Sony Ericsson

SO-01B

VPN（仮想プライベートネットワーク）展開ガイド

■ 免責事項：

本書の内容に関しては、将来予告なしに変更することがあります。

本書および本ソフトウェア使用により生じた損害、逸失利益または第三者からのいかなる請求につきましても、弊社では一切その責任を負えませんので、あらかじめご了承ください。

2010年2月　第1版
A-DPY-100-01(1)

目次

このガイドはシステム管理者用です。SO-01BのVPN機能を利用するための設定について説明します。

概要

VPN（Virtual Private Network）により、公衆の無線LANホットスポットや自宅のインターネット回線などを専用回線のように使用することで、外出先からの企業内へのセキュアなネットワーク接続を実現することが可能です。これにより、企業内のファイルサーバー、メールサーバー、WEBコンテンツなどのリソースに対して、安全にアクセスすることができます。
VPN機能を使用する際は、セキュリティに関して十分な知識を持った管理者の指導のもとご利用ください。万一、適切な設定が行われないままVPN機能を使用した場合、十分なセキュリティが確保されませんので、ご注意ください。

VPNプロトコル

SO-01BではVPNプロトコルをサポートしています。

VPNプロトコル	説明
PPTP	Point to Point Tunneling Protocol.
L2TP	Layer 2 Tunneling Protocol
L2TP/IPSec PSK	Layer 2 Tunneling Protocol / IP Security with Pre-shared key

PPTP

MPPEによる暗号化が利用可能です。暗号化を利用する場合は、ユーザー認証方式を暗号化対応のプロトコルとしてMS-CHAPまたはMS-CHAPv2を選択する必要があります。

L2TP

事前共有鍵による、機器認証に対応しています。

L2TP/IPSec PSK

事前共有鍵による、機器認証に対応しています。IPSecによる暗号化が利用可能です。

VPNプロトコルとそれぞれの認証・暗号化の組み合わせは以下の通りです。

VPNプロトコル	パケット認証	機器認証	暗号化	ユーザー認証
PPTP	—	—	暗号化なし、MPPE(RSA RC4 40bit,128bit)	MS-CHAPv2, MS-CHAP, CHAP, PAP
L2TP	—	事前共有鍵	—	
L2TP/IPSec PSK	AH, ESP	事前共有鍵	暗号化なし、DES, Triple-DES, AES	

IKEプロポーザル

SO-01Bが対応するIKEプロポーザルは次の通りです。

種別	値
DH Group	2(1024bit)
ISAKMP hash	MD5, SHA1
ISAKMP HMAC hash	HMAC-MD5, HMAC-SHA1
ISAKMP encryption	DES-CBC, 3DES-CBC, AES-CBC-128
IPSec encryption	DES-CBC, 3DES-CBC, AES-CBC-128
IPSec HMAC hash	HMAC-MD5, HMAC-SHA1

SO-01BのVPN設定と接続

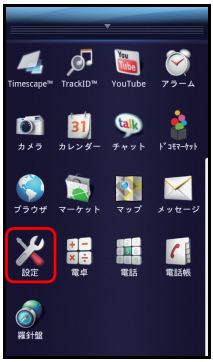
ここでは、SO-01BでのVPN設定方法と接続方法を説明します。この手順を繰り返すことで、複数のVPN接続プロファイルを作成し保存することもできます。

VPNの構成と保存

SO-01Bにて VPN構成を作成・変更・削除するときは、SO-01Bのアプリケーション画面より、「設定」→「ワイヤレス設定」→「VPN設定」とタップします。VPN構成を作成するときは「VPNの追加」をタップしたあと、使用するVPNプロトコルをタップします。また、既存の構成を変更または削除するときは一覧に表示されているVPN名を長くタッチします。

