11a（W52/W53）	18/15/12/9/0dBm
		IEEE802.11b/ IEEE802.11g	18/16.5/13.5/10.5/0dBm
	通信距離（目安）	IEEE802.11a（W52/W53）	15m
		IEEE802.11b/ IEEE802.11g	25m
有線 LAN インターフェース			100BASE-TX ／ 10BASE-T × 1 ポート （自動極性反転）
動作電源電圧			AC アダプタ使用時：AC100V 50Hz ／ 60Hz 電源供給ユニット使用時：DC48V
温湿度条件			・温度 5 ～ 35 ℃／湿度 20 ～ 80%RH （動作時） ・温度 -10 ～ 60 ℃／湿度 20 ～ 80%RH （非動作時） ［注］ただし、動作時、非動作時とも結露しないこと
消費電力			AC アダプタ使用時：約 10W （最大） 電源供給ユニット使用時：約 11W（最大）

表：ハードウェア仕様

項目	仕様
外形寸法	W190 × D130 × H40（mm）
質量	300g
VCCI	Class B
耐用年数	5 年
その他	・ Power over Ethernet（独自方式／ IEEE802.3af 方式） ・ 電源供給ユニット（オプション） ・ 盗難防止用ロック取り付け穴 ・ 延長アンテナ（ケーブル長 2.5m） ・ 取り付けユニット（本体用／ AC アダプタ用／延長アンテナ用）

■ソフトウェア仕様

表：ソフトウェア仕様

項目		仕様
セキュリティ	無線 LAN	・マルチプル SSID （VLAN 有効時 16 個） ・マルチプルセキュリティポリシー（VLAN 有効時 16 個） ・WEP （64 ビット、128 ビット、152 ビット）[注 1] ・MAC アドレスフィルタリング ・IEEE802.1X （EAP-MD5、EAP-TLS、EAP-TTLS、PEAP） ・SSID 認証 ・ANY キー接続拒否 ・SSID の隠蔽（ESS-ID 非通知） ・WPA 認証モード （PSK、RADIUS） ・WPA 暗号化方式 （TKIP、AES） ・IEEE802.11i (WPA2) 認証モード （PSK、RADIUS） ・IEEE802.11i (WPA2) 暗号化方式 （TKIP、AES） ・プライバシープロテクション ・無線 LAN 端末からのログイン制限 ・無線 LAN 端末からの SNMP アクセス制限
	有線 LAN	・認証 VLAN ・管理 VLAN の指定
管理機能		・リンクインテグリティ （ルート診断） ・PING テスト ・RADIUS アカウンティング ・syslog ・SNMP エージェント（v1/v2c） ・MIB（MIB-2/dot11/dot1pae/ 拡張） ・Web 設定画面用管理者パスワード （2 種：Read only、Read/Write） ・NTP 時刻設定 ・ファームウェア更新 ・設定内容ファイル保存／復元 ・無通信切断タイマー ・ポート番号 ・周辺無線 LAN アクセスポイント検出
ネットワーク機能	無線 LAN	・DHCP サーバー ・ローミング （FMWT シリーズ､FMWBR シリーズで同通信規格の無線 LAN 方式） ・WDS ・WMM ・簡易ロードバランス（接続台数制限） ・Proxy ARP ・ポート VLAN（SSID ごとに 16 個）
	有線 LAN	・タグ VLAN （16 個） ・DHCP サーバー ・DHCP クライアント
無線 LAN 機能		・Wi-Fi 認定 ・Super A/G ・無線スイッチ（RF スイッチ） ・送信電力制御（5 段階） ・DFS ・TPC ・IEEE802.11g プロテクション
無線 LAN 端末接続台数		・IEEE802.11a（W52/W53）：20 台 [注 2] ・IEEE802.11g：20 台 [注 2]
対応ブラウザ （設定画面）		Internet Explorer 5.0 以降

［注 1］ ネットワークキー（WEP）による暗号化は上記ビット数で行いますが、設定可能なビット数は固定長 24 ビットを引いた 40 ビット、104 ビット、128 ビットです。

［注 2］ お使いになる環境によっては、接続可能台数は減少することがあります。

■管理ソフトウェア仕様

表：管理ソフトウェア仕様

項目	仕様
名称	Dr.WLAPPer （ドクターラッパー）
対応 OS	・ Microsoft® Windows® XP Professional Service pack 1 以降 ・ Microsoft® Windows® XP Home Edition Service pack 1 以降 ・ Microsoft® Windows® 2000 Professional Service pack 3 以降 ［注 1］ ・ Microsoft® Windows Server™ 2003 Standard Edition

［注 1］ Microsoft® XML Parser (MSXML) 3.0 以降がインストールされている必要があります。Microsoft® XML Parser (MSXML) については、Microsoft のホームページをご覧ください。

2 MIB 情報一覧

本製品がサポートしている MIB 情報の一覧とトラップを記載します。

標準 MIB 対応オブジェクト一覧

本製品がサポートする標準 MIB の一覧です。

■system グループ（RFC1213）

表：標準 MIB：system グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	ACCESS
sysDescr	system.1	DisplayString	RO
sysObjectID	system.2	ObjectID	RO
sysUpTime	system.3	TimeTicks	RO
sysContact	system.4	DisplayString	RW
sysName	system.5	DisplayString	RW
sysLocation	system.6	DisplayString	RW
sysServices	system.7	INTEGER	RO

■interface グループ（RFC1213、RFC1573）

表：標準 MIB：interface グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	ACCESS
ifNumber	interfaces.1	INTEGER	RO
ifTable	interfaces.2	SEQUENCE OF	NA
ifEntry	ifTable.1	IfEntry	NA
ifIndex	ifEntry.1	INTEGER	RO
ifDescr	ifEntry.2	DisplayString	RO
ifType	ifEntry.3	INTEGER	RO
ifMtu	ifEntry.4	INTEGER	RO
ifSpeed	ifEntry.5	Gauge	RO
ifPhysAddress	ifEntry.6	PhysAddress	RO
ifAdminStatus	ifEntry.7	INTEGER	RW
ifOperStatus	ifEntry.8	INTEGER	RO
ifInOctets	ifEntry.10	Counter	RO
ifInUcastPkts	ifEntry.11	Counter	RO
ifInDiscards	ifEntry.13	Counter	RO
ifInErrors	ifEntry.14	Counter	RO
ifOutOctets	ifEntry.16	Counter	RO
ifOutUcastPkts	ifEntry.17	Counter	RO
ifOutDiscards	ifEntry.19	Counter	RO
ifOutErrors	ifEntry.20	Counter	RO
ifOutQLen	ifEntry.21	Gauge	RO
ifSpecific	ifEntry.22	ObjectID	RO

■address translation グループ（RFC1213）

表：標準 MIB：address translation グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	ACCESS
atTable	at.1	SEQUENCE OF	NA
atEntry	atTable.1	AtEntry	NA
atIfIndex	atEntry.1	INTEGER	RW
atPhysAddress	atEntry.2	PhysAddress	RW
atNetAddress	atEntry.3	NetworkAddress	RW

■ip グループ（RFC1213、RFC2011）

表：標準 MIB：ip グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	ACCESS
ipForwarding	ip.1	INTEGER	RW
ipDefaultTTL	ip.2	INTEGER	RW
ipInReceives	ip.3	Counter	RO
ipInHdrErrors	ip.4	Counter	RO
ipInAddrErrors	ip.5	Counter	RO
ipForwDatagrams	ip.6	Counter	RO
ipInUnknownProtos	ip.7	Counter	RO
ipInDiscards	ip.8	Counter	RO
ipInDelivers	ip.9	Counter	RO
ipOutRequests	ip.10	Counter	RO
ipOutDiscards	ip.11	Counter	RO
ipOutNoRoutes	ip.12	Counter	RO
ipReasmTimeout	ip.13	INTEGER	RO
ipReasmReqds	ip.14	Counter	RO
ipReasmOKs	ip.15	Counter	RO
ipReasmFails	ip.16	Counter	RO
ipFragOKs	ip.17	Counter	RO
ipFragFails	ip.18	Counter	RO
ipFragCreates	ip.19	Counter	RO

■icmp グループ（RFC1213、RFC2011）

表：標準 MIB：icmp グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	ACCESS
icmpInMsgs	icmp.1	Counter	RO
icmpInErrors	icmp.2	Counter	RO
icmpInDestUnreachs	icmp.3	Counter	RO
icmpInTimeExcds	icmp.4	Counter	RO
icmpInParmProbs	icmp.5	Counter	RO
icmpInSrcQuenchs	icmp.6	Counter	RO
icmpInRedirects	icmp.7	Counter	RO
icmpInEchos	icmp.8	Counter	RO
icmpInEchoReps	icmp.9	Counter	RO
icmpInTimestamps	icmp.10	Counter	RO
icmpInTimestampReps	icmp.11	Counter	RO
icmpInAddrMasks	icmp.12	Counter	RO
icmpInAddrMaskReps	icmp.13	Counter	RO
icmpOutMsgs	icmp.14	Counter	RO
icmpOutErrors	icmp.15	Counter	RO
icmpOutDestUnreachs	icmp.16	Counter	RO
icmpOutTimeExcds	icmp.17	Counter	RO
icmpOutParmProbs	icmp.18	Counter	RO
icmpOutSrcQuenchs	icmp.19	Counter	RO
icmpOutRedirects	icmp.20	Counter	RO
icmpOutEchos	icmp.21	Counter	RO
icmpOutEchoReps	icmp.22	Counter	RO
icmpOutTimestamps	icmp.23	Counter	RO
icmpOutTimestampReps	icmp.24	Counter	RO
icmpOutAddrMasks	icmp.25	Counter	RO
icmpOutAddrMaskReps	icmp.26	Counter	RO

■tcp グループ（RFC1213、RFC2012）

表：標準 MIB：tcp グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	ACCESS
tcpRtoAlgorithm	tcp.1	INTEGER	RO
tcpRtoMin	tcp.2	INTEGER	RO
tcpRtoMax	tcp.3	INTEGER	RO
tcpMaxConn	tcp.4	INTEGER	RO
tcpActiveOpens	tcp.5	Counter	RO
tcpPassiveOpens	tcp.6	Counter	RO
tcpAttemptFails	tcp.7	Counter	RO
tcpEstabResets	tcp.8	Counter	RO
tcpCurrEstab	tcp.9	Gauge	RO
tcpInSegs	tcp.10	Counter	RO
tcpOutSegs	tcp.11	Counter	RO
tcpRetransSegs	tcp.12	Counter	RO
tcpConnTable	tcp.13	SEQUENCE OF	NA
tcpConnEntry	tcpConnTable.1	TcpConnEntry	NA
tcpConnState	tcpConnEntry.1	INTEGER	RW
tcpConnLocalAddress	tcpConnEntry.2	IpAddress	RO
tcpConnLocalPort	tcpConnEntry.3	INTEGER	RO
tcpConnRemAddress	tcpConnEntry.4	IpAddress	RO
tcpConnRemPort	tcpConnEntry.5	INTEGER	RO
tcpInErrs	tcp.14	Counter	RO
tcpOutRsts	tcp.15	Counter	RO

■udp グループ（RFC1213、RFC2013）

表：標準 MIB：udp グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	ACCESS
udpInDatagrams	udp.1	Counter	RO
udpNoPorts	udp.2	Counter	RO
udpInErrors	udp.3	Counter	RO
udpOutDatagrams	udp.4	Counter	RO

■snmp グループ（RFC1213）

表：標準 MIB：snmp グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	ACCESS
snmpInPkts	snmp.1	Counter	RO
snmpOutPkts	snmp.2	Counter	RO
snmpInBadVersions	snmp.3	Counter	RO
snmpInBadCommunityNames	snmp.4	Counter	RO
snmpInBadCommunityUses	snmp.5	Counter	RO
snmpInASNParseErrs	snmp.6	Counter	RO
snmpInTooBigs	snmp.8	Counter	RO
snmpInNoSuchNames	snmp.9	Counter	RO
snmpInBadValues	snmp.10	Counter	RO
snmpInReadOnlys	snmp.11	Counter	RO
snmpInGenErrs	snmp.12	Counter	RO
snmpInTotalReqVars	snmp.13	Counter	RO
snmpInTotalSetVars	snmp.14	Counter	RO
snmpInGetRequests	snmp.15	Counter	RO
snmpInGetNexts	snmp.16	Counter	RO
snmpInSetRequests	snmp.17	Counter	RO
snmpInGetResponses	snmp.18	Counter	RO
snmpInTraps	snmp.19	Counter	RO
snmpOutTooBigs	snmp.20	Counter	RO
snmpOutNoSuchNames	snmp.21	Counter	RO
snmpOutBadValues	snmp.22	Counter	RO
snmpOutGenErrs	snmp.24	Counter	RO
snmpOutGetRequests	snmp.25	Counter	RO
snmpOutGetNexts	snmp.26	Counter	RO
snmpOutSetRequests	snmp.27	Counter	RO
snmpOutGetResponses	snmp.28	Counter	RO
snmpOutTraps	snmp.29	Counter	RO
snmpEnableAuthenTraps	snmp.30	INTEGER	RO

