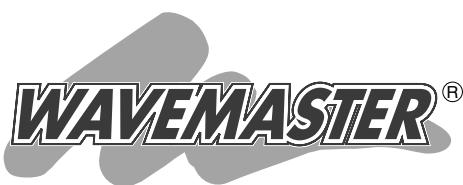
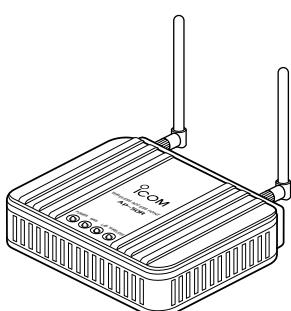


取扱説明書[活用編]



WIRELESS ACCESS POINT **AP-50R**

ブロードバンドルータ機能搭載
IEEE802.3af規格PoE対応



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



3ページ

ネットワーク設定

1

17ページ

無線LAN設定

2

35ページ

WAN側設定

3

53ページ

システム設定

4

61ページ

情報表示

5

65ページ

メンテナンス

6

71ページ

ご参考に

7

はじめに

本書は、本製品で設定できる機能について、各メニューの設定画面ごとに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。

※Microsoft® Windows® XP Professional、Microsoft® Windows® XP Home Editionは、Windows XPと表記します。

Microsoft® Windows® 2000 Professionalは、Windows 2000と表記します。

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

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

※本書は、Ver1.00のファームウェアを使用して説明しています。

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

登録商標について

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

◎WAVEMASTERは、アイコム株式会社の登録商標です。

◎Microsoft、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。

本文中の画面の使用に際して、米国Microsoft Corporationの許諾を得ています。

◎Adobe、Adobe Acrobatは、アドビシステムズ社の登録商標です。

◎Atheros、Total 802.11、Super A/Gロゴは、Atheros Communications, Inc. の登録商標です。

◎その他、本書に記載されている会社名、製品名は、各社の商標および登録商標です。

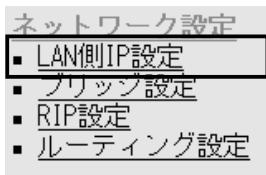
この章では、
「ネットワーク設定」メニューで表示される設定画面について説明します。

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
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	AP-50R
IPアドレス	②	192.168.0.1
サブネットマスク	③	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、[本体名称/IPアドレス設定]項目の[IPアドレス]欄と[サブネットマスク]欄、および[VLAN設定]項目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、および[VLAN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

「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〉や〈登録して再起動〉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用できます。

また、Telnet(☞7-2章)でログインしたときのログインメッセージにも使用されます。 (出荷時の設定: AP-50R)

入力形式: [http://web.本体名称/](例 http://web.AP-50R/)

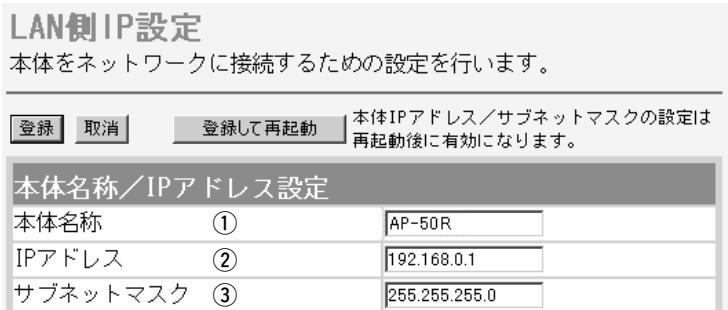
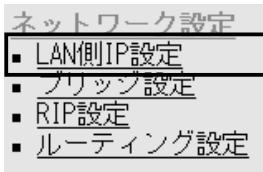
この場合、[DHCPサーバ設定]項目の[DNS代理応答を使用]欄を「する」(出荷時の設定)に設定しておく必要があります。

※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。

例 : [ネットワーク管理者から8個のグローバル固定IPアドレスを指定された場合の使いかた]

- ◎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(LAN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)

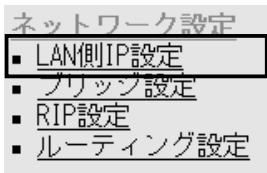
※指定以外のグローバルIPアドレスを使用することはできません。

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。

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。

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	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	<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

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る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。

※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るください。

※「0」を設定したときは、自動割り当てをしません。

④ サブネットマスク

[割り当て開始IPアドレス]欄に設定されたIPアドレスに対するサブネットマスクです。

(出荷時の設定：255.255.255.0)

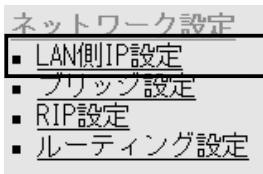
⑤ リース期間

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るおおす期限を設定します。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	<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	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	<input type="radio"/> しない <input checked="" type="radio"/> する	
プライマリDNSサーバ	⑨	DNSの代理応答機能を
セカンダリDNSサーバ	⑩	使用する場合は無効となります。
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、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しないかの設定です。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、本製品と接続する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

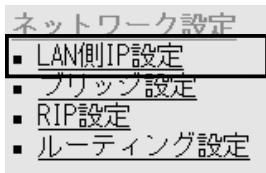
[プライマリDNSサーバ]欄と同様に、使い分けたいDNSサーバアドレスのもう一方を入力します。

※[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	<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	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	<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

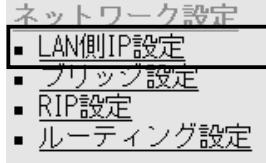
⑪ プライマリWINSサーバ …

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
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します。

※この項目には、最大16個の組み合わせを登録できます。

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。

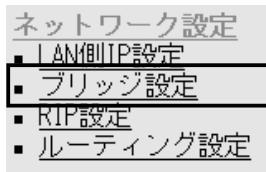
【登録例】

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



ブリッジ接続でスパニングツリー機能を設定するとき使用します。

ブリッジ設定

ブリッジ機能に関する設定を行います。

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

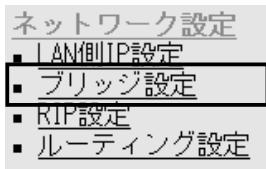
スパニングツリー機能を設定すると、経路障害のないときは、冗長リンクを検出して重複する経路のうち優先度の低い方を遮断します。

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 32768
エージングタイム(Ageing Time)	③ 300 秒
マックスエイジ(Max Age)	④ 20 秒
ハロータイム(Hello Time)	⑤ 2 秒
転送遅延(Forward Delay)	⑥ 15 秒
パスコスト(Path Cost)	⑦ 有線LAN 100 無線LAN 200
ポート優先度(Port Priority)	⑧ 有線LAN 128 無線LAN 128

② ブリッジ優先度

(Bridge Priority)

※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AP-5100A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

(Ageing Time)

※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

(Max Age)

※出荷時の設定でご使用されることを推奨します。

BPDUs(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

(Hello Time)

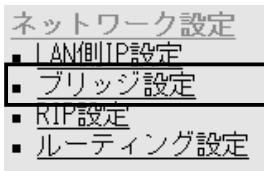
※出荷時の設定でご使用されることを推奨します。

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BPDUs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	32768	
エージングタイム(Ageing Time)	③	300	秒
マックスエイジ(Max Age)	④	20	秒
ハロータイム(Hello Time)	⑤	2	秒
転送遅延(Forward Delay)	⑥	15	秒
パスコスト(Path Cost)	⑦	有線LAN 100	無線LAN 200
ポート優先度(Port Priority)	⑧	有線LAN 128	無線LAN 128

⑥ 転送遅延

(Forward Delay)

※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設定します。

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

(Path Cost)

※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LAN：200)

⑧ ポート優先度

(Port Priority)

※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。

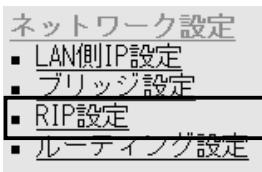
(出荷時の設定：有線LAN：128/無線LAN：128)

※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。

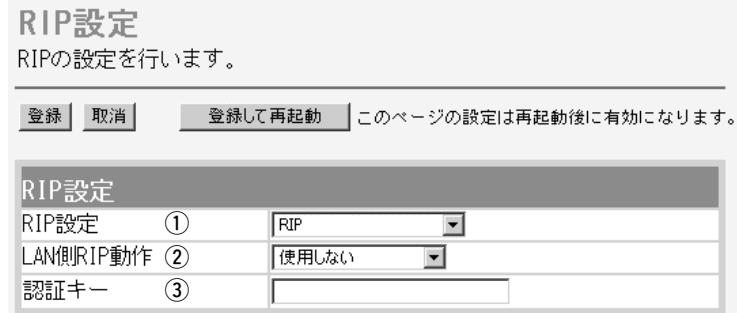
1 「ネットワーク設定」メニュー

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に使用します。



〈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、インター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。

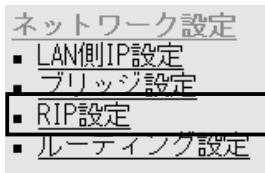
② LAN側RIP動作

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)

1-3.「RIP設定」画面

■ RIP設定(つづき)



RIP設定

RIP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。

RIP設定

RIP設定	①	<input type="text" value="RIP"/>
LAN側RIP動作	②	<input type="text" value="使用しない"/>
認証キー	③	<input type="text"/>

③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。

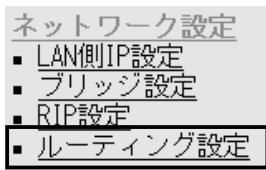
認証キーを設定すると、「RIP」を設定しているゲートウェイと、異なる認証キーを設定している「RIP2」、および認証キーを設定していない「RIP2」ゲートウェイからのRIPパケットを破棄します。

※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。

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



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「01: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

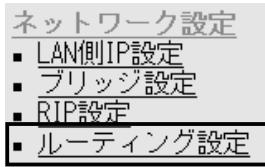
◎ misc : ブロードキャストに関するフレーム処理で作成

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。

最大32件まで登録できます。



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。

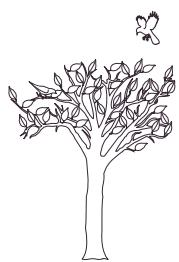
0(空白)～15まで入力できます。

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。



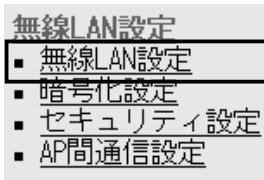
この章では、
「無線LAN設定」メニューで表示される設定画面について説明します。

2-1.「無線LAN設定」画面	18
■ BSSID	18
■ 無線LAN設定	18
2-2.「暗号化設定」画面	24
■ 暗号化設定	24
■ WEPキー	28
2-3.「セキュリティ設定」画面	29
■ RADIUS設定	29
■ 無線端末間通信設定	31
■ MACアドレスフィルタリング設定	32
2-4.「AP間通信設定」画面	33
■ BSSID	33
■ 通信AP設定	33

2 「無線LAN設定」メニュー

2-1.「無線LAN設定」画面

■ BSSID



本製品に内蔵された無線LANカードの[BSSID]を表示します。

無線LAN設定

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。

BSSID

00-90-C7-88-07-61

〈登録〉ボタン

[無線LAN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

[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。

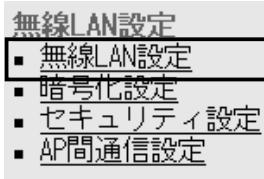
〈登録して再起動〉ボタン

本製品を再起動して、「無線LAN設定」画面で変更したすべての設定内容が有効になります。

BSSID

本製品では、「情報表示」メニューの「ネットワーク情報」画面に表示される[本体MACアドレス]と同じものを表示します。

■ 無線LAN設定



本製品に内蔵された無線LANカードに対する設定です。

無線LAN設定

SSID	①	LG
ANY接続拒否	②	<input checked="" type="radio"/> しない <input type="radio"/> する
チャンネル	③	11 (2462MHz)
Rts/Ctsスレッシュホールド	④	無し
11g保護機能	⑤	有効
パワーレベル	⑥	高
接続端末制限	⑦	255
Super A/Gを使用	⑧	しない

①SSID

無線ネットワークのグループ分けをするために使用します。

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できます。

この[SSID]が異なると本製品と無線で通信できません。

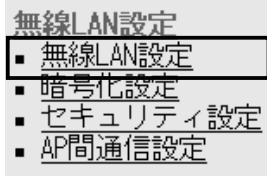
大文字/小文字の区別に注意して、任意の英数字、半角31文字以内で入力します。 (出荷時の設定: LG)

※[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。

2-1.「無線LAN設定」画面

■ 無線LAN設定(つづき)



② ANY接続拒否

「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、弊社製無線LANカード(SL-11やSL-110を除く)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」に対応する弊社製無線LANカードに付属の設定ユーティリティー」に検索されません。

※ご使用のパソコンにSL-50(ドライバーのVer.1.34以降)やSL-5000、SL-5000XG、SL-5100、SL-5200をインストールしたときは、出荷時から「ANY」モードで動作しています。

③ チャンネル

本製品が無線通信に使用するチャンネルを設定します。

(出荷時の設定: 11(2462MHz))

◎2.4GHz帯(IEEE802.11b/g規格)で通信するときは、「1～13」チャンネルを選択します。

◎5.2GHz帯(IEEE802.11a規格)で通信するときは、「34、38、42、46」チャンネルの中から選択します。

※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。

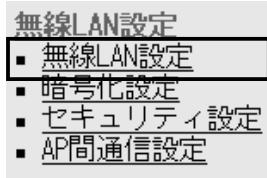
※本製品どうしを無線AP間通信(☞2-4章)するときは、相手の無線アクセスポイントと同じチャンネルに設定してください。

☞次ページにつづく

2 「無線LAN設定」メニュー

2-1.「無線LAN設定」画面

■ 無線LAN設定(つづき)



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

③ チャンネル(つづき)

近くに2.4GHz帯(IEEE802.11b/g)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。

※5.2GHz帯(IEEE802.11a)で通信する場合は、お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。



2-1.「無線LAN設定」画面

■ 無線LAN設定(つづき)

- 無線LAN設定
- 無線LAN設定
 - 暗号化設定
 - セキュリティ設定
 - AP間通信設定

無線LAN設定	
SSID	① LG
ANY接続拒否	② <input checked="" type="radio"/> しない <input type="radio"/> する
チャンネル	③ 11 (2462MHz)
Rts/Ctsスレッシュホールド	④ 無し
11g保護機能	⑤ 有効
パワーレベル	⑥ 高
接続端末制限	⑦ 255
Super A/Gを使用	⑧ しない

④ Rts/Ctsスレッシュ

ホールド
.....

