

Microsoft Entra CBAによる高アフィニティな認証バインド設定

Ver.1.0

2025 年 5 月

Copyright by JCCH Security Solution Systems Co., Ltd. All Rights reserved

- JCCH・セキュリティ・ソリューション・システムズ、JS3 およびそれらを含むロゴは日本および他の 国における株式会社 JCCH・セキュリティ・ソリューション・システムズの商標または登録商標です。
 Gléas は株式会社 JCCH・セキュリティ・ソリューション・システムズの商標です。
- その他本文中に記載されている製品名および社名は、それぞれ各社の商標または登録商標です。
- ・ Microsoft Corporation のガイドラインに従って画面写真を掲載しています。

Microsoft Entra CBA による高アフィニティな認証バインド設定

目次

1.	はじぬ	5に
	1.1.	本書について5
	1.2.	本書における環境
	1.3.	本書における構成
2.	Gléas	の設定8
	2.1.	証明書テンプレートの設定8
	2.2.	アカウント作成と証明書発行9
	2.3.	証明書の配布設定
3.	Entra	ID の設定13
	3.1.	認証局を登録13
	3.2.	グループの作成15
	3.3.	証明書ベース認証の有効化17
	3.3.1.	認証強度を構成18
	3.3.2.	証明書とユーザーの紐づけを構成20
	3.4.	ユーザー情報の更新21
	3.4.1.	証明書の属性値を取得21

Microsoft Entra CBA による高アフィニティな認証バインド設定

3.4.2.	証明書ユーザーID を設定23
4. クラ・	イアントの設定25
4.1.	クライアント証明書をインポート25
4.2.	証明書ベース認証
5. その	他
5.1.	証明書ユーザーID を用いた認証制御について30
5.2.	証明書ユーザ ID の取得について33
6. 問い	合わせ34

プライベート認証局 Gléas ホワイトペーパー Microsoft Entra CBA による高アフィニティな認証バインド設定

- 1. はじめに
- 1.1. 本書について

本書では、弊社製品 プライベートCA Gléas で発行したクライアント証明書を利用して、 Entra ID ユーザーと高い親和性 (高アフィニティ) をもった認証バインドによる証明書 ベース認証 (CBA)を行う設定例を記載します。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あらゆる環 境での動作を保証するものではありません。弊社製品を用いたシステム構築の一例とし てご活用いただけますようお願いいたします。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な場合は、 最終項のお問い合わせ先までお気軽にご連絡ください。

Microsoft Entra CBA による高アフィニティな認証バインド設定

1.2. 本書における環境

本書における手順は、以下の環境で動作確認を行っています。

➢ 認証基盤: Microsoft Entra ID

※以後「Entra ID」と記載します

> アプリケーション: マイ アプリ ポータル

※以後「マイ アプリ」と記載します

- > 認証局: JS3 プライベート認証局 Gléas (バージョン 2.7.1)
 ※以後「Gléas」と記載します
- クライアント: Windows 10 Pro (22H2) / Microsoft Edge 136.0.3240.50
 ※以後「Windows」と記載します

以下については、本書では説明を割愛します。

- Entra ID の基本設定
- Gléas のアカウント登録やクライアント証明書発行等の基本操作

これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている

Microsoft Entra CBA による高アフィニティな認証バインド設定

販売店にお問い合わせください。

1.3. 本書における構成

本書では、以下の構成で検証を行っています。



- 1. Gléas は、クライアントデバイス向けにクライアント証明書を発行する。
- 2. Entra ID に、Gléas の CA 証明書を登録して証明書の発行元を信頼する。
- 3. Entra ID に、m365 のログインに証明書認証を強制するように設定。
- 4. クライアントデバイスは、Gléas より証明書をインポートする。①
- 5. 利用者は、PCより マイ アプリ にアクセスする。②
- 6. マイ アプリ は、Entra ID にシングルサインオン。③
- クライアントデバイスは、Entra ID にクライアント証明書認証を行う。④、⑤
 このとき、証明書ベース認証 (Entra CBA) は、証明書の「サブジェクトキー識別子 (SKI) 」 属性と Entra ID の「ユーザ証明書 ID (UserCertificateIDs) 」属性を用いて認証を行う。
- 8. 認証成功すると、Entra ID は認可して マイ アプリ にログイン完了。⑥
- 9. 利用者は、 マイ アプリ を利用可能となる。⑦

