

# UT-VPN ブリッジ構築手順

2013/03/24

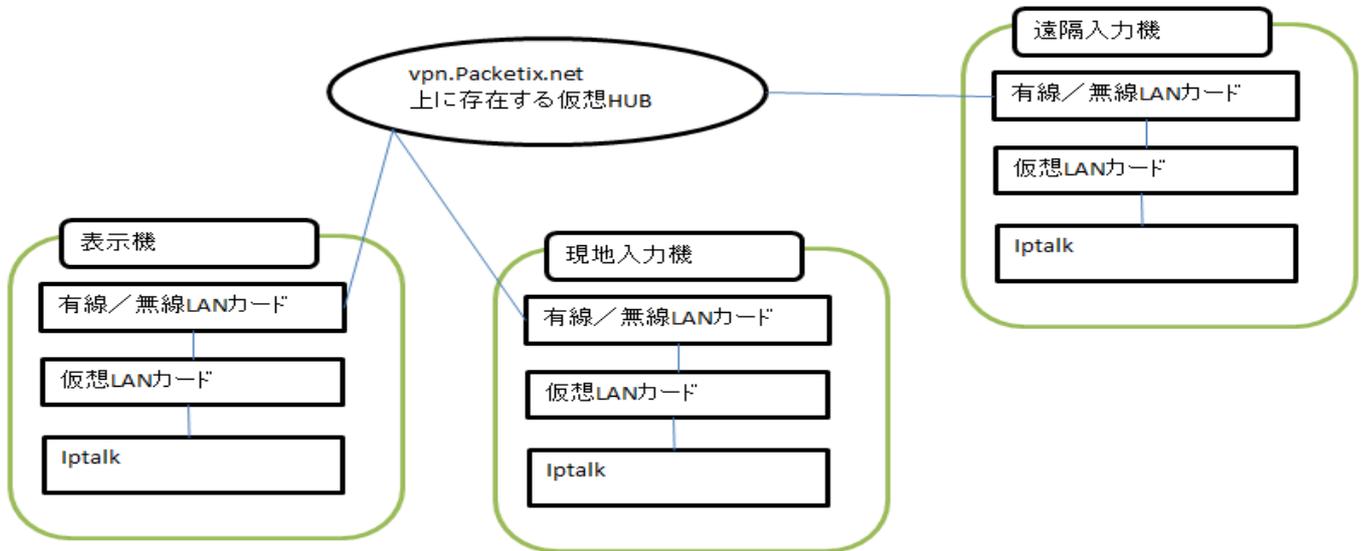
Ver1.1

大阪キャプショナーズ 米田

はじめに

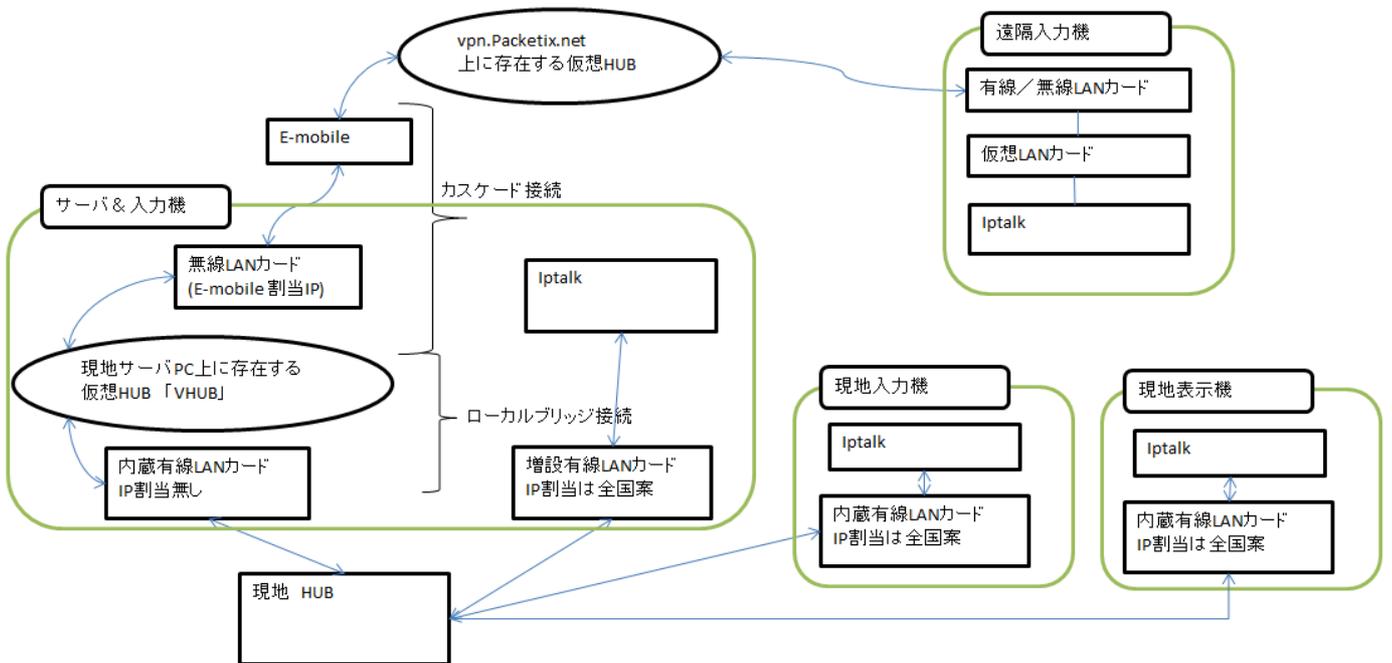
聴覚障害者向けの情報保障に遠隔入力導入されているが、現在の方法では、現地インターネット通信環境によっては不安定となることがある。

・現状（各 PC が個別に接続）



各 PC が個別で接続しているため、表示機の通信不良発生時は、情報保障が停止する。

・今回推奨する方法（ブリッジ接続）



現地 PC は HUB で接続しているため、インターネット通信不良発生時でも、現地 HUB 内だけで入力と表示が継続できるため、情報保障は停止しない。

## 事前準備 1 (機材とソフトの確認)

- ・遠隔入力機

インターネット接続環境、Skype、ヘッドセット、IpTalk PacketiX VPN Client 2.0", バージョン 2.20 ビルド 5280)

<http://www.softether.co.jp/jp/download/>

- ・現地入力機 (通常の字幕現場と同じであり今回説明無し)

ローカル LAN 接続環境、IpTalk

- ・現地サーバ&入力機 (今回説明)

インターネット接続環境、ローカル LAN 接続環境、USB-LAN 変換器 IpTalk、Skype、USB-音声変換、マイク、イヤホン、USB-HUB UT-VPN Server Version 1.01 Build7101 (64ビット/32ビット)

