マルチトラスト設定ガイド

（Microsoft Entra CBA 編）

2025 年 1 月 22 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	2025/1/22	公開キー基盤(プレビュー)の説明追加	

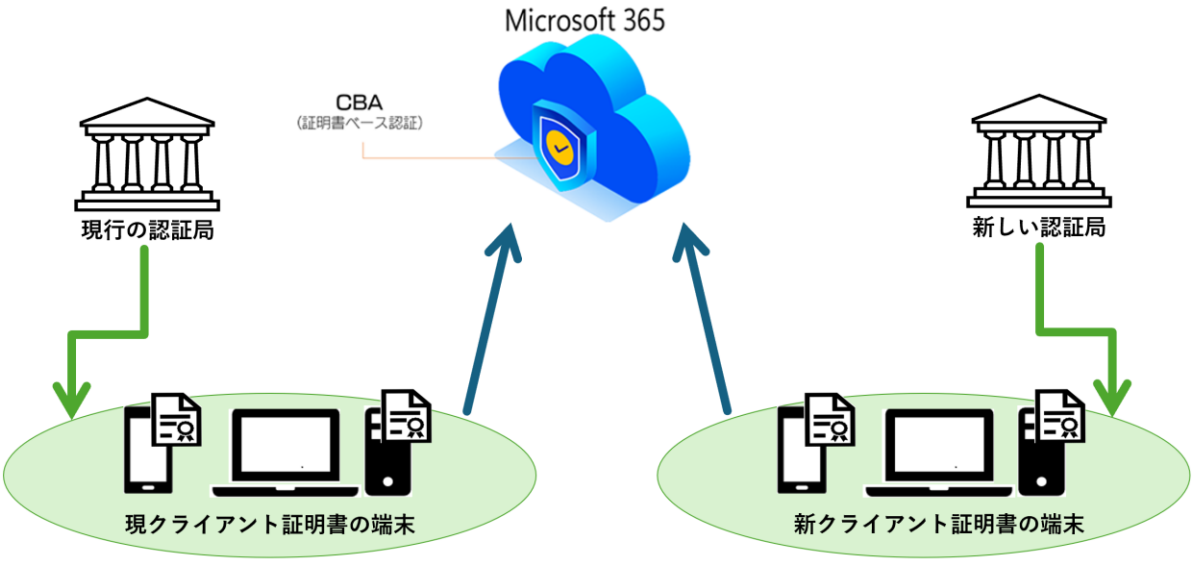
<目　次>

1. 概要

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 Microsoft Entra ID の証明書ベースの認証（CBA：Certificate-Based Authentication）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 CA6	Nippon RA Certification Authority 6	Nippon RA Certification Authority 6 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

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、Microsoft Entra CBA 用サービス向けマニュアルをご参照ください。

