NRA

FortiGate(OS 6.0)における クライアント証明書認証設定 手順

2023年01月18日

Ver. 1.02

改訂履歴

版	日　付	内　容	備　考
Ver. 1.00	--	初版作成	
Ver. 1.01	2022/7/25	誤植修正	
Ver. 1.02	2023/1/18	誤植修正	

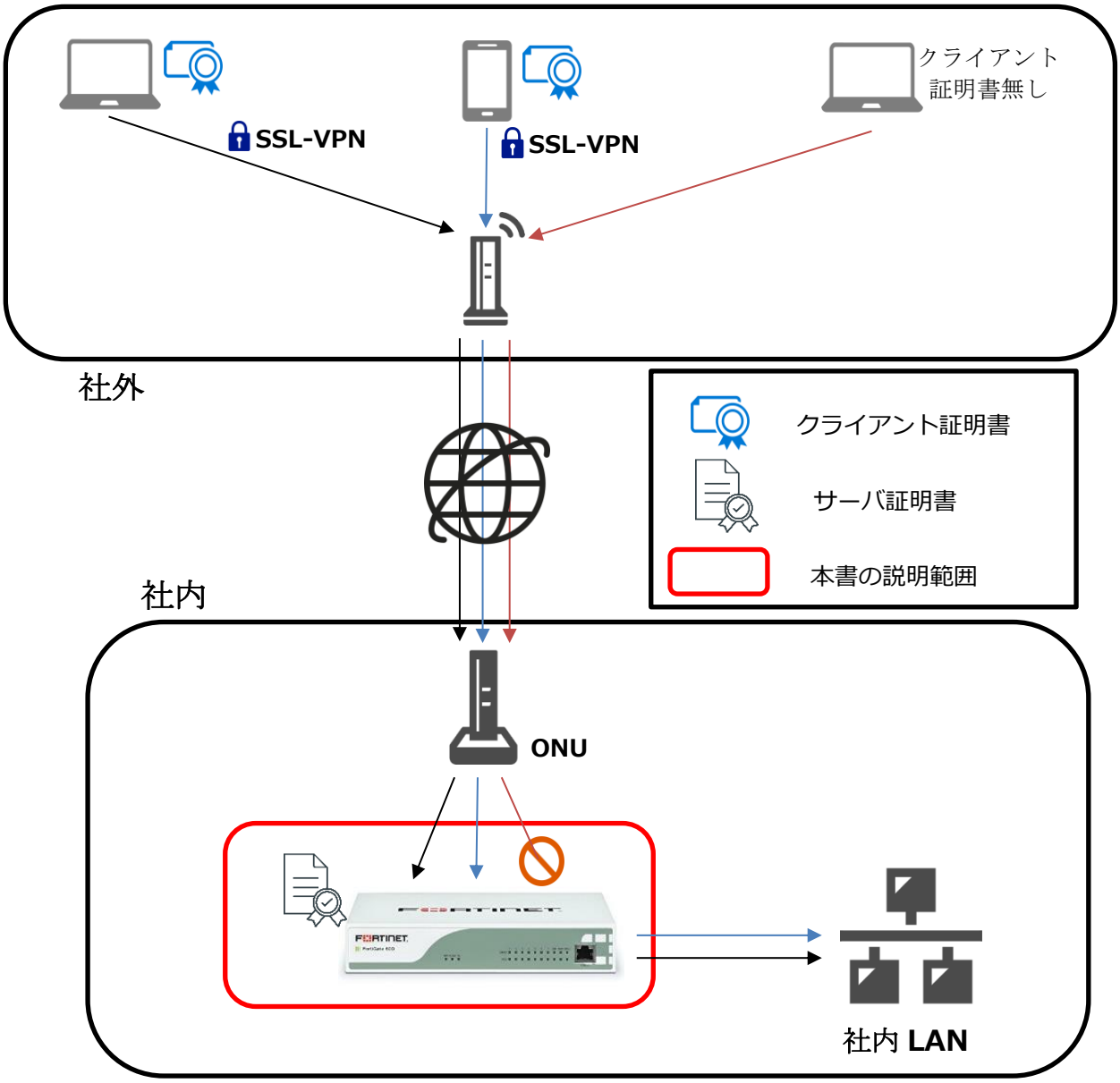
<目　次>

1. 概要

本書は Fortinet 社が提供している FortiGate(OS 6.0)における SSL-VPN 機能について、クライアント証明書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】



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

以下 URL よりダウンロードしてください

・https://www.nrapki.jp/nrawp/cert/NipponRARootCertificationAuthority.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)

https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority3.crt

・中間証明書(CA4)

https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority4.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)

http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority3/cdp.crl

・中間認証局(CA4)

http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority4/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、なければ CA3 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

