PacketiX VPN 4.0
アプライアンス
ユーザーズガイド

対象モデル型番

【Standard モデル】

EBAX/P4x

【Professionalモデル】

EBX3/P4x

【旧Standard モデルアップグレード後】

P3-x/BS600

Ver2.0.3

ぷらっとホーム株式会社

■ 商標について

- Microsoft は、Microsoft Corporation の商標です。
- Microsoft, MS-DOS, Windows, Windows NT, Microsoft Internet Explorer は、米国 Microsoft Corp.の米国およびその他の国における商標または、登録商標です。
- Linux は、Linus Torvalds 氏の米国およびその他の国における商標あるいは登録商標です。
- その他記載されている製品名などの固有名詞は、各社の商標または登録商標です。

■ 重要なお知らせ

本ガイドについて

本ガイドでは、PacketiX VPN 4.0 アプライアンスとしての基本的なご利用に関する操作方法を記述しており、PacketiX に関する詳細な説明はしておりません。詳細な説明が必要な場合には、別途専用に解説したユーザーズガイドを参照ください。

目次

第 1 章 はじめに

1-1. 本ガイドでの対象モデル

■Standard モデル（EBAX/P4x）

■Professional モデル（EBX3/P4x）

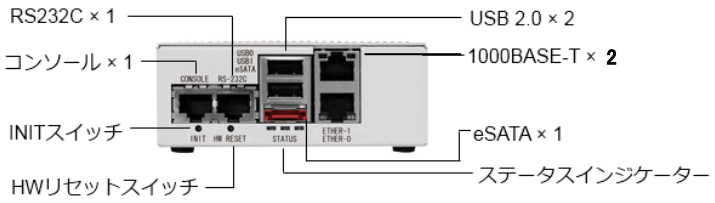
■旧 Standard モデル（P3-x/BS600）※ 4.0 搭載バージョンへのアップグレード後を想定

1-2. 各部の名称

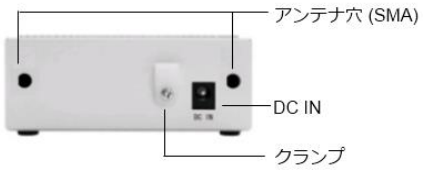
■Standard モデル

型番：EBAX/P4x

◆ 前面

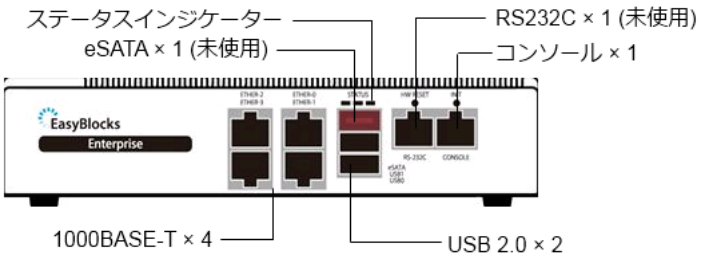


◆ 背面



■Professional モデル

型番：EBX3/P4x

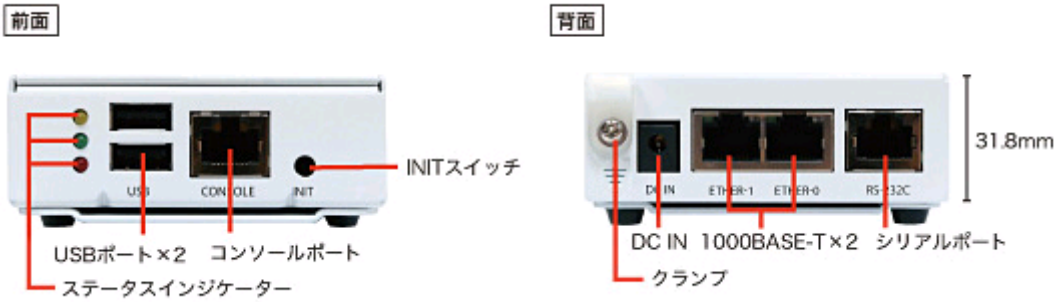


ケーブルクランプの取り付け：

AC-IN 下の穴に添付のクランプを差し込みます

■旧 Standard モデル

型番：P3-SS/BS600 および P3-BR/BS600 ※ 4.0 搭載バージョンへのアップグレード後を想定



1-3. INIT スイッチの操作

INIT スイッチの操作により、初期設定状態での起動、OS 起動時からの停止・再起動の実行が可能です。

初期設定状態での起動

本体 INIT スイッチを押しながら(5 秒程度)電源 ON する

OS 起動時からの再起動

INIT スイッチを 0～4 秒間(2 秒までは黄色点灯、4 秒までは緑色点灯となります)押下し続けた後に、スイッチを解放すると再起動処理が開始されます。

OS 起動時からの停止

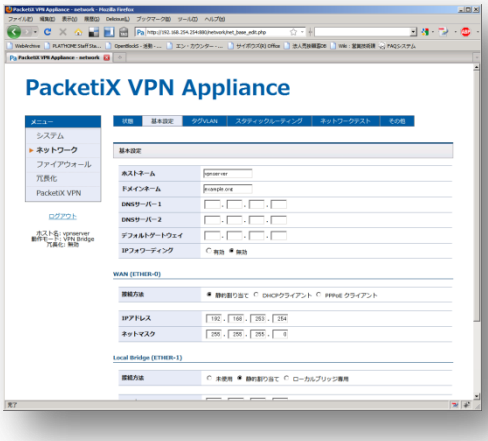
INIT スイッチを 5 秒以上(赤色点灯となります)押下し続けた後に、スイッチを解放すると停止処理が開始されます。停止完了後は、LED 全色が同時に点滅します。

1-4 運用管理について

PacketiX VPN 4.0 アプライアンスでは、運用管理用の設定インタフェースとして、OS の基本設定を行うための WEB I/F と、PacketiX VPN 用のサーバー管理マネージャをご利用頂きます。

■ WEB I/F

PacketiX VPN 4.0 アプライアンスの IP アドレスや NTP サーバーなど、サーバーとしてネットワークに設置するための基本的な項目を含め様々な内容を設定可能です。



■ PacketiX VPN サーバー管理マネージャ

PacketiX を使用した VPN 構築のための各種設定のために使用します。ユーザの登録や、カスケード先の仮想 HUB 等を設定いたします。

1-5. 出荷時設定情報

■ ホスト名

ホスト名：	vpn
ドメイン名：	example.org

■ IP アドレス

Ether-0 (eth0)	IP アドレス ：	192.168.254.254
	ネットマスク：	255.255.255.0
Ether-1 (eth1)	IP アドレス ：	192.168.253.254
	ネットマスク：	255.255.255.0
Ether-2 (eth2)	IP アドレス ：	未設定 (Professional のみ)
	ネットマスク：	
Ether-3 (eth3)	IP アドレス ：	
	ネットマスク：	

■ ネームサーバ

DNS サーバー：	未指定

■ Firewall

ネットワーク I/F：	Ether-0
許可：	Ping WEB I/F(TCP/880) Softether VPN(TCP/443)

第２章　ログイン・起動・停止

2-1. 起動方法

1. 必要なケーブルを接続します
   ◆ 必ず接続するもの
   ・AC ケーブル または AC アダプタ
   ・LAN ケーブル（1 本は必須）

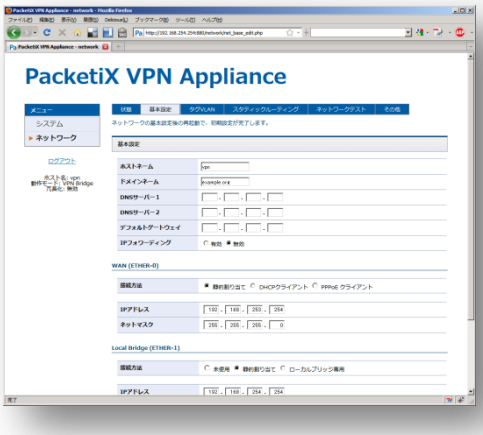
2. AC ケーブルまたは AC アダプタを接続して起動します
   1 分程度でシステムは稼働を開始します。
   LED が黄、緑、赤、緑、黄・・・のように、点灯・消灯と繰り返し始めれば起動が完了です。

2-2. システムへのログイン

WEB I/F からのログイン方法をご案内します。PacketiX VPN サーバー管理マネージャでのログイン方法については次章で紹介いたします。

PacketiX VPN 4.0 アプライアンスでは、本体 IP アドレス・DNS サーバー等の基本的な項目の設定のために WEB I/F 搭載しており、ブラウザからシステム管理が可能です

