

Microsoft Entra CBAによるMicrosoft 365ログイン

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 Microsoft 365 ログイン

目次

| 1. | はじめ | 51 - |
|----|---------|-------------------|
| | 1.1. | 本書について |
| | 1.2. | 本書における環境 |
| | 1.3. | 本書における構成 |
| 2. | . Entra | ID の設定9 |
| | 2.1. | 認証局を登録9 |
| | 2.2. | グループの作成11 |
| | 2.3. | 証明書ベース認証の有効化13 |
| | 2.3.1. | 認証強度を構成14 |
| | 2.3.2. | 証明書とユーザーの紐づけを構成16 |
| | 2.4. | 条件付きアクセスを構成18 |
| | 2.4.1. | セキュリティの規定値群の無効化18 |
| | 2.4.2. | 認証強度を構成20 |
| | 2.4.3. | アクセスポリシーを構成22 |
| 3. | . Gléas | の設定25 |
| | 3.1. | 証明書テンプレートの設定25 |

Microsoft Entra CBA による Microsoft 365 ログイン

| 3.2. | アカウント作成と証明書発行 | 26 |
|-------|--------------------------|----|
| 3.3. | 証明書の配布設定 (Windows 向け) | 29 |
| 3.4. | 証明書の配布設定 (iPhone 向け) | 31 |
| 3.5. | 証明書の配布設定 (Android 向け) | 34 |
| 4. クラ | イアントの設定 | 36 |
| 4.1. | Windows にクライアント証明書をインポート | 36 |
| 4.2. | iPhone にクライアント証明書をインポート | 38 |
| 4.3. | Android にクライアント証明書をインポート | 41 |
| 5. 証明 | 書ベース認証で m365 サインイン | 44 |
| 5.1. | Windows デバイスでサインイン | 44 |
| 5.2. | iPhone デバイスでサインイン | 47 |
| 5.3. | Android デバイスでサインイン | 49 |
| 6. その | 他 | 51 |
| 6.1. | サインインログについて | 51 |
| 6.2. | 証明書の失効確認について | 52 |
| 6.3. | 失効の即時反映について | 53 |
| 6.4. | 失効リストのサイズ制限について | 54 |

| 7. | い合わせ |
|----|------|
| | |

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)でMicrosoft 365にログインする構成の 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。

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

- > Officeアプリ: Microsoft 365
 ※以後「m365」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
- 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

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 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、iPhone、Android より m365 にアクセスする。②
- 6. m365 は、Entra ID にシングルサインオン。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 は認可して m365 ログイン完了。⑥
- 9. 利用者は、m365 を利用可能となる。⑦

2. Entra ID の設定

2.1. 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

| 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 ファイルをインボートします。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 wwz | |
| 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。

| 〒 アップロード 前 削除 ○ 更新 四 列 | | | | | | |
|--|------|-------------|--------|------|-------|--|
| ① 推奨されているアルゴリズム、キーの長さ、NIST 承認済み曲線のいずれかを必ず使用してください。 <u>詳細 〇</u> | | | | | | |
| 夕 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 による Microsoft 365 ログイン

2.2. 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

| 利してアリルーン | |
|--|--------|
| 反 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適用するグループ | ~ |
| 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 | ~ |
| 所有者 | |
| 1 人の所有者が選択されました | |
| メンバー | |
| 3 メンバーが羅択されました | |
| | |
| | |
| | |

セキュリティグループが作成されました。

| % 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 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 |
| 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 Microsoft 365 ログイン

2.3. 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

| Microsoft Entra CBA は、今後の新程能をサポート・ ({tenantid}) はテナント GUID を表します) に移行し [*] (certauth.login.microsoftoniine.com の下に 強くお勧めします。 詳細言報 | Fるために、certauth エンドボイントを certauth.login.mic ています。TLS 装置を備えたフィ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 | zrosoftoniine.com がら t{tenantid}.certauth.login.microsoftoniine.com 組織にある場合は、正規表現(1)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ンに応じてカスタマイズすること |
|---|--|---|
| 明書ペースの認証は、認証に x.509 証明書とエンターフ | 「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。 |
| 有効にする | | |
| グループの追加 | | |
| 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 Microsoft 365 ログイン

2.3.1. 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 | CRL 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 吟除外できます。 | | | | |
| CRL 検証を必須にする (推奨) CA を CRL 検証から除めする | ✓ 0.個の CA を選択済み | | | | |
| | +除外対象の追加 | | | | |
| 発行者ヒント | | | | | |
| 認証中に証明書ビッカーに有効な証明書の | 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、発行者ヒントを有効にします。 詳細情報 | | | | |
| 発行者とント | \checkmark | | | | |

