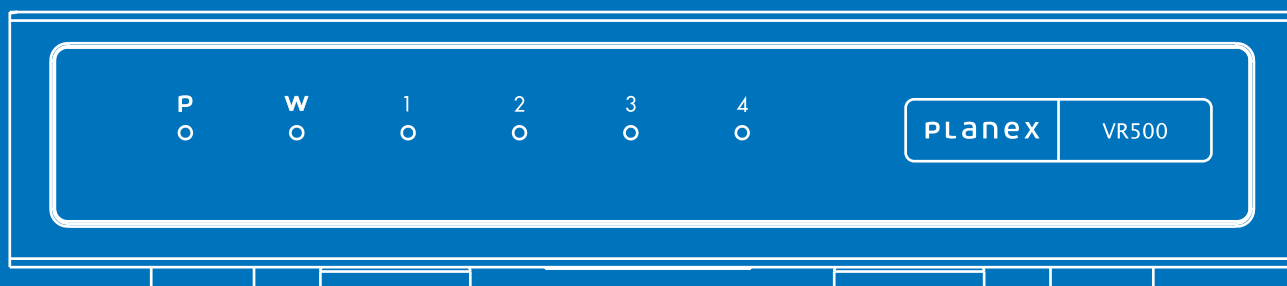


Planex COMM.

鎖国
SARUKU
VR500



本体操作ガイド

ユーザーズマニュアル

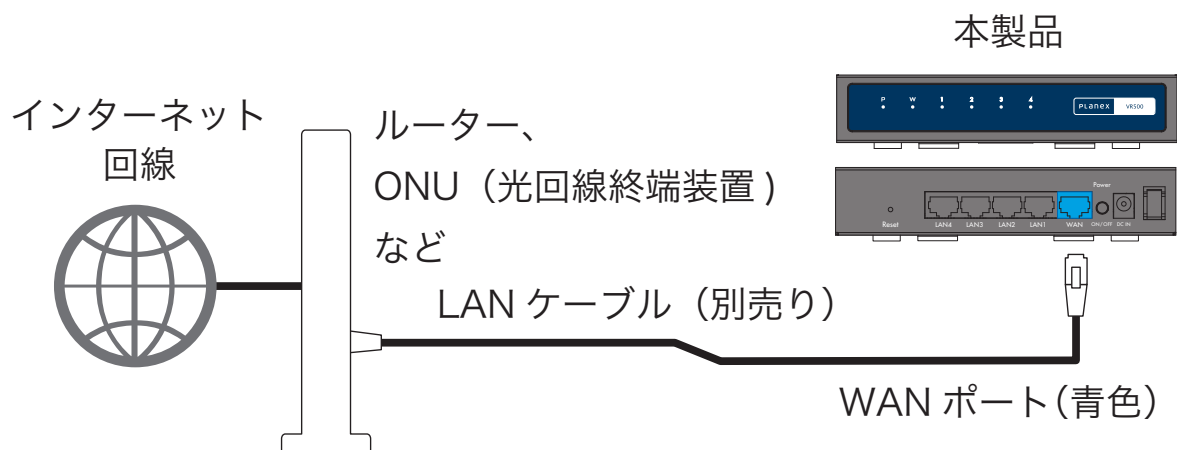
目次

1 使用方法	
1-1 接続する	p1
2 接続～設定画面	
2-1 端末と接続して設定画面を開く	p2
3 ルーター設定画面	
3-1 言語選択	p3
3-2 ステータス	p4
3-3 統計	p5
3-4 DHCPクライアント	p6
3-5 システムログ	p7
3-6 WAN DHCP	p8
3-6 WAN 固定IP	p9
3-6 WAN PPPoE	p10
3-7 LAN	p11
3-8 DHCP	p12
3-9 VPN パススルー	p13
3-10 MAC/IP/ポートフィルタ	p14
3-11 システムセキュリティ	p15
3-12 コンテンツフィルタ	p16
3-13 ポートフォワード	p17
3-14 ポートトリガー	p18
3-15 DMZ	p19
3-16 管理	p20
3-17 ファームウェア更新	p21
3-18 設定管理	p22
3-19 再起動	p23
4 ルーター設定画面	
4-1 ブラックリスト	p24
4-2 ホワイトリスト	p25
4-3 遮断ログ	p26
5 同梱物	
5-1 同梱物リスト	p27
5-2 別途ご用意いただくもの	p27
6 商品本体	
6-1 各部名称とはたらき	p28
7 工場出荷時の設定値	
7-1 設定値	p29

