ゲートウェイサービスからAWSマネジメントコンソールへシングルサインオンするための情報

目次

1. 概要
2. グループ管理者による初期設定
    a. AWSマネジメントコンソールの設定
    b. グループの設定
3. 利用フロー - ゲートウェイサービスからAWSマネジメントコンソールへシングルサインオン
4. その他

概要

学認クラウドゲートウェイサービス（以下、ゲートウェイサービス）に登録されているAWSマネジメントコンソールSPコネクタに任意のグループを接続することで、ゲートウェイサービス経由でAWSマネジメントコンソールにサインインするための手順を示します。

本ページでは以下の前提および要領で記載しています。

- AWSマネジメントコンソールはすでに利用可能な状態でご契約されていること。
- 本ページで「グループ」と記載しているものは、ゲートウェイサービスグループ機能で提供されるグループを指しています。AWSマネジメントコンソール上で作成したグループとは異なります。

> ⚠ 本機能は現在**ベータ版**として提供しております。
>
> 本機能が利用できるのはゲートウェイサービスに利用申請いただいた機関のみです。
>
> ゲートウェイサービスを介してその先のSPへログインするという性質上、各機関IdP所管部署の了解を得られた場合のみ提供しております。所属機関から了解を得られているか不明であるもしくはIdP所管部署の方で了解を与えたいという場合はお手数ですがゲートウェイサービスお問い合わせ先までご連絡ください。

> ⛔ AWSマネジメントコンソールのロール設定において、権限ポリシーの選択やeduPersonEntitlementで指定する利用グループが適切に設定されない場合、意図しない権限がメンバーに付与される・意図しない者にAWSマネジメントコンソールが利用されるなどの事故が発生しうる可能性がございます。十分にご注意いただいたうえで設定を行ってください。なお、設定の不備等による一切の責任は負いかねますので、あらかじめご了承ください。

グループ管理者による初期設定

AWSマネジメントコンソールの設定

AWSマネジメントコンソールでゲートウェイサービスとの連携およびログインしたユーザの付与する権限の設定を行います。

1. ご契約済みのAWSマネジメントコンソールにサインインし、IAMコンソール（https://console.aws.amazon.com/iam/）を開きます。
2. ナビゲーションペインの「ID プロバイダー」を開き、「プロバイダの作成」ボタンを選択します。

    a. 手順１：プロバイダの設定

「プロバイダーのタイプ」、「プロバイダ名」を入力、「メタデータドキュメント」にメタデータをアップロードします。設定後に「次のステップ」ボタンをクリックします。

プロバイダータイプは「SAML」を選択してください。

ほかにOpenID Connectが選択できますが、本ページでは取り扱いません。

プロバイダー名は任意の値を設定してください。本ページでは例として「cgtestprovider」をプロバイダー名に設定します。

メタデータドキュメントは「学認クラウドゲートウェイサービス連携のための情報」の「SP管理者に必要な情報」 からダウンロードできる学認クラウドゲートウェイサービス (IdP)のメタデータを指定します。

あらかじめダウンロードしておき、ファイルの選択からアップロードしてください。

ここで入力したプロバイダ名は次の手順（ロールの設定とグループ管理者の設定）で利用します。

b. 手順２：検証
設定した情報に問題がなければ、「作成」ボタンをクリックします。

3. ナビゲーションペインの「ロール」を開き、「ロールの作成」ボタンを選択します。

a. 「信頼されたエンティティの種類を選択」、「SAML プロバイダー」を設定します。設定後に「次のステップ: アクセス権限」ボタンをクリックします。

「信頼されたエンティティの種類を選択」では「SAML 2.0 フェデレーション」を選択します。

「SAML プロバイダー」はプロバイダの設定で作成したプロバイダー名をプルダウンメニューから選択します。本ページでは例としてすでに設定済みのプロバイダ「cgtestprovider」を選択しています。

直下のラジオボタンでは「プログラムによるアクセスとAWSマネジメントコンソールによるアクセスを許可する」を選択します。

本ページではAWSマネジメントコンソールにサインインさせることを目的としていますので、「プログラムによるアクセスのみを許可する」については取り扱いません。

「属性」は「SAML:aud」および「値」は「https://signin.aws.amazon.com/saml」があらかじめ設定され、グレーアウトされています。

