機能詳細編

LAN側の設定・・・・・1
セキュリティの設定 45
ポートフォワードの設定 ・・・・・ 99
VPNの設定・・・・・127
オプション設定・・・・・ 159
保守・管理・・・・・177

LAN側の設定

ここでは、主に本製品のLAN側の設定について解説します。本製品の設定は、 有線LAN接続でおこなってください。

IPアドレスの設定

本製品のLAN側ポートのIPアドレスを確認・変更する方法を解説します。

! ご注意

本製品のIPアドレスを変更する場合は、誤ったIPアドレスを設定することの ないようご注意ください。誤ったIPアドレスを設定すると、インターネットに 接続できなくなるなどのトラブルになることがあります。

LAN側ポートのIPアドレスを確認・変更する

購入時の状態では、本製品のLAN側ポートのIPアドレスは「192.168.1.1」が 設定されています。

すでにLANが構築されている環境に本製品を導入した場合などで、本製品の LAN側ポートのIPアドレスを変更する必要があるときは、次の手順で行います。

1 サイドバーから [ネットワーク詳細設定] アイコンをクリックします。



2 [LAN Ethernet]の、[修正] ボタンをクリックします。

문 추	ットワーク詳細設定 ―――		
接続名	ステータス	操作	画面に切り替わります。
🖌 WAN Ethernet	播続	修正	
LAN Ethernet	播続		
			🚾 ボタンをクリックします。

3 [詳細設定] ボタンをクリックします。

ارد≮ <mark>¦</mark>	・ワーク接続 LAN Ethernet	
	無効	画面に切り替わります。
报德名:	LAN Ethernet	
ステータス:	接続	
接続タイプ:	Ethernet	
MACアドレス:	100-000 cm 000-000-111	
IPアドレス:	1001 1008 5.2	
サブネットマスク:	2008-2005-2008-0	
DHCPサーバ:	有効	
受信パケット:	190	
送信パケット:	204	
	394	

4 本製品のLAN側ポートのIPアドレスは「IP設定」欄に表示されます。IPアドレスを変更するときは、必要に応じて各項目を設定します。

ត្រ	F細設定 LAN Ethernet	
基本設定		南に切り麸わります
ARES-13:	Ethernet	山に切り音りりより。
MAC7FL2:	00 90 10 00 11	
MTU:	B#100 ¥ 1500	
19Bok	ドアドレスを回転設定する 💌	
IPPPLA:		必安に応して口頃日で収定しより。
サブネットマスク:		
DHCPサーバ	1823 🛩	
割り当て開始ヨアドレス。	192 188 1 1	
割り当て終了19アドレス:	192 188 1 254	
サブネットマスク:	255 255 0	
WINST-HIPPPLA:	0 0 0	
リース再開:	60 (*)	
回クライアントにネスト名が読定されていないとおこネストな	新生産教師に書い当てる	
NAPT:	1000 ×	
テルマスプリック:	50	
マルチキャスト - IGNP Proxy Internal		
□ RIP - ルーティングプロトコル		

5 画面の一番下にある [OK] ボタンをクリックし、[ネットワーク接続 LAN Ethernet] 画面に戻ります。

※[OK] ボタンをクリックして [注意] 画面に切り替わる場合には、その内容 をご確認の上、さらに [OK] ボタンをクリックして [ネットワーク接続 LAN Ethernet] 画面に戻ってください。

6 [OK] ボタンをクリックし、[ネットワーク詳細設定] 画面に戻ります。

※WEBブラウザで本製品のIPアドレスを指定して設定ページにアクセスしていた場合、 続いて別の設定を行いたいときは、変更後のIPアドレスでアクセスし直してください。

MEMO

●LAN側のIPアドレスを変更したとき LAN側のIPアドレスやサブネットマスクを変更したときは、変更後の内容に合わせて [DHCPサーバ]の設定も変更してください。

●LAN内で起動しているパソコンがあるとき 本製品のLAN側ポートのIPアドレスを変更するときに、LAN内で起動しているパソコン がある場合は、本製品のIPアドレスを変更した後でIPアドレスを再取得してください。

NAPT (IPマスカレード)

本製品では、ルーティングのモードとしてNAPTに対応しています。

複数のプライベートIPアドレスを1つのグローバルIPアドレスに変換する機能で、 IPマスカレードとも呼ばれます。LAN側にプライベートIPアドレスを割り当て たパソコンが複数台あり、1つのグローバルIPアドレスでインターネットに接続 する運用形態のときは、NAPTを使用します。

NAPTを使用した場合、LAN内で割り当てられてる複数のプライベートIPアドレスが、インターネットへの接続時に1つのグローバルIPアドレスに変換されます。 さらに、ポート番号も変換されます。インターネット側からは、常に1台のパソ コンがインターネットに接続しているように見えます。



※NAPT機能を利用するための設定は必要はありません。本製品の運用を開始すると、 自動的にNAPT機能は有効になります。

DHCPサーバ設定

DHCPサーバ機能を利用すると、LAN内のパソコンやネットワーク機器がLAN に接続されるたびに、他のどれとも重複しないIPアドレスを自動で割り当てる ことができます。



本製品のDHCPサーバ機能は、特定のパソコンに常に固定のIPアドレスを割り 当てることもできます。

また固定のIPアドレスの割り当てと、動的なIPアドレスの割り当ての両方を設定 することもできます。

!ご注意

- ・本製品のDHCPサーバ機能はデフォルトで有効になっています。
- ・DHCPサーバ機能を使用しないときは、LAN側に接続されているパソコン すべてに、手動でIPアドレスを割り当ててください。
- ・パソコンに手動でIPアドレスを設定した場合、そのパソコンのホスト名やIP アドレスを本製品で管理することはできません。

DHCPサーバの基本設定

ここでは、DHCPサーバの基本的な設定について説明します

1 サイドバーから[カスタム設定]をクリックします。



2 [DHCPサーバ]をクリックします。



3 現在のDHCPサーバのサブネットマスク、IPアドレスの割り当て範囲が表示されます。設定を変更する場合は、[修正]ボタンをクリックします。

			ウサーバ		―― [DHCP サーバ]画面に切り [;] わります。
接続名	サービス	サブネットマスク	割り当て範囲	操作	
WAN Ethernet	無効				
LAN Ethernet	有効	1988, 2988, 2988, 20	100 100 1 1 - 100 100 1 204	192	―― 膝子 ギカンをクロックト キオ

4 [DHCP設定LAN Ethernet]画面が表示されます。 割り当てるIPアドレスの範囲、サブネットマスク、リース期間を設定し、 [OK]ボタンをクリックします。

_P	DHCP設定 - LAN Ethernet	[DHCP設定 LAN Ehternet
サービス		画面に切り替わります。
DHCPサーバ:	有効 🛩	
DHCPサーバ酸定		
割引当て開始IPアドレス:		
割当て終了IPアドレス:		
サブネットマスク:		
WINSサーバIPアドレス:		
リース期間:	60 () ()	
回クライアントにホスト名が設定されてい	はんと考にネスト名を自動的に割り当てる	-
C		
	VOK ATTYCH	― <u>-</u> クリックします。

[有効]

DHCPサーバ機能を有効にします。

[割り当て開始IPアドレス]

割り当てるIPアドレスの、開始アドレスを入力します。

[割り当て終了IPアドレス]

割り当てるIPアドレスの、終了アドレスを入力します。

[サブネットマスク]

割り当てるサブネットマスクを入力します。

[WINSサーバ]

WINSサーバを使用してる場合は、サーバアドレスを入力します。

[リース期間(分)]

割り当てるIPアドレスの有効期限を分単位で入力します。

[クライアントにホスト名が設定されていないときにホスト名を自動的に割り当てる] 接続されているパソコンまたはネットワーク機器にホスト名が設定されていない 場合、自動的にホスト名が設定されます。

- 5 [OK]ボタンをクリックし、[DHCPサーバ]画面に戻ります。
- 6 以上で設定は終了です。

DHCPサーバから固定のIPアドレスを割り当てる

ここでは、特定のパソコンやネットワーク機器にDHCPサーバから常に固定の IPアドレスを割り当てる方法について説明します。

● サイドバーから[カスタム設定]アイコンをクリックします。



2 [DHCPサーバ]アイコンをクリックします。



3 [DHCP設定]ボタンをクリックします。



4 [固定 IP 割り当ての追加]欄から[追加]ボタンをクリックします。

		" P di	HCP	定 —			
ቱ አ⊦ዳ	197ドレス	MAC7FUZ	섯	报数名	ステータス	リース期間	infi
pog	100.000.02	10.00.00.00.00.00	1005	LAN Ethernet	摇滚	43 分	91 11 2
固定IP割り当ての 追加							21.50
		_	戻る				

5 追加したいパソコンやネットワーク機器のホスト名、IPアドレス、MACア ドレスを入力し、[OK]ボタンをクリックします。



[ホスト名]

パソコンまたはネットワーク機器のホスト名を入力します。半角英数字を使用し、 1~63文字の範囲で入力してください。

[IPアドレス]

パソコンまたはネットワーク機器に割り当てるIPアドレスを入力します。

[MACアドレス]

IPアドレスを割り当てるパソコンまたはネットワーク機器のMACアドレスを入力 します。



6 追加したホストが[DHCP設定]画面に表示されているのを確認します。

		"Р он	ICP設	定			
ネスト名	IP7FUZ	MAC7FUZ	シイナ	接続名	ステータス	リース期間	建作
ptg	-		e te's	LAN Ethernet	接线	39 😚	111 1110 Q
pce	102.148.1.15	00.0010414444	BR	LAN Ethernet	接続	60 分	22 MB
国定IP割引当ての 追加							10.10

IPアドレスの修正

ここでは、既にDHCPサーバから自動にIPアドレスが割り当てられているパソ コンまたはネットワーク機器の設定を変更する方法について説明します。



1 サイドバーから[カスタム設定]アイコンをクリックします。

2 [DHCPサーバ]アイコンをクリックします。



3 [DHCP 設定]ボタンをクリックします。

	わります。		サーバ			
		建築作 目	割り当て範囲	サブネットマスク	サービス	接続名
		19 Z			無効	WAN Ethernet
		99 Z	192 108 1 1 - 192 108 1 254	295.255.295.2	有効	LAN Ethernet
			制引当て範囲	サブネットマスク	サービス 無効 有効	接続名 WAN Ethernet LAN Ethernet

4 設定を変更したいホストの [修正] ボタンをクリックします。

		 D	HCP	定			「DHCP 設定」 画面に切り巻	
*21-8	IP7ドレス	MAC7FUZ	왜	接続名	ステータス	リース構	1917	ります。
pog	198.088.1.2	00.00.00.04.04.04.0	\$061)	LAN Ethernet	接続	37 😚	🔟 🗖 🔍	3 6 9 6
固定1P割り当ての 追加							20.00	
								――― 🏧 ボタンをクリックします。
			戻る					

5 [固定割り当て]にチェックを付け、[OK]ボタンをクリックします。



6 タイプが [固定] になっているのを確認し、ホストの[修正]ボタンをクリック します。



7 IPアドレスを固定で割り当てたり、ホスト名、MACアドレスの修正を行う ことができます。

ホスト名:	þcg
IPアドレス:	
MACPFUZ:	
▼固定IP割り当て	

- 8 [OK]ボタンをクリックし、[DHCP設定]画面に戻ります。
- 9 以上で設定は終了です。

IPアドレスの削除

ここでは、登録済みのIPアドレスとホスト名の対応を削除する方法について説明します。

● サイドバーから[カスタム設定]をクリックします。



2 [DHCPサーバ]をクリックします。



3 [DHCP設定]ボタンをクリックします。

		🔐 онся				[DHCP サーバ]画面に切り替 わります。
接続名	サービス	サブネットマスク	割り当て範囲	操作		
WAN Ethernet	無効			19 22		
LAN Ethernet	有効	2995.2995.2995.0	180 188 1 1 - 190 188 1 254	10 ZZ		
			DHCPERE			- クリックします。

4 削除したいホストの [削除] ボタンをクリックします。

		J P DI	HCPE	12 —				<u> </u> [DHCP 設定]	画面に切り替
本スト名	IP7FLZ	масррия	51	接続名	ステータス	リース開 間	18111	r r)ます。	
pcg	100.000.00	RE 10.05 (M 14 Au 10	動的	LAN Ethernet	接続	43 😚	🖬 🏧 🔍			
固定IP割り当ての 追加							22	_		
								<u>i</u>	🍱 ボタンをク!	ノックします。
		•	戻る							

5 [戻る]ボタンをクリックし、[DHCPサーバ]画面に戻ります。

DHCPサーバ機能の有効/無効を設定する

ここでは、DHCPサーバ機能の有効/無効を設定する方法について説明します。

● サイドバーから[カスタム設定]をクリックします。



2 [DHCPサーバ]をクリックします。



3 現在のDHCPサーバのサブネットマスク、IPアドレスの割り当て範囲が表示されます。設定を変更する場合は、[修正] ボタンをクリックします。

			サーバ		[DHCP サーバ」 画面に切り わります。
接続名	サービス	サブネットマスク	割り当て範囲	1#ffe	
AN Ethernet	無効				
N Ethernet	有効	298.298.298.2	190 100 1 1 - 190 100 1 254	19 <u>2</u>	― 🚾 ボタンをクリックします

4 [DHCPサーバ]欄から[有効]または[無効]を選択します。

P	DHCP設定 - LAN Ethernet	│ ┃
サービス		画面に切り替わります。
DHCPサーバ:	有効 🗸	
DHCPサーバ設定	(有文)	
割り当て開始IPアドレス:		
書刊当て終了 IPアドレス:		選択します。
サブネットマスク:		
WINSサーバIPアドレス:	0 0 0	
リース期間:	60 対	
マクライアントにホスト名が設定されてい	ないときにホスト名を自動的に割り当てる	
C	✓ OK X キャンセル	

! ご注意

- ・DHCPサーバ機能を無効にした場合は、本製品のLAN側に接続されてるパソ コンまたはネットワーク機器に、手動でIPアドレスを設定してください。
- 5 [OK]ボタンをクリックし、[DHCPサーバ]画面に戻ります。
 - ※[OK] ボタンをクリックして [注意]画面に切り替わる場合には、その 内容をご確認の上、さらに [OK] ボタンをクリックして [DHCP サーバ] 画面に戻ってください。
- 6 以上で設定は終了です。

DNSサーバ設定

本製品のDNSサーバは、LAN内のパソコンやネットワーク機器のホスト名とIP アドレスの対応を管理しています。

DNSサーバはDHCPサーバと同じ対応表を参照しています。DHCPサーバの 設定時にホスト名を登録しておくと、他に特別な設定をせずに、ホスト名および 対応するIPアドレスがDNSサーバで管理されます。

! ご注意

- ・本製品のDNSサーバは、LAN内のドメイン名とIPアドレスの対応だけを管理しています。
- ・インターネット上のドメイン名を指定した通信では、本製品の「プロキシ DNS」機能が使用されます。

DHCPサーバによるホスト名とIPアドレスの確認

本製品のDNSサーバはDHCPサーバと同じ対応表を参照しています。 DHCPサーバでホスト名とIPアドレスを登録した場合は、DNSサーバにも反映 されます。

ここでは、DHCPサーバ機能で自動登録されたホスト名とIPアドレスを確認します

1 サイドバーから[カスタム設定]をクリックします。



2 [DHCPサーバ]をクリックします。



3 [DHCP設定]アイコンをクリックします。



4 DHCPサーバ機能により、本製品に登録されてるホスト名とそのIPアドレ スが表示されます。

			_JP o	HCP	定	_		
*21-8	IP7FVス	M	にアドレス	対す	集装名 LAN Ethernet	ステークス ステーク	タ リース期 間 60分	#ft
固定IP割引当ての 遅加								23.50
			-	東る				

- 5 [戻る]ボタンをクリックし、[DHCPサーバ]画面に戻ります。
- 6 [戻る]ボタンをクリックし、[カスタム設定]画面に戻ります。
- 7 [DNSサーバ]アイコンをクリックします。



8 本製品のDNSサーバに登録されてるホスト名とIPアドレスが表示されます。



9 以上で確認は終了です。

ホスト名とIPアドレスを手動で登録する

DHCPサーバ機能を使用しない場合は手動でホスト名とIPアドレスを登録する 必要があります。

1 サイドバーから[カスタム設定]アイコンをクリックします。



2 [DNSサーバ]アイコンをクリックします。



3 [DNSエントリの追加]から [追加] ボタンをクリックします。

3	骨 DNSサーバ		——— [DNS サーバ] 画面に切り替わ
木スト名	IP7Fレス	操作	ります。
pcg	2002/2008 1.2	NE ALE	
DNSエントリの追加		16.10	🌆 ボタンをクリックします。
	e 戻3		

4 DNSサーバに登録するホスト名とIPアドレスを入力し、[OK]ボタンをクリックします。



ホスト名とIPアドレスの修正

ホスト名やIPアドレスを変更したときは、DNSサーバに登録した情報も手動で 変更する必要があります。

! ご注意

- ・DHCPサーバ機能を有効にしているときは、パソコンのホスト名は自動的に DNSサーバに反映されます。手動でホスト名を変更する必要はありません。
- サイドバーから[カスタム設定]アイコンをクリックします。



2 [DNSサーバ]アイコンをクリックします。



3 情報を修正したいホスト名の [修正] ボタンをクリックします



4 ホスト名とIPアドレスを修正し、[OK]ボタンをクリックします。



※DHCPサーバによりIPアドレスを割り当てられたホストについては、 ホスト名のみ修正が可能です。

ホスト名とIPアドレスの削除

登録されているホスト名とIPアドレスの削除を行います。

1 サイドバーから[カスタム設定]アイコンをクリックします。



2 [DNSサーバ]アイコンをクリックします。



3 情報を削除したいホスト名の [削除] ボタンをクリックし、[戻る] ボタン をクリックします。

水2名 IP7Fレス 詳細 操作 M1 DHCP 37 38 M2 2~切花素 37 38		🚮 DNSサーバ							
×1 DHCP 2015 ×2 ユーザ定著 2015	ホスト名	IPアドレス	詳細	操作					
**2 ユーザ定義 西方 1000	Planex1	100.000.1.2	DHCP	第五百 月月18					
	planex2	192 108 1.171	ユーザ定義	18 IE (H) 19:					
こうトリの追加 単位	DNSエントリの追加			16.00					
		ب التي ا							

プロキシDNS

本製品には「プロキシDNS」機能が搭載されています。プロキシDNSとは、LAN 側の各パソコンからインターネット上のドメイン名を指定した接続(DNSの問い 合わせ)があった場合に、それをインターネット上のDNSサーバにフォワー ディングして、対応するIPアドレスを各パソコンに回答する機能です。 LAN側のパソコンからは、インターネット上のDNSサーバに代理で問い合わせて いることはわからず、単に、本製品がインターネット上のドメインと各IPアド レスの対応を管理するDNSサーバとして動作しているように見えます。



WAN側で複数セッションを接続している時には、LAN側のパソコンからDNSの 問い合わせがあった場合、本製品のプロキシDNS機能は、全てのセッション上 のDNSサーバに問い合わせのパケットを送信します。この場合、返答のあった DNSサーバのセッションを使用して通信を行います。2つ以上のセッションの DNSサーバから返答があった場合は、先に返答があった方のセッションを使用 します。

ルーティング設定

本製品は、ダイナミックルーティングのプロトコルとしてRIP、RIP Version2に 対応しています。また、スタティックルーティングにも対応しています。

ダイナミックルーティングの設定

ここでは、ダイナミックルーティングを設定し、動的に経路情報を登録する方 法について説明します。本製品のダイナミックルーティングを設定する場合は、 ダイナミックルーティングを有効にするインターフェイスを設定し、本製品の ダイナミックルーティング機能を有効にします。

1 サイドバーから [ネットワーク詳細設定] アイコンをクリックします。



2 [接続名]欄からダイナミックルーティングを有効にするインターフェイスの[修正]ボタンをクリックします。

문 *	ットワーク詳細設定		── [DHCP サーバ] 画面に切り替 わります。
接続名	ステータス	操作	
🖸 WAN Ethernet	接続	修正	
🖌 LAN Ethernet	接続	197E -	── 🚾 ボタンをクリックします。
- Law Editing			

 ここでは例として [LAN Ethernet]を選択します。他のインターフェイスを 選択した場合も同様の手順で進めてください。

4 [ネットワーク接続 LAN Ethernet]画面が表示されます。[詳細設定] ボタン をクリックします。

taxa.o.	LAN Ethorpot
	+#108
(7-94)	情况。
MACアドレス:	
IPアドレス:	
サブネットマスク:	255.255.255.0
DHCPサーバ:	有効
受信バケット:	1421
送信パケット:	2323

5 [デバイスメトリック] 欄から [RIP-ルーティングプロトコル] にチェック をつけます。

マクライアントにホスト名が設定されていないときにホスト名を自動的に割り当てる	
デバイスメトリック: 50	
▼マルチキャスト - IGMP Proxy Internal	
RIP - ルーティングプロトコル	──── チェックします。
✓ 0K X =+0200	

6 RIPの送受信設定を行います。[RIP受信設定]欄から本製品が受信する RIPの種類を選択します。[RIP送信設定]欄から本製品から送信する RIP の種類を選択します。

マルチキャスト - IGMP Proxy Intern	al	
RIP受信設定:	RIPv1/2 💌	
RIP送信設定:	RIPv2 - ブロードキャスト 💌	選択します。
	DK ★++ンセル	