Microsoft Entra CBA による高アフィニティな認証バインド設定

2. Gléas の設定

2.1. 証明書テンプレートの設定

Entra ID 証明書ベース認証の要件を満たすように Gléas のデフォルトテンプレートを

以下のように設定します。

※下記設定は、	Gléas納品時等に弊社で	で設定を既におこなっ [・]	ている場合があります
---------	---------------	-------------------------	------------

証明書の属性	データベースの項目		
発行局	[発行局名]		
暗号アルゴリズム	RSA暗号		
鍵長	2048bit		
ダイジェストアルゴリズム	SHA256		
有効日数	1年		
鍵用途	電子署名、鍵の暗号化		
拡張鍵用途	SSLクライアント認証		

Microsoft Entra CBA による高アフィニティな認証バインド設定

2.2. アカウント作成と証明書発行

クライアント証明書の発行対象となる Gléas アカウントを作成し、証明書を発行します。

Gléas RA (登録局) にログインします。

[アカウント]>[アカウント新規作成]メニューをクリックします。

- [その他の設定]の[証明書を発行する]をチェック
- [▶種類]から[CSV ファイルー括]を選択
- アカウント情報に以下を入力

項目	意味
アカウント名	証明書のサブジェクトー般名となります
名前 (姓)	UA に表示される名前(姓)となります
名前 (名)	UA に表示される名前(名)となります
パスワード	UA のログインパスワードとなります

● [作成]をクリック

トアカウント情報	۰.	上級者向け設定
>アカウント名 🚖]
>名前(姓) 📩]
>名前(名) 📩]
>メールアドレス]
> バスワード]
> バスワード(確認)]
> バスワード(自動生成)	パスワード生成	
▶プリンシバル名]
	ピモ 5 文	

Microsoft Entra CBA による高アフィニティな認証バインド設定

● [アカウント] > 詳細画面で [証明書発行] メニューをクリック

_					
	ST.	08 2	H 28	s=	
н.	all	미너 문	言无	17	

● 内容を確認し [発行] をクリック

下記の内容で証明書を発行します。よろしければ「発行	」を押してください。		
(発行)	

※しばらくするとアカウントに対してクライアント証明書に発行されます

Microsoft Entra CBA による高アフィニティな認証バインド設定

2.3. 証明書の配布設定

GléasのUA (申込局) より発行済み証明書をPCにインポートできるよう設定します。

※ 下記設定は、Gléas納品時等に弊社で設定を既におこなっている場合があります

Gléas RA (登録局) にログインします。

画面上部より[認証局]をクリックし認証局一覧画面に移動し、設定を行うUA (申込局)

をクリックします。

※ 実際はデフォルト申込局ではなく、その他の申込局の設定を編集します

▶ <u>Gleas Generic UA</u> Gleas デフォルト申込局

申込局詳細画面が開くので、基本設定で以下の設定を行います。

● [証明書ストアへのインポート]をチェック

UA 申込局

- 証明書ストアの選択で、[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]に

チェック

	UT.
トーケンへのインボート 管理するトーケン Gemalto.NETカード▼ ご 証明書ストアへのインボート 証明書ストアの種類 ユーザストア▼ ダウンロードを許可 ダウンロード可能時間(分) ご インボートワンスを利用する こ CA証明書を含めない 登録消費を引わない。 (保存)	

各項目の入力が終わったら、 [保存]をクリックします。

Microsoft Entra CBA による高アフィニティな認証バインド設定

また、認証デバイス設定の以下項目にチェックがないことを確認します。

- iPhone/iPad の設定の、[iPhone / iPad 用 UA を利用する]
- Android の設定の、[Android 用 UA を利用する]

Microsoft Entra CBA による高アフィニティな認証バインド設定

3. Entra ID の設定

3.1. 認証局を登録

証明書ベース認証と連携する認証局を登録します。

本手順の前にGléasよりルート証明書をダウンロードします。

※GléasのデフォルトCAのルート証明書 (PEM形式) のダウンロードURLは以下となります http://[GléasのFQDN]/crl/ia1.pem

Microsoft Entra 管理センター にログインします。

メニュー [保護] > [セキュリティセンター] を選択します。

[認証局]を選択し、[アップロード]をクリックします。

- [証明書] に Gléas のルート証明書を指定 ※拡張子が .cer でないとアップロードできないので、.pem を .cer に変更して指定
- [ルートCA証明書である] に [はい] を選択
- [証明書失効リストのURL] にCRL配布点のURLを入力
 ※GléasのデフォルトCRL配布点のURLは以下となります http://[GléasのFQDN]/crl/ia1.crl
- [デルタ証明書失効リストの URL] は指定しない
- [追加]をクリック

