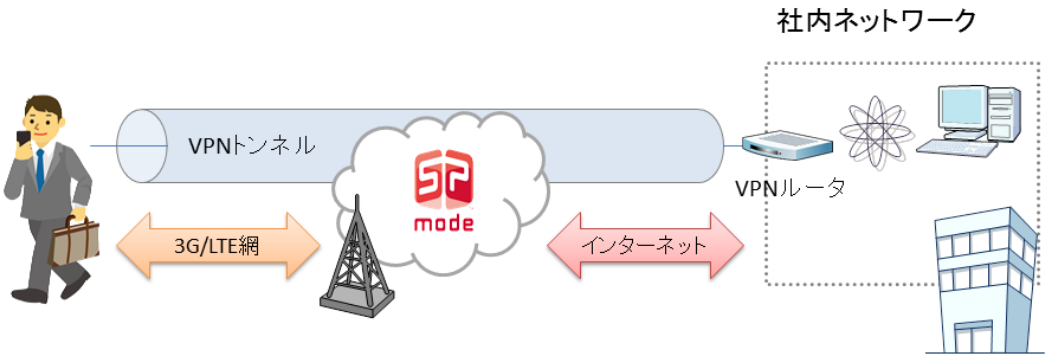
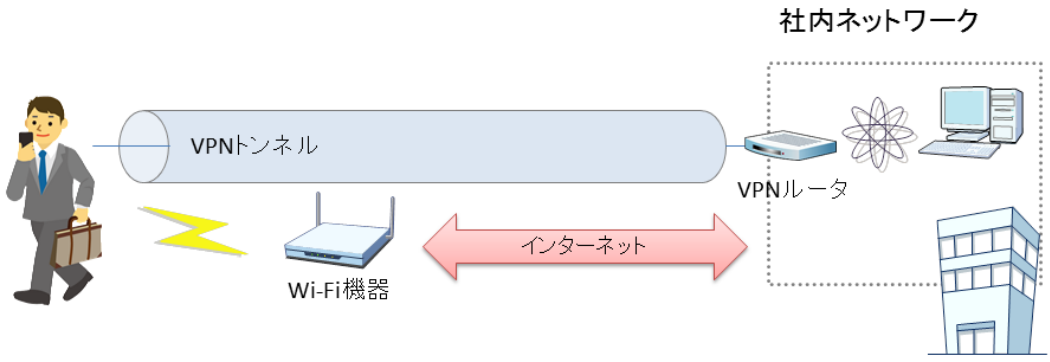
VPN

1. 概要

VPN とは Virtual Private Network の略称であり、インターネット等を介して端末と企業等のプライベートネットワーク（以下、「社内ネットワーク」とします）を接続する技術のことです。トンネリングや暗号化の技術により仮想的な専用線を実現し、セキュアな社内ネットワークへの接続を確立します。

NTT ドコモの提供する Android スマートフォン/タブレットにおいては、「L2TP/IPSec」、「IPSec Xauth」のプロトコルについて動作確認を行っております。





2. 機能（標準サポートプロトコル）

NTT ドコモの Android スマートフォン/タブレットでは標準で対応している VPN プロトコルがあります。本章では、動作確認を実施している「L2TP/IPSec」、「IPSec Xauth」について記載します。

◆ L2TP/IPSec（Layer 2 Tunneling Protocol/ Security Architecture for Internet Protocol）

L2TP は PPTP と L2F（Layer 2 Forwarding）を拡張した VPN 接続用のトンネリングプロトコルです。L2TP は暗号化機能を持たないため、通信データの暗号化機能を持つ IPSec と組み合わせて L2TP/IPSec として使用されます。

L2TP/IPSec を用いた VPN 接続について以下に記載します。なお、本プロトコルでは事前共有鍵（preshared key）にて通信相手の認証を行う「L2TP/IPSec PSK」、及びデジタル証明書(RSA)にて認証を行う「L2TP/IPSec RSA」が用意されております。

<<提供方式・機能>>

以下の方式・機能に対応しております。

・モード：トランスポート

・認証方式：MS-CHAP v2、MS-CHAP、PAP、CHAP

※Cisco ASA では、AAA サーバタイプが LOCAL の場合、CHAP 非対応となります。

・暗号アルゴリズム： 3DES、AES、AES-256

・ハッシュアルゴリズム：SHA-1

・DPD 機能：対応

・NAT トラバーサル：対応

※sp モードで接続する場合は、VPN ルータ側で NAT トラバーサルの設定が必要となります。

<<設定画面>>

L2TP/IPSec 使用時の VPN 設定画面は以下の通りです。

<<接続方法>>

L2TP/IPSec の VPN 接続方法は以下の通りです。接続時の設定により、アカウント情報（ユーザ名/パスワード）を保持することが可能です。

①使用する VPN 設定をタップします。
（ここでは「テスト（L2TP/IPSec PSK）」を選択）

②ユーザ名/パスワードを入力し、
「接続」をタップします。

<<動作確認機器>>

「L2TP/IPSec RSA」は、以下の機器で動作確認を行っております。

機器名	Cisco ASA 5506
製造元	シスコシステムズ合同会社
確認環境	ASA Version 9.5（2）
接続方法	・FOMA/Xi 網から mopera U を経由する通信 ・FOMA/Xi 網から sp モードを経由する通信 ・無線 LAN による通信

※ NTT ドコモでは、上記動作環境にて確認を実施しておりますが、機器としては ASA Version 8.4（1）以降を動作対象としております。

※ d-01K では、VPN 接続を端末から手動切断する際、VPN ルータ上のセッションが削除されません。（2018/2/7 時点）

(FOTA にて対処する予定です)