■ieee802dot11 グループ（ieee802dot11）

表：標準 MIB：ieee802dot11 グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	ACCESS
ieee802dot11	iso.member-body.us.ieee802dot11	–	–

■dot11smt グループ（ieee802dot11）

表：標準 MIB：dot11smt グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	ACCESS
dot11smt	ieee802dot11.1	—	—
dot11StationConfigTable	dot11smt.1	SEQUENCE OF	NA
dot11StationConfigEntry	dot11StationConfigTable.1	Dot11StationConfigEntry	NA
dot11StationId	dot11StationConfigEntry.1	MacAddress	RO
dot11CFPollable	dot11StationConfigEntry.3	TruthValue	RO
dot11CFPPeriod	dot11StationConfigEntry.4	INTEGER	RO
dot11CFPMaxDuration	dot11StationConfigEntry.5	INTEGER	RO
dot11PrivacyOptionImplemented	dot11StationConfigEntry.7	TruthValue	RO
dot11DesiredSSID	dot11StationConfigEntry.9	OCTECT STRING	RW
dot11DesiredBSSType	dot11StationConfigEntry.10	INTEGER	RO
dot11BeaconPeriod	dot11StationConfigEntry.12	INTEGER	RW
dot11DTIMPeriod	dot11StationConfigEntry.13	INTEGER	RW
dot11AuthenticationAlgorithmsTable	dot11smt.2	SEQUENCE OF	NA
dot11AuthenticationAlgorithmsEntry	dot11AuthenticationAlgorithmsTable.1	Dot11AuthenticationAlgorithmsEntry	NA
dot11AuthenticationAlgorithmsIndex	dot11AuthenticationAlgorithmsEntry.1	INTEGER	NA
dot11AuthenticationAlgorithm	dot11AuthenticationAlgorithmsEntry.2	INTEGER	RO
dot11AuthenticationAlgorithmsEnable	dot11AuthenticationAlgorithmsEntry.3	TruthValue	RO
dot11PrivacyTable	dot11smt.5	SEQUENCE OF	NA
dot11PrivacyEntry	dot11PrivacyTable.1	Dot11PrivacyEntry	NA
dot11PrivacyInvoked	dot11PrivacyEntry.1	TruthValue	RO
dot11WEPDefaultKeyID	dot11PrivacyEntry.2	INTEGER	RO
dot11WEPKeyMappingLength	dot11PrivacyEntry.3	INTEGER	RO
dot11ExcludeUnencrypted	dot11PrivacyEntry.4	TruthValue	RO
dot11WEPICVErrorCount	dot11PrivacyEntry.5	Counter32	RO
dot11WEPExcludedCount	dot11PrivacyEntry.6	Counter32	RO
dot11SMTnotification	dot11smt.6	—	—
dot11Disassociate	dot11SMTnotification.0.1	OBJECTS	—
dot11Deauthenticate	dot11SMTnotification.0.2	OBJECTS	—
dot11AuthenticateFail	dot11SMTnotification.0.3	OBJECTS	—

■dot11mac グループ（ieee802dot11）

表：標準 MIB：dot11mac グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	ACCESS
dot11mac	ieee802dot11.2	—	—
dot11OperationTable	dot11mac.1	SEQUENCE OF	NA
dot11OperationEntry	dot11OperationTable.1	Dot11OperationEntry	NA
dot11MACAddress	dot11OperationEtnry.1	MacAddress	RO
dot11RTSThreshold	dot11OperationEtnry.2	INTEGER	RW
dot11FragmentationThreshold	dot11OperationEtnry.5	INTEGER	RW
dot11MaxTransmitMSDULifetime	dot11OperationEntry.6	INTEGER	RO
dot11MaxReceiveLifetime	dot11OperationEntry.7	INTEGER	RO
dot11ManufacturerID	dot11OperationEtnry.8	DisplayString	RO
dot11ProductID	dot11OperationEtnry.9	DisplayString	RO
dot11CountersTable	dot11mac.2	SEQUENCE OF	NA
dot11CountersEntry	dot11CountersTable.1	Dot11CountersEntry	NA
dot11TransmittedFragmentCount	dot11CountersEntry.1	Counter32	RO
dot11MulticastTransmittedFrameCount	dot11CountersEntry.2	Counter32	RO
dot11FailedCount	dot11CountersEntry.3	Counter32	RO
dot11RetryCount	dot11CountersEntry.4	Counter32	RO
dot11MultipleRetryCount	dot11CountersEntry.5	Counter32	RO
dot11FrameDuplicateCount	dot11CountersEntry.6	Counter32	RO
dot11RTSSuccessCount	dot11CountersEntry.7	Counter32	RO
dot11RTSFailureCount	dot11CountersEntry.8	Counter32	RO
dot11ACKFailureCount	dot11CountersEntry.9	Counter32	RO
dot11ReceivedFragmentCount	dot11CountersEntry.10	Counter32	RO
dot11MulticastReceivedFrameCount	dot11CountersEntry.11	Counter32	RO
dot11FCSErrorCount	dot11CountersEntry.12	Counter32	RO
dot11TransmittedFrameCount	dot11CountersEntry.13	Counter32	RO
dot11WEPUndecryptableCount	dot11CountersEntry.14	Counter32	RO

■dot11resAttribute グループ（ieee802dot11）

表：標準 MIB：dot11resAttribute グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	ACCESS
dot11res	ieee802dot11.3	—	—
dot11resAttribute	dot11res.1	—	—
dot11ResourceTypeIDName	dot11resAttribute.1	DisplayString	RO
dot11ResourceInfoTable	dot11resAttribute.2	SEQUENCE OF	NA
dot11ResourceInfoEntry	dot11ResourceInfoTable.1	Dot11ResourceInfoEntry	NA
dot11manufacturerOUI	dot11ResourceInfoEntry.1	OCTECT STRING	RO
dot11manufacturerName	dot11ResourceInfoEntry.2	DisplayString	RO
dot11manufacturerProductName	dot11ResourceInfoEntry.3	DisplayString	RO
dot11manufacturerProductVerion	dot11ResourceInfoEntry.4	DisplayString	RO

■dot11phy グループ（ieee802dot11）

表：標準 MIB：dot11phy グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	ACCESS
dot11phy	ieee802dot11.4	—	—
dot11PhyOperationTable	dot11phy.1	SEQUENCE OF	NA
dot11PhyOperationEntry	dot11PhyOperationTable.1	Dot11PhyOperationEntry	NA
dot11PHYType	dot11PhyOperationEntry.1	INTEGER	RO
dot11CurrentRegDomain	dot11PhyOperationEntry.2	Integer32	RO
dot11TempType	dot11PhyOperationEntry.3	INTEGER	RO
dot11PhyAntennaTable	dot11phy.2	SEQUENCE OF	NA
dot11PhyAntennaEntry	dot11PhyAntennaTable.1	Dot11PhyAntennaEntry	NA
dot11CurrentTxAntenna	dot11PhyAntennaEntry.1	INTEGER	RO
dot11DiversitySupport	dot11PhyAntennaEntry.2	INTEGER	RO
dot11CurrentRxAntenna	dot11PhyAntennaEntry.3	Integer32	RO
dot11PhyTxPowerTable	dot11phy.3	SEQUENCE OF	NA
dot11PhyTxPowerEntry	dot11PhyTxPowerTable.1	SEQUENCE OF	NA
dot11NumberSupportedPowerLevels	dot11PhyTxPowerEntry.1	INTEGER	RO
dot11CurrentTxPowerLevel	dot11PhyTxPowerEntry.10	INTEGER	RW
dot11PhyDSSSTable	dot11phy.5	SEQUENCE OF	NA
dot11PhyDSSSEntry	dot11PhyDSSSTable.1	Dot11PhyDSSSEntry	NA
dot11CurrentChannel	dot11PhyDSSSEntry.1	INTEGER	RW
dot11RegDomainsSupportedTable	dot11phy.7	SEQUENCE OF	NA
dot11RegDomainsSupportEntry	dot11RegDomainsSupportedTable.1	Dot11RegDomainsSupportEntry	NA
dot11RegDomainsSupportIndex	dot11RegDomainsSupportEntry.1	Integer32	NA
dot11RegDomainsSupportValue	dot11RegDomainsSupportEntry.2	INTEGER	RO

■PAE グループ（ieee8021pae）

表：標準 MIB：PAE グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	ACCESS
ieee8021paeMIB	iso.std.iso8802.ieee802dot1.ieee802dot1mibs.1	—	—
paeMIBObjects	ieee8021paeMIB.1	—	—

■PAE System グループ（ieee8021pae）

表：標準 MIB：PAE System グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	ACCESS
dot1xPaeSystem	paeMIBObjects.1	—	—
dot1xPaePortTable	dot1xPaeSystem.2	SEQUENCE OF	NA
dot1xPaePortEntry	dot1xPaePortTable	Dot1xPaePortEntry	NA
dot1xPaePortNumber	dot1xPaePortEntry.1	InterfaceIndex	NA
dot1xPaePortProtocolVersion	dot1xPaePortEntry.2	Unsigned32	RO
dot1xPaePortInitialize	dot1xPaePortEntry.4	TruthValue	RW

■PAE Authenticator グループ（ieee8021pae）

表：標準 MIB：PAE Authenticator グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	ACCESS
dot1xPaeAuthenticator	paeMIBObjects.2	—	—
dot1xAuthConfigTable	dot1xPaeAuthenticator.1	SEQUENCE OF	NA
dot1xAuthConfigEntry	dot1xAuthConfigTable.1	Dot1xAuthConfigEntry	NA
dot1xAuthPaeState	dot1xAuthConfigEntry.1	INTEGER	RO
dot1xAuthBackendAuthState	dot1xAuthConfigEntry.2	INTEGER	RO
dot1xAuthAuthControlledPortStatus	dot1xAuthConfigEntry.5	PaeControlledPortStatus	RO
dot1xAuthAuthControlledPortControl	dot1xAuthConfigEntry.6	PaeControlledPortControl	RW
dot1xAuthQuietPeriod	dot1xAuthConfigEntry.7	Unsigned32	RW
dot1xAuthTxPeriod	dot1xAuthConfigEntry.8	Unsigned32	RW
dot1xAuthSuppTimeout	dot1xAuthConfigEntry.9	Unsigned32	RW
dot1xAuthServerTimeout	dot1xAuthConfigEntry.10	Unsigned32	RW
dot1xAuthMaxReq	dot1xAuthConfigEntry.11	Unsigned32	RW
dot1xAuthReAuthPeriod	dot1xAuthConfigEntry.12	Unsigned32	RW
dot1xAuthReAuthEnabled	dot1xAuthConfigEntry.13	Unsigned32	RW
dot1xAuthKeyTxEnabled	dot1xAuthConfigEntry.14	Unsigned32	RW
dot1xAuthDiagTable	dot1xPaeAuthenticator.3	SEQUENCE OF	NA
dot1xAuthDiagEntry	dot1xAuthDiagTable.1	Dot1xAuthDiagEntry	NA
dot1xAuthEntersConnecting	dot1xAuthDiagEntry.1	Counter32	RO
dot1xAuthEapLogoffsWhileConnecting	dot1xAuthDiagEntry.2	Counter32	RO
dot1xAuthEntersAuthenticating	dot1xAuthDiagEntry.3	Counter32	RO
dot1xAuthAuthSuccessWhileAuthenticating	dot1xAuthDiagEntry.4	Counter32	RO
dot1xAuthAuthTimeoutsWhileAuthenticating	dot1xAuthDiagEntry.5	Counter32	RO
dot1xAuthAuthFailWhileAuthenticating	dot1xAuthDiagEntry.6	Counter32	RO
dot1xAuthAuthReauthsWhileAuthenticating	dot1xAuthDiagEntry.7	Counter32	RO
dot1xAuthAuthEapStartsWhileAuthenticating	dot1xAuthDiagEntry.8	Counter32	RO
dot1xAuthAuthEapLogoffWhileAuthenticating	dot1xAuthDiagEntry.9	Counter32	RO
dot1xAuthAuthReauthsWhileAuthenticated	dot1xAuthDiagEntry.10	Counter32	RO
dot1xAuthAuthEapStartsWhileAuthenticated	dot1xAuthDiagEntry.11	Counter32	RO
dot1xAuthAuthEapLogoffWhileAuthenticated	dot1xAuthDiagEntry.12	Counter32	RO
dot1xAuthBackendResponses	dot1xAuthDiagEntry.13	Counter32	RO
dot1xAuthBackendAccessChallenges	dot1xAuthDiagEntry.14	Counter32	RO
dot1xAuthBackendOtherRequestsToSupplicant	dot1xAuthDiagEntry.15	Counter32	RO
dot1xAuthBackendNonNakResponsesFromSupplicant	dot1xAuthDiagEntry.16	Counter32	RO
dot1xAuthBackendAuthSuccesses	dot1xAuthDiagEntry.17	Counter32	RO
dot1xAuthBackendAuthFails	dot1xAuthDiagEntry.18	Counter32	RO
dot1xAuthSessionStatsTable	dot1xPaeAuthenticator.4	SEQUENCE OF	NA
dot1xAuthSessionStatsEntry	dot1xAuthSessionStatsTable.1	Dot1xAuthSessionStatsEntry	NA
dot1xAuthSessionId	dot1xAuthSessionStatsEntry.5	SnmpAdminString	RO
dot1xAuthSessionAuthenticMethod	dot1xAuthSessionStatsEntry.6	INTEGER	RO
dot1xAuthSessionUserName	dot1xAuthSessionStatsEntry.9	SnmpAdminString	RO

