マルチトラスト設定ガイド

（FortiGate 編）

2024 年 9 月 24 日

Ver. 1.10

改訂履歴

版	日　付	内　容	備　考
Ver. 1.00	--	初版作成	--
Ver. 1.10	2024/09/24	CA3G2 の失効リスト配布ポイントの変更	

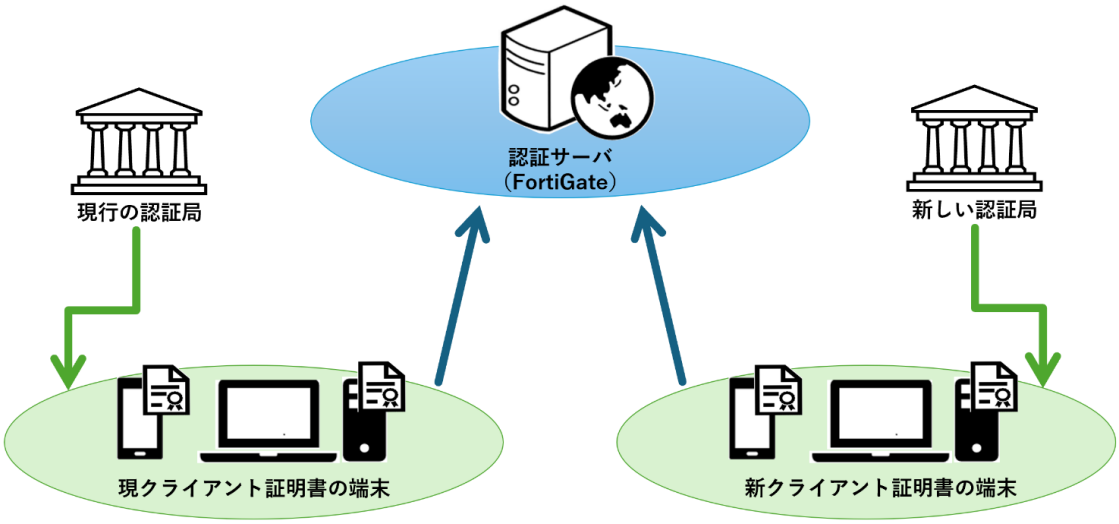
<目　次>

1. 概要

1.1. はじめに

本書は、NRA-PKI クライアント証明書の認証局（表 1）の世代交代（※1）に伴い、現行の認証局から発行したクライアント証明書と、新しい認証局から発行したクライアント証明書の両方を従来と同様にご利用頂くための FortiGate におけるマルチトラスト設定の手順を記載したものです。

【構成図】



【表 1 NRA-PKI の認証局】

	現行の認証局	新しい認証局
ルート認証局	Nippon RA Root Certification Authority	Nippon RA Root Certification Authority G2
中間認証局 CA3	Nippon RA Certification Authority 3	Nippon RA Certification Authority 3 G2
中間認証局 CA4	Nippon RA Certification Authority 4	Nippon RA Certification Authority 4 G2
中間認証局 CA5	Nippon RA Certification Authority 5	Nippon RA Certification Authority 5 G2

※1 現行のルート認証局および中間認証局の有効期限により新しい認証局への移行

1.2. 本書における注意事項

本書は既存のクライアント証明書認証に追加して、新しい認証局のクライアント証明書を認証する設定手順を記載しております。

詳しいクライアント証明書認証の設定手順については、FortiGate 設定ガイドをご参照ください。

また、中間認証局 CA3 以外をご利用の場合は、本書における「Nippon RA Certification Authority 3」および「CA3」という記載をご利用の中間認証局に置き換えてください。

ご利用の中間認証局の確認方法については、後記の Appendix1 を参照ください。

2. マルチトラストの設定手順

FortiGate における認証局世代交代に伴うマルチトラスト設定は以下の手順で行います。

2.1. 新しい認証局証明書のインポート

新しい認証局の証明書を FortiGate にインポートします。

2.2. 失効リスト（CRL）のインポート

新しい認証局から発行されるクライアント証明書の失効リスト（CRL）を設定します。

2.3. PKI ユーザの作成

新しい認証局から発行されるクライアント証明書で認証するためのユーザを新たに作成します。

2.1. 新しい認証局証明書のインポート

新しい認証局の証明書を FortiGate にインポートします。

(1) 新しい認証局のルート証明書および中間証明書を以下の URL よりダウンロードしてください。
使用する中間認証局の確認方法については、Appendix1 をご参照ください。

