

ユーザマニュアル

～Amazon Web Services～

第1.0版
2019/12/2

東日本電信電話株式会社

- 本マニュアルの一部または全部を東日本電信電話株式会社の許可なく複製することを禁じます。
- 本マニュアルの内容を予告なく変更することがあります。
- その他のサービス名などの固有名詞は、Amazon Web Services, Inc.の登録商標または商標です。
- 本文中のAmazon Web Services, Inc.の登録商標または商標には®マークは表示していません。
- 本マニュアルの操作画面は、2019年10月25日時点の画面です。実際の画面と異なる場合がございます。

1. 目次

1. 目次	3
2. 本マニュアルの位置づけ	4
3. IAMユーザ／ロール作成	5
3-1 IAMユーザ作成手順	5
3-2 IAMロール作成手順	11
3-3 (参考)アクセス権の境界を設定しない場合	17
4. コスト配分タグ	18
5. 問い合わせ先	19

2. 本マニュアルの位置づけ

NTT東日本のAWSリセール（以下、本サービス）をご契約いただき誠にありがとうございます。

本サービスでは、弊社にてお客様のアカウントを管理させていただいており、お客様のAWS環境にいくつか制限を設けております。

制限の適用方法として、「アクセス権限の境界（Permissions Boundary）※1」という仕組みを採用しています。

そのため、お客様ご自身でIAMユーザおよびIAMロールを作成される際に、この「アクセス権限の境界」の設定を実施いただく必要がございます。

本マニュアルでは、AWSマネジメントコンソールにおける、IAMユーザ／ロール作成手順を示します。「アクセス権限の境界」を正しく設定しない場合、エラーとなりユーザやロールを作成できません。

また、お客様ご自身にてコスト管理をされる際に使用可能なタグを、NTT東日本にて事前に設定しております。必要に応じてご利用ください。

※1 IAM エンティティのアクセス許可の境界 https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/access_policies_boundaries.html

3-1 IAMユーザー作成手順 (1/6)

- ① AWSマネジメントコンソールにて「Identity and Access Management(IAM)」へアクセス
- ② 「ユーザー」をクリック
- ③ 「ユーザーを追加」をクリック

ダッシュボード
グループ ②
ユーザー
ロール
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

③
ユーザーを追加 ユーザーの削除

Q ユーザー名またはアクセスキーでユーザーを検索 0件の結果を表示中

<input type="checkbox"/>	ユーザー名 ▾	グループ	アクセスキーの古さ	パスワードの古さ	最後のアクティビティ	MFA
--------------------------	---------	------	-----------	----------	------------	-----

Q IAMの検索

▼ AWS Organizations
Organization activity
Service control policies (SCPs)

3-1 IAMユーザ作成手順 (2/6)

- ① 「ユーザ名」を入力
- ② 「AWSアクセスの種類を選択」欄はお客様環境に合わせて設定
- ③ 「次のステップ」をクリック

ユーザーを追加

1 2 3 4 5

ユーザー詳細の設定

同じアクセスの種類とアクセス権限を使用して複数のユーザーを一度に追加できます。 [詳細はこちら](#)

ユーザー名* ①

[別のユーザーの追加](#)

AWS アクセスの種類を選択

これらのユーザーから AWS にアクセスする方法を選択します。アクセスキーと自動生成パスワードは前のステップで提供されています。 [詳細はこちら](#)

アクセスの種類* プログラムによるアクセス
AWS API、CLI、SDK などの開発ツールの **アクセスキー ID とシークレットアクセスキー** を有効にします。

AWS マネジメントコンソールへのアクセス
ユーザーに AWS マネジメントコンソールへのサインインを許可するための **パスワード** を有効にします。

コンソールのパスワード* 自動生成パスワード
 カスタムパスワード

パスワードのリセットが必要 ユーザーは次回のサインインで新しいパスワードを作成する必要があります
ユーザーは、自動的に `IAMUserChangePassword` ポリシーを取得し、自分のパスワードを変更できるようにします。

* 必須

[キャンセル](#) [次のステップ: アクセス権限](#) ③

3-1 IAMユーザー作成手順 (3/6)

