

### WIRELESS ACCESS POINT AP-3000G

無線ホットスポット対応  
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
13ページ	無線LAN設定	2
29ページ	WAN側設定	3
45ページ	システム設定	4
57ページ	情報表示	5
61ページ	Telnetガイド	6
65ページ	PPTPパススルーの設定	7

---

# 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、Ver1.09のファームウェアを使用して説明しています。

---

## 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。
- ©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。
- ©Macintosh、Mac-OSは、米国アップルコンピューター社の登録商標です。
- ©Netscape Navigatorは、Netscape Communications Corporationの商標です。
- ©Adobe、Acrobatは、アドビシステムズ社の登録商標です。
- ©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。

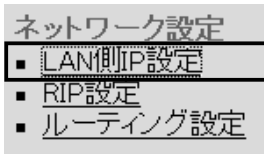
LANへの接続、RIP、スタティックルーティングの設定を行います。

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.「RIP設定」画面	9
■ RIP設定	9
■ RIPフィルタ設定	10
1-3.「ルーティング設定」画面	11
■ IP経路情報	11
■ スタティックルーティング設定	12

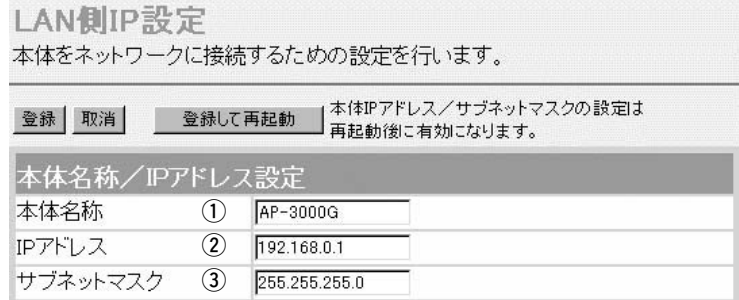
# 1 「ネットワーク設定」メニュー

## 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。



The image shows the 'LAN側IP設定' (LAN Side IP Settings) screen. At the top, it says 'LAN側IP設定' and '本体をネットワークに接続するための設定を行います。' (Perform settings for connecting the device to the network). Below this are buttons for '登録' (Register), '取消' (Cancel), and '登録して再起動' (Register and Restart). To the right of these buttons is a note: '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。' (The setting of the device IP address/subnet mask becomes effective after restart). The main section is titled '本体名称/IPアドレス設定' (Device Name/IP Address Setting) and contains three input fields: '本体名称' (Device Name) with value 'AP-3000G', 'IPアドレス' (IP Address) with value '192.168.0.1', and 'サブネットマスク' (Subnet Mask) with value '255.255.255.0'. Each field has a circled number (1, 2, 3) next to it.

〈登録〉ボタン ..... [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]欄の変更内容は、画面上で確定されるだけですので、〈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 ..... 「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が有効になります。

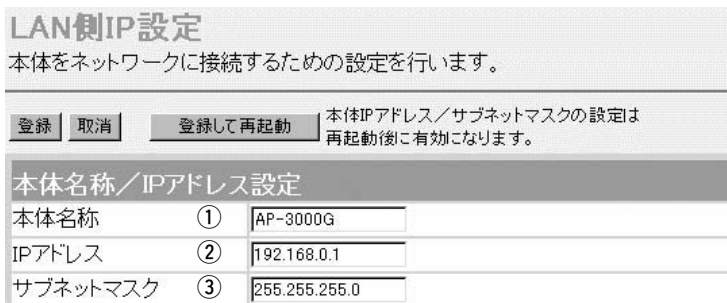
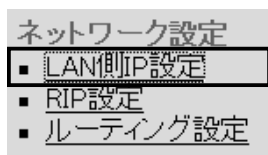
① 本体名称 ..... ネットワーク上で、本製品を識別する名前です。  
設定した名前は、本製品のLAN側に接続されたパソコンから、本製品に直接アクセスするためのドメイン名の一部として使えます。  
(出荷時の設定：AP-3000G)

**入力形式：[http://web.本体名称/]**

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。また、ほかのネットワーク機器と重複しないように、アルファベットで始まる半角英数字(A～Z、0～9、-)、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。  
※全角文字(15文字以内)も入力できますが、DNSサーバの代理応答機能は利用できなくなります。

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アドレスを入力します。

(出荷時の設定：192.168.0.1)

本製品を現在稼働中のネットワークに接続するときなど、そのネットワークに合わせた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。

※LAN側IPアドレスが「192.168.0.1」のルータタイプモデムに接続する場合は、「192.168.0.250」に変更してください。

また、「192.168.1.1」の場合は、「192.168.1.250」に変更してください。

なお、ルータタイプモデムのDHCPサーバ機能を使用する場合は、本製品の[DHCPサーバ設定]項目にある[DHCPサーバ機能を使用]欄を「しない」に変更してください。

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)

本製品を現在稼働中のネットワークに接続するときなど、そのネットワークに合わせたサブネットマスクに変更してください。

**[例]：固定IPアドレスを8個取得している場合**

(192.168.0.0～192.168.0.7)

サブネットマスクを「255.255.255.248」と設定する場合、「192.168.0.2～192.168.0.6」が同じネットワークとしてパソコンに割り当てできます。

この場合、下記のIPアドレスはパソコンに割り当てできません。

「192.168.0.0」：ネットワークアドレス

「192.168.0.1」：本製品のLAN側IPアドレス

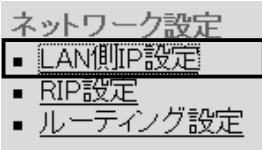
「192.168.0.7」：ブロードキャストアドレス

# 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。

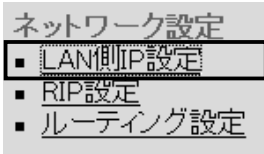


DHCPサーバ設定	
DHCPサーバ機能を使①	<input type="radio"/> しない <input checked="" type="radio"/> する
割り当て開始IPアドレス②	192.168.0.10
割り当て個数 ③	30 個
サブネットマスク ④	255.255.255.0
リース期間 ⑤	72 時間
ドメイン名 ⑥	
デフォルトゲートウェイ⑦	192.168.0.1
DNS代理応答を使用 ⑧	<input type="radio"/> しない <input checked="" type="radio"/> する
プライマリDNSサーバ ⑨	
セカンダリDNSサー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

- 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、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サーバがローカルIPアドレスを定期的に自動でパソコンに割り当てなおす期限を時間で指定します。  
設定できる範囲は、「1～9999」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、入力(半角英数字：127文字以内)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)

#### ネットワーク設定

- LAN側IP設定
- RIP設定
- ルーティング設定

DHCPサーバ設定	
DHCPサーバ機能を使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

特定のパソコンに割り当てるIPアドレスを固定するときの設定です。

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 .....

DHCPサーバ機能を使用して自動的に割り当てるIPアドレスを、特定のパソコンに固定するとき、パソコンのMACアドレスとIPアドレスの組み合わせを登録する欄です。

※入力後は、<追加>をクリックしてください。

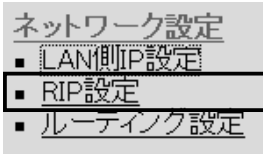
※最大16個の組み合わせまで登録できます。

登録するパソコンの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指定してください。



1-2.「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を使用します。



〈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(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(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 ……………

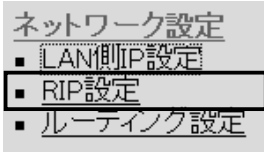
WAN側について、[RIP設定]欄で選択したRIPを「使用しない」、「受信のみ」、「受信も送信も行う」から選択します。

(出荷時の設定：使用しない)

# 1 「ネットワーク設定」メニュー

## 1-2.「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 RIP
LAN側RIP動作	② 使用しない
WAN側RIP動作	③ 使用しない
認証キー	④

#### ④ 認証キー .....

[RIP設定]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、他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]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

登録の追加

フィルタ動作	IPアドレス	サブネットマスク	
無視する	<input type="text"/>	<input type="text"/>	追加

現在の登録

フィルタ動作	IPアドレス	サブネットマスク	
--------	--------	----------	--

#### RIPフィルタ設定.....

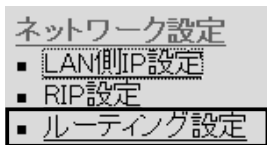
同一サブネットで使う複数のアクセスポイントやルータにおいて、特定のアクセスポイントやルータが出力するRIPパケットを受信しないように、そのパケットを出力するアクセスポイントやルータのIPアドレスとサブネットマスクを入力します。

最大16件の登録が可能です。

※入力後は、〈追加〉をクリックしてください。

### 1-3.「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、またはどの端末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。

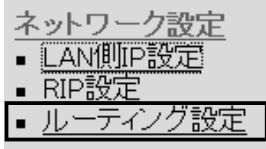
ルーティング設定					
通信経路（ルート）に関する設定を行います。					
IP経①情報	②	③	④	⑤	⑥
宛先	サブネットマスク	ゲートウェイ	経路	作成	メトリック
192.168.0.0	255.255.255.0	192.168.0.1	local	static	0
192.168.0.0	255.255.255.255	255.255.255.255	local	misc	0
192.168.0.1	255.255.255.255	192.168.0.1	local	static	0
192.168.0.255	255.255.255.255	255.255.255.255	local	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。  
 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 「ネットワーク設定」メニュー

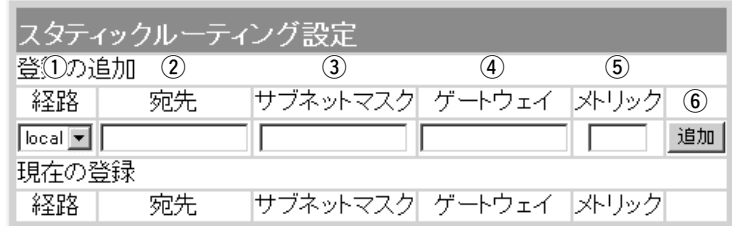
## 1-3.「ルーティング設定」画面(つづき)

### ■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。



スタティックルーティング設定					
①の追加	②	③	④	⑤	⑥
経路	宛先	サブネットマスク	ゲートウェイ	メトリック	
local	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	追加
現在の登録					
経路	宛先	サブネットマスク	ゲートウェイ	メトリック	

- 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。
- 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。  
※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。  
登録されると、その内容は[IP経路情報]項目に表示されません。

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

2-1.「セキュリティ設定」画面	14
■ RADIUS設定	14
■ 無線端末間通信設定	16
■ MACアドレスセキュリティー設定	17
2-2.「無線LAN設定」画面	18
■ BSSID	18
■ 無線LAN設定	18
2-3.「暗号化設定」画面	23
■ 暗号化設定	23
■ キー値	27

## 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

##### 無線LAN設定

##### ■ セキュリティ設定

##### ■ 無線LAN設定

##### ■ 暗号化設定

RADIUSサーバによる無線端末への認証接続についての設定を行います。

#### 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、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暗号化を行います。

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 しない する

② プライマリ セカンダリ

サーバアドレス ③

サーバのポート番号 ④

シークレットキー ⑤

再認証間隔 ⑥  分

〈登録〉ボタン ……………

[RADIUS設定]項目以外の設定内容が有効になります。  
「セキュリティ設定」画面で変更した内容を画面上で確定するボタンです。

※[MACアドレスセキュリティ設定]項目の変更内容は、画面上で確定されるだけですので、〈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。

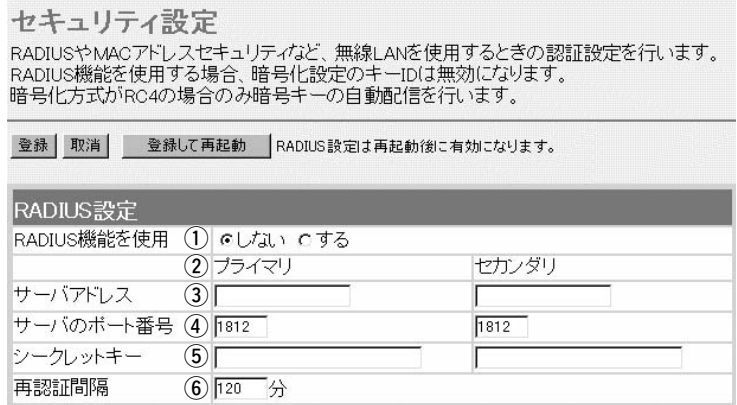
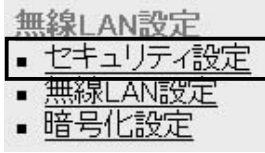
また、RADIUSサーバとの鍵交換は、「WEP RC4」を[暗号化方式]欄で設定しているとき有効で、クライアント側では、Windows XP標準のワイヤレスネットワーク接続の設定で、「キーは自動的に提供される(H)」にチェックマークが入っている状態に該当します。

