


2025.12

あなたの**AWS**情報資産は大丈夫…？

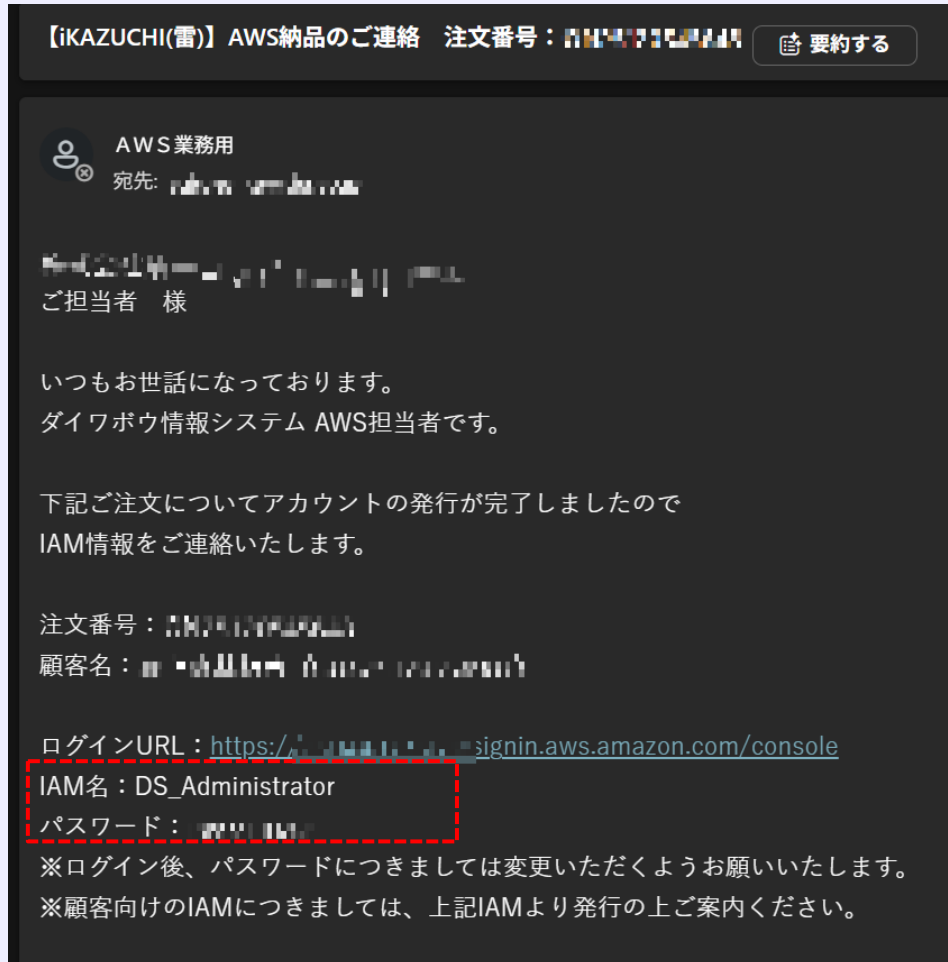
テナント乗っ取り防止対策について





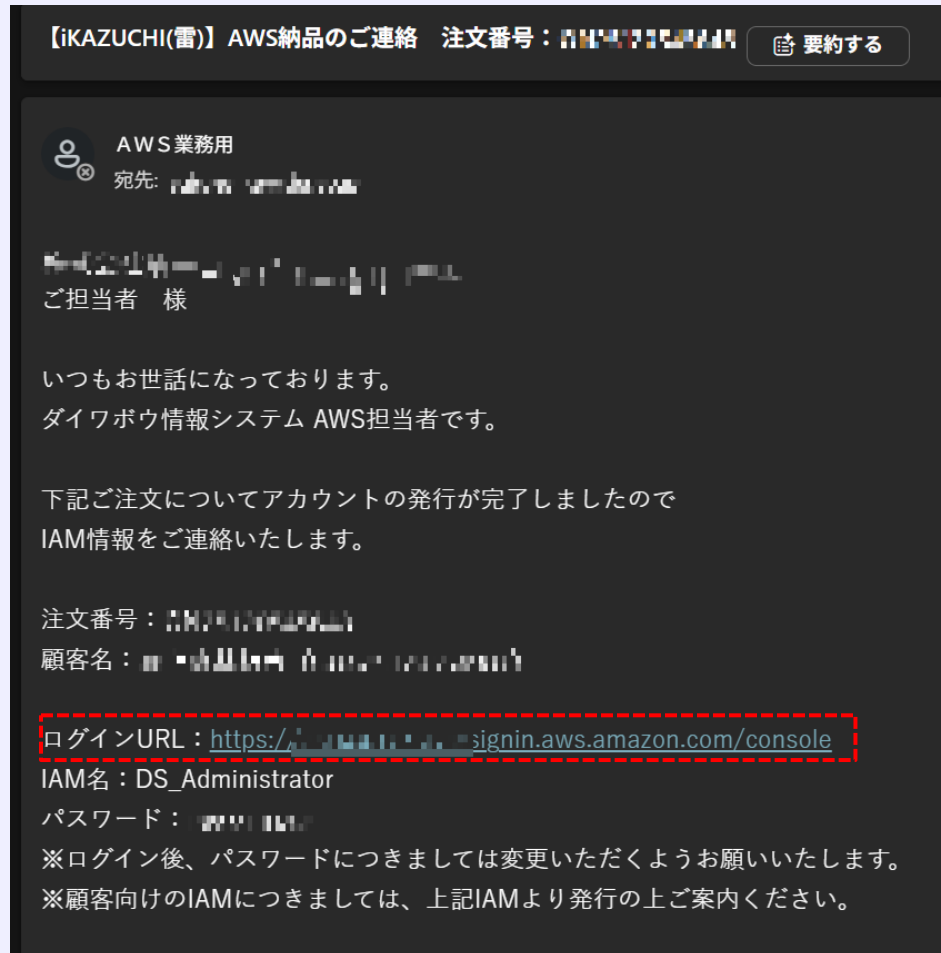
最近、外部からの不正アクセスによる「乗っ取り」被害が報告されています。
「乗っ取り」被害を防止するため、シナリオに沿って、
セキュリティ設定のご対応をお願い致します。

MFA(多要素認証)設定方法



DISからの「AWS納品のご連絡」メールから発行されたアカウントの「IAM名」と「パスワード」をメモします。
※AWSコンソールへのログインに使用します

MFA(多要素認証)設定方法



「ログインURL」を押下し、
AWSコンソールへのログイン画面へ遷移します。

MFA(多要素認証)設定方法

The screenshot shows the AWS IAM User Sign-in page. The AWS logo is at the top. The page title is "IAM ユーザーサインイン ①". There are three red dashed boxes highlighting the input fields: the first box is around the "アカウント ID またはエイリアス (持っていないか?)" field, the second box is around the "IAM ユーザー名" and "パスワード" fields, and the third box is around the "サインイン" button. Below the sign-in button is a link "新しい AWS アカウントを作成". At the bottom, there is a small disclaimer about AWS Customer Agreement and Cookies.

