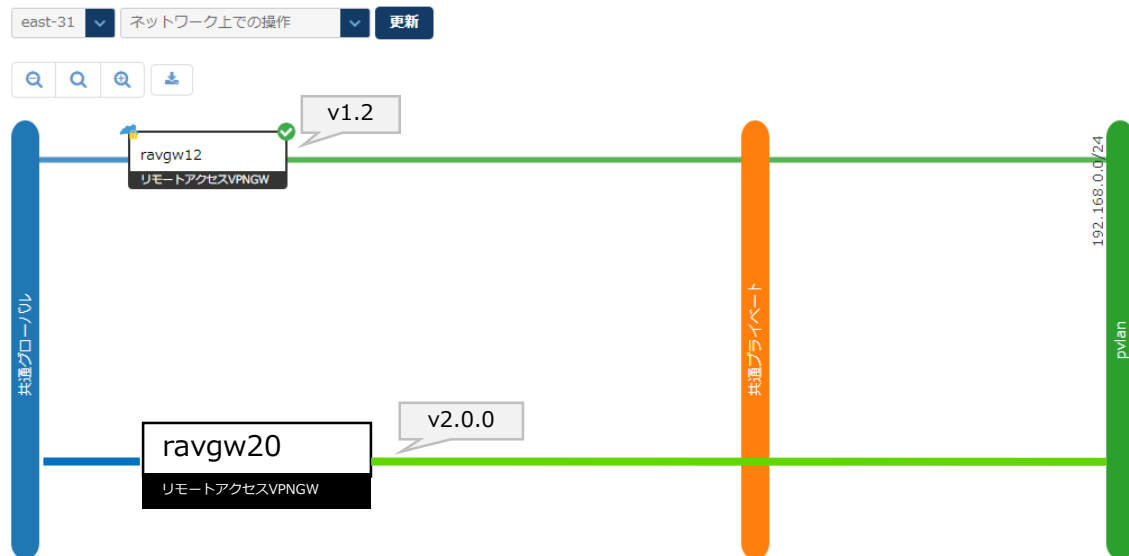


# リモートアクセスVPNゲートウェイv2.0.0への 移行方法について

富士通クラウドテクノロジーズ株式会社

リモートアクセスVPNゲートウェイ v2.0.0のリリース以降、リモートアクセスVPNゲートウェイの新規作成はv2.0.0のみとなります。既存のv1.2が接続されているプライベートLANに追加してv2.0.0の作成が可能です。(v1.2とv2.0.0を併用して利用が可能)

