

不安で夜眼れない
AWSアカウント管理者に送る
処方箋という名のハンズオン

Profile

角山 恵介 (Keisuke Kadoyama)

- SI歴 10年
 - エンタープライズ 4年
 - WEB 6年
 - 今年からまたエンタープライズへ
- AWS歴 6年
 - ソリューションアーキテクト
 - Cloud Migration / DevOps / Trouble Shooting



Questions ?

- とりあえずAWSアカウントを取得したが、そのまま使いはじめて大丈夫？
- 最初のシステムが本番稼働しはじめたけど、このまま次々システムを動かして問題はないの？
- なしくずし的にAWSアカウントが増えていってもこのままで大丈夫？
- AWSアカウントの管理をしているけど不安で夜も眠れないんだけど？

Overview

- AWSアカウントを取得して、最初にやっておくべき初期設定をハンズオン形式で学んでもらう
- 設定しない場合のリスクを理解してもらう
- セキュリティだけではなく設定しておくと便利なTipsも
- AWSアカウントの運用方法について学んでもらう
- ⚠️ 今日のハンズオンは1コイン程度の料金が発生します ⚠️

Information

- 会場のWiFi

SSID	GOTANDA-MESSE
Password	123412341234

- 本資料のURL
<http://bit.ly/jaws2017h1>

1. ルートアカウントの保護
2. IAMユーザーとパスワードポリシー
3. 証跡ログの設定
4. 構成管理の設定
5. Trusted Advisorの有効化
6. 請求周りの設定
7. EC2構築時にやること
8. サービス制限緩和
9. 複数のAWSアカウント運用におけるTips

AWSアカウント取得

アカウント周りのハンズオンなので、
すでに本番システムを動作させているAWSアカウントや、
管理者権限を持っていない場合は新規AWSアカウント取得を推奨

こちらを参照

<https://aws.amazon.com/jp/register-flow/>

必要なもの

- アカウント作成用のメールアドレスとパスワード
- 認証用のPINコードを受け取るための電話番号
- クレジットカード

- 1. ルートアカウントの保護**
2. IAMユーザーとパスワードポリシー
3. 証跡ログの設定
4. 構成管理の設定
5. Trusted Advisorの有効化
6. 請求周りの設定
7. EC2構築時にやること
8. サービス制限緩和
9. 複数のAWSアカウント運用におけるTips

1. ルートアカウントの保護

Why / Risk

- AWSのすべての操作が可能な管理者権限を持つアカウントのため、権限の制限がない
- ルートアカウントの情報が漏洩して乗っ取られると何でもされてしまう意図しない課金、既存システムの削除、システムが持つデータや情報の漏洩

Answer

- パスワードを複雑にする
- MFA (他要素認証) の有効化
- APIキーの削除
 - 不要なAPIキーを悪用されると、ログインしなくてもAWSを管理者権限で操作できてしまう
- 普段の操作にはルートアカウントを使用しない

1. ルートアカウントの保護

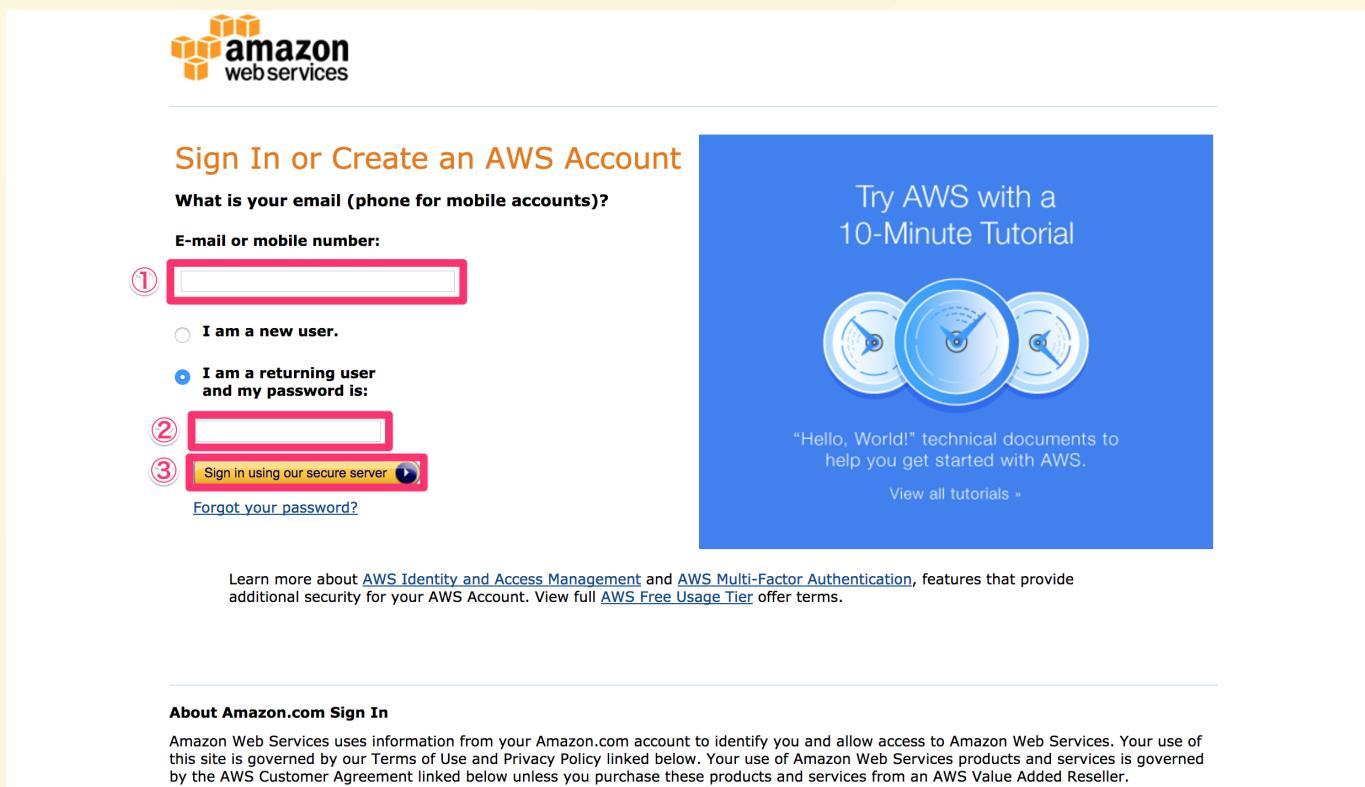
以下のURLアクセスして右上の[サインアップ]をクリック

<https://aws.amazon.com/jp/>



1. ルートアカウントの保護

- ①メールアドレス
- ②パスワードを入力して
- ③[Sign in using our secure server] をクリック



Sign In or Create an AWS Account

What is your email (phone for mobile accounts)?

E-mail or mobile number:

①

I am a new user.

I am a returning user and my password is:

②

③ Sign in using our secure server 

[Forgot your password?](#)

Learn more about [AWS Identity and Access Management](#) and [AWS Multi-Factor Authentication](#), features that provide additional security for your AWS Account. View full [AWS Free Usage Tier](#) offer terms.

About Amazon.com Sign In

Amazon Web Services uses information from your Amazon.com account to identify you and allow access to Amazon Web Services. Your use of this site is governed by our Terms of Use and Privacy Policy linked below. Your use of Amazon Web Services products and services is governed by the AWS Customer Agreement linked below unless you purchase these products and services from an AWS Value Added Reseller.

1. ルートアカウントの保護

AWSサービスの下に表示されているテキストボックスに [IAM] と入力し、表示されたIAMサービスをクリック

AWS サービス

IAM

IAM
ユーザーアクセスと暗号化キーの管理

Get Started

OpsWorks VPC

すべてのサービス

注目の次のステップ

コストの管理

コストと使用量の予算に基づいてリアルタイムの請求アラートを取得 今すぐ開始

ベストプラクティスの習得

AWS Trusted Advisor を使用して、セキュリティ、パフォーマンス、コスト、および可用性のベストプラクティスを得る 今すぐ開始

最新情報

AWS Batch のアナウンス

AWS Batch の一般提供開始。AWS Batch を使用することにより、開発者、科学者、およびエンジニアは、大規模なバッチジョブを簡単に処理することができます。 詳細はこちら

Amazon Lightsail のアナウンス

この新しいサービスを使用して、VPS を AWS で予測可能な低成本で起動および管理できるようになります。 詳細はこちら

1. ルートアカウントの保護

IAM = Identity and Access Management (無料)

「どのユーザがどのAWSリソースへアクセスできるか」を制御する仕組み
AWSのセキュリティの要

The screenshot shows the AWS IAM console's Root Account Protection dashboard. On the left, a sidebar lists navigation options like Groups, Users, Roles, Policies, and Account Settings. The main area displays statistics: 0 users, 0 groups, and 0 roles. Below this, a progress bar indicates 1 item completed out of 5. A list of tasks includes:

- ✓ ルートアクセスキーの削除 (Completed)
- ⚠ ルートアカウントの MFA を有効化 (Pending)
- ⚠ 個々の IAM ユーザーの作成 (Pending)
- ⚠ グループを使用してアクセス許可を割り当て (Pending)
- ⚠ IAM パスワードポリシーの適用 (Pending)

On the right, there's a video player titled "Introduction to AWS IAM" and a "Noteable Features" section.

1. ルートアカウントの保護

一番上の [ルートアクセスキーの削除] でルートアカウントのAPIキーを削除

The screenshot shows the AWS IAM console with the following details:

- Identity and Access Management へようこそ**
- IAM ユーザーのサインインリンク: [https://.signin.aws.amazon.com/console](https://<REDACTED>.signin.aws.amazon.com/console)
- IAM リソース**
 - ユーザー: 0
 - ロール: 1
 - グループ: 0
 - ID プロバイダ: 0
 - カスタマーマネジメントポリシー: 0
- セキュリティステータス**
 - ルートアクセスキーの削除 (checked)
 - 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る
 - IAM パスワードポリシーの適用
- 注目の機能**
 - Introduction to AWS IAM
- 追加情報**
 - IAM ドキュメント
 - Web ID フェデレーションのブレイクダウン
 - Policy Simulator
 - 動画: IAM リリース履歴、および追加のリソース

削除する場合は事前にシステム等で利用していないかよく確認

The screenshot shows the 'AWS Security Credentials' page with the following details:

セキュリティ認証情報

AWS アカウントの認証情報を管理するには、このページを使用します。AWS Identity and Access Management (IAM) ユーザーの認証情報を管理するには、[IAM コンソール](#) を使用します。

AWS 認証情報の種類と、その使用方法の詳細は、「AWS General Reference」の「[AWS Security Credentials](#)」を参照してください。

作成日	削除済み	アクセスキー ID	前回使用したもの	前回使用したリージョン	前回使用したサービス	ステータス	アクション
4月 27 2012		[REDACTED]	該当なし	N/A	N/A	有効	無効化 削除

[新しいアクセスキーの作成](#)

1. ルートアカウントの保護

[ルートアカウントのMFAを有効化] をクリックし、
[MFAの管理] をクリック

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with links like 'ダッシュボード', 'グループ', 'ユーザー', etc. The main area has a heading 'Identity and Access Management へようこそ'. Below it, there's a summary of IAM resources: 'ユーザー: 0', 'ロール: 0', 'グループ: 0', 'ID プロバイダー: 0', and 'カスタマー管理ポリシー: 0'. A progress bar indicates 'セキュリティステータス' with '5項目中 1項目が完了しています。'. A section titled 'ルートアカウントの MFA を有効化' is highlighted with a red box and a red arrow pointing to the 'MFA の管理' button. To the right, there's a '注目の機能' sidebar with a video thumbnail for 'Introduction to AWS IAM'.

1. ルートアカウントの保護

MFAとは？

MFA = Multi Factor Authentication

要はパスワード + αによる2段階認証 (6桁の認証コード)

仮想MFAデバイス

- Android / iOSアプリ: Authenticator / Authy
- Chrome Extension: [Authenticator](#)
- Firefox Extension: [Open Two-Factor Authenticator](#)