2. マルチトラストの設定手順

Apache 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アップロード

新しい認証局の証明書をアップロードします。

2.2. 証明書ベースの認証設定

新しい認証局から発行されたクライアント証明書の認証設定を行います。

2.1. 新しい認証局証明書のアップロード

「Microsoft Entra 管理センター」にて、新しい認証局の証明書をアップロードします。

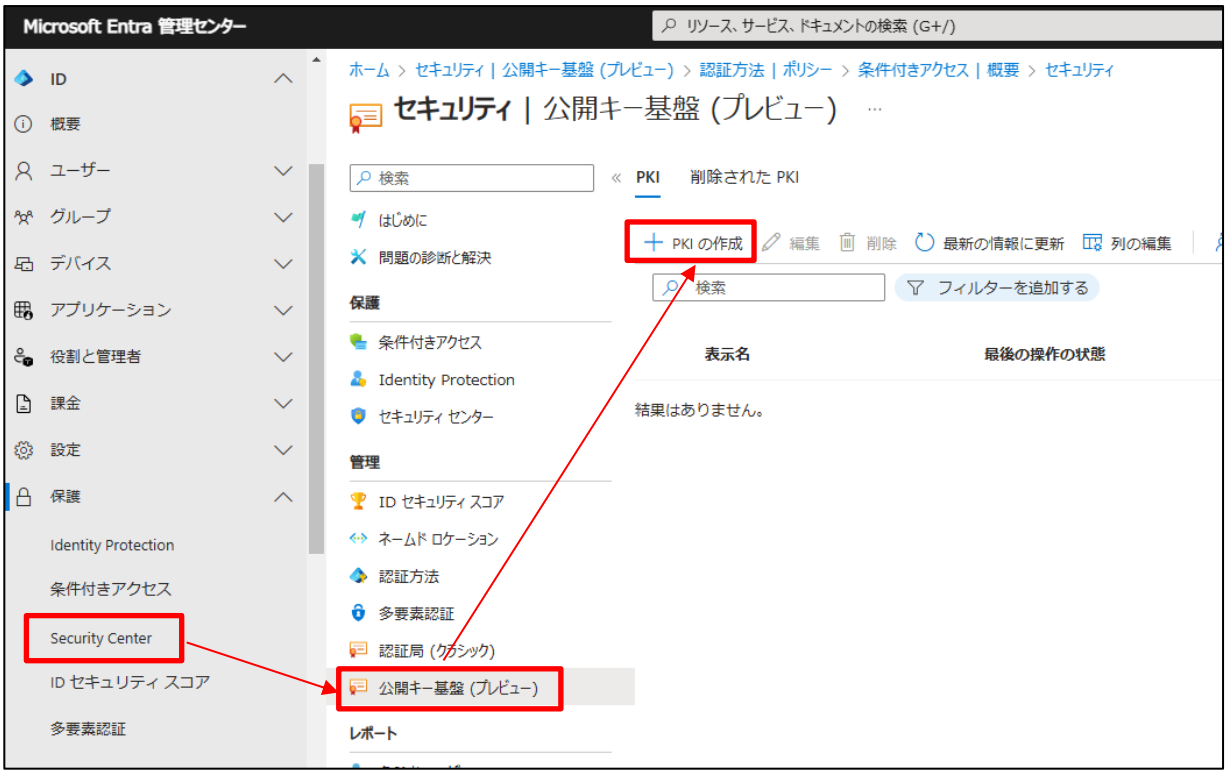
(1) 新しい認証局のルート証明書および中間証明書を取得してください。
以下の URL より対象の証明書をダウンロードしてください。

【新しい認証局の証明書】

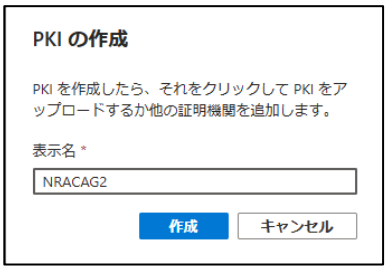
■ルート認証局 G２（Nippon RA Root Certification Authority G2）
https://www.nrapki.jp/nrawp/cert/NipponRARootCertificationAuthorityG2.cer

■中間認証局 CA６ G２（Nippon RA Certification Authority 6 G2）
https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority6G2.cer

(2) 「Microsoft Entra 管理センター」にアクセスし、左側メニューから「保護」-「Security Center」-「公開キー基盤(プレビュー)」-「PKI の作成」をクリックします。



(3) 表示名を入力する画面が表示されますので、任意の値を入力し作成をクリックします。



(4) 作成した PKI をクリックします。

(5) 「証明機関の追加」をクリックします。

(6) まず新ルート認証局証明書をアップロードします。「証明機関の追加」画面では以下を設定してください。

	設定項目	設定
1	証明書	NRA-PKI ルート認証局証明書 (ファイル名:NipponRARootCertificationAuthorityG2.cer)
2	この証明機関はルートですか?	はい
3	証明書失効リストの URL	【ルート認証局 G2 の失効リストの配布ポイント】を設定
4	差分証明書失効リストの URL	設定不要
5	発行者ヒントが有効になっていますか？	チェック

【ルート認証局 G2 の失効リストの配布ポイント】

http://mpkicrl.managedpki.ne.jp/mpki/NipponRARootCertificationAuthorityG2/cdp.crl

