FUJITSU Hybrid IT Service FJcloud-O
SSL-VPNサービス 切替ガイド

対象リージョン
東日本第３リージョン
西日本第３リージョン

2024年11月18日 1.3版
富士通株式会社

改訂履歴

版数	改訂日	概要
1.0	2024/4/16	新規作成
1.1	2024/8/1	・SSL-VPN V3 Connectionの概要 - 料金表へのリンクを追加 ・Step5：証明書の準備 - ルート証明書の形式について追加 - openssslのバージョンについて追加 ・Step7：接続設定ファイルの作成 - proxy経由の接続設定について追加 ・SSL-VPN V3 Connection利用時のトラブルシューティング - proxy設定について追加
1.2	2024/9/17	・Step2：SSL-VPN V3 Connectionの作成 - リクエストサンプルを改善
1.3	2024/11/18	・SSL-VPN V3 Connection切替作業時の注意事項 - セッション数拡張オプション未提供についての記載を削除 ・Step2：SSL-VPN V3 Connectionの作成 - 使用可能フレーバの制限についての記載を削除 ・SSL-VPN V3 Connectionでのセッション数拡張 - セッション拡張方法についての記載を修正

SSL-VPNサービスの切替について

- FJcloud-O（東3／西3リージョン）で提供しておりますSSL-VPN V2 Connection（以降SSL-VPN V2）は 2024/8/31 をもって新規受付停止・サポート終了となります。

  サポート終了後（2024/8/31）、2024/12/16 まではSSL-VPN V2をご利用いただけますが、2024/12/17以降はSSL-VPN V2が使用不可となります。
  サポート終了後（2024/8/31）は、障害調査や不具合・脆弱性の修正を提供できなくなります。

- 後継製品であるSSL-VPN V3 Connection（以降　SSL-VPN V3）を2024/7/1から提供します。
  SSL-VPN V2 サービス終了までにSSL-VPNの切替・移行をお願いします。

  ※ 東１、２/西１、２リージョンで提供中のSSL-VPN V2 Connectionは対象外です。

SSL-VPN V3 Connectionの概要

- SSL-VPN V3 Connectionでは、お客様のクライアント端末からFJcloud-O上に構築した仮想環境へのセキュアな接続機能（SSL-VPN機能）を提供します。
  SSL-VPN V3とSSL-VPN V2のサービス仕様概要は以下のとおりです。

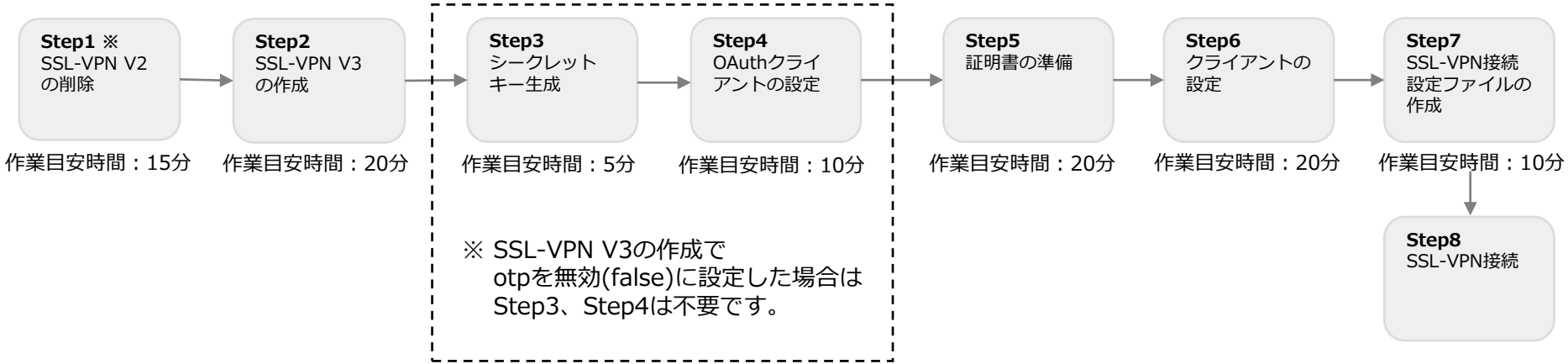
	項目	SSL-VPN V2 Connection	SSL-VPN V3 Connection
1	接続クライアント	SSL-VPN V2 専用クライアントソフト	OpenVPNクライアント
2	利用可能な証明書	FJcloud-O発行のクライアント証明書 自己署名証明書	同左
3	暗号プロトコル	TLS1.2	TLS1.3、TLS1.2
4	スプリットトンネル	なし（フルトンネルのみ提供）	同左
5	多要素認証	なし	あり（TOTP ※1）
6	ご利用料金	同時接続数２０までは無償	有償 ※2

※1 TOTP：Timebase OneTime Password　現在時刻をもとに発行されるワンタイムパスワード

※2 詳細はFJcloud-O 料金表をご確認ください。
https://doc.cloud.global.fujitsu.com/lib/common/jp/price-list/fjcloud/-o/iaas-network/

