



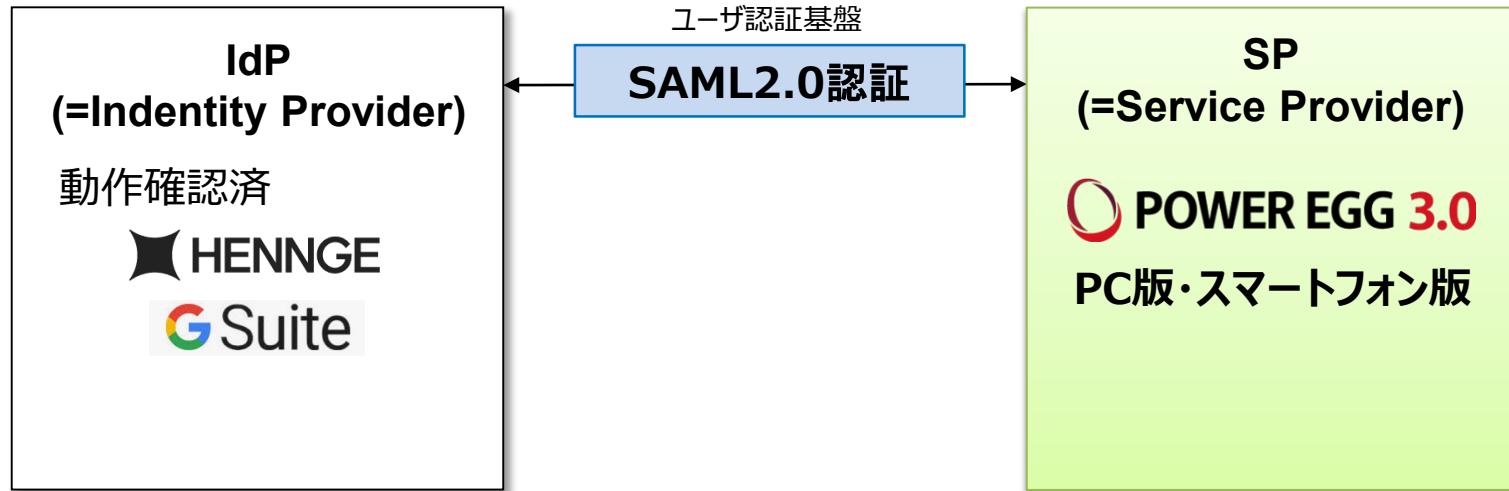
POWER EGG 3.0

SAML認証連携

2020年7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

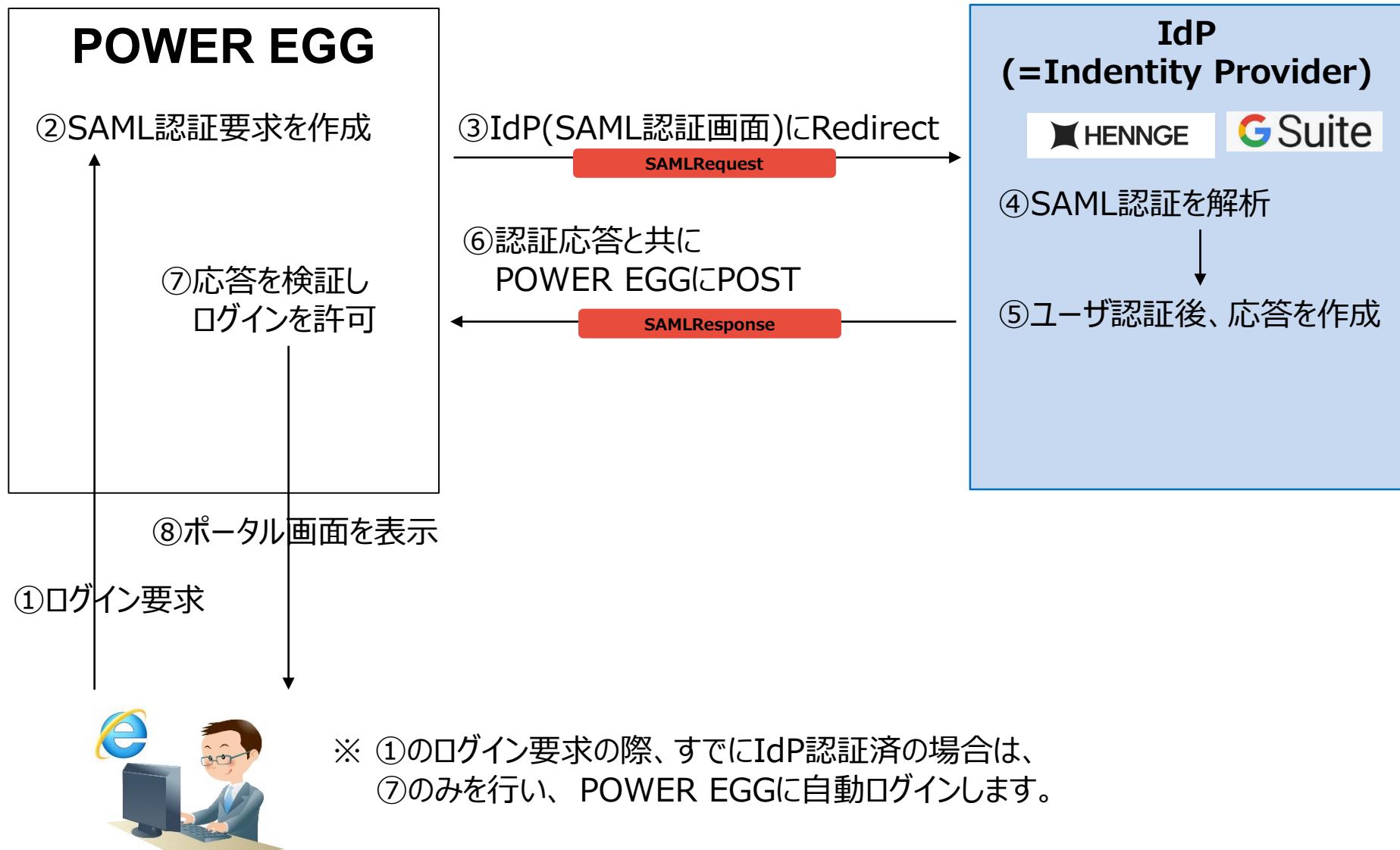
■ SAML2.0連携モデル



※ 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。



連携イメージ図

POWER EGG 3.0

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://\(サーバー名\):\(ポート\)/pe4j/samlLogin](http://(サーバー名):(ポート)/pe4j/samlLogin)

スマートフォン用 :

[http://\(サーバー名\):\(ポート\)/pe4x/?saml#/login](http://(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



