FortiGate(OS7.6)における IPsec-VPN クライアント証明書認証設定手順

2025 年 08 月 20 日

Ver. 1.00

改訂履歴

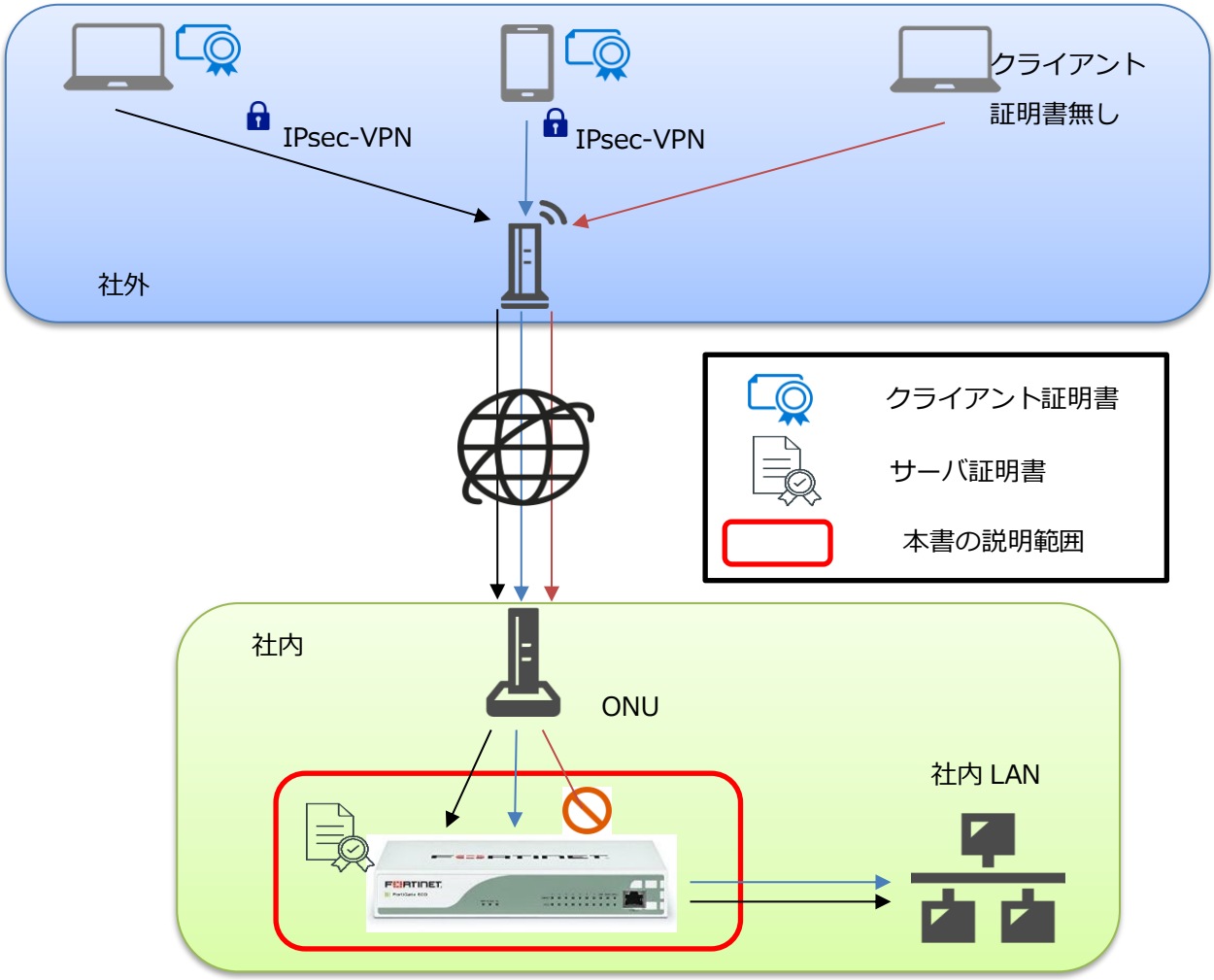
版	日　付	内　容	備　考
Ver. 1.00	--	初版作成	

<目　次>

1. 概要

本書は Fortinet 社が提供している FortiGate 60F における IPsec-VPN 機能について、クライアント証明書認証(X.509 認証)設定手順を説明いたします。
あくまで一例としてご紹介させていただいておりますので、詳細な設定等は FortiGate の販売店もしくはメーカーへお問い合わせください。

【構成イメージ】



動作確認を行った時点の製品情報は以下のとおりです。
バージョンが異なる場合はうまく動作しない可能性がございます。

Forti Gate 60F バージョン 7.6.3

OS	FortiClient バージョン
WindowsOS	7.4.3
iOS	7.4.7

※本バージョンにおいて、IPSec-VPN（X.509 認証）を利用した場合に、Android 版 FortiClient（Ver.7.4.3）での接続が失敗する事象を確認しております。（2025 年 7 月 23 日時点）

2. 事前準備

■SSL サーバ証明書

初期状態では自己署名のサーバ証明書が入っていますが、信頼性の観点から証明書ベンダーから調達することを推奨します。インストールする際には、PEM 形式に変換する必要があります。

■ルート証明書（G2）

以下 URL よりダウンロードしてください。

・https://www.nrapki.jp/nrawp/cert/NipponRARootCertificationAuthorityG2.crt

■中間証明書

ご利用中の中間認証局の証明書を以下の URL からダウンロードしてください。

・中間証明書(CA3 G2)
https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority3G2.crt

・中間証明書(CA4 G2)
https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority4G2.crt

■失効リスト配布 URL

失効リストをインポートする際に使用します。

・中間認証局(CA3 G2)
http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority3G2/cdp.crl

・中間認証局(CA4 G2)
http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority4G2/cdp.crl

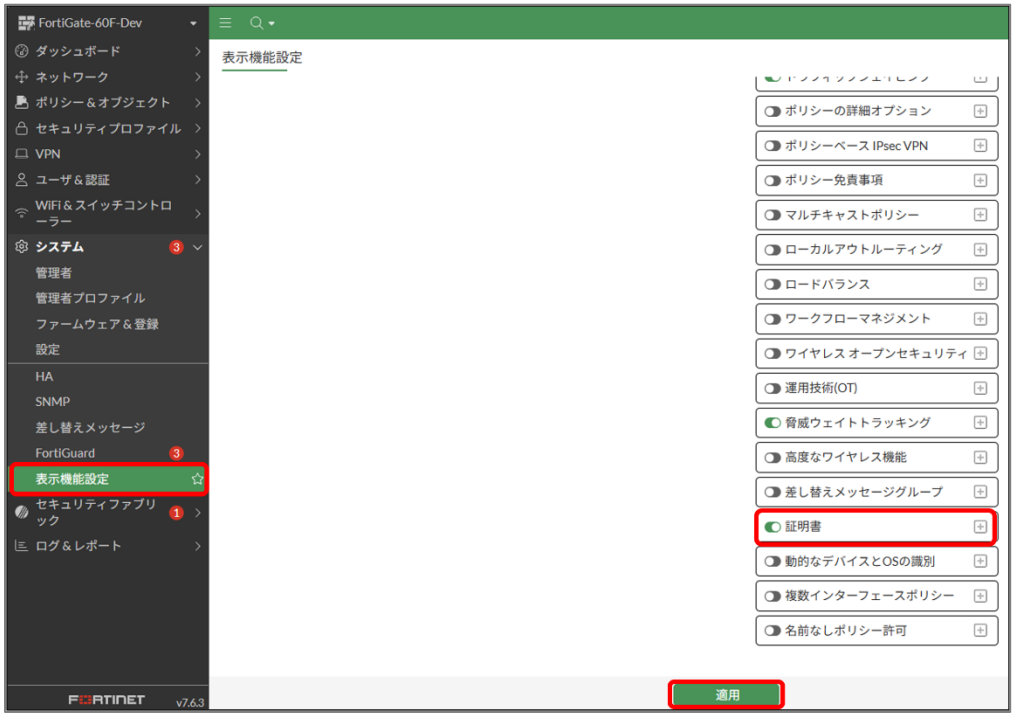
【ご利用中の中間認証局の確認方法】

以下画像の NRA-PKI システム管理画面にて、[利用者メンテナンス]をクリックしていただくと、適用されているサービス名が表示されます。サービス名の後に**（CA4）**という表記があれば CA4 G2、なければ CA3 G2 をご利用いただいております。

