

EasyBlocks

PacketiX VPN アプライアンス

ユーザーズガイド

ファームウェア Ver1.0.1 以降に対応

対象モデル
EBX9/P4x



■ 商標について

- 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

本書の内容の一部または全部を、無断で転載することとはご遠慮ください。

本書の内容は予告なしに変更することがあります。

本書の内容については、正確を期するように努めていますが、誤り等に起因する結果について責任を負いかねます。

目次

1. はじめに	5
1.1. 各部の名称	5
1.1.1. 型番: EBX9/P4x	5
1.2. ケーブルクランプの取り付け	6
1.2.1. 型番: EBX9/P4x	6
1.3. ステータスインジケータの点灯について	7
1.3.1. 型番: EBX9/P4x	7
1.4. 出荷時設定情報	8
1.4.1. IP アドレス	8
1.4.1.1. 型番: EBX9/P4x	8
1.4.2. WEB I/F の URL	8
1.4.2.1. 型番: EBX9/P4x	8
1.4.3. WEB I/F の管理者ユーザー	8
1.4.3.1. 型番: EBX9/P4x	8
1.4.4. シリアルコンソール/SSH 用 管理者ユーザー	8
1.4.4.1. 型番: EBX9/P4x	8
2. 設置・初期設定	10
2.1. 設置・設定のステップ	10
2.2. 初期設定	11
2.2.1. 設定端末の設定	11
2.2.2. WEB 操作画面の表示	12
2.2.3. 使用許諾契約書の確認	13
2.2.4. 初期設定	14
2.2.5. ネットワークの設定	15
2.2.6. IP ルーティングの設定	17
2.2.7. サービスの設定	18
2.2.8. 装置の停止	19
2.3. 設置	20
3. WEB 操作画面	21

3.1.	ダッシュボード	22
3.2.	PacketiX	23
3.2.1.	サービス	23
3.2.2.	ファイル管理	25
3.2.3.	アップデート	27
3.3.	システム	28
3.3.1.	時刻設定	28
3.3.2.	フィルタ開放	31
3.3.3.	WEB 管理者	33
3.3.4.	マイページ	34
3.3.5.	EasyBlocks	35
3.3.6.	S/N	36
3.4.	ネットワーク	37
3.4.1.	基本	37
3.4.2.	プロキシ	40
3.4.3.	ルーティング	41
3.4.4.	状態	43
3.5.	メンテナンス	44
3.5.1.	設定	44
3.5.2.	システムの更新	45
3.5.3.	停止・再起動	47
3.5.4.	サポート	47
3.6.	AirManage	48
3.6.1.	AirManage	48
3.6.2.	AirManage 登録	51
4.	PacketiX VPN Server サービス詳細設定	54
4.1.	設定管理用ツールのダウンロード	54
4.1.1.	非インストーラー版の場合	54
4.1.2.	インストーラー版の場合	56
4.2.	フィルタ開放	58
4.3.	VPN Server 向け詳細設定	59
4.3.1.	接続設定の構築	59

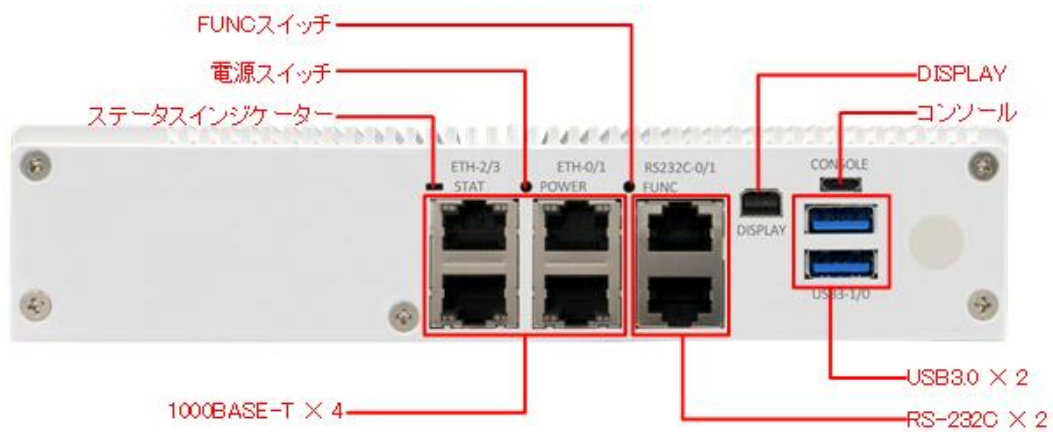
4.3.2.	VPN サーバーの構築.....	61
4.4.	VPN Bridge 向け詳細設定	65
4.4.1.	接続設定の構築	65
4.4.2.	VPN ブリッジの構築.....	67
4.5.	ライセンスの追加と削除	72
4.6.	PacketiX VPN Bridge について	73
4.7.	PacketiX VPN Client について	73
4.7.1.	PacketiX VPN Client のインストール	73
4.7.2.	PacketiX VPN Client の設定	74
5.	その他利用方法.....	76
5.1.	SSH でログイン	76
5.2.	シリアルコンソールでログイン	76
5.3.	ファクトリーリセット.....	77
5.4.	BIOS 設定	78
6.	注意事項	79
6.1.	電源断について	79
6.2.	ポート転送について	79
6.3.	ライセンスなしモデルへのライセンスキー追加について	79

1. はじめに

1.1. 各部の名称

1.1.1. 型番: EBX9/P4x

■ 前面コネクタ



■ 背面コネクタ



1.2. ケーブルクランプの取り付け

1.2.1. 型番: EBX9/P4x

AC-IN 上の穴に添付のクランプを差し込みます



1.3. ステータスインジケータの点灯について

1.3.1. 型番: EBX9/P4x

状態	ステータスインジケータ
停止中	ステータスインジケータは消灯しています。
起動処理中・停止処理中	ステータスインジケータは黄色点灯しています。
稼働中(通常稼働中)	ステータスインジケータは緑点滅しています。
稼働中(AirManage 加入失敗時)	ステータスインジケータは赤点灯しています。

1.4. 出荷時設定情報

1.4.1. IP アドレス

1.4.1.1. 型番: EBX9/P4x

インタフェース	IP アドレス	ネットマスク
Ether-0(eth0)	192.168.254.254	255.255.255.0
Ether-1(eth1)	未設定	未設定
Ether-2(eth2)	未設定	未設定
Ether-3(eth3)	未設定	未設定

1.4.2. WEB I/F の URL

1.4.2.1. 型番: EBX9/P4x

http://192.168.254.254:880/

※Edge、Chrome、Firefox 等の最新バージョン利用を推奨します。尚、WEB I/F では JavaScript を使用していますので、JavaScript は有効にしてください。

1.4.3. WEB I/F の管理者ユーザー

1.4.3.1. 型番: EBX9/P4x

初回アクセス時に、ご自身で設定していただきます。

1.4.4. シリアルコンソール/SSH 用 管理者ユーザー

1.4.4.1. 型番: EBX9/P4x

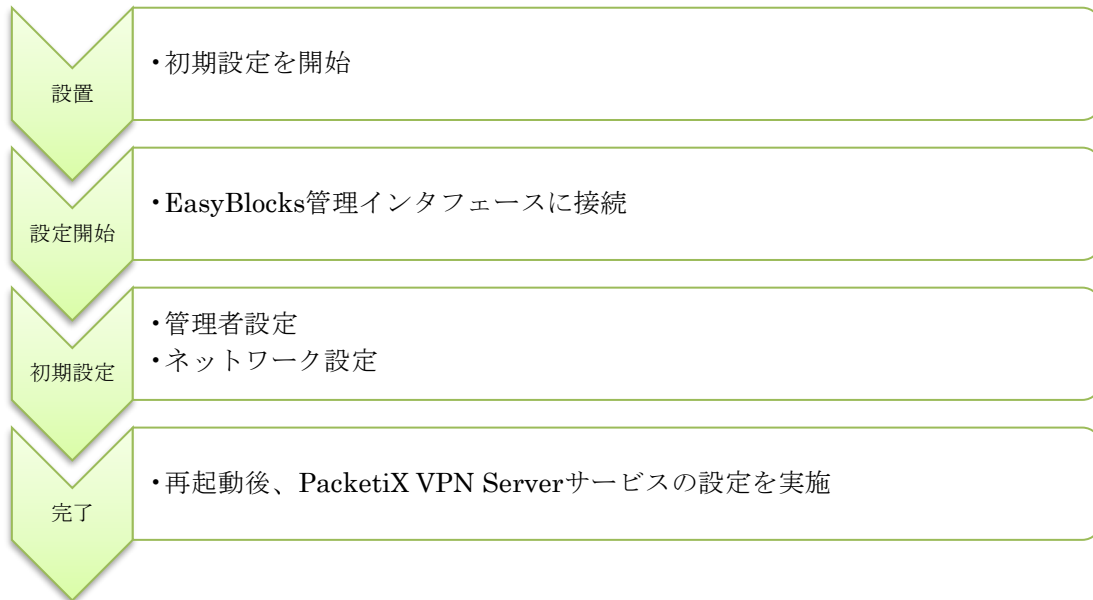
シリアルコンソールや SSH でのアクセスをしなくとも運用管理は可能ですが、必要な場合は以下の ID・パスワードを使用してください。

ID	ebsupport
パスワード	ebpacketix

※ebsupport ユーザーは `sudo` コマンドにて `bash` を使用可能です。そのため、`sudo bash` 後に必要に応じてコマンドをご使用ください。

2. 設置・初期設定

2.1. 設置・設定のステップ



2.2. 初期設定

2.2.1. 設定端末の設定

設定端末から WEB 操作画面にアクセスするための準備を行います。以下の手順で設定端末に設定を行ってください。

1. 本装置の ETHER-0 に設定端末を接続する。
2. 設定端末に 192.168.254.0/24 のホストアドレス（192.168.254.254 を除く）を設定する。

以下に設定端末の設定例を記します。

設定項目	設定値
IP アドレス	192.168.254.1
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	なし
DNS サーバアドレス	なし

表 2-a 設定端末の設定例

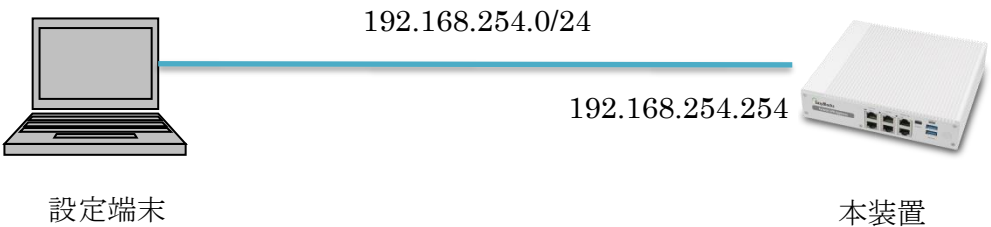


図 2-a 初期設定時のネットワーク構成

2.2.2. WEB 操作画面の表示

設定端末の WEB ブラウザで以下の URL を開いてください。

<http://192.168.254.254:880/>

2.2.3. 使用許諾契約書の確認



The screenshot shows the initial setup interface for EasyBlocks PacketiX VPN Server. At the top, the logo and product name are displayed. Below, the 'Initial Setup' (初期設定) section is active, and the 'End User License Agreement Confirmation' (使用許諾契約書の確認) step is highlighted. A scrollable text box contains the EULA terms in Japanese, including definitions and usage permissions. At the bottom, there are two buttons: 'I Agree' (同意する) and 'I Do Not Agree' (同意しない).

