



JCCH・セキュリティ・ソリューション・システムズ

# プライベート認証局Gléas ホワイトペーパー

## シングルサインオンによるGléas UAログイン (Google Workspace 連携)

Ver.1.1

2023年9月

- ・ 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。

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

目次

1. はじめに .....	5
1.1. 本書について .....	5
1.2. 本書における環境 .....	5
1.3. 本書における構成 .....	7
2. Gléas アカウントの登録 .....	8
2.1. Google Workspace のユーザ情報をエクスポート .....	8
2.2. Gléas にユーザ情報をインポート .....	9
3. SAML SP 署名用証明書の発行 .....	12
4. Google Workspace の設定 .....	14
4.1. カスタム SAML アプリの登録 .....	14
4.2. カスタム SAML アプリの公開 .....	18
5. Gléas の管理者設定 (Windows 向け) .....	19
6. クライアントからのアクセス (Windows) .....	22
6.1. シングルサインオンで UA にログイン .....	22
6.2. クライアント証明書のインポート .....	24

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

7. Gléas の管理者設定 (iPhone 向け) .....	26
8. クライアントからのアクセス (iPhone) .....	30
8.1. シングルサインオンで UA にログイン .....	30
8.2. クライアント証明書のインポート .....	32
9. Gléas の管理者設定 (Android 向け) .....	35
10. クライアントからのアクセス (Android) .....	40
10.1. シングルサインオンで UA にログイン .....	40
10.2. クライアント証明書のインポート .....	42
11. 問い合わせ .....	45

## 1. はじめに

### 1.1. 本書について

本書では、弊社製品「プライベート認証局 Gléas」のユーザ申込局 UA を、Google Workspace のカスタムSAMLアプリとして登録し、シングルサインオンで UA にログインする環境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利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。

➤ SAML IDP : Google Workspace

※以後「Google Workspace」と記載します

➤ SAML SP : JS3 プライベート認証局 Gléas (バージョン 2.6.0) UA

※以後「UA」と記載します

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

- ドメインコントローラ : Microsoft Windows Server 2016
  - ※以後「AD」と記載します。以下のツールをインストールしています
  - ◇ Google Cloud Directory Sync (Google WorkspaceへのID同期)
- JS3 プライベート認証局 Gléas (バージョン 2.6.0)
  - ※以後「Gléas」と記載します
- クライアント : Windows 10 Pro (21H1) / Microsoft Edge 104.0.1293.70
  - ※以後「Windows」と記載します
- クライアント : iPhone X (iOS 16) / Safari
  - ※以後「iPhone」と記載します
- クライアント : Google Pixel5 (Android 13) / Chrome
  - ※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。

- Google Workspaceの基本設定、およびADとのID同期方法
- Gléasでのユーザ登録やクライアント証明書発行等の基本操作
- Windows、iPhone での UA へのログイン方法

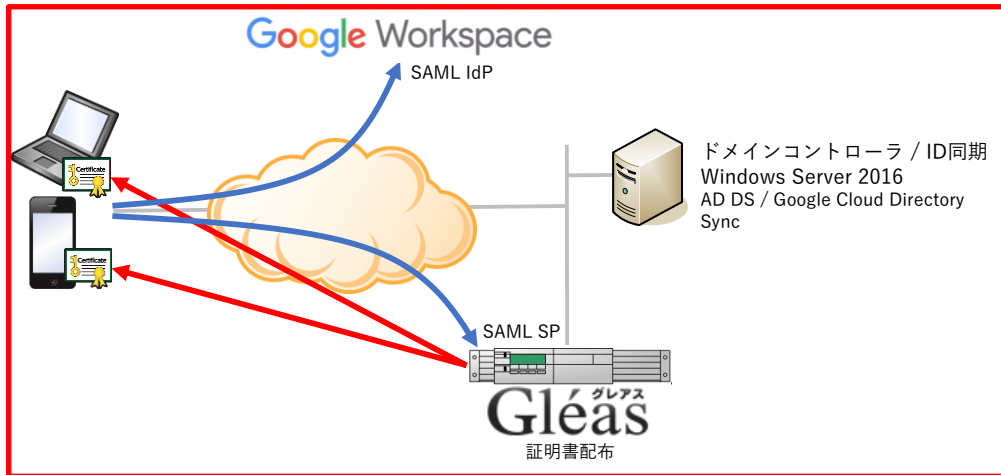
これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている

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  
シングルサインオンによる Gléas UA ログイン (Google Workspace 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。



1. Windowsでは、EdgeブラウザからUAへアクセス試行する
2. 認証連携先のGoogle Workspaceのログイン画面に画面遷移。Google Workspaceはパスワードを要求し、認証成功するとUAにログインした状態になる
3. iPhoneでは、SafariブラウザからUAへアクセス試行する
4. 認証連携先のGoogle Workspaceのログイン画面に画面遷移。Google Workspaceはパスワードを要求し、認証成功するとUAにログインした状態になる
5. Androidでは、ChromeブラウザからUAへアクセス試行する
6. 認証連携先のGoogle Workspaceのログイン画面に画面遷移。Google Workspaceはパスワードを要求し、認証成功するとUAにログインした状態になる

## 2. Gléas アカウントの登録

### 2.1. Google Workspace のユーザ情報をエクスポート

Google Workspace で管理しているユーザ情報をエクスポートします。

Google Workspace 管理コンソール にログインします。

[ディレクトリ] > [ユーザ]と進みます。



<input type="checkbox"/>	名前 ↑	メール	ステータス	最終ログイン	🗑️
<input type="checkbox"/>	👤 [ユーザー名]	[メールアドレス]	アクティブ	6 日前	
<input type="checkbox"/>	👤 [ユーザー名]	[メールアドレス]	アクティブ	1 週間前	
<input type="checkbox"/>	👤 [ユーザー名]	[メールアドレス]	アクティブ	1 週間前	

