

KY-BR-WL100 KY-BR-CB100 新機能ガイド



Message Terminal On Route

1	本書につい	いて	1
2	ファーム	ウェアのアップデート方法	2
	2-1 設知	定の保存	
	2-2 フ	ァームウェアのアップデート	6
	2-3 イン	ンタフェースのアップデート	8
	2-4 設治	定の復元	
З	各機能の詞	段定方法	15
	3-1 MA	ACアドレスフィルタリング(KY-BR-WL100のみ)	
	3-2 PF	PoEによる接続の設定	
	3-2-1	PPPoEの設定	
	3-2-2	PPPoE接続の確認	
	3-3 UF	PnP(Universal Plug and Play)の設定	
	3-3-1	UPnPコンポーネントのインストール	
	3-3-2	ルータのUPnP設定	
	3-3-3	UPnP設定の確認	
	3-4 フ	ァイアウォールの設定	
	3-4-1	アクセス制限設定	
	3-4-2	URLフィルタ設定	
	3-4-3	スケジュール設定	51
	3-4-4	セキュリティ設定	53
	3-4-5	DMZ&マルチNAT設定	60
	3-4-6	SNMP設定	64

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1)にいったん変更した後にアップデートを行って

故障の原因となります。

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。

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。

名前を付けて保存						<u>?×</u>
保存する場所(1):	🗀 backup		•	G 🤣	••• 🍤	
していたつアイル						
じ デスクトップ						
ک ۱۷×د‡۲۶ ک						
ארבאעב אד דר באעב אד						
र्ण इन २७२७-७						
	ファイル名(<u>N</u>):	backup_config.exe	>		•	(<u>保存(s</u>)
	ファイルの種類(工):	アプリケーション	-		•	キャンセル

※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。

ダウンロードの完了	
ダウンロードの完了	
保存しました	
192.168.2.1 - backup_config.exe	
ダウンロード: 60.3 KB を1 秒	
ダウンロード先: C:¥Documents and¥backup_config	.exe
転送率: 60.3 KB/秒	
🔲 ダウンロードの完了後、このダイアログ ボックスを閉じる(C)	
ファイルを開く(Q) フォルダを開く(E)	閉じる

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

┃ 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。

Microsoft	Internet Explorer	×
?	アップグレードを続行してもよろしいですか?	?
	0K キャンセル	

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。

Microsoft Internet Explorer						
アップグレードが終了するまでの約1分間、本製品は応答しませ 正常に動作していますので本製品の電源は切らないで下さい						
	ОК					

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。

Microsoft	Internet Explorer	1
?	アップグレードを続行してもよろしいですか?	
	OK キャンセル	

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。

Microsoft Internet Explorer						
アップグレードが終了するまでの約1分間、本製品は応答しませ 正常に動作していますので本製品の電源は切らないで下さい						
	ОК					

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。

🗿 http://192.168.2.1/ - Microsoft Internet Explorer						
ファイル(E) 編集(E) 表示(V)	お気に入り(4) ツール(1) ヘルプ(4)	1				
G 🛤 🔹 🕤 🕐 🖪 🔮 🐔	🌡 🔎 検索 👷 お気に入り 🔮 メディア 🥹 🙆 • 📮					
アドレス(D) 🕘 http://192.168.2.1		🖌 🄁 移動				
ファームウェアアップデート	ファームウェア アップデート					
<u>ルータの再起動</u>	入手したファームウェアのアップデートファイルの存在するバスを、ファイルを抱入力し、STARTEクレックしてびださし。 アップデートファイルでないファイル名は、絶対こ入力しないように注意してびたさしなる、アップテート中は、パンコン及びルータの電源を、絶対 にちのないよりご意見てびため、					
	アップグレード対象: ファームウェア 🔽					
	参照					
	姓の る					
ページが表示されました	I ■ 425-7	<u>ب</u> ه او				

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。

ファイルの選択					<u>? ×</u>
ファイルの場所型:	🗀 backup		•	G 🤣 📂 🎫	
は 最近使ったファイル び デスクトップ マイ ドキュメント で マイ ニンピュータ で 、 、 、 、 、 、 、 、 、 、 、 、 、	backup_configex				
Y1 ホットファク	- (1.7.0.0				(BB/(O))
	ファイル:谷(N): ファイルの種類(T):	backup_contig.exe			第10
	ノアイノレの理想(1):]すべてのファイル (*.*)		<u> </u>	***2727

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。



 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。

💁 http://19216821/wireless_mac.stm - Microsoft Internet Explorer 📃 🔍						
ファイル(E) 編集(E) 表示(V) お気(に入り(A) ツール(T) ヘルプ(H) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1						
→戻る・→・③ 2 2 2 (2)検索 回ね気に入り (3)メディア (3) 12・2 回・3 ♀						
アドレス(D) 📑 http://192.168.2	1/wireless_mac.stm 💌 必移動 リンク »					
KYOCERa	242 Ref 297 22-32 21-32 All 1					
1720-F#R	セットアップ ワイヤレス MACアドレスフィルタリング					
タイムゾーン設定	MACアドレスフィルタリングを利用すると、本体に登録されていないコンピュータからのアクセスを制限すること ができます。					
LAN 該定	・本様が構成するネットワークへの接続を許可するMACアドレスを登録方法と禁止するMACアドレスを登録方 法があります。登録タイプを選択してください。					
ワイヤレス設定 MACアドレスフィルタリング						
WAN 設定 ブリッジ	フィルタリング機能を使用しますか?					
動 <u>的IPアドレス</u> 静 <u>的IPアドレス</u> PPPoFモード	登録タイプ:					
	MACアドレス一覧					
DNS 設定	番号 MACアドレス					
拉張設定	1					
<u>UPnP設定</u> 仮想サーバ	2 : : : : : : : : : : : : : : : : : : :					
<u>ファイアウォール</u> SNMP	3					
その他の項目	4					
LogOut	5					
	6					
	7					
	8					
(a)						

- 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。
- 🔏 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

