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.1.0

2023 年 3 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。

目次

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。

- 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

- 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

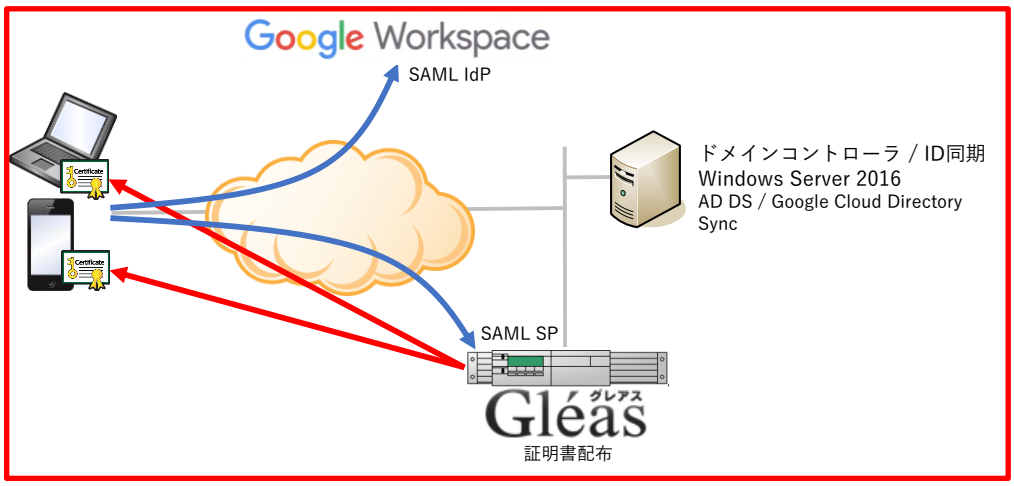
以下については、本書では説明を割愛します。

- 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。

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。

- [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

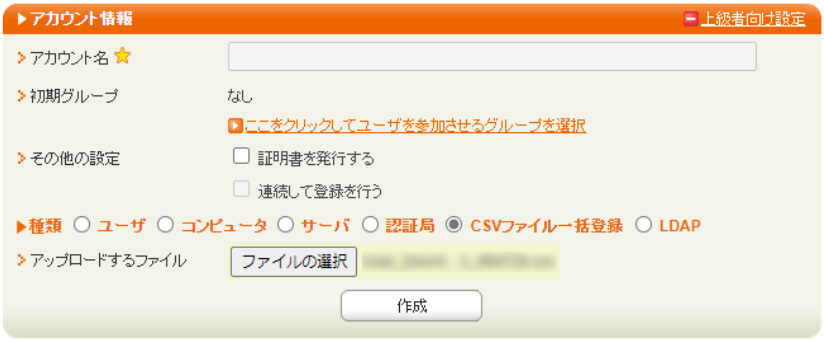
エクスポートしたユーザ情報を Gléas のアカウントとしてインポートします。

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。