- [ユーザーをダウンロード]をクリック
- [ファイル形式を選択]で「カンマ区切りの値(.csv)」を選択
- [ダウンロード]をクリック
- [CSV 形式でダウンロード]をクリック

Google Workspace のユーザ情報がダウンロードできました。



## 2.2. Gléas にユーザ情報をインポート

エクスポートしたユーザ情報を Gléas のアカウントとしてインポートします。

ダウンロードしたユーザ情報 CSV を Gléas の形式に修正します。

- CSV ファイルを開く
- 先頭行の “First Name [Required]” を “givenname” に修正
- 先頭行の “Last Name [Required]” を “sn” に修正
- 先頭行の “Email Address [Required]” を “cn” に修正
- CSV ファイルを保存

続いて、Gléasの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。

The screenshot shows a web interface for account creation. The title bar is orange and contains 'アカウント情報' and '上級者向け設定'. The main content area is light green and contains several sections: 'アカウント名' (Account Name) with a text input field; '初期グループ' (Initial Group) with a dropdown menu set to 'なし' (None) and a link to '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' (Click here to select a group to add users); 'その他の設定' (Other Settings) with checkboxes for '証明書を発行する' (Issue certificate) and '連続して登録を行う' (Register continuously); '種類' (Type) with radio buttons for 'ユーザ' (User), 'コンピュータ' (Computer), 'サーバ' (Server), '認証局' (CA), 'CSVファイル一括登録' (CSV File Bulk Registration - selected), and 'LDAP'; and 'アップロードするファイル' (Upload file) with a 'ファイルの選択' (File Selection) button and a file name input field. A '作成' (Create) button is at the bottom.

- [CSV ファイル一括登録]を選択
- [アップロードするファイル]で作成した CSV ファイルを選択

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

- [作成]をクリック

※[証明書を作成する]をチェックすると、インポートと一緒に証明書の発行が行われます。

**+ インポート内容の確認**

**👤 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	姓	名	メールアドレス	プリンシパル名
XXXXXXXXXXXXXXXXXXXX	山田	太郎		
XXXXXXXXXXXXXXXXXXXX	山田	太郎		
XXXXXXXXXXXXXXXXXXXX	山田	太郎		
XXXXXXXXXXXXXXXXXXXX	山田	太郎		
XXXXXXXXXXXXXXXXXXXX	山田	太郎		
XXXXXXXXXXXXXXXXXXXX	山田	太郎		
XXXXXXXXXXXXXXXXXXXX	山田	太郎		
XXXXXXXXXXXXXXXXXXXX	山田	太郎		
XXXXXXXXXXXXXXXXXXXX	山田	太郎		

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**

- 内容を確認し[実行]をクリック

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 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。



- [すべて許可する] をクリック
- [実行] をクリック

これで Google Workspace に登録されたユーザが Gléas のアカウントとしてインポートされました。

### 3. SAML SP 署名用証明書の発行

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の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 `saml_sp` を作成します。

新規アカウント作成

アカウント情報の入力

このページではアカウントの新規作成を行います。  
アカウントは証明書発行する対象(エンドエンティティ)のことで、このページで指定したアカウント名が証明書の発行先となります。  
★の付いている項目は入力必須項目です。

アカウント情報

アカウント名 ★ saml\_sp

名前(姓) ★ SAML

名前(名) ★ SP証明書

メールアドレス

パスワード

パスワード(確認)

パスワード(自動生成) パスワード生成

プリンシパル名

作成

[証明書発行]で `saml_sp` アカウントに対し証明書を発行します。

saml\_sp

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「サブジェクト」と「属性」の内容で証明書要求を作成します。  
右側のテ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。

発行

サブジェクト

CN=saml\_sp

O=JCCH Security Solution Systems

DC=local, jcch-sss

属性

発行局: [redacted]

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

Netscape 拡張: 有効

CRL 配布点: [redacted]

選択されているテンプレート

必須 デフォルト設定

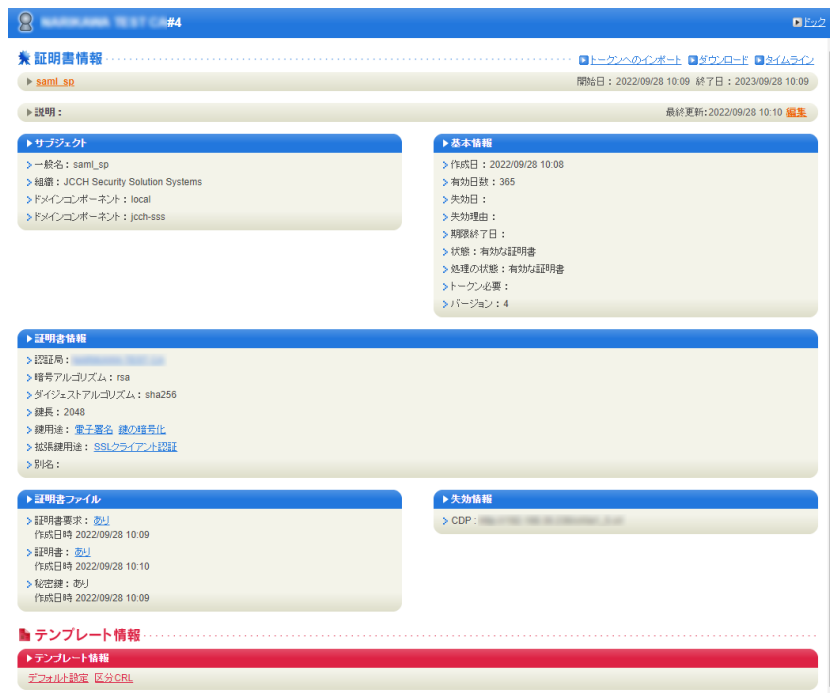
必須 区分CRL

選択可能なテンプレート

なし

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 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。