<http://utvpn.tsukuba.ac.jp/ja/download/>

☆ 現地サーバは1台だけ設定します。2台以上同じ接続を設定するとパケットがループしてしまうため、絶対に行わないで下さい。

## 事前準備 2 (仮想 HUB の作成)

ソフトイーサ株式会社の実験用オンラインサービス PacketiX.NET で自分たちが利用する仮想 HUB を構築する。

<http://www.packetix.net/jp/Default.aspx>

にある、「仮想 HUB の新規作成」をクリックして、規約の同意の後仮想 HUB 名とパスワード、連絡先メールを入れると構築できます。

ユーザの管理で、仮想 HUB にログインできるメンバーを設定します。

- ・ユーザは、遠隔入力者全てと、ブリッジ接続者の1名分が必須です。

認証方式は統一します。遠隔入力者には個別にパスワードを通知要

- ・仮想 DHCP は使わないので、無効に設定します

- ・仮想 HUB 管理パスワードは、忘れないようメモをおすすめします。

- ・IP アドレスは、全国案、独自割当でも網内で統一すれば問題ありません。

事前準備 3 設定項目が多いため、リストを作成します。

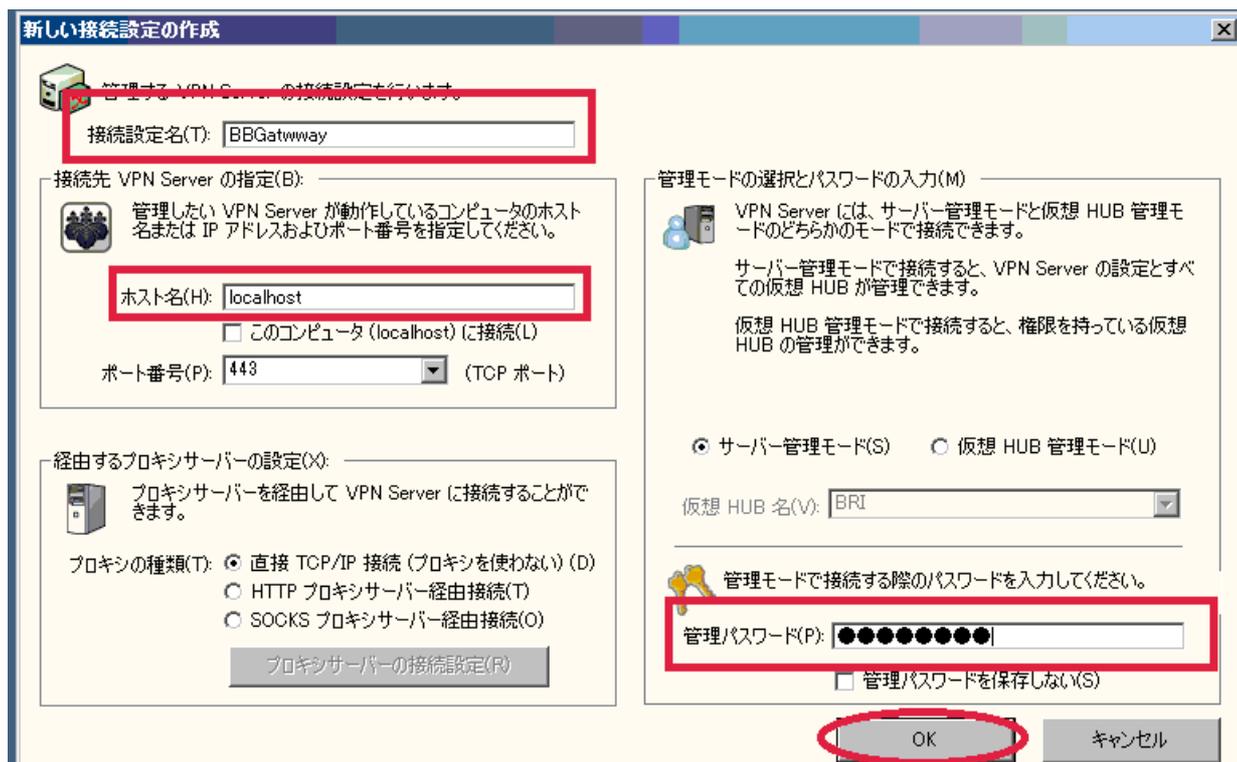
番号	内容	今回の設定例
A1	今回の全体設定の名前	BBGateway
A2	今回の全体設定用パスワード	(非公開)
A3	コンピュータ管理権限用パスワード	(非公開)
B1	事前準備 2 で Packetix.net 上に作成した仮想 HUB の名前	O-CAP
B2	事前準備 2 で Packetix.net 上に作成した仮想 HUB のユーザ名	OCAPUSER01
B3	事前準備 2 で Packetix.net 上に作成した仮想 HUB のユーザログイン方法	標準パスワード方式
B4	事前準備 2 で Packetix.net 上に作成した仮想 HUB のユーザのパスワード	(非公開)
C1	サーバ機で動作する仮想 HUB の名前	VHUB
C2	サーバ機で動作する仮想 HUB の管理パスワード	(非公開)
C3	サーバ機で動作する仮想 HUB のユーザ名	hoge1
C4	サーバ機で動作する仮想 HUB のユーザのログイン方法	匿名認証
C5	サーバ機で動作する仮想 HUB のユーザのパスワード	(匿名なので無し)
C6	仮想 HUB 間カスケード接続名	VPN-HUB
C7	パソコン本体有線 LAN アダプタ名	Atheros AP8131

## 事前準備 4 (UT-VPN Server 設定)

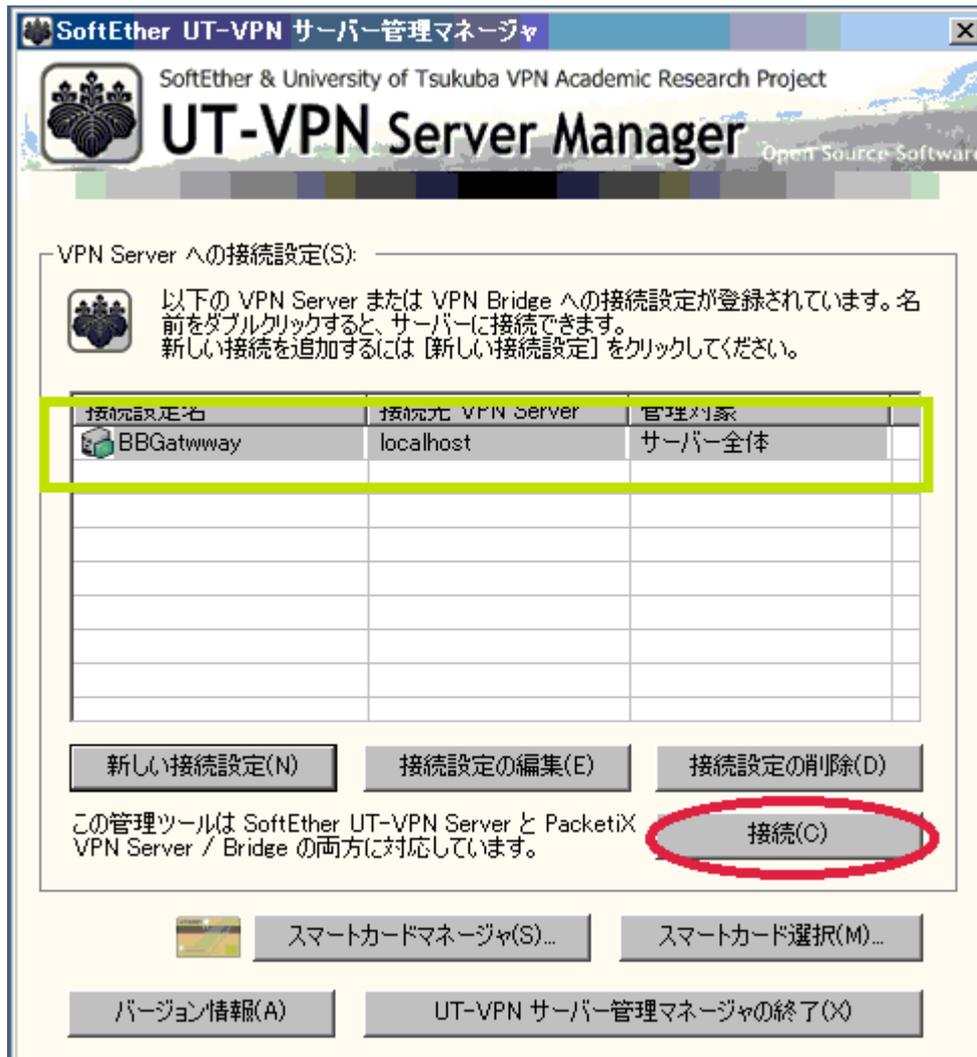
1) 管理者権限で UT-VPN Server を起動し、「新しい接続設定」をクリックする。



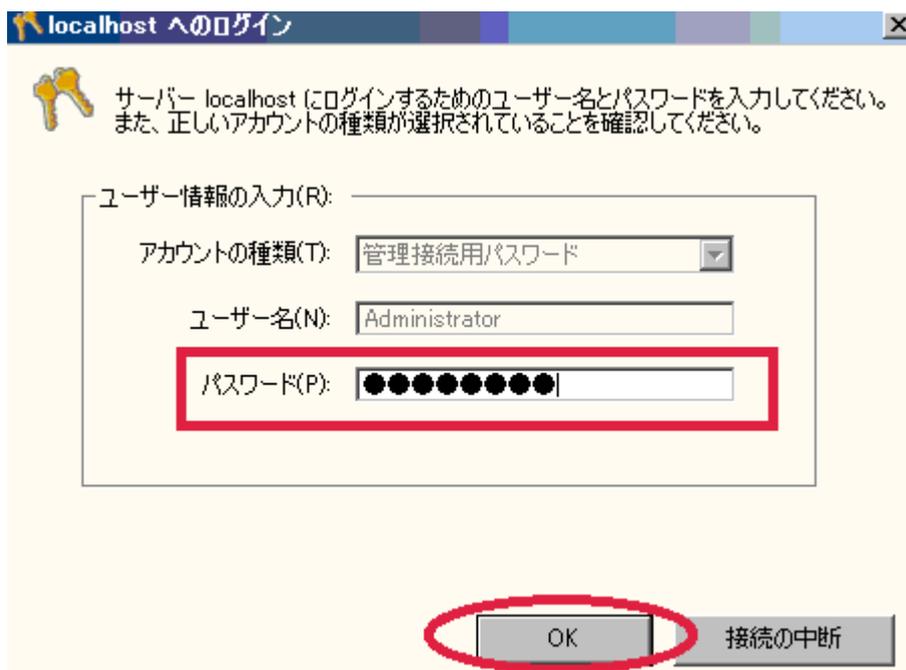
2) 接続設定名に A1、ホスト名「Localhost」、管理パス A2 を設定し、OK をクリック



