

# Microsoft Entra CBAによるシングルサインオン

(SAML連携)

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。

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

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 目次

1.	はじる	ちに
	1.1.	本書について7
	1.2.	本書における環境
	1.3.	本書における構成
2.	. Web	サーバの設定11
	2.1.	アプリケーション構成 11
	2.2.	サーバ証明書の登録12
	2.3.	SAML SP 証明書の登録15
	2.4.	SAML SP メタデータの登録18
	2.5.	ヴァーチャルホスト設定19
3.	. Entra	ID の設定
	3.1.	認証局を構成20
	3.2.	グループの作成22
	3.3.	証明書ベース認証の有効化24
	3.3.1.	認証強度を構成25
	3.3.2.	証明書とユーザーの紐づけを構成

### Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

	3.4.	条件付きアクセスを構成	29
	3.4.1.	セキュリティの規定値群の無効化	29
	3.4.2.	認証強度を構成	31
	3.5.	アプリケーションの登録	33
	3.5.1.	アプリケーションに SSO を構成	35
	3.5.2.	アプリケーションにユーザーを割り当て	42
	3.5.3.	アプリケーションへのアクセスポリシーを構成	45
4	. Web	サーバの設定	49
	4.1.	SAML IdP メタデータを Web サーバに登録	49
	4.2.	Web サーバ起動	49
5	. AP <del>ህ</del>	ーバの設定	50
	5.1.	構成	50
	5.2.	実装	51
	5.3.	AP サーバ起動	51
6	. Gléas	の設定	52
	6.1.	証明書テンプレートの設定	52
	6.2.	アカウント作成と証明書発行	53

### Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

6.3.	証明書の配布設定 (Windows 向け)	56
6.4.	証明書の配布設定 (iPhone 向け)	58
6.5.	証明書の配布設定(Android 向け)	61
7. クラ	イアントの設定	63
7.1.	Windows にクライアント証明書をインポート	63
7.2.	iPhone にクライアント証明書をインポート	65
7.3.	Android にクライアント証明書をインポート	68
8. 証明	書ベース認証によるアプリケーション利用	71
8.1.	Windows デバイスでアクセス	71
8.2.	iPhone デバイスでアクセス	75
8.3.	Android デバイスでアクセス	78
9. その	他	81
9.1.	ユーザー情報をアプリケーションに伝える	81
9.2.	サインインログについて	82
9.3.	証明書の失効確認について	83
9.4.	失効の即時反映について	84
9.5.	失効リストのサイズ制限について	85

# Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# プライベート認証局 Gléas ホワイトペーパー Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

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、 Microsoft Entra ID の証明書ベース認証 (CBA)をおこないWebアプリケーションにア クセスする構成の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 を使用したシングルサインオン (SAML 連携)

# 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

- > 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
- > Webサーバ: AlmaLinux9.4 / Apache 2.4.37

(mod\_ssl / mod\_auth\_mellon / mod\_proxy / mod\_headers) ※以後「Webサーバ」と記載します

- アプリケーションサーバ: AlmaLinux9.4 / Node.js v16.20.2
   ※以後「APサーバ」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
- > クライアント: iPhone 14 (iOS 18.3.1) / Safari 16.3

※以後「iPhone」と記載します

クライアント: Google Pixel 7 Android15 / Chrome 135.0.7049.111
 ※以後「Android」と記載します

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

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
- Webサーバの基本設定 (ネットワークや Apache の基本的な公開設定)
- APサーバの基本設定 (ネットワークや Node.js 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

販売店にお問い合わせください。

プライベート認証局 Gléas ホワイトペーパー Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 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。



- Gléas は、Web サーバ向けにサーバ証明書および SAML SP 証明書、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、アプリケーションを登録する。
- 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
- PC では Edge ブラウザ、iPhone では Safari ブラウザ、Android では Chrome ブラウザより Web サーバに HTTPS アクセスする。②
- 6. Web サーバは、Entra ID に SAML 認証要求。③
- Entra ID は、クライアントデバイスに認証を要求しクライアント証明書認証を行う。④、⑤
   証明書を提示しない、期限切れ、または失効している、端末はクライアント証明書認証に失敗。
- 8. 認証成功すると、Entra ID は SAML 認証応答を発行、Web サーバは SAML 認証応答を受け取り、ログイン完了。⑥
- 9. Web サーバは、アプリケーションにリバースプロキシしてサービス利用可能となる。⑦

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 2. Web サーバの設定

SAML SPとして動作するWebサーバを設定します。

※本手順では、サーバで事前にApacheがインストールされていることが前提です。
 ※Apacheは mod\_ssl, mod\_auth\_mellon, mod\_proxy, mod\_headers モジュールを有効化します。

# 2.1. アプリケーション構成

アプリケーションを公開するための構成を決定します。

アプリケーション名	SAMLデモアプリ
アプリケーションのURLパス	/saml_demo_app
サーバFQDN	sp.jcch-sss.com
プロキシURL	http://app-server:3000/saml_demo_app/
サーバ証明書のパス	/etc/httpd/conf/server.crt
サーバ秘密鍵のパス	/etc/httpd/conf/server.key
中間証明書のパス	/etc/httpd/conf/server-chain.crt
SAML SP証明書のパス	/etc/httpd/conf/saml_sp.crt
SAML SP秘密鍵のパス	/etc/httpd/conf/saml_sp.key
SAML SP の EntityID	https://sp.jcch-sss.com/saml_demo_app
SAML 名前ID形式	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Assertion Consumer ServiceのURLパス	/saml/saml_demo_app/postResponse
Single Logout ServiceのURLパス	/saml/saml_demo_app/logout
SAML SPメタデータのパス	/etc/httpd/conf/sp-metadata.xml
SAML IdPメタデータのパス	/etc/httpd/conf/idp-metadata.xml
アクセスログのパス	/etc/httpd/logs/saml_demo_app-access_log
エラーログのパス	/etc/httpd/logs/saml_demo_app-error_log
アプリケーションのサインオンURL	https://sp.jcch-sss.com/saml_demo_app/
認証ユーザをあらわすリクエストヘッダ	x-auth-user: "ユーザ プリンシパル名"

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 2.2. サーバ証明書の登録

Web サーバに適用するサーバ証明書を発行します。

※本手順では、Gléasで事前にサーバアカウントを作成してあることが前提です。 ※アカウント名、ホスト名は、2.1 項の [サーバFQDN] を入力

Gléas RA (登録局) にログインし、該当のサーバアカウントのページへ移動します。

(ウント 1、)±20					
ccount					<ul> <li>         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>
ブループ				1922	
roup 273	カウント情報・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	11日本の11日本の11日本の11日本の11日本の11日本の11日本の11日本	🕼 グループ情報		● サーバ証明書
E明書 ertificate トサー	-17	登録目時:	▶ ユーザグループ	日生加	② 認証局証明書
S証デバイス evice >ステ	- タス: 有効		> <u>SSLサーバ証明書</u>		
シブレート トリー	-バ困性	最終更新: 編集	トロールグループ	nt # 1	
emplate > ホス	h名:		>なし		保存
ウント操作					
ントー覧 🍡 証	明書発行の履歴				トック まアカウント (0)
請者一覧 ▶1					★証明書_(0)
ント新規作成	シリアル 開始	有効期限 スキ	テータス 失効日	暗号種別トークン	
書発行		証明書は発行る	好していません。		
ウント削除 🎽 テ	ンプレート情報				
200AN8	デジェクト				
	種別		必須テンプレート	任意テンプレート	
	一般名(CN)				
	ドメインコンボーネント(D0	2)			
	ŧ				
- 48 L	種房川		必須テンプレート	任意テンプレート	
	発行局				
	発行局 暗号アルゴリズム	RSAF音号			
	発行局 暗号アルニリズム 建長 なく22.7 トアロー・リンプノ	RSA##号 2048bit			
	発行局 暗号アルゴリズム 課長 ダイジェストアルゴリズム 右か叫取る	RSA#音号 2048bit SHA256 1座			
	<ul> <li>発行局</li> <li>暗号アルゴリズム</li> <li>建長</li> <li>ダイジェストアルゴリズム</li> <li>有効期限</li> <li>線用途</li> </ul>	RSA培告 RSA培告 2048bit SHA256 1年 電子医名 (1年)			
	発行局 増考アルニリズム 建築 ダイジェストアルニリズム 有効期限 親用達 約24週間後	RSA編号           2048bit           SH4256           1年           電子署名           諸の項号化           SSLサーバ22証			
	<ul> <li>第月局</li> <li>建長</li> <li>建長</li> <li>ダイジンストアルビリズム</li> <li>和防腸隙</li> <li>健用途</li> <li>鉱構織用途</li> </ul>	RSA#時代           2048bt           3H4256           1年           電子裏名           線の確而化           SSLグライアント2222			

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

小メニューの[証明書発行]をクリックし、アカウントに対し証明書を発行します。

	■詳細に戻る
東証明書発行 この画面では証明書要求の作成を行います。 左側の「サブジュクト」と「衛生」の内容で証明書要求を作成します。 右側のデンプレートの中から必要なものを選択して「発行」を押してください。	
▶証明表発行 >下記の内容で証明書を発行します。ようしければ「発行」を押してください。	◆ 上級者向け設定 発行
▶ サブジェクト > CN= > DC=	<ul> <li>▶ 選択されているテンプレート</li> <li>▶ 必須 デフォルト設定</li> <li>&gt; 必須 SSLサーパ証明書</li> </ul>
<ul> <li>▶ 昭任</li> <li>&gt; 発行局:</li> <li>&gt; 暗音アルゴリズム: RSA暗号</li> <li>&gt; 健長: 2048bit</li> <li>&gt; ダイジェストアルゴリズム: SHA256</li> <li>&gt; 物功日数: 1年</li> <li>&gt; 健用途:電子署名, 練の暗号化</li> <li>&gt; 批励採興所途: SSLサーバIZME, SSLクライアントIZME</li> <li>&gt; 別均(DNS):</li> </ul>	<ul> <li>▶ 選択可能なテンプレート</li> <li>&gt; なし</li> </ul>

