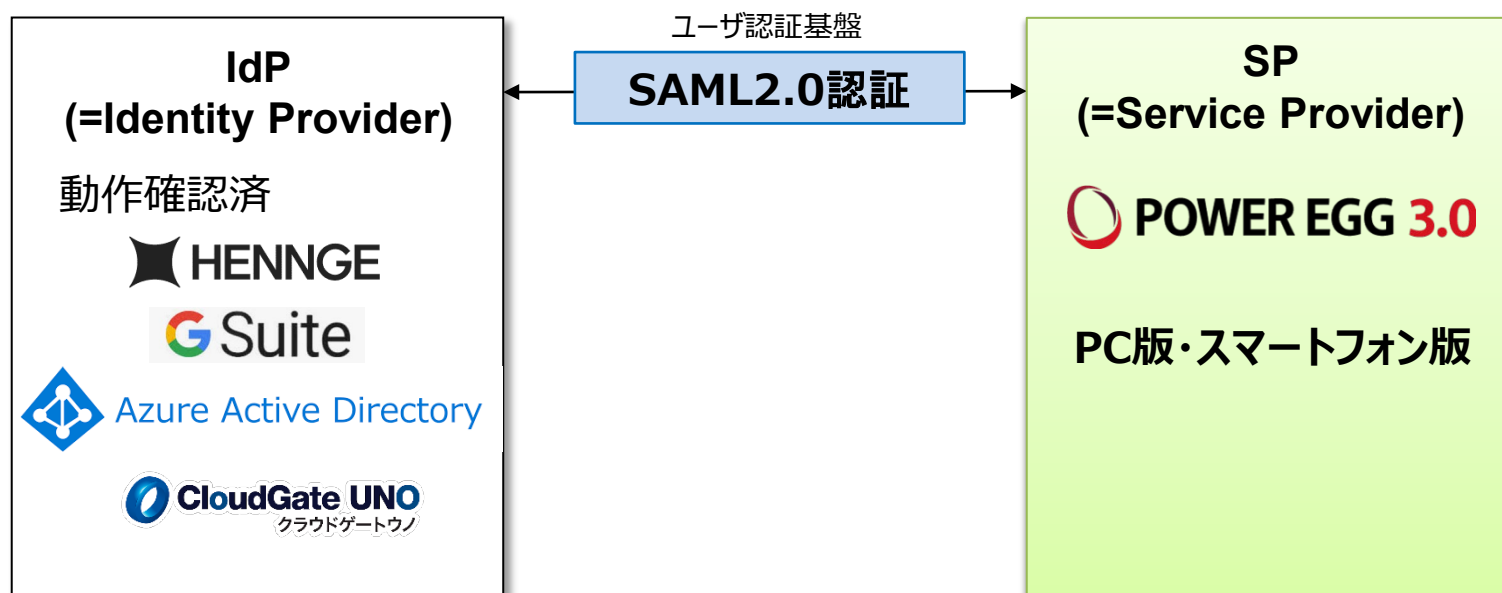


POWER EGG 3.0 SAML認証連携

2023年1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 |
| 2023/01/16 6.0版 | Gsuite、Azure ADのUI変更に伴い、画像を変更 一部表記を修正 留意事項を修正 |