RIP受信設定 RIP機能を無効にします。 なし RIPv1 RIPv1による、ルート情報の受信を行います。 RIPv2による、ルート情報の受信を行います。 RIPv2 RIPv1/2による、ルート情報の受信を行います。 RIPv1/2 RIP送信設定 RIP機能を無効にします。 なし RIPv1 RIPv1による、ルート情報の送信を行います。 RIPv2・ブロードキャストネットワーク内の不特定多数にRIPv2による、 ルート情報の送信を行います。 RIPv2・マルチキャスト 複数の相手を指定してRIPv2による、ルート 情報の送信を行います。

7 [OK] ボタンをクリックします。[注意] 画面が表示される場合は、内容を 確認したうえで [OK] ボタンをクリックします。

	(1) 注意					
設定画面への再ログイン:	設定を変更すると BRC-14VG 設定画面 への再ログインが必要になる場合があります。					
OK ボタンをクリックしてください。						
TOR STATES						

- 8 [ネットワーク接続 LAN Ethernet]画面に戻ります。
- 9 サイドバーから [カスタム設定] アイコンをクリックします。





11 [ルーティングプロトコル] 欄から [RIP-ルーティングプロトコル] に チェックがついてるか確認します。



12 [OK] ボタンをクリックします。

スタティックルーティングの経路情報を追加する

ここでは、経路情報を手動で設定する方法について説明します。経路情報の追加は、50以内とすることをお勧めします。※50以上の経路を設定すると、本製品の動作パフォーマンスに影響することがあります。

- 1 サイドバーから[カスタム設定]アイコンをクリックします。

2 [ルーティング]アイコンをクリックします。



3 [ルートの追加]から[追加]ボタンをクリックします。



4 経路情報を追加するインターフェースを選択し、経路情報を入力して[OK] ボタンをクリックします。

	₩ ルーティング設定	[ルーティング設定] 画面に切
接続名:	LAN Ethernet	り替わります。
送信先:		選択します。
ネットマスク:		
ゲートウェイ:		
メトリック:	2	
	✓ ok X ++>tzル	

[接続名]

スタティックルーティングを設定する転送先のインタフェースを [LAN Ehternet]、 [WAN Ehternet]、[WAN PPPoE] 等から選択します。

[送信先]

パケットの送信先となるネットワークアドレスを入力します。

[ネットマスク]

パケットの送信先のネットマスクを入力します。

[ゲートウェイ]

宛先のネットワークに到達するための、最初のゲートウェイのアドレスを入力 します。

[メトリック]

宛先のネットワークに到達するまでのホップカウント(経由するゲートウェイの数) を入力します。

5 [ルーティングテーブル]欄に設定したルーティング情報が追加されている ことを確認して[OK]ボタンをクリックします。

接続名	送信先	ゲートウェイ	ネットマスク	メトリック	ステータス	操作
LAN Ethernet	0.0.0.0	0.0.0.0	0000	•	適用しました	修正用的
ルートの追加						30.00
ルーティングプロ IRIP - ルーテ	トコル イングブロト	⊐ılı				
マレチキャ7	2					

スタティックルーティングの経路情報を修正する

ここでは、既に設定したスタティックルーティングの経路情報を修正する方法 について説明します。

1 サイドバーから[カスタム設定]アイコンをクリックします。



2 [ルーティング]アイコンをクリックします。


3 修正したい経路情報の[修正]ボタンをクリックします。

		*** π	レーティング			
ルーティンクテーン 接続名	フル 送信先	ゲートウェイ	ネットマスク	メトリック	ステータス	it fi
LAN Ethernet	191 108 111	100.368.1.380	255,255,255,2	2	適用しました	97 19
ルートの追加						10.00
ルーティングプロト	-JIL					
■ RIP - ルーディ	ングプロトコル					
マルチキャスト						
		🗸 ок	★キャンセル			

4 経路情報を修正し、[OK]ボタンをクリックします。

)	₩ ルーティング設定	
接続名:	LAN Ethernet 👻	
送信先:		
ネットマスク:		
ゲートウェイ:		
メトリック:	2	
·		
\langle	✓ OK	クリックします。

5 以上で設定は終了です。

スタティックルーティングの経路情報を削除する

ここでは、登録したスタティックルーティングを削除する方法について説明します。

1 サイドバーから[カスタム設定]アイコンをクリックします。



2 [ルーティング]アイコンをクリックします。



3 削除したい経路情報の[削除]ボタンをクリックします。

		**	. = 2.8				「川、 ティング] 両面に切りま
ルーティングテー	ブル	• •					
接続名	送信先	ゲートウェイ	ネットマスク	メトリック	ステータス	19 fr	10 0 0 0 0
LAN Ethernet	1982 1988 1913	100.108.1.108	255.255.255.0	2	通用しました	107 8112	
ルートの追加						20.00	
ルーティングブロ	1-JU						―― 🌆 ボタンをクリックします。
□ RIP - ルーティ	ヘンダブロトコル						
マルチキャスト							
		 ✓ OK 	× #+>121/				

4 [OK]ボタンをクリックします。

5 以上で設定は終了です。

UPnP 設定

Universal Plug and Play (UPnP:ユニバーサルプラグアンドプレイ)は、ネット ワークに接続するだけで、ネットワーク上の機器同士で簡単に通信できるように する規格です。本製品は、UPnPに対応しており、次の機能を使用できます。 ※購入時の設定でUPnPがONになっているため、特別な設定をする必要がありません。

- UPnPに対応しているOS(Windows[®] XPとWindows[®] Me)から、本製品を 検出できます。
- UPnPに対応しているOS(Windows[®] XPとWindows[®] Me)から本製品の状態を確認したり、設定を一部変更できます。
- 本製品に接続されているLAN内のパソコンから、Windows[®] Messengerや MSN[®] Messengerなど、UPnPに対応しているアプリケーションを使用する ことができます。

なお、Windows[®]98、Windows[®]2000およびMacintosh[®]はUPnPに対応していません。したがって、UPnPの機能を使用することはできません。

パソコンのUPnPの設定を確認する

お使いのパソコンが、UPnPが使用できる状態になっているか確認してください。

■ Windows[®] XPの場合

1 [スタート] ボタンをクリックし、[コントロールパネル] をクリックします。



2 [プログラムの追加と削除] ボタンをクリックし、画面左側にある [Windows コンポーネントの追加と削除] ボタンをクリックします。



3 [コンポーネント] 欄から [ネットワークサービス] を選択し、[詳細] ボタン をクリックします。

Windows コンポーネント ウィザード			
Windows コンポーネント Windows XP のコンボーネントを追加	ロまたは斉川政令できます。		
各チェック ポックスをクリックして、道 ポックスは、コンポーネントの一部が を表示するには、国料細」をクリックし コンポーネント(①)	uまた(前)除するコンボーネン) (ンストールされることを表しま) てください。	トを選んでください。影付きのチェック す。コンポーネントに含まれているもの	
アインデックス サービス プラスのほかのえっトワーク ファー	1126001#-82	0.0 MB	
			――― 選択します。
説明:特別なネットワーク	関連のさまざまなサービスやブロ	コ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:	56.7 MB 10183.6 MB	詳細 <u>()</u>	クリックします。
	< 戻る(B) 次へ(N)> キャンセル	

4 ネットワークサービスの詳細が表示されますので、[UPnPユーザーイン ターフェイス]の状態を確認します。

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、追加は友は判除するコンボーネントを選んでくださ 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。コンボーネン を表示するなばよ、目料細しをク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(Q):	い。影け者のチェック ンドに含まれているもの
UPhP 2-9-40/9-721/3	
	0.0 MB
	U.U MB
□ 📮 簡易 TCP/IP サービス	0.0 MB
は明正 ネットワークで検出された UPnP デバイスごとにアイコンを マイ す。また、必要な Windows フィイアウォールのボートを閉ぎます 必要なディスク領域の合計: 56.7 MB	ネットワーク」に表示しま す。
空きディスク領域: 10188.2 MB	and which have follow in the
OK	キャンセル

[UPnPユーザーインターフェイス] がチェックされているときは、パソコンの UPnPの機能が有効になっています。ダイアログを閉じてください。

チェックされていないときは、[UPnPユーザーインターフェイス] が無効に なっています。チェックを付け、[OK] ボタンをクリックします。画面の指示に 従って、インストールを続けてください。

5 以上で設定は終了です。

■Windows[®]Meの場合

【スタート]ボタンをクリックし、[設定]→[コントロールパネル]の順に クリックします。



2 [アプリケーションの追加と削除]ボタンをクリックします。[アプリケーションの追加と削除]ダイアログが表示されたら、[Windowsファイル] タブをクリックします。

アプリケーションの追加と削隊のプロパティ	?	×
インストールと削り Windows ファイル	1	クリックします。
各チェックボックスをクリックして、追加または削り除する 付きのチェックボックスは、エンボーネントの一部だけか します。[[詳細]]をクリックすると、エンボーネントの内容	ファイルを選択してください。影 インストールされることを意味 が表示されます。	
コンボーネントの種類(<u>C</u>):		
🗹 🚔 Outlook Express	5.0 MB 🔼	
■ 📻 アクセサリ	6.7 MB 💻	
☑ ■ アドレス帳	1.5 MB	
🗹 🥬 オンライン サービス	2.5 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: - 説明 インターネット電子メールおよびニュースグループリ す。	432 MB 00 MB 43675 MB ーダーを簡単に使用できま 手持任の). ディスク使用(1)。	
OK ¥	*ンセル 道用(<u>6</u>)	1

3 [コンポーネントの種類] 欄から[通信] を選択し、[詳細] ボタンをクリック します。

アプリケーションの追加と削除のプロパティ		<u>×</u>	
インストールと削除 Windows ファイル 起動ディスク		- 15	
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 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 します。 国洋細則をクリックすると、コンボーネントの内容が	イルを選択してください。身 ンストールされることを意味 表示されます。	影	
コンポーネントの種類(<u>C</u>):			
■ 塩 マルチメディア	1.6 MB 🔺		
	FAND		溜切します
			―――――――――――――――――――――――――――――――――――――
	0.0 110	·	
インストール済みコンポーネントのディスク領域:	20.3 MB		
必要なディスク領域:	0.0 MB		
- 説明	10300.9 MB		
ほかのコンピュータやオンライン サービスとの通信に使	うアクセサリです。		
選択数:6/10 個	≣羊糸田(<u>D</u>)		―――クリックします。
	ディスク使用(円)		
	<i>r</i>		
OK ++2	セル 適用(品)		

4 通信の詳細が表示されますので、[ユニバーサルプラグアンドプレイ]の状態 を確認します。

通信	×
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 (だざい。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、『詳細』をクリックして	ック ボックスをオンバこして (はオフにします。 影付 いることを意味します。 こください。
コンホーネンドの種類型 図 感 ダイヤルアップ ネットワーク ● 喰 ハイパーターミナル 図 ユニバーサル ブラグ アンド フレイ ■ 喩 類想プライベート 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: 空きディスク領域: 説明 ユニバーサル フラグ, アンド, フレイを使用すると、Window 	20.3 MB 0.0 MB 16348.3 MB ws と高機能装置と
の間で、シームレスな接続や通信が可能になります。	<u> 詳細(D)</u>

- 5 [ユニバーサルプラグアンドプレイ]がチェックされているときは、パソ コンがUPnPの機能が有効になっています。ダイアログを閉じてください。 チェックされていないときは、[ユニバーサルプラグアンドプレイ]が無効 になっています。チェックを付け、[OK]ボタンをクリックします。画面 の指示に従ってインストールを続けてください。
- 6 以上で設定は終了です。

本製品のUPnP機能をOFFにする

本製品でUPnP機能を使用しないときは、次のように操作します。

- **1** サイドバーの [カスタム設定] アイコンをクリックします。
- **2** [UPnP] アイコンをクリックします。



3 UPnPの機能をOFFにするときは、チェックボックスのチェックを外します。



- **4** [OK] ボタンをクリックします。
- 5 以上で設定は終了です。

セキュリティの設定

本製品の設定は、有線LAN接続でおこなってください。

セキュリティ機能

インターネットに接続すると、LAN内のパソコンがインターネットからの攻撃を 受けたり、不正なアクセスをされるという危険があります。そのため、LANを保護 する十分なセキュリティ対策を行うことが、快適にインターネットを使う上で重 要なポイントとなります。

本製品では、インターネットへの常時接続を行う上でのセキュリティ対策として 次の機能を搭載しています。

NAPT (IPマスカレード)	プロバイダから取得したグローバルIPアドレスを、LAN内のプライベ ートIPアドレスに変換する機能により、インターネット側からLAN内 のパソコンを特定できず、アクセスすることができません。このため、 外部からの不正アクセスが困難になります。
ステートフル・ パケット・イン スペクション	ファイアウォール方式として、ステートフル・パケット・インスペク ション方式を採用しています。通信セッションごとにパケットの整合 性を確認し、必要なポートだけを開くようにします。通信が終了する と利用したポートを遮断します。 さらに、インターネット側からのDoS(Denial of Services)攻撃パタ ーンを識別し、不正なアクセスを遮断することが可能です。
ALG (Application Level Gateway)	アプリケーションレベルでパケットの通過・遮断を判断します。
パケットフィル タリング	インターネットから送られてきたパケットを検査して通過させるかど うかを判断する機能です。どのような条件でパケットを通過させるか、 遮断するかをプロトコル/ポートごとに任意に設定できます。
バーチャル コンピュータ	LAN内の1台のパソコンをバーチャルコンピュータホストとすると、 WAN側からの全ての接続要求がバーチャルコンピュータホストに転送 されるようになります。
ID・パスワード によるユーザ認 証	本製品の設定を変更するには、ログインIDとパスワードが必要です。

セキュリティレベル設定

ここでは、本製品の基本的なセキュリティレベルの設定を行います。

セキュリティ対策を考える時は、実際のデータのやり取りの流れに合わせて 「LANからインターネットへの通信」と「インターネットからLANへの通信」の それぞれに対してルールを考える必要があります。

一般的には、LANからインターネットにはアクセスできるようにし、インター ネットからLANにはアクセスを拒否するように設定します。

本製品のセキュリティ機能には3段階のレベルがあらかじめ用意されています。 さらに、用途に応じて設定をカスタマイズすることができます。

使いたまコリアイ設定 第2720798月 (ローカムワー・ド (バーテルムエビニータ) (バモートアン2023年 (バワットライムタ) (ビキュリアイの)	 [セキュリティ設定] 画面に切 り替わります。
() (中本)974-0-6487 新田かい一	セキュリティの設定が3段階で 用意されています。 購入時の設定では、[セキュリティ レベル標準] が選択されています。

1 サイドバーから [セキュリティ設定] アイコンをクリックします。

2 必要に応じて、レベルを変更します。

セキュリティ レベル	インターネット側からの 接続要求	LAN 内のパソコンからの 接続要求
最大	拒否 インターネット側からLANにアク セスできません。ただし、[ローカル サーバ]と[リモートアクセス]画面 で設定したサービスは使用できます。	制限あり LAN内のパソコンで、WEBサー ビス、e-mailなどのよく使うイン ターネットのサービスのみ使用で きます。※
標準	拒否 インターネット側からLANにアク セスできません。ただし、[ローカ ルサーバ]と[リモートアクセス] 画面で設定したサービスは使用でき ます。	制限なし LAN内のパソコンで、すべてのイン ターネットのサービスが使用でき ます。
最小	制限なし インターネットから LAN へのアク セスをすべて許可します。	制限なし LAN内のパソコンで、すべてのイン ターネットのサービスが使用でき ます。

※[セキュリティレベル最大] を選択しているとき、LAN側のパソコンから使用できる インターネットのサービスは次のとおりです。

Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, SMTP



[セキュリティレベル最小]を選択すると、セキュリティ機能が一切適用されなくなりますので、必要な場合にのみ設定してください。

3 [IPフラグメントパケットを遮断する]をチェックします。

zstaniy∠ + 2 × stri⊐t	
□ IPフラグメントパケットを追診所する	— チェックします。
 ノOK メキャンセル 	

フラグメント化されたデータパケットを利用した攻撃を防ぐことができます。

※IPSecを利用する仮想プライベートネットワークやUDPをベースにしたサービスに よっては、IPフラグメントを利用するものがあります。このようなサービスを利用する ときは、チェックを外してください。

4 [OK] ボタンをチェックします。

選択したセキュリティレベルに変更されます。

パケットフィルタリング設定

本製品のパケットフィルタの機能は、本製品が受信したパケット、送信する パケットに対してあらかじめ設定してあるフィルタルールを適用します。 フィルタルールには、[LAN Ehternet ルール]、[WAN Ehternet ルール]、[WAN PPPoEルール]等があります。



ルール適用順

ルール適用順

パケットフィルタの設定

ここでは、本製品にパケットフィルタを設定する方法について説明します。

■パケットフィルタの新規設定

1 サイドバーから[セキュリティ設定]アイコンをクリックします。



2 [パケットフィルタ]タブをクリックします。

」 セキュリティ設定	[セキュリティ設定] 画面に
- 鉄設定 アクセス和限 ローカルサーバ バーチャルコンピュータ リモートアクセス数 パケットフィルタ セキ リティ	19 切り替わります。
① セキュリティレベル基大 割信がリハー・すべて観古 別信がリン・」を取引 法のサービスのみしおからWAMへの別信号時可:Telnet,FTP, HTTB,HTTB,OHS,IMAP,POP3,SMTP ② セキュリティレベル電車 割信がリン・」すべて許可 ③ セキュリティレベル電車 割信がリン・」すべて許可	────クリックします。
□19つち分ンCトバケットを追踪作する	
✓ OK X キャンセル	

3 [セキュリティ設定]画面が表示されます。

- 単設定 アクセスを原 ローカルサーバ バーチャルエビュータ リモートアクセス設定	[セキュリティ設定] 画面に 切り替わります。
パケットフィルシルールを設定する抽読を選択してくだき、5 受信メケット LAN Ethernet ルール WAN PPPOE ルール	
道信パケット LAN Ethernet II/~ II/	
WAN PPPOE ルール	

- 4 [受信パケット]欄、または[送信パケット]欄からルールを作成するインター フェースをクリックします。
- ※ここでは、例として[WAN PPPoEルール]を選択します。他のインターフェース を選択した場合は同様の手順で設定してください。

	🚅 セキュリティ設定			
一般設定 アクセス制限	ローカルサーバ バーチャルコンピュータ Uモートアクセン	ス設定 パケットフィルタ セキュ	リティログ	
	パウットフィルタルールを設定する接続を選択してく 受信パケット	ださい。		
	LAN Ethernet JV-JV	9 Z		
	WAN PPPOE ルール	(9 Z		
	送信パケット			
	LAN Ethernet ルール	修正		
	WAN PPPoE ルール	修正		ー例として選択します。
	د <u>ج</u> ه			

本製品で設定できるルール一覧

[LAN Ehternet ルール]

LANのポートに対して適用されるルールになります。

[WAN Ehternet ルール]

WANのポートに対して適用されるルールになります。

[WAN PPPoEルール]

WAN PPPoEのポートに対して適用されるルールになります。

[VPN PPTPルール]

VPN PPTPの接続に対して適用されるルールになります。

[VPN IPSecルール]

VPN IPSecの接続に対して適用されるルールになります。

[WAN PPPoEルール設定]画面が表示されます。
 [新規作成]欄から[追加]ボタンをクリックします。

		虜 wan pr	PoE ルール 設定			└ └ [WAN PPPoEルール設定
ルール ID 新知作成	送信元IPアドレス	送信先IPアドレス	サービス名	動作	ステータ 捜	画面に切り替わります。
新飛作成						
		 ✓ OK 	x #+>tzik			│ │ 500 ボタンをクリックします

6 [フィルタルールの追加]画面が表示されます。

」 「フィルタルールの追加		└── [フィルタルールの追加] 画
IP7Fレス		面に切り替わります。
送信元IPアドレス: 1個を指定 🔽 👂 0 0 0		
送信先IPアドレス: 1個を指定 🔽 0 ,0 ,0 ,0		
動作		
 破棄する 		
 転送する 		
このルールに合数するパケットと、このパケットに取りるセッションのパケットをすべて転送します。 セッションはSPI(Stateful Packet Inspection)により管理します。	la	
このルールに名数するパケットと、このパケット活躍わるセンタンのパケットをすべて転送します。 セッションパタPU(Stateful Packet Inspection)により管理します。 〇 転送するパケット) このルールに合数するパケットのみを転送します。 SPI(Stateful Packet Inspection)によるセッションの管理試行いません。	la la	
このルールに全数するパワットと、このパワットに取りたセンタンのパワットをすべて転送します。 セッションパタPI(Stateful Packet Inspection)により増増します。 〇 転送する(パワット) このルールに含まするパワットのみを転送します。 SPI(Stateful Packet Inspection)によるセットョンの管制は行いません。 Pグ協定	la la	

7 [IPアドレス]欄から送信元IPアドレス、送信先IPアドレスを入力します。

[すべて]を選択した場合は、全てのIPアドレスが対象になります。



[1個を指定]を選択した場合は、指定したIPアドレスが対象になります。

1個を指定 🖌 þ .0 .0 .0	
1個を指定 🗸 0 .0 .0 .0	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
	1個を指定 ♥ (D ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0 ,0