証明書詳細画面から[ダウンロード]をクリックし証明書をダウンロードします。

	► <u>Ev2</u>
★ 証明書情報 ─────	
	開始日: 終了日:
▶説明:	最終更新: 雪集
▶♥७७४४	▶基本情報
>一般名:	> 作成日:
>ドメインコンボーネント:	> 有効日数: 366
>ドメインコンボーネント:	> 失効日:
	> 失効理由:
	> 期限長終了日:
	> 状態: 有効な証明書
	> 処理の状態:有効な証明書
	>トークン必要:
	> バージョン:4
▶ 証明書情報 > 認証局:	
<ul> <li>▶ 証明書体報</li> <li>&gt;&gt; 記証局:</li> <li>&gt;&gt; 暗号アルゴリズム:rsa</li> <li>&gt;&gt; ダイジェストアルゴリズム:sha256</li> <li>&gt;&gt; 違果: 金子墨名 違の暗号止</li> <li>&gt;&gt; 拡張線用途:SSLサーバ翌延 SSLクライアン比較証</li> <li>&gt;&gt; 別応:DNS名:</li> </ul>	
<ul> <li></li></ul>	
<ul> <li>■ 証明書執報</li> <li>&gt;&gt; 昭芸局:</li> <li>&gt;&gt; 昭号アルコリズム: rsa</li> <li>&gt;&gt; ダイジェストアルゴリズム: sha256</li> <li>&gt;&gt; 鍵長: 2048</li> <li>&gt;&gt; 鍵用途: 電子常各:線の暗音化</li> <li>&gt;&gt; 加味線用途: SSLサーバ設証: SSLクライアンド設証</li> <li>&gt;&gt; 別応: DNS名:</li> </ul> > 証明書ファイル > 証明書要求: 恋儿	
<ul> <li> <b>証明書估報</b> </li> <li>             日電子アルニリンズム: rsa         </li> <li>             ピ号アルニリンズム: rsa         </li> </ul> <li>             御告:         <ul> <li>             ピラマルアルごりンズム: rsa</li> <li>             ダイジェストアルニリンズム: sha256         </li> <li>             御長:             2048         </li> </ul> </li> <li>             Will, 製品         <ul> <li></li></ul></li>	
<ul> <li>         ■ 証明書払給         &gt; 認証局:         &gt; 暗号アルゴリズム:rsa         &gt; タイシェストアルゴリズム:sha256         &gt; 總長:2048         &gt; 總長:2048         &gt; 總長:2048         &gt; 總長:2048         &gt; 總規造:<u>雪子署名:總の相号化</u>         &gt; 納保線用途:<u>SSLサーバ型経:SSLクライアント認証</u>         &gt; 影均名:<u>DNS名</u> </li> <li>         &gt; 証明書更不ん         &gt; 証明書更不ん         &gt; 証明書:<u>の見</u>         &gt; 証明書:<u>の見</u>         &gt; 証明書:<u>の見</u>         &gt; 近明書:<u>の見</u>         &gt; 近明書:<u>の見</u>         &gt; 近明書:<u>の見</u>         &gt; 近明書:<u>の見</u>         &gt; 近日書         &gt; 近日書         &gt; 回日書         &gt; 回日書</li></ul>	
<ul> <li>■研書体報</li> <li>&gt;認証局:</li> <li>&gt;暗号アルゴリズム:rsa</li> <li>&gt;ダイジェストアルゴリズム:sha256</li> <li>&gt; 選長:2048</li> <li>&gt; 20日本: 童子墨名:違の培告止</li> <li>&gt; 3個用途: 童子墨名:違の培告止</li> <li>&gt; 3個用途: 童子墨名:違の培告止</li> <li>&gt;&gt; 3回時書: 童子墨名:違の培告止</li> <li>&gt;&gt; 1005名:</li> </ul>	
<ul> <li>         ■ 福晴書仏報         &gt; 認証局:         &gt; 暗号アルゴリズム:rsa         &gt; ダイジェストアルゴリズム:sha256         &gt; 違長:電子電名:違の語号化         &gt; 湖田途:電子電名:違の語号化         &gt; 湖田湾:電子電名:違の語号化         &gt; 湖田湾吉ファイル         &gt; 副時書要求: あり (作成日時         &gt; 副時書: 赤り (作成日時)         &gt; 和時書: 赤り (作成日時)     </li> </ul>	
ば明書執報     は     認証局:     現号アルニリズム:rsa     メ     ポラアルニリズム:rsa     メ     ダイジェストアルニリズム:sha256     建果:2048     避肝途:電子常各:建の理音化     北球線開途:SSLサーバ型証 SSLウライアン上型証     メ     別応:DNS名     近明書ファイル     証明書であり     作成日時     秋密鍵:あり     作成日時     秋密鍵:あり     作成日時     マンブレート情報     テンブレート情報     テンブレート情報	

※ダウンロード時に証明書、秘密鍵を取り出す際のパスフレーズを指定します。

### Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

Gléasからダウンロードしたサーバ証明書 (.p12ファイル) をWebサーバにアップロード

します。

.p12ファイルからPEM形式の証明書を取り出して配置します。

※OpenSSLで行なう例 (パスフレーズの入力が必要となります)

openssl pkcs12 -in [.p12  $7 r \prec \nu$ ] -nokeys -clcerts | openssl x509 -out /etc/httpd/conf/server.crt chmod 644 /etc/httpd/conf/server.crt

### .p12ファイルからPEM形式の秘密鍵を取り出して配置します。

※OpenSSLで行なう例 (パスフレーズの入力が必要となります)

openssl pkcs12 -in [.p12  $7 r 4 \nu$ ] -nodes -nocerts | openssl rsa -out /etc/httpd/conf/server.key chmod 400 /etc/httpd/conf/server.key

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 2.3. SAML SP 証明書の登録

SAML SPとして使用する署名用証明書をGléasから発行します。

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]からアカウントを作成します。

※アカウント名は、2.1 項の [アプリケーションのURLパス] に準じたものを入力

🕂 新規アカウント作成	
2 アカウント情報の入: このページではアカウントの新規作 アカウントは証明書を発行する対象 ★の付いている項目は入力必須対	り 
▶ アカウント情報	▼上級者向け設定
>アカウント名 対	
>名前(姓) 🚖	
>名前(名) 📩	
>メールアドレス	
>バスワード	
>パスワード(確認)	
>パスワード(自動生成)	パスワード生成
>ブリンシバル名	
	(*E5\$

小メニューの[証明書発行]をクリックし、アカウントに対し証明書を発行します。

8	■詳細に戻る
★ 証明書発行 この画面では辺時書要求の作成を行います。 左側の「サブジェクト」と「際住」の内容で証明書要求を作成します。 右側のデンプレートの中から必要なものを違択して「発行」を押してください。	
▶ 証明書発行 > 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。	<ul> <li>上級者向打設定</li> </ul>
	発行
▶♥サブジェクト	▶選択されているテンプレート
> CN=	> 必須 デフォルト設定
> 0=	>必須区分CRL
500-	▶ 選択可能なデンプルート
▶屆性	stal.
> 発行局:	
>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	
> 課用途:電力著名, 課の増方化	
> 拡張提用述:SSLソフィアント記録 > Natscane titZE・ 右か	
> CRI 配布占:	
2 One Burlow .	

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

証明書詳細画面から[ダウンロード]をクリックし証明書をダウンロードします。

<b>トークンへの</b> 心ボート <b>●</b> ダウンロード <b>●</b> タイムライン   間始日: 終了日:   最終更新:
最終更新: <u>編集</u>
本 本
物情報 /P:

※ダウンロード時に証明書、秘密鍵を取り出す際のパスフレーズを指定します。

### Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

GléasからダウンロードしたSP証明書 (.p12ファイル) をWebサーバにアップロードし

ます。

.p12ファイルからPEM形式の証明書を取り出して配置します。

※OpenSSLで行なう例 (パスフレーズの入力が必要となります)

openssl pkcs12 -in [p12 ファイル] -nokeys -clcerts | openssl x509 -out /etc/httpd/conf/saml\_sp.crt chmod 644 /etc/httpd/conf/saml\_sp.crt

.p12ファイルからPEM形式の秘密鍵を取り出して配置します。

※OpenSSLで行なう例 (パスフレーズの入力が必要となります)

openssl pkcs12 -in [p12  $7 \pi 4 \mu$ ] -nodes -nocerts | openssl rsa -out /etc/httpd/conf/saml\_sp.key chmod 400 /etc/httpd/conf/saml\_sp.key