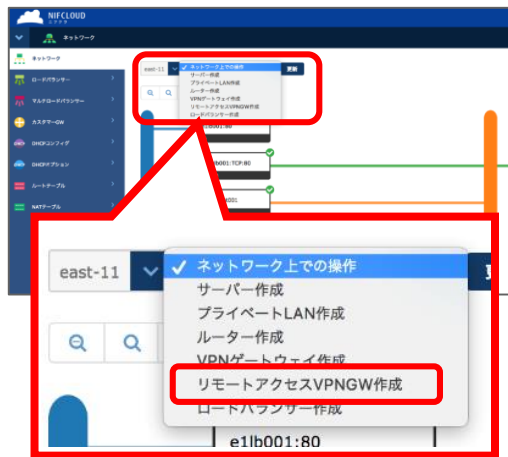
このためお客様はサービスを並行して移行期間を設ける事が出来ます。



# リモートアクセスVPNゲートウェイv2.0.0への移行方法

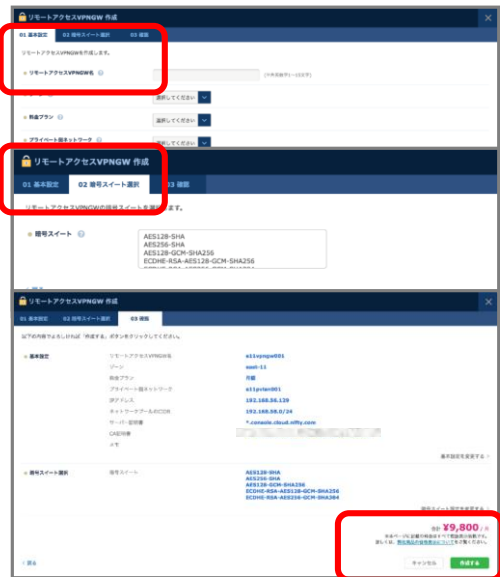
## Step1

ネットワーク設定から  
「リモートアクセスVPNGW作成」を選択  
v2.0.0リリース以降、同じプライベートLANに追加作成



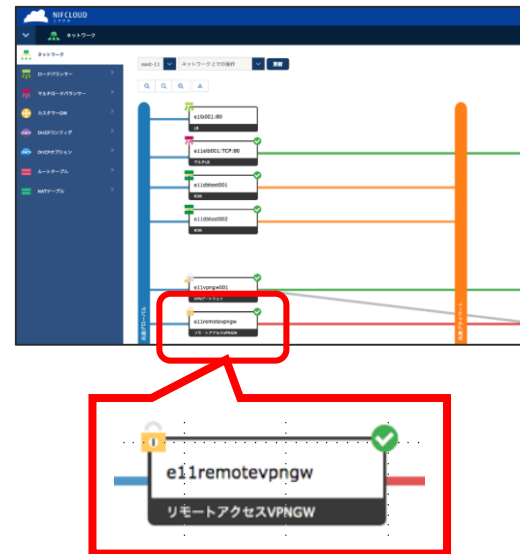
## Step2

プラン、ネットワークなど基本設定と暗号スイートを設定し、確認画面にて「作成」



## Step3

ネットワークに反映されたら、v2.0.0の作成完了  
1つのプライベートLANに2つのリモートアクセスVPNゲートウェイが存在する状態



※サーバー証明書・CA証明書は別途用意が必要です

# リモートアクセスVPNゲートウェイv2.0.0への移行方法

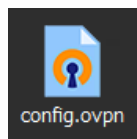
## Step4

コントロールパネルからリモートアクセスVPNゲートウェイv2.0.0の「ユーザー作成」を実行



## Step5

コントロールパネルから接続設定ファイルをダウンロードします。クライアントは配布されているOpenVPNのソフトウェアをご利用下さい。

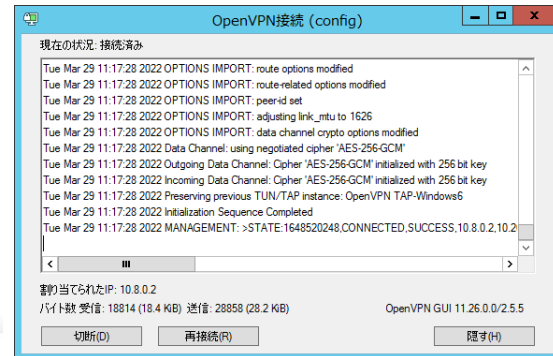


<https://www.openvpn.jp/download/>

4/ 11

## Step6

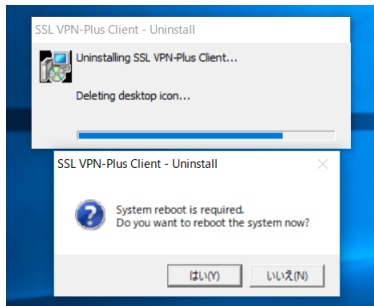
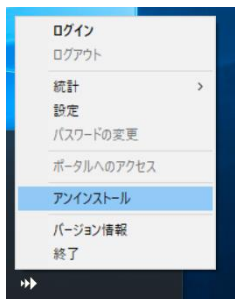
クライアントソフトウェアでSSL-VPN接続



