ICOM®

取扱説明書[活用編]

WAVEMASTER®

WIRELESS LAN UNIT

SE-3000

PoE専用

Icom Inc.

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。

もくじ

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

第1部

「単端末接続」モード編

本製品の動作モードを「単端末接続」に設定したとき、表示されるメニューの各画面についての説明です。

第1部

第1章 「接続」メニュー

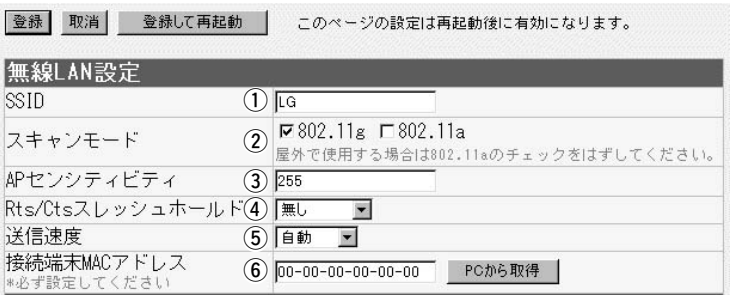
この章では、
「接続」メニューで表示される設定画面について説明します。

1 「接続」メニュー

1-1.「接続」画面

■無線LAN設定

本製品の無線通信に対する基本設定です。



〈登録〉ボタン …… 「接続」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 …… 「接続」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、「接続」画面で変更したすべての設定内容を有効にします。

①SSID …… 本製品と無線アクセスポイントには、通信相手をグループとして識別するための無線ネットワーク名として、SSIDが設定されています。 (出荷時の設定：LG〈半角〉)
同じグループで通信するお互いの無線LAN機器で、この[SSID]が異なると通信できません。
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。
※[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。

1-1.「接続」画面
■ 無線LAN設定(つづき)

② スキャンモード ……

★屋外で使用する場合は、必ず[802.11a]のチェックボックスにチェックマークを入れないでください。

本製品で使用する無線LAN規格(802.11a/802.11g)を設定します。
[802.11a]と[802.11g(802.11bを含む)]を同時に設定できます。　(出荷時の設定：802.11g)
[802.11a]と[802.11g]を同時に設定し、[送信速度]欄を「自動」に設定して使用する場合、[802.11a/b/g]が混在する環境では、通信環境の良い無線アクセスポイントに接続されます。

③ APセンシティビティ ……

無線アクセスポイントからの電波が途切れたとき、スキャンを開始するまでの間隔を設定します。
無線アクセスポイントの設置環境やネットワーク状況の影響でローミング動作がスムーズに行えないとき、この設定を変更すると通信状況が改善されます。
設定できる範囲は「10～255」です。　(出荷時の設定：255)
小さい数値を設定するほど、電波が途切れてからスキャンを開始するまでの間隔が短く、大きい数値を設定するほど、電波が途切れてからスキャンを開始するまでの間隔が長くなります。

1 「接続」メニュー

1-1.「接続」画面
■無線LAN設定(つづき)

④ Rts/Ctsスレッシュホールド ……

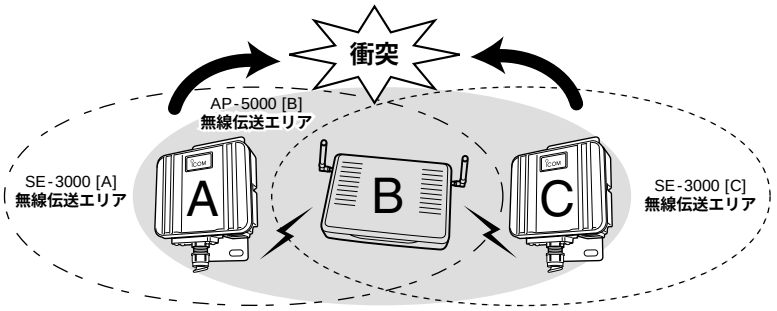
ネゴシエーションするために送るパケットのデータサイズを、「500バイト」または「1000バイト」から選択します。

(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、それぞれが無線アクセスポイント[B]と無線通信できても、互いが直接通信できない本製品[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、本製品[A]から送信要求(Rts)信号を受信した無線アクセスポイント[B]が、無線伝送エリア内にある本製品[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本製品[C]に無線アクセスポイント[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本製品[C]は、無線アクセスポイント[B]から受信完了通知(ACK)を受信するまで無線アクセスポイント[B]へのアクセスを自制することで、通信の衝突を防止できます。



1-1.「接続」画面
■ 無線LAN設定(つづき)

⑤ 送信速度 ……

「自動」を設定すると、環境の変化などで通信が不安定になっても、[スキャンモード]欄で設定した方式で通信が続行可能な速度に自動で切り替わります。　(出荷時の設定：自動)
[スキャンモード]欄で設定したモードによって、対応できる[送信速度]が異なります。
対応できない送信速度を設定した場合は、「自動」で動作します。
◎「802.11g」および「802.11a」を設定時、「自動」以外を設定したとき対応できる速度は、「54/48/36/24/18/12/9/6」Mbpsです。
◎「802.11b」を設定時、「自動」以外を設定したとき対応できる速度は、「11/5.5/2/1」Mbpsです。
※[スキャンモード]を「802.11a」に設定し、[送信速度]を「11/5.5/2/1」Mbpsのいずれかに設定したときは、送信速度の設定が「802.11a」に該当しないため、[送信速度]は「自動」で動作します。
※[802.11b]専用の無線アクセスポイントと通信する場合は、下の欄で「自動(出荷時の設定)/11/5.5/2/1」Mbpsのいずれかに設定すると使用できます。

⑥ 接続端末MACアドレス……

「単端末接続」モードに設定したときだけ表示される設定欄で、本製品とEthernetケーブルで接続されたパソコン(Ethernetカード)のMACアドレスを登録します。
(出荷時の設定：00-00-00-00-00-00)
登録するときは、〈PCから取得〉をクリックして、MACアドレスを取得後、〈登録して再起動〉をクリックします。
※本製品に接続するパソコンのMACアドレスが未登録の場合、「単端末接続」モードで無線通信できません。

1 「接続」メニュー

1-1.「接続」画面(つづき)

■暗号化設定

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

①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)

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

◎WEP RC4：無線LAN機器の暗号化として一般によく搭載されている暗号化方式です。
暗号化方式は、RC4(Rivest's Cipher 4)アルゴリズムをベースに構成されています。
暗号化するデータのブロック長が8ビットで、暗号化鍵(キー)の長さを選択できます。
※選択できる暗号化鍵(キー)の長さは、64(40)/128(104)/152(128)ビットの中から選択できます。

◎OCB AES：WEP RC4より強力で、標準化が推進されている次世代の暗号化方式です。
暗号化するデータのブロック長と暗号化鍵(キー)の長さは、128ビットです。
この128ビットに対して任意に鍵(キー)を設定できますので、[WEP RC4]より強力な暗号化方式です。

1-1.「接続」画面
■暗号化設定(つづき)

②キージェネレータ …… 暗号化および復号に使う鍵(キー)を生成するための文字列を設定します。
通信を行う相手間で同じ文字列(大文字/小文字の区別に注意して、任意の半角英数字/記号)を31文字以内で設定します。
なお、入力した文字はすべて「＊(アスタリスク)」で表示します。
(表示例：＊＊)
「暗号化方式」を選択して、〈登録〉をクリックすると、[キージェネレータ]欄に入力した文字列より生成された鍵(キー)を[キー値]項目のテキストボックスに表示します。
[キー値]項目の各キー番号のテキストボックスに生成される桁数および文字数は、選択する「暗号化方式」によって異なります。(取扱説明書[導入編]☞4-2章 ■暗号化鍵(キー)値の入力についてを参照)
※「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。

③キーID …… 暗号化に使用する鍵(キー)番号を設定します。 (出荷時の設定：1)
鍵(キー)番号は、通信する相手間でそれぞれ任意に選択できます。
[暗号化設定]項目の[暗号化方式]欄で、「RC4」または「OCB AES」が登録されているときは、「1」～「4」の中から選択できます。

1 「接続」メニュー

1-1.「接続」画面(つづき)

■キー値

暗号化鍵(キー)を直接入力するための設定です。

① 入力モード …… 暗号化鍵(キー)の入力のしかたを選びます。

(出荷時の設定：16進数)

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

※ASCII文字が設定されているときは、キージェネレータを使用できません。

② 鍵(キー)入力用ボックス … キージェネレータを使用しないとき、暗号化および復号に使用する鍵(キー)を、[入力モード]欄で設定された方法で、直接入力します。 (出荷時の設定：00-00-00-00-00)

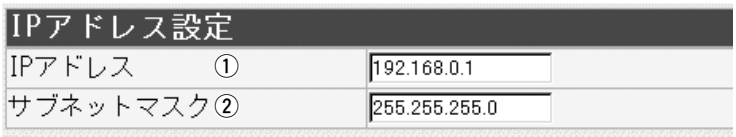
16進数表記で使用する以外のアルファベットを入力しても無効です。

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

使用するキーIDに対する鍵(キー)の内容が違うときは通信できません。

■IPアドレス設定

「単端末接続」モードに設定したときだけ表示される設定項目で、本製品のIPアドレスを設定します。



① IPアドレス …… 本製品のIPアドレスを入力します。

(出荷時の設定：192.168.0.1)

本製品の設定画面にアクセスするときは、この欄に設定したIPアドレスを指定すると、アクセスできます。

② サブネットマスク …… 本製品のサブネットマスク(同じネットワークグループで使用するIPアドレスの範囲)を設定します。

(出荷時の設定：255.255.255.0)

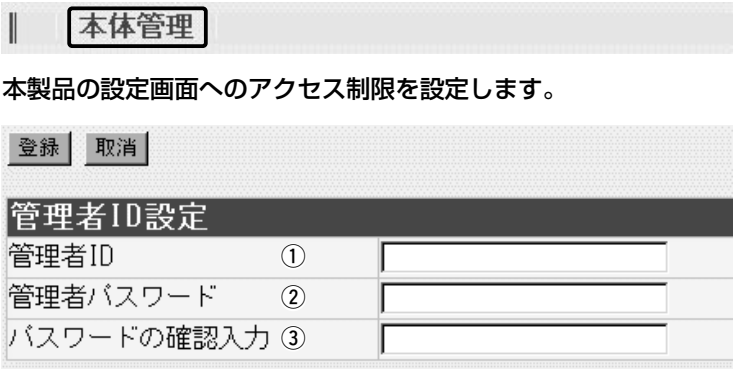
第1部

第2章 「本体管理」メニュー

この章では、
「本体管理」メニューで表示される設定画面について説明します。

2 「本体管理」メニュー

2-1.「本体管理」画面



■管理者ID設定

〈登録〉ボタン …… 「本体管理」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 …… 「本体管理」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：se3000)
[管理者ID]を設定すると、次回のアクセスからユーザー名の入力を求められますので、そこに[管理者ID]を入力します。

②管理者パスワード …… [管理者ID]に対するパスワードを設定する場合、大文字/小文字の区別に注意して、任意の英数字、半角31文字以内で入力します。
入力した文字は、すべて「＊(アスタリスク)」で表示されます。
(表示例：＊＊＊＊＊＊)
[管理者パスワード]を設定すると、次回のアクセスからパスワードの入力を求められますので、そこに[管理者パスワード]を入力します。

③パスワードの確認入力 …… 確認のために、パスワードを再入力します。
(表示例：＊＊＊＊＊＊)

第1部

第3章 「情報表示」メニュー

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。

3 「情報表示」メニュー

3-1.「インターフェイス情報」画面

■ネットワーク インターフェイス リスト

本製品のインターフェイスに対する[IPアドレス]と[サブネットマスク]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

■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		
Ethernet ①	状況	通信中
	送信パケット数	141
	受信パケット数	146
Wireless ②	状況	通信中
	送信パケット数	1
	受信パケット数	0

① Ethernet…… [有線LAN]ポートの通信状況と、そのときの送信と受信のパケット数を表示します。

② Wireless…… [無線LAN]ポートの通信状況と、そのときの送信と受信のパケット数を表示します。

3-1.「インターフェイス情報」画面(つづき)

■ 無線通信状態　　**無線アクセスポイントとの通信状態を表示します。**

無線通信状態		
SSID	①	manual
暗号化	②	無効
チャンネル	③	6CH (2437MHz)
信号レベル	④	45

① SSID …… 無線通信に使用する無線ネットワーク名(SSID)を表示します。

② 暗号化 …… 無線通信に暗号化が設定されているかどうかを表示します。

③ チャンネル …… 無線アクセスポイントとのチャンネルを表示します。

④ 信号レベル …… 無線アクセスポイントとの信号レベルを表示します。
表示される数値を通信の目安にしてください。

■ 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、本製品の底面部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-C7-68-04-79

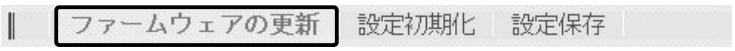
第1部

第4章 「メンテナンス」メニュー

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。

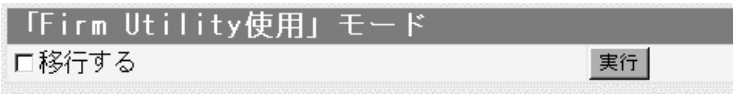
4 「メンテナンス」メニュー

4-1.「ファームウェアの更新」画面



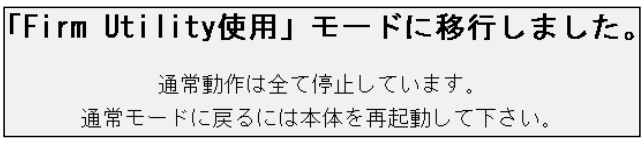
■「Firm Utility使用」モード

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

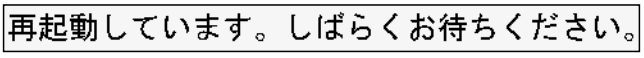
4-2.「設定初期化」画面

■設定初期化

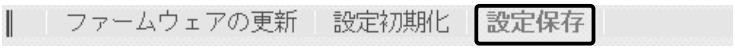
本製品の設定内容をすべて出荷時の状態に戻します。

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。



4-3.「設定保存」画面



■設定の保存と書き込み

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。

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。

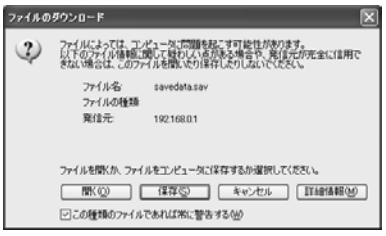
設定ファイルの保存先をテキストボックスに直接入力するか、〈参照...〉ボタンをクリックすると表示される右の画面から目的の設定ファイルを指定します。

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。
※WWWブラウザの「ファイル(F)」メニューから、[名前を付けて保存(A)...]をクリックして保存した「設定保存」画面のファイル(拡張子：.htm/.html)とは互換性がありませんので保存したファイルとして読み込むことはできません。

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。

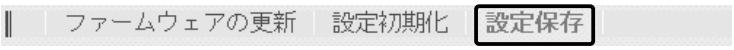
[設定の保存と書き込み]項目で[ファイルに保存]をクリックすると表示される右の画面から〈保存〉をクリックすると、設定ファイルを保存できます。



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。

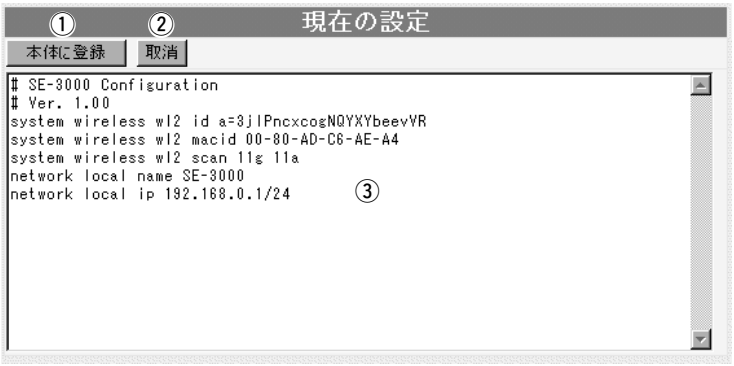
4 「メンテナンス」メニュー

4-3.「設定保存」画面(つづき)



■現在の設定

変更された設定内容の確認や設定ファイルをハイパーテキスト形式(.htm/.html)で保存、書き込みができます。



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。
※本製品のIPアドレスの設定が、「内容表示」部に表示されたIPアドレスと異なるときは、設定を本製品に登録できません。

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」部 …… 変更された設定内容を表示します。
この画面内容をパソコンに保存することで、本製品の設定をバックアップすることができます。
保存するときは、WWWブラウザの「ファイル(F)」メニューから、[名前を付けて保存(A)...]をクリックすると、保存できます。
※[設定の保存と書き込み]項目の「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)とは互換性がありませんので、読み込むことはできません。
※各画面で設定されたパスワードやキージェネレーター(無線LAN通信用暗号化鍵の生成元文字列)の内容は、暗号化されて表示されます。
そのため、保存されたファイルよりそれらが外部へ漏れることはありません。

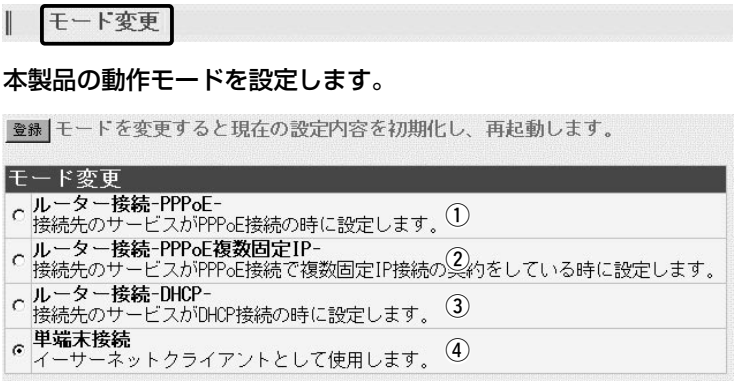
第1部

第5章 「モード変更」メニュー

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

5 「モード変更」メニュー

5-1.「モード変更」画面



■ モード変更

本製品の動作モードを設定します。

〈登録〉ボタン …… ここで変更した内容を確定すると同時に、それ以外の画面で設定した内容は出荷時の状態に戻して再起動します。

① ルーター接続 –PPPoE– … 回線接続先に[PPPoE]方式で無線接続できるサービスを契約している場合、本製品からインターネット回線に無線で接続するとき使用するモードです。

※ご契約の接続先がマルチセッションに対応していれば、同じパソコンから通常の「PPPoE」接続先とは別の「PPPoE」接続先にも接続できます。
また、2台のパソコンのうち1台は通常の「PPPoE」接続先に接続、残りの1台は別の「PPPoE」接続先に接続できます。

② ルーター接続 –PPPoE 複数固定IP– …… 回線接続先が[PPPoE]方式で無線接続でき、複数のグローバル固定IPアドレスを提供するサービスを契約している場合、グローバルIPアドレスを固定で付与したパソコンから本製品を介してインターネット回線に無線で接続するとき使用するモードです。

※ご契約の回線接続業者、またはプロバイダーから割り当てられた複数のグローバル固定IPアドレスを本製品のEthernetケーブルに接続されたパソコン(LAN側)で利用できます。
また、プライベートアドレスが割り当てられたパソコンと混在した環境でご利用いただけます。

★ご契約の回線接続業者、またはプロバイダーから割り当てられた複数のグローバル固定IPアドレス(例：8個の場合)の使いかたについては、第5部(本書)の第2章を参考にしてください。

③ ルーター接続 –DHCP–…… 回線接続先に[DHCP]方式で無線接続できるサービスを契約している場合、本製品からインターネット回線に無線で接続するとき使用するモードです。

④ 単端末接続(出荷時の設定) Ethernetポート搭載のパソコンと接続することで、無線クライアントとして弊社製無線アクセスポイントと通信するとき使用するモードです。
このとき、本製品のEthernetケーブルに接続できるパソコンは、1台だけです。

