NRA

Microsoft Entra CBA 設定ガイド

(クライアント証明書認証編)

2025年01月22日

Ver. 2.00

改訂履歴

版	日付	内容	備考
Ver.	2022/10/10	初版	
1.00	2023/10/10		
Ver.	2024/02/01	アフィニティバインドの説明追加	
1.10	2024/03/01		
Ver.	2024/00/19	CRL の検証、発行者ヒントの説明追加	
1.20	2024/09/10		
Vor		ルート、中間証明書および CRL を新認証局	
	2025/1/22	(G2)に変更	
2.00		公開キー基盤(プレビュー)の説明追加	

<目 次>

1. 概要	3
2. 事前準備	4
3. 設定手順	5
3.1. 認証局証明書のアップロード	6
3.2. 証明書ベースの認証設定	11
4. Appendix1(Windows PC での認証手順)	20

1. 概要

本書では弊社クライアント証明書を用いた Microsoft Entra ID(旧称 Azure AD)の証明書ベースの認証 (CBA: Certificate-Based Authentication)の設定方法を説明致します。

説明範囲としては Microsoft Entra CBA で証明書のみを使用した「単一要素認証」の設定になりますので、その他の設定についての詳細は Microsoft 社が提供している公式ドキュメントをご確認ください。

2. 事前準備

Microsoft Entra CBA の設定をするにあたり以下の点をご用意ください。

・認証ポリシー管理者の権限を持つ Microsoft アカウント

設定は「Microsoft Entra 管理センター(URL: <u>https://entra.microsoft.com/</u>)」にて行います。

「Microsoft Entra 管理センター」へは、上記アカウントにてログインする必要があります。

・NRA-PKI ルート認証局証明書(G2) (ファイル名: NipponRARootCertificationAuthorityG2.cer)
 ・NRA-PKI 中間認証局証明書(CA6 G2) (ファイル名: NipponRACertificationAuthority6G2.cer)
 上記 2 つの証明書については、レポジトリに公開されていますので以下より取得してください。

レポジトリ URL: https://www.nrapki.jp/client-certificate/repository-cba/

【注意事項】

クライアント証明書は、必ず中間認証局(CA6 G2)から発行されたものをお使いください。 中間認証局(CA6 G2)以外から発行されたクライアント証明書をご利用された場合、弊社では動作 保証できませんのであらかじめご了承ください。

現在、中間認証局(CA6 G2)以外から発行されたクライアント証明書をご利用のお客様で、 Microsoft Entra CBA でのご利用をご希望の場合は弊社サポート窓口(<u>support@nrapki.jp</u>)迄ご連絡 ください。

3. 設定手順

Microsoft Entra CBA の設定は「Microsoft Entra 管理センター」から以下の2ステップで行います。

- 3.2. 証明書ベースの認証設定......11

Microsoft Entra CBA の認証設定を行います

3.1. 認証局証明書のアップロード

Microsoft Entra CBA において NRA-PKI 中間認証局(CA6 G2)から発行されたクライアント証明書のみ に認証を制限するために、NRA-PKI 中間認証局(CA6 G2)と NRA-PKI ルート認証局証明書をアップロー ドします。アップロードした証明書は次項「証明書ベースの認証設定」で使用します。

- 「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。
 - (「Security Center」が表示されない場合は、「表示数を増やす」をクリック後にご確認ください)



② 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

③ 作成した PKI をクリックします。

ホーム > セキュリティ			
肩 セキュリティ 公開キ	ニー基盤 (プレビュー)		
	< 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	状態の詳細
aligned Identity Protection			
🟮 セキュリティ センター	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			

④ 「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	幾関の追加 🖉 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	7 フィルターを追加する		
〇〇名前	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。			

⑤ まず「NRA-PKI ルート認証局証明書(ファイル名: NipponRARootCertificationAuthorityG2.cer)」 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 12
証明書。
NipponRARootCertificationAuthorityG2.cer 参照
この証明機関はルートですか? *
O winz
証明書失効リストの URL
http://mpkicrl.managedpki.ne.jp/mpki/NipponRARootCertificationAuthorityG2/cdp.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設定を完了してください。

