学認クラウドゲートウェイサービス(2)

活用事例
– AWSコンソールSSOの実際 –

2020年6月9日

国立情報学研究所
クラウド基盤研究開発センター／クラウド支援室

小林 久美子

概要

1. はじめに

2. 利用の前提条件

3. AWSマネジメントコンソールへのSSOの実装
   (1) 手順
   (2) 実装
   (3) 注意事項

4. まとめ

1. はじめに

- AWS連携機能：AWSマネジメントコンソールへのSSO
  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コネクタに利用グループを接続

  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学認のIDでログインできるようになる

  設定手順詳細： https://meatwiki.nii.ac.jp/confluence/x/9Yp6Ag

※設定手順詳細で「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る。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る。

2. 利用の前提条件

(1) AWSマネジメントコンソールはすでに利用可能な状態で契約されていること。

(2) 現在「ベータ版」のため、利用できるのはゲートウェイサービス参加機関のみ。

(3) 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される。

※以下の場合はゲートウェイサービスお問い合わせ先に連絡
- 所属機関から了解を得られているか不明。
- IdP所管部署の方が了解を与えたい。

3. AWSマネジメントコンソールへのSSOの実装(1)

■ 手順

「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」をもとに、AWSアカウント管理者(A)とグループ管理者(G)が以下を行うことで、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SSOできるようになる。

(1) AWSマネジメントコンソールの設定(A)
ゲートウェイサービスと連携するための設定。
ログインしたユーザに付与する権限の設定。

(2) グループの作成とメンバーの招待（すでにある場合は省略）(G)
AWSマネジメントコンソールSPコネクタを接続するグループ。

(3) 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(G)
グループの利用Webサービスに「AWS Management Console」を追加。

4. AWSマネジメントコンソールへのSSOの実装(2)

- 実装[1]
  AWSアカウントのユーザに設定されているポリシー

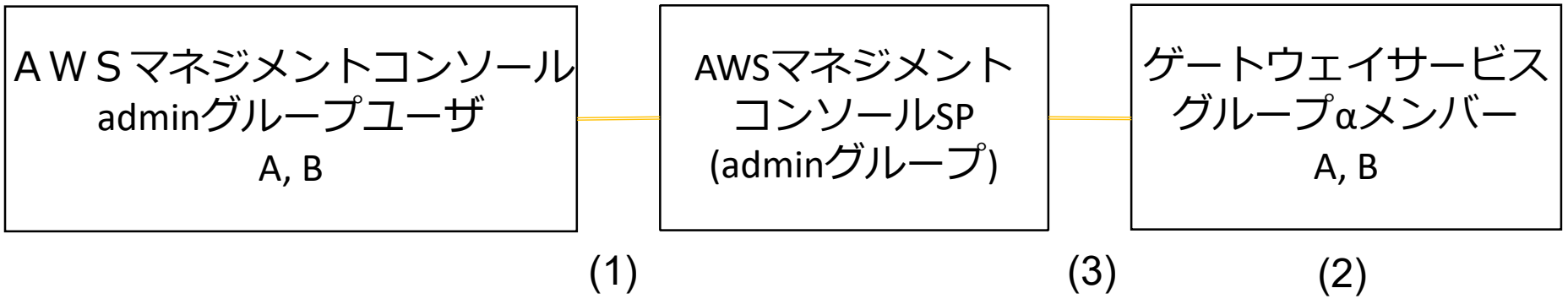
  ・adminグループのユーザ(A, B)
  AdministratorAccess, IAMUserChangePassword

  ・userグループのユーザ(C, D, E)
  IAMFullAccess, PowerUserAccess, IAMUserChangePassword

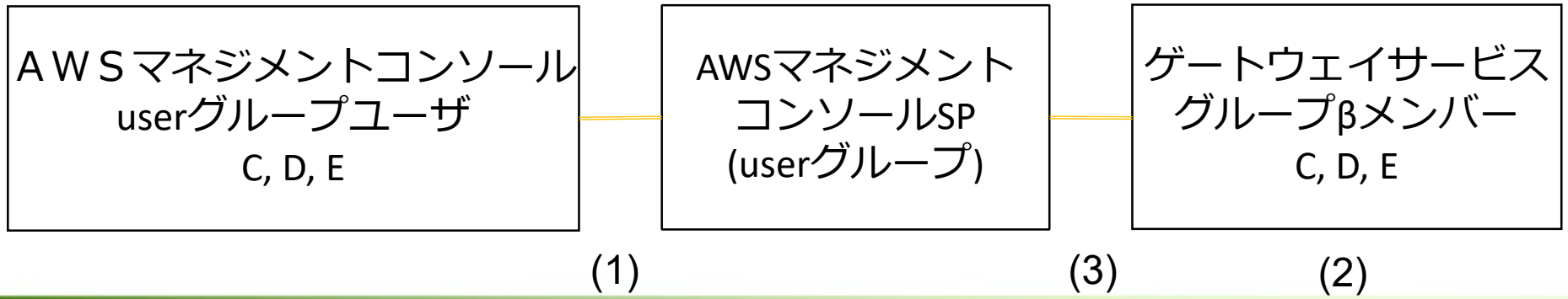
今回、AWSアカウント管理者とグループ管理者は同一。

4. AWSマネジメントコンソールへのSSOの実装(3)

■ 実装[2]
新しいグループαを作成し、adminグループのユーザがSSOできるようにした。



userグループのユーザもSSOできるようにするには、別のグループを作成する。



3. AWSマネジメントコンソールへのSSOの実装(4)

■注意事項

権限ポリシーの選択や利用グループが適切に設定されない場合、以下のような事故が発生しうる可能性がある。十分に注意した上で設定を行うこと。

・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

NGの例：
・AWSのuserグループユーザ用の(1)の設定で、adminユーザのポリシーを設定する。
・ユーザCをグループαのメンバーに招待する。

※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。

4. まとめ

(1)ゲートウェイサービスのAWS連携機能を利用して、AWSマネジメントコンソールへのSSOを実装した。

(2)本機能を利用するとゲートウェイサービスを介してAWSマネジメントコンソールへアクセスできるので、非常に便利である。

(3)権限ポリシーの選択や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たり、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あるため、十分に注意した上で設定を行う必要がある。

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

https://cloud.gakunin.jp/

学認クラウド　検索