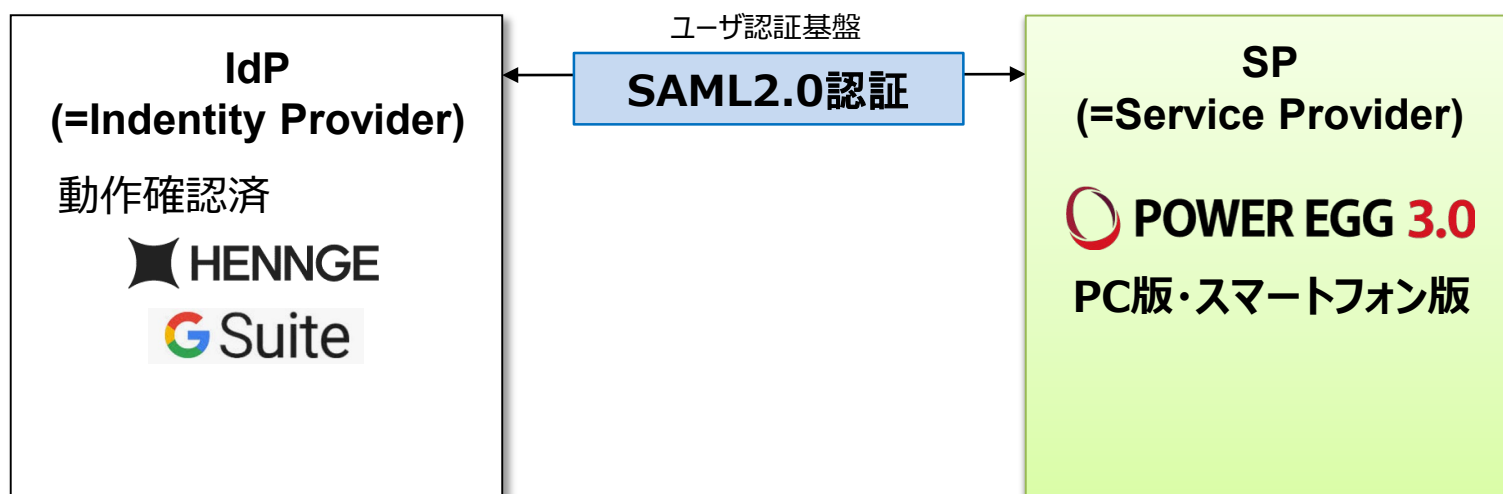


# POWER EGG 3.0 SAML認証連携

2019年9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

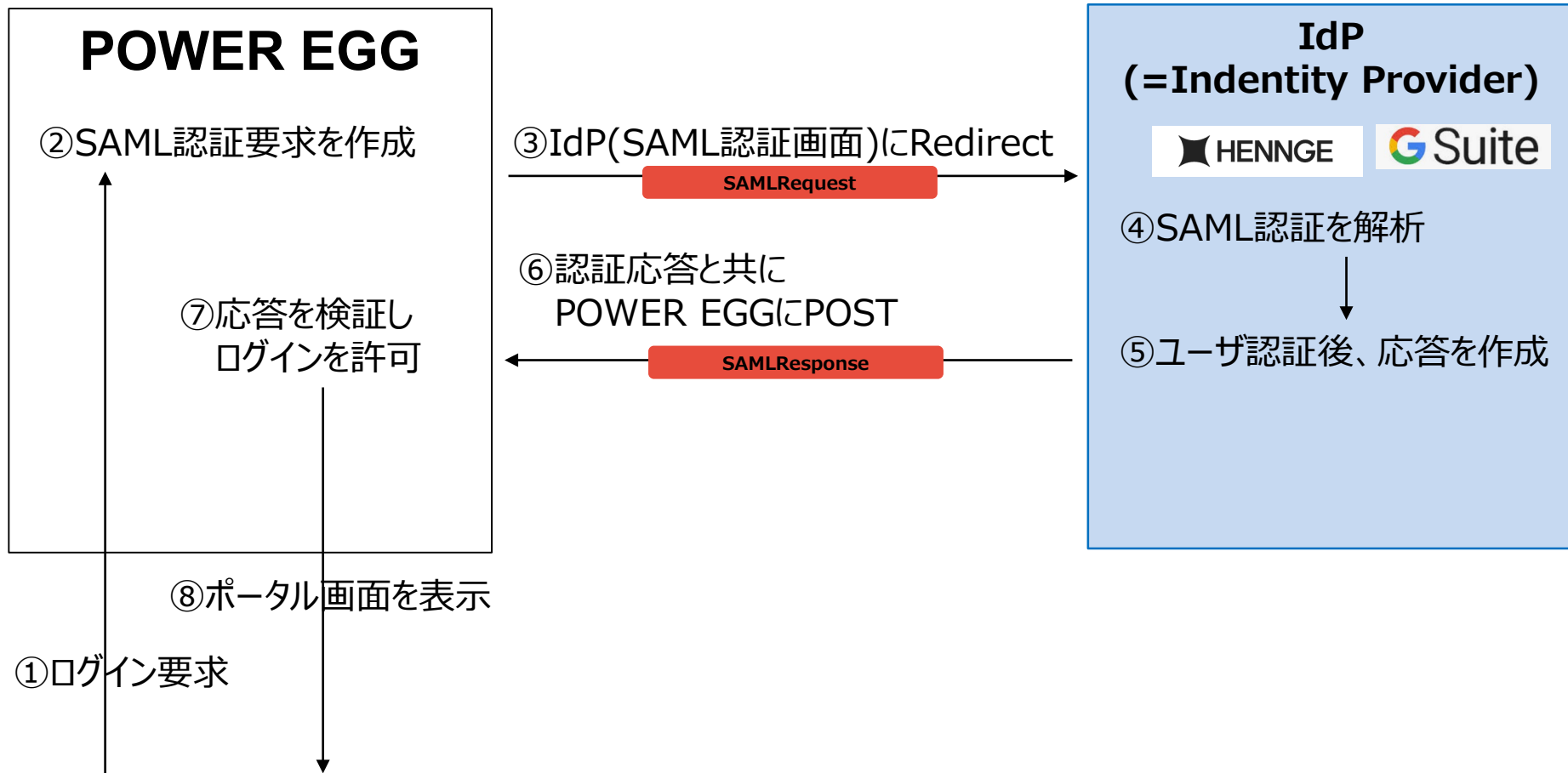
## ■ SAML2.0連携モデル



※ 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`

スマートフォン版 :

`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の場合、ログインID、Gsuiteの場合、メールアドレス)

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。

# IdP(HDEOne)へのPOWER EGGの登録

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 interface. On the left, the 'サービスプロバイダー設定' (Service Provider Settings) menu item is highlighted with a red box. A red arrow points from this menu item to the 'サービスプロバイダーの追加' (Add Service Provider) button in the main content area. Another red arrow points from this button to the 'カスタム' (Custom) button in the 'サービスプロバイダーの追加' dialog box. A third red arrow points from the 'カスタム' button to the '次へ' (Next) button at the bottom of the dialog box. The dialog box contains the following fields:

- 名前: POWER EGG SSO
- ACS URL: https://xxx.xxx.xxx.xxx/pe4j/samlLogin
- Entity ID: https://xxx.xxx.xxx.xxx/pe4j/
- Name ID: {user.username}
- ログインURL: [empty]
- 固有番号: [empty]
- セッション有効時間 (時間): 8

## PC用設定

名前	POWER EGG SSO
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
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)/pe4x/sso/samlLogin
Entity ID	http(s)://(サーバー名):(ポート)/pe4x
Name 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。



サービスプロバイダーの追加

成功: サービスプロバイダーが追加されました

プリセット + メタデータアップロード カスタム リンク

名前 ? POWER EGG SSO

ACS URL ? https://xxx.xxx.xxx.xxx/pe4j/samlLogin

Entity ID ? https://xxx.xxx.xxx.xxx/pe4j

Name ID ? {user.username}

ログインURL ?

固有番号 ?

