

機能詳細編

LAN側の設定	1
セキュリティの設定	45
LAN側パソコンサーバ公開設定	98
VPNの設定	126
オプション設定	157
保守・管理	166

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。

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

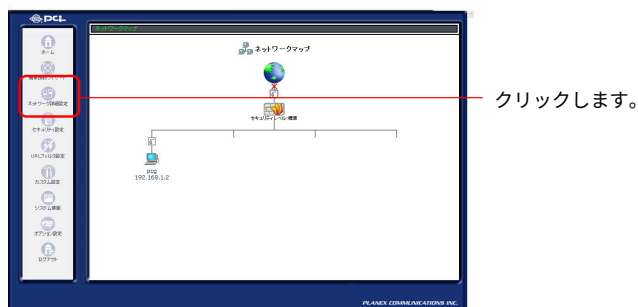
本製品の IP アドレスを変更する場合は、誤った IP アドレスを設定することのないようご注意ください。誤った IP アドレスを設定すると、インターネットに接続できなくなるなどのトラブルになることがあります。

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。



3 [詳細設定] ボタンをクリックします。



- 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。

「詳細設定 LAN Ethernet」画面に切り替わります。

必要に応じて各項目を設定します。

- 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

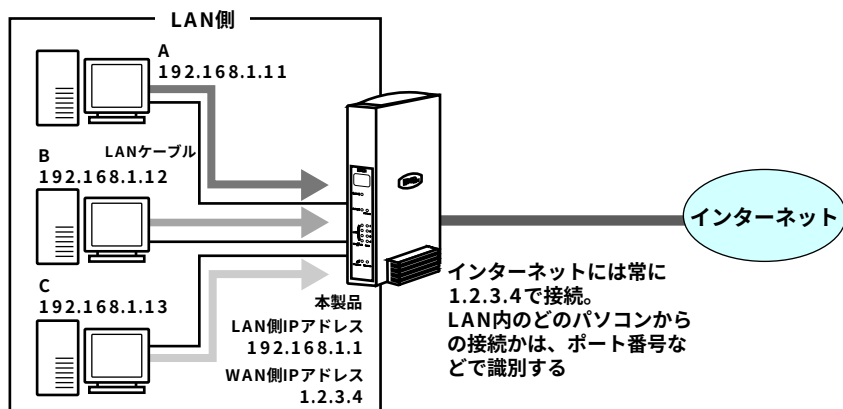
本製品のLAN側ポートのIPアドレスを変更するときに、LAN内で起動しているパソコンがある場合は、本製品のIPアドレスを変更した後でIPアドレスを再取得してください。

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。

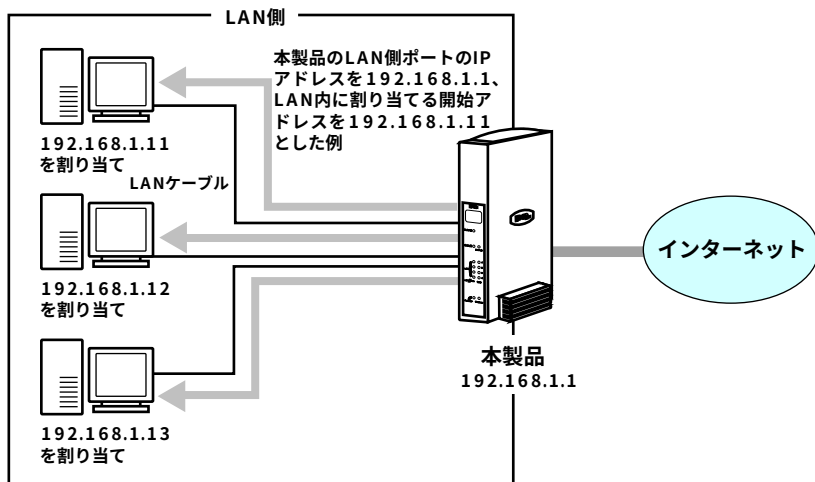
NAPTを使用した場合、LAN内で割り当てられてる複数のプライベートIPアドレスが、インターネットへの接続時に1つのグローバルIPアドレスに変換されます。さらに、ポート番号も変換されます。インターネット側からは、常に1台のパソコンがインターネットに接続しているように見えます。



※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することもできます。
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。

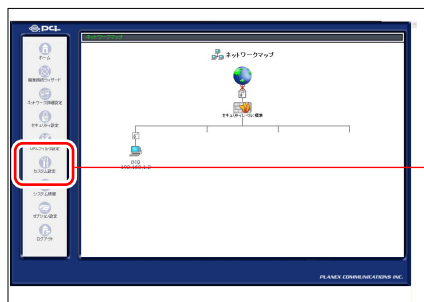
！ ご注意

- ・ 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]アイコンをクリックします。



クリックします。

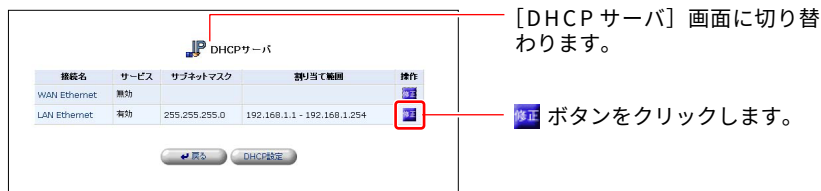
2 [DHCP サーバ]アイコンをクリックします。



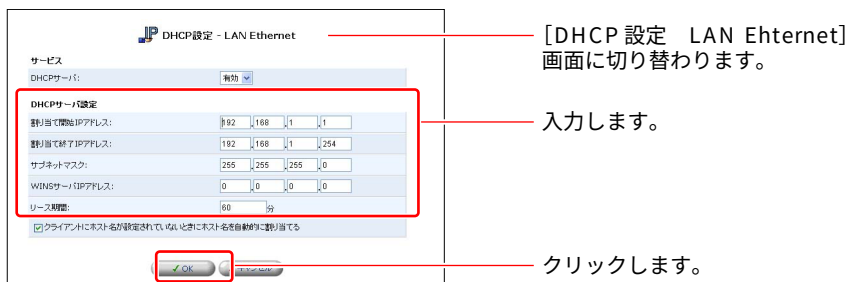
[カスタム設定] 画面に切り替わります。

クリックします。

- 3** 現在の DHCP サーバのサブネット、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。



- 4** [DHCP 設定 LAN Ethernet]の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。



[有効]

DHCP サーバ機能を有効にします。

[割り当て開始アドレス]

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。

[割り当てサブネットマスク]

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]

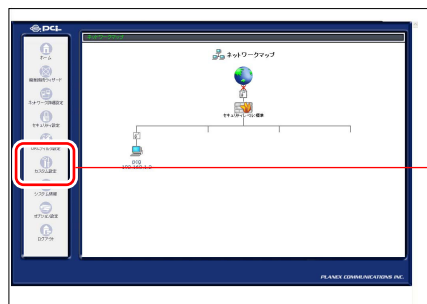
接続されているパソコンまたはネットワーク機器にホスト名が設定されていない場合自動的にホスト名が設定されます。

- 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。

- 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。



クリックします。

- 2 [DHCP サーバ]アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

クリックします。

3 [DHCP 設定]ボタンをクリックします。



[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	有効			[設定]
LAN Ethernet	有効	255.255.255.0	192.168.1.1 - 192.168.1.254	[設定]

戻る DHCP設定

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。



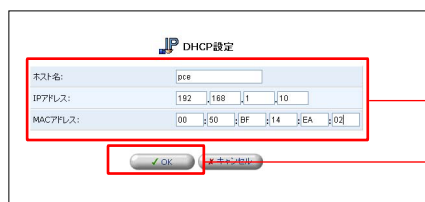
[DHCP 設定] 画面に切り替わります。

ホスト名	IPアドレス	MACアドレス	タイプ	接続名	ステータス	リース期間	操作
pcg	192.168.1.2	00:50:5f:14:ea:01	動的	LAN Ethernet	有効	43 分	[削除] [編集]
固定IP割り当ての追加							

戻る 追加

追加 ボタンをクリックします。

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。



DHCP設定

ホスト名: pce

IPアドレス: 192 . 168 . 1 . 10

MACアドレス: 00 : 50 : 5f : 14 : ea : 01

OK キーボードショートカット

入力します。

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。



ホスト名	IPアドレス	MACアドレス	タイプ	接続名	ステータス	リース期間	操作
010	192.168.1.2	00:50:b6:14:aa:01	静的	LAN1	接続中	30 分	 
018	192.168.1.10	00:50:b6:14:aa:02	固定	LAN1	接続中	60 分	 
既定IP数以上の追加							



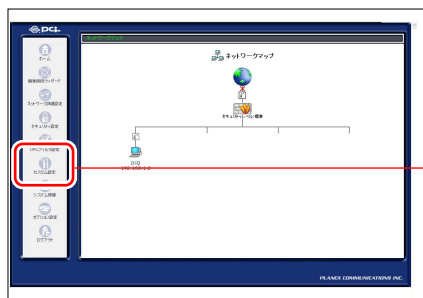
確認します。

7 以上で設定は終了です。

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。



クリックします。

2 [DHCPサーバ]アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

クリックします。

3 [DHCP 設定]ボタンをクリックします。

[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			設定
LAN Ethernet	有効	255.255.255.0	192.168.1.1 - 192.168.1.254	設定

戻る DHCP設定

クリックします。

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。

[DHCP 設定] 画面に切り替わります。

ホスト名	IPアドレス	MACアドレス	タイプ	接続名	ステータス	リース期間	操作
pcq	192.168.1.2	00:50:b7:14:ea:01	動的	LAN Ethernet	接続	37 分	修正
固定IP割り当ての追加							

戻る 修正

修正 ボタンをクリックします。

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。

固定IP割り当て

OK キャンセル

チェックします。

クリックします。

6 タイプが[固定割り当て]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。

確認します。

修正 ボタンをクリックします。

ホスト名	IPアドレス	MACアドレス	タイプ	接続名	ステータス	リース期間	操作
pcq	192.168.1.2	00:50:b7:14:ea:01	固定	LAN Ethernet	接続	36 分	修正
固定IP割り当ての追加							

- 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。

DHCP設定

ホスト名: pcg

IPアドレス: 192.168.1.2

MACアドレス: 00:50:bf:14:ea:01

☒ 固定IP割り当て

OK キャンセル

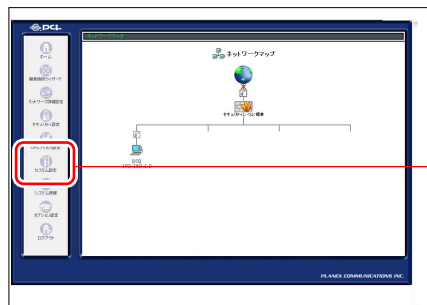
- 8** [OK]ボタンをクリックし、[DHCP 設定]画面に戻ります。

- 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。

1 サイドバーから[カスタム設定]をクリックします。



クリックします。

2 [DHCP サーバ]をクリックします。



[カスタム設定] 画面に切り替わります。

クリックします。

3 [DHCP 設定]ボタンをクリックします。

[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			
LAN Ethernet	有効	255.255.255.0	192.168.1.1 - 192.168.1.254	

戻る DHCP設定

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。

[DHCP 設定] 画面に切り替わります。

ホスト名	IPアドレス	MACアドレス	タイプ	接続名	ステータス	リリース時間	操作
p01	192.168.1.2	00:50:b7:14:ea:01	静的	LAN Ethernet	有効	43 分	削除

戻る 削除

削除 ボタンをクリックします。

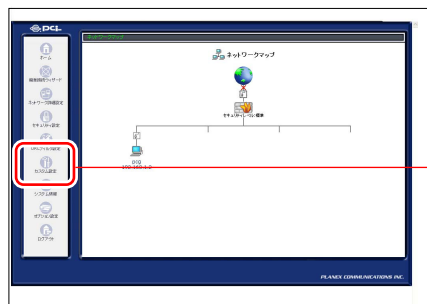
5 [戻る]ボタンをクリックし、[DHCP サーバ]画面に戻ります。

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。

1 サイドバーから[カスタム設定]をクリックします。



クリックします。

2 [DHCPサーバ]をクリックします。



[カスタム設定] 画面に切り替わります。

クリックします。

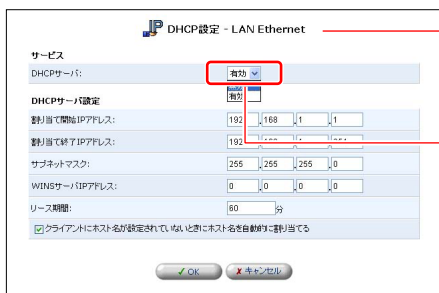
3 現在の DHCP サーバのサブネット、IP アドレスの割り当て範囲が表示されます。設定を変更する場合は、修正ボタンをクリックします。



[DHCP サーバ] 画面に切り替わります。

 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。



[DHCP 設定 LAN Ethernet] 画面に切り替わります。

選択します。

! 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 サーバと同じの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、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

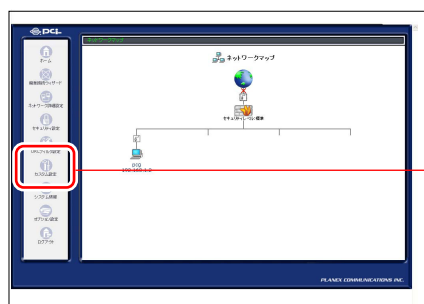
- 本製品の DNS サーバは、LAN 内のドメイン名と IP アドレスの対応だけを管理しています。
- インターネット上のドメイン名を指定した通信では、本製品の「プロキシ DNS」機能が使用されます。

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。



クリックします。

2 [DHCPサーバ]をクリックします。



[カスタム設定] 画面に切り替わります。

クリックします。

3 [DHCP 設定]アイコンをクリックします。

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	255.255.255.0	192.168.1.1 - 192.168.1.254	

戻る DHCP設定

[DHCP サーバ] 画面に切り替わります。

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。

ホスト名	IPアドレス	MACアドレス	タイプ	接続名	ステータス	リース期間	操作
pc2	192.168.1.2	08:00:14:aa:01:00	LAN Ethernet		有効	60分	

戻る

[DHCP 設定] 画面に切り替わります。

表示されます。

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。

カスタム設定

DNSサーバ

ダイナミックDNS

DHCPサーバ

ルーティング

ユーザー

日付と時刻

ファームウェアアップデート

PPTP

IPSec

UPnP

システム設定

MACアドレスの変更

移動ファイル

設定情報の初期化

設定情報の保存/読み込み

再起動

ファームウェア情報

[カスタム設定] 画面に切り替わります。

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。

ホスト名	IPアドレス	操作
pcg	192.168.1.2	 

[DNSエントリの追加](#)

[戻る](#)

[DNS サーバ] 画面に切り替わります。

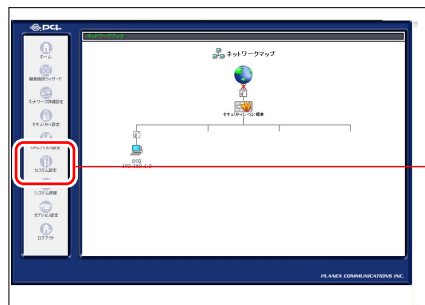
表示されます。

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。



クリックします。

- 2 [DNS サーバ]アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

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。



[DNS サーバ] 画面に切り替わります。

追加 ボタンをクリックします。

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。



[DNS エントリ] 画面に切り替わります。

入力します。

クリックします。

5 以上で設定は終了です。

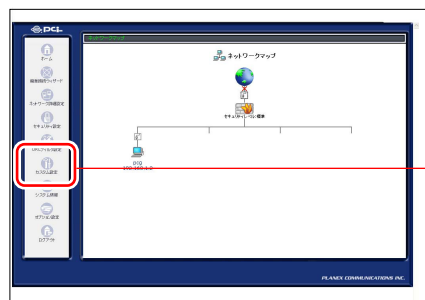
ホスト名とIPアドレスの修正

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。

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。



クリックします。

2 [DNSサーバ]アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

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

ホスト名	IPアドレス	操作
pcq	192.168.1.2	修正 削除
user1	192.168.1.100	修正 削除

DNSサーバの追加

戻る

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。

DNSエントリ

ホスト名: user1

IPアドレス: 192.168.1.100

OK

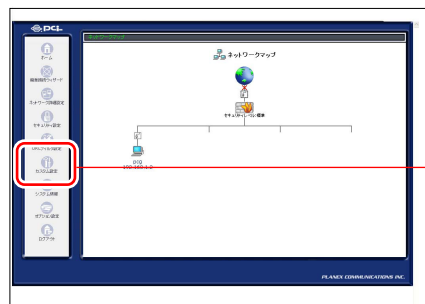
※ DHCPサーバによりIP アドレスを割り当てられたホストについては、ホスト名のみ修正が可能です。

5 以上で設定は終了です。.