第2部

「ルーター接続 –PPPoE–」モード編

本製品の動作モードを「ルーター接続 –PPPoE–」に設定したとき、表示されるメニューの各画面についての説明です。

第2部

第1章 「WAN側設定」メニュー

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。

1 「WAN側設定」メニュー

1-1.「WAN側」画面

■接続状況　　**登録された回線への接続状況を表示します。**

接続状況			
PPPoEセッション	①	第1セッション 接続	第2セッション 接続
接続状況	②	未接続	未接続
回線種別	③	PPPoE（自動接続）	PPPoE（手動接続）
DNSサーバ	④	-	-
本体側のIPアドレス	⑤	-	-
相手先のIPアドレス	⑥	-	-
接続時間	⑦	- 時間 - 分 - 秒	- 時間 - 分 - 秒

①PPPoEセッション …… 本製品に登録した回線接続先(第1および第2)への〈接続〉および〈切断〉ボタンです。
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。
マルチセッション対応の回線接続先への接続および切断は、[第2セッション]欄の〈接続〉および〈切断〉ボタンをクリックします。
※〈切断〉ボタンは、回線を接続したときに表示されます。

②接続状況 …… WAN側回線への接続状況を「未接続」/「接続中」で表示します。

③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)」のいずれかを表示します。

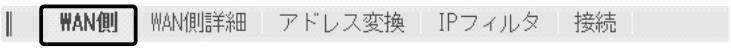
④DNSサーバ …… ご契約されている回線接続業者、またはプロバイダーのDNSサーバIPアドレスを表示します。

⑤本体側のIPアドレス …… 本製品のWAN側に設定されたIPアドレスを表示します。

⑥相手先のIPアドレス …… 契約されている回線接続業者、またはプロバイダーのIPアドレスを表示します。

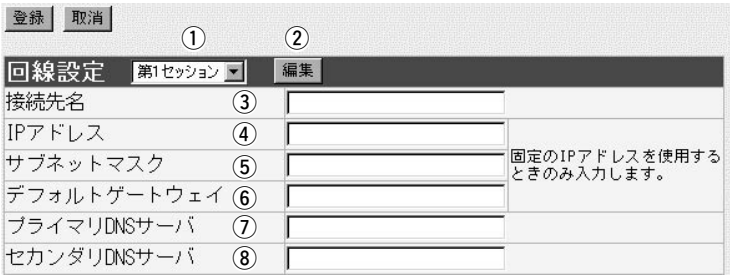
⑦接続時間 …… ご契約の回線接続業者、またはプロバイダーに接続してから、この画面にアクセスした時点までの時間を表示します。
最新の接続時間を表示させるときは、WWWブラウザの〈更新〉をクリックします。

1-1.「WAN側」画面(つづき)



■回線設定

本製品のWAN側についての設定です。



〈登録〉ボタン …… [回線設定]項目と[接続設定]項目の内容を確定するボタンです。

〈取消〉ボタン …… [回線設定]項目および[接続設定]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接続先選択 …… (第1/第2セッション) 〈▼〉をクリックして接続先を登録するセッションを選択してから、[回線設定]項目と[接続設定]項目の各欄を設定します。
※「第1セッション」側は、通常の「PPPoE」接続先を設定するとき使用します。
「第2セッション」側に設定しても使用できません。
※「第2セッション」を選択した場合、[回線設定]項目の各欄は空白(何も設定しない)の状態で使用します。
※「第2セッション」側選択時、[接続設定]項目の各欄は、マルチセッションする「PPPoE」接続先(NTTフレッツ·スクウェア)の設定に使用します。

②〈編集〉ボタン …… 登録した接続先の内容を変更する場合は、[接続先選択](①)欄の〈▼〉でセッションを選択して〈編集〉をクリックすると、[回線設定]項目の各欄に登録した内容を変更できます。

③接続先名 …… ご契約の回線接続業者、またはプロバイダーがわかるような名前を、任意の英数字、半角31(全角15)文字以内で入力します。
入力した名前は、この項目の[接続先選択](①)欄と、「WAN側詳細」画面にある[PPPoE詳細設定]項目の[接続先選択]欄に表示されます。

④IPアドレス …… 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ときに限り、本製品のWAN側IPアドレスを入力します。

⑤サブネットマスク …… 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。

1 「WAN側設定」メニュー

1-1.「WAN側」画面
■ 回線設定(つづき)

⑥ デフォルトゲートウェイ … 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。

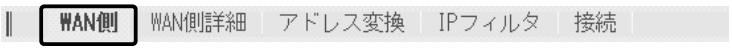
⑦ プライマリDNSサーバ …… ご契約の回線接続業者、またはプロバイダーからDNSサーバのアドレスが2つ指定されている場合は、どちらか一方、または指定されているプライマリDNSアドレスを入力します。

⑧ セカンダリDNSサーバ …… ご契約の回線接続業者、またはプロバイダーから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。

■ マルチセッション機能

本製品で「ルーター接続 –PPPoE –」モードを設定した場合だけ使用できる機能で、ご契約の接続先がマルチセッションに対応(フレッツ·ADSLやBフレッツ)していれば、同じパソコンから通常の「PPPoE」接続先とは別の「PPPoE」接続先(NTTフレッツ·スクウェア)にも接続できます。
また、2台のパソコンのうち1台は通常の「PPPoE」接続先に接続、残りの1台はマルチセッション対応の「PPPoE」接続先に接続できます。
※「第2セッション」側を使用する場合は、登録する接続先の回線がマルチセッションに対応している必要があります。
※本製品の場合、2003年6月現在に於いてマルチセッションに対応できる回線接続先は、NTTフレッツ·スクウェアだけです。
※お住まいの地域がNTTフレッツ·スクウェア提供地域であることをご確認ください。
※NTTフレッツ·スクウェアへの接続は、「第1セッション」側に通常の接続先として、フレッツ·ADSLやBフレッツを設定後、NTTフレッツ·スクウェア接続用の[ユーザID]と[パスワード]を「第2セッション」側の[接続設定]項目に追加してください。
また、「WAN側詳細」画面の[PPPoE詳細設定]項目にある[宛先ドメイン]欄に、「*.flets」と入力してください。
これを設定しない場合、NTTフレッツ·スクウェアのホームページを利用してサービスを受けることができません。
※NTTから提供される「フレッツ接続ツール」は不要です。

1-1.「WAN側」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。
※マルチセッションする場合、NTTフレッツ·スクウェアへの登録は、[回線設定]項目の[接続先選択]欄で「第2セッション」を選択してから、下記の説明を参考に設定してください。

① ユーザID …… 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。

② パスワード …… 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 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、「相手先に合わせる」(出荷時の設定)でご使用ください。

下記の内容は、マルチセッションに対応する接続先を設定してご使用になる場合にご覧ください。
【NTTフレッツ·スクウェアをご使用になるには】
以下の内容を[接続設定]項目に設定してください。
◎NTT西日本でご契約の場合
ユーザID　：**「flets@flets」**(半角文字)と入力
パスワード　：**「flets」**(半角文字)と入力
認証プロトコル：「接続先にあわせる」(出荷時の設定)を選択

◎NTT東日本でご契約の場合
ユーザID　：**「guest@flets」**(半角文字)と入力
パスワード　：**「guest」**(半角文字)と入力
認証プロトコル：「接続先にあわせる」(出荷時の設定)を選択

1 「WAN側設定」メニュー

1-1.「WAN側」画面(つづき)

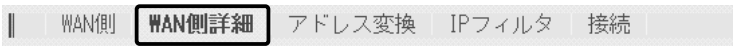
■ マルチセッションとは

「PPPoE」を本製品の回線種別に設定した場合だけ使用できる機能で、ご契約の接続先がマルチセッションに対応していれば、同じパソコンから通常の「PPPoE」接続先とは別の「PPPoE」接続先(NTTフレッツ･スクウェア)にも接続できます。
また、2台のパソコンのうち1台は通常の「PPPoE」接続先に接続、残りの1台はマルチセッション対応の「PPPoE」接続先に接続できます。

※「第2セッション」側を使用する場合は、登録する接続先の回線がマルチセッションに対応している必要があります。
※本製品の場合、2003年10月現在に於いてマルチセッションに対応できる回線接続先は、NTTフレッツ･スクウェアだけです。
※お住まいの地域がNTTフレッツ･スクウェア提供地域であることをご確認ください。
※NTTフレッツ･スクウェアへの接続は、[接続状況]項目の「第1セッション」側に、フレッツ･ADSLやBフレッツへの接続内容を設定した接続先名を選択し、「第2セッション」側にNTTフレッツ･スクウェアへの接続内容を設定した接続先名を選択してください。
また、「WAN側詳細」画面にある[PPPoE詳細設定]項目の[接続先選択]欄で、該当する接続先名を選び、[宛先ドメイン]欄に、「＊.flets」と入力してください。
これを設定しない場合、NTTフレッツ･スクウェアのホームページを利用してサービスを受けることができません。
※NTT東日本でご契約の場合、NTTフレッツ･スクウェアを本製品でお使いいただくには、「ネットワーク設定」メニューの「ルーティング」画面にある[スタティックルーティング設定]項目で設定の追加が必要です。(☞5-3章)
※NTTから提供される「フレッツ接続ツール」は不要です。

〈設定の手順について〉
5-3章(本書)には、NTTフレッツ･スクウェアの設定手順を記載しています。
右記の記載と併せてご覧ください。

1-2.「WAN側詳細」画面



■詳細設定

本製品のWAN側回線全般に機能する設定です。

ステルスモードを使用 ……

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

■PPPoE詳細設定

「PPPoE」接続についての詳細設定です。

①接続先選択 ……

詳細設定をする接続先名を〈▼〉をクリックして選択し、〈選択〉をクリックします。
テキストボックスには、[回線設定]項目の[接続先名]欄に入力した文字が表示されます。
※選択した接続先名が「第1セッション」のものか、「第2セッション」のものかを注意して設定してください。

②接続設定 ……

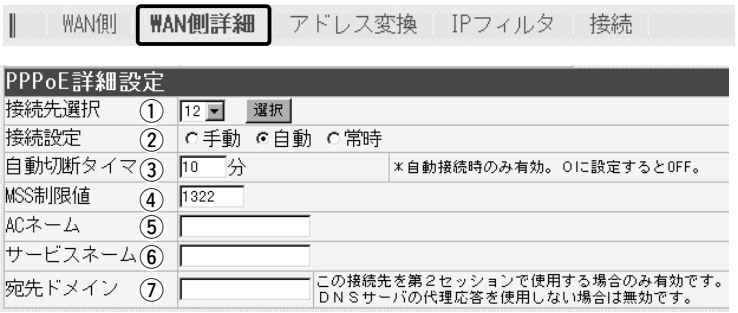
「PPPoE」回線への接続方法を選択します。(出荷時の設定：自動)
◎手動：「WAN側」画面の〈接続〉/〈切断〉ボタンで、回線を強制的に接続/切断します。
◎自動：パソコンからホームページやメールを見る操作を行うだけで、自動的に接続します。
◎常時：常時接続します。
本製品で指定した接続先(WAN側)と常に接続状態を保持します。

③自動切断タイマ ……

[接続設定](②)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。

1 「WAN側設定」メニュー

1-2.「WAN側詳細」画面
■PPPoE詳細設定(つづき)



④MSS制限値…… プロバイダーから指定されている場合に限り、WAN側回線への最大有効データ長を数字で指定します。 (出荷時の設定：1322)
設定できる範囲は、「536～1452」です。
MSS値とは、受信できる最大セグメント数のことです。
イーサネットパケットの最大長(MTU)は1500バイトと定められています。
これに対して、「PPPoE」や「フレッツ·ADSL」の最大データサイズは1322より小さい値となっていますが、現行のインターネットルータには、オーバーサイズのパケットを破棄するものがあります。よって、パケットの保護を優先するために小さめに設定しておく必要があります。

⚠警告

弊社では、MSS値を変更したことによって生じる結果については一切その責任を負いかねますので、あらかじめご了承ください。

⑤AC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。

⑥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。

⑦宛先ドメイン …… [接続先名](①)欄で、「第2セッション」側の名前を選択して〈選択〉をクリックすると表示される欄で、マルチセッションで接続する接続先(NTTフレッツ·スクウェアなど)を「第2セッション」に登録している場合、その接続先が使用するDNSサーバのドメインを設定します。
この欄には、ワイルドカードとして、「？」「＊」が使用できます。また「？」は任意の1文字、「＊」は任意の文字列として認識されます。
NTTフレッツ·スクウェアへ接続する場合、「＊.flets」を指定したときは、「www.flets」などのドメイン名として、その接続先が使用するDNSサーバに問い合わせをします。
※DNSサーバのIPアドレス入力しても無効です。
※本製品の「ネットワーク設定」メニューの「LAN側IP」画面に表示される[DHCPサーバ設定]項目で[DNS代理応答を使用]欄を「しない」に設定している場合は、無効です。

1-2.「WAN側詳細」画面(つづき)

■UPnP設定

①UPnPを使用 ……

UPnP(Universal Plug and Play)機能を使用するかしないかの設定です。　(出荷時の設定：しない)

UPnPを使用すると、NATトラバーサル対応のアプリケーションを、本製品に接続された有線パソコンから利用できます。

※使用時は、セキュリティーが低下しますので注意が必要です。

〈本製品のUPnP機能について〉

２００３年１月現在、下記のアプリケーションが本製品のUPnP(NATトラバーサル)機能に対応しています。

◎Windows Messenger (Version4.6以上)
　Windows XP専用アプリケーション

◎MSN Messenger (Version4.6以上)
　Windows 98/98SE/Me/2000専用アプリケーション

※MSN Messengerで音声チャットを行う場合は、「DirectX」のバージョン8.1以上が必要です。

※あらかじめIPフィルターを設定しているポートをMessengerで使用した場合は、UPnP機能が優先します。

※アプリケーションをバージョンアップする必要がある場合は、「Windows Update」などから行ってください。

②ポートマッピング有効期間

UPnP(NATトラバーサル)対応アプリケーションなどを使用するために、WAN側に対してポートを開いている期間を日数で設定します。

最大9999日まで設定できます。　(出荷時の設定：2)

※「0」日を設定すると、アプリケーションを正しく終了しなかった場合など、本製品を再起動するまでポートが開いたままになりますのでご注意ください。

1 「WAN側設定」メニュー

1-2.「WAN側詳細」画面(つづき)

■Messenger機能対応表

出荷時、UPnP機能は、「使用しない」に設定されています。

：UPnPが必要な機能を意味します。

○：対応　×：非対応

アプリケーション	機　能	UPnP機能を使用する	UPnP機能を使用しない(出荷時)
Windows Messenger ※Windows XP専用	サインイン	○	○
	メンバーの追加	○	○
	インスタントメッセージ	○	○
	音声チャット	○ (Version 4.6以上)	×
	ビデオチャット	○ (Version 4.6以上)	×
	アプリケーション共有	○ (Version 4.6以上)	×
	ホワイトボード	○ (Version 4.6以上)	×
	ファイル転送	×	×
	電話をかける	×	×
リモートアシスタンス ※Windows XP専用	デスクトップの制御	○ (Version 4.6.0082以上)	×
	音声会話	○ (Version 4.6.0082以上)	×
	ファイル転送	○ (Version 4.6.0082以上)	×
MSN Messenger ※Windows 98 Windows 98SE Windows Me Windows 2000	サインイン	○	○
	メンバーの追加	○	○
	インスタントメッセージ	○	○
	音声チャット	○ (Version 4.6以上、DirectX8.1以上)	×
	ファイル転送	×	×
NetMeeting	すべての機能	×	×

1-2.「WAN側詳細」画面(つづき)

■ Windows Messengerの制限について

〈制限〉

◎通信相手もUPnP対応ルーターを使用しているか、グローバルIPアドレスが割り当てられている必要があります。
◎Messengerでの音声チャットなどは、プロバイダーや接続業者から割り当てられるIPアドレスがプライベートIPアドレスの場合、使用できません。
◎静的マスカレードで使用しているポートが多い場合、Messengerの起動が遅かったり音声チャット等が利用できないことがあります。

〈再起動が必要な場合〉

下記のような原因でMessengerが使用できなくなったときは、Messengerを完全に終了してから再度起動してください。
◎Messengerを起動させた状態でポートマッピングの有効期間を経過したとき
◎Messenger起動後にNATおよび静的マスカレードの設定を変更したとき
◎パソコンがスリープ状態になったとき

1 「WAN側設定」メニュー

1-3.「アドレス変換」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」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」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)

②DMZホストIPアドレス … DMZホスト機能(非武装セグメント)を使用するホストの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、本製品とEthernetケーブルで接続されたパソコンでWWWサーバを運用したり、ネットワーク対戦ゲームなどが行えますが、セキュリティー上問題がありますのでご使用には十分注意してください。

③PPTPパススルーを使用 … 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。
(出荷時の設定：する)
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。

1-3.「アドレス変換」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。

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。

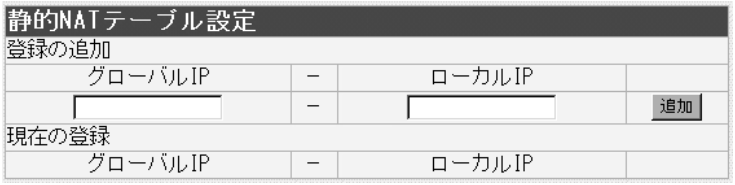
■DMZホスト機能と静的マスカレード機能の違い

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、セキュリティーが低下する。	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。

1 「WAN側設定」メニュー

1-3.「アドレス変換」画面(つづき)

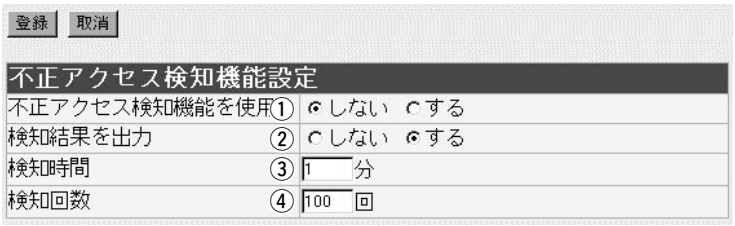
■ 静的NATテーブル設定　　**グローバルとプライベートのIPアドレス変換を行う設定です。**



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。

1-4.「IPフィルタ」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」項目で変更したすべての設定内容が有効になります。

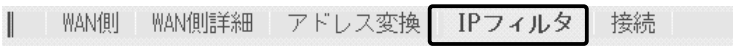
〈取消〉ボタン …… 「不正アクセス検知機能設定」項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

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

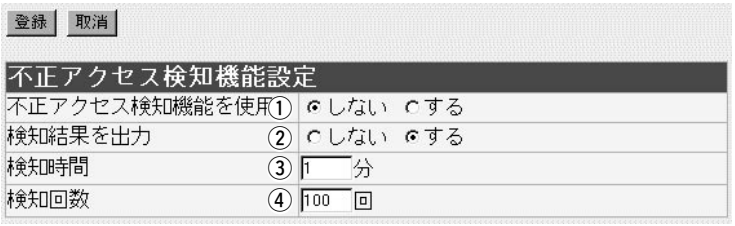
②検知結果を出力 …… 不正アクセスを検知したとき、検知結果を「情報表示」メニューの「通信記録」画面に表示するかしないかを選択します。
(出荷時の設定：する)
※このときの「通信記録」画面表示例は、第2部の4-1章をご覧ください。

1 「WAN側設定」メニュー

1-4.「IPフィルタ」画面



■不正アクセス検知機能設定(つづき)



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]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)

1-4.「IPフィルタ」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。

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。

〈登録〉ボタン

この項目で新規作成、または編集した内容をフィルターとして[現在の登録]項目に登録するボタンです。
※フィルター条件は、1つ以上指定してください。

② フィルタ方向 ……

パケットの通信方向で、WAN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。

1 「WAN側設定」メニュー

1-4.「IPフィルタ」画面
■IPフィルタ設定(つづき)

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。

1-4.「IPフィルタ」画面
■IPフィルタ設定(つづき)

⑤ 発信元ポート番号 …… フィルタリングの対象となる発信元のTCP/UDPポート番号を指定する項目です。数字で指定するときは、「指定」を選択して、番号を始点から終点まで連続で入力します。
入力できる範囲は、10進数で「1～65535」までの半角数字です。
また、特定のポートだけを指定するときは、始点だけ、または始点/終点に同一の番号を入力してください。
数字で指定しない場合は、ニーモニック(DNS、Finger、FTP、Gopher、NEWS、POP3、SMTP、Telnet、Web、Whois)から選択します。

