ゲートウェイサービスからAWSマネジメントコンソールヘシン 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。

介 本機能は現在ペ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ヘ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。_____

aws y -	・ビス 🗸 リソースグループ 🗸		グローバル × サポート ×
IAM の検索	プロバイダの作成 プロバイダの削除		C • 0
ダッシュボード	検索		結果件数: 0
グループ ユーザー	□ プロバイダ名 \$	タイプ 🗢	作成時刻 🗢
ロール	レコードが見つかりません。		
ポリシー			
ID プロバイダー			
アカウント設定			
認証情報レポート			
🔍 フィードバック 🤇	日本語 © 2008 - 2019, Ama;	zon Web Services, Inc. またはその腿連	会社。無断転用禁止。 プライバシーポリシー 利用規約

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。

<u> </u>	<u> </u>		
プロ	コバイダの作成	プロバイダの詞	设定
手順	1:プロバイダの設定	ー プロバイダーのタイプを選択	てします。
手順	2:検証	プロバイダーのタイプ*	SAML -
		プロバイダ名*	cgtestprovider 最大 128 文字まで、英歌字と「」を使用します。
		メタデータドキュメント・	C:\fakepath\cgidp-metadata.xml ファイルの選択
		* 必須	キャンセル 次のステップ
0	プロバイダー	タイプは「SAML」を	を選択してください。
	ほかにOpenl	D Connectが選択で	きますが、本ページでは取り扱いません。
0	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
0	メタデータド ンロードでき	キュメントは「 <mark>学認</mark> る学認クラウドゲー	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」 からタ 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。
▲ b. 手順2	ここで入力し :検証 た情報に問題か	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 設定し	ここで入力し :検証 た情報に問題か 3WS サービス	たプロバイダ名は次 、 なければ、「作成」 、 リソースグループ 、	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。 ボタンをクリックします。 2ローバレマ サポートマ
♪ b. 手順2 設定し プロ	ここで入力し :検証 た情報に問題か WS サービス JJ(イダの作成	たプロバイダ名は次 [*] なければ、「作成」 <u>* リソースグループ *</u> プロバイダ <i>ー</i> 1	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。 ボタンをクリックします。 ^{クローバル × サポート ×} 青報の検証
b. 手順2 設定し: プロ 手順	ここで入力し :検証 た情報に問題か コバイダの作成 11:プロバイダの段	たプロバイダ名は次 * リソースグループ * プロバイダード 以下のプロバイダー情報を移	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。 ボタンをクリックします。 グローバレ × サポート × 青報の検証 ^{縦します。[Create]をクリックして終了します。}
b. 手順2 設定し: プロ 手順 手順	ここで入力し :検証 た情報に問題か WS サービス ロバイダの作成 11:プロバイダの殺 2:検証	たプロバイダ名は次 なければ、「作成」 、 リソースグループ 、 プロバイダー作 以下のプロバイダー (明金を) プロバイダス cgtes タイプ SAM	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。 ボタンをクリックします。 <u>グローバレ マ サポートマ</u> 青報の検証 Ex回します。[Create]をクリックして終了します。 stprovider
b. 手順2 設定し で プロ 手順 手順	ここで入力し :検証 た情報に問題か コバイダの作成 11:プロバイダの殺 12:検証	たプロバイダ名は次 [*] なければ、「作成」 <u>プロバイダー</u> [*] [*] [*] [*] [*] [*] [*] [*] [*] [*]	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。 ボタンをクリックします。 クローバレ サポート × 青報の検証 ^転 します。[Create]をクリックして終了します。 stprowider L
b. 手順2 設定し. プロ 手順 手順	ここで入力し :検証 た情報に問題カ 3W5 サービス コバイダの作成 11: プロバイダの段 2: 検証	たプロバイダ名は次 [*] なければ、「作成」 * リソースグループ * プロバイダー [†] 以下のプロバイダー タイプ SAM	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。 ボタンをクリックします。 <u>クローバレ サポート ×</u> 青報の検証 離しまず。[Create]をクリックして終了します。 aprovider L