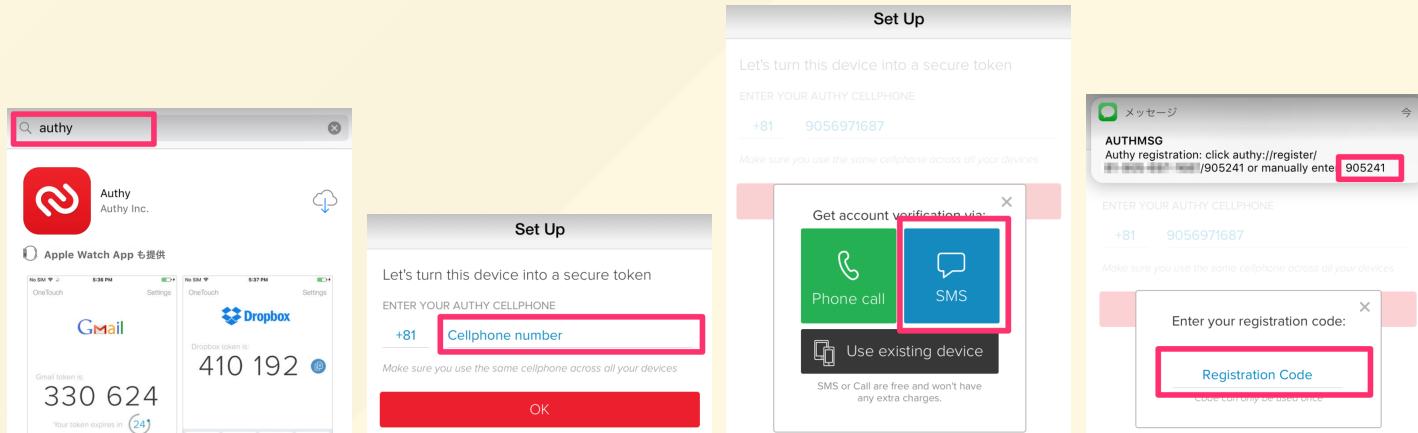
ハードウェアMFAデバイス



1. ルートアカウントの保護

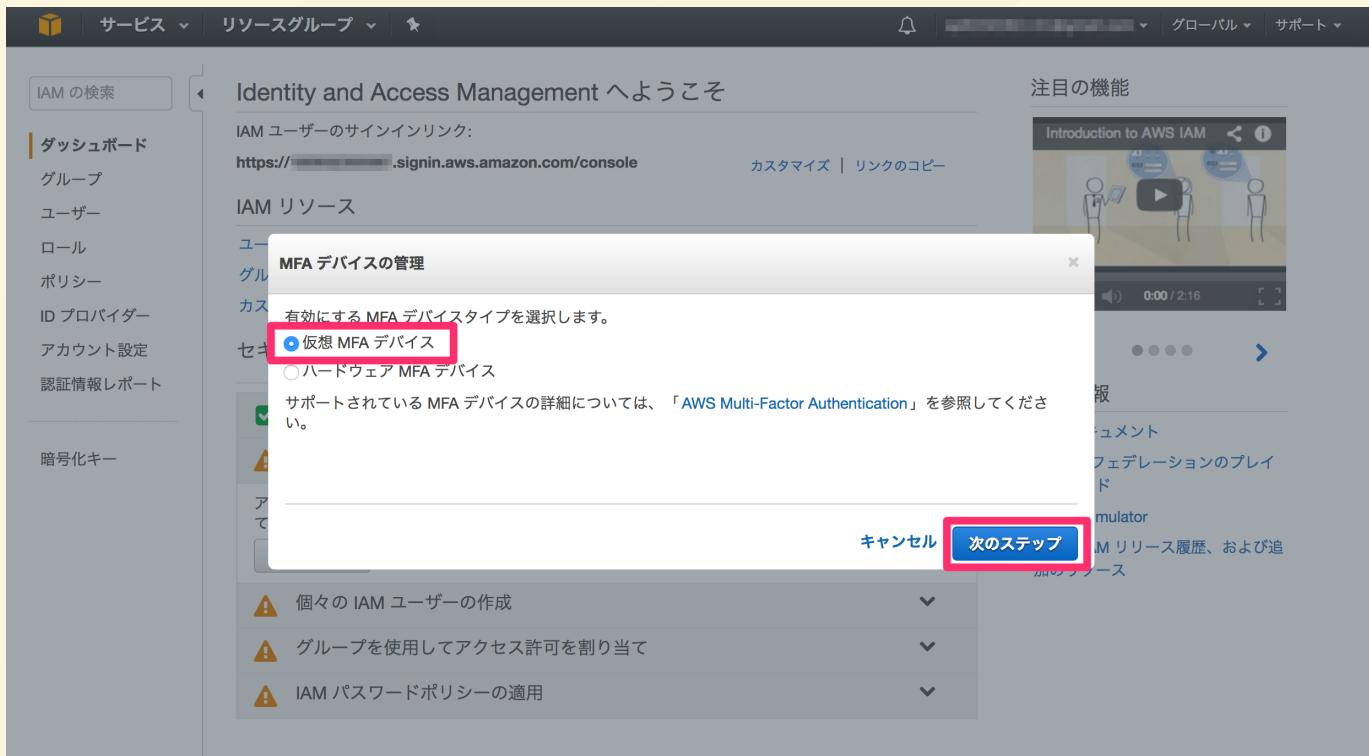
仮想MFAデバイスをお持ちでない方

Android / iOSスマートフォンをお持ちの方はアプリのストアより「Authy」と検索してアプリをダウンロード
起動してSMSで電話番号の認証をすませる



1. ルートアカウントの保護

[仮想MFAデバイス] を選択する

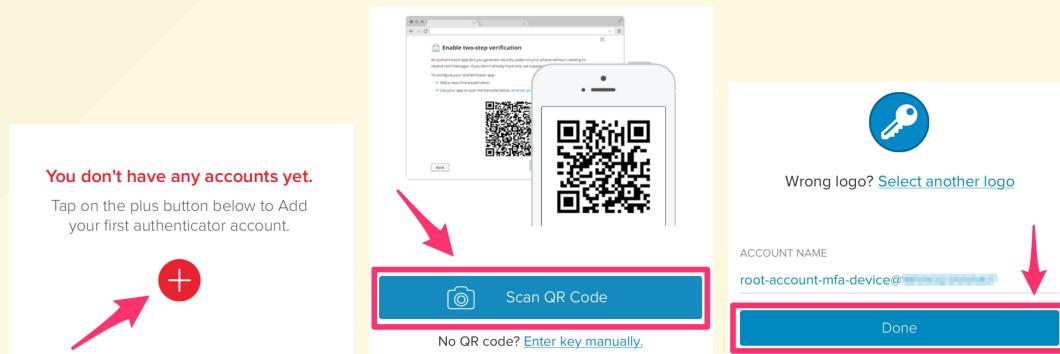


1. ルートアカウントの保護

QRコードが表示されるので、仮想MFAデバイスのアプリからスキャンする



Authyをお使いの方は [+] ボタンから [Scan QR Code] をタップして表示されているQRコードをスキャン

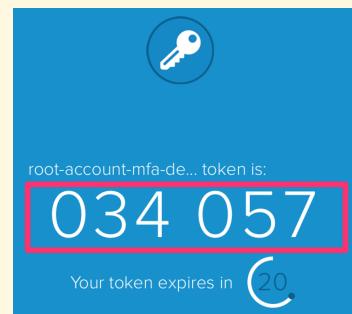


1. ルートアカウントの保護

仮想MFAデバイスに表示される認証コードを2つ入力して有効化
※2つの認証コードは異なるコードであること



Authyをお使いの方は以下の画面に表示される6桁の認証コードを入力



1. ルートアカウントの保護

無事ルートアカウントのMFAが有効になりました

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with links like 'ダッシュボード', 'グループ', 'ユーザー', 'ロール', 'ポリシー', etc. A red arrow points from the bottom-left towards the 'Root Account Protection' section. The main area has a heading 'Identity and Access Management へようこそ'. Below it, there's a link to the sign-in console and some statistics: 'ユーザー: 0', 'ロール: 0', 'グループ: 0', 'ID プロバイダ: 0', and 'カスタマー管理ポリシー: 0'. A progress bar indicates '5 項目中 2 項目が完了しています。'. The 'Root Account Protection' section contains several items: 'ルートアクセスキーの削除' (checked), 'ルートアカウントの MFA を有効化' (checked, highlighted with a red box), '個々の IAM ユーザーの作成' (warning icon), 'グループを使用してアクセス許可を割り当て' (warning icon), and 'IAM パスワードポリシーの適用' (warning icon). To the right, there's a '注目の機能' sidebar with a video thumbnail titled 'Introduction to AWS IAM'.

1. ルートアカウントの保護

確認のため一度サインアウトし、

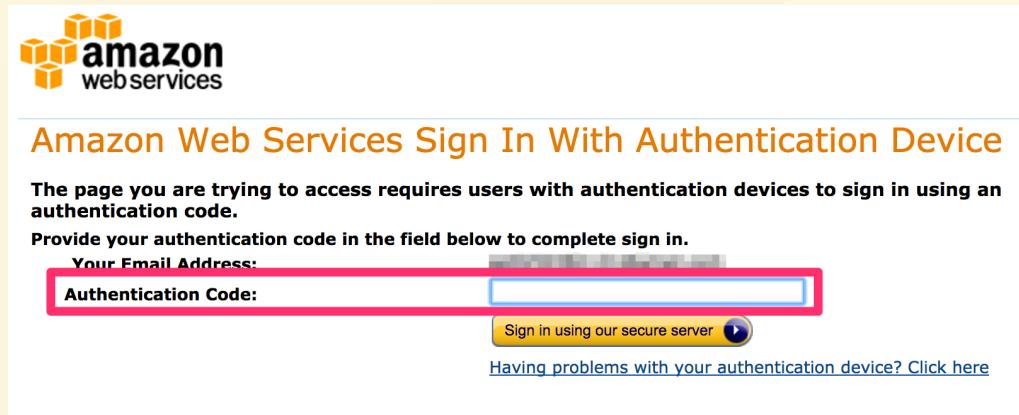


もう一度サインイン

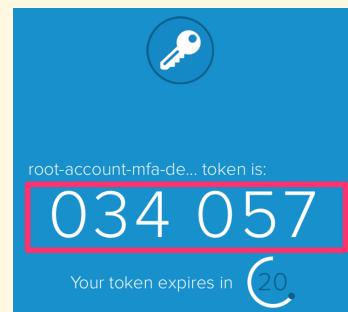


1. ルートアカウントの保護

メールアドレス、パスワードを入力後、登録した仮想MFAデバイスの認証コードが求められる



Authyをお使いの方は以下の画面に表示される6桁の認証コードを入力



1. ルートアカウントの保護

Why / Risk

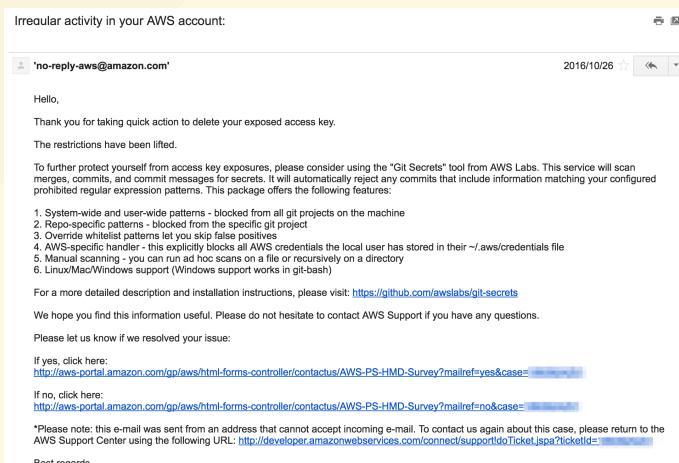
- AWSのすべての操作が可能な管理者権限を持つアカウントのため、権限の制限がない
- ルートアカウントの情報が漏洩して乗っ取られると何でもされてしまう意図しない課金、既存システムの削除、システムが持つデータや情報の漏洩

Answer

- パスワードを複雑にする
- MFA (他要素認証) の有効化
- APIキーの削除
 - 不要なAPIキーを悪用されると、ログインしなくてもAWSをAdmin権限で操作できてしまう
- 普段の操作にはルートアカウントを使用しない

Break

- APIキーは、不要なAPIキーの作成や、不適切な権限が付与されているかだけでなく、誤ってグローバルに公開されていないか要チェック
 - Amazonが公開しているgit-secretsというツールで、プログラムのgitリポジトリにAPIキーをcommitしていないかチェック
<https://github.com/awslabs/git-secrets>
 - もしグローバル公開されている場合、Amazonから警告メールが来ることも
※AWSアカウントへのアクセスが強制停止されることもあります



1. ルートアカウントの保護
2. IAMユーザーとパスワードポリシー
3. 証跡ログの設定
4. 構成管理の設定
5. Trusted Advisorの有効化
6. 請求周りの設定
7. EC2構築時にやること
8. サービス制限緩和
9. 複数のAWSアカウント運用におけるTips

2. IAMユーザとパスワードポリシー

Why / Risk

- 管理者権限を持ったルートアカウントの代わりに他のアカウントが必要
- AWSアカウントが漏洩した場合と同じく、IAMユーザーの権限で許容されている操作を何でもされてしまう
 - TBD: わかりづらい
- アカウントを共有していると誰が何をしたか証跡が追いづらい

Answer

- IAMユーザーと、権限を定義したIAMポリシーを作成
 - IAMユーザーは共有厳禁、人単位で作成
 - あわせてIAMグループによる権限管理をおすすめ
- IAMユーザーでもMFAを有効化する
- パスワードポリシーを設定して簡単なパスワードを設定できないように

2. IAMユーザとパスワードポリシー

IAMの画面を表示し、末尾の [IAMパスワードポリシーの適用] から [パスワードポリシーの管理] をクリック

The screenshot shows the AWS IAM Dashboard. On the left, a sidebar lists navigation options: IAM の検索, ダッシュボード, グループ, 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, and 暗号化キー. The 'ダッシュボード' option is selected. The main content area has a title 'Identity and Access Management へようこそ' and a sub-section 'IAM ユーザーのサインインリンク' with a URL. Below this are sections for 'IAM リソース' (User: 0, Group: 0, Role: 0, ID Provider: 0) and 'カスタマー管理ポリシー: 0'. A progress bar indicates 'セキュリティステータス' with '5 項目中 2 項目が完了しています'.

The 'IAM パスワードポリシーの適用' section is highlighted with a red box. It contains a note: 'パスワードポリシーを使用して、強力なパスワードの作成とそれらのパスワードの定期的なローテーションを IAM ユーザーに要求します。 詳細は[こちら](#)' and a button labeled 'パスワードポリシーの管理'.

To the right, there's a '注目の機能' section with a video thumbnail titled 'Introduction to AWS IAM' and a '追加情報' section with links to 'IAM ドキュメント', 'Web ID フェデレーションのプレイグラウンド', 'Policy Simulator', and '動画、IAM リリース履歴、および追加のリソース'.

2. IAMユーザとパスワードポリシー

パスワードポリシーを設定して [パスワードポリシーの適用] をクリック

The screenshot shows the AWS IAM service console with the 'Password Policy' section selected. A red box highlights the configuration options for a new password policy:

- Minimum password length: 8
- Checkboxes for required character types:
 - At least one uppercase letter
 - At least one lowercase letter
 - At least one digit
 - At least one non-alphanumeric character
- Checkboxes for user actions:
 - Allow password change
 - Allow password expiration (unchecked)
 - Prohibit password reuse (unchecked)
 - Limit password history (unchecked)
 - Require password reset by administrator (unchecked)
- Fields for password validity period and history length (both are empty)

At the bottom, there are two buttons: a blue button labeled 'Password Policyの適用' (Apply) and a red button labeled 'Password Policyの削除' (Delete).

2. IAMユーザとパスワードポリシー

左メニューから [ユーザー] をクリック



[ユーザーを追加] をクリック



2. IAMユーザとパスワードポリシー

ユーザーを追加

1 詳細 2 アクセス権限 3 確認 4 完了

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 ②
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 ③
 パスワードハッシュ

