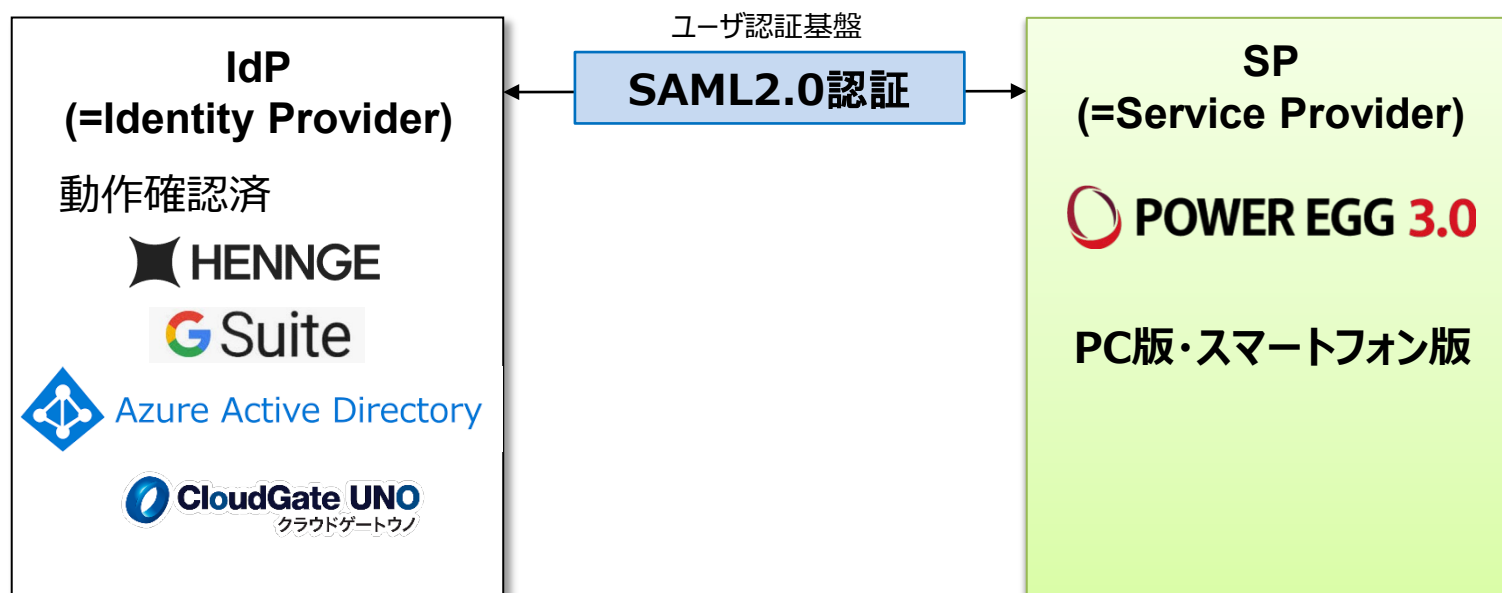


# POWER EGG 3.0 SAML認証連携

2022年3月  
ディサークル株式会社

修正日・版	修正箇所・内容
2019/09/01 1.0版	初版 発行
2020/07/03 2.0版	「制限・留意事項」に、IdPとの通信で利用可能なプロトコルに関する留意事項を追記 一部表記を修正
2020/11/19 3.0版	設定例に記載されているEntity IDの最後に"/"(スラッシュ)を追加 Azure AD、IIJ IDサービスとの連携を追記 HENNGE,GsuiteのUI変更に伴い、画像を変更
2022/02/18 4.0版	CloudGate Unoサービスとの連携を追記 一部表記を修正
2022/03/02 5.0版	CloudGate UNOのUI変更に伴い、「IdP(CloudGate UNO)への登録」を変更