初期設定画面



ネットワーク設定画面

URL：　http://192.168.254.254:880/（eth0 の場合）

2-3. 停止方法

適切なシャットダウン処理を行わずに、電源断を行った場合、VPN Server / Bridge の設定内容が保存されていない場合があります。必ず適切なシャットダウン処理を行って下さい。

■電源ボタンの押下

本体前面のINITスイッチを5秒以上(赤点灯になるまで)押下することで、シャットダウン処理が開始されます。シャットダウンが完了すると、全LEDが点滅します。

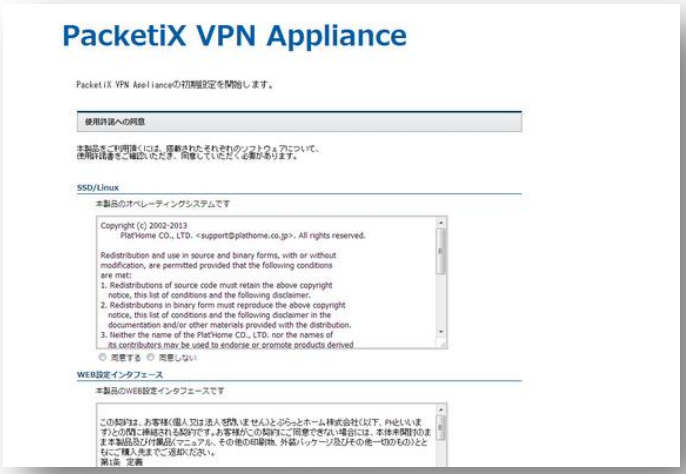
■WEB I/F

WEB I/Fにログイン後、「システム」→「メンテナンス」から「シャットダウン」を選びます。その後ページ中央にある実行ボタンをクリックします。

第３章　本体の設定

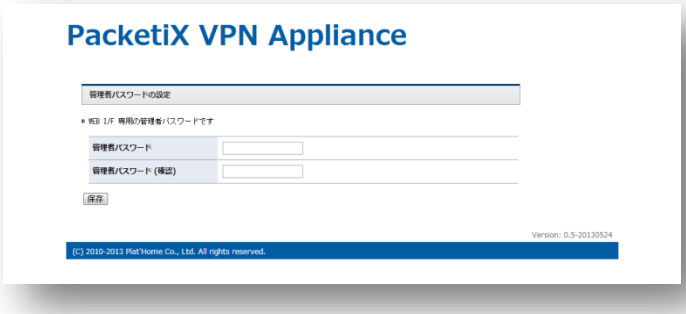
3-1. 初期設定

使用許諾の確認を行っていただきます。同意のチェックをつけないと、以降の設定は行えません。



動作モードを VPN Server または Bridge から選択します。

WEB I/F へのログインパスワードを設定します。



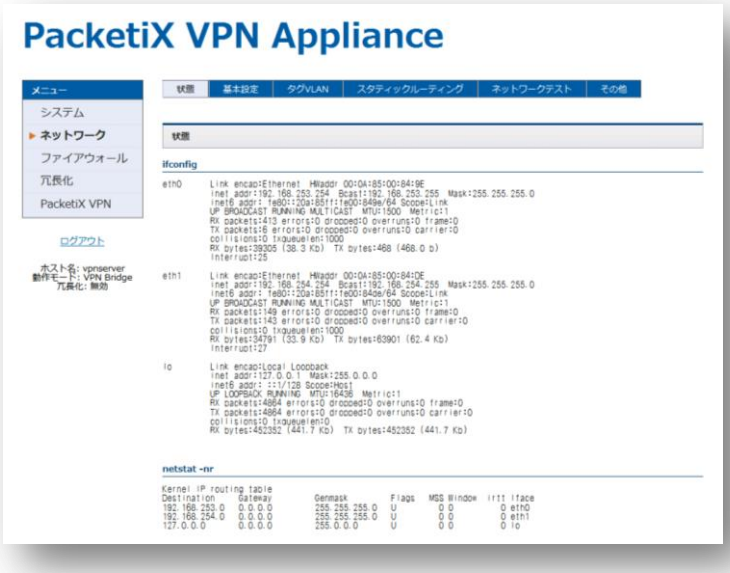
この後、ネットワーク設定の画面に遷移します。次項以降を参考に、サポートサービスやネットワークの設定を実施してください。

3-2. サポートサービスに関する設定

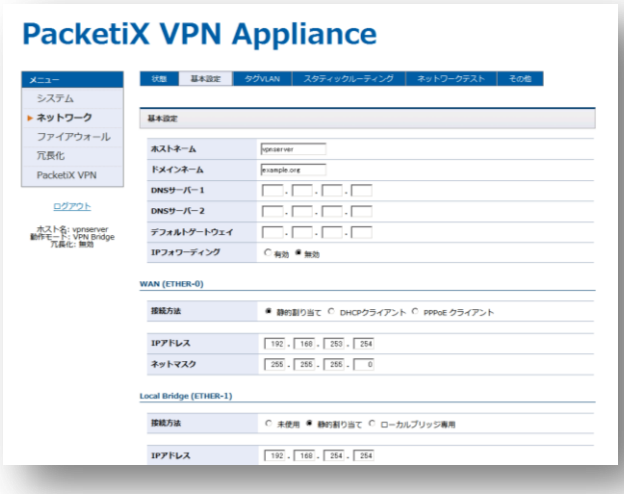
サポートサービス用に発行されたアカウント情報を登録してください。ソフトウェアのオンラインアップデートに必要となります。

3-3. ネットワーク設定変更

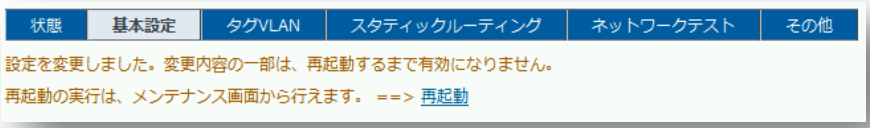
WEB I/F からログイン後、画面左メニューより「ネットワーク」を選択します。画面中央に、「状態」「基本設定」「タグ VLAN」等のメニューが並びます。



IP アドレスなどネットワークの基本的な内容を変更する場合は、「基本設定」を選択します。



各項目を記入後、「保存」ボタンを押下することで変更内容が保存されます。設定を本体に反映させるには、再起動が必要となります。

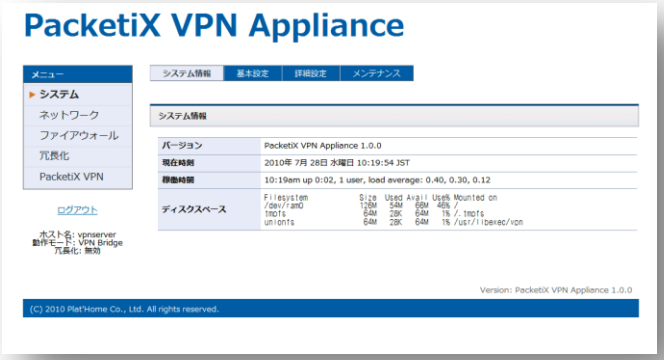


画面上に上図のように再起動を促す表示がされましたら、再起動のリンクをクリックするか左メニューより「システム」→「メンテナンス」と選択し、再起動の実行画面を表示して下さい。

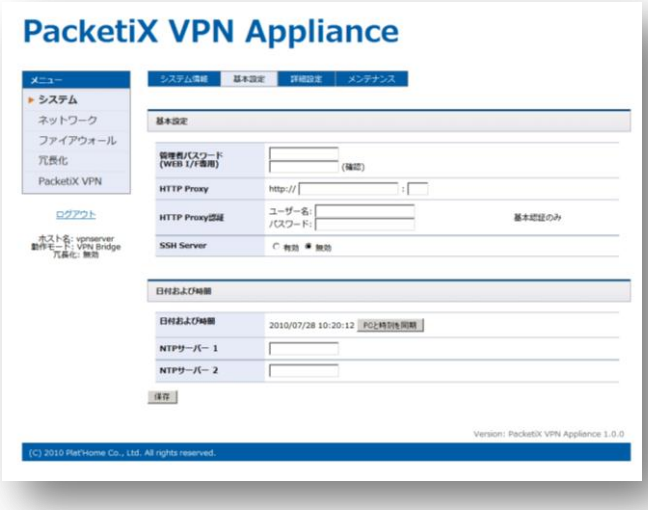
再起動ボタン押下後、画面中央に現れる実行ボタンを押下することで、再起動が行われ、変更した設定内容が反映されます。

