PacketiX Desktop VPN

RAPPORT

目次

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！

RAPPORT

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。

これで解決！

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※1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】

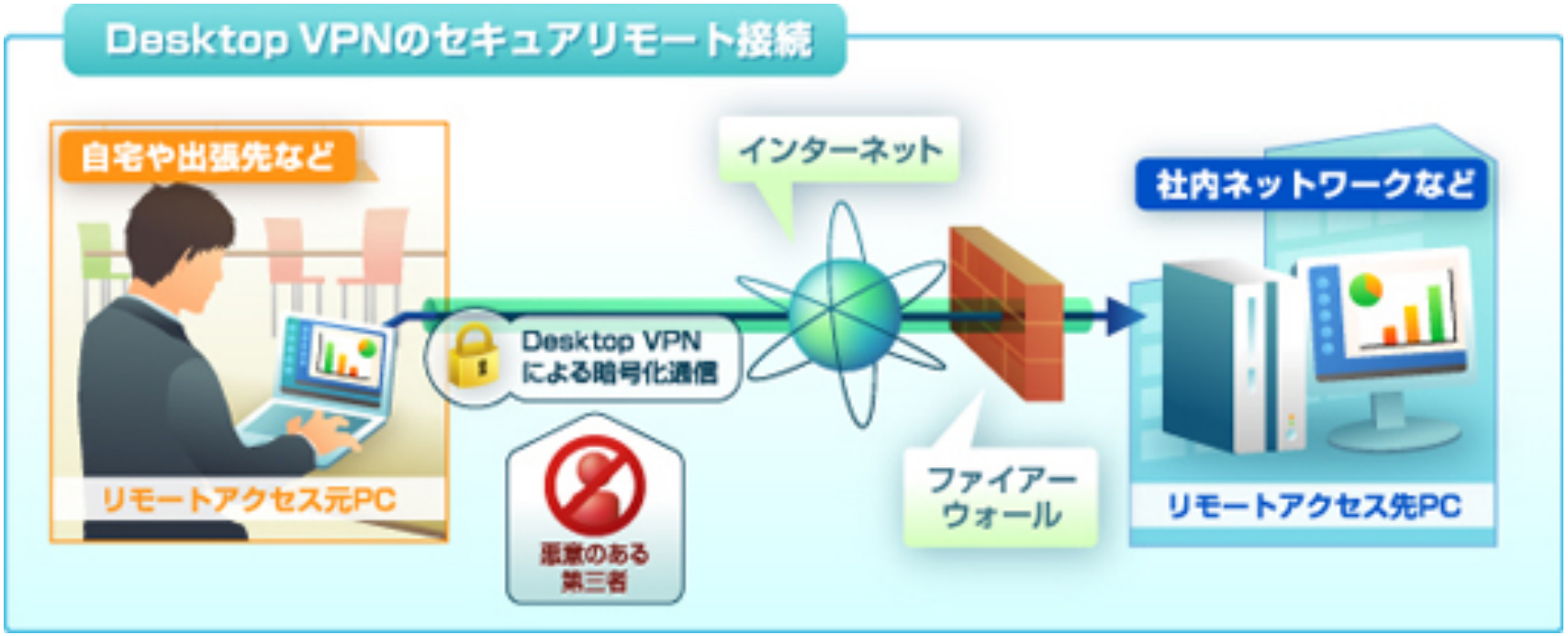
- 1ライセンス：　月額900円/年額10,800円（税抜）
- 初期費用：　なし
- 最低契約数：　1ライセンス～
- 最低契約期間：1ヶ月
- 年額一括払い：可