Microsoft Entra CBA による高アフィニティな認証バインド設定

証明書ファイルのアップロード	×
証明機関の証明書を含む .cer ファイルをインポートします。発行者、中間、およびルー 明機関の証明書が必要です。 詳細 ☑	·卜証
証明書 *	
ia1.cer	Đ
ルート CA 証明書である ①	
• Itu	
O uuz	
証明書失効リストの URL ①	
デルタ証明書失効リストの URL ①	
追加キャンセル	

認証局が登録されました。

〒 アップロード 前 削除 ○ 更新 Ⅲ 列							
① 推奨されているアルゴリズム、キーの長さ、NIST 承認済み曲編のいずれかを必ず使用してください。 <u>詳細 〇</u>							
シ 証明書の検索							
名前	ルート…	CRL エンドポイント	サムプリント	作成日:	有効期限:		
O="JCCH Security Solution Systems Co., Ltd.", DC= (±1)							

Microsoft Entra CBA による高アフィニティな認証バインド設定

3.2. グループの作成

証明書ベース認証を行う対象となるセキュリティグループを作成します。

メニュー [グループ] > [すべてのグループ]を選択します。

[新しいグループ] をクリックします。

- [グループの種類] に [セキュリティ] を選択
- [グループの名] に任意の名前を入力
 ※例) "Entra CBA グループ"
- [グループの説明]に任意の説明を入力
 ※例) "証明書ベース認証を適用するグループ"
- [メンバーシップの種類] に [割り当て済み] を選択

ループの所属メンバーとなるユーザーを選択

- [所有者]の[所有者が選択されていません]をクリックして、セキュリティグループの所有者となるユーザーを選択
- [メンバー]の [メンバーが選択されていません] をクリックして、セキュリティグ
- [作成] をクリック

Microsoft Entra CBA による高アフィニティな認証バインド設定

新しいグループ	
▶ フィードバックがある場合	
グループの種類* ①	
セキュリティ	\sim
グループ名* ①	
Entra CBA グループ	~
グループの説明 ①	
証明書ベース認証を運用するグループ	~
クループに Microsoft Entra ロールを割り当てることができる ① はい いいえ いにしたいプログロ時間 * ○	
メンバーシッジング電気 (***) 割り当て済み	~
所有者	,
1 人の所有者が羅択されました	
-7//<	
3 メンバーが選択されました	
(here)	
1F/08	

セキュリティグループが作成されました。

Entra C&A X Y 2 イルタ の追加 検索モード ● 次の値を含む 1 個のグループが見つかりました 名前11 オブジェクト ID グループの確知 メンバーシップの種類 電子メール	🧐 新しいグループ 🞍 グループ情報をダウンロード 💍 更新	◎ ビューの管理 ∨ │ 前 削除 │ 戻	フィードバックがある場合		
検索モード	Entra CBA	× マ フィルタ -の追加			
1 個のグループが見つかりました 名前 11 オブジェクト ID グループの確領 メンバーシップの確頼 電子メール	検索モード 👥 次の値を含む				
名前11 オブジェクト ID グループの種類 メンバーシップの種類 電子メール	1個のグループが見つかりました				
	2 3 i 1⊥	オブジェクト ID	グループの種類	メンバーシップの種類	電子メール
Ec Entra CBA グループ d1f9f73f-cc68-435c-aa95-0b8785206468 セキュリティ 割り当て済み	EC Entra CBA グループ	d1f9f73f-cc68-435c-aa95-0b8785206468	セキュリティ	割り当て済み	

Microsoft Entra CBA による高アフィニティな認証バインド設定

3.3. 証明書ベース認証の有効化

作成したセキュリティグループに対して証明書ベース認証を有効化します。

メニュー [保護] > [認証方法]を選択します。

[ポリシー]を選択し、[証明書ベースの認証]をクリックします。

[有効化およびターゲット] タブを選択します。

- [有効にする] を ON
- [含める] タブの [ターゲット] の [グループの選択] を選択
- [グループの追加]をクリックして作成したセキュリティグループを選択
- [保存]をクリック

