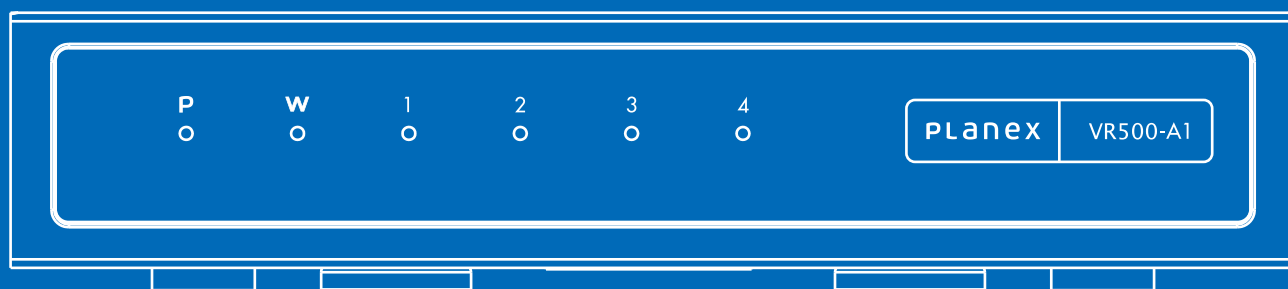


Planex COMM.

VPNルーター
ギガビット対応
有線タイプ

VR500-A1



本体操作ガイド

ユーザーズマニュアル

目次

1 設置

1-1 本体各部のはたらき	P1
1-2 接続方法	P2

2 本製品へのログイン

3 ステータス

3-1 ステータス	P6
3-2 統計	P8
3-3 DHCPクライアント	P9
3-4 システムログ	P10

4 インターネット設定

4-1 WAN	P11
4-2 LAN	P13
4-3 スタティックDHCP	P15
4-4 tagVLAN	P16
4-5 ポートVLAN	P19
4-6 VPNパススルー	P20
4-7 NAT	P21
4-8 ルーティング	P22
4-9 QoS	P25

5 ファイアウォール

5-1 MAC/IP/ポートフィルタ	P28
5-2 システムセキュリティ	P31
5-3 コンテンツフィルタ	P32
5-4 ポートフォワード	P34
5-5 ポートトリガー	P36
5-6 DMZ	P38

6 VPN

6-1 PPTP	P39
6-2 L2TP	P41
6-3 IPSec	P43

7 管理

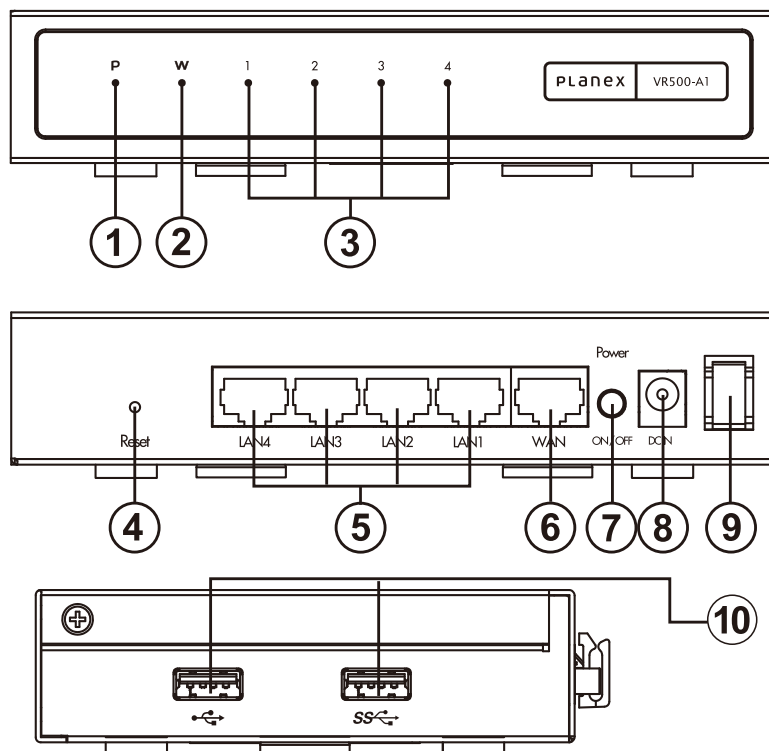
7-1 システム管理	P47
7-2 DDNS	P48
7-3 ファームウェア更新	P49
7-4 設定管理	P51
7-5 SNMP	P52
7-6 Syslog	P54
7-7 再起動	P55

8 仕様 (スペック表)

9 参考情報 (スマートフォンでの操作方法)

1. 設置

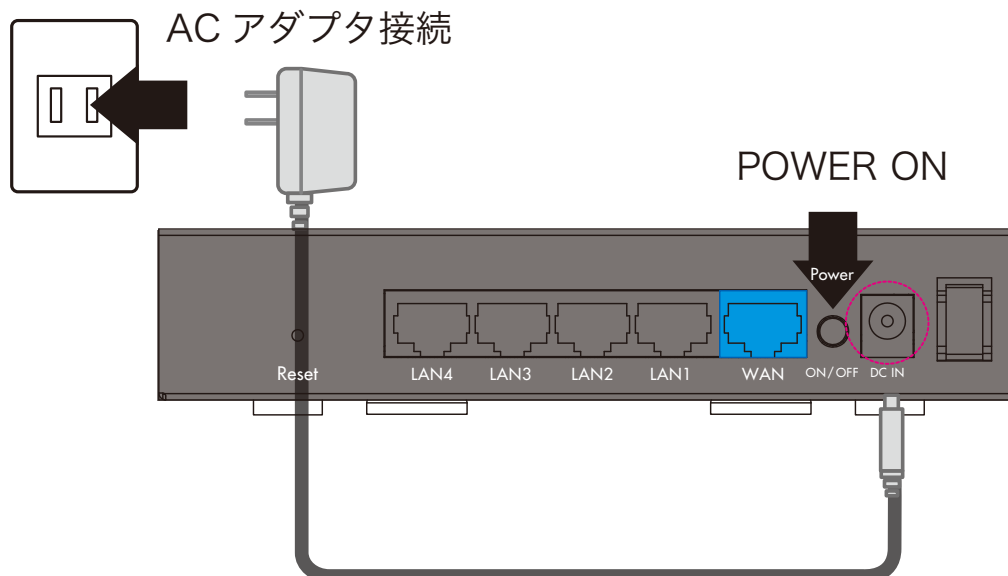
1.1 本体各部のはたらき



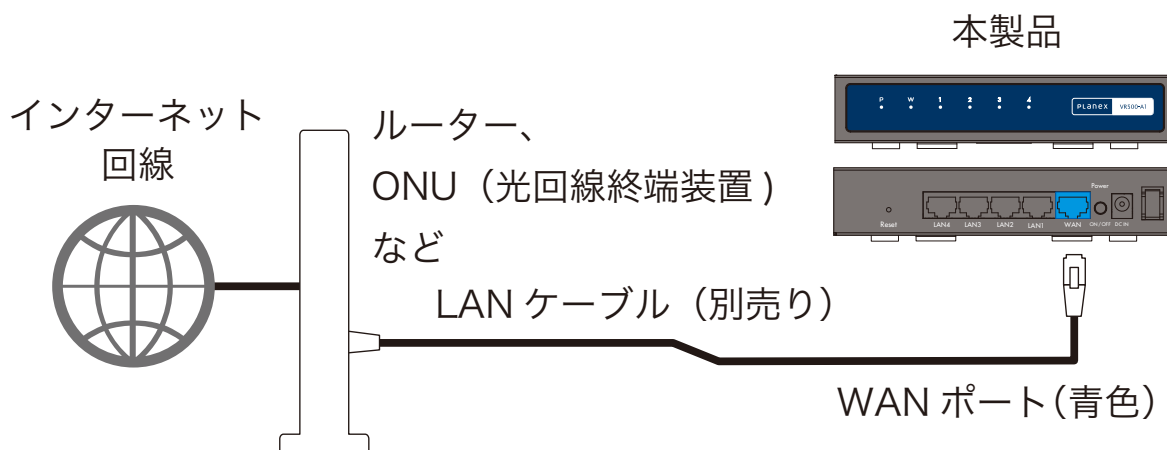
フロントパネルLED名称及び説明

	LED状態	説明
① Power LED	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スイッチ	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。	

1.2 接続方法



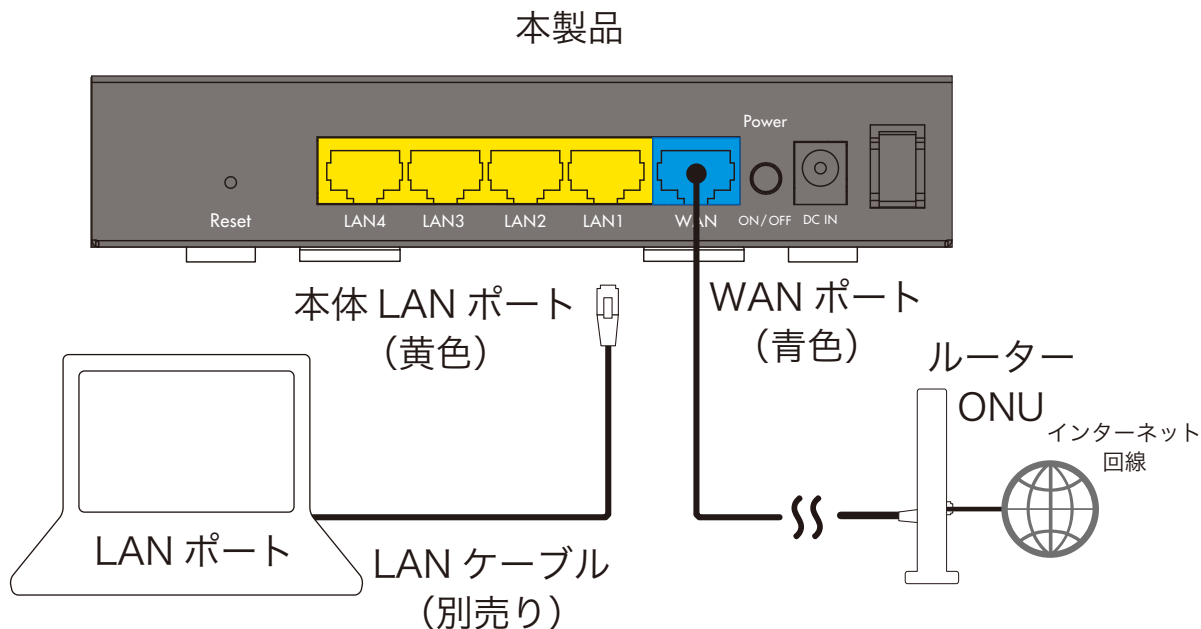
- ①まず本体のACアダプタ部をコンセントに差し込みDCジャックを本体に接続します。
- ②その後本体Powerスイッチを押し込み、電源を入れます。



