

AWS 資料

IMA ユーザの作成

改訂履歴

年月	版	作成者	詳細
2021 年 11 月 26 日	1.0	青山	新規作成

内容

1. IAM ユーザの作成.....	5
1.1. 手順.....	5
1.2. IAM ユーザーを作成する.....	6
2. 作成した IAM ユーザーに IAM ポリシーを適用する(1 で解決済み).....	9
3. AWS アカウント（ルートアカウント）の保護.....	11
3.1. AWS アカウントへ二段階認証を導入.....	11
3.1.1. IAM のページを開く.....	11
3.1.2. 「ルートアカウントの MFA を有効化」を選択して、「MFA の管理」ボタンをクリック.....	11
3.1.3. 「仮想 MFA デバイス」にチェックが入っていることを確認し、「次のステップ」ボタンをクリック.....	12
3.1.4. 注意書きを読んで、「今後はこのダイアログボックスを表示しない。」にチェックを入れて「次のステップ」ボタンをクリック.....	12
3.1.5. Google Authenticator など、QR コードを読み取って、表示された認証コード二つを入力し、「仮想 MFA の有効化」ボタンをクリック.....	13
3.1.6. 「完了」ボタンをクリック.....	13
4. グループの作成.....	14
4.1. IAM のページを開く.....	14
4.2. 「グループを使用してアクセス許可を割り当て」を選択し、「グループの管理」ボタンをクリック.....	14
4.3. 「新しいグループの作成」ボタンをクリック.....	14
4.4. グループ名を入力し、「次のステップ」ボタンをクリック.....	15
4.5. 「AdministratorAccess」ポリシーにチェックをいれて、「次のステップ」ボタンをクリック.....	15
4.6. 内容を確認し、「グループの作成」ボタンをクリック.....	15
4.7. グループ一覧から作成したグループをクリック.....	16
4.8. 「グループにユーザーを追加」ボタンをクリック.....	16
4.9. 作成したユーザーを選択し、「ユーザーの追加」ボタンをクリック.....	16
5. IAM パスワードポリシーの適用.....	17
5.1. IAM のページを開く.....	17
5.2. 「IAM パスワードポリシーの適用」を選択し、「パスワードポリシーの管理」ボタンをクリック.....	17

5.3. 任意のパスワードポリシーを設定し、「パスワードポリシーの適用」ボタンをクリック.....	17
---	----

1. IAM ユーザの作成

1.1. 手順

① ログイン

② AWS Identity and Access Management (IAM)サービス画面に移動する

左上にある「サービス」をクリックするか、隣のカラムに「IAM」を入力します。



左ペインに「Identity and Access Management (IAM)」と出てきたら OK です。



1.2. IAM ユーザーを作成する

左ペインから、「ユーザ」をクリックしましょう。



「ユーザーを追加」をクリックします。



ユーザーの設定をしていきます。

それぞれの設定を入力したら、右下から「次のステップ：アクセス権限」をクリックしてください。

設定値	設定内容
ユーザー名	IAM ユーザーの名前を設定してください。 アカウントの中ではユニークである必要があります。
アクセスの種類	そのユーザーが許可されるアクセスの方法を設定してください。 プログラムによるアクセス：Amazon CLI などを利用したアクセス方法 AWS マネジメントコンソールへのアクセス：Web ブラウザを利用したコンソールへのアクセス方法
コンソールのパスワード	自動でパスワードを生成されるようにするか、自身でパスワードを指定するかを設定してください。
パスワードのリセットが必要	初回ログイン時にパスワード変更を求めるかを設定してください。