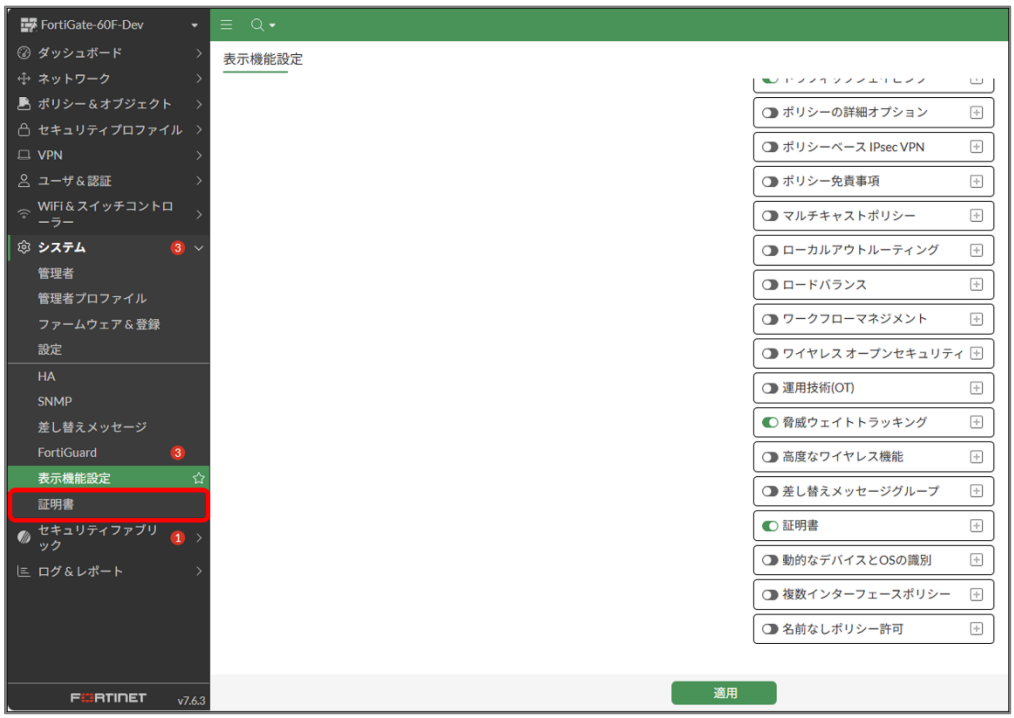
3. クライアント証明書認証をするための設定手順

3.1. 証明書メニューの有効化

管理画面から「システム」-「表示機能設定」より証明書を有効化し適用をクリックします。



下図のように「表示機能設定」の下に「証明書」の項目が表示されます。

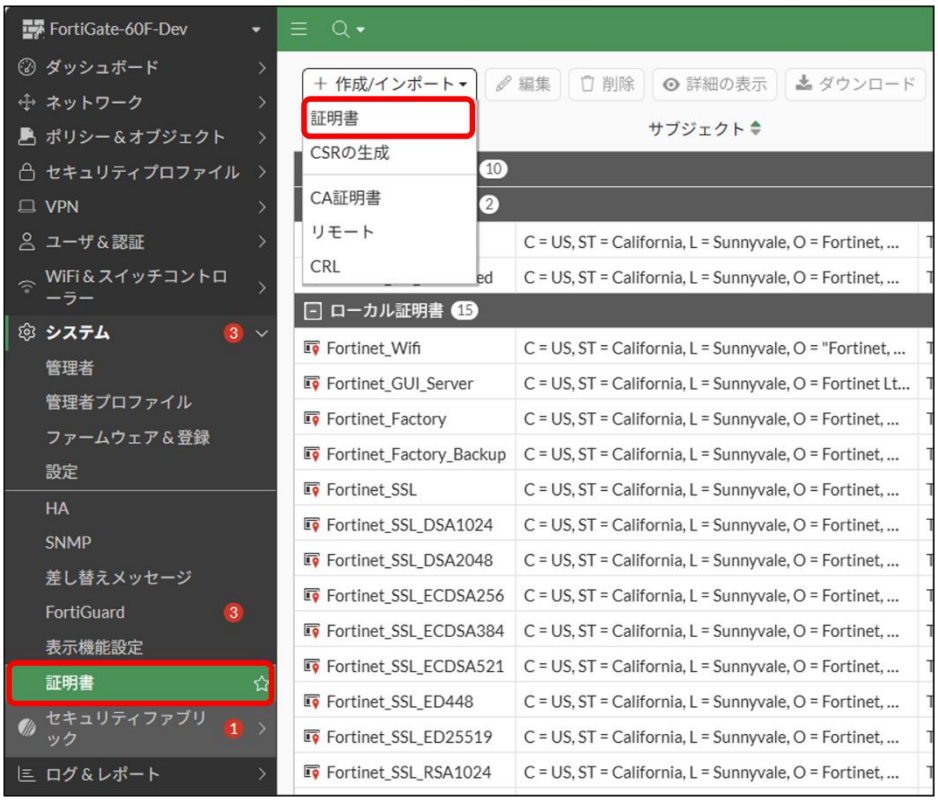


3.2. 証明書のインポート

事前準備で用意した各証明書とCRL(失効リスト)をインポートします。

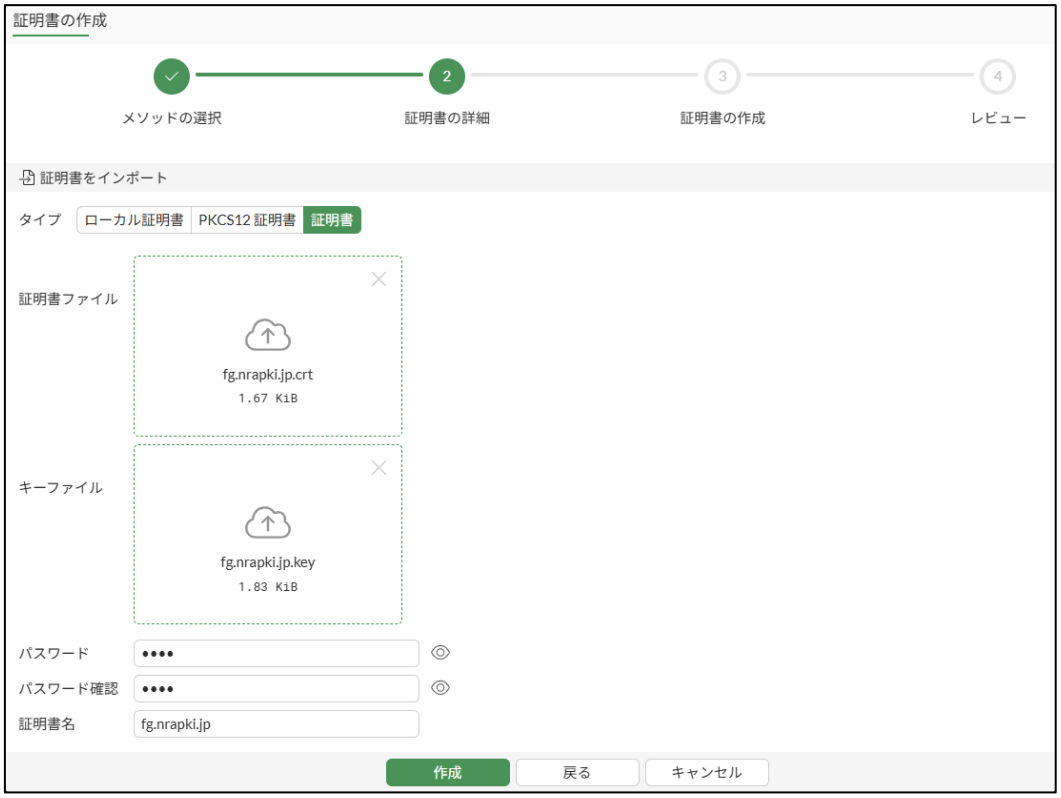
■サーバ証明書

「システム」-「証明書」を選択し、「作成/インポート」から「証明書」を選択します。

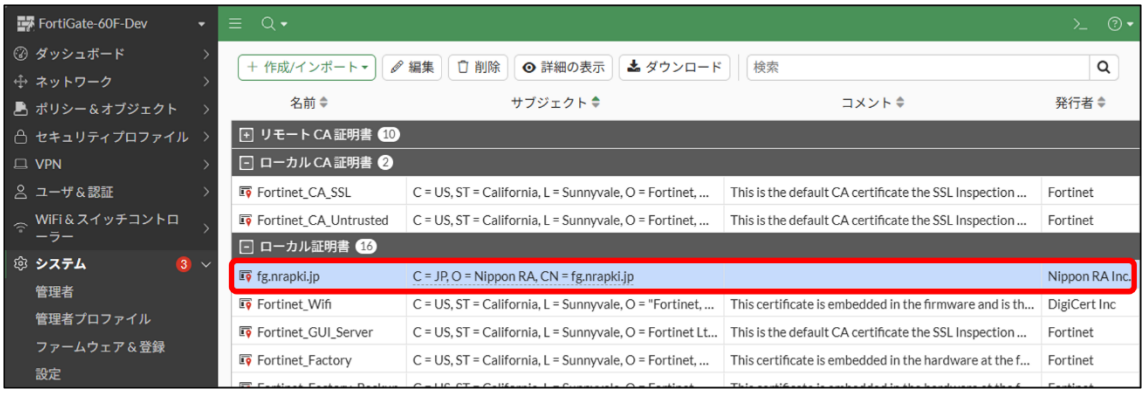


「証明書をインポート」を選択します。

「証明書の作成」画面が表示されます。「証明書」を選択し、証明書ファイル、キーファイル、パスワード(任意)を指定し作成をクリックします。

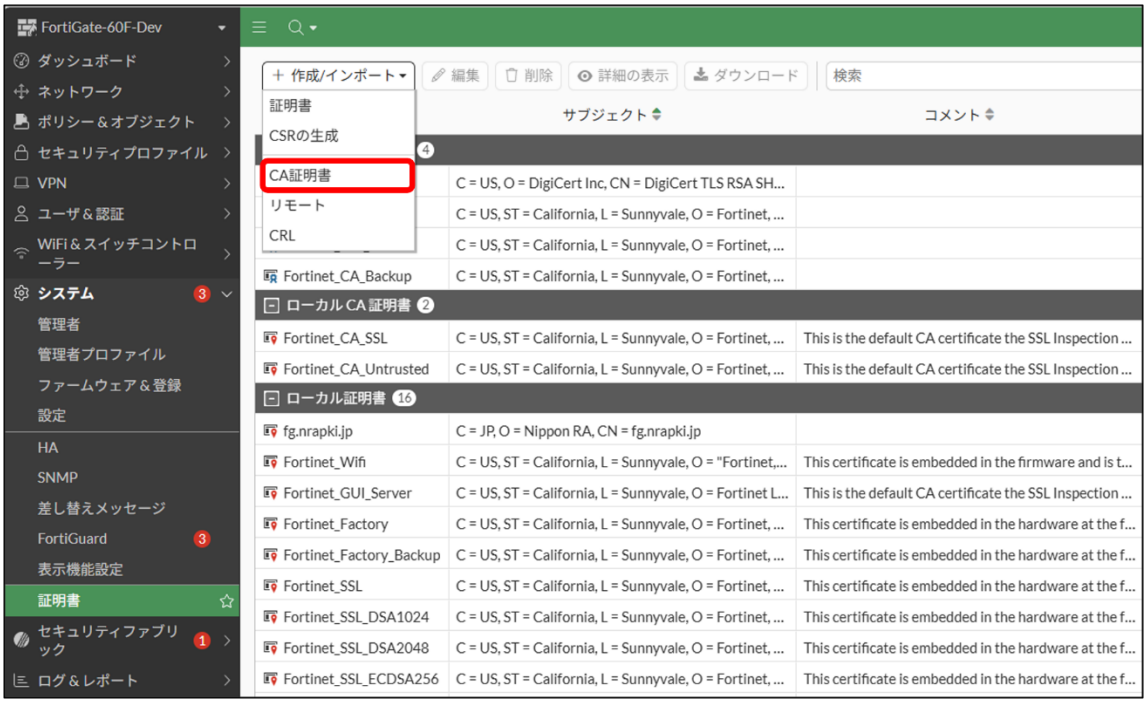


サーバ証明書がインポートされたことを確認します。



■ルート証明書、中間証明書

「システム」-「証明書」を選択し、「作成/インポート」から「CA 証明書」を選択します。



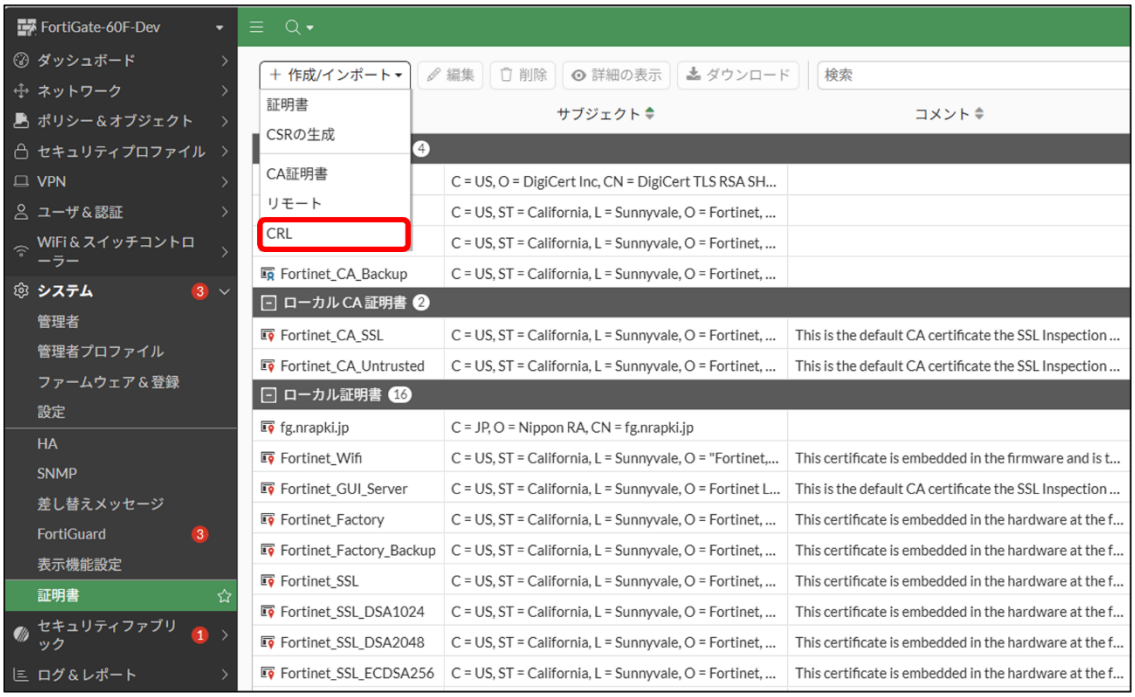
「ファイル」を選択し、ルート証明書を指定し OK をクリックします。

同手順にて中間証明書もインポートします。

ルート証明書、中間証明書がインポートされたことを確認します。

■CRL(失効リスト)

「システム」-「証明書」を選択し、「作成/インポート」から「CRL」を選択します。



「オンライン更新」-「HTTP」を選択し、CRL 配布ポイントの URL を入力し、OK をクリックします。

【補足】

既定の CRL の更新間隔は CRL の有効期限毎（NRA-PKI では 10 日間）となります。

■CRL 更新間隔の設定方法

CLI コンソールを使って以下コマンドを<>の中を実際の値にして設定します。

「update-interval」に更新間隔（秒）を指定してください。

config vpn certificate crl

edit <CRL の登録名>

set update-interval <任意の値>

next

end

設定が変更されているかを確認します。

■確認コマンド

show vpn certificate crl

【設定確認画面(例)】

CRL_1 の更新間隔（update-interval）を 3600（秒）に設定

```
FortiGate-60F  # show vpn certificate crl CRL_1
config vpn certificate crl
    edit "CRL_1"
        set range global
        set http-url "http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority4G2/cdp.crl"
        set update-interval 3600
    next
end
```

CRL(失効リスト)がうまく取得できない場合は OCSP レスポンダをお試しください。

OCSP レスポンダ URL
http://mpkiocsp.managedpki.ne.jp/mpkiocsp

■OCSP レスポンダの設定方法
CLI コンソールを使って以下コマンドを<>の中を実際の値にして設定します。