- ③次に本体のWANポートと上位ネットワーク(ISPなどからもらい受けた通信機器)に接続します。この際上位にルータが接続されている場合、本製品のVPNサーバ機能が、正常に動作しない場合がございます。上位ルータにてポートフォワードを設定するなど設置環境をよく確認してください。

2. 製品へのログイン

- ①本製品の設定を変更する場合は設定用の有線LANに対応したPCとウェブブラウジング機能のあるソフトウェアが必要です。



- ②PCを本体のLANポートと接続します。
- ③ブラウザを起動します。
- ④ブラウザのURL入力部分にhttp://192.168.111.1と入力しアクセスします。
- ⑤認証画面が表示されID/パスワードの問い合わせが表示されます。

このページを見るには、192.168.111.1:80にログインする必要があります。

パスワードは暗号化されずに送信されます。

名前:

パスワード:

このパスワードをキーチェーンに保存

キャンセル ログイン

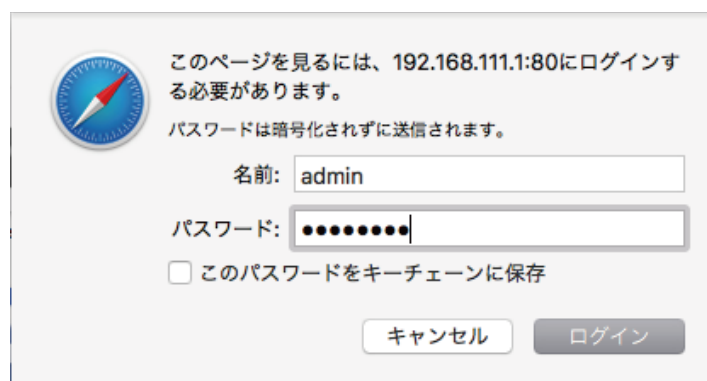
本製品の初期値は以下の通りです。

入力後[OK]ボタン(※ブラウザによって異なります)をクリックします。

初期値

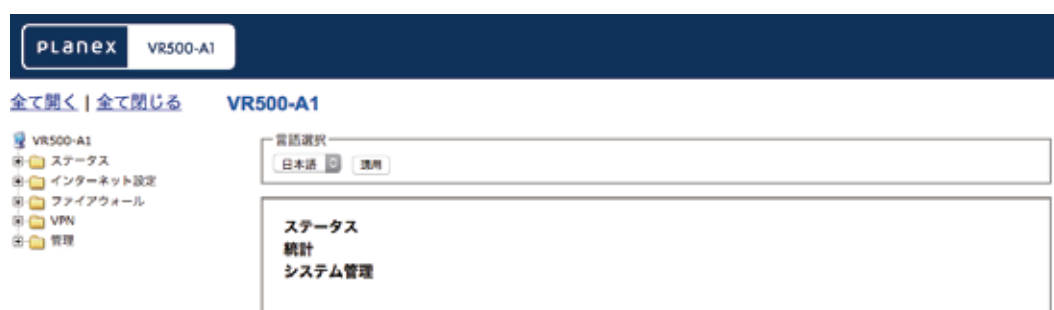
ID : admin

パスワード : password



The image shows a login interface for the VR500-A1 device. It features a blue circular logo with a compass needle on the left. The text reads: 'このページを見るには、192.168.111.1:80にログインする必要があります。' (To view this page, you need to log in to 192.168.111.1:80). Below this, it states 'パスワードは暗号化されずに送信されます。' (The password is transmitted without encryption). There are two input fields: '名前:' (Name) with the value 'admin' and 'パスワード:' (Password) with ten dots. A checkbox labeled 'このパスワードをキーチェーンに保存' (Save this password in the keychain) is present. At the bottom, there are two buttons: 'キャンセル' (Cancel) and 'ログイン' (Login).

⑥設定画面が表示されます。



画面上には左側に各設定項目のツリーメニューが表示されています。各設定項目について設定を行う際はメニューよりクリックしてください。右側に対応する設定ページが表示されます。



またメニューを選択する以前の状態では右側に言語切り替え(日本語/英語)並びにステータス、統計、システム管理へのショートカットが表示されております。言語を切り替える際はこのページにて切り替えを行ってください。このページを再度表示するにはメニュー最上部VR500-A1をクリックしてください。

3. ステータス

3.1 ステータス

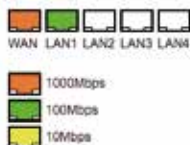
ステータスでは本製品の各種情報が確認できます。

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	v1.01 (Oct 26 2016)
システム稼働時間	XX hours, XX mins, XX secs
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	XX.XX.XX.XX
サブネットマスク	XX.XX.XX.XX
デフォルトゲートウェイ	XX.XX.XX.XX
プライマリDNS	XX.XX.XX.XX
セカンダリDNS	XX.XX.XX.XX
MACアドレス	00:22:CF:XX:XX:XX
ローカルネットワーク	
ローカルIPアドレス	YY.YY.YY.YY
ローカルサブネットマスク	YY.YY.YY.YY
MACアドレス	00:22:CF:YY:YY:YY

イーサネットポートステータス



システム情報・説明

ファームウェアバージョン

・現在動作しているファームウェアバージョンが表示されます。

システム稼働時間

・システムが動作してからの稼働時間を表示しています。

動作モード

・現在の動作モードが表示されています。

※本製品では”Gateway Mode”以外はございません。

インターネット設定・説明

接続タイプ

・WAN接続タイプが表示されています。

WAN IPアドレス

・WANインタフェースに割り当てられているIPv4アドレスが表示されています。

サブネットマスク

・WANインタフェースに接続されているネットワークのサブネットマスクが表示されています。

デフォルトゲートウェイ

- ・WANインタフェースに接続されているネットワークのデフォルトゲートウェイが表示されています。

プライマリDNS

- ・本製品がDNSリレーもしくは本製品自身が名前解決する際に使用するプライマリDNSが表示されています。

セカンダリDNS

- ・本製品がDNSリレーもしくは本製品自身が名前解決する際に使用するセカンダリDNSが表示されています。

MACアドレス

- ・WANインタフェースに設定されているMACアドレスが表示されます。

ローカルネットワーク・説明

ローカル IP アドレス

- ・LAN(vlan1)のネットワークにおける本機器のIPアドレスが表示されます。

ローカルサブネットマスク

- ・LAN(vlan1)のネットワークのサブネットマスクが表示されています。

MACアドレス

- ・LAN(vlan1)に設定されているMACアドレスが表示されます。

イーサネットポートステータス・説明

WAN,LAN1-4

- ・ポートのリンク速度およびアップリンクについて表示されています。

※概要

白:未接続(リンクダウン)

橙:1000Mbpsにてリンクアップ

緑:1000Mbpsにてリンクアップ

黄:10Mbpsにてリンクアップ

3.2 統計

統計では本製品の各種カウンタの現在の取得値(起動時からのカウント)が表示されます。再度表示させることで最新の情報に更新されます。

統計

統計を参照します。

メモリ	
メモリ合計	254472 kB
メモリ残量	214112 kB
WAN/LAN	
WAN受信パケット	3418809
WAN受信バイト	824637321
WAN送信パケット	38757781
WAN送信バイト	316077308
LAN受信パケット	34128204
LAN受信バイト	44752117904
LAN送信パケット	4768133
LAN送信バイト	397706164
全インターフェース	
インターフェース名	01
受信パケット	143
受信バイト	20954
送信パケット	143
送信バイト	20954
インターフェース名	#02
受信パケット	34128239
受信バイト	2285244490

メモリ・説明

メモリ合計

・システムで認識されているメモリ合計容量が表示されます。

メモリ残量

・システムで認識されているメモリ空き容量が表示されます。

WAN/LAN・説明

[WAN/LAN][受信/送信]パケット

・[WAN/LAN]インタフェースから[受信/送信]されたパケットのカウント値が表示されます。

[WAN/LAN][受信/送信]バイト

・[WAN/LAN]インタフェースから[受信/送信]されたバイトのカウント値が表示されます。

全インタフェース・説明

インタフェース名

・該当する内部インタフェース名が列挙・表示されます。

[受信/送信]パケット

・インタフェースから[受信/送信]されたパケットのカウント値が表示されます。

[受信/送信]バイト

・インタフェースから[受信/送信]されたバイトのカウント値が表示されます。

3.3 DHCPクライアント

本製品のDHCPサーバ機能が有効な場合、サーバより配布したIPv4アドレスおよびMACアドレスが表示されます。

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	MACアドレス	IPアドレス	リース残り時間
testmachine	00:22:CF:XX:XX:XX	192.168.111.100	23:38:57

DHCPクライアント・説明

ホストネーム

・DHCPクライアント機器から通知された機器のホストネーム情報を表示します。

MACアドレス

・DHCPクライアント機器のMACアドレスを表示します。

IPアドレス

・DHCPクライアント機器に割り当てたIPアドレスを表示します。

リース残り時間

・DHCPクライアント機器に割り当てたIPアドレスの残り有効期間を表示します。

※時:分:秒のフォーマットです。

3.4 システムログ

本製品のシステムログを表示します。問題解決の参考にしてください。

なお、ログの内容についてはサポートおよび案内しておりません。

あらかじめご了承ください。



システムログ・説明

リフレッシュ

・最新のログを表示します。

クリア

・現在のログキャッシュを消去します。

システムログ

・ログ内容が表示されます。

4. インターネット設定

4.1 WAN

WAN回線に応じ、インターネット接続設定を行うことができます。

WAN設定・説明

接続方式 固定IP/DHCP/PPPoEより選択

- ・接続方式を選択することができます。

初期値:DHCP

固定IP(接続方式にて固定IP選択時、表示)・説明

IPアドレス

- ・WANインタフェースに割り当てるIPv4アドレスを入力してください。

サブネットマスク

- ・WANインタフェースに接続するネットワークのサブネットマスクを入力してください。

デフォルトゲートウェイ

- ・WANインタフェースに接続するネットワークのデフォルトゲートウェイを入力してください。

プライマリDNSサーバ

- ・本製品がDNSリレーもしくは本製品自身が名前解決する際に使用するプライマリDNSを入力してください。

セカンダリDNSサーバ(オプション)