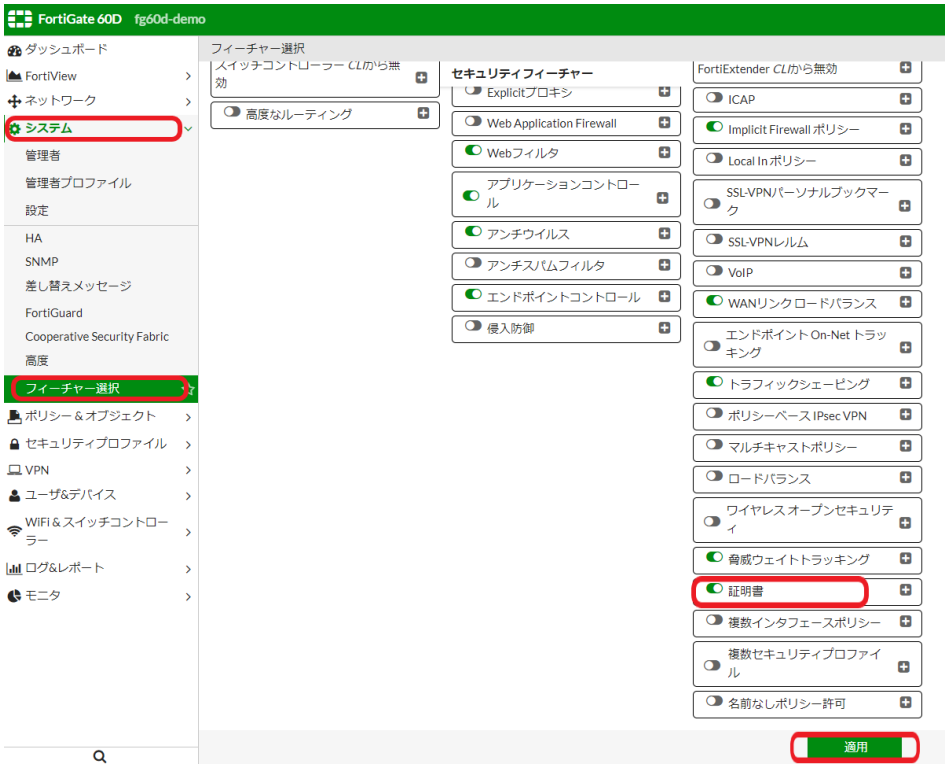
本項から詳細な設定手順に関する説明になります。

流れは次の通りです。

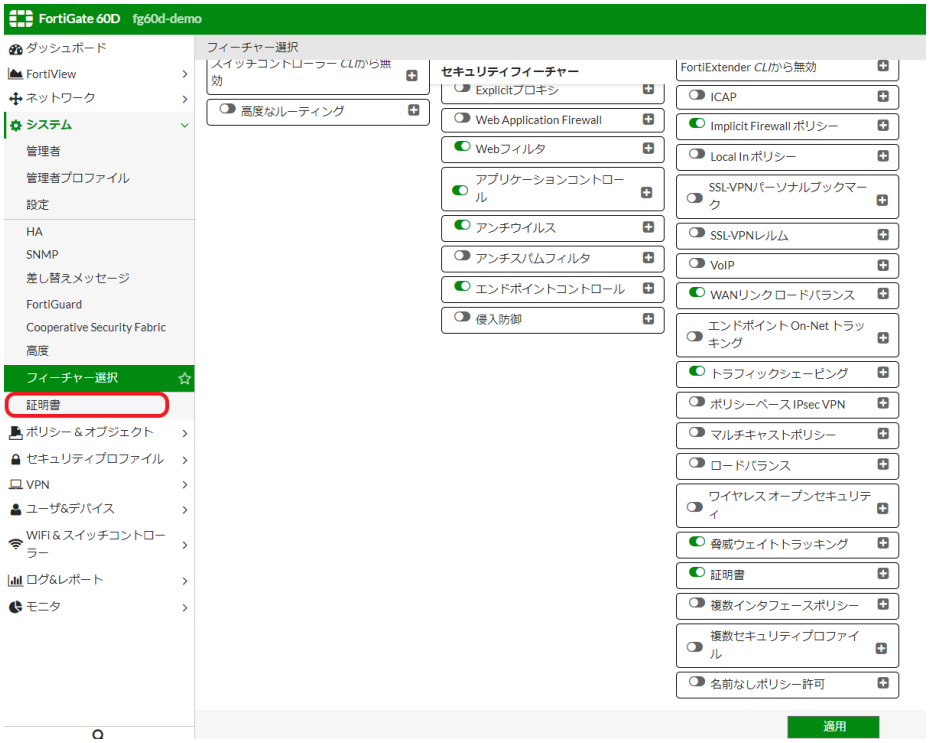
項目は以上です。次ページから各項目の説明の記載になります。

3.1. 証明書メニューの有効化

管理画面から「システム」-「フィーチャー選択」より証明書を有効化し適用をクリックします。



以下図のように「フィーチャー選択」の下に「証明書」の項目が表示されます。

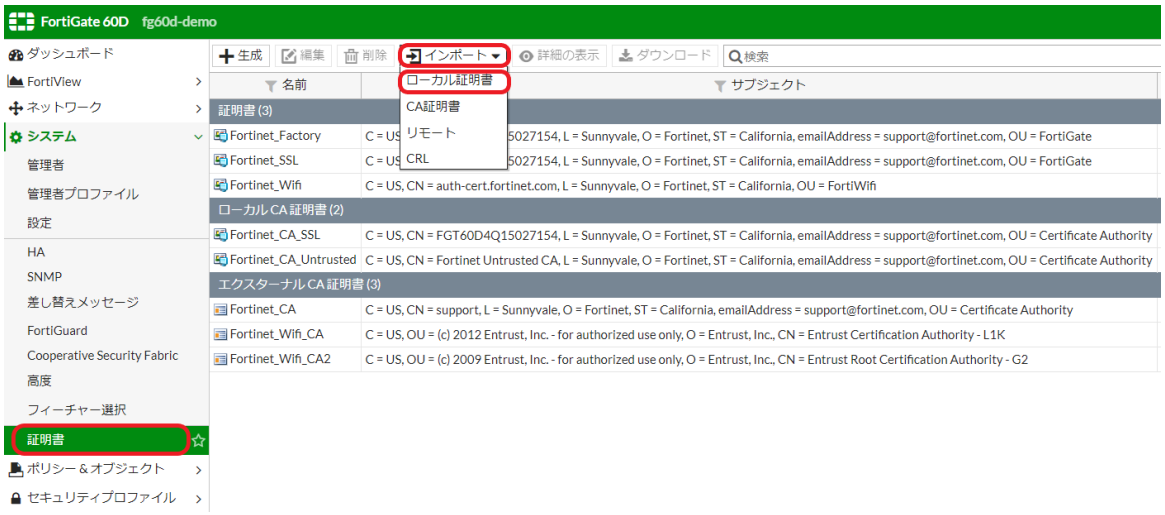


3.2. 証明書のインポート

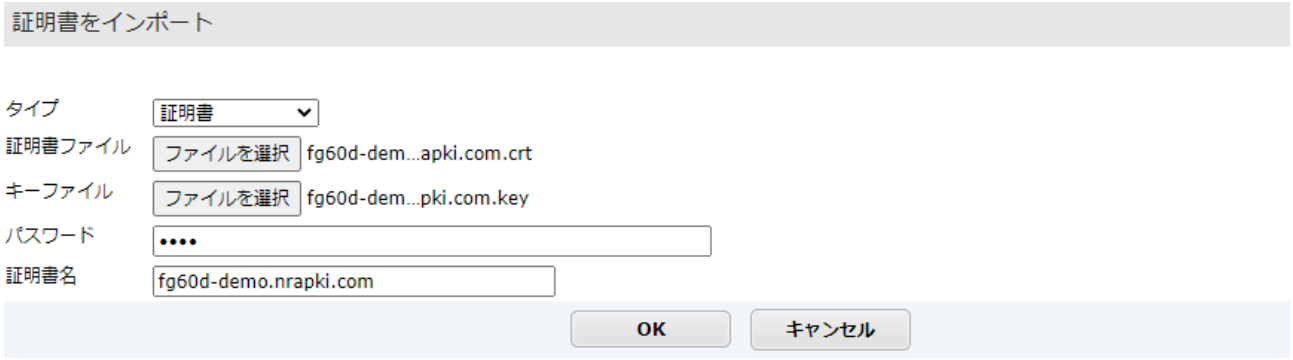
事前準備で用意した各証明書と CRL(失効リスト)をインポートします。

■サーバ証明書

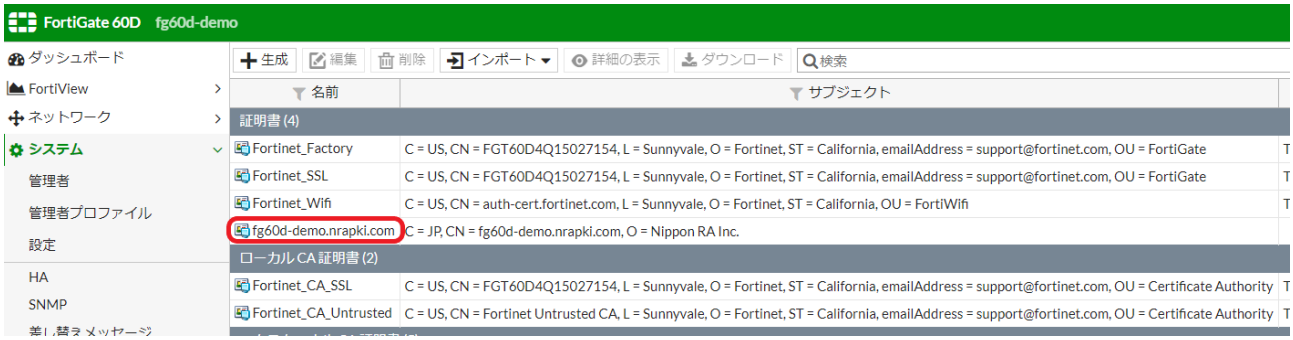
「システム」-「証明書」を選択し、「インポート」から「ローカル証明書」を選択します。



「証明書をインポート」の画面が表示されます。「タイプ」のリストから「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 OK をクリックします

