# NRA

# FortiGate(OS 7.2)における クライアント証明書認証設定 手順

2025年01月22日

Ver. 2.00

### 改訂履歴

版	日付	内容	備考
Ver.		初版作成	
1.00			
Ver.	2024/12/6	CRL 更新間隔の設定方法について追記	
1.10	2024/12/0		
Ver.	2025/1/22	ルート、中間証明書および CRL を新認証局	
2.00	2025/1/22	(G2)に変更	

### <目 次>

1. 概要	3
2. 事前準備	4
3. クライアント証明書認証をするための設定手順	6
3.1. 証明書メニューの有効化	7
3.2. 証明書のインポート	8
3.3. PKI ユーザの作成	15
3.4. グループの作成	17
3.5. SSL-VPN の設定	18
3.6. ポリシーの設定	19
4. ユーザ側での準備	20
4.1. Windows (Windows11)	21
4.2. iOS(iOS16.2)	22
4.3. Android(Android11)	26
5. サーバ証明書の入れ替え手順	29
5.1. 新しいサーバ証明書のインポート	30
5.2. サーバ証明書の設定	32

本書は Fortinet 社が提供している FortiGate(OS7.2)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。





# 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。

NRA	統合認	認証基盤	システム	
令和証明書サービス 令和 三郎 様 ログイン中	利用者メンテナンス	_		
● サービス情報メンテナンス 利用法人 詳細設定	利用法人組織の選択	利用者のメンテナ	×x	
利用者 メンテナンス 利用者 削除	令和証明書サービス 加入	組織情報		
ヘルプ     NRA-PKIシステム     サポートサイト	以下のサービスを選択して 「テストサービス(CA4			
● このサイトの実在証明	組織名	部門	住所	電話番号
	本社	東京 千代 △△	節 田区 〇〇町1-2-3 ビル 2階	123-4567-890

# 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。

FortiGate にて証明書を利用できるように設定します。

準備していただいた SSL サーバ証明書、ルート証明書、中間証明書、失効リストをインポートします。

3. PKI ユーザの作成......15

SSL-VPN を利用するユーザを登録します。

登録した SSL-VPN を利用するユーザのグループを作成します。

5. SSL-VPN の設定......18

SSL-VPN の機能に関する詳細設定をします。

SSL-VPN を利用時のアクセスに関するルールを作成します。

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。

## 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			×
1	2		4
メソッドの選択	証明書の詳細	証明書の作成	レビュー
音 証明書の自動提供			
Let's EncryptとACMEプロトコルを使 あります。	用して証明書の作成とメンテナン	スを自動化します。DDNSを有効に	するか、ドメインを購入する必要が
Let's Encryptを使用			
■ 新しい証明書の生成			
FortiGateは当社の自己署名CAを使用 信頼されたCAからのサーバ証明書を	して証明書を生成することができ 使用することを強く推奨します。	ます。 <u>Fortinet_CA_SSL</u>	
証明書の生成			
- 証明書をインポート			
既存の証明書をファイルアップロート	「でインポートします。		
証明書をインポート			
	キャン	セル	

「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。

証明書の作成					×
	Ø	-2-		-3-	
איע א	ッドの選択	証明書の詳細		証明書の作成	レビュー
- 証明書をインズ	ポート				
タイプ ローカ,	ル証明書 PKCS12証明書	E明書			
証明書ファイル	fg60f-7.nrapki.com.crt				
キーファイル	fg60f-7.nrapki.com.key				
パスワード	••••		0		
パスワード確認	••••		0		
証明書名	fg60f-7.nrapki.com				
		作成	戻る	キャンセル	]

