PacketiX Desktop VPN

PacketiX Desktop VPN



目次



■ PacketiX Desktop VPNとは

- サービス概要
- サービス特長
- 利用シーン
- ライセンス体系
- 動作環境
- お申し込み・お問い合わせ
- フリートライアル
- Appendix

PacketiX Desktop VPNとは



PacketiX Desktop VPNはSaaS型セキュリティサービスとして提供する、極めて簡単かつ 安全なリモートアクセスサービスです。インターネットに接続されているコンピュータであれ ば、離れた所にあるコンピュータに対してどこからでも接続でき、全ての通信がSSL-VPN により強力に暗号化されます。



※企業内端末に接続する際は、セキュリティポリシー上問題がないことを管理者にご確認のうえ、ご利用下さい。

こんな方におすすめ!



こんな問題に心当たりは・・・

- 出産や育児で離職中の従業員、通勤が難しい人材の活用や、IT管理者など社内の 専門職の在宅勤務を可能にしたい。
- 外出の多い営業やフィールドエンジニア、出張しがちな経営者が外出先から社内データ

や社内メールを活用したい。

- 営業所など、本社との専用回線がない環境でも、データを安全にやりとりしたい。
- 遠隔地にある店舗の業務用PCのメンテナンスや保守を本社から行いたい。



PacketiX Desktop VPNを導入して・・・

●強固なSSL暗号技術によるハイレベルなセキュリティ環境を提供
●接続元と接続先のPCにアプリケーションをインストールするだけ
●自社システムの構築や、高度なIT技術・運用の知識は不要
●シンクライアント・ライクな利用形態を実現

サービス概要



~いつでも、どこでも、必要なときに、

インターネット経由でオフィスや自宅のPCを遠隔操作!~

PacketiX Desktop VPNは、極めて簡単かつ安全なリモートアクセスサービスです!

遠隔地にあるPCでも、インターネットに接続されていれば、 どこからでもアクセス可能。 シンクライアント・ライクなテレワーク環境を低コストで実現できます。

すべての通信はSSL-VPN^{*}で強力に暗号化されているので、 安全にご利用いただけます。

【サービス価格】

1ライセンス:月額900円/年額10,800円(税抜)
 初期費用:なし
 最低契約数:1ライセンス~
 最低契約期間:1ヶ月
 年額一括払い:可

※1)SSL-VPN: Secure Sockets Layer - Virtual Private Network インターネットを介したリモートアクセス向けのVPN技術で、通信のプロトコルに、「通信内容の暗号化」「サーバ認証」「クライアント 証」という3つの機能を提供するSSL(Secure Socket Layer)を使用する仕組み。





1. ハイレベルなセキュリティ環境

- リモートアクセスの通信プロトコルをRSA1024bitで暗号化されたSSL-VPNトンネル内に流すことにより、強力な暗号化を実現
- リモートデスクトップ機能を使用しているため、編集するファイルをコピーする必要はなく、 ウィルスや情報漏えいの危険性を抑えることが可能

Desktop VPNのセキュアリ	リモート接続	
自宅や出張先など していた。 していた	インターネット Pp VPN 時代遺信 ファイアー ウォール	社内ネットワークなど
悪意の 第三	53 8	



2. 簡単設定で手間いらず

■ 接続元と接続先のPCにアプリケーションをインストールするだけ

■ 既存のネットワーク環境の設定変更が不要



STEP1 Desktop VPN Client DesktopVPNのクライアントソフトを起動し 接続先の「コンピュータID」を指定します。 BRELKS-SD HRS Auto BELANU ANDED. TTUNG. STEP2 Disking VPN 9 - IC: NO BEDDERD 1 - 9 - 202 REAL DRAWN VIN 7-//- 'SHILL'CE2-7-EEECARC/07-PARK 接続先の「ユーザ認証バスワード」を 入力します。 1117-103 71 10.7-10. QK RVOMS STEP3 -b-ranketmin 接続先コンピュータのWindowsログイン 画面が表示されるのでログインします。 AND MARKE US -- > TAY -- SALDAMAN SHIELDAT. ※Microsoftのリモートデスクトップ機能がない 1-9-442 C OSの場合は表示されません 107-101 (R) (47/05) 接続完了 これで接続先のコンピューターに 接続先の画面 リモートアクセス完了! あたかもそのコンピューターを手元の コンピュータのように操作できます。 接続元の画面

簡単接続



3. シンクライアント・ライクな利用形態

■ クライアントPCからのキーボードとマウス入力をリモートPCに伝送し、実行結果の画面伝送を受けるのみ

■ 編集するファイルをダウンロードする必要もなく、比較的低スペックのPCをクライアントとして利用可能
 ● クライアントPCには、OSおよび PacketiX Desktop VPN クライアント以外のソフトウェアは不要。



