

VPN接続機器

VPN Beagle Center Model 200

操作マニュアル

VPN Beagle Center 操作マニュアル

株式会社エーティーワークスは本マニュアルの記述のいかなる誤りに対しても責任を負うものではありません。

また、株式会社エーティーワークスは本マニュアルの記述の使用によるいかなる結果に対しても責任を負うものではありません。本マニュアルはお客様の責任で使用してください。

本マニュアルの内容は情報提供のみを目的としており、予告なしに変更される場合があります。

事前に株式会社エーティーワークスによる許可がない限り、本マニュアルのいかなる部分も複製することはできません。

また、株式会社エーティーワークスによる許可がない限り、本マニュアルを配布することはできません。

目次

1 章 VPN Beagle とは 5

- 1. はじめに 6
- 2. 商標について 6
- 3. VPN Beagle の特徴 7
- 4. 本文中に使用される記号について 7
- 5. ハードウェアの取り扱いについて 8
- 6. ハードウェアを取り扱う上での注意事項 9

2 章 セットアップ 12

- 1. 設置計画 13
- 2. 初期設定 15
- 3. システム構成例 19

3 章 VPN の管理 22

- 1. ソフトウェアクライアントの追加・編集・削除 23
- 2. ハードウェアクライアントの追加・編集・削除 29
- 3. 一括インポート／エクスポート 34

4 章 運用管理 36

- 1. Syslog 設定 37
- 2. サポート情報取得 38
- 3. バックアップ／リストア 39
- 4. ファームウェア 40
- 5. 再起動 41

5 章

管理画面の機能説明

42

1. ログイン画面	43
2. 基本設定	44
ネットワーク	44
ルーティング	45
3. アクセス制限	46
パスワード変更	46
接続許可 IP アドレス	47
4. VPN 設定	48
サーバー設定	48
ハードウェアクライアント設定（検索、追加、編集）	50
ソフトウェアクライアント設定（検索、追加、編集）	55
一括インポート／エクスポート	59
5. VPN 状態	60
接続状況	60
VPN 状態	61
VPN ログ	62
6. 運用管理	63
Syslog 設定	63
サポート情報取得	63
バックアップ／リストア	64
ファームウェア	65
再起動	65

6 章

コンソール管理

66

1. コンソール管理	67
------------------	----

7 章

付録

71

1. 付録 A. 仕様	71
-------------------	----

1

第 1 章

VPN Beagle とは

1. はじめに

2. 商標について

3. VPN Beagle の特徴

4. 本文中に使用される記号について

5. ハードウェアの取り扱いについて

6. ハードウェアを取り扱う上での注意事項

1. はじめに

このたびは株式会社エーティーワークスの VPN Beagle Center（以下、VPN Beagle）をお買い上げいただき、誠にありがとうございます。

VPN Beagle は、オープンソースである OpenVPN をベースに弊社が独自にカスタマイズした VPN 接続アプライアンスサーバーです。筐体は弊社オリジナルの 1/4U シャーシを採用しており、ラックを非常に効率よく使用することができます。専用の管理インターフェイスを搭載していますので、セットアップや運用管理を全て Web ブラウザから行うことができます。

本書をよくお読みいただき、本製品の機能や使用方法を十分理解したうえで、本製品をご使用になってください。

2. 商標について

Linux は、Linus Torvalds の米国およびその他の国における登録商標あるいは商標です。

Microsoft、Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。

その他、記載されている会社名、製品名は、各社の登録商標または商標です。なお、本文中では、®、TM マークは明記しておりません。

3. VPN Beagle の特徴

■ アカウントは無制限に作成可能

- アカウントは無制限に作成可能。また、アカウントの有効期限も管理画面にて、特定のアカウントを無効化し、VPN 接続不可とします。

■ VPN エンジンとして定評のあるオープンソースソフトウェア OpenVPN を採用

- VPN Beagle に接続するためのクライアントソフトも無料で取得可能
- OpenVPN クライアントソフトが対応している OS (Windows、Linux) にて接続可能。

■ VPN Beagle Point と組み合わせることで、安価に拠点間接続を実現

- 高価な専用線が必要となる拠点間接続を VPN Beagle Center と VPN Beagle Point を利用することで安価にセキュアなネットワークを構築することができます。

■ 専用 GUI により容易な運用管理

- Web ブラウザから操作できる専用管理画面で運用管理が容易です。
- 画面および HELP は全て日本語で記載されています。
- VPN 接続に必要なアカウント管理、証明書発行も簡単に行えます。
- 現在接続中のユーザーの確認や接続履歴を容易に確認できます。

4. 本文中に使用される記号について



注意

装置の取り扱いや設定手順において守らなければならない事項や注意が必要な事項を記述しています。



ポイント

装置の取り扱いや設定手順において知っておくと便利な点を記述しています。



参照

関連する項目やページを記述しています。

5. ハードウェアの取り扱いについて

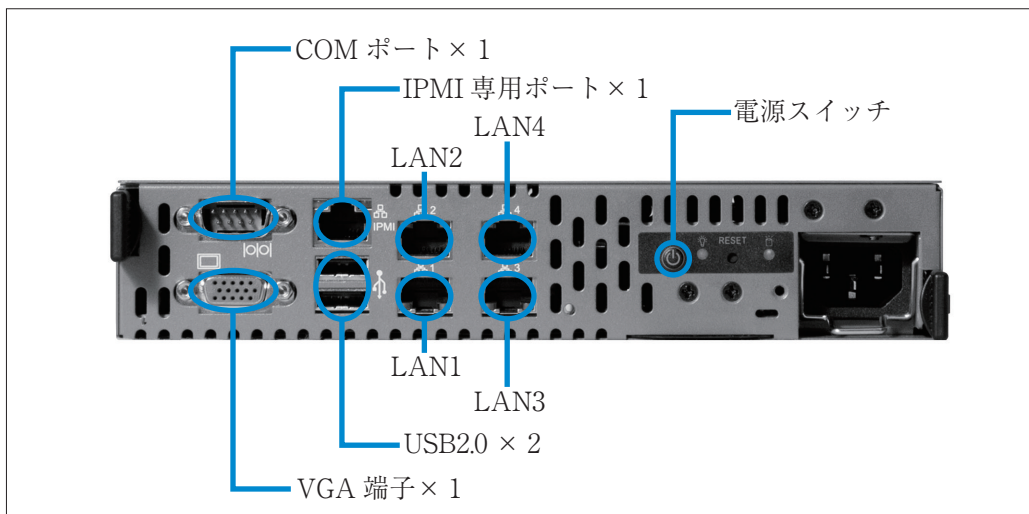


図 1-1. フロントパネル

電源スイッチ	押下すると電源が投入されます。
COM ポート	シリアルポートです。
VGA 端子	コンソール接続する場合、モニタを接続します。
USB2.0	USB2.0 ポートです。
LAN コネクター	LAN1、LAN2 を使用します。

! LAN3、LAN4 は使用しません。

6. ハードウェアを取り扱う上での注意事項

! 安全にお使いいただくために必ずお守りください。

お客様や他の方への危害や損害を未然に防ぎ、本製品を安全にご使用いただくために必ずお守りいただきたい事項を記載しました。安全にご使用いただくために必ずお読みになり、内容をよく理解された上でご使用ください。

警告及び注意

■ 表示された電源電圧で使用する

表示された電源電圧以外では使用しないでください。火災や感電の原因になります。

■ もし異常が起こったら

本機から煙が出たり、変なおいや音がしたら、直ちに安全にスイッチを切りコンセントからプラグを抜いてください。そのまま使用すると、火災や感電の原因となります。(修理につきましては弊社にお問い合わせください)

■ 濡れた手で本製品を触らないでください。また、濡れた手で電源プラグの抜き差しはしないでください

本体及び周辺機器の電源プラグが入っているときに濡れた手で触れると、感電や故障の原因となります。

また、電源プラグが接続されていなくても故障の原因となります。

濡れた手で電源プラグの抜き差しをすると、感電をする恐れがありますので、必ず乾いた手で抜き差ししてください。

■ 電源コードやプラグを破損させないでください

無理に曲げて設置したりすると、電源コードやプラグが破損し、火災や感電につながります。

■ 電源プラグは確実に差し込んでください

電源プラグを確実に差し込まないと、接触不良により火災や感電につながりますので、必ず根元まで確実に差し込んでください。また、定期的にプラグの状態を確認してください。

■ 電源コードのアース線は確実に配線してください

■ 雷が鳴っている時は、電源プラグに触れないでください

落雷時に感電する恐れがあります。

■ 電源プラグは定期的に埃などを取り除いてください

電源プラグに埃がついたまま使用しますと、ショートや絶縁不良となり、火災や感電の原因となります。埃を取り除く際は、プラグを抜き乾いた布で拭き取ってください。

■ 本体内部に、液体や異物を入れないでください

本体内に液体や異物が入った状態で使用すると、火災や感電、故障につながる恐れがあります。液体や異物が内部に入った場合は、直ちに安全にスイッチを切り、コンセントからプラグを抜いてください。修理につきましては弊社にお問い合わせください。

■ 高電圧機器の周辺で作業する場合、または高電圧機器を取り扱う場合は必ず2人以上で作業してください

高電圧機器の周辺で作業する場合や、高電圧機器を取り扱う場合は、万一の場合にそなえ、必ず作業員以外に主電源を切断することができるよう人員を配置してください。また、予めブレーカーなどの主電源スイッチの場所を確認してください。

■ 水分や湿気の多い場所での使用はお避けください

火災や感電、故障の原因となります。

■ 本体通気孔をふさがないでください

本体通気孔をふさいだ状態で使用すると、本体内部の温度が上がり、故障ややけどの原因となります。

■ 動作中のファンには指や異物を入れないでください

けがや故障の原因になります。

■ 本機の上に物をのせないでください。また、本機の上に乗らないでください

落下して怪我をしたり、本機が破損する恐れがあります。本機の上に重量物を置くと、ケースが変形し、内部の機器が破損し、火災や感電の原因となる恐れがあります。

■ 本製品を次のような場所に設置しないでください

- ・ 許容動作環境以外の場所
- ・ 直射日光が当たる場所
- ・ 振動が発生する場所
- ・ 火気の近く、または高温になる場所
- ・ 平坦でない場所
- ・ 漏電や漏水の恐れのある場所（故障や感電の恐れがあります）
- ・ 強い磁界が発生する場所
- ・ 不安定な場所

■ 本製品を落としたり、強い衝撃を与えないでください

本製品は精密機械ですので、衝撃を与えないように慎重に取り扱ってください。強い衝撃を与えると故障の原因となります。

■ 本機を移動する際はコード類を取り外してください

コードが破損し、火災や感電につながる恐れがありますので、必ずすべての接続をはずしてから移動してください。

■ 静電気による破損を防ぐ為、以下のことをお守りください

静電気によって、本製品が破損したり、データの損失、破損を引き起こす恐れがあります。

- ・本製品に触れる前に、必ず身近な金属に触れ、身体の静電気を取り除いてください。
- ・メモリやその他部品の端子部分に手を触れないでください。

■ 本製品を分解、修理、改造しないでください

火災・感電・故障のおそれがあります（保証の対象外となります）

2

第2章

セットアップ

1. 設置計画

2. 初期設定

3. システム構成例

1. 設置計画

公開 Web サーバーへ遠隔より管理を行うケースの場合、既存のネットワーク構成では外部からのアクセス許可を FireWall にて設定を行う必要があります。これにより、下記のような問題点もあります。

- FireWall の IP 単位での制限の場合、モバイル環境など動的に IP アドレスが変わる場合接続できなくなることがしばしば発生する。
- SSH接続が必要な場合、SSHポートを開放するなど多数のポートを開放する必要がある。