※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。

サービス特長

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



サービス特長

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

●ルータ、ファイウォール等のネットワーク
機器設定変更が不要

●PacketiX Desktop VPNサーバを遠隔PCに、
クライアントをアクセス元PCにインストール
する
だけで(※)セキュアなリモートアクセスを実現

●インターネットに接続されていれば、いつでも
どこでも利用可能

(※)クライアントはインストール不要の実行ファイル
形式も提供しています。

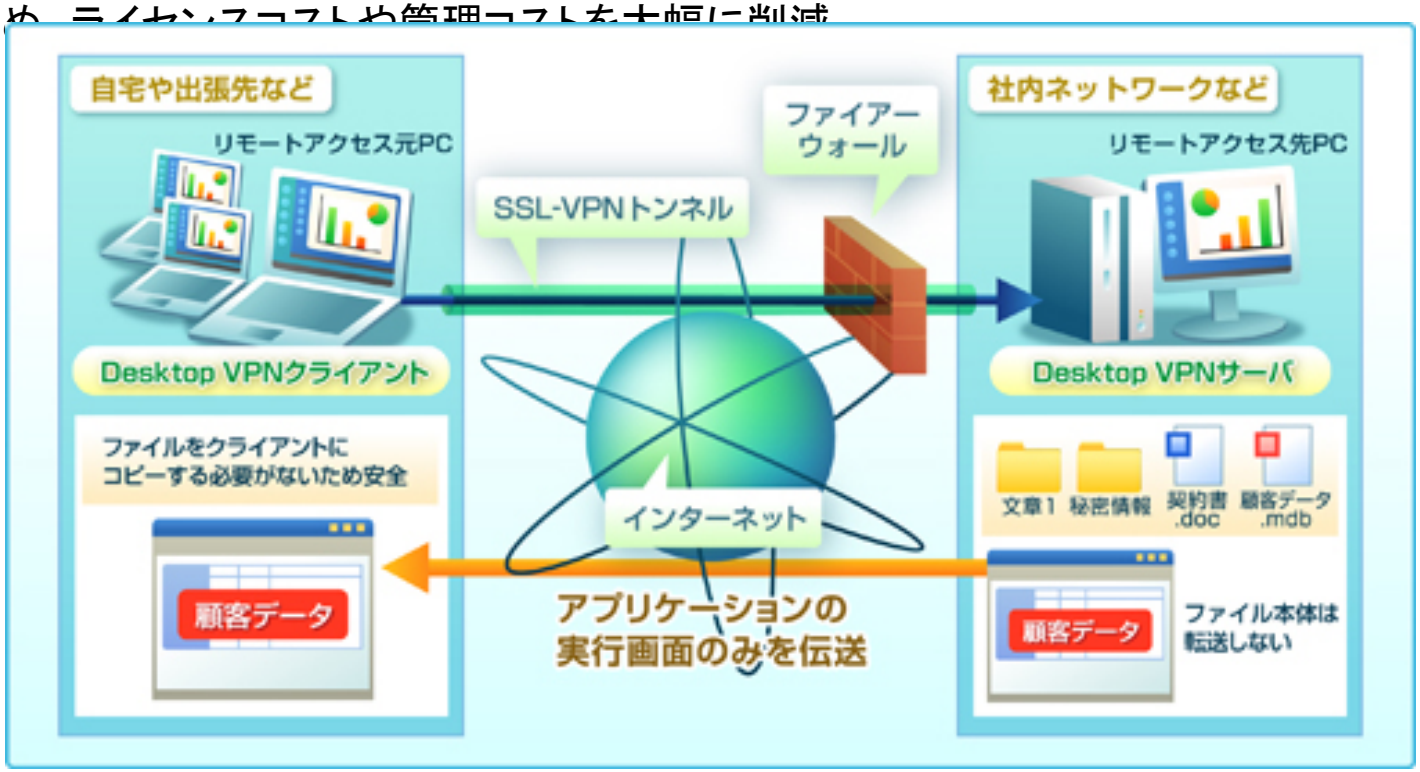
サービス特長

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。
そのため、ライセンスコストや管理コストを大幅に削減



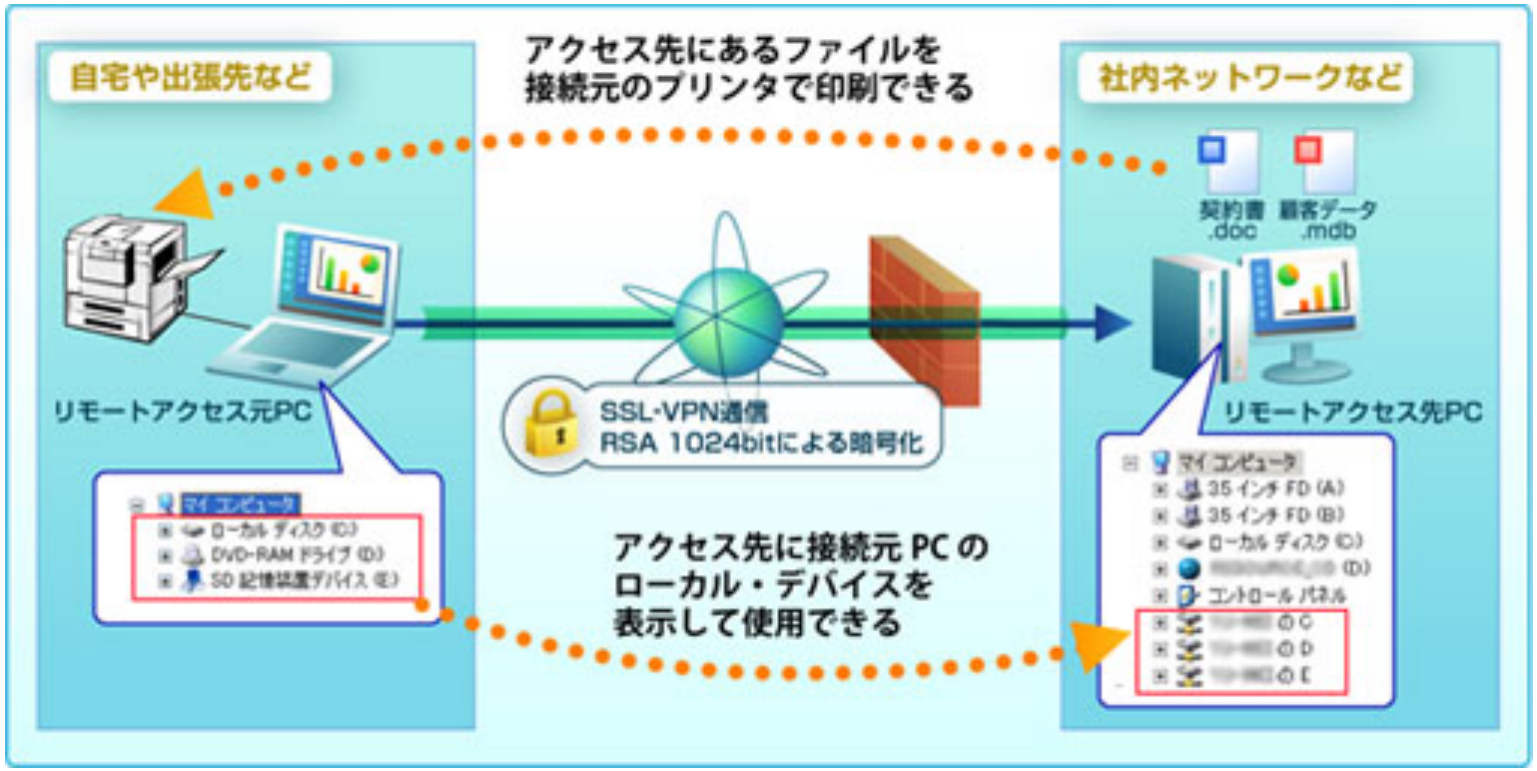
※一部のソフトウェアは、リモートアクセス時の使用についてライセンス上の特記事項がある場合があります。詳細は各ソフトウェアのライセンス許諾条件をご確認下さい。

サービス特長

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。

サービス特長

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。

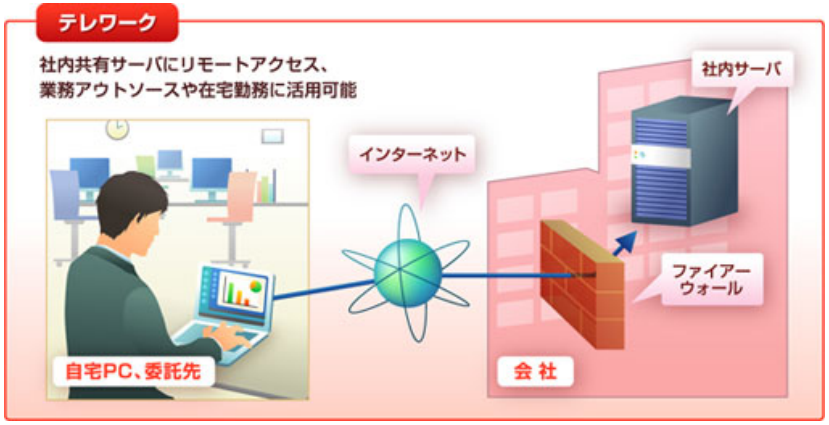
匿名認証	パスワードを必要とせず、ユーザ名のみで接続
パスワード認証	ユーザ名に対して個別のパスワードを設定
固有証明書認証	サーバ側で設定された特定の証明書と秘密鍵のペアを持つクライアントのみ接続
署名済み証明書認証	外部の認証機関の証明書を登録して、クライアントを認証
Radius認証	外部のRadiusサーバを使用してクライアントを認証
Windowsドメイン認証	外部のWindowsドメイン（NTドメイン、ActiveDirectoryドメイン）を使用してクライアントを認証

●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



「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。

「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。

「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。

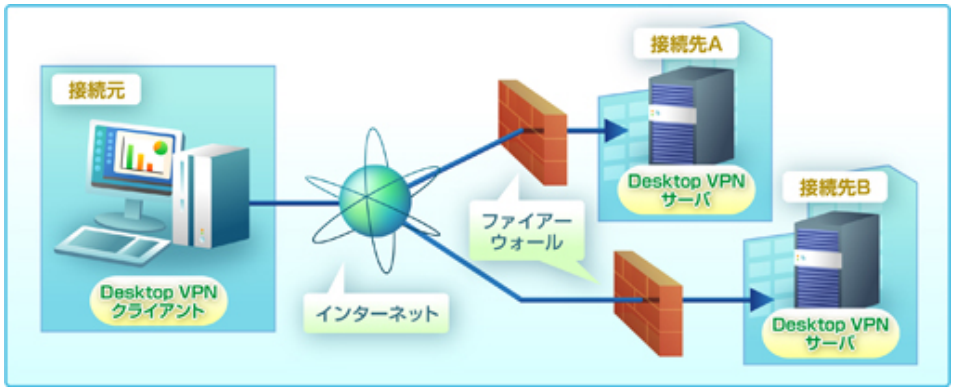
ライセンス体系

●ライセンス体系

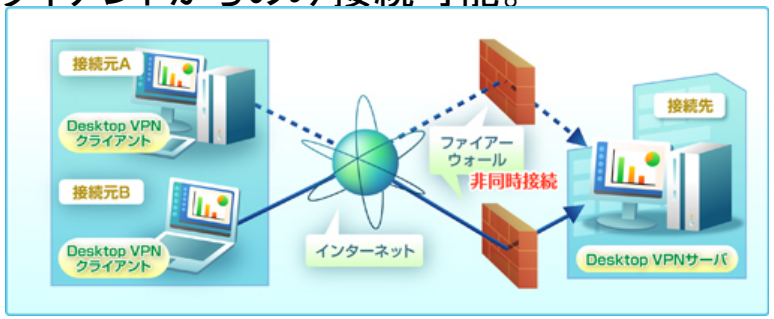
リモートアクセス先マシンに同時に1つのクライアントから接続するためのライセンスです。