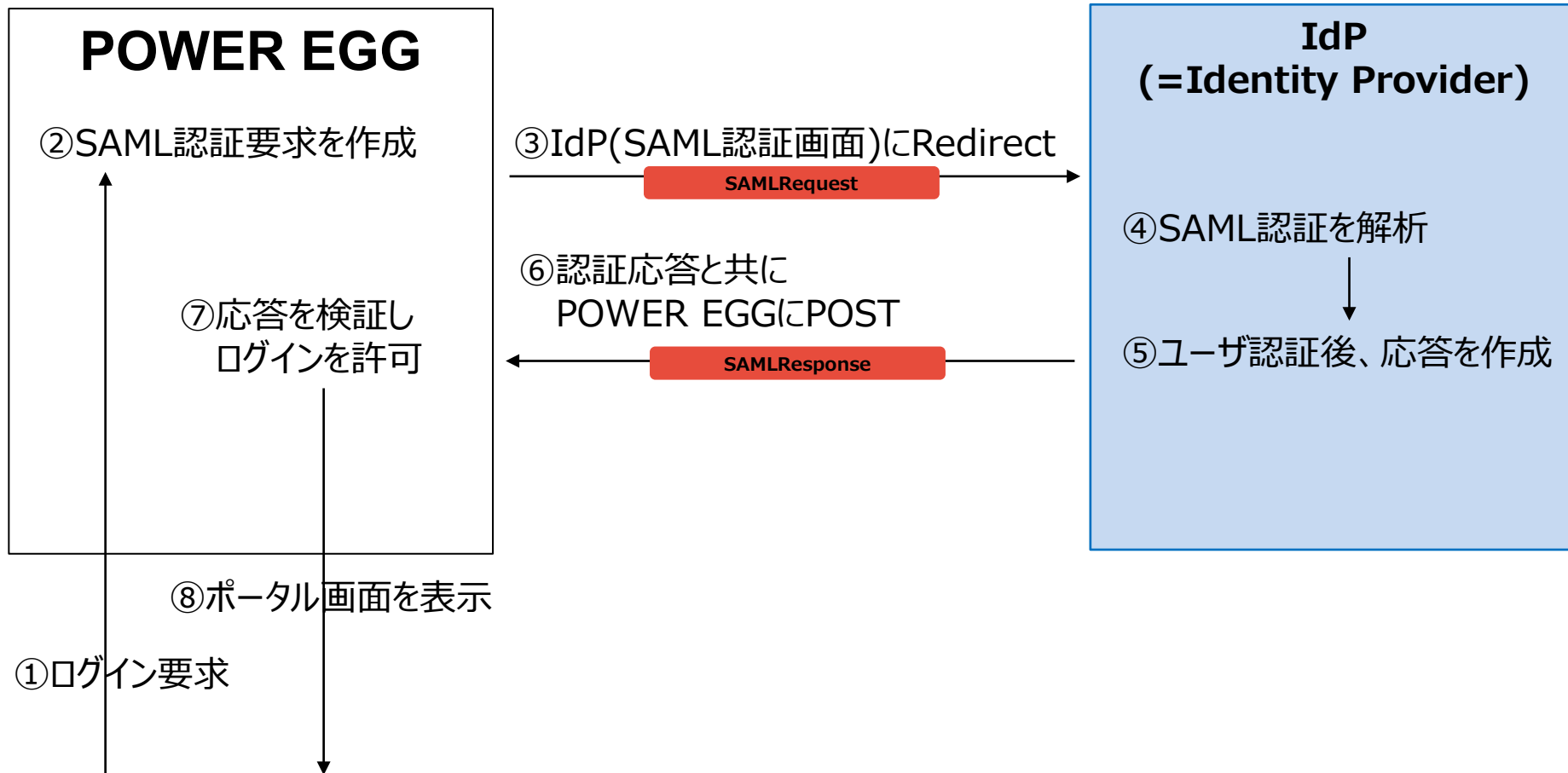
■ SAML2.0連携モデル



※ 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いるのは、HENNGE One、Gsuite、Azure AD、IIJ ID、CloudGate UNOサービスです。



※ 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。

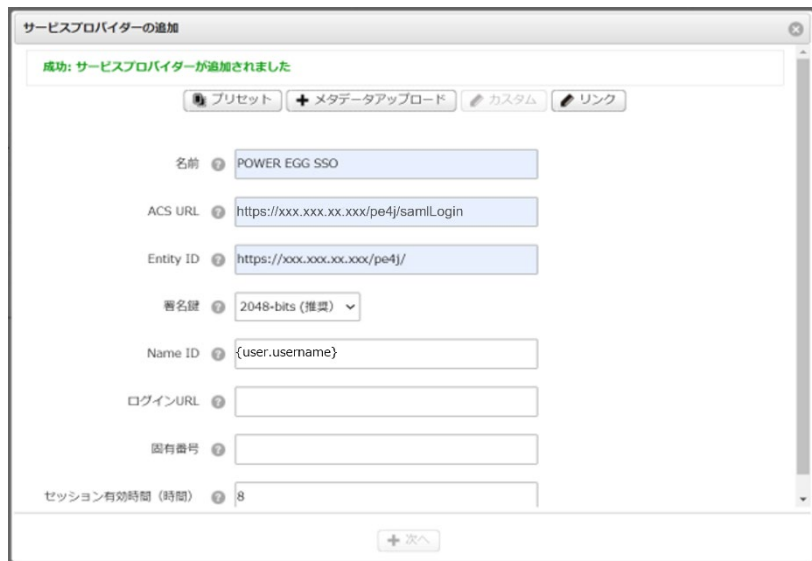
IdP(HDEOne)へのPOWER EGGの登録

HENNGE Oneの場合、管理アカウントで管理画面にログイン後、「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」ボタンをクリックします。表示された画面で「カスタム」ボタンをクリックし、下記の内容を入力後、「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。