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。



クリックします。

- 2 [DNSサーバ]アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

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、[OK]ボタンをクリックします。



[DNS サーバ] 画面に切り替わります。

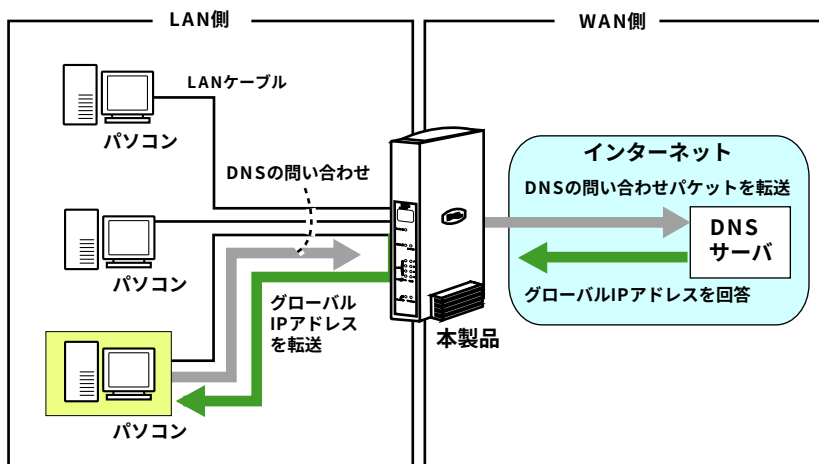
削除 ボタンをクリックします。

クリックします。

- 4 以上で設定は終了です。

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。

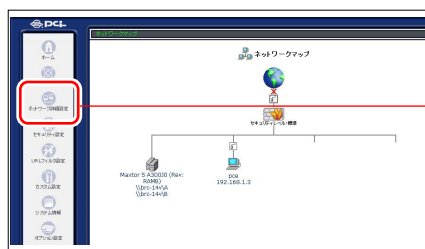
ルーティング設定

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。



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。

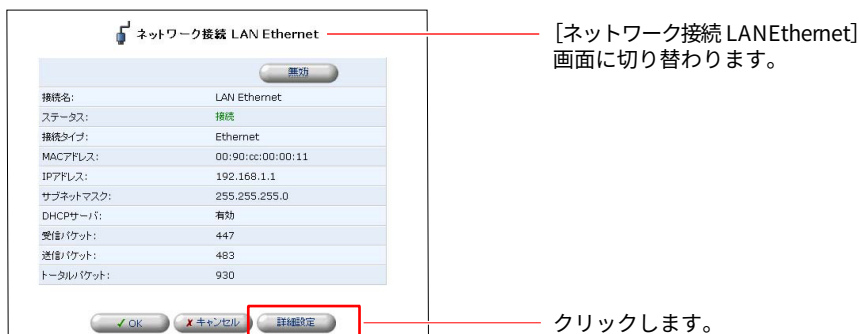


[DHCP サーバ] 画面に切り替わります。

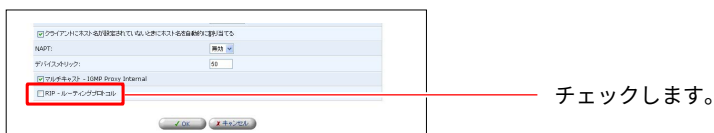
修正 ボタンをクリックします。

- 3 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場合は同様の手順でお進めください。

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。



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。



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。



RIP受信設定	
なし	RIP機能を無効にします。
RIPv1	RIPv1による、ルート情報の受信を行います。
RIPv2	RIPv2による、ルート情報の受信を行います。
RIPv1/2	RIPv1/2による、ルート情報の受信を行います。
RIP送信設定	
なし	RIP機能を無効にします。
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	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	RIPv2による、ルート情報の送信を行います。

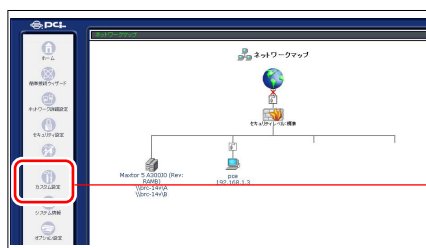
- 7** [OK] ボタンをクリックします。[注意] 画面が表示される場合は、内容を確認したうえで [OK] ボタンをクリックします。



クリックします。

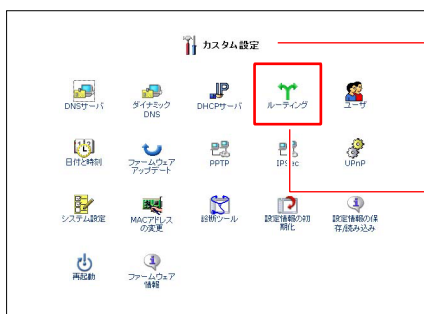
- 8** [ネットワーク接続 LAN Ethernet]画面に戻ります。

- 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。



クリックします。

- 10** [ルーティング] アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

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。

ルーティング

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	操作
ルーティングプロトコル						
☒ RIP - ルーティングプロトコル						
☐ マルチキャスト						

OK キャンセル

[ルーティング] 画面に切り替わります。

追加されます。

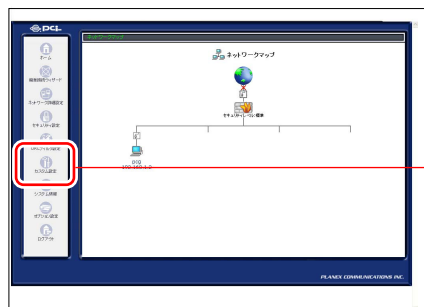
12 [OK] ボタンをクリックします。

13 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。

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。



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。



[カスタム設定] 画面に切り替わります。

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。



[ルーティング] 画面に切り替わります。

ボタンをクリックします。

4 経路情報を追加するデバイスを選択し、経路情報を入力します。

ルーティング設定

接続名: LAN Ethernet

送信先: 192.168.1.0

ネットマスク: 255.255.255.0

ゲートウェイ: 192.168.1.100

メトリック: 2

OK キャンセル

「ルーティング設定」画面に切り替わります。

選択します。

【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ーフェースを [LAN Ethernet]、[WAN Ethernet]、[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 [OK]ボタンをクリックします。[ルーティングプロトコル]欄に設定したルーティング情報が追加されます。

ルーティング

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	192.168.1.0	192.168.1.100	255.255.255.0	2	適用された	✓

追加の経路を追加

☒ 静的ルーティングプロトコル

OK キャンセル

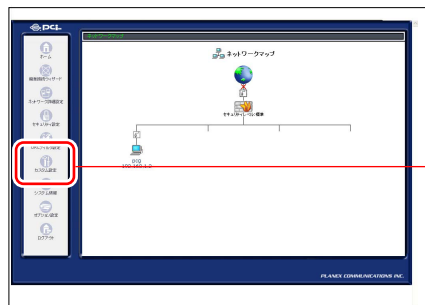
チェックします。

6 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する。



クリックします。

2 [ルーティング]アイコンをクリックする。



[カスタム設定] 画面に切り替わります。

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。

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	192.168.10.0	192.168.1.100	255.255.255.0	2	適用済み	修正

ルーティングプロトコル

☐ RIP - ルーティングプロトコル

☐ マルチキャスト

OK キャンセル

[ルーティング] 画面に切り替わります。

修正 ボタンをクリックします。

4 経路情報を修正し、[OK]ボタンをクリックします。

接続名: LAN Ethernet

送信先: 192 168 10 0

ネットマスク: 255 255 255 0

ゲートウェイ: 192 168 1 100

メトリック: 2

OK キャンセル

[ルーティング設定] 画面に切り替わります。

修正します。

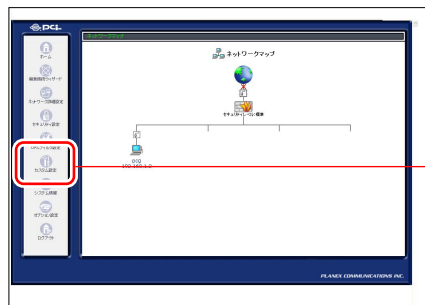
クリックします。

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する。



クリックします。

2 [ルーティング]アイコンをクリックする。



[カスタム設定] 画面に切り替わります。

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。

ルーティング

ルーティングテーブル

経路名	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	192.168.10.0	192.168.1.100	255.255.255.0	2	適用しました	
ルートの追加						

ルーティングプロトコル

☐ RIPv1 - ルーティングプロトコル

☒ マルチキャスト

[ルーティング] 画面に切り替わります。

 ボタンをクリックします。

4 [OK]ボタンをクリックします。

5 以上で設定は終了です。

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。



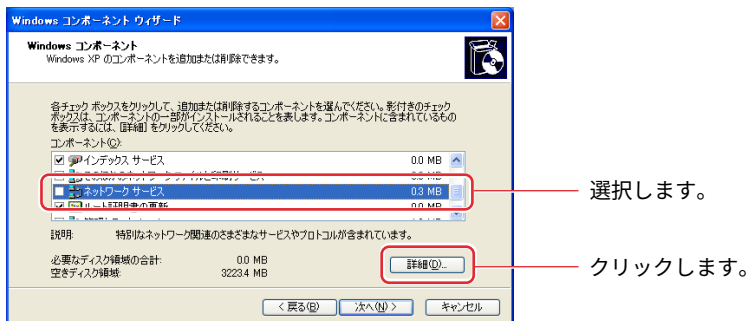
クリックします。

- 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。

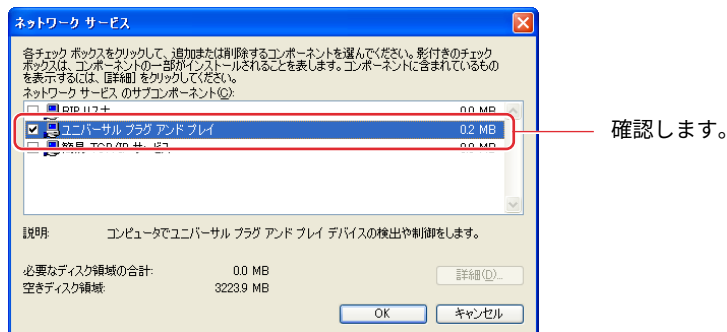


クリックします。

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。



4 ネットワークサービス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。



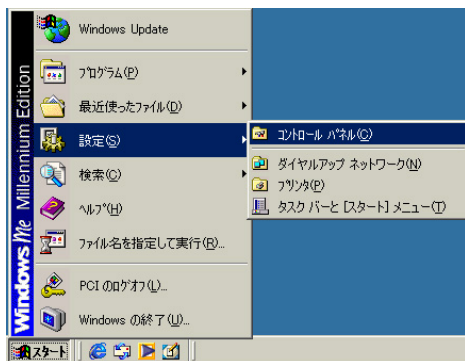
[ユニバーサルプラグアンドプレイ] がチェックされているときは、パソコンが UPnP の機能が有効になっています。ダイアログを閉じてください。

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。

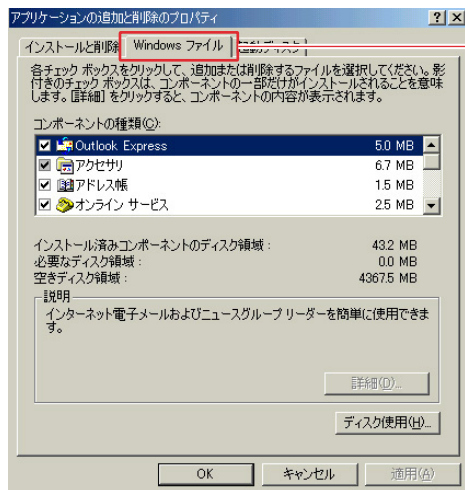
5 以上で設定は終了です。

■ Windows® Me の場合

- 1 [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。

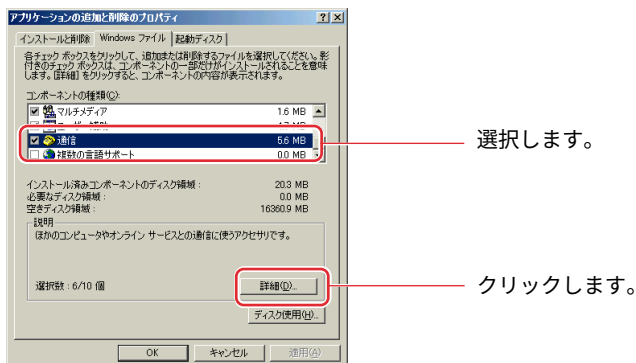


- 2 [アプリケーションの追加と削除] ボタンをクリックします。[アプリケーションの追加と削除] ダイアログが表示されたら、[Windows ファイル] タブをクリックします。

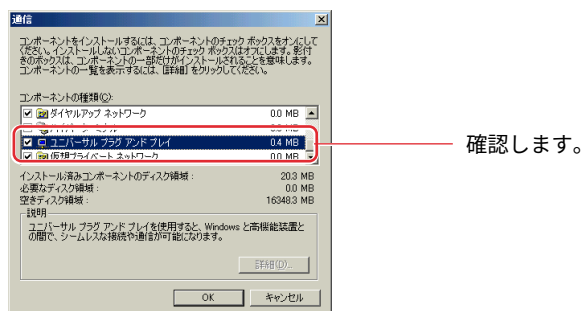


クリックします。

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。



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。



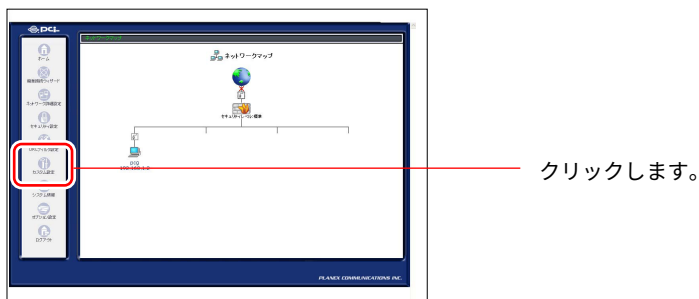
5 [ユニバーサルプラグアンドプレイ] がチェックされているときは、パソ コンが UPnP の機能が有効になっています。ダイアログを閉じてください。 チェックされていないときは、[ユニバーサルプラグアンドプレイ] が無 効になっています。チェックを付け、[OK] ボタンをクリックします。画 面の指示に従ってインストールを続けてください。

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。

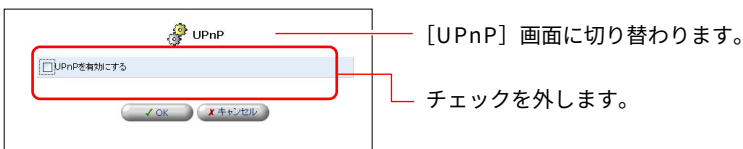
1 サイドバーの[カスタム設定]アイコンをクリックします。



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

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たりす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

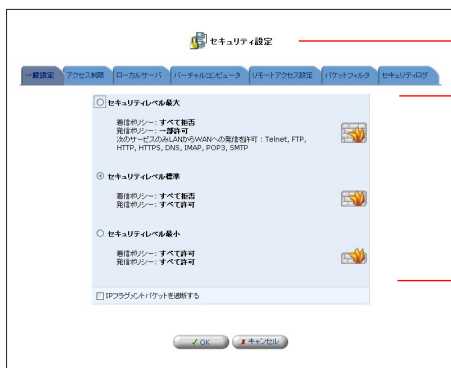
ここでは、本製品の基本的なセキュリティレベルの設定を行います。

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。

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。



[セキュリティ設定] 画面に切り替わります。

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。

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。

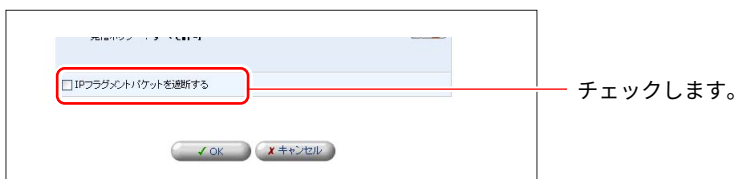
※ [セキュリティレベル最大] を選択しているとき、LAN 側のパソコンから使用できるインターネットのサービスは次のとおりです。

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

ご注意

[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。



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。

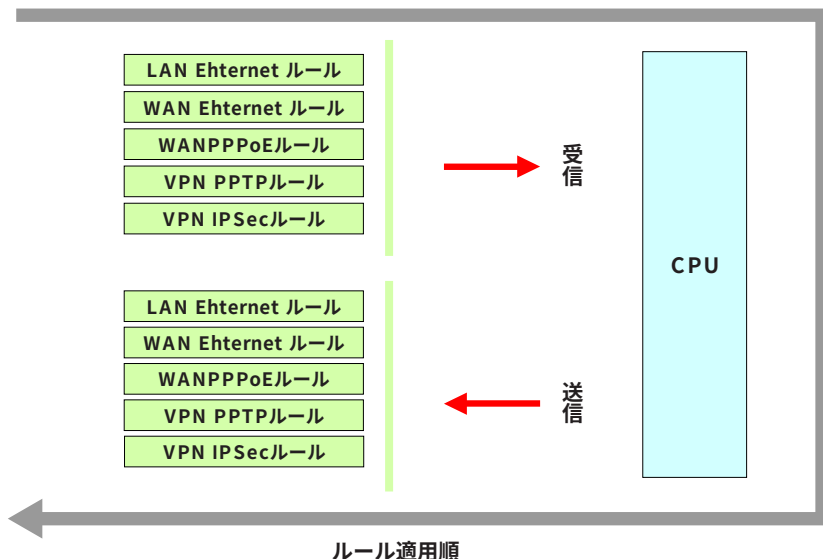
選択したセキュリティレベルに変更されます。

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 Ethernet ルール]、[WAN Ethernet ルール]、[WAN PPPoEルール]等があります。

ルール適用順

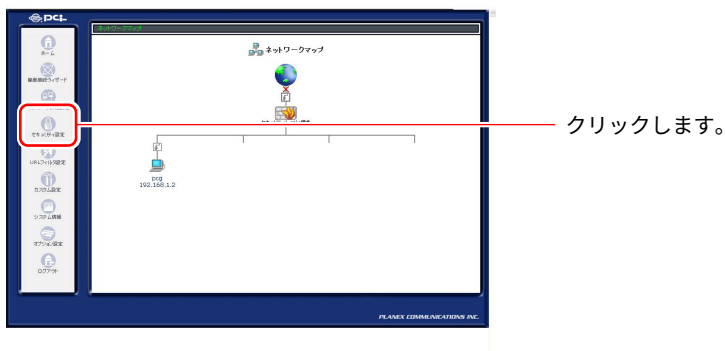


パケットフィルタの設定

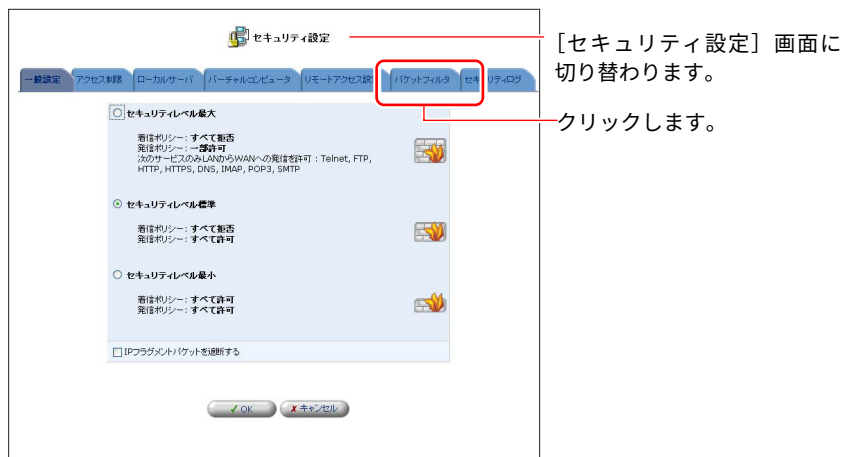
ここでは、本製品にパケットフィルタを設定する方法について説明します。

■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。



3 [セキュリティ設定]画面が表示されます。



[セキュリティ設定] 画面に切り替わります。

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。



例として選択します。

本製品で設定できるルール一覧

[LAN Ethernet 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 Ethernet 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。

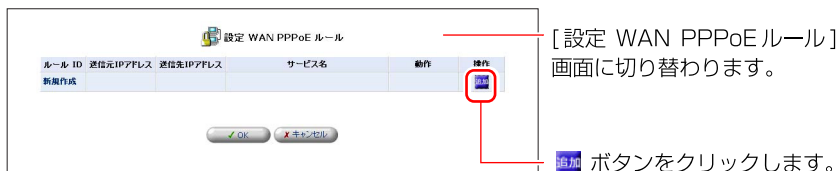
[VPN PPTP ルール]