・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。

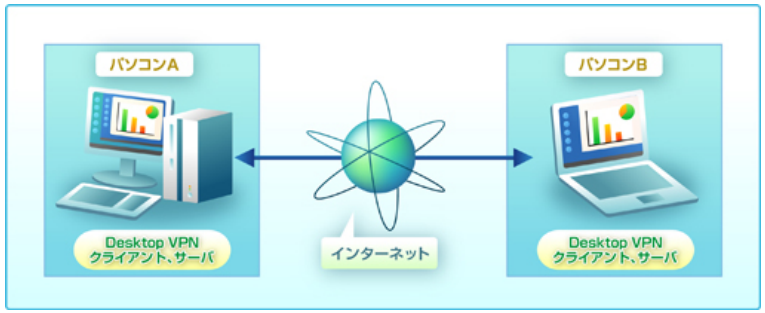
●必要ライセンス数の計算方法



必要ライセンス数:2



必要ライセンス数:1



必要ライセンス数:2

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
インターネット接続環境	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］ ※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一覧表

サーバ	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 2004/Windows XP Media Center Edition 2005/ 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 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
クライアント	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/ 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/

※システムモードインストールとユーザーモードインストール
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。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
30日間無料お試しダウンロードで、
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。

まずはご体験ください！

・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。

Appendix

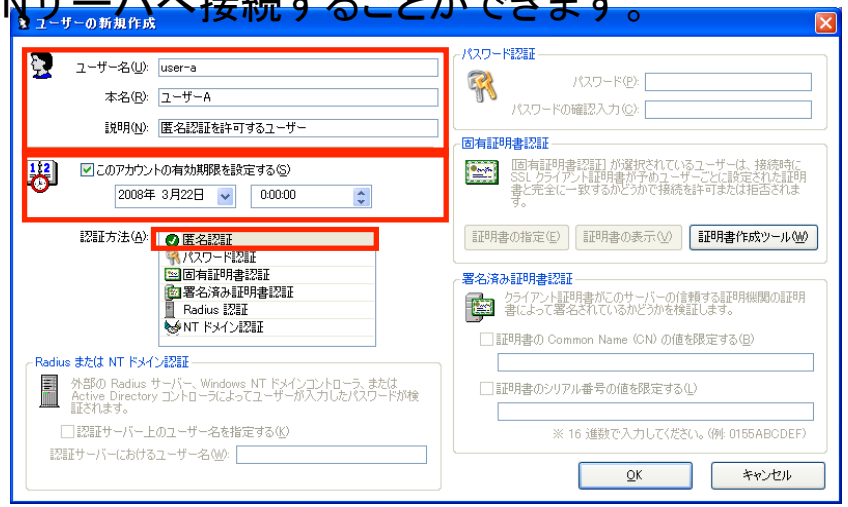
ユーザ認証機能①：匿名認証

■ 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。

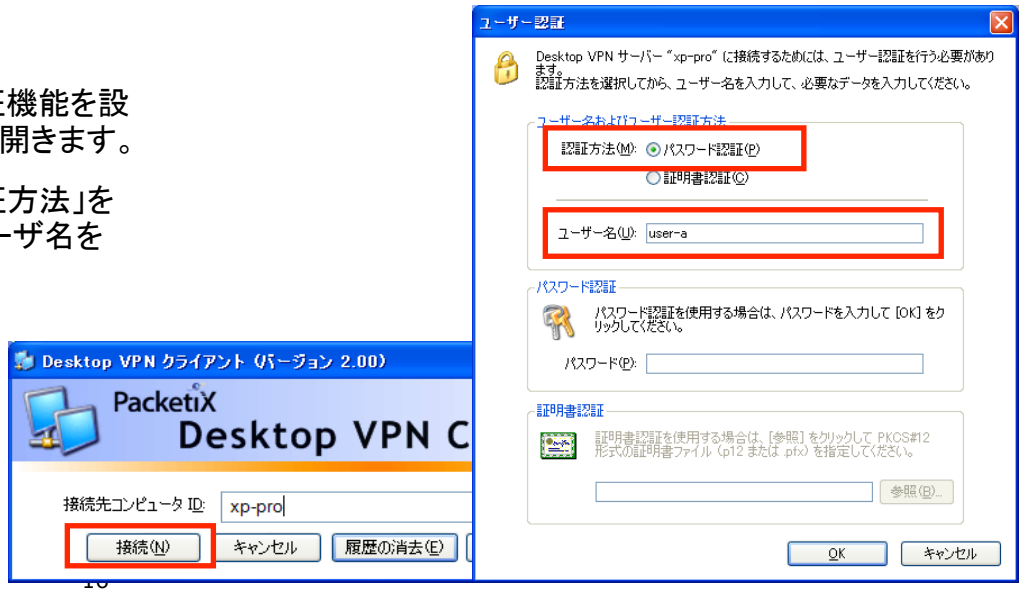
「ユーザー名」は接続時にクライアントで指定するユーザ名となります。ユーザ管理上の付加情報として「本名」や「説明」を追加することもできます。