※一部のソフトウェアは、リモートアクセス時の使用についてライセンス上の特記事項がある場合があり ます。詳細は各ソフトウェアのライセンス許諾条件をご確認下さい。



4. プリンタ・ディスクの共有が可能

■ リモートアクセス先のPC画面から、接続元PCのローカル・デバイス又はプリンタを使用することが可能

■ セキュリティーポリシーに従い、本機能を使用しない設定も可能



※セキュリティポリシーに従い、サーバ側で共有機能のON/OFFを設定することができます。



5. 強力・高度なセキュリティ対策機能を搭載

■ 不正アクセスを防止するため、さまざまなユーザ認証機能やアクセス制御機能を搭載

●高度なクライアント認証機能を搭載

ユーザ毎に以下の認証方式を選択でき、それぞれ接続できる有効期間を設定することも可能です。

	🗿 385-17-138888771422-5-18177688774.						
匿名認証	パスワードを必要とせず、ユーザ名のみで接続 2012年 2012年 100 100 100 100 100 100 100 100 100 10			600034084 600 600 600 600 600			
パスワード認証	ユーザ名に対して個別のパスワードを設定	D-am-1	3-4-4	WedowsF/HC/EEEE	NT POPULATE		lut.2
固有証明書認証	サーバ側で設定された特定の証明書と秘密鍵のペアを持つク	ライアン	ѵトのみ	⊁接続			
署名済み証明書認証	外部の認証機関の証明書を登録して、クライアントを認証						
Radius認証	外部のRadiusサーバを使用してクライアントを認証						
Windowsドメイン認証	外部のWindowsドメイン(NTドメイン、ActiveDirectoryドメイン)を使用してクライアントを認証						

●クライアントIPアドレスによるアクセス制御機能

特定のクライアントからの接続を制限したり、特定のクライアントのみ接続を許可するといった設定をすることで 、不正なアクセスをブロックできます。

●サーバ設定ツールの実行ユーザ制限
 接続先に複数のユーザが設定されている場合に、管理者以外のユーザによって設定が変更されてしまうことを防止できます。

●ログ出力機能

ファイルログの保存に加え、Windowsのイベントログへの出力、syslogサーバへの送信に対応しています。

利用シーン





「モバイルオフィス環境をセキュアに構築、 業務効率化と生産性の向上に貢献」

- ・外出の多い営業担当者が社内の見積作成システムに アクセスし見積書を作成。
- ・フィールドエンジニアが外出先から社内の顧客管理システムに アクセスし顧客情報を確認。
- ・経営者が出張先のホテルから社内メールを確認。



「低コストでテレワーク環境が構築でき、 中小企業のIT化推進インフラとして活用可能」

・出産や育児で離職中の従業員、通勤が難しい人材の活用などに。 ・営業所など本社との専用回線がない環境でのVPN回線として。 ・IT管理者など、社内の専門職の在宅勤務に。

※1つの接続先に複数のPCから同時にリモートアクセスはできません。



「遠隔地にある店舗の業務用PCに本社からリモートアクセスし、 日常のメンテナンスや保守を実施」

・IPアドレスの調査不要で接続作業が簡素化。

- ・プライベートIPアドレス環境でもアクセス可能。
- ・日本語入力・ファイル転送による利便性の向上。
- ・暗号化通信による安全性の向上。
- ・PCへの負荷が軽くスムーズな遠隔作業を実現。

ライセンス体系



●ライセンス体系

リモートアクセス先マシンに同時に1つのクライアントから接続するためのライセンスです。

- ・PacketiX Desktop VPNサーバソフトウェアをインストールするマシンごとにライセンスが 必要。
- •PacketiX Desktop VPNクライアントソフトウェアはライセンスフリー。
- ・PacketiX Desktop VPNサーバには「同時に」1つのクライアントからのみ接続可能。