b. 手順2 設定し プロ 手順 た 手順 イロ デー ション るWS	ここで入力し :検証 た情報に問題か コバイダの作成 1: プロバイダの路 2: 検証 ペインの「ロー サービス、 リソー	たプロバイダ名は次 [*] リソースグループ * プロバイダー「 以下のプロバイダー情報を移 プロバイダ名 cgtes タイプ SAMI	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。 ボタンをクリックします。 <u>クローバレ マ サポート マ</u> 青報の検証 離しまず。[Create]をクリックして終了します。 まprovider し <i>キャンセル </i>
b. 手順2 設定し プロ 手順 子順 イロ デーション awys	ここで入力し :検証 た情報に問題か WS サービス ロバイダの作成 1:ブロバイダの数 2:検証 ペインの「ロー サービス 、 リソー	たプロバイダ名は次 なければ、「作成」 、 リソースグループ 、 プロバイダード 以下のプロバイダー情報を移 プロバイダ cgles タイプ SAM	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。 ボタンをクリックします。 <u>クロールレ サポート・</u> 青報の検証 壁します、[Create]をクリックして終了します。 tprovider L ・ ・ いの作成」ボタンを選択します。 <u>グローバル サポート (RS) 作成</u>
 た. 手順2 設定し プロ デル デーション avvs の検索 (シュポード) 	ここで入力し : 検証 た情報に問題カ 3W5 サービス コノイイダの作成 11: プロバイダの没 2: 検証 ペインの「ロー サービス マリソー	たプロバイダ名は次 [*] リソースグループ * プロバイダー「 以下のプロバイダー「 以下のプロバイダー」 タイプ SAM	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。 ボタンをクリックします。 <u>クローバレ サポート・</u> 青報の検証 壁します。[Create]をクリックして終了します。 stprovider L ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
b. 手順2 設定し プロ 環 た 系 の検索 シュホード ーブ	ここで入力し : 検証 た情報に問題か 3005 サービス 301(イダの作成 11: プロノイダの換 12: 検証 ペインの「ロー サービス マ リソー (ロールの作成 ロールの	たプロバイダ名は次 [*] なければ、「作成」 * リソースグループ * プロバイダード 以下のプロバイダー情報を移 プロバイダー、 なければ、「作成」 * プロバイダー、 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	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。 ボタンをクリックします。 <u>クローバレ オポート イ</u> 青報の検証 経ビします、[Create]をクリックして終了します。 stprovider L ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
 た. 手順2 た. 手順2 す. 設定し ブロ デーション マーン <l< td=""><td>ここで入力し ::検証 た情報に問題カ 3W5 サービス コバイダの作成 11:プロバイダの段 2:検証 ペインの「ロー サービス、 リソー (ロールの作成 (ロールの作成</td><td>たプロバイダ名は次 [*] リソースグループ * プロバイダー「 以下のプロバイダー「 以下のプロバイダー「 は下のプロバイダー」 タイプ SAM</td><td>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。 ボタンをクリックします。 <u>プローパル サポート ~</u> 青報の検証 軽しまず、[Create]をクリックして終了します。 stprovider L ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・</td></l<>	ここで入力し ::検証 た情報に問題カ 3W5 サービス コバイダの作成 11:プロバイダの段 2:検証 ペインの「ロー サービス、 リソー (ロールの作成 (ロールの作成	たプロバイダ名は次 [*] リソースグループ * プロバイダー「 以下のプロバイダー「 以下のプロバイダー「 は下のプロバイダー」 タイプ SAM	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。 ボタンをクリックします。 <u>プローパル サポート ~</u> 青報の検証 軽しまず、[Create]をクリックして終了します。 stprovider L ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
 た. 手順2 た. 手順2 プロ デーション デーション の検索 パーブ・ボート パーブ・ボーー パーブ・ボーー パージュホード 	ここで入力し : 検証 た情報に問題か 3WS サービス コノ(イダの作成 11: プロノ(イダの) 2: 検証 ペインの「ロー サービス マリソー (ロールの作成 ロール4 の 秋気を ロール4	た プロバイ ダ名は次 ^く リソースグループ 、 プロバイダー「 以下のプロバイダー」 プロバイダー」 マロバイダー」 マロバイダー」 マロバイダー」 マロバイダー」 マロバイダー」 の マロバイダー」 マロバイター マロバ マロー マロバ マロー マロン マロ マロバ マロ マロ マロ マロ マロ マロ マロ マロ マロ マロ	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。 ボタンをクリックします。 <u>プローバル サポート イ</u> 青報の検証
