KYOCERA

KY-BR-WL100
KY-BR-CB100

新機能ガイド

METEOR
Message Terminal On Route

目次

1
本書について

本書ではMETEORホームページで公開されたファームウェアで提供された新機能について説明します。

従来の機能につきましては取扱説明書をご覧ください。

- **MACアドレスフィルタリング**（※この機能はKY-BR-WL100のみの新規追加機能です。）
  無線LANのクライアントをMACアドレスで制御することができます。登録したMACアドレスを持つクライアントを本機構成のネットワークに接続することを許可する方法と許可しない方法の2通りがあります。

- **PPPoE複数セッション**
  同時に複数のPPPoE接続が可能になります。

- **UPnP（ユニバーサル プラグ アンド プレイ）**
  UPnP対応のアプリケーションがご利用になれます。

- **アクセス制限**
  IPアドレスによってクライアントの外部へのアクセスを制限することができます。また、MACアドレスによるアクセス制限も可能です。
  メニューから「クライアントフィルタリング」は削除されますが、アクセス制限機能で同様の動作を行うことができます。

- **SPI（ステートフル パケット インスペクション）**
  動的なパケットフィルタリングを行い、IPフィルタリングでは防ぎきれない外部からの不正アクセスを防ぐことができます。

- **マルチNAT**
  複数のWAN側IPアドレスをLAN側のIPアドレスに対応させることができます。（最大7台）

- **SNMP**
  SNMP（Simple Network Management Protocol）は、ネットワークを構成する機器を管理するための仕組みです。
  本機はSNMPエージェントとして動作することができます。

2 ファームウェアのアップデート方法

アップデートを行うためには、ファームウェアとインタフェースのアップデートを行う必要があります。

ダウンロードしたファイルを解凍後、それぞれのアップデートファイルが解凍したフォルダにあることを確認してください。

インターネットエクスプローラなどのブラウザで本機の管理インタフェースを開いてください。

注意：

・アップデートを行うと工場出荷時の設定に戻ります。アップデートを行う前に、あらかじめ「設定の保存」（3ページ）を行っていただくと同時に設定内容をメモしておいてください。アップデート完了後「設定の復元」（11ページ）で以下の内容を復元できます。

設定復元可能項目：パスワード設定、LAN設定、ワイヤレス設定（KY-BR-WL100のみ）、WAN設定、DNS設定

・KY-BR-WL100のアップデート作業は、有線接続で行うことを推奨します。やむを得ず無線接続で行う場合には、ルータ本体、作業するクライアントともに、WEP設定をルータの初期値（WEP設定：「無効」）にいったん変更した後にアップデートを行ってください。WEP設定が有効のまま作業を行うと、アップデート処理後にルータにアクセスできなくなります。

・アップデート作業中は絶対に電源を切ったり、ケーブルを抜いたりしないでください。故障の原因となります。

2-1　設定の保存

ファームウェアのアップデートを行うと、工場出荷時の設定に戻ります。

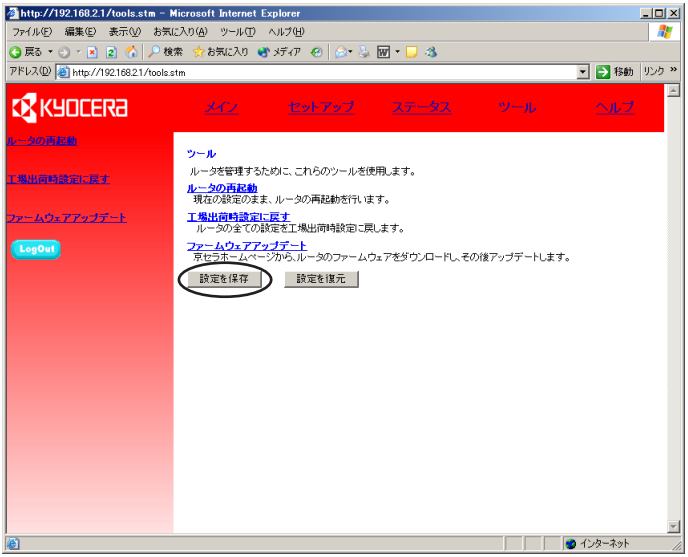
アップデートを行う前に、あらかじめ『設定を保存』を行っていただくと同時に、**必ず設定内容をメモしておいてください。**

アップデート完了後『設定を復元』で以下の内容を復元できます。

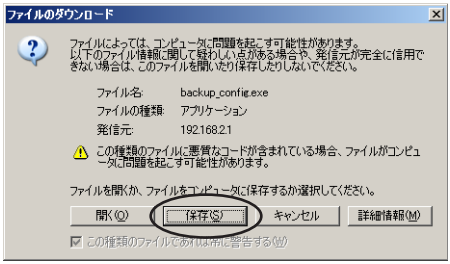
設定復元可能項目：パスワード設定、LAN設定、ワイヤレス設定（KY-BR-WL100のみ）、WAN設定、DNS設定

設定の保存方法は、以下の手順で行ってください。

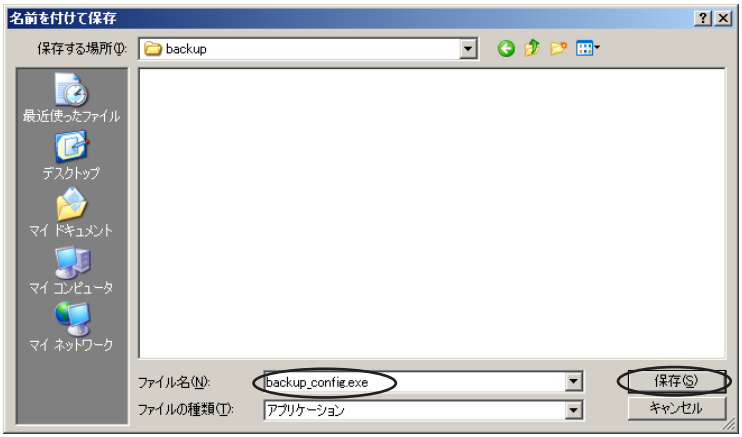
1 ログイン後、「ツール」を選択してください。ツール画面に表示された「設定を保存」ボタンをクリックしてください。



2「ファイルのダウンロード」画面が表示されますので、「保存」を選択してください。



3「名前を付けて保存」画面が表示されます。「backup_config.exe」というファイル名が表示されますので、ファイル名を変更せずに、任意の保存先フォルダに保存してください。

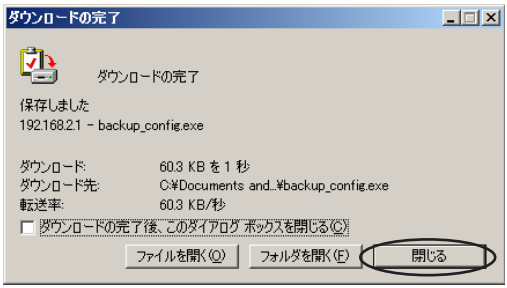


※ファイル名は、初期値の「backup_config.exe」から、絶対に変更しないでください。

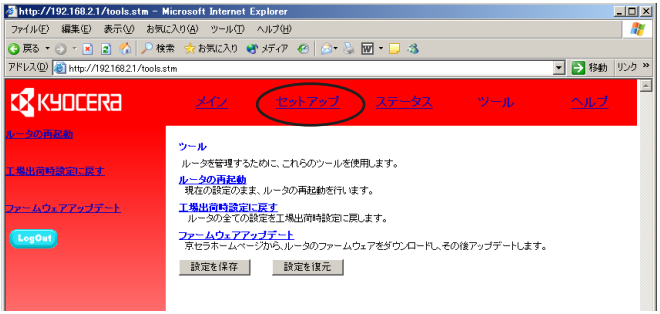
「設定を復元」時に「ファイルの照合に失敗」する場合があります。

異なる設定情報を複数保存する場合は、それぞれのファイルを、ファイル名を変更せずに別々のフォルダに保存してください。

4 ファイルのダウンロードが終わり、「ダウンロードの完了」画面が表示されます。「閉じる」をクリックして、画面を閉じてください。



5 「ツール」画面に戻ります。「セットアップ」をクリックして、「設定を保存」ではバックアップされない各設定項目（タイムゾーン設定、拡張設定の全項目）の設定内容を確認し、メモを取ってください。

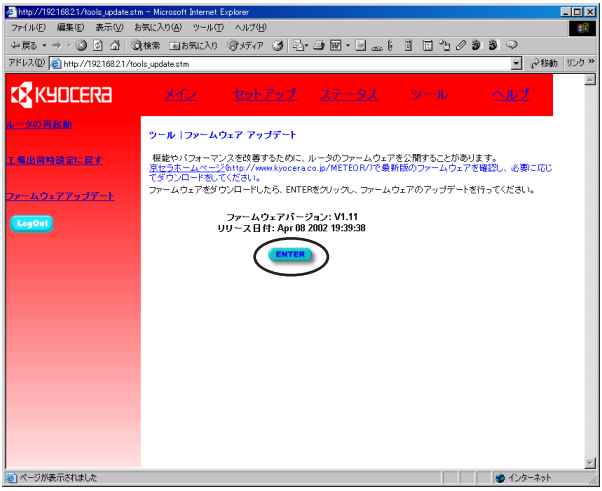


以上で設定の保存作業は終了です。

保存した設定の復元方法については、「2-4　設定の復元」（11ページ）をご覧ください。

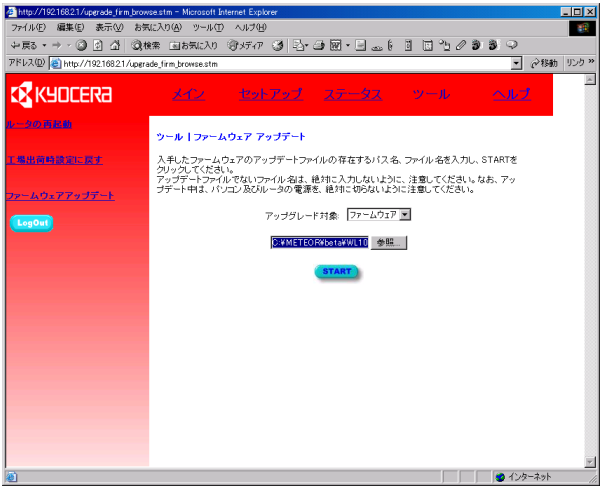
2-2 ファームウェアのアップデート

1 ログイン後、「ツール」→「ファームウェアアップデート」を選択してください。ファームウェアアップデート画面が表示されますので、「ENTER」をクリックしてください。



2 「アップグレード対象」の「▼」をクリックし、「ファームウェア」を選択してください。「参照」をクリックし、ダウンロードファイルを解凍したフォルダから、ファームウェアアップデートファイルを選択し、「開く」をクリックしてください。

※ファイル名が「fw」から始まるファイルを選択してください。



3 **「START」をクリックしてください。「アップグレードを続行してもよろしいですか？」というメッセージが表示されますので、「OK」をクリックしてください。アップグレードが開始されます。**

アップグレードが終了するまでの約1分間、本機は応答しません。正常に動作していますので**本機の電源を切らないでください。**

※アップデート中に電源を切ると、故障の原因となります。

4 **その後、ログイン画面が表示されれば、アップデートの完了です。**

注意：　「ページを表示できません」というページが表示されることがありますが、ネットワークが復旧するのを待ってから、最新の情報に更新を行うと、正常にログインページが表示されます。

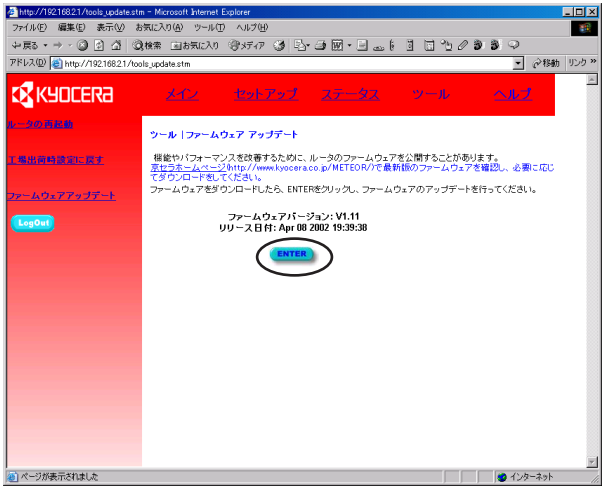
---

5 **アップデートの確認を行います。ログイン後、「ツール」→「ファームウェアアップデート」を選択してください。ファームウェアアップデート画面が表示されます。**

「ファームウェアバージョン」にダウンロードしたアップデートファイルと同じバージョンが表示されていれば、正常にファームウェアが更新されています。

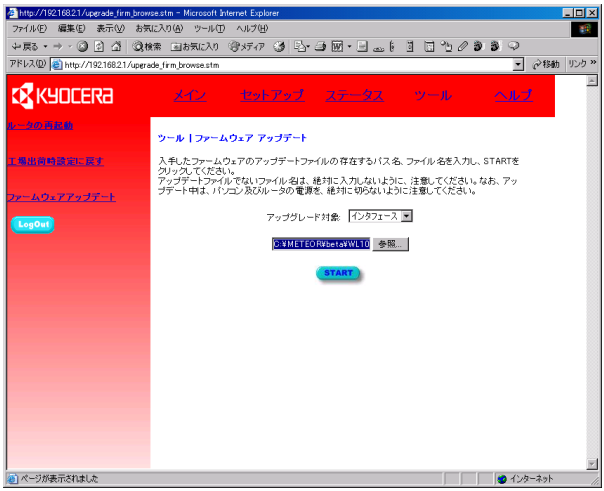
2-3 インタフェースのアップデート

1 ログイン後、「ツール」→「ファームウェアアップデート」を選択してください。ファームウェアアップデート画面が表示されますので、「ENTER」をクリックしてください。



2 「アップグレード対象」の「▼」をクリックし、「インタフェース」を選択してください。「参照」をクリックし、ダウンロードファイルを解凍したフォルダから、インタフェースアップデートファイルを選択し、「開く」をクリックしてください。

※ファイル名が「ui」から始まるファイルを選択してください。



3 **「START」をクリックしてください。「アップグレードを続行してもよろしいですか？」というメッセージが表示されますので、「OK」をクリックしてください。アップグレードが開始されます。**

アップグレードが終了するまでの約1分間、本機は応答しません。正常に動作していますので**本機の電源を切らないでください。**

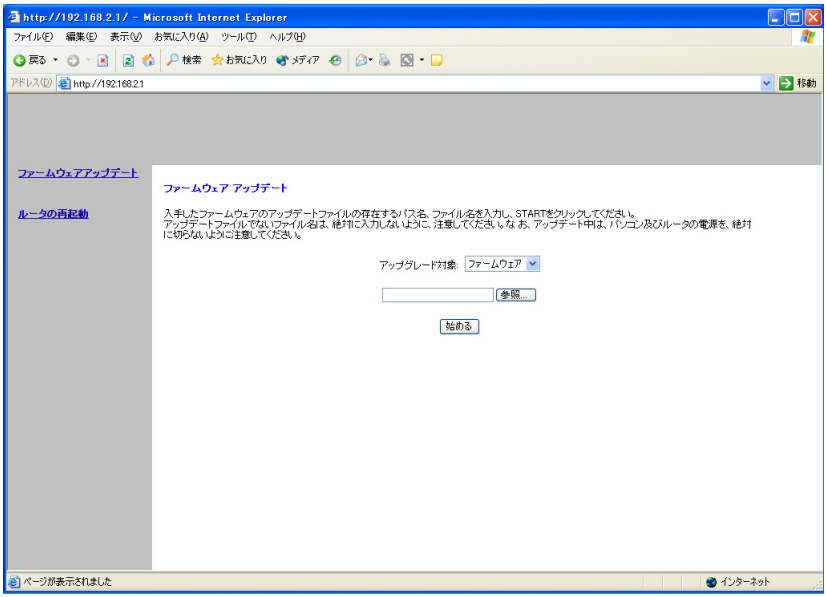
※アップデート中に電源を切ると、故障の原因となります。

4 **その後、ログイン画面が表示されれば、アップデートの完了です。**

注意：　「ページを表示できません」と表示されることがありますが、ネットワークが復旧するのを待ってから、最新の情報に更新を行うと、正常にログインページが表示されます。

