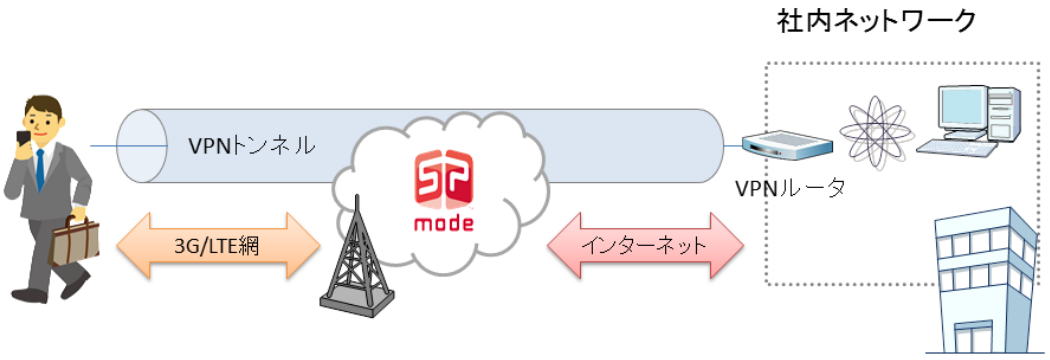
VPN

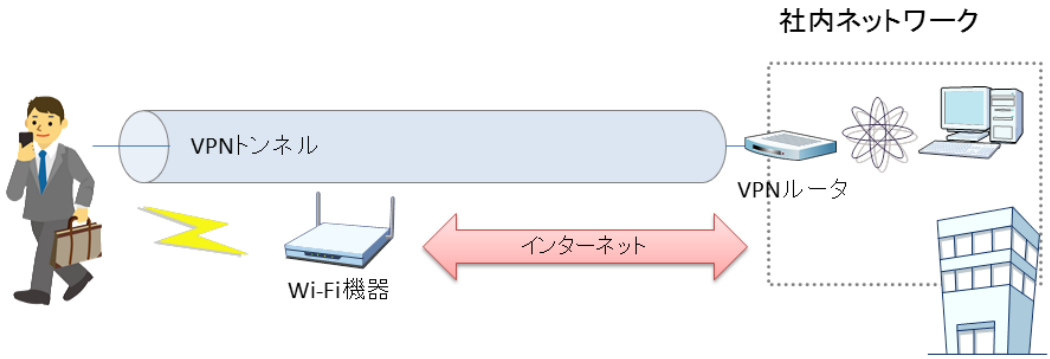
1. 概要

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「SECURITY for Biz」対応スマートフォン（タブレットも含み、以下同様とします）においては、「PPTP」、「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。

さらに、「SECURITY for Biz」対応スマートフォンの一部機種においては、シスコシステムズ合同会社の提供するクライアントアプリ「AnyConnect®」、ジュニパーネットワークス株式会社の提供する「Junos® Pulse」、及び F5 ネットワークスジャパン株式会社の提供する「F5 BIG-IP® Edge Client™」を利用した「SSL-VPN」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）

「SECURITY for Biz」対応スマートフォン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、NTT ドコモで動作確認を実施している「PPTP」、「L2TP/IPSec」、「IPSec Xauth」について記載します。

◆ PPTP（Point-to-Point Tunneling Protocol）

PPTP は通信プロトコルである PPP（Point-to-Point Protocol）を IP レイヤで機能するように拡張したトンネリングプロトコルです。

PPTP を用いた VPN 接続について以下に記載します。

<<提供方式>>

以下の方式に対応しております。

・認証方式：MS-CHAP v2、MS-CHAP、PAP、CHAP

・暗号化方式：なし、MPPE（PPP 暗号化）

※ MPPE を用いる場合、認証方式は MS-CHAP v2 または MS-CHAP になります。

<<設定画面>>

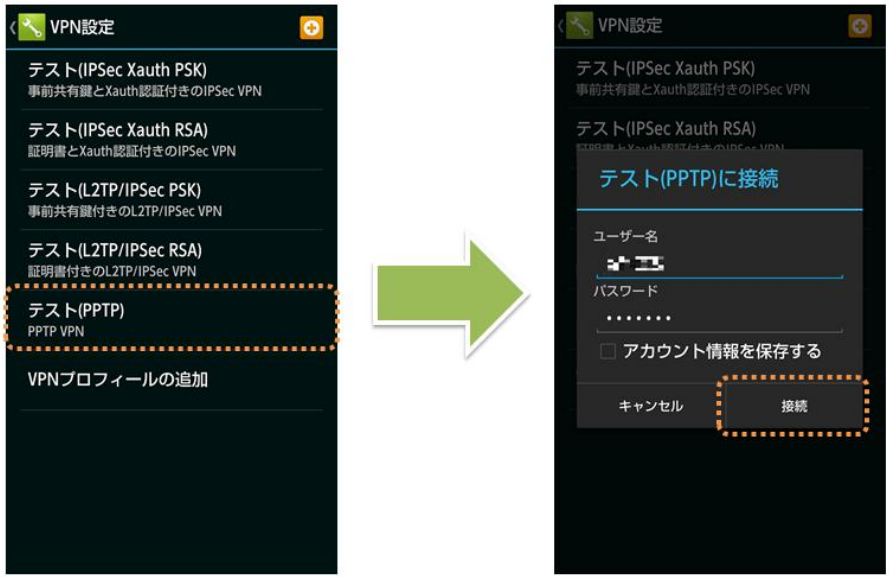
PPTP 使用時の VPN 設定画面は以下の通りです。

PPTP

※ 本ドキュメントに掲載している端末キャプチャ画像には説明のため AQUOS PHONE ZETA（SH-06E）を使用しております。

<<接続方法>>

PPTP 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（PPTP）」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	YAMAHA RTX1200
製造元	ヤマハ株式会社
確認環境	Rev.10.01.38
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 （ルータ側で PPTP パススルー設定が必要）