[範囲指定]を選択した場合は、指定したIPアドレスの範囲が対象になります。

IPアドレス		
送信元IPアドレス:	IPアドレスを範囲で指定 • 0 .0 .0 .0 - 0 .0 .0 .0	
送信先IPアドレス:	1977ドレスを範囲で指定 🔹 🛛 .0 .0 .0 .0 .0 .0 .0 .0 .0	,0,0,0,0,0,0

8 [動作]欄からフィルタの動作を選択します。



[破棄する]

パケットを破棄します。

[拒否する]

パケットを破棄して、TCP Reset または ICMP Host Unreachable パケットを送信 元に送信します。

[転送する]

このルールに合致するパケットと、このパケットに関わるセッションのパケット を転送します。

[転送する (パケット)]

このルールに合致するパケットのみを転送します。

- 9 [サービス名]欄に本製品に既に登録されているサービスやアプリケーション が表示されます。フィルタルールの対象となるサービスにチェックをつけます。
- ※リストにないサービスをフィルタする場合は、「新規にサービスを作成する場合」 を参照してください。

サービス名	プロトコル / ボート	
ユーザ定義サービス		
デフォルト定義サービス		
LI All Traffic	フルトコル すべて	
DNS - Domain Name Server	TCP 53-> 53 1024-65535-> 53 UDP 53-> 53 1024-65535-> 53	
FTP - File Transfer	TCP すべて-> 21	
HTTP - Web Server	TCP すべて-> 80	
HTTP - Secondary Web Server	TCP すべて -> 8080	
HTTPS - Secured Web Server	TCP すべて -> 443	
HTTPS - Secondary Secured Web Server	TCP すべて -> 8443	
TFTP - File Transfer	UDP 1024-65535 -> 69	
IMAP - Messaging Server	TCP すべて -> 143	── チェックし
NNTP - News Server	TCP すべて-> 119	
Ping - ICMP Echo Request	ICMP Echo Request	
POP3 - Incoming Mail	TCP すべて-> 110	
SNMP - Simple Network Management Protocol	UDP オペて -> 161	
SMTP - Outgoing Mail	TCP オペて-> 25	
TELNET - Remote Connection	TCP すべて -> 23	
TELNET - Secondary Remote Connection	TCP すべて -> 8023	
TELNETSSL - Secure Remote Connection over SSL	TCP すべて -> 992	

10 [OK]ボタンをクリックします。

	— クリックします。
--	------------

※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

11 複数のフィルタルールを作成する場合は、3~10の手順を繰り返します。

12 以上で設定は終了です。

■パケットフィルタの修正

サイドバーから[セキュリティ設定]アイコンをクリックします。



2 [パケットフィルタ]タブをクリックします。

- #設定 アクセス非際 ローカルサーバ バーチャルエンビュータ リモートアクセス設	パケットフィルタ セキ リティログ	│ [セキュリティ設定]画面に 切り替わります。
 ・ セキュリティレベル最大 新計ポリンー: すぐて数応 新計ポリンー: すぐて数応 がなけービスのみんがわらめMAN-の現住を許可: Telinet, FTP, HTP, NTP5, DN5, MA2, POP3, SMTP ・ 世や、コリティレベル電準 新計ポリンー: すぐて読あ 発見者がシンー: すべて許可 ・ 世キュリティレベル電本 		ークリックします。
新井和ジン-: すべて許可 見ば村ジン-: すべて許可 □ IP2555Ch1付かけ影響新する ✔ OK X キャンセル		

3 設定を変更したいインターフェースの [修正] ボタンをクリックします。

🍰 セキュリティ設定		
」 一級設定 アクセス制限 ローカルサーバ パーチャルコンピュータ リモートアクセス パケットフィルウルールが設定する様体を道路してくた	設定 パケットフィルタ セキュリティログ	切り省わります。
受信パケット		
LAN Ethernet $\mathcal{W} = \mathcal{W}$	191	
WAN PPPOE JU-JU	探正	
送信パケット		
LAN Ethernet ルール	19 II	
WAN PPPOE JU-JU	19 E	
Ø ES		

4 [WAN PPPoEルール設定]の画面が表示されますので、[操作]欄から [修正] ボタンをクリックします。

5 [フィルタルールの編集]画面が表示されますので、必要な項目の修正を行い [OK]ボタンをクリックします。

」 フィルタルールの編集	小 フィルタルールの編集				
IPアドレス: チベて w 送他のアドレス: チベて w 適応 「「「「「「」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」	0	面に切り替わります。			
 	ta	│ │ │ 修正します。			
○ 転送する(パット) このルールに含飲する(パットの水を転送します。 SPI(Stateful Packet Inspection)によるセットョンの管理は行いません。	ter				
ログ設定 □このルールに合款したいケットをログに記録する					

※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

6 以上で修正は終了です。

■パケットフィルタの削除

1 サイドバーから[セキュリティ設定]アイコンをクリックします。



2 [パケットフィルタ]タブをクリックします。



3 設定を削除したいインタフェースの[修正]ボタンをクリックします。

- 殷颢定 アクセス		27.敬定 パケットフィルク セキュリティログ	[セキュリティ設定] 画面に 切り替わります。
	パケットフィルタルールを設定する接続を選択して 受信パケット LAN Ethernet ルール	<th></th>	
	WAN PPPoE ルール 送信パケット LAN Ethernet ルール	3	
	WAN PPPOE JU-JU	91	
	e <u>E</u> 5		

4 [WAN PPPoEルール設定]画面が表示されます。[操作]欄から[削除] ボタン をクリックします。

5 以上で削除は終了です。

新規にサービスを作成する場合

ここでは、本製品にあらかじめ登録されていないサービスを設定する方法に ついて説明します。

1 [フィルタルールの追加]画面から、[ユーザ定義サービス]をクリックします。

	虜 フィルタルールの追	hı —		— [フィルタルールの追加]	由
IP7FUX				面に切り替わります。	
送信元19アドレス:	すべて	1			
送信先197ドレス:	7×7 >				
動作					
 破棄する 					
 ・ 拒否する ・ ・ ・	または ICMP Host Unreachable パケ	ットを送信元に送信します。			
○ 転送する このルールに会数するパケットと セッションはSPI(Stateful Pace	、このパケットに開わるセッションのパケット (et Inspection)におり管理します。	をすべて転送します。	60		
 転送する(パケット) この)ルールに合数するパケットの SPI(Stateful Packet Inspect 	のを転送します。 tion)によるセッションの管理は行いません	*	la		
ログ設定					
□このルールに合致したパケットをログ	に記録する				
	サービス名	プロトコ	コル / ポート	クリックレキオ	
ユーザ定義サービス		11		<i>― シ</i> リッシします。	
All Traffic		プロトコル オ	~7		

2 [ユーザ定義サービス]画面が表示されます。[新規作成]欄から[追加]ボタン をクリックします。

	」 ユーザ定義サービ		[ユーザ定義サービス]画面 に切り替わります。
新規作政	9-ビス名 () हुठे	ナロトコル / ボート	── ■ ボタンをクリックします。

3 [サービスの編集]画面が表示されます。[新規作成]欄から[追加] ボタンを クリックします。

サービス名: サービスの説明:	は Popplication	 [サービスの編集]画面に切 り替わります。
プロトコル 新規作成		🌆 ボタンをクリックします。
	✓ OK ★ 4+>20k	

4 [プロトコル]欄から使用するプロトコルを選択します。



[プロトコル]

対象にするプロトコルをTCP、UDP、ICMP、GRE、ESP、AH、その他から選択 します。

[送信元ポート/送信先ポート]

サービスやアプリケーションの発信元ポート/送信先ポート番号を入力します。 すべて →全てのポートを指定します。 1個を指定 →1つのポート番号を指定します。 範囲指定 →ポート番号の範囲を指定します。

[ICMPメッセージ]

対象にするICMPメッセージを選択します。

- 5 [OK]ボタンをクリックします。
- 6 [追加]ボタンをクリックすることで、複数のポートを指定することもできます。

	👘 サービスの編集		
サービス名:	Application		
サービスの説明:			
プロトコル	3M	練作	
TCP	すべて -> すべて	91 III III III III III III III III III I	
the im Proce			💷 🌆 ボタンをクリックしき

7 全ての設定が終了しましたら [サービス名] に任意の名前を入力し、[OK]ボタン をクリックします。 8 [ユーザ定義サービス]の画面に戻ります。[サービス名]欄に作成したユーザ 定義サービスが表示されるのを確認します。 [戻る]ボタンをクリックします。

小 コーザ定	義サービス	
サービス名 Application 時度行政		└── 確認します。
	• ·	│ │ │ │ クリックします。

g 新規に作成したサービスが[ユーザ定義サービス]欄に表示されます。

💁 フィルタルールの 追加													
IPアドレス													
送信元1Pアドレス:	1個を指定	v þ	.0	.0	.0								
送信先IPアドレス:	1個を指定	v 0	.0	.0	.0								
動作													
 ・ ・ ・								•					
- (D. I	CORNER TO ORING	I-BRIDZ.	17	No de la la la	and strategies	a dense		6m					
このルールに合致す? セッションはSPI(Sta の転送する(パケット) このルールに合致す? SPI(Stateful Pack	いけかっトと、このパウット ceful Packet Inspect いけかトのみを転送しま et Inspection)によるf	に思わる・ ion)により す。 2ッションの	セッションの リ管理しま り管理は行	Dバケットき す。 しません。	をすべて載え込	します。		la la					
このルールに合数す セッションはSPI(Sta の 転送する() 行ット) このルールに合数す SPI(Stateful Pack ログ設定	いけットと、このパケット ceful Packet Insped いけットのみを転送しま at Inspection)による+	に関わる・ ion)により す。 2ッションの	セッションの J管理しま の管理しま	Dパケットを す。 いません。	をすべて 第 五記	UIT.		la la					
このルールに含数すう セッションはSPI(Sta の転送する(パケット) このルールに含数すう SPI(Stateful Pack ログ設定	いけットと、このパケット Seful Packet Insped いけットのみを転送しま at Inspection)による+ rットを口灯に記録する	に思わる ion)によ す。 2ッションの	セッションの J管理しま の管理は行	Dパケットき す。 いません。	をすべて 第 5秒	出ます。		la la					
このルールに含数す3 セッションは3PI(Sta のルールに含数する(パケット) このルールに含数す5 SPI(Stateful Pack ログ酸定 □このルールに含数したパ?	sy (ケットと、この) (ケット seful Packet Insped sy (ケットのみを転送しま et Inspection)による+ rットを口りに記録する サービフ	1088わるよう ion)により す。 2ッションの :名	セッションの リ管理しま り管理は行	D//ケットを す。 しません。		£∪≢す.	ブロトコル /	€ø %ø #~-⊦					
このルールに含数すき セッションはSPI(Sta セッションはSPI(Sta のルールに含数すき SPI(Stateful Pack ログ設定 ローンのルールに含数したい? ユーザ定義サービス	s/ げットと、この) パット Seful Packet Insped So (ゲットのみ考察道)しま et Inspection) によろ・1 rットをログー記録する サービブ	1088わるよう ion)により す。 2ッションの 3名	セッションの り管理しま の管理しまう	D/ゲットき す。 しません。	€ ∮ ∧τ 0 233	出ます。	プロトコル /	& ⊗ ≭-⊦		+	=+	h=	1

10 以上で設定は終了です。

フィルタルールの例

ここでは、パケットフィルタの例としてNetBIOS関連で使われてるポート137~ 139のLANからWANへの通信を遮断する方法について説明します。 Windows®のLANで使われているNetBIOSのパケットにより、予期せぬインタ ーネットへの通信が発生する場合があります。NetBIOS関連で使われてるポート 137~139を遮断することで、予期せぬ通信を防ぎます。

方向	動作	プロト コル	送信元 IP アドレス	送信先 IP アドレス	送信元 ポート	送信元 IP アドレス
送信→ WAN Ehternet	破棄	TCP/ UDP	すべて	すべて	すべて	137~139,445

※WindowsMe/98SEの場合、「445」を設定する必要はありません。

1 サイドバーから[セキュリティ設定]アイコンをクリックします。



2 [パケットフィルタ]タブをクリックします。

	● セキュリティ設定		 [セキュリティ設定] 画面に
一般設定 アクセス制	限 ローカルサーバ バーチャルコンピュータ リモードアクセス数	パケットフィルタ セキ リティログ	切り替わります。
E	0 セキュリティレベル最大		<u>│</u> │ クリックします。
	者信がリシー : オイズ 拒否 発信がリン : 一部計可 洗のサービスのみLANがらWANへの発信素許可:Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, SMTP		
(⊙ セキュリティレベル標準		
	着信ポリシー: すべて拒否 発信ポリシー: すべて許可		
(○ セキュリティレベル最小		
	着信水リシー:すべて許可 発信ボリシー:すべて許可		
C	」IPフラヴメントパケットを通新する		
	✓ ok (X +*>tok)		

3 LAN側からWAN側へのNetBIOSのパケットを遮断するルールを作成します。 [受信パケット]欄から[LAN Ehternet ルール]の [修正] ボタンをクリックします。

🚅 セキュリティ設定	
- 総設置 アクセス発展 ローガルワーバ パーチャルコンピュータ リモートアクセ パケットフィルクルールを設定する構成を選択して 気気パケット LAN Ethernet ルール WAN PPPE ルール これ Ethernet ルール WAN PPPE ルール	



		虜 lan i	Ethernet ルール 設定	-		<mark>ー</mark> [LAN Ethernet ルール設
ルール ID 新規作成	送信元IPアドレス	送信先IPアドレス	サービス名	動作	ステータ: 操作	画面に切り替わります。
		- 1 Ok	x =+>>tzル			│ │

5 送信元IPアドレスに[すべて]、送信先IPアドレスに[すべて]を選択します。

送信先197ドレス:	■ 2×4			
◎ 破壊する				
C 拒否する パケットを破壊して、TCP Ret	se または ICMP Host Unreachable パケットを逆信元に逆信します。		;72	tRI.:
○ 転送する このルールに含数するパケッ セッションはSPI(Stateful P	-と、このパウットに聞わるセッションのパケットをすべて転送します。 acket Inspection/により管理します。	to a		1/07
○ 転送する(パケット) このルールに合数するパケット SPI(Stateful Packet Insp	ーのみを転送します。 ection)にころセッションの管理は行いません。	to .		
ログ設定				
E = (5,1) - (1,1) - (6,10) (5,177) - (1,10)	191:記録する		1	

6 [動作]欄から[破棄する]にチェックを付けます。



7 [ユーザ定義サービス]をクリックします。

虜 フィルタルールの追加		──[フィルタルールの追加] 匪
IP7FLZ		面に切り替わります。
送信元IP7FLス: すべて v		国にのション日にションのショッ
通信先即アドレス: すべて 💌		
¢bfi:		
 ・ ・ ・	•	
○ 転送する このルールに合数するパケットと、このパケットに取りるセッションのパケットをすべて転び セッションパスSPI(Stateful Packet Inspection)により増増します。	Elizt.	
○ 転送する(パワット) このルール/ご会談するパワットのみを転送します。 SPI(Stateful Packet Inspection)によるセッションの被職は代いません。	la	
口グ酸定		
□このルールに合致したパケットを口分に記録する		
14-129 B	プロトコル / ポート	
ユーザ定義サービス — Application	TCP すべて -> すべて	<u>-</u>
デフォルト定義サービス		

8 [ユーザ定義サービス]画面が表示されます。[新規作成]欄から [追加]ボタン をクリックします。

	j 2-17	定義サービス		
新規作成	サービス名	プロトコル / ポート	排作	
		Ro		│ ── ^{──} ボタンをクリックします │

9 [サービスの編集]の画面が表示されます。[新規作成]欄から [追加] ボタン をクリックします。

	🙀 サービスの編集		
サービス名:	Application		
サービスの説明:			
プロトコル	詳細	12PE	
新規作成			
			🌆 ボタンをクリックします
	✓ OK X ++>/tz//		

10 プロトコルから[TCP]を選択します。送信元ポートに[すべて]、送信先ポート に[範囲指定]を選択し、ポート番号に「137」~「139」を入力します。

※ Windows XP/2000のときは、同じ手順で「445」も設定します。

	👘 サービスの 編集	
プロトコル 送信元ポート:		─── 入力します。
送信先ポート:	戦団指定 🔍 137 - 139	
	 ✓ OK X キャンセル 	

11 [OK]ボタンをクリックします。

12 同様にUDPポートも遮断しますので、[追加]ボタンをクリックします。

	👘 サービスの 編集		
サービス名: サービスの説明:	Poplication		
プロトコル	# #		
TCP 新規作成	á√í -> 131-13A	クリックし	します。
	✓ OK X =+5200		

13 プロトコルから[UDP]を選択します。送信元ポートに[すべて]、送信先ポート に[範囲指定]を選択し、ポート番号に「137」~「139」を入力します。

プロトコル		
送信元ポート:	すべて 💌	3, 7, 1, =
送信先ポート:	範囲指定 💌 137 - 139	7/108

14 [OK]ボタンをクリックします。

15 [サービスの編集] 画面が表示されますので、サービス名に登録する名前 を入力し、[OK] ボタンをクリックします。

サービス名: サービスの説明:	レービスの編集 NetBIOS		入力します。
プロトコル	詳細	揉作	
тср	オペて -> 137-139	(8 Z M89	
UDP	すべて -> 137-139	(\$ Z M13	
新規作成		10.10	
	OK OK UT SALAN		│ │ │ │ クリックします。

16 [ユーザ定義サービス] 画面に戻ります。[サービス名] 欄に作成したユーザ 定義サービスが表示されるのを確認します。[戻る] ボタンをクリックし ます。

 2-	ザ定義サービス		
サービス名	プロトコル / ポート	操作	
NetBIOS	TCP すべて-> 137-139 UDP すべて-> 137-139	977 MIS	
新規作成		iB #0	
ринны	₩ ₽ 0	1997)	クリックしま

17 [ユーザ定義サービス]欄に作成したサービスが表示されますので、チェック を付け[OK]ボタンをクリックします。

	👘 フィルタルールの 追加		
IPアドレス			
送信元IPアドレス:	すべて 🗸		
送信先19アドレス:	すべて 🖌		
動作			
 破棄する 			
○ 転送する このルールに合数す? セッションはSPI(Star	い(ケットと、この)(ケットに開わるセッションの)(ケットをすべて) Jeful Packet Inspection)により管理します。	tëttj. 🆢	
○ 転送する(パケット) このルールに合致する SPI(Stateful Pack	い「ケットのみを転送します。 at Inspection)こよるセッションの管理は行いません。	la la	
口グ設定			
□このルールに合致したパ	「ットをログ」に記録する		
	サービス名	プロトコル / ポート	
ユーザ定義サービス			
WetBIOS		TCP すべて-> 137-139	イー・・・クレー
the second se			

※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

18 [OK]ボタンをクリックし、[パケットフィルタ]の画面に戻ります。

			Ethernet ルール 詰	定		
ער⊸ג ID	送信元IPアドレス	送信先IPアドレス	サービス名	動作	ステータ ス	排作
v o	すべて	すべて	NetBIOS	🌚 破棄する	有効	19 JE 8118
新規作成						50.00

19 [OK]ボタンをクリックします。

20 次に送信パケットの設定を行います。 [送信パケット]欄から[WAN PPPoEルール]の [修正] ボタンをクリックし ます。

一般設定 アクセス制限	(ローカルサーバ) バーチャルンピュータ リモートアイ	地ス設定 パケットフィルタ セキュリティログ	- [パケットフィルタ]画面に 切り替わります。
	パケットフィルタルールを設定する機能を選択し 気信パケット LAN Ethernet ルール WAN PEPPE ルール	T(SER 6	
	芝信ルケット LAN Ethernet ルール WAN PPPOE ルール		- <mark>ஊ</mark> ボタンをクリックします。

21 [新規作成]欄から [追加] ボタンをクリックします。

11-11		送信元197ドレス	wan	PPPoE ルール 設定 サービス名	i th/Fe	ステータス 棟	│ │ [WAN PPPoEルール設定] │ 画面に切り替わります。
新規作	FJŠ		2.10.200 71 074				
							│ <u>─</u> ஹ ボタンをクリックします

22 送信元IPアドレスに[すべて]、送信先IPアドレスに[すべて]を選択します。

📑 フィルタルールの 追加		
IP7FUZ		面に切り替わります。
送信元IPアドレス: すべて 💌		
送信先IPアドレス:		
的作		
 破棄する 		
C 拒否する		— 選択します。
パケットを破棄して、TCP Reset または ICMP Host Unreachable パケットを送信元に送信します。	•	
C 転送する		
このルールに含数するパケットと、このパケットご問わるセッションのパケットをすべて転送します。 セッションはSPI(Stateful Packet Inspection)により管理します。	la	

23 [動作]欄から[破棄する]にチェックを付けます。

1915			
送信元ドアドレス:	₹~(•		
述言先ドアドレス:	3~1		
● 破棄する			チェックします
バケットを破棄して、TCP Reset または	ICMP Host Unreachable パケットを送信元に送信します。) 1 9 7 0 8 9
○ 転送する	ha linaDharta s, s, es, éta linea serete™n ainai	A-	

22 [ユーザ定義サービス]欄に先ほど作成したサービスが表示されますので、 チェックを付け、[OK]ボタンをクリックします。

虜 フィルタルールの追加		└── [フィルタのルール追加] 画
IP7Fレス		
送信元IPアドレス: すべて 💌		
送信先IPアドレス: すべて 💌		
動作		
 破棄する 		
 WEE 3 6 このルールに合意するがワットと、このパワットに取りるセッションのパワットをすべて転送しま セッシュノはSPI(Stateful Packet Inspection)により管理します。 転送するパワット) このルールに合意するパワットのみ発転例にます。 SPI(Stateful Packet Inspection)によるセッションの管理は行いません。 	7. ka	
口グ設定		
□このルールに含数したパケットを口勿に記録する		
サービス名	ブロトコル / ポート	
ユーザ定義サービス		
WhatBIOS	TCP オペア -> 137-139	└── チェックします。
Lind	UDP すべて -> 137-139	