SSL-VPN V3 Connectionへの切替作業概要

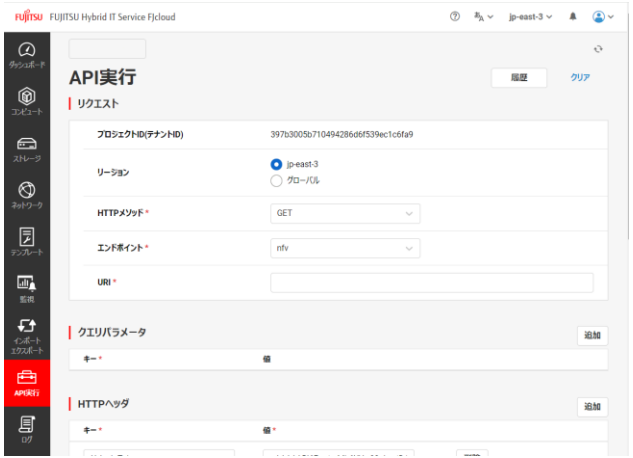
SSL-VPN V3 Connectionへの切替作業の流れは以下のとおりです。



※ SSL-VPN V2を削除できない場合は、
SSL-VPN V3用にサブネット、VPN Serviceを作成し、Step2から作業を実施してください。

SSL-VPN V3 Connection切替作業時の注意事項

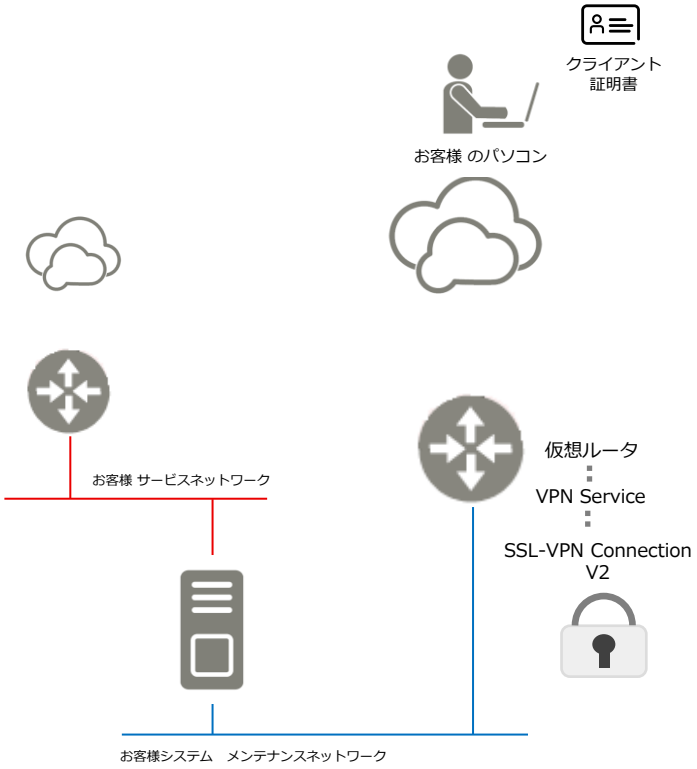
- SSL-VPN V2からSSL-VPN V3への切替にともない、external_address が変更されます。
  接続元（クライアント端末側）で接続制限を実施している環境では、設定の変更をお願いします。
- 本作業はAPI（REST API）で実施します。REST APIを実行できるクライアントアプリ（curl、Postmanなど）をご利用いただくか、IaaSポータルの「API実行」機能をご利用ください。



SSL-VPN V3 Connectionへの切替手順

- 右記の構成例をもとに、SSL-VPN V3への移行手順を次項以降で説明します。
  - SSL-VPN V2を既に利用中
  - FJcloud-O発行のクライアント証明書を利用
  - ワンタイムパスワードを利用

- 手順の中でコマンド例を記載しています。
  APIの詳細は、APIリファレンスを参照してください。
  https://doc.cloud.global.fujitsu.com/lib/iaas/jp/api-reference/v3/web/k5-iaas-api-reference/index.html