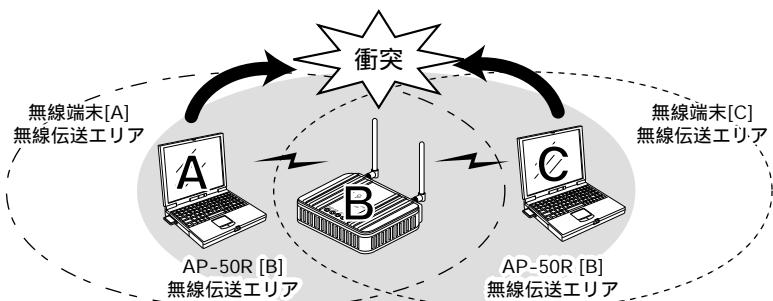
ネゴシエーションするために送るパケットのデータサイズを、「500バイト」または「1000バイト」から選択します。

(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端末[A]-[C]同士([A]に対して[C]、[C]に対して[A])のことを呼びます。

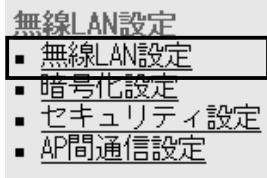
通信の衝突を防止するには、無線端末[A]から送信要求(Rts)信号を受信した本製品[B]が、無線伝送エリア内にある無線端末[A]および[C]に送信可能(Cts)信号を送り返すことで、Rts信号を送信していない無線端末[C]に本製品[B]が隠れ端末と通信中であることを認識させます。これにより、Rts信号を送信していない無線端末[C]は、無線ルータ[B]から受信完了通知(ACK)を受信するまで本製品[B]へのアクセスを自制して、通信の衝突を防止できます。



2 「無線LAN設定」メニュー

2-1.「無線LAN設定」画面

■ 無線LAN設定(つづき)



⑤ 11g保護機能

アクセスしてくる無線パソコンの無線LANの規格を認識して、接続を制限できます。
(出荷時の設定: 有効)

接続制限することで、[IEEE802.11b(11Mbps)]規格の通信を制限して、[IEEE802.11g(54Mbps)]規格の通信に影響され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。

⑥ パワーレベル

本製品に内蔵された無線LANカードの送信出力を設定します。

高/中/低(3段階)の中から選択できます。
(出荷時の設定: 高)

本製品の最大伝送距離は、パワーレベルが「高」の場合です。

パワーレベルを低くすると、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】

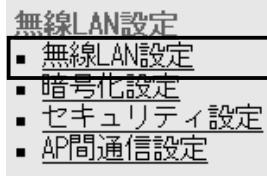
◎本製品から送信される電波が部屋の外に漏れるのを軽減したいとき

◎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軽減したいとき

2-1.「無線LAN設定」画面

■ 無線LAN設定(つづき)



⑦ 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)
接続制限を設定すると、本製品1台だけに接続が集中するのを防止(本製品の負荷を分散)できますので、接続集中による通信速度低下を防止できます。

⑧ Super A/Gを使用

米国Atheros Communications社が開発した、独自の無線LAN高速化技術です。 (出荷時の設定：しない)

「しない」、「する(圧縮なし)」、「する(圧縮あり)」から選択できます。
「する(圧縮あり)」を選択すると、通信速度がさらに向上します。

※すでに圧縮されているデータを取り扱う機会が多い場合、「する(圧縮あり)」を使用すると、圧縮されたデータを転送しているあいだは、速度が低下する原因となります。

このような場合は、「する(圧縮なし)」に設定してご使用ください。

※[Super A/G]の設定を「する(圧縮あり)」に設定して、無線AP間通信機能と暗号化[WEA(RC4)、OCB AES]機能を併せて使用する場合は、[キーインデックス(キーID)](☞P27)の設定を無線AP間通信する相手と同じ設定にしてください。

通信相手と異なる[キーインデックス(キーID)]を設定すると、通信できなくなります。

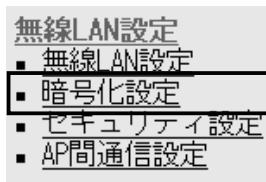
※無線パソコンに装着された無線LANカードが、Super A/Gに対応していない場合は、[Super A/G]を使用しないときと同じ状態になります。

※「SuperA」と「SuperG」は、別々に設定できません。

2 「無線LAN設定」メニュー

2-2.「暗号化設定」画面

■ 暗号化設定



無線LANで通信するデータを保護するために、暗号化するための設定です。

暗号化設定

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。
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

ネットワーク認証	①	両対応
暗号化方式	②	なし
PSK (Pre-Shared Key)	③	半角英数で8-63文字、または16進数で64桁を入力。
キー更新間隔	④	1 分
キージェネレータ	⑤	
キーインデックス	⑥	1

〈登録〉ボタン

「暗号化」画面で変更した内容を画面上で確定するボタンです。

変更した内容は、〈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」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〉や〈登録して再起動〉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」画面で変更したすべての設定内容を有効にします。

① ネットワーク認証

※弊社製無線LAN機器によ
っては、「認証モード」と
記載されています。

【暗号化方式】(②)欄で、「WEP RC4 64(40)」、「WEP RC4 128(104)」、「WEP RC4 152(128)」、「OCB AES 128(128)」を選択したとき、その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)

※通信相手とネットワーク認証の設定が異なると通信できません。

◎両対応

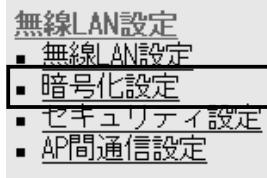
：無線LANのアクセスに対して、「オープンシステム」と「シェアードキー」を自動認識しますので、通信相手間で暗号化鍵(キー)が同じであれば通信可能です。

◎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。

2-2.「暗号化設定」画面

■ 暗号化設定(つづき)



暗号化設定

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。
キーの自動変更はRADiUS機能を使用する場合のみ有効です。

<input type="button" value="登録"/>	<input type="button" value="取消"/>	<input type="button" value="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			
ネットワーク認証	①	両対応	
暗号化方式	②	なし	
PSK (Pre-Shared Key)	③		
キー更新間隔	④	1 分	
キージェネレータ	⑤		
キーインデックス	⑥	1	

② 暗号化方式

無線伝送データを暗号化する方式を選択します。

(出荷時の設定:なし)

対応する暗号化方式は、「WEP RC4」、「OCB AES」、「WPA-PSK(TKIP/AES)」です。

異なる暗号化方式の相手とは互換性がありませんので、暗号化方式とビット数は、通信を行う相手間で、同じ設定にしてください。

◎WEP RC4 :

無線通信で一般によく使用されるセキュリティーです。

暗号化方式は、WEP 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。

※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。

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

◎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。

※Windows XP標準のワイヤレスネットワーク接続を使用して本製品に接続できません。

◎WPA-PSK(TKIP/AES) :

「WPA-PSK」は、Windows XP(Service Pack 1)に修正プログラムが適用されたパソコンで使用できる共有鍵認証方式です。暗号化方式は、「TKIP」と「AES」に対応しています。

※無線AP間通信機能を利用する場合、併せて使用できませんので、「WEP(RC4)/OCB AES」方式でご使用ください。

※SL-5200(弊社製無線LANカード)が装着されたWindows XP搭載のパソコンをご使用いただくと、Windows XP標準のワイヤレスネットワーク接続から本製品に接続できます。

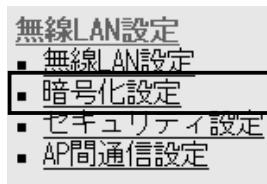
※「TKIP」と「AES」は、互換性がありません。

※「WEP(RC4)/OCB AES」とは、互換性がありません。

2 「無線LAN設定」メニュー

2-2.「暗号化設定」画面

■ 暗号化設定(つづき)



暗号化設定

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。
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			
ネットワーク認証	①	両対応	
暗号化方式	②	なし	
PSK (Pre-Shared Key)	③	半角英数で8~63文字、または16進数で64桁を入力。	
キー更新間隔	④	1	分
キージェネレータ	⑤		
キーインデックス	⑥	1	▼

③ PSK(Pre-Shared Key) …

[暗号化方式](②)欄で、「WPA-PSK(TKIP)」、または「WPA-PSK(AES)」を選択したとき、暗号化鍵(キー)を半角英数字で入力します。

※同じ暗号化方式を使用する相手と同じ暗号化鍵(キー)を設定してください。

※16進数で設定するときは、64桁を入力してください。

※ASCII文字で設定するときは、8~63文字を入力してください。

④ キー更新間隔 …

※弊社製無線LAN機器によ
っては、「Re-Key間隔」と
記載されています。

「WPA-PSK(TKIP)」、または「WPA-PSK(AES)」方式の暗号化を設定する場合、暗号化鍵(キー)の更新間隔を分単位で指定します。
(出荷時の設定：1分)

設定できる範囲は、「0~1440」です。

※「0」を設定した場合は、更新されません。

⑤ キージェネレータ …

[暗号化方式](②)欄で、「WEP RC4 64(40)」、「WEP RC4 128(104)」、「WEP RC4 152(128)」、「OCB AES 128(128)」を選択したとき、暗号化および復号に使う暗号化鍵(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。

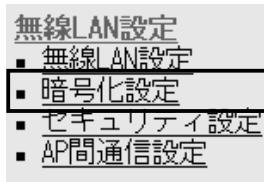
なお、入力した文字はすべて「*」で表示します。 (表示例：* *)
「暗号化方式」を選択して、〈登録〉をクリックすると、[キージェネレータ]欄に入力した文字列より生成された鍵(キー)を[WEPキー]項目のテキストボックスに表示します。

[WEPキー]項目(P28)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。
(取扱説明書[導入編]3-6章を参照)

次ページにつづく

2-2.「暗号化設定」画面

■ 暗号化設定(つづき)



暗号化設定

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。
キーの自動変更はRADiUS機能を使用する場合のみ有効です。

<input type="button" value="登録"/>	<input type="button" value="取消"/>	<input type="button" value="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			
ネットワーク認証	①	両対応	
暗号化方式	②	なし	
PSK (Pre-Shared Key)	③	半角英数で8-63文字、または16進数で64桁を入力。	
キー更新間隔	④	1 分	
キージェネレータ	⑤		
キーインデックス	⑥	1	

⑤キージェネレータ(つづき)

※「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、[WEPキー]項目のテキストボックスには表示されません。

※[WEPキー]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、[WEPキー]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。

※[WEPキー]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。

⑥キーインデックス

※弊社製無線LAN機器によっては、「キーID」と記載されています。

[暗号化方式](②)欄で、「WEP RC4 64(40)」、「WEP RC4 128(104)」、「WEP RC4 152(128)」、「OCB AES 128(128)」を選択したとき、[WEPキー]項目の「1」～「4」に設定された暗号化鍵(キー)のうち送信データの暗号化に使用する鍵(キー)を、テキストボックスの番号で指定します。

(出荷時の設定：1)

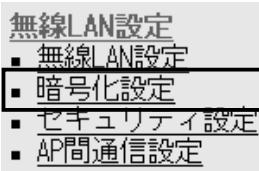
「1」～「4」に設定された暗号化鍵(キー)の内容が通信相手と同じであれば、通信する相手間で異なる番号を指定しても通信できます。
※本製品に無線LANで接続するパソコンの[キーID](キーインデックス)を設定するとき、Windows XP(Service Pack1を除く)標準のワイヤレスネットワーク接続を使用する場合は、[キーID](キーインデックス)の選択範囲が「0」～「3」で、本製品とは異なりますので注意してください。

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

2 「無線LAN設定」メニュー

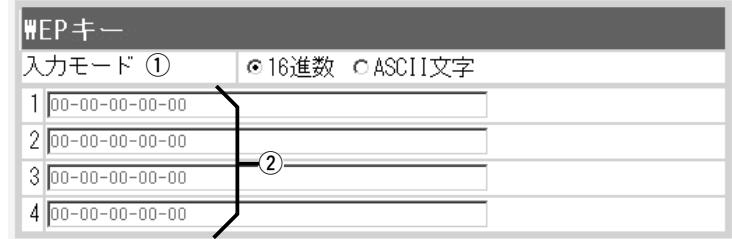
2-2.「暗号化設定」画面(つづき)

■ WEPキー



※弊社製無線LAN機器によ
っては、「キー値」と記載
されています。

「WEP RC4」、または「OCB AES」方式の暗号化で使用する暗号化
鍵(キー)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、[暗号化設定]項目の[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 ...