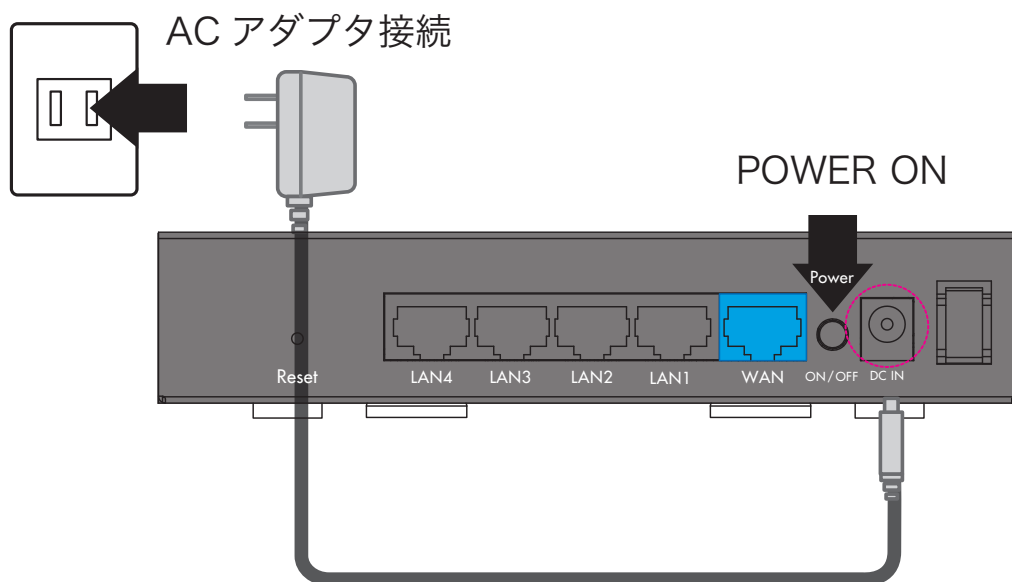
1. 使用方法

1-1 接続する

本製品の「WAN」（青色）ポートとルーターやONUなど通信機器をLANケーブルでつなぎます。



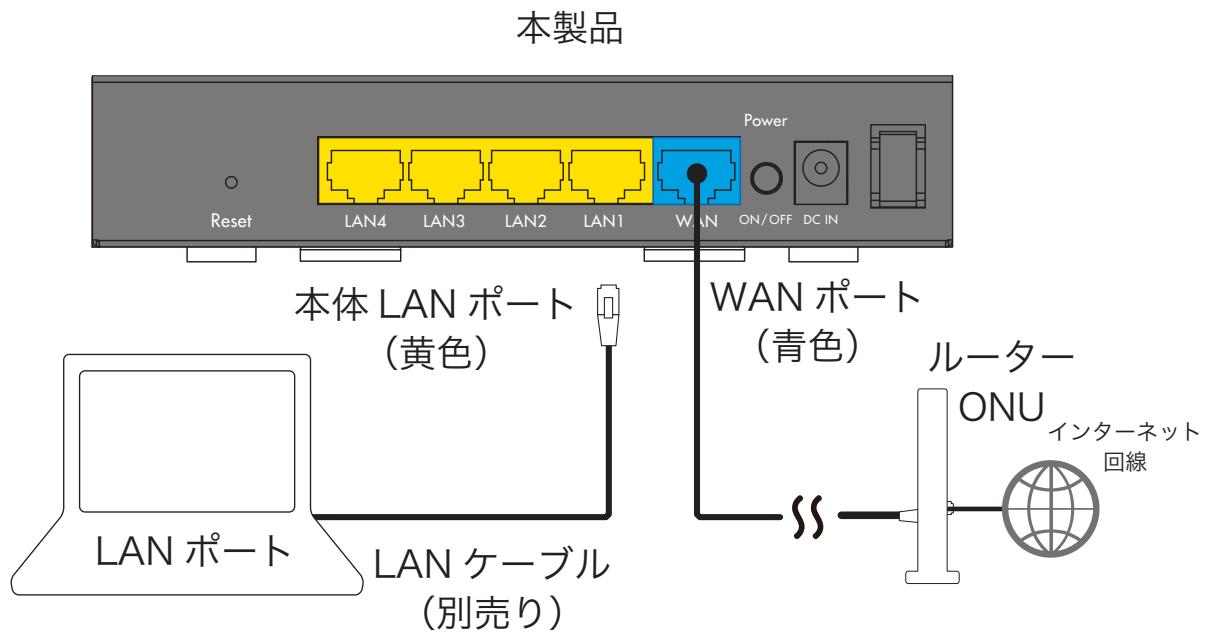
本製品にACアダプタを接続してPOWERボタンを「ON」にします。



2. 接続～設定画面

2-1 端末と接続して設定画面を開く

- 1) 本製品の「LAN」（黄）ポートとPCをLANケーブルで接続します。

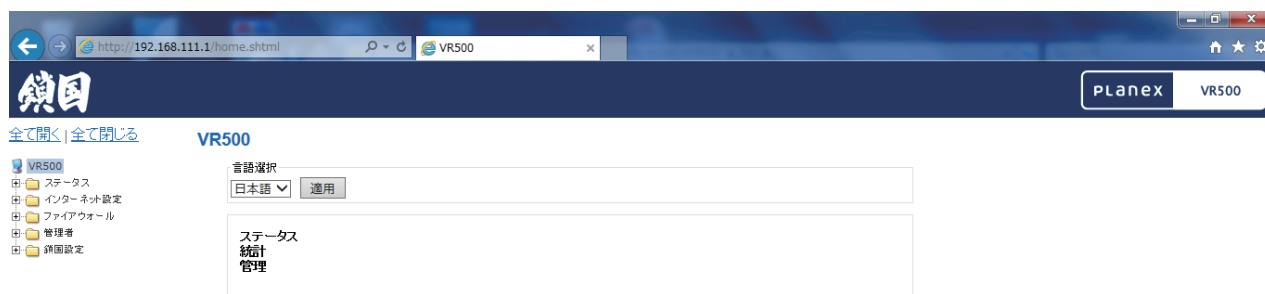


- 2) ブラウザを起動します。
- 3) ブラウザのアドレス欄に「192.168.111.1」と入力します。
(ただし、上位ルータが192.168.111.1だった場合は、192.168.110.1へ自動変更されます。)
- 4) ユーザー名に「admin」、パスワードに「password」を入力してOKをクリックします。