※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。

ダウンロードした.p12ファイルからPEM形式の証明書を取り出します。

※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 saml_sp.p12 -nokeys -clcerts | openssl x509 -out saml_sp.crt
```

※取得した証明書ファイル saml\_sp.crt を保存します。

ダウンロードした.p12ファイルからPEM形式の秘密鍵を取り出します。

※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 saml_sp.p12 -nodes -nocerts | openssl rsa -out saml_sp.key
```

※取り出した秘密鍵ファイル saml\_sp.key を保存します。

## 4. Google Workspace の設定

### 4.1. カスタム SAML アプリの登録

Google Workspace 管理コンソール にログインします。

[アプリ] > [ウェブアプリとモバイルアプリ]と進みます。

UA をカスタム SAML アプリとして登録します。

【アプリを追加】

- [アプリを追加]>[カスタム SAML アプリの追加]を選択
- [アプリ名]に SAML アプリの名前を入力
- [説明]にアプリの説明を入力
- [アプリのアイコン]に任意の画像をアップロード

× カスタム SAML アプリの追加

1 アプリの詳細 — 2 Google ID プロバイダの詳細 — 3 サービスプロバイダの詳細 — 4 属性のマッピング

アプリの詳細  
カスタム SAML アプリの詳細を入力してください。この情報はアプリのユーザーと共有されます。 [詳細](#)

アプリ名  
UA for Windows

説明  
Window向けUA

アプリのアイコン  
アプリのアイコンを添付してください。アップロードファイルのサイズの上限: 4 MB

プライベートCA  
Gléas UA  
for Windows

キャンセル 続行

入力後、[続行]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  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

- IdP メタデータをダウンロード
- [SSO の URL]をコピーしてメモ
- [エンティティ ID]をコピーしてメモ
- [証明書]をダウンロード
- [SHA-256 フィンガープリント]をコピーしてメモしておく

× カスタム SAML アプリの追加

✓ アプリの詳細 — 2 Google ID プロバイダの詳細 — 3 サービスプロバイダの詳細 — 4 属性のマッピング

SAML アプリに対するシングルサインオン (SSO) を設定するには、サービスプロバイダの指示に従ってください。 [詳細](#)

オプション 1: IdP メタデータをダウンロードする

[メタデータをダウンロード](#)

または

オプション 2: SSO の URL、エンティティ ID、証明書をコピーする

SSO の URL

エンティティ ID

証明書

[Google\\_2027-7-20-201132\\_SAML2\\_0](#) [ダウンロード](#)

有効期限: 2027/07/21

```
-----BEGIN CERTIFICATE-----
MIIDdDCCAlYgAwIBAgIGAYIj45W0MA0GC:SQGSib3DQEBCwUAMHsxFDASBgNVBAoT
C0dvb2dsZSBJ
bmluMRyWfAYDVQHEw1Nb3VudGFpbWV3MQ8wDQYDVQQDEwZhb29nbGUx
-----
```

SHA-256 フィンガープリント

[戻る](#) [キャンセル](#) [続行](#)

[続行]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  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

- [ACS の URL]を入力  
※https://[UA の FQDN]/ua/[UA の名前]/saml/acs
- [エンティティ ID]を入力  
※https://[UA の FQDN]/ua/[UA の名前]/saml
- [開始 URL]を入力  
※https://[UA の FQDN]/ua/[UA の名前]/saml/sso
- [署名付き応答]をチェック
- [名前 ID の形式]に「UNSPECIFIED」を選択
- [名前 ID]に「Basic Information > Primary email」を選択

× カスタム SAML アプリの追加

アプリの詳細 — Google ID プロバイダの詳細 — 3 サービスプロバイダの詳細 — 4 属性のマッピング

サービスプロバイダの詳細

シングルサインオンを設定するには、サービスプロバイダの詳細情報（ACS の URL やエンティティ ID など）の入力が必要です。 [詳細](#)

ACS の URL  
https://[ua.marthanas.local/profile-sss.local]/ua/[ua]/saml/acs

エンティティ ID  
https://[ua.marthanas.local/profile-sss.local]/ua/[ua]/saml

開始 URL (省略可)  
https://[ua.marthanas.local/profile-sss.local]/ua/[ua]/saml/sso

署名付き応答

名前 ID  
ID プロバイダでサポートされる名前 ID の形式を定義します。 [詳細](#)

名前 ID の形式  
UNSPECIFIED

名前 ID  
Basic Information > Primary email

戻る キャンセル **続行**

[続行]をクリックします。

※これにより Google Workspace ユーザのメールアドレスが UA ログインに使用されます。



プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

属性のマッピング追加は不要となります。

The screenshot shows a web interface for configuring a custom SAML application. The title bar reads '× カスタム SAML アプリの追加'. Below the title bar, there are four steps in a breadcrumb-like format: 'アプリの詳細', 'Google ID プロバイダの詳細', 'サービスプロバイダの詳細', and '4 属性のマッピング'. The main content area is titled '属性' (Attributes) and contains the following text: 'Google Directory のユーザー フィールドを追加および選択し、サービスプロバイダの属性にマッピングしてください。\*の付いた属性は必須です。詳細' (Add and select Google Directory user fields and map them to service provider attributes. Attributes with an asterisk are required. Details). Below this text, there are two columns: 'Google Directory の属性' and 'アプリの属性'. A 'マッピングを追加' (Add Mapping) button is located between these columns. The second section is titled 'グループメンバー (省略可)' (Group Members (Optional)) and contains the text: 'ここで追加したいいずれかのグループにユーザーが属している場合は、グループメンバー情報を SAML レスポンスで送信できます。' (If the user belongs to any of the groups you want to add here, you can send group member information in the SAML response). Below this, there are two columns: 'Google グループ' and 'アプリ属性'. Under 'Google グループ', there is a search input field labeled 'グループを検索'. Under 'アプリ属性', there is a text input field containing 'Groups'. At the bottom of the page, there are three buttons: '戻る' (Back), 'キャンセル' (Cancel), and '完了' (Complete).