・ファームウェア/インタフェースのアップデートに失敗した場合について

ファームウェア／インタフェースのアップデートに失敗した場合、ログイン時に次の画面（グレーの画面）が出る場合があります。



上記の画面が表示された場合は、再度ファームウェア／インタフェースのアップデートを行ってください。なお、アップデート作業中は、電源およびLANケーブルを絶対に抜かないようにしてください。故障の原因になります。

正常にアップデート作業が完了すると、ログインページ（赤い画面）が表示されるようになります。

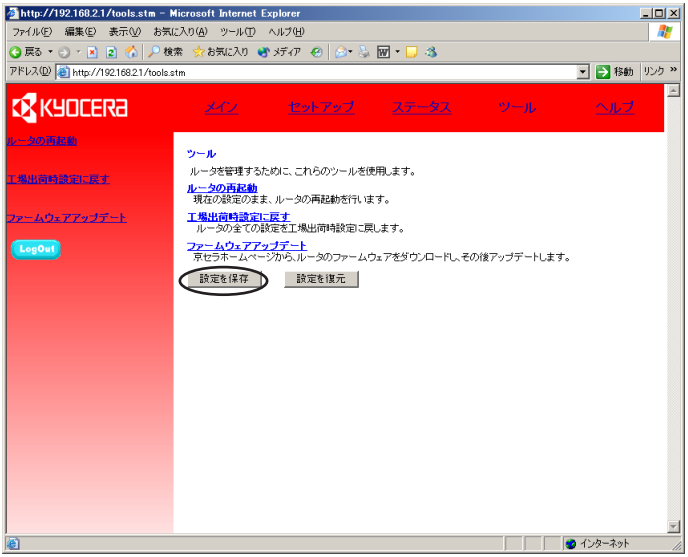
ログインページが表示されずに、同じ表示が出るような場合は、「ルータの再起動」をクリックし再起動を行ってください。

2-4 設定の復元

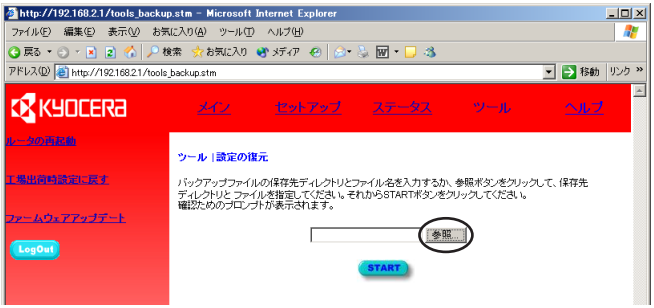
「設定を保存」で保存された設定情報は、「設定を復元」の作業を行うことにより、復元することができます。

「設定を復元」の作業は、以下の手順で行ってください。

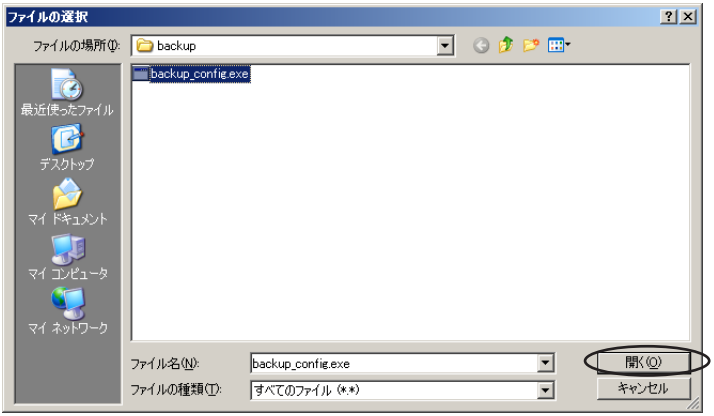
1 ログイン後、「ツール」を選択してください。ツール画面に表示された「設定を復元」をクリックしてください。



2「設定の復元」画面が表示されます。「参照」をクリックしてください。

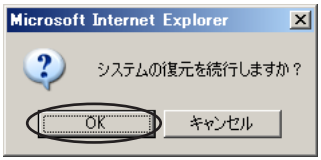


3「ファイルの選択」画面が表示されます。復元したい設定ファイルを選択して、「開く」をクリックしてください。

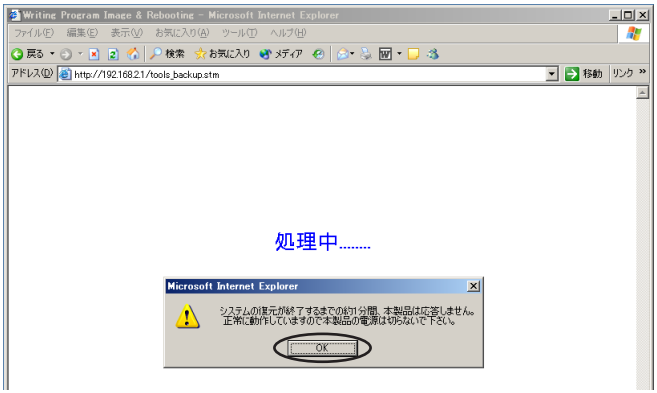


4 「設定の復元」画面に戻ります。「参照」の左の入力欄に、選択した設定ファイルのパスが入力されていることを確認して、「START」をクリックしてください。

5 次の画面が表示されますので、「OK」をクリックしてください。



6 次の画面が表示され、設定の復元作業が開始されます。復元作業には約1分間かかり、その間ルータは応答しなくなりますが、正常に動作していますので、「OK」をクリックして、しばらくお待ちください。



7 復元作業が終了して、ログインページが表示されたら、設定ファイルに保存されていた設定情報の復元は完了です。

8 設定ファイルに保存されていない各設定項目を、手動で復元します。
「設定を保存」の作業時にメモをした各設定情報（タイムゾーン設定、拡張設定の全項目）を用意の上、「ログイン」→「セットアップ」を選択して、各項目の設定の復元を行ってください。セットアップの方法については製品同梱の取扱説明書をご覧ください。

以上で、設定の復元作業は終了です。

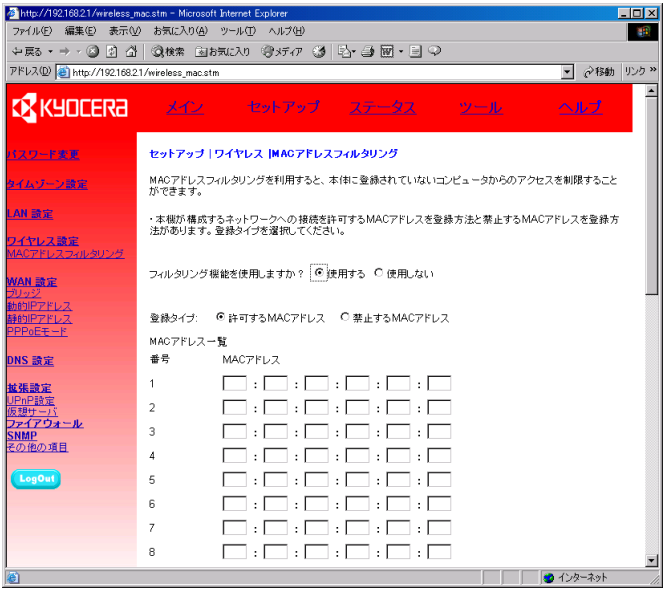
3
各機能の設定方法

3-1 MACアドレスフィルタリング（KY-BR-WL100のみ）

本機へのワイヤレス接続をMACアドレスでフィルタリングすることができます。

MACアドレスは最大32個登録でき、登録済みMACアドレスとの接続を許可する方法と、登録済みMACアドレスとの接続を禁止する方法の2通りがあります。

登録された無線LAN機器を使用しているクライアントの本機への無線接続の可否を設定できます。
初期値は「使用しない」です。



1 MACアドレスフィルタリングを設定します。「フィルタリング機能を使用しますか？」の「使用する」を選択してください。

2 使用する「登録タイプ」を選択してください。

3 許可または禁止する無線LAN機器のMACアドレスを入力してください。

4 登録するすべてのMACアドレスの入力が終わりましたら、「ENTER」をクリックしてください。

注意： 「フィルタリング機能を使用する」にチェックを入れ、以下のことを行った場合、有線接続にて管理ユーティリティに入り設定内容を修正するか、本機背面のリセットボタンを長押しし、工場出荷状態に戻してください。
・「許可するMACアドレス」で何も設定せずに「ENTER」をクリックしてしまった場合。
・「禁止するMACアドレス」で自分のMACアドレスを設定し「ENTER」をクリックしてしまった場合。

（MACアドレスの確認について）
MACアドレスは16進数（0～9、A～F）12桁で構成されるネットワーク機器固有の番号です。弊社無線LANカード「KY-LC-WL100」の場合、カード裏面に記載されている「00XXXXXXXXXX」の12桁の番号がMACアドレスです。

3-2 PPPoEによる接続の設定

プロバイダから指定されたユーザ名、パスワードを使用して、インターネットに接続を行います。本機はPPPoEプロトコルに対応していますので、ルータに接続情報を設定することによって、本機に接続されているどのパソコンからも、インターネットに接続することができるようになります。

PPPoE接続を行うには、プロバイダより送付される、

- ユーザ名
- パスワード
- DNSアドレス(指定がある場合のみ)

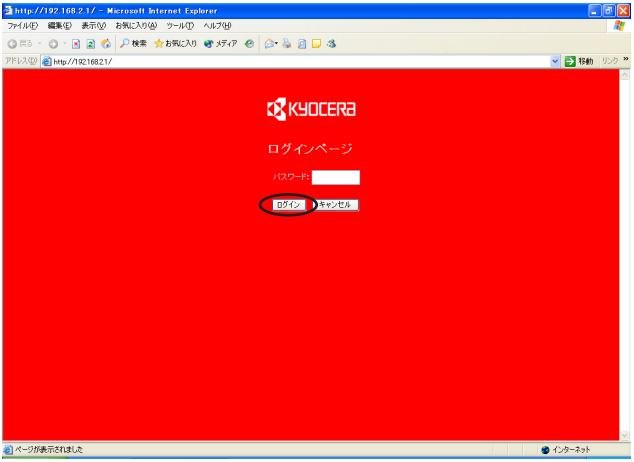
を設定する必要があります。

また、本機は接続先(プロバイダ名)を8ヵ所まで登録することができ、必要に応じて、接続先を切り替えることが可能です。

本機は同時に複数のPPPoE接続が可能ですが、ご利用のサービスにより、同時接続が可能な接続数は異なります。

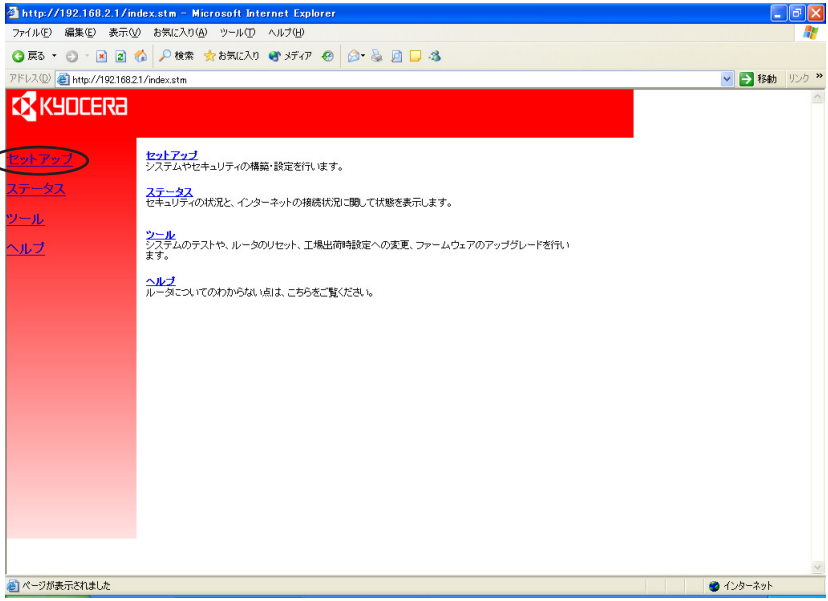
3-2-1 PPPoEの設定

1 管理インタフェースを開きます。Internet Explorerの「アドレス」バーに、本機のIPアドレス「http://192.168.2.1」を入力し、「ENTER」キーを押してください。ログインページが表示されない場合には、「http://192.168.2.1:80」と入力してください。



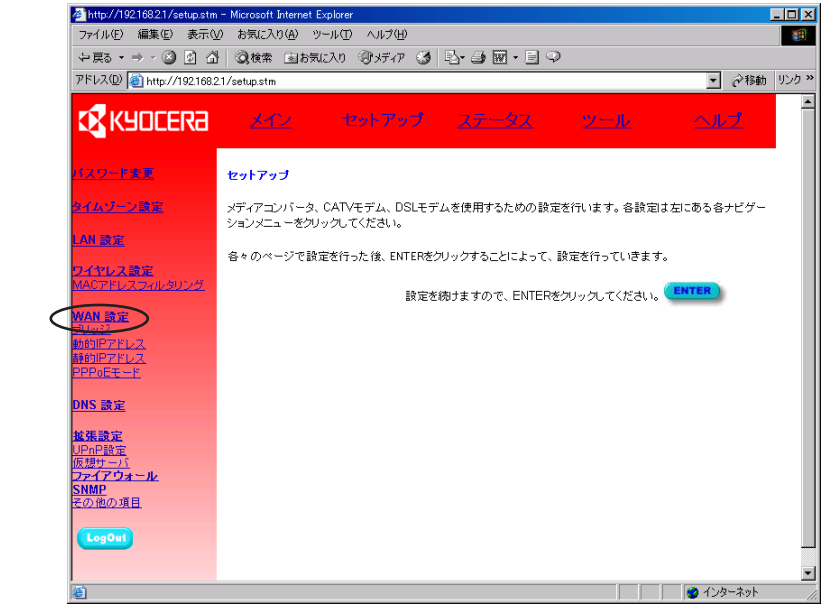
パスワードが設定されている場合は、パスワードを入力し、「ログイン」をクリックしてください。パスワードが設定されていない場合は、何も入力せずに「ログイン」をクリックしてください。