3) 接続設定が新規作成されるので、「接続」をクリック



4) 管理者権限のパスワード A3 を入力して「OK」をクリック



## 5) 「仮想 HUB の作成」 をクリック

VPN Server "localhost" の管理

このサーバーがホストしている仮想 HUB (Z):

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
BRI	オフライン	スタンドアロン	0	0	0	0	0
BRIDGE	オフライン	スタンドアロン	4	0	0	0	0
DEFAULT	オフライン	スタンドアロン	0	0	0	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 5555	動作中

新規作成(R)   削除(T)   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(E)   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)  
この VPN Server に関する情報(B)   TCP/IP コネクション一覧の表示(Y)  
Config 編集(D)

ローカルブリッジ設定(B)   レイヤ 3 スイッチ設定(S)   最新の状態に更新(H)   閉じる(X)

## 6) 仮想 HUB 名 C1、管理パス C2 を入力し 「OK」 をクリック

仮想 HUB の新規作成

仮想 HUB 名(N): VHUB

セキュリティ設定(S):  
この仮想 HUB の管理用パスワード  
パスワード(P): ●●●●●●●●  
確認入力(C): ●●●●●●●●  
 匿名ユーザーに対してこの仮想 HUB を列挙しない(U)

仮想 HUB の状態(J):  
仮想 HUB の状態を選択してください。  
 オンライン(E)    **オフライン(F)**

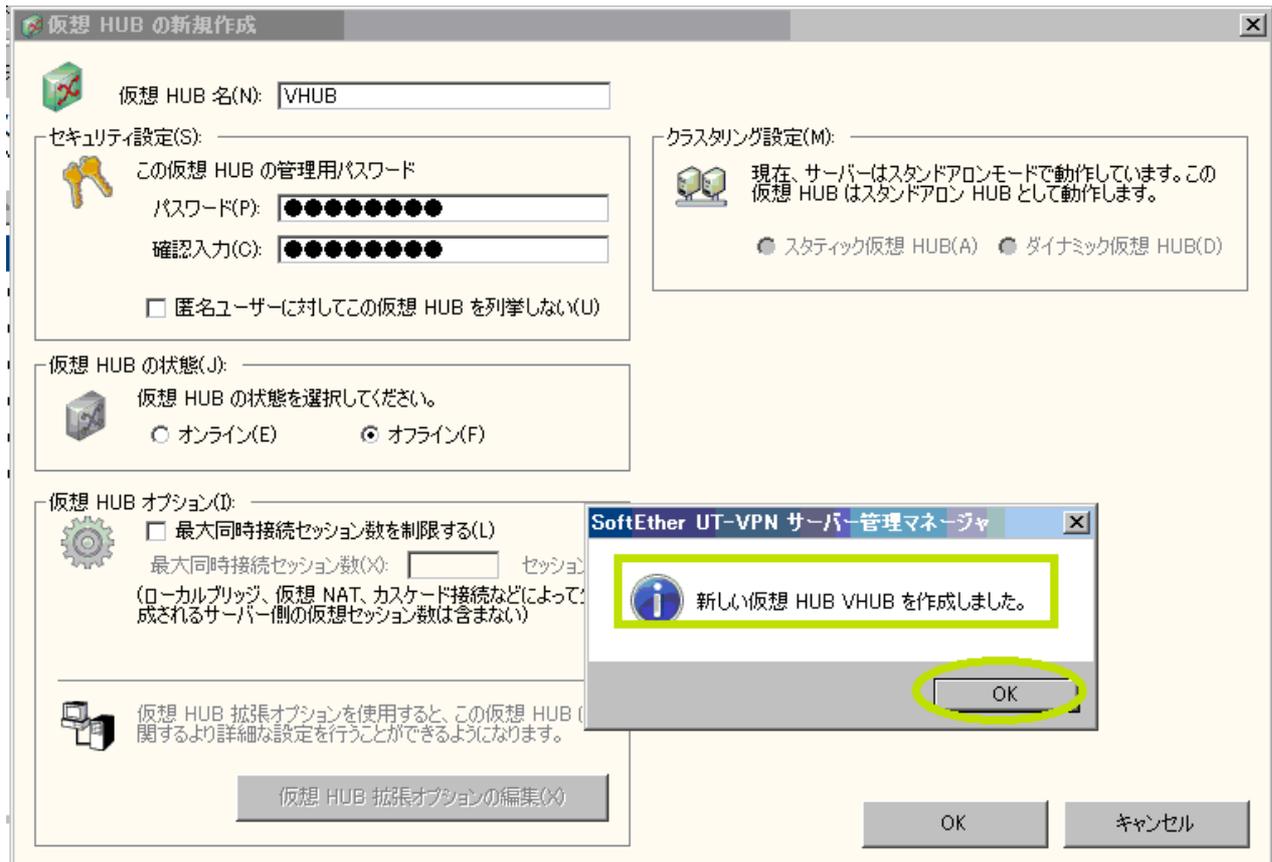
仮想 HUB オプション(O):  
 最大同時接続セッション数を制限する(L)  
最大同時接続セッション数(X):      セッション  
(ローカルブリッジ、仮想 NAT、カスケード接続などによって生成されるサーバー側の仮想セッション数は含まない)

仮想 HUB 拡張オプションを使用すると、この仮想 HUB に関するより詳細な設定を行うことができます。  
仮想 HUB 拡張オプションの編集(X)

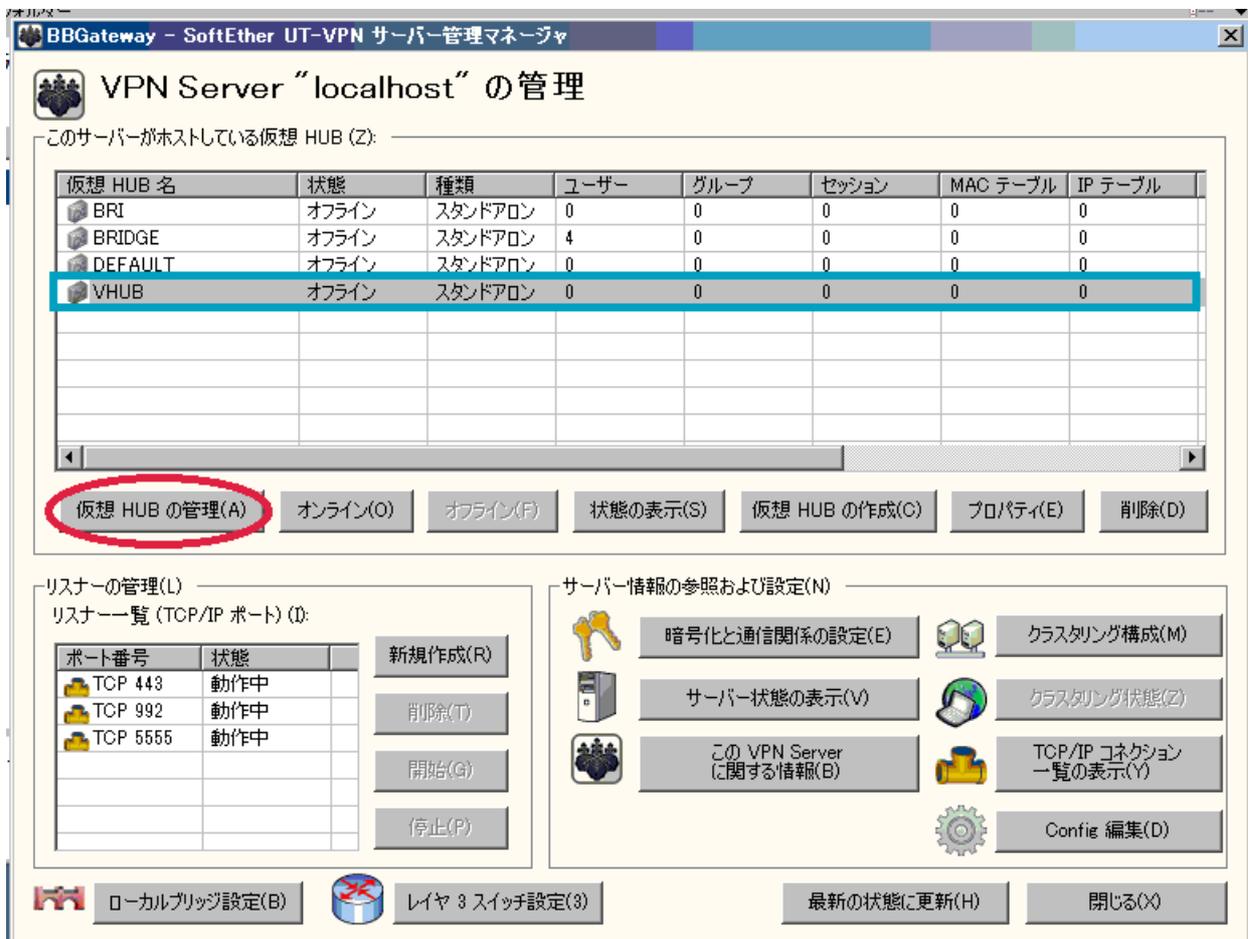
クラスタリング設定(M):  
現在、サーバーはスタンドアロンモードで動作しています。この仮想 HUB はスタンドアロン HUB として動作します。  
 スタティック仮想 HUB(A)    ダイナミック仮想 HUB(D)