+ 次へ



サービスプロバイダー設定

成功: サービスプロバイダーが変更されました

基本設定

名前 ? POWER EGG SSO

ダイレクトログインURL ? https://ap.sso.hdems.com/sso/o.d-circle.com/spc

ACS URL ? https://xxx.xxx.xxx.xxx/pe4j/samlLogin

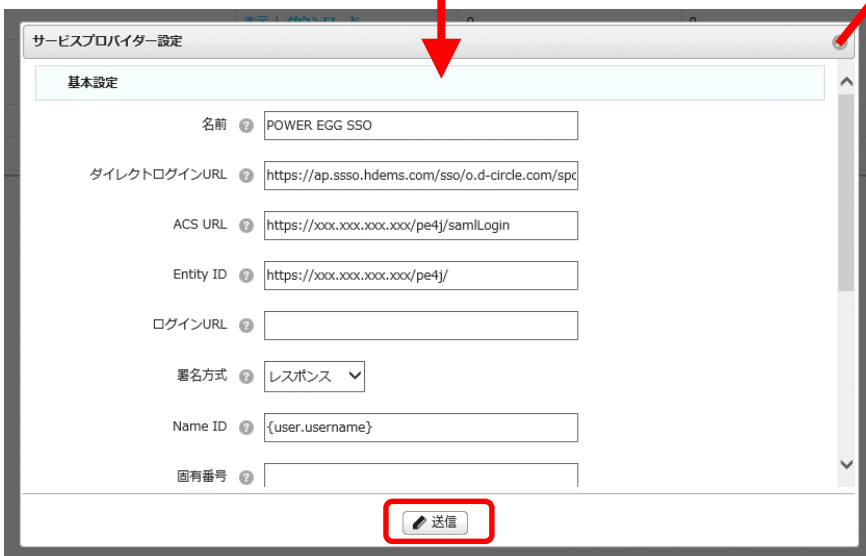
Entity ID ? https://xxx.xxx.xxx.xxx/pe4j

ログインURL ?

署名方式 ? レスポンス

Name ID ? {user.username}

送信



サービスプロバイダー設定

基本設定

名前 ? POWER EGG SSO

ダイレクトログインURL ? https://ap.sso.hdems.com/sso/o.d-circle.com/spc

ACS URL ? https://xxx.xxx.xxx.xxx/pe4j/samlLogin

Entity ID ? https://xxx.xxx.xxx.xxx/pe4j/

ログインURL ?

署名方式 ? レスポンス

Name ID ? {user.username}

固有番号 ?

送信



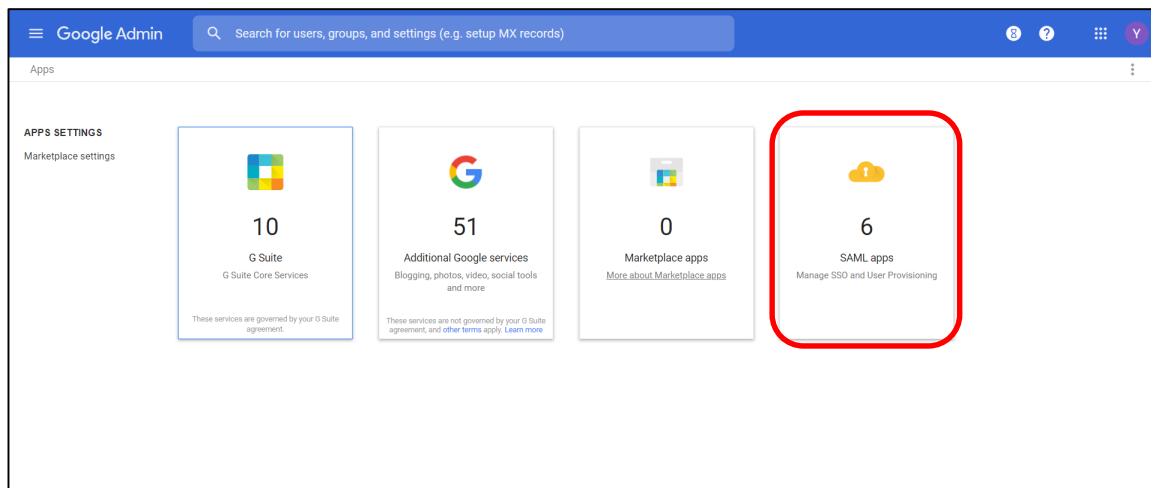
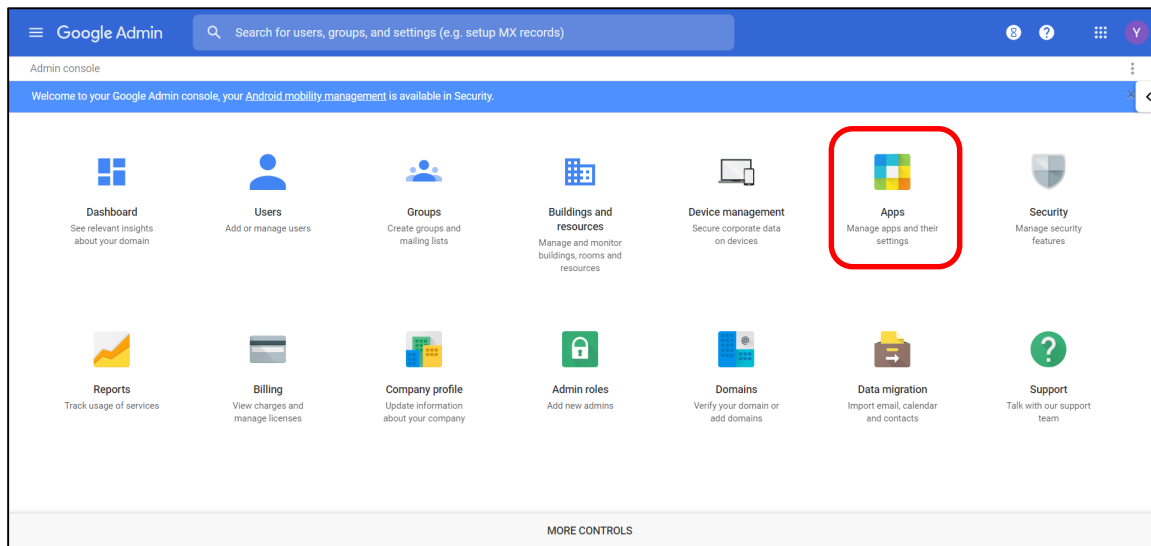
登録すると、一覧上に、以下の内容で表示されます。（完了と表示されていれば、確定されています）