- 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 による Microsoft 365 ログイン

- 証明書の属性 で [証明書の発行者] を選択
- [証明書の発行者] に先に登録した認証局を選択
- [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 \checkmark |
| 認証強度* |
| ○ 単一要素認証 |
| ● 多要素認証 |
| アフィニティ パインド * |
| • 低 |
| ○ 高 |
| |
| <u>追加</u> キャンセル |

● [保存] をクリック

Microsoft Entra CBA による Microsoft 365 ログイン

2.3.2.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。

● [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 |
| | |
| | |
| | |
| | |
| | |
| | |
| 追加 キャンセル | |

● [保存] をクリック

2.4. 条件付きアクセスを構成

m365 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。

2.4.1.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

| 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。 | 3 |
| 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 ピ | 7 |
| ○ 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 | |
| 保存 キャンセル | |

Microsoft Entra CBA による Microsoft 365 ログイン

2.4.2. 認証強度を構成

m365 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



| 新しい認認 | 証強度 | > |
|--------|------------------------------|---|
| 構成 レビ | а- | |
| 名前* | | |
| CBA 必須 | | |
| 説明 | | |
| 証明書ベース | ス認証を強制 | |
| | | |
| | | |
| ▶ 認証の | 組み合わせの検索 | |
| | | |
| | フィッシングに強い 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2.1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 による Microsoft 365 ログイン

2.4.3. アクセスポリシーを構成

m365 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。

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。

[ポリシー]を選択し、[+新しいポリシー]をクリックします。

- [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2.2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] に Office365 を選択
- 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、モバイルアプリとデスクトップクライアント
- アクセス制御 [許可] で[認証強度が必要] をチェックして、2.4.2項で構成した認証

強度を選択

Microsoft Entra CBA による Microsoft 365 ログイン

- ポリシーの有効化 [オン] を選択
- [作成] をクリック

| 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 🗸 |
| 割り当て |
| ユーザー 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 |
| しポート専用 (オン) オフ |
| 作成 |

アクセスポリシーが構成されました。

| 1 XEL 1348118. | 上 新しいゼロシーをテンプレートから | · · · · · · · · · · · · · · · · · · · | | | 〒 ゴルビュー機能 | |
|--|----------------------|---------------------------------------|---------------|--------------------|---------------------|-----|
| 十 新しいホリシー | 十 新しいホリシーをナノノレートから | 5 〒 小ワシー ファイルの | 07970-F > | < whath U 最新の情報に更新 | 156 フレビュー機能 | |
| Microsoft Entra 条件付きアクセス 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 | | | | | |
| - | Q 3 | | | | | |
| 4 | (全 4 項目中) | | | | | |
| 合計 | | | | | | |
| ▶ 検索 | | Y | ・フィルタ 一の追加 | | | |
| 4 個のポリシーのうち | 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 | cation 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 | cation 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 による Microsoft 365 ログイン

3. Gléas の設定

3.1. 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 による Microsoft 365 ログイン

3.2. 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

| ▶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t | ニュータ 〇 サーバ 〇 認証局 💿 CSVファイルー括登録 〇 LDAP | |
| > アップロードするファイル | ファイルの選択 upload.csv | |
| | 作后成 | |

● 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件を表示しています。 下部の「実行」ボタンを押すと、以下のファイルの内容がアカ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 | 5 4 | - 2 | メールアドレス | プリングルタ | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | 1000 | | | A - 5 M | |
| | | | | 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 による Microsoft 365 ログイン

[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ー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

3.3. 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 | |
|---|--|
| トークンへのインボート 証明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) CA証明書を含めない | 管理するトークン Gemalto NETカード × 証明書ストアの種類 ユーザストア × インボートワンスを利用する 登録申請を行わない 登録演みデバイスのみインボート許可 案件 |

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 Microsoft 365 ログイン

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]

3.4. 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 による Microsoft 365 ログイン

| ▶基本設定 | ▶上級者向け |
|---------------------------------|---|
| □ 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 | ✓ インボートワンスを利用する ✓ 登録申請を行わない ■ 登録済みデバイスのみインボート許可 |
| CA証明書を含めない | |
| | 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[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 による Microsoft 365 ログイン