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 ① POWER EGG SSO

ACS URL ① https://xxx.xxx.xx.xxx/pe4j/samlLogin

Entity ID ① https://xxx.xxx.xx.xxx/pe4j/

署名鍵 ① 2048-bits (推奨) ▼

Name ID ① {user.username}

ログインURL ①

固有番号 ①

セッション有効時間 (時間) ① 8

+ 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 ① POWER EGG SSO

ダイレクトログインURL ① https://ap.sso.hdems.com/portal/o.d-circle.com/s

ACS URL ① https://xxx.xxx.xx.xxx/pe4j/samlLogin

Entity ID ① https://xxx.xxx.xx.xxx/pe4j/

ログインURL ①

署名方式 ① レスポンス ▼

署名鍵 ① 2048-bits (推奨) ▼

送信



サービスプロバイダー設定

基本設定

名前 ① POWER EGG SSO

ダイレクトログインURL ① https://ap.sso.hdems.com/portal/o.d-circle.com/s

ACS URL ① https://xxx.xxx.xx.xxx/pe4j/samlLogin

Entity ID ① https://xxx.xxx.xx.xxx/pe4j/

ログインURL ①

署名方式 ① レスポンス ▼

署名鍵 ① 2048-bits (推奨) ▼

Name ID ① {user.username}

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)

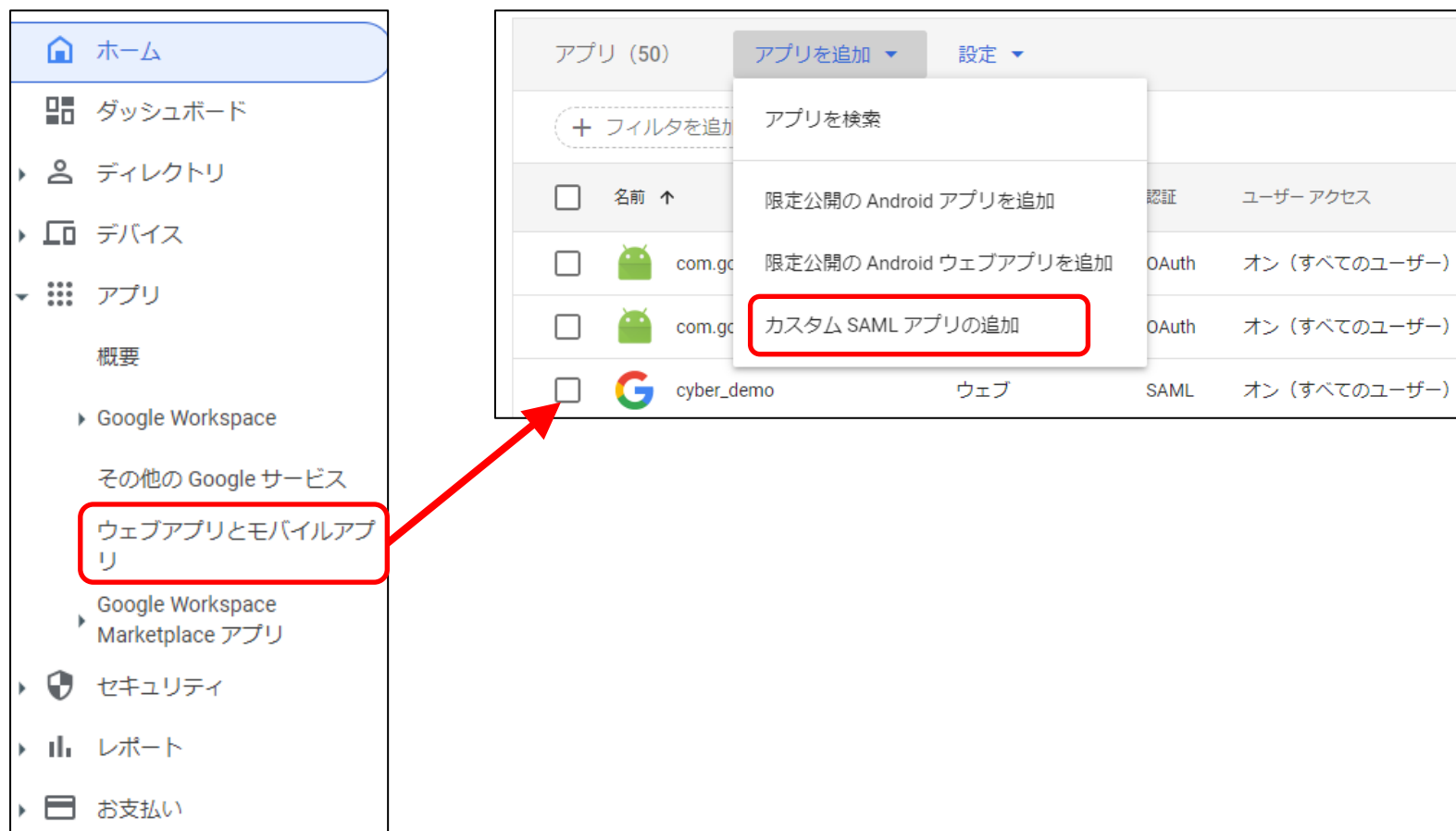
| | | | | | | | |
|---------------|----|--------|---|---|----|--|--|
| POWER EGG SSO | 表示 | ダウンロード | 0 | 0 | 完了 | | |
|---------------|----|--------|---|---|----|--|--|