■ 既存のネットワーク構成

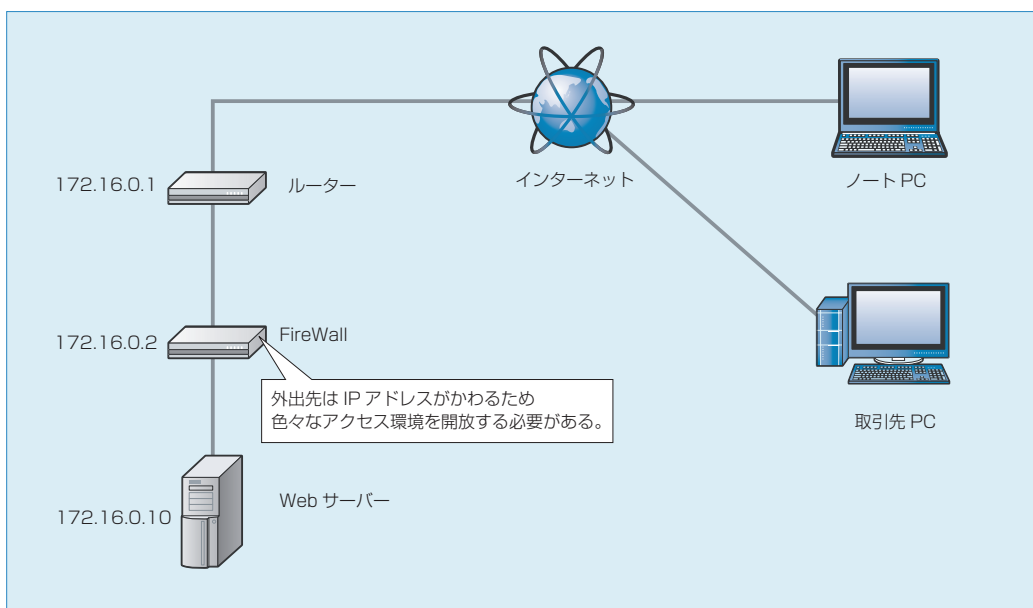


図 2-1 既存のネットワーク構成図

VPN Beagle Center を導入することで、既存の問題が解決されます。

- FireWall は VPN 接続ポートだけを開放すればよい
- VPN 接続は、証明書による認証のため、モバイル環境など IP アドレスが頻繁に変更しても影響がない
- 既存のネットワークに影響なく導入可能

! 便宜上、172.16.0.0/24 のネットワークをグローバルネットワークとして表記しています。

■ 導入後のネットワーク構成

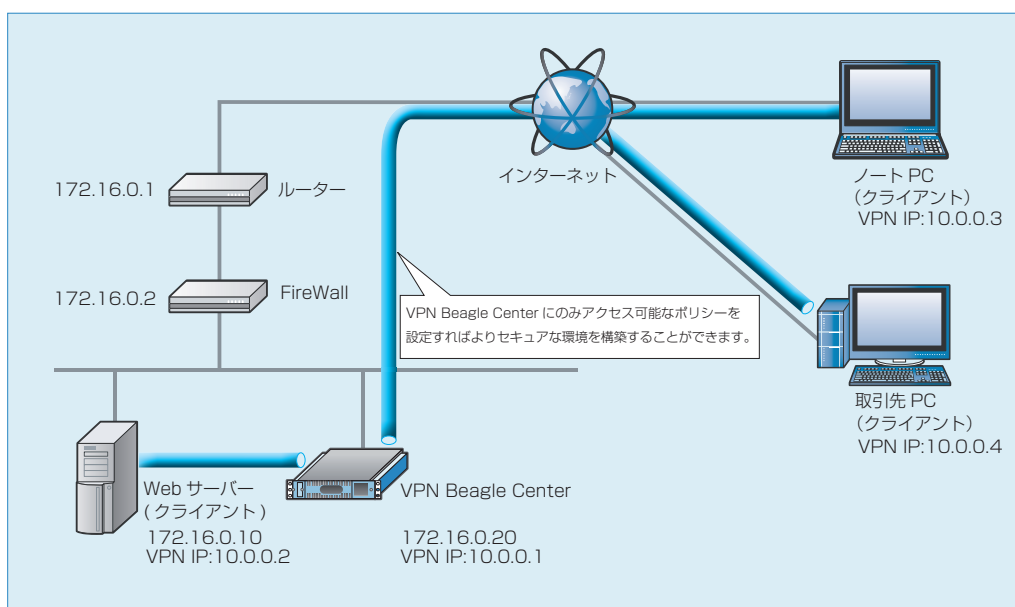


図 2-2 導入後のネットワーク構成図

2. 初期設定

VPN Beagle の工場出荷時は、次のようにネットワークが設定されています。

IPアドレス	192.168.1.1
ネットマスク	255.255.255.0
ゲートウェイ	192.168.1.254

次のいずれかの方法でネットワークの設定を行ってください。メンテナンス PC を利用した方法では、ネットワーク以外の項目についても設定可能ですので、こちらの方法を推奨します。

メンテナンス PC を利用して設定する (推奨)

■ 必要機器

- Web ブラウザ (Internet Explorer または Firefox) が使用できるメンテナンス PC (Windows ノート PC など)
- クロスケーブルまたは HUB とストレートケーブル

1. VPN Beagle とメンテナンス PC の接続

VPN Beagle の LAN1 とメンテナンス PC を、クロスケーブルを使用して接続します。図 2-3 のような状態となります。HUB とストレートケーブルを使用して VPN Beagle とメンテナンス PC それぞれを接続する方法でもかまいません (図 2-4)。この場合、HUB に VPN Beagle、メンテナンス PC 以外を接続しないようにご注意ください。

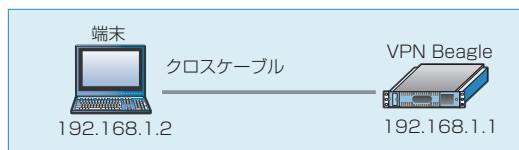


図 2-3 メンテナンス端末との接続

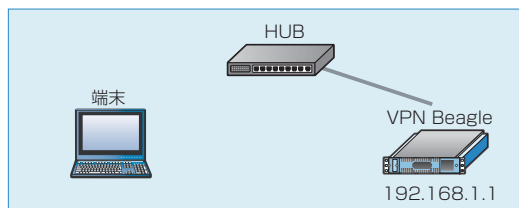


図 2-4 ストレートケーブル使用時

2. メンテナンス PC のネットワーク設定

VPN Beagle の工場出荷時のネットワーク設定は 192.168.1.1 / 255.255.255.0 となっています。メンテナンス PC のネットワークを次のように設定します。

IPアドレス	192.168.1.2
ネットマスク	255.255.255.0
ゲートウェイ	192.168.1.254 (任意)

3. VPN Beagle の電源投入

VPN Beagle のコンセントを電源に接続し、電源スイッチを押下します。

4. メンテナンス PC から Web ブラウザによる接続

メンテナンス PC 上の Web ブラウザにて次の URL を開きます。

<https://192.168.1.1:18180/>

図 2-5 のログイン画面が表示されます。

電源投入後、システムが起動するまで約 1 分程度の時間をおいてから、Web ブラウザによる接続を行ってください。

工場出荷時のログイン ID および初期パスワードは、装置に添付されているシートの Web 管理画面のログイン ID、パスワードを入力してください。

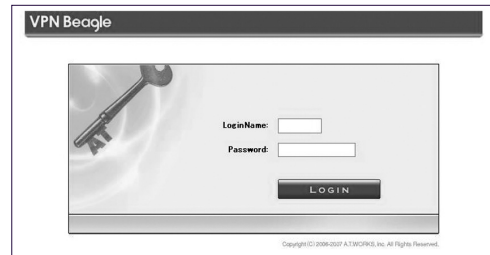


図 2-5 ログイン画面

! 図 2-5 のログイン画面が表示されない場合は、次の確認を行ってください。

- ・ VPN Beagle が電源投入されているか（電源ランプの確認）
- ・ VPN Beagle とメンテナンス PC、HUB がケーブルでしっかり結線されているか
- ・ メンテナンス PC のネットワーク設定が正しいか
- ・ 入力した URL が正しいか

VPN Beagle のネットワーク設定が変更されている場合、この URL では接続できません。VPN Beagle のネットワーク設定が不明な場合は、コンソール接続を利用してネットワークの再設定を行ってください。

5. ネットワーク設定

ネットワーク構成例（P. 44）を参考にネットワーク設定を行います。

【基本設定】 → 【ネットワーク】 を選択します。

 ネットワークの編集については P. 44 を参照してください。

6. パスワード変更

工場出荷時は初期パスワードのため、必ずパスワード変更を行ってください。

【アクセス制限】 → 【パスワード変更】 にてパスワード変更を行います。

 管理者パスワードの変更については P. 46 を参照してください。

7. 接続許可 IP アドレスの制限

工場出荷時はどの IP アドレスからも管理画面への接続を許可する状態のため、接続を許可する IP アドレスを設定して制限を行ってください。

【アクセス制限】→【接続許可 IP アドレス】にて VPN Beagle の管理画面への接続を許可する IP アドレスの制限を行います。接続許可 IP アドレスの登録が無い場合は、IP アドレスによる制限は働きませんが、1 件以上登録されているときには、登録 IP アドレス以外からの接続はできなくなります。

! 接続元 IP アドレスの制限については P. 46 を参照してください。

8. VPN Beagle の停止と設置

VPN Beagle の電源ボタンを長押しし（4 秒程度）、電源を切ります。

VPN Beagle を使用するネットワークに設置し電源を入れると、設定した IP アドレスで起動します。Web ブラウザで VPN Beagle に設定した IP アドレスを指定して管理画面を開き、設定を続けます。

[https:// \[VPN Beagle に設定した IP アドレス\] :18180/](https://[VPN Beagle に設定した IP アドレス]:18180/)

コンソール接続を利用して設定する

コンソール接続の場合、設定できるのは、LAN1 インターフェイスの IP アドレス、ネットマスク、デフォルトゲートウェイのみになります。コンソール接続による設定を行った後、メンテナンス PC を使用して Web ブラウザからその他の項目の設定を行う必要があります。

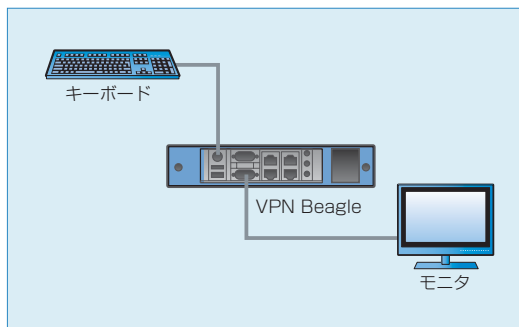


図 2-6 コンソール使用方法

■ 必要機器

- モニタ（D-sub 15 ピン VGA 端子）
- キーボード（PS/2 端子）

1. VPN Beagle と機器の接続

VPN Beagle の D-sub 端子にモニタを接続します。

VPN Beagle のキーボード端子に PS/2 キーボードを接続します。

2. VPN Beagle の電源投入

VPN Beagle のコンセントを電源に接続し、電源スイッチを押下します。
モニタにログインプロンプトが表示されますのでログイン ID とパスワードを入力します。このログイン ID およびパスワードは、装置に添付されているシートのコンソールログイン ID、パスワードを入力してください。



このログイン ID とパスワードは VPN Beagle の管理画面へのログイン ID、パスワードとは異なります。変更することはできません。

3. ネットワーク設定

ログインに成功するとメニューが表示されますので、ネットワーク設定を選択します。
本設定で設定可能な項目は、LAN1 ネットワークの次の項目に限定されます。

- IP アドレス
- ネットマスク
- ゲートウェイ

上記以外の設定項目はネットワーク設定後、メンテナンス PC を使用して Web ブラウザから設定してください。



コンソール管理からネットワーク設定を変更する方法は P. 67 を参照してください。

4. VPN Beagle の停止と設置

VPN Beagle の電源ボタンを押し、電源を切ります。
VPN Beagle を使用するネットワークに設置し、電源を入れると設定した IP アドレスで起動します。Web ブラウザで次の URL を開き、設定を継続します。

[https:// \[VPN Beagle に設定した IP アドレス\] :18180/](https://[VPN Beagle に設定した IP アドレス]:18180/)



本手順では、管理者パスワードの変更、接続元 IP アドレスの制限は行われておりません。VPN Beagle を使用するネットワークに設置後、Web ブラウザより管理画面にログインし、管理者パスワードの変更、接続元 IP アドレスの制限を実施してください。