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 2.4. SAML SP メタデータの登録

SAML SP を定義するためのメタデータ (.xmlファイル) を作成します。

※2.1 項の構成に準じた SAML SP メタデータを作成するコマンド実行例



### 作成された SAML SP メタデータダウンロードします。

※上記の例では /etc/httpd/conf/sp-metadata.xml

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 2.5. ヴァーチャルホスト設定

### アプリケーションを公開するためのヴァーチャルホストを設定します。

### ※2.1 項の構成に準じたヴァーチャルホスト設定を作成するコマンド実行例

OUTFILE=/etc/httpd/conf.d/vhost-saml_demo_app.conf APP=saml_demo_app FQDN=sp.jcch-sss.com SERVER_CERT=/etc/httpd/conf/server.crt SERVER_PKEY=/etc/httpd/conf/server.key SERVER_CHAIN=/etc/httpd/conf/server-chain.crt IdP_METADATA=/etc/httpd/conf/idp-metadata.xml SP_METADATA=/etc/httpd/conf/sp-metadata.xml SP_CERT=/etc/httpd/conf/saml_sp.crt SP_PKEY=/etc/httpd/conf/saml_sp.key SP_ENDPOINT=/saml/\$APP PROXYBASE=http://app-server:3000
cat << EOS > \$OUTFILE <virtualhost *:443=""> ServerName \$FQDN CustomLog logs/\$APP-access_log combined ErrorLog logs/\$APP-error_log</virtualhost>
SSLEngine on SSLCertificateFile \$SERVER_CERT SSLCertificateKeyFile \$SERVER_PKEY SSLCertificateChainFile \$SERVER_CHAIN
<location></location> MellonEnable info MellonEndpointPath \$SP_ENDPOINT MellonSPPrivateKeyFile \$SP_PKEY MellonSPCertFile \$SP_CERT MellonSPMetadataFile \$SP_METADATA MellonIdPMetadataFile \$IdP_METADATA
<location \$app=""> AuthType Mellon Require valid-user MellonEnable auth RequestHeader set X-AUTH-USER %{MELLON_NAME_ID}e env=MELLON_NAME_ID RequestHeader set X-Forwarded-Proto https RequestHeader set X-Forwarded-Port 443 </location>
ProxyPreserveHost On ProxyPass /\$APP \$PROXYBASE/\$APP ProxyPassReverse /\$APP \$PROXYBASE/\$APP  EOS
chmod 644 \$OUTFILE

プライベート認証局 Gléas ホワイトペーパー Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 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 を使用したシングルサインオン (SAML 連携)

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、およびルート 明機関の証明書が必要です。 詳細 🖸	証
証明書 *	
ia1.cer	Ð
ルート CA 証明書である ①	
● はい	
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	
<u>追加</u> キャンセル	

認証局が登録されました。

① 推奨されているアルゴリズム、キーの長さ、NIST 承認済み曲線のいずれかを必ず使用してください。 詳細 〇					
○ 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=	… はい				

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

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。

Microsoft Entra 管理センター にログインします。

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
- [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 ループの所属メンバーとなるユーザーを選択
- [作成] をクリック

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

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	
証明書ペース認証を達用するグループ	
グループに Microsoft Entra ロールを割り当てることができる ① (はい しいえ	
メンバーシップの種類 * ①	
割り当て済み	$\checkmark$
所有者	
1 人の所有者が羅択されました	
メンバー	
3 メンバーが選択されました	
1FD2	

### セキュリティグループが作成されました。

党 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 🗸 📄 削除 🛛 📈	フィードバックがある場合		
Entra CBA	× マ フィルタ 一の追加			
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 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	

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 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。

Microsoft Entra 管理センター にログインします。

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

証明書ベースの認証の設定		×			
<ul> <li>Microsoft Entra CBA は、今後の新編能をサポートす ((tenantid) はテナント GUID を表します) に移行して [*]. Deertauth.login.microsoftonline.com の下には 強くお勧めします。 詳細言説</li> </ul>	Microsoft Evtra CBA は、今後の新舗総合サポートするために、cetaudh コンドポイントを cetaudh.login microsoftonline.com から (Cetautid) cetaudh.login.microsoftonline.com ((cenantid) isアナ・A cuD を表します) に移行しています。TLS 資産を考えたンイアウォールまたはプロキンが目的にある場合は、正現表現 (*) を得入し、 (*) cetaudh.login.microsoftonline.com の下にある仕屋の名前と一致できるようにすることで extaudh コンドポイントの TLS 緑屋を開かに、使用する特定プロキンに応じてカスタイズすることを 強くな影のパッチ、世際活動				
註明書ペースの認証は、認証に×.509 証明書とエンタープ 有効化およびターグタト 有効におる ● 含める 除外 ターゲット ○ すべてのユーザー ● グループの選訳	ライズ公開キー基盤 (PKI) を使用するパスワードレスでプ	ケイシングに弾い認証方法です。詳細情報。			
グループの追加					
名前	種類	登録			
Entra CBA ヴループ	ヴループ	「省略可能」			
保存 破棄					

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 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。

Microsoft Entra 管理センター にログインします。

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 C 失敗します。証明機関を CRL 検証要件が	RL 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 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			
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 [低] を選択
- 認証バインド [+規則の追加] をクリック

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

- 証明書の属性 で [証明書の発行者] を選択
- [証明書の発行者] に先に登録した証明機関を選択
- [認証強度] に [多要素認証] を選択

※本構成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 [低] を選択

※本構成では証明書の別名(UPN) と Entra ID ユーザーの userPrincipalName 属性でバインド するため、「低」 を指定しています。

● [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) 🕕
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
<u>追加</u> キャンセル

● [保存] をクリック

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 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。

Microsoft Entra 管理センター にログインします。

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 [PrincipalName] を選択
- [ユーザー属性] に [userPrincipalname] を選択

※本構成では証明書の別名(UPN) をEntra ID ユーザーのUserPrincipalName 属性と突合して 認証します。

※証明書フィールド、ユーザー属性のマッピングの他の組み合わせは、Microsoft社の情報をご参照ください。

プライベート認証局 Gléas ホワイトペーパー Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

● [追加] をクリック

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	$\sim$
アフィニティ バインド	
低	$\sim$
ユーザー属性*	
userPrincipalName	$\sim$
<u>追加</u> キャンセル	

● [保存] をクリック

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 3.4. 条件付きアクセスを構成

アプリケーションへのアクセスに証明書ベース認証を強制するための設定を行います。

※条件付アクセスの利用には Entra ID Premium P1 または P2 ライセンスが必要となります。

# 3.4.1.セキュリティの規定値群の無効化

「条件付きアクセス」機能を有効化するため、セキュリティの規定値群設定を無効化し ます。

Microsoft Entra 管理センター にログインします。

メニュー [ホーム] > [概要] を選択し、[プロパティ] タブを選択します。

- [セキュリティの規定値の管理] をクリック
- [セキュリティの規定値群] に [無効] を選択
- [無効にする理由] に [組織では、条件付きアクセスの使用を計画しています] を選 択
- [条件付きアクセス ポリシーを有効にして、セキュリティの既定値群を置き換えます] をチェック
- [保存] をクリック
- 確認ダイアログで [無効化] をクリック

# Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

セキュリティの既定値群 ×
セキュリティの既定値群 (無効)
▲ セキュリティの既定値群が無効になっている場合、組織は ID 関連の一 般的な攻撃に対して脆弱です。
多要素認証を使用すると、アカウント侵害の 99.9% を停止させることができ ます。これは、セキュリティの既定値群によって提供される機能です。
Microsoft のセキュリティ チームによると、セキュリティの既定値群を有効にする ことで侵害率に 80% の低下が見られます。
無効にする理由 * このフィードバックは Microsoft の製品とサービスの改善に使用されます。 プラ イバシーに関する声明の表示 ♂
○ 多要素認証のサインアップ要求が多くなり過ぎる
○ サインイン情報の多要素認証チャレンジが多くなり過ぎる
○ 自分の組織でアプリまたはデバイスを使用できない
● 組織では、条件付きアクセスの使用を計画しています
条件付きアクセス ポリシーを有効にして、セキュリティの既定値群を 置き換えます
○ その他
<b>保存</b> キャンセル

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 3.4.2. 認証強度を構成

アプリケーションにアクセスする際に証明書提示を求めるように認証強度を構成します。

Microsoft Entra 管理センター にログインします。

メニュー [保護] > [条件付きアクセス] を選択します。

[認証強度] を選択し、[+新しい認証強度] をクリックします。

[構成] タブを選択します。

- [名前] に 任意の名前を入力
   ※例) "CBA必須"
- [説明] に 任意の説明を入力
   ※例) "証明書ベース認証を強制"
- [証明書ベースの認証 (多要素)] をチェック

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

新しい認識	証強度	)
構成 レビ	а-	
名前*		
CBA 必須		
説明		
証明書ベーン	ス認証を強制	
▶ 認証の	組み合わせの検索	
□ ~	<b>フィッシングに強い</b> MFA (3)	
	Windows Hello for Business	
	パスキー (FIDO2) 詳細設定オプション	
	証明書ベースの認証 (多要素) 詳細設定オプション	
前へ	次へ	

- 証明書ベース認証(多要素)の[詳細設定オプション]をクリック
- [テナント内の証明機関からの証明書の発行者]から3.1項で作成した認証局を選択
- [保存]をクリック

証明書ベースの認証 ×
構成すると、サインイン時に、許可されている証明書発行者と許可されたポリシー OID の いずれかが必要になります。 詳細 ☑
テナント内の証明機関からの証明書の発行者
O="JCCH Security Solution Systems Co., Ltd.", DC=com, DC=jcch-sss, CN=JCCH-SS 🗸
または
SubjectKeyldentifier 別の他の証明書の発行者 十
AND
カスタム ポリシー OID 十
前へ保存

