FortiGateで実装する、リモートアクセスソリューション

認証にクライアント証明書を採用した
SSL-VPN機能のセットアップ手順

NRA

資料構成

1. はじめに
2. リモートアクセスのニーズと課題
3. 本資料で検証した接続構成
4. FortiGate導入ステップ
5. SSL-VPN機能の利用に向けて準備
6. SSL-VPNセットアップ（クライアント証明書認証）
7. FortiClientセットアップ

Appendix：FortiGate初期設定

１．はじめに

- 本書では、リモートアクセスソリューションとして、Fortinet社 FortiGateのVPN機能をセキュアに利用する手順をご紹介します。

２．リモートアクセスのニーズと課題

ニーズ

・社外（外出先・出張先）から社内LANに接続して業務を行うために、リモートアクセス（VPNアクセス）の利用が普及している

セキュリティの課題

・ID/パスワードの認証設定が主流でインターネットが繋がるデバイスがあれば、どこからでもアクセス可能になっている

解決策：ID/パスワードにクライアント証明書の認証要素を追加する

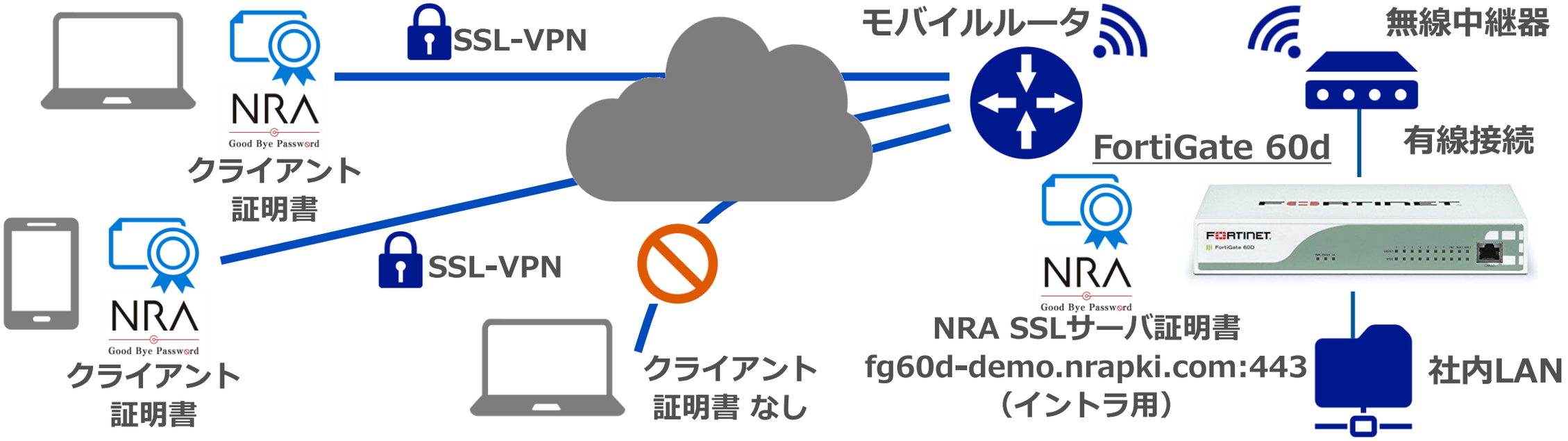
・リモートアクセスの許可デバイスの特定ができる

・デバイスの盗難／紛失時の不正利用を防止できる

3．本資料で検証した接続構成

接続構成

回線をモバイルルータで代用し、外部からのアクセスをクライアント証明書を保持した端末のみとする



４．FortiGate導入ステップ

①設計

- 初期パラメータの決定
- 導入環境のネットワークに合わせた設計（ポリシー、IF、ユーザ管理 など）

②現調

- 設置、電源投入
- 初期設定、外部疎通確認

③設定

- SSLサーバ証明書、認証局公開鍵、失効リスト（CRL）インポート
- グループ、ユーザ、VPNポリシー設定

本書で紹介する範囲

5．SSL-VPN機能の利用に向けての準備

NO	項目	例	備考
1	ホスト名	FGT60DXXXX	デフォルトはシリアル番号
2	VPNアクセス時のFQDN	FGT60DXXXX.zzz.co.jp	SSLサーバ証明書の発行に必要
3	管理者パスワード	AdminP@ssword	初期設定は、パスワードなし
4	アクセスグループ	sslvpn_group	任意グループ名を決定
5	アクセスユーザ	sslvpn_user00N	アクセスユーザを特定した払出し
6	アクセスユーザのパスワード	P@ssword	パスワードポリシーは重要

5．SSL-VPN機能の利用に向けての準備

- NRA SSLサーバ証明書の調達

  ⇒FortiGateへのインストールは、PEM形式となります
  　弊社からP12形式をPEM形式に変換し提供します

- NRA 発行局公開鍵（※設定ではダウンロードしたファイルを指定）

  ⇒NRAリポジトリから取得します。中間認証局はご利用の環境に合わせて取得してください。
  （※ご利用中の中間認証局の確認方法については次ページ参照)

  　http://www.nrapki.jp/products/repo.html
  　発行局公開鍵
  　ルート認証局　：http://www.nrapki.jp/products/images/NipponRARootCertificationAuthority.crt
  　中間証明局(CA3)：http://www.nrapki.jp/products/images/NipponRACertificationAuthority3.crt
  　中間認証局(CA4)：http://www.nrapki.jp/products/images/NipponRACertificationAuthority4.crt

- NRA 失効リスト配布URL（※設定ではURLを入力）

  　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

- NRA クライアント証明書の発行

  ⇒弊社と調整の元、提供します

5．SSL-VPN機能の利用に向けての準備

- ご利用中の中間認証局の確認方法

下図の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。

６．SSL-VPN設定（FortiOS 5.4、5.2、5.0）

① 証明書メニューのアクティベーション

② 証明書関連の設定

A) NRAのSSLサーバ証明書インポート

B) NRAの発行局（CA）の公開鍵インポート

C) NRAのCRL（失効リスト）インポート

③ インポートしたSSLサーバ証明書の指定

④ アクセスユーザ、グループの作成

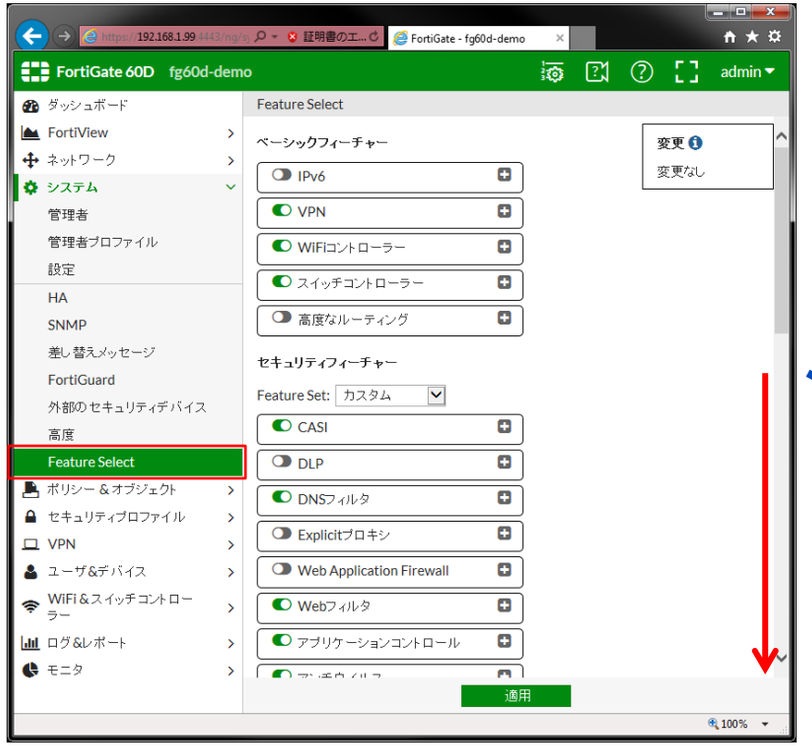
⑤ VPN設定

⑥ SSL-VPNポリシー作成

6．SSL-VPN設定（FortiOS 5.4）

①証明書メニューのアクティベーション

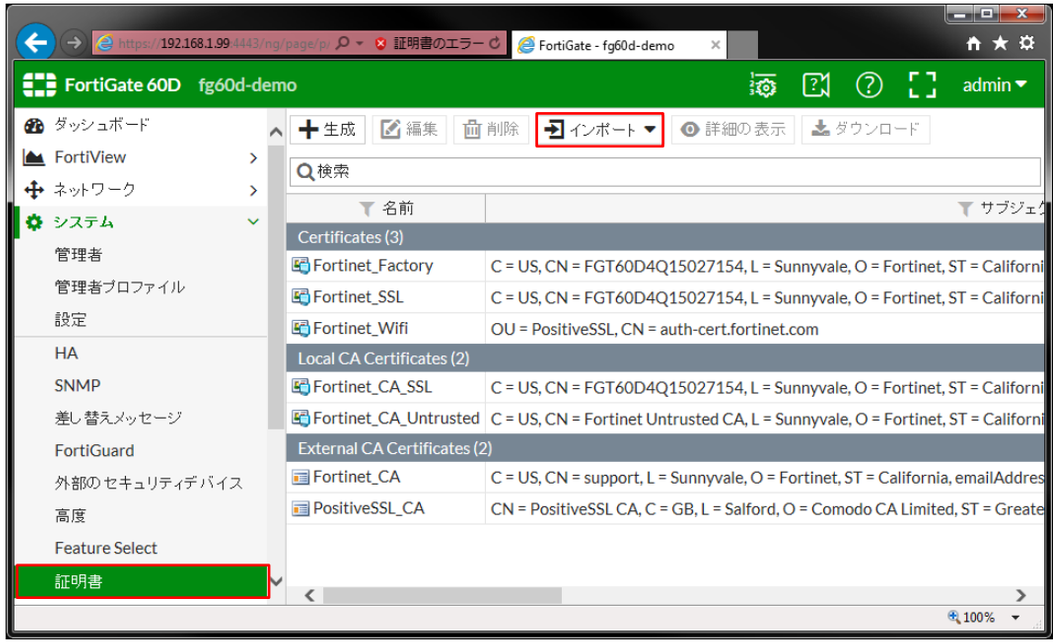
システム⇒Feature Select
下部にスクロール（さらに表示をクリック）



“証明書”をクリックしてON状態として、
“適用”をクリック

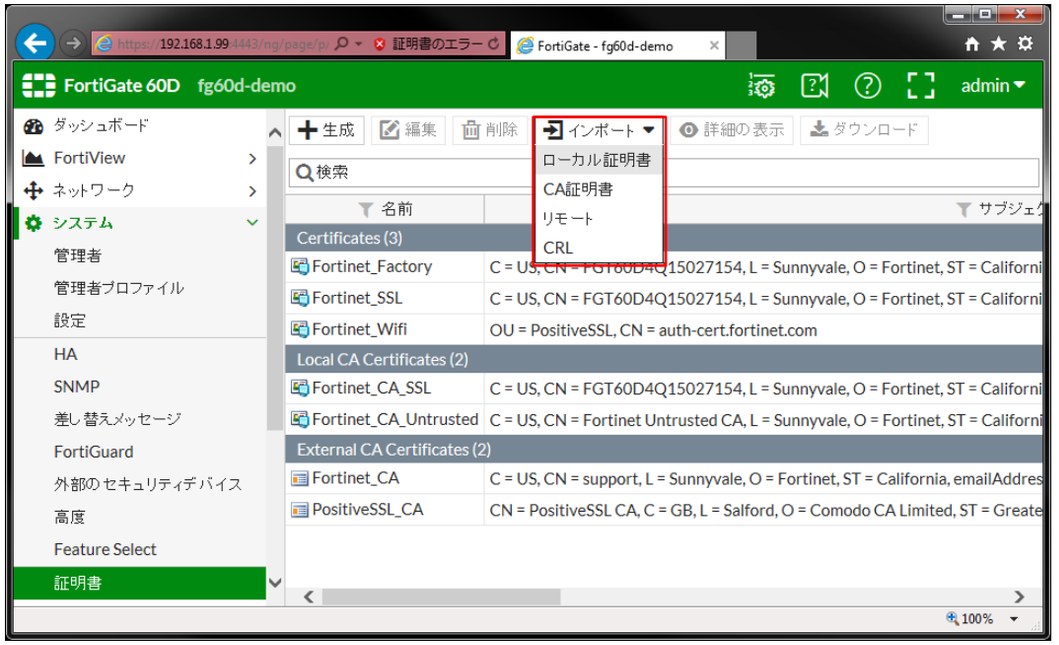
②証明書関連の設定

システム⇒証明書
上部の”インポート”メニューをクリック



インポート対象を選択

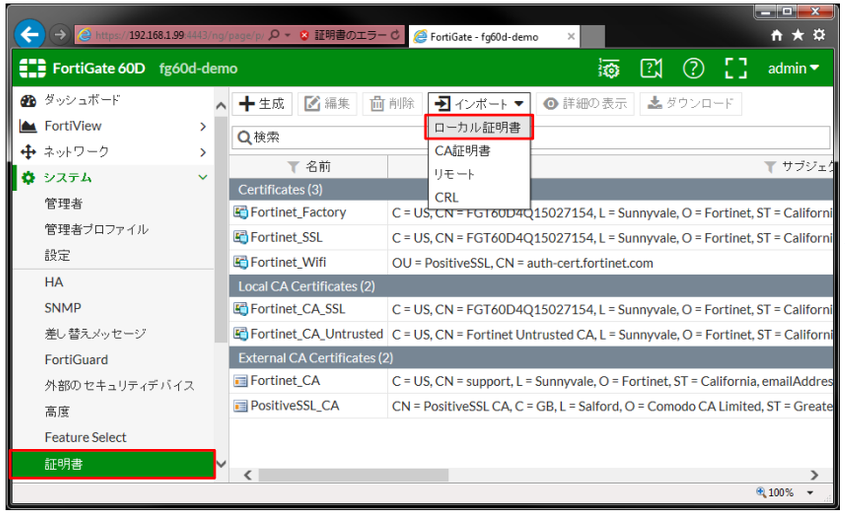
(A)ローカル証明書　：SSLサーバ証明書
(B)CA証明書　　：クライアント証明書発行局公開鍵
(C)CRL　　：クライアント証明書の失効リスト



