PLANEX COMM.





本体操作ガイド



1 使用方法
1-1 接続する・ pl
2 接続~設定画面
2-1 端末と接続して設定画面を開く····································
3 ルーター設定画面
3-1 言語選択······p3
<u>3-2 ステータス・・・・・ p4</u>
3-3 統計 ·······p5
<u>3-4 DHCPクライアント ·····・ p6</u>
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
3-7 LAN ······ p11
3-8 DHCP
<u>3-9 VPN パススルー ······p13</u>
<u>3-10 MAC/IP/ポートフィルタ · p14</u>
<u>3-11 システムセキュリティ ······ p15</u>
3-12 コンテンツフィルタ · p16
3-13 ポートフォワード · p17
<u>3-14 ポートトリガー ·p18</u>
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 · · · · · · · · · · · · · · · · · · ·
5-2 別途ご用意いただくもの・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
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 設定值 ······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
 - 本製品の「LAN」(黄)ポートとPCをLANケーブルで 接続します。



本製品

- 2) ブラウザを起動します。
- 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。
- 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。

3-1 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。

	L1/home.shtml ♀ ℃ 遵 VR500 ×		n ★ \$
領国		PLANEX	VR500
<u>全て開く 全て閉じる</u>	VR500		
 VR500 P → 27 - 5/3 P → 1/9 - 3/+ 設定 P → 7/7 ウォール P → 1/9 - 3/+ 設定 P → 1/9 - 3/4 P → 第四条 	言語選択 □日本語 ✔		
	ステータス 統計 管理		

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	IS COLOR PENEED	
ローカルネットワーク		
ローカルIPアドレス	192.168.111.1	
ローカルネットマスク	255.255.255.0	
MACアドレス	10 C3 C7 76 16 16	

イーサネットポートステータス





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。

у Е Л	
X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/ 竹小	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
TxØ)/ ናብት	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
P-50%-58582	101110-015	192.168.111.100	00:00:00

3-5 システムログ

システムログを表示します。

ボタン名	
リフレッシュ	最新のログを再描面します。
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
0	2 (b)(b)3 (b)(b) has seen based, (b)(a to benefit because has be (b))
0.000	1 (1/1/1/2) [Mark rear beauty] print to pressil pressure had an int [Mark 1
	1 (b) (c) (b) her set her) (b) (c) is the (c) here a line (c)
	3 (24)/22 [20] her can bend 1 [about a trank! transity her at [20]
	1 (2) (2) (2) and and here ([about a base] based here (a 20)
	1 10-11-2 Mar Mar Mart 1 10-04 In particul particular and an 15-11
	1 12 12 13 THE PROPERTY PROPERTY FOR THE
	1 TALLY THE PER PER PERS PERSON IN PERSON PERSON IN THE PERSON PERSON NEEDED
	I TATING THE PROPERTY FROM I PERSON PROPERTY FOR THE PERSON
	A TALENA THAT PER PER PERS I DAVID IN ATTEND AND THE REAL PROPERTY AND A TALENA
	I TATALA THAT PER AND PRESS TYPE IS ATTALA ANTIQUE MALLE AT THAT
	I TATA I AND TATA THE TATA I TATA
2	I TATA I TATA TATA TATA TATA AND I TATA TATA TATA I
1	I ILIA I ALL ALL ALL ALL ALL ALL ALL ALL
3	I II COLLI ALL DE CEL DECK AND I INTE I INTE I INTE I INTE I INTE I INTE
,	1 IL C. I. MILL DATA AND LODGE CONTRACT OF AND A DATA AND AND AND AND AND AND AND AND AND AN
	- In the second second based based of the second second in the second se
3	- TALL THE PARTY AND AND A CARD A CARD A CARD A CARD AND A CARD AND A CARD A CA
3	included their second second
3	in the second se
3	in the second se
3	I TOTAL THE MANAGEMENT AND A LOCAL AND AND A REAL ADDRESS.
3	I HAVE THE MAN AND AND AND A LOCAL AND AND A REAL AND A
3	a statute was seen and seen and and and the second set
J	1. Developing which preserves presents have been been been been been been been be
3	1. In 1919 St. 1980) Internating Street, and Alberty and Alberty St. International
J	1. 18-19-19 (White Sector Se
J	1. TELEVISING VERSES AND AND AND AN AND A STREAM AND
J	1. ISTOR 11. WHAT DATE COLORS AND
3	1. THE REPORT OF THE PROPERTY AND A DESCRIPTION OF THE PROPERTY AND A DESC
3	1 INTER 14 WARD DATE OVER DEPEND OF DEPENDENT OF A DATE AND A DATE.
3	I THERE WE SHOULD AND AND A AND A AND A AND A AND AND AN
0	1. TELEVIS AND
	1 INCOLULY WHAT MANAGEMENT INCOLUMN TO CONTRACT WITH
	to the set of the set
	I CONTRACT AND
-	I DEVELOP ON AN ADDRESS OF A DEVELOPMENT OF
3	I TATAL DI VALLE CARLE CARLE CARLE CARLES AND
,	I HAVE I WAR AND THE REAL IN THE REAL AND
3	I HARDER WARR CONTACT AND ADDRESS OF ADDRESS AND ADDRESS TO TANK AND ADDRESS
3	[18-34, 3] "Mail: Laws, and Lawsel", Mill, Ray & and American Statistics (
3	(18-26-20) which there using herein / Boy (M) (19-26, adding) and
J	[16-04-3] Well immunate immula + Ole moniformin unitarily - 104760
J	1 Hold 1 Well men and ments [10] we are 11 1000 1010 of 20, or 100-000 has been 1
J	[10-20-2] "Bibli Iman, and Imanally support, for Sent Port in 101
3	I Hold I will be and the best live all service had show write 1.4 lasted inter
J	. Heldell Weld have the ment's is relative any registered inducts:
Jan	1 05:00.51 vR500 kern.warm kernel: kalink gpio driver initialized
<	>