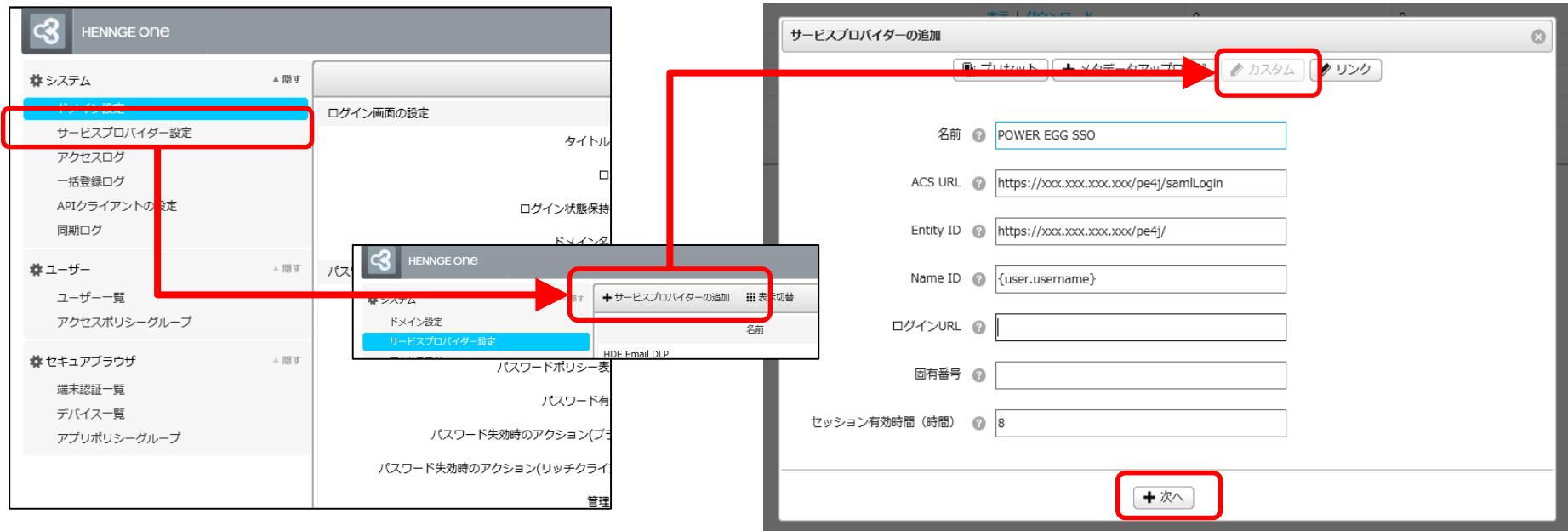
POWER EGG社員情報のメモ1：imaoka

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。



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}

IdP(HDEOne)へのPOWER EGGの登録



「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/pe4j/samlLogin
Entity ID: https://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.hdem.com/sso/o.d-circle.com/spc
ACS URL: https://xxx.xxx.xxx/pe4j/samlLogin
Entity ID: https://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.hdem.com/sso/o.d-circle.com/spc
ACS URL: https://xxx.xxx.xxx/pe4j/samlLogin
Entity ID: https://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）