### サーバ証明書がインポートされたことを確認します。

FortiGate-60F -	≡ Q.	
🕰 ダッシュボード 🔹 🔉	◆作成/インポート・	編集   自 削除   ◎ 詳細の表示   ▲ ダウンロード   検索   Q
中 ネットワーク  ・	名前≑	サブジェクト ≑
💄 ポリシー&オブジェクト 🔹 🔉	🖃 リモート CA 証明書 👍	
🔒 セキュリティプロファイル ゝ	Fortinet_Wifi_CA	C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA256 2020 CA1
□ VPN >	R Fortinet_CA	$C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate \ Authority, CN = fortinet-ca2, emailAddress = support \textcircled{\texttt{ofortion}} = California, Califo$
💄 ユーザ& 認証 🔹 ゝ	Fortinet_Sub_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = fortinet-subca2001, emailAddress = supp
	R Fortinet_CA_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress = support@fortine.extractional content of the support of the
▲ 2.7=1.	🖻 ローカルCA証明書 🤰	
	Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = FGT60FTK2109DDH8, emailAddress = st
官埋者	Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = Fortinet Untrusted CA, emailAddress = su
管理者プロファイル	🖃 ローカル証明書 16	
ファブリック管理	💀 fg60f-7.nrapki.com	C = JP, O = NipponRA, CN = fg60f-7.nrapki.com
設定	Fortinet_Wifi	C = US, ST = California, L = Sunnyvale, O = "Fortinet, Inc.", CN = auth-cert.fortinet.com
НА	Fortinet_GUI_Server	C = US, ST = California, L = Sunnyvale, O = Fortinet Ltd., OU = FortiGate, CN = FortiGate

#### ■ルート証明書、中間証明書

「システム」-「証明音」を選択し、「作成/インホート」から「CA証明音」を選択します。				
FortiGate-60F 🔹	≡ Ϙ,			
🕰 ダッシュポード 🔹 🔉	◆ 作成/インポート・ 🖉	編集   自 削除   ◎ 詳細の表示   ▲ ダウンロード   検索   Q		
	証明書	サブジェクト♥		
💄 ポリシー&オブジェクト 🔹 🔸	CSRの生成 4			
🔒 セキュリティプロファイル ゝ	CA証明書	C = US. O = DigiCert Inc, CN = DigiCert TLS RSA SHA256 2020 CA1		
묘 VPN >	リモート	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = fortinet-ca2, emailAddress = support@fo		
💄 ユーザ& 認証 🔹 ゝ	CRL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = fortinet-subca2001, emailAddress = supp		
	Fortinet_CA_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress = support@fortine		
	🕒 ローカル CA 証明書 <sub>2</sub>			
♥ <i>\$</i> ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = FGT60FTK2109DDH8, emailAddress = s		
管理者	Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = Fortinet Untrusted CA, emailAddress = su		
管理者プロファイル	□ □−カル証明書 16			
ファブリック管理	Fig60f-7.nrapki.com	C = JP, O = NipponRA, CN = fg60f-7.nrapki.com		
設定	Fortinet_Wifi	C = US, ST = California, L = Sunnyvale, O = "Fortinet, Inc.", CN = auth-cert.fortinet.com		
HA	Fortinet_GUI_Server	C = US, ST = California, L = Sunnyvale, O = Fortinet Ltd., OU = FortiGate, CN = FortiGate		
SNMP	Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@for		
差し替えメッセージ	Fortinet_Factory_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@for		
FortiGuard	Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@for		
表示機能設定	Fortinet_SSL_DSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@for		
証明書 ☆	Fortinet_SSL_DSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@for		
🕼 セキュリティファブリック ゝ	Fortinet_SSL_ECDSA256	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@fo		

### 「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。

CA証明書をイン	ポート	×
タイプ	オンラインSCEP ファイル	
アップロード	NipponRARootCertificationAuthorityG2.crt	
	OK キャンセル	

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。

🐺 FortiGate-60F	• ≡ Q	
🙆 ダッシュボード	▶ + 作成/インポート・ ●	編集   自 削除   ◎ 詳細の表示   ▲ ダウンロード   検索   Q
💠 ネットワーク	> 証明書	サブジェクト♥
💄 ポリシー&オブジェクト	> CSRの生成	
🔒 セキュリティプロファイル	> CA証明書	C = US. O = DigiCert Inc. CN = DigiCert TLS RSA SHA256 2020 CA1
므 VPN	> リモート	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = fortinet-ca2, emailAddress = support@for
💄 ユーザ&認証	> CRL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = fortinet-subca2001, emailAddress = supp
☆ WiFi&スイッチコントロー	> Fortinet_CA_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress = support@fortine
7-	ローカルCA証明書 2	
<b>ロ</b> システム	Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = FGT60FTK2109DDH8, emailAddress = s
管理者	Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = Fortinet Untrusted CA, emailAddress = su
管理者ブロファイル	□ ローカル証明書 16	
ファブリック管理	fg60f-7.nrapki.com	C = JP, O = NipponRA, CN = fg60f-7.nrapki.com
設定	Fortinet_Wifi	C = US, ST = California, L = Sunnyvale, O = "Fortinet, Inc.", CN = auth-cert.fortinet.com
НА	Fortinet_GUI_Server	C = US, ST = California, L = Sunnyvale, O = Fortinet Ltd., OU = FortiGate, CN = FortiGate
SNMP	Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@fo
差し替えメッセージ	Fortinet_Factory_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@fo
FortiGuard	Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@fo
表示機能設定	Fortinet_SSL_DSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@for
証明書	Fortinet_SSL_DSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support @ Fortigate, CN = FGT60FTK2109DDH8, FGT60FTK2109DDH8, CN = FGT60FTK2109DDH8, CN
🚳 セキュリティファブリック	> Fortinet_SSL_ECDSA256	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@fo