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 ④

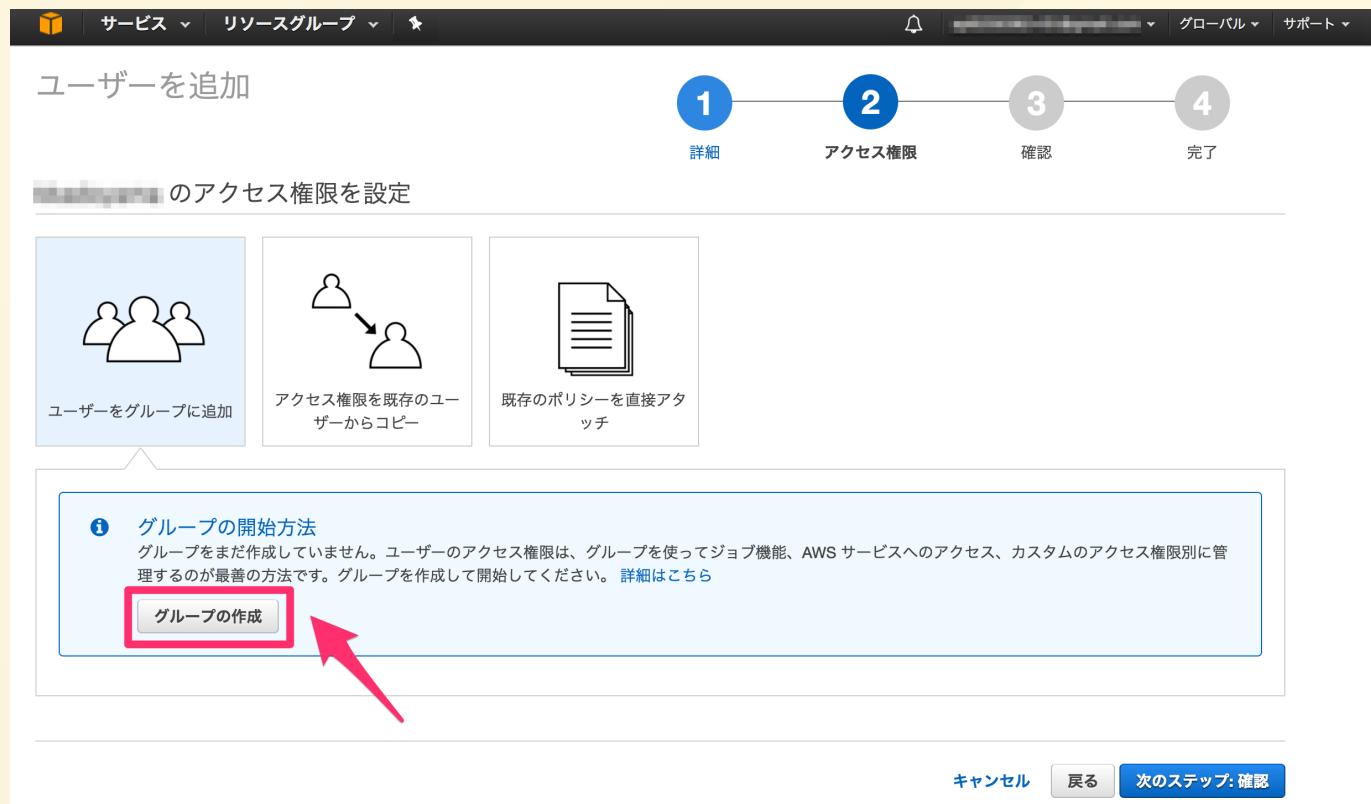
⑤

* 必須

キャンセル 次のステップ: アクセス権限

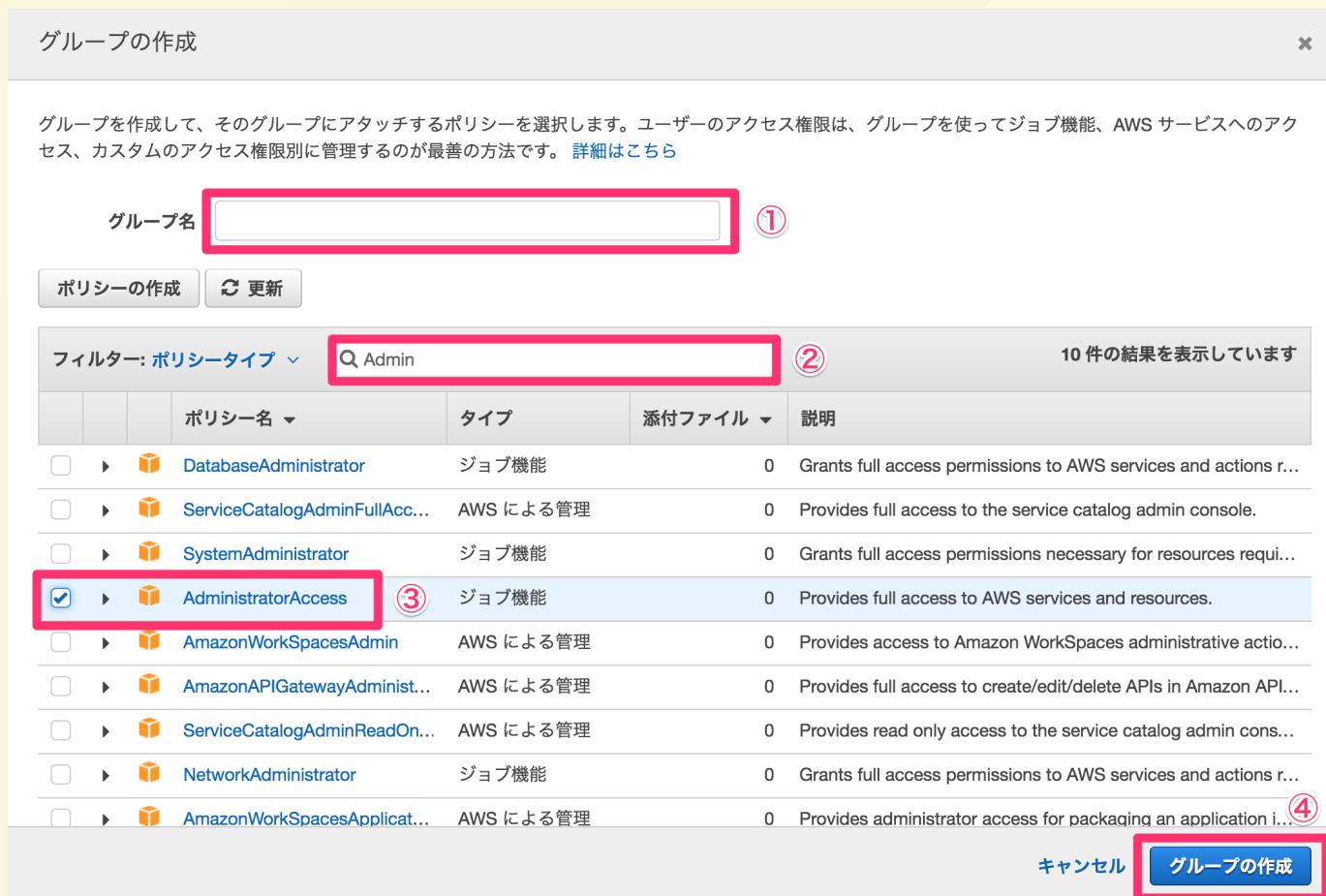
2. IAMユーザとパスワードポリシー

IAMグループを使って権限制御を行うため [グループの作成] をクリック



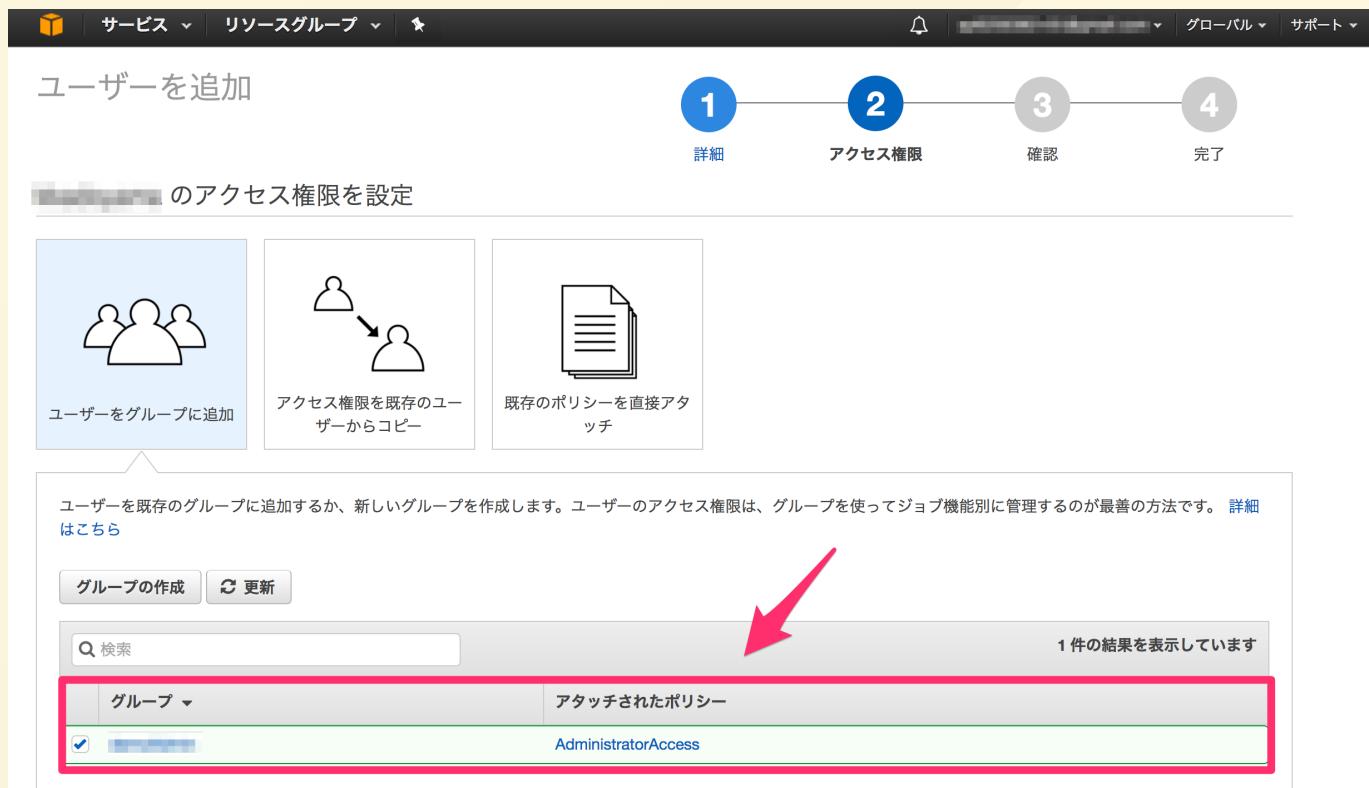
2. IAMユーザとパスワードポリシー

グループ名を入力し、[AdministratorAccess] ポリシーを選択して作成する



2. IAMユーザとパスワードポリシー

作成したIAMグループにチェックが入っていることを確認し、次へ



2. IAMユーザとパスワードポリシー

内容を確認し、[ユーザーの作成] をクリック



2. IAMユーザとパスワードポリシー

- ①サインイン用のURL、②パスワードをメモするか、
③Eメールでログイン情報を送信する

ユーザーを追加

1 詳細 2 アクセス権限 3 確認 4 完了

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 [https://\[REDACTED\].signin.aws.amazon.com/console](https://[REDACTED].signin.aws.amazon.com/console) でサインインできます

①

.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
▶	■■■■■	② ***** 表示	③ E メールの送信 ⏎

閉じる

2. IAMユーザとパスワードポリシー

IAMユーザーもMFAを有効にする

左メニューの [ユーザー] から作成したIAMユーザーの名前をクリック



The screenshot shows the AWS IAM service interface. The left sidebar has a 'ユーザー' (User) item highlighted with a red box. The main content area displays a table with one result. The table columns are: ユーザー名 (User Name), グループ (Groups), パスワード (Password), 最終サインイン (Last Sign-in), アクセスキー (Access Key), and 作成時刻 (Creation Date). The single row shows 'testuser' in the User Name column, and the Creation Date is '2017-03-05 18:12 UTC+0900'. A red box highlights the 'testuser' entry in the table.

ユーザー名	グループ	パスワード	最終サインイン	アクセスキー	作成時刻
testuser	1	該当なし	なし	2017-03-05 18:12 UTC+0900	X

2. IAMユーザとパスワードポリシー

- ① [認証情報] タブを選択し、
- ② [MFAデバイスの割り当て] をクリック

The screenshot shows the AWS IAM User Details page for a user named "kkadoyama". The left sidebar has a "User" section selected. The main content area shows the user's ARN, password status, and creation timestamp. Below this, there are four tabs: "Access Permissions", "Groups (1)", "Authentication" (which is highlighted with a red box and has a circled "①" above it), and "Access Advisor". Under the "Authentication" tab, there are sections for "Sign-in Authentication Information" and "MFA Device Assignment". The "MFA Device Assignment" section is highlighted with a red box and has a circled "②" above it.

先ほどのルートアカウントの手順と同様の手順で、
仮想MFAデバイスを有効にする

2. IAMユーザとパスワードポリシー

ここまでできたらルートアカウントの使用をやめるためサインアウトし、



IAMユーザーのサインイン用URLにアクセスする

<https://xxxxxxxxxxxx.signin.aws.amazon.com>

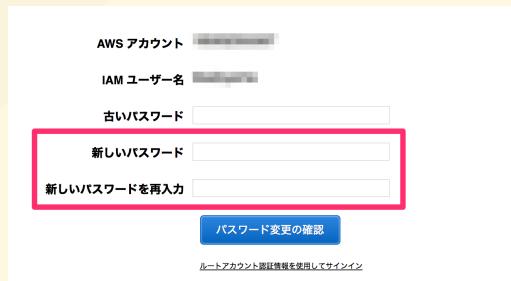


2. IAMユーザとパスワードポリシー

パスワードを入力するとMFAコードを求められ、



サインインに成功すると強制的に新しいパスワードの設定を求められる



2. IAMユーザとパスワードポリシー

ここまで出来たらセキュリティステータスを確認

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

The screenshot shows the AWS Identity and Access Management (IAM) console home page. The left sidebar includes links for IAM search, Dashboard, Groups, Users, Roles, Policies, ID Providers, Account Settings, and Authentication Reports. The main content area displays the following information:

- 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) (with "カスタマイズ" and "リンクのコピー" options)
- IAM リソース:**
 - ユーザー: 1 (ロール: 0)
 - グループ: 1 (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 5 項目が完了しています。
 - 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
 - IAM パスワードポリシーの適用
 - アクセスキーのローテーション

2. IAMユーザとパスワードポリシー

Why / Risk

- 管理者権限を持ったルートアカウントの代わりに他のアカウントが必要
- AWSアカウントが漏洩した場合と同じく、IAMユーザーの権限で許容されている操作を何でもされてしまう
- アカウントを共有していると誰が何をしたか証跡が追いづらい

Answer

- IAMユーザーと、権限を定義したIAMポリシーを作成
 - IAMユーザーは共有厳禁、人単位で作成
 - あわせてIAMグループによる管理をおすすめ
- IAMユーザーでもMFAを有効化する
- パスワードポリシーを設定して簡単なパスワードを設定できないように

Break

- IAMユーザーのサインイン用URL(アカウント番号)は任意の文字列に変更することが可能



- IAMユーザー本人にMFAを設定してもらう場合はこちらの公式チュートリアルを参考にIAMポリシーを設定する

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/tutorial_users-self-manage-mfa-and-creds.html

1. ルートアカウントの保護
2. IAMユーザーとパスワードポリシー
- 3. 証跡ログの設定**
4. 構成管理の設定
5. Trusted Advisorの有効化
6. 請求周りの設定
7. EC2構築時にやること
8. サービス制限緩和
9. 複数のAWSアカウント運用におけるTips