※ PPTP について、下記の技術情報が公開されています。
参考：JPCERT コーディネーションセンターによる注意喚起
（http://www.jpcert.or.jp/at/2012/at120027.html）

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

L2TP は PPTP と L2F（Layer 2 Fowarding）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

・暗号アルゴリズム： 3DES、AES、AES-256

・ハッシュアルゴリズム：MD5、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。

L2TP/IPSec PSK

L2TP/IPSec RSA

<<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>>

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® ASA5505
製造元	シスコシステムズ合同会社
確認環境	ASA Version 8.4（5）
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 8.0（4）以降を動作対象としております。

以下の機器は、「L2TP/IPSec PSK」のみ動作確認を行っております。（「L2TP/IPSec RSA」については動作確認外となります）

機器名	YAMAHA RTX1200
製造元	ヤマハ株式会社
確認環境	Rev.10.01.38
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.10.01.36 以降を動作対象としております。

※　一部機種においてはハッシュアルゴリズム「SHA-256」に対応しています。

機器名	CentreCOM AR560S
製造元	アライドテレシス株式会社
確認環境	Version 2.9.2-07
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 Version 2.9.2-07 以降を動作対象としております。

◆ **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：MD5、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。

IPSec Xauth PSK

IPSec Xauth RSA

<<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 ASA5505
製造元	シスコシステムズ合同会社
確認環境	ASA Version 8.4（5）
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

3. 機能（SSL-VPN）

SSL-VPN では、セッション層の暗号化プロトコルである SSL を用いて VPN 接続を実現しています。SSL-VPN を使用する場合、各ソリューションのクライアントアプリを導入する必要があります。

本章では、NTT ドコモで動作確認を実施している「AnyConnect」「Junos Pulse」「F5 BIG-IP Edge Client」について記載します。なお、各クライアントアプリは最新バージョンのご利用を推奨します。

◆ AnyConnect

シスコシステムズ合同会社の提供する「AnyConnect」について以下に記載します。

<<導入アプリ>>

AnyConnect による SSL-VPN 接続では、以下のクライアントアプリを導入する必要があります。

アプリ名	AnyConnect ICS+
開発者	Cisco Systems, Inc.
入手先	Google Play™

※ 一部機種においては、個別にアプリが用意されています。

<<動作確認機器>>

AnyConnect による SSL-VPN 接続では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 ASA5505
製造元	シスコシステムズ合同会社
確認環境	ASA Version 8.4（5）
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

※ AnyConnect の詳細につきましては、以下の URL をご参照ください。
（https://play.google.com/store/apps/details?id=com.cisco.anyconnect.vpn.android.avf）

◆ Junos Pulse

ジュニパーネットワークス株式会社の提供する「Junos Pulse」について以下に記載します。

<<導入アプリ>>

Junos Pulse による SSL-VPN 接続では、以下のクライアントアプリを導入する必要があります。

アプリ名	Junos Pulse
開発者	Juniper Networks, Inc. and Affiliates
入手先	Google Play

※　一部機種においては、個別にアプリが用意されています。

<<動作確認機器>>

Junos Pulse による SSL-VPN 接続では以下の機器について動作確認を行っております。

機器名	SA2500
製造元	ジュニパーネットワークス株式会社
確認環境	7.1R6(build 20169)
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

※　Junos Pulse の詳細につきましては、以下の URL をご参照ください。

（https://play.google.com/store/apps/details?id=net.juniper.junos.pulse.android）

◆ F5 BIG-IP Edge Client

F5 ネットワークスジャパン株式会社の提供する「F5 BIG-IP Edge Client」について以下に記載します。

<<導入アプリ>>

F5 BIG-IP Edge Client による SSL-VPN 接続では、以下のクライアントアプリを導入する必要があります。

アプリ名	F5 BIG-IP Edge Client
開発者	F5 BIG-IP Edge Client Inc.
入手先	Google Play

※　一部機種においては、個別にアプリが用意されています。

<<動作確認機器>>

F5 BIG-IP Edge Client による SSL-VPN 接続では以下の機器について動作確認を行っております。

機器名	F5 BIG-IP Edge Gateway™
製造元	F5 ネットワークスジャパン株式会社
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

※　F5 BIG-IP Edge Client の詳細につきましては、以下の URL をご参照ください。
（https://play.google.com/store/apps/details?id=com.f5.edge.client_ics）

4. 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。

5. 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 ASA5505
【シスコシステムズ合同会社】
http://www.cisco.com/web/JP/index.html

■ VPN ルータ製品：YAMAHA RTX1200
【ヤマハ株式会社】
http://jp.yamaha.com/

■ VPN ルータ製品：CentreCOM AR560S
【アライドテレシス株式会社】
http://www.allied-telesis.co.jp/

■ VPN ルータ製品：SA2500
【ジュニパーネットワークス株式会社】
http://www.juniper.net/jp/jp/

■ VPN ルータ製品：F5 BIG-IP Edge Gateway
【F5 ネットワークスジャパン株式会社】
http://www.f5networks.co.jp/

・ 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.docomo.biz/d/contact_wp3