このページでの「条件」では細やかな設定ができませんので、後述する手順で設定します。

b. 「Attach アクセス権限ポリシー」を設定します。選択後に「次のステップ: タグ」ボタンをクリックします。

AWSマネジメントコンソールにサインインしたときにどのような権限を持たせるかを設定します。

このページでは例として「AmazonS3FullAccess」を選択します。

権限ポリシーの選択が適切に設定されない場合、意図しない権限がメンバーに付与されるなどの事故が発生しうる可能性がございます。十分にご注意いただいたうえで設定を行ってください。なお、設定の不備等による一切の責任は負いかねますので、あらかじめご了承ください。

c. 「タグの追加（オプション）」を設定します。設定後、「次のステップ: 確認」ボタンをクリックしてください。

必要に応じて設定してください。

このページの例では特に必要でありませんので、入力しません。

d. 「ロール名」を入力します。入力後、「ロールの作成」ボタンをクリックします。

「ロール名」に任意の値を設定してください。このページでは例として「ロール名」に「cgtestrole」を設定しています。

所属する複数グループで本機能を使っている場合にロール名で区別する必要がありますので、グループ名とシングルサインオンで使用されるものであることを明記した"CGDevelopmentTeamSSO"のようなロール名にすることを推奨します。

> ⚠ ここで入力したロール名は次の手順（グループ管理者の設定）で利用します。

4. 作成したロールの条件を修正を行います。
   a. ナビゲーションペインから「ロール」を開き、作成したロール（このページの例では cgtestrole ）を開きます。
   b. 「信頼関係」タブから「信頼関係の編集」をクリックすると編集画面に入ります。