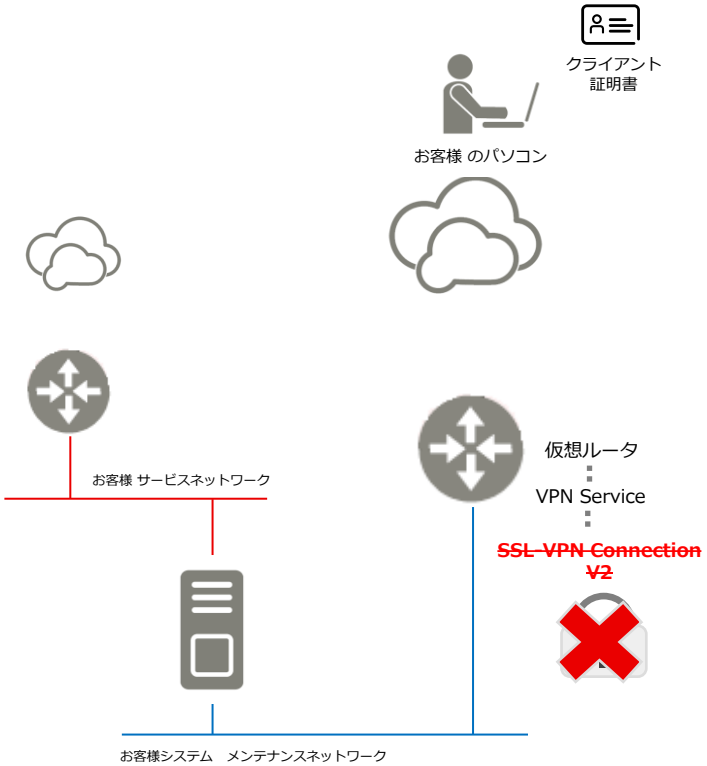
Step1：SSL-VPN V2 Connectionの削除

- 作成済みのSSL-VPN V2を削除します。

  リクエストサンプル
  　DELETE /vpn/nfv/ssl-vpn-v2-connections/{ssl-vpn id}

  ＊ssl-vpn idには対象のSSL-VPN V2のIDを指定してください。

  ＊SSL-VPN V2を設定していたVPN Serviceは削除しないでください。



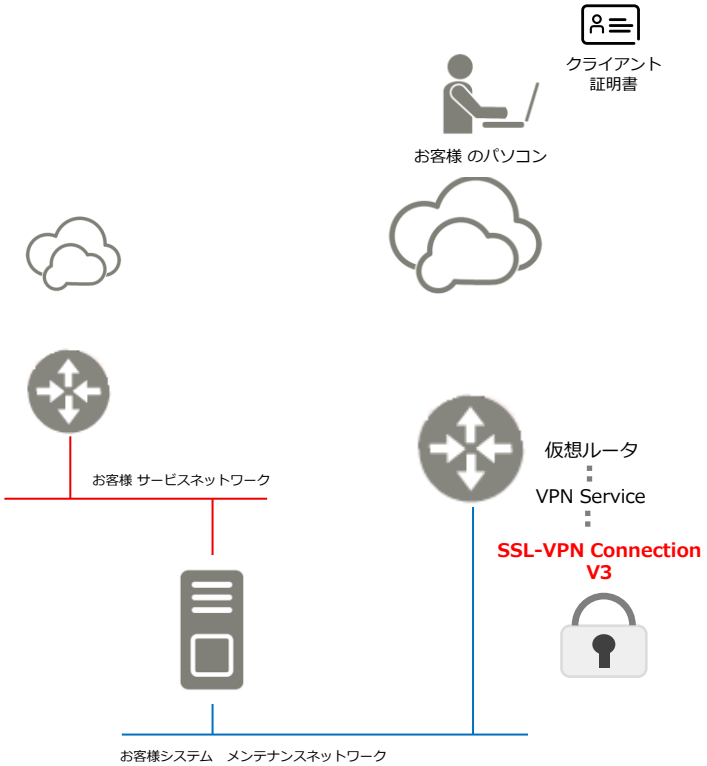
Step2：SSL-VPN V3 Connectionの作成

- VPN Serviceに対してSSL-VPN V3を作成します。

リクエストサンプル

```
POST /vpn/nfv/ssl-vpn-v3-connections
{
  "ssl_vpn_v3_connection": {
      "name": "ssl-vpn",
      "client_address_pool_cidr": "10.8.0.0/24",
      "vpnservice_id": "12345",
      "otp": true,                          ＊1
      "flavor": "small"                     ＊2
  }
}
```

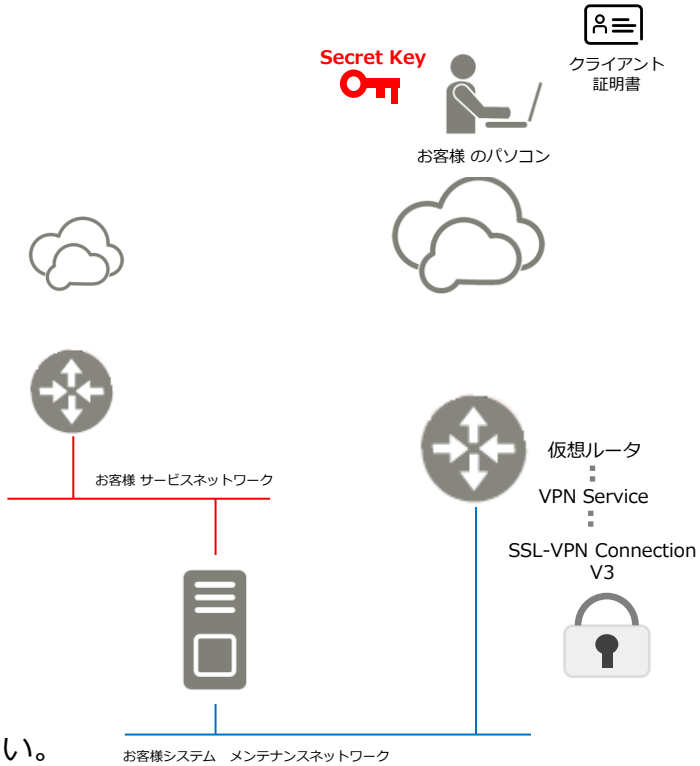
＊1　SSL-VPNの接続認証にワンタイムパスワードを利用
＊2　small（同時接続数20）のSSL-VPNフレーバを利用