- ① お客様にて必要な権限を付与（ポリシーのアタッチ、グループへの追加、など）
- ② 「既存のポリシーを直接アタッチ」をクリック
- ③ 「アクセス権限の境界の設定」をクリック ※まだ「次のステップ」はクリックしないでください

ユーザーを追加

1 2 3 4 5

▼ アクセス許可の設定 ②

ユーザーをグループに追加 アクセス権限を既存のユーザーからコピー **既存のポリシーを直接アタッチ**

ポリシーの作成

ポリシーのフィルタ ▼ 🔍 検索 476 件の結果を表示中

	ポリシー名 ▼	タイプ	次として使用	説明
<input checked="" type="checkbox"/>	AdministratorAccess	ジョブ機能	Permissions policy (7)	Provides full access to AWS services and...
<input type="checkbox"/>	Administrators	ユーザーによる管理	Permissions policy (1)	
<input type="checkbox"/>	AlexaForBusinessD...	AWS による管理	なし	Provide device setup access to AlexaFor...
<input type="checkbox"/>	AlexaForBusinessF...	AWS による管理	なし	Grants full access to AlexaForBusiness r...
<input type="checkbox"/>	AlexaForBusinessG...	AWS による管理	なし	Provide gateway execution access to Ale...
<input type="checkbox"/>	AlexaForBusinessP...	AWS による管理	なし	Provide access to Poly AVS devices
<input type="checkbox"/>	AlexaForBusinessR...	AWS による管理	なし	Provide read only access to AlexaForBus...

③

▼ アクセス権限の境界の設定

この user が持つことができる最大のアクセス権限を制御するアクセス権限の境界を設定します。これは、アクセス権限の管理を他社に委任するために使用する拡張機能です。 [詳細はこちら](#)

キャンセル 戻る 次のステップ: タグ

3-1 IAMユーザー作成手順 (4/6)

- ① 「アクセス権限の境界を使用して user の最大アクセス権限を制御する」を選択
- ② ポリシー一覧より「Boundary_for_CustomerAdmin」を選択
- ③ 「次のステップ」をクリック

Provide read only access to AlexaForBus...

▼ アクセス権限の境界の設定

この user が持つことができる最大のアクセス権限を制御するアクセス権限の境界を設定します。これは、アクセス権限の管理を他社に委任するために使用する拡張機能です。 [詳細はこちら](#)

アクセス権限の境界を設定せずに user を作成する

アクセス権限の境界を使用して user の最大アクセス権限を制御する

アクセス権限の境界を設定するポリシーを選択します

ポリシーの作成 🔄

ポリシーのフィルタ 8 件の結果を表示中

ポリシー名	タイプ	次として使用	説明
Boundary_for_Cust...	ユーザーによる管理	Boundary (1)	

キャンセル 戻る 次のステップ: タグ

3-1 IAMユーザー作成手順 (5/6)

- ① 必要に応じてタグを追加
- ② 「次のステップ」をクリック

ユーザーを追加

1 2 3 4 5

タグの追加 (オプション)

IAM タグは、ユーザー 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のユーザー情報を含めるか、役職などの説明文とすることができます。タグを使用して、このユーザー のアクセスを整理、追跡、制御できます。 [詳細はこちら](#)

キー	値 (オプション)	削除
① ① 新しいキーを追加		

さらに 50 個のタグを追加できます。

キャンセル 戻る ② 次のステップ: 確認

3-1 IAMユーザー作成手順 (6/6)

- ① アクセス権限の境界に「Boundary_for_CustomerAdmin」があることを確認
- ② その他、お客様にて設定したポリシー等が正しいか確認
- ③ 「ユーザーの作成」をクリック

ユーザーを追加

1 2 3 4 5

確認

選択内容を確認します。ユーザーを作成した後で、自動生成パスワードとアクセスキーを確認してダウンロードできます。

ユーザー詳細

ユーザー名	sample-user
AWS アクセスの種類	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へのアクセス
コンソールのパスワードの種類	自動生成
パスワードのリセットが必要	はい
アクセス権限の境界	Boundary_for_CustomerAdmin

アクセス権限の概要

次のポリシー例は、上記のユーザーにアタッチされます。

タイプ	名前
管理ポリシー	AdministratorAccess
管理ポリシー	IAMUserChangePassword

タグ

追加されたタグはありません。

キャンセル 戻る **ユーザーの作成**

3-2 IAMロール作成手順 (1/6)