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。

Anttp://192.168.2.1/isp.stm - Microsoft Internet Explorer								
ファイルビ 編集(1) 表示(2) お気に入り(4) ツールロ ヘルブ(1)								
🔾 戻る • 🕘 · 💌 🔹 🏠	◎ 戻る・ ◎ ・ ◎ ② 🏠 🔎 検索 🧙 お気に入り 🧐 メディア 🕗 😥・ 🦆 🔕 ・ 🖵 🌋							
アドレス(型) 🚑 http://192.168.2.	1/isp.stm				🚬 🔁 移動 リン:	5 »		
🕵 КУОСЕКА	<u>×112</u>	セットアップ	<u>77-97</u>	<u>ツール</u>	<u>~r</u>	*		
バスワード東東	セットアップ WAN	設定 PPPoEモード						
<u>タイムジーン講定</u> LAN 設定	インターネットへの接 接続先(プロバイダ名 必要に応じて接続先	徳に関する設定/変更を行 いを8ヶ所まで登録することが を切り替えることが可能です。	うことができます。 いでき、 。					
ワイヤレス設定 MACアドレスフィルタリング	・ブロバイダから連絡 ・利用する接続先くブ	されたユーザー名などの情報 コバイダ名)をリストより選択	網を「設定/変更」を押して) してください。	入力してください。				
WAN 設定	接待先一覧:							
<u>2092</u> 動的IPアドレス	番号 ユーザー名	接続先名	設定/変更	使用				
<u>静的IPアドレス</u> PPPoEモード			設定/変更	00 P				
TT OCC	2			5977 I				
DNS 設定	4							
越張設定	5			7UP				
UPnP設定 仮想サービ	6		設定/変更	5UP [
ファイアウォール	7		設定/変更	クリア 🗖				
その他の項目	8		設定/変更	<u> クリア</u>				
LegOut)		設定を抱けます。	かで、ENTERをクリックしてく	ださい。 (ENTER)		F		
巻] ページが表示されました					🕗 インターネット	11.		

「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。

Attp://192.168.2.1/wan_pppoe.stm/1 - Microsoft Internet Explorer							
ファイル(E) 編集(E) 表示(M) お気に入り(A) ツール(E) ヘルブ(E) 🥂							
🔇 戻る 🔹 🕤 🔹 👔 🐔	③ 戻る ▼ ③ ▼ 図 👔 🏠 🔎 検索 ☆ お気に入り 🔮 メディア 🥹 🙆 ▼ 😓 📓 ▼ 💭 33						
アドレス(型) 💩 http://192.168.2	アドレス(1) 👩 http://19216821/wan.pppoe.stm/1 📃 🛃 移動 リンク »						
KYOCERa	<u> 247 /</u>	セットアップ	<u>ステータス ツール ヘルプ</u>				
パスワード変更	セットアップ WAN 読む	全 PPPoE詳細	設定				
タイムワーン開定	PPPoEプロトコルによる持 ス名」はプロバイダより指	続設定を行いま。 定がある場合の。	す。下記の項目に、プロバイダより送付された情報を入力して下さい。「サービ み入力して下さい。				
LAN 設定	PPPOE EZETER						
	接続先名(プロバイダ名)		isp-a				
<u>MACアドレスフィルタリング</u>	ユーザー名		taro1234@isp-a.ne.jp				
WAN 設定 ブリッジ	パスワード		••••				
動 <u>的IPアドレス</u> 静的IPアドレス	パスワードの確認入力		••••				
PPPOEE	サービス名						
DNS 設定	MTU值		1454 (1440<=MTU(直<=1492)				
<mark>越張設定</mark> UPnP設定	自動切断までの時間		10 (分) 🗹 自動再接続				
仮想サーバ ファイアウォール SNMP			接続 切断				
その他の項目		10¢					
LogOut		EX.AE	2000 1 4 9 0 C ENTEN2 2 9 9 2 C C C C C C C C C C C C C C C				
			-				
」 ② ページが表示されました			ـــــــــــــــــــــــــــــــــــــ				

「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。

http://192.168.2.1/wan_pppor	e.stm/1 - Microsoft Internet i	Explorer			_ 🗆 ×
ファイル(E) 編集(E) 表示(<u>U</u>) お気に入り(<u>A</u>) ツール(①	ヘルプ(旦)			18
⇔戻る・⇒・③ 🕄 🖄	②検索 国お気に入り	@xf17 3	B- 3 🗑 - E 🖓		
アドレス(D) 🍯 http://192.168.2	.1/wan_pppoe.stm/1			•	∂ 移動 リンク ※
🛿 KYOCERA	<u>x72</u> t	Zットアップ	25-92	<u>2-11</u>	.ルプ
<u>バスワード変更</u>	セットアップ WAN 読	定 PPPoE詳4	建設定		
タイムゾーン設定	PPPoEプロトコルによる招 い。「サービス名」はプロ、	B続設定を行いま バイダより指定力	tす。下記の項目に、ブロバ がある場合のみ入力して下る	イダより送付された情報を入り すい。	わして下き
LAN 設定	PPPoE 認証設定				
ワイヤレス設定	接続先名(ブロバイダ名)		isp-a		
MACアドレスフィルタリング	ユーザー名		taro1234@isp-a.ne.jp		
WAN 設定	バスワード		****		
<u>20ッシ</u> 動的IPアドレス	バスワードの確認入力		****		
証的IPアドレス PPPoEモード	サービス名				
DNS 設定	MTU値		1454 (1440<=MTU値<=	1492)	
to ze sa co	自動切断までの時間		10 (分) 🗹 自	動再接続	
<u>UPnP設定</u> 仮 <u>想サーバ</u> ファイアウォール			接続切断		_
<u>SNMP</u> その他の項目	この接続を使用するIPア	ドレスの範囲:			
			192.168.2. 0 ~0		
Logour			192.168.2. 0 ~0		
	l		192.168.2. 0 ~0	J	
		設定を続け	ますので、ENTERをクリック		, _
(で) ページが表示されました				〇〇 10	·ダーネット //

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。

http://192.168.2.1/isp.st ファイル(F) 編集(F) 表示(M)	m - Microsoft Internet Exp お気に入り(A) ツール(T)	olorer ヘルプ(H)			
③ 戻る ▼ ③ × 図 ■ ☆	- 検索 ☆ お気に入り 🔮		5 0 · 🗆 🚳		
アドレス(D) (1) http://192.168.2	/isp.stm				F 参 移動 リンク ※
KYOCERa	<u>247</u> t	ットアップ 2	(<u>7-92</u>	<u>ツール</u>	
1720-FRE	セットアップ WAN 設定	PPPoEモード			
<u>タイム-ジーン論定</u> LAN 設定	インターネットへの接続に関う 接続先(ブロバイダ名)を8ヶ月 必要に応じて接続先を切り替	トる設定/変更を行うこ。 行まで登録することができ えることが可能です。	とができます。 き、		
<mark>ワイヤレス設定</mark> MACアドレスフィルタリング	・ブロバイダから連絡されたニ ・利用する接続先(ブロバイダ	1ーザー名などの情報を 名)をリストより選択して	「設定/変更」を押してア べださい。	、力してください。	
WAN 高定 フリンジ ジョンアドレス 静知アアドレス 静知アアドレス 静知アアレス 野中ロモード DNS 語定 リアの作数定 フレイアウォール SNMP その道の項目 LogOut	接続先一覧:	接続先名 [sp-a] [] []]]]]]]]]]]]]]]]	 設定/変更 	使用 クリア マ クリア ロ クリア ロ ク	>
ページが表示されました					▼ ▼ ▼ 1ンターネット