### 「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。

CRLをインポート	(	¢
インポート方式 フ:	アイルベースオンライン更新	
C HTTP		
HTTPサーバのURL	http://mpkicrl.managedpki.ne.jp/mpki/N	
LDAP		
SCEP		
	OK キャンセル	

### CRL がインポートされたことを確認します。

FortiGate-60F -	≣ Q	
🕰 ダッシュボード 💦 👌	◆作成/インポート・	・編集 自 削除 ◎ 詳細の表示 ▲ ダウンロード 検索 Q
	名前 \$	サブジェクト♥
🛃 ポリシー&オプジェクト 🔥		
🔒 セキュリティプロファイル ゝ	CRL_1	
묘 VPN >	- リモートCA証明書 🌀	
≗ ユーザ&認証 >	R CA_Cert_2	C = JP, O = Nippon RA Inc., CN = Nippon RA Certification Authority 4 G2
♥ WiFi & スイッチコントロー 、	R CA_Cert_1	C = JP, O = Nippon RA Inc., CN = Nippon RA Root Certification Authority G2
7-	Fortinet_Wifi_CA	C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA256 2020 CA1
¢ システム 2 ∨	Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = fortinet-ca2, emailAddress = support@fortin
管理者	Fortinet_Sub_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = fortinet-subca2001, emailAddress = support
管理者プロファイル	Fortinet_CA_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress = support@fortinet.c
ファブリック管理 1	□ □-カルCA証明書 2	
設定	Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = FGT60FTK2109DDH8, emailAddress = supp
НА	Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = Fortinet Untrusted CA, emailAddress = supp
SNMP	日 ローカル証明書 (17)	
差し替えメッセージ	202302071013303	C = JP, O = NipponRA, CN = fg60f-7.nrapki.com
FortiGuard 🚺	📭 fg60f-7.nrapki.com	C = JP, O = NipponRA, CN = fg60f-7.nrapki.com
表示機能設定	Fortinet_Wifi	C = US, ST = California, L = Sunnyvale, O = "Fortinet, Inc.", CN = auth-cert.fortinet.com
証明書 🗘	Fortinet_GUI_Server	C = US, ST = California, L = Sunnyvale, O = Fortinet Ltd., OU = FortiGate, CN = FortiGate
🕼 セキュリティファブリック ゝ	Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@fortin
■ ログ&レポート >	Fortinet_Factory_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@fortin
	Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@fortin

【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 (setti	.ng	) # get			
ocsp-status : enable					
ocsp-option	:	server			
ocsp-default-server	:	mpki_ocsp			
interface-select-met	h	od: 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-absenc	e	: ignore			
strict-ocsp-check	:	disable			
ssl-min-proto-version: default					
cmp-save-extra-certs	:	disable			
cmp-key-usage-checki	.nç	g: 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

enu

exit

# 3.3. PKI ユーザの作成

「ユーザ&認証」-「PKI」を選択し、「新規作成」を選択します。

FortiGate-60F	• ≡ Q		
の ダッシュボード	◆ 新規作成   承 編集   會 削除   検	Q	
💠 ネットワーク	名前	サブジェクト	CA
🖹 ポリシー&オブジェクト	testPKI		CA_Cert_1
🔒 セキュリティプロファイル	•		
묘 VPN	>		
💄 ユーザ&認証	·		
ユーザ定義			
ユーザグループ			
ゲスト管理			
LDAPサーバ			
RADIUSサーバ			
シングルサインオン			
認証設定			
FortiToken			
РКІ 1	2		
♥iFi&スイッチコントロー テー	>		