 た. 手順2 設定し プロ デル ジュボード パワ パワ	ここで入力し : 検証 た情報に問題か 3WS サービス コバイダの作成 1: ブロバイダの換 1: ブロバイダの設 1: ブロバイダの設 1: ブロバイダの設 1: ブロバイダの設 1: ブロバイダの設 1: ブロバイダの設 1: ブロバイダの設 1: ブロバイダの作成 コールの作成 ヘWSSee ヘWSSee ヘWSSee ヘWSSee	た プロバイ ダ名は次 ^S なければ、「作成」 <u>マリソースグループ 、</u> <u>プロバイダー情報を</u> <u>プロバイダー情報を</u> <u>プロバイダー情報を</u> <u>プロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイダー</u> <u>マロバイ</u> <u>マロバイ</u> <u>マロバ</u> <u>マロバイ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロバ</u> <u>マロ</u> <u>マロバ</u> <u>マロバ</u> <u>マロ</u> <u>マロバ</u> <u>マロ</u> <u>マロ</u> <u>マロ</u> <u>マロ</u> <u>マロ</u> <u>マロ</u> <u>マロ</u> <u>マロ</u> <u>マロ</u> <u>マロ</u> <u>マロ</u> <u>マロ</u> <u>マロ</u> <u>マ</u> <u>マ</u> <u>マ</u> <u>マ</u> <u>マ</u> <u>マ</u> <u>マ</u> <u>マ</u>	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。 ボタンをクリックします。 <u>クローバル ~ サボート ~</u> 青報のの検証 経ビはず,[Create]をクリックして終了します。 まprovider L <i>キャンセル</i> 戻る 作成 ・ <i>パ</i> の作成」ボタンを選択します。 <u>クローバル ~ サポート ~</u> <u>2 @ @</u> <u>35 ffの結果を表示</u> <u>G編されたエンティティ</u> 名 ffの結果を表示
 た ・手順2 ・ ・<!--</td--><td>ここで入力し : 検証 た情報に問題か 3WS サービス コバイダの作成 1: プロバイダの作成 1: プロバイダの酸 2: 検証 ペインの「ロー サービス マ リソー 「ロールの作成 」 「の作成 「ロールの作成 「ロールの作成 」 「の作成 「ロービス マ リソー</td><td>た プロバイ ダ名は次 なければ、「作成」 、 リソースグループ 、 プロバイダード 以下のプロバイダー のイガ SAMI シール」を開き、「ロー スグループ 、 こールの削除 ないてに、 Default Service-Linku viceR Default Service-Linku viceR Allows Amazon RDS</td><td>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。 ボタンをクリックします。 クローバル ケ サボート イ 青報のの検証 経ビはず, [Create]をクリックして城了します。 まprovider L</td>	ここで入力し : 検証 た情報に問題か 3WS サービス コバイダの作成 1: プロバイダの作成 1: プロバイダの酸 2: 検証 ペインの「ロー サービス マ リソー 「ロールの作成 」 「の作成 「ロールの作成 「ロールの作成 」 「の作成 「ロービス マ リソー	た プロバイ ダ名は次 なければ、「作成」 、 リソースグループ 、 プロバイダード 以下のプロバイダー のイガ SAMI シール」を開き、「ロー スグループ 、 こールの削除 ないてに、 Default Service-Linku viceR Default Service-Linku viceR Allows Amazon RDS	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。 ボタンをクリックします。 クローバル ケ サボート イ 青報のの検証 経ビはず, [Create]をクリックして城了します。 まprovider L

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。

aw	VS サービス ∨ リソースグループ ∨			グローバル 👻 サポート 👻	
	信頼されたエンティティの種類	を選択			^
	AWS サービス 別 EC2, Lambda、およびその 他 計	の AWS アカウント 客様またはサードパー ィーに属しています	ウェブ ID Cognito または任意の OpenID プロバイダ	SAML 2.0 フェデレー ション 企業ディレクトリ	
	SAML 2.0 を使用してフェデレーションされたユー はこちら	ザーがこのロールを引き	き受けてお客様のアカウントでアクショ	ンを実行することを許可します。詳細	
	SAML 2.0 プロバイダを選択				
	 API アクセス用のロールを作成している場合は、[/ ザーのアクセスを制限します。	Attribute] を選択してから	そのロールに含める値を入力します。	これにより、指定された属性をもつユー	
	SAML プロバイダー	cgtestprovider プログラムによる ・ プログラムによる	▼ 新しいプロパイダの作成 G 5アクセスのみを許可する 5アクセスと AWS マネジメントコンソ・	・ 更新 ールによるアクセスを許可する	
	属性	SAML:aud	•		
	値*	https://signin.aws.am	azon.com/saml		
	条件	♀ 条件の追加 (オプ	ション)		
	* 必須		キャンセル	次のステップ: アクセス権限	
Q 71	ードバック 🔇 日本語	© 2008 - 2019, Amaz	on Web Services, Inc. またはその関連会社。	黒斯転用禁止。 プライバシーポリシー 利用規約	
0	「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。	
(i)	「SAML プロバイダー」はプロ 例としてすでに設定済みのプロ	バイダの設定 バイダ「cgte	で作成したプロバイダ- stprovider」を選択して	-名をプルダウンメニューから ています。	ら選択します。本ページでは