キー生成器を使用しない場合やASCII文字で入力するとき
は、暗号化および復号化に使用する鍵(キー)を、[入力モード](①)
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)

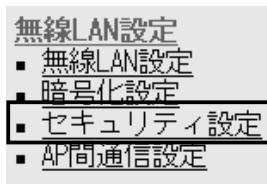
※16進数以外のアルファベットは、入力しても無効です。

※暗号化鍵(キー)は、通信する相手間で、すべての[キーインデッ
クス(キーID)]の値(1～4)に対して同じ内容に設定することをお
すすめします。

すべての[キーインデックス(キーID)]の値(1～4)に対して、暗
号化鍵が異なる場合、通信相手間で[キーインデックス(キーID)]
の設定が異なると、通信できないことがあります。

2-3.「セキュリティ設定」画面

■ RADIUS設定



RADIUSサーバを利用したIEEE802.1X認証についての設定です。

セキュリティ設定

RADIUSやMACアドレスフィルタリングなど、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、暗号化設定のキーインデックスは無効になります。

暗号化方式がRC4の場合のみWEPキーの自動配信を行います。

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。

RADIUS設定	
RADIUS機能を使用	① <input checked="" type="radio"/> しない <input type="radio"/> する
サーバアドレス	② プライマリ <input type="text"/> セカンダリ <input type="text"/>
サーバのポート番号	③ <input type="text"/> 1812 <input type="text"/> 1812
シークレットキー	④ <input type="text"/> <input type="text"/>
キーの自動変更を使う	⑤ <input checked="" type="radio"/> しない <input type="radio"/> する
再認証間隔	⑥ <input type="text"/> 120 <input type="text"/> 分

〈登録〉ボタン

「セキュリティ設定」画面の[MACアドレスフィルタリング設定]項目、および[無線端末間通信設定]項目の設定内容が有効になります。

※[RADIUS設定]項目の変更内容は、画面上で確定されるだけで、〈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サーバを利用して、IEEE802.1X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[キーインデックス]欄の設定は無効になります。

また、RADIUSサーバとの鍵交換は、「暗号化設定」画面にある[暗号化方式]欄で「WEP RC4」を設定するとき有効で、無線パソコン側では、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。

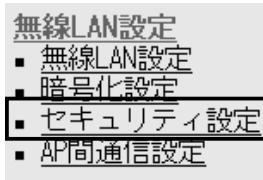
「暗号化設定」画面にある[暗号化方式]欄で「OCB AES」を設定するときは、RADIUS認証だけを行います。

このときは、RADIUSサーバと鍵交換をしません。

2 「無線LAN設定」メニュー

2-3.「セキュリティ設定」画面

■ RADIUS設定(つづき)



セキュリティ設定

RADIUSやMACアドレスフィルタリングなど、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、暗号化設定のキーインデックスは無効になります。

暗号化方式がRC4の場合のみWEPキーの自動配信を行います。

RADIUS設定は再起動後に有効になります。

RADIUS設定

RADIUS機能を使用 しない する

プライマリ

セカンダリ

サーバアドレス

サーバのポート番号

シークレットキー

キーの自動変更を使用 しない する

再認証間隔 分

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。

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ご確認ください。

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 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 2000(Service Pack4)やWindows XPを使って本製品にIEEE802.1X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とき設定します。

(出荷時の設定：する)

※弊社製無線LANカードに付属の設定ユーティリティーは、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ーをWindows XP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。

⑦ 再認証間隔

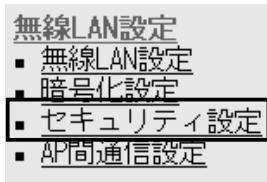
RADIUSサーバに再度認証を要求する間隔を分で設定します。

設定できる範囲は、「30～9999」です。 (出荷時の設定：120)

2-3.「セキュリティ設定」画面(つづき)

■ 無線端末間通信設定

無線パソコンどうしが本製品を介して通信するのを禁止するとき設定します。

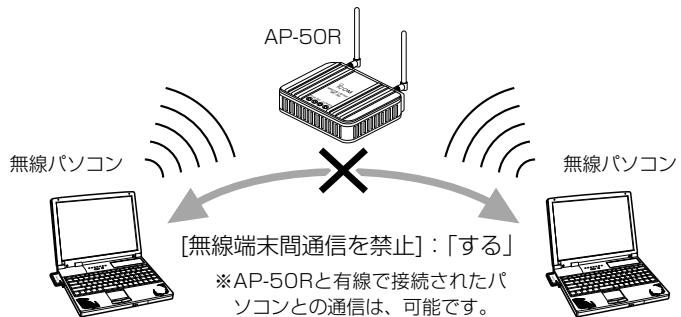


無線端末間通信を禁止

本製品を無線ホットスポット接続に利用するときなどは、設定を変更すると本製品を介して無線パソコンどうしが通信することを禁止できます。

(出荷時の設定：しない)

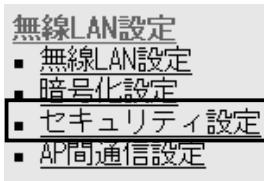
※この機能は、本製品で設定している無線チャンネルに該当する無線LAN規格の無線パソコンについて有効です。



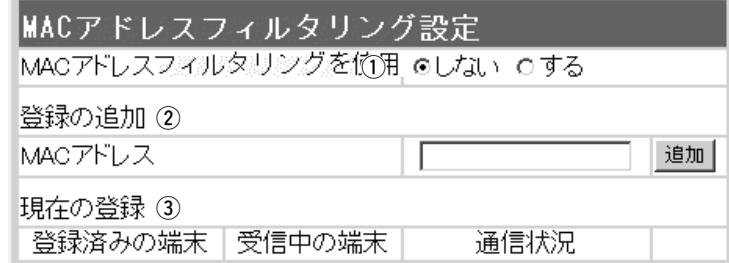
2 「無線LAN設定」メニュー

2-3.「セキュリティ設定」画面(つづき)

■ MACアドレスフィルタリング設定



通信を許可する無線端末のMACアドレスを登録することで、通信制限するとき必要な設定です。



① MACアドレス

フィルタリングを使用
※弊社製無線LAN機器によっては、「MACアドレスセキュリティ」と記載されています。

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のパソコン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アドレスフィルタリングが有効なとき、[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。

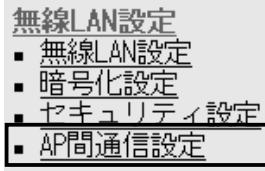
※最大256台分のMACアドレスを登録できます。
※入力は半角英数字で12桁(16進数)を入力します。
※入力後は〈追加〉をクリックして、[現在の登録]欄に登録されたことを確認してください。
※2つの入力例は、同じMACアドレスになります。
(入力例：00-90-c7-4B-00-32、0090c74B0032)

③ 現在の登録

本製品と無線で通信している端末の状況や登録済みの無線端末の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〉で登録の削除ができます。
受信中の端末欄に表示されているMACアドレスで登録されていないものは、〈追加〉ボタンが表示されますので、それをクリックすると、その端末のMACアドレスが登録できます。

2-4.「AP間通信設定」画面

■ BSSID



本製品に内蔵する無線LANカードの[BSSID]を表示します。

AP間通信設定

AP間通信 (Wireless Bridge) 機能の設定を行います。

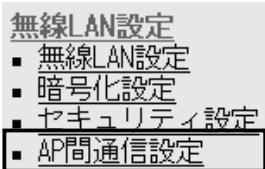
BSSID

00-90-C7-88-07-61

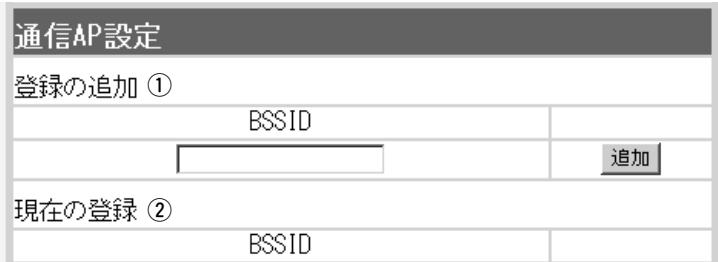
AP間通信を使用するときは、画面に表示された[BSSID]を相手側のAP-50Rに登録します。

また、本製品には相手側の[BSSID]を「ステーションリスト」に登録します。

■ 通信AP設定



AP間通信する相手のBSSIDを登録します。



①登録の追加

AP間通信する相手側(AP-50、SR-5200VoIP、SR-5000VoIP、AP-5100など)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-C7-88-00-65、0090C7880065)

②現在の登録

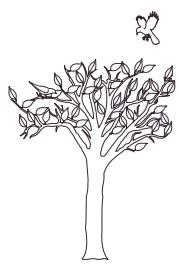
本製品に登録されている[BSSID]を表示します。

この欄に登録されている[BSSID]を持つ無線ルータや無線アクセスポイント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。





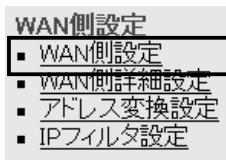
この章では、
「WAN側設定」メニューで表示される設定画面について説明します。

3-1.「WAN側設定」画面	36
■ 接続状況	36
■ 回線種別	37
■ 回線設定PPPoE/DHCP	38
■ 接続設定	39
3-2.「WAN側詳細設定」画面	40
■ 共通詳細設定	40
■ PPPoE詳細設定	42
3-3.「アドレス変換設定」画面	43
■ アドレス変換設定	43
■ パススルー設定	43
■ 静的マスカレードテーブル設定	44
■ DMZホスト機能と静的マスカレード機能の違い	44
■ 静的NATテーブル設定	45
3-4.「IPフィルタ設定」画面	46
■ 不正アクセス検知機能設定	46
■ IPフィルタ設定	48
■ 現在の登録	52

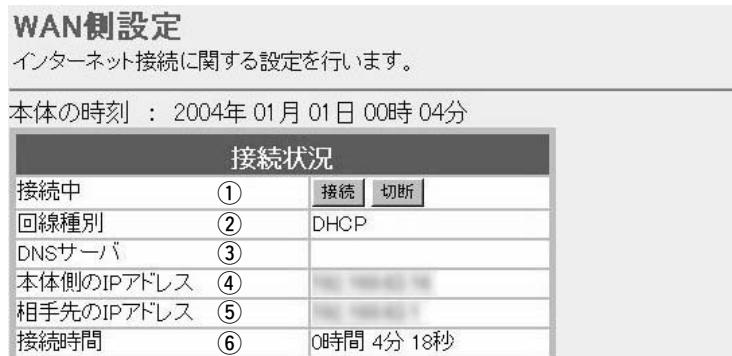
3 「WAN側設定」メニュー

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。



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

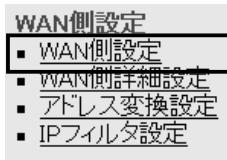
「DHCP」/「PPPoE」/「PPPoE複数固定IP」のいずれかが設定されている場合、契約されているプロバイダーのIPアドレスを表示します。

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、IP電話サービス対応のフレッツ・ADSLをご契約の場合に該当します。

◎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。

◎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。

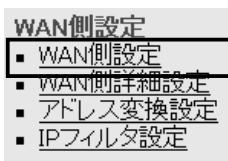
割り当てられた複数のIPアドレスの使いかたについては、「複数固定IPを使う」(☞7-1章)をご覧ください。

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画面。この画面で設定する項目が6つあります。①接続先名、②IPアドレス、③サブネットマスク、④デフォルトゲートウェイ、⑤プライマリDNSサーバ、⑥セカンダリDNSサーバ。各項目には入力欄があります。③サブネットマスクの欄の右側に、「固定のIPアドレスを使用するときのみ入力します。」と記載されています。

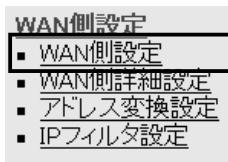
※回線種別を「PPPoE」に設定時の画面を例に説明しています。
※回線種別を「接続しない」に設定時は、表示されません。

- 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。
- ②IP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 <input type="checkbox"/> 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

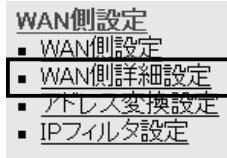
ご契約の回線接続業者、またはプロバイダーから指定された認証プロトコルを設定します。

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。

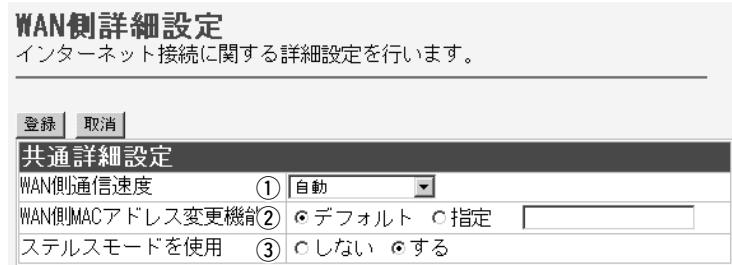
3 「WAN側設定」メニュー

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

本製品とLAN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す。

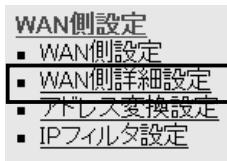
◎10(Full Duplex)：

[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す。

3-2.「WAN側詳細設定」画面

■ 共通詳細設定(つづき)



WAN側詳細設定

インターネット接続に関する詳細設定を行います。

登録

取消

共通詳細設定

WAN側通信速度	(1)	自動
WAN側MACアドレス変更機能	(2)	<input checked="" type="radio"/> デフォルト <input type="radio"/> 指定 <input type="text"/>
ステルスマードを使用	(3)	<input type="radio"/> しない <input checked="" type="radio"/> する

※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 ステルスマードを使用

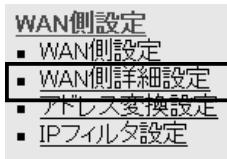
インターネットを使用して本製品に不正アクセスされた場合、Pingやポートスキャンに対して防御するかしないかの設定です。