「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。

2-1.「セキュリティ設定」画面

■ RADIUS設定(つづき)

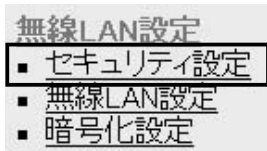


- ② プライマリ/セカンダリ …… [プライマリ]列に設定したサーバから応答がないとき、その次にアクセスさせるRADIUSサーバがあるときは、[セカンダリ]列にそのRADIUSサーバアドレスを設定します。
- ③ サーバアドレス …… 対象となるRADIUSサーバのIPアドレスを入力します。
- ④ サーバのポート番号 …… 対象となるRADIUSサーバの認証ポートを設定します。  
設定できる範囲は、「1～65535」です。(出荷時の設定：1812)  
※ご使用になるシステムによっては、出荷時の設定値と異なることがありますので確認してください。
- ⑤ シークレットキー …… この欄に設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 「無線LAN設定」メニュー

### 2-1.「セキュリティ設定」画面(つづき)

#### ■ 無線端末間通信設定



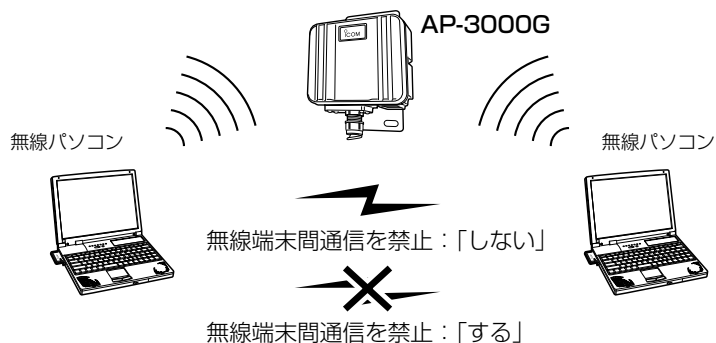
無線パソコンどうしが本製品を介して通信するのを禁止するとき設定します。



#### 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用として利用するときなどは、設定を変更すると無線端末どうしが本製品を介して通信することを禁止できます。(出荷時の設定：しない)

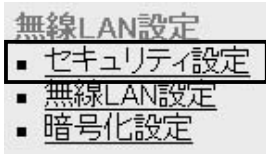
※この機能は、[IEEE802.11a/b/g]のいずれかの規格で通信するすべての無線パソコンが対象になります。



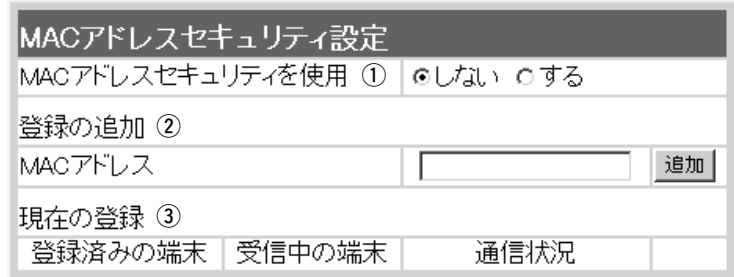


2-1.「セキュリティ設定」画面(つづき)

■ 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

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-c7-4B-00-32、0090c74B0032)

③ 現在の登録 ……………

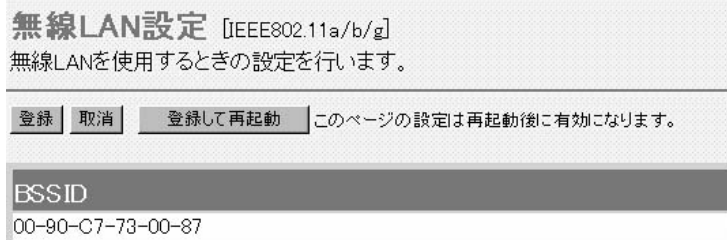
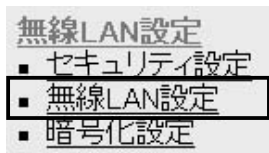
本製品と無線で通信している端末の状況や登録済みの無線端末のMACアドレスを表示します。  
登録されているMACアドレスは、〈削除〉で登録の削除が行えます。  
受信中の端末欄に表示されているMACアドレスで登録されていないものは、〈追加〉ボタンが表示されますので、それをクリックすると、その端末のMACアドレスが登録できます。

## 2 「無線LAN設定」メニュー

### 2-2.「無線LAN設定」画面 [IEEE802.11a/b/g]

#### ■ BSSID

本製品に内蔵された無線LANカードの[BSSID]を表示します。



〈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。

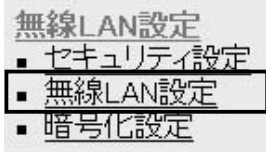
無線LAN設定		
SSID	①	LG
ANYを拒否	②	<input checked="" type="radio"/> しない <input type="radio"/> する
チャンネル	③	11 (2462MHz)
Rts/Ctsスレッシュホールド	④	無し
11g保護機能	⑤	無効
パワーレベル	⑥	高
接続端末制限	⑦	255

① SSID…………… 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。

2-2.「無線LAN設定」画面[IEEE802.11a/b/g]

■ 無線LAN設定(つづき)



無線LAN設定		
SSID	①	LG
ANYを拒否	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	無効
パワーレベル	⑥	高
接続端末制限	⑦	255

② ANYを拒否 ……………

※設定を「する」に変更すると、Windows XP標準のワイヤレスネットワーク接続には表示されません。

SSIDを「ANY」、または「any」と設定している無線端末を、本製品と同じSSIDが設定された無線ネットワークグループとして認識させるかさせないかを設定します。

同じ無線ネットワークグループの一員として識別させたいときは、「しない」を選択します。(出荷時の設定：しない)

③ チャンネル ……………

本製品が11Mbps(2.4GHz)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)

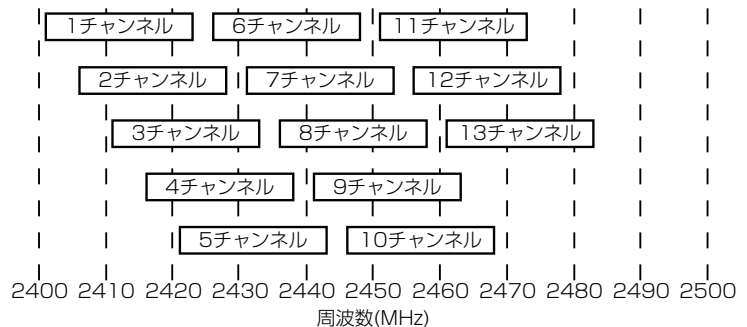
※無線端末側は、本製品のチャンネルを自動的に検知して通信します。

※近くに2.4GHz(11Mbps)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。

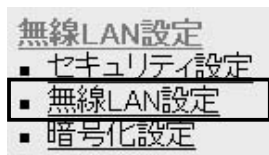
※5.2GHz帯(IEEE802.11a)で通信する場合は、お互いを異なるチャンネルに設定すれば、チャンネル間の電波干渉に配慮する必要はありません。



## 2 「無線LAN設定」メニュー

### 2-2. 「無線LAN設定」画面 [IEEE802.11a/b/g]

#### ■ 無線LAN設定(つづき)



無線LAN設定		
SSID	①	LG
ANYを拒否	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	無効
パワーレベル	⑥	高
接続端末制限	⑦	255

#### ④ Rts/Ctsスレッシュ

ホールド ……………

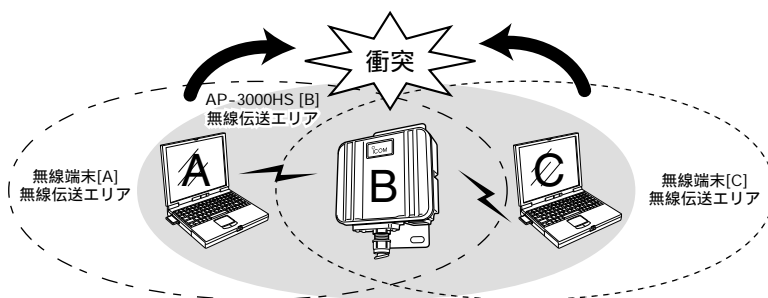
ネゴシエーションするために送るパケットのデータサイズを、「500バイト」または「1000バイト」から選択します。

(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。

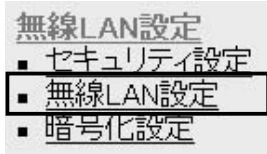
隠れ端末とは、下図のように、それぞれが本製品[B]と無線通信できても、互いが直接通信できない無線端末[A]-[C]同士([A]に対して[C]、[C]に対して[A])のことを呼びます。

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。



2-2.「無線LAN設定」画面[IEEE802.11a/b/g]

■ 無線LAN設定(つづき)



無線LAN設定		
SSID	①	LG
ANYを拒否	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	無効
パワーレベル	⑥	高
接続端末制限	⑦	255

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：無効)

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

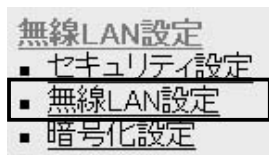
◎通信エリアを制限してセキュリティーを高めたいとき

◎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 「無線LAN設定」メニュー

### 2-2. 「無線LAN設定」画面 [IEEE802.11a/b/g]

#### ■ 無線LAN設定(つづき)



無線LAN設定		
SSID	①	LG
ANYを拒否	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	無効
パワーレベル	⑥	高
接続端末制限	⑦	255

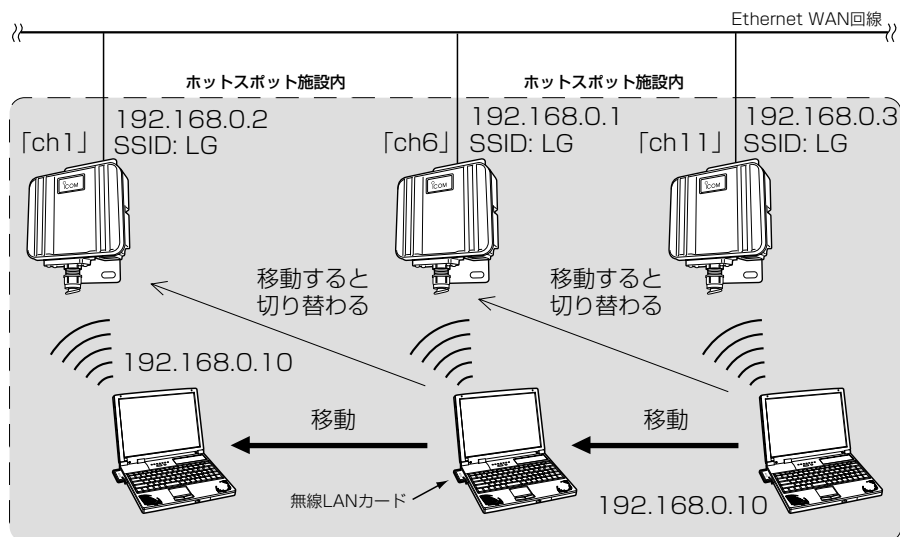
- ⑦ 接続端末制限 …………… 本製品に同時接続可能な無線パソコンの台数を設定します。設定できる範囲は、「1～255」です。(出荷時の設定：255) 接続制限を設定すると、本製品1台だけに接続が集中するのを防止(本製品の負荷を分散)できますので、接続集中による通信速度低下を防止できます。

#### 【ローミング機能について】

本製品を2台以上用意して、無線伝送エリアが重なるように複数設置することで、無線ホットスポットで通信できるエリアを拡大できます。

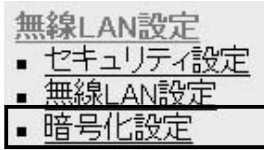
ホットスポットでアクセスしてくる無線端末は、移動しながら複数のホットスポットエリアにまたがった通信が可能になります。

※本製品どうしをEthernetで接続するときは、HUBを介して接続してください。

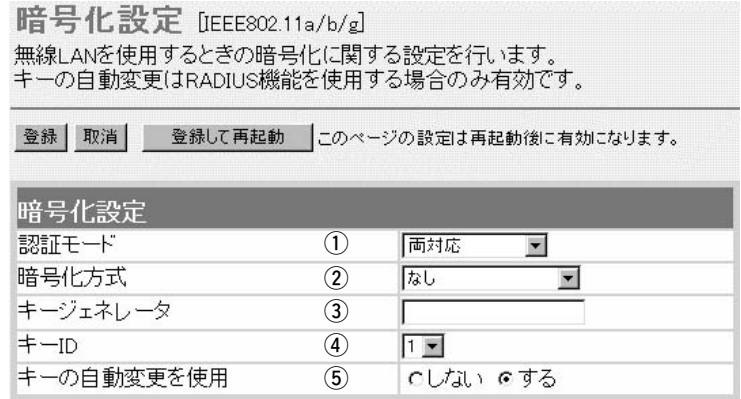


2-3.「暗号化設定」画面[IEEE802.11a/b/g]