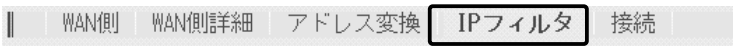
⑥ 宛先ポート番号 …… フィルタリングの対象となる宛先のTCP/UDPポート番号を指定する項目です。
数字で指定するときは、「指定」を選択して、番号を始点から終点まで連続で入力します。
入力できる範囲は、10進数で「1～65535」までの半角数字です。
また、特定のポートだけを指定するときは、始点だけ、または始点/終点に同一の番号を入力してください。
数字で指定しない場合は、ニーモニック(DNS、Finger、FTP、Gopher、NEWS、POP3、SMTP、Telnet、Web、Whois)から選択します。

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。

1 「WAN側設定」メニュー

1-4.「IPフィルタ」画面(つづき)



■現在の登録

現在の登録

		番号	方向	方法	プロトコル	発信元ポート番号	宛先ポート番号	発信元IPアドレス	宛先IPアドレス
編集	削除	57	WAN側から	透過	TCP	20	*	*	*
編集	削除	58	WAN側から	遮断	TCP_EST	*	*	*	*
編集	削除	59	両方	遮断	ALL	135	*	*	*
編集	削除	60	両方	遮断	ALL	*	135	*	*
編集	削除	61	両方	遮断	ALL	445	*	*	*
編集	削除	62	両方	遮断	ALL	*	445	*	*
編集	削除	63	両方	遮断	TCP	*	137 - 139	*	*
編集	削除	64	両方	遮断	UDP	137 - 139	137 - 139	*	*

現在登録されているIPフィルターを表示します。

【出荷時、登録されているフィルターについて】

◎57番　　：FTPをデフォルトで通過させる

◎58番　　：WAN側からの不正アクセス防止

◎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

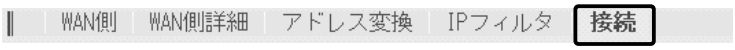
〈編集〉ボタンの右の欄に表示されたIPフィルターを編集するボタンです。

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。

1-5.「接続」画面



■無線LAN設定

本製品の無線通信に対する基本設定です。

〈登録〉ボタン ……

「接続」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 ……

「接続」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、「接続」画面で変更したすべての設定内容を有効にします。

①SSID ……

本製品と無線アクセスポイントには、通信相手をグループとして識別するための無線ネットワーク名として、SSIDが設定されています。　(出荷時の設定：LG〈半角〉)
同じグループで通信するお互いの無線LAN機器で、この[SSID]が異なると通信できません。
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。
※[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。

1 「WAN側設定」メニュー

1-5.「接続」画面
■無線LAN設定(つづき)

② スキャンモード ……

★屋外で使用する場合は、必ず[802.11a]のチェックボックスにチェックマークを入れないでください。

本製品で使用する無線LAN規格(802.11a/802.11g)を設定します。
[802.11a]と[802.11g(802.11bを含む)]を同時に設定できます。 (出荷時の設定：802.11g)
[802.11a]と[802.11g]を同時に設定し、[送信速度]欄を「自動」に設定して使用する場合、[802.11a/b/g]が混在する環境では、通信環境の良い無線アクセスポイントに接続されます。

③ APセンシティビティ……

無線アクセスポイントからの電波が途切れたとき、スキャンを開始するまでの間隔を設定します。
無線アクセスポイントの設置環境やネットワーク状況の影響でローミング動作がスムーズに行えないとき、この設定を変更すると通信状況が改善されます。
設定できる範囲は「10～255」です。 (出荷時の設定：255)
小さい数値を設定するほど、電波が途切れてからスキャンを開始するまでの間隔が短く、大きい数値を設定するほど、電波が途切れてからスキャンを開始するまでの間隔が長くなります。

1-5.「接続」画面
■ 無線LAN設定(つづき)

④ Rts/Ctsスレッシュホールド ……

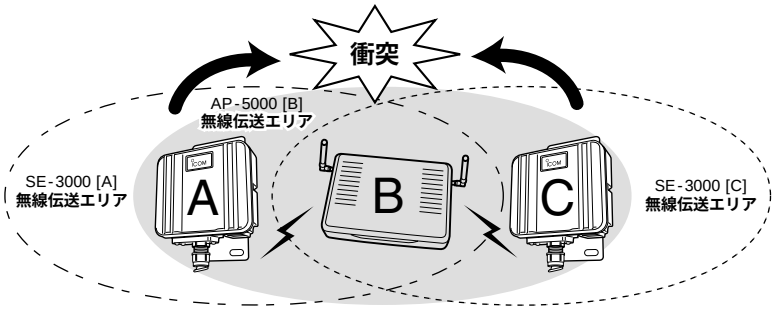
ネゴシエーションするために送るパケットのデータサイズを、「500バイト」または「1000バイト」から選択します。

(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。

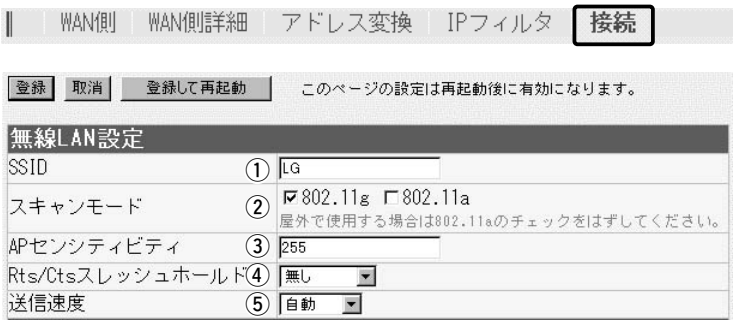
隠れ端末とは、下図のように、それぞれが無線アクセスポイント[B]と無線通信できても、互いが直接通信できない本製品[A]-[C]同士([A]に対して[C]、[C]に対して[A])のことを呼びます。

通信の衝突を防止するには、本製品[A]から送信要求(Rts)信号を受信した無線アクセスポイント[B]が、無線伝送エリア内にある本製品[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本製品[C]に無線アクセスポイント[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本製品[C]は、無線アクセスポイント[B]から受信完了通知(ACK)を受信するまで無線アクセスポイント[B]へのアクセスを自制することで、通信の衝突を防止できます。



1 「WAN側設定」メニュー

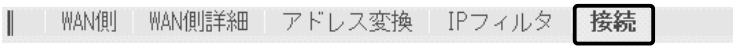
1-5.「接続」画面
■無線LAN設定(つづき)



⑤ 送信速度 ……

「自動」を設定すると、環境の変化などで通信が不安定になっても、[スキャンモード]欄で設定した方式で通信が続行可能な速度に自動で切り替わります。 (出荷時の設定：自動)
[スキャンモード]欄で設定したモードによって、対応できる[送信速度]が異なります。
対応できない送信速度を設定した場合は、「自動」で動作します。
◎「802.11g」および「802.11a」を設定時、「自動」以外を設定したとき対応できる速度は、「54/48/36/24/18/12/9/6」Mbpsです。
◎「802.11b」設定時、「自動」以外を設定したとき対応できる速度は、「11/5.5/2/1」Mbpsです。
※[スキャンモード]を「802.11a」に設定し、[送信速度]を「11/5.5/2/1」Mbpsのいずれかに設定したときは、送信速度の設定が「802.11a」に該当しないため、[送信速度]は「自動」で動作します。
※[802.11b]専用の無線アクセスポイントと通信する場合は、下の欄で「自動(出荷時の設定)/11/5.5/2/1」Mbpsのいずれかに設定すると使用できます。

1-5.「接続」画面(つづき)



■暗号化設定

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

① 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)

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

◎WEP RC4：無線LAN機器の暗号化として一般によく搭載されている暗号化方式です。
暗号化方式は、RC4(Rivest's Cipher 4)アルゴリズムをベースに構成されています。
暗号化するデータのブロック長が8ビットで、暗号化鍵(キー)の長さを選択できます。
※選択できる暗号化鍵(キー)の長さは、64(40)/128(104)/152(128)ビットの中から選択できます。

◎OCB AES：WEP RC4より強力で、標準化が推進されている次世代の暗号化方式です。
暗号化するデータのブロック長と暗号化鍵(キー)の長さは、128ビットです。
この128ビットに対して任意に鍵(キー)を設定できますので、[WEP RC4]より強力な暗号化方式です。

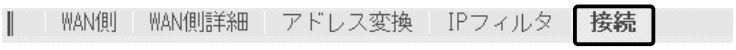
1 「WAN側設定」メニュー

1-5.「接続」画面
■暗号化設定(つづき)

②キージェネレータ …… 暗号化および復号に使う鍵(キー)を生成するための文字列を設定します。
通信を行う相手間で同じ文字列(大文字/小文字の区別に注意して、任意の半角英数字/記号)を31文字以内で設定します。
なお、入力した文字はすべて「＊(アスタリスク)」で表示します。
(表示例：＊＊)
「暗号化方式」を選択して、〈登録〉をクリックすると、[キージェネレータ]欄に入力した文字列より生成された鍵(キー)を[キー値]項目のテキストボックスに表示します。
[キー値]項目の各キー番号のテキストボックスに生成される桁数および文字数は、選択する「暗号化方式」によって異なります。(取扱説明書[導入編]☞4-2章 ■暗号化鍵(キー)値の入力についてを参照)
※「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。

③キーID …… 暗号化に使用する鍵(キー)番号を設定します。 (出荷時の設定：1)
鍵(キー)番号は、通信する相手間でそれぞれ任意に選択できます。
[暗号化設定]項目の[暗号化方式]欄で、「RC4」または「OCB AES」が登録されているときは、「1」～「4」の中から選択できます。

1-5.「接続」画面(つづき)



■ キー値

暗号化鍵(キー)を直接入力するための設定です。

① 入力モード ……　暗号化鍵(キー)の入力のしかたを選びます。
(出荷時の設定：16進数)
※入力モードを変更したときは、「接続」画面の〈登録〉ボタンをクリックしてから、暗号化鍵(キー)を入力してください。
※ASCII文字が設定されているときは、キージェネレータを使用できません。

② 鍵(キー)入力用ボックス …　キージェネレータを使用しないとき、暗号化および復号に使用する鍵(キー)を、[入力モード]欄で設定された方法で、直接入力します。(出荷時の設定：00-00-00-00-00)
16進数表記で使用する以外のアルファベットを入力しても無効です。
[キー値]は、通信する相手間で、使用するキーIDに対する鍵(キー)の内容を同じに設定してください。
使用するキーIDに対する鍵(キー)の内容が違うときは通信できません。

第2部

第2章 「ネットワーク設定」メニュー

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。

2 「ネットワーク設定」メニュー

2-1.「LAN側IP」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。

〈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」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」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、本製品とEthernetケーブルで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：SE-3000)

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。

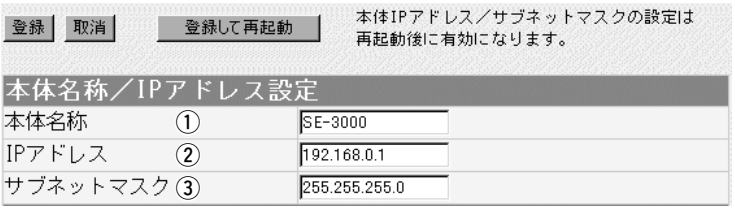
また、ほかのネットワーク機器と重複しないように、アルファベットで始まる半角英数字(A～Z、0～9、－)、31文字以内で設定します。

※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。

2-1.「LAN側IP」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]
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

2 「ネットワーク設定」メニュー

2-1.「LAN側IP」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	①	○しない ◉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	○しない ◉する
プライマリDNSサーバ	⑨	DNSの代理応答機能を使用する場合は無効となります。
セカンダリDNSサーバ	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。
本製品とEthernetケーブルで接続されたパソコンの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、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)

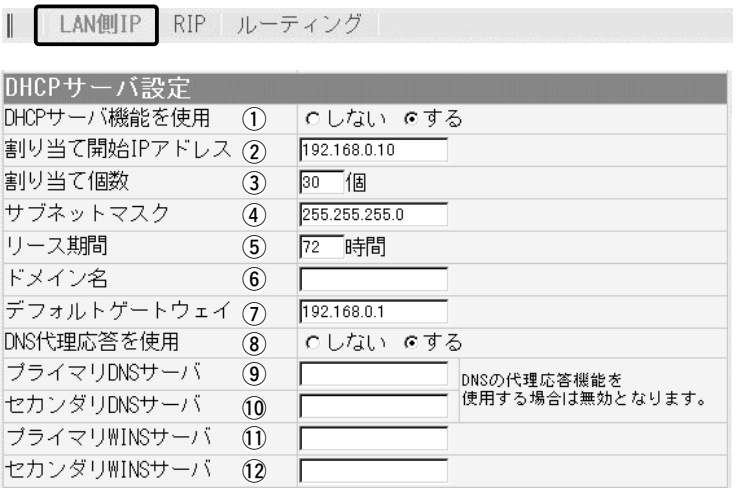
② 割り当て開始IPアドレス … 本製品とEthernetケーブルで接続されたパソコンへ、IPアドレスを自動で割り当てるときの開始アドレスを設定します。
(出荷時の設定：192.168.0.10)

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)

2-1.「LAN側IP」画面
■DHCPサーバ設定(つづき)



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サーバが本製品と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サーバの代理応答機能を使用する場合は無効になります。

2 「ネットワーク設定」メニュー

2-1.「LAN側IP」画面
■DHCPサーバ設定(つづき)

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」と同様に、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。

2-1.「LAN側IP」画面(つづき)

■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。

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。

【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。

2 「ネットワーク設定」メニュー

2-2.「RIP」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」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 …… 「RIP」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」画面で変更したすべての設定内容を有効にします。

①RIP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ローカル側RIP動作 …… ローカル側について、[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：受信のみ)

2-2.「RIP」画面
■RIP設定(つづき)

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、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](①)欄で「RIP」を設定する場合は、空白にします。

2 「ネットワーク設定」メニュー

2-3.「ルーティング」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。

IP経路情報

① 宛先	② サブネットマスク	③ ゲートウェイ	④ 経路	⑤ 作成	⑥ メトリック
0.0.0.0	0.0.0.0	0.0.0.0	01：WAN01	static	0
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。
◎ 01:WAN01：インターフェイスが「第1セッション」に設定された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「インターフェイス情報」画面にある[ネットワーク　インターフェイス　リスト]項目に表示します。

⑤ 作成 …… どのように経路情報が作成されたかを表示します。
◎static：スタティック(定義された)ルートにより作成
◎rip　　：ダイナミック(自動生成された)ルートにより作成
◎misc　：ブロードキャストに関係するフレーム処理で作成

⑥ メトリック …… [スタティックルーティング設定]項目の[メトリック]欄で設定された値やダイナミックルーティングで作成された経路のコストを表示します。

2-3.「ルーティング」画面(つづき)

■スタティックルーティング設定

パケットの中継経路を、意図的に定義するルーティングテーブルです。
登録できるのは、最大32件までです。

①経路 ……　回路の経路を指定します。
◎local　：登録する経路情報がLAN側の場合です。
◎01:WAN01：登録する経路情報が「第1セッション」に設定された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]項目に表示されます。

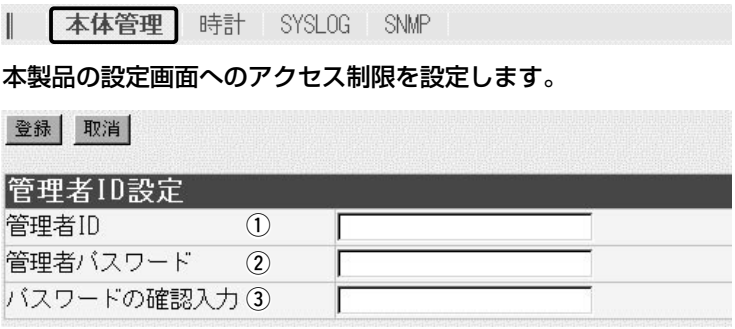
第2部

第3章 「システム設定」メニュー

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。

3 「システム設定」メニュー

3-1.「本体管理」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 …… 「本体管理」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 …… 「本体管理」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：se3000)
[管理者ID]を設定すると、次回のアクセスからユーザー名の入力を求められますので、そこに[管理者ID]を入力します。

② 管理者パスワード …… [管理者ID]に対するパスワードを設定する場合、大文字/小文字の区別に注意して、任意の英数字、半角31文字以内で入力します。
入力した文字は、すべて「＊(アスタリスク)」で表示されます。
(表示例：＊＊＊＊)
[管理者パスワード]を設定すると、次回のアクセスからパスワードの入力を求められますので、そこに[管理者パスワード]を入力します。

③ パスワードの確認入力 …… 確認のために、パスワードを再入力します。 (表示例：＊＊＊＊)

3-2.「時計」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 …… 「時計」画面で変更したすべての設定内容が有効になります。

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

① 本体の時刻 …… 本製品に設定されている時刻を表示します。

② 設定する時刻 …… 本製品の設定画面にアクセスしたとき、パソコンの時計設定を取得して表示します。
表示する時刻は、「時計」画面アクセス時に取得した時刻です。
※正確に設定したいときは、「時計」画面に再アクセスするかブラウザの〈更新〉ボタンをクリックしてから、〈登録〉をクリックしてください。

3 「システム設定」メニュー

3-2.「時計」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	○しない ◉する
NTPサーバ1　IPアドレス	②	133.100.9.2
NTPサーバ2　IPアドレス	③	
アクセス時間間隔	④	1 日
前回アクセス日時	⑤	----/--/-- --:--
次回アクセス日時	⑥	2003/01/02 00:00

①自動時計設定を使用 …… インターネット上に存在するタイムサーバに日時の問い合わせを行い、内部時計を自動設定します。　(出荷時の設定：する)

②NTP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)

③NTP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。
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。

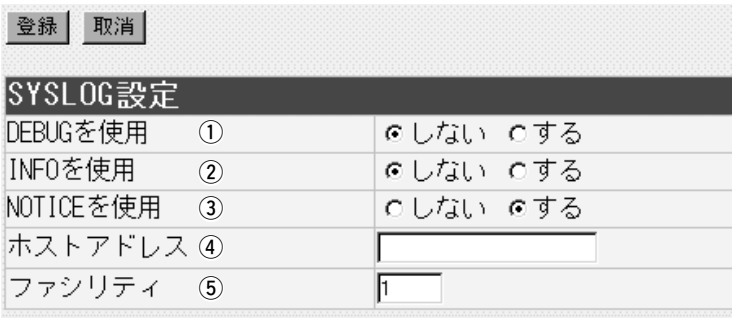
⑤前回アクセス日時 …… タイムサーバにアクセスした日時を表示します。

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。

3-3.「SYSLOG」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。



〈登録〉ボタン …… 「SYSLOG」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」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。

①DEBUG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)

②INFO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)

③NOTICE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。　(出荷時の設定：1)
設定できる範囲は、「0～23」です。
通常「1」を使用します。

3 「システム設定」メニュー

3-4.「SNMP」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」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」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。

①SNMP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。

第2部

第4章 「情報表示」メニュー

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。

4 「情報表示」メニュー

4-1.「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 クリア

日付・時間	通信記録
01/01 07:58:07	PPPoE01:サーバからの応答がありません
01/01 07:57:47	PPPoE01:PADI SENT
01/01 07:57:32	PPPoE01:PADI SENT
01/01 07:57:22	PPPoE01:PADI SENT

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 クリア

日付・時間	通信記録
12/11 11:36:17	TCP Syn Flooding: 172.20.252.210->172.20.101.51 TCP[6]:src=1784,dst=80
01/01 03:35:44	TCP Syn Flooding: 172.20.252.169->172.20.101.51 TCP[6]:src=2460,dst=80
01/01 03:34:00	DHCPC: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

4-2.「インターフェイス情報」画面

■ネットワーク インターフェイス リスト

本製品のインターフェイスに対する[IPアドレス]と[サブネットマスク]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	(取得中)	255.255.255.0

■ブリッジポート情報

本製品の各ポートごとに、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		
Ethernet	状況	通信中
	送信パケット数	141
	受信パケット数	146