config vpn certificate ocsp-server
edit <任意の値>※画像では mpki_ocsp
set url http://mpkiocsp.managedpki.ne.jp/mpkiocsp
set cert <中間 CA の登録名>
set unavail-action revoke
end
exit

設定が変更されているかを確認します。

■確認コマンド①
config vpn certificate ocsp-server
edit <設定した任意の値>
get

【設定完了画面①(例)】

```
FortiGate-60F (mpki_ocsp) # get
name                : mpki_ocsp
url                 : http://mpkiocsp.managedpki.ne.jp/mpkiocsp
cert                : CA_Cert_2
secondary-url       :
secondary-cert      :
unavail-action      : revoke
source-ip           : 0.0.0.0
```

■確認コマンド②

config vpn certificate setting

get

【設定完了画面②(例)】

```
FortiGate-60F (setting) # get
ocsp-status          : enable
ocsp-option          : server
ocsp-default-server  : mpki_ocsp
interface-select-method: auto
check-ca-cert        : enable
check-ca-chain       : disable
subject-match        : substring
subject-set          : subset
cn-match             : substring
cn-allow-multi       : enable
crl-verification:
    expiry               : ignore
    leaf-crl-absence     : ignore
    chain-crl-absence    : ignore
strict-ocsp-check    : disable
ssl-min-proto-version: default
cmp-save-extra-certs: disable
cmp-key-usage-checking: enable
cert-expire-warning : 14
certname-rsa1024     : Fortinet_SSL_RSA1024
certname-rsa2048     : Fortinet_SSL_RSA2048
certname-rsa4096     : Fortinet_SSL_RSA4096
certname-dsa1024     : Fortinet_SSL_DSA1024
certname-dsa2048     : Fortinet_SSL_DSA2048
certname-ecdsa256    : Fortinet_SSL_ECDSA256
certname-ecdsa384    : Fortinet_SSL_ECDSA384
certname-ecdsa521    : Fortinet_SSL_ECDSA521
certname-ed25519     : Fortinet_SSL_ED25519
certname-ed448       : Fortinet_SSL_ED448
```