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

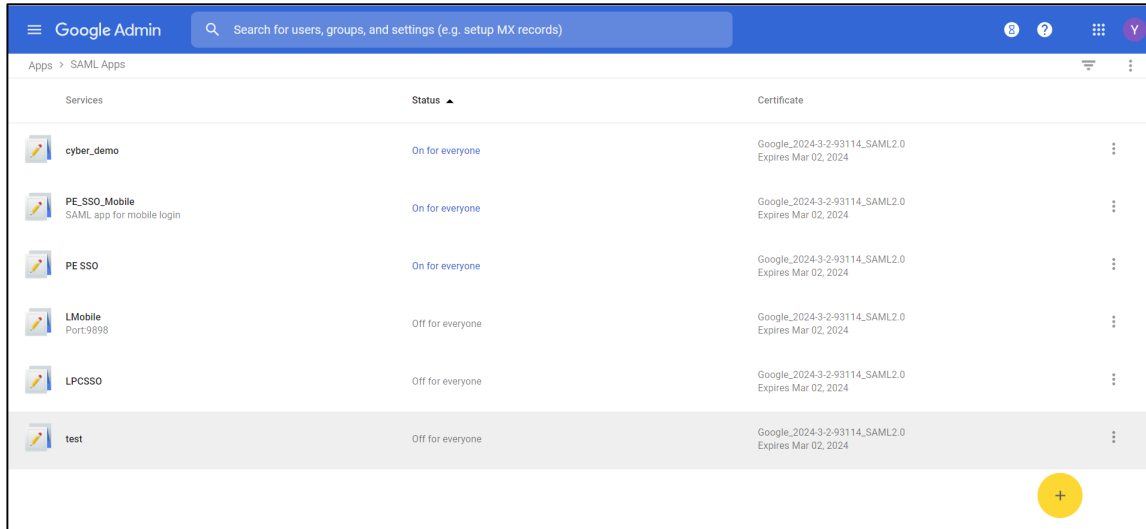
「ダウンロード」リンクをクリックすると、メタデータがダウンロードされます。  
このファイルをPOWER EGG側のSAML認証連携設定で、登録を行ってください。