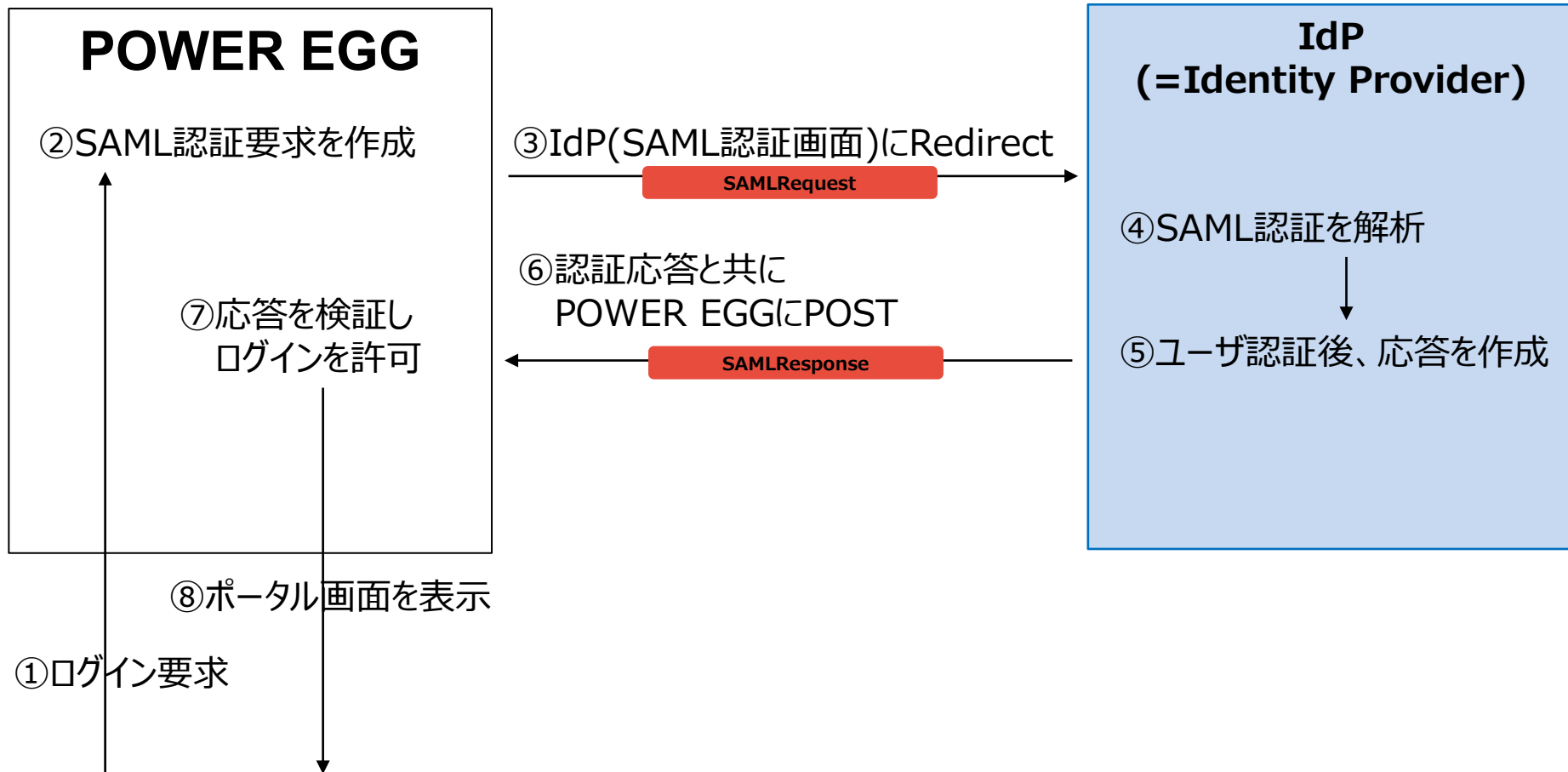
## ■ SAML2.0連携モデル



※ IdPについては、SAMLに関する以下の内容に対応しているIdPが利用可能です。

- ・ SAML バージョン : 2.0
- ・ SAML Bindings : リクエスト HTTP Redirect Bindingsのみ対応  
レスポンス HTTP POST Bindingsのみ対応

当社で検証を行っておりますのは、HENNGE One、Gsuite、Azure AD、IIJ ID、CloudGate UNOサービスとなります。



※ ①のログイン要求の際、すでにIdP認証済の場合は、⑦のみを行い、POWER EGGに自動ログインします。



SAML認証用のURLから、POWER EGGにログインする場合は以下の流れとなります。

①POWER EGGのSAML認証用のURLにアクセス

【SAML認証用URL】

PC用 : `http(s)://(サーバー名):(ポート)/pe4j/samlLogin`

スマートフォン用 :

`http(s)://(サーバー名):(ポート)/pe4x/?saml#/login`



②IdPのログイン画面にリダイレクト

例. HENNGE One、GSuiteのログイン画面を表示



③ログイン後、ナビビューを表示



認証プロトコルには、IdP側のアカウントを利用しています。  
(HENNGE One・IIJ IDサービスの場合はログインID、Gsuite・Azure ADの場合はメールアドレスを利用します)

IdP側のログインIDをPOWER EGGの社員情報の「メモ1」にセットします。

例： HENNGE OneのログインID： imaoka



POWER EGG社員情報のメモ1： imaoka

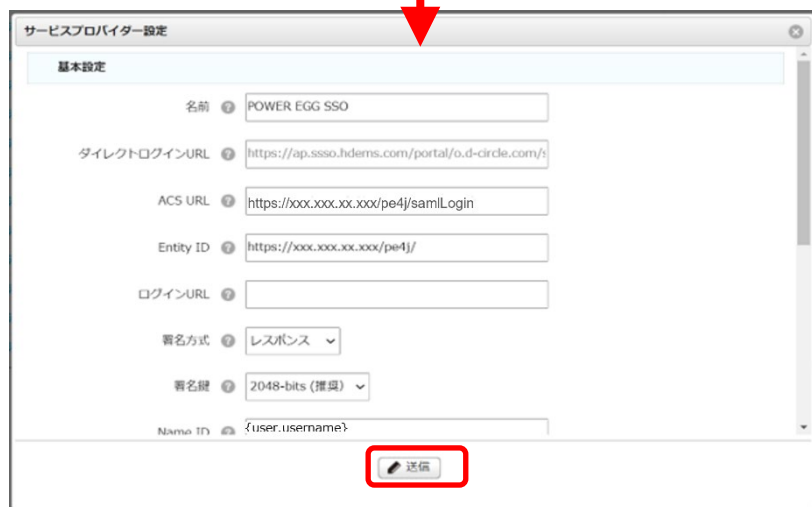
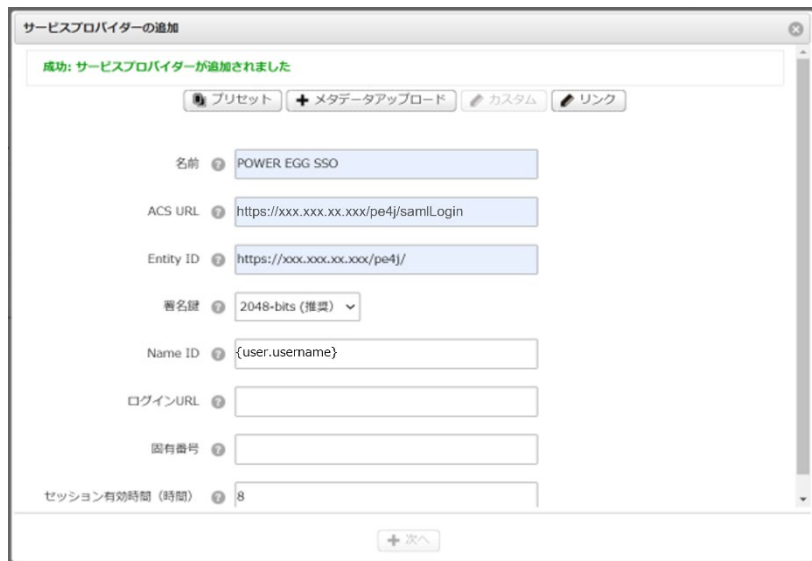
ユーザー等のIdPとの連携機能はありませんので、POWER EGGの組織情報（社員、部門等）はPOWER EGG側にあらかじめ登録しておく必要があります。

HENNGE Oneの場合、管理アカウントで管理画面にログインし、「サービスプロバイダー設定」を選択し、「サービスプロバイダーの追加」ボタンをクリックすると、表示された画面で「カスタム」ボタンをクリックすると、右下の設定画面が表示されます。右下に記載する内容を入力し、「次へ」ボタンをクリックします。

The screenshot shows the HENNGE One management console. On the left, the 'サービスプロバイダー設定' (Service Provider Settings) menu item is highlighted. A red arrow points to the '+ サービスプロバイダーの追加' (Add Service Provider) button. Another red arrow points to the 'リンク' (Link) button in the top right of the 'サービスプロバイダーの追加' (Add Service Provider) form. A third red arrow points to the '+ 次へ' (Next) button at the bottom of the form.