Hiorosoft Entra CBA は、今後の新聞総定サポートするために、certauth エンドポイントを certauth. login.microsoftonline.com がら t(terantid), 1572-6 (100 を見しまう), にあい この かし ふんせい しゅう (terantid), 1572-6 (100 を見しまう), にあい この かし ふんせい しゅう (terantid), 1572-6 (100 を見しまう), におい この かし ふんせい この い こい	正明書ベースの認証 の設定		
部書ペースの認証は、認証に x.509 証明書とエンタープライズ公開キー基値 (PKI) を使用する/(スクードレスでカイシングに強い認証方法です。詳細情報。 物格(および9ープト) 構成 有効にする ● 構成 有効にする ● クリーブの選択 グループの追加 名前 種類 登録 Entra CEA グループ グループ 福昭可能 ✓ X	Microsoft Entra CBA は、今後の新福能をサポートす ((tenantid) はテナント GUID を表します)に移行して [*]certauth.login.microsoftonline.com の下には 強くお勧めします。 <u>詳細情報</u>	るために、certauth エンドボイントを certauth.login.mix います。TLS 検査を備えたファイアウォールまたはプロキシが ある任意の名前と一致できるようにすることで certauth エン	crosoftonline.com から t{tenantid}.certauth.login.microsoftonline.c 組織にある場合は、正規表現()を導入し、 ドポイントの TLS 検査を無効にし、使用する特定プロキシに応じてカスタマイズする
構成 は309-751 構成 有効におよび9-751 構成 有効におよび9-751 低 有効におよび9-751	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。
ダループの逸加 名前 種類 登録 Entra CBA グループ グループ 省略可能	有効化およびタークット 構成 有効にする ●●● 含める 除外 ターゲット ● すべてのユーザー ● ヴループの選択		
名前 種類 登録 Entra CBA がループ グループ 省略可能 ×	グループの追加		
Entra CBA グループ グループ 省略可能 🗸 🗙	名前	種類	登録
	Entra CBA グループ	グループ	省略可能 🗸

Microsoft Entra CBA による高アフィニティな認証バインド設定

3.3.1. 認証強度を構成

証明書ベース認証の認証強度を設定するポリシーを構成します。

メニュー [保護] > [認証方法]を選択します。

[ポリシー]を選択し、[証明書ベースの認証]をクリックします。

[構成] タブを選択します。

- [CRL検証を必須にする] をチェック
- [発行者ヒント] をチェック

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 CRL 失敗します。証明機関を CRL 検証要件から	- チェックを必須にします。CRL 配布ポ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 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
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	

● 認証バインド [保護レベル] に [多要素認証] を選択

認証バインド [必須のアフィニティバインド] に [高] を選択

- 認証バインド [+規則の追加] をクリック
- 証明書の属性 で [証明書の発行者] を選択

Microsoft Entra CBA による高アフィニティな認証バインド設定

- [証明書の発行者] に先に登録した認証局を選択
- [認証強度] に [多要素認証] を選択

※本書では証明書を用いた認証を多要素認証として扱うように設定しています。

- [アフィニティ バインド] に [高] を選択
- [追加] をクリック

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
フィルターを適用しません 🗸
証明書の発行者 (クラシック) ①
O="JCCH Security Solution Systems Co., Ltd.", DC=com, DC=j 🗸
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

● [保存] をクリック

Microsoft Entra CBA による高アフィニティな認証バインド設定

3.3.2.証明書とユーザーの紐づけを構成

証明書ベース認証でクライアント証明書と Entra ID ユーザーを紐づけるポリシーを構成します。

メニュー [保護] > [認証方法]を選択します。

[ポリシー]を選択し、[証明書ベースの認証]をクリックします。

[構成] タブを選択します。

- ユーザー名バインド [+規則の追加] をクリック
- [証明書フィールド] に [SKI] を選択
- [ユーザー属性] に [CertificateUserIDs] を選択

※証明書のSKI (サブジェクト キー識別子) が Entra ID ユーザーの CertificateUserIDs 属性の 内容と一致するかをチェックして認証する設定とします。

● [追加] をクリック

ユーザー名バインド ポリシー規則の編集	\times
証明書フィールド。	
SKI	\sim
アフィニティ バインド	
高	\sim
ユーザー属性*	
CertificateUserIDs	\sim
 CertificateUserIDs は、証明書フィールド SKI にマップできる唯一のユーザー属性です 詳細 	
20 fm	

