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4月16日 1.0版
富士通株式会社

改訂履歴

版数	改訂日	変更箇所	概要
1.0	2024/4/16	全体	新規作成

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から提供予定です。
  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

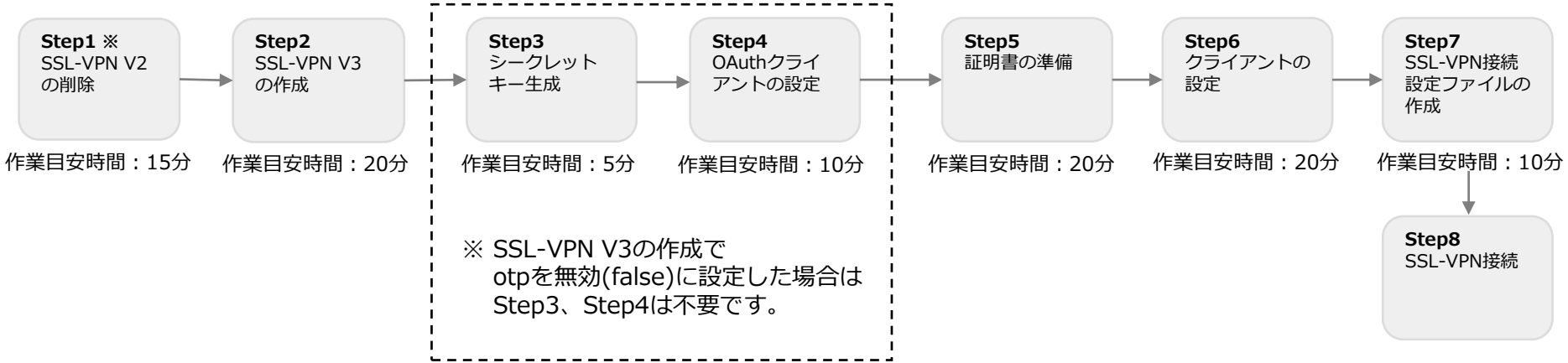
- SSL-VPN V3 Connectionでは、お客様のクライアント端末からFJcloud-O上に構築した仮想環境へのセキュアな接続機能（SSL-VPN機能）を提供します。
  SSL-VPN V3とSSL-VPN V2のサービス仕様概要は以下のとおりです。

	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 ※）
6	ご利用料金	同時接続数２０までは無償	未定（2024年5月公開予定）

※ 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

SSL-VPN V3 Connectionへの切替作業概要

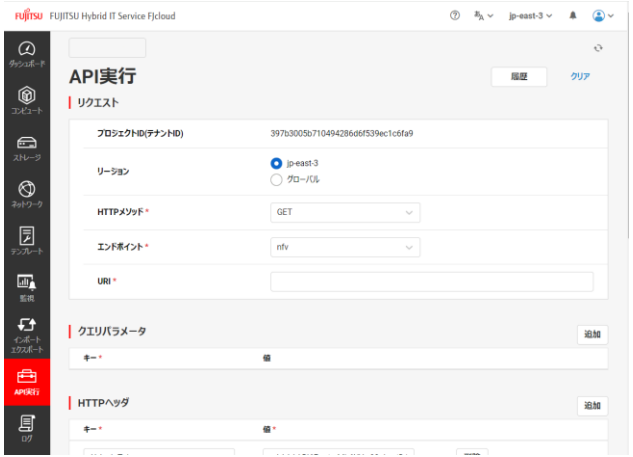
SSL-VPN V3 Connectionへの切替作業の流れは以下のとおりです。



※ 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 V3提供開始時点（2024/7/1）では、セッション数拡張オプションが未提供となっております。
  SSL-VPN V2のセッション数拡張オプション相当の機能が必要な場合は、ヘルプデスクへお問い合わせください。
  ※ 詳細は、「p21 SSL-VPN V3 Connectionでのセッション数拡張」を参照してください。
- 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。

