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います。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.

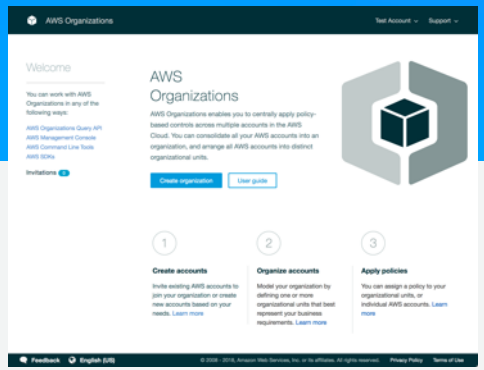
Agenda

- 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



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)

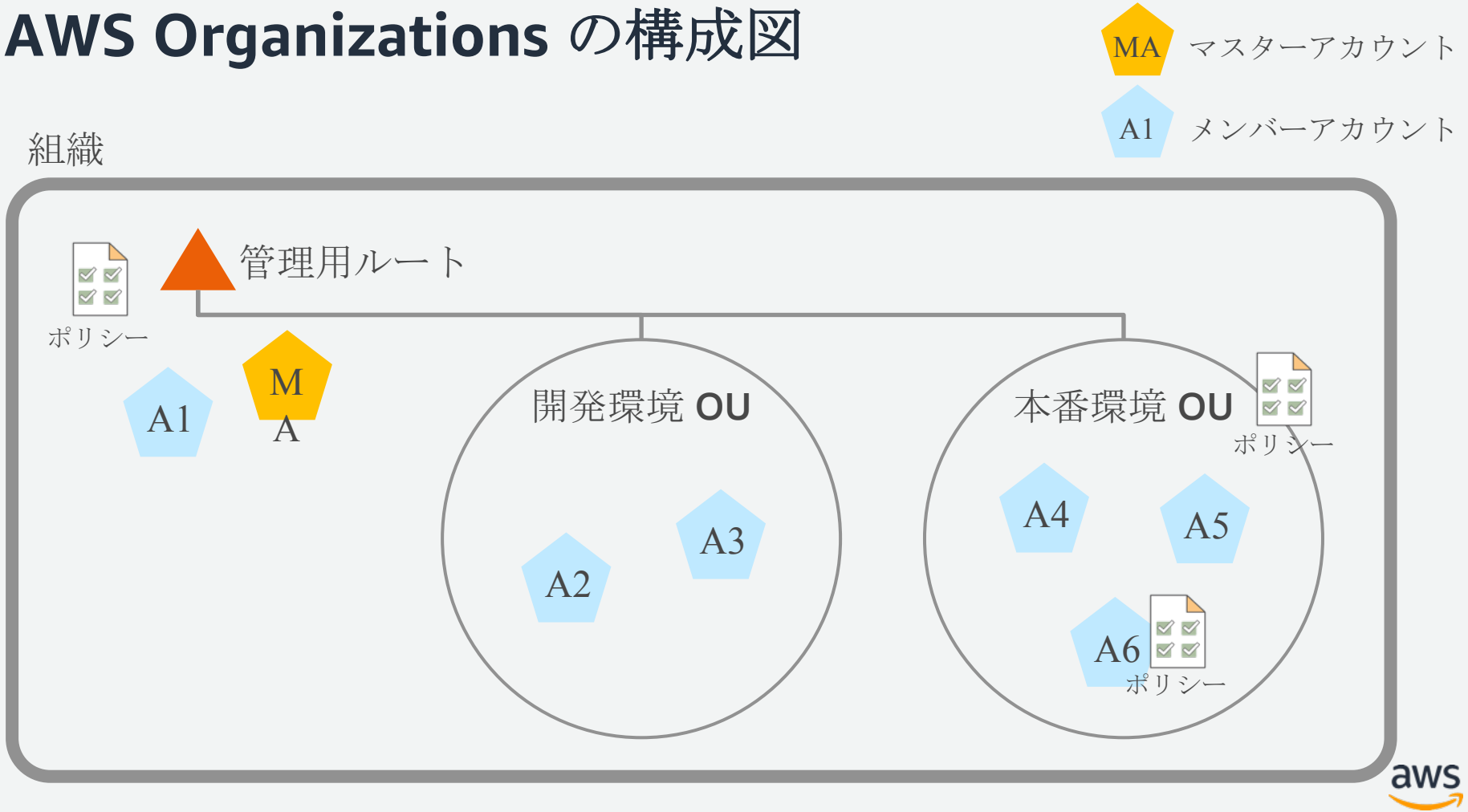
請求の簡素化

- 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	▪ 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 ▪ 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 ▪ AWS Organizationsで管理する最小単位
組織 (Organization)	▪ AWS Organizationsで一元管理する対象の全体 ▪ 複数AWSアカウントのセット
マスターアカウント	▪ AWS Organizations組織の全体を管理する権限を持つAWSアカウント
メンバーアカウント	▪ 組織内にあるマスターアカウント以外のAWSアカウント
組織単位 (OU)	▪ 組織内にある複数AWSアカウントのグループ
管理用ルート (root)	▪ 組織単位 (OU) 階層の開始点
組織ポリシー	▪ 組織内で適用してAWSアカウントを管理する仕組み
サービス管理ポリシー (SCP)	▪ 現在サポートされている唯一の組織ポリシーのタイプ ▪ 利用できるAWSサービスとアクションを制御

AWS Organizations の構成図



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) Consolidated Billing Only	(すべての機能) 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