- [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

- [作成]をクリック

- 内容を確認し[実行]をクリック

[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

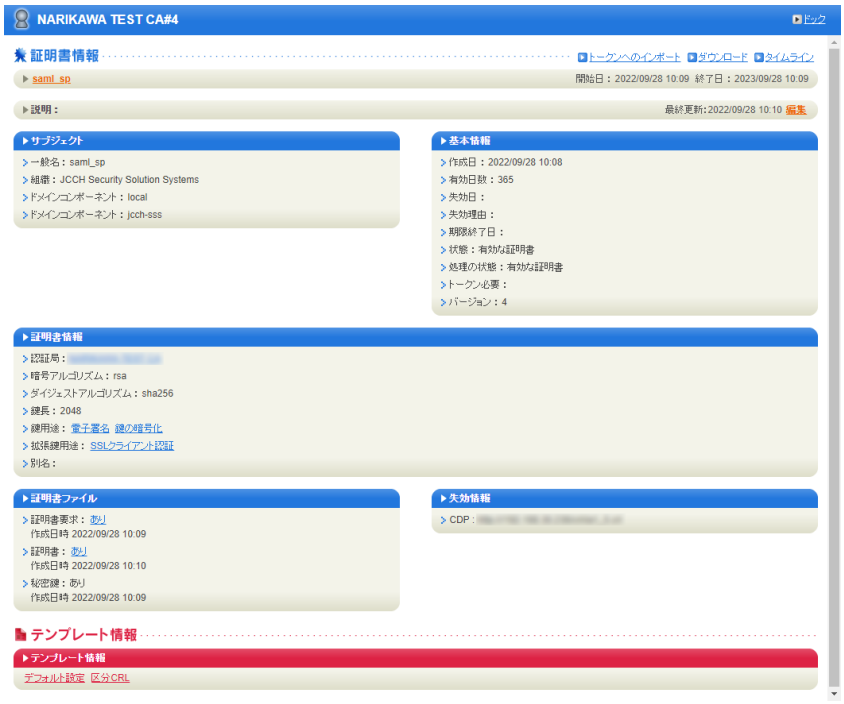
SAML SPとして使用する署名用証明書をGléasから発行します。

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。

[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。

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 -out saml_sp.crt -nokeys -clcerts
openssl x509 -in saml_sp.crt -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 -out saml_sp.key -nodes -nocerts
openssl rsa -in saml_sp.key -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

