



AWS  
**Black Belt**  
Online Seminar

# 【AWS Black Belt Online Seminar】 AWS Organizations

アマゾン ウェブ サービス ジャパン株式会社  
ソリューションアーキテクト 辻 義一

2018.02.14



# 自己紹介

## 辻 義一 (つじ よしかず)

📦 西日本担当 ソリューションアーキテクト

📦 簡単な経歴

- 大阪生まれの大阪育ち。
- 独立系SIerでインフラエンジニア。

📦 AWSのすきな所

～ 安い、早い、おもしろい～



# 内容についての注意点

- 本資料では2018年2月14日時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(<http://aws.amazon.com>)にてご確認ください。
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。
- 価格は税抜表記となっております。日本居住者のお客様が東京リージョンを使用する場合、別途消費税をご請求させていただきます。
- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at <http://aws.amazon.com/agreement/>. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

# Agenda

- 📦 AWS Organizationsについて
- 📦 使い始めるには
- 📦 機能・操作について
- 📦 一括請求について
- 📦 複数AWSアカウント利用のメリット



# AWS Organizations

複数の AWS アカウントをポリシーベースで管理します。

アカウントのグループに適用するポリシーを簡単に管理でき、アカウントの作成を自動化できます。



AWS Organizations の使用を開始する

The screenshot displays the AWS Organizations console. At the top, it says 'Welcome' and provides a brief overview of the service. A prominent 'Create organization' button is visible. Below this, there are three numbered steps: 1. Create accounts, 2. Organize accounts, and 3. Apply policies. The interface is clean and professional, with a dark header and a light main content area.

# AWS Organizations で実現できること

複数AWSアカウント  
を一元管理



- ❏ AWSアカウントをグループ化してポリシーを適用し利用サービスを制限

AWSアカウント  
新規作成の自動化



- ❏ コンソール、SDK、CLIでAWSアカウントを新規作成
- ❏ 作成操作をロギング (CloudTrail)

請求の簡素化

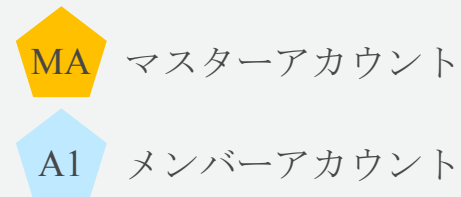


- ❏ 複数AWSアカウントの請求を一括 (旧Consolidated Billing)

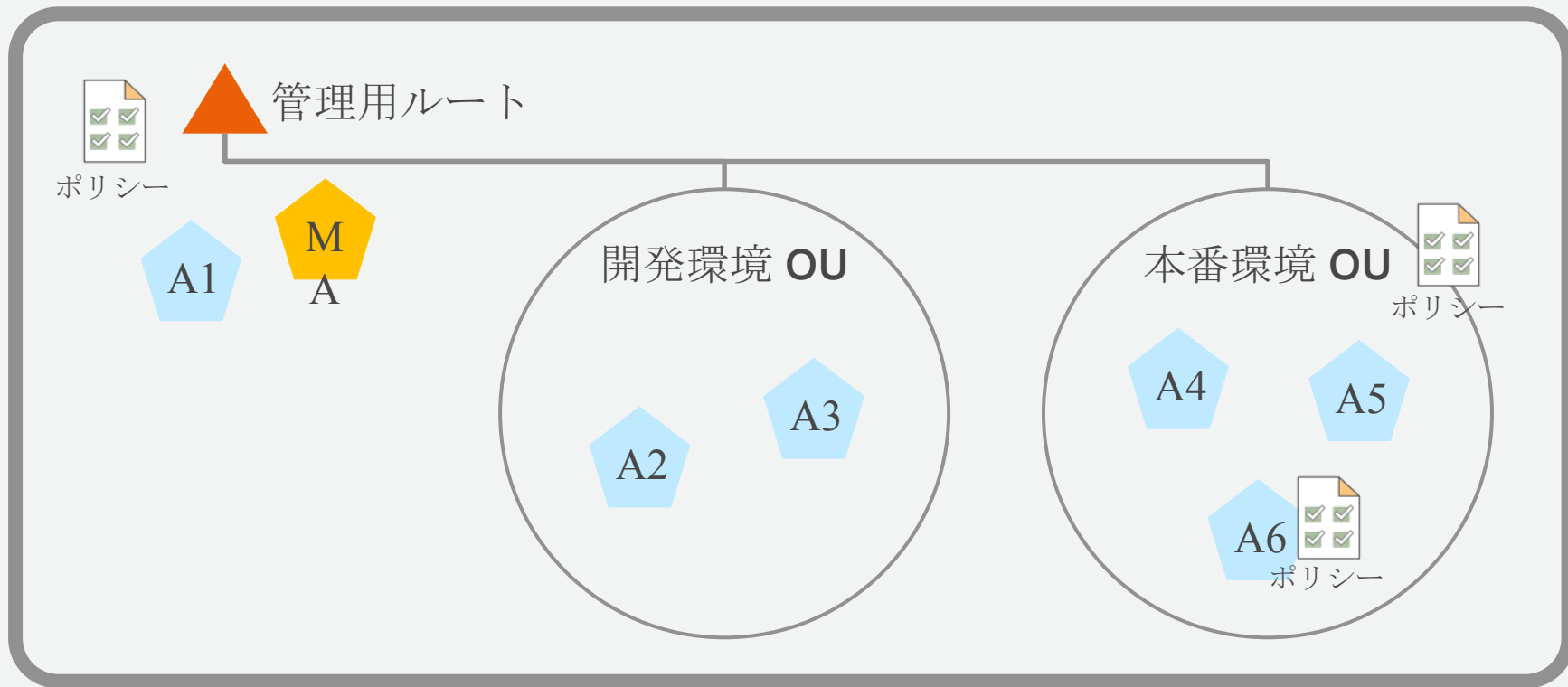
# AWS Organizations の構成要素

用語	説明
AWSアカウント or アカウント	<ul style="list-style-type: none"><li>▪ AWS契約の単位でメールアドレスや12桁のIDで識別される</li><li>▪ AWSアカウント内ではIAMでユーザ単位のアクセス制御などが行える</li><li>▪ AWS Organizationsで管理する最小単位</li></ul>
組織 (Organization)	<ul style="list-style-type: none"><li>▪ AWS Organizationsで一元管理する対象の全体</li><li>▪ 複数AWSアカウントのセット</li></ul>
マスターアカウント	<ul style="list-style-type: none"><li>▪ AWS Organizations組織の全体を管理する権限を持つAWSアカウント</li></ul>
メンバーアカウント	<ul style="list-style-type: none"><li>▪ 組織内にあるマスターアカウント以外のAWSアカウント</li></ul>
組織単位 (OU)	<ul style="list-style-type: none"><li>▪ 組織内にある複数AWSアカウントのグループ</li></ul>
管理用ルート (root)	<ul style="list-style-type: none"><li>▪ 組織単位 (OU) 階層の開始点</li></ul>
組織ポリシー	<ul style="list-style-type: none"><li>▪ 組織内で適用してAWSアカウントを管理する仕組み</li></ul>
サービス管理ポリシー (SCP)	<ul style="list-style-type: none"><li>▪ 現在サポートされている唯一の組織ポリシーのタイプ</li><li>▪ 利用できるAWSサービスとアクションを制御</li></ul>

# AWS Organizations の構成図



組織



 使い始めるには

# 使い始める前に - 機能セットを選択

どちらの機能セットを使用するか選択する。

(一括請求のみ)

(すべての機能)