EasyBlocks PacketiX VPN Server

初期設定

使用許諾契約書の確認

使用許諾契約書

この契約は、お客様とぶらっとホーム株式会社（以下、当社とします。）との間に締結される契約です。お客様がこの契約に同意できない場合には、本体未開封のまま本製品および付属品一式をご購入先まで返品ください。

第1条 定義
本契約における使用許諾の範囲は、当社製品「EasyBlocks シリーズ」付属の管理ツールをいい、WUI（ウェブ・ユーザー・インターフェース）ソフトウェア製品（以下、本ソフトウェア製品とします。）および取り扱い説明書などの付属資料一式が対象となります。
本契約において「知的財産権」とは、特許権（特許出願権を含む）著作権、ノウハウその他一切の知的創作物に対する権利または法律上の利益をいいます。

第2条 使用許諾
お客様は、本契約の全項目に合意することを条件として、本ソフトウェア製品を、契約対象のハードウェアにお

同意する 同意しない

使用許諾契約書の内容に同意する場合は「同意する」と書かれたボタンをクリックしてください。「同意しない」をクリックした場合、次の画面に進むことは出来ません。

2.2.4. 初期設定

EasyBlocks PacketiX VPN Server

初期設定

使用許諾契約書の確認

使用許諾契約書

管理者アカウント

ユーザー名

パスワード

パスワード (確認)

操作

管理者アカウント設定を行います。手順は以下のとおりです。

1. 各設定項目に値を入力する。
2. 保存ボタンをクリックする。

各設定項目の詳細については、以下の表をご確認ください。

◆ 管理者アカウント

設定項目	説明
ユーザー名	管理インターフェースへのログインに使用します。英数字を使用することが出来ます。
パスワード	管理インターフェースへのログインに使用します。
パスワード (確認)	入力したパスワードが意図したとおりの値であることを確認するために、再度、パスワードを入力してください。パスワードと一致しない場合は、再度、設定していただくことになります。

2.2.5. ネットワークの設定

基本

プロキシ

ルーティング

状態

共通設定

ホスト名 (?)

ebpacketix

ドメイン名 (?)

example.org

デフォルトゲートウェイ (?)

DNSサーバ1

DNSサーバ2

DNSサーバ3

サービスネットワーク (eth0)

使用する

☒ 静的IP ☐ ローカルブリッジ ☐ いいえ

IPアドレス

192.

168.

254.

254

 /

24

 (?)

サービスネットワーク (eth1)

使用する

☐ 静的IP ☐ ローカルブリッジ ☒ いいえ

サービスネットワーク (eth2)

使用する

☐ 静的IP ☐ ローカルブリッジ ☒ いいえ

サービスネットワーク (eth3)

使用する

☐ 静的IP ☐ ローカルブリッジ ☒ いいえ

操作

保存

ネットワークの設定を行います。手順は以下のとおりです。

1. 各設定項目の値を入力する。
2. 保存ボタンをクリックする。

設定項目は以下のとおりです。

◆ 共通設定

設定項目	説明
ホスト名	ホスト名を入力してください。英数字およびハイフンを使用する事が出来ます。
ドメイン名	ドメイン名を入力してください。
デフォルトゲートウェイ	デフォルトゲートウェイを設定してください。
DNS サーバ 1 ～ 3	DNS サーバの IP アドレスを設定してください。DNS サーバが 2 つ以上存在する場合は、DNS サーバ 2 および 3 にも DNS サーバの IP アドレスを入力してください。

◆ サービスネットワーク(eth0～eth3)

設定項目	説明
使用する	サービスネットワークで使用する本装置のインターフェースを「静的 IP」選択してください。 また、ローカルブリッジとして用いるインターフェースに関しては、「ローカルブリッジ」を選択してください。
IP アドレス	サービスネットワークで使用する本装置のインターフェースの IP アドレスを入力してください。

2.2.6. IP ルーティングの設定

基本

プロキシ

ルーティング

状態

静的ルーティングが必要な場合は、ここで設定を行います。

ターゲットとゲートウェイ (2)

ネットワークアドレス

/

(?)

ゲートウェイ

操作

保存

クリア

一覧

ネットワークアドレス

ネットマスク

ゲートウェイ

操作

サービスネットワークに接続した際に、操作端末から本装置にアクセスするために IP ルーティングの設定が必要である場合は、IP ルーティングの設定を行ってください。手順は以下のとおりです。

1. ネットワークタブをクリックする
2. ネットワークタブ内のルーティングタブをクリックする。
3. ネットワークアドレスおよびゲートウェイに、適宜、値を入力し、保存ボタンをクリックする。

保存したルートは画面下部の一覧に表示されます。既に設定したルートの編集や削除を行いたい場合は一覧の「編集/削除」をクリックしてください。設定項目は以下のとおりです。

◆ ターゲットとゲートウェイ

設定項目	説明
ネットワークアドレス	ネットワークアドレスとネットマスクを指定してください。
ゲートウェイ	ゲートウェイアドレスを設定してください。

2.2.7. サービスの設定

設置前に設定を完了したい場合は、サービスの設定を行ってください。設定方法については「3.2.1 サービス」をご確認ください。

2.2.8. 装置の停止



装置を停止します。手順は以下のとおりです。

1. メンテナンスタブをクリックする。
2. メンテナンスタブの中の停止・再起動タブをクリックする。
3. 「停止・再起動」の「停止」の横にある「ボタンを表示/非表示」ボタンをクリックする。
4. 「停止・再起動」の「停止」の横にある「実行」ボタンをクリックする。
5. 停止画面に遷移したら、実行ボタンをクリックする。
6. 「本当に実行しますか？」とポップアップが表示されるので、OK をクリックする。
7. ステータスインジケータの消灯を確認後、電源ケーブルと LAN ケーブルを抜く。

2.3. 設置

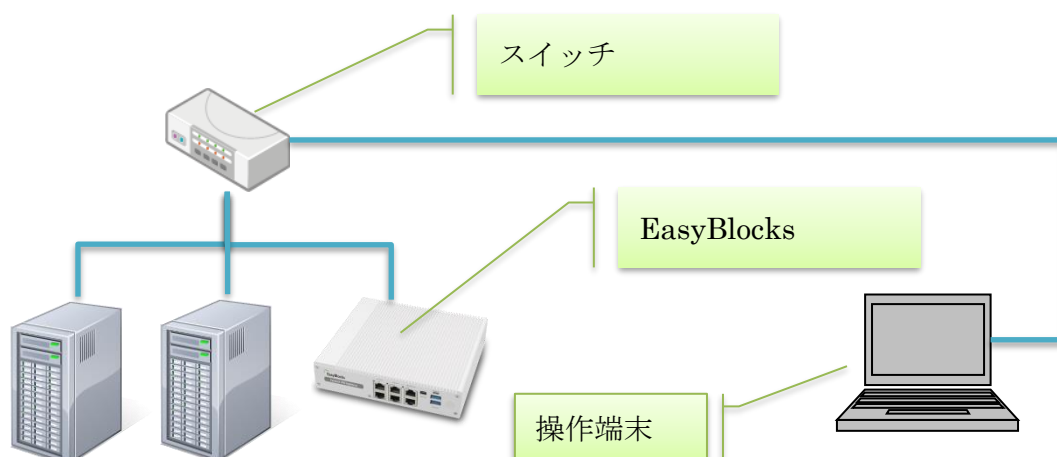


図 2-b 設置例

本装置をサービスネットワークに接続します。手順は以下のとおりです。

1. 本装置の使用するネットワークインターフェースに LAN ケーブルを接続する。
2. 本装置に接続した LAN ケーブルを、サービスネットワークのスイッチやルータに接続する。
3. ローカルブリッジを用いる場合、ローカルブリッジ用のネットワークインターフェースと該当のネットワークの LAN ケーブルを接続する。
4. 本装置に電源ケーブルを接続する。

3. WEB 操作画面

設定変更を行う場合は、操作端末から WEB ブラウザで操作画面を開いてください。
手順は以下のとおりです。

1. 操作端末の WEB ブラウザで以下の URL を開く。
`http://<使用ネットワークインターフェースの IP アドレス>:880`
例) <http://192.168.1.1:880>
2. 初期設定で設定したユーザー名およびパスワードを入力し、ログインボタンをクリックする。



図 3-a ログイン画面

3.1. ダッシュボード



システム全体の概要を表示します。各項目の詳細は以下の表のとおりです。

◆ ハードウェアリソース

項目	説明
CPU ロードアベレージ	過去 1 分間、過去 5 分間、過去 15 分間の CPU 負荷平均値です。
メインメモリ	表示される内容は以下のとおりです。 使用中/全体
ストレージ	表示される内容は以下のとおりです。 使用中/全体

◆ ネットワーク

項目	説明
FQDN	FQDN とは完全修飾ドメインのことです。 ホスト名とドメイン名を結合した値が表示されます。
ゲートウェイ	デフォルトゲートウェイが表示されます。
IPv4 アドレス(インターフェース名)	各インターフェースに割り当てられた IP アドレスが表示されます。

3.2. PacketiX

PacketiX VPN Server 機能の操作画面です。

3.2.1. サービス

サービス

ファイル管理

アップデート

サービスについて

起動 (2)

☐ 有効

☒ 無効

設定用管理ツール (2)

リンク

バージョン4.29-9680-rtm

操作

保存

動作ログ

動作ログが確認できませんでした。

サービス

ファイル管理

アップデート

サービスについて

起動 (2)

☒ 有効

☐ 無効

設定用管理ツール (2)

リンク

バージョン4.29-9680-rtm

プロセス操作

プロセス再起動

操作

保存

動作ログ

May 13 13:35:44 ebpacket ix: PacketiXサービスを起動しました。

◆ 起動

PacketiX VPN Server サービスを有効にする場合は「有効」を、無効にする場合は「無効」を選択してください。

◆ 設定管理用ツール

PacketiX VPN Server サービス自体の設定を行う場合には、設定用ツールが必要となります。右部にある「リンク」ボタンにてリンク先のタブから設定管理用ツール (PacketiX VPN Server Manager) のダウンロードを行ってください。

設定管理用ツールでの設定は EasyBlocks PacketiX VPN Server のフィルタ開放を行っている必要があります。後述の「3.3.2 フィルタ開放」を参考にポート開放を行ってください。

◆ バージョン

PacketiX VPN Server サービス自体のバージョンが記載されています。

◆ プロセス操作

意図しないサービスの停止等が発生したなど向けに、サービスプロセス再起動が行えます。

プロセスの再起動を行いたい場合には、「プロセスの再起動」ボタンを押してください。

3.2.2. ファイル管理



◆ ファイル管理

PacketiX VPN Server サービス自体にて用いているファイル一覧を確認できます。また、各種ログファイル等を選択し、「ダウンロード」ボタンを押すことによりダウンロードすることができます。

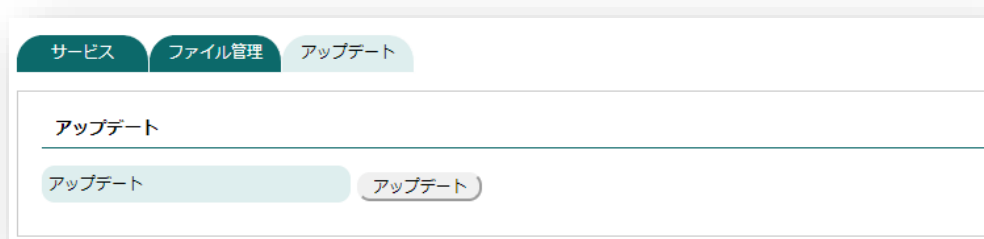
※上図の「vpn_server.config」というファイルが詳細設定ファイルです。詳細設定完了後、ダウンロードすることを推奨いたします。

◆ アップロード

アップロードプレフィックスにファイルをアップロードしたいディレクトリパスを設定します。また、ファイルを選択し、アップロードボタンを押すことでファイルをPacketiX VPN Server 内にアップロードすることができます。

※アクセス制限機能である「adminip.txt」ファイル等は本機能からアップロードしてください。

3.2.3. アップデート



◆ アップデート確認

インターネット環境を用いて PacketiX VPN Server サービス自体のアップデートの確認が行えます。

◆ アップデート

インターネット環境を用いて PacketiX VPN Server サービス自体のアップデートが行えます。

本処理は AirManage サービスを使用している必要があります。そのため、事前に AirManage サービスへ加入してください。

3.3. システム

3.3.1. 時刻設定

ダッシュボードPacketIXシステムネットワークメンテナンスAirManage技術情報

基本フィルタ開放WEB管理者マイページEasyBlocksS/N

Syslog通知 (?)