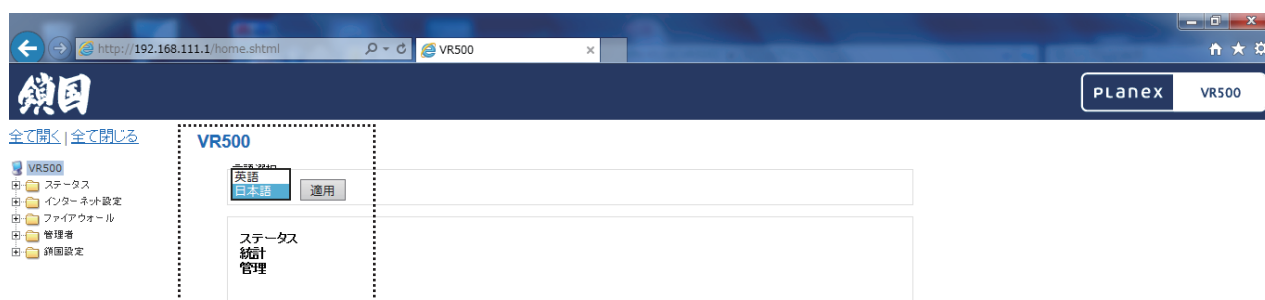
3. ルーター設定画面

3-1 言語選択

本製品の設定画面は、「日本語」（工場出荷時）と「英語」に対応しています。



任意の言語を選択して、[適用]ボタンを押して下さい。



3. ルーター設定画面

3-2 ステータス

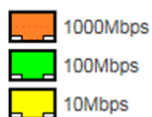
本製品の現在のステータスを表示します。

ステータス

ステータスを参照します。

システム情報	
ファームウェアバージョン	v1.08 (May 20 2016)
システム稼働時間	4 mins, 0 secs
システムプラットフォーム	MT7621 embedded switch
動作モード	Gateway Mode
インターネット設定	
接続タイプ	DHCP
WAN IPアドレス	192.168.12.69
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.12.1
プライマリDNS	192.168.1.20
セカンダリDNS	192.168.1.22
MACアドレス	88-23-27-19-00-00
ローカルネットワーク	
ローカルIPアドレス	192.168.111.1
ローカルネットワークマスク	255.255.255.0
MACアドレス	88-23-27-19-00-00

イーサネットポートステータス



3. ルーター設定画面

3-3 統計

本製品のステータスの内、統計データを表示します。

統計

統計を参照します。

メモリ	
メモリ合計	254488 kB
メモリ残量	221296 kB
WAN/LAN	
WAN受信パケット	1621
WAN受信バイト	189634
WAN送信パケット	1683
WAN送信バイト	192003
LAN受信パケット	2783
LAN受信バイト	274423
LAN送信パケット	1022
LAN送信バイト	1319563
全インターフェース	
名称	lo
Rxのパケット	54
Rxのバイト	3336
Txのパケット	54
Txのバイト	3336
名称	eth2
Rxのパケット	3179
Rxのバイト	354540
Txのパケット	1079
Txのバイト	1398188
名称	eth3
Rxのパケット	1889
Rxのバイト	227056
Txのパケット	1934
Txのバイト	210747
名称	vlan1
Rxのパケット	3070
Rxのバイト	296908
Txのパケット	1079
Txのバイト	1398188

3. ルーター設定画面

3-4 DHCPクライアント

本製品に接続されているクライアントのリストを表示します。

DHCPクライアントリスト

DHCPクライアントの一覧が表示されます。

DHCPクライアント			
ホストネーム (オプション)	MACアドレス	IPアドレス	リース残り時間
		192.168.111.100	00:00:00

3. ルーター設定画面

3-5 システムログ

システムログを表示します。

ボタン名	処理
リフレッシュ	最新のログを再描画します。
クリア	本体のログを消去します。

システムログ

リフレッシュ クリア

システムログ

```

Jan  1 09:00:01 VR500 kern.warn kernel: kalink gpio driver initialized

```

3. ルーター設定画面

3-6 WAN

WANの各種設定を行います。



1) DHCPの場合

上位よりDHCPによるIPアドレスの払い出しがある場合、「DHCP」（工場出荷時設定）を選択し [適用] ボタンを押します。

入力項目	内容
ホストネーム (オプション)	ホスト名によるDNSアップデートが必要な場合は設定してください

WAN設定

WANの各種設定を行います。

接続方式:		DHCP ▼
DHCP接続 		
ホストネーム (オプション)	<input type="text"/>	
MACアドレスコピー 		
有効	無効 ▼	
<input type="button" value="適用"/> <input type="button" value="キャンセル"/>		

3. ルーター設定画面

3-6 WAN

WANの各種設定を行います。

2) 固定IP接続の場合

本製品のWAN側を固定IPで運用する場合、「固定IP」を選択し、[適用]ボタンを押します。

入力項目	内容
IPアドレス	本製品のWAN側IPアドレスを入力してください。
サブネットマスク	WAN側サブネットマスクアドレスを入力してください。
デフォルトゲートウェイ	デフォルトゲートウェイアドレスを入力してください。
プライマリDNSサーバ	プライマリで利用するDNSサーバのアドレスを指定してください。
セカンダリDNSサーバ	プライマリで利用するDNSサーバのアドレスを指定してください。 ※省略可

WAN設定

WANの各種設定を行います。

接続方式: 固定IP ▼

固定IP接続	
IPアドレス	<input type="text" value="192.168.12.69"/>
サブネットマスク	<input type="text" value="255.255.255.0"/>
デフォルトゲートウェイ	<input type="text" value="192.168.12.1"/>
プライマリDNSサーバ	<input type="text" value="192.168.1.20"/>
セカンダリDNSサーバ	<input type="text" value="192.168.1.22"/>
MACアドレスコピー	
有効	無効 ▼

適用
キャンセル

3. ルーター設定画面

3-6 WAN

WANの各種設定を行います。

3) PPPoEの場合

本製品から直接ISP (Internet Service Provider)に接続する場合、「PPPoE」を選択し、[適応]ボタンを押します。

入力項目	内容
ユーザ名	契約ISPより通知されたIDを入力してください。
パスワード	契約ISPより通知されたパスワードを入力してください。
パスワードの確認	契約ISPより通知されたパスワードをもう一度入力してください。
動作モード	PPPoE接続方式を選択してください。 常時接続：常にISPに接続します。 オンデマンド：通信が発生した時にISPへ接続します。
通信時接続： アイドル時間 [分]	プライマリで利用するDNSサーバのアドレスを指定してください。 ※省略可

