# 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.		初版作成	
1.00			
Ver.	2025/1/22	公開キー基盤(プレビュー)の説明追加	
1.10	2025/1/22		

#### <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	

#### 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。

Microsoft 365

#### 【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。

М	icrosoft Entra 管理センター				
4	ID	^ *	ホーム > セキュリティ   公開キー基盤 (プレ	レビュー) > 認証方法 ポリシー > 条件付きアクセス 概要 > セキュリティ	
i	概要		🔁 セキュリティ   公開キ-	一基盤 (プレビュー)	
8	ユーザー	$\sim$	₽検索≪	PKI 削除された PKI	
የአየ	グループ	$\sim$	🌱 はじめに		
圮	デバイス	$\sim$	🗙 問題の診断と解決	+ PKIの作成 / 編集 凹 削除 ) 最新の情報に更新 口 列の編集	8
₩ <b>6</b>	アプリケーション	$\sim$	保護	● 検索 マ フィルターを追加する	
ී	役割と管理者	$\sim$	🍨 条件付きアクセス	表示名 最後の操作の状態	
	課金	~	Identity Protection     セキュリティ センター	/ 結果はありません。	
	設定	$\sim$	管理		
Α	保護	^	🏆 ID לדבוודי גבוד		
	Identity Protection		🖘 ネームド ロケーション		
	条件付きアクセス		🔷 認証方法		
ſ	Security Center		多要素認証		
Ľ			▶ 認証局 (クラシック)		
			₩1 公開キー基盤 (JVビュー)		
	<b>多</b> 要素認証		レポート		

(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 *
NRACAG2
作成キャンセル

(4) 作成した PKI をクリックします。

ホーム > セキュリティ	ホーム > セキュリティ					
🔁 セキュリティ   公開キ	📻 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	🕂 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			
保護	▶ 検索	▽ フィルターを追加する				
💺 条件付きアクセス	表示名	最後の操作の状態	状能の詳細			
Identity Protection	342514	PRESCOTINE FOR THE AREA	TO CONSTITUTE			
<ul> <li>セキュリティセンター</li> </ul>	NRACAG2	🕑 成功				
管理						
🏆 ID セキュリティ スコア						
↔ ネームド ロケーション						

(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) >		
<b>NRACAG2</b> … 証明機関			
CA 削除された CA			
↑ СВА РКІ 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
₽ 検索	▽ フィルターを追加する		
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	チェック	
	ますか?		

【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 ×
証明機關の証明書が含まれているファイルをインボートします。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 <sup>[2]</sup>
証明書 *       NipponRARootCertificationAuthorityG2.cer     參照
この証明機關はルートですか? *
<ul> <li>はい</li> <li>いいえ</li> </ul>
証明書失効リストの URL http://mpkicd.managedpki.ne.ip/mpki/NipponRABootCertificationAuthorityG2/cdp.cd
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? 🗸
保存 キャンセル

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	チェック
	ますか?	

【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ボートします。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 C
証明書 *
NipponRACertificationAuthority6G2.cer     参照       ×
この証明機闘はルートですか?*
<ul> <li>いいえ</li> </ul>
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? 🧹
保存 キャンセル

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						
↑ СВА РКІ のアップロード + 証5	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						
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		
CN=Nippon RA Root Certifica	ation A 🥑 いいえ	はい	はい	C844DEB386B		
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。