VPN PPTP の接続に対して適用されるルールになります。

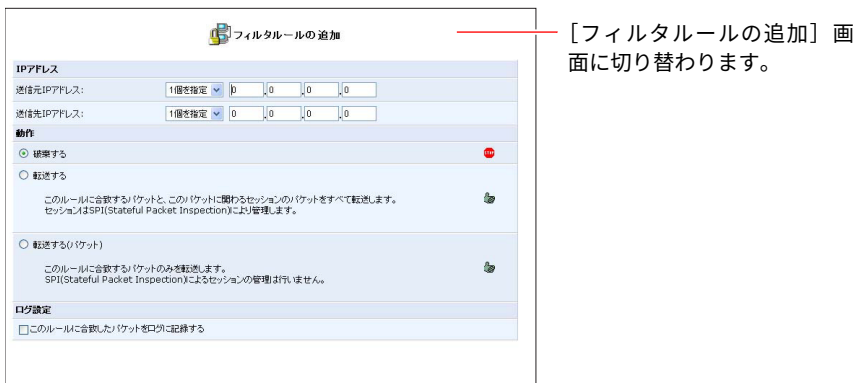
[VPN IPSec ルール]

VPN IPSec の接続に対して適用されるルールになります。

- 5** [設定 WAN PPPoE ルール]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。



- 6** [フィルタルールの追加]画面が表示されます。



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。

[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。

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。

[転送する (セッション)]

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通します。

[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通します。

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。

サービス名	プロトコル / ポート
☐ 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 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
☐ 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 すべて -> 161
☐ SMTP - Outgoing Mail	TCP すべて -> 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

チェックします。

10 [OK]ボタンをクリックします。

クリックします。

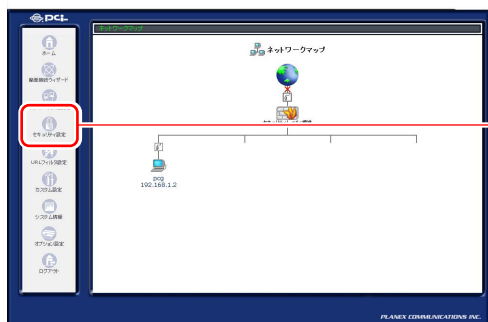
※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

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

- 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。



クリックします。

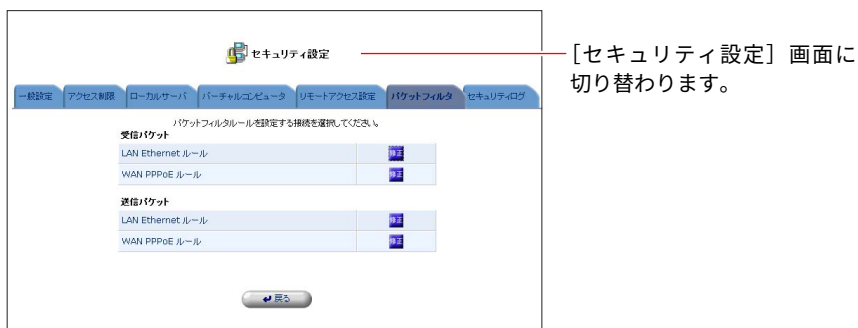
- 2 [パケットフィルタ]タブをクリックします。



[セキュリティ設定] 画面に切り替わります。

クリックします。

3 設定を変更したいインターフェースの修正ボタンをクリックします。



4 [設定 WAN PPPoE ルール]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。

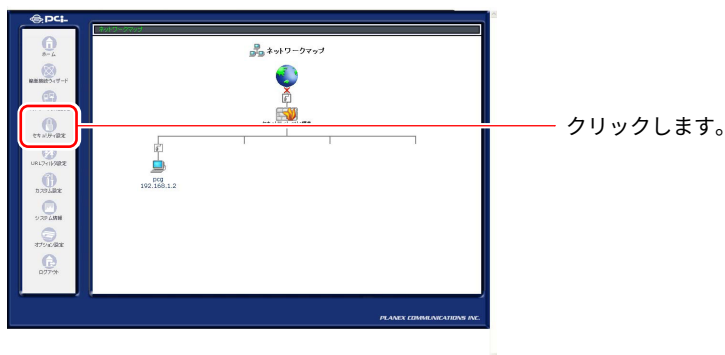


※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

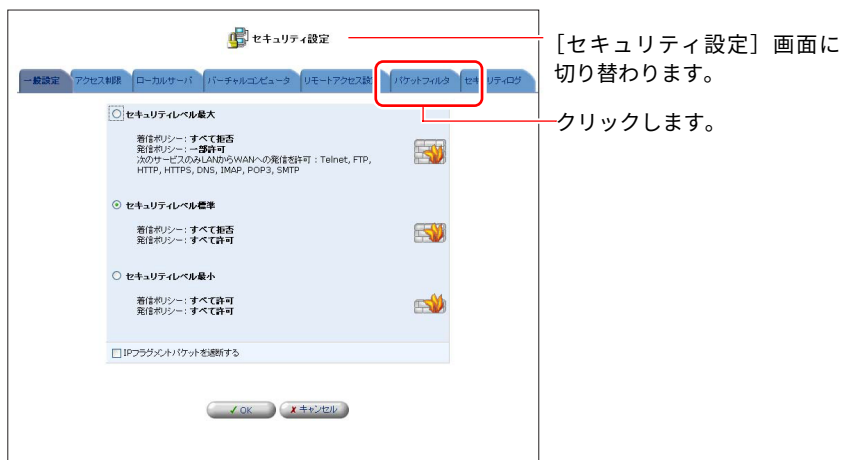
6 以上で修正は終了です。

■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。

セキュリティ設定

一般設定 アクセス制御 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 パケットフィルタ セキュリティログ

パケットフィルタルールを設定する操作を選択してください。

受信パケット

ルール名	操作
LAN Ethernet ルール	修正
WAN PPPoE ルール	修正

送信パケット

ルール名	操作
LAN Ethernet ルール	修正
WAN PPPoE ルール	修正

戻る

4 [設定 WAN PPPoE ルール]の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。

設定 WAN PPPoE ルール

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	操作
0	すべて	すべて	FTP	結果する	削除
新規作成					削除

OK キャンセル

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。

[フィルタールの追加] 画面に切り替わります。

クリックします。

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。

[ユーザ定義サービス] 画面に切り替わります。

追加 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。

[サービスの編集] 画面に切り替わります。

追加 ボタンをクリックします。

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。

[発信元ポート/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。

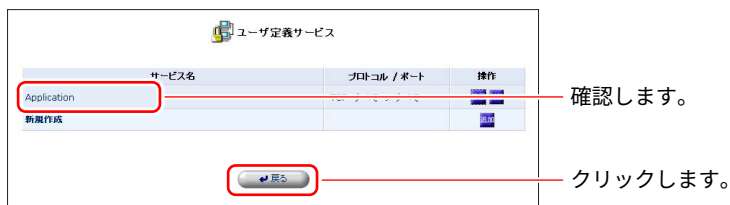
5 [OK]ボタンをクリックします。

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。



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。



- 9 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。



- 10 以上で設定は終了です。

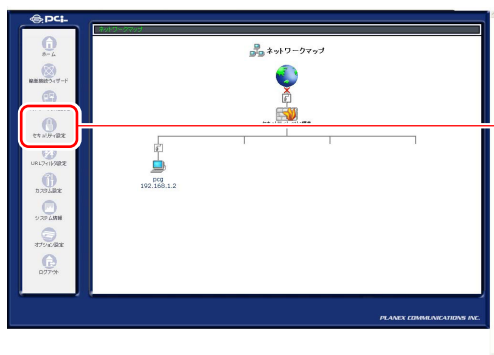
フィルタールの例

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。

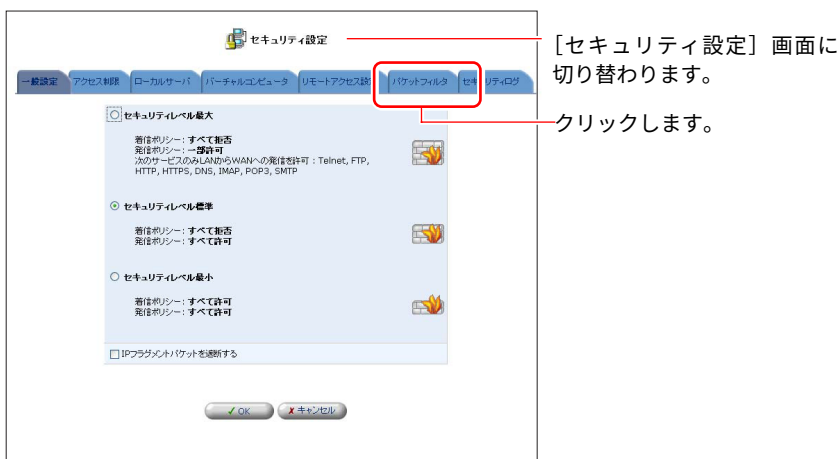
方向	動作	プロトコル	送信元 IP アドレス	送信先 IP アドレス	送信元ポート	送信元 IP アドレス
LAN Ethernet → 受信	破棄	TCP/UDP	すべて	すべて	すべて	137 ~ 139
送信 → WAN Ethernet	破棄	TCP/UDP	すべて	すべて	すべて	137 ~ 139

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。



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 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 Ethernet ルール] の修正ボタンをクリックします。



4 [新規作成]欄から追加ボタンをクリックします。



[設定 LAN Ethernet ルール] 画面に切り替わります。

追加 ボタンをクリックします。

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。



[フィルタールールの追加] 画面に切り替わります。

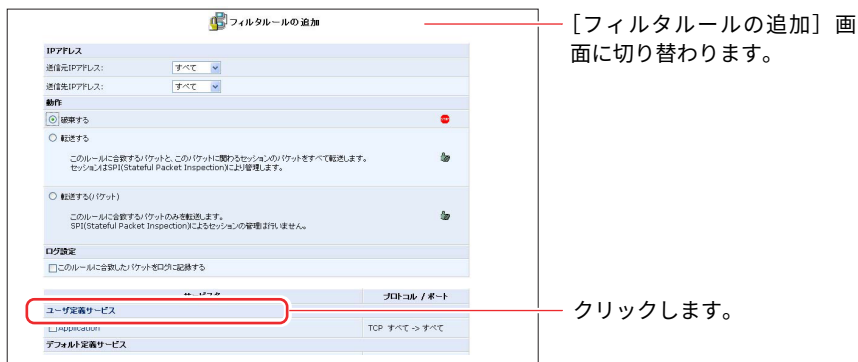
選択します。

6 [動作]欄から[破棄する]にチェックを付けます。



チェックします。

7 [ユーザ定義サービス]をクリックします。



[フィルタールの追加] 画面に切り替わります。

クリックします。

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。



追加 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。



追加 ボタンをクリックします。

- 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。

サービスの編集

プロトコル	TCP
送信元ポート:	すべて
送信先ポート:	範囲指定 137 - 139

OK 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: Application
サービスの説明:

プロトコル	詳細	操作
TCP	すべて -> 137-139	削除 追加
新規作成		追加

OK キャンセル

- 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。

サービスの編集

プロトコル	UDP
送信元ポート:	すべて
送信先ポート:	範囲指定 137 - 139

OK キャンセル

- 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。

サービスの編集

サービス名: NetBIOS

サービスの説明:

プロトコル	詳細	操作
TCP	すべて -> 137-139	削除
UDP	すべて -> 137-139	削除
新規作成		

OK Cancel

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。

ユーザ定義サービス

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	削除
新規作成		

戻る

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。

フィルタールの追加

IPアドレス

送信元IPアドレス: すべて

送信先IPアドレス: すべて

動作

☒ 遮断する

☐ 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。

☐ 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。SPI(Stateful Packet Inspection)によるセッションの管理は行いません。

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	プロトコル / ポート
ユーザ定義サービス	
☒ NetBIOS	TCP すべて -> 137-139

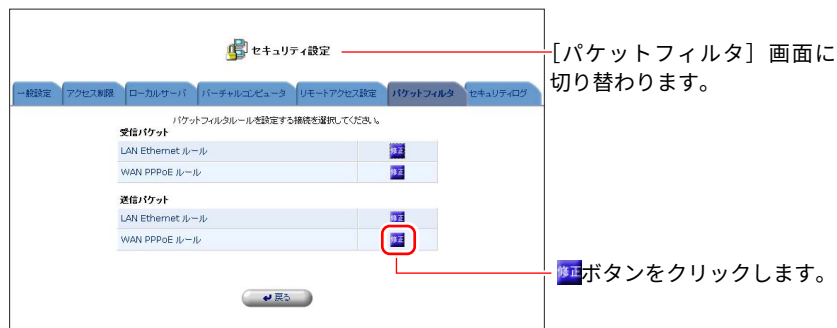
※[OK]ボタンは画面の下の方にあります。スクロールして表示してください。

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。



19 [OK]ボタンをクリックします。

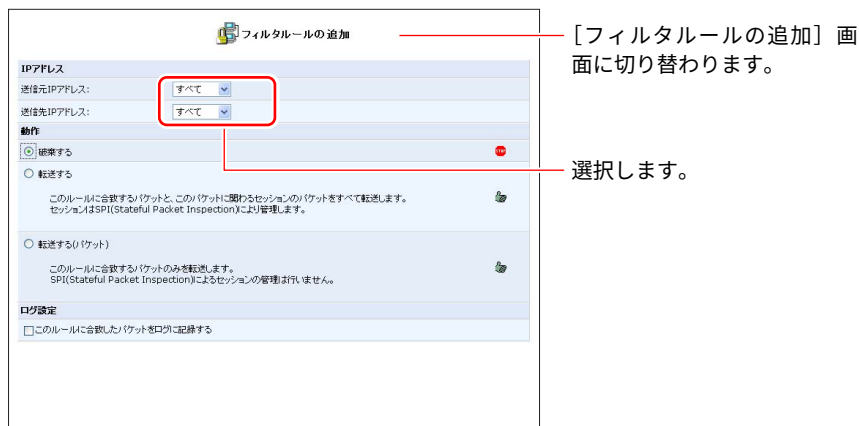
20 次に送信パケットの設定を行います。
[送信パケット]欄から[WAN PPPoE ルール]の修正ボタンをクリックします。



21 [新規作成]欄から追加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。



23 [動作]欄から[破棄する]にチェックを付けます。



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。

[フィルタのルール追加] 画面に切り替わります。

チェックします。

※[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。

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。

[設定 WAN PPPoE ルール] 画面に切り替わります。

クリックします。

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。

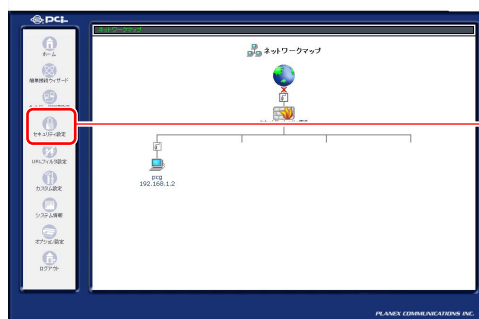
ご注意

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。



クリックします。

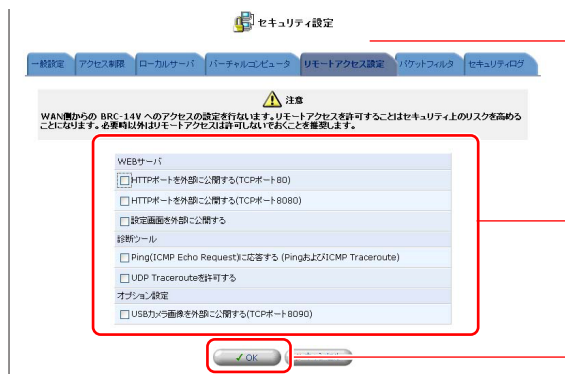
- 2 [リモートアクセス設定] タブをクリックします。



[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 WAN 側からのアクセスに関する設定を行います。



[リモートアクセス設定] 画面に切り替わります。

選択します。

クリックします。

WEB 設定画面	HTTP ポートを外部に公開する	本製品の HTTP ポートを外部に公開する場合に選択します。
	HTTP ポートを外部に公開する (TCP ポート 8080)	本製品の HTTP ポートを TCP 8080 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。
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。
	UDP を許可	tracert 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 Tracert 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/](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。

URL フィルタ設定

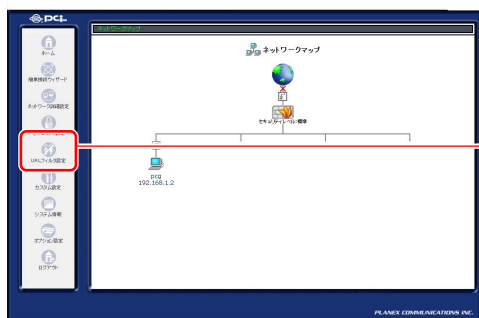
URL フィルタ機能を使うことで、LAN 側のパソコンから特定の WEB サイトを閲覧できないように設定できます。

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。

URL フィルタの設定

■ URL フィルタの新規作成

- 1 サイドバーから [URL フィルタ設定] アイコンをクリックします。



クリックします。

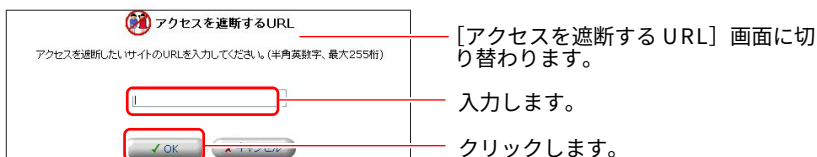
- 2 [新規作成] 欄から追加ボタンをクリックします。



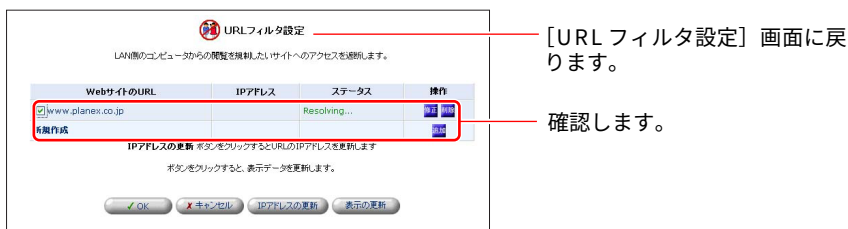
[URL フィルタ設定] 画面に切り替わります。

追加 ボタンをクリックします。

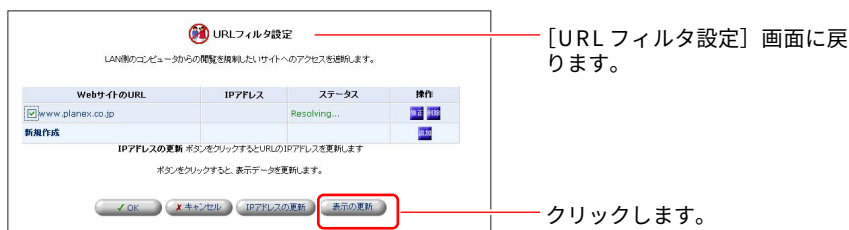
3 閲覧を禁止したいWEBサイトのURLまたはIPアドレスを入力し、[OK] ボタンをクリックします。