「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、左ツリーの「アプリ」を展開し、「ウェブアプリとモバイルアプリ」をクリックします。

次に、「アプリの追加」から「カスタムSAMLアプリの追加」をクリックします。



The screenshot shows the GSuite admin console interface. On the left is a navigation sidebar with the 'アプリ' (Apps) menu item selected and highlighted with a red box. A red arrow points from this menu item to the main content area. The main content area shows the 'アプリ (50)' page with a dropdown menu open for 'アプリを追加' (Add App). The dropdown menu lists several options, with 'カスタム SAML アプリの追加' (Add Custom SAML App) highlighted with a red box. Below the dropdown is a table of existing apps.

| 名前 | 認証 | ユーザー アクセス |
|-------------------------|-------|--------------------|
| 限定公開の Android アプリを追加 | | |
| 限定公開の Android ウェブアプリを追加 | OAuth | オン (すべてのユーザー) |
| カスタム SAML アプリの追加 | OAuth | オン (すべてのユーザー) |
| cyber_demo | ウェブ | SAML オン (すべてのユーザー) |

「ユーザーアクセス」をクリックして、「サービスのステータス」を「オン(すべてのユーザー)」に変更して「保存」をクリックします。



SAML

SA SAML for PE

- 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
- アプリの削除

ユーザー アクセス

特定のユーザーが管理対象アプリを利用できるようにするには、グループまたは組織部門を選択してください。 [詳細](#)

[詳細を表示](#)

オフ (すべてのユーザー)

サービスプロバイダの詳細

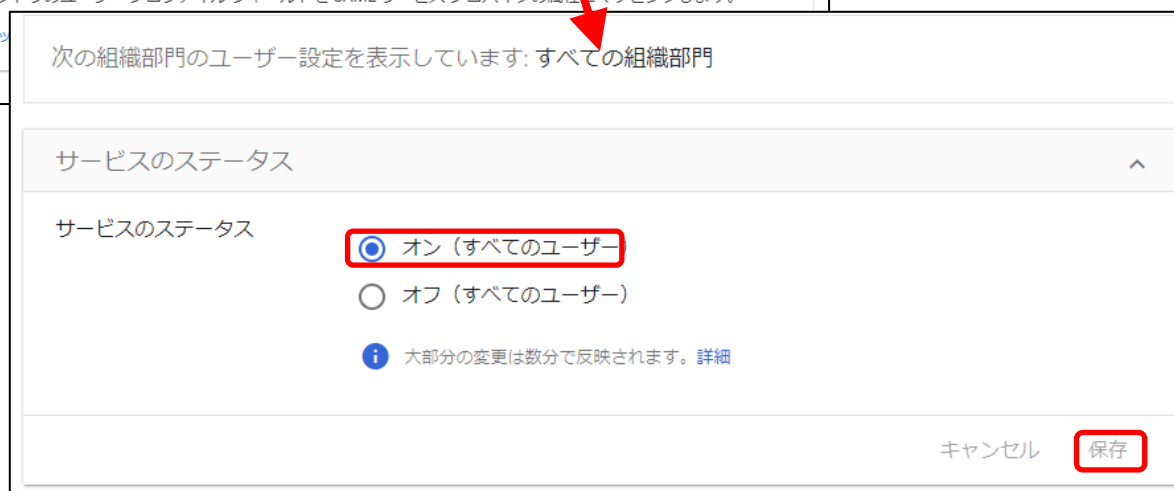
| 証明書 | ACSのURL | エンティティ ID |
|--|--|----------------------------------|
| Google_2024-3-1-163114_SAML2_0 (有効期限: 2024/03/02) | https://pedemo.poweregg.net/pe4j/samlLogin | http://pedemo.poweregg.net/pe4j/ |