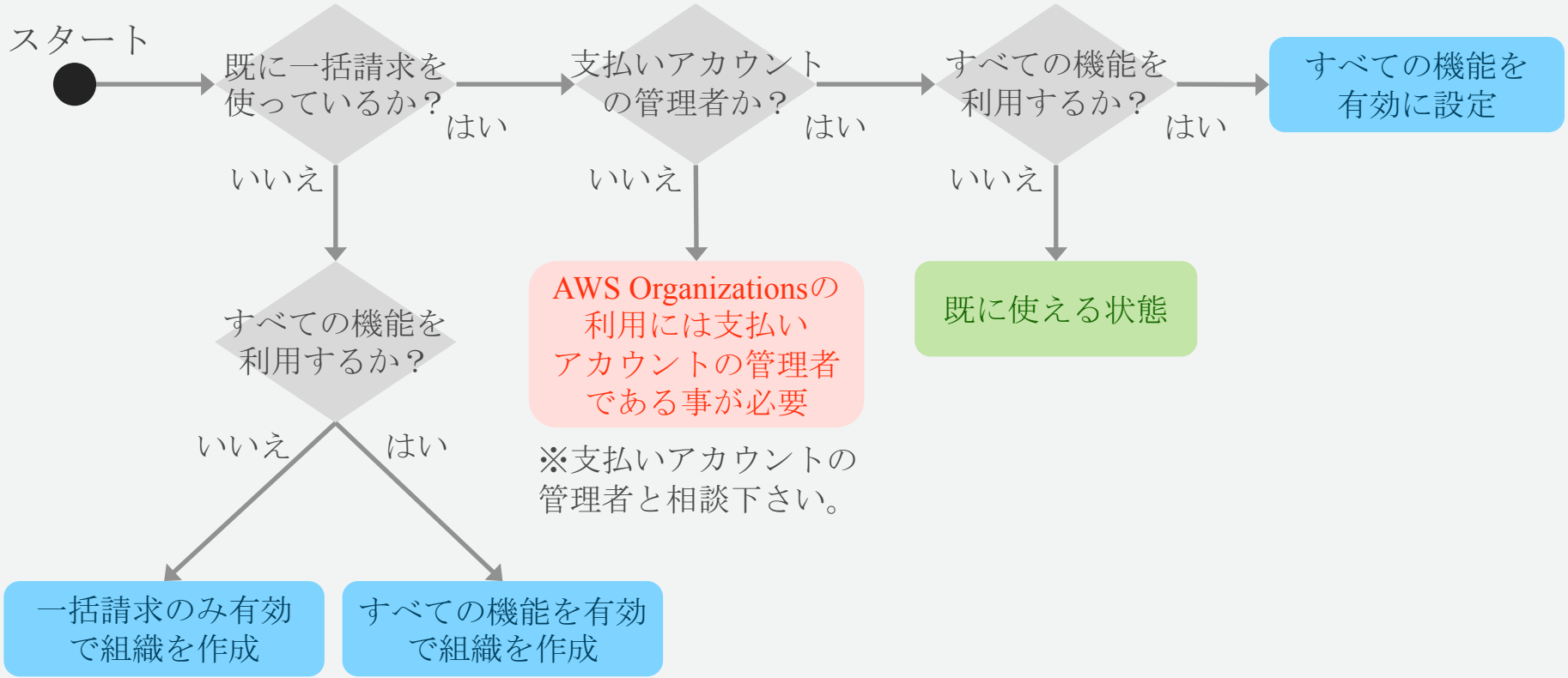
どのAWSアカウントをマスターカウントとするか選択する。

- 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。

aws

組織の作成 と 機能の有効化

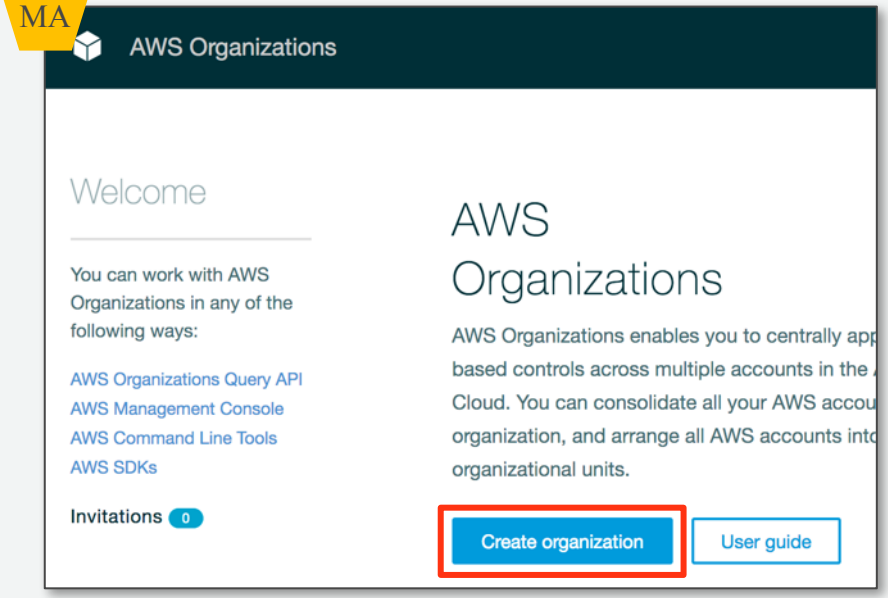


機能・操作について

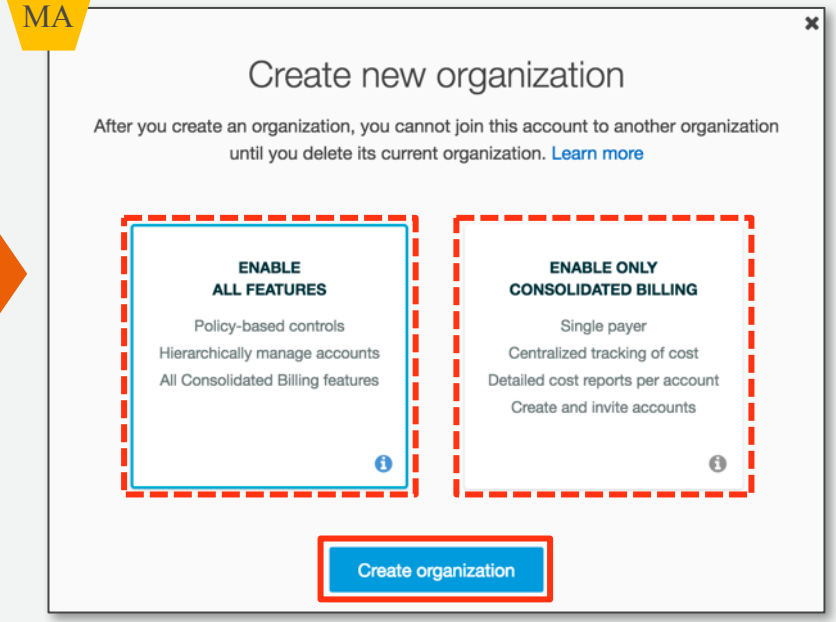
組織を作成する

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



2. 機能セットを選択する



https://docs.aws.amazon.com/ja_jp/organizations/latest/userguide/orgs_manage_create.html

すべての機能を後から有効にする (1/2)

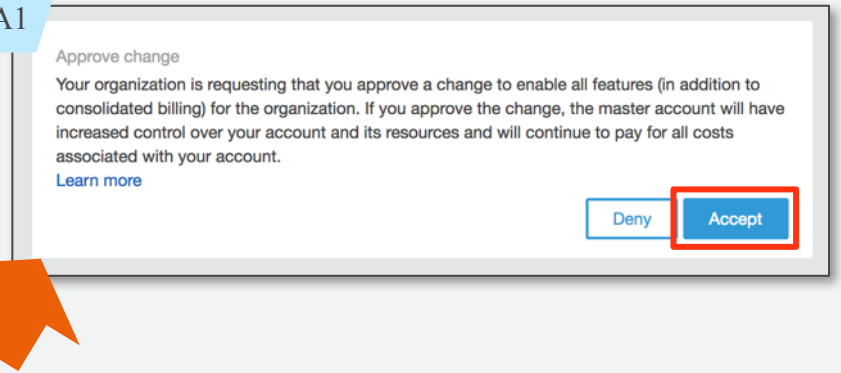