- ・本製品がDNSリレーもしくは本製品自身が名前解決する際に使用するセカンダリDNSを入力してください。(※省略可)

DHCP(接続方式にてDHCP選択時、表示)・説明

ホストネーム(オプション)

- ・DHCPサーバに通知するホストネームを入力してください。(※省略可)

PPPoE(接続方式にてPPPoE選択時、表示)・説明

ユーザ名

- ・ISPなど契約している接続サービスに記載されたユーザ名(例: xxxxx@example.co.jp)を入力してください。

パスワード

・ユーザ名に対応したパスワードを入力してください。

パスワードの確認

・入力内容を確認するため、再度入力してください。

動作モード

常時接続/オンデマンドより選択。

オンデマンド選択時、切断時間入力可。

・接続する際に接続を継続する(常時接続)か無通信状態の期間経過後切断する(オンデマンド)かを選択してください。オンデマンド選択時は切断時間を入力してください。

初期値:常時接続

MACアドレスコピー・説明

有効 無効/有効より選択

・WANインタフェースのMACアドレスを任意のものに変更できます。

本機能を利用する場合は有効を選択してください。

MACアドレス(有効選択時、表示)

・利用したいMACアドレス(例: aa:bb:cc:dd:ee:ff)を入力してください。

また”このPCのMACアドレスをコピー”ボタンをクリックすると自動的にお使いのPCのMACアドレスが入力されます。

入力後、適用ボタンをクリックすると設定が反映されます。

キャンセルボタンをクリックすると現在の設定値が再度読み込まれます。

4.2 LAN

LANネットワークの設定ができます。また本製品はDHCPサーバ機能を搭載し、設定を行うことができます。

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)	VR500-A1
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	00:22:CF:XX:XX:XX
DHCPサーバ有効/無効	有効 <input checked="" type="checkbox"/>
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
プライマリDNSサーバ	192.168.111.1
セカンダリDNSサーバ (オプション)	
デフォルトゲートウェイ	192.168.111.1
リース時間	86400 (1-259200)
802.1d スパニングツリー	無効 <input type="checkbox"/>

適用 キャンセル

LAN設定・説明

ホストネーム(オプション)

- ・LANネットワーク内より問い合わせがあった場合に応答するホストネームを入力してください。またこの設定値はシステムログにおいても利用されます。(※省略可)

IPアドレス

- ・LAN(vlan1)のネットワークにおける本製品のIPアドレスを入力してください。

初期値:192.168.111.1

サブネットマスク

- ・LAN(vlan1)のネットワークのサブネットマスクを入力してください。

初期値:255.255.255.0

MACアドレス

- ・LAN(vlan1)に設定されているMACアドレスが表示されます。

DHCPサーバ有効/無効 有効/無効より選択

- ・DHCPサーバ機能を利用する場合は有効を選択してください。

初期値:有効

開始IPアドレス (DHCPサーバ有効選択時、表示)

- ・DHCPサーバより配布するIPアドレスの開始アドレスを入力してください。

初期値:192.168.111.100

終了IPアドレス (DHCPサーバ有効選択時、表示)

- ・DHCPサーバより配布するIPアドレスの終了アドレスを入力してください。

初期値:192.168.111.200

サブネットマスク (DHCPサーバ有効選択時、表示)

- ・DHCPサーバより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。

初期値:255.255.255.0

プライマリDNSサーバ (DHCPサーバ有効選択時、表示)

- ・DHCPサーバより配布するプライマリDNSサーバのアドレスを入力してください。

初期値:192.168.111.1

セカンダリDNSサーバ(オプション) (DHCPサーバ有効選択時、表示)

- ・DHCPサーバより配布するセカンダリDNSサーバのアドレスを入力してください。(※省略可)

初期値:(空欄)

デフォルトゲートウェイ (DHCPサーバ有効選択時、表示)

- ・DHCPサーバより配布するデフォルトゲートウェイのアドレスを入力してください。

初期値:192.168.111.1

リース時間 (DHCPサーバ有効選択時、表示)

- ・DHCPサーバよりIPアドレスの有効期間を入力してください。

初期値:86400[秒]

802.1dスパニングツリー 有効/無効より選択

- ・STPによるパケット送出行う場合は有効を選択してください。

初期値:無効

入力後、適用ボタンをクリックすると設定が反映されます。

キャンセルボタンをクリックすると現在の設定値が再度読み込まれます。

LAN IPアドレス変更後は再起動に伴い、自動的にページ遷移します。もし遷移せず、設定を継続して行う場合はお手数ですが手入力していただきアクセスしてください。

4.3 スタティックDHCP

スタティックDHCPの設定ができます。MACアドレスに応じ一意のIPアドレスを割り当てることができます。



現在のスタティックDHCP設定・説明

No.

・エントリナンバーを表示します。

MACアドレス

・エントリに登録された固定のIPアドレスを割り当てるMACアドレスを表示します

IPアドレス

・エントリに登録されたMACアドレスに割り当てるIPアドレスを表示します

追加ボタンをクリックするとエントリを追加することができます。

選択項目の削除ボタンをクリックするとチェックボックスにチェックの入ったエントリを削除できます。

リセットボタンをクリックするとチェックボックスのチェックをすべて外すことができます。

追加ボタンをクリックした際に表示される画面について説明します。

スタティックDHCP設定・説明

MACアドレス

・追加するエントリの固定のIPアドレスを割り当てるMACアドレスを入力してください

IPアドレス

・追加するエントリのMACアドレスに割り当てるIPアドレスを入力してください

入力後、適用ボタンをクリックするとエントリが追加されます。

キャンセルボタンをクリックすると入力値が破棄され前の画面に遷移します。

4.4 tagVLAN

tagVLANの設定ができます。

LANネットワークをタグVLAN(IEEE802.1Q)によって分割することができます。

tagVLAN・説明

有効 有効/無効より選択

・tagVLAN利用時は有効を選択してください。

初期値:無効

tagVLAN間ルーティング

有効/無効より選択 (上項目にて有効選択時、選択可能)

・tagVLAN有効時、VLAN間にてルーティングを行う場合は有効を選択してください。

初期値:無効

入力後、適用ボタンをクリックすると設定が反映されます。

キャンセルボタンをクリックすると現在の設定値が再度読み込まれます。

現在のtagVLAN設定・説明

No.

・エントリナンバーを表示します。

VLAN ID

・エントリのVLAN IDを表示します。

名前

・VLANのインタフェース名を表示します。

IPアドレス

・インタフェースのIPアドレスを表示します。

サブネットマスク

・IPアドレスが所属するネットワークのサブネットマスクを表示します。

VLAN IDをクリックするとエントリを編集できます。

追加ボタンをクリックするとエントリを追加できます。

選択項目の削除ボタンをクリックするとチェックボックスにチェックの入ったエントリを削除できます。リセットボタンをクリックするとチェックボックスのチェックをすべて外すことができます。

追加ボタンをクリックした際に表示される画面について説明します。

tagVLAN詳細設定

tagVLANの詳細設定を行うことができます。

tagVLAN	
VLAN ID	<input type="text"/>
名前	<input type="text"/>
IPアドレス	<input type="text"/>
サブネットマスク	<input type="text"/>
ポートメンバー	<input type="checkbox"/> LAN1 <input type="checkbox"/> LAN2 <input type="checkbox"/> LAN3 <input type="checkbox"/> LAN4
DHCPサーバ有効/無効	無効 <input type="button" value="▼"/>
デフォルトゲートウェイ	<input type="text"/>
サブネットマスク	<input type="text"/>
プライマリDNSサーバ	<input type="text"/>
セカンダリDNSサーバ(オプション)	<input type="text"/>
開始IPアドレス	<input type="text"/>
終了IPアドレス	<input type="text"/>
リース期間	<input type="text"/>

tagVLAN・説明

VLAN ID

・追加するエントリに対するVLAN IDを入力してください。

名前

・追加するVLANのインタフェース名を入力してください。

IPアドレス

・追加するVLANのインタフェースに設定するIPアドレスを入力してください。

サブネットマスク

・設定するIPアドレスの所属するネットワークのサブネットマスクを入力してください。

ポートメンバー

・追加するVLANの通信に参加できるポートを選択してください。

DHCPサーバ有効/無効 有効/無効より選択

・DHCPサーバ機能を利用する場合は有効を選択してください。

初期値:有効

開始IPアドレス (DHCPサーバ有効選択時、入力可)

・DHCPサーバより配布するIPアドレスの開始アドレスを入力してください。

初期値:192.168.111.100

終了IPアドレス (DHCPサーバ有効選択時、入力可)

・DHCPサーバより配布するIPアドレスの終了アドレスを入力してください。

初期値:192.168.111.200

サブネットマスク (DHCPサーバ有効選択時、入力可)

・DHCPサーバより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。

初期値:255.255.255.0

サブネットマスク (DHCPサーバ有効選択時、入力可)

・DHCPサーバより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。

初期値:255.255.255.0

プライマリDNSサーバ (DHCPサーバ有効選択時、入力可)

・DHCPサーバより配布するプライマリDNSサーバのアドレスを入力してください。

初期値:192.168.111.1

セカンダリDNSサーバ(オプション) (DHCPサーバ有効選択時、入力可)

・DHCPサーバより配布するセカンダリDNSサーバのアドレスを入力してください。(※省略可)

初期値:(空欄)

デフォルトゲートウェイ (DHCPサーバ有効選択時、入力可)

・DHCPサーバより配布するデフォルトゲートウェイのアドレスを入力してください。

初期値:192.168.111.1

リース時間 (DHCPサーバ有効選択時、入力可)

・DHCPサーバよりIPアドレスの有効期間を入力してください。

初期値:86400[秒]