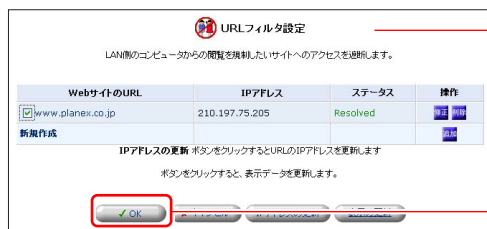
4 [WEBサイトのURL] の一覧に設定したWEBサイトが追加されます。



5 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 [Resolving] 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が適切なものが確認します。



- 6 入力された URL に対して、インターネット上に存在することが確認できると[IP アドレス]欄に IP アドレスが表示され[ステータス]欄は[Resolved]に変わります。また、インターネット上に存在を確認できなかった場合は、[ステータス]欄に[Error]と表示されます。



[URL フィルタ設定] 画面に切り替わります。

クリックします。

- 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。

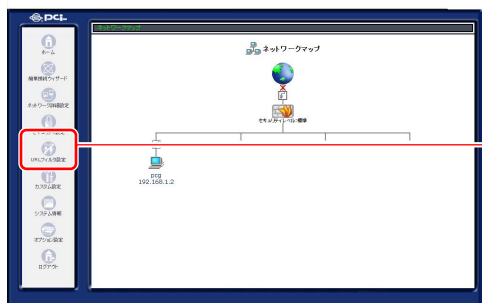
MEMO

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。

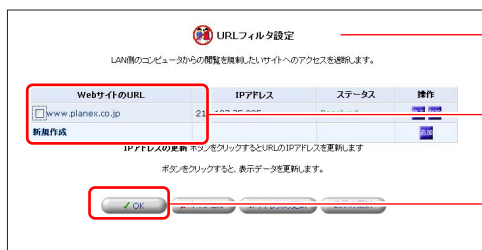
■ URL フィルタの有効/無効の切替

- 1 サイドバーから [URL フィルタ設定] アイコンをクリックします。



クリックします。

- 2 [WEBサイトのURL] 欄から URL 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。



[URL フィルタ設定] 画面に切り替わります。

チェックを外します。

クリックします。

- 3 [ステータス] 表示が Resolved から無効に替わります。再度、URL フィルタを有効にする場合はチェックを付けます。

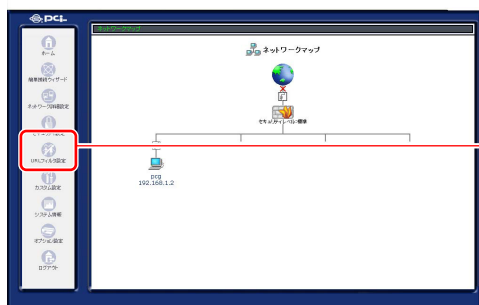


確認します。

- 4 以上で設定は終了です。

■ URL フィルタの修正

- 1 サイドバーから [URL フィルタ設定] アイコンをクリックします。



クリックします。

- 2 設定を変更したいWEBサイトのURLの修正ボタンをクリックします。



[URL フィルタ設定] 画面に切り替わります。

修正 ボタンをクリックします。

- 3 [アクセスを遮断する URL] の画面が表示されましたら、新しい 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。



[アクセスを遮断する URL] 画面に切り替わります。

確認します。

4 [WEBサイトのURL] の一覧に変更したWEBサイトが表示されます。



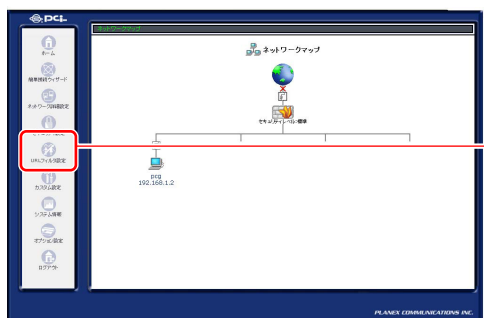
[URL フィルタ設定] 画面に切り替わります。

確認します。

5 以上で設定は終了です。

■ URL フィルタの削除

- 1 サイドバーから [URL フィルタ設定] アイコンをクリックします。



クリックします。

- 2 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。



ボタンをクリックします。

- 3 [OK] ボタンをクリックします。

- 4 以上で設定は終了です。

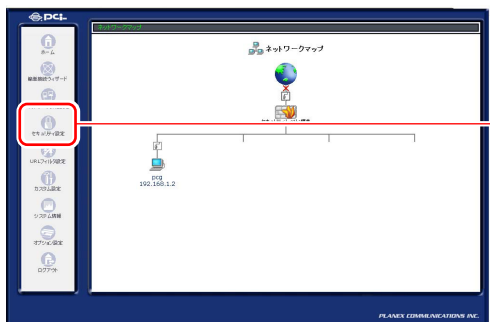
ログの管理

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。

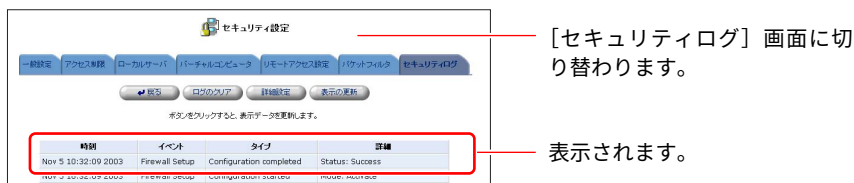


クリックします。

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。



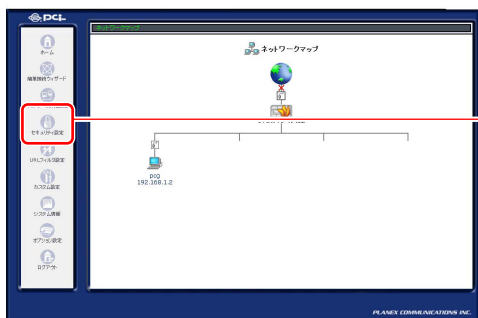
■ログの見方（例）

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分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。
Firewall Setup	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。
	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。



クリックします。

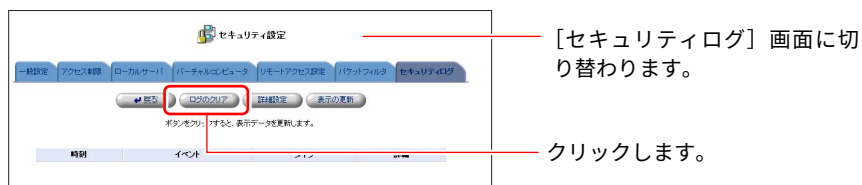
- 2 [セキュリティログ] タブをクリックします。



[セキュリティ設定] 画面に切り替わります。

クリックします。

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



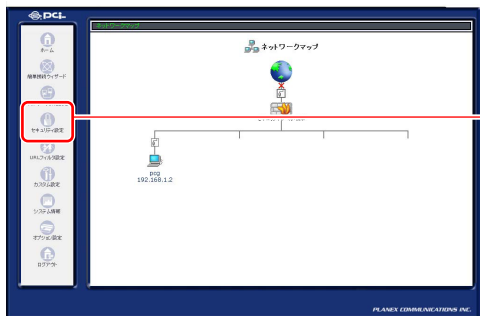
4 「戻る」 ボタンをクリックします。

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。



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。



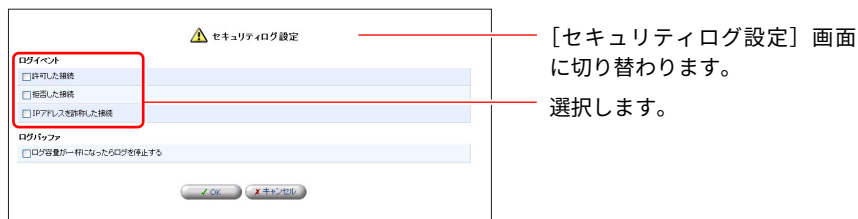
［セキュリティ設定］画面に切り替わります。

クリックします。

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。



[許可した接続]

LAN 側からインターネットへの接続、インターネット側から LAN への接続のうち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]

LAN 側からインターネットへの接続、インターネット側から LAN への接続のうち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。

[IP アドレスを詐称した接続]

LAN 側からインターネットへの接続、インターネット側から LAN への接続のうち送信元 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。

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。



[ログバッファ] 画面に切り替わります。
選択します。

[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。

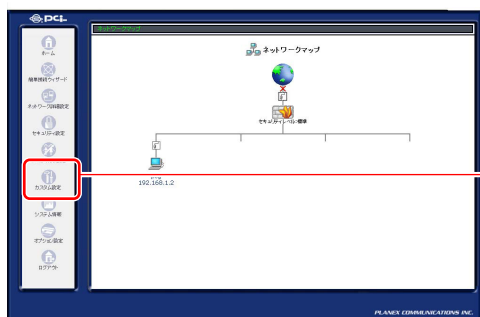
6 [OK] ボタンをクリックします。

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。



クリックします。

2 「ユーザ」アイコンをクリックします。



「カスタム設定」画面に切り替わります。

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。

 ユーザ

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			



[ユーザ] 画面に切り替わります。

修正 ボタンをクリックします。

4 [E-mailアドレス] 欄に、送信先の Mail アドレスを入力します。

 ユーザ設定

一般設定

フルネーム: administrator

ユーザ名 (大文字/小文字に注意): admin

新しいパスワード:

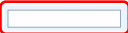
新しいパスワードの確認:

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: なし

セキュリティ通知レベル: なし

入力します。

- 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。

ユーザ設定

一般設定

フルネーム: Administrator

ユーザ名 (大文字/小文字に注意): admin

新しいパスワード:

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: なし

セキュリティ通知レベル:

OK キャンセル

入力します。

【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。

[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。

- 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

SMTPメールサーバ:

送信元メールアドレス:

入力します。

OK キャンセル

- 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。

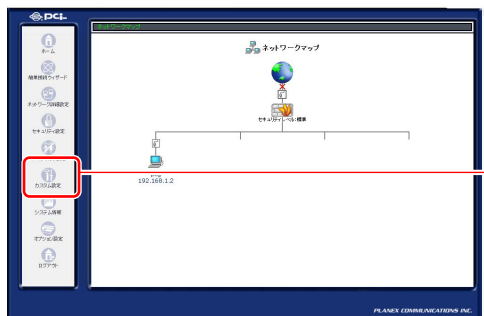
- 11** 以上で設定は終了です。

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。



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。



[カスタム設定] 画面に切り替わります。

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: 情報

システム通知 syslogサーバアドレス: 0.0.0.0

[システムリモートログ設定] 画面に切り替わります。

入力します。

[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。

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: 情報

セキュリティ通知 syslogサーバアドレス: 0.0.0.0

[セキュリティリモートログ設定] 画面に切り替わります。

入力します。

[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。

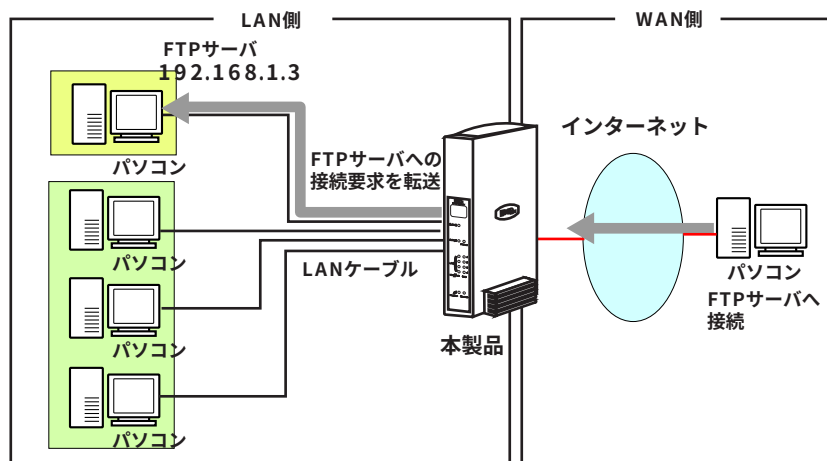
6 以上で設定は終了です。

LAN 側パソコンサーバ公開設定

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。

ローカルサーバ設定

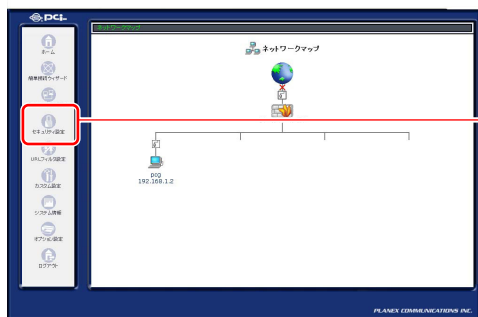
LAN 側のサーバをインターネットに公開するときや、オンラインゲームやチャットなどのソフトウェアを使うときはローカルサーバ機能の設定を行います。本製品には、あらかじめインターネットで使われるサービスやアプリケーションが登録されており、簡単に設定することができます。



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。



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。



[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 [新規作成]欄から追加ボタンをクリックします。



[ローカルサーバ] 画面に切り替わります。

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。



[ローカルサーバの追加] 画面に切り替わります。

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。

サービス名	プロトコル / ポート
デフォルト定義サービス	
☐ All Traffic	プロトコル: すべて
☐ DNS - Domain Name Server	TCP 53 → 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
☐ FTP - File Transfer	UDP 1024-65535 → 69
☐ IMAP - Messaging Server	TCP すべて → 143
☐ 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 すべて → 161
☐ SMTP - Outgoing Mail	TCP すべて → 25
☐ TELNET - Remote Connection	TCP すべて → 23

チェックします。

6 [OK]ボタンをクリックします。

☐ 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
☐ FTP - File Transfer	UDP 1024-65535 → 69
☐ IMAP - Messaging Server	TCP すべて → 143
☐ 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 すべて → 161
☐ SMTP - Outgoing Mail	TCP すべて → 25
☐ TELNET - Remote Connection	TCP すべて → 23
☐ TELNETSSL - Secure Remote Connection over SSL	TCP すべて → 992

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。

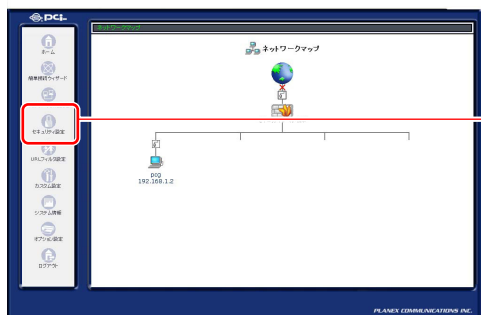
7 以上で設定は終了です。

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。



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。



[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 [新規作成]欄から追加ボタンをクリックします。



[ローカルサーバ] 画面に切り替わります。

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。



クリックします。

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。



[ユーザ定義サービス] 画面に切り替わります。

追加 ボタンをクリックします。

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] 画面に切り替わります。

追加 ボタンをクリックします。

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。

[発信元ポート/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。



[サービスの編集] 画面に戻ります。

クリックします。

8 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。

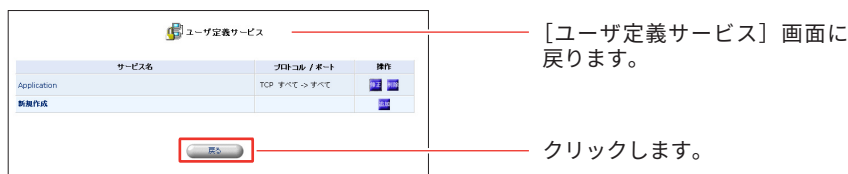


入力します。

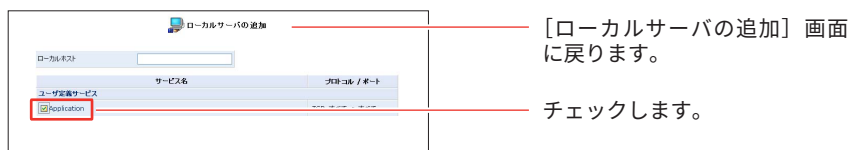
追加 ボタンをクリックします。

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。



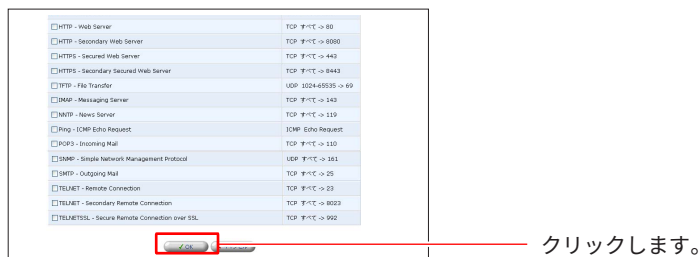
- 11** [ローカルサーバの追加]の画面に戻ります。
[ユーザ定義サービス]欄に作成したユーザ定義サービスが表示されてるのを確認し、チェックします。



- 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。



- 13** [OK]ボタンをクリックします。



※[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。



[ローカルサーバ] 画面に戻ります。

表示されます。

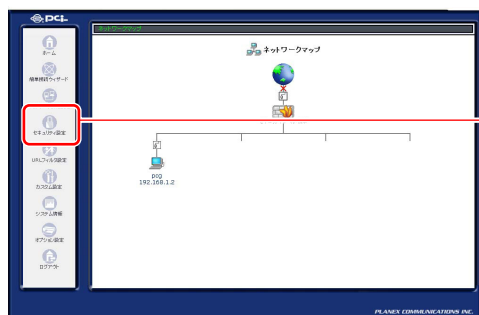
- 15** [OK]ボタンをクリックします。

- 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。



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。



[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 設定を変更するパソコンの修正ボタンをクリックします。



[ローカルサーバ] 画面に切り替わります。

修正 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] 画面に切り替わります。
クリックします。

- 5** [ユーザ定義サービス]の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。



[サービスの編集] 画面に切り替わります。
修正 ボタンをクリックします。

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



[サービスの編集] 画面に切り替わります。
修正 ボタンをクリックします。

- 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。



[サービスの編集] 画面に切り替わります。
修正します。
クリックします。

8 [OK]ボタンをクリックします。



[サービスの編集] 画面に切り替わります。

クリックします。

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。



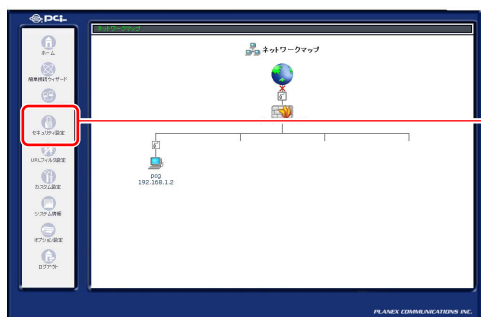
[サービスの編集] 画面に切り替わります。

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

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。



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。



[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 [新規作成]欄から追加ボタンをクリックします。

[ローカルサーバ] 画面に切り替わります。

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。

[ローカルサーバの追加] 画面に切り替わります。

クリックします。

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。

[ユーザ定義サービス] 画面に切り替わります。

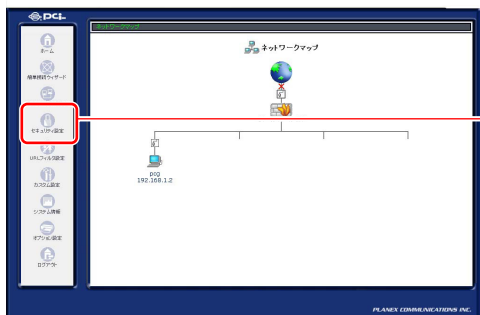
削除 ボタンをクリックします。

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。



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。



[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。

[ローカルサーバ] 画面に切り替わります。

修正 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。 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。