以前から一括請求を利用していた場合や新規の組織作成時に一括請求のみとしていた場合は、すべての機能を後から有効にする事ができる。

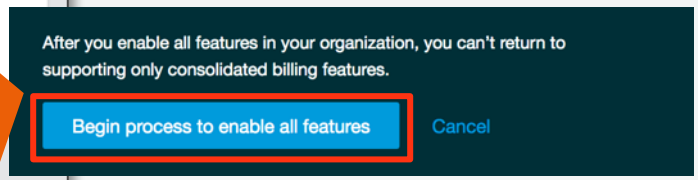
1. マスターアカウントの設定ですべての機能を有効にするプロセスを開始する

MA

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



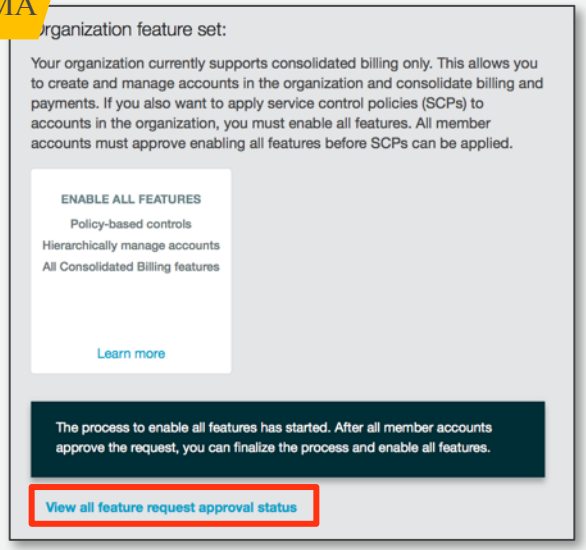


https://docs.aws.amazon.com/ja_jp/organizations/latest/userguide/orgs_manage_org_support-all-features.html#manage-begin-all-features

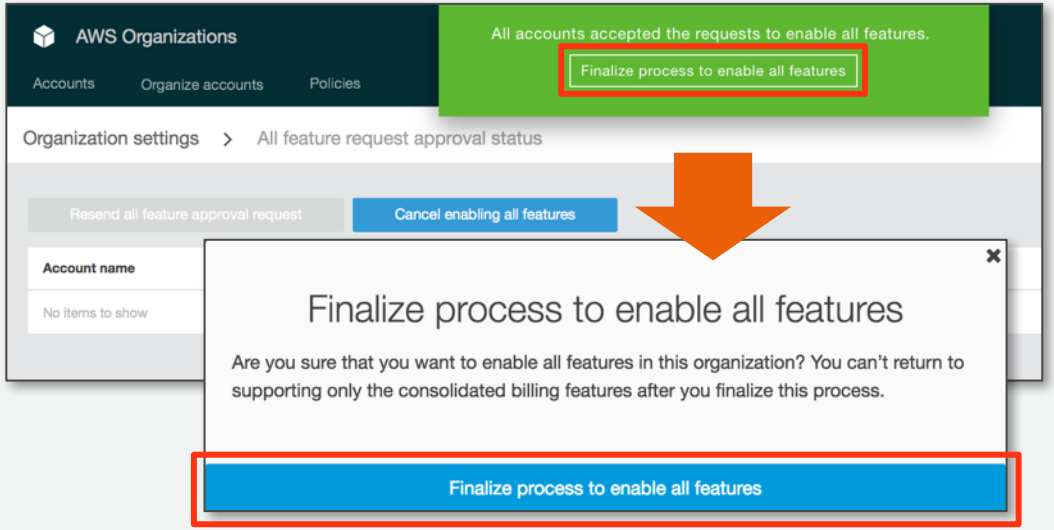
すべての機能を後から有効にする (2/2)