【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 | 用する 続を許可 | ☑ ログインバスワードで証明書を保護 |
| OTA(Over-the-air) | | |
| OTAエンロールメントを利 | 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 | 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 | |
| sss.profile) | | |
| ブロファイルの組織名 | JCCHセキュリティ・ソリュージ | ンョン・システムズ |
| 記印 | 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。

3.5. 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 による Microsoft 365 ログイン

| ▶基本設定 | ▶上級者向け |
|---------------------------------|---|
| □ 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 | ✓ インボートワンスを利用する ✓ 登録申請を行わない ■ 登録済みデバイスのみインボート許可 |
| CA証明書を含めない | |
| | 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 |
| □ ログインパスワードで証明書を保護 ☑ 数字のみの PIN を表示 証明書ダウンロードの種類 PKCS#12ダウンロード |
| 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。

4. クライアントの設定

4.1. 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。

| O エンドユーザロ | コグイン [UA] |
|------------------|-------------------------------|
| UA 'ٿ | ーザID、バスワードを入力してロ 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 ユーザ情報・・・ | | | | * |
| ▶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 Microsoft 365 ログイン

※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

| ¥ |
|---------------------|
| |
| E J [¢] |
| |
| ‡ |
|) |
| |

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 | × □ プライバートCA Gléas テスト] - ザ- × | + | | _ | 0 |
|--|-----------------------------------|------|------|--------------|-------|
| - → C | | | A* 1 | a (î) | • |
| | | | プライ | «-ьса Gléä | ž ua |
| テスト ユーザー | - さんのページ] | | | 0 | リグアウト |
| ユーザ情報 | ーザーさんのページ | | | | ~ |
| ▶ユーザ | ∑ | | | | . 1 |
| > 姓:テスト ネ > ユーザID: > メールアドレス > バスワード:*** | 5: ユーザー : | | | | 1 |
| 兼 証明書情報 | 8 | | | | |
| ▶ 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 | |
| \$1 | | #3 | | タワンロード済み | |

4.2. 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。

| | JJTK-FCA Gléas UA | ブ | əan-pca Gléäs 🗖 | | プライベートCA Gléas UA |
|----------------------|--|---|---|---------------|--|
| AnuraAl | さんのページ | AsuraAD CBA 3 | さんのページ | Azurak | さんのページ |
| ユーザロ | anormal-the-feet | ユーザID | anormal-dis-lost | ユーザID | advected the field |
| 姓 | Asura/AD CBA | 姓 | AssesAD CBA | 姓 | Assessed CBA |
| 名 | Test | 名 | hat | 名 | Test . |
| メール | screat da tertipolitik precosition | メール | the leaf light life arrival con- | メール | annat da tertipristi ornorañ on |
| 有効期限 Copyright (C | ダウンロード ログアウト) 2010-2022 JCCH Scearly Solution Systems Co.[Lil: All rights reserved. | この Web サイ ンロードしよ か? Copyrglet (C) 2010-5022 10 | トは構成プロファイルをダウ らとしています。許可します 無視 許可 、 CHSearly School Sympa (G. LK, All right reserved | 有効期 Copyng | プロファイルがダウンロードさ れました プロ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。 助 servered 閉じる |

※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 による Microsoft 365 ログイン

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 | > | \odot | OS Demo Profile | |
| ダウンロード済みのプロファイル | > | 署名者 未署名 說明 內容 証明書(| 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。

| ~ | | | | | |
|---|---------|--------|--------|---------|--|
| Star Star Star Star Star Star Star Star | | IOS De | ma Pra | illin . | |
| 署名者 | 未署名 | | | | |
| 説明 内容 | if en 🕿 | (2) | | | |

Microsoft Entra CBA による Microsoft 365 ログイン

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。



4.3. 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。 |
| ▶ユーザID | ead-cha-test |
| ▶パスワード | |

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。

| JETA-FCA Gléas UA | | JETR-FCA Gléäs UA | | JETK-FCA Gléäs | |
|---|---------------------------------|---|-----------------------------------|---|------------------------------|
| さんのページ | | さんのページ | | Answed Claring さんのページ | |
| ユーザID | aturead chartest | ユーザID | aturead chartest | 7 | Par - |
| 姓 | AzumAD 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 | ードを入力します。 |
| メール | ganten annaroad com | メール | tiggo/HMD annicrosoft cam | 2 | |
| JCCH-SSS demo2 CA | | JCCH-SSS demo2 CA | | + | ヤンセル OK |
| 有効期限 | ダウンロード | 証明書 PIN: | 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 | | ログアウト |
| Copyright (C) 2010-2022 JCCH Security Soluti reserved. | ion Systems Co.,Ltd. All rights | Copyright (C) 2010 2022 JCCH Security Solu reserved. | ition Systems Co.,Ltd. All rights | Copyright (C) 2010-2022 JCCH Security Solution 5 reserved. | Systems 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。