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。

Microsoft Internet Explorer	×
? ルータを再起動します。	
0K ++>>セル	

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。

Microsoft	Internet Explorer X
⚠	再起動が完了するまで、ルータの電源を切らないで下さい。
	<u>OK</u>

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

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。

ahttp://192.168.2.1/statu	us.stm – Microsoft Inter	net Explorer					- 🗆 🛛
ファイル(E) 編集(E) 表示(() お気に入り(A) ツール(T) ヘルプ(H)							A.
③ 戻る • ③ • 🗑 👔 🏠 🔎 検索 🏂 お気に入り 🔮 メディア 🕹 🙆 •							
アドレス(D) 🧃 http://192.168.2.1/s	status.stm					🖌 🔁 租	動 リンク ³⁰
KYOCERa	<u>2402</u>	<u> セットアップ</u>	ステータス	<u> </u>	<u>-11-</u>	ヘルプ	
<mark>ステ</mark> 現在	テー <mark>タス</mark> 主時刻01/01/2002 00:01:49						
イン Cabi WAA サイ フラ セカ 服	2 クーネット 4075 に 巻税 15まい そスク: 255,255,0 5まい マスク: 255,255,0 1-ウマイ:00,000,000,000 1-ママリのNS: 000,000,000 1-ママリのNS: 000,000,000 1-ジダリのNS: 000,000,000 1-ジダリのNS: 000,000,000	グートウェイ IP アドレス: 102:10 サブネルマスク: DHCP サーバ: 有 ファイアウォール:	8.2.1 265.265.255.0 动 有.5%	インフラ DHCPグ コードア ブートコ LANボー WANボー シリアル	オメーション ワライアント数:1 トージョン:VL03E(Aug 52) トレパークラン:VL00 トのMACアドレス:00-00-0 ウェアバージョン:01A (ナンバー:A123450789	002 10:19:18) 0-00-00-00 0-00-00-00	
900 890 890 890 890 890 890 890 890 890	POE Status (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	978-17025 255255250 255255250	ở~ŀ?⊊.4 000.000.000 000.000.000 000.000.000	794795018 000.000.000.000 000.000.000	1230-29 30045 000.000.000 000.000.000 000.000.000	解放 書換 解放 書換	_
tz+ Wat	キュリティログ N側からルータへのアクセス情報	۶.	DHCPクライ 現在ゲートウ.	アントログ ェイに接続されているE	DHCPクライアント情報		
	/01/2002 00:00:05 PPP. /01/2002 00:00:00 PPP. /01/2002 00:00:00 PPP. /01/2002 00:00:00 PPP. /01/2002 00:00:00 PPP. /01/2002 00:00:00 PPP. /01/2002 00:00:00 PP. /01/2002 00:00:00 PP. /01/2002 00:00:00 Dia	E receive PADT El start PPP El receive PADS Es send PADR DE receive PADD Es send PADI De cecive PADT I On Demand(PPPoE2	ip=192.163	8.2.100 mac=00	-40-28-80-28-E8	8	
(R	存						*
ê						🥥 インターネッ	小 _;;

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	0	0	0
音声チャット	0	0	0
ビデオチャット	0	0	—
電話をかける(.NET Voice Services)	0	×	×
ファイルの送受信	0	0	0
アプリケーション共有	0	0	—
ホワイトボード	0	0	_
リモートアシスタンス	0	0	—

- 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 (O3-xxxx-xxx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「 $^{\mathcal{V}}$ 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 のバージョン情報 🛛 🗙
	Windows* Messenger
<	Windows Messenger Version 4.7 (4.7.0105) Convicient (C) 1007-2002 Microsoft Corporation All rights reserved
	RSA Data Security Inc. からライセンス契約を受けたセキュリティソフトウェ アを搭載しています。
	OK

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。 「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。

🐻 プログラムの追;	加と削除		
	現在インストールされているプログラム:	並べ替え(<u>S</u>): 名前	~
プログラムの 変更と削除(H) プログラムの 追加(N)	 Adobe Acrobat 4.0 <u>サポート情報を参照するには、ここをクリックしてください。</u> このプログラムを変更したり、コンピュータから削除したりするには、[変更] または 削除: (ださい。 Angel Line for Windows Ver3.00 AudioRack p3.11 COLOR IMAGING LABO2 	サイズ 使用頻度 最終使用日 200] をクリックして 変更 サイズ サイズ サイズ	8.63MB 低 1、12/29 前明除 1.54MB 1.78MB 1.784MB
Windows ユノポーネントの 道加と肖明徐(A)	 EPSON ImagePalette EPSON PhotoQuicker3.0 EPSONフリンタトライパ・ユーテルフィ KYOCERA Wireless LAN AP Manager ODN Online Signup Kit Prius 壁紙 	サイズ サイズ サイズ	9.09MB 28.60MB 0.37MB
	g QuickCam 명 RealPlayer 4.0 ጩ SmaHey	サイズ	95.21 MB 1.27 MB
	聞 So-net Online Signup SuperDisk フォーマットユーティリティ	サイズ サイズ	0.01 MB 0.59 MB
			閉じる(②)

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。

Windows コンポーネント ウィザード	\mathbf{X}
Windows コンボーネント Windows XP のコンボーネントを追加または削除できます	
各チェック ボックスをクリックして、追加または削除するコン ボックスは、コンボーネントの一部がインストールされること を表示するには、国新細」をクリックしてください。 コンボーネント©:	パーネントを選んでください。影付きのチェック で表します。コンポーネントに含まれているもの
	0.0 MB 🔼
く ジネットワーク サービス	0.3 MB
▶ 12 小一下証明者の更新	U.U MB
□ 言意管理とモニタ ツール	1.9 MB 🥃
説明: 特別なネットワーク関連のさまざまなサー	-ビスやプロトコルが含まれています。
必要なディスク領域の合計: 0.0 MB	=¥¢m/D\
空きディスク領域: 841.5 MB	
	< 戻る(B) 次へ(N) > キャンセル

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。

ネットワーク サービス	
各チェック ボックスをクリックして、追加または削除するコンボーネントを選んでくだ ボックスは、コンボーネントの一部がインストールされることを表します。コンボーネ を表示するには、国料細目をワリックしてください。 ネットワーク サービス のサブコンボーネント(の):	さい。影付きのチェック ントに含まれているもの
	<u>0.0 MB</u>
▲ 単ユニハーサル フラク アンド フレイ 山、 ■簡易 TOP/IP サービス	0.0 MB
説明: コンピュータでユニバーサル ブラヴ アンド ブレイ デバイスの検討	出や制御をします。
必要なディスク領域の合計: 0.0 MB 空きディスク領域: 840.3 MB	[詳糸田(D)
ОК	**>セル