3. マスターアカウントの設定で
承認状況を確認する

MA



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

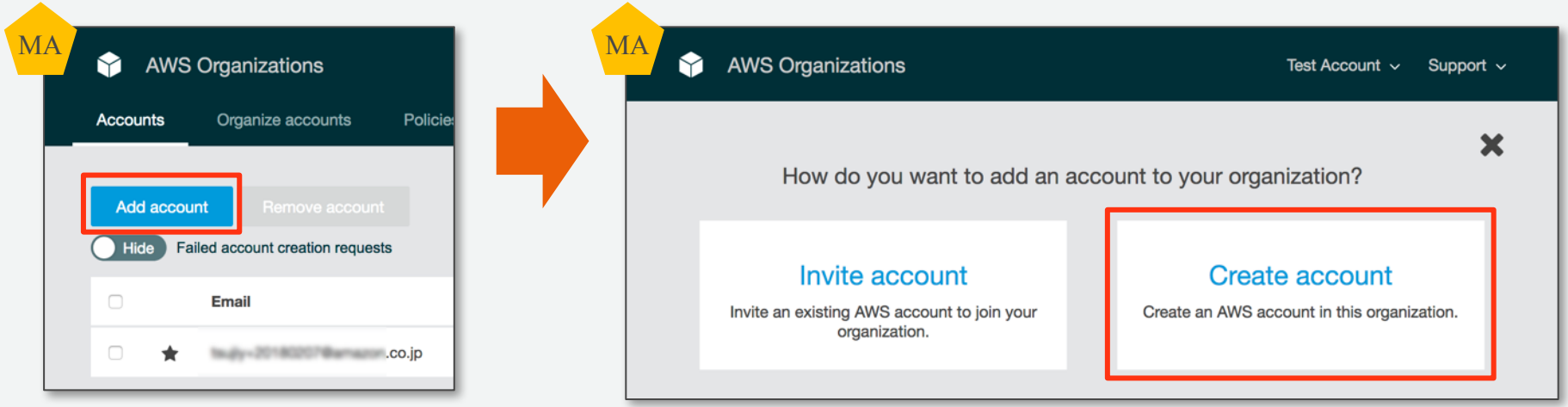


新規アカウントを作成 (1/2)

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

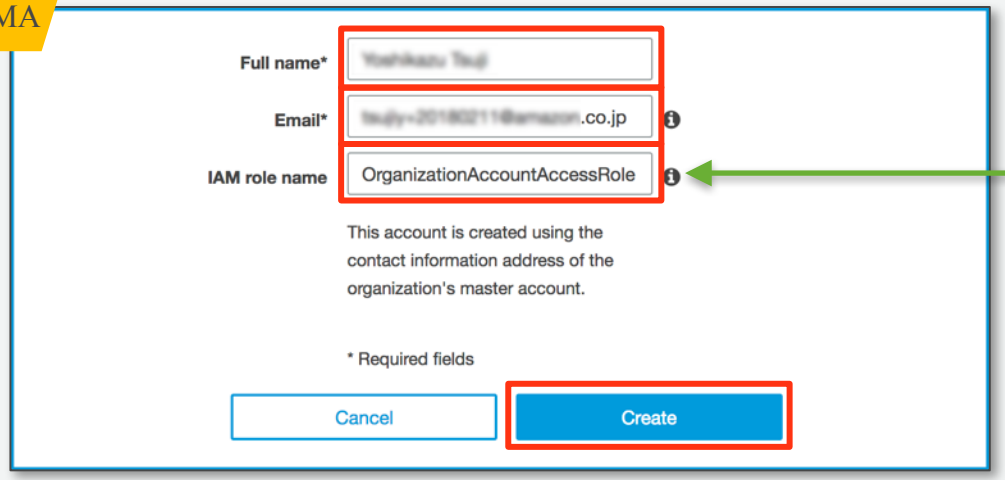


https://docs.aws.amazon.com/ja_jp/organizations/latest/userguide/orgs_manage_accounts_create.html

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



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。

https://docs.aws.amazon.com/ja_jp/organizations/latest/userguide/orgs_manage_accounts_access.html

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

MA

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_roles_use_switch-role-console.html

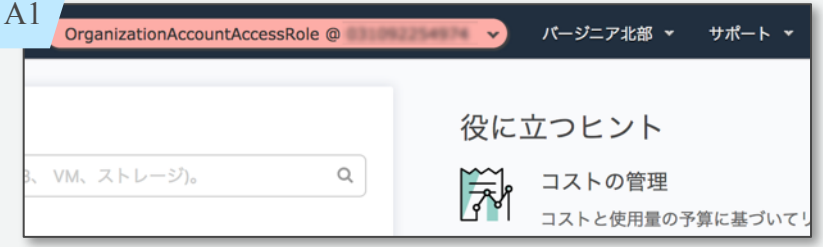
新規アカウントにログイン – スイッチロール (2/2)

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

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

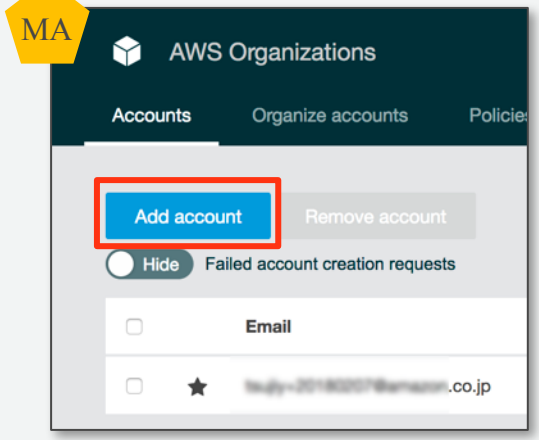


既存のAWSアカウントを組織内に追加する (1/3)

