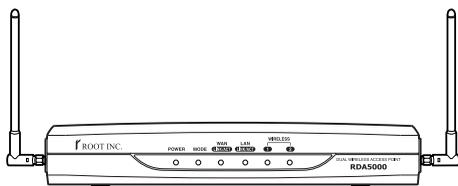


取扱説明書[導入編]

DUAL WIRELESS ACCESS POINT
RDA5000

本書は、最初にお読みください。
本製品を使うための基本的な内容について説明しています。
そのほかにも、各設定項目などを説明する取扱説明書[活用編]を収録していますので、必要に応じてご覧ください。



- ご使用になる前に **1**
- 有線LANで使う **2**
- 無線LANで使う **3**
- 回線接続ガイド **4**
- その他の基本設定 **5**
- 保守について **6**
- ご参考に **7**

はじめに

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

本製品は、IEEE802.11aとIEEE802.11b/g規格*の無線LANを内蔵するブロードバンド対応ワイヤレスアクセスポイントです。

ご使用前に、この取扱説明書をよくお読みいただき、本製品の性能を十分発揮していただくとともに、末長くご愛用くださいますようお願い申し上げます。

※本製品が対応する無線LAN規格は、以下の通りです。

IEEE802.11a：54Mbps(5.2GHz帯)

IEEE802.11b：11Mbps(2.4GHz帯)

IEEE802.11g：54Mbps(2.4GHz帯)

※[IEEE802.11b]規格は、[IEEE802.11g]規格と互換性がありますので、本製品の[IEEE802.11g]規格に設定された内容で通信できます。

※[IEEE802.11]規格(ch14)には対応していません。

登録商標について

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

本書に記載されている会社名、製品名は、各社の商標および登録商標です。

標準構成

本製品のパッケージには、次のものが同梱されています。

本製品をご使用になる前に、すべて揃っていることを確認してください。

- ◎RDA5000(本製品)……………1台
- ◎デュアル外部アンテナ(2.4/5.2GHz無線LAN用) ……2本
- ◎本体固定用金具……………1式
- ◎ACアダプター……………1個
- ◎Ethernetケーブル(3m)※[LAN/WAN]ポート接続用……………1本
- ◎CD(UTILITYディスク)……………1枚
- ◎電波干渉注意シール……………1枚
- ◎取扱説明書[導入編](CDに収録)
- ◎保証書

不足しているものがありましたら、お手数ですがお買い上げの販売店または弊社営業所サービス係までお問い合わせください。

ユーザー登録について

本製品のユーザー登録は、ルートホームページで行っています。

インターネットから、「<http://www.root-hq.com/>」にアクセスしていただき、ユーザー登録用フォームにしたがって必要事項をご記入ください。

ご登録いただけない場合、サポートサービスをご提供できませんのでご注意ください。

情報処理装置等電波障害自主規制について

この装置は、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A情報技術装置です。

この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。

この場合には使用者が適切な対策を講ずるよう要求されることがあります。

はじめに

本製品の概要について

- ◎本製品は、802.11b規格と互換性がある802.11g規格の無線LANカードと802.11a規格の無線LANカードを内蔵していますので、本製品1台で5.2GHz帯(54Mbps)と2.4GHz帯(54Mbps)の無線LANを構築できます。
- ◎異なる無線LAN規格の無線パソコンが本製品を介して相互に通信できます。
- ◎付属のアンテナは、5.2GHz帯と2.4GHz帯に対応するデュアル外部ダイバーシティー方式を採用しています。
- ◎別売の「分離式デュアル平面アンテナ」を2個1組でご使用いただくことで、ダイバーシティー方式で通信でき、設置環境に影響されない場所に設置できます。また、伝送距離についても付属アンテナの約1.5倍まで延長できます。
- ◎無線AP(アクセスポイント)間通信機能の搭載により、本製品どうしを無線ブリッジ接続できます。
- ◎スパニングツリー機能の搭載により、ネットワークループによるネットワーク障害を防止できます。
- ◎不正アクセス検知機能を搭載していますので、常時接続での信頼性が向上します。
- ◎次世代の暗号化セキュリティとしてWEP(RC4)より強力なOCB AESを搭載しています。
- ◎暗号化認証は、「シェアードキー」と「オープンシステム」の両モードに対応しています。
- ◎新しいセキュリティの国際規格であるIEEE802.1xを使用したユーザー認証に対応していますので、信頼性の高い無線通信が行えます。
- ◎有線LANは、10BASE-T/100BASE-TX(自動切り替え)に対応しています。
- ◎FTTH、xDSL、CATV回線の接続にも対応しています。
- ◎ネットワーク管理機能にはSNMPをサポートしています。
- ◎本製品は、技術基準適合証明を取得していますので、無線局の免許は不要です。

取り扱い上のご注意

- ◎動作中に接続ケーブルなどが外れたり、接続が不安定になると、誤動作の原因になります。コネクタをしっかりと接続してください。
動作中は、コネクタの接続部に触れないでください。
- ◎モデムおよびパソコンやその他の周辺機器の取扱いは、それぞれに付属する取扱説明書に記載する内容にしたがってください。
- ◎家庭環境で使用すると電波妨害を引き起こすことがあります。
このようなときは、本製品を、妨害を受けている機器からできるだけ離して設置してください。
- ◎本製品のCD(Adobe Readerを除く)は、本機専用ですので、本機以外の製品で使用しないでください。
- ◎本製品の設定ファイルや弊社ホームページ(<http://www.root-hq.com/>)より提供されるアップデート用ファームウェアファイルを、本製品以外の機器に組み込んだり、改変や分解したことによる障害、および本製品の故障、誤動作、不具合、破損、データの消失あるいは停電などの外部要因により通信、通話などの機会を失ったために生じる損害や逸失利益または第三者からのいかなる請求についても弊社は一切その責任を負いかねますのであらかじめご了承ください。
- ◎本書の著作権およびハードウェア、ソフトウェアに関する知的財産権は、すべてルート株式会社に帰属します。
- ◎本書の内容の一部または全部を無断で複製/転用することは、禁止されています。
- ◎本書およびハードウェア、ソフトウェア、外観の内容については、将来予告なしに変更することがあります。

表記について

本書は、次の表記規則にしたがって記述しています。

- 「 」表記：オペレーションシステム(OS)、ユーティリティ、メニュー、ウィンドウ(画面)の名称を(「」)で囲んで表記します。
- []表記：タブ名、アイコン名、テキストボックス名、チェックボックス名などを([])で囲んで表記します。
- 〈 〉表記：ダイアログボックスのコマンドボタンなどの名称を(〈 〉)で囲んで表記します。

※本書は、Ver1.18のファームウェアを使用して説明しています。

※Windows Millennium Editionは、Windows Meと表記します。

Windows 98 Second Editionは、Windows 98 SEと表記します。

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

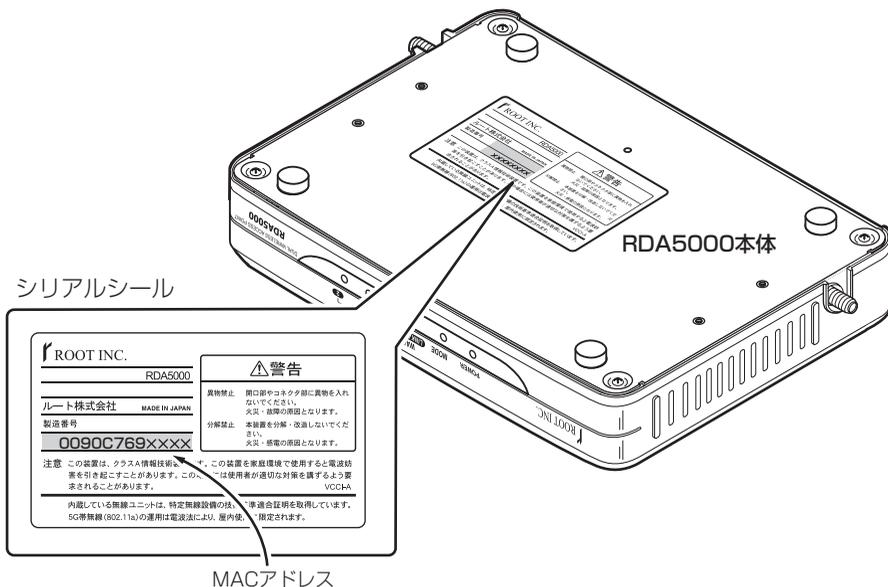
はじめに

MACアドレス表記について

本製品をインターネットに接続してご使用になる場合、ご契約の接続業者またはプロバイダーや提供を受けるサービスによっては、モデムに直接接続するネットワーク機器(本製品)がそれぞれ独自に持っているMACアドレス(機器固有の番号)を、接続業者またはプロバイダーに対して事前申請する必要があります。

そのような場合、申請および登録が完了するまで、本製品を利用してインターネットに接続できません。(すでに登録したMACアドレスでご使用の場合※取扱説明書[活用編]の[MSS制限値]参照)

MACアドレスは、モデムに直接接続するネットワーク機器(本製品など)がそれぞれ独自に持っている機器固有の番号で、下図のように本製品のシリアルシールに記載されています。



※シリアルシールの記載内容に変更があった場合、MACアドレスの記載位置は、お買い上げの製品によって若干異なる場合があります。

無線LANの電波法についてのご注意

- 電波法により、屋外で5.2GHz帯(IEEE802.11a)無線LANを使用することは禁じられています。
- 本製品に使用している無線装置は、電波法に基づく小電力データ通信システムの無線設備として、特定無線設備の認証を受けています。
したがって、本製品の使用に際しては、無線局の免許は必要ありません。
- 本製品を使用できるのは、日本国内に限られています。
本製品は、日本国内での使用を目的に設計・製造しています。
したがって、日本国外で使用された場合、本製品およびその他の機器を壊すおそれがあります。
また、その国の法令に抵触する場合がありますので、使用できません。
- 心臓ペースメーカーを使用している人の近くで、本製品をご使用にならないでください。
心臓ペースメーカーに電磁妨害をおよぼして、生命の危険があります。
- 医療機器の近くで本製品を使用しないでください。
医療機器に電磁妨害をおよぼして、生命の危険があります。
- 電子レンジの近くで本製品を使用しないでください。
電子レンジによって本製品の無線通信への電磁妨害が発生します。
- 本製品の無線装置は、電波法に基づく認証を受けていますので、本製品の分解や改造をしないでください。

はじめに

2.4GHz無線LANの電波干渉についてのご注意

2.4GHz帯(IEEE802.11b/g)無線LANで通信を行うときは、次のことがらに注意してご使用ください。

この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局(免許を必要とする無線局)および特定小電力無線局(免許を必要としない無線局)並びにアマチュア無線局(免許を必要とする無線局)が運用されています。

- この機器を使用する前に、近くで移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局が運用されていないことを確認してください。
- 万一、この機器から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか、または電波の発射を停止した上、下記連絡先にご連絡いただき、混信回避のための対処等(例えば、パーティションの設置など)についてご相談してください。
- その他、この機器から移動体識別用の特定小電力無線局あるいはアマチュア無線局に対して有害な電波干渉の事例が発生した場合など、何かお困りのことが起きたときは、次の連絡先へお問い合わせください。

連絡先：ルート株式会社

サービス窓口：03-5840-7601

■ 内蔵の2.4GHz帯(IEEE802.11b/g)無線LANカードについて

使用周波数帯域：2.4GHz帯を使用する無線設備

変調方式：DS-SS方式/OFDM方式

想定干渉距離：40m以下

周波数変更可否：全帯域を使用し、かつ移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局の帯域を回避可能

取扱説明書の構成について

本書では、本製品をご使用になる前に知っておいていただきたい新機能や基本的な内容と、インターネットやLANへ接続するための基本的な設定手順と接続方法について説明しています。

導入編には記載していない詳細な機能を設定する場合は、本製品に付属の活用編を参照してください。(本製品のCDにPDF形式で収められています。)

■ 導入編(CD収録)

本製品の基本的な使用方法について、本書を最初から順番に読みながら作業が進められるように構成されています。

詳細な機能についての情報は、活用編で説明していますので、必要に応じて参照してください。

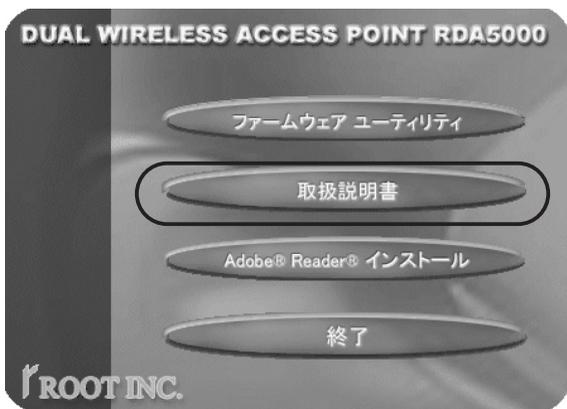
■ 活用編(CD収録)

本製品に設定できるさまざまな機能について、本製品の設定メニューごとに説明しています。

- ① 本製品のCDをご使用のCDドライブに挿入すると、Auto Run機能が動作して、メニュー画面を表示します。
- ② 〈取扱説明書〉をクリックします。

【お願い】

取扱説明書[活用編]をご覧いただくとき、Acrobat Reader4.0以上をインストールされていないかたは、〈取扱説明書〉ボタンをクリックする前に、〈Adobe Reader インストール〉ボタンをクリックして、表示される画面にしたがってインストールしたあとで、〈取扱説明書〉ボタンをクリックしてください。



※CD収録のファームウェアユーティリティは、下記のOSに対応しています。

Windows XP/2000/Me/98SE/98

※メニュー画面が表示されないときは、本製品のCDに収録された「AutoRun.exe」をダブルクリックしてください。

ご使用までの流れ

本製品を導入されるときは、次のステップにしたがってお読みください。
順番に基本的な設定ができる構成になっています。
各ステップの右端に記載する数字は、本書の参照ページです。



はじめに	i
ご使用までの流れ	ix
もくじ	x
安全上のご注意(必ずお読みください。)	xii

第1章 ご使用になる前に 1

1-1.前面パネル	2
1-2.後面パネル	3
1-3.デュアル外部アンテナについて	4
1-4.本製品のおもな機能	5
1-5.収容台数について	8
1-6.本製品の設置について	9
1-7.設定画面の名称と機能	12

第2章 有線LANで使う 15

2-1.Ethernetカードの装着	16
2-2.[LAN]ポートへのパソコン接続	17
2-3.アース線と電源を接続する	18
2-4.パソコンの電源を入れる	18
2-5.IPアドレスを確認する	19
2-6.設定画面へのアクセスを確認する	22

第3章 無線LANで使う 23

3-1.無線LANで通信するパソコンについて	24
3-2.無線LANの構築について	24
3-3.無線アクセスポイント機能を使用してみる	29
3-4.無線AP(アクセスポイント)間通信機能を使用してみる	32
3-5.無線ネットワーク名(SSID)を設定する	36
3-6.暗号化を設定する	37
3-7.MACアドレスセキュリティーを設定する	43
3-8.802.11b規格の通信を制限するには	44
3-9.スパンニングツリー機能を使用してみる	45

第4章 回線接続ガイド 47

Step1.回線接続業者との契約について	48
Step2.お使いになるモデムタイプの確認	48
Step3.ご契約回線への接続方法を確認する	49
Step4.回線種別を設定する	50
Step5.モデムと接続する	56
Step6.インターネットへの接続を確認する	58

第5章 その他の基本設定 59

5-1.本製品の時計を設定する	60
5-2.設定画面へのアクセスを制限するには	61
5-3.本体IPアドレスを変更するには	62
5-4.自動割り当て開始IPアドレスを変更するには	63
5-5.DHCPサーバ機能を停止するには	64

第6章 保守について 65

6-1.設定内容の確認または保存	66
6-2.保存された設定の書き込み	67
6-3.設定を出荷時の状態に戻す	68
6-4.ファームウェアをバージョンアップする	73
6-5.本製品のMACアドレスを確認するには	76

第7章 ご参考に 77

7-1.困ったときは	78
7-2.設定項目の初期値一覧	82
7-3.設定画面の構成について	84
7-4.機能一覧	86
7-5.各種ポート仕様	86
7-6.定格	87
7-7.故障のときは	91
7-8.用語解説	92

安全にご使用いただくために、必ずお読みください。

- ここに示した注意事項は、使用者および周囲の人への危害や財産への損害を未然に防ぎ、製品を安全に正しくご使用いただくために、守っていただきたい事項を示しています。
- 次の『△警告』『△注意』の内容をよく理解してから本文をお読みください。
- お読みになったあとは、いつでも読める場所へ大切に保管してください。

■ 本製品について

警告

下記の記載事項は、これを無視して誤った取り扱いをすると「使用者および周囲の人が、死亡または重傷を負う可能性が想定される内容」を示しています。

- ◎付属のACアダプター以外は使用しないでください。
火災、感電、故障の原因になります。
- ◎指定以外の付属品、および別売品は使用しないでください。
火災、感電、故障の原因になります。
- ◎DCジャック以外の端子に電源を接続しないでください。
火災、感電、故障の原因になります。
- ◎接続ケーブルを加工したり、無理に曲げたり、ねじったり、引っ張ったり、加熱したりしないでください。
傷ついて破損し、火災、感電、故障の原因になります。
- ◎接続ケーブルの上に重いものを載せたり、挟んだりしないでください。
傷ついて破損し、火災、感電、故障の原因になります。
- ◎電源コードや接続ケーブルは、赤ちゃんや小さなお子さまの手が届かない場所で使用、設置してください。
感電、けがの原因になります。
- ◎完全調整していますので、分解、改造は、絶対にしないでください。また、ご自分で修理しないでください。
火災、感電、故障の原因になります。
- ◎通気口をふさがないでください。
発熱などにより、火災、感電、故障の原因になります。
- ◎水などでぬれやすい場所(加湿器のそばなど)に設置しないでください。
火災、感電、故障の原因になります。
- ◎本製品を使用中は、ぬれた手で本製品に触れないでください。
感電の原因になります。
- ◎設置する場合は、必ずアース線を接続してください。また、アース線は、ガス管や水道管に接続しないでください。
火災、感電の原因になります。
- ◎万一、煙が出ている、変なおいがする、変な音がする、水などがに入った場合は、使用を中止してください。
そのまま使用すると、火災、感電、故障の原因になります。
すぐに、本製品に接続しているACアダプターのプラグとその他のケーブル類を取り外してください。
煙が出なくなるのを確認してからお買い上げの販売店、または弊社営業所サービス係に連絡してください。

安全上のご注意

■ 本製品について(つづき)

⚠ 注意

下記の記載事項は、これ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、および物的損害だけの発生が想定される内容」を示しています。

◎屋外に設置しないでください。

故障の原因になることがあります。

◎ぐらついた台の上や、傾いたところなど、不安定な場所に置かないでください。

落ちたり、倒れたりして火災、けが、故障の原因になることがあります。

◎湿気やホコリの多い場所、風通しの悪い場所には設置しないでください。

故障の原因になることがあります。

◎直射日光のあたる場所やヒーター、クーラーの吹き出し口など、温度変化の激しい場所では使用しないでください。

変形、変色、火災、故障の原因になることがあります。

◎説明と異なる接続をしないでください。また、本製品への接続を間違えないように十分注意してください。

故障の原因になることがあります。

◎強い磁界や静電気の発生する場所、温度、湿度が取扱説明書に定めた使用環境を超えるところでは使用しないでください。

故障の原因になることがあります。

◎テレビやラジオの近くで使用しないでください。

電波障害を与えたり、受けたりする原因になることがあります。

◎落としたり、強い衝撃を与えたりしないでください。

けが、故障の原因になることがあります。

◎上に乗ったり、重い物を載せたり、挟んだりしないでください。

故障の原因になることがあります。

◎近くに雷が発生したときは、ACアダプターを接続しているコンセントから抜いて、ご使用をお控えください。ケーブルの接続や切断、または製品の導入や保守の作業も行わないでください。

火災、感電の原因になることがあります。

◎結露するような場所で使用しないでください。温度差の激しい環境を急に移動した場合、結露するおそれがありますのでご注意ください。

変形、変色、火災、故障の原因になることがあります。

結露した場合、乾燥させるか、長い間同じ環境に置いたあと、ご使用ください。

◎長時間、使用しないときは、安全のため本製品に接続しているACアダプターを取り外してください。

発熱、発火、故障の原因になることがあります。

◎清掃するときは、シンナーやベンジンを絶対使用しないでください。

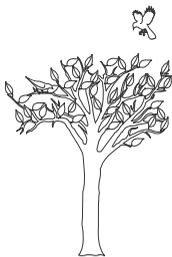
ケースが変質したり、塗料がはげる原因になることがあります。普段はやわらかい布で、汚れのひどいときは水で薄めた中性洗剤を少し含ませてふいてください。

■ ACアダプターについて(付属品)

警告

下記の記載事項は、これを無視して誤った取り扱いをすると「使用者および周囲の人が、死亡または重傷を負う可能性が想定される内容」を示しています。

- ◎本製品以外の機器で使用しないでください。
火災、感電、故障の原因になります。
- ◎AC100V以外の電源電圧で使用しないでください。
火災、感電、故障の原因になります。
- ◎抜き差しするときは、必ずDCコネクタやACアダプター本体を持って行ってください。
火災、感電、故障の原因になります。
- ◎ACアダプターは、コンセントの奥まで確実に差し込んでください。
差し込みが不十分な場合、火災、感電の原因になります。
- ◎電源コードを加工したり、無理に曲げたり、ねじったり、引っ張ったり、加熱したりしないでください。
傷ついて破損し、火災、感電、故障の原因になります。
- ◎電源コードの上に重いものを載せたり、挟んだりしないでください。
傷ついて破損し、火災、感電、故障の原因になります。
- ◎ACアダプターは、タコ足配線しないでください。
火災、感電、故障の原因になります。
- ◎ぬれた手でACアダプターや機器に絶対触れないでください。
感電の原因になります。
- ◎水などでぬれやすい場所で使用しないでください。
火災、感電、故障の原因になります。
- ◎アダプターの金属部分、およびその周辺にホコリが付着している場合は、乾いた布でよくふき取ってください。
そのまま使うと、火災の原因になります。
- ◎電源コードが傷ついたり、コンセントの差し込みがゆるいときは使用しないでください。
火災、感電、故障、データの消失または破損の原因になりますので、お買い上げの販売店、または弊社各営業所サービス係に連絡してください。



この章では、
本製品のおもな機能と設置方法などについて説明します。

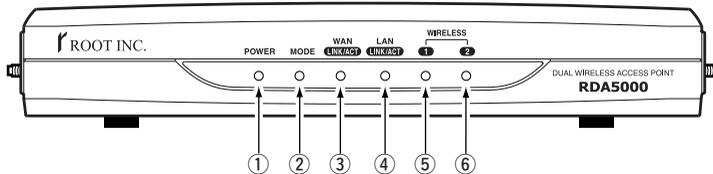
1-1.前面パネル	2
1-2.後面パネル	3
1-3.デュアル外部アンテナについて	4
■デュアル外部アンテナの取り付けかた	4
1-4.本製品のおもな機能	5
■無線AP(アクセスポイント)間通信機能	5
■スパンニングツリー機能	6
■無線セキュリティについて	7
1-5.収容台数について	8
■負荷分散機能について	8
1-6.本製品の設置について	9
■設置場所について	9
■無線通信距離について	9
■分離式デュアル平面アンテナ(別売品)	9
■設置方法について	10
1-7.設定画面の名称と機能	12
■設定画面について	12
■設定画面選択メニュー	13

【ご参考：Ethernetケーブルについて】

100BASE-TX(高速有線LAN)通信を行うには、本製品に付属するようなカテゴリ5以上のEthernetケーブルを使う必要があります。
カテゴリの低いものを同じLAN上に混用すると、一番低いグレードにあわせて全体のケーブル特性が低下するので、ご注意ください。

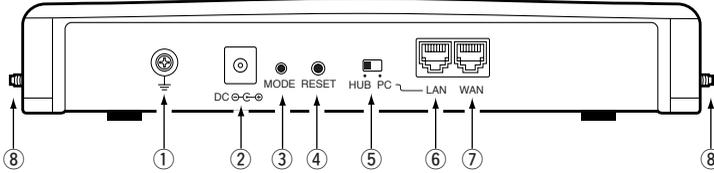
1 ご使用になる前に

1-1. 前面パネル



- ① [POWER]ランプ…… 点灯：本製品に電源が供給されているとき
[MODE]ランプと同時点滅：「設定初期化」モード
[MODE]ランプと交互点滅：「Firm Utility使用」モード
- ② [MODE]ランプ …… [POWER]ランプと同時点滅：「設定初期化」モード
[POWER]ランプと交互点滅：「Firm Utility使用」モード
- ③ [WAN **LINK/ACT**]
ランプ …………… 点灯：EthernetケーブルでWAN側と接続されたとき
点滅：WAN側とデータを送受信しているとき
- ④ [LAN **LINK/ACT**]
ランプ …………… 点灯：EthernetケーブルでLAN側と接続されたとき
点滅：LAN側とデータを送受信しているとき
- ⑤ [WIRELESS **1**]
ランプ …………… 点灯：802.11b/g規格の無線LANで通信を確立した時
消灯：以下の2通りがあります。
● 1～2分間以上、802.11b/g規格の無線LANで通信しない状態が継続したとき
● 本製品と通信中の802.11bおよび802.11g規格の無線パソコンが無線伝送エリア内に存在しないとき
- ⑥ [WIRELESS **2**]
ランプ …………… 点灯：802.11a規格の無線LANで通信を確立した時
消灯：以下の2通りがあります。
● 1～2分間以上、802.11a規格の無線LANで通信しない状態が継続したとき
● 本製品と通信中の802.11a規格の無線パソコンが無線伝送エリア内に存在しないとき

1-2. 後面パネル



- ① アース端子 …………… アース線を接続する端子です。
アース線は、市販品をご用意ください。
- ② DCジャック …………… 付属のACアダプターを接続します。
- ③ 〈MODE〉ボタン …… 「設定初期化」モードで動作させるときに使用します。
※ペンの先などを利用して押してください。(※6-3章)
- ④ 〈RESET〉ボタン …… 短く押すと、本製品を再起動(電源投入直後の状態)します。
※電源を入れなおすのと、同じ状態です。
- ⑤ [HUB/PC]スイッチ …… [LAN]ポートの極性を反転させるスイッチです。
出荷時の設定は、「PC」です。
HUBを本製品にカスケード接続するときは「HUB」側に切り替えます。
- ⑥ [LAN]ポート …… LAN側のイーサネットポート(RJ-45型)です。
Ethernetケーブルを使用して、パソコンやHUB、またはADSLやCATVのルータタイプモデムと接続します。
- ⑦ [WAN]ポート …… WAN側のイーサネットポート(RJ-45型)です。
Ethernetケーブルを使用して、ADSLやCATVのブリッジタイプモデムやメディアコンバーター(FTTH)と接続します。
- ⑧ アンテナコネクター …… 付属のデュアル外部アンテナ(2本)を接続します。

1 ご使用になる前に

1-3. デュアル外部アンテナについて

付属のアンテナは、本製品の無線LANで通信するときに使用します。

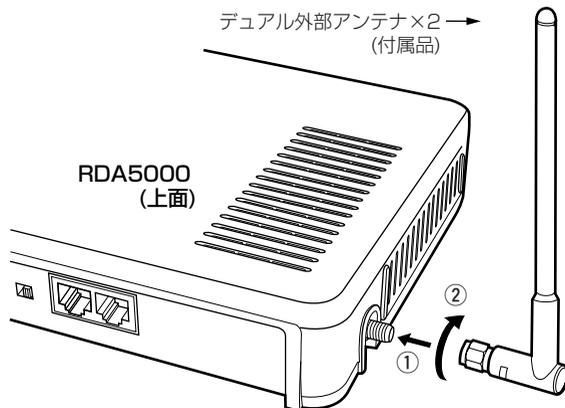
無線LANを使用するときは、2本のアンテナ(付属品)を本製品の側面に取り付けます。

2本のアンテナを接続すると、外部ダイバーシティーとして機能しますので、マルチパスに強く安定した電波状態で通信できます。

■ デュアル外部アンテナの取り付けかた

アンテナを取り付けるときは、ナットの部分を右方向に手で締まる程度まで回します。

左方向に回すと取り外しできます。(1本ずつ左右に取り付けてください。)



※分離式デュアル平面アンテナ(別売品)の接続について

分離式デュアル平面アンテナを2個1組でご使用いただくことで、デュアル(5.2/2.4GHz帯)ダイバーシティー方式で通信できます。

分離式デュアル平面アンテナを片側のアンテナコネクターだけに接続するときは、後面パネルから見て右側のコネクター(上記の図に示す位置)に接続してください。

残りのアンテナコネクターには、RDA5000に付属のデュアル外部アンテナを接続できます。

△警告

本製品に取り付けたアンテナの端を持って本製品を振り回さないでください。

本人や他人に当たって、けがや故障、および破損の原因になります。

△注意

本製品は、技術基準適合証明を取得していますので弊社指定以外のアンテナを使用できません。

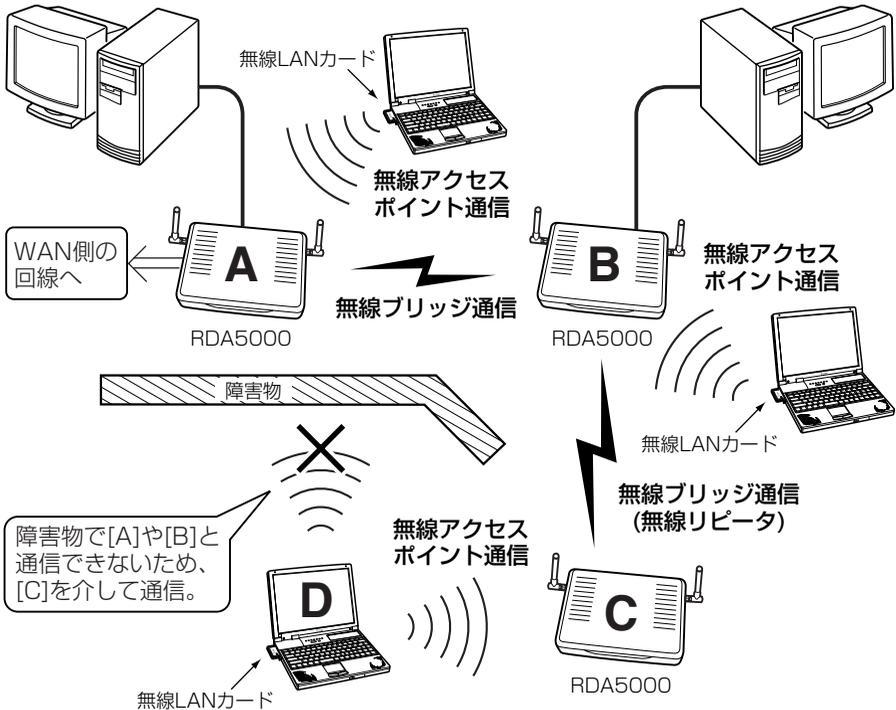
1-4. 本製品のおもな機能

■ 無線AP(アクセスポイント)間通信機能

無線AP間通信機能を使用すると、最高54Mbps(802.11a/802.11g)の伝送速度で本製品(図：A-B間)どうしを無線ブリッジで接続できます。

無線ブリッジ接続により、本製品どうしをワイヤレス接続しますので、リピータ(図：C)としても使用できます。

無線パソコン(図：D)の電波が障害物等で遮断されたとき、リピータ機能を使うと、本製品と無線ブリッジ接続されたもう一台の無線アクセスポイント(図：C)と通信して、障害物を回避させることができます。



※無線AP間通信機能は、本製品搭載の無線LAN規格(802.11a/g)で使用できます。

※無線ブリッジ(無線リピータを含む)を使用する場合は、通信相手とのあいだで本製品に内蔵された無線LANカードの[BSSID]を登録しあう必要があります。

上記の図では、[B]の[BSSID]を[A]と[C]のそれぞれに登録します。

また、[A]と[C]の[BSSID]を[B]に登録します。

各機器の[BSSID]は、本製品の設定画面にアクセスして確認してください。

※無線ブリッジとして収容できるのは、最大7台(自分の機器を含む)までです。

※リピータ機能で使用する場合は、本製品(図：BとC)の[SSID]を同じに設定してください。(図：A-B間は、リピータとして使用しないため異なる[SSID]でも可能です。)

1 ご使用になる前に

1-4. 本製品のおもな機能(つづき)

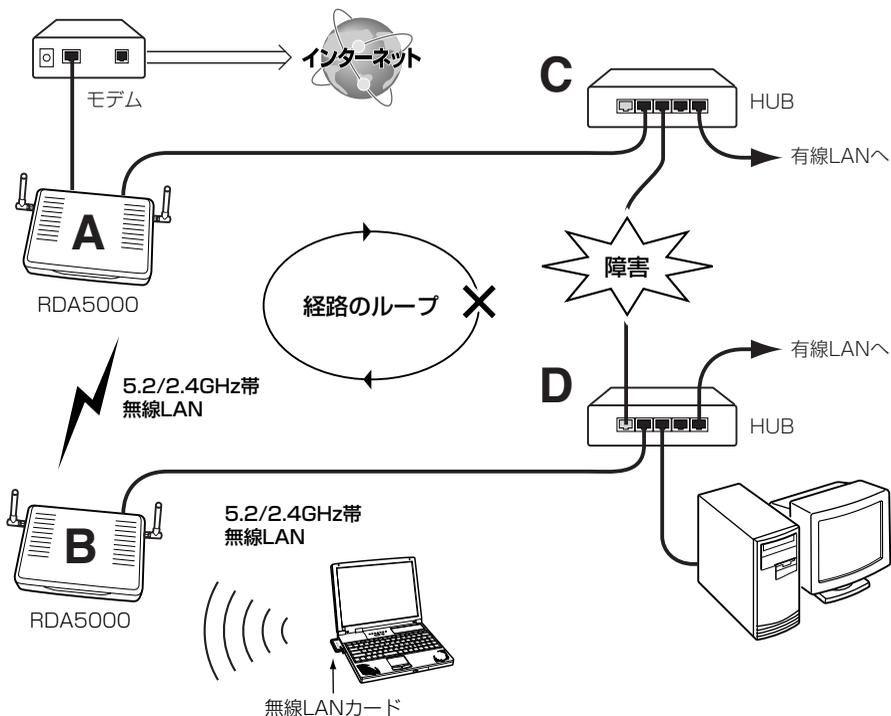
■ スパニングツリー機能

本製品は、ブリッジ間の通信において経路のループを検出し、パケットが無限に循環するのを回避して、最適な経路を作成する機能です。

下記のネットワーク例で、スパニングツリー機能を本製品(図：AとB)に設定した場合、障害のないときは、経路のループを検出して重複する経路のうち優先度の低い方(例、図：A-B間)を遮断します。

カスケード接続されたHUB(図：C-D間)の経路で通信障害が起こったときは、本製品(図：A-B間)の無線通信を有効にして、ネットワークの正常な稼働を保持します。

この機能を使用しない場合、ネットワーク上の通信パケットは、本製品とHUB(図：B→D→C→A→B)間を循環しつづけます。



■ 無線セキュリティについて

本製品は、下記のセキュリティを搭載しています。

※通信する相手と暗号化方式や暗号化ビット数の設定が異なると通信できません。

【WEP (RC4)】：無線LAN機器で一般によく搭載されている暗号化方式で、RC4(Rivest's Cipher 4)アルゴリズムをベースに構成されています。

暗号化するデータのブロック長が8ビットで、暗号化鍵の長さ(64/128/152ビット)を選択できます。

また、シェアードキーによる暗号化認証にも対応しています。

※152ビットは、無線LANカードによって非対応場合があります。

【OCB AES】：[WEP(RC4)]より強力で、標準化が推進されている次世代暗号化方式です。暗号化するデータのブロック長と暗号化鍵(キー)の長さは、128ビットです。

※OCB AES対応の無線LANカードにつきましては、別途お問い合わせください。

【IEEE 802.1x】：本製品との無線通信に使用する認証システムです。

「IEEE 802.1x」に対応した無線LANカード(※3-2章)を装着するWindows XP搭載のパソコンが必要です。

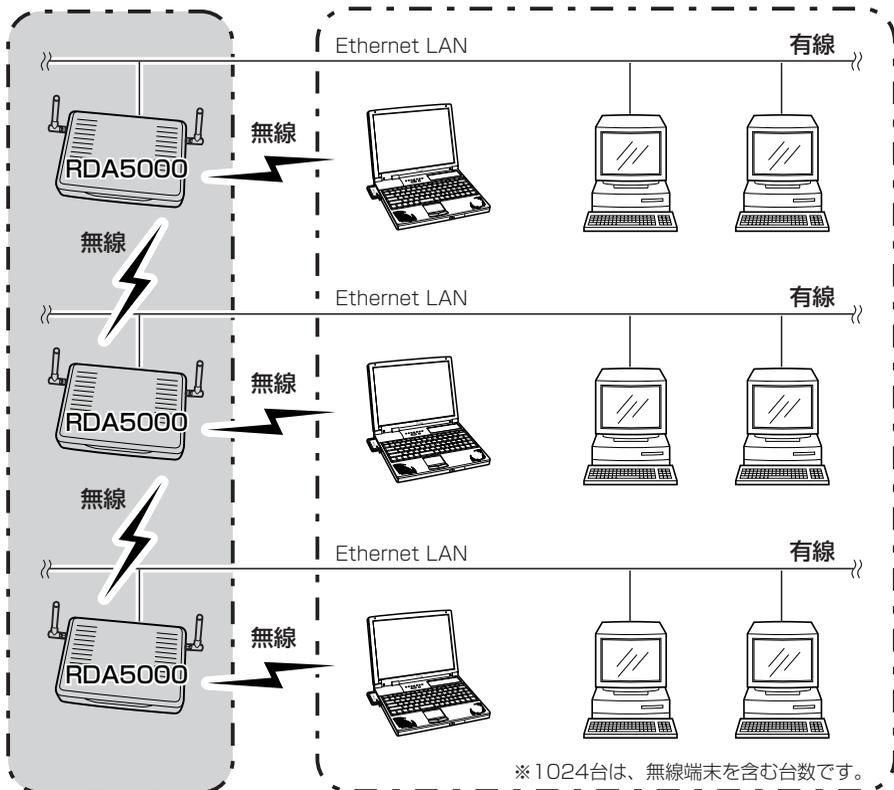
ユーザー認証に使用するサーバには、RADIUSを使用します。

【MACアドレス登録】：本製品との無線通信を許可する機器のMACアドレスを本製品に登録することで、通信相手を限定できます。

1 ご使用になる前に

1-5. 収容台数について

無線ネットワーク内に収容できる本製品とパソコンの理論的な台数を図に示します。
※カッコ内の数値は、複数の機器が煩雑に通信するような環境での推奨台数です。



7台まで収容可能
(推奨台数：3台)

[1024台]－[本製品の使用台数]まで収容可能
(本製品1台につき、無線端末：10台を推奨)

※1024台は、無線端末を含む台数です。

■ 負荷分散機能について

本製品に同時接続できる無線パソコンの台数を制限して、接続が集中するとき起こる通信速度の低下を防止する機能です。

IEEE802.11g規格とIEEE802.11a規格について、別々に設定できます。

出荷時、それぞれ、最大255台(出荷時の設定)に設定されています。

1-6. 本製品の設置について

本製品の設置に関する内容について説明します。

■ 設置場所について

無線LANでご使用になる場合、設置場所に注意してください。

設置条件は、次のとおりです。

設置条件によっては、通信範囲や速度に影響します。

◎室内で、なるべく見通しの良い(高い)場所

◎振動や傾きが無く、落下の危険がない安定した場所

◎その他、以下のことを考慮して設置してください。

- 本製品の上に物を置いたり、本製品どうしやほかの製品と重ねて置かないでください。
- 電波は壁やガラスを通過しますが、金属は通過しません。コンクリートの壁でも、金属補強材が埋め込まれていて、電波信号を遮断するものがあります。
- 通信範囲はオープンスペースだと最も広くなりますが、倉庫の中のように大きな金属製の壁があると、電波を反射することがあります。
- 床にはふつう、鋼製の梁がはいっており、金属製防火材が埋め込まれていることがあります。そのため多くの場合、違う階どうしでは通信できません。

■ 無線通信距離について

無線通信距離は、設置場所や通信周波数によって異なりますので、以下の見通し距離を目安にご使用ください。

- 無線AP(アクセスポイント)間通信 → **802.11a(5.2GHz)、54Mbps通信時**
 屋内：約30m以内
802.11g(2.4GHz)、54Mbps通信時
 屋内：約30m以内、屋外：約30m以内
- 無線AP(アクセスポイント)通信 → **802.11a(5.2GHz)、54Mbps通信時**
 屋内：約30m以内
802.11g(2.4GHz)、54Mbps通信時
 屋内：約30m以内、屋外：約30m以内
802.11b(2.4GHz)、11Mbps通信時
 屋内：約30m以内、屋外：約70m以内

■ 分離式デュアル平面アンテナ(別売品)

分離式デュアル平面アンテナを2個1組でご使用いただくことで、ダイバーシティー方式で通信でき、設置環境に影響されない場所に設置できます。

また、無線通信距離についても付属アンテナの約1.5倍まで延長できます。

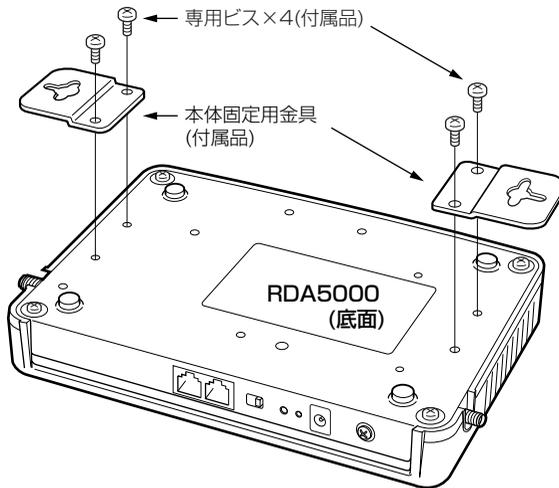
1 ご使用になる前に

1-6. 本製品の設置について(つづき)

■ 設置方法について

本製品を壁面や棚などに固定するときは、次の図を参考に付属の固定用金具を取り付けてからご使用ください。

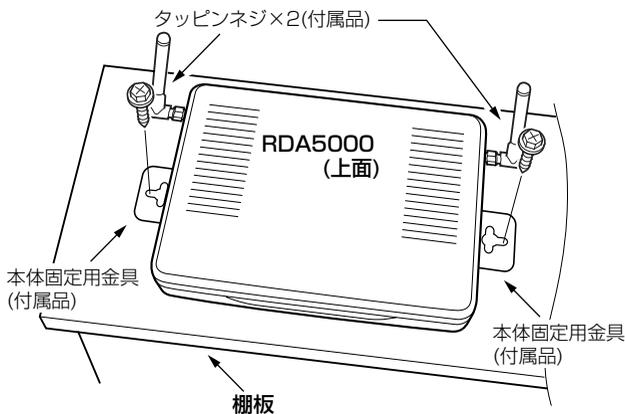
1. 金具を本製品に固定する



2. 本製品を固定する

〈棚の上に固定する場合〉

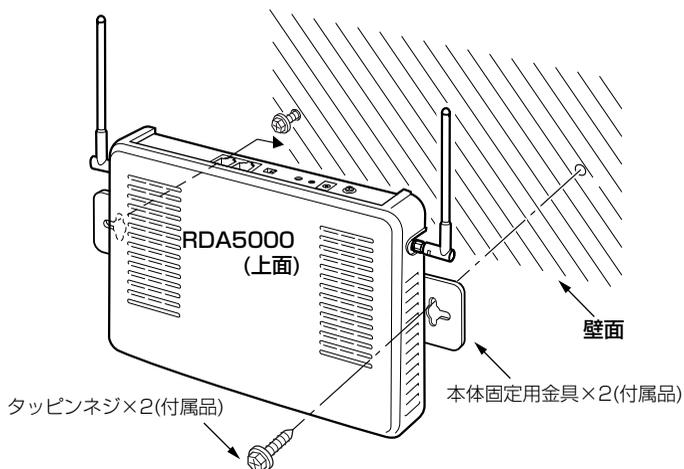
棚の上に置いた場合、本製品に接続されたACコードや接続ケーブルが、人体に触れるおそれがあるときは、落下防止のため、次の図のように、本体を付属の固定用金具で固定してください。



■ 設置方法について

2. 本製品を固定する(つづき)

〈壁面に、横向きにして固定する場合〉



1 ご使用になる前に

1-7. 設定画面の名称と機能

本製品の設定画面の名称と各画面に含まれる項目を説明します。



■ 設定画面について

設定画面表示エリア

設定画面選択メニューで選択されたタイトルの画面表示に切り替わります。

ホームページのリンク

本製品がインターネットできる状態で、**ROOT INC.** アイコン上にマウスカーソルを移動してクリックすると、ルートのホームページにアクセスできます。

<登録>/<取消>/<登録して再起動> ボタン表示しているメニュー画面に設定した内容の登録や取消をします。

本製品を再起動することで変更内容が有効になる項目については、**<登録して再起動>** をクリックします。

■ 設定画面選択メニュー

設定画面は、用途別に次の各メニューに分類されています。

各メニューのタイトル上にマウスカーソルを合わせてクリックして、表示された画面タイトルをクリックすると、その画面を「設定画面表示エリア」に表示します。

■ 「ネットワーク設定」メニュー

「LAN側IP設定」画面

- 本体名称/IPアドレス設定
- DHCPサーバ設定
- 静的DHCPサーバ設定

「ブリッジ設定」画面

- ブリッジ設定
- ※スパンニングツリー機能など

「RIP設定」画面

- RIP設定
- RIPフィルタ設定

「ルーティング設定」画面

- IP経路情報
- スタティックルーティング設定

■ 「無線LAN設定」メニュー

「セキュリティ設定」画面は、「IEEE802.11a/IEEE802.11g」共用です。

残りの画面は、下記のように分かれています。

◎[IEEE802.11a]の項目は、5.2GHz帯無線LANを設定します。

◎[IEEE802.11g]の項目は、2.4GHz帯無線LANを設定します。

※[IEEE802.11b]規格についての設定は、[IEEE802.11g]規格と互換性があるため [IEEE802.11g]の項目と共用しています。

「セキュリティ設定」画面(IEEE802.11a/g)

- RADIUS設定
- 無線端末間通信設定
- MACアドレスセキュリティ設定

「無線LAN設定」画面(IEEE802.11g)

- 無線LAN設定
- ※SSID、チャンネル、11g保護機能、パワーレベル、接続端末制限など

「暗号化設定」画面(IEEE802.11g)

- 暗号化設定
- キー値

「AP間通信設定」画面(IEEE802.11g)

