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. 1.00	2023/10/18	初版	
Ver. 1.10	2024/03/01	アフィニティバインドの説明追加	
Ver. 1.20	2024/09/18	CRL の検証、発行者ヒントの説明追加	
Ver. 2.00	2025/1/22	ルート、中間証明書および CRL を新認証局(G2)に変更 公開キー基盤(プレビュー)の説明追加	

<目　次>

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：https://entra.microsoft.com/)」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（support@nrapki.jp）迄ご連絡ください。

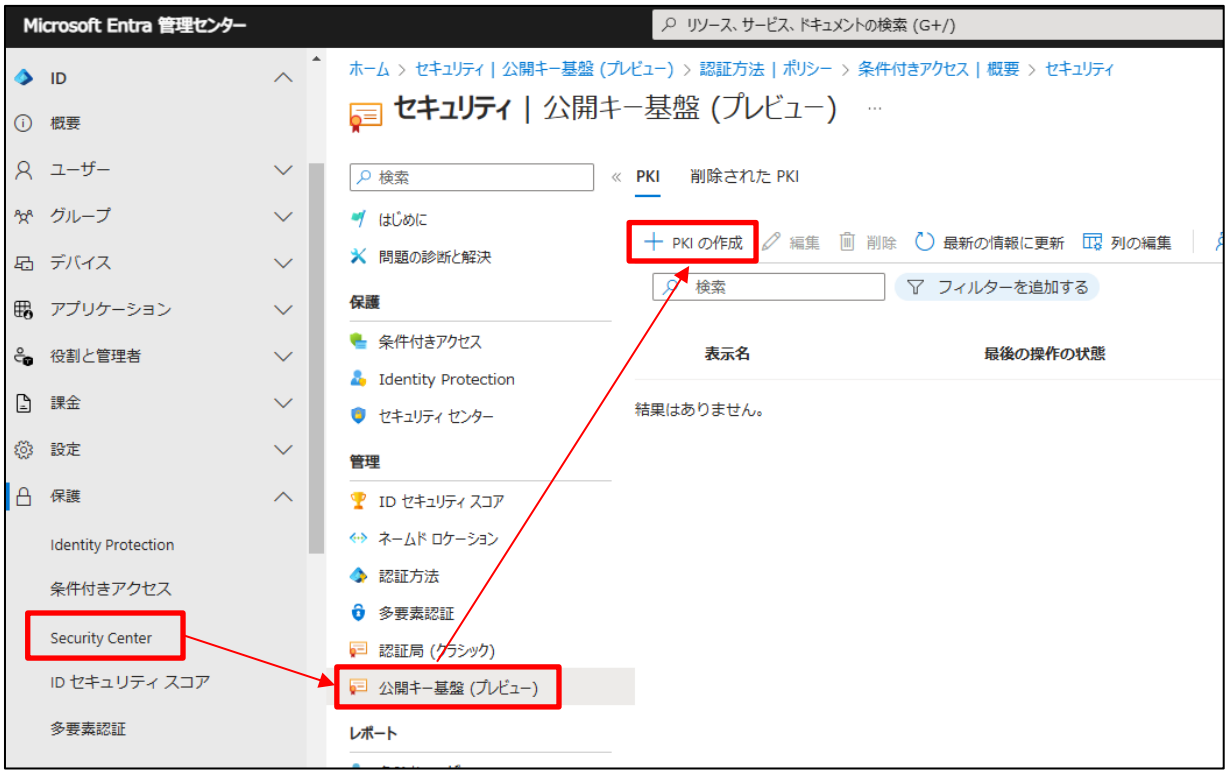
3. 設定手順

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。