2 メニュー画面が表示されますので、「セットアップ」をクリックしてください。



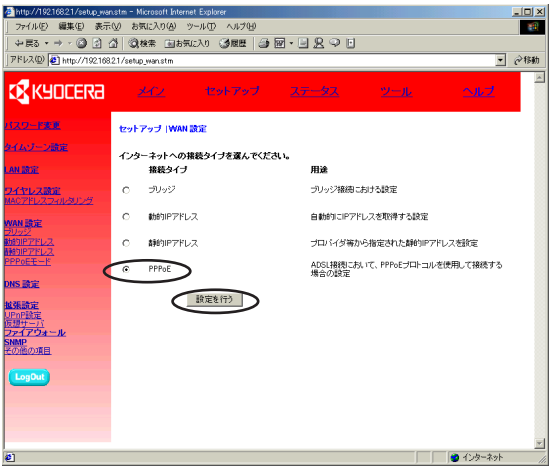
3 セットアップの説明画面が表示されます。

インターネットへの接続を行いますので、「WAN設定」をクリックしてください。



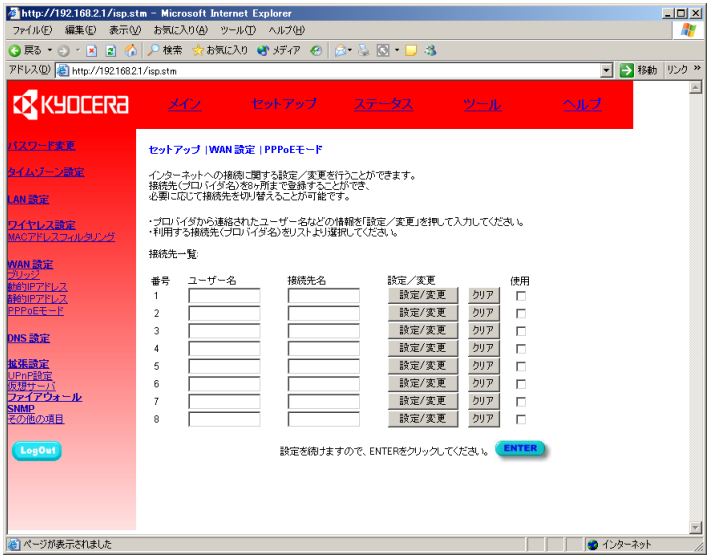
4 WAN設定の画面で、接続のタイプを選択します。

「PPPoE」をチェックして、「設定を行う」をクリックしてください。



5 接続先を設定します。新規に接続先を登録する場合は、接続先一覧の空欄となっている番号の「設定／変更」をクリックしてください。接続先の情報を変更する場合は接続先一覧の変更する「ユーザー名」、「接続先名」が表示されている番号の「設定／変更」をクリックしてください。接続先の情報を削除する場合は接続先一覧の削除する「ユーザー名」、「接続先名」が表示されている番号の「クリア」をクリックしてください。通常使用する接続先は、「番号1」に登録してください。

※・接続先が1か所のみの場合は接続先を「番号1」に登録してください。
・「設定の復元」を実行した場合は、「番号1」に登録されます。

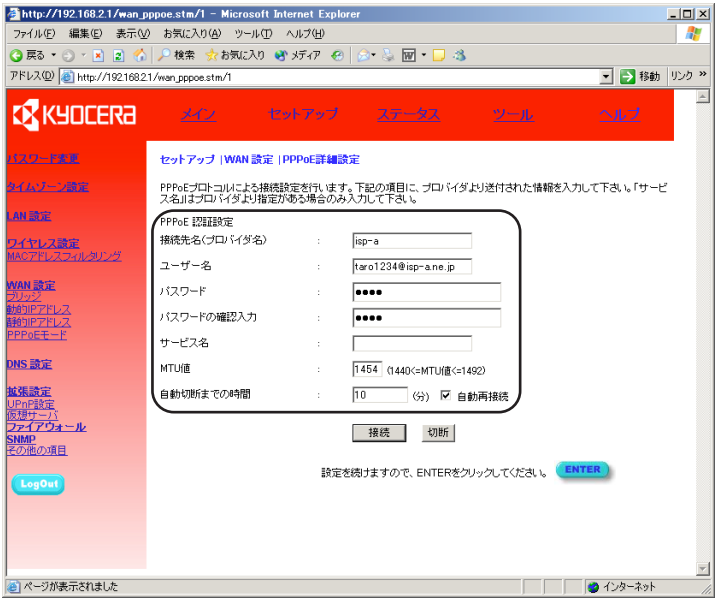


6 「PPPoEプロトコル」による接続設定を行います。

ユーザー名、パスワード、パスワードの確認入力の項目にプロバイダから指定された情報を入力してください。接続先名には任意の文字列を入力してください。

- 「サービス名」はプロバイダから指定がある場合のみ設定します。
- フレッツADSL、Bフレッツをご利用のお客様は、プロバイダから指定されたユーザ名の後に、「@プロバイダの識別名」を入力する必要があります。(例)お客様のユーザIDがtarou1234、プロバイダの識別名が、isp-a.ne.jpの場合、ユーザ名はtarou1234@isp-a.ne.jpとなります。
- 「自動切断までの時間」の初期値は10分です。「自動再接続」にチェックを入れると、切断処理後に自動的に再接続を行います。また、0分に設定すると自動切断しないので、常時接続になります。
- 「MTU値」は「1440～1492」の範囲で任意の値が設定できます。

  適切な「MTU値」は各プロバイダにご確認ください。



「接続」：登録済みの接続先と接続します。

「切断」：接続中の接続先と切断します。

初めて接続する場合は、「接続」をクリックせずに手順に従って設定を行ってください。

※上の画面は「番号1」詳細設定の画面例です。「番号2」～「番号8」の詳細設定の画面例は次ページの手順7にあります。

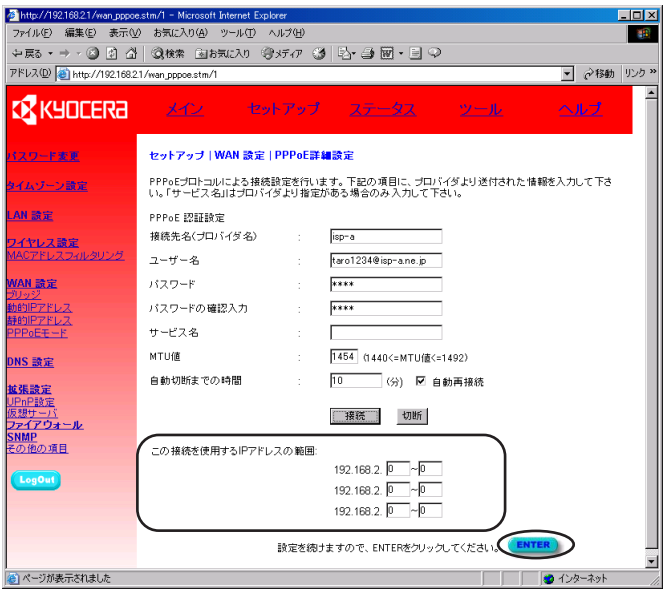
7 「この接続を利用するIPアドレスの範囲」を設定します。
この接続を利用するクライアントのIPアドレスの範囲を指定します。範囲は3パターンまで設定可能です。「番号1」の設定では、この設定項目はありません。「番号2」～「番号8」の接続を登録する場合には必ずIPアドレスを指定してください。

IPアドレスがどの接続先にも指定されていないクライアントは、自動的に「番号1」に登録されている接続先を使用します。

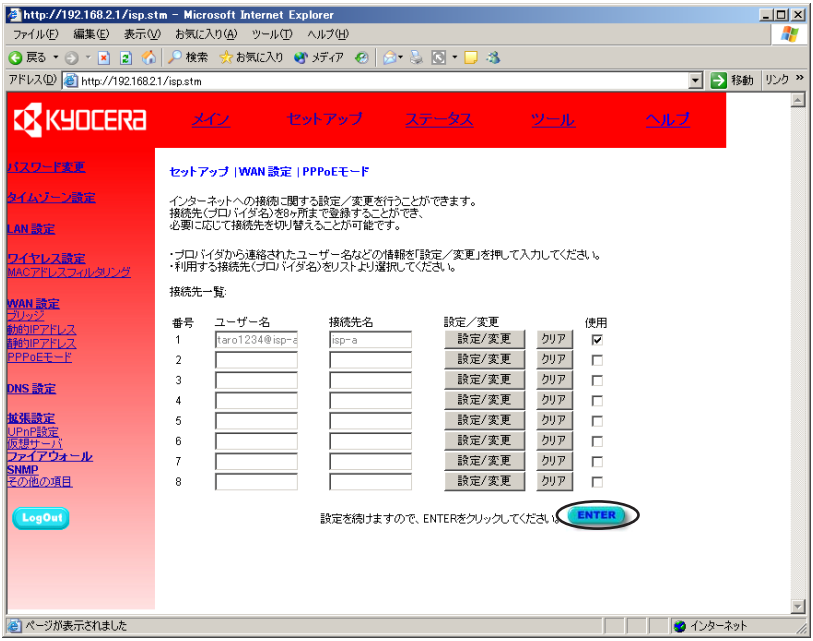
※電源のON/OFFなどによりクライアントPCに自動的に割り当てられているIPアドレスが変更される可能性があります。複数の接続先を登録してご利用になるお客様は、各クライアントPCを固定IPアドレスでIPアドレス管理を行うことをおすすめします。

※複数の登録先に同じIPアドレスを登録した場合は、接続先番号がもっとも小さい接続先に接続されます。

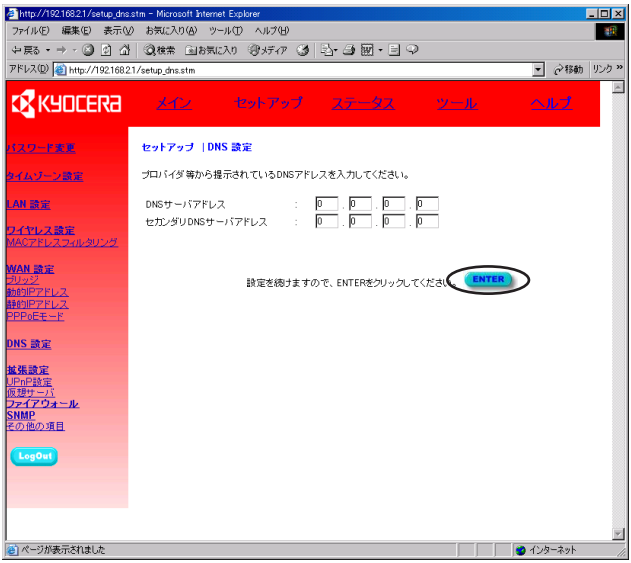
入力したら「ENTER」をクリックしてください。



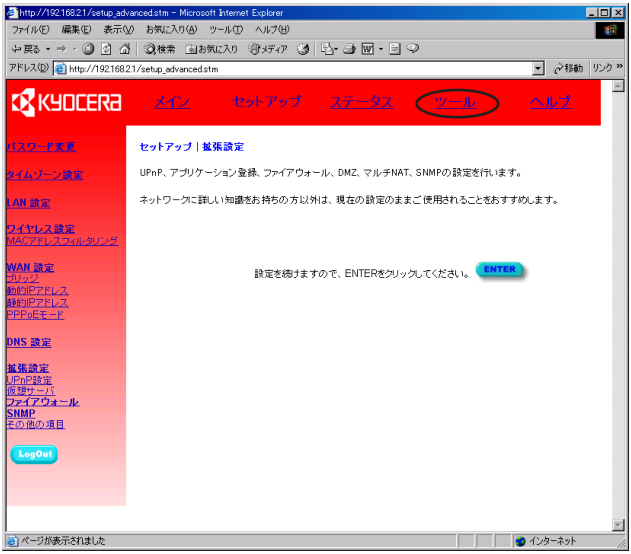
8 「PPPoEモード」画面に戻ります。登録した接続先が表示されます。接続先を複数登録する場合は続けて登録を行ってください。
接続先の登録が完了しましたら、接続を行う接続先の「使用」欄にチェックをして「ENTER」をクリックしてください。



9 DNSの設定画面が表示されます。DNSサーバのIPアドレス指定がプロバイダからある場合は、そのIPアドレスを入力してください。また、複数のプロバイダからDNSサーバのIPアドレスが指定されている場合は、その中の任意のIPアドレスを入力して、「ENTER」をクリックしてください。

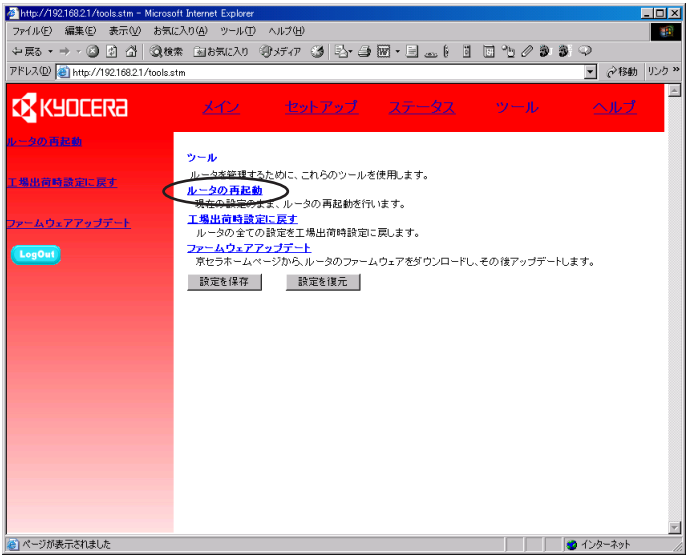


10 拡張設定画面が表示されます。ここでは設定は行いませんので、上部バーに表示されている「ツール」をクリックしてください。



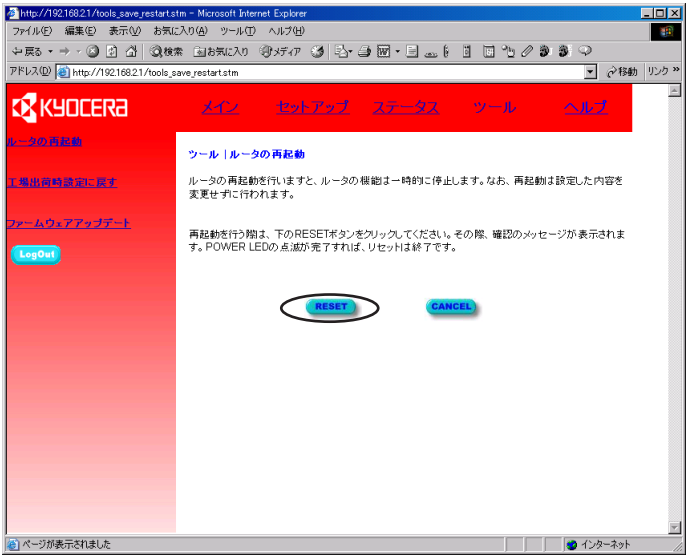
11 ツールの画面が表示されます。

今までの設定を有効にするために、「ルータの再起動」をクリックしてください。



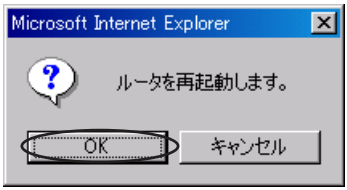
12 ルータの再起動画面が表示されます。

「RESET」をクリックしてください。



13 確認のメッセージが表示されます。

「OK」をクリックしてください。



14 再起動を行います。

再起動には1～2分ほどかかりますので、その間は電源を切らないでください。再起動後、本機は自動的にPPPoEの接続動作を行います。

再起動が終了すると、ログイン画面が表示されます。

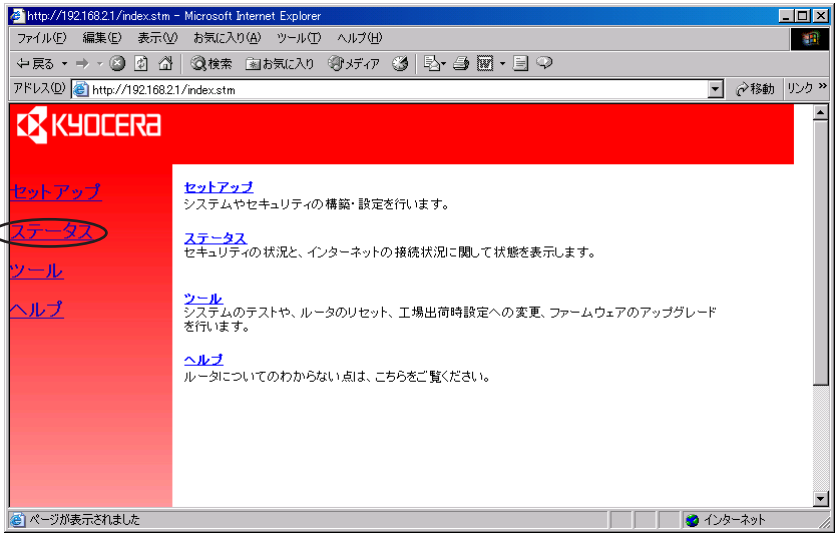
※・Windows XP/2000の場合、再起動中の画面右下に「ネットワークは接続されていません」というポップアップが出ることがありますが、再起動が終了すると、再び自動的に接続されます。