管理者パスワードの変更方法については P. 67 を参照してください。



接続元 IP アドレスの制限については P. 46 を参照してください。

3. システム構成例

クライアント PC 接続例

VPN Beagle Center と各クライアント間で VPN 接続を行うシステム構成です。

各クライアント用の設定情報は VPN Beagle Center の管理画面より簡単に作成することができます。



P. 23 ソフトウェアクライアントの追加・編集・削除 を参照してください。



各クライアントにて設定情報を導入する場合、別途 OpenVPN クライアントソフトのインストールが必要となります。

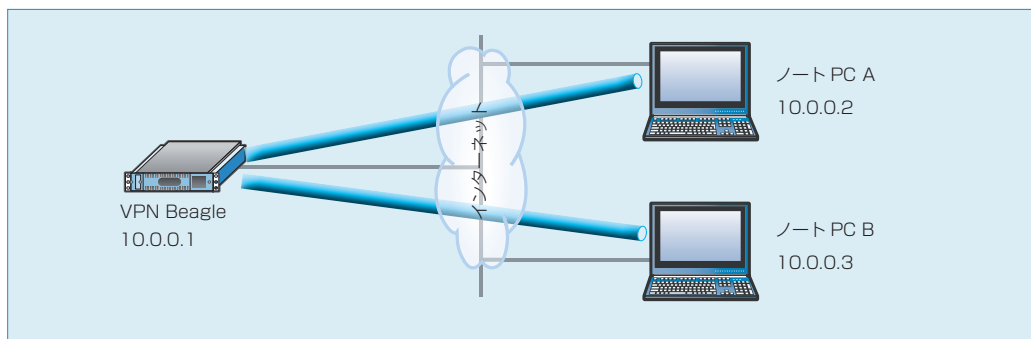


図 2-7 クライアント PC 接続例

拠点間接続例

VPN Beagle Center と VPN Beagle Point (別売) を組み合わせることで
本店と支店間など拠点間を VPN 接続により安全に通信することができます。
図の接続例の場合、支店内の各 PC には VPN リフトを導入することなく本店内のファイ
ルサーバーにアクセスすることができます。
また、VPN Beagle Point 用の設定情報は VPN Beagle Center の管理画面より
簡単に作成することができます

-  P. 29 ハードウェアクライアントの追加・編集・削除 を参照してください。
-  VPN Beagle Point の設置方法、設定情報の組み込み手順は
VPN Beagle Point マニュアルを参照してください。

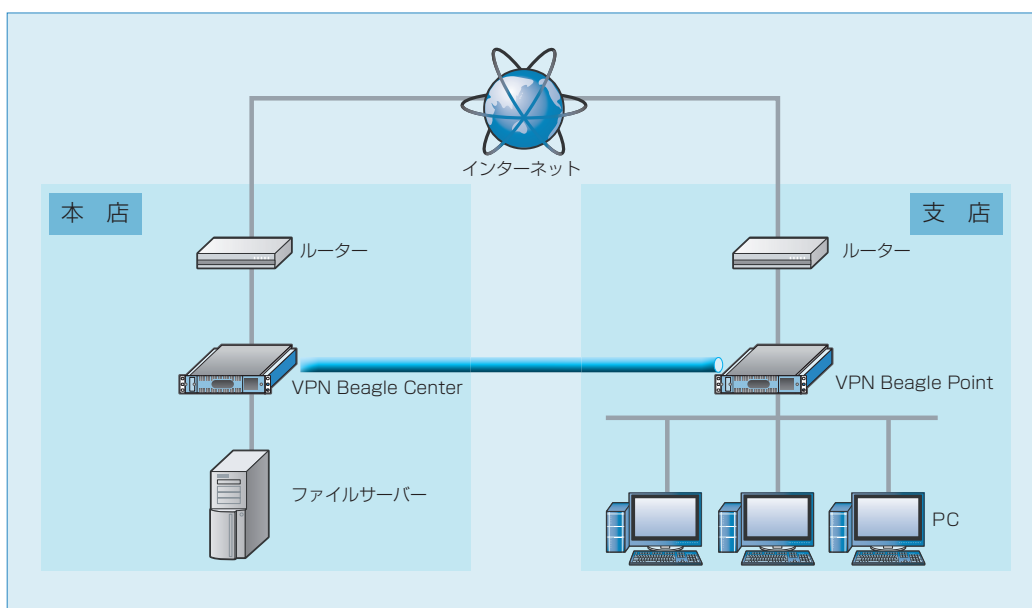


図 2-8 拠点間接続

クライアント間接続例

■ クライアント間接続が有効な場合

クライアント間接続機能を有効にすることで VPN 接続をおこなっているクライアント間同士で VPN 通信を行うことが可能です。

! クライアント間で安全に通信を行う用途の場合、有効にしてください。

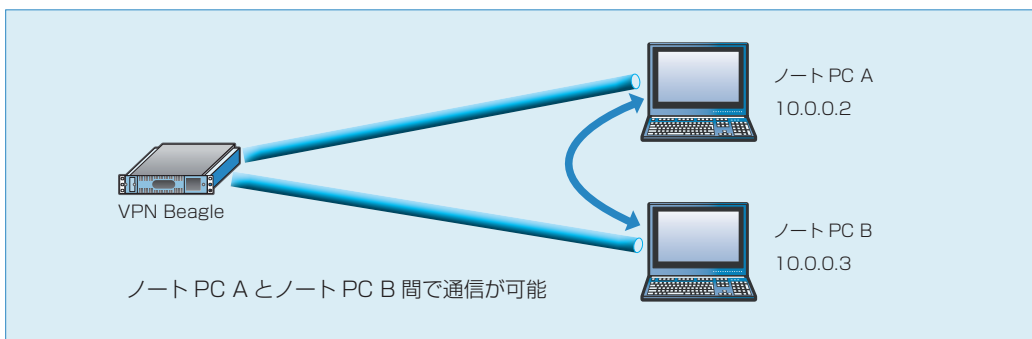


図 2-9 クライアント間接続が有効

■ クライアント間接続が無効な場合

クライアント間接続機能を無効にした場合、各クライアントは VPN Beagle Center およびそのローカルサーバーのみにアクセスが可能となります。

! クライアント間の通信を許可しない用途の場合、無効にしてください。

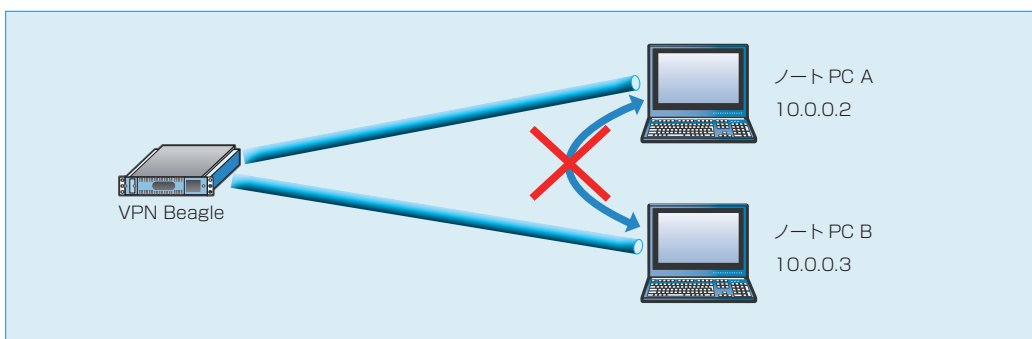


図 2-10 クライアント間接続が無効



クライアント接続機能の変更方法は
P. 47 管理画面→VPN 設定→サーバー設定を参照してください。

3

第 3 章

VPNの管理

1. ソフトウェアクライアントの追加・編集・削除
2. ハードウェアクライアントの追加・編集・削除
3. 一括インポート／エクスポート

1. ソフトウェアクライアントの追加・編集・削除

ソフトウェアクライアントの作成

Windows PC などの端末で仕様するクライアント情報を作成します。

1 追加

「追加」をクリックします。

ソフトウェアクライアント検索

1 追加 リフレッシュ

ユーザー名: 氏名:

IPアドレス: ☐ DHCP 有効 / 無効: ☒ 有効 ☐ 無効

登録日時: -- 年 -- 月 -- 日 ~ -- 年 -- 月 -- 日

検索 リセット

氏名 ▲▼	ユーザー名 ▲▼	IPアドレス	有効 / 無効	登録日時 ▲▼
佐藤	sato	DHCP	有効	2009/12/03 16:29:45
鈴木	suzuki	DHCP	有効	2009/12/03 16:29:29

0 / 1 合計: 2 件

図 3-1

2 適用

各入力項目を入力し、「適用」をクリックします。

PCクライアント追加

氏名:

ユーザー名:

パスワード:

IPアドレス: ☒ DHCP

証明書形式: ☒ ファイル ☐ トークン

トークンプレフィックス:

有効 / 無効: ☒ 有効 ☐ 無効

有効期限: / /

2 適用 リセット

図 3-2



各入力項目については、P. 56 運用管理のソフトウェアクライアントの追加を参照してください。

アカウントの作成に成功した場合、「ソフトウェアクライアント設定」画面にアカウントがリストされます。

3 対象アカウント

対象アカウントをクリックします。

4 ダウンロード

「ダウンロード」をクリックします。

対象アカウントの設定情報・証明書を含んだ「config.zip」というファイルがダウンロードされます。

ソフトウェアクライアント設定	
ユーザー名	suzuki
氏名	鈴木
有効 / 無効	☒ 有効 ☐ 無効
登録日時	2011/08/01 21:21:20
更新日時	
有効期限	2030/01/01 12:21:20
有効期限	2030 / 01 / 01
パスワード	
パスワード確認	
証明書形式	ファイル
トークンプレフィックス	
編集 <input checked="" type="button" value="4 ダウンロード"/> 削除	

図 3-3

Windows PC にて VPN 接続を行う例

※ VPN 接続対象 PC に既に OpenVPN クライアントソフトがインストール済みの場合
手順 1, 2 は飛ばしてください。

1. OpenVPN クライアントソフトをダウンロードします。

OpenVPN クライアントソフトは下記 URL からダウンロード可能です。

<http://openvpn.net/index.php/open-source/downloads.html>

windowsPC 用のクライアントソフトは「openvpn-xx.xx.xx-install.exe」という
実行形式のファイルです。

2. OpenVPN クライアントソフトをインストールします。

OpenVPN クライアントソフトのインストーラに従いインストールを行ってください。

3. クライアント設定情報・証明書を配置します。

ソフトウェアクライアントの作成手順にて取得した config.zip ファイルを解凍ソフトなどで展開します。

すると、VPN Beagle のホスト名がフォルダ名のディレクトリが現れます。

このディレクトリを OpenVPN クライアントソフトの設定情報格納フォルダにディレクトリごと移動します。

設定情報格納フォルダはデフォルト設定でインストールした場合

「C:\Program Files\OpenVPN\config」 となります。

4. OpenVPN クライアントを起動する。

「OpenVPN GUI」アイコンをクリックし、OpenVPN を起動します。

起動すると、タスクバーにアイコンが表示されます

5. VPN Beagle Center と接続する。

タスクバーのアイコンを右クリックします。

■ VPN 接続先が VPN Beagle Center のみの場合

メニューの一番上の接続を選択します。

パスワードを聞かれるので、アカウント作成時に設定したパスワードを入力します。

VPN 接続に成功した場合、タスクバーのアイコンが緑色に変わります。

■ VPN 接続先が複数登録済みの場合

メニューから接続先（VPN Beagle のホスト名）を選択し、サブメニューから接続を選択します。

パスワードを聞かれるので、アカウント作成時に設定したパスワードを入力します。

VPN 接続に成功した場合、タスクバーのアイコンが緑色に変わります。

ソフトウェアクライアントの編集

作成済みのソフトウェアクライアント情報を編集します。

- 1 サイドメニューにて「ソフトウェアクライアント設定」をクリックします。

対象アカウントをクリックします。

ソフトウェアクライアント検索

追加 リフレッシュ

ユーザー名: 氏名:

IPアドレス: ☐ DHCP 有効 / 無効: ☒ 有効 ☐ 無効

登録日時: -- 年 -- 月 -- 日 -- 年 -- 月 -- 日

検索 リセット

氏名 ▲▼	ユーザー名 ▲▼	IPアドレス	有効 / 無効	登録日時 ▲▼
佐藤	sato	DHCP	有効	2009/12/03 16:29:45
鈴木	suzuki	DHCP	有効	2009/12/03 16:29:29