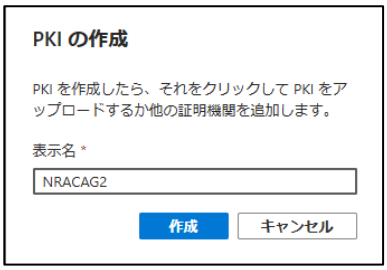
3.1. 認証局証明書のアップロード

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。

① 「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。



③ 作成した PKI をクリックします。

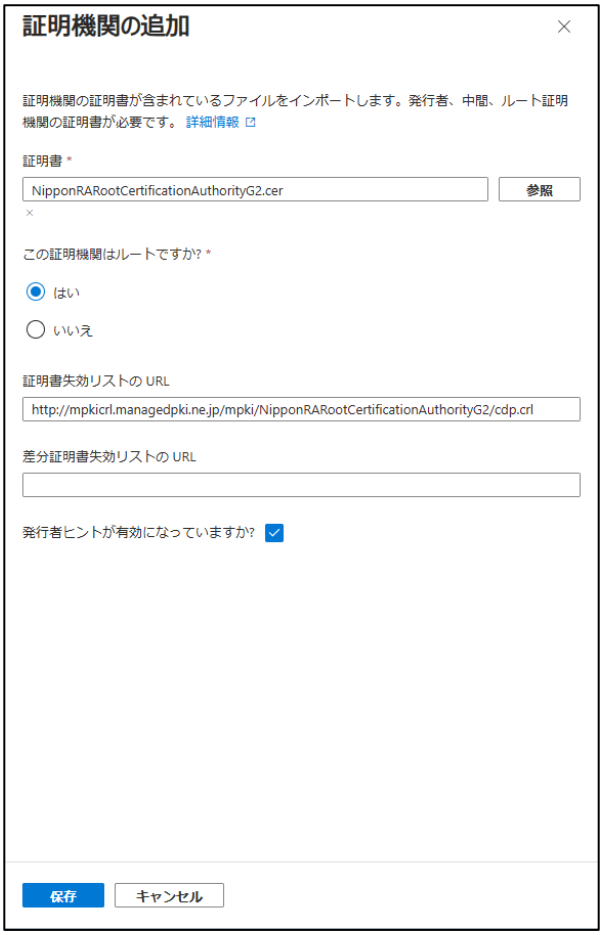
④ 「証明機関の追加」をクリックします。

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。

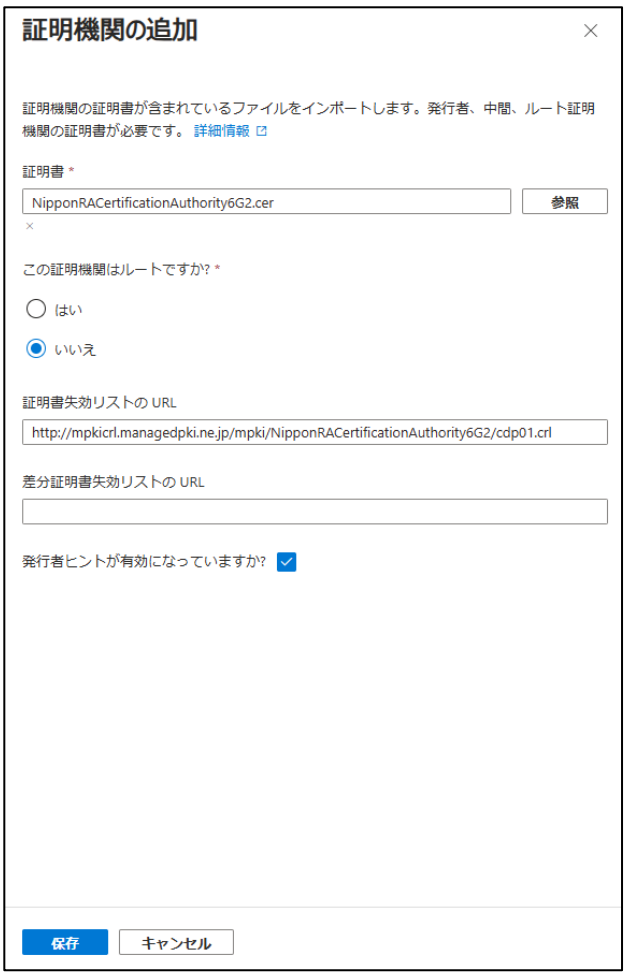
⑥ 次に「NRA-PKI 中間認証局証明書（ファイル名：NipponRACertificationAuthority6G2.cer)」をアップロードします。NRA-PKI ルート認証局証明書のアップロード手順同様に、再度「証明機関の追加」画面を開いてください。

