Spread Router シリーズ

ウェブユーザインターフェース操作マニュアル

Ver.1.1.8

NSTG
New System Technology Globalist

改訂履歴

版数	日付	変更箇所	内　　容
1.00	2014/10/30	初版	新規発行
1.01	2014/12/01	各章	各章に設定後の設定保存と再起動説明を記載
		シリアル変換	外部アクセス時の要フィルタ設定を追記
		WebUI ポート	外部アクセス時の要フィルタ設定を追記
1.02	2014/12/09	NTP/日付・時刻	時計用内蔵電池寿命を追記
		サイト情報の更新	開発サイトページ記載
1.10	2015/02/01	全般改訂	ファームウェア v1.02 へ改訂
1.11	2015/02/20	シリアル変換	シリアル変換できない場合の確認手段追記
1.12	2015/06/17	3G 通信モジュール	アンテナレベル表示についての注意点を追記
		シリアル変換	コンソールポートのアプリ利用時の設定に関する記述追加
1.13	2015/06/23	専用設定ファイル	専用設定ファイル項目を追加（ファームウェア v1.03 対応）
1.14	2015/07/02	コンソールポート変更	コンソールポートをアプリケーション利用させる設定を追記
1.15	2015/10/01	注意事項追記	インターネット利用時の注意事項について、ファームバージョン違いによる「設定の復帰」についてを記載。
		3G 通信モジュール	LTE 対応製品に関する追記
1.16	2016/1/15	インターネット利用時の注意事項	ファームウェア v1.05 の SSH デフォルトポート番号変更に関する記載
		5.1 フィルタ設定	
1.17	2016/11/10	20. VPN サービス OS 追記	VPN 対応 OS に関する記載を追加
1.18	2017/08/30	はじめに	3G/LTE モジュールの技適番号を記載

目次

はじめに

このたびは本製品をご購入いただきまして、誠にありがとうございます。
本書には、本製品を安全に使用していただくための重要な情報が記載されています。ご使用の前に本書をよくお読みになり、正しくお使いいただけますようお願い致します。
特に、本製品に添付されている「安全にお使いいただくために」をよく読み、理解されたうえで本製品をご使用ください。
また、本書は本製品の使用中、いつでも参照できるように大切に保管してください。

◆ **摘要**

本書は SpreadRouter ファームウェアの下記バージョンについて記載しています。

SpreadRouter-F/R firmware ver1.03+ (Jun 12 18:09:11 JST 2015)

SpreadRouter-F/R firmware ver1.04+ (Tue Sep 29 16:37:32 JST 2015)

SpreadRouter-F/R firmware ver1.05+ (Wed Jan 13 15:38:31 JST 2016)

◆ **ご注意**

1. 本書の内容の一部または全部を無断で転用、転載しないようお願いいたします。

2. 本書の内容および製品仕様、外観は、改良のため予告なく変更することがあります。

3. 本書の作成にあたっては万全を期しておりますが、本書の内容の誤りや省略に対して、また本書の適用の結果生じた間接損害を含め、いかなる損害についても責任を負いかねますのでご了承ください。

4. 製品の保証に関する規定については製品添付の製品保証書をご覧下さい。

5. 本製品にて提供されるファームウェアおよび本製品用として弊社より提供される更新用ファームウェアを、本製品に組み込んで使用する以外の方法で使用することは一切許可しておりません。

◆ **セキュリティの確保について**

パスワードを設定しない、もしくはデフォルトパスワードを使用する場合、ネットワーク上の誰からでも本装置の設定を行うことができます。

セキュリティの面からは非常に危険なため、ユニークなパスワードを設定することを強く推奨します。

◆ **最新情報の入手について**

弊社ホームページにて、製品の最新ファームウェア・マニュアル・製品情報を掲載しています。

下記の SpreadRouter 専用ホームページから、該当する製品名をクリックしてください。

SpreadRouter 専用サイト

http://m2m-nstg.jimdo.com/

また開発者向け情報も掲載しておりますので、是非ご覧ください。

開発者向け情報提供サイト SpreadRouter' Wiki

http://180.62.148.246/index.php

◆ **商標について**

- 「SpreadRouter」はエヌエスティ・グローバリスト株式会社の登録商標です。
- その他文中の商品名、会社名は、各社の商標または登録商標です。

◆SpreadRouter シリーズは、以下の技術基準適合番号の通信モジュールを採用しています。

製品名	通信モジュール	技適番号
SpreadRouter-R	ublox LISA-U200 3G module	R003-120375
SpreadRouter-F		
SpreadRouter-R_LTE	AM Telecom AMP520 LTE module	R003-140259

※尚、上記技適につきましては「通信モジュール」単体として取得しており、弊社製品「SpreadRouter」としての取得はしておりません。

インターネット利用時の注意事項

本製品を使用し、3G 回線や固定回線等からインターネットを利用する際、外部からの不正なアクセスが行われる可能性がございます。特に出荷時の設定では、ppp0(3G)や eth0/eth1(PPPoE)等の external となるインターフェースが該当します。

不正な攻撃対象として主に上げられるのは。

（１） SSH(22 番ポート)がデフォルトで「アクセス許可」としています。その為、不正なパスワードアタックの対象となる危険性もございますので、フィルタ設定で外部からのアクセスを「許可しない」にするか、SSH の接続ポート番号を 22 番以外にするなど構築される事をお勧めいたします。

※SSH ポート番号を変更する場合は、コンソールログイン後、/etc/ssh/sshd_config の Port 22　を変更します。

※尚、ファームウェアバージョン v1.05 からデフォルトの SSH ポート番号が 10022 に変更されました。

（２） Ping（ICMP）の応答を返さない。デフォルトでは Ping(ICMP)に対する応答は全て返す設定になっていますが、応答を返すことで踏み台サーバとして利用される可能性も考えられます。

※ICMP 応答を返さない設定は、コンソールログイン後、/etc/sysctl.conf を修正し、下記の行を追記すると ICMP 応答を返さなくなります。

net.ipv4.icmp_echo_ignore_all = 1

（３） Web 設定画面のポート番号変更。デフォルトでは 80 番ポートが web 設定画面のポートになり、インターネット上からはアクセス出来ない設定になっています。インターネットからも web 設定画面へアクセスしたい場合は、web 設定画面のポート番号変更と、設定画面パスワードの変更を行う事をお勧めいたします。

※設定の変更は「SpreadRouterWebUI 操作マニュアル」第 16 章を参照ください。

※コンソールにて設定を変更後は、#overlaycfg –s etc コマンドを入力し、再起動してください。

ファームウェアバージョン違いによる設定復帰時の注意点

＜注意１＞

ファームウェアバージョンが異なったものに対して、本体設定情報の「設定の復帰」を行った場合、全て反映されない可能性があります。

事前に必ず同じファームウェアバージョンで設定を行った状態で、「設定の保存」を行ってください。

＜注意２＞

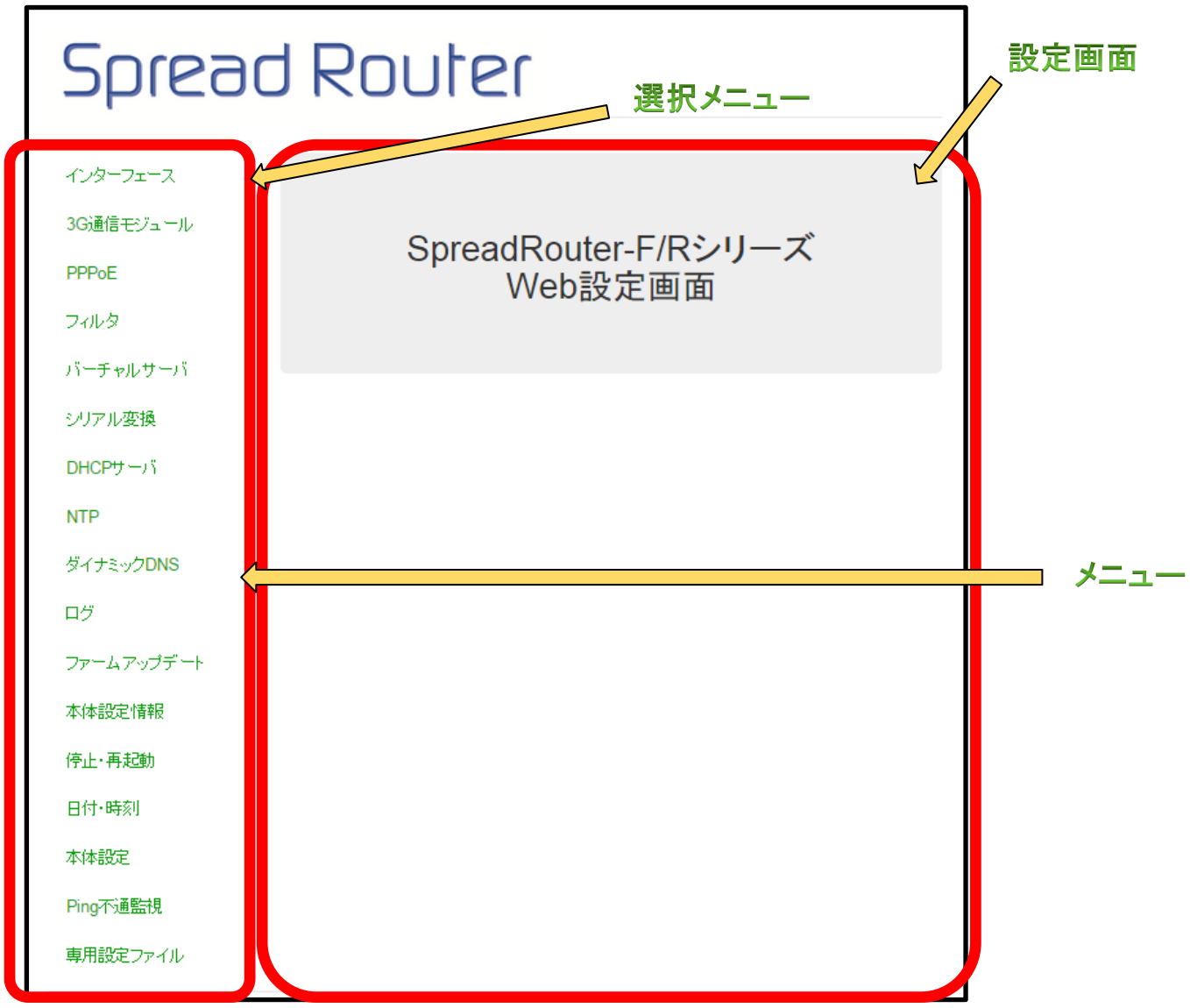
※設定の復帰を行った際、画面上は失敗しましたと表示されることがありますが、読込ファイルが正しい場合は再起動後に設定が反映されています。

第１章

概要

1.1. 基本画面構成・動作環境

◆ **基本画面構成**



画面は、左のメニュー部と右の設定画面部に分かれます。

選択したメニューは色が付きます。

◆ **動作環境**

本WebUIは、JavaScriptを使用しています。ご利用のウェブブラウザにおいて、JavaScript機能を有効にして下さい。

動作確認に使用した OS とウェブブラウザは以下の通りです。

Windows 7: Internet Explorer 11

Windows 7: Chrome 38

1.2. WebUI へのアクセス

◆ **WebUI へのアクセス**

パソコンと SpreadRouter の Ether0 または Ether1 ポートに LAN ケーブルを接続し、パソコンのブラウザを起動します。SpreadRouter には DHCP サーバが起動しているため、パソコン側のネットワーク設定は「IP アドレスを自動的に取得する」を選択しておくと簡単に設定することが可能です。