■ 暗号化設定



無線LANで通信するデータを保護するために、WEP機能で暗号化するための設定です。



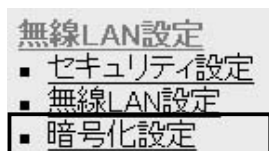
- 〈登録〉ボタン …………… [WEP設定]画面で変更したすべての設定内容が有効になります。
- 〈取消〉ボタン …………… [WEP設定]画面の設定内容を変更したとき、変更前の状態に戻すボタンです。  
なお〈登録〉をクリックすると、変更前の状態には戻りません。
- 〈登録して再起動〉ボタン …… 本製品を再起動して、「暗号化設定」画面で変更したすべての設定内容が有効になります。
- ① 認証モード …………… 暗号化を使用する無線LANからのアクセスに対する認証方式を設定します。 (出荷時の設定：両対応)  
※通信相手と認証モードが異なると通信できません。

  - ◎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

### 2-3.「暗号化設定」画面[IEEE802.11a/b/g]

#### ■ 暗号化設定(つづき)



**暗号化設定** [IEEE802.11a/b/g]

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		
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"/>
キーID	④	1 ▼
キーの自動変更を使用	⑤	<input type="radio"/> しない <input type="radio"/> する

#### ② 暗号化方式 .....

※「WEP RC4」、「OCB AES」は、それぞれ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)  
対応する暗号化方式は、「WEP RC4」、「OCB AES」です。  
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。

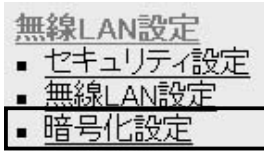
※暗号化鍵(キー)の長さは、64(40)/128(104)/152(128)ビットの中から選択できません。

◎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。



2-3.「暗号化設定」画面[IEEE802.11a/b/g]

■ 暗号化設定(つづき)



**暗号化設定** [IEEE802.11a/b/g]

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		
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	
キーID	④	1
キーの自動変更を使用	⑤	<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「\*」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。

(取扱説明書[導入編] 4-4章 「■ 暗号化鍵(キー)の入力と設定例について」を参照)

※「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。

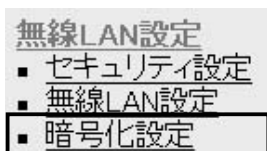
※通信相手間で文字列が異なる場合、暗号化されたデータを復号できません。

※「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

### 2-3.「暗号化設定」画面[IEEE802.11a/b/g]

#### ■ 暗号化設定(つづき)



**暗号化設定** [IEEE802.11a/b/g]  
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。

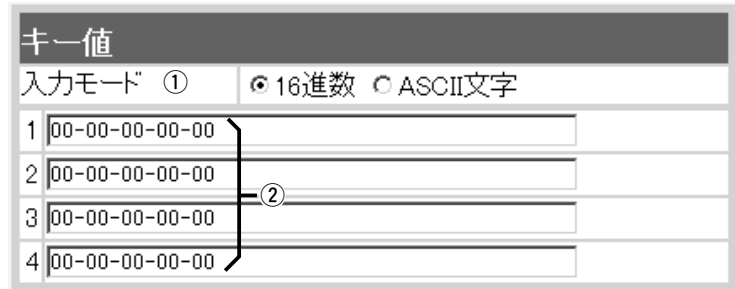
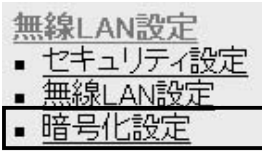
暗号化設定		
認証モード	①	両対応 ▼
暗号化方式	②	なし ▼
キージェネレータ	③	
キーID	④	1 ▼
キーの自動変更を使用	⑤	<input type="radio"/> しない <input checked="" type="radio"/> する

- ④ 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)  
設定できる範囲は、「1～4」です。  
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。
- ⑤ キーID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やXPを使って本製品にIEEE802.11x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。  
※弊社製無線LANカードに付属の設定ユーティリティは、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WindowsXP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。

2-3.「暗号化設定」画面[IEEE802.11a/b/g]

■ 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、暗号化および復号化に使用する鍵(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ID値(1~4)に対して同じ内容に設定しないと通信できません。

※このページには、何も記載していません。

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	30
■ 接続状況	30
■ 回線種別	31
■ 回線設定PPPoE/DHCP	32
■ 接続設定(※PPPoE設定時)	32
3-2.「WAN側詳細設定」画面	33
■ 共通詳細設定	33
■ PPPoE詳細設定	35
3-3.「アドレス変換設定」画面	37
■ アドレス変換設定	37
■ 静的マスカレードテーブル設定	38
■ 静的NATテーブル設定	38
3-4.「IPフィルタ設定」画面	39
■ IPフィルタ設定	39
■ 現在の登録	43

### 3 「WAN側設定」メニュー

#### 3-1. 「WAN側設定」画面

##### ■ 接続状況

###### 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

登録された回線への接続状況を表示します。

###### WAN側設定

インターネット接続に関する設定を行います。  
回線接続中は設定できません。

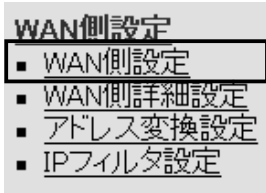
本体の時刻 : 2002年 01月 01日 00時 05分

接続状況		
未接続	①	<input type="button" value="接続"/> <input type="button" value="切断"/>
回線種別	②	LAN
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	- 時間 - 分 - 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、「PPPoE」または「DHCP」を選んで〈登録して再起動〉をクリックしたときは、〈接続〉/〈切断〉ボタンを表示します。  
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、「LAN」/「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…………… 「PPPoE」または「DHCP」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…………… 「PPPoE」または「DHCP」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 相手側のIPアドレス…………… 「PPPoE」または「DHCP」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、WWWブラウザの〈更新〉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。



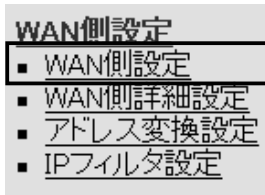
- 〈登録〉ボタン …………… [回線種別]項目以外の設定内容が有効になります。  
 ※[回線種別]項目を変更した場合は、画面上で確定されますが、  
 〈登録して再起動〉をクリックするまで有効になりません。
- 〈取消〉ボタン …………… 「WAN側設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。  
 なお 〈登録〉をクリックすると、変更前の状態には戻りません。
- 〈登録して再起動〉ボタン …… 本製品を再起動して、「WAN側設定」画面で変更したすべての設定内容が有効になります。
- 回線種別 …………… ご契約のプロバイダーや接続業者から指定された回線種別を選択します。  
 ◎LAN(出荷時の設定)  
 有線と無線で接続されたパソコンが本製品を介してLANで通信するとき使用します。  
 ◎PPPoE  
 本製品をWAN側の回線に接続するとき使用します。  
 WAN側のIPアドレスを、「PPPoE」で取得します。  
 ◎DHCP  
 本製品をWAN側の回線に接続するとき使用します。  
 WAN側のIPアドレスを、「DHCP」クライアントで取得します。  
 ※設定を有効にするためには、〈登録して再起動〉をクリックしてください。

### 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	
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。	
接続設定	
ユーザID ⑦	<input type="text"/>
パスワード ⑧	<input type="text"/>

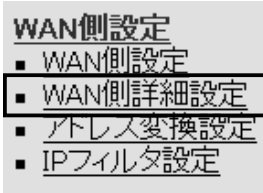
※「PPPoE」設定時の画面を例に説明しています。  
「DHCP」設定時は、[接続設定]項目は表示されません。

- 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。
- **接続設定**(※PPPoE設定時)
- 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。

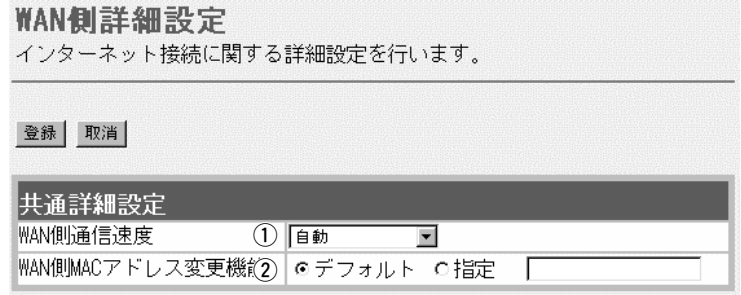


### 3-2.「WAN側詳細設定」画面

#### ■ 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。



※「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。

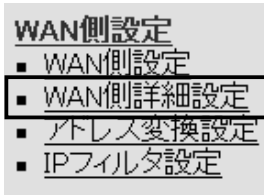
〈取消〉ボタン ..... 「WAN側詳細設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。  
 なお 〈登録〉をクリックすると、変更前の状態には戻りません。

- 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[Ethernet]ポートに接続す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。
    - [100Mbps(Half Duplex)]に対応する機器を本製品の[Ethernet]ポートに接続するときの設定です。
  - ◎100(Full Duplex)：
    - [100Mbps/Full Duplex]固定で通信します。
    - [100Mbps(Full Duplex)]に対応する機器を本製品の[Ethernet]ポートに接続するときの設定です。
  - ◎10(Half Duplex)：
    - [10Mbps(Half Duplex)]固定で通信します。
    - [10Mbps/Half Duplex]に対応する機器を本製品の[Ethernet]ポートに接続するときの設定です。
  - ◎10(Full Duplex)：
    - [10Mbps(Full Duplex)]固定で通信します。
    - [10Mbps/Full Duplex]に対応する機器を本製品の[Ethernet]ポートに接続するときの設定です。

## 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(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。

**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"/>

※「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 ……………

インターネットを、すでにMACアドレス登録が必要なプロバイダーでご使用の場合、登録された機器のMACアドレスで対応できません。(出荷時の設定：デフォルト)  
登録している機器の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

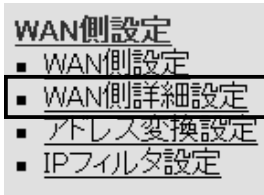
この機能をご利用になるときは、登録されているMACアドレスをよく確認していただき、設定値を間違えないように注意してください。

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。

3-2.「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	<input type="text"/>
サービスネー⑤	<input type="text"/>

※回線種別を「DHCP」に設定したときは、表示されません。

① 接続設定 ……………

回線への接続方法を選択します。 (出荷時の設定：自動)

- ◎手動：[接続状況]項目の〈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 自動切断タイマ ……………

[接続設定]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分で入力します。 (出荷時の設定：10)  
設定できる範囲は、「0(自動切断しない)~65535」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おりますが、現行のインターネットルータには、オーバーサイズの packets 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。

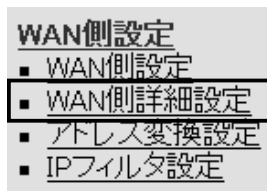
△警告

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。

### 3 「WAN側設定」メニュー

#### 3-2. 「WAN側詳細設定」画面

##### ■ PPPoE詳細設定(つづき)



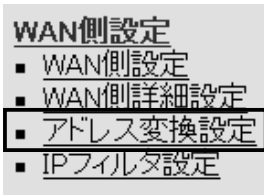
PPPoE詳細設定	
接続設定 ①	<input type="radio"/> 手動 <input checked="" type="radio"/> 自動 <input type="radio"/> 常時
自動切断タイ②	10 分 *自動接続時のみ有効です。0に設定するとOFFになります。
MSS制限値 ③	1322
ACネーム ④	<input type="text"/>
サービスネー⑤	<input type="text"/>

※回線種別を「DHCP」に設定したときは、表示されません。

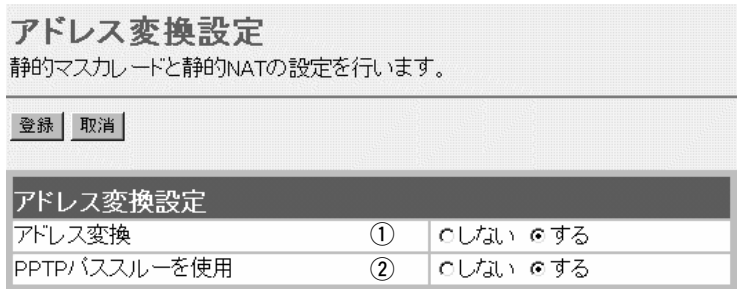
- ④ ACネーム…………… プロバイダーから指定されている場合に限り、指定のアクセスコンセントレーター名を入力します。
- ⑤ サービスネーム …… プロバイダーから指定されている場合に限り、指定のサービスネームを入力します。

### 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 PPTPパススルーを使用 ... 自宅のパソコンなどから、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。  
※使用例については、第7章(本書)を参考にパソコンを設定してください。  
(出荷時の設定：する)  
PPTPクライアントからのパケットをWAN側に転送「する」か「しない」かの設定です。

## 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

##### 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"/>	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。

#### ■ 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"/>	追加
現在の登録			
グローバルIP	-	ローカルIP	

プロバイダーおよび接続業者との契約で、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。

### 3-4.「IPフィルタ設定」画面

#### ■ IPフィルタ設定

- 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

特定条件を満たす内部または外部からのパケットを透過させたり、遮断させるフィルタの設定です。

#### IPフィルタ設定

IPフィルタの設定を行います。

IPフィルタ設定		追加 ①
番号	②	<input type="text"/>
フィルタ方向	③	<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	④	<input checked="" type="radio"/> 遮断 <input type="radio"/> 透過
プロトコル	⑤	TCP <input type="text"/> 指定時 <input type="text"/>
発信元ポート番号	⑥	すべて <input type="text"/> 指定時: <input type="text"/> ~ <input type="text"/>
宛先ポート番号	⑦	すべて <input type="text"/> 指定時: <input type="text"/> ~ <input type="text"/>
発信元IPアドレス	⑧	<input type="text"/> ~ <input type="text"/>
宛先IPアドレス	⑨	<input type="text"/> ~ <input type="text"/>

① <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として追加するボタンです。

追加されると、[IPフィルタ設定]項目の下にある登録リストに、その内容を表示します。

※フィルタ条件は、1つ以上指定してください。

② 番号 .....