- ① AWSマネジメントコンソールにて「Identity and Access Management(IAM)」へアクセス
- ② 「ロール」をクリック
- ③ 「ロールを作成」をクリック

ダッシュボード
グループ
ユーザー
② **ロール**
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

③ **ロールの作成** ロールの削除

検索 9件の結果を表示中

ロール名	説明	信頼されたエンティティ

IAM の検索

▼ AWS Organizations
Organization activity
Service control policies (SCPs)

3-2 IAMロール作成手順 (2/6)

- ① お客様にて必要なエンティティの種類を選択
- ② 「次のステップ」をクリック

ロールの作成

信頼されたエンティティの種類を選択 ①

1 2 3 4

AWS サービス
EC2、Lambda、およびその他

別の AWS アカウント
お客様またはサードパーティに属しています

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

AWS のサービスによるアクションの代行を許可します。 [詳細はこちら](#)

このロールを使用するサービスを選択

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

API Gateway	CodeDeploy	ElastiCache	Lambda	S3
AWS Backup	Comprehend	Elastic Beanstalk	Lex	SMS
AWS Chatbot	Config	Elastic Container Service	License Manager	SNS
AWS Support	Connect	Elastic Transcoder	Machine Learning	SWF
Amplify	DMS	ElasticLoadBalancing	Macie	SageMaker
AppStream 2.0	Data Lifecycle Manager	Forecast	MediaConvert	Security Hub
AppSync	Data Pipeline	Global Accelerator	Migration Hub	Service Catalog
Application Auto Scaling	DataSync	Glue	OpsWorks	Step Functions
Application Discovery Service	DeepLens	Greengrass	Personalize	Storage Gateway
Batch	Directory Service	GuardDuty	QLDB	Textract
CloudFormation	DynamoDB	Inspector	RAM	Transfer
CloudHSM	EC2	IoT	RDS	Trusted Advisor

* 必須

キャンセル **次のステップ: アクセス権限** ②

3-2 IAMロール作成手順 (3/6)

- ① 「Attach アクセス権限ポリシー」にて、必要なポリシーをアタッチ
- ② 「アクセス権限の境界の設定」をクリック
- ③ 「アクセス権限の境界を使用して user の最大アクセス権限を制御する」を選択

①

②

③

④

ロールの作成

▼ 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 🔄

ポリシーのフィルタ 570件の結果を表示中

<input type="checkbox"/>	ポリシー名	次として使用	説明
<input type="checkbox"/>	AdministratorAccess	Permissions policy (8)	Provides full access to AWS services ...
<input type="checkbox"/>	Administrators	Permissions policy (1)	
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	なし	Provide device setup access to Alexa...
<input type="checkbox"/>	AlexaForBusinessFullAccess	なし	Grants full access to AlexaForBusines...
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	なし	Provide gateway execution access to ...
<input type="checkbox"/>	AlexaForBusinessNetworkProfileServicePolicy	なし	This policy enables Alexa for Business...

▼ アクセス権限の境界の設定 ②

この role が持つことができる最大のアクセス権限を制御するアクセス権限の境界を設定します。これは、アクセス権限の管理を他社に委任するために使用する拡張機能です。 [詳細はこちら](#)

アクセス権限の境界を設定せずに role を作成する

アクセス権限の境界を使用して role の最大アクセス権限を制御する ③

アクセス権限の境界を設定するポリシーを選択します

* 必須

キャンセル 戻る 次のステップ: タグ

3-2 IAMロール作成手順 (4/6)

- ① ポリシー一覧より「Boundary_for_CustomerAdmin」を選択
- ② 「次のステップ」をクリック

この画面は、IAMコンソールの「アクセス権限の境界の設定」ページを示しています。このページでは、特定のロールに適用するアクセス権限の境界を設定するためのポリシーを選択します。

このrole が持つことができる最大のアクセス権限を制御するアクセス権限の境界を設定します。これは、アクセス権限の管理を他社に委任するために使用する拡張機能です。 [詳細はこちら](#)