「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。

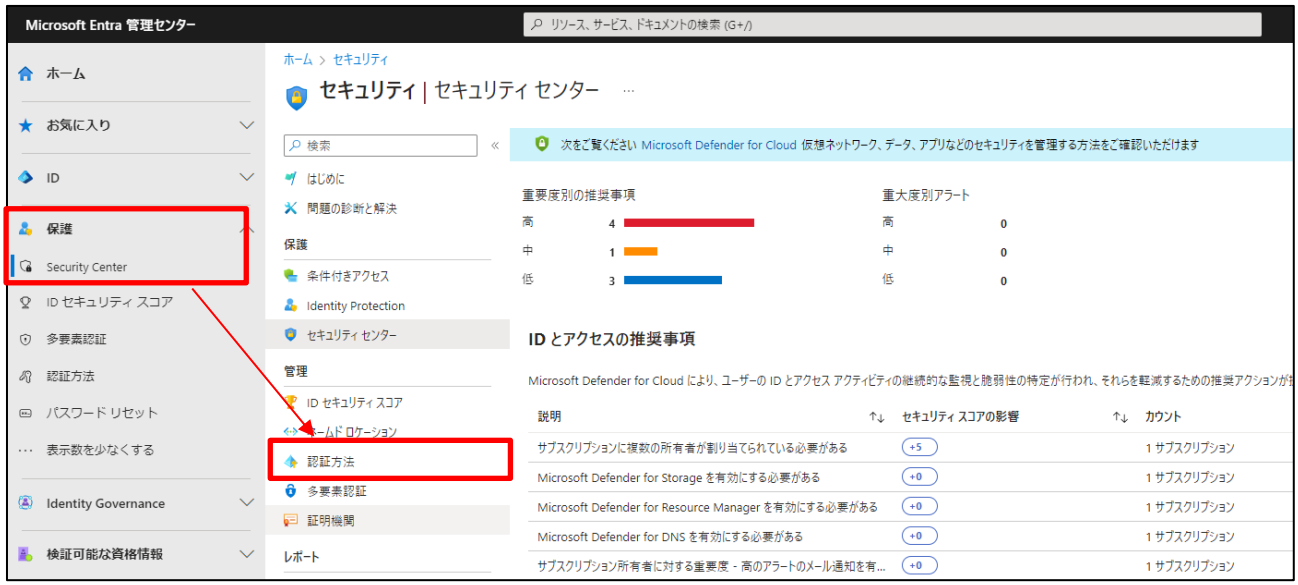
3.2. 証明書ベースの認証設定

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。



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。

「証明書ベースの認証の設定」画面が表示されます。

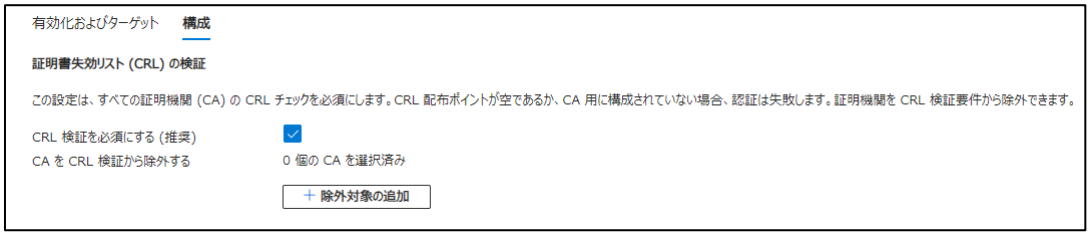
③　「有効化およびターゲット」タブで「証明書ベースの認証」を「有効」にします。

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。

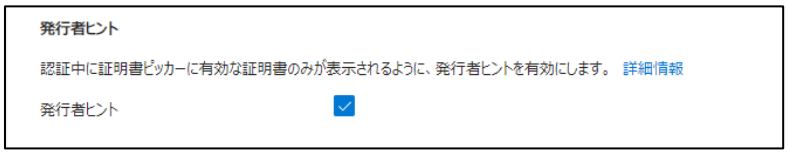
⑤ 「グループの追加」をクリックして表示される画面から証明書ベースの認証を設定するグループ（ここでは「TestGroup」とします）を追加します。グループが正しく追加されると以下のように表示されます。

⑥ 次に「構成」タブをクリックします。

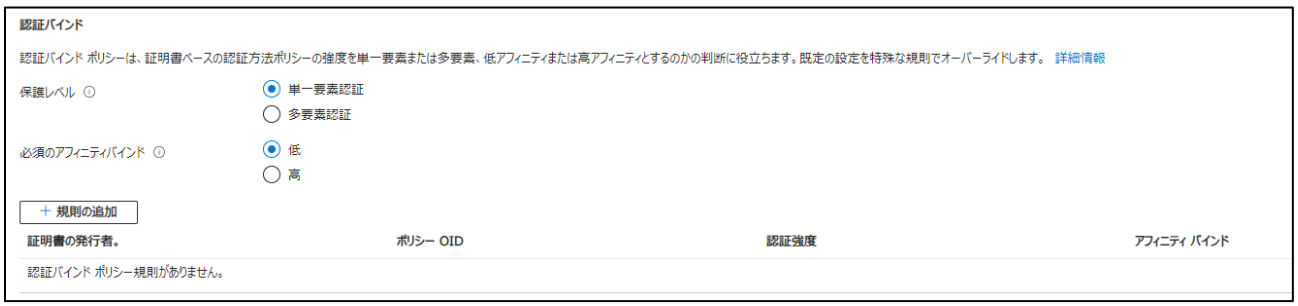
⑦ 「証明書失効リスト(CRL)の検証」において、「CRL 検証を必須にする (推奨)」にチェックを入れてください。