・「ページが表示できません」と表示された場合、ネットワークが復旧するのを待ってからブラウザの「表示」→「最新の情報に更新」を行うと、正常にログインページが表示されます。

以上で設定は完了しました。ここからは接続の確認になります。

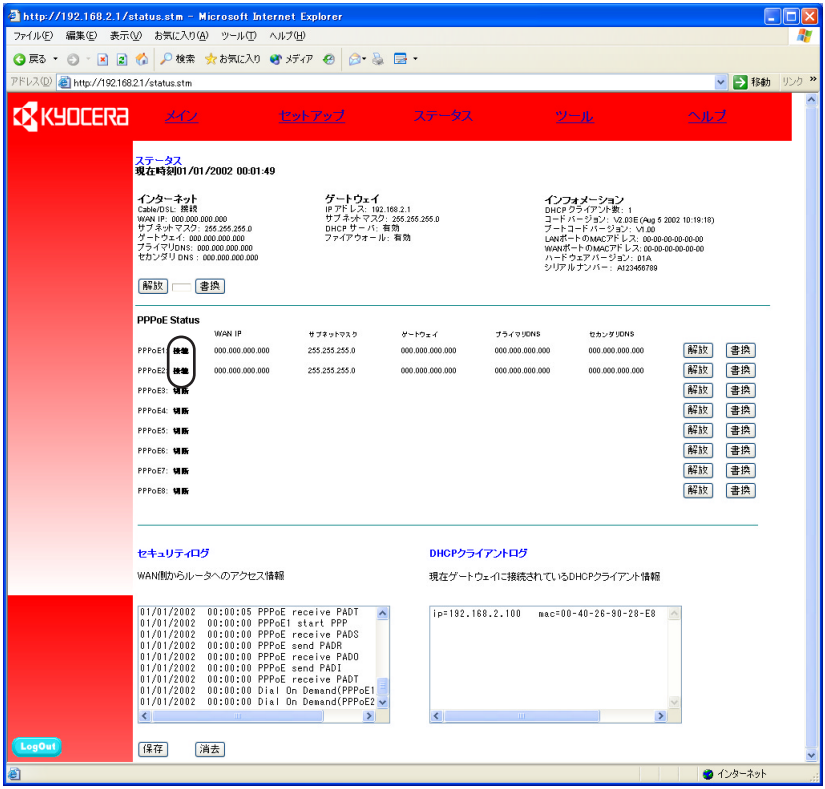
3-2-2　PPPoE接続の確認

1 PPPoE接続の確認をします。ブラウザで管理インタフェースを開き、「ステータス」をクリックしてください。



2 **「ステータス」画面が表示されます。**
接続に成功すると、PPPoE Statusの登録した接続先番号のステータスが、「接続」と表示されます。

※「接続」と表示されない場合でも、ブラウザで「最新の情報に更新」を行うと「接続」と表示される場合があります。「最新の情報に更新」を行っても「接続」と表示されない場合は再度、PPPoEの設定内容を確認してください。



接続の確認は以上です。画面左下の「LogOut」をクリックして、本機の設定を終了してください。

現在の設定を保存するには管理インタフェース上の「ツール」を選択し、「設定を保存」をクリックしてください。

3-3 UPnP（Universal Plug and Play）の設定

UPnP機能とは、Univesal Plug and Play（以下UPnP）機能の略で、この機能によりUPnP対応OSが本機を検出できるようになります。また、本機が構成するLAN内にあるパソコンから、Windows MessengerやMSN Messengerの音声チャットなどが利用できるようになります。

本機は、UPnP Internet Gateway Device機能を実装しています。この機能を利用すると、UPnPに対応したアプリケーションを利用することができます。

本機のUPnP機能を使用するにはUPnP対応のOSが必要です。標準でUPnPを搭載しているOSは以下のとおりです。

- Windows XP
- Windows Me

UPnPを利用した通信を行うためには、アプリケーション側の対応も必要です。UPnP対応のアプリケーションは以下のとおりです。

・Windows Messenger version4.7（4.7.0105）以上

Windows XPに標準搭載されているインスタントメッセージングソフト(IM)です。インターネットを使ったテレビ電話(ビデオチャット)などが可能です。

・MSN Messenger version5.0（5.0.0540）以上

Windows XP/2000/Me/98/95/NT4.0以上で利用することができるインスタントメッセージングソフト(IM)です。インターネット電話(音声チャット)などが可能です。ただし、UPnPを利用できるのはWindows XP/Meに限定されます。

注意：　インターネット接続タイプをPPPoEでご利用の場合、UPnPの規格制約上、Messengerの各機能はPPPoEの1番目の接続でのみご利用になれます。PPPoEの2～8番目の接続ではご利用になれませんのご注意ください。

本機のUPnP機能により利用可能になるWindows Messenger, MSN Messengerの機能は以下のとおりです。

	Windows Messenger	MSN Messenger	
		Windows XP	Windows Me
インスタントメッセージ	○	○	○
音声チャット	○	○	○
ビデオチャット	○	○	−
電話をかける(.NET Voice Services)	○	×	×
ファイルの送受信	○	○	○
アプリケーション共有	○	○	−
ホワイトボード	○	○	−
リモートアシスタンス	○	○	−

注意：
- 音声チャットには、音声入力/出力のためのマイク/スピーカ、またはヘッドセットが必要です。
- ビデオチャットには、マイク/スピーカまたはヘッドセットと、映像入力を行うためのカメラ(USB接続カメラなど)が必要です。音声チャットやビデオチャットは、パソコンどうしでしか利用できませんが、「電話をかける」(NET Voice Services)では、NTT一般公衆回線(03-xxxx-xxxxなど)に電話をかけることができます。ただしこの機能を利用するためには.NET Voice Servicesプロバイダとの契約が必要です。
- Windows Updateのすべての更新を適用することを推奨します。
- 本機のDMZ機能を利用し、LAN側のホストPCでWindows MessengerやMSN Messengerを使う場合は、本機のUPnP機能を有効にする必要はありません。また、ご利用のブロードバンドサービスによっては、ユーザに対してプライベートIPアドレスを割り当てることがあります。このような場合、Messengerの各機能は利用できないことがあります。
- UPnPという仕組みは、家庭内LANなどの小規模ネットワークでのプラグアンドプレイ環境実現を目的としています。また、ブロードキャストやマルチキャストを多用するため、帯域の利用効率は良くありません。したがって中規模以上のネットワークでのUPnP利用は推奨しません。
- UPnP規格では、UPnPデバイスはDHCPクライアント機能を実装することが必須となっていますが、ブロードバンドルータである本機の仕様上、LAN側DHCPクライアント機能は実装していません。
- UPnPについては下記のサイトをご覧ください。
- UPnP Forum：UPnP標準仕様　http://www.upnp.org/
- UPnP Implementers Corporation：UPnP対応機器　http://www.upnp-ic.org/
- Microsoft Netmeetingには対応していません。

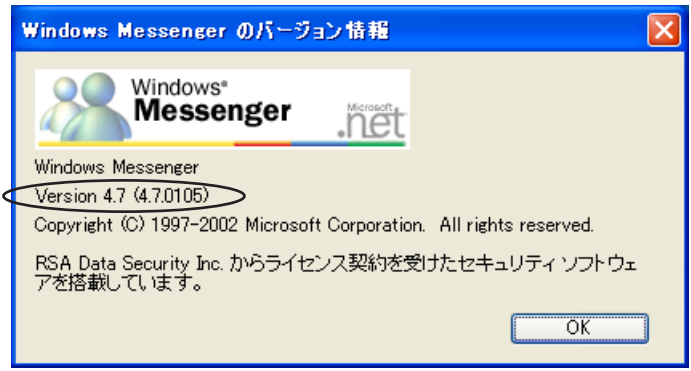
3-3-1　UPnPコンポーネントのインストール

Windows XP

Windows Messengerのバージョンの確認

Windows Messenger version4.7（4.7.0105）以降がインストールされていることを確認してください。

Windows Messengerのバージョンは、Windows Messengerのメニューから「ヘルプ」→「Windows Messengerのバージョン情報」で確認することができます。Windows Messengerのバージョンが4.7（4.7.0105）より以前のバージョンの場合は、Windows Updateからダウンロードしてインストールすることができます。

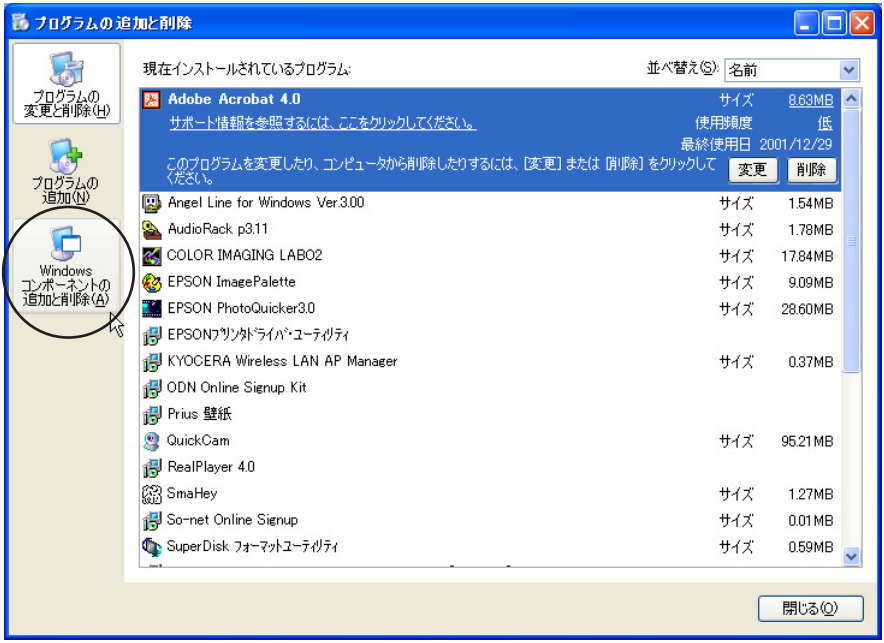


Windows Messengerのオーディオに関するアップデート

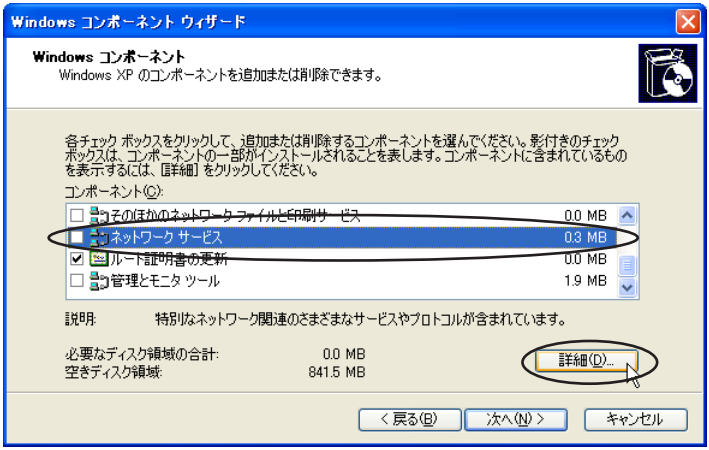
Windows Messengerのオーディオに関するアップデートが適用されているかどうか確認します。

Windows Updateを実行し、更新の一覧に「Windows Messengerのオーディオに関するアップデート」が表示される場合はそれを選択してインストールしてください。

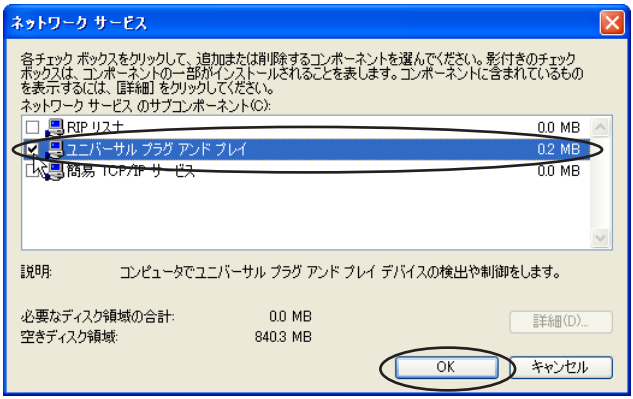
1 「スタート」→「コントロールパネル」→「プログラムの追加と削除」を選択し、「Windowsコンポーネントの追加と削除」をクリックします。



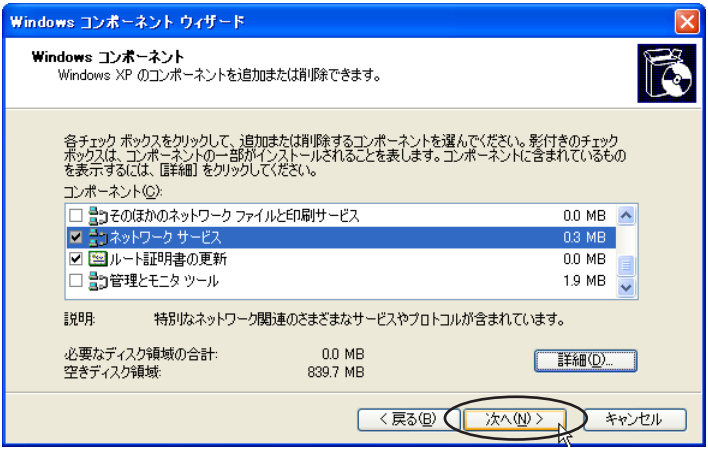
2「Windows コンポーネント ウィザード」画面が表示されますので、「ネットワーク サービス」を選択し、「詳細」をクリックしてください。

