Sony Ericsson

VPN（仮想プライベートネットワーク）展開ガイド

SO-03C ／ SO-01D ／ SO-02D ／ SO-03D ／ IS12S 用

目次

このガイドはシステム管理者用です。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）を活用すると、公衆の無線LANスポットや自宅などのインターネット回線から企業内のLANへ、セキュアなネットワークアクセスが実現できます。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
L2TP	Layer 2 Tunneling Protocol
L2TP/IPSec PSK	Layer 2 Tunneling Protocol / IP Security with Pre-shared key
L2TP/IPSec CRT	Layer 2 Tunneling Protocol / IP Security with Certificate

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接続方式としてMS-CHAPまたはMS-CHAPv2を選択する必要があります。

L2TP

事前共有キー（shared secret）によるL2TPトンネル認証に対応しています。

L2TP/IPSec PSK

事前共有キー（shared secret）によるL2TPトンネル認証、および事前共有キー（pre-shared-key）によるIKE認証に対応しています。IPSecによる暗号化が利用可能です。

L2TP/IPSec CRT

事前共有キー（shared secret）によるL2TPトンネル認証、および証明書によるIKE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接続方式とそれぞれの認証・暗号化の組み合わせは以下の通りです。

VPN接続方式	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※1, CHAP※2, PAP※2
L2TP	—	—	—	MS-CHAPv2, MS-CHAP, CHAP, PAP
L2TP/IPSec PSK	ESP	事前共有キー	DES Triple-DES AES	
L2TP/IPSec CRT	ESP	証明書		

※1 暗号化なし、MPPE 128bitの場合のみ使用可能。
※2 暗号化なしの場合のみ使用可能。

IKEプロポーザル

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	SHA1, MD5
ISAKMP HMAC hash	HMAC-SHA1, HMAC-MD5
ISAKMP encryption	DES-CBC, 3DES-CBC
IPSec encryption	DES-CBC, 3DES-CBC, AES-CBC-128
IPSec HMAC hash	HMAC-SHA1, HMAC-MD5

VPN設定と接続

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。

VPN接続プロファイルの設定と保存

1 設定メニュー画面で「無線とネットワーク」→「VPN設定」をタップする

2 「VPNの追加」をタップする

3 追加するVPNの種類をタップする

VPN詳細設定画面でVPN接続プロファイルを設定してください。

4 保存する

VPN接続プロファイルが保存され、VPN設定画面に作成したVPN接続プロファイルが表示されます。VPN接続プロファイルを変更または削除する場合は、一覧表示されているVPN名を長くタッチしてください。

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
VPN名	このVPN接続プロファイル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。
暗号化を有効にする	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	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。

■ L2TP VPN設定

項目名	説明
VPN名	このVPN接続プロファイル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	VPNサーバーのセキュリティポリシーに合わせて、L2TPトンネル認証を有効にする場合はチェックを入れます。
L2TPセキュリティ保護を設定する	「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キー(shared secret)を設定します。VPNサーバーで定義されているL2TPトンネル認証のための事前共有キー(shared secret)と同じ文字列を設定します。

項目名	説明
DNS検索ドメイン	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。

■ L2TP/IPSec PSK VPN設定

項目名	説明
VPN名	このVPN接続プロファイル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事前共有キーの設定	IPSecの認証(IKE SA)のための事前共有キー(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キー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	VPNサーバーのセキュリティポリシーに合わせて、L2TPトンネル認証を有効にする場合はチェックを入れます。
L2TPセキュリティ保護を設定する	「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キー(shared secret)を設定します。VPNサーバーで定義されているL2TPトンネル認証のための事前共有キー(shared secret)と同じ文字列を設定します。
DNS検索ドメイン	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。

■ L2TP/IPSec CRT VPN設定

事前に証明書のインストールを行う必要があります。

項目名	説明
VPN名	このVPN接続プロファイル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	VPNサーバーのセキュリティポリシーに合わせて、L2TPトンネル認証を有効にする場合はチェックを入れます。
L2TPセキュリティ保護を設定する	「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キー(shared secret)を設定します。VPNサーバーで定義されているL2TPトンネル認証のための事前共有キー(shared secret)と同じ文字列を設定します。
証明書を設定する	本端末用の証明書を設定します。証明書はあらかじめインストールしておく必要があります。詳しくは、「証明書のインストールについて」（P.6）をご参照ください。
CA証明書を設定する	CA証明書を設定します。証明書はあらかじめインストールしておく必要があります。詳しくは、「証明書のインストールについて」（P.6）をご参照ください。

項目名	説明
DNS検索ドメイン	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。

証明書のインストールについて

L2TP/IPSec CRTを設定する際は、あらかじめ必要な証明書をインストールしておく必要があります。証明書のインストール手順には、WEBサイトに証明書を配置しWEBサイトにアクセスしてダウンロードする方法や、microSDカードにコピーしておく方法などがあります。

証明書をmicroSDカードからインストールする場合、ルートフォルダにサーバー管理者から提供された「.p12」ファイルを配置します。その後、設定メニュー画面で「現在地情報とセキュリティ」→「SDカードからインストール」をタップします。証明書を選択中にパスワード入力画面が表示された場合は、サーバー管理者から指示されたパスワードを入力してください。その後、証明書名の設定画面が表示されます。任意の名称を設定してください。

インストールされた証明書は、L2TP/IPSec CRT設定の「証明書を設定する」項目で選択できるようになります。

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の事前共有キーは暗号化され、端末内に保存されます。
認証情報ストレージのパスワードは、端末の電源オフ、または「設定」→「現在地情報とセキュリティ」の認証情報ストレージにある「安全な認証情報の使用」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」→「現在地情報とセキュリティ」→「パスワードの設定」をタップしてパスワードの変更ができ、「設定」→「現在地情報とセキュリティ」→「ストレージの消去」をタップし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

1 VPN設定画面で接続するVPN名をタップする

2 ユーザー認証ダイアログが表示されたら、必要な認証情報を入力し、「接続」をタップする

接続すると通知アイコンが表示されます。

VPNの切断

1 通知パネルを開き、VPN接続中を示す通知をタップする

VPN接続は切断され、切断が完了すると通知パネルに表示されます。

■ 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。
本書の一部または全部を無断で複写することは禁止されています。また、個人としてご利用になるほかは、著作権法上、弊社に無断では使用できませんのでご注意ください。
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。
「Android」は、Google Inc. の商標または登録商標です。
その他、本書で記載しているシステム名、製品名などは各社の商標または登録商標です。
なお、本文中では TM マーク、® マークは表記しておりません。

2012年3月　第7版
1250-1800.7