下図の赤枠内の項目を設定し OK をクリックします。

FortiGate-60F 🔹	≡ Q
🙆 ダッシュボード 💦 👌	新規PKIユーザ
	名前 Sample//m
🖹 ポリシー&オブジェクト 🔹 🔉	サブジェクト SampleVpn@nrapki.jp
🔒 セキュリティプロファイル ゝ	CA CA_Cert_2
모 VPN >	
💄 ユーザ&認証 🛛 🗸 🗸	
ユーザ定義	
ユーザグループ	
ゲスト管理	
LDAPサーバ	
RADIUSサーバ	
シングルサインオン	
認証設定	
FortiToken	
PKI ☆	
♥iFi&スイッチコントロー ラー	
Ф         ЭХТА         >	
🐠 セキュリティファブリック ゝ	OK キャンセル

■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&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

# 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。

FortiGate-60F	≡ Q.		
🙆 ダッシュボード 💦 👌	◆新規作成 ● 編集 幅 クローン 會 削除 検索 Q		
♣ ネットワーク	グループ名≑	グループタイプ ≑	メンバー ≑
💄 ポリシー&オブジェクト 🔹	Guest-group	■ ファイアウォール	🛔 guest
🔒 セキュリティプロファイル ゝ	SSO_Guest_Users	℡ Fortinetシングルサインオン(FSSO)	
묘 VPN >			
💄 ユーザ&認証 🔷 🗸	J		
ユーザ定義			
ユーザグループ 😚			

### 下図の赤枠内の項目を設定し OK をクリックします。

🐺 FortiGate-60F	- = Q
🕰 ダッシュボード 💦 👌	新規ユーザグループ
<ul> <li></li></ul>	名前 vpn-test
▲ ホリシー&オフジェクト >	タイプ ファイアウォール
	Fortinetシングルサインオン(FSSO) RADIUSシングルサインオン(RSSO)
묘 VPN >	ゲスト
🛓 ユーザ&認証 🛛 🗸 🗸	メンバー 🔈 SampleVpn 🗙
ユーザ定義	+
ユーザグループ 😭	
ゲスト管理	
LDAPサーバ	
RADIUSサーバ	
シングルサインオン	
認証設定	
FortiToken	
РКІ	OK キャンセル
WiFi&スイッチコントロ	

### ■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 PKI ユーザを選択

# 3.5. SSL-VPN の設定

「VPN」-「SSL-VPN 設定」から下図の赤枠の項目を設定し「適用」をクリックします。

FortiGate-60F	Ξ Q.			
	SSLVPN股定			
+ ネットワーク >	接续設定 0			
占 ポリシー&オブジェクト 🔹 👌	SSLVPNを有効 C			
🔒 セキュリティプロファイル >	リッスンするインターフェース Mill want ¥			
⊑ VPN Ý	リッスンするポート 443			
オーバーレイコントローラ				
iParch \All.	Webt = Tr / 7 L 4 2 9 9 A 7 8 8 A - Tr     http://12.168.77.2443			
IPosett atf - K				
iParchンネルテンプレー	プラー/121時間 WY 1g60f-7.nrapki.com ・ WT00863.appin: 11月/1			
h	The Last File システレット (			
SSL-VPNボータル	アイドルログアウト			
SSL-VPN設定 合	クライアント証明書を要求			
SSL-VPNクライアント				
VPNロケーションマップ	トンネルモートクライアント設定 0			
▲ ユーザ&認証 >	アトレス範囲			
♥WFi&スイッチコントロー ラー	トンネルユーザは、以下の範囲内のIPを受け取ります: 10.212.134.200 - 10.212.134.210			
\$ \$774 \$				
セキュリティファブリック >	UNSサーバを指定 ①			
ビログ&レポート >				
	Webモードの設定			
	言語 0 ブラウザの設定 システム			
	問題ポータルマッピング 0			
	◆新規作成 / 補助 首 創房 ■ SSL-VPH設定の送信			
	ユーザ/グループ キボータル キ			
	關 vpn-test full-access			
	すべてのその他のユーザ/グループ tunnel-access			
	0			
FERTINET	<b>渔</b> 用			

■設定例

リッスンするインターフェース: wan1

リッスンするポート: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」-「ファイアウォールポリシー」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。