●必要ライセンス数の計算方法







必要ライセンス数:1





動作環境



OS	下記対応OS一覧表を参照			
CPU	Intel Pentium以上のWindowsが動作するCPU [推奨:Intel Pentium2世代以降]			
メモリ	32MB以上[推奨:128MB]			
ハードディスク	32MB以上の空き容量			
モニタ	色数16ビット以上、解像度800×600以上			
インターネット	28.8Kbps以上のインターネットアクセス回線 [推奨:1.5Mbps以上のブロードバンドアクセス回線]			
接続環境	※通信における遅延が少なくスループットが高いほど快適にソフトウェアを使用いただけます。			
■対応OSー	覧表			
	システムモード/ユーザーモードともにインストール可能なOS			
Windows 2000 Server/Windows 2000 Advanced Server/				
	Windows XP Professional/Windows XP Professional x64 Edition/Windows XP Tablet PC Edition/Windows XP Tablet PC Edition 2005/ Windows XP Media Center Edition 2005/			
	Windows Server 2003 Standard Edition/Windows Server 2003 Standard x64 Edition/Windows Server 2003 Enterprise Edition/			
++バ	Windows Server 2003 Enterprise x64 Edition/Windows Server 2003 R2 Standard Edition/			
9-73	Windows Server 2003 R2 Standard Enterprise Edition/Windows Server 2003 R2 Standard Enterprise x64 Edition/			
	Windows Vista Business/Windows Vista Enterprise/Windows Vista Ultimate			
	ユーザーモードのみインストール可能なOS			
	Windows 2000 Professional Edition/Windows XP Home Edition/			
	Windows Vista Home Basic/Windows Vista Home Premium			
インストール可能なOS				
	Windows 2000 Professional/Windows 2000 Server/Windows 2000 Advanced Server/			
	Windows XP Professional/ Windows XP Professional x64 Edition/Windows XP Home Edition/Windows XP Tablet PC Edition/			
	Windows XP Tablet PC Edition 2005/Windows XP Media Center Edition 2004/Windows XP Media Center Edition 2005/			
クライアント	Windows Server 2003 Standard Edition/Windows Server 2003 Standard x64 Edition/Windows Server 2003 Enterprise Edition/			
	Windows Server 2003 Enterprise x64 Edition/Windows Server 2003 R2 Standard Edition/			
	Windows Server 2003 R2 Standard x64 Edition/Windows Server 2003 R2 Enterprise Edition/			
	Windows Server 2003 R2 Enterprise x64 Edition/			
	Windows Vista Home Basic/Windows Vista Home Premium/Windows Vista Business/Windows Vista Enterprise/Windows Vista Ultimate/			
※システムモード	·····································			

システムモード:遠隔操作にマイクロソフト社の「リモートデスクトップ接続」を内部的に用いるため、「リモートデスクトップ接続」で提供されるすべての機能が利用可能

ユーザーモード:「PacketiX Desktop VPN内蔵の代替機能による接続」を用います3。この場合、ディスクやプリンタなどデバイスの共有機能は利用不可

フリートライアル

まずはPacketiX Desktop VPNの <u>30日間無料お試しダウンロード</u>で、 リモートアクセスで実現される新たな世界をご体験ください

・本サービスと同じすべての機能が体験できます。
 ・インストール後、30日間ご利用頂けます。

※お試しダウンロードのお申し込みは不要です。 ※評価版にはインストーラ版と実行ファイル版がございます。





RAPPORT

Appendix



ユーザ認証機能①:匿名認証



■ 匿名認証はもっとも簡単なユーザ認証の方法です。匿名認証に設定されたユーザはパスワードを

必要とせずにユーザ名のみで PacketiX Desktop VPNサーバへ接続することができます。

匿名認証での接続を許可するユーザを作成するには、ユーザの設 定画面にて認証方法を「匿名認証」に設定します。

「ユーザー名」は接続時にクライアントで指定するユーザ名となります。 ユーザ管理上の付加情報として「本名」や「説明」を追加することもで きます。

ユーザが接続できる期間を設定する場合は、「このアカウントの有効 期限を設定する」にチェックを入れ、任意の日付を設定してください。



PacketiX Desktop VPNクライアントから高度なユーザ認証機能を設定したサーバへ接続すると、「ユーザー認証」ウィンドウが開きます。

匿名認証を設定したユーザーで認証するためには、「認証方法」を 「パスワード認証」に設定し、「ユーザー名」に設定したユーザ名を 入力し「OK」をクリックします。



レーザー認証

ユーザ認証機能②:パスワード認証



■ パスワード認証は、ユーザ名に対して個別のパスワードを設定することができます。

パスワード認証での接続を許可するユーザを作成するに は、ユーザの設定画面にて認証方法を「パスワード認証」 に設定します。

「ユーザー名」は接続時にクライアントで指定するユーザ名 となります。ユーザ管理上の付加情報として「本名」や「説 明」を追加することもできます。「パスワード認証」の欄で入 カしたパスワードがクライアント接続時に入力するパスワ ードとなります。

ユーザが接続できる期間を設定する場合は、「このアカウ ントの有効期限を設定する」にチェックを入れ、任意の日付 を設定してください。

📱 ユーザーの新規作成 8 ユーザー名(U): user-b **R** パスワード(P): ***************** 本名(B): ユーザーB パスワードの確認入力(ご): *********************** 説明(N): パスワード認証による認証 国有証明書認証1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 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 ▼このアカウントの有効期限を設定する(S) 將 2008年 3月22日 👽 0:00:00 マーザーの管理 このサーバーに変換されているユー 認証方法(A): 🕜 医交辺距 証明書の指定(E) 証明書の表示(V) 証明書作成ツール(W) 🔍 パスワード認証 (2) 固有前明書設計 署名済み証明書認証 ユーザー名 本品 ユーザーA 図署名済み証明書認証 クライアント証明書がこのサーバー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。 Radius 21 WINT ドメイン記録 □ 証明書の Common Name (CN) の値を限定する(B) 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 証がれます。 □ 証明まか:川アル素是の値を限定する(1) □ 認証サーバー上のユーザー名を指定する(K) ※ 16 進数で入力してください。(例: 0155ABCDEF) 認証サーバーにおけるユーザー名(W): OK キャンセル 新規的標準 編集(2) ユーザー保持表示(2) 第2時(2) 最新された(1)(三世時(2)) 開たる(2)