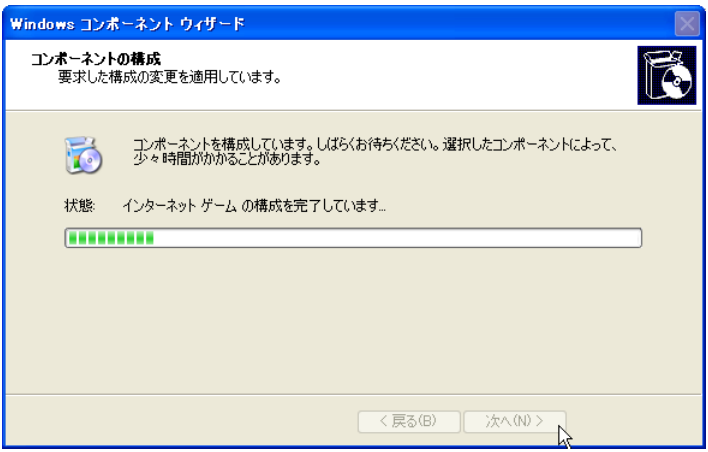


3「ネットワーク サービス」画面が表示されますので、「ユニバーサル プラグ アンド プレイ」にチェックを入れ、「OK」をクリックしてください。

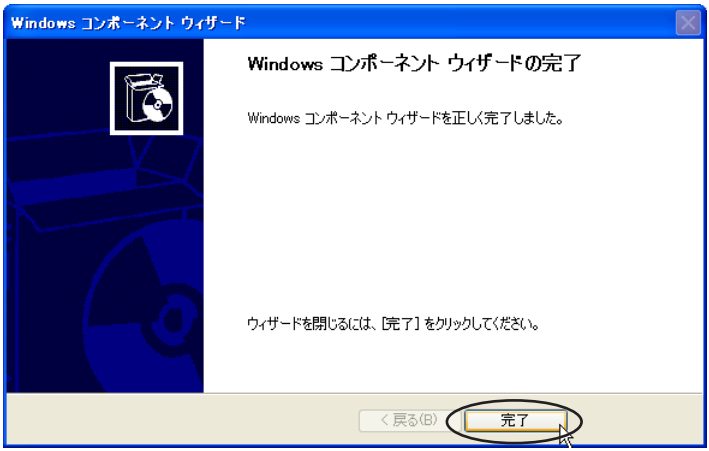


4 「Windows コンポーネント ウィザード」画面に戻りますので、「次へ」をクリックしてください。UPnPのインストールが開始されます。この際にWindows XPのCD-ROMを要求される場合があります。





5 「完了」をクリックすると、UPnPコンポーネントのインストールが完了します。

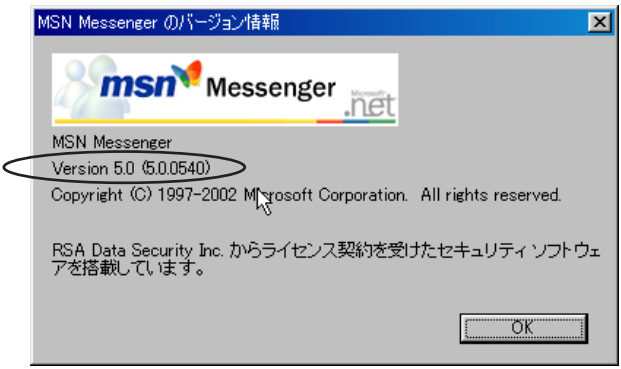


Windows XP/Me

MSN Messengerのバージョンの確認

MSN Messenger version5.0（5.0.0540）以降がインストールされていることを確認してください。

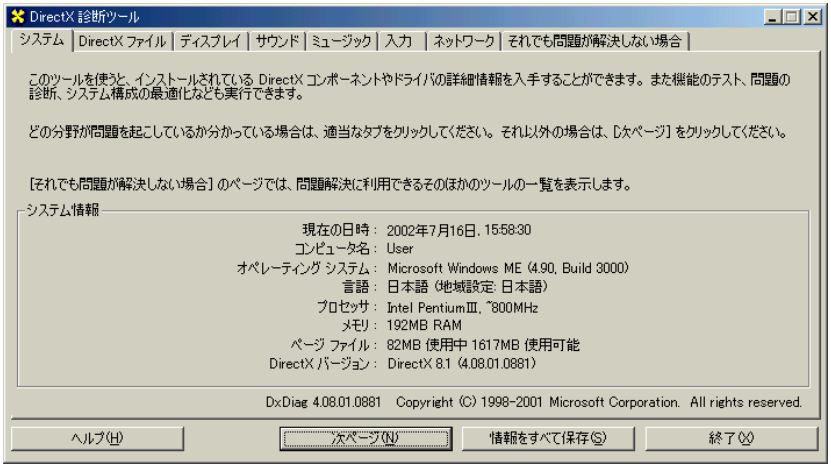
MSN Messengerのバージョンは、MSN Messengerの「ヘルプ」→「MSN Messengerのバージョン情報」で確認することができます。 MSN Messengerのバージョンが5.0（5.0.0540）より以前のバージョンの場合は、Windows Updateからダウンロードしてインストールすることができます。



DirectXのバージョンの確認

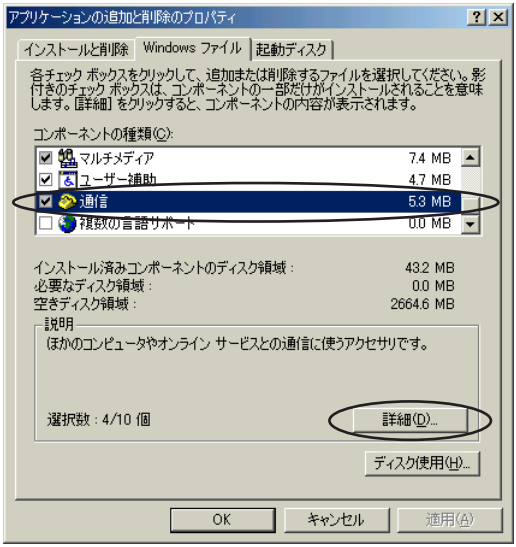
DirectX8.1以降をインストールしてあるかどうか確認してください。

DirectXのバージョンは、「ファイル名を指定して実行」で「dxdiag」を実行することで確認することができます。DirectXのバージョンが8.1より以前のバージョンの場合は、Windows Updateからダウンロード/インストールすることができます。

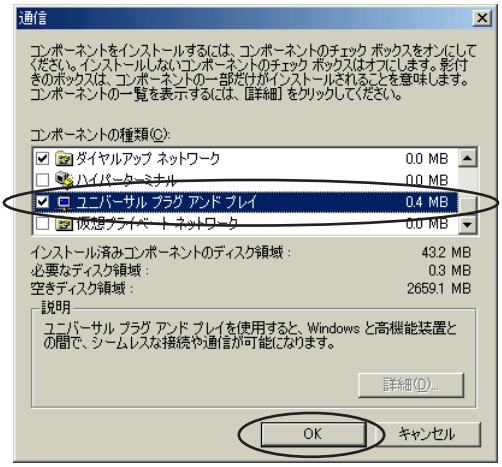


1 「スタート」→「設定」→「コントロールパネル」→「アプリケーションの追加と削除」を選択し、「Windowsファイル」タブをクリックしてください。

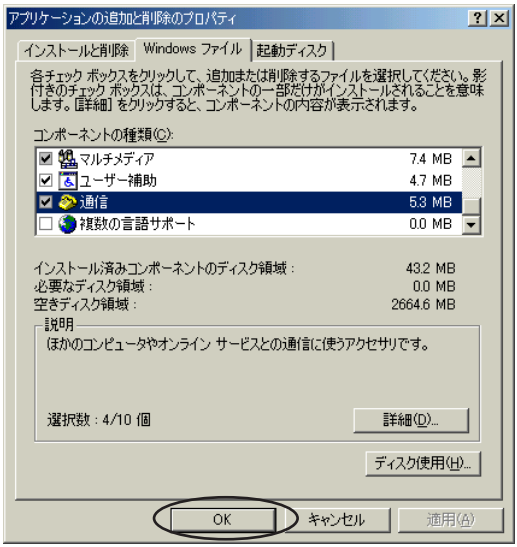
2 「Windows ファイル」画面が表示されますので、「通信」を選択し、「詳細」をクリックしてください。

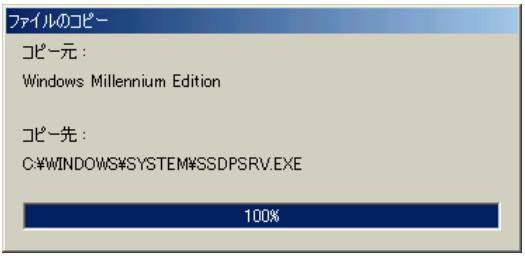


3 「ユニバーサル プラグ アンド プレイ」にチェックをいれ、「OK」をクリックしてください。

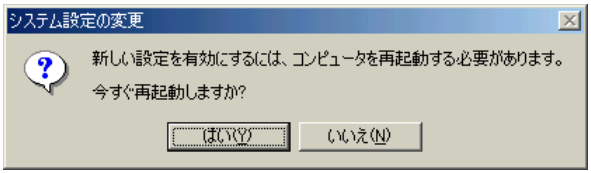


4 「Windowsファイル」画面に戻りますので、「OK」をクリックしてください。UPnPのインストールが開始されます。





「システム設定の変更」画面が表示されます。インストールが完了しました。パソコンの再起動後に、UPnPが有効になります。



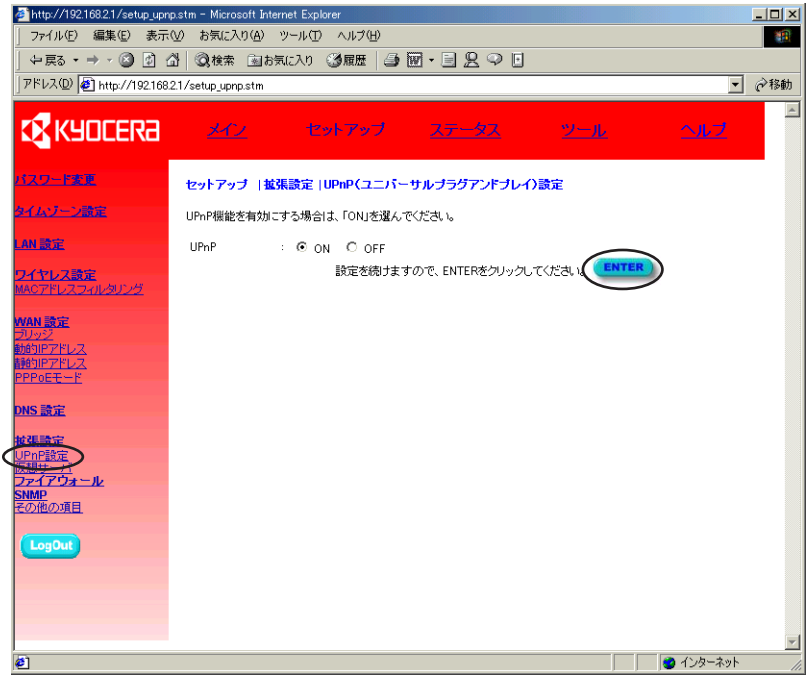
3-3-2　ルータのUPnP設定

本機を使用してUPnPを利用した通信を行うには、本機のUPnP機能を有効にする必要があります。

UPnPを有効にするためには 「ON」を選択します。

「ENTER」をクリックしてください。

※ 工場出荷時の設定ではUPnPは「OFF」に設定されています。

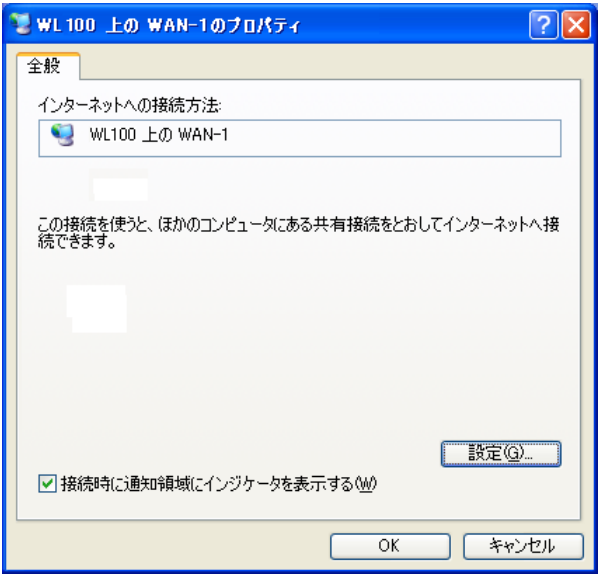


3-3-3　UPnP設定の確認

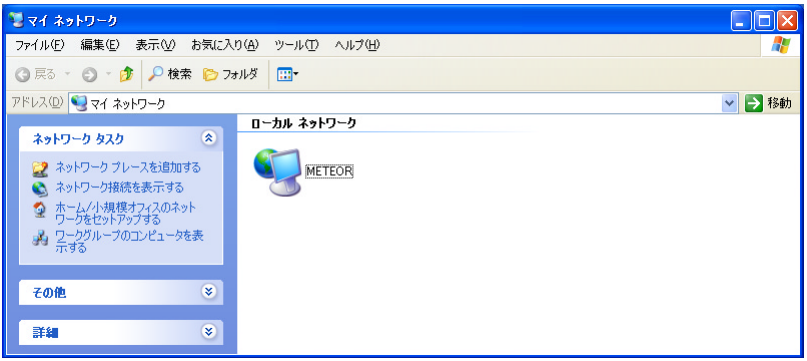
Windows XP

1 Windows XPおよび、本機のUPnP設定が正常に完了すると、本機とパソコンが接続した際、「ネットワーク接続」画面の「インターネットゲートウェイ」欄にアイコンが表示されます。

アイコンを右クリックし、「プロパティ」を選択すると、本機の接続のプロパティが表示されます。



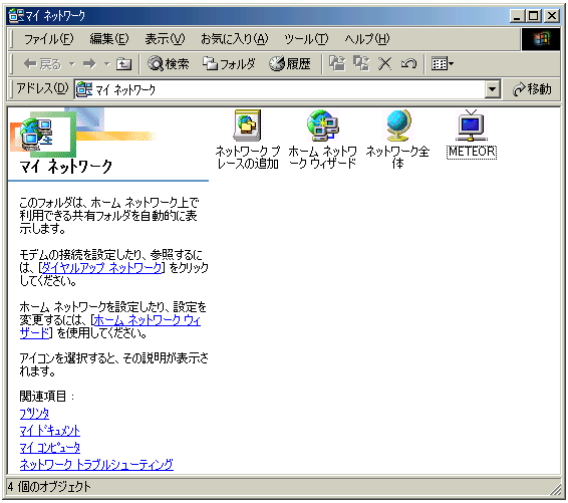
2 「マイネットワーク」のローカルネットワーク欄に「METEOR」アイコンが表示されるようになります。アイコンをダブルクリックすると本機の管理ユーティリティが表示され、ここから本機の設定を行うことができます。



アイコンを右クリックし、「プロパティ」を選択すると、本機のプロパティが表示されます。

Windows Me

1 Windows Meおよび、本機のUPnP設定が正常に完了すると、本機とパソコンが接続した際、「マイネットワーク」画面に「METEOR」アイコンが表示されます。アイコンをダブルクリックすると本機の管理ユーティリティが表示され、ここから本機の設定を行うことができます。



アイコンを右クリックし、「プロパティ」を選択すると、本機のプロパティが表示されます。

3-4 ファイアウォールの設定

本機には、一般的な簡易ファイアウォールであるNAT/IPマスカレードに加え、高機能ファイアウォール機能として、「ステートフルパケットインスペクション（SPI）」機能およびDoS攻撃防御機能を搭載しています。

初期値は「使用する」です。

ファイアウォール機能を無効にするためには、「使用しない」を選択し、「ENTER」をクリックしてください。左側のメニューから「アクセス制限」、「URLフィルタ」、「スケジュール」、「セキュリティ」、「DMZ＆マルチNAT」の各項目が表示されなくなります。

※
- ファイアウォールを「使用しない」設定でご使用になる場合、外部からの不正アクセスを受ける可能性が高くなります。ファイアウォールは「使用する」の設定でご使用になることをおすすめします。
- 外部からの不正アクセスを受けると動作が不安定になり、ルータの再起動または工場出荷時状態にしないと正常に復帰しない場合があります。
- ファイアウォール機能を使用すると、スループットは低下します。