3. 証跡ログの設定

Why / Risk

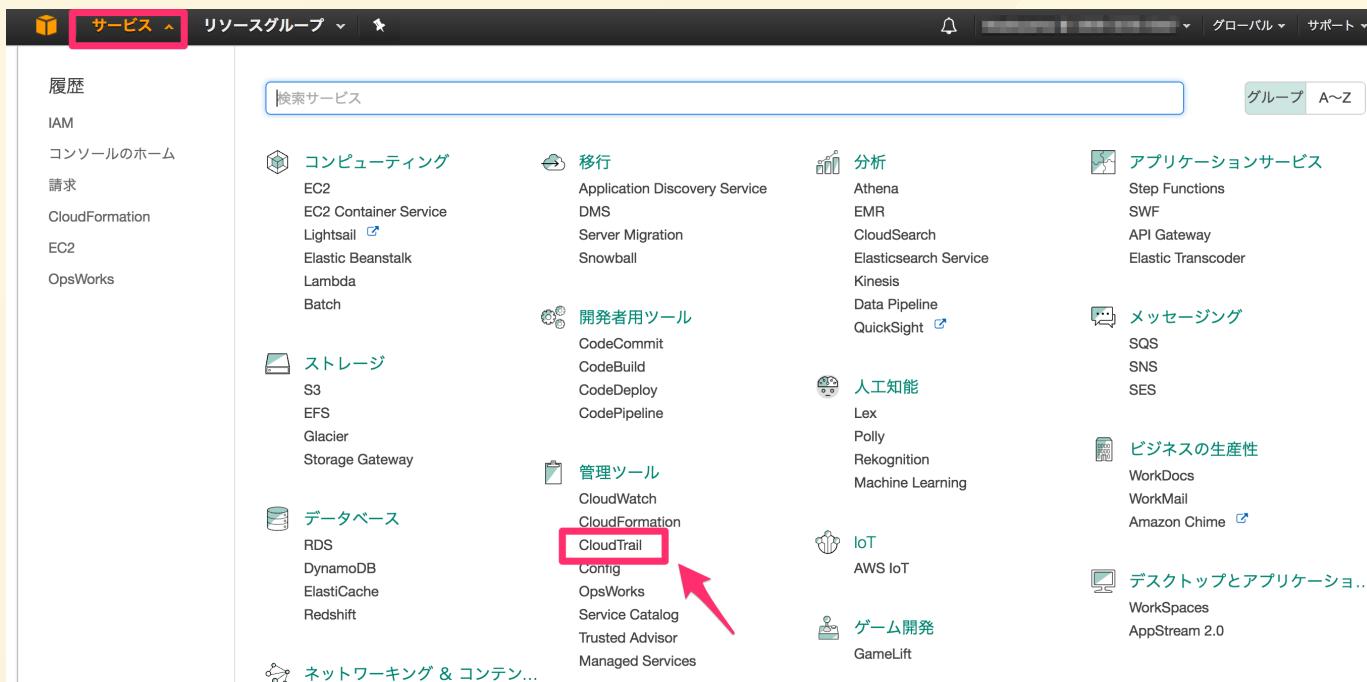
- どの操作を誰が行ったのかわからない
- 悪意のある内部犯行があった場合に犯人がわからない
- 高額なリソースをこっそり使われても誰が利用したのかわからない

Answer

- CloudTrailの有効化
 - 管理コンソールやAPIによる操作を証跡ログとして記録する
 - CloudTrailは最初の1つだけなら無料
 - ログを保存するS3のストレージ料金が別途発生
- 利用していないリージョンでも不正利用を記録できるように有効に
- 制限ではなく、あくまで抑止力

3. 証跡ログの設定

左上の [サービス] から [CloudTrail] をクリック



3. 証跡ログの設定

右上のリージョン選択で [東京] リージョンを選択
[今すぐ始める] をクリック



3. 証跡ログの設定

- ①証跡名は好きな名前を、
- ②認証情報は全てのリージョンに適用する、
- ③④証跡ログを保存するS3バケットは新規で作成

The screenshot shows the 'CloudTrail の有効化' (Enable CloudTrail) page. It includes a note about CloudTrail's pricing, a title, and four configuration fields, each marked with a circled number from 1 to 4. A red box highlights the '有効化' (Enable) button at the bottom right.

CloudTrail の料金はどのように設定されているか？
CloudTrail のイベント処理は 1 つまでの証跡による処理は無料です。追加の証跡によるイベント処理には料金が発生します。詳細について
は、次を参照してください。[料金表](#)。

CloudTrail の有効化

証跡名* ①

証跡情報を全てのリージョンに
適用 ② はい いいえ

新しい S3 バケットを作成しま
すか ③ はい いいえ

S3 バケット* ④

[詳細 »](#)

* 必須のフィールド

有効化

3. 証跡ログの設定

設定完了

The screenshot shows the AWS CloudTrail console with the 'Trail Information' page. The top navigation bar includes 'サービス' (Services), 'リソースグループ' (Resource Groups), and a star icon. The main content area has a title '証跡情報' (Trail Information) and a note about CloudTrail pricing. A button '新規の証跡情報の追加' (Add new trail information) is visible. Below is a table with columns: 名前 (Name), リージョン (Region), S3 バケット (S3 Bucket), ログファイルのプレフィックス (Log file prefix), [CloudWatch Logs] ロググループ (CloudWatch Logs Log group), and ログのステータス (Log status). One row is listed: 'すべて' (All) under Name, 'すべて' (All) under Region, 'awslogs' under S3 Bucket, 'awslogs' under Log file prefix, '[CloudWatch Logs] ロググループ' under Log group, and 'オン' (On) with the timestamp '03-05-2017, 9:35 pm'.

S3に出力されたログ

The screenshot shows the AWS Services Catalog search results for 'CloudTrail'. The search bar at the top contains the query 'CloudTrail'. The results are categorized into several groups: 'コンピューティング' (Computing) including EC2, EC2 Container Service, Lightsail, Elastic Beanstalk, Lambda, and Batch; 'ストレージ' (Storage) including S3, EFS, Glacier, and Storage Gateway; '移行' (Migration) including Application Discovery Service, DMS, Server Migration, and Snowball; '開発者用ツール' (Developer Tools) including CodeCommit, CodeBuild, CodeDeploy, and CodePipeline; '分析' (Analytics) including Athena, EMR, CloudSearch, Elasticsearch Service, Kinesis, Data Pipeline, and QuickSight; '人工知能' (Machine Learning) including Lex, Polly, Rekognition, and Machine Learning; 'アプリケーションサービス' (Application Services) including Step Functions, SWF, API Gateway, and Elastic Transcoder; 'メッセージング' (Messaging) including SQS, SNS, and SES; and 'ビジネスの生産性' (Business Productivity) including WorkDocs. The 'S3' service is highlighted with a red box.

3. 証跡ログの設定

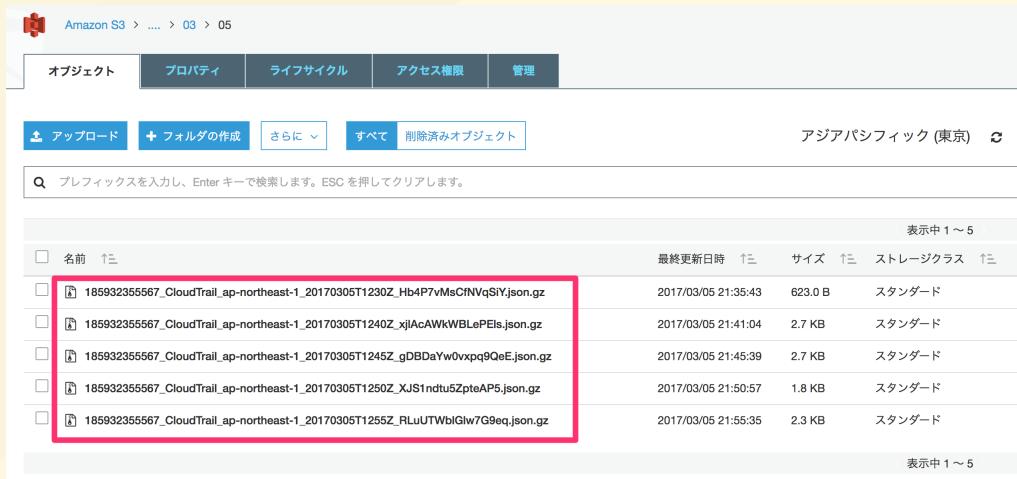
CloudTrailの証跡ログが出力されているS3バケット



The screenshot shows the Amazon S3 console with a single bucket listed:

パケット名	リージョン	作成日
cloudtrail-ap-northeast-1	アジアパシフィック (東京)	2017/03/05 21:33:35

JSON形式で圧縮して保存されている



The screenshot shows the object details for a CloudTrail log file in the Amazon S3 console. The file path is `03/05/185932355567_CloudTrail_ap-northeast-1_20170305T1230Z_Hb4P7vMsCrNVqSiY.json.gz`. The file content is displayed as compressed JSON.

最終更新日時	サイズ	ストレージクラス
2017/03/05 21:35:43	623.0 B	スタンダード
2017/03/05 21:41:04	2.7 KB	スタンダード
2017/03/05 21:45:39	2.7 KB	スタンダード
2017/03/05 21:50:57	1.8 KB	スタンダード
2017/03/05 21:55:35	2.3 KB	スタンダード

3. 証跡ログの設定

Why / Risk

- どの操作を誰が行ったのかわからない
- 悪意のある内部犯行があった場合に犯人がわからない
- 高額なリソースをこっそり使われても誰が利用したのかわからない

Answer

- CloudTrailの有効化
 - 管理コンソールやAPIによる操作を証跡ログとして記録する
 - CloudTrailは最初の1つだけなら無料
 - ログを保存するS3のストレージ料金が別途発生
- 利用していないリージョンでも不正利用を記録するできるように有効に
- 制限ではなく、あくまで抑止力

Break

- S3に保存されるログは自動で暗号化される
 - KMSというAWSのサービスと連携させることでユーザ独自の秘密鍵で暗号化させることができる
- CloudWatch LogsやSNSなどAWSの他サービスと連携させることで、ただログを残すだけでなく、「特定のリソースが削除された」、「ルートアカウントでログインが発生した」など特定のイベントを元にメール通知などが可能
- 証跡ログはJSON形式で保存されるため、他のログ可視化サービスと連携させることでもっと見やすく管理することが可能
 - Splunk
 - Graylog
 - CloudCheckr
 - DataDog
 - etc...

<https://aws.amazon.com/jp/cloudtrail/partners/>

1. ルートアカウントの保護
2. IAMユーザーとパスワードポリシー
3. 証跡ログの設定
- 4. 構成管理の設定**
5. Trusted Advisorの有効化
6. 請求周りの設定
7. EC2構築時にやること
8. サービス制限緩和
9. 複数のAWSアカウント運用におけるTips

4. 構成管理の設定

Why / Risk

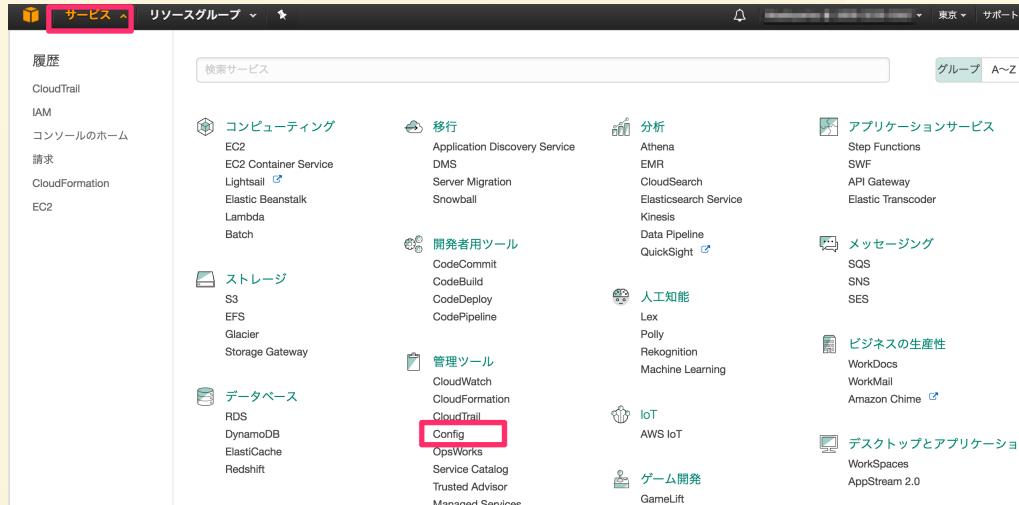
- いつ誰が何をしたか、はCloudTrailの証跡ログから追えるが、そのときAWSのリソースがどういう状態だったかわからない
 - 一応証跡ログを順番に追っていけば再現できなくはない... 😅
- 昨年の年末セール対応ってサーバ何台用意してましたっけ?
 - ドキュメントには20台ってあるけど、当日増やした気が...

Answer

- AWS Configの有効化
 - AWSリソースの状態や、各リソースのRelationship (関係) を記録
 - AWS Configは記録されるごとに料金が発生
 - ログを保存するS3ストレージ料金が別途発生
 - TBD: ここいる？

4. 構成管理の設定

左上の [サービス] から [Config] をクリック



[Get started] をクリック



4. 構成管理の設定

- ①[Include global resource] にチェック
- ②構成管理ログを保存するS3バケットは新規で作成

The screenshot shows the 'Set up AWS Config' wizard at Step 1: Settings. The page title is 'Settings'. It instructs the user to specify AWS resources for recording, an S3 bucket for files, and an SNS topic for notifications. It notes that AWS Config records changes for all supported resources by default, and users can also choose to record changes for supported global resources.

Resource types to record:

- All resources: Record all resources supported in this region (1)
- Include global resources (e.g., AWS IAM resources): (1)

Amazon S3 bucket*

Your bucket receives configuration history and configuration snapshot files, which contain details for the resources that AWS Config records.

Create a bucket (2)

Choose a bucket from your account

Choose a bucket from another account

Bucket name*: config-bucket-[REDACTED] / Prefix (optional) / AWSLogs/[REDACTED]/Config/ap-northeast-1

4. 構成管理の設定

- ③SNS Topicを設定することで構成に変化があった際に通知できる
④Config roleはAWS Configが利用するIAMロール(権限)の設定
いずれもデフォルト値のまま [Next]

Step 3: Review

Amazon SNS topic

Stream configuration changes and notifications to an Amazon SNS topic.

Create a topic

Choose a topic from your account

Choose a topic from another account ⓘ

Topic name* config-topic

AWS Config role*

Grant AWS Config read-only access to your AWS resources so that it can record configuration information, and grant it permission to send this information to Amazon S3 and Amazon SNS.

Create a role

Choose a role from your account

Role name* config-role-ap-northeast-1

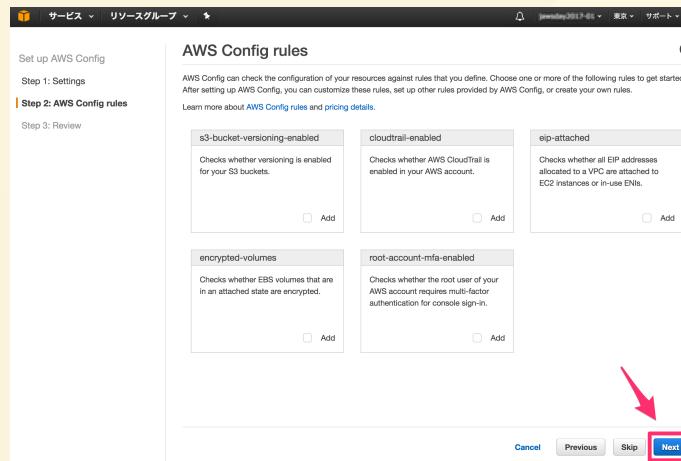
* Required

Cancel

Next

4. 構成管理の設定

AWS Configは構成管理の記録だけでなく、特定のルールに沿った設定が行われているかチェックが可能
今回はとくにチェックを入れず [Next]



自分たちの運用ルールに沿ったルールを設定 (カスタムルールの作成も可能)

- EBSは必ず暗号化する
- S3は必ずバージョニングを有効にする
- IAMユーザーは必ずMFAを有効にする
- etc...

4. 構成管理の設定

内容を確認して [Confirm]

The screenshot shows the 'Review' step of the AWS Config setup wizard. The left sidebar lists steps: 'Set up AWS Config', 'Step 1: Settings', 'Step 2: AWS Config rules', and 'Step 3: Review'. The 'Step 3: Review' section is highlighted with an orange border. The main content area is divided into two sections: 'AWS Config rules (2)' and 'Settings'.