(出荷時の設定：する)

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」で使用するとき設定します。

接続設定	① <input type="radio"/> 手動 <input checked="" type="radio"/> 自動 <input type="radio"/> 常時
自動切断タイマー	② 10 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)
①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。
②自動：パソコンからホームページやメールを見る操作をするだけで、自動的に接続します。
③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自動切断タイマー

[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。
※常時接続でご使用の場合は、「0」を設定します。

③MSS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。
一般に、MSS値は、フラグメントが発生しない範囲で大きいほど良いとされています。
しかし、[PPPoE]回線のMTUは、通常のEthernetのMTU(1500バイト)より小さいため、MSS値が大きくなりすぎると、パケットがインターネット上を通過しないことがありますので、ご注意ください。

④ACネーム

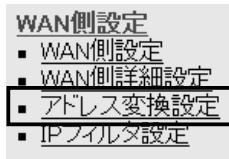
プロバイダーから指定されている場合に限り、指定のACネーム(アクセスコンセントレーター名)を入力します。

⑤サービスネーム

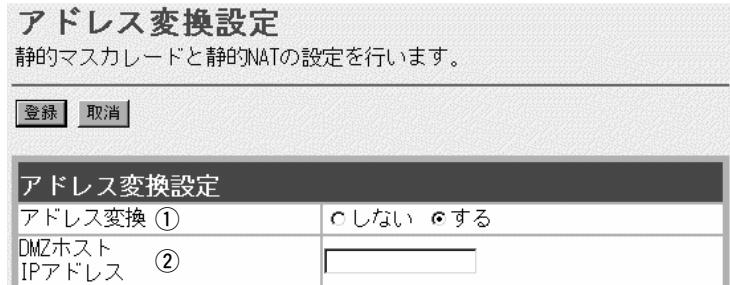
プロバイダーから指定されている場合に限り、指定のサービスネームを入力します。

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 アドレス変換

静的マスカレード機能、静的NAT機能を使用して、指定したグローバルアドレスをプライベートアドレスに変換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.....

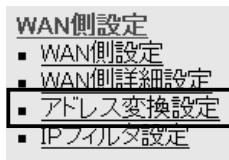
DMZホスト機能(非武装セグメント)の対象となるパソコン(ホスト)のIPアドレスを入力します。

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できるが、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ーが低下しますので、ご使用には十分ご注意ください。

※DMZホスト機能を静的マスカレードテーブルや静的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

※使用例については、本書7-3章を参考に、パソコンを設定してください。

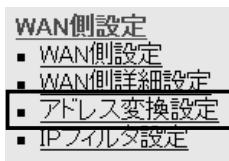
マルチプロトコル仮想プライベートネットワーク(VPN)をサポートするネットワーク技術で、クライアントからのPPTPパケットをWAN側に転送するかしないかの設定です。

(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画面。上部には「静的マスカレードテーブル設定」というヘッダーがあります。下部には「登録の追加」と「現在の登録」の2つのセクションがあります。各セクションには「ローカルIP」、「プロトコル」、「ポート」、「開始ポート」、「終了ポート」などの入力欄があります。右側には「追加」ボタンがあります。

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。

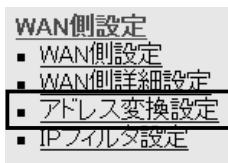
■ DMZホスト機能と静的マスカレード機能の違い

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

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="text"/>	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。

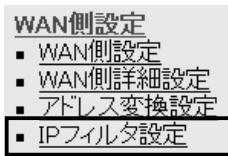
◎ローカルIP：任意のプライベートIPアドレスを入力します。

※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。

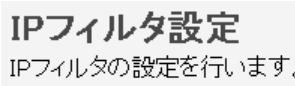
3 「WAN側設定」メニュー

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。



〈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)

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 type="radio"/> しない <input checked="" 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

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。

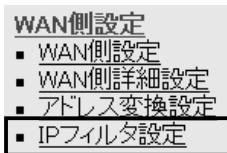
[検知時間](③)欄で設定した時間内に設定回数以上のアクセスを検知すると、不正アクセスと判断します。

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ーの設定です。

IPフィルタ設定画面。以下の項目が表示されています。

IPフィルタ設定		追加
番号	①	□
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="checkbox"/> 指定時: □
発信元ポート番号	⑤	指定 <input type="checkbox"/> 指定時: □ ~ □
宛先ポート番号	⑥	指定 <input type="checkbox"/> 指定時: □ ~ □
発信元IPアドレス	⑦	□ ~ □
宛先IPアドレス	⑧	□ ~ □

〈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。

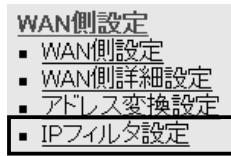
◎WAN側から : WAN側から本製品が受信するIPパケットに対して、アドレス変換のあとにフィルタリング処理をします。

◎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、アドレス変換の前にフィルタリング処理をします。

◎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します。

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 checked="" 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="button" value="▼"/> 指定時: <input type="text"/>
発信元ポート番号	⑤	指定 <input type="button" value="▼"/> 指定時: <input type="text"/> ~ <input type="text"/>
宛先ポート番号	⑥	指定 <input type="button" value="▼"/> 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すが、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)

- 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="checkbox"/> 指定時: <input type="text"/>
発信元ポート番号	(5)	指定 <input type="checkbox"/> 指定時: <input type="text"/> ~ <input type="text"/>
宛先ポート番号	(6)	指定 <input type="checkbox"/> 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、二一モニック(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、二一モニック(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="button" value="▼"/> 指定時: <input type="text"/>
発信元ポート番号	⑤	指定 <input type="button" value="▼"/> 指定時: <input type="text"/> ~ <input type="text"/>
宛先ポート番号	⑥	指定 <input type="button" value="▼"/> 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(つづき)

■ 現在の登録

- 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

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

◎59~64番 : Windowsのアプリケーションを外部からリモートコントロールされる危険性を防止

〈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〉ボタンをクリックすると、IPフィルターが削除されます。

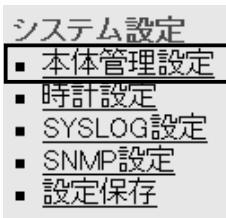
この章では、
「システム設定」メニューで表示される設定画面について説明します。

4-1.「本体管理設定」画面	54
■ 管理者ID設定	54
■ 管理者IPアドレス	55
4-2.「時計設定」画面	56
■ 内部時計設定	56
■ 自動時計設定	57
4-3.「SYSLOG設定」画面	58
■ SYSLOG設定	58
4-4.「SNMP設定」画面	59
■ SNMP設定	59

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。



〈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文字以内で入力します。
(入力例：user)
[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)」、または「●(黒丸)」で表示されます。
(入力例：userpass 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。

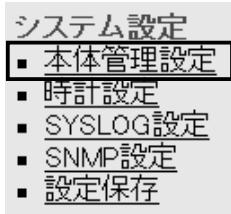
③パスワードの確認入力

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)

■ 管理者IPアドレス



本製品の設定画面へのアクセスをIPアドレスで制限するときの設定です。

管理者IPアドレス	
管理者IP1	<input type="text"/>
管理者IP2	<input type="text"/>
管理者IP3	<input type="text"/>

本製品の設定画面へのアクセスを制限する場合に、管理者が本製品に有線または無線でアクセスするパソコンのIPアドレスを3台まで登録できます。 (入力例：192.168.0.5)

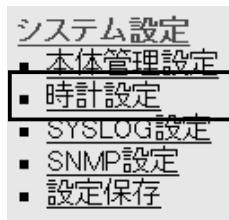
※[管理者IPアドレス]を設定すると、IPアドレスが登録されたパソコン以外は、次のアクセスから本製品の設定画面にアクセスできなくなります。

※空白の場合は、本製品に接続するすべてのパソコンが設定画面にアクセスできます。

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。



〈登録〉ボタン

[自動時計設定]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

「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の時刻を、最初に表示します。

※〈取消〉ボタンをクリックすると、空白になります。

WWWブラウザの〈更新〉ボタンをクリックすると、パソコンの時計設定を取得して表示します。

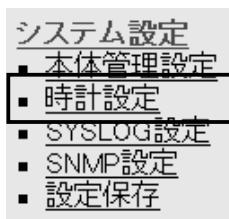
③ 〈時刻設定〉ボタン

[設定する時刻](②)欄に表示された時刻を本製品に設定するボタンです。

時刻を正確に設定するときは、本製品の設定画面に再度アクセスしなおすか、WWWブラウザの〈更新〉ボタンをクリックしてから、〈時刻設定〉ボタン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。

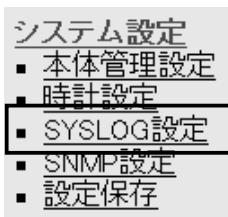
自動時計設定	
自動時計設定を使用	<input type="radio"/> しない <input checked="" type="radio"/> する
NTPサーバ1 IPアドレス	133.100.9.2
NTPサーバ2 IPアドレス	
アクセス時間間隔	1 日
前回アクセス日時	----/--/-- --:--
次回アクセス日時	2003/01/02 00:00

- 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して、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す。
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。

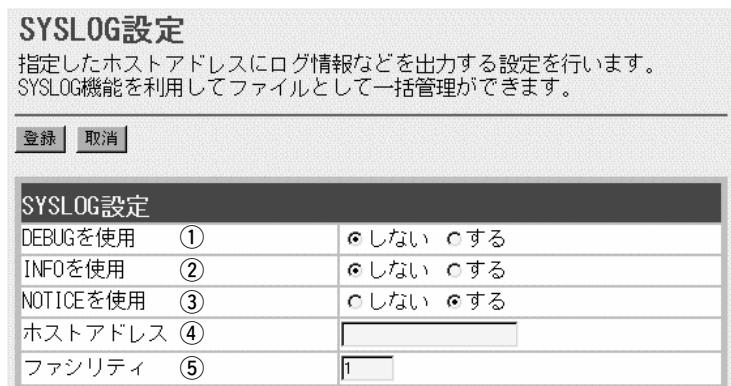
4 「システム設定」メニュー

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を出力する設定をします。



〈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

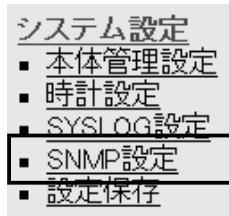
SYSLOG機能を使用する場合、SYSLOGを受けるホストのアドレスを入力します。
ホストはSYSLOGサーバ機能に対応している必要があります。

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。
(出荷時の設定：1)
通常「1」を使用します。

4-4.「SNMP設定」画面

■ SNMP設定



TCP/IPネットワークにおいて、ネットワーク上の各ホストから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	public
-----------------	--------

コミュニティID(SET) ③	private
-----------------	---------

〈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「しない」かを選択します。

(出荷時の設定：する)

② コミュニティID(GET)

本製品の設定情報をSNMP管理ツール側から読み出すことを許可するIDを設定します。

(出荷時の設定：public)

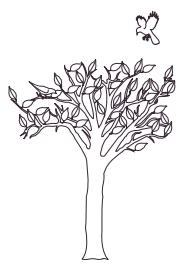
入力は、半角31文字以内の英数字で入力します。

③ コミュニティID(SET)

本製品の設定情報をSNMP管理ツール側から変更することを許可するIDを設定します。

(出荷時の設定：private)

入力は、半角31文字以内の英数字で入力します。



この章では、
「情報表示」メニューで表示される設定画面について説明します。

5-1.「通信記録」画面	62
■ 通信記録	62
5-2.「ネットワーク情報」画面	62
■ ネットワーク インターフェイス リスト	62
■ ブリッジポート情報	63
■ 本体MACアドレス	63

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	
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 [172.20.0.5]
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 [172.20.0.5]

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	
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 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	██████████	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	9
		受信パケット数	18
Wireless	②	状況	通信中
		送信パケット数	8
		受信パケット数	0
Wireless Bridge	③	状況	通信中
00-90-C7-90-00-02		送信パケット数	8
		受信パケット数	0

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 Wireless 無線通信状況と、そのときの送信と受信のパケット数を表示します。

③ Wireless Bridge 無線AP間通信の状況と、そのときの送信と受信のパケット数を表示します。

また、通信相手側の[BSSID]を表示します。

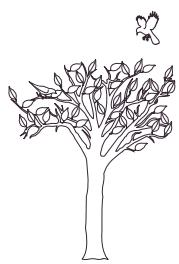
■ 本体MACアドレス



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。

本体MACアドレス
00-90-C7-95-00-66



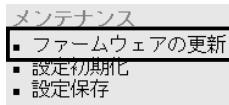
この章では、
「メンテナンス」メニューで表示される設定画面について説明します。

6-1.「ファームウェアの更新」画面	66
■ ファームウェアファイルを指定	66
■ 「Firm Utility使用」モード	67
6-2.「設定初期化」画面	68
■ 「設定初期化」画面	68
6-3.「設定保存」画面	69
■ 設定の保存と書き込み	69
■ 現在の設定	70