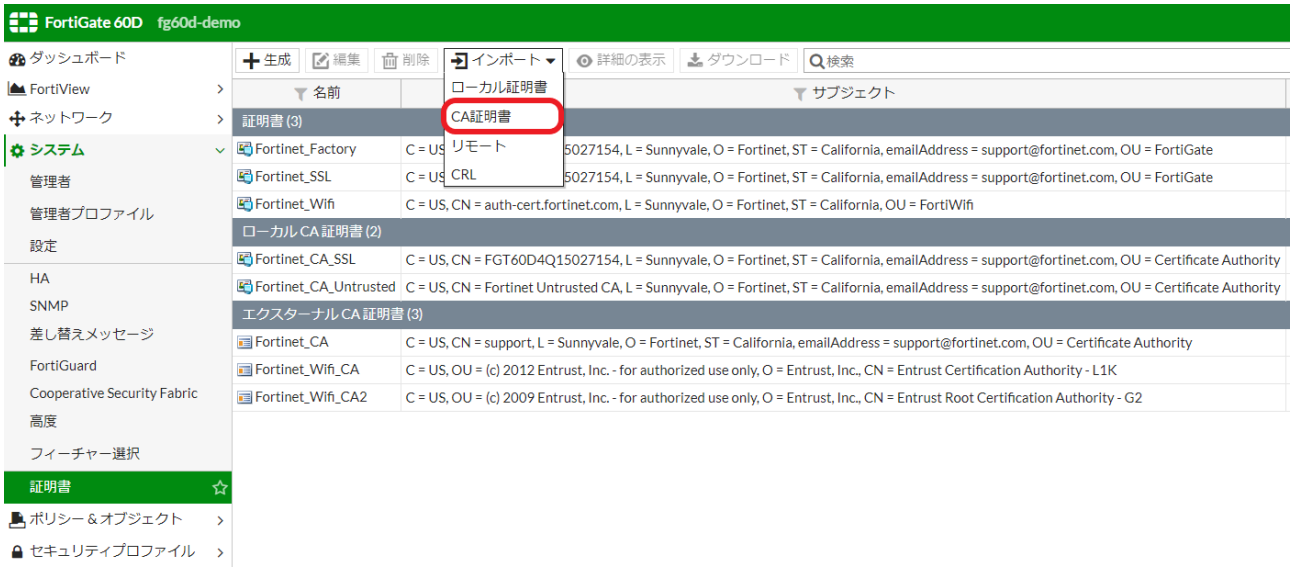


サーバ証明書がインポートされたことを確認します。

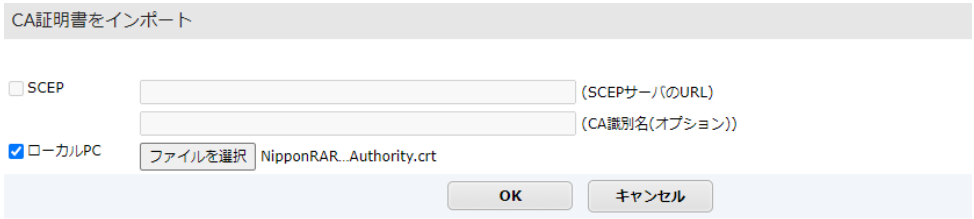


■ルート証明書、中間証明書

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

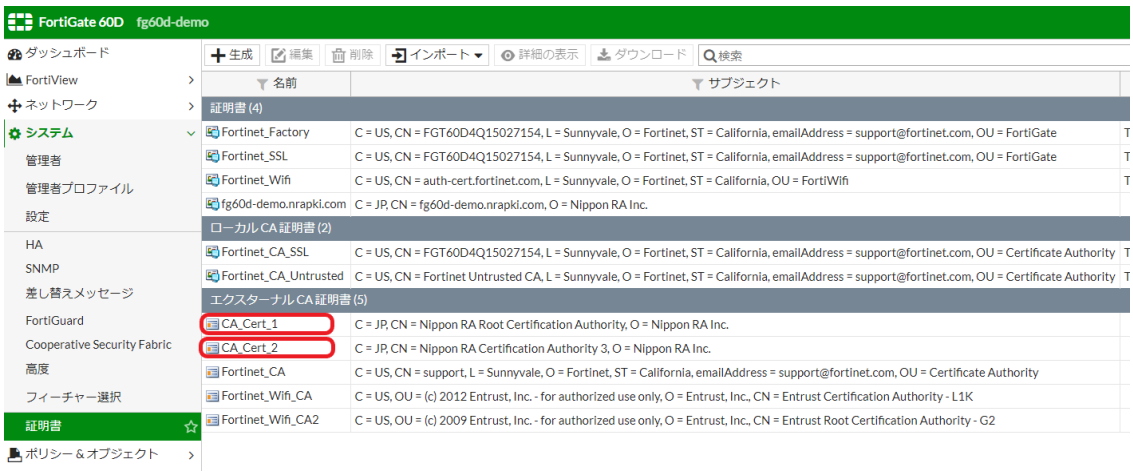


「ローカル PC」を選択し「ファイルを選択」からルート証明書を選択し OK クリックします。



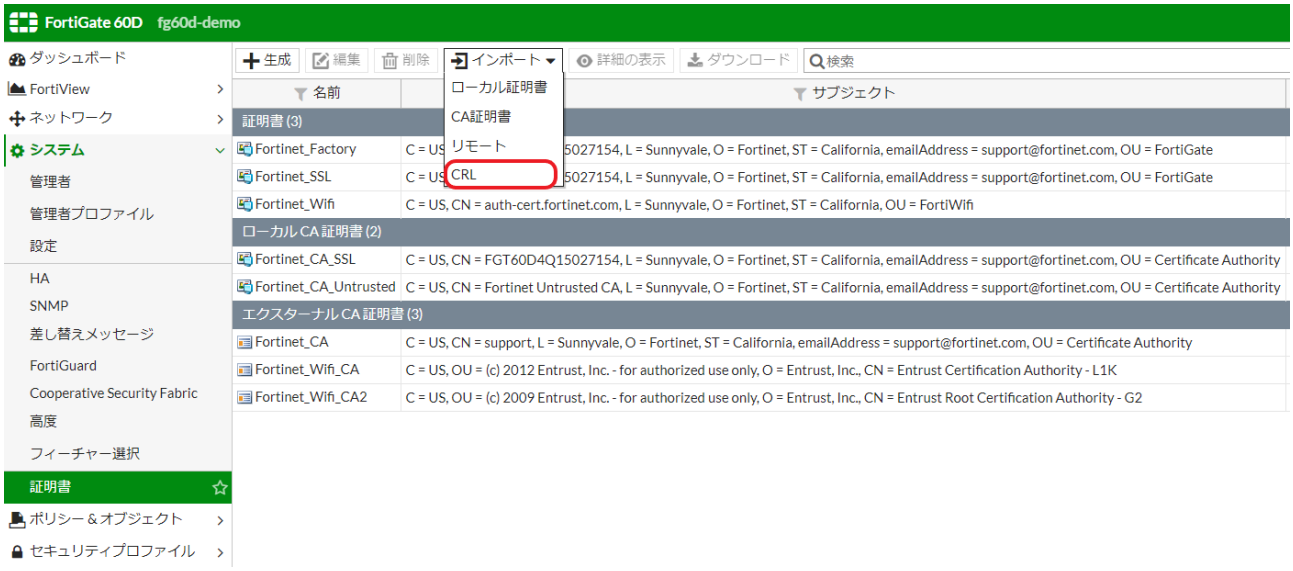
同手順にて中間証明書もインポートします。

ルート証明書、中間証明書をインポートされたことを確認します。



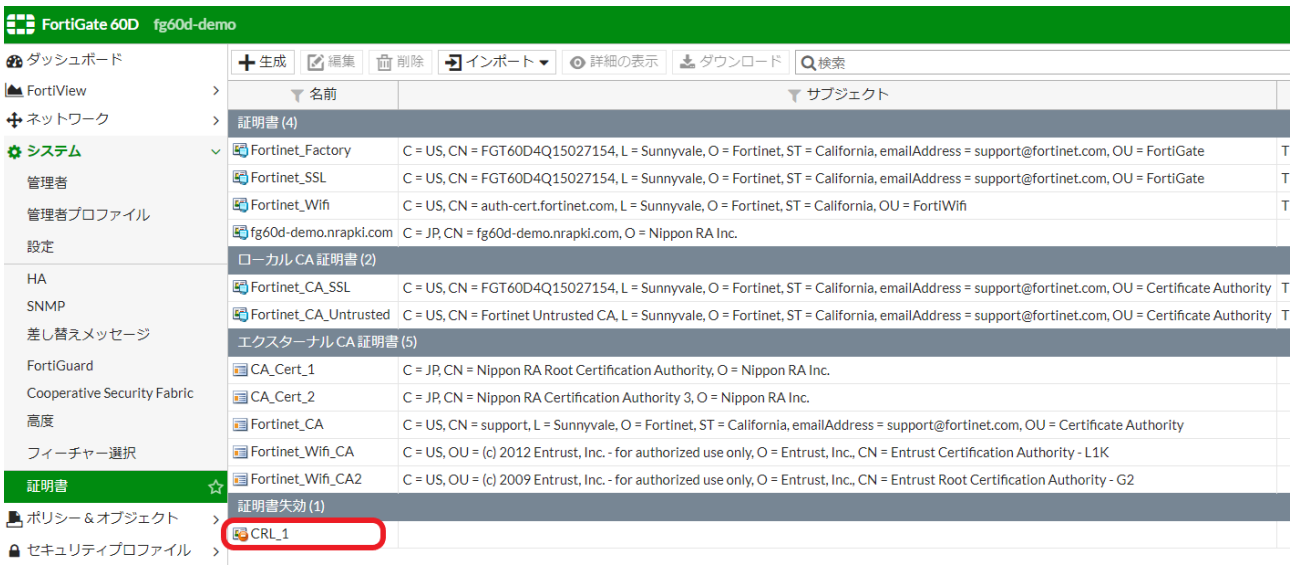
■CRL(失効リスト)

「システム」-「証明書」を選択し、「インポート」から「CRL」を選択します



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。

CRL がインポートされたことを確認します



【補足】

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)】

```
FGT50E5619031121 (mpki_ocsp) # get
name                : mpki_ocsp
url                 : http://mpkiocsp.managedpki.ne.jp/mpkiocsp
cert                : CA_Cert_1
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)】