PC用設定	
名前	POWER EGG SSO
ACS URL	http(s)://(サーバー名):(ポート番号)/pe4j/samlLogin
Entity ID	http(s)://(サーバー名):(ポート番号)/pe4j/
署名鍵	1024-bits または 2048-bits(推奨)
Name ID	{user.username}
スマートフォン用設定	
名前	POWER EGG MOBILE SSO
ACS URL	http(s)://(サーバー名):(ポート番号)/pe4x/sso/samlLogin
Entity ID	http(s)://(サーバー名):(ポート番号)/pe4x/
署名鍵	1024-bits または 2048-bits(推奨)
Nome ID	{user.username}

「次へ」ボタンをクリックすると以下の画面へ切り替わります。「送信」ボタンをクリックすると、確定されます。





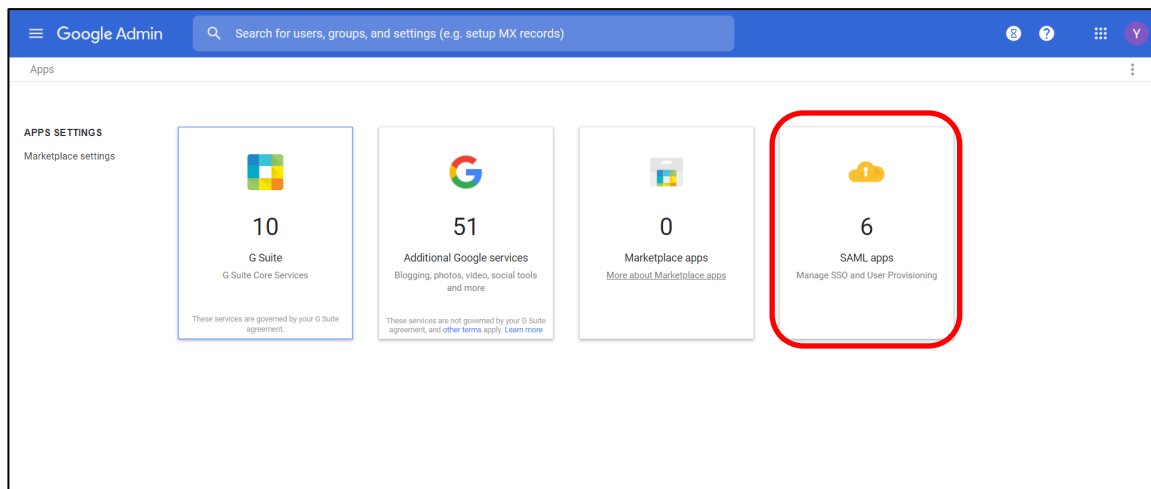
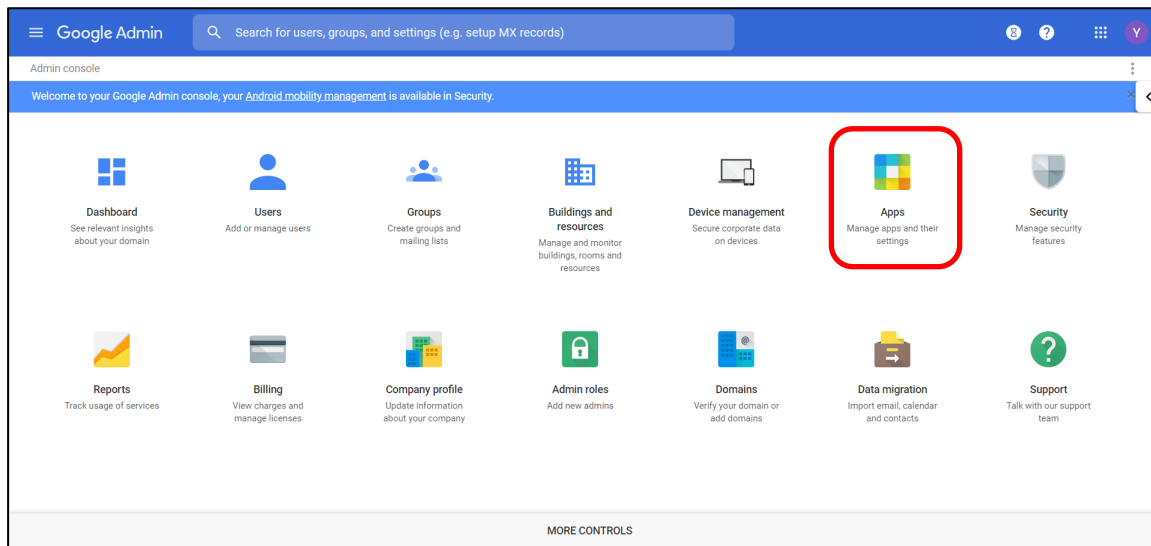
登録すると、一覧上に、以下の内容で表示されます。(完了と表示されていれば、確定されています)

POWER EGG SSO	表示	ダウンロード	0	0	完了		
---------------	----	--------	---	---	----	--	--

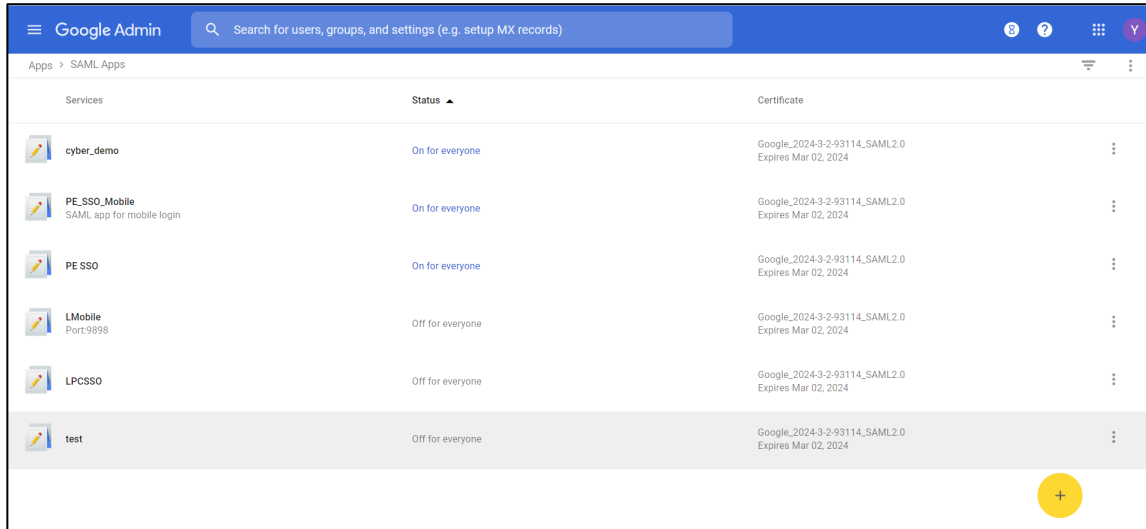
「ダウンロード」リンクをクリックすると、メタデータがダウンロードされます。  
このファイルをPOWER EGG側のSAML認証連携設定で、登録を行ってください。