(1 / 1 合計: 2 件)

図 3-4

ソフトウェアクライアント編集画面では下記の項目を編集することができますが各項目で設定情報・証明書への影響が異なります。

ソフトウェアクライアント設定

1 ユーザー名: suzuki

2 氏名: 鈴木

3 有効 / 無効: ☒ 有効 ☐ 無効

登録日時: 2011/08/01 21:21:20

更新日時:

有効期限: 2030/01/01 12:21:20

4 有効期限: 2030 / 01 / 01

5 パスワード:

パスワード確認:

証明書形式: ファイル

トークンプレフィックス:

6 編集 ダウンロード 削除

図 3-5

② 氏名

変更により VPN 接続・設定情報への影響はありません。

③ 有効／無効

証明書の状態を設定します。

【有効】にした場合、対象クライアントの VPN 接続が可能になります。

【無効】にした場合、対象クライアントの VPN 接続が拒否されます。



クライアントが接続中の状態で【有効】→【無効】に変更した場合、接続はしばらく（最長1時間程度）接続は維持します。接続中のクライアントを即座に切断したい場合は、クライアントの削除を行ってください。

④ 有効期限

ソフトウェアクライアントのクライアント証明書の有効期限を編集してください。

⑤ パスワード

証明書に設定されるパスワードを編集してください。

⑥ 「編集」をクリックします。

有効期限、パスワードを編集した場合、設定情報が更新され古い設定情報では接続できなくなります。

そのため再度新しい設定情報をダウンロードし、PC に適用しなおしてください。

ソフトウェアクライアントの削除

作成済みのソフトウェアクライアント情報を編集します。

- 1 サイドメニューにて「ソフトウェアクライアント設定」をクリックします。

対象アカウントをクリックします。

ソフトウェアクライアント検索

追加 リフレッシュ

ユーザー名: 氏名:

IPアドレス: ☐ DHCP 有効 / 無効: ☒ 有効 ☐ 無効

登録日時: -- 年 -- 月 -- 日 ~ -- 年 -- 月 -- 日

検索 リセット

氏名 ▲▼	ユーザー名 ▲▼	IPアドレス	有効 / 無効	登録日時 ▲▼
佐藤	sato	DHCP	有効	2009/12/03 16:29:45
鈴木	1 suzuki	DHCP	有効	2009/12/03 16:29:29

0 / 1 合計: 2 件

図 3-6

- 2 「削除」をクリックします。

ソフトウェアクライアント設定

ユーザー名: suzuki

氏名: 鈴木

有効 / 無効: ☒ 有効 ☐ 無効

登録日時: 2009/12/03 16:29:29

更新日時:

有効期限: 2030/01/01 07:29:29

有効期限: 2030 / 01 / 01

パスワード:

パスワード確認:

編集 ダウンロード 2 削除

図 3-7

! クライアントの削除を行った場合、クライアント接続中であっても即座に切断されます。

2. ハードウェアクライアントの追加・編集・削除

ハードウェアクライアントの作成

ハードウェアクライアントは拠点間接続を行う VPN Beagle Point 用のアカウントとなります。

- ① サイドメニューにて「ハードウェアクライアント設定」をクリックします。

「追加」をクリックします。

ハードウェアクライアント検索

1 追加 リフレッシュ

ユーザー名: 氏名:

IPアドレス: ☐ DHCP 有効 / 無効: ☒ 有効 ☐ 無効

登録日時: -- 年 -- 月 -- 日 ~ -- 年 -- 月 -- 日

検索 リセット

氏名 ▲▼	ユーザー名 ▲▼	IPアドレス	有効 / 無効	登録日時 ▲▼
福岡支店	hukuoka	DHCP	有効	2009/12/03 16:26:03
大阪支店	oosaka	DHCP	有効	2009/12/03 16:25:35

0 / 1 合計: 2 件

図 3-8

- ② 各入力項目を入力し、「適用」をクリックします。

ルータクライアント追加

氏名: 大阪支店

ユーザー名: oosaka

IPアドレス: ☒ DHCP

有効 / 無効: ☒ 有効 ☐ 無効

ハードウェア情報

IPアドレス: ☒ DHCP

ネットマスク:

ゲートウェイ:

DNS サーバ:

LAN情報

ネットワークアドレス: 192 168 100 0

ネットマスク: 255 255 255 0

有効期限: 2030 / 1 / 1

2 適用 リセット

図 3-9



各入力項目については、P.56 運用管理のソフトウェアクライアントの追加を参照してください。

アカウントの作成に成功した場合、「ソフトウェアクライアント設定」画面にアカウントがリストされます。

① 対象アカウントをクリックします。

ハードウェアクライアント検索

ユーザー名: 氏名:

IPアドレス: ☐ DHCP 有効 / 無効: ☒ 有効 ☐ 無効

登録日時: -- 年 -- 月 -- 日 ~ -- 年 -- 月 -- 日

検索 リセット

氏名 ▲▼	ユーザー名 ▲▼	IPアドレス	有効 / 無効	登録日時 ▲▼
福岡支店	hukuoka	DHCP	有効	2009/12/03 16:26:03
大阪支店	oosaka	DHCP	有効	2009/12/03 16:25:35

(1 / 1 合計: 2 件)

図 3-10

② 「ダウンロード」をクリックします。

対象アカウントの設定情報・証明書を含んだ「config.tgz」というファイルがダウンロードされます。

ルータクライアント編集

ユーザー名: oosaka

氏名: 大阪支店

IPアドレス: ☒ DHCP

有効 / 無効: ☒ 有効 ☐ 無効

ハードウェア情報

IPアドレス: ☒ DHCP

ネットマスク:

ゲートウェイ:

DNSサーバー:

LAN情報

ネットワークアドレス: 192 168 100 0

ネットマスク: 255 255 255 0

登録日時: 2009/12/03 16:25:35

更新日時:

有効期限: 2030/01/01 07:25:35

有効期限: 2030 / 01 / 01

編集 2 ダウンロード 削除

図 3-11

このファイルは VPN Beagle Point の設置時に使用します。

VPN Beagle Point の設置・設定手順については VPN Beagle Point マニュアルをご確認ください。

ハードウェアクライアントの編集

作成済みのハードウェアクライアント情報を編集します。

- 1 サイドメニューにて「ハードウェアクライアント設定」をクリックします。

対象アカウントをクリックします。

氏名 Δ▽	ユーザー名 Δ▽	IPアドレス	有効 / 無効	登録日時 Δ▽
福岡支店	hukuoka	DHCP	有効	2009/12/03 16:26:03
大阪支店	oosaka	DHCP	有効	2009/12/03 16:25:35

0 / 1 合計: 2 件

図 3-12

ハードクライアント編集画面では下記の項目を編集することができますが
各項目で設定情報・証明書への影響が異なります。

ルータクライアント編集

ユーザー名: oosaka

2 氏名: 大阪支店

3 有効 / 無効: ☒ 有効 ☐ 無効

4 ハードウェア情報

IPアドレス: ☒ DHCP

ネットマスク:

ゲートウェイ:

DNS サーバ:

LAN情報

ネットワークアドレス: 192 168 100 0

ネットマスク: 255 255 255 0

登録日時: 2009/12/03 16:25:35

更新日時:

有効期限: 2030/01/01 07:25:35

5 有効期限: 2030 / 01 / 01

6 編集 ダウンロード 削除

図 3-13

② 氏名

変更により VPN Beagle Point への影響はありません。

③ 有効／無効

設定情報の更新はありません。

証明書の状態を設定します。

【有効】にした場合、対象クライアントの VPN 接続が可能になります。

【無効】にした場合、対象クライアントの VPN 接続が拒否されます。



クライアントが接続中の状態で【有効】→【無効】に変更した場合、接続はしばらく（最長 1 時間程度）接続は維持します。
接続中のクライアントを即座に切断したい場合は、クライアントの削除を行ってください。

④ ハードウェア情報・LAN 情報の各種情報

現状の VPN Beagle Point の動作に影響はありません。

⑤ 有効期限

有効期限を変更した場合、設定情報が更新されます。

そのため変更完了後は、古い設定情報では接続できなくなります。

VPN Beagle Point が接続中にハードウェアクライアントのクライアント証明書の有効期限を編集してください。

⑥ 【編集】

「編集」をクリックします。

ハードウェア情報・LAN 情報・有効期限を変更した場合は設定情報をダウンロードの上 VPN Beagle Point への再適用および VPN Beagle Point の再起動をおこなってください

ハードウェアクライアントの削除

作成済みのハードウェアクライアント情報を編集します。

① サイドメニューにて「ハードウェアクライアント設定」をクリックします。

対象アカウントをクリックします。

ハードウェアクライアント検索

ユーザー名: 氏名: 有効 / 無効: ☒ 有効 ☐ 無効

IPアドレス: ☐ DHCP

登録日時: -- 年 -- 月 -- 日 ~ -- 年 -- 月 -- 日

検索 リセット

氏名 ▲▼	ユーザー名 ▲▼	IPアドレス	有効 / 無効	登録日時 ▲▼
福岡支店	hukuoka	DHCP	有効	2009/12/03 16:26:03
大阪支店	oosaka	DHCP	有効	2009/12/03 16:25:35

(1 / 1 合計: 2 件)

図 3-14

② 「削除」をクリックします。

ルータクライアント編集

ユーザー名: oosaka

氏名: 大阪支店

IPアドレス: ☒ DHCP

有効 / 無効: ☒ 有効 ☐ 無効

ハードウェア情報

IPアドレス: ☒ DHCP

ネットマスク:

ゲートウェイ:

DNSサーバー:

LAN情報

ネットワークアドレス: 192 168 100 0

ネットマスク: 255 255 255 0

登録日時: 2009/12/03 16:25:35

更新日時:

有効期限: 2030/01/01 07:25:35

有効期限: 2030 / 01 / 01

編集 ダウンロード 削除

図 3-15

クライアントの削除を行った場合、クライアント接続中であっても即座に切断されます。

3. 一括インポート／エクスポート

大量のソフトウェアアカウントを一括インポートすることができます。

また、アカウント情報を一括エクスポートすることができます。

一括インポート

CSV形式ファイルにアカウントを設定することで一括アカウント登録することが可能です。

CSV形式の書式は以下のとおりです。

1 列目	ユーザー名	英数字とアンダースコア (_) のみ入力可能です。
2 列目	パスワード	英数字とアンダースコア (_) のみ入力可能です。
3 列目	氏 名	必須項目ではありません。特に制限はありません。
4 列目	IP アドレス	仮想 IP アドレスを設定してください。 DHCP 指定の場合は「DHCP」と入力してください。
5 列目	有効／無効	アカウントの有効／無効を入力します。 有効ならば「Enable」、無効なら「Disable」と入力します。
6 列目	有効期限	アカウントの有効期限を入力します。 yyyy/mm/dd と日付形式で入力します。
7 列目	証明書形式	証明書形式を入力します。証明書形式がファイル形式ならば「file」 トークン (PKCS#12) 形式ならば「token」と入力します。
8 列目	トークン プレフィックス	明書形式がトークンの場合にトークンプレフィックスを入力します。 空白の場合、サーバ設定に設定されているデフォルトトークンプレフィックスの値が使用されます。

■ CSV ファイル例

	A	B	C	D	E	F	G	H
1	#ユーザー名	パスワード	氏名	IPアドレス	有効/無効	有効期限	証明書形式	トークンプレフィックス
2	satou	6LS8HsIn	佐藤	DHCP	Enable	2020/10/1	file	
3	tanaka	eP6q/Kh	田中	DHCP	Enable	2020/10/1	file	
4	yamada	82BK/Y4f	山田	10.0.0.10	Enable	2025/1/20	file	
5	suzuki	k8K/bU4:	鈴木	DHCP	Enable	2030/2/5	token	prefix
6	kato	28/LoMDa	加藤	DHCP	Enable	2030/2/5	token	prefix
7								
8								