**Consolidated  
Billing Only**

**All Feature**

マスターアカウントへの一括請求



アカウントの新規作成・招待・  
削除



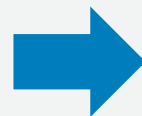
サービスコントロールポリシー  
による一元管理



# 使い始める前に - 機能セットを選択

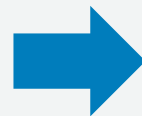
どちらの機能セットで使用するかを選択する。

支払い代行を行うだけの時



**Consolidated  
Billing Only**

企業内で複数アカウントを統制したい時



**All Feature**

# 使い始める前に - マスターアカウントの選択



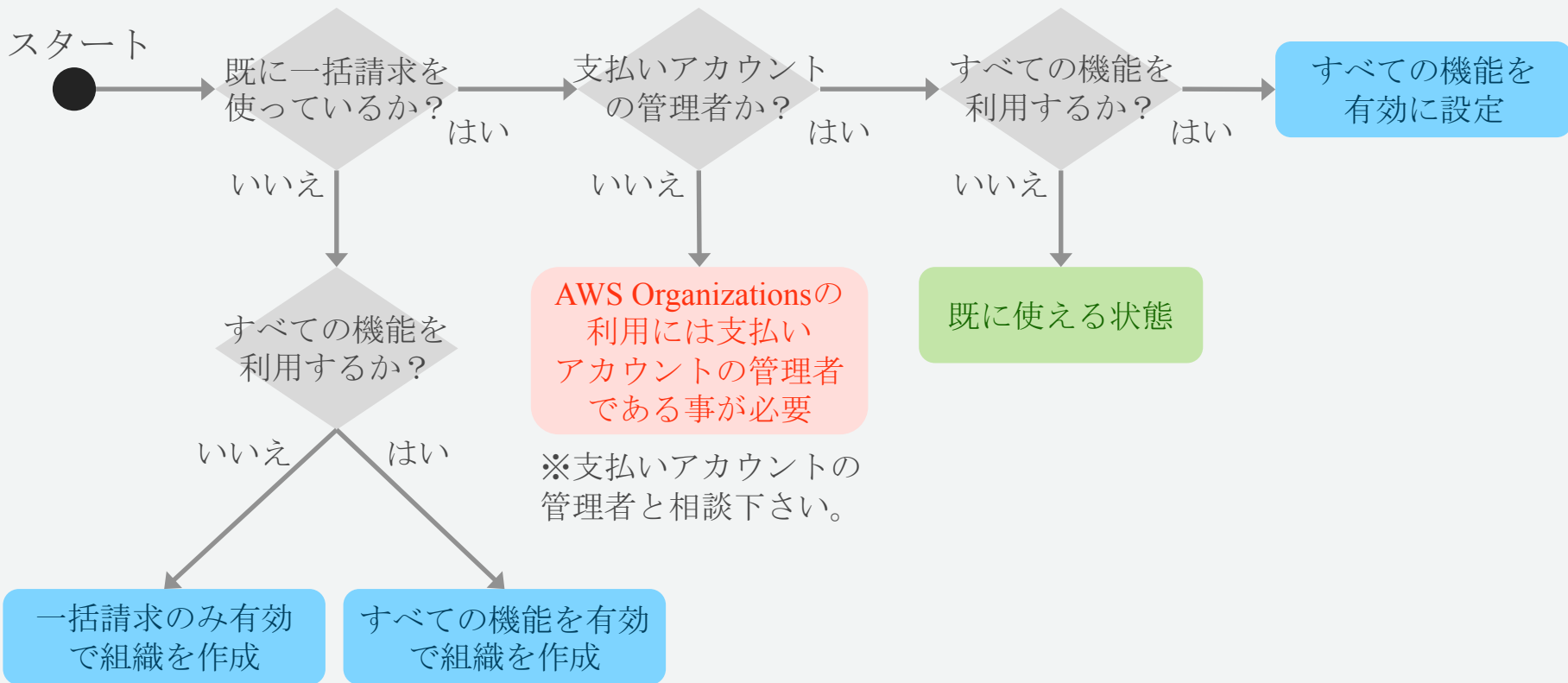
どの**AWS**アカウントをマスターアカウントとするか選択する。

 マスターアカウントは以下の役割・権限を持つため慎重に決定

- 組織全体の**AWS**利用料の支払い
- 新規**AWS**アカウントの作成
- 既存**AWS**アカウントの招待
- 組織内に登録された**AWS**アカウントの削除
- 組織ポリシーの適用

マスターアカウントは基本的にリソースなどを作成しないアカウントにするのがおすすめ。

# 組織の作成 と 機能の有効化

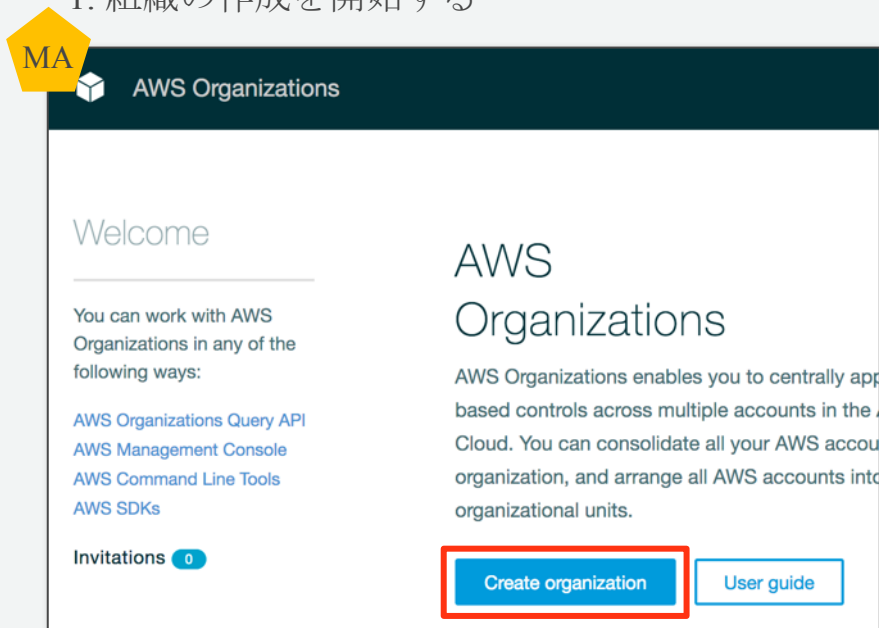


# 機能・操作について

# 組織を作成する

マスターアカウントにしたいAWSアカウントで組織の作成を開始し、機能セットを選択する。

## 1. 組織の作成を開始する



MA

AWS Organizations

Welcome

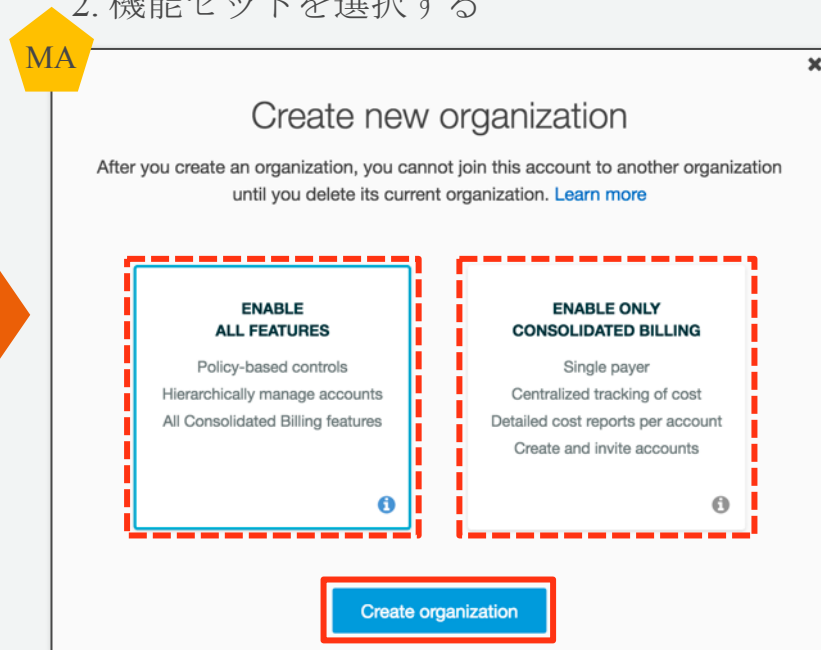
You can work with AWS Organizations in any of the following ways:

- [AWS Organizations Query API](#)
- [AWS Management Console](#)
- [AWS Command Line Tools](#)
- [AWS SDKs](#)

Invitations 0

**Create organization** [User guide](#)

## 2. 機能セットを選択する



MA

### Create new organization

After you create an organization, you cannot join this account to another organization until you delete its current organization. [Learn more](#)

**ENABLE ALL FEATURES**

- Policy-based controls
- Hierarchically manage accounts
- All Consolidated Billing features

**ENABLE ONLY CONSOLIDATED BILLING**

- Single payer
- Centralized tracking of cost
- Detailed cost reports per account
- Create and invite accounts

**Create organization**

# すべての機能を後から有効にする (1/2)

以前から一括請求を利用していた場合や新規の組織作成時に一括請求のみとしていた場合は、すべての機能を後から有効にする事ができる。

1. マスターアカウントの設定ですべての機能を有効にするプロセスを開始する

**MA**

Organization feature set:

Your organization currently supports consolidated billing only. This allows you to create and manage accounts in the organization and consolidate billing and payments. If you also want to apply service control policies (SCPs) to accounts in the organization, you must enable all features. All member accounts must approve enabling all features before SCPs can be applied.

<b>ENABLE ONLY CONSOLIDATED BILLING</b> Single payer Centralized tracking of cost Detailed cost reports per account Create and invite accounts <a href="#">Learn more</a>	<b>ENABLE ALL FEATURES</b> Policy-based controls Hierarchically manage accounts All Consolidated Billing features <a href="#">Learn more</a>
--	--

[Begin process to enable all features](#)

2. 組織内に登録されているメンバーアカウント全てで合意する

**A1**

Approve change

Your organization is requesting that you approve a change to enable all features (in addition to consolidated billing) for the organization. If you approve the change, the master account will have increased control over your account and its resources and will continue to pay for all costs associated with your account.

[Learn more](#)

After you enable all features in your organization, you can't return to supporting only consolidated billing features.

[Begin process to enable all features](#)

# すべての機能を後から有効にする (2/2)

3. マスターアカウントの設定で承認状況を確認する

MA

Organization feature set:

Your organization currently supports consolidated billing only. This allows you to create and manage accounts in the organization and consolidate billing and payments. If you also want to apply service control policies (SCPs) to accounts in the organization, you must enable all features. All member accounts must approve enabling all features before SCPs can be applied.

**ENABLE ALL FEATURES**

- Policy-based controls
- Hierarchically manage accounts
- All Consolidated Billing features

[Learn more](#)

The process to enable all features has started. After all member accounts approve the request, you can finalize the process and enable all features.

[View all feature request approval status](#)



4. 全てのアカウントで終了していれば、すべての機能を有効化できる

AWS Organizations

All accounts accepted the requests to enable all features.

[Finalize process to enable all features](#)

Accounts Organize accounts Policies

Organization settings > All feature request approval status

Resend all feature approval request [Cancel enabling all features](#)

Account name

No items to show

**Finalize process to enable all features**

Are you sure that you want to enable all features in this organization? You can't return to supporting only the consolidated billing features after you finalize this process.

[Finalize process to enable all features](#)

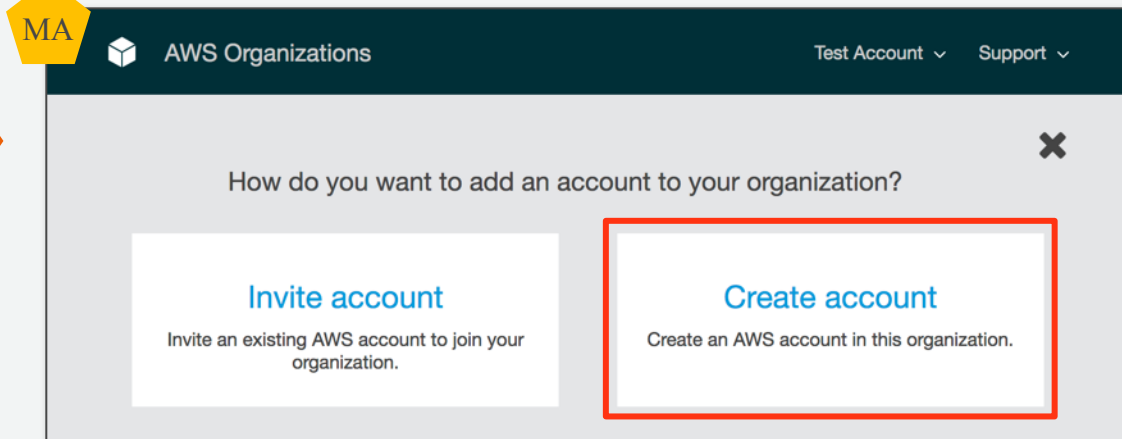
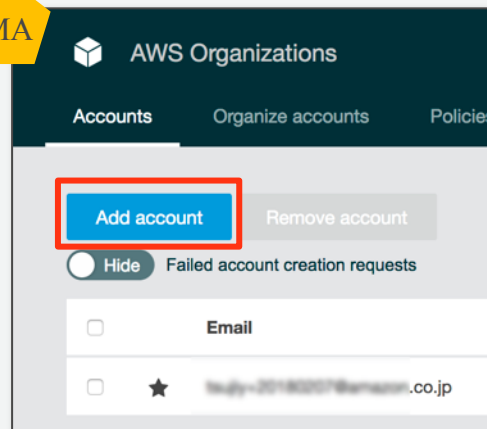
# 新規アカウントを作成 (1/2)

新しいアカウントを作成する。作成されたアカウントは組織に追加され、管理用ルートに配置される。

これまで**Web**から住所・クレジットカード情報入力、電話番号認証が必要だったアカウント作成が簡単にできる。

1. アカウントの追加を開始する

2. 追加方法として作成を選ぶ



# 新規アカウントを作成 (2/2)

3. 作成するアカウントの名前、メールアドレス、IAMロール名を指定して作成する

MA

Full name\*

Email\*

IAM role name

This account is created using the contact information address of the organization's master account.

\* Required fields

管理者権限のあるロールが新規アカウントに作成され、マスターアカウントとの信頼関係が設定される。

マスターアカウントからの管理を考えるとロール名は統一するのがおすすめ。

# 新規アカウントにログイン

AWS Organizationsで新規作成したアカウントに初回ログインするには以下方法がある。

- 📦 ルートアカウントのパスワードをリセットする
- 📦 スイッチロールする
- 📦 AWS SSOなどでフェデレーションしてログインする

招待して追加したアカウント含め、利用するユーザが複数のパスワードを覚えずに使える方法で集中管理するのがおすすめ。

# 新規アカウントにログイン - スイッチロール (1/2)

新規アカウント作成時にロール名を指定していれば、マスターアカウント内のIAMユーザやロールに権限を付与してログインできる。

1. 新規アカウントへのログインを許可する  
IAMユーザやロールにアクセス権限を付与する

```
MA {  
  "Version": "2012-10-17",  
  "Statement": [{  
    "Effect": "Allow",  
    "Action": "sts:AssumeRole",  
    "Resource":  
    "arn:aws:iam::123456789012:role/Organization  
AccountAccessRole"  
  }]  
}
```