Ethernet …… [有線LAN]ポートの通信状況と、そのときの送信と受信のパケット数を表示します。
※[有線LAN]ポートと[無線LAN]ポート間をルーティングしますので、[有線LAN]ポートの情報だけを表示します。

■無線通信状態

無線アクセスポイントとの通信状態を表示します。

無線通信状態		
SSID	①	manual
暗号化	②	無効
チャンネル	③	6CH (2437MHz)
信号レベル	④	45

①SSID …… 無線通信に使用する無線ネットワーク名(SSID)を表示します。

②暗号化 …… 無線通信に暗号化が設定されているかどうかを表示します。

③チャンネル …… 無線アクセスポイントとのチャンネルを表示します。

④信号レベル …… 無線アクセスポイントとの信号レベルを表示します。
表示される数値を通信の目安にしてください。

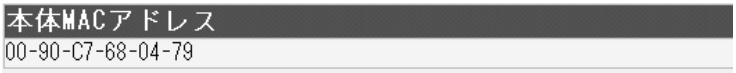
4 「情報表示」メニュー

4-2.「インターフェイス情報」画面(つづき)

■ 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、本製品の底面部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。



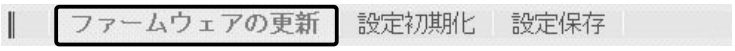
第2部

第5章 「メンテナンス」メニュー

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。

5 「メンテナンス」メニュー

5-1.「ファームウェアの更新」画面

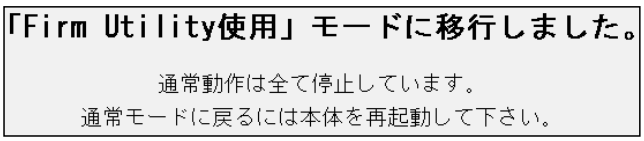


■「Firm Utility使用」モード

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

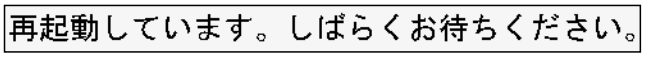
5-2.「設定初期化」画面

■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。

[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。

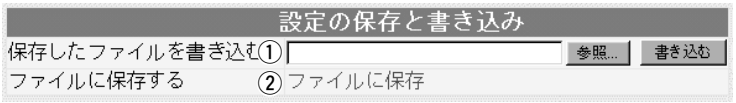
●次の画面を表示後、出荷時の状態になります。



5-3.「設定保存」画面

■設定の保存と書き込み

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。



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...〉ボタンをクリックすると表示される右の画面から目的の設定ファイルを指定します。

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。
※WWWブラウザの「ファイル(F)」メニューから、[名前を付けて保存(A)...]をクリックして保存した「設定保存」画面のファイル(拡張子：.htm/.html)とは互換性がありませんので保存したファイルとして読み込むことはできません。

②ファイルに保存する ……

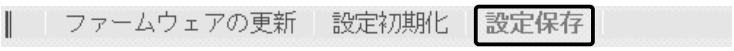
本製品すべての設定内容をパソコンに保存することで、本製品の設定をバックアップすることができます。

[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〉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。

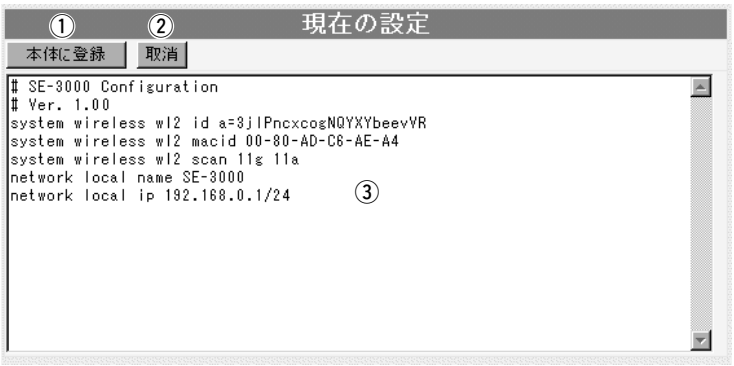
5 「メンテナンス」メニュー

5-3.「設定保存」画面(つづき)



■現在の設定

変更された設定内容の確認や設定ファイルをハイパーテキスト形式(.htm/.html)で保存、書き込みができます。



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。
※本製品のIPアドレスの設定が、「内容表示」部に表示されたIPアドレスと異なるときは、設定を本製品に登録できません。

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」部 …… 変更された設定内容を表示します。
この画面内容をパソコンに保存することで、本製品の設定をバックアップすることができます。
保存するときは、WWWブラウザの「ファイル(F)」メニューから、[名前を付けて保存(A)...]をクリックすると、保存できます。
※[設定の保存と書き込み]項目の「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)とは互換性がありませんので、読み込むことはできません。
※各画面で設定されたパスワードやキージェネレーター(無線LAN通信用暗号化鍵の生成元文字列)の内容は、暗号化されて表示されます。
そのため、保存されたファイルよりそれらが外部へ漏れることはありません。

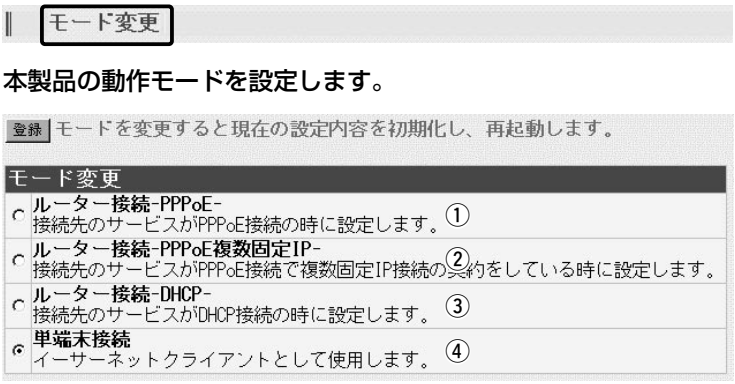
第2部

第6章 「モード変更」メニュー

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

6 「モード変更」メニュー

6-1.「モード変更」画面



■モード変更

本製品の動作モードを設定します。

〈登録〉ボタン …… ここで変更した内容を確定すると同時に、それ以外の画面で設定した内容は出荷時の状態に戻して再起動します。

① ルーター接続 –PPPoE– … 回線接続先に[PPPoE]方式で無線接続できるサービスを契約している場合、本製品からインターネット回線に無線で接続するとき使用するモードです。

※ご契約の接続先がマルチセッションに対応していれば、同じパソコンから通常の「PPPoE」接続先とは別の「PPPoE」接続先にも接続できます。
また、2台のパソコンのうち1台は通常の「PPPoE」接続先に接続、残りの1台は別の「PPPoE」接続先に接続できます。

② ルーター接続 –PPPoE 複数固定IP– …… 回線接続先が[PPPoE]方式で無線接続でき、複数のグローバル固定IPアドレスを提供するサービスを契約している場合、グローバルIPアドレスを固定で付与したパソコンから本製品を介してインターネット回線に無線で接続するとき使用するモードです。

※ご契約の回線接続業者、またはプロバイダーから割り当てられた複数のグローバル固定IPアドレスを本製品のEthernetケーブルに接続されたパソコン(LAN側)で利用できます。
また、プライベートアドレスが割り当てられたパソコンと混在した環境でご利用いただけます。

★ご契約の回線接続業者、またはプロバイダーから割り当てられた複数のグローバル固定IPアドレス(例：8個の場合)の使いかたについては、第5部(本書)の第2章を参考にしてください。

③ ルーター接続 –DHCP–…… 回線接続先に[DHCP]方式で無線接続できるサービスを契約している場合、本製品からインターネット回線に無線で接続するとき使用するモードです。

④ 単端末接続(出荷時の設定) Ethernetポート搭載のパソコンと接続することで、無線クライアントとして弊社製無線アクセスポイントと通信するとき使用するモードです。
このとき、本製品のEthernetケーブルに接続できるパソコンは、1台だけです。

第3部

「ルーター接続 –PPPoE複数固定IP–」モード編

本製品の動作モードを「ルーター接続 –PPPoE複数固定IP–」に設定したとき、表示されるメニューの各画面についての説明です。

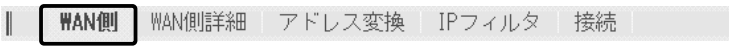
第3部

第1章 「WAN側設定」メニュー

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。

1 「WAN側設定」メニュー

1-1.「WAN側」画面



■接続状況

登録された回線への接続状況を表示します。

接続状況		
接続状況 接続	①	未接続
回線種別	②	PPPoE（自動接続）
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 接続状況 …… WAN側回線への接続状況を「未接続」/「接続中」で表示します。
本製品に登録した回線接続先に手動で接続および切断するときは、画面上の〈接続〉および〈切断〉ボタンをクリックします。
※〈切断〉ボタンは、回線を接続したとき表示されます。

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)」のいずれかを表示します。

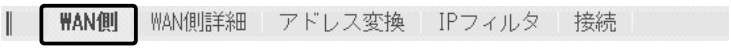
③ DNSサーバ …… ご契約されている回線接続業者、またはプロバイダーのDNSサーバIPアドレスを表示します。

④ 本体側のIPアドレス …… 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 …… 契約されている回線接続業者、またはプロバイダーのIPアドレスを表示します。

⑥ 接続時間 …… ご契約の回線接続業者、または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。

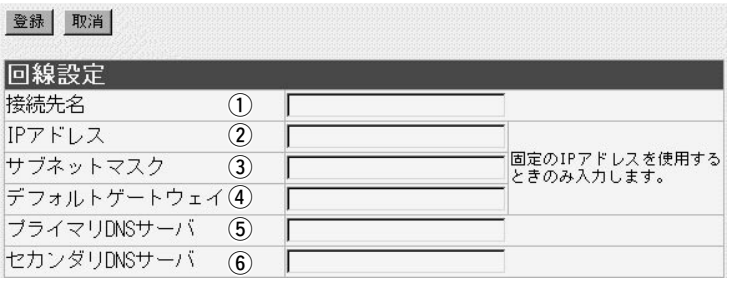
1-1.「WAN側」画面(つづき)



■ 回線設定

★ご契約の回線接続業者、またはプロバイダーから割り当てられた複数のグローバル固定IPアドレス(例：8個の場合)の使いかたについては、第5部(本書)の第2章を参考にしてください。

本製品のWAN側についての設定です。



〈登録〉ボタン …… [回線設定]項目と[接続設定]項目の内容を確定するボタンです。

〈取消〉ボタン …… [回線設定]項目および[接続設定]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 接続先名 …… ご契約の回線接続業者、またはプロバイダーがわかるような名前を、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 …… ご契約の回線接続業者、またはプロバイダー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。
※複数固定IPアドレスサービスをご契約の場合についても、指定された固定IPアドレスの中から、1つをこの欄に入力します。

③ サブネットマスク …… 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。
※複数固定IPアドレスサービスをご契約の場合についても、指定されたサブネットマスクをこの欄に入力します。

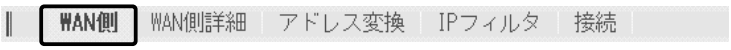
④ デフォルトゲートウェイ … ご契約の回線接続業者、またはプロバイダーから指定されたときに限り、本製品のデフォルトゲートウェイを入力します。

⑤ プライマリDNSサーバ …… ご契約の回線接続業者、またはプロバイダーから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 …… ご契約の回線接続業者、またはプロバイダーから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。

1 「WAN側設定」メニュー

1-1.「WAN側」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。

① ユーザID …… 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。

② パスワード …… 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 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、「相手先に合わせる」(出荷時の設定)でご使用ください。

1-2.「WAN側詳細」画面

■詳細設定

本製品のWAN側回線全般に機能する設定です。

ステルスモードを使用 ……　インターネットを使用して本製品に不正アクセスされた場合、Pingやポートスキャンに対して防御するかしないかの設定です。
(出荷時の設定：する)

■PPPoE詳細設定

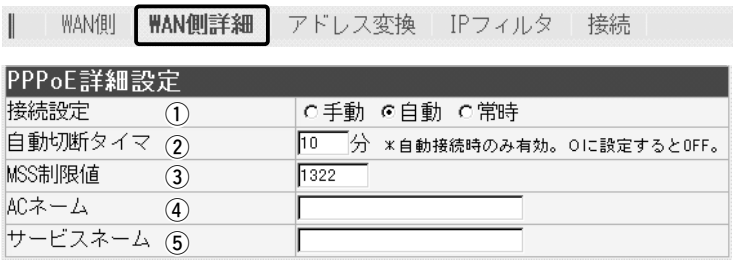
「PPPoE」接続についての詳細設定です。

① 接続設定 ……　「PPPoE」回線への接続方法を選択します。(出荷時の設定：自動)
◎手動：「WAN側」画面の〈接続〉/〈切断〉ボタンで、回線を強制的に接続/切断します。
◎自動：パソコンからホームページやメールを見る操作を行うだけで、自動的に接続します。
◎常時：常時接続します。
本製品で指定した接続先(WAN側)と常に接続状態を保持します。

② 自動切断タイマ ……　[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。

1 「WAN側設定」メニュー

1-2.「WAN側詳細」画面
■ PPPoE詳細設定(つづき)



③ MSS制限値 …… プロバイダーから指定されている場合に限り、WAN側回線への最大有効データ長を数字で指定します。　(出荷時の設定：1322)
設定できる範囲は、「536～1452」です。
MSS値とは、受信できる最大セグメント数のことです。
イーサネットパケットの最大長(MTU)は1500バイトと定められています。
これに対して、「PPPoE」や「フレッツ·ADSL」の最大データサイズは1322より小さい値となっていますが、現行のインターネットルータには、オーバーサイズのパケットを破棄するものがあります。よって、パケットの保護を優先するために小さめに設定しておく必要があります。
⚠警告
弊社では、MSS値を変更したことによって生じる結果については一切その責任を負いかねますので、あらかじめご了承ください。

④ ACネーム…… プロバイダーから指定されている場合に限り、指定の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。

1-2.「WAN側詳細」画面(つづき)

■ **UPnP設定**

①UPnPを使用 ……

UPnP(Universal Plug and Play)機能を使用するかしないかの設定です。　(出荷時の設定：しない)

UPnPを使用すると、NATトラバーサル対応のアプリケーションを、本製品に接続された有線パソコンから利用できます。

※使用時は、セキュリティーが低下しますので注意が必要です。

〈本製品のUPnP機能について〉

２００３年１月現在、下記のアプリケーションが本製品のUPnP(NATトラバーサル)機能に対応しています。

◎Windows Messenger (Version4.6以上)
　Windows XP専用アプリケーション

◎MSN Messenger (Version4.6以上)
　Windows 98/98SE/Me/2000専用アプリケーション

※MSN Messengerで音声チャットを行う場合は、「DirectX」のバージョン8.1以上が必要です。

※あらかじめIPフィルターを設定しているポートをMessengerで使用した場合は、UPnP機能が優先します。

※アプリケーションをバージョンアップする必要がある場合は、「Windows Update」などから行ってください。

②ポートマッピング有効期間

※ポートマッピング機能は、「複数固定IP接続」でグローバルIPアドレスを割り当てられたパソコンには機能しません。

UPnP(NATトラバーサル)対応アプリケーションなどを使用するために、WAN側に対してポートを開いている期間を日数で設定します。

最大9999日まで設定できます。　(出荷時の設定：2)

※「0」日を設定すると、アプリケーションを正しく終了しなかった場合など、本製品を再起動するまでポートが開いたままになりますのでご注意ください。

1 「WAN側設定」メニュー

1-2.「WAN側詳細」画面(つづき)

■ Messenger機能対応表

出荷時、UPnP機能は、「使用しない」に設定されています。

：UPnPが必要な機能を意味します。

○：対応　×：非対応

アプリケーション	機　能	UPnP機能を使用する	UPnP機能を使用しない(出荷時)
Windows Messenger ※Windows XP専用	サインイン	○	○
	メンバーの追加	○	○
	インスタントメッセージ	○	○
	音声チャット	○ (Version 4.6以上)	×
	ビデオチャット	○ (Version 4.6以上)	×
	アプリケーション共有	○ (Version 4.6以上)	×
	ホワイトボード	○ (Version 4.6以上)	×
	ファイル転送	×	×
	電話をかける	×	×
リモートアシスタンス ※Windows XP専用	デスクトップの制御	○ (Version 4.6.0082以上)	×
	音声会話	○ (Version 4.6.0082以上)	×
	ファイル転送	○ (Version 4.6.0082以上)	×
MSN Messenger ※Windows 98 Windows 98SE Windows Me Windows 2000	サインイン	○	○
	メンバーの追加	○	○
	インスタントメッセージ	○	○
	音声チャット	○ (Version 4.6以上、DirectX8.1以上)	×
	ファイル転送	×	×
NetMeeting	すべての機能	×	×

1-2.「WAN側詳細」画面(つづき)

■ Windows Messengerの制限について

〈制限〉

◎通信相手もUPnP対応ルーターを使用しているか、グローバルIPアドレスが割り当てられている必要があります。
◎Messengerでの音声チャットなどは、プロバイダーや接続業者から割り当てられるIPアドレスがプライベートIPアドレスの場合、使用できません。
◎静的マスカレードで使用しているポートが多い場合、Messengerの起動が遅かったり音声チャット等が利用できないことがあります。

〈再起動が必要な場合〉

下記のような原因でMessengerが使用できなくなったときは、Messengerを完全に終了してから再度起動してください。
◎Messengerを起動させた状態でポートマッピングの有効期間を経過したとき
◎Messenger起動後にNATおよび静的マスカレードの設定を変更したとき
◎パソコンがスリープ状態になったとき

1 「WAN側設定」メニュー

1-3.「アドレス変換」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」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」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)

②DMZホストIPアドレス … DMZホスト機能(非武装セグメント)を使用するホストの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、本製品とEthernetケーブルで接続されたパソコンでWWWサーバを運用したり、ネットワーク対戦ゲームなどが行えますが、セキュリティー上問題がありますのでご使用には十分注意してください。

③PPTPパススルーを使用 … 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。
(出荷時の設定：する)
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。

1-3.「アドレス変換」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。

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。

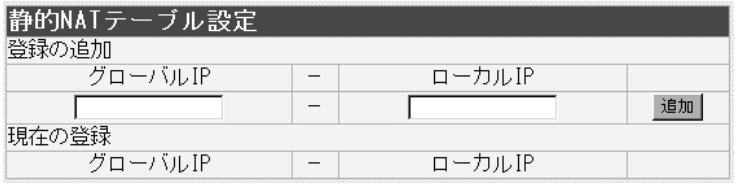
■DMZホスト機能と静的マスカレード機能の違い

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、セキュリティーが低下する。	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。

1 「WAN側設定」メニュー

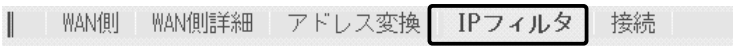
1-3.「アドレス変換」画面(つづき)

■ 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。**



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。

1-4.「IPフィルタ」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」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 ……　「不正アクセス検知機能設定」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。

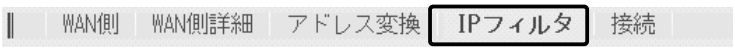
①不正アクセス検知機能を使用　不正アクセス検知機能を使用するかしないかを選択します。
(出荷時の設定：しない)
検知できる内容は以下の通りです。

◎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

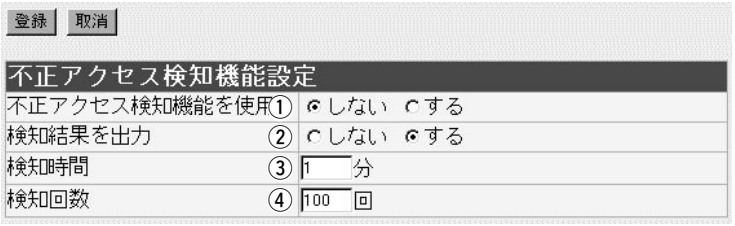
②検知結果を出力 ……　不正アクセスを検知したとき、検知結果を「情報表示」メニューの「通信記録」画面に表示するかしないかを選択します。
(出荷時の設定：する)
※このときの「通信記録」画面表示例は、第3部の4-1章をご覧ください。