入力後、[続行]をクリックします。

- 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

[続行]をクリックします。

- [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

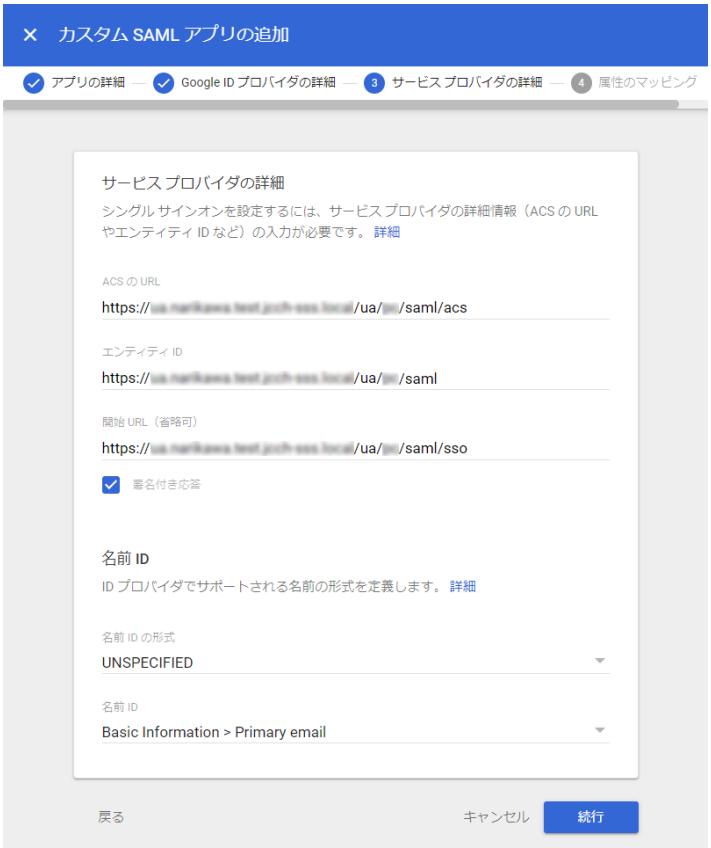
- [開始 URL]を入力

  ※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



[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。

属性のマッピング追加は不要となります。

[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。

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。

- [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

[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。

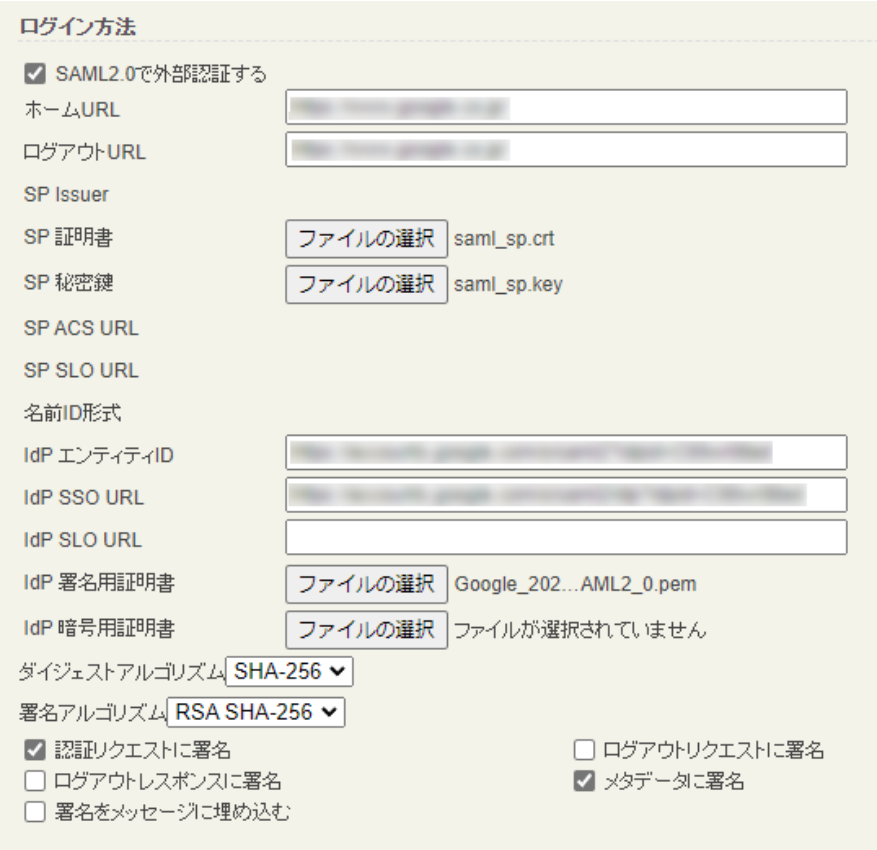
- [証明書ストアへのインポート]をチェック
- 証明書ストアの選択で、[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]にチェック