	直下のラジオボタンでは「プロ ます。	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
	本ページではAWSマネジメント のみを許可する」については取	・コンソールに り扱いません。	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
0	「属性」は「SAML:aud」およ されています。	び「値」は「H	nttps://signin.aws.ama	zon.com/saml」があらかじ&	の設定され、グレーアウト
⚠	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	する手順で設定します。	
[Attac	h アクセス権限ポリシー」を設	まします。 選択	₹後に「次のステップ:	タグ」ボタンをクリックしま	ŧ,
av	NS サービス v リソースグループ	·		グローバル マ サポート マ	
	ロールの作成			1 2 3 4	^
	 ◆ Attach アクセス権限ポリシー 				
	新しいロールにアタッチするポリシーを 1 つ以	上選択します。			
	ポリシーの作成			C	
	ポリシーのフィルタ v Q 検索			514 件の結果を表示中	
	ポリシー名 🗸	z	欠として使用	説明	
		C33 /2	жU		
	AmazonS3FullAccess	1.		Provides read only access to all buckets via	
	AmazonSageMakerFullAccess	te te	al.	Provides full access to Amazon Sage	
	-	1,	<i>\$</i> [,	Provides read only access to Amazon	
* v2	缅		キャンセル	戻る 次のステップ: タグ	
*± ₹ 71	・ ・ ・ ・		なし なし なし キャンセル eb Services, Inc. またはその間違会社、無限	Provides read only access to all buck Provides full access to Amazon Sage Provides read only access to Amazon 反 の ステップ:タグ 範囲線止。 プライパシーボリシー 利用規約	

		IISSTUIACCESS] を医訳	します。			
 権限ポリシー ざいます。+ で、あらかじ 	の選択が適切に設定 分にご注意いただい めご了承ください。	されない場合、意図しな たうえで設定を行ってく	い権限がメンバ ださい。なお、	ーに付与される 設定の不備等に	るなどの事故が こよる一切の責	発生しうる可能 任は負いかねま ⁻
タグの追加(オプシ	′ョン)」を設定しま	す。設定後、「次のスラ	-ップ: 確認」ボ	タンをクリック	フしてください。	5
aws サ ービス	▼ リソースグループ ~			グローバル 👻 サ	ポート *	
ロールの	乍成			1 2	3 4	
タグの追加	(オプション)					
IAM タグは、ロール きます タグを使用	レに追加できるキーと値のペアで	す。タグには、E メールアドレスなど(該理 追跡 制御できます 詳細(け)	のユーザー情報を含めるカ てちら	、役職などの説明文と	することがで	
±	値(オプシ				削除	
新しいキーを追					1313	
さらに 50 個の夕	グを追加できます。					
			キャンセル 戻	る 次のステップ:	確認	
🗨 フィードバック 🔇 日ネ	k語 © 201	8 - 2019, Amazon Web Services, Inc. または	その関連会社。無断転用禁止。	プライバシーポリシー	- 利用規約	
∩ 必要に応じて	設定してください。					
てのページの	個では特に必要であ	りませくので トカトま	++ /			
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。			
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。 			
このページの コール名」を入力し ^{aws} サービス	例では特に必要であ - ・ます。入力後、「ロ ~ リソースグループ ~	りませんので、入力しま ――――――――――――――――――ーーーーーーーーーーーーーーーーーーー	せん。 7 リックします。	9⊐-Nu × サ	#−ト ▼	
このページの コール名」を入力し aws サービス ロールの	例では特に必要であ .ます。入力後、「ロ 、 リソースグループ、 乍成	りませんので、入力しま ――――――――――――――――――――――――ーーーーーーーーーーーーー	せん。 "リックします。	90-Jul + 43	#−ト ▼	
このページの コール名」を入力し aws サービス ロールの(確認	例では特に必要であ ・ます。入力後、「ロ 、 リソースグループ 、 作成	りませんので、入力しま ―――――――――――――――――――――――――ーーーーーーーーーーーー	せん。 7 リックします。	90-JUL * 97	₩-► ▼ 3 4	
このページの コール名」を入力し aws サービス ロールの 確認 以下に必要な情報の	例では特に必要であ ・ます。入力後、「ロ ・ リソースグループ ~ 作成 * * ####LUTC2000Juを見直して	りませんので、入力しま ールの作成」ボタンをく ^{から、作成してください。}	せん。 	90-/01 × 9/	π−ト ▼ 3 4	
このページの コール名」を入力し aws サービス ロールの 確認 _{以下に必要な情報}	例では特に必要であ ・ます。入力後、「ロ 、 リソースグループ 、 作成 * #症してこのロールを見直して ロール名・	りませんので、入力しま ールの作成」ボタンをク ^{から、作成してください。} cgtestrole	せん。 יリックします。 -	90-JUL * 47	₩-► ¥ 3 4	