1 「WAN側設定」メニュー

1-4.「IPフィルタ」画面



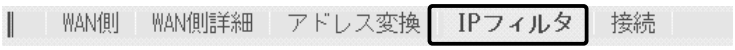
■ 不正アクセス検知機能設定(つづき)



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]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)

1-4.「IPフィルタ」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フィルターは、「複数固定IP接続」でグローバルIPアドレスを割り当てられたパソコンに対しても機能します。

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。

〈登録〉ボタン

この項目で新規作成、または編集した内容をフィルターとして[現在の登録]項目に登録するボタンです。
※フィルター条件は、1つ以上指定してください。

② フィルタ方向 ……

パケットの通信方向で、WAN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。

1 「WAN側設定」メニュー

1-4.「IPフィルタ」画面
■IPフィルタ設定(つづき)

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。

1-4.「IPフィルタ」画面
■IPフィルタ設定(つづき)

⑤ 発信元ポート番号 ……

フィルタリングの対象となる発信元のTCP/UDPポート番号を指定する項目です。数字で指定するときは、「指定」を選択して、番号を始点から終点まで連続で入力します。
入力できる範囲は、10進数で「1～65535」までの半角数字です。
また、特定のポートだけを指定するときは、始点だけ、または始点/終点に同一の番号を入力してください。
数字で指定しない場合は、ニーモニック(DNS、Finger、FTP、Gopher、NEWS、POP3、SMTP、Telnet、Web、Whois)から選択します。

⑥ 宛先ポート番号 ……

フィルタリングの対象となる宛先のTCP/UDPポート番号を指定する項目です。
数字で指定するときは、「指定」を選択して、番号を始点から終点まで連続で入力します。
入力できる範囲は、10進数で「1～65535」までの半角数字です。
また、特定のポートだけを指定するときは、始点だけ、または始点/終点に同一の番号を入力してください。
数字で指定しない場合は、ニーモニック(DNS、Finger、FTP、Gopher、NEWS、POP3、SMTP、Telnet、Web、Whois)から選択します。

⑦ 発信元IPアドレス ……

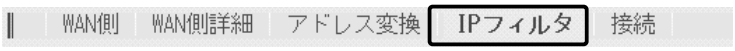
発信元ホストのIPアドレスを設定することにより、特定のホストからのパケットをフィルタリングします。
何も入力しない場合は、すべてのアドレスを対象とします。
発信元ホストのIPアドレスを始点から終点まで連続で入力します。
また、特定の発信元ホストだけを指定するときは、始点だけ入力してください。

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。

1 「WAN側設定」メニュー

1-4.「IPフィルタ」画面(つづき)



■現在の登録

現在の登録

		番号	方向	方法	プロトコル	発信元ポート番号	宛先ポート番号	発信元IPアドレス	宛先IPアドレス
編集	削除	57	WAN側から	透過	TCP	20	*	*	*
編集	削除	58	WAN側から	遮断	TCP_EST	*	*	*	*
編集	削除	59	両方	遮断	ALL	135	*	*	*
編集	削除	60	両方	遮断	ALL	*	135	*	*
編集	削除	61	両方	遮断	ALL	445	*	*	*
編集	削除	62	両方	遮断	ALL	*	445	*	*
編集	削除	63	両方	遮断	TCP	*	137 - 139	*	*
編集	削除	64	両方	遮断	UDP	137 - 139	137 - 139	*	*

現在登録されているIPフィルターを表示します。

【出荷時、登録されているフィルターについて】

◎57番　　：FTPをデフォルトで通過させる
◎58番　　：WAN側からの不正アクセス防止
◎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

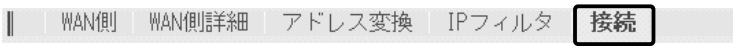
〈編集〉ボタン

〈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。

1-5.「接続」画面



■ 無線LAN設定

本製品の無線通信に対する基本設定です。

〈登録〉ボタン ……

「接続」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 ……

「接続」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、「接続」画面で変更したすべての設定内容を有効にします。

①SSID ……

本製品と無線アクセスポイントには、通信相手をグループとして識別するための無線ネットワーク名として、SSIDが設定されています。　(出荷時の設定：LG〈半角〉)
同じグループで通信するお互いの無線LAN機器で、この[SSID]が異なると通信できません。
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。
※[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。

1 「WAN側設定」メニュー

1-5.「接続」画面
■無線LAN設定(つづき)

② スキャンモード ……

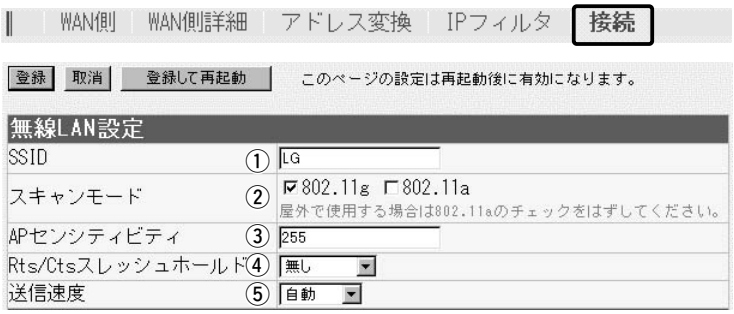
本製品で使用する無線LAN規格(802.11a/802.11g)を設定します。
[802.11a]と[802.11g(802.11bを含む)]を同時に設定できます。 (出荷時の設定：802.11g)
[802.11a]と[802.11g]を同時に設定し、[送信速度]欄を「自動」に設定して使用する場合、[802.11a/b/g]が混在する環境では、通信環境の良い無線アクセスポイントに接続されます。

★屋外で使用する場合は、必ず[802.11a]のチェックボックスにチェックマークを入れないでください。

③ APセンシティビティ ……

無線アクセスポイントからの電波が途切れたとき、スキャンを開始するまでの間隔を設定します。
無線アクセスポイントの設置環境やネットワーク状況の影響でローミング動作がスムーズに行えないとき、この設定を変更すると通信状況が改善されます。
設定できる範囲は「10～255」です。 (出荷時の設定：255)
小さい数値を設定するほど、電波が途切れてからスキャンを開始するまでの間隔が短く、大きい数値を設定するほど、電波が途切れてからスキャンを開始するまでの間隔が長くなります。

1-5.「接続」画面
■ 無線LAN設定(つづき)



④ Rts/Ctsスレッシュホールド ……

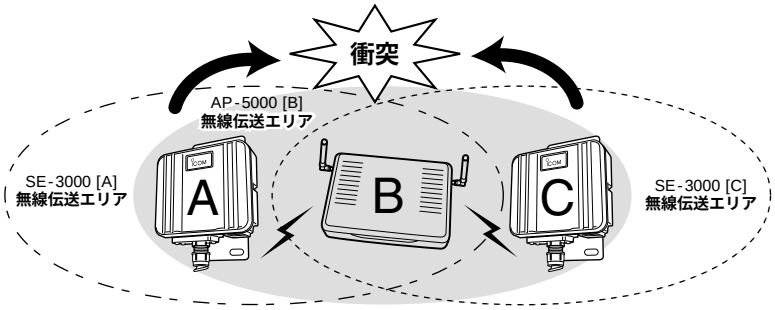
ネゴシエーションするために送るパケットのデータサイズを、「500バイト」または「1000バイト」から選択します。

(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、それぞれが無線アクセスポイント[B]と無線通信できても、互いが直接通信できない本製品[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、本製品[A]から送信要求(Rts)信号を受信した無線アクセスポイント[B]が、無線伝送エリア内にある本製品[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本製品[C]に無線アクセスポイント[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本製品[C]は、無線アクセスポイント[B]から受信完了通知(ACK)を受信するまで無線アクセスポイント[B]へのアクセスを自制することで、通信の衝突を防止できます。



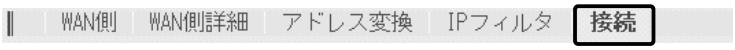
1 「WAN側設定」メニュー

1-5.「接続」画面
■無線LAN設定(つづき)

⑤ 送信速度 ……

「自動」を設定すると、環境の変化などで通信が不安定になっても、[スキャンモード]欄で設定した方式で通信が続行可能な速度に自動で切り替わります。 (出荷時の設定：自動)
[スキャンモード]欄で設定したモードによって、対応できる[送信速度]が異なります。
対応できない送信速度を設定した場合は、「自動」で動作します。
◎「802.11g」および「802.11a」を設定時、「自動」以外を設定したとき対応できる速度は、「54/48/36/24/18/12/9/6」Mbpsです。
◎「802.11b」設定時、「自動」以外を設定したとき対応できる速度は、「11/5.5/2/1」Mbpsです。
※[スキャンモード]を「802.11a」に設定し、[送信速度]を「11/5.5/2/1」Mbpsのいずれかに設定したときは、送信速度の設定が「802.11a」に該当しないため、[送信速度]は「自動」で動作します。
※[802.11b]専用の無線アクセスポイントと通信する場合は、下の欄で「自動(出荷時の設定)/11/5.5/2/1」Mbpsのいずれかに設定すると使用できます。

1-5.「接続」画面(つづき)



■暗号化設定

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

① 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)
暗号化方式には、「RC4」、「OCB AES」があります。
通信を行う相手間で、ビット数も含め同じ方式を選択してください。

◎WEP RC4：無線LAN機器の暗号化として一般によく搭載されている暗号化方式です。
暗号化方式は、RC4(Rivest's Cipher 4)アルゴリズムをベースに構成されています。
暗号化するデータのブロック長が8ビットで、暗号化鍵(キー)の長さを選択できます。
※選択できる暗号化鍵(キー)の長さは、64(40)/128(104)/152(128)ビットの中から選択できます。

◎OCB AES：WEP RC4より強力で、標準化が推進されている次世代の暗号化方式です。
暗号化するデータのブロック長と暗号化鍵(キー)の長さは、128ビットです。
この128ビットに対して任意に鍵(キー)を設定できますので、[WEP RC4]より強力な暗号化方式です。

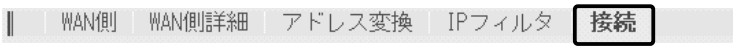
1 「WAN側設定」メニュー

1-5.「接続」画面
■暗号化設定(つづき)

②キージェネレータ …… 暗号化および復号に使う鍵(キー)を生成するための文字列を設定します。
通信を行う相手間で同じ文字列(大文字/小文字の区別に注意して、任意の半角英数字/記号)を31文字以内で設定します。
なお、入力した文字はすべて「＊(アスタリスク)」で表示します。
(表示例：＊＊)
「暗号化方式」を選択して、〈登録〉をクリックすると、[キージェネレータ]欄に入力した文字列より生成された鍵(キー)を[キー値]項目のテキストボックスに表示します。
[キー値]項目の各キー番号のテキストボックスに生成される桁数および文字数は、選択する「暗号化方式」によって異なります。(取扱説明書[導入編]☞4-2章 ■暗号化鍵(キー)値の入力についてを参照)
※「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。

③キーID …… 暗号化に使用する鍵(キー)番号を設定します。 (出荷時の設定：1)
鍵(キー)番号は、通信する相手間でそれぞれ任意に選択できます。
[暗号化設定]項目の[暗号化方式]欄で、「RC4」または「OCB AES」が登録されているときは、「1」～「4」の中から選択できます。

1-5.「接続」画面(つづき)



■ キー値

暗号化鍵(キー)を直接入力するための設定です。

① 入力モード ……　暗号化鍵(キー)の入力のしかたを選びます。
(出荷時の設定：16進数)
※入力モードを変更したときは、「接続」画面の〈登録〉ボタンをクリックしてから、暗号化鍵(キー)を入力してください。
※ASCII文字が設定されているときは、キージェネレータを使用できません。

② 鍵(キー)入力用ボックス …　キージェネレータを使用しないとき、暗号化および復号に使用する鍵(キー)を、[入力モード]欄で設定された方法で、直接入力します。(出荷時の設定：00-00-00-00-00)
16進数表記で使用する以外のアルファベットを入力しても無効です。
[キー値]は、通信する相手間で、使用するキーIDに対する鍵(キー)の内容を同じに設定してください。
使用するキーIDに対する鍵(キー)の内容が違うときは通信できません。

第3部

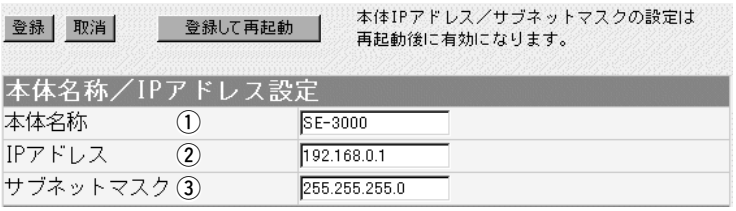
第2章 「ネットワーク設定」メニュー

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。

2 「ネットワーク設定」メニュー

2-1.「LAN側IP」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。**



〈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」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」画面で変更したすべての設定内容が有効になります。

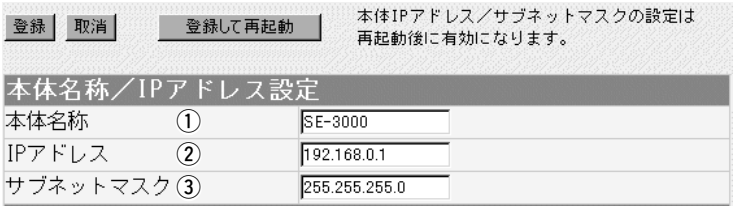
①本体名称 …… ネットワーク上で、本製品を識別する名前です。
設定した名前は、本製品とEthernetケーブルで接続されたパソコンから、本製品に直接アクセスするためのドメイン名の一部として使えます。　(出荷時の設定：SE-3000)

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。

2-1.「LAN側IP」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]
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

2 「ネットワーク設定」メニュー

2-1.「LAN側IP」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。

※NAT/IPマスカレード機能は、「複数固定IP接続」でグローバルIPアドレスを割り当てられたパソコンには機能しません。

DHCPサーバ設定		
DHCPサーバ機能を使用	①	○しない ◉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	○しない ◉する
プライマリDNSサーバ	⑨	DNSの代理応答機能を使用する場合は無効となります。
セカンダリDNSサーバ	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。
本製品とEthernetケーブルで接続されたパソコンの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、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 … 本製品とEthernetケーブルで接続されたパソコンへ、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)

2-1.「LAN側IP」画面
■DHCPサーバ設定(つづき)

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サーバが本製品と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サーバの代理応答機能を使用する場合は無効になります。

2 「ネットワーク設定」メニュー

2-1.「LAN側IP」画面
■DHCPサーバ設定(つづき)

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」と同様に、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。

2-1.「LAN側IP」画面(つづき)

■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。

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。
【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。

2 「ネットワーク設定」メニュー

2-2.「RIP」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」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 …… 「RIP」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」画面で変更したすべての設定内容を有効にします。

①RIP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ローカル側RIP動作 …… ローカル側について、[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：受信のみ)

2-2.「RIP」画面
■RIP設定(つづき)

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、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](①)欄で「RIP」を設定する場合は、空白にします。

2 「ネットワーク設定」メニュー

2-3.「ルーティング」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。

IP経路情報

① 宛先	② サブネットマスク	③ ゲートウェイ	④ 経路	⑤ 作成	⑥ メトリック
0.0.0.0	0.0.0.0	0.0.0.0	01：WAN01	static	0
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。
◎ 01:WAN01：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「インターフェイス情報」画面にある[ネットワーク　インターフェイス　リスト]項目に表示します。

⑤ 作成 …… どのように経路情報が作成されたかを表示します。
◎static：スタティック(定義された)ルートにより作成
◎rip　　：ダイナミック(自動生成された)ルートにより作成
◎misc　：ブロードキャストに関係するフレーム処理で作成

⑥ メトリック …… [スタティックルーティング設定]項目の[メトリック]欄で設定された値やダイナミックルーティングで作成された経路のコストを表示します。

2-3.「ルーティング」画面(つづき)

■スタティックルーティング設定

パケットの中継経路を、意図的に定義するルーティングテーブルです。
登録できるのは、最大32件までです。

①経路 ……　回路の経路を指定します。
◎local　　：登録する経路情報がLAN側の場合です。
◎01:WAN01：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]項目に表示されます。

第3部

第3章 「システム設定」メニュー

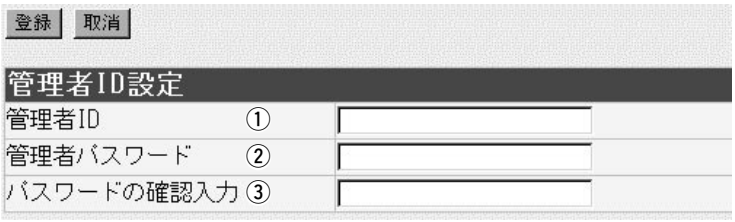
この章では、
「システム設定」メニューで表示される設定画面について説明します。

3 「システム設定」メニュー

3-1.「本体管理」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 …… 「本体管理」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 …… 「本体管理」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：se3000)
[管理者ID]を設定すると、次回のアクセスからユーザー名の入力を求められますので、そこに[管理者ID]を入力します。

② 管理者パスワード …… [管理者ID]に対するパスワードを設定する場合、大文字/小文字の区別に注意して、任意の英数字、半角31文字以内で入力します。
入力した文字は、すべて「＊(アスタリスク)」で表示されます。
(表示例：＊＊＊＊)
[管理者パスワード]を設定すると、次回のアクセスからパスワードの入力を求められますので、そこに[管理者パスワード]を入力します。

③ パスワードの確認入力 …… 確認のために、パスワードを再入力します。 (表示例：＊＊＊＊)

3-2.「時計」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 …… 「時計」画面で変更したすべての設定内容が有効になります。

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

① 本体の時刻 …… 本製品に設定されている時刻を表示します。

② 設定する時刻 …… 本製品の設定画面にアクセスしたとき、パソコンの時計設定を取得して表示します。
表示する時刻は、「時計」画面アクセス時に取得した時刻です。
※正確に設定したいときは、「時計」画面に再アクセスするかブラウザの〈更新〉ボタンをクリックしてから、〈登録〉をクリックしてください。

3 「システム設定」メニュー

3-2.「時計」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	○しない ◉する
NTPサーバ1　IPアドレス	②	133.100.9.2
NTPサーバ2　IPアドレス	③	
アクセス時間間隔	④	1 日
前回アクセス日時	⑤	----/--/-- --:--
次回アクセス日時	⑥	2003/01/02 00:00

①自動時計設定を使用 …… インターネット上に存在するタイムサーバに日時の問い合わせを行い、内部時計を自動設定します。　(出荷時の設定：する)

②NTP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)

③NTP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。
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。

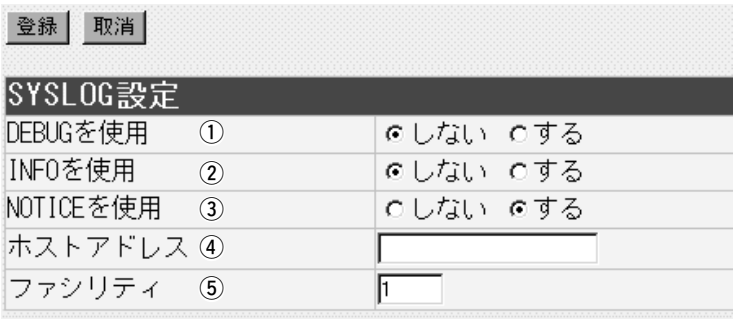
⑤前回アクセス日時 …… タイムサーバにアクセスした日時を表示します。

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。

3-3.「SYSLOG」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。



〈登録〉ボタン …… 「SYSLOG」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」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。

①DEBUG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)

②INFO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)

③NOTICE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。　(出荷時の設定：1)
設定できる範囲は、「0～23」です。
通常「1」を使用します。

3 「システム設定」メニュー

3-4.「SNMP」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」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」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。

①SNMP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。

第3部

第4章 「情報表示」メニュー

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。

4 「情報表示」メニュー

4-1.「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 クリア

日付・時間	通信記録
01/01 07:58:07	PPPoE01:サーバからの応答がありません
01/01 07:57:47	PPPoE01:PADI SENT
01/01 07:57:32	PPPoE01:PADI SENT
01/01 07:57:22	PPPoE01:PADI SENT