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）

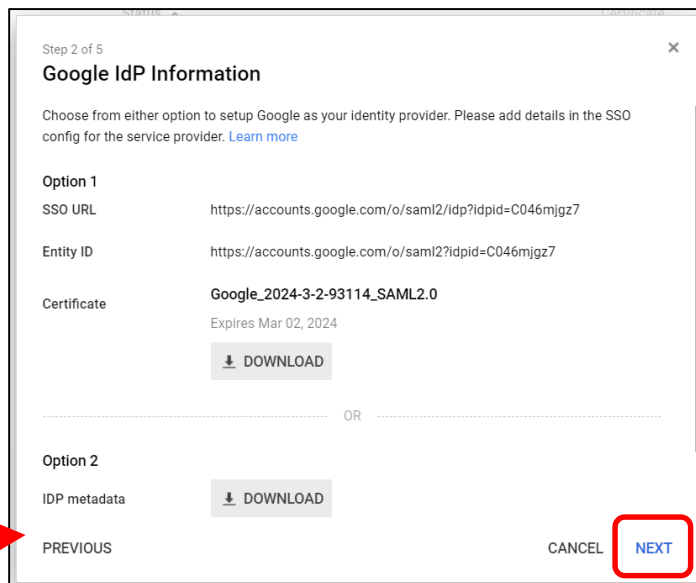
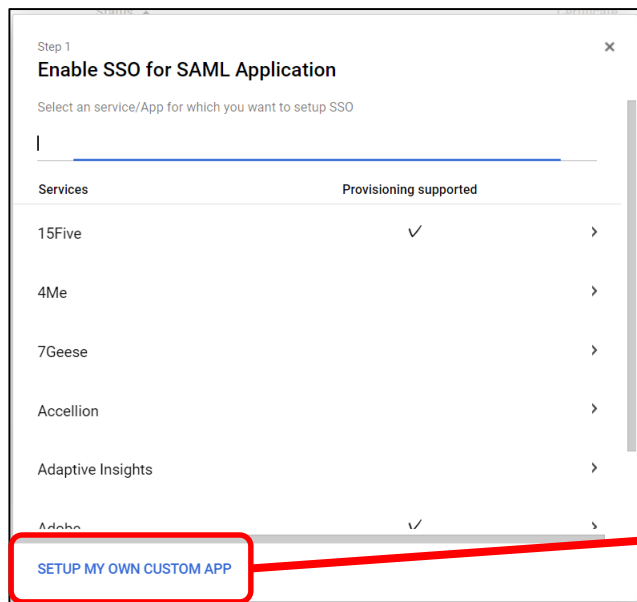
GSuiteの場合、管理アカウントで管理画面にログインして、「Apps」リンクをクリックします。次に、「SAML apps」リンクをクリックします。



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 \* POWER EGG SSO app-id: power\_egg\_sso

Description SAML認証用

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 \* https://xxx.xxx.xxx.xxx/pe4j/samlLogin