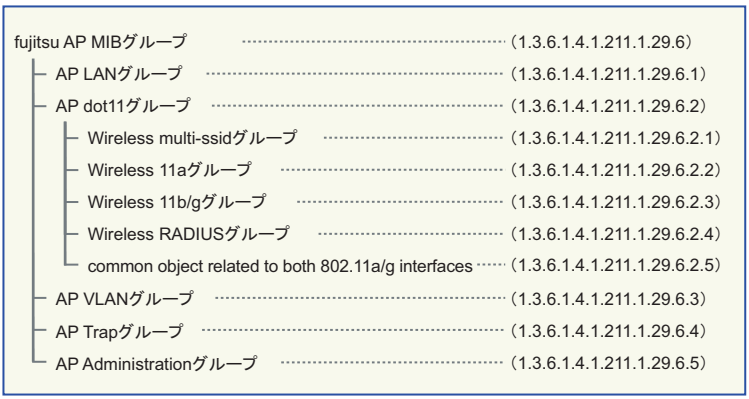
拡張 MIB 対応オブジェクト一覧

本製品がサポートする拡張 MIB の一覧です。

POINT

拡張 MIB のツリー構造について

本製品の拡張 MIB のツリー構造を図で示しています。() 内はオブジェクト ID です。



■ fujitsu AP MIB グループ

オブジェクト ID ：1.3.6.1.4.1.211.1.29.6

表：拡張 MIB：fujitsu AP MIB グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	値	ACCESS	説明
fjap	enterprises.fujitsu.product.pcLan.6	–	1.3.6.1.4.1.211.1.29.6	–	–

■AP LAN グループ

オブジェクト ID ：1.3.6.1.4.1.211.1.29.6.1

表：拡張 MIB：AP LAN グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	値	ACCESS	説明
fjapLan	fjap.1	–	–	–	–
lanConnectMode	fjapLan.1	INTEGER	DHCP クライアント (0), 手動設定 (1)	RW	IP アドレス取得方法
lanDhcpServerSwitch	fjapLan.2	INTEGER	無効 (0), 有効 (1)	RW	DHCP サーバー機能の有効／無効
lanDhcpServerLsRangeStart	fjapLan.3	IpAddress	–	RW	DHCP で割り当てるアドレス範囲の開始アドレス
lanDhcpServerLsRangeEnd	fjapLan.4	IpAddress	–	RW	DHCP で割り当てるアドレス範囲の終了アドレス
lanDhcpServerLsTime	fjapLan.5	Integer32	0 ～ 99999	RW	DHCP サービスのアドレスリース時間
lanDhcpServerDefaultGateway	fjapLan.6	IpAddress	–	RW	DHCP サービスのデフォルトゲートウェイ
lanDhcpServerPrimaryDNS	fjapLan.7	IpAddress	–	RW	DHCPサービスのDNSサーバー IP アドレスその 1
lanDhcpServerSecondaryDNS	fjapLan.8	IpAddress	–	RW	DHCPサービスのDNSサーバー IP アドレスその 2
lanDhcpServerTertiaryDNS	fjapLan.9	IpAddress	–	RW	DHCPサービスのDNSサーバー IP アドレスその 3
lanDhcpServerPrimaryWINS	fjapLan.10	IpAddress	–	RW	DHCP サービスの WINS サーバー IP アドレスその 1
lanDhcpServerSecondaryWINS	fjapLan.11	IpAddress	–	RW	DHCP サービスの WINS サーバー IP アドレスその 2
lanDhcpServerTertiaryWINS	fjapLan.12	IpAddress	–	RW	DHCP サービスの WINS サーバー IP アドレスその 3
proxyARP	fjapLan.13	INTEGER	無効 (0), 有効 (1)	RW	proxyARP の有効／無効

■AP dot11 グループ

オブジェクト ID ：1.3.6.1.4.1.211.1.29.6.2

表：拡張 MIB：AP dot11 グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	値	ACCESS	説明
fjapDot11	fjap.2	–	–	–	–

■Wireless multi-ssid グループ

オブジェクト ID ：1.3.6.1.4.1.211.1.29.6.2.1

表：拡張 MIB：Wireless multi-ssid グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	値	ACCESS	説明
multissid	fjapDot11.1	—	—	—	—
multissidCtrlTable	multissid.1	SEQUENCE OF	—	NA	—
multissidCtrlEntry	multissidCtrlTable.1	MultissidCtrlEntry	—	NA	—
multissidCtrlIndex	multissidCtrlEntry.1	Integer32	1 ～ 16	NA	SNMP 管理の対象ネットワークプロファイル番号
multissidCtrlSSID	multissidCtrlEntry.2	OCTET STRING	—	RW	対象ネットワークプロファイルの SSID
multissidCtrlInterface	multissidCtrlEntry.3	INTEGER	両方 (0), 11b/11g(1), 11a(2)	RW	対象ネットワークプロファイルの無線 LAN インターフェース
multissidCtrlSecurityPolicy	multissidCtrlEntry.4	Integer32	1 ～ 16	RW	SNMP 管理の対象セキュリティポリシー番号
multissidCtrlvlanId	multissidCtrlEntry.5	Integer32	1 ～ 16	RW	SNMP 管理の対象 VLAN ID
securityPolicyTable	multissid.2	SEQUENCE OF	—	NA	—
securityPolicyEntry	securityPolicyTable.1	SecurityPolicyEntry	—	NA	—
securityPolicyIndex	securityPolicyEntry.1	Integer32	1 ～ 16	NA	設定済のセキュリティポリシー数
securityPolicyName	securityPolicyEntry.2	OCTET STRING	0 ～ 30	RW	対象セキュリティポリシーのポリシー名
securityPolicyAuthMode	securityPolicyEntry.3	INTEGER	ベーシック (0), アドバンスド (1)	RW	セキュリティのモード
securityPolicy1xSwitch	securityPolicyEntry.4	INTEGER	未使用 (0), 使用 (1)	RW	IEEE802.1X 機能の使用／未使用
securityPolicy1xKeyDist	securityPolicyEntry.5	INTEGER	無効 (0), 有効 (1)	RW	キーの配信の有効／無効
securityPolicy1xReauth	securityPolicyEntry.6	INTEGER	無効 (0), 有効 (1)	RW	キー配信時の再認証の有効／無効
securityPolicy1xReKeyInterval	securityPolicyEntry.7	Integer32	15 ～ 1440	RW	キー更新間隔 (分)
securityPolicyWpaAuthMode	securityPolicyEntry.8	INTEGER	WPA-PSK(0), WPA(1), 11i-PSK(2), 11i(3), Auto-PSK(4), Auto(5)	RW	WPA の認証モード
wpaGrpkeyRekeyInterval	securityPolicyEntry.9	Integer32	900 ～ 86400	RW	グループキー更新間隔(秒)
securityPolicyWpaEncMode	securityPolicyEntry.10	INTEGER	TKIP(0), AES(1), 自動 (2)	RW	WPA の暗号化方式
securityPolicyWpaPSKMode	securityPolicyEntry.11	INTEGER	パスフレーズ (0), 16 進数 (1)	RW	PSK のフォーマット
securityPolicyACLMode	securityPolicyEntry.12	INTEGER	無効 (0), 許可 (1), 拒否 (2)	RW	MAC アドレスフィルタリングのアドレス制御の設定
dot11RadiusSsidAuth	securityPolicyEntry.15	INTEGER	無効 (0), 有効 (1)	RW	SSID 認証の有効／無効
aclCtrlTable	multissid.3	SEQUENCE OF	—	NA	—
aclCtrlEntry	aclCtrlTable.1	AclCtrlEntry	—	NA	—
aclCtrlIndex	aclCtrlEntry.1	Integer32	1 ～ 128	NA	アドレス一覧に登録済の MAC アドレス数
aclCtrlMacAddress	aclCtrlEntry.2	MacAddress	—	RO	アクセス制御対象の MAC アドレス

■Wireless 11a グループ

オブジェクト ID ：1.3.6.1.4.1.211.1.29.6.2.2

表：拡張 MIB：Wireless 11a グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	値	ACCESS	説明
dot11a	fjapDot11.2	—	—	—	—
dot11aSuppressSSID	dot11a.1	INTEGER	無効 (0), 有効 (1)	RW	ANY 接続拒否の有効／無効
dot11aStationID	dot11a.2	MacAddress	—	RO	IEEE802.11a の BSSID
dot11aDesiredSSID	dot11a.3	OCTET STRING	—	RW	IEEE802.11a の SSID
dot11aChannel	dot11a.4	Integer32	Auto(0), 36, 40, 44, 48, 52, 56, 60, 64	RW	チャンネル設定
dot11aSuperA	dot11a.5	INTEGER	無効 (0), 有効 (1)	RW	Super A の有効／無効
dot11aWDS	dot11a.6	INTEGER	無効 (0), 有効 (1)	RW	WDS の有効／無効
dot11aBeaconPeriod	dot11a.8	Integer32	20 ～ 1000	RW	ビーコン間隔 (1.024ms)
dot11aRTSThreshold	dot11a.9	Integer32	1 ～ 2346	RW	RTS スレッショルド (バイト)
dot11aFragmentationThreshold	dot11a.10	Integer32	256 ～ 2346	RW	フラグメントスレッショルド (バイト)
dot11aTXRate	dot11a.11	Integer32	自動 (0), 6 ～ 54	RW	通信可能速度 (Mbps)
dot11aTransmitPower	dot11a.12	INTEGER	最大 (0), 大 (1), 中 (2), 小 (3), 最小 (4)	RW	無線出力の設定
dot11aDiversitySupport	dot11a.13	INTEGER	両方 (0), 1(1), 2(2)	RW	アンテナ選択の設定
dot11aDTIMPeriod	dot11a.14	Integer32	1 ～ 255	RW	DTIM 間隔
dot11aRadioSwitch	dot11a.15	INTEGER	オフ (0), オン (1)	RW	無線スイッチのオン／オフ
dot11aRadioStatus	dot11a.16	INTEGER	停止中 (0), 稼働中 (1), 経路異常発生中 (2)	RO	11a 無線 I/F の状態
dot11aWMM	dot11a.17	INTEGER	無効 (0), 有効 (1)	RW	WMM の有効／無効
dot11aLoadBalance	dot11a.18	INTEGER	無効 (0), 有効 (1)	RW	ロードバランスの有効／無効
dot11aMaxClient	dot11a.19	Integer32	1 ～ 30	RW	最大接続可能クライアント数
dot11aSupportChannel	dot11a.20	INTEGER	J52(0), W52(1), W52+W53(2)	RO	サポートしているチャンネル