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 クリア

日付・時間	通信記録
12/11 11:36:17	TCP Syn Flooding: 172.20.252.210->172.20.101.51 TCP[6]:src=1784,dst=80
01/01 03:35:44	TCP Syn Flooding: 172.20.252.169->172.20.101.51 TCP[6]:src=2460,dst=80
01/01 03:34:00	DHCPC: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

4-2.「インターフェイス情報」画面

■ネットワーク インターフェイス リスト

本製品のインターフェイスに対する[IPアドレス]と[サブネットマスク]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	(取得中)	255.255.255.0

■ブリッジポート情報

本製品の各ポートごとに、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		
Ethernet	状況	通信中
	送信パケット数	141
	受信パケット数	146

Ethernet …… [有線LAN]ポートの通信状況と、そのときの送信と受信のパケット数を表示します。
※[有線LAN]ポートと[無線LAN]ポート間をルーティングしますので、[有線LAN]ポートの情報だけを表示します。

■無線通信状態

無線アクセスポイントとの通信状態を表示します。

無線通信状態		
SSID	①	manual
暗号化	②	無効
チャンネル	③	6CH (2437MHz)
信号レベル	④	45

①SSID …… 無線通信に使用する無線ネットワーク名(SSID)を表示します。

②暗号化 …… 無線通信に暗号化が設定されているかどうかを表示します。

③チャンネル …… 無線アクセスポイントとのチャンネルを表示します。

④信号レベル …… 無線アクセスポイントとの信号レベルを表示します。
表示される数値を通信の目安にしてください。

4 「情報表示」メニュー

4-2.「インターフェイス情報」画面(つづき)

■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、本製品の底面部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。

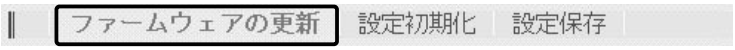
第3部

第5章 「メンテナンス」メニュー

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。

5 「メンテナンス」メニュー

5-1.「ファームウェアの更新」画面

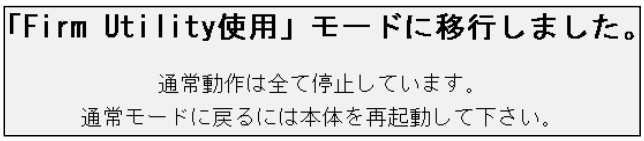


■「Firm Utility使用」モード

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

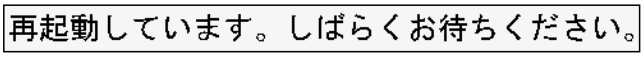
5-2.「設定初期化」画面

■設定初期化

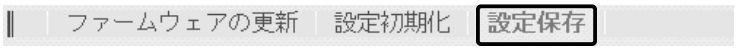
本製品の設定内容をすべて出荷時の状態に戻します。

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。

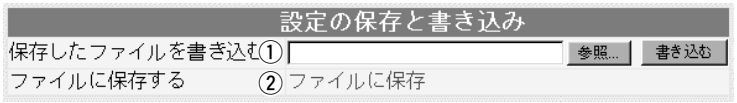


5-3.「設定保存」画面



■設定の保存と書き込み

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。



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。

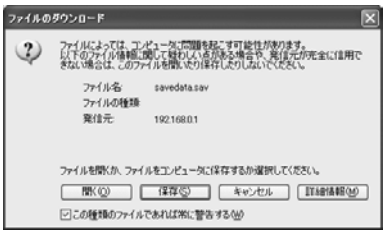
設定ファイルの保存先をテキストボックスに直接入力するか、〈参照...〉ボタンをクリックすると表示される右の画面から目的の設定ファイルを指定します。

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。
※WWWブラウザの「ファイル(F)」メニューから、[名前を付けて保存(A)...]をクリックして保存した「設定保存」画面のファイル(拡張子：.htm/.html)とは互換性がありませんので保存したファイルとして読み込むことはできません。

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。

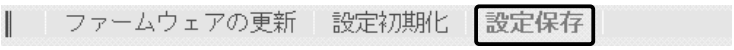
[設定の保存と書き込み]項目で[ファイルに保存]をクリックすると表示される右の画面から〈保存〉をクリックすると、設定ファイルを保存できます。



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。

5 「メンテナンス」メニュー

5-3.「設定保存」画面(つづき)



■現在の設定

変更された設定内容の確認や設定ファイルをハイパーテキスト形式(.htm/.html)で保存、書き込みができます。

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。
※本製品のIPアドレスの設定が、「内容表示」部に表示されたIPアドレスと異なるときは、設定を本製品に登録できません。

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」部 …… 変更された設定内容を表示します。
この画面内容をパソコンに保存することで、本製品の設定をバックアップすることができます。
保存するときは、WWWブラウザの「ファイル(F)」メニューから、[名前を付けて保存(A)...]をクリックすると、保存できます。
※[設定の保存と書き込み]項目の「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)とは互換性がありませんので、読み込むことはできません。
※各画面で設定されたパスワードやキージェネレーター(無線LAN通信用暗号化鍵の生成元文字列)の内容は、暗号化されて表示されます。
そのため、保存されたファイルよりそれらが外部へ漏れることはありません。

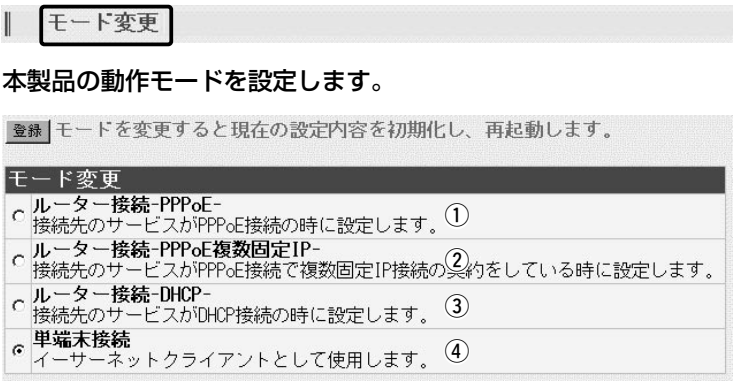
第3部

第6章 「モード変更」メニュー

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

6 「モード変更」メニュー

6-1.「モード変更」画面



■ モード変更

本製品の動作モードを設定します。

〈登録〉ボタン …… ここで変更した内容を確定すると同時に、それ以外の画面で設定した内容は出荷時の状態に戻して再起動します。

① ルーター接続 –PPPoE– … 回線接続先に[PPPoE]方式で無線接続できるサービスを契約している場合、本製品からインターネット回線に無線で接続するとき使用するモードです。

※ご契約の接続先がマルチセッションに対応していれば、同じパソコンから通常の「PPPoE」接続先とは別の「PPPoE」接続先にも接続できます。
また、2台のパソコンのうち1台は通常の「PPPoE」接続先に接続、残りの1台は別の「PPPoE」接続先に接続できます。

② ルーター接続 –PPPoE 複数固定IP– …… 回線接続先が[PPPoE]方式で無線接続でき、複数のグローバル固定IPアドレスを提供するサービスを契約している場合、グローバルIPアドレスを固定で付与したパソコンから本製品を介してインターネット回線に無線で接続するとき使用するモードです。

※ご契約の回線接続業者、またはプロバイダーから割り当てられた複数のグローバル固定IPアドレスを本製品のEthernetケーブルに接続されたパソコン(LAN側)で利用できます。
また、プライベートアドレスが割り当てられたパソコンと混在した環境でご利用いただけます。

★ご契約の回線接続業者、またはプロバイダーから割り当てられた複数のグローバル固定IPアドレス(例：8個の場合)の使いかたについては、第5部(本書)の第2章を参考にしてください。

③ ルーター接続 –DHCP–…… 回線接続先に[DHCP]方式で無線接続できるサービスを契約している場合、本製品からインターネット回線に無線で接続するとき使用するモードです。

④ 単端末接続(出荷時の設定) Ethernetポート搭載のパソコンと接続することで、無線クライアントとして弊社製無線アクセスポイントと通信するとき使用するモードです。
このとき、本製品のEthernetケーブルに接続できるパソコンは、1台だけです。

第4部

「ルーター接続 –DHCP–」モード編

本製品の動作モードを「ルーター接続 –DHCP–」に設定したとき、表示されるメニューの各画面についての説明です。

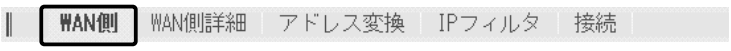
第4部

第1章 「WAN側設定」メニュー

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。

1 「WAN側設定」メニュー

1-1.「WAN側」画面



■接続状況

登録された回線への接続状況を表示します。

接続状況		
接続状況 切断	①	接続中
回線種別	②	DHCP
DNSサーバ	③	-
本体側のIPアドレス	④	-
相手先のIPアドレス	⑤	-
接続時間	⑥	- 時間 - 分 - 秒

① 接続状況 …… WAN側回線への接続状況を「未接続」/「接続中」で表示します。
本製品に登録した回線接続先に手動で接続および切断するときは、画面上の〈接続〉および〈切断〉ボタンをクリックします。
※〈接続〉ボタンは、回線を切断したとき表示されます。

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(DHCP)を表示します。

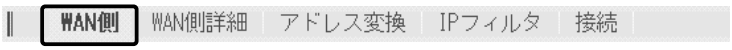
③ DNSサーバ …… ご契約されている回線接続業者、またはプロバイダーのDNSサーバIPアドレスを表示します。

④ 本体側のIPアドレス …… 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 …… 契約されている回線接続業者、またはプロバイダーのIPアドレスを表示します。

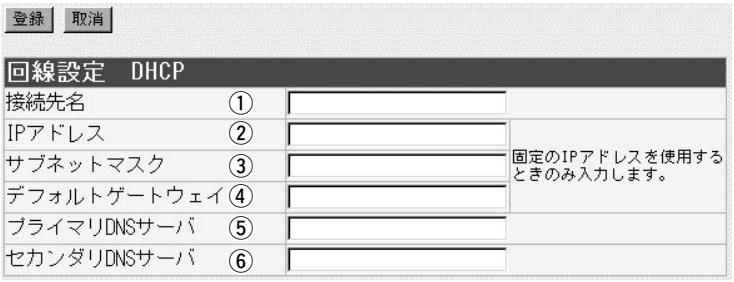
⑥ 接続時間 …… ご契約の回線接続業者、またはプロバイダーに接続してから、この画面にアクセスした時点までの時間を表示します。
最新の接続時間を表示させるときは、WWWブラウザの〈更新〉をクリックします。

1-1.「WAN側」画面(つづき)



■ 回線設定 DHCP

本製品のWAN側についての設定です。



〈登録〉ボタン …… [回線設定]項目の内容を確定するボタンです。

〈取消〉ボタン …… [回線設定]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 接続先名 …… ご契約の回線接続業者、またはプロバイダーがわかるような名前を、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 …… ご契約の回線接続業者、またはプロバイダー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 …… ご契約の回線接続業者、またはプロバイダー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 … ご契約の回線接続業者、またはプロバイダー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…… ご契約の回線接続業者、またはプロバイダーから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…… ご契約の回線接続業者、またはプロバイダーから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。

1 「WAN側設定」メニュー

1-2.「WAN側詳細」画面

■詳細設定

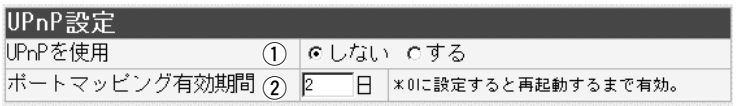
本製品のWAN側回線全般に機能する設定です。

ステルスモードを使用 ……

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

(出荷時の設定：する)

■UPnP設定



①UPnPを使用 ……

UPnP(Universal Plug and Play)機能を使用するかしないかの設定です。 (出荷時の設定：しない)

UPnPを使用すると、NATトラバーサル対応のアプリケーションを、本製品に接続された有線パソコンから利用できます。

※使用時は、セキュリティーが低下しますので注意が必要です。

〈本製品のUPnP機能について〉

２００３年１月現在、下記のアプリケーションが本製品のUPnP(NATトラバーサル)機能に対応しています。

◎Windows Messenger (Version4.6以上)
　Windows XP専用アプリケーション

◎MSN Messenger (Version4.6以上)
　Windows 98/98SE/Me/2000専用アプリケーション

※MSN Messengerで音声チャットを行う場合は、「DirectX」のバージョン8.1以上が必要です。

※あらかじめIPフィルターを設定しているポートをMessengerで使用した場合は、UPnP機能が優先します。

※アプリケーションをバージョンアップする必要がある場合は、「Windows Update」などから行ってください。

②ポートマッピング有効期間

UPnP(NATトラバーサル)対応アプリケーションなどを使用するために、WAN側に対してポートを開いている期間を日数で設定します。

最大9999日まで設定できます。 (出荷時の設定：2)

※「0」日を設定すると、アプリケーションを正しく終了しなかった場合など、本製品を再起動するまでポートが開いたままになりますのでご注意ください。

1-2.「WAN側詳細」画面(つづき)

■ Messenger機能対応表

出荷時、UPnP機能は、「使用しない」に設定されています。

：UPnPが必要な機能を意味します。

○：対応　×：非対応

アプリケーション	機　能	UPnP機能を使用する	UPnP機能を使用しない(出荷時)
Windows Messenger ※Windows XP専用	サインイン	○	○
	メンバーの追加	○	○
	インスタントメッセージ	○	○
	音声チャット	○ (Version 4.6以上)	×
	ビデオチャット	○ (Version 4.6以上)	×
	アプリケーション共有	○ (Version 4.6以上)	×
	ホワイトボード	○ (Version 4.6以上)	×
	ファイル転送	×	×
	電話をかける	×	×
リモートアシスタンス ※Windows XP専用	デスクトップの制御	○ (Version 4.6.0082以上)	×
	音声会話	○ (Version 4.6.0082以上)	×
	ファイル転送	○ (Version 4.6.0082以上)	×
MSN Messenger ※Windows 98 Windows 98SE Windows Me Windows 2000	サインイン	○	○
	メンバーの追加	○	○
	インスタントメッセージ	○	○
	音声チャット	○ (Version 4.6以上、DirectX8.1以上)	×
	ファイル転送	×	×
NetMeeting	すべての機能	×	×

1 「WAN側設定」メニュー

1-2.「WAN側詳細」画面(つづき)

■ Windows Messengerの制限について

〈制限〉

◎通信相手もUPnP対応ルーターを使用しているか、グローバルIPアドレスが割り当てられている必要があります。
◎Messengerでの音声チャットなどは、プロバイダーや接続業者から割り当てられるIPアドレスがプライベートIPアドレスの場合、使用できません。
◎静的マスカレードで使用しているポートが多い場合、Messengerの起動が遅かったり音声チャット等が利用できないことがあります。

〈再起動が必要な場合〉

下記のような原因でMessengerが使用できなくなったときは、Messengerを完全に終了してから再度起動してください。
◎Messengerを起動させた状態でポートマッピングの有効期間を経過したとき
◎Messenger起動後にNATおよび静的マスカレードの設定を変更したとき
◎パソコンがスリープ状態になったとき

1-3.「アドレス変換」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」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」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)

②DMZホストIPアドレス … DMZホスト機能(非武装セグメント)を使用するホストの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、本製品とEthernetケーブルで接続されたパソコンでWWWサーバを運用したり、ネットワーク対戦ゲームなどが行えますが、セキュリティー上問題がありますのでご使用には十分注意してください。

③PPTPパススルーを使用 … 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。
(出荷時の設定：する)
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。

1 「WAN側設定」メニュー

1-3.「アドレス変換」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。

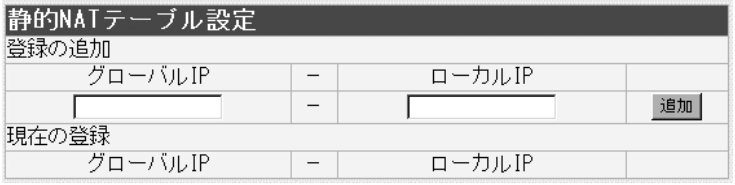
マスカレードIP(ルータグローバルIP)に対して、アクセスしてきたパケットをプロトコルにより判定し、ここで指定したプライベートIPアドレスを割り当てたローカル端末へアドレス変換します。
最大32個のマスカレードテーブルを設定できます。
◎ローカルIP：プライベートIPアドレスを入力します。
◎プロトコル：TCP、UDP、TCP/UDP、GREから選択します。
◎ポート　　：選択したプロトコルに対するポートを数字で指定するときは、「指定」を選択します。
数字で指定しない場合は、ニーモニック(DNS、Finger、FTP、Gopher、NEWS、POP3、SMTP、Telnet、Web、Whois)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、セキュリティーが低下する。	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。

1-3.「アドレス変換」画面(つづき)

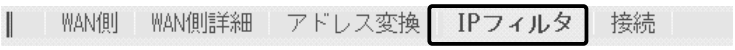
■静的NATテーブル設定　　**グローバルとプライベートのIPアドレス変換を行う設定です。**



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。

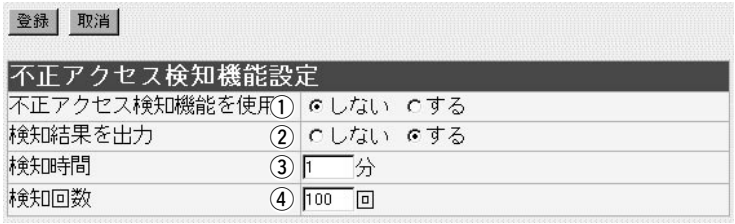
1 「WAN側設定」メニュー

1-4.「IPフィルタ」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」項目で変更したすべての設定内容が有効になります。

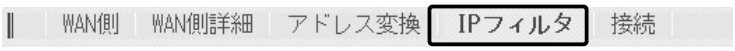
〈取消〉ボタン …… 「不正アクセス検知機能設定」項目の設定内容を変更したとき、変更前の状態に戻すボタンです。
なお〈登録〉をクリックすると、変更前の状態には戻りません。

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。

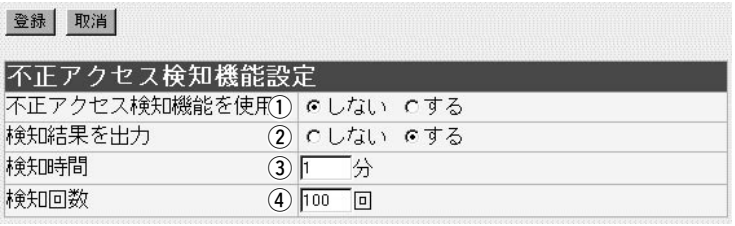
◎IP Spoofing ：偽りのLAN側アドレスでパケットを受けたとき
◎Land attack ：始点IPアドレスと終点IPアドレスが同じパケットを受けたとき
◎TCP Syn Flooding：設定した[検知時間]以内に設定した[検知回数]より多い接続要求(SYN)を受けたとき
◎Tiny Fragmenting：Tiny fragment attack(RFC 1858で定義)を受けたとき
◎Source Routing ：Loose routing IP optを検出したとき
Loose source routing headerを受けたとき
Strict routing IP opt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、第4部の4-1章をご覧ください。

1-4.「IPフィルタ」画面



■不正アクセス検知機能設定(つづき)

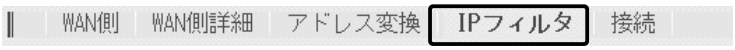


③検知時間 …… 「TCP Syn Flooding」を検知する時間を設定します。
設定できる範囲は、「1～60(分)」です。　(出荷時の設定：1)

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]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)

1 「WAN側設定」メニュー

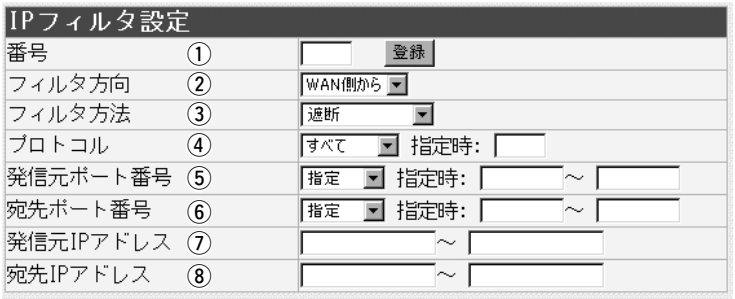
1-4.「IPフィルタ」画面(つづき)