AWS Config rules (2)

- cloudtrail-enabled**: Checks whether AWS CloudTrail is enabled in your AWS account. Optionally, you can specify which S3 bucket, SNS topic, and Amazon CloudWatch Logs ARN to use.
- root-account-mfa-enabled**: Checks whether the root user of your AWS account requires multi-factor authentication for console sign-in.

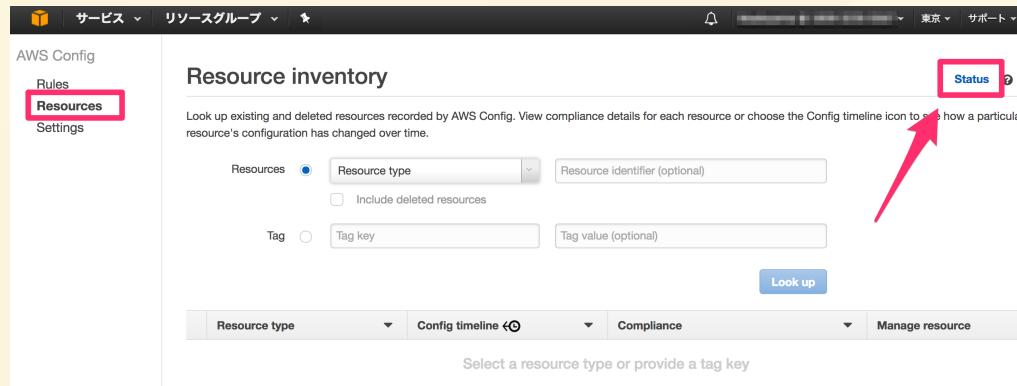
Settings

- Resource types**: All resources (including global resources)
- Amazon S3 bucket**: config-bucket-██████████
- Amazon SNS topic**: config-topic
- AWS Config role**: config-role-ap-northeast-1

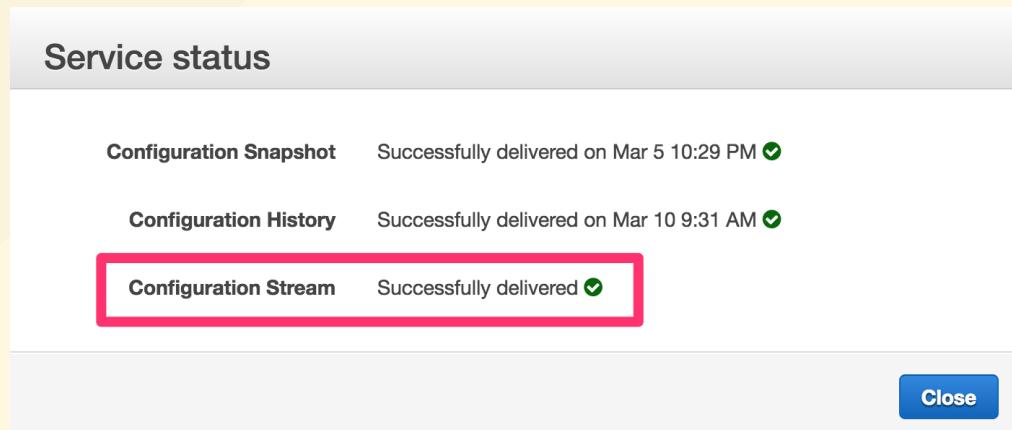
At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Confirm'. The 'Confirm' button is highlighted with a red rectangle.

4. 構成管理の設定

左メニューの [Resources] をクリックして [Status] をクリック



[Configuration Stream] が Successfully になっていればOK
あとは勝手にリソース情報を収集して記録していく



4. 構成管理の設定

[Resources] で表示したいAWSリソースを選択して [Look up]

The screenshot shows the 'Resource inventory' page in the AWS Config console. At the top, there's a dropdown labeled 'Resources' with 'EC2: Instance' selected. To the right of the dropdown is a search bar and a 'Resource identifier (optional)' input field. Below the dropdown, there are two radio buttons: 'Tag' (unchecked) and 'Resource type' (checked). A dropdown menu lists several AWS services: ACM, Certificate, CloudTrail, Trail, EC2 (selected), CustomerGateway, EIP, Host, InternetGateway, and NetworkAcl. The 'EC2' item is highlighted with a red box. On the right side of the page, there are sections for 'Compliance' and 'Manage resource'. A large blue 'Look up' button is also highlighted with a red box.

イベントの発生時刻と内容、前後でリソースの状態がどうなったかが記録される
TBD

The screenshot shows the AWS Config timeline view for an EC2 instance. The top navigation bar includes the AWS logo, 'AWS Config', and a search bar. Below the navigation, the title is 'EC2 Instance i-...'. A timestamp 'on March 07, 2017 2:20:59 PM JST (UTC+09:00)' is displayed. To the right are buttons for 'Managed instance information' and 'Manage resource'. The main area shows a horizontal timeline with several greyed-out time points. In the center, a light blue box highlights the event '07th March 2017 2:20:59 PM' with the number '1 Event' below it. To the right of this highlighted box is another light blue box for '07th March 2017 2:20:59 PM'. On the far right, there are arrows pointing left and right, and a button labeled 'Now' with a calendar icon.

4. 構成管理の設定

Why / Risk

- いつ誰が何をしたか、はCloudTrailの証跡ログから追えるが、そのときAWSのリソースがどういう状態だったかわからない
 - 一応証跡ログを順番に追っていけば再現できなくはない... 😅
- 昨年の年末セール対応ってサーバ何台用意してましたっけ?
 - ドキュメントには20台ってあるけど、当日増やした気が...

Answer

- AWS Configの有効化
 - AWSリソースの状態や、各リソースのRelationship (関係) を記録
 - AWS Configは記録されるの料金が発生
 - ログを保存するS3ストレージ料金が別途発生

Break

- CloudTrailやAWS Configのログは延々と溜まり続ける
 - S3バケットのログはLifecycle機能で一定期間過ぎたら自動削除
 - CloudWatch Logsのログは保持期間の設定で自動削除
- AWS ConfigもCloudTrailと同じく外部サービスと連携して可視化
 - Splunk
 - Logstorage
 - CloudCheckr
 - 2ndWatch
 - etc...

<https://aws.amazon.com/jp/config/partners/>

1. ルートアカウントの保護
2. IAMユーザーとパスワードポリシー
3. 証跡ログの設定
4. 構成管理の設定
- 5. Trusted Advisorの有効化**
6. 請求周りの設定
7. EC2構築時にやること
8. サービス制限緩和
9. 複数のAWSアカウント運用におけるTips

TBD: Trusted Advisorの有効化ではない

5. Trusted Advisor

Why / Risk

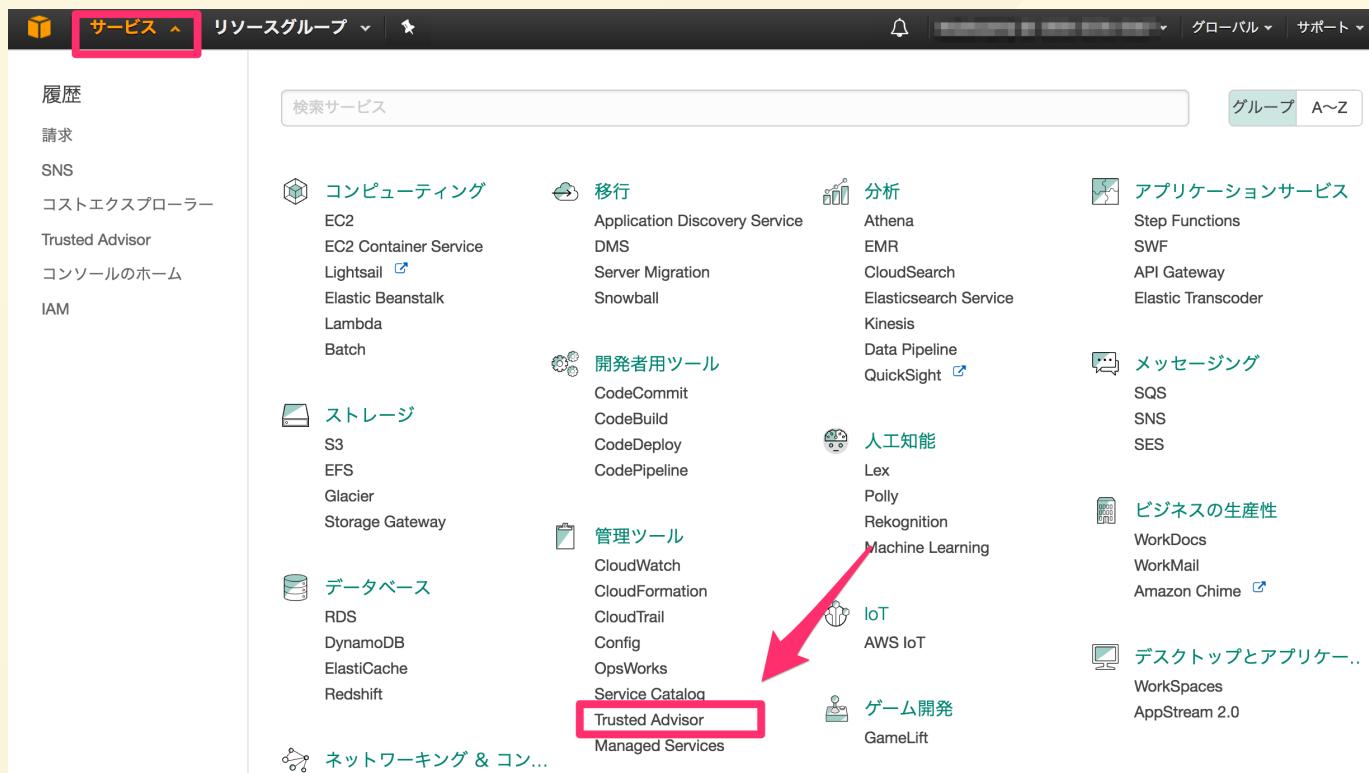
- 現状のAWS設定に危険な設定がないか不安
- 人手ではチェックしきれない、適切なチェックができない

Answer

- Trusted Advisorで以下の4項目を自動でチェックしてレコメンド
 - コスト最適化 (不要なリソースの発見など)
 - パフォーマンス (スペック不足やAWSの制限に達していないかなど)
 - セキュリティ (AWSサービスの権限設定や危険なポート許可など)
 - フォールトトレランス (冗長化やバックアップの設定など)
- Trusted Advisorは無料、サポートレベルによりチェック項目が増加

5. Trusted Advisor

左上の [サービス] から [Trusted Advisor] をクリック



5. Trusted Advisor

4項目がすべてグリーンになっているかチェック



The screenshot shows the Trusted Advisor Dashboard with four main sections: Cost Optimization, Performance, Security, and Fault Tolerance. Each section has a summary icon and a status bar indicating 0 issues (green checkmark), 0 alerts (yellow triangle), and 0 critical issues (red exclamation mark). A red box highlights the status bars for all four categories.

セクション	問題数	警告数	危険度
コスト最適化	0	0	!
パフォーマンス	1	0	!
セキュリティ	3	0	!
フォールトトレランス	0	0	!

推奨されるアクション

- セキュリティグループ - 開かれたポート**
特定のポートに対して無制限アクセス(0.0.0.0/0)を許可しているセキュリティグループのルールをチェックします。
0個中0個のセキュリティグループのルールは、特定のポートに対して無制限アクセスを許可しています。
- IAM の使用**
この機能は、AWS Identity and Access Management (IAM)が使用されているかについてチェックします。
少なくとも一人の IAM ユーザーが作成されました。
- ルートアカウントのMFA**
このチェックではルートアカウントでMFAが有効にされていない場合にアラートを表示します。
このルートアカウントでは、MFAが有効にされておりません。
- サービス制限**

5. Trusted Advisor

先ほど作業したルートアカウントのMFAが有効でなかったり、EC2に対して不要だと思われるポートが許可されていると以下のように警告が表示される

Trusted Advisor ダッシュボード

コスト最適化 パフォーマンス セキュリティ フォールトトレランス

コスト最適化	パフォーマンス	セキュリティ	フォールトトレランス
0 ✓ 0 ▲ 0 !	1 ✓ 0 ▲ 0 !	1 ✓ 1 ▲ 1 !	0 ✓ 0 ▲ 0 !

推奨されるアクション

▶ ! セキュリティグループ - 開かれたポート 更新済み: 37分前

特定のポートに対して無制限アクセス(0.0.0.0/0)を許可しているセキュリティグループのルールをチェックします。

232個中92個のセキュリティグループのルールは、特定のポートに対して無制限アクセスを許可しています。

▶ ! ルートアカウントのMFA 更新済み: 37分前

このチェックではルートアカウントでMFAが有効にされていない場合にアラートを表示します。

このルートアカウントでは MFAが有効にされておりません。

5. Trusted Advisor

[通知設定] から変化があった場合にメールでの通知を行うことができる

通知設定

AWS Trusted Advisor のステータスを最新の状態に保つ為に更新結果とコスト節約の見積もりを毎週メールで受け取りましょう。

通知メールの受信者の選択と通知言語の設定を行うことができます。 Billing and Cost Management console の [Account Settings](#) ページにて受信者のメールアドレスを変更可能です。 (アカウント設定ページにアクセスするためにはログインが必要です。)

受信者

請求に関する連絡先: メールアドレスを設定してください
 ナレレーションに関する連絡先: メールアドレスを設定してください
 セキュリティに関する連絡先: メールアドレスを設定してください

通知の言語 日本語

更新

受信するメールアドレスを設定

▼代替の連絡先

継続的に適切な人物に参加してもらうために、請求、操作、セキュリティに関する通知タイプごとに別の連絡先を追加できます。別の連絡先を指定するには、[編集] ボタンをクリックします。

主要アカウント所有者は、すべての E メール連絡を継続的に受信することに注意してください。

請求

連絡先: なし

操作

連絡先: なし

セキュリティ

連絡先: なし

編集

5. Trusted Advisor

Why / Risk

- 現状のAWS設定に危険な設定がないか不安
- 人手ではチェックしきれない、適切なチェックができない

Answer

- Trusted Advisorで以下の4項目を自動でチェックしてレコメンド
 - コスト最適化 (不要なリソースの発見など)
 - パフォーマンス (スペック不足やAWSの制限に達していないかなど)
 - セキュリティ (AWSサービスの権限設定や危険なポート許可など)
 - フォールトトレランス (冗長化やバックアップの設定など)
- Trusted Advisorは無料、サポートレベルによりチェック項目が増加

Break

サポートによりチェック項目が増加

- Basicプラン (Free)
チェック項目数4つ (コスト最適化とフォールトトレランスはなし)



- Businessサポートの場合 (月額料金1割増し or \$100)
チェック項目数55個

<https://aws.amazon.com/jp/premiumsupport/trustedadvisor/best-practices/>



1. ルートアカウントの保護
2. IAMユーザーとパスワードポリシー
3. 証跡ログの設定
4. 構成管理の設定
5. Trusted Advisorの有効化
- 6. 請求周りの設定**
7. EC2構築時にやること
8. サービス制限緩和
9. 複数のAWSアカウント運用におけるTips