**123456789012**は新規アカウントのAWS ID  
**OrganizationAccountAccessRole**は新規アカウント作成時に  
指定したロール名

2. ロールの切り替えの設定を開始する



# 新規アカウントにログイン - スイッチロール (2/2)

3. 切り替える先のアカウントのAWS IDとロールを指定する

MA

## ロールの切り替え

ロールを切り替えることによって、単一ユーザーを使用する AWS アカウント全体にわたるリソースを管理できるようになります。ロールを切り替えるときは、新しいロールに割り当てられるアクセス許可を一時的に使用します。このアクセス許可はロールの終了時まで使用され、その後は元のアクセス許可に戻ります。 [詳細はこちら](#)。

ロールの切り替え

許可します。AWS 管理者が...を設定してアカウントでロールの詳細が提供されるので、ロールを切り替えることができます。 [詳細はこちら](#)。

アカウント\*  ⓘ

ロール\*  ⓘ

表示名  ⓘ

色 a a a a a a

\*必須

キャンセル

ロールの切り替え

4. 新規アカウントでロールとして操作できるようになる

A1

OrganizationAccountAccessRole @ 031092254874 | パージニア北部 | サポート

役に立つヒント

コストの管理  
コストと使用量の予算に基づいて

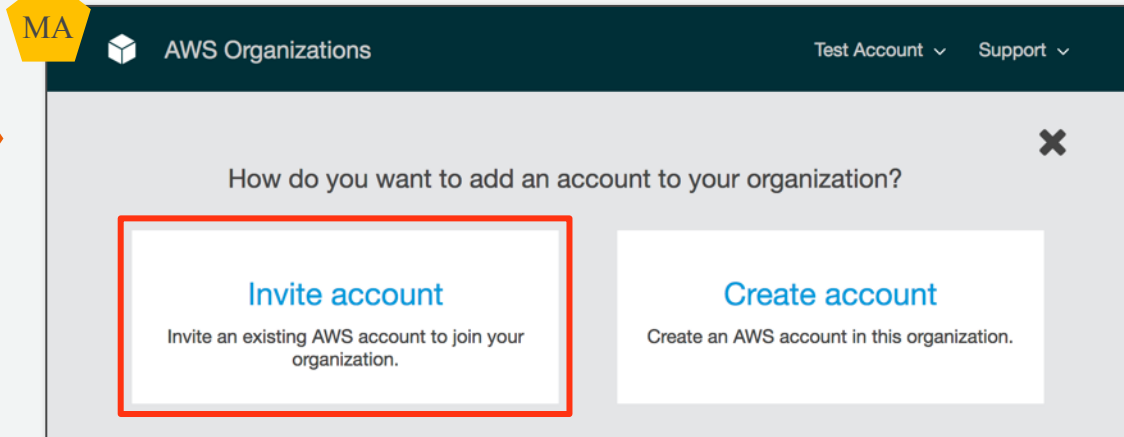
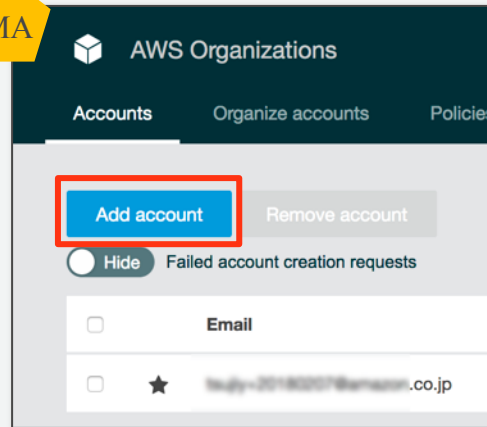
# 既存のAWSアカウントを組織内に追加する (1/3)

マスターアカウントから既存のAWSアカウントを招待をして、組織に追加できる。追加後は管理用ルートに配置され、SCPの適用や一括請求の対象となる。

マスターアカウントから管理するためのロールは作成されないため、必要に応じて手動で作成する。※AWS Organizations とサービスにリンクされたロールは自動作成される。

1. アカウントの追加を開始する

2. 追加方法として招待を選ぶ



# 既存のAWSアカウントを組織内に追加する (2/3)

3. 招待したいアカウントの指定とメッセージを入力して招待する

MA

Account ID or email\*

Enter multiple email addresses or account IDs separated by commas.

Notes

You may optionally include a note with your request.

\* Required fields

4. 対象アカウントで招待を確認する

A1

AWS Organizations

Welcome

You can work with AWS Organizations in any of the following ways:

- [AWS Organizations Query API](#)
- [AWS Management Console](#)
- [AWS Command Line Tools](#)
- [AWS SDKs](#)

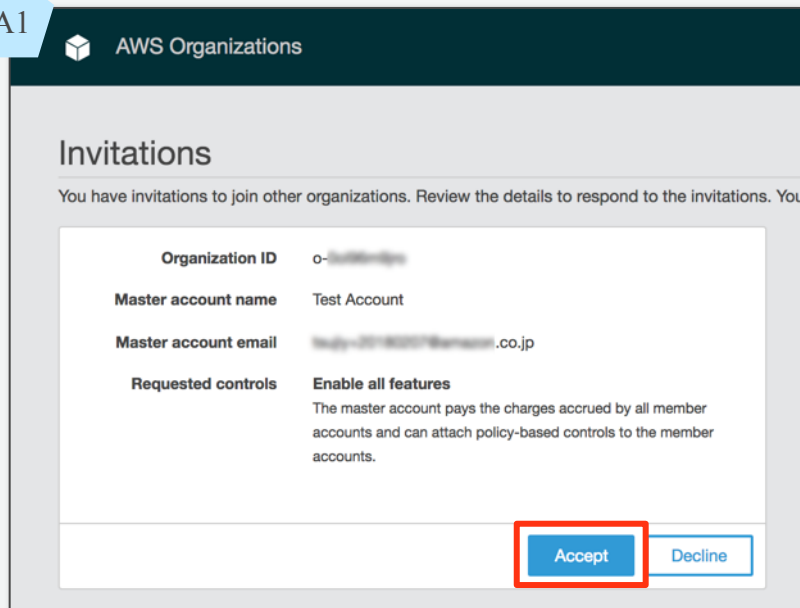
**Invitations 1**

Create organization

# 既存のAWSアカウントを組織内に追加する (3/3)

## 5. 招待内容を確認して、招待を受ける

A1



**Organization ID** o-123456789

**Master account name** Test Account

**Master account email** test@123456789.co.jp

**Requested controls** **Enable all features**  
The master account pays the charges accrued by all member accounts and can attach policy-based controls to the member accounts.

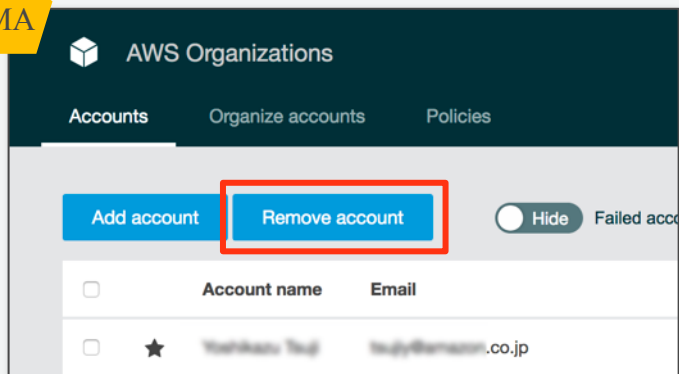
# 組織からアカウントを削除 (1/5)