入力後、適用ボタンをクリックするとエントリが追加されます。

キャンセルボタンをクリックすると入力値が破棄され前の画面に遷移します。

4.5 ポートVLAN

ポートVLAN機能を設定できます。

ポート毎にPVIDを設定することでVLANタグが挿入されていないフレームの扱いを制御することができます。

ポートVLAN設定

ポートVLANの設定を行うことが出来ます。

現在のポートVLAN設定		
ポート	PVID	VLANメンバー
LAN1	1	1
LAN2	1	1
LAN3	1	1
LAN4	1	1

現在のポートVLAN設定・説明

ポート

・対応するポートが列挙・表示されます。

PVID

・ポートに設定されているPVIDが表示されます。

VLANメンバー

・ポートの所属するVLANが表示されます。

設定を変更したいポートのリンク部分を選択すると表示される画面について説明します。

ポートVLAN詳細設定

ポートVLANの詳細設定を行うことが出来ます。

ポートVLAN詳細設定	
ポート	1
PVID	1 (Vlan)
VLANメンバー	1 (Vlan)

適用 キャンセル

ポートVLAN詳細設定・説明

ポート

・設定を変更するポートが表示されます。

PVID 列挙される現在のVLANより一つ選択

・ポートのタグなしフレームをどのVLANとして扱うかを選択します。

VLANメンバー 列挙される現在のVLANより選択

・ポートをどのVLANと通信できるようにするか選択してください。

選択後、適用ボタンをクリックするとエントリが更新されます。

キャンセルボタンをクリックすると選択が破棄され前の画面に遷移します。

4.6 VPN パススルー

VPNパススルー機能が設定できます。

WANとLANとのVPN接続に対し簡易的なフィルタリングやIPv6パケットのブリッジ転送を設定できます。



VPNパススルー設定・説明

L2TP,IPSecパススルー 有効/無効より選択

・L2TPおよびIPSecをLAN内より許可する場合は有効を選択してください

初期値:無効

PPTPパススルー 有効/無効より選択

・PPTPをLAN内より許可する場合は有効を選択してください

初期値:無効

IPv6パススルー 有効/無効より選択

・IPv6通信をWAN/LAN間でブリッジングする場合は有効を選択してください

初期値:無効

入力後、適用ボタンをクリックすると設定が反映されます。

キャンセルボタンをクリックすると現在の設定値が再度読み込まれます。

4.7 NAT

NAT機能を変更できます。

WAN側とのアドレスポート変換を行い、複数の端末がWANネットワークにアクセスできるようになります。

NAT設定	
有効	<input checked="" type="checkbox"/>
TCPタイムアウト(秒)	180
UDPタイムアウト(秒)	180

NAT設定・説明

NAT 有効/無効より選択

- ・NAT機能を利用する場合は有効を選択してください。

初期値:有効

TCPタイムアウト(秒) 1-9999の範囲で入力

- ・TCPセッションの変換ルール有効時間を入力してください。

初期値:180

UDPタイムアウト(秒) 1-9999の範囲で入力

- ・UDPセッションの変換ルール有効時間を入力してください。

初期値:180

入力後、適用ボタンをクリックすると設定が反映されます。

キャンセルボタンをクリックすると現在の設定値が再度読み込まれます。

4.8 ルーティング

ルーティング機能を変更できます。

静的ルート情報の設定、およびRIPによるダイナミックルーティングを設定することができます。

スタティックルーティング設定

スタティックルーティングの設定を行います。

スタティックルーティングの追加	
送信先	<input type="text"/>
タイプ	ホスト
ゲートウェイ	<input type="text"/>
インターフェース	LAN
コメント (オプション)	<input type="text"/>

適用 リセット

ルーティングテーブル									
No.	送信先	ネットマスク	ゲートウェイ	フラグ	メトリック	Ref	使用数	インターフェース	コメント
1	255.255.255.255	255.255.255.255	0.0.0.0	S	0	0	0	LAN(vlan1)	
2	192.168.111.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(vlan1)	
3	10.10.10.0	255.255.255.0	0.0.0.0	1	0	0	0	WAN(eth3)	
4	192.168.222.0	255.255.255.0	10.10.10.6	3	0	0	0	WAN(eth3)	
5	0.0.0.0	0.0.0.0	10.10.10.254	3	1	0	0	WAN(eth3)	

削除 リセット

ダイナミックルーティング設定

ダイナミックルーティング(RIP)の設定を行います。

ダイナミックルーティングプロトコル	
有効	無効
RIP 設定	無効
RIP MD5 キーID	<input type="text"/>
RIP MD5 キー文字列	<input type="text"/>

適用 リセット

スタティックルーティングの追加・説明

送信先

・静的ルートを利用する送信先を入力してください。

タイプ ホスト/ネットより選択

・特定のIPアドレスのみを対象とする(ホスト)のか、特定のネットワークを対象とする(ネット)のかを選択してください。

サブネットマスク (タイプ:ネット選択時、表示)

・転送するネットワークのサブネットマスクを入力してください。

ゲートウェイ

・転送先のアドレスを本機器のLAN IPの範囲で入力してください。

インタフェース WAN/LAN/カスタムより選択

・転送先のネットワークが所属するインタフェースを選択もしくはカスタム選択時に入力して下さい。

コメント(オプション)

- ・追加するエントリに対してのコメントを入力してください。(※省略可)

追加ボタンをクリックするとエントリを追加することができます。

リセットボタンをクリックすると入力内容を破棄することができます。

ルーティングテーブル・説明

No.

- ・エントリナンバーを表示します。

送信先

- ・ルーティングされる送信先を表示します。

ネットマスク

- ・ルーティングされるネットワークのサブネットマスクを表示します。

ゲートウェイ

- ・転送先IPアドレスが表示されます。

フラグ

- ・エントリに設定されているフラグ情報を表示します。

メトリック

- ・対象ネットワークに到達するのに経由するルータ数が表示されます。

Ref

- ・ルーティングルールの参照回数を表示します。

使用数

- ・ルーティングが行われた回数を表示します。

インターフェース

- ・転送先インタフェースを表示します。

コメント

- ・エントリに設定されているコメントを表示します。

削除ボタンをクリックするとチェックボックスにチェックの入ったエントリを削除できます。

リセットボタンをクリックするとチェックボックスのチェックをすべて外すことができます。

ダイナミックルーティングプロトコル・説明

有効 無効/RIP-1/RIP-2B/RIP-2Mより選択

- ・RIPを有効にする場合は動作するバージョンを選択してくださいRIP-2B(ブロードキャストモード),RIP-2M(マルチキャストモード)です。

RIP認証 (有効:RIP-2B,RIP-2M選択時、選択可能)

- ・RIP-2の認証方式のうちMD5認証のみ対応しております。利用する場合は有効を選択してください。

RIP MD5 キーID (RIP認証:有効時入力可能)

・認証に用いるMD5キーIDおよび文字列の組のうちキーIDを入力してください。

RIP MD5 キー文字列 (RIP認証:有効時入力可能)

・認証に用いるMD5キーIDおよび文字列の組のうちキー文字列を入力してください。

入力後、適用ボタンをクリックすると設定が反映されます。

キャンセルボタンをクリックすると現在の設定値が再度読み込まれます。

4.9 QoS

QoS機能を設定できます。

特定の通信を速度制限、優先度をつけることで通信を整理することができます。

QoS設定

特定のアプリケーションの帯域保証をQoS設定で行うことができます。

QoS設定	
QoS(Quality of Service)	無効
アップロード帯域	ユーザ定義 Bits/sec
ダウンロード帯域	ユーザ定義 Bits/sec
QoSタイプ	DRR
予約帯域(QoS対象外の通信)	0% (標準値: 10%)

実行

QoS設定・説明

QoS (Quality of Service) 無効/双方向/アップロード/ダウンロードより選択

・QoS制御を行う場合は有効を選択してください。

初期値:無効

アップロード帯域 速度一覧より選択、もしくはカスタム選択の上入力 (QoS:無効以外選択時、入力可)

・WAN側接続回線の実効アップロード速度を選択および入力してください。ここでのアップロード速度は本製品からWANネットワークにデータ転送する速度のことです。

ダウンロード帯域 速度一覧より選択、もしくはカスタム選択の上入力 (QoS: 無効以外選択時、入力可)

・WAN側接続回線の実効ダウンロード速度を選択および入力してください。ここでのダウンロード速度はWANネットワークから本製品にデータ転送する速度のことです。

QoSタイプ DRR/SPQ/DRR+SPQより選択 (QoS: 無効以外選択時、選択可)

・QoS制御の方式について選択してください。

DRR:空き帯域がなくなるまで分配比率に応じ帯域を分割し続けます。

SPQ:パケットの送信順序を優先度に応じ並び替えます。

DRR+SPQ:優先通信についてパケットの有線送信を行いつつ、通常以下の通信に帯域を確保します。

予約帯域(QoS対象外の通信) 0/10/20/30/40%より選択 (QoS: 無効以外選択時、選択可)

・QoS管理されない余剰帯域を選択してください。

QoSアップロードグループ設定 (QoS: 双方向/アップロード選択時、表示)・説明
優先度 – 最高 0-100%(10%刻み)より選択 (QoSタイプ:DRR選択時、選択可)
・優先度が最高であるパケットの保証帯域および制限帯域を選択してください。
優先度 – 高 0-100%(10%刻み)より選択 (QoSタイプ:DRR選択時、選択可)
・優先度が高であるパケットの保証帯域および制限帯域を選択してください。
優先度 – 普通 0-100%(10%刻み)より選択 (QoSタイプ:SPQ以外選択時、選択可)
・優先度が普通であるパケットの保証帯域および制限帯域を選択してください。
優先度 – 低 0-100%(10%刻み)より選択 (QoSタイプ:SPQ以外選択時、選択可)
・優先度が低であるパケットの保証帯域および制限帯域を選択してください。

QoSダウンロードグループ設定 (QoS: 双方向/ダウンロード選択時、表示)・説明
優先度 – 最高 0-100%(10%刻み)より選択 (QoSタイプ:DRR選択時、選択可)
・優先度が最高であるパケットの保証帯域および制限帯域を選択してください。
優先度 – 高 0-100%(10%刻み)より選択 (QoSタイプ:DRR選択時、選択可)
・優先度が高であるパケットの保証帯域および制限帯域を選択してください。
優先度 – 普通 0-100%(10%刻み)より選択 (QoSタイプ:SPQ以外選択時、選択可)
・優先度が普通であるパケットの保証帯域および制限帯域を選択してください。
優先度 – 低 0-100%(10%刻み)より選択 (QoSタイプ:SPQ以外選択時、選択可)
・優先度が低であるパケットの保証帯域および制限帯域を選択してください。

入力後、実行ボタンをクリックすると設定が反映されます。

アップロードルール (QoS: 双方向/アップロード選択時、表示) ・ 説明

No.