3-4. WEB I/F の管理者パスワード

WEB I/F からログイン後、画面左メニューより「システム」を選択します。画面中央に、「システム情報」「基本設定」等のメニューが並びます。



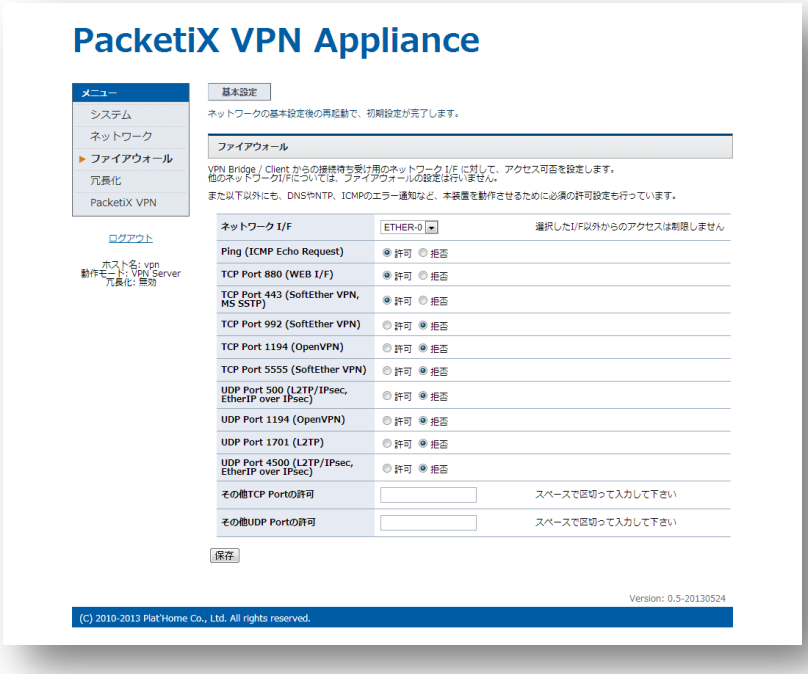
管理者パスワードを変更するには、「基本設定」を選択します。



管理者パスワードの項目に、確認も含めて 2 箇所パスワードを入力し、「保存」ボタンを押下することで変更内容が保存されます。次回ログイン時より、変更したパスワードが必要になります。

3-5. ファイアウォール

WEB I/F からログイン後、画面左メニューより「ファイアウォール」を選択します。画面中央に、「基本設定」のメニューが表示されます。



ファイアウォール設定をしたいネットワーク I/F(外部からの接続を受け付ける I/F)を選択し、許可したい通信を許可・拒否を選択して下さい。各項目を記入後、「保存」ボタンを押下することで変更内容が保存されます。設定を本体に反映させるには、再起動が必要となります。

3-6. 冗長化

WEB I/F からログイン後、画面左メニューより「冗長化」を選択します。画面中央に、「概要」が表示され、冗長化動作に関する解説と注意書きが記載されています。設定を行うには、上部タブから「基本設定」を表示します。

■ 冗長化機能について

本機の冗長化機能では、VRRP(Virtual Router Redundancy Protocol)を用いて実現しています。マルチキャスト通信によって、お互いの状態を監視しマスターとバックアップの切り替えを行います。

本機に接続しようとするクライアントは、この仮想的な IP アドレスを接続先として設定します。また、上位のルータで静的 NAT やパケットフィルタリングを行う場合も、この仮想的な IP アドレスを用いて下さい。

■ 制限

WAN(Ether-0)ポートを、PPPoE クライアントとして設定している場合は利用できません。

■ 冗長化の設定について

◇ 必須の設定項目

冗長化機能を利用する場合、以下の項目の設定が必須です。

- 冗長化動作
- 物理 I/F
- 仮想 IP アドレス

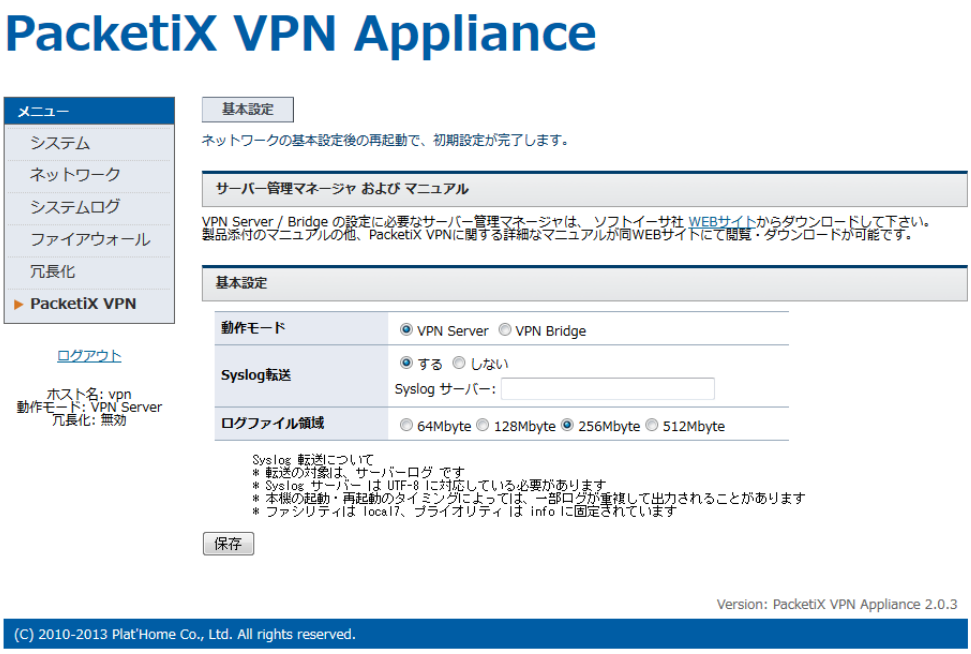
◇ その他の設定項目

通常は、必須項目以外を変更する必要はありません。
変更を行う場合は、内容について良く注意して下さい。

- 初期状態
  フェイルバックする場合は、1 台をマスター、網一方をバックアップに設定します
- フェイルバック
  障害からの復旧後、マスターに設定したノードにサービスを切り替える場合に設定します
- VRRP ID
  同じネットワークで VRRP を使用している場合は、重複しない値を設定します
- プライオリティ
  バックアップが複数ある場合に、優先したいノードに大きな数値を設定します
- 監視間隔
  お互いの監視間隔を秒で設定します
- 他の監視 I/F
  ローカルブリッジ専用のインタフェースを使用している時、抜線を監視する場合に設定します
- メール通知
  サービスの稼働、切り替わり時にメール通知する場合に設定します
  SMTP 認証には対応していません
- 設定・ログ同期
  通常設定変更の必要はありません

3-7. PacketiX VPN

WEB I/F からログイン後、画面左メニューより「PacketX VPN」を選択します。画面中央に、「基本設定」のメニューが表示されます。



この設定メニューでは、PacketiX VPN の基本設定として、動作モードと Syslog 転送、ログファイル領域のサイズを設定します。

■動作モード

「VPN Server」モードと「VPN Bridge」モードのいずれかを選択します。

■Syslog 転送

- 本機のサーバーログを Syslog サーバーに転送したい場合に「する」を選択し、Syslog サーバーの IP アドレスまたは FQDN を設定します。
- Syslog サーバーは UTF-8 に対応している必要があります。
- 本機の起動・再起動のタイミングによっては、一部のログが重複して出力されることがあります。
- ファシリティは local7、プライオリティは info に固定されています。

■ログファイル領域

- PacketiX VPN のログファイル領域のサイズを指定します。デフォルト値は 256MB です。
- 目安としては、1 日分の想定ログ量の 2 倍以上のサイズ設定をしてください。
- また、この設定の変更後は、PacketiX サーバ管理マネージャの Config ファイル内の、「uint64 AutoDeleteCheckDiskFreeSpaceMin」の値も以下に示す「PaketiX VPN Server のログ保存の動作