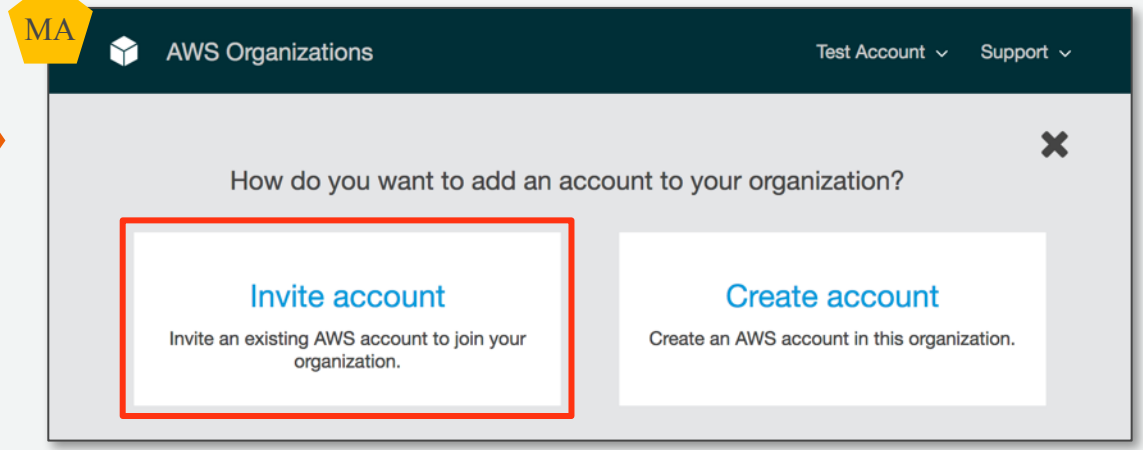
マスターアカウントから既存のAWSアカウントを招待をして、組織に追加できる。追加後は管理用ルートに配置され、SCPの適用や一括請求の対象となる。

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

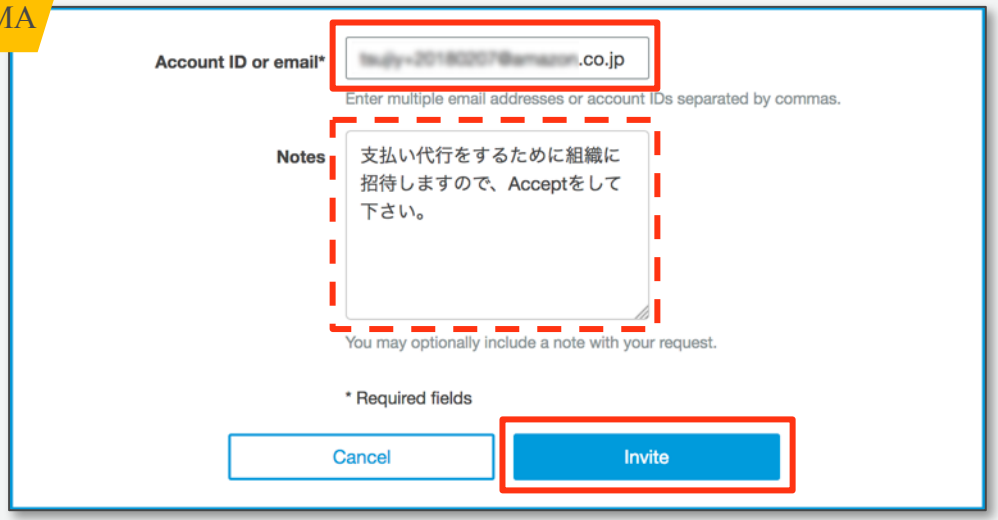


https://docs.aws.amazon.com/ja_jp/organizations/latest/userguide/orgs_manage_accounts_invites.html

既存のAWSアカウントを組織内に追加する (2/3)