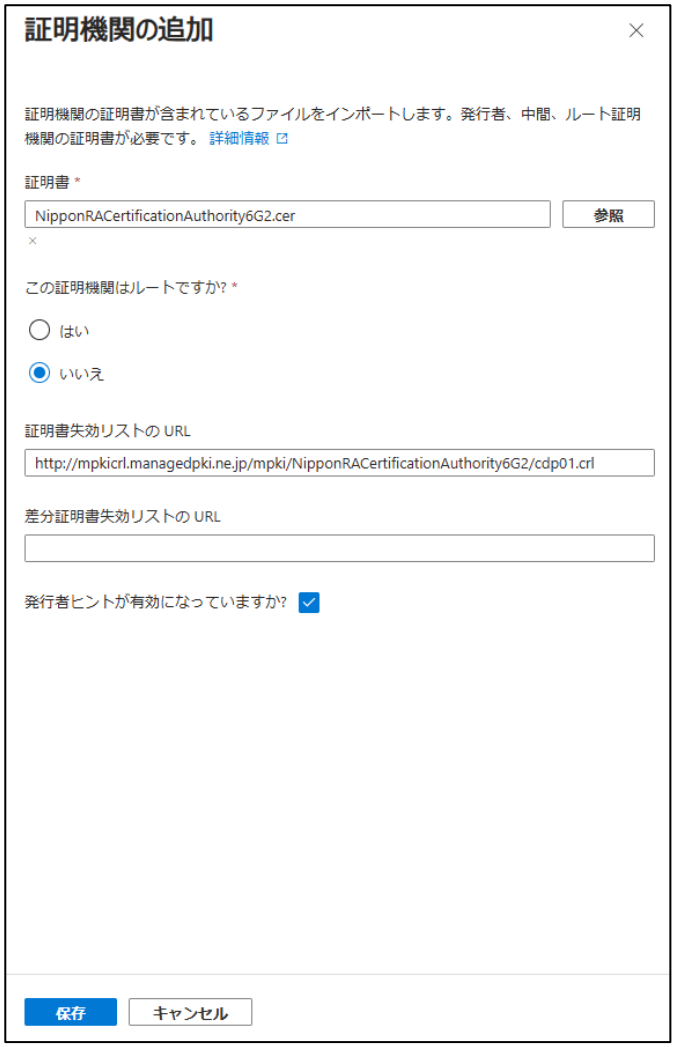
設定後、画面下部の「保存」ボタンをクリックしてください。

(7) 次に新中間認証局証明書をアップロードします。ルート認証局証明書のアップロード手順同様に、再度「証明機関の追加」画面を開き、以下を設定してください。

	設定項目	設定
1	証明書	NRA-PKI 中間認証局証明書 （ファイル名：NipponRACertificationAuthority6G2.cer）
2	この証明機関はルートですか?	いいえ
3	証明書失効リストの URL	【中間認証局 CA6 G2 の失効リストの配布ポイント】を設定
4	差分証明書失効リストの URL	設定不要
5	発行者ヒントが有効になっていますか？	チェック