■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フィルターは、「複数固定IP接続」でグローバルIPアドレスを割り当てられたパソコンに対しても機能します。



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。

〈登録〉ボタン

この項目で新規作成、または編集した内容をフィルターとして[現在の登録]項目に登録するボタンです。
※フィルター条件は、1つ以上指定してください。

② フィルタ方向 ……

パケットの通信方向で、WAN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。

1-4.「IPフィルタ」画面
■IPフィルタ設定(つづき)

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。

1 「WAN側設定」メニュー

1-4.「IPフィルタ」画面
■IPフィルタ設定(つづき)

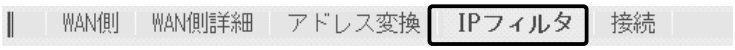
⑤ 発信元ポート番号 …… フィルタリングの対象となる発信元のTCP/UDPポート番号を指定する項目です。数字で指定するときは、「指定」を選択して、番号を始点から終点まで連続で入力します。
入力できる範囲は、10進数で「1～65535」までの半角数字です。
また、特定のポートだけを指定するときは、始点だけ、または始点/終点に同一の番号を入力してください。
数字で指定しない場合は、ニーモニック(DNS、Finger、FTP、Gopher、NEWS、POP3、SMTP、Telnet、Web、Whois)から選択します。

⑥ 宛先ポート番号 …… フィルタリングの対象となる宛先のTCP/UDPポート番号を指定する項目です。
数字で指定するときは、「指定」を選択して、番号を始点から終点まで連続で入力します。
入力できる範囲は、10進数で「1～65535」までの半角数字です。
また、特定のポートだけを指定するときは、始点だけ、または始点/終点に同一の番号を入力してください。
数字で指定しない場合は、ニーモニック(DNS、Finger、FTP、Gopher、NEWS、POP3、SMTP、Telnet、Web、Whois)から選択します。

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。

1-4.「IPフィルタ」画面(つづき)



■ 現在の登録

現在の登録

		番号	方向	方法	プロトコル	発信元ポート番号	宛先ポート番号	発信元IPアドレス	宛先IPアドレス
編集	削除	57	WAN側から	透過	TCP	20	*	*	*
編集	削除	58	WAN側から	遮断	TCP_EST	*	*	*	*
編集	削除	59	両方	遮断	ALL	135	*	*	*
編集	削除	60	両方	遮断	ALL	*	135	*	*
編集	削除	61	両方	遮断	ALL	445	*	*	*
編集	削除	62	両方	遮断	ALL	*	445	*	*
編集	削除	63	両方	遮断	TCP	*	137 - 139	*	*
編集	削除	64	両方	遮断	UDP	137 - 139	137 - 139	*	*

現在登録されているIPフィルターを表示します。

【出荷時、登録されているフィルターについて】

◎57番　　：FTPをデフォルトで通過させる
◎58番　　：WAN側からの不正アクセス防止
◎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

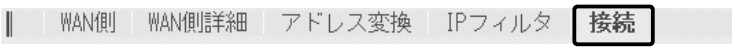
〈編集〉ボタンの右の欄に表示されたIPフィルターを編集するボタンです。
編集する欄の〈編集〉ボタンをクリックすると、その内容を[IPフィルタ設定]項目の各欄に表示します。

〈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。

1 「WAN側設定」メニュー

1-5.「接続」画面



■ 無線LAN設定

本製品の無線通信に対する基本設定です。

〈登録〉ボタン ……

「接続」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 ……

「接続」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。

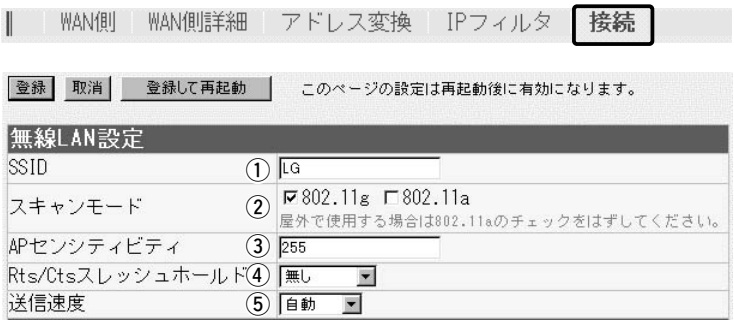
〈登録して再起動〉ボタン ……

本製品を再起動して、「接続」画面で変更したすべての設定内容を有効にします。

①SSID ……

本製品と無線アクセスポイントには、通信相手をグループとして識別するための無線ネットワーク名として、SSIDが設定されています。 (出荷時の設定：LG〈半角〉)
同じグループで通信するお互いの無線LAN機器で、この[SSID]が異なると通信できません。
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。
※[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。

1-5.「接続」画面
■無線LAN設定(つづき)



②スキャンモード ……

★屋外で使用する場合は、必ず[802.11a]のチェックボックスにチェックマークを入れないでください。

本製品で使用する無線LAN規格(802.11a/802.11g)を設定します。
[802.11a]と[802.11g(802.11bを含む)]を同時に設定できます。　(出荷時の設定：802.11g)
[802.11a]と[802.11g]を同時に設定し、[送信速度]欄を「自動」に設定して使用する場合、[802.11a/b/g]が混在する環境では、通信環境の良い無線アクセスポイントに接続されます。

③APセンシティビティ……

無線アクセスポイントからの電波が途切れたとき、スキャンを開始するまでの間隔を設定します。
無線アクセスポイントの設置環境やネットワーク状況の影響でローミング動作がスムーズに行えないとき、この設定を変更すると通信状況が改善されます。
設定できる範囲は「10～255」です。　(出荷時の設定：255)
小さい数値を設定するほど、電波が途切れてからスキャンを開始するまでの間隔が短く、大きい数値を設定するほど、電波が途切れてからスキャンを開始するまでの間隔が長くなります。

1 「WAN側設定」メニュー

1-5.「接続」画面
■無線LAN設定(つづき)

④ Rts/Ctsスレッシュホールド ……

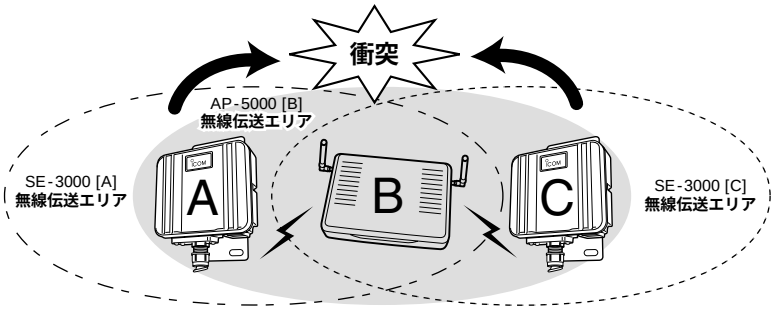
ネゴシエーションするために送るパケットのデータサイズを、「500バイト」または「1000バイト」から選択します。

(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、それぞれが無線アクセスポイント[B]と無線通信できても、互いが直接通信できない本製品[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、本製品[A]から送信要求(Rts)信号を受信した無線アクセスポイント[B]が、無線伝送エリア内にある本製品[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本製品[C]に無線アクセスポイント[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本製品[C]は、無線アクセスポイント[B]から受信完了通知(ACK)を受信するまで無線アクセスポイント[B]へのアクセスを自制することで、通信の衝突を防止できます。



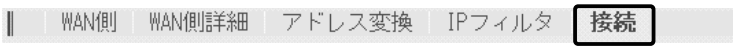
1-5.「接続」画面
■無線LAN設定(つづき)

⑤送信速度 ……

「自動」を設定すると、環境の変化などで通信が不安定になっても、[スキャンモード]欄で設定した方式で通信が続行可能な速度に自動で切り替わります。　(出荷時の設定：自動)
[スキャンモード]欄で設定したモードによって、対応できる[送信速度]が異なります。
対応できない送信速度を設定した場合は、「自動」で動作します。
◎「802.11g」および「802.11a」を設定時、「自動」以外を設定したとき対応できる速度は、「54/48/36/24/18/12/9/6」Mbpsです。
◎「802.11b」設定時、「自動」以外を設定したとき対応できる速度は、「11/5.5/2/1」Mbpsです。
※[スキャンモード]を「802.11a」に設定し、[送信速度]を「11/5.5/2/1」Mbpsのいずれかに設定したときは、送信速度の設定が「802.11a」に該当しないため、[送信速度]は「自動」で動作します。
※[802.11b]専用の無線アクセスポイントと通信する場合は、下の欄で「自動(出荷時の設定)/11/5.5/2/1」Mbpsのいずれかに設定すると使用できます。

1 「WAN側設定」メニュー

1-5.「接続」画面(つづき)



■暗号化設定

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

① 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)

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

◎WEP RC4：無線LAN機器の暗号化として一般によく搭載されている暗号化方式です。
暗号化方式は、RC4(Rivest's Cipher 4)アルゴリズムをベースに構成されています。
暗号化するデータのブロック長が8ビットで、暗号化鍵(キー)の長さを選択できます。
※選択できる暗号化鍵(キー)の長さは、64(40)/128(104)/152(128)ビットの中から選択できます。

◎OCB AES：WEP RC4より強力で、標準化が推進されている次世代の暗号化方式です。
暗号化するデータのブロック長と暗号化鍵(キー)の長さは、128ビットです。
この128ビットに対して任意に鍵(キー)を設定できますので、[WEP RC4]より強力な暗号化方式です。

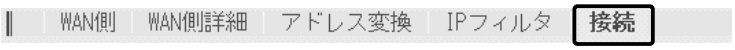
1-5.「接続」画面
■暗号化設定(つづき)

②キージェネレータ …… 暗号化および復号に使う鍵(キー)を生成するための文字列を設定します。
通信を行う相手間で同じ文字列(大文字/小文字の区別に注意して、任意の半角英数字/記号)を31文字以内で設定します。
なお、入力した文字はすべて「＊(アスタリスク)」で表示します。
(表示例：＊＊)
「暗号化方式」を選択して、〈登録〉をクリックすると、[キージェネレータ]欄に入力した文字列より生成された鍵(キー)を[キー値]項目のテキストボックスに表示します。
[キー値]項目の各キー番号のテキストボックスに生成される桁数および文字数は、選択する「暗号化方式」によって異なります。(取扱説明書[導入編]☞4-2章 ■暗号化鍵(キー)値の入力についてを参照)
※「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。

③キーID …… 暗号化に使用する鍵(キー)番号を設定します。 (出荷時の設定：1)
鍵(キー)番号は、通信する相手間でそれぞれ任意に選択できます。
[暗号化設定]項目の[暗号化方式]欄で、「RC4」または「OCB AES」が登録されているときは、「1」～「4」の中から選択できます。

1 「WAN側設定」メニュー

1-5.「接続」画面(つづき)



■キー値

暗号化鍵(キー)を直接入力するための設定です。

① 入力モード …… 暗号化鍵(キー)の入力のしかたを選びます。

(出荷時の設定：16進数)

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

※ASCII文字が設定されているときは、キージェネレータを使用できません。

② 鍵(キー)入力用ボックス … キージェネレータを使用しないとき、暗号化および復号に使用する鍵(キー)を、[入力モード]欄で設定された方法で、直接入力します。 (出荷時の設定：00-00-00-00-00)

16進数表記で使用する以外のアルファベットを入力しても無効です。

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

使用するキーIDに対する鍵(キー)の内容が違うときは通信できません。

第4部

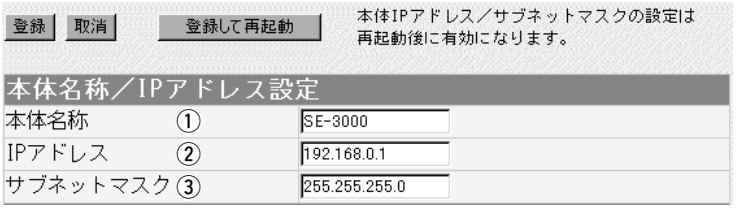
第2章 「ネットワーク設定」メニュー

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。

2 「ネットワーク設定」メニュー

2-1.「LAN側IP」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。**



〈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」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」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、本製品とEthernetケーブルで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：SE-3000)

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。

2-1.「LAN側IP」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]
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

2 「ネットワーク設定」メニュー

2-1.「LAN側IP」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	①	○しない ◉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	○しない ◉する
プライマリDNSサーバ	⑨	DNSの代理応答機能を使用する場合は無効となります。
セカンダリDNSサーバ	⑩	
プライマリWINSサーバ	⑪	
セカンダリWINSサーバ	⑫	

①DHCP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。本製品とEthernetケーブルで接続されたパソコンの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、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)

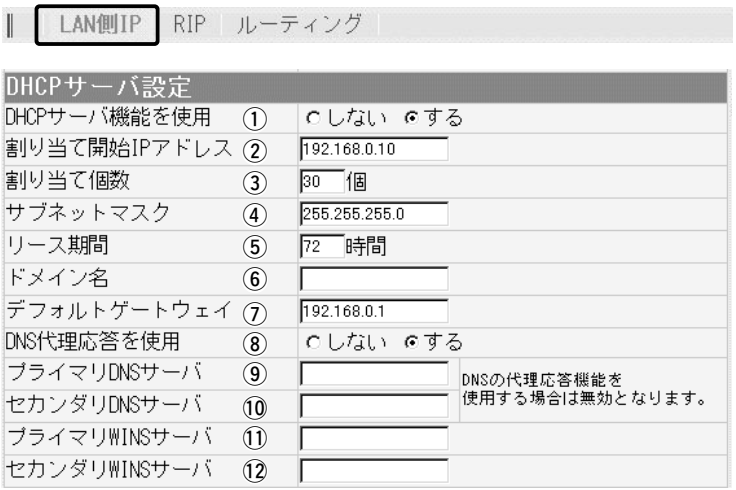
②割り当て開始IPアドレス …　本製品とEthernetケーブルで接続されたパソコンへ、IPアドレスを自動で割り当てるときの開始アドレスを設定します。
(出荷時の設定：192.168.0.10)

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)

2-1.「LAN側IP」画面
■DHCPサーバ設定(つづき)



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サーバが本製品と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)

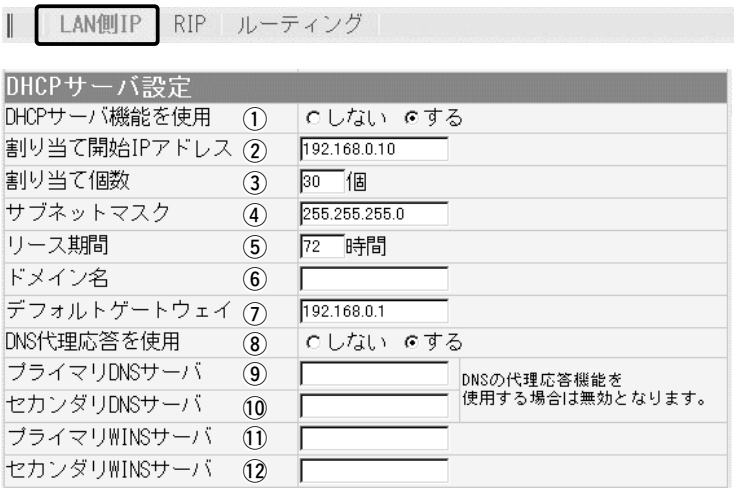
⑧ DNS代理応答を使用 …… 本製品を代理DNSサーバとして使用するかしないかの設定です。
代理DNSサーバ機能とは、パソコンからのDNS要求をプロバイダー側のDNSサーバへ転送する機能です。 (出荷時の設定：する)
代理DNSサーバ機能を利用すると、ネットワーク上のパソコンのDNSサーバを本製品のアドレスに設定している場合、本製品が接続する先のDNSサーバのアドレスが変更になったときでも、パソコンの設定を変更する必要がありませんので便利です。

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サーバの代理応答機能を使用する場合は無効になります。

2 「ネットワーク設定」メニュー

2-1.「LAN側IP」画面
■DHCPサーバ設定(つづき)



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」と同様に、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。

2-1.「LAN側IP」画面(つづき)

■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。

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。
【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。

2 「ネットワーク設定」メニュー

2-2.「RIP」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」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 …… 「RIP」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」画面で変更したすべての設定内容を有効にします。

①RIP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ローカル側RIP動作 …… ローカル側について、[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：受信のみ)

2-2.「RIP」画面
■RIP設定(つづき)

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、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](①)欄で「RIP」を設定する場合は、空白にします。

2 「ネットワーク設定」メニュー

2-3.「ルーティング」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。

IP経路情報

① 宛先	② サブネットマスク	③ ゲートウェイ	④ 経路	⑤ 作成	⑥ 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「インターフェイス情報」画面にある[ネットワーク　インターフェイス　リスト]項目に表示します。

⑤ 作成 …… どのように経路情報が作成されたかを表示します。
◎static：スタティック(定義された)ルートにより作成
◎rip　　：ダイナミック(自動生成された)ルートにより作成
◎misc　：ブロードキャストに関係するフレーム処理で作成

⑥ メトリック …… [スタティックルーティング設定]項目の[メトリック]欄で設定された値やダイナミックルーティングで作成された経路のコストを表示します。

2-3.「ルーティング」画面(つづき)

■スタティックルーティング設定

パケットの中継経路を、意図的に定義するルーティングテーブルです。
登録できるのは、最大32件までです。

①経路 …… 回路の経路を指定します。
◎local：登録する経路情報がLAN側の場合です。
◎WAN：登録する経路情報がWAN側の場合です。

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]項目に表示されます。

第4部

第3章 「システム設定」メニュー

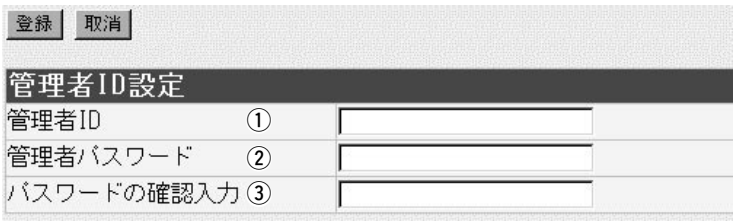
この章では、
「システム設定」メニューで表示される設定画面について説明します。

3 「システム設定」メニュー

3-1.「本体管理」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 …… 「本体管理」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 …… 「本体管理」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：se3000)
[管理者ID]を設定すると、次回のアクセスからユーザー名の入力を求められますので、そこに[管理者ID]を入力します。

② 管理者パスワード …… [管理者ID]に対するパスワードを設定する場合、大文字/小文字の区別に注意して、任意の英数字、半角31文字以内で入力します。
入力した文字は、すべて「＊(アスタリスク)」で表示されます。
(表示例：＊＊＊＊)
[管理者パスワード]を設定すると、次回のアクセスからパスワードの入力を求められますので、そこに[管理者パスワード]を入力します。

③ パスワードの確認入力 …… 確認のために、パスワードを再入力します。 (表示例：＊＊＊＊)

3-2.「時計」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 …… 「時計」画面で変更したすべての設定内容が有効になります。

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

① 本体の時刻 …… 本製品に設定されている時刻を表示します。

② 設定する時刻 …… 本製品の設定画面にアクセスしたとき、パソコンの時計設定を取得して表示します。
表示する時刻は、「時計」画面アクセス時に取得した時刻です。
※正確に設定したいときは、「時計」画面に再アクセスするかブラウザの〈更新〉ボタンをクリックしてから、〈登録〉をクリックしてください。

3 「システム設定」メニュー

3-2.「時計」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	しない ◉する
NTPサーバ1　IPアドレス	②	133.100.9.2
NTPサーバ2　IPアドレス	③	
アクセス時間間隔	④	1 日
前回アクセス日時	⑤	----/--/-- --:--
次回アクセス日時	⑥	2003/01/02 00:00

①自動時計設定を使用 …… インターネット上に存在するタイムサーバに日時の問い合わせを行い、内部時計を自動設定します。　(出荷時の設定：する)

②NTP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)

③NTP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。
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。