■Wireless 11b/g グループ

オブジェクト ID ：1.3.6.1.4.1.211.1.29.6.2.3

表：拡張 MIB：Wireless 11b/g グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	値	ACCESS	説明
dot11g	fjapDot11.3	—	—	—	—
dot11gSuppressSSID	dot11g.1	INTEGER	無効 (0), 有効 (1)	RW	ANY 接続拒否の有効／無効
dot11gStationID	dot11g.2	MacAddress	—	RO	IEEE802.11b/IEEE802.11g の BSSID
dot11gDesiredSSID	dot11g.3	OCTET STRING	—	RW	IEEE802.11b/IEEE802.11g の SSID
dot11gWirelessMode	dot11g.4	INTEGER	11b&11g(0), 11g(54Mbps) のみ (1), 11b(11Mbps) のみ (2)	RW	IEEE802.11b/IEEE802.11g のモード
dot11gChannel	dot11g.5	Integer32	Auto(1-14ch)(-1), Auto(1-11ch)(0), 1 ～ 14	RW	チャンネル設定
dot11gSuperG	dot11g.6	INTEGER	無効 (0), 有効 (1)	RW	Super G の有効／無効
dot11gWDS	dot11g.7	INTEGER	無効 (0), 有効 (1)	RW	WDS の有効／無効
dot11gBeaconPeriod	dot11g.9	Integer32	20 ～ 1000	RW	ビーコン間隔 (1.024ms)
dot11gRTSThreshold	dot11g.10	Integer32	1 ～ 2346	RW	RTS スレッショルド (バイト)
dot11gFragmentationThreshold	dot11g.11	Integer32	256 ～ 2346	RW	フラグメントスレッショルド (バイト)
dot11gBasicRate	dot11g.12	INTEGER	1、2Mbps(0), 1、2、5.5、11Mbps(1)	RW	ベーシックレート (Mbps)
dot11gTXRate	dot11g.13	Integer32	自動 (0), 1 ～ 54	RW	通信可能速度 (Mbps)
dot11gProtection	dot11g.14	INTEGER	オフ (0), 自動 (1)	RW	11g プロテクションの自動／オフ
dot11gTransmitPower	dot11g.15	INTEGER	最大 (0), 大 (1), 中 (2), 小 (3), 最小 (4)	RW	無線出力の設定
dot11gDiversitySupport	dot11g.16	INTEGER	両方 (0), 1(1), 2(2)	RW	アンテナ選択の設定
dot11gDTIMPeriod	dot11g.17	Integer32	1 ～ 255	RW	DTIM 間隔
dot11gShortPreamble	dot11g.18	INTEGER	無効 (0), 有効 (1)	RW	ショートプリアンブルの有効／無効
dot11gMultiCountryCode	dot11g.19	INTEGER	無効 (0), 有効 (1)	RW	国コードの有効／無効
dot11gRadioSwitch	dot11g.20	INTEGER	オフ (0), オン (1)	RW	無線スイッチのオン／オフ
dot11gRadioStatus	dot11g.21	INTEGER	停止中 (0), 稼働中 (1), 経路異常発生中 (2)	RO	11g 無線 I/F の状態
dot11gWMM	dot11g.22	INTEGER	無効 (0), 有効 (1)	RW	WMM の有効／無効
dot11gLoadBalance	dot11g.23	INTEGER	無効 (0), 有効 (1)	RW	ロードバランスの有効／無効
dot11gMaxClient	dot11g.24	Integer32	1 ～ 30	RW	最大接続可能クライアント数

■Wireless RADIUS グループ

オブジェクト ID ：1.3.6.1.4.1.211.1.29.6.2.4

表：拡張 MIB：Wireless RADIUS グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	値	ACCESS	説明
dot11Radius	fjapDot11.4	—	—	—	—
dot11RadiusSrv1Use	dot11Radius.1	INTEGER	未使用 (0), 使用 (1)	RW	RADIUS サーバー 1 の使用／未使用
dot11RadiusSrv1Address	dot11Radius.2	IpAddress	—	RW	RADIUS サーバー 1 の IP アドレス
dot11RadiusSrv1Port	dot11Radius.3	Integer32	1 ～ 65535	RW	RADIUS サーバー 1 のポート
dot11RadiusSrv1Secret	dot11Radius.4	DisplayString	0 ～ 20	RW	RADIUS サーバー 1 の共有シークレット
dot11RadiusSrv1AccPort	dot11Radius.5	Integer32	1 ～ 65535	RW	RADIUS サーバー 1 のアカウンティング用ポート
dot11RadiusSrv2Use	dot11Radius.6	INTEGER	未使用 (0), 使用 (1)	RW	RADIUS サーバー 2 の使用／未使用
dot11RadiusSrv2Address	dot11Radius.7	IpAddress	—	RW	RADIUS サーバー 2 の IP アドレス
dot11RadiusSrv2Port	dot11Radius.8	Integer32	1 ～ 65535	RW	RADIUS サーバー 2 のポート
dot11RadiusSrv2Secret	dot11Radius.9	DisplayString	0 ～ 20	RW	RADIUS サーバー 2 の共有シークレット
dot11RadiusSrv2AccPort	dot11Radius.10	Integer32	1 ～ 65535	RW	RADIUS サーバー 2 のアカウンティング用ポート
dot11RadiusAccountingSrvAddress	dot11Radius.11	IpAddress	—	RW	アカウンティングサーバーの IP アドレス
dot11RadiusAccountingSrvPort	dot11Radius.12	Integer32	1 ～ 65535	RW	アカウンティングサーバーのポート
dot11RadiusAccountingSrvSecret	dot11Radius.13	DisplayString	0 ～ 20	RW	アカウンティングサーバーの共有シークレット
dot11RadiusRetryInterval	dot11Radius.14	Integer32	1 ～ 60	RW	リトライ間隔 (秒)
dot11RadiusRetryTimes	dot11Radius.15	Integer32	1 ～ 10	RW	リトライ回数 (回／サーバー)
dot11RadiusCycleTimes	dot11Radius.16	Integer32	1 ～ 5	RW	サイクル数 (回)

■common object related to both 802.11a/g interfaces

オブジェクト ID ：1.3.6.1.4.1.211.1.29.6.2.5

表：拡張 MIB：common object related to both 802.11a/g interfaces グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	値	ACCESS	説明
dot11InactivityTimer	fjapDot11.5	Integer32	0 ～ 86400	RW	無通信切断タイマー

■AP VLAN グループ

オブジェクト ID ：1.3.6.1.4.1.211.1.29.6.3

表：拡張 MIB：AP VLAN グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	値	ACCESS	説明
fjapVlan	fjap.3	—	—	—	—
vlanCtrlSwitch	fjapVlan.1	INTEGER	無効 (0), 通常 VLAN(1), 認証 VLAN(2)	RW	VLAN 機能の有効／無効
vlanManagement	fjapVlan.2	Integer32	1 ～ 16	RW	管理 VLAN 番号
vlanCtrlTable	fjapVlan.3	SEQUENCE OF	—	NA	—
vlanCtrlEntry	vlanCtrlTable.1	VlanCtrlEntry	—	NA	—
vlanCtrlIndex	vlanCtrlEntry.1	Integer32	1 ～ 16	NA	SNMP 管理の対象の VLAN 番号
vlanCtrlName	vlanCtrlEntry.2	OCTET STRING	0 ～ 16	RW	対象 VLAN の VLAN 名
vlanCtrlID	vlanCtrlEntry.3	Integer32	0 ～ 4094	RW	対象 VLAN の VLAN ID
vlanCtrlClass	vlanCtrlEntry.4	Integer32	1 ～ 8	RW	対象 VLAN のサービスクラス
vlanManagementID	fjapVlan.4	Integer32	0 ～ 4094	RW	管理 VLAN ID

■AP Trap グループ

オブジェクト ID ：1.3.6.1.4.1.211.1.29.6.4

表：拡張 MIB：AP Trap グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	値	ACCESS	説明
fjapTrap	fjap.4	—	—	—	—

■AP Administration グループ

オブジェクト ID ：1.3.6.1.4.1.211.1.29.6.5

表：拡張 MIB：AP Administration グループ一覧

名称	オブジェクト識別子	SYNTAX（データタイプ）	値	ACCESS	説明
fjapAdmin	fjap.5	—	—	—	—
adminNtpSwitch	fjapAdmin.1	INTEGER	手動設定 (0), Network Time Protocol(1)	RW	システム時刻の設定方法
adminNtpAddress	fjapAdmin.2	IpAddress	—	RW	NTP サーバーの IP アドレス
adminNtpInterval	fjapAdmin.3	INTEGER	1, 2, 7	RW	NTP での時刻取得間隔 (日)
adminNtpTimezone	fjapAdmin.4	Integer32	-12 ～ 13	RW	タイムゾーンの設定（GMT との時差）
adminYear	fjapAdmin.5	Integer32	2000 ～ 2037	RW	日付設定 (年)
adminMonth	fjapAdmin.6	Integer32	1 ～ 12	RW	日付設定 (月)
adminDay	fjapAdmin.7	Integer32	1 ～ 31	RW	日付設定 (日)
adminHour	fjapAdmin.8	Integer32	0 ～ 23	RW	時刻設定 (時)
adminMinute	fjapAdmin.9	Integer32	0 ～ 59	RW	時刻設定 (分)
adminLANPort	fjapAdmin.10	Integer32	AUTO/AUTO(0), 100Mbps/Full Duplex(1), 100Mbps/Half Duplex(2), 10Mbps Full Duplex(3), 10Mbps Half Duplex(4)	RW	有線 LAN のポート設定
adminPrivProtection	fjapAdmin.11	INTEGER	無効 (0), 有効 (1)	RW	プライバシープロテクションの有効／無効
adminLinkIntegrity	fjapAdmin.12	INTEGER	無効 (0), 有効 (1)	RW	リンクインテグリティの有効／無効
adminRCAddress1	fjapAdmin.13	IpAddress	—	RW	リンクインテグリティ宛先 IP アドレスその 1
adminRCAddress2	fjapAdmin.14	IpAddress	—	RW	リンクインテグリティ宛先 IP アドレスその 2
adminRCAddress3	fjapAdmin.15	IpAddress	—	RW	リンクインテグリティ宛先 IP アドレスその 3
adminRCInterval	fjapAdmin.16	Integer32	1 ～ 600	RW	リンクインテグリティのチェック間隔（秒）
adminRCRetry	fjapAdmin.17	Integer32	0 ～ 5	RW	リンクインテグリティのリトライ回数
adminSysLogEnable	fjapAdmin.18	INTEGER	無効 (0), 有効 (1)	RW	syslog 機能の有効／無効
sysLogOutgoingLevel	fjapAdmin.19	Integer32	0 ～ 7	RW	syslog 送出レベルの設定
sysLogImmediateOutgoingLevel	fjapAdmin.20	Integer32	0 ～ 7	RW	syslog 即時送出レベルの設定
adminLogSrv1Use	fjapAdmin.21	INTEGER	無効 (0), 有効 (1)	RW	syslog サーバー 1 の有効／無効
adminLogSrv1Address	fjapAdmin.22	IpAddress	—	RW	syslog サーバー1 の IP アドレス
adminLogSrv1Port	fjapAdmin.23	Integer32	1 ～ 65535	RW	syslog サーバー 1 のポート番号
adminLogSrv2Use	fjapAdmin.24	INTEGER	無効 (0), 有効 (1)	RW	syslog サーバー 2 の有効／無効
adminLogSrv2Address	fjapAdmin.25	IpAddress	—	RW	syslog サーバー2 の IP アドレス
adminLogSrv2Port	fjapAdmin.26	Integer32	1 ～ 65535	RW	syslog サーバー 2 のポート番号
adminReboot	fjapAdmin.27	INTEGER	通常 (0), 再起動 (1)	RW	装置を再起動させる
adminMonitoring	fjapAdmin.28	INTEGER	無効 (0), 有効 (1)	RW	監視機能の有効／無効
monitoringInterval	fjapAdmin.29	Integer32	1 ～ 3600	RW	監視間隔（秒）
loginWlan	fjapAdmin.30	INTEGER	拒否 (0), 許可 (1)	RW	無線からのログインの許可／拒否
loginPort	fjapAdmin.31	Integer32	1 ～ 65535	RW	設定画面のポート番号
snmpWlan	fjapAdmin.32	INTEGER	拒否 (0), 許可 (1)	RW	無線からの SNMP アクセスの許可／拒否

トラップ一覧

特定の情報については、SNMP で管理するネットワーク機器上で特別な状態の変化が発生した場合に、トラップという機能を用いてエージェントからマネージャにメッセージを通知し、本製品の状態の変化を監視することができます。
サポートしているトラップを説明します。

- ColdStart
  本製品の電源を入れたとき、または本製品の設定を変更したときに、マネージャに対して 1 回だけ通知します。
- WarmStart
  本製品の再起動時に、マネージャに対して 1 回だけ通知します。
- LinkUp
  本製品の LAN コネクタが物理的に接続された状態になったとき、マネージャに対して通知します。また、本製品の電源を入れたとき、再起動時、および設定を変更した時にも通知する場合があります。
- LinkDown
  本製品の LAN コネクタが物理的に切断された状態になったとき、マネージャに対して通知します。また、本製品の電源を入れたとき、再起動時、および設定を変更したときにも通知する場合があります。
- AuthenticationFailure
  SNMP のコミュニティ名の認証に失敗したときに、マネージャに対して通知します。

3 syslog メッセージ一覧

本製品がサポートしている syslog のメッセージ一覧を記載します。

表：送出レベルの定義

送出レベル	定義	説明
0	Emergency	緊急に対処する必要がある状態の通知。システムが使用不可能など。
1	Alert	システムの異常などに対する警告。システムの故障など。
2	Critical	致命的なエラーが発生している状態の通知。ハードウェアの故障など。
3	Error	機能の一部などにエラーが発生している状態の通知。モジュールのエラーなど。
4	Warning	警告メッセージ。不正アクセスなど。
5	Notice	重要な通知。特別なイベントの発生など。
6	Informational	情報の通知。通常のイベントの発生など。
7	Debug	テスト、デバック用の解析メッセージ。