【新しい認証局の証明書】

■ルート認証局 G２（Nippon RA Root Certification Authority G2）
https://www.nrapki.jp/nrawp/cert/NipponRARootCertificationAuthorityG2.crt

■中間認証局 CA３ G２（Nippon RA Certification Authority 3 G2）
https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority3G2.crt

■中間認証局 CA４ G２（Nippon RA Certification Authority 4 G2）
https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority4G2.crt

(2) FortiGate の管理画面にログインし、「システム」-「証明書」-「作成/インポート」-「CA 証明書」とクリックします。

(3) 「ファイル」を選択し、「アップロード」からルート証明書を指定し OK をクリックします。

(4) 同手順にて中間証明書をインポートします。

(5) 新しい認証局の証明書がインポートされたことを確認してください。

2.2. 失効リスト（CRL）のインポート

新しい認証局の失効リストをインポートします、

(1) 新しい認証局の失効リスト（CRL）の配布ポイントは以下になります。

■新しい認証局の失効リスト（CRL）の配布ポイント

・中間認証局 CA３ G２（Nippon RA Certification Authority 3 G2）の失効リスト

http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority3G2/cdp.crl

・中間認証局 CA４ G２（Nippon RA Certification Authority 4 G2）の失効リスト

http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority4G2/cdp.crl

(2) 「システム」-「証明書」-「作成/インポート」-「CRL」とクリックします。

(3) 「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。

(4) CRL がインポートされたことを確認します。

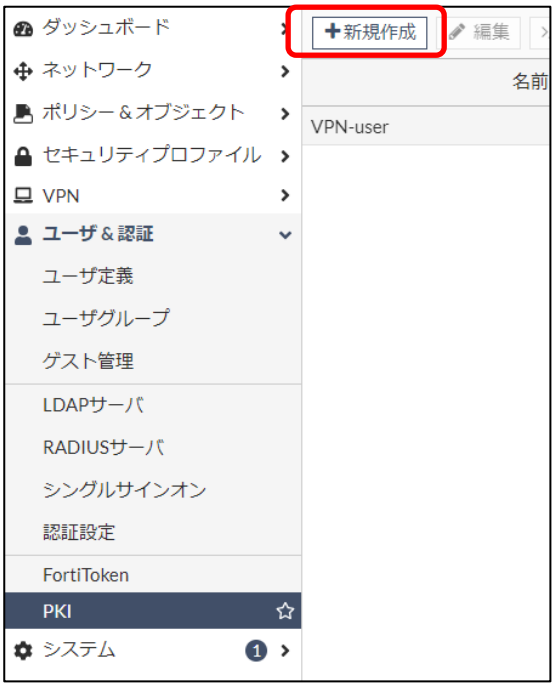
※OCSP レスポンダをご利用の場合は、CLI から以下コマンドを参考に中間 CA の値を新中間 CA の値に変更してください。

config vpn certificate ocsp-server
edit <ocsp 登録名>
set cert <新中間 CA の登録名>
end
exit