- [次へ] をクリックして [レビュー] タブに遷移
- [作成]をクリック

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 3.5. アプリケーションの登録

Entra ID にエンタープライズ アプリケーションを登録します。

Microsoft Entra 管理センター にログインします。

メニュー [アプリケーション] > [エンタープライズ アプリケーション]を選択します。

[すべてのアプリケーション] を選択し、[+新しいアプリケーション] をクリックします。

[Microsoft Entra ギャラリーを参照する] で [+独自のアプリケーションの作成] をク

リックします。

- [お使いのアプリの名前は何ですか?] に任意の名前を入力
   ※ここでは 2.1 項の [アプリケーション名] を入力
- [アプリケーションでどのような操作を行いたいですか?] に [ギャラリーに見つか

らないその他のアプリケーションを統合します]を選択

● [作成] をクリック

独自のアプリケーションの作成 ×
№ 7ィードバックがある場合
独自のアブリケーションを開発している場合、アブリケーション プロキシを使用している場合、またはギャラリーに ないアブリケーションを統合する必要がある場合は、ここで独自のアブリケーションを作成できます。
お使いのアプリの名前は何ですか?
アプリケーションでどのような操作を行いたいですか?
<ul> <li>オンプレミスのアプリケーションへのセキュリティで保護されたリモート アクセス用のアプリケーション プロキシ を構成します</li> </ul>
○ アプリケーションを登録して Microsoft Entra ID と統合します (開発中のアプリ)
● ギャラリーに見つからないその他のアプリケーションを統合します (ギャラリー以外)
fend

# アプリケーションが登録されました。

戦 エンタープライズ アプリケーション	既要 …	
■ 概要	ペープロパティ	
(1) デプロイ計画	名前①	
★ 問題の診断と解決	S	
管理	アプリケーション ID ①	
1 วือパティ		
A 所有者		
🚨 ロールと管理者		
🎎 ユーザーとグループ	Getting Started	
Э シングル サインオン		
プロビジョニング	👤 1。ユーザーとグループの割り当て	∋ 2。シングル サインオンの設定
🐻 アプリケーション プロキシ	特定のユーザーおよびグループにアプリケーション	ユーザーが自分の Microsoft Entra 資格情報 を使用して、アプリケーションにサインインできるよう
📀 セルフサービス	へのアクセスを付与 ユーザーとグループの割り当て	
🧧 カスタム セキュリティ属性		作業の開始
セキュリティ		
● 条件付きアクセス	③ 3. ユーザー アカウントのプロビジョーング	4. 冬件付きアクヤフ
🔒 アクセス許可	アプリケーションでユーザー アカウントを自動的	カスタマイズ可能なアクセス ポリシーによる、この
♥ トークンの暗号化	に作成および削除 作業の開始	アプリケーションへの安全なアクセス。 ポリシーの作成
アクティビティ		
サインイン ログ		
前 使用状況と分析情報	G 5. tu 7 tu - tu 7	
国 監査ログ	ユーザーが Microsoft Entra 資格情報を使用	
🔓 プロビジョニング ログ	してアプリケーションへのアクセスを要求できるよう にする	
📁 アクセス レビュー	作業の開始	
トラブルシューティング + サポート		
新しいサポート リクエスト	What's New	
	Sign in charts have moved! The new Insights view shows sign in info along with ot Delete Application has moved to Properties You can now delete your application from the Propertie	her useful application data. View insights
	Getting started has moved to Overview The Getting Started page has been replaced by the ste	ps above

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 3.5.1. アプリケーションに SSO を構成

登録したアプリケーションにシングルサインオンを構成します。

シングルサインオンの設定 [作業の開始] をクリックします。



### シングル サインオン方式の選択 画面で [SAML] を選択し、「SAML によるシングル

サインオンのセットアップ」画面に遷移します。

↑ メタデータ ファイルをアップロードする り シングル サー	<b>(ンオン モードの変更</b> 🛛 このアプリケーションをTest │ …
SAML によるシングル サインオンのセット	アップ
フェデレーション プロトコルに基づく SSO 実装により、セキュリラ OpenID Connect または OAuth が使用されていない既存 い。詳細については、こちらをご覧ください。	Fィ、信頼性、エンド ユーザー エクスペリエンスが向上し、実装が容易になります。 Fのアプリケーションの場合は、できるだけ SAML シングル サインオンを選択してくださ
以下をお読みください 構成ガイド 🕑 SAMLデモアプリ を統合	きするためのヘルプ。
<ol> <li>基本的な SAML 構成</li> </ol>	
識別子 (エンティティ ID)	必須
応答 URL (Assertion Consumer Service URL)	必須
サインオン URL	省略可能
リレー状態 (省略可能)	省略可能
ログアウト URL (省略可能)	省略可能

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

[メタデータファイルをアップロードする] をクリックします。

- 2.4 項でダウンロードした SAML SP メタデータを選択
- [追加] をクリック

↑ メタデータ ファイル	レをアップロードする 🏷 シングル サインオン モードの変更 淫 このアプリケーションをTest 🕴 ・・・
メタデータ ファイノ	レをアップロードします。
以下のフィールドの値 ファイルが SAMLデモ	は SAMLデモアプリ によって提供されます。 値を手動で入力することもできますし、 構成済みの SAML メタデータ ·アプリ によって提供されている場合にはそれをアップロードすることもできます。

- [識別子 (エンティティ ID) ] が入力されていることを確認
- [応答 URL (Assertion Consumer Service URL)] が入力されていることを確認
- [サインオン URL (省略可能)] にアプリケーションのサインオン URL を入力
   ※2.1 項の [アプリケーションのサインオン URL] を入力
- [リレー状態 (省略可能)] は入力されていないことを確認
- [ログアウト URL (省略可能)] が入力されていることを確認
- [保存] をクリック
Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

基本的な SAML 構成			
📙 保存 🛛 🔗 フィードバックがある場合			
識別子 (エンティティ ID) * ① Microsoft Entra ID に対してアプリケーションを識別する一意の ID。この値は、Microsoft Ent 一意である必要があります。既定の識別子は、IDP で開始された SSO の SAML 応答の対象ユ	ra ID テナント内ル ーザーになります。	のすべてのアプリケ-	-ションで
		既定	
識別子の追加		V 0	
応答 URL (Assertion Consumer Service URL) * ① 応答 URL は、アプリケーションが認証トークンを受け取る場所です。これは、SAML では *"Asser 呼ばれます。	tion Consume	r Service¥" (A0	CS) とも
	<i>ተ</i> ン…	既定	
応答 URL の追加	0	V 0	
サインオン URL (省略可能) サービス プロバイダーによって開始されたシングル サインオンを実行する場合は、サインオン URL が インイン ページの URL です。ID プロバイダーによって開始されたシングル サインオンを実行する場合	使用されます。 この ふ、このフィールドは	値は、アプリケーシ ・不要です。	ョンのサ
The is at an arranged and an			~
リレー状態(省略可能)① リレー状態は、認証が完了した後にユーザーのリダイレクト先となるアプリケーションを指示します。通知 の場所に移動する URL または URL パスです。 -	常、 <i>値は、ユーザ</i> ー	-をアプリケーションド	内の特定
リレー状態を入力してください			
ログアウト URL (省略可能) この URL は、SAML ログアウト応答をアプリケーションに返送するために使用します。			~

#### [X] をクリックして閉じます。

※エンタープライズ アプリケーションのシングルサインオンのテスト確認が表示されたら [いいえ、
 後で test します] をクリックします。

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

②属性とクレーム [編集]をクリックします。

- [必要な要求]の[一意のユーザー識別子(名前 ID)]の値をクリック
- [名前識別子の形式]に[電子メールアドレス]を選択
- [ソース] に [属性] を選択
- [ソース属性] に [user.userprincipalname] を選択
- [保存] をクリック

	$\times$
ードバックがある場合	
nameidentifier	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims	
電子メール アドレス	$\sim$
● 属性 ○ 変換 ○ ディレクトリスキーマ拡張	
user.userprincipalname	$\sim$
	-ドバックがある場合          nameidentifier         http://schemas.xmlsoap.org/ws/2005/05/identity/claims         電子メール アドレス <ul> <li>属性</li></ul>

# プライベート認証局 Gléas ホワイトペーパー Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

### ● [追加の要求] に以下を設定

名前	名前空間	ソース	ソース属性
name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	属性	user.userprincipalname
surname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	属性	user.surname
givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	属性	user.givenname
emailaddress	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	属性	user.mail

属性とクレーム			×
+ 新しいウレームの追加 + グループ要求を追加する ミミ 列 │ 🖓 フィードバック	がある場合		
必要な要求			
クレーム名	種類	值	
一意のユーザー識別子 (名前 ID)	SAML	user.userprincipalnam…	•••
追加の要求			
クレーム名	種類	值	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	SAML	user.mail	•••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname	•••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname	•••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname	•••
✓ 詳細設定			

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

③SAML 証明書 [トークン署名証明書]の[編集]をクリックします。

- [署名オプション] に [SAML 応答とアサーションへの署名]を選択
- [署名アルゴリズム] に [SHA-256] を選択
- [通知の電子メールアドレス] は未使用なのでそのまま
- [保存] をクリック

SAML 署名証明書 お使いのアプリに対して発行される SAML トークンに署名するために Microsoft Entra ID によって使用される証明書を管理します。				
🗄 保存 🕇 新し	い証明書 🕇 証明書	わインボート 🛛 📈 フィードバックがある場合		
状態	有効期限	拇印		
アクティブ				
署名オプション		SAML アサーションへの署名	$\sim$	
署名アルゴリズム		SHA-256	$\sim$	
通知の電子メールフ	アドレス			
			Ĩ	