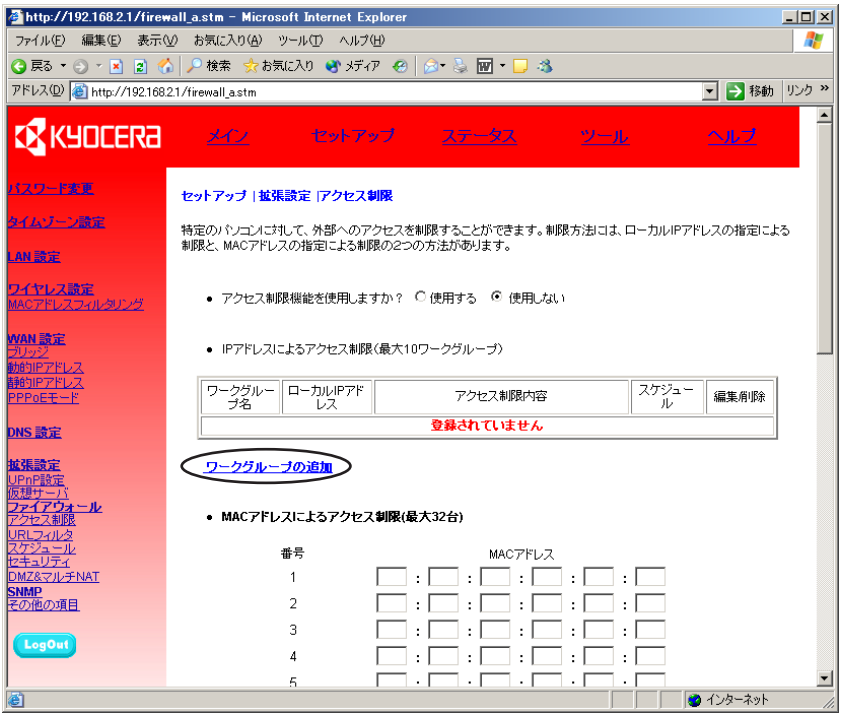
3-4-1　アクセス制限設定

特定のパソコンに対して、外部へのアクセスを制御することができます。制御方法には、「IPアドレスによるアクセス制限」と「MACアドレスによるアクセス制限」の2つの方法があります。

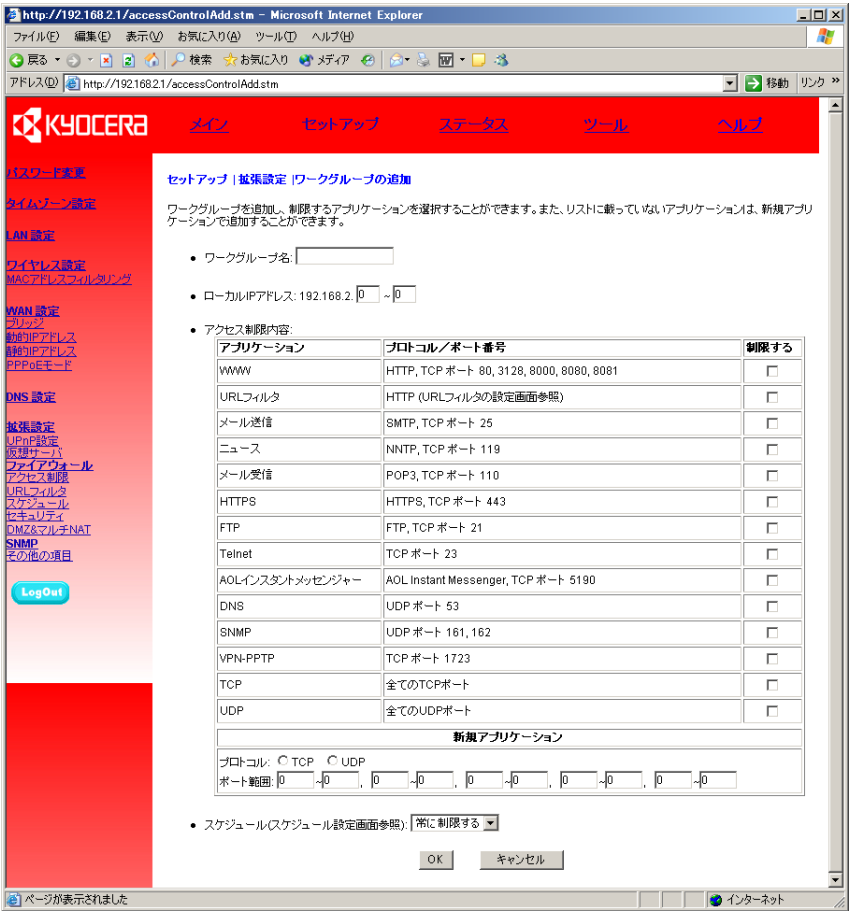
※１つのパソコンに対してIPアドレスとMACアドレスの両方の制限を設定した場合、MACアドレスの設定が優先されます。

<IPアドレスによるアクセス制限をする場合>

1 **ワークグループを作成します。「ワークグループの追加」をクリックしてください。**



2 「ワークグループの追加」画面が表示されます。次ページの表を参考にIPアドレスによるアクセス制限の設定を行ってください。



設定/表示項目	内容
ワークグループ名	任意のワークグループの名称を入力します。最大10件まで登録できます。
ローカルIPアドレス	制限するパソコンのローカルIPアドレスの範囲を指定します。
アクセス制限内容	外部アクセスを制限する項目の「制限する」にチェックマークをつけます。

注意： 「アクセス制限内容」の「URLフィルタ」を設定する場合は、ワークグループの追加を行う前に、「URLフィルタ」の設定を行ってください。設定方法は「3-4-2　URLフィルタ設定」（49ページ）を参照してください。

設定/表示項目	内容
新規アプリケーション	アクセス制限内容のリストに載っていないアプリケーションを追加します。
プロトコル	制限するアプリケーションのプロトコルを指定します。
ポート範囲	制限するアプリケーションのポート番号を指定します。

注意： 追加するアプリケーションのプロトコルがＴＣＰとＵＤＰ両方ある場合は、ワークグループを分けて登録してください。

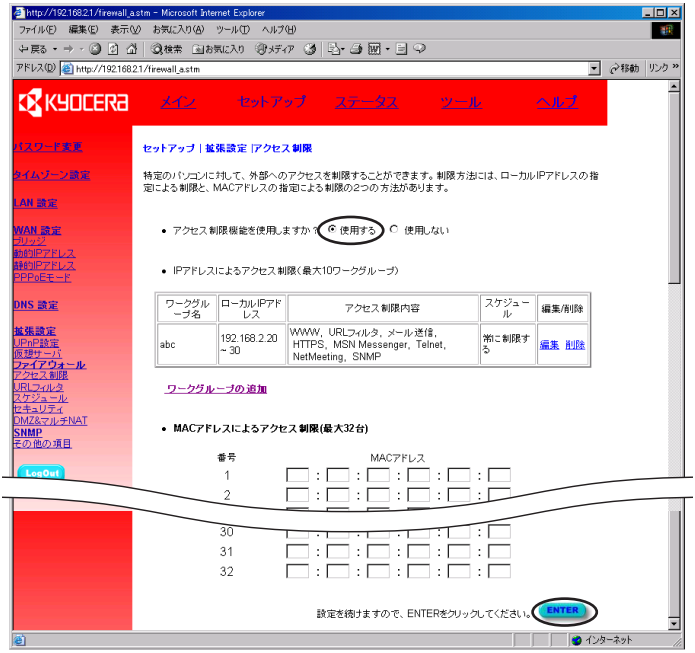
3 「スケジュール」を選択してください。

「スケジュール」で設定した内容を選択することができます。設定していない場合は「常に制限する」になっています。詳細は「3-4-3　スケジュール設定」（51ページ）を参照してください。

4 「OK」をクリックしてください。

「アクセス制限」に戻ります。「IPアドレスによるアクセス制限」に設定した内容が表示されます。

5 「アクセス制限機能を使用しますか？」の「使用する」を選択して、「ENTER」をクリックしてください。

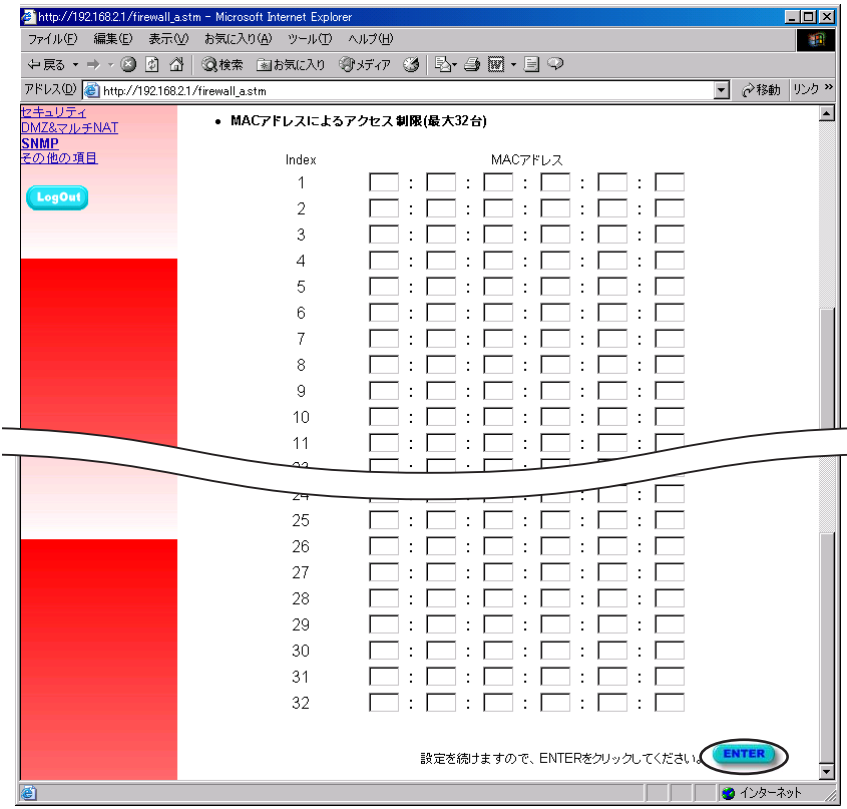


[編集]：ワークグループの内容を編集することができます。

[削除]：設定したワークグループを削除することができます。

<MACアドレスによるアクセス制限をする場合>

1 外部アクセスを制限するMACアドレスを指定してください。（最大32台まで制限できます。）



2 登録するすべてのMACアドレスの入力が終わりましたら「ENTER」をクリックしてください。

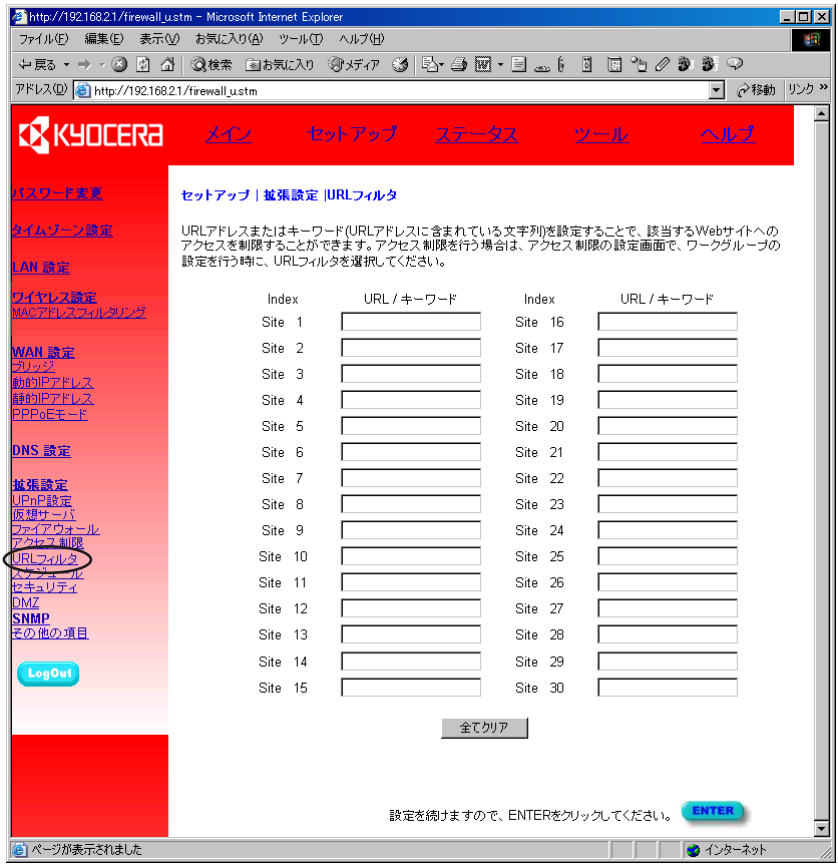
注意： ここで設定されたMACアドレスは、すべてのアクセスが制限されます。アプリケーションごとに制限したい場合は、「IPアドレスによるアクセス制限」を行ってください。

3-4-2　URLフィルタ設定

URLアドレスまたはキーワード（URLアドレスに含まれている文字）を指定することで、該当するWebサイトへのアクセスを制限することができます。

この設定を有効にするには、「3-4-1　アクセス制限設定」（37ページ）の設定画面で「ワークグループの追加」を設定する際に、「アクセス制限内容」でURLフィルタを「制限する」に設定してください。