最大64件のフィルタを登録できます。

入力できる範囲は、「1～64」です。

フィルタを登録すると、本製品が受信または送信するパケットごとに、登録リストに表示されたフィルタと比較します。

[番号]欄では、フィルタを比較する順位を指定します。

フィルタ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。

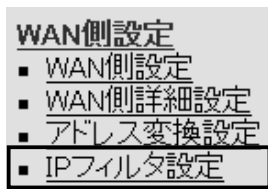
フィルタの条件に一致した時点で、それ以降の識別番号のフィルタは比較しません。

※57～64は、出荷時から設定されています。

### 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

IPフィルタの設定を行います。

IPフィルタ設定		追加 ①
番号	②	<input type="text"/>
フィルタ方向	③	<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	④	<input checked="" type="radio"/> 遮断 <input type="radio"/> 透過
プロトコル	⑤	TCP 指定時 <input type="text"/>
発信元ポート番号	⑥	すべて 指定時: <input type="text"/> ~ <input type="text"/>
宛先ポート番号	⑦	すべて 指定時: <input type="text"/> ~ <input type="text"/>
発信元IPアドレス	⑧	<input type="text"/> ~ <input type="text"/>
宛先IPアドレス	⑨	<input type="text"/> ~ <input type="text"/>

#### ③ フィルタ方向 ……………

パケットの通信方向で、WAN側またはLAN側から本製品に対して、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。

#### ④ フィルタ方法 ……………

フィルタリングの方法は、以下の2通りから選択します。

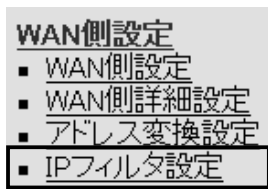
◎遮断：フィルタリングの条件に一致した場合、そのパケットをすべて破棄します。

◎透過：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。



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

IPフィルタの設定を行います。

IPフィルタ設定		追加 ①
番号	②	<input type="text"/>
フィルタ方向	③	<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	④	<input checked="" type="radio"/> 遮断 <input type="radio"/> 透過
プロトコル	⑤	TCP <input type="text"/> 指定時 <input type="text"/>
発信元ポート番号	⑥	すべて <input type="text"/> 指定時: <input type="text"/> ~ <input type="text"/>
宛先ポート番号	⑦	すべて <input type="text"/> 指定時: <input type="text"/> ~ <input type="text"/>
発信元IPアドレス	⑧	<input type="text"/> ~ <input type="text"/>
宛先IPアドレス	⑨	<input type="text"/> ~ <input type="text"/>

⑤ 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。

- ◎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。
- ◎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。

⑥ 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。

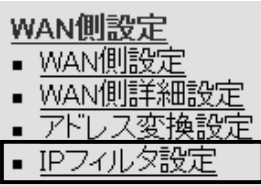
設定できる範囲は、10進数で「1~65535」までの半角数字です。また、特定のポートだけを指定するときは、始点だけ、または始点/終点に同一の番号を入力してください。

数字で指定しない場合は、「すべて」、またはニーモニック(DNS、Finger、FTP、Gopher、NEWS、POP3、SMTP、Telnet、Web、Whois)から選択します。

### 3 「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

IPフィルタの設定を行います。

IPフィルタ設定		追加 ①
番号	②	<input type="text"/>
フィルタ方向	③	<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	④	<input checked="" type="radio"/> 遮断 <input type="radio"/> 透過
プロトコル	⑤	TCP <input type="text"/> 指定時 <input type="text"/>
発信元ポート番号	⑥	すべて <input type="text"/> 指定時: <input type="text"/> ~ <input type="text"/>
宛先ポート番号	⑦	すべて <input type="text"/> 指定時: <input type="text"/> ~ <input type="text"/>
発信元IPアドレス	⑧	<input type="text"/> ~ <input type="text"/>
宛先IPアドレス	⑨	<input type="text"/> ~ <input type="text"/>

#### ⑦ 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。

設定できる範囲は、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、「すべて」、またはニーモニック(DNS、Finger、FTP、Gopher、NEWS、POP3、SMTP、Telnet、Web、Whois)から選択します。

#### ⑧ 発信元IPアドレス ……………

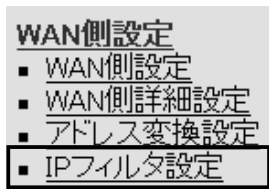
発信元ホストのIPアドレスを設定することにより、特定のホストからのパケットをフィルタリングします。

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。

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

IPフィルタの設定を行います。

IPフィルタ設定		追加 ①
番号	②	<input type="text"/>
フィルタ方向	③	<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	④	<input checked="" type="radio"/> 遮断 <input type="radio"/> 透過
プロトコル	⑤	TCP <input type="text"/> 指定時 <input type="text"/>
発信元ポート番号	⑥	すべて <input type="text"/> 指定時: <input type="text"/> ~ <input type="text"/>
宛先ポート番号	⑦	すべて <input type="text"/> 指定時: <input type="text"/> ~ <input type="text"/>
発信元IPアドレス	⑧	<input type="text"/> ~ <input type="text"/>
宛先IPアドレス	⑨	<input type="text"/> ~ <input type="text"/>

⑨ 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。

■ 現在の登録

現在登録されているIPフィルターを表示します。

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
<input type="button" value="編集"/>	<input type="button" value="削除"/>	57	WAN側から	透過	TCP	20	*	*	*
<input type="button" value="編集"/>	<input type="button" value="削除"/>	58	WAN側から	遮断	TCP_EST	*	*	*	*
<input type="button" value="編集"/>	<input type="button" value="削除"/>	59	両方	遮断	ALL	135	*	*	*
<input type="button" value="編集"/>	<input type="button" value="削除"/>	60	両方	遮断	ALL	*	135	*	*
<input type="button" value="編集"/>	<input type="button" value="削除"/>	61	両方	遮断	ALL	445	*	*	*
<input type="button" value="編集"/>	<input type="button" value="削除"/>	62	両方	遮断	ALL	*	445	*	*
<input type="button" value="編集"/>	<input type="button" value="削除"/>	63	両方	遮断	TCP	*	137 - 139	*	*
<input type="button" value="編集"/>	<input type="button" value="削除"/>	64	両方	遮断	UDP	137 - 139	137 - 139	*	*

【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側からの不正アクセス防止
- ◎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〉をクリックすると、その右の欄に表示されたIPフィルターが削除されます。

※このページには、何も記載していません。

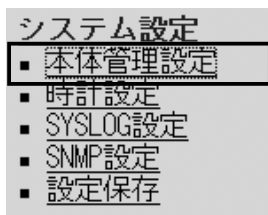
管理者以外への接続制限、本体時計、SYSLOG、SNMP、設定内容の保存、設定初期化の設定を行います。

4-1.「本体管理設定」画面	46
■ 管理者ID設定	46
■ 管理者IPアドレス	47
■ 設定初期化	47
■ 「Firm Utility使用」モード	48
4-2.「時計設定」画面	49
■ 内部時計設定	49
■ 自動時計設定	50
■ 接続制限設定	51
4-3.「SYSLOG設定」画面	52
■ SYSLOG設定	52
4-4.「SNMP設定」画面	53
■ SNMP設定	53
4-5.「設定保存」画面	54
■ 設定の保存と書き込み	54
■ 現在の設定	55

## 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



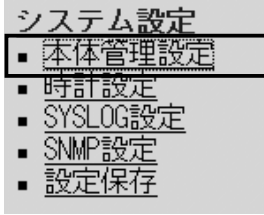
本製品の設定画面へのアクセス制限を設定します。

A screenshot of the '本体管理設定' (Main Management Settings) page. The page title is '本体管理設定' and the subtitle is '管理者IDなどの設定を行います。' (Perform settings for administrator ID, etc.). There are two buttons: '登録' (Register) and '取消' (Cancel). Below the buttons is a form titled '管理者ID設定' (Administrator ID Settings) with three input fields: '管理者ID' (Administrator ID) with a circled 1, '管理者パスワード' (Administrator Password) with a circled 2, and 'パスワードの確認入力' (Password Confirmation Input) with a circled 3.

- 〈登録〉ボタン …………… 「本体管理設定」画面で変更したすべての設定内容が有効になりません。
- 〈取消〉ボタン …………… 「本体管理設定」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 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：AP3000G)  
[管理者ID]を設定すると、次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、管理者が本製品のLAN側から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、次回のアクセスからIPアドレスが登録されたパソコン以外は、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、本製品のLAN側のすべてのパソコンから設定画面にアクセスできます。

※本製品のWANからのアクセスについては、出荷時に登録しているIPフィルターで遮断します。

## ■ 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	
<input type="checkbox"/> 初期化する	<input type="button" value="実行"/>

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。

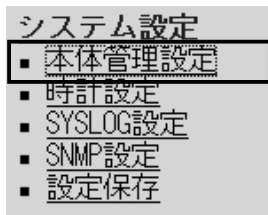
- 次の画面を表示後、出荷時の状態になります。

再起動しています。しばらくお待ちください。

## 4 「システム設定」メニュー

### 4-1. 「本体管理設定」画面(つづき)

#### ■ 「Firm Utility使用」モード

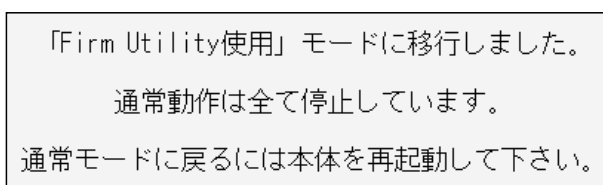


本製品に付属の「Firm Utility」を使用して、本製品を出荷時の状態に戻したり、ファームウェアをバージョンアップするとき使用します。



「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。

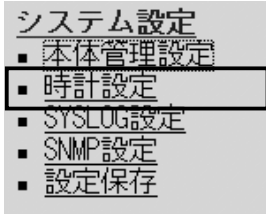
※「Firm Utility使用」モードに移行後も、本製品に設定された内容で動作しますが、「LAN」以外の回線種別が設定されているときは、無線LANでしか本製品と通信できません。

※「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。

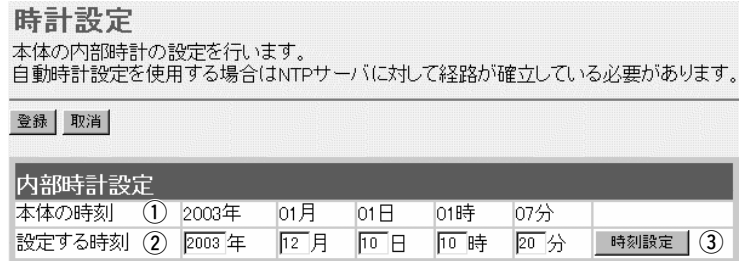


4-2.「時計設定」画面

■ 内部時計設定



本製品の内部時計を設定します。

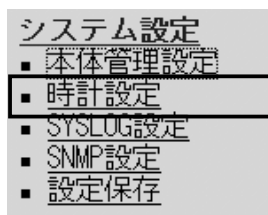


- 〈登録〉ボタン …………… [内部時計設定]以外の「時計」画面にある項目で変更したすべての設定内容が有効になります。
- 〈取消〉ボタン …………… 「時計設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。  
 なお〈登録〉をクリックすると、変更前の状態には戻りません。
- ① 本体の時刻 …………… 本製品に設定されている時刻を表示します。
- ② 設定する時刻 …………… 本製品の設定画面にアクセスしたときの時刻を、最初に表示します。  
 ※〈取消〉ボタンをクリックすると、空白になります。  
 WWWブラウザの〈更新〉ボタンをクリックすると、パソコンの時計設定を取得して表示します。
- ③ 時刻設定 …………… [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 「システム設定」メニュー

