

NRA

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>

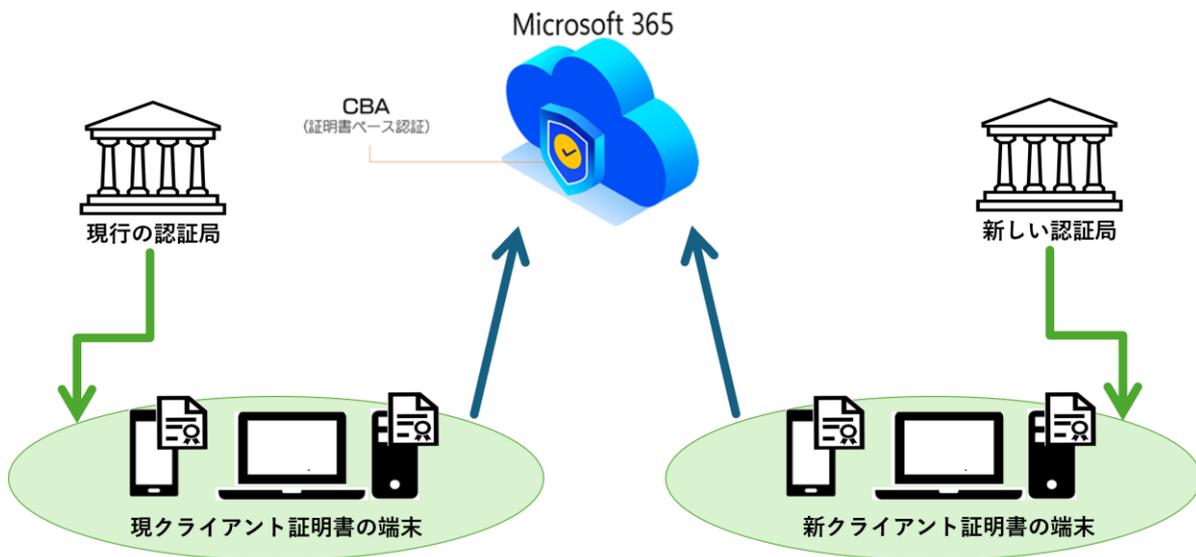
1. 概要	3
2. マルチトラストの設定手順.....	5
2.1. 新しい認証局証明書のアップロード	6
2.2. 証明書ベースの認証設定	11

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】

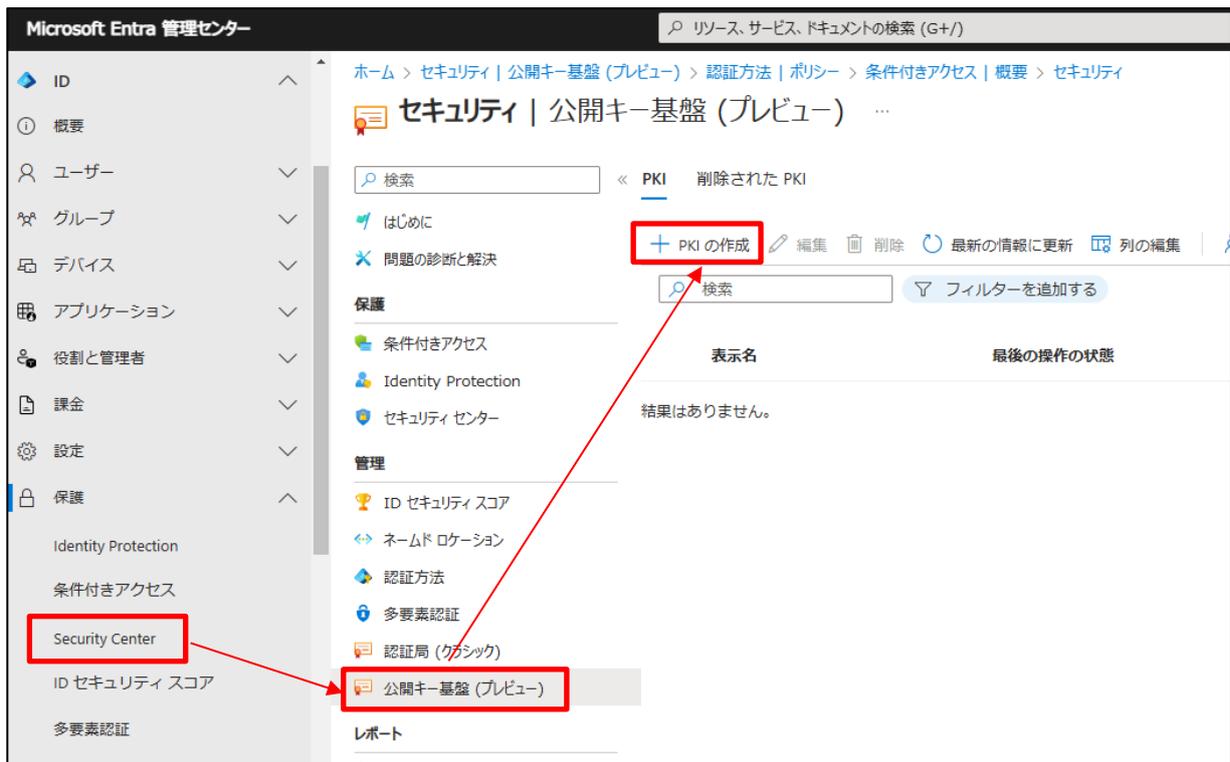
■ ルート認証局 G2 (Nippon RA Root Certification Authority G2)

<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。

PKI の作成

PKI を作成したら、それをクリックして PKI をアップロードするか他の証明機関を追加します。

表示名 *

(4) 作成した PKI をクリックします。

ホーム > セキュリティ

セキュリティ | 公開キー基盤 (プレビュー) ...