図 3-16

① 作成した CSV ファイルを選択し、「実行」をクリックします。

各アカウントごとにインポート結果が出力されます。

■ インポート結果例



図 3-17

! インポートできなかったアカウントについてはエラーメッセージを元に CSV 設定内容を再度ご確認ください。

一括エクスポート

現在のソフトウェアクライアントのアカウント情報を一括出力します。

- ① 一括エクスポート欄の、「実行」をクリックします。

アカウントリストが CSV 形式でダウンロードできます。

■ エクスポート結果結果例

	A	B	C	D	E	F	G	H
1	#ユーザー名	パスワード	氏名	IPアドレス	有効/無効	有効期限	証明書形式	トークンプレフィックス
2	satou	6LS8Hsln	佐藤	DHCP	Enable	2020/10/1	file	
3	tanaka	eP6q7Kh	田中	DHCP	Enable	2020/10/1	file	
4	yamada	82BK7Y4f	山田	10.0.0.10	Enable	2025/1/20	file	
5	suzuki	k8K/bU4:	鈴木	DHCP	Enable	2030/2/5	token	prefix
6	katou	28/L0MDa	加藤	DHCP	Enable	2030/2/5	token	prefix
7								
8								

図 3-18

4

第 4 章

運用管理

1. Syslog 設定

2. サポート情報取得

3. バックアップ／リストア

4. ファームウェア

5. 再起動

1. Syslog 設定

VPN Beagle が出力する Syslog を Syslog サーバーに転送する機能です。

! Syslog の出力内容については、マニュアルにてサポートしておりません。

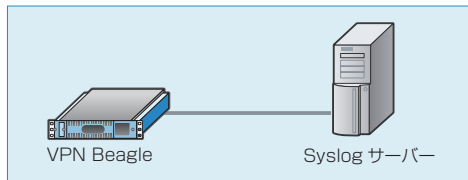


図 4-1 Syslog サーバーとの通信

■ VPN Beagle の設定

- ①【通知設定】→【Syslog】を選択してください。

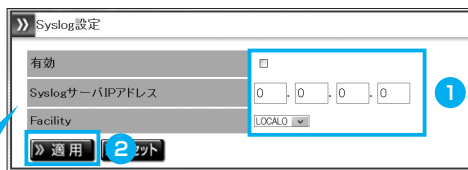


図 4-2 Syslog 設定画面

Syslog を有効にする場合

有効	チェックボックスにチェックをいれます。
IP アドレス	Syslog の転送先サーバーを設定します。
facility	Syslog の facility を設定します。

- ②上記の設定を行い、「適用」をクリックしてください（図 4-2）。

■ Syslog サーバーの設定

Syslog サーバーにて、VPN Beagle の Syslog を受信できるよう設定してください。設定後、VPN Beagle からの Syslog が受信されていることを確認してください。

! Syslog サーバーにおける Syslog 設定については、Syslog サーバーの OS もしくはソフトのマニュアルを参照してください。

2. サポート情報取得

VPN Beagle の動作について当社で調査を行う場合に、取得してご提供いただく場合に使用します。

サポート情報取得手順

- ① 【運用管理】 → 【サポート情報取得】 を選択します。
- ② 「実行」 をクリックするとサポート情報のダウンロードが開始されます（図 4-3）。

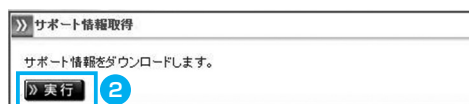


図 4-3

！ ダウンロード手順はご使用のブラウザによって異なります。

3. バックアップ／リストア

VPN Beagle の設定のバックアップとリストアを行う場合に使用します。

設定情報のバックアップ

VPN Beagle の設定情報をバックアップします。

「**実行**」ボタンをクリックすると、VPN Beagle の設定情報がダウンロードできます。

1 【実行】

VPN Beagle の設定情報を
バックアップします。



図 4-4

- ❗ ファイルのダウンロード手順はご使用のブラウザによって異なります。
- ❗ ダウンロードしたファイルを編集すると、正常にリストアできなくなります。
ダウンロードしたファイルは編集を行わずそのまま保管してください。

設定情報のリストア

バックアップした VPN Beagle の設定情報をリストアします。

「**参照**」ボタンをクリックし、VPN Beagle の設定情報のバックアップファイルを指定します。

「**実行**」ボタンをクリックすると、指定したバックアップファイルを用いて、VPN Beagle の設定情報がリストアできます。

1 【参照】

VPN Beagle の設定情報のバック
アップファイルを指定します。



図 4-5

2 【実行】

VPN Beagle の設定情報をリストアします。

- ❗ リストア完了後は即座にシステムが再起動されます。
- ❗ リストアに失敗した場合、以下の項目をご確認ください。
 - ・指定したファイルがバックアップ手順で取得したファイルかどうか。
 - ・取得したファイルを編集していないか。

4. ファームウェア

VPN Beagle では、機能追加や不具合対応によりファームウェアの提供を行うことがあります。

最新のファームウェアは弊社ウェブページをご確認の上、入手してください。

<http://online.atworks.co.jp>

- ❗ ファームウェアのアップデートを行う前に「設定情報のバックアップ」を実施し、設定情報を控えておいてください。
- 📁 「設定情報のバックアップ」については、P. 39を参照してください。
- ❗ ファームウェアのアップデート失敗や VPN Beagle 本製品の故障の原因となる場合があります。

ファームウェアバージョンの確認

VPN Beagle のファームウェアのバージョンは下記の手順で確認することができます（図4-6）。

【運用管理】→【ファームウェア】を選択してください。

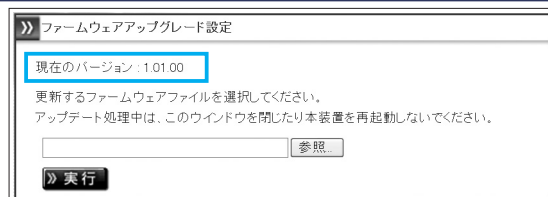


図 4-6 バージョン表示画面

ファームウェアのアップデート手順

❗ 本手順は VPN Beagle の再起動が発生します。

- ❶ 弊社ウェブページより、更新するファームウェアをダウンロードしてください。

<http://online.atworks.co.jp>

- ❷ 【運用管理】→【ファームウェア】を選択してください。

- ❸ 取得したファームウェアを入力してください。

または、「参照」をクリックすると、ディレクトリ一覧が表示されます。ここからファームウェアを選択します。

- ❹ ファームウェアを選択後、「実行」をクリックするとファームウェアのアップデートが開始されます（図47）。ファームウェアのアップデートに成功すると、自動的に再起動が実施されます。再起動後に再度「ファームウェアバージョンの確認」手順にてアップデートされたことを確認してください。

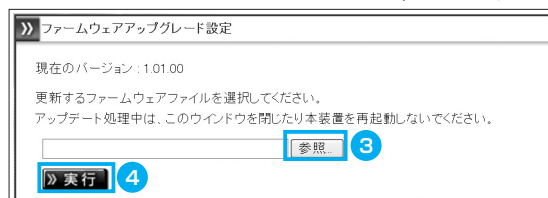


図 4-7 バージョン表示画面

5. 再起動

VPN Beagle の再起動を行う場合に使用します。

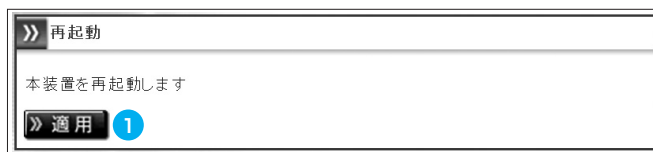


図 4-8

① 【適用】

VPN Beagle の再起動を行います。

5

第 5 章

管理画面の機能説明

1. ログイン画面

2. 基本設定

3. アクセス制限

4. VPN 設定

5. VPN 状態

6. 運用管理

1. ログイン画面

1 VPN Beagle のログイン画面を表示します。

ブラウザにて以下の URL を入力します。

[https:// \[VPN Beagle の IP アドレス\] :18180/](https://[VPN Beagle の IP アドレス]:18180/)

2 VPN Beagle のログイン画面を表示します。

ログイン名・ログインパスワードを入力してログインします。

 パスワードを忘れた場合は、P.68 を参照してください。

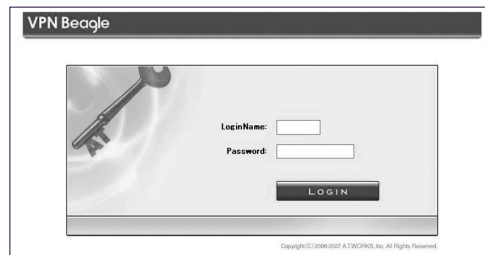


図 5-1



図 5-2

2. 基本設定

ネットワーク

VPN Beagle のネットワーク設定を表示・編集を行います。

サイドメニューにて「ネットワーク」をクリックします。

ネットワーク	
1 ホスト名	vpnbeagle
2 IPアドレス	192 168 1 1
3 ネットマスク	255 255 255 0
4 デフォルトゲートウェイ	192 168 1 254
5 プライマリDNSサーバ	0 0 0 0
6 セカンダリDNSサーバ	0 0 0 0
7 NTPサーバ	ntp.nict.jp
8 適用	9 リセット

図 5-3

1 IP アドレス

本装置のホスト名を設定します。

2 ネットマスク

本装置のネットマスクを設定します。

3 デフォルトゲートウェイ

本装置のデフォルトゲートウェイを設定します。

4 プライマリ DNS サーバー

本装置のプライマリ DNS サーバーを設定します。

5 セカンダリ DNS サーバー

本装置のセカンダリ DNS サーバーを設定します。

6 NTP サーバー

本装置の NTP サーバーを設定します。

7 【適用】

変更内容を本装置に反映します。

8 【リセット】

変更内容を初期化します。

ルーティング

VPN Beagle のルーティング設定の表示・編集を行います。

サイドメニューにて「ネットワーク」をクリックします。

宛先ネットワーク	宛先ネットマスク	ゲートウェイ	
172.16.0.0	255.255.255.0	10.10.0.1	1 削除
172.16.1.0	255.255.255.0	10.10.0.10	削除

宛先ネットワーク	宛先ネットマスク	ゲートウェイ
2	3	4

5 追加 6 リセット

図 5-4

1 削除

設定したルーティング設定を削除します。

2 宛先ネットワーク

ルーティング先のネットワークアドレスを設定します。

3 宛先ネットマスク

ルーティング先のネットマスクを設定します。

4 ゲートウェイ

ルーティング先へ経由するゲートウェイアドレスを設定します。

5 追加

設定内容を本装置に追加します。

6 リセット

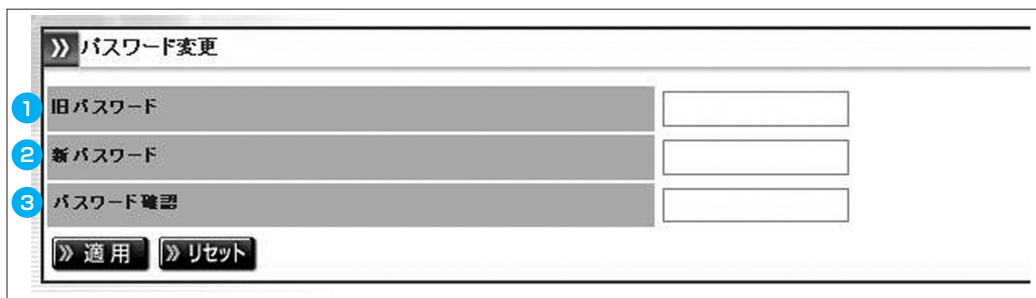
設定内容を初期化します。

3. アクセス制限

パスワード変更

管理画面のログインパスワードを変更することができます。

サイドメニューにて「パスワード変更」をクリックします。



The screenshot shows a web form titled 'パスワード変更' (Change Password). It contains three input fields: '旧パスワード' (Old Password), '新パスワード' (New Password), and 'パスワード確認' (Confirm Password). Below the fields are two buttons: '適用' (Apply) and 'リセット' (Reset). The form is enclosed in a light gray border with a title bar.