差異がある場合は以下コマンドを参考に変更してください。

config vpn certificate setting

set ocsp-status enable

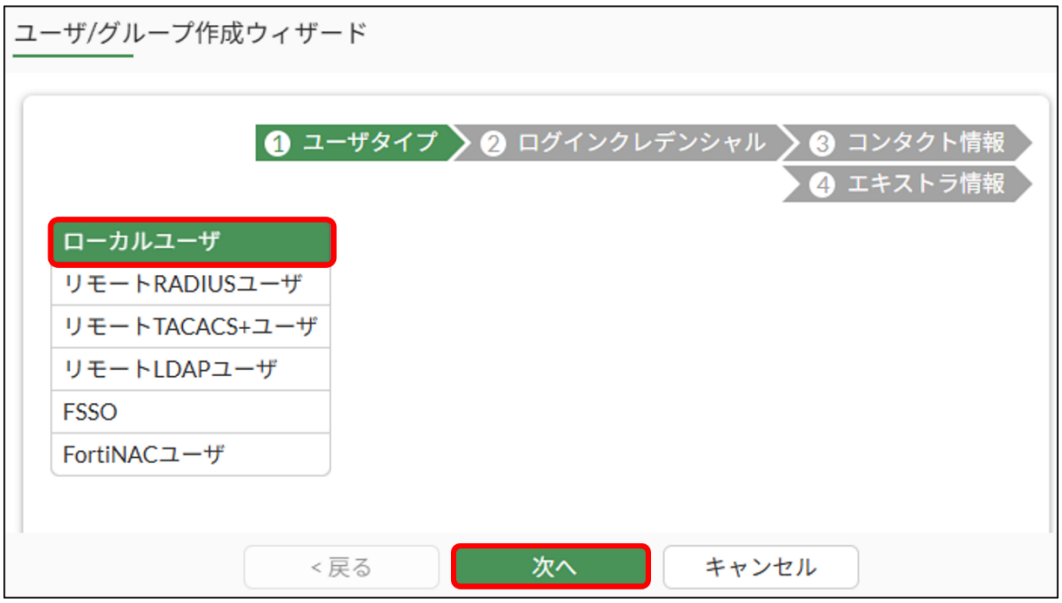
end

exit

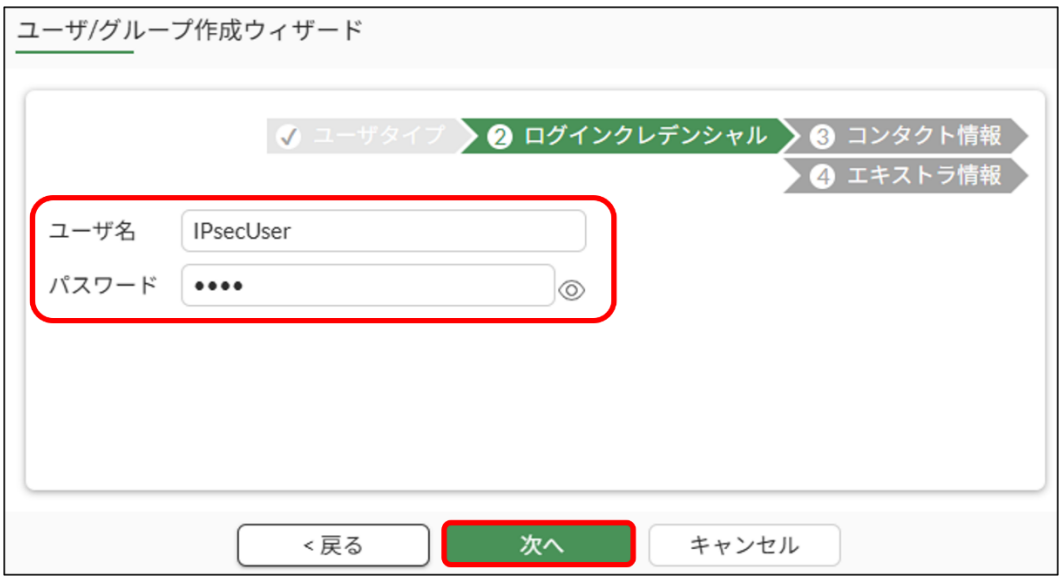
3.3. ローカルユーザの作成

「ユーザ&認証」-「ユーザ定義」から「新規作成」を選択します。

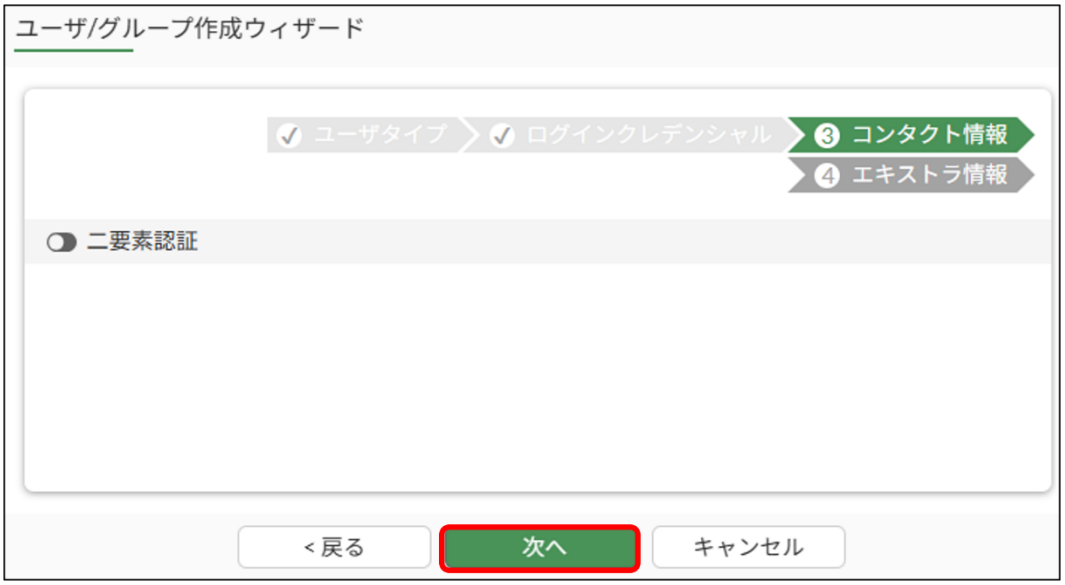
「ローカルユーザ」を選択し、次へをクリックします。



ユーザ名とパスワードを設定して、次へをクリックします。



二要素認証は必要に応じて設定してください。

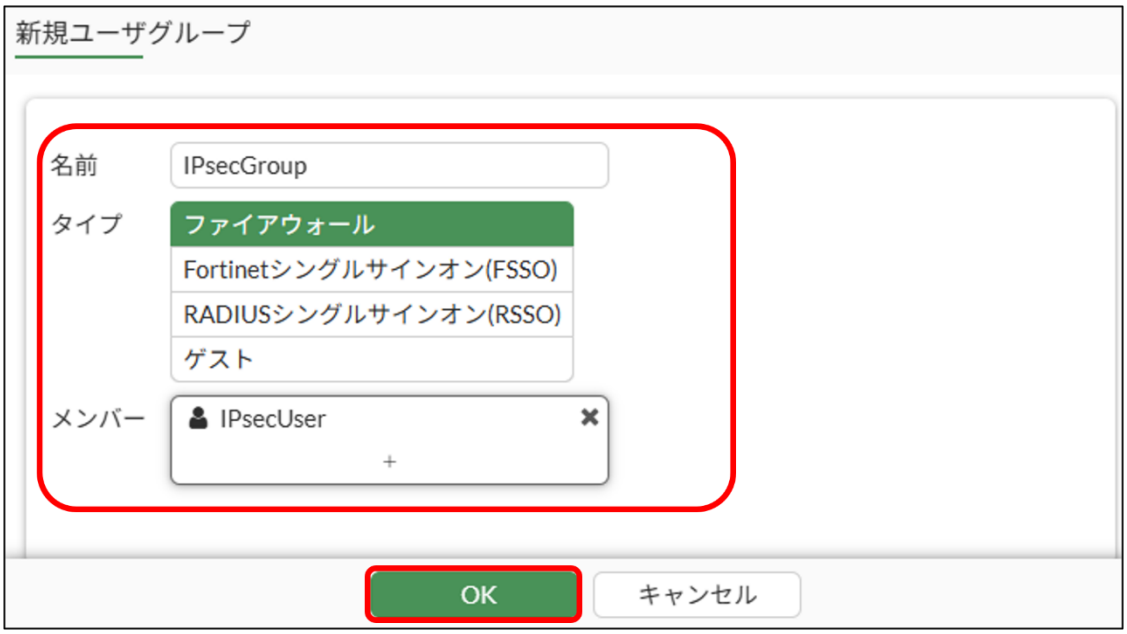


「サブミット」をクリックします。

3.4. グループの作成

「ユーザ&認証」-「ユーザグループ」から「新規作成」を選択します。

下図の赤枠内の項目を設定し OK をクリックします。



■設定例

名前：任意の値

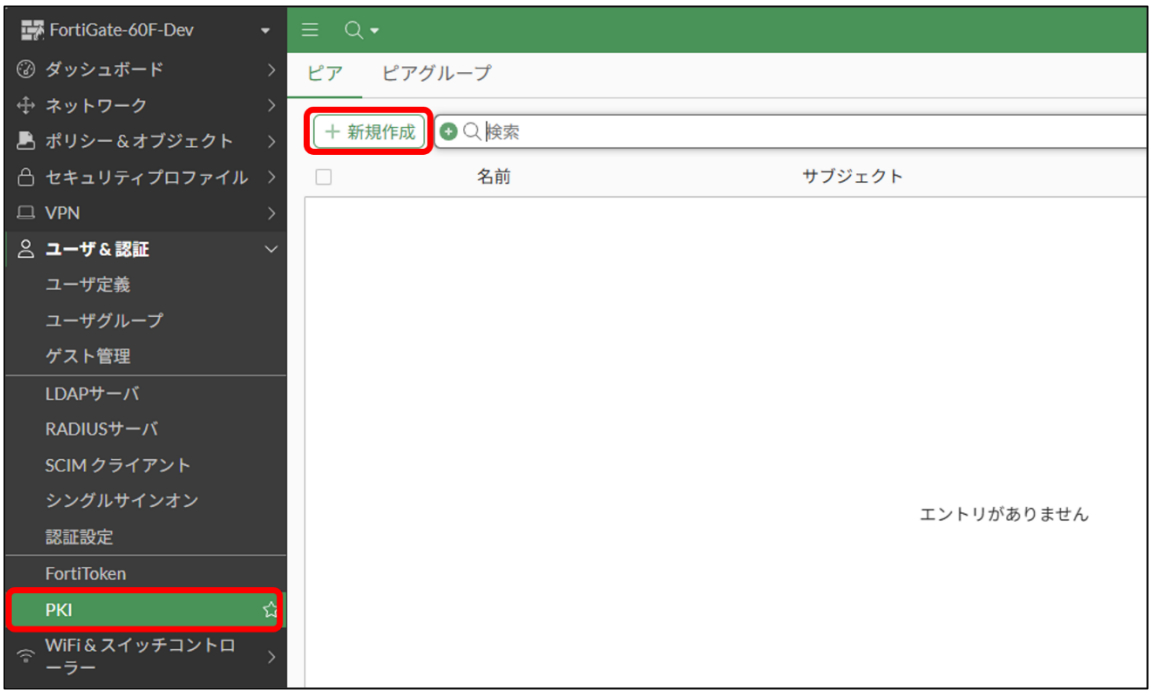
タイプ：ファイアウォール

メンバー：作成したユーザ

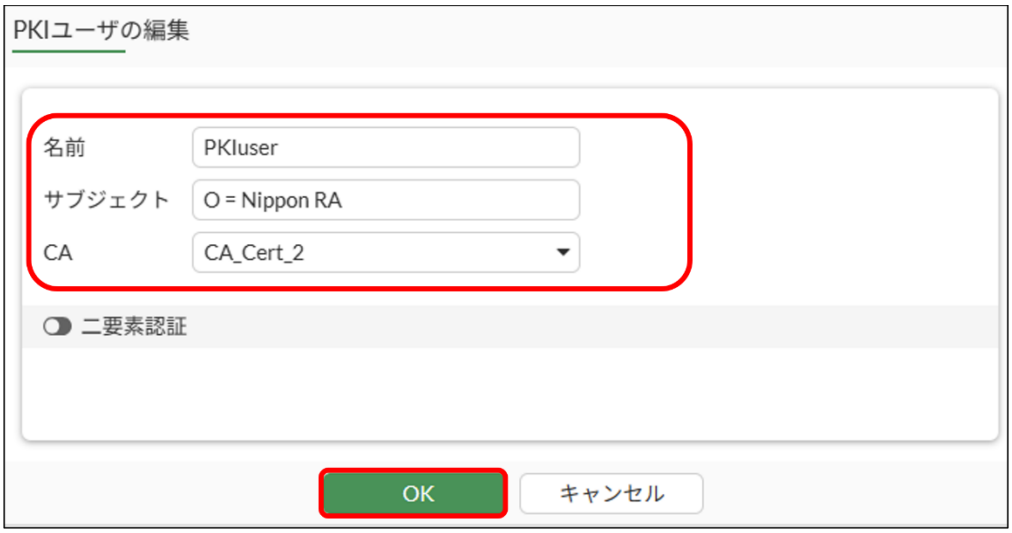
3.5. PKI ユーザの作成

証明書認証を行うユーザの条件を設定するため、PKI ユーザの作成を行います。

「ユーザ&認証」-「PKI」を選択し、「新規作成」を選択します。



下図の赤枠内の項目を設定し OK をクリックします。



■設定例

名前：任意の値

サブジェクト：任意の値　※【補足 1】参照

CA：インポートした中間証明書

※二要素認証は必要に応じて設定してください。

【補足 1】サブジェクトについて