- IEEE802.11g BSSID
- 通信AP設定
- ※無線AP間通信機能を使用するための相手側BSSIDの登録など

「無線LAN設定」画面(IEEE802.11a)

- 無線LAN設定
- ※SSID、チャンネル、パワーレベル、接続端末制限など

「暗号化設定」画面(IEEE802.11a)

- 暗号化設定
- キー値

「AP間通信設定」画面(IEEE802.11a)

- IEEE802.11a BSSID
- 通信AP設定
- ※無線AP間通信機能を使用するための相手側BSSIDの登録など

1 ご使用になる前に

1-7. 設定画面の名称と機能

■ 設定画面選択メニュー(つづき)

■ 「WAN側設定」メニュー

「WAN側設定」画面

- 接続状況
- 回線種別
 - ※[回線種別]を選択して〈登録〉ボタンをクリックすると、次の項目を表示します。
 - 回線設定
 - 接続設定(DHCP設定時を除く)

「WAN側詳細設定」画面

- PPPoE詳細設定(PPPoE設定時)
- 共通詳細設定

■ 「システム設定」メニュー

「本体管理設定」画面

- 管理者ID設定
- 設定初期化
- 「Firm Utility使用」モード

「時計設定」画面

- 内部時計設定
- 自動時計設定

■ 「情報表示」メニュー

「通信記録」画面

- 通信記録
 - ※WAN側の通信記録を表示します。

「アドレス変換設定」画面

- アドレス変換設定
 - ※DMZホスト機能など
- パススルー設定
- 静的マスカレードテーブル設定
- 静的NATテーブル設定

「IPフィルタ設定」画面

- 不正アクセス検知機能設定
- IPフィルタ設定

「SYSLOG設定」画面

- SYSLOG設定

「SNMP」画面

- SNMP設定

「設定保存」画面

本製品の設定内容の確認や設定内容の保存に使用します。

「ネットワーク情報」画面

- ネットワーク インターフェイス リスト
- ブリッジポート情報
- 本体MACアドレス

この章では、

パソコンを本製品の[LAN]ポートに接続してご使用になる場合、パソコンの接続と設定について説明します。

2-1.Ethernetカードの装着	16
■ デスクトップ型パソコンの場合	16
■ ノートブック型パソコンの場合	16
2-2.[LAN]ポートへのパソコン接続	17
■ 1台のパソコンを接続する場合	17
■ 2台以上のパソコンを接続する場合	17
2-3.アース線と電源を接続する	18
2-4.パソコンの電源を入れる	18
2-5.IPアドレスを確認する	19
■ Windows XPの場合	19
■ Windows 98/98 SE/Meの場合	20
■ Windows 2000の場合	21
■ IPアドレスの取得に失敗したときは？	21
2-6.設定画面へのアクセスを確認する	22
■ 「LAN側IP設定」画面(※最初に表示される画面です。)	22

【HUBへの接続について】

本製品は54Mbpsの高速無線ユニットを内蔵しているため、接続する有線LANについても高速通信が行えるよう設計されています。

本製品に低速なHUBを接続した場合、意図しない動作で通信に障害を与えることがありますので、必ず100BASE-TX対応のスイッチングHUBをご使用ください。

2 有線LANで使う

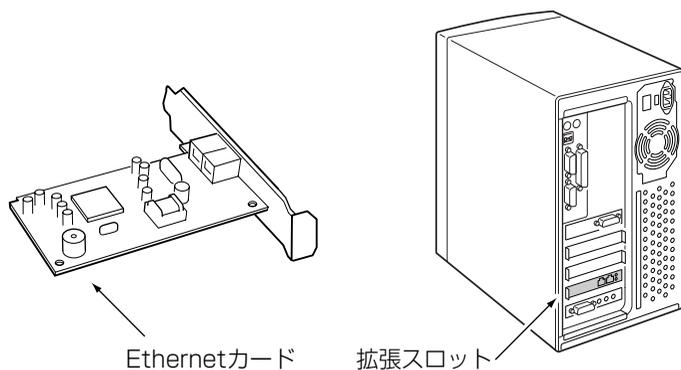
2-1. Ethernetカードの装着

本製品を有線LANでご使用になる場合は、Ethernetケーブルが接続できるパソコンをご用意ください。

すでに有線LANでご使用のパソコンから設定される場合は、既存の有線LANからそのパソコンを外してください。

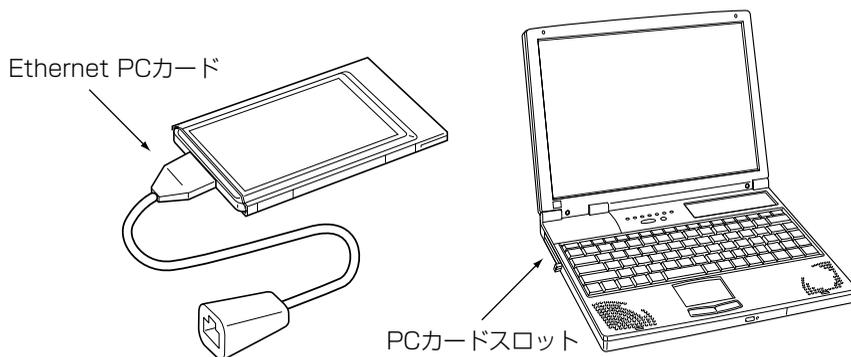
■ デスクトップ型パソコンの場合

[Ethernet]ケーブルを直接接続できない場合は、拡張スロットにEthernetカードの取り付けが必要です。



■ ノートブック型パソコンの場合

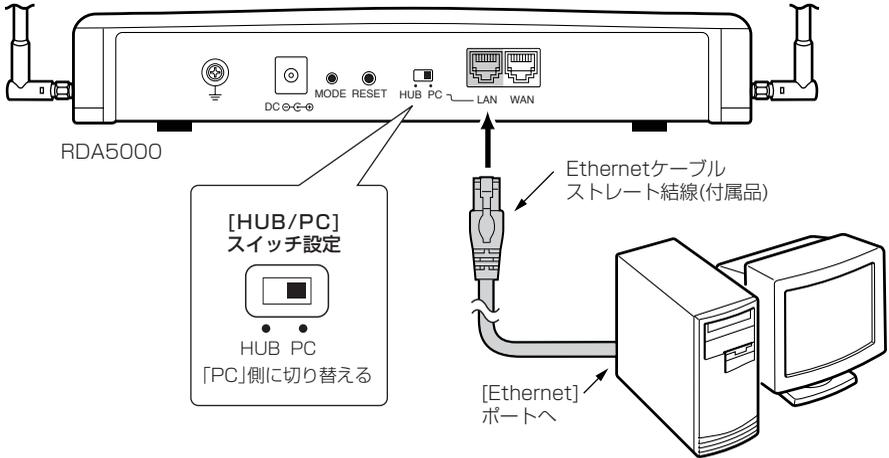
[Ethernet]ケーブルを直接接続できない場合は、PCカードスロットにEthernetカードの取り付けが必要です。



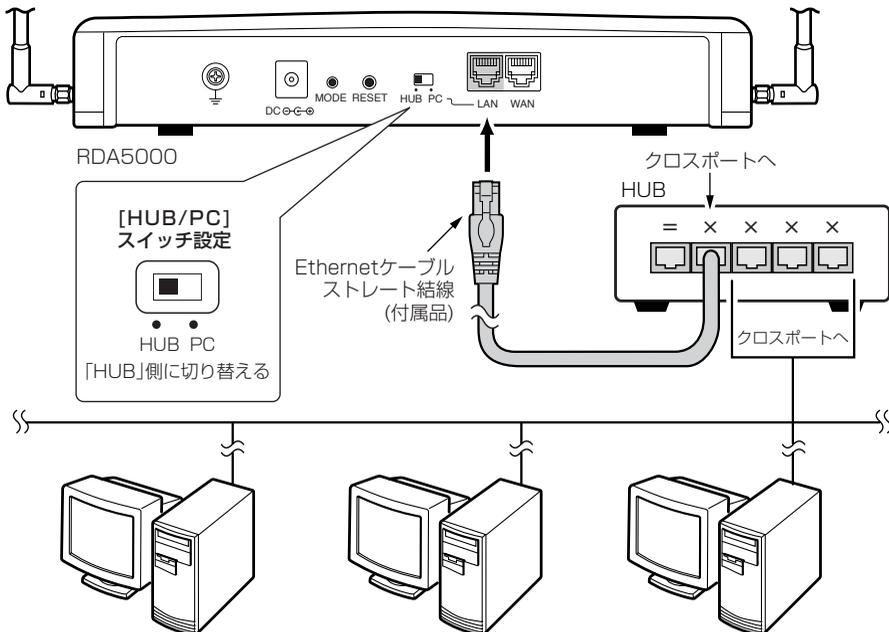
2-2. [LAN]ポートへのパソコン接続

△注意 接続するときは、本製品および接続する機器の電源を切った状態で行ってください。

■ 1台のパソコンを接続する場合

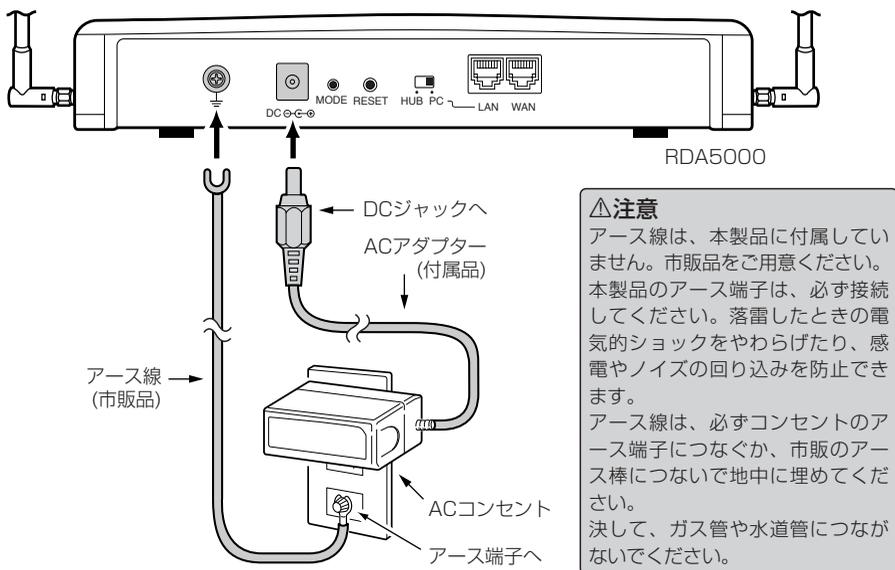


■ 2台以上のパソコンを接続する場合

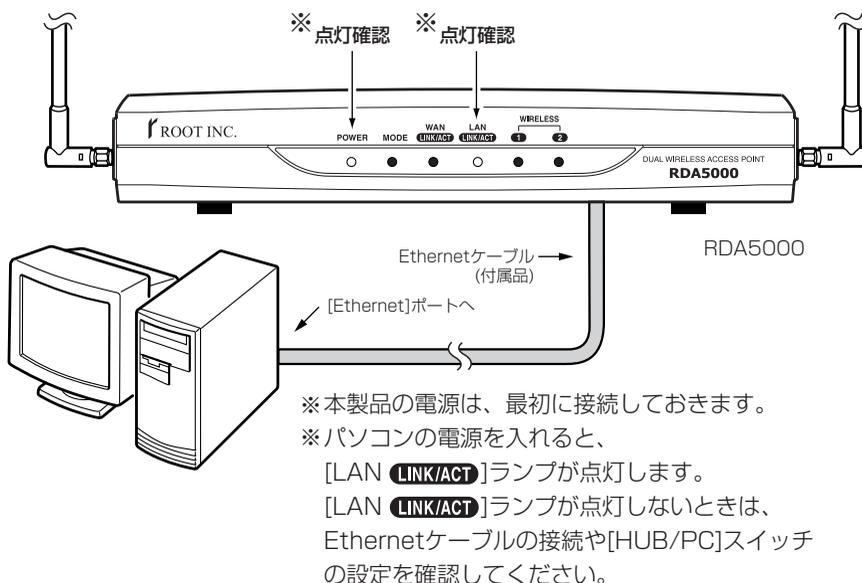


2 有線LANで使う

2-3. アース線と電源を接続する



2-4. パソコンの電源を入れる



2-5. IPアドレスを確認する

正しく接続されると、パソコンのIPアドレスを本製品から自動で割り当てます。

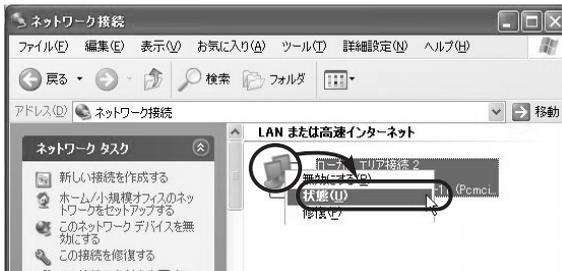
ここでは、パソコンに割り当てられたIPアドレスを確認する方法について説明します。

※本製品に接続するすべてのパソコンは、IPアドレスを「自動取得」できるように設定されている必要があります。

■ Windows XPの場合

〈確認のしかた〉

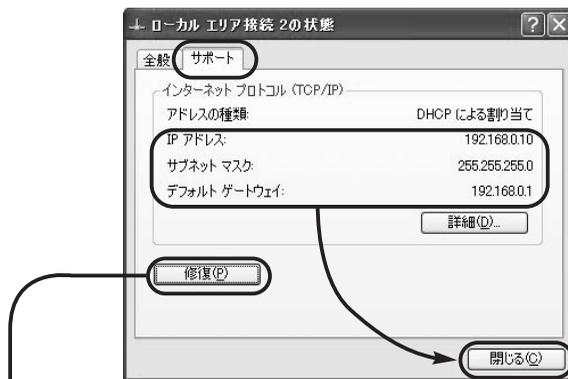
- 1.マウスを〈スタート〉→[コントロールパネル(C)]の順に操作します。
- 2.コントロールパネルから、[ネットワークとインターネット接続]をクリックします。
- 3.[ネットワーク接続]アイコンをクリックします。
- 4.ご使用のEthernetカード名が表示された[ローカルエリア接続]アイコンを右クリックすると表示されるメニューから、[状態(U)]をクリックします。



2

- 5.[サポート]タブをクリックします。

- 本製品から取得したパソコンのIPアドレスを表示します。



〈ご参考に〉

上記画面の〈修復(R)〉をクリックすると、本製品からパソコンのIPアドレスを再取得します。

2 有線LANで使う

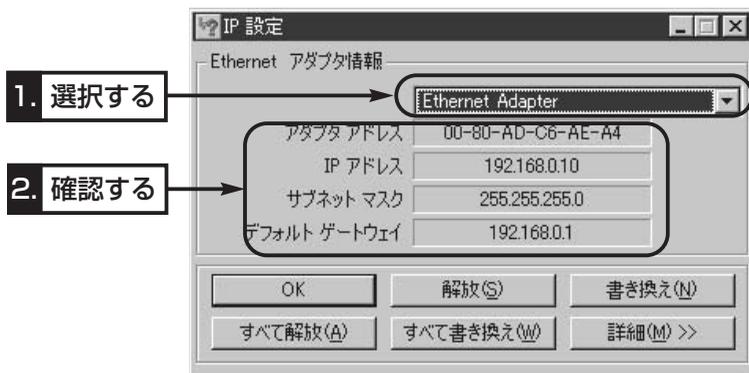
2-5. IPアドレスを確認する(つづき)

■ Windows 98/98 SE/Meの場合

インストールされたOSの[Windows]フォルダーに収められた「winipcfg.exe」というアプリケーションで確認します。

〈確認のしかた〉

- 1.マウスを〈スタート〉→[ファイル名を指定して実行(B)]の順番に操作します。
- 2.コマンドラインボックスに「winipcfg」と半角入力して、[ENTER]キーを押します。
- 3.テキストボックスの[▼]をクリックして、ご使用のEthernetカード名を選択します。
 - 本製品から取得したパソコンのIPアドレスを表示します。



〈画面の表示項目について〉

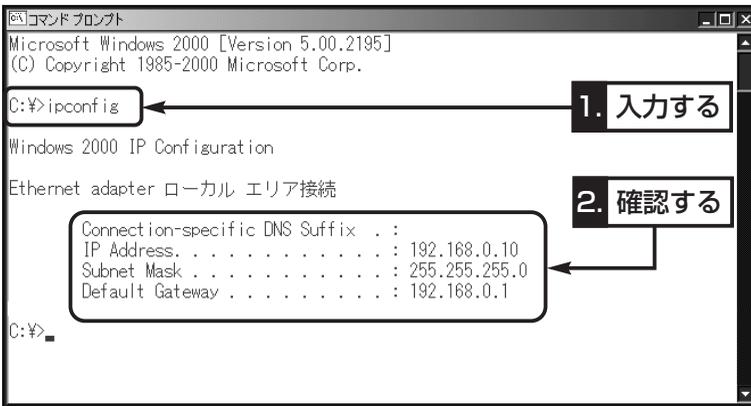
- ◎アダプタアドレス : Ethernet LANカードのMACアドレス
- ◎IPアドレス : パソコンのIPアドレス
- ◎サブネットマスク : パソコンのサブネットマスク
- ◎デフォルトゲートウェイ : 本製品のLAN側のIPアドレス

■ Windows 2000の場合

コマンドプロンプト画面から「ipconfig」を実行します。

〈確認のしかた〉

- 1.マウスを〈スタート〉→[プログラム(P)]→[アクセサリ]→[コマンドプロンプト]の順番に操作します。
- 2.ipconfigとコマンドを入力して、[Enter]キーを押します。
※コマンドラインのオプションについては、「ipconfig /?」を実行してご確認ください。
- 3.パソコンに割り当てられたIPアドレスを次の画面で確認します。
 - 本製品から取得したパソコンのIPアドレスを表示します。



2

〈ご参考に〉

下記のコマンドを上記画面で実行すると、本製品からパソコンのIPアドレスを解放したり取得したりできます。

- ◎ipconfig /release : すべてのアダプタについて、IPアドレスを解放します。
- ◎ipconfig /renew : すべてのアダプタについて、IPアドレスを取得します。

■ IPアドレスの取得に失敗したときは？

出荷時、1台目のパソコンに割り当てられるIPアドレスは、「192.168.0.10」です。それ以降、接続するパソコンには、「192.168.0.11～」と順番に割り当てられます。本製品からのIPアドレス取得に失敗したときは、表示されたIPアドレスのネットワーク部が「192.168.0」と異なる場合や「192.168.0.1」(出荷時の設定)がデフォルトゲートウェイとして表示されていない場合は、IPアドレスの自動割り当てに失敗している可能性があります。

このようなときは、ご使用のEthernetカードのIPアドレスについての設定およびケーブルの接続を確認してから、パソコンを再起動してみてください。

再起動したら、もう一度、上記の手順でIPアドレスを確認してください。

2 有線LANで使う

2-6. 設定画面へのアクセスを確認する

有線LANで接続したパソコンのWWWブラウザから本製品を設定する画面にアクセスする手順について説明します。

※パソコンのWWWブラウザは、Microsoft Internet Explorer5.0以降、または Netscape Navigator6.0以降をご用意ください。

〈設定画面の呼び出しかた〉

- 1.WWWブラウザを起動します。
※本書では、Internet Explorer6.0を使って説明しています。
- 2.本製品に設定されたIPアドレスをWWWブラウザのアドレスバーに指定します。
「http://192.168.0.1/」(出荷時の場合)と入力して、[Enter]キーを押します。
 - 「ネットワーク設定」メニューの「LAN側IP設定」画面を最初に表示します。※下記に示す画面は、本製品の出荷時、または全設定を初期化したときの状態です。

■「LAN側IP設定」画面(※最初に表示される画面です。)



この章では、

パソコンを本製品にワイヤレス接続してご使用になる場合、パソコンの接続と設定について説明します。

3-1.無線LANで通信するパソコンについて	24
3-2.無線LANの構築について	24
■ 無線ネットワーク名	24
■ 無線セキュリティ	25
■ アクセスポイント機能について	25
■ ローミング機能について	26
■ リピータ機能について	27
■ 無線LAN構築時のご注意	28
3-3.無線アクセスポイント機能を使用してみる	29
3-4.無線AP(アクセスポイント)間通信機能を使用してみる	32
3-5.無線ネットワーク名(SSID)を設定する	36
3-6.暗号化を設定する	37
■ 16進数で暗号化鍵(キー)を入力するには	37
■ ASCII文字→16進数変換表	38
■ ASCII文字で暗号化鍵(キー)を入力するには	39
■ 暗号化鍵(キー)値の入力について	40
■ キーIDの設定について	40
■ 鍵(キー)値の設定例	41
■ キージェネレータで暗号化鍵(キー)を生成するには	42
3-7.MACアドレスセキュリティを設定する	43
3-8.802.11b規格の通信を制限するには	44
3-9.スパニングツリー機能を使用してみる	45

3 無線LANで使う

3-1. 無線LANで通信するパソコンについて

本製品と無線LANで通信する場合は、無線LAN機能搭載のパソコンをご用意ください。本製品は、3つ(IEEE802.11a/b/g)の無線LAN規格に対応しています。推奨無線LANカードにつきましては、弊社営業部までお問い合わせください。

3-2. 無線LANの構築について

複数の無線パソコンで本製品をご使用になるとき、知っておいていただきたい本製品の機能やセキュリティなどの設定について説明します。

※本製品は、Macintoshへの無線接続には対応していませんのでご注意ください。

■無線ネットワーク名

本製品と無線LANカードには、通信するお互いを識別するための無線ネットワーク名として、SSIDが設定されています。

SSID

出荷時は、LG 〈半角〉
に設定されています。

無線ルータや無線アクセスポイントが無線伝送エリア内に数台存在しているような場合、個々の無線ネットワークグループを異なる[SSID(無線ネットワーク名)]で識別させることで、異なる無線ネットワークグループからの混信を防止します。

同じグループで通信するお互いの無線LAN機器で、この[SSID]が異なると通信できません。

※無線パソコン側で「ANY」モード(アクセスポイント自動検索機能)が設定されていると、[SSID]の設定に関係なく、無線パソコンからの通信が可能になります。この無線パソコンとの通信を拒否する場合は、「無線ネットワーク名(SSID)を設定する」(☞3-5章)の画面を参考に、[ANYを拒否]を「する」に変更してください。

【ご参考に】

ご使用になる無線LAN機器によっては、無線ネットワーク名が「ESS ID」と記載されていますが、「SSID」と同じ意味として使用されています。

3-2. 無線LANの構築について(つづき)

■ 無線セキュリティ

本製品は、無線LAN通信に必要なセキュリティとして、次の機能を搭載しています。これらの項目や設定について詳しくは、取扱説明書[活用編]をご覧ください。

MACアドレス登録 ……

出荷時は、登録されていません。

同一無線ネットワークグループ内の通信において、あらかじめ本製品に登録されたMACアドレスを持つ無線パソコンだけにアクセスを許可するとき使用します。

WEP(RC4)/OCB AES

出荷時は、設定されていません。

無線ネットワーク間で送受信するデータを、設定された文字列を元に暗号化して安全性を確保します。通信相手と暗号化方式や鍵(キー)の設定が異なるときは、通信できません。

※WEP(RC4)とOCB AESは、互換性がありません。

IEEE 802.1x ……

出荷時は、設定されていません。

RADIUSサーバを使用して、無線LANからのアクセスにユーザー認証を設ける機能です。

パソコンは、Windows XP搭載で、「IEEE 802.1x」対応の無線LANカードをご用意ください。(推奨無線LANカードにつきましては、弊社営業部までお問い合わせください。)

■ アクセスポイント機能について

本製品は、IEEE802.11a/b/gの無線アクセスポイントとして機能します。

無線アクセスポイントを使うことで、本製品を介して無線パソコンとデータをやりとることができます。また、本製品と有線LANを接続することで、無線LANと有線LANのデータをやりとりしたり、無線パソコンからモデムと接続された本製品を中継してインターネットに接続できます。

※本製品に多くの無線パソコン、またはIEEE802.11b規格とIEEE802.11g規格の無線パソコンが同時にアクセスすると、通信速度が著しく低下することがあります。

同じ無線LAN規格*で同時に使える無線パソコンの台数は、最大255台までですが、10台以下とすることをお勧めします。

IEEE802.11b規格とIEEE802.11g規格の無線パソコンが混在する環境では、[11g保護機能](※3-8章)と併せてご使用ください。

★IEEE802.11b規格の無線パソコンは、本製品のIEEE802.11g規格に含まれるものとします。



3 無線LANで使う

3-2. 無線LANの構築について(つづき)

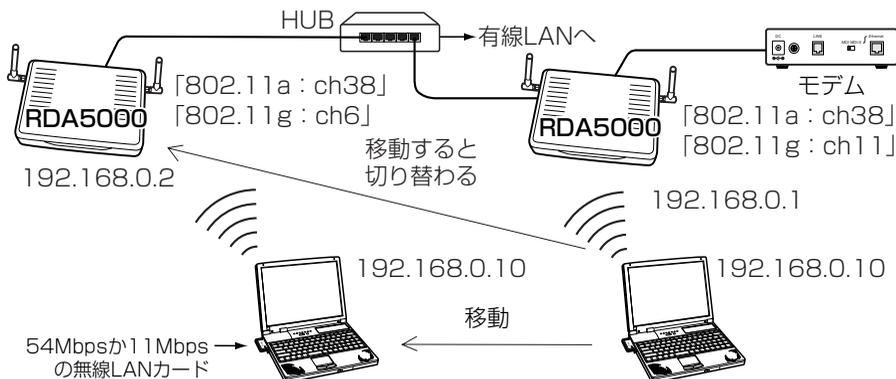
■ ローミング機能について

本製品を2台以上用意して、それぞれを有線LANと接続することにより、無線パソコンを移動させても、自動的に電波の状況のよいアクセスポイント(本製品)に切り替えることによって、無線伝送エリアが広がり、工場や倉庫のように広い場所で移動しながら無線LANを利用できるようになります。

※ローミング機能を使用する場合、すべての本製品と無線パソコンは、無線ネットワーク名(SSID)や暗号化の設定をすべて同じにしてください。(※設定が異なると通信できません。)

※2.4GHz帯(IEEE802.11b/g)で通信するときは、電波干渉を避けるため、本製品の「チャンネル」は、相手側と4チャンネル以上空けて設定してください。(※P28)

5.2GHz(IEEE802.11a)で通信する場合、互いを異なるチャンネルに設定すれば、チャンネル間の電波干渉に配慮する必要はありません。

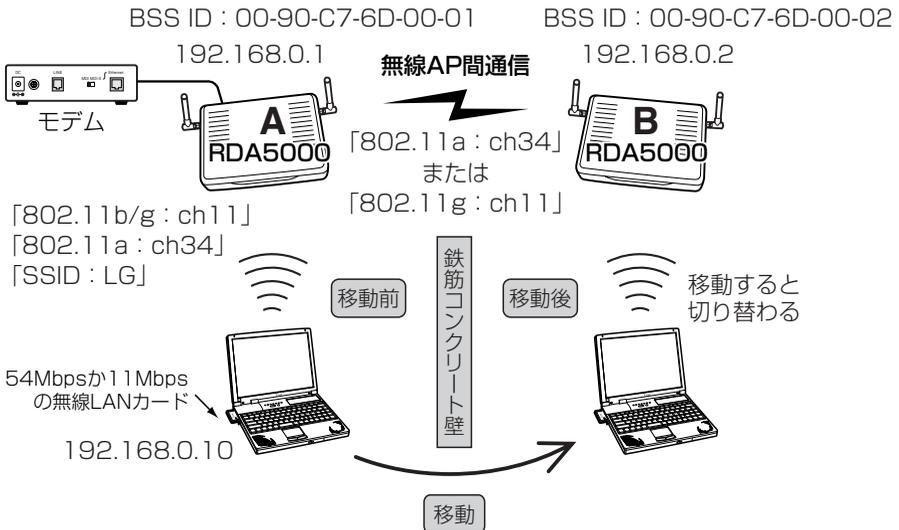


3-2. 無線LANの構築について(つづき)

■ リピータ機能について

リピータとは、無線AP(アクセスポイント)間通信する相手側の機器を無線中継器として使用する機能です。

2台以上の本製品を用意して、それぞれの機器に相手の[BSSID]を登録して使用します。無線パソコンの移動や障害物などの影響で本製品(図：A)と通信できなくなっても、この機能を利用することで自動的に電波の状況のよい無線アクセスポイント(図：B)を中継して通信を継続できるようになります。



※同時に無線AP間通信できる台数は、最大7台(自分の機器を含む)までです。

※無線AP間通信する本製品は、すべて同じ「チャンネル」に設定してください。

※無線AP間通信機能は、あらかじめ通信相手の[BSSID]を本製品に登録してください。登録していないほかの本製品とは通信できません。

802.11a規格と802.11g規格について、別々に登録できます。

※リピータ機能で使用する場合は、本製品(図：AとB)の[SSID]を同じに設定してください。

※上記の図に加えて、次のような接続をした場合は、経路のループ形成(冗長リンク)を回避するためスパンニングツリー機能(※3-9章)を設定する必要があります。

- 同一ネットワーク上に無線AP間通信する本製品が3台以上ある場合
- 無線AP間通信で稼働している本製品(図：A-B間)どうしをEthernetケーブルで接続した場合
- 本製品(図：A-B間)どうしを、802.11a規格と802.11g規格の無線ブリッジで接続した場合

3 無線LANで使う

3-2. 無線LANの構築について(つづき)

■無線LAN構築時のご注意

◎DHCPサーバ機能が設定された本製品などが同一ネットワーク内に複数存在すると、IPアドレスが重複して不測の事態になりますので、接続に注意してください。

※出荷時、本製品のDHCPサーバ機能は有効に設定されています。

◎ローミング機能を使用する場合、すべての本製品と無線パソコンは、無線ネットワーク名(SSID)や暗号化の設定をすべて同じにしてください。(※設定が異なると通信できません。)

◎本製品どうしを無線AP間通信だけに使用する場合は、それぞれの機器に異なる無線ネットワーク名(SSID)を設定できますが、リピータ機能でも使用する場合は、リピータとなる相手側の本製品と同じ[SSID]を設定してください。

相手側の本製品と[SSID]が異なると、リピータとして使用できません。

◎本製品は、IEEE802.11規格(14チャンネル)の無線通信には対応していません。

◎無線AP(アクセスポイント)間通信機能を使用する場合、相手側と「チャンネル」を同じに設定してください。(※チャンネルが異なると無線AP間通信できません。)

◎近くで別の無線ネットワークグループが2.4GHz帯(IEEE802.11b/g)で通信するときは、電波干渉を避けるため、本製品の「チャンネル」は、別の無線ネットワークグループのチャンネルから4チャンネル以上空けて設定してください。

それ以下のときは、図に示すように帯域の1部が重複するため混信する可能性があります。

例えば、お互いの設定が、1-6-11チャンネルに設定すると混信しません。

※5.2GHz帯(IEEE802.11a)で通信する場合、互いを異なるチャンネルに設定すれば、チャンネル間の電波干渉に配慮する必要はありません。



3-3. 無線アクセスポイント機能を使用してみる

無線LANカードを装着したパソコンを例に、本製品の無線アクセスポイント機能を使用できるようにするまでの手順を説明します。

※本製品の無線アクセスポイントに関する設定は、出荷時の状態とします。

※本製品は、Macintoshへの無線接続には対応していませんのでご注意ください。

Step1. 無線LANと通信できるパソコンを準備する

次の手順で無線LANカードのドライバーとユーティリティを準備します。

- 1.無線LANカード(54Mbpsまたは11Mbps対応)を用意します。
※Ethernetケーブルをパソコンに接続している場合は、取り外してください。
- 2.ドライバーを無線LANカードに付属の取扱説明書を参考にインストールします。
※インストール後、無線LANカードをパソコンに装着します。
パソコンの設定を変更しない状態では、IPアドレスをDHCPサーバから自動取得できる状態になっていますので、この状態で通信を確認します。
※確認のため、本製品のDHCPサーバ機能は、「有効(出荷時の設定)」で使います。
- 3.無線LANカードの設定ユーティリティをインストールします。
※無線LANカードの設定や通信状況およびIPアドレスの確認に使用します。
※ご使用になる無線LANカードにより、設定方法が異なる場合があります。

Step2. 無線LANカードの設定を確認する

無線LANカードに付属のユーティリティを使用して、以下の設定項目を確認します。

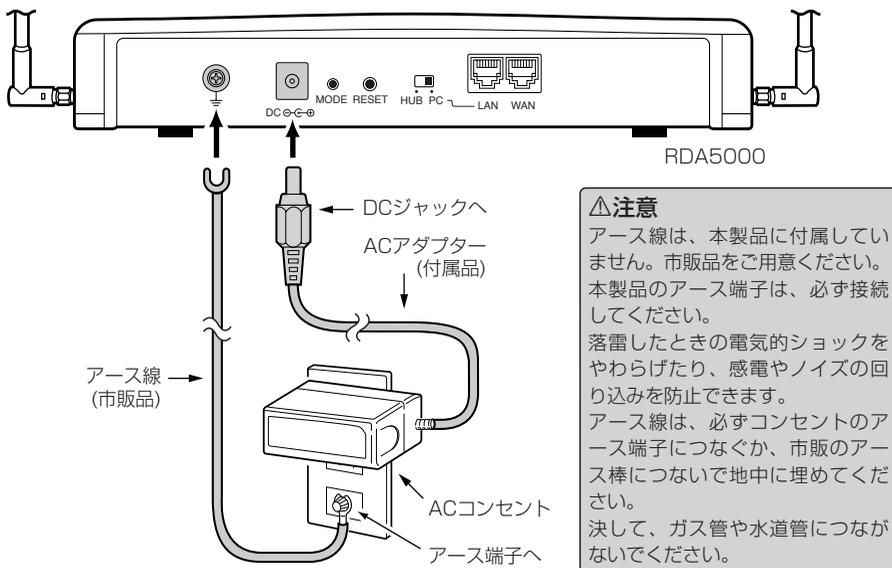
- ネットワーク設定：インフラストラクチャ
本製品と通信するときは、「インフラストラクチャ」モードを選択します。
- SSID：LG (半角大文字)
本製品の設定(出荷時：半角大文字で、「LG」と同じにします。

3 無線LANで使う

3-3. 無線アクセスポイント機能を使用してみる(つづき)

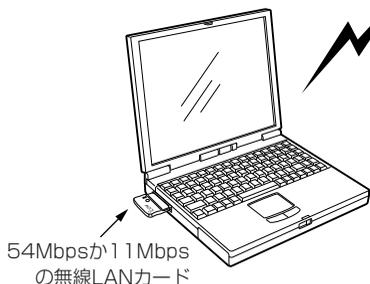
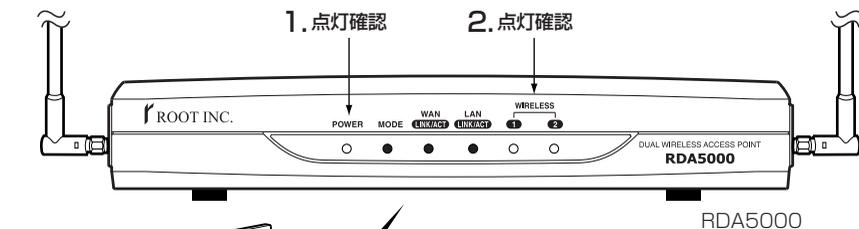
Step3. 通信を確認する

1. 下記の図を参考に、アース線とACアダプターを接続します。



2. 無線LANで通信できるパソコンの電源を入れます。

※[WIRELESS]ランプが消灯している場合、IPアドレスの自動割り当てに失敗していることがありますので、パソコンを再起動後にランプの点灯を確認してください。



1. 本製品の電源は、最初に接続しておきます。
 - [POWER]ランプが点灯します。
2. パソコンの電源を入れます。
 - 802.11b/g規格で無線通信を確立したときは、[WIRELESS ①]が点灯します。
 - 802.11a規格で無線通信を確立したときは、[WIRELESS ②]が点灯します。

3-3. 無線アクセスポイント機能を使用してみる(つづき)

Step5. 設定画面へのアクセスを確認する

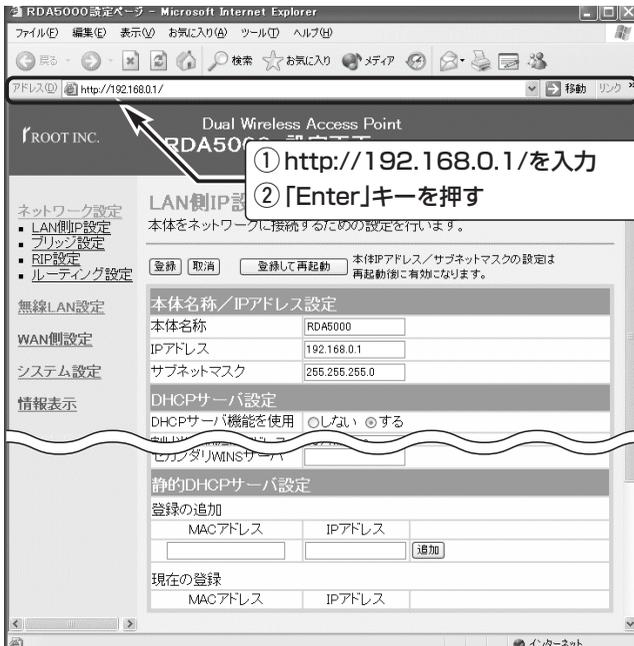
本製品と無線通信しているパソコンにインストールされたWWWブラウザから本製品を設定する画面にアクセスする手順について説明します。

※パソコンのWWWブラウザは、Microsoft Internet Explorer5.0以降、または Netscape Navigator6.0以降をご用意ください。

〈設定画面の呼び出しかた〉

- 1.WWWブラウザを起動します。
※本書では、Internet Explorer6.0を使って説明しています。
- 2.本製品に設定されたIPアドレスをWWWブラウザのアドレスバーに指定します。
「http://192.168.0.1/」(出荷時の場合)と入力して、[Enter]キーを押します。
※下記に示す画面は、本製品の出荷時、または全設定を初期化したときの状態です。

■ 「LAN側IP設定」画面(※最初に表示される画面です。)



3 無線LANで使う

3-4. 無線AP(アクセスポイント)間通信機能を使用してみる

無線AP間通信機能を使用することで、最大54Mbpsの通信速度で本製品どうしを無線ブリッジ接続できます。(※1-4章)

無線ブリッジで接続された本製品は、リピータ(※P27)として使用できます。

下記の図を例に、通信できるようにするまでに最低限必要な項目の設定と無線AP間通信の確認方法について説明します。

また、本製品をそれぞれ、[A]と[B]として説明します。

※無線AP間通信は、通信相手の[BSSID]を登録するまで機能しません。

[BSSID]の登録は、802.11a規格と802.11g規格で別々に行えます。

ここでは、802.11a規格で無線AP間通信する例を説明しています。

DHCPサーバ機能：「ON」(出荷時の設定)

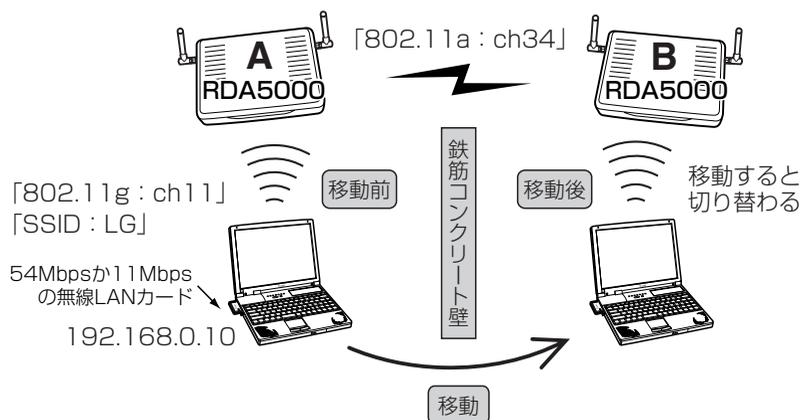
192.168.0.1

BSSID：00-90-C7-6D-00-01

DHCPサーバ機能：「OFF」

192.168.0.2

BSSID：00-90-C7-6D-00-02



Step 1. 無線LANと通信できるパソコンを準備する

IEEE802.11g規格で通信できるパソコンを使用することを例に説明します。

※本製品は、Macintoshへの無線接続には対応していませんのでご注意ください。

1. 本製品にIEEE802.11g規格の無線LANで通信できるパソコン(1台)を用意します。
2. 本製品(2台)を用意します。
3. パソコンが本製品[A]と本製品[B]のそれぞれと無線で通信できることを、「無線アクセスポイント機能を使用してみる」(※3-3章)の手順を参考に確認します。

- 通信できる状態になると、本製品の[WIRELESS 1]ランプが点灯します。

※本製品[A]と本製品[B]が設定などで手元にある場合は、どちらか一方だけ電源を入れて、交互に確認するようにしてください。

3-4. 無線AP(アクセスポイント)間通信機能を使用してみる(つづき)

Step2. 本製品[A]と[B]の[BSSID]を確認する

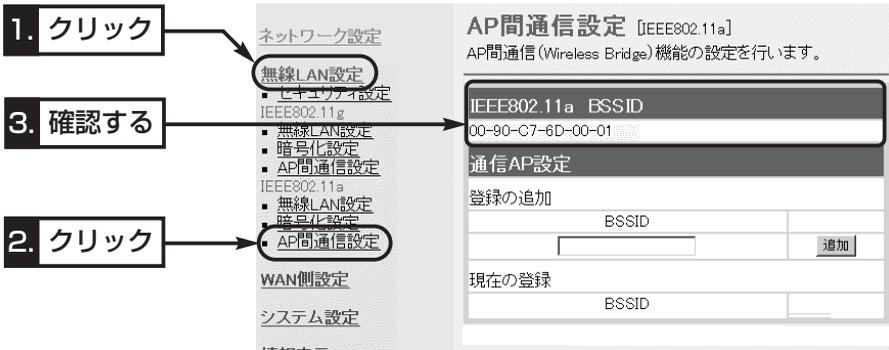
本製品どうしを無線で通信させるには、本製品に内蔵された無線LANカードの[BSSID]を互いの機器間で登録し合う必要があります。

本製品の[BSSID]は、次の手順で確認します。(例：IEEE802.11a側)

※[BSSID]は、IEEE802.11a規格とIEEE802.11g規格で異なります。

また、本製品のMACアドレスとも異なりますので、確認のときはご注意ください。

1. 本製品の設定画面にアクセス(※3-3章Step5.)して、「無線LAN設定」メニューの [IEEE802.11a] から「AP間通信設定」をクリックします。
 - 「AP間通信設定」画面を表示します。
2. [IEEE802.11a BSSID]項目に12桁で表示されている数字が通信相手側の本製品に登録する[BSSID]です。(表示例：00-90-C7-6D-00-01)

**Step3. 本製品[A]の設定**(※画面による説明は、次ページ参照)

本製品[B]の[BSSID]を本製品[A]に設定する手順です。

1. 本製品の設定画面にアクセス(※3-3章Step5.)して、「無線LAN設定」メニューの [IEEE802.11a] から「AP間通信設定」をクリックします。
 - 「AP間通信設定」画面を表示します。
2. Step2.で確認した本製品[B]の[BSSID]を、本製品[A]の[通信AP設定]項目にある [登録の追加(BSSID)]欄に半角英数字で入力します。(入力例：00-90-C7-6D-00-02)
3. [登録の追加(MACアドレス)]欄の右にある〈追加〉をクリックします。
 - 入力した[BSSID]が[現在の登録(BSSID)]欄に表示されます。

3 無線LANで使う

3-4. 無線AP(アクセスポイント)間通信機能を使用してみる(つづき)

Step3. 本製品[A]の設定(つづき)

1. クリック → ネットワーク設定

3. 入力する → 無線LAN設定

2. クリック → 無線LAN設定

4. クリック → AP間通信設定

5. 確認する → AP間通信設定

AP間通信設定 [IEEE802.11a]

AP間通信(Wireless Bridge)機能の設定を行います。

IEEE802.11a BSSID
00-90-C7-6D-00-01

通信AP設定

登録の追加

BSSID	追加
0090c76d0002	<input type="button" value="追加"/>

現在の登録

BSSID	削除
00-90-C7-6D-00-02	<input type="button" value="削除"/>

Step4. 本製品[B]の設定

LAN側のIPアドレスとDHCPサーバ機能の変更、[BSSID]の登録手順を併せて説明します。

1. 「ネットワーク設定」メニューをクリックします。
 - 「ネットワーク設定」メニューの「LAN側IP設定」画面を表示します。
2. LAN側のIPアドレスを「192.168.0.2」に変更します。
3. DHCPサーバ機能を「使用しない」に変更します。
4. 「LAN側IP設定」画面で、〈登録して再起動〉をクリックします。
 - ※IPアドレスとDHCPサーバ機能の変更手順について詳しくは、本書5-3章～5-5章をご覧ください。
5. Step3.の手順と同様に、Step2.で確認した本製品[A]の[BSSID]を、本製品[B]の[通信AP設定]項目にある[登録の追加(BSSID)]欄に半角英数字で入力します。
(入力例：00-90-C7-6D-00-01)

1. クリック → ネットワーク設定

4. クリック → 登録して再起動

2. 入力する → IPアドレス

3. クリック → DHCPサーバ機能を使用しない

LAN側IP設定

本体をネットワークに接続するための設定を行います。

本体IPアドレス/サブネットマスクの設定は再起動後に有効になります。

本体名称/IPアドレス設定

本体名称	RDAB000
IPアドレス	192.168.0.2
サブネットマスク	255.255.255.0

DHCPサーバ設定

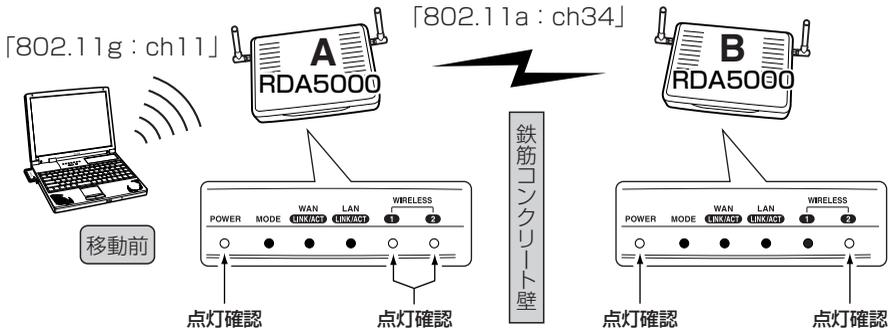
DHCPサーバ機能を使用 しない する

割り当て開始IPアドレス	192.168.0.10
--------------	--------------

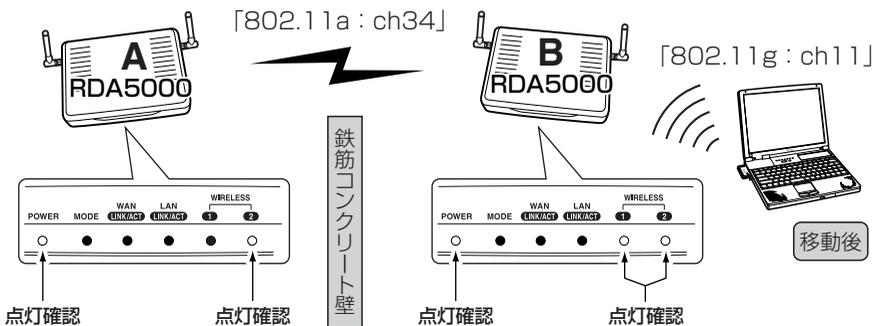
3-4. 無線AP(アクセスポイント)間通信機能を使用してみる(つづき)