※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

23 [OK]ボタンをクリックし、[パケットフィルタ]の画面に戻ります。

		虜 wa	N PPPoE ルール 設定			
ルール ID	送信元IPアドレス	送信先IPアドレス	サービス名	動作	ステータス	操作
o 되	すべて	すべて	すべてのサービス	🌚 破棄する	有効	修正 削除
新規作成						18. 1 0

24 以上で設定は終了です。
リモートアクセス設定

リモートアクセス機能を使うことで、インターネット側から本製品にアクセスし、 各種設定を行うことができます。

デフォルト設定ではLANを保護するためにリモートアクセスを許可していません。



不正アクセスにより本製品の設定を変更されないよう、通常はリモートアクセス を無効に設定しておき、必要な場合のみ許可するようにしてください。 本製品に設定されたリモートアクセス機能は、ローカルサーバ、バーチャルコン ピュータより優先されます。

リモートアクセスの設定

1 サイドバーから [セキュリティ設定] アイコンをクリックします。



2 [リモートアクセス設定] タブをクリックします。

使用で アクセスを採 ローカルサーバ バーチャルエピュータ (パモーチアクセス発音) パクパクマパタ セキュ	[セキュリティ設定] 画面に切 り替わります。
 ● 世キョリティレマル最大 新信和リシー: オペて配否 発信ポリシー: 一番菊(マ) ハイアレ、「ロアレ、」、「のいいへの発信を当年: 1 tek pt, FTP, イイTP, ITTPS, USIS, MAP: POPS, SMTP ● 世キョリティレマル電車 新信和リシー: オペて振否 発行やリン: オペて振否 新信和リンー: オペて振否 ● 世キョリティレマル電本 ● 世キョリティレマル電本 	クリックします。
第12枚ジン-: すべて許可 「アンラジスント/(ウットを送給がする	

3 WAN側からのアクセスに関する設定を行います。



設定画面	WEBサーバを 外部に公開する (プライマリポート)	本製品のHTTPポートをTCP80ポートで外部に公開 する場合に選択します。
	WEBサーバを 外部に公開する (セカンダリポート)	本製品のHTTPポートをTCP8080ポートで外部に公 開する場合に選択します。
	設定画面を外部 に公開する	本製品の設定画面を外部に公開する場合に選択し ます。上記「プライマリポート」、または「セカン ダリポート」をあわせてチェックします。
診断ツール	Pingに応答する	Pingコマンドに返答する場合は選択します。
	UDPTraceroute を許可する	Tracerouteコマンドなどで、UDP上のルート確認を する場合は選択します。
オプション 設定		USBカメラから画面を外部に公開する場合に選択し ます。

ご注意

- ・Windows ◎ から Traceroute コマンドを使用して、ルートの追跡を行う場合は [Ping に応答する] をチェックしてください。
- ・設定画面をWAN側から見るには、以下のURLを指定してアクセスします。
 設定画面用アドレス: http://(WAN側アドレス)/setting/
- 4 [OK] ボタンをクリックします。
- 5 以上で設定は終了です。

サイトフィルタ設定

サイトフィルタ機能を使うことで、LAN側のパソコンから特定のWEBサイトを 閲覧できないように設定できます。

例えば、公序良俗に反するようなWEBサイトをあらかじめ本製品に設定しておくことで、LAN側のパソコンからそのサイトの閲覧を禁止することができます。 サイトフィルタの登録件数は、50以内とすることをお勧めします。 ※50以上の登録すると、本製品の動作パフォーマンスに影響することがあります。

サイトフィルタの設定

■サイトフィルタの新規作成

- サイドバーから [セキュリティ設定] アイコンをクリックします。
- **2** [サイトフィルタ] タブをクリックします。
- 3 [新規作成]欄から[追加]ボタンをクリックします。

- 総定 ローカルサード バーチャルスピュータ レモートアクビス タイトフルタ パックトフル ビキュリティ 総定					[サイトフィルタ]画面に切り 替わります。
LAN側のコンピュータかられ	違したサイトへのアクセスを				
IPアドレスまたは本スト名 IPアドレス ステータス 第一 新規作成 IPアドレス ステータス 第一					🎫 ボタンをクリックします。
表示の更新 ポタンモン	ックすると、表示データを更詳				
	アアドレスの更新 アアドレスの更新 ア				

4 閲覧を禁止したいWEBサイトのURLまたはIPアドレスを入力し、[OK] ボタンをクリックします。



5 [IPアドレスまたはホスト名]の一覧に設定したWEBサイトが追加されます。

G	● セキュリティ設定				
- 税設定 ローカルサーバ パーチャルコンピュータ レムN制のコンピュータから	ノモートアクセス サイ 御記したサイトへのアクセ	トフィルタ パケットフィル	レタ セキュリティログ	1	
IPアFレスまたはネスト名	IP7FLZ	ステータス 暗認中		<u>م </u>	- 確認します
助用作数 表示の更新ポタンを	19111733 (11) (11) (11) (11) (11) (11) (11) (1				
✓ OK (X + #22)	IPTHL200	新 表示の更新			

6 URLが追加されると、追加されたURLがインターネット上に存在するか 自動的にチェックします。この間、[ステータス]欄には[確認中]と表示 されます。[表示の更新]ボタンをクリックして、入力されたURLが適切 なものか確認します。

	虜 セキュリティ設定		
観定 ローカルサーバ バーチャルコ	ノビュータ リモートアクセス サイ	1771119 187917411	ターセキュリティロ
LANIN7):	ンピュータから推取したサイトへのアクセ	2スを通知します。	
IPアドレスまたはネスト名	IP7Fレス	ステータス	ittri
🕑 www.planex.co.jp	0.000	確認済み	99 ZE (M18)

- **7** [OK] ボタンをクリックすると、設定が有効になります。
- 8 以上で設定は終了です。

MEMO

ステータスに [Error] が表示される場合

→WEBブラウザを起動し設定したURLを入力し、WEBブラウザに表示される か確認してください。正しく表示されたときは、本製品に設定したURLが 間違ってる可能性があります。

■サイトフィルタの有効/無効の切替

- サイドバーから[セキュリティ設定]アイコンをクリックします。
- **2** [サイトフィルタ] タブをクリックします。
- **3** [IPアドレスまたはホスト名] 欄からサイトフィルタを無効にしたいWEB サイトのチェックを外し、[OK] ボタンをクリックします。

, ê	🔓 セキュリティ設定			
- 戦闘法 ローカルサーバ バーチャルゴンピュータ LAN時のコンピュータ	リモートアクセス サイト	フィルタ パケットフィル	タ セキュリティログ	1
IPアドレスまたはホスト名 ビ www.planex.co.jp	IP7FVZ	ステータス ロロックス		────────────────────────────────────
新規作成 表示の更新ポタン	をクリックすると、表示データを	変形します。	8 .55) ±)) 'e)r08 9
	1996 C 19701 C 1996	──── クリックします。		

- **4** [ネットワークマップ] 画面がを表示されます。再度 [セキュリティ設定] アイコンをクリックし、[サイトフィルタ]タブをクリックします。
- **5** [サイトフィルタ]を表示します。[ステータス]表示が[無効] に替わり ます。再度、サイトフィルタを有効にする場合はチェックを付けます。

	「レキュリティ設定			
- 般設定 ローカルサーバ パーチャルコンピュー:	リモートアクセス サー	1174119 1179174119	セキュリティログ	
LANINのコンピュー:	から指定したサイトへのアク	セスを通知。ます。		
IPアドレスまたは本スト名	IP7FU2		infi	T
www.planex.co.jp	0.0.00	無95		 - 催認し
新规作成			ats.htt	
表示の更新 ポラ	いきクリックすると、表示デー:	タを更新します。		

6 以上で設定は終了です。

■サイトフィルタの修正

- ↑ サイドバーから [セキュリティ設定] アイコンをクリックします。
- 2 [サイトフィルタ] タブをクリックします。
- **3** 設定を変更したいWEBサイトのIPアドレスの[修正] ボタンをクリック します。

	🛃 セキュリティ設定			
- 教諭を定 ローカルサーバ パーチャルコンピュー:	リモートアクセス サイ	トフィルタ パケットフィルタ	セキュリティログ	
LAN側のコンピュー:	から指定したサイトへのアクモ	2スを適新します。		
IPアドレスまたはホスト名	IPアドレス	ステータス	n	
新規作成		SELUTION .		· · · · · · · · · · · · · · · · · · ·
表示の更新 ボジ	ノをクリックすると、表示データ	这更新します。		
× ∞	2200 IP7FL201	新 表示の更新		

4 [アクセスを遮断するサイト]の画面が表示されましたら、新しいIPアドレス、またはホスト名を入力し、[OK] ボタンをクリックします。

よい戦からのアクセスを追 いるサイト	[アクセスを遮断するサイト] 画 面に切り替わります。
V OK I WALKARD	│ │ 確認します。

[IPアドレスまたはホスト名]の一覧に変更したWEBサイトが表示されます。

wan 🕼	PPPoE ルール 設定			
ルール 10 芝信元1071レス 芝信先1071レス 新聞作品	サービス名 メキャンセル	動作	ステータス 推作	確認します。

6 以上で設定は終了です。

■サイトフィルタの削除

- ↑ サイドバーから [セキュリティ設定] アイコンをクリックします。
- 2 [サイトフィルタ] タブをクリックします。
- **3** 設定を削除したいWEBサイトのURLの [削除] ボタンをクリックします。

ß	セキュリティ設定		
- 税設定 ローカルサーバ パーチャルコンピュータ	リモートアクセス サイトフィルタ パケットフィル	ターセキュリティログ	
IP7FLZまたはホスト名	IP7ドレス ステータス 黒効		│ ■ ■ ボタンをクリックします
新展作成			
✓ OK X = #2/2	3ル IP78しスの更新 表示の更新		

- **4** [OK] ボタンをクリックします。
- 5 以上で設定は終了です。

ログの管理

ここでは、LAN側のパソコンからインターネットへの接続やインターネット側からLANへの接続、設定ページへのアクセスなどのログ情報を設定します。

セキュリティログの確認

■ログを見る

1 サイドバーから [セキュリティ設定] アイコンをクリックします。



2 [セキュリティログ] タブをクリックします。



3 [セキュリティログ] 画面が表示されます。現在のセキュリティに関する ログが確認できます。



■ログの見方(例)

イベント	種類	説明
Inbound/ Outbound Traffic	Connection accepted	接続要求がファイアウォールのセキュリティポリ シーに適合していた場合に表示されます。
	Accepted - Host probed	ファイアウォールのセキュリティポリシーに適合 したTCP接続要求があったが、インターネット側の ホストが信頼できるかどうかわからない場合に表示 されます。この場合、インターネット側のホストに 認証が試みられます。 ※インターネット側からの接続要求に対してのみ表示され ます。
	Accepted - Host trusted	認証を試みていたホストから応答があった場合に 表示されます。 ※インターネット側からの接続要求に対してのみ表示され ます。
	Accepted - Internal traffic	すべてのパケットがLAN側のホスト同士の間で自由 に行き来できる場合に表示されます。
	Connection Refused- Policy violation	接続要求がファイアウォールのセキュリティポリ シーに違反している場合に表示されます。
	Blocked - IP Fragment	ファイアウォールですべてのIPフラグメントをブ ロックする設定を行った場合で、IPフラグメントが ブロックされたときに表示されます。エラーはブ ロックされたフラグメントごとに表示されます。
	Blocked - IP Source Routes	IP ヘッダに始点経路制御オプションが設定されて いることが原因で、パケットがブロックされたとき に表示されます。
	Blocked - State-table error	ファイアウォールによってステートテーブル(LAN 側のパソコンやネットワーク機器間のセッション 状態に関する情報)が調査または操作されている間 に、エラーがあった場合に表示されます。パケット はブロックされます。
Firewall Setup	Aborting configuration	ファイアウォールに関する設定がキャンセルされた ときに表示されます。
	Configuration completed	ファイアウォールに関する設定が完了したときに 表示されます。

WBM Login	Authentication Success	設定ページへのログインが成功したときに表示され ます。
	Authentication Failure	設定ページへのログインが失敗したときに表示され ます。
System Up/Down	The system is going DOWN for reboot	本製品を再起動するために終了したときに表示され ます。
	The system is UP!	本製品が起動したときに表示されます。

■ログのクリア

1 サイドバーから[セキュリティ設定]アイコンをクリックします。



2 [セキュリティログ] タブをクリックします。

	· [セキュリティ設定] 画面に 切り替わります。
	-クリックレキオ
取給約シン-: すべて許可 ● セキュリティレベル最小 割(約リン-: すべて許可 回(ドワラガンCA)(かっ)を認知する	->597089.
くの、 Xキャンセル	

3 [ログのクリア] ボタンをクリックすると、画面に表示されているログが消去されます。

() セキュリティ裁定] [セキュリティログ] 画面に切
一般な 75と24歳 ローカルサーバ パーチャルンビュラ レモードアクに2次度 パパットフィルタ せきょりティログ ・ ES ビジのフアフ 田線な 長元の支那 株分元/シル アキシ 表示・少支期にます。	り替わります。
	クリックします。

- 4 [戻る] ボタンをクリックします。
- 5 以上で設定は終了します。

■ログの詳細設定

ここでは、ログの保存に関する設定について説明します。

1 サイドバーから [セキュリティ設定] アイコンをクリックします。



2 [セキュリティログ] タブをクリックします。

● セキュリティ後定 - #22 72に242 (ローカルサーバ (バーチャルコメシュータ (レモートアクセン223) (パットフィ) (ローカル・ログ	[セキュリティ設定] 画面に 切り替わります。
他も30万化へを載入 耐谷リン-:: すべて読者 別はサリン-:: つきづき いかジーンにつきづき ・ ひちょうジェレベを載す 一 ひちょうジェレベを載す 耐谷リン-:: すべて読者 別を申リン-: すべて読者 ● セキュリティレベを載す 香噌やリン-: すべて読者 ● セキュリティレベを載本 香噌やリン-: すべて読者 ● セキュリティレベを載本 香噌やリン-: すべて読者 ● ロドゥンラジントい けっトを送解すと	ノ クリックします。
(Z 0K) (X 46500)	

3 [詳細設定] ボタンをクリックします。



4 [ログイベント]欄から保存するログ内容を選択します。

世キュリティログ設定] [セキュリティログ設定] 画面
ログイベント	に切り谷わります。
口报统状態	└── 選択します。
□ IPアドレスを詐称した接続	
ログバッファ	
□ ログ容量が一杯になったらログを停止する	
✓ OK X ++>>tz₩	

[許可した接続]

ファイアウォールの通過を許可されたものがログに保存されます。

[拒否した接続]

ファイアウォールの通過を拒否されたものがログに保存されます。

[接続状態]

接続の有効・無効の切替えをログに保存します。

[IPアドレスを詐称した接続]

送信元IPアドレスを詐称してファイアウォールの通過を拒否されたものがログに 保存されます。



全てのチェックをオンにすると、本製品のパフォーマンスが低下する可能性が あります。 5 [ログバッファ]欄からログ容量が一杯になったときの設定を選択します。

	2	
□ロジ容量が一杯になったらロジを停止する	J	選択します。
~ 0	× キャンセル	

[ログ容量が一杯になったらログを停止する]

ログを保存するメモリが一杯になったときにログの保存を停止する場合は、チェック します。 ログを保存するメモリが一杯になったとき古いログを消去し、続けてログを保存 する時はチェックを外します。

- **6** [OK] ボタンをクリックします。
- 7 以上で設定は終了します。

E-Mail 通知機能の設定

本製品は、システムや回線、ファイアウォールに何かしらの異常が発生した場合 電子メールで管理者に通知することができます。

1 サイドバーから [カスタム設定] アイコンをクリックします。



2 [ユーザ] アイコンをクリックします。



3 E-mail通知機能を設定するユーザの [修正] ボタンをクリックします。

[E-mailアドレス]欄に、送信先のMailアドレスを入力します。

2	2 ユーザ設定	│ ╷── [ユーザ設定] 画面に切り替わ
一般設定		ります。
フルネーム:	Administrator	
ユーザ名 (大文字/小文字に注意)	admin	
新しし パスワード:	•••••	
新しいパスワードの確認:	•••••	
権段:	 ご 使現者権限 □ PPTP リモートアクセス □ ファイルサーバからのファイルの読み込み ☑ ファイルサーバへのファイルの書き込み □ USBカメラ 	
E-Mail通知設定	SMTPメールサーバの設定	
E-Mailアドレス:		└── 入力します。
システム通知レベル:	tal 💌	
A A AND AND AND AND	ta. 🗸	

5 [システム通知レベル]欄から通知する内容を選択します。 システム通知は、システム情報に関するメッセージを送信します。

Administrator	
admin	
•••••	
•••••	
 ○ 管理者権限 □ PPTP リモートアクセス ビ ファイルリケー バからのファイルの読み込み ビ ファイルサーバへのファイルの書き込み □ USBカメラ 	
SMTPメールサーバの設定	
13L V	―― 入力しま
ペレ エラー 警告 (情報	
	Administrator admin admin ************************************

[エラー]

本製品が正しく動作していないなどの、致命的なエラーが発生した際にメッセージ を送信します。

[警告]

注意を要するエラーが発生した際にメッセージを送信します。 警告を選択した場合は、エラーレベルのメッセージも送信されます。

[情報]

ユーザが本製品を利用したときに表示されるメッセージが送信されます。 情報を選択した場合は、エラーレベル、警告レベルのメッセージも送信されます。 6 [セキュリティ通知レベル]欄から通知する内容を選択します。 セキュリティ通知は、セキュリティログに表示されるメッセージを送信 します。

一般設定		
フルネーム:	Administrator	
ユーザ名 (大文字/小文字に注意)	admin	
新しし パスワード:	•••••	
新しいパスワードの確認:	•••••	
権限:	 ○ 管理者権限 ○ PPTP リモートアクセス ○ ファイルサーバからのファイルの読み込み ○ ファイルサーバへのファイルの書き込み ○ USBカメラ 	
E-Mail通知設定	SMTPメールサーバの設定	
E-Mailアドレス:		
システム通知レベル:	tal 💌	
セキュリティ通知レベル:		└── 選択しま │

[エラー]

重大なセキュリティイベントが発生した際に、メッセージを送信します。

[警告]

注意を要するセキュリティイベントが発生した際にメッセージを送信します。 警告を選択した場合は、エラーレベルのメッセージも送信されます。

[情報]

ユーザが本製品を利用したときに表示されるメッセージが送信されます。 情報を選択した場合は、エラーレベル、警告レベルのメッセージも送信されます。

7 本製品からメールを送信するための、SMTPメールサーバの設定をします。 [SMTPメールサーバの設定]をクリックします。

E-Mail通知設定	SMTPメールサーバの設定	選択します。
E-Mailアドレス:		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

8 [SMTPメールサーバ]欄にメールサーバのアドレスを入力します。
 [送信元メールアドレス]欄に送信元のメールアドレスを入力します。

SMTPメールサーバ:	1		―― 入力し
送信元メールアドレス:			

9 [OK] ボタンをクリックし、[ユーザ設定] 画面に戻ります。

10 [OK] ボタンをクリックします。

11 以上で設定は終了です。

Syslogの設定

本製品には、システムや回線、ファイアウォールに何かしらの異常が発生した 場合Syslogサーバにログを送信することができます。 ここでは、ログをSyslogサーバに送信するための設定を説明します。

1 サイドバーから[カスタム設定]アイコンをクリックします。



2 [システム設定] アイコンをクリックします。



3 [システム通知レベル] 欄から通知する内容を選択し、[システム通知 Syslogサーバアドレス] に syslogサーバのアドレスを入力します。

システムリモートログ設定
システム通知レベル:
システム通知 syslogサーバアドレス: 0 0 0 0

[エラー]

システムに関する重大なメッセージを送信します。

[警告]

システムに関する注意を要するメッセージを送信します。 警告を選択した場合は、エラーレベルのメッセージも送信されます。

[情報]

ユーザが本製品を利用したときに表示されるメッセージが送信されます。 情報を選択した場合は、エラーレベル、警告レベルのメッセージも送信されます。 4 [セキュリティ通知レベル]欄から通知する内容を選択し、[セキュリティ 通知 syslog サーバアドレス]にSyslog サーバのアドレスを入力します。 セキュリティ通知は、セキュリティログに表示されるメッセージを送信 します。

[エラー]

重大なセキュリティイベントに関するメッセージを送信します。

[警告]

注意を要するセキュリティイベントに関するメッセージを送信します。 警告を選択した場合は、エラーレベルのメッセージも送信されます。

[情報]

ユーザが本製品を利用したときに表示されるメッセージが送信されます。 情報を選択した場合は、エラーレベル、警告レベルのメッセージも送信されます。

- **5** [OK] ボタンをクリックします。
- 6 以上で設定は終了です。

ポートフォワードの設定

ここでは、LAN側に設定したパソコンを公開するときに必要な設定について 説明します。

本製品の設定は有線LAN接続でおこなってください。

ローカルサーバ設定

LAN側のサーバをインターネットに公開するときや、オンラインゲームやチャット などのソフトウェアを使うときはローカルサーバ機能の設定を行います。 本製品には、あらかじめインターネットで使われるサービスやアプリケーション が登録されており、簡単に設定することができます。