■無線 LAN ／ WPA

表：無線 LAN ／ WPA に関する syslog メッセージ一覧

送出レベル	分類	メッセージ	説明
4	wlan	Unknown client [MAC address] tried to associate with [SSID].	MAC アドレスフィルタリングで接続を拒否している、または接続を許可されていない無線 LAN 端末が本製品に接続しようとしました。
4	wpa	4-way handshake with the client [MAC address] failed.	無線 LAN 端末との、WPA 接続の 4-way ハンドシェークは失敗しました。
4	wpa	First MIC error was detected.	1 番目の MIC エラーを検出しました。
4	wpa	Second MIC error was detected within 60 seconds after first MIC error.	1 番目の MIC エラーの検出後 60 秒以内に、2 番目の MIC エラーを検出しました。
4	wlan	The channel will be changed by DFS.	IEEE802.11a インターフェースのチャンネルは DFS のレーダー波検出により変更されます。
5	wpa	4-way handshake with the client [MAC address] succeeded.	無線 LAN 端末との、WPA 接続の 4-way ハンドシェークが成功しました。
5	wlan	Client [MAC address] reached the inactivity disconnection timing.	無線 LAN 端末は無通信切断の時間に達しました。
5	wlan	Client [MAC address] in [SSID] was deauthenticated.	本製品は無線 LAN 端末との接続を切断しました。
6	wlan	Client [MAC address] associated with [SSID].	無線 LAN 端末が本製品に接続しました。
6	wlan	Client [MAC address] disassociated from [SSID].	無線 LAN 端末が本製品との接続を切断しました。
7	wpa	4-way handshake with the client [MAC address] started.	無線 LAN 端末との、WPA 接続の 4-way ハンドシェークを開始しました。
7	Kernel	Wireless driver [11a / 11b/g] was loaded and initialized.	起動時に、本製品は無線ドライバの読み込みと初期化を完了しました。
7	wlan	Inactivity disconnection timer is set to [NUMBER] seconds.	無通信切断タイマーは指定された値に設定されています。

■IEEE802.1X

表：IEEE802.1X に関する syslog メッセージ一覧

送出レベル	分類	メッセージ	説明
4	IEEE802.1X	Authentication about the client [MAC address] failed.	RADIUS サーバーから’Access-Reject’メッセージを受信しました。
5	IEEE802.1X	Authentication about the client [MAC address] succeeded.	RADIUS サーバーから’Access-Accept’メッセージを受信しました。
5	IEEE802.1X	RADIUS server [IP address] did not respond, so the authenticator switched the server [IP address] to access. The client is [MAC address].	一方の RADIUS サーバーに対して指定された回数のアクセスを行いましたが、RADIUS サーバーは’Access-Request’に対して応答しませんでした。そのため、のアクセス先をもう一方の RADIUS サーバーに切り替えました。
5	IEEE802.1X	Primary server [IP address] recovered, so the authenticator switches the server to the primary one.The client is [MAC address].	RADIUS サーバーのアクセス方法が「プライマリ / セカンダリ」のとき、優先サーバーは「故障」状態から復帰し、本製品はそれを認識しました。そしてアクセス先を優先サーバーへ切り替えました。
5	IEEE802.1X	Retry sequence reached the end. The client is [MAC address].	指定されたサイクル数のリトライを終えても､RADIUS サーバーは、応答しませんでした。
5	IEEE802.1X	Authentication about the client [MAC address] started.	本製品は無線 LAN 端末の認証を開始しました。
7	Kernel	IEEE 802.1x module was loaded and initialized.	起動時に、本製品は 802.1X モジュールの読み込みと初期化を完了しました。

■RADIUS アカウンティング

表：RADIUS アカウンティングに関する syslog メッセージ一覧

送出レベル	分類	メッセージ	説明
6	radiusacc	Accounting-Request was sent to the RADIUS accounting server [IP address].	本製品は’Accounting-Request’を RADIUS アカウンティングサーバーへ送信しました。
6	radiusacc	Accounting-Response was received from [IP address].	本製品は RADIUS アカウンティングサーバーから’Accounting-Response’を受信しました。

■DHCP サービス

表：DHCP サービスに関する syslog メッセージ一覧

送出レベル	分類	メッセージ	説明
2	dhcp	No more IP address is leased.	本製品は DHCP discover または DHCP request を受信しましたが、何らかの理由（リースできるアドレスがない、DHCP サービスが無効になっているなど）でアドレスをリースすることができませんでした。
2	dhcp	Address pool is empty.	本製品は DHCP リース範囲のアドレスをすべてリースし、アドレスプールは空になりました。
5	dhcp	DHCP server leased [IP address] to [MAC address].	本製品はクライアントからの DHCP request に対して DHCP ack を送信しました。
5	dhcp	The lease time of [MAC address]expired.	クライアントへのリースが有効期限に達しました。
6	dhcp	DHCP discover was received from [MAC address].	本製品はクライアントから DHCP discover を受信しました。
6	dhcp	DHCP server transmitted DHCP offer to [MAC address]. Offered IP address was [IP address].	本製品はクライアントに対して DHCP offer を送信しました。
6	dhcp	DHCP request was received from [MAC address].	本製品はクライアントから DHCP request を受信しました。
6	dhcp	[IP address] is used by [MAC address].	クライアントからの DHCP request で受信した IP アドレスはすでに他のクライアントにリースされています。
7	kernel	DHCP service was loaded and initialized.	起動時に、本製品は DHCP サービスモジュールの読み込みと初期化を完了しました。

■VLAN

表：VLAN に関する syslog メッセージ一覧

送出レベル	分類	メッセージ	説明
5	vlan	SSID [SSID] is assigned to VLAN ID [VID]. The [I/F is 11b/g / I/F is 11a / I/Fs are 11b/g and 11a].	本製品はこの SSID を指定された VLAN に割り当てます。この SSID は指定された無線 LAN インターフェースに割り当てられます。
6	vlan	Security policy of SSID [SSID] is [security policy name].	この SSID は指定されたセキュリティポリシーに従います。
6	vlan	COS of SSID [SSID] is [COS value].	この SSID の COS 値は指定された値です。
7	kernel	VLAN module was loaded and initialized.	起動時に、本製品は VLAN モジュールの読み込みと初期化を完了しました。

■SNMP エージェント

表：SNMP エージェントに関する syslog メッセージ一覧

送出レベル	分類	メッセージ	説明
4	snmp	SNMP agent received [Get / Set] request from [IP address], but authentication failed.	本製品は、異なるコミュニティ名を持つ SNMP メッセージを受信しました。
6	snmp	SNMP agent sent Trap to [IP address].	本製品は SNMP マネージャにトラップを送信しました。
7	snmp	SNMP agent was loaded and initialized.	起動時に、本製品は SNMP エージェントモジュールの読み込みと初期化を完了しました。

■認証 VLAN

表：認証 VLAN に関する syslog メッセージ一覧

送出レベル	分類	メッセージ	説明
4	authvlan	The value of attriburte [Attribute] was incorrect.	RADIUS サーバーから、不正なアトリビュートの値を受信しました。
5	authvlan	Client [MAC Address] was assigned to VLAN ID [VID].	本製品は、クライアントに対して VLAN ID を割り当てました。
5	authvlan	Authentication VLAN is enabled.	起動時に、本製品は認証 VLAN サービスモジュールを有効にしました。
6	vlan	VLAN ID [VID] was set to management VLAN.	本製品の管理 VLAN ID は指定された値です。
7	vlan	Tunnel-Type is [Value of Tunnel-Type].	RADIUS サーバーから、Tunnel-Type の値を受信しました。
7	vlan	Tunnel-Medium-Type is [Value of Tunnel-Medium-Type].	RADIUS サーバーから、Tunnel-Medium-Type の値を受信しました。

■接続台数制限

表：接続台数制限に関する syslog メッセージ一覧

送出レベル	分類	メッセージ	説明
5	kernel	Load balancing function was loaded and initialized.	起動時に、本製品は接続台数制限モジュールの読み込みと初期化を完了しました。
5	wlan	The number of associations on [11a / 11b/g]reached the upper limit.	IEEE802. [11a / 11b/g] の接続台数は、上限に達しました。
6	wlan	AP is now able to accept new association on [11a / 11b/g].	IEEE802. [11a / 11b/g]インターフェースにクライアントが接続できるようになりました。
7	wlan	Current number of associations on [11a / 11b/g]is [NUMBER].	現在IEEE802.[11a / 11b/g]インターフェースに接続しているクライアントの台数です。
7	wlan	The number of associations on [11a / 11b/g]is restricted to [NUMBER].	IEEE802.[11a / 11b/g] インターフェースへ接続可能なクライアントの台数は、指定された値です。

■AP 検出

表：AP 検出に関する syslog メッセージ一覧

送出レベル	分類	メッセージ	説明
5	kernel	Monitoring function was loaded and initialized.	起動時に、本製品は AP 検出モジュールの読み込みと初期化を完了しました。
6	monitor	AP detected the access point [BSSID]. SSID is [SSID], channel is [channel], and RSSI value is [value].	本製品は、無線 LAN アクセスポイントを検出しました。SSID, チャンネル , 無線強度は指定された値です。
6	monitor	AP detected the access point [BSSID]. SSID doesn't exist, channel is [channel], and RSSI value is [value].	製品は、AP を検出しました。SSID は存在しません。チャンネル , 無線強度は指定された値です。
7	monitor	Periodical monitoring is executed at [value] second's intervals on [11a / 11b/g].	IEEE802. [11a / 11b/g]インターフェースの次のスキャンまでの間隔は、指定された秒数です。
7	monitor	AP started to find BSSs of other APs on [11a / 11b/g].	本製品は、IEEE802. [11a / 11b/g] インターフェースの無線 LAN アクセスポイント検出を開始しました。

■SSID 認証

表：SSID 認証に関する syslog メッセージ一覧

送出レベル	分類	メッセージ	説明
5	IEEE802.1X	SSID authentication is enabled on SSID.	起動時に、本製品は SSID 認証機能を有効にしました。
6	IEEE802.1X	The user [user name] is allowed to access SSID [value].	指定された SSIDに接続したユーザーは通信を許可されました。
4	IEEE802.1X	The user [user name] on the client [MAC Address] has associated with unallowable SSID [Value].	指定された SSID に接続したユーザーは通信を許可されませんでした。

■WMM

表：WMM に関する syslog メッセージ一覧

送出レベル	分類	メッセージ	説明
5	WMM	WMM function is enabled on [11a / 11b/g].	起動時に、本製品は IEEE802. [11a / 11b/g] インターフェースの WMM を有効にしました。
7	WMM	Client [MAC address] is WMM compliant.	無線 LAN 端末は WMM に対応しています。

■その他

表：その他の syslog メッセージ一覧

送出レベル	分類	メッセージ	説明
3	http	User [user name] failed to login for the web UI from [IP address].	本製品の設定画面にアクセスしようとしましたが、ユーザー名またはパスワードが間違っていたため、ユーザー認証は失敗しました。
4	kernel	Ping to [IP address] for link integrity failed. Wireless function stopped.	リンクインテグリティ機能で、すべての宛先への PING が失敗したため、本製品は無線機能を停止しました。
4	kernel	The irregular firmware file came in.	不正なファームウェアが指定されました。
5	kernel	Initialization succeeded .	正常に初期化を完了しました。
5	kernel	Ping to [IP address] for link integrity succeeded. Wireless function started.	リンクインテグリティ機能で、本製品からの PING に対し少なくとも一つの宛先が応答したため、本製品は無線機能を再開しました。
5	ntp	System time synchronized with NTP server.	本製品は NTP サーバーからの時刻同期パケットを受信しました。
5	ntp	System time was not able to synchronize with NTP server.	本製品は NTP サーバーとのシステム時刻の同期に失敗しました。
5	kernel	DHCP client leased the address [IP address] from the server [IP address].	本製品は DHCP サーバーから IP アドレスを取得しました。
5	kernel	LAN port was linked up.	本製品の有線 LAN コネクタが物理的に接続され、通信可能状態になりました。

表：その他の syslog メッセージ一覧

送出レベル	分類	メッセージ	説明
5	kernel	LAN port was linked down.	本製品の有線 LAN コネクタが物理的に切断され、通信不可能状態になりました。
5	kernel	Ping to [IP address] for link integrity failed.	リンクインテグリティ機能の宛先 IP アドレスから、PING に対して’ICMP Echo’以外の応答を受信しました。
5	kernel	Proxy ARP function is enabled.	起動時に、本製品は Proxy ARP 機能を有効にしました。
6	kernel	Ping to [IP address] for link integrity succeeded.	リンクインテグリティ機能の宛先 IP アドレスから、‘ICMP Echo’を受信しました。
6	http	User [user name] logged in for the web UI.	ユーザーが本製品の設定画面にアクセスし、本製品はユーザーの認証に成功しました。