🗰 FortiGate-60F 🔹 🔹	≣ Q.		
Ø ダッシュポード >	新規ポリシー		
	名前 0	vpn-test	
🛃 ポリシー&オブジェクト 🗸 🗸	著信インターフェース	SSL-VPN tunnel interface (ssl.roo *	
ファイアウォールポリシー ☆	発信インターフェース	🖷 wani 👻	
アドレス	送信元	I All X 퍫 vpn-test X	
インターネットサービス データベース	宛先	+ Dall ×	
サービス	スケジュール	Ta always	
スケジュール	サービス	Ø ALL ×	
バーチャルル		•	
ルプール	アクション	✓ 許可 ◎ 拒否	
プロトコルオプション	インフルクションエード	70 4 7 7000 4 7	
トラフィックシェイピング	1 1 2200 222 - 1-		
🔒 セキュリティプロファイル >	ファイアウォール/ネット	ワークオプション	
⊒ VPN >	NAT O		
▲ ユーザ&認証 →	IPプール設定	発信インターフェースのアドレスを使用 ダイナミックIPブールを使う	
⇔ WiFi&スイッチコントロー >	送信元ポートの保持 🗇		
	プロトコルオプション		
• <i>SATA</i>	わたっいティブロファイ		
セキュリティファブリック >	2+2)/1/2//1/		
出 ログ&レポート >	アンナワイルス	3	
	DNSZALA	9	
	アプリケーションコント		
	IPS	0	
	ファイルフィルタ	0	
	SSLインスペクション	🚾 no-inspection 🔹 🌶	
	ロギングオプション		
	許可トラフィックをログ	セキュリティイベント すべてのセッション	
	コメント コメント記2	/ O/1023	
	このポリシーを有効化 🕊	<u></u>	
			OKキャンセル

■設定例

着信インターフェース:SSL-VPN トンネルインターフェース 発信インターフェース: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(OS7.2)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

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。

流れは次の通りです。

4.1. Windows(Windows11) ......21 Windows 端末における FortiClient の設定をします。

4.2. iOS(iOS16.2)......22

iOS 端末における FortiClient の設定をします。

Android 端末における FortiClient の設定をします。

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。

# 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。

	SSEVPN IPSEC VPN AML	
接続名	vpntest	
説明	テスト	
リモートGW	0.0.00	ж
	◆リモートゲートウェイを追加	
	✓ ポートの編集 443	
	VPNトンネルのシングルサインイン (SSO) を有効	好比
クライアント証明書	Sample Vpn / Nippon RA Certification Authority 4 G2	× 👁
認証	🔘 ユーザ名入力 🔘 ユーザ名を保存 🔾 無効	
	IPv4/IPv6デュアルスタックアドレスを有効化。	

■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:チェックを入れ、SSL-VPN 設定で設定した「リッスンするポート」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

■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 iTunes を使用します。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。

iTunes 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)を配置してください。

iOS 端末を USB で接続し、iTunes を起動し「ファイル共有」-「FortiClientVPN」を選択してください。

↔ ♦ ₩	-0	<b>É</b>	
ファイル(F) 編集(E) 表示(V) コントロール(	こ) アカウント(A) ヘルプ(H)	NRA-PKI	
NRA-PRI         ▲           12808         6% □ +           BZ         5% □ +           III         5% □ +           IIII         5% □ +           IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	ファイル共有 以下のAppでは、iPadとごのコンピ App FortiClientVPN	1-92の間で書類を転送できます。 書類 このり このり	ストから、iPadで専項を表示するAppを選択してください。
		空き領域: 115.83 GB	同期終了

「ファイルを追加」よりクライアント証明書を指定し、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」をクリックしてください。

≪ ▶ ₩	0		<b>É</b>		Q~ 検索	
ファイル(F) 編集(E) 表示(V	) コントロール(C) アカウント(A)	ヘルプ(H)	NRA-PKI			
NRA-PKI     12200     12200     12200     123-3979     1-12-3979     1-4     ラス直     1710-世報祖     写真     1710-世報祖     123-3979     1-4     710-世報祖     ブック     1-4     710-世報祖     ブック     1-4     デンク     1-4     デンク     1-4     デンク     1-4     デンク     1-4     デンク     1-4     デンク	± 77 № Т Ар	イル共有 のAppでは、iPadとこのコンピュータと p FortiClientVPN	の間で書類を転送できます。 FortiClientVPN	Iの書類 112	8 KB 今日 15: 77fルを追加.	16 <i>保存</i>
			空き領域: 115.78 GB		同期	終了

以上でクライアント証明書のインポートは完了です。

### 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。

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

VPN	
UPGRADE TO THE FULL VERSION TO ACCESS ADDITIONAL FEATURE	RES AND RECEIVE TECHNICAL SUPPORT
Connections	Select Connection >
VPN	0
Status	