[上級者向け]をクリックします。

- [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

- [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



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。

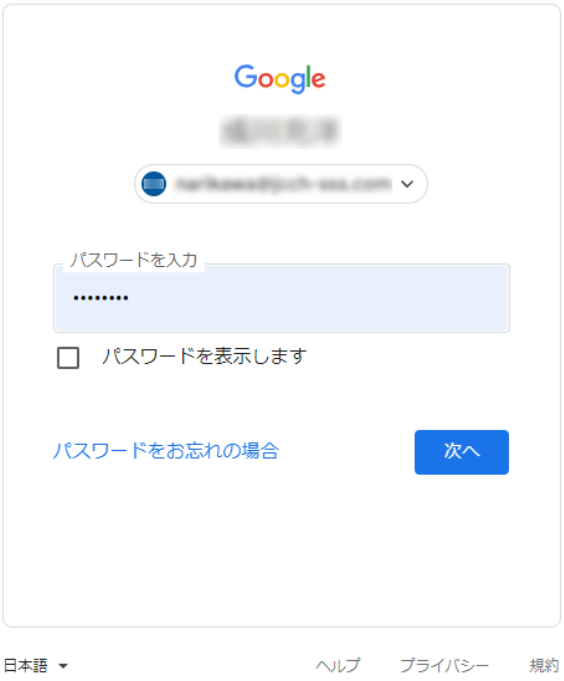
6. クライアントからのアクセス（Windows）

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。

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。

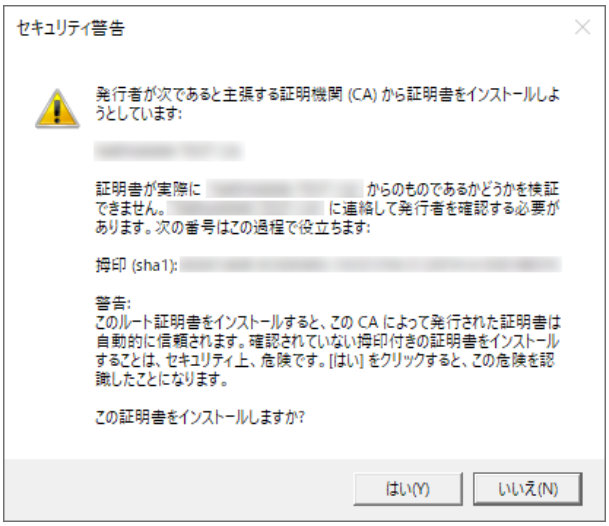
アプリ一覧から登録した「カスタムSAMLアプリ」を選択します。

UAにログインし、ユーザ専用ページが表示されます。

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



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。

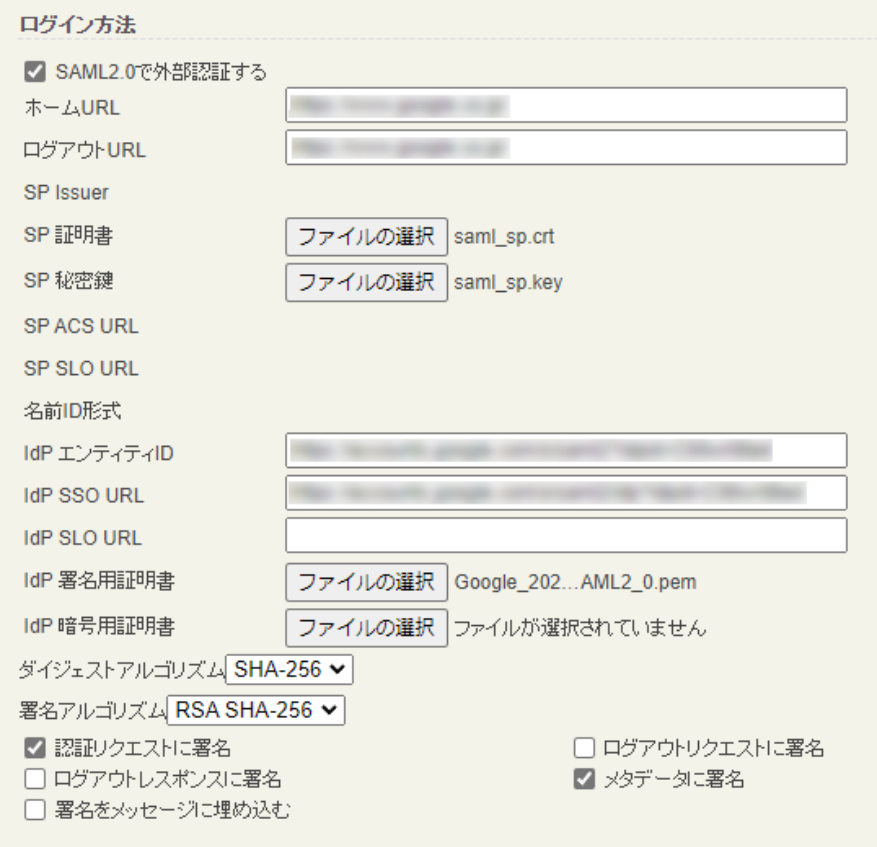
- [ダウンロードを許可]をチェック
- [ダウンロード可能時間(分)]の設定・[インポートワンスを利用する]にチェック