aws

IAM ユーザーサインイン ①

アカウント ID またはエイリアス
(持っていないか?)

☐ このアカウントを記憶する

IAM ユーザー名

パスワード

☐ パスワードを表示 [お困りですか?](#)

サインイン

ルートユーザーの E メールを使用したサインイン

[新しい AWS アカウントを作成](#)

続行すると、AWS [AWS カスタマーアグリーメント](#) サービスまたはその他の契約に同意したものとみなされます [プライバシー通知](#)。このサイトは必須の Cookie を使用しています。詳細については [当社のクッキー通知](#) を、当社をご覧ください。

「アカウント ID」には自動で入力されているためそのまま変更せずに使用します。

「IAM ユーザー名」には先ほどメモした「IAM名」を入力し、「パスワード」には先ほどメモした「パスワード」を入力します。

「サインイン」を押下します。

初回ログインの場合は次ページからの「初期パスワードの変更」を実施
二回目以降で、パスワードの変更が済んでいたら、22ページへ移動し、作業を実施

MFA(多要素認証)設定方法

aws

パスワードのリセット ⓘ

アカウント **XXXXXXXXXX** のパスワードの有効期限が切れているか、リセットが必要です。

続行するには、古いパスワードを確認し、**XXXXXXXXXX** の新しいパスワードを設定してください。(お客様ではありませんか?)

古いパスワード

.....

☐ パスワードを表示

新しいパスワード

.....

新しいパスワードの確認

.....