[完了]をクリックします。

※カスタム SAML アプリは、UA 毎に登録する必要があります。PC と iOS などデバイス種類ごとに複数の UA を利用している場合などは、それぞれカスタム SAML アプリを登録する必要があります。

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

## 4.2. カスタム SAML アプリの公開

Google Workspace 管理コンソール にログインします。

[アプリ] > [ウェブアプリとモバイルアプリ]と進みます。

登録したカスタム SAML アプリを選択します。

The screenshot shows the configuration page for a SAML application. On the left, there is a sidebar with the following options: SAML (highlighted), UA for Windows, Window向けUA, SAML ログインをテスト, メタデータをダウンロード, 詳細を編集, and アプリの削除. The main content area is divided into three sections: 1. ユーザー アクセス: A dropdown menu showing 'オフ (すべてのユーザー)'. Below it, there is a link for '詳細を表示'. 2. サービスプロバイダの詳細: A table with columns for '証明書', 'ACS の URL', and 'エンティティ ID'. The values are: 'Google\_2027-7-20-201132\_SAML2\_0 (有効期限: 2027/07/21)', 'https://ua.narikawa.test.jcch-sss.local/ua/pc/saml/acs', and 'https://ua.narikawa.test.jcch-sss.local/ua/pc'. 3. SAML 属性のマッピング: A section stating that SAML attribute mapping is not configured and providing a link to 'SAML 属性のマッピングを設定'.

- [ユーザーアクセス]をクリック
- [サービスのステータス]を「オン」に設定

The screenshot shows the 'サービスのステータス' (Service Status) configuration page. It features a title bar with 'サービスのステータス' and an upward arrow. Below the title bar, there is a section for 'サービスのステータス' with two radio button options: 'オン (すべてのユーザー)' (selected) and 'オフ (すべてのユーザー)'. Below these options is an information icon and the text '大部分の変更は数分で反映されます。詳細'. At the bottom of the page, there is a blue bar with the text '未保存の変更が 1 件あります' and two buttons: 'キャンセル' and '保存'.

[保存]をクリックします。

## 5. Gléas の管理者設定 (Windows 向け)

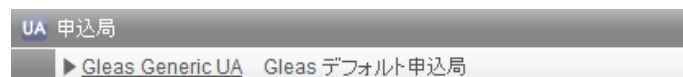
GléasのWindows向けUA (申込局) をGoogle WorkspaceのカスタムSAMLアプリとして動作するように設定します。

※ 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

GléasのRA (登録局) にログインします。

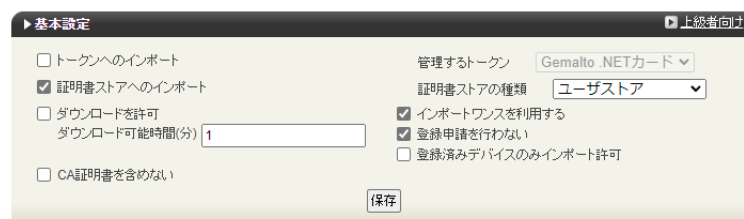
画面上部より[認証局]をクリックし認証局一覧画面に移動し、設定を行うUA (申込局) をクリックします。

※ 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



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
- 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



[上級者向け]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  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

- [SAML2.0 で外部認証する]をチェック
- [ホーム URL]に https://www.google.co.jp/ と入力
- [ログアウト URL]に https://www.google.co.jp/ と入力
- [SP 証明書]に SAML SP 署名用証明書ファイルを指定
- [SP 秘密鍵]に SAML SP 署名用証明書の秘密鍵ファイルを指定
- [IdP エンティティ ID]に Google WorkSpace の設定の際にコピーした「エンティティ ID 」を入力
- [IdP SSO URL]に Google WorkSpace の設定の際にコピーした「SSO の URL」を入力
- [IdP SLO URL]は空欄
- [IdP 署名用証明書]に Google WorkSpace の設定の際にダウンロードした「証明書」(Google\_YYYY-MM-DD-XXXX\_SAML2\_0.pem)をアップロード
- [IdP 暗号用証明書]は指定しない
- [ダイジェストアルゴリズム]に「SHA-256」を選択
- [署名アルゴリズム]に「RSA SHA-256」を選択
- [署名リクエストに署名]をチェック
- [ログアウトリクエストに署名]はチェックしない
- [ログアウトレスポンスに署名]はチェックしない

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

- [メタデータに署名する]をチェック
- [署名をメッセージに埋め込む]はチェックしない

ログイン方法

SAML2.0で外部認証する

ホームURL

ログアウトURL

SP Issuer

SP 証明書  saml\_sp.crt

SP 秘密鍵  saml\_sp.key

SP ACS URL

SP SLO URL

名前ID形式

IdP エンティティID

IdP SSO URL

IdP SLO URL

IdP 署名用証明書  Google\_202...AML2\_0.pem

IdP 暗号用証明書  ファイルが選択されていません

ダイジェストアルゴリズム  ▼

署名アルゴリズム  ▼

認証リクエストに署名  ログアウトリクエストに署名

ログアウトレスポンスに署名  メタデータに署名

署名をメッセージに埋め込む

設定完了後、[保存]をクリックし保存します。

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]