WAN設定

WANの各種設定を行います。

接続方式: PPPoE ▼

PPPoE接続

ユーザ名	<input style="width: 90%;" type="text" value="pppoe_user"/>
パスワード	<input style="width: 90%;" type="password" value="....."/>
パスワードの確認	<input style="width: 90%;" type="password" value="....."/>
動作モード	<div style="display: flex; align-items: center;"> 常時接続 ▼ </div> <div style="margin-top: 5px;"> On demand Mode: Idle Time <input style="width: 40px; text-align: center;" type="text" value="5"/> minutes </div>

MACアドレスコピー

有効	無効 ▼
----	--

適用
キャンセル

4) MACアドレスコピー

WAN側で本製品既存のMACアドレスを利用しない場合は有効を選択してください。

入力項目	内容
MACアドレス	WAN側で利用するMACアドレスを入力してください。 有効時のみ設定可能です。

3. ルーター設定画面


3-7 LAN

本製品のLAN側の設定を行います。各項目を設定後、[適用]ボタンを押してください

入力項目	内容
ホストネーム	LAN内で用いるホストネームを入力してください。
IPアドレス	本機器のLAN側IPを入力してください。
サブネットマスク	本機器のLAN側サブネットマスクアドレスを入力してください。
DHCPタイプ	DHCP機能を利用する場合は有効を選択してください。
開始IPアドレス	DHCPサーバが配布するIPアドレスのうち開始アドレスを入力してください。
終了IPアドレス	DHCPサーバが配布するIPアドレスのうち終端アドレスを入力してください。
サブネットマスク	DHCPサーバが配布するサブネットマスクアドレスを入力してください。
プライマリDNSサーバ	DHCPサーバが配布するプライマリDNSサーバアドレスを入力してください。
セカンダリDNSサーバ	DHCPサーバが配布するセカンダリDNSサーバアドレスを入力してください。
デフォルトゲートウェイ	DHCPサーバが配布するデフォルトゲートウェイアドレスを入力してください。
リース時間	DHCPサーバが配布するIPアドレスのリース有効期限を入力してください。
802.1d スパニングツリー	STPによるループバック防止を行う場合は有効を選択してください。

LAN設定

LANのIPアドレスやDHCPサーバの設定を行います。

LAN設定 	
ホストネーム (オプション)	<input type="text" value="VR500"/>
IPアドレス	<input type="text" value="192.168.111.1"/>
サブネットマスク	<input type="text" value="255.255.255.0"/>
MACアドレス	<input type="text" value=""/>
DHCPタイプ	<input type="text" value="サーバ ▼"/>
開始IPアドレス	<input type="text" value="192.168.111.100"/>
終了IPアドレス	<input type="text" value="192.168.111.200"/>
サブネットマスク	<input type="text" value="255.255.255.0"/>
プライマリDNSサーバ	<input type="text" value="192.168.111.1"/>
セカンダリDNSサーバ	<input type="text" value=""/>
デフォルトゲートウェイ	<input type="text" value="192.168.111.1"/>
リース時間	<input type="text" value="86400"/>
802.1d スパニングツリー	<input type="text" value="無効 ▼"/>

3. ルーター設定画面

3-8 DHCP

DHCPクライアントに、静的アドレス(固定IPアドレス)を割り当てることができます。

DHCP 静的アドレス設定

DHCPクライアントに、静的アドレス(固定IPアドレス)を割り当てることができます。


現在のDHCP 静的アドレス設定		
No.	MACアドレス	IPアドレス
<input type="button" value="追加"/> <input type="button" value="選択項目の削除"/> <input type="button" value="リセット"/>		

[追加]ボタンを押すとDHCPクライアントの追加画面に遷移します。

入力項目	内容
MACアドレス	静的割り当てを行う機器のMACアドレスを入力してください。
IPアドレス	静的割り当てを行うMACアドレスに対し割り当てるMACアドレスを入力してください。

DHCP 静的アドレス設定

静的アドレスの設定を行います。

DHCP静的アドレス設定 	
MACアドレス	<input type="text"/>
IPアドレス	<input type="text"/>
<input type="button" value="適用"/> <input type="button" value="キャンセル"/>	

3. ルーター設定画面


3-9 VPN パススルー

L2TP、IPsec、PPTP、IPv6のパススルー設定を行います。

入力項目	内容
L2TP,IPsecパススルー	L2TP,IpsecをLAN側で利用する場合は有効を選択します。
PPTPパススルー	PPTPをLAN側で利用する場合は有効を選択します。
IPv6パススルー	WAN側とIPv6ブリッジングする場合は有効を選択します。

VPNパススルー

L2TP、IPsec、PPTP、IPv6のパススルー設定を行います。

VPNパススルー 	
L2TP, IPsecパススルー	無効 ▼
PPTPパススルー	無効 ▼
IPv6パススルー	無効 ▼

3. ルーター設定画面

3-10 MAC/IP/ポート フィルタ

インターネット上のウィルスやワーム等からネットワークを守るために、ファイアウォールを設定することも出来ます。

1)基本設定


入力項目	内容
MAC/IP/ポートフィルタ	パケットフィルタリングを行う場合は有効を選択してください。
標準方針	作成するルールに従って運用方法を選択してください。


2)MAC/IP/ポート フィルタ設定

入力項目	内容
送信元MACアドレス	送信元MACアドレスによってフィルタリングする場合は該当するMACアドレスを入力してください。
宛先IPアドレス	送信先IPアドレスによってフィルタリングする場合は該当するIPアドレスを入力してください。
送信元IPアドレス	送信先IPアドレスによってフィルタリングする場合は該当するIPアドレスを入力してください。
プロトコル	プロトコルによってフィルタリングする場合は該当するプロトコルを入力してください。
宛先ポート番号の範囲	IP通信先ポート番号によってフィルタリングする場合は該当するポート番号を入力してください。
送信元ポート番号の範囲	IP通信元ポート番号によってフィルタリングする場合は該当するポート番号を入力してください。
動作	ルールに合致した場合の挙動を選択してください。
コメント	作成するルールに付与するコメントを入力してください。