Microsoft Entra CBA による高アフィニティな認証バインド設定

3.4. ユーザー情報の更新

配布した証明書で認証が行えるように Entra ID ユーザーの証明書ユーザーID

(CertificateUserIDs) 属性に証明書を特定するための情報を設定します。

3.4.1.証明書の属性値を取得

本書では発行した証明書を特定するための固有値として、「サブジェクト キー識別子 (SKI)」を使用します。

Gléas RA (登録局) にログインします。

[アカウント]>[アカウント一覧]メニューをクリックします。

[アカウント]>アカウント一覧 画面から2.2項で作成したアカウントを検索し、

[アカウント]>詳細 画面に遷移します。

- 証明書発行の履歴 から発行した証明書の行をクリック
- [証明書]>詳細 画面の証明書ファイルのリンクから証明書をダウンロード



Microsoft Entra CBA による高アフィニティな認証バインド設定

- ダウンロードした証明書ファイルを開き、[詳細]タブを選択
- [サブジェクト キー識別子] フィールドの値をコピーして控えておく

💽 証明書	×
全般 詳細 証明のパス	
表示(S): <すべて>	~
フィールド	値
□ 公開キーのバラメーター □ 基本制限 □ サブジェクトキー識別子	And and the state of the state
 20 機関キー識別子 20 拡張キー使用法 20 キー使用法 	クライアント認証 (1.3.6.1.5.5.7 Digital Signature, Key Encip
IIII 1997	*
	プロパティの編集(E) ファイルにコピー(C)
	ОК

Microsoft Entra CBA による高アフィニティな認証バインド設定

3.4.2. 証明書ユーザーID を設定

対象の Entra ID ユーザーに証明書ユーザーID (CertificateUserIDs) を追加します。

メニュー [ID] > [ユーザー]を選択します。

[すべてのユーザー] から対象のユーザーを選択し、[概要] 画面を表示します。

- [プロパティの編集] をクリック
- 認可情報 の [+証明書ユーザIDの編集] をクリック
- 入力欄に3.4.1項で取得した証明書の固有値を入力

X509:<SKI>1433506CD38FA413DF86BC27B8C650949E247ADC

※<SKI>の後に 証明書の[サブジェクト キー識別子] を入力 ※入力値は Entra CBA の仕様に準じた形式で入力してください。 ※証明書ユーザIDは最大10個登録可能 プライベート認証局 Gléas ホワイトペーパー Microsoft Entra CBA による高アフィニティな認証バインド設定

● [保存] をクリック

証明書ユーザー ID の編集 × 入力できる証明書ユーザー ID は 5 つまでです。 ×
 CertificateUserids は、証明書ペースの認証の一部として使用され、特定の形式であることが 必要です<u>詳細情報</u>
X509: <ski></ski>
+ 追加
保存 キャンセル

● [保存] をクリックしてプロパティを保存

プライベート認証局 Gléas ホワイトペーパー Microsoft Entra CBA による高アフィニティな認証バインド設定

4. クライアントの設定

4.1. クライアント証明書をインポート

Edgeブラウザから UAにアクセスします。

※URL https://[UAのFQDN]/[UAの名前]/ua

ログイン画面が表示されるので、ユーザIDとパスワードを入力しログインします。

● エンドユーザロ	コグイン [UA]
UA 'ª	ーザID、バスワードを入力して口 インしてください。
▶ユーザID	
▶バスワード	
	ログイン

ログインすると、ユーザ専用ページが表示されます。

[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行

われます。

プライベートCA Gléas テスト	⊐-#- × +			- 0
\rightarrow C \clubsuit	1		A٥	6 🧕 🤹 💼
			ブ	^{メライベートCA} Gléäs UA
スト ユーザー さ	んのページ]			■ログアウト
レーザ情報				
🖉 テスト ユーザ・	ーさんのページ			
2ーザ情報・・				*
▶ユーザ	登録日時:	100.00.00		
>姓: 굿자 名: 그	-17-			
> ユーリロ. > メールアドレス:				
> パスワード: *******	*****			
🐇 STOP 🕸 #3.40				
★ 証明音 情報 …				
▶ 発行済み証明書				
		シリアル	有効期限	
#	2017/2			