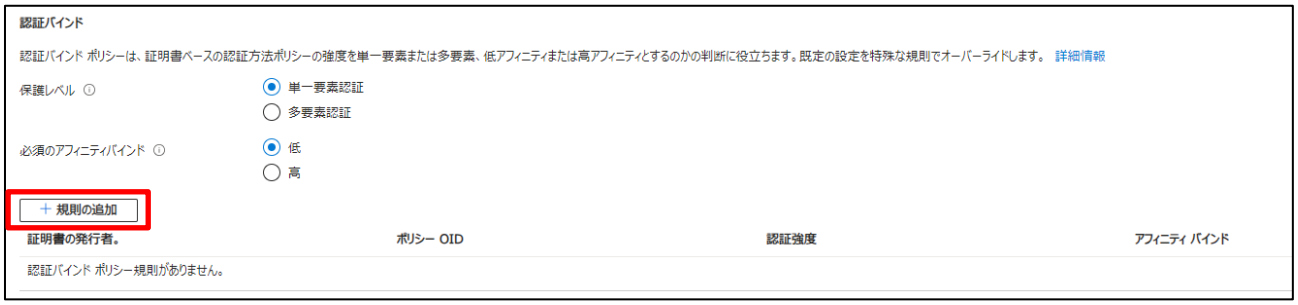
⑧ 「発行者ヒント」にはチェックを入れてください。



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。



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）を設定します。

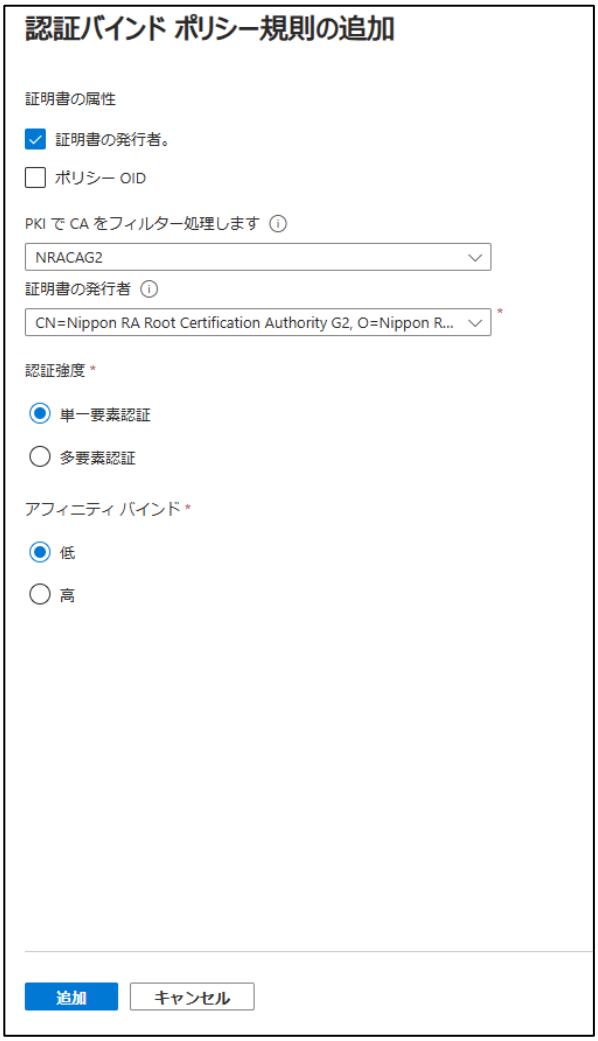


「認証バインド ポリシー規則の追加」画面では先にアップロードした以下の２つの認証局（証明書の発行者）を設定します。

・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。

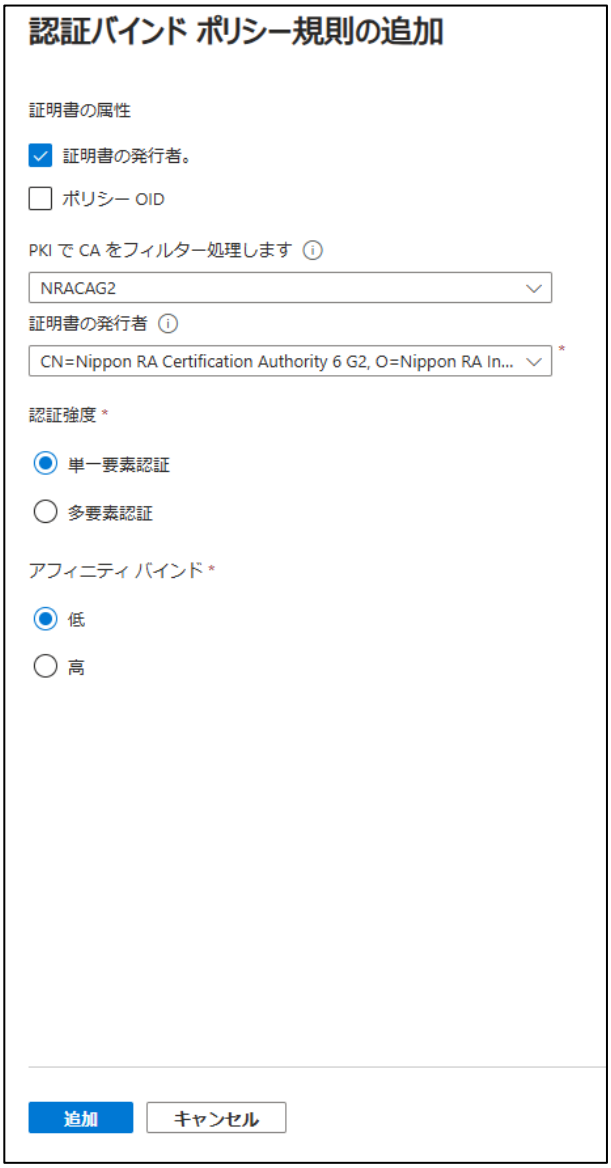
	設定項目	設定
1	証明書の属性	証明書の発行者
2	PKI で CA をフィルター処理します	作成した PKI
3	証明書の発行者	CN=Nippon RA Root Certification Authority G2, …