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。



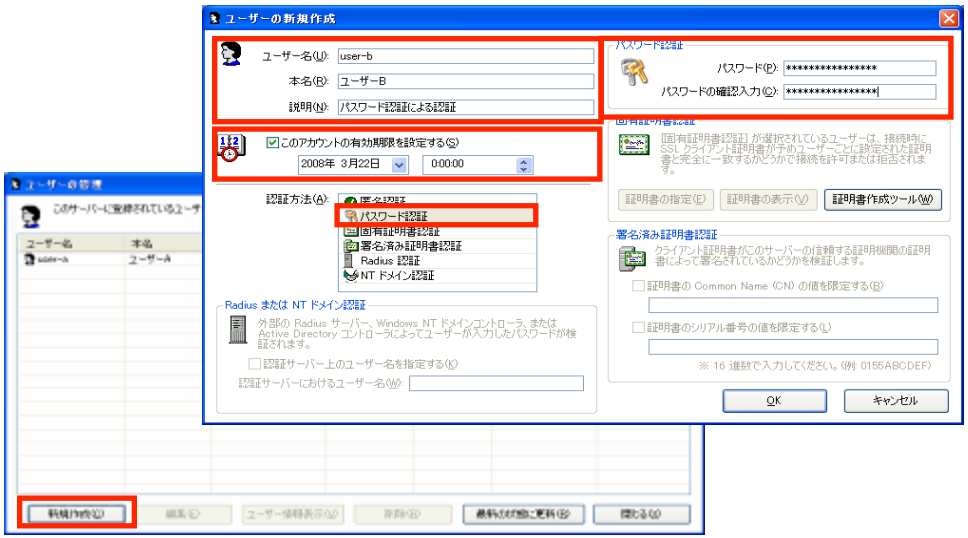
ユーザ認証機能②：パスワード認証

■ 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。

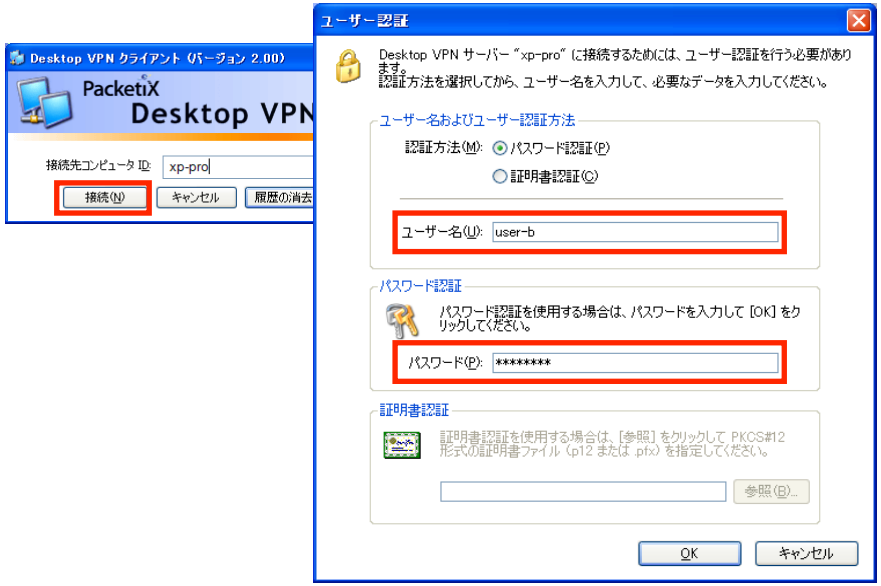
「ユーザー名」は接続時にクライアントで指定するユーザ名となります。ユーザ管理上の付加情報として「本名」や「説明」を追加することもできます。「パスワード認証」の欄で入力したパスワードがクライアント接続時に入力するパスワードとなります。

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。



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。

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。



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。

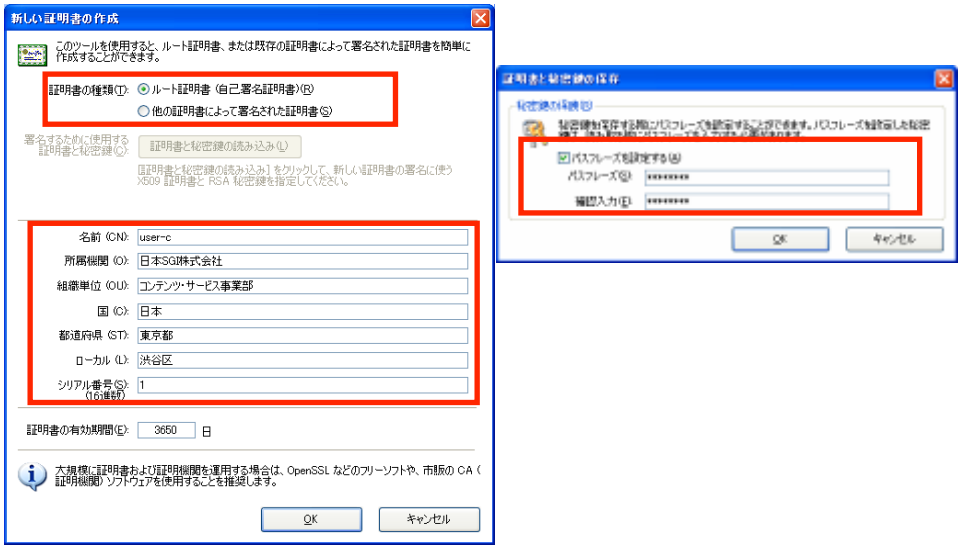
固有証明書認証での接続を許可するユーザを作成するには、ユーザの設定画面にて 認証方法を「固有証明書認証」に設定します。

「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。

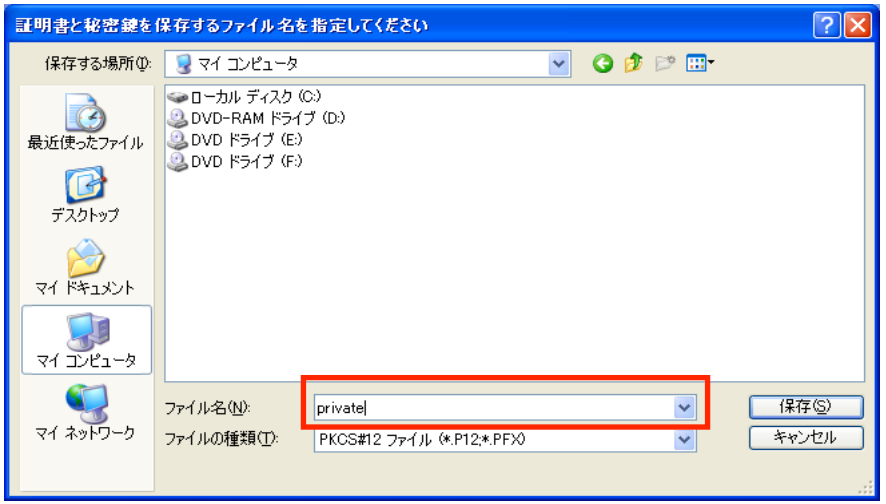
次に「固有証明書認証」の登録をおこないます。既に証明書と秘密鍵のペアを持っている場合、「証明書の指定」から証明書ファイルを選択し設定することで、認証に利用することができます。 新規に証明書と秘密鍵を作成するには、「固有証明書認証」の欄の「証明書作成ツール」をクリックします。

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。



ユーザ認証機能③-2：固有証明書認証

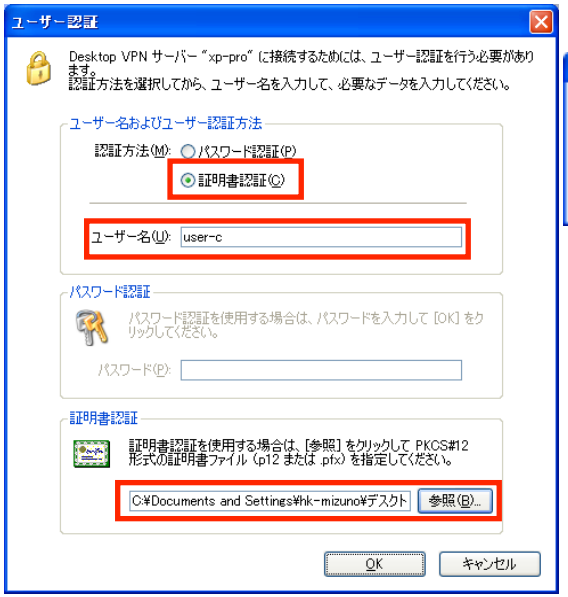
「証明書と秘密鍵を保存するファイル名を指定してください」というウィンドウが開いたら、証明書と秘密鍵の含まれたファイル（PKCS#12ファイル）を適当な名前を付けて保存します。PacketiX Desktop VPNクライアントは このファイルを使用して認証を行いますので、保存したファイルはPacketiX Desktop VPNクライアントのPCにコピーします。