```
FGT50E5619031121 (setting) # get
ocsp-status         : enable
ssl-ocsp-status     : enable
ssl-ocsp-option     : server
ocsp-default-server : mpki_ocsp
check-ca-cert       : enable
check-ca-chain      : disable
subject-match       : substring
cn-match            : substring
strict-crl-check    : disable
strict-ocsp-check   : disable
ssl-min-proto-version: default
cmp-save-extra-certs: disable
certname-rsa1024    : Fortinet_SSL_RSA1024
certname-rsa2048    : Fortinet_SSL_RSA2048
certname-dsa1024    : Fortinet_SSL_DSA1024
certname-dsa2048    : Fortinet_SSL_DSA2048
certname-ecdsa256   : Fortinet_SSL_ECDSA256
certname-ecdsa384   : Fortinet_SSL_ECDSA384
```

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

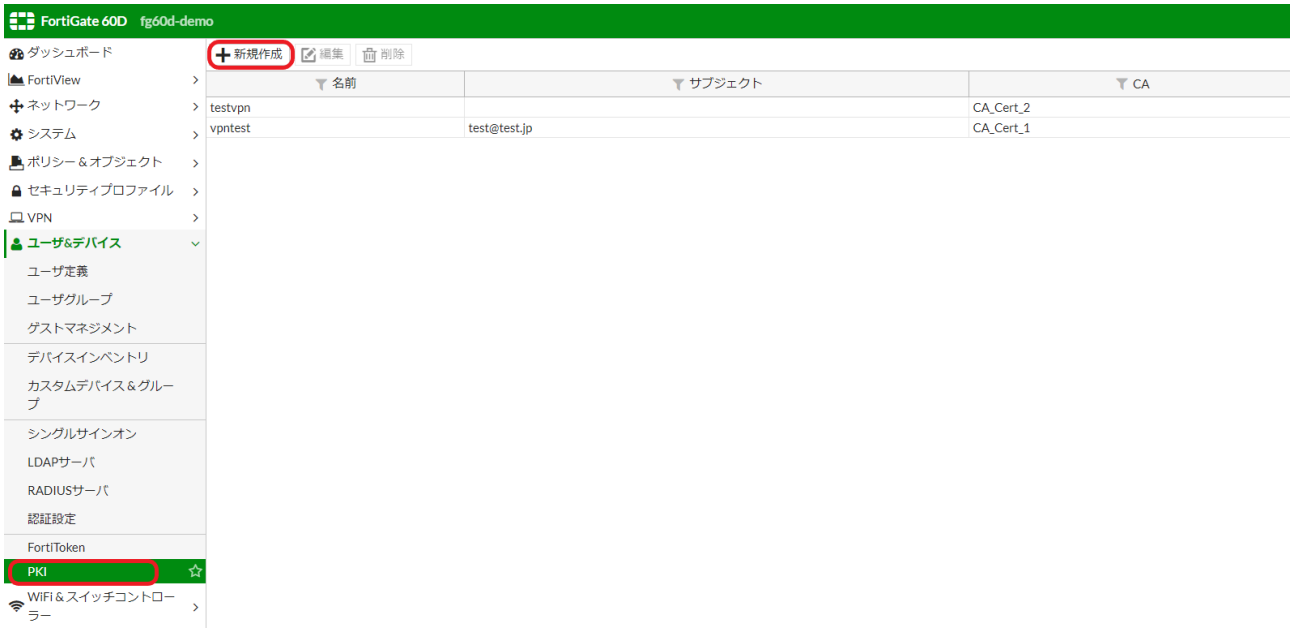
set ocsp-status enable

end

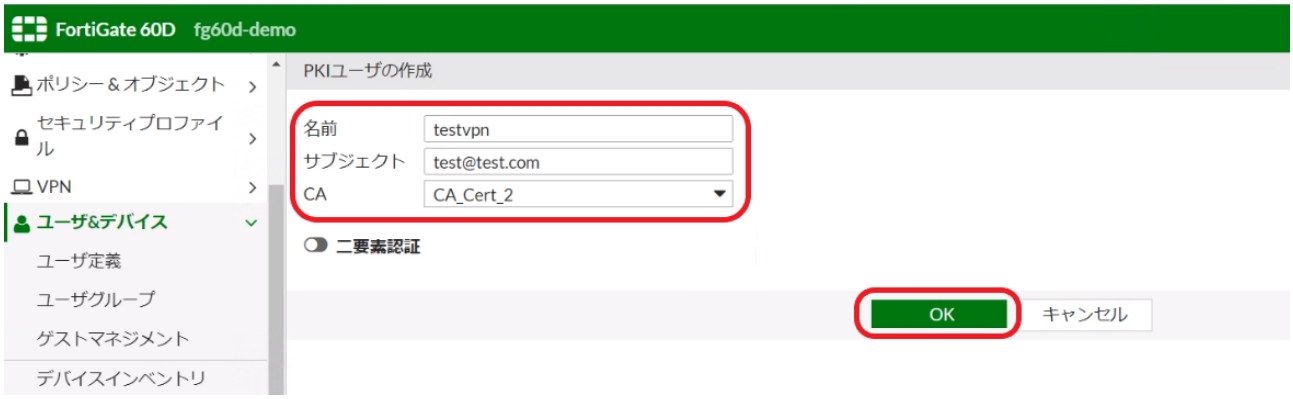