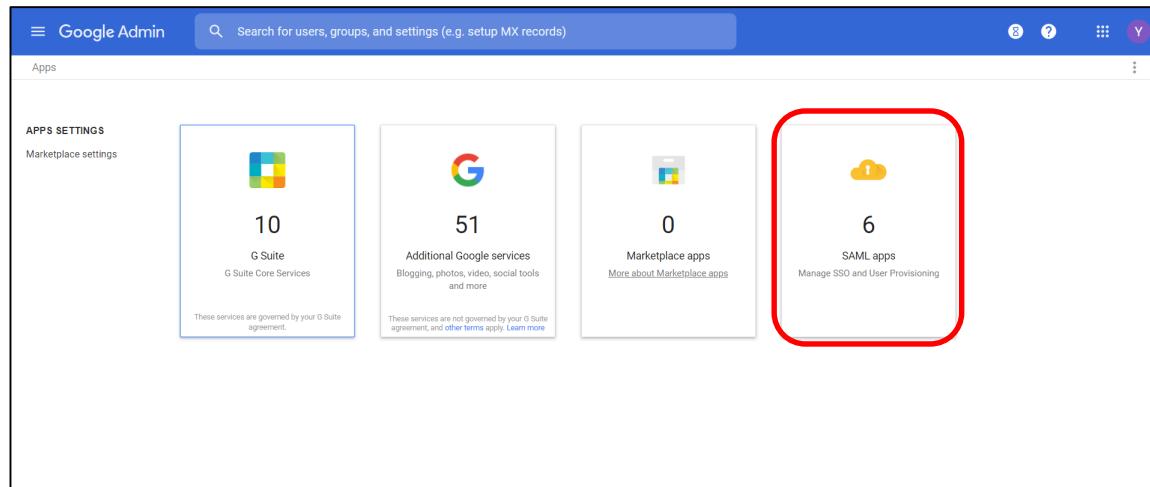
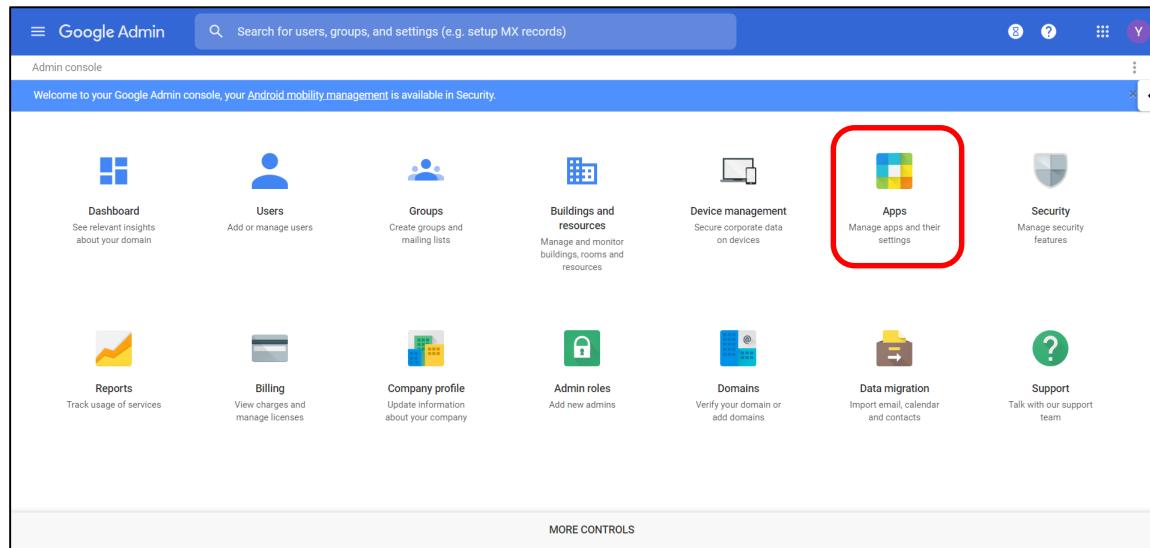
「ダウンロード」リンクをクリックすると、メタデータがダウンロードされます。
このファイルをPOWER EGG側のSAML認証連携設定で、登録を行ってください。

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)

IdP(GSuite)へのPOWER EGGの登録



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。



IdP(GSuite)へのPOWER EGGの登録



新規で登録する場合、+ボタンをクリックします。

The screenshot shows the Google Admin interface for managing SAML applications. The page title is "Google Admin" and the sub-section is "SAML Apps". A search bar at the top is empty. The main content is a table with the following data:

Services	Status	Certificate
cyber_demo	On for everyone	Google_2024-3-2-93114_SAML2.0 Expires Mar 02, 2024
PE_SSO_Mobile SAML app for mobile login	On for everyone	Google_2024-3-2-93114_SAML2.0 Expires Mar 02, 2024
PE_SSO	On for everyone	Google_2024-3-2-93114_SAML2.0 Expires Mar 02, 2024
LMobile Port:9898	Off for everyone	Google_2024-3-2-93114_SAML2.0 Expires Mar 02, 2024
LPCSSO	Off for everyone	Google_2024-3-2-93114_SAML2.0 Expires Mar 02, 2024
test	Off for everyone	Google_2024-3-2-93114_SAML2.0 Expires Mar 02, 2024