図 5-5

① 旧パスワード

現在のパスワードを入力します。パスワードが一致しなければ変更できません。

② 新パスワード

新しいパスワードを入力します。英数字およびハイフン (-)、アンダースコア (_) だけが使用可能です。

③ パスワード確認

新しいパスワードを再入力します。新パスワードと再入力したパスワードが一致しなければ変更できません。

接続許可 IP アドレス

管理画面に接続を許可する IP アドレスを設定します。

サイドメニューにて「接続許可 IP アドレス」をクリックします。

The screenshot displays the '接続許可 IP アドレス' (Connection Allowed IP Address) management interface. It is divided into two main sections. The first section, titled '1 接続許可IPアドレス', contains two input fields: 'IPアドレス' and 'ネットマスク'. The second section, titled '2 接続許可IPアドレス追加', contains two input fields: 'IPアドレス' and 'ネットマスク'. The 'IPアドレス' field in section 2 is populated with the values 192, 168, 1, and 1, each in its own box. The 'ネットマスク' field in section 2 is populated with the values 255, 255, 255, and 255, each in its own box. Below these fields are two buttons: '追加' (Add) and 'リセット' (Reset).

図 5-6

1 接続許可 IP アドレス

本機の管理画面に接続を許可するIPアドレスとネットマスクです。

【削除】 ボタンを押すと、対象のIPアドレスとネットマスクが削除されます。



接続許可IPアドレスが設定されていない場合、
全てのIPアドレスから接続が可能です。

2 接続許可 IP アドレス追加

本機の管理画面に接続を許可するIPアドレスとネットマスクを追加することができます。

4. VPN 設定

サーバー設定

サイドメニューにて「サーバー設定」をクリックします。
サーバーの設定を行います。



安全にお使いいただくために必ずお守りください。

図 5-7

1 管理画面接続ポート

管理画面接続に使用するポート番号を表示します。

2 ネットワークアドレス

VPN サービスが使用するネットワークアドレスを指定します。

対象システムで重複しないプライベートアドレスを指定してください。

3 ネットマスク

VPN サービスが使用するネットワークのネットマスクを指定します。

④ VPN サーバー仮想 IP アドレス

本装置の VPN 上の IP アドレスを表示します。

⑤ DHCP 開始 IP アドレス

VPN 内で DHCP が割り当て可能な開始 IP アドレスを指定します。

⑥ DHCP 終了 IP アドレス

VPN 内で DHCP が割り当て可能な終了 IP アドレスを指定します。

⑦ VPN サーバー名

VPN サーバーのサーバー名もしくは IP アドレスを指定します。

⑧ VPN サーバーポート番号

VPN サービスの使用するポート番号を指定します。

⑨ 最大接続数

VPN サーバーに同時に接続できる最大クライアント数を指定します。

⑩ デフォルト証明書形式

アカウント追加時の証明書形式のデフォルト値を設定します。

ファイル・・・ファイル形式の証明書

トークン・・・USB トークンなどで使用可能な PKCS#12 形式の証明書

⑪ デフォルトトークンプレフィックス

証明書形式をトークンに設定した場合のユーザー名に追加する。

プレフィックスのデフォルトを設定します。

⑫ クライアント接続許可

VPN サーバーに接続しているクライアント間の通信を許可したい場合、本オプションを指定します。本オプションを有効にした場合、VPN サーバーに接続しているクライアント間で通信が可能となります。

⑬ クライアントログイン許可

登録しているクライアントが管理画面にログインを許可したい場合、本オプションを指定します。ただし、アクセス可能なのはログインしたクライアントの情報編集画面のみとなります。

⑭ ネットワークアドレス

VPN サーバーのローカルネットワークアドレスを表示します。

⑮ ネットマスク

VPN サーバーのローカルネットワークのネットマスクを表示します。

⑯ ネットワークアドレス

追加する VPN サーバーのローカルネットワークアドレスを指定します。

⑰ ネットマスク

追加する VPN サーバーのローカルネットワークのネットマスクを指定します。

ハードウェアクライアント検索

サイドメニューにて「ハードウェアクライアント設定」をクリックします。

Figure 5-8 shows the 'Hardware Client Search' interface. It features several search criteria: 1. User Name, 2. Surname, 3. IP Address (with a DHCP checkbox), 4. Valid/Invalid status (radio buttons for '有効' and '無効'), 5. Registration Date/Time (date and time pickers). Action buttons include 6. Add, 7. Refresh, 8. Search, and 9. Reset. A table at the bottom displays results with columns for Client Name, User Name, IP Address, Valid/Invalid status, and Registration Date/Time. Two results are shown: '福岡支店' (Fukuoka Branch) and '大阪支店' (Osaka Branch). The status bar indicates '0 / 1 合計: 2 件'.

氏名 △▽	ユーザー名 △▽	IPアドレス	有効 / 無効	登録日時 △▽
福岡支店	hukuoka	DHCP	有効	2009/12/03 16:26:03
大阪支店	osaka	DHCP	有効	2009/12/03 16:25:35

0 / 1 合計: 2 件

図 5-8

1 ユーザー名

入力した文字列を含むユーザー名をもつハードウェアクライアントを全て検索することができます。

2 氏名

入力した文字列を含む氏名をもつハードウェアクライアントを全て検索することができます。

3 IP アドレス

入力した IP アドレスに完全に一致したハードウェアクライアントのみ検索することができます。DHCP をチェックした場合、DHCP を有効にしたハードウェアクライアントを検索することができます。

4 有効 / 無効

証明書の状態です。【有効】または【無効】を選択することができます。

5 登録日時

証明書の登録日時です。設定期間内に登録されたハードウェアクライアントを全て検索することができます。

6 【追加】

ハードウェアクライアントの新規追加画面を表示します。

7 【リフレッシュ】

画面を更新します。

8 【検索】

設定した検索条件にて検索を実施します。

9 【リセット】

検索条件を全てクリアします。

10 【氏名】 【ユーザー名】

クリックすると対象ルータクライアントの編集画面を表示します。

ハードウェアクライアント追加

サイドメニューにて「ハードウェアクライアント設定」をクリックします。
右上の【追加】ボタンをクリックします。

ルータクライアント追加

1 氏名: 大阪支店

2 ユーザー名: oosaka

3 IPアドレス: [][][][] ☒ DHCP

4 有効 / 無効: ☒ 有効 ☐ 無効

ハードウェア情報

5 IPアドレス: [][][][] ☒ DHCP

6 ネットマスク: [][][][]

7 ゲートウェイ: [][][][]

8 DNSサーバ: [][][][]

LAN情報

9 ネットワークアドレス: [192][168][100][0]

10 ネットマスク: [255][255][255][0]

11 有効期限: 2030 / 1 / 1

12 適用 13 リセット

図 5-9

1 氏名

氏名を入力することができます。必須項目ではありません。

2 ユーザー名

ユーザー名を設定してください。英数字とアンダースコア (_) のみ入力可能です。

3 IP アドレス

対象ルータの仮想 IP アドレスを設定してください。DHCP 指定の場合は「DHCP」と表示されます。

4 有効 / 無効

証明書の状態を設定します。

【有効】にした場合、対象クライアントの VPN 接続が可能になります。

【無効】にした場合、対象クライアントの VPN 接続が拒否されます。

■ ハードウェア情報

⑤ IP アドレス

ハードウェアクライアントの IP アドレスを設定してください

DHCP 指定の場合は「DHCP」を設定してください。

⑥ ネットマスク

ハードウェアクライアントのネットマスクを設定してください。

⑦ ゲートウェイ

ハードウェアクライアントのゲートウェイを設定してください。

⑧ DNS サーバー

ハードウェアクライアントが参照する DNS サーバーを設定してください。

■ LAN 情報

⑨ ネットワークアドレス

対象ハードウェアの配置されるネットワークのネットワークアドレスを設定してください。

IP アドレスが DHCP 指定の場合でも設定してください。

⑩ ネットマスク

対象ハードウェアの配置されるネットワークのネットマスクを設定してください。

IP アドレスが DHCP 指定の場合でも設定してください。

⑪ 有効期限

ハードウェアクライアントのクライアント証明書の有効期限を設定してください。

⑫ 【適用】

ハードウェアクライアントのクライアント設定を追加します。

⑬ 【リセット】

設定内容をクリアします。

ハードウェアクライアント編集

サイドメニューにて「ハードウェアクライアント設定」をクリックします。
追加済みクライアントの氏名もしくはユーザー名をクリックします。

ルータクライアント編集

1 ユーザー名 oosaka

2 氏名 大阪支店

3 IPアドレス ☒ DHCP

4 有効 / 無効 ☒ 有効 ☐ 無効

ハードウェア情報

5 IPアドレス ☒ DHCP

6 ネットマスク

7 ゲートウェイ

8 DNSサーバ

LAN情報

9 ネットワークアドレス 192 168 100 0

10 ネットマスク 255 255 255 0

11 登録日時 2009/12/03 16:25:35

12 更新日時

13 有効期限 2030/01/01 07:25:35

有効期限 2030 / 01 / 01

14 編集 15 ダウンロード 16 削除

図 5-10

1 ユーザー名

ユーザー名は編集することができません。

2 氏名

氏名を編集することができます。

3 IP アドレス

対象ルータの仮想 IP アドレスを設定してください。DHCP 指定の場合は「DHCP」と表示されます。

4 有効／無効

証明書の状態を設定します。

【有効】にした場合、対象クライアントの VPN 接続が可能になります。

【無効】にした場合、対象クライアントの VPN 接続が拒否されます。



クライアントが接続中の状態で【有効】→【無効】に変更した場合、接続はしばらく（最長1時間程度）接続は維持します。接続中のクライアントを即座に切断したい場合は、クライアントの削除を行ってください。

■ ハードウェア情報

5 IP アドレス

ハードウェアクライアントの IP アドレスを設定してください。

DHCP 指定の場合は「DHCP」を設定してください。

6 ネットマスク

ハードウェアクライアントのネットマスクを設定してください。

7 ゲートウェイ

ハードウェアクライアントのゲートウェイを設定してください。

8 DNS サーバー

ハードウェアクライアントが参照する DNS サーバーを設定してください。

■ LAN 情報

9 ネットワークアドレス

対象ハードウェアの配置されるネットワークのネットワークアドレスを設定してください。IP アドレスが DHCP 指定の場合でも設定してください。

10 ネットマスク

対象ハードウェアの配置されるネットワークのネットマスクを設定してください。IP アドレスが DHCP 指定の場合でも設定してください。

11 登録日時

証明書が最初に作成された日時を表示します。

12 更新日時

証明書が最後に更新された日時を表示します。

13 有効期限

ハードウェアクライアントのクライアント証明書の有効期限を編集してください。

14 【編集】

クライアント設定の編集内容を更新されます。【有効期限】を更新した場合は、証明書が更新されますので【ダウンロード】にて証明書を再取得してください。

15 【ダウンロード】

ハードウェアクライアントの設定情報をダウンロードし取得できます。

16 【削除】

対象ハードウェアの設定情報を削除します。【削除】を押したときに対象ハードウェアが接続されている場合は、即座に接続が解除されます。

ソフトウェアクライアント検索

サイドメニューにて「ソフトウェアクライアント設定」をクリックします。

ソフトウェアクライアント検索

1 ユーザー名 2 氏名

3 IPアドレス ☐ DHCP 4 有効 / 無効 ☒ 有効 ☐ 無効

5 登録日時 -- 年 -- 月 -- 日 ~ -- 年 -- 月 -- 日

8 検索 9 リセット 6 追加 7 リフレッシュ

氏名 ▲▼	ユーザー名 ▲▼	IPアドレス	有効 / 無効	登録日時 ▲▼
佐藤	sato	DHCP	有効	2009/12/03 16:29:45
鈴木	suzuki	DHCP	有効	2009/12/03 16:29:29

0 / 1 合計 : 2 件

図 5-11

1 ユーザー名

入力した文字列を含むユーザー名をもつソフトウェアクライアントを全て検索することができます。

2 氏名

入力した文字列を含む氏名をもつソフトウェアクライアントを全て検索することができます。

3 IP アドレス

入力した IP アドレスに完全に一致したソフトウェアクライアントのみ検索することができます。DHCP をチェックした場合、DHCP を有効にしたソフトウェアクライアントを検索することができます。

4 有効／無効

証明書の状態です。【有効】または【無効】を選択することができます。

5 登録日時

証明書の登録日時です。設定期間内に登録されたソフトウェアクライアントを全て検索することができます。

6 【追加】

ソフトウェアクライアントの新規追加画面を表示します。

7 【リフレッシュ】

画面を更新します。

8 【検索】

設定した検索条件にて検索を実施します。

9 【リセット】

検索条件を全てクリアします。

10 【氏名】【ユーザー名】

クリックすると対象ルータクライアントの編集画面を表示します。

ソフトウェアクライアント追加

サイドメニューにて「ソフトウェアクライアント設定」をクリックします。

右上の【追加】ボタンをクリックします。

The screenshot shows a web form titled 'PCクライアント追加'. It has the following fields and controls:

- 1 氏名 (Name): Text input field with '鈴木' (Suzuki) entered.
- 2 ユーザー名 (Username): Text input field with 'suzuki' entered.
- 3 パスワード (Password): Password input field with masked characters.
- 4 IPアドレス (IP Address): IP input fields with '10', '0', '0' entered, and a checked 'DHCP' checkbox.
- 5 証明書形式 (Certificate Type): Radio buttons for 'ファイル' (File) and 'トークン' (Token). 'ファイル' is selected.
- 6 トークンプレフィックス (Token Prefix): Text input field.
- 7 有効 / 無効 (Valid / Invalid): Radio buttons for '有効' (Valid) and '無効' (Invalid). '有効' is selected.
- 8 有効期限 (Validity Period): Date input fields showing '2030 / 1 / 1'.
- 9 Buttons: '適用' (Apply) and 'リセット' (Reset).