通知を行う

☐ はい ☒ いいえ

ファシリティ

local3 ▼

プロセス監視

プロセス監視 (?)

無効 ▼

時刻設定 (?)

タイムゾーン

Asia/Tokyo ▼

PCと時刻を同期 (?)

2020/05/13 13:38:25同期

ntpサーバ1 (?)

☐ オプションを使う

ntpサーバ2

☐ オプションを使う

ntpサーバ3

☐ オプションを使う

操作

保存

◆ Syslog 通知

Syslog通知 (?)

通知を行う

☐ はい ☒ いいえ

ファシリティ

local3 ▼

Syslog通知 (?)

通知を行う

☒ はい
☐ いいえ

Syslogサーバ

1. 172.16.7.224
2.
3.

ファシリティ

local3 ▼

本装置のシステム稼働・停止、サービスの起動・停止及び定期稼働を Syslog にて他ホストに対して通知することができます。

本画面の設定項目は以下のとおりです。

項目	説明
通知を行う	Syslog 通知を行うかどうかの設定を行います。
Syslog サーバ 1 ～ 3	Syslog を通知するサーバを IP アドレスまたは FQDN にて設定します。3 台まで設定可能です。
ファシリティ	送信する Syslog のファシリティを設定します。

◆ Syslog 通知

プロセス監視

プロセス監視 (2)

無効 ▼

プロセス監視	システム稼働におけるプロセスチェックを定期的(3 分毎)に行います。意図しないプロセスの終了時にアラートが発生します。
--------	---

※アラート内容はダッシュボードに表示されます。また、AirManage を使用している場合、AirManage 側にもアラートが上がるようになっています。

時刻設定 (?)

タイムゾーン Asia/Tokyo ▼

PCと時刻を同期 (?) 2020/04/13 14:41:55 同期

ntpサーバ1(2) ☐ オプションを使う

ntpサーバ2 ☐ オプションを使う

ntpサーバ3 ☐ オプションを使う

◆ 時刻設定

タイムゾーン	設置場所のタイムゾーン又は UTC を選択出来ます
PC と時刻を同期	操作用 PC の時刻情報を装置におくり反映させます
NTP サーバ	3 台まで設定可能 指定した NTP サーバから時刻情報の取得を行います。また、各サーバ毎に NTP オプションを設定可能です。

※ EasyBlocks では NTP サービスが稼働しています。そのため、NTP サーバとして使用することが可能です。

3.3.2. フィルタ開放

ダッシュボードPacketiXシステムネットワークメンテナンスAirManage技術情報

基本フィルタ開放WEB管理者マイページEasyBlocksS/N

フィルタ開放

SSH(Port:22)

☐ 開放する☒ 開放しない

PacketiX VPN,MS SSTP(Port:443)

☐ 開放する☒ 開放しない

PacketiX VPN(Port:992)

☐ 開放する☒ 開放しない

PacketiX VPN(Port:5555)

☐ 開放する☒ 開放しない

PacketiX VPN(Port:8888)

☐ 開放する☒ 開放しない

OpenVPN(Port:1194)

☐ 開放する☒ 開放しない

L2TP(Port:1701)

☐ 開放する☒ 開放しない

L2TP/IPsec(Port:500)

☐ 開放する☒ 開放しない

L2TP/IPsec(Port:4500)

☐ 開放する☒ 開放しない

その他(TCP Port) (?)

その他(UDP Port) (?)

操作

保存

◆ フィルタ開放

フィルタ開放

SSH(Port:22)

☐ 開放する
☒ 開放しない

PacketiX VPN,MS SSTP(Port:443)

☐ 開放する
☒ 開放しない

PacketiX VPN(Port:992)

☐ 開放する
☒ 開放しない

PacketiX VPN(Port:5555)

☐ 開放する
☒ 開放しない

PacketiX VPN(Port:8888)

☐ 開放する
☒ 開放しない

OpenVPN(Port:1194)

☐ 開放する
☒ 開放しない

L2TP(Port:1701)

☐ 開放する
☒ 開放しない

L2TP/IPsec(Port:500)

☐ 開放する
☒ 開放しない

L2TP/IPsec(Port:4500)

☐ 開放する
☒ 開放しない

その他(TCP Port) (?)

その他(UDP Port) (?)

SSH(Port:22)

☒ 開放する
☐ 開放しない

Port:22 解放インターフェース

☐ eth0
☐ eth1
☐ eth2
☐ eth3

EasyBlocks のフィルタを開放することができます。PacketiX VPN Server サービスではサービス提供を行う上でフィルタ開放を行う必要があります。尚、サービス名が記載されている項目については、各インターフェース毎に設定可能です。

SSH(Port:22)	SSH サービスのフィルタ開放を行います。通常では開放する必要はありません。
PacketiX VPN,MS SSTP(Port:443)	PacketiX VPN Server サービスのフィルタ開放を行います。尚、本ポートは設定用のポート番号となります。
PacketiX VPN(Port:992)	PacketiX VPN Server サービスのフィルタ開放を行います。
PacketiX VPN(Port:5555)	PacketiX VPN Server サービスのフィルタ開放を行います。

PacketiX VPN(Port:8888)	PacketiX VPN Server サービスのフィルタ開放を行います。
OpenVPN(Port:1194)	Open VPN サービスのフィルタ開放を行います。
L2TP(Port:1701)	L2TP サービスのフィルタ開放を行います。
L2TP/IPsec(Port:500)	L2TP/IPsec サービスのフィルタ開放を行います。
L2TP/IPsec(Port:4500)	L2TP/IPsec サービスのフィルタ開放を行います。
その他(TCP Port)	上記項目以外で開放したい TCP のポート番号をスペース区切りにて指定してください。尚、指定したポート番号は全インターフェースに開放されます。
その他(UDP Port)	上記項目以外で開放したい UDP のポート番号をスペース区切りにて指定してください。尚、指定したポート番号は全インターフェースに開放されます。

3.3.3. WEB 管理者

ダッシュボード
PacketiX
システム
ネットワーク
メンテナンス
AirManage
技術情報

基本
フィルタ開放
WEB管理者
マイページ
EasyBlocks
S/N

追加・変更

ユーザー名 (2)

パスワード

操作

保存

クリア

一覧

ユーザー名

操作

admin
[編集 / 削除](#)

◆ 追加・変更

The screenshot shows a web interface with a top navigation bar containing tabs: 基本, フィルタ開放, WEB管理者, マイページ, EasyBlocks, and S/N. The 'WEB管理者' tab is selected. Below the navigation bar, the '追加・変更' section is active. It contains two input fields: 'ユーザー名 (?)' and 'パスワード'. Below these fields is a '操作' (Action) section with two buttons: '保存' (Save) and 'クリア' (Clear).

ユーザー名	WEB I/F にアクセスする WEB 管理者を追加(変更)するユーザー名を設定します。
パスワード	WEB I/F にアクセスする WEB 管理者を追加(変更)するユーザーのパスワードを設定します。

3.3.4. マイページ

The screenshot shows a web interface with a top navigation bar containing tabs: ダッシュボード, PacketiX, システム, ネットワーク, メンテナンス, AirManage, and 技術情報. The 'システム' tab is selected. Below the navigation bar, the 'マイページ' section is active. It contains two input fields: 'ユーザー名' (with the value 'admin') and 'パスワード'. Below these fields is a '操作' (Action) section with two buttons: '保存' (Save) and 'クリア' (Clear).

◆ 登録情報の編集

登録情報の編集

ユーザー名 admin

パスワード

操作

保存 クリア

ユーザー名	ログイン中のアカウントの登録情報を編集するため、ユーザー名は変更できません
パスワード	変更するパスワードを入力します。

3.3.5. EasyBlocks

ダッシュボード PacketiX システム ネットワーク メンテナンス AirManage 技術情報

基本 フィルタ開放 WEB管理者 マイページ EasyBlocks S/N

使用許諾/オープンソースライセンス

選択 選択したものを表示します ▼

EasyBlocksについて

バージョン [システム]

◆ 使用許諾/オープンソースライセンス

EasyBlocks PacketiX VPN Server で使用しているソフトウェアのライセンス情報を見ることが出来ます。

◆ バージョン

EasyBlocks PacketiX VPN Server 本装置自体のバージョンが確認できます。

3.3.6. S/N



◆ 本体シリアル番号

EasyBlocks 本体のシリアル番号を確認することができます。

3.4. ネットワーク

3.4.1. 基本

The screenshot displays the 'Network' configuration page in the PacketiX management interface. The top navigation bar includes 'ダッシュボード', 'PacketiX', 'システム', 'ネットワーク' (selected), 'メンテナンス', 'AirManage', and '技術情報'. Below this, the 'Network' section has four sub-tabs: '基本' (selected), 'プロキシ', 'ルーティング', and '状態'. The '基本' tab is divided into two main sections: '共通設定' (Common Settings) and 'サービスネットワーク' (Service Networks).

共通設定 (Common Settings)

- ホスト名 (2): ebpacketix
- ドメイン名 (2): example.org
- デフォルトゲートウェイ (2): 172.16.7.1
- DNSサーバ1: 172.16.2.6
- DNSサーバ2:
- DNSサーバ3:

サービスネットワーク (eth0)

- 使用する: ☒ 静的IP ☐ ローカルブリッジ ☐ いいえ
- IPアドレス: 172.16.7.233 / 24 (2)

サービスネットワーク (eth1)

- 使用する: ☐ 静的IP ☒ ローカルブリッジ ☐ いいえ

サービスネットワーク (eth2)

- 使用する: ☐ 静的IP ☐ ローカルブリッジ ☒ いいえ

サービスネットワーク (eth3)

- 使用する: ☐ 静的IP ☐ ローカルブリッジ ☒ いいえ

操作

- 保存

ネットワーク設定を行う画面です。設定の手順は以下のとおりです。

1. 各設定項目に値を入力する。
2. 画面下部、操作の保存ボタンをクリックする。
3. 再起動を行う。

設定項目は以下のとおりです。

項目	説明
ホスト名	本装置に割り当てるホスト名を入力してください。使用できる文字は英数字とハイフンです。
ドメイン名	本装置を設置したネットワークのドメイン名を入力してください。
デフォルトゲートウェイ	デフォルトゲートウェイの IP アドレスを入力してください。
DNS サーバ 1 ～ 3	名前解決に使用する DNS サーバの IP アドレスを指定してください。複数の DNS サーバを指定する場合は、DNS サーバ 2 および DNS サーバ 3 にも DNS サーバの IP アドレスを入力してください。

◆ サービスネットワーク (eth0～)

サービスネットワーク (eth0)

使用する

☒ 静的IP
☐ ローカルブリッジ
☐ いいえ

IPアドレス

172.16.7.233 / 24 (?)