Updated 2017.12  
AWS Organizationsで新規に作成した  
アカウントもご自身で削除可能に

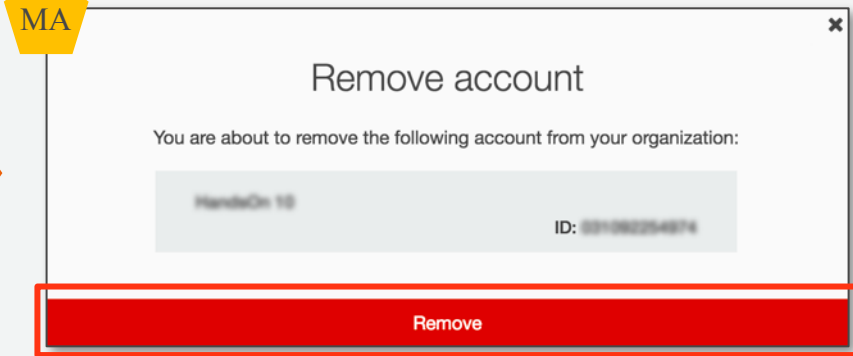
アカウントを組織内から削除できる。

削除されたアカウントは独立したアカウントとなり、個別に請求などが開始される。アカウント自体が消されるわけではなく、使い続けれる。

## 1. アカウントの削除を開始する



## 2. 削除する



# 組織からアカウントを削除 (2/5)

## 【AWS Organizationsで新規に作成したアカウントの場合】

3. 以下のメッセージが表示され、  
対象アカウントでサインアップ手続が必要

MA

### Remove account

One or more of the member accounts that you want to remove has not completed the account **sign-up steps**. Before you can remove the account from your organization, you must **sign in** to the account and provide the required information to operate as a standalone account. This might include:

- Providing contact information
- Providing a valid payment method
- Agreeing to the terms of the AWS Customer Agreement
- Completing phone verification
- Choosing a support option

HandOn 10 ID: 031062254874

Remove failed

Sign-in options ▶

4. URLをどちらかの方法で開く

MA

### Sign-in options

Copy and paste the sign-in link below into a **different browser application** or a **private, incognito browser window** to access the member account and provide the required information. This keeps you signed in to your current session.

<https://031062254874.signin.aws.amazon.com/cons> [Copy link](#)

OR

Choose **Sign in** to access the member account in this window and provide the required information. **This signs you out of your current session.**

HandOn 10 ID: 031062254874 [Sign in](#)

※招待して追加したアカウントではサインアップ手続きは必要ないが、  
今も有効な支払い方法が登録されているかなどを再確認。

# 組織からアカウントを削除 (3/5)

5. ルートアカウントのログインに切り替える

6. 削除したいアカウントのメールアドレスを入力する

7. ルートアカウントのパスワードがわからない場合はリセットしてパスワードを入力する



aws

アカウント:

ユーザー名:

パスワード:

[サインイン](#)

[ルートアカウント認証情報を使用してサインイン](#)



aws

### サインイン ⓘ

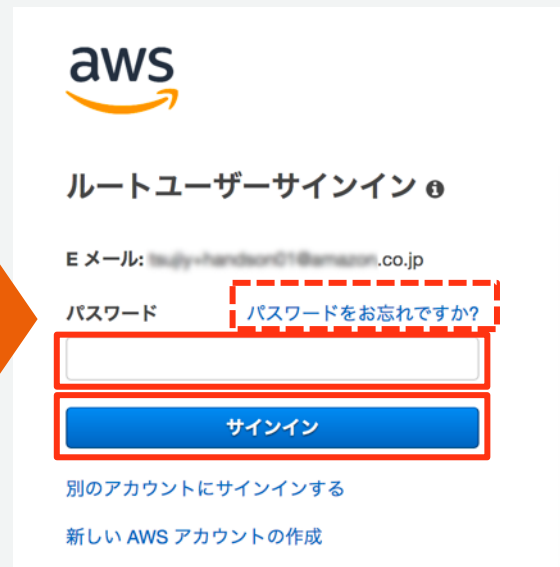
AWS アカウントの E メールアドレス

IAM ユーザーとしてサインインするには、アカウント ID または アカウントエイリアスを入力してください。

[次へ](#)

— AWS のご利用は初めてですか? —

[新しい AWS アカウントの作成](#)



aws

### ルートユーザーサインイン ⓘ

E メール:

パスワード

[サインイン](#)

[別のアカウントにサインインする](#)

[新しい AWS アカウントの作成](#)

# 組織からアカウントを削除 (4/5)

8. 連絡先情報を入力する

A1

連絡先情報

すべてのフィールドは必須です。

アカウントの種類を選択し、次のフィールドに連絡先の詳細を入力してください。

アカウントの種類  プロフェッショナル  パーソナル

フルネーム

会社名

電話番号

国/地域  
アメリカ

AWS カスタマーアグリーメント の諸条件を確認済みで、同意する場合はここをチェックしてください

アカウントを作成して続行

9. 支払情報を入力する

A1

支払情報

お客様の身元を確認できるように、支払い情報を入力してください。使用量が **AWS 無料利用枠の上限** を超えない限り、お客様には課金されません。詳細については、よくある質問をご確認ください。

クレジット/デビットカード番号

有効期限日  
02 2018

カード保有者の氏名

請求先住所  
 連絡先住所を使用する

新しい住所を使用する

セキュアな送信

10. 電話による確認に対応する

A1

電話による確認

すぐにお客様に自動通話が発信されます。求められたら、AWS ウェブサイトからの 4 桁の番号を電話のキーボードで入力してください。

電話番号の入力  
以下に情報を入力し、[すぐに連絡を受ける] をクリックしてください。

国/地域コード  
日本 (+81)

電話番号 内線

セキュリティチェック

aw6n7b

上に表示された文字を入力してください

すぐに連絡を受ける

※連絡先情報入力の画面が出ない場合は、再度4のURLを入力する

# 組織からアカウントを削除 (5/5)

## 11. サポートプランを選択する

A1

### サポートプランの選択

AWS では、お客様のニーズに合ったさまざまなサポートプランをご用意しています。お客様の AWS の使用に最も合ったサポートプランを選択してください。詳細はこちら



#### ベーシックプラン

無料

- すべてのアカウントに含まれています
- フォーラムとリソースへの 24 時間 365 日対応のセルフサービスアクセス
- セキュリティとパフォーマンスを向上させるためのベストプラクティスのチェック
- ヘルステータスと通知へのアクセス



#### 開発者プラン

29 USD/月～

- 早期の採用、テスト、開発
- AWS サポートへの営業時間中の E メールでのアクセス
- 1 人の主な担当者による無制限のサポートケースのオープンが可能
- 非実稼働システムに対する 12 時間の応答時間



#### ビジネスプラン

100 USD/月～

- 実稼働のワークロードおよびビジネスクリティカルな依存関係使用
- AWS サポートへの 24 時間 365 日のチャット、電話、E メールでのアクセス
- 無制限の担当者による無制限のサポートケースのオープンが可能
- 実稼働システムに対する 1 時間の応答時間

#### エンタープライズレベルのサポートが必要ですか？

AWS でのビジネスワークロードおよびミッションクリティカルなワークロードの実行の詳細については、アカウントマネージャーにお問い合わせください (15,000 USD/月～)。詳細はこちら

## 12. 組織から外す

A1



### AWS Organizations

Your account belongs to the following organization:

Organization ID:

o-~~(banned)~~

Master account email:

testy@amazon.co.jp

Leave organization

Organization features enabled

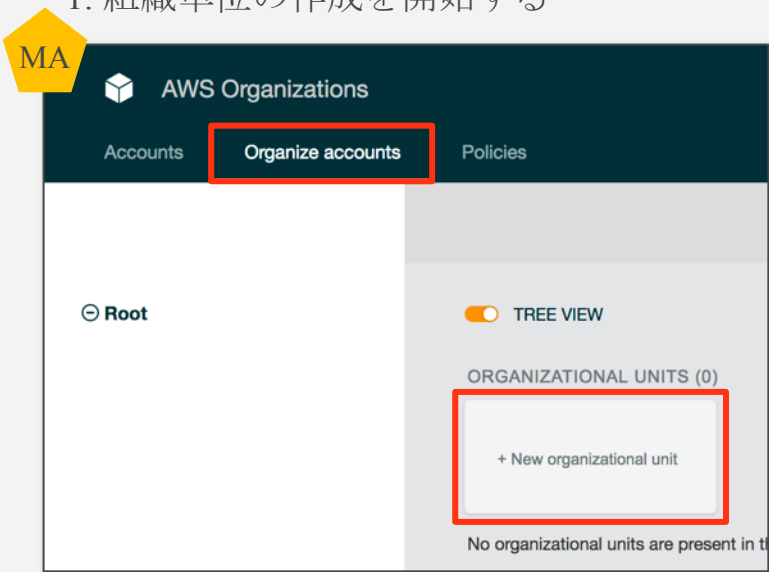
All features enabled: The organization that your account is in pays for your account and can apply organization policies that can restrict what your account can do.