OK   キャンセル

7) サーバ機での仮想 HUB 作成を確認し、「OK」をクリック



8) 作成した HUB を選択し、「仮想 HUB の管理」をクリック





1 1) ユーザ名 C3 と認証方式 C4 を設定し「OK」をクリック

ユーザーの新規作成

ユーザー名(U): hoge1  
本名(R): テストユーザ1  
説明(N): test1

グループ名 (省略可能):  
このアカウントの有効期限を設定する(S)  
2013年 3月 9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(W):

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(Y) 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  
固有証明書認証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予め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 F)

OK キャンセル

1 2) ユーザの作成を確認し、「OK」をクリック

ユーザーの新規作成

ユーザー名(U): hoge1  
本名(R): テストユーザ1  
説明(N): test1

グループ名 (省略可能):  
このアカウントの有効期限を設定する(S)  
2013年 3月 9日

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(W):

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(Y) 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  
固有証明書認証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予め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 F)

SoftEther UT-VPN サーバー管理マネージャ  
ユーザー hoge1 を作成しました。  
OK

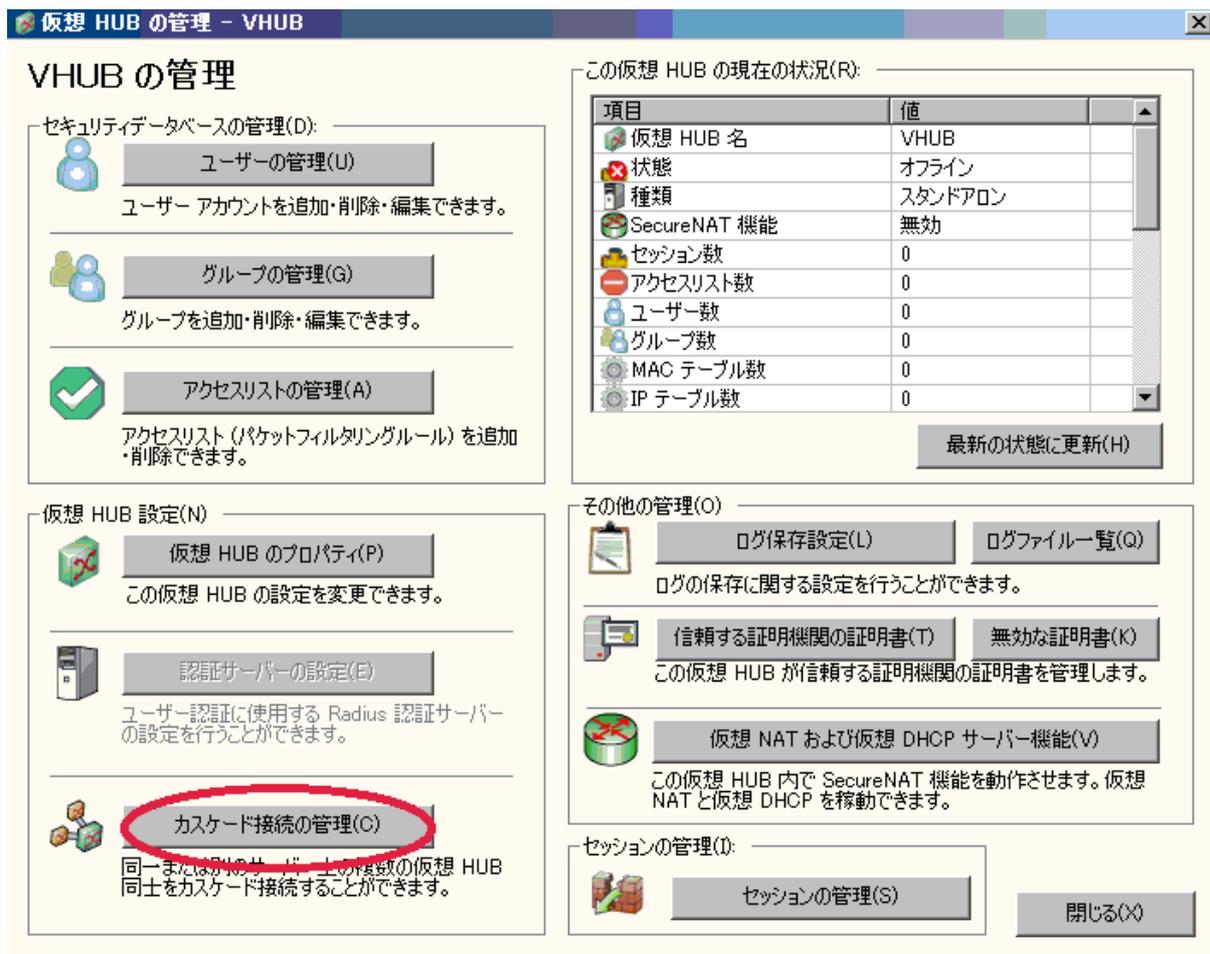
OK キャンセル

1 3) 今回は特に使わないが、5名程度作成し、「閉じる」をクリック



Vpn.packetix.net が停止している際に利用することがある。

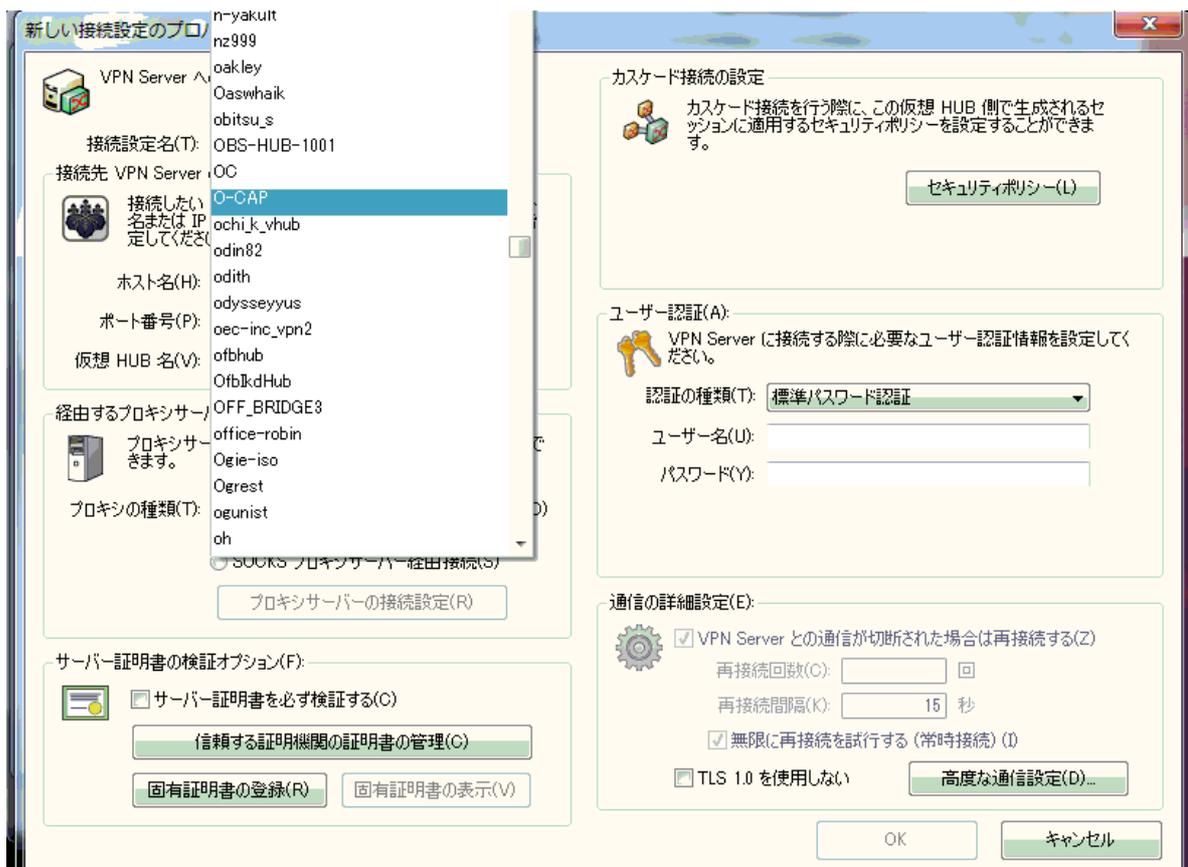
1 4) 「カスケード接続の管理」をクリック



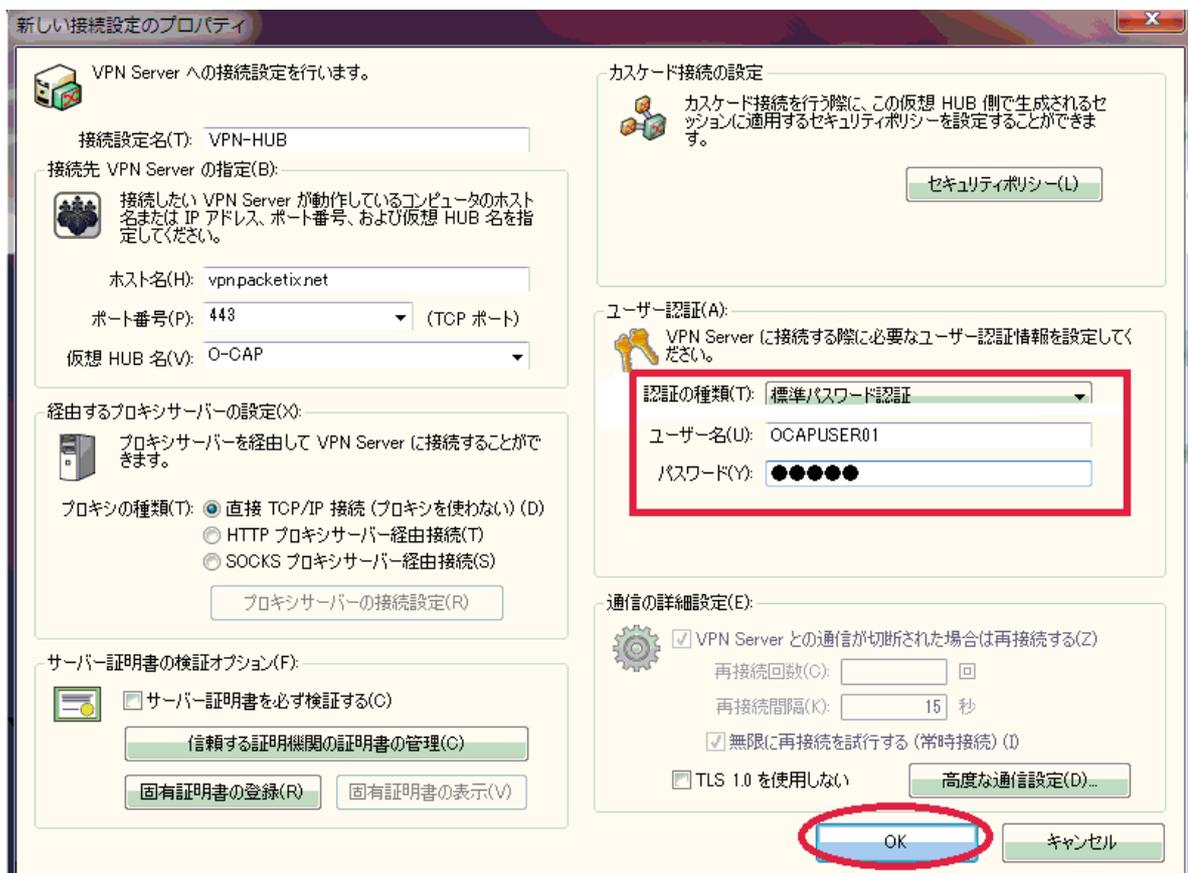
カスケードサーバ機上の仮想 HUB と VPN.packetix.net の仮想 HUB を相互接続する操作となる。