 ⑥ 次に「NRA-PKI 中間認証局証明書(ファイル名: NipponRACertificationAuthority6G2.cer)」をアッ プロードします。NRA-PKI 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」 画面を開いてください。

「証明書ファイルのアップロード」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 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 参照 ×
この証明機関はルートですか?*
(141)
 دردی
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設定を完了してください。

⑦ 作成した PKI に、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終了です。

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							
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 Certification	n A 🕑 いいえ	はい	はい	C844DEB386B				
CN=Nippon RA Certification Aut	hori 🕑 いいえ	いいえ	はい	529FD1ADEE8				

3.2. 証明書ベースの認証設定

Microsoft Entra CBA において認証するユーザと証明書の設定を行います。

【補足】

本項では例として「TestGroup」というグループに対して証明書ベースの認証設定を行います。設定後「TestGroup」に属するユーザ「testuser001@nrapki.jp」が NRA-PKI クライアント証明書で Microsoft Entra ID に認証する手順は次項で説明します。

① 「Microsoft Entra 管理センター」の左側メニュー「保護」-「Security Center」-「認証方法」をクリ ックしてください。

N	licrosoft Entra 管理センター		クリソース、サービス、ドキュメントの検索 (G+/)				
\$	ホーム	^ѫ ーム > セŧュリティ () セキュリティ セキュリテ	ィセンター				
*	お気に入り 🗸 🗸		② 次をご覧ください Microsoft Defender for Cloud 仮想ネットワ	ーク、テ	"ータ、アプリなどのセキュリティを管理する方法	をご確言	忍いただけます
۵	ID ~	♥ はじめに	重要度別の推奨事項	Ī	[大度別アラート		
2,	保護		商 4	商	ī 0		
G	Security Center	休護 	⊕ 1 —	+ ~	0		
Q	ID セキュリティ スコア	HITEFTEX Identity Protection	低 3	1世	÷ 0		
\odot	多要素認証	🟮 セキュリティ センター	ID とアクセスの推奨事項				
43	認証方法	管理 	Microsoft Defender for Cloud により、ユーザーの ID とアクセス アクテ	ายังา	の継続的な監視と脆弱性の特定が行われ、	それらき	*軽減するための推奨アクションが持
	パスワード リセット		説明	\uparrow_{\downarrow}	セキュリティ スコアの影響	\uparrow_{\downarrow}	カウント
	表示数を少なくする	↔ ⇒-Δト U/-ジョノ	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
		→ 認証力法	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
۲	Identity Governance \lor	▶ ジジェ 部 Ш	Microsoft Defender for Resource Manager を有効にする必要が	ある	+0		1 サブスクリプション
	体就可能的次体结和		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
-	快証り能/み見恰旧教 >	レホート	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な	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。

Microsoft Entra 管理センター	-		₽ リソース、サービス	、ドキュメントの検索 (G+/)	
^ ホ ーム		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 の 検索 《	🔗 フィードバックが	ある場合	
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ブ内である場合は、それを認証とバスワードのリセット	トに使用できます (-
<mark>▲</mark> 保護	^	 ホリシー パスワード保護 	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 バスワード リセットのレガシ ポリシーは廃止され、すべての認証方法を認 は、このコントロールを使用します。詳細情報	証方法ポリシーによ
G Security Center		🔒 登録キャンペーン		移行の管理	
♀ ID セキュリティ スコア		 認証強度 設定 	メソッド	ターゲット	有効
 ⑦ 多要素認証 		影相	FIDO2 セキュリティ	+-	いいえ
<i>4</i> ? 認証方法		<u>血に</u> ダインディビティ	Microsoft Authen	ıticator	いいえ
∞ パスワードリセット		ユーザー登録の詳細	SMS		いいえ
・・・ 表示数を少なくする		■ 登録とリセットのイベント	一時アクセスパス		いいえ
			サード パーティ製のン	ילאלי OATH トークン	いいえ
Identity Governance	\sim		音声通話		いいえ
			Х-Л/ ОТР		はい
検証可能な資格情報	\checkmark		証明書ベースの認識	Ē	いいえ
クセス許可の管理					