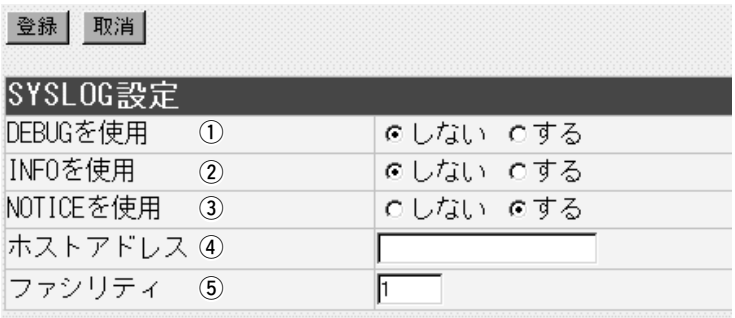
⑤前回アクセス日時 …… タイムサーバにアクセスした日時を表示します。

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。

3-3.「SYSLOG」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。



〈登録〉ボタン …… 「SYSLOG」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」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。

①DEBUG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)

②INFO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)

③NOTICE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。　(出荷時の設定：1)
設定できる範囲は、「0～23」です。
通常「1」を使用します。

3 「システム設定」メニュー

3-4.「SNMP」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」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」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。

①SNMP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。

第4部

第4章 「情報表示」メニュー

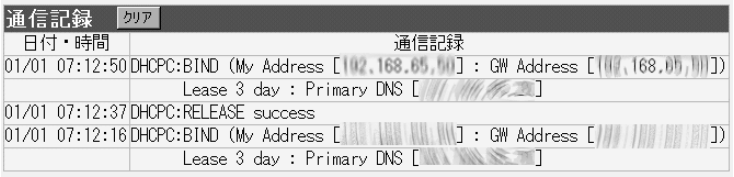
この章では、
「情報表示」メニューで表示される設定画面について説明します。

4 「情報表示」メニュー

4-1.「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。

【不正アクセス検知時の通信記録表示例】

4-2.「インターフェイス情報」画面

■ネットワーク インターフェイス リスト

本製品のインターフェイスに対する[IPアドレス]と[サブネットマスク]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	[redacted]	255.255.255.0

■ブリッジポート情報

本製品の各ポートごとに、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		
Ethernet	状況	通信中
	送信パケット数	141
	受信パケット数	146

Ethernet …… [有線LAN]ポートの通信状況と、そのときの送信と受信のパケット数を表示します。
※[有線LAN]ポートと[無線LAN]ポート間をルーティングしますので、[有線LAN]ポートの情報だけを表示します。

■無線通信状態

無線アクセスポイントとの通信状態を表示します。

無線通信状態		
SSID	①	manual
暗号化	②	無効
チャンネル	③	6CH (2437MHz)
信号レベル	④	45

①SSID …… 無線通信に使用する無線ネットワーク名(SSID)を表示します。

②暗号化 …… 無線通信に暗号化が設定されているかどうかを表示します。

③チャンネル …… 無線アクセスポイントとのチャンネルを表示します。

④信号レベル …… 無線アクセスポイントとの信号レベルを表示します。
表示される数値を通信の目安にしてください。

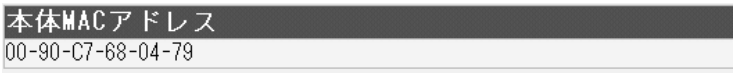
4 「情報表示」メニュー

4-2.「インターフェイス情報」画面(つづき)

■ 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、本製品の底面部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。



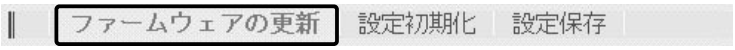
第4部

第5章 「メンテナンス」メニュー

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。

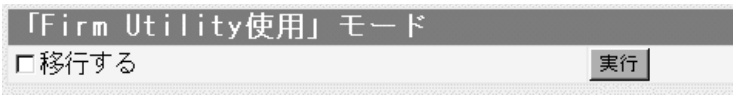
5 「メンテナンス」メニュー

5-1.「ファームウェアの更新」画面



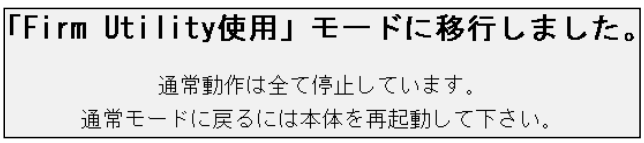
■「Firm Utility使用」モード

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

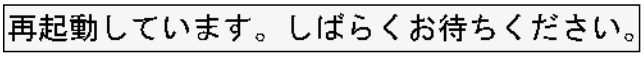
5-2.「設定初期化」画面

■設定初期化

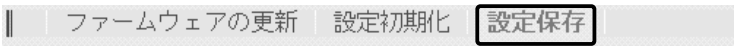
本製品の設定内容をすべて出荷時の状態に戻します。

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。



5-3.「設定保存」画面



■設定の保存と書き込み

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。

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...〉ボタンをクリックすると表示される右の画面から目的の設定ファイルを指定します。

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。
※WWWブラウザの「ファイル(F)」メニューから、[名前を付けて保存(A)...]をクリックして保存した「設定保存」画面のファイル(拡張子：.htm/.html)とは互換性がありませんので保存したファイルとして読み込むことはできません。

② ファイルに保存する ……

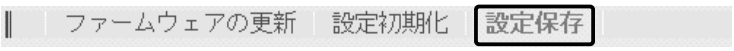
本製品すべての設定内容をパソコンに保存することで、本製品の設定をバックアップすることができます。

[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〉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。

5 「メンテナンス」メニュー

5-3.「設定保存」画面(つづき)



■現在の設定

変更された設定内容の確認や設定ファイルをハイパーテキスト形式(.htm/.html)で保存、書き込みができます。

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。
※本製品のIPアドレスの設定が、「内容表示」部に表示されたIPアドレスと異なるときは、設定を本製品に登録できません。

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」部 …… 変更された設定内容を表示します。
この画面内容をパソコンに保存することで、本製品の設定をバックアップすることができます。
保存するときは、WWWブラウザの「ファイル(F)」メニューから、[名前を付けて保存(A)...]をクリックすると、保存できます。
※[設定の保存と書き込み]項目の「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)とは互換性がありませんので、読み込むことはできません。
※各画面で設定されたパスワードやキージェネレーター(無線LAN通信用暗号化鍵の生成元文字列)の内容は、暗号化されて表示されます。
そのため、保存されたファイルよりそれらが外部へ漏れることはありません。

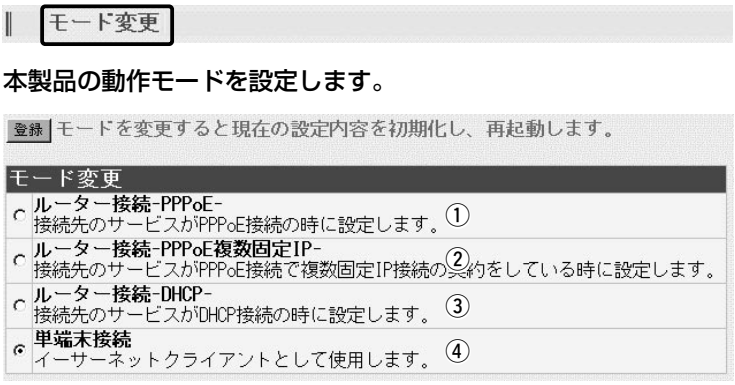
第4部

第6章 「モード変更」メニュー

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

6 「モード変更」メニュー

6-1.「モード変更」画面



■ モード変更

本製品の動作モードを設定します。

〈登録〉ボタン …… ここで変更した内容を確定すると同時に、それ以外の画面で設定した内容は出荷時の状態に戻して再起動します。

① ルーター接続 –PPPoE– … 回線接続先に[PPPoE]方式で無線接続できるサービスを契約している場合、本製品からインターネット回線に無線で接続するとき使用するモードです。

※ご契約の接続先がマルチセッションに対応していれば、同じパソコンから通常の「PPPoE」接続先とは別の「PPPoE」接続先にも接続できます。
また、2台のパソコンのうち1台は通常の「PPPoE」接続先に接続、残りの1台は別の「PPPoE」接続先に接続できます。

② ルーター接続 –PPPoE 複数固定IP– …… 回線接続先が[PPPoE]方式で無線接続でき、複数のグローバル固定IPアドレスを提供するサービスを契約している場合、グローバルIPアドレスを固定で付与したパソコンから本製品を介してインターネット回線に無線で接続するとき使用するモードです。

※ご契約の回線接続業者、またはプロバイダーから割り当てられた複数のグローバル固定IPアドレスを本製品のEthernetケーブルに接続されたパソコン(LAN側)で利用できます。
また、プライベートアドレスが割り当てられたパソコンと混在した環境でご利用いただけます。

★ご契約の回線接続業者、またはプロバイダーから割り当てられた複数のグローバル固定IPアドレス(例：8個の場合)の使いかたについては、第5部(本書)の第2章を参考にしてください。

③ ルーター接続 –DHCP–…… 回線接続先に[DHCP]方式で無線接続できるサービスを契約している場合、本製品からインターネット回線に無線で接続するとき使用するモードです。

④ 単端末接続(出荷時の設定) Ethernetポート搭載のパソコンと接続することで、無線クライアントとして弊社製無線アクセスポイントと通信するとき使用するモードです。
このとき、本製品のEthernetケーブルに接続できるパソコンは、1台だけです。

第5部

ご参考に

本製品をご使用いただくとき、参考にしていただきたい内容について記載しています。

1 Telnetについて

1-1.Telnetによる接続

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。

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 XP/Windows 2000の場合

①Windows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。

③Telnet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」画面で設定した[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 SE-3000!)が表示されます。

■ Windows 98/98 SE/Meの場合

①Windows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。

③Telnet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」画面で設定した[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 SE-3000!)が表示されます。

1-2.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

2 複数固定IPアドレスサービスについて

2-1.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「ルーター接続 –PPPoE複数固定IP–」(☞第3部)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。

2-2.グローバル固定IPアドレスの使いかた

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

◎割り当てられた指定の8個：172.16.0.48 ～172.16.0.55
◎サブネットマスク　　：255.255.255.248
◎ネットワークIPアドレス　：172.16.0.48(使用できません)
◎ブロードキャストアドレス：172.16.0.55(使用できません)
◎172.16.0.49(WAN側IPアドレスとして本製品に設定)
◎172.16.0.50(本製品に接続するパソコンに使用可能)
◎172.16.0.51(本製品に接続するパソコンに使用可能)
◎172.16.0.52(本製品に接続するパソコンに使用可能)
◎172.16.0.53(本製品に接続するパソコンに使用可能)
◎172.16.0.54(本製品に接続するパソコンに使用可能)

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

NTTフレッツ・スクウェアに接続するには 3

3-1.NTT東日本でご契約の場合

〈本製品の設定手順〉

1.「WAN側設定」メニューで、NTT東日本フレッツ･スクウェアへの接続先設定を行います。
※接続先を追加する場合は、[回線設定]項目の右にある〈▼〉をクリックして、「追加」を選択してください。
2.**「フレッツスクウェア」**を[接続先名]欄に入力します。
3.**「guest@flets」**(半角文字)を[ユーザID]欄に入力します。
4.**「guest」**(半角文字)を[パスワード]欄に入力します。
5.〈登録〉をクリックします。
6.「WAN側設定」メニューの「WAN側詳細」画面にある[PPPoE詳細設定]項目で、[接続先選択]欄から「フレッツ･スクウェア」を選択します。
7.〈選択〉をクリックします。
8.**「＊.flets」**を[宛先ドメイン]欄に入力します。
9.〈登録〉をクリックします。
10.「WAN側設定」メニューの「WAN側」画面にある[接続状況]項目で、第2セッションの列にある[接続先の選択]欄から「フレッツ･スクウェア」を選択します。
11.第1セッションの列にある[接続先の選択]欄には、通常インターネットへ接続するのに使用する接続先名を選択します。
12.第1セッションと第2セッションの〈切断〉をクリックして、回線を切断します。
13.「ネットワーク設定」メニューの「ルーティング」画面にある[スタティックルーティング設定]項目で、下記のルーティングテーブルを作成します。(合計11行)
※合計11行の[経路]欄は、すべてに「フレッツ･スクウェア」を選択してください。
※合計11行の[ゲートウェイ]欄は、すべて何も入力しないでください。
※合計11行の[メトリック]欄は、すべてに「1」(半角)を入力してください。

〈宛先〉	〈サブネットマスク〉
220.210.194.0	255.255.255.128
220.210.195.0	255.255.255.192
220.210.195.64	255.255.255.224
220.210.196.0	255.255.255.0
220.210.197.0	255. 255.255.192
220.210.197.64	255.255.255.224
220.210.197.96	255.255.255.224
220.210.198.0	255.255.255.192
220.210.199.0	255.255.255.224
172.25.0.0	255.255.0.0
172.27.0.0	255.255.0.0

(2003年9月現在)

3 NTTフレッツ・スクウェアに接続するには

3-1.NTT東日本でご契約の場合

〈本製品の設定手順〉(つづき)

14.「WAN側」画面にある[接続状況]項目で、第1セッションと第2セッションの[接続先の選択]欄の右にある〈接続〉をクリックします。
※すでに接続されている場合は、操作の必要はありません。

15.インターネットへの接続(第1セッション側)を確認します。
(例：http://www.icom.co.jp/)

16.WWWブラウザのアドレスバーに下記のアドレスを入力して、NTTフレッツ･スクウェア(第2セッション側)への接続を確認します。
http://www.flets/

【スタティックルーティングの設定について】
NTT東日本のフレッツ･スクウェアをご利用になる場合、ルーティングテーブルに設定するアドレスは、変更になることがあります。
変更された場合、ルーティングテーブルの設定を変更してください。
変更しない場合は、NTT東日本のフレッツ･スクウェアのホームページにアクセスできません。
ルーティングテーブルに設定するアドレスについては、NTT東日本のフレッツ･スクウェアに接続してから、「http://routing.flets/routing.html」(2003年9月現在)でご確認ください。

【NTT東日本のフレッツ・スクウェアを第2セッションで利用できないときは？】
「WAN側設定」メニューの「WAN側」画面にある[接続状況]項目で、第1セッションの列にある[接続先の選択]欄で「フレッツ･スクウェア」を指定すると、ルーティングテーブルの設定をしなくても、**「http://www.flets/」**にアクセスできます。
この状態で、「http://routing.flets/routing.html」(2003年9月現在)にアクセスして、ルーティングテーブルに設定するアドレスの最新情報を確認してください。

3-2.NTT西日本でご契約の場合

〈本製品の設定手順〉

1.「WAN側設定」メニューで、NTT西日本フレッツ･スクウェアへの接続先設定を行います。
※接続先を追加する場合は、[回線設定]項目の右にある〈▼〉をクリックして、「追加」を選択してください。
2.**「フレッツスクウェア」**を[接続先名]欄に入力します。
3.**「flets@flets」**(半角文字)を[ユーザID]欄に入力します。
4.**「flets」**(半角文字)を[パスワード]欄に入力します。
5.〈登録〉をクリックします。
6.「WAN側設定」メニューの「WAN側詳細」画面にある[PPPoE詳細設定]項目で、[接続先選択]欄から「フレッツ･スクウェア」を選択します。
7.〈選択〉をクリックします。
8.**「＊.flets」**を[宛先ドメイン]欄に入力します。
9.〈登録〉をクリックします。
10.「WAN側設定」メニューの「WAN側」画面にある[接続状況]項目で、第2セッションの列にある[接続先の選択]欄から「フレッツ･スクウェア」を選択します。
11.第1セッションの列にある[接続先の選択]欄には、通常インターネットへ接続するのに使用する接続先名を選択します。
12.第1セッションと第2セッションの〈切断〉をクリックして、回線を切断します。
13.「WAN側」画面にある[接続状況]項目で、第1セッションと第2セッションの[接続先の選択]欄の右にある〈接続〉をクリックします。
※すでに接続されている場合は、操作の必要はありません。
14.インターネットへの接続(第1セッション側)を確認します。
(例：http://www.icom.co.jp/)
15.WWWブラウザのアドレスバーに下記のアドレスを入力して、NTTフレッツ･スクウェア(第2セッション側)への接続を確認します。
http://www.flets/

ファームウェアVer.1.10以降で、無線LAN関係の設定で変更になった機能について説明します。

◎説明には、「単端末接続」モード設定時の画面を使用しています。

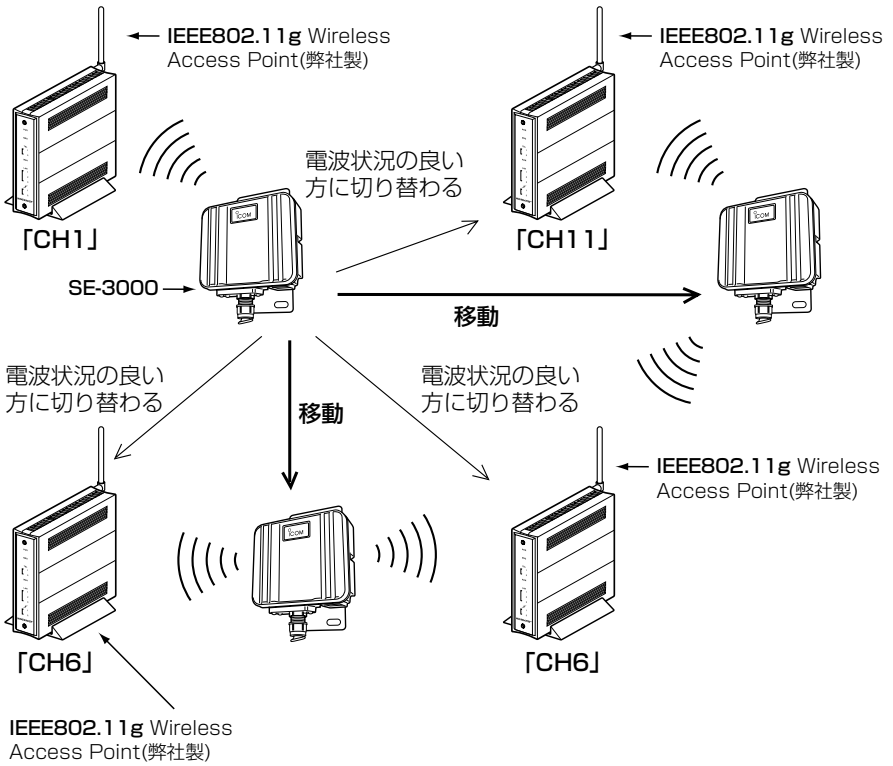
① スマートローミングを使用

[スキャンモード]で設定している無線LAN規格で使用可能なチャンネルを定期的にスキャンさせることにより、無線アクセスポイントへの切り替えが遅れないようにする機能です。

(出荷時の設定：しない)

本書(P7、P48、P104、P107)で記載の[APセンシティビティ]は、ファームウェアver.1.10以降では、使用できません。

ver.1.10以前のファームウェアで、[APセンシティビティ]を出荷時の設定でご使用の場合は、[スマートローミングを使用]欄を「しない」(出荷時の設定)に設定してご使用ください。



※[SSID]や暗号化の設定は、すべて同じにしてください。

◎説明には、「単端末接続」モード設定時の画面を使用しています。

②Super 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。

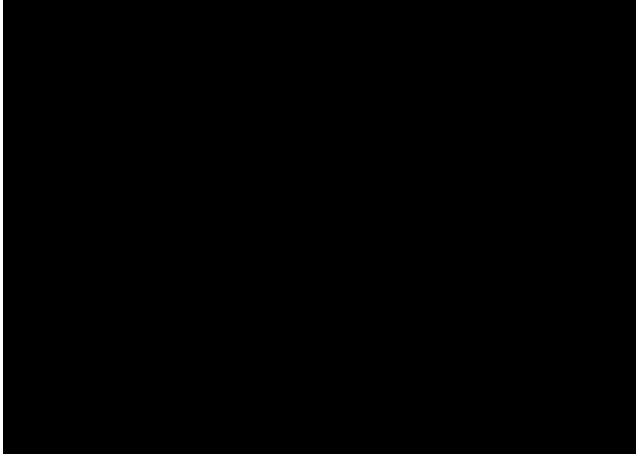
「する(圧縮あり)」を選択すると、通信速度がさらに向上します。

※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。

※無線アクセスポイントが、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。

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。

A-6316 I-2J-①