MAC/IPポート フィルタ設定

インターネット上のウィルスやワーム等からネットワークを守るために、ファイアウォールを設定することも出来ます。

基本設定 	
MAC/IP/ポートフィルタ	<input type="button" value="無効"/> ▼
標準方針: ルールに沿わないパケットの通過を	<input type="button" value="許可しない"/> ▼
<input type="button" value="適用"/> <input type="button" value="リセット"/>	

MAC/IP/ポート フィルタ設定 	
送信元MACアドレス	<input type="text"/>
宛先IPアドレス	<input type="text"/>
送信元IPアドレス	<input type="text"/>
プロトコル	<input type="button" value="None"/> ▼
宛先ポート番号の範囲	<input type="text"/> - <input type="text"/>
送信元ポート番号の範囲	<input type="text"/> - <input type="text"/>
動作	<input type="button" value="許可"/> ▼
コメント	<input type="text"/>
<small>(登録できる最大設定数: 32.)</small>	
<input type="button" value="適用"/> <input type="button" value="リセット"/>	

設定済みフィルタ									
No.	送信元MACアドレス	宛先IPアドレス	送信元IPアドレス	プロトコル	宛先ポート番号の範囲	送信元ポート番号の範囲	動作	コメント	パケット数
下記リストのみ許可する									
-									
<input type="button" value="選択項目の削除"/> <input type="button" value="リセット"/>									

3. ルーター設定画面

3-11 システムセキュリティ

本機器自体を保護するために、システムセキュリティを設定することができます。

入力項目	内容
遠隔管理	許可：WAN側からWebUIへのアクセスを許可します。 拒否：WAN側からWebUIへアクセスすることが出来ません。
WAN側からのPingをブロック	無効：WAN側からのPingに応答します。 有効：WAN側からのPingに応答しません。
ポートスキャンブロック	無効：WAN側からのポートスキャンを通します。 有効：WAN側からのポートスキャンをブロックします。
Dos攻撃ブロック	無効：WAN側からのDos攻撃をブロックしません。 有効：WAN側からのDos攻撃をブロックします。
SPIファイアウォール	無効：SPIを無効にします。 有効：SPIを有効にします。

システムセキュリティ設定

本機器自体を保護するために、システムセキュリティを設定することができます。

遠隔管理	
遠隔管理(WAN経由)	拒否 ▼
WAN側からのPing	
WAN側からのPingをブロック	有効 ▼
ポートスキャンブロック	
ポートスキャンブロック	有効 ▼
DoS攻撃(SYN flood攻撃)ブロック	
DoS攻撃(SYN flood攻撃)ブロック	有効 ▼
SPI(Stateful Packet Inspection)	
SPIファイアウォール	有効 ▼

3. ルーター設定画面

3-12 コンテンツフィルタ

不適切なWebサイトへのアクセスを制限することができます。

1) Webコンテンツフィルタ

入力項目	内容
Proxy	チェックを追加すると、HTTP Proxyを利用したサイトにアクセスできなくなります。
JavaScript	チェックを追加すると、JavaScriptで別ページをロードするようなサイトが動作しなくなります。
ActiveX	チェックを追加すると、ActiveXを利用したページが動作しなくなります。

2) URLフィルタセッティング

アクセスを禁止したいURLを設定します。URL(ドメイン部及びそれ以降)を設定すると、そのURLにアクセスできなくなります。

3) Webホストフィルタ設定

アクセスを禁止したいURLを設定します。任意のURL(ドメイン部)を設定すると、そのURLにアクセスできなくなります。

コンテンツフィルタの設定

不適切なWebサイトへのアクセスを制限することができます。

Webコンテンツフィルタ	
フィルタ	<input type="checkbox"/> Proxy <input type="checkbox"/> JavaScript <input type="checkbox"/> ActiveX
<input type="button" value="適用"/> <input type="button" value="リセット"/>	

URLフィルタセッティング

設定済みURLフィルタ	
No.	URL
<input type="button" value="削除"/> <input type="button" value="リセット"/>	

URLフィルタの追加	
URL:	<input type="text"/>
<input type="button" value="追加"/> <input type="button" value="リセット"/>	

Webホストフィルタ設定

設定済みWebホストフィルタ	
No.	ホスト(キーワード)
<input type="button" value="削除"/> <input type="button" value="リセット"/>	

ホスト(キーワード)の追加	
キーワード	<input type="text"/>
<input type="button" value="追加"/> <input type="button" value="リセット"/>	

3. ルーター設定画面


3-13 ポートフォワード

登録した仮想サーバへのアクセスを、ローカルネットワーク内の特定機器に転送します。

入力項目	内容
ポートフォワード設定	ルーターWAN側に着信した通信をLAN側に転送する場合は有効を選択してください。
IPアドレス	転送先のLAN内IPアドレスを入力してください。
ポート番号の範囲	転送する通信のルータWAN側着信ポートを入力してください。
プロトコル	転送するプロトコルを選択してください。
コメント	この設定に対するコメントを入力してください。

ポートフォワード設定

登録した仮想サーバへのアクセスを、ローカルネットワーク内の特定機器に転送します。

ポートフォワード設定 	
ポートフォワード設定	無効 ▼
IPアドレス	<input type="text"/>
ポート番号の範囲	<input type="text"/> - <input type="text"/>
プロトコル	TCP&UDP ▼
コメント	<input type="text"/>

(登録できる最大設定数: 32.)