「証明書ベースの認証の設定」画面が表示されます。

Microsoft Entra 管理センター	ノ リソース、サービス、ドキュメントの検索 (G+/)
↑ ホーム	 ホーム > 認証方法 ポリシー > 証明書ベースの認証の設定 …
★ お気に入り 、	-
♦ ID	↓ 証明書ペースの認証 (CBA) が有効になっているユーザーには有効な証明書があることを確認してください。CBA は今要素認証 (MFA) に対応しているため、有効な証明書がない場合、ユーザーは、CBA を 2 番目の要素として使
👃 保護 🗸	証明書ペースの認証は、認証にx.509証明書とエンターブライズ公開キー基盤 (PKI)を使用するバスワードレスでファイシングに強い認証方法です。詳細情報。
G Security Center	有効化およびターブット 構成
♀ ID セキュリティ スコア	有効にする
 多要素認証 	含める 除外
<i>A</i> ? 認証方法	7-ガット ◎ まべてのコーザー ○ グループの選択
∞ パスワードリセット	名前 種類
・・・ 表示数を少なくする	すべてのユーザー グループ
Identity Governance	
👗 検証可能な資格情報	

③ 「有効化およびターゲット」タブで「証明書ベースの認証」を「有効」にします。

M	licrosoft Entra 管理センター	ノ リソース、サービス、ドキュメントの検索 (G+/)
\$	ѫ–д	ホーム > 認証方法 ポリシー > 証明書ベースの認証の設定 …
*	お気に入り 🗸 🗸	
4	ID 🗸	● 証明書ベースの認証 (CBA) が有効になっているユーザーには有効な証明書があることを確認してください。CBA は多要素認証 (MFA) に対応しているため、有効な証明書がない場合、ユーザーは、CBA を 2 番目の要素として
2.	保護 へ	証明書ペースの認証は、認証に x.509 証明書とエンターブ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強い認証方法です。詳細情報。
G	Security Center	有効化およびターゲット 構成
Q	ID セキュリティ スコア	
\odot	多要素認証	
13	認証方法	
	パスワード リセット	ターナット • すべくのユーサー () クルーフの選択
	表示数を少なくする	→ #7 (EM) すべてのユーザー グループ
۲	Identity Governance \checkmark	

④ 次に「有効にする」ボタンの下にある「含める」タブの「ターゲット」を「グループを選択」にチェックを入れます。

Microsoft Entra 管理センター		<i>P</i> リソース、	サービス、ドキュメントの検索 (G+/)
↑ ホーム		ホーム > 認証方法 ポリシー > 証明書ベースの認証の設定 …	
★ お気に入り	\sim		
♦ ID	\sim	● 証明書ベースの認証 (CBA) が有効になっているユーザーには有対	かな証明書があることを確認してください。 CBA は多要素認証 (MFA) に対応しているため、有効な証明書がない場合、ユーザーは、 CBA を 2 番目の要素として
<mark>▲</mark> 保護	^	証明書ベースの認証は、認証に x.509 証明書とエンタープライズ公	開キー基盤 (PKI) を使用するバスワードレスでファイシングに強い認証方法です。詳細情報。
G Security Center		有効化およびターゲット 構成	
♀ ID セキュリティ スコア			
 	ſ	Anz Pol	
47 認証方法			
∞ パスワードリセット		ダーリット () すべてのユーザー (●) ジルーブの進択 グループの追加	
・・・ 表示数を少なくする		名前	種類
Identity Governance	~	すべてのユーザー	グループ
errance dentity governance	~		

⑤ 「グループの追加」をクリックして表示される画面から証明書ベースの認証を設定するグループ(ここでは「TestGroup」とします)を追加します。グループが正しく追加されると以下のように表示されます。