4	認証強度	単一要素認証
5	アフィニティ バインド	低



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

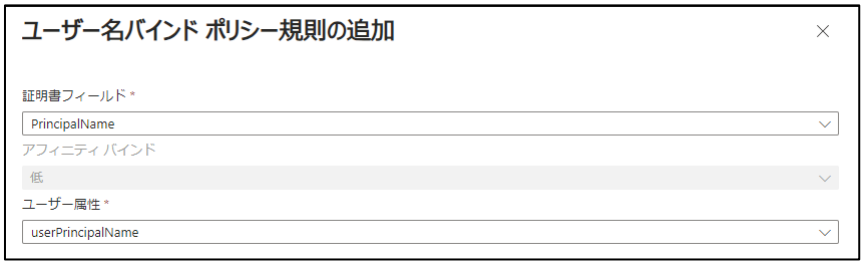


設定後、画面下部の「追加」ボタンをクリックして設定を完了してください。

「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。

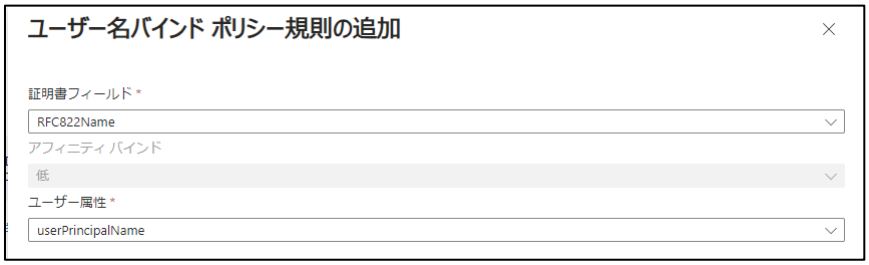
⑩ 次に「ユーザー名バインド」を設定します。「規則の追加」をクリックすると、「ユーザー名バインドポリシー規則の追加」画面が表示されます。

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



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」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。