サービスネットワーク (eth1)

使用する

☐ 静的IP
☒ ローカルブリッジ
☐ いいえ

各ネットワークインターフェースの IP アドレス及びローカルブリッジを設定する画面です。設定の手順は以下のとおりです。

1. サービスネットワークとして使用するインターフェースの「静的 IP」、「ローカルブリッジ」、「いいえ」欄のラジオボタンを選択する。
2. 静的 IP の場合、設定項目に値を入力する。
3. 画面下部、操作の保存ボタンをクリックする。
4. 再起動を行う。

設定項目は以下のとおりです。

項目	説明
使用する	サービスネットワークで使用する本装置のインターフェースを「静的 IP」選択してください。 また、ローカルブリッジとして用いるインターフェースに関しては、「ローカルブリッジ」を選択してください。
IP アドレス	サービスネットワークで使用する本装置のインターフェースの IP アドレスを入力してください。

3.4.2. プロキシ

The screenshot shows the 'ネットワーク' (Network) tab in the PacketIX interface. Under the 'プロキシ' (Proxy) sub-tab, there is a section titled 'プロキシ(必要な場合)' (Proxy (if needed)). This section contains three input fields: 'アドレス:ポート' (Address:Port) with the value 'http://(proxy.example.org) : (8080)', 'BASIC認証(必要な場合)' (BASIC authentication (if needed)) with 'ユーザーID: (username)' and 'パスワード: (password)', and '非Proxyアクセスホスト' (Non-proxy access host) with the value '(127.0.0.1,localhost)'. Below these fields is an '操作' (Operation) section with a '保存' (Save) button.

◆ プロキシ

This is a close-up of the 'プロキシ(必要な場合)' (Proxy (if needed)) section. It shows the following fields and values:

- アドレス:ポート: http://(proxy.example.org) : (8080)
- BASIC認証(必要な場合): ユーザーID: (username) パスワード: (password)
- 非Proxyアクセスホスト: (127.0.0.1,localhost)

外部への WEB アクセスに HTTP proxy を経由する必要がある環境では、本装置内で用いているソフトウェアのオンラインアップデートに本設定が必要となります。設定の手順は以下のとおりです。

1. 各設定項目に値を入力する。
2. 操作の保存ボタンをクリックする
3. 再起動を行う。

設定項目は以下の通りです。

項目	説明
アドレス：ポート	HTTP proxy の URL とポート番号を入力してください。
BASIC 認証	HTTP proxy に認証が必要である場合は、ユーザーID とパスワードを入力してください。
非 Proxy アクセスホスト	HTTP proxy を非経由でアクセスする際に用いるホストを”,”区切りにて指定します。また、AirManage 及びダイナミック DNS 機能では HTTP 通信を行っております。非経由にてアクセスしたい場合には FQDN を追加してください。

3.4.3. ルーティング

ダッシュボードPacketIXシステムネットワークメンテナンスAirManage技術情報

基本プロキシルーティング状態

静的ルーティングが必要な場合は、ここで設定を行います。

ターゲットとゲートウェイ (2)

ネットワークアドレス

ゲートウェイ

操作

保存

クリア

一覧

ネットワークアドレス

ネットマスク

ゲートウェイ

操作

静的ルーティング設定を行う画面です。設定の手順は以下のとおりです。

41/80

1. 各設定項目に値を入力する。
2. 操作の保存ボタンをクリックする。
3. 再起動を行う。

保存が完了すると、画面下部の一覧に設定した内容が反映されます。

設定項目は以下のとおりです。

項目	説明
ネットワークアドレス	パケットの送信先のネットワークアドレスとネットマスク（プレフィックス長）を指定してください。
ゲートウェイ	ゲートウェイの IP アドレスを入力してください。

3.4.4. 状態

ダッシュボードPacketIXシステムネットワークメンテナンスAirManage技術情報

基本プロキシルーティング状態

状態

ip addr show up

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0a:85:14:ff:f4 brd ff:ff:ff:ff:ff:ff
    inet 172.16.7.233/24 brd 172.16.7.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20a:85ff:fe14:fff4/64 scope link
        valid_lft forever preferred_lft forever
5: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether 00:0a:85:14:ff:f5 brd ff:ff:ff:ff:ff:ff
```

netstat -nr

Kernel IP routing table						
Destination	Gateway	Genmask	Flags	MSS	Window	irtt Iface
0.0.0.0	172.16.7.1	0.0.0.0	UG	0	0	0 eth0
172.16.7.0	0.0.0.0	255.255.255.0	U	0	0	0 eth0

arp -an

```
? (172.16.7.116) at d0:50:99:1a:14:cb [ether] on eth0
? (172.16.7.1) at 00:a0:de:85:73:41 [ether] on eth0
```

/etc/hosts

```
#
# $ssdlinux: hosts,v 1.1.1.1 2002/05/01 15:55:18 kanoh Exp $
#
# Host Database
# This file should contain the addresses and aliases
# for local hosts that share this file.
# It is used only for "ifconfig" and other operations
# before the nameserver is started.
#
::1                localhost
127.0.0.1          localhost
127.0.0.1          ebpacketix.example.org
```

/etc/resolv.conf