PC用で登録した設定からダウンロードしてください。  
(スマートフォン用で登録した設定からでも同一内容がダウンロードされます)

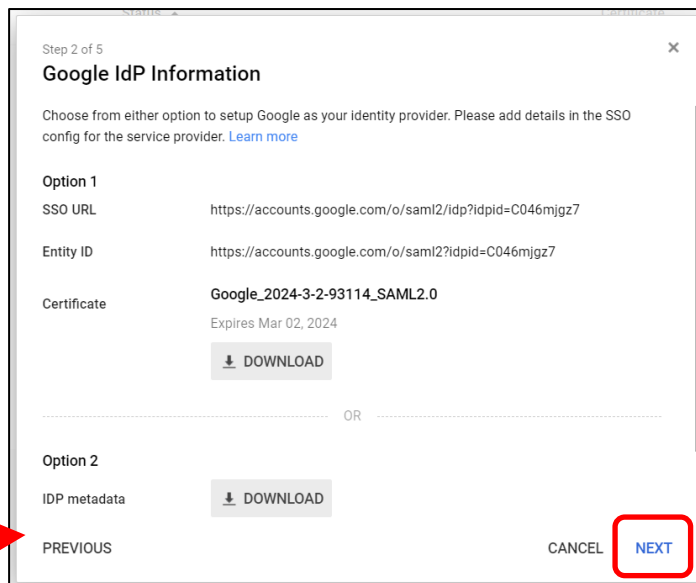
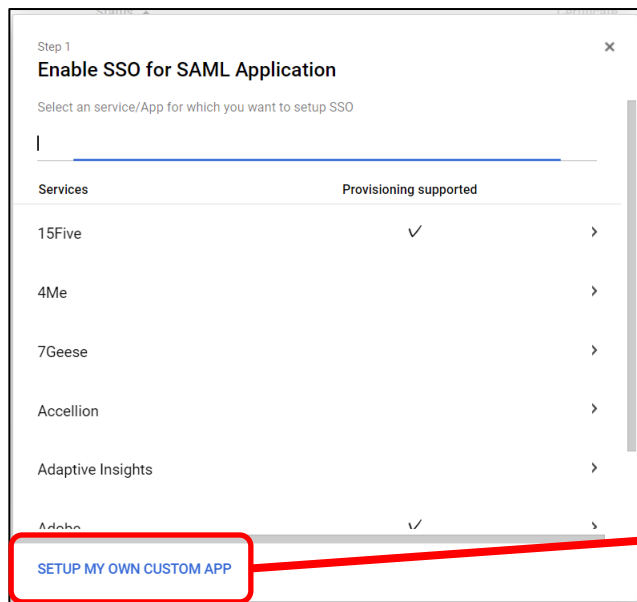
GSuiteの場合、管理アカウントで管理画面にログインして、「Apps」リンクをクリックします。次に、「SAML apps」リンクをクリックします。



新規で登録する場合、+ ボタンをクリックします。



Step1では、「SETUP MY OWN CUSTOM APP」リンクをクリックします。  
Step2では、初期値のまま、NEXTボタンをクリックします。



Step3、4では、以下の内容を入力し、NEXTボタンをクリックします。

Step 3 of 5

### Basic information for your Custom App

Please provide the basic information needed to configure your Custom App. This information will be viewed by end-users of the application.

Application Name \*  app-id: power\_egg\_sso

Description

Upload logo

This logo will be displayed for all users who have access to this application. Please upload a .png or .gif image of size 256 x 256 pixels.

PREVIOUS CANCEL NEXT



Step 4 of 5

### Service Provider Details

Please provide service provider details to configure SSO for your Custom App. The ACS url and Entity ID are mandatory.