ブラウザのアドレスバーに　http://192.168.1.1/　を入力しアクセスしてください。

なお、SpreadRouter シリーズのイーサネットポート初期状態の IP アドレスは以下の通りです。

インターフェース名	IP アドレス
ETHER 0 (eth0)	192.168.1.1
ETHER 1 (eth1)	192.168.1.1

アクセスするとログイン画面が表示されます。(表示される画面は、お使いのブラウザによって異なります)

Microsoft Internet Explorer の場合

Google Chrome の場合

初期アカウントは以下の通りです。

アカウント名	パスワード
admin	admin

第２章

インターフェース

第 2 章　インターフェース

2.1 インターフェース設定

◆　インターフェース設定は、SpreadRouter のイーサネットポートの設定を行います。イーサネットポートは、ETHER0/ETHER1 の 2 ポートあります。設定は大きく分けて 2 つあり、SpreadRouter のイーサネットポートの IP アドレスを 2 ポート共、同じ IP アドレスに割当てるブリッジインターフェース設定。もう一つはイーサネットポート個別に IP アドレスを割り当てる個別インターフェース設定があります。

※出荷状態はブリッジインターフェース設定です。

	ブリッジインターフェース	個別インターフェース
IP アドレス	同じ IP アドレスを割り当てる	ETHER0/ETHER1 にそれぞれ別の IP アドレスを割り当てる
主な使用イメージ	家庭用ブロードバンドルータの LAN ポートの様な使用イメージ。LAN 側機器を複数接続したい場合	片側を WAN ポート（PPPoE 含む）、片側を LAN ポートとして使用したり、フィルタリング設定を細かく設定したい場合
WAN ポート/LAN ポートとして使用	×	○
PPPoE 1 ポート/LAN 1 ポートとして使用	×	○

2.1 インターフェース設定

◆　ブリッジインターフェース設定

➢　ブリッジインターフェース(br0)

ブリッジ機能を利用する際に生成されるブリッジインターフェースの IP アドレスを設定します。

IP アドレス取得方法を「DHCP から取得」にした場合は IP アドレス、ネットマスクは空欄にしますが、ブリッジインターフェースを通常使用する際は、手動設定を設定してください。

出荷状態は「手動設定」で IP アドレスは 192.168.1.1 が設定されています。

※「ブリッジインターフェース(br0))は「共通インターフェース設定」でブリッジ「使用する」を選択した場合に表示されます。

※PPPoE 接続を使用する場合は、ブリッジインターフェースは使用できませんので、PPPoE 接続設定前に「ブリッジ使用しない」設定を行ってください。

第 2 章　インターフェース

2.1 インターフェース設定

◆ 個別インターフェース設定

➢ イーサネットインターフェース(ETHER0/eth0) / イーサネットインターフェース(ETHER1/eth1)の IP アドレスを設定します。

IP アドレス取得方法を「DHCP から取得」にした場合は IP アドレス、ネットマスクは空欄にします。

※出荷状態ではブリッジインターフェース設定が有効になっています。3G を使用せず、イーサネットポートを片側 WAN ポート、片側 LAN ポートとして使用したい場合は、P.14 を参照ください。

2.1 インターフェース設定

◆　共通インターフェース設定

デフォルトゲートウェイ、DNS サーバを設定します。ブリッジ「使用する」を選択すると、イーサネットインターフェース(ETHER0/eth0) / イーサネットインターフェース(ETHER1/eth1)をブリッジし、ブリッジインターフェース(br0)を作成します。これにより 2 つのイーサネットポートを 2 ポートのスイッチングハブのように利用することができます。

出荷状態はブリッジインターフェースを使用するになっています。

3G を使用する際は、デフォルトゲートウェイ、プライマリ DNS、セカンダリ DNS 設定は空欄で使用する事が可能です。(回線契約内容によっては設定が必要な場合がございます)

＜注意 1＞

IP アドレスを変更した場合、即時に反映されますので、WebUI でアクセスしているインターフェースの IP アドレスを変更した場合は「設定に失敗しました」と表示されます。

WebUI での設定を続けるには、パソコンのネットワーク設定等を確認し、変更後の IP アドレスに対して再度 WebUI 設定画面への接続を行ってください。

＜注意 2＞

「設定」ボタンを押下しても本体への保存は行われません。そのまま電源を抜くと設定した値は消えてしまいます。

設定した値を本体に保存する場合、WebUI の「停止・再起動」にて「本体再起動」または「本体シャットダウン」を行ってください。

2.2. 設定メモ（片側 WAN ポート、片側 LAN ポート）

第 2 章　インターフェース

2.1 インターフェース設定

★設定メモ：

3G を使用せず、イーサネットポートを片側 WAN ポート、片側 LAN ポートとして使用したい場合

＜設定例＞

ETHER0 を WAN ポート（SpreadRouter IP を DHCP から取得）

ETHER1 を LAN ポート（SpreadRouter IP 手動設定で 192.168.1.1、LAN 側ネットワークに対し DHCP サーバ有効）

■３Ｇ通信モジュール設定　回線接続「しない」に設定。

2.1 インターフェース設定

★設定メモ：

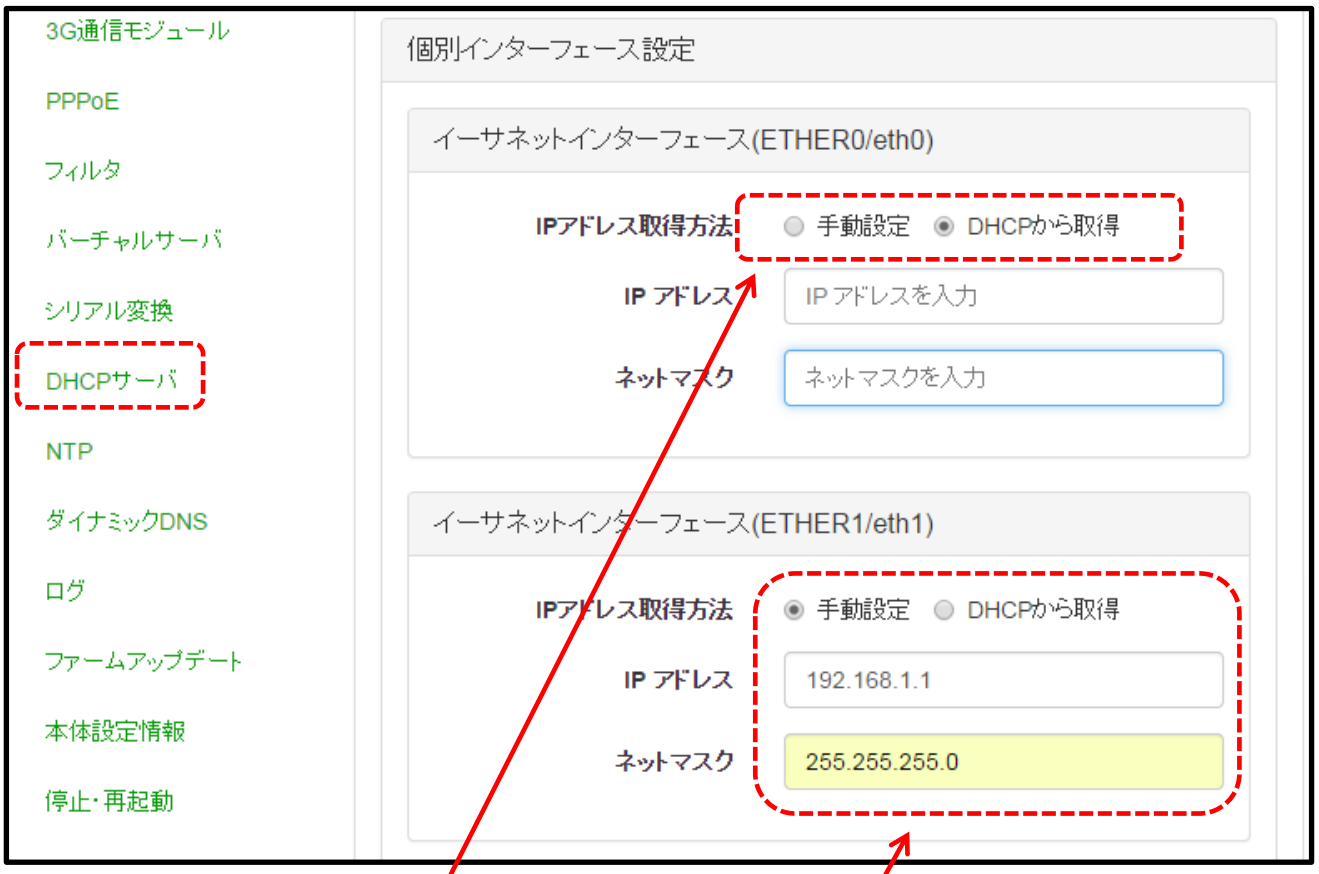
3G を使用せず、イーサネットポートを片側 WAN ポート、片側 LAN ポートとして使用したい場合

■インターフェース設定　ブリッジ「使用しない」に設定。

2.1 インターフェース設定

★設定メモ：

3G を使用せず、イーサネットポートを片側 WAN ポート、片側 LAN ポートとして使用したい場合



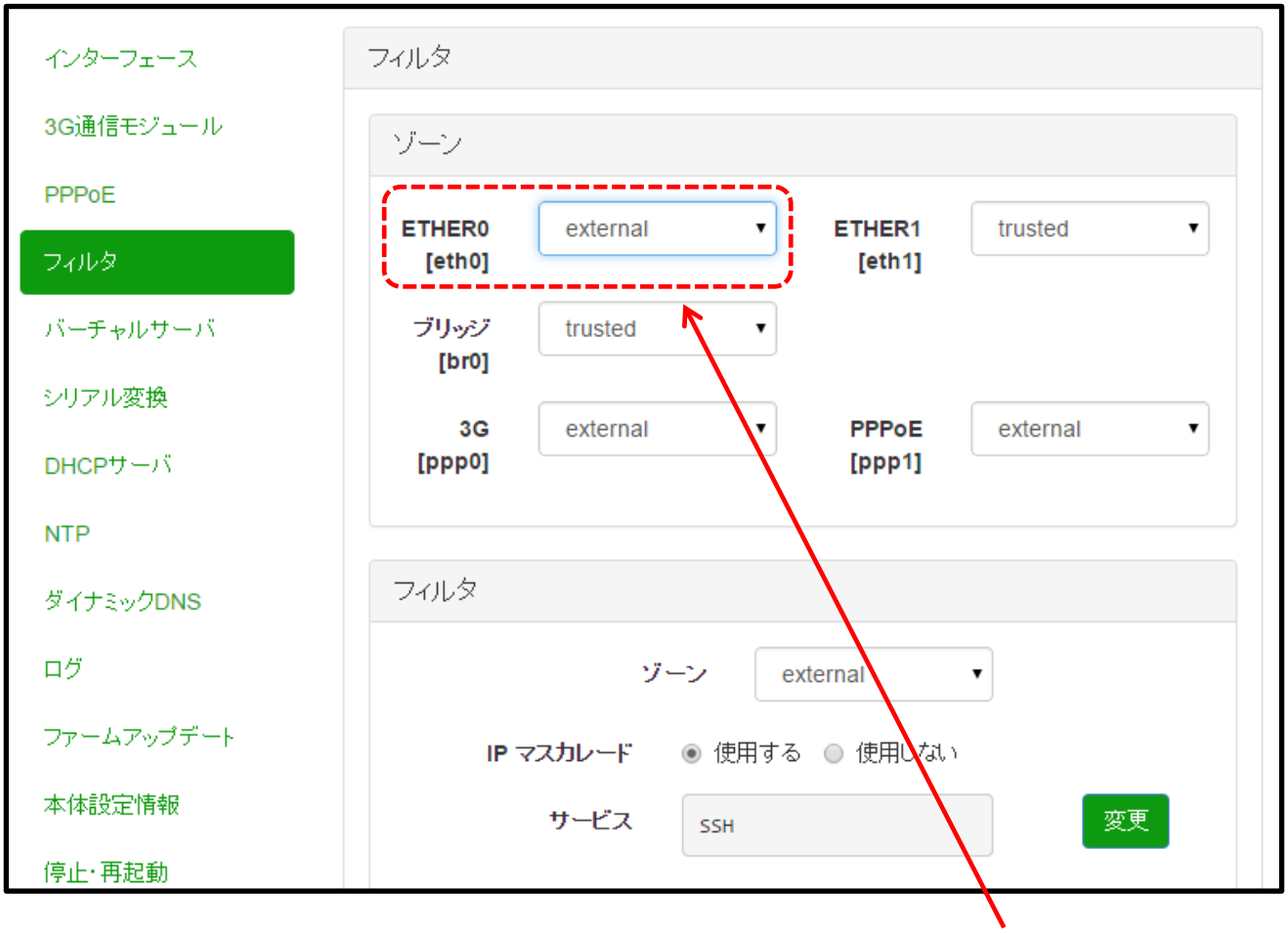
■WAN 側（ETHER0）は DHCP サーバから割当を受ける為、「DHCP」から取得