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* Demo-User

+ 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。

次の画面では、作成する IAM ユーザーに対して IAM ポリシー等を利用して権限を付与することが可能です。

詳細な設定はせず、下記項目を選択し、「次のステップ：タグ」をクリックしてください。

▼ アクセス許可の設定

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

① クリック

ポリシーの作成

ポリシーのフィルタ ▼ Q 検索 647 件の結果を表示中

	ポリシー名 ▼	タイプ	次として使用
<input checked="" type="checkbox"/>	AdministratorAccess		Permissions policy (1)
<input type="checkbox"/>	AdministratorAccess-Amplify	AWS による管理	なし
<input type="checkbox"/>	AdministratorAccess-AWSElasticBeanstalk	AWS による管理	なし
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS による管理	なし
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS による管理	なし
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS による管理	なし
<input type="checkbox"/>	AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS による管理	なし
<input type="checkbox"/>	AlexaForBusinessPolyDelegatedAccessPolicy	AWS による管理	なし

② チェックボックスにチェック

更に、「次のステップ：確認」をクリックします。

確認の画面が出てきますので、その画面上で「ユーザーの作成」をクリックしてください。

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	Demo-User
AWS アクセスの種類	AWS マネジメントコンソールへのアクセス - パスワードを使用
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	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	IAMUserChangePassword

タグ

追加されたタグはありません。

パスワードを自動で生成されるように設定した場合は、

「csv のダウンロード」か、「パスワード」で「表示」をクリックしてパスワードを確認してください。パスワード情報を確認できる画面はここだけです。注意してください。

確認が終わりましたら「閉じる」をクリックしてください。



成功

以下に示すユーザーを正常に作成しました。ユーザーのセキュリティ認証情報を確認してダウンロードできます。AWS マネジメントコンソールへのサインイン手順を E メールでユーザーに送信することもできます。今回が、これらの認証情報をダウンロードできる最後の機会です。ただし、新しい認証情報はいつでも作成できます。

AWS マネジメントコンソールへのアクセス権を持つユーザーは「」でサインインできます

 .csv のダウンロード

	ユーザー	パスワード	ログイン手順を E メールで送信
▶	 Demo-User	***** 表示	Eメールの送信 

2. 作成した IAM ユーザーに IAM ポリシーを適用する(1 で解決済み)

IAM ユーザーに対して、権限を新たに付与していきます。

ユーザ名をクリックします



つぎに、「アクセス権限の追加」をクリックしてください。



管理者権限用の IAM ポリシーをアタッチしていきます。

①「既存のポリシーを直接アタッチ」をクリックします

②「AdministratorAccess」（こちらが管理者権限の IAM ポリシーです）のチェックボックスをチェックします

操作が終わったら、「次のステップ：確認」をクリックしてください。

Demo-User にアクセス権限を追加

アクセス許可の付与

IAM ポリシーを使用してアクセス権限を付与します。既存のポリシーを割り当てるか、新しいポリシーを作成できます。

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

① クリック

ポリシーの作成

ポリシーのフィルタ

ポリシー名
<input type="checkbox"/> AdministratorAccess
<input type="checkbox"/> AdministratorAccess-Amplify
<input type="checkbox"/> AdministratorAccess-AWSElasticBeanstalk

② チェックボックスにチェック

追加されるアクセス権限を確認し、「アクセス権限の追加」をクリックします。

Demo-User にアクセス権限を追加

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

追加した IAM ポリシーがアタッチされていることをご確認ください。

アクセス権限 グループ タグ 認証情報 アクセスアドバイザー

▼ Permissions policies (2 適用済みポリシー)

アクセス権限の追加

ポリシー名 ▼

直接アタッチ済み

- ▶ AdministratorAccess
- ▶ IAMUserChangePassword

▶ Permissions boundary (not set)

3. AWS アカウント（ルートアカウント）の保護

3.1. AWS アカウントへ二段階認証を導入

AWS アカウントでのログインは、AWS アカウント作成時のメールアドレス・パスワードだけでできてしまう。心許ないにもほどがあるので、まずは二段階認証を設定しよう。