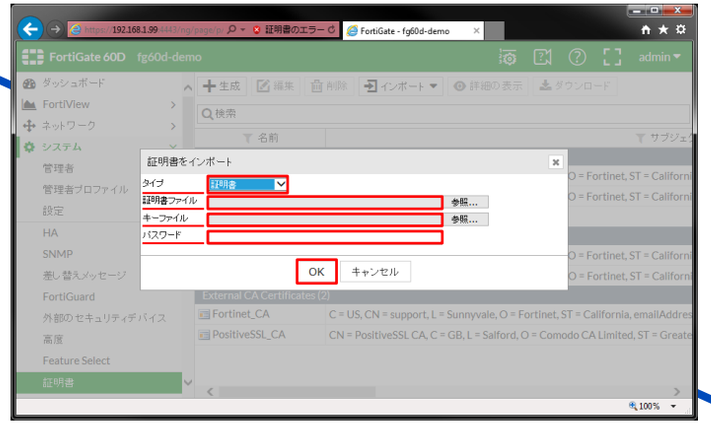
②－A）証明書関連の設定

SSLサーバ証明書のインポート

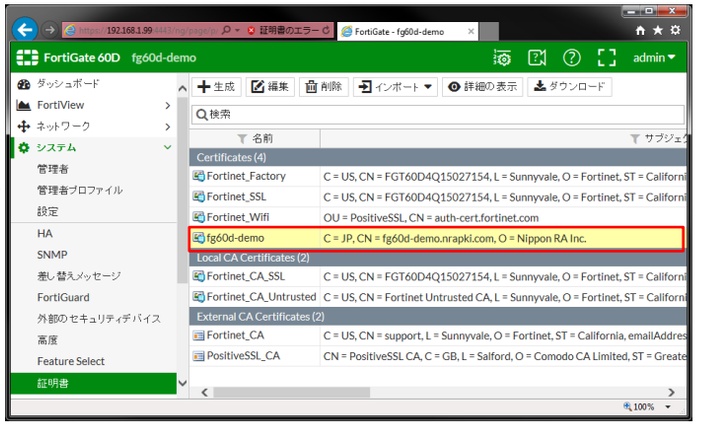
上部の”インポート”メニューから
”ローカル証明書”をクリック



“タイプ”のリストから”証明書”を選択し、証明書、キーファイル、パスワードを指定して”OK”をクリック



SSLサーバ証明書が、インポートされたことを確認

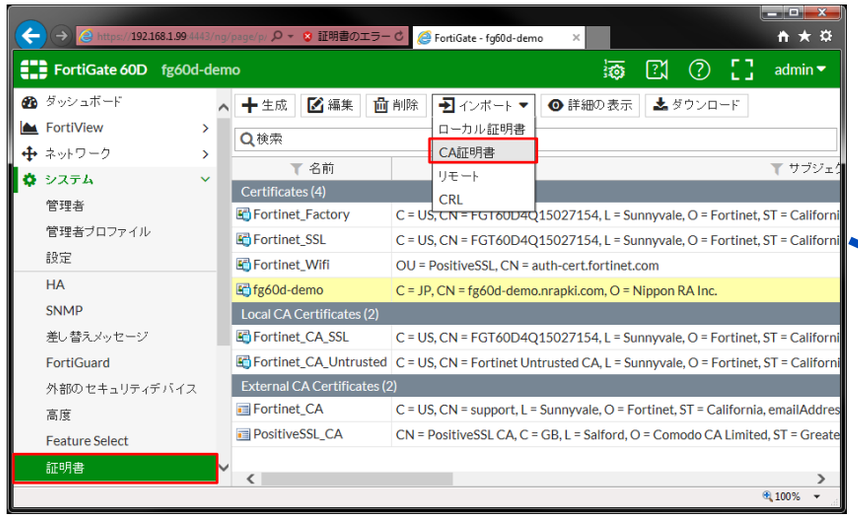


※初期状態は工場出荷の自己署名のサーバ証明書がセットされているが、信頼性の観点で証明書ベンダーからの調達促される

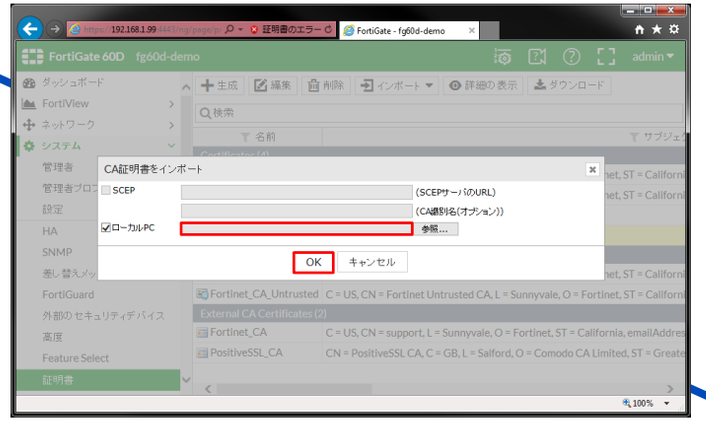
②－B）証明書関連の設定

<u>発行局（CA：中間のみ）の公開鍵インポート</u>

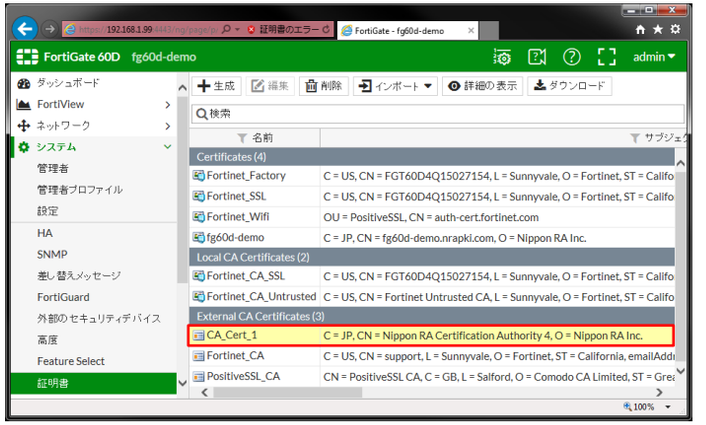
上部の”インポート”メニューから
”CA証明書”をクリック



”ローカルPC”を選択、予め取得した
発行局（CA）公開鍵ファイルを指定
し”OK”をクリック



発行局（CA）公開鍵がイ
ンポートされたことを確認

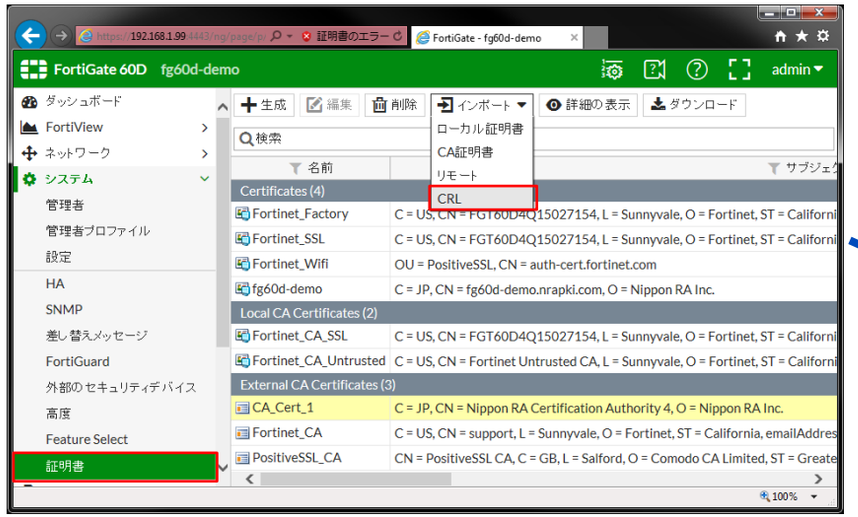


※<u>発行局（CA）の公開鍵とは、クライアント証明の発行機関を証明する証明書</u>

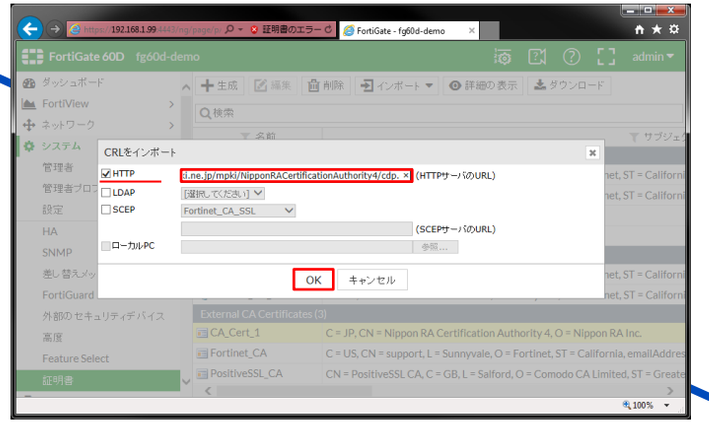
②－C）証明書関連の設定

CRL（失効リスト）インポート

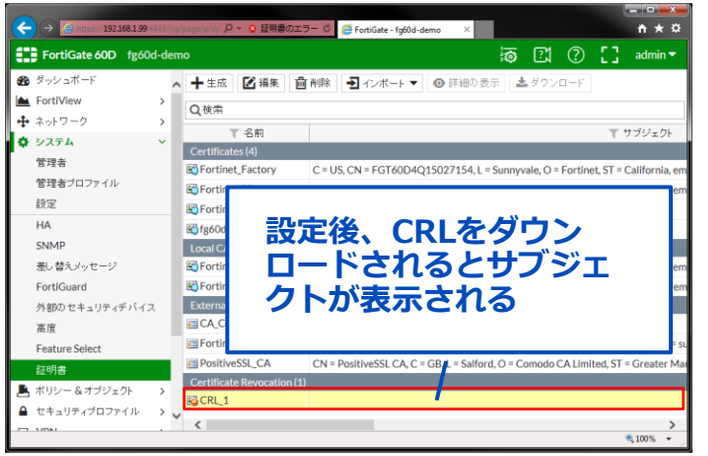
上部の”インポート”メニューから
”CRL”をクリック



“HTTP”を選択、失効リスト（CRL）
の配布URLを指定し”OK”をクリック



失効リスト（CRL）がイン
ポートされたことを確認

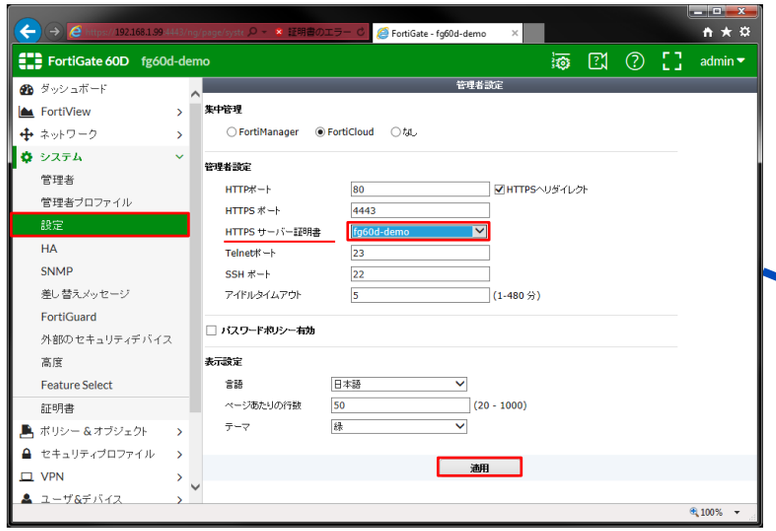


※CRL（失効リスト）とは、無効としたクライアント
証明書のシリアル値のブラックリスト

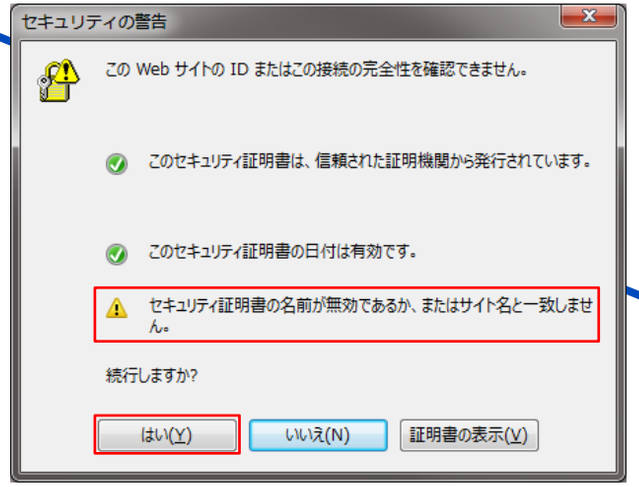
③インポートしたSSLサーバ証明書の指定

システム⇒設定

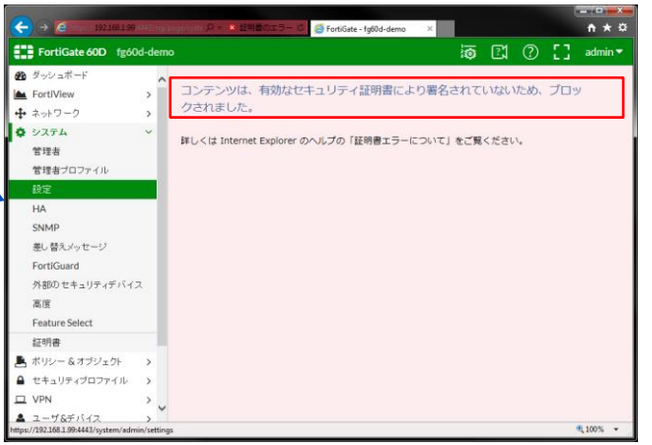
”HTTPSサーバー証明書”のリストボックスから
インポートしたSSLサーバ証明書のコモンネーム（ホスト名）を選択し、”適用”をクリック



本操作でアクセスしているURL（IPアドレス）
とインポートしたSSLサーバ証明書のコモンネーム（FQDN）が一致しないため警告が表示されるが、これは正常動作なので”はい”をクリック