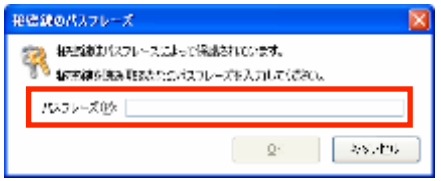


PacketiX Desktop VPNクライアントから高度なユーザ認証機能を設定したサーバへ接続すると、「ユーザー認証」ウィンドウが開きます。

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。

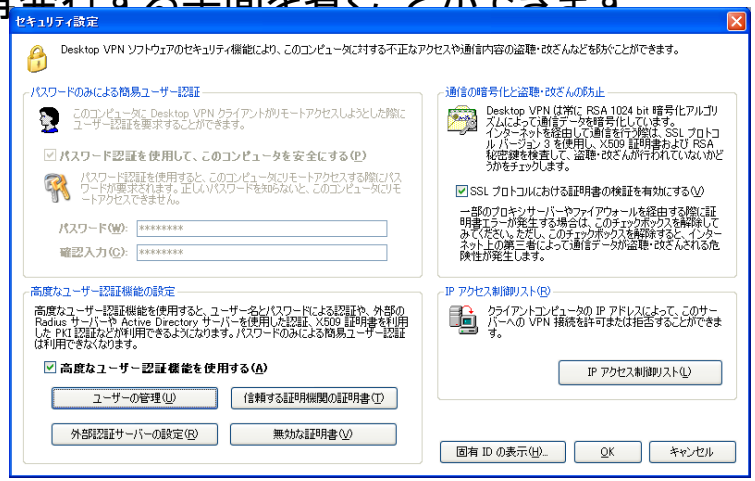




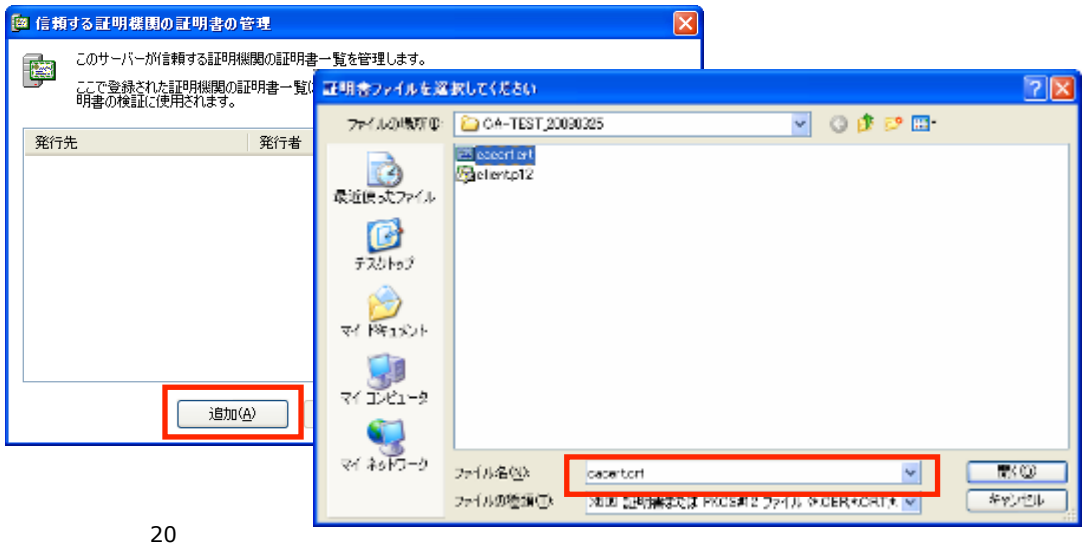
ユーザ認証機能④-1：署名済み証明書認証

■ 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

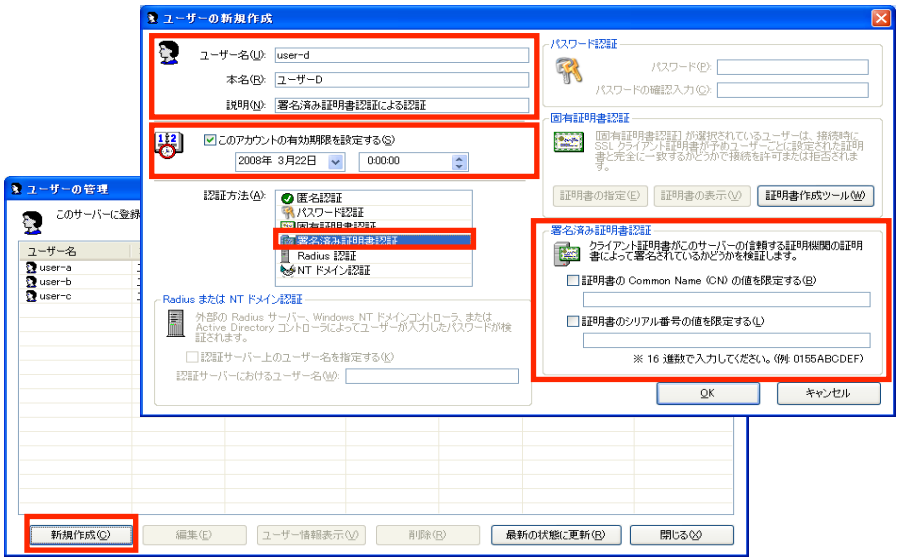
次に署名済み証明書認証での接続を許可するユーザを作成します。

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。

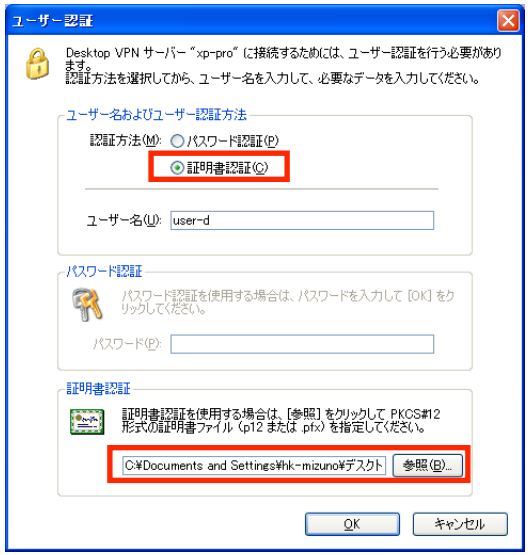
また、認証に使用できる証明書を特定の証明書に限定する場合は、「署名済み証明書認証」の「証明書のCommon Name(CN)の値を限定する」と「証明書のシリアル番号の値を限定する」の項目を必要に応じて設定してください。これにより特定の署名済み証明書を持ったユーザだけが接続できるようになります。



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。

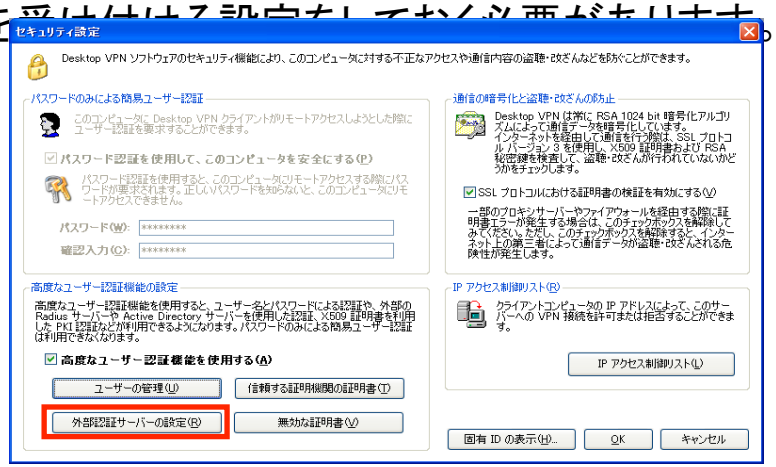
「秘密鍵のパスフレーズ」ウィンドウが表示されたら、証明書を作成した際のパスフレーズを入力し、「OK」を押します。