このページの コール名」を入力し aws リービス ロールの 確認 _{以下に必要な情報}	例では特に必要であ ます。入力後、「ロ 、 リソースグループ 、 作成 [#] 推定してこのロールを見直して ロール名 [*]	りませんので、入力しま ールの作成」ボタンをく から、作成してください。 cgtestrole 英語字と「+=、@-」を使用します。 風大64	せん。 7 リックします。 [×]	90-Ju + 93	₹-ト▼ 3 4	
このページの コール名」を入力し aws サービス ロールの 確認 _{以下に必要な情報}	例では特に必要であ ・ます。入力後、「ロ 、 リソースグループ 、 作成 * 増定してこのロールを見直して ロール名・	りませんので、入力しま ールの作成」ボタンをく から、作成してください。 cglestrole GakuNin Cloud Gateway Service Tes	せん。 7 リックします。 	90-JUL * 9,	1t−ト × 3 4	
このページの コール名」を入力し aws サービス ロールの 確認 以下に必要な情報	例では特に必要であ ます。入力後、「ロ 、 リソースグループ 、 作成 部ましてこのロールを見直して ロール名・ ロールの説明	りませんので、入力しま ールの作成」ボタンをく から、作成してください。 cgtestrole 英歌字と「+=,@-」を使用します。 最大らく GatuMin Cloud Gateway Service Tes	せん。 7 リックします。 ¹ ¹ ¹ ¹ ¹ ¹	Ø⊡–Júl ▼ 92 1 2	₫	
このページの コール名」を入力し aws サービス ロールの 確認 以下に必要な情報	例では特に必要であ *ます。入力後、「ロ * リソースグループ * 作成 * # # 店 に ロール名・ ロールの説明	りませんので、入力しま ールの作成」ボタンをく ^{DPら、作成してください。} cgtestrole ^{R数字と「+=} .@-」を使用します。最大64 <u>GakuNin</u> Cloud Gateway Service Tes	せん。 7 リックします。 	<i>θ</i> α- <i>Λ</i> υ • 9 λ	#−►▼	
このページの コール名」を入力し () サービス ロールの 確認 以下に必要な情報	例では特に必要であ *ます。入力後、「ロ * リソースグループ * 作成 #指定してこのロールを見直して ロール名・ ロールの説明	りませんので、入力しま ールの作成」ボタンを から、作成してください。 cglestrole 変数字と「+=_@」を使用します。最大 64 <u>Gekullin</u> Cloud Galeway Service Tes 意大 1000 文字。英数字と「+=_@」を使	せん。 7 リックします 。 	グローバル × サス (1) (2) (#-► ▼ 3 4	
このページの コール名」を入力し aws サービス ロールの 確認 以下に必要な情報	例では特に必要であ ます。入力後、「ロ 、リソースグループ、 作成 印ルを見直して ロール名・ ロールの説明	りませんので、入力しま ールの作成」ボタンをク いら、作成してください。 cgtestrole 発酵子と「+=、@-」」を使用します。最大64 <u>Gatullin</u> Cloud Gateway Service Tes at 1000 文字。英数字と「+=、@-」を使 Dプロノ(イダ arn:aws.iam.	せん。 7 リックします。 文字。 1 Role 目します。	9——Ли ~ 9/ 1 2 (#−► ▼ 3 4	
このページの コール名」を入力し () サービス ロールの 確認 以下に必要な情報	例では特に必要であ *ます。入力後、「ロ * リソースグループ * 作成 #描定してこのロールを見直して ロール名・ ロールの説明 信頼されたエンティティ ポリシー	りませんので、入力しま ールの作成」ボタンをク から、作成してください。 cglestrole 気歌字と「+=、@・_」を使用します。最大& GatuMin Cloud Gateway Service Tes 歌大 1000 文字。英歌字と「+=、@・_」を使 D プロパイダ arn.aws.iam.	せん。 フリックします。 	クローバル マ サ	1 1 1 1 1 1 1 1 1 1	
このページの コール名」を入力し (ロールの) 確認 以下に必要な情報	例では特に必要であ ます。入力後、「ロ 、リソースグループ 、 作成 電猫注してこのロールを見直して ロールる: ロールの説明 信頼されたエンティティ ポリシー アクセス権限の境界	りませんので、入力しま ールの作成」ボタンをク いら、作成してください。 cgtestrole 東京チと「+=_@」を使用します。最大64 <u>Catuallin</u> Cloud Gateway Service Tes 最大 1000 文字。英歌字と「+=_@_」を使 D プロノ(イダ arr: aws: iam: AmazonS3FullAccess C アクセス推開の境界が設定されています	せん。 7 リックします。 文字。 1 Role 目します。 ====================================	9—Ли • 9/ 1 2	#−►▼	
このページの コール名」を入力し (ロールの) 確認 以下に必要な情報	例では特に必要であ ・ます。入力後、「ロ 、 リソースグループ 、 作成 電描定してこのロールを見直して ロール名・ ロールの説明 信頼されたエンティティ ポリシー アクセス権限の境界	りませんので、入力しま ールの作成」ボタンをく から、作成してください。 cgtestrole 変数字と「+=_@」を使用します。最大64 GatuNin Cloud Gateway Service Tes 最大 1000 文字。英数字と「+=_@」を使 D プロノ(イダ am:aws:iam:	せん。 フリックします。 マリックします。 ロンステ・ ロ Role 和します。 asami-provider/cgtest	クローバル マ サ	1 1 − ► ▼ 3 4	