・エントリナンバーを表示します。

名前

・エントリネームを表示します。

グループ

・振り分け先優先度を表示します。

情報

・振り分けルールを表示します。

アップロードルールを追加ボタンをクリックするとエントリを追加することができます。
削除ボタンをクリックするとチェックボックスにチェックの入ったエントリを削除できます。

ルールを追加ボタンをクリックした際に表示される画面について説明します。

QoS設定

特定のアプリケーションの帯域保証をQoS設定で行うことができます。

ルール設定	
方向	アップロード
名前	<input type="text"/>
グループ	優先度・遅延 <input type="button" value="D"/>
MACアドレス	<input type="text"/>
送信先IPアドレス	<input type="text"/>
送信元IPアドレス	<input type="text"/>
パケット長	<input type="text"/> - <input type="text"/>
DSCP	<input type="text"/> <input type="button" value="D"/>
プロトコル	<input type="text"/> <input type="button" value="D"/>

ルール設定・説明

方向

・追加するルールの適用先を表示します。

名前

・エントリネームを入力してください。

グループ

・振り分け先優先度を入力してください。

MACアドレス(※)

・制御対象フレームのMACアドレスを入力してください。

送信先IPアドレス(※)

・制御対象パケットの送信先IPv4アドレスを入力してください。

送信元IPアドレス(※)

・制御対象パケットの送信元IPv4アドレスを入力してください。

パケット長(※)

・制御対象パケットの長さを入力してください。

DSCP(※) BE/AF11-43/EFより選択

・制御対象パケットのDSCP優先度を入力してください。

プロトコル(※) TCP/UDPより選択

・制御対象パケットのプロトコルを入力してください。

(※)のうちいずれか1つ以上を入力してください。

入力後、適用ボタンをクリックするとエントリが追加されます。

5. ファイヤーウォール

5.1 MAC/IP/ポートフィルタ

MAC/IP/ポートフィルタ設定が変更できます。

特定の通信のWAN-LAN間転送を遮断することができます。

MAC/IP/ポート フィルタ設定

インターネット上のウイ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

標準方針：ルールに該当しないパケットの通過を

MAC/IP/ポート フィルタ設定

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

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 (オプション)

(設定可能上限:32)

現在のフィルタ設定

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
上記に該当しないパケットは許可しない									

基本設定・説明

MAC/IP/ポートフィルタ 有効/無効より選択

・特定の通信についてネットワークをまたいで転送されるのを遮断する場合は有効を選択してください。

初期値:無効

基本方針 許可する/許可しないより選択

・フィルタに合致した場合のパケットの処理について選択してください。

許可する:フィルタに合致したパケットを遮断します。

許可しない:フィルタに合致したパケットのみ転送いたします。

選択後、適用ボタンをクリックすると設定が反映されます。

リセットボタンをクリックすると現在の設定値が再度読み込まれます。

MAC/IP/ポートフィルタ設定・説明

送信元MACアドレス(※)

- ・フィルタ対象フレームのMACアドレスを入力してください

宛先IPアドレス(※)

- ・フィルタ対象パケットの宛先IPv4アドレスを入力してください

送信元IPアドレス(※)

- ・フィルタ対象パケットの送信元IPv4アドレスを入力してください

プロトコル None/TCP/UDP/ICMPより選択

- ・フィルタ対象パケットのプロトコルを選択してください

宛先ポートの範囲(※)

- ・フィルタ対象パケットの宛先ポートの範囲を入力してください

送信元ポートの範囲(※)

- ・フィルタ対象パケットの送信元ポートの範囲を入力してください

動作 許可/許可しないより選択

- ・合致した場合の処理について選択してください。

動作するためには基本方針と異なるものを選んでください。

コメント(オプション)

- ・エントリに対するコメントを入力してください。(※省略可)

(※) のうちいずれか1つ以上を入力してください。

入力後、適用ボタンをクリックするとエントリが追加されます。

リセットボタンをクリックすると入力内容を破棄することができます。

現在のフィルタ設定・説明

No.

- ・エントリナンバーを表示します。

送信元MACアドレス

- ・フィルタ対象の送信元MACアドレスを表示します。

宛先IPアドレス

- ・フィルタ対象の宛先IPアドレスを表示します。

送信元IPアドレス

- ・フィルタ対象の送信元IPアドレスを表示します。

プロトコル

- ・フィルタ対象のプロトコルを表示します。

宛先ポートの範囲

- ・フィルタ対象の宛先ポートを表示します。

送信元ポートの範囲

- ・フィルタ対象の送信元ポートを表示します。

動作

- ・フィルタ対象のパケットの処理を表示します。

コメント

- ・エントリに付与されたコメントを表示します。

パケット数

- ・フィルタを行ったパケットを表示します。

選択項目の削除ボタンをクリックするとチェックボックスにチェックの入ったエントリを削除できます。

リセットボタンをクリックするとチェックボックスのチェックをすべて外すことができます。

5.2 システムセキュリティ

システムセキュリティ設定が変更できます。
本製品の運用ポリシーを変更することができます。

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。

システムセキュリティ設定	
遠隔管理 (WAN経由)	無効 <input type="radio"/>
WAN側からのPingをブロック	有効 <input checked="" type="radio"/>
ポートスキャンブロック	有効 <input checked="" type="radio"/>
DoS攻撃 (SYN flood攻撃) ブロック	有効 <input checked="" type="radio"/>
SPIファイアウォール	有効 <input checked="" type="radio"/>

適用 リセット

システムセキュリティ設定・説明

遠隔管理(WAN経由) 有効/無効より選択

- ・WAN側ネットワークから本製品へアクセスがあった時にWeb管理画面を表示する場合は有効を選択してください。

初期値:無効

WAN側からのPingをブロック 有効/無効より選択

- ・WAN側からのPingに応答しない場合は有効を選択してください。

初期値:有効

ポートスキャンブロック 有効/無効より選択

- ・クリスマスツリーパケットによるポートスキャンに対して応答を返さない場合は有効を選択してください。

初期値:有効

DoS攻撃(SYN flood攻撃)ブロック 有効/無効より選択

- ・SYN flood攻撃を受けている際にSYN cookieを確認して通信を選別する場合は有効を選択してください。

初期値:有効

SPIファイアウォール 有効/無効より選択

- ・LAN→WAN転送パケットの期待戻り通信以外遮断する場合は有効を選択してください。

初期値:有効

選択後、適用ボタンをクリックすると設定が反映されます。

リセットボタンをクリックすると現在の設定値が再度読み込まれます。

5.3 コンテンツフィルタ

コンテンツフィルタ設定を変更できます。

Webコンテンツをフィルタすることができます。

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フィルタ設定

URLフィルタの追加

URL:

追加 リセット

現在のURLフィルタ設定

No.	URL

削除 リセット

Webホストフィルタ設定

ホスト(キーワード)の追加

キーワード:

追加 リセット

現在のWebホストフィルタ設定

No.	ホスト(キーワード)

削除 リセット

Webコンテンツフィルタ・説明

フィルタ Proxy/JavaScript/ActiveXより任意選択

・Webコンテンツについて80/3128/8080ポートにおける通信についてフィルタリングを行う場合は有効を選択してください。

Proxy:プロキシ通信をフィルタリングする場合は選択してください。

JavaScript:.jsファイルのダウンロードを抑止する場合は選択してください。

ActiveX:.ocxファイルのダウンロードを抑止する場合は選択してください。

初期値:いずれも未チェック。

選択後、適用ボタンをクリックすると設定が反映されます。

リセットボタンをクリックすると現在の設定値が再度読み込まれます。

URLフィルタの追加・説明

URL

- ・URLもしくはURLの一部が含まれているアクセスを遮断する場合は該当部分を入力してください。

入力後、追加ボタンをクリックするとエントリが追加されます。

リセットボタンをクリックすると入力内容を破棄することができます。

現在のURLフィルタ設定・説明

No.

- ・エントリナンバーを表示します。

URL

- ・アクセスを遮断するURLもしくはURLの一部を表示します。

削除ボタンをクリックするとチェックボックスにチェックの入ったエントリを削除できます。

リセットボタンをクリックするとチェックボックスのチェックをすべて外すことができます。

ホスト(キーワード)の追加・説明

URL

- ・キーワードが含まれているアクセスを遮断する場合は該当部分を入力してください。

入力後、追加ボタンをクリックするとエントリが追加されます。

リセットボタンをクリックすると入力内容を破棄することができます。

現在のWebホストフィルタ設定・説明

No.

- ・エントリナンバーを表示します。

ホスト(キーワード)

- ・アクセスを遮断するホスト(キーワード)を表示します。

削除ボタンをクリックするとチェックボックスにチェックの入ったエントリを削除できます。

リセットボタンをクリックするとチェックボックスのチェックをすべて外すことができます。

5.4 ポートフォワード

ポートフォワード設定が変更できます。

WANネットワークから本製品へのアクセスをLANネットワークの特定機器に転送することができます。

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 <input type="checkbox"/>
IPアドレス	<input type="text"/>
ポート番号の範囲	<input type="text"/>
プロトコル	TCP&UDP <input type="checkbox"/>
コメント (オプション)	<input type="text"/>

(設定可能な上限:32)

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
<input type="button" value="追加項目の削除"/> <input type="button" value="リセット"/>				

ポートフォワード設定・説明

ポートフォワード設定 有効/無効より選択

・ポートフォワード機能を利用する場合は有効を選択してください。

IPアドレス

・転送するLANネットワーク機器のIPv4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WANネットワークからの着信ポートを入力してください。

プロトコル TCP/UDP/TCP+UDPより選択

転送するプロトコルを選択してください。

コメント(オプション)

・エントリに対するコメントを入力してください(※省略可)

入力後、適用ボタンをクリックするとエントリの追加もしくは設定の変更がされます。

リセットボタンをクリックすると入力内容を破棄することができます。

現在のポートフォワード設定・説明

No.