```
nameserver 172.16.2.6
```

以下のコマンドの結果を確認する事が出来ます。

- ip addr show up
- netstat -nr
- arp -an
- cat /etc/hosts
- cat /etc/resolv.conf

3.5. メンテナンス

3.5.1. 設定

設定

システムの更新

停止・再起動

サポート

設定情報

エクスポート (2)

実行

インポート (2)

ファイルを選択

選択されていません

実行

エクスポート	EasyBlocks 全体の設定をエクスポート
インポート	// をインポート

本項目でのエクスポート及びインポートでは、PacketiX VPN Server サービスの詳細設定は含まれません。そのため、PacketiX VPN Server サービスの詳細設定のエクスポートについては、「3.2.2 ファイル管理」にてダウンロードを行ってください。また、インポートについては設定管理用ツール(PacketiX VPN Server Manager)の Config 編集機能を用いてください。

3.5.2. システムの更新

設定

システムの更新

停止・再起動

サポート

アップデート

オンライン

(確認結果)

更新有無を確認

オフライン

ファイルを選択

選択されていません

実行

設定

システムの更新

停止・再起動

サポート

アップデート

オンライン

更新があります

更新有無を確認

更新予約をする

更新情報

オフライン

ファイルを選択

選択されていません

実行

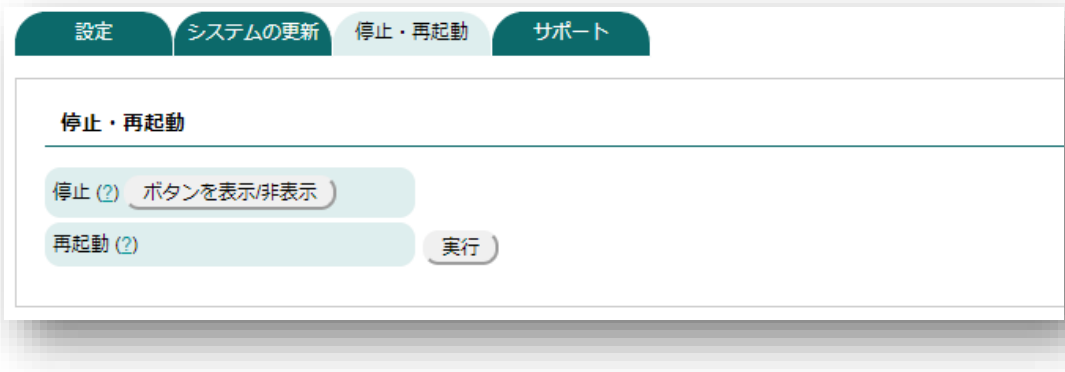
* Packages list

ebpacketix-srv-webui 0.1.0-1 -> 0.1.0-2

オンライン	<p>「更新有無を確認」ボタンを押すことによりインターネット接続を用いて、アップデートデータがあるか確認を行います。</p> <p>また、アップデートデータが存在する場合、「更新予約をする」ボタンが表示されます。このボタンを押し、再起動を行うことで、アップデートが行われます。</p>
オフライン	<p>オフラインアップデート用のファイルをアップロードすることで、インターネット接続がなくても本製品のアップデートを実行します。再起動を行うことでアップデートが行われます。</p>

オンラインアップデートは **AirManage** サービスを使用している必要があります。
 そのため、事前に **AirManage** サービスへ加入してください。

3.5.3. 停止・再起動



停止	EasyBlocks を停止します
再起動	// を再起動します

3.5.4. サポート

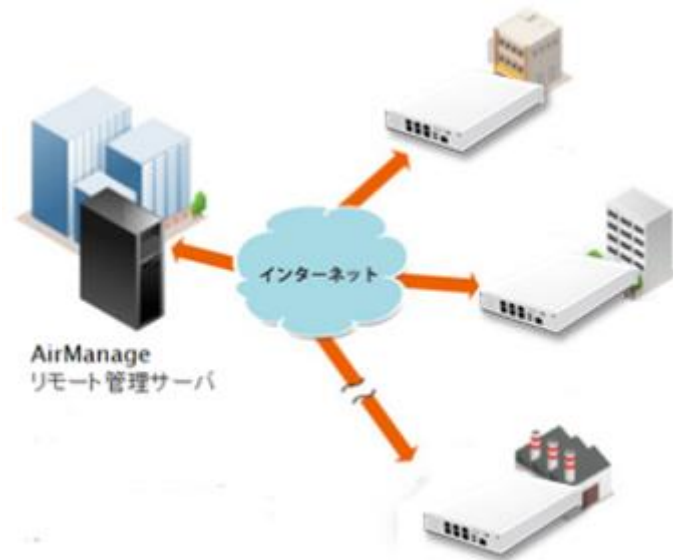


問い合わせ先	弊社サポートの連絡先を記載しております。
ログ・環境情報取得	不具合等の問い合わせ時には、こちらでダウンロードした情報をお送り下さい。状況確認の参考にさせていただきます。ダウンロードできるデータは、tar + gzip 形式でありご自身で内容をご確認いただくことも可能です。

3.6. AirManage

AirManage は遠隔地に配備した EasyBlocks を管理する機能です。

AirManage はインターネット上に用意している AirManage リモート管理サーバと各 EasyBlocks 間で通信を行い、各 EasyBlocks の管理や制御等を行います。



3.6.1. AirManage

AirManage サービスを使用する場合には、事前に AirManage リモート管理サーバ側に EasyBlocks を登録する必要があります。登録が未完了の場合や確認を行いたい場合は「AirManage 登録」を先に実施してください。

AirManage	AirManage登録
AirManage	
使用設定	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
操作	
<input type="button" value="保存"/>	

AirManage
AirManage登録

AirManage

使用設定

☒ 使用する
 ☐ 使用しない

Caution) 設定を保存すると本項目は適用されます。そのため、サービス有効状態のまま保存すると再適用されますのでご注意ください。

適用方法

☒ サービス加入のみ
 ☐ ゼロコンフィグ(ネットワーク設定保持)
 ☐ ゼロコンフィグ

サービス適用URL

事前確認

操作

保存

使用設定	AirManage サービスを使用するかの設定を選択します。
適用方法	<p>AirManage サービスに参加する際の設定方法を以下から選択します。</p> <ul style="list-style-type: none"> ●サービス加入のみ AirManage サーバへアクセスを行うのみです。コンフィグは適用されませんが、サービスに加入し各種機能が使用可能となります。 ●ゼロコンフィグ(ネットワーク設定保持) AirManage サーバからコンフィグをダウンロードしネットワークの設定以外について EasyBlocks へ適用します。 ●ゼロコンフィグ AirManage サーバからコンフィグをダウンロードし全ての設定を EasyBlocks へ適用します。
サービス適用 URL	<p>サービス加入の際に弊社から連絡のあった FQDN 情報をフォームに入力します。</p> <p>※後述の AirManage 登録にて確認まで済ませた場合、フォームは自動で反映されます。</p>
事前確認	<p>「確認」ボタンを押すことでノード側のネットワーク及び設定している URL 情報を用いて、AirManage サーバ側に登録されているか確認を行います</p>

事前確認の「確認」ボタンを押し **AirManage** が問題なく利用できる状態の場合、「保存&実行」ボタンが表示されます。「保存&実行」を押した場合、即座に **AirManage** を利用する為の再起動処理が行われます。

3.6.2. AirManage 登録

本項目では、EasyBlocks がインターネットへの接続が行える必用があります。

AirManage

AirManage登録

AirManage登録手順

AirManageを利用する場合、以下の手順に従って本体の登録を完了する必要があります。
尚、既にアカウント作成及びテナントの作成が完了している場合に、本体登録までの手順を省略することができます。
その場合には、各フェーズでは確認を行うのみで問題ありません。
i. アカウント作成
ii. テナント作成
iii. 本体登録

AirManageを使用するにはサブスクリプションへ加入する必要があります。
サブスクリプションの有効期限の確認や期限の延長に関しては [こちら](#) をご使用ください。

AirManageアカウント確認

E-Mail

test@example.com

操作

アカウント確認

◆ アカウント確認

AirManage のアカウントが存在しているかの確認を行います。存在していない場合、アカウント作成フォームが表示されます。尚、アカウントが存在しテナントに所属していない場合、テナント作成フォームが表示されます。

E-Mail	AirManage サービスのログインアカウントに用いる E-Mail アドレスを入力します。
操作	「アカウント確認」ボタンを押すことにより、AirManage サービスのアカウントが存在しているか確認を行います。

◆ アカウント作成

AirManage のアカウントが存在していない場合、アカウントを作成する必要があります。

アカウント名	AirManage サービスにて表示されるアカウント名を入力します。
パスワード	AirManage サービスにログインする際のパスワードを入力します。パスワードに使用可能な文字は” ” (スペース)を除く半角英数字となります。また、文字数は最低 8 文字となります。
パスワード(確認用)	AirManage サービスにログインする際の確認用のパスワードを入力します。
操作	「アカウント作成」 ボタンを押すことにより、AirManage サービスのアカウント作成処理を行います。 作成処理が正常に行われた場合、設定している E-Mail アドレス宛に仮登録受付メールが届きます。メール本文内からのブラウザでアクセスすることで、本登録が行われます。

アカウント作成ボタンを押してから 15 分以内にメール内の URL から WEB アクセスを行ってください。

WEB アクセスを行わず一定時間を経過した場合、登録作業中の情報は破棄されるため再度アカウント作成ボタンを押す必要があります。

◆ テナント作成

アカウントがテナントに所属していない場合、テナント作成フォームが表示されます。

テナント記号	ユーザーが所属するテナントをユニークに扱う為、記号(名称)を入力します。入力可能文字は英数字及び記号の”_”となります。
操作	「テナント作成」 ボタンを押すことにより、テナントの作成処理が行われます。既に同一名のテナントが存在する場合には作成できません。

◆ 本体登録確認

AirManage サービスに、EasyBlocks 本体が登録されているか確認を行います。登録されていない場合、本体登録フォームが表示されます。

操作	「本体登録確認」ボタンを押すことにより、EasyBlocks 本体が AirManage に登録されているか確認を行います。 既に問題なく登録されている場合には、AirManage の初回アクセス設定部の設定を反映する確認のポップアップが表示されますので、「OK」等の了承するボタンを押してください。
----	---

◆ 本体登録

AirManage に EasyBlocks 本体の登録を行います。

ノード名	AirManage のテナント内で EasyBlocks 本体をユニークに識別する為のノード名を入力します。 入力可能文字は英数字及び記号の”_”となります。
操作	「本体登録」ボタンを押すことにより、EasyBlocks 本体がテナント一覧で選択しているテナントに対して、入力したノード名で AirManage に登録されます。 正常に登録できた場合、AirManage の初回アクセス設定部の設定を反映する確認のポップアップが表示されますので、「OK」等の了承するボタンを押してください。

登録が完了したら、”3.6.1 AirManage”を参考に AirManage の利用開始を行ってください。

4. PacketiX VPN Server サービス詳細設定

4.1. 設定管理用ツールのダウンロード

設定管理用ツール(PacketiX VPN Server Manager)のダウンロードを行います。サービスタブのリンクボタンからアクセスまたは以下の URL からダウンロードを行ってください。

(インストーラー版をダウンロードした場合には、インストーラーの指示に従いインストール作業を行ってください。)

※ダウンロード URL

<http://www.packetix-download.com/>

4.1.1. 非インストーラー版の場合

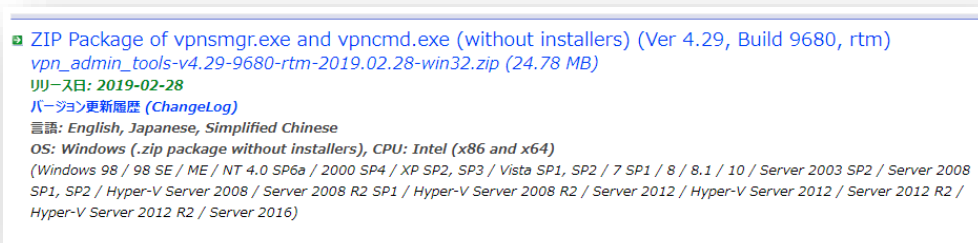
下図のように選択を行い、対象の設定管理用ツールを選択します。



The screenshot shows the 'PacketiX VPN ダウンロードセンター' (PacketiX VPN Download Center) web page. It features a header with the title and a link to the software company's website. Below the header, there are four sections for selecting download options, each with a dropdown menu:

- ダウンロードするソフトウェアを選択** (Select software to download): PacketiX VPN (Commercial) ▼
- コンポーネントを選択** (Select component): PacketiX VPN Server Manager for Windows ▼
- プラットフォームを選択** (Select platform): Windows (.zip package without installers) ▼
- CPU を選択** (Select CPU): Intel (x86 and x64) ▼

設定管理用ツールのバージョンは rtm ver. を推奨します。



ダウンロード後、Zip ファイルがダウンロードされますので、解凍を行います。

名前	更新日時	種類	サイズ