に関して」を参考に、適宜変更してください。

■PaketiX VPN Server のログ保存の動作に関して

- PaketiX VPN Server では、ログ保存エリアの空き容量を 5 分おきにチェックし Config ファイル内の設定パラメータ uint64 AutoDeleteCheckDiskFreeSpaceMin の値より空き容量が小さくなった場合　指定サイズが確保できるよう古いログファイルから削除します。
- uint64 AutoDeleteCheckDiskFreeSpaceMin ののデフォルト設定サイズは、100MB です。
- ログファイルには　下記 3 種類があり、5 分間に保存される容量が全体で設定パラメータ uint64 AutoDeleteCheckDiskFreeSpaceMin の値を超えないように注意してください
  - サーバログ　　0 時にローテート

    仮想 hub ごとに
  - セキュリティログ　　ローテートタイミング指定可能
  - パケットログ　　ローテートタイミング指定可能
- ログの量の多い環境の場合、セキュリティログ、パケットログは　ローテートタイミングを　1 分単位とし　5 分おきの空きの容量チェックで　現在書き込んでいるログファイルが削除されないようにすることをお勧めします。
- 「uint64 AutoDeleteCheckDiskFreeSpaceMin」の値の変更手順

1. PacketiX サーバー管理マネージャで接続後、「Config 編集」の"ファイルに保存"にて保存した Config ファイルの以下の個所を修正します。

```
declare ServerConfiguration
{
        uint64 AutoDeleteCheckDiskFreeSpaceMin 104857600
```

2. 修正した Config ファイルを再度「Config 編集」の"ファイルからインポートして書き込み"にて読み込んでください。

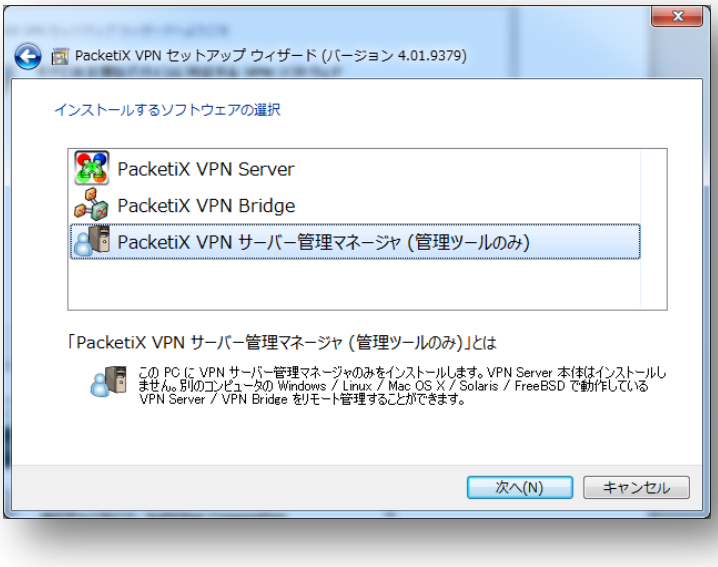
第 4 章 PacketiX VPN の設定

4-1. サーバー管理マネージャのインストール

サーバー管理マネージャは、Windows 環境でのみ利用可能です。PacketiX VPN 開発元 WEB サイトより、インストーラをダウンロードして導入します。

URL： http://www.packetix-download.com/

インストールは、画面の指示に従い進めてください。以下画面で「PacketiX VPN サーバー管理マネージャ(管理ツールのみ)」を選択することで導入できます。



4-2. ライセンスの取得

PacketiX VPN 4.0 のライセンス取得にあたっては下記 2 つの情報が必須となります。

・「ライセンス発行キー」

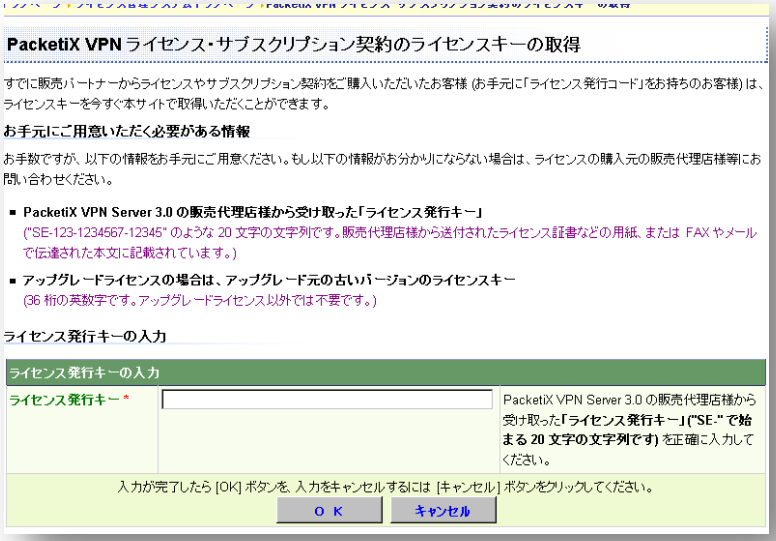
・「SoftEther ID」

「ライセンス発行キー」は弊社から PacketiX VPN 4.0 を購入頂いた際に添付しております、「PacketiX VPN 4.0 ライセンス/契約 発行証明書」内に表記があります。また「SoftEther ID」はお客様で取得を行う必要がございます。

ライセンスの発行を行うには、SoftEther 社のサイト(ライセンス管理システム：http://www.softether.co.jp/jp/lm/)に Web ブラウザでアクセスを行います。

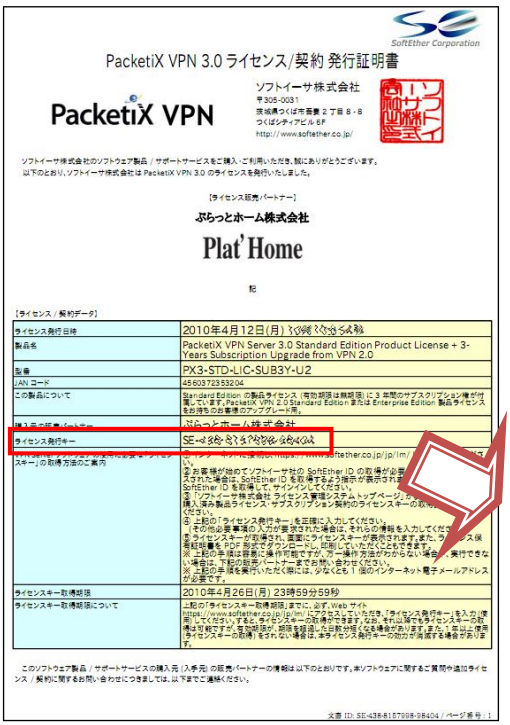
「SoftEther ID」をお持ちでは無い場合、下記の様な画面ではなく取得を促す表記が出て参りますので画面の指示に従って ID の取得を行って下さい。

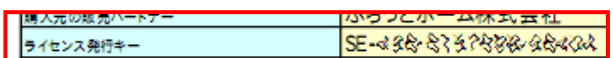
「SoftEther ID」を持っており、サインイン済の場合、上記の様な画面が表示されます。Web ページ中央付近に「購入済み製品ライセンス・サブスクリプション契約のライセンスキーの取得」というリンクがありますのでそちらをクリックします。



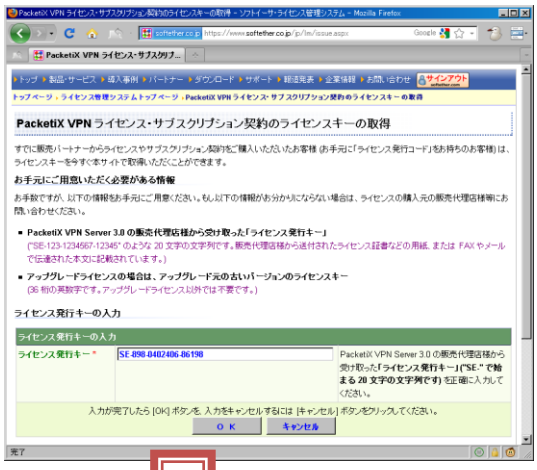
続いて表示されるページに「ライセンス発行キー」を入力する箇所がありますので「PacketiX VPN 4.0 ライセンス/契約 発行証明書」内にある「ライセンス発行キー」を入力します。

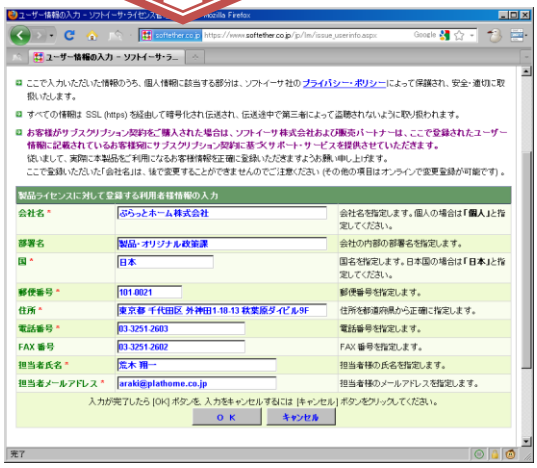
「ライセンス発行キー」は「PacketiX VPN 4.0 ライセンス/契約 発行証明書」内に
” SE-XXX-XXXXXXX-XXXXX”のフォーマットで表記がございます。