# リモートアクセスVPNゲートウェイv2.0.0への移行方法

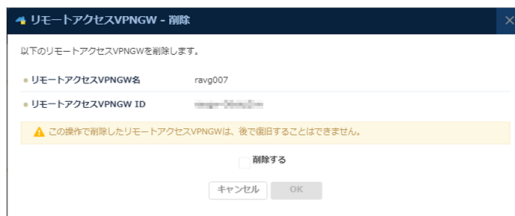
## Step7

動作確認後、クライアント端末からこれまで利用していたv1.2のクライアントソフトウェアをアンインストールします



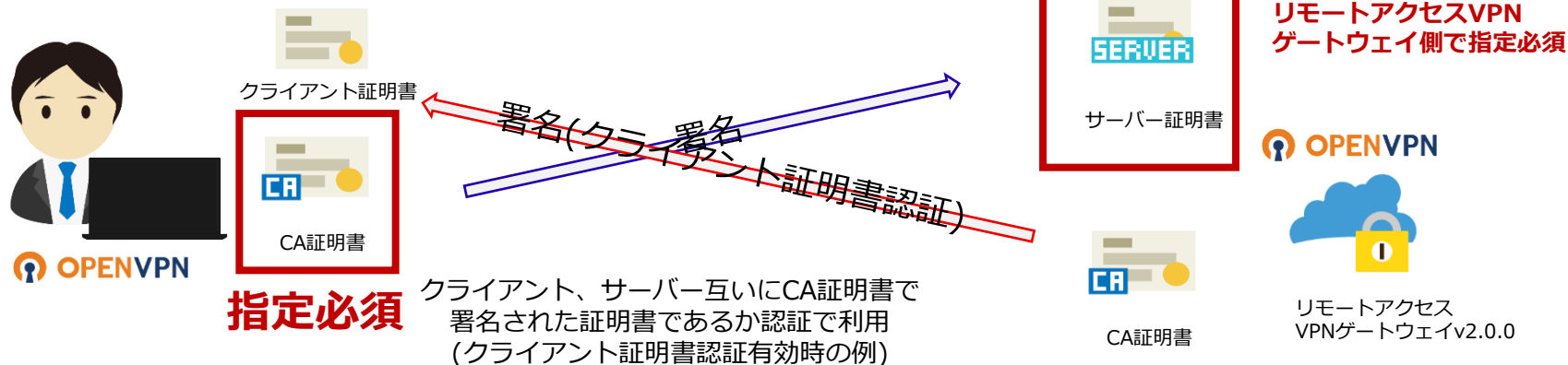
## Step8

お客様環境のクライアント端末の移行がすべて完了した後にv1.2を削除します



- v1.2とv2.0.0のリモートアクセスVPNゲートウェイを併用する場合、プライベートLANに接続するIPアドレスが重複しないように設定してください。重複した場合、正常に通信できません。
- ニフクラ上のサーバーのファイアウォールで、v1.2のリモートアクセスVPNゲートウェイのプライベートLAN IPアドレスを許可している場合、追加したv2.0.0のプライベートLAN IPアドレスの許可ルール追加が必要になります。

## ●v2.0.0でのサーバー証明書の取り扱い



- v2.0.0ではリモートアクセスVPNゲートウェイに設定するサーバー証明書を署名したCA証明書を必ずクライアント端末側の設定ファイル内で指定する必要があります。このためv1.2のリモートアクセスVPNゲートウェイに公的CAで発行されたサーバー証明書を設定され、引き続きv2.0.0で同じサーバー証明書を利用する場合にはクライアント端末に公的CAのルート証明書を設定する必要があります。  
公的CAのルート証明書は一般公開されているため、第三者がクライアント端末で接続を試行でき、サーバー証明書の認証機能として形骸化します。  
このためv2.0.0では独自CAで署名されたサーバー証明書を設定することを推奨します。
- 現在サーバー証明書を設定されていないお客様は、v2.0.0ではサーバー証明書の指定が必要となります。

移行に伴いサーバー証明書の再作成または新規作成を実施頂く必要があります。  
(独自CAはOpenSSLコマンドやOSSのツールで無償で作成可能です)

## ● v2.0.0でのサーバー証明書の要件

- v2.0.0で利用出来るサーバー証明書の要件として、Key Usage および Extend key Usageが指定されている必要があります。  
詳細はクラウド技術仕様（リモートアクセスVPNゲートウェイ:証明書）をご参照ください。  
[https://pfs.nifcloud.com/spec/ra\\_vpngw/cert.htm](https://pfs.nifcloud.com/spec/ra_vpngw/cert.htm)
- 現在ご利用のサーバー証明書が要件に合致していない場合、サーバー証明書を再生成して頂く必要があります。  
**(独自CAはOpenSSLコマンドやOSSのツールで無償で作成可能です)**  
作成手順の詳細はクラウドユーザーガイド（リモートアクセスVPNゲートウェイ：Easy-RSAを使った自己署名証明書作成手順）をご参照ください。  
[https://pfs.nifcloud.com/guide/cp/ra\\_vpngw/cert\\_easy-rsa.htm](https://pfs.nifcloud.com/guide/cp/ra_vpngw/cert_easy-rsa.htm)  
  
証明書を作成するツールも公開しています。  
<https://github.com/nifcloud/genca>

## ● ユーザーアカウントの移行

- 既存のリモートアクセスVPNゲートウェイv1.2でご利用のユーザーアカウントは、v2.0.0で新規作成が必要となります。
- 大規模環境(数百ユーザーアカウント等)でご利用のお客様に対し、効率的な移行ツールを公開しています。  
<https://github.com/nifcloud/nifcloud-ravgw-miguser>



現在リモートアクセスVPNゲートウェイ v1.2 にてトンネルモードでフルトンネルをご利用のお客様については、リモートアクセスVPNゲートウェイ v2.0.0では分割トンネルのみ対応しているため、分割トンネルへのご利用変更をご検討ください。

- クラウド 機能・サービス（リモートアクセスVPNゲートウェイ）
  - [https://pfs.nifcloud.com/service/ra\\_vpngw.htm](https://pfs.nifcloud.com/service/ra_vpngw.htm)
- クラウド技術仕様（リモートアクセスVPNゲートウェイ）
  - [https://pfs.nifcloud.com/spec/ra\\_vpngw/](https://pfs.nifcloud.com/spec/ra_vpngw/)
- ユーザーガイド：コンピューティング
  - <https://pfs.nifcloud.com/guide/cp/#%E3%83%AA%E3%83%A2%E3%83%BC%E3%83%88%E3%82%A2%E3%82%AF%E3%82%BB%E3%82%B9vpn%E3%82%B2%E3%83%BC%E3%83%88%E3%82%A6%E3%82%A7%E3%82%A4>

# No Boundary & Connecting



Fujitsu Cloud Technologies