hamcore.se2	2019/02/28 19:21	SE2 ファイル	22,092 KB
ReadMeFirst_Important_Notices_cn.txt	2019/02/28 19:21	テキスト文書	31 KB
ReadMeFirst_Important_Notices_en.txt	2019/02/28 19:21	テキスト文書	36 KB
ReadMeFirst_Important_Notices_ja.txt	2019/02/28 19:21	テキスト文書	50 KB
ReadMeFirst_License.txt	2019/02/28 19:21	テキスト文書	63 KB
vpncmd.exe	2019/02/28 19:21	アプリケーション	3,934 KB
vpnsmgr.exe	2019/02/28 19:21	アプリケーション	3,935 KB

設定管理用ツールを起動する場合には、「vpnsmgr.exe」を実行してください。

4.1.2. インストーラー版の場合

下図のように選択を行い、対象の設定管理用ツールを選択します。



PacketiX VPN ダウンロードセンター

ダウンロードするソフトウェアを選択

PacketiX VPN (Commercial) ▼

コンポーネントを選択

PacketiX VPN Server Manager for Windows ▼

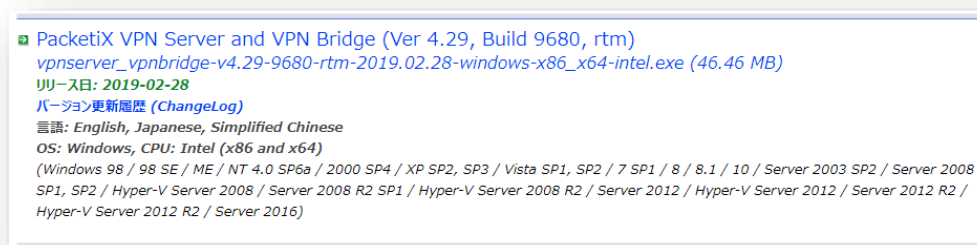
プラットフォームを選択

Windows ▼

CPU を選択

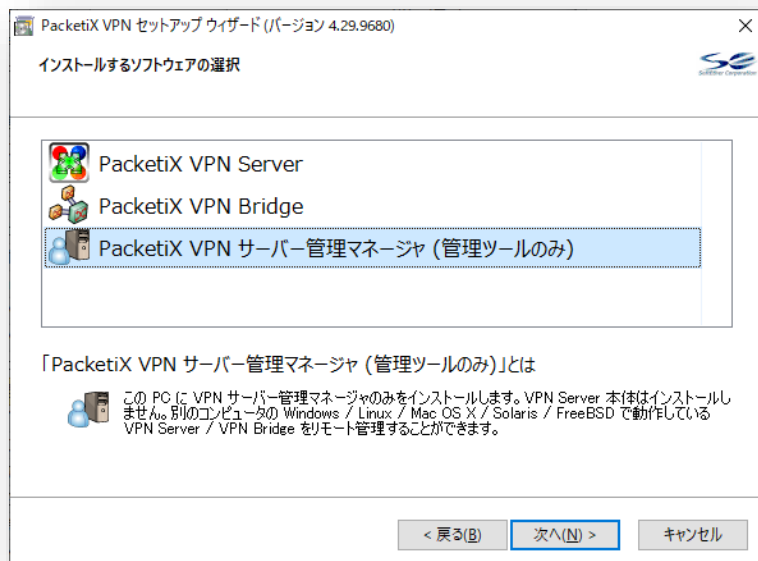
Intel (x86 and x64) ▼

設定管理用ツールのバージョンは **rtm ver.**を推奨します。



PacketiX VPN Server and VPN Bridge (Ver 4.29, Build 9680, rtm)
[vpnserver_vpnbridge-v4.29-9680-rtm-2019.02.28-windows-x86_x64-intel.exe \(46.46 MB\)](#)
リリース日: 2019-02-28
[バージョン更新履歴 \(ChangeLog\)](#)
言語: English, Japanese, Simplified Chinese
OS: Windows, CPU: Intel (x86 and x64)
(Windows 98 / 98 SE / ME / NT 4.0 SP6a / 2000 SP4 / XP SP2, SP3 / Vista SP1, SP2 / 7 SP1 / 8 / 8.1 / 10 / Server 2003 SP2 / Server 2008 SP1, SP2 / Hyper-V Server 2008 / Server 2008 R2 SP1 / Hyper-V Server 2008 R2 / Server 2012 / Hyper-V Server 2012 / Server 2012 R2 / Hyper-V Server 2012 R2 / Server 2016)

ダウンロードした、インストーラーを起動しアナウンスに沿ってインストールを行います。尚、インストールするソフトウェアの選択では「PacketiX VPN サーバー管理マネージャ(管理ツールのみ)」を選択してください。



設定管理用ツールを起動する場合には、スタートメニューから「VPN サーバー管理(ツール)」を実行してください。



4.2. フィルタ開放

設定管理用ツールにて PacketiX VPN Server サービスの詳細設定を行う場合、443 番、992 番、8888 番のいずれかのポートを開放する必要があります。また、実際の PacketiX VPN Server サービス自体の運用を行う場合には、使用する対応サービスのポートを開放する必要があります。

そのため、「3.3.2 フィルタ開放」を参照しフィルタの開放を行ってください。

基本

フィルタ開放

WEB管理者

マイページ

EasyBlocks

S/N

フィルタ開放

SSH(Port:22)

☐ 開放する ☒ 開放しない

PacketiX VPN,MS SSTP(Port:443)

☒ 開放する ☐ 開放しない

Port:443 解放インターフェース

☒ eth0 ☐ eth1 ☐ eth2 ☐ eth3

PacketiX VPN(Port:992)

☐ 開放する ☒ 開放しない

PacketiX VPN(Port:5555)

☐ 開放する ☒ 開放しない

PacketiX VPN(Port:8888)

☐ 開放する ☒ 開放しない

OpenVPN(Port:1194)

☐ 開放する ☒ 開放しない

L2TP(Port:1701)

☐ 開放する ☒ 開放しない

L2TP/IPsec(Port:500)

☐ 開放する ☒ 開放しない

L2TP/IPsec(Port:4500)

☐ 開放する ☒ 開放しない

その他(TCP Port) (?)

その他(UDP Port) (?)

操作

保存

4.3. VPN Server 向け詳細設定

Standard/Professional/Enterprise Edition を 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。

本装置を VPN Server として運用する場合、付属のライセンス発行キーを用いてライセンスキーの発行を行ってください。

ライセンスキー発行後、「ライセンスの追加と削除」にてライセンスの追加を行ってください。

4.3.1. 接続設定の構築

管理マネージャーを起動します。初回起動の為、接続先の作成が必要となります。その為、「新しい接続設定」をクリックします。



接続設定名及びホスト名を入力します。尚、ポート番号を変更し運用する場合にはポート番号についても変更を行います。

新しい接続設定の作成

管理する VPN Server の接続設定を行います。

接続設定名(N): PacketiX_VPN

接続先 VPN Server の指定(B):

管理したい VPN Server が動作しているコンピュータのホスト名または IP アドレスおよびポート番号を指定してください。

ホスト名(H): 172.16.7.238

☐ このコンピュータ (localhost) に接続(L)

ポート番号(P): 443 (TCP ポート)

経由するプロキシサーバーの設定(O):

プロキシサーバーを経由して VPN Server に接続することができます。

プロキシの種類(Y):

- ☒ 直接 TCP/IP 接続 (プロキシを使わない) (D)
- ☐ HTTP プロキシサーバー経由接続(I)
- ☐ SOCKS プロキシサーバー経由接続(X)

プロキシサーバーの接続設定(R)

管理モードの選択とパスワードの入力(M)

VPN Server (には、サーバー管理モードと仮想 HUB 管理モードのどちらかのモードで接続できます。

サーバー管理モードで接続すると、VPN Server の設定とすべての仮想 HUB が管理できます。

仮想 HUB 管理モードで接続すると、権限を持っている仮想 HUB の管理ができます。

☒ サーバー管理モード(S) ☐ 仮想 HUB 管理モード(U)

仮想 HUB 名(V):

管理モードで接続する際のパスワードを入力してください。

管理パスワード(A):

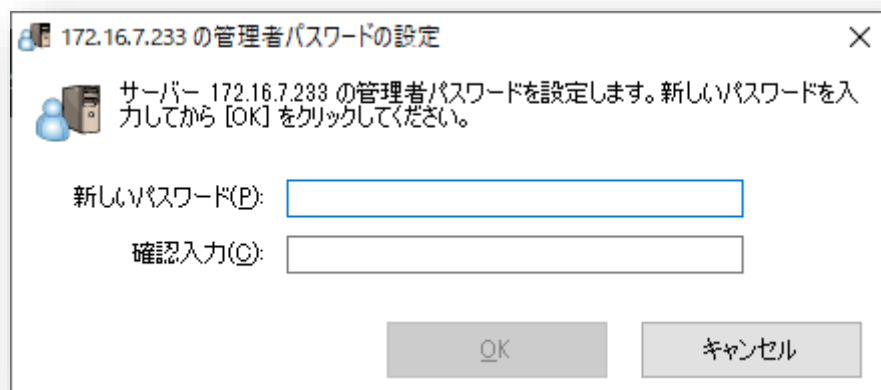
☐ 管理パスワードを保存しない(X)

OK キャンセル

4.3.2. VPN サーバーの構築

上記で構築した接続先に対して接続を行います。接続が行えない場合、サービスが起動していない、フィルタが開放されていない、ネットワーク的に接続できない等の可能性があります。

初回接続時は、管理者パスワードの設定を求められますので、管理者パスワードを設定します。



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。「リモートアクセス VPN サーバー」にチェックを入れ、「次へ」を選択します。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。

PacketiX VPN Server / Bridge 簡易セットアップ

PacketiX VPN Server / Bridge 簡易セットアップ

このセットアッププログラムを使用すると、PacketiX VPN Server または VPN Bridge を以下の用途や目的のために簡単にセットアップすることができます。セットアップ終了後は、VPN サーバー管理マネージャを用いて、より詳細な設定を自由に行うことができます。

構築しようとしている VPN サーバーの種類を選択してください。複数の用途のための VPN サーバーを構築しようとしている場合は、複数の種類を選択することができます。

☒ **リモートアクセス VPN サーバー(R)**

リモートアクセス VPN は、たとえば社内 LAN などの既存の Ethernet セグメントに対して、インターネットなどを経由して遠隔地の VPN クライアントコンピュータが VPN 接続することができる形態の VPN 構成です。
VPN Server に接続した VPN クライアントコンピュータは、社内の Ethernet に対して直接 LAN ケーブルで接続しているのと同等の状態でネットワークにアクセスできるようになります。



☐ **拠点間接続 VPN サーバーまたはブリッジ(S)**

拠点間接続 VPN は、既存の 2 箇所以上の拠点の Ethernet セグメント同士を VPN 接続する形態の VPN 構成です。
VPN 接続されたそれぞれの拠点同士はレイヤ 2 レベルで同一のセグメントとなりますので、各拠点内のコンピュータ同士が同一ネットワーク内にあるものとして通信することができます。

この VPN Server の役割を選択してください。

☐ 拠点間接続 VPN の中心となり、他拠点からの接続を受け入れる VPN Server (M)

☐ 各拠点に設置する VPN Server または VPN Bridge (E)



☐ **高度な機能を用いた VPN (Q)**

クラスタリング機能や仮想レイヤ 3 スイッチ機能などの高度な機能を提供する VPN システムを構築する場合。

[次へ] をクリックすると、セットアップを開始します。[閉じる] をクリックすると、このセットアップ画面を閉じ、手動ですべての設定を行うことができます。

次へ(N) 閉じる(C)

いくつかの画面が表示された後、ユーザー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、事前に WEB UI にてローカルブリッジとして設定したインターフェースをこの画面上で仮想 HUB に接続する物理 I/F として選択しておきます。


簡易セットアップの実行
×



この VPN Server / VPN Bridge のセットアップを完了するには、下記のタスクのうち必要なものを実行してください。

1. VPN 接続を受け入れるためのユーザーの作成


 この VPN Server がリモートアクセス VPN を受け入れる場合、または拠点間接続 VPN において中心となり他拠点からの接続を受け入れる場合は、VPN 接続を受け入れるためにユーザーを作成しておく必要があります。

ユーザーを作成する(U)

2. 接続先の VPN Server への接続設定


 拠点間接続 VPN における各拠点に設置する VPN Server または VPN Bridge の場合は、各 VPN 拠点からの接続を受け付ける、中心となる VPN Server のアドレスなどを入力して、その VPN Server への接続を確立する必要があります。

接続先の VPN Server への接続設定を行う(Q)

3. ローカルブリッジの設定


 VPN 経由で LAN にアクセスするためには、VPN 側の仮想的な Ethernet セグメントと物理的な Ethernet セグメントとの間を「ローカルブリッジ接続」機能でブリッジ接続する必要があります。

VPN に対してブリッジ接続する既存の Ethernet デバイス (LAN カード) を選択してください。

ブリッジ接続する Ethernet デバイスを選択してください

必要な設定がすべて完了したら、[閉じる] をクリックしてください。VPN Server / VPN Bridge の詳細な管理画面が表示されます。その後は必要な場合に詳細な設定を行ってください。

閉じる(C)

ユーザー作成では、ユーザー名、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。