Microsoft Entra CBA による高アフィニティな認証バインド設定

※証明書インポート時にルート証明書のインポート警告が出現する場合は、システム管理者に拇印を 確認するなど正当性を確認してから[はい]をクリックします

セキュリテ	1警告	\times
	発行者が次であると主張する証明機関 (CA) から証明書をインストールしよ うとしています:	
	証明書が実際に からのものであるかどうかを検証 できません。 に連絡して発行者を確認する必要が あります。次の番号はこの過程で役立ちます:	
	拇印 (sha1):	
	警告: このルート証明書をインストールすると、この CA によって発行された証明書は 自動的に信頼されます。確認されていない拇印付きの証明書をインストール することは、セキュリティ上、危険です。[はい]をクリックすると、この危険を認 識したことになります。 この証明書をインストールしますか?	
	はい(Y) しいえ(N)	

インポートワンス機能を有効にしている場合は、インポート完了後に強制的にログアウ

トさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度ロ

グインしてインポートを行うことはできません。

Google	🗙 🔟 プライベートCA Gléas テスト ユーザー 🗙	+		- 0
\rightarrow C	The land back of privation in the		Aø	යි 💿 🗘 🚺
			プラ	ам-рса Gléäs ua
テスト ユーザー さん	レのページ]			■ログアウト
ューザ情報 ② テスト ユーザー	さんのページ	_	_	
2ユーザ情報				•
▶ ユーザ	登録日時:	10.00		
≫姓:テスト 名:ユー >ユーザID:	<i>щ</i> -			
> メールアドレス: > バスワード:*********	*****			
≹ 証明書情報 ····				
▶ 発行済み証明書				
#	発行局	シリアル	有効期限	証明書ストアヘインポート

Microsoft Entra CBA による高アフィニティな認証バインド設定

4.2. 証明書ベース認証

Edgeブラウザから マイ アプリ ポータル にサインインを試みます

%https://myapps.microsoft.com/

Entra ID のサインイン画面に遷移します。

ユーザー名を入力して次へをクリックします。

() サイ) ICCH Security Solution Systems
ፖክウ:	ハにアクセスできない場合
ランド	用 変更するときは、AAD管理センター > 会社のブ
Q	サインイン オプション

[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。

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	j.	
	サインイン	

Microsoft Entra CBA による高アフィニティな認証バインド設定

クライアント証明書を選択して[OK]ボタンをクリックします。

認証用の証明書の選択 サイト		×
では資格情報が必要です:		
٦		
証明書情報	ок	キャンセル

[はい]または[いいえ]をクリックすると、サインインできます。

サインインの状能を維持しますか?			
これによ す。	り、サインインを求	えめられる回数を	咸らすことができま
	後このメッセージを	2表示しない いいえ	<u>(‡1)</u>

Microsoft Entra CBA による高アフィニティな認証バインド設定

証明書を持っていない場合、

失効済み証明書を提示した場合、

Entra ID側の証明書ユーザーID情報と合致しない証明書を提示した場合

に認証は失敗します。



プライベート認証局 Gléas ホワイトペーパー Microsoft Entra CBA による高アフィニティな認証バインド設定

5. その他

5.1. 証明書ユーザーID を用いた認証制御について

高アフィニティな設定で証明書ベース認証を構成した場合、デバイスから提示された証 明書とEntra IDの証明書ユーザーID (CertificateUserIDs) の合致をもって認証が行われ ます。

この仕組みにより特定証明書に対する認証可否をEntra ID 側から制御可能となります。 例えば、デバイスを紛失したなどの理由で即時の認証停止が必要な場合、Entra ID のか ら証明書ユーザーID (CertificateUserIDs) か削除することで証明書認証を禁止すること ができます。