Step5. 通信を確認する

1. 確認のため、パソコンの電源が入っている場合は、電源を切るか無線LANカードを取り外してください。
2. 本製品[A]と本製品[B]のアース線とACアダプターを接続して無線AP間通信を確認します。
※[WIRELESS ②]ランプが点灯しないときは、通信できていません。
本製品[A]と本製品[B]に登録した相手側の[BSSID]を確認してください。
3. パソコンの電源を入れて、本製品[A]との通信を確認します。
※本製品[A]の[WIRELESS ①]ランプが点灯しないときは、無線パソコンと通信できていません。



4. 通信中のパソコンを移動させて、本製品[B]との通信を確認します。
本製品[A]の[WIRELESS ①]ランプは、1~2分後に消灯します。
※本製品[B]の[WIRELESS ①]ランプが点灯しないときは、無線パソコンと通信できていません。
5. IPアドレスや通信状況の確認は、3-3章(Step4.)と同じように行います。



3 無線LANで使う

3-5. 無線ネットワーク名(SSID)を設定する

無線ネットワーク名(SSID)の設定を変更する手順について、IEEE802.11a側の設定を例に説明します。

※IEEE802.11g規格とIEEE802.11a規格について、別々に設定できます。

※無線AP間通信だけに使用する(リピータ機能を使用しない)場合は、互いに異なる[SSID]でも無線AP間通信できます。

※「SSID」については、本書3-2章をご覧ください。

〈設定のしかた〉

1. 本製品の設定画面にアクセス(※3-3章Step5.)して、「無線LAN設定」メニューの[IEEE802.11a]から「無線LAN設定」をクリックします。

●「無線LAN設定」画面を表示します。

2. 「SSID」を[無線LAN設定]項目の[SSID]欄と[SSIDの確認入力]欄に、大文字/小文字の区別に注意して、任意の英数字(半角31文字以内)で入力します。

入力した文字は、すべて「*(アスタリスク)」で表示されます。

(入力例: root 表示例: ****)

3. 〈登録して再起動〉をクリックします。

4. クリック

◎画面: [IEEE802.11a]

1. クリック

2. クリック

3. 入力する

無線LAN設定 [IEEE802.11a]
無線LANを使用するときの設定を行います。

登録 取消 登録して再起動 (このページの設定は再起動後に有効になります。)

無線LAN設定	
IEEE802.11aを使用	<input type="radio"/> しない <input checked="" type="radio"/> する
SSID	****
SSIDの確認入力	****
ANYを拒否	<input checked="" type="radio"/> しない <input type="radio"/> する
チャンネル	34 (5.170MHz)
Rts/Ctsスレッシュホールド	無し
パワーレベル	高
接続端末制限	255

△SSID: 「ANY」での不正アクセスについて

「ANY」モード(アクセスポイント自動検索接続機能)対応の無線パソコンに設定された[SSID]が「空白」(無線LANカードによっては「ANY」)に設定されていると、本製品に設定された[SSID]に関係なくこれらの無線パソコンからの本製品検索やアクセスを許可した状態になります。

本製品検索やアクセスを許可しない場合は、上記画面で「ANYを拒否」欄の設定を「する」に変更してください。

また、「する」に変更した場合、Windows XP標準のワイヤレスネットワーク接続を使用する無線パソコンに表示される「利用できるワイヤレス ネットワーク」一覧にも本製品の無線ネットワーク名(SSID)を表示しません。

3-6. 暗号化を設定する

暗号化鍵(キー)によるセキュリティの設定は、16進数またはASCII文字で[キー値]のテキストボックスに直接入力する方法と、[キージェネレータ]のテキストボックスに任意の英数字や記号を入力する方法があります。

※IEEE802.11g規格とIEEE802.11a規格について、別々に設定できます。

※無線AP間通信を使用する場合も、本製品どうしおよび無線LANのパソコンが同じ暗号化セキュリティを設定しないと通信できません。

※暗号化については、「無線LANの構築について」(※3-2章)をご覧ください。

■ 16進数で暗号化鍵(キー)を入力するには

暗号化鍵を[キー値]のテキストボックスに16進数で直接入力する手順です。

下記は、設定に必要なおまな条件で、IEEE802.11a規格の場合を例に説明します。

[認証モード]：「両対応」(出荷時の設定)

[暗号化方式]：「WEP RC4 128(104)」ビット

[入力モード]：「16進数」(出荷時の設定)

[キーID]：「2」

〈設定のしかた〉

通信する相手の機器にも同じ設定をしてください。

1. 本製品の設定画面にアクセス(※3-3章Step5.)して、「無線LAN設定」メニューの「IEEE802.11a」から「暗号化設定」をクリックします。

●「暗号化設定」画面を表示します。

2. [暗号化方式]を「WEP RC4 128(104)」ビットに選択します。

※「なし(出荷時の設定)」の場合は、暗号化セキュリティが無効になります。

3. [キーID]を「2」に選択します。

4. 「登録」をクリックします。(※次ページの操作後、下記「7.」を実行)

7. クリック

5. クリック

※次ページで「6.」を操作後、「7.」を操作します。

1. クリック

2. クリック

3. 選択する

4. 選択する

[入力モード]が「16進数」であることを確認します。

◎画面：[IEEE802.11a]

ネットワーク設定

無線LAN設定

IEEE802.11g

無線LAN設定

暗号化設定

AP間通信設定

IEEE802.11a

無線LAN設定

暗号化設定

AP間通信設定

暗号化設定 [IEEE802.11a]

無線LANを使用するときの暗号化に関する設定を行います。
認証方式は暗号化方式が「RC4」以外の時は「オープンシステム」のみ設定可能です。
キーの自動変更はRADUIS機能を使用する場合のみ有効です。

登録 取消 登録して再起動

暗号化設定

認証モード 両対応

暗号化方式 WEP RC4 128(104)

キージェネレータ

ファクター 0

キーID 2

キーの自動変更を使用 しない

キー値

入力モード 16進数

3 無線LANで使う

3-6. 暗号化を設定する

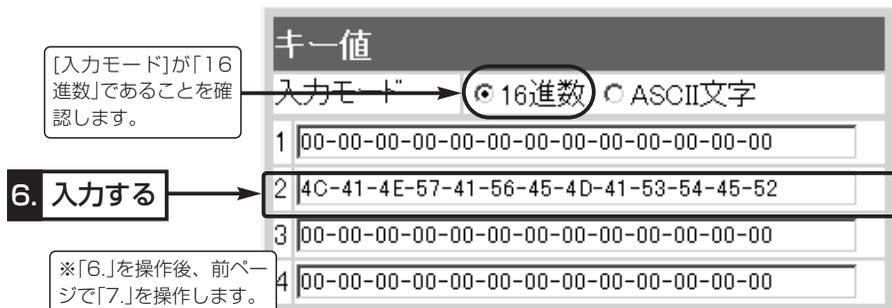
■ 16進数で暗号化鍵(キー)を入力するには(つづき)

5. [キー値]を、[キーID]が「2」のテキストボックスに16進数で入力します。

[キーID]が通信相手間で異なる設定をする場合でも、[キー値]は、同じテキストボックスに同じ値を設定しないと通信できません。

(入力例1 : 4c414e574156454d4153544552)

(入力例2 : 4c-41-4e-57-41-56-45-4d-41-53-54-45-52)



6. <登録して再起動>をクリックします。

■ ASCII文字→16進数変換表

ご使用になる無線LANカードや無線LAN対応のパソコンが両方の入力モードに対応していない場合は、下記の変換表を参考にパソコンに設定するキーを指示してください。

[例] 16進数で「4c414e574156454d4153544552」(26桁)を設定している場合、ASCII文字では、「ROOTINACCESS」(13文字)になります。

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

3-6. 暗号化を設定する(つづき)

■ ASCII文字で暗号化鍵(キー)を入力するには

暗号化鍵を[キー値]のテキストボックスにASCII文字で直接入力する手順です。

下記は、設定に必要なおまな条件で、IEEE802.11a規格の場合を例に説明します。

[認証モード] : 「両対応」(出荷時の設定)

[暗号化方式] : 「WEP RC4 128(104)」ビット

[入力モード] : 「ASCII文字」

[キーID] : 「2」

〈設定のしかた〉

通信する相手の機器にも同じ設定をしてください。

1. 本製品の設定画面にアクセス(※3-3章Step5.)して、「無線LAN設定」メニューの「IEEE802.11a」から「暗号化設定」をクリックします。
 - 「暗号化設定」画面を表示します。
2. 「暗号化方式」を「WEP RC4 128(104)」に選択します。
 - ※ 「なし(出荷時の設定)」の場合は、暗号化セキュリティが無効になります。
3. 「キーID」を「2」に選択します。
4. 「キー値」項目の「入力モード」欄で、「ASCII文字」のラジオボタンをクリックします。
5. 「登録」をクリックします。(※次ページの操作後、下記「8.」を実行)

ネットワーク設定

無線LAN設定

IEEE802.11g

IEEE802.11a

暗号化設定

暗号化設定 [IEEE802.11a]

無線LANを使用するときの暗号化に関する設定を行います。
認証方式は暗号化方式が「RC4」以外の時は「オープンシステム」のみ設定可能です。
キーの自動変更はRAJUS機能を使用する場合のみ有効です。

登録 取消 登録して再起動

このページの設定は再起動後に有効になります。

暗号化設定

認証モード 両対応

暗号化方式 WEP RC4 128(104)

キージェネレータ

ファクター 0

キーID 2

キーの自動変更を使用 はい する

キー値

入力モード 16進数 ASCII文字

◎画面 : [IEEE802.11a]

1. クリック

2. クリック

3. 選択する

4. 選択する

5. クリック

6. クリック

8. クリック

※次ページで「7.」を操作後、「8.」を操作します。

3 無線LANで使う

3-6. 暗号化を設定する

■ ASCII文字で暗号化鍵(キー)を入力するには(つづき)

6. [キー値]を、[キーID]が「2」のテキストボックスにASCII文字で入力します。

[キーID]が通信相手間で異なる設定をする場合でも、[キー値]は、同じテキストボックスに同じ値を設定しないと通信できません。(入力例：ROOTINACCESS)



7. <登録して再起動>をクリックします。

■ 暗号化鍵(キー)値の入力について

[暗号化方式]と[入力モード]の設定によって暗号化鍵(キー)に入力する桁数および文字数が下記のように異なります。

※入力モードを「16進数→ASCII文字」または「ASCII文字→16進数」に変更したときは、設定画面上で <登録> をクリックしてから鍵(キー)を入力してください。

【無線LAN規格：IEEE802.11a/b/g】

認証モード	入力モード		16進数 (HEX)	ASCII文字
	暗号化方式			
オープンシステム	シェアードキー	WEP RC4 64(40)ビット	10桁	5文字(半角)
		WEP RC4 128(104)ビット	26桁	13文字(半角)
		WEP RC4 152(128)ビット	32桁	16文字(半角)
		OCB AES 128(128)ビット	32桁	16文字(半角)

※入力できる桁数および文字数は、()内のビット数に対する値です。

■ キーIDの設定について(※Windows XP Service Pack1を除く)

無線LAN機器によっては[キーID]の選択範囲は、「1」～「4」ですが、Windows XP標準のワイヤレスネットワーク接続の選択範囲は、「0」～「3」になっています。

本製品で、「1」を選択した場合は、Windows XPの[キーのインデックス(詳細)(X)]で「0」を設定するのと同じ意味になります。

3-6. 暗号化を設定する(つづき)

■ 鍵(キー)値の設定例

「RC4 128(104)」ビットの暗号化方式を例に、[キー値]項目のテキストボックスに暗号化鍵(キー)を16進数(26桁)で直接入力する場合を説明します。

※例として、キーID「2」と「3」に、「48-6f-74-73-70-6f-74-41-63-63-65-73-73」と「57-41-56-45-4d-41-53-54-45-52-4c-41-4e」を下記のように入力します。

◎キーID「2」のキー値(鍵)が同じなので通信できます。

RDA5000側



無線LANカード側(イメージ)

キーID 2

キー値

入力モード 16進数 ASCII文字

1 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

2 48-6F-74-73-70-6F-74-41-63-63-65-73-73

3 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

4 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

キーID 02

キー	値
01	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
02	48-6F-74-73-70-6F-74-41-63-63-65-73-73
03	00.00.00.00.00.00.00.00.00.00.00.00.00.00.00
04	00.00.00.00.00.00.00.00.00.00.00.00.00.00.00

16進数入力 ASCII文字入力

◎キーID「2」とキーID「3」のキー値(鍵)が同じなので通信できます。

RDA5000側



無線LANカード側(イメージ)

キーID 2

キー値

入力モード 16進数 ASCII文字

1 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

2 48-6F-74-73-70-6F-74-41-63-63-65-73-73

3 57-41-56-45-4D-41-53-54-45-52-4C-41-4E

4 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

キーID 03

キー	値
01	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
02	48-6F-74-73-70-6F-74-41-63-63-65-73-73
03	57-41-56-45-4D-41-53-54-45-52-4C-41-4E
04	00.00.00.00.00.00.00.00.00.00.00.00.00.00.00

16進数入力 ASCII文字入力

◎キーID「2」とキーID「3」のキー値(鍵)が異なるので通信できません。

RDA5000側



無線LANカード側(イメージ)

キーID 2

キー値

入力モード 16進数 ASCII文字

1 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

2 48-6F-74-73-70-6F-74-41-63-63-65-73-73

3 57-41-56-45-4D-41-53-54-45-52-4C-41-4E

4 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

キーID 03

キー	値
01	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
02	57-41-56-45-4D-41-53-54-45-52-4C-41-4E
03	48-6F-74-73-70-6F-74-41-63-63-65-73-73
04	00.00.00.00.00.00.00.00.00.00.00.00.00.00.00

16進数入力 ASCII文字入力

3 無線LANで使う

3-6. 暗号化を設定する(つづき)

■ キージェネレータで暗号化鍵(キー)を生成するには

[キー値]項目の[入力モード]欄を「16進数」(出荷時の設定)に設定するとき、使用できる機能です。

任意の文字列をキージェネレータに入力すると、暗号化鍵(キー)を[キー値]のテキストボックスに自動生成できます。

下記は、設定に必要なおまな条件で、IEEE802.11a規格の場合を例に説明します。

[認証モード]: 「両対応」(出荷時の設定)

[暗号化方式]: 「WEP RC4 128(104)」ビット

[入力モード]: 「16進数」(出荷時の設定 ※ASCII文字の場合は、使用できません。)

〈設定のしかた〉

1. 本製品の設定画面にアクセス(☞3-3章Step5.)して、「無線LAN設定」メニューの [IEEE802.11a] から「暗号化設定」をクリックします。

- 「暗号化設定」画面を表示します。

2. 「暗号化方式」を「WEP RC4 128(104)」に選択します。

※ 「なし」(出荷時の設定)の場合は、暗号化セキュリティが無効になります。

3. 任意の英数字および文字列(半角31文字以内)を[キージェネレータ]欄に入力します。

入力した内容は、すべて「*(アスタリスク)」で表示されます。

(入力例: rda5000 表示例: *****)

4. 〈登録して再起動〉をクリックします。

5. クリック

1. クリック

3. 選択する

2. クリック

4. 選択する

[入力モード]が「16進数」であることを確認します。

〈登録して再起動〉後、暗号化鍵(キー)が自動生成されます。

ネットワーク設定

無線LAN設定 [IEEE802.11a]

無線LANを使用するときの暗号化に関する設定を行います。
認証方式は暗号化方式が「RC4」以外の時は「オープンシステム」のみ設定可能です。
キーの自動変更はRADIUS機能を使用する場合のみ有効です。

登録 取消 登録して再起動 (このページの設定は再起動後に有効になります。)

暗号化設定

認証モード	両対応
暗号化方式	WEP RC4 128(104)
キージェネレータ	*****
ファクター	0
キーID	1
キーの自動変更を使用	<input type="checkbox"/> しない <input checked="" type="checkbox"/> する

キー値

入力モード	<input checked="" type="radio"/> 16進数 <input type="radio"/> ASCII文字
1	EC-04-5E-99-30-DE-11-B5-8E-3C-51-0D-09
2	01-F6-8C-ED-06-36-E7-6A-A2-49-35-EE-28
3	08-5A-3E-5C-68-0F-50-05-88-9B-AC-B3-47
4	04-28-E9-BE-29-46-16-09-F3-65-AA-B6-9E

◎画面: [IEEE802.11a]

3-7. MACアドレスセキュリティを設定する

MACアドレス(※3-2章)を登録する手順について説明します。

登録されたMACアドレスを持つパソコンと無線で通信できます。

〈設定のしかた〉

1. 本製品の設定画面にアクセス(※3-3章Step5.)して、「無線LAN設定」メニューをクリックします。
 - 「セキュリティ設定」画面を表示します。
 2. [MACアドレスセキュリティ設定]項目の[MACアドレスセキュリティを使用]欄で、「する」のラジオボタンをクリックします。
 3. 〈登録〉をクリックします。
 4. 本製品と通信する無線パソコン(無線LANカード)のMACアドレスを[登録の追加(MACアドレス)]欄に、半角英数字で入力します。
(入力例：00-90-c7-33-00-14、0090c7330014)
 5. [登録の追加(MACアドレス)]欄の右にある〈追加〉をクリックします。
 - [現在の登録(登録済みの端末)]欄に追加した無線パソコンのMACアドレスが表示されます。
- ※ 通信を許可したい無線パソコンが[現在の登録(受信中の端末)]欄に表示されている場合は、「通信不許可」を表示する欄の右にある〈追加〉をクリックします。

3. クリック

2. クリック

1. クリック

4. 入力する

5. クリック

登録済みのMACアドレスを削除するボタンです。

アクセス権のない無線パソコンのMACアドレスを登録するボタンです。

ネットワーク設定

無線LAN設定

セキュリティ設定

IEEE802.11g

- 無線LAN設定
- 暗号化設定
- AP間通信設定

IEEE802.11g

- 無線LAN設定
- 暗号化設定
- AP間通信設定

セキュリティ設定

RADIUSやMACアドレスセキュリティなど、無線LANを使用するときの認証設定を行います。RADIUS機能を使用する場合は、暗号化設定のキーIDは無効になります。暗号化方式がRC4の場合のみ暗号キーの自動通信を行います。

登録 取消 登録して再起動 RADIUS設定は再起動後に有効になります。

MACアドレスセキュリティ設定

MACアドレスセキュリティを使用 しない する

登録の追加

MACアドレス

0090c7330014 追加

現在の登録

登録済みの端末	受信中の端末	通信状況	
00-90-C7-8C-00-14	00-90-C7-6C-00-14	通信中	削除
00-90-C7-6C-00-32		登録済	削除
	00-90-C7-6E-00-CB	通信不許可	追加

現在の登録

登録済

00-90-C7-8C-00-14	00-90-C7-6C-00-14	通信中	削除
00-90-C7-6C-00-32		登録済	削除
	00-90-C7-6E-00-CB	通信不許可	追加

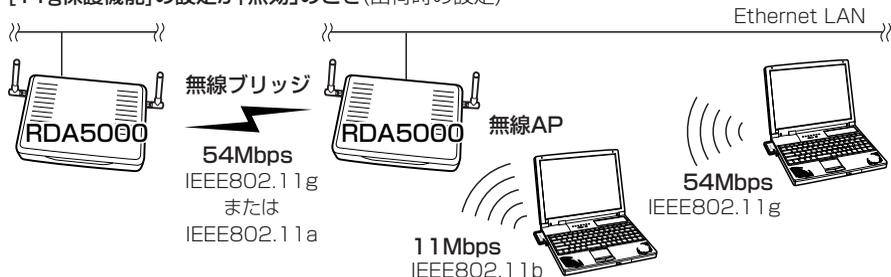
3 無線LANで使う

3-8. 802.11b規格の通信を制限するには

IEEE802.11g規格とIEEE802.11b規格で本製品にアクセスする無線パソコンが混在する環境で、IEEE802.11g規格との通信を優先したり、IEEE802.11g規格との通信だけに限定できます。

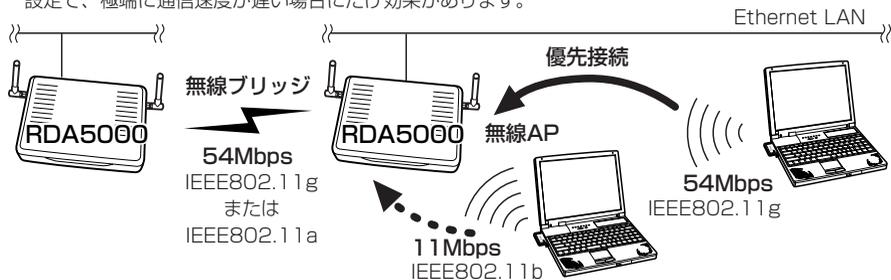
[11g保護機能]の設定によって、図のような通信ができます。

[11g保護機能]の設定が「無効」のとき(出荷時の設定)

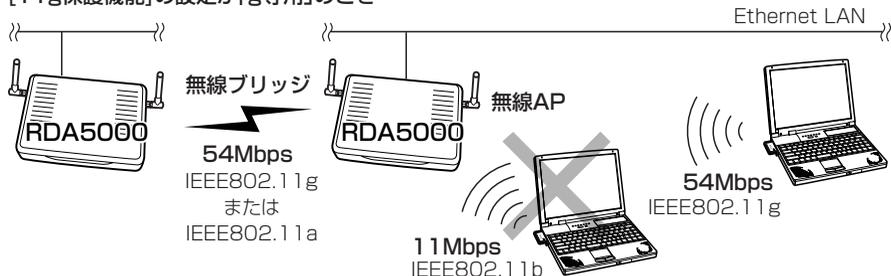


[11g保護機能]の設定が「有効」のとき

※IEEE802.11b規格との混在により、IEEE802.11g規格の速度が低下するのを防止でき、出荷時の設定で、極端に通信速度が遅い場合にだけ効果があります。



[11g保護機能]の設定が「g専用」のとき



※[11g保護機能]は、「無線LAN設定」メニューの[IEEE802.11g]から「無線LAN設定」をクリックして表示される画面で設定できます。

3-9. スパニングツリー機能を使用してみる

スパニングツリー機能を本製品に設定すると、有線LANに経路障害が起きたとき、代わりに無線LAN(無線ブリッジ)で通信を継続できます。

下記の図に示す接続例の場合、有線LANの経路に障害がないときは、優先度の低い無線LANのポートを停止しています。

※下記の図を例に、スパニングツリー機能で通信できるようにするまでに最低限必要な項目の設定について説明します。

また、本製品をそれぞれ、[A]と[B]として説明します。



Step 1. 無線AP間通信を設定する

設定手順は、IEEE802.11a規格の無線AP間通信機能を例にしています。

1. [無線LAN設定](802.11a)画面(☞3-5章)で、本製品[A]と本製品[B]の[SSID]が同じ設定であることを確認します。(出荷時の設定：[LG](半角大文字))
2. [無線LAN設定](802.11a)画面で、本製品[A]と本製品[B]の[チャンネル]が同じ設定であることを確認します。(出荷時の設定：34(5170MHz))
3. 「無線AP(アクセスポイント)間通信機能を使用してみる」(☞3-4章)の設定例を参考に、本製品に内蔵された802.11a規格側無線LANカードの[BSSID]を、相手のRDA5000に登録します。

自分のRDA5000には、相手側の本製品に内蔵された802.11a規格側無線LANカードの[BSSID]に登録します。

※本製品のIPアドレスやDHCPサーバの設定は、ご使用になる環境に合わせて設定されている状態とします。

3 無線LANで使う

3-9. スパニングツリー機能を使用してみる(つづき)

Step2. スパニングツリー機能を設定する

スパニングツリー機能を本製品[A]と本製品[B]に設定します。

1. 本製品の設定画面にアクセス(※3-3章Step5.)して、「ネットワーク設定」メニューから「ブリッジ設定」をクリックします。
 - 「ブリッジ設定」画面を表示します。
2. 「スパニングツリー機能を使用」欄で「する」のラジオボタンをクリックします。
3. 「登録して再起動」をクリックします。

ネットワーク設定
LAN/IPv4設定
ブリッジ設定
IPv6設定
ルーティング設定

無線LAN設定
WAN側設定
システム設定
情報表示

ブリッジ設定

ブリッジ機能に関する設定を行います。

登録 取消 登録して再起動 (このページの設定は再起動後に有効になります。)

ブリッジ設定

スパニングツリー機能を使用	<input type="radio"/> しない <input checked="" type="radio"/> する	
ブリッジ優先度(Bridge Priority)	32768	
エージングタイム(Aging Time)	300 秒	
マックスエイジ(Max. Age)	20 秒	
ハロータイム(Hello Time)	2 秒	
転送遅延(Forward Delay)	15 秒	
パスコスト(Path Cost)	有線LAN	100
	無線[802.11g]	200
	無線[802.11a]	200
ポート優先度(Port Priority)	有線LAN	128
	無線[802.11g]	128
	無線[802.11a]	128

ご参考に- 優先度について

ブリッジ接続された本製品の経路優先度は、ブリッジ優先度→パスコスト→ポート優先度の順に決定され、各設定値の小さい方が優先されます。

ご使用のネットワークの形態によって、これらの設定値で優先度を設定してください。前ページの接続例の場合、ブリッジ優先度は、本製品[A]と本製品[B]で同じ設定値「32768(出荷時の設定)」のため、MACアドレスの小さい本製品[A]を優先します。本製品[A]のパスコストは、[無線802.11a]の設定値「200(出荷時の設定)」より[有線LAN]に設定された設定値「100(出荷時の設定)」のほうが小さいため、有線LANの経路が優先されます。

ポート優先度は、[有線LAN]と[無線802.11a]の設定値が同じ設定値「128(出荷時の設定)」のため比較の対象にはなりません。

この章では、本製品をブロードバンドモデムまたはメディアコンバーターに接続してインターネットする場合の設定について説明しています。

2章～3章で設定後、Step1.～Step6.にしたがって設定してください。

Step1.回線接続業者との契約について	48
Step2.お使いになるモデムタイプの確認	48
Step3.ご契約回線への接続方法を確認する	49
■ ルータタイプモデムをご使用のかた	49
■ ブリッジタイプモデムやメディアコンバーターをご使用のかた	49
■ MACアドレスの申請が必要なときは	49
Step4.回線種別を設定する	50
■ ルータタイプモデムをご使用のかた	50
■ ブリッジタイプモデムやメディアコンバーターをご使用のかた	50
Step4-1.「接続しない」を設定した場合	51
Step4-2.「DHCP」方式を設定した場合	52
Step4-3.「DHCP」方式で指定の「固定IPアドレス」がある場合	53
Step4-4.「PPPoE」方式を指定した場合	54
Step4-5.「PPPoE複数固定IP」方式を設定した場合	55
Step5.モデムと接続する	56
■ ルータタイプモデムと接続する場合	56
■ ブリッジタイプモデムやメディアコンバーターと接続する場合	57
Step6.インターネットへの接続を確認する	58
■ ルータタイプモデムをご使用のかた	58
■ ブリッジタイプモデムやメディアコンバーターをご使用のかた	58

【接続業者から配布のPPPoE接続ソフトウェアについて】

Windows XP以前のOSをご利用のかたで、「PPPoE」/「PPPoE複数固定IP」方式で接続する場合は、接続業者またはプロバイダーから配布されるPPPoE接続用ソフトウェアのインストールは不要です。すでに、ご使用のパソコンにインストールされているときは、そのソフトウェアのアンインストールをするか自動接続設定を「無効」に変更してください。

本章に記載の接続業者およびプロバイダーは、弊社で接続確認しておりますが、記載各社への直接の問い合わせは、ご遠慮願います。

4 回線接続ガイド

Step1. ➤ 2. ➤ 3. ➤ 4. ➤ 5. ➤ 6.

Step1. 回線接続業者との契約について

インターネットに接続するためには、接続業者との契約および工事が完了している必要があります。

契約や工事の完了についてご不明な場合は、ご契約の接続業者やお買い上げの販売店などにご相談ください。

Step2. お使いになるモデムタイプの確認

ご契約の接続業者から供給されるADSLモデムやCATVケーブルモデムには、ルータタイプとブリッジタイプがあります。

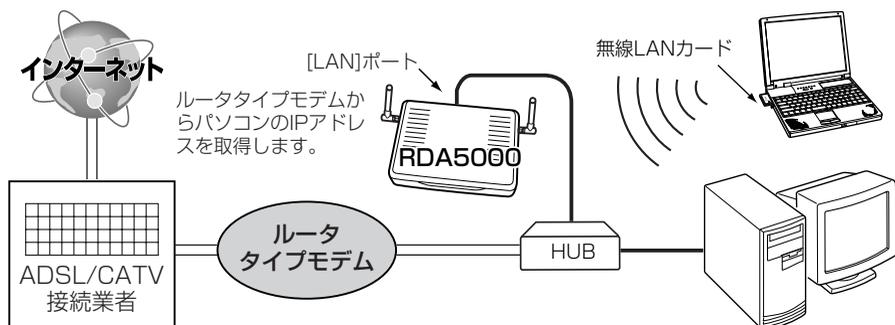
※[FTTH](メディアコンバーター)でご使用の場合は、ブリッジタイプをご覧ください。

ご契約の接続業者やサービスによって、供給されるモデムタイプや回線への接続方法が異なりますので、本製品を設定する前に下記のことを確認してください。

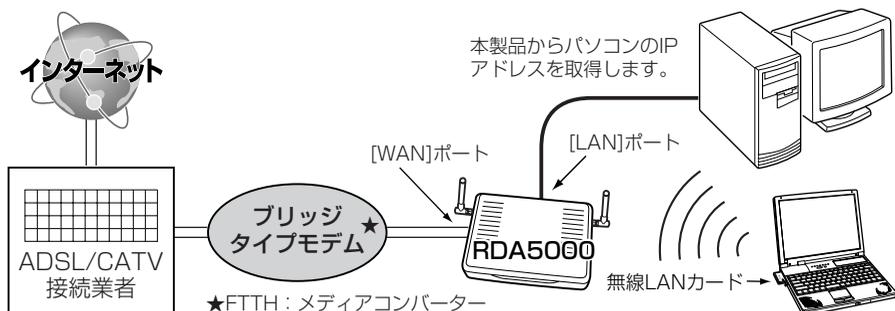
各タイプのモデムで本製品をご使用になる場合は、図のようになります。

ルータタイプ：ルータ機能搭載のモデムです。

このモデムにHUBを接続して複数のパソコンで使うタイプで、接続されたパソコンには、ルータタイプモデムからプライベートIPアドレスが割り当てられます。



ブリッジタイプ：通常1台のパソコンをモデムに接続して使うタイプで、接続されたパソコンには、ご契約のプロバイダーからIPアドレスが割り当てられます。



★FTTH：メディアコンバーター

Step3. ご契約回線への接続方法を確認する

■ ルータタイプモデムをご使用のかた(☞Step4.→Step4-1.)

アッカネットワークスやイー・アクセスなどでご契約の場合に該当します。

ご使用のルータタイプモデムのLAN側IPアドレスと重複する場合は、本製品のLAN側IPアドレス(出荷時：192.168.0.1)の変更が必要ですので、あらかじめモデムのLAN側IPアドレスを、モデムに付属する取扱説明書でご確認ください。

■ ブリッジタイプモデムやメディアコンバーターをご使用のかた

ご契約の接続業者からブリッジタイプモデムまたはメディアコンバーターを供給されている場合、接続業者またはプロバイダーからインターネットへの接続方法と設定内容が指定されます。

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

◆「DHCP」方式での接続を指定された場合(☞Step4.→Step4-2.)

CATVやYAHOO! BBでご契約の場合に該当し、本製品のWAN側に設定するIPアドレスをプロバイダーから自動取得する方式です。

- コンピュータ名(ホスト名/本体名称)
- ドメイン名

◆「固定IPアドレス」での接続を指定された場合(☞Step4.→Step4-3.)

本製品のWAN側に設定するIPアドレスがプロバイダーから指定されます。

- コンピュータ名(ホスト名/本体名称)
- ドメイン名
- 固定IPアドレス
- サブネットマスク
- デフォルトゲートウェイ
- プライマリDNSサーバのIPアドレス
- セカンダリDNSサーバのIPアドレス

◆「PPPoE」方式での接続を指定された場合(☞Step4.→Step4-4.)

Bフレッツ(FTH)やフレッツ・ADSLでご契約された場合などに該当する方式です。

- ユーザID(アカウントID)
- パスワード(ログインパスワード)
- 固定IPアドレス
- サブネットマスク
- デフォルトゲートウェイ
- プライマリDNSサーバのIPアドレス
- セカンダリDNSサーバのIPアドレス

◆「PPPoE複数固定IP」方式での接続を指定された場合(☞Step4.→Step4-5.)

ご契約のプロバイダーから割り当てられるグローバル固定IPアドレスの範囲にしたがって、本製品のWAN側と本製品に接続されたパソコンに直接設定する方式です。

- ユーザID(アカウントID)
- パスワード(ログインパスワード)
- 契約した数の固定IPアドレス
- サブネットマスク
- デフォルトゲートウェイ
- プライマリDNSサーバのIPアドレス
- セカンダリDNSサーバのIPアドレス

■ MACアドレスの申請が必要なときは(はじめに☞Pv)

※MACアドレスは、本製品のシリアルシールに12桁で記載されています。

詳しくは、「MACアドレス表記について」(はじめに☞Pv)をご確認ください。

4 回線接続ガイド

1. > 2. > 3. > Step4. > 5. > 6.

Step4. 回線種別を設定する

本製品の[回線種別]を回線への接続方法に応じて変更します。

■ ルータータイプモデムをご使用のかた：「接続しない」を設定します。

■ ブリッジタイプモデムやメディアコンバーターをご使用のかた：
次のいずれかに設定します。

- ◆ 「DHCP」方式での接続を指定された場合 ⇨ 「DHCP」を設定
- ◆ 「固定IPアドレス」での接続を指定された場合 ⇨ 「DHCP」を設定
- ◆ 「PPPoE」方式での接続を指定された場合 ⇨ 「PPPoE」を設定
- ◆ 「PPPoE」方式で「複数固定IP」の契約をされた場合 ⇨ 「PPPoE複数固定IP」を設定

〈設定のしかた〉

1. 本製品の設定画面にアクセスして、「WAN側設定」メニューをクリックします。
 - 「WAN側設定」画面を表示します。
 2. [回線種別]項目で該当する接続方法のラジオボタンをクリックします。
 3. ほかの項目についても設定を続けますので、〈登録〉をクリックします。
 - 選択された接続方法に応じた画面を表示します。
- ※ 〈登録して再起動〉は、すべての設定が完了後に行います。
モデムの接続は、あとで行います。

ネットワーク設定
無線LAN設定
WAN側設定
WAN側詳細設定
アドレス変換設定
IPフィルタ設定
システム設定
情報表示

WAN側設定

インターネット接続に関する設定を行います。

本体の時刻：2003年01月01日01時08分

接続状況	
未接続	-
回線種別	接続しない
DNSサーバ	-
本体側のIPアドレス	-
相手先のIPアドレス	-
接続時間	- 時間 - 分 - 秒

接続しない DHCP PPPoE PPPoE複数固定IP

回線種別の設定は再起動後に有効になります。

4. 回線種別以外にプロバイダーから指定された内容を設定します。

設定した回線種別によって、設定する画面や方法が異なります。

これ以降の説明は、記載の箇所をご覧ください。

- ◆ 「接続しない」を設定した場合 ⇨ Step4-1.に進みます。
- ◆ 「DHCP」方式を設定した場合 ⇨ Step4-2.に進みます。
- ◆ 「DHCP」方式で指定の「固定IPアドレス」がある場合 ⇨ Step4-3.に進みます。
- ◆ 「PPPoE」方式を設定した場合 ⇨ Step4-4.に進みます。
- ◆ 「PPPoE複数固定IP」方式を設定した場合 ⇨ Step4-5.に進みます。

Step4-1.「接続しない」を設定した場合

ルータタイプモデムのDHCPサーバ機能を使用しますので、次の手順で本製品のDHCPサーバ機能を無効に変更します。

また、ご使用のルータタイプモデムのLAN側IPアドレスと重複する場合は、本製品のLAN側IPアドレス(出荷時：192.168.0.1)の変更が必要です。

例えば、ルータタイプモデムのLAN側IPアドレスが「192.168.0.1」の場合は「192.168.0.250」に変更し、「192.168.1.1」の場合は「192.168.1.250」に変更してください。

本書では、「192.168.0.250」に変更する手順を説明します。

〈変更のしかた〉

- 1.「ネットワーク設定」メニューをクリックします。
 - 「LAN側IP設定」画面を表示します。
- 2.[本体名称/IPアドレス設定]項目の[IPアドレス]欄で、本製品のLAN側IPアドレスを変更します。
(変更例：192.168.0.250)
- 3.[DHCPサーバ設定]項目の[DHCPサーバ機能を使用]欄で、「しない」のラジオボタンをクリックします。
- 4.〈登録して再起動〉をクリックします。
 - 変更された設定項目の内容が有効になります。

The screenshot shows the 'LAN側IP設定' (LAN Side IP Settings) page. On the left is a navigation menu with 'ネットワーク設定' (Network Settings) selected. The main content area is titled 'LAN側IP設定' and includes a sub-section 'DHCPサーバ設定' (DHCP Server Settings). In this section, the 'DHCPサーバ機能を使用' (Use DHCP Server Function) option is set to 'しない' (No). The '登録して再起動' (Register and Restart) button is highlighted with a callout box.

1. クリック → ネットワーク設定

4. クリック → 登録して再起動

2. 入力する → IPアドレス

3. クリック → しない

LAN側IP設定	
本体をネットワークに接続するための設定を行います。	
登録	取消
登録して再起動 (本体IPアドレス/サブネットマスクの設定は再起動後に有効になります。)	
本体名称/IPアドレス設定	
本体名称	FD45000
IPアドレス	192.168.0.250
サブネットマスク	255.255.255.0
DHCPサーバ設定	
DHCPサーバ機能を使用	<input checked="" type="radio"/> しない <input type="radio"/> する
割り当て開始IPアドレス	192.168.0.10
割り当て個数	80 個
サブネットマスク	255.255.255.0
リース期間	72 時間
ドメイン名	
デフォルトゲートウェイ	192.168.0.1
DNS代理応答を使用	<input type="radio"/> しない <input checked="" type="radio"/> する

4 回線接続ガイド

1. > 2. > 3. > Step4-2. > 5. > 6.

Step4. 回線種別を設定する(つづき)

Step4-2. 「DHCP」方式を設定した場合

〈設定のしかた〉

1. 「ネットワーク設定」メニューをクリックします。
 - 「LAN側IP設定」画面を表示します。
2. プロバイダーから指定された「本体名称」と「ドメイン名」を入力します。
3. 〈登録して再起動〉をクリックします。
 - 変更された設定項目の内容が有効になります。

The screenshot shows the 'LAN側IP設定' (LAN Side IP Setting) screen. The left sidebar contains a menu with 'ネットワーク設定' (Network Setting) selected. The main area is divided into sections: '本体名称/IPアドレス設定' (Device Name/IP Address Setting) and 'DHCPサーバ設定' (DHCP Server Setting). Callouts indicate the following actions:

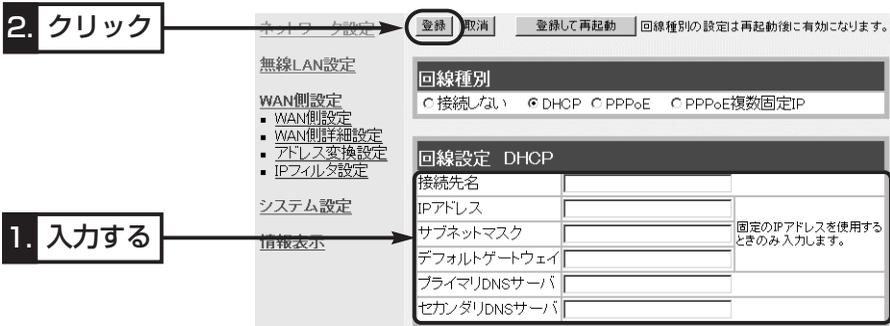
- 1. クリック**: Click on 'ネットワーク設定' in the sidebar.
- 2. 入力する**: Enter 'RDA5000' in the '本体名称' (Device Name) field.
- 3. 入力する**: Enter a domain name in the 'ドメイン名' (Domain Name) field.
- 4. クリック**: Click on the '登録して再起動' (Register and Restart) button.

本体名称/IPアドレス設定	
本体名称	RDA5000
IPアドレス	192.168.0.1
サブネットマスク	255.255.255.0

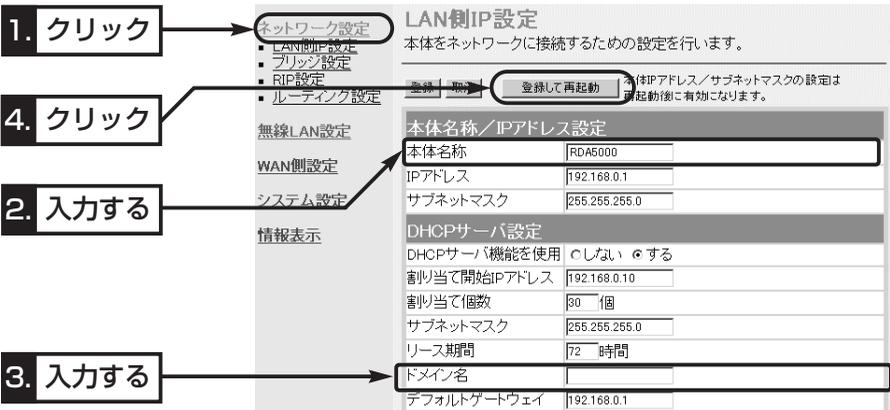
DHCPサーバ設定	
DHCPサーバ機能を使用	<input type="radio"/> しない <input checked="" type="radio"/> する
割り当て開始IPアドレス	192.168.0.10
割り当て個数	30 個
サブネットマスク	255.255.255.0
リース期間	72 時間
ドメイン名	
デフォルトゲートウェイ	192.168.0.1

Step4-3. 「DHCP」方式で指定の「固定IPアドレス」がある場合 〈設定のしかた〉

1. プロバイダーから指定された内容を「WAN側設定」画面の「回線設定 DHCP」に設定します。
※指定のない項目は、空白のままにしておきます。
2. 設定を続けますので、〈登録〉をクリックします。



3. 「ネットワーク設定」メニューをクリックします。
 - 「LAN側IP設定」画面を表示します。
4. プロバイダーから指定された「本体名称」と「ドメイン名」を入力します。
5. 〈登録して再起動〉をクリックします。
 - 変更された設定項目の内容が有効になります。



4 回線接続ガイド

1. > 2. > 3. > Step4-4. > 5. > 6.

Step4. 回線種別を設定する(つづき)

Step4-4. 「PPPoE」方式を指定した場合

〈設定のしかた〉

1. プロバイダーから指定された内容を「WAN側設定」画面の「回線設定 PPPoE」と「接続設定」に入力します。
※指定のない項目は、空白のままにしておきます。
2. 〈登録して再起動〉をクリックします。
 - 入力された設定項目の内容が有効になります。

4. クリック

登録して再起動 回線種別の設定は再起動後に有効になります。

ネットワーク設定

無線LAN設定

WAN側設定

- WAN側設定
- WAN側詳細設定
- アドレス変換設定
- IPフィルタ設定

システム設定

情報表示

回線種別

接続しない DHCP PPPoE PPPoE複数固定IP

回線設定 PPPoE

接続先名	
IPアドレス	
サブネットマスク	固定のIPアドレスを使用するときのみ入力します。
デフォルトゲートウェイ	
プライマリDNSサーバ	
セカンダリDNSサーバ	

接続設定

ユーザID	
パスワード	
認証プロトコル	相手に合わせる ▼

1. 入力する

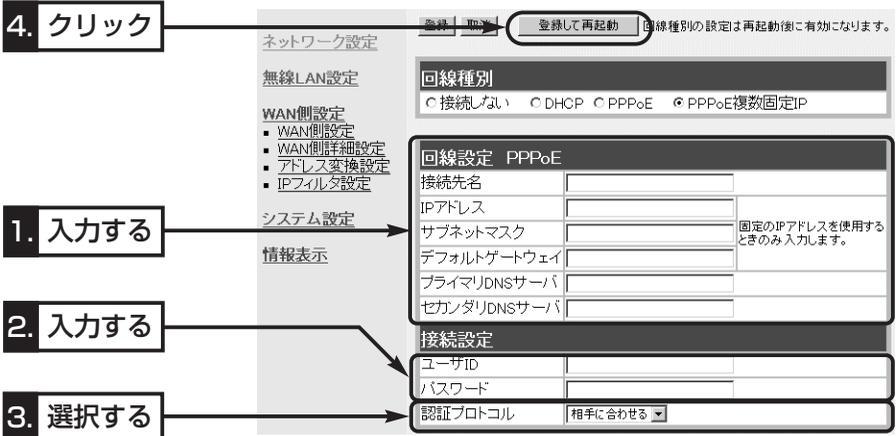
2. 入力する

3. 選択する

Step4-5. 「PPPoE複数固定IP」方式を設定した場合

〈設定のしかた〉

1. プロバイダーから指定された内容を「WAN側設定」画面の「回線設定 PPPoE」と「接続設定」に入力します。
 - ※プロバイダーから指定された利用可能な複数のグローバル固定IPアドレスのうち1つを、「回線設定 PPPoE」項目の「IPアドレス」欄に入力します。
ネットワークIPアドレスとブロードキャストアドレスを除く残りのグローバル固定IPアドレスは、本製品に接続するパソコンに直接割り当てます。
 - ※指定のない項目は、空白のままにしておきます。
2. 「登録して再起動」をクリックします。
 - 入力された設定項目の内容が有効になります。



■ グローバル固定IPアドレスの使いかた

ご契約のプロバイダーから8個のグローバル固定IPアドレスを指定された場合を例に、その使いかたを説明します。

- ◎割り当てられた指定の8個 : 172.16.0.48 ~ 172.16.0.55
- ◎サブネットマスク : 255.255.255.248
- ◎ネットワークIPアドレス : 172.16.0.48(使用できません)
- ◎ブロードキャストアドレス : 172.16.0.55(使用できません)
- ◎172.16.0.49(WAN側IPアドレスとして本製品に設定)
- ◎172.16.0.50~172.16.0.54(本製品に接続するパソコンに使用可能)
- ※指定以外のグローバルIPアドレスを使用することはできません。

また、連続で指定された複数のグローバル固定IPアドレスのうち、最初(ネットワークアドレス)と最後(ブロードキャストアドレス)は、ネットワーク上でホストに割り当てて使用できない規則になっています。

4 回線接続ガイド

1. > 2. > 3. > 4. > Step5. > 6.