■LAN 側（ETHER1）は手動で 192.168.1.1 を割当。尚、LAN 側の IP アドレスのセグメントを変える場合は、
SpreadRouter の DHCP サーバ設定の割当も変更する事。（例えば LAN 側を 192.168.20.xx や、10.10.10.1 等への変更）

2.1 インターフェース設定

★設定メモ：

3G を使用せず、イーサネットポートを片側 WAN ポート、片側 LAN ポートとして使用したい場合



■ETHER0 を WAN 側ポートとして動作させるために、フィルタ設定でゾーンを「trusted」から「external」に変更する。

第３章

３Ｇ通信モジュール

第３章　３Ｇ通信モジュール

3.1 ３Ｇ通信モジュール状態

◆ 状態表示

現在使用中の接続状態を表示します。

接続状態は、接続中であれば「接続中」、接続されていなければ「未接続」と表示します。

アンテナレベルは、「最高」、「高」、「中」、「低」で表示します。

接続中であれば、取得中の IP アドレスが表示されます。

※各状態表示は自動更新されません。アンテナレベルの状態等を更新したい場合には、ブラウザの更新ボタンを押下するか、設定画面の別のメニューを開き、再度３Ｇ通信モジュール設定画面を開いてください、

＜アンテナレベル表示について＞

※本体動作中に SIM カードをセットした場合はアンテナレベルの更新は行われません。この場合、3G モジュール設定を行った段階でアンテナレベルが更新されます。

本体電源が OFF の状態で SIM カードをセットし、電源投入するとアンテナ状態は更新されます。

（本体の ANT-LED も同様です）

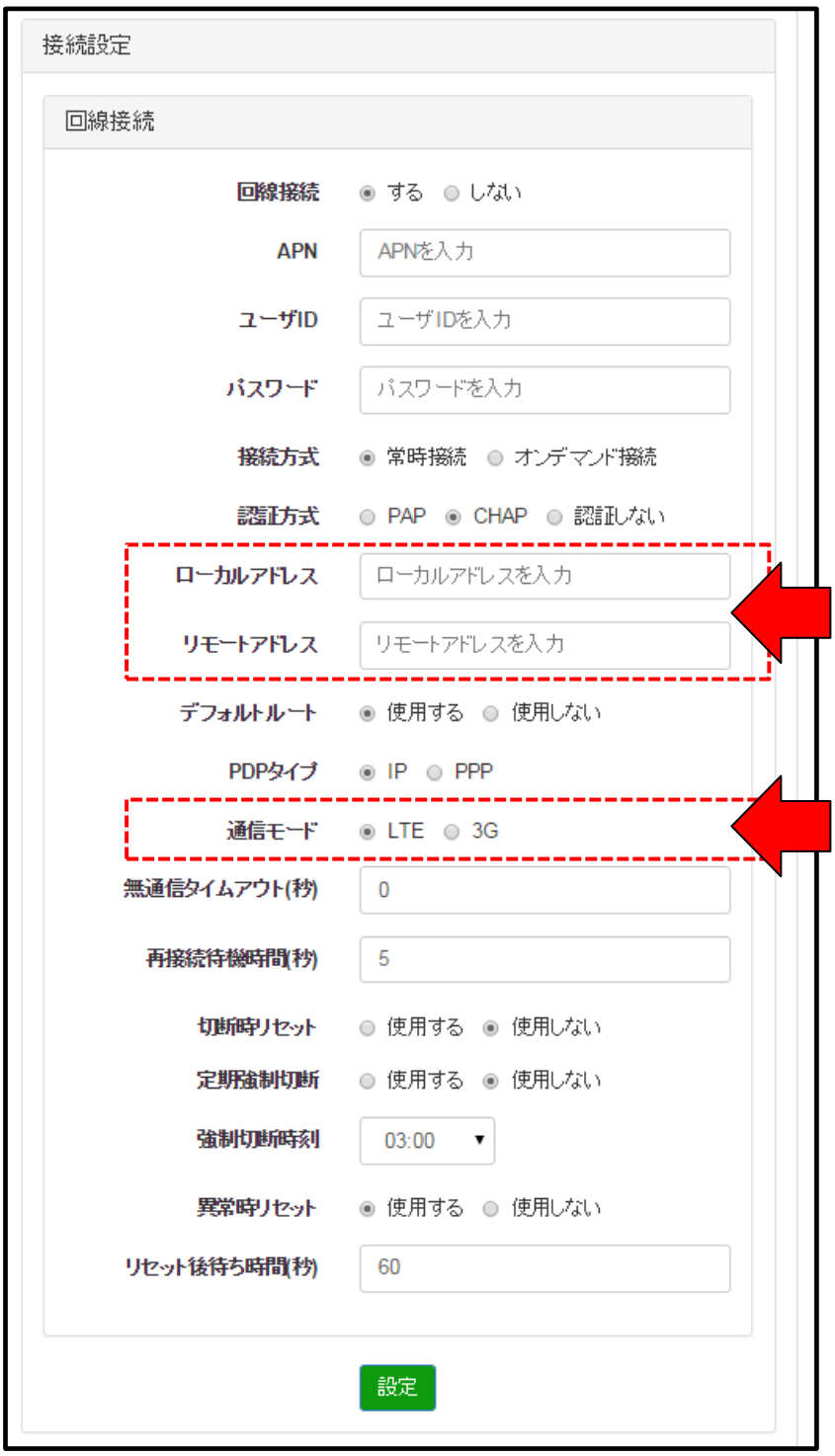
第 3 章　通信モジュール

3. 2 通信モジュール設定

◆　接続設定

通信モジュールの情報を設定します。

入力完了後、「設定」ボタンをクリックして設定内容を更新させます。



通常、空欄指定で可

LTE 対応製品のみ表示

3.2 通信モジュール設定

接続設定

項目	設定	説明	デフォルト
回線接続	する/しない	3G 回線接続を行う場合は、「する」にチェックを入れ、以降の設定を入力します。	しない
APN	APN 名を入力	契約している SIM カードの APN 名を設定します。	
ユーザ ID	ユーザ ID を入力	契約している SIM カードのユーザ ID を設定します。	
パスワード	パスワードを入力	契約している SIM カードのパスワードを設定します。	
接続方式	常時接続/ オンデマンド接続	常時接続：3G が切断されても自動再接続を行います。 オンデマンド接続：3G が切断された場合、LAN 側から外部にパケットが出るタイミングで 3G 接続を行います。※LAN 側から 3G へパケットが出ようとしない限り 3G 接続が行われません。	常時接続
認証方式	PAP/CHAP/認証しない	契約している SIM カードの認証方式を設定します。	CHAP
ローカルアドレス	契約 SIM 指定アドレス	通常空欄指定です。※次ページ参照	
リモートアドレス	契約 SIM 指定アドレス	通常空欄指定です。※次ページ参照	
デフォルトルート	使用する/使用しない	通常使用時は「使用する」を選択します。	使用する
PDP タイプ	IP/PPP	契約している SIM カードの PDP タイプを設定します。	IP
通信モード	LTE/3G	契約 SIM カードによって選択します。LTE 版のみ表示	
無通信タイムアウト（秒）	0 ～ 300	3G が一定時間無通信の場合、回線切断する時間を設定します。タイムアウトの時間は 0～300（秒）で設定します。常時接続の場合は、0 を設定します。	0
再接続待機時間（秒）	0 ～ 300	3G が再接続するまでの待機時間を 0～300（秒）で設定します。	5
切断時リセット	使用する/使用しない	回線切断時に通信モジュールのリセットを行うか選択します。	使用しない
定期強制切断	使用する/使用しない	定期的に 3G 回線を強制切断するか選択します。	使用しない
強制切断時刻（時）	0:00 ～ 23:00	定期強制切断を使用時の強制切断時刻を選択します。	3:00
異常時リセット	使用する/使用しない	通信モジュール異常時にリセットを行うかの選択をします。	使用する
リセット後待ち時間（秒）	0 ～ 300	切断時および異常時に行うリセット後の待ち時間を 0～300（秒）で設定します。 ※短い時間を設定した場合、モジュール状態によっては復旧処理で失敗を繰り返すことがあります。	60

※APN、ユーザ ID、パスワード、認証方式、PDP タイプは、使用する SIM の情報に合わせた設定をしてください。

3.2 通信モジュール設定

＜注意１＞

3G 設定を変更し、「設定」ボタンを押下した際、即時反映される項目と再起動後に有効になるものがございます。
既に 3G 設定済の SIM カードを別の SIM カードに変更した場合、即時反映できない場合などがあります。
各設定を反映させるには、再起動を行ってください。

＜注意２＞

「設定」ボタンを押下しても本体への保存は行われません。そのまま電源を抜くと設定した値は消えてしまいます。
設定した値を本体に保存する場合、WebUI の「停止・再起動」にて「本体再起動」または「本体シャットダウン」を行ってください。

＜注意３＞

ローカルアドレス、リモートアドレスは、SIM カード契約を行った際に、本機に設定を行う必要がある場合に、入力します。尚、弊社供給の SIM カードで固定 IP アドレス契約の場合は、自動で固定アドレスを割り当てる為、通常入力不要です。

＜注意４＞

LTE 対応製品 SpreadRouter の場合、LTE-SIM カードと 3G-SIM カードを選択する項目が表示されます。SIM カードが LTE 回線対応の場合、LTE にチェックを行います。SIM カードが 3G 回線契約の場合は、3G にチェックを入れてください。（設定する APN に依存します）

第 4 章

PPPoE

第 4 章　PPPoE

4. 1 PPPoE 設定

◆　状態表示

現在使用中の接続状態を表示します。

接続状態は接続中であれば「接続中」、接続されていなければ「未接続」と表示します。

取得 IP アドレスには ppp1 に設定された IP アドレスを表示します。

第 4 章　PPPoE

4.1 PPPoE 設定

◆　接続設定

PPPoE の接続情報を設定します。

入力完了後、「設定」ボタンを押下して設定を更新します。

接続設定

項目	設定	説明	デフォルト
回線接続	する/しない	PPPoE 接続を行う場合は、「する」にチェックを入れ、以降の設定を入力します。	しない
インターフェース	eth0(ETHER0)/eth1(ETHER1)	使用するインターフェース「eth0」「eth1」を選択します。	eth0
MTU	MTU 値を入力	デフォルト値 1454 です。	1454
ユーザ ID	ユーザ ID を入力	契約している SIM カードのユーザ ID を設定します。	
パスワード	パスワードを入力	契約している SIM カードのパスワードを設定します。	
デフォルトルート	使用する/使用しない	通常使用時は「使用する」を選択します。	使用する