「ライセンス発行キー」を入力後「OK」をクリックすると確認画面に移ります。表示されている情報が正しければそのまま「OK」を押して次に進みます。

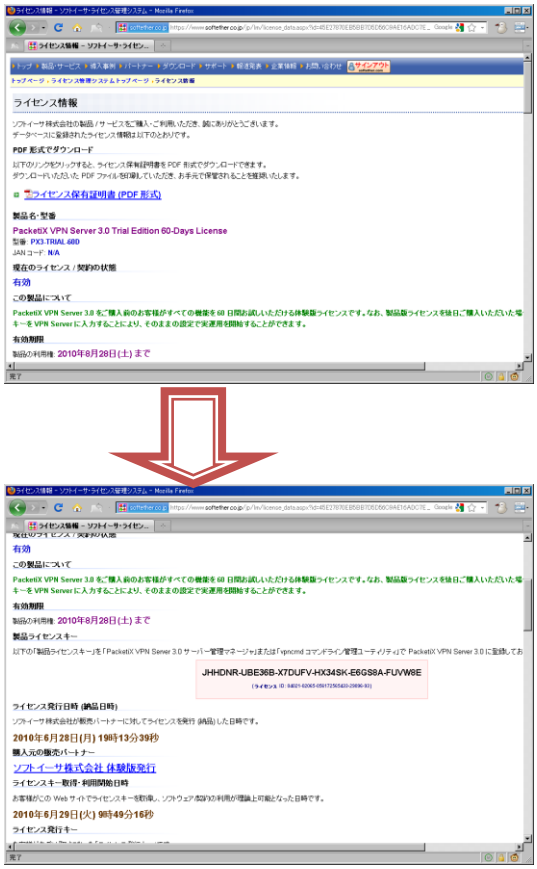




続いて表示される内容を確認後、ページ下部の「OK」を押して進みます。

「ライセンス取得の確認」ページが表示されるので確認後に「OK」を選びます。

「ライセンス情報」のページに移ります。本ページの中央部に発行ライセンスが表示されています。ここで発行された文字列が PacketiX VPN 4.0 のライセンスとなります。また、ライセンス保有証明書内にも表記がありますのでダウンロードして保持頂く事をお勧め致します。



■ライセンスの有効性及び諸情報の確認方法
以下サイトにて、お持ちのライセンスに関する有効性と諸情報の確認が可能です
http://license.softether.com/

4-3. PacketiX サーバー管理マネージャの接続制限

PacketiX サーバー管理マネージャで接続出来る端末を IP アドレスで制限することが出来ます。以下 に具体的な手順を説明します。

1. SSH か、シリアルコンソールにて接続する(ログインユーザーID：support, パスワード:plathome)
2. /usr/libexec/vpn ディレクトリ内に、ファイル名が"adminip.txt"のファイルを作成します。
3. adminip.txt に、接続を許可したい端末の IP アドレスを記述する
   許可したい IP アドレスを 1 行づつ記述します。192.168.10.0/24 といったように CIDR 形式で記述することで、ネットワークで指定することも出来ます。
   記述方法については、ソフトイーサ社の WEB マニュアルの「3.3.18 IP アドレスによるリモート管理接続元の制限」をご参照ください。
   http://www.softether.jp/
4. adminip.txt 追加後、WEB 管理画面の「システム」の「メンテナンス」より、再起動を実施してください。

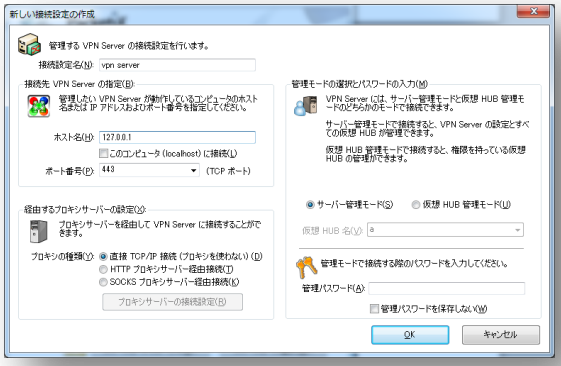
4-4. VPN Server の設定

VPN Server としての基本的な設定方法を記載します。詳細な設定に関しては、開発元 WEB サイトで参照可能なマニュアルを参照の上ご利用ください。

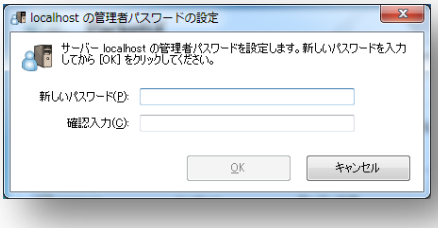
1. 管理マネージャの起動

まだ何も設定がされていないので、接続先の設定を行います。「新しい接続設定」をクリックします。

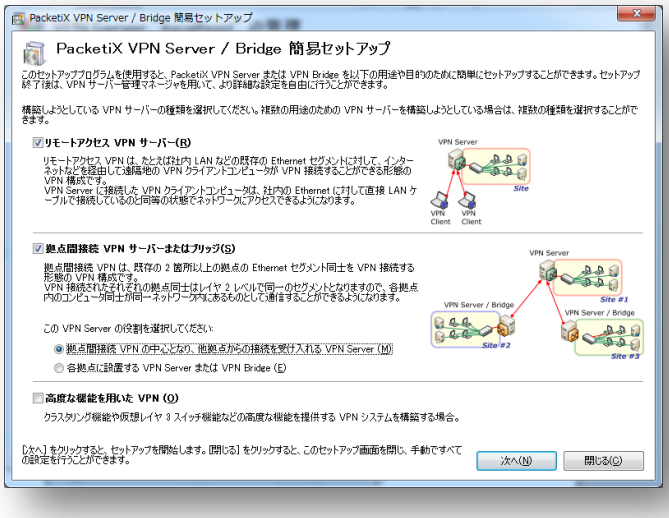
接続設定名、ホスト名が最低限必要です。



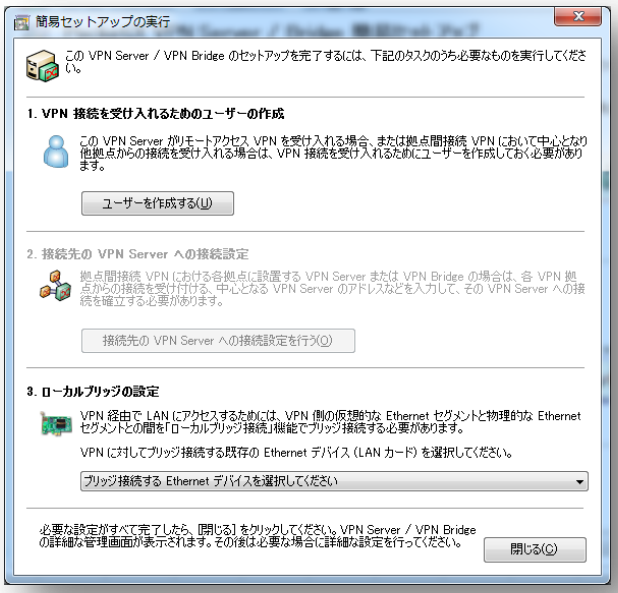
初回接続時は、管理者パスワードの設定を求められます。



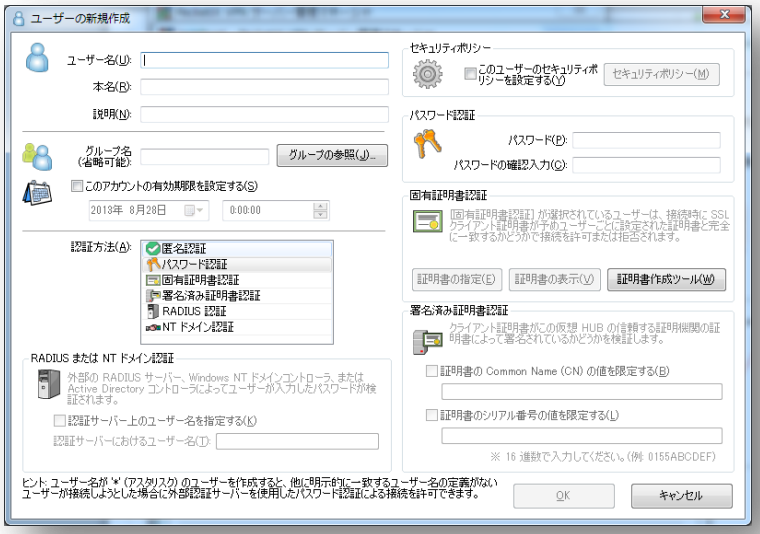
仮想 HUB が 1 つもない初期状態では、管理セットアップウィザードが表示されます。画面の指示に従い、仮想 HUB 名の指定、ダイナミック DNS や IPsec/L2TP/EtherIP/L2TPV3、VPN Azure 等を設定します。