ユーザーの新規作成

ユーザー名(U):

本名(B):

説明(N):

グループ名 (省略可能): グループの参照(R)...

☐ このアカウントの有効期限を設定する(S)

2020年 5月 14日 0:00:00

認証方法(A):

- ☒ 匿名認証
- ☐ パスワード認証
- ☐ 固有証明書認証
- ☐ 署名済み証明書認証
- ☐ RADIUS 認証
- ☐ NT ドメイン認証

RADIUS または NT ドメイン認証

外部の RADIUS サーバー、Windows NT ドメインコントローラ、または Active Directory コントローラによってユーザーが入力したパスワードが検証されます。

☐ 認証サーバー上のユーザー名を指定する(K)

認証サーバーにおけるユーザー名(O):

セキュリティポリシー

☐ このユーザーのセキュリティポリシーを設定する(V) セキュリティポリシー(M)

パスワード認証

パスワード(P):

パスワードの確認入力(C):

固有証明書認証

固有証明書が選択されているユーザーは、接続時に SSL クライアント証明書がそのユーザーごとに設定された証明書と完全に一致するかどうかで接続を許可または拒否されます。

証明書の指定(E) 証明書の表示(V) 証明書作成ツール(W)

署名済み証明書認証

クライアント証明書がこの仮想 HUB の信頼する証明機関の証明書によって署名されているかどうかを検証します。

☐ 証明書の Common Name (CN) の値を限定する(B)

☐ 証明書のシリアル番号の値を限定する(L)

※ 16 進数で入力してください。(例: 0155ABCDE)

ヒント: ユーザー名が * (アスタリスク) のユーザーを作成すると、他の明示的に一致するユーザー名の定義がないユーザーが接続しようとした場合に外部認証サーバーを使用したパスワード認証による接続を許可できます。

OK キャンセル

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。

PacketiX_VPN - PacketiX VPN サーバー管理マネージャ

VPN Server "172.16.7.233" の管理

仮想 HUB 名	状態	種類	ユーザー	グループ	セッション	MAC テーブル	IP テーブル
VPN	オンライン	スタンダード	1	0	1	0	0

仮想 HUB の管理(A) オンライン(O) オフライン(E) 状態の表示(S) 仮想 HUB の作成(Q) プロパティ(E) 削除(D)

リスナーの管理(L)

リスナー一覧 (TCP/IP ポート):

ポート番号	状態
TCP 443	動作中
TCP 992	動作中
TCP 1194	動作中
TCP 8888	動作中

新規作成(B) 削除(D) 開始(G) 停止(P)

サーバー情報の参照および設定(N)

暗号化と通信関係の設定(W) クラスタリング構成(M)

サーバー状態の表示(V) クラスタリング状態(Z)

PacketiX VPN Server に関する情報(Q) TCP/IP コネクション一覧の表示(Y)

ライセンスの追加と削除(L) Config 編集(K)

ローカルブリッジ設定(B) レイヤ 3 スイッチ設定(S) IPsec / L2TP 設定 OpenVPN / MS-SSTP 設定

ダイナミック DNS 設定 VPN Azure 設定 最新の状態に更新(H) 閉じる(X)

現在の DDNS ホスト名: vpn28624425.softether.net

4.4. VPN Bridge 向け詳細設定

ブリッジモデルの VPN Server を Bridge 運用する場合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。

本装置を VPN Bridge として運用する場合、付属のライセンスキーを使用し「ライセンスの追加と削除」にてライセンスの追加を行ってください。

4.4.1. 接続設定の構築

管理マネージャーを起動します。初回起動の為、接続先の作成が必要となります。その為、「新しい接続設定」をクリックします。



接続設定名及びホスト名を入力します。尚、ポート番号を変更し運用する場合にはポート番号についても変更を行います。

新しい接続設定の作成

管理する VPN Server の接続設定を行います。

接続設定名(N): PacketiX_VPN

接続先 VPN Server の指定(B):

管理したい VPN Server が動作しているコンピュータのホスト名または IP アドレスおよびポート番号を指定してください。

ホスト名(H): 172.16.7.238

☐ このコンピュータ (localhost) に接続(L)

ポート番号(P): 443 (TCP ポート)

経由するプロキシサーバーの設定(O):

プロキシサーバーを経由して VPN Server に接続することができます。

プロキシの種類(Y):

- ☒ 直接 TCP/IP 接続 (プロキシを使わない) (D)
- ☐ HTTP プロキシサーバー経由接続(I)
- ☐ SOCKS プロキシサーバー経由接続(K)

プロキシサーバーの接続設定(R)

管理モードの選択とパスワードの入力(M)

VPN Server (には、サーバー管理モードと仮想 HUB 管理モードのどちらかのモードで接続できます。

サーバー管理モードで接続すると、VPN Server の設定とすべての仮想 HUB が管理できます。

仮想 HUB 管理モードで接続すると、権限を持っている仮想 HUB の管理ができます。

☒ サーバー管理モード(S) ☐ 仮想 HUB 管理モード(U)

仮想 HUB 名(V):

管理モードで接続する際のパスワードを入力してください。

管理パスワード(A):

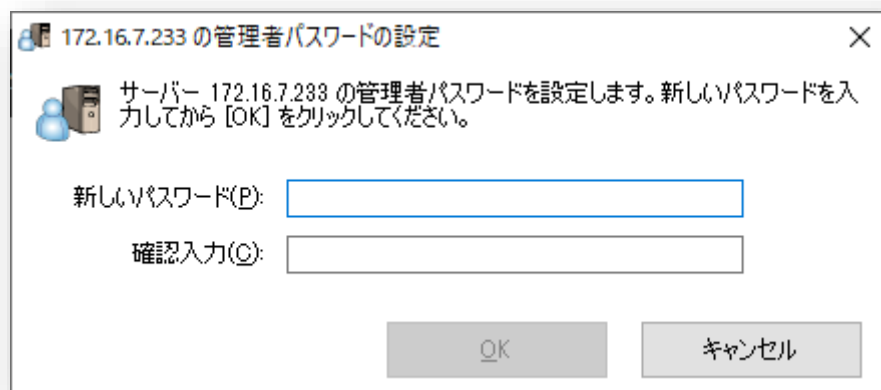
☐ 管理パスワードを保存しない(N)

OK キャンセル

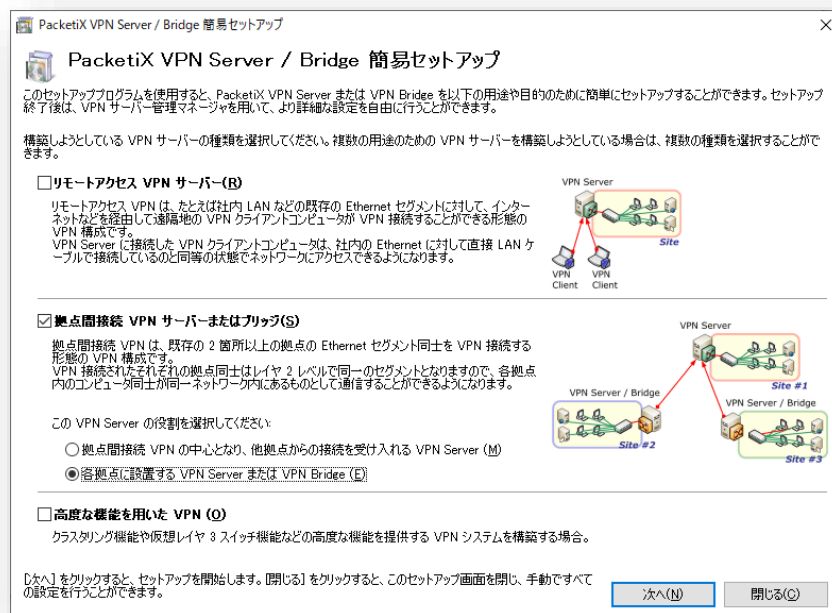
4.4.2. VPN ブリッジの構築

上記で構築した接続先に対して接続を行います。接続が行えない場合、サービスが起動していない、フィルタが開放されていない、ネットワーク的に接続できない等の可能性があります。

初回接続時は、管理者パスワードの設定を求められますので、管理者パスワードを設定します。



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。「拠点間接続 VPN サーバーまたはブリッジ」にチェックを入れ、「次へ」を選択します。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、接続先の VPN Server への接続設定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、事前に WEB UI にてローカルブリッジとして設定したインターフェースをこの画面上で仮想 HUB に接続する物理 I/F として選択しておきます。

簡易セットアップの実行

×



この VPN Server / VPN Bridge のセットアップを完了するには、下記のタスクのうち必要なものを実行してください。

1. VPN 接続を受け入れるためのユーザーの作成



この VPN Server がリモートアクセス VPN を受け入れる場合、または拠点間接続 VPN において中心となり他拠点からの接続を受け入れる場合は、VPN 接続を受け入れるためにユーザーを作成しておく必要があります。

ユーザーを作成する(U)

2. 接続先の VPN Server への接続設定



拠点間接続 VPN における各拠点に設置する VPN Server または VPN Bridge の場合は、各 VPN 拠点からの接続を受け付ける、中心となる VPN Server のアドレスなどを入力して、その VPN Server への接続を確立する必要があります。

接続先の VPN Server への接続設定を行う(Q)

3. ローカルブリッジの設定



VPN 経由で LAN にアクセスするためには、VPN 側の仮想的な Ethernet セグメントと物理的な Ethernet セグメントとの間を「ローカルブリッジ接続」機能でブリッジ接続する必要があります。

VPN に対してブリッジ接続する既存の Ethernet デバイス (LAN カード) を選択してください。

ブリッジ接続する Ethernet デバイスを選択してください

必要な設定がすべて完了したら、[閉じる] をクリックしてください。VPN Server / VPN Bridge の詳細な管理画面が表示されます。その後は必要な場合に詳細な設定を行ってください。

閉じる(C)

接続先の **VPN Server** への接続設定では、接続設定名、接続先 **VPN Server** の指定、ユーザー認証が最低限必要です。その他パラメータは必要に応じて設定します。

新しい接続設定のプロパティ

VPN Server への接続設定を行います。

接続設定名(E):

接続先 VPN Server の指定(B):

接続したい VPN Server が動作しているコンピュータのホスト名または IP アドレス、ポート番号、および仮想 HUB 名を指定してください。

ホスト名(H):

ポート番号(P):

443

☐ NAT-T 無効

仮想 HUB 名(Y):

経由するプロキシサーバーの設定(O):

プロキシサーバーを経由して VPN Server に接続することができます。

プロキシの種類(M):

☒ 直接 TCP/IP 接続 (プロキシを使わない) (D)
☐ HTTP プロキシサーバーを経由接続(Q)
☐ SOCKS プロキシサーバーを経由接続(S)

プロキシサーバーの接続設定(Z)

サーバー証明書の検証オプション(E):

☐ サーバー証明書を必ず検証する(S)

信頼する証明期間の証明書の管理(L)

固有証明書の登録(F)

固有証明書の表示(S)

カスケード接続の設定

カスケード接続を行う際に、この仮想 HUB 内で生成されるセキュリティポリシーを設定することができます。

セキュリティポリシー(L)

ユーザー認証(A)

VPN Server に接続する際に必要なユーザー認証情報を設定してください。

認証の種類(M):

標準パスワード認証

ユーザー名(U):

パスワード(P):

通信の詳細設定(O)

☒ VPN Server との通信が切断された場合は再接続する(Z)

再接続回数(Q):

回

再接続間隔(M):

15

秒

☒ 無限に再接続を試行する (常時接続) (I)

☐ SSL 3.0 を使用する(J)

高度な通信設定(U)

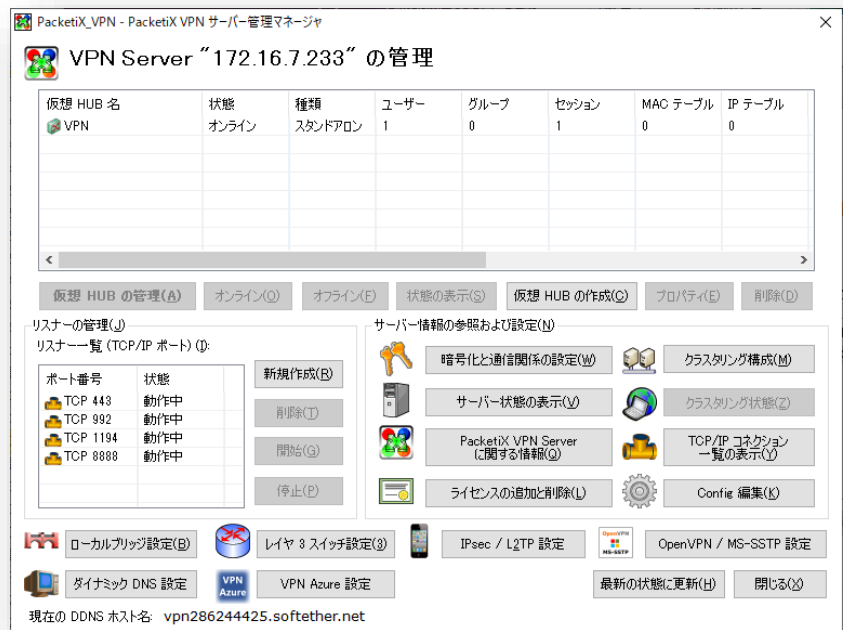
OK

キャンセル

接続先の **VPN Server** への接続設定が完了すると、以下のような状態ウィンドウが表示されます。設定した接続設定の状態が”オンライン(接続済み)”となっていることを確認してください。

[illegible]

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。



4.5. ライセンスの追加と削除

本装置を使用するには、有効な PcketiX VPN Server ライセンスを設定する必要があります。
管理画面から取得済のライセンスキーを入力します。

PacketiX_VPN - PacketiX VPN サーバー管理マネージャ

VPN Server "172.16.7.233" の管理

仮想 HUB 名	状態	種類	ユーザー	グループ	セッション	MAC テーブル	IP テーブル
VPN	オンライン	スタンドアロン	1	0	1	0	0

仮想 HUB の管理(A) オンライン(O) オフライン(F) 状態の表示(S) 仮想 HUB の作成(C) プロパティ(E) 削除(D)

リスナーの管理(L)
リスナー一覧 (TCP/IP ポート) (I):

ポート番号	状態
TCP 443	動作中
TCP 992	動作中
TCP 1194	動作中
TCP 8888	動作中

新規作成(R) 削除(I) 開始(G) 停止(P)

サーバー情報の参照および設定(N)

暗号化と通信関係の設定(W) クラスタリング構成(M)
サーバー状態の表示(V) クラスタリング状態(Z)
PacketiX VPN Server に関する情報(Q) TCP/IP コネクション一覧の表示(Y)
ライセンスの追加と削除(L) Config 編集(K)

ローカルブリッジ設定(B) レイヤ 3 スイッチ設定(S) IPsec / L2TP 設定 OpenVPN / MS-SSTP 設定