6 「メンテナンス」メニュー

6-1.「ファームウェアの更新」画面

■ フームウェアファイルを指定

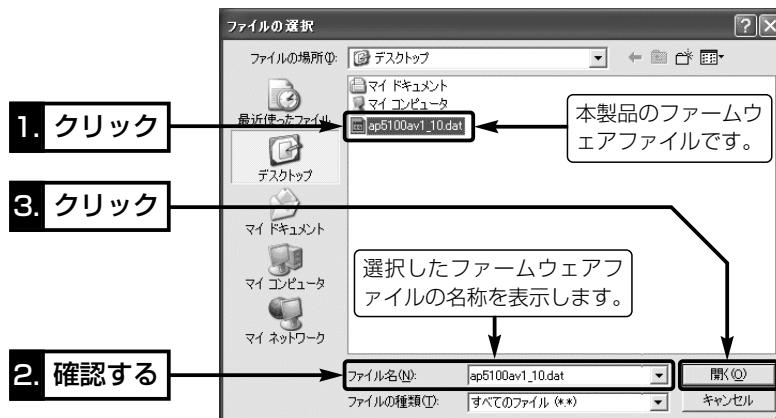


本製品のファームウェアをバージョンアップするときなど、アイコムホームページからダウンロードしているファームウェアファイルを指定して書き込むとき使用します。



① <参照...> ボタン

パソコンに保存しているファームウェアファイル(拡張子 : .dat)の保存先をテキストボックスに直接入力する代わりに、このボタンをクリックして表示される「ファイルの選択」画面(☞下記参照)ら目的の設定ファイルをクリックして、<開く(Q)> をクリックすると、指定したファイルとその階層がテキストボックスに自動入力されます。

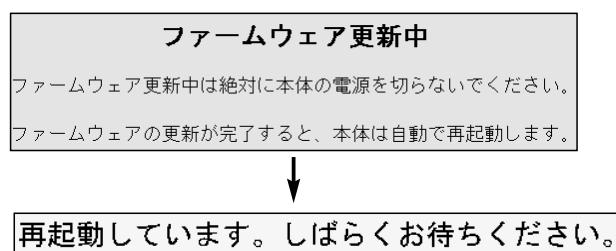


② <書き込み> ボタン

テキストボックスに表示された保存先のファームウェアファイル(拡張子 : .dat)を本製品に書き込みます。

本製品の設定画面が表示されるまで、そのまま待ちます。

- 書き込み中は、次の画面を表示後、「再起動しています。しばらくおまちください。」と表示します。



6-1.「ファームウェアの更新」画面(つづき)

■「Firm Utility使用」モード

- メンテナンス
- ファームウェアの更新
 - 設定初期化
 - 設定保存

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す。

「Firm Utility使用」モード

移行する

実行

「Firm Utility使用」モードにするとときは、[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。

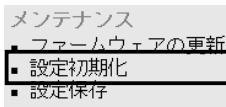
※「Firm Utility使用」モードに移行しないと、「Firm Utility」と本製品が通信できません。

6 「メンテナンス」メニュー

6-2.「設定初期化」画面

■ 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。



設定初期化

本体の設定を初期化し、必要に応じて再起動します。

設定初期化

初期化する

実行

[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。

6-3.「設定保存」画面

■ 設定の保存と書き込み

- メンテナンス
 - フームウェアの更新
 - 設定初期化
 - 設定保存

本製品の設定内容を保存したり、保存した設定ファイルを本製品に書き込んだりします。

設定保存

全設定内容を保存することができます。

設定の保存と書き込み

保存したファイルを書き込む① [参照...] [書き込む]
ファイルに保存する ② [ファイルに保存]

① 保存したファイルを
書き込む

[ファイルに保存する](②)欄の操作で保存した設定ファイル(拡張子: .sav)内容を本製品に書き込むとき使用します。

設定ファイルの保存先をテキストボックスに直接入力するか、〈参照...〉ボタンをクリックします。



右上の画面から目的の設定ファイルをクリックして、〈開く(O)〉をクリックします。

テキストボックスに保存先を指定後、〈書き込み〉ボタンをクリックすると、本製品にその設定内容を書き込みます。

書き込む前の設定内容は、消去されますのでご注意ください。

※市販のソフトウェアなどで編集したものは、誤動作の原因になりますので、本製品に登録しないでください。

② ファイルに保存する

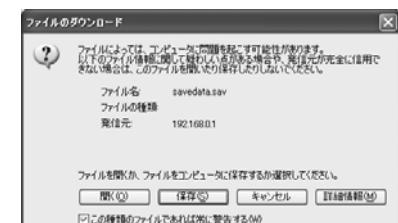
本製品すべての設定内容をパソコンに保存することで、本製品の設定をバックアップすることができます。

[設定の保存と書き込み]項目

で[ファイルに保存]をクリックすると表示される右の画面から〈保存(S)〉をクリックすると、設定ファイルを保存できます。

設定ファイルのファイル形式(拡張子)は、「.sav」です。

保存したファイルは、[保存したファイルを書き込む](①)欄の操作で、本製品自身や本製品を使用する別の相手に書き込みできます。



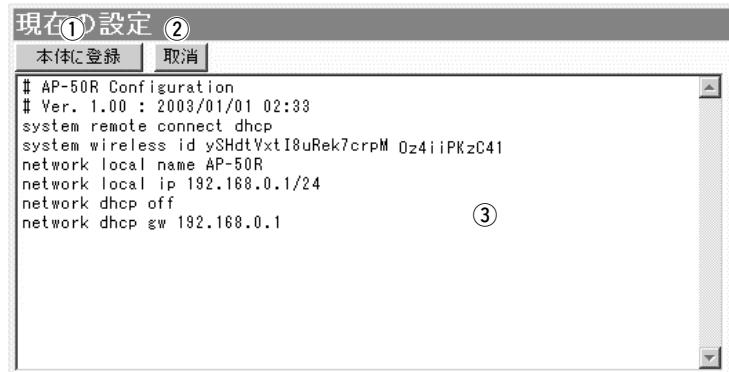
6 「メンテナンス」メニュー

6-3.「設定保存」画面(つづき)

■ 現在の設定

- メンテナンス
 - フームウェアの更新
 - 設定初期化
 - 設定保存

本製品の設定変更内容を確認したり、表示された内容を本製品に書き込みします。



① 〈本体に登録〉ボタン

「内容表示」(③)部に表示された内容を、本製品に書き込みます。

※[設定の保存と書き込み]項目(P79)の「ファイルに保存」をクリックして保存した設定ファイル(拡張子 : .sav)は、このボタンを使用して書き込みできません。

② 〈取消〉ボタン

「内容表示」(③)部に表示された内容を変更したとき、変更を取り消して、変更前の内容に戻します。

※〈本体に登録〉ボタンをクリックすると、変更前の内容には戻りません。

③ 「内容表示」画面

基本的な設定と初期値から変更された設定を表示します。

この画面内容を設定ファイルとしてパソコンに保存するときは、[設定の保存と書き込み]項目(P79)を使用してください。

※各画面で設定されたSSID、パスワード、キージェネレータ(暗号化鍵の生成元文字列)の内容は、暗号化されて表示されます。そのため、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。

この章では、

複数固定IPアドレスサービス、Telnetによる接続、PPTPパススルーで使用するパソコンの設定、Webサーバを公開するための設定について説明します。

7-1.複数固定IPアドレスサービスを使うには	72
■ グローバル固定IPアドレスの使いかた	72
7-2.Telnetによる接続	73
■ Windows 2000/Windows XPの場合	73
■ Windows 98/98 SE/Meの場合	73
■ オンラインヘルプ	74
7-3.PPTPパススルーで使用するパソコンの設定	75
■ Windows XPをクライアントに使用する場合	75
■ Windows 2000をクライアントに使用する場合	80
■ Windows Meをクライアントに使用する場合	84
7-4.Web公開の設定例	91
1. WWWサーバの設定	91
2. Web公開の設定	92

7-1.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」[P47](#))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。

■ 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。

7-2.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 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(P64)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 AP-50R! You are administrator!)が表示されます。

■ 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(P64)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 AP-50R! You are administrator!)が表示されます。

7 ご参考に

7-2.Telnetによる接続(つづき)

■オンラインヘルプ

Telnetを使用したターミナルソフトの接続では、オンラインで、コマンドリファレンスを参照できます。

◎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。

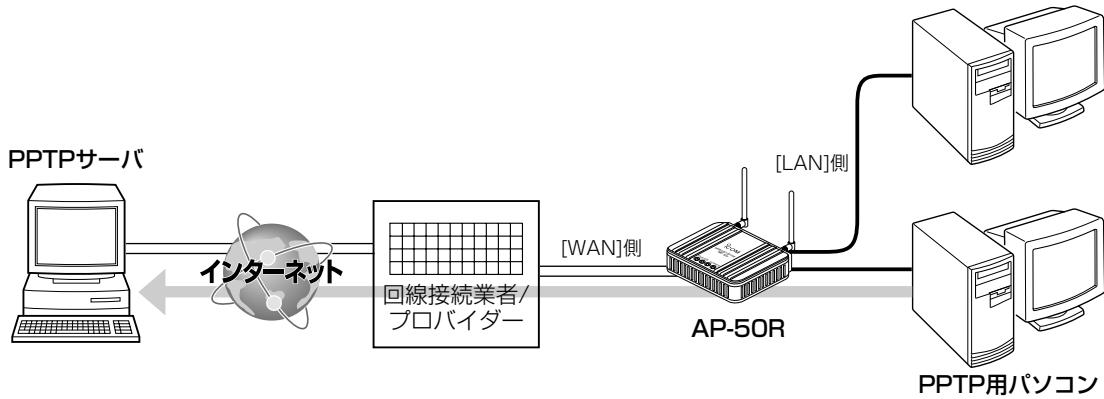
例) r[Tab]→re

re[Tab]→restart remote

res[Tab]→restart

7-3.PPTPパススルーで使用するパソコンの設定

■ Windows XPをクライアントに使用する場合



〈PPTP用のパソコン設定例〉

◎Windows XPの場合

ご契約のプロバイダーを介して、インターネットで会社のネットワークに接続するような場合の設定例です。

〈設定の手順〉

- ① 設定に使用するパソコンを起動します。
- ② 「ログオン」画面が表示されたら、管理者のユーザー名でログオンします。
- ③ 起動したら、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。
- ④ 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。
- ⑤ [ネットワーク接続]アイコンをクリックします。(下図)



- ⑥ [新しい接続を作成する]をクリックします。(下図)



7 ご参考に

7-3.PPTPパススルーで使用するパソコンの設定

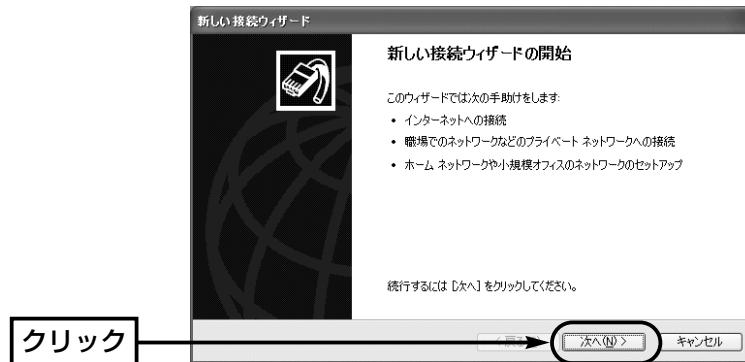
■ Windows XPをクライアントに使用する場合

〈PPTP用のパソコン設定例〉

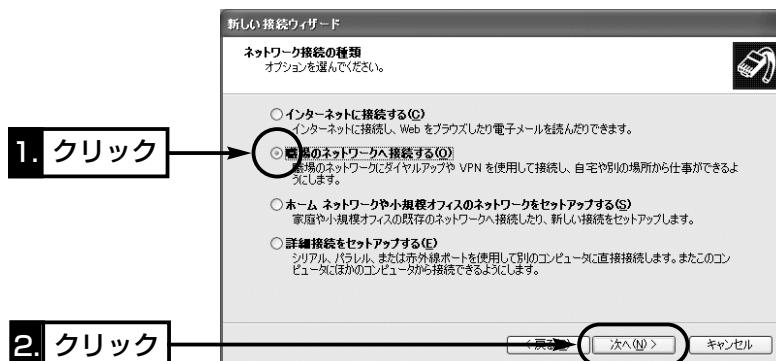
◎Windows XPの場合

〈設定の手順〉(つづき)

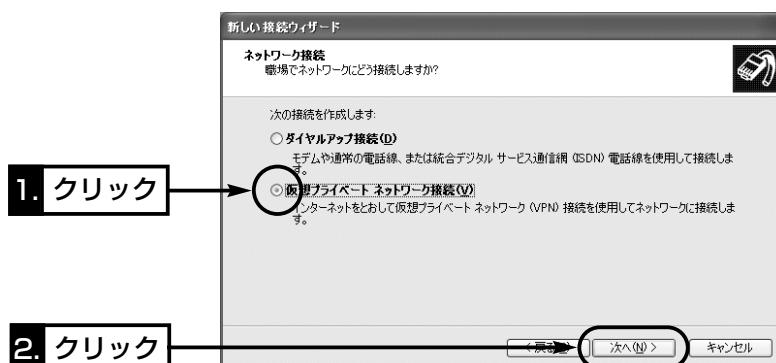
⑦ 〈次へ(N)〉をクリックします。



⑧ [職場のネットワークへ接続する(W)]のラジオボタンをクリックして、〈次へ(N)〉をクリックします。



⑨ [仮想プライベート ネットワーク接続(V)]のラジオボタンをクリックして、〈次へ(N)〉をクリックします。



7-3.PPTPパススルーで使用するパソコンの設定

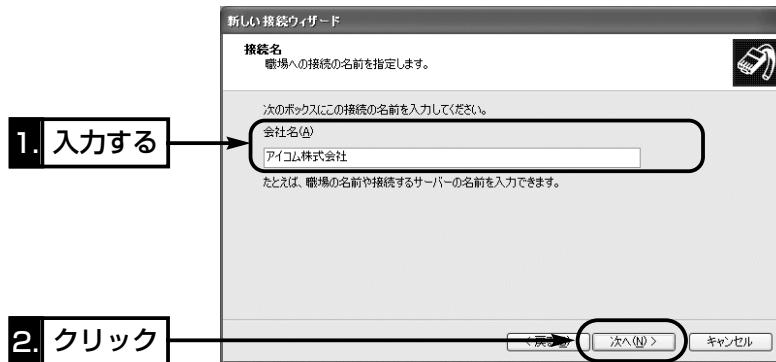
■ Windows XPをクライアントに使用する場合

<PPTP用のパソコン設定例>

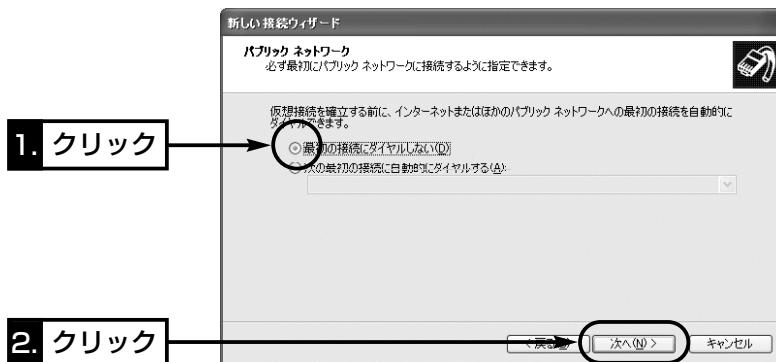
◎Windows XPの場合

<設定の手順> (つづき)