4 RADIUS アトリビュート一覧

本製品がサポートしている RADIUS 認証、および RADIUS アカウンティングのアトリビュート一覧を記載します。

表：RADIUS アトリビュート一覧

タイプ	アトリビュート	認証／アカウンティング	RADIUS パケットタイプ	属性値	説明
1	User-Name	RADIUS 認証 RADIUS アカウンティング	Access-Request Access-Accept	String	ユーザー名を示します。RADIUS アカウンティングの場合は、無線 LAN 端末の MAC アドレスを示します。
4	NAS-IP-Address	RADIUS 認証 RADIUS アカウンティング	Access-Request	Address (4 octets)	Address に本製品の IP アドレスが格納されます。
5	NAS-Port	RADIUS 認証 RADIUS アカウンティング	Access-Request	Port Number (4 octets)	Port Number に本製品の物理ポート番号が格納されます。
6	Service-Type	RADIUS 認証	Access-Request Access-Accept	Value (4 octets)	Value:2 = Framed (接続に適切な 802 フレームを使用しなければならないことを示します。)
12	Framed-MTU	RADIUS 認証	Access-Request Access-Accept	Value (4 octets)	Value = 1488 (10 進)
24	State	RADIUS 認証	Access-Request Access-Accept Access-Challenge	String	基本的に、サーバーからの Access-Challenge で送信され、Challengeに対する新しいAccess-Request で無線 LAN 端末からサーバーに変更なしで送信されます。
25	Class	RADIUS 認証	Access-Accept Accounting-Request	String	認証要求とアカウンティング要求の整合性をチェックする値です。
26	Vendor-Specific	RADIUS 認証	Access-Accept	Vendor-ID	ベンダ独自の拡張機能を示します。 Vendor-ID の上位 octet は 0 で、下位 3octets は RFC1700 で定義されるように、ネットワークバイトオーダのベンダの SMI ネットワークマネージメント私企業コードです。 String は 1octet 以上。String の情報（ベンダ独自の拡張機能）は実装に依存します。 Vendor-ID = 9 (Cisco) Vendor type = 1 Attribute-Specific = ssid=aaaaa (aaaaa は SSID、"ssid=aaaaa" が値です。)
27	Session-Timeout	RADIUS 認証	Access-Accept Access-Challenge	Value (4 octets)	再認証処理を開始するまでの時間を示します。 Value = 再認証処理を開始するまでの最大秒数
28	Idle-Timeout	RADIUS 認証	Access-Accept Access-Challenge	Value (4 octets)	ユーザーが許されるアイドル接続の (データ転送を行わないままセッションを接続できる）最大連続秒数を示します。 Value = アイドル接続の最大秒数
30	Called-Station-ID	RADIUS 認証	Access-Request	String	String に本製品の MAC アドレスと SSID が格納されます。 ("aa-bb-cc-dd-ee-ff:SSID" の形式)
31	Calling-Station-ID	RADIUS 認証	Access-Request	Address (17 octets)	Address に無線 LAN 端末の MAC アドレスが格納されます。
32	NAS-Identifier	RADIUS 認証 RADIUS アカウンティング	Access-Request	String	本製品を識別する文字列が格納されます。
40	Acct-Status-Type	RADIUS アカウンティング	Accounting-Request	Value (4 octets)	ユーザーサービス、アカウンティングの開始と終了を示します。 Value:1 = Start (ユーザーサービスの開始) Value:2 = Stop (ユーザーサービスの終了)
41	Acct-Delay-Time	RADIUS アカウンティング	Accounting-Request	Value (4 octets)	無線 LAN 端末が今までに何秒間このレコードを送ろうとしていたかを示します。

表：RADIUS アトリビュート一覧

タイプ	アトリビュート	認証／アカウンティング	RADIUS パケットタイプ	属性値	説明
42	Acct-Input-Octets	RADIUS アカウンティング	Accounting-Request	Value (4 octets)	サービスが提供されているポートで何オクテット受信したかを示します。Acct-Status-Type が Stop の場合にのみ存在します。 Value = 受信オクテット数
43	Acct-Output-Octets	RADIUS アカウンティング	Accounting-Request	Value (4 octets)	サービスが提供されているポートで何オクテット送信したかを示します。Acct-Status-Type が Stop の場合にのみ存在します。 Value = 送信オクテット数
44	Acct-Session-ID	RADIUS アカウンティング	Accounting-Request	Text	ユニークなアカウンティング ID を示します。開始と終了で同じ ID を持ちます。Text は UTF-8 形式で格納されます。
45	Acct-Authentic	RADIUS アカウンティング	Accounting-Request	Value (4 octets)	ユーザーがどのように認証されたかを示します。 Value:1 = RADIUS 認証 Value:2 = Local 認証
46	Acct-Session-Time	RADIUS アカウンティング	Accounting-Request	Value (4 octets)	ユーザーが何秒間サービスを受けたかを示します。Acct-Status-Type が Stop の場合のみ存在します。 Value = ユーザーがサービスを受けた時間 (秒)
47	Acct-Input-Packets	RADIUS アカウンティング	Accounting-Request	Value (4 octets)	サービスが提供されているポートで何パケット受信したかを示します。Acct-Status-Type が Stop の場合のみ存在します。 Value = 受信パケット数
48	Acct-Output-Packets	RADIUS アカウンティング	Accounting-Request	Value (4 octets)	サービスが提供されているポートで何パケット送信したかを示します。Acct-Status-Type が Stop の場合のみ存在します。 Value = 送信パケット数
49	Acct-Terminate-Cause	RADIUS アカウンティング	Accounting-Request	Value (4 octets)	どのようにセッションが終了したかを示します。 Value:1 = User Request Value:2 = Lost Carrier Value:4 = Idol Timeout Value:5 = Session Timeout Value:6 = Admin Reset Value:7 = Admin Reboot Value:10 = NAS Request Value:11 = NAS Reboot Value:19 = Supplicant Restart Value:20 = Reauthentication Failure Value:21 = Port Reinitialized Value:22 = Port Administratively Disabled
61	NAS-Port-Type	RADIUS 認証 RADIUS アカウンティング	Access-Request	Value (4 octets)	Value:19 = Wireless - IEEE802.11
64	Tunnel-Type	RADIUS 認証	Access-Accept	Tag + Value (3 octets)	トンネル (カプセル化) のタイプを示します。 Tag = 0x00 (unused) Value:13 = VLAN
65	Tunnel-Medium-Type	RADIUS 認証	Access-Accept	Tag + Value (3 octets)	トンネルの媒体を示します。 Tag = 0x00 (unused) Value:6 = 802 (includes all 802 media plus Ethernet "canonical format")

表：RADIUS アトリビュート一覧

タイプ	アトリビュート	認証／アカウンティング	RADIUS パケットタイプ	属性値	説明
77	Connect-Info	RADIUS 認証	Access-Request	Text	認証要求側の接続状態を示すために、本製品から送信される。Text は UTF-8 形式で格納されます。
79	EAP-Message	RADIUS 認証	Access-Request Access-Accept Access-Reject Access-Challenge	String	EAP パケットをカプセル化するために使用されます。String は EAP パケットが格納されます。
80	Message-Authenticator	RADIUS 認証	Access-Request Access-Accept Access-Reject Access-Challenge	Value (16 octets)	EAP-Message の保護として使用されます。 Value = HMAC-MD5 (Type, Identifier, Length, Request, Authenticator, Attribute)
81	Tunnel-Private-Group-ID	RADIUS 認証	Access-Accept	Tag + String	VLAN-ID を示します。 Tag が 0 のとき、Tag は省略されます。 Tag の値が 0x20 以上の場合、Tag ではなく String(VLAN-ID)の先頭バイトと解釈します。 String は VLAN-ID を示します。（例：VLAN ID が 10 のとき、0x31, 0x30 の 2 バイト） ユーザー名からRADIUSサーバーが判断します。
87	NAS-Port-Id	RADIUS 認証	Access-Request	Text	認証側が認証要求側の認証に使用するポートを識別するために使用されます。Text は UTF-8 形式で格納されます。

5 リサイクルについて

本製品を廃棄するときは、次の点にご注意ください。

■本製品の廃棄について

本製品（付属品を含む）を廃棄する場合は、「廃棄物の処理及び清掃に関する法律」の規制を受けます。

・法人、企業のお客様へ
　本製品を廃棄する場合は、産業廃棄物の扱いとなりますので、産業廃棄物処分業の許可を取得している会社に処分を委託する必要があります。弊社は、「富士通リサイクルシステム」を用意し、お客様の廃棄のお手伝いをしておりますのでご利用ください。
　詳しくは、ホームページ（http://eco.fujitsu.com/jp/5g/products/recycleindex.html）の「富士通リサイクルシステム」をご覧ください。
・個人のお客様へ
　個人のお客様は、上記「富士通リサイクル受付センター」をご利用いただけません。本製品を廃棄する場合は、一般廃棄物の扱いとなりますので、地方自治体の廃棄処理に関連する条例または規則に従ってください。

■注意事項

本製品を廃棄する場合は、本製品の設定内容を初期化して、ご購入時の状態に戻してください。初期化の方法については、「初期化（LOAD DEFAULT ボタン）」（→ P.176）をご覧ください。

6 用語集

このマニュアルの中で使われている用語の解説です。

■数字／アルファベットで始まる用語

□ A

AES（Advanced Encryption Standard）

現在用いられている DES、3DES に代わる次世代の標準暗号化方式で、強固な暗号化方式として無線 LAN への幅広い普及が見込まれています。暗号化アルゴリズムには、ベルギーの暗号開発者が開発した「Rijndael（ラインダール）」が採用され、データを固定のブロック長で区切ってそれぞれ暗号化を行います。データ長は 128、192、256 ビット、鍵の長さは 128、192、256 ビットがサポートされていて暗号強度は非常に高く設計されています。

ANY 接続拒否

IEEE802.11 規格では、SSID を「ANY」に設定すれば、無線 LAN アクセスポイントに接続できるように定められています（これを、ANY キーによる接続が許可されていると言います）。これは、公共の場（ホテルのロビーや空港など）で簡単に無線 LAN ネットワーク接続サービスを行えるように想定したためですが、セキュリティが脆弱となる可能性があります。この機能を有効にすることで、SSID を「ANY」に設定した無線 LAN 端末からの接続を拒否することができます。

ARP（Address Resolution Protocol）

通信を行うためには、通信相手の MAC アドレスをパケットのあて先フィールドに指定する必要があります。TCP/IP のアプリケーションでは、通信相手の IP アドレスはわかっても、MAC アドレスはわからないため、通信を開始するホストが、相手の IP アドレスを元に MAC アドレスを取得する必要があります。この IP アドレスから MAC アドレスを取得するためのプロトコルが ARP です。通信を開始するホストが、通信相手の IP アドレスを指定して ARP 要求をブロードキャストすると、ネットワーク上のすべてのホストはこのパケットを確認し、指定されている IP アドレスが自身のアドレスであった場合に、自身の MAC アドレスを返信します。

□ C

CA（Certification Authority）

IEEE802.1X 機能の EAP-TLS 認証などを利用する場合に、クライアントやサーバーの正当性を証明するために使用される電子証明書を発行する機関です。電子証明書の所有者の身元を確認し、証明します。

□ D

DFS（Dynamic Frequency Control）

航空管制レーダーや気象レーダーなどで使用されるレーダー波との電波干渉を防止するための無線 LAN アクセスポイントの機能です。IEEE802.11a で使用できるチャンネルにこれらのレーダー波が使用する周波数帯（W53）が追加されたことで、この機能が必要となりました。無線 LAN アクセスポイントは電波の送出を開始する前の 1 分間でレーダーの干渉波の有無を確認し、検出した場合はそのチャンネルを検出時から 30 分間無効にし、かつ検出時から 10 秒以内に使用するチャンネルを自動的に変更します。

また、レーダー波の検出は、無線 LAN アクセスポイントの起動時に行われた後も定期的に行われます。レーダー波が検出された場合には、DFS が行われ、使用するチャンネルが変更されるため、1 分以上通信が切断されます。

DHCP（Dynamic Host Configuration Protocol）

IP アドレスなどの通信に関するパラメータを、自動取得するために使用するプロトコルです。IP アドレスを与える側を DHCP サーバー、IP アドレスを与えられる側を DHCP クライアントと呼びます。

DNS（Domain Name System）

コンピュータに割り当てた、IP アドレスとホスト名との対応を管理する機能です。IP アドレスがわからないコンピュータでも、ホスト名がわかっていれば、そのコンピュータと通信できます。

DS-SS 方式（Direct Sequence Spread Spectrum）

無線 LAN の国際標準規格 IEEE802.11b で定められた通信方式で、スペクトラム拡散方式の 1 つです。通信中にノイズが発生しても、通信への影響を受けにくいように設計されているため、信頼性の高いデータ通信が可能です。

□ E

EAP-MD5（Extensible Authentication Protocol-Message Digest 5）

IEEE802.1X の認証プロトコルの 1 つです。EAP-MD5 では、ID とパスワードを使って認証を行います。

EAP-TLS（Extensible Authentication Protocol-Transport Layer Security）

IEEE802.1X の認証プロトコルの 1 つです。EAP-TLS では、電子証明書を使って認証を行います。

EAP-TTLS（Extensible Authentication Protocol-Tunneled Transport Layer Security）

IEEE802.1X の認証プロトコルの 1 つです。EAP-TTLS では、電子証明書および ID、パスワードを使って認証を行います。

□ F

FTP（File Transfer Protocol）

ファイルを転送するときに使われるネットワークプロトコルです。写真データや音声データなどデータサイズが比較的大きなファイルを送受信するときや、Web サイトからファイルのダウンロードを行う場合などによく使われます。