※ブリッジインターフェース使用時 PPPoE 接続は使用できません。

第 4 章　PPPoE

4.1 PPPoE 設定

＜注意１＞

「設定」ボタンを押下すると変更した設定は即時反映されますが、本体への保存は行われません。そのまま電源を抜くと設定した値は消えてしまいます。

設定した値を本体に保存する場合、WebUI の「停止・再起動」にて「本体再起動」または「本体シャットダウン」を行ってください。

第５章

フィルタ

第5章　フィルタ

5.1 フィルタ設定

◆　ゾーン

インターフェースが属するゾーンを設定します。

ゾーンは trusted / internal /external から選択します。

※出荷状態のフィルタゾーン設定

3G と PPPoE は外向きのネットワークに設定するため、「external」を選択します。

ブリッジ/ETHER0/ETHER1 は全て内向きのネットワークに設定するため、「trusted」または「internal」を選択します。

主な用途としては、ETHER0 または ETHER1 を WAN ポートとして使用する場合、「trusted」を「external」に設定変更します。

第 5 章　フィルタ

5.1 フィルタ設定

◆　フィルタ

ゾーンを選択して、IP マスカレード、許可するサービス、フィルタルールの設定を行います。

項目	設定	主な設定内容
ゾーン	external/internal	設定するゾーンを選択します。(主に external)
IP マスカレード	使用する/使用しない	通常 external 選択時は IP マスカレード使用するを選択します。
サービス	特定サービスを選択	選択された内向きのコネクションのみ Accept します。
ルール	プロトコル、ターゲット、アドレス、ポートを設定	サービスで選択できないユーザー指定のルールを設定します。 主な用途は外部へ WebUI アクセスの許可、外部からのシリアル変換サーバ許可等。

5.1 フィルタ設定

デフォルトでは各ゾーンは以下のように設定されています。

ゾーン名	インターフェース	サービス	マスカレード	備考
trusted	ブリッジ(br0) ETHER0(eth0) ETHER1(eth1)			全ての内向きパケットを受入（Accept） ※設定変更不可
internal	なし	dhcpv6-client, ipp-client, mdns, samba-client, ssh	使用しない	選択された内向きのコネクションのみ Accept （内部ネットワーク用）
external	3G(ppp0) PPPoE(ppp1)	ssh 使用ポート	使用する	選択された内向きのコネクションのみ Accept （IP Masquerade が有効な外部ネットワーク）

※trusted の設定を変更することはできません。eth0、eth1、br0 にフィルタを設定したい場合はゾーンを internal に変更してフィルタを設定してください。

5.1 フィルタ設定

➢ サービスの変更

「変更」ボタンをクリックすると以下のようなサービスの一覧が表示されますので通信を許可したいサービスをチェックし「OK」をクリックします。

※上記は一般的なサービスのポート番号であり、本製品自身が搭載している機能として記載しているわけではありません。

※上記画面での SSH サービスとはポート番号 22 番の一般的なデフォルトポート番号になります。

5.1 フィルタ設定

➢ ルール追加

「+追加ボタン」を押すと以下のような画面がプロトコル、ポート等を入力する画面が表示されますので必要な項目を入力して「OK」をクリックします。

- プロトコル：「TCP」「UDP」から選択します。
- ターゲット：「accept」「drop」「reject」から選択します。
- 宛先アドレス：宛先アドレス指定する場合に設定します。
- 宛先ポート：宛先ポート番号（1～65535）を設定します。
- 送信元アドレス：送信元アドレスを指定する場合に設定します。

※設定可能な入力項目の組み合わせは以下の通りです。

プロトコル	ターゲット	宛先アドレス	宛先ポート	送信元アドレス
○	○	―	○	―
○	○	○	○	―
○	○	○	○	○

➢ ターゲットについて

accept：許可

drop　：破棄　パケットを全て破棄します。

reject：拒絶　パケットを破棄した事を送信者に返答します。

5.1 フィルタ設定

v1.05 の場合、SSH ポートが 10022 番です。

- ルールの編集

  設定済みのルールを編集するには編集ボタンをクリックします。設定内容が表示されますので変更した項目を変更して「OK」をクリックします。

- ルールの削除

  設定済みのルールを削除するには削除ボタンをクリックします。

◆ 設定の反映

インターフェースのゾーン割当、サービス変更、ルールの追加等の設定を行った場合、これだけでは設定は反映されていません。最後に「設定」ボタンをクリックすることで設定が反映されます。

＜注意１＞

「設定」ボタンを押下すると変更した設定は即時反映されますが、本体への保存は行われません。そのまま電源を抜くと設定した値は消えてしまいます。

設定した値を本体に保存する場合、WebUI の「停止・再起動」にて「本体再起動」または「本体シャットダウン」を行ってください。

＜注意２＞

シリアル変換設定で外部からアクセスする場合は、フィルタ設定で該当ポートを Accept する必要があります。

（設定の際は、TCP or UDP、Accept、宛先ポートの指定を行ってください。「宛先」と「送信元」アドレスは不要）

第 6 章

バーチャルサーバ

第 6 章　バーチャルサーバ

6.1 バーチャルサーバ設定

◆　バーチャルサーバ

バーチャルサーバの設定追加、編集、削除を行います。

- ゾーン　：「external」「internal」から選択します。

※ゾーンは、「第 5 章 フィルタ」より設定したゾーンに合わせて選択します。

第 6 章　バーチャルサーバ

6.1 バーチャルサーバ設定

➢ バーチャルサーバのルール追加

「ゾーン」を選択した後に、「追加」をクリックすることにより、新規追加画面が表示されます。

入力が完了したら「OK」をクリックし、バーチャルサーバ画面より「設定」をクリックすることで、設定内容が反映されます。

- プロトコル　：「TCP」「UDP」より選択します。
- 仮想サーバアドレス　：公開するサーバの IP アドレスを IPv4 アドレス形式で入力します。
- 仮想サーバポート　：公開する仮想サーバのポート番号を 1～65535 までの値で入力します。
- 実サーバアドレス　：実サーバの IP アドレスを IPv4 アドレス形式で入力します。
- 実サーバポート　：実サーバのポート番号を 1～65535 までの値で入力します。

6.1 バーチャルサーバ設定

＜注意＞

※バーチャルサーバの設定で、入力できる項目の組み合わせは下記になります。

プロトコル	仮想サーバ アドレス	仮想サーバ ポート	実サーバ アドレス	実サーバ ポート
○		○	○	○
○	○	○	○	○
○	○	○	○	-

6.1 バーチャルサーバ設定

➢ バーチャルサーバのルール編集

追加したルールの編集を行います。

編集するルールの「編集」マークをクリックすることにより、変更画面が表示されます。

編集したい項目を変更し、「OK」をクリックします。バーチャルサーバ画面より「設定」をクリックすることで、設定内容が反映されます。

※編集時は上段に「値に誤りがあります」と表示されることもありますが、そのまま編集可能です。

- プロトコル　：「TCP」「UDP」より選択します。
- 仮想サーバアドレス　：公開するサーバの IP アドレスを IPv4 アドレス形式で入力します。
- 仮想サーバポート　：公開する仮想サーバのポート番号を 1～65535 までの値で入力します。
- 実サーバアドレス　：実サーバの IP アドレスを IPv4 アドレス形式で入力します。
- 実サーバポート　：実サーバのポート番号を 1～65535 までの値で入力します。

6.1 バーチャルサーバ設定

- バーチャルサーバのルール削除

  追加したルールの削除を行います。

  削除するルールの「削除」マークをクリックすることにより、削除画面が表示されます。

  削除するには「OK」をクリックします。バーチャルサーバ画面より「設定」をクリックすることで、設定内容が削除されます。

＜注意１＞

「設定」ボタンを押下すると変更した設定は即時反映されますが、本体への保存は行われません。そのまま電源を抜くと設定した値は消えてしまいます。

設定した値を本体に保存する場合、WebUI の「停止・再起動」にて「本体再起動」または「本体シャットダウン」を行ってください。

第７章

シリアル変換

第 7 章　シリアル変換

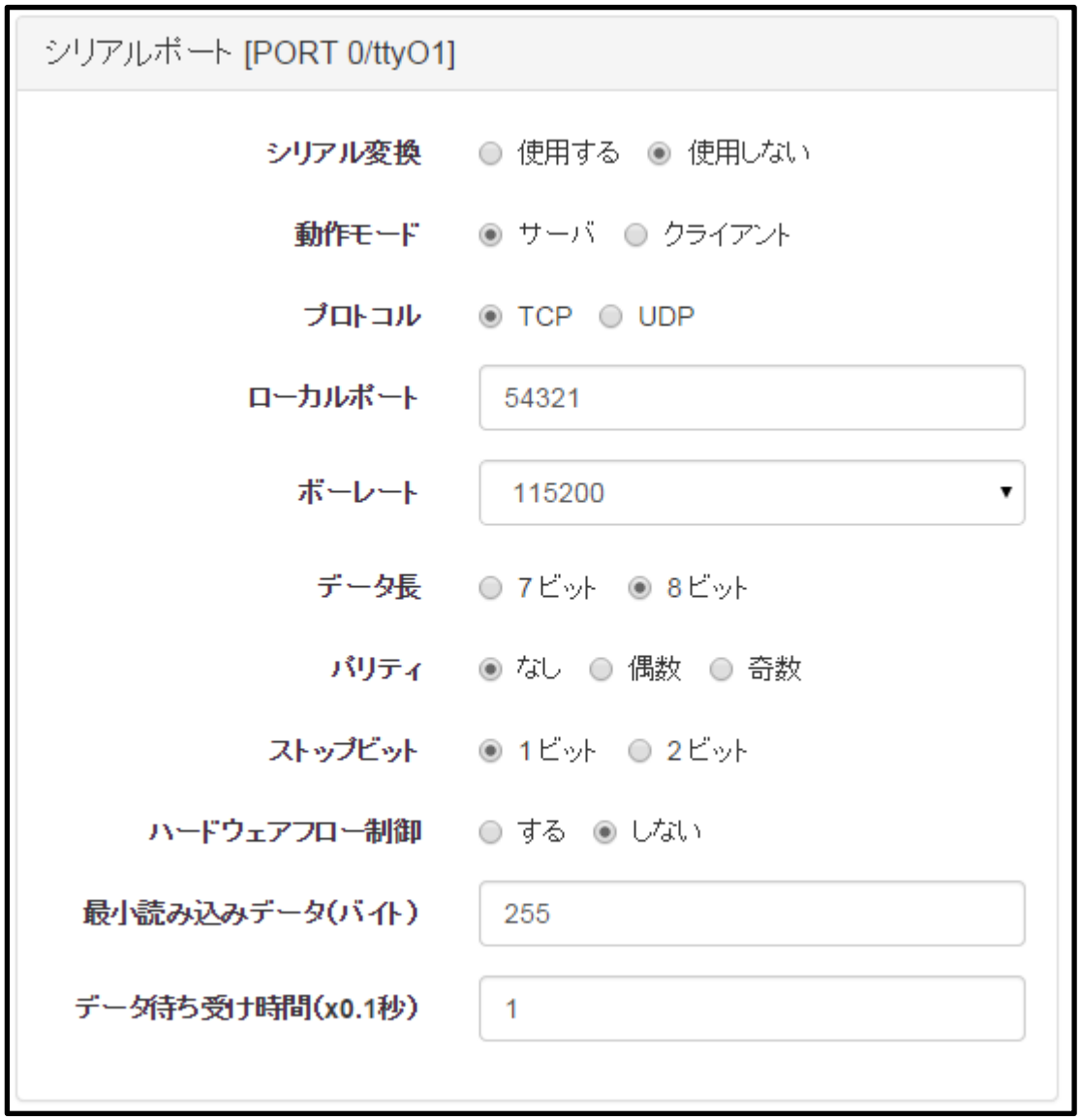
7.1 シリアル変換設定

◆　シリアル変換設定

シリアルと TCP または UDP のプロトコル変換機能を利用する場合に設定します。

➢　シリアルポート(PORT 0/ttyO1)