Microsoft Entra CBA による高アフィニティな認証バインド設定

以下は証明書認証の制御を PowerShell で行うコマンド例です

● PowerShell を起動

※以降の操作の前に Microsoft Entra モジュールのインストールが必要です。

Install-Module Microsoft.Entra -AllowClobber

● 証明書ユーザーID を追加して認可

```
# Entra ID に接続
Connect-Entra -Scopes User.ReadWrite.All
# 証明書ファイルから証明書ユーザ ID を取得(*は証明書ファイルのパス名)
$targetCertPath = '*******'
\label{eq:certUserId} \ensuremath{\$} certUserId = (Get-EntraUserCertificateUserIdsFromCertificate - Path \ensuremath{\$} targetCertPath). SKI
# 現在の Entra ID ユーザー情報を取得(*はプリンシパル名)
$targetUserId = '********'
$user = Get-EntraUserCBAAuthorizationInfo -UserId $targetUserId
# 新しい認可情報を作成
newAuthorizationInfo = @{ certificateUserIds = @()}
foreach ($item in $user.AuthorizationInfo.CertificateUserIds) {
  $newAuthorizationInfo.certificateUserIds += $item.OriginalString
$newAuthorizationInfo.certificateUserIds +=$certUserId
#証明書ユーザ ID を更新
\label{eq:select} \ensuremath{\$} uri = \ensuremath{"https://graph.microsoft.com/v1.0/users/\${targetUserId}/?\$select=authorizationinfo"}
headers = @{'ConsistencyLevel' = 'eventual' }
params = @{authorizationInfo = $newAuthorizationInfo}
Invoke-MGGraphRequest -Method patch -Uri $uri -OutputType PSObject -Headers $headers -Body $params
# Entra ID から切断
Disconnect-Entra
```

※この操作以降、指定された証明書での認可されます

Microsoft Entra CBA による高アフィニティな認証バインド設定

● 証明書ユーザーID を削除して認認可拒否

```
# Entra ID に接続
 Connect-Entra -Scopes User.ReadWrite.All
 # 証明書ファイルから証明書ユーザ ID を取得(*は証明書ファイルのパス名)
 $targetCertPath = '**********
 \label{eq:certUserId} \ensuremath{\texttt{scertUserId}} = ({\ensuremath{\texttt{Get-EntraUserCertificateUserIdsFromCertificate}} - {\ensuremath{\texttt{Path}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\scertPath}\ensuremath{\texttt{scertPath}}\ensuremath{\texttt{scertPath}}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath}\ensuremath{\scertPath}\ensuremath}\ensuremath{\scertPath}\ensuremath}\ensuremath{\scertPath}\ensuremath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath{\scertPath}\ensuremath}\ensuremath}\ensuremath{\scertPath}\ensuremath}\ensuremath{\scertPath}\ensuremath}\ensuremath{\scertPath}\ensuremath}\ensure
 # 現在の Entra ID ユーザー情報を取得(*はプリンシパル名)
 $targetUserId = '*********
 $user = Get-EntraUserCBAAuthorizationInfo -UserId $targetUserId
# 新しい認可情報を作成
newAuthorizationInfo = @{ certificateUserIds = @()}
foreach ($item in $user.AuthorizationInfo.CertificateUserIds | Where-Object {$_.OriginalString -ne $certUserId }) {
          $newAuthorizationInfo.certificateUserIds += $item.OriginalString
 #証明書ユーザ ID を更新
 \label{eq:select} \end{tabular} \end{tabular} $$ uri = "https://graph.microsoft.com/v1.0/users/${targetUserId}/?$select=authorizationinfo" $$ uri = "https://graph.microsoft.com/v1.0/users/${targetUserId}/?$} $$ uri = "https://graph.microsoft.com/v1.0/users/${{targetUserId}/?$} $$ uri = "https://graph.microsoft.com
 $headers = @{'ConsistencyLevel' = 'eventual' }
 params = @{ authorizationInfo = @{ certificateUserIds = $newCertUserIds }}
Invoke-MGGraphRequest -Method patch -Uri $uri -OutputType PSObject -Headers $headers -Body $params
 # Entra ID から切断
 Disconnect-Entra
```

※この操作以降、指定された証明書では認可拒否されます

Microsoft Entra CBA による高アフィニティな認証バインド設定

5.2. 証明書ユーザ ID の取得について

弊社では、Gléas から発行済み証明書の情報を Entra ID の証明書ユーザ ID 形式で CSV

エクスポートする機能も提供可能です。

また、CSV をアップロードして EntraID の証明書ユーザ ID を更新する PowerShell サン

プルコードなども提供可能ですのでご検討の際にはご相談ください。

プライベート認証局 Gléas ホワイトペーパー Microsoft Entra CBA による高アフィニティな認証バインド設定

6. 問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■Gléasや本検証内容、テスト用証明書の提供に関するお問い合わせ

株式会社JCCH・セキュリティ・ソリューション・システムズ

Tel: 050-3821-2195

Mail: sales@jcch-sss.com