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。

[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

- [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



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。

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

【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）

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。

[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。

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

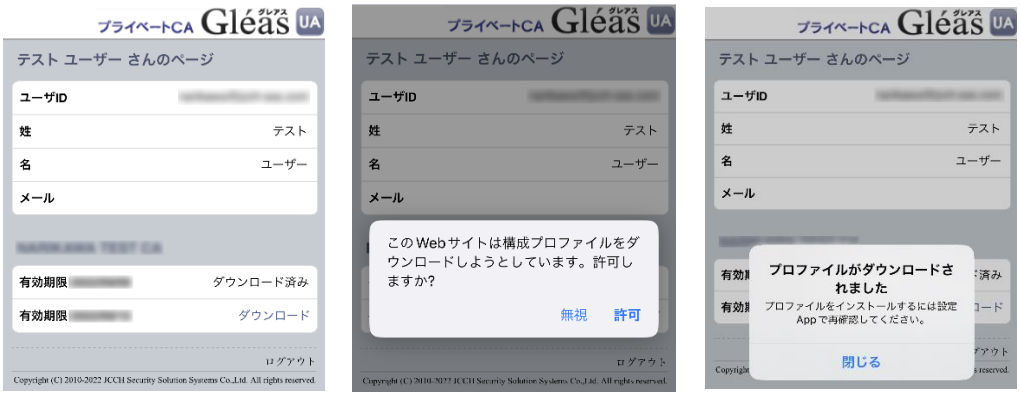
[次へ]をクリックしてログインします。

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。

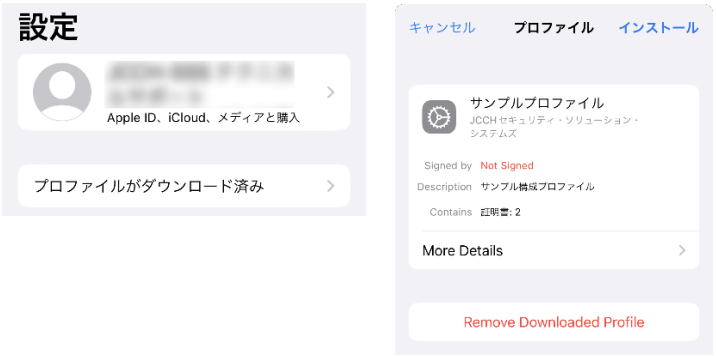
8.2. クライアント証明書のインポート

[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。