1 アプリケーション画面より「設定」をタップする

設定画面が表示されます。ホーム画面にて[⊞]を押したあと「設定」をタップすることによっても同じ操作が可能です。



2 設定画面から「ワイヤレス設定」をタップする

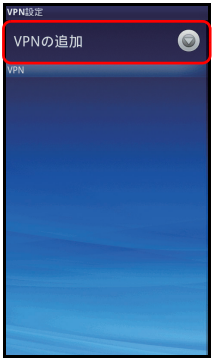
ワイヤレス設定画面が表示されます。

3 ワイヤレス設定画面から「VPN設定」をタップする

VPN設定画面が表示されます。

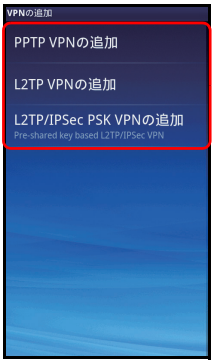
4 VPN設定画面から「VPNの追加」をタップする

VPNの追加画面が表示されます。



5 追加するVPNの種類をタップする

VPN詳細設定画面が表示されます。次項を参考にVPN構成の値を設定してください。



■ PPTP VPN設定

PPTP VPNの追加をタップしたときは次のような画面が表示されます。

次の表に従って値を設定します。

項目名	説明
VPN名	このVPN構成の任意の名称を設定します。
VPNサーバーの設定	VPNサーバーのFQDNまたはIPアドレスを設定します。
暗号化を無効にする	MPPE(Microsoft Point-to-Point Encryption)によるデータ暗号化を行うかどうかを設定します。VPNサーバーのセキュリティポリシーにあわせて設定します。データ暗号化を有効にする場合はチェックを付けます。有効にした場合の暗号化強度は40bitまたは128bitがVPNサーバー設定により自動的に選択されます。
DNS検索ドメイン	追加の検索ドメインをドメイン名で入力します。設定しない場合は空白のままにします。

■ L2TP VPN設定

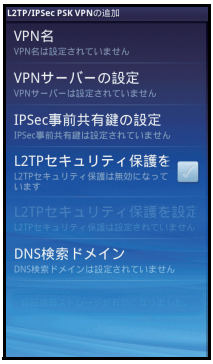
L2TP VPNの追加をタップしたときは次のような画面が表示されます。

次の表に従って値を設定します。

項目名	説明
VPN名	このVPN構成の任意の名称を設定します。
VPNサーバーの設定	VPNサーバーのFQDNまたはIPアドレスを設定します。
L2TPセキュリティ保護を有効にする	L2TP のトンネル認証を行うかどうかを設定します。VPNサーバーの認証設定にあわせて設定します。トンネル認証を有効にする場合はチェックを付けます。
L2TPセキュリティ保護の設定	「L2TPセキュリティ保護を有効にする」とした場合に値を設定します。L2TP トンネル認証の事前共有鍵(shared secret)を設定します。VPNサーバーで定義されているトンネル認証のための事前共有鍵(shared secret)と同じ文字列を設定します。
DNS検索ドメイン	追加の検索ドメインをドメイン名で入力します。設定しない場合は空白のままにします。

■ L2TP/IPSec PSK VPN設定

L2TP/IPSec PSK VPNの追加をタップしたときは次のような画面が表示されます。



次の表に従って値を設定します。

項目名	説明
VPN名	このVPN構成の任意の名称を設定します。
VPNサーバーの設定	VPNサーバーのFQDNまたはIPアドレスを設定します。
IPSec事前共有鍵の設定	IPSecの認証(IKE SA)のための事前共有鍵(pre-shared key)を設定します。VPNサーバーで定義されている機器認証のための事前共有鍵と同じ文字列を設定します。
L2TPセキュリティ保護を有効にする	L2TP のトンネル認証を行うかどうかを設定します。VPNサーバーの認証設定にあわせて設定します。トンネル認証を有効にする場合はチェックを付けます。