・エントリナンバーを表示します。

IPアドレス

・転送先IPアドレスを表示します。

ポート番号の範囲

・遁走対象ポート番号を表示します。

プロトコル

- ・転送対象プロトコルを表示します。

コメント

- ・エントリに付与されたコメントを表示します。

選択項目の削除ボタンをクリックするとチェックボックスにチェックの入ったエントリを削除できます。

リセットボタンをクリックするとチェックボックスのチェックをすべて外すことができます。

5.5 ポートトリガー

ポートトリガー設定を変更できます。

特定ポートへのアクセスが確認できた際にポートに応じて追加でフォワーディングポートを設けることができます。

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のみ、WAN側の着信ポートを突きます。

ポートトリガー設定	
ポートトリガー設定	無効 <input type="checkbox"/>
トリガーポートのプロトコル	TCP <input type="checkbox"/> UDP <input type="checkbox"/>
トリガーポート	<input type="text"/>
着信ポートのプロトコル	TCP <input type="checkbox"/> UDP <input type="checkbox"/>
着信ポート	<input type="text"/>
コメント(オプション)	<input type="text"/>

(設定可能上限: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

ポートトリガー設定・説明

ポートトリガー設定 有効/無効より選択

・トリガーポート機能を利用す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 TCP/UDPより選択

・転送開始基準となる通信のプロトコルを選択してください。

トリガーポート

・転送開始基準となる通信のポート番号を入力してください。

着信ポートのプロトコル TCP/UDPより選択

・転送する着信のプロトコルを選択してください。

着信ポート

・転送する着信のポート番号を選択してください。

コメント(オプション)

・エントリに対するコメントを入力してください。(※省略可)

入力後、適用ボタンをクリックするとエントリの追加もしくは設定の変更がされます。

リセットボタンをクリックすると入力内容を破棄することができます。

現在のポートトリガー設定・説明

No.

・エントリナンバーを表示します

トリガーポートのプロトコル

・転送開始基準となる通信のプロトコルを表示します

トリガーポート

- ・転送開始基準となる通信のポート番号を表示します。

着信ポートのプロトコル

- ・転送する着信のプロトコルを表示します。

着信ポート

- ・転送する着信のポート番号を表示します。

コメント(オプション)

- ・エントリに付与されたコメントを表示します。

選択項目の削除ボタンをクリックするとチェックボックスにチェックの入ったエントリを削除できます。

リセットボタンをクリックするとチェックボックスのチェックをすべて外すことができます。

5.6 DMZ

DMZ機能を変更できます。

未定義のWANネットワークからの着信をLANネットワークの特定機器に転送できます。



DMZ設定・説明

DMZ設定 有効/無効より選択

- ・DMZ機能を利用する場合は有効を選択してください。

初期値:無効

DMZ IPアドレス

- ・転送先のLANネットワークIPv4アドレスを入力してください。

TCPポート80を除く

- ・本製品のWANネットワークからの管理をする場合などTCP80番を除外対象とする場合は選択してください。

入力後、適用ボタンをクリックすると設定が変更されます。

リセットボタンをクリックすると入力内容を破棄することができます。

6. VPN

6.1 PPTP

PPTP機能を変更できます。

レガシー端末などからVPN接続することができます。

※macOS10.12およびiOS10以降はPPTPサーバへの接続機能がございません。

あらかじめご了承ください。

PPTPサーバ設定
PPTPサーバの設定を行います。

PPTPサーバ設定

有効	無効
ローカルIPアドレス	192.168.111.1
IPアドレス範囲	192.168.111.201 ~ 192.168.111.220

適用 キャンセル

アカウント

ユーザ名	<input type="text"/>
パスワード	<input type="password"/>
IPアドレス (オプション)	<input type="text"/>

追加 リセット

現在のアカウント設定

No.	ステータス	ユーザ名	IPアドレス

削除 リセット

PPTPサーバ機能・説明

有効 有効/無効より選択

・PPTPサーバ機能を利用する場合は有効を選択してください。

初期値:無効

ローカルIPアドレス

・本製品のLANネットワークアドレスを入力してください。

IPアドレス範囲

・接続された端末に割り当てるIPアドレスを入力してください。

入力後、適用ボタンをクリックすると設定が変更されます。

キャンセルボタンをクリックすると現在の設定値が再度読み込まれます。

アカウント・説明

ユーザ名

・PPTPサーバに接続する際に使う新規登録アカウントのIDを入力してください。

パスワード

・PPTPサーバに接続する際に使う新規登録アカウントのパスワードを入力してください。

IPアドレス(オプション)

- ・アカウントにIPv4アドレスを固定で割り当てる場合は入力してください。(※省略可)

入力後、追加ボタンをクリックするとアカウントが追加されます。

リセットボタンをクリックすると入力内容を破棄することができます。

現在のアカウント設定・説明

ユーザ名

- ・登録されたアカウントのユーザ名を表示します。

ステータス

- ・アカウントの接続状況を表示します。

IPアドレス

- ・アカウントが接続された場合割り当てられたIPアドレスを表示します。

削除ボタンをクリックするとチェックボックスにチェックの入ったアカウントを削除できます。

リセットボタンをクリックするとチェックボックスのチェックをすべて外すことができます。

6.2 L2TP

L2TP機能を変更できます。

スマートフォンなどからVPN接続することができます。

※Android6以降から接続する際はいずれのフェーズ認証にもSHA1もしくはMD5を選択してください。

L2TPサーバ設定
L2TPサーバの設定を行います。

L2TPサーバ設定	
有効	無効 <input type="radio"/>
ローカルIPアドレス	192.168.111.1
IPアドレス範囲	192.168.111.221 - 192.168.111.240
L2TP over IPsec設定	
L2TP over IPsec	無効 <input type="radio"/>
セキュリティ設定	
キーイングモード	GREv1 with Pre-shared key <input type="radio"/>
DHグループ	14 (modp2048) <input type="radio"/>
フェーズ1暗号化	AES256 <input type="radio"/>
フェーズ1認証	SHA256 <input type="radio"/>
フェーズ2暗号化	AES256 <input type="radio"/>
フェーズ2認証	SHA256 <input type="radio"/>
プレシェアードキー	<input type="text"/>

アカウント	
ユーザ名	<input type="text"/>
パスワード	<input type="password"/>
IPアドレス (オプション)	<input type="text"/>

現在のアカウント設定			
No.	ステータス	ユーザ名	IPアドレス

L2TPサーバ機能・説明

有効 有効/無効より選択

・L2TPサーバ機能を利用する場合は有効を選択してください

初期値:無効

ローカルIPアドレス

・本製品のLANネットワークアドレスを入力してください

IPアドレス範囲

・接続された端末に割り当てるIPアドレスを入力してください

L2TP over IPsec設定 (L2TPサーバ機能:有効時、選択可)・説明

L2TP over IPsec 有効/無効より選択

・L2TP接続する際にIPsecによる暗号化経路を利用する場合は有効を選択してください

初期値:無効

セキュリティ設定 (L2TP over IPSec:有効時、選択入力可)・説明

キーイングモード IKEv1 with Pre-shared key/ IKEv2 with Pre-shared keyより選択

・IPSecによる鍵交換方式を選択してください。

初期値: IKEv1 with Pre-shared key

DHグループ 1/2/5/14より選択

・鍵交換時に利用するDHアルゴリズムに用いる鍵長を選択してください

フェーズ1暗号化 3DES/AES128/AES192/AES256より選択

・フェーズ1で行われる暗号化方式を選択してください

フェーズ1認証 MD5/SHA1/SHA256

・フェーズ1で行われるハッシュ化方式を選択してください

フェーズ2暗号化

3DES/AES128/AES192/AES256より選択

・フェーズ2で行われる暗号化方式を選択してください

フェーズ2認証 MD5/SHA1/SHA256

・フェーズ2で行われるハッシュ化方式を選択してください

プレシェアードキー 接続相手を認証する際に用いる共通パスフレーズを入力してください

入力後、適用ボタンをクリックすると設定が変更されます。

キャンセルボタンをクリックすると現在の設定値が再度読み込まれます。

アカウント・説明

ユーザ名

・L2TP/IPSecサーバに接続する際に使う新規登録アカウントのIDを入力してください

パスワード

・L2TP/IPSecサーバに接続する際に使う新規登録アカウントのパスワードを入力してください

IPアドレス(オプション)

・アカウントにIPv4アドレスを固定で割り当てる場合は入力してください(※省略可)

入力後、追加ボタンをクリックするとアカウントが追加されます。

リセットボタンをクリックすると入力内容を破棄することができます。

現在のアカウント設定・説明

ユーザ名

・登録されたアカウントのユーザ名を表示します

ステータス

・アカウントの接続状況を表示します

IPアドレス

・アカウントが接続された場合割り当てられたIPアドレスを表示します

削除ボタンをクリックするとチェックボックスにチェックの入ったアカウントを削除できます。

リセットボタンをクリックするとチェックボックスのチェックをすべて外すことができます。

6.3 IPSec

IPSec設定を変更できます。

遠隔地と相互にVPNによるネットワーク接続することができます。

IPSec設定

IPSecの設定を行います。

IPSecトンネル設定	
トンネル名	<input type="text"/>
開始タイプ	ignore
ローカルネットワーク設定	
ローカルアドレス	<input type="text"/>
ローカルセキュリティゲートウェイタイプ	IPアドレス
IPアドレス	<input type="text"/>
ローカルネットワークアドレス	<input type="text"/>
サブネットマスク	<input type="text"/>
リモートネットワーク設定	
リモートアドレス	<input type="text"/>
リモートセキュリティゲートウェイタイプ	IPアドレス
IPアドレス	<input type="text"/>
リモートネットワークアドレス	<input type="text"/>
サブネットマスク	<input type="text"/>
セキュリティ設定	
キーイングモード	IKEv1 with Pre-shared key
フェーズ1DHグループ	1 (modp768)
フェーズ1暗号化	3DES
フェーズ1認証	MD5
Perfect Forward Secrecy	無効
フェーズ2暗号化	3DES
フェーズ2認証	MD5
プレシェアードキー	<input type="text"/>
詳細設定	
アグレッシブモード	無効
DPDアクション	None
DPD間隔(秒)	30
Expiry - IKE SA(時間)	3
Expiry - IPSec SA(時間)	1
Rekeying(分)	9

IPSec設定	
ログレベル	-1: 無し

現在のIPSecトンネル設定					
No.	ステータス	トンネル名	ローカルアドレス	リモートアドレス	コントロール
<input type="button" value="削除"/> <input type="button" value="リセット"/>					

IPSecトンネル設定・説明

トンネル名

- ・エントリに付与する名前を半角英数字にて入力してください。

開始タイプ Ignore/Add/Route/Startより選択

- ・動作モードを選択してください。

初期値:Ignore

Ignore:無効

Add:手動接続

Route:接続があった際に自動接続

Start:起動時に自動接続

ローカルネットワーク設定・説明

ローカルアドレス

- ・本製品のWAN側IPアドレスもしくはドメイン名(FQDN)を入力してください。

ローカルセキュリティゲートウェイタイプ IPアドレス/ホスト名(FQDN)/E-mailアドレス (User FQDN)より選択

- ・本製品の認証に用いるIDの種別を入力してください。

初期値:IPアドレス

(ローカルセキュリティゲートウェイタイプにて選択したものが表示されます)