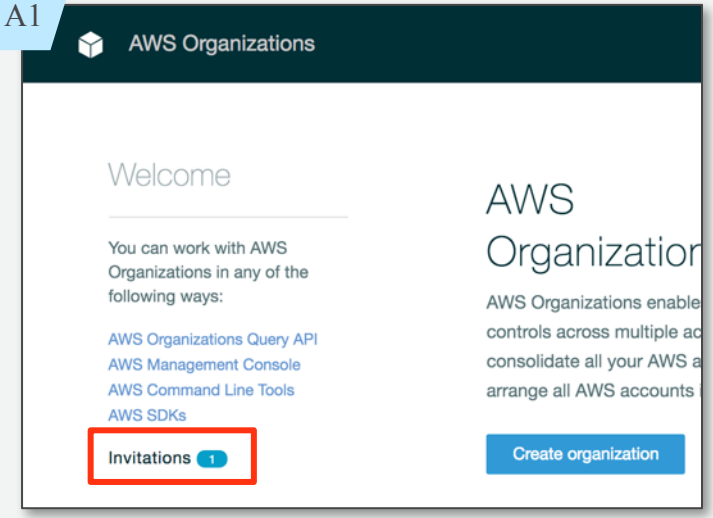
3. 招待したいアカウントの指定と
メッセージを入力して招待する

MA



4. 対象アカウントで招待を確認する

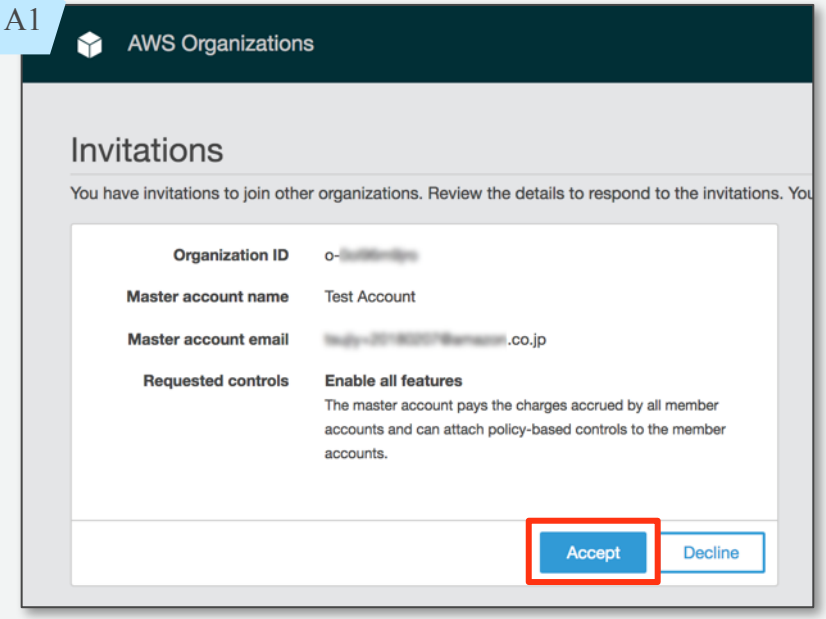
A1



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



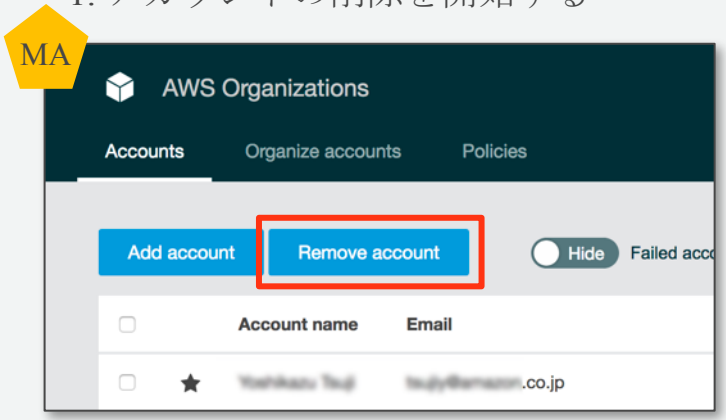
組織からアカウントを削除 (1/5)

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

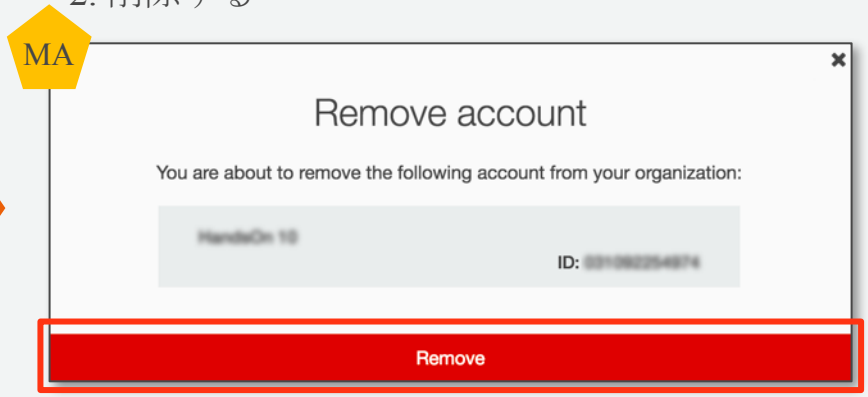
アカウントを組織内から削除できる。

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



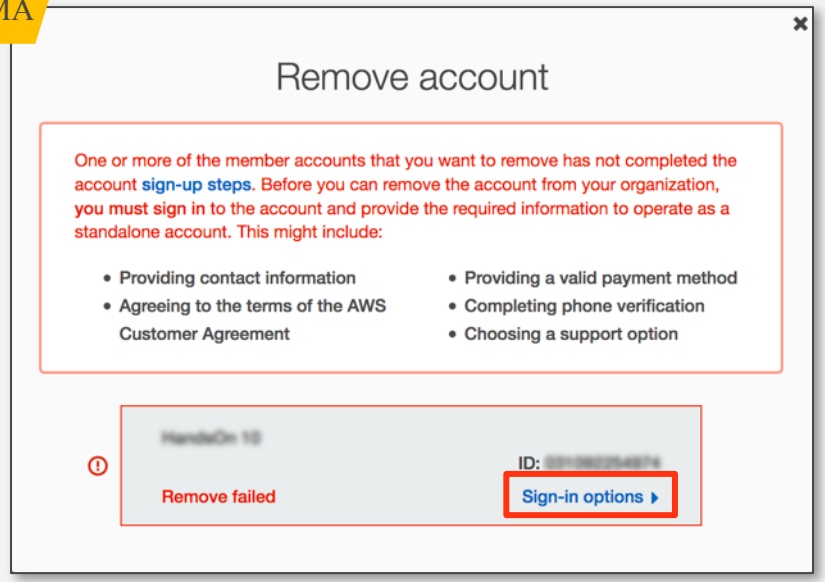
https://docs.aws.amazon.com/ja_jp/organizations/latest/userguide/orgs_manage_accounts_remove.html