SAML 属性のマッピング

SAML 属性のマッピングが設定されていません

Google ディレクトリのユーザー プロファイル フィールドを SAML サービスプロバイダの属性にマッピングします。

[SAML 属性のマ...](#)



次の組織部門のユーザー設定を表示しています: すべての組織部門

サービスのステータス

サービスのステータス

オン (すべてのユーザー)

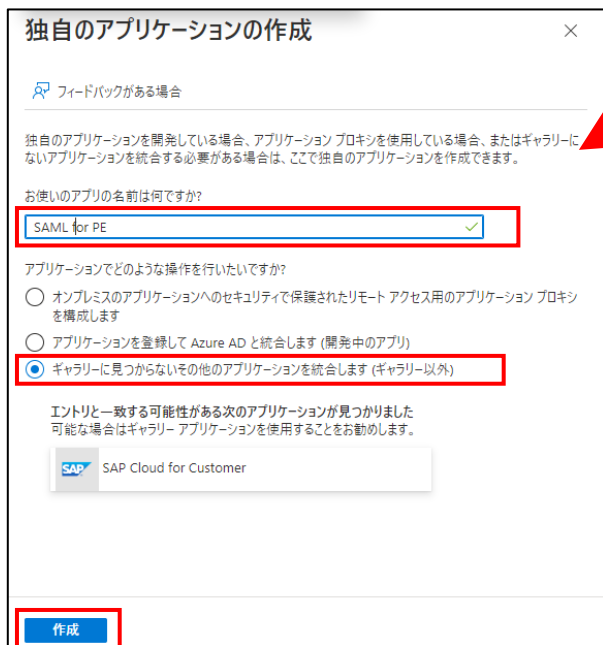
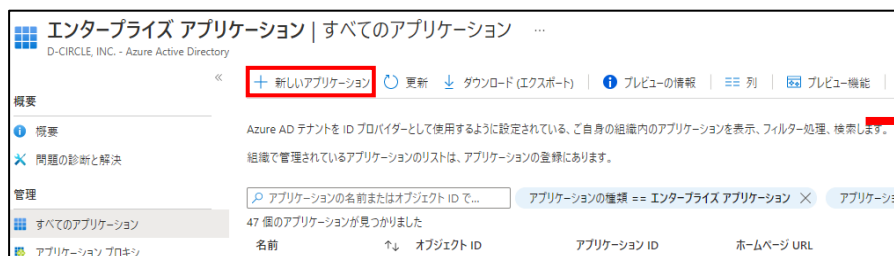
オフ (すべてのユーザー)

[i](#) 大部分の変更は数分で反映されます。 [詳細](#)

キャンセル **保存**

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、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、「独自のアプリケーションの作成」を選択後、任意のアプリケーション名を入力し、「ギャラリーに見つからないその他のアプリケーションを統合します(ギャラリー以外)」を選択して「作成」をクリックします。



IdP(Azure AD)へのPOWER EGGの登録

エンタープライズアプリケーションの一覧から登録したアプリケーションに移動し、「シングルサインオン」を選択後、「SAML」を選択します。次に、基本的なSAML構成の「編集」リンクをクリックします。



SAML for PE | シングル サインオン ...
エンタープライズアプリケーション

概要
デプロイ計画
問題の診断と解決

管理

プロパティ
所有者
ロールと管理者
ユーザーとグループ

シングルサインオン

プロビジョニング
アプリケーション プロキシ
セルフサービス
カスタム セキュリティ属性 (プレビュー)