「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 | | |
|-------------|--|----|--|
| 7 | VPN とアプリユーザー証明書 Wi-Fi 証明書 | | |
| Cop rese | 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 による Microsoft 365 ログイン

[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。

| | さんのペ | ージ |
|----------------|------------------|------------------------------|
| ユーザID | | and the first |
| 姓 | | Accessible 1986 |
| 名 | | 764 |
| X — II. | scored the local | period and the second second |
| ~ // | | |
| | Annual T.M. | |
| 有効期限 | Annual CA | ダウンロード済み |

5. 証明書ベース認証で m365 サインイン

5.1. Windows デバイスでサインイン

デスクトップアプリから m365 にサインインを試みると、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。

| | : |
|------------------------------|---|
| Microsoft | |
| サインイン | |
| | |
| アカウントがない場合 アカウントを 作成しましょう | |
| 次へ | |
| | |
| | |
| | |
| | |

[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。

| (3) KOI Security Subdion Systems |
|---|
| パスワードの入力 |
| /CZ9-ド |
| パスワード地志れた場合 |
| 証明書またはスマートカードを使用する サインイン |
| JS3テスト用 変更するときは、AAD管理センター > 会社のブ ランド |
| |

Microsoft Entra CBA による Microsoft 365 ログイン

[証明書の選択]ダイアログで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。

※パスワードを入力しても証明書の提示を強制されます。

| Γ | Windows | セキュリティ | | | × |
|---|----------|-------------|-------|-------|---|
| | 証明書 | 書の選択 | | | |
| | サイト | | | | |
| | | に対する資格情報が必要 | 要です: | | |
| | <u>.</u> | | | | |
| | · | 発行者: | - | | |
| | | 有効期間: | =1 ++ | | |
| | | 証明書のノロハリイを参 | いいより | | |
| | その他 | | | | |
| | | OK | | キャンセル | |

[OK]または[いいえ、このアプリのみにサインインします]をクリックすると、m365 に

サインインされます。

| | \times |
|---|----------|
| | |
| | |
| すべてのアプリにサインインしたままにする | |
| | |
| Windows でお客様のアカウントか記憶され、このデバイスでアプリや Web サイトに目動的にサインインします。これにより、ログインが求められる回数が減ります。 | 3 |
| | |
| 組織がデバイスを管理できるようにする | |
| | |
| ○ このオノションを連択すると、管理電がゲノリのインストール、設定の期限、デバイスのリセットをリモートで実行できるようになります。このデバイスのデータとアプリにアクセスするために、お客様がこのオブションを有効にするように相構から求められる場合があります。 | |
| | |
| | |
| | |
| | |
| | |
| | |
| いいえ、このアプリのみにサインインします | |
| | |
| ОК | |
| | |
| 1 | |

Microsoft Entra CBA による Microsoft 365 ログイン

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認証に失敗します。



5.2. iPhone デバイスでサインイン

モバイルアプリから m365 にサインインを試みると、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。

| Microsoft | |
|-----------|--|
| サインイン | |
| | |
| | |
| | |

クライアント証明書を選択して[選択]をタップします。



※デバイス内に証明書が1つのみ場合、この画面はスキップ

[続行]をタップすると、m365 にサインインされます。



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認証に失敗します。

| 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: | | | | |
| 現在のブラウザーを閉じてください 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 | | | | |
| | | | | |

Microsoft Entra CBA による Microsoft 365 ログイン

5.3. Android デバイスでサインイン

モバイルアプリから m365 にサインインを試みると、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矢印をタップします。



クライアント証明書を選択して[選択]をタップします。



Microsoft Entra CBA による Microsoft 365 ログイン

再度クライアント証明書を選択して[選択]をタップすると、m365 にサインインされま

す。



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認証に失敗します。



6. その他

6.1. 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 [保護] > [条件付アクセス]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 | 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 による Microsoft 365 ログイン

6.2. 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)

2.1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 L番号 #3 |
| | | | 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 による Microsoft 365 ログイン

6.3. 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

6.4. 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。

7. 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