シリアルポート(PORT 0/ttyO1)を利用する場合に設定します。



第 7 章　シリアル変換

7.1 シリアル変換設定

項目	設定	説明	デフォルト
シリアル変換	使用する/使用しない	シリアル変換機能を使用する場合は「使用する」を選択し、以降の項目を設定します。	しない
動作モード	サーバ/クライアント	サーバ：SpreadRouter が指定ポートで待受けるモード。（ソケットサーバ機能） クライアント：SpreadRouter が指定 IP アドレス・ポートに接続するモード。（ソケットクライアント）	サーバ
プロトコル	TCP/UDP	通信プロトコルを「TCP」「UDP」のどちらを利用するか選択します。	TCP
ローカルポート	ポート番号	サーバ動作時の待ち受けポート（1～65535）、UDP クライアント時の送信元ポート（1～65535）を意味します。(TCP クライアント時はこの設定は無視されます。） ※SpreadRouter 内部で使用中のポートは設定できません。	54321 コンソールは空欄
接続先アドレス	IP アドレス	クライアント動作時の接続先 IP アドレスを設定します。（サーバ動作時はこの設定は無視されます。） ※ホスト名指定は不可	
接続先ポート	ポート番号	クライアント動作時の接続先ポート（1～65535）を設定します。（サーバ動作時はこの設定は無視されます。）	
最小読み込みデータ（バイト） ※注記	読込バイト数	シリアルデータを読み込む際の最小データサイズを設定します。	255
データ待ち受け時間（x0.1 秒）	待ち時間	最小読み込みデータに満たない場合、ここで設定した時間データを受信しなければデータを読み込みます。	1

ボーレート/データ長/パリティ/ストップビット/ハードウェアフロー制御は接続するシリアル端末の仕様に合わせて設定します。

7.1 シリアル変換設定

ボーレートに関する設定は下表のとおりです

	PORT0(tty01)	CONSOLE(tty00)
SpreadRouter-F	1200bps～921600bps	1200bps～460800bps
SpreadRouter-R	1200bps～460800bps	1200bps～460800bps

- コンソールポート(CONSOLE/tty00)

  コンソールポート(CONSOLE/tty00)を利用する場合に設定します。コンソールポートをシリアル変換機能で利用するには事前にブートローダより Linux コンソール出力を止めるための設定を行う必要があります。設定手順については別紙「コンソールポートのアプリ利用.pdf」を参照ください。。設定項目は「シリアルポート(Port 0/tty01)」と同様です。

  （※CONSOLE ポートをシリアル変換機能した場合、電源投入時や再起動時に必ずブートメッセージが 115200bps で出力されます。このメッセージにより接続されている外部機器が異常動作にならないことをご確認の上、ご使用ください。）

＜注意１＞

「設定」ボタンを押下すると変更した設定は即時反映されますが、本体への保存は行われません。そのまま電源を抜くと設定した値は消えてしまいます。

設定した値を本体に保存する場合、WebUI の「停止・再起動」にて「本体再起動」または「本体シャットダウン」を行ってください。

＜注意２＞

シリアル変換のサーバモードで 3G や WAN ポート側（external ゾーン）からアクセスする場合は、設定したローカルポート番号をフィルタ設定で「Accept」してください。

※注記　「最小読み込みデータ（バイト）」について

シリアルから SpreadRouter にデータが送られてきたものを、「最小読み込みデータ」バイト数を受け取って TCP 側に送信するという意味になります。 例えば　10　という設定の時に、シリアル側から途切れ無く

“abcdefg1234567890AAAAABBBBBCCCCCDDDDDEEEEEFFFFF”

を受信した場合、“abcdefg123” の時点で TCP 側に 1 つのパケットとして送信することになります。そして 2 パケット目に残りの“4567890AAAAABBBBBCCCCCDDDDDEEEEEFFFFF”が送信されます。

また、最小読み込みデータに満たないデータを受信した場合は、「データ待ち受け時間」を過ぎた時点で送信されます。

これが、SpreadRouter のシリアル変換機能でのシリアルから TCP への送信仕様になります。

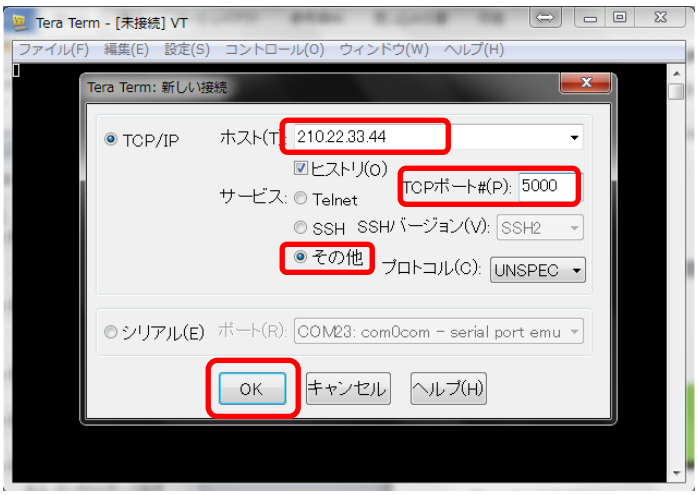
シリアルからのデータが途切れ無く多く出てくる場合は、「最小読み込みデータ」を最大の 255 に設定してください。

7.1 シリアル変換設定

■シリアル疎通確認方法

シリアル変換設定を行い、通信が出来ない場合の切り分け方法として以下のこと試してください。(TCP サーバモード時)

フリーウェアの TeraTerm を起動し、接続先の IP アドレス、ポート番号を指定し接続を行います。



接続を行い下記の様に接続に失敗する場合。

以下の事が考えられます。

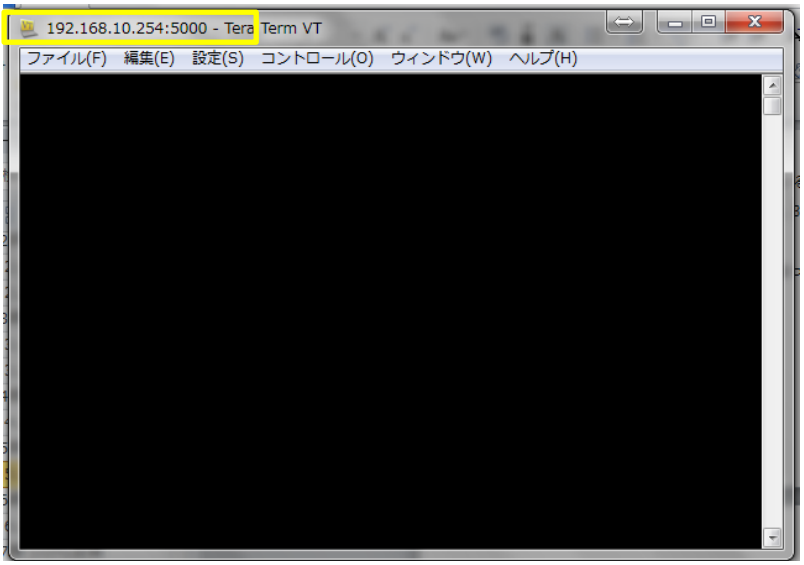
・IP アドレス・ポートの設定が間違っている。

・IP アドレス・ポートの設定は正しいが、3G 経由（外部）からのアクセスの場合、フィルタ設定で該当ポートを Accept する設定が不足している。

・設定が TCP サーバモード以外の設定になっている。

7.1 シリアル変換設定

下記の様に接続は出来たが、シリアルにデータが流れない場合



以下の事が考えられます。

・シリアル設定のボーレートやストップビット設定等があっていない。

・PORT0 と CONSOLE が間違っている

・シリアルケーブルの相手機器とのピンアサインが異なっている

・RS232C（SpreadRouter-R）モデルに、RS485 ケーブル（GND/T+/T-）を接続している

・RS485（SpreadRouter-F）モデルに、RS232 シリアルケーブルを接続している

・CONSOLE 使用時に、DipSW でブートメニューから CONSOLE ポートのアプリケーション使用に設定を変えていない

第 8 章

DCHP

第 8 章　DHCP

8.1 DHCP 設定

◆ DHCP 設定

DHCP サーバ機能を設定します。

割当 IP アドレスには、DHCP クライアントに割り当てる IP アドレスの範囲を指定します。

DHCP サーバ機能を行わないようにするには、DHCP「無効にする」を選択します。

- DHCP サーバ：「有効にする」「無効にする」から選択します。
- 割当 IP アドレス：

  DHCP クライアントに割り当てる IP アドレスの範囲を IPv4 アドレス形式で入力します。

出荷時設定は、DHCP サーバは有効です。割当 IP アドレスは、192.168.1.100 ～ 192.168.1.200 です。

＜注意 1＞

「設定」ボタンを押下すると変更した設定は即時反映されますが、本体への保存は行われません。そのまま電源を抜くと設定した値は消えてしまいます。

設定した値を本体に保存する場合、WebUI の「停止・再起動」にて「本体再起動」または「本体シャットダウン」を行ってください。

第 9 章

NTP

第 9 章　NTP

9.1 NTP 設定

◆　NTP 設定

NTP 設定には、NTP に準拠した「NTP 時刻同期」と、１日１回時刻合わせを行う「定期時刻合わせ」の２種類が存在します。

デフォルトでは「NTP 時刻同期」は使用しない、「**定期時刻合わせ**」は**使用する**設定です。

下図はデフォルト状態の画面です。

デフォルトではプライマリ NTP として「ntp.nict.jp」が設定されています。プライマリ NTP、セカンダリ NTP は IP アドレスまたは FQDN で設定可能です。時刻合わせを行う時間を設定します。