セキュリティ
条件付きアクセス

シングルサインオン方式の選択 判断に役立つ

無効
シングルサインオンが有効になっていません。
ユーザーは、[マイ アプリ] からアプリを起動できません。

SAML
SAML (Security Assertion Markup Language) プロトコルを使用した、アプリケーションに対する多機能かつセキュリティで保護された認証。

パスワードベース
Web ブラウザーの拡張機能またはモバイルア



SAML for PE | SAML ベースのサインオン ...
エンタープライズアプリケーション

概要
デプロイ計画
問題の診断と解決

管理

プロパティ
所有者
ロールと管理者
ユーザーとグループ

シングルサインオン

プロビジョニング
アプリケーション プロキシ
セルフサービス
カスタム セキュリティ属性 (プレビュー)

セキュリティ
条件付きアクセス

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 このアプリケーションをTest ...

SAML によるシングル サインオンのセットアップ

フェデレーション プロトコルに基づく SSO 実装により、セキュリティ、信頼性、エンド ユーザー エクスペリエンスが向上し、実装が容易になります。OpenID Connect または OAuth が使用されていない既存のアプリケーションの場合は、できるだけ SAML シングル サインオンを選択してください。詳細については、こちらをご覧ください。

以下をお読みください [構成ガイド](#) SAML 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) | 省略可能 |
| ログアウト URL (省略可能) | 省略可能 |

2 属性とクレーム

⚠️ 手順 1 で必須フィールドに入力してください

| | |
|-----------|----------------|
| givenname | user.givenname |
| surname | user.surname |

下記の内容を入力し、「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 | フィードバックがある場合

識別子 (エンティティ ID) * ⓘ

Azure Active Directory に対してアプリケーションを識別する一意の ID。この値は、Azure Active Directory テナント内のすべてのアプリケーションで一意である必要があります。既定の識別子は、IDP で開始された SSO の SAML 応答の対象ユーザーになります。

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

識別子の追加

応答 URL (Assertion Consumer Service URL) * ⓘ

応答 URL は、アプリケーションが認証トークンを受け取る場所です。これは、SAML では "Assertion Consumer Service" (ACS) とも呼ばれます。

| | イン... | 既定 | |
|---|--------------------------|-------------------------------------|--------------------------|
| https://ssltest.poweregg.net/pe4x/sso/samlLogin | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| https://ssltest.poweregg.net/pe4j/samlLogin | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

応答 URL の追加

PC用、スマホ用の設定

| | |
|-------|--|
| 識別子 | https://(サーバー名):(ポート)/pe4j/ |
| | https://(サーバー名):(ポート)/pe4x/ |
| 応答URL | https://(サーバー名):(ポート)/pe4j/samlLogin |
| | https://(サーバー名):(ポート)/pe4x/sso/samlLogin |

3 SAML 証明書

| | | |
|------------------------|---|--------------------|
| トークン署名証明書 | | 編集 |
| 状態 | アクティブ | |
| 拇印 | 6FFC2CCD2AF027F3344BE93925A76D09E6A06776 | |
| 有効期限 | 2026/1/16 15:36:02 | |
| 通知用メール | nakamura@o.d-circle.com | |
| アプリのフェデレーション メタデータ URL | <input type="text" value="https://login.microsoftonline.com/2006d..."/> | |
| 証明書 (Base64) | ダウンロード | |
| 証明書 (未加工) | ダウンロード | |
| フェデレーション メタデータ XML | ダウンロード | |

検証証明書 (省略可能) (プレビュー) [編集](#)

| | |
|--------|-----|
| 必須 | いいえ |
| アクティブ | 0 |
| 有効期限切れ | 0 |

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 > Azure AD ギャラリーの参照 > SAML for PE

SAML 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

[+ ユーザーまたはグループの追加](#) [割り当ての編集](#) [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マイアプリ内に表示されます。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。