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】

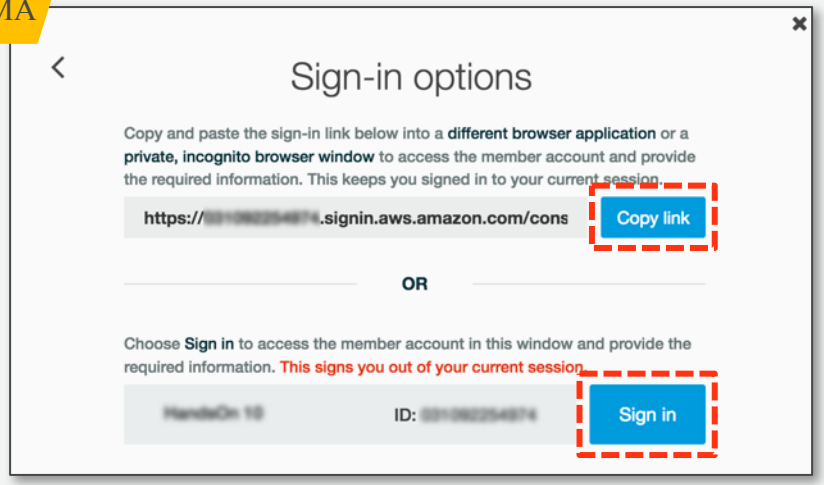
3. 以下のメッセージが表示され、
   対象アカウントでサインアップ手続が必要

MA



4. URLをどちらかの方法で開く

MA



※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)

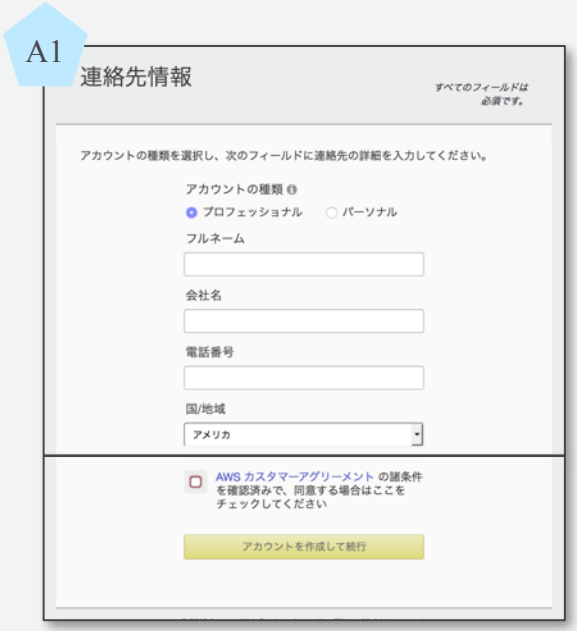
5. ルートアカウントのログインに切り替える

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

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



※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

9. 支払情報を入力する

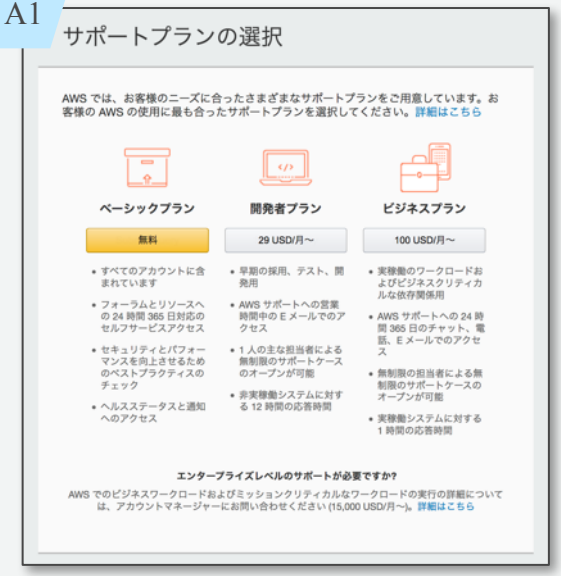
10. 電話による確認に対応する

組織からアカウントを削除 (5/5)