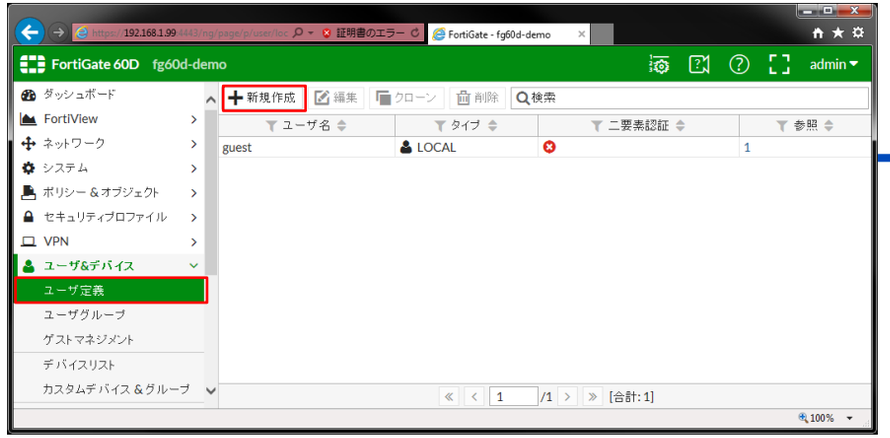


警告が表示されますが、設定は完了



④アクセスユーザ、グループの作成

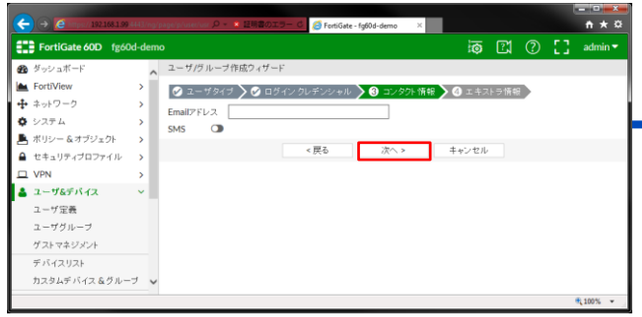
ユーザ＆デバイス⇒ユーザ定義
“新規作成”をクリック



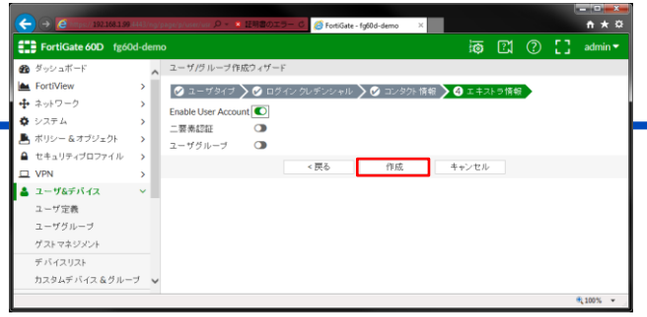
“ローカルユーザ”が選択された
状態で“次へ”をクリック

“ユーザ名”、”パスワード”を任
意で入力し“次へ”をクリック

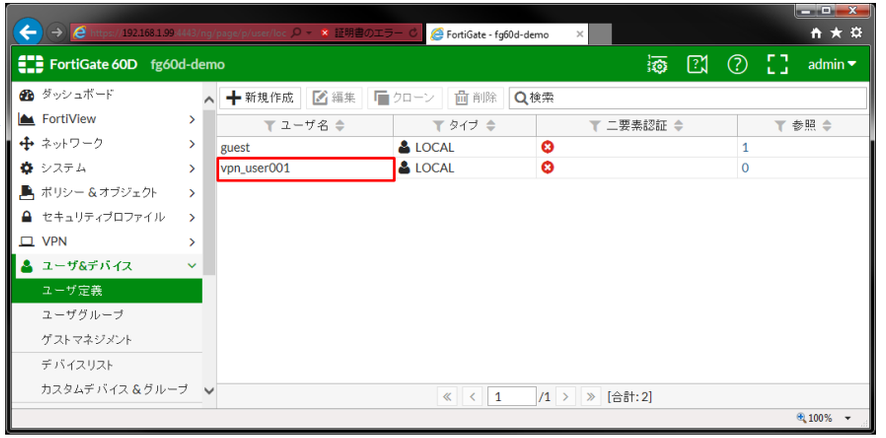
“次へ”をクリック



“作成”をクリック



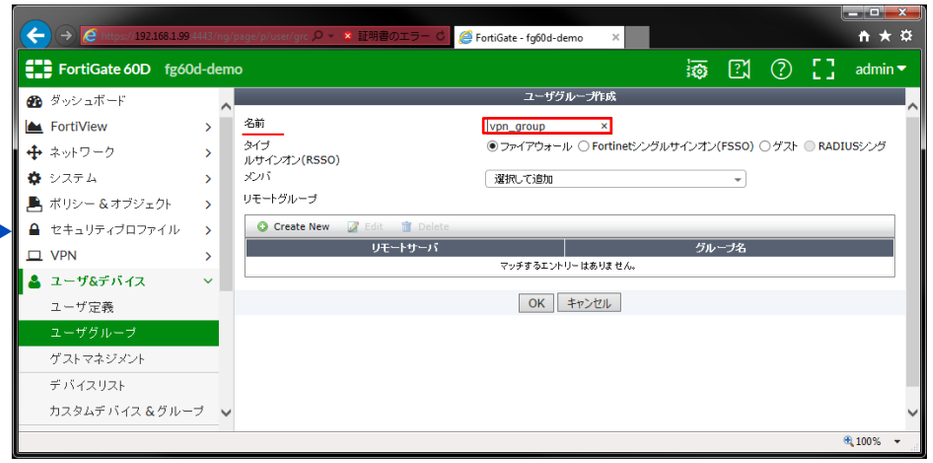
作成したユーザが表示されることを確認



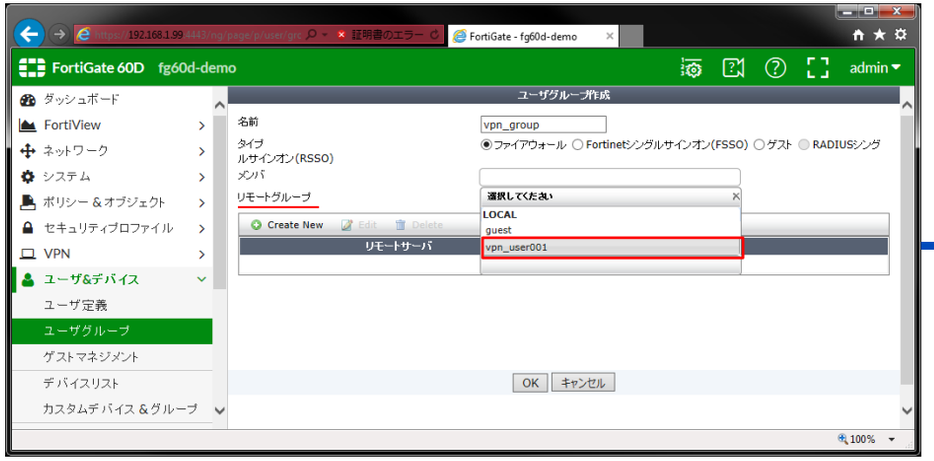
④アクセスユーザ、グループの作成

ユーザ＆デバイス⇒ユーザグループ
“新規作成”をクリック

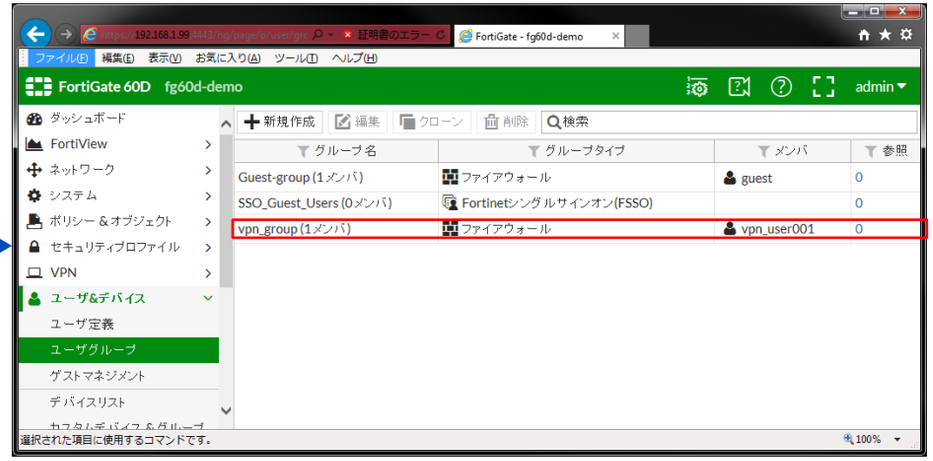
任意のグループ名を入力



グループに所属するユーザを指定し、”OK”をクリック

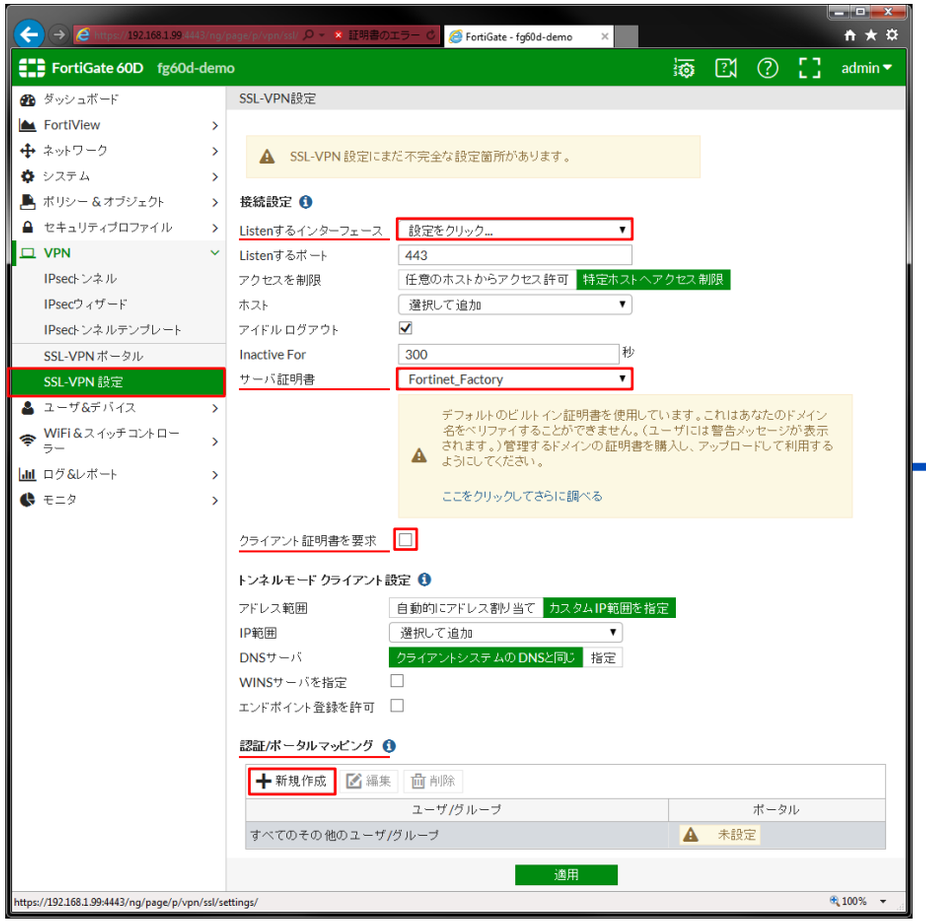


作成したグループを確認

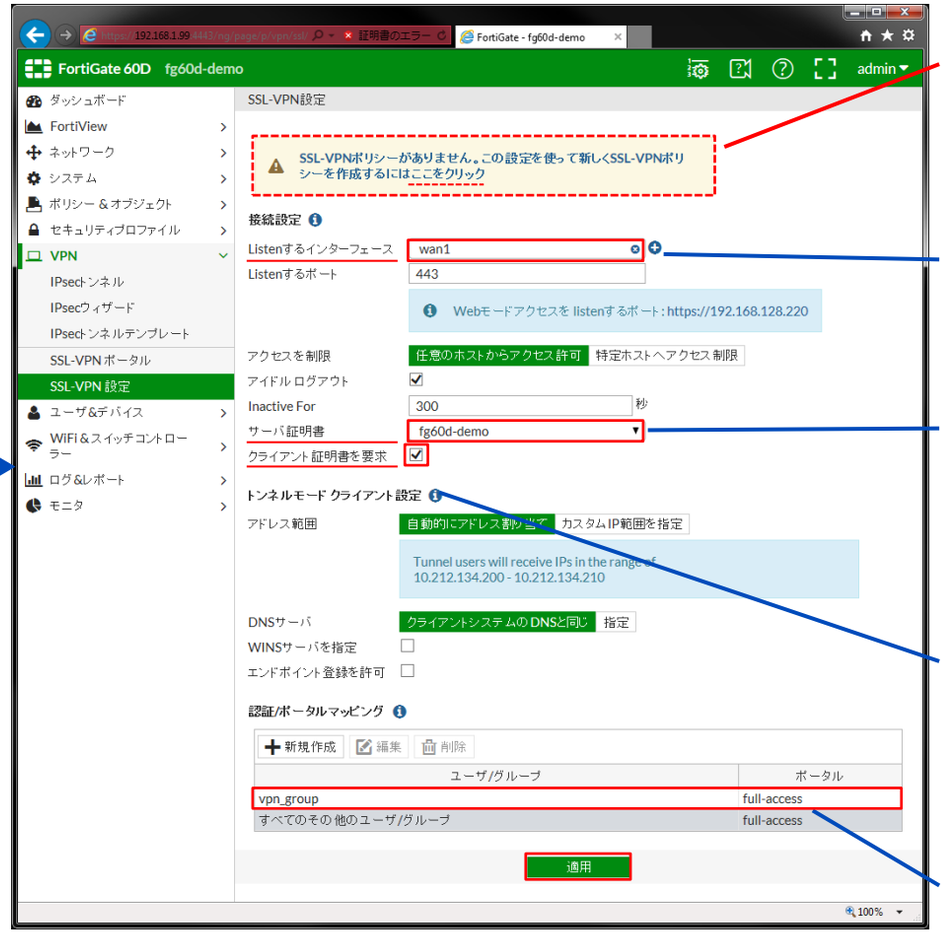


⑤VPN設定

VPN⇒SSL-VPN設定
設定する項目の例



各種設定し、上部インフォメーションから
リンクしてSSL-VPNポリシーを作成



各種SSL-VPN設定後に、”適用”をクリック
VPNポリシー作成に進む

本手順で使用したポート

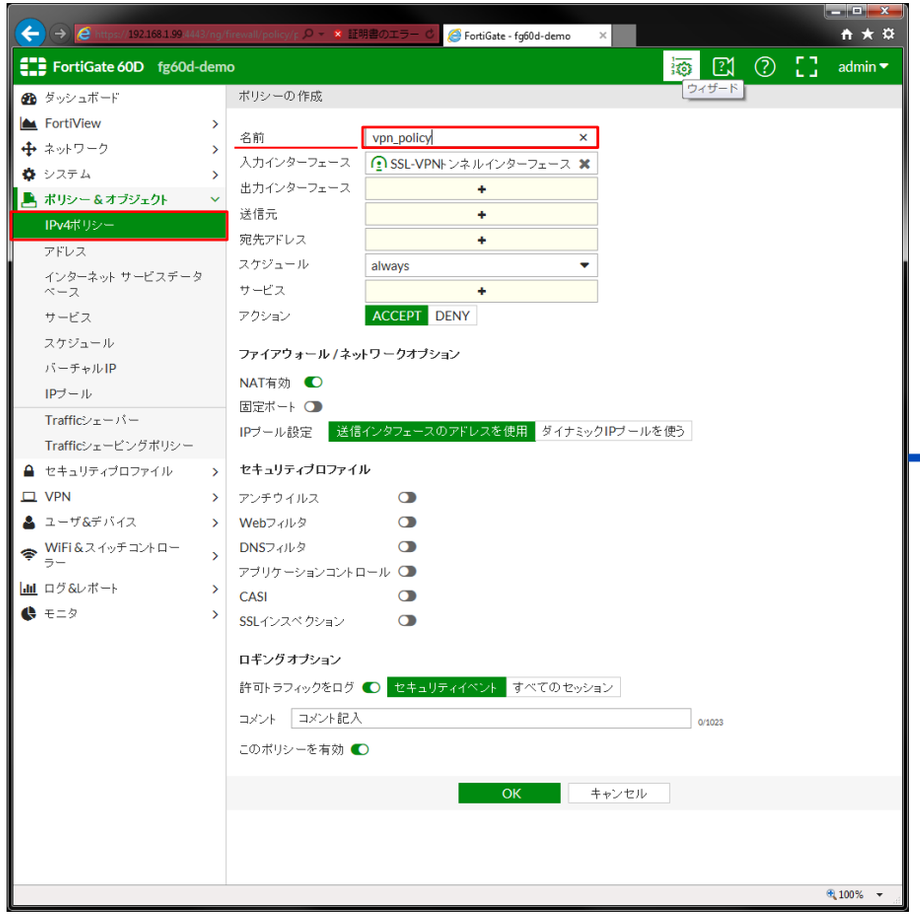
予めインポートしたサーバ証明書のコモンネーム（ホスト名）を指定

SSL-VPNアクセス時に、ID/パスワードとクライアント証明書の２要素認証するためにチェック

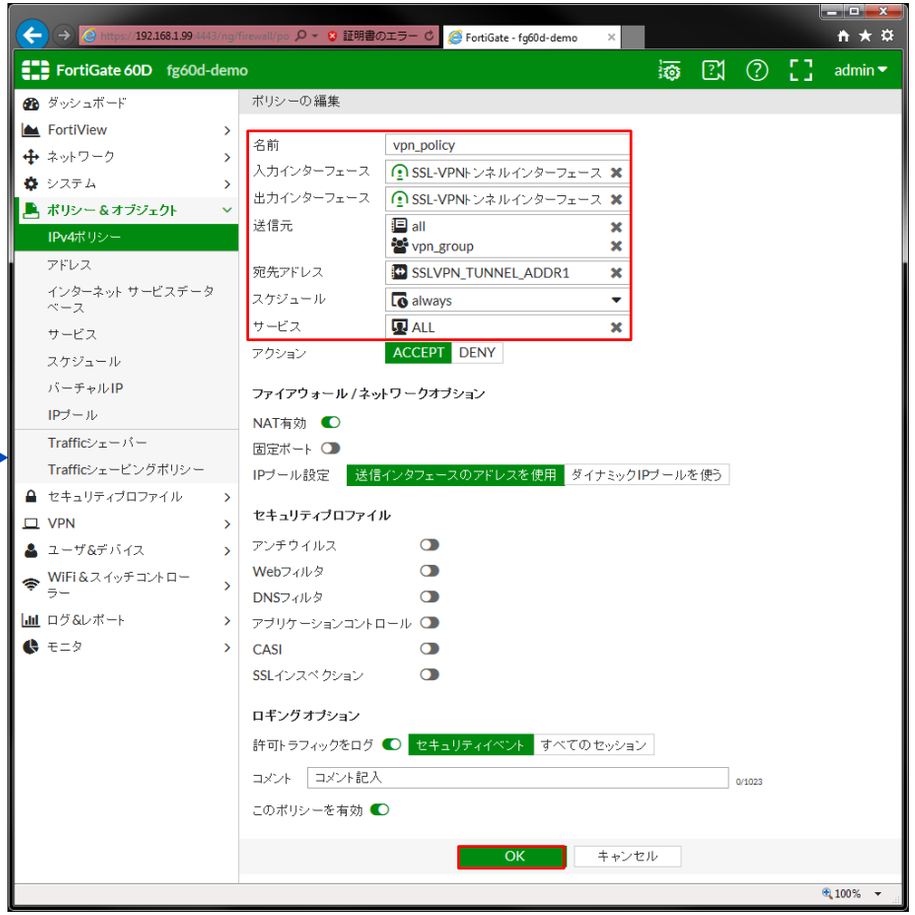
予め作成したSS-VPNアクセス用のグループを指定

⑥SSL-VPNポリシー作成

“ポリシー＆オブジェクト”⇒IPv4ポリシー
※“SSL-VPN設定”からリンクした設定画面
　任意のポリシー名を入力し、各項目を設定



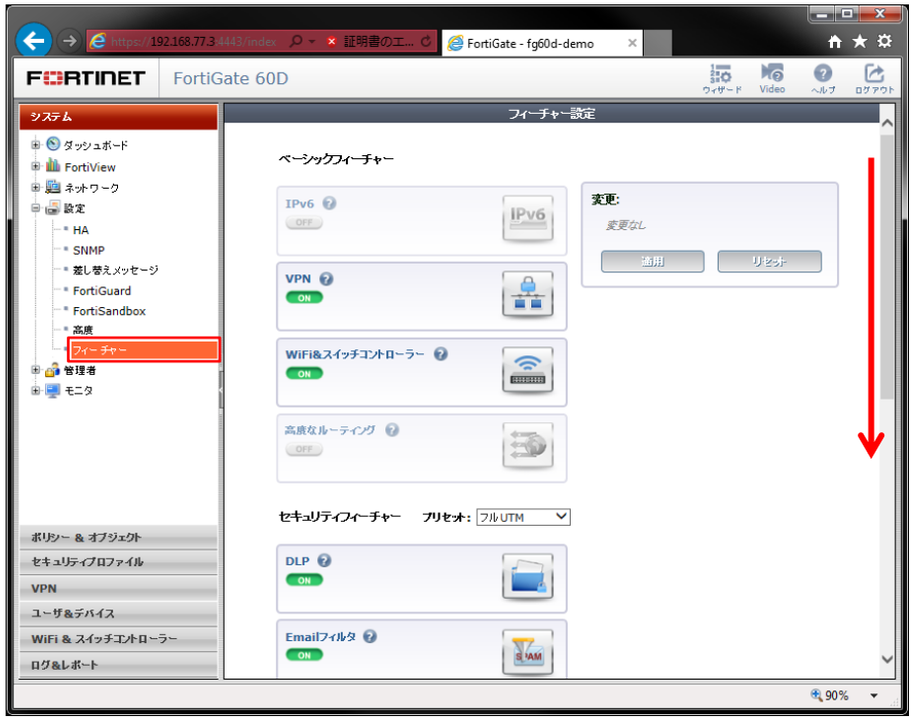
設定する箇所の例各種設定し、“OK”をクリック
SSL-VPNポリシーの作成が完了
※ネットワーク設定は、利用環境に依存します



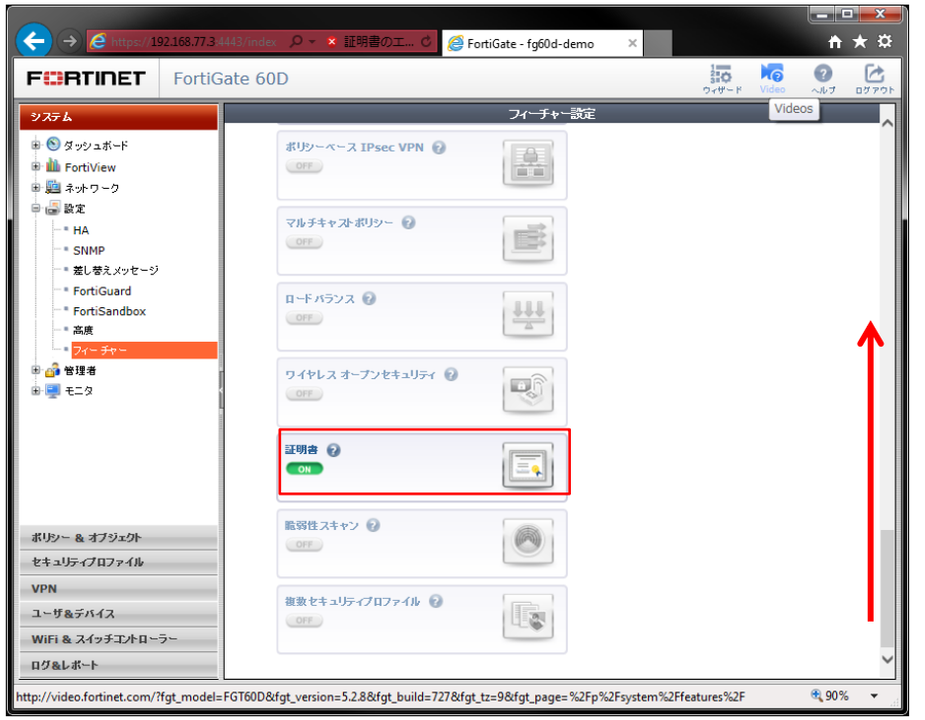
6．SSL-VPN設定（FortiOS 5.2）

①証明書メニューのアクティベーション

システム⇒設定⇒フィーチャー
下部にスクロール（さらに表示をクリック）

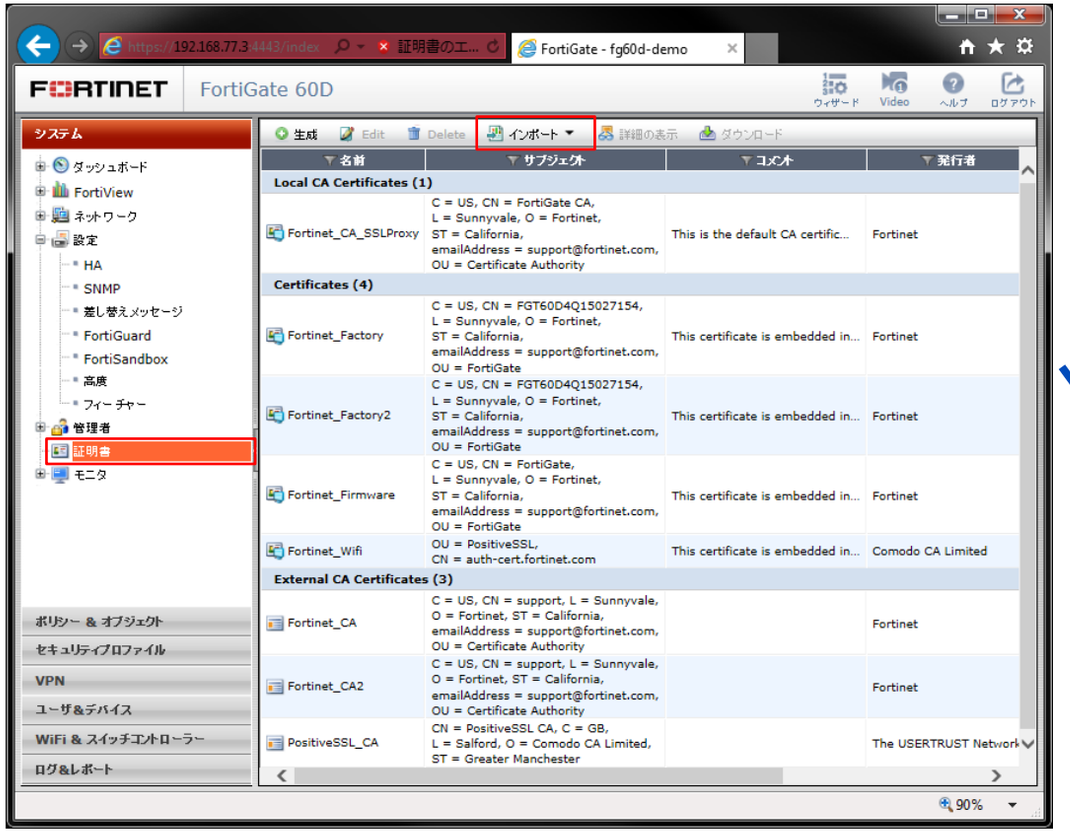


“証明書”をクリックしてON状態として、
上部にスクロールし“適用”をクリック



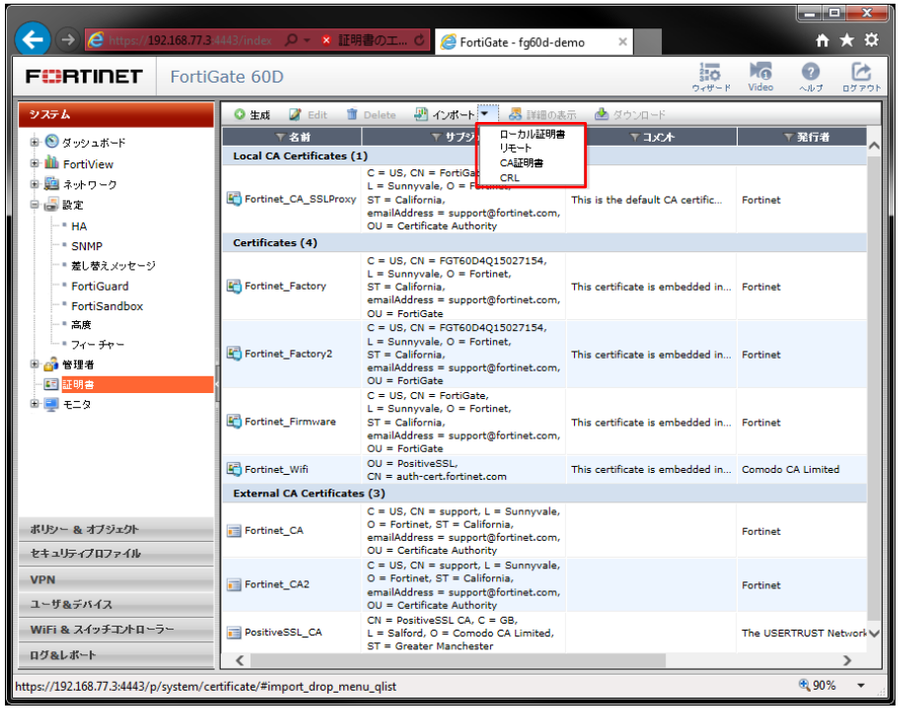
②証明書関連の設定

システム⇒証明書
上部の”インポート”メニューをクリック



インポート対象を選択

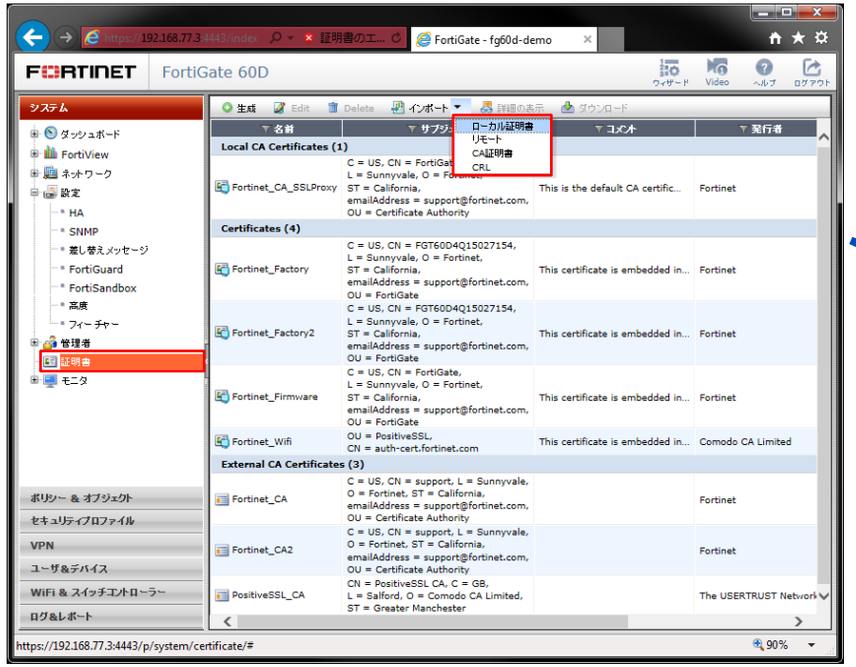
(A)ローカル証明書　：SSLサーバ証明書
(B)CA証明書　　：クライアント証明書発行局公開鍵
(C)CRL　　：クライアント証明書の失効リスト