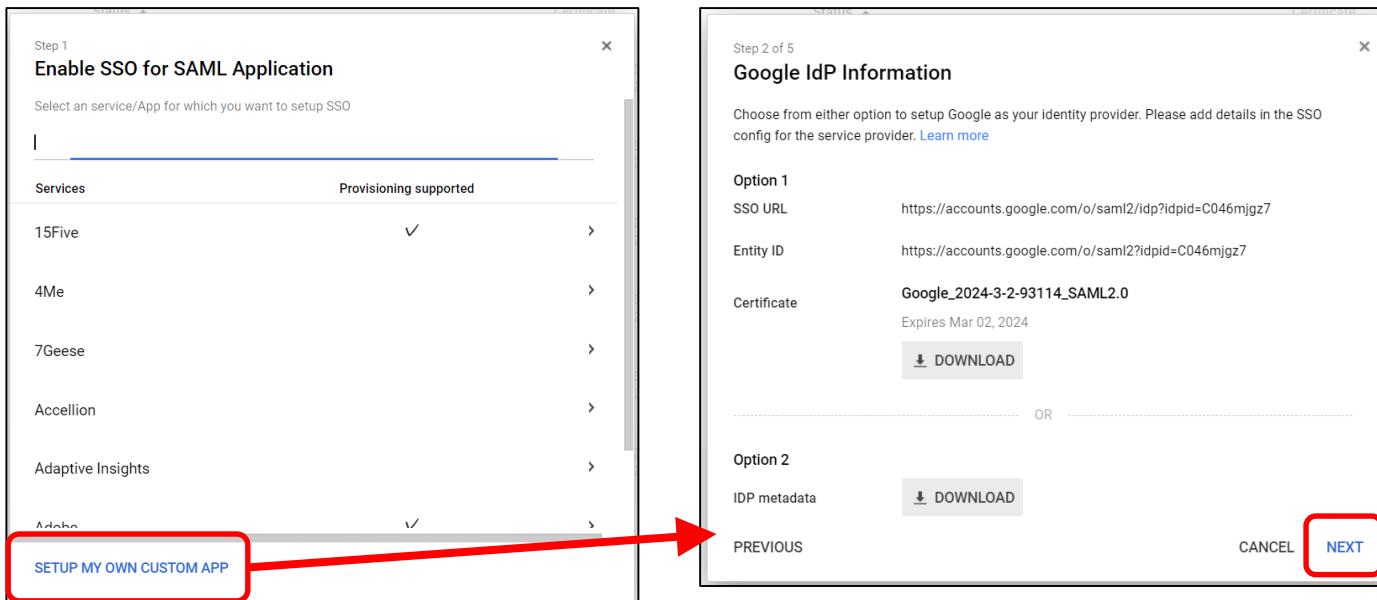
A large yellow circle with a black plus sign (+) is overlaid on the bottom right of the table area, indicating where to click to add a new service.

IdP(GSuite)へのPOWER EGGの登録

POWER EGG 3.0

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。



IdP(GSuite)へのPOWER EGGの登録

POWER EGG 3.0

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	<input type="button" value="CHOOSE FILE"/>	
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	<input type="checkbox"/>	
Signed Response	<input type="checkbox"/>	
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