- ・本製品の認証に用いるIDを入力してください。

ローカルネットワークアドレス

- ・本製品のLANネットワークアドレスを入力してください。

サブネットマスク

- ・本製品のLANネットワークのサブネットマスクを入力してください。

リモートネットワーク設定・説明

リモートアドレス

- ・接続先のWAN側IPアドレスもしくはドメイン名(FQDN)を入力してください。

リモートセキュリティゲートウェイタイプ

- ・接続先の認証に用いるIDの種別を入力してください。

(リモートセキュリティゲートウェイタイプにて選択したものが表示されます)

- ・接続先の認証に用いるIDを入力してください。

リモートネットワークアドレス

- ・接続先のLANネットワークアドレスを入力してください。

サブネットマスク

- ・接続先のLANネットワークのサブネットマスクを入力してください。

セキュリティ設定・説明

キーイングモード IKEv1 with Pre-shared key/ IKEv2 with Pre-shared keyより選択

- ・IPSecによる鍵交換方式を選択してください。

初期値: IKEv1 with Pre-shared key

DHグループ1/2/5/14より選択

- ・鍵交換時に利用するDHアルゴリズムに用いる鍵長を選択してください。

フェーズ1暗号化3DES/AES128/AES192/AES256より選択

- ・フェーズ1で行われる暗号化方式を選択してください。

フェーズ1認証 MD5/SHA1/SHA256

・フェーズ1で行われるハッシュ化方式を選択してください。

Perfect Forward Secrecy 有効/無効より選択

・派生した鍵を用いないことで通信の被解読範囲が全体に及ぶのを防ぐ場合は有効を選択してください。

初期値: 無効

フェーズ2暗号化 3DES/AES128/AES192/AES256より選択

・フェーズ2で行われる暗号化方式を選択してください。

フェーズ2認証 MD5/SHA1/SHA256

・フェーズ2で行われるハッシュ化方式を選択してください。

プレシェアードキー

・接続相手を認証する際に用いる共通パスフレーズを入力してください。

詳細設定・説明

アグレッシブモード 有効/無効より選択

・安全性の代わりに接続性を高める場合は有効を選択してください。

初期値:無効

DPDアクション None/Clear/Hold/Restart

・DPDによる接続先との疎通確認に失敗した場合の挙動を選択してください。

None:DPDによる疎通確認を行いません。

Clear:DPDによる確認は行いますが切断時に何もしません。

Hold:DPDによる確認を行い、再度相手側への通信が行われる場合は再接続を行います。

Restart: DPDによる確認を行い、切断時には直ちに再接続を試みます。

DPD間隔

・R_U_THEREメッセージなどをやり取りする間隔を入力してください。

Expiry – IKE SA

・IKE SAの継続時間を入力してください。

Expiry – IPSec SA

・IPSec SAの継続時間を入力してください。

一般的にIKE SA>IPSec SAの値を設定してください。

Rekeying

・継続時間終了の何分前に新経路を設けるか入力してください。

一般的にIPSec SA >Rekeyingの値を設定してください。

入力後、追加ボタンをクリックするとIPSecトンネル設定が追加されます。

キャンセルボタンをクリックすると入力内容が破棄されます。

IPSec設定・説明

ログレベル -1/0/1/2より選択

・システムログに記載するIPSecのログ種別を選択してください。

初期値:-1:無し

選択後、適用ボタンをクリックすると設定が変更されます。

キャンセルボタンをクリックすると現在の設定値が再度読み込まれます。

現在のIPSecトンネル設定・説明

No.

・エントリナンバーが表示されます。

ステータス

・接続状況が表示されます。

トンネル名

・トンネルに付与された名前が表示されます。

ローカルアドレス

・ローカルアドレスが表示されます。

リモートアドレス

・リモートアドレスが表示されます。

コントロール

・接続ボタンをクリックすると接続待ちの場合は発呼を行います。

切断ボタンをクリックすると接続中の場合は切断を行います

エントリ名をクリックするとトンネル設定を編集することができます。

削除ボタンをクリックするとチェックボックスにチェックの入ったトンネルを削除できます。

リセットボタンをクリックするとチェックボックスのチェックをすべて外すことができます。

7. 管理

7.1 システム管理

システム管理設定を変更することができます。Web管理画面へのログイン情報等変更することができます。

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	admin
パスワード	*****
ウォッチドッグ	有効 <input type="checkbox"/>

適用 キャンセル

NTP設定	
現在時刻	XX Oct XX XX:XX:XX GMT X: <input type="checkbox"/> ホストと同期
タイムゾーン	(GMT+09:00) Japan, Korea <input type="button" value="▼"/>
NTPサーバ	ntp.nict.jp

適用 キャンセル

管理者設定・説明

アカウント

・Web管理画面へのログインに用いる変更後のアカウントIDを入力してください。

パスワード

・Web管理画面へのログインに用いる変更後のアカウントパスワードを入力してください。

ウォッチドッグ 有効/無効より選択

・CPUが処理を進められないような状態のとき、自動的に再起動を行う場合は有効を選択してください。

初期値:有効

選択後、適用ボタンをクリックすると設定が変更されます。

キャンセルボタンをクリックすると現在の設定値が再度読み込まれます。

NTP設定・説明

現在時刻

・本製品の内部時刻を表示します。

ホストと同期ボタンをクリックすると閲覧しているブラウザより時刻情報を秒数切り捨てにて本製品に適用します。

タイムゾーン タイムゾーン一覧より選択

・本製品に適用するタイムゾーンを選択してください。

システムログやオートファームアップのタイミングに利用されます。

NTPサーバ

・NTPによる時刻同期をする参照サーバを入力してください。

初期値:ntp.nict.jp

選択後、適用ボタンをクリックすると設定が変更されます。

キャンセルボタンをクリックすると現在の設定値が再度読み込まれます。

7.2 DDNS

DDNS設定を変更することができます。

IPアドレスが固定でない場合にWANネットワークからのアクセスを簡便にできます。

DDNS設定

ダイナミックDNS設定を変更できます。

DDNS設定	
DDNSサービス名:	なし
通知IP取得先:	WANインタフェース
アカウント:	
パスワード:	
ホスト名:	

適用 キャンセル

DDNS設定・説明

DDNSサービス名 なし/mydns.jp/no-ip.com/ DP-21.net/CyberGateより選択

・DDNSサービスを利用する場合は一覧から選択してください。

初期値:なし

通知IP取得先 WANインタフェース/ネットワークより選択 (DDNSサービス名:なし選択時以外、選択可)

・DDNSサービスに通知するIPv4アドレスの取得方法を選択してください。

WANインタフェース:WANネットワークより本製品が割り当てを受けているIPアドレスを取得します。

ネットワーク:本製品のリモートホストIPv4アドレスを取得します。

アカウント (DDNSサービス名:なし選択時以外、入力可)

・利用するDDNSサービスに登録しているアカウントIDを入力してください。

パスワード (DDNSサービス名:なし選択時以外、入力可)

・利用するDDNSサービスに登録しているアカウントパスワードを入力してください。

ホスト名 (DDNSサービス名:なし選択時以外、入力可)

・利用するホスト名を入力してください。

選択後、適用ボタンをクリックすると設定が変更されます。

キャンセルボタンをクリックすると現在の設定値が再度読み込まれます。

7.3 ファームウェア更新

ファームウェア更新設定について設定できます。

弊社Webページなどで本製品のアップデートが公開された場合、アップデートの有無や更新などを設定できます。

※ファームウェアアップデート中は電源を切らないでください。起動しなくなるまたは正常な動作をしなくなる恐れがあります。電源断などでファームウェア更新に失敗した場合は弊社サポートセンターでの修理が必要となります。

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	v1.01
最新	取得できませんでした
更新開始	

ローカルファームウェアアップデート	
ファームウェアファイルの場所	ファイルを選択 選択されていません
適用	

自動アップデート	
有効	無効 <input type="checkbox"/>
適用	

ファームウェアバージョン・説明

現在

・現在稼働しているファームウェアのバージョンを表示します。

最新

・弊社Webにて最新版ファームウェアが公開されている場合、そのバージョンを表示します。
ファームウェアが公開されていないまたは情報が取得できない場合、「取得できませんでした。」と表示します。

ファームウェアが公開され現在稼働しているバージョンより最新版が新しい場合更新開始ボタンをクリックすることができます。

クリックするとWANネットワーク経由でファームウェアを取得しアップデートを行います。

ローカルファームウェアアップデート・説明

ファームウェアファイルの場所

・ファイルの選択ボタンをクリックして適用するファームウェアを選択してください。

選択後、適用ボタンをクリックするとファームウェアが選択したファイルで更新されます。

自動アップデート・説明

有効 有効無効より選択

・自動アップデート機能を利用する場合は有効を選択してください。

有効時、深夜帯にファームウェアの更新を確認し自動的にファームウェアを適用します。

選択後、適用ボタンをクリックすると設定が変更されます。

7.4 設定管理

設定管理することができます。

現在の設定値をファイルとしてリカバリ用に保存したり、書き戻したり、初期設定に戻したりすることができます。



設定のバックアップ・説明

バックアップ

・クリックすると”VR500_(年月日時分秒).bin”というファイル名で現在の設定値が保存できます。

設定の復元・説明

設定ファイルの場所

・設定ファイルを選択し、復元ボタンをクリックすると設定ファイルによって現在の設定が書き込まれます。

初期化・説明

初期化

・クリックするとファームウェア内のデフォルト設定値にて設定が書き戻され初期値に設定変更できます。

7.5 SNMP

SNMP設定を変更できます。

運用上必要な情報を簡潔に扱うことができます。

SNMP設定

SNMPを設定できます。

SNMP設定	
有効	無効
コミュニティ名	public
システムロケーション	
システム名	VR500-A1
システムコンタクト	

適用 キャンセル

SNMPトラップ設定	
有効	無効
コミュニティ名	public
宛先アドレス	
ポート	162

適用 キャンセル

SNMP設定・説明

有効 有効/無効より選択

・SNMP機能を利用する場合は有効を選択してください。

初期値:無効

コミュニティ名 (有効選択時、入力可)