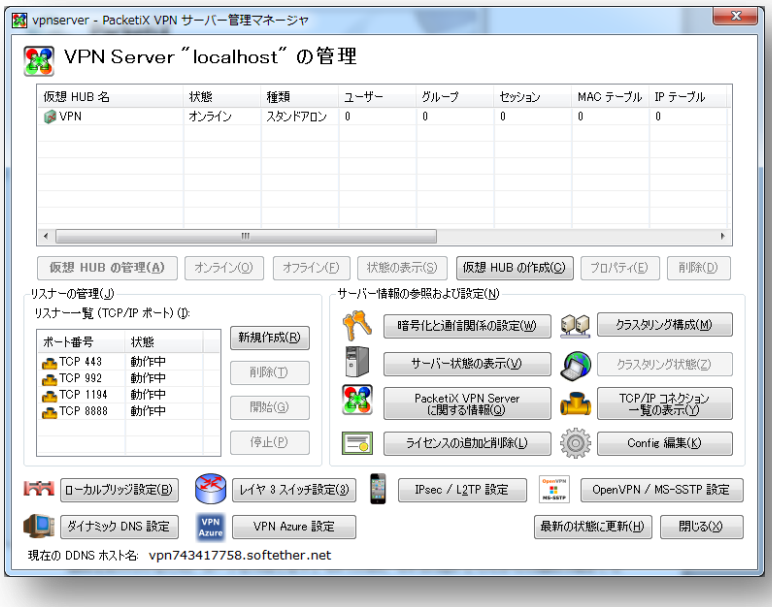
いくつかの画面が表示された後、ユーザ作成とローカルブリッジの設定画面が表示されます。ローカルブリッジについては、この画面上で仮想 HUB に接続する物理 I/F を選択しておきます。



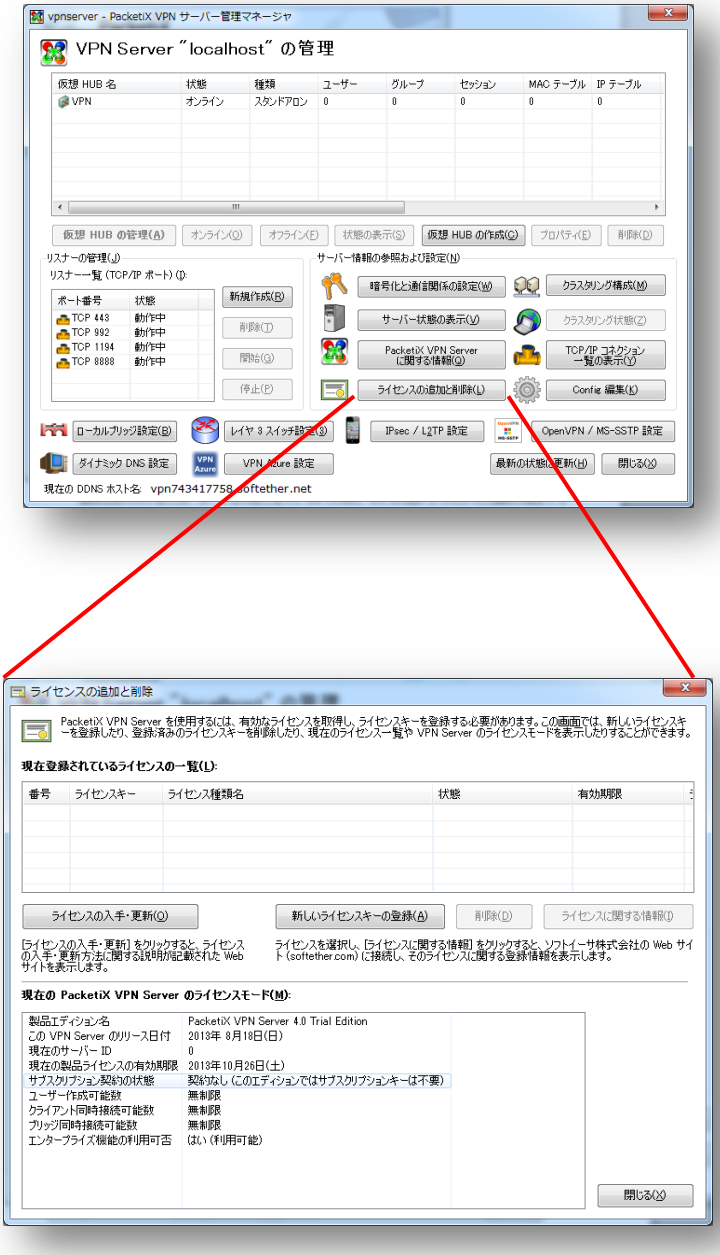
ユーザ作成では、ユーザ名、パスワードが最低限必要です。その他パラメータは必要に応じて設定します。



機能設定が完了すると、管理画面の最初に戻ります。次回接続以降は、ウィザードは表示されずに、この画面から開始されます。



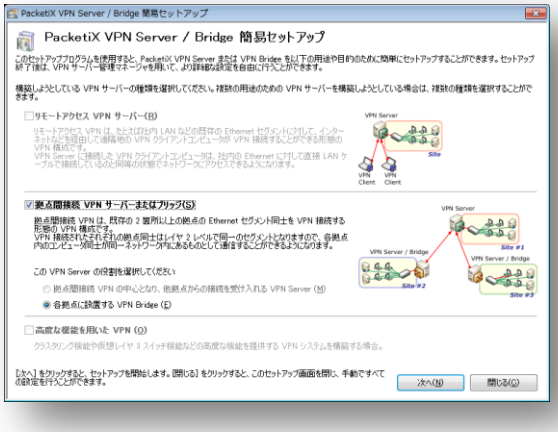
管理画面から、取得済みのライセンスキーを登録します。



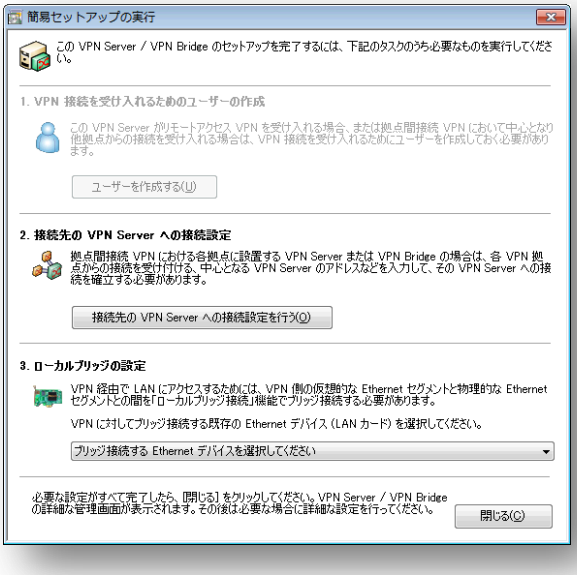
4-5. VPN Bridge の設定

Bridge に対して設定のための接続を行う方法は、Server と全く同じです。接続を行うと、Server の機能が制限された状態で表示されます。VPN Server と同じく、サーバー管理マネージャを使用します。「4-3. VPN Server の設定」の参照し、予めサーバー管理マネージャのインストールと設定を実施して下さい。