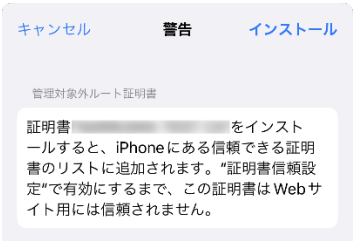


[インストール]をタップして続行してください。

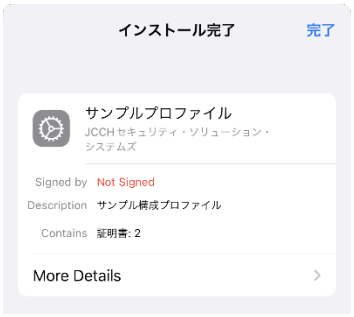
インストール中にルート証明書のインストール確認画面が現れるので、内容を確認し

[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。

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。

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。

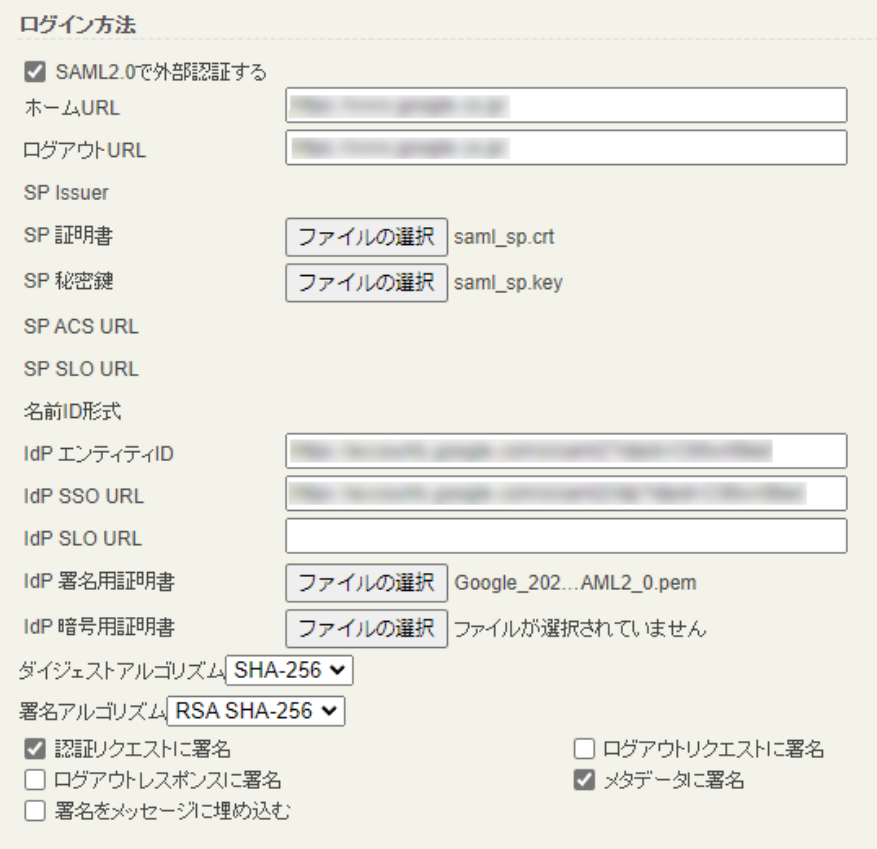
- [ダウンロードを許可]をチェック
- [ダウンロード可能時間(分)]の設定・[インポートワンスを利用する]にチェック

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。

[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
- [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



設定完了後、[保存]をクリックし保存します。

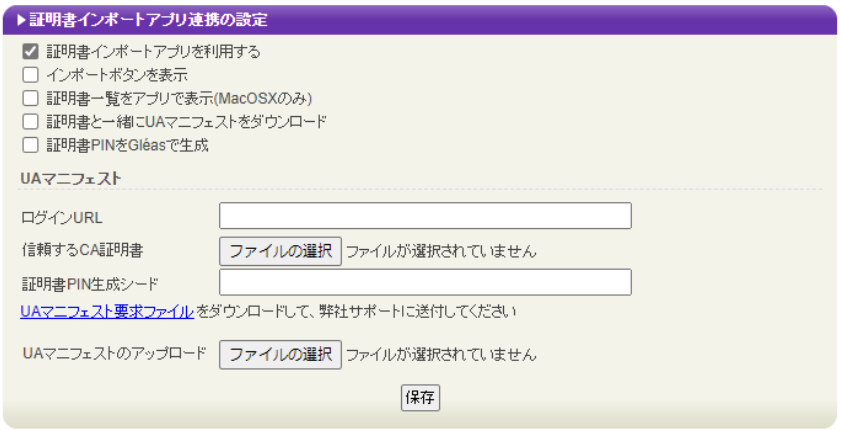
[認証デバイス情報]の[Androidの設定]までスクロールし、[Android用UAを利用する]をチェックします。