以上でGléasの設定は終了です。

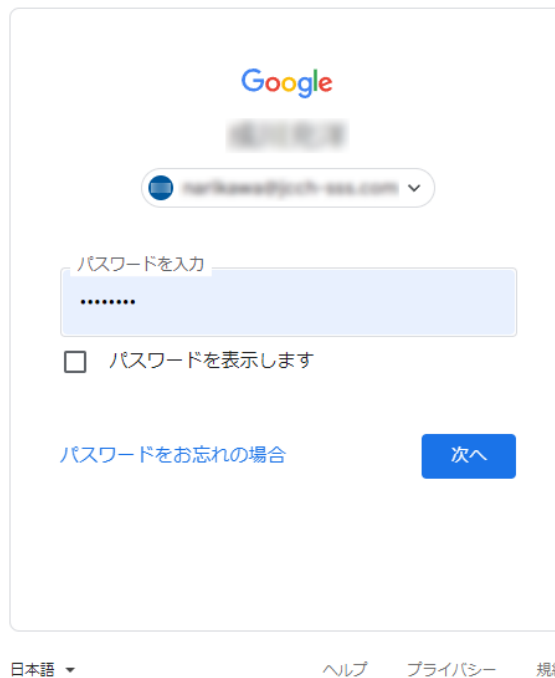
## 6. クライアントからのアクセス (Windows)

### 6.1. シングルサインオンで UA にログイン

PCのブラウザ (Edge) で、UAのシングルサインオンURLにアクセスします。

※URL `https://[UAのFQDN]/ua/[UAの名前]/saml/sso`

アクセスするとGoogle Workspaceのログインページに遷移します。

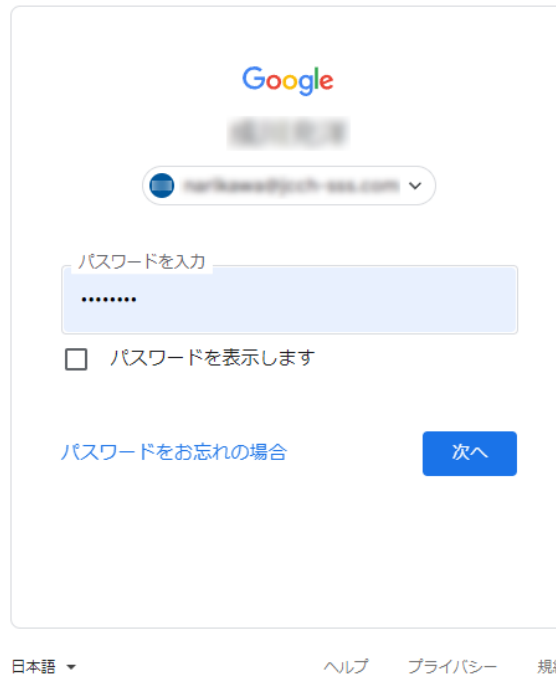


[次へ]をクリックします。

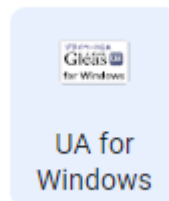
UAにログインし、ユーザ専用ページが表示されます。

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

Google Workspaceのアプリ一覧からログインすることもできます。



[次へ]をクリックしてログインします。



アプリ一覧から登録した「カスタムSAMLアプリ」を選択します。

UAにログインし、ユーザ専用ページが表示されます。

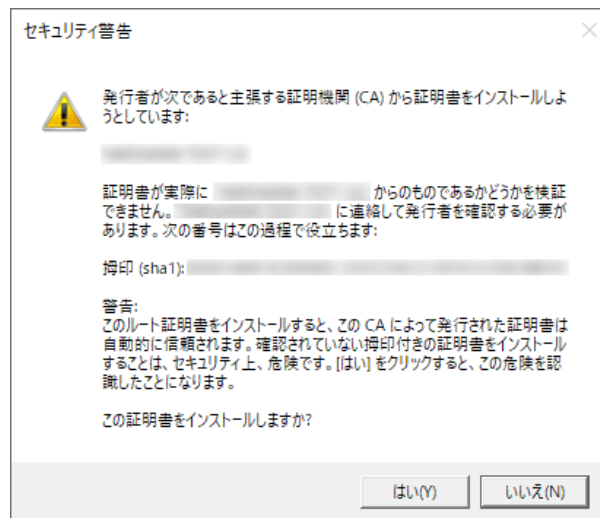
プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

## 6.2. クライアント証明書のインポート

[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。



※ 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





プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

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。



## 7. Gléas の管理者設定 (iPhone 向け)

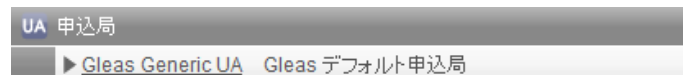
GléasのiPhone向けUA (申込局) をGoogle WorkspaceのカスタムSAMLアプリとして動作するように設定します。

※ 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

Gléasの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



[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、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。

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

基本設定 上級者向け

トークンへのインポート

証明書ストアへのインポート

ダウンロードを許可  
ダウンロード可能時間(分)