Step3：ワンタイムパスワードのシークレットキーを生成

- SSL-VPN接続に利用するワンタイムパスワードの
  シークレットキー（シード）を発行します。

  ※ シークレットキーはユーザごとに必要です。
  ※ シークレットキーは生成後、APIによる確認・参照
  できないため、紛失しないよう管理してください。
  ※ シークレットキーの紛失などにより再発行する場合は、
  該当ユーザのシークレットキーをAPIで無効化（削除）
  したあと、再度シークレットキーを生成してください。



リクエストサンプル

POST /vpn/nfv/ssl-vpn-v3-connections/{ssl-vpn id}/otp

```
{
    "ssl_vpn_v3_connection": {
        "user_id": "aaaaa-aaaaa-aaaa-aaaaa"
    }
}
```

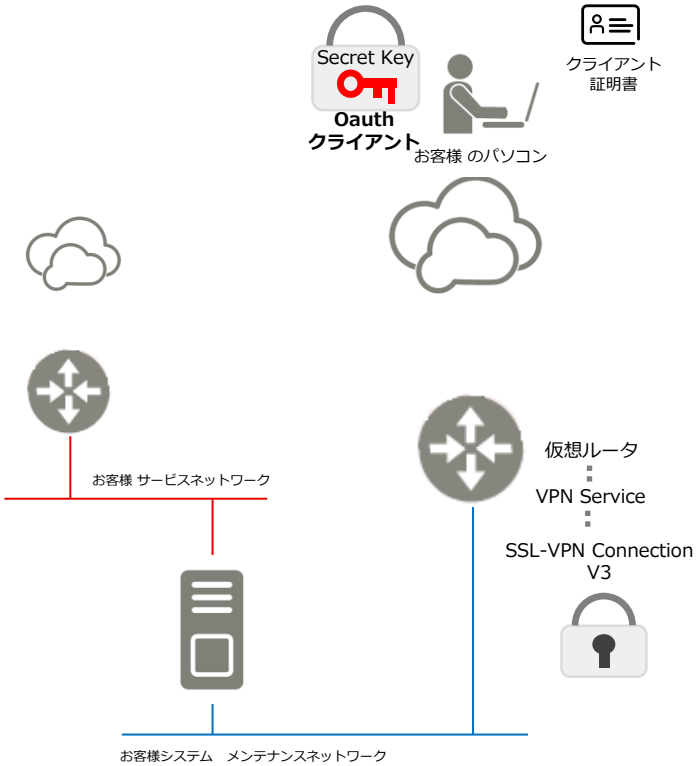
＊ssl-vpn id はStep2で作成したSSL-VPN V3のIDを指定してください。
＊user_id はSSL-VPN V3を作成したprojectに所属している
ユーザIDを指定してください。
＊APIの実行ユーザとuser_idは一致させてください。

Step4： OAuthクライアントの設定

- SSL-VPN接続で利用するワンタイムパスワードを発行できるクライアントソフトウェアを設定します。

SSL-VPN接続ではTOTPによる認証を行っています。
TOTPをサポートするOAuthクライアントに、
Step3で発行したシークレットキー（シード）を設定し、
ワンタイムパスワードを発行できるようにしてください。

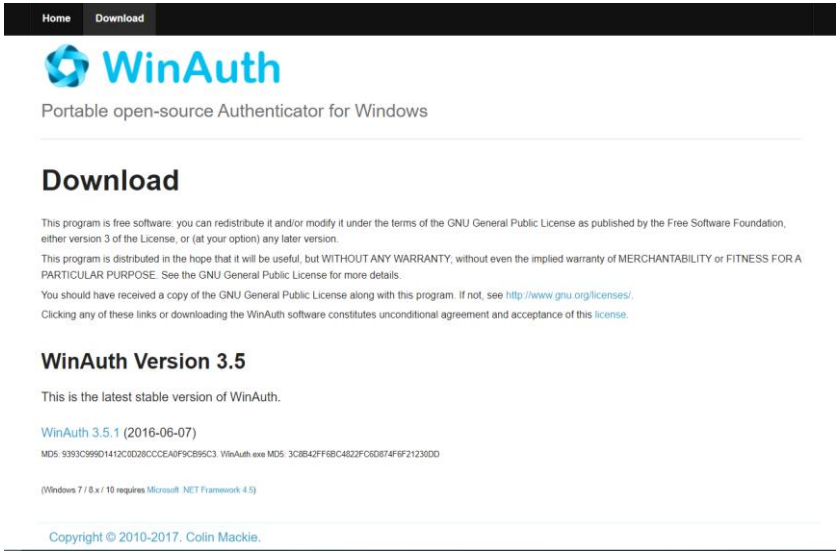
※ OAuthクライアントは、Microsoft Authenticator、Google Authenticator、WinAuth、 Authyなどが該当します。