[ローカルサーバの編集] 画面に切り替わります。

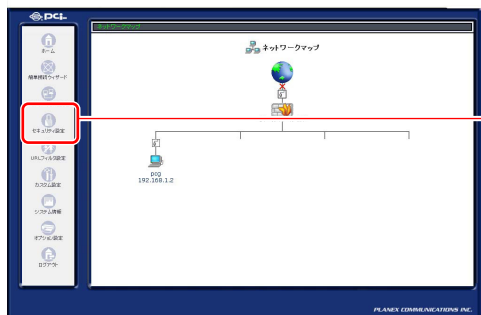
変更します。

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。



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。



[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 [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。



[ローカルサーバ] 画面に切り替わります。

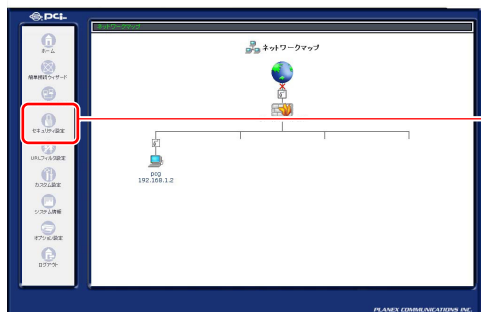
チェックを外します。

4 [OK] ボタンをクリックします。

5 以上で設定は終了です。

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。



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。



[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 設定を削除したいサービスの削除ボタンをクリックします。

[ローカルサーバ] 画面に切り替わります。

ローカルサーバID	ローカルIP	サービス名	操作
192.168.1.10	192.168.1.10	Application	編集 削除

削除 ボタンをクリックします。

4 [OK]ボタンをクリックします。

5 以上で設定は終了です。

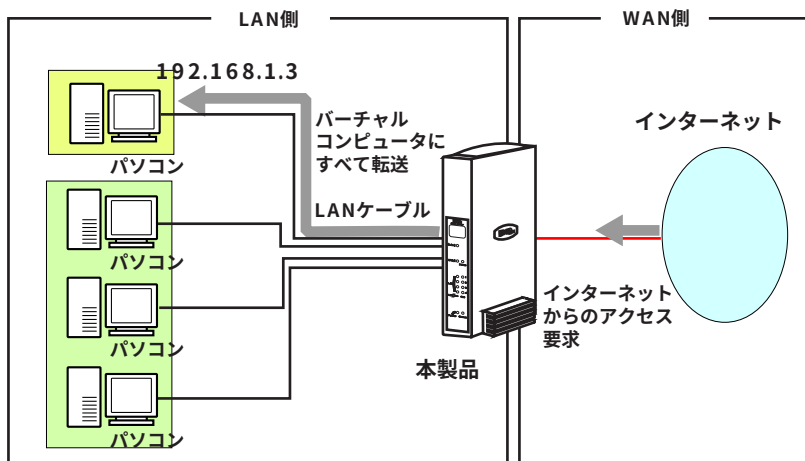
バーチャルコンピュータの設定

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。



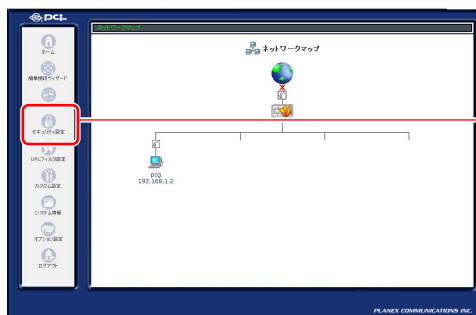
インターネットから LAN 側へのアクセス要求を受け取ると、本製品は[ローカルサーバ]機能で登録されてる宛先を除き、すべてバーチャルコンピュータへその要求を転送します。

LAN 側のパソコンをバーチャルコンピュータに設定する

ここでは、LAN 側のパソコンをインターネットに公開するためのバーチャルコンピュータの設定について説明します。

■ 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。



クリックします。

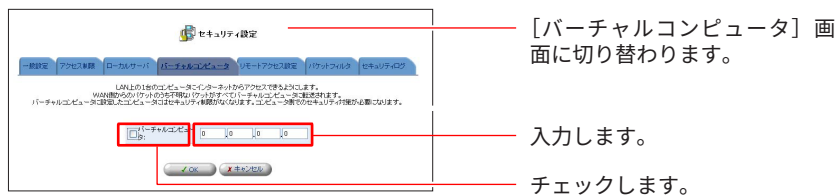
- 2 [バーチャルコンピュータ]タブをクリックします。



[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 [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。

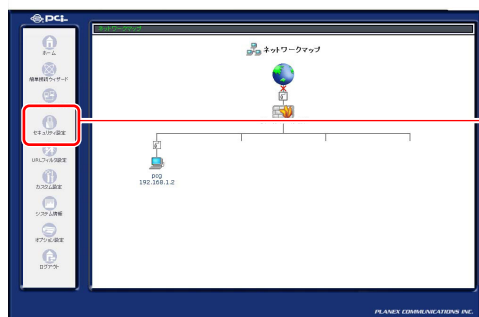


4 [OK]ボタンをクリックします。

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

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。



クリックします。

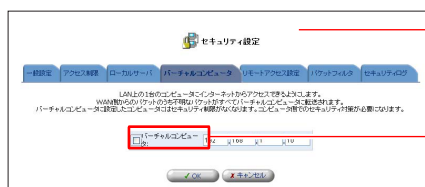
2 [バーチャルコンピュータ]タブをクリックします。



[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 [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。



[バーチャルコンピュータ] 画面に切り替わります。

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 アドレスが変わってしまう場合があります。

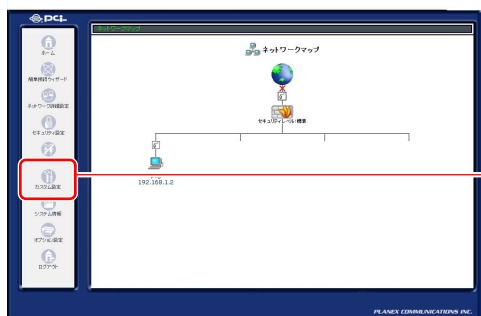
ダイナミック DNS を使用すると、本製品の IP アドレスをダイナミック DNS サーバに一定間隔で通知することで、IP アドレスが変わった場合でも固定のホスト名が使用できます。

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（2003 年 11 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。

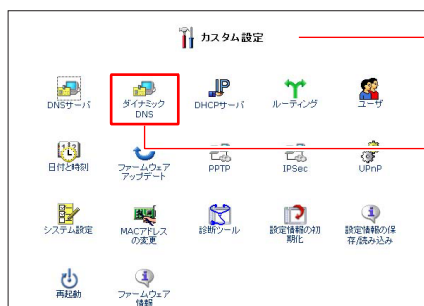
ダイナミック DNS の設定

- 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。



クリックします。

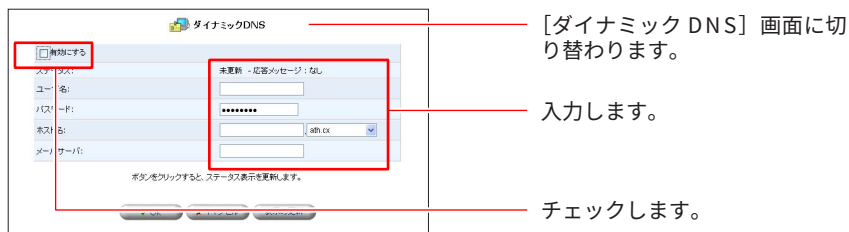
- 2 [ダイナミック DNS]アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

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]

テキスト欄に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。

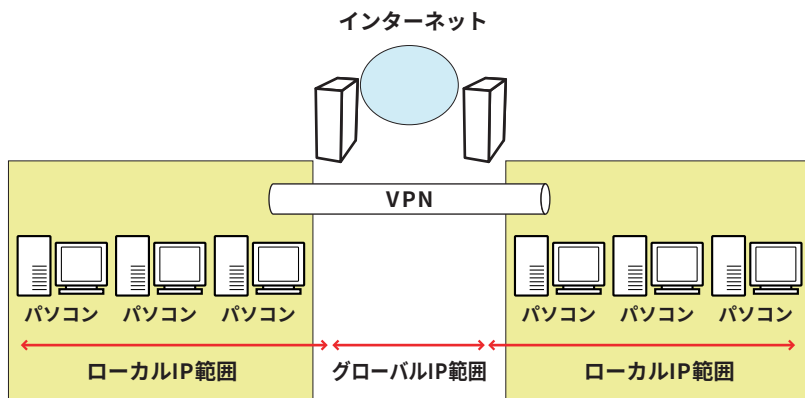
- 4** [OK]ボタンをクリックします。

- 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 アドレスを定期的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。



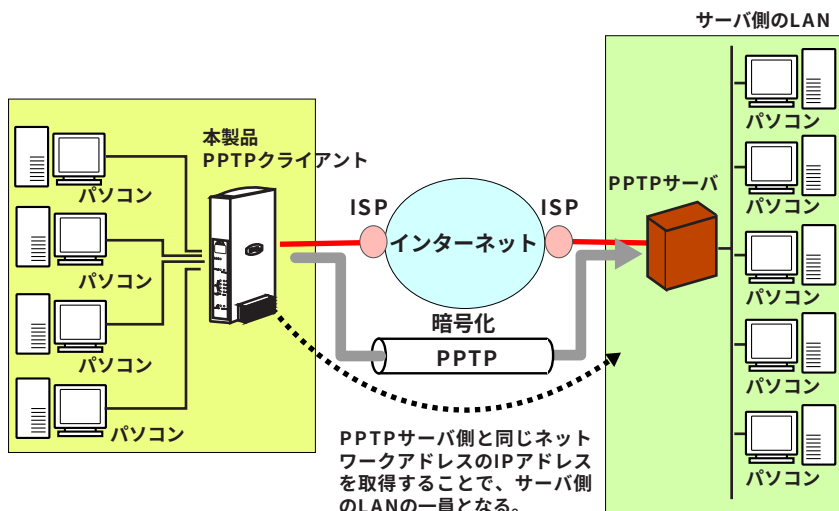
VPN を構築するには、簡単接続ウィザードによる設定をした後、ネットワーク詳細設定によって、詳細な設定が可能です。次ページの簡単接続ウィザードから設定を進めてください。なお、すでに簡単接続ウィザードによる VPN 接続設定が終わっている場合は、「ネットワーク詳細設定による設定」に進んでください。

簡単接続ウィザードによる設定

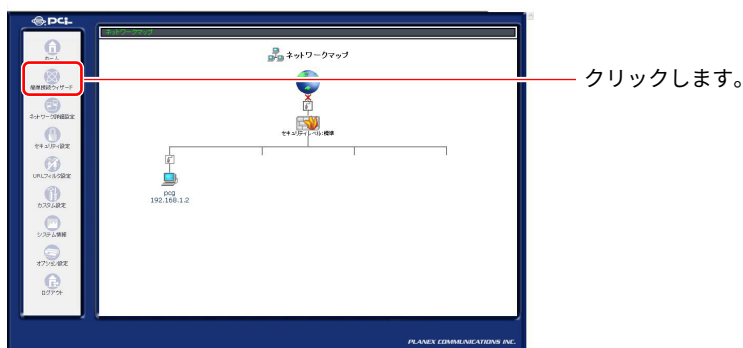
ここでは、簡単接続ウィザードを使いVPNを構築する方法について説明します。本製品はPPTPサーバ、PPTPクライアント、IPSecに対応しています。ご利用する環境に合わせて設定を進めてください。

■ PPTP クライアントの設定

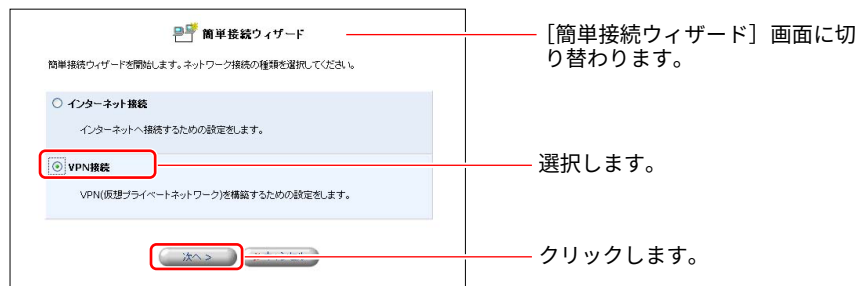
本製品をPPTPクライアントとして使用する場合の設定について説明します。



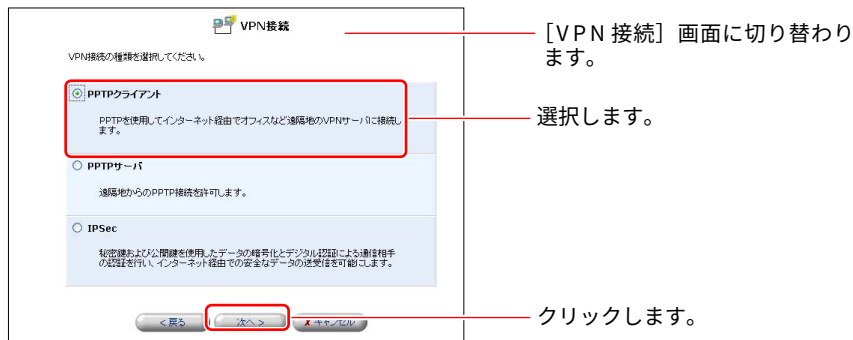
1 サイドバーから[簡単接続ウィザード]アイコンをクリックします。



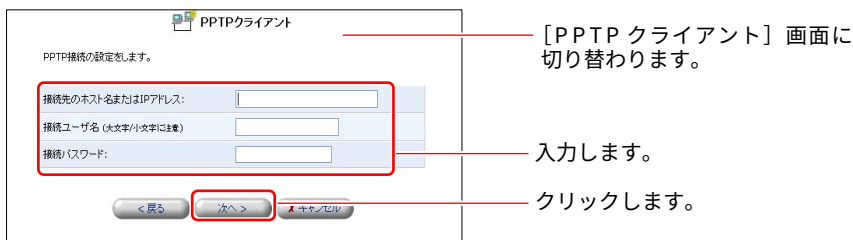
2 [VPN 接続]を選択し、[次へ]ボタンをクリックします。



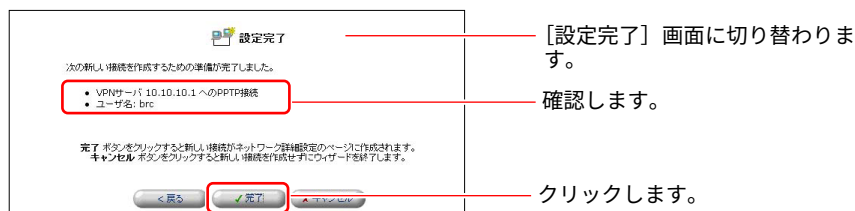
3 [PPTP クライアント]を選択し、[次へ]ボタンをクリックします



- 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。
[接続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。

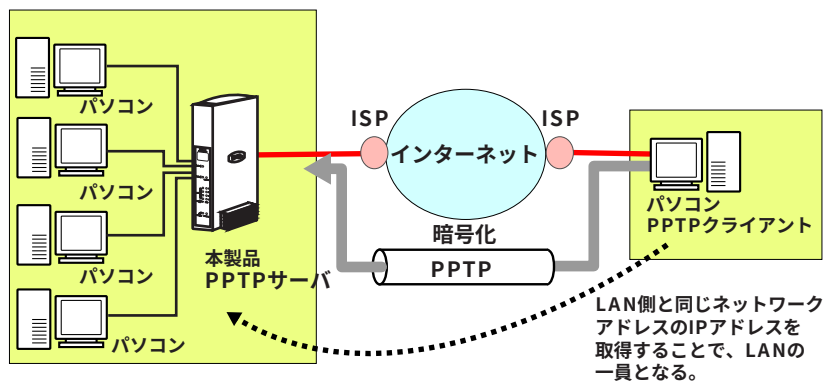


- 5** [接続完了]画面が表示されます。
PPTP 接続するサーバ名またはIP アドレスを確認し、[完了]ボタンをクリックします。

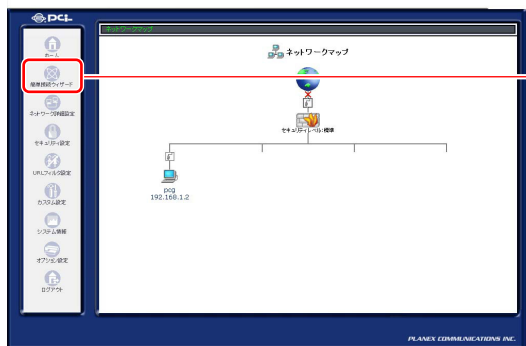


■ PPTP サーバの設定

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。

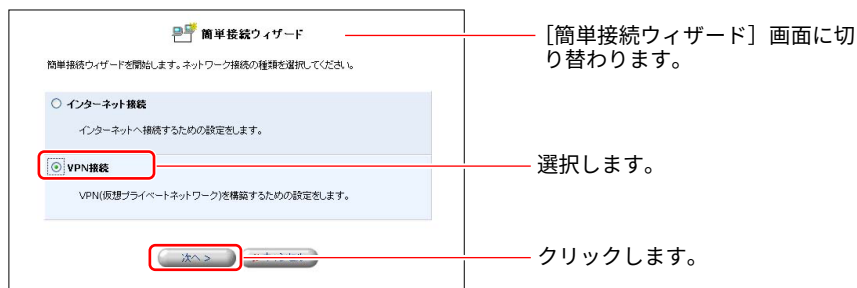


1 サイドバーから[簡単接続ウィザード]アイコンをクリックします。

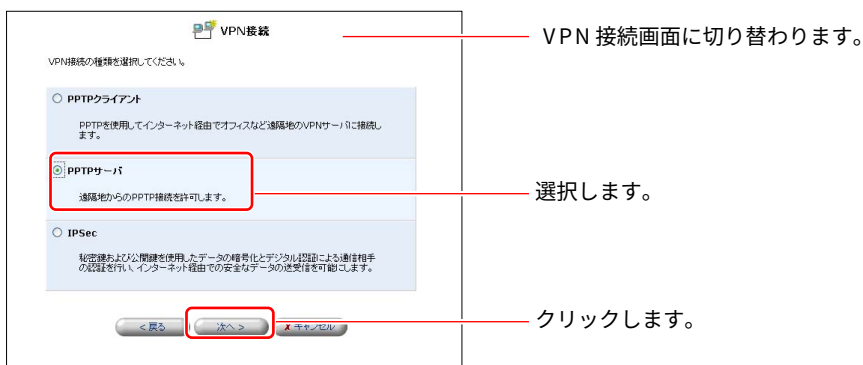


クリックします。

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。



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。



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。

[ユーザ設定] 画面に切り替わります。

入力します。

チェックします。

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。

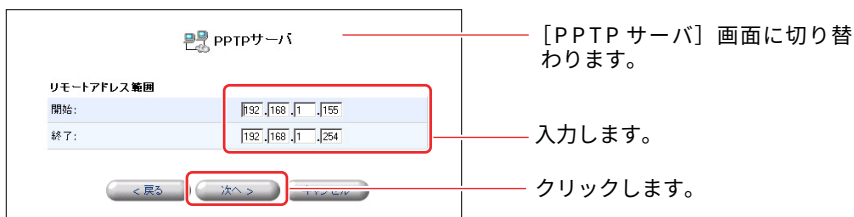
[ユーザ] 画面に戻ります。

クリックします。

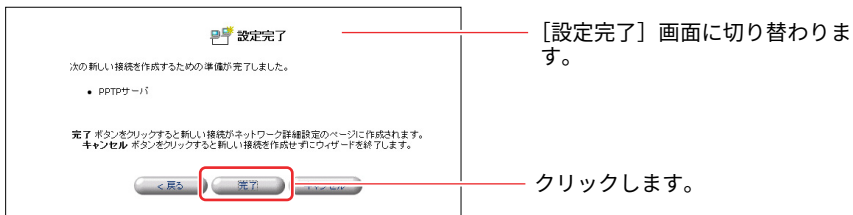
フルネーム	ユーザ名	権限	操作
Administrator	admin	管理者権限	[編集] [削除]
user	user	PPTP リモートアクセス	[編集] [削除]