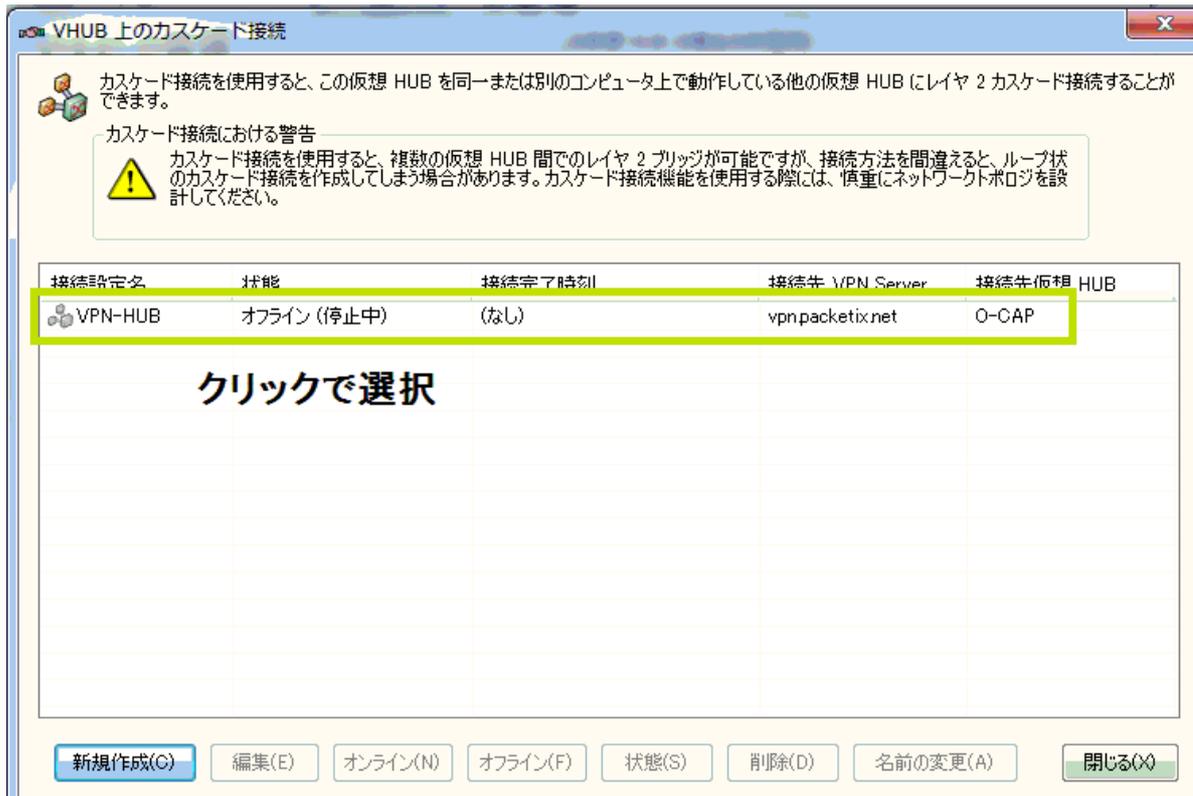
1 7) 一覧が列举されるので、B1 を探して選択。



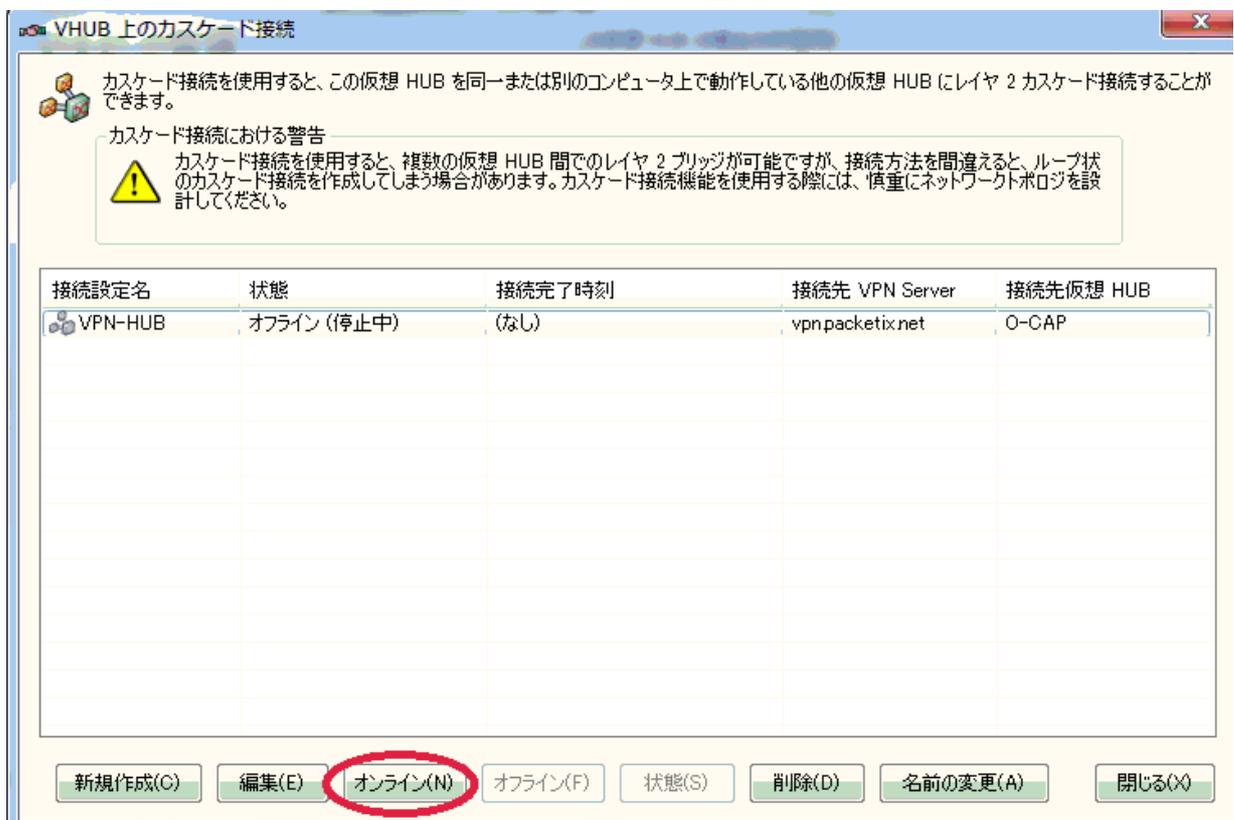
1 8) ユーザ名 B2,認証方法 B3,パスワード B4 を入力し  
「OK」をクリック