### 「Add Configuration」をタップします。

< VPN	VPN	Done
Add Configuration		
Scan QR Code to add VPN		
USER VPN GATEWAY		

下図の赤枠内の項目を入力し「Use Certificate」を有効にし、「File Name」をタップします。

< VPN	Add/Edit VPN	Save
ACCOUNT INFO		
Name		vpntes
Host		https://fg60f-7.nrapki.com
Ð	Add remote gateway	
Port		44
SSO		
User		SampleVp
CLIENT CERTIFICATE		
Use Certificate		
File Name		>
Passphrase		
Summary		

### 事前にインポートしたクライアント証明書を選択します。

< Cancel			
FILE NAME			
ForticlientTest.p12	2		

「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。

VPN     Add/Edit VPN     Save       ACCOUNT INFO     Name     vpntest       Host     https://fg60f-7.nrapki.com       Add remote gateway     Add remote gateway       Port     443       SSO     O       User     SampleVpn       CLIENT CERTIFICATE     O       File Name     ForticlientTest.p12 >       Passphrase     Summary			
ACCOUNT INFO Name vpntest Host https://fg60f-7.nrapki.com Add remote gateway Port 443 SSO 00 User SampleVpn CLIENT CERTIFICATE Use Certificate  File Name ForticlientTest.p12 > Passphrase Summary	< VPN	Add/Edit VPN	Save
Name     vpntest       Host     https://tg60f-7.nrapki.com       Add remote gateway     Add remote gateway       Port     443       SSO     0       User     SampleVpn       cLEENT CERTIFICATE     0       Use Certificate     0       File Name     ForticlientTest.p12 >       Passphrase     0	ACCOUNT INFO		
Host https://fg60f-7.nrapki.com Add remote gateway Port 443 SS0 00 User SampleVpn CLIENT CERTIFICATE Use Certificate  File Name ForticlientTest.p12 > Passphrase Summary	Name		vpntest
Add remote gateway Port 443 SSO 443 User SampleVpn CLIENT CERTIFICATE Use Certificate File Name ForticlientTest.p12 > Passphrase Summary	Host		https://fg60f-7.nrapki.com
Port     443       SSO     0       User     SampleVpn       CLIENT CERTIFICATE     0       Use Certificate     0       File Name     ForticlientTest.p12 >       Passphrase     0       Summary     0	Ð	Add remote gateway	
SSO O SampleVpn CLIENT CERTIFICATE Use Certificate File Name ForticlientTest.p12 > Passphrase Summary	Port		443
User SampleVpr CLIENT CERTIFICATE Use Certificate File Name ForticlientTest.p12 > Passphrase Summary	SSO		
CLIENT CERTIFICATE Use Certificate File Name ForticlientTest.p12 > Passphrase Summary	User		SampleVpn
Use Certificate  File Name ForticlientTest.p12 > Passphrase Summary	CLIENT CERTIFICATE		
File Name ForticlientTest.p12 > Passphrase Summary	Use Certificate		
Passphrase Summary	File Name		ForticlientTest.p12 >
Summary	Passphrase		
	Summary		
	Summary		

クライアント証明書のコモンネームを確認して「OK」をタップします。

< VPN	Add/Edit VPN	Save
ACCOUNT INFO		
Name		vpntest
Host		https://fg60f-7.nrapki.com
0	Add remote gateway	
Port		443
SSO		
User		SampleVpn
CLIENT CERTIFICATE		
Use Certificate	Summary Forticlient Test	
File Name	ок	ForticlientTest.p12 >
Passphrase		
Summary		

### 「Save」をタップします。

< VPN	Add/Edit VPN	Save
ACCOUNT INFO		
Name		vpntest
Host		https://fg60f-7.nrapki.com
•	Add remote gateway	
Port		443
SSO		
User		SampleVpn
CLIENT CERTIFICATE		
Use Certificate		
File Name		ForticlientTest.p12 >
Passphrase		
Summary		Forticlient Test

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

### ■設定例

Name : 任意の値

Host:FortiGateのFQDN

Port:SSL-VPN 設定で設定した「リッスンするポート」を指定

SSO : 任意

User: SSL-VPN 設定で設定した PKI ユーザ

Use Certificate:有効

File Name: PKI ユーザ作成時に指定したクライアント証明書

Passphrase: クライアント証明書のパスワード

# 4.3. Android (Android11)

■クライアント証明書のインポート

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選択します。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 で指定できません。