認証する証明書をサブジェクトにより制限します。証明書のサブジェクト O（会社名）で制限する場合は、『O = xxxxxxx』の形式で入力して下さい。

空欄の場合、CA で設定した中間証明書の認証局で発行した証明書を認証します。

【補足 2】

「ユーザ&認証」に「PKI」の項目がない場合は、CLI から以下コマンドにて一度登録してください。

登録後に管理画面からログアウトし、再度ログインすると管理画面に「PKI」の項目が表示されます。

config user peer

edit <ユーザ名> ※任意の値

set ca CA_Cert_1（CA_Cert_1 は中間証明書。必要に応じて名前は変更）

<Email アドレス>（あとで UI で変更可能。今設定しなくても OK。）

end

exit

【補足 3】

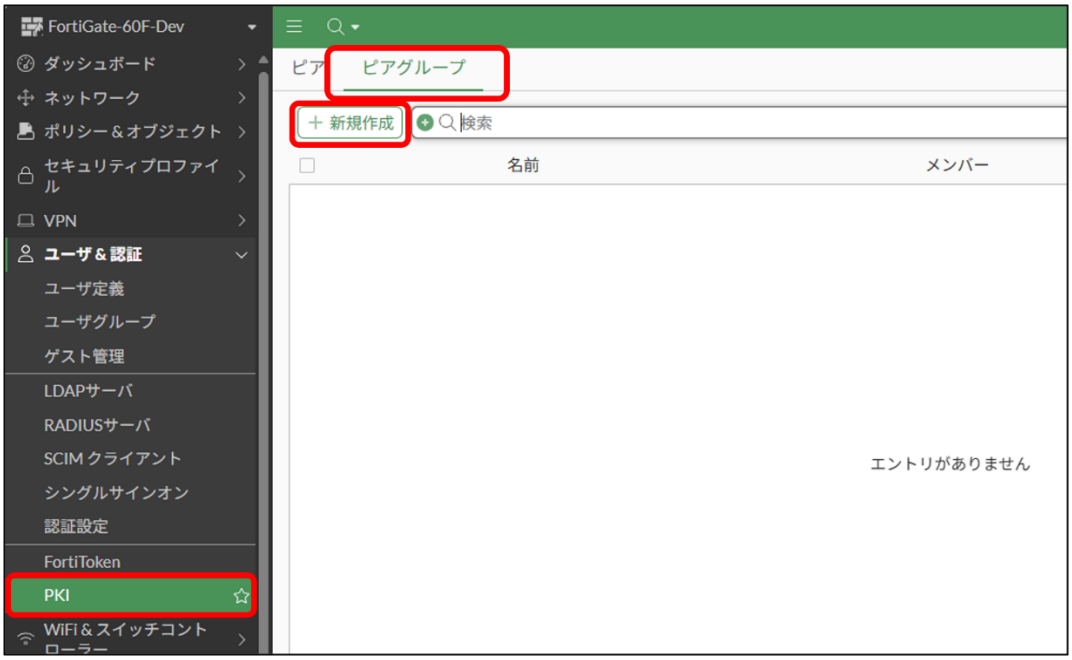
認証局世代交代におけるマルチトラスト設定を行う場合は、「CA」が旧認証局の PKI ユーザと新認証局の PKI ユーザをそれぞれ作成して、後記の PKI グループにて各 PKI ユーザを追加してください。

3.6. PKI グループの作成

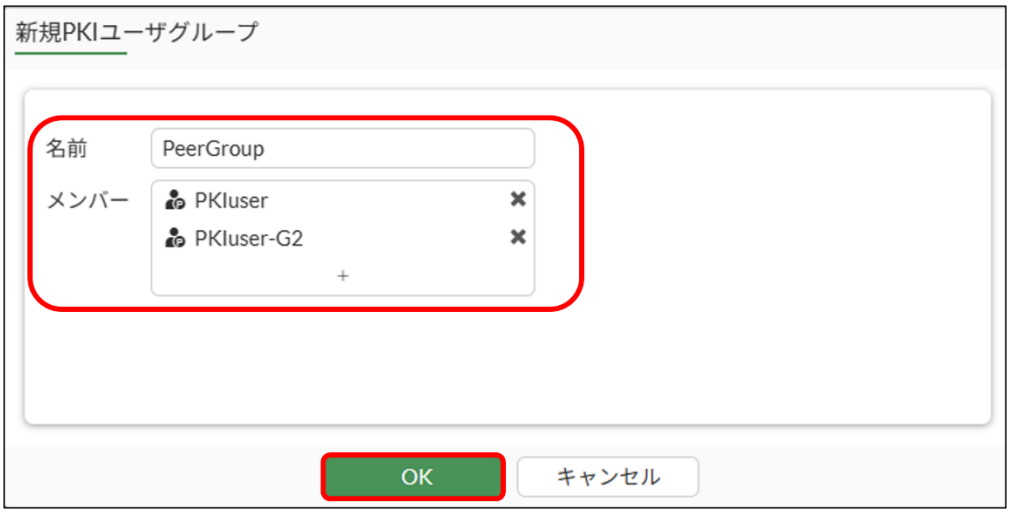
1 つの IPsec トンネルに複数の PKI ユーザを設定したい場合は、PKI グループを作成する必要があります。

設定する PKI ユーザが 1 つの場合は、本設定は不要です。

「ユーザ&認証」-「PKI」を選択し、画面上の「ピアグループ」を選択した上で「新規作成」をクリックします。



グループに含める PKI ユーザを選択し「OK」をクリックします。



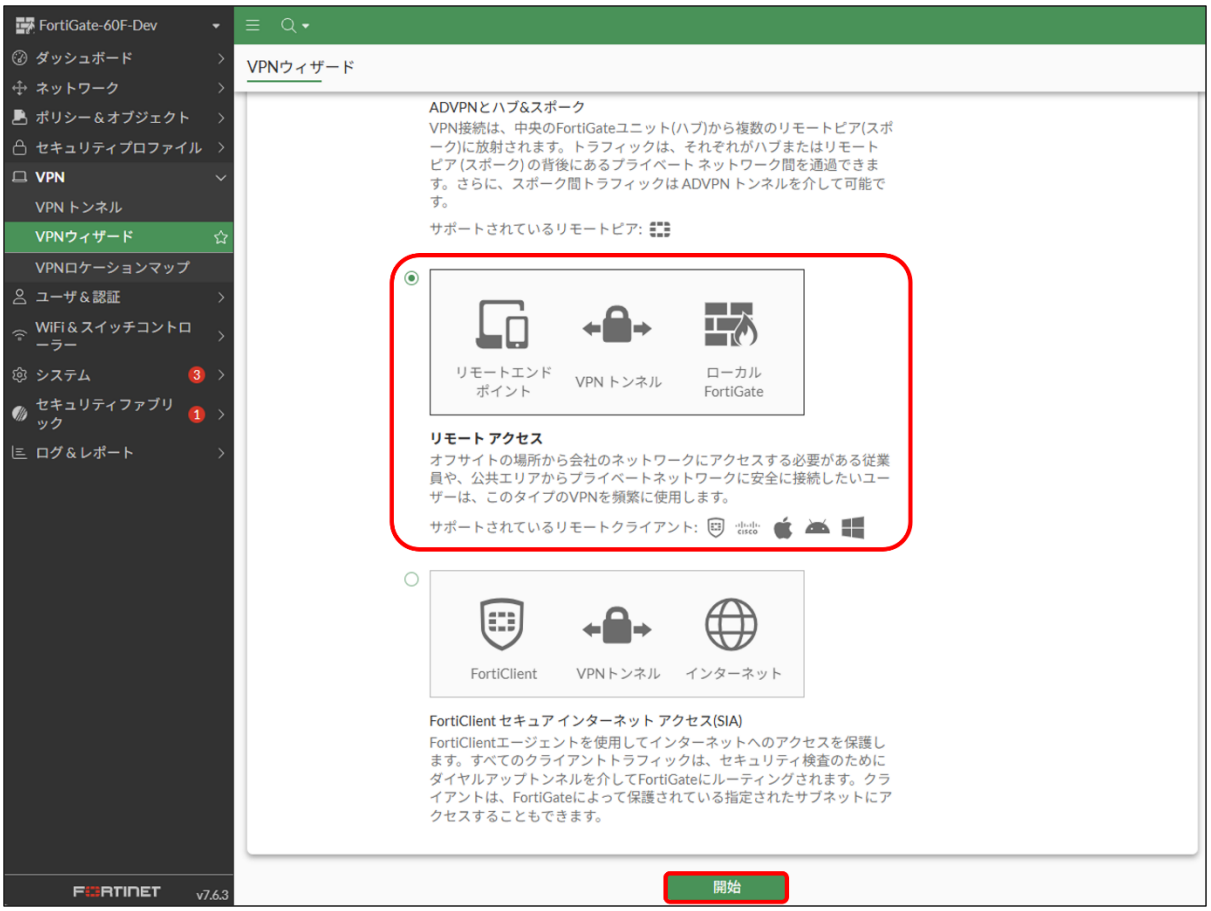
【補足】

認証局の世代交代におけるマルチトラスト設定を行う場合は、旧認証局の PKI ユーザと新認証局の PKI ユーザをメンバーに追加することで新旧認証局の証明書を認証することが可能となります。