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。

Windows コンポーネント ウィザード		
Windows コンボーネント Windows XP のコンポーネントを追	加または削除できます。	
各チェック ボックスをクリックして、 追 ボックスは、コンボーネントの一部が を表示するには、 耳半細1 をクリック コンボーネント(Q)・	珈琲をは削除するコンボーネントを バインストールされることを表します。 してください。	遅んでください。影付きのチェック コンボーネントに含まれているもの
🗆 言うそのほかのネットワーク ファ	ァイルと印刷サービス	0.0 MB 🔼
🗷 🎫 ネットワーク サービス		0.3 MB
☑ 🖾 ルート証明書の更新		0.0 MB
□ 📑 管理とモニタ ツール		1.9 MB 🥃
説明: 特別なネットワー:	ク関連のさまざまなサービスやプロト:	コルが含まれています。
必要なディスク領域の合計: 空きディスク領域:	0.0 MB 839.7 MB	■ Ĭ¥糸囲(<u>D</u>)
	< 戻る(<u>B</u>)	(次へ(1)) キャンセル

Windows コンポーネント ウィザード	\mathbf{X}
コンボーネントの構成 要求した構成の変更を適用しています。	B
コンボーネントを構成しています。しばらくお待ちください。選択したコンボーネントによって、 少々時間がかかることがあります。	
状態 インターネット ゲーム の構成を完了しています	
< 戻る(B) 次へ(N) >	

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。



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。

	MSN Messenger のバージョン情報
	Messenger
	MSN Messenger
\triangleleft	Version 5.0 (5.0.0540)
	Copyright (C) 1997-2002 M[gosoft Corporation. All rights reserved.
	RSA Data Security Inc. からライセンス契約を受けたセキュリティ ソフトウェ アを搭載しています。
	<u> </u>

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。

🗶 DirectX 診断ツール
システム DirectX ファイル ディスプレイ サウンド ミュージック 入力 ネットワーク それでも問題が解決しない場合
このツールを使うと、インストールされている DirectX コンポーネントやドライバの詳細情報を入手することができます。また機能のテスト、問題の 診断、システム構成の最適化なども実行できます。
どの分野が問題を起こしているか分かっている場合は、適当なタブをクリックしてください。それ以外の場合は、D欠ページ]をクリックしてください。
[それでも問題が解決しない場合] のページでは、問題解決に利用できるそのほかのツールの一覧を表示します。 ←システム情報
現在の日時: 2002年7月16日, 1558:30
コンピュータ名: User
オペレーティング システム: Microsoft Windows ME (4.90, Build 3000)
言語:日本語(地理設定:日本語)
JUC277: Intel PentumIII, 800MHz
スモジー 192/110 (小田) 161/100 (中田市約)
DirectX (1+3) Child (1991) DirectX 81 (40801 0881)
DxDiag 4.08.01.0881 Copyright (C) 1998-2001 Microsoft Corporation. All rights reserved.
ヘルプ(出) (ホパージ(U) 情報をすべて保存(S) 終了 (S)

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。

アプリケーションの追加と削り除のプロパティ					
インストールと削りを Windows ファイル 記動ディスク					
フロッピーディスクまたは CD-ROM から新しいプログラムをインストー ルするには、ビインストール]をクリックしてください。					
[<u>1526-</u> µ \$]					
次のソフトウェアは自動的に背単命できます。プログラムを削除した り、インストール済みのコンポーネントを変更するには、一覧から選 択して「自加と削除」をクリックしてください①					
AdjustClock Adobe Acrobat 5.0 Aplix WroOR 6.0 ATI ディスフレイ ドライバ ユーティリティ Black JumboDog File Visor4 FinePrint 2000 FinePrint 2000 HP Desk Jet 895C Series 領除専用) KaoRu					
适加之前服余(B)					

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。

アプリケーションの追加と削除のプロパティ	? ×
インストールと削除 Windows ファイル 起動ディスク	
各チェックボックスをクリックして、追加または削除するファイルを選択 付きのチェックボックスは、コンボーネントの一部だけがインストール。 します。 賃料細」をクリックすると、コンボーネントの内容が表示されま	てしてください。影 されることを意味 さす。
コンポーネントの種類(<u>C</u>):	
✓ 4 マルチメディア	7.4 MB 🔺
☑ 🐷 ユーザー補助	4.7 MB
	5.3 MB
□ 🔕 複数の言語サポート	0.0 MB 💌
インストール済みコンポーネントのディスク領域: 必要なディスク領域: 空きディスク領域: 説明 (ほかのコンピュータやオンライン サービスとの達信に使うアクセサリ	432 MB 0.0 MB 2664.6 MB です。
選択数: 4/10 個 詳	細(D)
<u><u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u></u>	入夕使用(<u>H</u>)
OK キャンセル	適用(<u>A</u>)

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。

ì	通信	2	хI	
	コンボーネントをインストールするには、コンボーネントのチェッ (ださい。インストールしないコンボーネントのチェック ボックス きのボックスは、コンボーネントの一部だけがインストールされ コンボーネントの一覧を表示するには、国幹細」をクリックして	ウ ボックスをオンにして はオフにします。影付 ふことを意味します。 ください。		
	コンポーネントの種類():			
	■ 🖾 ダイヤルアップ ネットワーク	0.0 MB 🔺		
<	🗾 💻 ユニバーサル ブラグ アンド ブレイ	0.4 MB	2	
	□ ■ 仮想プライベート ネットワーク	0.0 MB 💌		
	インストール済みコンボーネントのディスク領域: 必要なディスク領域: 空をディスク領域: =888	43.2 MB 0.3 MB 2659.1 MB		
	コニバーサル ブラヴ アンド ブレイを使用すると、Window の間で、シームレスな接続や通信が可能になります。	s と高機能装置と		
		詳細(0)		
	OK ++>セル			

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。

アプリケーションの追加と削除のプロパティ	? ×
インストールと削除 Windows ファイル 起動ディスク	
各チェックボックスをクリックして、追加または削除するファイルを選択してくださ 付きのチェックボックスは、コンボーネントの一部だけがインストールされることを します。『詳細』をクリックすると、コンボーネントの内容が表示されます。	,)。影 意味
コンポーネントの種類(<u>C)</u> :	
✓ 払マルチメディア 7.4 MB	•
✓ 【▲ユーザー補助 4.7 MB	
✓ 今通信 5.3 MB	
□ 🔕 複数の言語サポート 0.0 MB	•
インストール済みコンボーネントのディスク領域: 432 ME 必要なディスク領域: 00 ME 空きディスク領域: 2664.6 ME 説明 (ほかのコンピュータやオンライン サービスとの3動信に(使うアクセサリです。	
選択数:4/10 個 詳細(D)	
ディスク使用()	Ð
OK キャンセル 適用	(<u>A</u>)



「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。

システム設定の変更					
?	新しい設定を有効にするには、コンピュータを再起動する必要があります。 今すぐ再起動しますか?				
	<u>(ぱい(?)</u> いいえ(<u>N</u>)				