ACS URL \*

Entity ID \*

Start URL

Signed Response

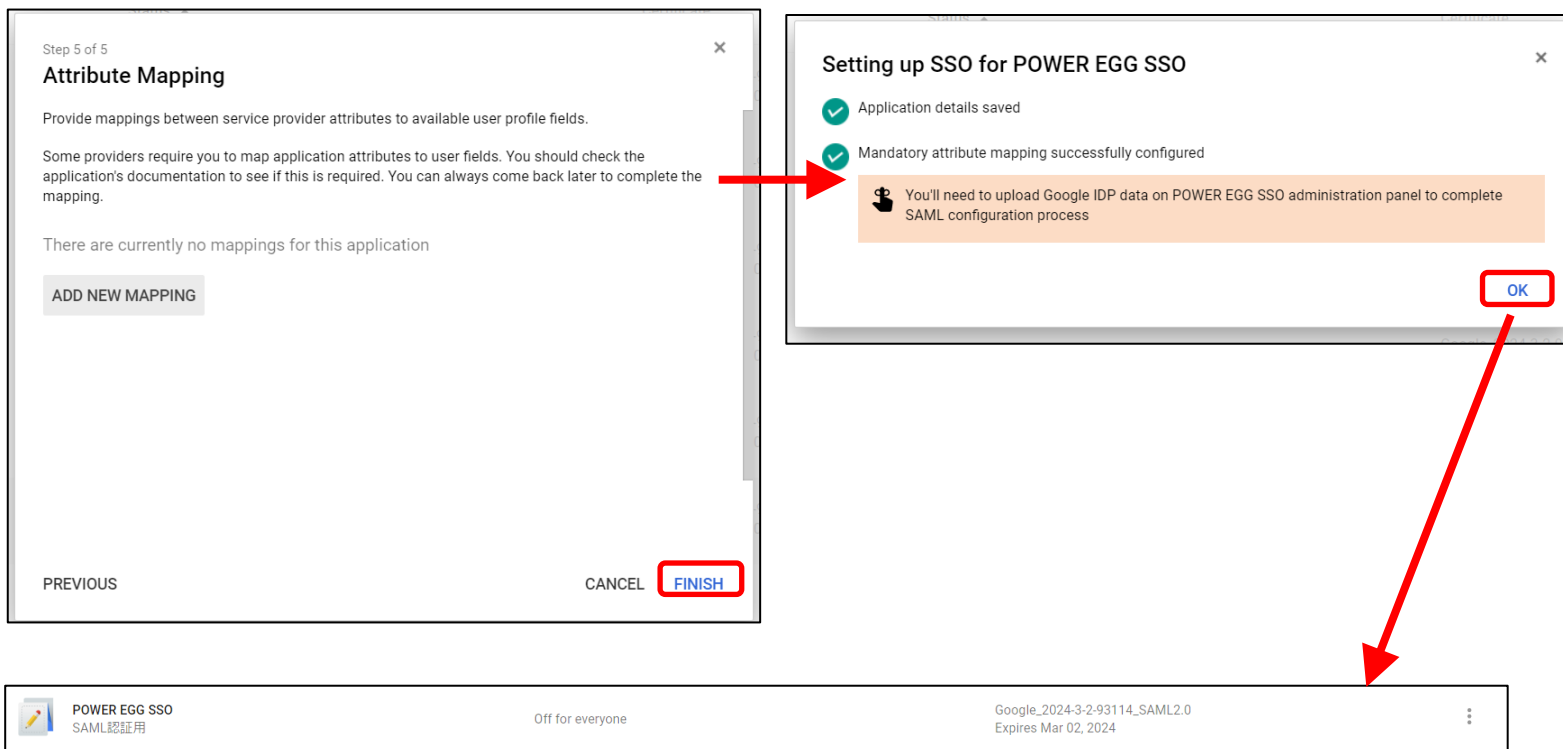
Name ID

Name ID Format

PREVIOUS CANCEL NEXT

PC用設定	
Application Name	POWER EGG SSO
Description	SAML認証用
ACS URL	http(s)://(サーバー名):(ポート)/pe4j/samlLogin
Entity ID	http(s)://(サーバー名):(ポート)/pe4j/
スマートフォン用設定	
Application Name	POWER EGG MOBILE SSO
Description	SAML認証用(スマートフォン用)
ACS URL	http(s)://(サーバー名):(ポート)/pe4x/sso/samlLogin
Entity ID	http(s)://(サーバー名):(ポート)/pe4x/

Step5では、そのまま、FINISHボタンをクリックします。登録された旨が表示されるので、OKボタンをクリックします。登録後、一覧上に、以下のように表示されます。

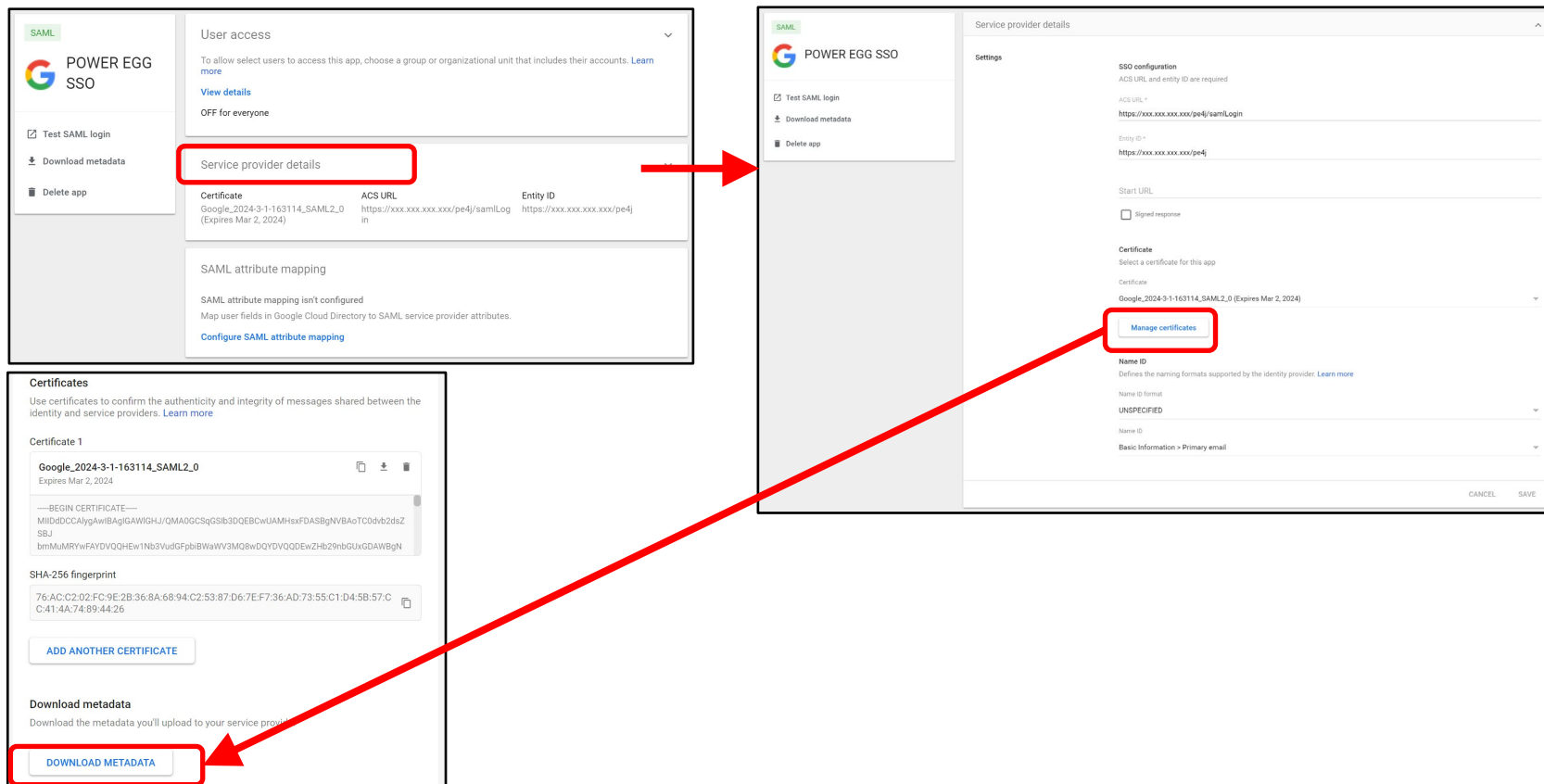


The image shows a sequence of three screenshots illustrating the SSO configuration process:

- Step 5 of 5: Attribute Mapping**: A dialog box with the title "Attribute Mapping" and a close button (X). The text reads: "Provide mappings between service provider attributes to available user profile fields. Some providers require you to map application attributes to user fields. You should check the application's documentation to see if this is required. You can always come back later to complete the mapping. There are currently no mappings for this application." Below the text is an "ADD NEW MAPPING" button. At the bottom are "PREVIOUS", "CANCEL", and "FINISH" buttons. A red arrow points from the "FINISH" button to the next dialog.
- Setting up SSO for POWER EGG SSO**: A confirmation dialog with a close button (X). It lists two successful steps: "Application details saved" and "Mandatory attribute mapping successfully configured". A message box with a download icon states: "You'll need to upload Google IDP data on POWER EGG SSO administration panel to complete SAML configuration process". An "OK" button is at the bottom right. A red arrow points from the "OK" button to the application listing below.
- Application Listing**: A table showing the configured application. The first row is highlighted:

Application Name	Status	Configuration
POWER EGG SSO SAML認証用	Off for everyone	Google_2024-3-2-93114_SAML2.0 Expires Mar 02, 2024