IdP(GSuite)へのPOWER EGGの登録



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。

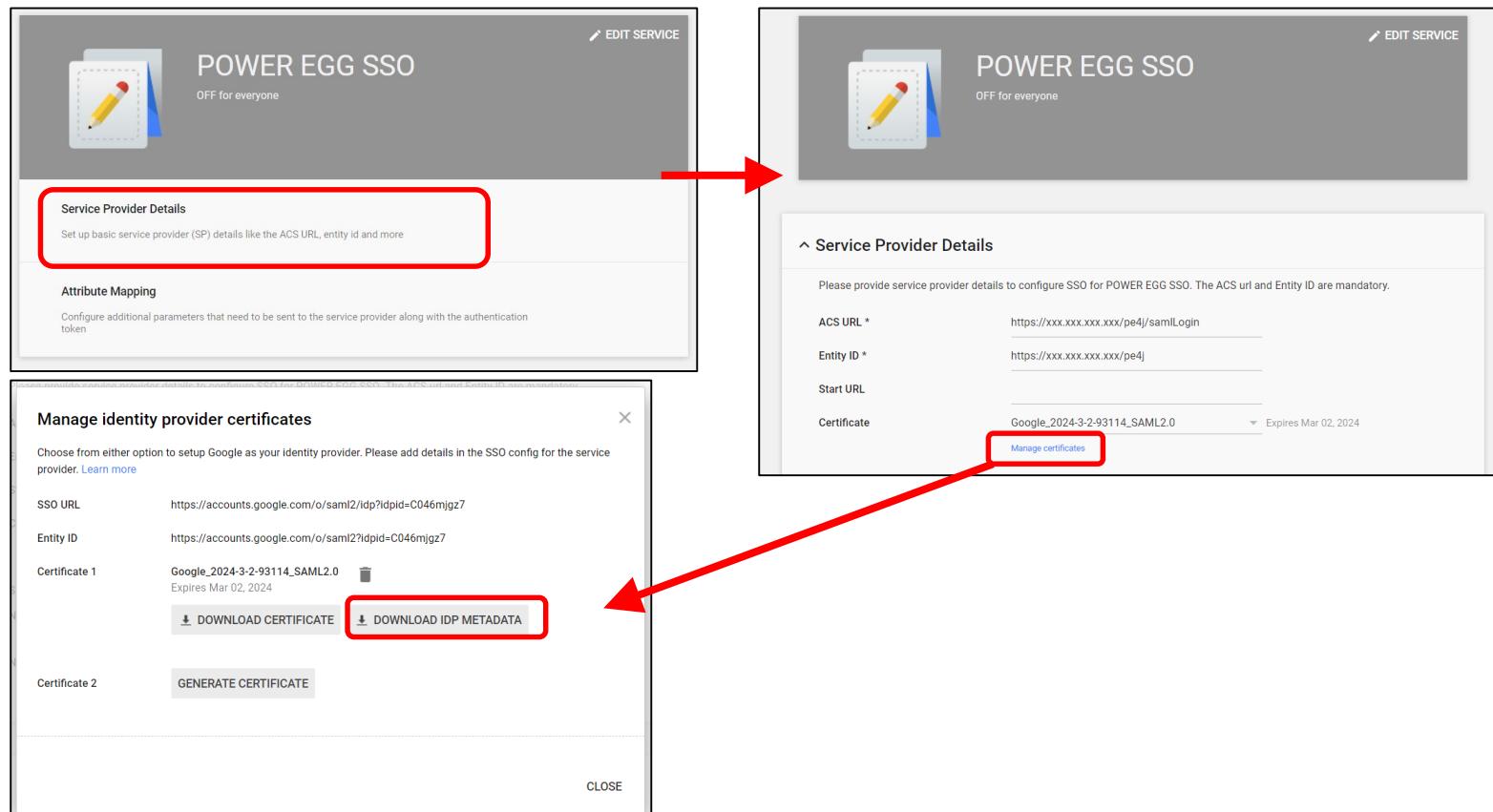
The screenshot shows the configuration process for setting up SSO. It consists of two main windows and a summary table.

- Attribute Mapping Window:** A modal window titled "Attribute Mapping" with the sub-instruction "Step 5 of 5". It contains a note about mapping service provider attributes to user profile fields and a message stating "There are currently no mappings for this application". A red arrow points from the "FINISH" button in this window to the "OK" button in the success message window.
- Success Message Window:** A modal window titled "Setting up SSO for POWER EGG SSO" with two green checkmarks:
 - Application details saved
 - Mandatory attribute mapping successfully configuredA message box 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 of this window, also highlighted with a red box.
- Summary Table:** A table at the bottom showing the configuration status for "Google_2024-3-2-93114_SAML2.0". It includes columns for "POWER EGG SSO", "SAML認証用", "Status" (Off for everyone), and "Expires Mar 02, 2024".

IdP(GSuite)へのPOWER EGGの登録



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。



- ・「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認証設定]

システム環境の設定

※ 共通操作

※ ログイン・パスワード環境

※ ナビビュー分割画面

※ ナビビュー環境

※ メール環境

※ ログ・閲覧履歴環境

※ 個人設定

※ テーマ設定

※ SAML認証設定

● 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 * federationmetadata-2.xml(2KB)
※ 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) * https://xxx.xxx.xxx.xxx/pe4j/samlLogin
IdP側からのPostBackURLを設定します。(PC用)

ACS URL (スマートフォン用) https://xxx.xxx.xxx.xxx/pe4x/sso/samlLogin
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。

- PCI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。
- 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。