Microsoft Entra 管理センター				
↑ ホーム	<ul> <li>ホ-ム &gt; セキュリティ</li> <li>         セキュリティ   セキュリ     </li> </ul>	ティ センター		
★ お気に入り	✓	🤨 次をご覧ください Microsoft Defender for Cloud 仮想ネット!	フーク、データ、アプリなどのセキュリティを管理する	5方法をご確認いただけます
ID	<ul> <li>ダ はじめに</li> <li>※ 問題の診断と解決</li> </ul>	重要度別の推奨事項	重大度別アラート	
▲ 保護	(保護	商 4	商 0	
G Security Center		中 1 <b>—</b>	中 0	
♀ ID セキュリティスコア	ldentity Protection	10 3	100	
<ul> <li>         · 多要素認証     </li> </ul>	🌻 セキュリティ センター	IDとアクセスの推奨事項		
47 認証方法	管理	Microsoft Defender for Cloud により、ユーザーの ID とアクセス アクラ	ティビティの継続的な監視と脆弱性の特定が行	われ、それらを軽減するための推奨アクションが
─ パスワードリセット	♀ ID セキュリティスコア ◆ ネームドロケーション	説明	↑↓ セキュリティ スコアの影響	↑↓ カウント
・・・ 表示数を少なくする		サブスクリプションに複数の所有者が割り当てられている必要がある	+5	1 サブスクリプション
	■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	Microsoft Defender for Storage を有効にする必要がある	+0	1 サブスクリプション
Identity Governance	▶ 証明機関	Microsoft Defender for Resource Manager を有効にする必要か	「ある +0	1 サブスクリプション
▲ 14元司台小次19/注和		Microsoft Defender for DNS を有効にする必要がある	+0	1 サブスクリプション
一 (実証り貼/み貸借) 自我	<ul><li>ベート</li></ul>	サブスクリプション所有者に対する重要度 - 高のアラートのメール通知	を有 (+0)	1 サブスクリプション

(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。

Ν	Aicrosoft Entra 管理センター				ドキュメントの検索 (G+/)	
<b>^</b>	- <b>л</b> -А		ホーム > ▲ 認証方法   ポリシー			
*	お気に入り	$\sim$	日本RA株式会社 - Azure AD セキュリティ ク 検索 《	🔗 フィードバックがま	55場合	
۵	ID	$\sim$	管理	このポリシーを使用して	- 、ユーザーが登録して使用できる認証方法を構成します。ユーザーが方法のスコープ内である場合は、それを認証とバスワードのリセットに使	ミ用できます (一
<b>4</b> G	<b>保護</b> Security Center	^	<ul> <li>◆ ポリシー</li> <li>◆ パスワード保護</li> <li>▲ 登録キャンペーン</li> </ul>	移行の管理	2024 年 9 月 30 日に多要素認証およびセルフサービス パスワード リセットのレガン ポリシーは廃止され、すべての認証方法を認証方; は、2のコントロールを使用します。 詳細情報 移行の管理	法ポリシーによっ
₽ Ω	ID セキュリティ スコア		<ul> <li>認証強度</li> <li>設定</li> </ul>	メソッド	ターダット	有効
• 47	認証方法		監視 	FIDO2 セキュリティ 의 Microsoft Authent	i= icator	いいえ いいえ
	パスワードリセット		■ ユーザー登録の詳細	SMS 一時アクセス パス		いいえ いいえ
	- 衣示説で少心く 9 つ		登録とりセットのイベント   ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	サード バーティ製のソ	7トウェア OATH トークン	いいえ
۲	Identity Governance	$\sim$	₩ T指接FEO相未	音声通話		いいえ
	<b>输证可能</b> 疗资格结据	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	1			はい
	アクセス許可の管理			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。

Microsof	t Entra 管理センター		𝒫 リソース、サービス、ドキュメントの検索 (G+/)	
Contraction (1995) Contraction (1995)	~	~	ホーム > 認証方法   ポリシー > <b> 証明書ベースの認証の設定</b>	
La 課金		$\sim$		
(2) 設定		$\sim$		
合 保護		$\sim$	Microsoft Entra CBA は、今後の新機能をサポートするために、certauth エンドポイントを certauth.login.microsoftonline.com から t {tenantId}.certauth. る場合は、正規表現 [*] を導入し、(*.]certauth.login.microsoftonline.com の下にある任意の名前と一致できるようにすることで certauth エンドポイントの TLS	.login.mi 5 検査を無
🕃 Identit	y Governance	$\sim$		
ତ୍ତି Externa	al Identities	~	証明書ペースの認証は、認証に x.509 証明書とエンタープライズ公開キー基盤 (PKI) を使用するパスワードレスでファイシングに進い認証方法です。詳細情報。	
೫ ユーザ	ー エクスペリエンス	$\sim$	有効化およびターグット構成	
G 1.17	リッド管理	$\sim$		
≫ 監視と	正常性	$\sim$	<b>含める</b> 除外	
··· 表示数	を少なくする		ターゲット 🔿 すべてのユーザー 💿 グループの選択	
		- 1	グループの追加	
🎝 保護		^	名前 種類	
Identit	y Protection		CBAtest グループ	
🕞 条件付	きアクセス			
G Securit	y Center			