ここで、アプリケーションのアプリのロールにユーザーとグループを割り当てます。このアプリケーションの新しいアプリのロールを作成するには、[アプリケーション登録](#)を使用します。

| 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 | | |

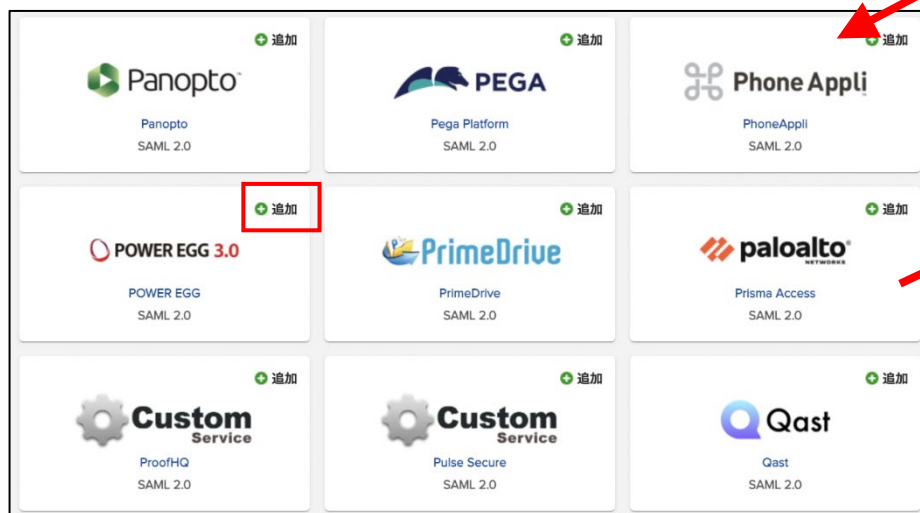
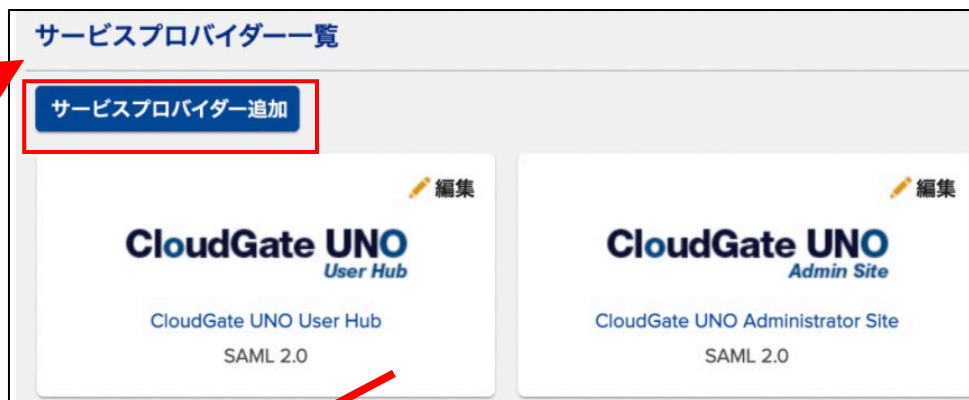
ユーザとグループから、シングルサインオンを許可するユーザを追加します。

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 |
| CloudGate UNO User Hub | CloudGate UNO 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="radio"/> いいえ |
| SP-initiated SSO | <input checked="" type="radio"/> 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 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IdP情報

| | |
|------------------------|---|
| プロバイダー名 | <code>https://echizen.cloudgate.jp/sso/d-circle/</code> 📄 コピー |
| ログインURL | <code>https://echizen.cloudgate.jp/sso/d-circle/login.xhtml</code> 📄 コピー |
| ログアウトURL | <code>https://echizen.cloudgate.jp/sso/d-circle/logout.xhtml</code> 📄 コピー |
| 証明書 | 📄 ダウンロード |
| 証明書のフィンガープリント (SHA1) | <code>AD 3F D6 01 9A 91 C1 DC 59 29 82 9B 5F 1F 62 4F 1D 88 8F 74</code> 📄 コピー |
| 証明書のフィンガープリント (SHA256) | <code>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</code> 📄 コピー |
| 証明書のフィンガープリント (MD5) | <code>C8 8C C6 E6 D6 C0 ED E9 CF EA 1D 47 41 97 1E D3</code> 📄 コピー |
| SAML 2.0 メタデータ | 📄 ダウンロード |

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。

- 下記機能は、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。）
 - ・PCリマインダー
 - ・リマインダー for iPhone
 - ・リマインダー for Android
 - ・組織図エディタ
- 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いるIdPは、HENNGE One、IIJ ID、Azure AD、Gsuite、CloudGate UNO サービスです。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います。
- 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。