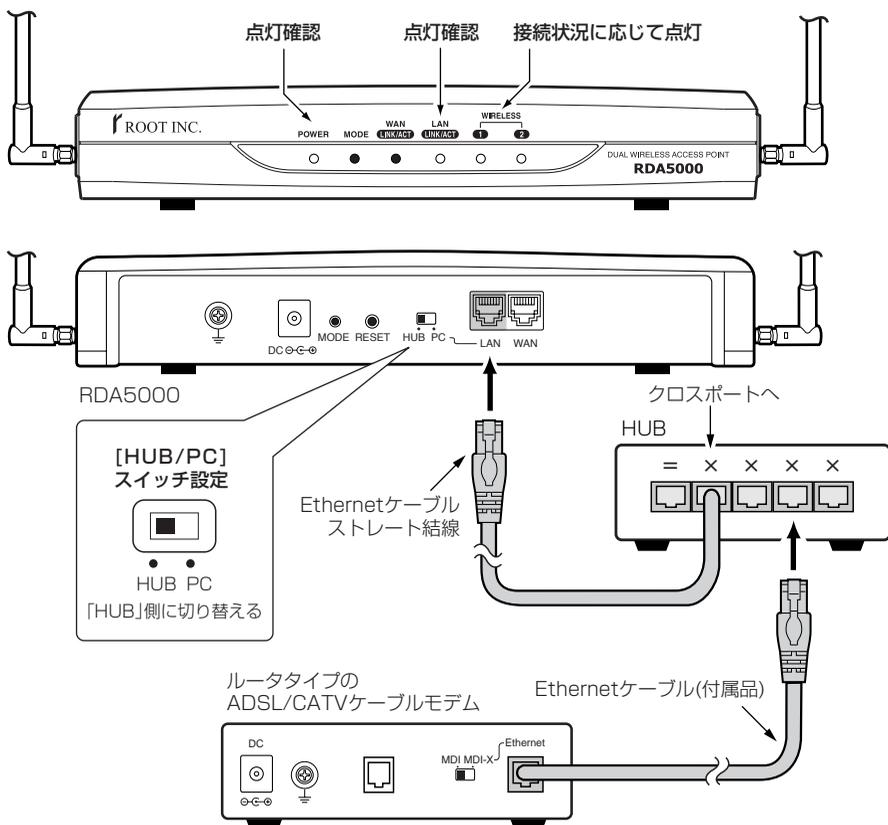
Step5. モデムと接続する

ADSLまたはCATVでご使用の場合は、お使いのモデムタイプ(☞Step2.)に該当する接続方法にしたがって接続します。

FTTHでご使用の場合は、メディアコンバーターを接続します。

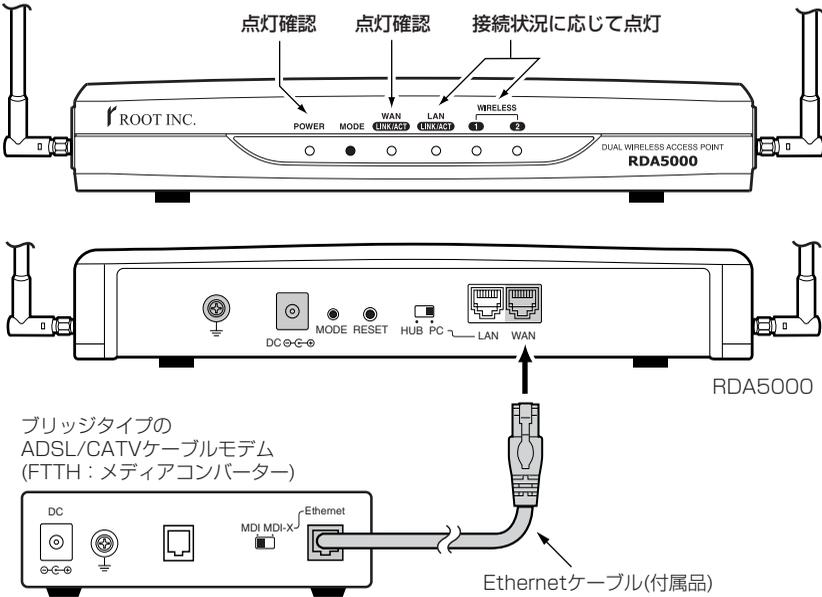
■ ルータタイプモデムと接続する場合

下記の図を参考に、本製品とルータタイプモデムを接続します。



■ブリッジタイプモデムやメディアコンバーターと接続する場合

下記の図を参考に、本製品とブリッジタイプモデムまたはメディアコンバーターを接続します。



4 回線接続ガイド

1. > 2. > 3. > 4. > 5. > Step6.

Step6. インターネットへの接続を確認する

本製品とモデムを接続後、インターネットに接続する方法について説明します。

■ ルータータイプモデムをご使用のかた

〈接続のしかた〉

WWWブラウザを起動して、アドレスバーにお好みのURLを入力するとインターネットできます。
(例:http://www.root-hq.com)

■ ブリッジタイプモデムやメディアコンバーターをご使用のかた

〈接続のしかた〉

1.本製品の設定画面にアクセスします。

- 「ネットワーク設定」メニューの「LAN側IP設定」画面を最初に表示します。

2.「WAN側設定」メニューをクリックします。

- 「WAN側設定」画面を表示します。

3.「接続状況」項目の一番上の欄に「接続中」と表示されている場合は、WWWブラウザのアドレスバーにお好みのURLを入力するとインターネットできます。

(例:http://www.root-hq.com)

「未接続」と表示されているときは、表示されている右側の〈接続〉ボタンをクリックすると接続を開始します。

※「PPPoE」または「PPPoE複数固定IP」で接続している場合は、自動接続が設定されていますので、WWWブラウザのアドレスバーにお好みのURLを入力するとインターネットできます。また、自動切断タイマー(10分)により、設定時間以上インターネットへのアクセスがないときは、切断されます。

4.回線を強制切断するときは、〈切断〉ボタンをクリックします。

The screenshot shows the 'WAN側設定' (WAN Side Settings) page of the RDA5000 Dual Wireless Access Point. The browser address bar shows 'http://192.168.0.1/'. The page title is 'Dual Wireless Access Point RDA5000 設定画面 Ver. 1.18'. The '接続状況' (Connection Status) table shows '接続中' (Connected) with buttons for '[接続]' and '[切断]'. A callout box explains that clicking these buttons manually starts or stops the connection.

1. 入力する → http://192.168.0.1/ [Enter]キーを押す

2. クリック → WAN側設定

3. 確認する → 接続状況

接続状況

接続中	[接続] [切断]
回線種別	PPPoE(自動接続)
DNSサーバ	-
本体側のIPアドレス	-
相手先のIPアドレス	-
接続時間	-時間-分-秒

手動で「接続」または「切断」するときクリックします。

この章では、そのほかに設定が必要と思われる機能や設定の参考としていただくための
内容について説明しています。

5-1.本製品の時計を設定する	60
5-2.設定画面へのアクセスを制限するには	61
5-3.本体IPアドレスを変更するには	62
5-4.自動割り当て開始IPアドレスを変更するには	63
5-5.DHCPサーバ機能を停止するには	64

5 その他の基本設定

5-1. 本製品の時計を設定する

本製品の内部時計を設定する手順について説明します。

内部時計設定を行わないと通信記録を正しく表示できませんので、導入後すぐに設定されることをお勧めします。

〈設定のしかた〉

1. 本製品の設定画面にアクセスして、「システム設定」メニューから「時計設定」をクリックします。
 - 「時計設定」画面を表示します。
2. [内部時計設定]項目の[設定する時刻]欄に、パソコンから自動取得した時刻が設定されているのを確認して、〈登録〉をクリックします。
 - ※表示されている時刻がパソコンと異なるときは、もう一度、手順1.から操作を行うと正確な時刻が登録できます。
3. 内部時計に設定された時刻が[内部時計設定]項目の[本体の時刻]欄に表示されていることを確認します。

4. クリック

1. クリック

2. クリック

5. 確認する

3. 確認する

ネットワーク設定

無線LAN設定

WAN側設定

システム設定

本体管理設定

時計設定

STP/LOG設定

SNMP設定

設定保存

情報表示

時計設定

本体の内部時計の設定を行います。

登録 取消

内部時計設定

本体の時刻	2002年	10月	07日	14時	43分
設定する時刻	2002年	10月	07日	14時	43分

自動時計設定

自動時計設定を使用	<input type="radio"/> しない <input checked="" type="radio"/> する
NTPサーバ1 IPアドレス	133.100.9.2
NTPサーバ2 IPアドレス	
アクセス時間間隔	1 日
前回アクセス日時	----/--/--
次回アクセス日時	2002/10/08 14:37

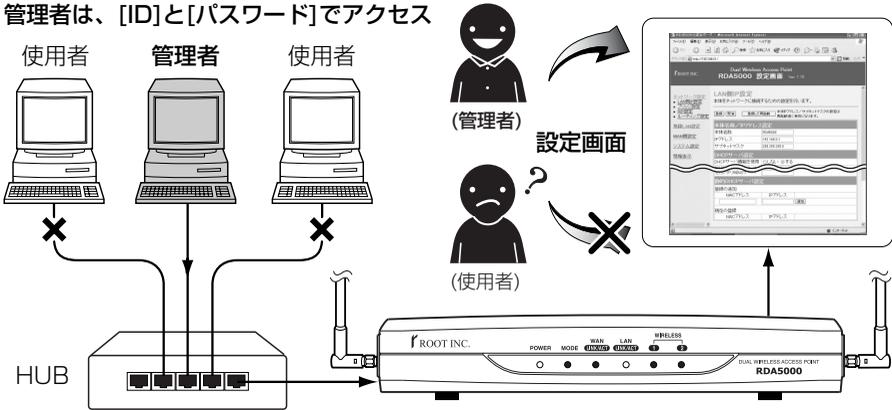
△注意 本製品の電源を切ると、本製品の内部時計の設定が出荷時の状態に戻ります。全設定の初期化、停電や不慮の事故で電源が一時的にでも切れたときは、再設定が必要です。なお、設定を初期化しても、自動時計が設定されていますので、インターネットに接続できる状態に設定後は、自動的に時計が設定されます。

5-2. 設定画面へのアクセスを制限するには

管理者用の[管理者ID]と[管理者パスワード]を設定することで、管理者以外がWWWブラウザから本製品の設定を変更できないようにします。

[管理者ID]と[管理者パスワード]が設定されていると、アクセスのとき[ユーザー名(U)]と[パスワード(P)]の入力を求める画面が表示されるようになります。

管理者は、[ID]と[パスワード]でアクセス



〈設定のしかた〉

IDとパスワードは、大文字/小文字の区別に注意して入力してください。

1. 本製品の設定画面にアクセスして、「システム設定」メニューをクリックします。
 - 「本体管理設定」画面を表示します。
2. [管理者ID設定]項目の[管理者ID]欄に、任意の英数字[半角31(全角15)文字以内]で入力します。
(入力例：user)
3. [管理者ID設定]項目の[管理者パスワード]欄と[パスワードの確認入力]欄に、任意の英数字(半角31文字以内)で入力します。
入力した文字は、すべて「*(アスタリスク)」で表示されます。
(入力例：userpass 表示例：*****)
4. 〈登録〉をクリックします。

3. クリック → 登録

1. クリック → システム設定

2. 入力する → 管理者ID設定

管理者ID設定	
管理者ID	user
管理者パスワード	*****
パスワードの確認入力	*****

設定初期化
 初期化する
 「Firm Utility使用」モード
 移行する

5 その他の基本設定

5-3. 本体IPアドレスを変更するには

既存のLANやルータタイプモデムに接続する場合、本製品を出荷時の状態で使うと、既存のネットワーク機器に割り当てられているIPアドレスと重複する可能性があります。このようなとき、本製品のLAN側IPアドレスを変更する手順について説明します。

〈変更のしかた〉

1. 本製品の設定画面にアクセスします。
 - 「ネットワーク設定」メニューの「LAN側IP設定」画面を最初に表示します。
2. 「本体名称/IPアドレス設定」項目の「IPアドレス」欄で、本製品のLAN側IPアドレスを変更します。
 - ※ 接続するほかのネットワークとIPアドレスが重複しないようにしてください。
 - ※ 本製品のDHCPサーバ機能を使用する場合で、本製品のLAN側IPアドレスの「ネットワーク部」を変更したときは、自動割り当て開始IPアドレスのネットワーク部も併せて変更(※5-4章)してから、手順3.の操作を行ってください。
3. 〈登録して再起動〉をクリックします。
 - 設定した内容が有効になります。



4. 本製品のDHCPサーバ機能を使用している場合は、パソコンのIPアドレスを取り直さずか、パソコンを再起動してください。
また、パソコンのIPアドレスを固定している場合は、パソコンに設定されたIPアドレスのネットワーク部を本製品と同じに変更してください。

【IPアドレスの割り当てかた】

IPアドレスは、「ネットワーク部」と「ホスト部」の2つの要素から成り立っています。出荷時の本製品のIPアドレス「192.168.0.1」(クラスC)を例とすると、最初の「192.168.0.」までが「ネットワーク部」で、残りの「1」を「ホスト部」といいます。「ネットワーク部」が同じIPアドレスを持つネットワーク機器(パソコンなど)は、同じネットワーク上にあると認識されます。

さらに「ホスト部」によって同じネットワーク上にある各ネットワーク機器を識別しています。以上のことから、IPアドレスを割り当てるときは、次のことに注意してください。

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

5-4. 自動割り当て開始IPアドレスを変更するには

本製品のDHCPサーバ機能を使うときなど、本製品のIPアドレス(ネットワーク部)を変更しているときは、自動割り当て開始IPアドレスの「ネットワーク部」も併せて変更する必要があります。

ここでは、自動割り当て開始IPアドレスを変更する手順について説明します。

〈変更のしかた〉

1. 本製品の設定画面にアクセスします。
 - 「ネットワーク設定」メニューの「LAN側IP設定」画面を最初に表示します。
2. [DHCPサーバ設定]項目の[割り当て開始IPアドレス]欄に、自動割り当て開始IPアドレスを入力します。
 - ※ 自動割り当て開始IPアドレスのネットワーク部が、本製品のIPアドレスのネットワーク部と同じになるように設定してください。
3. 〈登録して再起動〉をクリックします。
 - 設定した内容が有効になります。

3. クリック

1. 変更する

2. 変更する

ネットワーク設定

- LAN側IP設定
- ブリッジ設定
- RIP設定
- ルーティング設定

無線LAN設定

WAN側設定

システム設定

情報表示

LAN側IP設定
 本体をネットワークに接続するための設定を行います。

登録して再起動 本体IPアドレス/サブネットマスクの設定は再起動後に有効になります。

本体名称/IPアドレス設定

本体名称	RD4E000
IPアドレス	192.168.0.1
サブネットマスク	255.255.255.0

DHCPサーバ設定

DHCPサーバ機能を使用 しない する

割り当て開始IPアドレス	192.168.0.10
割り当て個数	30 個
サブネットマスク	255.255.255.0
リース期間	72 時間
ドメイン名	
デフォルトゲートウェイ	192.168.0.1

DNS代理応答を使用 しない する

プライマリDNSサーバ DNSの代理応答機能を使用する場合は無効となります。

セカンダリDNSサーバ

【DHCPサーバ機能について】
 本製品のDHCPサーバ機能を有効(出荷時の設定)にすると、パソコンが本製品に接続したときに、本製品からIPアドレスを自動的に取得することができます。
 本製品を既存のLANやルータタイプモデムにつなぐ場合、本製品がパソコンに自動で割り当てるIPアドレスの範囲が、既存のネットワーク機器(パソコンなど)の固定で割り当てたIPアドレスと重複しないように設定してください。

【自動割り当て個数について】
 本製品で設定できる自動割り当て可能なIPアドレスの個数は、0(割り当てしない)～128個(無線LANを含む)までです。
 出荷時の割り当て開始IPアドレスとサブネットマスクの設定値の場合、理論上割り当て可能なIPアドレスの個数は、最大254個までですが、128個を超える分については、手動でクライアントに割り当ててください。

5 その他の基本設定

5-5. DHCPサーバ機能を停止するには

本製品をDHCPサーバが存在する既存のLANへの接続や、ルータタイプモデム(※4章 Step5.)のDHCPサーバを使用するときなどは、本製品のDHCPサーバ機能を停止させる必要があります。

〈変更のしかた〉

- 1.本製品の設定画面にアクセスします。
 - 「ネットワーク設定」メニューの「LAN側IP設定」画面を最初に表示します。
- 2.[DHCPサーバ設定]項目の「DHCPサーバ機能を使用」欄で、「しない」のラジオボタンをクリックします。
- 3.〈登録〉をクリックします。
 - DHCPサーバ機能が停止します。



- 4.本製品の[LAN]ポートをDHCPサーバが存在する既存のLANに接続しなおします。
- 5.既存のLANに接続されたパソコンから本製品のLAN側IPアドレス(出荷時の設定：192.168.0.1)を指定して、本製品の設定画面にアクセスできることを確認します。

この章では、

本製品の設定内容保存や初期化、ファームウェアのバージョンアップ、本体MACアドレスを確認する手順について説明しています。必要なときにお読みください。

6-1. 設定内容の確認または保存	66
6-2. 保存された設定の書き込み	67
6-3. 設定を出荷時の状態に戻す	68
Ⓐ <MODE> ボタンを使う	68
Ⓑ 設定画面を使う	70
Ⓒ 「Firm Utility」を使う	71
6-4. ファームウェアをバージョンアップする	73
■ ファームウェアについて	73
■ バージョンアップについてのご注意	73
■ 「Firm Utility」でバージョンアップする前に	74
■ バージョンアップのしかた	74
6-5. 本製品のMACアドレスを確認するには	76

6 保守について

6-1. 設定内容の確認または保存

本製品の設定画面で変更された内容を確認したり、その内容をハイパーテキスト (HTML)形式のファイルに保存できます。

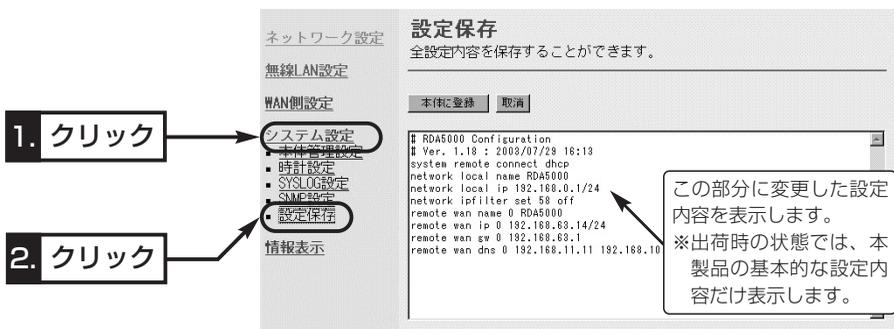
設定を保存しておく、と、不用意な事故によって設定内容が失われたときに利用できます。

〈確認と保存のしかた〉

1. 本製品の設定画面にアクセスして、「システム設定」メニューから「設定保存」をクリックします。

- 「設定保存」画面に、基本的な設定内容と変更された内容の一覧が表示されます。

※テキストボックス内の内容を直接削ったり書き替えたりしてから、保存しないでください。



2. 「設定保存」画面が表示された状態で、WWWブラウザの「ファイル (F)」メニューから、[名前を付けて保存(A)...]をクリックします。

- 「Webページの保存」画面を表示します。

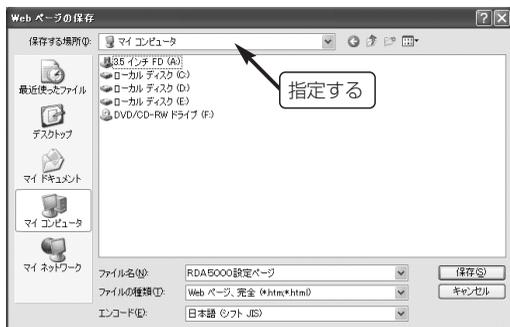
3. [保存する場所(I)]を指定して、任意の名前を[ファイル名(N)]ボックスに入力します。

※「Netscape Navigator」の場合、拡張子を[.htm]か[.html]に変更してください。

4. 「Internet Explorer」の場合、[ファイルの種類(I)]は、「Webページ、完全(*.htm, *.html)」を選択します。

※保存ファイルの漢字コードを選択できる場合は、JISを選択して保存してください。

5. 〈保存(S)〉をクリックすると、指定した場所に設定ファイルが保存されます。



「設定保存」画面でのパスワード表示

SSIDやパスワード、キージェネレータ (暗号化鍵の生成元文字列)の内容を、「設定保存」画面内に暗号化して表示しますので、保存された設定ファイルよりこれらの情報が外部に漏れることはありません。

6-2. 保存された設定の書き込み

6-1章で保存した設定ファイルを本製品の設定画面に書き込む手順を説明します。

＜書き込みのしかた＞

1. 本製品に接続したパソコンから、保存された「htm」の拡張子がついた設定ファイルの上にカーソルを移動して、ダブルクリックします。
 - 「設定保存」画面を表示します。
2. 必要があれば、設定ファイルのテキストボックス内で設定内容の編集が行えます。
3. 「本体に登録」をクリックします。

※編集前に表示されていた本製品のIPアドレスに向けて設定ファイルの内容を転送しますので、内容を編集したときなどは、本製品(転送先)のIPアドレスを設定ファイル編集前のIPアドレスに設定しておく必要があります。



RDA5000設定
ページ.htm

クリック

ネットワーク設定
無線LAN設定
WAN側設定
システム設定
本体設定

設定保存
全設定内容を保存することができます。

本体に登録 取消

本製品のIPアドレスを編集したときは、転送先のIPアドレスが、ここで編集する前の状態に設定されていないと転送できません。

```
# RDA5000 Configuration
# Ver. 1.19 : 2003/07/29 16:13
system remote connect dhcp
network local name RDA5000
network local ip 192.168.0.1/24
network interface eth 192.168
remote wan name 0 RDA5000
remote wan ip 192.168.68.14/24
remote wan gw 192.168.68.1
remote wan dns 0 192.168.11.11 192.168.10.10
```

保存された設定ファイルの内容を表示します。

4. 「本体に登録」をクリックすると、設定ファイルの内容が本製品に書き込まれます。
 - ※設定を書き込んだあと続いて設定を行うときは、設定書き込みのために開いた画面を使用すると誤動作の原因になります。新たに起動したWWWブラウザから、設定画面にアクセスをやりなおすようにしてください。

△注意 本製品で作成した設定ファイルを同じ機種どうしやほかの機種に書き込まないでください。

6 保守について

6-3. 設定を出荷時の状態に戻す

ネットワーク構成を変更するときなど、本製品の設定をはじめからやりなおしたり、既存の設定データをすべて消去したいなど、そのときの状況に応じて次の3通りの方法で設定内容を出荷時の状態に戻す(初期化する)ことができます。

- Ⓐ 〈MODE〉ボタンを使う(※操作するときは、ペンの先などを利用します。)
- Ⓑ 設定画面を使う(☞P70)
- Ⓒ 「Firm Utility」を使う(☞P71)

Ⓐ 〈MODE〉ボタンを使う

この方法で初期化を実行すると、すべての設定項目が出荷時の状態になります。本製品に設定されたIPアドレスが不明な場合など、本製品の設定画面が呼び出せないときに、次の手順で初期化が行えます。

※無線パソコンから初期化操作をする場合は、パソコン側の[SSID]や[暗号化]セキュリティの設定を出荷時の状態に戻してから行ってください。

〈初期化のしかた〉

1. 本製品に接続するDCコネクタを外して、電源を切ります。
2. 本製品に接続するすべてのネットワーク機器を外します。
3. DCコネクタを本製品につないで、電源を入れます。
4. 〈MODE〉ボタンを押しながら、〈RESET〉ボタンだけを短く押し離します。
5. [POWER]ランプと[MODE]ランプが同時点滅に切り替わったら、〈MODE〉ボタンを離します。
 - 「設定初期化」モードに移行して動作を開始します。
 - ※ 移行しないときは、本製品の電源を入れなおすか〈RESET〉ボタン(☞1-2章)を押して、はじめからやりなおしてください。
6. 本製品に有線または無線で接続するパソコンを起動します。
7. WWWブラウザを起動して、本製品の出荷時のIPアドレス(192.168.0.1)を指定します。

【「設定初期化」モードについて】

〈MODE〉ボタンの操作で「設定初期化」モードに移行すると、実際に初期化操作(次ページ手順8.の操作)が行われるまで、一時的に本製品のIPアドレスやSSID、回線種別を出荷時の設定に置き換えます。手順8.の操作をしないで、本製品の電源を再投入すると、元の状態に戻ります。

8. [設定初期化モード]画面が表示されたら、〈初期化実行〉をクリックします。



9. 〈再起動〉をクリックします。



10. 本製品のランプが「設定初期化」モードに以降する前の状態に戻って、「ネットワーク設定」メニューの「LAN側IP設定」画面を表示したら、本製品の初期化が完了です。

- 再起動中は、次の画面を表示します。

再起動しています。しばらくお待ちください。

6 保守について

6-3. 設定を出荷時の状態に戻す(つづき)

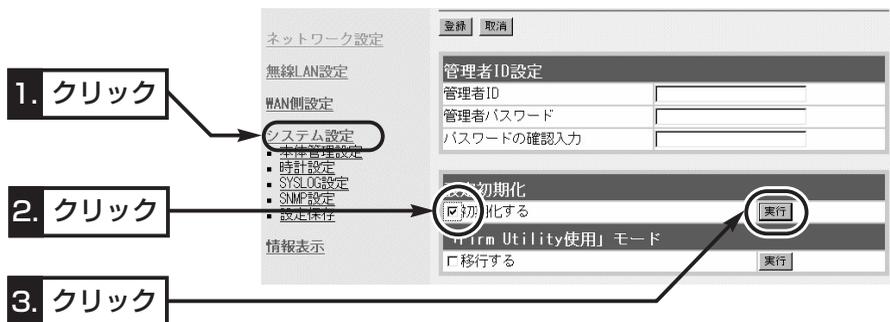
⑧ 設定画面を使う

本製品に設定されたIPアドレスがわかっていて、そのIPアドレスで設定画面にアクセスできるときは、本製品の設定画面を使用してすべての設定を出荷時の状態に戻せます。

〈初期化のしかた〉

初期化は、「本体管理設定」画面から行います。

1. 本製品の設定画面にアクセスして、「システム設定」メニューをクリックします。
 - 「本体管理設定」画面を表示します。
2. [設定初期化]項目で「初期化する」のチェックボックスをクリックして、チェックを入れます。
3. 〈実行〉 をクリックします。



4. 次の画面を表示後、本製品の初期化が完了します。

再起動しています。しばらくお待ちください。

㊦ 「Firm Utility」を使う

「Firm Utility」を使用して初期化する手順について説明します。

「Firm Utility」は、本製品のCDから起動できます。

◆Firm Utilityを使う前に◆

「Firm Utility」を使用して本製品の設定を出荷時の状態に戻すには、使用するパソコンを本製品に有線または無線で通信できる状態にしておく必要があります。

その次に、本製品の「本体管理設定」画面から「Firm Utility使用」モードに切り替えてください。

切り替えないときは、「Firm Utility」を使用して初期化できません。

※「Firm Utility使用」モードに移行後も、本製品の設定内容に変化はありません。

〈初期化のしかた〉

1. 本製品の設定画面にアクセスして、「システム設定」メニューをクリックします。
 - 「本体管理設定」画面を表示します。
2. 「Firm Utility使用モード」項目で「移行する」のチェックボックスをクリックして、チェックを入れます。
3. 「実行」をクリックします。



4. 右の画面を表示して「Firm Utility使用」モードで動作を開始します。

- 「Firm Utility使用」モードで動作中は、前面パネルの[POWER]と[MODE]ランプが交互点滅を繰り返します。

「Firm Utility使用」モードに移行しました。
通常動作は全て停止しています。
通常モードに戻るには本体を再起動して下さい。

【「Firm Utility使用」モードでのセキュリティについて】

本製品の「無線LAN設定」メニュー「暗号化設定」画面で、暗号化セキュリティが設定されている場合は、「Firm Utility使用」モードで動作しているときも有効です。

このような場合、パソコン側に暗号化セキュリティが設定されていないと、無線パソコンから「Firm Utility」を使うことができません。

6 保守について

6-3. 設定を出荷時の状態に戻す

◎ 「Firm Utility」を使う 〈初期化のしかた〉 (つづき)

5. 本製品のCDをご使用のCDドライブに挿入します。

- CDドライブのAuto Run機能が動作して、メニュー画面を表示します。

6. 〈ファームウェア ユーティリティ〉 をクリックします。

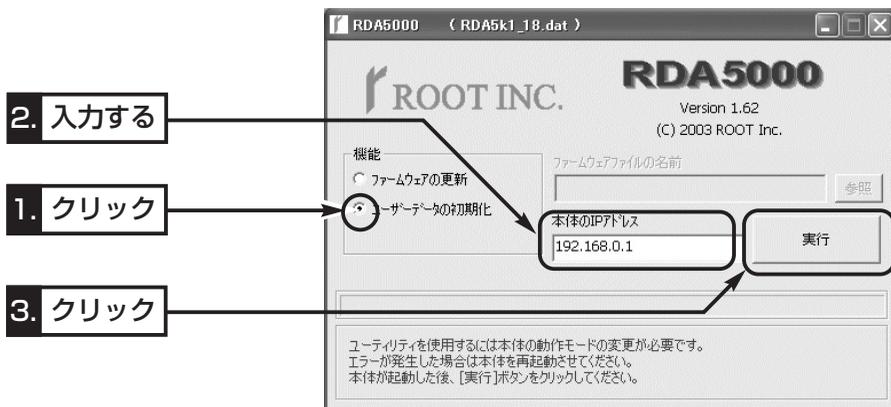
- 「Firm Utility」が起動します。

7. [ユーザーデータの初期化]のラジオボタンをクリックします。

[本体のIPアドレス]のテキストボックスに本製品のLAN側IPアドレスを入力してから、〈実行〉 をクリックします。

8. 「ユーザーデータの初期化が完了しました。」というメッセージが「Firm Utility」の画面に表示されたら、本製品の初期化が完了です。

※設定は、初期化する前の設定画面を閉じて、新しく開きなおした設定画面から設定を行ってください。



△注意 「Firm Utility」実行中は、「Firm Utility」を終了したり、本製品の電源を切ったりしないでください。
途中で作業を中断すると、データの消失や誤動作の原因になりますのでご注意ください。
画面に「……が完了しました。」と表示されるまでお待ちください。

6-4. ファームウェアをバージョンアップする

「Firm Utility」を使用してバージョンアップする手順について説明します。

「Firm Utility」は、本製品のCDから起動します。

■ ファームウェアについて

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

このプログラムは、機能の拡張や改良のため、バージョンアップを行うことがあります。バージョンアップの作業を行う前に、本製品の設定画面にアクセスして、次のフレーム内に表示するバージョン情報を確認してください。

バージョンアップをすると、機能の追加など、本製品を最良の状態に保つことができます。



■ バージョンアップについてのご注意

ファームウェア転送時のエラー防止のため、「Firm Utility」を使用するパソコン(有線または無線で本製品に接続できること)を本製品と1対1で接続してください。

本製品とパソコンを有線で接続できる環境がある場合は、できるだけ有線で接続することをおすすめします。

- 無線で本製品に接続する場合は以下のことを守ってください。

Ethernetケーブルを本製品に接続しているときは、取り外してください。

無線通信の距離は、1m以内にしてください。

- ◆記載する操作の結果については、自己責任の範囲となりますので、次のことを守って作業を始めてください。

◎「Firm Utility」は、本製品に付属のCDに収録されたもの以外を使用しないでください。

◎本製品の設定ファイルや弊社ホームページ(<http://www.root-hq.com/>)より提供されるアップデート用ファームウェアファイルを、本製品以外の機器に組み込んだり、改変や分解したことによる障害、および本製品の故障、誤動作、不具合、破損、データの消失あるいは停電などの外部要因により通信、通話などの機会を失ったために生じる損害や逸失利益または第三者からのいかなる請求についても弊社は一切その責任を負いかねますのであらかじめご了承ください。

6 保守について

6-4. ファームウェアをバージョンアップする(つづき)

■「Firm Utility」でバージョンアップする前に

「Firm Utility」を使用してファームウェアをバージョンアップするには、使用するパソコンを本製品に有線または無線で通信できる状態にしておく必要があります。

その次に、本製品の「本体管理設定」画面から「Firm Utility使用」モードに切り替えてください。

切り替えないときは、「Firm Utility」を使用してファームウェアをバージョンアップできません。

※「Firm Utility使用」モードに移行しただけでは、バージョンアップできません。

■バージョンアップのしかた

1. 本製品の設定画面にアクセスして、「システム設定」メニューをクリックします。
 - 「本体管理設定」画面を表示します。
2. 「Firm Utility使用モード」項目で「移行する」のチェックボックスをクリックして、チェックを入れます。
3. 「実行」をクリックします。



4. 右の画面を表示して「Firm Utility使用」モードで動作を開始します。

- 「Firm Utility使用」モードで動作中は、前面パネルの[POWER]と[MODE]ランプが交互点滅を繰り返します。

「Firm Utility使用」モードに移行しました。
通常動作は全て停止しています。
通常モードに戻るには本体を再起動して下さい。

【バージョンアップにかかる時間について】

ファームウェアのデータファイルを本製品に転送して再起動が完了するまでの時間の目安です。

- 転送=30~60秒
- 再起動=10秒

5.本製品のCDをご使用のCDドライブに挿入します。

- CDドライブのAuto Run機能が動作して、メニュー画面を表示します。

6.〈ファームウェア ユーティリティ〉をクリックします。

- 「Firm Utility」が起動します。

7.[ファームウェアの更新]のラジオボタンをクリックします。

ダウンロードした本製品の新しいファームウェアファイル(拡張子：dat)へのリンク先を[ファームウェアファイルの名前]のテキストボックスに直接入力するか、〈参照〉をクリックして選択します。

8.[本体のIPアドレス]のテキストボックスに本製品のLAN側IPアドレスを入力してから、〈実行〉をクリックします。

9.「ファームウェアの更新が完了しました。」というメッセージが「Firm Utility」の画面に表示されたら、本製品のバージョンアップが完了です。

※バージョンアップ完了後、本製品の設定画面にアクセスできないときは、本製品の電源を入れなおしてから、再度アクセスしてください。

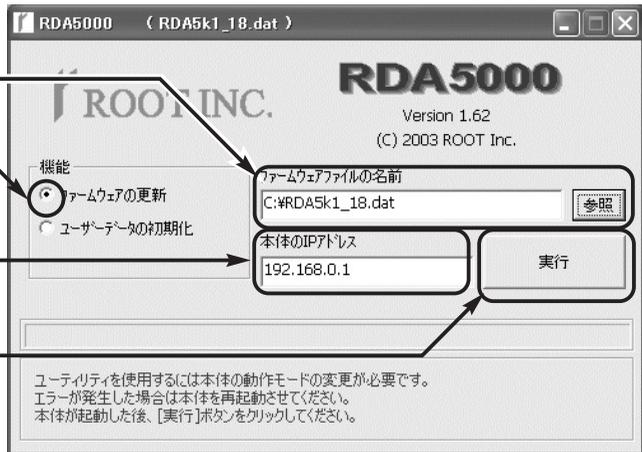


2. 入力する

1. クリック

3. 入力する

4. クリック



6 保守について

6-5. 本製品のMACアドレスを確認するには

ご契約のプロバイダーにMACアドレスの申請および登録が必要な場合など、次の手順を参考に本製品のMACアドレスを確認してください。

※このMACアドレスは、本製品の底面パネルに貼られたシリアルシールにも12桁で記載されています。(はじめにP. v)

〈確認のしかた〉

1. 本製品の設定画面にアクセスして、「情報表示」メニューから「ネットワーク情報」をクリックします。
 - 「ネットワーク情報」画面を表示します。
2. [本体MACアドレス]項目に本製品のMACアドレスを表示します。

The screenshot shows the 'ネットワーク情報' (Network Information) screen. On the left, a navigation menu includes 'ネットワーク設定', '無線LAN設定', 'WAN側設定', 'システム設定', '情報表示', and 'ネットワーク情報'. Step 1 points to 'ネットワーク情報' in the menu. Step 2 points to the 'ネットワーク情報' item in the '情報表示' dropdown. Step 3 points to the '本体MACアドレス' field, which displays '00-90-C7-69-00-9A'. The main content area shows a table of network interfaces and bridge port information.

ネットワーク	インターフェイス	IPアドレス	サブネットマスク
local		192.168.0.1	255.255.255.0

ブリッジポート情報	
ポート	通信情報
	状況 通信中

本体MACアドレス
00-90-C7-69-00-9A

※無線AP間通信機能を[IEEE802.11g]規格または[IEEE802.11a]規格の無線LANで使用する場合、登録に必要な「BSSID」を確認するには、「無線LAN設定」メニューから、無線AP間通信機能で使用する無線LAN規格の「AP間通信設定」画面をクリックして、確認(P. 3-4章Step.2.)してください。

「ネットワーク情報」画面に表示されるMACアドレスとは異なりますのでご注意ください。

この章では、

おもなトラブルの対処方法、設定画面の構成、設定項目の初期値、仕様や定格について説明しています。

7-1.困ったときは	78
■ CDをドライブに挿入後、メニュー画面を表示しない	78
■ [POWER]ランプが点灯しない	78
■ [LAN]ランプが点灯しない	78
■ パソコンのIPアドレスを自動取得できない	78
■ [WIRELESS]ランプが点灯しない	79
■ [WIRELESS]ランプが点灯しているが通信できない	79
■ [WAN]ランプが点灯しない	80
■ インターネットに接続できない	80
■ WAN側から本製品にアクセスできない	81
7-2.設定項目の初期値一覧	82
7-3.設定画面の構成について	84
7-4.機能一覧	86
7-5.各種ポート仕様	86
7-6.定格	87
■ 一般仕様	87
■ 有線部	87
■ 無線部【5.2GHz帯・54Mbps(IEEE802.11a準拠)】	88
■ 対応無線LANカードについて(5.2GHz帯/IEEE802.11a)	88
■ 無線部【2.4GHz帯・54Mbps(IEEE802.11g準拠)】	89
■ 対応無線LANカードについて(2.4GHz帯/IEEE802.11g)	89
■ 無線部【2.4GHz帯・11Mbps(IEEE802.11b準拠)】	90
■ 対応無線LANカードについて(2.4GHz帯/IEEE802.11b)	90
7-7.故障のときは	91
7-8.用語解説	92

7 ご参考に

7-1. 困ったときは

下記の〈症状〉でお困りの場合の対処方法について説明しています。

〈症状〉CDをドライブに挿入後、メニュー画面を表示しない

〈原因〉CDのAuto Run機能が動作しない

対処：CDに収録されている「AutoRun.exe」を直接ダブルクリックする

〈症状〉[POWER]ランプが点灯しない

〈原因1〉ACアダプターが本製品に接続されていない

対処：ACアダプターおよびDCプラグの接続を確認する

〈原因2〉ACアダプターをパソコンなどの電源と連動したコンセントに接続している

対処：本製品のACアダプターを壁などのコンセントに直接接続する

〈症状〉[LAN]ランプが点灯しない

〈原因1〉Ethernetケーブルが本製品と正しく接続されていない

対処：Ethernetケーブルを[LAN]ポートに接続している場合は、
[PC/HUB]スイッチの設定を確認する

〈原因2〉パソコンまたはHUBの電源が入っていないか、EthernetケーブルでHUB
のカスケードポートと接続している

対処：パソコンまたはHUBの電源を確認して、付属のEthernetケーブル
でHUBのクロスポートと接続する

〈原因3〉ルータタイプモデムの電源が入っていない、または接続を間違えている

対処：ルータタイプモデムの電源および接続を確認する

〈原因4〉パソコンのEthernetカードが機能していない

対処：パソコンを既存の有線LANやブロードバンドモデムに直接接続す
るなどして、Ethernetカードが正常動作していることを確認する

〈原因5〉使用するEthernetカードを「使用不可」に設定している

対処：Windowsのデバイスマネージャで、使用する「ネットワークアダプ
タ」のプロパティから「使用不可」にしていないことを確認する

〈症状〉パソコンのIPアドレスを自動取得できない

〈原因1〉ルータタイプモデムと本製品のDHCPサーバ機能が設定された状態で接続
したため、本製品とのあいだでIPアドレスの競合が起きている

対処：本製品のDHCPサーバ機能を「OFF」(4章 Step4-1.)にする

〈原因2〉パソコンを起動したあとで、本製品およびルータタイプモデムの電源を入
れた

対処：本製品およびルータタイプモデムの電源を入れた状態で、パソコン
を再起動する、または本書2-5章を参考にIPアドレスを再取得させ
る

〈症状〉パソコンのIPアドレスを自動取得できない(つづき)

〈原因3〉EthernetカードのIPアドレスを固定に設定している

対処：パソコンのIPアドレスの設定を「IPアドレスを自動的に取得」に変更して確認する

〈原因4〉パソコンに装着された無線LANカードとEthernetカードが同時に動作している

対処：どちらかのカードを取り外すか、OSのデバイスマネージャなどで、どちらかを「使用不可」に設定する

〈症状〉 [WIRELESS]ランプが点灯しない

〈原因1〉パソコンに装着する無線LANカードが機能していない

対処：無線LANカードのドライバーが正しくインストールされていることを確認する

〈原因2〉通信終了後、無通信状態が1～2分以上続いた

対処：本製品に再度アクセスしたとき点灯することを確認する

〈原因3〉パソコンを起動したあとで、本製品およびルータタイプモデムの電源を入れた

対処：本製品およびルータタイプモデムの電源を入れた状態で、パソコンを再起動する

〈原因4〉無線LANカードの無線通信モードがアドホックになっている

対処：無線LANカードの無線通信モードをインフラストラクチャに変更する

〈原因5〉SSID(もしくはESSID)の設定が異なっている

対処：本製品と無線パソコンのSSID(もしくはESSID)の設定を確認する

〈原因6〉無線AP間通信機能を使用する場合で、通信相手の「BSSID」が登録されていない。

対処：互いが使用する本製品の無線LAN規格の画面に、通信相手の「BSSID」が登録されているか、正しく入力されているかどうかを確認する

〈原因7〉暗号化認証モードが異なるタイプである

対処：無線LANカードまたは本製品の認証モードを同じに設定する

〈原因8〉本製品の自動検索接続(ANY)機能を「無効」に設定している

対処：「無線LAN設定」画面で[ANYを拒否]を「しない」に設定する

〈症状〉 [WIRELESS]ランプが点灯しているが通信できない

〈原因1〉暗号化セキュリティの設定が異なっている

対処：本製品と無線パソコンの暗号化セキュリティの設定を確認する

〈原因2〉MACアドレスセキュリティーを使用している

対処：無線LANカードのMACアドレスを本製品に登録する

7 ご参考に

7-1. 困ったときは(つづき)

〈症状〉 [WAN]ランプが点灯しない

- 〈原因1〉ブリッジタイプモデムまたはメディアコンバーターの電源が入っていない
対処：電源が入っていることを確認する
- 〈原因2〉本製品とブリッジタイプモデムまたはメディアコンバーターが接続されていない
対処：本製品の[WAN]ポートとブリッジタイプモデムまたはメディアコンバーターをEthernetケーブルで接続する
- 〈原因3〉本製品とブリッジタイプモデムまたはメディアコンバーターを接続しているEthernetケーブルの結線方式(ストレート、クロス)がプロバイダーの指定するケーブルと異なる
対処：プロバイダーが指定(ブリッジタイプモデムまたはメディアコンバーターに付属)するケーブルを使用する

〈症状〉 インターネットに接続できない

- 〈原因1〉プロバイダーに契約をしたが、工事完了または使用開始の通知がない
対処：契約または工事の完了日をご契約のプロバイダーに確認する
- 〈原因2〉使用する機器のMACアドレスを登録していない
対処：登録が必要なプロバイダーの場合は、本製品のMACアドレスを登録する
すでに登録しているMACアドレスがある場合は、そのMACアドレスを「WAN側詳細設定」画面の[WAN側MACアドレス変更機能]欄に入力する
- 〈原因3〉ブリッジタイプモデムまたはメディアコンバーターをご使用の場合で、ご契約のプロバイダーへの接続方法を間違えている
対処：該当する接続方法(PPPoE、DHCPクライアント、固定IPアドレス)を、ご契約のプロバイダーに確認する
- 〈原因4〉モデムタイプの設定(ブリッジ/ルータ選択)を間違えている
対処：4章(本書)のStep2.を参考に、ご使用のモデムタイプを確認する
- 〈原因5〉ブロードバンドモデムまたはメディアコンバーターが本製品と正しく接続されていない
対処：ブリッジタイプモデムの場合は、本製品の[WAN]ポートと接続するルータタイプモデムまたはメディアコンバーターの場合は、本製品の[LAN]ポートと接続する
- 〈原因6〉回線種別が正しく選択されていない
対処：4章(本書)のStep3.～4.を参考に選択を確認する

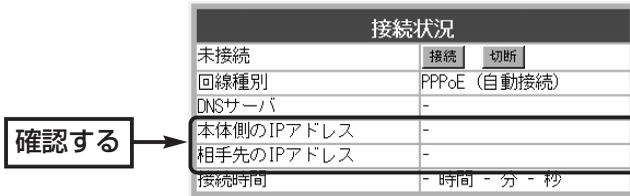
〈症状〉 インターネットに接続できない(つづき)