☐ パスワードを表示 一致

パスワード変更の確認

[別のアカウントにサインインする](#)

「古いパスワード」にはメモした「パスワード」を入力します。

「新しいパスワード」と「新しいパスワードの確認」には新たにログインに使用するパスワードを入力します。

- パスワードの文字数制限：8～128 文字
- パスワードの要件：
大文字、小文字、数字、英数字以外の文字(! @ # \$ % ^ & * () _ + - = [] { } | ')のうち、最低3つの文字タイプの組み合わせ
- AWSアカウント名またはEメールアドレスと同じでないこと
- 有効期限のないパスワード

「パスワード変更の確認」を押下します。

MFA(多要素認証)設定方法

aws

✓ パスワードのリセットに成功しました

パスワードのリセット

IAM ユーザー [masked] パスワードが正常にリセットされました。

サインインを続行

「パスワードのリセットに成功しました」と出たら変更完了

「サインインを続行」を押下します。

MFA(多要素認証)設定方法



MFA(多要素認証)設定方法



「IAM」を選択します。

MFA(多要素認証)設定方法

The screenshot shows the AWS IAM console interface. In the left-hand navigation pane, under the 'IAM の検索' (Search IAM) section, the 'ユーザー' (Users) link is highlighted with a red dashed box. A purple arrow points from this link to a purple callout box on the right side of the image. The main content area displays the 'IAM ダッシュボード' (IAM Dashboard) with various metrics and links.

「ユーザー」を選択します。

最新情報

- Amazon Bedrock が開発の効率化のために API キーを導入. 4 か月前
- AWS サービスリファレンス情報が、サービスアクションのアノテーションのサポートを開始. 5 か月前
- AWS はリソースコントロールポリシー (RCP) のサポートを 2 つの追加サービスに拡大. 5 か月前
- AWS IAM が、すべてのアカウントタイプでルートユーザーに MFA の適用を開始. 5 か月前