PacketiX Desktop VPNクライアントから高度なユー・	げ認
証機能を設定したサーバへ接続すると、「ユーザー語	忍証」
ウィンドウが開きます。	

パスワード認証を設定したユーザーで認証するためには、 「認証方法」を「パスワード認証」に設定し、「ユーザー名」 に設定したユーザー名を、「パスワード」に設定したパス ワードを入力し「OK」をクリックします。

	ューザー認証
sktop VPN クライアント (パーラョン 2.00) PacketiX Desktop VPN	Pesktop VPN サーバー "xp-pro" に接続するためには、ユーザー認証を行う必要があり ます。 認証方法を選択してから、ユーザー名を入力して、必要なデータを入力してください。 ユーザー名わよびユーザー認証方法
接続先コンピュータ D: xp-pro	認証方法(M): ④ パスワード認証(P) ○ 証明書認証(C)
	ユーザー名(U): user-b
	パスワード認証を使用する場合は、パスワードを入力して [OK] をク リックしてください。 パスワード(P): [********

4

ユーザ認証機能③-1:固有証明書認証



■ 固有証明書認証はユーザ名とパスワードではなく証明書を使って認証する方法です。 サーバ側で設定された特定の証明書と秘密鍵のペアを持つクライアントのみが接続できます。

固有証明書認証での接続を許可するユーザを作成す るには、ユーザの設定画面にて認証方法を「固有証明 書認証」に設定します。

「ユーザー名」は接続時にクライアントで指定するユー ザ名となります。ユーザ管理上の付加情報として「本 名」や「説明」を追加することもできます。

ユーザが接続できる期間を設定する場合は、「このアカ ウントの有効期限を設定する」にチェックを入れ、任意 の日付を設定してください。

次に「固有証明書認証」の登録をおこないます。既に 証明書と秘密鍵のペアを持っている場合、「証明書の 指定」から証明書ファイルを選択し設定することで、認 証に利用することができます。新規に証明書と秘密鍵 を作成するには、「固有証明書認証」の欄の「証明書作 成ツール」をクリックします。

証明書作成ツールで新しい証明書を作成するには、 「新しい証明書の作成」ウィンドウにて 証明書の種類 を「ルート証明書」に設定し、下の欄の各項目を入力 します。「OK」ボタンを押すとパスフレーズを入力する 画面が表示されるので、適当なパスフレーズを入力し 「OK」をクリックします。



名前 (Ch): 国政府書と保密意識の成功とみ() 福田県書と保密意識の成功とみ() 近辺府書と保密意識の成功とみ() 回「ホスルーズを建立する」でできます。「アンチャオー」のコーースを建する 名前 (Ch): யarre 加速の構成力を定 名前 (Ch): யarre 加速の構成力を定 方前 (Ch): யarre 加速の構成力を定 加速の構成力を定 のテンプ・サービス事業部 加速の構成力を定 面は何用きを(ST): 日本 の 和趣事性位(Gu): 日、 万プ・フ・サービス事業部 日 (S): 面は原作場(ST): 日本 日 (S): エー・	ました 能
名前 (ON) user-c ● 所腐個間 (0) 日本50時式会社 ● 縮準位 (00) コンテンツ・サービス事業部 ● 面 (2) 日本 ● 約返回風 (57) 東京都 ●	1
所居機関 (D): 日本SGI株式会社 組織単位 (DU): コンテンツ・サービス事業部 国 (C): 日本 総造枠県 GT): 東京都	穴电瓜
 細糖単位のい:コンテンツ・サービス事業部 国(な) 日本 約適研得(57) 庫克部 	
国 (C): 日本	
都道府県 (ST): 東京都	
ローカル (L): 洪谷区	
シリアル番号(5): 1 (1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(

ユーザ認証機能③-2:固有証明書認証



「証明書と秘密鍵を保存するファイル名を指定してくだ さい」というウィンドウが開いたら、証明書と秘密鍵の 含まれたファイル(PKCS#12ファイル)を適当な名前を 付けて保存します。PacketiX Desktop VPNクライアン トは このファイルを使用して認証を行いますので、保 存したファイルはPacketiX Desktop VPNクライアントの PCにコピーします。