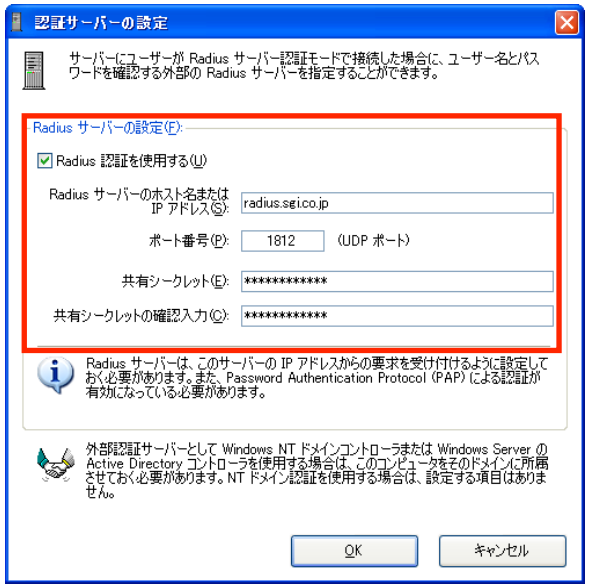
ユーザ認証機能⑤-1：Radius認証

■ 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受けはじめる設定をしておく必要があります。

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。



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。

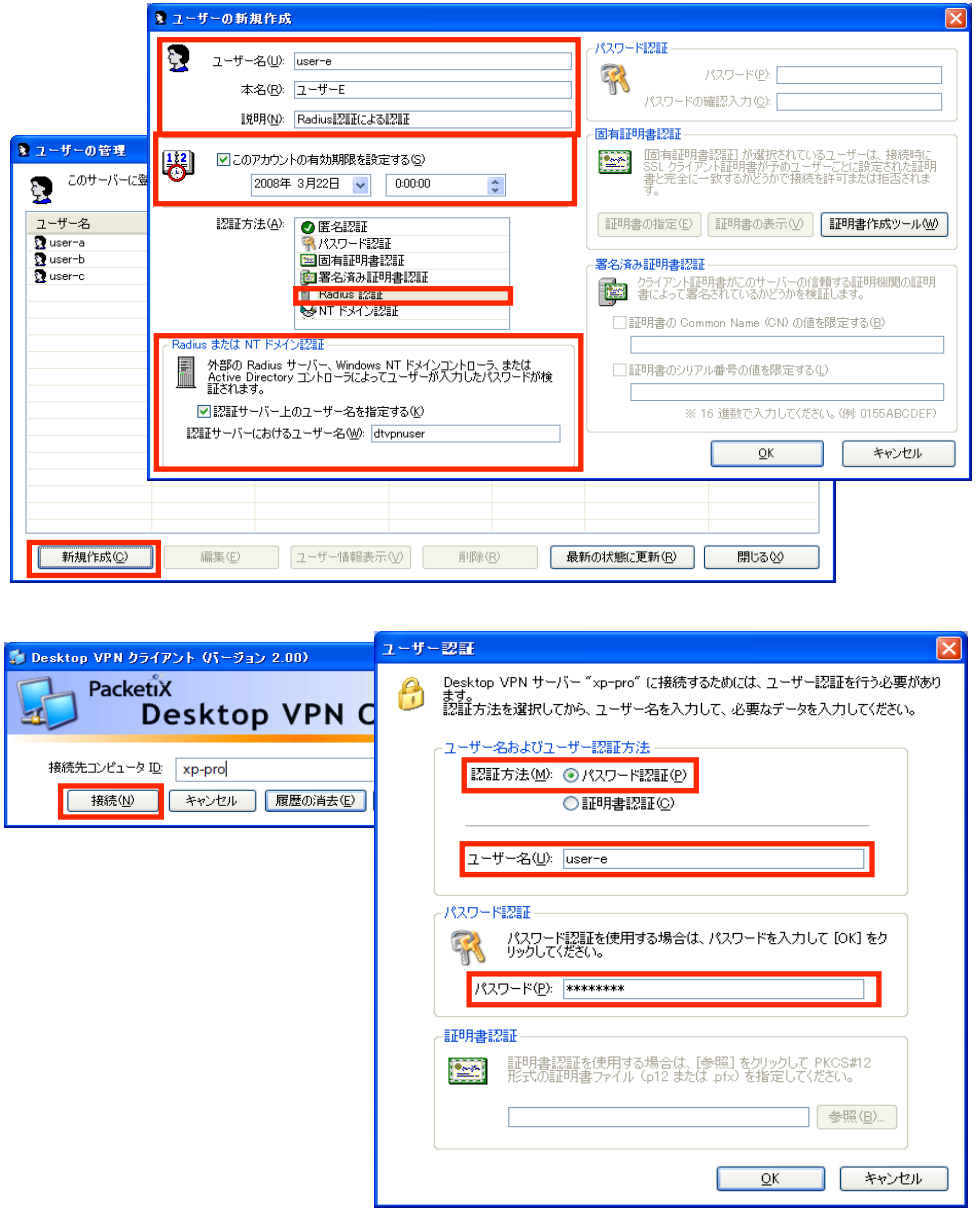
「ユーザー名」は接続時にクライアントで指定するユーザー名となります。PacketiX Desktop VPNサーバは、Radiusサーバ上の同じユーザ名を認証情報として使用します。ユーザ管理上の付加情報として「本名」や「説明」を追加することもできます。

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。



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（NT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 Desktop 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。

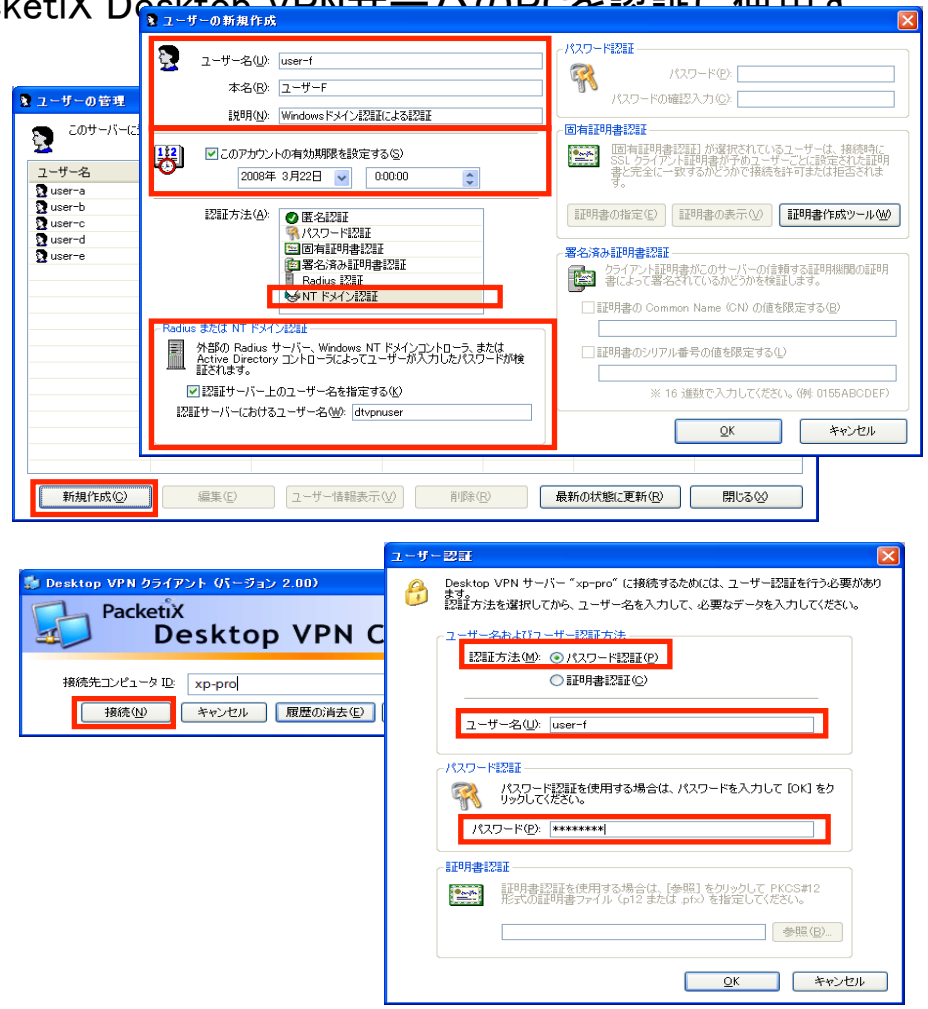
「ユーザー名」は接続時にクライアントで指定するユーザ名となります。PacketiX Desktop VPNサーバは、Windowsドメイン上の同じユーザ名を認証情報として使用します。ユーザ管理上の付加情報として「本名」や「説明」を追加することもできます。