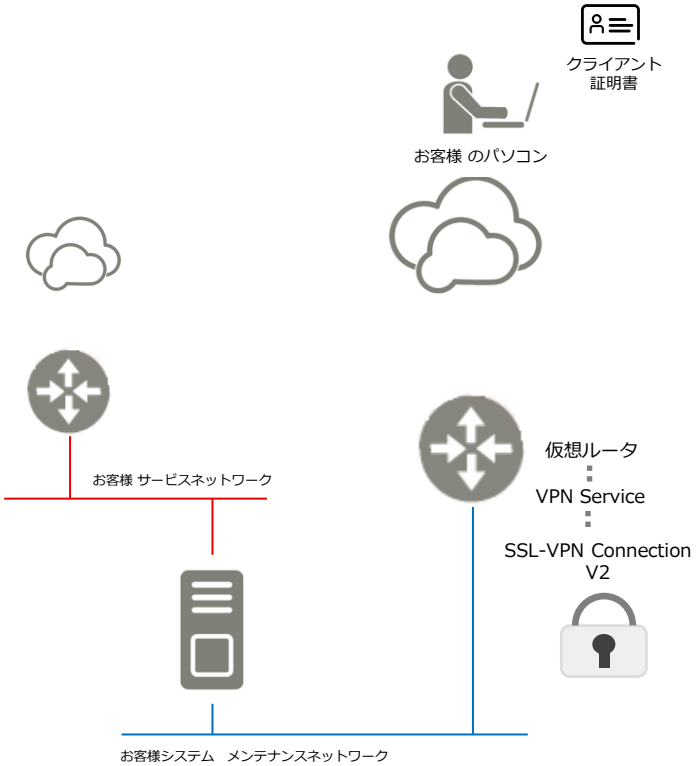


SSL-VPN V3 Connectionへの切替手順

- 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

  ※ APIリファレンスの公開は2024年6月です。



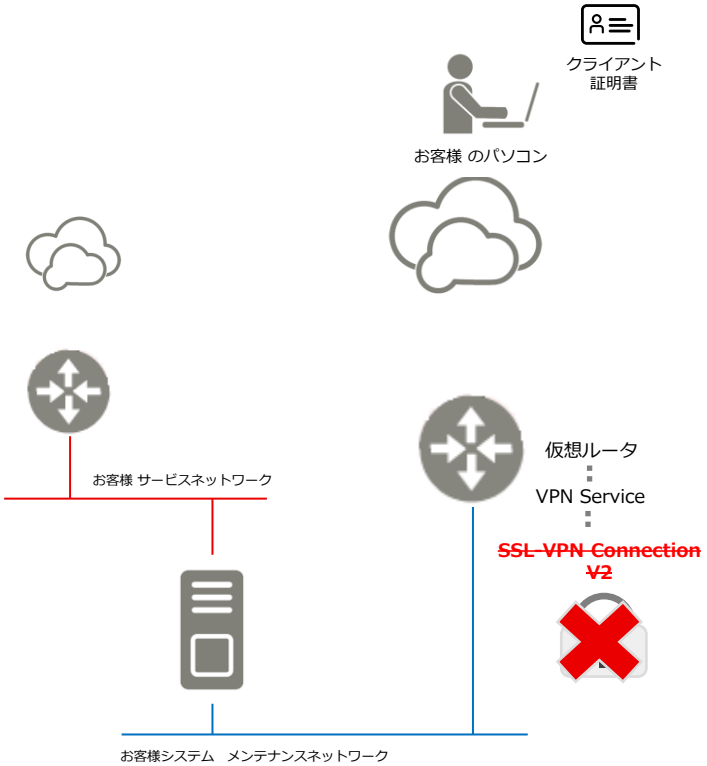
Step1：SSL-VPN V2 Connectionの削除

- 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。



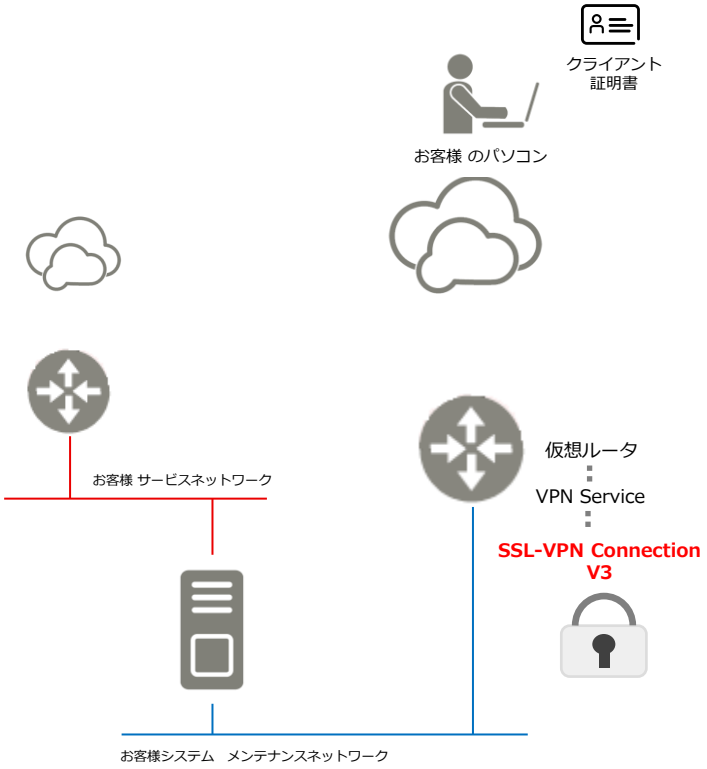