PacketiX Desktop VPNクライアントから高度なユーザ 認証機能を設定したサーバへ接続すると、「ユーザー 認証」ウィンドウが開きます。

固有証明書認証を設定したユーザで認証するために は、認証方法を「証明書認証」に設定し、ユーザ名に PacketiX Desktop VPNサーバで設定したユーザー名 を入力します。「証明書ファイル」としてPacketiX Desktop VPNサーバからコピーしたファイル (PKCS#12ファイル)を指定し「OK」ボタンを押します。

「秘密鍵のパスフレーズ」ウィンドウが表示されたら、 PacketiX Desktop VPNサーバで証明書を作成した 際のパスフレーズを入力し、「OK」を押します。

ューザー認証	
Pesktop VPN サーバー "xp-pro" に接続するためには、ユーザー認証を行う必要があり 認証方法を選択してから、ユーザー名を入力して、必要なデータを入力してください。 ユーザー名もよびユーザー認証方法 認証方法を選択してから、ユーザー名を入力して、必要なデータを入力してください。 ユーザー名(い: ロッテー) ① 証明書認証(の) ユーザー名(い: ロッテー) ① 証明書認証(の) パスワード認証で パスワード認証を使用する場合は、パスワードを入力して [OK] をク リックしてください。 パスワード(P): 証明書認証 証明書認証を使用する場合は、「参照] をクリックして PKCS#12 形式の証明書フィイル、(p)2 または、p(x)を指定してください。	現在課題の代入フレーズ 図 単語課題の代表フレーズ 単語課題の代表フレーズによって発展されたのです。 単語課題の代表のためになった。 パスワレーズ(注入) パスワレーズ(注入) ①
C¥Documents and Settings¥hk-mizuno¥デスクト 参照(B)	

ユーザ認証機能④-1:署名済み証明書認証



■ 署名済み証明書認証では、外部の認証機関の証明書を登録することで、すでに発行されている 証明書を使用してクライアントを認証することができます。別途すでに証明書認証方式のシス テム

を運用している場合にクライアントごとに証明書を再発行する手間を省くことができます

PacketiX Desktop VPNサーバで署名済み証明書認 証を設定するには、まず外部の証明機関の証明書を 設定する必要があります。「セキュリティ設定」ウィンド ウから「信頼する証明機関の証明書」を選択します。





「信頼する証明書機関の証明書の管理」ウィンドウ が開いたら「追加」をクリックし、登録する証明書機 関の証明書を選択します。

ユーザ認証機能④-2:署名済み証明書認証



次に署名済み証明書認証での接続を許可するユーザを作成します。

署名済み証明書認証での接続を許可するユーザを作成するには、 ユーザの設定画面にて認証方法を「署名済み証明書認証」に設定 します。

「ユーザー名」は接続時にクライアントで指定するユーザ名となりま す。ユーザ管理上の付加情報として「本名」や「説明」を追加するこ ともできます。

ユーザが接続できる期間を設定する場合は、「このアカウントの有 効期限を設定する」にチェックを入れ、任意の日付を設定してくださ い。

また、認証に使用できる証明書を特定の証明書に限定する場合は、 「署名済み証明書認証」の「証明書のCommon Name(CN)の値を限 定する」と「証明書のシリアル番号の値を限定する」の項目を必要 に応じて設定してください。これにより特定の署名済み証明書を持 ったユーザだけが接続できるようになります。

PacketiX Desktop VPNクライアントから高度なユーザ認証機能を設定したサーバへ接続すると、「ユーザー認証」ウィンドウが開きます。

署名済み証明書認証を設定したユーザで認証するためには、認証 方法を「証明書認証」に設定し、ユーザ名にPacketiX Desktop VPN サーバで設定したユーザ名を入力します。「証明書ファイル」として PacketiX Desktop VPNサーバにて設定されている信頼された証明 機関で署名された証明書ファイル(PKCS#12ファイル)を指定し「OK」 ボタンを押します。

「秘密鍵のパスフレーズ」ウィンドウが表示されたら、証明書を作成した際のパスフレーズを入力し、「OK」を押します。



ユーザー認証
Desktop VPN サーバー "xp-pro" に接続するためには、ユーザー認証を行う必要があり ます。 認証方法を選択してから、ユーザー名を入力して、必要なデータを入力してください。
- ユーザー名わよびユーザー認証方法 認証方法(例) ◎ パスワード認証(例) ● 証明書認証(例)
ユーザー名(U): luser-d
パスワード記録
イスワード2000を使用する場合は、パスワードを入力して [OK] をク リックしてください。
パスワード(2):
証明書認証
証明書認証を使用する場合は、(参照)をクリックして PKCS#12 形式の証明書ファイル (p12 または pfx)を指定して(たさい。
[C/¥Documents and Settings¥hk-mizuno¥デスクト] 参照(B)