6. 請求周りの設定

Why / Risk

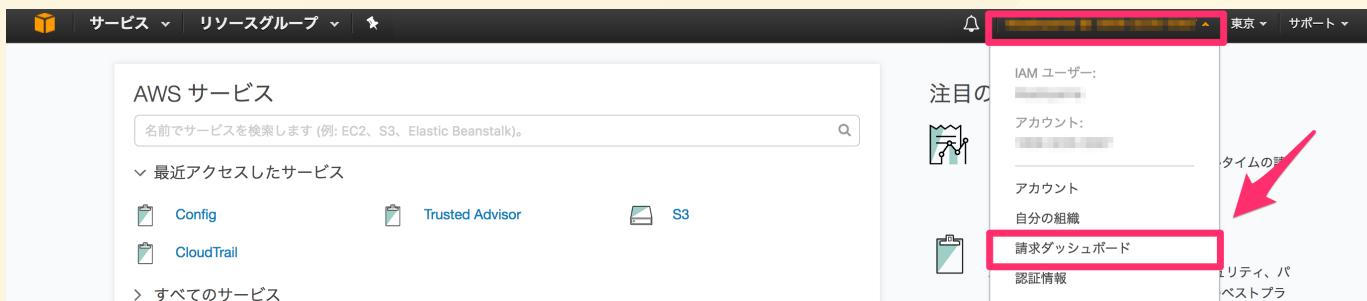
- デフォルトでは料金を見るのにルートアカウントが必要になる
- 気づかぬうちにAWSの料金が予算をオーバーしていた
- 意図していない支払いが発生していた

Answer

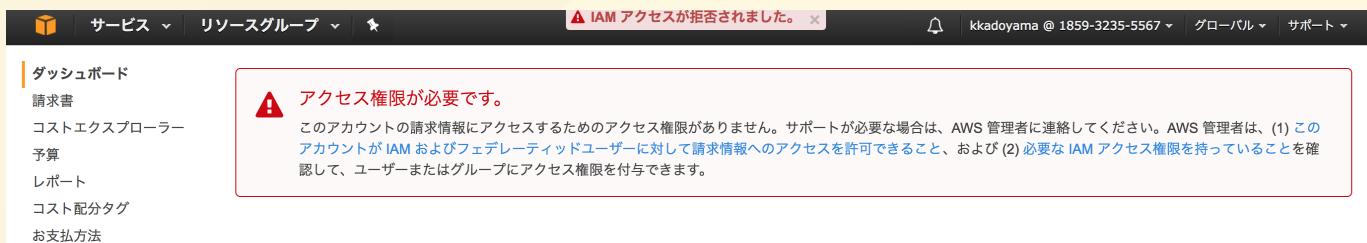
- IAMユーザーでも見れるようにする
 - 経理の方など請求周りの権限のみを持ったユーザーの作成
- コストエクスプローラーにより料金の詳細な分析
- 毎月の実績や予測の予算を設定
- 毎月の料金をメールで受信する

6. 請求周りの設定 (IAM User)

メニューから [請求ダッシュボード] をクリック



アクセス権限がないため拒否される

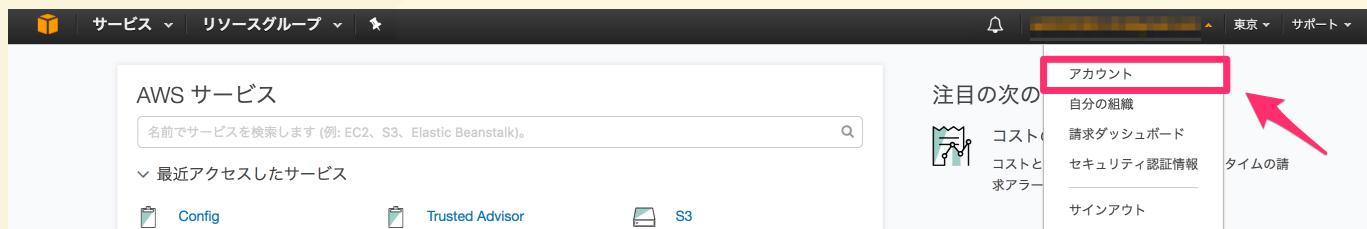


6. 請求周りの設定 (IAM User)

一度サインアウトし、ルートアカウントでサインインし直す



メニューから [アカウント] をクリック



6. 請求周りの設定 (IAM User)

[IAMユーザー/ロールによる請求情報へのアクセス] の編集をクリックし、

▼IAM ユーザー/ロールによる請求情報へのアクセス

IAM ユーザーおよびフェデレーティッドユーザーに対して、請求情報にアクセスするためのロールのアクセス権限を付与できます。これには、アカウント設定、支払方法、およびレポートの各ページへのアクセスが含まれます。どのユーザー やロールに請求情報へのアクセスを許可するかは、IAM ポリシーを作成して制御できます。詳細については、「[請求情報へのアクセスコントロール](#)」を参照してください。

IAM ユーザー/ロールによる請求情報へのアクセスは無効になっています。

[編集](#)

[IAMアクセスのアクティブ化] を設定

▼IAM ユーザー/ロールによる請求情報へのアクセス

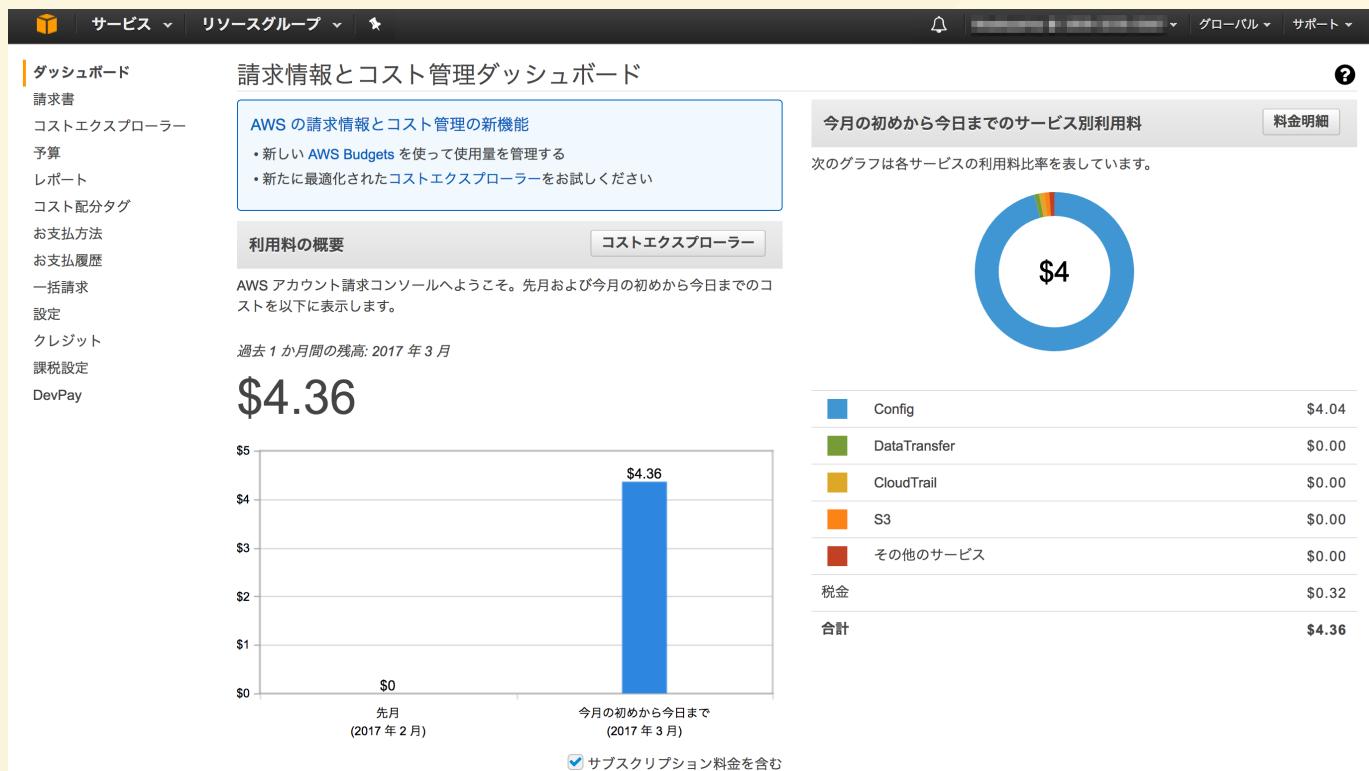
IAM ユーザーおよびフェデレーティッドユーザーに対して、請求情報にアクセスするためのロールのアクセス権限を付与できます。これには、アカウント設定、支払方法、およびレポートの各ページへのアクセスが含まれます。どのユーザー やロールに請求情報へのアクセスを許可するかは、IAM ポリシーを作成して制御できます。詳細については、「[請求情報へのアクセスコントロール](#)」を参照してください。

IAM アクセスのアクティブ化

[更新](#) [キャンセル](#)

6. 請求周りの設定 (IAM User)

再度サインアウトしてIAMユーザーでサインインし直し、メニューから [請求ダッシュボード] へアクセス



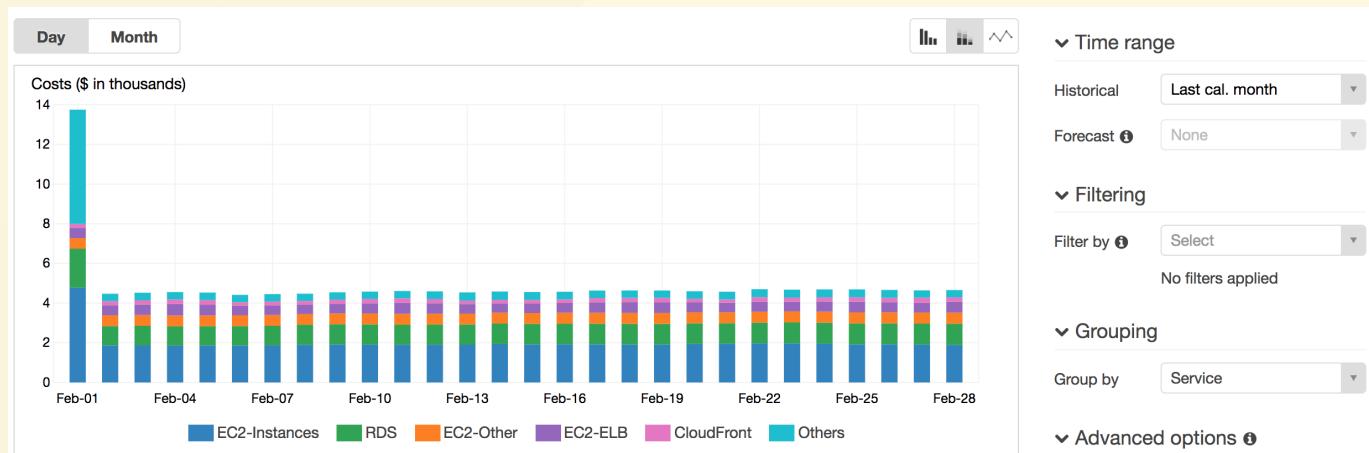
月のAWSサービス別の料金が表示される

6. 請求周りの設定 (Cost Explorer)

コストエクスプローラー

コストエクスプローラーを使用すれば自由な分析が可能 (利用は無料)

- 日別／月別／年別の料金や推移
- 任意のタグでグルーピングした料金
- Consolidated Billingでまとめた各AWSアカウントの料金など



6. 請求周りの設定 (Cost Explorer)

コストエクスプローラーの有効化



The screenshot shows the AWS Cost Explorer setup page. On the left, a sidebar lists various options: ダッシュボード, 請求書, コストエクスプローラー (which is selected and highlighted with a red box), 予算, レポート, コスト配分タグ, お支払方法, お支払履歴, 一括請求, 設定, クレジット, 課税設定, DevPay. The main content area has a title 'コストエクスプローラーへようこそ' and a sub-section '機能の説明'. A large blue button labeled 'コストエクスプローラーを有効化' is highlighted with a red box and a red arrow points to it from below. Below the button, there are three sections: '構成済みのビューを使用する', '使用量を分析', and 'ダウンロードまたはブックマーク', each with a corresponding icon and a '詳細情報」 link.

6. 請求周りの設定 (Budgets)

予算

設定することで、料金が超過する／超過することが予想される場合などにアラートを送信することができる



The screenshot shows the AWS Budgets console interface. On the left, a sidebar menu lists various options: ダッシュボード, 請求書, コストエクスプローラー, **予算**, レポート, コスト配分タグ, お支払方法, お支払履歴, 一括請求, 設定, クレジット, 課税設定, DevPay. The '予算' option is highlighted with a red box. In the main content area, the title 'AWS Budgets' is displayed above a descriptive text: 'AWS Budgets では、AWS のコストや使用量が設定値を超えたか、超えることが予想される場合に自動アラートを送信するカスタム予算を迅速に作成することができます。'. Below this is a large blue button labeled '予算を作成' (Create Budget), which is also highlighted with a red box and has a red arrow pointing towards it from the bottom-left. Further down, there are three sections: 'AWS Budgets の開始方法' (How to start using AWS Budgets), '予算の作成および管理' (Create and manage budgets), 'フィルタを使用して予算を絞り込む' (Filter budgets), and '予算に通知を追加する' (Add notifications to budgets). Each section contains a brief description and an associated icon.