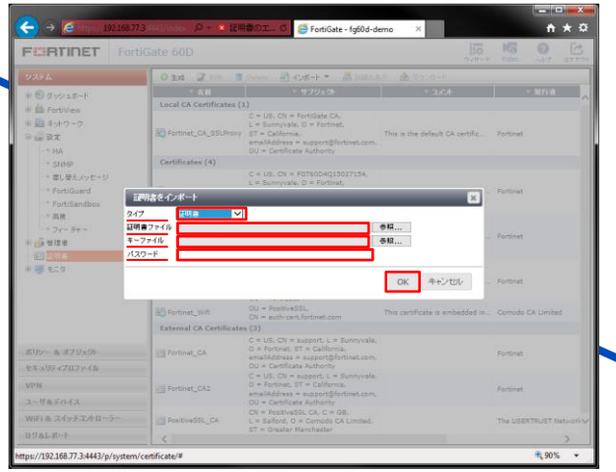
②－A）証明書関連の設定

SSLサーバ証明書のインポート

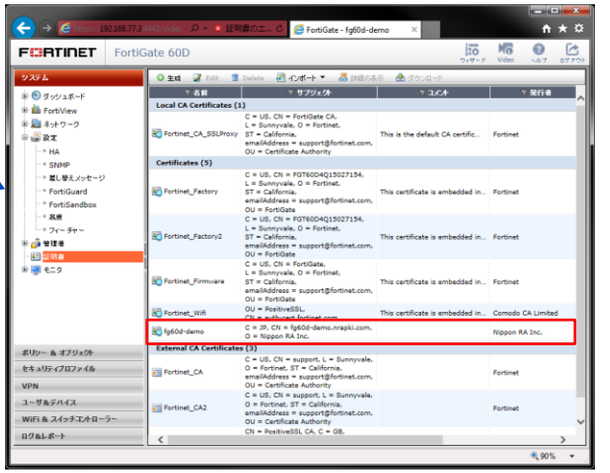
上部の”インポート”メニューから
”ローカル証明書”をクリック



“タイプ”のリストから”証明書”を選択し、証明書、キーファイル、パスワードを指定して”OK”をクリック



SSLサーバ証明書が、インポートされたことを確認

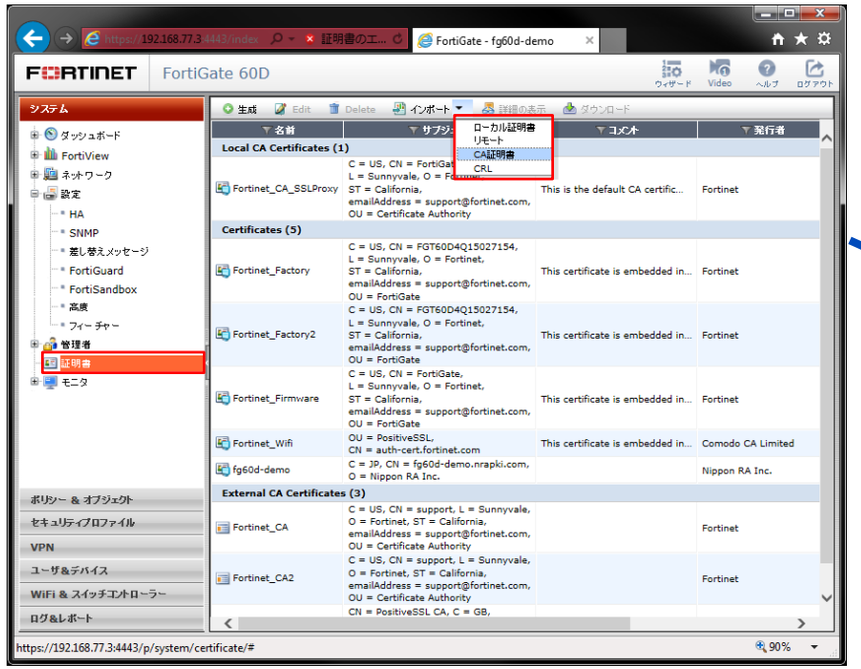


※初期状態は工場出荷の自己署名のサーバ証明書がセットされているが、信頼性の観点で証明書ベンダーからの調達促される

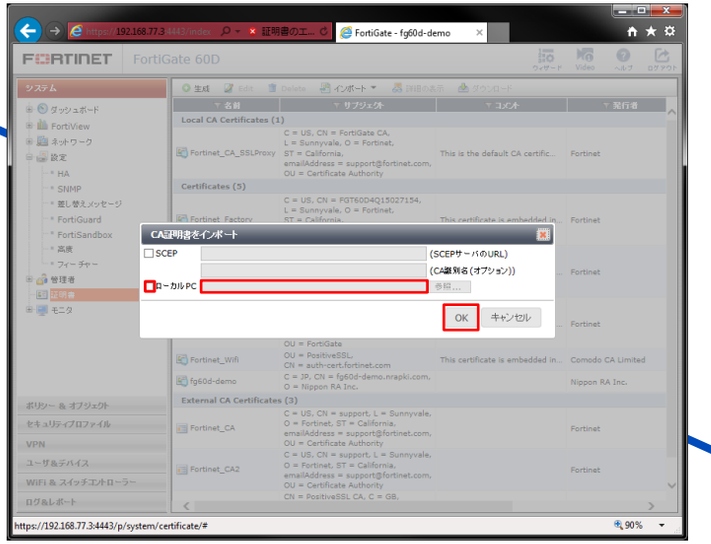
②－B）証明書関連の設定

<u>発行局（CA：中間のみ）の公開鍵インポート</u>

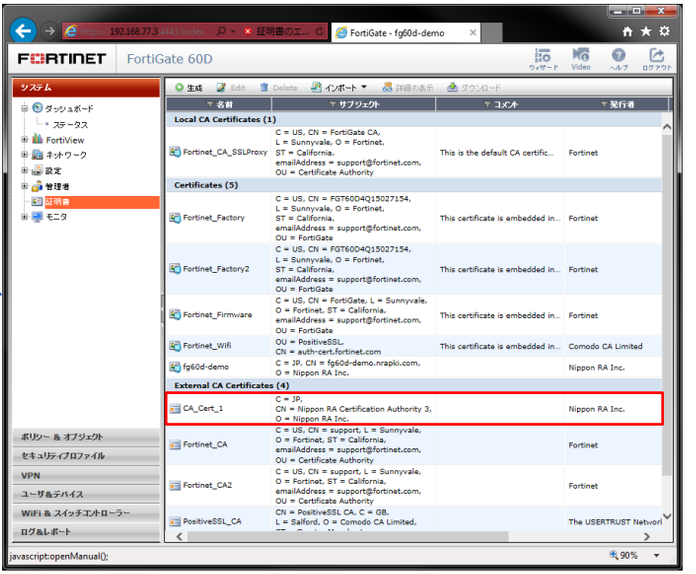
上部の”インポート”メニューから
”CA証明書”をクリック



“ローカルPC”を選択、予め取得した
発行局（CA）公開鍵ファイルを指定
し”OK”をクリック



発行局（CA）公開鍵がイ
ンポートされたことを確認

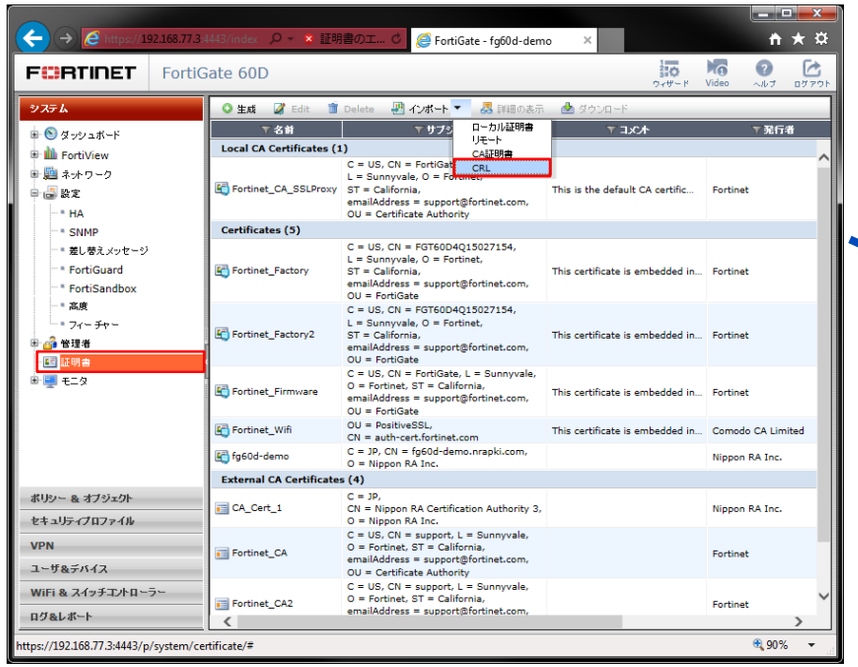


※<u>発行局（CA）の公開鍵とは、クライアント証明の発行機関を証明する証明書</u>

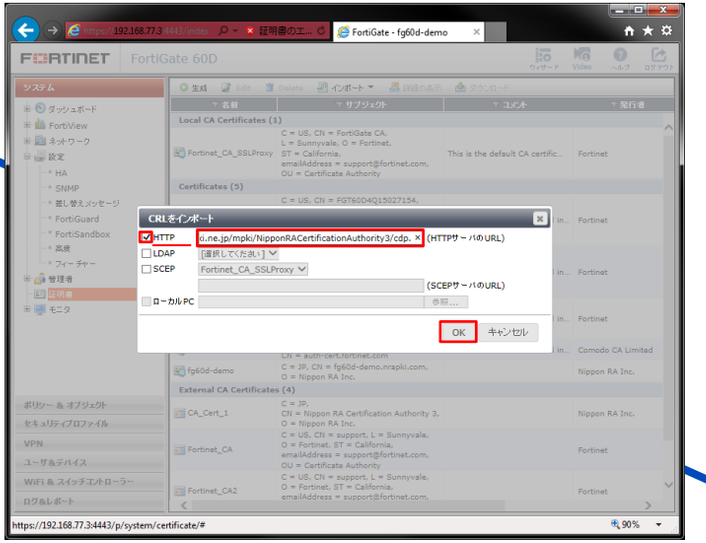
②－C）証明書関連の設定

CRL（失効リスト）インポート

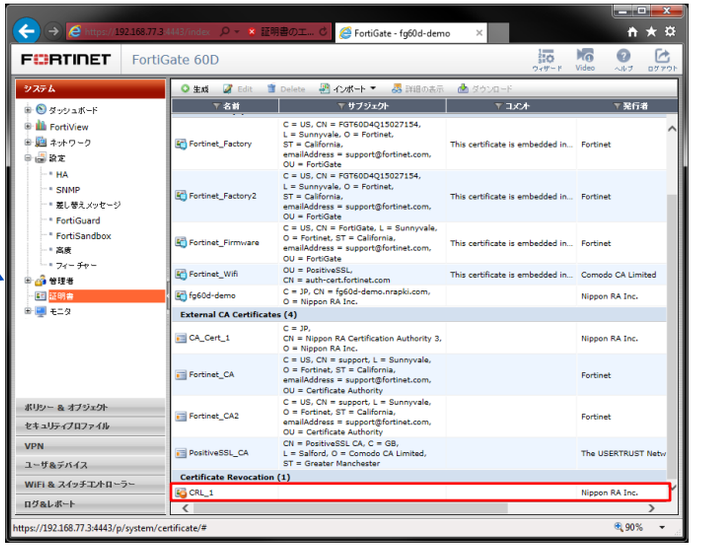
上部の”インポート”メニューから
”CRL”をクリック



“HTTP”を選択、失効リスト（CRL）
の配布URLを指定し”OK”をクリック



失効リスト（CRL）がイン
ポートされたことを確認

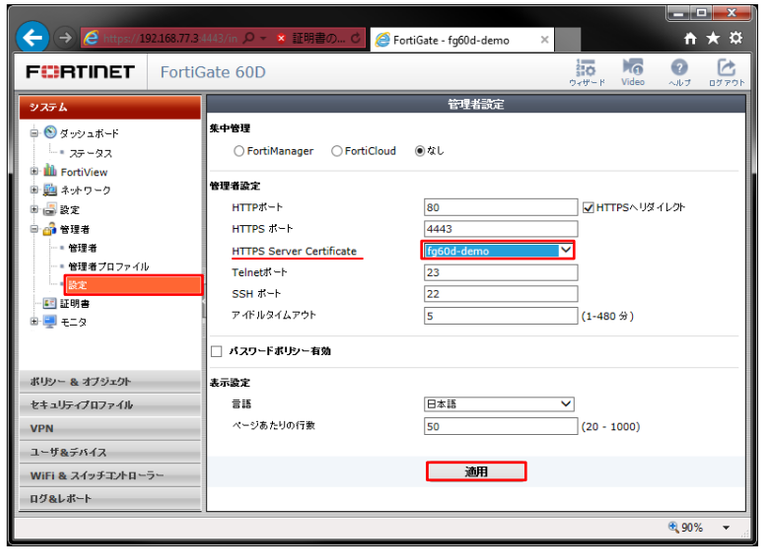


※CRL（失効リスト）とは、無効としたクライアント
証明書のシリアル値のブラックリスト

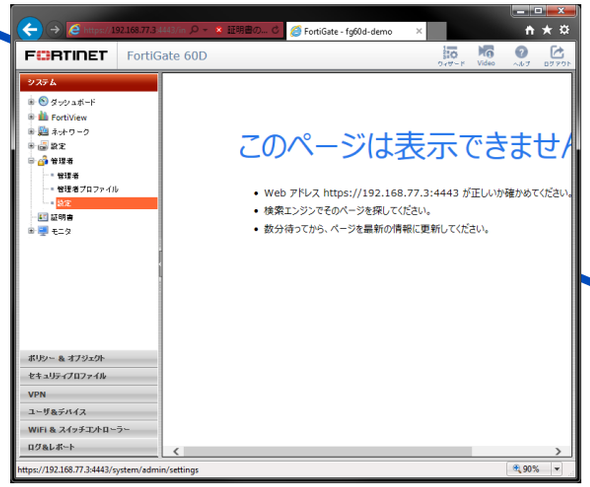
③インポートしたSSLサーバ証明書の指定

システム⇒管理者⇒設定

”HTTPSサーバー証明書”のリストボックスから
インポートしたSSLサーバ証明書のコモンネーム（ホスト名）を選択し、”適用”をクリック



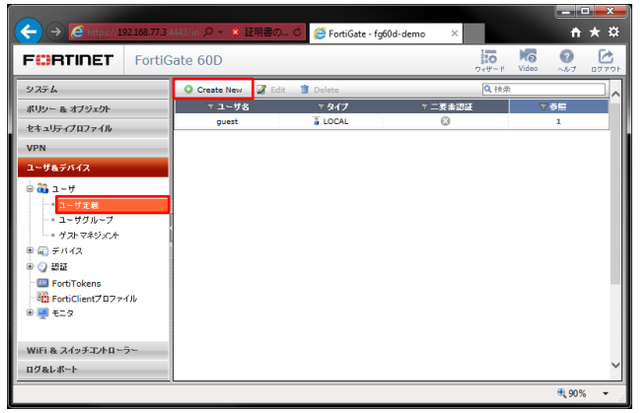
本操作でアクセスしているURL（IPアドレス）
とインポートしたSSLサーバ証明書のコモンネーム（FQDN）が一致しないためページエラーがでるが、これは正常動作なので”はい”をクリック