■ Radius認証を使用すると、PacketiX Desktop VPNサーバは外部のRadiusサーバを使用してクライア ントを認証することができます。Radius認証を使用する場合、Radiusサーバを別途用意し、Radius サー

バにて PacketiX Desktop VPNサーバからの認証を発生はよる記事がたしてたく必要がたします

PacketiX Desktop VPNサーバでRadius認証を設定するには、まず「セキュリティ設定」の画面にて「外部認証サーバーの設定」を行います。

「Radiusサーバーの設定」で「Radius認証を使用する」 にチェックを入れ、「Radiusサーバーのホスト名または IPアドレス」と「ポート番号」「共有シークレット」をそれ ぞれ入力し「OK」を押します。



📱 認証サーバーの設定 🛛 🗙				
サーバーにユーザーが Radius サーバー認証モードで接続した場合に、ユーザー名とパス ワードを確認する外部の Radius サーバーを指定することができます。				
- Radius サーバーの設定(<u>F</u>):				
✓ Radius 認証を使用する(U)				
Radius サーバーのホスト名または IP アドレスS: radius.sgi.co.jp				
ポート番号(<u>P</u>): 1812 (UDP ポート)				
共有シークレット(E): ***********				
共有シークレットの確認入力(位): **********				
Padius サーバーは、このサーバーの IP アドレスからの要求を受け付けるように設定して おく必要があります。また、Password Authentication Protocol (PAP) による認識が 有効になっている必要があります。				
外部認証サーバーとして Windows NT ドメインコントローラまたは Windows Server の Active Directory コントローラを使用する場合は、このコンピュータをそのドメインに所属 させておく必要があります。NT ドメイン認証を使用する場合は、設定する項目はありま せん。				
<u>QK</u> ++>tell				

ユーザ認証機能(5-2: Radius認証



次にRadius認証での接続を許可するユーザを作成します。

Radius認証での接続を許可するユーザを作成するには、ユ ーザの設定画面にて認証方法を「Radius認証」に設定しま す。

「ユーザー名」は接続時にクライアントで指定するユーザー 名となります。PacketiX Desktop VPNサーバは、Radiusサー バ上の同じユーザ名を認証情報として使用します。ユーザ管 理上の付加情報として「本名」や「説明」を追加することもで きます。

ユーザが接続できる期間を設定する場合は、「このアカウントの有効期限を設定する」にチェックを入れ、任意の日付を 設定してください。

Radiusサーバ上の異なるユーザで認証を行うためには、 「RadiusまたはNTドメイン認証」の「認証サーバー上のユー ザー名を指定する」のチェックを入れ、Radiusサーバとの認 証に使用するユーザー名を指定します。

PacketiX Desktop VPNクライアントから高度なユーザ認証機能を設定したサーバへ接続すると、「ユーザー認証」ウィンドウが開きます。

Radius認証を設定したユーザで認証するためには、「認証方法」を「パスワード認証」に設定し、「ユーザー名」にPacketiX Desktop VPNサーバで設定したユーザー名を、「パスワード」 に該当するRadiusユーザのパスワードを入力し「OK」をクリッ クします。



esktop VPN クライアント(パージョン 2.00)	ユーザ・	-22.37
PacketiX Desktop VPN C	ð	Desktop VPN サーバー "xp-pro" に接続するためには、ユーザー認証を行う必要があり ます。 認証方法を選択してから、ユーザー名を入力して、必要なデータを入力してください。
接続先コンピュータ ID: xp-pro 接続(M) キャンセル 展歴の消去(E)		- ユーザー名およびユーザー認証方法 認証方法(M): ◎パスワード認証(P) ◎証明書認証(Q)
		ユーザー名(<u>U</u>): [user-e
		パスワード認証正 パスワード認証を使用する場合は、パスワードを入力して [OK] をク リックしてください。
		パスワード(空): ********
		- 証明書認証 証明書認証を使用する場合は、「参照」をクリックして PKCS#12 形式の証明書ファイル (p12 またば ptx)を指定してください。
		<u></u>

ユーザ認証機能⑥:Windowsドメイン認証



■ Windowsドメイン認証を使用すると、PacketiX Desktop VPNサーバは外部のWindowsドメイン(N Tド

メイン、ActiveDirectoryドメイン)を使用してクライアントを認証することができます。

Windowsドメイン認証を使用する場合は、予めPacketiX Destan VPNサーバのPCを認証に使用す

るドメインに参加させておく必要があります。 Windows認証での接続を許可するユーザを作成するには、ユーザの設定画面にて認証方法を「NTドメイン認証」に設定します。