Microsoft Entra 管理センター	シ リソース、サービス、ドキュメントの検索 (G+/)
♠ ホーム	ホーム > 認証方法 ポリシー > 証明書ベースの認証の設定 …
★ お気に入り	
♦ ID	◆ ① 証明書ペースの認証 (CBA) が有効になっているユーザーには有効な証明書があることを確認してください。CBA は多要素認証 (MFA) に対応しているため、有効な証明書がない場合、ユーザーは、CBA を 2 番目の要素として使
▲ 保護	へ 証明者ペースの認証は、認証に x.509 証明者とエンターブ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強い認証方法です。詳細情報。
G Security Center	有効化およびターゲット 構成
♀ ID セキュリティ スコア	
 · 多要素認証 	会MZ 险化
<i>4</i> ? 認証方法	日の3 mm/r ターゲット ○ すべてのコーザー ● グルーブの選択
∞ パスワードリセット	グループの追加
・・・ 表示数を少なくする	名前 種類
Identity Governance	TestGroup ℓ/lν−ブ

⑥ 次に「構成」タブをクリックします。

м	icrosoft Entra 管理センター		、シリソース、サービス、ドキュメントの検索 (G+/)	
^	木一ム		ホーム > 認証方法 ポリシー > 証明書ベースの認証の設定 …	
*	お気に入り	\sim		
۵	ID	\sim	● 証明巻ベースの認証 (CBA) が有効になっているユーザーには有効な証明巻があることを確認してください。CBA は多要素認証 (MFA) に対応して	いるため、有効な証明書がない場合、ユーザーは、CBA を 2 番目の要素として使
4	保護	^	証明書ベースの認証は、認証に x.509 証明書とエンターブ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強い認証方法で	す。詳細情報。
C 0 0	Security Center ID セキュリティ スコア		有効化およびターゲット 構成 有効にする ()	
43	≫ ¥ #804L 認証方法		含める 除外 ターゲット ○ すべてのユーザー ● グループの選択	
(PL)	バスリートリゼット		グループの追加	
	表示数を少なくする		名前	種類
۲	Identity Governance	\sim	TestGroup	グループ

⑦ 「証明書失効リスト(CRL)の検証」において、「CRL 検証を必須にする (推奨)」にチェックを入れてく ださい。

有効化およびターゲット 構成	
証明書失効リスト (CRL) の検証	
この設定は、すべての証明機関 (CA) の Cl	RL チェックを必須にします。CRL 配布ボイントが空であるか、CA 用に構成されていない場合、認証は失敗します。証明機關を CRL 検証要件から除外できます。
CRL 検証を必須にする (推奨)	
CA を CRL 検証から除外する	0 個の CA を選択済み
	+ 除外対象の追加
	+ 除外対象の追加

⑧ 「発行者ヒント」にはチェックを入れてください。

発行者ヒント		
認証中に証明書ピッカーに有効な証明書のみが表示されるように、発行者と	ントを有効にします。 詳細情報	
発行者とント		

⑨ 「認証バインド」では「保護レベル」は「単一要素認証」、「必須のアフィニティバインド」は「低」が

選択されていることをご確認ください。

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	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ーライドします。 詳細情報			
保護レベル ①	 単一要素認証 多要素認証 			
必須のアフィニティバインド ①	● 低○ 高			
+ 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 バインド
認証バインド ポリシー規則がありません。				

次に「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、認証を許可する認証局(証明書の発行者)を設定しま

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ーライドします。 詳細情報			
保護レベル ①	 単一要素認証 多要素認証 		
必須のアフィニティバインド ①	● 低○ 高		
+ 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 バインド

「認証バインド ポリシー規則の追加」画面では先にアップロードした以下の2つの認証局(証明書の発行者)を設定します。

・NRA-PKI ルート認証局証明書(ファイル名: NipponRARootCertificationAuthorityG2.cer)

・NRA-PKI 中間認証局証明書(ファイル名: NipponRACertificationAuthority6G2.cer)

まず「NRA-PKI ルート認証局証明書(ファイル名:NipponRARootCertificationAuthorityG2.cer)」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 🕦
NRACAG2 V
証明書の発行者()
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
追加 キャンセル

設定後、画面下部の「追加」ボタンをクリックして設定を完了してください。

次に「NRA-PKI 中間認証局証明書(ファイル名: NipponRACertificationAuthority6G2.cer)」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 ①
NRACAG2 ~
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