【中間認証局 CA6 G2 の失効リストの配布ポイント】

http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority6G2/cdp01.crl



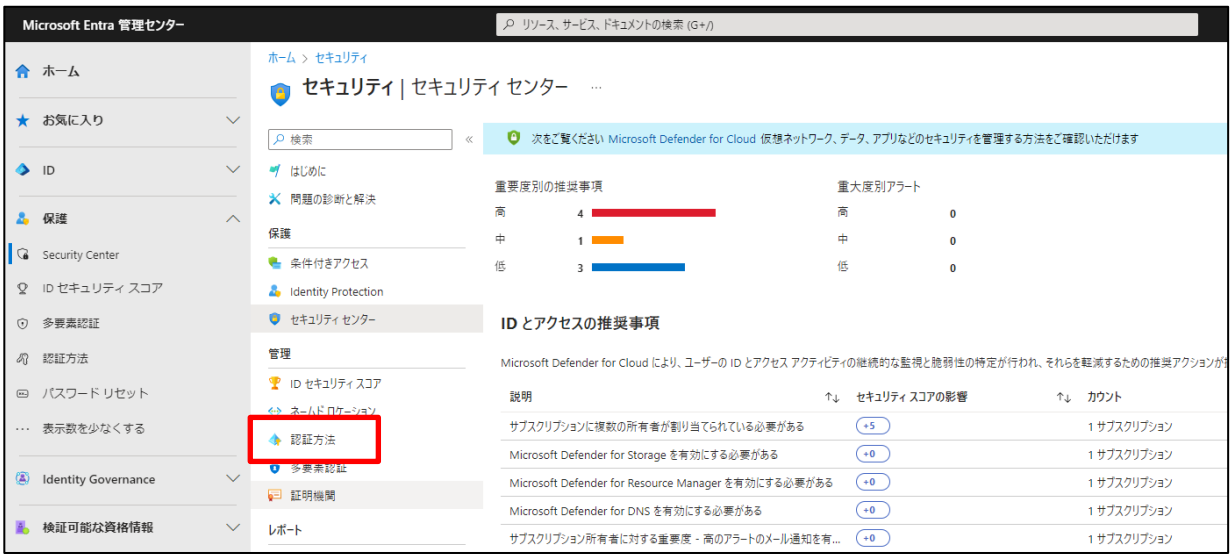
設定後、画面下部の「保存」ボタンをクリックしてください。

(8) 作成した PKI に、新しくアップロードした２つの認証局証明書が表示されていれば、認証局証明書のアップロードは完了です。

2.2. 証明書ベースの認証設定

新しい認証局から発行した証明書で認証するための設定を行います。

(1) 左側メニューから「保護」-「Security Center」-「認証方法」をクリックしてください。



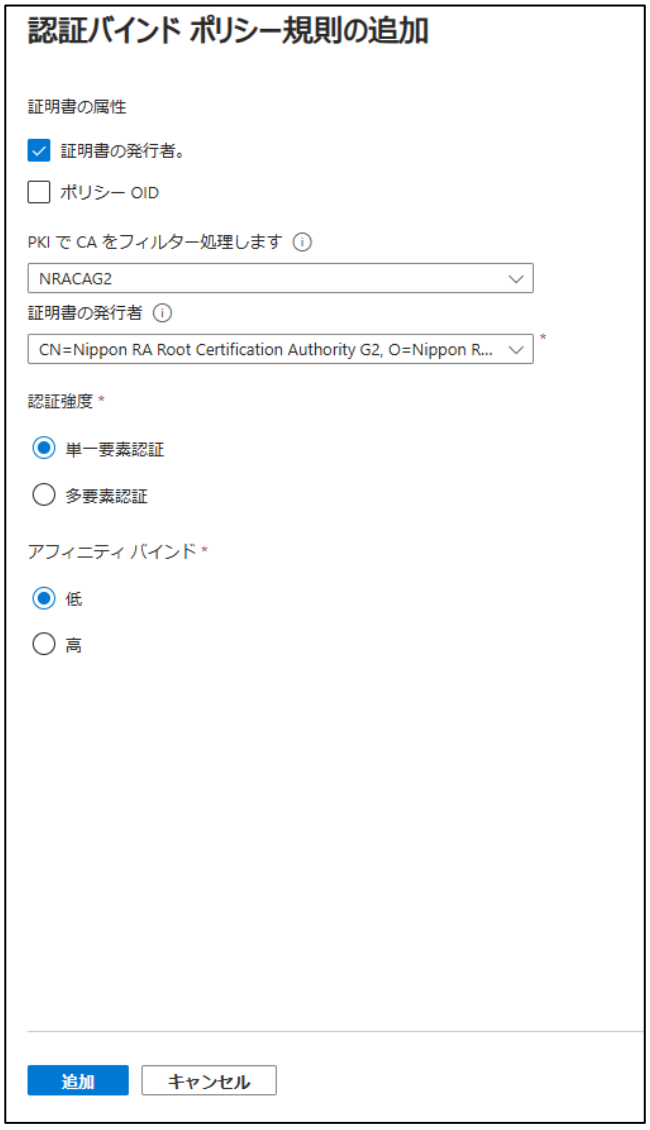
(2) 「認証方法 | ポリシー」画面が表示されますので「証明書ベースの認証」をクリックしてください。