CA証明書を含まない

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

インポートワンスを利用する

登録申請を行わない

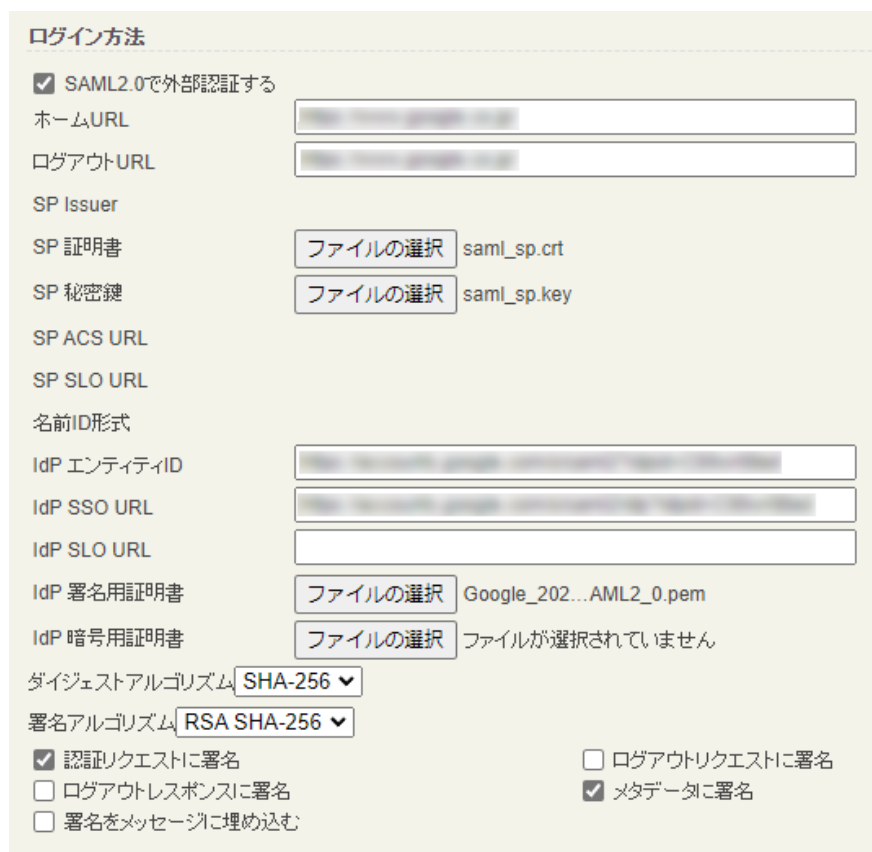
登録済みデバイスのみインポート許可

[上級者向け]をクリックします。

- [SAML2.0 で外部認証する]をチェック
- [ホーム URL]に <https://www.google.co.jp/> と入力
- [ログアウト URL]に <https://www.google.co.jp/> と入力
- [SP 証明書]に SAML SP 署名用証明書ファイルを指定
- [SP 秘密鍵]に SAML SP 署名用証明書の秘密鍵ファイルを指定
- [IdP エンティティ ID]に Google WorkSpace の設定の際にコピーした「エンティティ ID」を入力
- [IdP SSO URL]に Google WorkSpace の設定の際にコピーした「SSO の URL」を入力
- [IdP SLO URL]は空欄
- [IdP 署名用証明書]に Google WorkSpace の設定の際にダウンロードした「証明書」(Google\_YYYY-MM-DD-XXXX\_SAML2\_0.pem)をアップロード
- [IdP 暗号用証明書]は指定しない
- [ダイジェストアルゴリズム]に「SHA-256」を選択
- [署名アルゴリズム]に「RSA SHA-256」を選択

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

- [署名リクエストに署名]をチェック
- [ログアウトリクエストに署名]はチェックしない
- [ログアウトレスポンスに署名]はチェックしない
- [メタデータに署名する]をチェック
- [署名をメッセージに埋め込む]はチェックしない



ログイン方法

SAML2.0で外部認証する

ホームURL

ログアウトURL

SP Issuer

SP 証明書  saml\_sp.crt

SP 秘密鍵  saml\_sp.key

SP ACS URL

SP SLO URL

名前ID形式

IdP エンティティID

IdP SSO URL

IdP SLO URL

IdP 署名用証明書  Google\_202...AML2\_0.pem

IdP 暗号用証明書  ファイルが選択されていません

ダイジェストアルゴリズム

署名アルゴリズム

認証リクエストに署名  ログアウトリクエストに署名

ログアウトレスポンスに署名  メタデータに署名

署名をメッセージに埋め込む

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。

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

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な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

【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 用レイアウトを使用する  ログインパスワードで証明書を保護

Mac OS X 10.7以降の接続を許可

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) サンプルプロファイル

識別子(例: com.jcch-sss.profile) 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

説明 サンプ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。

以上でGléasの設定は終了です。

## 8. クライアントからのアクセス (iPhone)

### 8.1. シングルサインオンで UA にログイン

iPhoneのブラウザ (Safari) で、UAのシングルサインオンURLにアクセスします。

※URL `https://[UAのFQDN]/ua/[UAの名前]/saml/sso`

アクセスするとGoogle Workspaceのログインページに遷移します。



Google

パスワードを入力

パスワードを表示します

[パスワードをお忘れの場合](#) [次へ](#)