Step2：SSL-VPN V3 Connectionの作成

- 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
  }
}
```

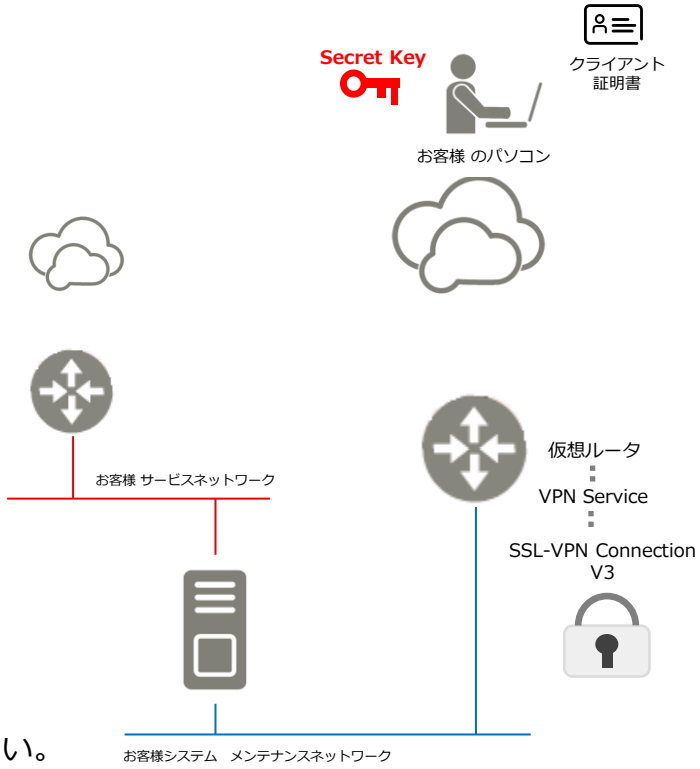
＊1　SSL-VPNの接続認証にワンタイムパスワードを利用
＊2　small（同時接続数20）のSSL-VPNフレーバを利用
　　※現在、smallフレーバのみ提供しています。



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"
    }
}
```