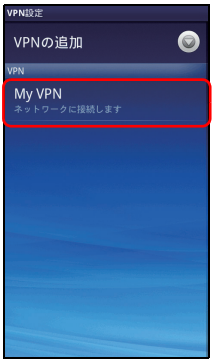
項目名	説明
L2TPセキュリティ保護の設定	「L2TPセキュリティ保護を有効にする」とした場合に値を設定します。L2TP トンネル認証の事前共有鍵(shared secret)を設定します。VPNサーバーで定義されているトンネル認証のための事前共有鍵(shared secret)と同じ文字列を設定します。
DNS検索ドメイン	追加の検索ドメインをドメイン名で入力します。設定しない場合は空白のままにします。

6 [▦]を押して「保存」をタップする

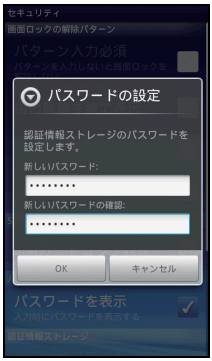
VPN構成が保存され接続の準備が完了します。
途中で作成を中止する場合は「キャンセル」をタップします。

7 VPN設定画面に作成したVPN構成が表示される

VPN構成が保存され接続の準備が完了します。
構成を変更または削除する場合は、一覧表示されているVPN名を長くタッチします。
VPN構成は複数作成することができます。



（参考）認証情報ストレージについて



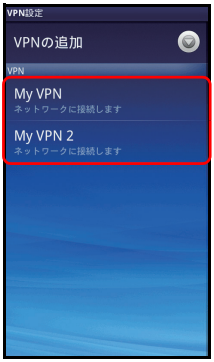
L2TP VPN設定で「L2TPセキュリティ保護を有効にする」にチェックをつけて保存をタップした場合、またはL2TP/IPSec PSK VPNの追加をタップした場合は、初回のみ右のような認証情報ストレージのパスワード設定画面が表示されます。
認証情報ストレージによってL2TP VPNおよびL2TP/IPSec PSK VPNの事前共有鍵はAES 128bit CBC暗号化され、SO-01B内に保存されます。
認証情報ストレージのパスワードは、SO-01B電源オフ、または「設定」→「セキュリティ」の認証情報ストレージにある「安全な認証情報を使用する」のチェックを外した場合に再度入力が必要となります。また、「設定」→「セキュリティ」→「パスワードの設定」にてパスワードの変更ができ、「設定」→「セキュリティ」→「ストレージをクリアする」にてパスワードの削除と認証情報ストレージ内の情報の削除ができます。