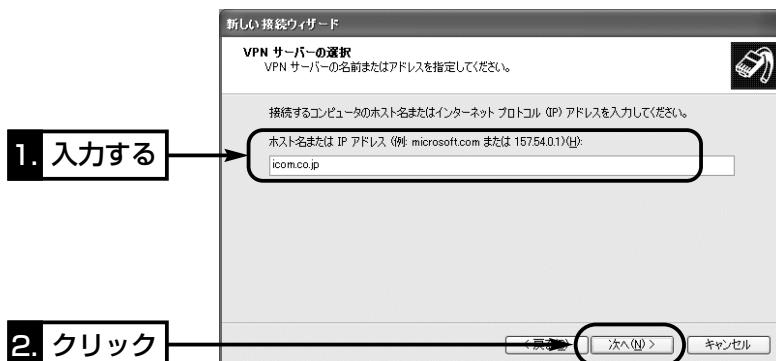
- ⑩ 接続先名を[会社名(A)]のテキストボックスに入力して、<次へ(N)>をクリックします。



- ⑪ 次の画面が表示されたときは、[最初の接続にダイヤルしない(D)]をクリックして、<次へ(N)>をクリックします。



- ⑫ ネットワーク管理者から指定された接続先のホスト名、またはIPアドレスを入力して、<次へ(N)>をクリックします。



7 ご参考に

7-3.PPTPパススルーで使用するパソコンの設定

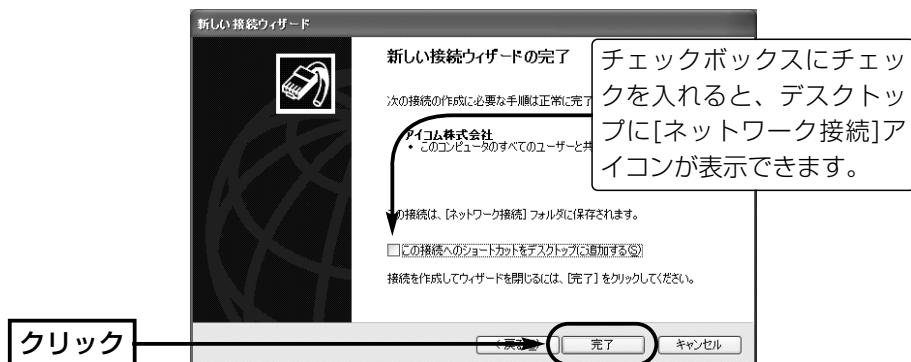
■ Windows XPをクライアントに使用する場合

〈PPTP用のパソコン設定例〉

◎Windows XPの場合

〈設定の手順〉(つづき)

⑬ 〈完了〉をクリックします。



⑭ PPTPサーバに設定された[ユーザー名(U)]と[パスワード(P)]を入力して、〈接続(C)〉をクリックします。



※上記画面で〈キャンセル〉をクリックした場合の接続方法は、次ページで説明しています。

7-3.PPTPパススルーで使用するパソコンの設定

■ Windows XPをクライアントに使用する場合

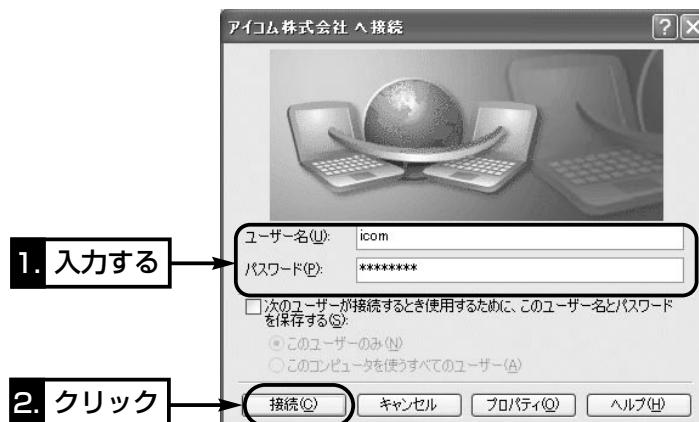
<PPTP用のパソコン設定例>

◎Windows XPの場合(つづき) <設定後、接続するには>

- ① <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 仮想プライベート ネットワークにあるアイコンをクリックします。



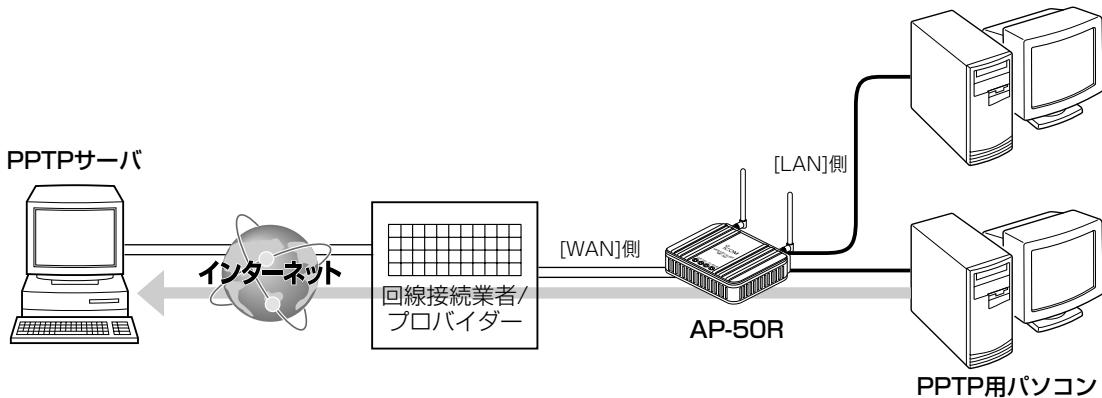
- ⑤ PPTPサーバに設定された[ユーザー名(U)]と[パスワード(P)]を入力して、<接続(C)>をクリックします。



7 ご参考に

7-3.PPTPパススルーで使用するパソコンの設定(つづき)

■ Windows 2000をクライアントに使用する場合



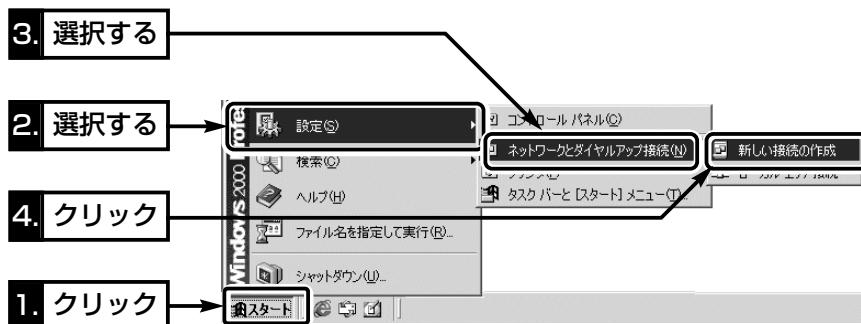
〈PPTP用のパソコン設定例〉

◎Windows 2000の場合

ご契約のプロバイダーを介して、インターネットで会社のネットワークに接続するような場合の設定例です。

〈設定の手順〉

- ① マウスを〈スタート〉→[設定(S)]→[ネットワークとダイヤルアップ接続(N)]の順番に操作して、[新しい接続の作成]をクリックします。



- ② 〈次へ(N)〉をクリックします。



7-3.PPTPパススルーで使用するパソコンの設定

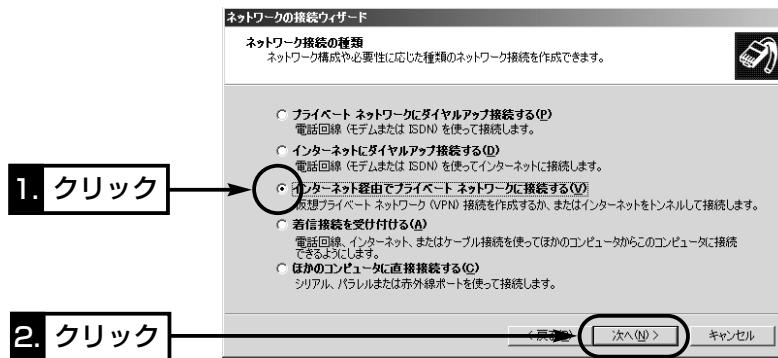
■ Windows 2000をクライアントに使用する場合

<PPTP用のパソコン設定例>

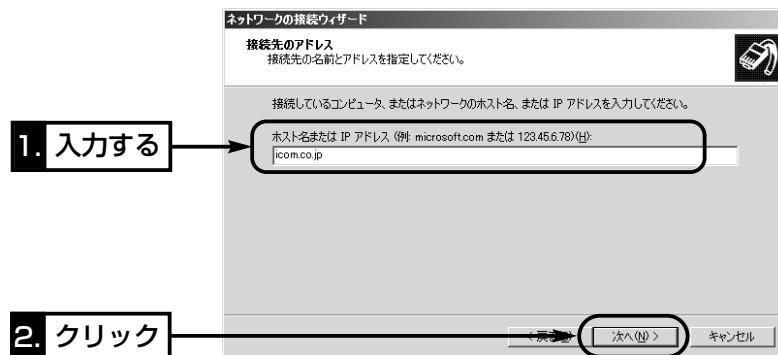
◎Windows 2000の場合

<設定の手順> (つづき)

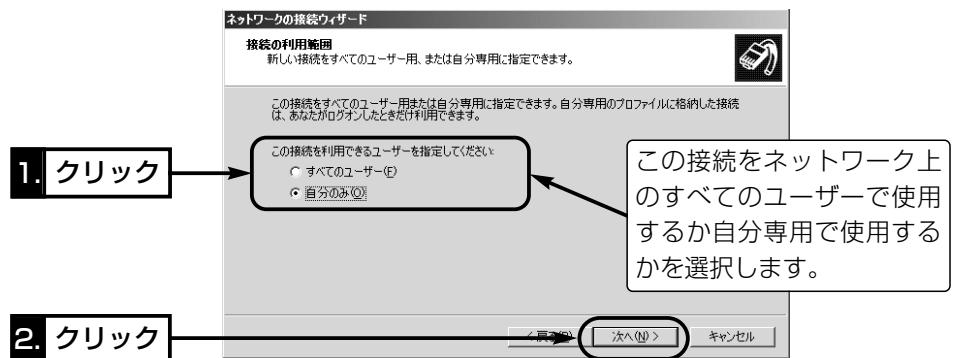
- ③ [インターネット経由でプライベート ネットワークに接続する (V)]のラジオボタンをクリックして、<次へ(N)> をクリックします。



- ④ ネットワーク管理者から指定された接続先のホスト名、または IP アドレスを入力して、<次へ(N)> をクリックします。



- ⑤ 使用目的に該当する(例：自分のみ(C))ラジオボタンをクリックしてから、<次へ(N)> をクリックします。



7 ご参考に

7-3.PPTPパススルーで使用するパソコンの設定

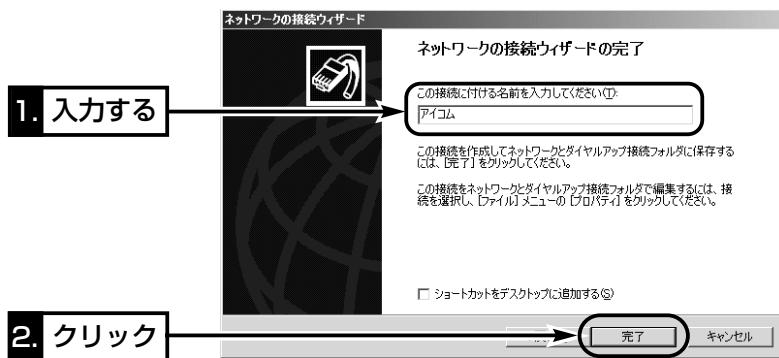
■ Windows 2000をクライアントに使用する場合

〈PPTP用のパソコン設定例〉

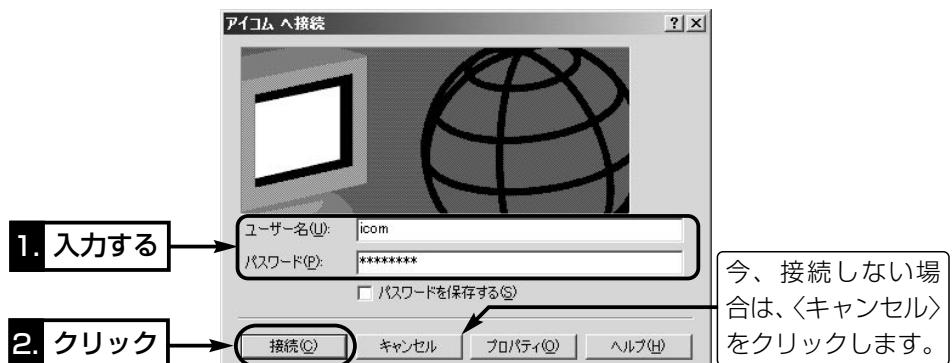
◎Windows 2000の場合

〈設定の手順〉(つづき)