6. 請求周りの設定 (Budgets)

月別の予測コストが、指定した予算の80%を超過した場合にメールで通知

TBD: コスト額

予算の作成

AWS コストあるいは使用量が設定したしきい値を超過した場合、あるいは超過すると予測された場合に、自動的にアラートするようにカスタム予算を作成します。

① 予算の詳細

名前* 月額AWS予算

コストまたは使用量を選択 コスト

期間 月別

開始日 17/03/01

終了日 -

予算額* 1,000.00

AWS 予算の作成

② 含められる関連コスト

サービス
 関連アカウント
 タグ
 購入オプション
 アベイラビリティーゾーン
 API オペレーション

③ 通知 (省略可能)

請求アラームを作成すると、現在のまたは予測された AWS の料金が選択したしきい値に達したときに、メールアラートを受信できます。
通知を受信するには、E メール連絡先または SNS トピックの ARN を少なくとも 1 つ指定してください。

通知のタイミング: 予測 > 80 % (予算額)

連絡電子メール: [redacted]@gmail.com

SNS トピックの ARN: 有効な SNS トピックの ARN を入力してください

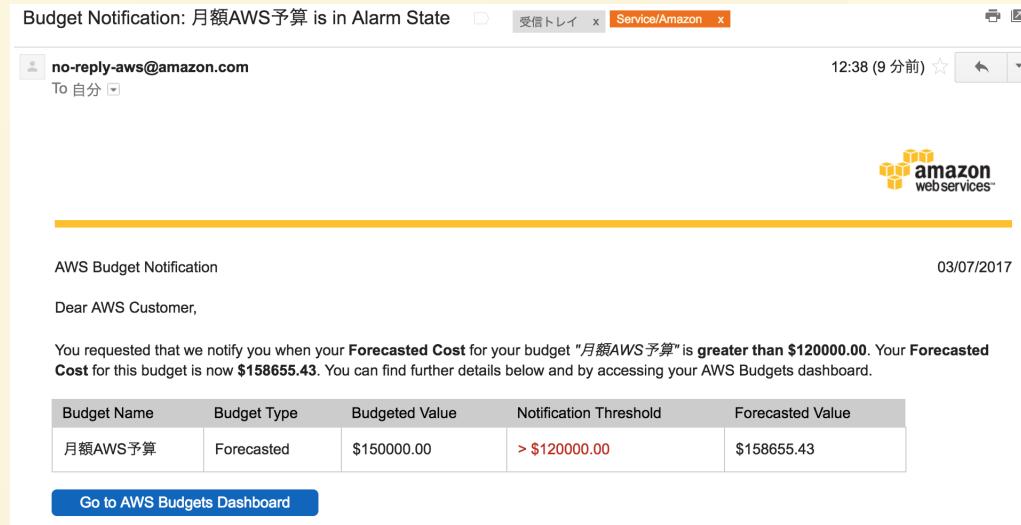
SNS トピックポリシーステートメント: +新しい通知の追加

* 必須 キャンセル 作成



6. 請求周りの設定 (Budgets)

実際にAWSから送られてくるメール



6. 請求周りの設定 (Mail)

毎月の請求書 (PDF) をメールで受信する

The screenshot shows the AWS Billing and Cost Management console's 'Settings' page. On the left, a sidebar lists various options: ダッシュボード, 請求書, コストエクスプローラー, 預算, レポート, コスト配分タグ, お支払方法, お支払履歴, 一括請求, **設定**, クレジット, 課税設定, DevPay. The '設定' option is highlighted with a red box. The main content area is titled '設定'. It contains three sections with checkboxes:

- 電子メールで PDF 版請求書を受け取る**
PDF 版請求書を電子メールで受け取りたい場合は、このサービスをオンにしてください。請求書は、請求対象月の翌月 3 日頃に発行されます。
- 請求アラートを受け取る**
AWS の利用料金と毎月発生する料金を自動的に監視する場合は、このサービスをオンにしてください。これにより、容易に AWS での使用料金を調べて管理することができます。請求アラートで、料金が設定した値に達したときにメール通知を受け取る様に設定することができます。また請求アラートは一度オンにするとオフに戻す事はできません。[請求アラートを管理する](#) または、[新しい予算機能をお試しください!](#)
- 請求レポートを受け取る**
AWS の料金に関する進行中のレポートを毎日 1 回以上に受け取るには、この機能をオンにします。下記で指定された S3 バケットにレポートが配信されます。レポートは支払アカウントに対してのみ配信されます。連結アカウントでは請求レポートを受け取ることができません。

Below these sections, there is a text input field labeled 'S3 バケットに保存:' containing 'バケット名' and a '検証' button. At the bottom, there is a blue '設定の保存' button.

6. 請求周りの設定

Why / Risk

- 料金を見るのにルートアカウントが必要になる
- 気づかぬうちにAWSの料金が予算をオーバーしていた
- 意図していない支払いが発生していた

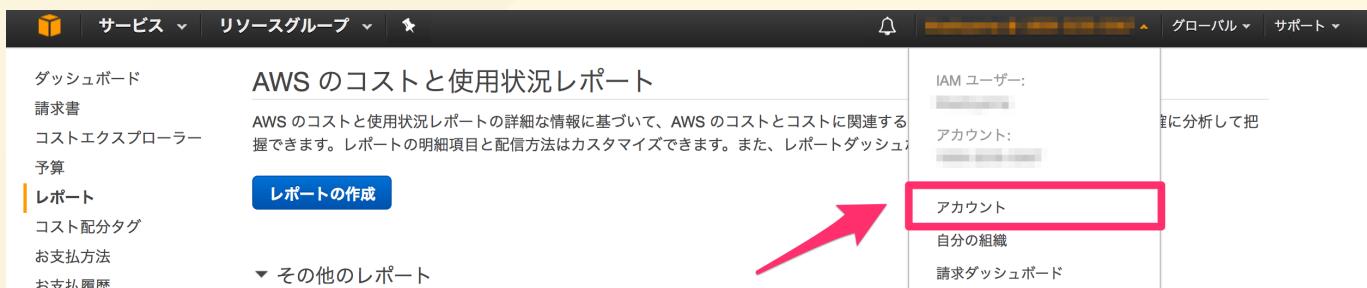
Answer

- IAMユーザーでも見れるようにする
 - 経理の方など請求周りのみ権限を持ったユーザーの作成
- コストエクスプローラーにより料金の詳細な分析
- 毎月の実績や予測の予算を設定
- 毎月の料金をメールで受信する

Break

アカウントや請求周りは他にもこんな設定が

- 支払い通貨の変更 (\$ → ¥)
 - クレカの手数料込みのレート or AWSのレート
- 秘密の質問の設定
- AWSからのマーケティングメールの受信設定
- 時間別の詳細料金レポートをS3にcsv出力



自分の組織／環境にあわせて適切な設定を

1. ルートアカウントの保護
2. IAMユーザーとパスワードポリシー
3. 証跡ログの設定
4. 構成管理の設定
5. Trusted Advisorの有効化
6. 請求周りの設定
7. EC2構築時にやること
8. サービス制限緩和
9. 複数のAWSアカウント運用におけるTips

9. 複数のAWSアカウント運用

Why / Risk

- システム／環境が増えればAWSアカウントも増える
 - AWSのサービス制限の中にはアカウント単位のものもある
- ログイン用のIAMユーザー↑↑
 - システム数 × 環境数 × 担当者数 = 
- アカウントごとに請求されることで請求処理の手間

Answer

- 担当者につきIAMユーザーは1つで複数のAWSアカウントにログイン
 - Switch RoleによるAWSアカウント切り替え
- 複数AWSアカウントの請求を1つにまとめる
 - Consolidated Billing (一括請求)

9. 複数のAWSアカウント運用

Switch Role

IAMユーザー = ログインやAPIでのアクセスに使用

IAMロール = IAMポリシー(権限)が付与された役割

TBD: 図

9. 複数のAWSアカウント運用

Consolidated Billing

実際に請求がくる親アカウント1つと、
支払いをしてもらう子アカウント複数を、
Consolidated Billingアカウントファミリーとして紐付ける

ボリューム割引やファミリー間のReserved Instances共有などのメリットも

9. 複数のAWSアカウント運用

AWS Organizations

<https://aws.amazon.com/jp/about-aws/whats-new/2017/02/aws-organizations-now-generally-available/>

The screenshot shows the AWS website with a dark header. The header includes a 'メニュー' button, the 'amazon web services' logo, navigation links for '開始方法', '製品', 'ソリューション', '料金表', 'ソフトウェア', '詳細', '日本語', 'アカウント', and a yellow 'サインアップ' button.

The main content area has a title 'AWS Organizations が一般公開されました' (AWS Organizations has been generally available) in orange. Below it, a date '上の投稿: Feb 27, 2017' is shown. The text explains that AWS Organizations provides management for multiple AWS accounts, allowing for centralized policy management across accounts. It also mentions Service Control Policies (SCPs) and automated account creation via APIs.

On the left sidebar, there's a 'AWSについて' section with links to 'AWSについて', 'グローバルインフラストラクチャ', '最新情報', 'AWS メディア掲載記事', and '国内のセミナー・イベントスケジュール'. There's also a '関連リンク' section with links to 'クラウドとは?', 'クラウドの強みとメリット', and 'AWS クラウド 無料利用枠'.

- Consolidated Billing + 複数AWSアカウント管理
- AWSアカウントを階層管理できてポリシーを適用することで機能を制限
TBD: 自動化も

9. 複数のAWSアカウント運用

TBD: Organizationsを使う場合と使わない場合の図

TBD: 概念図とこのハンズオンでやろうとしていることのゴールの図

9. 複数のAWSアカウント運用

以下のURLにアクセスし、[使用を開始する]

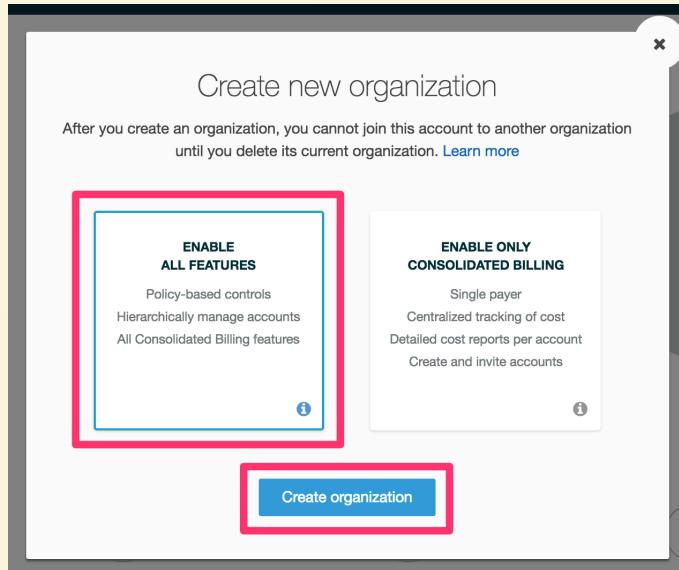
<https://aws.amazon.com/jp/organizations/>



[Create Organization] をクリック

9. 複数のAWSアカウント運用

[ENABLE ALL FEATURES] をクリック

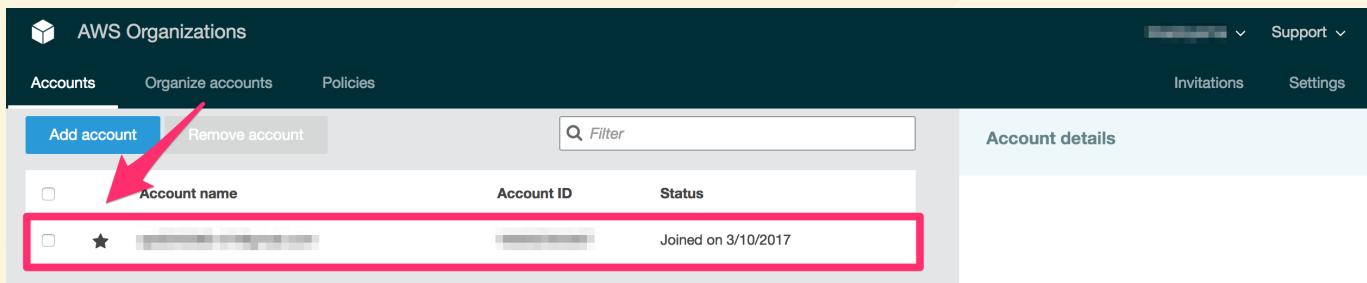


- ENABLE ONLY CONSOLIDATED BILLING
 - これまでのConsolidated Billingのみの機能、請求をまとめるだけ
- ENABLE ALL FEATURES
 - 上記に加え、ポリシーによる権限管理や今後実装されるであろう機能が利用可能

9. 複数のAWSアカウント運用

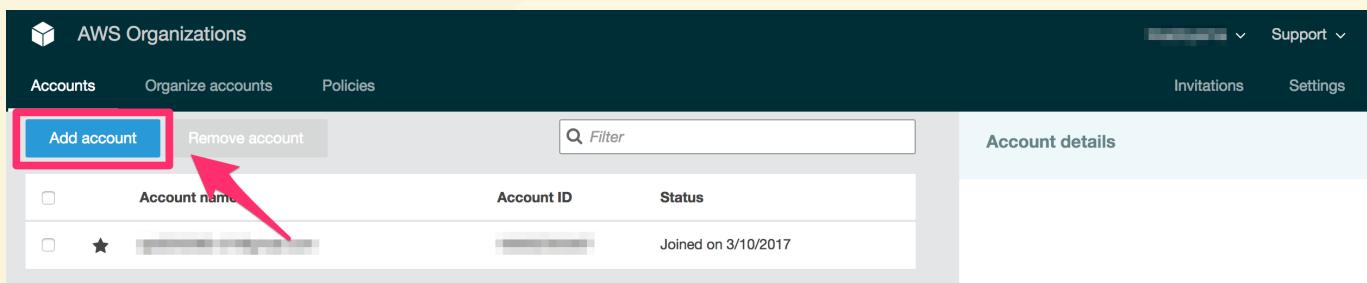
★ マスターアカウントになる

※Consolidated Billingでいう親アカウント (実際に請求がくる)



The screenshot shows the AWS Organizations console with the 'Accounts' tab selected. At the top, there are buttons for 'Add account' (highlighted with a red arrow) and 'Remove account'. Below is a table with columns: 'Account name', 'Account ID', and 'Status'. One account is listed, marked with a star icon in the 'Account name' column. A red box highlights this row. To the right, there's a sidebar titled 'Account details'.

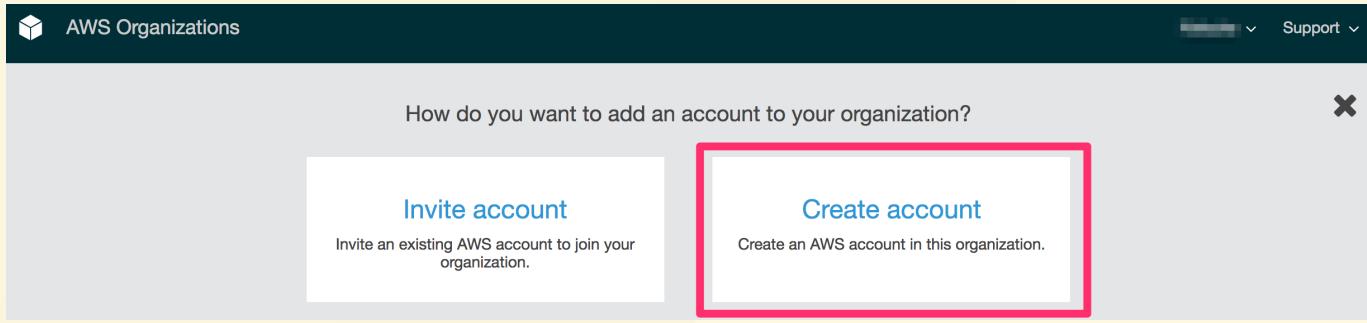
左上の [Add account] からAWSアカウントを追加



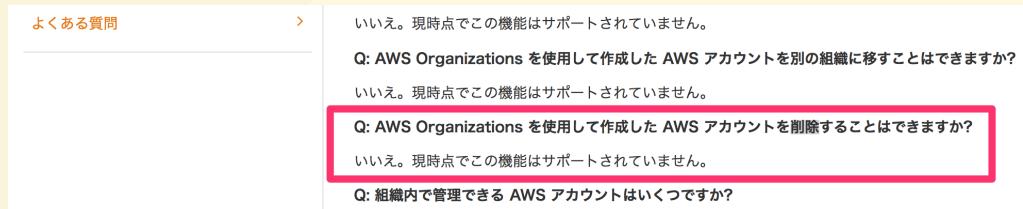
This screenshot is similar to the one above, showing the AWS Organizations console. The 'Add account' button is highlighted with a red box and a red arrow points to it from below, indicating where to click to add a new account.