検索 << PKI 削除された PKI

はじめに

問題の診断と解決

保護

- 条件付きアクセス
- Identity Protection
- セキュリティ センター

管理

- ID セキュリティ スコア
- ネームド ロケーション

+ PKI の作成 編集 削除 最新の情報に更新 列の編集 フィードバックがある場合

検索 フィルターを追加する

	表示名	最後の操作の状態	状態の詳細
<input type="checkbox"/>	NRACAG2	成功	

(5) 「証明機関の追加」をクリックします。

ホーム > セキュリティ | 公開キー基盤 (プレビュー) >

NRACAG2 ...

証明機関

CA 削除された CA

↑ CBA PKI のアップロード + 証明機関の追加 編集 削除 最新の情報に更新 列の編集 フィードバックがある場合

検索 フィルターを追加する

<input type="checkbox"/>	名前	有効期限切れ	ルート証明書	発行者ヒント
結果はありません。				

(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>

証明機関の追加

証明機関の証明書が含まれているファイルをインポートします。発行者、中間、ルート証明機関の証明書が必要です。 [詳細情報](#)

証明書 *

NipponRARootCertificationAuthorityG2.cer

この証明機関はルートですか? *

はい

いいえ

証明書失効リストの URL

差分証明書失効リストの URL

発行者ヒントが有効になっていますか?

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>

証明機関の追加 ×

証明機関の証明書が含まれているファイルをインポートします。発行者、中間、ルート証明機関の証明書が必要です。 [詳細情報](#)

証明書 *

NipponRACertificationAuthority6G2.cer

×

この証明機関はルートですか? *

はい

いいえ

証明書失効リストの URL

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

差分証明書失効リストの URL

発行者ヒントが有効になっていますか?

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。

NRACAG2 ...

証明機関

CA 削除された CA

↑ CBA PKI のアップロード + 証明機関の追加 編集 削除 最新の情報に更新 列の編集 フィードバックがある場合

検索 フィルターを追加する

<input type="checkbox"/>	名前	有効期限切れ	ルート証明書	発行者ヒントが有効	拇印
<input type="checkbox"/>	CN=Nippon RA Root Certification A...	✔ いいえ	はい	はい	C844DEB386B
<input type="checkbox"/>	CN=Nippon RA Certification Authori...	✔ いいえ	いいえ	はい	529FD1ADEE8

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。

The screenshot shows the Microsoft Entra Security Center interface. The left-hand navigation pane is expanded to '保護' (Protection), and the '認証方法' (Authentication Methods) option is highlighted with a red box. The main content area displays the 'セキュリティセンター' (Security Center) dashboard, including a search bar, a notification banner for Microsoft Defender for Cloud, and several security metrics and recommendations.

(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。

The screenshot shows the '認証方法 | ポリシー' (Authentication Methods | Policies) page in Microsoft Entra. The left-hand navigation pane is expanded to '認証方法' (Authentication Methods), and the '証明書ベースの認証' (Certificate-based authentication) option is highlighted with a red box. The main content area displays the policy configuration page, including a search bar, a notification banner, and a table of authentication methods.

メソッド	ターゲット	有効
FIDO2 セキュリティキー		いいえ
Microsoft Authenticator		いいえ
SMS		いいえ
一時アクセスパス		いいえ
サードパーティ製のソフトウェア OATH トークン		いいえ
音声通話		いいえ
メール OTP		はい
証明書ベースの認証		いいえ

(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

認証バインド ポリシー規則の追加

証明書の属性

証明書の発行者。

ポリシー OID

PKI で CA をフィルター処理します ①

NRACAG2 ▼

証明書の発行者 ①

CN=Nippon RA Root Certification Authority G2, O=Nippon R... ▼ *

認証強度 *

単一要素認証

多要素認証

アフィニティ バインド *

低

高

(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

認証バインド ポリシー規則の追加

証明書の属性

証明書の発行者。
 ポリシー OID

PKI で CA をフィルター処理します ⓘ
NRACAG2

証明書の発行者 ⓘ
CN=Nippon RA Certification Authority 6 G2, O=Nippon RA In... *

認証強度 *

単一要素認証
 多要素認証

アフィニティ バインド *

低
 高

(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。

証明書の発行者。	ポリシー OID	認証強度	アフィニティ バインド
CN=Nippon RA Certification Authority 6, O=Nippon RA I...	N/A	単一要素	低
CN=Nippon RA Root Certification Authority, O=Nippon R...	N/A	単一要素	低
CN=Nippon RA Root Certification Authority G2, O=Nippo...	N/A	単一要素	低
CN=Nippon RA Certification Authority 6 G2, O=Nippon ...	N/A	単一要素	低

ユーザー名バインド

クラウドのユーザー属性のいずれかとバインドする X.509 証明書フィールドを 1 つ選択します。 [詳細情報](#)

証明書フィールド	アフィニティ バインド	ユーザー属性
RFC822Name	低	userPrincipalName
PrincipalName	低	userPrincipalName

以上でマルチトラストの設定は完了です。