設定後、画面下部の「追加」ボタンをクリックして設定を完了してください。

「証明書ベースの認証の設定」画面に、追加した2つの認証局(証明書の発行者)が設定されていること

を確認してください。

認証パインド			
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ーライドします。 詳細情報			
保護レベル ①	 単一要素認証 多要素認証 		
必須のアフィニティバインド ①	● 低○ 高		
+ 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 バインド
CN=Nippon RA Root Certification A	authority G2, O=Nippo… N/A	単一要素	低
CN=Nippon RA Certification Author	rity 6 G2, O=Nippon R···· 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	
十 規則の追加		
証明書フィールド	アフィニティ バインド	ユーザー属性
特別なルールが追加されていません。		

「証明書フィールド」に「PrincipalName」、「ユーザー属性」に「userPrincipalName」を選択し追加し

ユーザー名バインド ポリシー規則の追加	
証明書フィールド・	
PrincipalName	
アフィニティ バインド	
低	
ユーザー属性*	
userPrincipalName	

再度「規則の追加」をクリックし、「ユーザー名バインド ポリシー規則の追加」画面を表示します。

そして「証明書フィールド」に「RFC822Name」、「ユーザー属性」に「userPrincipalName」を選択し 追加します。

ユーザー名バインド ポリシー規則の追加	×
証明書フィールド・	
RFC822Name	\sim
アフィニティ バインド	
低	\sim
ユーザー属性*	
userPrincipalName	\sim

「ユーザー名バインド」に追加した2つの規則が表示されていることを確認してください。

ユーザー名パインド				
フ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				
+ 規則の追加				
証明書フィールド	アフィニティ バインド	ユーザー属性		
PrincipalName	低	userPrincipalName		
RFC822Name	低	userPrincipalName		

⑪ 画面下部にある「保存」ボタンをクリックしてください。

以上で設定は完了になります。

4. Appendix1(Windows PC での認証手順)

実際に Windows PC にクライアント証明書をインストールして、Microsoft Entra ID にアクセス(認証)する手順を説明します。

NRA-PKI クライアント証明書の発行手順、Windows PC への証明書インストール手順については、 以下の別資料を参照ください

NRA-PKI クライアント証明書発行手順
 URL: <u>https://www.nrapki.jp/support/?p=1574</u>
 ※「利用法人管理者マニュアル (Microsoft Entra CBA 用のサービス専用)」をご確認ください。
 NRA-PKI クライアント証明書インストール手順
 URL: <u>https://www.nrapki.jp/support/?p=462</u>

 ブラウザを起動し Microsoft の「アカウントサインイン」サイト(<u>https://myapps.microsoft.com</u>) にアクセスします。表示された「サインイン」画面でアカウントを入力し「次へ」をクリックします (本資料では「testuser001@nrapki.jp」アカウントでサインインを試行します)。



「パスワードの入力」画面が表示されますので、下部にある「証明書またはスマートカードを使用する」をクリックします。

← testuser001@nrapki.jp	
パスワードの入力	
パスワード	
パスワードを忘れた場合	
証明書またはスマートカードを使用する	

【補足】Microsoft Entra ID の仕様上パスワード入力画面は無効化できません。(2024年9月時点) パスワードのみでのログインを避けたい場合は、多要素認証や管理者がパスワードを管理する等の回 避策をご検討ください。

③ ブラウザ上部に「証明書の選択」画面が表示されます。Windows PC にインストールされているクライ アント証明書が表示されますので適切なクライアント証明書を選択して「OK」ボタンをクリックして ください。