（参考） OAuthクライアントの導入例

- Windowsで利用可能なWinAuthの導入手順を説明します。

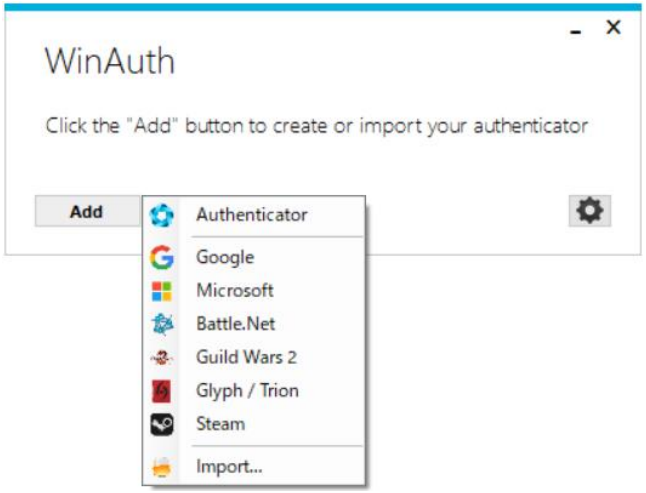
手順１：Webページ（https://winauth.github.io/winauth/download.html）から
WinAuthをダウンロードしてください。



（参考） OAuthクライアントの導入例

手順２：ダウンロードしたzipファイルを解凍し、WinAuth.exeを起動してください。

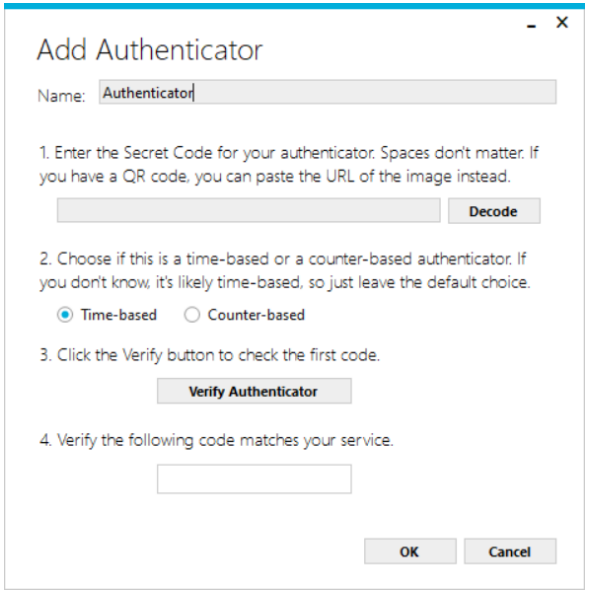
手順３：WinAuth.exeを起動し、「Add」→「Authenticator」をクリックしてください。



（参考） OAuthクライアントの導入例

手順４：Nameに任意の名称を設定し、Step3で取得したシークレットキーを入力してください。

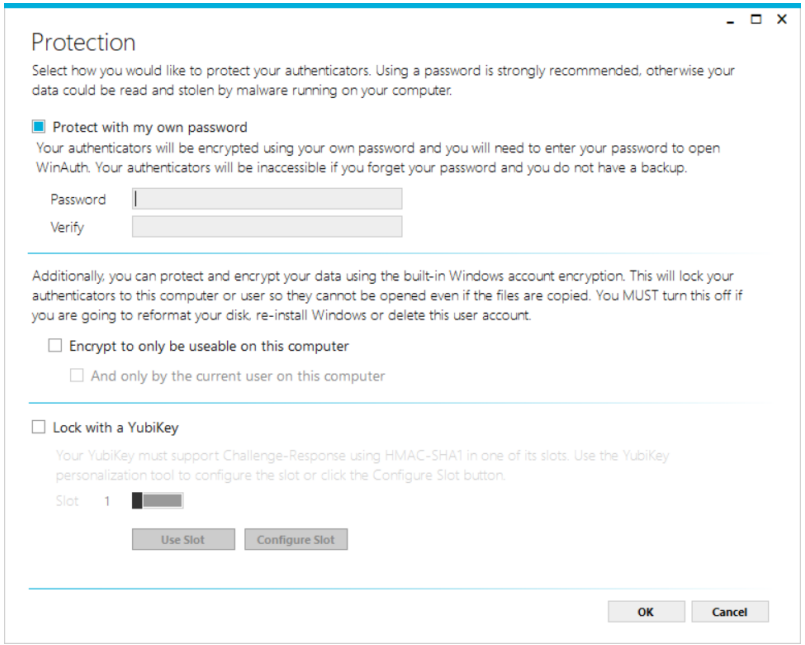
手順５：「Verify Authenticator」をクリックし、
「Verify the following code matches your service」に６桁のワンタイムパスワードが表示されることを確認できたら「OK」をクリックしてください。