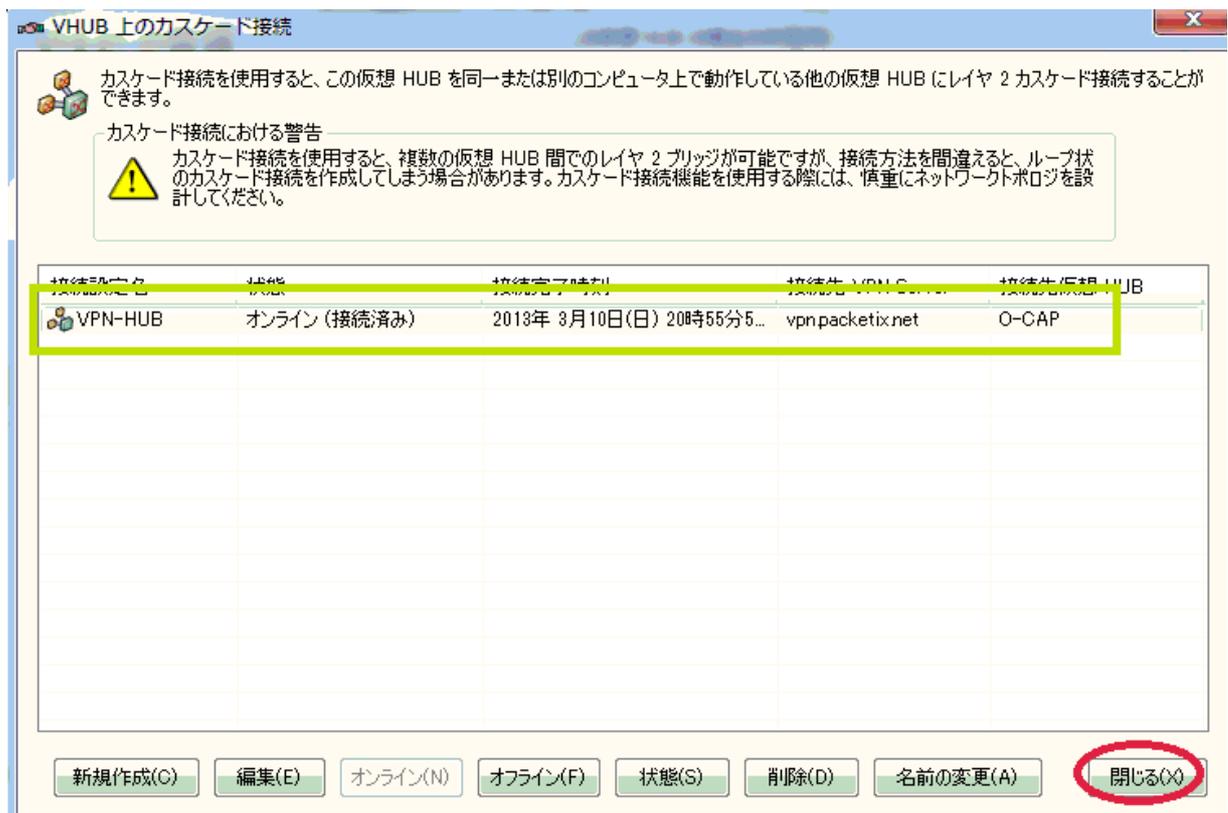
## 1 9) 仮想 HUB が新規作成されたことを確認しクリックで選択



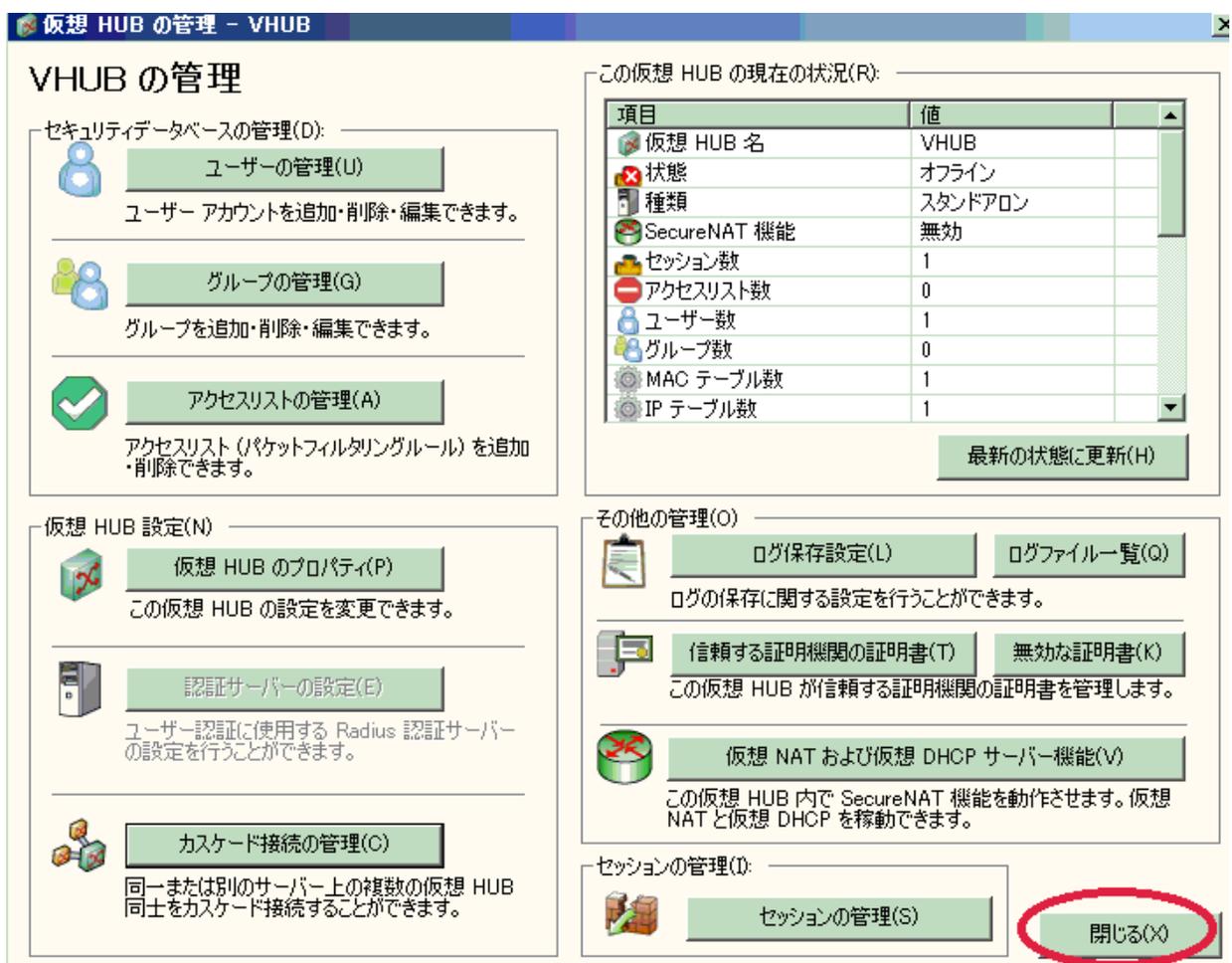
## 2 0) 「オンライン」をクリック



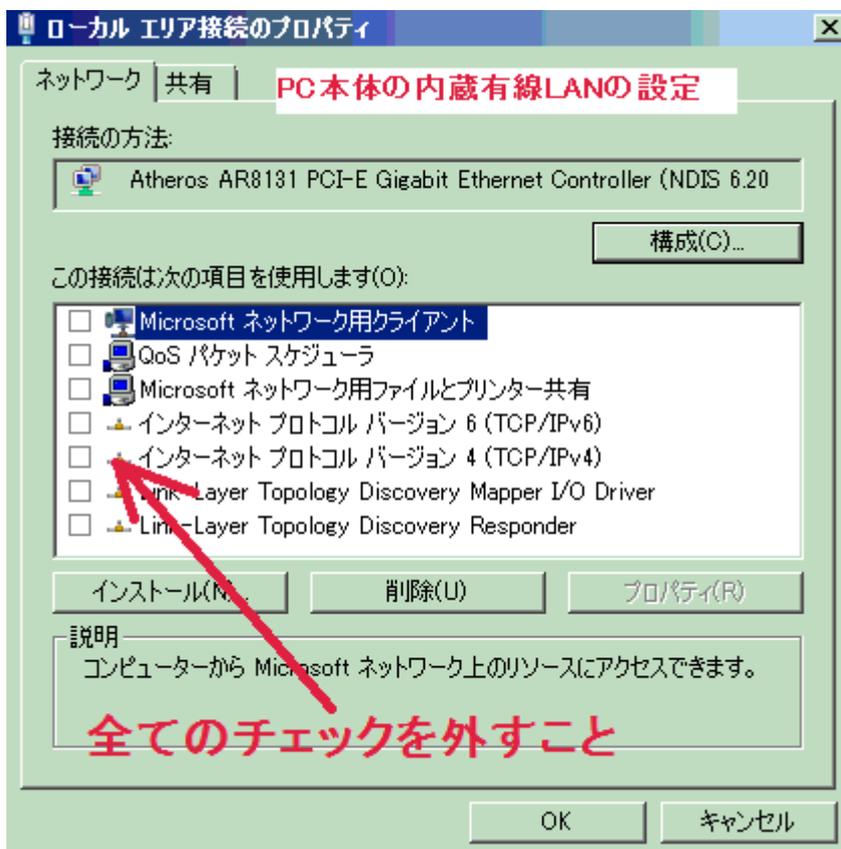
- 2 1) 「オンライン (接続済み)」を確認し「閉じる」をクリック  
 オンラインにならない場合、B2,B3,B4 が正しいか確認する。



- 2 2) 仮想 HUB の管理画面に戻るので「閉じる」をクリック



23) この時点で、コントロールパネルからローカルブリッジ接続用の LAN アダプタ C7 (サーバ機内蔵有線 LAN) のプロパティを変更する。  
(全てのバインドを外す)



(説明) パソコン内部で稼働している仮想 HUB と現地の HUB を物理的に接続する際、IP アドレスは不要であるため。

逆に、この有線 LAN カードに IP アドレスを設定すると、パケットが二重に送信されるため、IpTalk では、送信した文字が二重に表示される不具合が発生する。

(表示部、連絡窓、8人モニタが二重表示となる)

24) 「ローカルブリッジの設定」をクリックする。

25) 仮想 HUB 名 C1, LAN カード C7 を選択し  
「ローカルブリッジを追加」をクリック

## 26) 「注意書き」を確認し、「OK」をクリックする。

ローカルブリッジ設定

ローカルブリッジを使用すると、この VPN Server 上で動作する仮想 HUB と物理的な Ethernet デバイス (LAN カード) との間でレイヤ 2 ブリッジ接続を構成することができます。  
また、システムに tap デバイス (仮想のネットワークインターフェイス) を作成し、仮想 HUB との間でブリッジ接続することもできます。(Linux 版のみサポート)

番号	仮想 HUB 名	ブリッジ先 LAN カードまたは tap デバイス名	状態
1	VHUB	Atheros L1C PCI-E Ethernet Controller	動作中

SoftEther UT-VPN サーバー管理マネージャ

**i** 物理的な LAN カードに対してブリッジを行う場合、新しいブリッジ接続を作成した直後の状態では、一部の LAN カードでは仮想ネットワーク内のコンピュータからブリッジ接続に使用している LAN カード自身に対する TCP/IP 通信が正しく行えない場合があります。(特に、Intel や Broadcom 製 LAN カードなどでこの現象が発生する場合があります。)

その場合は、一度 VPN Server / Bridge が動作しているコンピュータを再起動してください。コンピュータの再起動後に正しく通信できるようになります。