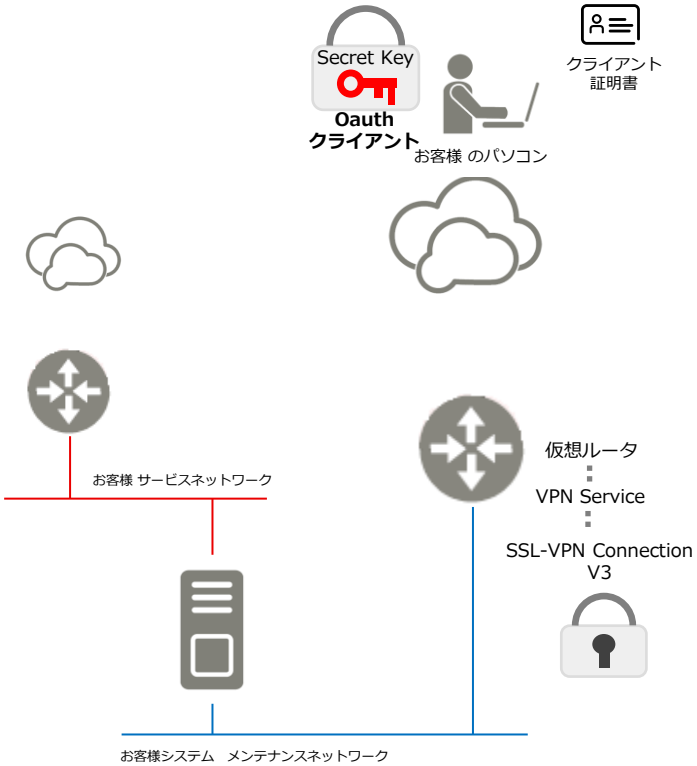
＊ssl-vpn id はStep2で作成したSSL-VPN V3のIDを指定してください。
＊user_id はSSL-VPN V3を作成したprojectに所属している
ユーザIDを指定してください。
＊APIの実行ユーザとuser_idは一致させてください。

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。

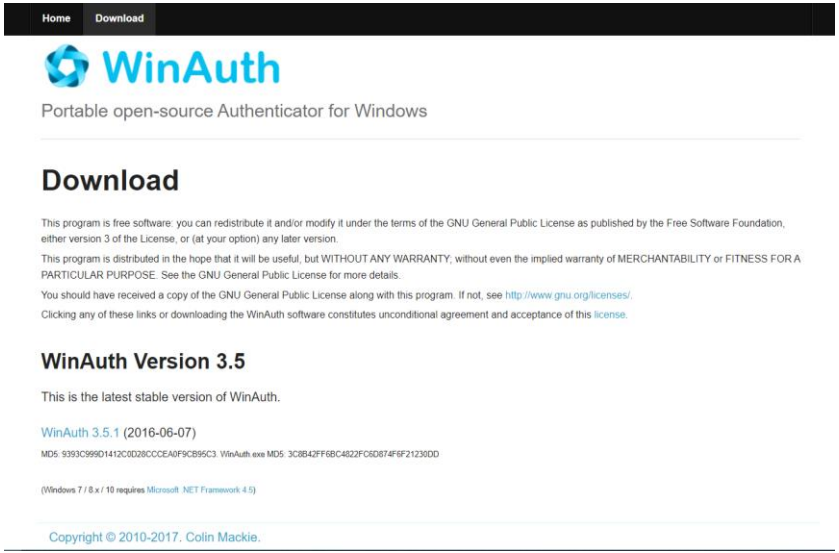
※ OAuthクライアントは、Microsoft Authenticator、Google Authenticator、WinAuth、 Authyなどが該当します。



（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。

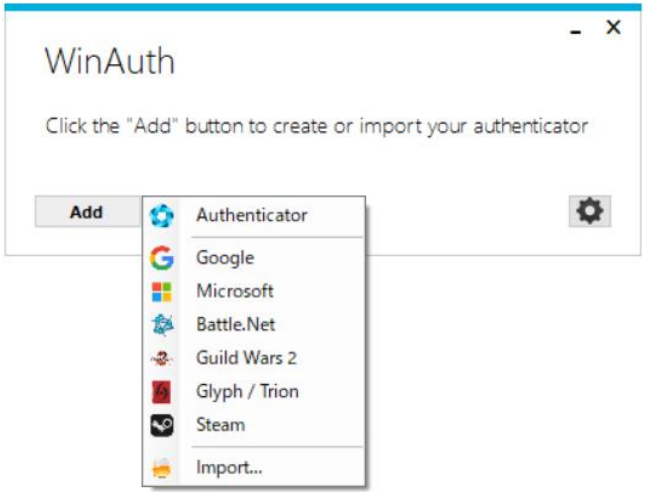
手順１：Webページ（https://winauth.github.io/winauth/download.html）から
WinAuthをダウンロードしてください。