ローカルサーバの設定

ここでは、ローカルサーバの詳細な設定を行います。

1 サイドバーから[セキュリティ設定]アイコンをクリックします。



2 [ローカルサーバ]タブをクリックします。

- 新設定 77世2382 (ローカルワーバ パーチャルコンビュータ) リモートアクセス832 (パワットフィルス セキュリア・ログ	[セキュリティ設定]画面に切 り替わります。
① 性をもソア・ ~ ~ *	クリックします。

3 [新規作成]欄から [追加] ボタンをクリックします。



4 [ローカルサーバの追加]画面が表示されます。 [ローカルホスト]欄にローカルサーバを設定するパソコンのIPアドレスを 入力します。

	の追加	ーーー [ローカルサーバの追加] 画面 に切り替わります。
サービス名 ユーザ定義サービス デフォルト定義サービス	Jakas / #~k	
All Traffic	プロトロル すべて	
		――― 入力します。

- 5 [デフォルト定義サービス]欄に本製品に既に登録されているサービスや アプリケーションが表示されます。インターネットに公開するサービスや、 使用するアプリケーションを選択し、チェックします。
- ※リストにないサービスを使用する場合は、「新規に作成したサービスでローカル サーバを設定する場合」を参照してください。

サービス名	プロトコル / ポート	
ユーザ定義サービス		
アノオルド定義サービス 「All Traffic	プロトコル すべて	
 []DNS - Domain Name Server	TCP 53 -> 53 1024-65535 -> 53 UDP 53 -> 53 1024-65535 -> 53	
FTP - File Transfer	TCP すべて -> 21	
HTTP - Web Server	TCP すべて -> 80	
HTTP - Secondary Web Server	TCP すべて->8080	
HTTPS - Secured Web Server	TCP オペモ-> 443	――― チェックしき
HTTPS - Secondary Secured Web Server	TCP オペモ-> 8443	
TFTP - File Transfer	UDP 1024-65535 -> 69	
IMAP - Messaging Server	TCP 才べて→143	
NNTP - News Server	TCP オペ℃→119	
Ping - ICMP Echo Request	ICMP Echo Request	
POP3 - Incoming Mail	TCP すべて -> 110	
C DIVP - Disple Network Management Protocol	00P \$ 10 - 101	
SMTP - Outgoing Mail	TCP $\# < \tau > 25$	
TELNET - Remote Connection	TCP #<7 -> 23	

6 [OK]ボタンをクリックします。

CHIP - Web Server	TCP #/47 -> 80
HTTP - Secondary Web Server	TCP #<<℃ > 8080
HTTPS - Secured Web Server	TCP # <t -=""> 443</t>
HTTPS - Secondary Secured Web Server	TCP #117 -> 8443
TFTP - File Transfer	UDP 1024-65535 > 69
DMP - Messaging Server	TCP $\#\!\ll\!T \gg 143$
NNTP - News Server	TCP $\#\!<\!\!\!\!<\!\!\!\!\!\!\tau\sim119$
Ping - ICMP Echo Request	ICMP Echo Request
POP3 - Incoming Nail	TCP $\#\!<\!$
SNMP - Simple Network Management Protocol	UDP すべて -> 161
SMTP - Outgoing Mail	TCP #<< > 25
TELNET - Remote Connection	TCP #~~C > 23
TELNET - Secondary Remote Connection	TCP すべて > 8023
TELNETSSL - Secure Remote Connection over SSL	TCP #<<7 -> 992

※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

以上で設定は終了です。

新規に作成したサービスでローカルサーバを設定する場合

■ユーザ定義サービスの新規作成

ここでは、本製品にあらかじめ登録されていないサービスを設定し、ローカル サーバを利用する方法について説明します。

1 サイドバーから[セキュリティ設定]アイコンをクリックします。



2 [ローカルサーバ]タブをクリックします。

- #352 77セス制作 ローカルワーバ パーチャルコンビュータ リモートアクセス設定 パクットフィルス セキュリティログ	— [セキュリティ設定]画面に切 り替わります。
● セキュンテ・	クリックします。

3 [新規作成]欄から [追加] ボタンをクリックします。



4 新規サービスを登録します。 [ユーザ定義サービス]をクリックします。

	💭 ローカルサーバの 🕍	hu	
口-九6-82)			
2-17家業サービス	サービス名	プロトコル / ポート	<u></u>
77781 487 CA			2022
TAI Traffic		プロトコル オペア	

5 [ユーザ定義サービス]画面が表示されます。 [新規作成]欄から[追加]ボタンをクリックします。

第 ユーザ定義サービス]	[ユーザ定義サービス] 画面に 切り替わります。	
新規作成	サービス名	プロトコル / ポート	1847) 		ボタンをクリックします。
	₩ 展5				

6 [サービスの編集]画面が表示されます。 [新規作成]欄から[追加]ボタンをクリックします。

			――― [サービスの編集] 画面に切り
サービス名:	Application		替わります。
サービスの説明:			
プロトコル	IFA	1411	
新規作成		<u></u>	――― 🏧 ホタノをクリックします。
	✓ OK X #+>tz/		

6 [プロトコル]欄から使用するプロトコルを選択し、ポート番号を入力します。

[プロトコル]

対象にするプロトコルをTCP、UDP、ICMP、GRE、ESP、AH、その他から選択 します。その他を選択したときは、対象にするプロトコル番号を直接指定して ください。

[送信元ポート/送信先ポート]

サービスやアプリケーションのポート番号を入力します。 すべて →全てのポートを指定します。 1個を指定→1つのポート番号を指定します。 範囲指定 →ポート番号の範囲を指定します。

[ICMPメッセージ]

対象にするICMPメッセージを選択します。

7 [OK]ボタンをクリックします。



8 さらに [追加] ボタンをクリックすることで、複数のポートを指定する こともできます。



9 全ての設定が終了しましたら、[サービス名]欄に任意の名前を入力し、[OK] ボタンをクリックします。 10 [ユーザ定義サービス]の画面に戻ります。

[サービス名]欄に作成したユーザ定義サービスが表示されてるのを確認 します。[戻る]ボタンをクリックします。

☞ ユーザ定義サービス			
サービス名	プロトコル / ポート	律作	戻ります。
Application	TCP すべて -> すべて	92 80	
新规作成		it: to	
	R ð		ーーーー クリックします。

11 [ローカルサーバの追加]の画面に戻ります。 [ユーザ定義サービス]欄に作成したユーザ定義サービスが表示されてるの を確認し、チェックします。

🌉 ローカルサーバの追加		「ローカルサーバの追加」	面面
口一力ル本スト		に戻ります。	
サービス名	プロトコル / ポート		
ユーザ定義サービス 図 hpp fration		チェックします。	
) <u>+</u>)) 0000	

12 ローカルサーバ機能を使用するパソコンの設定を行います。 [ローカルホスト]欄にローカルサーバ機能を使用するパソコンのIPアドレス を入力します。

	💂 ローカルサーバの	逾加
ローカルホスト	1001000100	
	サービス名	プロトコル / ポート
ユーザ定義サービス		
Application		TCP すべて -> すべて

13 [OK]ボタンをクリックします。

HTTP - Web Server	TCP #~~T -> 80
HTTP - Secondary Web Server	TCP #157 > 8080
HTTPS - Secured Web Server	TCP 3 <7 > 443
HTTPS - Secondary Secured Web Server	TCP #<7℃ -> 8443
TFTP - File Transfer	UDP 1024-65535 > 69
DKAP - Messaging Server	TCP 才べて → 143
NNTP - News Server	TCP $\#\!\!\!\!/\!\!\!/ \tau \gg 119$
Ping - ICMP Echo Request	ICMP Echo Request
POP3 - Incoming Mail	TCP $\#\!<\!\!\!\!\!<\!$
SNMP - Simple Network Nanagement Protocol	UDP #<<7 > 161
SMTP - Outgoing Mail	TCP #<<℃ >> 25
TELNET - Remote Connection	TCP 91-17 -> 23
TELNET - Secondary Remote Connection	TCP オペて -> 8023
TELNETSSL - Secure Remote Connection over SSL	TCP #<<7 >> 992

※[OK]ボタンは画面の下の方にあります。スクロールして表示させてください。

14 [ローカルサーバ]の画面に戻ります。ローカルサーバで使用するサービス とパソコンのIPアドレスが表示されます。

REAL 702780 P-M-9	● セキュリティ パ の株式のサーバニインターキットから7	設定 モートアクセス設定 100ットフィ ウセスできるように、ます。	13 27407499
ローカルネスト	0-20-10	サービス名	1815
192.168.1.10	Resolving	Application	8 Z (H)
Marina			200

- **15** [OK]ボタンをクリックします。
- 16 以上で設定は終了です。
■ユーザ定義サービスの修正

ここでは、既に作成したユーザ定義サービスを修正する方法について説明します。 **1** サイドバーから[セキュリティ設定]アイコンをクリックします。



2 [ローカルサーバ]タブをクリックします。

- 載調定 アクセス制成 ローカルサーバ パーチャルコンビュータ リモートアクセス制定 パケットフィルタ セキュレディログ	│ ── [セキュリティ設定]画面に切 │ り替わります。
● 七キュリテ・ペル象大 前信やり - ・ すぐて転着 前信やり - ・ つみは人部やいろいう言葉部子: Televet, FTP, ● 七キュリテ・ペル電準 前信や) - ・ すぐて転着 夏日やり - ・ すぐて転着 ● 七キュリテ・レージを有 ● 七キュリテ・レージを有	クリックします。
記録がジー・すべな新す - ロッフラランシトバゲットを感謝する - マット (ダートを感謝する)	

3 設定を変更するパソコンの [修正] ボタンをクリックします。

	」 をキュリティ語	12]	
ー教授定 7クセス制限 ローカルサー LANEの	-パ パーチャルロビュータ 料金のサーバにインターネットからア	モートアクセス設定 パケットフィル クセスできるようにします。	ゆ セキュリティログ		「ローカルサーバ」の設定画面
D~JJJJJ #21	□- <i>b</i> i/IP	サービス名 Application	2017) 022 <u>000</u>		に切り替わります。
ы́ялуя ∠ ск	X \$ \$260 (197%)	20Em Atoen]	姬 ボタンをクリックします。

4 [ローカルサーバの編集]画面が表示されます。 [ユーザー定義サービス]をクリックします。

)ローカルサーバの編集		
ローカルネスト	THE PART OF		
ユーザ定義サービス	7-EX6	プロトコル / ボート	――― クリックします。
Application		700 #477 5 #477	

5 [ユーザ定義サービス]画面が表示されます。設定を変更したいサービスの [修正] ボタンをクリックします。

j 2−45	2義サービス	
サービス名 Application	プロトコル / ボート TCP すべて -> すべて	
新規作成		――― 🏧 ボタンをクリックします。
	50 D	

6 [サービスの編集]画面が表示されます。設定を変更したいプロトコルの [修正] ボタンをクリックします。

	虜 サービスの編集		
サービス名:	Application		おわります
サービスの説明:			自わりより。
거마누그ル	1740	- 1813	
TCP	オペモ シ オペモ	22	
新规作成			
PERCENC			――― 🚾 ボタンをクリックします
	V OK X++DAZE		_

7 [サービスの編集]の画面が表示されます。設定を変更したい項目を修正し、 [OK]ボタンをクリックします。



8 [OK]ボタンをクリックします。

	A	1	 「サービフの編隹]
	1 - CX0 - E		
-6.7.6:	Jeptication		替わります。
22.0100			
카마니ル	24	20	
)P	プル を < プルを	02 33	
M/G/G		100 C	

9 [ユーザ定義サービス]画面に戻ります。 [戻る]ボタンをクリックします。

<u></u> +7€1	夜 サービス		
サービス名	プロトコル / ポート	操作	
Application	UDP すべて -> すべて	19 Z MIS	
新規作成		10.00	
- v R:	<u> </u>		ーーーー クリックします。

10 以上で設定は終了です。

■ユーザ定義サービスの削除

サイドバーから[セキュリティ設定]アイコンをクリックします。



2 [ローカルサーバ]タブをクリックします。

- #数字 77セスBR ローカルターバ パーチャルコンビュータ リモートアクセスBR ハバフットフィルス セキュリアィログ	[セキュリティ設定]画面に切 り替わります。
● たちょりア・ ペル最大 酸性り ・すって転帯 酸化り ・・うみすう パロワ・1つ約37 ・・のあう ● たちょりア・ ・・小化電琴 副前や) ・・すって転帯 見目や) ・・すって転帯 見目や) ・・すって転帯 別目や) ・・すって転帯 別目や) ・・すっては両す 回りフランシトドグットも思約する	クリックします。

3 [新規作成]欄から [追加] ボタンをクリックします。



4 [ユーザ定義サービス]をクリックします。

	
ローカルペスト ユーザに高サービス サービス名 プロトコル / ポート	
EJAppRiation デフォルト変換サービス	29220690
DAI Traffic 3™ viation	

5 [ユーザ定義サービス]の画面が表示されます。削除したいサービスの [削除] ボタンをクリックします。



- 6 [戻る]ボタンをクリックします。
- 7 以上で設定は終了です。

設定したローカルサーバの修正

1 サイドバーから[セキュリティ設定]アイコンをクリックします。



2 [ローカルサーバ]タブをクリックします。

- 新設定 アクセスを取 ローカルワーバ パーチャルコンセータ リモートアクセス設定 パワットフィルク セキュリティログ	[セキュリティ設定]画面に切 り替わります。
・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	クリックします。

3 設定を変更したいパソコンの [修正] ボタンをクリックします。



4 [ローカルサーバーの編集] 画面が表示されます。 使用するサービスまたはパソコンのIPアドレスを変更できます。

D-101#2F	■ ■ ■ ■ ■ ■ ■ ■ ーカルサーバの割	¥]	[ローカルサーバの編集] に切り替わります。	画面
	サ- パス名	プロトコル / ポート			
ユーザ定義サービス					
Application		UDP すべて -> すべて		<u>+</u> ==, , ,	
				変更します。	

- 5 [OK]ボタンをクリックします。
- 6 以上で設定は終了です。

ローカルサーバの有効/無効の切替

1 サイドバーから[セキュリティ設定]アイコンをクリックします。



2 [ローカルサーバ]タブをクリックします。

- 新設定 7クセス和区 ローカルターバ パーチャルコンビュータ リメモートアクセス和E パケットフィルタ セキュレディログ	[セキュリティ設定]画面に切 り替わります。
● セキュリテ・ペル最大 町(44) ・・・・・・・・・・・・・・・・・・・・・・・・	クリックします。
他はやジン・すべて許可 発展やジン・すべて許可 レマンラジンとトバラットを送所する	

3 [ローカルホスト]欄からサービスを無効にしたいIPアドレスのチェックを 外します。



- [OK] ボタンをクリックします。
- 5 以上で設定は終了です。

設定したローカルサーバの削除

1 サイドバーから[セキュリティ設定]アイコンをクリックします。



2 [ローカルサーバ]タブをクリックします。

・ 世界コリティ設定 ・ 世界コリティ設定 アクセス8課 ローカルサーバ ハーチャルスピュータ リモートアクセス非定 パケットフィルタ セキュリティログ	│ [セキュリティ設定]画面に切 │ り替わります。
() セメルア ベメル 化 酒(オリ)・・・すべて転汚 オリア・・・・ボボオコ ガリア・・・・・・ボボオコ ガリア・・・・・・・・・・・・・・・・・・・・・・・・・	クリックします。





- 4 [OK]ボタンをクリックします。
- 5 以上で設定は終了です。

バーチャルコンピュータの設定

バーチャルコンピュータ機能を使用すると、LAN側にある1台のパソコンをイン ターネット上に公開できます。次のようなときに、バーチャルコンピュータを 指定します。

- ・[ローカルサーバ]機能のリストにはないオンラインゲームやビデオ会議用の ソフトウェアで、使用するポートなどの情報が公開されていない場合。
- ・セキュリティの制限無しに、1台のパソコンで全てのサービスをインターネット に公開する場合。

! ご注意

- ・バーチャルコンピュータとして、複数のパソコンを設定することはできません。
- バーチャルコンピュータとして設定したパソコンは、ファイアウォールで保護 されていないため、外部から攻撃を受ける恐れがあります。
- ・ローカルサーバ機能とバーチャルコンピュータ機能を同時に設定している ときは、ローカルサーバの設定が優先されます。
- DMZ (ポート)機能とバーチャルコンピュータ機能を同時に設定することは できません。



インターネットからLAN側へのアクセス要求を受け取ると、本製品は[ローカル サーバ]機能で登録されてる宛先を除き、すべてバーチャルコンピュータへその 要求を転送します。

LAN側のパソコンをバーチャルコンピュータに設定する

■ バーチャルコンピュータ設定

1 サイドバーから[セキュリティ設定]アイコンをクリックします。



2 [バーチャルコンピュータ]タブをクリックします。

「秋田王」フクセス4回 ローカルタール パーチャルエズムータ DVEーチアクセス8日王 パクットつルスターズ - 秋田王 アクセス4回 ローカルタール パーチャルエズムータ DVEーチアクセス8日王 パクットつルスタービー	[セキュリティ設定] 画面に切 り替わります。
● セキュリティレールなど #101/20-1-95/03 ● ビヤュリティレールの #1071-1072-05/03 ● ビヤュリティレールの #1071-1072-05/03	ー クリックします。
□ IP>95/50H109+5588#55	

3 [バーチャルコンピュータ IPアドレス]欄にチェックを付け、バーチャル コンピュータにするパソコンのIPアドレスを入力します。



- 4 [OK]ボタンをクリックします。
- 5 以上で設定は終了です。

■ バーチャルコンピュータの有効/無効の切替

● サイドバーから[セキュリティ設定]アイコンをクリックします。



2 [バーチャルコンピュータ]タブをクリックします。

使 セキュリア (設定 「新設定 アクセスを図 ロールシター」ド パーチャルスペム・ジ レモートアクセス設定 パリットフィルグ セキュリティログ	└── [セキュリティ設定]画面に切 り替わります。
● セキュリティレーダあるス 取得センシー:すべて転着 別がワービスの人は例をかい、ついの現合気や目:Telenet_FFP, いけい、HTV、HTV、HTV、HTV、HTV、GS, JAND ● セキュリティレーダあ名年 取得センシー:すべて転着 取得センシー:すべて転着 取得センシー:すべて転着 取得センシー:すべて転着 取得センシー:すべて転着 取得センシー:すべて転着 取得センシー:すべて転着 取得センシー:すべて転着 取得センシー:すべて転着 取得センシー:すべて転着 のは、日本シング、日本を必要が、 ● ビアコラクシント107ットを駆除する	ー クリックします。

3 [バーチャルコンピュータIPアドレス]欄からチェックを外します。



- 4 [OK]ボタンをクリックします。
- 5 以上で設定は終了です。

ダイナミック DNS の設定

WEBサーバなどをインターネットに公開するときは、固定のグローバルIPアドレスが本製品に割り当てられている必要があります。しかし、インターネットに常時接続していても切断、再接続の際に動的にIPアドレスが変ってしまう場合があります。

ダイナミックDNSを使用すると、本製品のIPアドレスをダイナミックDNSサーバ に一定間隔で通知することで、IPアドレスが変わった場合でも固定のホスト名が 使用できます。

ダイナミックDNSは、下記に対応しています。

- DynDNS.org
- Dynamic DO!.jp
- MyDNS.JP
- ※「Dynamic DO!.jp」と「MyDNS.JP」は、「カスタム設定」から「ダイナミック DNS(国内のサービス)」を選択することで利用できます

! ご注意

- ・本製品は「www.dyndns.org」ダイナミックDNSサービスに対応しています。
 本製品のダイナミックDNSの設定を行う前に、「www.dyndns.org」にアクセスし、ユーザ名、パスワード、ホスト名の登録を行ってください。
- 「www.dyndns.org」は、無償のサービスです(2005年5月現在)。
 また、プロバイダによっては本設定を使わなくても、ダイナミックDNSを
 実現することが出来る場合があります。詳しくは、プロバイダにお問い合わせ下さい。

ダイナミックDNSの設定

1 サイドバーから[カスタム設定]アイコンをクリックします。 ここでは、DynDNS.orgを例に説明します。



2 [ダイナミックDNS(DynDNS.org)]アイコンをクリックします。



3 [ダイナミックDNS]の画面が表示されます。 [有効にする]欄にチェックを付け、ダイナミックDNSサービスに登録した 内容をもとに各項目を入力します。



[ステータス]

現在の更新情報が表示されます。

[ユーザ名]

ダイナミックDNSサービスに登録されているユーザ名を入力します。

[パスワード]

ダイナミックDNSサービスに登録されているユーザパスワードを入力します。

[ホスト名]

登録したホスト名とドメイン名を入力してください。

[メールサーバ]

メールサーバを登録したい場合は、メールサーバのホスト名を入力します。

- ▲ [OK]ボタンをクリックします。
- 5 以上で設定は終了です。

設定が完了するとダイナミックDNSサーバへ本製品が取得しているIP アドレスを24時間毎に通知するようになります。

VPNの設定

VPN (Virtual Private Network) は、データのカプセル化や暗号化などのセキュリ ティ技術を使って、インターネットを仮想的に、専用線で接続したWANのよう に利用する技術です。VPNを構築するためには、PPTP (Point to Point Tunneling Protocol)やIPSec (IP Security)などのプロトコルが用いられます。 ここでは、PPTPとIPSecによるVPN接続の方法について説明します。 本製品は、PPTPサーバとPPTPクライアントおよびIPSecの機能を搭載して いるため、パソコンにVPN用のソフトウェアを導入する必要もなく、強固な