### 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

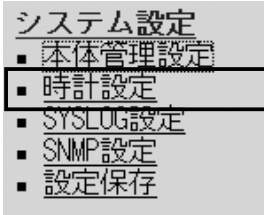
※本製品の回線種別を「LAN」で使用する場合は、NTPサーバへの問い合わせ先(経路)を「ルーティング設定」画面で設定することで自動時計設定機能が使用できます。

ルーティングテーブルを設定しないときは、問い合わせできません。

- 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 …… 最初にアクセスさせたいタイムサーバの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させる間隔を日で設定します。  
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。  
「PPPoE」による手動接続では、前回アクセスした日から設定した日数が経過している場合は、接続時にアクセスします。  
常時接続では、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。

## 4-2.「時計設定」画面(つづき)

## ■ 接続制限設定



本製品にLANで接続するパソコンからのアクセスを制限します。

接続制限設定		有効曜日						
		日	月	火	水	木	金	土
制限時間								
00 : 00 ~ 00 : 00		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 : 00 ~ 00 : 00		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 : 00 ~ 00 : 00		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

時間の入力は、24時制で行います。

指定する曜日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ます。

入力後は、〈登録〉をクリックします。

停電などに備えて、自動時計設定機能を併せてご使用になることをお勧めします。

※曜日を指定しないときは、機能しません。

※1つの登録で2日間にわたるような登録はできません。

※「本体管理設定」画面で、管理者IPアドレスにLAN側のIPアドレスを登録しているパソコンからは、この設定に関係なくいつでもアクセスできます。

## △警告

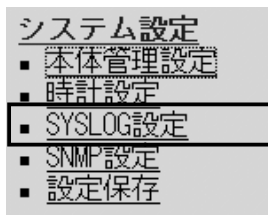
接続制限設定の前に、管理者IPアドレスを設定しておくことをお勧めします。

管理者IPアドレス(4-1章)が設定されていない状態で、接続制限設定を使用すると、その制限時間帯は、本製品にLANで接続するすべてのパソコンと通信できなくなります。

## 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

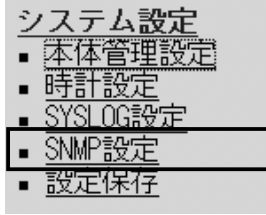
#### SYSLOG設定

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"/>

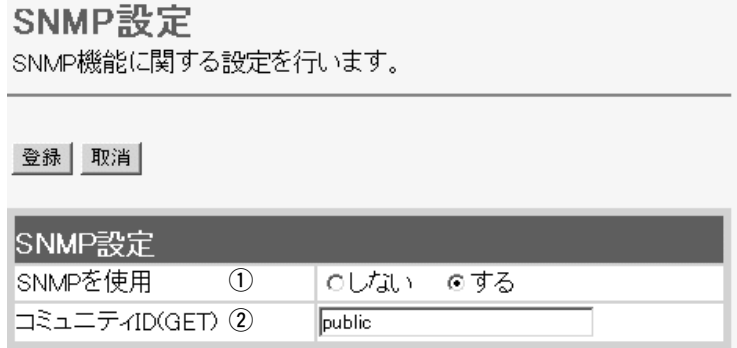
- 〈登録〉ボタン ..... 「SYSLOG設定」画面で変更したすべての設定内容が有効になります。
- 〈取消〉ボタン ..... 「SYSLOG設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。  
なお〈登録〉をクリックすると、変更前の状態には戻りません。
- ① DEBUGを使用 ..... 各種デバッグ情報をSYSLOGに出力「する」か「しない」かを選択します。  
(出荷時の設定：しない)
- ② INFOを使用 ..... INFOタイプのメッセージをSYSLOGに出力「する」か「しない」かを選択します。  
(出荷時の設定：しない)
- ③ NOTICEを使用 ..... 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



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。

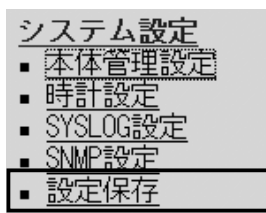


- 〈登録〉ボタン …………… 「SNMP設定」画面で変更したすべての設定内容が有効になります。
- 〈取消〉ボタン …………… 「SNMP設定」画面の設定内容を変更したとき、変更前の状態に戻すボタンです。  
なお〈登録〉をクリックすると、変更前の状態には戻りません。
- ① SNMPを使用 …………… SNMP機能を使用「する」か「しない」かを選択します。  
(出荷時の設定：する)
- ② コミュニティID(GET) …… 本製品から設定情報をSNMP管理ツール側で読み出すことを許可するIDを設定します。  
(出荷時の設定：public)  
入力は、半角31文字以内の英数字で入力します。

## 4 「システム設定」メニュー

### 4-5.「設定保存」画面

#### ■ 設定の保存と書き込み



#### ① 保存したファイルを書き込む ……………

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



[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。

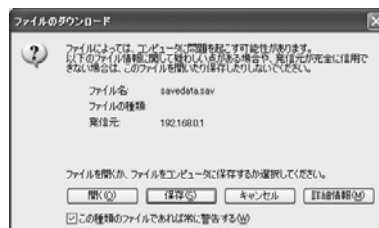
#### ② ファイルに保存する ……………

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。

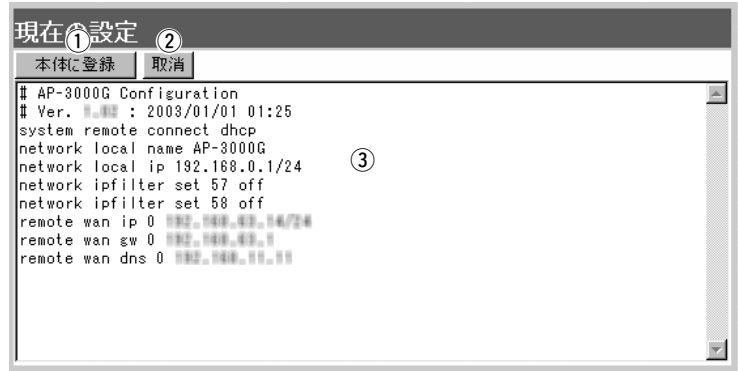
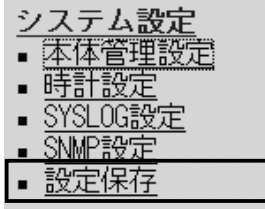
保存したファイルは、[保存したファイルを書き込む](①)欄の操作で、本製品自身や本製品を使用する別の相手に書き込みできます。



4-5.「設定保存」画面(つづき)

■ 現在の設定

本製品の設定変更内容を確認したり、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」(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(☞P50)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、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。  
 この画面内容をパソコンに保存するときは、[設定の保存と書き込み]項目(☞P50)を使用してください。  
 ※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せん。  
 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。

※このページには、何も記載していません。



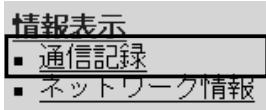
WAN側回線の通信記録、本製品のMACアドレス表示、ネットワークインターフェイスリストを表示します。

5-1.「通信記録」画面 .....	58
■ 通信記録 .....	58
5-2.「ネットワーク情報」画面 .....	59
■ ネットワーク インターフェイス リスト .....	59
■ ブリッジポート情報 .....	59
■ 本体MACアドレス .....	59

## 5 「情報表示」メニュー

### 5-1.「通信記録」画面

#### ■ 通信記録



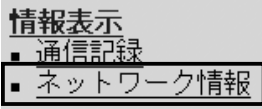
WAN側回線の通信記録を表示します。



通信記録の履歴は、〈クリア〉をクリックすると消去できます。

## 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	192.168.63.14	255.255.255.0

※回線種別が「PPPoE」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。

### ■ ブリッジポート情報

本製品の使用ポートについて、ブリッジ通信の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	
	状況	通信中
Ethernet ①	送信パケット数	113
	受信パケット数	224
	状況	通信中
Wireless ②	送信パケット数	92
	受信パケット数	0

※回線種別の設定により表示される内容が異なります。

#### ① Ethernet.....

有線LAN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LAN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。

#### 本体MACアドレス

00-90-C7-FF-FF-FF

※このページには、何も記載していません。

Telnetによる接続方法とオンラインヘルプの見かたについて説明します。

6-1. Telnetによる接続 .....	62
■ Windows 98/98 SE/Meの場合 .....	62
■ Windows 2000/Windows XPの場合 .....	62
6-2. オンラインヘルプ .....	63

## 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。  
設定したユーザ名とパスワードを入力してログインしてください。  
※初期値では[User]、[Password]ともに設定されていません。  
何も入力せずに[Enter]キーを押してください。
- ⑥ ログインメッセージ(Welcome to AP-3000G!)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。  
設定したユーザ名とパスワードを入力してログインしてください。  
※初期値では[User]、[Password]ともに設定されていません。  
何も入力せずに[Enter]キーを押してください。
- ⑤ ログインメッセージ(Welcome to AP-3000G!)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数文字入力し[Tab]キーを押すと、コマンド名が補完されます。入力した文字に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

※このページには、何も記載していません。

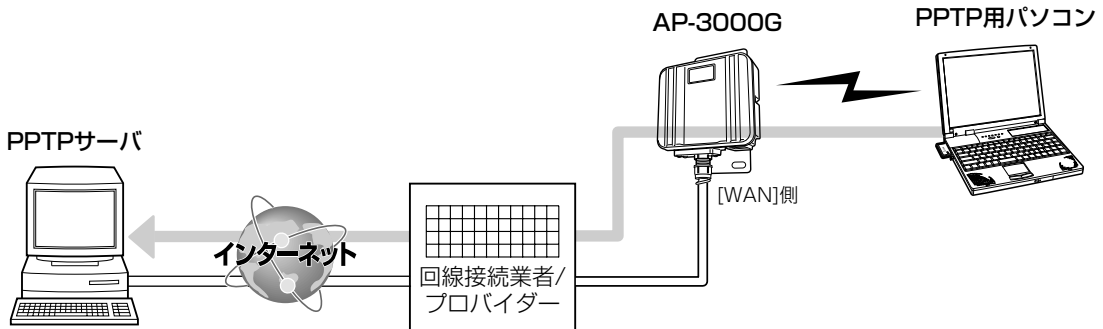


PPTPパススルーで使用するパソコンの設定について説明します。

7-1.Windows XPをクライアントに使用する場合 .....	66
7-2.Windows 2000をクライアントに使用する場合 .....	71
7-3.Windows Meをクライアントに使用する場合 .....	75

## 7 PPTPパススルーの設定

### 7-1.Windows XPをクライアントにする場合



#### 〈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。



- 6.[新しい接続を作成する]をクリックします。

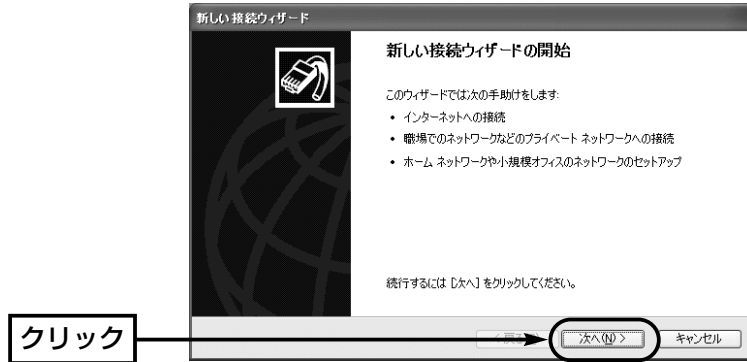


7-1.Windows XPをクライアントに使用する場合  
 〈PPTP用のパソコン設定例〉

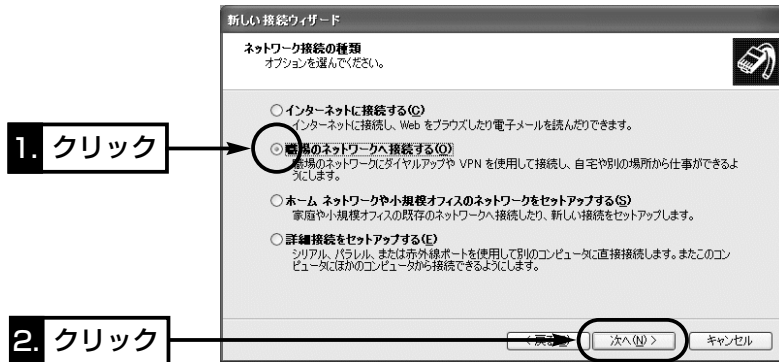
◎Windows XPの場合

〈設定の手順〉(つづき)