このページの コール名」を入力し いい の ロールの 確認 以下に必要な情報 が 追加されたタグは都	例では特に必要であ ・ます。入力後、「ロ ・ます。入力後、「ロ ・ で 作成 電描されたエンティティ ポリシー アクセス権限の境界 ちりません。	りませんので、入力しま ールの作成」ボタンをク から、作成してください。 cgtestrole 天教字と「+=_@」を使用します。最大64 GakuNin Cloud Gateway Service Tes 最大 1000 文字。英教字と「+=_@_」を使用 D プロノ(イダ am:aws:iam: AmazonS3FullAccess [2] アクセス権限の境界が設定されていませ	せん。 7 リックします。 マリックします。 マラ・ t Role 和します。	9 — Лоц ∨ 99. 1 2 (≭−ト ▼ 3 4	
このページの コール名」を入力し (ロールの) 確認 以下に必要な情報の <i>協加されたタグは</i> 都 ・必須	例では特に必要であ ・ます。入力後、「ロ 、 リソースグループ 、 作成 ご指定してこのロールを見直して ロール名・ ロールの説明 低額されたエンティティ ポリシー アクセス権限の境界 ちりません。	りませんので、入力しま ールの作成」ボタンをく から、作成してください。 cgtestrole 酸素と「+=_@-」を使用します。最大64 GatuMin Cloud Gateway Service Tes at 1000 文字。英数字と「+=,@-」を使 D プロノ(イダ arn.aws.iam. AmazonS3FullAccess [プ アクセス権限の境界が設定されていまけ	せん。 フリックします。 マネ・ I Role BLます。 まaml-provider/cgtest さん キャンセル	グローバル マ サ 1 2 (provider	K→ト × 3 4	
このページの ロール名」を入力し aws サービス ロールの 確認 以下に必要な情報の 追加されたタグはる *必須 マーードバック ② 日2	例では特に必要であ ・ます。入力後、「ロ ・ます。入力後、「ロ ・ます。入力後、「ロ ・ます。入力後、「ロ ・ にののです。 「「「「」」」 「「」」」 「「」」」 「「」」」 「」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」 「」」 「」」」 「」」」 「」」」 「」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」 「	りませんので、入力しま ールの作成」ボタンをグ から、作成してください。 cglestrole 愛数字と「+=、@-」」を使用します。最大ら GakuNin Cloud Gateway Service Tes at 1000 文字。英数字と「+=、@-」を使 D プロノ(イダ arn:aws:lam: AmazonS3FullAccess C アクセス権限の境界が設定されていまけ	せん。 アリックします。 マンマ・ 1 Role 日します。 こ、 ネー、 コー、 コー、 コー、 コー、 コー、 コー、 コー、 コ	グローバル × サ (1) (2) (provider 厚る) ロールの プライバシーボリシー	ポート ▼ 3 4	
このページの コール名」を入力し aws サービス ロールの 確認 以下に必要な情報 が必須 マイードバック マ 日本	例では特に必要であ ます。入力後、「ロ 、リソースグループ 、 「 下成 「 「 「 「 「 」 「 」 」 、 、 、 、 、 、 、 、 、 、 、	りませんので、入力しま ールの作成」ボタンをク いら、作成してください。 cgtestrole 定意を「r=_@」を使用します。最大64 <u>GatuNin</u> Cloud Gateway Service Tes 国大 1000 文字。英数字と「+=_@_」を使 D プロノ(イダ arn.aws.iam. AmazonS3FullAccess [プ アクセス権限の境界が設定されていまけ 82-2019, Amazon Web Services, Inc または	せん。 7 リックします。 7 以ックします。 (Role 目します。 まami-provider/cgtest さん キャンセル 2 の間連会社、無時転用禁止	グローバル マ サル 1 2 (provider 厚る ロールの プライバ (Sーボリ Sー	ポート マ 3	
このページの コール名」を入力し (ロールの) 確認 以下に必要な情報 <i>追加されたタグは</i> ・必須 マィードバック ② 日2	例では特に必要であ *ます。入力後、「ロ * リソースグループ * 作成 * 作成 ロールを見直して ロール名・ ロールの説明 低額されたエンティティ ポリシー アクセス権限の境界 50ません。 * * * * * * * * * * * * *	りませんので、入力しま ールの作成」ボタンをく から、作成してください。 cgtestrole 数字と「+=_@-」を使用します。最大64 GatuMin Cloud Gateway Service Tes at 1000 文字。英数字と「+=_@-」を使 D プロノ(イダ arn:aws.iam: AmazonS3FullAccess [3] アクセス権限の境界が設定されていまけ 8 - 2019. Amazon Web Services, Inc. または	せん。 7 リックします。 文字. t Role 乱します。 こ sami-provider/cgtest さん モャンセル CODW連会社、無所転用禁止.	グローバル × サ 1 2 (1 2) (provider	ポート ▼ 3 4	

⚠



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。

IAM の検索	•	□-ル > cgtestrole 概要					ロールの削除
ダッシュボード		D—JL ARN	am:aws:iam::	ole/cgtestrole 🖉			
クルーノ		ロールの説明	GakuNin Cloud Gateway Servi	ce Test Role 編集	E.		