certauth.login.microsoftonline.com:443 での認証に使用する証明書を選択してください 住名 発行元 シリアル番号 testuser001 Nippon RA Certifica 1B02EB 証明書情報 OK キャンセル 証明書情報 OK キャンセル こに切書でサインインするる デバイスによってセキュリティ ウィンドウが開かれます。 手順に従ってサインインしてください。 スマート カードを使用している場合は、正しく挿入されている ことをご確認ください。	証明書の選択 ×			
住名 発行元 シリアル番号 testuser001 Nippon RA Certifica 1B02EB 証明書情報 OK キャンセル 正明書情報 のK キャンセル 正明書情報 アK キャンセル エロリョー デバイスによってセキュリティ ウィンドウが開かれます。 手順に従ってサインインしてください。 スマートカードを使用している場合は、正しく挿入されている ことをご確認ください。	certauth.login.microsoftonline.com	:443 での認証に使用する証明	月書を選択してください	
testuser001 Nippon RA Certifica 1B02EB 証明書情報 のて キャンセル 正明書情報 のて キャンセル 正明書でサインインする デバイスによってセキュリティ ウィンドウが開かれます。 手順に従ってサインインしてください。 デバイスによってセキュリティ ウィンドウが開かれます。 スマート カードを使用している場合は、正しく挿入されている ことをご確認ください。	 件名	発行元	シリアル番号	
ぼ明書情報 の て モャンセル 証明書でサインインする デバイスによってセキュリティウィンドウが開かれます。 手順に従ってサインインしてください。 スマートカードを使用している場合は、正しく挿入されている ことをご確認ください。	testuser001	Nippon RA Certifica	1B02EB	
証明書でサインインする デバイスによってセキュリティウィンドウが開かれます。 手順に従ってサインインしてください。 スマートカードを使用している場合は、正しく挿入されている ことをご確認ください。	証明書情報	Г	ОК +7	ンセル
デバイスによってセキュリティ ウィンドウが開かれます。 手順に従ってサインインしてください。 スマート カードを使用している場合は、正しく挿入されている ことをご確認ください。	証明書でも	ー サインインする		
スマートカードを使用している場合は、正しく挿入されている ことをご確認ください。	デバイスによってセ 手順に従ってサイン	キュリティ ウィンドウが開た ンインしてください。	かれます。	
	スマート カードを付 ことをご確認くださ!	使用している場合は、正しい。	べ挿入されている	

④ 「サインインの状態を維持しますか?」画面が表示された場合は、「はい」もしくは「いいえ」のどち らかをクリックしてください。

Microsoft	
testuser001@nrapki.jp	
サインインの状態を維持しますか?	
これにより、サインインを求められる回数を減らすことができま す。	
── 今後このメッセージを表示しない	
いいえ <u>はい</u>	

⑤ ログイン認証が成功すると、以下の通りユーザの「アプリダッシュボード」が表示されます。

My Apps	× +				~ -		×
\leftarrow \rightarrow C \square myapps	.microsoft.com				🗟 🖻 🕁		:
דע דע איז 🗸					Q,	т)
アプリ ダッミ	レユボード	日 アプリ	の追加 🕣 コレクシ	日本RA株式会社	tostusor00	サインアウト	l
Apps				Т	testuser001@nra <u>アカウントを表示</u> 組織の切り替え	∎ apki.jp	l
V Apps				(月) 別のアカ!	うントでサインインする		1
aws	:	E E	×	:		:	1
AWS Single-Account	Access	Engage	Excel		Forms		1
	:	· · ·	N	:		:	l
Lists		OneDrive	OneNote		Planner		
٠	:	>	P	:	S	:	
Power Apps		Power Automate	PowerPoint		SharePoint		
	:	s	L ji	:	V	:	Ŧ

【補足】

クライアント証明書の認証が拒否された場合(クライアント証明書の失効を含む)、以下のような画 面が表示されます。

Microsoft
証明書の検証に失敗しました
次の手順を実行して、もう一度お試しください:
1. 現在のブラウザーを閉じてください 2. 新しいブラウザーを開いてサインインしてください 3. 証明書を選択してください
スマート カードを使用している場合は、正しく挿入されている ことをご確認ください。
詳細
その他のサインイン方法

「詳細」をクリックすると検証失敗の詳細が表示されます。「Massage」部分にその理由が表示され



【証明書検証失敗のメッセージ例】

 \cdot Validation of given certificate for certificate based authentication failed.

原因・・・選択したクライアント証明書が認証する為の証明書ではない可能性があります

• Certificate has been revoked.

原因・・・証明書が失効されている可能性があります

以上