また、大半の無線 LAN アダプタはプロミスキャスモードでのパケットの送受信に対応していない場合が多いため、ローカルブリッジに使用できない場合があります。このような場合は、無線 LAN アダプタではなく通常の LAN カードの使用を検討してください。

OK

※ 稼働中の任意の LAN カードとの間でブリッジできますが、高負荷環境においてはブリッジ専用 LAN カードを用意することをお勧めします。

ローカルブリッジを追加(A)

ローカルブリッジの設定は、VPN Server ごとに個別に定義されます。クラスタリング環境での他のクラスタメンバサーバーへは影響しません。

閉じる(X)

## 27) 動作中になったことを確認し「閉じる」をクリック

ローカルブリッジ設定

ローカルブリッジを使用すると、この VPN Server 上で動作する仮想 HUB と物理的な Ethernet デバイス (LAN カード) との間でレイヤ 2 ブリッジ接続を構成することができます。  
また、システムに tap デバイス (仮想のネットワークインターフェイス) を作成し、仮想 HUB との間でブリッジ接続することもできます。(Linux 版のみサポート)

番号	仮想 HUB 名	ブリッジ先 LAN カードまたは tap デバイス名	状態
1	VHUB	Atheros L1C PCI-E Ethernet Controller	動作中

タグ VLAN / パケット透過設定ツール(G)

ローカルブリッジの削除(D)

新しいローカルブリッジの定義(N):

ブリッジする仮想 HUB を選択するか、名前を入力してください。

仮想 HUB(H):

ブリッジ先の Ethernet デバイス (LAN カード) を選択してください。

LAN カード(L): ローカル エリア接続 [Atheros L1C PCI-E Ethernet Controller]

※ 稼働中の任意の LAN カードとの間でブリッジできますが、高負荷環境においてはブリッジ専用 LAN カードを用意することをお勧めします。

ローカルブリッジを追加(A)

ローカルブリッジの設定は、VPN Server ごとに個別に定義されます。クラスタリング環境での他のクラスタメンバサーバーへは影響しません。

閉じる(X)

## 28) 仮想 HUB C1 を選択し、オンラインをクリック

VPN Server "localhost" の管理

このサーバーがホストしている仮想 HUB (Z):