適用

リセット

現在のポートフォワード設定

No.	IPアドレス	ポート番号の範囲	プロトコル	コメント

選択項目の削除

リセット

3. ルーター設定画面


3-14 ポートトリガー

ポートトリガーは LAN側から指定ポートへアクセスする際にのみ、WAN側の着信ポートを開きます。

入力項目	内容
ポートトリガー設定	LAN側機器からのアクセスに応じ、WAN側からLAN側機器の待ち受けポートへ通信を転送する必要がある場合は有効を選択してください。
トリガーポートのプロトコル	転送条件となるLAN側機器から外部へのアクセスに用いるプロトコルを選択してください。
トリガーポート	転送条件となるLAN側機器から外部へのアクセスに用いるポート番号を選択してください。
着信ポートのプロトコル	転送条件に合致した場合、WAN側からLAN側機器へ転送すべきプロトコルを選択してください。
着信ポート	転送条件に合致した場合、WAN側からLAN側機器へ転送すべきポートを選択してください。
コメント	この設定に対するコメントを入力してください※省略可。

ポートトリガー設定

ポートトリガーは LAN側から指定ポートへアクセスする際にのみ、WAN側の着信ポートを開きます。

ポートトリガー設定 	
ポートトリガー設定	<input type="text" value="無効"/>
トリガーポートのプロトコル	<input type="text" value="TCP"/>
トリガーポート	<input type="text"/>
着信ポートのプロトコル	<input type="text" value="TCP"/>
着信ポート	<input type="text"/>
コメント	<input type="text"/>

(登録できる最大設定数: 32.)

現在のポートトリガー設定					
No.	トリガーポートのプロトコル	トリガーポート	着信ポートのプロトコル	着信ポート	コメント

3. ルーター設定画面

3-15 DMZ

DMZ設定をすることでLAN上の1台の機器をインターネット側からアクセスできるようにします。

入力項目	内容
DMZ設定	WAN側へ着信した転送先の不明なパケットについてLAN側機器へ転送する場合は有効を選択してください。
DMZ IPアドレス	転送先のLAN側機器IPアドレスを入力してください。
TCP ポート80を除く	WAN側TCPプロトコル80番ポートへのアクセスを転送しない場合にはチェックを有効にしてください。

DMZ設定

DMZ設定をすることでLAN上の1台の機器をインターネット側からアクセスできるようにします。

DMZ設定 	
DMZ設定	無効 <input type="button" value="v"/>
DMZ IPアドレス	<input type="text"/>

TCP ポート80を除く

3. ルーター設定画面

3-16 管理

管理者アカウントとパスワード、NTP設定を変更できます。

1) Webコンテンツフィルタ

入力項目	内容
アカウント	本管理画面にログインする際に用いるIDを入力してください。
パスワード	本管理画面にログインする際に用いるIDに対応するパスワードを入力してください。
ウォッチドッグ	機器が異常動作をした際にリセットを自動的に行うようにする場合は有効を選択してください。

2) NTP設定

入力項目	内容
アカウント	本管理画面にログインする際に用いるIDを入力してください。
パスワード	本管理画面にログインする際に用いるIDに対応するパスワードを入力してください。
ウォッチドッグ	機器が異常動作をした際にリセットを自動的に行うようにする場合は有効を選択してください。

システム管理

管理者アカウントとパスワード、NTP設定を変更できます。

管理者設定 	
アカウント	<input type="text" value="admin"/>
パスワード	<input type="password" value="●●●●●●"/>
ウォッチドッグ	<input checked="" type="checkbox" value="有効"/>

適用

キャンセル

NTP設定 	
現在時刻	<input type="text" value="Thu Jan 1 09:07:12 GMT 19"/> <input type="button" value="ホストと同期"/>
タイムゾーン	<input type="text" value="(GMT+09:00) Japan, Korea"/> ▼
NTPサーバー	<input type="text" value="ntp.nict.jp"/>

適用

キャンセル

3. ルーター設定画面

3-17 ファームウェア更新


最新の機能をご利用いただくためにファームウェアのアップデートを行ってください。

更新には1分ほどかかります。その間は電源を切ったりしないでください。正常な動作をしなくなる恐れがあります。

入力項目	内容
更新開始	インターネット上のファームウェアを用いて更新する場合は押してください。
ファイルを選択	接続しているPCから更新する場合は、ファームウェアファイルを選択してください。
自動アップデート	有効に設定しておく、最新版ファームウェアが公開された時に自動でアップデートします。

ファームウェアアップデート

最新の機能をご利用いただくためにファームウェアのアップデートを行ってください。
更新には1分ほどかかります。その間は電源を切ったりしないでください。正常な動作をしなくなる恐れがあります。

ファームウェアバージョン 	
現在	v1.08
最新	can not be acquired <input type="button" value="更新開始"/>
ローカルファームウェアアップデート	
場所	<input type="text"/> <input type="button" value="参照..."/> <input type="button" value="適用"/>
自動アップデート	
有効	<input type="button" value="有効"/> <input type="button" value="適用"/>

3. ルーター設定画面

3-18 設定管理

設定を保存/復元、設定の初期化をすることができます。

入力項目	内容
設定の保存	現在の設定情報をローカルPCに保存する場合に押します。
設定の読み込み	ローカルPCに保存された設定情報を読み込む場合に、ファイル名を指定し、[読み込み]ボタンを押します。
設定の初期化	全ての設定を工場出荷時に戻す場合に[初期化]ボタンを押します。

設定管理

設定を保存/復元したり、設定の初期化をすることができます。

設定の保存	
保存ボタン	<input type="button" value="保存"/>

設定の読み込み	
設定ファイルの場所	<input type="text"/> <input type="button" value="参照..."/>
<input type="button" value="読み込み"/> <input type="button" value="キャンセル"/>	