3.7. IPsec ウィザードの設定

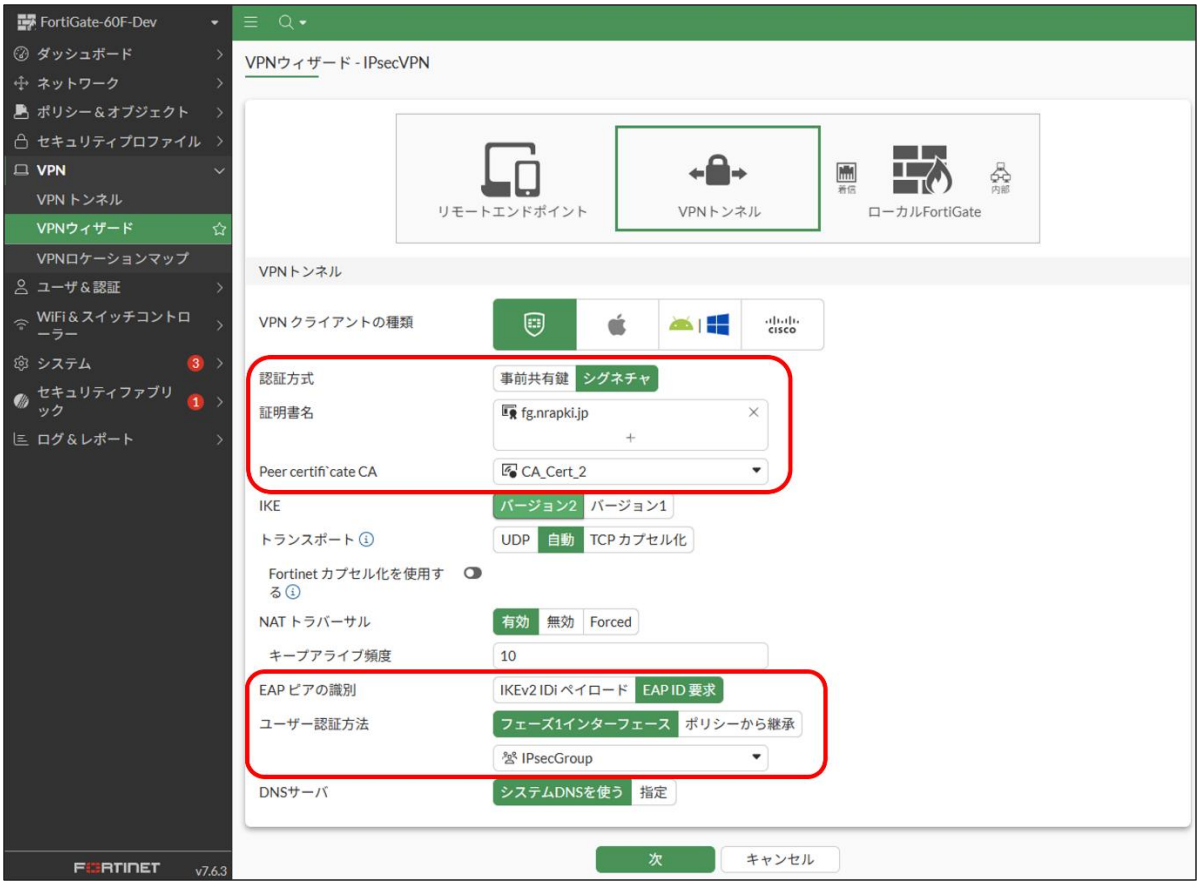
「VPN」-「VPN ウィザード」を選択し、トンネル名を設定します。

続いて「リモートアクセス」を選択して、「開始」をクリックします。



下図の赤枠を設定します。

その他の項目は必要に応じて設定し、「次」をクリックします。



■設定例

認証方式：シグネチャ

証明書名：インポートしたサーバ証明書

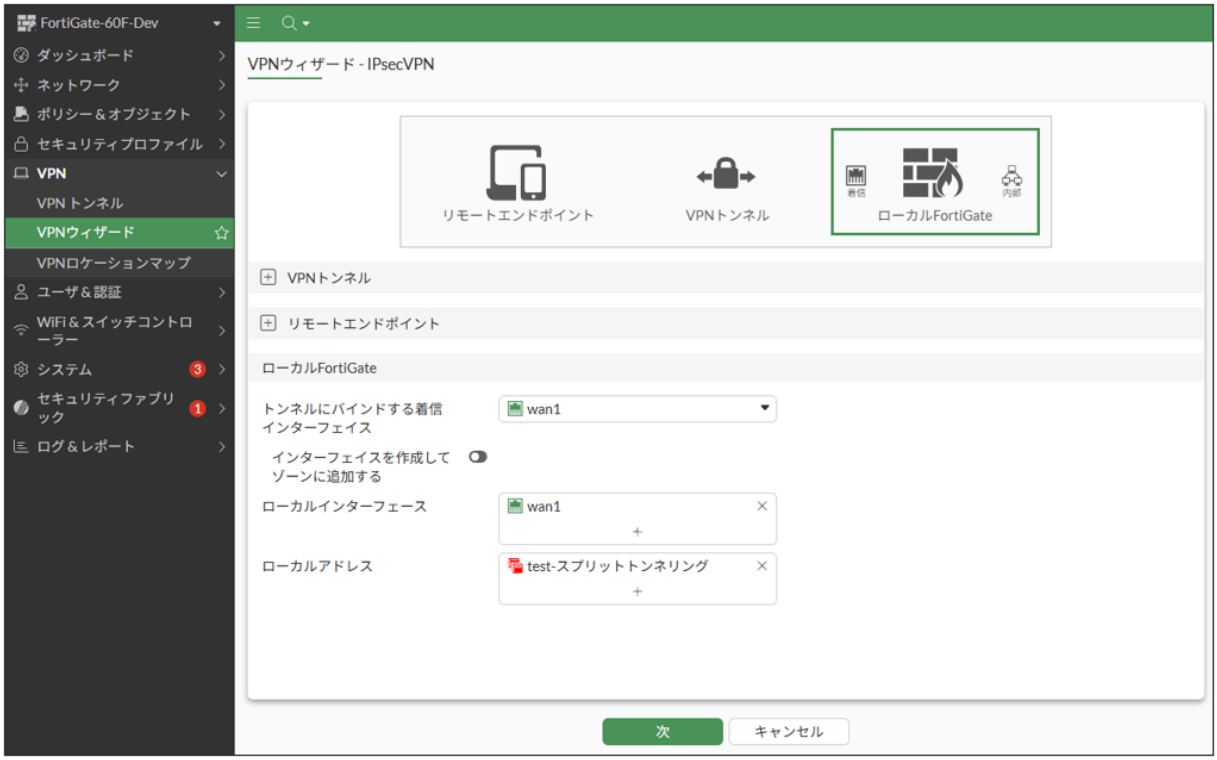
Peer certificate CA：インポートした中間証明書

EAP ピアの識別：EAP ID 要求

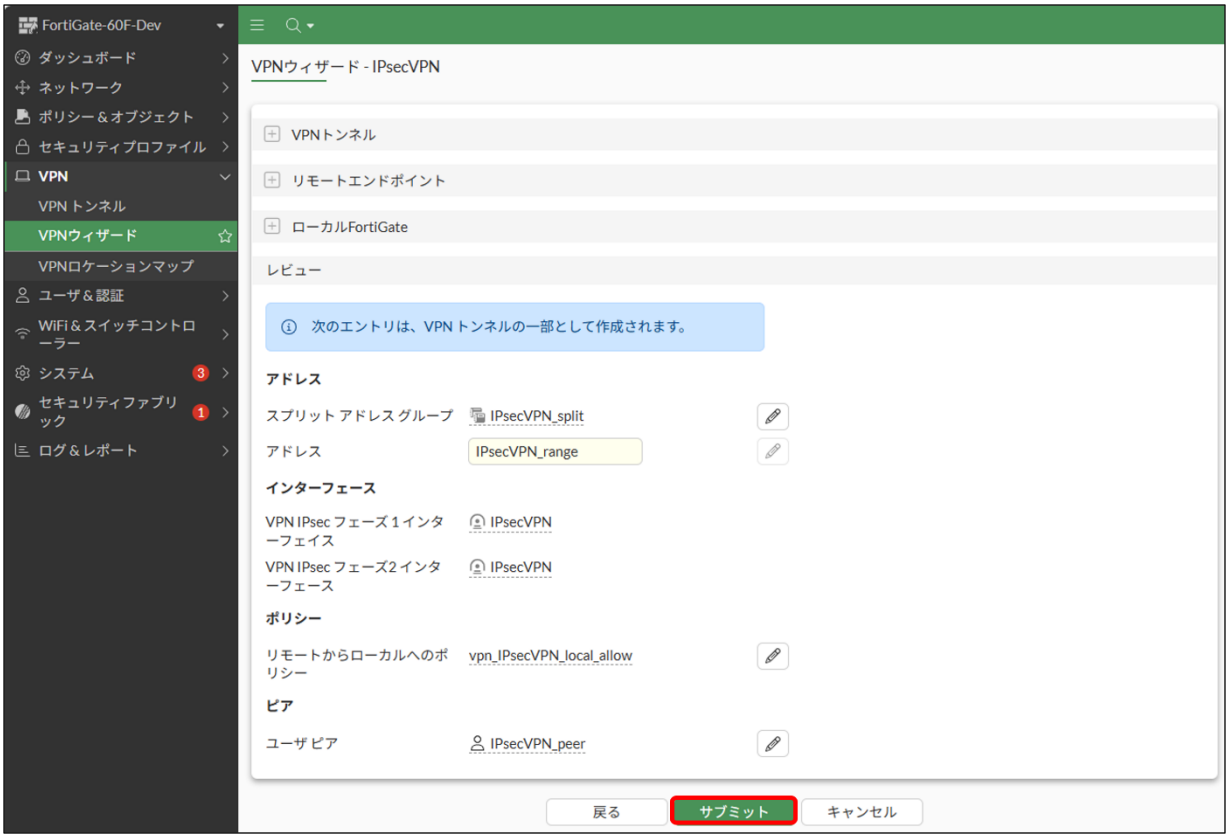
ユーザ認証方法：[フェーズ１インターフェース］－［作成したグループ］

リモートエンドポイントをご利用の環境に応じて設定し「次」をクリックします。

続いて、ローカル FortiGate を設定し「次」をクリックします。



確認画面が表示されるので、設定の確認を行い「サブミット」をクリックします。



3.8. IPsec トンネルの設定

「VPN」-「VPN トンネル」から作成した IPsec トンネルを選択します。

認証項目の下図赤枠を設定し OK をクリックします。

■設定例

受理されたピア ID：「ピア証明書」または「ピア証明書グループ」

ピア証明書：作成した PKI ユーザまたは PKI グループ

※受理されたピア ID にて認証する証明書を制限します。必要に応じて設定してください。

【補足】

IKE「バージョン１」の設定で iOS 端末で VPN 接続する際は、モードをメインに変更する必要がある場合がございます。

■モードの変更方法

下図赤枠のモードを「メイン（ID 保護）」に設定してください。

3.9. ポリシーの設定

「ポリシー&オブジェクト」-「ファイアウォールポリシー」から作成した IPsec トンネルのポリシーを選択します。

VPN 接続に必要な（下図の赤枠内）設定をし「OK」をクリックします。

■設定例

スケジュール：always

着信インターフェース：作成した VPN トンネル

発信インターフェース：wan1（内側の設定は lan）

送信元：IPsecVPN_range

宛先：all（スプリットトンネリング使う際は接続先アドレスを指定）