〈原因7〉 [WAN](プロバイダー)側からIPアドレスが取得できていない

対処：下記の手順にしたがって、IPアドレスを確認する

確認できないときは、本製品とブリッジタイプモデムまたはメディアコンバーターの接続を確認する

[WAN]側から取得したIPアドレスを確認するときは、本製品の設定画面にアクセスして、[接続状況]に表示される内容を確認する



〈原因8〉 〈切断〉 ボタンで、回線を強制的に切断している

対処：[接続状況]に表示される 〈接続〉 ボタンで、回線を強制的に接続する

〈原因9〉 DNSサーバのIPアドレスが正しく指定されていない

対処：「ネットワーク設定」メニューまたは「WAN側設定」メニューでDNSサーバの設定を確認する

〈症状〉 WAN側から本製品にアクセスできない

〈原因〉 出荷時に登録されているIPフィルターでWAN側から本製品へのアクセスを遮断しているため

△注意 IPフィルターの変更によるセキュリティの低下で生じる結果については、弊社では一切その責任を負いかねますので、あらかじめご了承ください。

7 ご参考に

7-2. 設定項目の初期値一覧

本製品の設定画面について、設定項目の初期値を示します。

■「ネットワーク設定」メニュー

「LAN側IP設定」画面

本体名称/IPアドレス設定

- 本体名称：RDA5000
- IPアドレス：192.168.0.1
- サブネットマスク：255.255.255.0

DHCPサーバ設定

- DHCPサーバ機能を使用：する
- 割り当て開始IPアドレス：192.168.0.10
- 割り当て個数：30個
- サブネットマスク：255.255.255.0
- リース期間：72時間
- デフォルトゲートウェイ：192.168.0.1
- DNS代理応答を使用：する

「RIP設定」画面

RIP設定

- RIP設定：RIP
- LAN側RIP動作：使用しない
- WAN側RIP動作：使用しない

■「無線LAN設定」メニュー

「セキュリティ設定」画面

RADIUS設定

- RADIUS機能を使用：しない
- サーバのポート番号：

プライマリ：1812
セカンダリ：1812

- 再認証間隔(分)：120

無線端末間通信設定

- 無線端末間通信を禁止：しない

MACアドレスセキュリティ設定

- MACアドレスセキュリティを使用：しない

「暗号化設定」画面[802.11g/a]

暗号化設定

- 認証モード：両対応
- 暗号化方式：なし
- ファクター：0
- キーID：1
- キーの自動変更を使用：する

キー値

- 入力モード：16進数
- 1~4：00-00-00-00-00

「ブリッジ設定」画面

ブリッジ設定

- スパニングツリー機能を使用：しない
 - ブリッジ優先度(Bridge Priority)：32768
 - エージングタイム(Aging Time)：300
 - マックスエイジ(Max Age)：20
 - ハロータイム>Hello Time)：2
 - 転送遅延(Forward Delay)：15
 - パスコスト(Path Cost)：
- 有線LAN：100
無線[802.11g]：200
無線[802.11a]：200
- ポート優先度(Port Priority)：
- 有線LAN：128
無線[802.11g]：128
無線[802.11a]：128

「無線LAN設定」画面

無線LAN設定[802.11g]

- IEEE802.11gを使用：する
- SSID：** (半角大文字LG)
- SSIDの確認入力：** (半角大文字LG)
- ANYを拒否：しない
- チャンネル：11(2462MHz)
- Rts/Ctsスレッシュホールド：無し
- 11g保護機能：無効
- パワーレベル：高
- 接続端末制限：255

無線LAN設定[802.11a]

- IEEE802.11aを使用：する
- SSID：** (半角大文字LG)
- SSIDの確認入力：** (半角大文字LG)
- ANYを拒否：しない
- チャンネル：34(5170MHz)
- Rts/Ctsスレッシュホールド：無し
- パワーレベル：高
- 接続端末制限：255

7-2. 設定項目の初期値一覧(つづき)

■ 「WAN側設定」メニュー

「WAN側設定」画面

- 回線種別：接続しない

「WAN側詳細設定」画面

共通詳細設定

- WAN側通信速度：自動
- WAN側MACアドレス変更機能：デフォルト
- ステルスモードを使用：しない

「アドレス変換設定」画面

アドレス変換設定

- アドレス変換：する

パススルー設定

- PPTPパススルーを使用：する

「IPフィルタ設定」画面

不正アクセス検知機能設定

- 不正アクセス検知機能設定を利用：しない
- 検知結果を出力：する
- 検知時間：1分
- 検知回数：100回

現在の登録(IPフィルタ)

- 57番(FTPをデフォルトで通過させる)
- 58番(WAN側からの不正アクセス防止)
- 59、60番(Windowsのアプリケーションを外部からリモートコントロールされる危険性を防止)
- 61～64番(Windowsが行う定期的な通信によって起こる「意図しない自動接続」を防止)

「PPPoE」または「PPPoE複数固定IP」を設定時、表示される設定項目の初期値一覧

■ 「WAN側設定」メニュー

「WAN側設定」画面

- 認証プロトコル：相手に合わせる

「WAN側詳細設定」画面

PPPoE詳細設定

- 接続設定：自動
- 自動切断タイマー(分)：10
- MSS制限値：1322

■ 「システム設定」メニュー

「時計設定」画面

自動時計設定

- 自動時計設定を使用：する
- NTPサーバ1 IPアドレス：133.100.9.2
- アクセス時間間隔：1日

「SYSLOG設定」画面

SYSLOG設定

- DEBUGを使用：しない
- INFOを使用：しない
- NOTICEを使用：する
- ファシリティ：1

「SNMP設定」画面

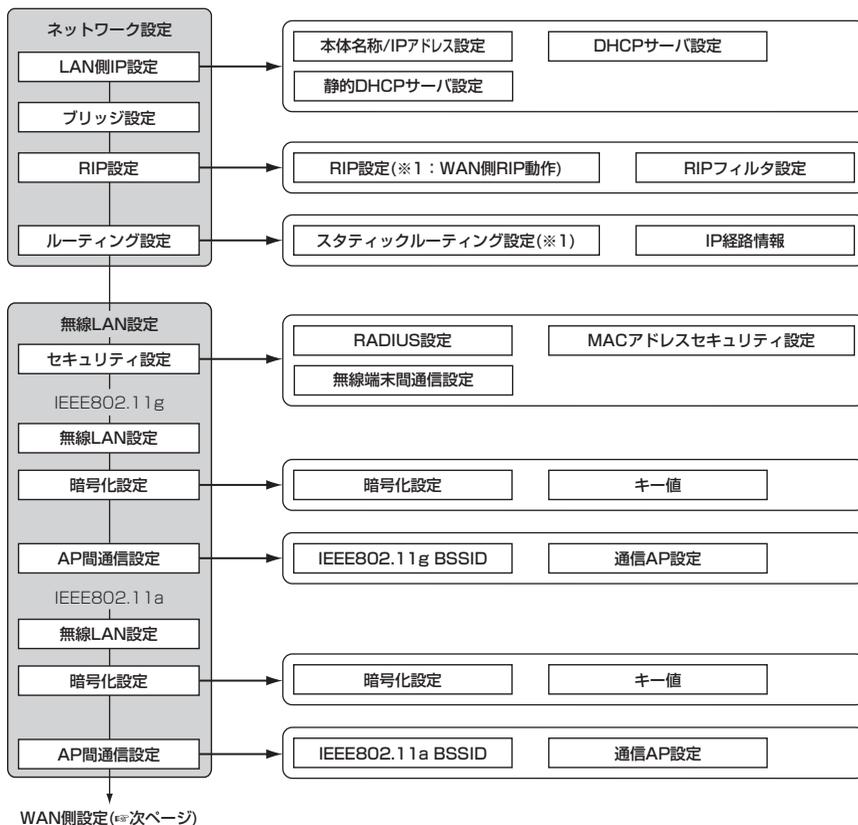
SNMP設定

- SNMPを使用：する
- コミュニティID(GET)：public

7 ご参考に

7-3. 設定画面の構成について

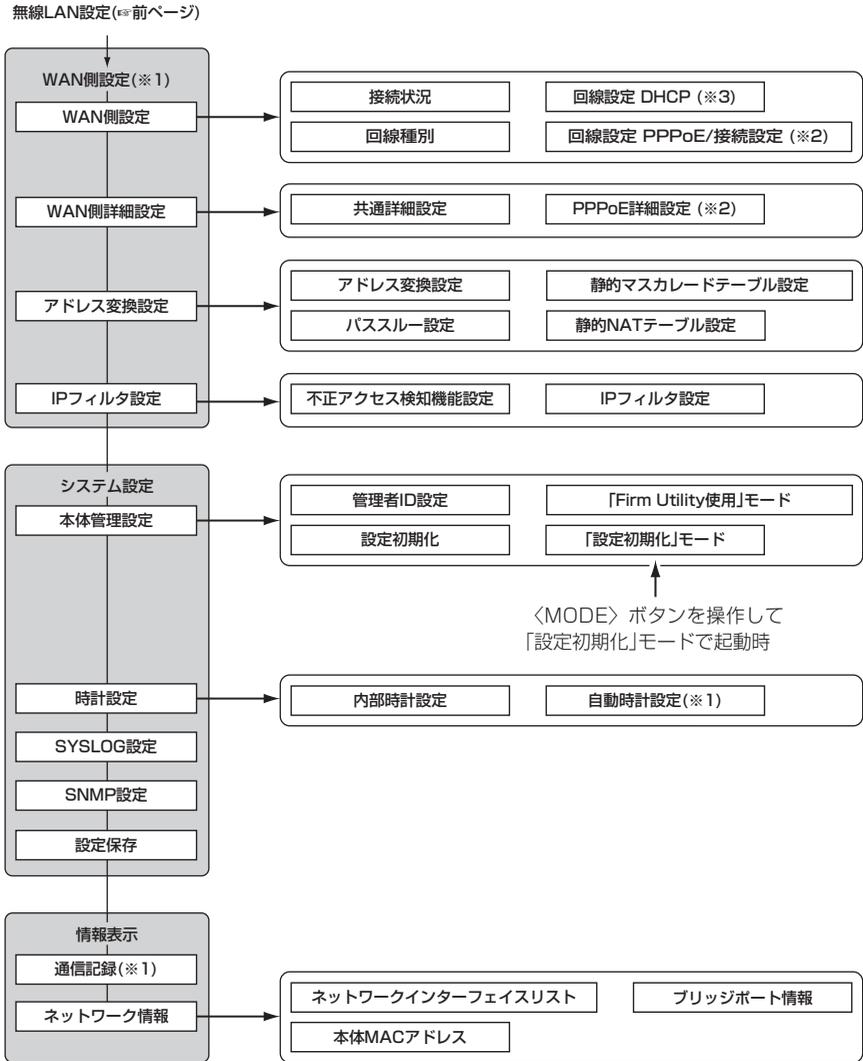
WWWブラウザに表示される本製品の設定画面の構成について説明しています。



■ は、各メニューを示します。

※1. 回線種別で、「接続しない」(出荷時の設定)に設定するとき無効な機能

7-3. 設定画面の構成について(つづき)



□ は、各メニューを示します。

- ※1. 回線種別で、「接続しない」(出荷時の設定)に設定するとき無効な機能
- ※2. 回線種別で、「PPPoE」、「PPPoE複数固定IP」を設定したとき表示します。
- ※3. 回線種別で、「DHCP」を設定したとき表示します。

7 ご参考に

7-4. 機能一覧

■ 無線LAN機能

- IEEE802.11a(54Mbps) 無線LAN
- IEEE802.11b(11Mbps) 無線LAN
- IEEE802.11g(54Mbps) 無線LAN
- 11g保護機能(IEEE802.11g)
- アクセスポイント機能
- ローミング機能
- SSID(Service Set-Identifier)
- MACアドレスセキュリティー
- ANY端末接続拒否機能
- 無線AP間通信機能(IEEE802.11a/g)
- 無線端末間通信禁止機能
- 無線暗号化セキュリティー
WEP RC4(Wired Equivalent Privacy)
OCB AES(Offset Code Book Advanced Encryption Standard)
- 暗号化認証
(オープンシステム/シェアードキー)
- IEEE802.1x認証
- 負荷分散機能

■ ルータ機能

- 自動接続/自動切断機能(「PPPoE」または「PPPoE複数固定IP」設定時)
- 各種接続制限機能
- PPPoE、PPPoE複数固定IP、DHCP固定IP接続方式に対応
- ルーティングプロトコル
TCP/IP(RIP、RIP2、スタティック)
- スタティックルーティング機能(WAN-LAN間)
- IPフィルタ機能
- スパニングツリー機能
- RIP機能(RIP2対応)
- 静的IPマスカレード
- NAT/IPマスカレード
- DMZ機能
- DNS代理応答機能
- DHCPサーバ機能(LAN側)
- DHCPスタティック機能
- 不正アクセス検知機能設定
- PPTPパススルー機能

■ ネットワーク管理機能

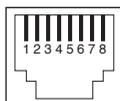
- SYSLOG
- SNMP

■ その他

- 内部時計設定
- 内部時計自動設定
- WWWメンテナンス
- ファームウェアのバージョンアップ
- TELNETメンテナンス
- 管理者ID設定

7-5. 各種ポート仕様

■ [LAN/WAN]ポート(RJ-45型)



- | | |
|---------|--------------|
| 1.送信(+) | 2.送信(-) |
| 3.受信(+) | 4.~5.DC電源(+) |
| 6.受信(-) | 7.~8.Ground |

※4.~5.、7.~8.番ピンは、Ethernet電源供給ユニット接続時に使用します。

7-6. 定格

■ 一般仕様

- 入力電圧 : DC7.5V標準(DC7.125~7.825V)
ACアダプター(付属品)は、AC100V±5%
- 消費電流 : 1.2A(最大)
- 接地方式 : マイナス接地
- 使用環境 : 温度0~+55°C、湿度5~95%(結露状態を除く)
- 外形寸法 : 230(W)×38(H)×167(D)mm(突起物を除く)
- 重量 : 約780g(付属品を除く)
- 適合規格 : クラスA情報技術装置(VCCI)

■ 有線部

● インターフェイス :

[WAN]部 : [Ethernet]ポート(RJ-45型)×1
 ※IEEE802.3/10BASE-T準拠
 ※IEEE802.3u/100BASE-TX準拠

[有線LAN]部 : [Ethernet]ポート(RJ-45型)×1
 ※極性反転スイッチ有り
 ※IEEE802.3/10BASE-T準拠
 ※IEEE802.3u/100BASE-TX準拠

[無線LAN]部 : miniPCI(Type III)カード×2

[ユーザー]部 : 状態表示ランプ(POWER、MODE、WAN **LINK/ACT**、LAN **LINK/ACT**、WIRELESS **1 / 2**)、[HUB/PC]スイッチ、〈MODE〉ボタン、〈RESET〉ボタン

- 適用回線 : CATV、xDSL、FTTH、ローカル
- 通信速度 : [WAN]部 : 10/100Mbps(自動切り替え/全二重)
[LAN]部 : 10/100Mbps(自動切り替え/全二重)

※定格・仕様・外観等は改良のため予告なく変更する場合があります。

7 ご参考に

7-6. 定格(つづき)

■ 無線部【5.2GHz帯・54Mbps(IEEE802.11a準拠)】

- 国際規格：IEEE802.11a準拠
- 国内規格：ARIB STD-T71
- 通信方式：単信方式
- 電送方式：直交周波数分割多重方式(OFDM)
- 変調方式：OFDM-BPSK、QPSK、16QAM、64QAM
- 使用周波数範囲：5150～5250MHz(5.2GHz帯)
- チャンネル数：全4ch
- 通信速度：自動、54/48/36/24/18/12/9/6Mbps
- 最大伝送距離：屋内(見通し)：約30m以内(54Mbps通信時)
※電波法により、屋内使用に限定されます。
- グループ通信：SSID(ANY拒否機能搭載)
- 外部アンテナ：ダイバーシティーアンテナ
- セキュリティ：WEP(RC4)：64(40)/128(104)/152(128)ビット
OCB AES：128(128)ビット
MACアドレス登録
- 送信出力：10mW/MHz以下
- 受信感度：-65dBm以下(54Mbps)
※フレームエラーレート=10%
- 復調方式：OFDM復調
- 対応機種：PC/AT互換機(DOS/V)

※最大伝送距離は、通信速度や環境によって異なります。

※伝送距離は、通信速度や環境によって異なります。

■ 対応無線LANカードについて(5.2GHz帯/54Mbps)

本製品と無線で通信を行うパソコンに装着する5.2GHz帯(IEEE802.11a)無線LAN製品は、弊社推奨のものをご使用ください。

(2003年04月現在)

■ 無線部【2.4GHz帯・54Mbps(IEEE802.11g準拠)】

- 国際規格：IEEE802.11g準拠
- 国内規格：ARIB STD-T66
- 通信方式：単信方式
- 電送方式：直交周波数分割多重方式(OFDM)
- 変調方式：OFDM-BPSK、QPSK、16QAM、64QAM
- 使用周波数範囲：2400～2483.5MHz(2.4GHz帯)
- チャンネル数：全13ch
- 通信速度：自動、54/48/36/24/18/12/9/6Mbps
- 最大伝送距離：屋内(見通し)：約30m以内(54Mbps通信時)
屋外(見通し)：約30m以内(54Mbps通信時)
- グループ通信：SSID(ANY拒否機能搭載)
- 外部アンテナ：ダイバーシティーアンテナ
- セキュリティ：WEP(RC4)：64(40)/128(104)/152(128)ビット
OCB AES：128(128)ビット
MACアドレス登録
- 送信出力：10mW/MHz以下
- 受信感度：-62dBm以下(54Mbps)
※フレームエラーレート=10%
- 復調方式：OFDM復調
- 対応機種：PC/AT互換機(DOS/V)

※最大伝送距離は、通信速度や環境によって異なります。

※定格・仕様・外観等は改良のため予告なく変更する場合があります。

■ 対応無線LANカードについて(2.4GHz帯/54Mbps)

本製品と無線で通信を行うパソコンに装着する2.4GHz帯(IEEE802.11g)無線LAN製品は、弊社推奨のものをご使用ください。

(2003年04月現在)

7 ご参考に

7-6. 定格(つづき)

■ 無線部【2.4GHz帯・11Mbps(IEEE802.11b準拠)】

- 国際規格：IEEE802.11b準拠
- 国内規格：ARIB STD-T66
- 通信方式：単信方式
- 電送方式：直接スペクトラム拡散
- 変調方式：DBPSK、DQPSK、CCK/バーガー符号
- 使用周波数範囲：2400～2483.5MHz(2.4GHz帯)
- チャンネル数：全13ch
- 通信速度：自動、11/5.5/2/1Mbps
- 最大伝送距離：屋内(見通し)：約30m以内(11Mbps通信時)
屋外(見通し)：約70m以内(11Mbps通信時)
- グループ通信：SSID(ANY拒否機能搭載)
- 外部アンテナ：ダイバーシティーアンテナ
- セキュリティ：WEP(RC4)：64(40)/128(104)/152(128)ビット
OCB AES：128(128)ビット
MACアドレス登録
- 送信出力：10mW/MHz以下
- 受信感度：-76dBm以下(11Mbps)
※フレームエラーレート=8%
- 復調方式：デジタル復調(マッチドフィルター方式)
- 対応機種：PC/AT互換機(DOS/V)

※最大伝送距離は、通信速度や環境によって異なります。

※定格・仕様・外観等は改良のため予告なく変更する場合があります。

■ 対応無線LANカードについて(2.4GHz帯/11Mbps)

本製品と無線で通信を行うパソコンに装着する2.4GHz帯(IEEE802.11b)無線LAN製品は、弊社推奨のものをご使用ください。

(2003年04月現在)

7-7. 故障のときは

●保証書について

保証書は販売店で所定事項(お買い上げ日、販売店名)を記入のうえお渡しいたします
ので、記載内容をご確認いただき、大切に保管してください。

●修理を依頼されるとき

取扱説明書にしたがって、もう一度、本製品とパソコンの設定などを調べていただき、
それでも具合の悪いときは、次の処置をしてください。

保証期間中は

お買い上げの販売店にご連絡ください。

保証規定にしたがって修理させていただきますので、保証書を添えてご依頼ください。

保証期間後は

お買い上げの販売店にご連絡ください。

修理することにより機能を維持できる製品については、ご希望により有料で修理させて
いただきます。

●アフターサービスについてわからないときは

お買い上げの販売店またはサポート窓口にお問い合わせください。

7-8. 用語解説

ADSL(Asymmetric Digital Subscriber Line)

加入者電話回線を使用して数Mbps～数十Mbpsのデジタル伝送を行う通信方式です。

基本的に常時接続で、データの送信と受信で通信速度が違い受信側が高速となっています。ADSLでは従来の音声通話とは違った周波数を用いるため電話局の交換機を使用できず、電話局側にもADSLモデムを設置する必要があります。

ADSLモデム

パソコンやルータをADSL回線に接続するために使用する通信機器。

AES(Advanced Encryption Standard)

無線LANの通信を暗号化して送受信する次世代の暗号化方式で、ラウンド変換を繰り返し実行することで、安全性を確保します。無線LANカードによる通信の盗聴を防止できます。

BSSID(Basic Service Set-Identifier)

無線LANをMAC層で識別するためのIDです。本製品の無線AP間通信機能で使用しています。

CATV(Cable Television)

電波ではなく銅線などの物理的な線を使用したテレビ放送を家庭に配信する仕組み。電波よりもチャンネル数が多いため、通常のテレビ放送以外にCATV会社が番組を独自に配信したり、衛星放送を配信していることもある。この放送用のチャンネルを使用してインターネット接続サービスを行うCATVの会社があり、このサービスをCATVインターネットサービスという。

DHCPサーバ

DHCP(Dynamic Host Configuration Protocol) は、TCP/IPというネットワーク上で、クライアントがサーバから必要な情報を自動的に取得するプロトコルです。DHCPサーバは、ネットワーク情報として、“IPアドレス”、“デフォルトゲートウェイ”、“ドメイン名”などを管理しています。DHCPサーバ機能を持つ本製品は、DHCPクライアント(パソコン)が起動すると、IPアドレスやデフォルトゲートウェイ、DNSアドレスなどを割り振ります。

DMZ(De-Militarized Zone)

プライベートネットワーク内で、ファイアウォールで外部ネットワークからも内部ネットワークからも隔離された領域。

DNS(Domain Name System)

TCP/IPネットワークにおける名前解決サービスのことです。

DNSにしたがって、ドメイン名サーバにコンピューター名やドメイン名を登録して、ドメイン名サービスを提供しています。ドメイン名サービスを利用すると、IPアドレスなどの数字ではなく、分かりやすいドメイン名やホスト名で、目的のサイトを指定できます。

ESS-ID(Extended Service Set-Identifier)

SSIDを参照

ETHERNET

ゼロックス社、DEC社、インテル社によって開発されたLANの通信方式です。使用するケーブルによって、10BASE-T、100BASE-TX、10BASE-5、10BASE-2などのタイプがあります。

FTP(File Transfer Protocol)

ネットワーク上のクライアントとホストコンピューターとの間で、ファイルの転送を行なうためのプロトコルです。

FTTH(Fiber To The Home)

光ファイバーを使ったインターネット接続サービスです。

HTML(Hyper Text Markup Language)

WWWサーバでのドキュメントを記述するための言語で、通常文書の中にタグを埋め込んでいく方式で作成されます。WWWページを記述する言語として利用されています。

HTTP(Hyper Text Transfer Protocol)

HTMLの転送に使うプロトコルです。WWWブラウザでURLを入力すると、HTTPを使用してWWWサーバからパソコンのWWWブラウザへHTML文書が転送されます。転送された文書は、WWWブラウザによって解釈して画面に表示されます。

HUB

ハブを参照

IEEE 802.1x

LAN内のユーザー認証を定めた規格で、本製品では無線パソコンから有線パソコンへ通信を開始するときに認証を行います。

ユーザー認証に使用するサーバには、RADIUSを使用します。

パソコンは、Windows XP搭載で、無線LANカードは、IEEE 802.11に対応している必要があります。

Internet Explorer

WindowsやMac OSに標準で付属しているブラウザソフトのことです。

IP

インターネットで使われるプロトコルです。IPを中心に、その上位にはアプリケーション層のポート番号があり、下位には通信回線層のポート番号が積層されることでインターネットを形成しています。

IP マスカレード

LAN側で使用しているプライベートIPアドレスをWAN側で使用しているグローバルIPアドレスに、[複数：1]で変換する機能です。

IP(Internet Protocol)アドレス

TCP/IPプロトコルを使用して、構築されたネットワークにおいて、接続しているすべての機器を区別するために付ける32ビットのアドレスです。

通常は、8ビットずつ4つに区切って、10進数の数字列で表されます。(例：192.168.0.1) また、プライベートIPアドレスは、ネットワークの管理者が独自に設定するIPアドレスです。アドレス管理機関やプロバイダーに、申請を行う必要はありませんが、以下の規則にしたがって割り振らなければなりません。

外部のネットワークと接続する場合にはアドレス変換を行い、グローバルIPアドレスに変換する必要があります。

次のIPアドレスをプライベートIPアドレスとして、自由に使用できます。

クラスA：10.0.0.0～10.255.255.225

クラスB：172.16.0.0～172.31.255.225

クラスC：192.168.0.0～

192.168.255.225

ISP(Internet Service Provider)

プロバイダーを参照

LAN(Local Area Network)

同一フロアや敷地内の比較的小さな規模のネットワークのことです。

MACアドレス

(Media Access Control Address)

個々の有線または無線LANカードに設定されている物理アドレスです。

このアドレスは、LANカードの製造メーカーが世界中で重複しない独自の番号で管理しています。Ethernetや無線LANカードでは、このアドレスを元にしてフレームの送受信をしています。

NAT(Network Address Translator)

LAN側で使用しているプライベートIPアドレスをWAN側で使用しているグローバルIPアドレスに1対1で変換する機能です。

OCB AES(Offset Code Book Advanced Encryption Standard)

AESより強力で、標準化が推進されている次世代暗号化方式です。

ONU(Optical Network Unit)

光ファイバーからEthernet信号に変換する装置です。

PoE(Power over Ethernet)

Ethernetケーブルを使用して特定のネットワーク機器に電源供給を行う方法です。

電源供給を受けるネットワーク機器は、PoEに対応している必要があります。

PPP(Point to Point Protocol)

WANにおいて端末が1対1で通信を行うためのプロトコルです。

PPPoE(PPP over Ethernet)

パソコンとプロバイダーのあいだでPPP接続するプロトコルの一種です。

パソコンのPPPクライアント機能を使用して、電話局のアクセスサーバとのあいだにPPP接続を確立します。

PPTP(Point to Point Tunneling Protocol)

インターネット回線を使用してVPNを行うために必要なプロトコルです。

7 ご参考に

7-8. 用語解説(つづき)

RIP(Routing Information Protocol)

ルータ間で、経路情報を交換するTCP/IPネットワークで使用されるプロトコルです。

この情報をもとに、ルータはパケットを正しい相手に送ります。

現在、「Version1」と「Version2」が存在し、「Version2」では、ブロードキャストだけでなくマルチキャストが扱えます。また、ネットマスクを扱えるため、CIDR(classless inter-domain routing)に対応しています。

SNMP(Simple Network Management Protocol)

TCP/IPネットワークにおいて、ネットワーク上の各ホストから自動的に情報を収集して、ネットワーク管理を行うためのプロトコルです。

SSID(Service Set Identifier)

無線LANで、複数のネットワークグループを通信可能なエリア内に形成するときの識別用の名前です。本製品と通信する無線ネットワークグループは、無線パソコンを本製品と同じSSID(もしくはESSID)に設定します。

SYSLOG

システムメッセージをネットワーク上に出力する機能です。

この機能に対応していると、SYSLOGサーバによって、ログ情報を管理できます。

TCP/IP

主要なOSでサポートする現在最も普及したインターネットの基本プロトコルです。

SMTP、FTPなどは、このプロトコルを利用しています。

Open Transportを搭載したMacintoshには、TCP/IPコントロールパネルが標準で搭載されています。

TELNET

CUI(Character User Interface)を使用して、ほかのネットワーク機器を遠隔操作するためのプロトコルです。

本製品は、TELNETに対応しています。

URL(Uniform Resource Locator)

インターネット上のホームページなどにアクセスするために指定します。

弊社URLは、<http://www.root-hq.com/>です。

WAN(Wide Area Network)

LANどうしを一般電話回線、ADSL、CATVなどで結ぶことでできる比較的大規模なネットワークです。

WEP(Wired Equivalent Privacy)

無線LANの通信を暗号化して送受信する一般的な機能です。

無線LAN通信の盗聴を防止できます。

WWWブラウザ

WWWホームページを閲覧したり、WWWサーバを検索に使うアプリケーションです。

アプリケーションには、「Internet Explorer」や「Netscape Navigator」があります。

xDSL

既存の電話線を使用し、128k~52Mbpsの伝送速度でデジタル通信を行うDSL技術の総称です。

10BASE-T

Ethernetの規格の1つで、ツイストペアケーブルを用いた、10Mbit/sの速度をもつものです。

100BASE-TX

Ethernetの規格の1つで、カテゴリ5のツイストペアケーブルを用いた100Mbit/sの速度をもつものです。

アクセスポイント

プロバイダ経由でインターネットを利用するとき、その拠点の総称です。

本製品のように、有線LANと無線LANをつなぐブリッジとして機能する機器の総称としても使われます。

イーサネット

ETHERNETを参照

インターネット

世界中のパソコンをIPを使用して接続したネットワークの総称です。

オープンシステム(Open System)認証

無線LANが暗号化を使用して無線アクセスポイントと通信する場合、認証を行わない方式です。認証を行う方式は「シェアードキー」と呼ばれます。

暗号化機能搭載の無線LAN搭載パソコンは、この方式に対応しています。

クライアント

ネットワークにおいて、サーバに対し情報の提供などのサービスを要求し、その返答を受ける端末またはアプリケーションの総称です。

グローバルIPアドレス

インターネット上のどの機器とも重複するものがない世界で唯一のアドレスです。

サブネットマスク(ネットマスク)

IPアドレスをネットワーク部とホスト部に分けるための区切りを指します。

例えば、IPアドレスが「192.168.0.1」、サブネットマスクが「255.255.255.0」とすると、ネットワーク部は「192.168.0」、ホスト部は末尾の「1」になります。

シェアードキー(Shared Key)認証

無線LANが暗号化を使用して無線アクセスポイントと通信する場合、設定された暗号化鍵(キー)を利用して互いが共通の暗号化鍵を持っていることを確認する方式です。

認証をしない方式は「オープンシステム」と呼ばれます。

スパンニングツリー

ブリッジによってループ状に形成されたLANでパケットが無限に循環するのを防止する機能が備わったネットワークのことです。

ループ状に形成されたLANの検出に使用されるアルゴリズムやループを解除するプロトコルを総称している場合があります。

ダイバーシティー受信

複数のアンテナで電波を受信させ、環境の変化に応じて受信状態のよい方のアンテナに切り替えて信号を受信する方式です。

ドメイン名

IPアドレスの状態では人間には理解しにくいので、IPアドレスの所属グループをドメインとしてドメイン名が割り当てられます。

例)root@bbb.co.jpという電子メールアドレスの場合、bbb.co.jpがドメイン名です。

トラフィック

ネットワーク上のパケットの流れやネットワークの回線にかかる負荷(データ量)のことです。

トラフィックが大きくなると、データ転送の遅れやデータ欠落が起こる可能性があります。

認証

インターネットなどを利用して、ネットワークにアクセスしてくるユーザーが、パスワードとユーザーIDを入力して、アクセスの権利があるかどうかを確認することです。

ネットマスク

サブネットマスクを参照

ネットワーク

データなどを転送するために、サーバ、ワークステーション、パソコンなどの機器が、ケーブルやADSL回線を介して、通信網と接続された状態をいいます。

パケット

データが送受信される際の単位です。送受信に必要な情報を持つヘッダ部と、送りたいデータそのものであるデータ部から構成されています。

パスワード

ネットワークセキュリティ上、ユーザーがネットワークにアクセスするために入力する鍵となる文字列で、パスワードを設定すると、ユーザーがあらかじめ設定された文字列を正しく入力したとき、アクセスが可能になります。

ハブ(HUB)

ネットワークを構築するときに必要になる装置です。

10BASE-Tまたは100BASE-TXケーブルを使用して本製品と接続します。

100Mbpsで通信をするときは、カテゴリ-5のツイストペアケーブルを使用すると同時に、HUBも100BASE-TXに対応している必要があります。

7 ご参考に

7-8. 用語解説(つづき)

フラッシュメモリー

本製品が持つ書き込みが可能な記憶装置です。ここに貯えられた情報は電源を切っても消えないで保存されます。

ブラウザ

WWWサーバからHTML文書を手入して、表示する機能を持ったアプリケーションです。本製品では、代表的なInternet Explorerを使用して説明しています。

プロトコル

通信で、データの送受信を行うときにしたがうべき手順を定義したものの。

ブロードキャスト

同一ネットワーク内のすべてのハードウェアへパケットを一斉に送信(同報通信)することです。

プロバイダー

インターネットサービスプロバイダー(ISP)の略で、インターネットへの接続サービスを提供する業者のことです。

ポート番号

TCPやUDPでアプリケーションを識別するための番号です。例えば、WWWは、TCPの80番、メールは、TCPの25番というように決められています。

マルチキャスト

同一ネットワーク内で、複数のハードウェアを指定してパケットを一斉に送信(同報通信)することです。

マルチパス

高周波を受信する場合、コンクリートや金属製の壁に電波が反射して、直接波と反射波が混ざった状態で受信されること。

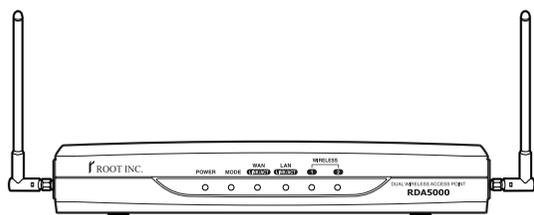
ルート株式会社

住所 : 113-0024 東京都文京区西片1-17-8 KSビル2F

TEL : 03-5840-7601

E-mail : support@root-hq.com

DUAL WIRELESS ACCESS POINT RDA5000



各章について

各メニューの設定画面について説明しています。
設定画面は、用途別に下記の各メニューに分類されています。

参照ページ



メニュー名など



3ページ 	ネットワーク設定	1
17ページ 	無線LAN設定	2
49ページ 	WAN側設定	3
67ページ 	システム設定	4
75ページ 	情報表示	5
79ページ 	Telnetガイド	6
83ページ 	Web公開の設定例	7
87ページ 	複数固定IPを使う	8

はじめに

本書は、本製品で設定できるさまざまな機能について、各メニューの設定画面について詳しく説明しています。取扱説明書[導入編]に記載されていない詳細な機能を設定するときなど、本書と併せてご覧ください。

表記について

本書は、次の規則にしたがって表記しています。

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

[] 表記……各設定画面の設定項目名を([])で囲んで表記します。

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

※本書は、Ver1.18のファームウェアを使用して説明しています。

※Windows 98 Second Editionは、Windows 98 SEと表記します。

Windows Millennium Editionは、Windows Meと表記します。

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

登録商標について

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

©本書に記載されている会社名、製品名は、各社の商標および登録商標です。

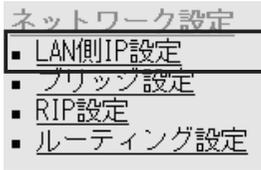
LANへの接続、スパンニングツリー機能、RIP、スタティックルーティングの設定を行います。

1-1.「LAN側IP設定」画面	4
■ 本体名称/IPアドレス設定	4
■ DHCPサーバ設定	6
■ 静的DHCPサーバ設定	8
1-2.「ブリッジ設定」画面	9
■ ブリッジ設定	9
1-3.「RIP設定」画面	12
■ RIP設定	12
■ RIPフィルタ設定	13
1-4.「ルーティング設定」画面	14
■ IP経路情報	14
■ スタティックルーティング設定	15

1 「ネットワーク設定」メニュー

1-1. 「LAN側IP設定」画面

■ 本体名称/IPアドレス設定



本製品の名称とLAN側IPアドレスを設定します。

LAN側IP設定			
本体をネットワークに接続するための設定を行います。			
登録	取消	登録して再起動	本体IPアドレス/サブネットマスクの設定は再起動後に有効になります。
本体名称/IPアドレス設定			
本体名称	①	<input type="text" value="RDA5000"/>	
IPアドレス	②	<input type="text" value="192.168.0.1"/>	
サブネットマスク	③	<input type="text" value="255.255.255.0"/>	

〈登録〉ボタン ……………

「LAN側IP設定」画面の設定内容を変更したとき、[IPアドレス]欄と[サブネットマスク]欄以外の設定内容が有効になります。
※[IPアドレス]欄と[サブネットマスク]欄を変更した場合は、画面上で確定されますが、〈登録して再起動〉をクリックするまで有効になりません。

〈取消〉ボタン ……………

「LAN側IP設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

〈登録して再起動〉ボタン ……

本製品を再起動して、「LAN側IP設定」画面で変更したすべての設定内容を有効にします。

① 本体名称 ……………

ネットワーク上で、本製品を識別する名前です。
設定した名前は、本製品のLAN側に接続されたパソコンから、本製品に直接アクセスするためのドメイン名の一部として使えます。
(出荷時の設定：RDA5000)

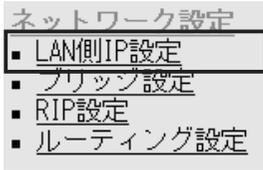
入力形式：[http://web.本体名称/] (例 http://web.RDA5000/)
この場合、[DHCPサーバ設定]項目の[DNS代理応答を使用]欄を「する」(出荷時の設定)に設定しておく必要があります。

※ほかのネットワーク機器との重複に注意して、アルファベットで始まる半角英数字(A～Z、0～9、-)を、31文字以内で設定します。

※登録できない文字は、「#,%/, : , ? , @ , ¥ , '」の8種類です。

1-1.「LAN側IP設定」画面

■ 本体名称/IPアドレス設定(つづき)



- ② IPアドレス 本製品のLAN側IPアドレスの設定です。
 (出荷時の設定：192.168.0.1)
 本製品を稼働中のネットワークに接続するときなど、そのLANに合わせたネットワークIPアドレスに変更してください。
 ※本製品のDHCPサーバ機能を使用する場合は、[DHCPサーバ設定]項目の[割り当て開始IPアドレス]欄についてもネットワーク部を同じに設定してください。

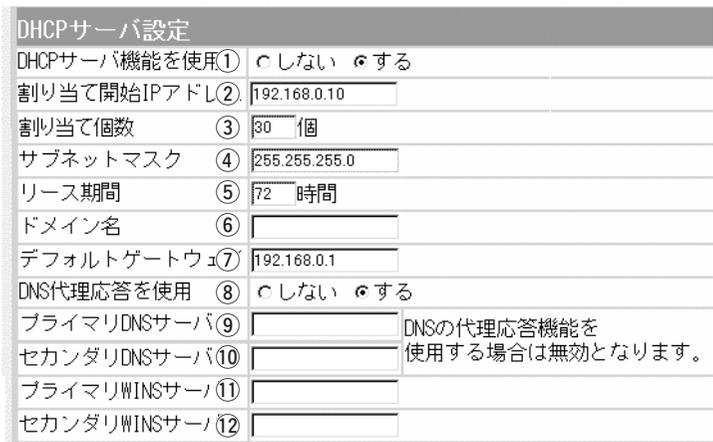
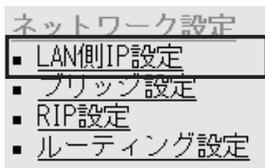
- ③ サブネットマスク 本製品のサブネットマスク(同じネットワークで使用するIPアドレスの範囲)を設定します。 (出荷時の設定：255.255.255.0)
 本製品を稼働中のネットワークに接続するときなど、そのLANに合わせたサブネットマスクに変更してください。

1 「ネットワーク設定」メニュー

1-1.「LAN側IP設定」画面(つづき)

■ DHCPサーバ設定

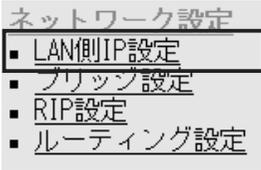
DHCPサーバ機能についての設定です。



- ① DHCPサーバ機能を使用 … 本製品をDHCPサーバとして使用するかしないかを設定します。本製品のLAN側に有線および無線で直接接続しているパソコンのTCP/IP設定を、「IPアドレスを自動的に取得する」と設定している場合、パソコンは、本製品のDHCPクライアントになります。この機能によって、動的にDHCPサーバである本製品からIPアドレス/サブネットマスク、ルータやDNSサーバのIPアドレス/ドメイン名が与えられます。(出荷時の設定：する)
- ② 割り当て開始IPアドレス … 本製品のLAN側に有線および無線で直接接続するパソコンへ、IPアドレスを自動で割り当てるときの開始アドレスを設定します。(出荷時の設定：192.168.0.10)
- ③ 割り当て個数 …………… [割り当て開始IPアドレス]欄に設定されたIPアドレスから連続で自動割り当て可能なアドレスの最大個数は、0～128(無線LANで接続するパソコンを含む)までです。(出荷時の設定：30)
※128個を超える分については、設定できませんので手動でクライアントに割り当ててください。
※「0」を設定したときは、自動割り当てを行いません。
- ④ サブネットマスク …………… [割り当て開始IPアドレス]欄に設定されたIPアドレスに対するサブネットマスクです。(出荷時の設定：255.255.255.0)
- ⑤ リース期間 …………… DHCPサーバが自動でローカルIPアドレスを定期的に、有線および無線パソコンに割り当てなおす期限を指定します。設定できる範囲は、「1～9999(時間)」です。(出荷時の設定：72)

1-1.「LAN側IP設定」画面

■ DHCPサーバ設定(つづき)



DHCPサーバ設定	
DHCPサーバ機能を使用①	<input type="radio"/> しない <input checked="" type="radio"/> する
割り当て開始IPアドレス②	192.168.0.10
割り当て個数③	30 個
サブネットマスク④	255.255.255.0
リース期間⑤	72 時間
ドメイン名⑥	
デフォルトゲートウェイ⑦	192.168.0.1
DNS代理応答を使用⑧	<input type="radio"/> しない <input checked="" type="radio"/> する
プライマリDNSサーバ⑨	
セカンダリDNSサーバ⑩	
プライマリWINSサーバ⑪	
セカンダリWINSサーバ⑫	

- ⑥ **ドメイン名** ドメイン名を使用しているときや、プロバイダーからドメイン名を指定されたときなど必要があれば、DHCPサーバが有線および無線で接続するパソコンに通知するネットワークアドレスのドメイン名を、127文字(半角英数字)以内で入力します。

- ⑦ **デフォルトゲートウェイ** ... ご契約のプロバイダーやネットワーク管理者から指定された場合に限り、LAN側に通知するゲートウェイを入力します。
(出荷時の設定：192.168.0.1)

- ⑧ **DNS代理応答を使用** 本製品を代理DNSサーバとして使用するかどうかの設定です。代理DNSサーバ機能とは、パソコンからのDNS要求をプロバイダー側のDNSサーバへ転送する機能です。(出荷時の設定：する)代理DNSサーバ機能を利用すると、ネットワーク上のパソコンのDNSサーバを本製品のアドレスに設定している場合、本製品が接続する先のDNSサーバのアドレスが変更になったときでも、パソコンの設定を変更する必要がありませんので便利です。

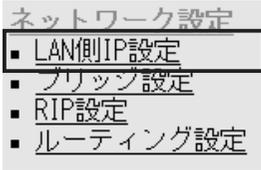
- ⑨ **プライマリDNSサーバ** 本製品のDHCPサーバ機能を使用する場合に有効な機能で、必要に応じて使い分けたいDNSサーバのアドレスが2つある場合は、優先したい方のアドレスを入力します。
入力すると、本製品のIPアドレスの代わりに設定したDNSサーバアドレスをDHCPクライアントに通知します。
※[DNS代理応答を使用]欄を「する」(出荷時の設定)に設定する場合は、無効になります。

- ⑩ **セカンダリDNSサーバ** [プライマリDNSサーバ]欄と同様に、使い分けたいDNSサーバアドレスのもう一方を入力します。
※[DNS代理応答を使用]欄を「する」(出荷時の設定)に設定する場合は、無効になります。

1 「ネットワーク設定」メニュー

1-1.「LAN側IP設定」画面

■ DHCPサーバ設定(つづき)



DHCPサーバ設定	
DHCPサーバ機能を使用①	<input type="radio"/> しない <input checked="" type="radio"/> する
割り当て開始IPアドレス②	192.168.0.10
割り当て個数③	30 個
サブネットマスク④	255.255.255.0
リース期間⑤	72 時間
ドメイン名⑥	
デフォルトゲートウェイ⑦	192.168.0.1
DNS代理応答を使用⑧	<input type="radio"/> しない <input checked="" type="radio"/> する
プライマリDNSサーバ⑨	
セカンダリDNSサーバ⑩	
プライマリWINSサーバ⑪	
セカンダリWINSサーバ⑫	

⑪ プライマリWINSサーバ ...

Microsoftネットワークを使ってWINSサーバを利用する場合は、WINSサーバアドレスを入力します。WINSサーバのアドレスが2つある場合は、優先したい方のアドレスを入力します。

⑫ セカンダリWINSサーバ ...