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。

🦠 ネットワーク接続			
ファイル(E) 編集(E) 表示	〒① お気に入り)(A) ツール(T) 詳細設定(N) ヘルプ(H)	AU
3 戻る - 🌖 - 🎓 🏓	🔎 検索 🌔 フォ	лиў 🛄 -	
アドレス(D) 🔕 ネットワーク接	続		🖌 🄁 移動
ネットワーカ ねつか	8	LAN または高速インターネット	<u>^</u>
*)F5 5 5A5		ローカル エリア接続	
関連項目	۲	名効 BUFFALO LPC3-CLX Fast Ether	
えの第			
COIR	U	129-491 9-1911	-
	۲	WL100 上の WAN-1 接続	
		インターネット接続	
			_
			~

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。

💐 WL 100 上の WAN-1 ወታ ወለታ ብ
全般
インターネットへの接続方法
🧐 WL100 上の WAN-1
この接続を使うと、ほかのコンピュータにある共有接続をとおしてインターネットへ接続できます。
設定(g)
☑ 接続時に通知領域にインジケータを表示する(型)

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。

😻 マイ ネットワーク	
ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)	A.
③ 戻る 🔹 🌖 🔹 🏂 🔑 検索 🌔 フォルダ 🛄・	
アドレス(2) 🧐 マイ ネットワーク	💙 芝 移動
ローカル ネットワーク	
ネットワーク タスク 🔹	
 	
その他 😵	
IF和	

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。

METEORのプロパテ	ſ	×
全般		
	METEOR	
製造元:	Kyocera	
モデル名:	METEOR	
モデル番号:	KY-BR-WL100	
i兑8月:	METEOR KY-BR-WL100	
デバイスのアドレス:	http://192.168.2.1/	
	開じる キャンセル	

Windows Me

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。

http://192.168.2.1/firewall main.stm - Microsoft Internet Explorer _ 🗆 🗵 ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H) 🔇 戻る 🔹 🕤 💌 😰 🐔 🔎 検索 👷 お気に入り 😵 メディア 🤣 🎰 💀 🕞 📮 🦓 Name
 Nam
 Nam
 Nam
 アドレス(D) 🍯 http://192.168.2.1/firewall_main.stm **KX**KYOCERa 「スワード変更 セットアップ | 拡張設定 |ファイアウォール ファイアウォールを使用するためには「使用する」を選択し「ENTER」アイコンをクリックしてください。ファイアウォール機 能を有効にすると、SPI、DOS攻撃防御機能、クライアントPCのアクセス制限(クライアントフィルタリング)、DMZ、マルラ 等の設定が行えます。より安全な環境お使いいただくため、ファイアウォールを「使用する」に設定することをお勧めしま マルチ <u>AN 設定</u> <u> アイヤレス設定</u> ファイアウォール機能を使用しますか? 💿 使用する 🔘 使用しない VAN 設定 的IPアドレス 設定を続けますので、ENTERをクリックしてください。 DNS 設定 **女張設定** JPnP設定 ベッシュー ファイアウォール アクセス制限 IRLフィルタ (<u>ケジュー)</u> 2キュリティ DMZ&マルチNAT SNMP その他の項目 🗌 🥝 インターネット e1

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>

┦ 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。

🗿 http://192.168.2.1/firewall_a.stm - Microsoft Internet Explorer					
ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(D) ヘルプ(H) 🧗					
🔾 戻る ㅋ 🕥 - 💌 👔 🔮	\│ 🔎 検索 , st気に入り 🔮 メディ	P 🔗 🔗 🗟 🖬 = 🖵 🚳			
アドレスの (1) 10216821/firewall_astm					
KYOCERa	<u>×12</u> tyl7	ップ <u>ステータス ツー</u> ル	<u>Arz</u>		
パスワード業更	セットアップ 拡張設定 アクセス	則限			
タイムワーン設定	特定のパリコンに対して、外部へのア	クセスを制限することができます。制限方法には、「	コーカルIPアドレスの指定による		
LAN設定	制限と、MACアドレスの指定による制	限の2つの方法があります。			
<mark>ワイヤレス読定</mark> MACアドレスフィルタリング	• アクセス制限機能を使用しますか? C 使用する C 使用しない				
WAN 設定 ブリッジ 動的IPアドレス	• IPアドレスによるアクセス制限(最大10ワークグループ)				
静的IPアドレス PPPoEモード	ワークグルー ローカルIPアド ブ名 レス	アクセス制限内容	スケジュー ル 編集削除		
DNS 設定		登録されていません			
<mark>拡張設定</mark> UPnP設定 仮想サーバ	<u>ワークヴルーゴの追加</u>				
ファイアウォール アクセス制限 UPIフィルタ	• MACアドレスによるアクセス制限(最大32台)				
スケジュール	番号	MACアドレス			
DMZ& TILFNAT	1				
SNMP その他の項目	2				
	3				
LogOut	4				
	5		_		
e			<u>२</u> ४२४ - २०४ - 🖉		

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。

http://192.168.2.1/accessControlAdd.stm - Microsoft Internet Explorer					_D×	
ファイル(E) 編集(E) 表示(V) お気(こ入り(A) ツール(T) ヘルプ(H) 🧤						
G 戻る • 🕤 · 🖹 💈 🔮	↓	🕂 አቻィア 😁 🙆)• 💺 🐨 • 🖵 🚳			
アドレス(D) 🥘 http://192.168:	2.1/accessControlAdd.stm				No. 100 (100 - 100	
KYOCERa	<u>342</u>	セットアップ	<u>77-97</u>	<u>ツール</u>	<u>ヘルプ</u>	
<u>1129-FRE</u>	セットアップ 拡張設定	ワークグルーブの追	Int			
タイムゾーン設定	ワークグループを追加し、# ケーションで追加することか	叫限するアプリケーショ Fできます。	ンを選択することができます。ま	た、リストに載っていないアプリケー	ションは、新規アプリ	
LAN 該定 ワイヤレス設定	• ワークグループ名:					
MACアドレスフィルタリング	 ローカルIPアドレス 	: 192.168.2. 0 ~ C	1			
WAN 設定 ブリッジ	 アクセス制限内容・ 					
<u>動的IPアドレス</u> 静的IPアドレス	アプリケーショ	ン チ	ロトコル/ボート番号		制限する	
PPPoEE-F	WWW	н	TP, TCP ポート 80, 3128, 800	00, 8080, 8081		
DNS 設定	URLフィルタ	н	TP (URLフィルタの設定画面参	1照)		
拉張設定	メール送信	SN	ITP, TCP ポート 25			
<u>UPnP設定</u> 仮想サーバ	ニュース	NI	NTP, TCP ポート 119			
<u>ファイアウォール</u> アクセス制限	メール受信	PC	P3, TCP ポート 110			
URLフィルタ スケジュール	HTTPS	н	TPS, TCP ポート 443			
セキュリティ DMZ&マルチNAT	FTP	FT	P, TCP ポート 21			
<u>SNMP</u> その他の項目	Teinet	то	Pポート 23			
	AOLインスタント	メッセンジャー AC	L Instant Messenger, TCP ポ	·		
LogOut	DNS	UE	DPポート 53			
	SNMP	UE	DPポート 161, 162			
	VPN-PPTP	тс	Pポート 1723			
	TCP		てのTCPポート			
	UDP		てのUDPポート			
			新規アブリケーショ	aン		
	小一「單四田」					
	 スケジュール(スケ) 	ジュール設定画面参照): 常に制限する 💌			
OK キャンセル ▼						
🕘 ページが表示されました					インターネット //	