ユーザの追加

- 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。



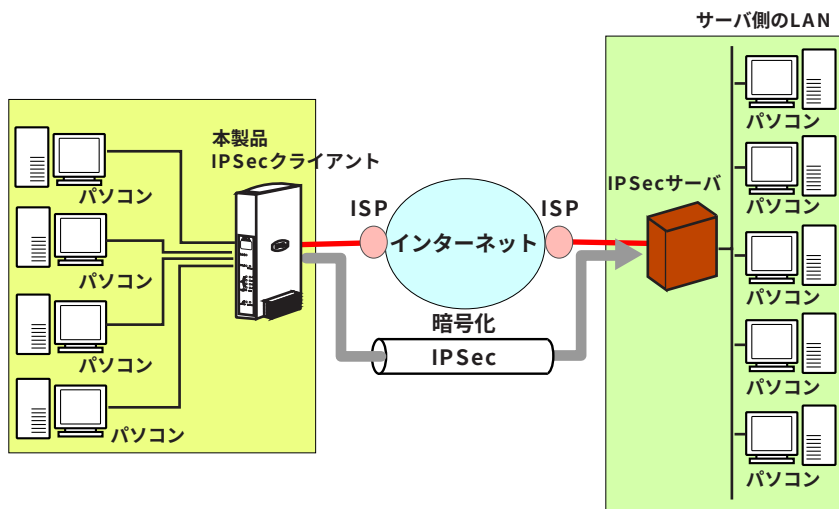
- 8** [設定完了]画面が表示されます。
[完了]ボタンをクリックします。



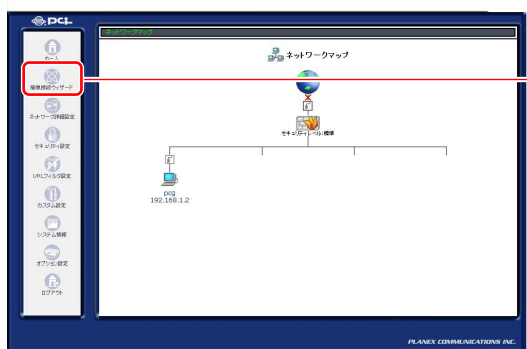
インターネットに接続されている場合、PPTPクライアントの設定が完了すると、自動的にPPTPサーバへ接続を行います。

■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。

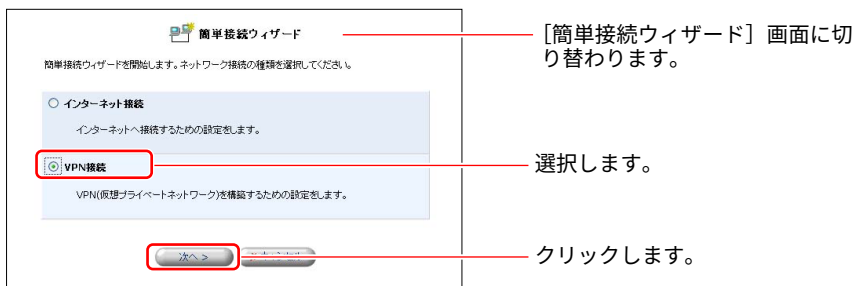


- 1 サイドバーから[簡単接続ウィザード]アイコンをクリックします。

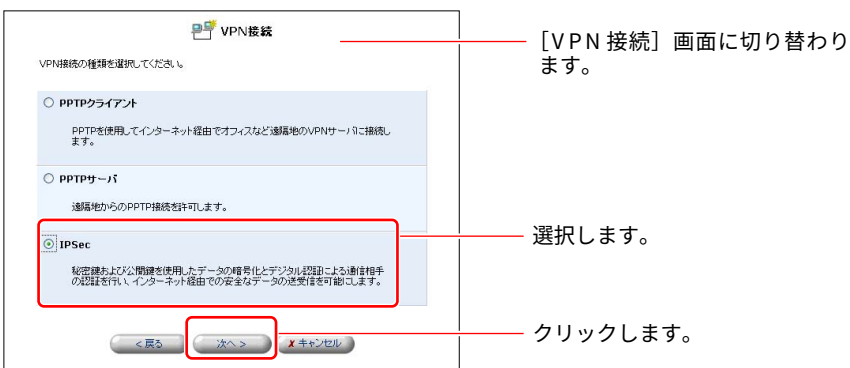


クリックします。

2 [VPN 接続]を選択し、[次へ]ボタンをクリックします。



3 [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。



The screenshot shows the 'IPSec' configuration window. At the top, it says 'IPSec接続の設定をします。' (Configure IPSec connection). Below this, there are four input fields: '接続先のホスト名またはIPアドレス:' (Host name or IP address of the peer), 'リモートサブネット:' (Remote subnet), 'リモートサブネットアドレス:' (Remote subnet address), and 'リモートサブネットマスク:' (Remote subnet mask). Each of these four fields is enclosed in a red rectangular box. Below these is a field for '共通鍵(Shared Secret):' (Shared secret). At the bottom, there are three buttons: '< 戻る' (Back), '次へ >' (Next), and a disabled button. The '次へ >' button is highlighted with a red rectangular box.

[IP Sec] 画面に切り替わります。

入力します。

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]

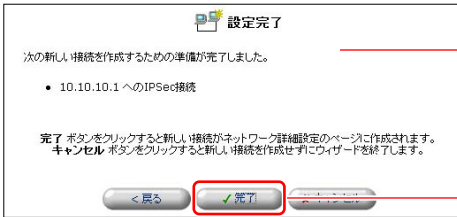
IPSec で接続する相手側のサブネットマスクを入力します。

[共通鍵]

IPSec 間で認証を行うときに使う事前共有鍵を入力します。

鍵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。



The screenshot shows the '設定完了' (Setup Complete) window. At the top, it says '設定完了' (Setup Complete). Below this, it says '次の新しい接続を作成するための準備が完了しました。' (Preparation for creating the next new connection is complete). There is a bullet point: '10.10.10.1 へのIPSec接続' (IPSec connection to 10.10.10.1). Below this, it says '完了 ボタンをク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ずにウィザードを終了します。' (Clicking the '完了' button creates a new connection on the network detail settings page. Clicking the 'キャンセル' button ends the wizard without creating a new connection). At the bottom, there are three buttons: '< 戻る' (Back), '完了' (Complete), and a disabled button. The '完了' button is highlighted with a red rectangular box.

[設定完了] 画面に切り替わります。

[完了] ボタンをクリックします。
[完了] ボタンは続けてクリックせず、1 回のみクリックしてください。

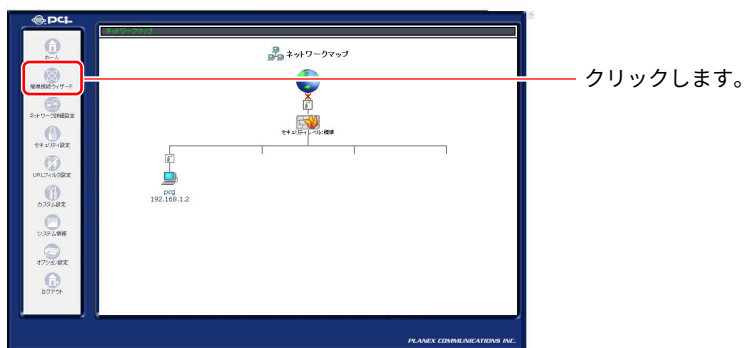
ネットワーク詳細設定による設定

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。

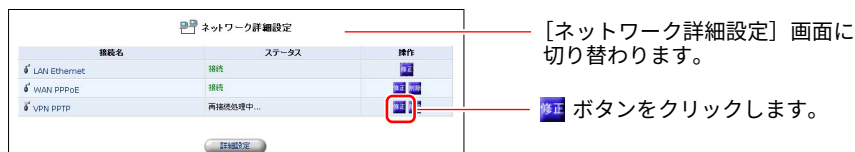
VPN の詳細な設定をするためには、あらかじめ「簡単接続ウィザード」による設定を終了しておく必要があります。

■ 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。



- 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。



- 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、基本設定、PPP、PPP 認証、PPP 暗号化、IP の設定方法などを設定します。

◎基本設定、PPP、PPP 認証の設定

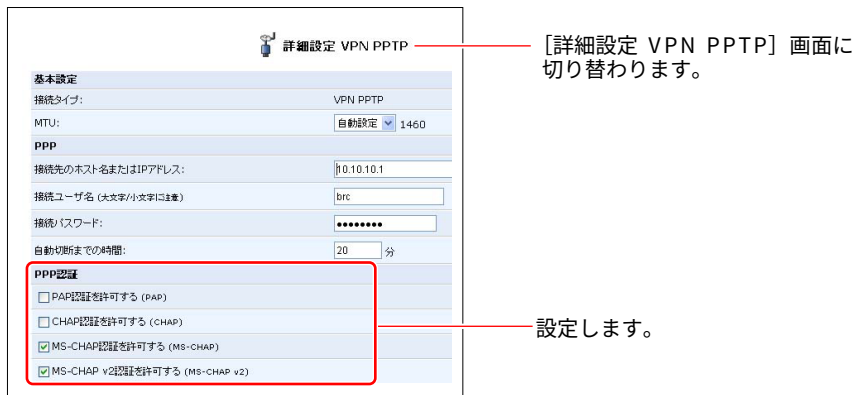
[PPP]

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。



◎ 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。



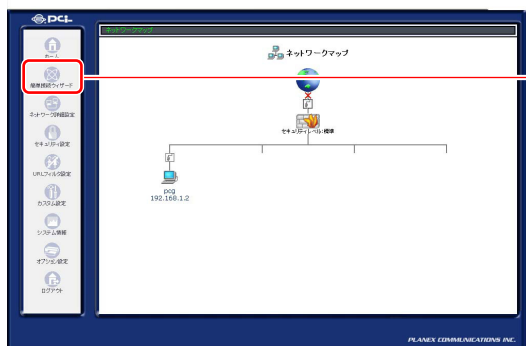
設定します。

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



クリックします。

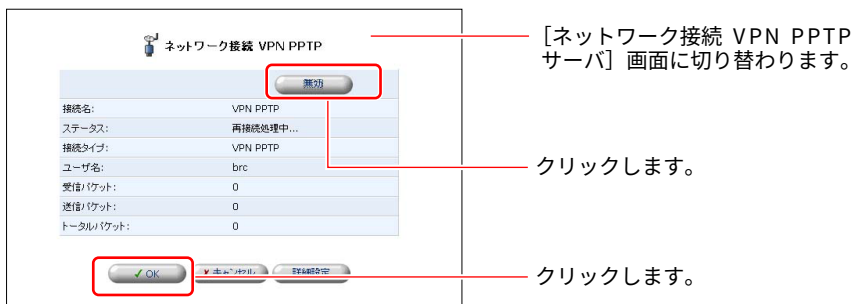
2 [接続名] 欄から削除する VPN PPTP 接続の [修正] ボタンをクリックします。



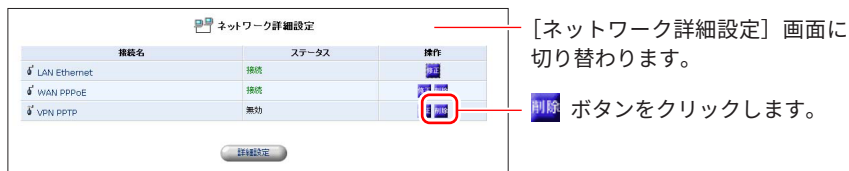
[ネットワーク詳細設定] 画面に切り替わります。

修正 ボタンをクリックします。

- 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 PPTP接続の[削除]ボタンをクリックします。

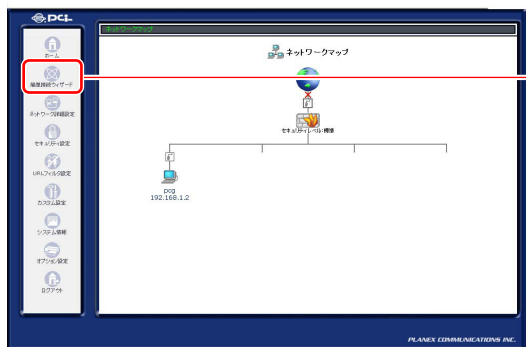


- 5** [戻る]ボタンをクリックします。

- 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



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」画面に切り替わります。

修正 ボタンをクリックします。

※ 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] 画面に切り替わります。

表示されます。

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。



設定します。

[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。

[ユーザ]

クリックすると、ユーザの設定を行うことができます。

[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。

リモートアドレス範囲				
開始:	192	168	1	155
終了:	192	168	1	254

接続名	ステータス	操作
-----	-------	----

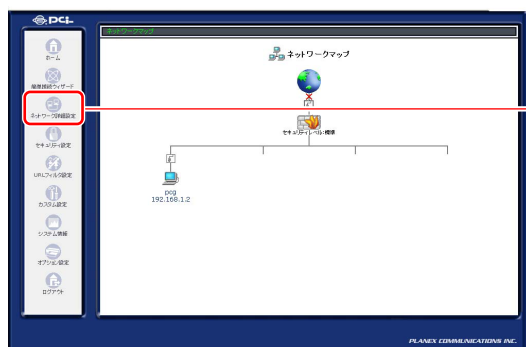
OK キャンセル 基本設定

確認します。

- 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



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。



「ネットワーク詳細設定」画面に切り替わります。

修正 ボタンをクリックします。

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。



「ネットワーク接続 VPN IPsec」画面に切り替わります。

クリックします。

4 「詳細設定 VPN IPsec」画面が表示されます。

[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

[MTU]

MTU を設定します。

[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。

[鍵交換方式]

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を選択します。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 鍵交換方式を自動に設定します。
鍵交換方式を【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。

設定します。

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】

鍵の有効期限を秒単位で設定します。

【Rekey Margin】

Rekey（鍵の再生成）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。

- ・共通鍵方式：
共通鍵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。)
- ・公開鍵方式：
公開鍵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。

IPSec IKE, Phase 2

ライフタイム (秒: 1-86400) 28000

☒ PFS有効 (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)

認証アルゴリズム (ESP)

☒ MD5

☐ SHA1

ハッシュアルゴリズム (AH)

☒ MD5

☒ SHA1

デバイスメトリック: 10

☐ マルチキャスト - IGMP Proxy Default

☐ RIP - ルーティングプロトコル

OK Cancel

設定します。

IPSec IKE, Phase 2

[ライフタイム]

鍵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。

[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。

[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。

[DNS サーバ]

DNS サーバの設定を行います。DNS サーバの IP アドレスを自動的に取得するか、DNS サーバのアドレスを固定設定するかを選択します。固定設定を選択した場合は、プライマリ DNS サーバとセカンダリ DNS サーバの IP アドレスを入力します。

また、[DNS サーバ] をクリックすると、カスタム設定で DNS サーバを選択した場合と同じ処理を行います。

[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] 画面に切り替わります。

チェックをはずしてください。

■鍵交換方式を手動に設定する場合

鍵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 手動設定

セキュリティポリシーグループ - SPI: (48ビット、例: 100 - #####)

ローカル:

リモート:

☐ ローカルとリモートで異なる暗号化キーを使用する

IPSec プロトコル:

暗号化アルゴリズム:

キー:

認証アルゴリズム:

キー:

デバイスリンク:

☐ マルチキャスト - IGMP Proxy Default

☐ RIP - ルーティングプロトコル

- 入力します。

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。

- 1 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] 画面に切り替わります。

修正 ボ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。



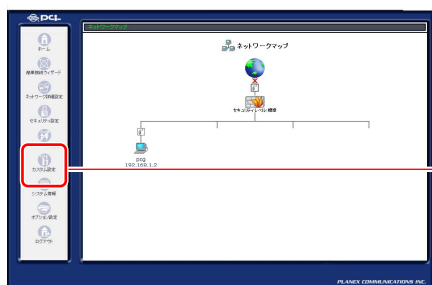
[ネットワーク接続 VPN IPsec] 画面に切り替わります。

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。

■鍵の再生成

- 1 サイドバーから [カスタム設定] アイコンを選択します。



選択します。

- 2 [IPSec] アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

クリックします。

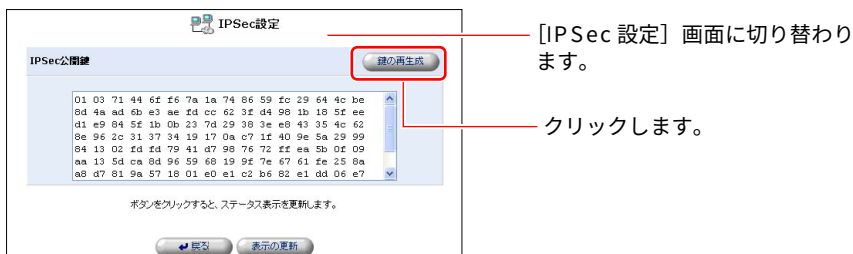
- 3 [IPSec] 画面が表示されます。[詳細設定ボタン] をクリックします。