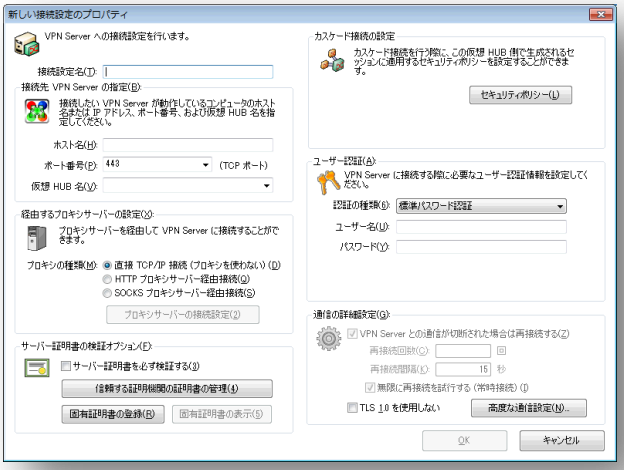
初期状態では、管理セットアップウィザードが表示されます。VPN Bridge では、VPN Server への接続とローカルブリッジの設定以外にやることはありませんので、選択肢はありません。画面に従って進めてください。



VPN Server への接続とローカルブリッジの設定画面が表示されます。ローカルブリッジについては、この画面上で仮想 HUB に接続する物理 I/F を選択しておきます。



VPN Server への接続では、接続設定名、ホスト名、ポート番号、仮想 HUB 名、ユーザ名、パスワードが最低限必要です。その他パラメータは必要に応じて設定します。



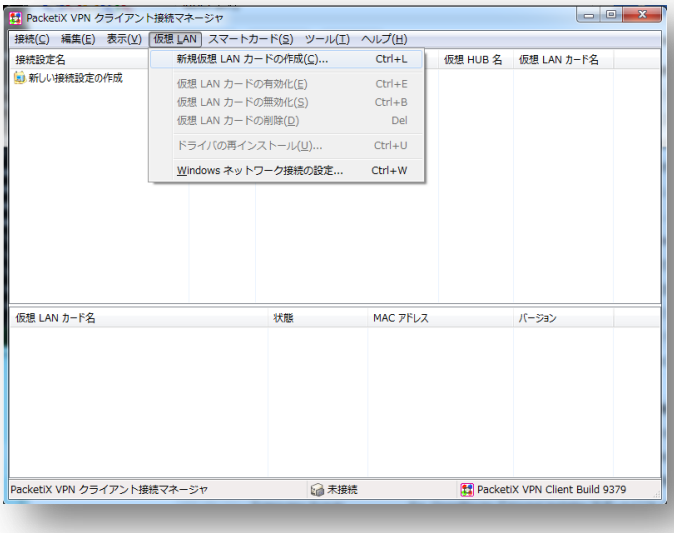
4-6. VPN Client のインストールと設定

VPN Client は、Windows/Linux 環境で利用可能です。PacketiX VPN 開発元 WEB サイトより、インストーラをダウンロードして導入します。ここでは Windows を例に説明を行います。

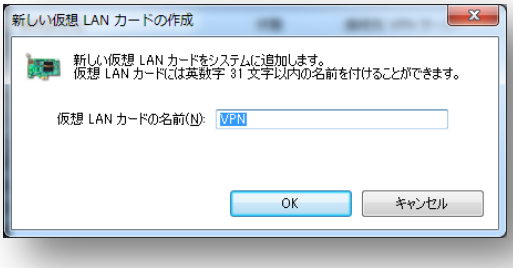
URL： http://www.packetix-download.com/

インストールは、画面の指示に従い進めてください。

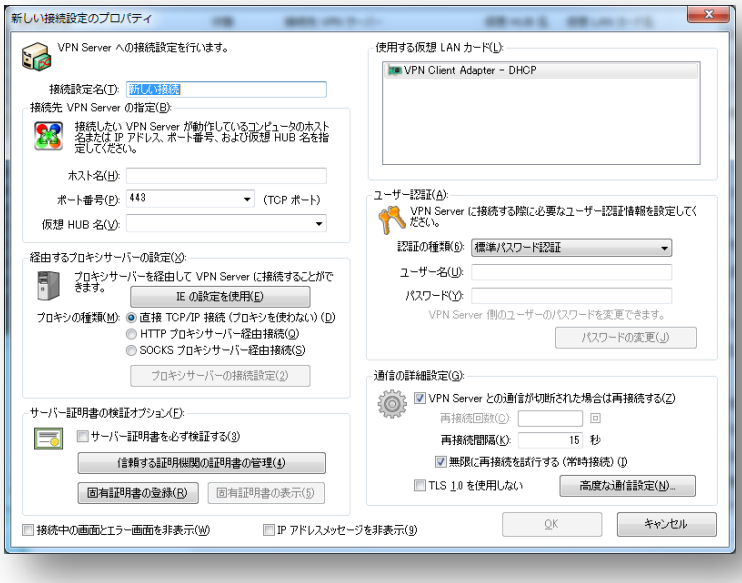
最初に仮想 LAN カードの作成を行います。



任意の名称をつけて作成を実行します。



VPN Server への接続では、接続設定名、ホスト名、ポート番号、仮想 HUB 名、ユーザ名、パスワードが最低限必要です。その他パラメータは必要に応じて設定します。

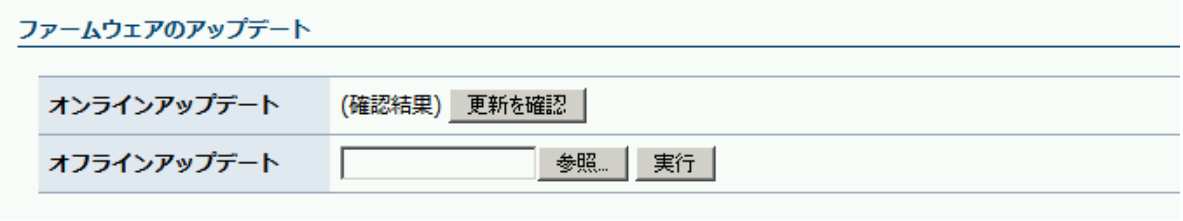


第 5 章 本体のファームウェア更新

本製品ではストレージを搭載していない代わりに、本体基板上の FlashROM に OS とプログラムを 1 つのファイルに結合したファームウェアを書き込んでいます。WEB I/F 上でファームウェアの更新確認・ダウンロード・アップデートの実行を全て行うオンラインアップデート、又は予めダウンロードしたファームウェアを WEB I/F を利用して送りつけるオフラインアップデートが利用できます。

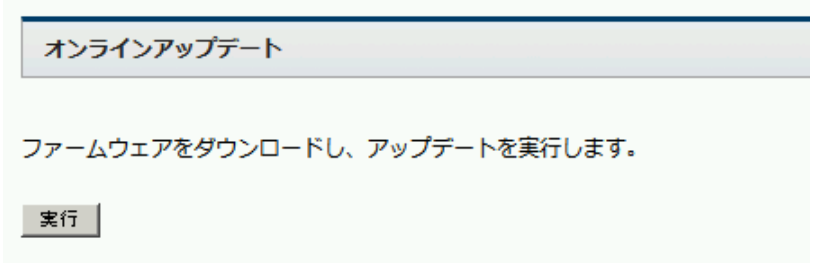
5-1. オンラインアップデート

WEB I/F からログイン後、画面左メニューより「システム」を選択します。画面中央に、「システム状態」「基本設定」等のメニューが並びますので、「メンテナンス」を選択します。画面中央に、「ファームウェアのアップデート」メニューが表示されます。



「更新を確認」ボタンを押下することで、弊社 FTP サーバと通信を行い、最新バージョンの有無を確認し、結果を表示します。

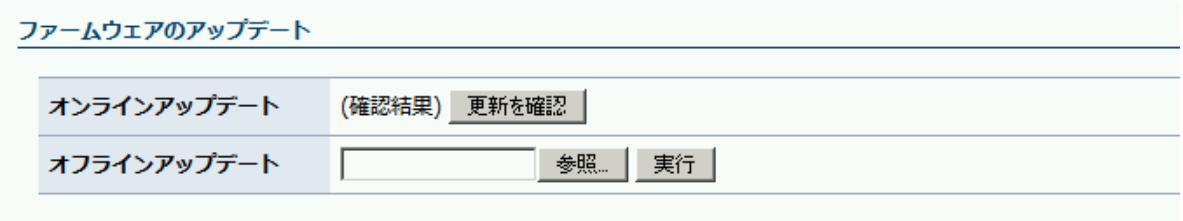
ファームウェアの更新がある場合は、バージョン番号と「更新を実行」ボタンが表示されます。