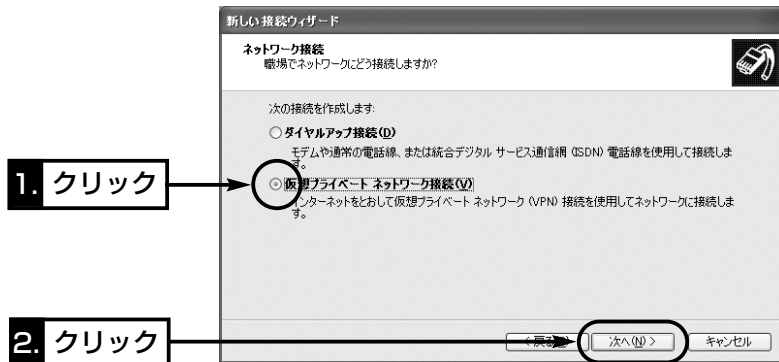
7. 〈次へ(N)〉 をクリックします。



8.[職場のネットワークへ接続する(Q)]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 PPTPパススルーの設定

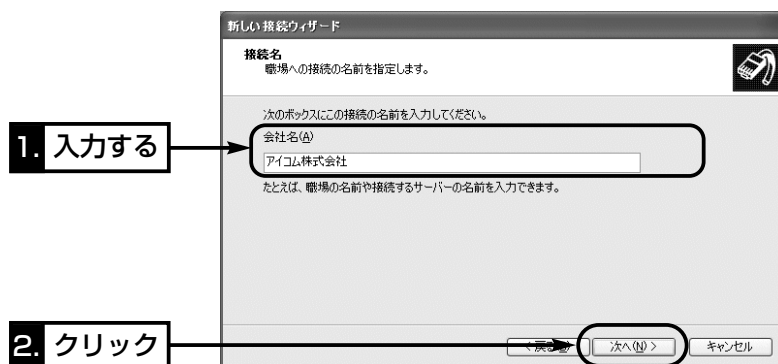
### 7-1.Windows XPをクライアントに使用する場合

〈PPTP用のパソコン設定例〉

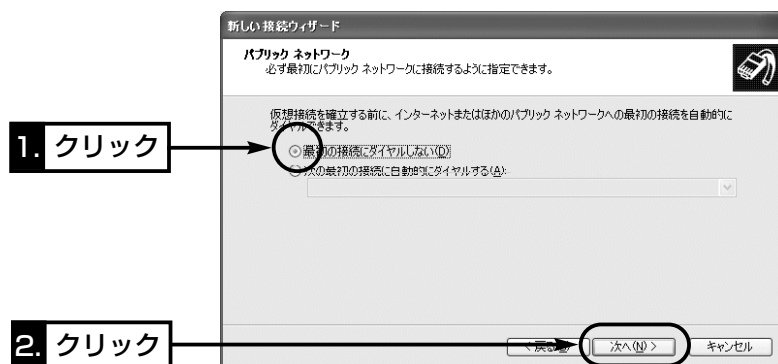
◎Windows XPの場合

〈設定の手順〉(つづき)

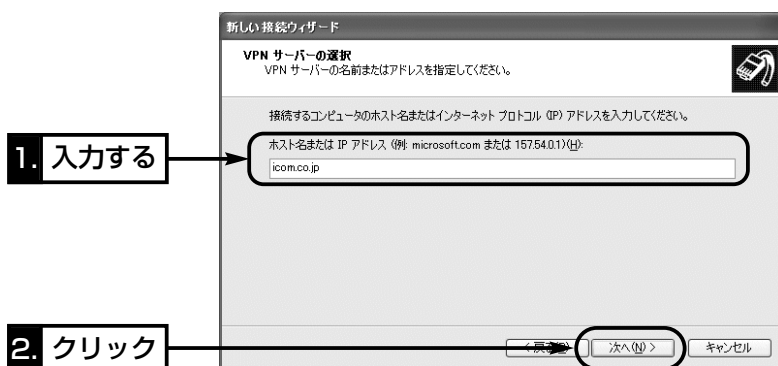
10.接続先名を[会社名(A)]のテキストボックスに入力して、〈次へ(N)〉をクリックします。



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。

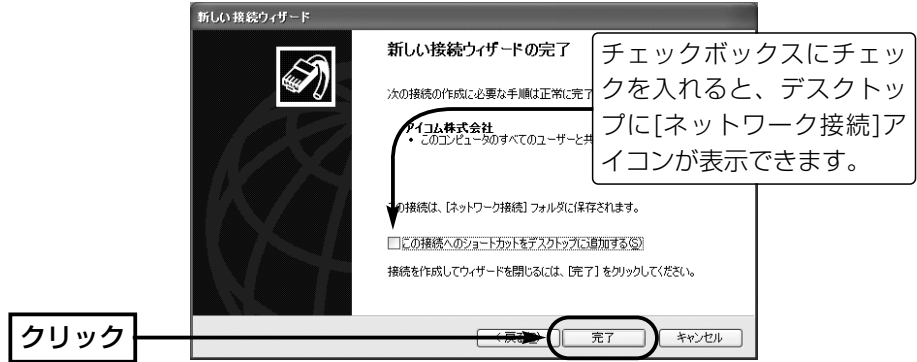


7-1.Windows XPをクライアントに使用する場合  
 <PPTP用のパソコン設定例>

©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 PPTPパススルーの設定

### 7-1.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〉

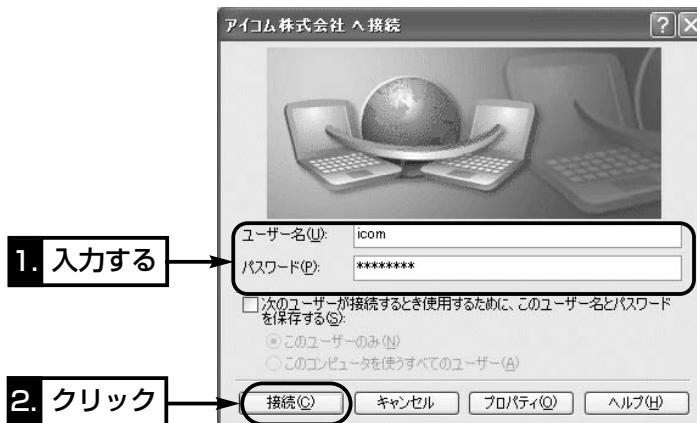
◎Windows XPの場合

〈設定の手順〉(つづき)

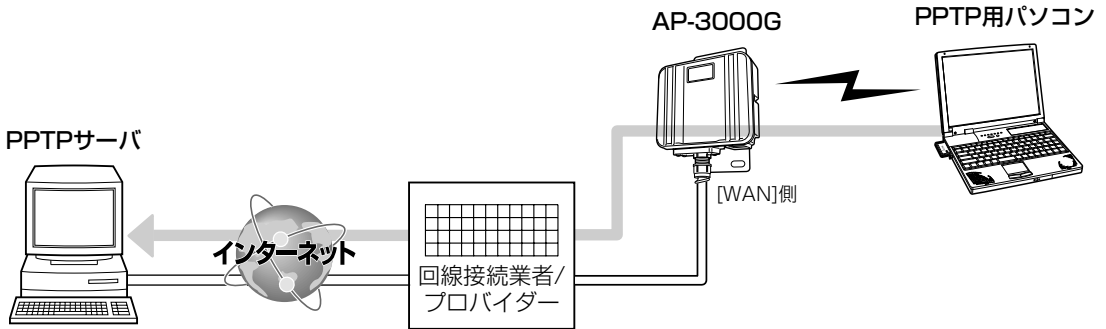
1. 〈スタート〉 → [コントロールパネル(C)]の順に操作します。
2. コントロールパネルから、[ネットワークとインターネット接続]をクリックします。
3. [ネットワーク接続]アイコンをクリックします。
4. 仮想プライベート ネットワークにあるアイコンをクリックします。



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。



7-2.Windows 2000をクライアントにする場合



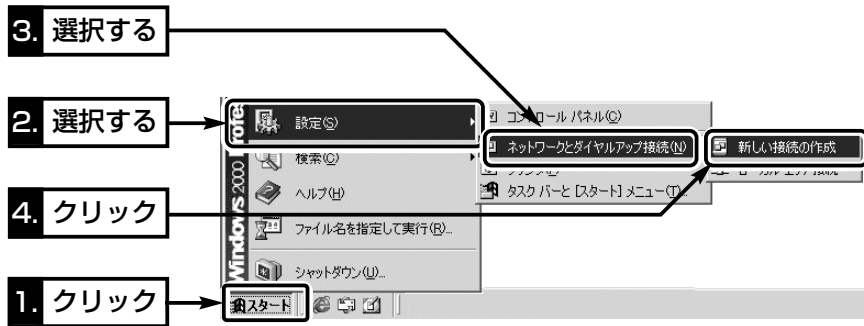
〈PPTP用のパソコン設定例〉

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。

©Windows 2000の場合

〈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 PPTPパススルーの設定

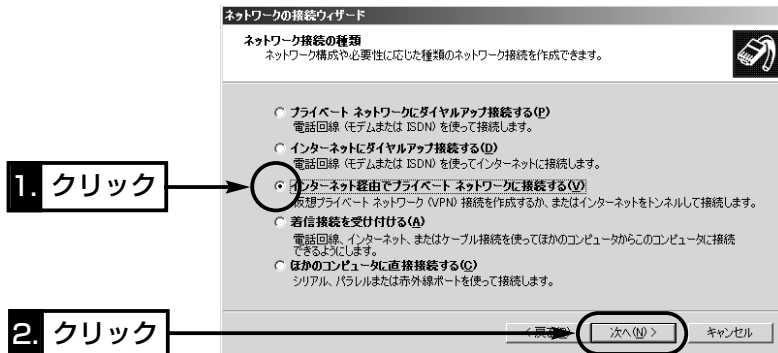
### 7-2.Windows 2000をクライアントに使用する場合

〈PPTP用のパソコン設定例〉

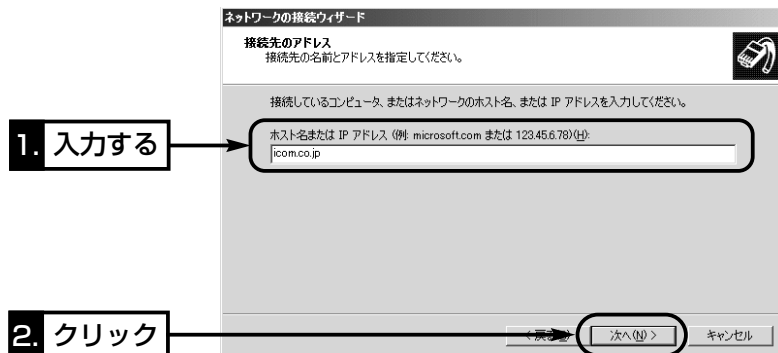
◎Windows 2000の場合

〈設定の手順〉(つづき)

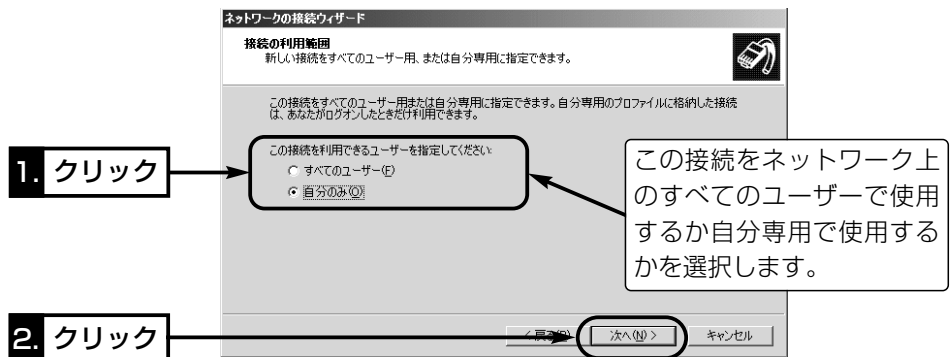
- 3.[インターネット経由でプライベート ネットワークに接続する (V)]のラジオボタンをクリックして、〈次へ(N)〉 をクリックします。