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）

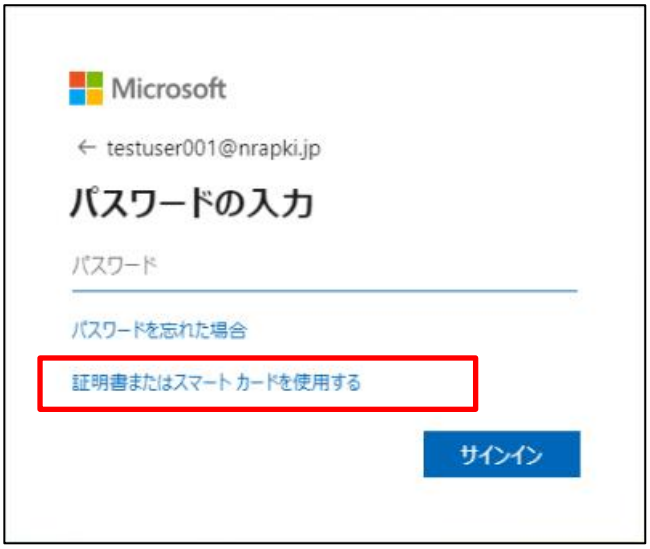
実際に Windows PC にクライアント証明書をインストールして、Microsoft Entra ID にアクセス（認証）する手順を説明します。

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：https://www.nrapki.jp/support/?p=1574
※「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：https://www.nrapki.jp/support/?p=462

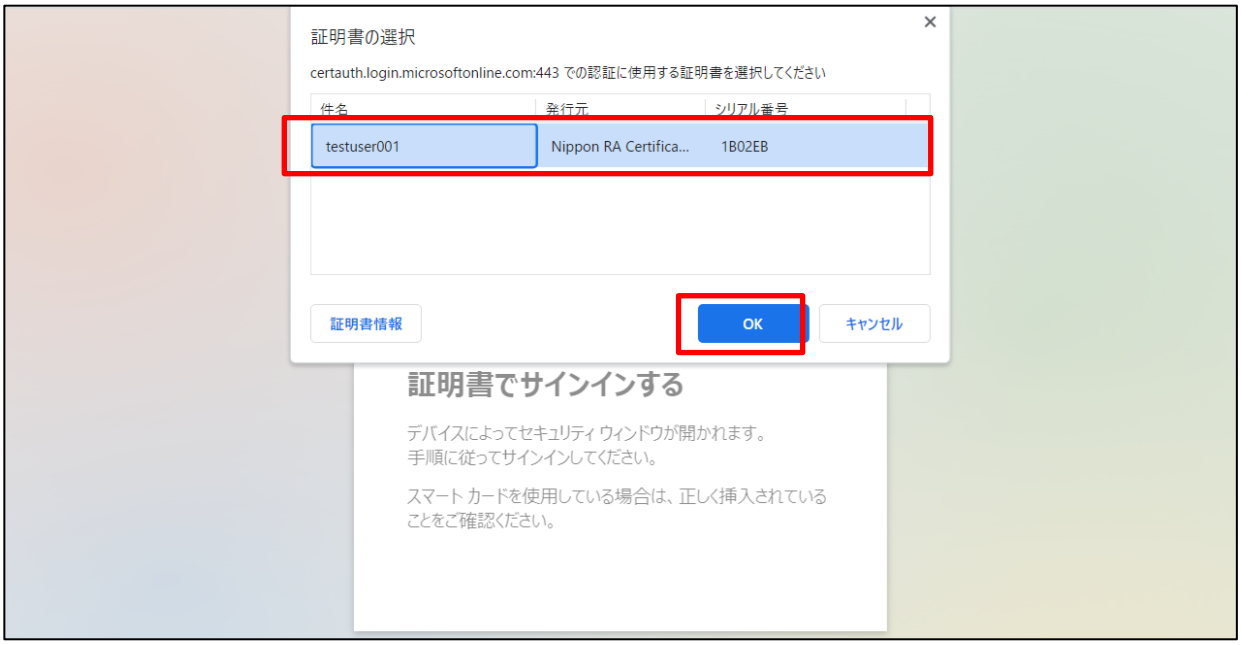
① ブラウザを起動し Microsoft の「アカウントサインイン」サイト（https://myapps.microsoft.com）にアクセスします。表示された「サインイン」画面でアカウントを入力し「次へ」をクリックします（本資料では「testuser001@nrapki.jp」アカウントでサインインを試行します）。