ダイナミック DNS 設定 VPN Azure 設定 最新の状態で更新(H) 閉じる(O)

現在の DDNS ホスト名: vpn28624-1425.softether.net

ライセンスの追加と削除

PacketiX VPN Server を使用するには、有効なライセンスを取得し、ライセンスキーを登録する必要があります。この画面では、新しいライセンスキーを登録したり、登録済みのライセンスキーを削除したり、現在のライセンス一覧や VPN Server のライセンスモードを表示したりすることができます。

現在登録されているライセンスの一覧(L):

番号	ライセンスキー	ライセンス種類名	状態	有効期限

ライセンスの入手・更新(O) 新しいライセンスキーの登録(A) 削除(D) ライセンスに関する情報(I)

[ライセンスの入手・更新] をクリックすると、ライセンスの入手・更新方法に関する説明が記載された Web サイトを表示します。 ライセンスを選択し、[ライセンスに関する情報] をクリックすると、ソフトウェア株式会社の Web サイト (softether.com) に接続し、そのライセンスに関する登録情報を表示します。

現在の PacketiX VPN Server のライセンスモード(M):

製品エディション名	PacketiX VPN Server 4.0 Trial Edition
この VPN Server のリリース日付	2019年 2月28日(木)
現在のサーバー ID	0
現在の製品ライセンスの有効期限	2020年 7月11日(土)
サブスクリプション契約の状態	契約なし (このエディションではサブスクリプションキーは不要)
ユーザー作成可能数	無制限
クライアント同時接続可能数	無制限
ブリッジ同時接続可能数	無制限
エンタープライズ機能の利用可否	はい (利用可能)

閉じる(O)

4.6. PacketiX VPN Bridge について

本装置に対して、PacketiX VPN Bridge が接続することが可能です。

PacketiX VPN Bridge を用いる場合には、対応したハードウェアをご用意いただき、本装置への接続設定を行ってください。

4.7. PacketiX VPN Client について

4.7.1. PacketiX VPN Client のインストール

本装置へ各 PC 等が VPN Client として接続するソフトウェア(PacketiX VPN Client)は以下の URL からダウンロードすることができます。対応 OS の rtm ver.のソフトウェアをダウンロードし、インストールを行ってください。インストールは画面の指示に従い実施してください。

※ダウンロード URL

<http://www.packetix-download.com/>



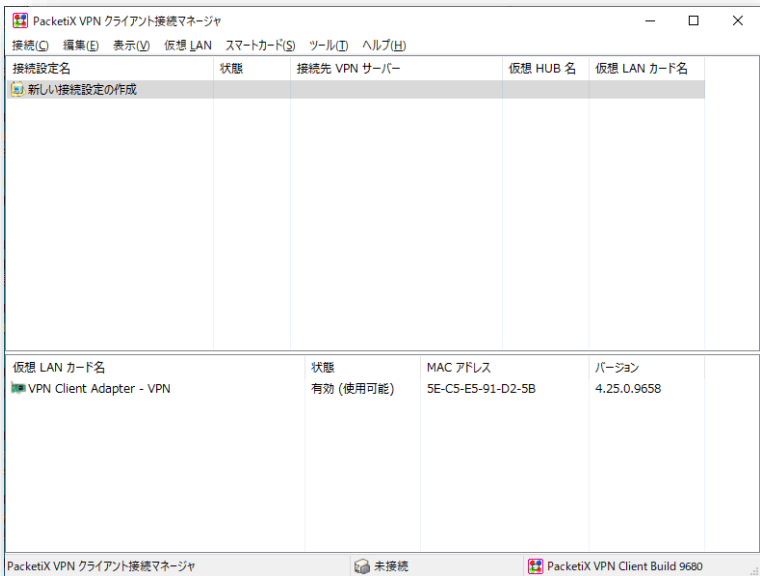
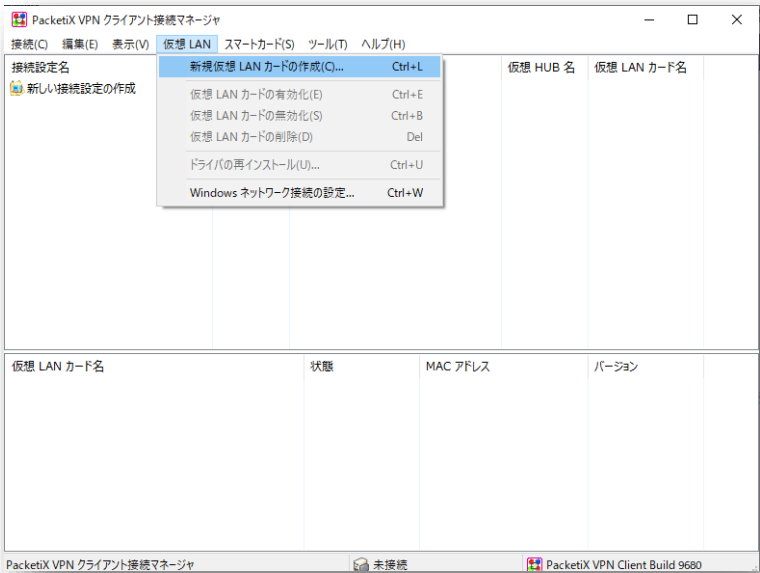
The screenshot shows the 'PacketiX VPN ダウンロードセンター' (PacketiX VPN Download Center) website. It features three dropdown menus for selection:

- ダウンロードするソフトウェアを選択** (Select software to download): Set to 'PacketiX VPN (Commercial)'.
- コンポーネントを選択** (Select component): Set to 'PacketiX VPN Client'.
- プラットフォームを選択** (Select platform): A dropdown menu with 'Windows' selected, and 'Linux' and 'Mac OS X' as visible options.

4.7.2. PacketiX VPN Client の設定

インストールした PacketiX VPN Client を起動し、仮想 LAN を作成します。

仮想 LAN 名は任意で問題ありません。



仮想 LAN 作成後、VPN Server への接続設定を行います。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。また、それ以外のパラメータは必要に応じて設定します。

The screenshot shows the '新しい接続設定のプロパティ' (New Connection Properties) dialog box. The '接続設定名' (Connection Name) field is highlighted with a red box and contains '新しい接続'. The '接続先' (Destination) is 'VPN Server の指定' (Specify VPN Server). The '接続したい VPN Server が動作しているコンピュータのホスト名または IP アドレス、ポート番号、および仮想 HUB 名を指定してください。' (Specify the host name or IP address, port number, and virtual HUB name of the computer where the VPN Server you want to connect is operating.) section has three fields: 'ホスト名(H)' (Host Name), 'ポート番号(P)' (Port Number) set to 443, and '仮想 HUB 名(V)' (Virtual HUB Name). The '経由するプロキシサーバーの設定' (Proxy Server Settings) section shows 'プロキシサーバーを経由して VPN Server に接続することができます。' (You can connect to the VPN Server via the proxy server.) and 'IE の設定を使用(E)' (Use IE settings). The 'プロキシの種類' (Proxy Type) is set to '直接 TCP/IP 接続 (プロキシを使わない) (D)' (Direct TCP/IP connection (no proxy)). The 'サーバー証明書の検証オプション' (Certificate Verification Options) section shows 'サーバー証明書を必ず検証する' (Always verify server certificate) is selected. The 'ユーザー認証' (User Authentication) section shows '標準パスワード認証' (Standard password authentication) selected, with 'ユーザー名(U)' (Username) and 'パスワード(P)' fields highlighted with a red box. The '通信の詳細設定' (Communication Detailed Settings) section shows 'VPN Server との通信が切断された場合は再接続する' (Reconnect if communication with VPN Server is disconnected) checked, with '再接続回数' (Reconnect times) set to 1 and '再接続間隔' (Reconnect interval) set to 15 seconds. The 'SSL 3.0 を使用する' (Use SSL 3.0) checkbox is unchecked. The '高度な通信設定' (Advanced communication settings) button is visible.

新しい接続設定のプロパティ

VPN Server への接続設定を行います。

接続設定名(I): **新しい接続**

接続先: VPN Server の指定(O)

接続したい VPN Server が動作しているコンピュータのホスト名または IP アドレス、ポート番号、および仮想 HUB 名を指定してください。

ホスト名(H):

ポート番号(P): 443 ☐ NAT-T 無効

仮想 HUB 名(V):

経由するプロキシサーバーの設定(O):

プロキシサーバーを経由して VPN Server に接続することができます。

IE の設定を使用(E)

プロキシの種類(M): ☒ 直接 TCP/IP 接続 (プロキシを使わない) (D)
☐ HTTP プロキシサーバー経由接続(Q)
☐ SOCKS プロキシサーバー経由接続(S)

プロキシサーバーの接続設定(2)

サーバー証明書の検証オプション(E):

☐ サーバー証明書を必ず検証する(3)

信頼する証明機関の証明書の管理(4)

固有証明書の登録(R) 固有証明書の表示(S)

使用する仮想 LAN カード(L):

VPN Client Adapter - VPN

ユーザー認証(A):

VPN Server に接続する際に必要なユーザー認証情報を設定してください。

認証の種類(B): 標準パスワード認証

ユーザー名(U):

パスワード(P):

VPN Server 側のユーザーのパスワードを変更できます。

パスワードの変更(J)

通信の詳細設定(G):

☒ VPN Server との通信が切断された場合は再接続する(Z)

再接続回数(C): 1 回

再接続間隔(K): 15 秒

☒ 無限に再接続を試行する (常時接続) (I)

☐ SSL 3.0 を使用する(L) 高度な通信設定(M)...

☐ 接続中の画面とエラー画面を非表示(W) ☐ IP アドレスメッセージを非表示(Y)

OK キャンセル

5. その他利用方法

5.1. SSH でログイン

本装置の IP アドレスに対して、SSH クライアントソフトウェア(Teraterm や putty 等)を用いて操作します。出荷時の IP アドレス・パスワード情報は、「出荷時設定情報」を参照ください。

5.2. シリアルコンソールでログイン

EasyBlocks の CONSOLE ポートと操作用の PC を接続し、シリアルコンソールソフトウェア(Teraterm や putty 等)を用いて操作します。コンソール用変換アダプタは、PC 側のシリアルポートに直接接続します。PC 側にシリアルポートが無い場合は、別途 USB-シリアル変換アダプタ等をご用意ください。

ボーレート	115200bps
データ	8bit
パリティ	なし
ストップビット	1

5.3. ファクトリーリセット

工場出荷状態に戻す場合、コンソールケーブルを接続しコンソールソフトウェアにてターミナルを表示してください。EasyBlocks 本体を再起動し、起動時の Grub メニュー表示時に”v”キーを入力し、”Factory Reset Mode”にカーソルを合わせて Enter キーを押してください。これにより工場出荷状態へと戻ります。

尚、工場出荷状態へと戻る為、設定等は消えますのでご注意ください。



5.4. BIOS 設定

本装置を起動し、画面表示が出た所で **Esc** キーを押すと BIOS 設定画面に入ることが出来ます。BIOS 設定値は変更しないで下さい。誤って変更した際には以下の設定を行って下さい。

[Save & Exit] - [Restore Defaults]と選択してください。

6. 注意事項

6.1. 電源断について

EasyBlocks PacketiX VPN Server では、SSD ストレージを搭載しております。唐突な電源断は故障の原因となる場合がありますので、電源を落とす場合は以下のいずれかを実施してください。

- WEB UI からの停止
- コンソールまたは SSH によるログイン後の `poweroff` コマンド
- PWR スイッチを押しての停止

6.2. ポート転送について

EasyBlocks PacketiX VPN Server をルーター配下に設置する場合、ルーターから対象サービスポートに対してポート転送を行う必要があります。そのため、ルーターのポート転送を設定してください。

6.3. ライセンスなしモデルへのライセンスキー追加について

本装置のライセンスなしモデルはコールドスタンバイ機となります。ライセンスモデルを実運用に切り替える場合には、切り替え元の Edition またはブリッジモデルのライセンスキーをご使用ください。

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