メニューの遷移で警告が表示される場合は、ブラウザを閉じてログインし直す

④アクセスユーザ、グループの作成

ユーザ＆デバイス⇒ユーザ定義
“新規作成”をクリック



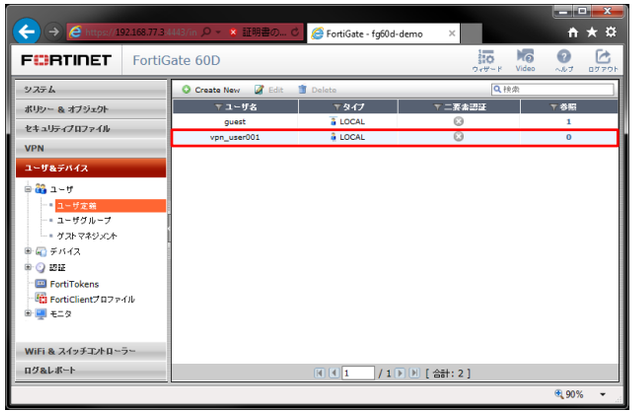
“ローカルユーザ”が選択された
状態で“NEXT”をクリック

“ユーザ名”、”パスワード”を任
意で入力し“NEXT”をクリック

“NEXT”をクリック

“Done”をクリック

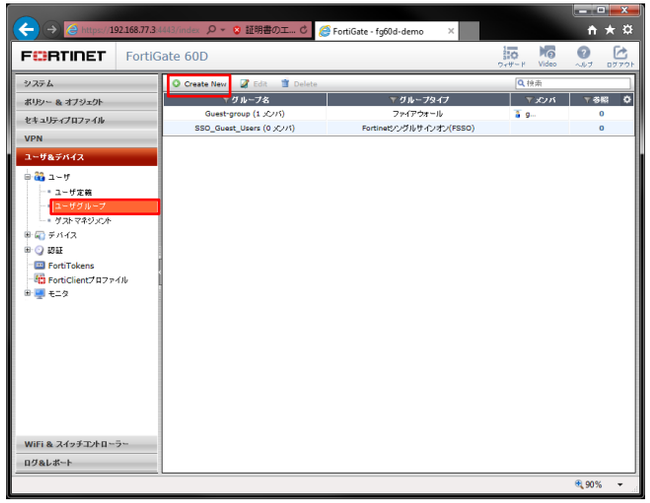
作成したユーザが表示されることを確認



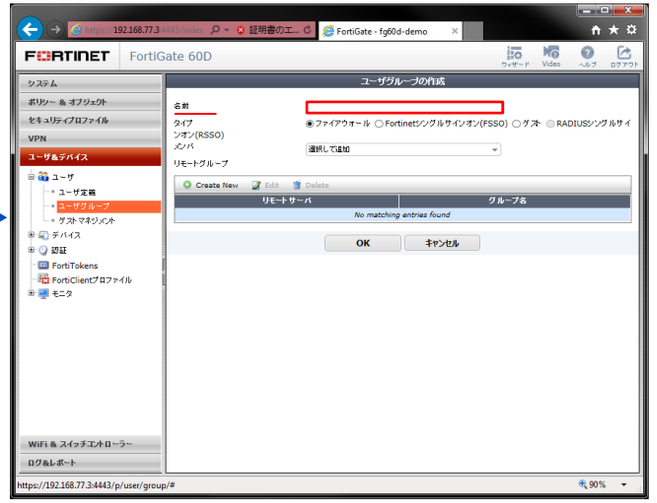
④アクセスユーザ、グループの作成

ユーザ＆デバイス⇒ユーザグループ

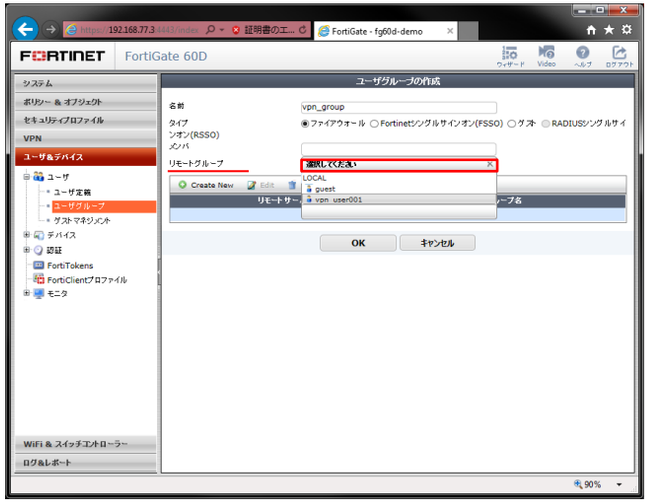
“新規作成”をクリック



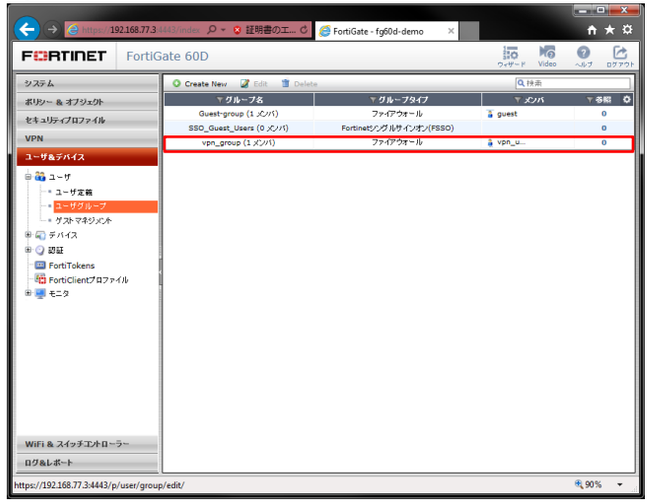
任意のグループ名を入力



グループに所属するユーザを指定し、”OK”をクリック

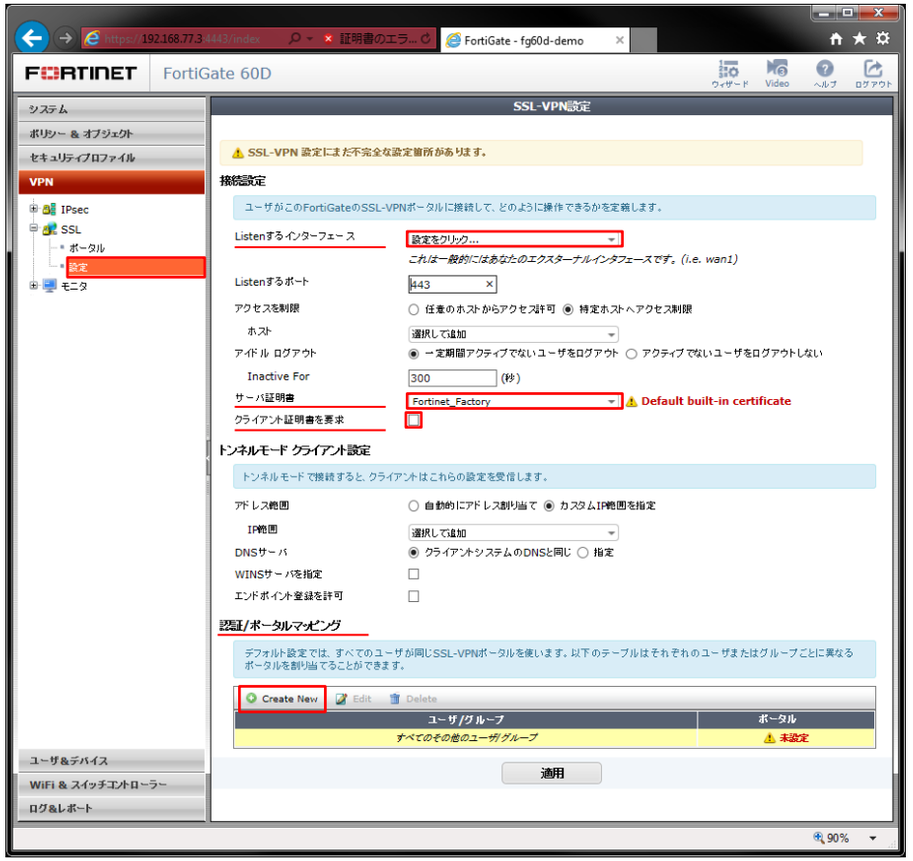


作成したグループを確認

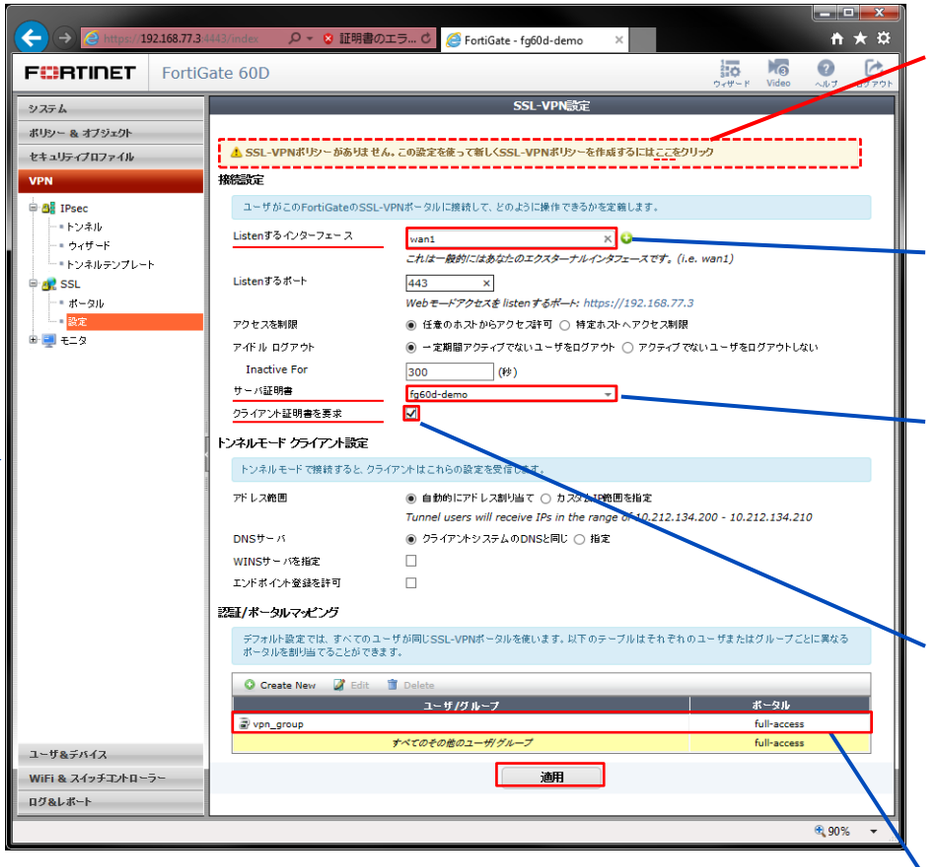


⑤VPN設定

VPN⇒SSL-VPN設定
設定する項目の例



各種設定し、上部インフォメーションから
リンクしてSSL-VPNポリシーを作成



各種SSL-VPN設定後に、”ここ”をクリック
VPNポリシー作成に進む

本手順で使用したポート

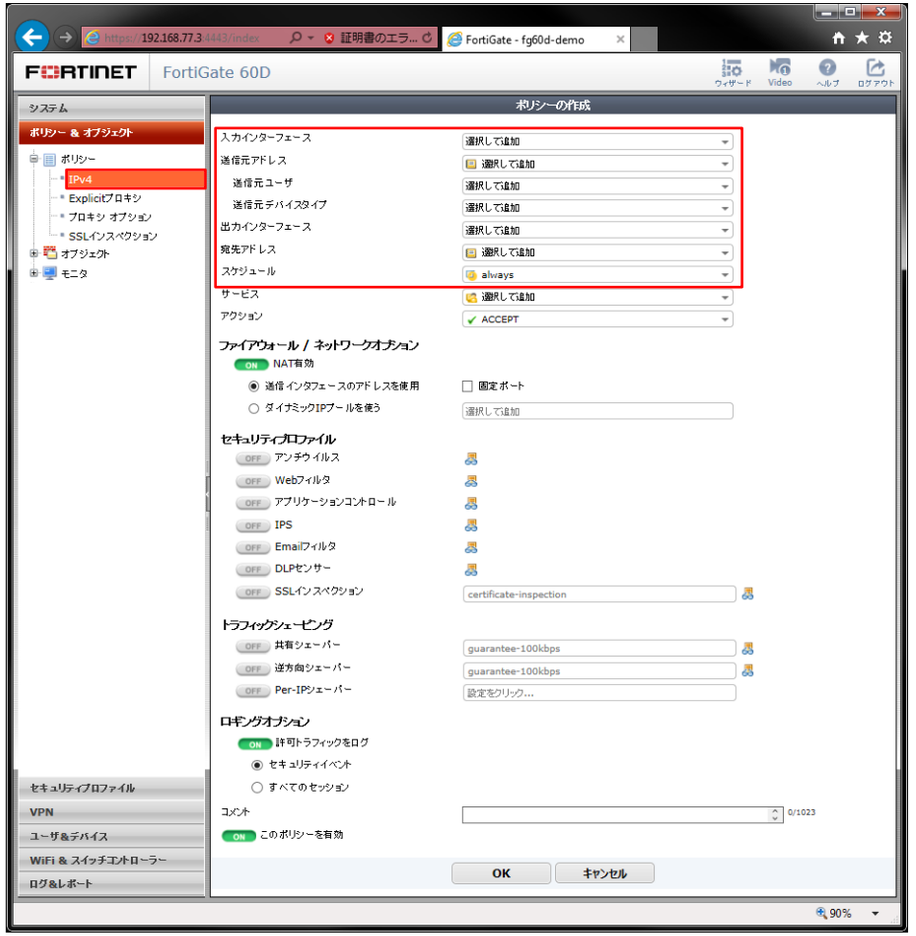
予めインポートしたサーバ証明書のコモンネーム（ホスト名）を指定

SSL-VPNアクセス時に、ID/パスワードとクライアント証明書の２要素認証するためにチェック

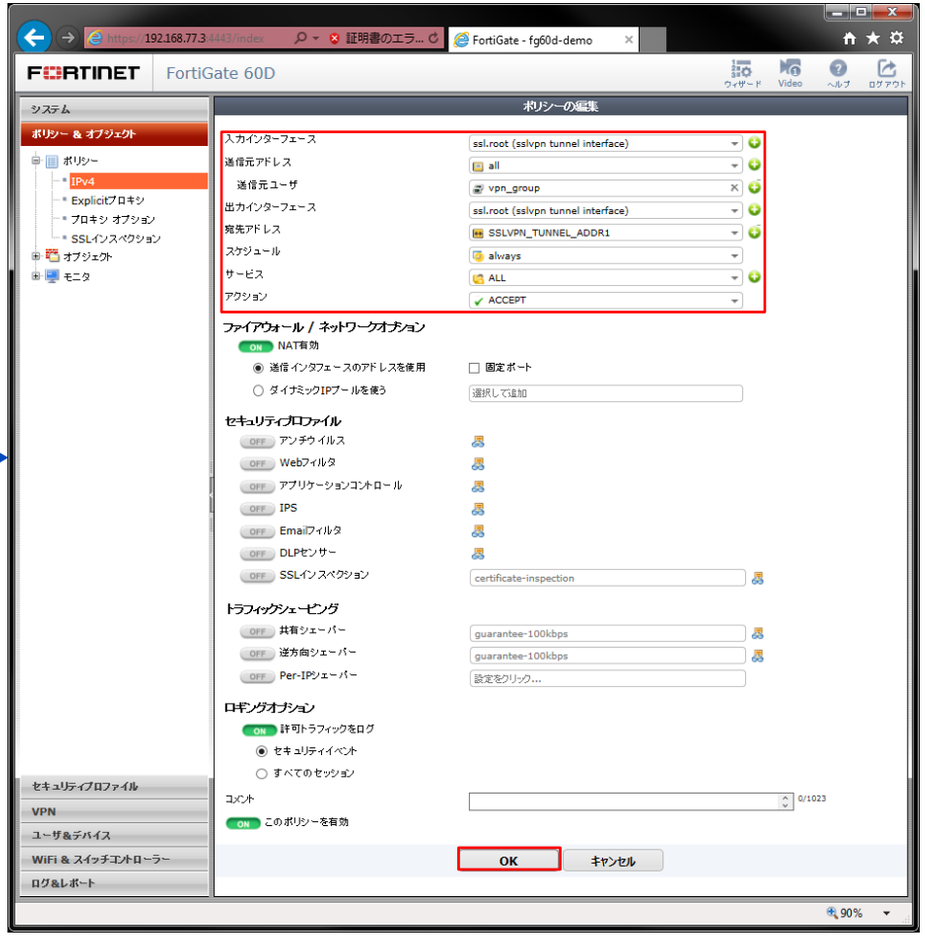
予め作成したSS-VPNアクセス用のグループを指定

⑥SSL-VPNポリシー作成

“ポリシー＆オブジェクト”⇒IPv4
※“SSL-VPN設定”からリンクした設定画面
　任意のポリシー名を入力し、各項目を設定



設定する箇所の各種設定し、“OK”をクリック
SSL-VPNポリシーの作成が完了
※ネットワーク設定は、利用環境に依存します



6．SSL-VPN設定（FortiOS 5.0）

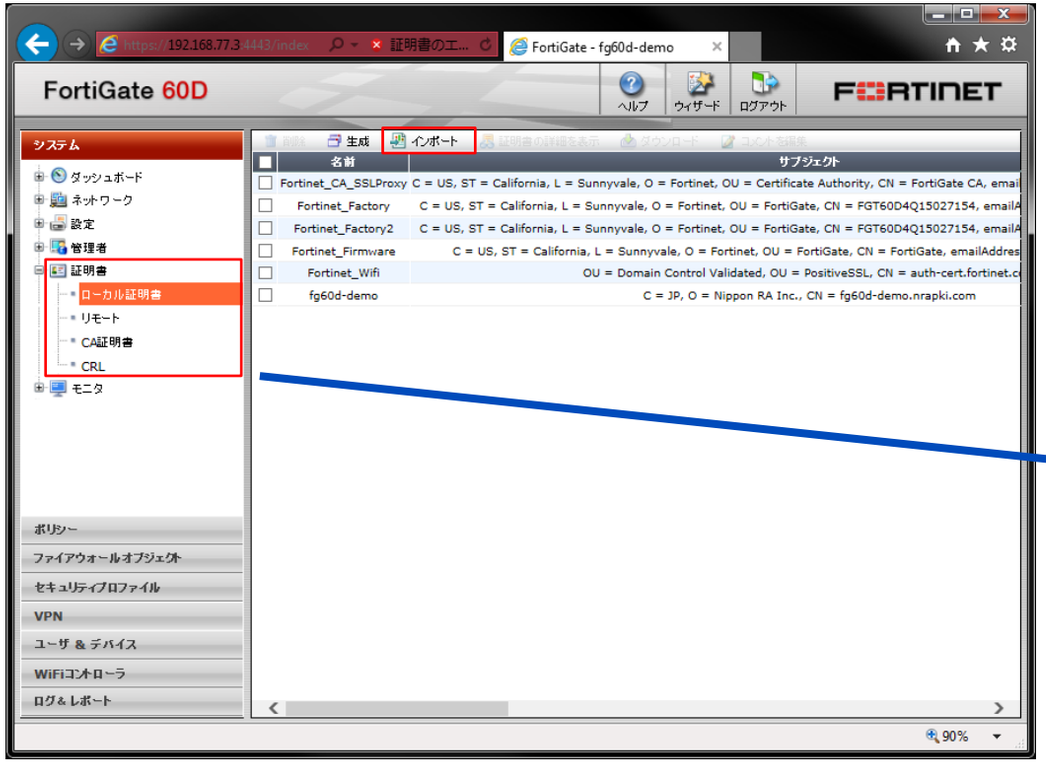
①証明書メニューのアクティベーション

システム⇒設定⇒フィーチャー
下部にスクロール（さらに表示をクリック）

“証明書”をクリックしてON状態として、
上部にスクロールし“適用”をクリック

②証明書関連の設定

システム⇒証明書⇒各証明書
上部の”インポート”メニューをクリック



インポート対象をメニューで選択

ローカル証明書	：SSLサーバ証明書
CA証明書	：クライアント証明書発行局公開鍵（ルート）
CA証明書	：クライアント証明書発行局公開鍵（中間）
CRL	：クライアント証明書の失効リスト

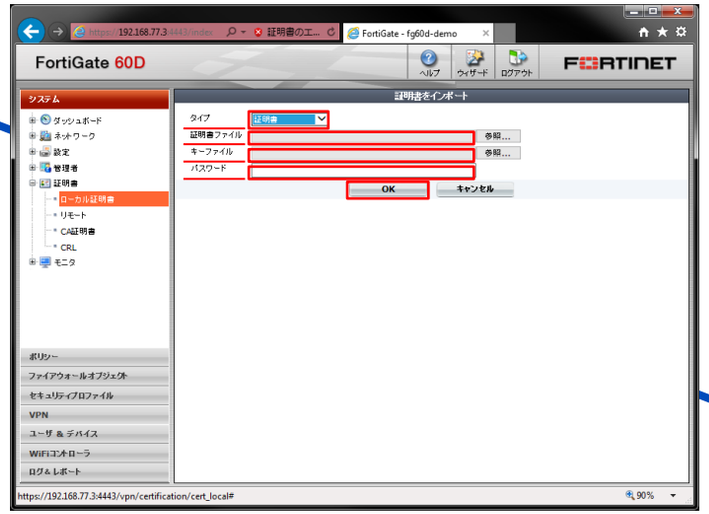
②－A）証明書関連の設定

SSLサーバ証明書のインポート

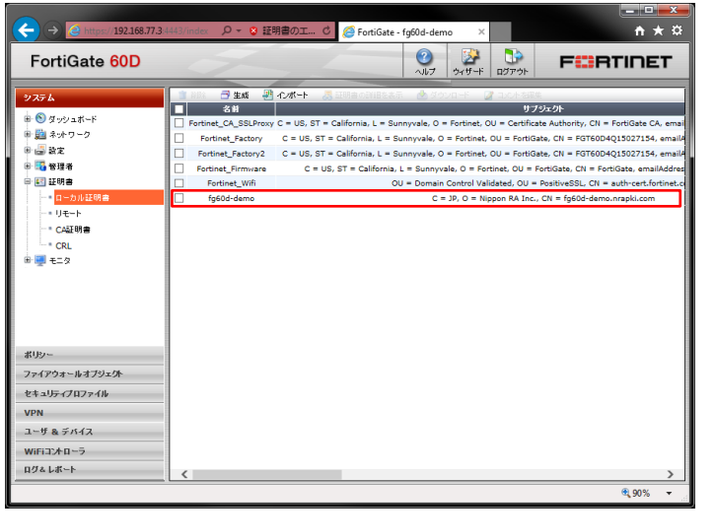
証明書⇒ローカル証明書

タイプのリストから”証明書”を選択

証明書ファイル、キーファイル、パスワードを指定して”OK”をクリック



SSLサーバ証明書が、インポートされたことを確認



※初期状態は工場出荷の自己署名のサーバ証明書がセットされているが、信頼性の観点で証明書ベンダーからの調達促される

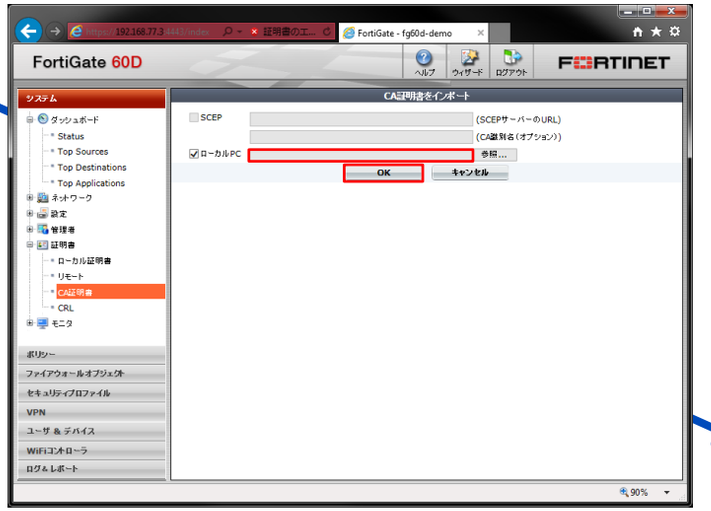
②－B）証明書関連の設定

<u>発行局（CA：ルート、中間の両方）の公開鍵インポート</u>

証明書⇒CA証明書

”ローカルPC”にチェック

予め取得した発行局（CA）公開鍵ファイル（ルート、中間）を指定し”OK”をクリック



発行局（CA）公開鍵がインポートされたことを確認

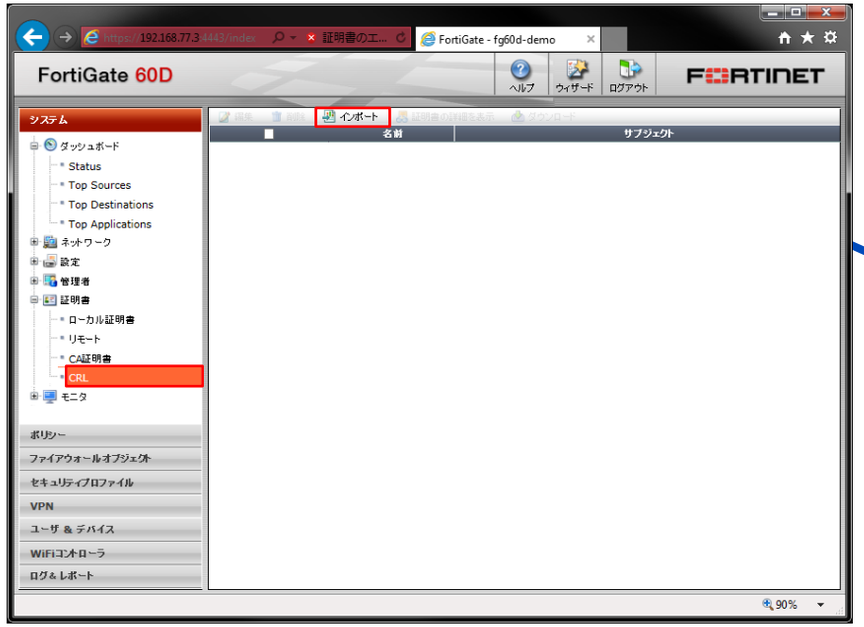
※<u>発行局（CA）の公開鍵とは、クライアント証明の発行機関を証明する証明書</u>

②－C）証明書関連の設定

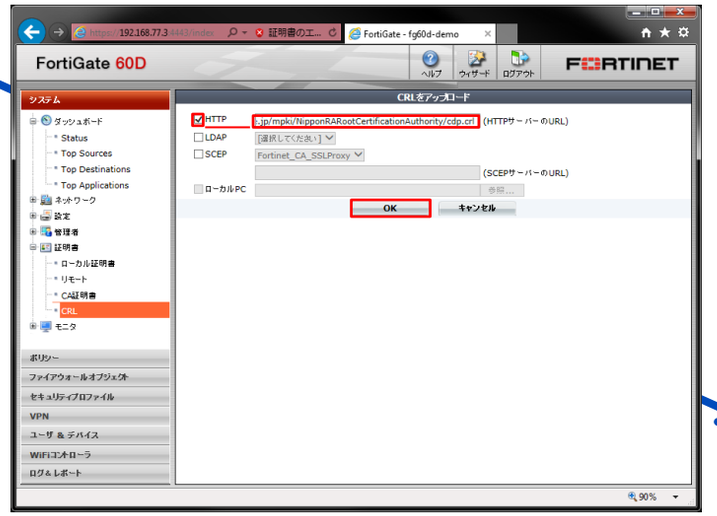
CRL（失効リスト）インポート

証明書⇒CRL

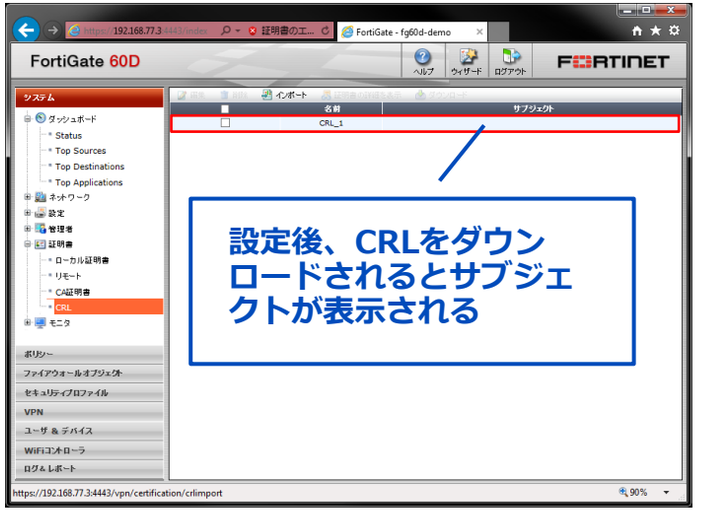
”インポート”をクリック



“HTTP”にチェックを入れ、失効リスト（CRL）の配布URLを指定し”OK”をクリック



失効リスト（CRL）がインポートされたことを確認



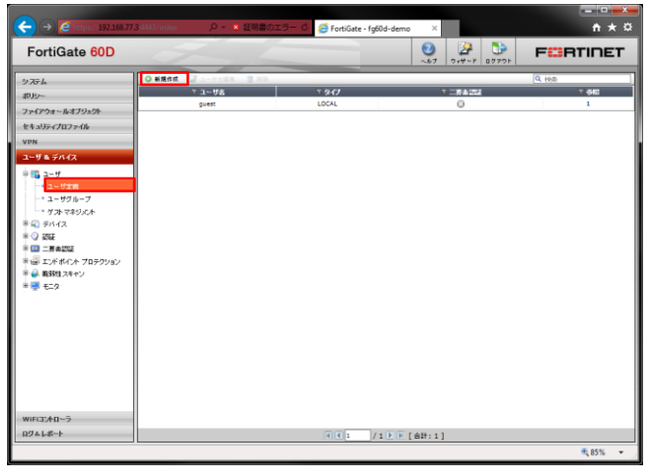
※CRL（失効リスト）とは、無効としたクライアント証明書のシリアル値のブラックリスト