図 5-12

1 氏名

氏名を入力することができます。必須項目ではありません。

2 ユーザー名

ユーザー名を設定してください。英数字とアンダースコア (_) のみ入力可能です。

3 IP アドレス

対象ルータの仮想 IP アドレスを設定してください。DHCP 指定の場合は「DHCP」と表示されます。

4 証明書形式

証明書形式を選択します。表示されます。

ファイル・・・ファイル形式の証明書

トークン・・・USB トークンなどで使用可能な PKCS#12 形式の証明書

5 トークンプレフィックス

証明書形式をトークンに設定した場合のユーザー名に追加する。

プレフィックスを設定します。

6 有効 / 無効

証明書の状態を設定します。

【有効】にした場合、対象クライアントの VPN 接続が可能になります。

【無効】にした場合、対象クライアントの VPN 接続が拒否されます。

7 有効期限

ソフトウェアクライアントのクライアント証明書の有効期限を設定してください。

8 【適用】

ソフトウェアクライアントのクライアント設定を追加します。

9 【リセット】

設定内容をクリアします。

ソフトウェアクライアント編集

サイドメニューにて「ソフトウェアクライアント設定」をクリックします。

追加済みクライアントの氏名もしくはユーザー名をクリックします。

ソフトウェアクライアント設定	
1 ユーザー名	suzuki
2 氏名	鈴木
3 有効 / 無効	☒ 有効 ☐ 無効
4 登録日時	2011/08/01 21:21:20
5 更新日時	
6 有効期限	2030/01/01 12:21:20
7 有効期限	2030 / 01 / 01
8 パスワード	
9 パスワード確認	
10 証明書形式	ファイル
11 トークンプレフィックス	
12	編集 13 ダウンロード 14 削除

図 5-13

1 氏名

氏名を編集することができます。

2 ユーザー名

ユーザー名は編集することができません。

3 IP アドレス

対象ルータの仮想 IP アドレスを設定してください。DHCP 指定の場合は「DHCP」と表示されます。

4 有効／無効

証明書の状態を設定します。

【有効】にした場合、対象クライアントの VPN 接続が可能になります。

【無効】にした場合、対象クライアントの VPN 接続が拒否されます。



クライアントが接続中の状態で【有効】→【無効】に変更した場合、接続はしばらく（最長 1 時間程度）接続は維持します。接続中のクライアントを即座に切断したい場合は、クライアントの削除を行ってください。

5 登録日時

証明書が最初に作成された日時を表示します。

5 有効期限

ソフトウェアクライアントのクライアント証明書の有効期限を設定してください。

6 更新日時

証明書が最後に更新された日時を表示します。

7 有効期限

ソフトウェアクライアントのクライアント証明書の有効期限を編集してください。

8 パスワード

証明書に設定されるパスワードを編集してください。

9 パスワード確認

確認のため、もう一度パスワードを入力してください。

10 証明書形式

対象アカウントの証明書形式を表示します。

11 トークンプレフィックス

対象アカウントの証明書形式がトークンの場合、プレフィックスを表示します。

12 【編集】

クライアント設定の編集内容を更新されます。

【有効期限】もしくは【パスワード】を更新した場合は、証明書が更新されますので【ダウンロード】にて証明書を再取得してください。

13 【ダウンロード】

ソフトウェアクライアントの設定情報をダウンロードし取得できます。

14 【削除】

対象ソフトウェアの設定情報を削除します。

【削除】を押したときに対象ソフトウェアが接続されている場合は、即座に接続が解除されます。

一括インポート／エクスポート

サイドメニューにて「ソフトウェアクライアント設定」をクリックします。

1 一括インポート

インポートファイル(CSV形式) 参照...

» 実行

2 一括エクスポート

» 実行

図 5-14

1 一括インポート

ソフトウェアクライアントを一括インポートします。【参照】ボタンを押し、インポートファイル（CSV 形式）を指定します。

【実行】ボタンを押すと、指定したインポートファイルを用いて、一括インポートします。

2 一括エクスポート

現在のソフトウェアクライアントを一括エクスポートします。

【実行】ボタンを押すと、ソフトウェアクライアント情報がダウンロードできます。

5. VPN 状態

接続状況

各ユーザーの接続状況を表示します。

各種条件にてクライアントを抽出することができます。

サイドメニューにて「接続状況」をクリックします。

The screenshot shows a web application for managing VPN connections. At the top, there's a title '接続状況' (Connection Status) and a 'リフレッシュ' (Refresh) button. Below are several search filters: 'ユーザー名' (User Name), '氏名' (Surname), 'IPアドレス' (IP Address), '接続状況' (Connection Status), and '接続/切断日時' (Connection/Disconnection Date and Time). There are also '検索' (Search) and 'リセット' (Reset) buttons. The search results are displayed in a table with columns: '氏名' (Surname), 'ユーザー名' (User Name), 'IPアドレス' (IP Address), '接続状況' (Connection Status), and '接続/切断日時' (Connection/Disconnection Date and Time). The table shows four clients: sato, suzuki, hukuoka, and oosaka, all with a status of '切断' (Disconnected). A footer indicates '(1 / 1 合計 : 4 件)' (1 / 1 Total: 4 items).

氏名 ▲▼	ユーザー名 ▲▼	IPアドレス	接続状況	接続/切断日時 ▲▼
佐藤	sato	DHCP	切断	2009/12/03 16:29:45
鈴木	suzuki	DHCP	切断	2009/12/03 16:29:29
福岡支店	hukuoka	DHCP	切断	2009/12/03 16:26:03
大阪支店	oosaka	DHCP	切断	2009/12/03 16:25:35

図 5-15

1 ユーザー名

入力した文字列を含むユーザー名をもつクライアントを全て検索することができます。

2 氏名

入力した文字列を含む氏名をもつクライアントを全て検索することができます。

3 IP アドレス

入力した IP アドレスに完全に一致したクライアントのみ検索することができます。

4 接続状況

ユーザーの接続状況です。【接続】または【切断】を選択することができます。

5 接続／切断日時

ユーザーの接続／切断日時です。

設定期間内に接続または切断が発生したクライアントを全て検索することができます。

6 【リフレッシュ】

画面を更新します。

7 【適用】

設定した検索条件にて検索を実施します。

8 【リセット】

検索条件を全てクリアします。

VPN 状態

VPN サービスの起動状態を確認することができます。

1 サービス	2 プロセスID	3 プロセス
openvpn	1485	起動中
httpd	1164	起動中

図 5-16

① サービス

動作しているサービス名を表示します。

② プロセス ID

サービスの使用プロセス ID を表示します。

③ プロセス

対象サービスの動作状態を表示します。

VPN ログ

各ユーザーが接続または切断したログを表示します。各種条件にてログを抽出することができます。

サイドメニューにて「VPN ログ設定」をクリックします。

The screenshot shows the 'VPN ログ' (VPN Log) management page. It features a search form with the following elements:

- 1 ユーザー名** (User Name): Text input field.
- 2 氏名** (Surname): Text input field.
- 3 IPアドレス** (IP Address): Text input field.
- 4 メッセージ** (Message): Dropdown menu.
- 5 接続/切断日時** (Connection/Disconnection Date/Time): Date and time range selector.
- 7 検索** (Search): Button to execute the search.
- 8 リセット** (Reset): Button to clear search conditions.
- 6 リフレッシュ** (Refresh): Button to reload the page.

Below the search form is a table displaying the search results:

氏名 ▲▼	ユーザー名 ▲▼	IPアドレス	接続/切断日時 ▲▼	メッセージ
佐藤	sato	10.0.0.3	2009/12/03 16:36:45	切断
佐藤	sato	10.0.0.3	2009/12/03 16:35:58	接続
鈴木	suzuki	10.0.0.2	2009/12/03 16:35:51	切断
鈴木	suzuki	10.0.0.2	2009/12/03 16:35:06	接続

At the bottom of the table, it indicates '(1 / 1 合計: 4 件)' (1 / 1 Total: 4 items).