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)を配置してください。

ご利用の Android 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、任意のトンネル名を入力してください。VPN タイプ「SSL VPN」を選択して「作成」 をタップします。

	FortiClient VPN	≡
VPN追加		
vpntest		
VPNタイプ ・ SSL VPN		
O IPsec VPN		
	作成	

### 下図の赤枠内の項目を入力し、「証明書」をタップします。

FortiClient VPN	=
SSL VPN股定	
トンネル名 vpntest	
ポート 443	>
Servers fg60f-7.nrapki.com	>
ユーザ名 SampleVpn	>
<b>証明書</b> PKCS12フォーマットのX.509証明書	>
Single Sign On <sup>無効</sup>	>
Prompt User Credentials <sup>無効</sup>	>
VPN削除	
<b>VPNトンネルプロファイル削除</b> このVPN設定を削除し、VPNトンネルリストから消去します。	

クライアント証明書を指定し、クライアント証明書のパスワードを入力し「OK」をタップします。

	FortiClient VPN		Ξ
SSL VPN股定			
	•		
Servi 1960f-7	• 		
ユー Sample	キャンセル	ок	
証明書 PKCS12フォーマットのX.5	609証明書		
Single Sign On <sup>無効</sup>			

### クライアント証明書が指定されます。

FortiClient VPN	≡
SSL VPN股定	
トンネル名 vpntest	
ポート 443	>
Servers fg60f-7.nrapki.com	>
ユーザ名 SampleVpn	>
証明書 CN=Nippon RA Certification Authority 4,0=Nippon RA Inc.,C=JP	>
Single Sign On <sup>無効</sup>	>
Prompt User Credentials <sup>無効</sup>	>
VPN削除	
<b>VPNトンネルプロファイル削除</b> このVPN設定を削除し、VPNトンネルリストから消去します。	

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

■設定例
 トンネル名:任意
 ポート:SSL-VPN 設定で設定した「リッスンするポート」を指定
 Servers: FortiGate の FQDN
 ユーザ名:SSL-VPN 設定で設定した PKI ユーザ
 証明書: PKI ユーザ作成時に指定したクライアント証明書
 Single Sign On:任意
 Prompt User Credentials: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。

### 「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。

FortiGate-60F -	≡ Q.	
🙆 ダッシュボード 🔹 🔉	┃ 🕈 作成/インポート▼ 🛛 🖋	編集 📄 削除 💿 詳細の表示 🛓 ダウンロード 🛛 検索 🔍 🔍
	証明書	サブジェクト♥
🖺 ポリシー&オブジェクト 🔹 🔉	CSRの生成 ④	
🔒 セキュリティプロファイル ゝ	CA証明書	C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA256 2020 CA1
🖵 VPN 🔶	リモート	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = fortinet-ca2, emailAddress = support@for
💄 ユーザ&認証 🔹 ゝ	CRL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = fortinet-subca2001, emailAddress = supp
♥iFi&スイッチコントロー >	R Fortinet_CA_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress = support@fortine
>	🖸 ローカル CA 証明書 🤰	
	Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = FGT60FTK2109DDH8, emailAddress = su
	Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = Fortinet Untrusted CA, emailAddress = su
管理者フロファイル	🖸 ローカル証明書 15	
ファブリック管理	Fortinet_Wifi	C = US, ST = California, L = Sunnyvale, O = "Fortinet, Inc.", CN = auth-cert.fortinet.com
設定	Fortinet_GUI_Server	C = US, ST = California, L = Sunnyvale, O = Fortinet Ltd., OU = FortiGate, CN = FortiGate
HA	Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@fortioned = Support@Support@Fortioned = Support@Fortioned = Support@F
SNMP	Fortinet_Factory_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@for
差し替えメッセージ	Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@fortioned = Support@Support@Fortioned = Support@Fortioned = Support@F
FortiGuard	Fortinet_SSL_DSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@fortioned =
表示機能設定	Fortinet_SSL_DSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@for
証明書 🖒	Fortinet_SSL_ECDSA256	C=US,ST=California,L=Sunnyvale,O=Fortinet,OU=FortiGate,CN=FGT60FTK2109DDH8,emailAddress=support@for
🕼 セキュリティファブリック ゝ	Fortinet_SSL_ECDSA384	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@formula = Support@Fortical
回 ログ&レポート >	Fortinet_SSL_ECDSA521	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FGT60FTK2109DDH8, emailAddress = support@formula = Support@Support@Formula = Support@Formula = Support@Formula = Support@Formula = Support@Support@Formula = Support@Formula = S