設定の初期化	
初期化ボタン	<input type="button" value="初期化する"/>

3. ルーター設定画面

3-19 再起動

本製品を再起動する場合、[再起動]ボタンを押します。

再起動

再起動

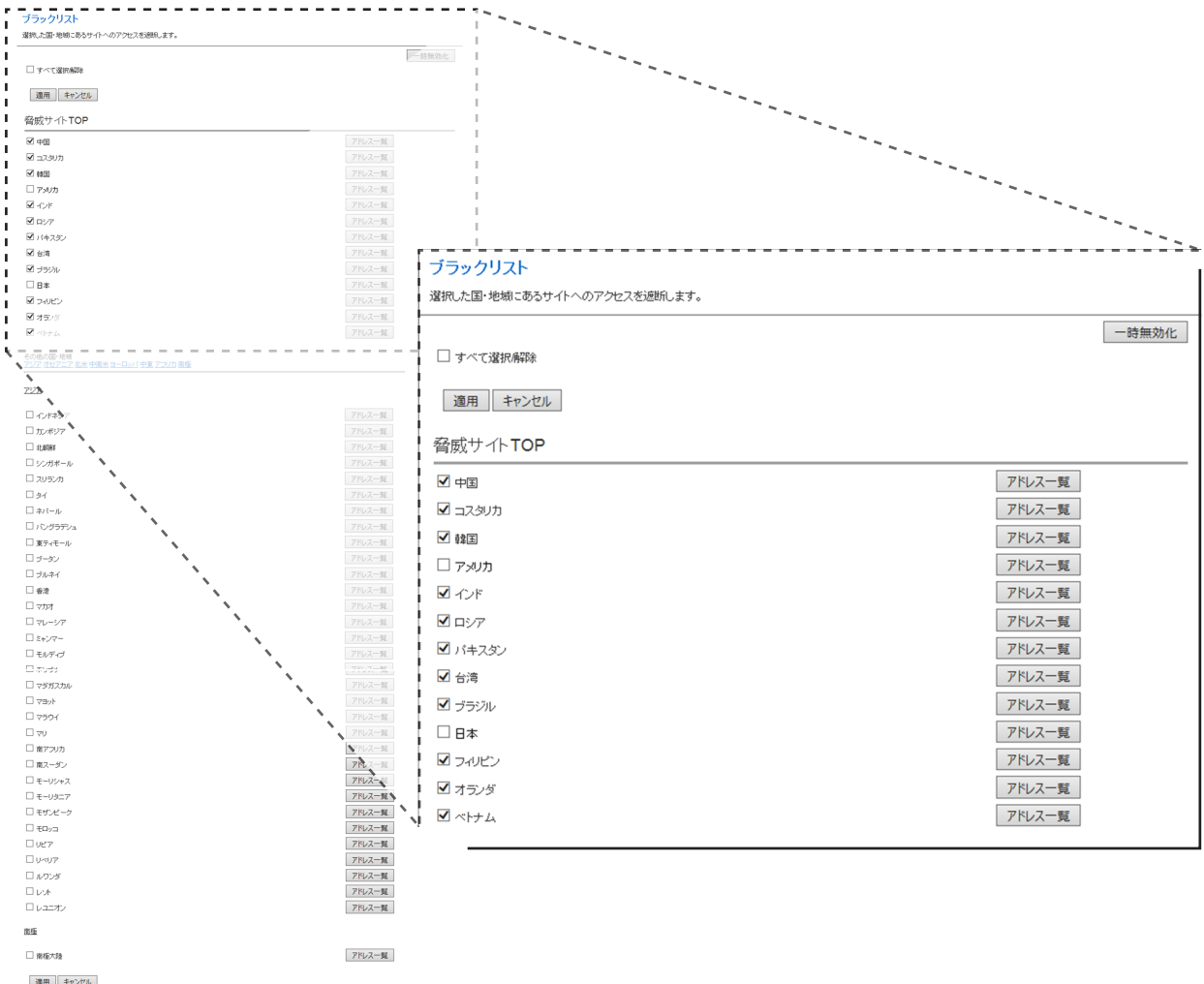
4. ルーター設定画面

4-1 ブラックリスト

選択した国・地域にあるサイトへのアクセスを遮断します。

入力項目	内容
一時無効化	鎖国機能を一時的に無効化します。無効化する時間を、3分、15分、60分より選択してください。
国・地域の選択	アクセスを遮断する国・地域を選択します。

遮断したい国・地域にチェックを入れ、[適用]ボタンを押して下さい。「脅威サイトTOP」は国立研究開発法人 情報通信研究機構(NICT)が公開しているデータを元に設定しており(※)、工場出荷時は「日本」と「アメリカ」以外を遮断する設定です。必要に応じて遮断設定を変更してください。
 ※: NICTはダークネット(インターネット上で等卓可能な未使用IPアドレス空間)のトラフィックを監視することでサイバー攻撃の状況を把握しようとしており、国別のホスト数やパケット数も公開しています。これらのランキングで上位の国・地域を危険と考え、「脅威サイトTOP」として設定しています。NICTのリストは毎日変化するので、ご購入された時期によって設定画面上の「脅威サイトTOP」とNICTのリストが一致しないことがあります。



4. ルーター設定画面

4-2 ホワイトリスト

通信を許可するIPアドレス/ホスト名を設定します。ホワイトリストに設定されたIPアドレス/ホスト名は例えばブラックリストで設定された国・地域の中であったとしてもアクセスを許可します。

1) ホワイトリストの追加/削除

入力項目	内容
IPアドレスまたはホスト名	鎖国機能を一時的に無効化します。無効化する時間を、3分、15分、
コメント	60分より選択してください。
ホワイトリスト以外をすべて遮断する	アクセスを遮断する国・地域を選択します。

2) バックアップ

登録したホワイトリストのバックアップを行うことができます。

3) リストア

ローカルで作成したホワイトリストや弊社の提供するホワイトリストをアップロードすることができます。

ホワイトリスト

一時無効化

ホワイトリスト追加/削除

IPアドレスまたはホスト名 コメント

IPアドレスは範囲指定もできます。(例: 1.0.0.0-1.0.3.255)

ホスト名にはワイルドカード指定もできます。(例: *.abc.com、abc.*)

ホワイトリスト以外をすべて遮断する

ホワイトリスト一覧

	アドレス	コメント	選択
ページ:			