（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。

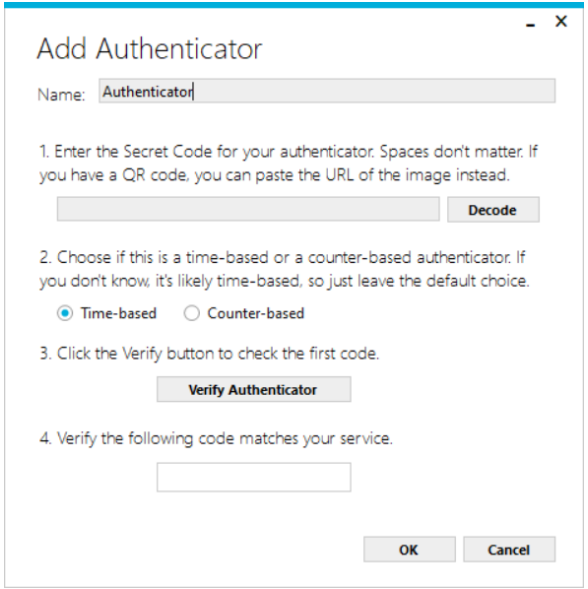
手順３：WinAuth.exeを起動し、「Add」→「Authenticator」をクリックしてください。



（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。

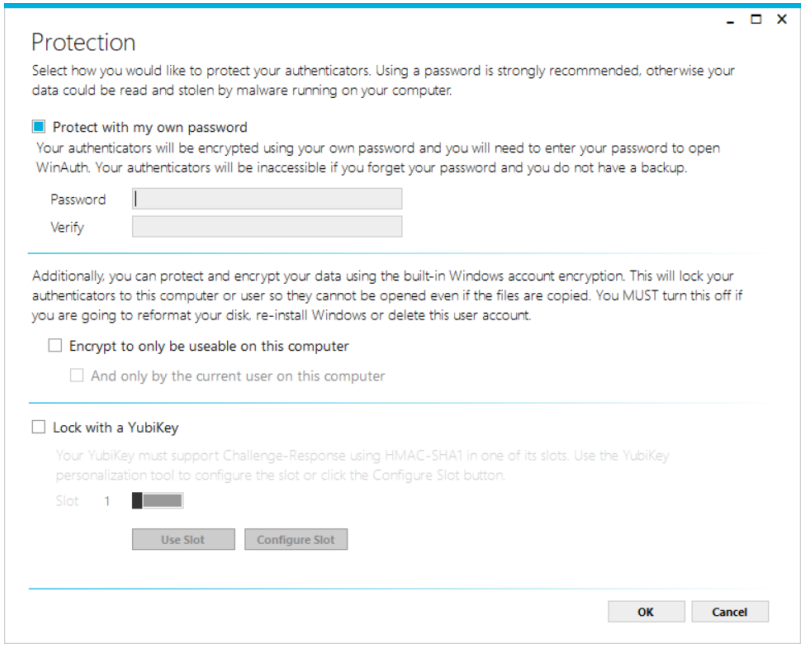
手順５：「Verify Authenticator」をクリックし、
「Verify the following code matches your service」に６桁のワンタイムパスワードが表示されることを確認できたら「OK」をクリックしてください。