### 「証明書をインポート」を選択します。

証明書の作成			×
	2	3	4
メソッドの選択	証明書の詳細	証明書の作成	レビュー
音 証明書の自動提供			
Let's EncryptとACMEプロトコルを使用 あります。	して証明書の作成とメンテナン	マスを自動化します。DDNSを有効にす	するか、ドメインを購入する必要が
Let's Encryptを使用			
■ 新しい証明書の生成			
FortiGateは当社の自己署名CAを使用し 信頼されたCAからのサーバ証明書を使	ノて証明書を生成することができ 用することを強く推奨します。	きます。 Fortinet_CA_SSL	
証明書の生成			
- 1 証明書をインポート			
既存の証明書をファイルアップロード	でインポートします。		
証明書をインポート			
	キャン	ンセル	

「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。

証明書の作成					:
	<b>⊘</b>	-2-		-3-	
メソ	ッドの選択	証明書の詳細		証明書の作成	レビュー
- 1 証明書をイン	ポート				
タイプ ローカ	ル証明書 PKCS12証明書	E明書			
証明書ファイル	fg60f-7.nrapki.com.crt				
キーファイル	fg60f-7.nrapki.com.key				
パスワード	••••		0		
パスワード確認	••••		0		
証明書名	fg60f-7.nrapki.com				
		作成	戻る	キャンセル	

### サーバ証明書がインポートされたことを確認します。

🐺 FortiGate-60F 🛛 👻	≡ Q	
🙃 ダッシュボード 🔹 🔉	◆ 作成/インポート・	編集   自 削除   ◎ 詳細の表示   ▲ ダウンロード   検索   Q
中 ネットワーク  ・	名前≑	サブジェクト⇔
💄 ポリシー&オブジェクト 🔹 🕨	🖸 リモートCA証明書 🕢	
🔒 セキュリティプロファイル ゝ	R Fortinet_Wifi_CA	C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA256 2020 CA1
묘 VPN ›	R Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = fortinet-ca2, emailAddress = support@for
💄 ユーザ& 認証 🔹 ゝ	Fortinet_Sub_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = fortinet-subca2001, emailAddress = supp
☆ WiFi&スイッチコントロー      、         、         、         、	R Fortinet_CA_Backup	$C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate \ Authority, CN = support, emailAddress = support \textcircled{o} fortinet, OU = Certificate \ Authority, CN = support, emailAddress = support \textcircled{o} fortinet, OU = Certificate \ Authority, CN = support, emailAddress = support \textcircled{o} fortinet, OU = Certificate \ Authority, CN = support, emailAddress = support \textcircled{o} fortinet, OU = Certificate \ Authority, CN = support, emailAddress = support \textcircled{o} fortinet, OU = Certificate \ Authority, CN = support, emailAddress = support \textcircled{o} fortinet, OU = Certificate \ Authority, CN = support, emailAddress = support \textcircled{o} fortinet, OU = Certificate \ Authority, CN = support, emailAddress = support \textcircled{o} fortinet, OU = Certificate \ Authority, CN = support, emailAddress = support \textcircled{o} fortinet, OU = Certificate \ Authority, CN = support, emailAddress = support \textcircled{o} fortinet, OU = Certificate \ fortinet, OU = Certificate fortinet, OU = Certificate fortinet, OU = Certificate fortinet, OU = Certificate fortinet, OU = $
A 3.7=1	🖸 ローカル CA 証明書 🥑	
	Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = FGT60FTK2109DDH8, emailAddress = su
管埋者	Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = Fortinet Untrusted CA, emailAddress = su
管理者プロファイル	🖸 ローカル証明書 16	
ファブリック管理	💀 fg60f-7.nrapki.com	C = JP, O = NipponRA, CN = fg60f-7.nrapki.com
設定	Fortinet_Wifi	C = US, ST = California, L = Sunnyvale, O = "Fortinet, Inc.", CN = auth-cert.fortinet.com
НА	Fortinet_GUI_Server	C = US, ST = California, L = Sunnyvale, O = Fortinet Ltd., OU = FortiGate, CN = FortiGate

## 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。