「ユーザー名」は接続時にクライアントで指定するユーザ名となりま す。PacketiX Desktop VPNサーバは、Windowsドメイン上の同じユ ーザ名を認証情報として使用します。ユーザ管理上の付加情報と して「本名」や「説明」を追加することもできます。

ユーザが接続できる期間を設定する場合は、「このアカウントの有 効期限を設定する」にチェックを入れ、任意の日付を設定してくださ い。

Windowsドメイン上の異なるユーザで認証を行うためには、「Radius またはNTドメイン認証」の「認証サーバー上のユーザ名を指定す る」のチェックを入れ、Windowsドメインとの認証に使用するユーザ 名を指定します。

PacketiX Desktop VPNクライアントから高度なユーザー認証機能を 設定したサーバへ接続すると、「ユーザー認証」ウィンドウが開きま す。

Windowsドメイン認証を設定したユーザで認証するためには、「認証 方法」を「パスワード認証」に設定し、「ユーザー名」にPacketiX Desktop VPNサーバで設定したユーザー名を、「パスワード」に該当 するWindowsドメインユーザのパスワードを入力し「OK」をクリックしま

す。 ※Windowsドメイン認証はシングルサインオンには対応しておりません。

システムモードでインストールされたサーバに接続する場合には、再度ユーザ名とパスワードによる認証が必要となります。





クライアントIPアドレスによるアクセス制御機能



- PacketiX Desktop VPNサーバでは、特定のPacketiX Desktop VPNクライアントからの接続を制限したり、特定のPacketiX Desktop VPNクライアントのみから接続を許可することができます。PacketiX Desktop VPNサーバに接続できるクライアントを制限できますので、不正なアクセスをブロックできます。
- クライアントIPアドレスによるアクセス制御を設定するには、以下の操作を 行います。
- 1. 「PacketiX Desktop VPNサーバ設定ツール」から「セキュリティ設定」を 選択し、「IPアクセス制御リスト」を選択します。
- IPアクセス制御リスト」ウィンドウには、現在のアクセス制御リストが表示されます。IPアドレスによるフィルタリング設定を行うには、「ルールの追加」を選択します。
- 3. 「IPアクセス制御リストのルール項目の編集」ウィンドウでルールの詳細 を設定します。「単一のIPアドレス」もしくは「複数のIPアドレス」を指 定して、アクセス制御をしたいIPアドレスを設定します。IPアドレスの アクセス制御は、該当IPアドレスのクライアントのみから接続させる か、該当IPアドレスのクライアントからの接続を拒否するかの設定が できます。※
- IPアドレスの制御ルールを設定すると、「IPアクセス制御リスト」にルー ルが追加されます。同じIPアドレスに対し異なるルールが設定されている場合、上位に書かれているルールが適応されます。「保存」を押 すことで追加されたアクセス制御設定が有効になります。
- ※ デフォルトルールとして すべてのアクセスを拒否する設定を行う場合は、 アドレス 0.0.0.0 ネットマスク 0.0.0.0 を指定します。
- ※インターネットへ接続する際にルータやプロキシサーバを経由する場合 は、クライアント IP アドレスは インターネットへ接続する際に使用さ れている ルータやプロキシサーバのアドレスとなります。



サーバ設定ツールの起動ユーザ制限



■ PacketiX Desktop VPNサーバでは、サーバ設定ツールを起動するためのパスワードを設定するとともに、設定ツールを起動できるユーザを制限することが可能です。

接続先のPCに複数のユーザが存在する場合に、特定の管理ユーザのみが設定ツールを起動 できる

ようにすることで、一般ユーザによって設定を変更されることを防ぐことができます。

設定ツール起動後、「設定用パスワードの設定」画面にて、設定ツールを起動できるユーザを制限することができます。 チェックボックスを設定することにより、現在ログイン中のユーザのみがサーバ設定ツールを開くことができるようになります。