（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。

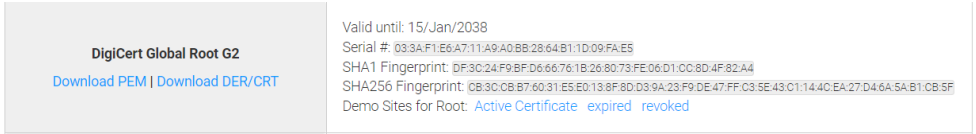


Step5：証明書の準備

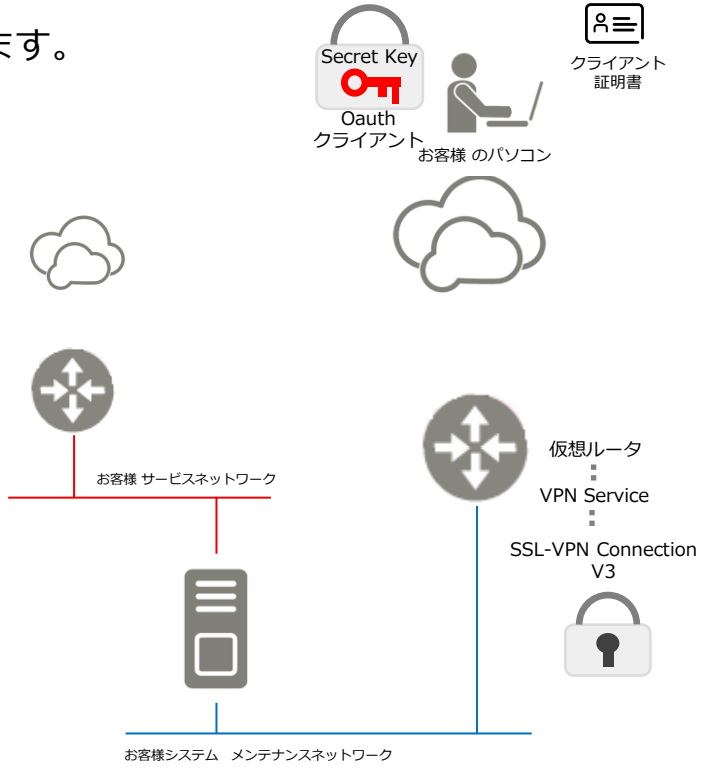
- SSL-VPN接続でクライアント側が利用する証明書を準備します。

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



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

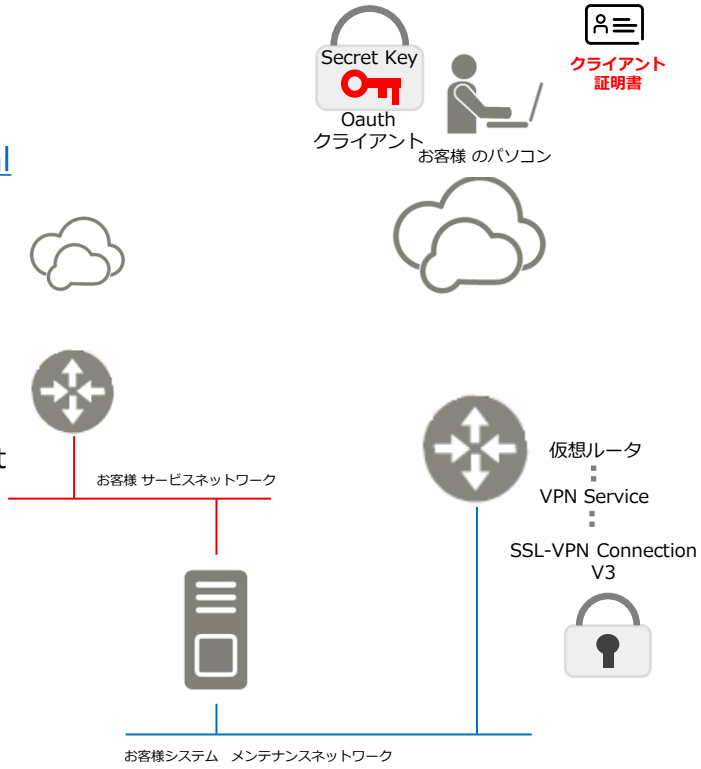
FJcloudポータルからクライアント証明書を取得します。
詳細は以下のURLを参照してください。
https://doc.cloud.global.fujitsu.com/lib/common/jp/FJCS_General_ja/FJCSPortal_UserGuide_ja/section3-3/#_15