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。

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。)

🖉 http://192.168.2.1/firewall_a	astm - Microsoft Internet Explorer	
ファイル(E) 編集(E) 表示((火) お気に入り(A) ツール(T) ヘルブ(H)	1
(中戻る ▼ ⇒ → 🙆 🖾 🖆	🖞 ②検索 国は気に入り ③ゲイア 🎯 🛂・🤩 🔟・ 🖯 🍳	
アドレス(D) (32.1/firewall_a.stm	
セキュリティ DMZ&マルチNAT	• MACアドレスによるアクセス 制限(最大32台)	
<u>SNMP</u> その他の項目	Index MACアドレス	
	1	
LogOut	2 : : : : : : : : : : : : : : : : : : :	
	3 🗌 : 🖂 : 🖂 : 🖂 : 🖂	
	4 🗌 : 🔂 : 🔂 : 🔂 : 🔂	
	5	
	6	
	7	
	8	
	9	
	10::::::	
	25	
	26::::::	
	27	
	29::::::	
	30::::::	
	31::::::	
	32	
		\frown
	設定を続けますので、ENTERをクリックしてください	
e i		 インターネット

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。

http://192.168.2.1/firewall_u	ıstm - Microsoft Internet Exp	orer				<u>- 🗆 ×</u>
ファイル(E) 編集(E) 表示(⊻) お気に入り(<u>A</u>) ツール(T)	ヘルプ(円)				
(+) 戻る ▼ ⇒ ▼ (2) (2) (2)	②検索 画お気に入り	জিংগন 🎯 🔤 🤅) 🗹 • 🗐 • 🖾 •	10%	<u> </u>	
アドレス(D) 🕘 http://192.168:	2.1/firewall_ustm				▶ 🖓移動	925 ×
KYOCERA	<u>x1</u> 2 te	ットアップ <u>ス</u>	<u>7-92</u>	<u>u-n</u>	<u> ヘルプ</u>	Î
パスワード東東	セットアップ 拡張設定	URLフィルタ				
タイムゾーン講定 LAN 読定	URLアドレスまたはキーワ アクセスを制限することが・ 設定を行う時に、URLフィル	ード(URLアドレスに含ま できます。アクセス制限を ッタを選択してください。	れている文字列)を設 行う場合は、アクセス	定することで、 該当 2、制限の 設定画面で	するWebサイトへの ミ、ワークグループの	
<mark>ワイヤレス設定</mark> MACアドレスフィルタリング	Index Site 1	URL / キーワード	Index Site 16	URL/+·	ーワード	
WAN 設定 	Site 2		Site 17			
<u>動的IPアドレス</u>	Site 3		Site 18			
<u>朝的ビアトレス</u> PPPoEモード	Site 4		Site 19			
DNS 풍순	Site 5		Site 20			
DITS BOR	Site 7					
<u>拡張設定</u> UPnP設定	Site 8		Site 23			
<u>仮想サーバ</u> ファイアウォール	Site 9		Site 24			
アクセス 制限 URI フィルタ	Site 10		Site 25			
ス ケジェール セキュリティ	Site 11		Site 26			
DMZ	Site 12		Site 27			
<u>SNMP</u> その他の項目	Site 13		Site 28			
	Site 14		Site 29			
Logout	Site 15		Site 30			
		設定を続ける	全てクリア ますので、ENTERを分	リックしてください。	ENTER	
 ページが表示されました 					🔮 インターネット	-

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。

🖉 http://192.168.2.1/firewall_ru	ule.stm – Microsoft Internet Expl	orer	
ファイル(E) 編集(E) 表示()	かうしょう (A) ツール(T)	ヘルブ(圧)	
수 戻る 🔹 🔿 🔹 🙆	②検索 国お気に入り 🍕	🦻 がっ 🧭 🔁 🐨 🖓 🔍	
アドレス(D) 🙆 http://192.168.2	2.1/firewall_rule.stm		▼
KYOCERa	<u>x1</u> 2 to	トアップ <u>ステータス ツー</u> ノ	k Alž
<u>パスワード変更</u>	セットアップ 拡張設定	マケジュール	
<u>タイムゾーン設定</u>	アクセス制限を行うスケジュ に、登録したスケジュールを	ールを登録できます。アクセス制限の設定画面で、「 選択してください。	フークグループの設定を行う時
LAN 設定			
<mark>ワイヤレス設定</mark> MACアドレスフィルタリング	 スケジュールリスト(最大10件まで)	
	登錄名	コメント	編集/削除
<u>ブリッジ</u>	test01	testtest	編集削除
<u>動的IPアドレス</u> 静的IPアドレス PPPoEモード	スケジュールの追加	\triangleright	
DNS 設定			
<mark>拡張設定</mark> UPnP設定 仮想サーバ		設定を続けますので、ENTERをクリック	わてください。 ENTER
<u>ファイアワォニル</u> アクセ <u>ス制限</u> URLフィルタ			
<u>スケジュール</u> セキュリティ			
DMZ&マルチNAT			
<u>SNMP</u> <u>その他の項目</u>			
LogOut			Y
🥶 ページが表示されました			

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。

🚈 http://192.168.2.1/firewall_ru	ule_a.stm - Microsoft Interne	t Explorer				<u> </u>
J ファイル(E) 編集(E) 表示	:(⊻) お気に入り(<u>A</u>) ツール	(日) くこう(日)				
↓ 仲戻る ▾ ⇒ ▾ 🙆 🖞 (🖞 🔍検索 🖻 お気に入	り 🥝履歴 🏻 🎒 🔟 🔹	<u> </u>			
アドレス(D) 🛃 http://192.168	.2.1/firewall_rule_a.stm				•	@移動
KYOCERa	<u>347</u> 2	セットアップ 2	17-92	<u>""-""</u>	ヘルプ	
<u>パスワード水正</u>	セットアップ 拡張設定	スケジュールの設定				
タイムゾーン設定	登錄名:					
LAN設定						
<mark>ワイヤレス設定</mark> MACアドレスフィルタリング	コメンド. 制限する時間:				-1	
<u>WAN 設定</u> ブリッジ	BZ	開始時間(時分) 時45分-)入力例:午前8 約 ->08:45	《了時間(時分)入力例:18時15 分->18:15	i	
<u>動的IPアドレス</u> <u>静的IPアドレス</u>	毎	3	: D			
PPPoEt-r	日日	18	:	:		
DNS 設定	月時	18 🗌 :		:		
	火間	8				
<u>していて設定</u> 仮想サーバ ファイアウォール	7/58	18 🗌 :				
アクセス制限 URLフィルタ	木町	18	-	:		
ス <u>ケジュール</u> セキュリティ	金印	18 🗌 :	· 🗆 🔰	:		
<u>DMZ&マルチNAT</u> SNMP その他の項目	±B			:		
LogOut		OK	キャンセル			•
🕗 ページが表示されました					ンターネット	//.