[Learn more](#)

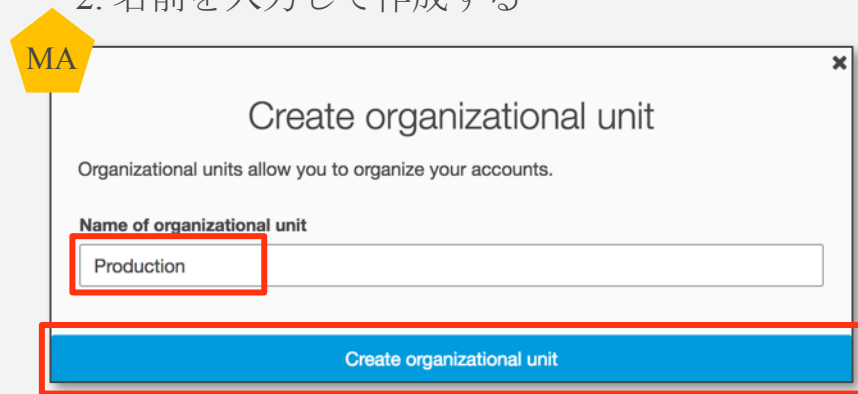
# 組織単位 (OU) の作成

アカウントの整理やポリシーの一括適用のために、組織単位 (OU) を作成して、アカウントを入れる事ができる。

1. 組織単位の作成を開始する



2. 名前を入力して作成する



# サービスコントロールポリシー (SCP) (1/6)

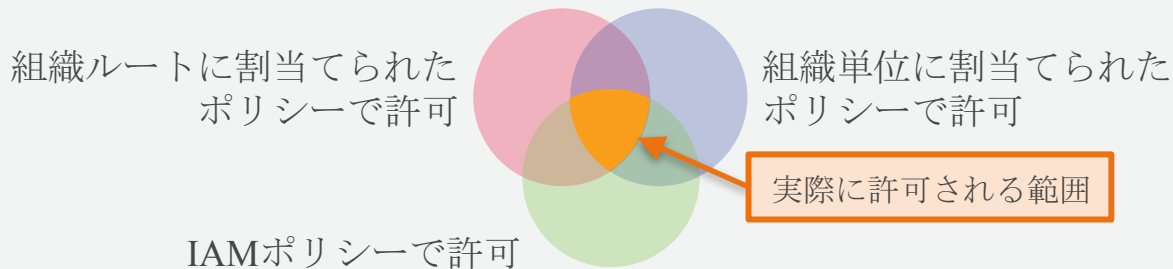
利用できる唯一の組織ポリシーのタイプで以下の事ができる。

- ❏ 組織内の以下に対して割当てることができる、階層構造に基づいて継承して適用される。
  - 組織ルート
  - 組織単位 (OU)
  - アカウント
- ❏ マスターアカウントは適用対象外。メンバーアカウントでは、IAMユーザ・ロールだけではなくルートアカウントも対象。
- ❏ サービスやAPIのアクションへのアクセス制限を許可・禁止できる。  
※対象のプリンシパルやリソースを指定する事はできず、全体に許可・禁止が適応される。

# サービスコントロールポリシー (SCP) (2/6)

ポリシーの許可・拒否は以下のように機能する。

- ❏ 複数のポリシーがアカウントに適応される場合、許可は**AND**条件となる。
- ❏ アカウント内のアクセス権限に対してフィルタとして動作する。
  - 許可：**SCP**は必要条件だが、十分条件ではない。**SCP**で許可されていても**IAM**ポリシーやリソースポリシーで許可されていないと、利用できない。



- 拒否：**SCP**で拒否とすると他で許可されていても、利用できない。

SCPやIAMポリシーで明示的に拒否 > IAMポリシーとSCPで許可 > 暗示的拒否 (デフォルト)

# サービスコントロールポリシー (SCP) (3/6)

実際にはポリシーを使って以下のどちらの方式で管理する事が考えられる。

**ブラックリスト方式** 特定のサービスやアクションを**禁止**するポリシーを作成し割当て

**ホワイトリスト方式** 特定のサービスやアクションを**許可**するポリシーを作成し割当て

- 📦 ホワイトリストで管理する場合は、デフォルトで割当てられている全サービスを許可する「FullAWSAccess」を削除する。
- 📦 ユースケースとしては社内ルールや規制、特定の第三者認証の有無に基づき特定サービスのみ提供したい場合に制限する事が考えられる。

# サービスコントロールポリシー (SCP) (4/6)

ポリシーはIAMと同じ構文ルール。制御は **Effect** と **Action** の内容で実現する。**Resource** は \* で固定、**Principal** は利用不可となっている。

ポリシー例：

全サービスを許可 (FullAWSAccess)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

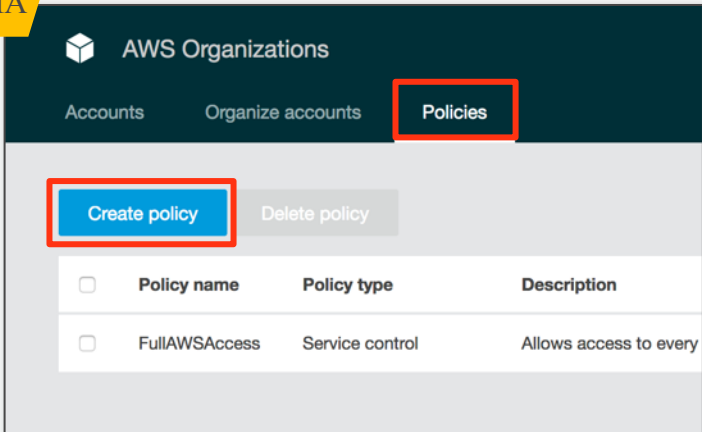
S3のみを許可

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

# サービスコントロールポリシー (SCP) (5/6)

1. ポリシー作成を開始する

MA



AWS Organizations

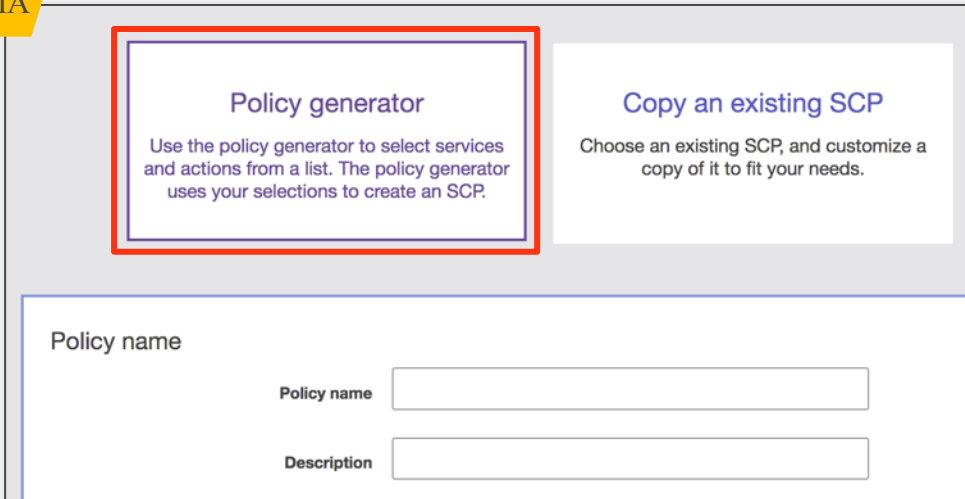
Accounts Organize accounts **Policies**

**Create policy** Delete policy

<input type="checkbox"/>	Policy name	Policy type	Description
<input type="checkbox"/>	FullAWSAccess	Service control	Allows access to every

2. ポリシーの作成方法を選択する

MA



**Policy generator**  
Use the policy generator to select services and actions from a list. The policy generator uses your selections to create an SCP.