② 「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。

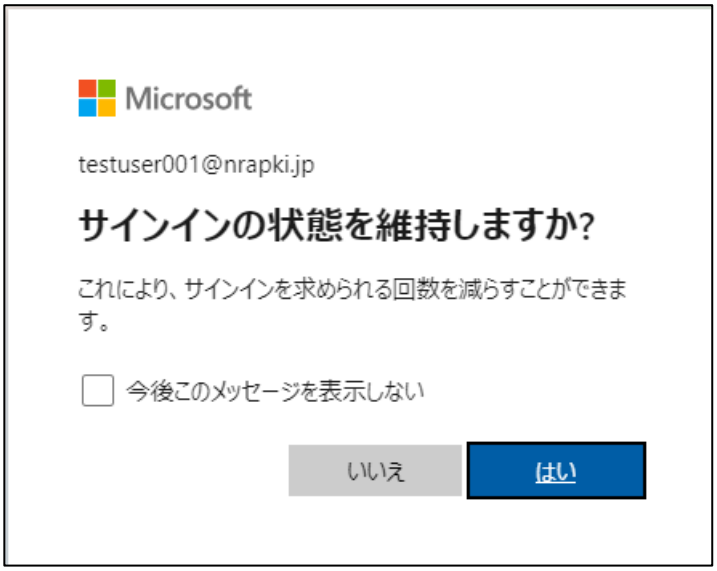


【補足】Microsoft Entra ID の仕様上パスワード入力画面は無効化できません。(2024 年 9 月時点)
パスワードのみでのログインを避けたい場合は、多要素認証や管理者がパスワードを管理する等の回避策をご検討ください。

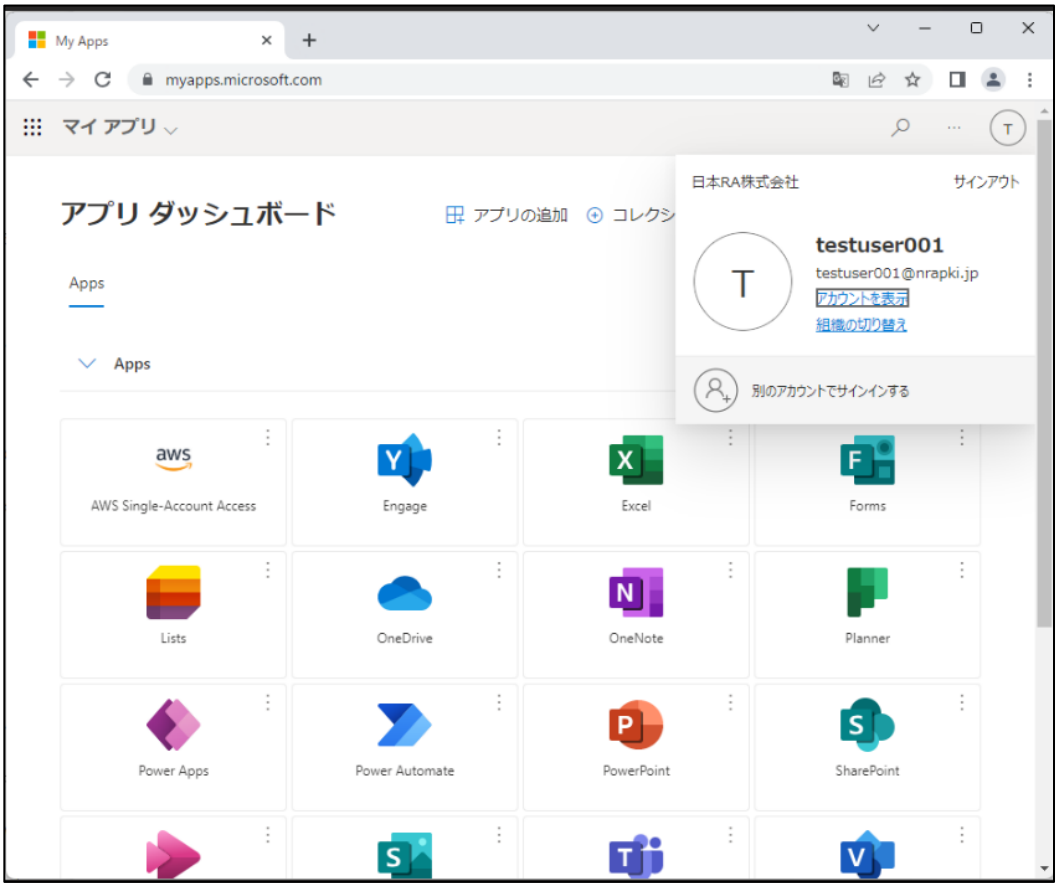
③ ブラウザ上部に「証明書の選択」画面が表示されます。Windows PC にインストールされているクライアント証明書が表示されますので適切なクライアント証明書を選択して「OK」ボタンをクリックしてください。



