VPN 設定ガイド

Android OS 4.0 ／ 4.1 用

このガイドはシステム管理者用です。VPN（仮想プライベートネットワーク）機能を利用するための設定について説明します。

目次

概要

Virtual Private Network （VPN)は主にインターネットなどの公の通信インフラを通して、リモートネットワークを相互接続するプライベートネットワークです。VPNはトンネルプロトコルと暗号化などのセキュリティ手段によって安全な接続を確保しています。例えば、VPNを利用して、公衆無線LANアクセスポイントや家庭内インターネットから保護された企業内LANへ安全に接続して、ファイルサーバー、メールサーバー、WEBコンテンツなどの企業リソースにアクセスすることができます。

■ VPN機能のご利用およびサーバーの設置について

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。
VPNサーバーをお客様ご自身で構築する場合は、適切なVPN製品を選択して適切な設定を行ってください。
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は、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製品に関するご質問や対応情報については、各VPN機器メーカーにお問い合わせください。

VPN接続方式

次のVPN接続方式をサポートしています。

VPN接続方式	説明
PPTP	Point to Point Tunneling Protocolを利用します。初期設定は、PPP暗号化MPPEになります。
L2TP/IPSec PSK	IPSEC事前共有キー暗号でLayer 2 Tunneling Protocolを利用します。
L2TP/IPSec RSA	IPSEC RSA 公開キー暗号でLayer 2 Tunneling Protocolを利用します。
IPSec Xauth PSK	事前共有キー暗号によるX Window認証に基づく接続方式です。
IPSec Xauth RSA	公開キー暗号によるX Window認証に基づく接続方式です。

PPTP

ポイント･ツー･ポイント･トンネル･プロトコル(Point to Point Tunneling Protocol)。

L2TP/IPSec PSK

Layer 2 Tunneling Protocol認証とInternet Protocol Securityプロトコル群で指定した事前共有キーでの暗号化。

L2TP/IPSec RSA

Layer 2 Tunneling Protocol認証とInternet Protocol Securityプロトコル群で指定したRASでの暗号化。RSAは公開キー暗号化アルゴリズムの一種。

IPSec Xauth PSK

認証とInternet Protocol Securityプロトコル群で指定したX System Authorizationでの暗号化。事前共有キーを認証に利用。

IPSec Xauth RSA

認証とInternet Protocol Securityプロトコル群で指定したX System Authorizationでの暗号化。RSA、公開キー暗号化を利用。

VPN設定

VPNをご利用の際には、あらかじめVPN接続プロファイルを作成し保存しておきます。
複数のVPN接続プロファイルを保存することもできます。
設定や接続の手順については、お使いの端末の取扱説明書をご参照ください。

VPN接続プロファイルの設定について

■ PPTP VPN設定

項目名	説明
名前	VPN接続名を入力します。
サーバーアドレス	VPNサーバーのFQDNまたはIPアドレスを設定します。
PPP暗号化（MPPE）	VPNサーバーのセキュリティポリシーに合わせて、データ暗号化を有効にする場合はチェックを入れます。
DNS検索ドメイン（「詳細オプションを表示する」にチェックが入っている場合）	DNS検索ドメインを設定する場合はドメイン名を設定します。
DNS サーバー（「詳細オプションを表示する」にチェックが入っている場合）	DNSサーバーを設定します。
転送ルート（「詳細オプションを表示する」にチェックが入っている場合）	転送ルートを設定します。

■ L2TP/IPSec PSK VPN設定

項目	説明
名前	VPN接続名を入力します。
サーバーアドレス	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	L2TPトンネル認証の共有キー（shared secret）を設定します。VPNサーバーで定義されたL2TPトンネル認証用の共有キー（shared secret）と同じ文字列を設定します。
IPSec ID	IPSec識別子を設定します。
IPSec事前共有鍵	事前共有キー（password）を設定します。
DNS検索ドメイン（「詳細オプションを表示する」にチェックが入っている場合）	DNS検索ドメインを設定する必要がある場合にドメインネームを設定します。
DNSサーバー（「詳細オプションを表示する」にチェックが入っている場合）	DNSサーバーを設定します。

項目	説明
転送ルート（「詳細オプションを表示する」にチェックが入っている場合）	転送ルートを設定します。

■ L2TP/IPSec RSA VPN設定

項目	説明
名前	VPN接続名を入力します。
サーバーアドレス	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	L2TPトンネル認証の共有キー（shared secret）を設定します。VPNサーバーで定義されたL2TPトンネル認証用の共有キー（shared secret）と同じ文字列を設定します。
IPSecユーザー証明書	インストール済みの証明書を選択します。
IPSec CA証明書	証明書を発行した権限のある事業者の証明書を選択します。初期設定では、サーバーを確認しません。
IPSecサーバー証明書	サーバーの証明書を選択します。初期設定ではサーバーから受信されます。
DNS検索ドメイン（「詳細オプションを表示する」にチェックが入っている場合）	DNS検索ドメインを設定する必要がある場合にドメインネームを設定します。
DNSサーバー（「詳細オプションを表示する」にチェックが入っている場合）	DNSサーバーを設定します。
転送ルート（「詳細オプションを表示する」にチェックが入っている場合）	転送ルートを設定します。

■ IPSec Xauth PSK VPN設定

項目	説明
名前	VPN接続名を入力します。
サーバーアドレス	VPNサーバーのFQDNまたはIPアドレスを設定します。
IPSec ID	IPSec識別子を設定します。
IPSec事前共有鍵	事前共有キー（password）を設定します。
DNS検索ドメイン（「詳細オプションを表示する」にチェックが入っている場合）	DNS検索ドメインを設定する必要がある場合にドメインネームを設定します。
DNSサーバー（「詳細オプションを表示する」にチェックが入っている場合）	DNSサーバーを設定します。

項目	説明
転送ルート（「詳細オプションを表示する」にチェックが入っている場合）	転送ルートを設定します。

■ IPSec Xauth RSA VPN設定

項目	説明
名前	VPN接続名を入力します。
サーバーアドレス	VPNサーバーのFQDNまたはIPアドレスを設定します。
IPSecユーザー証明書	インストール済みの証明書を選択します。
IPSec CA証明書	証明書を発行した権限のある事業者の証明書を選択します。初期設定では、サーバーを確認しません。
IPSecサーバー証明書	サーバーの証明書を選択します。初期設定ではサーバーから受信されます。
DNS検索ドメイン（「詳細オプションを表示する」にチェックが入っている場合）	DNS検索ドメインを設定する必要がある場合にドメインネームを設定します。
DNSサーバー（「詳細オプションを表示する」にチェックが入っている場合）	DNSサーバーを設定します。
転送ルート（「詳細オプションを表示する」にチェックが入っている場合）	転送ルートを設定します。

2013年6月　第3版
1266-3273.3