③インポートしたSSLサーバ証明書の指定

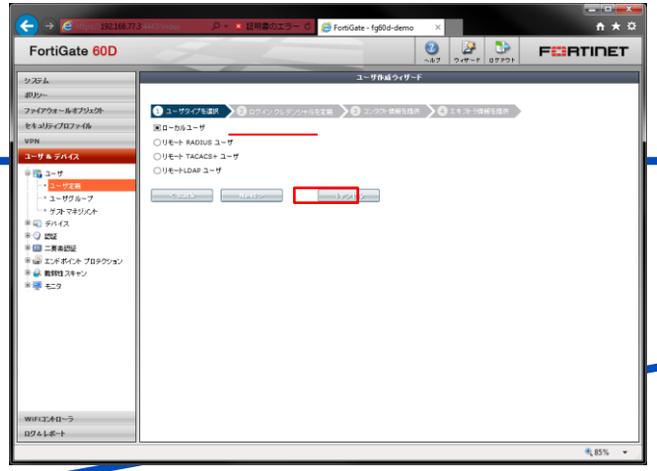
FortiOS 5.0では、本手順不要

④アクセスユーザ、グループの作成

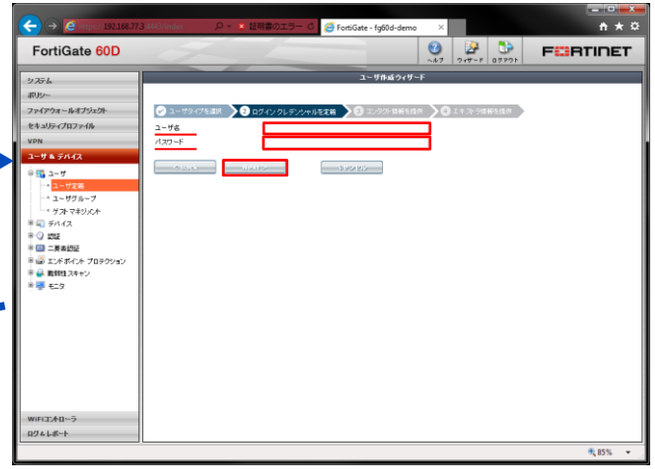
ユーザ＆デバイス⇒ユーザ定義
“新規作成”をクリック



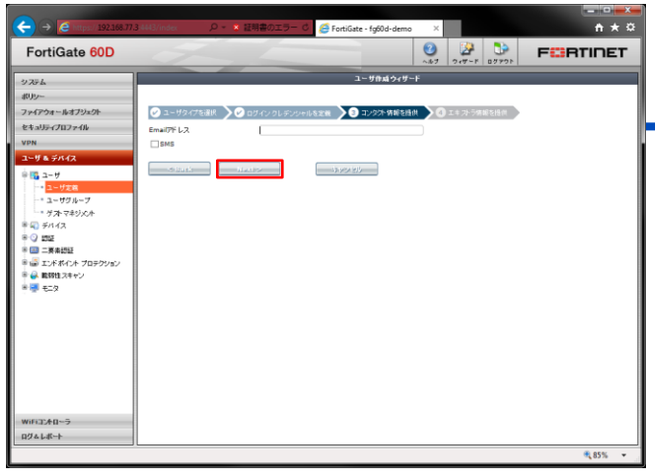
“ローカルユーザ”が選択された
状態で“NEXT”をクリック



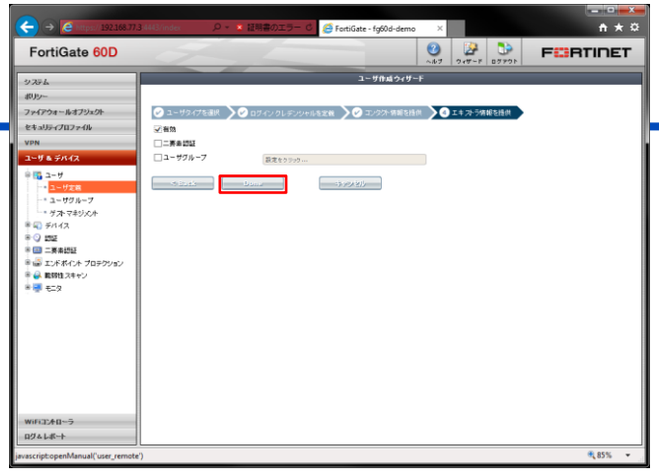
“ユーザ名”、”パスワード”を任
意で入力し“NEXT”をクリック



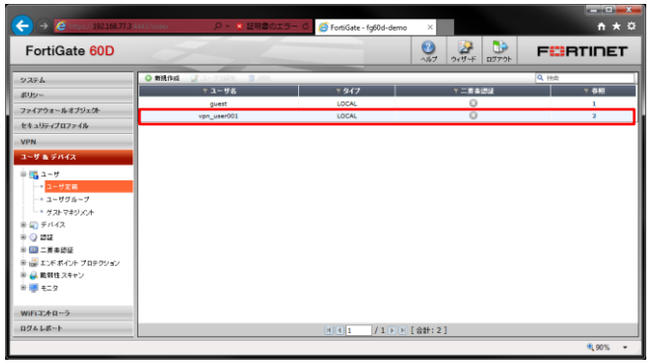
“NEXT”をクリック



“Done”をクリック

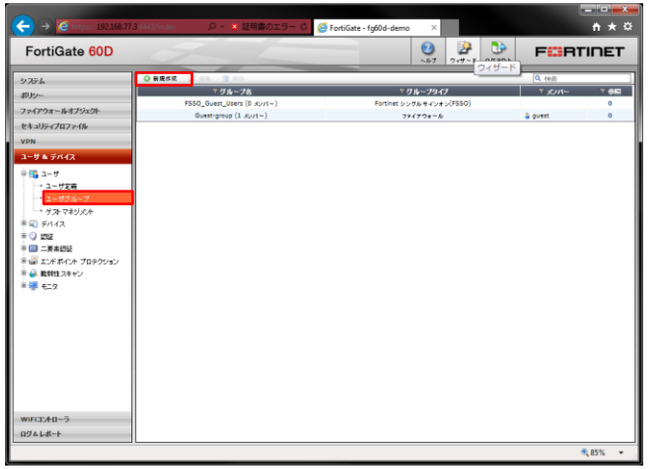


作成したユーザが表示されることを確認

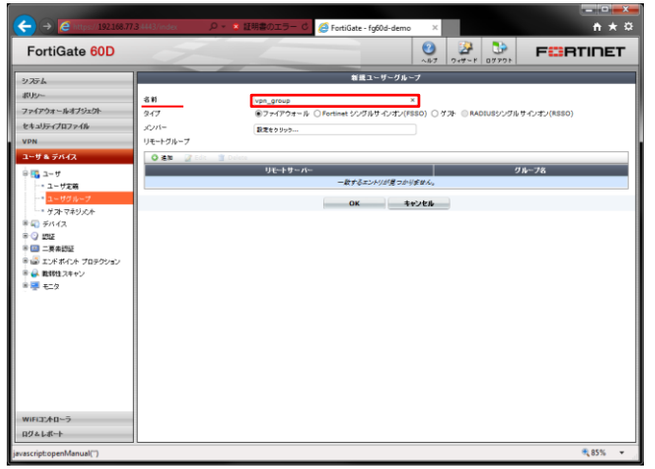


④アクセスユーザ、グループの作成

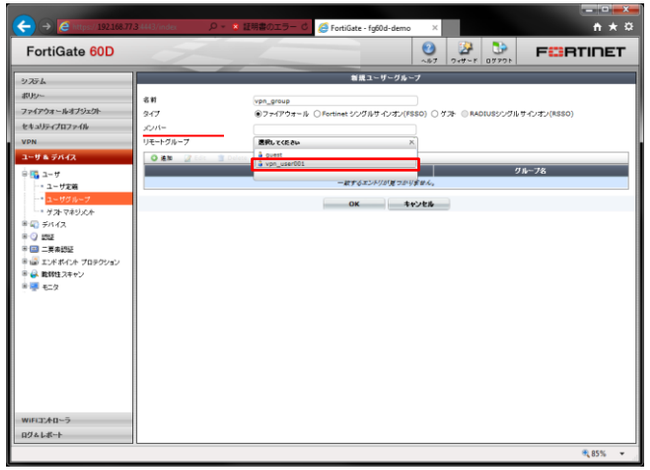
ユーザ＆デバイス⇒ユーザグループ
“新規作成”をクリック



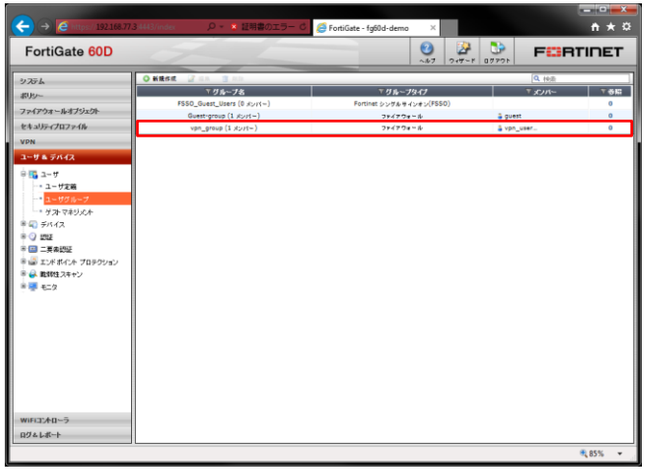
任意のグループ名を入力



グループに所属するユーザを指定し、”OK”をクリック



作成したグループを確認



⑤VPN設定

VPN⇒SSL⇒設定
設定する項目の例

初期値のIPプールを指定

予めインポートしたサーバ証明書のコモンネーム（ホスト名）を指定

SSL-VPNアクセス時に、ID/パスワードとクライアント証明書の２要素認証するためにチェック

⑥SSL-VPNポリシー作成

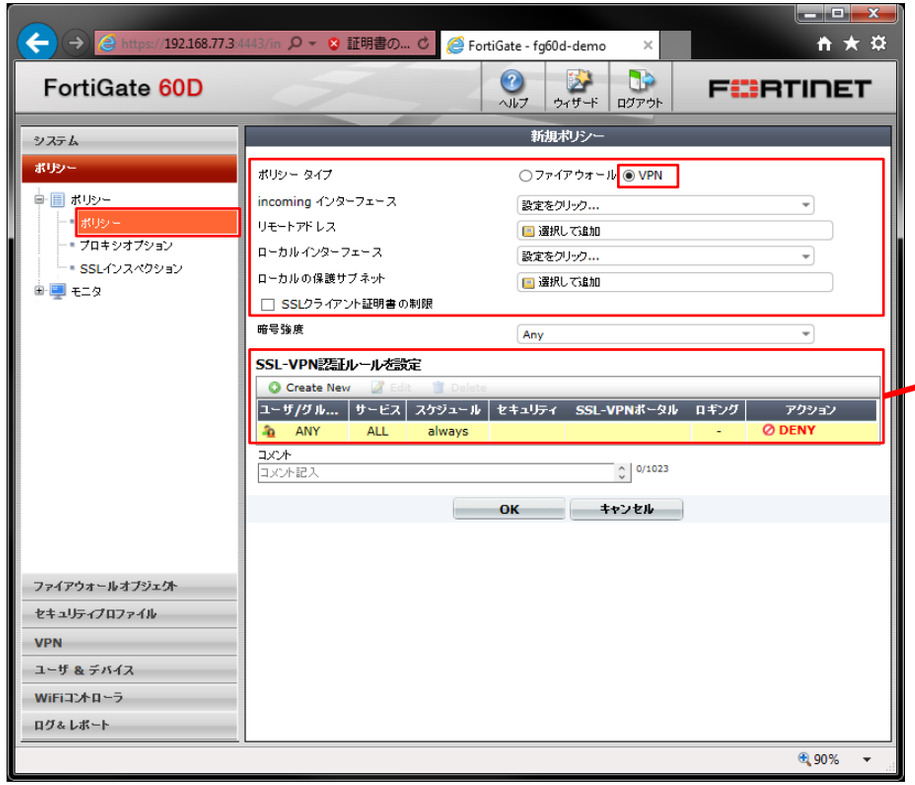
ポリシー⇒ポリシー

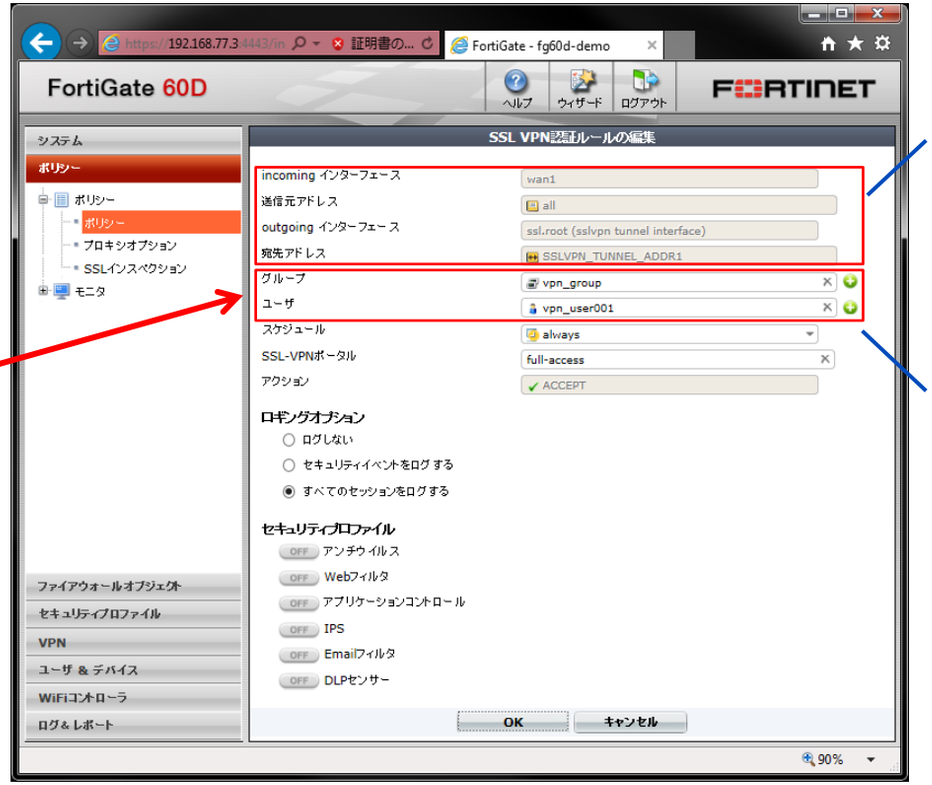
・上部、“VPN”を指定し各項目を設定

・”SSL-VPN認証ルールを設定”は、
予め作成したグループ・ユーザを指定し追加

各種設定後の内容を確認

※ネットワーク設定は、利用環境に依存します。





本手順で使用したポート（インターフェース）、IPアドレス

送信元、アクセスグループ（ユーザ）を設定時に、”SSL-VPN認証ルールを設定”

7．FortiClientセットアップ

①　Windows環境（Windows10）

A)　クライアント証明書のインポート
B)　FortiClientのインストール
C)　SSL-VPN接続設定・接続

②　iOS環境（iOS9.3.2）

A)　FortiClientにクライアント証明書のインポート
B)　FortiClientのインストール
C)　SSL-VPN接続設定
D)　SSL-VPN接続

③　Android環境（Android6.0.1）

A)　FortiClientのインストール
B)　SSL-VPN接続設定
C)　SSL-VPN接続

①Windows環境（Windows10）

■補足

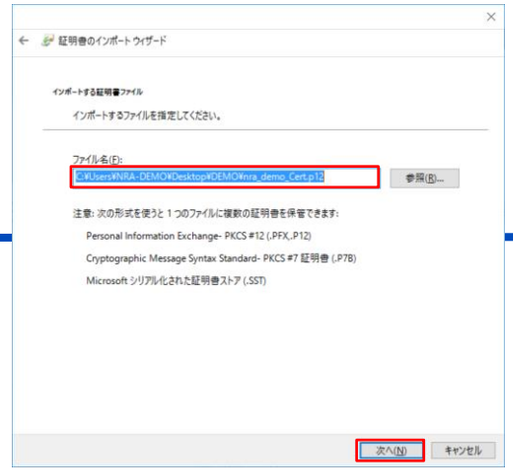
- FortiClientから指定するクライアント証明書はOS標準のストアから指定する
- FortiClientを”Complete：完全”インストールするとアンチウィルス、Webセキュリティ機能がバンドルされた形でインストールされる

①－Ａ）クライアント証明書のインポート（Windows10）

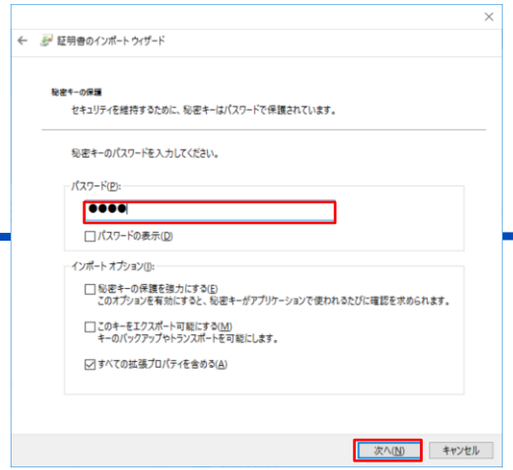
例）拡張子が”p12”であるクライアント証明書をダブルクリックし、標準ウィザードでインポート

ウィザードが開始、“次へ”をクリック

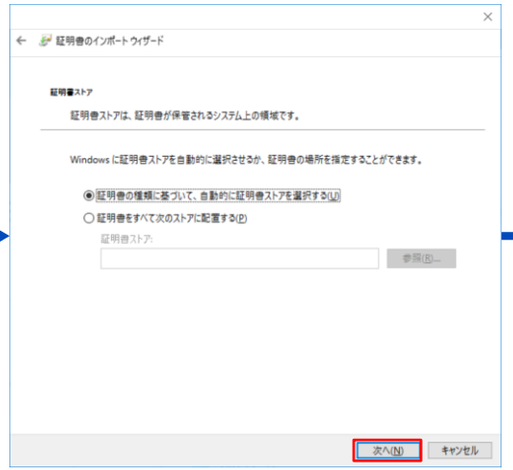
証明書ファイルを指定し、“次へ”をクリック



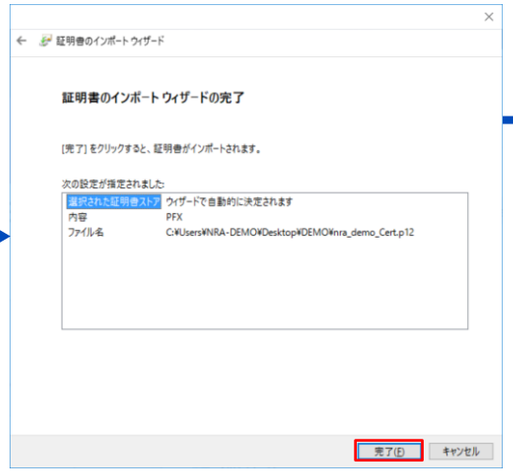
パスワードを入力し、“次へ”をクリック



“次へ”をクリック

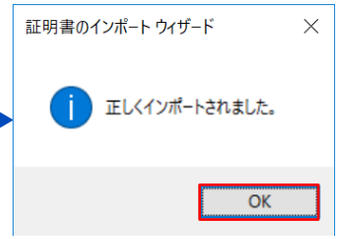


ウィザード完了、“次へ”をクリック



初回、確認されるが、”はい”をクリック

“OK”をクリックしてインポート完了

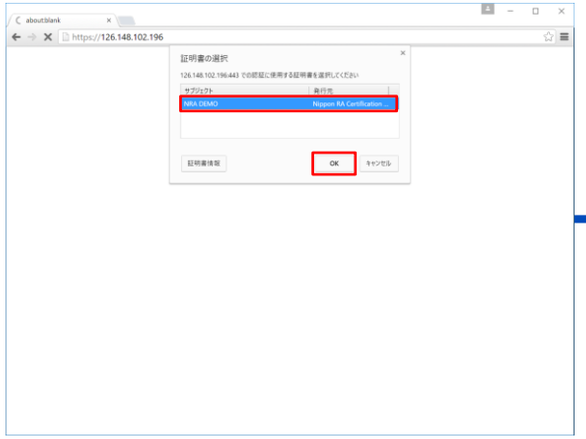


弊社の証明書発行サービスをご利用いただくと自動でインポートするツールをご提供します。

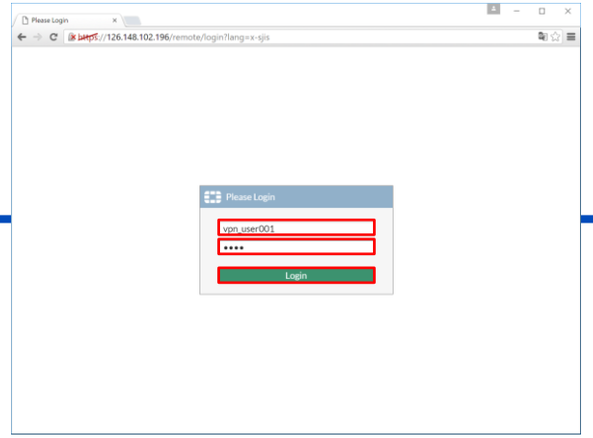
①－Ｂ）FortiClientのインストール

FortiGateにSSL-VPN設定した URL（FQDN）にブラウザでアクセスしFortiClientをダウンロード

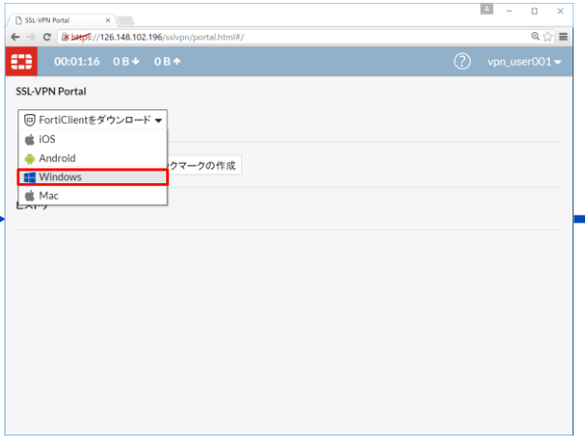
クライアント証明書を選択して、”OK”をクリック



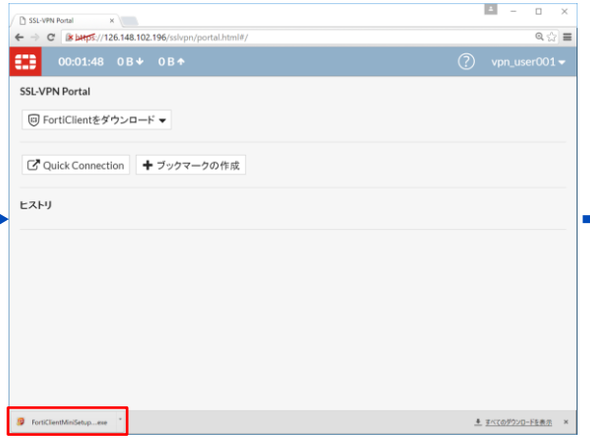
ID、パスワードを入力し、“Login”をクリック



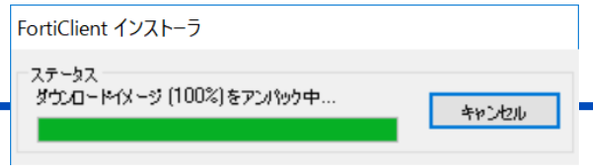
FortiClientをダウンロードするOSを指定



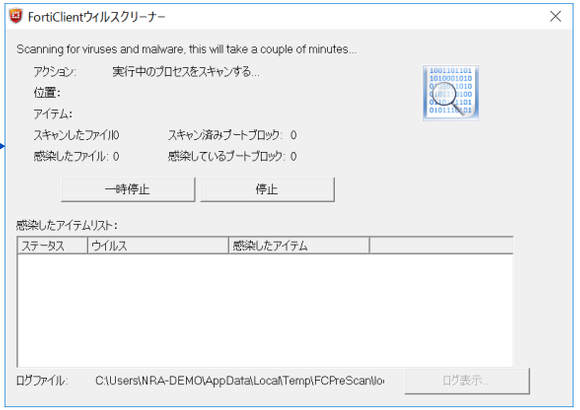
ダウンロードしたファイルをクリックして実行



FortiClientのインストーラが起動する準備

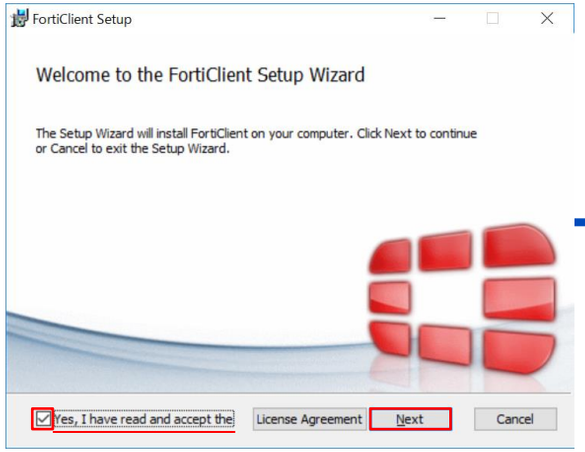


標準のウィルスチェッカーが実行されてから
FortiClientのインストーラが起動

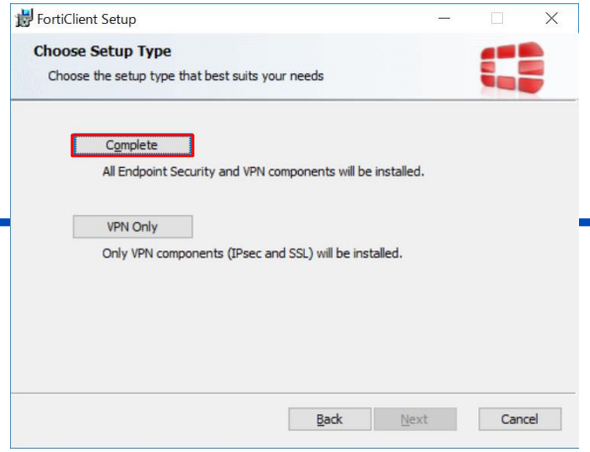


①－Ｂ）FortiClientのインストール

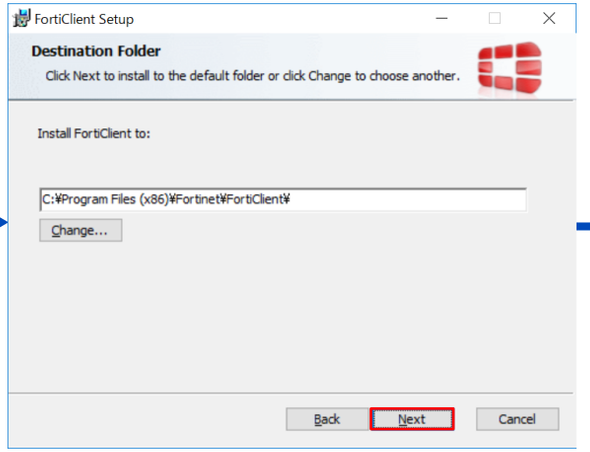
ライセンス同意にチェックを入れ、”NEXT”をクリック



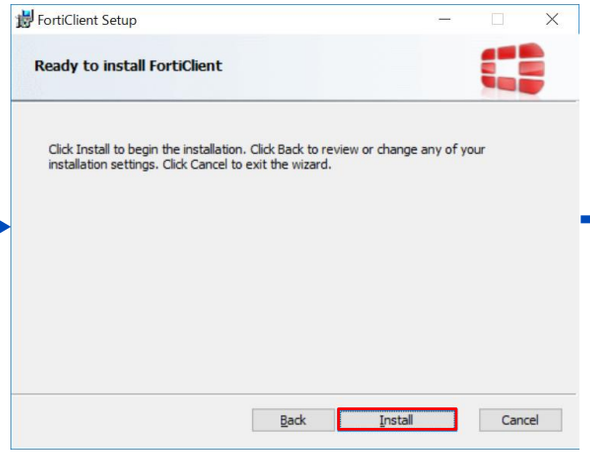
”Complete”をクリック
（アンチウィルス、Webセキュリティがバンドル）