「プライマリWINSサーバ」と同様、WINSサーバのアドレスが2つある場合は、残りの一方を入力します。

■ 静的DHCPサーバ設定

指定したIPアドレスを特定のパソコンに固定で割り当てるときの設定です。

静的DHCPサーバ設定		
登録の追加		
MACアドレス	IPアドレス	
<input type="text"/>	<input type="text"/>	<input type="button" value="追加"/>
現在の登録		
MACアドレス	IPアドレス	

静的DHCPサーバ設定

本製品のDHCPサーバ機能を使用時、自動で割り当てるIPアドレスを、特定のクライアントに固定して割り当てるとき、そのクライアントのMACアドレスと固定で割り当てるIPアドレスとの組み合わせを登録する欄です。

※この欄には、最大16個の組み合わせまで登録できます。

登録するクライアントのIPアドレスは、DHCPサーバ機能による割り当て範囲および本製品のIPアドレスと重複しないように設定してください。

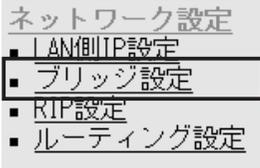
【登録例】

登録した内容を取り消すときは、該当する欄の〈削除〉をクリックします。

現在の登録		
MACアドレス	IPアドレス	
00-90-C7-6C-00-14	192.168.0.50	<input type="button" value="削除"/>

1-2.「ブリッジ設定」画面

■ブリッジ設定



スパニングツリー機能をブリッジ通信する本製品に設定します。

ブリッジ設定
 ブリッジ機能に関する設定を行います。

登録 取消 登録して再起動 このページの設定は再起動後に有効になります。

ブリッジ設定		
スパニングツリー機能を使用	①	<input checked="" type="radio"/> しない <input type="radio"/> する
ブリッジ優先度(Bridge Priority)	②	<input type="text" value="32768"/>
エージングタイム(Aging Time)	③	<input type="text" value="300"/> 秒
マックスエイジ(Max Age)	④	<input type="text" value="20"/> 秒
ハロータイム(Hello Time)	⑤	<input type="text" value="2"/> 秒
転送遅延(Forward Delay)	⑥	<input type="text" value="15"/> 秒
パスコスト(Path Cost)	有線LAN	<input type="text" value="100"/>
	⑦ 無線[802.11g]	<input type="text" value="200"/>
	無線[802.11a]	<input type="text" value="200"/>
ポート優先度(Port Priority)	有線LAN	<input type="text" value="128"/>
	⑧ 無線[802.11g]	<input type="text" value="128"/>
	無線[802.11a]	<input type="text" value="128"/>

〈登録〉ボタン [ブリッジ設定]項目で変更した内容を画面上で確定するボタンです。
 ※ 〈登録して再起動〉をクリックするまで有効になりません。

〈取消〉ボタン [ブリッジ設定]項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
 なお 〈登録〉をクリックすると、変更前の状態には戻りません。

〈登録して再起動〉ボタン 本製品を再起動して、[ブリッジ設定]項目で変更したすべての設定内容を有効にします。

① スパニングツリー機能を使用

経路のループを検出し、パケットが無限に循環するのを回避して、最適な経路を作成する機能を使用するかしないかを設定します。

(出荷時の設定：しない)

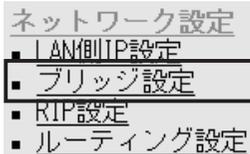
スパニングツリー機能を設定すると、経路障害のないときは、冗長リンクを検出して重複する経路のうち優先度の低い方を遮断します。

ブリッジ間で経路障害が起こったときは、正常時に遮断されていた経路を使用してネットワークの正常な稼働を保証します。

1 「ネットワーク設定」メニュー

1-2.「ブリッジ設定」画面

■ブリッジ設定(つづき)



ブリッジ設定

ブリッジ機能に関する設定を行います。

登録 取消 登録して再起動 このページの設定は再起動後に有効になります。

ブリッジ設定		
スパンニングツリー機能を使用	①	<input checked="" type="radio"/> しない <input type="radio"/> する
ブリッジ優先度(Bridge Priority)	②	<input type="text" value="32768"/>
エージングタイム(Aging Time)	③	<input type="text" value="300"/> 秒
マックスエイジ(Max Age)	④	<input type="text" value="20"/> 秒
ハロータイム(Hello Time)	⑤	<input type="text" value="2"/> 秒
転送遅延(Forward Delay)	⑥	<input type="text" value="15"/> 秒
パスコスト(Path Cost)	有線LAN	<input type="text" value="100"/>
	⑦ 無線[802.11g]	<input type="text" value="200"/>
	無線[802.11a]	<input type="text" value="200"/>
ポート優先度(Port Priority)	有線LAN	<input type="text" value="128"/>
	⑧ 無線[802.11g]	<input type="text" value="128"/>
	無線[802.11a]	<input type="text" value="128"/>

②ブリッジ優先度 ……………

※出荷時の設定でご使用されることを推奨します。

ブリッジで通信する本製品の優先度を決定する値で、設定値が小さいほど、優先度が高くなります。

設定できる範囲は「0～65535」で、一番優先度が高いRDA5000が、そのネットワークのルートブリッジになります。

(出荷時の設定：32768)

※同じ値が設定された機器がある場合は、MACアドレスの小さい機器の優先度が高くなります。

③エージングタイム ……………

※出荷時の設定でご使用されることを推奨します。

本製品が自動学習したMACアドレスをアドレステーブルに記憶しておく時間を指定します。(出荷時の設定：300)

設定できる範囲は、「15～1000000(秒)」です。

無通信状態がこの欄に設定された時間つづくと、アドレステーブルから削除されます。

④マックスエイジ ……………

※出荷時の設定でご使用されることを推奨します。

BPDU(Bridge Protocol Data Unit)を指定します。

設定できる範囲は、「6～40(秒)」です。(出荷時の設定：20)

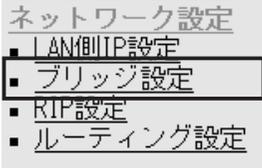
⑤ハロータイム ……………

※出荷時の設定でご使用されることを推奨します。

本製品がルートブリッジとして動作するとき、本製品からBPDU情報を送出する間隔を設定します。

設定できる範囲は、「1～10(秒)」です。(出荷時の設定：2)

1-2.「ブリッジ設定」画面
 ■ブリッジ設定(つづき)



ブリッジ設定
 ブリッジ機能に関する設定を行います。

登録 取消 登録して再起動 このページの設定は再起動後に有効になります。

ブリッジ設定		
スパンニングツリー機能を使用	①	<input checked="" type="radio"/> しない <input type="radio"/> する
ブリッジ優先度(Bridge Priority)	②	<input type="text" value="32768"/>
エージングタイム(Aging Time)	③	<input type="text" value="300"/> 秒
マックスエイジ(Max Age)	④	<input type="text" value="20"/> 秒
ハロータイム(Hello Time)	⑤	<input type="text" value="2"/> 秒
転送遅延(Forward Delay)	⑥	<input type="text" value="15"/> 秒
パスコスト(Path Cost)	有線LAN	<input type="text" value="100"/>
	⑦ 無線[802.11g]	<input type="text" value="200"/>
	無線[802.11a]	<input type="text" value="200"/>
ポート優先度(Port Priority)	有線LAN	<input type="text" value="128"/>
	⑧ 無線[802.11g]	<input type="text" value="128"/>
	無線[802.11a]	<input type="text" value="128"/>

⑥ **転送遅延**
 ※出荷時の設定でご使用されることを推奨します。

ネットワークの再編成中に学習したMACアドレスの有効期限を指定します。
 設定できる範囲は、「4～30(秒)」です。 (出荷時の設定：15)

⑦ **パスコスト**
 ※出荷時の設定でご使用されることを推奨します。

ネットワーク全体のブリッジとルートブリッジ間の優先データパスの決定に利用される値で、各ポートからルートブリッジまでの経路コストが小さいブリッジが優先されます。
 設定できる範囲は、「1～65536」です。

(出荷時の設定：有線LAN：100
 無線[802.11g]：200
 無線[802.11a]：200)

⑧ **ポート優先度**
 ※出荷時の設定でご使用されることを推奨します。

ブリッジで通信する本製品のポートごとに優先度を決定する値で、設定値が小さいほど、ポート優先度が高くなります。
 設定できる範囲は、「0～255」です。

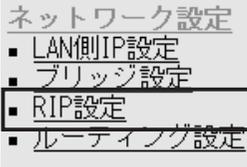
(出荷時の設定：有線LAN：128
 無線[802.11g]：128
 無線[802.11a]：128)

※各ポートで同じ値が設定されている場合は、物理的なポート番号の小さい順に優先度が高くなります。

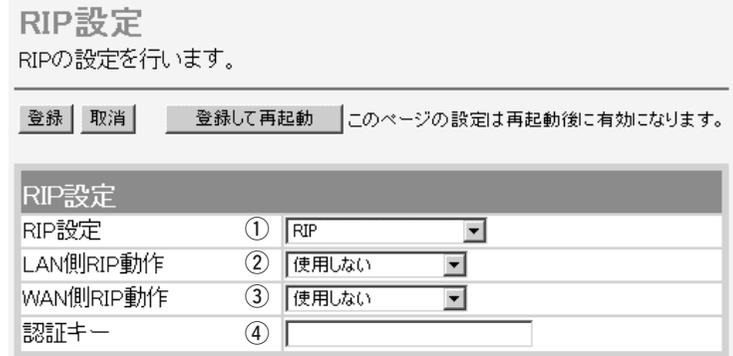
1 「ネットワーク設定」メニュー

1-3.「RIP設定」画面

■ RIP設定



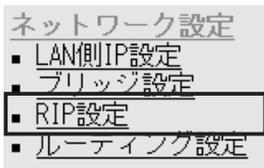
隣接ルータやアクセスポイントと経路情報を交換して、経路を動的に作成するとき 사용합니다。



- 〈登録〉ボタン 「RIP設定」画面で変更した内容を画面上で確定するボタンです。
※ 〈登録して再起動〉をクリックするまで有効になりません。
- 〈取消〉ボタン 「RIP設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお 〈登録〉をクリックすると、変更前の状態には戻りません。
- 〈登録して再起動〉ボタン 本製品を再起動して、「RIP設定」画面で変更したすべての設定内容を有効にします。
- ① RIP設定 RIPの種類を選択します。 (出荷時の設定：RIP)
○RIP : RIPの「Version1」を使用します。
○RIP2(ブロードキャスト) :
RIPの「Version2」を使用して、ブロードキャストアドレスにパケットを送信します。
○RIP2(マルチキャスト) :
RIPの「Version2」を使用して、マルチキャストアドレスにパケットを送信します。
- 【RIP2について】**
RIP2は、可変長サブネットマスクに対応していますので、イントラネット環境でも利用できます。
受信については、ブロードキャスト/マルチキャストの区別なく受け入れます。
- ② LAN側RIP動作 LAN側について、[RIP設定]欄で選択したRIPを「使用しない」、「受信のみ」、「受信も送信も行う」から選択します。
(出荷時の設定：使用しない)
- ③ WAN側RIP動作 WAN側について、[RIP設定]欄で選択したRIPを「使用しない」、「受信のみ」、「受信も送信も行う」から選択します。
(出荷時の設定：使用しない)

1-3.「RIP設定」画面

■ RIP設定(つづき)



④ 認証キー

[RIP設定]①欄で、「RIP2(マルチキャスト)」または「RIP2(ブロードキャスト)」を設定する場合、そのRIP動作を認証するためのキーを入力します。

入力は、大文字/小文字の区別にご注意して、半角15文字以内で入力します。

また、ほかのルータやアクセスポイントに設定されている認証キーと同じ設定にします。

認証キーを設定すると、「RIP」を設定しているゲートウェイと、異なる認証キーを設定している「RIP2」、および認証キーを設定していない「RIP2」ゲートウェイからのRIPパケットを破棄します。

※RIPを使用しない場合、または[RIP設定]①欄で「RIP」を設定する場合は、空白にします。

■ RIPフィルタ設定

RIPフィルターについての設定です。



RIPフィルタ設定.....

同一サブネットで使う複数のアクセスポイントやルータにおいて、特定のアクセスポイントやルータが出力するRIPパケットを受信しないように、そのパケットを出力するアクセスポイントやルータのIPアドレスとサブネットマスクを入力します。

最大16件の登録が可能です。

【登録例】

登録した内容を取り消すときは、該当する欄の〈削除〉をクリックします。



1 「ネットワーク設定」メニュー

1-4.「ルーティング設定」画面

■ IP経路情報

ネットワーク設定

- LAN側IP設定
- ブリッジ設定
- RIP設定
- ルーティング設定

ルータがパケットの送信において、そのパケットをどのルータ、またはどのパソコンに配送すべきかの情報を表示します。

この項目には、[スタティックルーティング設定]項目で追加した経路も表示されます。

ルーティング設定

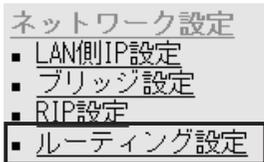
通信経路（ルート）に関する設定を行います。

IP経路①情報	②	③	④	⑤	⑥
宛先	サブネットマスク	ゲートウェイ	経路	作成	メトリック
192.168.0.0	255.255.255.0	192.168.0.1	local	static	0
192.168.0.0	255.255.255.255	255.255.255.255	local	misc	0
192.168.0.1	255.255.255.255	192.168.0.1	local	static	0
192.168.0.255	255.255.255.255	255.255.255.255	local	misc	0

- ① 宛先 ルーティングの対象となるパケットの宛先IPアドレスを表示します。
- ② サブネットマスク ルーティングの対象となるパケットの宛先IPアドレスに対するサブネットマスクを表示します。
- ③ ゲートウェイ ルーティングの対象となるパケットの宛先IPアドレスに対するゲートウェイを表示します。
- ④ 経路 ルーティングの対象となるパケットの宛先IPアドレスに対する転送先インターフェイスを表示します。
◎ local：インターフェイスがLAN側の場合です。
◎ wan：インターフェイスがWAN側の場合です。
※「wan」と表示されるのは、回線種別を「DHCP」にしたときです。
回線種別を「PPPoE」または「PPPoE複数固定IP」に設定したときは、「WAN側設定」画面で[接続先名]欄に設定された内容を「O1:WAN」に代わって表示します。
※インターフェイスの詳細は、「情報表示」メニューの「ネットワーク情報」画面にある[ネットワーク インターフェイス リスト]項目に表示します。
- ⑤ 作成 どのように経路情報が作成されたかを表示します。
◎ static：スタティック(定義された)ルートにより作成
◎ rip：ダイナミック(自動生成された)ルートにより作成
◎ misc：ブロードキャストに関係するフレーム処理で作成
- ⑥ メトリック [スタティックルーティング設定]項目の[メトリック]欄で設定された値やダイナミックルーティングで作成された経路のコストを表示します。

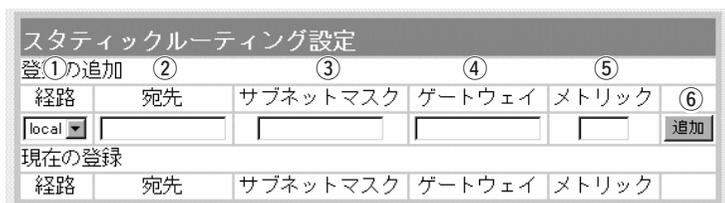
1-4.「ルーティング設定」画面(つづき)

■ スタティックルーティング設定



パケットの中継経路を、意図的に定義するルーティングテーブルです。

登録できるのは、最大32件までです。



- ① 経路 回路の経路を指定します。
 ◎ local : 登録する経路情報がLAN側の場合です。
 ◎ wan : 登録する経路情報がWAN側の場合です。
 ※「wan」と表示されるのは、回線種別を「DHCP」にしたときです。
 回線種別を「PPPoE」または「PPPoE複数固定IP」に設定したときは、「WAN側設定」画面で「接続先名」欄に設定された内容を「01:WAN」に代わって表示します。
- ② 宛先 経路にLAN側を選択したときは、対象となる相手先のIPアドレスを入力します。
 経路にWAN側を選択したときは、対象となる相手先のネットワークIPアドレスを入力します。
 ※IPアドレスは、ゲートウェイのネットワーク部と同じにします。
- ③ サブネットマスク 対象となる宛先のIPアドレスに対するサブネットマスクを入力します。
- ④ ゲートウェイ ルーティングの対象となるパケット転送先ルータのゲートウェイを入力します。
 ※入力は、[経路]欄で入力したIPアドレスのネットワーク部と同じにします。
- ⑤ メトリック 宛先までのコストを表す数値を入力します。
 数値が小さければ転送能力の高い回線と見なされ、数値が大きければ転送能力が低い回線と見なされます。
 0(空白)~15まで入力できます。
- ⑥ <追加> 設定した内容で「IP経路情報」項目に登録します。
 登録されると、その内容は「IP経路情報」項目に表示されます。
 ※操作後は、「現在の登録」欄に登録されたことを確認してください。



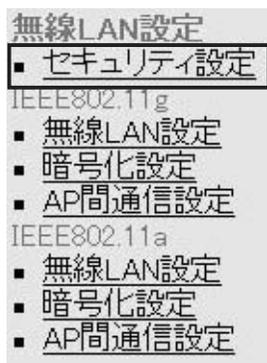
MACアドレスセキュリティー、無線端末間通信禁止機能、無線ネットワーク名、RADIUS認証、暗号化セキュリティー、AP間通信機能の設定を行います。

2-1.「セキュリティ設定」画面	18
■ RADIUS設定	18
■ 無線端末間通信設定	19
■ MACアドレスセキュリティー設定	20
2-2.「無線LAN設定」画面[IEEE802.11g]	21
■ 無線LAN設定	21
2-3.「暗号化設定」画面[IEEE802.11g]	28
■ 暗号化設定	28
■ キー値	32
■ ご参考に	33
2-4.キー値の設定例	34
■ 無線アクセスポイント通信の場合	34
■ 無線AP(アクセスポイント)間通信の場合	35
2-5.「AP間通信設定」画面[IEEE802.11g]	36
■ IEEE802.11g BSSID	36
■ 通信AP設定	36
2-6.「無線LAN設定」画面[IEEE802.11a]	37
■ 無線LAN設定	37
2-7.「暗号化設定」画面[IEEE802.11a]	41
■ 暗号化設定	41
■ キー値	45
■ ご参考に	46
2-8.「AP間通信設定」画面[IEEE802.11a]	47
■ IEEE802.11a BSSID	47
■ 通信AP設定	47

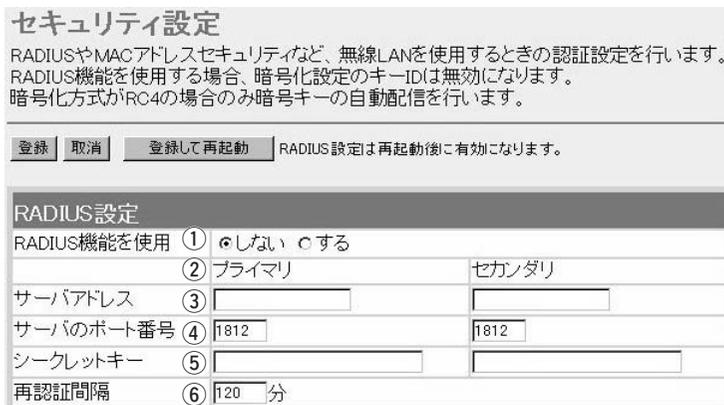
2 「無線LAN設定」メニュー

2-1.「セキュリティ設定」画面

■ RADIUS設定



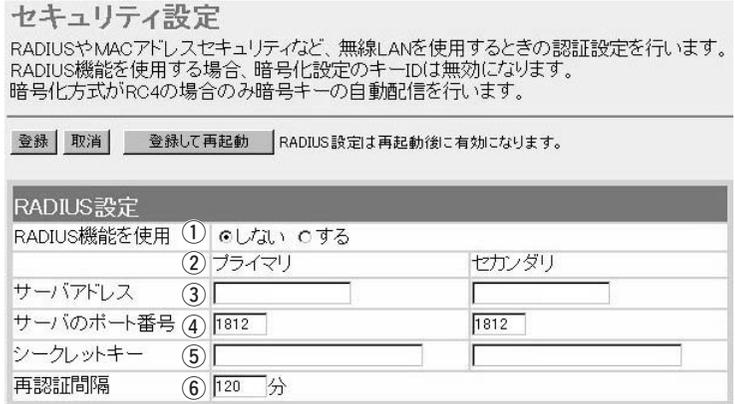
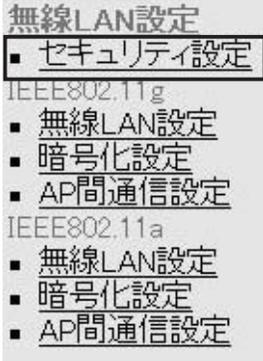
RADIUSサーバによる無線パソコンへの認証接続についての設定を行います。



- 〈登録〉ボタン …………… [MACアドレスセキュリティ設定]項目の内容が有効になります。
※[RADIUS設定]項目を変更した場合は、画面上で確定されますが、〈登録して再起動〉をクリックするまで有効になりません。
- 〈取消〉ボタン …………… 「セキュリティ設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。
- 〈登録して再起動〉ボタン …… 本製品を再起動して、「セキュリティ設定」画面で変更したすべての設定内容を有効にします。
- ① RADIUS機能を使用 ……… RADIUSサーバを使って無線パソコンへの認証をするかしないかを選択します。 (出荷時の設定：しない)
本製品は、EAP-MD5とEAP-TLSに対応しています。
「RADIUS機能を使用する」に設定している場合は、「暗号化設定」画面の[キーID]欄の設定は無効になります。
また、RADIUSサーバとの鍵交換は、「WEP RC4」を[暗号化方式]欄で設定しているとき有効で、クライアント側では、Windows XP標準のワイヤレスネットワーク接続の設定で、「キーは自動的に提供される(H)」にチェックマークが入っている状態に該当します。
「OCB AES」を[暗号化方式]欄で設定しているときは、RADIUS認証だけを行います。
このときは、RADIUSサーバと鍵交換は行いません。
- ② プライマリ/セカンダリ …… [プライマリ]列に設定したサーバから応答がないとき、その次にアクセスさせるRADIUSサーバがあるときは、[セカンダリ]列にそのRADIUSサーバアドレスを設定します。

2-1.「セキュリティ設定」画面

■ RADIUS設定(つづき)



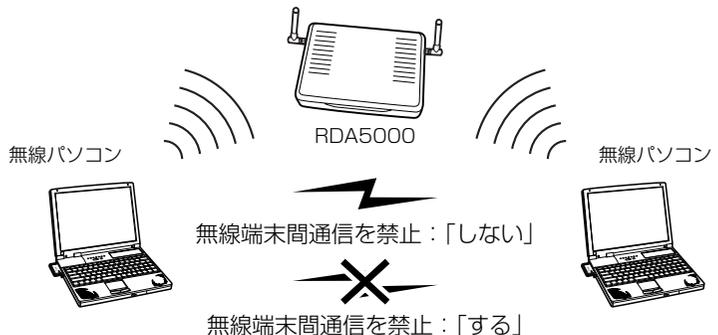
- ③ サーバアドレス 対象となるRADIUSサーバのIPアドレスを入力します。
- ④ サーバのポート番号 対象となるRADIUSサーバの認証ポートを設定します。設定できる範囲は、「1～65535」です。(出荷時の設定：1812) ※ご使用になるシステムによっては、出荷時の設定値と異なることがありますので確認してください。
- ⑤ シークレットキー この欄に設定されたキーを使用して本製品とRADIUSサーバ間の通信パケットを暗号化します。RADIUSサーバに設定された値と同じ値を入力します。入力は、半角31文字以内の英数字で入力します。
- ⑥ 再認証間隔 RADIUSサーバに再度認証を要求する間隔を設定します。設定できる範囲は、「30～9999(分)」です。(出荷時の設定：120)

■ 無線端末間通信設定

本製品を介してパソコンどうしが無線通信するのを禁止するとき設定します。

この機能は、[IEEE802.11a/b/g]のいずれかの規格で通信するすべての無線パソコンが対象になります。

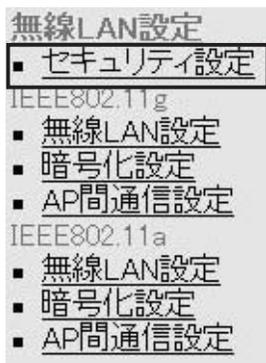
(出荷時の設定：しない)



2 「無線LAN設定」メニュー

2-1.「セキュリティ設定」画面(つづき)

■ MACアドレスセキュリティ設定



通信を許可する無線パソコンのMACアドレスを登録することで、登録していない無線パソコンからの通信を制限するとき必要な設定です。

MACアドレスセキュリティ設定		
MACアドレスセキュリティを使用 ①	<input checked="" type="radio"/> しない <input type="radio"/> する	
登録の追加 ②		
MACアドレス	<input type="text"/>	<input type="button" value="追加"/>
現在の登録 ③		
登録済みの端末	受信中の端末	通信状況

① MACアドレス

セキュリティを使用 ………

本製品に登録されたMACアドレスを持つ無線LANのパソコンだけが、本製品にワイヤレス接続できるようにするかしないかを選択します。
(出荷時の設定：しない)
「する」を選択すると、[現在の登録]欄に登録されていないMACアドレスを持つ無線LANからのアクセスを防止します。

② 登録の追加 ……………

この欄に対象となる無線LANカードのMACアドレスを入力して〈追加〉をクリックすると、[登録済みの端末]欄に登録されます。
MACアドレスセキュリティが有効なとき、[登録済みの端末]欄に表示されたMACアドレスをもつ無線LANカードとだけ通信できます。

※最大256台分のMACアドレスを登録できます。

※入力は半角英数字で12桁(16進数)を入力します。

※入力後は〈追加〉をクリックして、[現在の登録]欄に登録されたことを確認してください。

※2つの入力例は、同じMACアドレスになります。

(入力例：00-90-C7-6E-00-9A、0090C76E009A)

③ 現在の登録 ……………

本製品と無線で通信しているパソコンの状況や登録済みの無線パソコンのMACアドレスを表示します。

登録されているMACアドレスは、〈削除〉で登録の削除が行えません。

なお、登録されていないMACアドレスを持つ無線パソコンも[受信中の端末]欄にMACアドレスが表示されますので、その欄に表示される〈追加〉ボタンをクリックすることで、そのパソコンのMACアドレスを追加登録できます。

2-2.「無線LAN設定」画面 [IEEE802.11g]

■ 無線LAN設定

54Mbps(2.4GHz帯)の内蔵無線LANカードに対する設定です。



無線LAN設定 [IEEE802.11g]

無線LANを使用するときの設定を行います。

登録 取消 登録して再起動 このページの設定は再起動後に有効になります。

無線LAN設定		
IEEE802.11gを使用	①	<input type="radio"/> しない <input checked="" type="radio"/> する
SSID	②	**
SSIDの確認入力	③	**
ANYを拒否	④	<input checked="" type="radio"/> しない <input type="radio"/> する
チャンネル	⑤	11(2462MHz) ▾
Rts/Ctsスレッシュホールド	⑥	無し ▾
11g保護機能	⑦	無効 ▾
パワーレベル	⑧	高 ▾
接続端末制限	⑨	255

〈登録〉ボタン ……………

[IEEE802.11gを使用]欄以外の設定内容が有効になります。
 ※[IEEE802.11gを使用]欄を変更した場合は、画面上で確定されますが、〈登録して再起動〉をクリックするまで有効になりません。

〈取消〉ボタン ……………

[無線LAN設定]項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
 なお〈登録〉をクリックすると、変更前の状態には戻りません。

〈登録して再起動〉ボタン ……

本製品を再起動して、[無線LAN設定]項目で変更したすべての設定内容を有効にします。

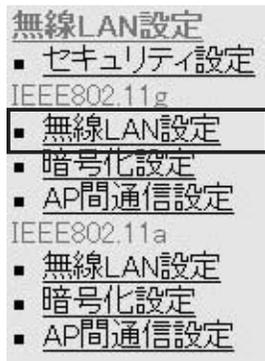
① IEEE802.11gを使用 ……

IEEE802.11g(2.4GHz帯)規格の無線アクセスポイント機能を無効にするとき設定します。(出荷時の設定：する)
 ※「しない」(無効)に設定すると、IEEE802.11b規格の通信もできなくなります。

2 「無線LAN設定」メニュー

2-2.「無線LAN設定」画面[IEEE802.11g]

■無線LAN設定(つづき)



無線LAN設定 [IEEE802.11g]
無線LANを使用するときの設定を行います。

このページの設定は再起動後に有効になります。

無線LAN設定		
IEEE802.11gを使用	①	<input type="radio"/> しない <input checked="" type="radio"/> する
SSID	②	<input type="text" value="**"/>
SSIDの確認入力	③	<input type="text" value="**"/>
ANYを拒否	④	<input checked="" type="radio"/> しない <input type="radio"/> する
チャンネル	⑤	<input type="text" value="11 (2462MHz)"/>
Rts/Ctsスレッシュホールド	⑥	<input type="text" value="無し"/>
11g保護機能	⑦	<input type="text" value="無効"/>
パワーレベル	⑧	<input type="text" value="高"/>
接続端末制限	⑨	<input type="text" value="255"/>

② SSID.....

無線ルータや無線アクセスポイントが無線伝送エリア内に複数存在しているような場合、個々の無線ネットワークグループを[SSID(無線ネットワーク名)]で識別したり、異なる無線ネットワーク名で通信するグループからの混信を防止します。

この[SSID]が異なると本製品と無線で通信できません。

セキュリティーというよりは、むしろ無線ネットワークのグループ分けを設定するために使用します。

大文字/小文字の区別にご注意して、任意の英数字、半角31文字以内で入力します。

(出荷時の設定：LG)

また、入力した文字はすべて「*(アスタリスク)」で表示されます。

(表示例：**)

※[SSID]と[ESS ID]は、同じ意味で使用しています。

本製品以外の無線LAN機器では、[ESS ID]と表記されている場合があります。

③ SSIDの確認入力.....

確認のため、[SSID]を再入力します。

(表示例：**)

2-2.「無線LAN設定」画面[IEEE802.11g]

■無線LAN設定(つづき)

- 無線LAN設定
 - セキュリティ設定
 - IEEE802.11g
 - 無線LAN設定
 - 暗号化設定
 - AP間通信設定
 - IEEE802.11a
 - 無線LAN設定
 - 暗号化設定
 - AP間通信設定

無線LAN設定 [IEEE802.11g]
無線LANを使用するときの設定を行います。

登録 取消 登録して再起動 このページの設定は再起動後に有効になります。

無線LAN設定		
IEEE802.11gを使用	①	<input type="radio"/> しない <input checked="" type="radio"/> する
SSID	②	**
SSIDの確認入力	③	**
ANYを拒否	④	<input checked="" type="radio"/> しない <input type="radio"/> する
チャンネル	⑤	11 (2462MHz) ▾
Rts/Ctsスレッシュホールド	⑥	無し ▾
11g保護機能	⑦	無効 ▾
パワーレベル	⑧	高 ▾
接続端末制限	⑨	255

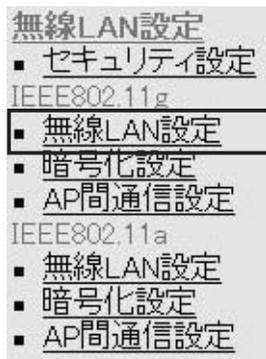
④ ANYを拒否

「ANY」モード(アクセスポイント自動検索接続機能)で動作している無線パソコンからの検索や接続を拒否するかしないかを設定します。
(出荷時の設定：しない)
出荷時の設定では、無線LANカードを装着するパソコンとの接続が容易になるように、これらの無線パソコンからの検索や接続を許可しています。
この設定を「する」にした場合、「ANY」モードで通信する無線パソコンが使用する「Windows XP標準のワイヤレスネットワーク接続」に検索されません。

2 「無線LAN設定」メニュー

2-2.「無線LAN設定」画面[IEEE802.11g]

■無線LAN設定(つづき)



無線LAN設定 [IEEE802.11g]

無線LANを使用するときの設定を行います。

登録 **取消** **登録して再起動** このページの設定は再起動後に有効になります。

無線LAN設定		
IEEE802.11gを使用	①	<input type="radio"/> しない <input checked="" type="radio"/> する
SSID	②	**
SSIDの確認入力	③	**
ANYを拒否	④	<input checked="" type="radio"/> しない <input type="radio"/> する
チャンネル	⑤	11(2462MHz) ▼
Rts/Ctsスレッシュホールド	⑥	無し ▼
11g保護機能	⑦	無効 ▼
パワーレベル	⑧	高 ▼
接続端末制限	⑨	255

⑤ チャンネル

本製品が2.4GHz帯(IEEE802.11b規格およびIEEE802.11g規格)の無線通信に使用する無線通信チャンネルを設定します。

(出荷時の設定：11(2462MHz))

※無線パソコン側は、本製品のチャンネルを自動的に検知して通信します。

※近くに2.4GHz帯(IEEE802.11b規格およびIEEE802.11g規格)の無線アクセスポイント機能で通信する別の無線ネットワークグループが存在するときは、電波干渉を避けるため、本製品の「チャンネル」は、別の無線ネットワークグループと4チャンネル以上空けて設定してください。

それ以下のときは、図に示すように帯域の1部が重複するため混信する可能性があります。

例えば、お互いの設定が、1-6-11チャンネルに設定すると混信しません。

※本製品は、14チャンネルでの運用はできません。



2-2.「無線LAN設定」画面[IEEE802.11g]

■無線LAN設定(つづき)

- 無線LAN設定
 - セキュリティ設定
 - IEEE802.11g
 - 無線LAN設定
 - 暗号化設定
 - AP間通信設定
 - IEEE802.11a
 - 無線LAN設定
 - 暗号化設定
 - AP間通信設定

無線LAN設定 [IEEE802.11g]

無線LANを使用するときの設定を行います。

登録 取消 登録して再起動 このページの設定は再起動後に有効になります。

無線LAN設定		
IEEE802.11gを使用	①	<input type="radio"/> しない <input checked="" type="radio"/> する
SSID	②	**
SSIDの確認入力	③	**
ANYを拒否	④	<input checked="" type="radio"/> しない <input type="radio"/> する
チャンネル	⑤	11 (2462MHz)
Rts/Ctsスレッシュホール⑥	⑥	無し
11g保護機能	⑦	無効
パワーレベル	⑧	高
接続端末制限	⑨	255

⑥ Rts/Ctsスレッシュ

ホールド

ネゴシエーションするために送るパケットのデータサイズを、「500バイト」または「1000バイト」から選択します。

(出荷時の設定：無し)

Rts/Cts(Request to Send/Clear to Send)スレッシュホールドを設定すると、隠れ端末の影響による通信速度の低下を防止できます。

隠れ端末とは、下図のように、それぞれが本製品[B]と無線通信できても、互いが直接通信できない無線パソコン[A]-[C]どうし([A]に対して[C]、[C]に対して[A])のことを呼びます。

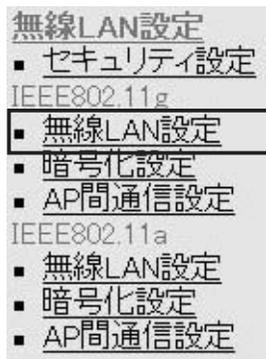
通信の衝突を防止するには、無線パソコン[A]から送信要求(Rts)信号を受信した本製品[B]が、無線伝送エリア内にある無線パソコン[A]および[C]に送信可能(Cts)信号を送り返すことで、Rts信号を送信していない無線パソコン[C]に本製品[B]が隠れ端末と通信中であることを認識させます。これにより、Rts信号を送信していない無線パソコン[C]は、本製品[B]から受信完了通知(ACK)を受信するまで本製品[B]へのアクセスを自制して、通信の衝突を防止できます。



2 「無線LAN設定」メニュー

2-2.「無線LAN設定」画面[IEEE802.11g]

■無線LAN設定(つづき)



無線LAN設定 [IEEE802.11g]
無線LANを使用するときの設定を行います。

このページの設定は再起動後に有効になります。

無線LAN設定		
IEEE802.11gを使用	①	<input type="radio"/> しない <input checked="" type="radio"/> する
SSID	②	<input type="text" value="**"/>
SSIDの確認入力	③	<input type="text" value="**"/>
ANYを拒否	④	<input checked="" type="radio"/> しない <input type="radio"/> する
チャンネル	⑤	<input type="text" value="11(2462MHz)"/>
Rts/Ctsスレッシュホールド	⑥	<input type="text" value="無し"/>
11g保護機能	⑦	<input type="text" value="無効"/>
パワーレベル	⑧	<input type="text" value="高"/>
接続端末制限	⑨	<input type="text" value="255"/>

⑦ 11g保護機能

無線LAN規格でアクセス制限するとき設定します。

(出荷時の設定：無効)

設定することで、[IEEE802.11b(11Mbps)]規格の通信を制限して、[IEEE802.11g(54Mbps)]規格の通信が[IEEE802.11b]規格の通信により影響を受けないように保護します。

◎「無効」：[IEEE802.11g]規格または[IEEE802.11b]規格の無線パソコンと通信できます。

◎「有効」：[IEEE802.11b]規格と混在するネットワーク環境で、[IEEE802.11g]規格の通信速度が極端に遅い場合に設定します。

「有効」に設定すると、[IEEE802.11g]規格の無線パソコンとの通信を優先させます。

優先させることで、[IEEE802.11g]規格の通信速度が低下することを防止できます。

◎「g専用」：[IEEE802.11g]規格の無線パソコンとだけ通信できます。

2-2.「無線LAN設定」画面[IEEE802.11g]

■無線LAN設定(つづき)



無線LAN設定 [IEEE802.11g]

無線LANを使用するときの設定を行います。

登録 取消 登録して再起動 このページの設定は再起動後に有効になります。

無線LAN設定

IEEE802.11gを使用	①	<input type="radio"/> しない <input checked="" type="radio"/> する
SSID	②	**
SSIDの確認入力	③	**
ANYを拒否	④	<input checked="" type="radio"/> しない <input type="radio"/> する
チャンネル	⑤	11 (2462MHz)
Rts/Ctsスレッシュホールド	⑥	無し
11g保護機能	⑦	無効
パワーレベル	⑧	高
接続端末制限	⑨	255

⑧ パワーレベル ……………

内蔵された[IEEE802.11g]対応無線LANカードの送信出力を設定します。 (出荷時の設定：高)

高/中/低(3段階)の中から選択できます。

本製品の最大伝送距離は、パワーレベルが「高」の場合です。

パワーレベルを低くすると、それに比例して伝送距離も短くなります。

【パワーレベルを低くする目的について】

- ◎本製品から送信される電波が部屋の外に漏れるのを防止したいとき
- ◎通信エリアを制限してセキュリティーを高めたいとき
- ◎比較的狭いエリアに複数台の無線アクセスポイントが設置された環境で、近くの無線クライアントや無線アクセスポイントとの電波干渉を無くして、通信速度の低下などを防止したいとき

⑨ 接続端末制限 ……………

本製品に同時接続可能な無線パソコンの台数を設定します。

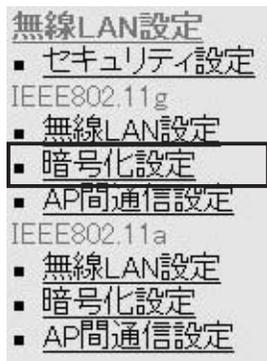
設定できる範囲は、「1～255」です。 (出荷時の設定：255)

接続制限されていると、接続が集中することで通信速度が低下するのを防止できます。(負荷分散機能)

2 「無線LAN設定」メニュー

2-3.「暗号化設定」画面[IEEE802.11g]

■ 暗号化設定



54Mbps(2.4GHz)の無線LANで通信するデータを保護するために、無線送信データを暗号化するための設定です。

※無線AP間通信する場合も、本製品どうしおよび無線パソコンが同じ暗号化鍵(キー)を設定しないと通信できません。

暗号化設定 [IEEE802.11g]

無線LANを使用するときの暗号化に関する設定を行います。
認証方式は暗号化方式が「RC4」以外の時は「オープンシステム」のみ設定可能です。
キーの自動変更はRADIUS機能を使用する場合のみ有効です。

このページの設定は再起動後に有効になります。

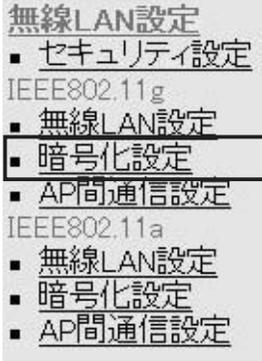
暗号化設定

認証モード	①	<input type="text" value="両対応"/>
暗号化方式	②	<input type="text" value="なし"/>
キージェネレータ	③	<input type="text"/>
ファクター	④	<input type="text" value="0"/>
キーID	⑤	<input type="text" value="1"/>
キーの自動変更を使用	⑥	<input type="checkbox"/> しない <input checked="" type="checkbox"/> する

- <登録> ボタン 「暗号化設定」画面で変更したすべての設定内容が有効になります。
- <取消> ボタン 「暗号化設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお <登録> をクリックすると、変更前の状態には戻りません。
- <登録して再起動> ボタン 本製品を再起動して、[暗号化設定]項目で変更したすべての設定内容を有効にします。
- ① 認証モード 暗号化を使用する無線LANからのアクセスに対する認証方式を設定します。(出荷時の設定：両対応)
※通信相手と認証モードが異なると通信できません。
- ◎両対応 : 無線LANのアクセスに対して、「オープンシステム」と「シェアードキー」を自動認識しますので、通信相手間で暗号化鍵(キー)が同じであれば通信可能です。
 - ◎オープンシステム : 無線LANのアクセスに対して認証を行いません。
 - ◎シェアードキー : 無線LANのアクセスに対して通信相手と同じ暗号化鍵(キー)かどうかを認証します。

2-3.「暗号化設定」画面[IEEE802.11g]

■ 暗号化設定(つづき)



暗号化設定 [IEEE802.11g]

無線LANを使用するときの暗号化に関する設定を行います。
認証方式は暗号化方式が「RC4」以外の時は「オープンシステム」のみ設定可能です。
キーの自動変更はRADIUS機能を使用する場合のみ有効です。

登録 取消 登録して再起動 このページの設定は再起動後に有効になります。

暗号化設定		
認証モード	①	両対応
暗号化方式	②	なし
キージェネレータ	③	
ファクター	④	0
キーID	⑤	1
キーの自動変更を使用	⑥	<input type="checkbox"/> しない <input checked="" type="checkbox"/> する

- ② 暗号化方式
 ※「WEP RC4」と「OCB AES」には、互換性はありません。

無線伝送データを暗号化する方式と暗号化ビット数を選択します。
 (出荷時の設定：なし)

暗号化方式には、「WEP RC4」、「OCB AES」があります。
 通信を行う相手間で、ビット数も含め同じ方式を選択してください。

◎WEP RC4

無線LAN機器の暗号化として一般によく搭載されている暗号化方式です。

暗号化方式は、RC4(Rivest's Cipher 4)アルゴリズムをベースに構成されています。

暗号化するデータのブロック長が8ビットで、暗号化鍵(キー)の長さを選択できます。

※選択できる暗号化鍵(キー)の長さは、64(40)/128(104)/152(128)ビットの中から選択できます。

◎OCB AES

WEP RC4より強力で、標準化が推進されている次世代の暗号化方式です。

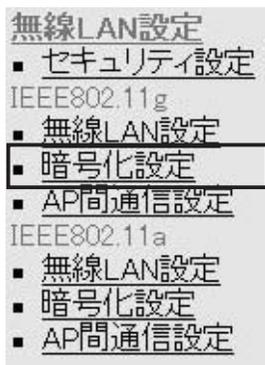
暗号化するデータのブロック長と暗号化鍵(キー)の長さは、128ビットです。

この128ビットに対して任意に鍵(キー)を設定できますので、[WEP RC4]より強力な暗号化方式です。

2 「無線LAN設定」メニュー

2-3.「暗号化設定」画面[IEEE802.11g]

■ 暗号化設定(つづき)



暗号化設定 [IEEE802.11g]

無線LANを使用するときの暗号化に関する設定を行います。
認証方式は暗号化方式が「RC4」以外の時は「オープンシステム」のみ設定可能です。
キーの自動変更はRADIUS機能を使用する場合のみ有効です。

このページの設定は再起動後に有効になります。

暗号化設定

認証モード	①	<input type="text" value="両対応"/>
暗号化方式	②	<input type="text" value="なし"/>
キージェネレータ	③	<input type="text"/>
ファクター	④	<input type="text" value="0"/>
キーID	⑤	<input type="text" value="1"/>
キーの自動変更を使用	⑥	<input type="checkbox"/> しない <input type="checkbox"/> する

③ キージェネレータ ……………

暗号化および復号に使う鍵(キー)を生成するための文字列を設定します。

通信を行う相手間で同じ文字列(大文字/小文字の区別に注意して、任意の半角英数字/記号)を31文字以内で設定します。

なお、入力した文字はすべて「*(アスタリスク)」で表示します。

(表示例：**)

「暗号化方式」を選択して、〈登録〉をクリックすると、[キージェネレータ]欄に入力した文字列より生成された鍵(キー)を[キー値]項目のテキストボックスに表示します。

[キー値]項目の各キー番号のテキストボックスに生成される桁数および文字数は、選択する「暗号化方式」によって異なります。

詳しくは、取扱説明書[導入編](3-6章) ■ 暗号化鍵(キー)値の入力について)をご覧ください。

※「WEP RC4」の場合、先頭の24ビットは、一定時間ごとに内容を自動更新して設定されますので、「キー値」項目のテキストボックスには表示されません。

※[キー値]項目の[入力モード]が「ASCII文字」に設定されている場合は、キージェネレータを使用できません。

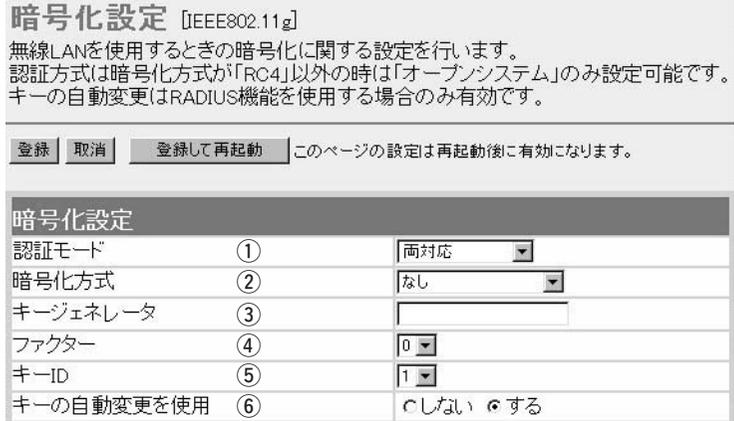
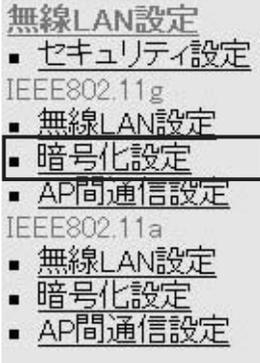
※[暗号化方式]欄で「なし」が選択されていると、[キー値]項目の各キー番号のテキストボックスに鍵(キー)が生成されません。

※通信相手間で文字列が異なる場合、暗号化されたデータを復号できません。

※[キー値]項目から直接設定するときは、[キージェネレータ]欄には何も表示されません。

2-3.「暗号化設定」画面[IEEE802.11g]

■ 暗号化設定(つづき)



④ ファクター ……………

暗号化するレベルを設定します。(出荷時の設定：0)
 通信する相手間で異なるレベルを設定しても通信できます。
 「0」を選択すると、一番セキュリティが高くなります。
 各値の暗号化レベルは、次のようになります。
 「0」＝ 1パケットごとに内部暗号キーを変更する
 「1」＝ 10パケットごとに内部暗号キーを変更する
 「2」＝ 50パケットごとに内部暗号キーを変更する
 「3」＝ 100パケットごとに内部暗号キーを変更する

⑤ キーID ……………

暗号化に使用する鍵(キー)番号を設定します。(出荷時の設定：1)
 鍵(キー)番号は、通信する相手間でそれぞれ任意に選択できます。
 [暗号化設定]項目の[暗号化方式]欄で、「WEP RC4」または「OCB AES」が登録されているときは、「1」～「4」の中から選択できます。

⑥ キーの自動変更を使用 ……

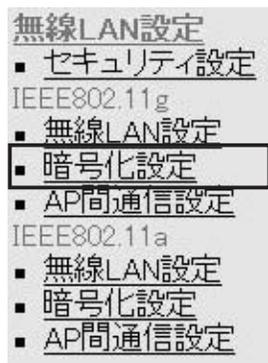
本製品のRADIUS機能を使用するとき有効な機能で、Windows X P 標準のワイヤレスネットワーク接続を使って本製品に I E E E 802.1x 認証でアクセスする無線パソコンに対して、RADIUSサーバから定期的に異なるキーをその無線パソコンに自動で割り当てる機能を使用して認証させるとき設定します。
 ※無線LANカードに付属の設定ユーティリティによっては、この機能に対応していませんので、この設定ユーティリティを Windows X P にインストールして使用している無線パソコンに対しては、機能しません。