🎐 Desktop VPN サーバー設定ツール (パージョン 2.00)	
Desktop VPN Server	設定用パスワードの設定
インターネット通信に関する設定() コンピュータ ID: nakajima_note 変更(c) 元に戻す(B) コンピュータ ID: ロークタ ID: インターネット上でこのコンピュータを読別するための名前です。英数 デキまどバハイフンを使ったがきな名前にいっても変更できます。 通信の方法: HTTP クロキシ経由 接続 プロキシサーバーの設定(P) プロキシサーバーの設定を行ってください。 プロキシサーバーの設定(P) プロキシサーバーの設定を行ってください。 プロキシサーバーの設定(P) プロキシサーバーの設定を行ってください。 クロキンサーバーの設定(P) プロキシサーバーの設定(P) グロキンサーバーの設定(P) プロキンサーバーの設定(P) グロキンサーバーの設定(P) 現在の状態 EU(インターネットに接続されています。 のコンピュータの ID は「nakajima_note」です。 オーバーの設定(P) クライアントからの 現在、Desktop VPN ウライアントを使用してインターネ い経由でこのコンピュータに見てんできます。 グライアントからの 現在、Desktop VPN ウライアントを使用してインターネ い経由でこのコンピュータに見てんできます。 グライアントからの 現在、Desktop VPN ウライアントを使用してインターネ い経由でこのコンピュータに見てんできます。 グライアントからの 現在の主体の設定(P) 単し、日本(D) 推続を禁止する(E) その他の設定(P) セキュリティに関する設定です。 レキュリティ(定関する設定です。 パーブョン/情報(D) 回有D(U) 教力につくつ 第一、 アニークの 原作(大ちののパスワードを設定します。) 原定します。 アントウェアの動が作わ容に関する設定での 設定用パスワードの設定(W) 設定します。 設定します。 設定の方での 設定のの 設定します。 設定します。 設定します。 <t< th=""><th> ○ Desktop VPN サーバー設定ツールを起動するためのパスワードを設定することができます。パスワードを設定すると、次回から設定ツールを起動するためにパスワードの入力が要求されるようになります。 パスワードの設定 パスワードを設定する(リ) パスワード(P): ************************************</th></t<>	 ○ Desktop VPN サーバー設定ツールを起動するためのパスワードを設定することができます。パスワードを設定すると、次回から設定ツールを起動するためにパスワードの入力が要求されるようになります。 パスワードの設定 パスワードを設定する(リ) パスワード(P): ************************************

ログ出力先の変更



■ PacketiX Desktop VPNサーバ では、従来のファイルによるログの保存に加え、Window sの



ログの保存方法を設定するには、PacketiX Desktop VPNサーバ設定ツールから「動作設定」を選択します。右上の「ログ保存」の欄で、有効にするログの出力方法にチェックを入れます。

※syslogプロトコルによるログの送信を行なうには、syslogサーバを別途用意する必要があります。 ※syslogプロトコルによるログはUTF-8フォーマットで送信されます。

PacketiX Desktop VPNサーバによる共有機能の設定 🕗 RAPPORT

■ PacketiX Desktop VPNサーバでは、PacketiX Desktop VPNクライアントの共有機能を禁止・許可 する

ことができます。これにより、PacketiX Desktop VPNクライアント側の設定によらず、PacketiX Desktop VPNサーバ側でリソース共有機能の管理が行えます。 共有機能の禁止設定をおこなうには、以下の操作を行います。

- 1. 「PacketiX Desktop VPNサーバ設定ツール」から「動作設定」をクリック
- 2. 「動作設定」の「共有機能の禁止」から「共有機能を禁止する」にチェックを付ける。

※共有機能の禁止設定を行った場合、以前のバージョンのクライアントからの接続ができなくなる場合がございます。

わたまたで Desktop VPN サーバー ソフトウェアの動作に関する設定を行うことができます。		※クライアント側での共有機能設定
Classical VIN Class	D'502群 Desktap VPN Server @動作D57ァイルを採存するひ D57ァイルを採存するひ D57ァイルを採存するひ D57ァイルを採存するひ systex ウードースの ホートを中心 ちい ホートを中心 ちい ホートを中心 ちい ホートを中心 ちい アンバシン目前を表示していた。 オード・ マンジングを入った オートの マンジングを入った オートの マンジングを入った オートの マンジングを入った オートの マンジングを入った オー マンジング オー マンジング マンジン	各クライアントごとに共有機能設定のON/OFFを変更できます。
その他の設定(1) セキュリティに関する設定です。 セキュリティに関する設定です。 セキュリティに関する設定です。 セキュリティングをついたの情報を表示します。 バージョン情報(2). 図有ID(U)- エンフトウェアの動作内容に関する設定で 酸定が完了したら、I開しる] ボタンをクリックしてこの画面を閉じてください。 閉じる (2)		□ プリンタの共有構築を使用する(P) □ シリアネボートの共有構築を使用する(P) □ シリアネボートの共有構築を使用する(S) ① これらいて、オルトレアの、(Printers Server 2013, Windows Viria Glassican / Entaprise / Entaprise / United Windows Server 2013)、Windows Viria Glassican / Entaprise / Interested, Works Server 2013 (Windows Viria Glassican / Entaprise / Interested, Works Server 2013)、Windows Viria Glassican / Entaprise / Interested, Works Server 2013 (Windows Viria Glassican / Entaprise / Interested, Works Server 2013)、Windows Viria Glassican / Entaprise / Interested, Works Server 2013 (Windows Viria Glassican / Entaprise / Interested, Works Server 2013)、Windows Viria Glassican / Entaprise / Interested, Works Server 2013 (Windows Viria Glassican / Entaprise / Interested, Windows Server 2013) Interested, Windows Server 2013 Interested, Windows Server 2013 Interested