   c. 信頼関係の編集画面で接続を許可する利用グループの指定を追加し、「信頼ポリシーの更新」ボタンをクリックします。

      このページの例では利用するグループ（グループID）は「cgtestgroup」とします。後述する「グループの設定」もご参照ください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::アカウントID:saml-provider/cgtestprovider"
      },
      "Action": "sts:AssumeRoleWithSAML",
      "Condition": {
        "StringEquals": {
          "SAML:aud": "https://signin.aws.amazon.com/saml"
        },
        "ForAnyValue:StringEquals": {
          "SAML:eduPersonEntitlement": "https://cg.gakunin.jp/gr/cgtestgroup"
        }
        ↑ 赤字で示した条件を追加してください。後述する「グループの設定」で接続するグループを追加します。
      }
    }
  ]
}
```

> ℹ ゲートウェイサービスからAWSマネジメントコンソールにはグループ情報（isMemberOf）をeduPersonEntitlementの属性値として送信します。このほかに利用する属性があればAWSマニュアル（ IAM および AWS STS の条件コンテキストキー ）を参照してください。
>
> グループ情報（isMemberOf）の形式は「https://cg.gakunin.jp/gr/GROUPID」となります。「AWS Management Console」SPコネクタに接続するグループ情報を設定してください。ここではグループID cgtestgroup として作成された「https://cg.gakunin.jp/gr/cgtestgroup」を指定しています。
>
> また、どのグループ情報に一致すればよいかという条件は ForAnyValue:StringEquals を用いていますが、他の条件を記述する必要があればAWSマニュアル（ 複数のキー値をテストする条件を作成する（オペレーションの設定） ）を参照してください。

eduPersonEntitlementで指定する利用グループが適切に設定されない場合、意図しない者にAWSマネジメントコンソールが利用されるなどの事故が発生しうる可能性がございます。十分にご注意いただいたうえで設定を行ってください。なお、設定の不備等による一切の責任は負いかねますので、あらかじめご了承ください。

以下の通りになっていれば問題ありません。

d. 「条件」が次の通りになっていれば問題ありません。

表示されている「ロール ARN」と「信頼されたエンティティ」をメモします。

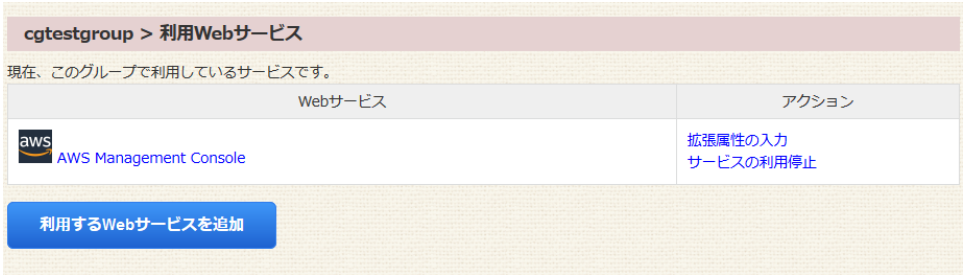
例では「ロール ARN」は「arn:aws:iam::***アカウントID***:role/cgtestrole」、「信頼されたエンティティ」は「arn:aws:iam::***アカウントID***:saml-provider/cgtestprovider」となっています。

グループの設定

1. グループをAWSマネジメントコンソールSPコネクタに接続します
   新規に作成するグループか、もしくは既存のグループの「利用Webサービス」から「AWS Management Console」を利用Webサービスとして追加します。
   グループの新規作成は「グループを作成する」、利用Webサービスの追加は「サービスを利用する」の手順をそれぞれ参照してください。
   このページの例では、グループIDは 「cgtestgroup」とします。

既存グループでグループIDが不明な場合は「グループを修正する」で確認してください。

2. グループ固有の値を設定
グループをAWSマネジメントコンソールSPコネクタに接続すると、当該グループの利用Webサービスに「AWS Management Console」が表示されます。アクションから「拡張属性の入力」を開きます。



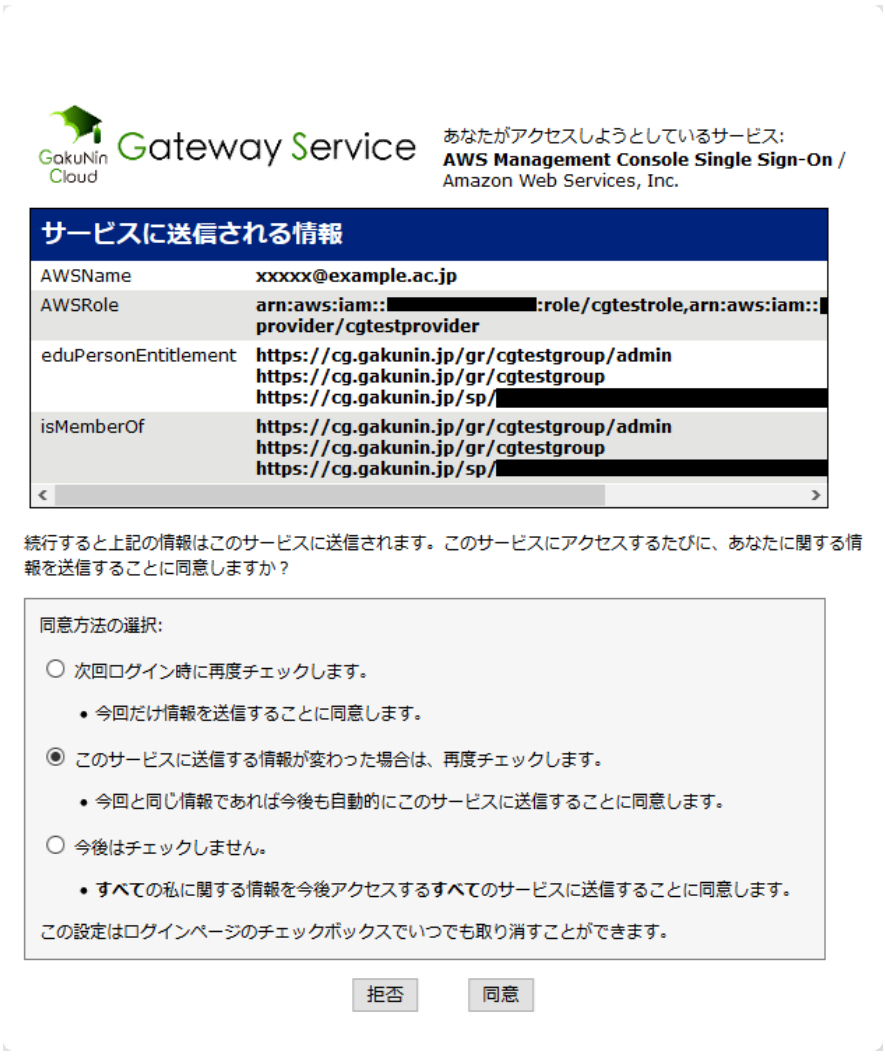
3. 属性の値を入力します。