（参考） OAuthクライアントの導入例

以下、必要に応じて設定してください。（任意）

手順６：シークレットキーをパスワードで保護する必要がある場合は、Password、Verifyに任意のパスワードを設定してください。

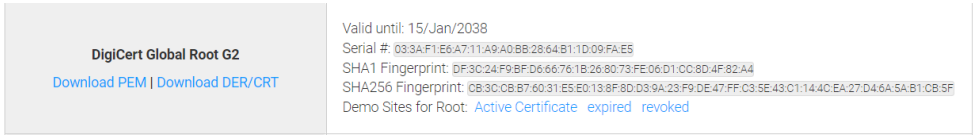


Step5：証明書の準備

- SSL-VPN接続でクライアント側が利用する証明書を準備します。

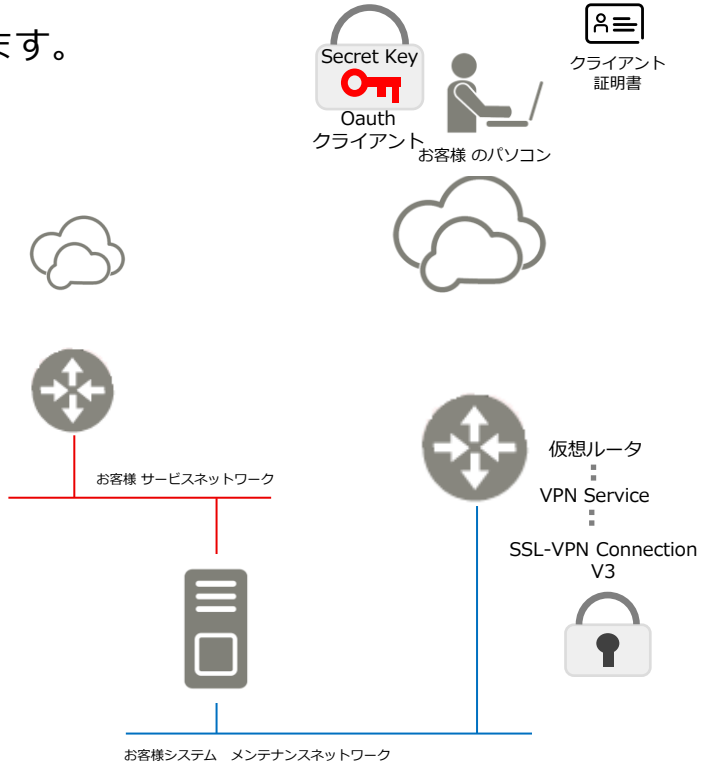
以下のDigiCertのHPから、CA証明書として
ルート証明書[DigiCert Global Root G2]をダウンロードします。

https://www.digicert.com/kb/digicert-root-certificates.htm



※ pem形式のルート証明書をダウンロードしてください。

以降の手順で利用するため、
ファイル名を「**ca.crt**」にリネームしてください。



Step5：証明書の準備

FJcloudポータルからクライアント証明書を取得します。
詳細は以下のURLを参照してください。
https://doc.cloud.global.fujitsu.com/lib/common/jp/FJCS_General_ja/FJCSPortal_UserGuide_ja/section3-3/#_15

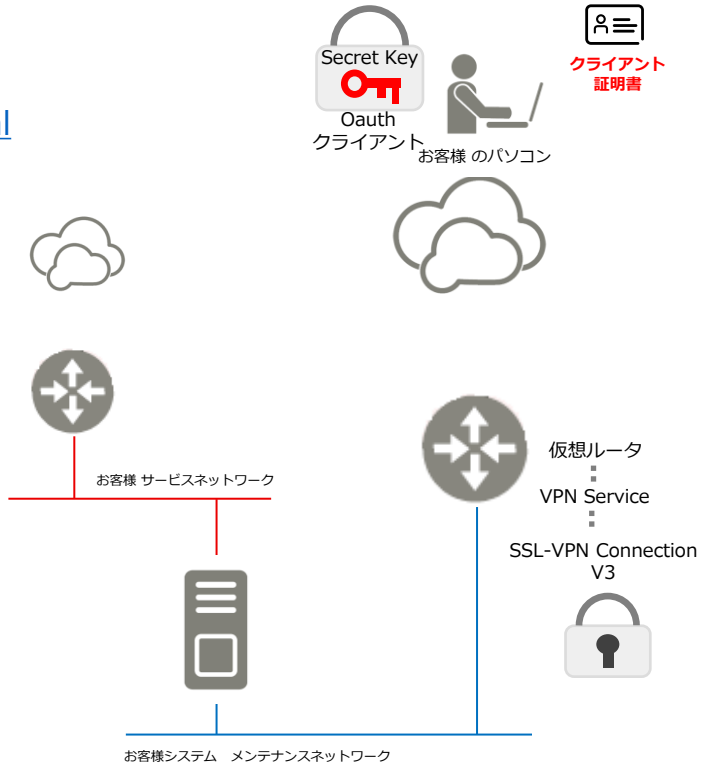
クライアント証明書取得後、OpenVPNクライアントで利用するため
openssslコマンドを用いてpem形式へ変換し、秘密鍵を抽出します。

- 証明書形式の変更
  openssl pkcs12 -in <クライアント証明書> -clcerts -nokeys -out client.crt
- 秘密鍵の抽出
  openssl pkcs12 -in <クライアント証明書> -clcerts -out client.key

コマンド例
openssl pkcs12 -in EndUser.p12 -clcerts -nokeys -out client.crt
openssl pkcs12 -in EndUser.p12 -clcerts -out client.key