セキュリティ機能をもつ VPNを構築することができます。



VPNを構築するには、簡単接続ウィザードによる設定をした後、ネットワーク 詳細設定によって、詳細な設定が可能です。次ページの簡単接続ウィザード から設定を進めてください。必要に応じて、すでに簡単接続ウィザードによる VPN接続設定が終わっている場合は、「ネットワーク詳細設定による設定」に進 んでください。

簡単接続ウィザードによる設定

ここでは、簡単接続ウィザードを使いVPNを構築する方法について説明します。 本製品はPPTPサーバ、PPTPクライアント、IPSecに対応しています。ご利用 する環境に合わせて設定を進めてください。

PPTPサーバと各クライアント、またはIPSecの各拠点は、LAN側をそれぞれ別のセグメントにする必要があります。

■ PPTP クライアントの設定

本製品をPPTPクライアントとして使用する場合の設定について説明します。



128

1 サイドバーから[簡単接続ウィザード]アイコンをクリックします。



2 [VPN接続]を選択し、[次へ]ボタンをクリックします。

商単接続ウィザード 商単接続ウィザードを開始します。ネックワーク接続の種類を選択してださい。	[簡単接続ウィザード] 画面に切 り替わります。
 ・	選択します。
	クリックします。

3 [PPTP クライアント]を選択し、[次へ]ボタンをクリックします

₽ [₽] VPN接続] [\/PN 培結] 面面に切り基わり
VPN接続の種類を選択してください。	ます。
PPTPクライアント PPTPや党使用してインターネット磁曲でオフィスなど3線等他のVPNサーバに接続し ます。	選択します。
○ PPTPサーパ 遠隔地からのPPTP接続を許可します。	
○ IPSec 初告課をよび公開課を使用したデータの場号化とデジタル2回却による謝目相手 の記録を行い、インターネット提出での安全なデータの注意性を可能によす。	
< 25 x++5.70V	クリックします。

4 リモートアクセスするサーバの設定に従い、PPTP接続の設定を行います。 [送信先のホスト名またはIPアドレス]に接続するPPTPサーバのIPアドレス を入力し、[接続ユーザ名]、[接続パスワード]に接続する時のユーザ名と パスワードを入力します。 [次へ]ボタンをクリックします。

PTP 損限の設定をします。] [PPTP クライアント] 画面に 切り替わります。
送信先のホスト名またはJPアドレス: 掃読ユーザ名 (火☆≠/l☆≠/l注意): 描読/(スワード:	入力します。
	クリックします。

5 [接続完了]画面が表示されます。
 PPTP接続するサーバ名またはIPアドレスを確認し、[完了]ボタンをクリックします。

洗の新し、場感ぎ作成するための準備が完了しました。	<u>│</u> [設定完了] 画面に切り替わりま │す。
 ・ VPNサーバ ・ ユーザ名: 	│ │ 確認します。
完了 ボタンをクリックすると新しい 接続ガネットワーク算紙組設定のページュ作成されます。 キャンセル ボタンをクリックすると新しい 接続を作成せずにワッイザードを終了します。	
	クリックします。

■ PPTP サーバの設定

本製品をPPTPサーバとして使用する場合の設定について説明します。



1 サイドバーから[簡単接続ウィザード]アイコンをクリックします。



2 [VPN接続]を選択し、[次へ]ボタンをクリックします。



3 [PPTPサーバ]を選択し、[次へ]ボタンをクリックします。

₽ [₽] ₩PN接続	VPN 接続画面に切り替わります。
VPN根kの確認を選択してください。	
○ PPTPクライアント PPTPを使用してインターネット経由でオフィスなど遠隔地のVPNサーノ3に接続し ます。	
 ● PPTPサーバ 過隔地からのPPTP接続を許可します。 	選択します。
○ 1PSec 転送課表にびた問題を使用したデータの接着化とデジタル認識による適性相手 の認識を行い、インターネット経由での安全なデータの決定す意可能にします。	
< E5	クリックします。

4 PPTPサーバにアクセスを許可する為のユーザ設定を行います。 [ユーザの追加]の[追加]ボタンをクリックします。

PPTP接续档	并可するユーザをf	🌠 ユーザ		――― [ユーザ] 画面に切り替わります。
フルネーム	ユーザ名	権限	操作	
Administrator	admin	管理者権限 ファイルサーバからのファイルの読み込み ファイルサーバへのファイルの書き込み		
ユーザの追加			10.00	――― 🏧 ボタンをクリックします。
	< R ð) 次へ > メ キャンセル		

5 [一般設定]欄のフルネーム、ユーザ名、新しいパスワード、新しいパスワード の確認に登録するユーザの設定を入力し、[権限]欄からPPTPリモートアク セスにチェックをつけます。

2	2 ユーザ設定	ーーー [ユーザ設定] 画面に切り替わり
一般設定		よる。
フルネーム:	brc	
ユーザ名 (大文字/小文字に注意)	brc	
新ししい(スワード:		——— 人力します。
新し、パスワードの確認:	••••	
権限:	□ 年頃ま物現 ビアアアリモートアクセス □ ファイルサー」 (%にペーノルコン) (約32.54) □ ファイルサーバへのファイルの書き込み □ US8カメラ	――― チェックします。
E-Mail通知設定	SMTPメールサーバの設定	
E-Mailアドレス:		
システム通知レベル:	tau 🗸	
セキュリティ通知レベル:	tal 💌	
	к =+>121/	―― クリックします。

6 ユーザの追加または修正、削除が終わると[ユーザ]画面に戻りますので、 [次へ]ボタンをクリックします。

C - ノリー・ C - ノー・ C - ノー・
フルキーム ユーザ名 種聚 性作 ministrator admin 管理希望 0
フルチーム ユーザ名 催練 操作 dministrator admin 管理者権限 1
dministrator admin 管理者権限 pm
ser user PPTPUモートアクセス 📴 🎟
–ரீறங் ய

7 PPTP クライアントのリモートアドレスを入力します。

PPTP サーバにリモートアクセスするユーザに割り当てる IP アドレスの範囲 を入力し、「次へ」ボタンをクリックします。



8 [設定完了]画面が表示されます。 [完了]ボタンをクリックします。

a 🗳 2644 7	[設定完了] 画面に切り替わりま
次の新しい接続を作成するための準備が充了しました。	9.0
 ppppサーバ 	
完了 ボタンをグリックすると新しい接続がネットワーク詳細設定のページに作成されます。 キャンセル ボタンをクリックすると新しい接続を作成せ fricウィザードを終了します。	
(< 戻る) (第71)	クリックします。

インターネットに接続されている場合、PPTPクライアントの設定が完了 すると、自動的にPPTPサーバへ接続を行います。

■IPSecの設定

本製品を使いIPSecによるVPN接続を行う場合の設定について説明します。



1 サイドバーから[簡単接続ウィザード]アイコンをクリックします。



2 [VPN接続]を選択し、[次へ]ボタンをクリックします。

簡単接続ウィザード 簡単接続ウィザードを開始します。ネットワーク接続の推動を選択してださい。	〕[簡単接続ウィザード]画面に切 り替わります。
 インターネット撮談 インターネットへ撮談するための設定をします。 アPN撮談 VPN(原想ブライベートネットワーク)を構築するための設定をします。 	選択します。
	クリックします。

3 [IPSec]を選択し、[次へ]ボタンをクリックします。



4 接続するIPSecの情報を入力し、[次へ]ボタンをクリックします。 設定により入力する項目が異なる場合があります。

P ^P IPSec	[IP Sec] 画面に切り替わります。
IPSec搗铳の設定をします。	
接続先のホスト名またはIPアドレス: リモートサブネット	
リモートサブネットアドレス: 0	──── 入力します。
シェアードキー:	
< 戻る (法へ >) · · · · · · · · · · · · · · · · · ·	クリックします。

[接続先のホスト名またはIPアドレス]

IPSecで接続する相手側のIPアドレスを入力します。

[リモートサブネットアドレス]

IPsecで接続する相手側のネットワークアドレスを入力します。

[リモートサブネットマスク]

IPSecで接続する相手側のサブネットマスクを入力します。

[シェアードキー]

IPSec間で認証を行うときに使う事前共有キーを入力します。

キーの値は両方のルータで同じ値を入力します。

5 [設定完了]画面が表示されます。[完了]ボタンをクリックします。



ネットワーク詳細設定による設定

PPTPクライアントやサーバに関する詳細な設定と、IPSecの詳細設定について 説明します。

VPNの詳細な設定をするためには、あらかじめ「簡単接続ウィザード」による設 定を終了しておく必要があります。

■ PPTP クライアントの詳細設定

1 サイドバーから [ネットワーク詳細設定] アイコンをクリックします。



2 [ネットワーク詳細設定] 画面が表示されます。詳細な設定を行う VPN PPTP 接続の [修正] ボタンをクリックします。

	📲 ネットワーク詳細設定		
接続名	ステータス	操作	切り替わります。
o LAN Ethernet	掃統	97	9J9 E199 8 98
6 WAN PPPOE	报晓	80 II (100	
VPN PPTP	再接绕処理中		🚮 ボタンをクロックしまう

3 [ネットワーク詳細設定 VPN PPTP] 画面が表示されます。接続名、ステー タス、ユーザ名等が表示されていますので、確認して[詳細設定] ボタンを クリックします。

<u>م</u> ال	ットワーク接続 VPN PPTP	───── [ネットワーク接続 VPN P ↓ サーバ] 画面に切り替わりる
	無効	
接続名:	VPN PPTP	
ステータス:	再接続処理中	
接続タイプ:	VPN PPTP	
ユーザ名:	brc	――― 確認します。
受信パケット:	0	
送信パケット:	0	
トータルパケット:	0	
√ ок	★キャンセル 「詳細設定 」	 クリックします。

4 [詳細設定 VPN PPTP] 画面が表示されます。PPTP サーバ管理者の通知 に従って設定します。

◎基本設定、PPP、PPP認証の設定

[PPP]

接続先のホスト名またはIPアドレス、接続ユーザ名、接続パスワードには、簡単 接続ウィザードで設定した内容が表示されています。変更する必要がある項目を 修正します。

自動切断までの時間は、PPTPによる通信が中断したときに接続を切断するまでの 時間を分単位で入力します。

[PPP認証設定]

ユーザ認証のためのプロトコルを選択します。PPP暗号化で「暗号化を許可する」 場合は、MS-CHAP またはMS-CHAP v2 を選択します。

	🍟 詳細設定 VPN	РРТР ———	<u> </u>	[詳細設定 VPN F	PTP]	画面(
基本設定				切り省わります。		
揺続タイプ:	VPN PP	TP				
MTU:	自動設定	Ë 🔽 1460				
РРР						
接続先のホスト名またはIPアドレス:	10.10.10	0.1				
接続ユーザ名 (大文字/小文字に注意)	brc					
撤続パスワード:		••				
自動切断までの時間:	20	分				
PPP認証						
□ PAP認証を許可する (PAP)						
□ CHAP認証を許可する (CHAP)			<u> </u>	設定します。		
✔MS-CHAP認証を許可する (MS-CHAP)						
☑ MS-CHAP y2認証表許可すろ (MS-CHAP #2)						

◎ PPP 暗号化、IP 設定

パケットの暗号化に関する設定を行います。

[PPP暗号化]

- ・暗号化を必ず要求する:
 暗号化通信を要求するときにチェックします。サーバが拒否するとPPTP通信は
 確立されません。
- ・暗号化を許可する:
 暗号化にMPPE (Microsoft Point-to-Point Encrypeion)を使用します。40bitの
 キーで暗号化するか、128bitのキーを使うかで、MPPE-40かMPPE-128を選択します。
- MPPE暗号化モード:
 暗号化のモード(Stateless または Stateful)を選択します。Statelessはパケット ごとに暗号化キーを変更するので、通信の安全性は高くなります。Statefulは 複数のパケット単位で暗号化キーを変更します。
 暗号化を許可する場合は、上のPPP認証で、MS-CHAPまたは、MS-CHAP v2 が選択されていることを確認してください。

[IP設定]

IPアドレスを固定にするか、自動取得するかを選択します。 [サブネットマスクを置き換える]は、固定のサブネットマスクを利用するときに チェックし、そのときのサブネットマスクを指定します。

[DNSサーバ]

DNSサーバアドレスを自動取得するのか、固定設定にするのかを選択します。固定 にする場合は、プライマリとセカンダリDNSサーバのIPアドレスを指定します。 なお、[DNSサーバ]をクリックすると、[カスタム設定]で[DNSサーバ]を選んだ 状態になります。

[デバイスメトリック]

メトリックの値を入力します。

! ご注意

必ず [NAPT] は有効の状態でお使いください。

PPP暗号化		
□ 暗号化を必ず要求する (サーバが把否したとき	(1240MF)	
✓暗号化老許可する (MPPE-40Bit)		
✓最強の暗号化を許可する (MPPE-1288 H)		
MPPE暗号化モード:	Stateless 🛩	
IP設定	IPアドレスを自動取得する 💌	――― 設定します。
DNSサーバ	DNSサーバアドレスを自動取得する 💌	
NAPT:	有効 🖌	
デバイスメトリック:	10	
□マルチキャスト - IGMP Proxy Default		

5 [OK] ボタンをクリックすると設定が有効になり、[ネットワーク接続 VPN PPTP] 画面に戻ります。

■ PPTP クライアントの削除

ここでは、既に登録してあるPPTPクライアント接続を削除する場合について 説明します。

1 サイドバーから [ネットワーク詳細設定] アイコンをクリックします



2 [接続名]欄から削除する VPN PPTP 接続の[修正]ボタンをクリックします。

ステータス 操作	切り麸わります
19 E	9556155898
80 M 8	
Auge	――― 🏧 ボタンをクリックします。
	48項中

3 回線が接続されてる場合は、[無効]ボタンをクリックし、回線をいったん 切断します。[OK]ボタンをクリックします。

6 ≉:	ットワーク接続 VPN PPTP	
接続名:	VPN PPTP	
ステータス:	再接続処理中	
接続タイブ:	VPN PPTP	
ユーザ名:	brc	― <u>-</u> クリックします。
受信バケット:	0	
送信パケット:	0	
トータルパケット:	0	
Сис	Y ± ω [*] .470Ⅱ, 詳純報告会	クリックします。

4 [接続名]欄から削除する VPN PPTP 接続の[削除]ボタンをクリックします。

	骨 ネットワーク詳細設定		└ [ネットワーク詳細設定] 画面
接続名	ステータス	操作	切り麸わります
LAN Ethemet	报线	20	のり目100よ9。
WAN PPPOE	接绕	200	
VPN PPTP	無効	E MIS	🕂 🌃 ボタンをクリックします。

- 5 [戻る]ボタンをクリックします。
- 6 以上で設定は終了です。
■ PPTP サーバの詳細設定

1 サイドバーから [ネットワーク詳細設定] アイコンをクリックします



2 [ネットワーク詳細設定] 画面が表示されます。詳細な設定を行う VPN PPTP サーバ接続の [修正] ボタンをクリックします。

	₽₽ ネットワーク詳細設定	
接続名	ステータス	排作
الم LAN Ethemet	报纸	97
6 WAN PPPOE	报统	10 II 10
PS pptpサーバ	报続待機中	10 T
	I¥kalkiz	

※PPTPサーバを削除する場合は、[修正] ボタンをクリックし、[PPTPサーバ] 画面の[有効] 欄からチェックを外します。

3 [PPTPサーバ] 画面が表示されます。

[詳細設定] ボタンをクリックします。 なお、ここでユーザの編集、PPTPクライアントの接続設定も可能です。

		[PPTP サ ー バ] 画面に切り替わ
PPTPサーバ		ります。
ステータス:	报统诗棚中	
☑有効		
🗳 ユーザ		
リモートアドレス範囲		
開始:		
終了:		── 表示されます。
接続		
接続名	ステータス 操作	
 ✓ OK 	 メキャンセル 詳細設定 	クリックします。

4 [PPTPサーバ] 画面が表示されます。PPTPサーバの詳細な設定を行います。

■ 二 ☆ PPTPサーバ		
PPTPサーバ		ן (
ステータス:	接続待機中	
☑有効		
್ಷ ೨–ザ		
自動切断までの時間(分):	20	
▶認証が必要		シューシュ
許可する認証アルゴリズム:	□ PAP □ CHAP ☑ MS-CHAP-V1 ☑ MS-CHAP-V2	取たしより
▶暗号化が必要		
許可する暗号化アルゴリズム:	MPPE-40 MPPE-128	
MPPE暗号化モード:	Stateless 🗸	

[ステータス]

PPTP サーバの接続状況を表示します。

[有効]

PPTPサーバを有効にするときにチェックします。このチェックをはずすと、 PPTPサーバとして動作しなくなり、接続状況にも反映されなくなり、また詳細 設定の画面からも削除されます。

[自動切断までの時間]

PPTPによる通信が中断したときに、接続を切断するまでの時間を分単位で入力します。

[ユーザセキュリティ]

PPTPを使用した通信での認証と暗号化について設定します。

- ・認証が必要: PPTPクライアントが接続するときに、ユーザ認証を必要とするときにチェック します。接続テストなど特別な場合を除いて必ずチェックを入れてください。
- ・暗号化が必要: PPTPクライアントが接続するときに、暗号化通信を要求する場合にチェックします。

[許可する認証アルゴリズム]

ユーザセキュリティで認証が必要にチェックをした場合、認証のアルゴリズムを PAP、CHAP、MS-CHAP-v1、MS-CHAP-v2 から選択します。暗号化をする場合 は、MS-CHAP-v1かMS-CHAP-v2をチェックしてください

[許可する暗号化アルゴリズム]

ユーザセキュリティで暗号化が必要にチェックをした場合、暗号化アルゴリズム をMPPE-40 と MPPE-128 から選択します。

[MPPE暗号化モード]

暗号化のモード (Stateless または Stateful)を選択します。

- Stateless:
 パケットごとに暗号化キーを変更するので、通信の安全性は高くなります。
- Stateful: 複数のパケット単位で暗号化キーを変更します。
- 5 [簡単接続ウィザード]で設定した、リモートアドレス、クライアントとして 動作する場合のPPTPクライアントの設定が表示されます。クリックし修正 することが可能です。

開始:		A reason	
終了:			
接続			確認しま
按结点	フテータフ	操作	

6 [OK] ボタンをクリックすると、設定が有効になりネットワーク詳細設定 画面に戻ります。[基本設定] ボタンをクリックすると、PPTPサーバの最初 の画面に戻ります。

■IPSecの詳細設定

1 サイドバーから [ネットワーク詳細設定] アイコンをクリックします



2 [ネットワーク詳細設定] 画面が表示されます。詳細な設定を行う VPN IPSec 接続の [修正] ボタンをクリックします。

	◎◎ ナットワック詳細語空	
接続名	ステータス	操作
🕯 LAN Ethernet	接続	9 I
6 WAN PPPOE	接続	(8.7. WH
VPN IPSec	接続待ち	
	EVANER:	
	annual	

3 [ネットワーク接続 VPN IPSec] 画面が表示されます。[詳細設定] ボタン をクリックします。

<u>ن</u> ب	トワーク接続 VPN IPSec	
	無助	
报続名:	VPN IPSec	
ステータス:	扱続待ち	
接続タイプ:	VPN IPSec	
IPアドレス:	83.084.0.050	
サブネットマスク:	1995-0.0-0	
 ✓ OK 	メキャンセル 詳細設定	─ <u>├</u> ─── クリックします。

「詳細設定 VPN IPSec」 画面が表示されます。

基本設定	
権続タイプ:	VPN IPSec
IPSec	
機続先のホスト名また」はIPアドレス:	100.00.00.0
防御モード:	トンキリング
ローカルサブネット	
ローカルサブネットアドレス:	the line is in
ローカルサブネットマスク:	
リモートサブネット:	
リモートサブネットアドレス:	in the test
リモートサブネットマスク:	
ロデータ圧縮 (IRCOMPTITE TIL)	

- [詳細設定 VPN IPSec] 画面に 切り替わります。

ここで次の項目を設定します。

基本設定

[接続先のホスト名またはIPアドレス]

簡単接続ウィザードで設定した接続先が表示されています。必要であれば修正 します。

[ローカルサブネット]

本製品のLAN側のサブネットアドレス、サブネットマスクを設定します。

[リモートサブネット]

接続先のサブネットアドレスとサブネットマスクを入力します。

[データ圧縮]

データ圧縮をするときにチェックします。

[キー交換方式]

暗号化アルゴリズムや鍵交換のためのSAの合意をとる方式を選択します。

・自動:

IKE (Internet Key Exchange)を使って、SAの合意を通信時に自動的に行う場合 に選択します。通常は、自動に設定しておきます。

・手動:

SAの合意をあらかじめ手動で設定しておく場合に選択します。画面が手動用に 切り替わります。

! ご注意

必ず手動モードは「トンネリング」の状態でお使いください。

5 キー交換方式を自動に設定します。

キー交換方式を [自動] に設定した場合、次の2つのフェーズの設定を行い ます。まず、IPSec IKE, Phase 1の設定をします。

建交换方式:	自動(IKE) 🖌	
IPSec IKE, Phase 1		
接续减行回数	3 💌	
ライフタイム (粉:1-28800)	3600	
Rekey Margin (線の再生成を期間のh の何分前に開始するか: 1-540)	540	
Rekey Fuzz (Rekey Marginをランダムに変更する %: 1-200)	100	
認証アルコリズム	共通續(Shared Secret) 🖌	
共通醒(Shared Secret)	test	
暗号化アルゴリズム		
DES-CBC		
SDES-CBC		
ハッシュアルゴリズム		
W MD5		
SHA1		
Diffie-Hellman Group		
DH Group 1 (768 bit)		
✓ DH Group 2 (1024 ын)		
DH Group 5 (1536 bit)		

IPSec IKE, Phase 1

[接続試行回数]

ネゴシエーションの試行回数を設定します。

[ライフタイム]

キーの有効期限を秒単位で設定します。

[Rekey Margin]

Rekey (キーの再生成)を期限切れの何秒前に開始するかを設定します。

[Rekey Fuzz]

Rekey Marginをランダムに変更するパーセンテージを設定します。

[認証アルゴリズム]

認証の方式を選択します。

- ・シェアードキー方式: 共通キー方式を選択する場合は、事前共有キーの文字列を入力します。 (かんたん設定ウィザードで入力した鍵が表示されます。)
- ・公開キー方式: 公開キー方式を使用する場合に、キーの文字列を入力します。

[暗号化アルゴリズム]

使用する暗号化アルゴリズムをチェックします。

[ハッシュアルゴリズム]

使用するハッシュのアルゴリズムをチェックします。

[Diffie-Hellman-Group]

対応するグループをチェックします。

6 次にIPSec IKE, Phase 2の設定をします。

ライフタイム (砂: 1-86400) I PFS有効 (Perfect Forward Secrecy)	28000		
I PFS有助 (Perfect Forward Secrecy)			
暗号化アルゴリズム			
AH(暗号化なし)			
ESP(暗号化なし)			
ESP(DES-CBC)			
ESP(3DES-CBC)			
提展アルゴリズム ((ESP))			設定しまる
₩ MD5			NEUG 9
SHA1			
ハッシュアルゴリズム ((AH))			
W MD5			
♥ SHA1			
デバイスメトリック:	10		
□マルチキャスト - IGMP Proxy Default			
TIRIP - ルーティングプロトコル			

IPSec IKE, Phase 2

[ライフタイム]

キーの有効期限を秒単位で設定します。

[PFS有効]

Secrecy(PFS)を使用する場合にチェックします。

[AH]

認証ヘッダの設定をします。ハッシュアルゴリズムを選択します。

[ESP]

暗号ペイロードの設定をします。暗号化アルゴリズムと認証アルゴリズムの設定 をします。

[デバイスメトリック]

メトリックの値を入力します。

- 7 「詳細設定 VPN IPSec]画面の設定内容を確認し、[OK] ボタンをクリック して、設定を有効にします。
- 8 IPSecを利用しVPNを構築する場合は、IPフラグメントパケットを透過 させる必要がありますので、[セキュリティ設定] 画面で、[IPフラグメント パケットを遮断する] のチェックをはずしてください。

「「」 セキュリティ設定		<u> </u> [セキュリティ設定]画面に切り
- 戦闘定 アクセス制限 ローカルサーバ バーチャルコンピュータ リモート	ウセス酸モ パケットフィルタ セキュリティロダ	替わります。
○セキュリティレベル最大		
着信がリント: すべて相応 発信がリント: 一部許可 決めジナビスのXLAMからWAIへの発信を許可: Teir HTTP, HTTPS, DNS, IMAP, POP3, SMTP	iet, FTP,	
・ セキュリティレベル標準		
著信やパシー: すべて拒否 発信やパシー: すべて許可	E	
○ セキュリティレベル最小		
着信やパシー: すべて許可 発信やパシー: すべて許可	=	
□IPフラヴェントパケットを追続する		└─── チェックをはずしてください。
(Z OK) (X 4+5/25	0	

■キー交換方式を手動に設定する場合

キー交換方式で手動を選択したときは、接続先の設定にあわせて暗号化アルゴ リズム、認証アルゴリズムを設定する必要があります。

IPSec 手動總交換		
セキュリティインテックス - SP1: (1688) ローカル: リモート:	0 0	
ローカルとリモートで異なる暗号化キ	ーを使用する	
(PSecプロトコル:	ESP 🛩	
暗号化アルゴリズム:	3DES-CBC 💌	
キー :		し スカレキマ
121日アルゴリズム:	SHA1 🗸	1000
+-:		
デバイスメトリック:	10	
□マルチキャスト - IGMP Proxy De	fault	
□ RIP - ルーティングプロトコル		
	✓ CK (X = + 5/20/)	

暗号化アルゴリズム、認証アルゴリズムのキーは、16進数8桁ずつに区切って 入力してください。

■VPNの接続、切断

サーバ側、クライアント側でインターネットに接続すると、自動的にLAN同士 が接続されます。

 IPSecによる通信を切断したい場合は、[ネットワーク詳細設定] 画面で、 [VPN IPSec] の[修正] ボタンをクリックします。

₽┓ ネットワーク詳細設定			[ネットワーク詳細設定] 画面
接続名	ステータス	i#fe	切り基わります
🖌 LAN Ethernet	招徒	伸正	9J9日12969。
6 WAN PPPOE	接线	(9 E ALI)	
🗸 VPN IPSec	揺続待ち		
	IF KELLE		―― 🏧 ホタンをクリックしてください

2 [ネットワーク接続 VPN IPSec] 画面になりますので、[無効] ボタンを クリックします。

أ ^ب	小ワーク接続 VPN IPSec	
接続名:	VPN IPSec	
ステータス:	接続待ち	
接続タイプ:	VPN IPSec	
IPアドレス:	83. 200 A. 200	
サブネットマスク:	2705-0.0-0	
		─ <u>↓</u> クリックします。

IPSec接続に関してその他次の設定が可能です。

■キーの再生成

1 サイドバーから [カスタム設定] アイコンを選択します。



2 [IPSec] アイコンをクリックします。



3 [IPSec] 画面が表示されます。[詳細設定] ボタンをクリックします。

	Prec IPSec		 [IPSec] 画面に切り替わります
不正アクセス通販			
回海劝			
最大リトライ回数	5		
送班和中国 (19)	60		
接続			
捕获名	ステータス	操作	
o vpn Ipsec	播続待ち	神道 利禄	
(vok			クリックします。

4 [IPSec設定]画面が表示されます。[キーの再生成] ボタンをクリックし、 再生成を行います。



5 表示の更新ボタンをクリックすると、再生成されたキーが表示されます。 [戻る] ボタンをクリックすると [IPSec] 画面に戻ります。

■IPSec ログの設定

IPSec通信のログに関する設定を変更することができます。

1 カスタム設定で [IPSec] アイコンをクリックし、IPSec 画面で [ログ設定] ボタンをクリックします。

	Prec IPSec		[[PSec] 画	面に切り替わり	=
不正アクセス通断						
「「「御女功」						
最大リトライ回政	5					
运用和书籍(MP)	60					
接続						
接続名	ステータス	律作				
VPN IPSec	捕獲待ち	98 正 利約				
 ✓ ok. 			:	クリックしま	す。	

2 [IPSecログ設定] 画面が表示されます。記録したい内容にチェックを つけます。

Image: State State State State Image: State State State Image: State State State State Image: State State State Image: State State State State Image: State State State Image: State State State State Image: State State State Image: State State State State State Image: State State State State Image: State State State State State State Image: State State State State State Image: State	₽∰ IPScログ厳定	
	企業 注意 すべてのJPSetGZダオジョンを自知にすると 88(C-14V のバフォーマンスに影響します。	わります。
Privacy free dools Privacy free doo	10003/100g	ه و ی <i>د</i> د ۱
The start is the start and benefition and benefition The start is the start is start in the start is start is start in the start in the start is start in the start in the start is start in the start is start in the start is start in the start	Massage's Raw Bytes	
	Message's Encryption	
	Message's input Structure	
eveness advances (regroup	Message's Output Structure	
	Verbose Automatic Keyling	
	Everbose IKE IPSec Interaction	
	Verbose Private Keys	
Therefore the second and the s	IPSect29202	
	Turneling Code	
Developacitaministration color	Turneling Transmit Code	「 チェック」 きす
Thermal Head And The Resolution code Impared Head The Resolution code	Usen-8pace Communication Code	
The second seco	Transform Selection and Manipulation Code	
Takat terminakan oleh Takat Kerupatan oleh Takat Taka Taka	Internal Route Table Manipulation code	
	Secure Association Table Manipulation code	
Devenues fraudure cole	Radij Tree Nanipulation Code	
Ellautheritistion Transforms Code	Encryptions Transforms Code	
	Authentication Transforms Code	

3 [OK] ボタンをクリックすると設定が有効になり、[IPSec] 画面に戻ります。

IPSecの削除

ここでは、既に登録してある IPSec 接続を削除する場合について説明します。

1 サイドバーから [ネットワーク詳細設定] アイコンをクリックします



2 [接続名]欄から削除するVPN IPSec接続の[修正]ボタンをクリックします。

g	◎ えっしり こう詳細語空	
Ľ	「「ネットノーン計翻設定	
接続名	ステータス	操作
🦸 LAN Ethernet	接続	MI.
6 WAN PPPOE	接続	(8)正 (FIL)
VPN IPSec	接続待ち	
	IVANISE	

3 回線が接続されてる場合は、[無効]ボタンをクリックし、回線をいったん 切断します。[OK]ボタンをクリックします。



4 [接続名]欄から削除する VPN IPSec 接続の[削除]ボタンをクリックします。

B9 +	ロニカ鉄細糖電		[フットワーク詳細設定]
E +9	ドリージ計雑設定		
推続名	ステータス	推作	切り耸わります。
oʻ LAN Ethernet	接続	10 II	
6 WAN PPPOE	接続	WIR MIR	
o VPN IPSec	接続待ち	25 7.122	――― 🌃 ボタンをクリックしき
C	IXABIRDE		
-			

5 以上で設定は終了です。

オプション設定

ここでは、本製品を利用してオプション機能を設定します。本製品の設定は、 有線LAN接続でおこなってください。

VRRP

本製品は、VRRP機能に対応しており、ルータの冗長化を行うことができます。 VRRPを設定することで、通常利用している回線・ルータが何らかの理由により 切断されたときに、同一グループ内のルータが自動的に通信が継承できます。 この機能を使用するためには、VRRP機能に対応した複数のルータを1つのグ ループに所属させておく必要があります。 以下の設定例を使用して紹介します。

[設定例]

各ルータに実際に存在しない仮想IPアドレスを設定し、マスタールータからの 回線が何らかの原因で不具合が発生したとき、バックアップルータが代わりに 通信を開始します。

	マスタールータ (BRC-W14VG①)	バックアップルータ (BRC-W14VG②)
IPアドレス	192.168.50.250	192.168.50.250
VRRP ID	1	1
優先度	250	100
プリエンプトモード	有効	有効



1 設定例イメージのように接続し、マスタールータ側にログインします。



2 サイドバーから [カスタム設定] アイコンをクリックします。

3 「カスタム設定」が表示されますので、[VRRP]アイコンをクリックします。



4 「VRRP」が表示されますので、「仮想ルータの追加」をクリックします。

	Y VRR	P			
仮想ルータIPアドレス	VRRP ID	優先度	ステータス	操作	
仮想ルータの追加 ―				1010	クリックし
				-	

- 5 「VRRP設定」が表示されますので、下記項目を設定します。
 - ①「IPアドレス」に「192.168.50.250」を入力します。
 - (1-255)」に「1」を入力します。
 - ③「優先度」に「250」を入力します。
 - ④「プリエンプトモードを有効にする」のチェックをオンにします。
 - ⑤「監視対象」で監視する対象を選びます。
 - ⑥ [有効]ボタンをクリックします。

۲ ۲	VRRP設定
IPアドレス:	192 168 50 250
VRRP ID(1-255):	1
VRRP达I書面場: 優先度(1-255):	250
■ プリエンプトモードを有効にす	73
監視対象:	WAN PPPOE WAN PPPOE 2
有効	

6 続いて、バックアップルータ側の設定を行います。バックアップルータに ログインし、2から5の手順をおこないます。 7 「VRRP 設定」が表示されますので、下記項目を設定します。

- ①「IPアドレス」に「192.168.50.250」を入力します。
- ②「VRRP ID (1-255)」に「1」を入力します。
- ③「優先度」に「100」を入力します。
- ④「プリエンプトモードを有効にする」のチェックをオンにします。
- ⑤「監視対象」で監視する対象を選びます。
- ⑥ [有効]ボタンをクリックします。

۲		
IPアドレス:	192 .168 .50 .250	 入力します。
VRRP ID(1-255):	1	
VRRP送信間隔:	1 秒	
優先度(1-255):	100	
☑ プリエンプトモードを有効にす	\$	
監視対象:	 WAN PPPoE WAN PPPoE 2 	
有効		クリックします。

以上で、設定が完了しました。

!ご注意

[BRC-W14VG側]

・DHCPサーバ機能は、[無効]に設定することをお勧めします。

[各コンピュータ側]

- ①IPアドレスを手動で設定し、「デフォルトゲートウェイ」に仮想IPアドレスを 設定します。設定例の場合は、「192.168.50.250」です。
- ②DNSサーバは、プロバイダから指定されたDNSサーバを設定することをお勧め します。

[IPアドレス]

VRRPで利用する仮想ルータのIPアドレスを設定します。クライアントのデフォル トゲートウェイアドレスにはこのIPアドレスを設定します。

 同じVRRP IDに属するルータのIPアドレスを指定するとき 仮想ルータのIPアドレスを持つルータがマスタルータとなり、他のルータはバッ クアップルータになります。

○実在しないIPアドレスを指定するとき マスタルータは優先度の設定によって自動的に決定されます。IPアドレスは同一 サブネットのIPアドレスを設定します。

[VRRP ID]

仮想ルータで利用するグループのIDを設定します。値は1~255までの数値で設定します。初期値は0です。

VRRP IDを同じ値に設定したルータは同一グループに属し、1台がマスタルータとして動作し他はバックアップルータとして動作します。

マスタルータ停止時に、バックアップルータへ処理を移行し、通信を継続します。

[VRRP送信間隔]

VRRPに設定されたルータがLANへ送信するパケットの送信間隔を設定します。単位は秒です。初期値は1秒です。

マスタルータがパケットを送信し、バックアップルータが受信することでVRRPが 動作していることがわかるようになります。

[優先度]

VRRPで動作するルータの優先度を設定します。値は1~255までの数値で設定します。初期値は100です。値が大きいほど優先度は高くなります。

[プリエンプトモードを有効にする]

プリエンプトモードを設定します。プリエンプトモードの設定でマスタルータの選 ばれ方が変わります。

○プリエンプトモードが有効のとき

VRRPで動作するルータに優先度の高いルータが加わるとマスタルータが移行し ます。有効で利用されることをお勧めします。

○プリエンプトモードが無効のとき マスタルータ停止時などでバックアップルータへ移行したあと、優先度の高い VRRPのルータが加わってもマスタルータは移行しません。

[監視対象]

既存の接続から監視対象を選びます。

IPv6ブリッジ

本製品は、IPv6ブリッジ機能に対応しています。WAN-LAN間の通信データを ブリッジすることができます。

これにより、通常のPPPoEによるインターネット接続とFLET'S.NETなどのIPv6 ネットワークをLAN側に設置されたパソコンで同時にご利用頂くことが可能にな ります。

※パソコンのIPv6設定については、お使いのパソコン及びOSの取扱説明書などを参照して ください。



1 サイドバーから [カスタム設定] アイコンをクリックします。

[IPv6ブリッジ] アイコンをクリックします。



「IPv6ブリッジを有効にする」のチェックをオンにします。

₽ [■] IPv6ブリッジ	
	── チェックします。
✓ OK ★+>ンセル	

[OK] ボタンをクリックします。

PPPoE ブリッジ

本製品は、PPPoEブリッジ機能に対応しています。本機能を利用することで、 LAN側に接続したパソコンが直接PPPoE接続して通信することができます。

※パソコンのPPPoE接続の設定については、お使いのパソコン及びお使いの取扱説明書を ご覧ください。

1 サイドバーから [カスタム設定] アイコンをクリックします。





3 「PPPoEブリッジを有効にする」のチェックをオンにします。

PPPoEブリッジ	
	チェックします。
✓ OK X キャンセ2ル	

4 [OK] ボタンをクリックします。

USBカメラの設定

本製品のUSBインタフェースに接続したUSBカメラ(別売)で撮影した静止画 や動画を、リモートアクセスしたPCや携帯電話で見ることができます。 ここでは、USBカメラを有効にする設定と画像を見る方法について説明します。 本体に接続できるUSBカメラは1台のみです。



※本機能は、USBカメラ「BRC-EE260」にのみ対応しています。その他のUSB カメラには対応していません。本製品へのUSBカメラ接続方法は、USBカメラ 「BRC-EE260」の取扱説明書をご参考ください。 USBカメラ設定

● サイドバーから [オプション設定] アイコンをクリックします。



2 [オプション設定] 画面が表示されます。[USBカメラ]アイコンをクリックします。





[USBカメラ] 設定画面が表示されます。本製品にUSBカメラ接続後、 「オン] にチェックをつけます。

	🧕 USBカメラ		
USBカメラ: 動画ビットレート:	 ● オン・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	チェックしま	;す。
USBカメラを撤続していない状態で「オン」に設定して	<u>入</u> 注意 にもUSBカメラは有効にはなりません。		
	OK キャンセル		

! ご注意

- ・[USBカメラ] 設定画面の「オン/オフ」は、デフォルトの設定が「オフ」になっています。
- ・USBカメラが「オン]の状態でカメラを取り外すと、自動的に「オフ」に切り 替わります。
- **4** [画像ビットレート]から[高 (512Kbps)]または[低 (128Kbps)]のいず れかを選択します。
- [OK] ボタンをクリックします。
 USBカメラの撮影とストリーミングの画像の配信が自動的に始まります。

■インターネットからカメラ画像を見る場合

1 サイドバーから [セキュリティ設定] アイコンをクリックします。



2 [セキュリティ設定] 画面が表示されます。[リモートアクセス] ボタンを クリックします。

	虜 セキュリティ設定		
- 敏政定 75世	2008 ローカルサーバ バーチャルコンピュータ リモートアクセス設定		└──── クリックします。
	◎セキュリティレベル最大		
	着信わジンー: すべて振活 気信和ジンー: - 3月3 月 次のサービスのみにムがかSWANへの発信支持町:Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3, SMTP		
	⊙ セキュリティレペル標準		
	著信和パシー: すべて報告 発信和パシー: すべて終可		
	○ セキュリティレペル最小		
	着信約パシー: すべて許可 発信約パシー: すべて許可	***	
	□₽フララシントノイケットを過新する		

3 [リモートアクセス設定]画面が表示されます。 [WEBサーバを外部に公開する (プライマリポート)]または [WEBサーバを 外部に公開する (セカンダリポート)]から使用していないポート番号の方に チェックし、[USBカメラ画像を外部に公開する (TCPポート8090)] にチェ ックをつけます。



- **4** [OK] ボタンをクリックします。
- 5 以上で設定は終了です。

PCや携帯電話で画像を見る

■画像を見るための条件

USBカメラで取り込んだ画像をPCや携帯電話で見る場合、コンピュータや携帯 電話の種類によって以下のソフトウェアや条件が必要となります。

端末	静止画サイズ	動画サイズ	必要なソフトウェア・条件
			Microsoft [®] Internet Explorer5.5以上
Windows®	320×240	320×240	Netscape Navigator [®] 6.0以上
			Microsoft [®] Windows [®] Media Player7.0以上
			Microsoft [®] Internet Explorer5.5以上
			Netscape Navigator [®] 6.0以上
Macintosh®	320×240	320×240	Microsoft [®] Windows [®] Media Player Mac板
			(Windows [®] Media Player for Mac OS [®] X,
			Windows [®] Media Player 7.1 for Mac OS [®] 8-9
	000.0040	000.0040	Netscape Navigator [®] 6.0以上
Linux	320×240	320×240	Mplayerなど
100 total and a second	110.00		JPEG画像をサポートしている機種のみ。
携帝電話	112×96	なし	機種によっては利用できない場合があります。

■コンピュータで画像を見る

本製品にパソコンからリモートアクセスして、画像を見る方法について説明します。※BRC-14Vの画面を使用して説明します。

- 1 ブラウザから、URLを指定してリモートアクセスします。
 - ・インターネットからアクセスする場合 「http:// (WAN側アドレス) /cam/」
 - ・LANからアクセスする場合 「http://(LAN側アドレス)/cam/」

2 本製品にリモートアクセスすると、ログイン認証を行ないます。すでに登録してあるユーザ名とパスワードを入力してください。はじめてアクセスするときは、事前にログインユーザ名、パスワードを設定しなければなりません。設定方法は、180ページの「ログインユーザ名とログインパスワードの設定」を参照してください。



- ※なお、この認証機能は、撮影された画像・動画を特定の相手にのみ公開することを完全に保証する ものでありません。
- 3 ログイン認証終了後、[BRC-W14VG・ライブカメラ]画面が表示されます。 画面にあるメニューから、観覧するカメラ画像の種類を選択します。



[カメラ画像・静止画]