URLフィルタは、全ワークグループの設定に対して共通の設定となります。



1 アクセスを制限するURLまたはキーワードを入力してください。

最大30件まで登録できます。

※以下のようにURL（アドレス）を部分的に設定することも可能です。

例）

・http://www.kyocera.co.jp
・kyocera
・kyocera.co.jp

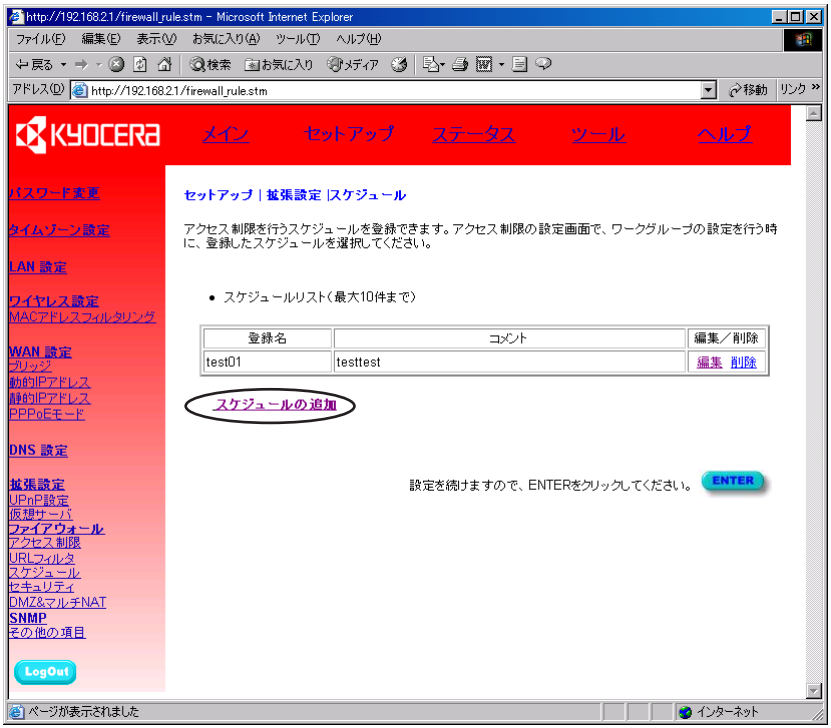
[全てクリア]：設定データをすべてクリアすることができます。

2 入力したら「ENTER」をクリックしてください。

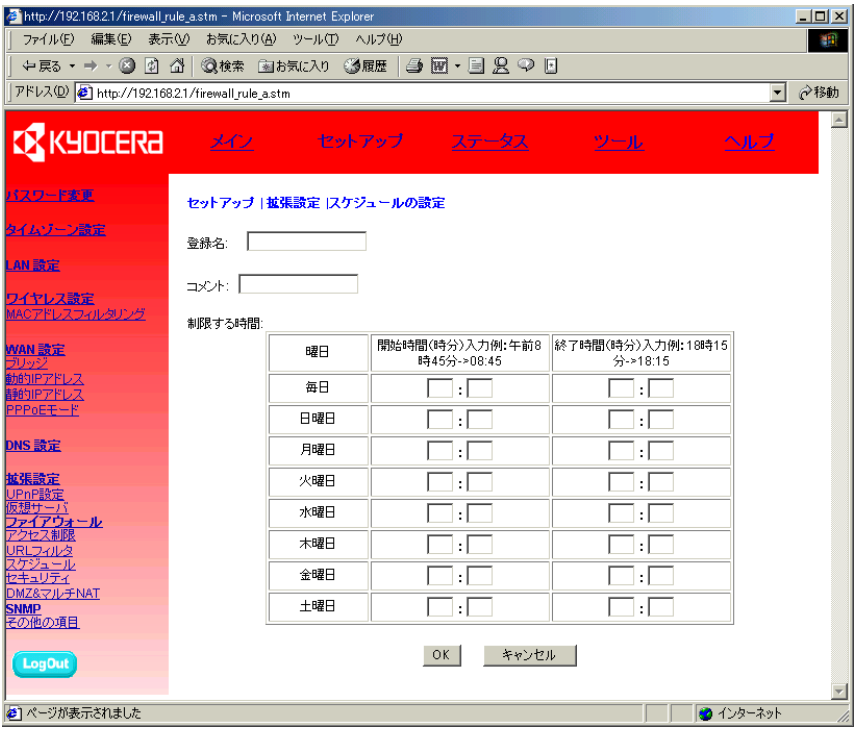
3-4-3　スケジュール設定

アクセス制限を行うスケジュールを登録します。「アクセス制限」の画面で「ワークグループ」の設定を行うときに、登録したスケジュールが選択できます。

1「スケジュールの追加」をクリックしてください。



2 下記の表を参考に、スケジュールの設定を行ってください。最大10件まで登録できます。設定したら、「OK」をクリックしてください。



設定/表示項目		内容
登録名		スケジュールを登録する任意の名前を入力します。
コメント		設定した理由など任意の内容を入力します。
制限する時間	曜日	アクセス制限をする曜日
	開始時間	アクセス制限を開始する時間を入力します。
		開始時間は0：00から設定できます。
	終了時間	アクセス制限を終了する時間を入力します。
		終了時間は23：59まで設定できます。

3-4-4　セキュリティ設定

SPI（ステートフルパケットインスペクション）およびDoS攻撃防御の設定をすることができます。

一般的なルータが搭載しているパケットフィルタリングは、IPパケットのアドレスやポート番号などのＩＰパケットのヘッダ情報をパラメータにし、パケットの許可・拒否をユーザが設定を行ったルールに基づいてフィルタリングを行います。

一方ステートフルパケットインスペクションは、IPパケットのヘッダ情報に加えパケットのデータ部の内容やフラグの状態に加えてより高いレイヤな監視(アプリケーションレベルのプロトコルまで含んだ監視)を行います。

また従来のパケットフィルタリングでは、ポートを開いた上でフィルタリングを行いますが、SPIはアプリケーション（HTTPなど）が使用中の間だけ必要なポートを開き、未使用のポートは閉じたままにしておくことができます。また、セッションを終了したときにはすぐにポートを閉じます。

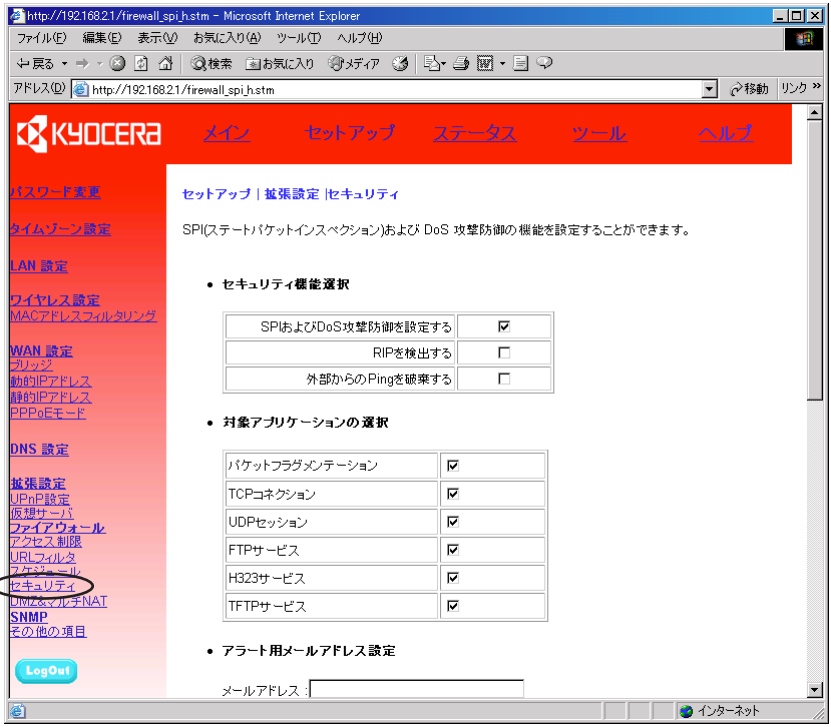
このような動的なパケットフィルタリングといえるSPIでは、IPフィルタリングでは防ぐことのできなかった外部からの不正アクセスを防ぐことが可能になります。

DoS攻撃防御機能では、外部からの連続的な不正アクセスにより、サーバやルータ自身を動作不能にさせる攻撃に対し、不正アクセスを検知した場合、一定時間に新たな接続を回避したり、検知した内容をメールで送信する機能により、ルータ本体やローカルネットワークの機器を保護します。

本機のファイアウォール機能で防御できるDoS攻撃の種類は下記の通りです。

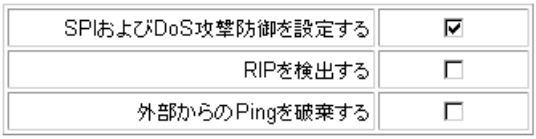
- Ping of Death (Ping flood) attack
- SYN flood attack
- IP flagment attack (Teardrop attack)
- Brute-force attack
- Land attack
- IP Spoofing attack
- IP with zero length
- TCP null scan (Port Scan attack)
- UDP port loopback
- Snork

1 SPI（ステートフルパケットインスペクション）およびDoS攻撃防御のパラメータの設定を行うことができます。TCP/IPプロトコルに詳しい方以外は、初期値の設定でご使用ください。（以下はセキュリティ機能設定画面の一部です。）



[セキュリティ]機能選択

- **セキュリティ機能選択**



SPIおよびDoS攻撃防御を設定する	本機のファイアウォール機能であるステートフルパケットインスペクションおよびDoS攻撃防御の機能を動作させる場合にチェックを入れます。（初期値：設定する）
RIP検出	WAN側からのRIP要求パケットを検出します（初期値：検出しない）
外部からのPingパケットを破棄する	WAN側からのPingの要求パケットを破棄します。WAN側からのPingやポートスキャンを行っても本機の存在を隠すことが可能になるステルスモードになります。（初期値：破棄しない）

[対象とするアプリケーション]

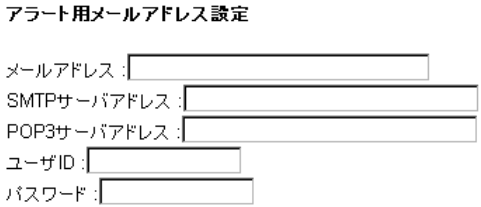
SPIおよびDoS攻撃防御の機能で監視を行う対象にチェックマークを付けます。（初期値：すべてチェック）

- **対象アプリケーションの選択**

フラグメンテーションパケット　：フラグメントされたパケットを監視します。
TCPコネクション　：TCPのコネクション状況を監視します。
UDPコネクション　：UDPのセッション状況を監視します。
FTPサービス　：FTPサービスの状況を監視します。
H.323サービス　：H.323サービスの状況を監視します。
TFTPサービス　：TFTPサービスの状況を監視します。

[アラート用メールアドレス設定]

DoS攻撃があった場合、ブロックを行った直後に攻撃を受けたパケットの情報をメールで通知します。



設定/表示項目	内容
メールアドレス	攻撃を受けた場合の通知先のメールアドレスを入力します。* 半角で39文字まで入力できます。
SMTPサーバアドレス	送信用メールサーバ（SMTP）のアドレスを入力します。
POP3サーバアドレス	受信用メールサーバ（POP）のアドレスを入力します。
ユーザID	メールサーバへのログインID（メールID）を入力します。 半角で39文字まで入力できます。
パスワード	メールサーバへのログインパスワード（メールパスワード）を入力します。半角で19文字まで入力できます。

*アラートメールの通知先（To:）と通知元（From:）は同じメールアドレスになります。

以下のようなメールが送られます。（件名：Alert Message!!!）

```
------------------------------
Your router Alert Information
Time:03/25/2002 , 10:05:11
Message:LAND
Souce  : ***.***.***.***,X
Destination: ***.***.***.***,X
------------------------------
```

Time　　：攻撃を受け、ルータがブロックした時刻

Message　：Ping of Death (Ping flood) attack, SYN flood attack, IP fragment attack (Teardrop attack), Brute-force attack, Land attack, IP Spoofing attack, IP with zero length, TCP null scan (Port Scan attack), UDP port loopback, Snork

Source　　：攻撃を受けたパケットのヘッダの送信元IPアドレスを表示します。

Destination：攻撃を受けたパケットのヘッダの送信先IPアドレスを表示します。

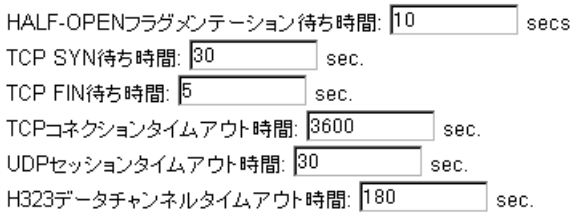
- 検出した攻撃はすべてアラートメールにて通知します。

注意：
- アラートメール送信機能は「IMAP4」、「HTTP」には対応しておりません。
- メール送信に失敗した場合、10秒ごとにリトライを行います。
- リトライ中に複数の攻撃を検出した場合、最大5件までのアラートメールを保持しており、6件以上の攻撃を検出した場合には古いアラートメールから順に破棄されます。

[コネクションポリシー]

セッション情報を管理する時間を設定します。

- **コネクションポリシー**



設定/表示項目	内容
HALF-OPENフラグメンテーション待ち時間(sec.)	フラグメンテーションパケットの応答時間 初期値：10(秒)　範囲：1～120(秒)
TCP SYN待ち時間(sec.)	TCPセッションが確立するまでの待ち時間です。 初期値：30(秒)　範囲：1～120(秒)
TCP FIN 待ち時間(sec.)	TCPセッションが終了するまでの待ち時間です。 初期値：5(秒)　範囲：1～60(秒)
TCPコネクションタイムアウト時間(sec.)	TCP接続が非アクティブでオープンしたままの状態から切断するまでの待ち時間です。 初期値：3600(秒)　範囲：1800～7200(秒)
UDPセッションタイムアウト時間(sec.)	UDP接続が非アクティブでオープンしたままの状態から切断するまでの待ち時間です。 初期値：30(秒)　範囲：1～120(秒)
H.323データチャネルタイムアウト時間	H.323接続が非アクティブでオープンしたままの状態から切断するまでの待ち時間です。 初期値：180(秒)　範囲：0～3600(秒)

[DoS攻撃検出基準]

DoS攻撃を検出する基準を設定します。

DoS攻撃検出基準

トータルTCP/UDPインコンプリートセッション数　上限: 300 セッション
トータルTCP/UDPインコンプリートセッション数　下限: 250 セッション
TCP/UDPインコンプリートセッション(分)数　上限: 250 セッション
TCP/UDPインコンプリートセッション(分)数　下限: 200 セッション
同一ホストからの最大TCP/UDPインコンプリートセッション数: 10
同一ホストからのTCP/UDPインコンプリートセッション検出時間: 300 msec.
同一ホストからの最大フラグメンテーションパケット数: 30
HALF-OPENフラグメンテーション検出時間: 10000 msec.
フラッデングクラッカーブロック時間: 300 sec.

設定/表示項目	内容
トータル TCP/UDPインコンプリートセッション数上限：（セッション）	この設定値を超えるとすべてのTCP/UDPセッションを以下下限値を下回るまでブロックします。 初期値：300　範囲：1～300
トータル TCP/UDPインコンプリートセッション数下限：（セッション）	この設定値を下回るとセッションを再開します。 初期値：250　範囲：1～250
TCP/UDPインコンプリートセッション数上限：(セッション)	1分間に非アクティブでオープン状態のセッションがこの設定値を超えると、セッションの削減を開始します。 初期値：250　範囲：1～250
TCP/UDPインコンプリートセッション数下限：(セッション)	1分間に非アクティブでオープン状態のセッションがこの設定値を下回ると、セッションの削減を中止します。 初期値：200　範囲：1～200
同一ホストからの最大TCP/UDPインコンプリートセッション数	同一ホストからのオープン状態のセッションがこの設定値を超えるとフラッディングクラッカーブロックタイム設定時間の間、新たな接続を拒否します。 初期値：10　範囲：1～50
同一ホストからのTCP/UDPインコンプリートセッション検出時間：(msec.)	同一ホストからのオープン状態のセッションが検出する間隔を設定します。 初期値：300　範囲：50～5000
同一ホストからの最大フラグメンテーションパケット数	同一ホストから発生した、断片化されたパケットの最大許容数です。これを超えると、フラッディングクラッカーブロックタイムの間、新たな接続を拒否します。 初期値：30　範囲：1～150
HALF-OPENフラグメンテーション検出時間：(msec.)	同一ホストから発生した、断片化されたパケットを検出する間隔を設定します。 初期値：10000　範囲：10～60000
フラッディングクラッカーブロックタイム：(msec.)	同一ホストからの攻撃に対して新たな接続を拒否する時間を設定します。 初期値：300　範囲：0～30000