- 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。

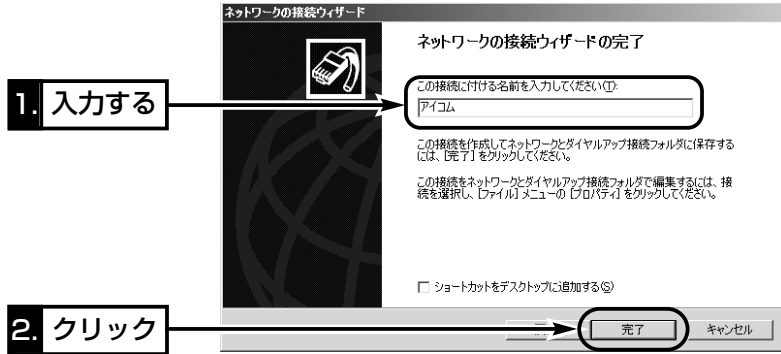




7-2.Windows 2000をクライアントに使用する場合  
 <PPTP用のパソコン設定例>

©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。



7.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 PPTPパススルーの設定

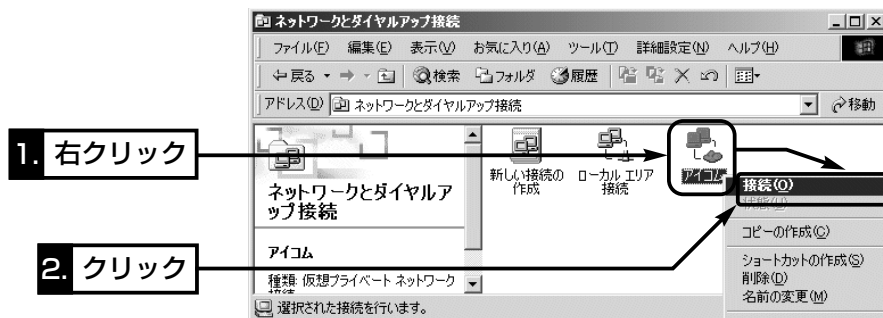
7-2.Windows 2000をクライアントに使用する場合

〈PPTP用のパソコン設定例〉

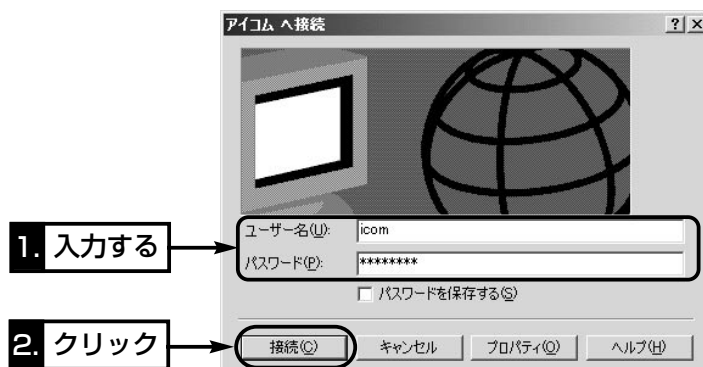
◎Windows 2000の場合(つづき)

〈設定後、接続するには〉

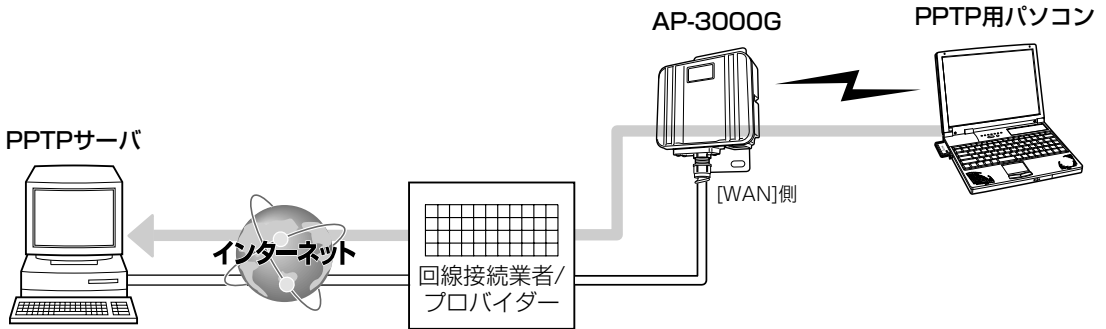
- 1.マウスを 〈スタート〉 →[設定(S)]→[ネットワークとダイヤルアップ接続(N)]の順番に操作します。
- 2.新しく作成されたアイコンを右クリックして、[接続(C)]をクリックします。



- 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(C)〉をクリックします。



7-3.Windows Meをクライアントに使用する場合



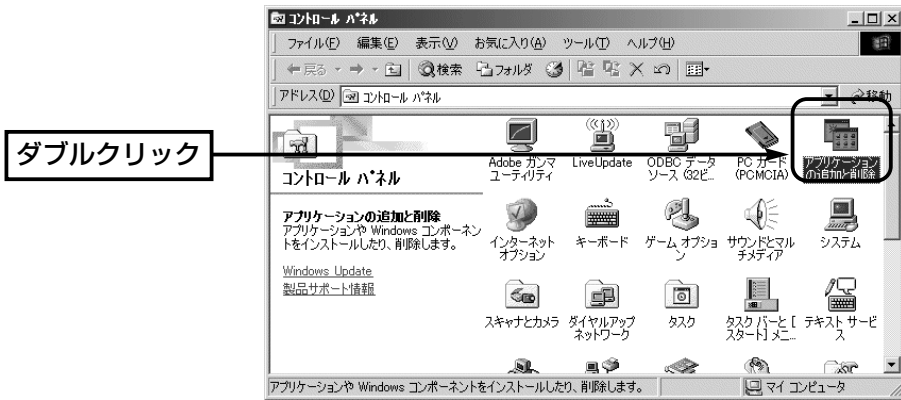
〈PPTP用のパソコン設定例〉

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。

◎Windows Meの場合

〈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 PPTPパススルーの設定

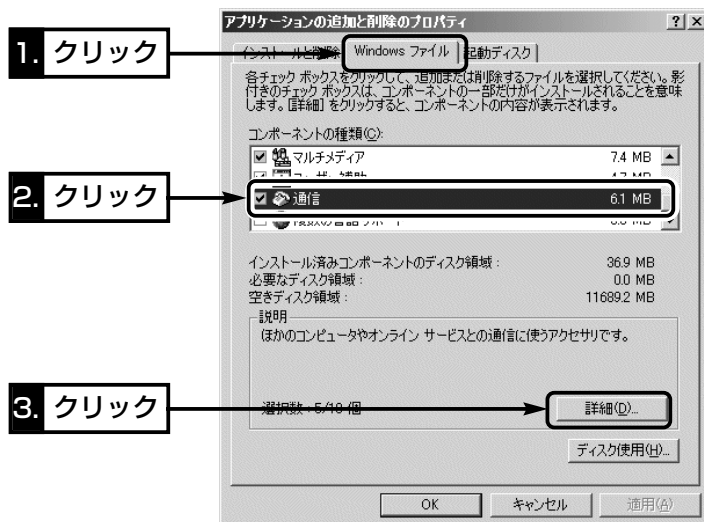
### 7-3.Windows Meをクライアントに使用する場合

〈PPTP用のパソコン設定例〉

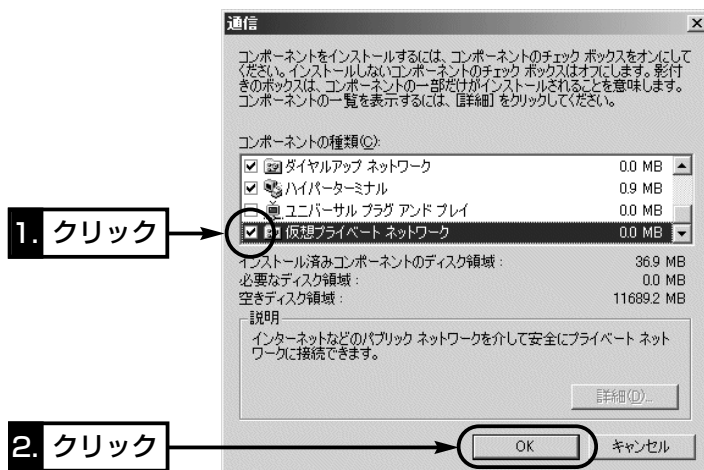
◎Windows Meの場合

〈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。

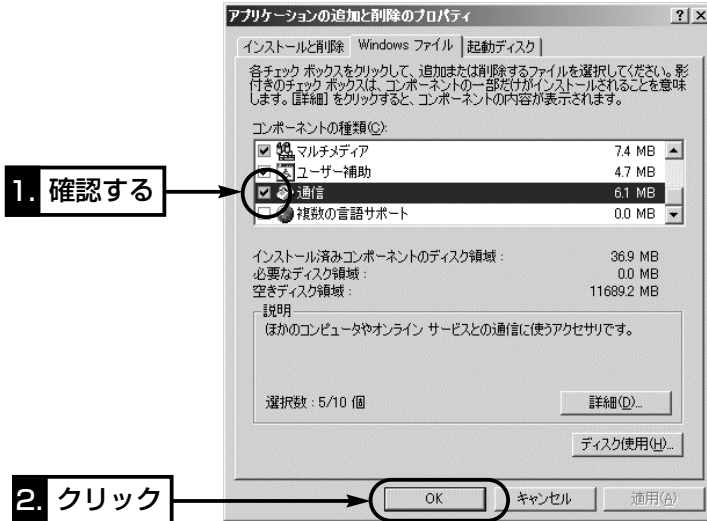


7-3.Windows Meをクライアントに使用する場合  
 <PPTP用のパソコン設定例>

©Windows Meの場合

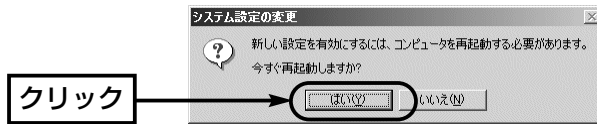
<設定の手順> (つづき)

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。

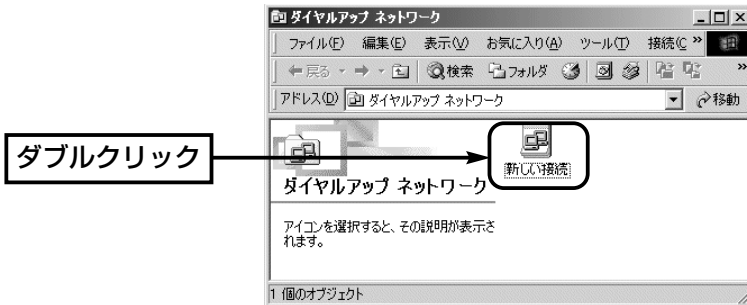


6. <はい(Y)> をクリックします。

- 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。



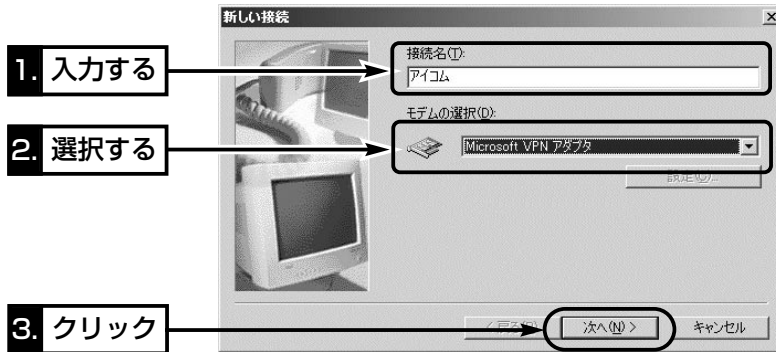
## 7 PPTPパススルーの設定

7-3.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〉

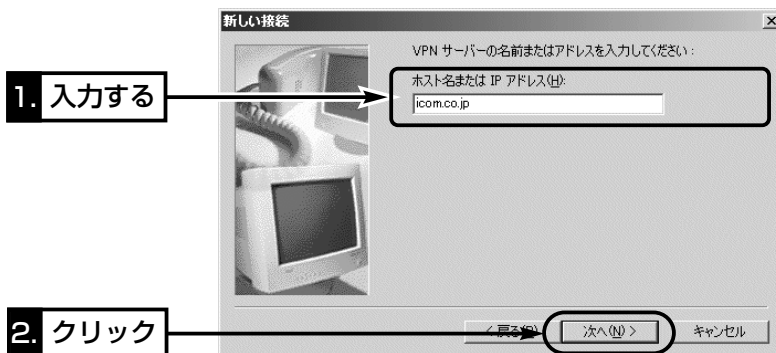
◎Windows Meの場合

〈設定の手順〉(つづき)

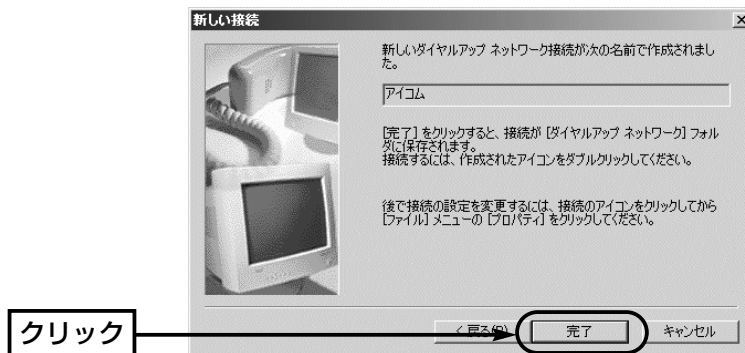
- 8.[接続名(I)]には、あとでわかるように、任意で接続先名を入力します。
- 9.[モデムの選択(D)]から、「Microsoft VPN アダプタ」を選択して、〈次へ(N)〉をクリックします。