メタデータのダウンロードは、以下の手順で、メタデータダウンロードの画面へ遷移します。

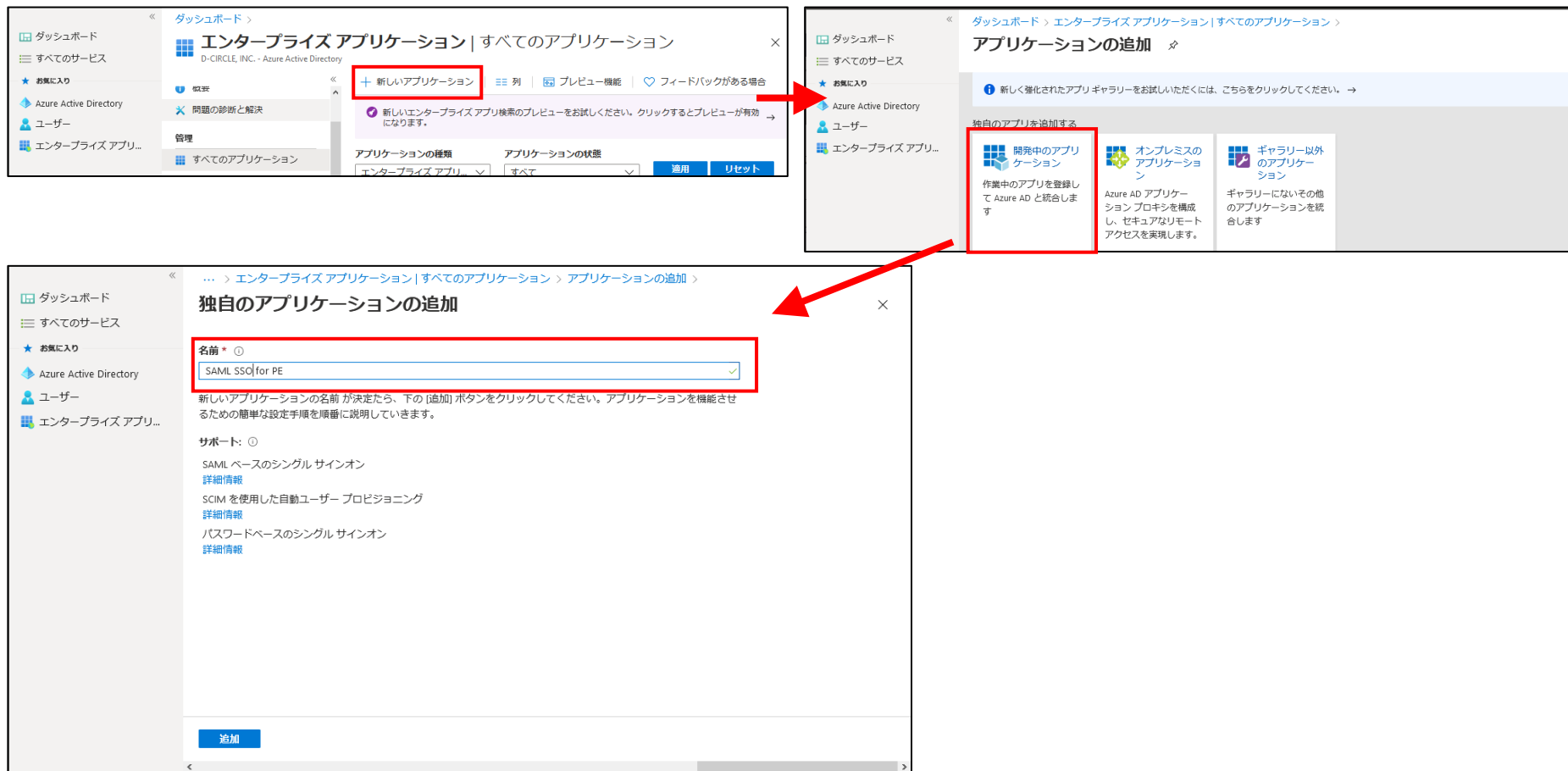


The screenshot illustrates the steps to download metadata in the POWER EGG SSO interface. It shows three panels: 1) The 'Service provider details' section where the 'Download metadata' link is highlighted with a red box. 2) The 'Settings' page where the 'Download metadata' link is also highlighted with a red box. 3) The 'Certificates' page where the 'Download metadata' button is highlighted with a red box. Red arrows indicate the flow from the first panel to the second, and then from the second panel to the third.

- 「DOWNLOAD IDP METADATA」リンクを押すと、メタデータがダウンロードされます。  
このファイルをPOWER EGG側のSAML認証連携設定で、登録を行ってください。
- PC用で登録した設定からダウンロードしてください。  
(スマートフォン用で登録した設定からでも同一内容がダウンロードされます)

# IdP(Azure AD)へのPOWER EGGの登録

Azure ADの場合、管理アカウントで管理画面にログインして、エンタープライズアプリケーションの「新しいアプリケーション」を選択します。次に、「ギャラリー以外のアプリケーション」を選択し、任意のアプリケーション名を入力します。



The image consists of three screenshots from the Azure AD portal, illustrating the process of adding a custom application. Red boxes and arrows highlight the key steps:

- Top Left Screenshot:** Shows the 'Enterprise Applications' management page. A red box highlights the '+ 新しいアプリケーション' (New Application) button.
- Top Right Screenshot:** Shows the 'Add Application' page. A red box highlights the '開発中のアプリケーション' (In Development) option under '独自のアプリを追加する' (Add your own app).
- Bottom Screenshot:** Shows the 'Add your own app' configuration page. A red box highlights the '名前' (Name) input field, which contains 'SAML SSO for PE'.



登録したアプリケーションの「シングルサインオン」、次に「SAML」を選択します。基本的なSAML構成の「編集」リンクをクリックします。



## SAMLによるシングルサインオンのセットアップ

以下をお読みください [構成ガイド](#) SAML SSO for PE を統合するためのヘルプ。

### 1 基本的な SAML 構成 編集

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
ログアウト URL	省略可能

### 2 ユーザー属性とクレーム 編集

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
一意のユーザー ID	user.userprincipalname

下に記載する内容を入力し、「保存」をクリックします。  
 識別子、応答URLには、PC用・スマホ用両方の設定を行います。

### 基本的な SAML 構成

 保存

**識別子 (エンティティ ID) \*** ⓘ

既定の識別子は、IDP-initiated SSO の SAML 応答の対象となります

既定

https://ssltest.poweregg.net/pe4j/	<input checked="" type="checkbox"/>	ⓘ	
https://ssltest.poweregg.net/pe4x/	<input type="checkbox"/>	ⓘ	