□ H

HTTP（HyperText Transfer Protocol）

データを転送するときに使われる代表的なネットワークプロトコルです。HTML（Hyper Text Markup Language）で作成された文書ファイルや、関連する写真、音声および動画などさまざまなデータの送受信に利用されます。

□ I

ICMP（Internet Control Message Protocol）

通信回線の状況を確認する際に使用されるプロトコルで、PING などで使用されます。

IEEE802.11a

IEEE（米国電気電子学会）で LAN 技術の標準を策定している 802 委員会が定めた、無線 LAN の規格の 1 つです。5GHz 帯を使った高速無線 LAN の規格で、最大 54Mbps の通信が行えます。変調方式として、エラー訂正に優れた OFDM 方式を採用しています。

IEEE802.11b

IEEE（米国電気電子学会）で LAN 技術の標準を策定している 802 委員会が定めた、無線 LAN の規格の 1 つです。無線免許なしで自由に使える 2.4GHz 帯の電波（ISM バンド）を使い、最大 11Mbps の速度で通信を行うことができます。

IEEE802.11e

IEEE（米国電気電子学会）で LAN 技術の標準を策定している 802 委員会が定めている無線 LAN 規格の 1 つです。IEEE802.11a や IEEE802.11b/IEEE802.11g との互換性を保ちながら WMM などの QoS 技術を使用することができます。

IEEE802.11g

IEEE（米国電気電子学会）で LAN 技術の標準を策定している 802 委員会が定めた、無線 LAN の規格の 1 つです。従来の IEEE802.11b と互換性を持ち、同じ 2.4GHz 帯を使いながら、最大で 54Mbps の速度で通信を行うことができます。

IEEE802.11g プロテクション

IEEE802.11g と IEEE802.11b との共存環境において通信速度の低下を防ぐ機能です。IEEE802.11g 規格で定義されています。IEEE802.11b の無線 LAN 端末と IEEE802.11g の無線 LAN 端末は変調方式が異なるため、お互いが通信していることを認識できません。このため、IEEE802.11g の無線 LAN 端末が通信中にもかかわらず IEEE802.11b の無線 LAN 端末は通信を試み、通信の衝突が発生します。このような場合、各無線 LAN 端末がデータ再送を行うため通信速度が低下します。そこで、IEEE802.11b の無線 LAN 端末に対して IEEE802.11g で通信を開始することを通知して、通信の衝突を防ぎます。

IEEE802.11i （WPA2）

無線 LAN のセキュリティ規格です。WPA は IEEE802.11i の一部を先取りして規格化されたもので、いわゆる IEEE802.11i のドラフトバージョンですが、WPA2 は IEEE802.11i を完全にサポートする規格です。AES を完全にサポートするなど、WPA よりさらに強力な暗号化技術に対応しています。WPA と下位互換性を持ち、WPA 無線 LAN 端末と通信することができます。

IEEE802.1D

IEEE（米国電気電子学会）で LAN 技術の標準を策定している 802 委員会が定めた、LAN で使用されるパケットに優先情報を付加する規格です。設定された優先情報で通信データを管理することで、一定の通信速度を保証することが可能になります。

IEEE802.1X

ネットワークでのクライアント認証方式を定めた IEEE 標準プロトコルです。クライアントは、RADIUS サーバーとの認証が成功しない限り、ネットワークにアクセスすることはできません。認証の種類には電子証明書を使った EAP-TLS、ID ／パスワードを使った EAP-MD5、電子証明書および ID ／パスワードを使った EAP-TTLS ／ PEAP などがあります。EAP-TLS/EAP-TTLS/PEAP では、クライアントと RADIUS サーバーで相互認証が成功するとセッションごとにネットワークキーが自動的に生成され、クライアントに配信されます。このため、無線 LAN 端末で個々にネットワークキーを設定する必要がありません。また、通信中にもネットワークキーを自動的に変更するためセキュリティが高まります。

IEEE802.3af

IEEE（米国電気電子学会）で LAN 技術の標準を策定している 802 委員会が定めた、LAN ケーブル経由でネットワーク機器に電源供給する規格です。

IP（Internet Protocol）

TCP/IP を構成するプロトコルの 1 つです。ネットワーク上の各通信機器に割り当てられた IP アドレスを利用して、機器間の通信経路の制御方法を定義しています。データが受信されたかどうかを確認するしくみを持たないプロトコルであるため、確実にデータが伝送される保証がありません。通常は TCP または UDP を上位レイヤとして通信を行いますが、信頼性を高くするためには TCP を併用します。

IP アドレス（Internet Protocol Address）

TCP/IP 環境で、コンピュータが通信するために使用するアドレスです。

現在使用されている IPv4 では、1 から 255 までの 4 個の数値で表します（例：192.168.100.123）。

また、IP アドレスには、グローバルアドレスとプライベートアドレスがあります。

□ L

LAN（Local Area Network）

同一フロアやビルなどの比較的狭い範囲で、コンピュータどうしを接続したネットワーク環境をいいます。

□ M

MAC アドレス（Media Access Control Address）

ネットワークカードに固有の物理アドレスです。

Ethernet ならバイト長で、先頭の 3 バイトはベンダコードとして IEEE が管理／割り当てを行っています。残り 3 バイトは各ベンダで独自に（重複しないように）管理しているコードですので、結果として、世界中で同じ物理アドレスを持つ Ethernet カードは存在せず、すべて異なるアドレスが割り当てられていることになります。Ethernet ではこのアドレスを元にフレームの送受信を行っています。

MAC アドレスフィルタリング

無線 LAN アクセスポイントに接続している無線 LAN 端末の MAC アドレスを判別し、無線 LAN アクセスポイントへの無線 LAN 端末のアクセスを制御するセキュリティ機能です。登録している無線 LAN 端末のみ接続できるようにしたり、登録している無線 LAN 端末の接続を制限したりすることができます。

MIB（Management Information Base）

SNMP で管理されるネットワーク機器に必ず保持されている管理情報データベースです。どのような情報が保持されているかは機器により異なります。MIB の種類には、RFC（Request For Comment）に規定されている標準 MIB や、ネットワーク機器のメーカーが独自に作成したプライベート MIB（または拡張 MIB）などがあります。

MIC（Message Integrity Code）

受信時にデータの改ざんを検知する機能です。この機能により改ざんされたパケットによるアクセスポイントへの不正接続やアタック攻撃を防止して、メッセージの完全性を保証します。

□ N

NTP（Network Time Protocol ）

ネットワークで結ばれたコンピュータや、ルータなどのネットワーク機器の間で、時刻を同期させるためのプロトコルです。インターネット上や LAN 上の NTP サーバーを指定すると、指定した NTP サーバーから時刻情報を取得します。

□ O

OFDM 方式（Orthogonal Frequency Division Multiplexing）

直交周波数分割多重のことで、多数の直交するキャリア信号を多重化するデジタル変調方式です。IEEE802.11a と IEEE802.11g で採用されているほか、地上波デジタル TV 放送でも使われています。エラー訂正に優れ、限られた無線帯域で高速な通信を実現する変調技術です。

□ P

PEAP（Protected Extensible Authentication Protocol）

IEEE802.1X の認証プロトコルの 1 つです。電子証明書を使って認証を行います。また、認証パケット自体をカプセル化するため、セキュリティレベルが高くなります。

PING（Packet INternet Groper）

インターネットやイントラネットなどの TCP/IP ネットワークで、相手先のコンピュータと通信できているかどうかや、通信回線の状況を確認するコマンドです。

Power over Ethernet

LAN ケーブル（カテゴリー 5 のツイストペアケーブル）を経由して、無線 LAN アクセスポイントに電源を供給する機能です。この機能を利用することにより、電源ケーブルが不要となり、新たにコンセントを作るなどの電源工事が不要となります。

Proxy ARP

ARP 要求を代理応答する機能です。本製品では、有線 LAN 側から受信した配下の無線 LAN 端末宛の ARP 要求に代理応答します。これにより、無線 LAN のトラフィックを軽減します。

□ Q

QoS（Quality of Service）

通信サービスの品質を保証するための機能や技術の総称です。ネットワーク上を流れているパケットには、Web アクセスやメール、ファイル転送などさまざまなサービスを提供するアプリケーションのものがあります。通常これらのパケットは、区別されることなく順番に処理されるため、それぞれのサービスに応じた品質を保証することはできません。QoS の技術では、パケットの優先度が考慮され、それぞれのサービスに必要な帯域幅を確保したり、遅延を少なくしたりすることが可能となります。これにより、アプリケーションが提供するサービスの品質を維持することができます。

□ R

RADIUS（Remote Authentication Dial-In User Service）

クライアント認証およびアカウント情報を提供するための業界標準プロトコルです。RADIUS を使用することにより、クライアント認証を集中管理したり、そのアカウントログを記録したりすることができます。

RADIUS アカウンティング

アカウンティングとは、アクセスログを記録することです。RADIUS アカウンティングは、RADIUS のアクセスログをアカウンティングサーバーに送出します。

RFC（Request for Comments）

インターネットで利用される技術を標準化する組織 IETF（Internet Engineering Task Force）によって発行される文書です。この文書にはインターネットに係わるさまざまな技術的仕様、ルールおよび知識などが含まれ、それぞれ通し番号を付けて公開されます。

RSSI（Received Signal Strength Indicator）

無線の電波信号の強さ（シグナルレベル）を表し、通信品質を評価する指標です。アクセスポイントが送出するビーコンパケットから取得します。建物の構造・材質／障害物／ソフトウェア／設置状況／電波状況などの使用環境により、数値は変動し、数値が大きい装置ほど安定した通信を行うことができます。

□ S

SNMP（Simple Network Management Protocol）

ネットワーク管理用のプロトコルで、ネットワークに接続されたルータなどの通信機器をネットワーク経由で監視、管理するために利用されます。SNMP のネットワークは、管理対象機器に実装されたエージェントと管理するコンピュータにインストールされたマネージャとで構成されます。

SNMP エージェント

SNMP で管理対象機器に実装されたインターフェースで、管理対象機器に保持された MIB と呼ばれる管理情報データベースを操作して、マネージャからの要求に対し、MIB 情報を返信したり、データベースを変更したりします。また、管理対象機器に特別なステータス変化が発生した場合、トラップをマネージャに通知します。

SNMP マネージャ

SNMP で管理するコンピュータにインストールされたソフトウェアで、管理対象機器のステータスや統計情報を要求したり、管理対象機器に保持された MIB と呼ばれる管理情報データベースの変更を要求したりして、管理対象機器の状態や統計情報を監視、管理します。SNMP マネージャを導入すると、ネットワークに接続されたルータやプリンタ、コンピュータなど SNMP に対応した通信機器の情報を一元管理することができるようになります。

SSID（Security Set Identifier）

無線 LAN ネットワークを構成するとき、混信やデータの盗難などを防ぐために、グループ分けをします。このグループ分けを「SSID」で行います。さらに、セキュリティ強化のためにネットワークキーを設定し、「SSID」とネットワークキーが一致しないと、通信できないようになっています。

SSID の隠蔽

無線 LAN のセキュリティ対策の 1 つです。

無線 LAN アクセスポイントが定期的に発信するビーコンというパケットには、SSID の情報が暗号化されずに含まれています。このため、Windows XP の機能や無線 LAN アクセスポイントを検索するようなユーティリティを利用すると、無線 LAN アクセスポイントの SSID を取得することができます。

SSID の隠蔽は、ビーコンに SSID の情報を載せないようにする機能です。この機能を有効にすることで、第三者から容易に SSID を取得されないようにして、不正に接続されるのを防ぎます。

本製品では、「ANY 接続拒否」を有効に設定すると SSID の隠蔽も有効になります。

Super A、Super G

米国アセロス・コミュニケーションズ社の開発した無線高速化技術です。通信データフレームをバースト転送する技術に加え、データの圧縮を行うことによって、無線通信をより高速化します。

Super A は IEEE802.11a 無線 LAN インターフェースに、Super G は IEEE802.11g 無線 LAN インターフェースにそれぞれ対応しています。

syslog

syslog とは、システムで発生したイベントや情報のログを、メッセージとしてネットワーク上に転送したり、ファイルに記録したりする機能です。

本製品では、ログを syslog サーバーに通知することができます。イベントログを通知することにより、syslog サーバー上で本製品の監視を行うことができます。障害の早期発見と解決に役立ちます。

□ T

TCP（Transmission Control Protocol）

TCP/IP を構成するプロトコルの 1 つです。コネクション型の通信で、送信したデータが正しく送信先に届いたかどうかの確認を行い、エラーが発生した場合データの再送を行います。UDP と比較すると、信頼性が高く安定した通信が行えますが、通信速度は低くなります。

TCP/IP（Transmission Control Protocol/Internet Protocol）

インターネット標準プロトコルであり、現在最も普及しているプロトコルです。TCP、UDP、IP など多くの関連プロトコルから構成されており、上位アプリケーションとのデータの受け渡しを行うための基盤となります。