exit

3.3. PKI ユーザの作成

「ユーザ&デバイス」-「PKI」を選択し、新規作成を選択。



以下画像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。サブジェクト E(メールアドレス)で判断する場合には『xxxx@xx.xx』のように、E=などは入力せずメールアドレスのみ入力してください。

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。

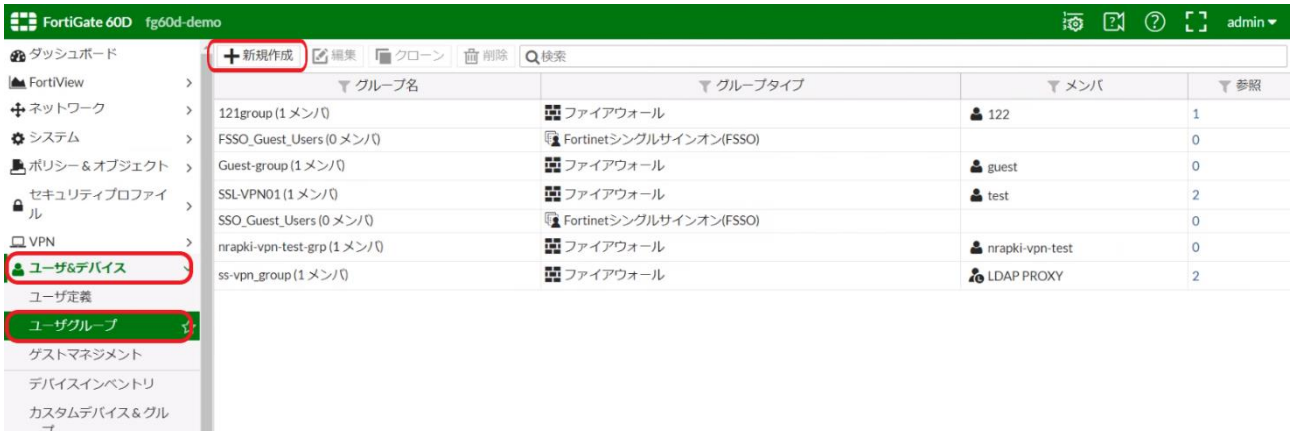
【補足 2】

「ユーザ&デバイス」に「PKI」を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。
登録後に一度管理画面がらログアウトし、再度ログインすると管理画面から「PKI」の項目が表示されます。

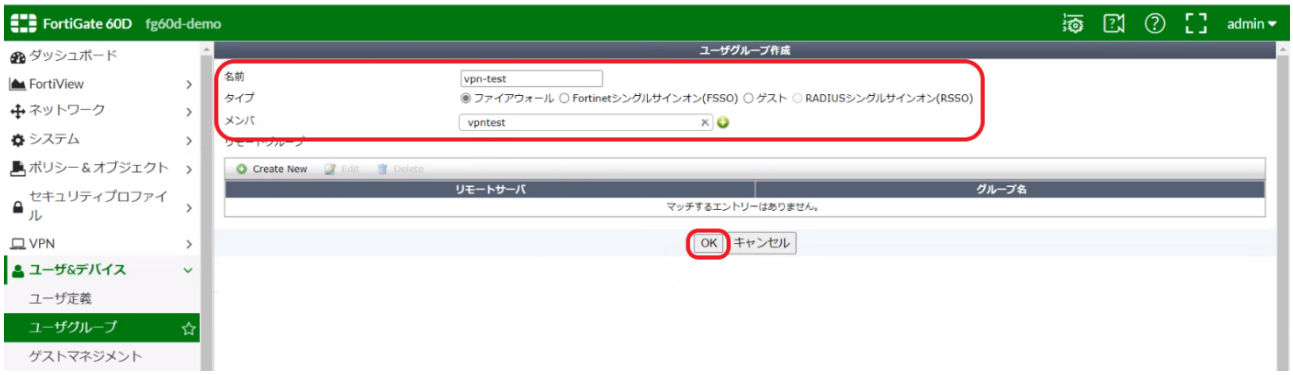
config user peer
edit <ユーザ名> ※任意の値
set ca CA_Cert_1（CA_cert_1 は中間証明書。必要に応じて名前は変更）
 <Email アドレス>（あとで UI で変更可能。今設定しなくても OK。）
end
exit

3.4. グループの作成

「ユーザ&デバイス」-「ユーザグループ」から「新規作成」をクリックします。



以下画像の赤枠内の項目を設定し OK をクリックします。



■設定例

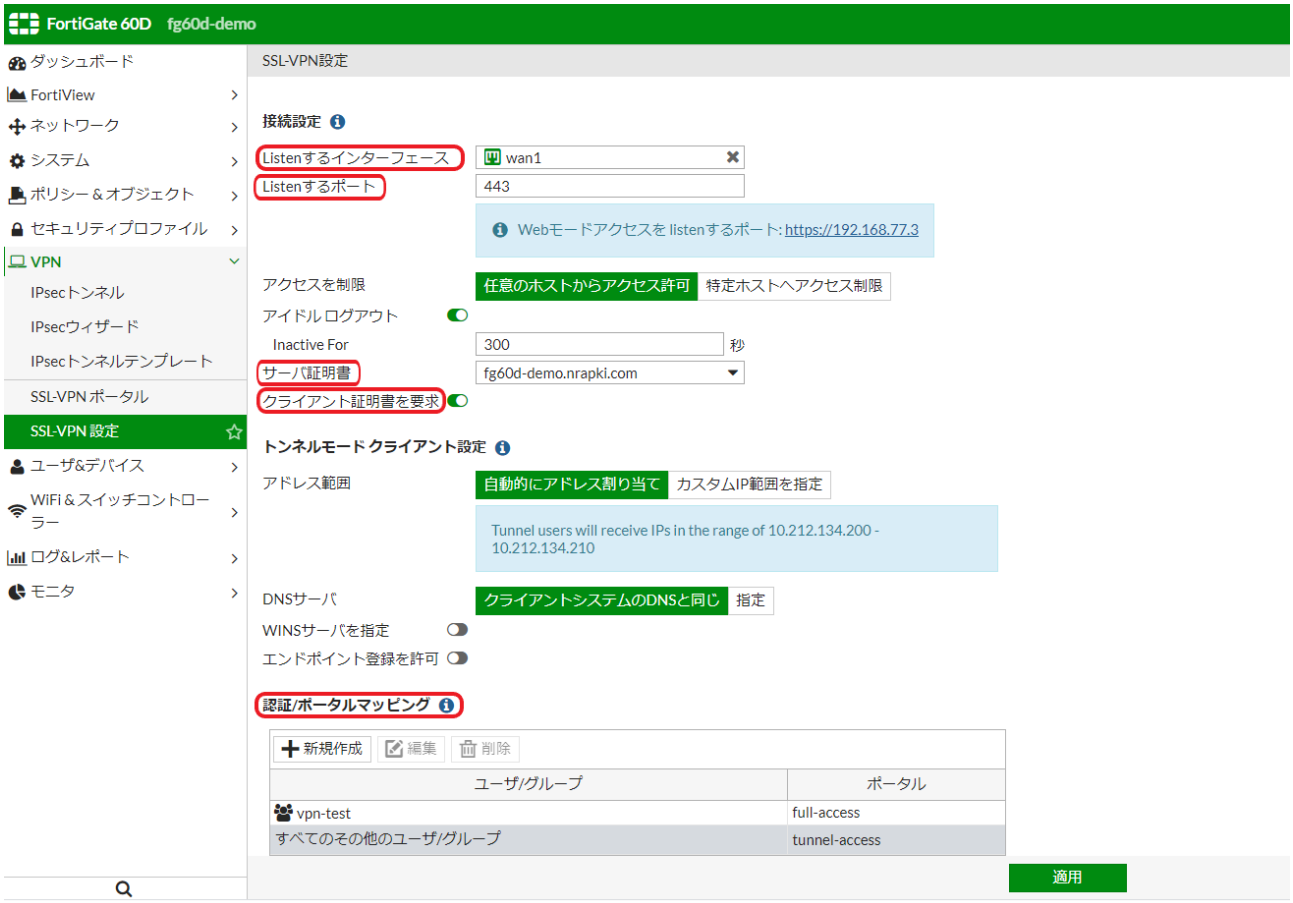
名前：任意の値

タイプ：ファイアウォール

メンバ：作成した PKI ユーザを選択

3.5. SSL-VPN の設定

「VPN」-「SSL-VPN 設定」から以下画像の赤枠の項目を設定し「適用」をクリックします。