- ⑥あとでわかるように、任意で接続先名を入力して、〈次へ(N)〉をクリックします。



- ⑦PPTPサーバに設定された[ユーザー名(U)]と[パスワード(P)]を入力して、〈接続(C)〉をクリックします。



※上記画面で〈キャンセル〉をクリックした場合の接続方法は、次ページで説明しています。

7-3.PPTPパススルーで使用するパソコンの設定

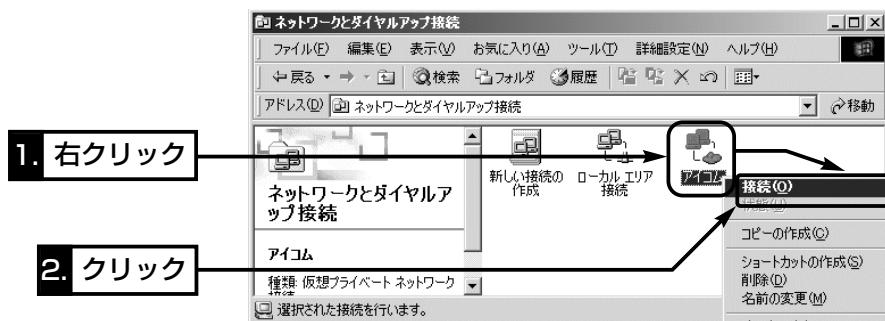
■ Windows 2000をクライアントに使用する場合

<PPTP用のパソコン設定例>

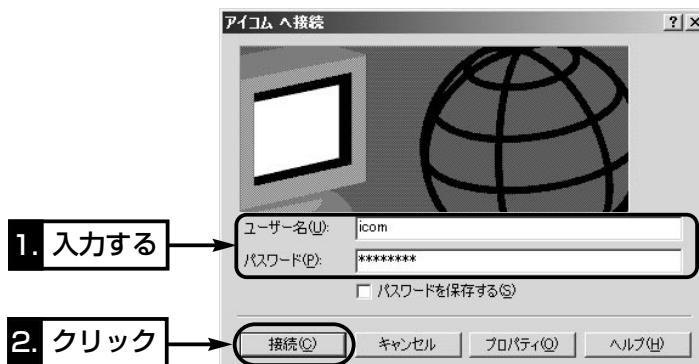
◎Windows 2000の場合(つづき)

<設定後、接続するには>

- ①マウスを <スタート> → [設定(S)] → [ネットワークとダイヤルアップ接続(N)] の順番に操作します。
- ②新しく作成されたアイコンを右クリックして、[接続(C)]をクリックします。



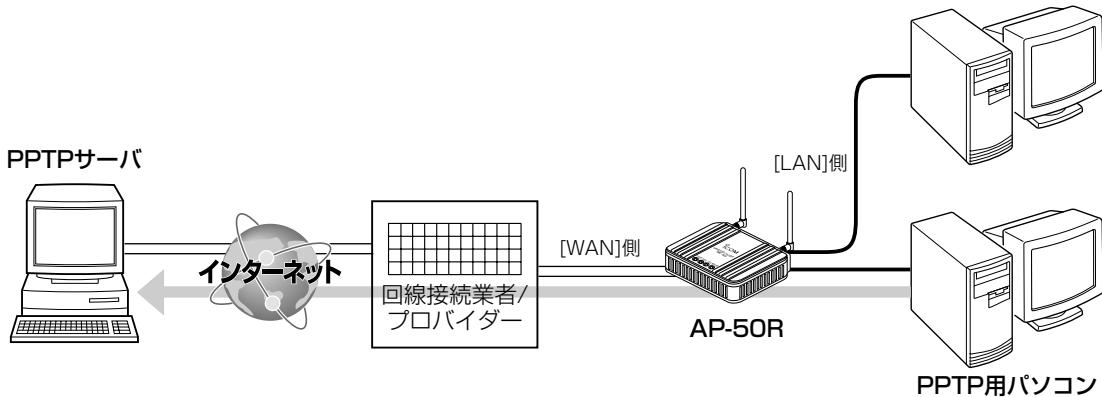
- ③PPTPサーバに設定された[ユーザー名(U)]と[パスワード(P)]を入力して、<接続(C)>をクリックします。



7 ご参考に

7-3.PPTPパススルーで使用するパソコンの設定(つづき)

■ Windows Meをクライアントに使用する場合



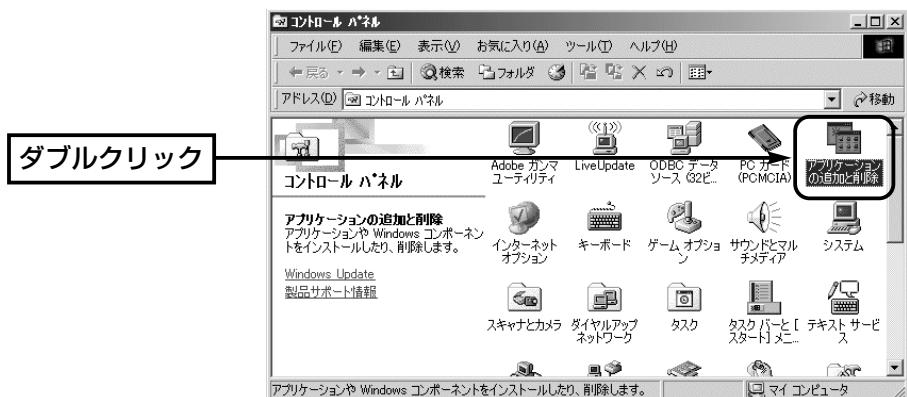
〈PPTP用のパソコン設定例〉

◎Windows Meの場合

ご契約のプロバイダーを介して、インターネットで会社のネットワークに接続するような場合の設定例です。

〈設定の手順〉

- ① マウスを〈スタート〉→[設定(S)]→[コントロールパネル(C)]の順番に操作します。
- ② [アプリケーションの追加と削除]をダブルクリックします。



7-3.PPTPパススルーで使用するパソコンの設定

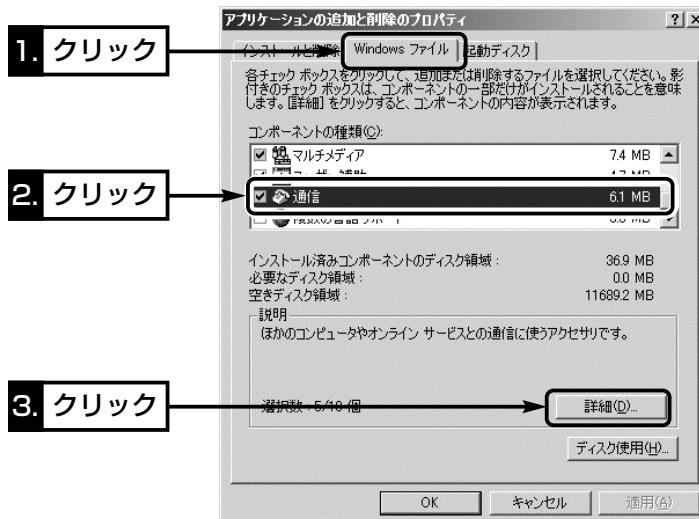
■ Windows Meをクライアントに使用する場合

<PPTP用のパソコン設定例>

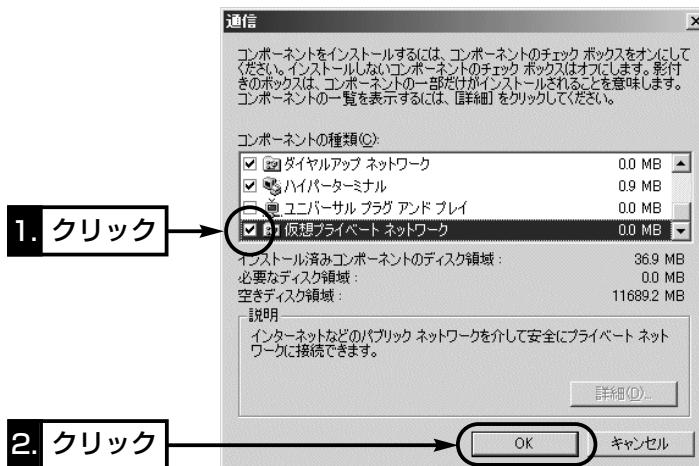
◎Windows Meの場合

<設定の手順> (つづき)

- ③ [Windows ファイル]タブ→[通信]→<詳細(D)> の順にクリックします。



- ④ [仮想プライベート ネットワーク]のチェックボックスにチェックを入れてから、<OK> をクリックします。



7 ご参考に

7-3.PPTPパススルーで使用するパソコンの設定

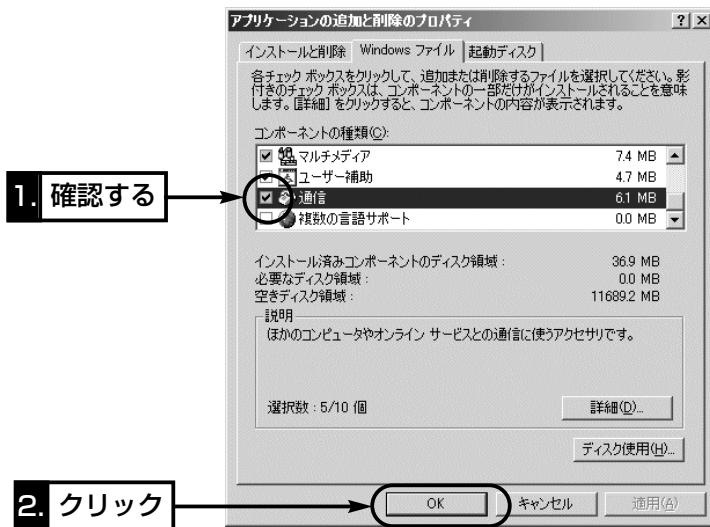
■ Windows Meをクライアントに使用する場合

〈PPTP用のパソコン設定例〉

◎Windows Meの場合

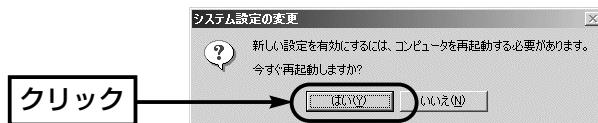
〈設定の手順〉(つづき)

- ⑤ [通信]にチェックマークが入っていることを確認して、〈OK〉をクリックします。

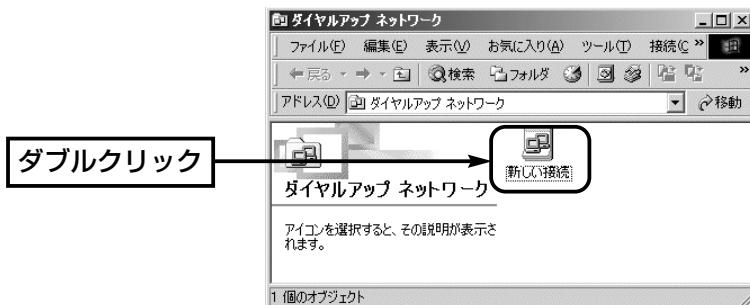


- ⑥ 〈はい(Y)〉をクリックします。

- パソコンが再起動します。



- ⑦ マウスを〈スタート〉→[設定(S)]→[ネットワークとダイヤルアップ接続(N)]の順番に操作して、[新しい接続]をダブルクリックします。



7-3.PPTPパススルーで使用するパソコンの設定

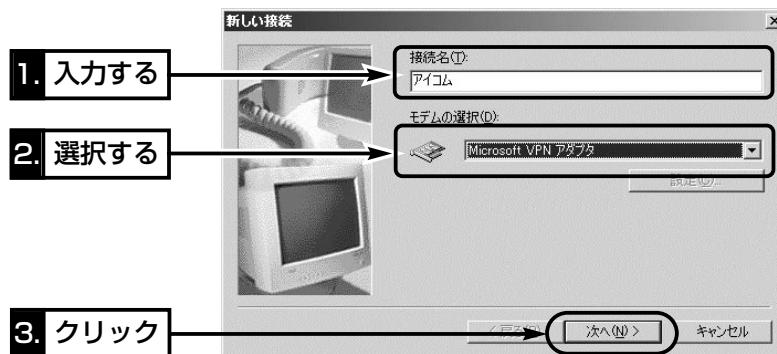
■ Windows Meをクライアントに使用する場合

<PPTP用のパソコン設定例>

◎Windows Meの場合

<設定の手順> (つづき)