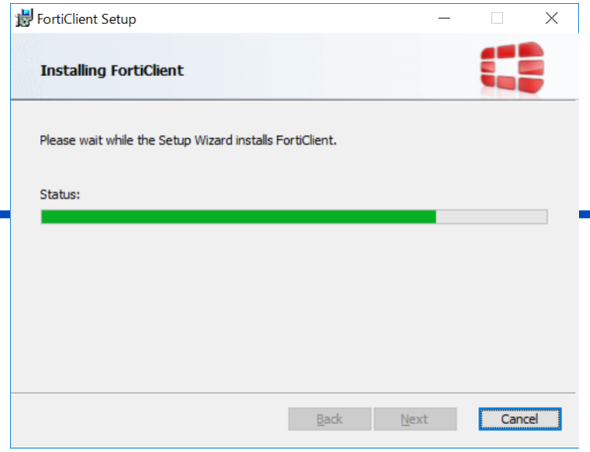
“Next”をクリック



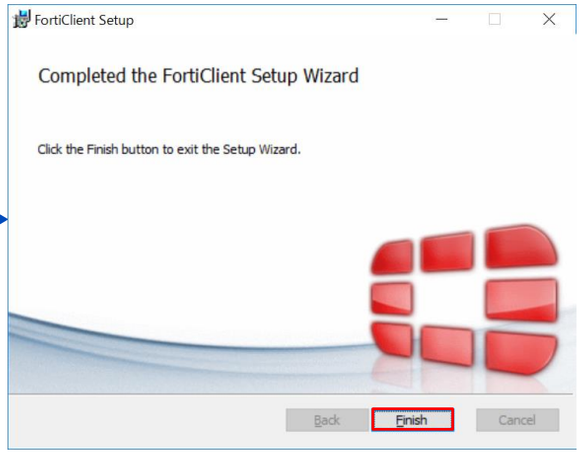
”Install”をクリック



インストール進捗が表示



“Finish”をクリックしてインストール完了

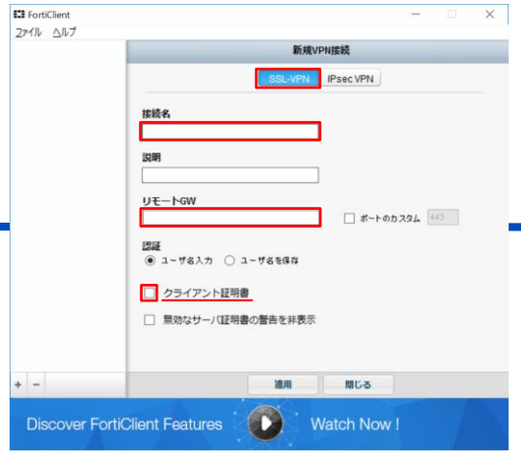


①－C）SSL-VPN接続設定・接続

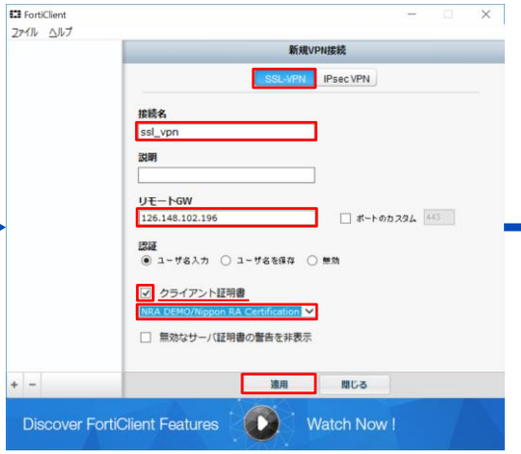
“ID/パスワード” + “クライアント証明書”と認証要素を２つとしたSSL-VPN接続設定

“リモートアクセス”⇒”VPN設定”をクリック

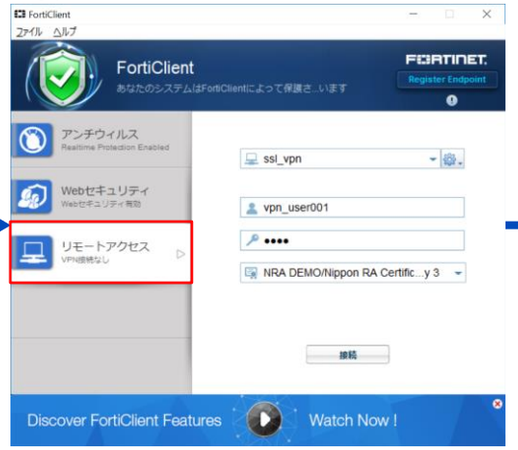
上部、”SSL-VPN”を選択し各項目の入力、
“クライアント証明書”にチェック



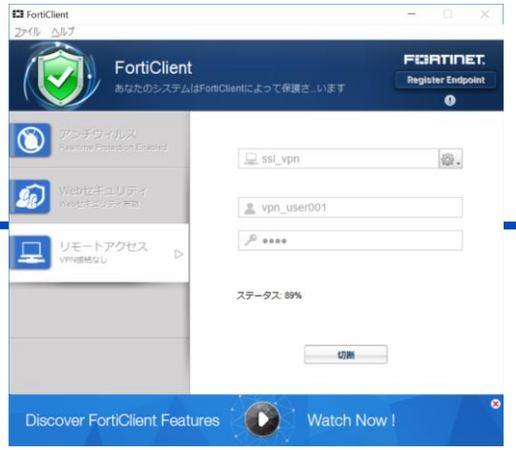
予め、インポートしたクライアント証明書を
選択し、”適用”をクリック



“リモートアクセス”⇒ID/パスワードを入力し
“接続”をクリック



ID/パスワード＋クライアント証明書
の２要素認証でSSL-VPN接続が開始



SSL-VPN接続が開始され、
接続先、状態が表示

②iOS環境（iOS9.3.2）

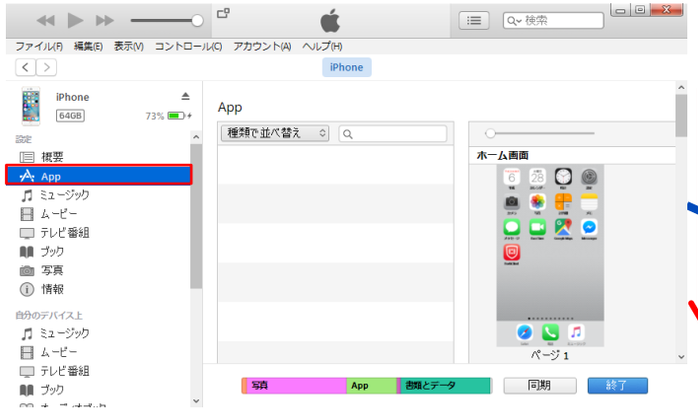
■補足

- FortiClientへのクライアント証明書インストールは iTuneを使用する
  - 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で指定できない
- 事前に iTuneを実行するデバイス（例：WindowsPC）の任意のローカルフォルダにクライアント証明書ファイル（拡張子P12形式）を配置する

②－A）FortiClientにクライアント証明書のインポート

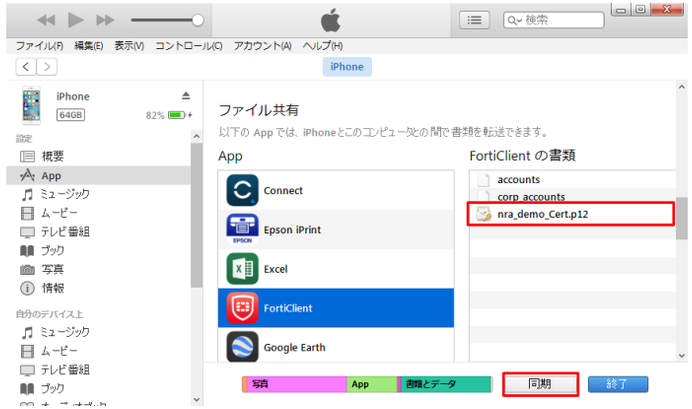
予め、iOSにインポートするクライアント証明書（拡張子P12形式）をiTune実行デバイスに配置

iOSデバイスをUSBで接続し、iTuneを実行
“APP”をクリックし、右ペインを下方へ移動



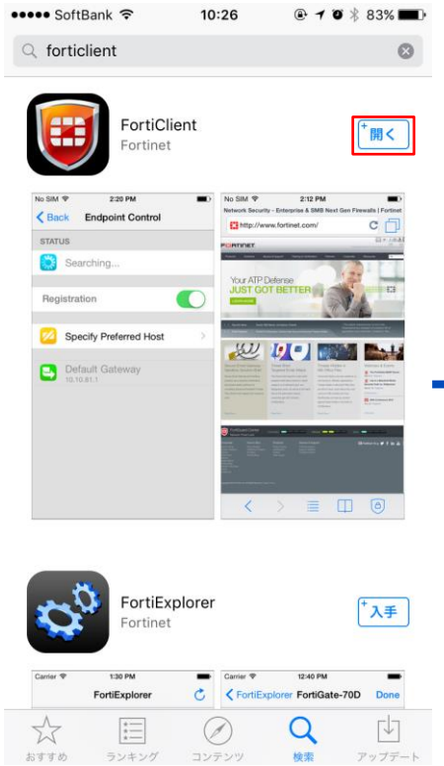
“ファイル共有”⇒”FortiClient”を選択し、iTune実行デバイスに配置した
クライアント証明書をドラッグ＆ドロップ

クライアント証明書がインポートされたこと
を確認し、“同期”をクリック

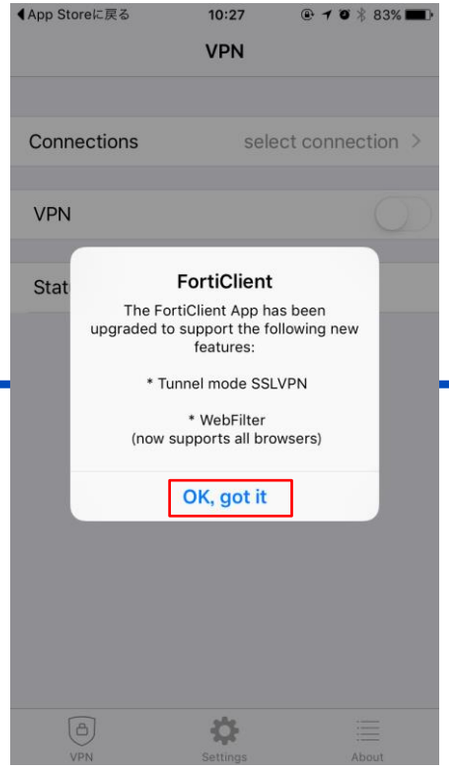


②－Ｂ）FortiClientのインストール

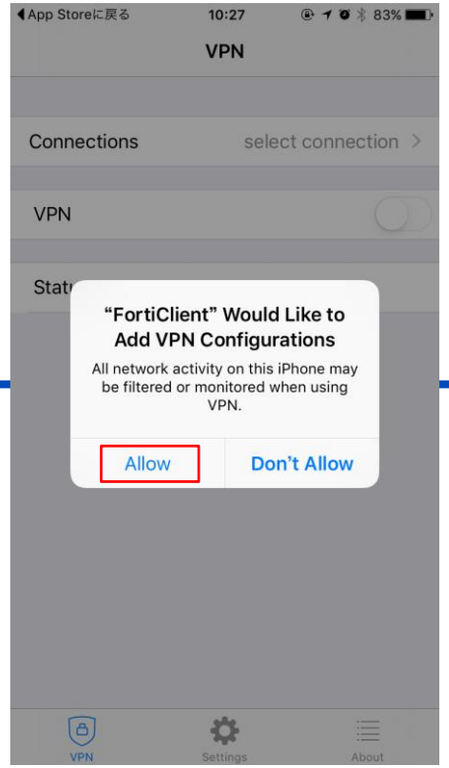
“App Store”から”FortiClient”をインストール後に、”開く”をタップ



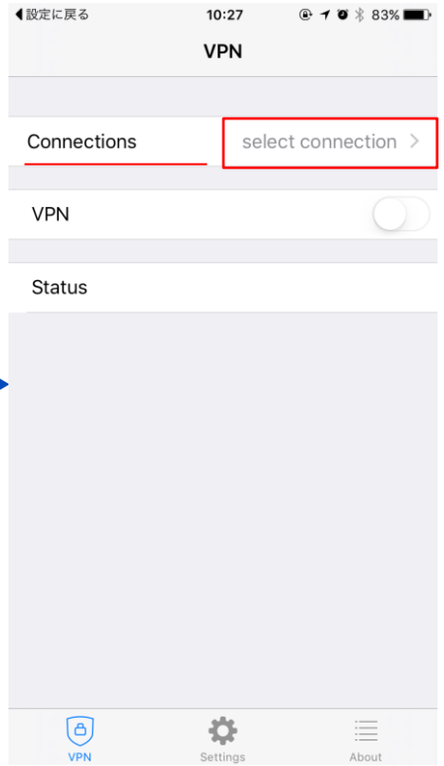
”FortiClient”の機能を確認し、“OK”をタップ



iOSに”FortiClient”がVPN設定追加の許可を確認し、”Allow”をタップ



“Connection”
⇒”Select Connection＞”をタップして設定に進む



②－C）SSL-VPN接続設定

“Add Configuration”
をタップ

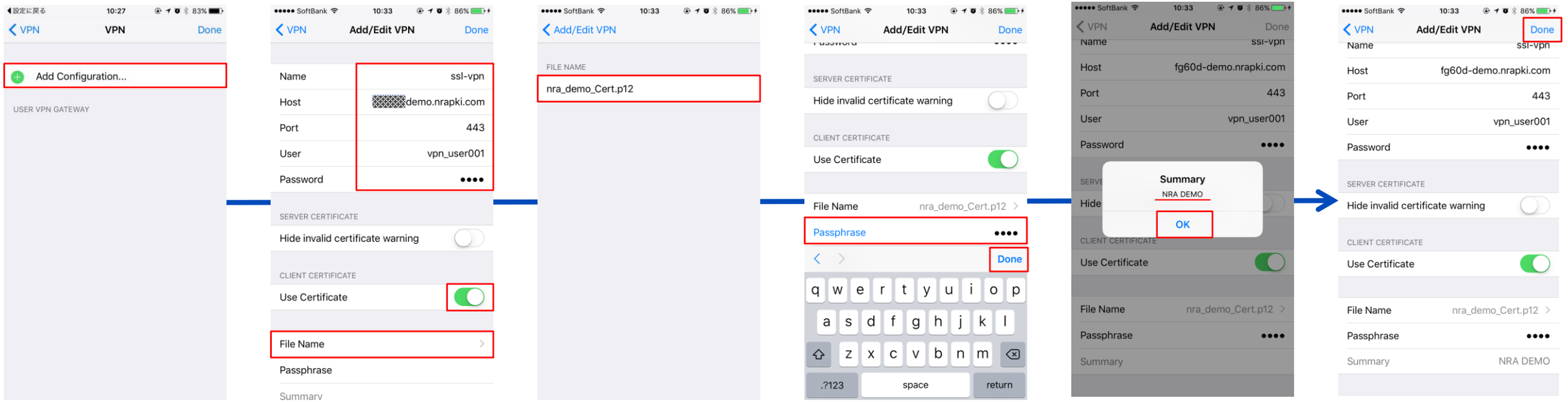
各種パラメータを入力、
“Use Certificate”をON状態
とし、下方に表示された
”File Name”をタップ

②－A）でインポートした
クライアント証明書ファ
イルをタップ

“Passphase”に
クライアント証明書の
パスワードを入力し、
“Done”をタップ

クライアント証明書の
コモンネーム表示後に
“OK”をタップ

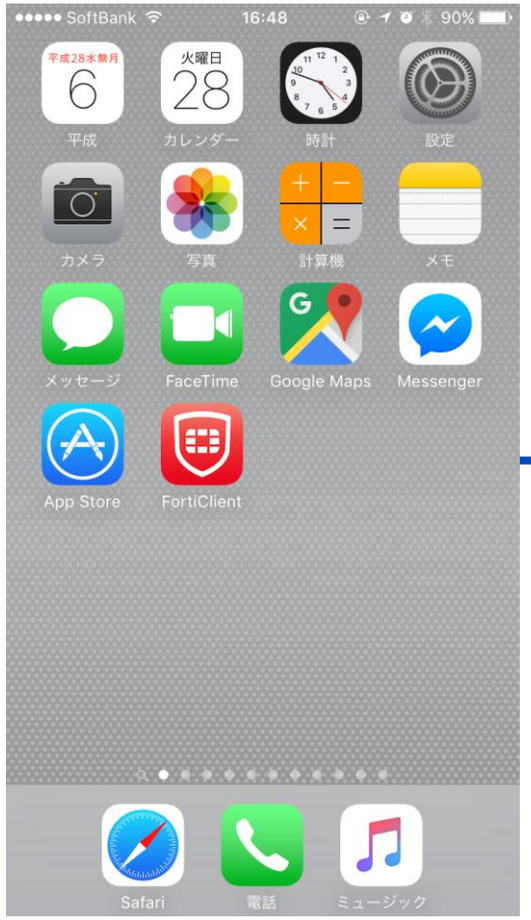
“Done”をタップして、
クライアント証明書で
認証するVPN設定は完了



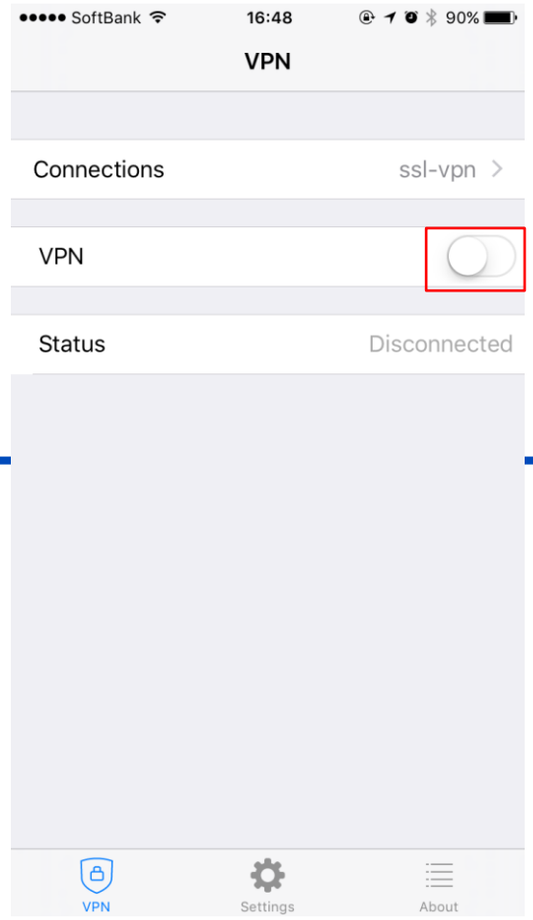
Name　　：任意のVPN接続名
Host　　：FortiGateのFQDN
Port　　：ポート番号
User　　：FortiGateのSSL-VPN用登録ユーザ
Password　：FortiGateのSSL-VPN用登録ユーザのパスワード