■設定例

Listen するインターフェース：wan1

Listen するポート：任意（後述「ユーザ側での準備」で使用します）

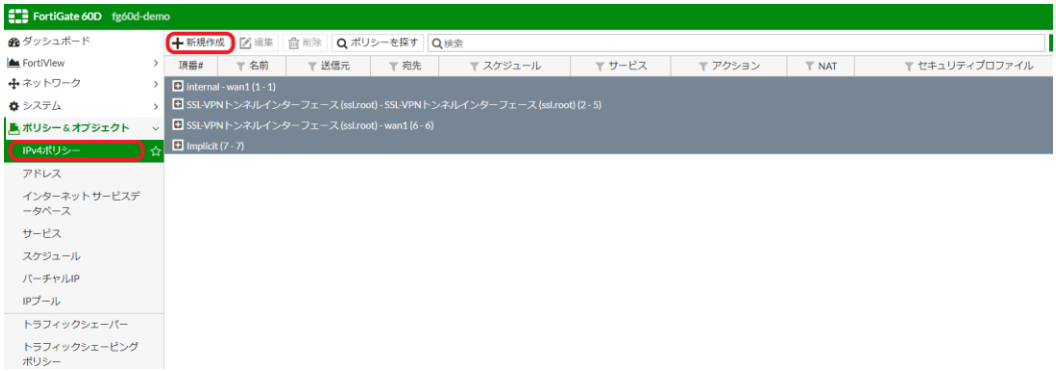
サーバ証明書：インポートしたサーバ証明書を選択

クライアント証明書を要求：チェック

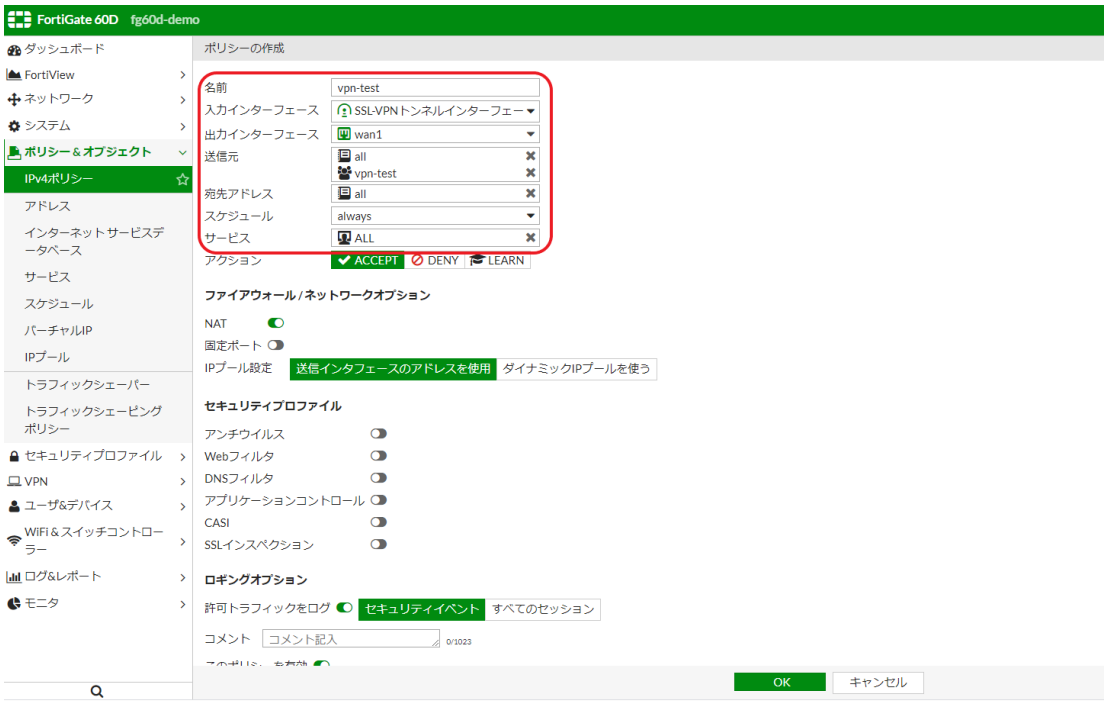
認証/ポータルマッピング：新規作成をクリックし、「ユーザ/グループ」は作成した PKI ユーザが入っているグループ、ポータルは任意で設定。

3.6. ポリシーの設定

「ポリシー&オブジェクト」-「IPv4 ポリシー」から新規作成をクリックします。



以下画像の赤枠内の項目を設定し OK をクリックします。



■設定例

入力インターフェース：SSL-VPN トンネルインターフェース

出力インターフェース：wan1（内側の設定は lan）

送信元：all、SSLVPN-UserGroup

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）

スケジュール：always

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(OS6.0)における SSL-VPN 機能の設定は完了です。

4. ユーザ側での準備(WindowsPC)

ユーザのご利用の端末にて Forticliant をダウンロード･インストールしてください。

Forticliant を起動し、「リモートアクセス」から「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：SSL-VPN

接続名：任意の値

説明：任意の値