2 入力したら「ENTER」をクリックしてください。

本機は、工場出荷時ではWindowsで使用されるNet BIOS over TCP/IP(NBT)で使われるパケットはWAN側に送出しません。

DMZ＆マルチNAT設定の場合、その設定PCに対してSPI機能は動作しませんが、DoS攻撃防止機能は動作します。

仮想サーバ設定時は、SPI機能およびDoS攻撃防御機能は動作します。

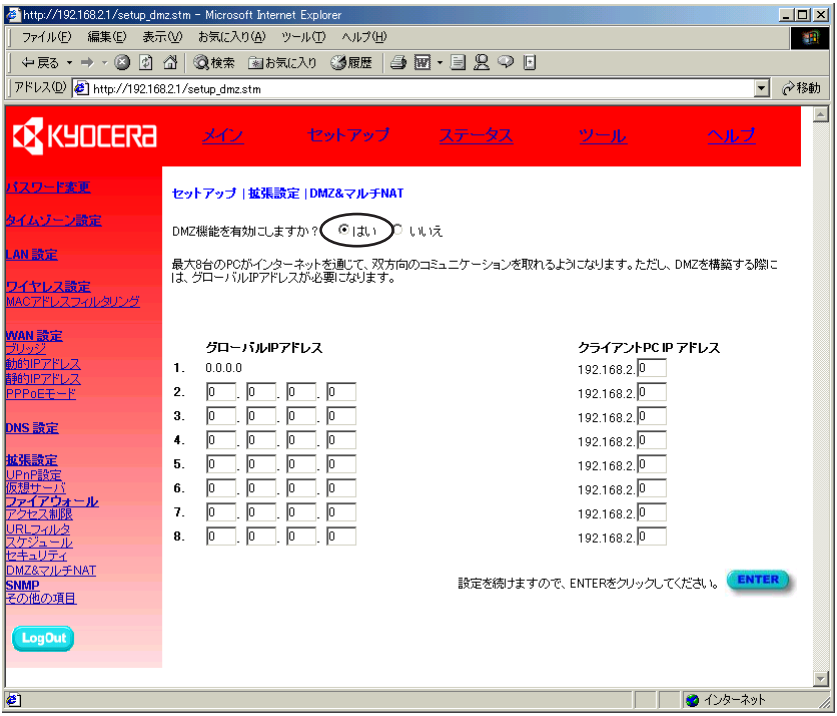
3-4-5　DMZ&マルチNAT設定

＜DMZ＞

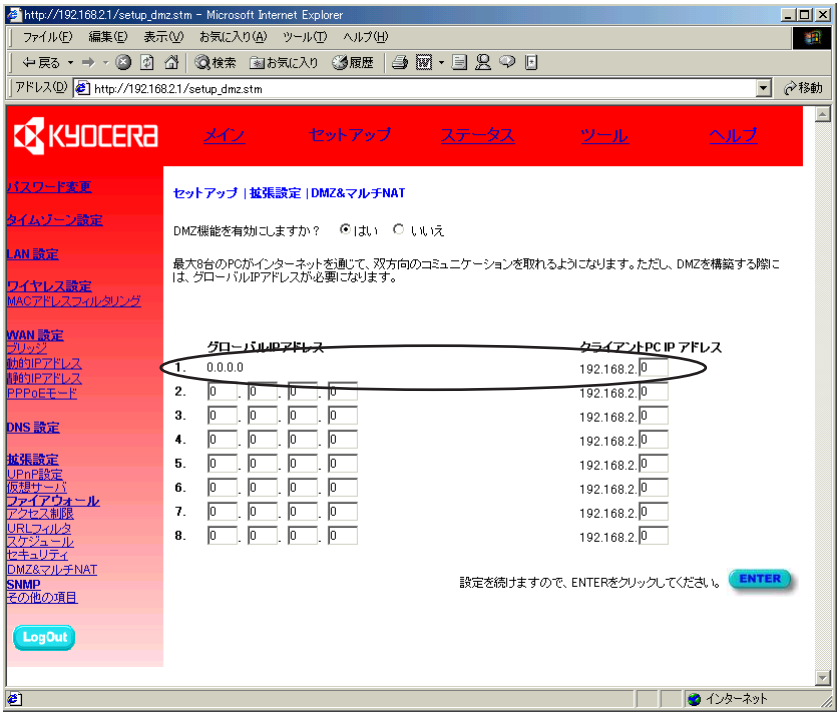
DMZ(DeMilitarized Zone)機能を使用することにより、外部からのパケットをすべて1台のパソコンやサーバーに転送することが可能になります。ネットワークアプリケーションやネットワークゲームを利用する場合で、仮想サーバでは動作しない場合に利用します。

注意：　複数グローバルIPアドレスを利用したい場合は、「マルチNAT」（62ページ）をご覧ください。また、複数IPアドレスを利用する場合も、DMZとして機能します。

1「DMZ機能を有効にしますか？」の「はい」を選択してください。



2 以下の画面内の「グローバルIPアドレス」と「クライアントPC IPアドレス」対応一覧の「1」のみがDMZの対象になります。グローバルIPアドレスの「1」には、自動的にWAN側IPアドレスが表示されます。
次にDMZ機能を設定したいクライアントPC IPアドレスを入力します。



注意：
- DMZ機能を使用する場合、パソコンのローカルIPアドレスは固定で設定してください。
- グローバルIPアドレスを自動取得している場合は、「クライアントPC IPアドレス」の1番上の欄に、DMZを指定したいパソコンのローカルIPアドレスを入力してください。
- 2～8番目はマルチNAT機能の対象となります。

3 入力が完了したら「ENTER」をクリックしてください。

＜マルチNAT＞

マルチNAT機能により、プロバイダから割り当てられた複数のグローバルIPアドレスを最大7個のローカルIPアドレスと対応させることができます。

この機能を利用することにより、グローバルIPアドレスを固定する必要のあるサービスを利用できます。

対応可能なローカルIPアドレス数

・8個のグローバルIPアドレスサービスの場合：6個

・16個以上のグローバルIPアドレスサービスの場合：7個

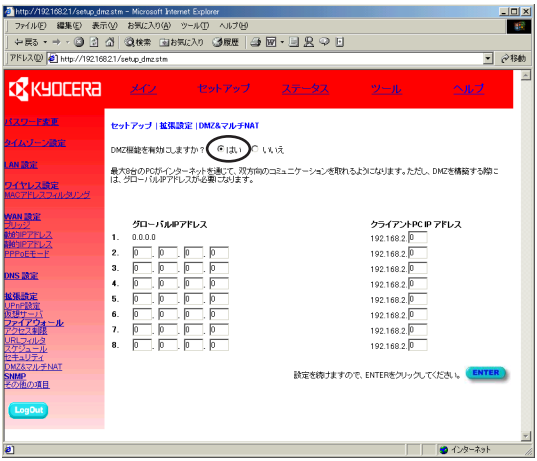
以下は8個のグローバルIPを固定的に割り当てるサービス（Unnumbered）を利用する場合の設定例を示しています。

No.	グローバルIPアドレス	ローカルIPアドレス
1	200.200.200.1	—
2	200.200.200.2	192.168.2.100
3	200.200.200.3	192.168.2.101
4	200.200.200.4	192.168.2.102
5	200.200.200.5	192.168.2.103
6	200.200.200.6	192.168.2.104
7	200.200.200.7	192.168.2.105
8	—	—

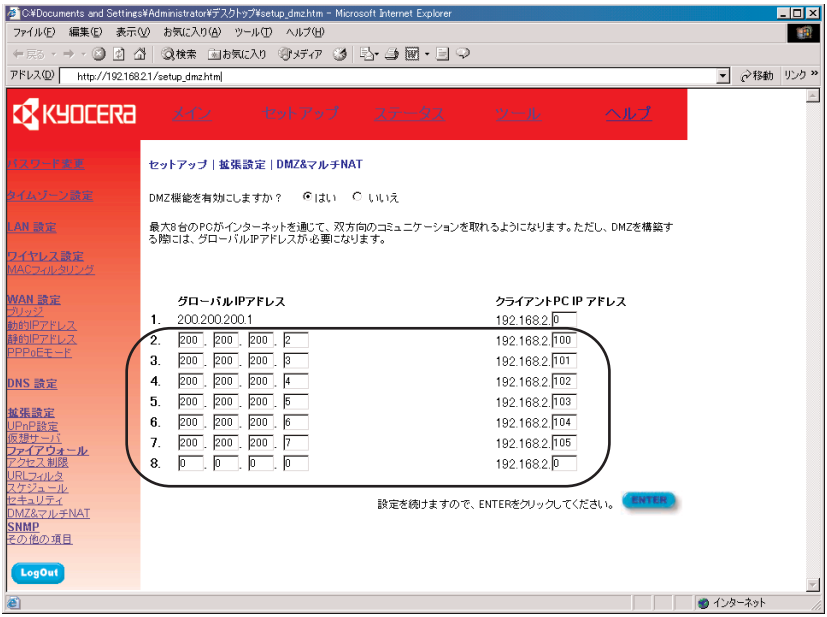
上記では、200.200.200.1～200.200.200.8の8個のグローバルIPアドレスを取得した場合の設定を示していますが、このうち、200.200.200.1はネットワークアドレス、200.200.200.8はブロードキャストアドレスとして使用されます。

また、この場合WAN側IPアドレスとして200.200.200.1が設定されているため、マルチNAT機能を使用して、ローカルIPアドレスと1対1で対応させることができるのは、200.200.200.2～200.200.200.7の6つのグローバルIPアドレスだけとなります。

1 **「DMZ機能を有効にしますか？」の「はい」を選択してください。**



2 2～7に各「グローバルIPアドレス」と対応させる「クライアントPC IPアドレス」を入力してください。
（16個以上のグローバルIPアドレスを固定的に割り当てるサービスをご使用の場合は、2～8に入力してください。



注意： マルチNAT機能を使用する場合、パソコンのローカルIPアドレスは固定で設定してください。

3 入力が完了したら「ENTER」をクリックしてください。

3-4-6　SNMP設定

ネットワークを構成するネットワーク機器を管理するための仕組みで、管理対象となる機器をSNMPエージェントといい、管理対象機器を制御する機器をSNMPマネージャといいます。

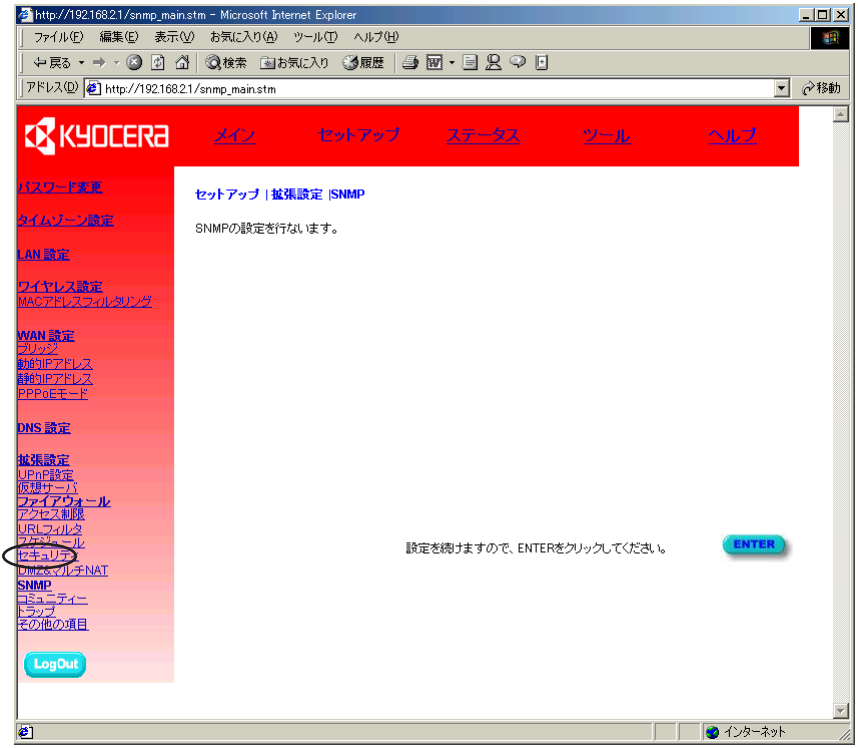
本機では、SNMPのバージョン１およびバージョン2Cを搭載しています。

本機はSNMPエージェントとして動作します。（本機背面のプリンタポートに接続されているプリンタは、管理対象外です。）

この機能をご利用になるためには別途SNMPマネージャアプリケーションが必要となります。

マネージャ側の設定についてはSNMPマネージャアプリケーションをご確認ください。

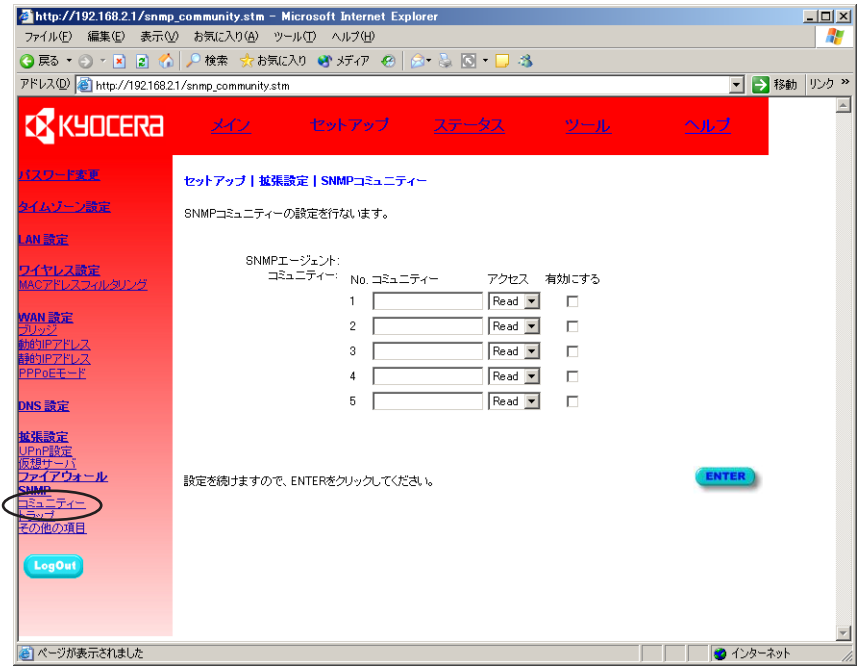
左フレームから「SNMP」をクリックすると、左フレームに「コミュニティー」と「トラップ」が表示され、SNMPの設定が可能になります。



- コミュニティー

SNMPの仕組みでは、SNMPマネージャがSNMPエージェントにアクセスし、SNMPエージェントが所有する情報を収集します。多数の機器が存在する場合を考え、それぞれのグループとして扱えるようにコミュニティーを設定します。（初期値：無効）

1 左フレームから「コミュニティー」をクリックしてください。



2 次の表を参考に設定を行ってください。

設定/表示項目	内容
No.	最大5つのコミュニティーを設定できます。
コミュニティー	SNMPマネージャと本機がやり取りを行うための名前を設定します（半角で最大16文字）
アクセス	SNMPマネージャからのアクセスに対し情報を読み出しのみの場合は「Read」を、書き込み可能にする場合は「Write」を選択します。
有効にする	登録しているコミュニティーを有効にする場合はチェックを入れます（初期値：すべて無効）

3 入力したら「ENTER」をクリックしてください。

- トラップ

SNMPエージェントで何らかの異常が発生した場合には、SNMPエージェント側から情報を送信する機能であるSNMPトラップを設定します。（初期値：無効）

1 左フレームから「トラップ」をクリックしてください。

2 次の表を参考に設定を行ってください。

設定/表示項目	内容
No.	最大5つのトラップを設定できます。
IPアドレス	SNMPマネージャのIPアドレスを入力します。
コミュニティー	SNMPマネージャと本機がやりとりを行うための名前を設定します。（半角で最大16文字）
バージョン	トラップを利用しない場合は、「無効」を選択します。 SNMPを利用する場合は、バージョン[V1]、[V2c]を選択します。

3 入力したら「ENTER」をクリックしてください。

ご相談窓口

京セラへのお問い合わせ　　2002年12月現在

製品に関する相談、および修理に関するお問い合わせは、お買い上げの販売店または下記にご連絡ください。

京セラテクニカルサービスセンター

● 0120-461-172 （一般電話よりおかけください）
受付時間： 9:00～19:00
（土・日・祝日および弊社休日
受付時間：9:00～12:00　13:00～17:00）

サービス窓口	住所
東　京	〒150-8303　東京都渋谷区神宮前6-27-8 京セラ原宿ビルB1

携帯通信は京セラ
Communication by Design

ホームページに最新情報が公開されています。
ホームページ：http://www.kyocera.co.jp/METEOR/

京セラ株式会社

V2.0