**応答 URL (Assertion Consumer Service URL) \*** ⓘ

既定の応答 URL は、IDP-initiated SSO の SAML 応答の宛先になります

既定

https://ssltest.poweregg.net/pe4j/samlLogin	<input checked="" type="checkbox"/>	ⓘ	
https://ssltest.poweregg.net/pe4x/sso/samlLogin	<input type="checkbox"/>	ⓘ	

**サインオン URL** ⓘ

サインオン URL を入力してください

## PC用、スマホ用の設定

識別子	http(s)://(サーバー名):(ポート)/pe4j/
	http(s)://(サーバー名):(ポート)/pe4x/
応答URL	http(s)://(サーバー名):(ポート)/pe4j/samlLogin
	http(s)://(サーバー名):(ポート)/pe4x/sso/samlLogin

メタデータ ファイルをアップロードする シングル サインオン モードの変更 ...

name	user.userprincipalname
一意のユーザー ID	user.userprincipalname

**3** SAML 署名証明書 [編集](#)

状態	アクティブ
拇印	F943FBA075FC594C3C40ACF302DA5048E5E96B3B
有効期限	2023/8/25 9:20:32
通知用メール	matsushita@o.d-circle.com
アプリのフェデレーション メタデータ URL	<a href="https://login.microsoftonline.com/200...">https://login.microsoftonline.com/200...</a>
証明書 (Base64)	<a href="#">ダウンロード</a>
証明書 (未加工)	<a href="#">ダウンロード</a>
フェデレーション メタデータ XML	<a href="#">ダウンロード</a>

フェデレーション メタデータXMLのダウンロードリンクからメタデータをダウンロードします。

ダッシュボード > エンタープライズ アプリケーション | すべてのアプリケーション >

## SAML SSO for PE | ユーザーとグループ

エンタープライズ アプリケーション

[+ ユーザーの追加](#) [編集](#) [削除](#) [資格情報の更新](#) | [列](#) | ...

**i** アプリケーションは、割り当てられたユーザーのアクセス パネルに表示されます。これを表示しないようにするには、プロパティの中で [ユーザーに表示しますか?] を [いいえ] に設定します。

最初の 100 件を表示しています。すべてのユーザーとグループを検索するには、表示名を入力してくだ...

表示名	オブジェクトの種類	割り当てられたロール
アプリケーションの割り当てが見つかりませんでした		

管理

- 概要
- デプロイ計画
- 問題の診断と解決
- ユーザーとグループ

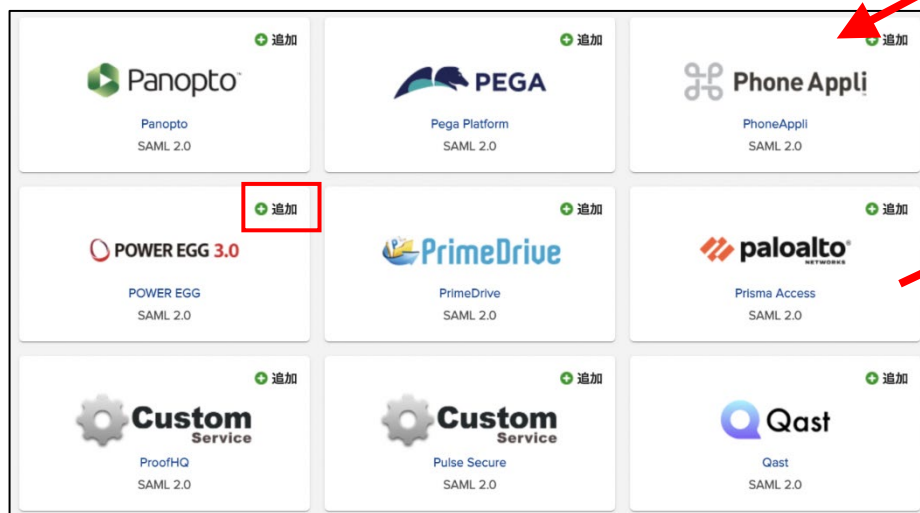
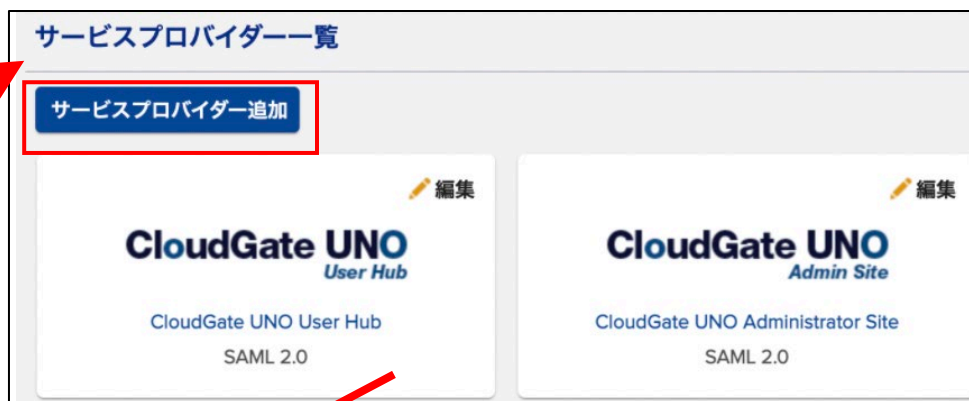
ユーザとグループから、シングルサインオンを許可するユーザを追加します。

# IdP(CloudGate UNO)への登録

CloudGate UNOの場合、管理アカウントで管理画面にログインして、左メニューの一覧から「設定」の「サービスプロバイダー」へ移動、「サービスプロバイダー追加」を選択します。

サービスプロバイダーの一覧から「POWEREGG 3.0」の「追加」を選択して、「表示名」に「POWER EGG」と入力して「追加」を選択します。

※ご利用の契約状況によっては最初から一覧に追加されている場合があります。





# IdP(CloudGate UNO)への登録

サービスプロバイダーに一覧に、「POWER EGG」が追加されていることを確認します。

サービスプロバイダー一覧

サービスプロバイダー追加

 編集	 編集
<b>CloudGate UNO</b> User Hub	<b>CloudGate UNO</b> Admin Site
CloudGate UNO User Hub SAML 2.0	CloudGate UNO Administrator Site SAML 2.0
 編集	
	
POWER EGG SAML 2.0	

サービスプロバイダー一覧のPOWEREGGのサービスの「編集」をクリックして、「シングルサインオン設定」からSAMLの設定を登録し、「保存」をクリックします。

サービスプロバイダー一覧 ▶ POWEREGG

一般設定   **シングルサインオン設定**   プロビジョニング設定

---

### SAML 2.0の設定

サインオンメソッド	SAML 2.0
IdP-initiated SSO	<input type="checkbox"/> いいえ
SP-initiated SSO	<input checked="" type="checkbox"/> はい
Sign-on URL / SAML endpoint URL / SSO URL*	https://test.poweregg.net/pe4j/samlLogin
Issuer / Provider name / Entity ID	https://test.poweregg.net/pe4j/
Assertion consumer service URL	https://test.peoweregg.net/pe4j/samlLogin
Name IDの形式	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress ▼