※ 実行するときにパスワードを要求されます。
　証明書を発行する際に設定したパスワードを入力してください。

※OpenSSL 3.0以降で実行する場合、-legacy を追加してください。



Step6：クライアントの設定

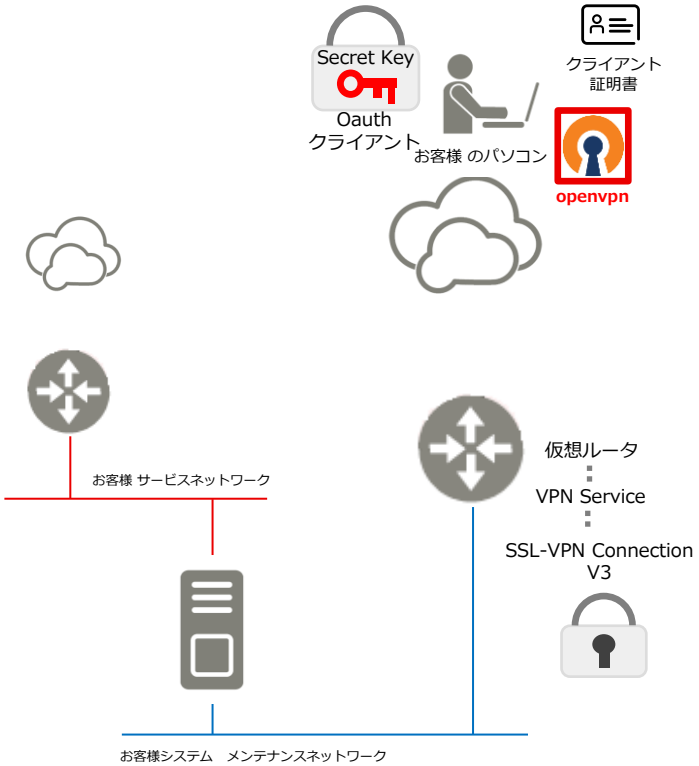
- SSL-VPN接続クライアント（OpenVPNクライアント）をインストールします。

  OpenVPNクライアントを以下からダウンロードして、
  クライアント端末にインストールしてください。
  https://openvpn.net/community-downloads/

  versionはOpenVPN 2.6.10をご利用ください。

  クライアントのインストール後、Step5で準備した
  各証明書を所定のフォルダに格納してください。
  - CA証明書(ca.crt)
  - クライアント証明書(client.crt)
  - クライアント秘密鍵(client.key)

  ※ OpenVPNクライアントのデフォルトの証明書格納場所は、
  C:¥Program Files¥OpenVPN¥config です。

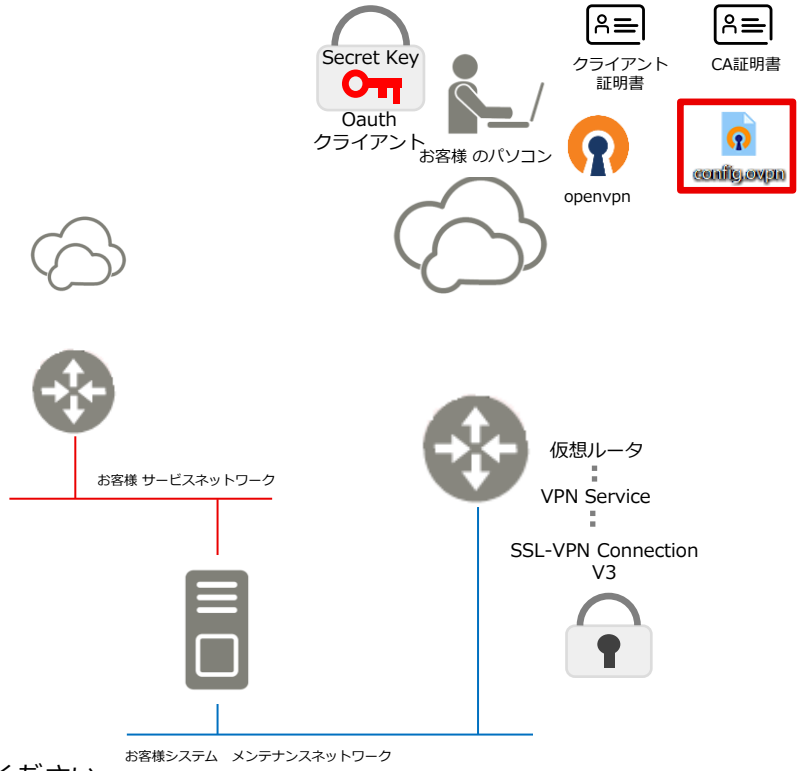


Step7：接続設定ファイルの作成

- SSL-VPN接続で利用する
  クライアント接続設定ファイルを作成します。

  以下のサンプルテンプレートを参照して、
  接続設定ファイル（拡張子は".ovpn"）を作成し
  C:¥Program Files¥OpenVPN¥config に格納してください。

```
client
dev tun
proto tcp
remote xxx.xxx.xxx.xxx 443   ※1
resolv-retry infinite
nobind
auth-user-pass                ※2
static-challenge pin otp      ※2
persist-key
persist-tun
ca ca.crt                  ※3
cert client.crt            ※3
key client.key             ※3
remote-cert-tls server
data-ciphers AES-256-GCM
http-proxy yyy.yyy.yyy.yyy zzzz stdin basic   ※4
```



※1 SSL-VPN V3のexternal_addressを指定してください。
※2 ワンタイムパスワードを利用する場合は記載してください。
※3 サーバ証明書のCA証明書、クライアント証明書、秘密鍵の格納場所を指定してください。
※4 proxyサーバのアドレス、ポートを指定してください。
　　proxy経由で接続しない場合は、該当行を削除してください。