3.1.1. IAM のページを開く

3.1.2. 「ルートアカウントの MFA を有効化」を選択して、「MFA の管理」ボタンをクリック

Identity and Access Management へようこそ

IAM ユーザーのサインインリンク:
[https://\[redacted\]signin.aws.amazon.com/console](https://[redacted]signin.aws.amazon.com/console) [カスタマイズ](#) | [リンクのコピー](#)

IAM リソース

ユーザー: 0 ロール: 0
グループ: 0 ID プロバイダ: 0
カスタマー管理ポリシー: 0

セキュリティステータス 5 項目中 1 項目が完了しています。

✓	ルートアクセスキーの削除	▼
⚠	ルートアカウントの MFA を有効化	▲
<p>アカウントのセキュリティを保てるように、AWS ルートアカウントで多要素認証（MFA）を有効化して、別の保護レイヤーを追加します。 詳細はこちら</p> <p>MFA の管理</p>		
⚠	個々の IAM ユーザーの作成	▼
⚠	グループを使用してアクセス許可を割り当て	▼
⚠	IAM パスワードポリシーの適用	▼

3.1.3. 「仮想 MFA デバイス」にチェックが入っていることを確認し、「次のステップ」ボタンをクリック

MFA デバイスの管理

有効にする MFA デバイスタイプを選択します。

☒ 仮想 MFA デバイス

☐ ハードウェア MFA デバイス

サポートされている MFA デバイスの詳細については、「[AWS Multi-Factor Authentication](#)」を参照してください。

キャンセル

次のステップ

3.1.4. 注意書きを読んで、「今後はこのダイアログボックスを表示しない。」にチェックを入れて「次のステップ」ボタンをクリック

MFA デバイスの管理

仮想 MFA デバイスを有効にするには、最初に AWS MFA と互換性のあるアプリケーションをユーザーのスマートフォン、PC、またはその他のデバイスにインストールする必要があります。AWS MFA と互換性のあるアプリケーションのリストは、[こちら](#)を参照してください。アプリケーションがインストールされたら、[次のステップ] をクリックして仮想 MFA を設定します。

☒ 今後はこのダイアログボックスを表示しない。

キャンセル

戻る

次のステップ

3.1.5. Google Authenticatorなどで、QRコードを読み取って、表示された認証コード二つを入力し、「仮想 MFA の有効化」ボタンをクリック

MFA デバイスの管理

仮想 MFA アプリケーションが QR コードのスキャンをサポートしている場合は、スマートフォンのカメラで次の画像をスキャンします。



Google Authenticatorなどで QRコードを読み取る

▶ 手動設定のシークレットキーを表示

アプリケーションを設定したら、下のボックスに 2 つの連続する認証コードを入力し、[仮想 MFA の有効化] をクリックします。

認証コード 1

123456

認証コード 2

987654

キャンセル

戻る

仮想 MFA の有効化

3.1.6. 「完了」ボタンをクリック

MFA デバイスの管理

MFA デバイスは正常に関連付けられました。

完了

4. グループの作成

権限を設定したグループを作成し、ユーザを所属させます。

4.1. IAM のページを開く

<https://console.aws.amazon.com/iam/home>

4.2. 「グループを使用してアクセス許可を割り当て」を選択し、「グループの管理」ボタンをクリック

セキュリティステータス 5 項目中 3 項目が完了しています。

✓	ルートアクセスキーの削除	▼
✓	ルートアカウントの MFA を有効化	▼
✓	個々の IAM ユーザーの作成	▼
⚠	グループを使用してアクセス許可を割り当て	▲

アカウントのアクセス許可の管理と監査を簡略化するため、IAM ユーザーへのアクセス許可の割り当てに IAM グループを使用してください。 [詳細はこちら](#)