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。



Step6：クライアントの設定

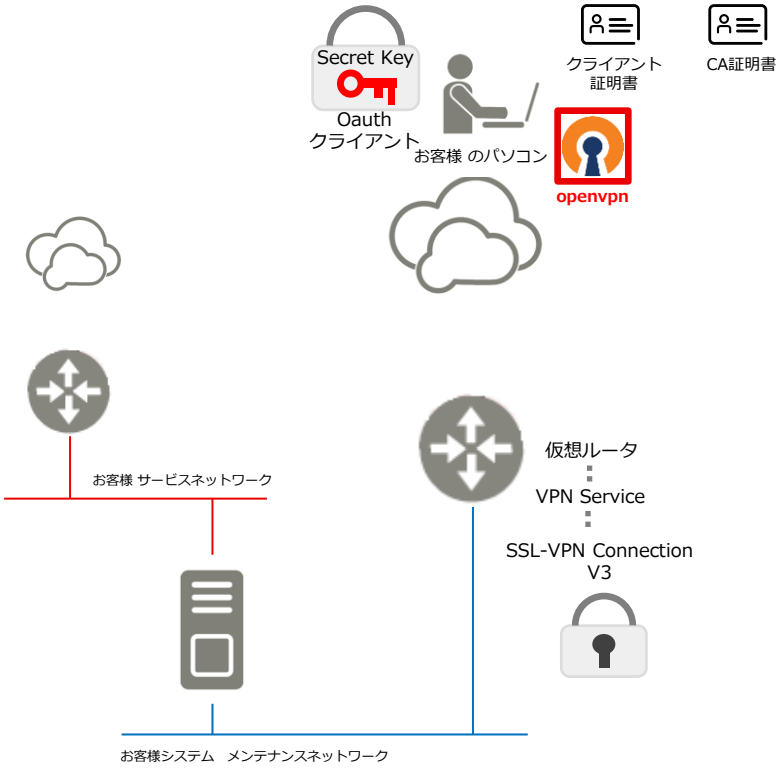
- SSL-VPN接続クライアント（OpenVPNクライアント）をインストールします。