画面中央に現れる実行ボタンを押下することで、ダウンロードが行われます。画面上に再起動を促すメッセージが表示されますので、画面の指示に従い再起動を行って下さい。

5-2. オフラインアップデート

実行画面は前項のオンラインアップデートと同じです。



予めダウンロードしたファームウェアファイルを、参照ボタンを押下し選択、実行ボタンを押下することで操作 PC から本製品にデータが送信されます。その後、画面上に再起動を促すメッセージが表示されますので、画面の指示に従い再起動を行って下さい。

ファームウェアファイルのダウンロードは、サポートサービスのユーザーサイトより実施してください。

第 6 章 サブスクリプションについて

6-1. サブスクリプション契約詳細

法人様向けエディションでは、1 年間または 3 年間の初回のサブスクリプション契約が製品ライセンスに標準で含まれています。標準のサブスクリプション契約が満了した後、継続を希望される場合は、1 年または 3 年ごとにサブスクリプション契約を更新することができます。

サブスクリプション契約が切れた場合でも、ソフトウェアは引き続き継続使用できます。サブスクリプション契約を締結いただいている限り、今後拡張される新機能の提供、バグや不具合の迅速な修正（パッチのダウンロード）および PacketiX VPN 4.0 等のメジャーバージョンアップを無償で受けることができますので、延長をお勧めいたします。サブスクリプション契約を更新しないこともできますが、以下のような理由ですべてのお客様にサブスクリプション契約の更新をお勧めします。

法人様向けエディションでは、「サブスクリプション契約」の契約期限内のみ、PacketiX VPN 4.0 の最新の新機能（機能拡張）やセキュリティホール・不具合・バグ等を修正するためのアップデートファイルをダウンロードしてインストールすることができます。

契約が切れた場合でも、契約期間中にリリースされたバージョンのソフトウェアは永続的に使用可能です。

サブスクリプション契約に関するポリシー

弊社およびソフトイーサ株式会社は、サブスクリプション契約期間中のお客様に対して、当該サブスクリプション契約に関連付けられている購入済みの PacketiX VPN 4.0 製品ライセンスのご利用にあたって以下のサービスを提供いたします。詳しくはお問合せください。

1. セキュリティパッチの無償提供 (2 営業日以内)。※アプライアンスについては、この限りではありません
   ソフトイーサ株式会社は、PacketiX VPN 4.0 にセキュリティホールが発見された場合は、そのセキュリティホールの修正が完了してから 2 営業日以内に、すべてのサブスクリプション契約者様にアップデートの案内を送付し、ダウンロード提供を開始します。すべてのサブスクリプション契約者様 は、サブスクリプション契約中に限り、そのアップデートモジュールをダウンロードし適用することができます。
2. 不具合の修正または新機能の無償提供。
   ソフトイーサ株式会社は、PacketiX VPN 4.0 にセキュリティホール以外の一般的な不具合・バグが発見された場合や、新機能が開発された場合は、随時、すべてのサブスクリプション契約者様にアップデー トの案内を送付し、ダウンロード提供を開始します。すべてのサブスクリプション契約者様は、サブスクリプション契約中に限り、そのアップデートモジュール をダウンロードし適用することができます。
3. 無償のメジャーバージョンアップ。
   次期メジャーバージョンアップ版（PacketiX VPN 4.0 を予定）が無償で提供されます。メジャーバージョンアップの度に新たな費用がかかりません。

4. 弊社からサポートを受ける権利。
   弊社に対して、電話・FAX・電子メールによるサポートを要求することができ、サブスクリプション契約期間中はサポートを受けることができます。
5. 弊社が十分なサポートを提供しない場合にソフトイーサ株式会社に対して直接サポートを要求する権利。
   万一、弊社がお客様からのサポート要求に迅速（最長でも 5 営業日以内）に返答をしない場合や、返答が不十分な場合、または弊社が破綻または事業縮小した後の場合は、ソフトイーサ株式会社が直接サポートを提供します。この場合 は、原則として電子メールまたは FAX でのやりとりでサポートを開始し、その後、ソフトイーサ株式会社が必要と判断した場合のみ電話または現地訪問によるサポートが行われる場合があります。
6. ソフトイーサ株式会社による個別カスタマイズサービス。
   お客様からの強いご要望があった場合は、ソフトイーサ株式会社は、そのお客様からいただくサブスクリプション料金の年間料金を勘案し、合理的であると判断 した場合は、無償で個別カスタマイズサービスを行います。ただし、カスタマイズにかかる費用が明らかにサブスクリプション料金の年間料金を超過すると合理 的に判断した場合は、追加料金をいただく契約を締結した上でカスタマイズを行います。詳しくはお問合せください。

6-2. ご連絡先

■電話での問い合わせ

03-5213-4372
月～金曜日（祝祭日、年末年始を除く）9:30～18:00

■E メールでの問い合わせ

support@plathome.co.jp

■返送先

〒102-0073
東京都千代田区九段北 4-1-3
日本ビルディング九段別館 3F
ぷらっとホーム株式会社 カスタマーケア課 宛

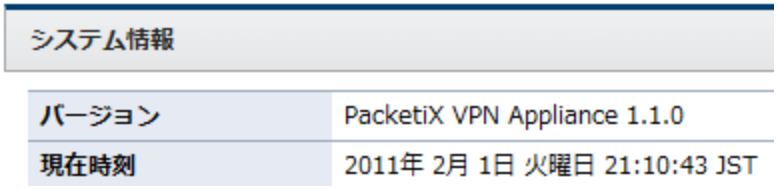
6-3. トラブル時の調査について

ご利用において、意図しない動作や希望する動作をしない場合に確認頂きたい内容を、以下に記述します。それぞれご確認頂き、ご利用環境の構成情報と併せて、前項のお問い合せ先までご連絡下さい。

◆ ファームウェアバージョン

WEB I/F

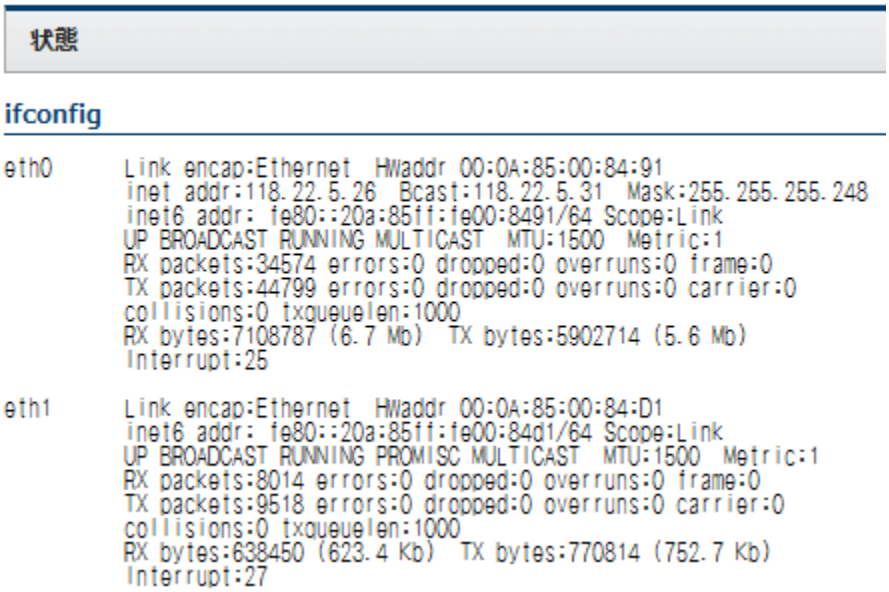
「システム」→「システム情報」で確認できます



◆ ネットワーク設定

WEB I/F

「ネットワーク」→「状態」で確認できます



◆ 設定情報の取得

WEB I/F 及び PacketiX VPN の設定情報を取得します。

- WEB I/F

  WEB I/F の「システム」→「メンテナンス」から、「WEB I/F 設定のエクスポート」を実施します

- PacketiX VPN

  サーバー管理マネージャより、接続直後の画面右下の「Config 編集」から、ファイルに保存を実施します。

- WEB I/F 及び PacketiX VPN
  USB メモリ等のストレージデバイスを用意頂き、WEB I/F の「システム」→「メンテナンス」から、設定のバックアップを実施します。前述の「WEB I/F 設定のエクスポート」と PacketiX VPN の「Config 編集」で取得可能なデータ両方を含みます。

2014 年 8 月
落丁・乱丁の場合はお取替えいたします。
PacketiX VPN 4.0 アプライアンス ユーザーズガイド
Standard / Professional Edition 版

ぷらっとホーム株式会社
〒102-0073　東京都千代田区九段北 4-1-3　日本ビルディング九段別館 3F