プライベート認証局 Gléas ホワイトペーパー Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

● [アプリのフェデレーション メタデータ URL] をコピーして保存しておく

	成ガイド 🗗 SAMLデモアプリ を統合す	るためのヘルプ。	
基本的な S	AML 構成		/2 ¥E
識別子 (エン 応答 URL ( RL) サインオン UI リレー状態 (・ ログアウト UF	구·구구 ID) Assertion Consumer Service U 입 웹 (首略可能) 입 (首略可能)	https:// https:// https:// <i>首和可能</i> https://	
属性とクレー	لم		<i>0</i> #
givenname surname emailaddre name 一意のユーサ	2 255 F— ID	user.givenname user.surname user.mail user.userprincipalname user.userprincipalname	
有効期限 通知用メール アプリのフェデ 証明書 (Ba 証明書 (未) フェデレーショ	, レーション メタデータ URL se64) 加工) ン メタデータ XML	https://login.microsoftonline.com/d2b7c5b8… で ダウンロード ダウンロード ダウンロード	]
<b>検証証明書</b> 必須 アクティブ 有効期限切	(オプション) N	いいえ 0 0	<i>0</i> 編
SAMLデモフ	アプリ のセットアップ		
Microsoft E ログイン URL	Entra ID とリンクするアプリケーションを材 -	構成する必要があります。 https://login.microsoftonline.com/d2b7c5b8… 『ハ	]
Microsoft E	Entra 識別子	https://sts.windows.net/d2b7c5b8-3049-41 ··· 🕅	]
-	RL	https://login.microsoftonline.com/d2b7c5b8… Ph	

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

3.5.2.アプリケーションにユーザーを割り当て

登録したアプリケーションにセキュリティグループを割り当て、ユーザーが利用できる

ようにします。

[ユーザーとグループの割り当て] をクリックします。



ユーザーとグループ 画面で [+ユーザーまたはグループの追加] をクリックします。

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

● 3.2 項で作成したセキュリティグループを選択

割り当ての追加 … JCCHセキュリティンリューションシステムズ
▲ アプリケーションにグループを割り当てると、そのグループ内の直接のユーザーだけがアクセスできるようになります。割り当ては、入れ × 子になったグループにカスケードされません。
ユーザーとグループ 1 個のグループが選択されました。 ロールを選択してください User
割り当て

● [割り当て]をクリック



アプリケーションにセキュリティグループが割り当てられました。

🕂 ユーザーまたはグループの追加 🛛 🖉	割り当ての編集 📋 削除 🔑 🕽	負格情報の更新 │ 〓〓 列 │ ・・・		
アプリケーションは、割り当てられたユーザ- ーザーに表示しますか?]を[いいえ]に認	-のマイ アプリ内に表示されます。これを表示 注定します。	〒しないようにするには、プロパティの中で [ユ →		
ここで、アプリケーションのアプリのロールにユーザーとグループを割り当てます。このアプリケーションの新しいアプリのロールを作成するには、 アプリケーション登録を使用します。				
♀ 最初の 200 件を表示しています。すべてのユ…				
表示名	オブジェクトの種類	割り当てられたロール		
EC Entra CBA グループ	グループ	User		

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

### 3.5.3.アプリケーションへのアクセスポリシーを構成

登録したアプリケーションに条件付きアクセスを割当て、証明書ベース認証を強制しま

す。

条件付きアクセス [ポリシーの作成] をクリックします。



条件付アクセス 画面で [+新しいポリシー] をクリックします。

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

- [名前] に 任意の名前を入力
   ※例) "CBA 強制ポリシー"
- 作成した認証強度を選択して[選択]をクリック
- 割り当て [ユーザー]で3.2項で作成したグループを選択
- 割り当て [ターゲットリソース]で対象アプリケーションが選択済みなことを確認
- 割り当て [ネットワーク]でアクセス元ネットワークを選択
   ※例) 任意のネットワークまたは場所
- 割り当て [条件]の[デバイスプラットフォーム] でアクセス元デバイスを選択
   ※例) Windows、iOS、Android、macOS
- 割り当て [条件]の[クライアントアプリ] でアクセス元アプリを選択
   ※例) ブラウザー
- アクセス制御 [許可] で[認証強度が必要] をチェックして、3.4.2項で構成した認証
   強度を選択
- ポリシーの有効化 [オン] を選択
- [作成] をクリック

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

新規 … 条件付きアクセス ボリシー
シグナルを統合し、意思決定を行い、組織のポリシーを 適用するために、条件付きアクセス ポリシーに基づいて アクセスを制御します。 詳細情報 🖉
名前 * CBA 強制ポリシー  V
割り当て
<b>ユ−ザ−</b> ①
組み込まれた特定のユーザー
ターゲット リソース ①
1 個のリソースが含められました
ネットワーク 新規 ①
任意のネットワークまたは場所
 条件 ①
3 個の条件が選択されました
アクセス制御
許可 ①
1 個のコントロールが選択されました
セッション ①
0 個のコントロールが選択されました
ポリシーの有効化
レポート専用 (オン) オフ
作成

# プライベート認証局 Gléas ホワイトペーパー Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

アプリケーションにアクセスポリシーが構成されました。

十 新しいポリシー	┼ 新しいポリシーをテンプレートから	う  ポリシー ファイルの	のアップロード <i>Ș</i>	🔾 What If 🕐 最新の情報に更新	r マレビュー機能	
Microsoft Entra 条件作	けきアクセス ポリシーは、アクセスの制御	を適用して組織のセキュリ	ティを維持するため	りに使用されます。 詳細 🛛		
すべてのポリシ	Microsoft マネージド ポリシー					
-	<b>9</b> 3					
4	(全 4 項目中)					
合計						
♀ 検索		T	· フィルタ 一の追加			
4個のボリシーのうち	5 4 個が見つかりました					
ポリシー名		タグ	状態	アラート	作成日	更新日
Multifactor authenti	ication for all users	MICROSOFT マネージド	オン		2024/11/13 18:27:46	
Block legacy authen	tication	MICROSOFT マネージド	オン		2024/11/13 18:27:41	
Multifactor authenti	ication for admins	MICROSOFT マネージド	オン		2024/11/13 18:27:35	
CBA 強制ポリシー			オン		2024/11/14 12:48:49	

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

## 4. Web サーバの設定

### 4.1. SAML IdP メタデータを Web サーバに登録

Webサーバで、Entra IDから SAML IdP メタデータをダウンロードします。

※以下のコマンドで 2.1 項の [SAML IdPメタデータのパス] に配置 ※IdPメタデータURL は3.5.1 項で取得した [アプリのフェデレーション メタデータ URL] を使用

curl -o /etc/httpd/conf/idp-metadata.xml [IdP メタデータ URL] chmod 644 /etc/httpd/conf/idp-metadata.xml

### 4.2. Web サーバ起動

準備ができたらWeb サーバを起動します。

これによりWebサーバは SAML SP として動作します。

※以下のコマンドで Webサーバを起動

sudo systemctl enable httpd sudo systemctl start httpd

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 5. AP サーバの設定

APサーバを設定します。

※本手順は、APサーバに Node.js がインストールされていることが前提となります。

### 5.1. 構成

検証用アプリケーションの構成を決めます。

Listen tcpポート番号	3000
ログインユーザー表示	認証済みEntra ID のユーザー プリンシパル名を出力
ログアウトリンク表示	Single Logout Service へのリンクを出力
	リンクを踏むとログアウト後、Rootパスヘリダイレクト
その他	HTTPリクエストヘッダを出力

#### Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

### 5.2. 実装

アプリケーションを Node.js で実装します。

```
※以下のコマンドで 5.1 項の構成に準じたアプリケーションを実装
```

```
cat << 'EOS' > /usr/local/src/saml demo app.is
"use strict";
const http = require("http");
const listen_port = 3000;
const slo_path = "/saml/saml_demo_app/logout";
const return_to = "https://sp.jcch-sss.com/";
const server = http.createServer((request, response) => {
     var headers = '
     Object.keys(request.headers).forEach((key) => {
       headers = headers + `${key}: ${request.headers[key]}¥n`
     });
     response.writeHead(200, {"Content-Type": "text/html; charset=UTF-8",
"Cache-Control": "no-cache"});
     response.write(`¥
<html><body>¥n¥
   <h1>Welcome! </h1>¥n¥
  <h4>${request.headers["x-auth-user"]}</h4>¥n¥
<a href='${slo_path}?ReturnTo=${return_to}'>Logout</a>¥n¥
  <h3>Request Header</h3>
  ¥
     ${headers}¥
¥n¥
</body></html>¥n¥
`);
     response.end();
});
server.listen(listen_port);
console.log(`The server has started and is listening on port : ${listen_port}`);
EOS
chmod 644 /usr/local/src/saml_demo_app.js
```

### 5.3. AP サーバ起動

node /usr/local/src/saml\_demo\_app.js

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 6. Gléas の設定

### 6.1. 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納品時等に弊社で設定を既におこなっている	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
別名 (プリンシパル名)	アカウント (プリンシパル名)

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

### 6.2. 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]メニューから[上級者向け設定」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
- [アップロードする]にローカルの CSV ファイルを選択

※CSV ファイルは以下の形式

列名	値
cn	アカウント名
	※証明書のサブジェクトー般名となります
	※UA のログインユーザ ID となります
sn	名前 (姓)
givenname	名前 (名)
password	パスワード
	※UA のログインパスワードとなります
upn	プリンシパル名
	※証明書の別名 (UPN) となります
	※Entra ID のユーザー プリンシパル名と一致させてください