**Copy an existing SCP**  
Choose an existing SCP, and customize a copy of it to fit your needs.

Policy name

Policy name

Description

# サービスコントロールポリシー (SCP) (6/6)

## 3. ポリシー名やポリシー内容を設定して作成する

MA

Policy name

Policy name

Description

Choose effect

Choose Overall Effect  Deny

Select Deny to block all users and roles from accessing the services and actions that you specify below.

Service APIs that are listed in your policy will be blocked by default.

Statement builder

Select Service  Select action

+ Add statement

Service	Actions	Effect
Amazon S3	*	Allow <input type="button" value="✕"/>

# その他の行える操作

## 📦 組織

- 組織を削除

## 📦 アカウント

- アカウントを特定の組織単位に移動

## 📦 組織単位 (OU)

- 組織単位を削除
- 組織単位の名前を変更

## 📦 ポリシー

- ポリシーの削除
- ポリシーの変更
- ポリシーを管理用ルート、組織、アカウントに割り当て
- ポリシーを管理用ルート、組織、アカウントから割り当て解除

# AWS CLIで操作

マネージメントコンソールと同じ操作がAWS CLIでも行える。リージョンは **us-east-1** にする。

※請求情報などの登録はAWS Organizationsの一部ではなく、AWS CLIから行えないため削除の完全自動化は行えない。

## 📦 組織を作成する

- すべての機能を有効
- 一括請求のみを有効

```
$ aws --region us-east-1 organizations create-organization --feature-set ALL
```

```
$ aws --region us-east-1 organizations create-organization --feature-set CONSOLIDATED_BILLING
```

## 📦 新規アカウントを作成する

```
$ aws --region us-east-1 organizations create-account --email user@example.com --account-name "Account Friendly Name" --role-name OrganizationAccountAccessRole --iam-user-access-to-billing ALLOW
```

※メンバーアカウントのIAMユーザに請求情報の参照を許可するか指定できる。

## 📦 既存アカウントを招待する

```
$ aws --region us-east-1 organizations invite-account-to-organization --target Id=123456789012,Type=ACCOUNT
```

# 一括請求について

# 一括請求 (Consolidated Billing)

組織内の全てのAWSアカウントの利用料が1つの請求として、まとめてマスターアカウントにされるようになる。

📦 AWS Organizations 提供前の一括請求と同じ。

📦 ボリュームディスクアカウントが合算して計算される。

📦 リザーブドインスタンスによる割引がデフォルトで共有される。

(特定アカウントに割引が共有されないよう設定可能) Updated 2017.11

📦 各アカウントの請求額も確認できるが、リザーブドインスタンスによる割引が共有された状態での請求額となる。

📦 使用状況レポートでは割引を共有しない場合の料金 (Unblended Rate) も確認が可能。

# 複数**AWS**アカウント利用のメリット

# 一般的な課題

本格的にAWSを使い始めると・・・

権限



を

プロジェクト  
単位

本番環境  
開発環境

で明確に分離

料金



エンドユーザ  
企業単位

など

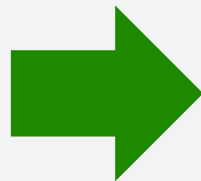
という必要が出てくる事が多い

# 1 アカウントのみで分離

分離する方法はあるが、要件によっては分離しきれない場合がある。

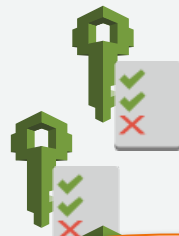


AWS リソース



IAMユーザと  
IAMポリシー

使用状況レポート  
とタグ付け

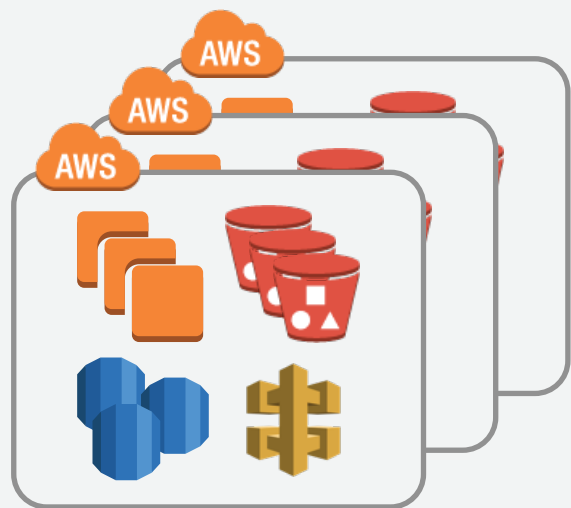
A document icon with a white background and a folded top-right corner. It features a large green dollar sign (\$) at the top left. Below it is a table with two columns: 'リソース' (Resources) and 'タグ' (Tags).

リソース	タグ
AAAA	PJ-A
	PJ-B
	PJ-A

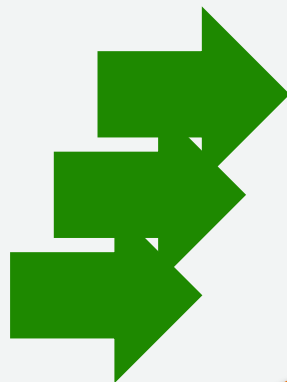
要件によっては  
分離しきれない

# 複数アカウントにして分離

複数アカウントにすることで明確に分離できるようになる。  
複雑になってしまうため、トレードオフを考慮して複数アカウントにすることがおすすめ。



AWS リソースを  
別々の AWS アカウントに分離



アカウントを越えて  
・データコピー  
・ネットワーク接続  
・一括請求  
も可能

デメリットがあるが  
解決策もある

# 2つの方式を比較 (1/2)

## 1アカウントのみで分離

## 複数アカウントにして分離

### 権限の分離

○ IAM Policyで権限制御  
(実現したい制御内容によっては実現が難しかったり、管理に手間がかりすぎる場合もある。)

◎ IAM Policyに加えてアカウントで区切って権限制御  
(AWS Organizationのポリシーでアカウントを越えた制御も追加で可能。)

### 料金の分離

△ リソースタグを付けて使用状況レポートで確認  
(リソースタグに対応していないサービスやトラフィックなどはコストを分離できない。また、タグ付けや集計に手間がかかる。リザーブドインスタンスを個別に適用などはできない。)

○ アカウントごとに料金が明記される  
(デフォルトではRIによる値引きが共有されてBlended Rateが適用されるが、無効にする事もできる。値引きを共有しつつも、値引きを特定アカウント優先で適応した料金を確認するにはRIを該当アカウントで購入し、Unblended Rateでの料金計算が必要。)