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。

ー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。

ー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。)

<mark>参</mark> http://192.168.2.1/firewall ファイル(E) 編集(E) 表示	_spijhstm - Microsoft Internet Explorer のの お気に入れ(A) ツール(T) へルプ(H)					
(中戻る ▼ ⇒ → 図 図)	☆ ②検索 函お気に入り ③メディア	3 B- 6) 🖩 • 🗏 🖓			
- — アドレス(①) 🍯 http://192.16	82.1/firewall_spi_h.stm				• 🔗 移動	リンク
KYOCERa	<u>メイン</u> セットアップ	' <u>27</u>	<u>\$7</u>	<u>ツール</u>	ヘルプ	
<u>「スワード変更</u>	セットアップ 拡張設定 セキュリテ	1				
イムワーン設定	SPI(ステートパケットインスペクション)お	sよび DoS 攻	「撃防御の機能を	設定することができます。		
AN 設定						
<u> ノイヤレス設定</u>	● セキュリティ機能選択					
<u>IACアドレスフィルタリング</u>	SPIおよびDoS攻撃防御	を設定する				
/AN 設定	RIF	を検出する				
加切アドレス	外部からのPing	を破棄する				
<u>#1511Pアドレス</u> 2 <u>PPoEモード</u>	• 対象アブリケーションの選択					
INS 設定	パケットフラグメンテーション					
<mark>续張設定</mark> IPnP設定	TCPコネクション	v				
<u>限サーバ</u> アイアウォール	UDPセッション	v				
<u>'クセス制限</u> RLフィルタ	FTPサービス	V				
<u>クロジョンル</u> 2キュリティ	H323サービス	V				
MIZ& JUFNAT	TFTPサービス	V				
の他の項目		_				
LogOut	 	É				
	メールアドレス :					
Ê)) インターネット	

[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	
RIPを検出する	
外部からのPingを破棄する	

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)

• 対象アブリケーションの選択

パケットフラグメンテーション	
TCPコネクション	
UDPセッション	
FTPサービス	
H323サービス	
TFTPサービス	

フラグメンテーションパケット TCPコネクション UDPコネクション FTPサービス H.323サービス TFTPサービス

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のコネクション状況を監視します。

:UDPのセッション状況を監視します。

:FTPサービスの状況を監視します。

: H.323サービスの状況を監視します。

: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。

• アラート用メールアドレス設定



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

HALF-OPENフラグメンテーション待ち時間: 10 🛚 🛛	secs
TCP SYN待ち時間: 30 sec.	
TCP FIN待ち時間: <mark>5</mark> sec.	
TCPコネクションタイムアウト時間: 3600 sec.	
UDPセッションタイムアウト時間: 30 sec.	
H323データチャンネルタイムアウト時間: 180 sec	

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インコンブリートセッション数 上限: 300	セッション
トータルTCP/UDPインコンブ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インコンブリートセッション(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: 🛽	00 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	この設定値を超えるとすべてのTCP/UDPセッションを以下
コンプリートセッション	下限値を下回るまでブロックします。
数上限:(セッション)	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	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
ートセッション数上限:	定値を超えると、セッションの削減を開始します。
(セッション)	初期値:250 範囲:1~250
TCP/UDPインコンプリ	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
ートセッション数下限:	定値を下回ると、セッションの削減を中止します。
(セッション)	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	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
テーション検出時間:	間隔を設定します。
(msec.)	初期値:10000 範囲:10~60000
フラッディングクラッカ	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
ーブロックタイム:	設定します。
(msec.)	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。

┃「DMZ機能を有効にしますか?」の「はい」を選択してください。

🏄 http://192.168.2.1/setup_dm	mzstm - Microsoft Internet Explorer				
ファイル(E) 編集(E) 表示	示(v) お気に入り(A) ツール(I) ヘルブ(H)				
◆戻る・→・◎ ◎ ☆ ◎ 検索 国お気に入り ③履歴 ● 圖・目 奥 ♀ □					
」アドレス(D) 🛃 http://192.168	882.1/setup_dmz.stm	∂移動			
KYOCERa	<u>メイン 1504797 27:352 ツル ヘルプ</u>	A			
1720-1980E	セットアップ 拡張設定 DMZ&マルチNAT				
タイムゾーン設定	DMZ機能を有効にしますか? (ではい) いいえ				
LAN 設定	最大8台のPCがインターネットを通じて、双方向のコミュニケーションを取れるようになります。ただし、DMZを構築する際に				
ワイヤレス設定 MACアドレスフィルタリング	は、グローバルIPアドレスが必要になります。				
WAN 設定	グロー いいのマドレフ クライマントロケル マドレフ				
シリン 動的IPアドレス	1. 0.0.0 192.168.2.0				
PPPOET-F	2 . 0 . 0 . 0 . 192.168.2.0				
DNC 建中	3 . 0 . 0 . 0 . 192.168.2.0				
DNS ERA-	4 . 0 . 0 . 0 . 192.168.2.0				
<u>拡張設定</u> UPnP設定	5. 0 . 0 . 0 . 192.168.2.0				
<u>仮想サーバ</u> ファイアウォール	6 . 0 . 0 . 0 . 192.168.2.0				
<u>アクセス制限</u> URI フィルタ	7. 0 . 0 . 0 . 192.168.2.0				
スケジュール	8. 0 . 0 . 0				
	設定を待けますので FNTFRをクリックしてください。				
その他の項目	acted about 3 07 ct Linter 2 5 5 7 0 ct (cc) 16				
LogOut					
		-			
@]		1.			

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

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。	>

Anttp://19216821/setup_dmz.stm - Microsoft Internet Explorer				
] ファイル(E) 編集(E) 表示	(い) お気に入り(A) ツール(T) ヘルブ(H)			
↓ ↓ 戻る ▼ ⇒ ▼ 🙆 🖄	☆ ②検索 図お気に入り ③履歴 ④ 20			
アドレス(D) 創 http://192.160	321/setup_dmz.stm		_	
KYOCERa	<u>242</u> セットアップ	<u>27-92</u> <u>2</u>	<u>-r ~rz</u>	
1720-FXX	セットアップ 拡張設定 DMZ&マルチNAT			
タイムゾーン設定	DMZ機能を有効にしますか? ⊙ はい ○ いい	ā		
LAN 設定	最大8台のPCがインターネットを通じて、双方向のコ	ミュニケーションを取れるようこな	ります。ただし、DMZを構築する際に	
ワイヤレス設定 MACアドレスフィルタリング	は、グローバルIPアドレスが必要になります。		_	
WAN 設定 ブリッジ	グローバルルアドレス	<u>ク</u> =	WZYFEC IP 7FUZ	
静的アアドレス	1. 0.0.0	192	.168.2.0	
PPPOEE		192	.168.2.U	
DNS 設定	4. 0 0 0 0	192	168.2.0	
	5. 0 0 0	192	.168.2.0	
の目的設定	6. 0. 0. 0.	192	.168.2.0	
<u>アクセス制限</u>	7. 0. 0. 0. 0	192	.168.2.0	
<u>スケジュール</u> セキュリティ	8. 0 . 0 . 0	192	.168.2.0	
DMZ& TUFNAT		設定を結けますので FNTE		
その他の項目		BARE CINED & 9 00 CC LINE	11279770 C (22010)	
LonOut				
(é)			। 🔰 🖉 ব১৯–৯৬৮ 🥢	