サービス：ALL

※その他の項目は任意で設定してください。

以上で FortiGate における IPsec-VPN 機能の設定は完了です。

4. ユーザ側での準備

本項はユーザ側の端末で使用する FortiClient の設定手順の説明になります。

4.1. Windows（Windows11）

ご利用の Windows 端末にて FortiClient をダウンロード･インストールしてください。

FortiClient を起動し、「新規接続の追加」より、以下を参考に設定を追加してください。

■設定例

VPN：IPsec VPN

接続名：任意の値

説明：任意の値

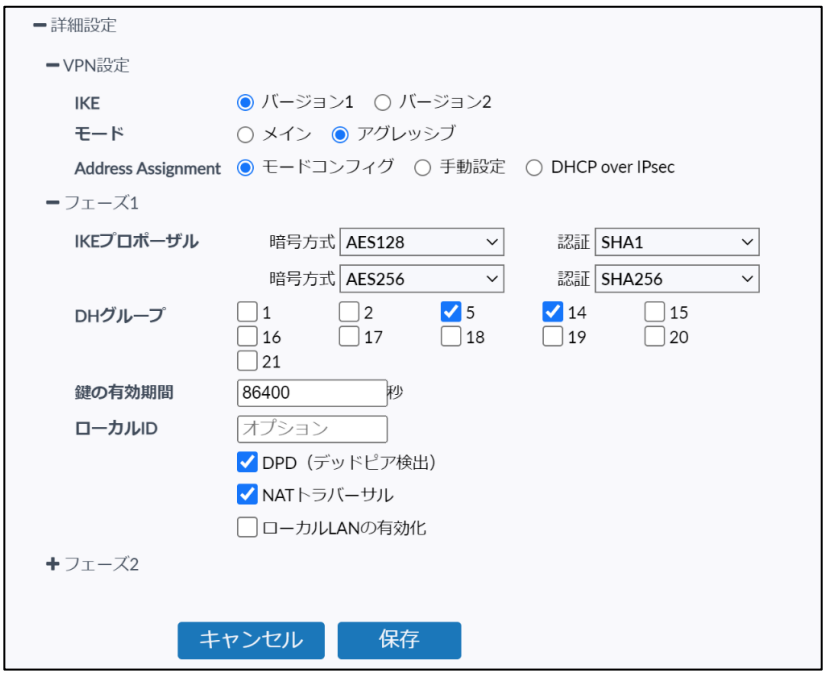
リモート GW：FortiGate の FQDN

認証方式：X.509 証明書

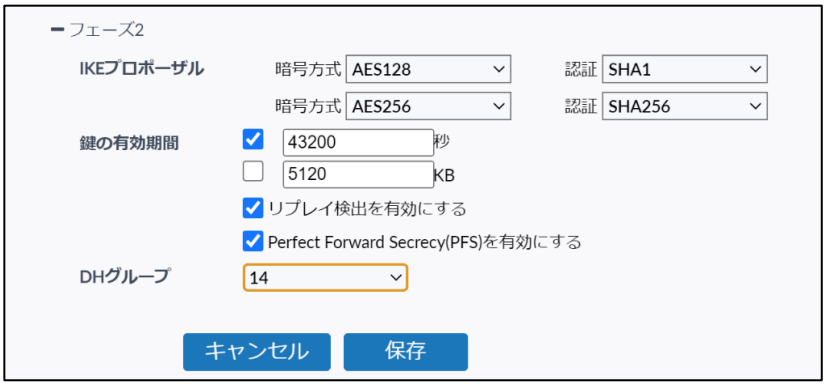
クライアント証明書：ピア証明書で指定した証明書を選択

ユーザ名：ローカルユーザ名

「詳細設定」-「VPN 設定」と「フェーズ 1」 をクリックし、FortiGate 側の IPsec トンネルの設定に合わせて下記設定を行ってください。



続けて「フェーズ 2」をクリックし下記設定を行い、「保存」をクリックします。



以上で Windows 端末における FortiClient の VPN 設定は完了です。

【補足】IPsec トンネルの設定内容の確認方法

FortiGate の CLI コンソールを使って以下コマンドを実行し確認してください。

■フェーズ 1

config vpn ipsec phase1-interface

get <IPsec トンネル名>

■フェーズ 2

config vpn ipsec phase2-interface

get <IPsec トンネル名>

4.2. iOS（iOS18.5）

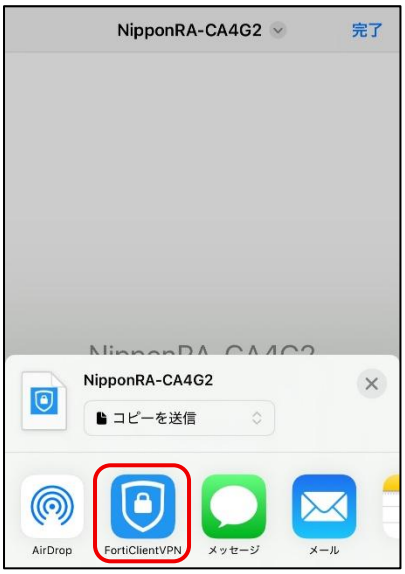
■クライアント証明書のインポート

FortiClient へのクライアント証明書のインポートは、証明書ファイルの拡張子を.p12 から.fctp12 に変更する必要があります。iOS 標準のプロファイル（証明書ストア）にインストールしたクライアント証明書は FortiClient で指定できません。