定期時刻合わせを「使用しない」に合わせると、下記画面に変わります。

第 9 章　NTP

9.1 NTP 設定

NTP での時刻同期を行いたい場合は、「NTP 時刻同期」を使用するを選択します。

NTP により時刻同期を行うかを設定します。

デフォルトではプライマリ NTP として「ntp.nict.jp」が設定されていますが、出荷時設定では時刻同期を使用しない設定です。

プライマリ NTP、セカンダリ NTP は IP アドレスまたは FQDN で設定可能です。

時刻同期を行うには、NTP 時刻同期を「使用する」を選択します。

＜注意１＞

「設定」ボタンを押下すると変更した設定は即時反映されますが、本体への保存は行われません。そのまま電源を抜くと設定した値は消えてしまいます。

設定した値を本体に保存する場合、WebUI の「停止・再起動」にて「本体再起動」または「本体シャットダウン」を行ってください。

＜注意２＞

NTP 時刻同期を行う場合、NTP 仕様に沿った動作になるためパケット量が増加します。

3G 回線プランが従量制プランの場合、パケット超過になることもございますのでご注意ください。

パケットを抑えたい場合には、１日１回の**定期時刻合わせ**をご使用ください。

＜メモ＞

本体に内蔵されている時計用電池は通電無しの状態で約 5 年間保持されます。

第 10 章

ダイナミック DNS

第 10 章　ダイナミック DNS

10.1 ダイナミック DNS 設定

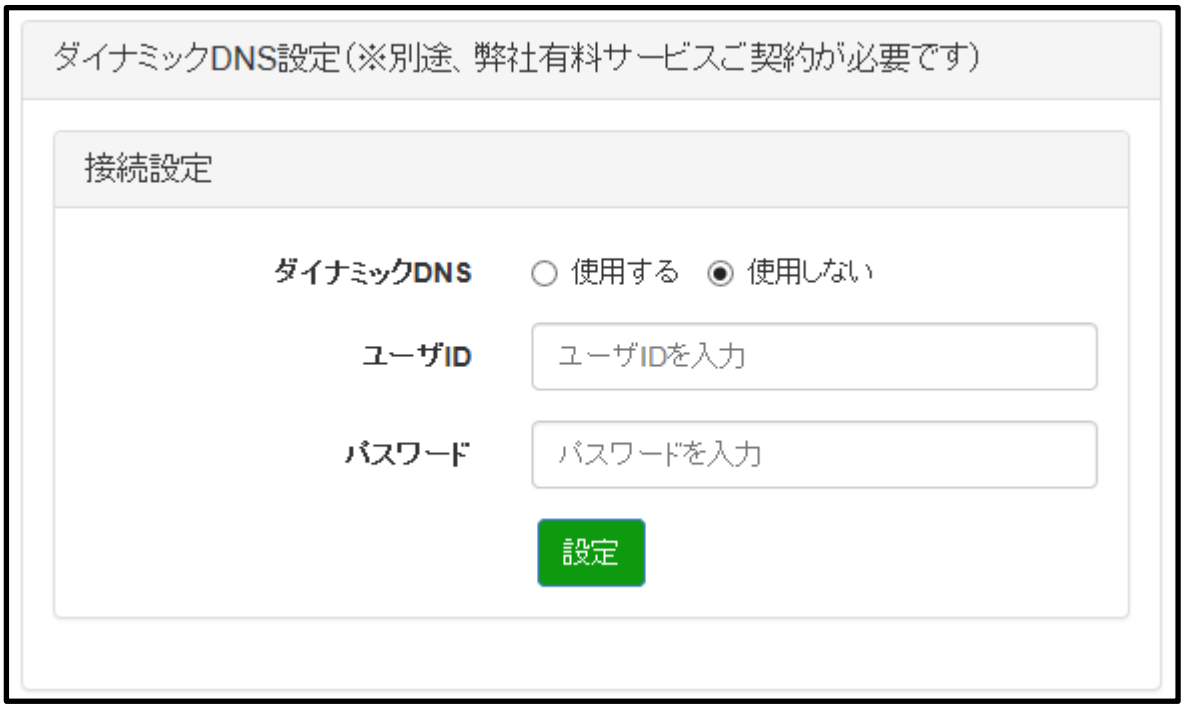
弊社有料サービスのダイナミック DNS に対応した機能です。

通信モジュール接続時に、ダイナミック DNS サーバに対して登録を行います。

ダイナミック DNS サービスを使用するには別途契約が必要です。サービスご利用に関するお問い合わせは弊社サポート窓口までご連絡願います。

➢ 接続設定

ダイナミック DNS のユーザ ID とパスワードを設定します。



- ダイナミック DNS　：弊社提供ダイナミック DNS サービスの「使用する」「使用しない」を選択します。
- ユーザ ID　　：弊社提供ダイナミック DNS サービスを契約した際のユーザ ID を入力します。
- パスワード　　：弊社提供 DNS サービスを契約した際のパスワードを入力します。

＜注意１＞

「設定」ボタンを押下すると変更した設定は即時反映されますが、本体への保存は行われません。そのまま電源を抜くと設定した値は消えてしまいます。

設定した値を本体に保存する場合、WebUI の「停止・再起動」にて「本体再起動」または「本体シャットダウン」を行ってください。

第11章

ログ

第 11 章　ログ

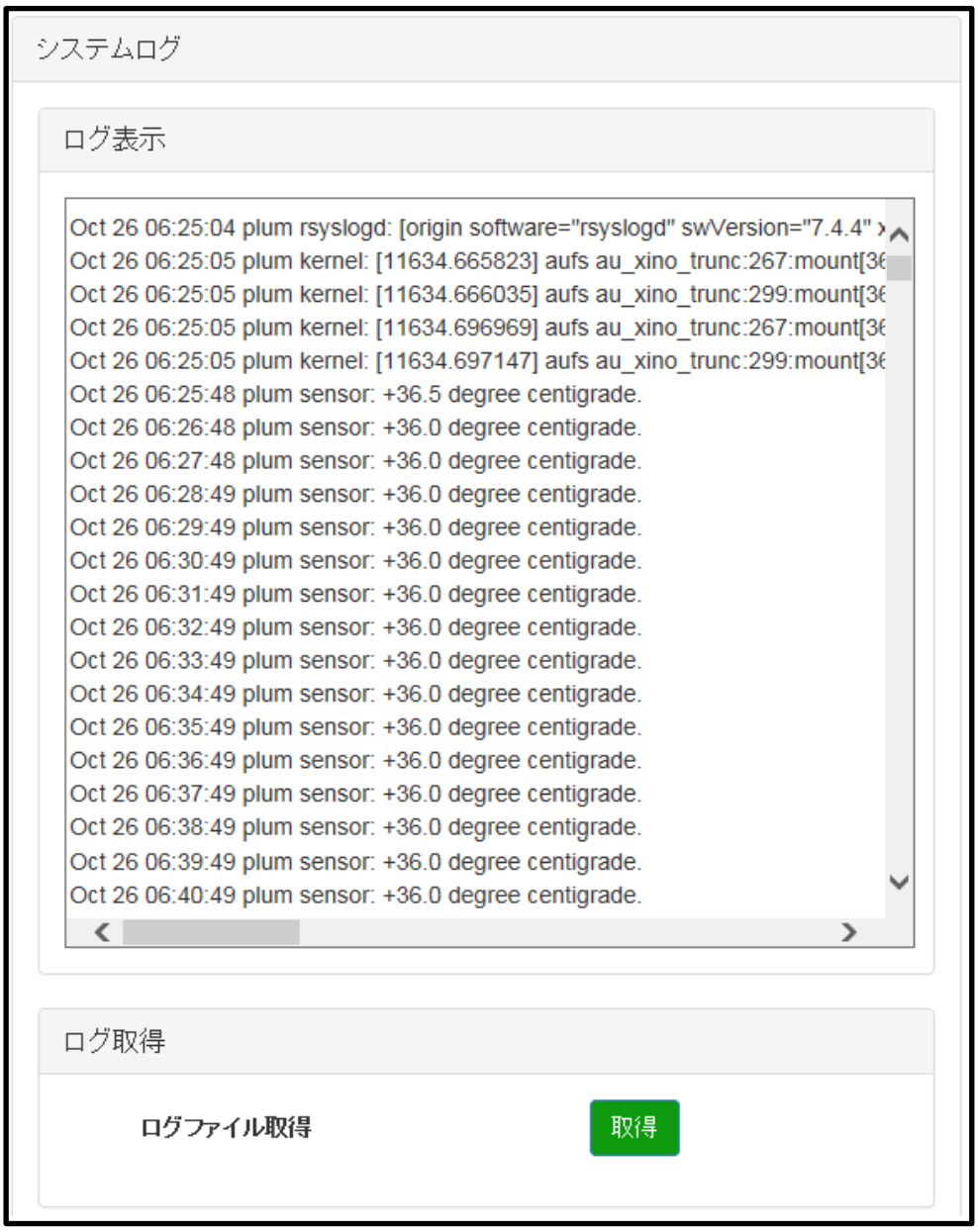
11.1 ログ表示

◆　ログ表示

WebUI 上でログ（/var/log/syslog）を表示して確認することができます。

◆　ログ取得

「取得」によりログファイル（/var/log/syslog）をダウンロードすることができます。



※過去のログに関しては直近 6 日分を本体内部に保存してあります。取得するには ssh 等で接続し、/var/log ディレクトリ内のファイルを取得してください。

第 12 章

ファームアップデート

第 12 章　ファームアップデート

12.1 ファームアップデート

◆　ファームバージョン

現在使用中のファームウェアのバージョンを表示して確認することができます。

◆　ファームアップデート

SpreadRouter 本体のファームウェアの更新を行います。

➢　ファームウェアアップロード

パソコン上のファームウェアイメージファイルを、WebUI を経由して本装置に送信します。

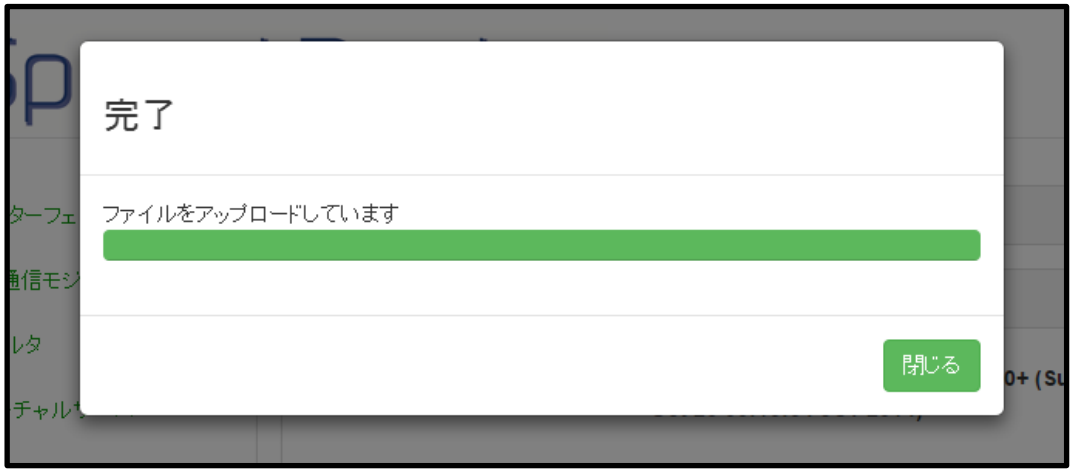
「設定」ボタンをクリックして更新するファームウェアを SpreadRouter 本体にアップロードします。

第 12 章　ファームアップデート

12.1 ファームアップデート

- ファームウェアアップロード完了

  ファームウェアアップロード完了後には、「完了」と表示されます。



- ファームウェアアップデート

  ファームウェアの送信に成功すると、ファイルサイズと MD5 値が表示されます。

  MD5 値が正しければ、「設定」をクリックし、ファームウェアのアップデートを実行します。

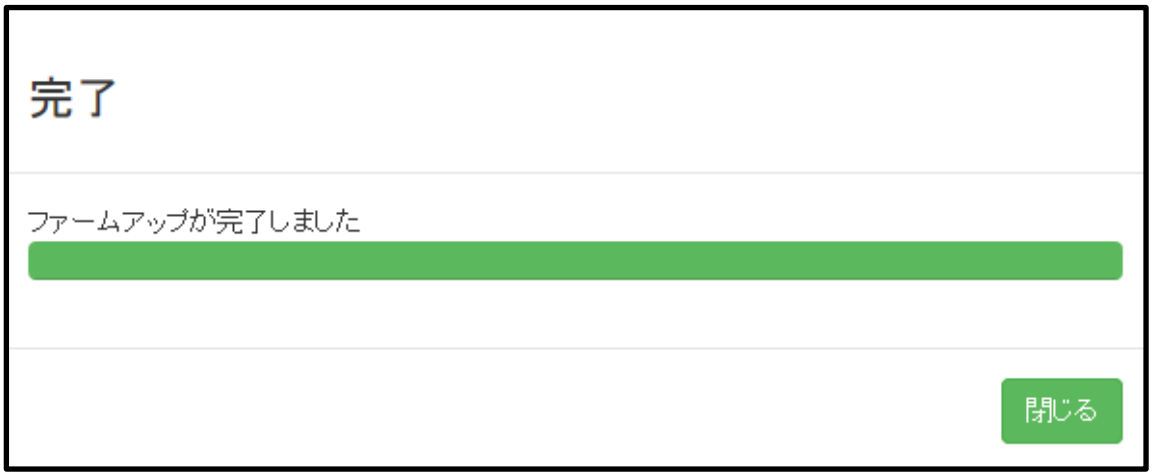
※ファームウェアは 60MB 以上のサイズがありますので、3G 経由の遠隔からの更新の場合、30 分～1 時間以上アップロードに時間が掛かる可能性がございます。