クリックすると静止画のページを表示します。

[カメラ画像・動画]

クリックすると動画のページを表示します。

[カメラページトップ]

このメインページを表示します。

メニュー項目を選択することで、どの画面からでも随時切り替えることできます。

「カメラ画像・静止画」を選択した場合、「ライブカメラ静止画像」画面が Δ 表示されます。「更新] ボタンをクリックすると、現在の画像を更新します。



[カメラ画像・動画]を選択した場合、「ライブカメラ動画」 画面が表示さ 5 れます。



「BRC-W14VG・ライブカメラ 動画〕画面に切り替わります。

! ご注意

- ・動画配信の場合、ネットワークの状況やWindows[®] Media Playerのバッファリ ング処理等のため、画像が表示されるまでに時間がかかる場合があります。
- ・動画、静止画ともに画像の輝度、コントラストなどの調整を行うことはでき ません。

■携帯電話で画像を見る

本製品に携帯電話からリモートアクセスして、画像を見る方法について説明します。

1 携帯電話のブラウザから、URLを指定してリモートアクセスします。

・携帯電話用アドレス: http://(WAN側アドレス)/i/

2 本製品にリモートアクセスすると、ログイン認証を行ないます。すでに登録してあるユーザ名とパスワードを入力してください。はじめてアクセスするときは、事前にログインユーザ名、パスワードを設定しなければなりません。設定方法は、180ページの「ログインユーザ名とログインパスワードの設定」を参照してください。



3 ログイン認証終了後、画像表示用のメインページが表示されます。[更新] ボタンをクリックすると、現在の画像を更新します。



保守・管理

本製品の運用開始後にネットワークの接続状態の確認や、管理者のログイン名 やパスワードの変更方法などを説明します。本製品の設定は、有線LAN接続で おこなってください。

機器状況の確認

接続状態の確認

各接続ポートごとに通信状態やアドレス情報等が確認できます。

◀ サイドバーから[システム情報]アイコンをクリックします。



[WAN Ehternet]

PPPoE以外の方法でインターネットに接続している場合の、WAN側の通信の状況 が確認できます。

[WAN PPPoE]

PPPoEでインターネットに接続している場合のWAN側の通信の状況が確認できます。

[LAN Ehternet]

LAN側の通信の状況が確認できます。

[VPN PPTP]

本製品がPPTPクライアントである場合の通信の状況が確認できます。

[VPN IPSec]

IPSecで通信している状況が確認できます。

稼動時間の確認

ここでは本製品が稼動してからの現在までの時間を確認できます。

● PLNEX ■ -1 = -1 ■ -1 = -1 ■ -1 = -1 ■ -1 = -1 ■ -1 = -

1 サイドバーから[システム情報]アイコンをクリックします。

2 [稼動時間] タブをクリックします。

岐 トラフィック シフ	(テムロダ 稼働時間		<u></u> クリックしま
接続名	WAN Ethernet	LAN Ethernet	
ステータス	動作中	接続	
接続タイプ	Ethernet	Ethernet	
MAC7FUZ	100-100 cor 000-000-020	00-90 ee 00-00-11	
IPアドレス		1982 2088 2.5	
サブネットマスク		1748.2766.2766.0	
DHCPサーバ	第.95	有効	
受信パケット	28826	10694	
送信パケット	11847	15109	
トータルバケット	40673	25803	
	(BINER OF	表示の更新	

●画面表示の自動更新を停止する

[カスタム設定] 画面 – [システム設定] 画面で [システム情報ページの表示の自動更新を 行う] をチェックしているときは、[システム情報] の各画面は一定間隔で自動更新され ます。このとき、[システム情報] の各画面の [自動更新 Off] ボタンをクリックすると、 [表示の更新] ボタンをクリックした時のみ、[システム情報] の各画面の内容が更新 されるようになります。
ログインユーザ名・ログインパスワード設定

本製品のログインユーザ名とパスワードの登録、変更、または削除ができます。 ユーザは50以内とすることをお勧めします。

※50以上のユーザを設定すると、本製品の動作パフォーマンスに影響すること があります。

ログインユーザ名とログインパスワードの設定

■ユーザの新規作成

1 サイドバーから [カスタム設定] アイコンをクリックします。



2 [ユーザ] アイコンをクリックします。



3 [ユーザの追加] 欄から「追加」 ボタンをクリックします。



4 [ユーザ設定] 画面が表示されます。 フルネーム、ユーザ名、新しいパスワードを入力します。

		ります。	
フルネーム: ユーザ名 (大文字/小文字に注意)			
新し、パスワード:		- 入力します。	
新し、パスワードの確認:			

[フルネーム]

登録するユーザのフルネームを入力します。半角英数字で128桁まで入力できます。

[ユーザ名]

新しく登録するユーザのログイン名を入力します。半角英数字で64桁まで入力 できます。

[新しいパスワード]

ユーザがログイン時に使用するパスワードを入力します。半角英数字で64桁まで 入力できます。

大文字と小文字は区別されますのでご注意ください。

[新しいパスワードの確認]

「新しいパスワード」と同じパスワードを再度入力します。

5 本製品での権限を設定します。

権限:	□管理者権限 □ PPT リモードプセス □ ファイルサーバからのファイルの読み込み □ ファイルサーバへのファイルの書き込み □ USbカメラ
-----	--

[管理者権限]

ユーザを管理者として登録する場合は、チェックします。

[PPTPリモートアクセス]

PPTPによる VPN 接続を許可する場合は、チェックします。

[ファイルサーバからのファイルの読み込み]

USBハードディスク接続時に、ディスク内のファイルの読み込みを許可する場合は、 チェックします。

[ファイルサーバからのファイルの書き込み]

USBハードディスク接続時に、ディスク内のファイルの書き込みを許可する場合は、 チェックします。

[USBカメラ]

USBカメラ接続機能に、カメラ画像の閲覧を許可する場合は、チェックします。

6 E-mail通知を利用する場合は、E-mailアドレス、システム通知レベル、セキュリティ通知レベルを設定します。

E-Mailアドレス:		
システム通知レベル:	tal. 💌	REUS S
セキュリティ通知レベル:	tal 🗸	

※E-mail通知機能に関してはE-mail通知機能をご参照ください

7 [OK] ボタンをクリックします。



8 以上で設定は終了です。

1 サイドバーから [カスタム設定] アイコンをクリックします。



2 [ユーザ] アイコンをクリックします。



3 設定を変更したいユーザの[修正]ボタンをクリックします。



[ユーザ設定] 画面が表示されます。修正したい項目の変更を行い、[OK] ボタンをクリックします。

一般設定	ユーザ設定	[ユーザ設定] ります。	画面に切り替わ
フルネーム:	Planex		
ユーザ名 (大文字/小文字に注意):	planex		
新しいパスワード:	•••••		
新しいパスワードの確認:	•••••		
稽段:	 管理者権限 PPTP リモートアクセス ファイルのサーバからのファイルの様 み込み Dアイルサーバへのファイルの書き USBカメラ 		
E-Mail通知設定	SMTPメールサーバの設定		
E-Mailアドレス:			
システム通知レベル:	tal 💌		
セキュリティ通知レベル:	tal 💌		
Слок	We day to show	 クリックします	- o

5 以上で設定は終了です。

■ユーザの削除

1 サイドバーから [カスタム設定] アイコンをクリックします。



2 [ユーザ] アイコンをクリックします。



3 設定を削除したいユーザの「削除」ボタンをクリックします。



!ご注意

購入時に登録されてるAdministratorは削除することができません。

4 以上で設定は終了です。

システム設定

本製品のホスト名やLAN側のドメイン名などを設定できます。



1 サイドバーから[カスタム設定]アイコンをクリックします。

2 [システム設定] アイコンをクリックします。



3 [システム]欄に本製品のホスト名、ドメイン名を入力します。



[ホスト名]

本製品のホスト名を入力します。

- [ローカルドメイン] LAN内で使用したいドメイン名を入力します。
- 4 USBハードディスクを接続している場合、[ファイルサーバ]欄から [NetBIOSワークグループ名]を入力します。

ファイルサーバ		
NetBIOSリークタルーラ名:	Teatring	 └── 設定します。 │

[NetBIOS ワークグループ名]

LAN内で使用するワークグループ名を入力します。

5 [設定画面]欄から[システム情報ページの表示の自動更新を行う]、[ネット ワーク設定の変更時に確認を行う]を設定します。

設定画面		
	り自動更新を行なう	
▼ネットワーク設定の変更時に	確認を行なう	
セッションライフタイム:	900 秒	設定します。

[システム情報ページの表示の自動更新を行う]

[システム情報] 画面の表示を自動的に更新させたい場合は、チェックします。

[ネットワーク設定の変更時に確認を行う]

ネットワークに関する変更をしたときに、確認メッセージを表示させたい場合は、 チェックします。 **6** [システムリモートログ設定]、[セキュリティリモートログ設定]を利用する 場合は設定をします。

システムリモートロク設定		
システム通知レベル:	なし 💌	
セキュリティリモートログ設定		
セキュリティ通知レベル:	なし 💌	

※リモートログ設定に関しては、Syslogの設定をご参照ください。

7 ユーザ設定で E-mail 通知機能を利用している場合は、[SMTPメールサーバ] 欄にメールサーバのアドレスを入力します。

]
SMTPメールサーバ	
SMTPメールサーバ:	<u> </u> 入力します。
送信元メールアドレス:	

- 8 [OK] ボタンをクリックします。
- 9 以上で設定は終了です。

日付と時刻の設定

本製品の日付や時刻の設定を変更できます。

1 サイドバーから [カスタム設定] アイコンをクリックします。



2 [日付と時刻] アイコンをクリックします。



3 手動設定する場合は、新しい日付と時刻を入力します。

	行 日付と時刻		[日付と時刻] ります	画面に切り替わ
手動設定			50.00	
日付:	11月 🗸 5 🖌 2003 🗸			
1991:	14 : 57 : 32		設定します。	

4 自動設定する場合は、[自動設定]欄から[有効]にチェックします。



5 [NTPサーバアドレス]、[更新間隔]を入力します。

[NTPサーバアドレス]

指定したアドレスから時刻を指定します。

[更新間隔]

時刻を更新する間隔を指定します。

- 6 [OK] ボタンをクリックします。
- 7 以上で設定は終了です。

ファームウェアの更新

本製品の購入後、当社のホームページからダウンロードしたファイルを使って、 最新のファームウェアにアップデートすることができます。ファームウエアの アップデートの前には、本製品の設定内容を書き残し、必ず有線LAN接続する コンピュータでおこなってください。

! ご注意

- ・インターネットに接続している場合は、アップデートを行う前に全ての通信 を切断してください。また、LAN内のパソコンはアップデート作業を行う パソコンを除いて全て電源をOFFにしてください。
- ・ファイアウォールやウィルススキャンソフトがインストールされてるパソコン
 でアップデート作業を行う場合は、事前にソフトウェアを終了してください。
- このアップデートは当社が独自に提供するサービスです。新機能の追加や性能の増強を保証するものではありません。
- ・ファームウエアの更新中は、他の操作をおこなったり、本製品のACアダプタ、 LANケーブルは絶対に抜かないでください。ファームウエアの更新の失敗や、 本製品の故障の原因となる場合があります。
- 1 当社のホームページから最新のファームウェアをダウンロードします。 ダウンロードしたファイルは、アップデート作業を行うパソコンのハード ディスクなどに保存してください。
- 2 サイドバーから [カスタム設定] アイコンをクリックします。



4 [ファームウェアアップデートの準備]の画面が表示されます。 [参照]ボタンをクリックし、ダウンロードしたファームウェアのファイル を指定します。



5 [開く] ボタンをクリックします。



6 [OK] ボタンをクリックすると、ファームウェアアップデートの準備が 開始されます。

ご注意

ファームウェアアップデートの準備中は、絶対に本製品の電源を切ったり、LAN ケーブルを抜いたりしないでください。ファームウェアアップデートの準備には、 数十秒間かかります。[OK] ボタンをクリックしたら、そのまましばらくお待ち ください。

7 ファームウェアアップデートの準備が終了すると、[ファームウェアアップ デート]の画面が表示されます。 [現在のバージョン]と[新しいバージョン]に表示されるバージョン番号 に間違いが無いか確認してください。 [OK]ボタンをクリックすると、ファームウェアのアップデートが開始 されます。

! ご注意

ファームウェアのアップデート中は、絶対に本製品の電源を切ったり、LAN ケーブルを抜いたりしないでください。ファームウェアアップデートには、 数十秒間かかります。[OK] ボタンをクリックしたら、そのまましばらくお待ち ください。

- 8 アップデートが終了すると、本製品は自動的に再起動します。新しいバージョンのファームウェアは再起動後に有効になります。
- 9 再起動が完了すると、ログイン画面に戻ります。以上でファームウェアの 更新は終了です。

! ご注意

本製品以外のファームウェアを使ってアップデートを行うことはできません。 無理にアップデートを行うと本製品が動作しなくなりますので、ご注意ください。

診断ツール

本製品からパソコンなどのネットワーク端末に対して Pingを送信することが できます。



1 サイドバーから [カスタム設定] アイコンをクリックします。

2 [診断ツール] アイコンをクリックします。



3 [送信先IPアドレスまたはホスト名]欄にPingを送信したいIPアドレス またはホスト名を入力します。

武 診断ツール	[診断ツール]画面に切り替わ ―― ります。
Diac (Trub E-ba) 通貨用ロアドノ支払は本 ブナータス: ステータス: ボダンペクリックすると、ステータス表示変更新にます。	―― 入力します。
€ RO (BITORM)	― クリックします。

4 [送信] ボタンをクリックすると、本製品から宛先にPingが送信されます。

	🔀 診断ツール	
Ding (ICMD F	cha)	
送信先IPアドレス はホスト名:	くまた	
フテータフィ	10元は1.2の時間中	――― 表示されます

5 [ステータス]欄に送信結果が表示されます。

No. of Concession, Name			
	送信		
戈功しました			
/4 送信, 4/4 受信, 0% 損失			
を小 = 1 ms 現大 = 3 ms 呼均 = 1 ms			
The second se	\$JDLました /4 逆信, 4/4 受信, 0% 損失 秋 = 1 ms 秋 = 3 ms 約 = 1 ms	3功にました /4 逆信, 4/4 受信, 0% 損失 	はJULました /4 送信, 4/4 気信, 0% 損失 ▶/→ = 1 ms /均 = 1 ms

- **6** [戻る] ボタンをクリックします。
- 7 以上で設定は終了です。

本製品の初期化

設定ページから本製品の設定内容を消去して、購入時の状態に戻すことができ ます。

※本体にあるリセットスイッチを使って、設定を消去することもできます。

! ご注意

この機能を使うと、設定ページにアクセスするためのパスワードを含め、変更 した設定内容がすべて消去されます。また、本製品のLAN側ポートのIPアドレ スを変更していた場合は、購入時の「192.168.1.1」に戻ります。ご注意ください。



1 サイドバーから [カスタム設定] アイコンをクリックします。

2 [設定情報の初期化]アイコンをクリックします。



3 [OK] ボタンをクリックします。

12 設定情報の初期化	
	台わります。
日本人とうに実行してもようしん」ですか?	
CZ GR I A TYZEV	│ 」 [OK] ボタンをクリックします。

4 初期化が始まります。



5 設定内容の消去が終わると、設定ページに初めてログインするときの画面 に切り替わります。

BRC- W14VG 設 ブラウザに http:/ きます。 ブラウザのお気に) W14VG 設定画面	全 BRC-w14VG 設定画面 定画面 への最初のログインです。 /brcw14vg.home/と入力すると、BRC-W14VG設定画面にアクセスで VJ (ブックマーク)に http://brcw14vg.home/ を追加すると BRC- に関単にアクセスできます。	
ブラウザ	追加方法	
Internet Explorer	お気に入りに追加 をクリック	
Netscape	CTRL+D キーを押す	
その他	ブラウザの 'ブックマークの追加' を選択して、 http://brc w14vg.home/ を追加	
	С х ок	[OK] ボタンをクリックします。

※画面が切り替わらないときは、[ログイン]ボタンをクリックしてください。

6 ユーザ名とパスワードを入力し、[OK] ボタンをクリックします。 [ネットワークマップ設定画面] に切り替わります。

	│ ──[ログイン設定]画面に切り替わ │ ります。 ── 入力します。
新し、ログインパスワード: 新し、ログインパスワードの福 設:	クリックします。

[ログインユーザ名]

設定ページにログインするユーザ名を入力します。

[新しいログインパスワード]

パスワードを入力します。

[新しいログインパスワードの確認]

[新しいログインパスワード]の内容をもう一度入力します。

7 [OK] ボタンをクリックすると、設定ページの [ネットワークマップ設定 画面] に切り替わります。

設定情報の読み込み

1 サイドバーから [カスタム設定] アイコンをクリックします。



2 カスタム設定の [設定情報の保存/読み込み] アイコンをクリックします。



3 [設定情報の読み込み] ボタンをクリックします。



4 [設定情報の読み込み]の画面が表示されます。 [参照]ボタンをクリックし、設定ファイルを指定します。

€● 設定情報の読み込み] [設定情報の読み込み]の画面が
設定情報ファイルを選択して OK ボタンをクリックしてください。設定情報ファイルの読み込みが開始されます。	表示されます。
	│ │ クリックします。
✓ OK (X キャンセル)	

5 [開く]ボタンをクリックします。

ファイルの選択					? 🛛
ファイルの場所・	D: 🧰 設定ファイル		- +	a 💣 🖬•	
最近使ったファイ)					
デスクトップ					
6					
۲۲ F¥ュメント					
₹1 I)/Ľ1-Ø					
マイ ネットワーク					
	ファイル:名(11):			-	RR(©)
	ファイルの種類①	すべてのファイル (*,*)		-	74701

6 [OK] ボタンをクリックすると、設定情報の読み込みの準備が開始され ます。 7 設定情報の読み込みの準備が終了すると、[設定情報のアップデート]の 画面が表示されます。

[現在のバージョン] と [新しいバージョン] にはファームウェアのバー ジョンが表示されます。

バージョンが同じことをご確認の上、[OK] ボタンをクリックしてください。

設定情報のアップデート 設定情報のアップデート 設定情報ファイルの読み込みが売了しました。		
現在のバージョン:	バージョン	
新しいバージョン:	バージョン	
新しい	ージョンへのアップデートを実行しますか?	
		クリックします。

! ご注意

- 「現在のバージョン」と「新しいバージョン」にはファームウェアのバージョンが表示されます。
- ファームウェアのバージョンが異なると設定情報のアップデートができない
 場合がありますのでご注意ください。
- 8 アップデートが終了すると、本製品は自動的に再起動します。新しい設定 情報は再起動後に有効になります。
- **9** 再起動が完了すると、ログイン画面に戻ります。以上で設定情報の読み 込みは終了です。

設定情報の保存

1 サイドバーから [カスタム設定] アイコンをクリックします。



2 カスタム設定の[設定情報の保存/読み込み]アイコンをクリックします。



3 [設定情報の読み込み] ボタンをクリックします。



- 4 [ファイルのダウンロード]の画面が表示されます。[保存]ボタンをクリックしてコンピュータに保存します。
- 5 以上で設定情報の保存は終了です。

再起動

本製品の再起動を行います。

1 サイドバーから [カスタム設定] アイコンをクリックします。



2 [再起動]アイコンをクリックします。



[OK] ボタンをクリックします。



4 再起動が完了すると、ログイン画面に切り替わります。

SNMP

SNMPを設定することで、ネットワークに接続された機器類をネットワーク経由 で監視することができます。

※SNMP機能を使用するためには、別途SNMPマネージャなどが必要です。



サイドバーから[カスタム設定]アイコンをクリックします。

2 [SNMP] アイコンをクリックします。



3 「SNMPを有効にする」のチェックをオンにし、コミュニティ名(セキュリ ティ)を入力します。

🔗 SNMP	
コミュニティ名(リード): public ユミュニティ名(リード): private	チェックします
✓ OK ★キシセル	

[コミュニティ名(リード)]

監視対象サーバのステータスを収集するのみのセキュリティ(コミュニティ)を設 定します。初期値は、「public」になります。

[コミュニティ名(リード/ライト)]

サーバの設定変更(ディスクスレッショルドの設定や、IMLの消去等)に伴う操作を行うときのセキュリティ(コミュニティ)を設定します。初期値は、「private」となります。

MACアドレスの変更

MACアドレスで接続を管理しているときなど、機材を変更することによって接続 ができなくなる場合があります。そのようなことを避けるためにも、MACアドレ スを手動で変更することができます。

- PLANEX G. 品 ネットワークマップ (図) 簡単接続ウィザ・ 24.14 6 ¢, () 29488 クリックします。 システム体新 Planex1 192.168.1.2 Planex2 192.168.1.3 179 NRCE **R**
- **1** サイドバーから [カスタム設定] アイコンをクリックします。

2 「MACアドレスの変更」アイコンをクリックします。



3 変更したいMACアドレスを入力します。

	MACアドレスの変更	
ボート: 変更後のMACアドレス:	WAN Ethemet	┃ ┃ 入力します
	✓ OK X キャンセル	

[OK] ボタンをクリックします。

ファームウェア情報

本製品のファームウェアのバージョンを確認できます。

1 サイドバーから [カスタム設定] アイコンをクリックします。



2 [ファームウェア情報] アイコンをクリックします。



④ ファームウェア情報			- [ファームウェア情報]	画面に切
バージョン:	3.7.33.1.8		り替わります。	
	「東京」			