- 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。

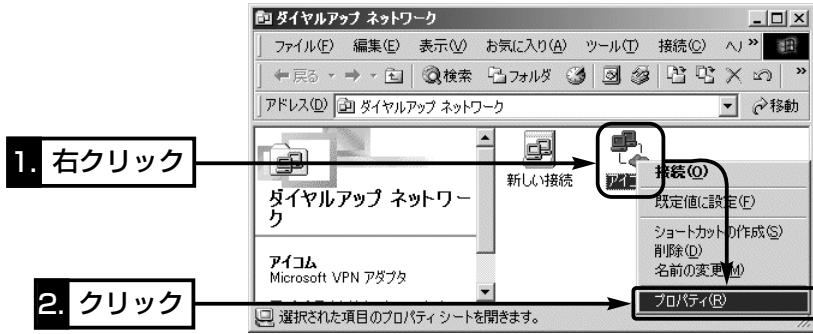


7-3.Windows Meをクライアントに使用する場合  
 <PPTP用のパソコン設定例>

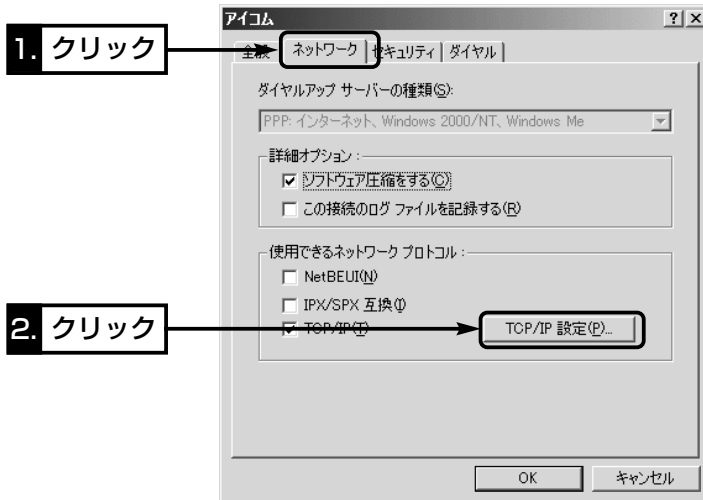
©Windows Meの場合

<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 (R)]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。



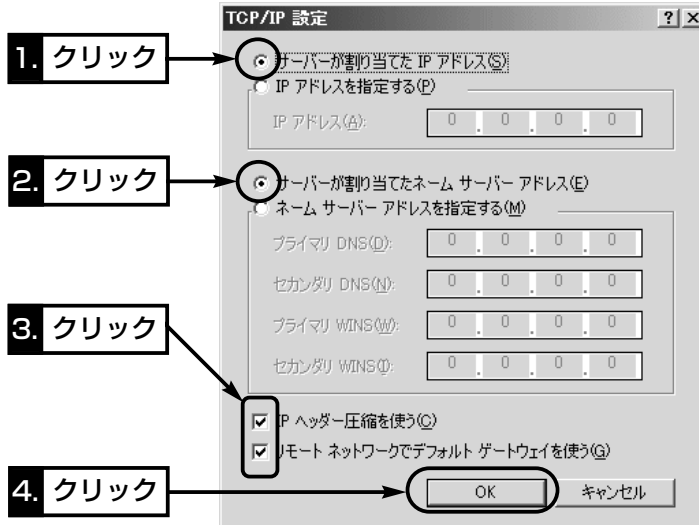
## 7 PPTPパススルーの設定

7-3.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〉

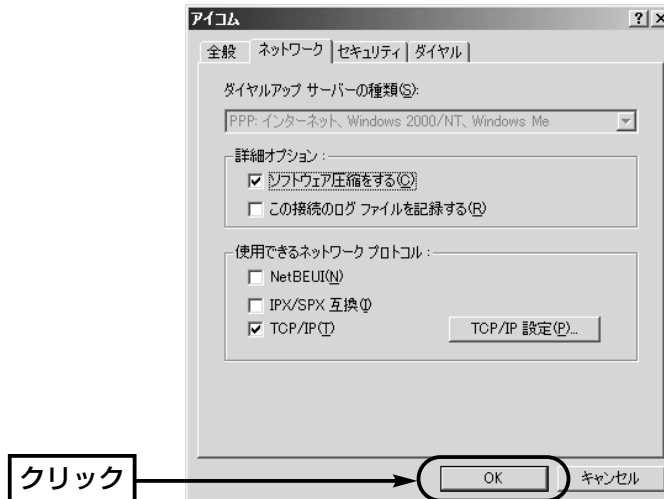
©Windows Meの場合

〈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。

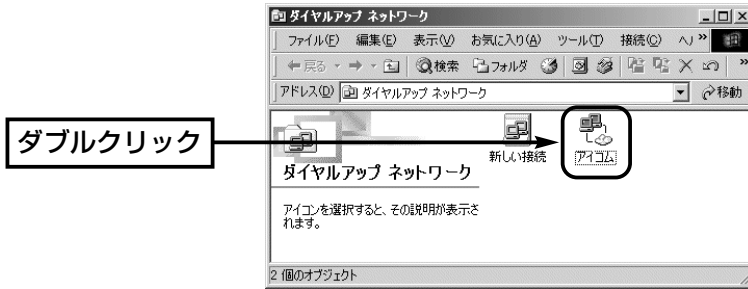




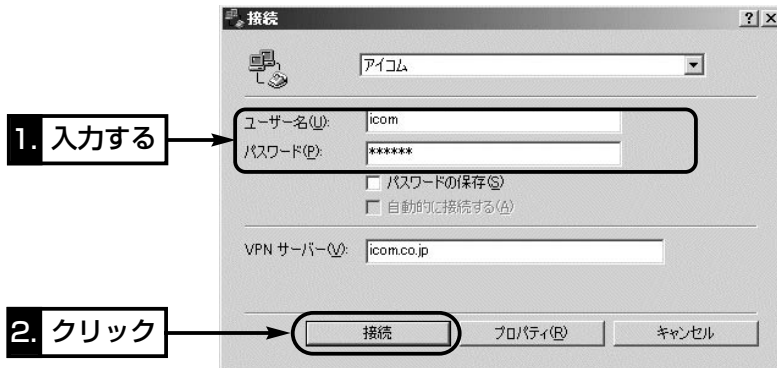
7-3.Windows Meをクライアントに使用する場合  
 <PPTP用のパソコン設定例>  
 ©Windows Meの場合(つづき)

<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。



高品質がテーマです。

## 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	福岡市南区塩原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。

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。  
この補足説明書は、ファームウェア Ver.1.04以降で、「無線LAN設定」メニューに追加された新機能について説明しています。

■ RADIUS設定

- 無線LAN設定
- セキュリティ設定
- 無線LAN設定
- 暗号化設定

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

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き設定します。(出荷時の設定：する)  
※無線パソコンは、Windows XP 標準のワイヤレスネットワーク接続を使用してください。  
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。

■ 無線LAN設定

- 無線LAN設定
- セキュリティ設定
- 無線LAN設定
- 暗号化設定

無線LAN設定	
SSID	
ANYを拒否	<input type="radio"/> しない <input checked="" type="radio"/> する
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	有効
パワーレベル	高
接続端末制限	255
Super A/Gを使用	しない

Super A/G .....

※SL-5200を装着するパソコンと[Super A/G]対応ドライバーをご用意いただくことで、[Super A/G]で通信できます。  
なお、対応ドライバーは、弊社ホームページより公開を予定しています。(2004年6月現在)

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]機能で通信する場合、SL-5200(弊社製無線LANカード)をパソコンに装着しているとき有効です。

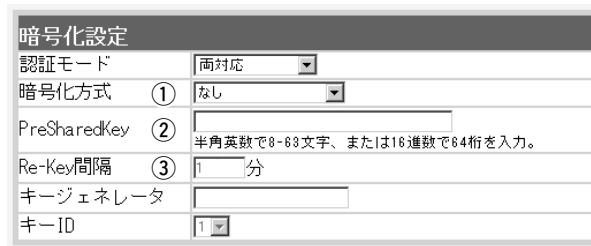
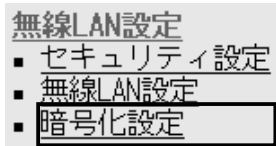
パソコンに装着された無線LANカードが、[Super A/G]に対応していない場合は、[Super A/G]を使用しなると同じ状態になります。

アイコム株式会社

本 社	547-0003 大阪市平野区加美南1-1-32	TEL 011-820-3888	大阪営業所	547-0004 大阪市平野区加美野作1-6-19	TEL 06-6793-0331
北海道営業所	003-0806 札幌市白石区菊水6条2-2-7	TEL 022-298-6211	広島営業所	733-0942 広島市西区井口3-1-1	TEL 082-501-4321
仙台営業所	983-0857 仙台市宮城野区東十番丁54-1	TEL 03-3455-0331	四国営業所	760-0071 高松市藤塚町3-19-43	TEL 087-835-3723
東京営業所	108-0022 東京都港区海岸3-3-18	TEL 052-832-2525	九州営業所	815-0032 福岡市南区塩原4-5-48	TEL 092-541-0211
名古屋営業所	468-0066 名古屋市中区元八事3-249				

高品質がテーマです。

## ■ 暗号化設定



### ① 暗号化方式 ……………

※SL-5200を装着するパソコンと、[WPA-PSK(TKIP/AES)]方式で通信できます。

WPA-PSK(TKIP/AES) :

[WPA-PSK]は、Windows XP(Service Pack1)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。

※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。

※パソコンに装着する無線LANカードが、SL-5000XG、SL-5100の場合は、[WPA-PSK(TKIP/AES)]方式で通信できません。

※無線パソコン側の暗号化方式と異なるときは、通信できません。

※「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 PreSharedKey……………

※SL-5200を装着するパソコンと、[WPA-PSK(TKIP/AES)]方式で通信するとき、有効です。

[暗号化方式](①)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。

### ③ Re-Key間隔 ……………

※SL-5200を装着するパソコンと、[WPA-PSK(TKIP/AES)]方式で通信するとき、有効です。

[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。

## ■ [WPA-PSK(TKIP/AES)]暗号化方式を設定するには

[WPA-PSK(TKIP)/(AES)]の暗号化鍵(キー)による設定は、16進数で64桁を入力する方法、またはASCII文字で8~63文字を入力する方法があります。

パソコンに装着するSL-5200にも同じ設定をしてください。

画面は、下記の条件を設定するときの例です。

[暗号化方式] : 「WPA-PSK(TKIP)」

[PreSharedKey] : 「WAVEMASTER」(ASCII文字：8~63文字で入力します。)

[Re-Key間隔] : 「1」分(出荷時の設定)

### <AP-3000G側>

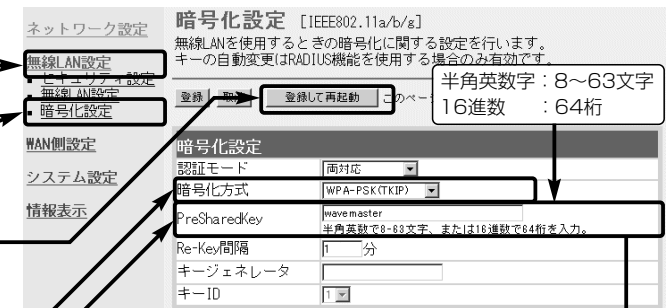
1. クリック

2. クリック

5. クリック

3. 選択する

4. 入力する



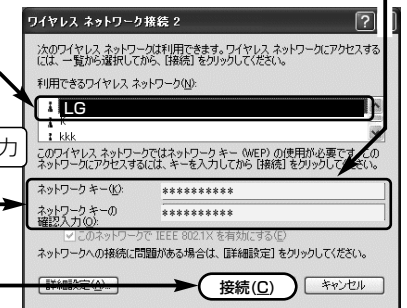
### <無線パソコン側>

① クリック

② PreSharedKeyの入力

③ クリック

Windows XP(Service Pack1)に修正プログラムが適用していただくことで、WPA暗号化認証方式を無線パソコン側で使用できます。



※無線パソコンは、Windows XP(Service Pack1)に修正プログラムが適用されたもので、接続ツールは、Windows XP標準のワイヤレスネットワーク接続をご使用ください。

※2004年6月現在、「WPA-PSK(TKIP/AES)」暗号化に対応する弊社製無線LANカードは、SL-5200だけです。

SL-5200に付属の設定ユーティリティは、「WPA-PSK(TKIP/AES)」方式に対応していませんので、Windows XP標準のワイヤレスネットワーク接続をご使用ください。