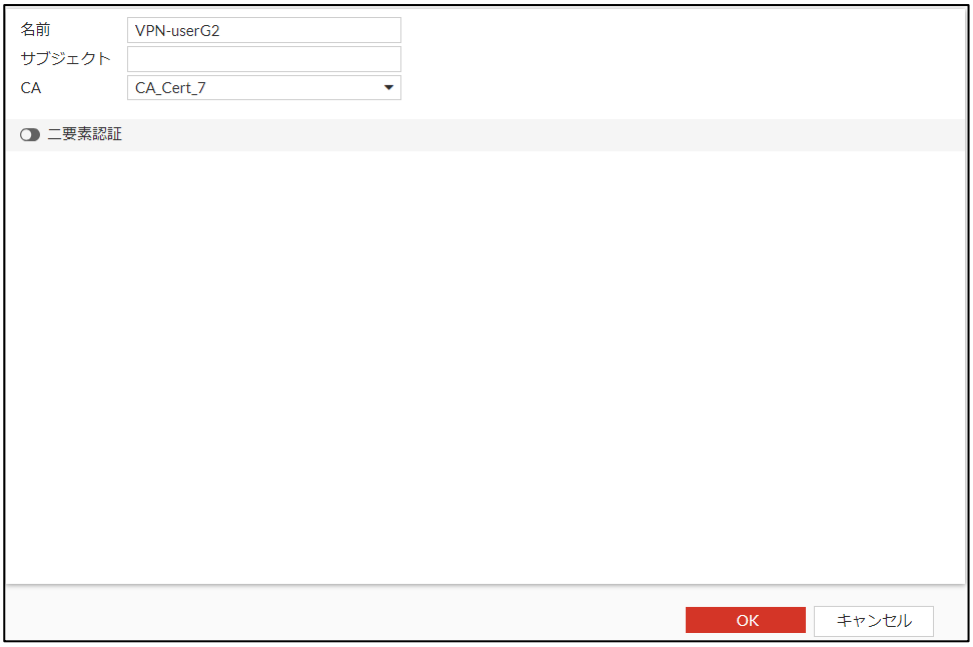
2.3. PKI ユーザの作成

既存の PKI ユーザとは別に新たに新しい認証局の証明書で認証するための PKI ユーザを作成します

(1) 「ユーザ&認証」-「PKI」-「新規作成」をクリックします。

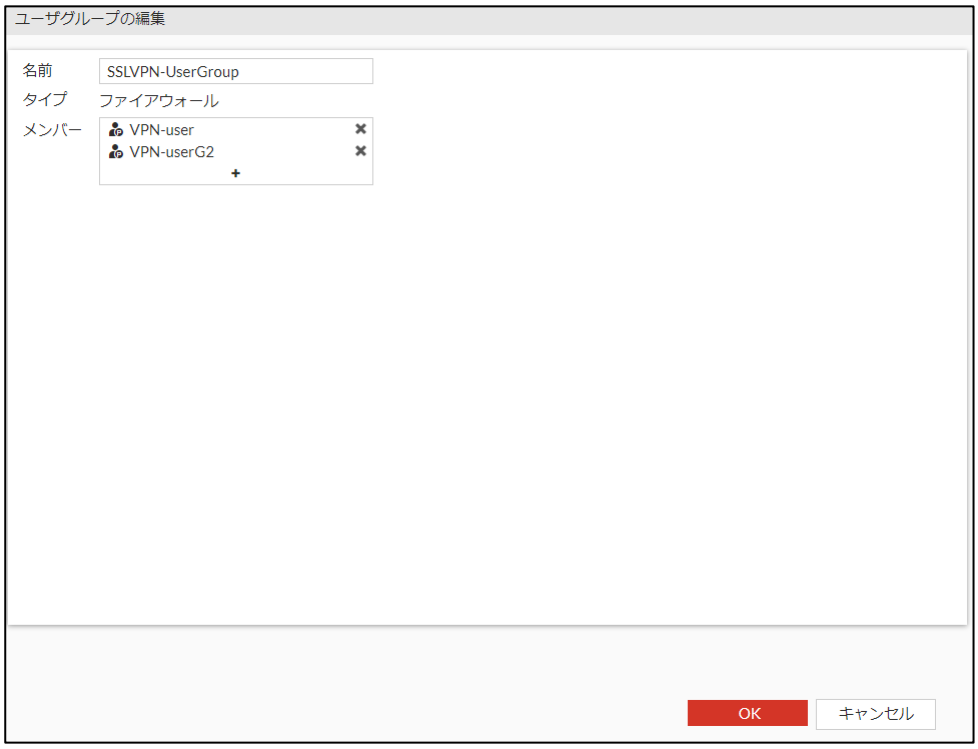


(2) 「名前」に任意の値を入力し、「CA」に手順 2-1 でインポートした新しい中間証明書を指定してください。その他の設定は既存ユーザの設定と合わせて「OK」をクリックしてください。



(3) 次に作成した新しい PKI ユーザを SSL-VPN を利用するグループに追加します。「ユーザ&デバイス」-「ユーザグループ」とクリックし、SSL-VPN を利用するグループを選択し編集をクリックします。

(4) メンバーに新しく作成した PKI ユーザを追加し「OK」をクリックします。



以上で設定は完了です。

3. Appendix1（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。サービス名の後の（CA4）等の表記がご利用いただいている中間認証局です。表記がなければ CA3 をご利用いただいております。