・SNMPコミュニティ名を入力してください。

初期値:public

システムロケーション (有効選択時、入力可)

・設置場所を入力してください。(※省略可)

システム名 (有効選択時、入力可)

・本製品のシステム名を入力してください。(※省略可)

システムコンタクト (有効選択時、入力可)

・本製品の管理者アドレスを入力してください。(※省略可)

選択後、適用ボタンをクリックすると設定が変更されます。

キャンセルボタンをクリックすると現在の設定値が再度読み込まれます。

SNMPトラップ設定・説明

有効 有効/無効より選択

・SNMP trap機能を利用する場合は有効を選択してください。

初期値:無効

コミュニティ名 (有効選択時、入力可)

・SNMP trapの通知コミュニティ名を入力してください。

初期値:public

宛先アドレス (有効選択時、入力可)

・Trapを送付するIPv4アドレスを入力してください。

ポート (有効選択時、入力可)

・Trap受信ポートを入力してください。

初期値:162

入力後、適用ボタンをクリックすると設定が変更されます。

キャンセルボタンをクリックすると現在の設定値が再度読み込まれます。

7.6 Syslog

Syslog設定を変更できます。本製品のシステムログを外部に転送できます。



Syslog設定	
有効	無効
リモートアドレス	
リモートポート	514
ログレベル	Debug

適用 キャンセル

Syslog設定・説明

有効 有効/無効より選択

・Syslog転送を行う場合は有効を選択してください。

リモートアドレス

・転送先IPv4アドレスを入力してください。

リモートポート

・転送先ポート番号を入力してください。

ログレベル ログレベル一覧より選択

・転送するログレベルを選択してください。

入力後、適用ボタンをクリックすると設定が変更されます。

キャンセルボタンをクリックすると現在の設定値が再度読み込まれます。

7.7 再起動

再起動することができます。

動作が不安定な場合や、期待した動作をしない場合に行うと改善する場合があります。

再起動

再起動

再起動・説明

再起動

・クリックすると再起動します。

8. 仕様

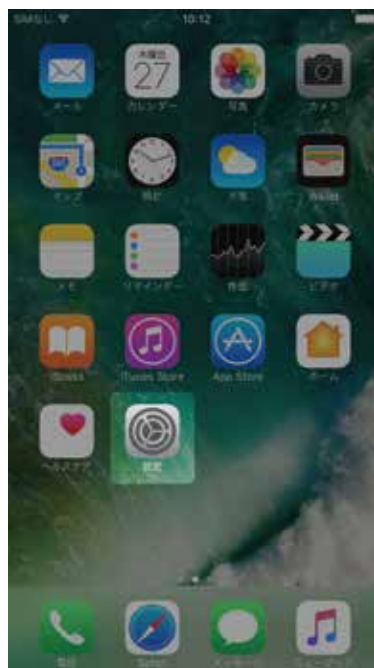
型番	VR500-A1
有線部仕様	
対応規格	IEEE802.3ab(1000BASE-T) IEEE802.3u(100BASE-TX) IEEE802.3i(10BASE-T)
インターフェース	RJ-45ポート×5(WAN×1、LAN×4)
伝送速度	1000/100/10Mbps(オートネゴシエーション)
ネットワークケーブル	1000BASE-T:カテゴリ5e以上 100BASE-TX:カテゴリ5以上 10BASE-T:カテゴリ3以上
ソフトウェア仕様	
VPN機能	
サポートプロトコル	IPsec、L2TP over IPsec、PPTP
暗号化方式(IPsec)	3DES/AES128/AES192/AES256
認証方式(IPsec)	MD5/SHA1/SHA256
VPN対地数(IPSec/L2TP)	10
VPN対地数(PPTP)	5
Tunnel Keep-Alive	Dead Peer Detection
NAT traversal	対応
WAN設定	
IPアドレス取得方法	IPアドレス自動取得(DHCPクライアント) 固定IP(手動設定) PPPoEクライアント
セキュリティ	ステートフルパケットインスペクション(SPI)、DoS攻撃防止、 IP/ポートフィルタリング、WEBサイトブロック、DMZホスト、 IPSec/PPTP/L2TP パススルー
対応DDNSサービス	DP-21.NET(有料)、cybergate(有償)、MyDNS(無償)、no-ip(無償)
DNS Local Database	非対応
LAN設定	固定IPアドレス(手動設定) DHCPサーバ(有効/無効)
IPv6	未対応
ハードウェア仕様	
ハードウェアスイッチ	RESETボタン、POWERスイッチ
LED	[P]ower,[W]AN,LAN[1]-[4]
消費電力	最大約 4.5W
電源	DC12V 1A
外形寸法	約148(W)×29(H)×105(D)mm
重量	約483g (本体のみ)
動作時環境	温度:0~40°C 湿度:10~90% (結露なきこと)
保存時環境	温度:-20~75°C 湿度:10~90% (結露なきこと)
その他	
対応OS	Windows(R) 10(32/64bit) / Windows(R) 8.1(32/64bit) / Windows(R) 8(32/64bit) / Windows(R) 7(32/64bit) macOS 10.12/Mac OS X10.11/10.10/10.9/10.8/10.7/10.6
各種設定方法	WEBブラウザ
保証期間	1年間
同梱物	VR500-A1(本製品)、ACアダプタ、印刷物一式(マニュアル、保証書等)

9. 参考情報（スマートフォンでの操作）

9.1 iPhone

1. iPhoneにて本製品にVPN接続する場合(2016/10現在iOS10.1/iPhone7にて確認)

① iPhoneの設定アプリをタップします。



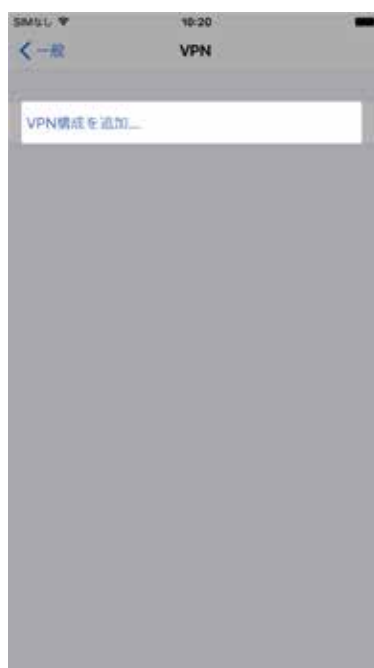
② 一般をタップします。



③ スクロールし、VPNを選択します。



④ VPN構成を追加…をタップします。



⑤ タイプをタップし、L2TPをタップします。



⑥ 各項目に設定事項を入力します。



- ① 説明にこのVPN接続に付与する名前を入力してください。
- ② サーバに本製品のWANネットワークのIPアドレスもしくはDDNS設定を行っている場合はホスト名を入力してください。
- ③ アカウントにはVPN>L2TPにて設定したアカウントより接続に用いるアカウントIDを入力してください。
- ④ アカウントパスワードを入力してください。空欄にした場合、接続のたびに入力する形となります。
- ⑤ シークレットではVPN>L2TPにて設定したプレシェアードキーを入力してください。

⑦ 入力後完了をタップします。



⑧ VPN設定画面に戻ります。

接続するには状況のトグルボタンをタップし、オンにすると接続中に状況が変化します。また接続中は画面上部にVPN接続中であることを示すマークが表示されます。



9.2 Android

2. Androidにて本製品にVPN接続する場合(2016/10現在Android4.1.2/SOL21にて確認)

- ① (事前準備)VPNを利用するには端末のセキュリティ設定をする必要があります。
電源を入れた際にパスワードや暗証番号、パターンなど追加の操作が必要なく、ホーム画面が表示される場合は予めセキュリティ設定を行ってください。
- ② 設定アプリをタップします。



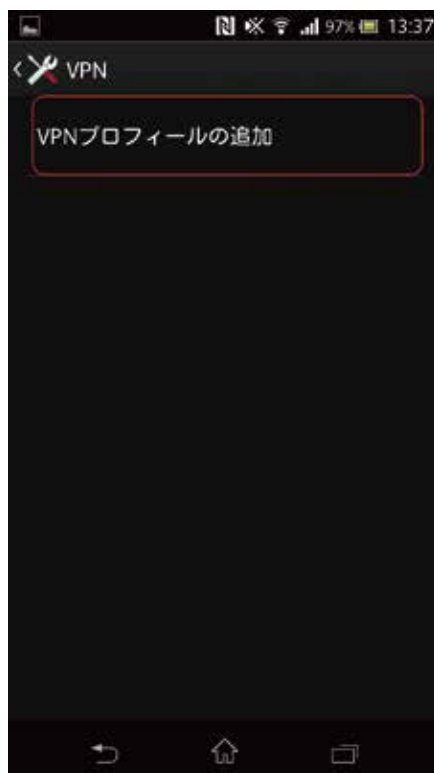
- ③ その他の設定をタップします。(一部の機種では”無線とネットワーク”内の”もっと見る”の場合があります)



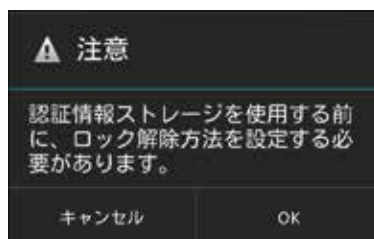
- ④ VPNをタップします。



- ⑤ VPNプロフィールの追加をタップします。



この際①のセキュリティ設定を行っていない場合ダイアログがされます。
この場合はOKをタップし、設定を再度行ってください。



⑥ VPNタイプを変更します。



⑦ 各項目に設定事項を入力します。



- ① 説明にこのVPN接続に付与する名前を入力してください。
- ② サーバに本製品のWANネットワークのIPアドレスもしくはDDNS設定を行っている場合はホスト名を入力してください。
- ③ IPSec事前共有鍵にVPN>L2TPにて設定したプレシェアードキーを入力してください。

⑧ 保存をタップします。



⑨ VPN設定画面に戻ります。
接続する際は追加したVPN設定をタップします。



⑩ 認証情報を入力します。



- ④ ユーザー名にはVPN>L2TPにて設定したアカウントより接続に用いるアカウントIDを入力してください
- ⑤ アカウントパスワードを入力してください。

⑪ 接続をタップします。

接続すると”接続されました”にテキストが変化します。また接続中は画面上部にVPN接続中であることを示す鍵マークが表示されます。