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。

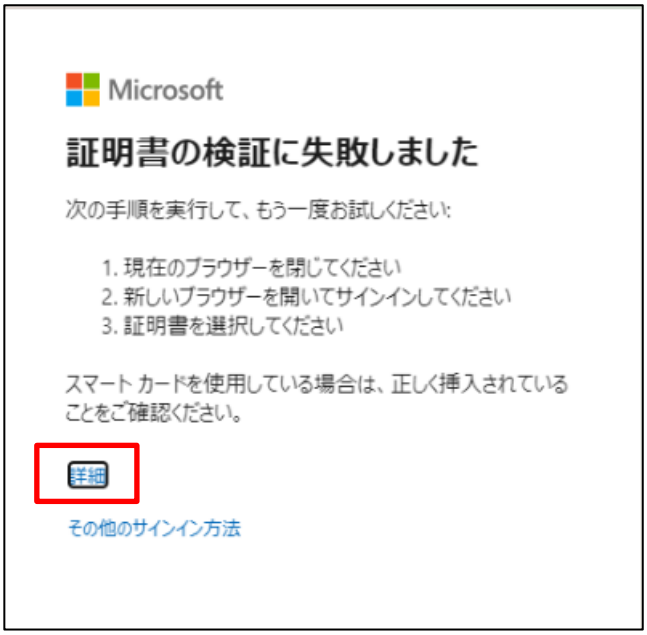


⑤ ログイン認証が成功すると、以下の通りユーザの「アプリダッシュボード」が表示されます。

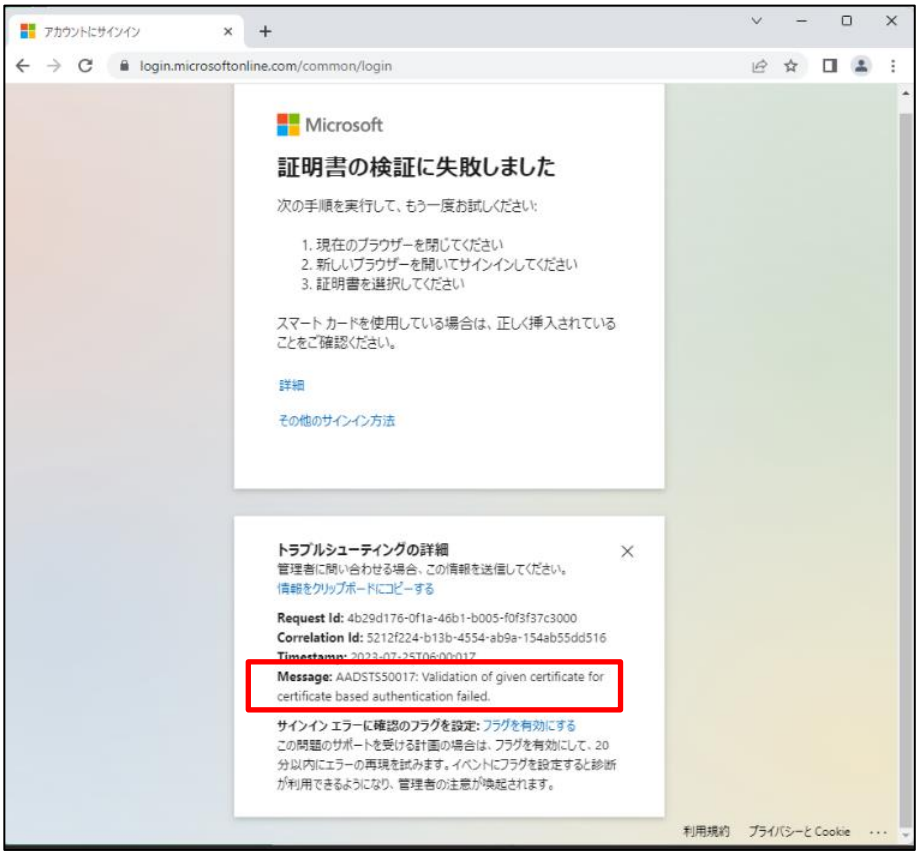


【補足】

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。



「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ます。



【証明書検証失敗のメッセージ例】

・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