Entity ID \* https://xxx.xxx.xxx.xxx/pe4j

Start URL

Signed Response

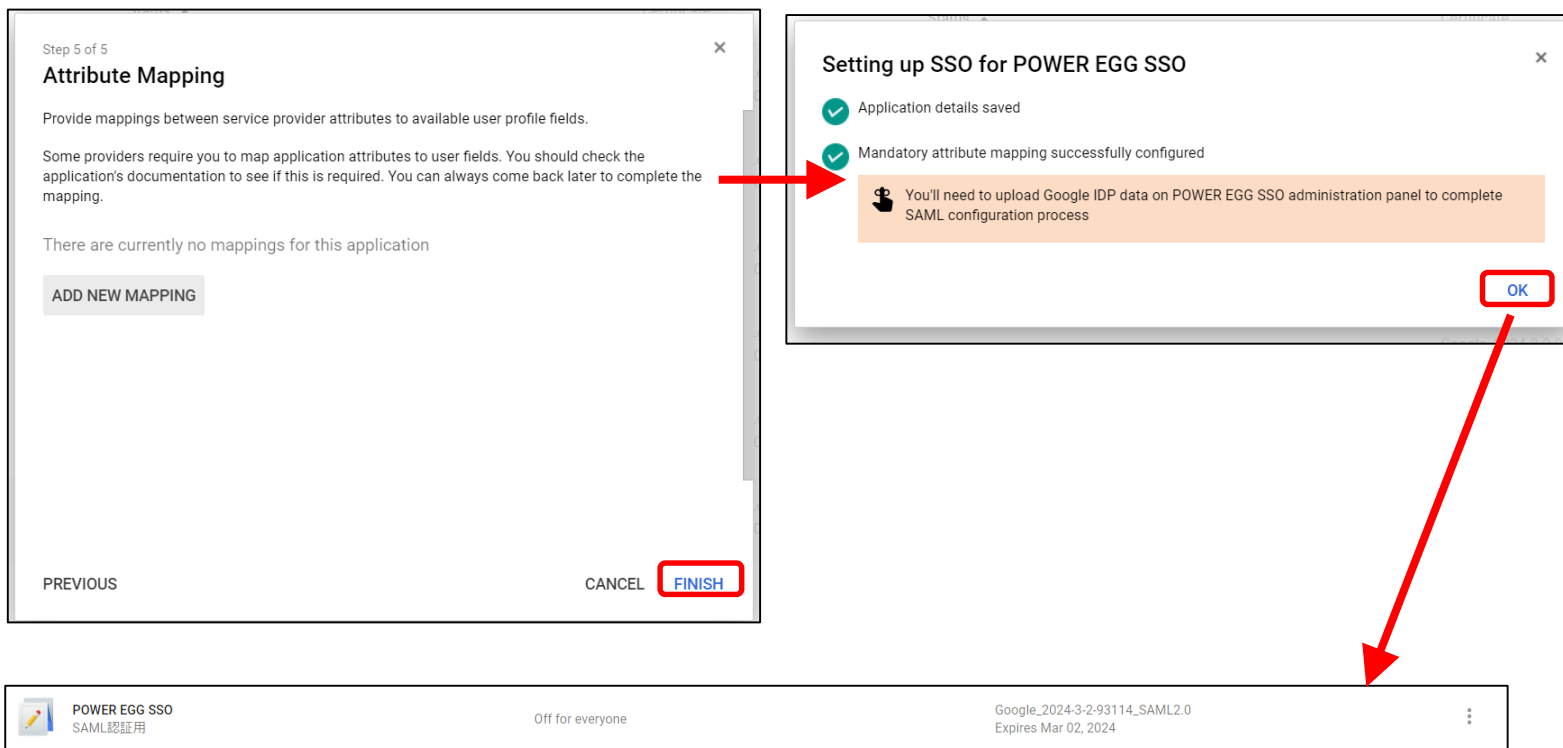
Name ID Basic Information Primary Email

Name ID Format UNSPECIFIED

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。

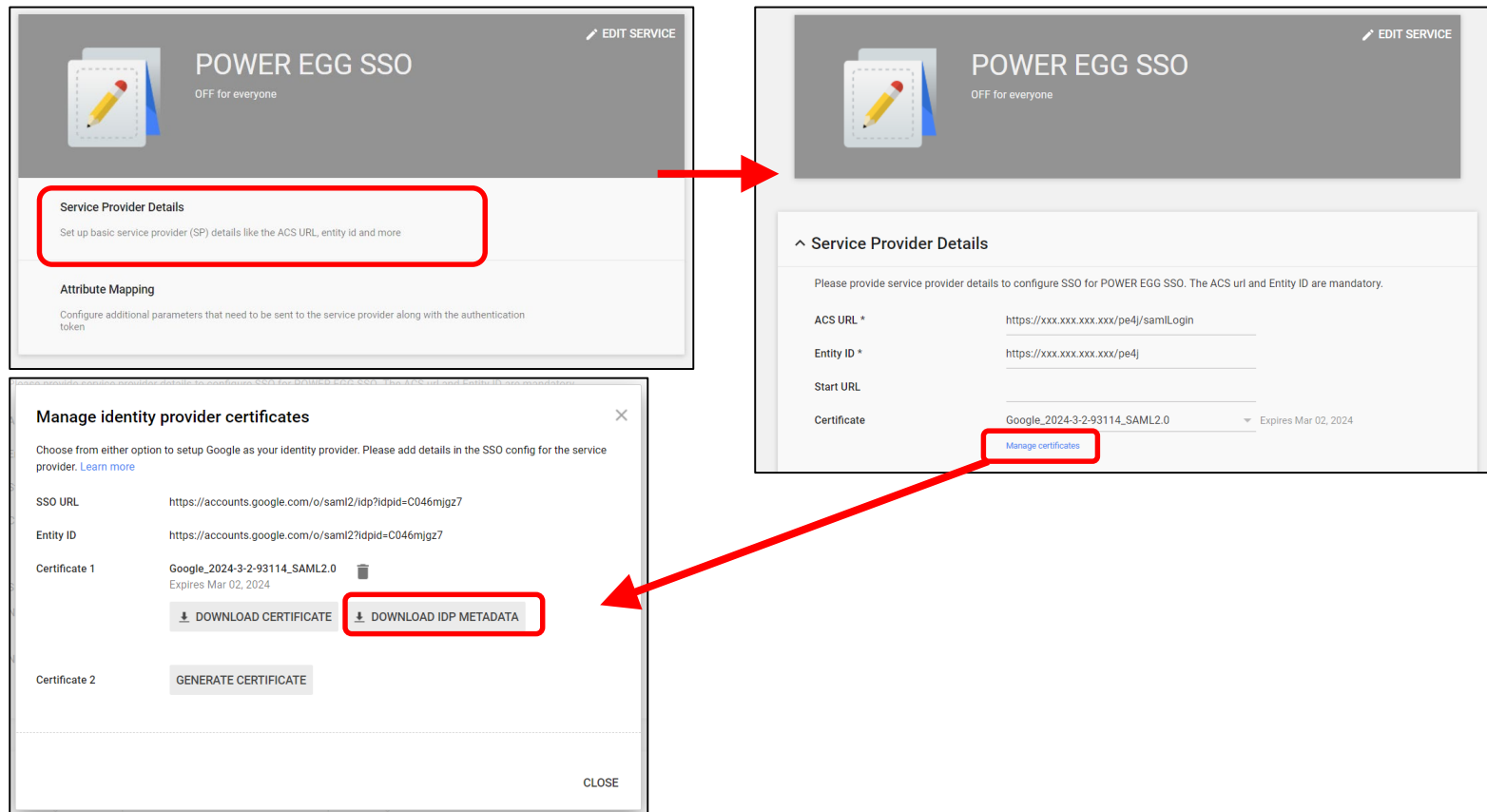


The image shows a three-step process for SSO configuration:

- Attribute Mapping:** A dialog box titled "Step 5 of 5 Attribute Mapping" with instructions to provide mappings between service provider attributes and user profile fields. It includes an "ADD NEW MAPPING" button and "PREVIOUS", "CANCEL", and "FINISH" buttons at the bottom. A red box highlights the "FINISH" button.
- Setting up SSO for POWER EGG SSO:** A confirmation dialog box showing two successful steps: "Application details saved" and "Mandatory attribute mapping successfully configured". It includes a warning message: "You'll need to upload Google IDP data on POWER EGG SSO administration panel to complete SAML configuration process" and an "OK" button. A red box highlights the "OK" button.
- SSO Configuration List:** A table showing the configured SSO application. A red arrow points from the "OK" button in the previous dialog to this table.

Icon	Application Name	Status	Configuration	Expiration
	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 image shows a sequence of two screenshots from the POWER EGG SSO configuration interface. The first screenshot shows the 'Service Provider Details' section with a red box around the text 'Set up basic service provider (SP) details like the ACS URL, entity id and more'. A red arrow points from this box to the second screenshot. The second screenshot shows the 'Service Provider Details' form with fields for ACS URL, Entity ID, Start URL, and Certificate. A red box highlights the 'Manage certificates' link below the Certificate field. A second red arrow points from this link to a third screenshot. The third screenshot is a modal dialog titled 'Manage identity provider certificates' with a 'CLOSE' button. It contains fields for SSO URL and Entity ID, and a table of certificates. The 'Certificate 1' row shows 'Google\_2024-3-2-93114\_SAML2.0' with an expiration date of 'Expires Mar 02, 2024'. Below this row, there are two buttons: 'DOWNLOAD CERTIFICATE' and 'DOWNLOAD IDP METADATA', with the latter highlighted by a red box.

- 「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)

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認証連携設定]

### 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、2019年9月時点で、HENNGE One、GSuiteとなっております。また、どちらも、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。