TKIP（Temporal Key Integrity Protocol）

WEP に代わる暗号化方式です。静的な WEP に対し、動的にネットワークキーを生成します。ネットワークキーをパケットごとに自動的に更新したり、通信データを複雑にしたりして、暗号強度を大幅に高めています。

TPC（Transmit Power Control）

航空管制レーダーや気象レーダーなどで使用されるレーダー波との電波干渉を防止するための無線 LAN アクセスポイントの機能です。IEEE802.11a で使用できるチャンネルにこれらのレーダー波が使用する周波数帯（W53）が追加されたことで、この機能が必要となりました。無線 LAN アクセスポイントは、同周波数帯を利用する他の通信との干渉を防止するため、不必要に強い電波を出力しなくても通信品質の維持が可能な場合は、電波出力を自動的に 3dB（50%）低くして通信を行い干渉を最小化します。

□ U

UDP（User Datagram Protocol）

TCP/IP を構成するプロトコルの 1 つです。信頼性が低いコネクションレス型の通信で、送信したデータが正しく送信先に届いたかどうかの確認を行わず、エラーが発生してもデータの再送を行いません。TCP と比較すると、信頼性は低く通信は安定しませんが、高速なデータ通信が可能です。

□ V

VLAN（Virtual LAN）

企業内のネットワークにおいて、物理的なネットワーク接続とは別に、仮想的なネットワークグループ（VLAN グループ）を形成することです。同一グループでのみ通信を可能にし、別グループとの通信を制限することが可能です。本製品では、タグ付 VLAN と認証 VLAN をサポートしています。

VLAN ID

VLAN フレームが所属する VLAN を識別するための 12 ビット長の ID です。

□ W

WDS（Wireless Distribution System）

有線 LAN に接続している無線 LAN アクセスポイントと、もう 1 台の無線 LAN アクセスポイントをリンクさせる機能です。これによって、通信距離を延長したり、電波の届かない場所へ電波を中継したりできるようにします。アクセスポイント間通信、リピータ機能などと呼ばれる場合もあります。

WEP（Wired Equivalent Privacy）

無線 LAN でデータ通信を行う際に使用される、データの暗号化方式です。WEP で使用するキーとなる文字列を指定することにより無線区間の通信が暗号化されます。ネットワークキーの長さは、40、104、128 ビットから選択できます。

Wi-Fi®（Wireless Fidelity）

無線 LAN の互換性接続を保証する団体「Wi-Fi Alliance」の相互接続性テストに合格していることを示します。

WINS（Windows Internet Name Service）

NetBIOS 名による IP アドレス変換（名前解決）機能を、TCP/IP 上で実現するためのサービスです。サーバーとクライアントが直接データの送受信を行い、名前解決を実現するので、ブロードキャストによるネットワーク負荷を軽減することができます。また、ルータを介した環境や DHCP 環境での名前解決にも対応することができます。

WMM（Wi-Fi Multimedia）

WMM は IEEE802.11e で策定されている QoS 規格のうち、データの種類に基づいて優先制御する方式です。データを識別して、種類によって 4 種類のアクセスカテゴリに分類し、カテゴリごとに送信待ち時間やデータ送信時間に違いを付与して制御します。

WPA（Wi-Fi Protected Access）

WEP に代わる無線 LAN の暗号化方式の規格です。従来の SSID や WEP に加えて、クライアント認証機能、および暗号化方式に TKIP、AES を実装するなど、セキュリティ強度が向上しています。

WPA-PSK（WPA Pre-Shared Key）

WPA の家庭向け簡易認証方式です。PSK が無線 LAN 端末と一致した場合、相互認証を行います。適合する PSK を設定した無線 LAN 端末以外は通信できません。

■ひらがな／カタカナ／漢字で始まる用語

□ あ行

オープンシステム認証

無線 LAN のネットワーク認証の 1 つです。認証の際にネットワークキーの確認を行わないため、無線 LAN 端末は正しいネットワークキーを提示しなくても無線 LAN アクセスポイントと接続することができます。しかし、実際に通信を行う場合には同じネットワークキーが設定されている必要があります。オープンキー認証と呼ばれる場合があります。

□ か行

共有キー（シェアードキー）認証

無線 LAN のネットワーク認証の 1 つです。無線 LAN アクセスポイントは無線 LAN 端末に対して、同じネットワークキーが設定されているかどうかを認証の際に確認します。無線 LAN 端末が誤ったネットワークキーを使用している場合や、ネットワークキーが設定されていない場合は認証に失敗し、無線 LAN アクセスポイントと通信できなくなります。

グループキー

PSK によって生成されるキーのうちブロードキャスト／マルチキャストに使用されるキーを、グループキーといいます。

グローバルアドレス

インターネットで使われる IP アドレスです。国内では、JPNIC（日本ネットワークインフォメーションセンター）により管理されています。

コミュニティ名

SNMP で管理するネットワーク全体の識別子です。機器間認証のためのパスワードとして使用されるため、SNMP で通信するエージェントとマネージャの組み合わせには同じコミュニティ名を設定する必要があります。同じコミュニティ名を定義したエージェントとマネージャのみの通信を許可することで、セキュリティを確保しています。

コリジョン

同一 LAN 上の伝送路において、通信データが衝突することを示します。
端末数が多いネットワークなどで発生しやすく、2 台以上の端末からほぼ同時にデータが送信されることによって発生します。コリジョンが発生すると、通信データが破損してしまう場合があります。このような場合、各端末がデータ再送を行うため通信速度が低下します。

□ さ行

サブネットマスク

TCP/IP ネットワークは、複数の小さなネットワーク（サブネット）に分割されて管理されます。IP アドレスは、そのサブネットのアドレスと、個々のコンピュータのアドレスから構成されています。IP アドレスの何ビットがサブネットのアドレスかを定義するのが、サブネットマスクです。

サービスクラス

IEEE802.1D で規定されている 4 ビットの優先情報です。

□ た行

チャンネル

無線 LAN 端末や無線 LAN アクセスポイントで通信するために使用する、無線の周波数帯を表します。

デフォルトゲートウェイ

別のネットワークに所属するコンピュータとデータ通信を行う場合に、データの転送を行うコンピュータやルータなどの機器を指します。

ドメイン名

インターネットやイントラネット上のコンピュータやネットワークを、アルファベットや数字、または記号で表す固有の識別子です。富士通パソコン情報ページは「fmworld.net」がドメイン名（トップドメイン）になります。

トラップ

SNMP で管理するネットワーク機器上で特別な状態の変化が発生した場合に、エージェントからマネージャに通知するメッセージです。これにより、マネージャは管理対象機器の状態の変化を監視することができます。トラップされる情報は機器により異なりますが、主にシステムの起動や再起動、リンクダウン、リンクアップなどが通知されます。

□ な行

ネットワークアドレス

ネットワークアドレスとは、IP アドレスから個々のネットワーク機器を識別するホストアドレス部分を除いた部分で、ひとつのネットワークに対してひとつ与えられます。同一 LAN 上に存在するすべてのネットワーク機器には、同じネットワークアドレスを設定する必要があります。

IP アドレスが 192.168.2.1、サブネットマスクが 255.255.255.0 の場合、ネットワークアドレスは 192.168.2.0 になります。

ネットワークアドレスは、IP アドレスのホストアドレス部分を 0 としたものです。

ネットワークキー

無線 LAN でデータ通信を行う際に、データを暗号化するために使用する鍵情報です。

ネットワークセグメント

LAN上で構成されたネットワークの単位のことをネットワークセグメントと言います。ネットワークセグメントはルータなどにより分割され、異なるネットワークセグメント間の通信は通常、ルータなどを介して可能になります。

ネットワーク認証

無線 LAN 端末が、無線 LAN アクセスポイントと接続する場合に行う認証方式を指します。オープンシステム認証と、共有キー（シェアードキー）認証があります。認証方法は、それぞれの無線 LAN 端末に設定されていなければならず、通信したい無線 LAN アクセスポイントの設定とも一致している必要があります。認証モードと呼ばれる場合もあります。

□ は行

パケット

コンピュータの通信時に使用するデータの小さなまとまりを指します。パケットの中には送信元アドレス、送信先アドレス、実データなどが含まれ、このデータのやりとりを行うことでメールの送受信やホームページの表示などを行うことができます。

パスフレーズ

WPA の認証方式の 1 つ、PSK 認証で使用するネットワークキーを ASCII 文字で設定した値のことを指します。

ファームウェア

ハードウェアに組みこまれていて、基本的な動作／制御を行うプログラムです。本製品では、新機能の追加や改善のために、バージョンアップ用ファームウェアをご提供する場合があります。

ファイアウォール

通常、外部から内部のネットワークへの不正なアクセスを防ぐために設置する装置や、機能を指します。コンピュータなどに保存された重要なデータが、盗まれたり改ざんされたりしないようにします。

プライバシープロテクション

本製品を介した無線 LAN ネットワーク内で、無線 LAN 端末間通信を不可にする機能です。他の無線 LAN 端末からの個人情報の盗み見や、共有フォルダへのアクセスを防御できます。これにより、無線 LAN スポットサービスなど不特定多数の利用者が存在する環境で、各利用者のプライバシーを保護することができます。

プライベートアドレス

家庭内や企業内などの閉じたネットワーク（LAN）の中で使われる IP アドレスです。次の IP アドレスが、プライベートアドレスとして、家庭内や組織内などの LAN の中で自由に使えることになっています。

- 10.0.0.0 ～ 10.255.255.255
- 172.16.0.0 ～ 172.31.255.255
- 192.168.0.0 ～ 192.168.255.255

プリアンブル

無線LANアクセスポイントと無線LAN端末間で送受信されるパケットの先頭に付加される情報で、受信側が同期をとるために使用されます。情報の長さによって、ロングプリアンブルとショートプリアンブルがあります。

ロングプリアンブルは、常に同じ長さの情報を送ります。ショートプリアンブルと比較すると、信頼性が高く安定した通信が行えますが、通信速度は遅くなります。

ショートプリアンブルは、プリアンブルの長さを短くします。ロングプリアンブルと比較すると、信頼性は低く通信は安定しませんが、通信速度は速くなります。

ブロードキャスト

同一ネットワーク内のすべてのコンピュータにデータを送信することです。送信時に使用するパケットをブロードキャストパケットといい、ブロードキャストパケットが送信される範囲をブロードキャストドメインといいます。

プロキシサーバー

インターネット（WAN）側と LAN 側の中間に存在し、直接インターネット通信ができないコンピュータの代理（プロキシ）をして、インターネット通信を実現させるサーバーの総称です。主に企業などの社内ネットワークで利用されます。プロキシサーバーのキャッシュ機能や通信経路の変更機能によって、インターネット通信の高速化、サーバーやネットワークの負荷軽減ができます。また双方向通信を制限して、社内ネットワークの効率的運用やセキュリティの向上を実現できます。

プロトコル

コンピュータ間でのデータの受け渡しを行うための手順や規則です。データの送受信方法、通信エラー時の処理など、通信を行うために必要な条件を、すべて手順化しておくことで、規則正しい情報の伝達が行えます。

ポート番号

インターネットなど TCP/IP を使用した通信の際に使用される番号です。サーバーで使用されるサービスごとに割り当てられて区別されるため、同時に複数の相手と通信を行うことが可能になります。

ホストアドレス

IP アドレスからネットワークアドレス部分を除いた部分で、同一ネットワーク上で個々のネットワーク機器を識別するためのアドレスです。同一ネットワーク上に存在するすべてのネットワーク機器には、異なるホストアドレスを設定する必要があります。

□ ま行

マルチキャスト

ネットワーク上のコンピュータをグループ分けしているときに、グループをあて先に指定してデータを送信することをマルチキャストといいます。グループに所属しているすべてのコンピュータにデータが届きます。送信時に使用するパケットをマルチキャストパケットといいます。

マルチプル SSID

1 つの無線 LAN インターフェースに複数の SSID を設定して、複数の無線 LAN ネットワークを同時に構築する機能です。

□ ら行

リンクインテグリティ

ローミング機能を使用しているネットワークで利用できる機能です。指定した有線LAN側経路（本製品、本製品に接続している有線経路、HUB）を常時監視します。そして、経路の異常を検知すると無線電波を停止して、強制的に無線 LAN 端末をローミングさせます。こうして、無線 LAN 端末がネットワークから切断されるのを防ぐことができます。

ローミング

無線 LAN 通信を行っているコンピュータが、複数の無線 LAN アクセスポイント間を移動できるようにする機能です。例えば、ビルの各フロアに無線 LAN アクセスポイントを設置しておくことで、どこに移動してもネットワークアクセスが可能となります。

索引

あ行

か行

さ行

た行

な行

は行

ま行

ら行

ワイヤレス LAN ステーション FMWT-56AG 取扱説明書

B5FY-7021-01 Z2-00

発行日　2006 年 7 月
発行責任　富士通株式会社