VPNの接続

VPNを構成後、以下の手順に従いVPNの接続を行います。

1 VPN設定画面にて接続する「VPN名」をタップする

VPNサーバーへの接続が開始されます。

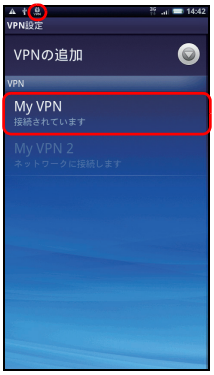


2 ユーザー認証ダイアログが表示され、「ユーザー名」と「パスワード」を入力する

VPNサーバーであらかじめ定義されたものを入力します。ユーザー名の入力を次回より省略したい場合は、「ユーザー名を保存」へチェックを入れます。

3 接続と認証が成功するとVPN接続アイコンが通知領域に表示される

VPN名の表示が「接続されています」に変わります。



VPNの切断

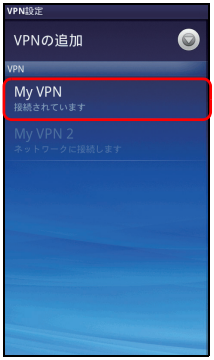
VPNを切断するには以下の手順に従います。

1 通知領域を開き、VPNの通知をタップする

VPN設定画面が表示されます。

2 接続中の「VPN名」をタップする

VPNサーバーとの切断が開始されます。

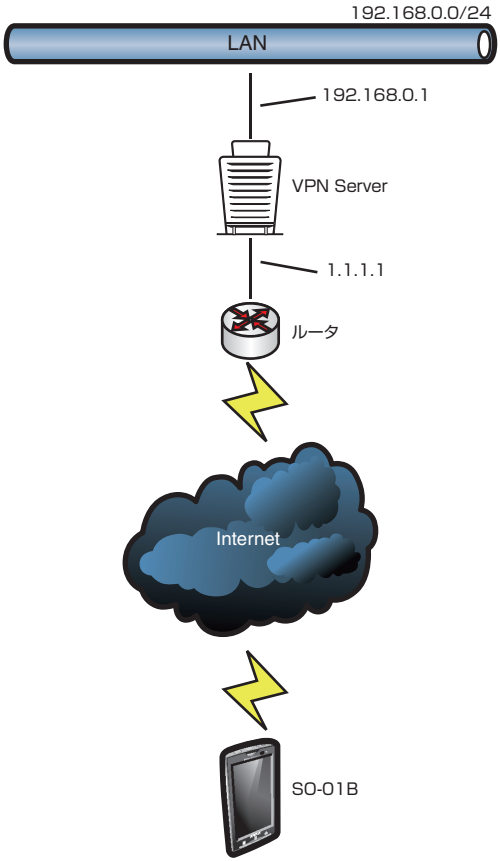


3 切断が完了されると通知領域にVPNの通知が表示される

VPNサーバーとの切断が完了しました。

付録:VPNサーバーの設定例

ここでは、VPNサーバーの設定例として、Microsoft Windows Server 2003を用いたVPNサーバーの構成を説明します。説明の中で具体的なIPアドレスが記載されていますが、説明を分かりやすくするための例として用いていますので、実際にはVPNサーバーを設置するネットワークに準じたものを使用してください。
本構成では次のような環境を想定しています。



通信プロトコル

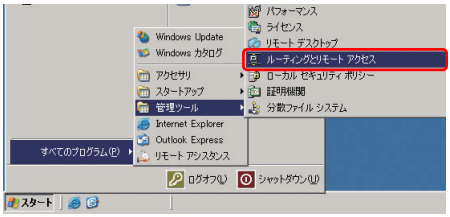
VPNサーバーへの通信経路にルーター・ファイアウォールが設置されている場合は、利用するVPNプロトコルに応じて、必要な通信が許可されていることを確認します。それぞれのVPNプロトコルで利用する通信プロトコルは次の通りです。

VPNプロトコル	ポート番号	プロトコル番号	備考
PPTP	1723	6/TCP	PPTP
	—	47/GRE	General Routing Encapsulation
L2TP/IPSec PSK	1701	17/UDP	L2TP
	500	17/UDP	ISAKMP
	4500	17/UDP	IPSec NAT-Traversal
	—	50/ESP	Encapsulation Security Payload

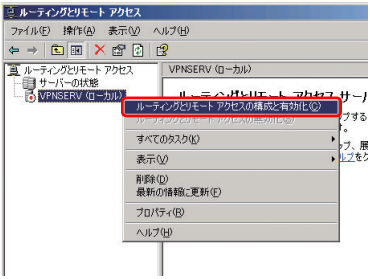
ルーティングとリモートアクセスの設定

VPNサーバーソフトウェアとして、Windows Server 2003へインストール済みの「ルーティングとリモートアクセス」を使用します。

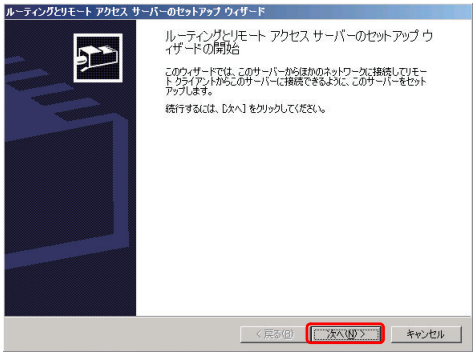
1 「スタート」→「管理ツール」→「ルーティングとリモートアクセス」をクリックする