2 「無線LAN設定」メニュー

2-3.「暗号化設定」画面[IEEE802.11g](つづき)

■ キー値

暗号化鍵(キー)を直接入力するための設定です。



① 入力モード ……………

暗号化鍵(キー)の入力のしかたを選びます。

(出荷時の設定：16進数)

※入力モードを変更したときは、「暗号化設定」画面の〈登録〉ボタンをクリックしてから、暗号化鍵(キー)を入力してください。

※ASCII文字が設定されているときは、キージェネレータを使用できません。

② 鍵(キー)入力用ボックス …

キージェネレータを使用しないとき、暗号化および復号に使用する鍵(キー)を、[入力モード]欄で設定された方法で、直接入力します。

(出荷時の設定：00-00-00-00-00)

16進数表記で使用する以外のアルファベットを入力しても無効です。

[キー値]は、通信する相手間で、使用するキーIDに対する鍵(キー)の内容を同じに設定してください。

使用するキーIDに対する鍵(キー)の内容が違うときは通信できません。

2-3.「暗号化設定」画面[IEEE802.11g](つづき)

■ご参考に 次の表は、取扱説明書[導入編](☞3-6章)にも掲載されています。設定の参考にしてください。

【入力する桁数および文字数】

設定によってキー入力用ボックスに入力する桁数および文字数が下記のように異なります。

認証モード	入力モード		16進数 (HEX)	ASCII文字
	暗号化方式			
オープンシステム	シェアードキー	WEP RC4 64(40)ビット	10桁	5文字(半角)
		WEP RC4 128(104)ビット	26桁	13文字(半角)
		WEP RC4 152(128)ビット	32桁	16文字(半角)
		OCB AES 128(128)ビット	32桁	16文字(半角)

※入力できる桁数および文字数は、()内のビット数に対する値です。

【ASCII文字→16進数変換表】

ご使用になる無線LANカードや無線LAN対応のパソコンが両方の入力モードに対応していない場合は、下記の変換表を参考にパソコンに設定するキーを指示してください。

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

2 「無線LAN設定」メニュー

2-4. キー値の設定例

「WEP RC4 128(104)」ビットの暗号化方式を例に、[キー値]項目のテキストボックスに鍵(キー)を16進数(26桁)で直接入力する場合の設定例を説明します。

※例として、キーID「2」と「3」に、「48-6f-74-73-70-6f-74-41-63-63-65-73-73」と「57-41-56-45-4d-41-53-54-45-52-4c-41-4e」を下記のように入力します。

※暗号化鍵(キー)の設定は、802.11a規格(5.2GHz帯)と802.11g規格(2.4GHz帯)で別々に行えます。

■ 無線アクセスポイント通信の場合

◎キーID「2」の鍵(キー)が同じなので通信できます。

RDA5000側

キーID	2
キー値	
入力モード	<input checked="" type="radio"/> 16進数 <input type="radio"/> ASCII文字
1	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
2	48-6F-74-73-70-6F-74-41-63-63-65-73-73
3	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
4	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

双方向通信可能



無線LANカード側(イメージ)

キーID	02
キー	値
01	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
02	48-6F-74-73-70-6F-74-41-63-63-65-73-73
03	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
04	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
<input checked="" type="radio"/> 16進数入力 <input type="radio"/> ASCII文字入力	

◎キーID「2」とキーID「3」の鍵(キー)が同じなので通信できます。

RDA5000側

キーID	2
キー値	
入力モード	<input checked="" type="radio"/> 16進数 <input type="radio"/> ASCII文字
1	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
2	48-6F-74-73-70-6F-74-41-63-63-65-73-73
3	57-41-56-45-4D-41-53-54-45-52-4C-41-4E
4	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

双方向通信可能



無線LANカード側(イメージ)

キーID	03
キー	値
01	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
02	48-6F-74-73-70-6F-74-41-63-63-65-73-73
03	57-41-56-45-4D-41-53-54-45-52-4C-41-4E
04	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
<input checked="" type="radio"/> 16進数入力 <input type="radio"/> ASCII文字入力	

◎キーID「2」とキーID「3」の鍵(キー)が異なるので通信できません。

RDA5000側

キーID	2
キー値	
入力モード	<input checked="" type="radio"/> 16進数 <input type="radio"/> ASCII文字
1	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
2	48-6F-74-73-70-6F-74-41-63-63-65-73-73
3	57-41-56-45-4D-41-53-54-45-52-4C-41-4E
4	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

通信不可能



無線LANカード側(イメージ)

キーID	03
キー	値
01	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
02	57-41-56-45-4D-41-53-54-45-52-4C-41-4E
03	48-6F-74-73-70-6F-74-41-63-63-65-73-73
04	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
<input checked="" type="radio"/> 16進数入力 <input type="radio"/> ASCII文字入力	

2-4. キー値の設定例(つづき)

■ 無線AP(アクセスポイント)間通信の場合

◎ キーID「2」とキーID「3」の鍵(キー)が同じなので通信できます。

キーID 2

キー値

入力モード 16進数 ASCII文字

1 00-00-00-00-00-00-00-00-00-00-00-00

2 48-6F-74-73-70-6F-74-41-63-63-65-73-73

3 57-41-56-45-4D-41-53-54-45-52-4C-41-4E

4 00-00-00-00-00-00-00-00-00-00-00-00

双方向通信可能

キーID 3

キー値

入力モード 16進数 ASCII文字

1 00-00-00-00-00-00-00-00-00-00-00-00

2 48-6F-74-73-70-6F-74-41-63-63-65-73-73

3 57-41-56-45-4D-41-53-54-45-52-4C-41-4E

4 00-00-00-00-00-00-00-00-00-00-00-00

◎ キーID「2」とキーID「3」の鍵(キー)が異なるので通信できません。

キーID 2

キー値

入力モード 16進数 ASCII文字

1 00-00-00-00-00-00-00-00-00-00-00-00

2 48-6F-74-73-70-6F-74-41-63-63-65-73-73

3 57-41-56-45-4D-41-53-54-45-52-4C-41-4E

4 00-00-00-00-00-00-00-00-00-00-00-00

通信不可能

キーID 3

キー値

入力モード 16進数 ASCII文字

1 00-00-00-00-00-00-00-00-00-00-00-00

2 57-41-56-45-4D-41-53-54-45-52-4C-41-4E

3 48-6F-74-73-70-6F-74-41-63-63-65-73-73

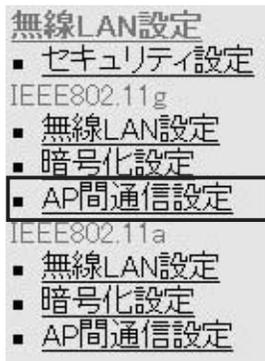
4 00-00-00-00-00-00-00-00-00-00-00-00

2 「無線LAN設定」メニュー

2-5.「AP間通信設定」画面[IEEE802.11g]

■ IEEE802.11g BSSID

本製品に内蔵する54Mbps(2.4GHz帯)無線LANカードの[BSSID]を表示します。



AP間通信設定 [IEEE802.11g]

AP間通信 (Wireless Bridge) 機能の設定を行います。

IEEE802.11g BSSID

00-90-C7-6D-00-10

画面に表示された[BSSID]を相手側のRDA5000に登録します。また、本製品には相手側の[BSSID]を「通信AP設定」に登録します。

■ 通信AP設定

54Mbps(5.2GHz帯)でAP間通信するとき設定します。

通信AP設定	
登録の追加 ①	
BSSID	<input type="text"/>
	<input type="button" value="追加"/>
現在の登録 ②	
BSSID	<input type="text"/>

① 登録の追加 ……………

AP間通信する相手(RDA5000)の[BSSID]を入力します。

※ <追加> をクリックすると、入力した[BSSID]が有効になります。

※最大6台分の[BSSID]が登録できます。

※[BSSID]の入力は、半角英数字で12桁(16進数)を入力します。

※[BSSID]を次のように入力すると、同じ[BSSID]として処理します。

(入力例：00-90-c7-6D-00-30、0090c76D0030)

② 現在の登録 ……………

本製品に登録されている[BSSID]を表示します。

この欄に登録されている[BSSID]を持つ機器と本製品のあいだでAP間通信できます。

【登録例】

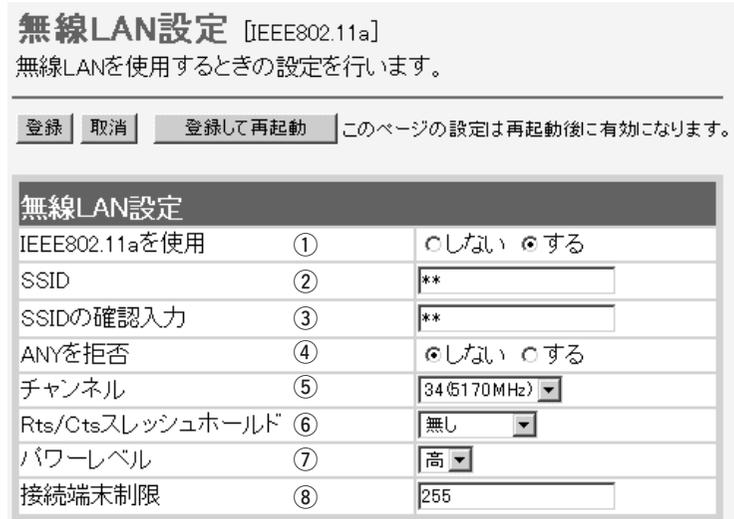
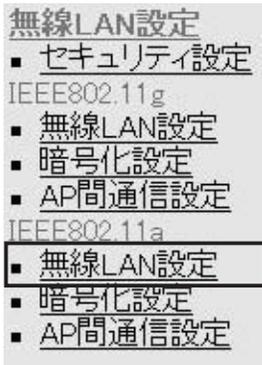
登録した内容を取り消すときは、該当する欄の<削除>をクリックします。

現在の登録	
BSSID	<input type="text"/>
00-90-C7-6D-00-30	<input type="button" value="削除"/>

2-6. 「無線LAN設定」画面 [IEEE802.11a]

■ 無線LAN設定

54Mbps(5.2GHz帯)の内蔵無線LANカードに対する設定です。



〈登録〉ボタン ……………

[IEEE802.11aを使用]欄以外の設定内容が有効になります。
 ※[IEEE802.11aを使用]欄を変更した場合は、画面上で確定されますが、〈登録して再起動〉をクリックするまで有効になりません。

〈取消〉ボタン ……………

[無線LAN設定]項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
 なお〈登録〉をクリックすると、変更前の状態には戻りません。

〈登録して再起動〉ボタン ……

本製品を再起動して、[無線LAN設定]項目で変更したすべての設定内容を有効にします。

① IEEE802.11aを使用 ……

IEEE802.11a(5.2GHz帯)規格の無線アクセスポイント機能を無効にするとき設定します。
 (出荷時の設定：する)

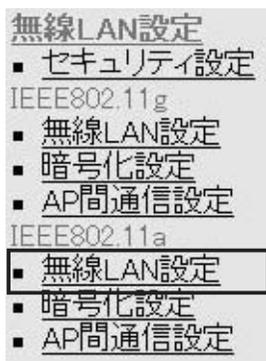
② SSID……………

無線ルータや無線アクセスポイントが無線伝送エリア内に数台存在しているような場合、個々の無線ネットワークグループを[SSID(無線ネットワーク名)]で識別したり、異なる無線ネットワーク名で通信するグループからの混信を防止します。
 この[SSID]が異なると本製品と無線で通信できません。
 セキュリティというよりは、むしろ無線ネットワークのグループ分けを設定するために使用します。
 大文字/小文字の区別に注意して、任意の英数字、半角31文字以内で入力します。
 (出荷時の設定：LG)
 また、入力した文字はすべて「*(アスタリスク)」で表示されます。
 (表示例：**)
 ※本製品以外の無線LAN機器では、[ESSID]と表記されている場合があります。

2 「無線LAN設定」メニュー

2-6.「無線LAN設定」画面[IEEE802.11a]

■無線LAN設定(つづき)



無線LAN設定 [IEEE802.11a]
無線LANを使用するときの設定を行います。

登録 取消 登録して再起動 このページの設定は再起動後に有効になります。

無線LAN設定		
IEEE802.11aを使用	①	<input type="radio"/> しない <input checked="" type="radio"/> する
SSID	②	<input type="text" value="**"/>
SSIDの確認入力	③	<input type="text" value="**"/>
ANYを拒否	④	<input checked="" type="radio"/> しない <input type="radio"/> する
チャンネル	⑤	<input type="text" value="34(5170MHz)"/>
Rts/Ctsスレッシュホールド*	⑥	<input type="text" value="無し"/>
パワーレベル	⑦	<input type="text" value="高"/>
接続端末制限	⑧	<input type="text" value="255"/>

- ③ SSIDの確認入力 …………… 確認のため、[SSID]を再入力します。 (表示例：**)
- ④ ANYを拒否 …………… 「ANY」モード(アクセスポイント自動検索接続機能)で動作している無線パソコンからの検索や接続を拒否するかしないかを設定します。 (出荷時の設定：しない)
出荷時の設定では、無線LANカードを装着するパソコンとの接続が容易になるように、これらの無線パソコンからの検索や接続を許可しています。
この設定を「する」にした場合、「ANY」モードで通信する無線パソコンが使用する「Windows XP標準のワイヤレスネットワーク接続」や「無線ネット表示に対応する無線LANカードに付属の設定ユーティリティ」に検索されません。
- ⑤ チャンネル …………… 本製品が5.2GHz帯(IEEE802.11a規格)の無線通信に使用する無線通信チャンネルを設定します。 (出荷時の設定：34(5170MHz))
※本製品どうしを無線AP間通信するときは、同じチャンネルに設定してください。
※無線パソコン側は、本製品のチャンネルを自動的に検知して通信します。
※近くに5.2GHz帯(IEEE802.11a規格)の無線アクセスポイント機能で通信する別の無線ネットワークグループが存在する場合でも、互いを異なるチャンネルに設定していれば、チャンネル間の電波干渉に配慮する必要はありません。

2-6.「無線LAN設定」画面[IEEE802.11a]

■無線LAN設定(つづき)

- 無線LAN設定
- セキュリティ設定
- IEEE802.11g
- 無線LAN設定
 - 暗号化設定
 - AP間通信設定
- IEEE802.11a
- 無線LAN設定
 - 暗号化設定
 - AP間通信設定

無線LAN設定 [IEEE802.11a]
無線LANを使用するときの設定を行います。

登録 取消 登録して再起動 このページの設定は再起動後に有効になります。

無線LAN設定		
IEEE802.11aを使用	①	<input type="radio"/> しない <input checked="" type="radio"/> する
SSID	②	**
SSIDの確認入力	③	**
ANYを拒否	④	<input checked="" type="radio"/> しない <input type="radio"/> する
チャンネル	⑤	34 (5170MHz)
Rts/Ctsスレッシュホールド	⑥	無し
パワーレベル	⑦	高
接続端末制限	⑧	255

⑥ Rts/Ctsスレッシュ
ホールド

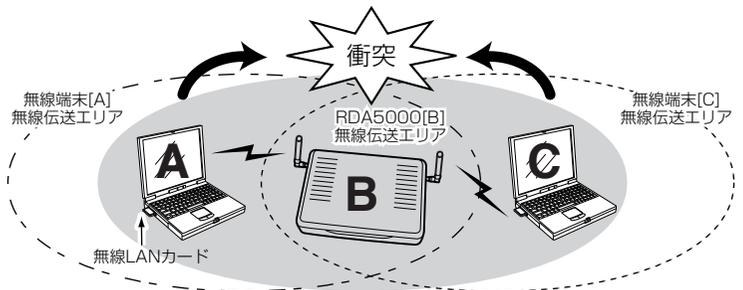
ネゴシエーションするために送るパケットのデータサイズを、「500バイト」または「1000バイト」から選択します。

(出荷時の設定：無し)

Rts/Cts(Request to Send/Clear to Send)スレッシュホールドを設定すると、隠れ端末の影響による通信速度の低下を防止できます。

隠れ端末とは、下図のように、それぞれが本製品[B]と無線通信できても、互いが直接通信できない無線パソコン[A]-[C]どうし([A]に対して[C]、[C]に対して[A])のことを呼びます。

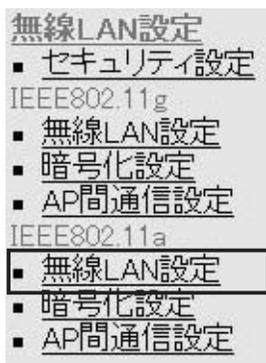
通信の衝突を防止するには、無線パソコン[A]から送信要求(Rts)信号を受信した本製品[B]が、無線伝送エリア内にある無線パソコン[A]および[C]に送信可能(Cts)信号を送り返すことで、Rts信号を送信していない無線パソコン[C]に本製品[B]が隠れ端末と通信中であることを認識させます。これにより、Rts信号を送信していない無線パソコン[C]は、本製品[B]から受信完了通知(ACK)を受信するまで本製品[B]へのアクセスを自制して、通信の衝突を防止できます。



2 「無線LAN設定」メニュー

2-6.「無線LAN設定」画面[IEEE802.11a]

■無線LAN設定(つづき)



無線LAN設定 [IEEE802.11a]

無線LANを使用するときの設定を行います。

登録 取消 登録して再起動 このページの設定は再起動後に有効になります。

無線LAN設定		
IEEE802.11aを使用	①	<input type="radio"/> しない <input checked="" type="radio"/> する
SSID	②	<input type="text" value="**"/>
SSIDの確認入力	③	<input type="text" value="**"/>
ANYを拒否	④	<input checked="" type="radio"/> しない <input type="radio"/> する
チャンネル	⑤	<input type="text" value="34(5170MHz)"/>
Rts/Ctsスレッシュホールド	⑥	<input type="text" value="無し"/>
パワーレベル	⑦	<input type="text" value="高"/>
接続端末制限	⑧	<input type="text" value="255"/>

⑦ パワーレベル

内蔵された[IEEE802.11a]対応無線LANカードの送信出力を設定します。 (出荷時の設定：高)

高/中/低(3段階)の中から選択できます。

本製品の最大伝送距離は、パワーレベルが「高」の場合です。

パワーレベルを低くすると、それに比例して伝送距離も短くなります。

【パワーレベルを低くする目的について】

◎本製品から送信される電波が部屋の外に漏れるのを防止したいとき

◎通信エリアを制限してセキュリティーを高めたいとき

◎比較的狭いエリアに複数台の無線アクセスポイントが設置された環境で、近くの無線クライアントや無線アクセスポイントとの電波干渉を無くして、通信速度の低下などを防止したいとき

⑧ 接続端末制限

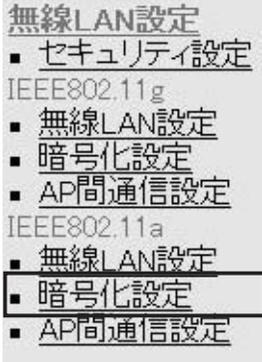
本製品に同時接続可能な無線パソコンの台数を設定します。

設定できる範囲は、「1～255」です。 (出荷時の設定：255)

接続制限されていると、接続が集中することで通信速度が低下するのを防止できます。(負荷分散機能)

2-7.「暗号化設定」画面[IEEE802.11a]

■ 暗号化設定



54Mbps(5.2GHz)の無線LANで通信するデータを保護するために、通信データを暗号化するための設定です。

※無線AP間通信する場合も、本製品どうしおよび無線パソコンが同じ暗号化鍵(キー)を設定しないと通信できません。

暗号化設定 [IEEE802.11a]

無線LANを使用するときの暗号化に関する設定を行います。
 認証方式は暗号化方式が「RC4」以外の時は「オープンシステム」のみ設定可能です。
 キーの自動変更はRADIUS機能を使用する場合のみ有効です。

登録 取消 登録して再起動 このページの設定は再起動後に有効になります。

暗号化設定		
認証モード	①	両対応
暗号化方式	②	なし
キージェネレータ	③	
ファクター	④	0
キーID	⑤	1
キーの自動変更を使用	⑥	<input type="radio"/> しない <input checked="" type="radio"/> する

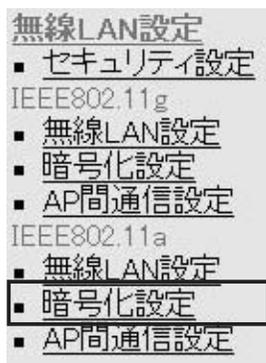
- 〈登録〉ボタン …………… 「暗号化設定」画面で変更した内容を画面上で確定するボタンです。
 ※ 〈登録して再起動〉をクリックするまで有効になりません。
- 〈取消〉ボタン …………… 「暗号化設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
 なお 〈登録〉をクリックすると、変更前の状態には戻りません。
- 〈登録して再起動〉ボタン …… 本製品を再起動して、「暗号化設定」画面で変更したすべての設定内容を有効にします。
- ① 認証モード …………… 暗号化を使用する無線LANからのアクセスに対する認証方式を設定します。 (出荷時の設定：両対応)
 ※通信相手と認証モードが異なると通信できません。

 - ◎両対応 : 無線LANのアクセスに対して、「オープンシステム」と「シェアードキー」を自動認識しますので、通信相手間で暗号化鍵(キー)が同じであれば通信可能です。
 - ◎オープンシステム : 無線LANのアクセスに対して認証を行いません。
 - ◎シェアードキー : 無線LANのアクセスに対して通信相手と同じ暗号化鍵(キー)かどうかを認証します。

2 「無線LAN設定」メニュー

2-7.「暗号化設定」画面[IEEE802.11a]

■ 暗号化設定(つづき)



暗号化設定 [IEEE802.11a]

無線LANを使用するときの暗号化に関する設定を行います。
認証方式は暗号化方式が「RC4」以外の時は「オープンシステム」のみ設定可能です。
キーの自動変更はRADIUS機能を使用する場合のみ有効です。

登録 取消 登録して再起動 このページの設定は再起動後に有効になります。

暗号化設定

認証モード	①	両対応
暗号化方式	②	なし
キージェネレータ	③	
ファクター	④	0
キーID	⑤	1
キーの自動変更を使用	⑥	<input type="radio"/> しない <input checked="" type="radio"/> する

- ② 暗号化方式 ………………
※「WEP RC4」と「OCB AES」には、互換性はありません。

無線伝送データを暗号化する方式と暗号化ビット数を選択します。
(出荷時の設定：なし)

暗号化方式には、「WEP RC4」、「OCB AES」があります。
通信を行う相手間で、ビット数も含め同じ方式を選択してください。

◎WEP RC4

無線LAN機器の暗号化として一般によく搭載されている暗号化方式です。

暗号化方式は、RC4(Rivest's Cipher 4)アルゴリズムをベースに構成されています。

暗号化するデータのブロック長が8ビットで、暗号化鍵(キー)の長さを選択できます。

※選択できる暗号化鍵(キー)の長さは、64(40)/128(104)/152(128)ビットの中から選択できます。

◎OCB AES

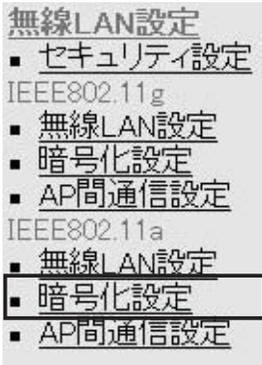
WEP RC4より強力で、標準化が推進されている次世代の暗号化方式です。

暗号化するデータのブロック長と暗号化鍵(キー)の長さは、128ビットです。

この128ビットに対して任意に鍵(キー)を設定できますので、[WEP RC4]より強力な暗号化方式です。

2-7.「暗号化設定」画面[IEEE802.11a]

■ 暗号化設定(つづき)



暗号化設定 [IEEE802.11a]

無線LANを使用するときの暗号化に関する設定を行います。
 認証方式は暗号化方式が「RC4」以外の時は「オープンシステム」のみ設定可能です。
 キーの自動変更はRADIUS機能を使用する場合のみ有効です。

登録 取消 登録して再起動 このページの設定は再起動後に有効になります。

暗号化設定		
認証モード	①	両対応 ▼
暗号化方式	②	なし ▼
キージェネレータ	③	<input type="text"/>
ファクター	④	0 ▼
キーID	⑤	1 ▼
キーの自動変更を使用	⑥	<input type="radio"/> しない <input checked="" type="radio"/> する

③ キージェネレータ ……………

暗号化および復号に使う鍵(キー)を生成するための文字列を設定します。

通信を行う相手間で同じ文字列(大文字/小文字の区別に注意して、任意の半角英数字/記号)を31文字以内で設定します。

なお、入力した文字はすべて「*(アスタリスク)」で表示します。

(表示例：**)

「暗号化方式」を選択して、〈登録〉をクリックすると、[キージェネレータ]欄に入力した文字列より生成された鍵(キー)を[キー値]項目のテキストボックスに表示します。

[キー値]項目の各キー番号のテキストボックスに生成される桁数および文字数は、選択する「暗号化方式」によって異なります。

詳しくは、取扱説明書[導入編](3-6章 ■ 暗号化鍵(キー)値の入力について)をご覧ください。

※「WEP RC4」の場合、先頭の24ビットは、一定時間ごとに内容を自動更新して設定されますので、「キー値」項目のテキストボックスには表示されません。

※[キー値]項目の[入力モード]が「ASCII文字」に設定されている場合は、キージェネレータを使用できません。

※[暗号化方式]欄で「なし」が選択されていると、[キー値]項目の各キー番号のテキストボックスに鍵(キー)が生成されません。

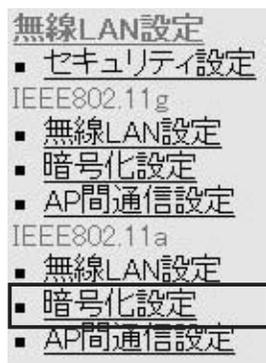
※通信相手間で文字列が異なる場合、暗号化されたデータを復号できません。

※[キー値]項目から直接設定するときは、[キージェネレータ]欄には何も表示されません。

2 「無線LAN設定」メニュー

2-7.「暗号化設定」画面[IEEE802.11a]

■ 暗号化設定(つづき)



暗号化設定 [IEEE802.11a]

無線LANを使用するときの暗号化に関する設定を行います。
認証方式は暗号化方式が「RC4」以外の時は「オープンシステム」のみ設定可能です。
キーの自動変更はRADIUS機能を使用する場合のみ有効です。

登録 取消 登録して再起動 このページの設定は再起動後に有効になります。

暗号化設定

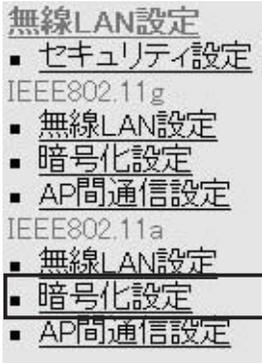
認証モード	①	両対応
暗号化方式	②	なし
キージェネレータ	③	
ファクター	④	0
キーID	⑤	1
キーの自動変更を使用	⑥	<input type="radio"/> しない <input checked="" type="radio"/> する

- ④ **ファクター** 暗号化するレベルを設定します。 (出荷時の設定：0)
通信する相手間で異なるレベルを設定しても通信できます。
「0」を選択すると、一番セキュリティが高くなります。
各値の暗号化レベルは、次のようになります。
「0」= 1パケットごとに内部暗号キーを変更する
「1」= 10パケットごとに内部暗号キーを変更する
「2」= 50パケットごとに内部暗号キーを変更する
「3」= 100パケットごとに内部暗号キーを変更する
- ⑤ **キーID** 暗号化に使用する鍵(キー)番号を設定します。 (出荷時の設定：1)
鍵(キー)番号は、通信する相手間でそれぞれ任意に選択できます。
[暗号化設定]項目の[暗号化方式]欄で、「WEP RC4」または「OCB AES」が登録されているときは、「1」～「4」の中から選択できます。
- ⑥ **キーの自動変更を使用** 本製品のRADIUS機能を使用するとき有効な機能で、Windows X P 標準のワイヤレスネットワーク接続を使って本製品に IEEE 802.1x 認証でアクセスする無線パソコンに対して、RADIUSサーバから定期的に異なるキーをその無線パソコンに自動で割り当てる機能を使用して認証させるとき設定します。
※無線LANカードに付属の設定ユーティリティによっては、この機能に対応していませんので、この設定ユーティリティを Windows X P にインストールして使用している無線パソコンに対しては、機能しません。

2-7.「暗号化設定」画面[IEEE802.11a](つづき)

■ キー値

暗号化鍵(キー)を直接入力するための設定です。



キー値	
入力モード ①	<input checked="" type="radio"/> 16進数 <input type="radio"/> ASCII文字
1	00-00-00-00-00
2	00-00-00-00-00
3	00-00-00-00-00
4	00-00-00-00-00

① 入力モード ……………

暗号化鍵(キー)の入力のしかたを選びます。

(出荷時の設定：16進数)

※入力モードを変更したときは、「暗号化設定」画面の〈登録〉ボタンをクリックしてから、暗号化鍵(キー)を入力してください。

※ASCII文字が設定されているときは、キージェネレータを使用できません。

② 鍵(キー)入力用ボックス …

キージェネレータを使用しないとき、暗号化および復号に使用する鍵(キー)を、[入力モード]欄で設定された方法で、直接入力します。

(出荷時の設定：00-00-00-00-00)

16進数表記で使用する以外のアルファベットを入力しても無効です。

[キー値]は、通信する相手間で、使用するキーIDに対する鍵(キー)の内容を同じに設定してください。

使用するキーIDに対する鍵(キー)の内容が違うときは通信できません。

2 「無線LAN設定」メニュー

2-7.「暗号化設定」画面[IEEE802.11a](つづき)

■ご参考に

次の表は、取扱説明書[導入編]([☞](#)3-6章)にも掲載されています。
設定の参考にしてください。

【入力する桁数および文字数】

設定によってキー入力用ボックスに入力する桁数および文字数が下記のように異なります。

認証モード	入力モード		16進数 (HEX)	ASCII文字
	暗号化方式			
オープン システム	シェアード キー	WEP RC4 64(40)ビット	10桁	5文字(半角)
		WEP RC4 128(104)ビット	26桁	13文字(半角)
		WEP RC4 152(128)ビット	32桁	16文字(半角)
		OCB AES 128(128)ビット	32桁	16文字(半角)

※入力できる桁数および文字数は、()内のビット数に対する値です。

【ASCII文字→16進数変換表】

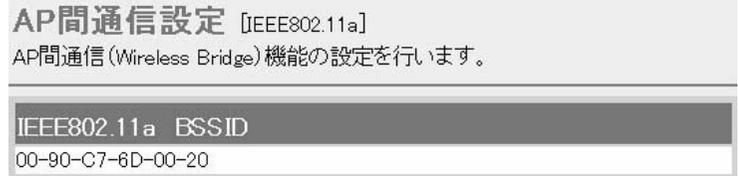
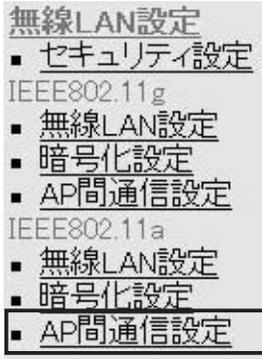
ご使用になる無線LANカードや無線LAN対応のパソコンが両方の入力モードに対応していない場合は、下記の変換表を参考にパソコンに設定するキーを指示してください。

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

2-8.「AP間通信設定」画面[IEEE802.11a]

■ IEEE802.11a BSSID

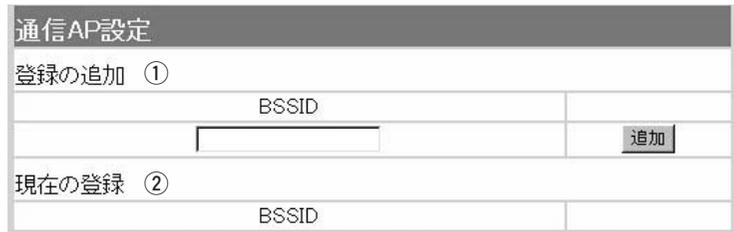
本製品に内蔵する54Mbps(5.2GHz帯)無線LANカードの[BSSID]を表示します。



画面に表示された[BSSID]を相手側のRDA5000に登録します。また、本製品には相手側の[BSSID]を「通信AP設定」に登録します。

■ 通信AP設定

54Mbps(5.2GHz帯)でAP間通信するとき設定します。



① 登録の追加 ……………

AP間通信する相手(RDA5000)の[BSSID]を入力します。
 ※〈追加〉をクリックすると、入力した[BSSID]が有効になります。
 ※最大6台分の[BSSID]が登録できます。
 ※[BSSID]の入力は、半角英数字で12桁(16進数)を入力します。
 ※[BSSID]を次のように入力すると、同じ[BSSID]として処理します。
 (入力例：00-90-c7-6D-00-30、0090c76D0030)

② 現在の登録 ……………

本製品に登録されている[BSSID]を表示します。
 この欄に登録されている[BSSID]を持つ機器と本製品のあいだでAP間通信できます。
【登録例】
 登録した内容を取り消すときは、該当する欄の〈削除〉をクリックします。





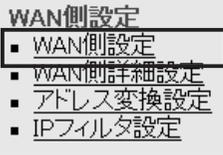
本製品をインターネットと接続するための設定で、ご契約のプロバイダー情報の設定やIPフィルタの設定は、このメニューで行います。

3-1.「WAN側設定」画面	50
■ 接続状況	50
■ 回線種別	51
■ 回線設定PPPoE/DHCP	52
■ 接続設定	53
3-2.「WAN側詳細設定」画面	54
■ 共通詳細設定	54
■ PPPoE詳細設定	56
3-3.「アドレス変換設定」画面	57
■ アドレス変換設定	57
■ パススルー設定	57
■ 静的マスカレードテーブル設定	58
■ DMZホスト機能と静的マスカレード機能の違い	58
■ 静的NATテーブル設定	59
3-4.「IPフィルタ設定」画面	60
■ 不正アクセス検知機能設定	60
■ IPフィルタ設定	62
■ 現在の登録	66

3 「WAN側設定」メニュー

3-1. 「WAN側設定」画面

■ 接続状況



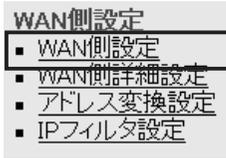
登録された回線への接続状況を表示します。

接続状況		
接続中	①	<input type="button" value="接続"/> <input type="button" value="切断"/>
回線種別	②	DHCP
DNSサーバ	③	
本体側のIPアドレス	④	
相手先のIPアドレス	⑤	
接続時間	⑥	0時間 4分 18秒

- ① 未接続/接続中…………… WAN側回線への接続状況を「未接続」/「接続中」で表示します。
[回線種別]項目で、「接続しない」が設定されているときは、
〈接続〉 / 〈切断〉 ボタンは表示しません。
手動で回線を接続したり、切断するときは、このボタンをクリックします。
- ② 回線種別…………… 現在本製品に設定されている回線への接続方式を表示します。
設定されている接続方式および方法に応じて「PPPoE(手動接続)」
/「PPPoE(自動接続)」/「PPPoE(常時接続)」/「DHCP」のいずれか
を表示します。
- ③ DNSサーバ…………… 「DHCP」/「PPPoE」/「PPPoE複数固定IP」のいずれかが設定され
ている場合、契約されているプロバイダーのDNSサーバIPアドレ
スを表示します。
- ④ 本体側のIPアドレス…………… 「DHCP」/「PPPoE」/「PPPoE複数固定IP」のいずれかが設定され
ている場合、本製品のWAN側に設定されたIPアドレスを表示しま
す。
- ⑤ 相手先のIPアドレス…………… 「DHCP」/「PPPoE」/「PPPoE複数固定IP」のいずれかが設定され
ている場合、契約されているプロバイダーのIPアドレスを表示し
ます。
- ⑥ 接続時間…………… ご契約されているプロバイダーに接続してから、この画面にアク
セスした時点までの時間を表示します。
最新の接続時間を表示させるときは、「WAN側設定」メニューで
「WAN側設定」をクリックします。

3-1.「WAN側設定」画面(つづき)

■ 回線種別



本製品の回線種別についての設定です。



〈登録〉ボタン ……………

[回線種別]項目以外の設定内容が有効になります。
 ※[回線種別]項目を変更した場合は、画面上で確定されますが、
 〈登録して再起動〉をクリックするまで有効になりません。

〈取消〉ボタン ……………

「WAN側設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
 なお 〈登録〉をクリックすると、変更前の状態には戻りません。

〈登録して再起動〉ボタン ……

「WAN側設定」画面で変更したすべての設定内容が有効になります。
 ※[回線種別]項目を変更した場合は、本製品を再起動します。

回線種別 ……………

本製品で使用する回線種別を選択します。

◎接続しない(出荷時の設定)

ルータタイプモデムと接続する場合など、回線を本製品のWAN側ポートに接続しない場合で、本製品を無線アクセスポイントとして使用するとき設定します。

※アッカネットワークスやイー・アクセスをご契約の場合に該当します。

◎PPPoE

回線を本製品のWAN側ポートに接続する場合で、本製品のWAN側IPアドレスを、ご契約のプロバイダーや接続業者から「PPPoE」方式で取得します。

※Bフレッツやフレッツ・ADSLをご契約の場合に該当します。

◎PPPoE複数固定IP

回線を本製品のWAN側ポートに接続する場合で、ご契約のプロバイダーや接続業者から割り当てられた複数のIPアドレスのうち1つを本製品のWAN側IPアドレスに設定し、残りは本製品のLAN側に接続されたパソコンに直接割り当てて使用するとき、設定します。

割り当てられた複数のIPアドレスの使いかたについては、「複数固定IPを使う」(※8章)をご覧ください。

◎DHCP

回線を本製品のWAN側ポートに接続する場合で、本製品のWAN側IPアドレスを、ご契約のプロバイダーや接続業者から「DHCP」方式で取得します。

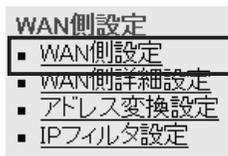
※CATVやYAHOO! BBをご契約の場合に該当します。

3 「WAN側設定」メニュー

3-1. 「WAN側設定」画面(つづき)

■ 回線設定 PPPoE/DHCP

本製品のWAN側についての設定です。



回線設定 PPPoE	
接続先名 ①	<input type="text"/>
IPアドレス ②	<input type="text"/>
サブネットマスク ③	<input type="text"/>
デフォルトゲートウェイ ④	<input type="text"/>
プライマリDNSサーバ ⑤	<input type="text"/>
セカンダリDNSサーバ ⑥	<input type="text"/>

固定のIPアドレスを使用するときのみ入力します。

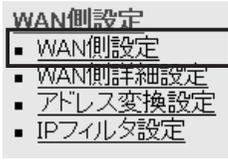
※回線種別を「PPPoE」に設定時の画面を例に説明しています。

※回線種別を「接続しない」に設定時は、表示されません。

- ① 接続先名 ご契約になっているプロバイダーの名前を、任意の英数字、半角31(全角15)文字以内で入力します。
- ② IPアドレス ご契約のプロバイダーやネットワーク管理者から指定されたときに限り、本製品のWAN側IPアドレスを入力します。
- ③ サブネットマスク ご契約のプロバイダーやネットワーク管理者から指定されたときに限り、本製品のWAN側のサブネットマスクを入力します。
- ④ デフォルトゲートウェイ ... ご契約のプロバイダーやネットワーク管理者から指定されたときに限り、本製品のデフォルトゲートウェイを入力します。
- ⑤ プライマリDNSサーバ プロバイダーからDNSサーバのアドレスが2つ指定されている場合は、どちらか一方、または指定されているプライマリDNSアドレスを入力します。
- ⑥ セカンダリDNSサーバ プロバイダーからDNSサーバのアドレスが2つ指定されている場合は、どちらか一方、または指定されているセカンダリDNSアドレスを入力します。

3-1.「WAN側設定」画面(つづき)

■ 接続設定



接続先からの指定に応じて入力します。

接続設定	
ユーザID	⑦ <input type="text"/>
パスワード	⑧ <input type="text"/>
認証プロトコル	⑨ 相手に合わせる ▼

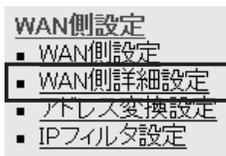
※回線種別を「接続しない」/「DHCP」設定時は、表示されません。

- ⑦ ユーザID プロバイダーから指定されたログインユーザー名またはアカウント名を大文字/小文字の表記に注意して、入力します。
- ⑧ パスワード プロバイダーから指定されたログインパスワードを大文字/小文字の表記に注意して、入力します。
- ⑨ 認証プロトコル ご契約の回線接続業者、またはプロバイダーから指定された認証プロトコルを設定します。
指定のない場合は、「相手に合わせる」(出荷時の設定)でご使用ください。

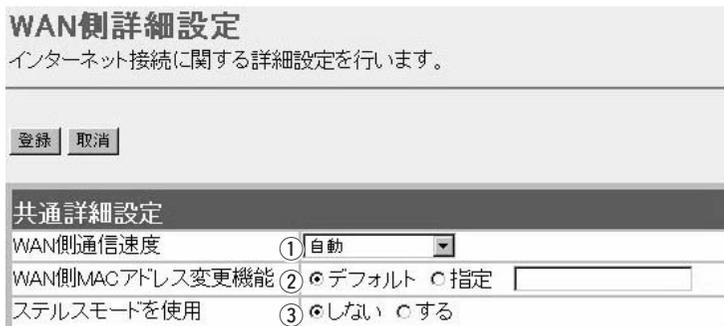
3 「WAN側設定」メニュー

3-2.「WAN側詳細設定」画面

■ 共通詳細設定



本製品のWAN側回線に共通する詳細設定です。



※回線種別を「接続しない」/「DHCP」設定時は、[共通詳細設定]項目だけ表示されます。

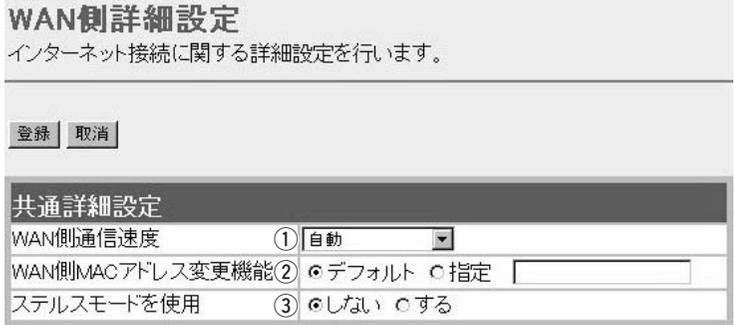
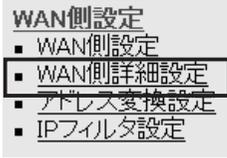
〈登録〉ボタン 「WAN側詳細設定」画面で変更したすべての設定内容が有効になります。

〈取消〉ボタン 「WAN側詳細設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

- ① WAN側通信速度..... 本製品の[WAN]ポートとEthernetケーブルで接続された機器間のリンクスピードの設定です。 (出荷時の設定：自動)
- ◎自動：本製品の[WAN]ポートに接続されている機器の通信速度に合わせて自動で設定されます。
 - ◎100(Half Duplex)
[100Mbps(Half Duplex)]固定で通信します。
本製品の[WAN]ポートに接続されている機器が、[100Mbps(Half Duplex)]に対応しているとき設定できます。
 - ◎100(Full Duplex)
[100Mbps/Full Duplex]固定で通信します。
本製品の[WAN]ポートに接続している機器が、[100Mbps(Full Duplex)]に対応しているとき設定できます。
 - ◎10(Half Duplex)
[10Mbps(Half Duplex)]固定で通信します。
本製品の[WAN]ポートに接続されている機器が、[10Mbps(Half Duplex)]に対応しているとき設定できません。
 - ◎10(Full Duplex)
[10Mbps(Full Duplex)]固定で通信します。
本製品の[WAN]ポートに接続されている機器が、[10Mbps/Full Duplex]に対応しているとき設定できません。

3-2.「WAN側詳細設定」画面

■ 共通詳細設定(つづき)



※回線種別を「接続しない」/「DHCP」設定時は、[共通詳細設定]項目だけ表示されます。

② WAN側MACアドレス
変更機能 ……………

MACアドレス申請が必要なプロバイダーで、すでにインターネットをご使用の場合、プロバイダーに申請されているMACアドレスを入力できます。(出荷時の設定：デフォルト)
申請しているMACアドレスを入力したときは、「指定」のラジオボタンをクリックしてから「登録」をクリックします。

△警告

この機能をご利用になるときは、申請されているMACアドレスをよく確認していただき、設定値を間違えないように注意してください。

設定値を誤ってご使用になられた場合によって生じる結果については一切その責任を負いかねますので、あらかじめご了承ください。

③ ステルスモードを使用 ……

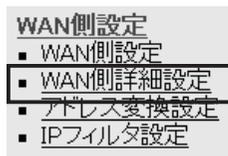
インターネットを使用して本製品に不正アクセスされた場合、Pingやポートスキャンに対して防御するかしないかの設定です。(出荷時の設定：しない)

3 「WAN側設定」メニュー

3-2. 「WAN側詳細設定」画面(つづき)

■ PPPoE詳細設定

「PPPoE」で使用する時設定します。



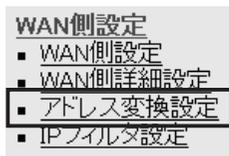
PPPoE詳細設定	
接続設定 ①	<input type="radio"/> 手動 <input checked="" type="radio"/> 自動 <input type="radio"/> 常時
自動切断タイム②	00 分 * 自動接続時のみ有効です。0に設定するとOFFになります。
MSS制限値 ③	1322
ACネーム ④	
サービスネーム⑤	