属性名「AWSRole」の値に「AWSマネジメントコンソールの設定」の手順で設定した「ロール ARN」と「信頼されたエンティティ」をカンマ区切り（例 arn:aws:iam::***アカウントID***:role/***ロール名***,arn:aws:iam::***アカウントID***:saml-provider/***プロバイダ名***）」で入力し、保存ボタンを押します。

利用フロー - ゲートウェイサービスからAWSマネジメントコンソールへシングルサインオン

1. ゲートウェイトップ画面から「AWS Management Console」の「グループ表示」を開き、表示されるグループをクリックしてください。

2. グループを選択後にAWSマネジメントコンソールにサインインが行われます。
多くの場合はすでにゲートウェイサービスにログインしているためシングルサインオン（SSO）によりAWSマネジメントコンソールにサインインされますが、もしタイムアウト等でSSOしない場合は所属機関IdPで認証してください。
以下のように「サービスに送信される情報」を選択する画面が表示される場合があります。これはゲートウェイサービス側の画面で、ユーザが当該サービスに属性を送信することに同意するための画面です。送信する属性について問題なければ「同意」ボタンをクリックします。なお、送信される属性は以下の通りです。

- **AWSRoleSessionName**: ゲートウェイサービスが付与する永続的な仮名識別子（いわゆるeduPersonTargetedID）
- **AWSRole**: グループ管理者が入力したAWSアカウントID・ロール名・IDプロバイダ名
- **eduPersonEntitlement**: 所属するグループ情報



⚠ ソフトウェアの不具合により上記の「サービスに送信される情報」を選択する画面が表示された後にAWSにサインインできない場合があります。「次回ログイン時に再度チェックします。」**以外** を選択してご利用ください。
「同意」ボタンをクリックした直後にエラーとなった場合はお手数をおかけして申し訳ございませんが、もう一度1.の手順からやり直してください。

利用可能なグループが複数ある場合には、AWSサインイン前に以下のようなロールの選択画面が表示され、利用したいロールを選択する必要があります。どのロールを選択すべきか不明な場合はグループ管理者へお問い合わせください。

問い合わせを受けたグループ管理者の方は、利用者が選択すべきAWSアカウントIDとロールの組み合わせを利用者へ連絡してください。

AWSマネジメントコンソールにサインインしたあと以下のような画面となります。
サインインしたユーザ名はフェデレーションログインとして認識され「ロール名/ランダムな文字列」の形式で表示されます。

その他

- グループに複数の異なる機関のメンバーがいる場合はそれぞれの機関が以下2つの条件を満たしている必要があります。そうでない機関のメンバーについては「利用フロー - ゲートウェイサービスからAWSマネジメントコンソールへシングルサインオン」で説明しているシングルサインオン（SSO）はできません。
    1. メンバーの所属機関がゲートウェイサービスに参加していること（「学認クラウドゲートウェイサービス」をご参照ください）
    2. IdP管理者によりAWSコンソールが利用できるようになっていること（「グループの設定」をご参照ください）
- AWSマネジメントコンソールへのSSOは、本ページで紹介しているように「ゲートウェイサービスから送信される属性を元にAWSのロールに紐づけてログインした状態にする」方法で行われます。これはサービスがSSOのために提供している機能に依存する部分で、他のクラウドサービスでは「IdPから送信されたメールアドレス等の属性を元にSPのローカルアカウントに紐づけてログインした状態にする」形でのSSOが一般的かと思われます。AWSマネジメントコンソールの場合には特定のローカルアカウント（IAMユーザ等）に紐づける形ではない点にご注意ください。個々のユーザにローカルアカウントを作成しておくという煩雑さがない一方、サービス上では個々人を区別する手段は、自動的に割り当てられるユーザー名以外にはありません。
- グループとAWSマネジメントコンソールの設定に関する設定例の一つとして『学認クラウドゲートウェイサービス(2)「活用事例 ー AWSコンソールSSOの実際 ー 」』（学術情報基盤オープンフォーラム2020資料）を公開しておりますのでご参照ください。
- インシデント発生時の調査にAWSマネジメントコンソール上のユーザー名から利用者の紐づけ情報が必要な場合には、学認クラウドゲートウェイサービスサポートが窓口として対応いたします。利用申請時の責任者より学認クラウドゲートウェイサービスサポートにお問い合わせください。