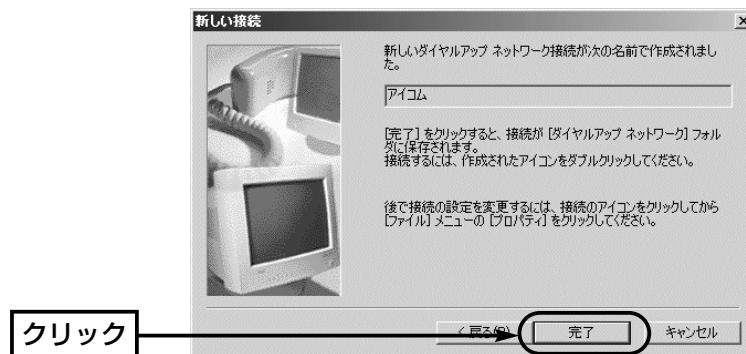
- ⑧ [接続名(I)]には、あとでわかるように、任意で接続先名を入力します。
 ⑨ [モデムの選択(D)]から、「Microsoft VPN アダプタ」を選択して、<次へ(N)> をクリックします。



- ⑩ ネットワーク管理者から指定された接続先のホスト名、または IPアドレスを入力して、<次へ(N)> をクリックします。



- ⑪ <完了> をクリックします。



7 ご参考に

7-3.PPTPパススルーで使用するパソコンの設定

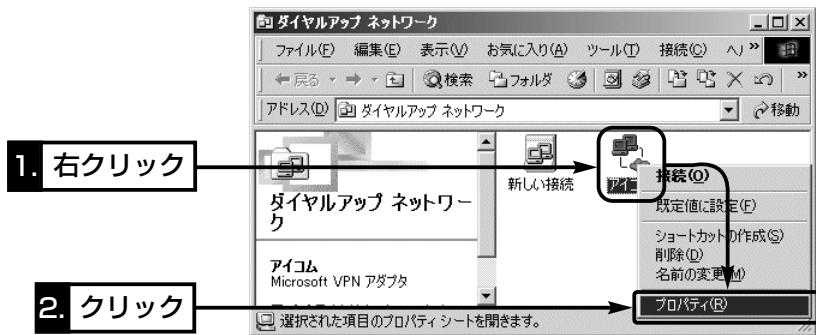
■ Windows Meをクライアントに使用する場合

〈PPTP用のパソコン設定例〉

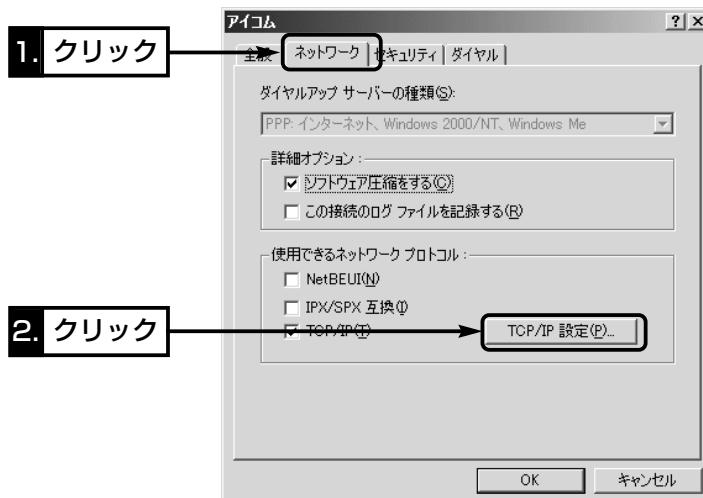
◎Windows Meの場合

〈設定の手順〉(つづき)

- ⑫新しく作成されたアイコンを右クリックして、[プロパティ(B)]をクリックします。



- ⑬[ネットワーク]タブ→〈TCP/IP 設定(P)...〉の順にクリックします。



7-3.PPTPパススルーで使用するパソコンの設定

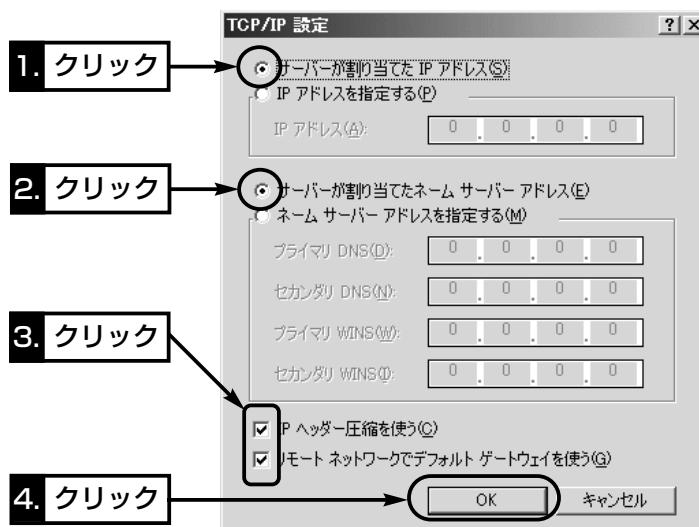
■ Windows Meをクライアントに使用する場合

<PPTP用のパソコン設定例>

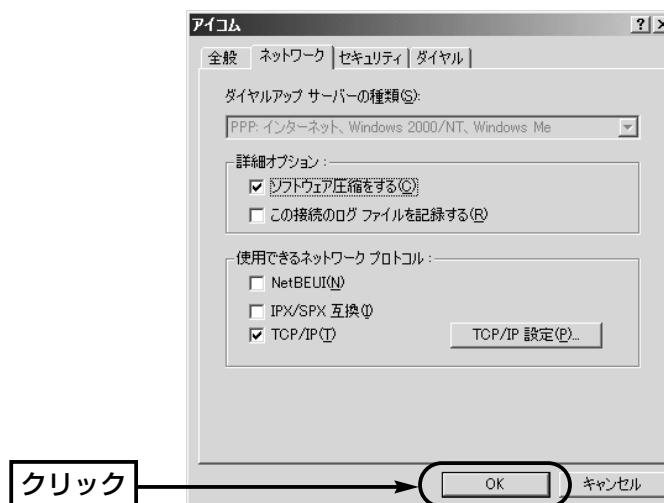
◎Windows Meの場合

<設定の手順> (つづき)

⑭ ラジオボタンとチェックボックスをクリックして、下記の画面の状態にして、<OK>をクリックします。



⑮ <OK> をクリックします。



7 ご参考に

7-3.PPTPパススルーで使用するパソコンの設定

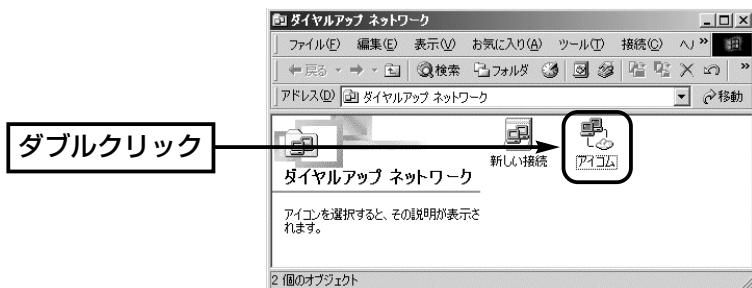
■ Windows Meをクライアントに使用する場合

〈PPTP用のパソコン設定例〉

◎Windows Meの場合(つづき)

〈接続の手順〉

- ① マウスを〈スタート〉→[設定(S)]→[ダイヤルアップネットワーク(N)]の順番に操作します。
- ② 新しく作成されたアイコンをダブルクリックします。

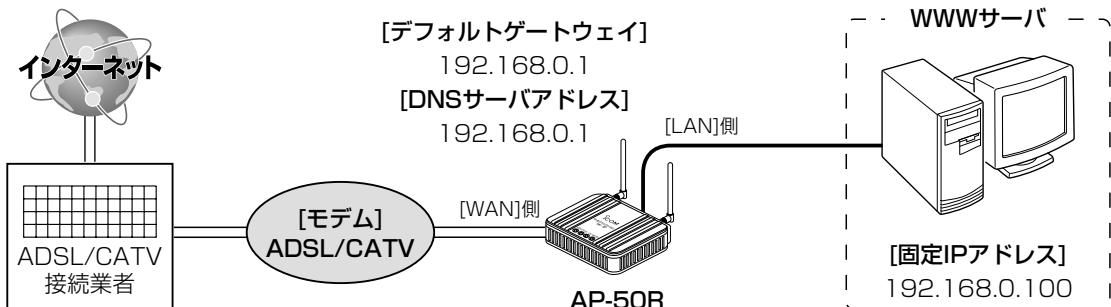


- ③ PPTPサーバに設定された[ユーザー名(U)]と[パスワード(P)]を入力して、〈接続〉をクリックします。



7-4. 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。



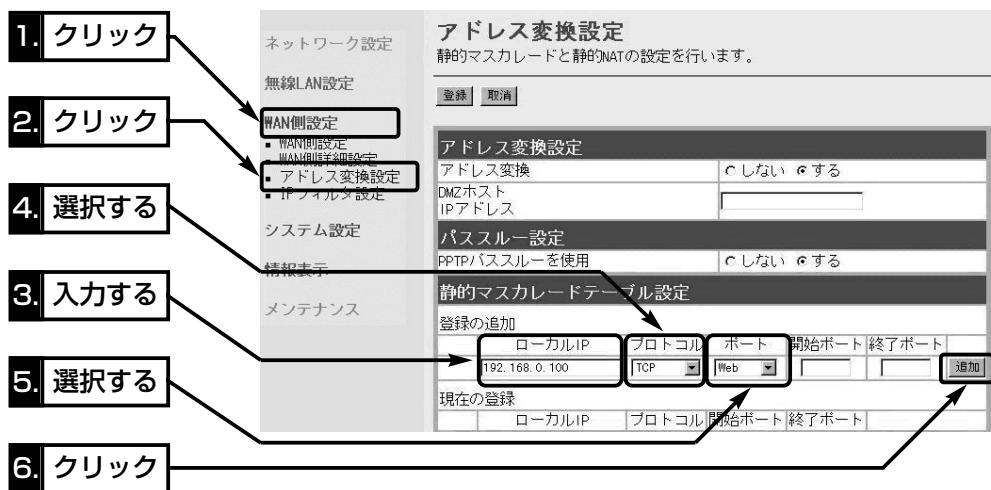
1. WWWサーバの設定

- 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。

7-4. Web公開の設定例(つづき)

2. Web公開の設定

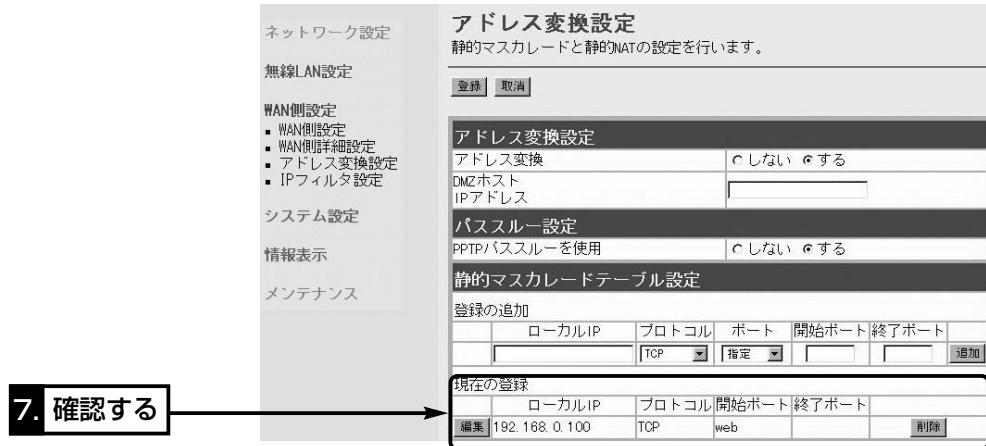
- ①本製品の設定画面にアクセスして、「WAN側設定」メニューの「アドレス変換設定」をクリックします。
 - 「アドレス変換設定」画面を表示します。
- ②パソコンの固定IPアドレス(例：192.168.0.100)を[静的マスカレード設定]項目の[登録の追加]-[ローカルIP]欄に入力します。
- ③指定するプロトコルは「TCP」で、[静的マスカレード設定]項目の[登録の追加]-[プロトコル]欄で選択します。
- ④指定するポートは「Web(80番)」で、[静的マスカレード設定]項目の[登録の追加]-[ポート]欄で選択します。
- ⑤〈追加〉をクリックします。



7-4. Web公開の設定例

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「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[フィルタ方法]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。



7 ご参考に

7-4. Web公開の設定例

2. Web公開の設定(つづき)

⑯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	番号/元ポート番号/宛先ポート番号	番号/元IPアドレス/宛先IPアドレス	ポート	IPアドレス
編集	削除	57	WAN側から(送り)	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。

アイコム株式会社

本社	547-0003	大阪市平野区加美南1-1-32	
北海道営業所	003-0806	札幌市白石区菊水6条2-2-7	TEL 011-820-3888
仙台営業所	983-0857	仙台市宮城野区東十番丁54-1	TEL 022-298-6211
東京営業所	108-0022	東京都港区海岸3-3-18	TEL 03-3455-0331
名古屋営業所	468-0066	名古屋市天白区元八事3-249	TEL 052-832-2525
大阪営業所	547-0004	大阪市平野区加美鞍作1-6-19	TEL 06-6793-0331
広島営業所	733-0842	広島市西区井口3-1-1	TEL 082-501-4321
四国営業所	760-0071	高松市藤塚町3-19-43	TEL 087-835-3723
九州営業所	815-0032	福岡市南区塙原4-5-48	TEL 092-541-0211

●サービスについてのお問い合わせは各営業所サービス係宛にお願いします。