バックアップ

ホワイトリストをファイルに保存

リストア

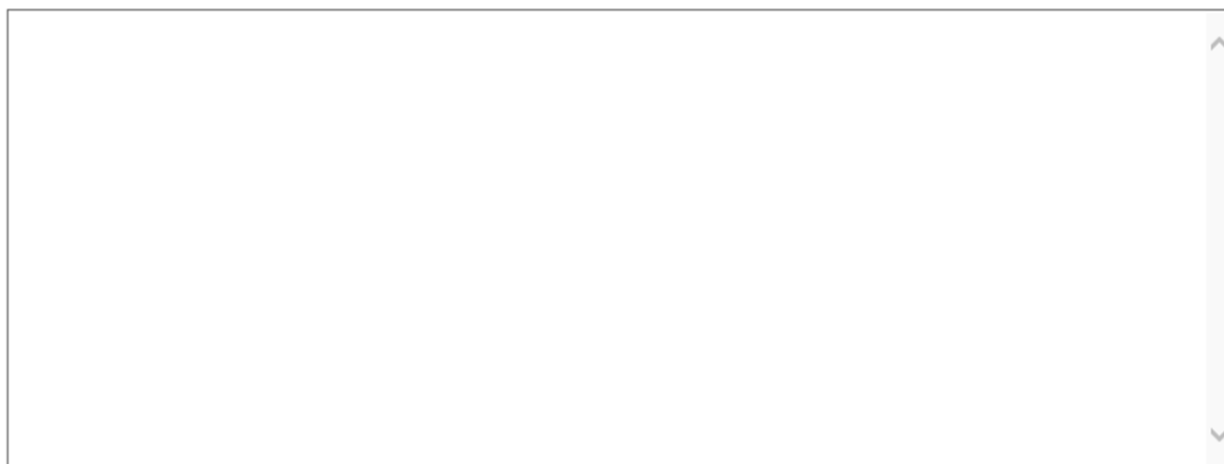
ホワイトリストをファイルから読み込み

4. ルーター設定画面

4-3 遮断ログ

遮断ログの表示とファイル出力、syslogサーバへの転送設定が行えます。

遮断ログ



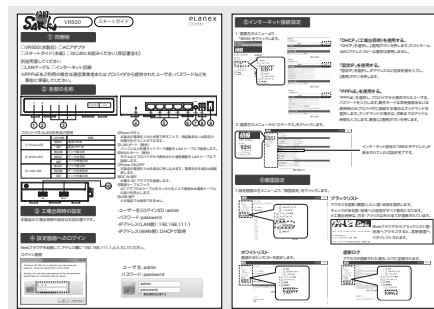
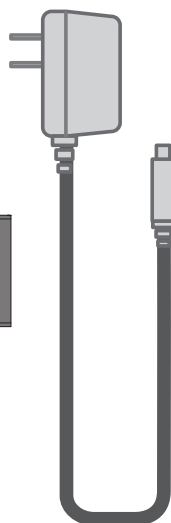
Syslogサーバ

syslogサーバのIPアドレスまたはホスト名

5. 同梱物

5-1 同梱物リスト

同梱物	数量
VR500 (本製品)	1
ACアダプタ	1
設定ガイド (保証書を含む)	1

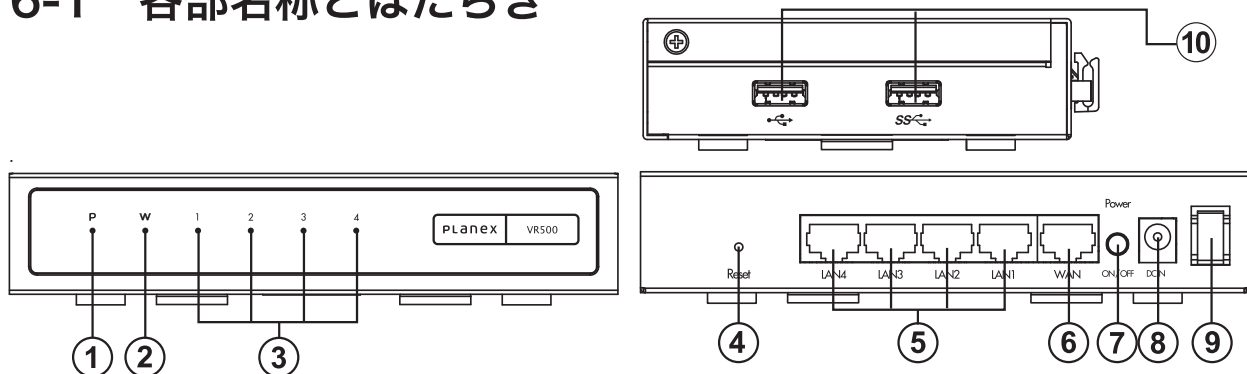


5-2 別途ご用意いただくもの

LANケーブル

6. 製品本体

6-1 各部名称とはたらき



フロントパネルLED名称及び説明

	LED状態	説明
① PowerLED	緑点灯	電源 ON 時
	消灯	電源 OFF 時
② WAN LED	緑点滅	リンク確立時
	緑点灯	データ送受信
	消灯	リンク未確立時
③ LAN LED	緑点灯	リンク確立時
	緑点滅	データ送受信時
	消灯	リンク未確立時

④Reset ボタン

本製品の電源を入れた状態で押すことで、再起動あるいは設定の初期化を行うことができます。

⑤LAN ポート (黄色)

パソコンなど各種ネットワーク機器を LAN ケーブルで接続します。

⑥WAN ポート (青色)

モデムなどプロバイダから提供された通信機器を LAN ケーブルで接続します。

⑦Power ON/OFF

本製品の電源を入れる場合に押し込みます。電源を切る場合は再度押します。

⑧DC IN 端子

付属の AC アダプタを接続します。

⑨電源ケーブルフック

AC アダプタのケーブルをひっかけることで意図せぬ電源ケーブルの抜けを防止します。

⑩USB 端子

※本製品では使用できません。

7. 工場出荷時設定

7-1 本製品の工場出荷時の設定内容は以下のとおりです。

ユーザ名 (ログインID)	admin
パスワード	password
IPアドレス	192.168.111.1 ただし、上位ルーターが192.168.111.1の場合、 192.168.110.1へ自動変更されます。