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
BRIDGE	オフライン	スタンドアロン	4	0	0	0	0
DEFAULT	オフライン	スタンドアロン	0	0	0	0	0
VHUB	オフライン	スタンドアロン	1	0	0	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 5555	動作中

新規作成(R) 削除(T) 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(E) 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)  
この VPN Server に関する情報(B) TCP/IP コネクション一覧の表示(Y)  
Config 編集(D)

ローカルブリッジ設定(B) レイヤ 3 スイッチ設定(3) 最新の状態に更新(H) 閉じる(X)

## 29) オンラインを確認し、サーバ管理マネージャーを閉じる

VPN Server "localhost" の管理

このサーバーがホストしている仮想 HUB (Z):

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
BRI	オフライン	スタンドアロン	0	0	0	0	0
BRIDGE	オフライン	スタンドアロン	4	0	0	0	0
DEFAULT	オフライン	スタンドアロン	0	0	0	0	0
VHUB	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 5555	動作中

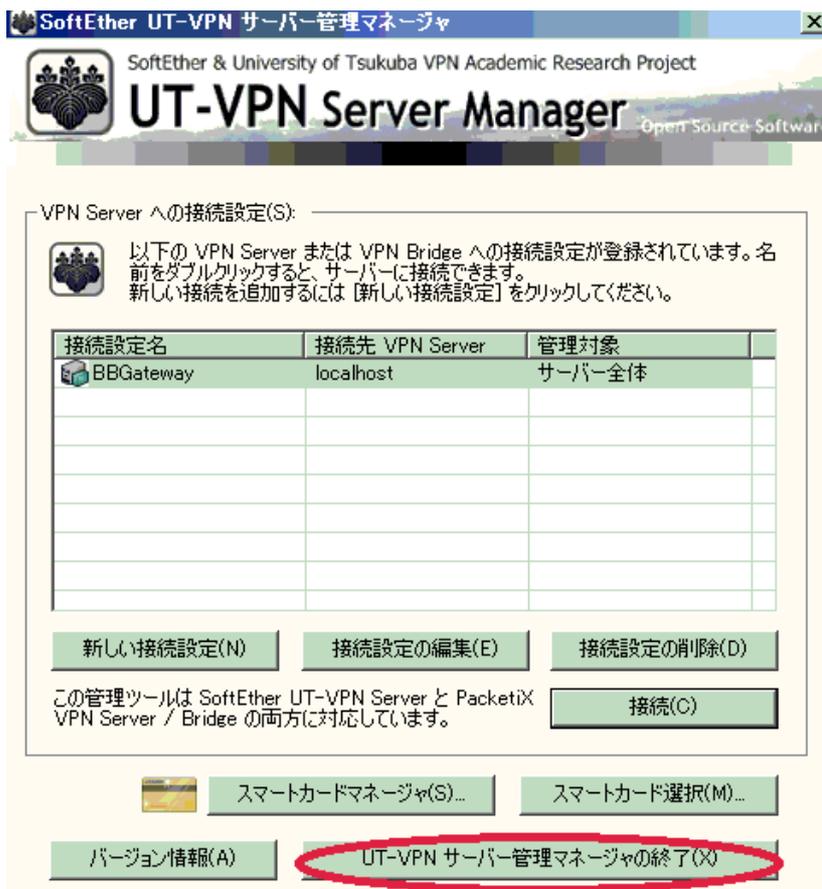
新規作成(R) 削除(T) 開始(G) 停止(P)

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(E) 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)  
この VPN Server に関する情報(B) TCP/IP コネクション一覧の表示(Y)  
Config 編集(D)

ローカルブリッジ設定(B) レイヤ 3 スイッチ設定(3) 最新の状態に更新(H) **閉じる(X)**

### 30) VPN サーバマネージャを閉じる

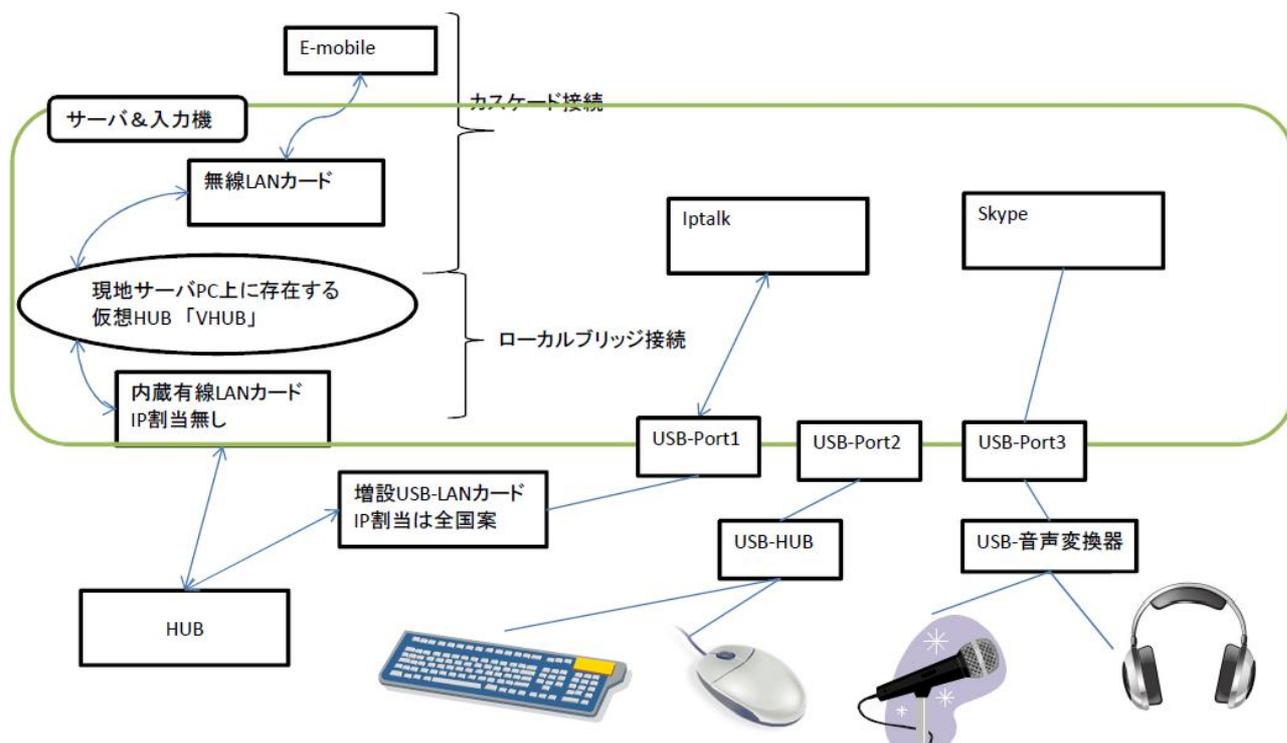


以上の操作により、vpn.packetix.net の仮想 HUB に接続した遠隔入力機と現地 HUB の入力機・表示機が同一ネットに繋がります。

停止時は、仮想 HUB のカスケード接続、ローカルブリッジ接続を共に停止してください。一度設定が完了したら、次からは

- vpn.packetix.net 上の仮想 HUB へのカスケード接続  
(手順 14, 20、21 参照)
  - サーバ機上の仮想 HUB のオンライン化  
(手順 28 参照)
  - ローカルブリッジの動作確認
- で動作します。

## サーバ&入力機 最終形態



### ・ vpn.packetix.net 停止時の対応について

このサービスは、無償実験ネットであるため、softEther 社の都合による停止がまれにあります。この時の対応は、現地仮想 HUB をネットに公開することで対応できます。

- ・ サーバ PC の無線 LAN の IP アドレスを調査する。
- ・ 調査した IP を元に、無線 LAN を自動設定ではなく固定 IP にする。
- ・ e-mobile にログインし、静的 IP マスカレードを設定する。

グローバル→無線 LAN IP アドレス TCP/UDP ポート 443

- ・ サーバ PC のグローバル IP アドレスを調査し、遠隔入力者に通知

<http://www.ugtop.com/spill.shtml>

- ・ サーバへのログイン方法は、C3,C4,C5 を通知する。

### ★ UT-VPN の今後のアップデートについて ★

UT-VPNは、今後 SoftEther プロジェクトに移行されます。

SoftEther VPN 1.0 (フリーウェア)

現状は英語版のみです。 <http://www.softether.org/>

## 改変履歴

2013/3/23 ver 1.0 初版作成

2013/3/24 ver1.1 語句訂正 paketix→packetix

32bit 版対応と今後の対応を追記