[次へ]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

Google Workspaceのアプリ一覧からログインすることもできます。



[次へ]をクリックしてログインします。



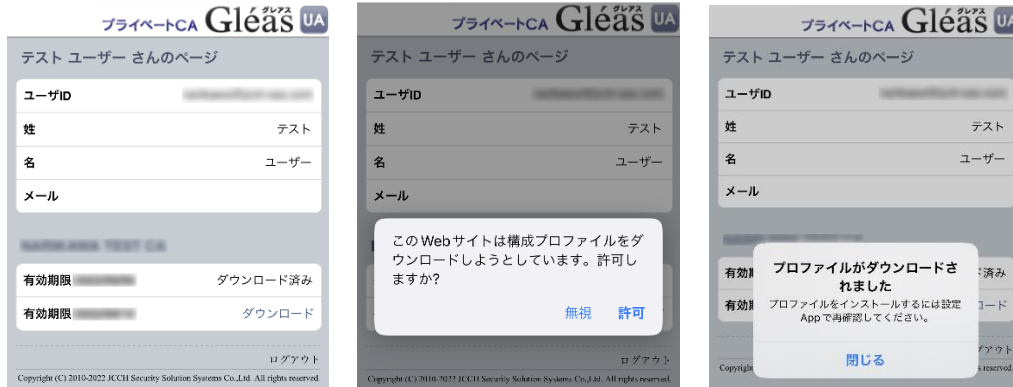
ログイン後、アプリ一覧から登録した「カスタムSAMLアプリ」を選択します。

UAにログインし、ユーザ専用ページが表示されます。

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

## 8.2. クライアント証明書のインポート

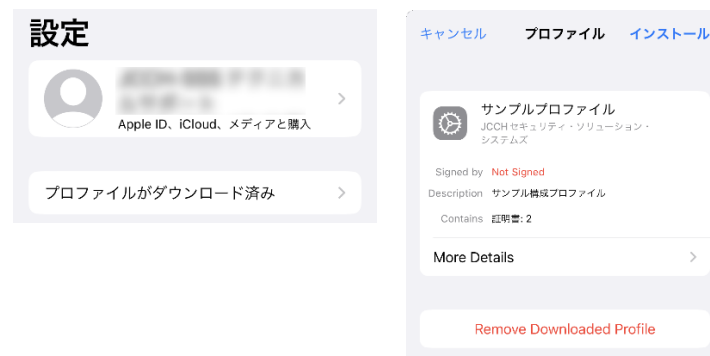
[ダウンロード]をタップし、構成プロファイルのダウンロードをおこないます。



※ 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

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。



[インストール]をタップして続行してください。

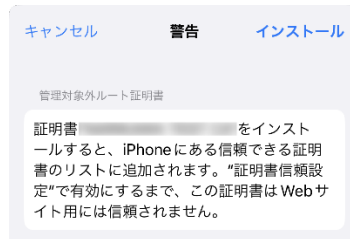


プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

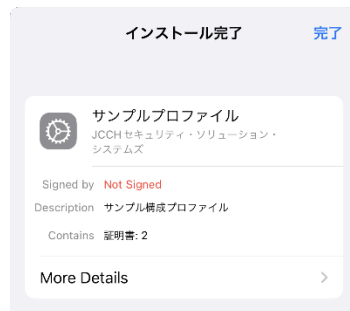
インストール中にルート証明書のインストール確認画面が現れるので、内容を確認し

[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。



なお [More Details]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。



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。

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

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。



The screenshot shows a user profile page for a test user. The header includes the logo 'プライベートCA Gléas UA' and the text 'テストユーザーさんのページ'. The profile information is as follows:

ユーザーID	[Redacted]
姓	テスト
名	ユーザー
メール	[Redacted]
有効期限	ダウンロード済み
有効期限	ダウンロード済み

At the bottom right, there is a 'ログアウト' (Logout) button. The footer contains the copyright notice: 'Copyright (C) 2010-2022 JCCH Security Solution Systems Co.,Ltd. All rights reserved.'

## 9. Gléas の管理者設定 (Android 向け)

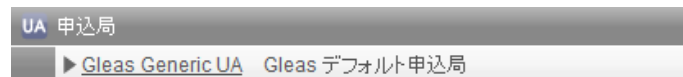
GléasのAndroid向けUA (申込局) をGoogle WorkspaceのカスタムSAMLアプリとして動作するように設定します。

※ 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

Gléasの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



[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。

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

基本設定 上級者向け

トークンへのインポート

証明書ストアへのインポート

ダウンロードを許可  
ダウンロード可能時間(分) 1

CA証明書を含まない

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

インポートワンスを使用する

登録申請を行わない

登録済みデバイスのみインポート許可

保存

[上級者向け]をクリックします。

- [SAML2.0 で外部認証する]をチェック
- [ホーム URL]に <https://www.google.co.jp/> と入力
- [ログアウト URL]に <https://www.google.co.jp/> と入力
- [SP 証明書]に SAML SP 署名用証明書ファイルを指定
- [SP 秘密鍵]に SAML SP 署名用証明書の秘密鍵ファイルを指定
- [IdP エンティティ ID]に Google WorkSpace の設定の際にコピーした「エンティティ ID」を入力
- [IdP SSO URL]に Google WorkSpace の設定の際にコピーした「SSO の URL」を入力
- [IdP SLO URL]は空欄
- [IdP 署名用証明書]に Google WorkSpace の設定の際にダウンロードした「証明書」(Google\_YYYY-MM-DD-XXXX\_SAML2\_0.pem)をアップロード
- [IdP 暗号用証明書]は指定しない
- [ダイジェストアルゴリズム]に「SHA-256」を選択

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

- [署名アルゴリズム]に「RSA SHA-256」を選択
- [署名リクエストに署名]をチェック
- [ログアウトリクエストに署名]はチェックしない
- [ログアウトレスポンスに署名]はチェックしない
- [メタデータに署名する]をチェック
- [署名をメッセージに埋め込む]はチェックしない

ログイン方法

SAML2.0で外部認証する

ホームURL

ログアウトURL

SP Issuer

SP 証明書  saml\_sp.crt

SP 秘密鍵  saml\_sp.key

SP ACS URL

SP SLO URL

名前ID形式

IdP エンティティID

IdP SSO URL

IdP SLO URL

IdP 署名用証明書  Google\_202...AML2\_0.pem

IdP 暗号用証明書  ファイルが選択されていません

ダイジェストアルゴリズム

署名アルゴリズム

認証リクエストに署名  ログアウトリクエストに署名

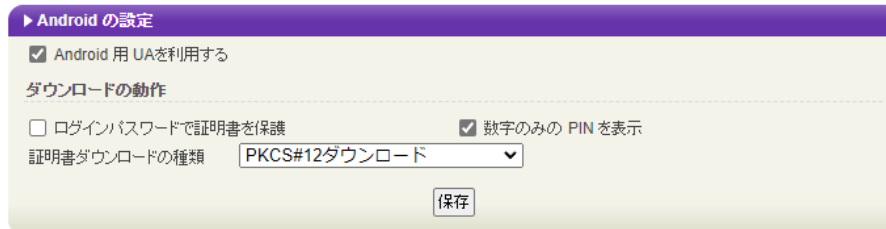
ログアウトレスポンスに署名  メタデータに署名

署名をメッセージに埋め込む

設定完了後、[保存]をクリックし保存します。

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

[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。



証明書のダウンロードに必要な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  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

証明書インポートアプリ CertImporter for Android を使用する場合は、[証明書インポートアプリ連携の設定] までスクロールし、[証明書インポートアプリを利用する]をチェックします。

▶ 証明書インポートアプリ連携の設定

- 証明書インポートアプリを利用する
- インポートボタンを表示
- 証明書一覧をアプリで表示(MacOSXのみ)
- 証明書と一緒にUAMニフェストをダウンロード
- 証明書PINをGléasで生成