● [作成]をクリック

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

▶アカウント情報		日上級者向け設定
>アカウント名 📩		
> 初期グループ	なし	
	■ここをクリックしてユーザを参加させるグループを選択	
> その他の設定	☑ 証明書を発行する	
	□ 連続して登録を行う	
▶種類 ○ ユーザ ○ コン	ミュータ ○ サーバ ○ 認証局 ◉ CSVファイルー括登録 ○ LDAP	
> アップロードするファイル	ファイルの選択 upload.csv	
	作成	

### ● 内容を確認し[実行]をクリック

🕂 インボート内容の確認				
指定したファイルの内容 指定されたファイルの最初の9件を表示してい 下部の「実行」ボタンを押すと、以下のファイ、	います。 ルの内容がアナ	コウント登録申請	者一覧に反映されます。	
▶指定されたファイルの最初の9件				
アカウント名	姓	名	メールアドレス	プリンシバル名
The second second second second second				
				全 9件

▶このファイルで間違いがなければ「実行」ボタンを押してください。

実行

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

[アカウント]>[登録申請者一覧]メニューを選択します。

※しばらくするとアップロードしたユーザ情報がアカウント登録申請として登録されます

- [全て許可する」をクリック
- [実行]をクリック



CSV の内容が Gléas アカウントとしてインポートされます。

※しばらくするとアップロードしたアカウントに対してクライアント証明書が自動的に発行されます

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

### 6.3. 証明書の配布設定 (Windows 向け)

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

▶基本設定	▶上級者向け
<ul> <li>トーグンへのインボート</li> <li>         ご即書ストアへのインボート         ダウンロードを許可         ダウンロード可能時間(分)         1         CA証明書を含めない         </li> </ul>	<ul> <li>管理するトークン Gemalto NETカード ▼</li> <li>証明書ストアの種類 ユーザストア ▼</li> <li>インボートワンスを利用する</li> <li>登録申請を行わない</li> <li>登録常請みデバイスのみインボート許可</li> </ul>
	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 を使用したシングルサインオン (SAML 連携)

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 を使用したシングルサインオン (SAML 連携)

### 6.4. 証明書の配布設定 (iPhone 向け)

GléasのUA (申込局) より発行済み証明書を iOS 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]部分で以下の設定を行います。

● [ダウンロードを許可]をチェック

UA 申込局

● [ダウンロード可能時間(分)]の設定・[インポートワンスを利用する]にチェック

この設定を行うと、GléasのUAからインポートから指定した時間 (分) を経過した後は、 構成プロファイルのダウンロードが不可能になります(インポートロック機能)。これ により複数台のデバイスへの構成プロファイルのインストールを制限することができま

す。

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

▶基本設定	日上級者向上
□ トークンへのインボート	管理するトークン Gemalto .NETカード 🗸
□ 証明書ストアへのインポート	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) 1	<ul> <li>✓ インボートワンスを利用する</li> <li>✓ 登録申請を行わない</li> <li>● 登録済みデバイスのみインボート許可</li> </ul>
<ul> <li>CA証明書を含めない</li> </ul>	
(i	禄存

設定完了後、[保存]をクリックし保存します。

[認証デバイス情報]の[iPhone/iPadの設定]までスクロールし、[iPhone/iPad用UAを利

用する]をチェックします。

🧳 認証デバイス情報		
▶ iPhone / iPadの設定		
🗌 iPhone/iPad 用 UA を利用する		
	保存	

構成プロファイルに必要となる情報の入力画面が展開されるので、以下設定を行います。

【画面レイアウト】

- [iPhone用レイアウトを利用する]をチェック
- [ログインパスワードで証明書を保護]をチェック

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

【iPhone構成プロファイル基本設定】

● [名前]、[識別子]に任意の文字を入力 (必須項目)

🦸 認証デバイス情報		
▶iPhone / iPadの設定		
🔽 iPhone/iPad 用 UA を利	用する	
画面レイアウト		
✓ iPhone 用レイアウトを使 ○ Mac OS X 10.7以降の持	閉する ✓ ログインパスワードで証明書を保護 意徳を許可	
OTA(Over-the-air)		
OTAエンロールメントを利	川用する 🗌 接続する iOS デバイスを認証する	
OTA用SCEP URL		
OTA用認証局	デフォルトを利用	
iPhone 構成プロファイル基	基本設定	
名前(デバイス上に表示)	サンブルプロファイル	
識別子(例: com.jcch-	local.jcch-sss.profile	
プロファイルの組織名	JCCHセキュリティ・ソリューション・システムズ	
記名日	サンブル構成プロファイル	

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 を使用したシングルサインオン (SAML 連携)

### 6.5. 証明書の配布設定 (Android 向け)

GléasのUA (申込局) より発行済み証明書を Android 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

UA 申込局 ▶<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]部分で以下の設定を行います。

● [ダウンロードを許可]をチェック

● [ダウンロード可能時間(分)]の設定・[インポートワンスを利用する]にチェック

この設定を行うと、GléasのUAからインポートから指定した時間(分)を経過した後は、

証明書ファイルのダウンロードが不可能になります (インポートロック機能)。これに

より複数台のデバイスへの証明書ファイルのインストールを制限することができます。

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

▶基本設定	□上級者向辻
□ トークンへのインボート	管理するトークン Gemalto .NETカード 🗸
□ 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) 1	<ul> <li>✓ インボートワンスを利用する</li> <li>✓ 登録申請を行わない</li> <li>● 登録済みデバイスのみインボート許可</li> </ul>
<ul> <li>CA証明書を含めない</li> </ul>	
	保存

設定完了後、[保存]をクリックし保存します。

[認証デバイス情報]の[Androidの設定]までスクロールし、[Android用UAを利用する]を

チェックします。

▶ Android の設定
✓ Android 用 UAを利用する
ダウンロードの動作
<ul> <li>□ ログインパスワードで証明書を保護</li> <li>☑ 数字のみの PIN を表示</li> <li>証明書ダウンロードの種類</li> <li>○ PKCS#12ダウンロード</li> </ul>
保存

証明書のダウンロードに必要となる情報の入力画面が展開されるので、以下設定を行い

ます。

- [数字のみのPINを表示]をチェック
- [証明書ダウンロードの種類]]を[PKCS#12ダウンロード]を選択

各項目の入力が終わったら、 [保存]をクリックします。

プライベート認証局 Gléas ホワイトペーパー Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 7. クライアントの設定

7.1. Windows にクライアント証明書をインポート

PCのブラウザ (Edge) で、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。

●エンドユーザログイン [UA]
●ユーザID、パスワード巻入力して口 ダインしてくだきい。
▶ユーザID
▶パスワード
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。

$\rightarrow$ C $\bullet$				Α	1 6 0	₲   🧔	٠
				5	プライベートCA	Gléäs	Ŝ UA
スト ユーザー さ	ふんのページ]						バアウト
ユーザ情報						-	-
📿 テスト ユーザ・	ーさんのページ						
							_
▶ ユーザ情報							
<b>2 ユーザ情報</b> ···· ▶ ユーザ		登録日時:					
<ul> <li>▶ ユーザ情報 ····</li> <li>▶ ユーザ</li> <li>&gt; 姓: テスト 名: ユ</li> </ul>	L-ザ-	登録日時:					
<ul> <li>2 ユーザ情報</li> <li>▶ ユーザ</li> <li>&gt; 姓: テスト 名: ユ</li> <li>&gt; ユーザID:</li> </ul>	レーザー	登録日時:					
★ ユーザ情報・・・・ ★ ユーザ ★ は: テスト 名: ユ ★ ユーザID: ★ パンワード・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	1- <del>1</del> -	登録日時:					
▶ ユーザ情報・・・・ ▶ ユーザ > 姓: テスト 名: ユ > ユーザID: > メールアドレス: > パスワード: ************************************	iーitー	登録日時:					
・ユーザ情報・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	1ーザー	<b>瓷品曰時:</b>					
2 ユーザ情報・・・ ・ ユーザ ・ シューザ ・ シューザロ: ・ メールアドレス: ・ パスワード: ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	Lーザー 	<b>瓷品口時:</b>					
ユーザ情報・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	1ーザー  発行局	<b>瓷品曰時:</b>	 ) ) ) ) ) ) ) ) ) )	有効期限	証明書スト	7~42#~⊦	

#### Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

※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	<b>1</b> 警告	$\times$
<u> </u>	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。確認されていない毎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) いいえ(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 (	÷		A" te		٠
			プライ・	х-ьса Gléã	Š UA
テスト ユーザー ;	さんのページ]				ログアウト
ューザ情報 ② テスト ユーサ	fーさんのページ	_	_		~
▲ユーザ情報・	登録日時:				
> 姓: テスト 名: . > ユーザロ: > メールアドレス: > パスワード: ******	J-f-				
<b>業 証明書情報</b> →					
▶ 発行済み証明書					
# <u>\$1</u>	発行局	シリアル #3	有効期限	証明書スドアヘインボート ダウンロード済み	- 1

プライベート認証局 Gléas ホワイトペーパー Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

### 7.2. iPhone にクライアント証明書をインポート

iPhoneのブラウザ (Safari) で、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。



ログインすると、ユーザ専用ページが表示されます。

[ダウンロード]をタップし、構成プロファイルのダウンロードをおこないます。

JETA-PCA Gléas	A JETA-FCA GIÉAS UA	JETR-FCA Gléäs UA
さんのページ	さんのページ	さんのページ
ユーザロ	ユーザID	ユーザロ
姓 ••••••	姓	the Research Class
名	名	名
メール	メール	メール
<b>有効期限</b> ダウンロート ログアク Cepyright (1) 2010-2022 JOCH Scenarty Solution Systems Co., LM. All rights reserv	この Web サイトは構成プロファイルをダウ ンロードしようとしています。許可します か? Add 許可 Copyright (C) 2016-2022 ICCH Security Scholar Systems Co. L.S. All right reserved	有効期 プロファイルがダウンロードされました パンファイルをインストールするには設定 Appで可耐能してください。 別じる