## PC用の場合の設定

Sign-on URL / SAML endpoint URL / SSO URL	http(s)://(サーバー名):(ポート)/pe4j/samlLogin
Issuer / Provider name / Entity ID	http(s)://(サーバー名):(ポート)/pe4j/
Assertion consumer service URL	http(s)://(サーバー名):(ポート)/pe4j/samlLogin

## スマートフォン用の場合の設定

Sign-on URL / SAML endpoint URL / SSO URL	http(s)://(サーバー名):(ポート)/pe4x/?saml#/login
Issuer / Provider name / Entity ID	http(s)://(サーバー名):(ポート)/pe4x/
Assertion consumer service URL	http(s)://(サーバー名):(ポート)/pe4x/sso/samlLogin

メタデータについて、「シングルサインオン設定」の「SAML 2.0 メタデータ」からダウンロードしてください。

一般設定	<b>シングルサインオン設定</b>	プロビジョニング設定
------	--------------------	------------

---

### SAML 2.0のIdP情報

プロバイダー名	https://echizen.cloudgate.jp/sso/d-circle/ <a href="#">📄 コピー</a>
ログインURL	https://echizen.cloudgate.jp/sso/d-circle/login.xhtml <a href="#">📄 コピー</a>
ログアウトURL	https://echizen.cloudgate.jp/sso/d-circle/logout.xhtml <a href="#">📄 コピー</a>
証明書	<a href="#">📄 ダウンロード</a>
証明書のフィンガープリント (SHA1)	AD 3F D6 01 9A 91 C1 DC 59 29 82 9B 5F 1F 62 4F 1D 88 8F 74 <a href="#">📄 コピー</a>
証明書のフィンガープリント (SHA256)	EB EB E7 CE 1F 61 DA 2E D7 2C 82 8B 72 9E 9C F7 35 91 1B 5B D2 FF A5 FB 4D EF 98 BC 51 57 86 5C <a href="#">📄 コピー</a>
証明書のフィンガープリント (MD5)	C8 8C C6 E6 D6 C0 ED E9 CF EA 1D 47 41 97 1E D3 <a href="#">📄 コピー</a>
<b>SAML 2.0 メタデータ</b>	<a href="#">📄 ダウンロード</a>

# IdP(CloudGate UNO)への登録

サービスプロバイダーの設定後、SAML認証を利用するユーザーについて、ユーザーごとに設定を有効にしてください。

メニューの「ユーザー」をクリックし、「ユーザー一覧」から対象のユーザーをクリックし、「サービス」からPOWEREGGのサービスへチェックを入れ、「保存」をクリックしてください。

※POWEREGGのサービスに記載されている「アカウントID」がPOWEREGGの各ユーザーの「メモ1」で設定するユーザーIDとなります。

アカウント管理

- ユーザー
- グループ
- 連絡先
- ロール
- 一括処理

ユーザー

現在の階層 ディサークル > d-circle

作成 削除 移動 その他の操作

ユーザーID	表示名	サービス	プロフィール	ステータス	最終サインオン
ooishi@d-circle	大石 学	デフォルト			2021/08/04 14:50:32
temp_admin@d-circle	temp_admin	デフォルト			2021/08/10 10:35:24

作成 削除 移動 その他の操作

サービス

- CloudGate UNO User Hub  
アカウントID\* ooishi@d-circle
- CloudGate UNO Administrator Site  
アカウントID\* ooishi @d-circle
- CloudGate UNO Address Book  
アカウントID\* ooishi@d-circle
- POWEREGG  
アカウントID\* ooishi

ロールを割り当てる必要があります。割り当てない場合は操作できません。



POWER EGGからIdPに接続するための情報として、以下の情報を設定します。

## POWER EGG[システム設定]-[システム環境の設定]-[SAML認証設定]

### システム環境の設定

システム環境の設定(SAML認証設定)

設定

\* は必須項目です。

**SAML認証**  有効にする  無効にする  
SAML認証を有効にするかどうかを設定します。

**SAML認証用** 添付ファイルを追加(計1件)

**メタデータ \***   
 全てを選択  選択を解除  選択したファイルを削除  
Identity Provider (IdP) のメタデータを選択します。

**ACS URL (PC用) \***   
IdP側からのPostBackURLを設定します。(PC用)

**ACS URL (スマートフォン用)**   
IdP側からのPostBackURLを設定します。(スマートフォン用)

設定

## 【各項目の設定情報】

SAML認証 : SAML認証連携を使用する場合は「有効にする」を選択してください  
(初期状態時は「無効にする」)

SAML認証用メタデータ : IdPからダウンロードしたメタデータを添付し、登録してください

ACS URL(PC用) : 以下のURLで設定します。  
http(s)://(サーバー名※):(ポート)/pe4j/samlLogin  
※ サーバー名、または、IPアドレス  
例) https://peserver/pe4j/samlLogin

ACS URL(スマートフォン用): 以下のURLで設定します。  
http(s)://(サーバー名※):(ポート)/pe4x/sso/samlLogin  
※ サーバー名、または、IPアドレス  
例) https://peserver/pe4x/sso/samlLogin

※ ACS URL(PC用)、ACS URL(スマートフォン用)の値はIdP側に登録した内容と一致させるようにしてください。

- PCリマインダー、リマインダー for iPhone、リマインダー for Androidは、SAML認証のシングルサインオンには対応していません。（※POWER EGGに登録されているユーザーIDとパスワードでログインする必要があります。）
- ログインしていない状態から、POWER EGGの特定のページにアクセスするときに表示される「ログイン画面」はSAML認証連携に対応していません。
- Office365連携との併用はできません。また、IdPについても、複数のIdPの併用ができません。
- 弊社で検証を行っておりますIdPにつきましては、2020年11月時点で、HENNGE One、Gsuite、Azure AD、IIJ IDサービスとなっております。また、いずれも、PC版、スマートフォン版からのSAML認証連携に対応しております。
- IdPとPOWER EGG間の通信で使用可能なプロトコル（HTTP、HTTPS）については、ご利用になるIdP側の制限に従います。IdPによっては、HTTPS プロトコルのみ接続許可している場合もありますので、詳細はIdP提供元にご確認ください。
- IdP(IIJ IDサービス)へのPOWER EGGの登録については、IIJ様にお問い合わせください。