また、3G 回線プランが従量制の場合、パケット超過になる可能性がございますので、更新の際には十分ご注意願います。

12.1 ファームアップデート

➢ ファームウェアアップデート完了

ファームウェアアップデート完了後には、「ファームアップが完了しました」と表示されます。



＜注意＞

「ファームアップが完了しました」メッセージが出ても、[閉じる]ボタンが表示されない場合があります。その際には、ブラウザの更新ボタンを押下してください。ファームアップは完了していますので、SpreadRouter 本体の再起動へ進んでください。

➢ SpreadRouter 本体の再起動

『第 14 章停止・再起動』より、SpreadRouter 本体の再起動を実施します。

再起動後、ファームウェアが更新されていることを確認します。

第 13 章

本体設定情報

第 13 章　本体設定情報

13.1 設定の保存・復帰・初期化

設定の保存・復帰の機能は、1 台の SpreadRouter 本体の設定情報を他の本体にコピーすることができ、クローンを作成することができます。このため共通化できる設定情報を一度作成しておくことで、初期設定の簡略化が可能になります。

◆　設定の保存

設定画面で変更した設定内容をファイルとしてパソコンにダウンロードし保存する機能です。

「保存」ボタン押下でダウンロードを開始します。

13.1 設定の保存・復帰・初期化

◆　設定の復帰

「設定の保存」でダウンロードした設定ファイルを本体にアップロードし設定を復元します。

「ファイルを選択」ボタンでアップロードする設定ファイル選択し、「復帰」ボタンを押下でファイルのアップロードを開始します。

※設定ファイルアップロード後、設定を反映させるには SpreadRouter 本体の再起動を行ってください。

ファームウェアバージョンが異なったものに対して、本体設定情報の「設定の復帰」を行った場合、

全て反映されない可能性があります。

事前に必ず、同じファームウェアバージョンで設定を行った状態で、「設定の保存」を行ってください。

※設定の復帰を行った際、画面上は失敗しましたと表示されることがありますが、読込ファイルが正しい場合は再起動後に設定が反映されています。

◆　設定の初期化

設定画面で変更した設定を消去し設定データをデフォルト値に戻します。

「初期化」ボタンで設定データの消去を行います。

※設定の初期化を有効にするには SpreadRouter 本体の再起動が必要です。

第 14 章

停止・再起動

第 14 章　停止・再起動

14.1 停止・再起動設定

◆　即時停止・再起動

「停止」で SpreadRouter 本体をシャットダウンします。

「再起動」で SpreadRouter 本体の再起動を行います。

※「停止」または「再起動」により行われるシャットダウン処理により各設定情報が保存されます。

◆　定期リブート

1 日に 1 回の定期リブートを行うかを設定します。

定期リブート「使用する」を選択し、再起動時間（0:00～23:00 ※1 時間単位）を設定すると設定した時間に再起動を行います。

※出荷設定は定期リブートを使用する設定です。長期運用にてご使用の場合は、定期リブート機能を使用することを推奨いたします。

第 15 章

日付・時刻

第 15 章　日付・時刻

15.1 日付・時刻設定

◆　日付・時刻設定

日付・時刻設定では、システム時刻の変更を行います。

「日付」の年、月、日および、「時刻」の時、分、秒の項目入力が完了した後「設定」ボタンをクリックして変更内容を更新させます。

- 年 ： 2000～2036 までの範囲で設定します。
- 月 ： 1～12 までの範囲で設定します。
- 日 ：1～31 までの範囲で設定します。
- 時 ：0～23 までの範囲で設定します。
- 分 ：0～59 までの範囲で設定します。
- 秒 ：0～59 までの範囲で設定します。

尚、本体に内蔵されている時計用電池は通電無しの状態で約 5 年間保持されます。

第 16 章

本体設定

第 16 章　本体設定

16.1 本体設定

◆　設定画面のパスワード変更

Web 設定画面のログインパスワードを変更します。(半角英数記号 16 文字　※使用可能記号は"'¥以外)

ユーザは「admin」固定で変更できません。

◆　Web 設定画面ポート変更

Web 設定画面のポート番号を変更したい場合にポート番号 (1～65535) を指定します。設定は即時反映されますので、WebUI での設定を続けるには変更後のポートに再接続してください。

※使用中ポートは設定できません。

※デフォルト使用中ポート一覧

TCP : 111 , 80 , 8080 , 4112 , 53 , 22

UDP : 53 , 67 , 111 , 123

その他、動的に割り当てられるポートもございますのでご注意願います。

第 16 章　本体設定

16.1 本体設定

＜注意１＞

「設定」ボタンを押下すると変更した設定は即時反映されますが、本体への保存は行われません。そのまま電源を抜くと設定した値は消えてしまいます。

設定した値を本体に保存する場合、WebUI の「停止・再起動」にて「本体再起動」または「本体シャットダウン」を行ってください。

＜注意２＞

WebUI 設定画面を 3G や WAN ポート側（external ゾーン）からアクセスする場合は、設定した設定画面ポート番号をフィルタ設定で「Accept」してください。

第 17 章

Ping 不通監視

第 17 章　Ping 不通監視

17.1　Ping 不通監視設定

本機能は定期的に指定されたアドレスへ Ping を行い、指定先から Ping の応答が得られなかった場合、SpreadRouter 本体を通信不通と判断し、SpreadRouter 自身を再起動する機能です。

◆　Ping 不通監視

定期的に Ping 不通監視をする場合は「監視する」を選択し、以降の設定を行います。デフォルトは「監視しない」。

◆　Ping 対象アドレス

Ping 送出先の IP アドレスを指定します。指定は IP アドレス形式のみとなりホスト名は入力できません。

◆　Ping 間隔

Ping 送出間隔を指定します。[5 分/10 分/15 分/20 分/30 分/60 分/120 分/240 分]。デフォルト 10 分。

※１サイクルに実施する ping は 5 秒間隔で 3 パケット送出を５回繰り返し、１度でも応答を受けた場合は、通信可能と判断し再起動は行われません。

＜注意１＞

Ping 送出先アドレスを間違えたり、存在しないアドレスを指定すると Ping 失敗を繰り返すので、頻繁に再起動が発生します。

＜注意２＞

Ping を送出を行う事で 3G 回線使用時にはパケット量が発生しますので、回線プランに気を付けてください。

＜注意３＞

「設定」ボタンを押下すると変更した設定は即時反映されますが、本体への保存は行われません。そのまま電源を抜くと設定した値は消えてしまいます。

設定した値を本体に保存する場合、WebUI の「停止・再起動」にて「本体再起動」または「本体シャットダウン」を行ってください。

第 18 章

専用設定ファイル

第 18 章　専用設定ファイル

18.1　専用設定ファイル設定

本機能は SpreadRouter ファームウェア v1.03 以降に追加された機能です。

SpreadRouter 内で動作するオリジナルの専用プログラムを開発した際に、その専用プログラムが使用する設定ファイルを SpreadRouter に保存します。

専用プログラム自体は予め本体にインストールいただき、設定のみ手軽に変更したい場合を想定した使用方法になります。

プログラム開発時に各設定を変更したい場合は、本機能を使用した設計で開発することも可能です。

◆　専用プログラムの設定ファイル

「ファイルを選択」ボタンでアップロードする設定ファイル選択し、「アップロード」ボタンを押下でファイルのアップロードを開始します。

18.2. 設定ファイルの保存場所

保存される設定ファイルは以下のとおりです。

項目	内容
保存先ディレクトリ	/etc/default/
保存ファイル名	SpreadCtrl.ini

“「アップロード」後、新しい設定でプログラムを実行するには本体再起動か本体シャットダウンを行うことで有効になります。“と記載がありますが、開発したプログラムが常に本設定ファイルを読み込む様な仕組みであれば、再起動は不要かと思います。

第 19 章

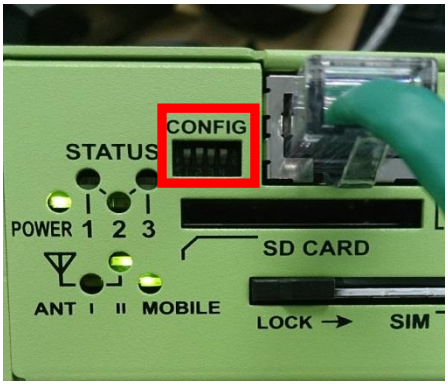
コンソールポート変更

第 19 章　コンソールポート変更

19.1　コンソールポート変更

本機能はコンソールポート（RS232C）をとアプリケーションポートとして利用する場合の設定です。

◆　DipSW 変更



本体の電源を OFF にして DipSW の左側２個を下にセットします。
［↓　↓　↑　↑］　にします。

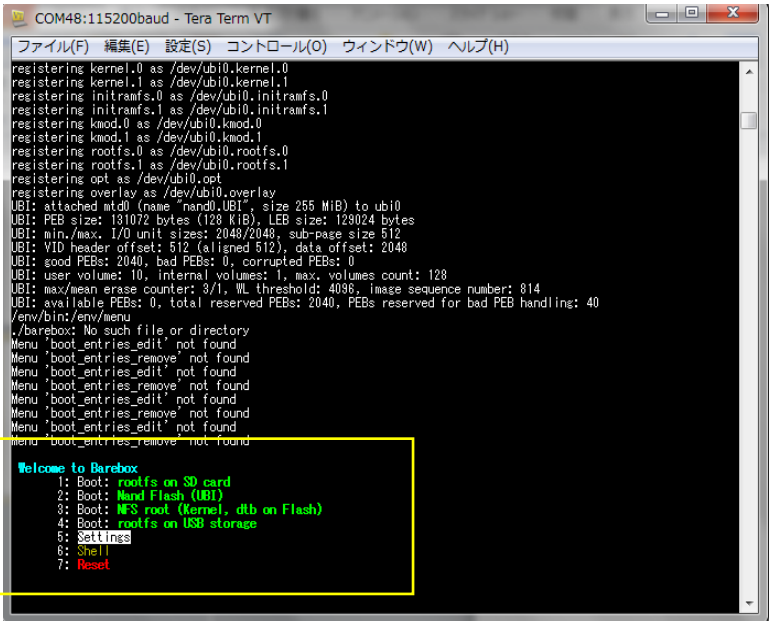
◆　DipSW 変更

本体の CONSOLE とパソコンをシリアルケーブルで接続し、パソコンはターミナルソフトを起動。

［シリアル設定］　ボーレート 115200 / データ長 8 / ストップビット 1 / パリティ無　/ フロー制御無

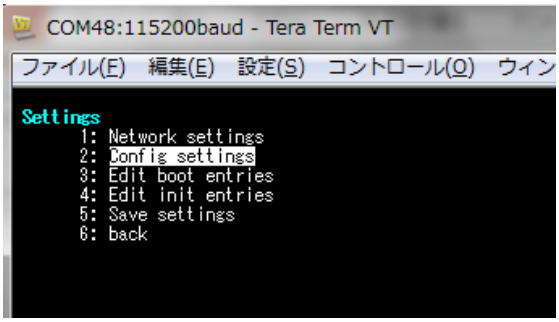
※パソコン側を市販の USB シリアルケーブルで接続の場合は、両方オスオスの端子で変換が必要です。