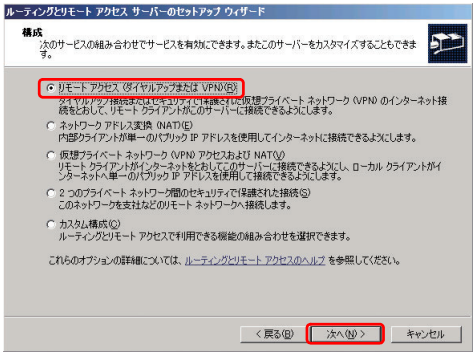
2 「(VPNサーバー名)」を右クリック →「ルーティングとリモートアクセスの構成と有効化」を選択する



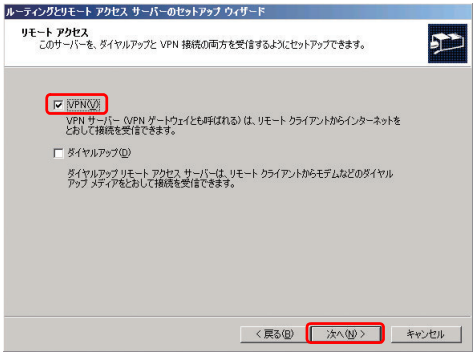
3 「ルーティングとリモートアクセスサーバーのセットアップウィザード」が起動するので、「次へ」をクリックする



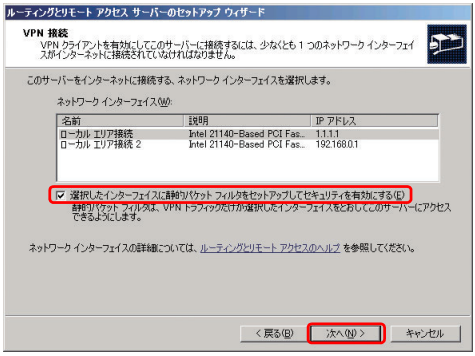
4 「リモートアクセス（ダイヤルアップまたはVPN）」を選択し、「次へ」をクリックする



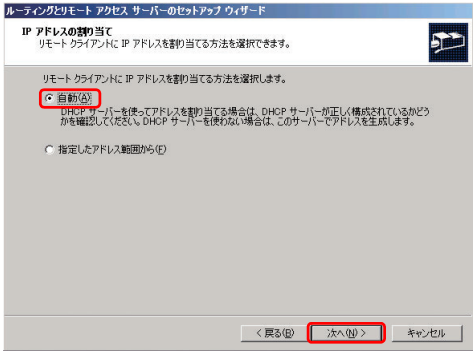
5 「VPN」を選択し、「次へ」をクリックする



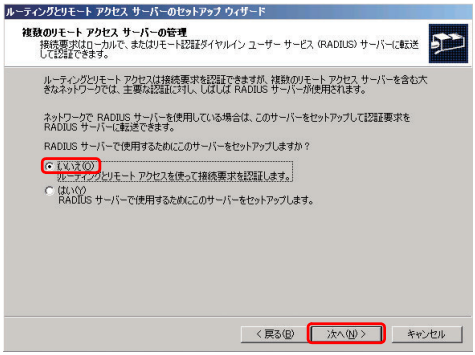
6 インターネット側に接続されているネットワークインターフェースとして「ローカルエリア接続」を選択し、さらに「選択したインターフェースに静的パケットフィルタをセットアップしてセキュリティを有効にする」を選択し、「次へ」をクリックする