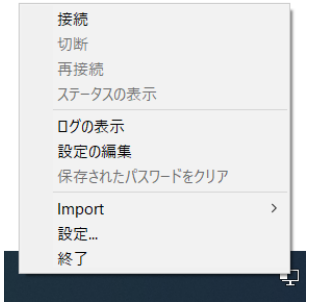
Step8：SSL-VPN接続する

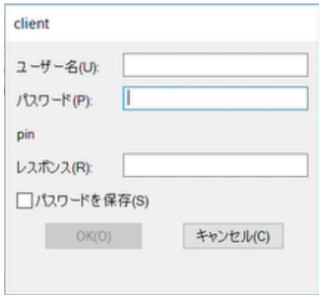
- SSL-VPN接続します。

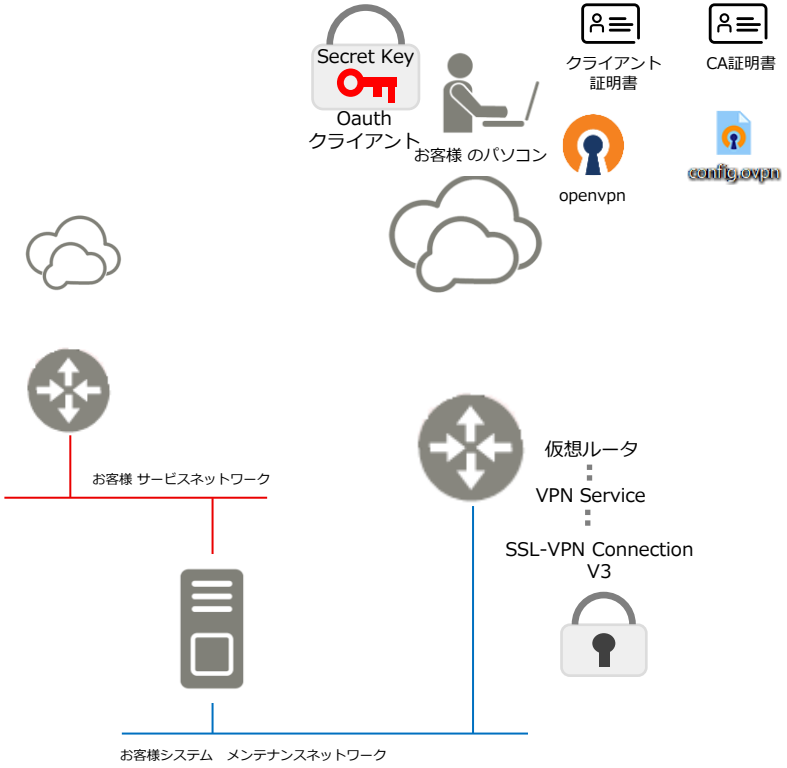
タスクトレイにあるOpenVPNアイコンを右クリックし、
「接続」を選択してください。

ワンタイムパスワードを有効にしている場合、
ユーザ認証を要求されます。

ユーザ名　：ユーザID
パスワード：空欄
レスポンス：OAuthクライアントで発行したワンタイムパスワード







SSL-VPN V3 Connectionでのセッション数拡張

- SSL-VPN接続のセッション数を255(※)まで希望する場合、セッション数拡張用のフレーバー(normal)を指定してSSL-VPNコネクションを作成してください。セッション数20でSSL-VPNコネクションを作成した場合は、セッション数拡張用のフレーバー(normal)を指定してSSL-VPNコネクションを更新してください。

  ※ SSL-VPN V2 Connectionのセッション拡張オプション
  （1コネクション当たり255セッション）相当

SSL-VPN V3 Connection利用時のトラブルシューティング

- SSL-VPN V3の作成が失敗する
  - VPN Service、SSL-VPN V2の状態をご確認ください。

    1つのVPN Serviceに対し、SSL-VPNは1つのみ設定可能です。
    SSL-VPN V2またはIPsec site connectionが設定されているVPN ServiceにSSL-VPN V3を作成できないため、
    新規にVPN Serviceを作成するか該当のSSL-VPN V2またはIPsec site connectionを削除してください。

- SSL-VPN V3への接続が失敗する
  - OpenVPNクライアントのバージョンをご確認ください。

    検証済みバージョンは、「2.6.10」です。
    これ以外のバージョンでも動作する可能性はありますが、未検証となるため「2.6.10」を利用してください。
  - 接続ユーザのシークレットキーの発行をご確認ください。

    ワンタイムパスワードによる接続では、ユーザごとに異なるシークレットキーを発行する必要があります。
    異なるユーザが発行したシークレットキーによるワンタイムパスワードを利用すると、接続に失敗します。
  - OAuthクライアントを動作させている端末の時刻同期をご確認ください。

    TOPTベースのため端末の時刻が大幅にずれている場合、正常にワンタイムパスワードを発行できません。
    時刻同期を行ったあと、再度ワンタイムパスワードの発行、接続を試行してください。
  - proxy設定をご確認ください。

    proxy経由で接続するには追加の設定が必要になる場合があります。
    Step7に記載の proxy設定を参照しコンフィグが適切に設定されているか確認してください。

Thank you