※クロスケーブル（クロス変換アダプタ等）が必要になりますので、ご注意ください。

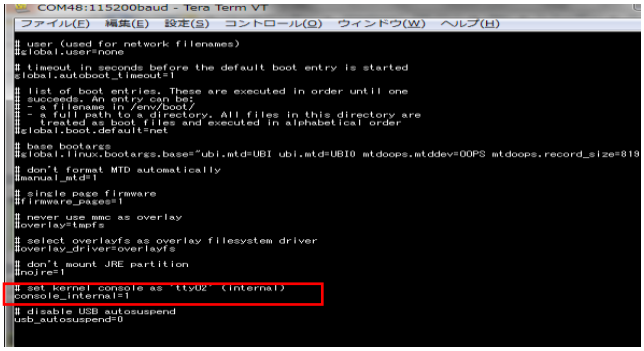


本体電源を ON すると
下記のメニューが表示されます。

５．Settings を選択



2. Config settings を選択

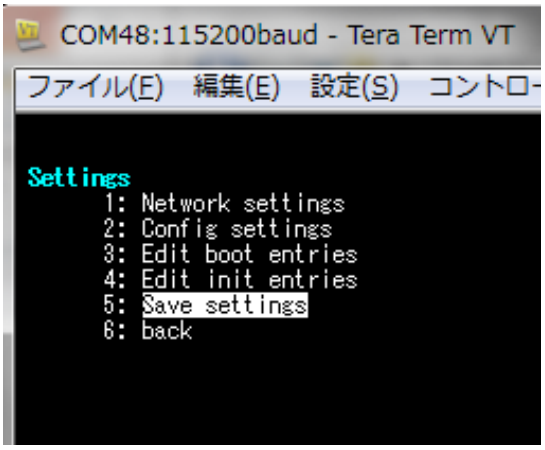


コンフィグファイルの下の方にある

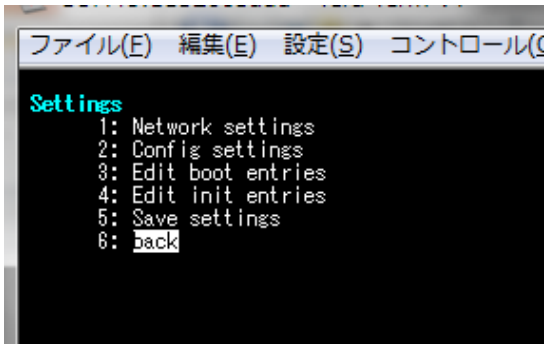
#console_internal=1

のコメント　# を外します。

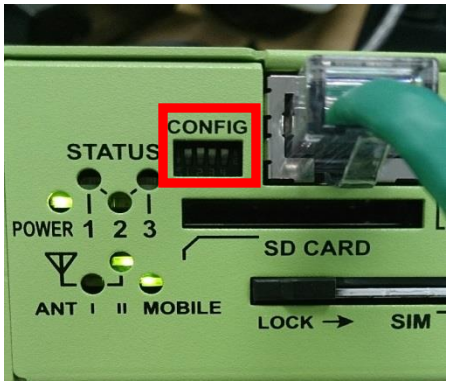
外したら、CTRL+D キーで保存します。



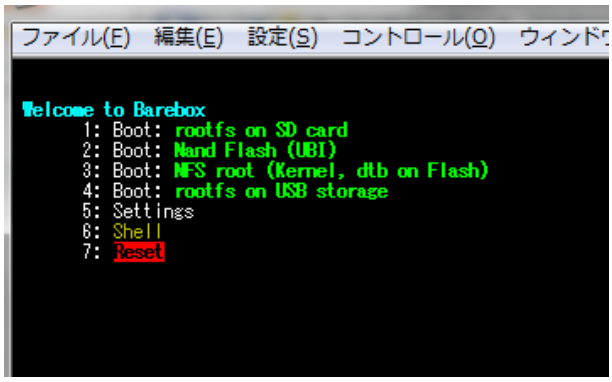
5. Save settings を選択



6. back を選択



本体の DipSW　を全て　［↑　↑↑　↑］　向きに戻します。



7. Reset を選択で再起動します。

再起動後は、WebUI のシリアル変換機能のコンソールポート（tty00）を設定することで使用可能になります。

※注意点

コンソールポートは本体電源投入時に Linux　ブートメッセージが必ず出力されます。

接続機器側に影響が出ないかご確認願います。

※コンソールポートを元に戻す場合は、同様の手順で #console_internal=1 コメントを追加し戻してください。

第 20 章

VPN サービス対応 OS について(有償サービス)

第 20 章　VPN 対応 OS について

20.1　VPN 対応 OS について

VPN 対応 SpreadRouter ファームウェアは標準のファームウェアに、L2TP-IPsec のサーバモードを搭載した専用ファームウェアになります。（有償にてアップデートまたは出荷時インストール）

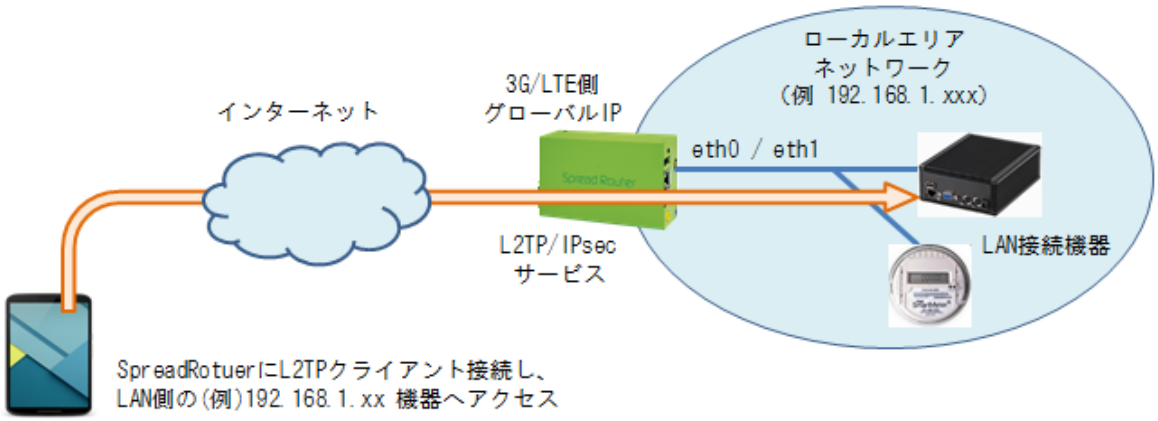
◆対応仕様

SpreadRouter は L2TP-IPsec のサーバモードに対応しています。

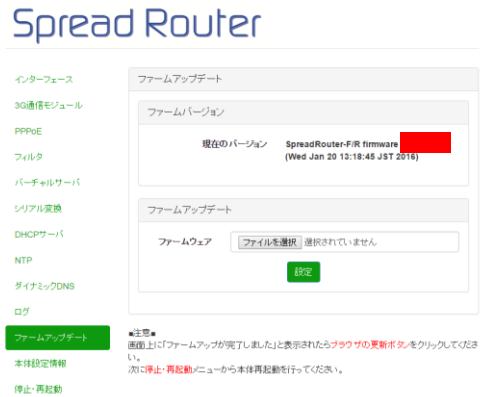
◆動作確認端末

Android、iPhone 等のスマートフォン。

◆構成



◆ファームウェア(OS)バージョン確認



Ver 1.061+ が VPN 搭載最新バージョンになります。（2016 年 11 月 1 日時点）

第 20 章　VPN 対応 OS について

20.2　VPN の主な設定方法

◆主な設定方法

基本的な流れは、VPN 用設定ファイル(テキストファイル)を作成し、SpreadRouterWeb 設定画面の「L2TP/IPSec 設定ファイル」メニューで読み込ませた後、スマートフォンなどの端末から設定した情報でアクセスします。

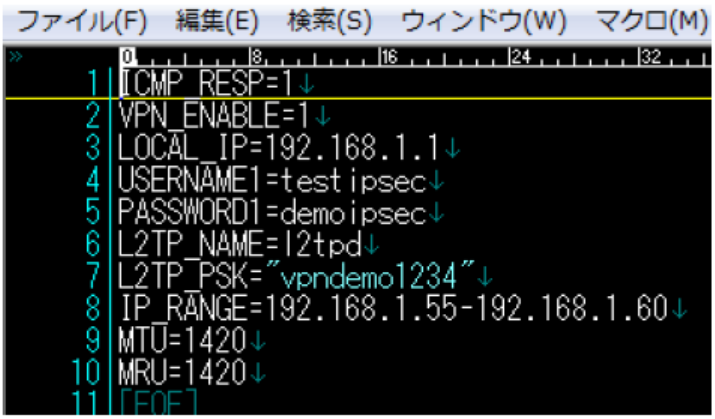
◆作成する設定ファイル（SpreadVpn.ini）

SpreadRouter に読み込ませるテキストの ini ファイルは、指定のキーワード=値で記述します。

■設定ファイル説明　SpreadVpn.ini

項目名	必須	内容	設定例	備考
ICMP_RESP		ICMP応答有り無し	1 応答しない / 0 応答する	デフォルト：応答する
VPN_ENABLE	◎	L2TP/IPSec使用/未使用	1 使用する / 0 使用しない	
LOCAL_IP	○	SpreadRouterのローカル側IP	192.168.1.1	VPN_ENABLE=1 時は必須
USERNAME1	○	L2TP接続ユーザID	usertest	VPN_ENABLE=1 時は必須
PASSWORD1	○	L2TP接続パスワード	testpass	VPN_ENABLE=1 時は必須
L2TP_NAME	○	L2TP接続名	l2tpd	VPN_ENABLE=1 時は必須
L2TP_PSK	○	L2TP事前共有鍵	1234abc	VPN_ENABLE=1 時は必須
IP_RANGE	○	クライアントIPレンジ	192.168.1.10-192.168.1.15	VPN_ENABLE=1 時は必須
MTU		MTU 最大伝送ユニット	1420	VPN_ENABLE=1 時に有効
MRU		MRU 最大受信ユニット	1420	VPN_ENABLE=1 時に有効

※設定ファイル内にはコメントなどの記入は追記しないでください。

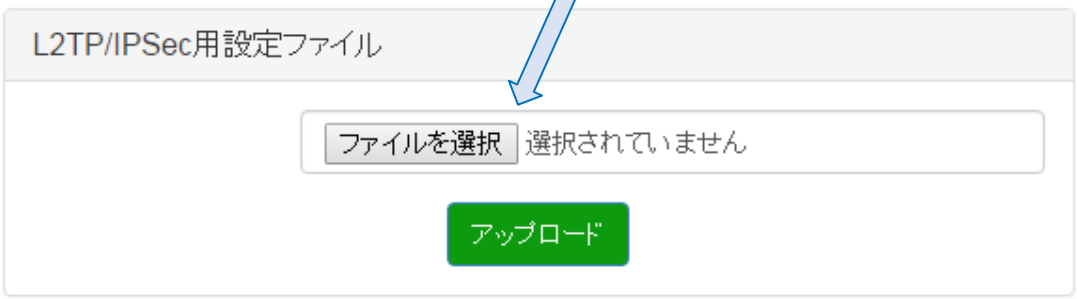


20.2　VPN の主な設定方法

◆PC で作成した設定ファイル（SpreadVpn.ini）を SpreadRouter に反映させます。

Web 設定画面の「L2TP/IPsec 設定ファイル」メニューを選択。

SpreadVpn.ini を読み込ませます。



■注意■
「アップロード」後、新しい設定でプログラムを実行にするには本体再起動か本体シャットダウンを行うことで有効になります。

作成した L2TP/IPSec 用設定ファイルをアップロードします。

アップロードが完了したら、本体を再起動してください。

再起動したら VPN クライアント（iPhone または Android 端末等）より接続が可能になります。

第 20 章　VPN 対応 OS について

20.3　クライアント側の設定サンプル、その他制限事項

◆クライアント側の設定例

◆VPN 制限事項

（１）WAN 側のインターフェースは、3G(LTE)に限定されます。

PPPoE やイーサネットを WAN ポートとして使用する場合は、VPN 接続はできません。

（２）VPN セッション接続は同時に１つしか通信できません。

VPN ではなく、インターネット接続(グローバル IP 接続)は可能です。

（３）VPN 接続中は一時的にドメインアクセスができないため、IP アドレスでの接続行ってください。

SpreadRouter シリーズ ウェブユーザインターフェース操作マニュアル Ver.1.1.8

2017 年 8 月版

発行 エヌエスティ・グローバリスト株式会社