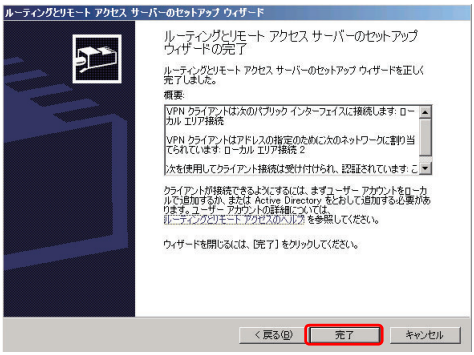
7 「自動」を選択し、「次へ」をクリックする



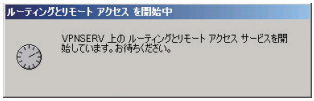
8 本構成例ではRADIUSサーバーを使用しないため、「いいえ」を選択し、「次へ」をクリックする



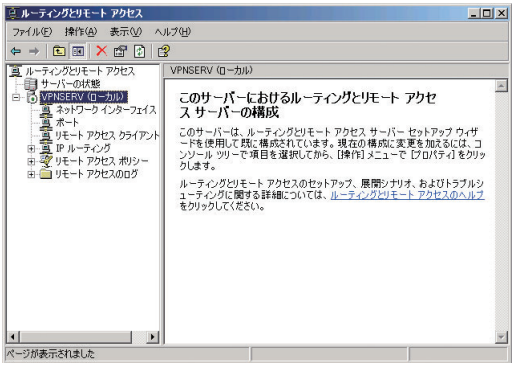
9 「完了」をクリックする



10 サービスの開始中のアニメーションウィンドウが表示されるので、しばらく待つ

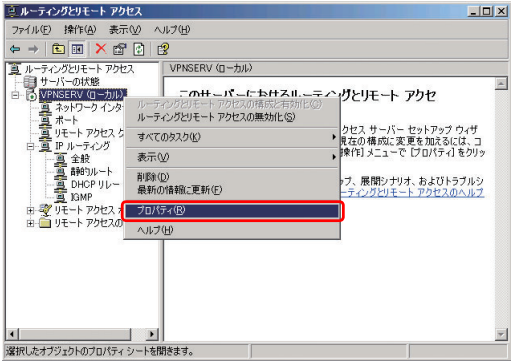


11 ルーティングとリモートアクセスサービスが開始される

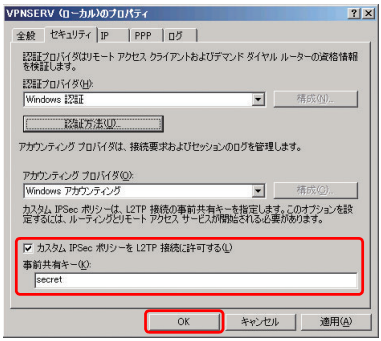


以上で、PPTPでのVPN接続が可能となりました。L2TP/IPSec PSKでのVPN接続を設定する場合は、ひきつづき次の手順へ進んでください。

12 左ペイン内「ルーティングとリモートアクセス」→「(VPNサーバー名)」を右クリックし、プロパティをクリックする



13「セキュリティ」タブにて、「カスタムIPSecポリシーをL2TP接続に許可する」にチェックをし、さらに事前共有キーを入力（例：「secret」)、その後「OK」をクリックする



以上で、L2TP/IPSec PSKでのVPN接続設定が完了しました。

・参考URL（Microsoft TechNetより）：
- VPNサーバーとファイアウォールの構成
  http://technet.microsoft.com/ja-jp/library/cc737500(WS.10).aspx
- データの暗号化
  http://technet.microsoft.com/ja-jp/library/cc785633(WS.10).aspx
- 認証プロトコルと認証方法
  http://technet.microsoft.com/ja-jp/library/cc738300(WS.10).aspx
- トンネリング プロトコル
  http://technet.microsoft.com/ja-jp/library/cc786069(WS.10).aspx
- パケット フィルタを管理する
  http://technet.microsoft.com/ja-jp/library/cc784616(WS.10).aspx