3-6 WAN

WANの各種設定を行います。

 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 V
DHCP接続 🎬		
ホストネーム (オプション)		
масアドレスコピー 🎬		
有効		無効 ∨
		適用 キャンセル

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 ▼
固定叩接続 🎬	
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サーバ	192.168.1.20
セカンダリDNSサーバ	192.168.1.22
мсアドレスコピー <mark>*</mark> *	
有効	(無効 ∨)

3-6 WAN

WANの各種設定を行います。

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。

入力店日	山、
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:	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。
アイドル時間 [分]	※省略可

WAN設定

WANの各種設定を行います。

接続方式:	PPPoE V	
PPPoE接続 🎬		
ユーザ名	pppoe_user	
バスワード	•••••	
バスワードの確認	•••••	
動作モード	常時接続 🗸	
	On demand Mode: Idle Time 5 minutes	
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	
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。

3-7 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	
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。

lanete 🎬	
ホストネーム (オブション)	VR500
IPアドレス	192.168.111.1
サブネットマスク	255.255.255.0
MACアドレス	
DHCPタイプ	サーバ・
開始IPアドレス	192.168.111.100
終了IPアドレス	192.168.111.200
サブネットマスク	255.255.255.0
ブライマリDNSサーバ	192.168.111.1
セカンダリDNSサーバ	
デフォルトゲートウェイ	192.168.111.1
リース時間	86400
802.1d スパニングツリー	無効 ∨

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		
	追加 選択項目の削除 リセット	x		

[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	
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
	人力してくたさい。

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 🎬			
MAC7FUZ			
IPアドレス			

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	
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のバ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 ~)	

3-10 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	(無効 ∨)	
標準方針:ルールに沿わないパケットの通過を	許可しない 🗸	

適用 リセット

MAC/IP/ボート フィルク感定 🎇							
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	None V						
宛先ボート番号の範囲							
送信元ポート番号の範囲	- ト番号の範囲						
動作		許可 🗸]				
登録できる最大設定数: 32.) 適用 リセット							
設定済みフィルタ							
No. 送信元MACアドレス 宛	時IPアドレス	送信元IPアドレス	プロトコル	宛先ボート番号の範囲	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 -							
	違択項目の削除 リセット						

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事ができます。

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	無効:WAN側からのPingに応答します。
Pingをブロック	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事ができます。

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 🗸		
ポートスキャンプロック			
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ファイアーウォール	有効 🗸		
		適用 リセット	

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、JavaScrip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	Proxy JavaScript ActiveX
	適用 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
	削除 リセット
URLフィルタの追加	
URL:	
	追加リセット
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)
	削除 リセット
ホスト(キーワード)の追加	
キーワード	
	追加リセット

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	
ポート番号の範囲	
プロトコル	TCP&UDP V
(登録できる最大設定数・32)	

永じさる菆八該定殿: 32.)

リセット 適用

現在のボ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	אטא⊏
		選択項目の削除 リセット		

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	無効 ∨
トリガーボートのプロトコル	TCP V
トリガーポート	
着信ボートのプロトコル	TCP V
着信ボート	
(登録できる最大設定数: 32.)	
	適用 リセット

現在のオ	ペートトリガー設定				
No.	トリガーポートのプロトコル	トリガーポート	著信ポートのプロトコル	著信ポート	

選択項目の削除 リセット

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 ~
DMZ IPアドレス	

TCP ポート80を除く

適用 リセット

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バスワード、NTP設定を変更できます。

管理者設定 ү			
アカウント	admin]	
パスワード	•••••		
ウォッチドッグ	「有効 ✔		
5455155			

キャンセル

適用

NTP設定 🍟	
現在時刻	Thu Jan 1 09:07:12 GMT 19 ホストと同期
タイムゾーン	(GMT+09:00) Japan, Korea
NTPサーバー	ntp.nict.jp
	適用 キャンセル

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と、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 ү			
現在	v1.08		
最新	can not be acquired 更新開始		
ローカルファームウェアアップデート			
場所	参照 適用		
自動アッフテテート			
有効	「有効 ∨」 適用		

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	保存

設定の読み込み	
設定ファイルの場所	参照
	読み込み キャンセル

設定の初期化	
初期化ポタン	初期化する

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

4-1 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。



4-2 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	アクセスを遮断する国・地域を選択します。
すべて遮断する	

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出来ます。

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。

不	ワイ	トリ	マト	

ホワイトリスト追加/削除 IPアドレスまたはホスト名 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、 コーホワイトリスト以外をすべて遮断する	コメント abc.*)	
適用」「キャンセル」		
ホワイトリスト一覧 アドレス	⊐℃ト	選択
ページ:	すべて削除 キャンセル	
バックアップ ホワイトリストをファイルに保存 保存		
リストア ホワイトリストをファイルから読み込み アップロード	参照	

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

		^
		~
	更新 クリア 遮断ログをファイルに保存 簡易ログ表示 抽出ログ表示	
Syslogサーバー		

syslogサーバーのIPアドレスまたはホスト名		適用	Ħ

5. 同梱物

5-1 同梱物リスト

 同梱物 VR500(本製品) ACアダプタ 設定ガイド(保証書を含む) 	数量 1 1 1	
P W 1 2 3 4	PLanex VR500	<image/> <text></text>

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。