ב-ש- ש-ש		インスタンスプロファイル ARN	4				
ポリシー		パス	/				
ID プロバイダー		作成時刻	2019-05-11 12:32 UTC+0900				
アカウント設定		最大 CLI/API セッション期間	1 時間 編集				
認証情報レポート		アクセス権限 信頼関係	タグ アクセスアドバイザー	セッションの	無効化		
啼号//七—		ロールと、ロールのアクセス条件	キを引き受けることができる信頼さ	れたエンティティ	を表示できま	ます。 ポリシードキュメン	ントの表示
-01 C H		信頼関係の編集					
		信頼されたエンティティ		条件			
		以下の信頼されたエンティティマ とができます。	こは、このロールを引き受けるこ	以下の条件で 方法とタイミ	は、信頼され ングを定義し	たエンティティがロール ます。	を引き受ける
		信頼されたエンティティ		条件	‡ -	値	
			ml.provider/catestprovider	StringEquals	SAMI aud	https://signin.aws.amaz	

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。
     }
   }
 ]
}
```

 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「h ttps://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。

(1)

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。

	リソースグループ 、	グローバル 🔻	サポート 👻
信頼関係の編集	信頼関係の編集 以下のアクセスコントロールポリシードキュメントを編集して、信頼関係をカスタマイズできます。		
	<pre>#USP_EXELECT 100000 THINST Camability of the complete the maximum and system that the complete the maximum and the complete the co</pre>	stprovider" gtestgroup"	
	- +r:	ンセル 信頼が	ペリシーの更新

d. 「条件」が次の通りになっていれば問題ありません。

	概要								[ロールの削除
ダッシュボード			0-,	JL ARN	am:aws:iam::	role/cgtestrole d	ත			
グループ			ロール	の説明	GakuNin Cloud	Gateway Service Test Role				
ユーザー		インスタンスプ	ロファイル	JL ARN	ත					
ロール				パス	1					
ポリシー			f i	F成時刻	2019-05-11 12:3	32 UTC+0900				
ID プロバイダー		品大 CLI/AP	1 セッショ	シ期間	1時間編集					
アカウント設定			1- 14	-						
認証情報レポート	アリセス権限	偏親関係	90	100	x/F/17-	セッションの無効化				
	ロールと、ロー	ールのアクセスダ	条件を引き	受けること	とができる信頼さ	れたエンティティを表示でき	ます。 ポリシードキュメントの	表示		
暗号化キー	信頼関係の編	6 #								
暗号化ギー	信頼責係の制	二 ンティティ					条件			
暗号化干一	信頼団係の総 信頼されたエ 以下の信頼され	ま集 : ンティティ 1たエンティテ・	ィでは、こ	このロールを	を引き受けること	ができます。	条件 以下の条件では、信頼され す。	たエンティティがロールを引き	受ける方法とタイミング	を定義しま
暗号化丰一	信頼関係の 創 信頼されたエ 以下の信頼され 信頼されたエ	鉄 ンティティ 1たエンティテ・ ンティティ	ィでは、こ	このロールオ	を引き受けること;	ができます。	条件 以下の条件では、信頼され す。	たエンティティがロールを引き	受ける方法とタイミング	を定義しま
错号 化千一	信頼関係の領 信頼されたエ 以下の信頼され 信頼されたエ am:aws:lam:	5集 ンティティ 1たエンティテ・ ンティティ	ィでは、こ sami-provi	このロールオ ider/cgtestp	を引き受けること: provider	ができます。	条件 以下の条件では、信頼され す。 条件 StringEquals	たエンティティがロールを引き キー SAML:aud	受ける方法とタイミング 値 https://signin.aws.am	「を定義しま
暗号化丰一	信頼団係の 信頼されたエ 以下の信頼され G頼されたエン am:aws.iam.	(大) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	ィでは、こ sami-provi	このロールオ ider/cgtestp	を引き受けること: provider	ができます。	<mark>条件</mark> 以下の条件では、信頼され す。 条 <mark>件</mark> StringEquals	たエンティティがロールを引き キー SAML:aud	受ける方法とタイミング <mark>値</mark> https://signin.aws.am	を定義しま izon.com/saml
₩99化ギー	信頼回係の 信頼されたエ 以下の信頼され 「 朝たれたエ am:awsiam:	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	ィでは、こ sami-provi	このロールオ ider/cgtest	を引き受けること: provider	ができます。	<mark>条件</mark> 以下の条件では、信頼され す。 条 <mark>件</mark> StringEquals ForAnyValue StringEquals	たエンティティがロールを引き キー SAML:aud SAML:eduPersonEntitlement	受ける方法とタイミング 値 https://signin.aws.am https://cg.gakunin.jp/c	を定義しま izon.com/saml
错号化千一	低税関係の総 信頼されたエ 以下の信頼され 伝頼されたエ amawsiam	また ンティティ 北たエンティテ・ ンティティ	ィでは、こ sami-provi	このロールオ ider/cgtest	を引き受けること: provider	ができます。	<mark>条件</mark> 以下の条件では、信頼され す。 <mark>条件</mark> StringEquals ForAnyValue:StringEquals	たエンティティがロールを引き キー SAML:aud SAML.eduPersonEntitlement	受ける方法とタイミング <mark>値</mark> https://signin.aws.am: https://cg.gakunin.jp/c	で定義しま izon.com/saml r/cgtestgroup
暗号化书一	気納司係のは 信頼されたエ 以下の信頼され これ これ これ これ これ これ これ これ これ こ	5年 ンティティ 1たエンティテ・ ンティティ	イでは、こ sami-provi	ごのロールオ Ider/cgtestp	を引き受けること。 provider	ができます。	<mark>条件</mark> 以下の永千では、信頼され す。 <mark>条件</mark> StringEquals ForAnyValue StringEquals	たエンディディがロールを引き キー SAMLaud SAMLeduPersonEntitlement	受ける方法とタイミング 値 https://signin.aws.am: https://cg.gakunin.jp/g	を定義しま izon.com/saml r/cgtestgroup