「L2TP/IPSec PSK」は、以下の機器で動作確認を行っております。

機器名	YAMAHA RTX1210
製造元	ヤマハ株式会社
確認環境	Rev.14.01.14
接続方法	・FOMA/Xi 網から mopera U を経由する通信 ・FOMA/Xi 網から sp モードを経由する通信 ・無線 LAN による通信

※ NTT ドコモでは、上記動作環境にて確認を実施しておりますが、機器としては Rev.14.01.05 以降を動作対象としております。

※ 一部機種（Z-01K、MO-01K 以外の機種）では、ハッシュアルゴリズム「SHA-256」に対応しています。

※ d-01K では、VPN 接続を端末から手動切断する際、VPN ルータ上のセッションが削除されません。（2018/2/7 時点）
(FOTA にて対処する予定です)

◆ IPSec Xauth（Security Architecture for Internet Protocol/eXtended AUTHentication）

IPSec Xauth は IPSec を拡張したプロトコルです。IPSec では基本的にユーザ認証が定義されていないため、Xauth によるユーザ認証を行うことでセキュリティを高めています。

IPSec Xauth を用いた VPN 接続について以下に記載します。なお、本プロトコルでは事前共有鍵（preshared key）にて通信相手の認証を行う「IPSec Xauth PSK」、及びデジタル証明書(RSA)にて認証を行う「IPSec Xauth RSA」が用意されております。

<<提供方式・機能>>

以下の方式・機能に対応しております。

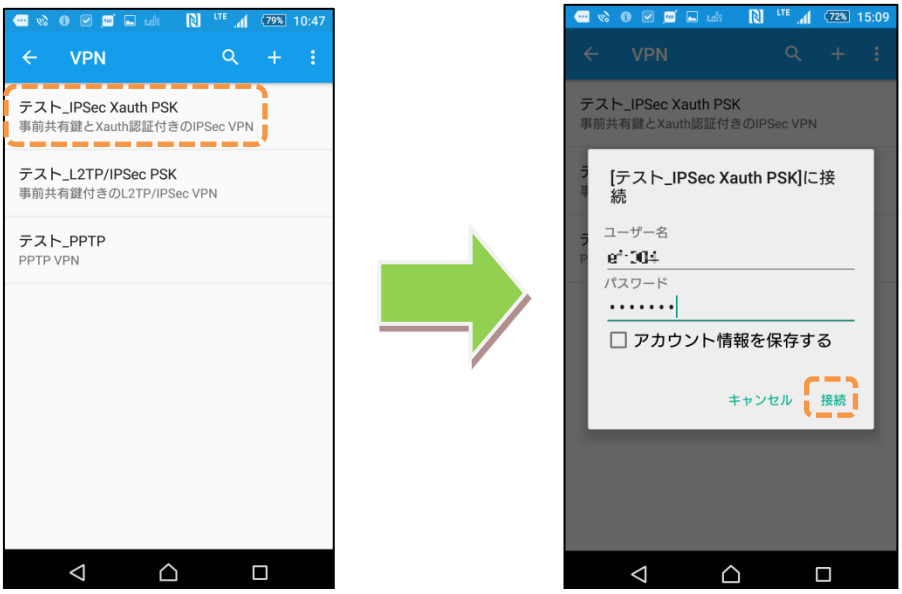
・モード：トンネルモード
・暗号アルゴリズム： 3DES、AES-128、AES-256
・ハッシュアルゴリズム：SHA-1
・DPD 機能：対応
・NAT トラバーサル：対応
※sp モードで接続する場合は、VPN ルータ側で NAT トラバーサルの設定が必要となります。

<<設定画面>>

IPSec Xauth 使用時の VPN 設定画面は以下の通りです。

<<接続方法>>

IPSec Xauth の VPN 接続方法は以下の通りです。接続時の設定により、アカウント情報（ユーザ名/パスワード）を保持することが可能です。



①使用する VPN 設定をタップします。
（ここでは「テスト（IPSec Xauth PSK）」を選択）

②ユーザ名/パスワードを入力し、
「接続」をタップします。

<<動作確認機器>>

以下の機器について動作確認を行っております。

機器名	Cisco ASA 5506
製造元	シスコシステムズ合同会社
確認環境	ASA Version 9.5（2）
接続方法	・FOMA/Xi 網から mopera U を経由する通信 ・FOMA/Xi 網から sp モードを経由する通信 ・無線 LAN による通信

※ d-01K では、VPN 接続を端末から手動切断する際、VPN ルータ上のセッションが削除されません。（2018/2/7 時点）
(FOTA にて対処する予定です)

3. 注意事項

- 機種により対応状況や操作方法が異なる場合があります。
- 本ドキュメントの掲載内容について、お客様環境での動作を完全に保証するものではございません。
- 本ドキュメント掲載のサービス内容、商品の仕様・性能などは、予告なしに変更する場合があります。
- 本ドキュメント掲載のアクセスフロー、URL などは、予告なしに変更する場合があります。
- 掲載されている会社名、商品名は、各社の商標または登録商標です。
- 本ドキュメントから許可なく転記、複写することを固く禁じます。

4. お問い合わせ先

- VPN ルータ製品の詳細、設定方法については、VPN ルータ販売店または製造元ベンダにお問い合わせください。

  ■ VPN ルータ製品：Cisco ASA 5506
  【シスコシステムズ合同会社】
  https://www.cisco.com/web/JP/index.html

  ■ VPN ルータ製品：YAMAHA RTX1210
  【ヤマハ株式会社】
  http://jp.yamaha.com/

- 機種毎の対応状況、操作方法、動作確認状況、及びその他のご不明な点につきましては下記窓口までメールにてお問い合わせください。
  【NTT ドコモお客様窓口】
  http://www.nttdocomo.co.jp/biz/support/