※ より多く

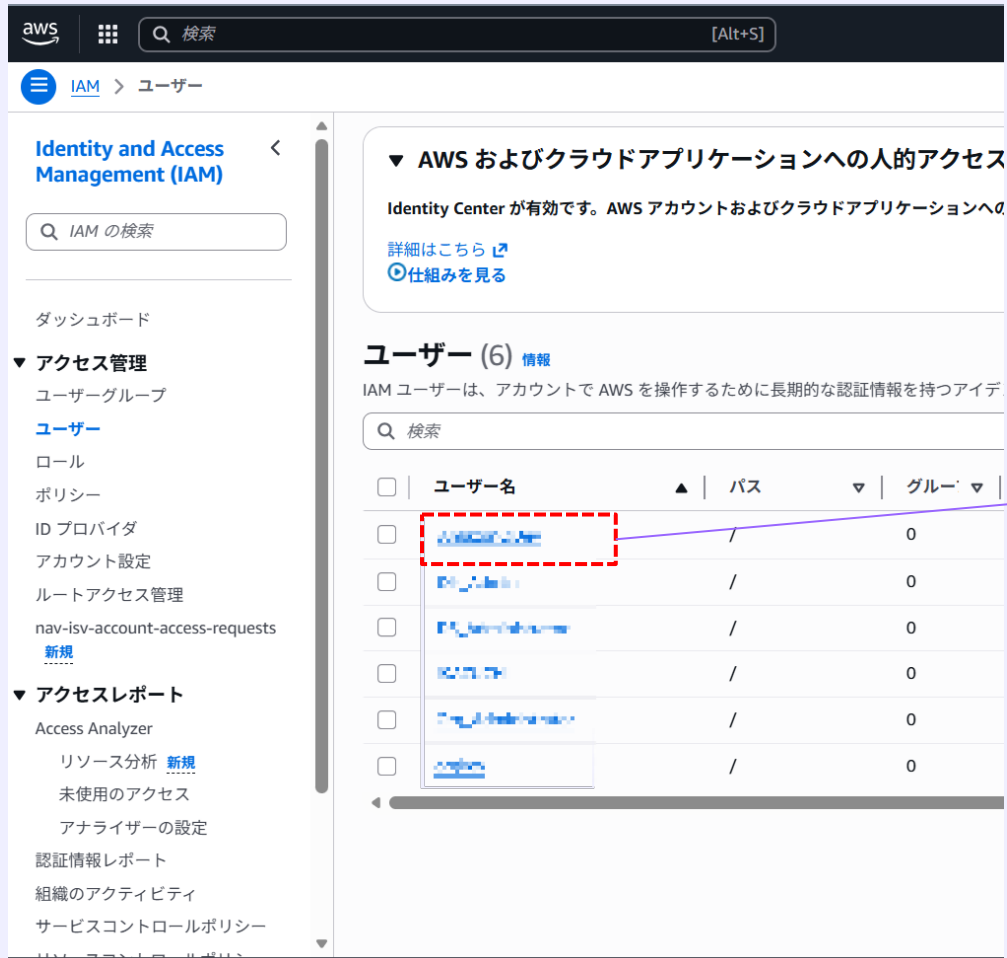
ツール

- ポリシーシミュレータ
- シミュレータは、選択したポリシーを評価し、指定した各アクションの有効な許可を決定します。

追加情報

- IAM でのセキュリティのベストプラクティス
- IAM ドキュメント

MFA(多要素認証)設定方法



The screenshot shows the AWS IAM console interface. On the left, the navigation pane is open, showing 'IAM > ユーザー' (IAM > Users). The main content area displays 'AWS およびクラウドアプリケーションへの人的アクセス' (Human access to AWS and cloud applications) and 'ユーザー (6) 情報' (Users (6) information). Below this, a table lists the users. The first user, 'root@123456789012', is highlighted with a red dashed box. A purple arrow points from this box to a purple callout box on the right.

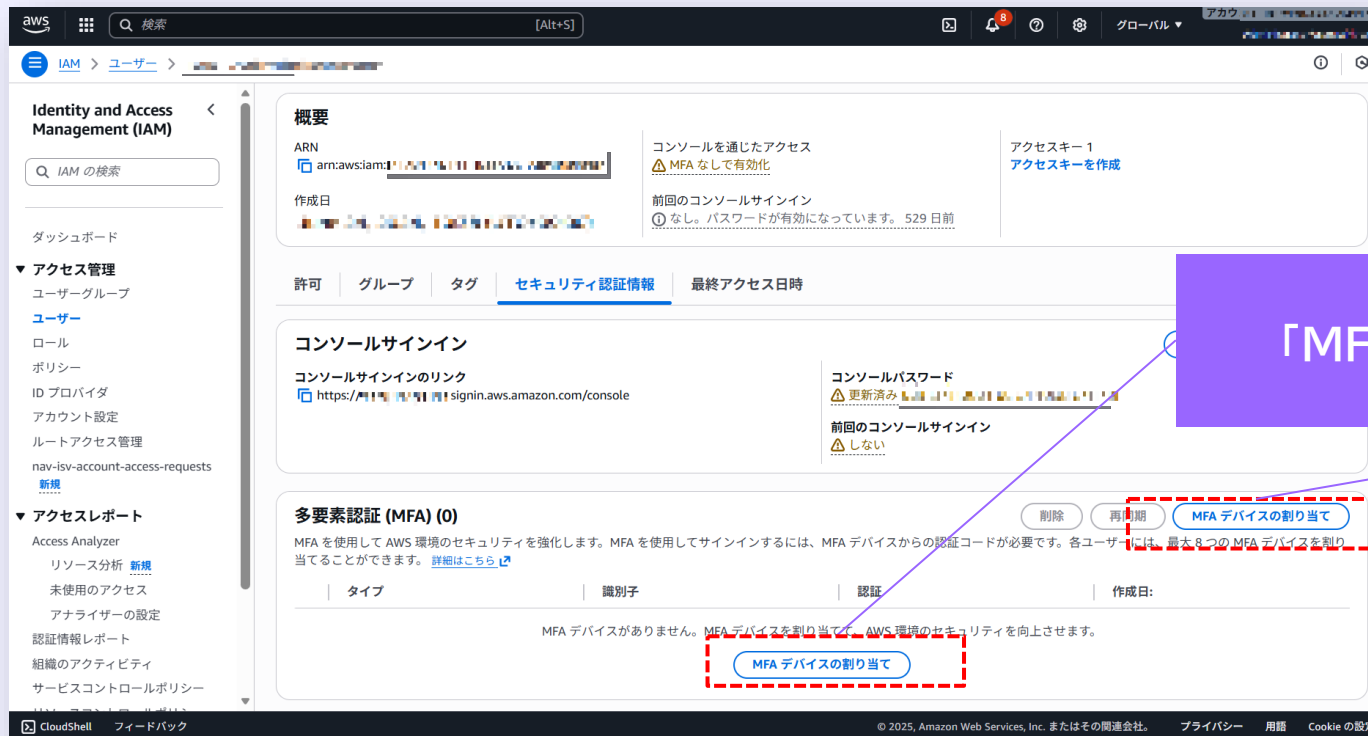
	ユーザー名	パス	グループ
<input type="checkbox"/>	root@123456789012	/	0
<input type="checkbox"/>	...	/	0
<input type="checkbox"/>	...	/	0
<input type="checkbox"/>	...	/	0
<input type="checkbox"/>	...	/	0
<input type="checkbox"/>	...	/	0