(3)「証明書ベースの認証の設定」画面が表示されますので、「構成」タブをクリックしてください。

(4)「必須のアフィニティバインド」の下にある「規則の追加」をクリックします。右側に「認証バインドポリシー規則の追加」画面が表示されますので、先ほどアップロードした新しい認証局（証明書の発行者）を設定します。

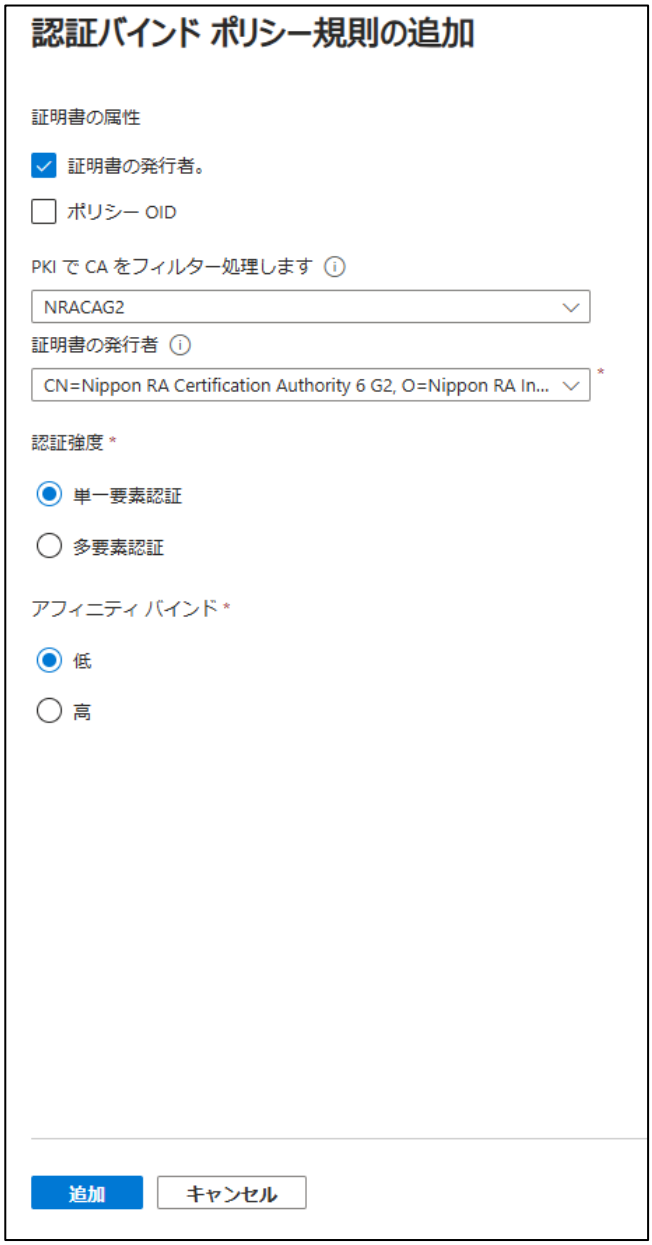
(5) まず新ルート認証局情報を設定します。以下を参考に設定してください。

	設定項目	設定
1	証明書の属性	証明書の発行者
2	PKI で CA をフィルター処理します	作成した PKI
3	証明書の発行者	CN=Nippon RA Root Certification Authority G2, …
4	認証強度	単一要素認証
5	アフィニティ バインド	低



(6) 次に新中間認証局情報を設定します。再度「規則の追加」をクリックして「認証バインド ポリシー規則の追加」画面を開き、以下を参考に設定してください。

	設定項目	設定
1	証明書の属性	証明書の発行者
2	PKI で CA をフィルター処理します	作成した PKI
3	証明書の発行者	CN=Nippon RA Certification Authority 6 G2, …
4	認証強度	単一要素認証
5	アフィニティ バインド	低



(7) 「証明書ベースの認証の設定」画面にて、追加した２つの認証局情報が設定されていることを確認して「保存」をクリックしてください。

以上でマルチトラストの設定は完了です。