※回線種別を「接続しない」/「DHCP」設定時は、表示されません。

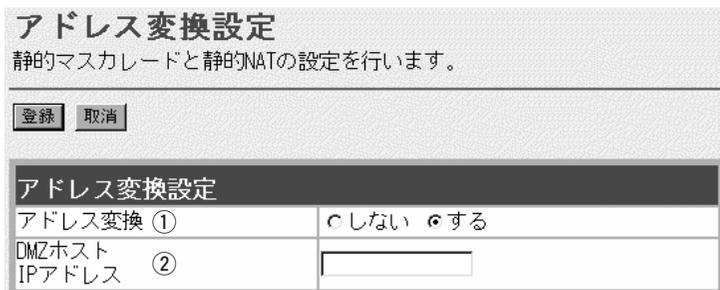
- ① 接続設定 「PPPoE」回線への接続方法を選択します。(出荷時の設定：自動)
◎手動：「WAN側設定」画面の〈接続〉/〈切断〉ボタンで、回線を強制的に接続/切断します。
◎自動：パソコンからホームページやメールを見る操作を行うだけで、自動的に接続します。
◎常時：常時接続します。
本製品で指定した接続先(WAN側)と常に接続状態を保持します。
- ② 自動切断タイム [接続設定]①欄で「自動」を設定している場合、WAN側への送出パケットがなくなってから回線を切断するまでの時間を入力します。(出荷時の設定：10)
設定できる範囲は、「0(自動切断しない)~65535(分)」です。
- ③ MSS制限値 プロバイダーから指定されている場合に限り、WAN側回線への最大有効データ長を数字で指定します。(出荷時の設定：1322)
設定できる範囲は、「536~1452」です。
MSS値とは、受信できる最大セグメント数のことです。
イーサネットパケットの最大長(MTU)は1500バイトと定められています。
これに対して、「PPPoE」や「フレッツADSL」の最大データサイズは1322より小さい値となっていますが、現行のインターネットルータには、オーバーサイズのパケットを破棄するものがあります。
よって、パケットの保護を優先するために小さめに設定しておく必要があります。
△警告
弊社では、MSS値を変更したことによって生じる結果については一切その責任を負いかねますので、あらかじめご了承ください。
- ④ ACネーム プロバイダーから指定されている場合に限り、指定のACネーム(アクセスコンセントレーター名)を入力します。
- ⑤ サービスネーム プロバイダーから指定されている場合に限り、指定のサービスネームを入力します。

3-3.「アドレス変換設定」画面

■ アドレス変換設定



アドレス変換機能を設定します。



〈登録〉ボタン 「アドレス変換設定」画面で変更したすべての設定内容が有効になります。

〈取消〉ボタン 「アドレス変換設定」画面の設定内容を変更したとき、変更前の状態に戻るボタンです。
 なお〈登録〉をクリックすると、変更前の状態には戻りません。

① アドレス変換 DMZホスト機能、静的マスカレード機能、静的NAT機能を使用して、グローバルアドレスをプライベートアドレスに変換するかしないかを選択します。
 (出荷時の設定：する)

② DMZホストIPアドレス DMZホスト機能(非武装セグメント)の対象となるパソコン(ホスト)のIPアドレスを入力します。
 DMZホスト機能を使うと、WAN(インターネット)側から発信されたすべてのIPフレームを、LAN側に存在する特定IPアドレスへ転送できます。
 転送することにより、本製品のLAN側に存在するパソコンでWWWサーバを運用したり、ネットワーク対戦ゲームなどが行えますが、転送先に設定したパソコンのIPアドレスに対してセキュリティが低下しますので、ご使用には十分注意してください。
 ※DMZホスト機能を静的マスカレードテーブルや静的NATテーブルと同時に使用した場合は、静的マスカレードテーブルおよび静的NATテーブルの設定が優先されます。

■ パススルー設定

インターネット経由で社内LANの仮想プライベートネットワーク(VPN)サーバにアクセスするとき設定します。

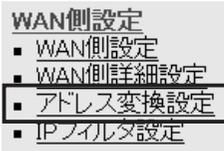


PPTPパススルーを使用 マルチプロトコル仮想プライベートネットワーク(VPN)をサポートするネットワーク技術で、クライアントからのPPTPパケットをWAN側に転送するかしないかの設定です。
 (出荷時の設定：する)

3 「WAN側設定」メニュー

3-3.「アドレス変換設定」画面(つづき)

■ 静的マスカレードテーブル設定



IPマスカレード変換を静的に行う設定です。

静的マスカレードテーブル設定				
登録の追加				
ローカルIP	プロトコル	ポート	開始ポート	終了ポート
<input type="text"/>	TCP	指定	<input type="text"/>	<input type="text"/>
<input type="button" value="追加"/>				
現在の登録				
ローカルIP	プロトコル	開始ポート	終了ポート	

マスカレードIP(ルータグローバルIP)に対して、アクセスしてきたパケットをプロトコルにより判定し、ここで指定したプライベートIPアドレスを割り当てたローカル端末へアドレス変換します。最大32個のマスカレードテーブルを設定できます。

- ◎ローカルIP：プライベートIPアドレスを入力します。
 - ◎プロトコル：TCP、UDP、TCP/UDP、GREから選択します。
 - ◎ポート：選択したプロトコルに対するポートを数字で指定するときは、「指定」を選択します。
数字で指定しない場合は、ニーモニック(DNS、Finger、FTP、Gopher、NEWS、POP3、SMTP、Telnet、Web、Whois)から選択します。
 - ◎開始ポート：プロトコルに対する開始ポート番号を入力します。
 - ◎終了ポート：プロトコルに対する終了ポート番号を入力します。
- ※入力後は〈追加〉をクリックして、[現在の登録]欄に登録されたことを確認してください。

■ DMZホスト機能と静的マスカレード機能の違い

DMZホスト機能	静的マスカレード機能
プロトコルやポート番号の指定が不要。	プロトコルやポート番号の指定が必要。
転送先として指定できるホストのIPアドレスは、1つだけである。	異なるプロトコルやポート番号ごとに、複数の転送先を設定できる。
転送先の変更が容易にできる。	転送先は、プロトコルやポート番号ごとに指定されているため、変更が複雑である。
転送先に指定したホストについては、セキュリティが低下する。	静的マスカレードテーブルに登録していないプロトコルやポート番号は、遮断される。

3-3.「アドレス変換設定」画面(つづき)

■ 静的NATテーブル設定

- WAN側設定
 - WAN側設定
 - WAN側詳細設定
 - **アドレス変換設定**
 - IPフィルタ設定

グローバルとプライベートのIPアドレス変換を行う設定です。

静的NATテーブル設定			
登録の追加			
グローバルIP	-	ローカルIP	
<input type="text"/>	-	<input type="text"/>	<input type="button" value="追加"/>
現在の登録			
グローバルIP	-	ローカルIP	

プロバイダーとのLAN型契約などで、複数のグローバルIPアドレスを取得した場合に、ローカルIPアドレスに1対1で変換させるためのテーブル設定です。

最大32個のNATテーブルを設定できます。

◎グローバルIP：指定されたグローバルIPアドレスを入力します。

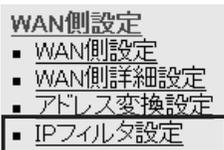
◎ローカルIP：任意のプライベートIPアドレスを入力します。

※入力後は〈追加〉をクリックして、[現在の登録]欄に登録されたことを確認してください。

3 「WAN側設定」メニュー

3-4.「IPフィルタ設定」画面

■不正アクセス検知機能設定



WAN側回線から本製品に不正な攻撃を受けたことを検知してIPフィルターの手前で阻止する機能を設定します。

IPフィルタ設定

IPフィルタの設定を行います。

登録 取消

不正アクセス検知機能設定

不正アクセス検知機能を使用 ①	<input checked="" type="radio"/> しない <input type="radio"/> する
検知結果を出力 ②	<input type="radio"/> しない <input checked="" type="radio"/> する
検知時間 ③	1 分
検知回数 ④	100 回

〈登録〉ボタン ……………

「不正アクセス検知機能設定」画面で変更したすべての設定内容が有効になります。

〈取消〉ボタン ……………

「不正アクセス検知機能設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

① 不正アクセス検知機能を使用

不正アクセス検知機能を使用するかしないかを選択します。
(出荷時の設定：しない)

検知できる内容は以下の通りです。

- ◎IP Spoofing : 偽りのLAN側アドレスでパケットを受けたとき
- ◎Land attack : 始点IPアドレスと終点IPアドレスが同じパケットを受けたとき
- ◎TCP Syn Flooding : 設定した[検知時間]以内に設定した[検知回数]より多い接続要求(SYN)を受けたとき
- ◎Tiny Fragmenting : Tiny fragment attack(RFC 1858で定義)を受けたとき
- ◎Source Routing : Loose routing IP optを検出したとき
Loose source routing headerを受けたとき
Strict routing IP optを検出したとき
Strict source routing headerを受けたとき

② 検知結果を出力 ……………

不正アクセスを検知したとき、検知結果を「情報表示」メニューの「通信記録」画面に表示するかしないかを選択します。
(出荷時の設定：する)

※このときの「通信記録」画面表示例は、5-1章をご覧ください。

3-4.「IPフィルタ設定」画面

■ 不正アクセス検知機能設定(つづき)

- WAN側設定
 - WAN側設定
 - WAN側詳細設定
 - アドレス変換設定
 - IPフィルタ設定

IPフィルタ設定

IPフィルタの設定を行います。

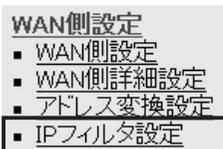
不正アクセス検知機能設定		
不正アクセス検知機能を使用	①	<input checked="" type="radio"/> しない <input type="radio"/> する
検知結果を出力	②	<input type="radio"/> しない <input checked="" type="radio"/> する
検知時間	③	1 <input type="text" value=""/> 分
検知回数	④	100 <input type="text" value=""/> 回

- ③ 検知時間 「TCP Syn Flooding」を検知する時間を設定します。
設定できる範囲は、「1～60(分)」です。 (出荷時の設定：1)
- ④ 検知回数 「TCP Syn Flooding」を検知する回数を設定します。
[検知時間](③)欄で設定した時間内に設定回数以上のアクセスを検知すると、不正アクセスと判断します。
設定できる範囲は、「5～999(回)」です。 (出荷時の設定：100)

3 「WAN側設定」メニュー

3-4.「IPフィルタ設定」画面(つづき)

■ IPフィルタ設定



特定条件を満たす内部または外部からのパケットを通過させたり、通過を阻止させるフィルタの設定です。

IPフィルタ設定		追加
番号	①	<input type="text"/>
フィルタ方向	②	<input type="radio"/> WAN側から <input checked="" type="radio"/> LAN側から <input type="radio"/> 両方
フィルタ方法	③	<input checked="" type="radio"/> 遮断 <input type="radio"/> 透過 <input type="radio"/> 透過(接続中)
プロトコル	④	すべて <input type="text"/> 指定時: <input type="text"/>
発信元ポート番号	⑤	指定 <input type="text"/> 指定時: <input type="text"/> ~ <input type="text"/>
宛先ポート番号	⑥	指定 <input type="text"/> 指定時: <input type="text"/> ~ <input type="text"/>
発信元IPアドレス	⑦	<input type="text"/> ~ <input type="text"/>
宛先IPアドレス	⑧	<input type="text"/> ~ <input type="text"/>

〈追加〉ボタン

[IPフィルタ設定]項目で作成、または編集した内容をフィルターとして追加するボタンです。

追加されると、その内容を[現在の登録]項目に一覧で表示します。
※フィルター条件は、1つ以上指定してください。

① 番号

最大64件のフィルターを登録できます。

入力できる範囲は、「1~64」です。

フィルターを登録すると、本製品が受信または送信するパケットごとに、[現在の登録]項目に表示されたフィルターと比較します。

[番号]欄では、フィルターを比較する順位を指定します。

フィルターを複数設定しているときは、番号の小さい順番に比較を開始します。

フィルターの条件に一致した時点で、それ以降の識別番号のフィルターは比較しません。

② フィルタ方向

パケットの通信方向で、本製品のWAN側とLAN側に対して、フィルターの対象となる方向を設定します。

以下の中から選択してください。

◎WAN側から：WAN側から本製品が受信するIPパケットに対して、フィルタリング処理を行います。

※フィルタリング処理は、アドレス変換のあとに行います。

◎LAN側から：本製品からWAN側に送信するIPパケットに対して、フィルタリング処理を行います。

※フィルタリング処理は、アドレス変換の前に行います。

◎両方：本製品からWAN側に送信、およびWAN側から受信する両方のIPパケットに対して、フィルタリング処理を行います。

3-4.「IPフィルタ設定」画面

■ IPフィルタ設定(つづき)

- WAN側設定
 - WAN側設定
 - WAN側詳細設定
 - アドレス変換設定
 - IPフィルタ設定

IPフィルタ設定		追加
番号	①	<input type="text"/>
フィルタ方向	②	<input type="radio"/> WAN側から <input checked="" type="radio"/> LAN側から <input type="radio"/> 両方
フィルタ方法	③	<input checked="" type="radio"/> 遮断 <input type="radio"/> 透過 <input type="radio"/> 透過(接続中)
プロトコル	④	すべて <input type="text"/> 指定時: <input type="text"/>
発信元ポート番号	⑤	指定 <input type="text"/> 指定時: <input type="text"/> ~ <input type="text"/>
宛先ポート番号	⑥	指定 <input type="text"/> 指定時: <input type="text"/> ~ <input type="text"/>
発信元IPアドレス	⑦	<input type="text"/> ~ <input type="text"/>
宛先IPアドレス	⑧	<input type="text"/> ~ <input type="text"/>

③ フィルタ方法

フィルタリングの方法は、以下の3通りから選択します。

- ◎遮断 : 回線の接続に関係なく、フィルタリングの条件に一致した場合、そのパケットをすべて破棄します。
- ◎透過 : 回線の接続に関係なく、フィルタリングの条件に一致した場合、そのパケットをすべて通過させます。
- ◎透過(接続中) : 回線がすでに接続されている状態で、フィルタリングの条件に一致した場合、そのパケットを通過させませんが、回線が接続されていない場合には、そのパケットを破棄します。
このように、パケットの送信をきっかけに自動発呼することを防止するときに設定してください。

④ プロトコル

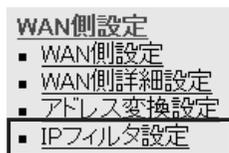
フィルタリングの対象となるパケットのトランスポート層プロトコルを選ぶ項目です。

- ◎指定 : 右のテキストボックスに、IP層ヘッダーに含まれる上位層プロトコル番号を入力します。
プロトコル番号は、10進数で0~255までの半角数字を入力してください。
- ◎すべて : すべてのプロトコルの条件に一致します。
- ◎TCP : TCPプロトコルの条件だけに一致します。
- ◎TCP_FIN : TCP_FIN/RSTのパケットが処理の対象になります。
- ◎TCP_EST : TCP_SYNフラグのパケットが処理の対象になります。
- ◎UDP : UDPプロトコルの条件だけに一致します。
- ◎ICMP : ICMPプロトコルの条件だけに一致します。
- ◎GRE : GREプロトコルの条件だけに一致します。

3 「WAN側設定」メニュー

3-4.「IPフィルタ設定」画面

■ IPフィルタ設定(つづき)



IPフィルタ設定		追加
番号	①	<input type="text"/>
フィルタ方向	②	<input type="radio"/> WAN側から <input checked="" type="radio"/> LAN側から <input type="radio"/> 両方
フィルタ方法	③	<input checked="" type="radio"/> 遮断 <input type="radio"/> 透過 <input type="radio"/> 透過(接続中)
プロトコル	④	すべて <input type="text"/> 指定時: <input type="text"/>
発信元ポート番号	⑤	指定 <input type="text"/> 指定時: <input type="text"/> ~ <input type="text"/>
宛先ポート番号	⑥	指定 <input type="text"/> 指定時: <input type="text"/> ~ <input type="text"/>
発信元IPアドレス	⑦	<input type="text"/> ~ <input type="text"/>
宛先IPアドレス	⑧	<input type="text"/> ~ <input type="text"/>

⑤ 発信元ポート番号 ……………

フィルタリングの対象となる発信元のTCP/UDPポート番号を指定する項目です。

数字で指定するときは、「指定」を選択して、番号を始点から終点まで連続で入力します。

入力できる範囲は、10進数で「1～65535」までの半角数字です。また、特定のポートだけを指定するときは、始点だけ、または始点/終点に同一の番号を入力してください。

数字で指定しない場合は、ニーモニック(DNS、Finger、FTP、Gopher、NEWS、POP3、SMTP、Telnet、Web、Whois)から選択します。

⑥ 宛先ポート番号 ……………

フィルタリングの対象となる宛先のTCP/UDPポート番号を指定する項目です。

数字で指定するときは、「指定」を選択して、番号を始点から終点まで連続で入力します。

入力できる範囲は、10進数で「1～65535」までの半角数字です。また、特定のポートだけを指定するときは、始点だけ、または始点/終点に同一の番号を入力してください。

数字で指定しない場合は、ニーモニック(DNS、Finger、FTP、Gopher、NEWS、POP3、SMTP、Telnet、Web、Whois)から選択します。

3-4.「IPフィルタ設定」画面

■ IPフィルタ設定(つづき)

- WAN側設定
 - WAN側設定
 - WAN側詳細設定
 - アドレス変換設定
 - IPフィルタ設定

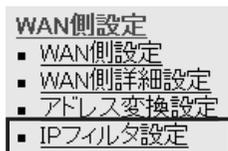
IPフィルタ設定		追加
番号	①	<input type="text"/>
フィルタ方向	②	<input type="radio"/> WAN側から <input checked="" type="radio"/> LAN側から <input type="radio"/> 両方
フィルタ方法	③	<input checked="" type="radio"/> 遮断 <input type="radio"/> 透過 <input type="radio"/> 透過(接続中)
プロトコル	④	すべて <input type="text"/> 指定時: <input type="text"/>
発信元ポート番号	⑤	指定 <input type="text"/> 指定時: <input type="text"/> ~ <input type="text"/>
宛先ポート番号	⑥	指定 <input type="text"/> 指定時: <input type="text"/> ~ <input type="text"/>
発信元IPアドレス	⑦	<input type="text"/> ~ <input type="text"/>
宛先IPアドレス	⑧	<input type="text"/> ~ <input type="text"/>

- ⑦ 発信元IPアドレス …………… 発信元ホストのIPアドレスを設定することにより、特定のホストからのパケットをフィルタリングします。
何も入力しない場合は、すべてのアドレスを対象とします。
発信元ホストのIPアドレスを始点から終点まで連続で入力します。
また、特定の発信元ホストだけを指定するときは、始点だけ入力してください。
- ⑧ 宛先IPアドレス …………… 宛先ホストのIPアドレスを設定することにより、特定のホストに対するパケットをフィルタリングします。
始点に何も入力しない場合は、すべてのアドレスを対象とします。
宛先ホストのIPアドレスを始点から終点まで連続で入力します。
また、特定の宛先ホストだけを指定するときは、始点だけ入力してください。

3 「WAN側設定」メニュー

3-4.「IPフィルタ設定」画面

■ 現在の登録



現在の登録		番号	方向	方法	プロトコル	発信元ポート番号	宛先ポート番号	発信元IPアドレス	宛先IPアドレス
編集	削除	57	WAN側から	透過	TCP	20	*	*	*
編集	削除	58	WAN側から	遮断	TCP_EST	*	*	*	*
編集	削除	59	両方	遮断	ALL	135	*	*	*
編集	削除	60	両方	遮断	ALL	*	135	*	*
編集	削除	61	両方	遮断	ALL	445	*	*	*
編集	削除	62	両方	遮断	ALL	*	445	*	*
編集	削除	63	両方	遮断	TCP	*	137 - 139	*	*
編集	削除	64	両方	遮断	UDP	137 - 139	137 - 139	*	*

現在登録されているIPフィルターを表示します。

【出荷時、登録されているフィルターについて】

- ◎57番 : FTPをデフォルトで通過させる
- ◎58番 : WAN側からの不正パケット防止
- ◎59、60番 : Windowsのアプリケーションを外部からリモートコントロールされる危険性を防止
- ◎61～64番 : Windowsが行う定期的な通信によって起こる「意図しない自動接続」を防止

〈編集〉ボタン

〈編集〉ボタンの右の欄に表示されたIPフィルターを編集するボタンです。

編集する欄の〈編集〉ボタンをクリックすると、その内容を「IPフィルタ設定」項目の各欄に表示します。

〈削除〉ボタン

〈削除〉をクリックすると、IPフィルターを削除されます。

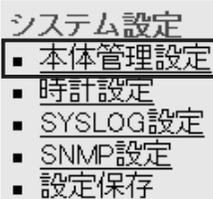
設定画面へのアクセス制限、本体時計、SYSLOG、SNMP、設定内容の保存、設定初期化の設定を行います。

4-1.「本体管理設定」画面	68
■ 管理者ID設定	68
■ 設定初期化	69
■ 「Firm Utility使用」モード	69
4-2.「時計設定」画面	70
■ 内部時計設定	70
■ 自動時計設定	71
4-3.「SYSLOG設定」画面	72
■ SYSLOG設定	72
4-4.「SNMP設定」画面	73
■ SNMP設定	73
4-5.「設定保存」画面	74

4 「システム設定」メニュー

4-1.「本体管理設定」画面

■ 管理者ID設定



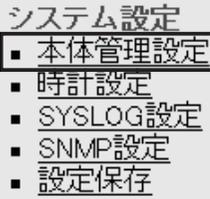
本製品の設定画面へのアクセス制限を設定します。

管理者ID設定		
管理者ID	①	<input type="text"/>
管理者パスワード	②	<input type="password"/>
パスワードの確認入力	③	<input type="password"/>

- 〈登録〉ボタン …………… [管理者ID設定]項目で変更したすべての設定内容が有効になります。
- 〈取消〉ボタン …………… [管理者ID設定]項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。
- ① 管理者ID …………… 本製品の設定画面へのアクセスを制限する場合に、管理者としての名前を、大文字/小文字の区別に注意して、任意の英数字、半角31(全角15)文字以内で入力します。(入力例：RDA5000)
[管理者ID]を設定すると、次回のアクセスからユーザー名の入力を求められますので、そこに[管理者ID]を入力します。
- ② 管理者パスワード …………… [管理者ID]に対するパスワードを設定する場合、大文字/小文字の区別に注意して、任意の英数字、半角31文字以内で入力します。
入力した文字は、すべて「*(アスタリスク)」で表示されます。
(表示例：****)
[管理者パスワード]を設定すると、次回のアクセスからパスワードの入力を求められますので、そこに[管理者パスワード]を入力します。
- ③ パスワードの確認入力 …… 確認のために、パスワードを再入力します。(表示例：****)

4-1. 「本体管理設定」画面(つづき)

■ 設定初期化



本製品の設定内容をすべて出荷時の状態に戻します。



[初期化する]欄のチェックボックスをクリックしてチェックマークを入れてから、〈実行〉ボタンをクリックします。

- 次の画面を表示後、出荷時の状態になります。

再起動しています。しばらくお待ちください。

■ 「Firm Utility使用」モード

本製品に付属の「Firm Utility」を使用して、本製品を出荷時の状態に戻したり、ファームウェアをバージョンアップするとき使用しません。



「Firm Utility使用」モードにするときは、[移行する]欄のチェックボックスをクリックしてチェックマークを入れてから、〈実行〉ボタンをクリックします。

- 次の画面を表示して、「Firm Utility使用」モードに移行します。

「Firm Utility使用」モードに移行しました。
通常動作は全て停止しています。
通常モードに戻るには本体を再起動して下さい。

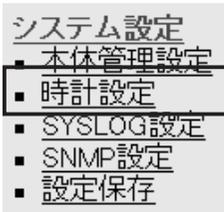
※「Firm Utility使用」モードに移行後も、本製品に設定された内容で動作します。

※「Firm Utility使用」モードに移行しないと、「Firm Utility」と本製品が通信できません。

4 「システム設定」メニュー

4-2. 「時計設定」画面

■ 内部時計設定



本製品の内部時計を設定します。

時計設定
本体の内部時計の設定を行います。

登録 取消

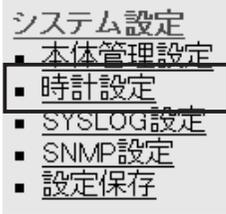
内部時計設定

本体の時刻 ①	2003年	01月	01日	02時	17分
設定する時刻 ②	2003年	06月	27日	10時	37分

- 〈登録〉ボタン 「時計設定」画面で変更したすべての設定内容が有効になります。
- 〈取消〉ボタン 「時計設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。
- ① 本体の時刻 本製品に設定されている時刻を表示します。
- ② 設定する時刻 本製品の設定画面にアクセスしたとき、パソコンの時計設定を取得して表示します。
表示する時刻は、「時計設定」画面アクセス時に取得した時刻です。
※正確に設定したいときは、「時計設定」画面に再アクセスするかブラウザの〈更新〉ボタンをクリックしてから、〈登録〉をクリックしてください。

4-2.「時計設定」画面(つづき)

■ 自動時計設定



本製品の内部時計を自動設定するとき、アクセスするタイムサーバの設定です。

自動時計設定		
自動時計設定を使用 ①	<input type="radio"/> しない <input checked="" type="radio"/> する	
NTPサーバ1 IPアドレス ②	<input type="text" value="133.100.9.2"/>	
NTPサーバ2 IPアドレス ③	<input type="text"/>	
アクセス時間間隔 ④	<input type="text" value="1"/> 日	
前回アクセス日時 ⑤	----/--/-- --:--	
次回アクセス日時 ⑥	2003/01/02 00:00	

- ① 自動時計設定を使用 …………… インターネット上に存在するタイムサーバに日時の問い合わせを行い、内部時計を自動設定します。 (出荷時の設定：する)

- ② NTPサーバ1 IPアドレス …………… 最初にアクセスするタイムサーバのIPアドレスを入力します。 (出荷時の設定：133.100.9.2)

- ③ NTPサーバ2 IPアドレス …………… [NTPサーバ1 IPアドレス]の次にアクセスさせるタイムサーバがあるときは、そのIPアドレスを入力します。
返答がないときは、再度[NTPサーバ1 IPアドレス]で設定したタイムサーバにアクセスします。

- ④ アクセス時間間隔 …………… タイムサーバにアクセスする間隔を設定します。
設定できる範囲は、「0～99」です。 (出荷時の設定：1)
「0」を設定したときは、タイムサーバにアクセスを行いません。
回線に手動で接続したとき、前回アクセスした日から設定した日数が経過しているときは、接続時にタイムサーバにアクセスしません。
回線への常時接続を設定しているときは、設定した日数にしたがってアクセスします。

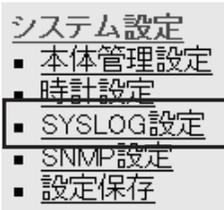
- ⑤ 前回アクセス日時 …………… タイムサーバにアクセスした日時を表示します。

- ⑥ 次回アクセス日時 …………… タイムサーバにアクセスする予定日時を、[前回アクセス日時]欄と[アクセス時間間隔]欄で設定された日数より算出して表示します。

4 「システム設定」メニュー

4-3.「SYSLOG設定」画面

■ SYSLOG設定



指定したホストアドレスにログ情報などを出力する設定を行います。

SYSLOG設定

指定したホストアドレスにログ情報などを出力する設定を行います。SYSLOG機能を利用してファイルとして一括管理ができます。

登録 取消

SYSLOG設定		
DEBUGを使用 ①		<input checked="" type="radio"/> しない <input type="radio"/> する
INFOを使用 ②		<input checked="" type="radio"/> しない <input type="radio"/> する
NOTICEを使用 ③		<input type="radio"/> しない <input checked="" type="radio"/> する
ホストアドレス ④		<input type="text"/>
ファシリティ ⑤		<input type="text" value="1"/>

〈登録〉ボタン …………… 「SYSLOG設定」画面で変更したすべての設定内容が有効になります。

〈取消〉ボタン …………… 「SYSLOG設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

① DEBUGを使用 …………… 各種デバッグ情報をSYSLOGに出力するかしないかを選択します。
(出荷時の設定：しない)

② INFOを使用 …………… INFOタイプのメッセージをSYSLOGに出力するかしないかを選択します。
(出荷時の設定：しない)

③ NOTICEを使用 …………… NOTICEタイプのメッセージをSYSLOGに出力するかしないかを選択します。
(出荷時の設定：する)

④ ホストアドレス …………… SYSLOG機能を使用する場合、SYSLOGを受けるホストのアドレスを入力します。
ホストはSYSLOGサーバ機能に対応している必要があります。

⑤ ファシリティ …………… SYSLOGのファシリティを入力します。
設定できる範囲は、「0～23」です。
通常「1」を使用します。
(出荷時の設定：1)

4-4.「SNMP設定」画面

■ SNMP設定

- システム設定
 - 本体管理設定
 - 時計設定
 - SYSLOG設定
 - **SNMP設定**
 - 設定保存

TCP/IPネットワークにおいて、ネットワーク上の各ホストから自動的に情報を収集してネットワーク管理するときの設定です。

SNMP設定

SNMP機能に関する設定を行います。

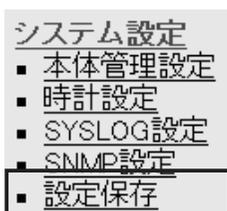
登録
取消

SNMP設定	
SNMPを使用 ①	<input type="radio"/> しない <input checked="" type="radio"/> する
コミュニティID(GET) ②	<input style="width: 80%;" type="text" value="public"/>

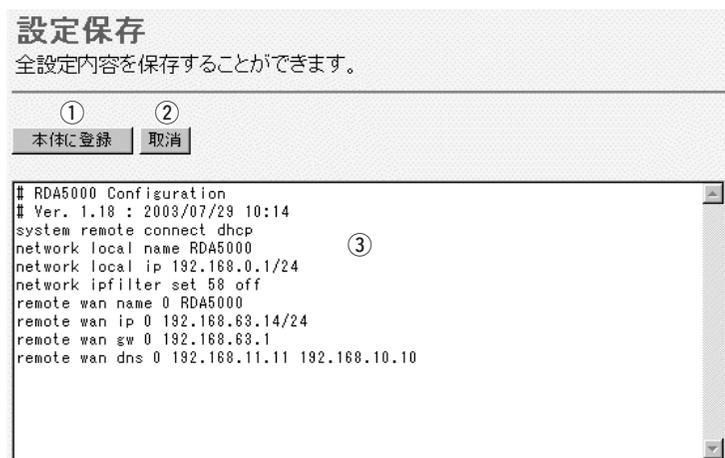
- 〈登録〉ボタン …………… 「SNMP設定」画面で変更したすべての設定内容が有効になります。
- 〈取消〉ボタン …………… 「SNMP設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。
 なお〈登録〉をクリックすると、変更前の状態には戻りません。
- ① SNMPを使用 …………… SNMP機能を使用するかどうかを選択します。
 (出荷時の設定：する)
- ② コミュニティID(GET) …… 本製品から設定情報をSNMP管理ツール側で読み出すことを許可するIDを設定します。
 (出荷時の設定：public)
 入力は、半角31文字以内の英数字で入力します。

4 「システム設定」メニュー

4-5. 「設定保存」画面



本製品の全設定内容を確認したり、設定した内容を設定ファイルとして保存を行います。



- ① <本体に登録> ボタン …………… 「内容表示」画面に表示している内容を、設定画面に書き込みます。
- ② <取消> ボタン …………… 「内容表示」画面に表示された内容を変更したとき、変更を取り消して、このファイルを最初に開いたときの内容に戻します。
- ③ 「内容表示」画面 …………… 基本的な設定内容と変更された設定内容を表示します。
この画面内容をパソコンに保存することで、本製品の設定をバックアップできます。
保存した設定ファイルを開いたときは、保存されている変更内容を表示します。
なお、各画面で設定されたパスワードやキージェネレーター(無線LAN通信用暗号化鍵の生成元文字列)の内容は、暗号化されて表示されます。
そのため、保存されたファイルよりそれらが外部へ漏れることはありません。
※「内容表示」画面の内容を編集したときは、編集前に表示されていた本製品のIPアドレスに向けて設定ファイルの内容を転送しますので、内容を編集したときなどは、本製品(転送先)のIPアドレスを設定ファイル編集前のIPアドレスに設定しておく必要

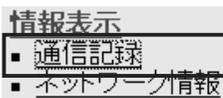
WAN側回線の通信記録、本製品のMACアドレス表示、ネットワークインターフェイスリスト、ブリッジポート情報を表示します。

5-1.「通信記録」画面	76
■ 通信記録	76
5-2.「ネットワーク情報」画面	76
■ ネットワーク インターフェイス リスト	76
■ ブリッジポート情報	77
■ 本体MACアドレス	77

5 「情報表示」メニュー

5-1.「通信記録」画面

■ 通信記録



WAN側回線の通信記録を表示します。

通信記録	
WAN側回線の通信記録を表示します。	
通信記録 <input type="button" value="クリア"/>	
日付・時間	通信記録
09/11 11:42:47	DHCP:BIND (My Address [172.20.252.227] : GW Address [172.20.0.1]) Lease 1 day Lease 24 hour : Primary DNS [172.16.0.5]
09/11 11:42:39	DHCP:RELEASE success
01/01 00:00:05	DHCP:BIND (My Address [172.20.252.227] : GW Address [172.20.0.1]) Lease 1 day Lease 24 hour : Primary DNS [172.16.0.5]

通信記録の履歴は、〈クリア〉をクリックすると消去できます。

【不正アクセス検知時の通信記録表示例】

通信記録	
WAN側回線の通信記録を表示します。	
通信記録 <input type="button" value="クリア"/>	
日付・時間	通信記録
12/11 11:36:17	TCP Syn Flooding: 172.20.252.210->172.20.101.51 TCP[6]src=1784,dst=80
01/01 03:35:44	TCP Syn Flooding: 172.20.252.169->172.20.101.51 TCP[6]src=2460,dst=80
01/01 03:34:00	DHCP:RELEASE success
01/01 03:29:16	TCP Syn Flooding: 172.20.252.169->172.20.252.94 TCP[6]src=2178,dst=80
01/01 03:28:25	TCP Syn Flooding: 172.20.252.210->172.20.252.94 TCP[6]src=1464,dst=80
01/01 03:22:03	TCP Syn Flooding: 172.20.252.169->172.20.252.94 TCP[6]src=2114,dst=80
01/01 03:19:05	TCP Syn Flooding: 172.20.252.169->172.20.252.94 TCP[6]src=1863,dst=80

5-2.「ネットワーク情報」画面

■ ネットワーク インターフェイス リスト



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

ネットワーク情報

ネットワークインターフェイスリストと本体MACアドレスを表示します。

ネットワーク インターフェイス リスト		
インターフェイス	IPアドレス	サブネットマスク
local	192.168.0.1	255.255.255.0
wan	172.20.11.109	255.255.0.0

※回線種別が[PPPoE]/[PPPoE複数固定IP]設定時、[wan]インターフェイスに対する表示は、回線に接続されるまで表示されません。

5-2.「ネットワーク情報」画面(つづき)

■ブリッジポート情報

本製品の各ポートごとに、通信状況とパケットの数を表示します。



ブリッジポート情報		
ポート	通信情報	
Ethernet ①	状況	通信中
	送信パケット数	2
	受信パケット数	0
IEEE802.11a ②	状況	通信中
	送信パケット数	2
	受信パケット数	0
IEEE802.11g ③	状況	通信中
	送信パケット数	32
	受信パケット数	35

① Ethernet……………

[LAN]ポートの通信状況と、そのときの送信と受信のパケット数を表示します。

② IEEE802.11a ……

54Mbps(5.2GHz)無線LANポートの通信状況と、そのときの送信と受信のパケット数を表示します。

③ IEEE802.11g ……

54Mbps(2.4GHz)無線LANポートの通信状況と、そのときの送信と受信のパケット数を表示します。

■本体MAC アドレス

本製品のMACアドレスを表示します。

※このMACアドレスは、本製品の底面パネルに貼られているシリアルシールにも12桁で記載されています。





Telnetによる接続方法とオンラインヘルプについて説明します。

6-1. Telnetによる接続	80
■ Windows 98/98 SE/Meの場合	80
■ Windows 2000/Windows XPの場合	80
6-2. オンラインヘルプ	81

6 Telnetガイド

6-1. Telnetによる接続

Telnetでの接続について説明します。
ご使用のOSやTelnetクライアントが異なるときは、それぞれの使用方法をご確認ください。

■ Windows 98/98 SE/Meの場合

- ① Windowsを起動します。
- ② [スタート]メニューから[ファイル名を指定して実行]を選択します。
名前欄に「Telnet.exe」と入力し、<OK>をクリックします。
- ③ Telnetクライアントが起動しますので、メニューバーから[接続]→[リモートシステム]を選択します。
- ④ [接続]ダイアログボックスが表示されます。
ホスト名、ポート、ターミナルの種類を下記のように選択して、<接続(C)>ボタンをクリックします。
ホスト名：本製品のIPアドレス(出荷時の設定：192.168.0.1)
ポート：telnet(23)
ターミナルの種類：vt100
- ⑤ [User]と[Password]が要求されます。
本製品の「本体管理設定」画面で設定(※4-1章)した[管理者ID]と[管理者パスワード]を入力してログインしてください。
※出荷時は、[User]と[Password]は設定されていませんから、何も入力しないで[Enter]キーを押してください。
- ⑥ ログインメッセージ(Welcome to RDA5000!)が表示されます。

■ Windows 2000/Windows XPの場合

- ① Windowsを起動します。
- ② [スタート]メニューから[ファイル名を指定して実行]を選択します。名前欄に「Telnet.exe」と入力し、<OK>をクリックします。
- ③ Telnetクライアントが起動しますので、下記のように指定します。
Microsoft Telnet>open 本製品のIPアドレス
(工場出荷時の設定：192.168.0.1)
- ④ [User]と[Password]が要求されます。
本製品の「本体管理設定」画面で設定(※4-1章)した[管理者ID]と[管理者パスワード]を入力してログインしてください。
※出荷時は、[User]と[Password]は設定されていませんから、何も入力しないで[Enter]キーを押してください。
- ⑤ ログインメッセージ(Welcome to RDA5000!)が表示されます。

6-2.オンラインヘルプ

オンラインで、コマンドリファレンスを参照することができます。

- ◎コマンド一覧 …………… [Tab]キーを押すと、使用できるコマンドの一覧が表示されます。コマンド名の入力に続いて[Tab]キーを押すと、サブコマンドの一覧が表示されます。
- ◎コマンドヘルプ …………… コマンドの意味を知りたい時は、コマンド名の入力に続いて[?]キーを押すとコマンドのヘルプが表示されます。
- ◎コマンド名の補完 …………… コマンド名を先頭から途中まで入力し[Tab]キーを押すと、コマンド名が補完されます。入力した文字に続くコマンドが一つしか無いときは、コマンド名を最後まで補完します。
 - 例) cl[Tab]→clear複数のコマンドがあるときは、同じ文字列の所までを補完します。さらに[Tab]キーを押すと、コマンドの候補を表示します。
 - 例) r[Tab]→re
 - re[Tab]→restart remote
 - res[Tab]→restart

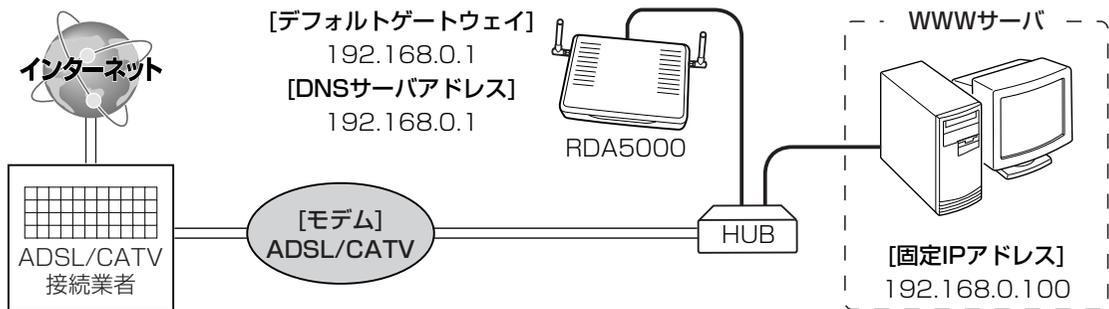


Webサーバを公開するための設定について説明します。

1.WWWサーバの設定.....	84
2.Web公開の設定	84

7 Web公開の設定例

本製品を使用してWebサーバを公開するための準備と本製品の設定例を、下記の図を例に説明します。



1. WWWサーバの設定

- ①WWWサーバとして使用するパソコンのIPアドレスがDHCPサーバから自動的に取得する設定になっている場合は、[TCP/IP]のプロパティで、IPアドレスを固定(例：192.168.0.100)します。
- ②「デフォルトゲートウェイ」と「DNSサーバアドレス」は、本製品に出荷時設定された値(192.168.0.1)を使用すると仮定しますので、それらも併せて設定します。
- ③設定後、このパソコンからインターネットに接続できることを確認します。

2. Web公開の設定

- ①本製品の設定画面にアクセスして、「WAN側設定」メニューの「アドレス変換設定」をクリックします。
 - 「アドレス変換設定」画面を表示します。
- ②パソコンの固定IPアドレス(例：192.168.0.100)を[静的マスカレード設定]項目の[登録の追加]-[ローカルIP]欄に入力します。
- ③指定するプロトコルは「TCP」で、[静的マスカレード設定]項目の[登録の追加]-[プロトコル]欄で選択します。
- ④指定するポートは「Web(80番)」で、[静的マスカレード設定]項目の[登録の追加]-[ポート]欄で選択します。
- ⑤「追加」をクリックします。

The screenshot shows the 'アドレス変換設定' (Address Translation Settings) screen. The left sidebar has 'ネットワーク設定' (Network Settings) expanded, with 'WAN側設定' (WAN Side Settings) selected. 'アドレス変換設定' (Address Translation Settings) is highlighted. The main area shows '静的マスカレードと静的NATの設定を行います。' (Configure static masquerade and static NAT). Below are sections for 'アドレス変換設定' (Address Translation Settings), 'パススルー設定' (Pass-through Settings), and '静的マスカレードテーブル設定' (Static Masquerade Table Settings). The '静的マスカレードテーブル設定' section has a table with columns: 'ローカルIP' (Local IP), 'プロトコル' (Protocol), 'ポート' (Port), '開始ポート' (Start Port), and '終了ポート' (End Port). A row is being added with '192.168.0.100', 'TCP', and 'Web'. A '追加' (Add) button is at the bottom right. Numbered callouts 1-6 point to: 1. Clicking 'アドレス変換設定' in the sidebar; 2. Clicking '登録の追加' (Add); 4. Selecting 'ローカルIP'; 3. Inputting '192.168.0.100'; 5. Selecting 'TCP' and 'Web'; 6. Clicking '追加'.

2. Web公開の設定(つづき)

⑥設定した内容を[静的マスカレード設定]項目の[現在の登録]欄で確認します。

7. 確認する

ローカルIP	プロトコル	ポート	開始ポート	終了ポート
192.168.0.100	TCP	web		

- ⑦「[WAN側設定]メニューの「[IPフィルタ設定]」をクリックします。
- 「[IPフィルタ設定]」画面を表示します。
- ⑧「56」を「[IPフィルタ設定]」項目の「[番号]」欄に入力します。
- ⑨指定するフィルタ方向は「[WAN側から]」で、「[IPフィルタ設定]」項目の「[フィルタ方向]」欄で選択します。
- ⑩指定するフィルタ方法は「[透過]」で、「[IPフィルタ設定]」項目の「[フィルタ方向]」欄で選択します。
- ⑪指定するプロトコルは「[TCP]」で、「[IPフィルタ設定]」項目の「[プロトコル]」欄で選択します。
- ⑫指定する宛先ポート番号は「[80]」(Web)で、「[IPフィルタ設定]」項目の「[宛先ポート番号]」欄に入力します。
- ⑬宛先IPアドレスは、パソコンの固定IPアドレス(例：192.168.0.100)で、「[IPフィルタ設定]」項目の「[宛先IPアドレス]」欄に入力します。
- ⑭「<追加>」をクリックします。

12. クリック

9. 設定する

8. クリック

10. 入力する

11. 入力する

番号	56
フィルタ方向	<input checked="" type="radio"/> WAN側から <input type="radio"/> LAN側から <input type="radio"/> 両方
フィルタ方法	<input type="radio"/> 遮断 <input checked="" type="radio"/> 透過 <input type="radio"/> 透過(接続中)
プロトコル	TCP 指定時: []
発信元ポート番号	指定 [] 指定時: [] ~ []
宛先ポート番号	指定 [] 指定時: 80 ~ []
発信元IPアドレス	[] ~ []
宛先IPアドレス	192.168.0.100 ~ []

7 Web公開の設定例

2. Web公開の設定(つづき)

⑮設定した内容を[現在の登録]項目で確認できたら設定完了です。

13. 確認する

現在の登録											
		番号	方向	方法	プロトコル	送信元ポート	番号	宛先ポート	番号	送信元IPアドレス	宛先IPアドレス
編集	削除	56	WAN側から	透過	TCP	*		web	*		192.168.0.100
編集	削除	57	WAN側から	透過	TCP	20		*	*		*
編集	削除	58	WAN側から	遮断	TCP_EST	*		*	*		*
編集	削除	59	両方	遮断	ALL	135		*	*		*
編集	削除	60	両方	遮断	ALL	*		135	*		*
編集	削除	61	両方	遮断	ALL	445		*	*		*
編集	削除	62	両方	遮断	ALL	*		445	*		*
編集	削除	63	両方	遮断	TCP	*		137 - 139	*		*
編集	削除	64	両方	遮断	UDP	137 - 139		137 - 139	*		*

【ご参考に】

グローバルアドレスでのホームページ公開を確認するときは、本製品のWAN側から行ってください。

複数固定IPアドレスサービスについて説明します。

8-1. 複数固定IPアドレスサービスを使うには	88
8-2. グローバル固定IPアドレスの使いかた	88

8 複数固定IPを使う

8-1.複数固定IPアドレスサービスを使うには

ご契約の回線接続業者、またはプロバイダーがこのサービスを提供している場合、このサービスをご契約になると、回線接続業者、またはプロバイダーから利用可能な複数のグローバル固定IPアドレスを指定されます。

これらのグローバル固定IPアドレスは、本製品の動作モードを「PPPoE複数固定IP」(「**回線種別**」※3-1章)に変更することで、本製品のEthernetケーブルに接続されたパソコン(LAN側)に直接設定して利用できます。

また、本製品のDHCPサーバ機能などで、自動割り当てされたプライベートアドレスのパソコンと混在した環境でご利用いただけます。

8-2.グローバル固定IPアドレスの使いかた

ご契約の回線接続業者、またはプロバイダーから8個のグローバル固定IPアドレスを指定された場合を例に、その使いかたを説明します。

◎割り当てられた指定の8個：172.16.0.48～172.16.0.55

◎サブネットマスク：255.255.255.248

◎ネットワークIPアドレス：172.16.0.48(使用できません)

◎ブロードキャストアドレス：172.16.0.55(使用できません)

◎172.16.0.49(WAN側IPアドレスとして本製品に設定)

◎172.16.0.50(本製品に接続するパソコンに使用可能)

◎172.16.0.51(本製品に接続するパソコンに使用可能)

◎172.16.0.52(本製品に接続するパソコンに使用可能)

◎172.16.0.53(本製品に接続するパソコンに使用可能)

◎172.16.0.54(本製品に接続するパソコンに使用可能)

※指定以外のグローバルIPアドレスを使用することはできません。

また、連続で指定された複数のグローバル固定IPアドレスのうち、最初(ネットワークアドレス)と最後(ブロードキャストアドレス)は、ネットワーク上でホストに割り当てて使用できない規則になっています。

ルート株式会社

住 所 : 113-0024 東京都文京区西片1-17-8 KSビル2F

TEL : 03-5840-7601

E-mail : support@root-hq.com