[IPSec] 画面に切り替わります。

クリックします。

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

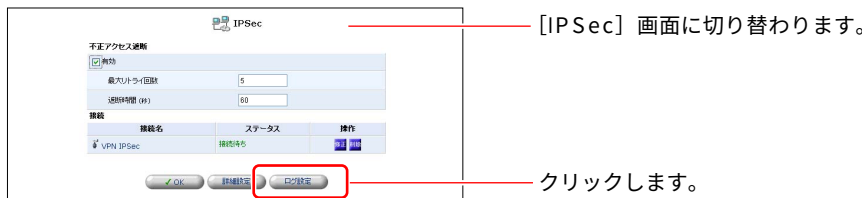


- 5** 表示の更新ボタンをクリックすると、再生成されたキーが表示されます。[戻る] ボタンをクリックすると [IPSec] 画面に戻ります。

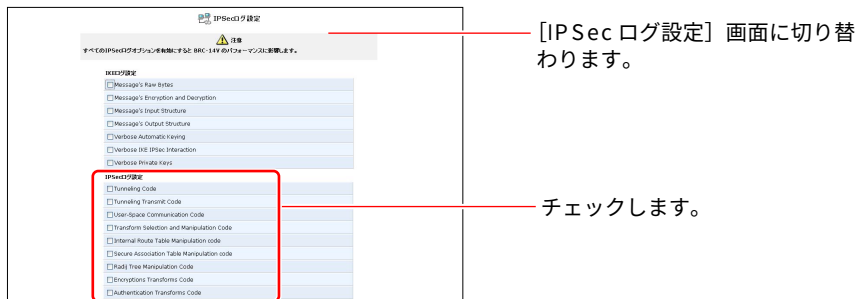
■IPSec ログの設定

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。



- 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。

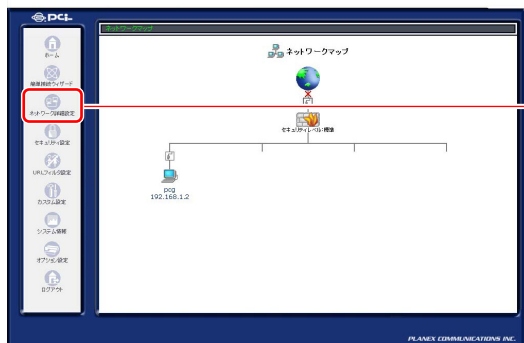


- 3 [OK] ボタンをクリックすると設定が有効になり、[IPSec] 画面に戻ります。

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



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。



[ネットワーク詳細設定] 画面に切り替わります。

修正 ボタンをクリックします。

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。



[ネットワーク接続 VPN IPSec] 画面に切り替わります。

クリックします。

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。

ネットワーク詳細設定

接続名	ステータス	操作
LAN Ethernet	接続	削除
WAN PPPoE	接続	削除
VPN IPsec	接続中	削除

詳細設定

[ネットワーク詳細設定] 画面に切り替わります。

削除 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。

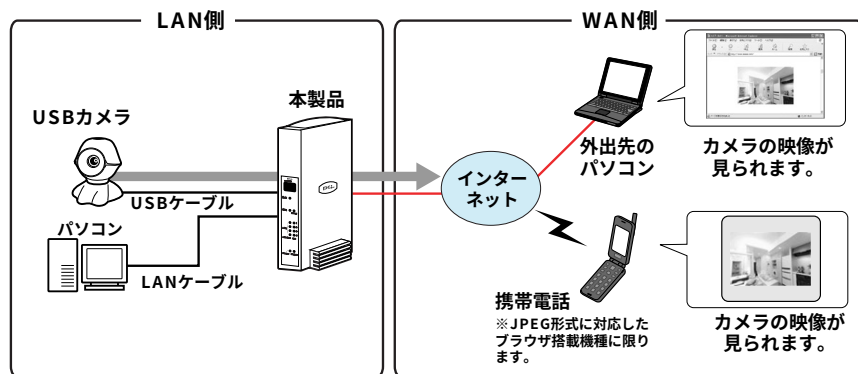
- 6** 以上で設定は終了です。

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。

USB カメラの設定

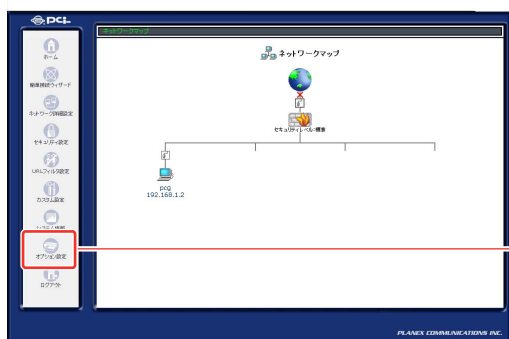
本製品のUSB インタフェースに接続したUSB カメラ（別売）で撮影した静止画や動画を、リモートアクセスしたPCや携帯電話で見ることができます。ここでは、USB カメラを有効にする設定と画像を見る方法について説明します。本体に接続できるUSB カメラは1台のみです。



※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。

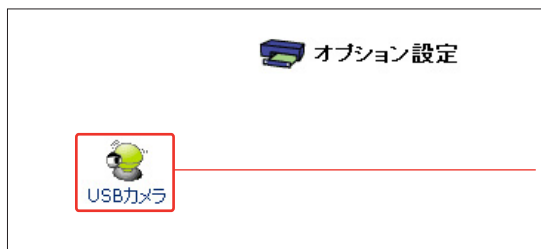
USB カメラ設定

- 1 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。



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。



クリックします。

- 3** [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。



チェックします。

! ご注意

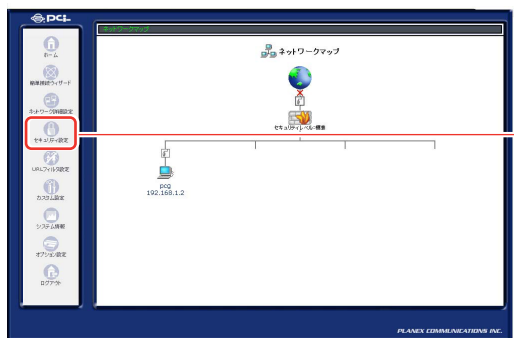
- [USB カメラ] 設定画面の「オン／オフ」は、デフォルトの設定が「オフ」になっています。
- USB カメラが「オン」の状態でカメラを取り外すと、自動的に「オフ」に切り替わります。

- 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。

- 5** [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。



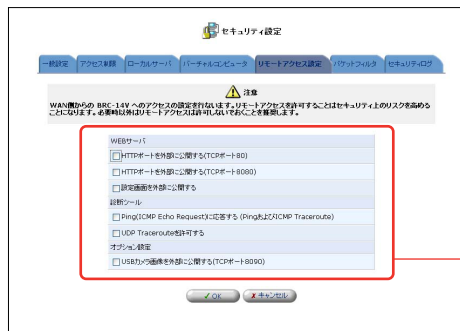
クリックします。

- 2 「セキュリティ設定」画面が表示されます。[リモートアクセス設定] をクリックします。



クリックします。

- 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 (TCPポート 80)] または [WEBサーバを外部に公開する (TCP8080)] 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 (TCP8090)] にチェックをつけます。



選択します。

- 4** [OK] ボタンをクリックします。

- 5** 以上で設定は終了です。

■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、PC 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
Windows [®]	320×240	320×240	Microsoft [®] Internet Explorer4.0以上 Netscape Navigator [®] 6.0以上 Microsoft [®] Windows [®] Media Player7.0以上
Macintosh [®]	320×240	320×240	Microsoft [®] Internet Explorer4.0以上 Netscape Navigator [®] 6.0以上 Microsoft [®] Windows [®] Media Player Mac板 (Windows [®] Media Player for Mac OS [®] X, Windows [®] Media Player 7.1 for Mac OS [®] 8-9
Linux	320×240	320×240	Netscape Navigator [®] 6.0以上 Mplayerなど
携帯電話	112×96	なし	JPEG画像をサポートしている機種のみ。 機種によっては利用できない場合があります。

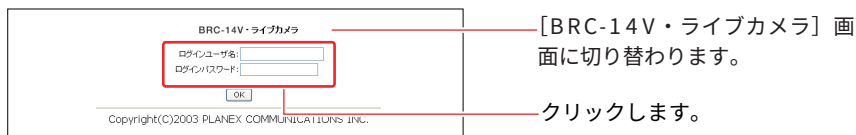
■ PCで画像を見る

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。

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。



※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はありません。

3 ログイン認証終了後、[BRC-14V・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ができます。

- 4** [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。



[BRC-14V・ライブカメラ静止画像] 画面に切り替わります。

クリックします。

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



[BRC-14V・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。

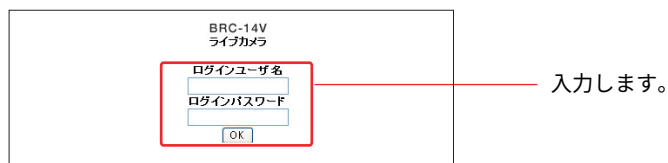
■携帯電話で画像を見る

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。



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。

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。

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。

[システム情報] 画面に切り替わります。



接続名	WAN Ethernet	LAN Ethernet	WAN PPPoE
ステータス	接続	接続	接続
物理ポート			WAN Ethernet
接続タイプ	Ethernet	Ethernet	PPPoE
MACアドレス	00:90:cc:00:00:22	00:90:cc:00:00:11	
IPアドレス	192.168.1.1	61.194.6.152	
サブネットマスク		255.255.255.0	255.0.0.0
ブロードキャスト		230.153.246.3	
DHCPサーバ		202.239.113.18 202.239.113.26	
DHCPサーバ	有効	有効	
ユーザ名			is7840020@fb22.sphere.ne.jp
宛先/ゲート	23396	7841	15495
送信/宛先	10453	11156	325
トータル/宛先	35849	18997	16020

このボタンをクリックすると、最新の情報に更新されます。

[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。

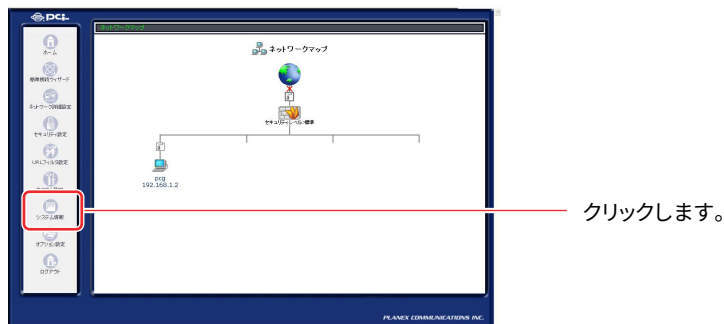
[VPN IPSec]

IPSec で通信している状況が確認できます。

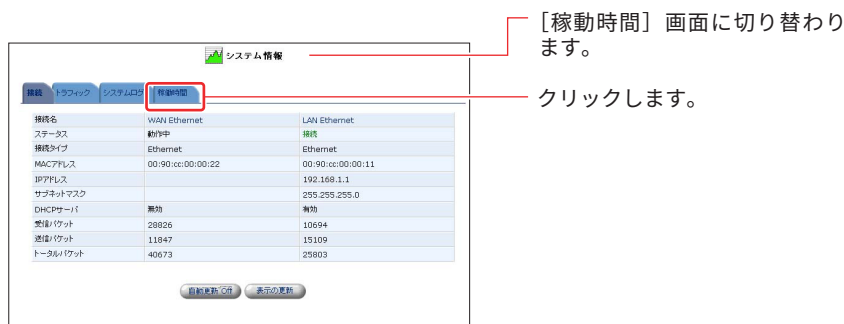
稼働時間の確認

ここでは本製品が稼働してからの現在までの時間を確認できます。

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 [稼働時間] タブをクリックします。



● 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、[今すぐ更新] 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。

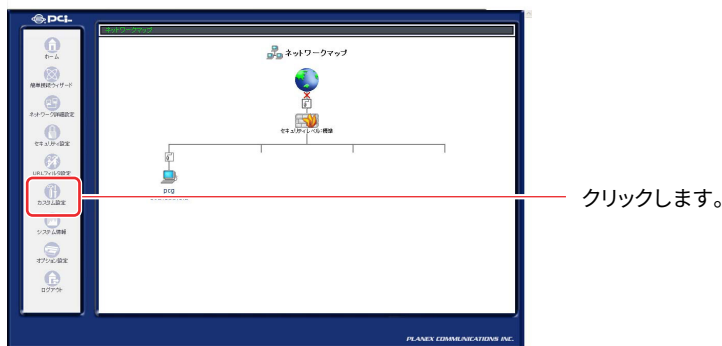
ログインユーザ名・ログインパスワード設定

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。

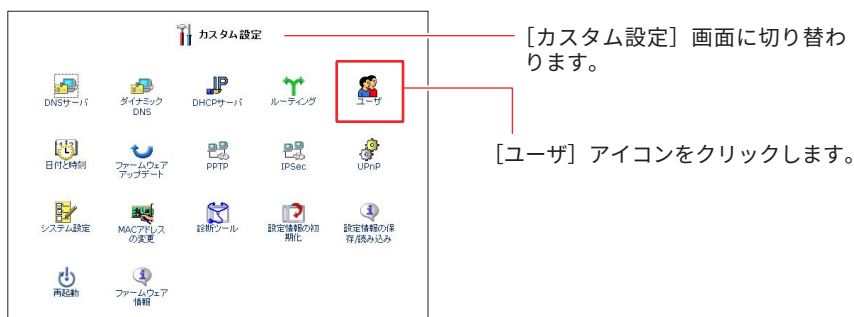
ログインユーザ名とログインパスワードの設定

■ユーザの新規作成

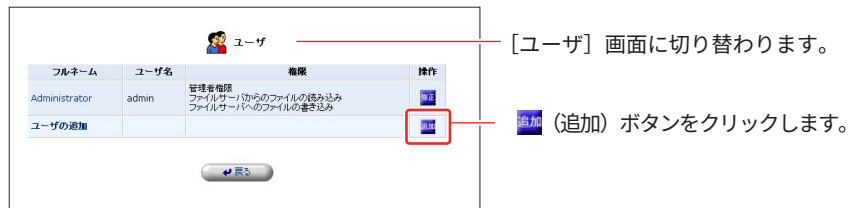
- 1 サイドバーから「カスタム設定」アイコンをクリックします。



- 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。

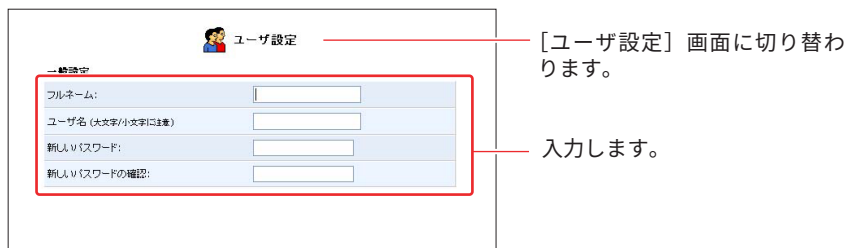


[ユーザ] 画面に切り替わります。

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			

追加 (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。



[ユーザ設定] 画面に切り替わります。

入力します。

[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 ☐ 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
-----	--

[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通知設定		SMTPメールサーバの設定
E-Mailアドレス:		設定します。
システム通知レベル:	なし ▼	
セキュリティ通知レベル:	なし ▼	

※ 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

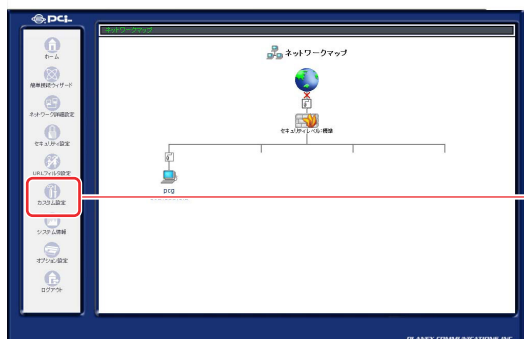
7 [OK] ボタンをクリックします。

OK キャンセル	クリックします。
--	----------

8 以上で設定は終了です。

■ユーザの修正

- 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。



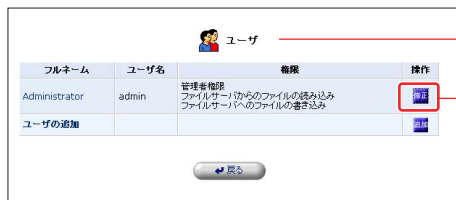
- 2 [ユーザ] アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

[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] 画面に切り替わります。

修正（修正）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。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。

ユーザ設定

一般設定

フルネーム: administrator

ユーザ名 (大文字/小文字に注意): admin

新しいパスワード: *****

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
- ☒ ファイルサーバーからのファイルの読み込み
- ☒ ファイルサーバーへのファイルの書き込み
- ☐ USBカメラ

E-Mail通知設定

SMTPメールサーバーの設定

E-Mailアドレス:

システム通知レベル: なし

セキュリティ通知レベル: なし

OK

キャンセル

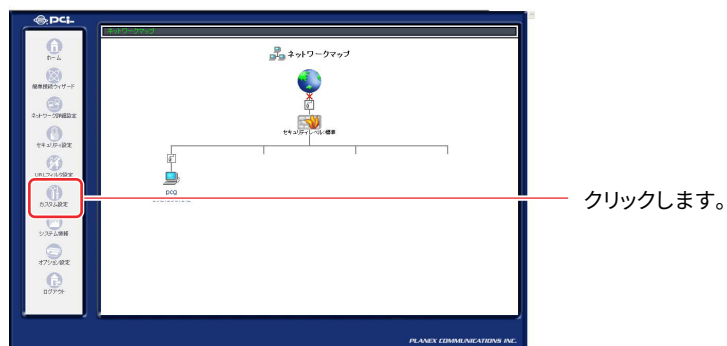
[ユーザ設定] 画面に切り替わります。

クリックします。

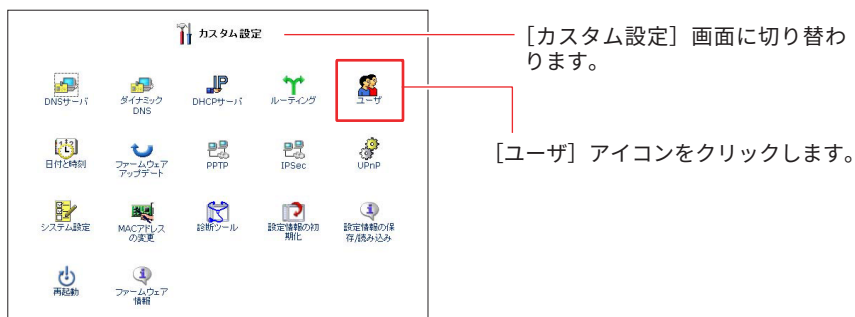
5 以上で設定は終了です。

■ユーザの削除

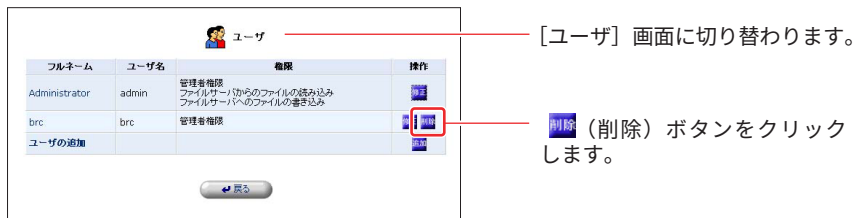
1 サイドバーから [カスタム設定] アイコンをクリックします。



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

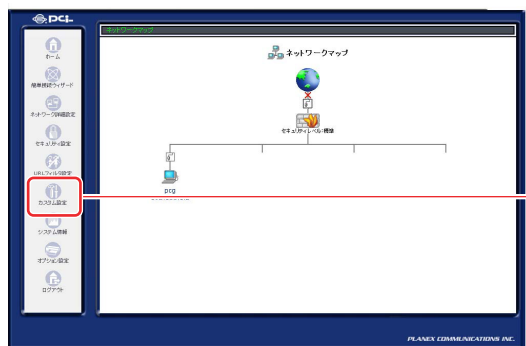
購入時に登録されてる Administrator は削除することができません。

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。



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。



[カスタム設定] 画面に切り替わります。

[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。



[システム設定] 画面に切り替わります。

[システム] 欄に本商品のホスト名、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。



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グ設定

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 ▼

設定します。

※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:

送信元メールアドレス:

入力します。

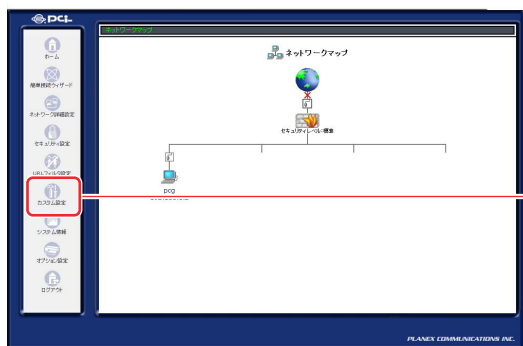
8 [OK] ボタンをクリックします。

9 以上で設定は終了です。

日付と時刻の設定

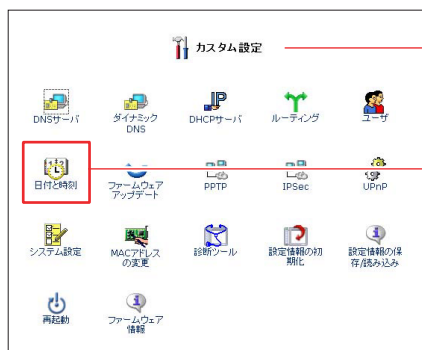
本製品の日付や時刻の設定を変更できます。

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。



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。



「カスタム設定」画面に切り替わります。

「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。

日付と時刻

手動設定

日付: 11月 5 2002

時刻: 14 : 57 : 32

[日付と時刻] 画面に切り替わります。

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。

自動設定

☒ 有効

プロトコル: ☐ TOD(Time Of Day) ☒ NTP(Network Time Protocol)

更新間隔: 24 時間

NTPサーバアドレス: 210.172.160.87

ステータス: 時刻同期成功

ボタンをクリックすると、ステータス表示を更新します。

OK キャンセル 表示の更新

チェックします。

5 [NTP サーバアドレス]、[ステータス]、[プロトコル]、[更新時間] 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。

[プロトコル]

プロトコルの種類。通常は NTP を指定してください。

[更新時間]

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

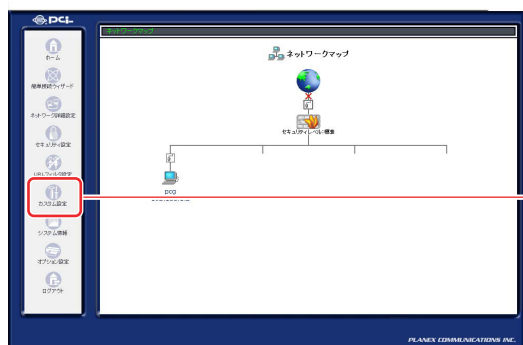
本製品の購入後、当社のホームページからダウンロードしたファイルを使って、最新のファームウェアにアップデートすることができます。

！ 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。

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。



クリックします。

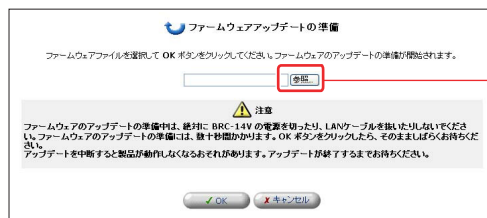
3 [ファームウェアアップデート] アイコンをクリックします。



[カスタム設定] 画面に切り替わります。

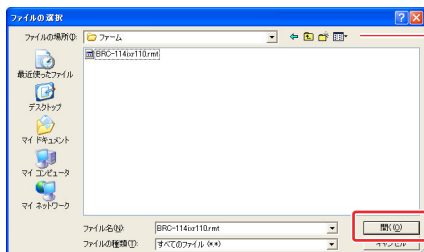
[ファームウェアアップデート] アイコンをクリックします。

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。



クリックします。

5 [開く] ボタンをクリックします。



※ Windows® XP のダイアログです。ご使用の OS により、ダイアログは異なります。

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。

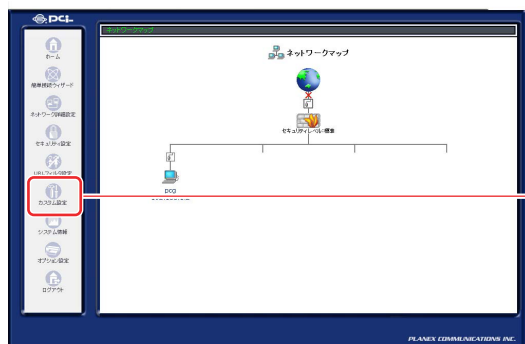
! **ご注意**

本商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。



クリックします。

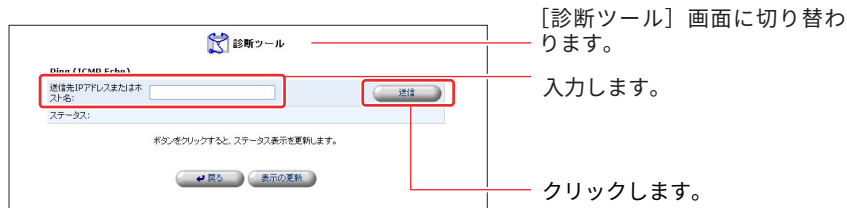
- 2 [診断ツール] アイコンをクリックします。



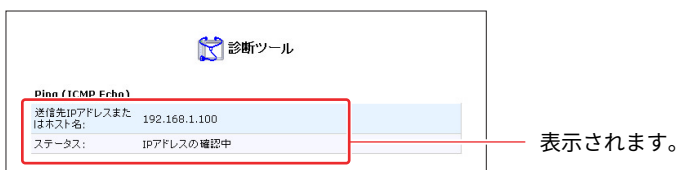
[カスタム設定] 画面に切り替わります。

クリックします。

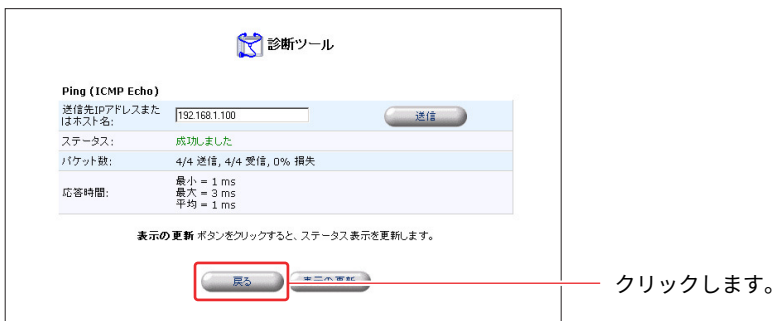
3 [送信先IPアドレスまたはホスト名] 欄に Ping を送信したいIP アドレスまたはホスト名を入力します。



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



5 [ステータス] 欄に送信結果が表示されます。



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。

本製品の初期化

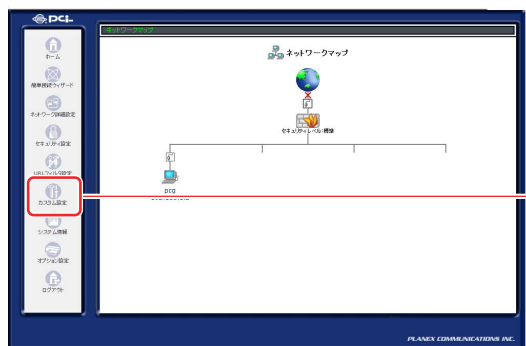
設定ページから本製品の設定内容を消去して、購入時の状態に戻すことができます。

※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。



クリックします。

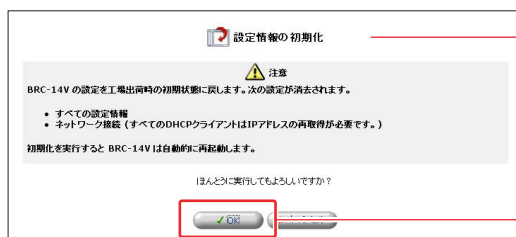
2 「設定情報の初期化」アイコンをクリックします。



「カスタム設定」画面に切り替わります。

クリックします。

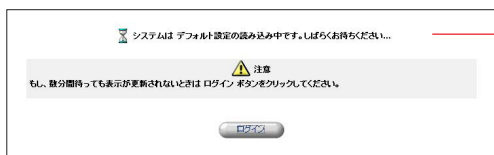
3 [OK] ボタンをクリックします。



「設定情報の初期化」画面に切り替わります。

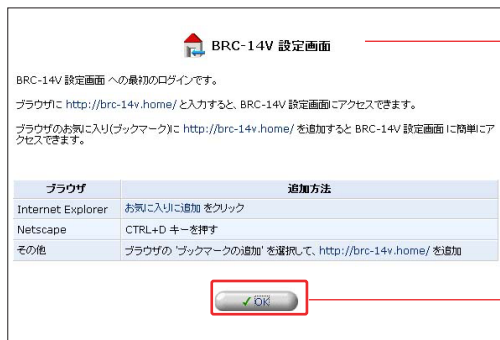
[OK] ボタンをクリックします。

4 初期化が始まります。



設定内容の消去が開始します。
消去中は、この画面が表示されます。

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-14V 設定画面」に切り替わります。

[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

BRC-14V のログインユーザ名とログインパスワードを設定してください。

ログインユーザ名: admin

新しいログインパスワード:

新しいログインパスワードの確認:

OK

[ログイン設定] 画面に切り替わります。

入力します。

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。

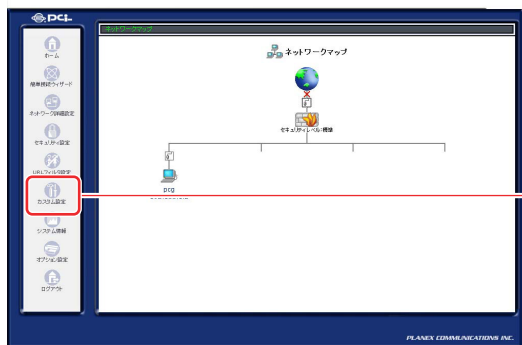
[新しいログインパスワードの確認]

[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。



クリックします。

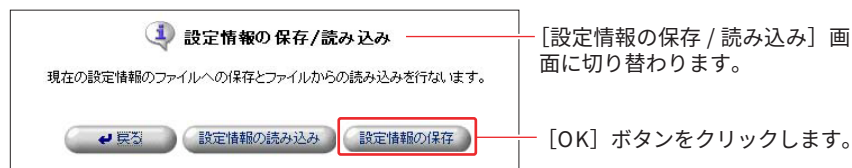
2 カスタム設定の「設定情報の保存/読み込み」アイコンをクリックします。



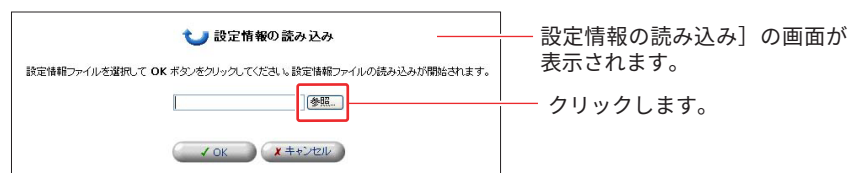
「カスタム設定」画面に切り替わります。

クリックします。

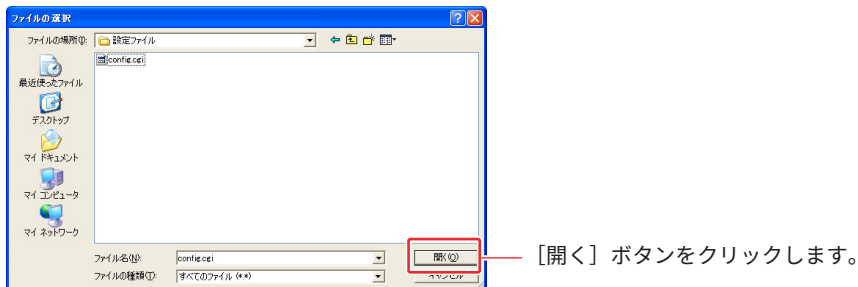
3 「設定情報の読み込み」 ボタンをクリックします。



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。



5 「開く」ボタンをクリックします。

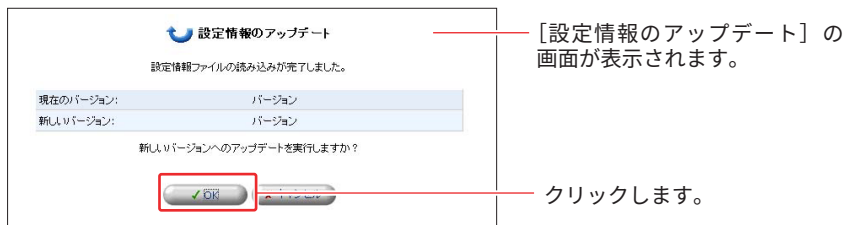


6 [OK] ボタンをクリックすると、設定情報の読み込みの準備が開始されます。

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。



! **ご注意**

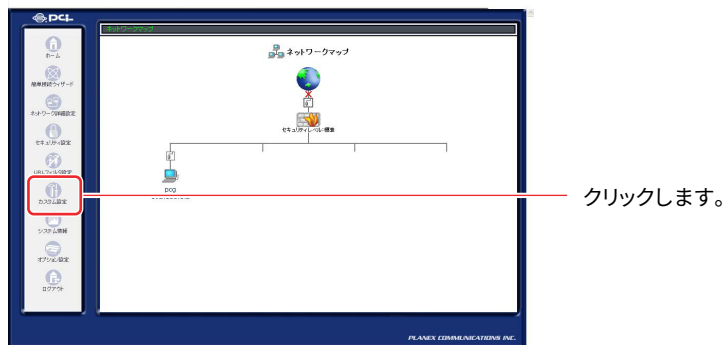
- ・ [現在のバージョン] と [新しいバージョン] にはファームウェアのバージョンが表示されます。
- ・ ファームウェアのバージョンが異なると設定情報のアップデートができない場合がありますのでご注意ください。

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

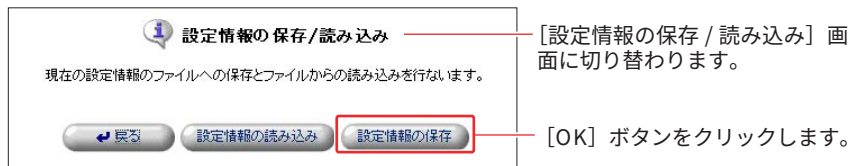
- 1 サイドバーから [カスタム設定] アイコンをクリックします。



- 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。



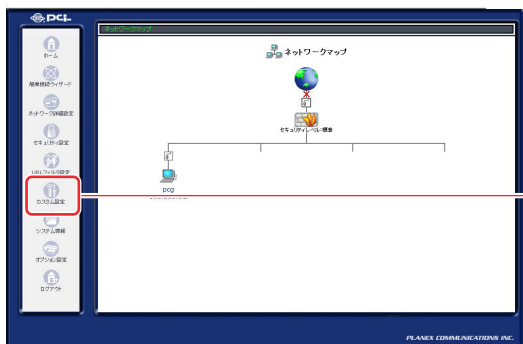
- 4 [ファイルのダウンロード] の画面が表示されます。[保存] ボタンをクリックしてコンピュータに保存します。

- 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。



クリックします。

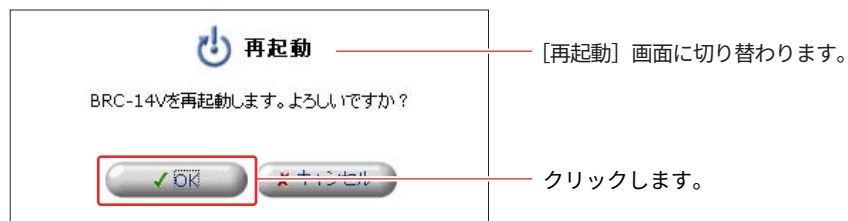
2 「再起動」アイコンをクリックします。



「カスタム設定」画面に切り替わります。

クリックします。

3 [OK] ボタンをクリックします。

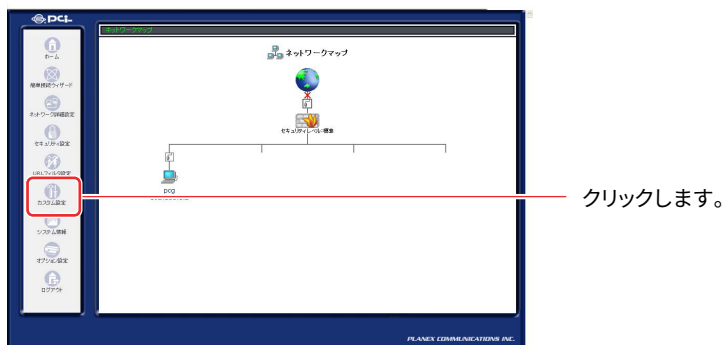


4 再起動が完了すると、ログイン画面に切り替わります。

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。

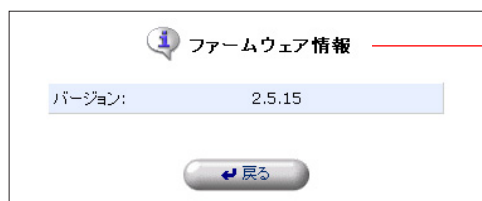
1 サイドバーから「カスタム設定」アイコンをクリックします。



2 「ファームウェア情報」アイコンをクリックします。



3 本製品のファームウェアのバージョンが表示されます。



「ファームウェア情報」画面に切り替わります。