9. 複数のAWSアカウント運用

[Create account] からAWSアカウントを新規作成



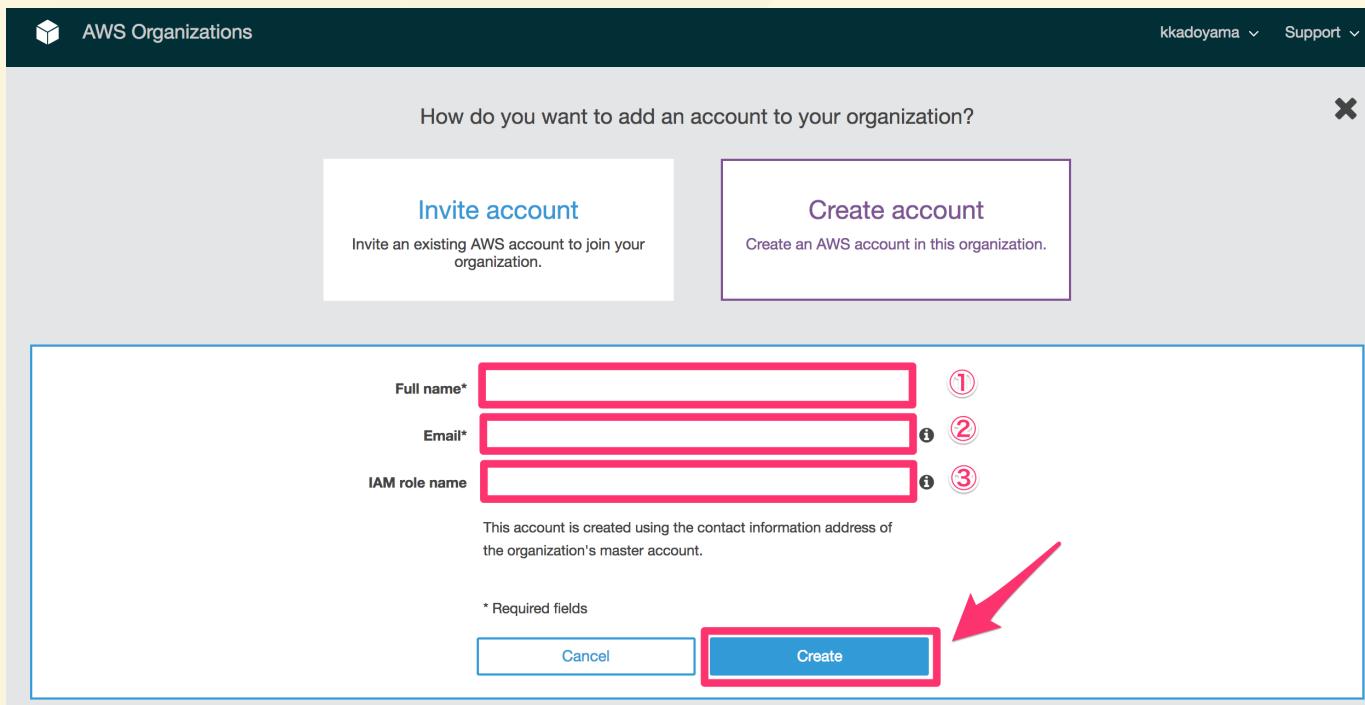
[Create account] で新規作成したAWSアカウントは現状削除できない
ただし解約はできる、、、AWS Organazations上から消せないだけ？



[Remove account] しようとしても。。

9. 複数のAWSアカウント運用

- ①[Full name] はAWSアカウント名
- ②[Email] はAWSアカウントを作成する際に入力するメールアドレスで一意
※ハンズオンの最初で作成したメールアドレスとは異なるものを設定
- ③[IAM role name] は作成するAWSアカウントに用意されるIAMロール名
※未指定だと [OrganizationAccountAccessRole] になる



9. 複数のAWSアカウント運用

AWSアカウントの追加が完了

※追加されたAWSアカウントの [Account ID] をメモ

The screenshot shows the AWS Organizations console with the 'Accounts' tab selected. A new account has been added and is highlighted with a red box. The account details show it was created on 3/10/2017.

右上のIAMユーザー名をクリックし [ロールの切り替え]

The screenshot shows the AWS IAM console with the user menu open. The 'Role Switch' option is highlighted with a red box.

9. 複数のAWSアカウント運用

- ①[アカウント] には先ほどメモした作成したAWSアカウントの [Account ID] (12桁数字) を入力
- ②[ロール] には作成したAWSアカウントのIAMロール名を入力
※作成時に未指定の場合は [OrganizationAccountAccessRole]
- ③[表示名] はエイリアスなので好みで

ロールの切り替え

単一ユーザーIDとパスワードを使用しているAWSアカウント全体にわたって、リソースの管理を許可します。AWS管理者がロールを設定してアカウントとロールの詳細が提供されると、ロールを切り替えることができるようになります。[詳細はこちら。](#)

アカウント* ⓘ ①

ロール* ⓘ ②

表示名 ⓘ ③

色

*必須 キャンセル ロールの切り替え



9. 複数のAWSアカウント運用

TBD: 切り替わったあとの図

TBD: スライドの場所

9. 複数のAWSアカウント運用

AWSアカウントが切り替わりました

右上のアカウント名が [IAMロール名]@[Account ID] になっています
※[表示名] を設定した場合は [表示名] になります

左上の [サービス] から [IAM] をクリック

The screenshot shows the AWS Management Console's top navigation bar. The 'Services' button is highlighted in red. To its right are dropdown menus for 'リソースグループ' (Resources Groups) and a user profile ('jaws @ 936995010458'). On the far right are links for '東京' (Tokyo) and 'サポート' (Support). Below the navigation bar, the main content area displays a grid of service icons and names. The 'IAM' service icon, which is a key icon, is also highlighted with a red box.

初期状態のIAMの画面が表示される

The screenshot shows the 'Identity and Access Management' (IAM) service dashboard. The left sidebar contains a 'ダッシュボード' (Dashboard) section with links for 'グループ', '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', and '認証情報レポート'. Below this is a '鍵' (Key) section. The main content area has a header 'Identity and Access Management へようこそ' and a sub-header 'IAM ユーザーのサインインリンク: https://[REDACTED].signin.aws.amazon.com/console'. It displays statistics: 'ユーザー: 0', 'グループ: 0', 'ロール: 1', and 'ID プロバイダ: 0'. A 'カスタマイズ' (Customize) and 'リンクのコピー' (Copy link) button is shown. On the right, there's a '注目の機能' (Featured Functionality) section with a video thumbnail titled 'Introduction to AWS IAM' and a 'セキュリティステータス' (Security Status) summary. At the bottom, there's a '追加情報' (Additional Information) section with links for 'IAM ID キュメント', 'Web ID フェデレーションのフレイグ', 'Policy Simulator', and '動画: IAM リリース履歴、および追加のリソース'.

9. 複数のAWSアカウント運用

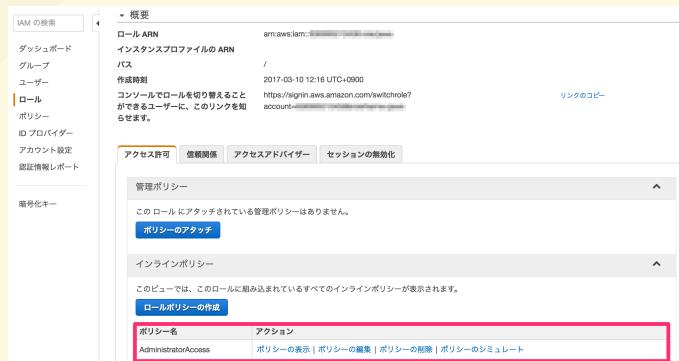
左メニューから [ロール] をクリック

AWS OrganizationsからAWSアカウント作成の際に指定したIAMロールが表示されるので、ロール名をクリック



[AdministratorAccess] ポリシーが設定されている

今後はこのIAMロールを起点に、必要なIAMロールを作成してマスターアカウントから切り替えて利用する

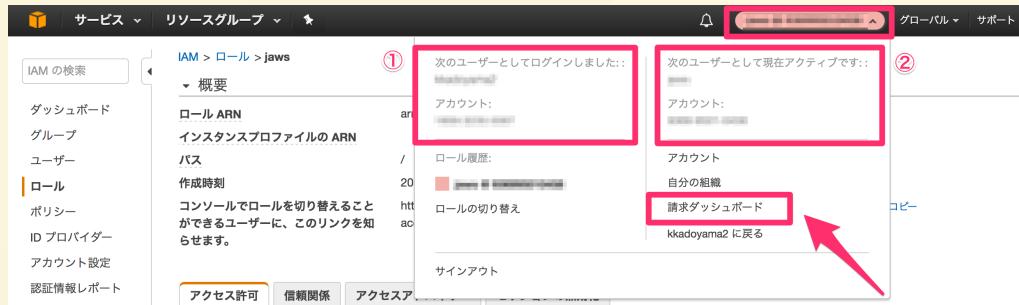


9. 複数のAWSアカウント運用

右上のアカウント名をクリック

- ①がAWSコンソールにログインしたIAMユーザーとAWSアカウントの情報
- ②が現在操作中の切り替えた先のIAMロールとAWSアカウントの情報

[請求ダッシュボード] をクリック



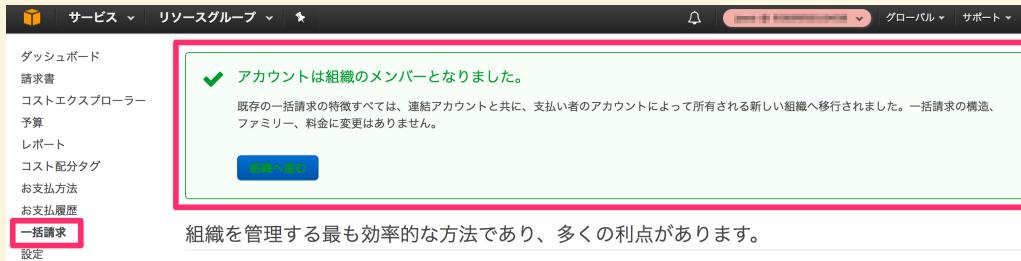
最初から料金が見える状態になっている (P68の設定不要)



9. 複数のAWSアカウント運用

左メニューから [一括請求] をクリック

AWS Organizationsのメンバーで、料金請求はマスター アカウントにまとめられている

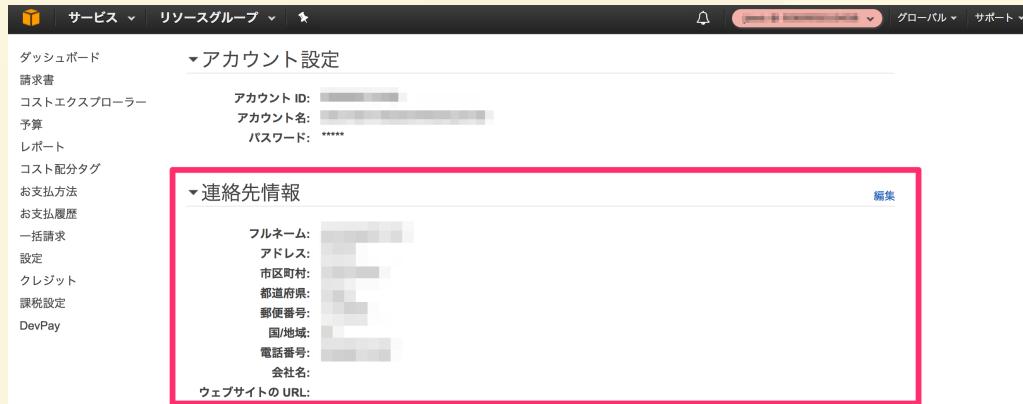


右上のアカウント名クリックから [アカウント] へ



9. 複数のAWSアカウント運用

AWSアカウントの住所など連絡先はマスター アカウントと同じものが設定されている



右上のアカウント名クリックから [xxx (IAMユーザー名) に戻る] で切り替え元のAWSアカウントに戻る
※ハンズオンだと最初に作成したIAMユーザー



9. 複数のAWSアカウント運用

Why / Risk

- システム／環境が増えればAWSアカウントも増える
 - AWSのサービス制限の中にはアカウント単位のものもある
- ログイン用のIAMユーザー↑↑
 - システム数 × 環境数 × 担当者数 = 
- アカウントごとに請求されることで請求処理の手間

Answer

- AWS Organizationsを利用してAWSアカウントを一元管理
 - 担当者につきIAMユーザーは1つで複数のAWSアカウントにログイン
 - Switch RoleによるAWSアカウント切り替え
 - 複数AWSアカウントの請求を1つにまとめる

Break

AWS Organazations Tips (1/2)

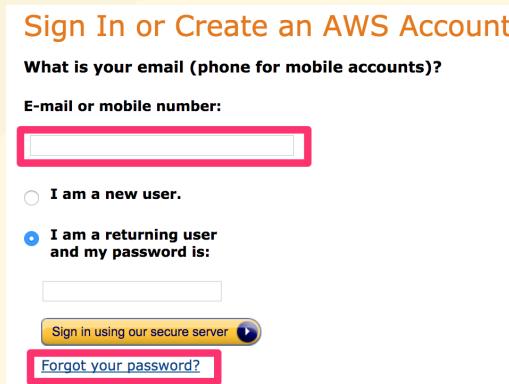
- ポリシー (Service Control Policies: SCPs) により、各AWSアカウントで利用できるサービスとオペレーションを制限できる
 - サービスはEC2とS3のみ利用可能だが、EC2のTerminate禁止など
 - AWS OrganazationsのポリシーとIAMポリシーによる両方の制限
 - システムに必要なサービスのみ制限したり、本番環境で不要なサービス作成を制限したり
- OUというAWSアカウントをグループにした単位を作成

TBD

Break

AWS Organazations Tips (2/2)

- AWS OrganazationsからAWSアカウントを作成した場合のルートアカウントは?
 - 存在するがパスワード未設定の状態になっている
 - サインイン時の [Forgot your password?] から設定すれば使えるようになりました



EC2-Mail送信制限緩和や侵入テスト申請など、どうしてもルートアカウントが必要な場面で

まとめ

- AWSアカウントを取得したら、MFAの設定やIAMユーザーの利用、証跡ログの記録など要件にあわせて初期設定をしておきましょう
※本番環境はとくに注意
- 設定しない場合でも、どういうリスクがあるかは把握しておきましょう
- 複数のAWSアカウントの運用は請求処理や作成するIAMユーザー数の観点からAWS Organazationsを使うと便利です
- AWSアカウントやコストの管理は自己責任(ユーザー責任)です
- 予算超過のアラートやコストエクスプローラー、Trusted Advisorなど無料で利用できる便利なサービスが揃っています
- 夜も眠れない場合はAWSサポートやSAの方に相談を 

Wrap up

使用したリソースの削除

- AWS Organizationsで作成したAWSアカウントの解約
※アカウントページから
- CloudFormationのスタック削除
- CloudTrail、 AWS Configの削除
- S3バケット、 SNSのトピック、 CloudWatch Logsのロググループ削除
- 不要なIAMユーザー、 IAMグループの削除

Thanks!! & Questions?

本セッションの内容は以上です
お疲れ様でした
このあともJAWS DAYS 2017をお楽しみください

EOF