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。

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。



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。

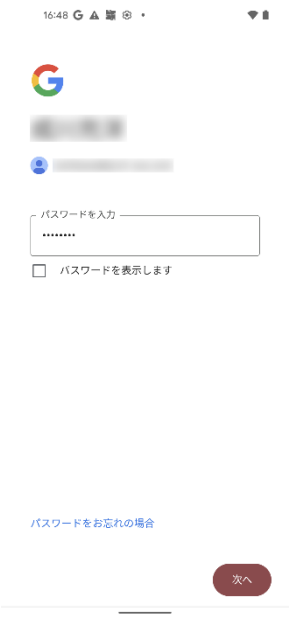
10.クライアントからのアクセス（Android）

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

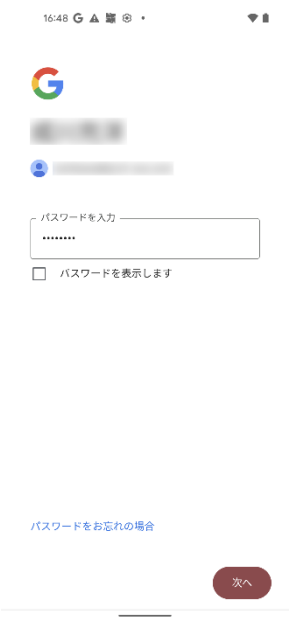
アクセスするとGoogle Workspaceのログインページに遷移します。



[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。

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



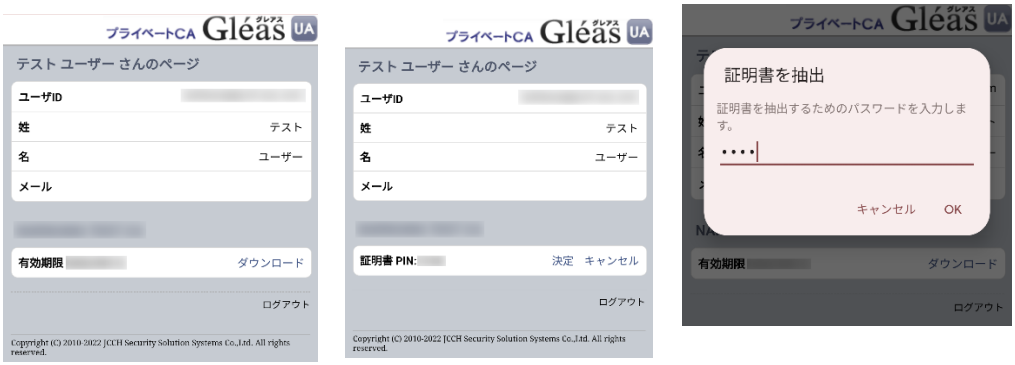
[次へ]をクリックしてログインします。

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。

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。

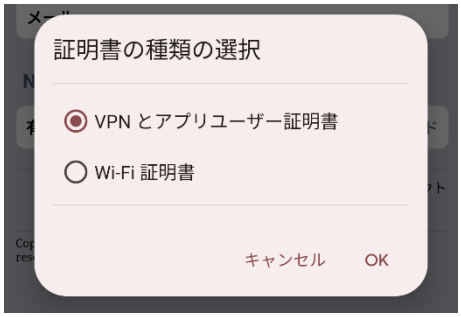


※ 「証明書 PIN」の値を「証明書を抽出」のパスワードとして入力します。

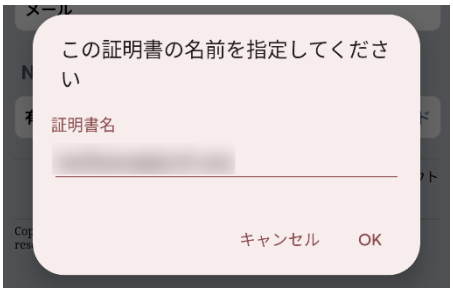
※ インポートロックを有効にしている場合は、この時点からカウントが開始されます

[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。

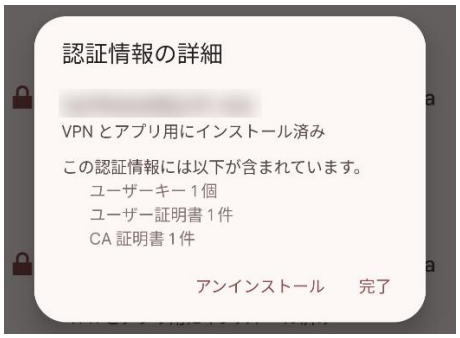


[OK]をタップします。

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。

[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