(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。

認証バインド		
認証バインド ポリシーは、証明書ベースの	認証方法ポリシーの強度を単一要素または多要素、低アフィニティまたは高アフィニテ	ティとするのかの判断に役立ちます。既定の設定を特殊な規則でオーバ
保護レベル ①	<ul> <li>单一要素認証</li> <li>多要素認証</li> </ul>	
必須のアフィニティバインド ①	<ul> <li>● 低</li> <li>○ 高</li> </ul>	
十規則の追加		511 877 244 min
証明書の発行者。		認証为見受
CN=Nippon RA Certification Aut	hority 6, O=Nippon RA I… N/A	単一要素
CN=Nippon RA Root Certificatio	n Authority, O=Nippon R… N/A	単一要素
ユー <b>ザー名バインド</b> クラウドのコーザー屎性のいずわかとバイン	ドする 2 500 証明書フィールドを 1 つ選択します。 詳細情報	

(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(i)
NRACAG2 V
証明書の発行者()
CN=Nippon RA Root Certification Authority G2, O=Nippon R $\checkmark$
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
追加キャンセル

(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 V
証明書の発行者()
CN=Nippon RA Certification Authority 6 G2, O=Nippon RA In $\checkmark$ *
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
追加キャンセル

(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。

+ 規則の追加			
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
CN=Nippon RA Certification Authority	y 6, O=Nippon RA I… N/A	単一要素	低
CN=Nippon RA Root Certification Aut	hority, O=Nippon R… N/A	単一要素	低
CN=Nippon RA Root Certification Aut	hority G2, O=Nippo… N/A	単一要素	低
CN=Nippon RA Certification Authority	y 6 G2, O=Nippon ··· N/A	単一要素	低
ユーサー名ハイント 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 つ違択します。 詳細情報		
ユーサーモルイフト クラウドのユーザー属性のいずれかとバインドする (二十 規則の追加) 耳田豊フィールド	X.509 証明書フィールドを1つ違択します。 詳細清報 アフィーティ バインド		┐_+f-冨性:
ユーフー 石ハイント クラウドのユーザー属性のいずれかとバインドする (十規則の追加) 証明書フィールド BECS222Name	X.509 証明書フィールドを 1 つ道択します。 詳細情報 アフィニティ バインド		ユーザー属性
<u>ユーフースハイノド</u> クラウドのユーザー属性のいずれかとパインドする <u>+ 規則の追加</u> 証明書フィールド RFC822Name PrincipalName	X.509 証明書フィールドを 1 つ違択します。 詳細情報 アフィニティ バインド 低 任		ユーザー属性 userPrincipalName userPrincipalName
<u>ユーフースハイノド</u> クラウドのユーザー属性のいずれかとパインドする <u>+規則の追加</u> 証明書フィールド RFC822Name PrincipalName	X.509 証明書フィールドを 1 つ違択します。 詳細情報 アフィニティ バインド 低 低		ユーザー属性 userPrincipalName userPrincipalName
ユーフーオンハファ クラウドのユーザー属性のいずれかとパインドする (十 規則の追加) 証明書フィールド RFC822Name PrincipalName	X.509 証明書フィールドを 1 つ違択します。 詳細清報 アフィニティ バインド 低 低		ユーザー属性 userPrincipalName userPrincipalName
ユーフーをスパインド クラウドのユーザー属性のいずれかとパインドする (十 規則の追加) 証明書フィールド RFC822Name PrincipalName	X.509 証明書フィールドを 1 つ違択します。 詳細情報 アフィニティ バインド 低 低		ユーザー属性 userPrincipalName userPrincipalName
<u>ユーフータノイフト</u> クラウドのユーザー属性のいずれかとバインドする <u>+規則の追加</u> 証明書フィールド RFC822Name PrincipalName	X.509 証明書フィールドを 1 つ違択します。 詳細情報 アフィニティ バインド 低 低		ユーザー属性 userPrincipalName userPrincipalName

以上でマルチトラストの設定は完了です。