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。

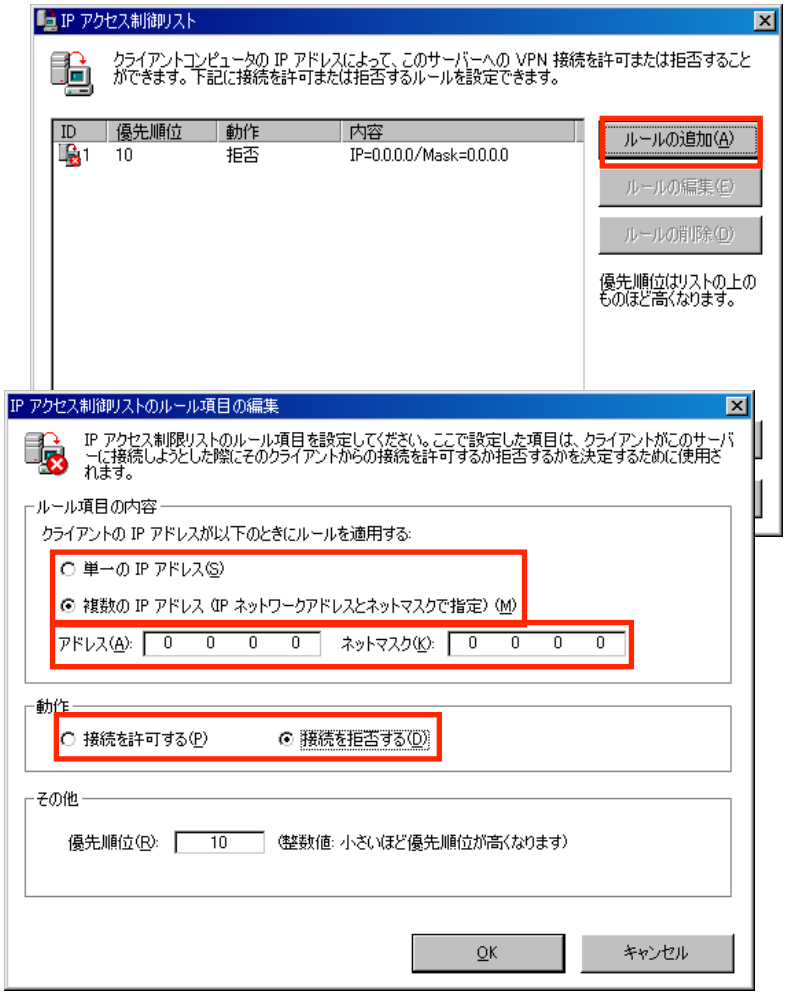
2. 「IPアクセス制御リスト」ウィンドウには、現在のアクセス制御リストが表示されます。IPアドレスによるフィルタリング設定を行うには、「ルールの追加」を選択します。

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。※

4. 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。

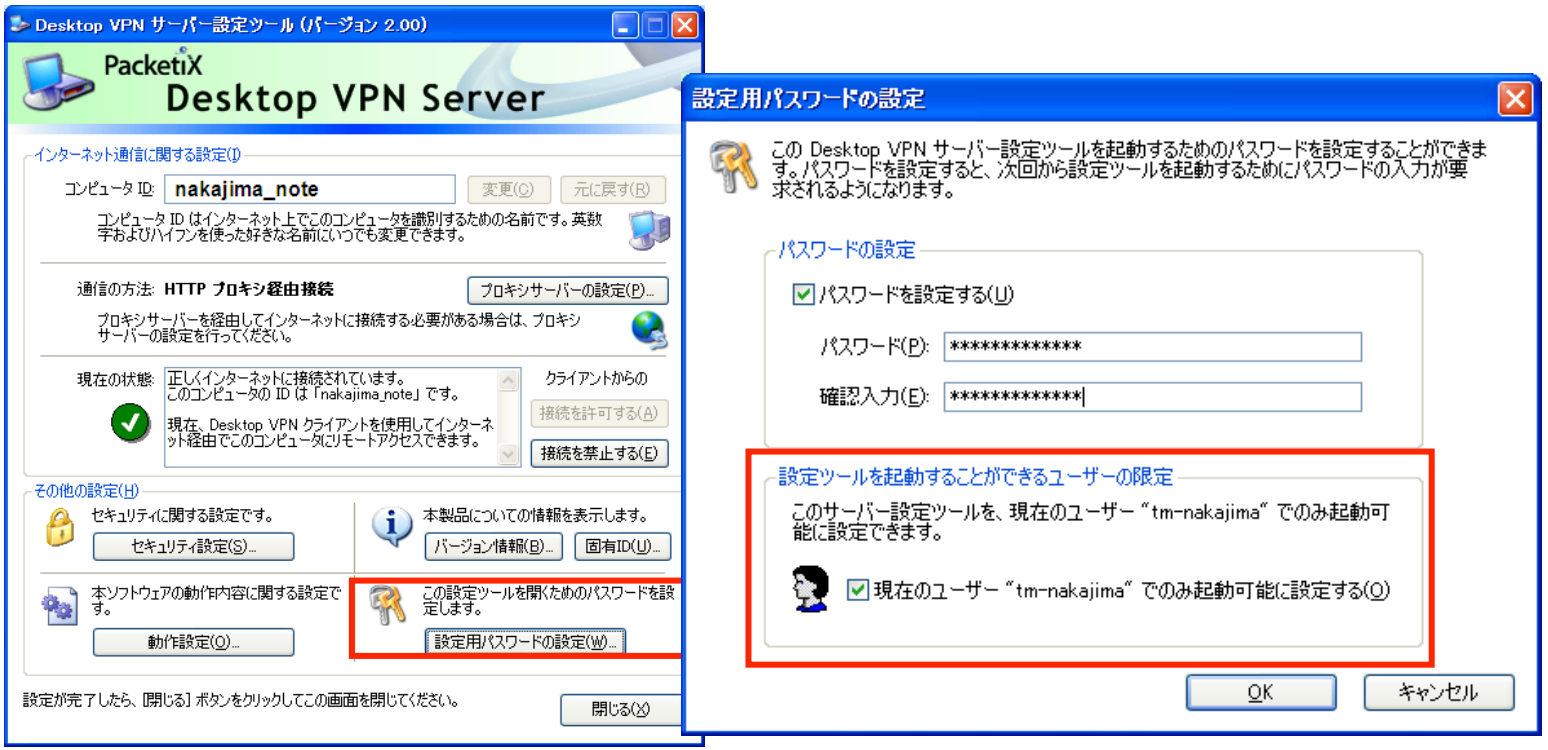
※インターネットへ接続する際にルータやプロキシサーバを経由する場合は、クライアント IP アドレスは インターネットへ接続する際に使用されている ルータやプロキシサーバのアドレスとなります。