UAMニフェスト

ログインURL

信頼するCA証明書  ファイルが選択されていません

証明書PIN生成シード

[UAMニフェスト要求ファイル](#) をダウンロードして、弊社サポートに送付してください

UAMニフェストのアップロード  ファイルが選択されていません

入力が終わったら、 [保存]をクリックします。

以上でGléasの設定は終了です。

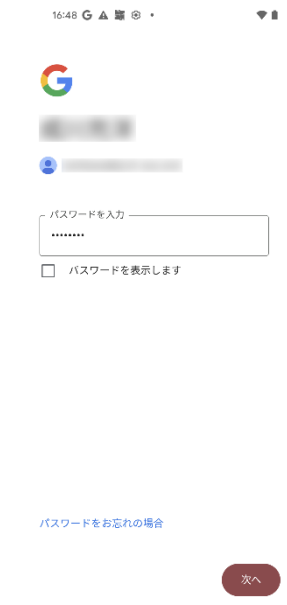
## 10. クライアントからのアクセス (Android)

### 10.1. シングルサインオンで UA にログイン

Androidのブラウザ (Chrome) で、UAのシングルサインオンURLにアクセスします。

※URL `https://[UAのFQDN]/ua/[UAの名前]/saml/sso`

アクセスするとGoogle Workspaceのログインページに遷移します。



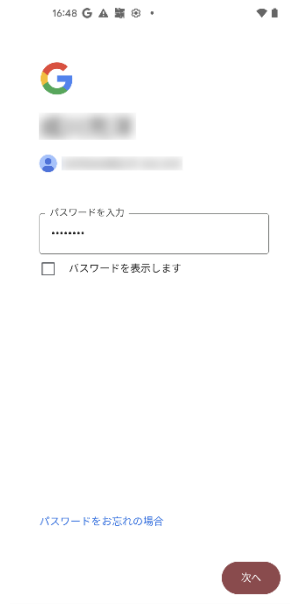
[次へ]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

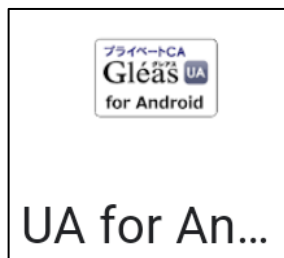


プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

Google Workspaceのアプリ一覧からログインすることもできます。



[次へ]をクリックしてログインします。



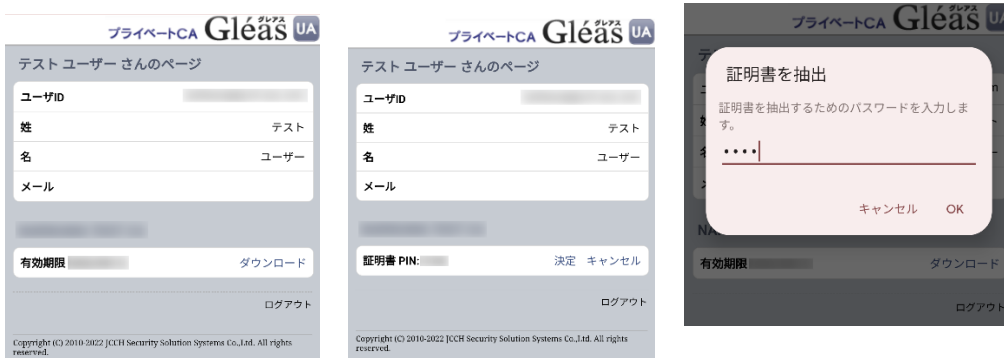
ログイン後、アプリ一覧から登録した「カスタムSAMLアプリ」を選択します。

UAにログインし、ユーザ専用ページが表示されます。

プライベート認証局 Gleás ホワイトペーパー  
シングルサインオンによる Gleás UA ログイン (Google Workspace 連携)

## 10.2. クライアント証明書のインポート

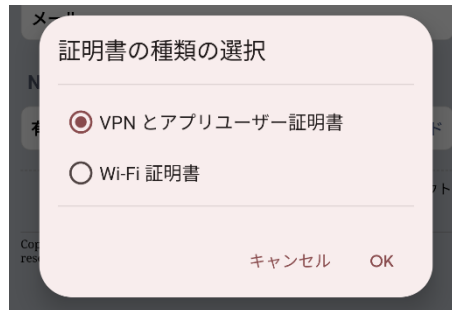
[ダウンロード]をタップし、証明書ファイルのダウンロードをおこないます。



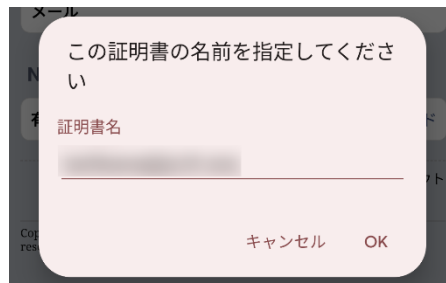
- ※ 「証明書 PIN」の値を「証明書を抽出」のパスワードとして入力します。
- ※ インポートロックを有効にしている場合は、この時点からカウントが開始されます

[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。



[OK]をタップして続行してください。



[OK]をタップします。

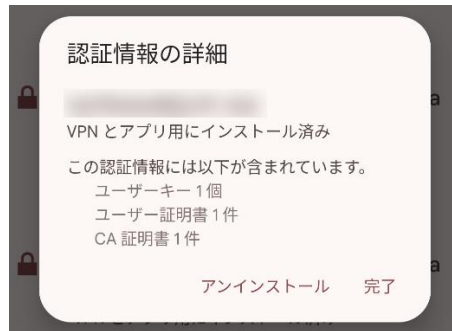
プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 連携)

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。

プライベート認証局 Gléas ホワイトペーパー  
シングルサインオンによる Gléas UA ログイン (Google Workspace 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。



## 11. 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](mailto:sales@jcch-sss.com)