図 5-17

1 ユーザー名

入力した文字列を含むユーザー名をもつクライアントを全て検索することができます。

2 氏名

入力した文字列を含む氏名をもつクライアントを全て検索することができます。

3 IPアドレス

入力した IP アドレスに完全に一致したクライアントのみ検索することができます。

4 メッセージ

メッセージです。【接続】または【切断】を選択することができます。

5 接続／切断日時

ユーザーの接続／切断日時です。

設定期間内に接続または切断が発生したクライアントを全て検索することができます。

6 【リフレッシュ】

画面を更新します。

7 【適用】

設定した検索条件にて検索を実施します。

8 【リセット】

検索条件を全てクリアします。

6. 運用管理

Syslog設定

本装置が出力する Syslog をリモート Syslog サーバーに転送することができます。
サイドメニューにて「Syslog 設定」をクリックします。

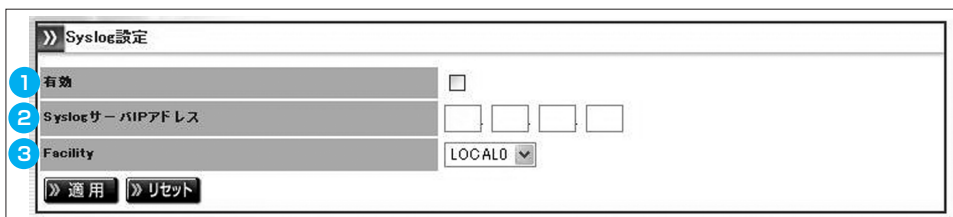


図 5-18

1 有効

有効にした場合、本機のログを Syslog サーバーに転送します。

2 IP アドレス

本機のログの転送先 Syslog サーバーの IP アドレスです。

3 facility

本機のログの facility です。

サポート情報取得

本装置の動作について弊社で調査を行う場合に取得してご提供いただく場合に使用します。
サイドメニューにて「サポート情報取得」をクリックします。

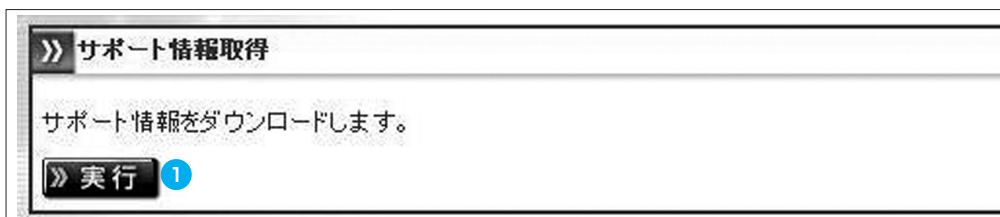


図 5-19

1 【実行】

サポート情報をダウンロードします。

バックアップ／リストア

各ユーザーが接続または切断したログを表示します。各種条件にてログを抽出することができます。

サイドメニューにて「VPN ログ設定」をクリックします。

■ バックアップ設定

設定情報をバックアップします。



図 5-19

① 【実行】

設定情報のバックアップファイルをダウンロードできます。

■ リストア設定



図 5-20

① 参照

バックアップしておいたファイルを指定します。

② 【実行】

指定したファイルを用いて設定情報をリストアできます。

ファームウェア

本装置のファームウェアバージョンの確認およびバージョンアップを行います。

サイドメニューにて「ファームウェア」をクリックします。

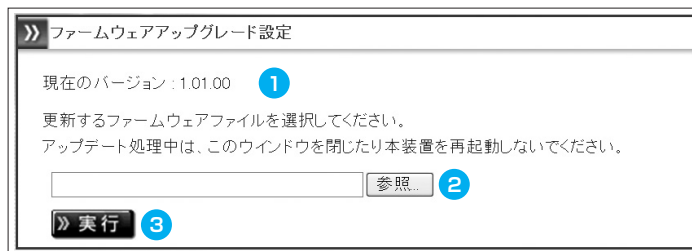


図 5-21

① 現在のバージョン

現在のファームウェアバージョンが表示されます。

② 参照

新しいファームウェアファイルを指定します。

③ 【実行】

指定したファイルを用いてファームウェアのバージョンアップを実行します。



バージョンアップ後は自動的に本装置は再起動されます。
ファームウェアをアップデートすると接続中のクライアントとの接続は全て切断されます。

再起動

本装置を再起動します。

サイドメニューにて「再起動」をクリックします。

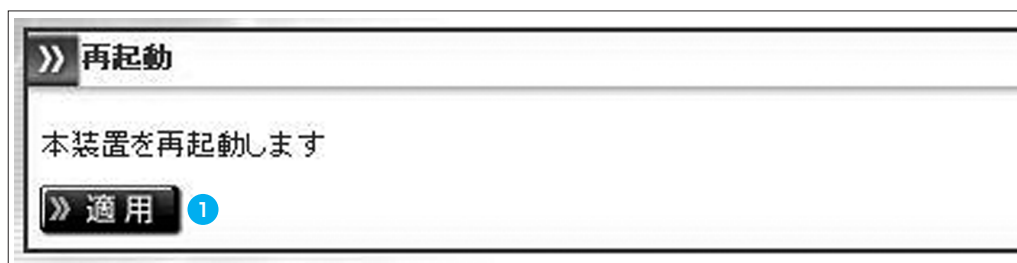


図 5-22

① 【適用】

本装置を再起動します。

6

第 6 章

コンソール管理

1. コンソール管理

1. コンソール管理

VPN Beagle のコンソール管理画面をお使いいただくための手順を説明します。

VPN Beagle にモニタ，キーボードを接続してください。

 VPN Beagle のフロントパネルについては P 8 を参照してください。

VPN Beagle のコンセントを電源に接続し，電源スイッチを押下します。

モニタにログインプロンプトが表示されますのでログイン ID とパスワードを入力します。このログイン ID およびパスワードは、装置に添付されているシートのコンソールログイン ID、パスワードを入力してください。

```
login: admin
Password:
```

図 4-1 ログイン画面

```
ログイン ID  admin
パスワード  *****
```

 このログイン ID とパスワードは VPN Beagle の管理画面へのログイン ID、パスワードとは異なります。変更することはできません。

ログインすると，コンソール管理メニューが表示されます。

```
Login: admin
Password:

1 --- Initialize configuration
2 --- Change WEB UI password
3 --- Change network setting
4 --- Change local network setting
5 --- Clear allow IP address list
6 --- Show network setting
7 --- Execute ping
8 --- Reboot
9 --- Exit
Please input [1-9]:
```

図 4-2 コンソール管理メニュー

工場出荷時設定に戻したい場合

VPN Beagle の設定を工場出荷時に戻す場合、管理メニューにて 1 を入力します。設定を初期化するか確認を求められますので、よろしければ y を入力してください。

```
Login: admin
Password:

1 --- Initialize configuration
2 --- Change WEB UI password
3 --- Change network setting
4 --- Change local network setting
5 --- Clear allow IP address list
6 --- Show network setting
7 --- Execute ping
8 --- Reboot
9 --- Exit
Please input [1-9]: 1

Do you want to initialize the configuration?[y/n]: y
```

図 4-3 設定の初期化

管理者パスワードを忘れた場合

Webインタフェ이스の管理者パスワードを忘れた場合、管理メニューにて 2 を入力します。新しいパスワードの入力を求められますので、パスワードの再設定を行います。

```
Login: admin
Password:

1 -- Initialize configuration
2 -- Change WEB UI password
3 -- Change network setting
4 -- Change local network setting
5 -- Clear allow IP address list
6 -- Show network setting
7 -- Execute ping
8 -- Reboot
9 -- Exit
Please input [1-9]: 2

Input new password:
```

図 4-4 パスワードの再設定

グローバルネットワーク設定を変更したい場合

VPN Beagle のグローバルネットワーク設定を変更する場合、管理メニューにて 3 を入力します。新しいIPアドレス、ネットマスク、ゲートウェイを入力し再設定を行ってください。

```
Login: admin
Password:

1 -- Initialize configuration
2 -- Change WEB UI password
3 -- Change network setting
4 -- Change local network setting
5 -- Clear allow IP address list
6 -- Show network setting
7 -- Execute ping
8 -- Reboot
9 -- Exit
Please input [1-9]: 3

Input new IP address: 172.16.0.10
Input new NetMask: 255.255.255.0
Input new Gateway: 172.16.0.1
```

図 4-5 グローバルネットワーク設定の変更

ローカルネットワーク設定を変更したい場合

VPN Beagle のローカルネットワーク設定を変更する場合、管理メニューにて 4 を入力します。新しいIPアドレス、ネットマスクを入力し再設定を行ってください。

```
Login: admin
Password:

1 -- Initialize configuration
2 -- Change WEB UI password
3 -- Change network setting
4 -- Change local network setting
5 -- Clear allow IP address list
6 -- Show network setting
7 -- Execute ping
8 -- Reboot
9 -- Exit
Please input [1-9]: 4

Input new IP address: 192.168.100.10
Input new NetMask: 255.255.255.0
```

図 4-6 ローカルネットワーク設定の変更

管理画面へのアクセス制限をクリアしたい場合

VPN Beagle の Web インタフェ이스へのアクセス制限をクリアする場合、管理メニューにて 5 を入力します。ただちにアクセス制限は解除されますので Web インタフェ이스にて再度アクセス制限を行ってください。

```
Login: admin
Password:

1 -- Initialize configuration
2 -- Change WEB UI password
3 -- Change network setting
4 -- Change local network setting
5 -- Clear allow IP address list
6 -- Show network setting
7 -- Execute ping
8 -- Reboot
9 -- Exit
Please input [1-9]: 5

Allow IP address list cleared!
```

図 4-7 アクセス制限のクリア

ネットワーク設定を確認したい場合

ネットワーク設定を確認したい場合、
管理メニューにて6を入力します。
現在のネットワーク設定が表示されます。

```
Login: admin
Password:

1 -- Initialize configuration
2 -- Change WEB UI password
3 -- Change network setting
4 -- Change local network setting
5 -- Clear allow IP address list
6 -- Show network setting
7 -- Execute ping
8 -- Reboot
9 -- Exit
Please input [1-9]: 6

Current Setting:
IP Address:      192.168.0.10
Net Mask:        255.255.255.0
Default Gateway: 192.168.0.1
```

図 4-8 ネットワーク設定確認

ネットワークの疎通を確認したい場合

VPN Beagle のネットワークの疎通を確認したい場合、管理メニューにて7を入力します。対象のIPアドレスとの疎通結果が表示されます。もし疎通結果が失敗していた場合（図4-9）、VPN Beagle のネットワーク設定やネットワークの配線をみなおしてください。

```
Login: admin
Password:

1 -- Initialize configuration
2 -- Change WEB UI password
3 -- Change network setting
4 -- Change local network setting
5 -- Clear allow IP address list
6 -- Show network setting
7 -- Execute ping
8 -- Reboot
9 -- Exit
Please input [1-9]: 7

Input destination IP address: 192.168.0.1
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=128 time=1.5 ms
64 bytes from 192.168.0.1: icmp_seq=1 ttl=128 time=1.5 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=128 time=1.1 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=128 time=1.6 ms

--- 192.168.24.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.1/1.4/1.6 ms
```

図 4-9 ネットワーク疎通確認（疎通成功）

```
Login: admin
Password:

1 -- Initialize configuration
2 -- Change WEB UI password
3 -- Change network setting
4 -- Change local network setting
5 -- Clear allow IP address list
6 -- Show network setting
7 -- Execute ping
8 -- Reboot
9 -- Exit
Please input [1-9]: 7

Input destination IP address: 192.168.0.100
PING 192.168.0.100 (192.168.0.100): 56 data bytes

--- 192.168.0.100 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
```

図 4-10 ネットワーク疎通確認（疎通失敗）

VPN Beagleを再起動したい場合

VPN Beagleを再起動する場合、管理メニューにて8を入力します。

再起動してよいか確認を求められますので、よろしければyを入力してください。

VPN Beagle は再起動されます。

```
Login: admin
Password:

1 -- Initialize configuration
2 -- Change WEB UI password
3 -- Change network setting
4 -- Change local network setting
5 -- Clear allow IP address list
6 -- Show network setting
7 -- Execute ping
8 -- Reboot
9 -- Exit
Please input [1-9]: 8

Do you want to reboot the system?[y/n]:y

Please wait for system rebooting...
```

図 4-11 VPN Beagle の再起動

コンソール管理メニューを終了したい場合

コンソール管理メニューを終了する場合、管理メニューにて9を入力します。ただちにコンソール管理メニューは終了し、ログインプロンプトが表示されます。

```
Login: admin
Password:

1 -- Initialize configuration
2 -- Change WEB UI password
3 -- Change network setting
4 -- Change local network setting
5 -- Clear allow IP address list
6 -- Show network setting
7 -- Execute ping
8 -- Reboot
9 -- Exit
Please input [1-9]: 9

Login:
```

図 4-12 コンソール管理メニューの終了

付録 A、仕様

VPN Beagle	
対応ネットワーク構成	ゲートウェイ型
暗号化方式 / 暗号 / 認証	SSLv3 / TLSv1
	HMAC-SHA1 160bit
VPN クライアント数	無制限
アカウント管理	有効期限設定、接続有効／無効制御
	アカウント一括インポート／エクスポート機能
VPN管理機能	同時接続数制限
	クライアント間通信制限
	現在の接続状況確認
	接続履歴確認
その他機能	設定ファイルのバックアップ／リストア
	ファームウェアアップデート機能
ネットワークインターフェイス	1000BASE-T (4ポート) ※ 1
使用電源	AC100V ± 10V (50 / 60Hz)
平均電力消費量	30W
寸法	単体：44.45(H) × 200(W) × 350(D)mm
	ラックマウントキット：44.45(H) × 441(W) × 350(D)mm ※ 2
質量	3kg ラックマウントキット 2kg
付属品	電源ケーブル、VPN Beagle 専用ラックマウントキット、VPN Beagle 操作マニュアル

※ 1 LAN 3、LAN4 は使用しません。

※ 2 1/4U サーバーをラッキングする際は、付属のラックマウントキットが必要です。

メモ

付録

メモ

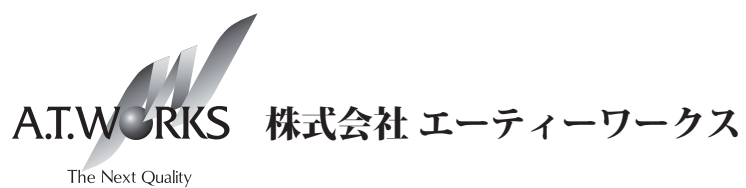
付録

VPN Beagle Center Model 200 操作マニュアル

2012年6月1日（第1版）

株式会社 エーティーワークス

東京本社：〒106-6137
東京都港区六本木6丁目10番1号 六本木ヒルズ森タワー 37階
富山本社：〒930-0856
富山県富山市牛島新町4号5番 エーティーワークス本社ビル
TEL：0120-0-41414
E-Mail：query@atworks.co.jp
<http://www.atworks.co.jp>
<http://online.atworks.co.jp>（オンラインショップページ）
<http://www.at-link.ad.jp>（at+link 専用サーバサービス）



The Next Quality

Copyright © A.T.WORKS, Inc. All rights reserved.