リモート GW：fortiGate のグローバル IP アドレス

ポートの編集：チェック入れ、4.SSL-VPN 設定で設定した「Listen するポート」を指定

クライアント証明書：PKI ユーザ作成時に指定した証明書を選択

認証：任意

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。

事前準備

・新しい SSL サーバ証明書(PEM 形式)

流れは次の通りです。

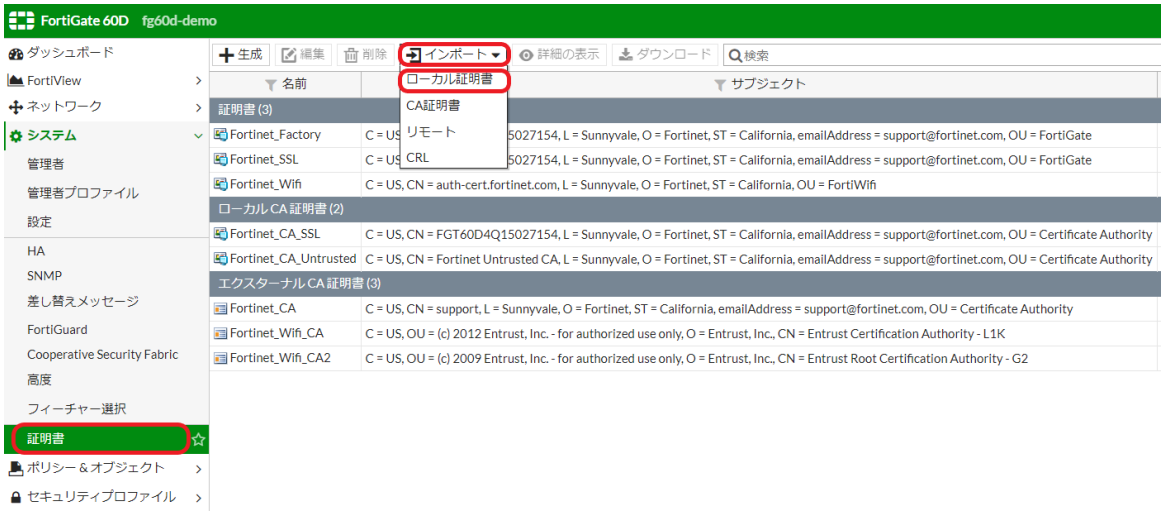
準備していただいた新しい SSL サーバ証明書をインポートします

インポートした新しいサーバ証明書と現在設定しているサーバ証明書を入れ替えます。

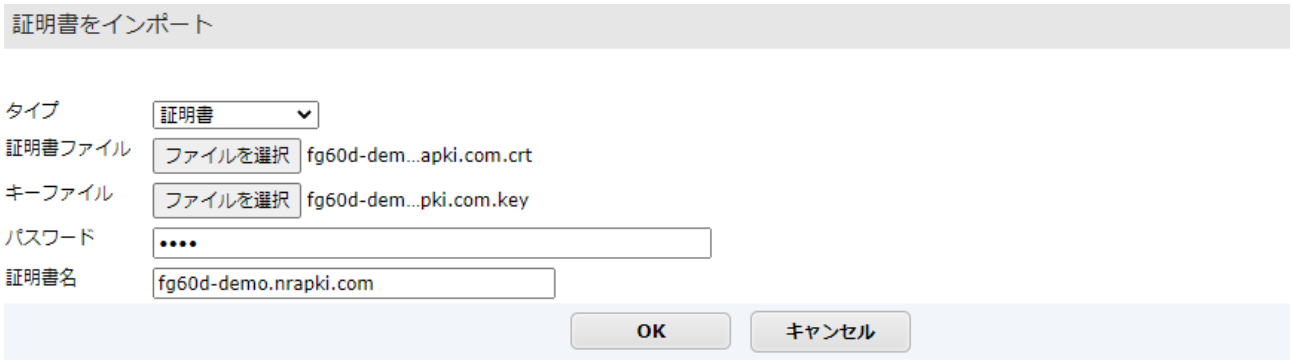
項目は以上です。次ページから各項目の説明の記載になります。

5.1. 新しいサーバ証明書のインポート

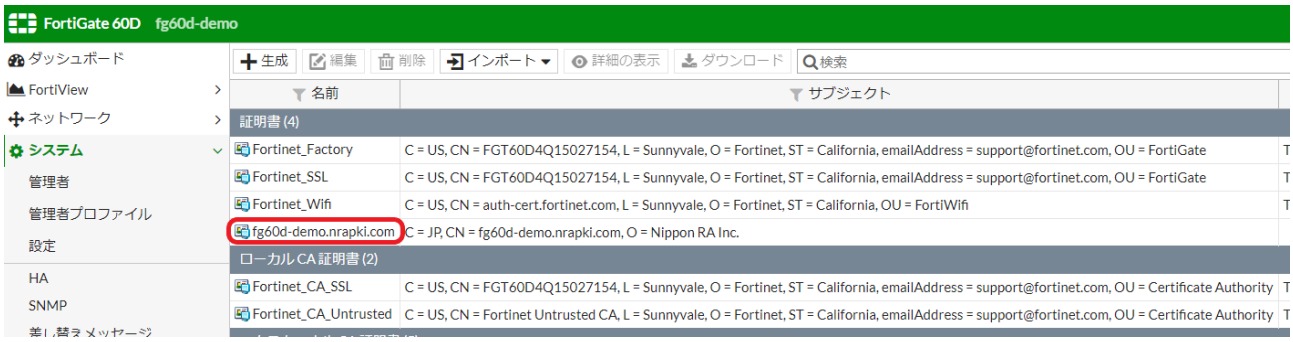
「システム」-「証明書」を選択し、「インポート」から「ローカル証明書」を選択します。



「証明書をインポート」の画面が表示されます。「タイプ」のリストから「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 OK をクリックします

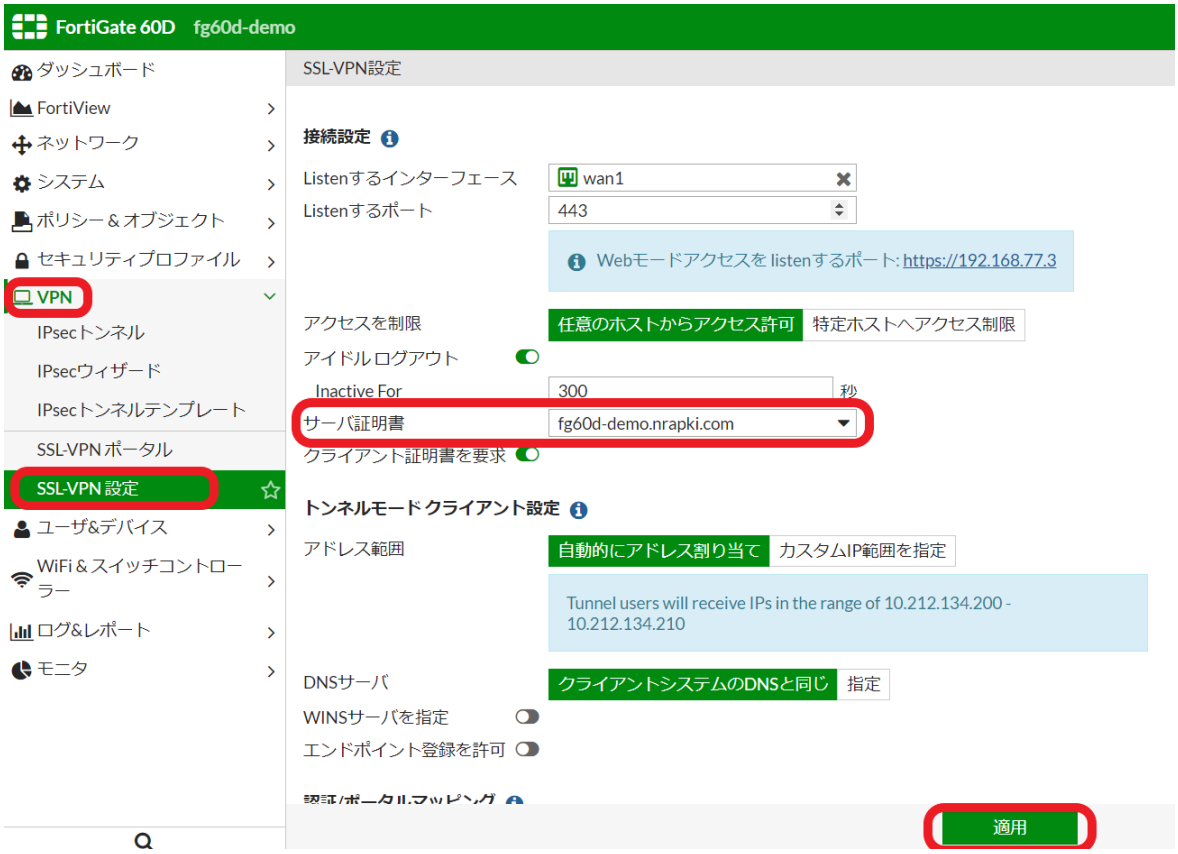


サーバ証明書がインポートされたことを確認します。



5.2. サーバ証明書の設定

「VPN」-「SSL-VPN 設定」から「サーバ証明書」の項目をインポートした新しい証明書に変更し、「適用」をクリックします。



以上の手順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。