  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。



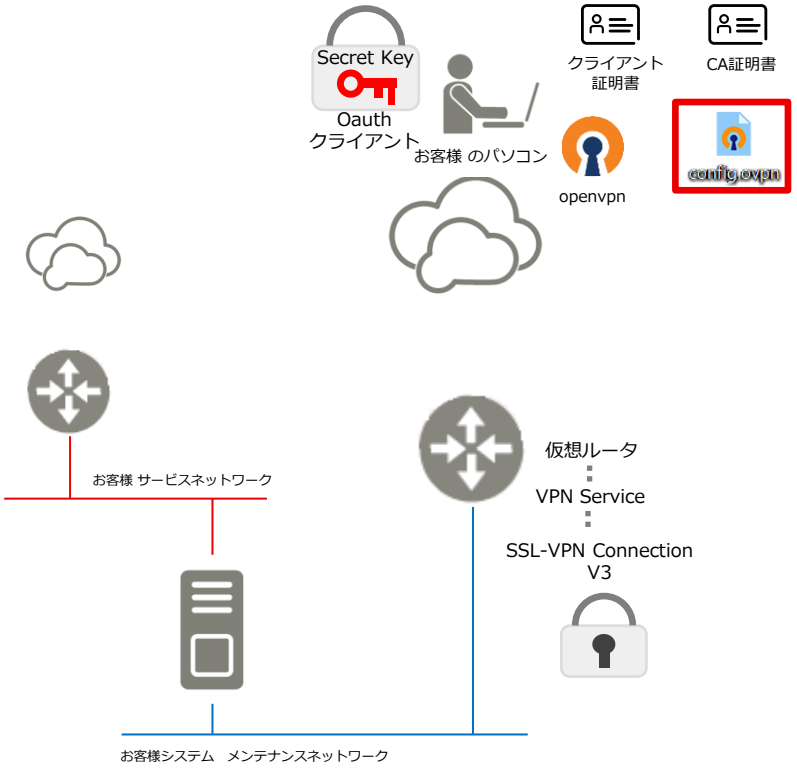
Step7：接続設定ファイルの作成

- 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-passstatic-challenge pin otp      ※2
Persist-key
Persist-tun
ca ca.crt                ※3
cert client.crt          ※3
key client.key           ※3
remote-cert-tls servercipher AES-128-CBC
ncp-ciphers AES-128-CBC
```

※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。



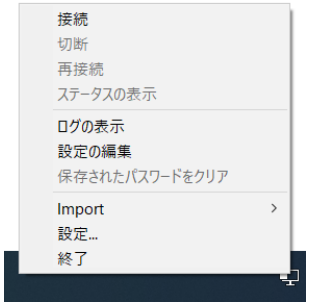
Step8：SSL-VPN接続を行う

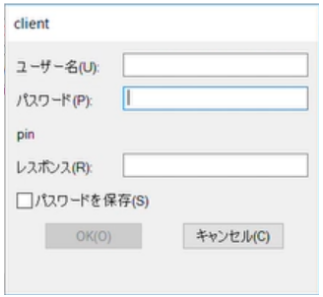
- SSL-VPN接続を行います。

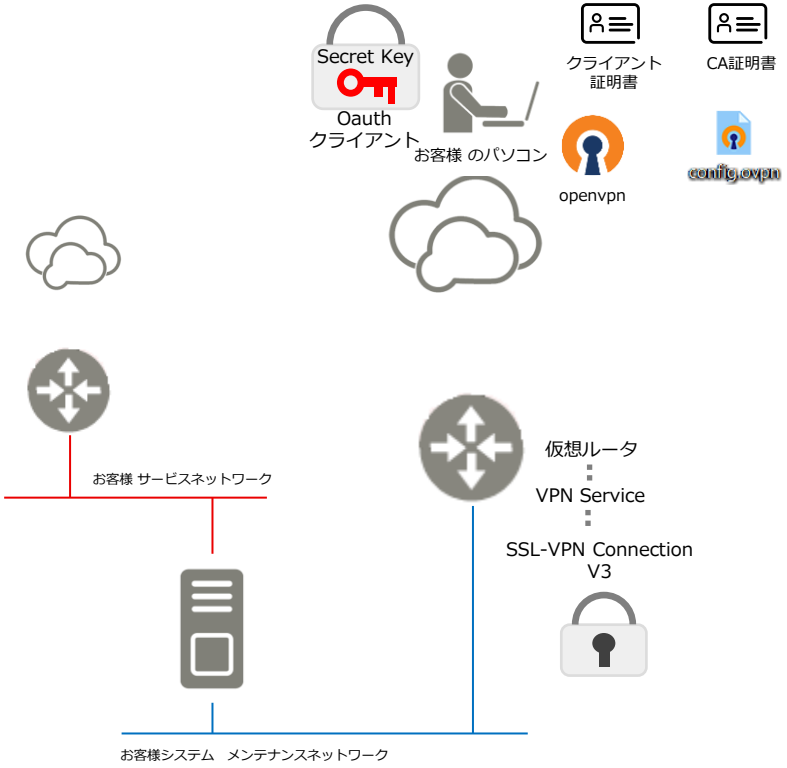
タスクトレイにあるOpenVPNアイコンを右クリックし、
「接続」を選択してください。

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、ヘルプデスクにお問い合わせください。

  ※ 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

- ヘルプデスク側でセッション数拡張（最大同時接続数255）を個別適用いたします。

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が設定されているVPN ServiceにSSL-VPN V3を作成できないため、SSL-VPN V2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。

Thank you