サーバ設定ツールの起動ユーザ制限

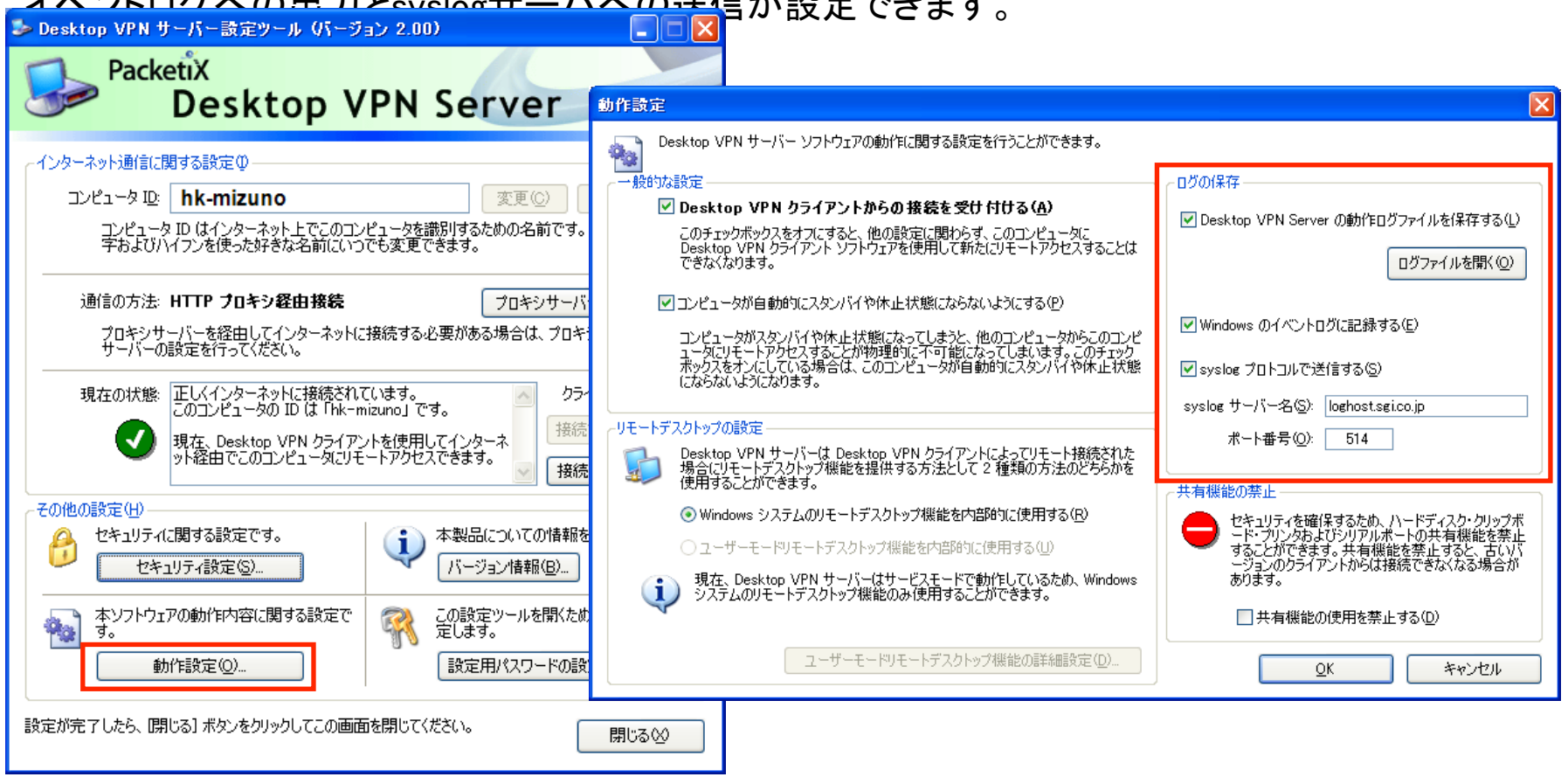
■ PacketiX Desktop VPNサーバでは、サーバ設定ツールを起動するためのパスワードを設定するとともに、設定ツールを起動できるユーザを制限することが可能です。
接続先のPCに複数のユーザが存在する場合に、特定の管理ユーザのみが設定ツールを起動できる
ようにすることで、一般ユーザによって設定を変更されることを防ぐことができます。

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。



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、Windowsの
イベントログへの出力とsyslogサーバへの送信が設定できます。



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。

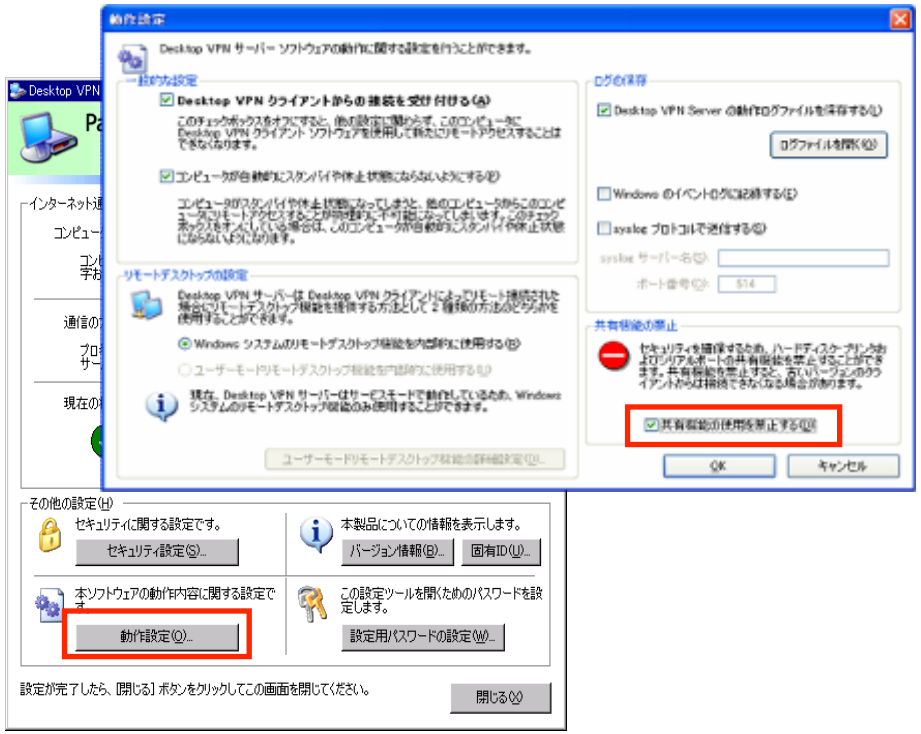
PacketiX Desktop VPNサーバによる共有機能の設定

■ 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。



※クライアント側での共有機能設定

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。