グループの管理

⚠ IAM パスワードポリシーの適用 ▼

4.3. 「新しいグループの作成」ボタンをクリック

ダッシュボード

IAM の検索

詳細

グループ

ユーザー

ロール

新しいグループの作成 グループのアクション ▼

フィルター

<input type="checkbox"/>	グループ名 ⇅	ユーザー	イ
レコードが見つかりません。			

4.4. グループ名を入力し、「次のステップ」ボタンをクリック

グループ名の設定

グループ名を指定します。グループ名はいつでも編集できます。

グループ名:
例: Developers または ProjectAlpha
最大 128 文字

キャンセル

次のステップ

4.5. 「AdministratorAccess」ポリシーにチェックをいれて、「次のステップ」ボタンをクリック

ポリシーのアタッチ

アタッチするポリシーを 1 個以上選択してください。グループは、それぞれ 10 個までのポリシーをアタッチできます。

フィルター: ポリシータイプ ▾		フィルター	結果件数: 183		
	ポリシー名 ⇅	アタッチされたエンティティ ⇅	作成時刻 ⇅	編集時刻 ⇅	
<input checked="" type="checkbox"/>	 AdministratorAccess	0	2015-02-07 03:39...	2015-02-07 03...	
<input type="checkbox"/>	 AmazonAPIGatewa...	0	2015-07-10 02:34...	2015-07-10 02...	
<input type="checkbox"/>	 AmazonAPIGatewa...	0	2015-07-10 02:36...	2015-07-10 02...	
<input type="checkbox"/>	 AmazonAPIGatewa...	0	2015-11-12 08:41...	2015-11-12 08...	
<input type="checkbox"/>	 AmazonAppStream...	0	2015-02-07 03:40...	2015-02-07 03...	

キャンセル

戻る

次のステップ

4.6. 内容を確認し、「グループの作成」ボタンをクリック

確認

続行するには、以下の情報を確認し、[グループの作成] をクリックします。

グループ名 nekopunch-group

[グループ名の編集](#)

ポリシー arn:aws:iam::aws:policy/AdministratorAccess

[ポリシーの編集](#)

キャンセル

戻る

グループの作成

4.7. グループ一覧から作成したグループをクリック



4.8. 「グループにユーザーを追加」ボタンをクリック



4.9. 作成したユーザを選択し、「ユーザーの追加」ボタンをクリック

nekopunch-group グループに追加するユーザーを選択



ここで設定している「AdministratorAccess」は、AWS アカウントに次ぐ強力な権限なので常用してはいけません。
AWS に慣れてきたら、適切な範囲の権限設定に変更します。

5. IAM パスワードポリシーの適用

デフォルトの設定では、パスワードポリシーがかなり緩いので、可能な範囲で縛りを入れよう。

5.1. IAM のページを開く

<https://console.aws.amazon.com/iam/home>

5.2. 「IAM パスワードポリシーの適用」を選択し、「パスワードポリシーの管理」ボタンをクリック



5.3. 任意のパスワードポリシーを設定し、「パスワードポリシーの適用」ボタンをクリック

企業単位のセキュリティポリシーを適用します

▼ パスワードポリシー

パスワードポリシーは、IAM ユーザーが設定できるパスワードの種類を定義するルールのセットです。パスワードポリシーの詳細については、「IAM の使用」の「パスワードの管理」を参照してください。

現在、この AWS アカウントにパスワードポリシーはありません。以下のパスワードポリシーを指定します。

パスワードの最小長:

☒ 少なくとも 1 つの大文字が必要 ⓘ
☒ 少なくとも 1 つの小文字が必要 ⓘ
☒ 少なくとも 1 つの数字が必要 ⓘ
☐ 少なくとも 1 つの英数字以外の文字が必要 ⓘ
☒ ユーザーにパスワードの変更を許可 ⓘ
☐ パスワードの失効を許可 ⓘ
パスワードの有効期間 (日数):
☐ パスワードの再利用を禁止 ⓘ
記憶するパスワードの数:
☐ パスワードの有効期限で管理者のリセットが必要 ⓘ

オプションの設定はドキュメントを参照

[https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/
id_credentials_passwords_account-policy.html](https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html)