贈列化キー	信頼可任の に 構造 れた工 に 下の 信頼 された工 : am aws iam 日本語	5集 ンティティ 北たエンティテ・ ンティティ	イでは、こ sami-provi	ごの□−ルオ	を引き受けること: provider	ができます。 の2	会件 以下の条件では、信頼され す。	たエンディティがロールを引き キー SAML adu SAML eduPersonEntillement ne. 非たはその検達会社。物味有明	受ける方法とタイミング 値 https://signin.aws.ams https://cg.gakunin.jp/ t止、 プライバシーポリ	「を定義しま uzon.com/saml r/cgtestgroup シー 利用規約

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。

•	cgtestgroup > Webサービスの選択		
20	Dグループで利用するWebサービスを選択してください。		
	Webサービス	サービス側の承認	説明
ē	AWS Management Console	不要	AWS Management Console Single Sign-On

(ĵ) 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。

cgtestgroup > 利用Webサービス	
現在、このグループで利用しているサービスです。	
Webサービス	アクション
aws AWS Management Console	拡張属性の入力 サービスの利用停止
利用するWebサービスを追加	

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。

cgtestgroup > 拡張属性の入力	
ナービス名: AWS Management Console	
属性名	值
AWSRole (https://aws.amazon.com/SAML/Attributes/Role)	arn:aws:iam:: 入力補の追加
保存	キャンセル

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ヘ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。

AWS AWS Ma	nagement …
グループ表示	0
	🔁 cgtestgroup

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



AWS Management Console Single Sign-On / Amazon Web Services, Inc.

サービスに送信さ	サービスに送信される情報			
AWSName	xxxxx@example.ac.jp			
AWSRole	arn:aws:iam:::role/cgtestrole,arn:aws:iam:: provider/cgtestprovider			
eduPersonEntitlement	https://cg.gakunin.jp/gr/cgtestgroup/admin https://cg.gakunin.jp/gr/cgtestgroup https://cg.gakunin.jp/sp/			
isMemberOf	https://cg.gakunin.jp/gr/cgtestgroup/admin https://cg.gakunin.jp/gr/cgtestgroup https://cg.gakunin.jp/sp/			
<	>			

統行すると上記の情報はこのサービスに送信されます。このサービスにアクセスするたびに、あなたに関する情 報を送信することに同意しますか?

同意方法の選択:							
○ 次回ログイン時に再度チェックします。							
• 今回だけ情報を送信することに同意します。							
● このサービスに送信する情報が変わった場合は、再度チェックします。							
 今回と同じ情報であれば今後も自動的にこのサービスに送信することに同意します。 							
○ 今後はチェックしません。							
 すべての私に関する情報を今後アクセスするすべてのサービスに送信することに同意します。 							
この設定はログインページのチェックボックスでいつでも取り消すことができます。							
拒否同意							

↑ 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。

aws		
	ロールの選択:	
	▼ Account: 3f	
	⊖ samI-EC2ReadOnlyAccess	
	▼ Account: 64	
	sami-S3FullAccess	
	サインイン	
	日本語	
	利用規約 <u>プライバシーボリシー</u> © 1990-2019, Amazon Web Services, Inc. or its affiliates.	

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。

	9-24 • 97-4	510 5 * ¥			A cycanore analysis and a second seco	- A/(1.4 -	
	AWS マネ	ジメントコ	レソール	フェデ cgtestr アカウ	レーションログイン: role/xxxxxife.ac.jp >ト:		
	AWS のサービス			マイア マイ組	カウント 織		
	サービスを検索する SR、キーフード、国家学を入力できます。 Q、例:Atelational Database Service、データベース、RDS ▶ すべてのサービス ソリユーションの構築 シングルなウィザードと目動にされたワークフローで作用を観察しましょう。			マイ請求ダッシュボード スイッチロール ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー		用してマネジ	
					AWS を試す		
				Amazon RDS リレーショナルデータベースの設定、運用、拡張をクラウ ドで、 詳細はこちら [2]			
	依拠マシンを記録する ウェブアブリを描集する 仮型サーバーを使用して EC2 を使用 Elastic Beanstalk を使用 算する 2~3分 6 分 Lightsalk を使用 1/2 く分 1/2 く分 1/2 く分			Amazon SageMaker すべての開発者とデータサイエンティストの 習。 詳細はごちら C			
	O	ි			AWS Marketplace AWS で実行できる一般的なソフトウェア製 入、デブロイします。 詳細はごちら ご	品を検索、購	
	loT デバイスを接続する	開発プロジェクトを開始す	ドメインを登録する				

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 AWSコン ソールSSOの実際 – 」』(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。