ご利用の iOS 端末にて FortiClient をダウンロード･インストールしてください。

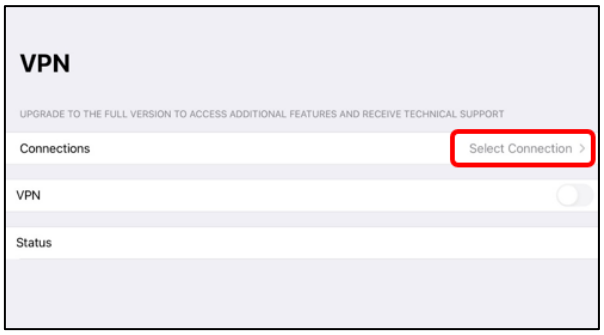
拡張子を.fctp12 に変更した証明書ファイルを iOS 端末に配布します。

証明書ファイルを選択して、FortiClient アプリにコピーします。

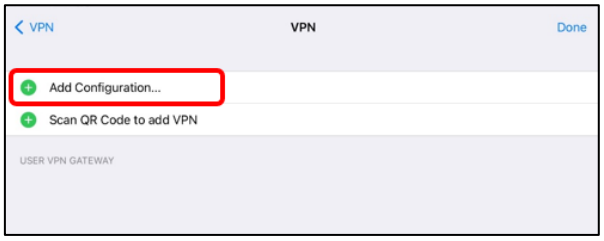


「OK」をタップし、クライアント証明書のインポートは完了です。

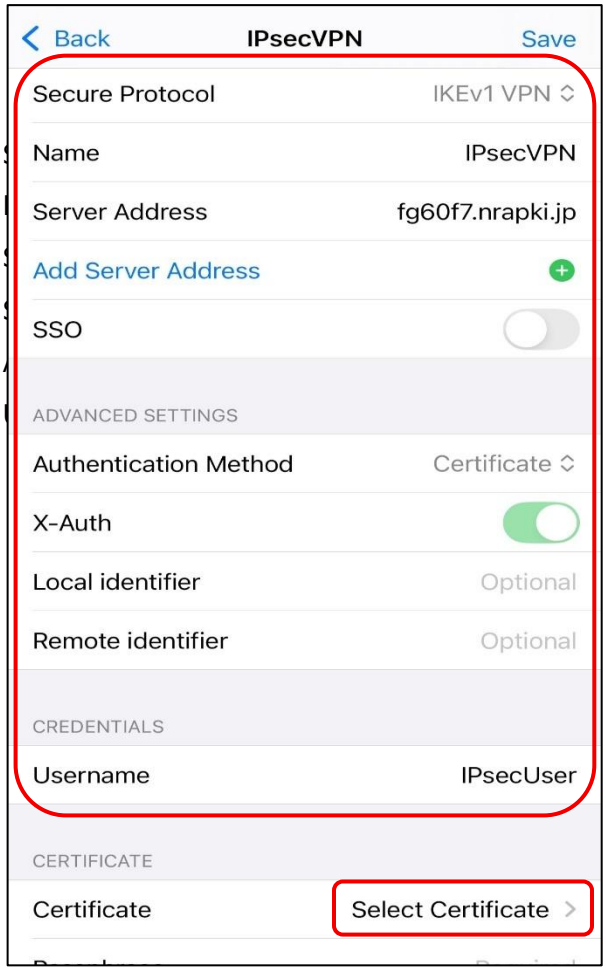
FortiClient を起動し、「Select Connection」をタップします。



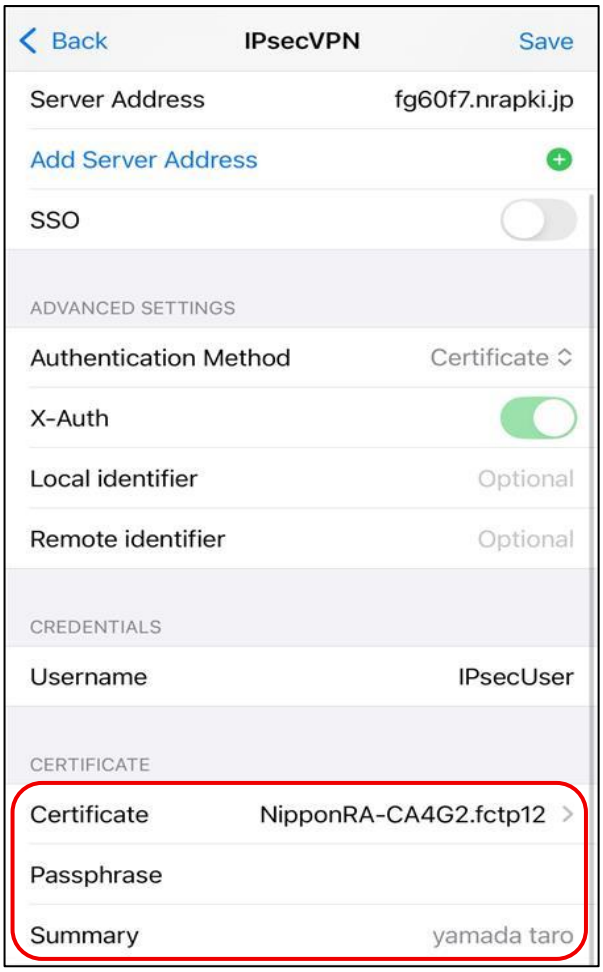
「Add Configuration」をタップします。



FortiGate 側の IPsec トンネルの設定に合わせて下図の赤枠内の項目を入力し、「Select Certificate」をタップします。



事前にインポートしたクライアント証明書を選択し、「Passphrase」にクライアント証明書のパスワードを入力してください。



「Save」をタップします。

以上で iOS 端末における FortiClient の VPN 設定は完了です。

5. サーバ証明書の入れ替え手順

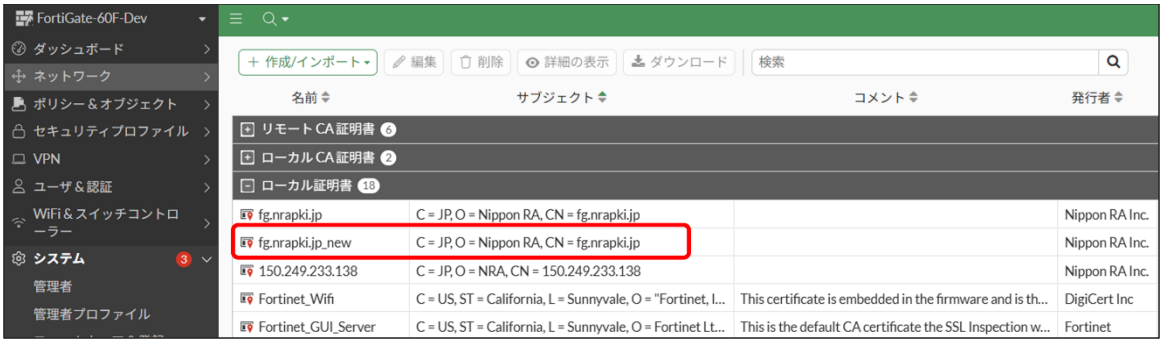
本項ではインポートしたサーバ証明書の入れ替え手順の説明になります。

サーバ証明書の有効期限が切れる前に実施してください。

5.1. 新しいサーバ証明書のインポート

3.2. 証明書のインポートの手順で新しいサーバ証明書をインポートします。

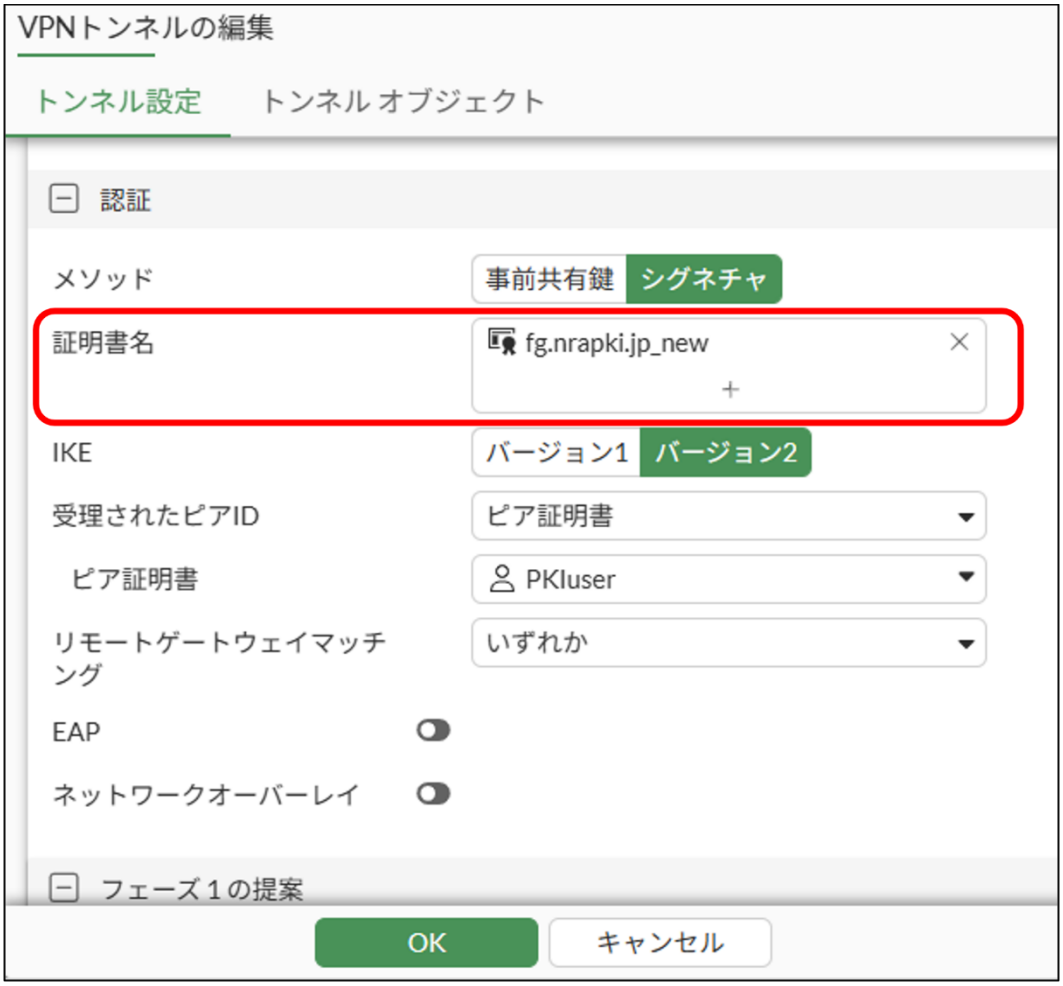
サーバ証明書がインポートされたことを確認します。



5.2. サーバ証明書の設定

「VPN」-「VPN トンネル」から対象の IPsec トンネルを選択します。

認証項目の「証明書名」を新しいサーバ証明書に変更して、「OK」をクリックします。



以上でサーバ証明書入れ替え完了です。古いサーバ証明書は必要に応じて削除してください。