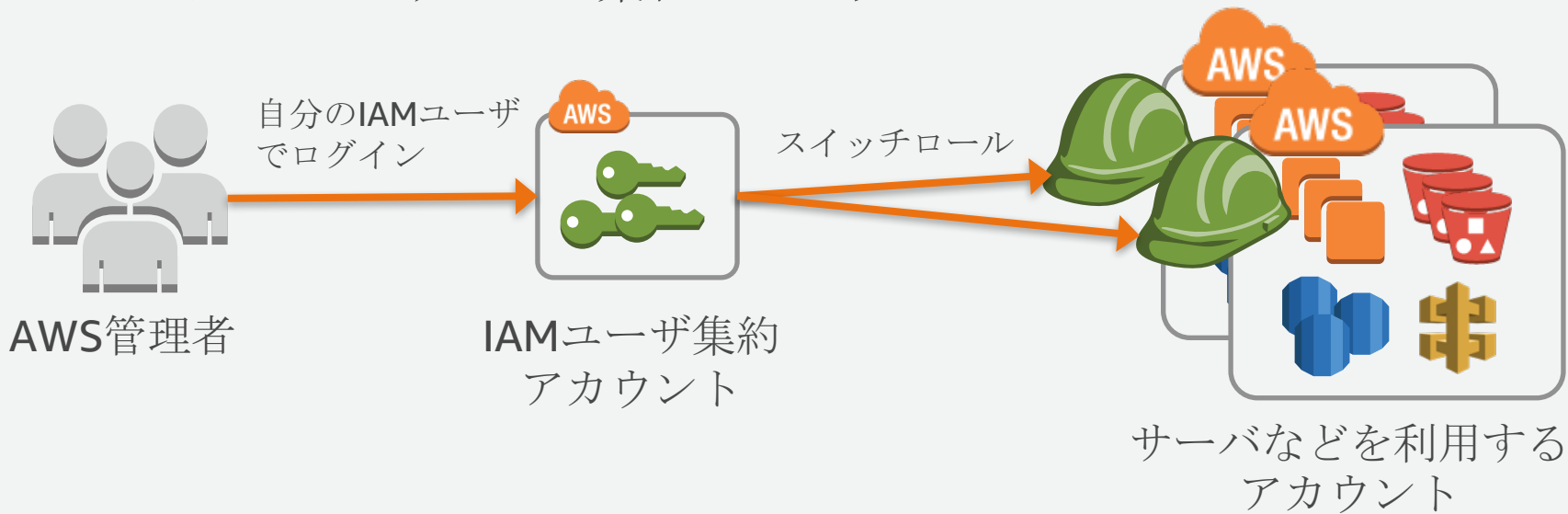
## 2つの方式を比較 (2/2)

	1アカウントのみで分離	複数アカウントにして分離
支払い	○	○ <b>AWS Organizations</b> で一括請求
料金	○	○ ボリュームディスカウントの合算やRI値引きの共有が行われる
VPN/Direct Connect	○ 1つのVPCしか使わない場合は1接続で対応できる	△ VPN接続はVPCごとに必要、Direct ConnectはキャリアサービスによってはVPCごとの契約が必要 (VPCごとではないサービスもあり)
管理ユーザの管理	○	○ AWS SSOやスイッチロールで管理ユーザを管理する手間を抑えられる
システム間連携	○	○ VPC Peeringやスナップショット共有などの機能あり

# AWS管理ユーザの管理 (1/2)

AWS管理者がAWSを操作する際に適切にログが残るように、個人ごとのIAMユーザを利用する事が通常望ましい。ただし、複数のAWSアカウントを利用する場合は、重複して管理しなくて済むように2つの方法がある。

## 📦 IAMユーザを1アカウントに集約しスイッチロール



# AWS管理ユーザの管理 (2/2)

## 📦 AWS SSOを利用

AWS SSOを利用すると、社内の既存のActive Directoryユーザのユーザ名・パスワードで複数のAWSアカウントのマネジメントコンソールへSSOを実現できる。



 最後に

# AWS Organizationsを活用したサービス

## AWS SSO

Active DirectoryユーザにAWS Organizationsの組織内にあるAWSアカウントを対象に、マネージメントコンソールへのSSOを提供する。

## AWS CloudFormation

CloudFormationのスタックセットはテンプレートをAWS Organizationsの組織単位を対象に複数のAWSアカウントにまたがってデプロイできる。

# 最後に

複数AWSアカウントを使い分けしやすい  
仕組みが整ってきている。

セキュリティ要件やネットワーク構成、  
利用料管理を考慮して、積極的に活用下さい。

# 参考URL

## 📦 AWS Organizations 開始時のブログ記事

<https://aws.amazon.com/jp/blogs/news/aws-organizations-policy-based-management-for-multiple-aws-accounts/>

## 📦 AWS Organizations を使って End-to-End でアカウント作成を自動化する方法

<https://aws.amazon.com/jp/blogs/security/how-to-use-aws-organizations-to-automate-end-to-end-account-creation/>

## 📦 Re:Invent 2017セッション

- SID311 Designing Security and Governance Across Multiple AWS Accounts  
<https://www.youtube.com/watch?v=71fD8Oenwxc>
- SID321 How Capital One Applies AWS Organizations Best Practices to Manage Multiple AWS Accounts  
<https://www.youtube.com/watch?v=ZKpkF17d0Oo>
- SID331 Architecting Security and Governance Across a MultiAccount Strategy  
<https://www.youtube.com/watch?v=71fD8Oenwxc&t=20s>

# FAQ

## 📦 マスターアカウントを別のアカウントに変更するには？

変更するには一旦全てのメンバーアカウントを削除してから組織を削除して、新しいマスターアカウントで組織を再作成し、全てのメンバーアカウントを招待する流れとなる。アカウント数が多い場合はかなり手間がかかるため、組織作成時は慎重にマスターアカウントを選択する事。

## 📦 メンバーアカウントを登録している組織を変えるには？

まずメンバーアカウントを組織から削除してから、組織に招待する。一時的に、独立したアカウントとなるため、その間の請求がそのアカウントの請求先に発生する可能性があるため注意。

## 📦 AWSアカウントを組織から削除ではなく、利用停止したい場合は？

対象アカウントを組織から削除した上で、そのアカウントの解約操作を行う。

## 📦 メンバーアカウントがさらに組織を作れないか？

組織を多重構成にすることはできない。現在の組織の構成を見直して対応を。

# オンラインセミナー資料の配置場所

## AWS クラウドサービス活用資料集

- <http://aws.amazon.com/jp/aws-jp-introduction/>

			
<b>サービス別資料</b>	<b>ソリューション別資料</b>	<b>業種別資料</b>	<b>その他の資料</b>
無料オンラインセミナー「Black Belt Online Seminar」のサービスカット資料他、AWSのTechメンバーによる各サービスの解説資料がご覧いただけます。	無料オンラインセミナー「Black Belt Online Seminar」のソリューションカット資料他、特定のソリューションについてのAWS活用方法がご覧いただけます。	無料オンラインセミナー「Black Belt Online Seminar」のインダストリーカット資料他、特定の業界のユースケースがご覧いただけます。	イベントに関する資料やアップデート情報などがご覧いただけます。

## AWS Solutions Architect ブログ

- 最新の情報、セミナー中のQ&A等が掲載されています
- <http://aws.typepad.com/sajp/>

# 公式Twitter/Facebook AWSの最新情報をお届けします



@awscloud\_jp



検索

もしくは  
<http://on.fb.me/1vR8yWm>

最新技術情報、イベント情報、お役立ち情報、  
お得なキャンペーン情報などを日々更新しています！

# AWSの導入、お問い合わせのご相談

AWSクラウド導入に関するご質問、お見積り、資料請求をご希望のお客様は以下のリンクよりお気軽にご相談ください

<https://aws.amazon.com/jp/contact-us/aws-sales/>

お問い合わせ	<h2>日本担当チームへのお問い合わせ</h2>
日本担当チームへのお問い合わせ >	AWS クラウド導入に関するご質問、お見積り、資料請求をご希望のお客様は、以下のフォームよりお気軽にご相談ください。平日営業時間内に日本オフィス担当者よりご連絡させていただきます。
関連リンク フォーラム	※ご請求金額またはアカウントに関する質問は <a href="#">こちらからお問い合わせください</a> 。 ※Amazon.com または Kindle のサポートに問い合わせは <a href="#">こちらからお問い合わせください</a> 。
	アスタリスク(*)は必須情報となります。  姓* <input type="text"/>  名* <input type="text"/>

※「AWS 問い合わせ」で検索してください

aws