※インポートロックを有効にしている場合は、この時点からカウントが開始されます

### Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

画面の表示にしたがい設定を開くと、プロファイルがダウンロードされた旨が表示され

るので、インストールをおこないます。

設定	キャンセル	プロファイル	インストール
Apple ID、iCloud、メディアと購入		OS Demo Profile	
ダウンロード済みのプロファイル	署名者 <mark>未署名</mark> 說明 內容 <b>証明書(</b>	2)	
	詳細		>
	ダウンロ	ード済みプロファィ	ルを削除

[インストール]をタップして続行してください。

インストール中にルート証明書のインストール確認画面が現れるので、内容を確認し

[インストール]をタップして続行してください。

※ここでインストールされるルート証明書は、通常のケースではGléasのルート認証局証明書になります



インストール完了画面になりますので、[完了]をタップして終了します。

<b>姿</b> 名者 <b>未要名</b> 最明 内容 <b>証明書 (2)</b>		インストール完了	完了
要名者 <b>未要名</b> 武功 内容 <b>証明書 (2)</b>	Ø	JS3 KD5 Demo Profile	
內容 <b>証明書 (2)</b>	署名者 説明	末署名	
	内容	証明書(2)	

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

なお [詳細]をタップすると、インストールされた証明書情報を見ることができます。

必要に応じて確認してください。

< 戻る	JS3 IOS Demo Profile	
証明書	(2)	
0	発行元: 有効期限:	>
0	発行元: 有効期限:	>

Safariに戻り、[ログアウト]をタップしてUAからログアウトします。

以上で、iPhoneでの構成プロファイルのインストールは終了です。

なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より 管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロ ード済み」という表記に変わり、以後のダウンロードは一切不可となります。



プライベート認証局 Gléas ホワイトペーパー Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

### 7.3. Android にクライアント証明書をインポート

Androidのブラウザ (Chrome) で、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。

・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	(ン [UA]
	D、パスワードを入力し インしてください。

ログインすると、ユーザ専用ページが表示されます。

[ダウンロード]をタップし、証明書ファイルのダウンロードをおこないます。

プライ	K-FCA Gléäs UA	プライベ	-pca Gléäs 🔼	プライベートCA	Gléås 🛯
AsseeAD CBA Teel さん	のページ	ネット・ネラ こうみ うっき さんの	)ページ	AnnualD CBA Test さんのページ	\$
ユーザID	aturead chartest	ユーザID	sturned the test	2 ATTORNAL AND IN	1
姓	AzureAD CBA	姓	AzureAD CBA	証明書を抽出	
名	Test	名	Test	証明書を抽出するためのパスワート	ドを入力します。
メール	keigochikt annicraaft.com	メール	etgjor/MR overcrosoft.com		
JCCH-SSS demo2 CA		JCCH-SSS demo2 CA		۲++	ven ok
有効期限	ダウンロード	証明書 PIN: massime	決定 キャンセル	有効期限	ダウンロード
	ログアウト		ログアウト	na an an 1997 ann an 1997 a	ログアウト
Copyright (C) 2010-2022 JCCH Security served.	Solution Systems Co.,Ltd. All rights	Copyright (C) 2010-2022 JCCH Security Sol reserved.	ution Systems Co.,Ltd. All rights	Copyright (C) 2010 2022 JCCH Security Solution Syste reserved.	ms Co.,Ltd. All rights

※「証明書 PIN」の値を「証明書を抽出」のパスワードとして入力します。 ※インポートロックを有効にしている場合は、この時点からカウントが開始されます

[OK]をタップして続行してください。

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

「証明書の種類の用途」のダイアログが出るので、用途を選択します。

J	証明書の種類の選択		
ŧ	● VPN とアプリユーザー証明書 ○ Wi-Fi 証明書		۲ ۲
Cop rest	キャンセル	ОК	

[OK]をタップして続行してください。

JC	この証明書の名前を指定してください	۲
F	証明書名	۲
Cop rest	キャンセル OK	

[OK]をタップします。

Chromeに戻り、[ログアウト]をタップしてUAからログアウトします。

以上で、Androidでの証明書ファイルのインストールは終了です。

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

[設定]>[セキュリティ]>[詳細設定]>[暗号化と認証情報]>[ユーザー認証情報]>[証明書 の名前]とタップすると、インストールされた証明書情報を見ることができます。必要 に応じて確認してください。



なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より 管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロ ード済み」という表記に変わり、以後のダウンロードは一切不可となります。

757~-FCA Gleas
さんのページ
and the first
Accessible (State
764
the second se
ダウンロード済み

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 8. 証明書ベース認証によるアプリケーション利用

8.1. Windows デバイスでアクセス

PCのブラウザ (Edge) から2.1項の「アプリケーションのサインオンURL」にアクセスす

ると、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。

び JCCH Security Solution Systems サインイン	
アカウントにアクセスできない場合	次へ
用 変更するときは、AAD管 ランド	理センター > 会社のブ
🔍 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	
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	
	サインイン

プライベート認証局 Gléas ホワイトペーパー Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

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 <sup>サイト</sup>		>
では資格情報が必要です:		
証明書情報	ОК	キャンセル

※パスワードを入力しても証明書の提示を強制されます。

[はい]または[いいえ]をクリックすると、サインインしてWebアプリケーションにアク

セスできます。

JCCH Security Solution Sys	items	
サインインの状	態を維持し	っますか?
これにより、サインインをす す。	<sup>えめられる</sup> 回数を	咸らすことができま
🗌 今後このメッセージ	を表示しない	
	いいえ	<u>(±U)</u>
用 変更するとき	きは、AAD管理も	ンター > 会社のブ
### Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

#### ※以下は、アプリケーションにアクセスした例

Welcome!
all developed wells put on one
Logout
Request Header
<ul> <li>host: sp.jcch-ss.com</li> <li>cache-control: max-age=0</li> <li>uprade-inscure-requests: 1</li> <li>user-agent: Mozilla/S10 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36 Edg/130.0.0</li> <li>accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng*/*;q=0.8,application/signed-exchange;v=b3;q=0.7</li> <li>sec-fetch-mde: navigate</li> <li>sec-fetch-mde: navigate</li> <li>sec-fetch-dest: document</li> <li>sec-chua-mobile: 70</li> <li>sec-chua-mobile: 70</li> <li>sec-chua-mobile: 70</li> <li>sec-chua-mobile: 70</li> <li>sec-chua-platform: "Windows"</li> <li>referer: https://login.microsoftonline.com/</li> <li>accept-language: ja,en;q=0.9,en-GB;q=0.8,en-US;q=0.7</li> <li>cookie:</li> <li>rl_group_id=RudderEncrypt%3AU2FsdGVkX19ATVmH0q9nKM8vkjFkmdrjlepLtFSZ36J7Qqy%2FAr3EExxS72MK20V0kMYN2dFylnJvkqaqR1juEA%3D%3D;</li> <li>rl_group_id=RudderEncrypt%3AU2FsdGVkX19ATVmH0q9nKM8vkjFkmdrjlepLtFSZ36J7Qq%2FAr3EExxS72MK20V0kMYN2dFylnJvkqaqR1juEA%3D%3D;</li> <li>rl_group_id=RudderEncrypt%3AU2FsdGVkX19ATVmH0q9nKM8vkjFkmdrjlepLtFSZ36J7Qq%2FAr3EExxS72MK20V0kMYN2dFylnJvkqaqR1juEA%3D%3D;</li> <li>rl_group_id=RudderEncrypt%3AU2FsdGVkX19ATVmH0q9nKM8vkjFkmdrjlepLtFSZ36J7Qq%2FAr3EExxS72MK20V0kMYN2dFylnJvkqaqR1juEA%3D%3D;</li> <li>rl_group_id=RudderEncrypt%3AU2FsdGVkX19ATVmH0q9nKM8vkjFkmdrjlepLtFSZ36J7Qq%2FAr3EExxS72MK20V0kMYN2dFylnJvkqaqR1juEA%3D%3D;</li> <li>rl_group_id=RudderEncrypt%3AU2FsdGVkX19ATVmH0q9nKM8vkjFkmdrjlepLtFSZ36J7Qq%2FAr3EExxS72MK20V0kMYN2dFylnJvkqaqR1juEA%3D%3D;</li> <li>rl_group_id=RudderEncrypt%3AU2FsdGVkX19ATVmH0q9nKM8vkjFkmdrjlepLtFSZ36J7Qq%2FAr3EExxS72MK20V0kMYN2dFylnJvkqaqR1juEA%3D%3D;</li> <li>rl_group_id=RudderEncrypt%3AU2FsdGVkX19AEDIM2gpNiAG0w2FAr3EExKP%3D;</li> <li>rl_sforwarded-Encrypt%3AU2FsdGVkX19AEDIM2gpNiAG0w2FAr3EExKP%3D;</li> <li>rl_isroit_AraudetEncrypt%3AU2FsdGVkX19AEDIM2gpNiAG0w2FAr3EExKP%3D;</li> <li>rl_isroit_AraudetEncrypt%3AU2FsdGVkX19AEDIM2gpNiAG0w2FAr3EExKP%3D;</li> <li>rl_isroit_AraudetEncrypt%3A</li></ul>

#### Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

### 証明書を持っていない場合や、失効済み証明書を提示した場合はアクセスに失敗します。

#### ※以下は失効されたクライアント証明書でアクセスした例



Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

## 8.2. iPhone デバイスでアクセス

iPhoneのブラウザ (Safari) から2.1項の「アプリケーションのサインオンURL」にアク

セスすると、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タップします。

サインイン
アカウントにアクセスできない場合
次へ
用 変更するときは、AAD管理センタ — > 会社のプランド
🔍 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]をタップします。

クライアント証明書を選択して[選択]をタップします。

~	-
パスワードの入力	" (c (t
パスワード	クライアント証明書が必要です このWebサイトに接続するときに使用する
パスワードを忘れた場合	証明書を選択してください。
証明書またはスマート カードを使用する	an ann faor sarflach s
サインイン	
用 変更するときは、AAD管理センタ - > 会社のブランド	キャンセル

※デバイス内に証明書が1つのみ場合、証明書の選択画面はスキップ

#### Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

[はい]または[いいえ]をタップすると、サインインしてWebアプリケーションにアクセ

#### スできます。

サインインの状態を維持します か2
<b>ノ</b> ^・ 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>
用 変更するときは、AAD管理センタ ー > 会社のブランド

#### ※以下は、アプリケーションにアクセスした例

#### Welcome!

#### Logout

#### Request Header

- host: sp.jcch-sss.com
- accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8
- · sec-fetch-site: cross-site
- priority: u=0, i
- sec-fetch-mode: navigate
- user-agent: Mozilla/5.0 (iPhone; CPU iPhone OS 18\_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.0 Mobile/15E148 Safari/604.1
- accept-language: ja
- sec-fetch-dest: document
- referer: https://login.microsoftonline.com/
- accept-encoding: gzip, deflate, br
  cookie: mellon-cookie=830f79d53332dc5fd2f99a45b4ef9ab8
- x-auth-user:
- x-forwarded-proto: https
- x-forwarded-port: 443
- x-forwarded-for:
- x-forwarded-host: sp.jcch-sss.com • x-forwarded-server: sp.jcch-sss.com
- connection: Keep-Alive

#### Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

### 証明書を持っていない場合や、失効済み証明書を提示した場合はアクセスに失敗します。

#### ※以下は失効されたクライアント証明書でアクセスした例



Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

## 8.3. Android デバイスでアクセス

Adroidのブラウザ (Chrome) から2.1項の「アプリケーションのサインオンURL」にア

クセスすると、Entra ID のサインイン画面に遷移します。

[ユーザー名]を入力して次へをタップします。



クライアント証明書を選択して[選択]をタップします。

証明書の選択			
アプリChromeから証明書がリクエストされま した。証明書を選択すると、今後アプリはサー バーに対してこのIDを利用できるようになりま す。 アプリはリクエストしているサーバーを			
として識別しまし たが、アプリを信頼している場合にのみ、証明書 へのアクセス権をアプリに許可してください。			
0			
۲			
	拒否	選択	

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

[はい]または[いいえ]をタップすると、サインインしてWebアプリケーションにアクセ

### スできます。

11 March 2017 10 March 2017
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>
用 変更するときは、AAD管理センタ ー > 会社のブランド

※以下は、アプリケーションにアクセスした例

Welcome!	
Logout	
Request Header	
<ul> <li>host: sp.jcch-sss.com</li> <li>cache-control: max-age=0</li> <li>upgrade-insecure-requests: 1</li> <li>user-agent: Mozilla/5.0 (Linux; Android 10; K)</li> <li>AppleWebKit/537.36 (KHTML, like Gecko)</li> <li>Chrome/130.0.0.0 Mobile Safari/537.36</li> <li>accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif exchange;v=b3;q=0.7</li> <li>sec-fetch-site: cross-site</li> <li>sec-fetch-idest: document</li> <li>sec-ch-ua-mobile: ?1</li> <li>sec-ch-ua-mobile: ?1</li> <li>sec-ch-ua-platform: "Android"</li> <li>referer: https://login.microsoftonline.com/</li> <li>accept-language: ja-JP,ja;q=0.9,en-US;q=0.7</li> <li>cookie: mellon- cookie: mellon- cookie: mellon-</li> <li>x-auth-user:</li> </ul>	image/webj
<ul> <li>x-forwarded-proto: https</li> <li>x-forwarded-port: 443</li> <li>x-forwarded-for:</li> <li>x-forwarded-host: sp.jcch-sss.com</li> <li>x-forwarded-server: sp.jcch-sss.com</li> </ul>	

#### Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

### 証明書を持っていない場合や、失効済み証明書を提示した場合はアクセスに失敗します。

#### ※以下は失効されたクライアント証明書でアクセスした例



Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

9. その他

### 9.1. ユーザー情報をアプリケーションに伝える

本書の構成では、Entra ID ユーザー情報がアプリケーションに連携されます。

• Entra ID がSAML認証応答を発行

認証が成功すると、Entra ID はSAML認証応答を発行します SAML認証応答のメッセージには認証済みユーザー情報が含まれます メッセージには名前IDとして Entra ID のユーザー プリンシパル名が記載されます ※その他 [追加の要求] として他のユーザー情報も送信可能です (3.5.6項の「属性とクレー ム」)

WebサーバがSAML認証応答を受け取る

WebサーバはSAML認証応答から取り出したユーザー情報をリクエストヘッダに追加します リクエストヘッダを追加したHTTPリクエストをアプリケーションにリバースプロキシします ※設定例は 2.5 項を参照

● アプリケーションがユーザー情報を受け取る

リクエストヘッダからユーザー情報を取り出すことができます ※実装例は 5.2 項を参照



Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

## 9.2. サインインログについて

証明書ベース認証の状況は、Entra ID のサインイン ログから確認することができます。

Microsoft Entra 管理センター にログインします。

メニュー [アプリケーション] > [エンタープライズ アプリケーション]を選択します。

[すべてのアプリケーション] から対象のアプリケーションを選択します。

[サインイン ログ] をクリックするとログが一覧表示されます。

一覧からは以下を確認することができます。

ユーザー	サインインしたユーザー
アプリケーション	アクセスしたアプリケーション
状態	成功:認証が成功したログ
	失敗:認証が失敗したログ
	中断:証明書を要求しているログ
IPアドレス	アクセス元IPアドレス

証明書を要求しているログは [状態] が中断となっているのでログを選択すると、

[アクティビティの詳細:サインイン] から以下を確認できます。

基本情報	基本情報 許可された時刻 アクセス日時			
	ユーザー	アクセスしたユーザー		
	アプリケーション	アクセスしたアプリケーション		
場所	IPアドレス	アクセス元IPアドレス		
デバイス情報	ブラウザ	アクセスブラウザの種類		
	オペレーティングシステム	アクセスOSの種類		
認証の詳細	認証方法	証明書認証のときは X.509 Certificate		
	成功	true なら認証成功		
追加の詳細	ユーザー証明書の***	認証時に提示された証明書情報		

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

## 9.3. 証明書の失効確認について

証明書ベース認証は、証明書の失効を確認するために証明書失効リスト(CRL)を使用しま

す。 (OCSPはサポートされていません)

3.1項で登録した [証明書失効リストのURL] からCRLをダウンロードしてキャッシュし ます。CRLの有効期間が切れると最新のCRLを再ダウンロードしてキャッシュを更新し ます。

証明書ベース認証は、このキャッシュされたCRLを用いて失効確認を行うため、認証局 での証明書失効操作は即時反映されません。

認証局管理者	証明書#1失効操作 CRL#2	に掲載			
Gléås	CRL#2発行 CRL番号 #1	CRL#1有効期阻 CRI	Q CRL#3発行	CRL#2有効期 CR	限
<b></b>			CRL#2キャッシュ		CRL#3キャッシュ
Azure Active Directory	CRL番号 #1		CRL番号 #2		CRL番号 #3
	証明書#1 有効		証明書#1 失効		

※失効操作が失効確認に反映されるまでのイメージ

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

### 9.4. 失効の即時反映について

証明書ベース認証では、手動操作による失効リストの即時反映が行えません。

利用者がデバイスを紛失したなどの理由で即時の失効が運用上必要な場合、Entra ID 上

でユーザーの認証トークンを無効化することでアクセスを無効にする方法が考えられま

す。

認証を無効化してサインインを停止するコマンド例

● PowerShell を起動

※以降の操作の前に Microsoft Graph SDK をインストールが必要です。

Install-Module Microsoft.Graph

● 適切な資格情報で MgGraph サービスに接続

Connect-MgGraph -Scopes User.ReadWrite.All

● 認証トークンの無効化

Revoke-MgUserSignInSession -UserId [ユーザー プリンシパル名]

※この操作で現在の認証が無効化されます

● サインインを停止

Update-MgUser -UserId [ユーザー プリンシパル名] -AccountEnabled:\$False

※この操作で指定ユーザーのサインインが禁止されます

Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

## 9.5. 失効リストのサイズ制限について

証明書ベース認証で扱える失効リスト (CRL) は 20MB のサイズ制限があります。

失効リストに記載される失効情報は、該当証明書の有効期限まで記載され続けるため、

有効期間が長い証明書を運用する場合には失効リストの肥大化にもご留意ください。

プライベート認証局 Gléas ホワイトペーパー Microsoft Entra CBA を使用したシングルサインオン (SAML 連携)

# 10.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