②－D）SSL-VPN接続

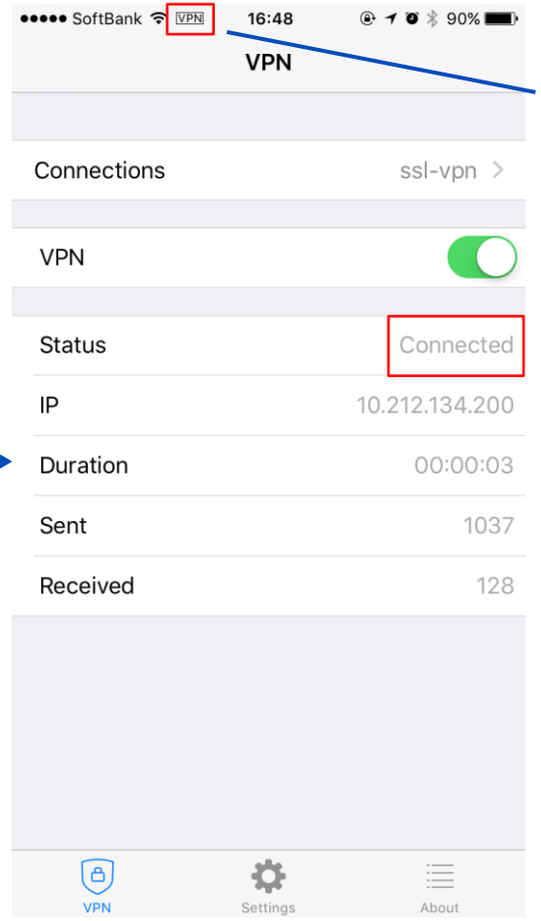
“FortiClient”をタップ



“VPN”をタップし接続開始



“Status”が、”Connected”になり、SSL-VPN接続完了



上部に”VPN”のアイコンからもSSL-VPN接続状態を確認可能

③Android環境（Android6.0.1）

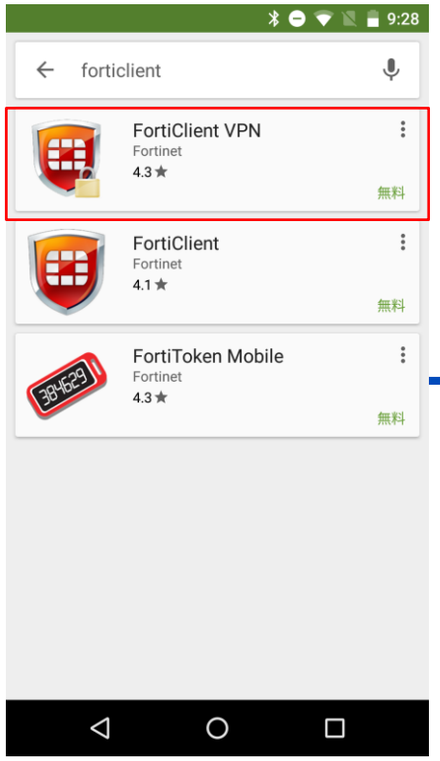
■補足

- FortiClientから指定するクライアント証明書は内蔵ストレージからファイル指定する
  - Android標準の認証ストレージにインストールしたクライアント証明書はFortiClientで指定できない
- 事前に、Androidの内蔵ストレージにクライアント証明書ファイル（拡張子P12形式）を配置する
  - 例としては、WindowsPCにUSB接続してストレージにコピーする

③－A）FortiClientのインストール

予め、Androidにインポートするクライアント証明書（拡張子P12形式）をローカルフォルダに配置

“Play ストア”から
”FortiClient VPN”をタップ

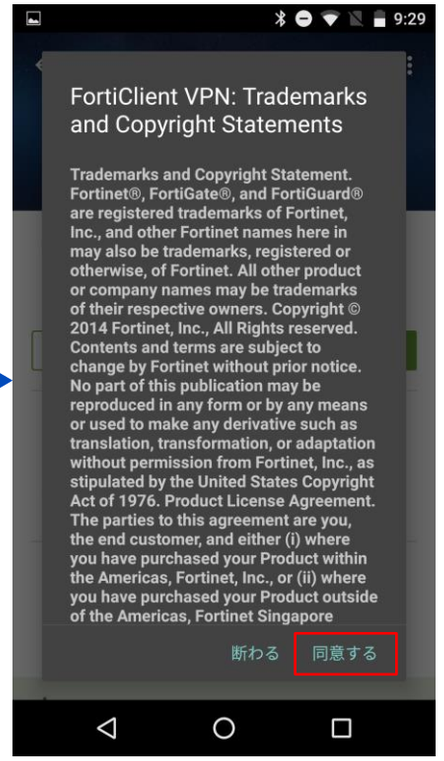


”インストール”をタップ

Androidの新機能を確認し
”次へ”をタップ

“開く”をタップ

商標、著作権を確認し、
“同意する”をタップ



③－Ｂ）SSL-VPN接続設定

任意のVPN名の入力、
VPNタイプを”SSL VPN”
として、作成をタップ

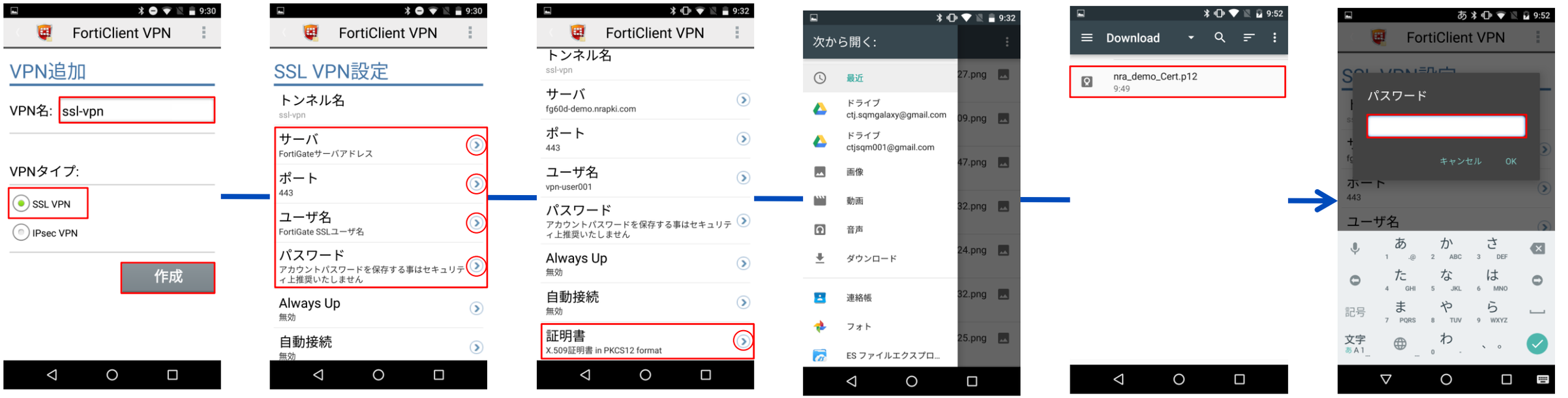
各種任意項目の“＞”を
タップし入力

設定画面の下方へ移動し、
“証明書”の“＞”をタップ

クライアント証明書を配
置したストレージに移動
ここでは、ダウンロード
フォルダを例

クライアント証明書を
タップ

クライアント証明書の
パスワードを入力し、
“OK”をタップ



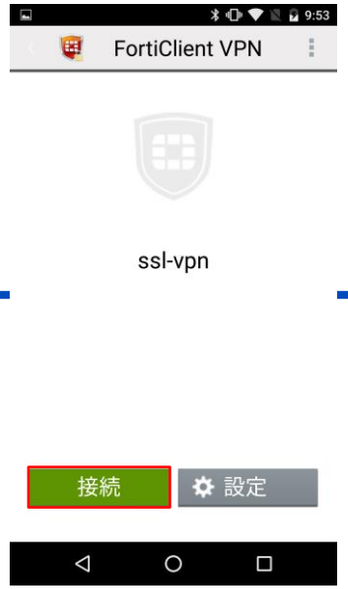
サーバ　　：FortiGateのFQDN
ポート　　：ポート番号
ユーザ名　　：FortiGateのSSL-VPN用登録ユーザ
パスワード　　：FortiGateのSSL-VPN用登録ユーザのパスワード

③－C）SSL-VPN接続

上部に”鍵”のアイコンからもSSL-VPN接続状態を確認可能

設定したVPN名をタップ

“接続”をタップ



ユーザ名、パスワードを入力し、”ログイン”をタップ

インフォメーションを確認し、”OK”をタップ

接続状況を確認

接続が完了

Appendix：初期設定

① 管理者パスワードの変更
② 管理サイトポート、表示言語の変更
③ タイムゾーンの変更
④ ホスト名の変更

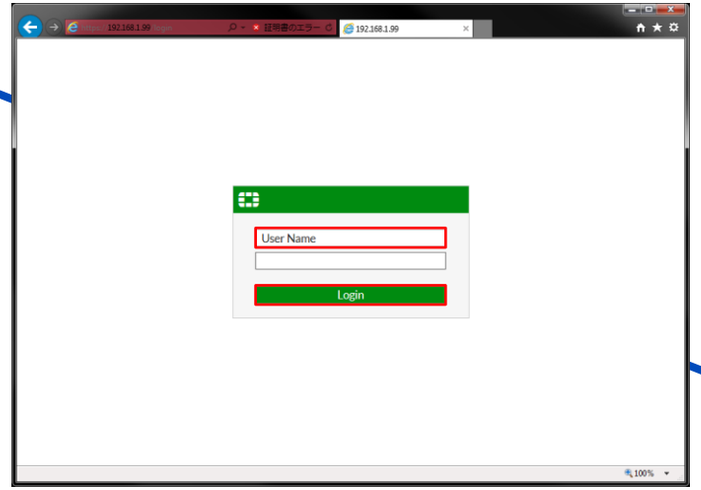
初期設定

下記、初期管理サイトURLにアクセス。
https://192.168.1.99/login

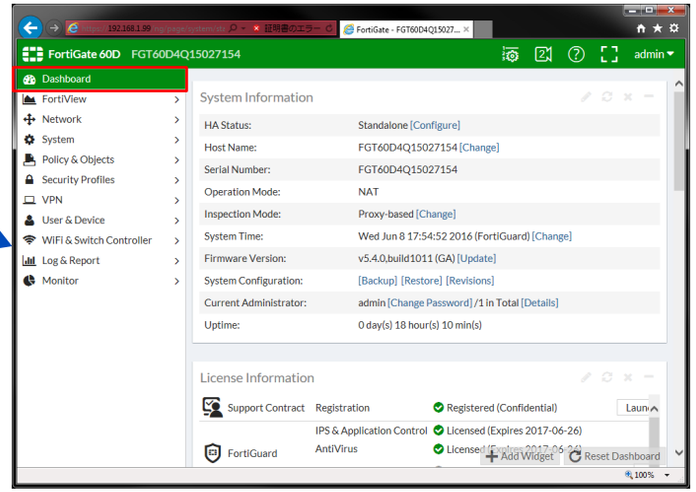
ファームウェアが、5.4の画面イメージ

LANケーブルをFortiGateの
ポート1に挿入しPCと接続
（DHCPでIP払出し）

初期は、”User Name”に admin
を入力しログインをクリック



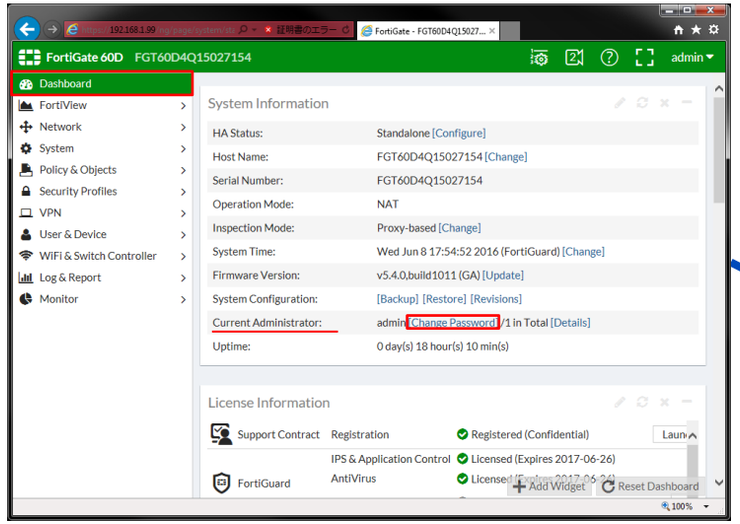
System⇒Dashboard⇒Status
各パラメータを”Change”で変更



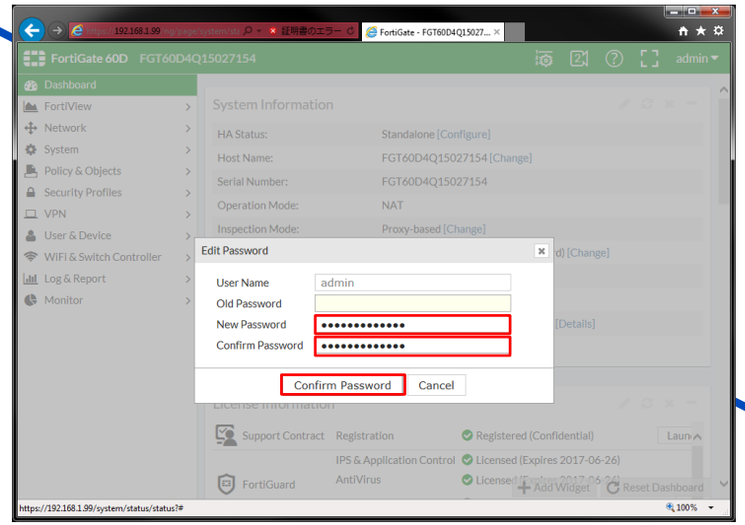
ホスト名、システムタイム、ファーム
ウェア、管理者パスワードが変更可能

①管理者パスワードの変更

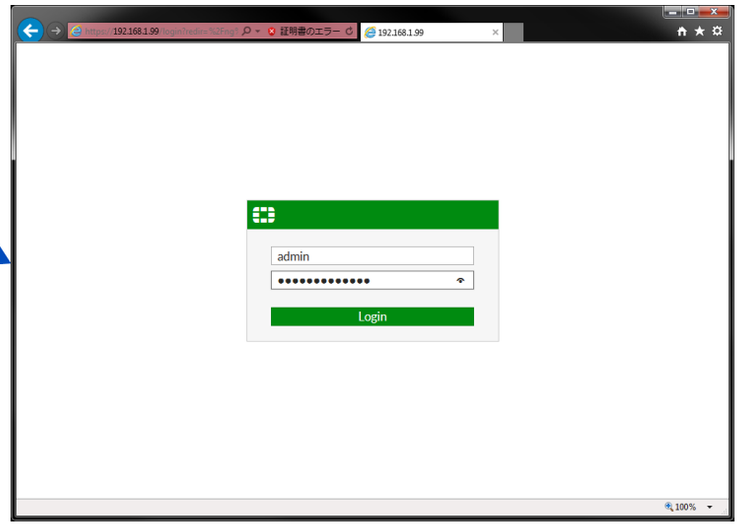
System⇒Dashboard
”Change Password”をクリック



“Old Password”は入力せず、設定する
Passwordを入力し”Confirm Password”
をクリック

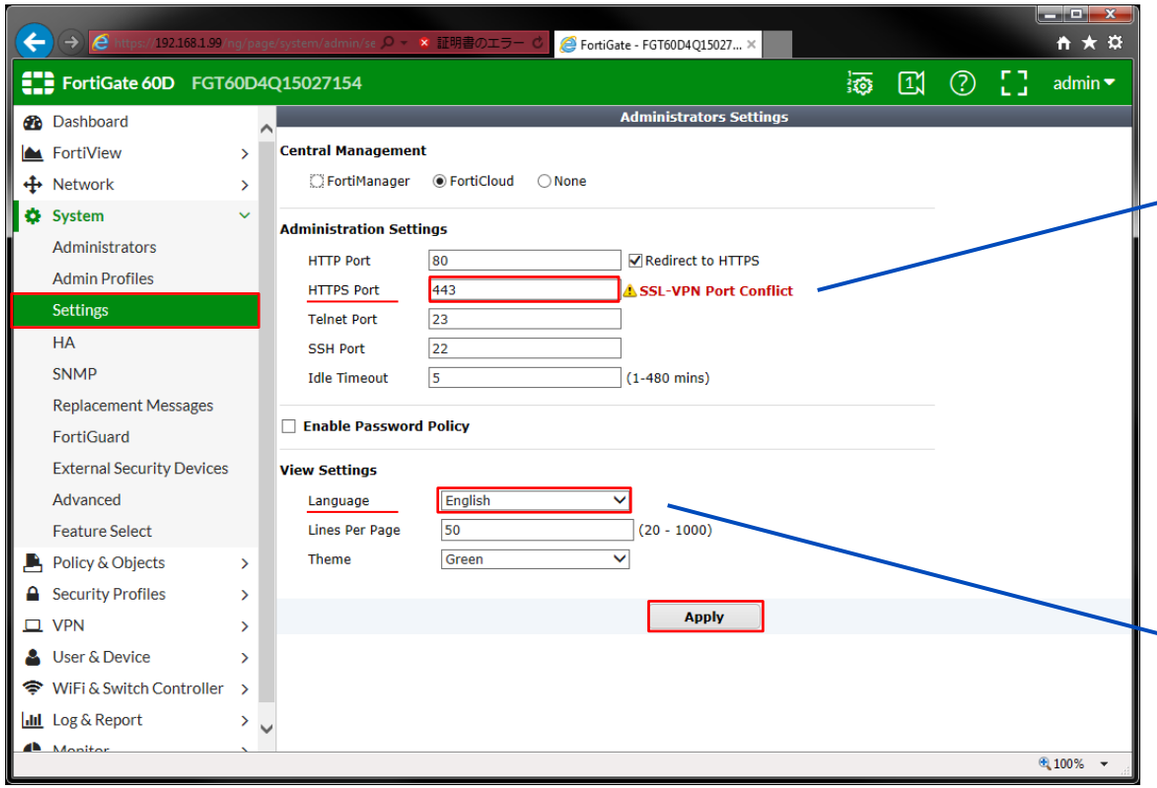


“User Name”に”Admin”を入力し新パスワードで”Login”をクリック



②管理サイトポート、表示言語の変更

System⇒Admin⇒Settings
“HTTPS Port”、”Language“を任意に変更し
“Apply”をクリック



SSL-VPN機能で443ポートを使用する為、管理画面用の”HTTPS Port”を443ポート以外の任意ポート番号に変更します

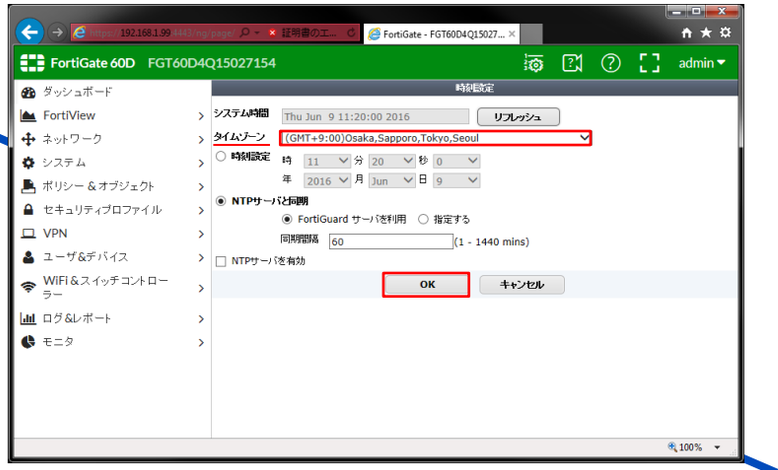
“Apply”（適用）後に、変更したポートを指定した管理サイトURLにログインし直します

表示を”English”⇒”Japanese”に変更します

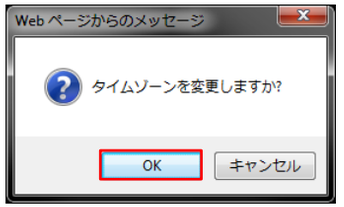
③タイムゾーンの変更

システム⇒ダッシュボード
“システム時間”の”変更”をクリック

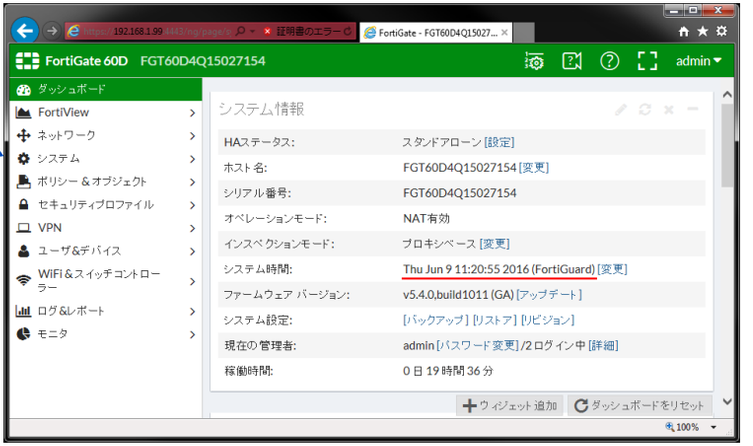
タイムゾーン一覧から選択し”OK”をクリック
（GMT+9:00）Osaka,Sapporo,Tokyo,Seoul



タイムゾーンを選択するとダイアログが表示されるので、”OK”をクリックする



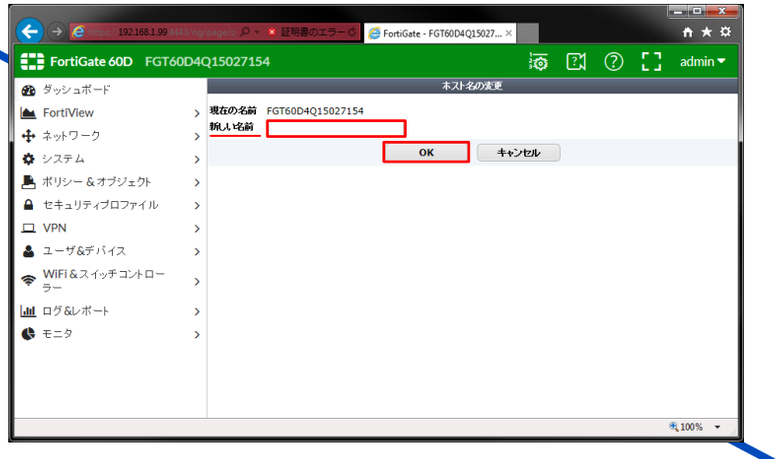
システム時間が現在時間になっていることを確認



④ホスト名の変更

システム⇒ダッシュボード
“ホスト名”の”変更”をクリック

新しい名前にホスト名を入力し
”OK”をクリック



変更したホスト名になっていることを確認