アクセス権限の境界を設定せずに role を作成する
 アクセス権限の境界を使用して role の最大アクセス権限を制御する

アクセス権限の境界を設定するポリシーを選択します

ポリシーの作成 🔄

ポリシーのフィルタ 8件の結果を表示中

ポリシー名	次として使用	説明
<input checked="" type="radio"/> Boundary_for_CustomerAdmin	<input type="checkbox"/>	Boundary (2)

* 必須 キャンセル 戻る 次のステップ: タグ

3-2 IAMロール作成手順 (5/6)

- ① 必要に応じてタグを追加
- ② 「次のステップ」をクリック

ロールの作成

1 2 3 4

タグの追加 (オプション)

IAM タグは、ロール 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のユーザー情報を含めるか、役職などの説明文とすることができます。タグを使用して、このロールのアクセスを整理、追跡、制御できます。 [詳細はこちら](#)

キー	値 (オプション)	削除
<input type="text" value="新しいキーを追加"/>	<input type="text"/>	①

さらに 50 個のタグを追加できます。

キャンセル 戻る **次のステップ: 確認** ②

3-2 IAMロール作成手順 (6/6)

- ① アクセス権限の境界に「Boundary_for_CustomerAdmin」があることを確認
- ② その他、お客様にて設定したポリシー等が正しいか確認
- ③ 「ロールの作成」をクリック

ロールの作成

1 2 3 4

確認

以下に必要な情報を指定してこのロールを見直してから、作成してください。

ロール名*
英数字と「+,@,_」を使用します。最大 64 文字。

ロールの説明
最大 1000 文字。英数字と「+,@,_」を使用します。

信頼されたエンティティ AWS のサービス: ec2.amazonaws.com

ポリシー  AdministratorAccess [🔗](#)

アクセス権限の境界 [🔗](#)

追加されたタグはありません。

* 必須

キャンセル 戻る **ロールの作成**

3-3 (参考)アクセス権限の境界を設定しない場合

- アクセス権限の境界にて「Boundary_for_CustomerAdmin」を設定せずにIAMユーザ/ロールの作成を行う場合、下記のようにエラーとなり作成ができません。

ユーザーを追加

1 2 3 4 5

❗ ユーザーを作成できません
AWSはリクエストされたユーザーを作成できませんでした。 [詳細はこちら](#)

User:arn:aws:iam::[redacted]:user:[redacted] is not authorized to perform: iam:CreateUser on resource: arn:aws:iam::[redacted]:user/sample-user01 with an explicit deny

確認

選択内容を確認します。ユーザーを作成した後で、自動生成パスワードとアクセスキーを確認してダウンロードできます。

ユーザー詳細

ユーザー名	sample-user01
AWS アクセスの種類	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へのアクセス
コンソールのパスワードの種類	カスタム
パスワードのリセットが必要	いいえ
アクセス権限の境界	アクセス権限の境界が設定されていません

アクセス権限の概要

次のポリシー例は、上記のユーザーにアタッチされます。

タイプ	名前
管理ポリシー	AdministratorAccess

タグ

追加されたタグはありません。

キャンセル 戻る **ユーザーの作成**

4. コスト配分タグについて

- お客様にてコスト配分タグによるコスト管理が可能です。
- 必要に応じてリソースにタグ付けし、ご利用ください。

■ 使用可能なコスト配分タグ

- Name
- Owner
- Department
- Application
- Category1
- Category2
- Category3

■ 注意事項

お客様にてBillingコンソールへアクセスいただくにあたり、下記注意願います。

- 「課税設定」は変更しないでください。

5. 問い合わせ先

- 本マニュアルやAWS操作方法に関するお問い合わせは、下記までご連絡をお願いします。

■ Webお問い合わせフォーム

<https://business.ntt-east.co.jp/gf/form.php?service=gi0538&type=pc>

※お問い合わせ時に必要な「アカウント管理番号」は、『アカウント発行のご案内』に記載のCSIから始まる番号です。



【参考】 Amazon Web Services (AWS)がご利用できない際のお問い合わせ

<https://business.ntt-east.co.jp/gf/form.php?service=gi0539&type=pc>

※お問い合わせ時に必要な「アカウント管理番号」は、『アカウント発行のご案内』に記載のCSIから始まる番号です。