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200.200.1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。

┦「DMZ機能を有効にしますか?」の「はい」を選択してください。

Alpha 19216821/setup_drr	a stm – Microsoft Internet Explorer	-OX			
」ファイル(E) 編集(E) 表示	その お気に入り(点) ツール(① ヘルプ(3)	100			
- 2月25 - → - ◎ 21 21 (2)(秋本 回15月12)0 (2)(周囲 22) 回 - 目 22 (2) 日					
アドレス(2) 🛃 http://192.168	321/setup_dmz.stm	@移動			
KYOCERa	202 Pot797 20232 2.16 542	4			
129-F#1	セットアップ 拡張設定 DMZ&マルチNAT				
タイムソーン設定	DMZ標線を有効コンますか?				
LAN 1832	8+04-0015 / Jul - 1. LEB-7 00+00-02 /- 2 / #896 2 F2(-24) + 7 542 DM7#822+285	. 🛛			
ワイヤレス論定 MACTドレスフィルタリング	新たら世のドレルサンダーイングを通じて、ガンドのシュニンシーンヨンをAKK (のようによります。たたし、UMLをMM数すのMH 13、ジロードルドアドレスが必要になります。	-			
YAN 建定 プリッジ プリッジ 対応アフトレス 特効アフトレス 特効アフトレス 日からモニト DNS 設定 以PAF設定 以PAF設定 切研サール、	στο στο <th t<="" th="" στο<=""><th></th></th>	<th></th>			
ファイアウォール アクセス制限	7. 0 0 0 0 192168.2 0				
URLフィルタ スケジュール セキュリティ DMZ&マルチNAT SNMP	8. 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0	R)			
王の他の項目 LogOut	• 125-331	<u>_</u>			

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)

(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。

C#Documents and Setting:	s¥Administrator¥デスクトップ¥setup_dmz.htm - Microsoft Internet Explorer		_ 🗆 🗙
ファイル(E) 編集(E) 表示	◎ お気に入り(色) ツール(① ヘルプ(日)		19
← 戻る → → 🕥 🙆 🖞	🖞 🔍検索 🖻 あ気に入り ③メディア 🎯 🔄 🎒 🗐 🔍		
アドレス(D) http://192.168	321/setup_dmz.htm		▼
			*
KX KYOCERa		<u>ツール ヘルプ</u>	
A first state of the state of the			
<u>ハスワード変更</u>	セットアッフ 塩張設定 UMZ&マルナNAT		
タイムワーン設定	DMZ機能を有効にしますか? ・ ・ にはい ・ C いいえ		
LAN 該定	最大8台のPGがインターネットを通じて、双方向のコミュニケーションを取 る際には、グローバルIPアドレスが必要になります。	れるようになります。ただし、DMZを構築す	
<u>ワイヤレス設定</u>			
MACフィルタリング			
WAN 設定	ダローバル伊アドレス	クライマントPC IP マドレフ	
ブリッジ	1 2002002001	192 168 2 0	
<u>朝町IPアドレス</u> 静的IPアドレス	2 200 200 200 2	192 168 2 100	
PPPOEt-K	3 200 200 200 3	192 168 2 101	
DNS 등中	4 200 200 4	192 168 2 102	
DIVO BOLL	5 200 200 5	192 168 2 103	
拉張設定	6 200 200 80	192.168.2.104	
<u>UPhP設定</u> 仮想サーバ	7 200 200 200 7	102.160.2.105	
ファイアウォール アクセス制限	2 0 0 0 0	100.160.0	
URLJANS		192.108.2.p	
<u>スケジュール</u> セキュリティ	砂合を使けませの多い		
DMZ&マルチNAT	ague 2000 a 900 C.	ENTER299990 C()280%	
<u>SNMP</u> その他の項目			
LogOut			-
A	i		

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。

http://192.168.2.1/snmp フー(リル) 使生化) まこの	_community.stm - Microsoft Internet Explorer	
		
アドレス(D) 🕘 http://192168.2	1/snmp_community.stm	▼ 予 移動 リンク ※
KYOCERa	<u>メイン</u> セットアップ <u>ステータス ソール</u>	<u>NF7</u>
バスワード東東	セットアップ 拡張設定 SNMPコミュニティー	
タイムワーン設定	SNMPコミュニティーの設定を行ないます。	
LAN 助モ 2-(キリンス酸主 MACTFUスラムルタリング WAN 設定 フリック2 MOIPFFUス PPPのモモード DNS 設定 UPPの国産工 いなサインタール SMAIP TELLの一 その他のの1	SNMPI-ジェント: コミュニティー: No.コミュニティー アクセス 有効にする 1 Read V 2 Read V 3 Read V 4 Read V 5 Read V 5 Read V	ENTER
 ページが表示されました		インターネット //.

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。

http://192.1682.1/snmp_trap. ファイル(E) 編集(E) 表示(M) (中国3、中国・(2) 同) ペ	stm - Microsoft Internet Explorer) お気に入り(A) ツール(D) ヘルグ(H) の 始本 つけちについ (Minutanon (A) Explored To (T) (T) やん の (A)	
アドレスD () http://192.1682	Qana taostm Samo taostm	✓ ✓ ✓ ✓ ✓
KYOCERa	メイシー セットアップ <u>ステータス ツール</u>	ヘルブ
<u>パスワード東東</u>	基本設定 拡張設定 SNMP	
タイムワーン設定	SNMPトラップの設定を行ないます。	
LAN 読定 ワイヤレス読定	SNMP エージェント: トラップ:	
MAC7Fレスフィルタリング WAN 設定 タリッジ あ約日7Fレス 静約日7Fレス PPPのモモード DNS 設定 UPnP設定 気想サーバ、 ファイアウォール	No. IP 7ドレス コミュニティー パージョン 1 0 0 0 第効・ 2 0 0 0 第効・ 3 0 0 0 第効・ 4 0 0 0 第効・ 5 0 0 0 第効・	
SMMP Resist Total Confecture LogOut	験定を掲すますので、ENTERをクリックしてください。	ENTER
◎) パージが表示されました		インカーネット

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
 ● 図 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



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