MFA認証を設定するIAMユーザーを選択します。

MFA(多要素認証)設定方法



MFA(多要素認証)設定方法



「MFAデバイスの割り当て」を選択します。

MFA(多要素認証)設定方法

MFA デバイスを選択 [Info](#)

MFA device name

デバイス名

この名前は、このデバイスの識別 ARN 内で使用されます。

AWS_MFA

最大 64 文字です。有効な文字: A~Z、a~z、0~9、および +, =, ., @, _ - (ハイフン)

コンソール上でデバイスを識別するための
任意のMFAデバイス名を入力します。

MFA(多要素認証)設定方法

MFA device

デバイスオプション

ユーザー名とパスワードに加えて、このデバイスを使用してアカウントへの認証を行います。



パスキーまたはセキュリティキー

指紋、顔、または画面ロックを使用して認証します。このデバイスでパスキーを作成するか、FIDO2 セキュリティキーなどの別のデバイスを使用してください。



認証アプリケーション

モバイルデバイスまたはコンピュータにインストールされたアプリケーションによって生成されたコードを使用して認証します。



ハードウェア TOTP トークン

ハードウェア TOTP トークンまたは他のハードウェアデバイスによって生成されたコードを使用して認証します。

キャンセル

次へ

登録したいMFA認証の種類を選択します。
※Google AuthenticatorやMicrosoft Authenticatorを選択する場合は「認証アプリケーション」を選択します。

「次へ」を選択します。

MFA(多要素認証)設定方法

デバイスの設定 Info

認証アプリケーション

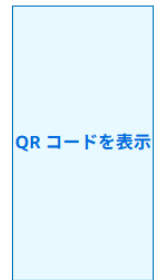
仮想 MFA デバイスはデバイス上で動作するアプリケーションで、QR コードをスキャンすることで設定できます。

1

Google Authenticator、Duo Mobile、Authy アプリなどの互換性のあるアプリケーションを、モバイルデバイスまたはコンピュータにインストールします。

[互換性のあるアプリケーションのリストを表示](#)

2



認証アプリを開いて、このページで **【QRコードを表示】** を選択し、アプリを使用してコードをスキャンします。または、シークレットキーを入力することもできます。

3

2つの連続した MFA コードを以下で入力してください

仮想アプリケーションのコードを以下で入力してください

MFA コード 1

30秒待ってから、2つ目のコードエントリを入力してください。

MFA コード 2

キャンセル

前へ

MFA を追加

「QRコードを表示」を押下し、表示されたQRコードをインストールしている認証アプリケーションで読み取ります。

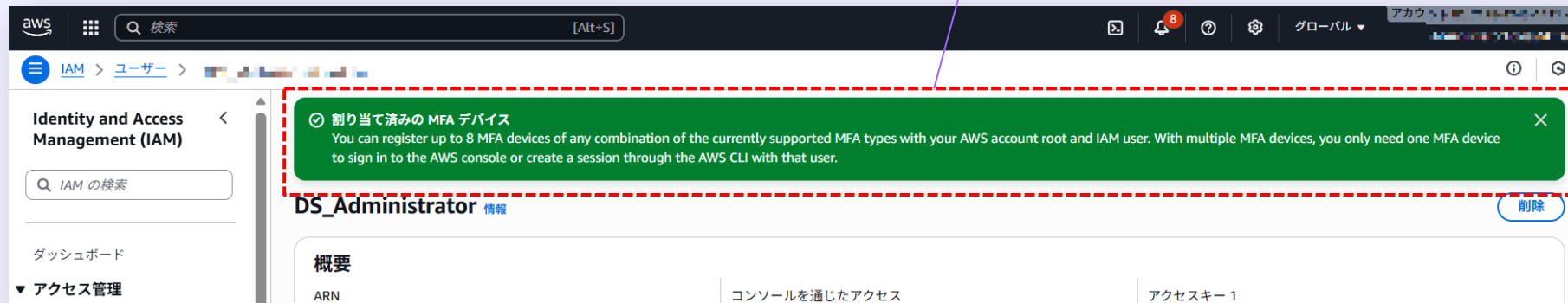
認証アプリケーションで表示された6桁の数字を入力します。

30秒待機し、認証アプリケーションで表示されたもう一つの6桁の数字を入力します。

「MFAを追加」を選択します。

MFA(多要素認証)設定方法

「割り当て済みのMFAデバイス」と表示されたら
設定完了です。



確実にMFA設定を実施し、
AWS情報資産を守りましょう！





ダイワボウ情報システム株式会社