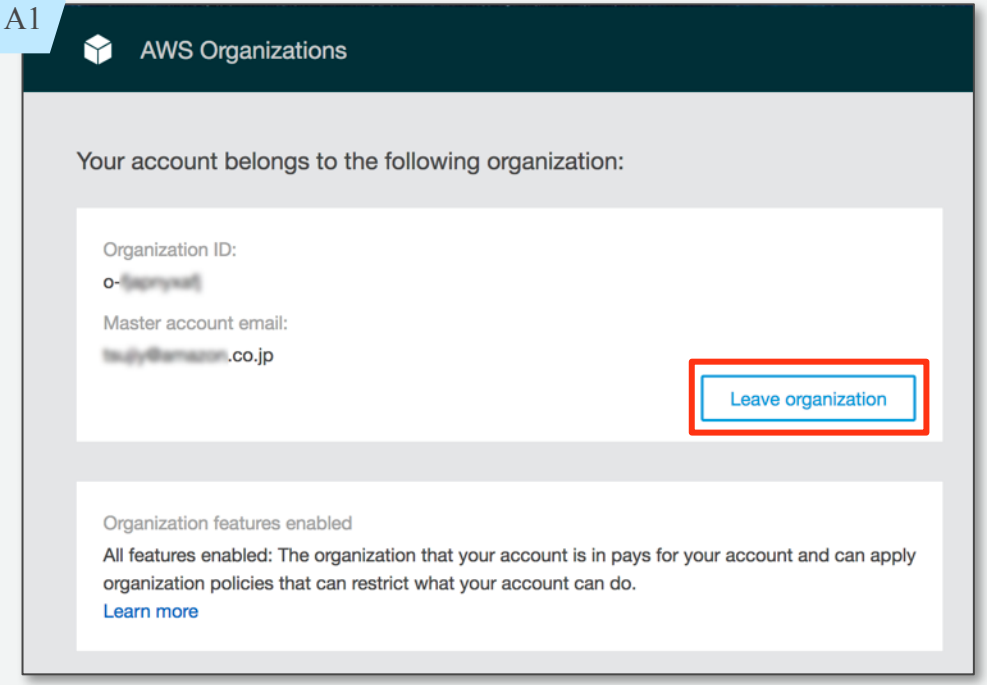
11. サポートプランを選択する

12. 組織から外す

A1



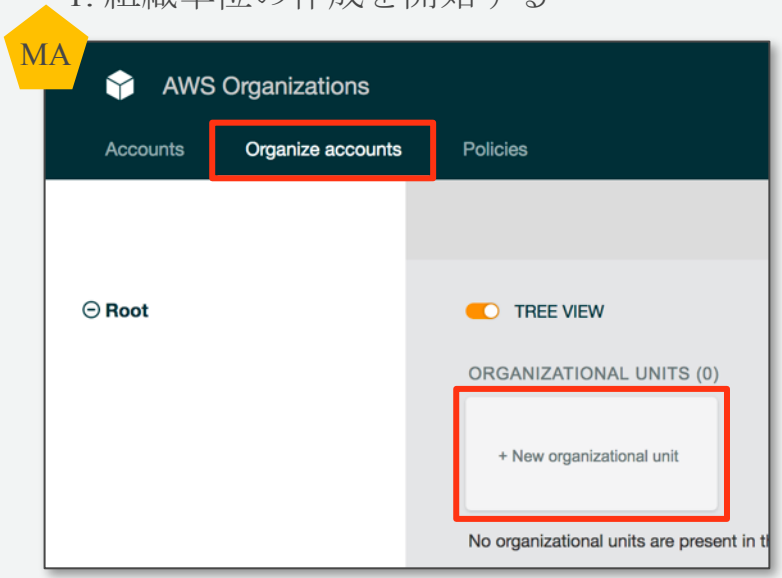
A1



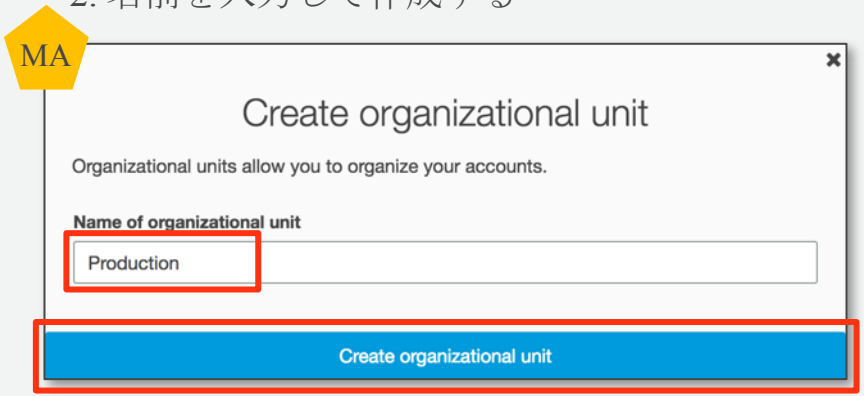
組織単位 (OU) の作成

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



https://docs.aws.amazon.com/ja_jp/organizations/latest/userguide/orgs_manage_ous.html#create_ou

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事ができ、階層構造に基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。

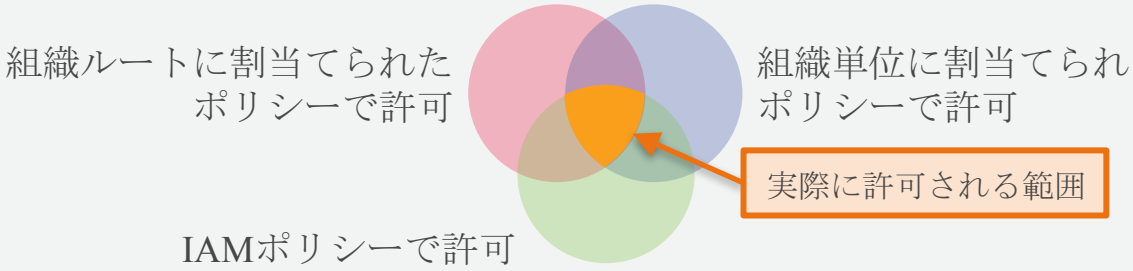
※対象のプリンシパルやリソースを指定する事はできず、全体に許可・禁止が適応される。

https://docs.aws.amazon.com/ja_jp/organizations/latest/userguide/orgs_manage_policies_about-scps.html

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。

https://docs.aws.amazon.com/ja_jp/organizations/latest/userguide/orgs_manage_policies_about-scps.html#SCP_strategies

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": "*"
      }
   ]
}
```

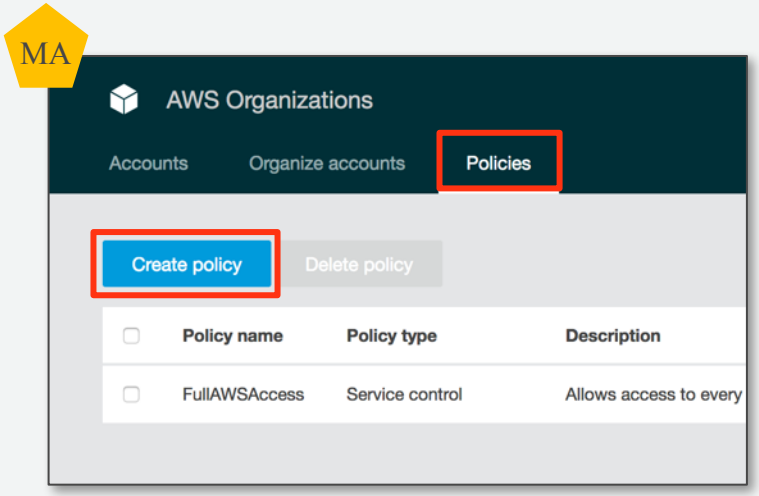
S3のみを許可

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

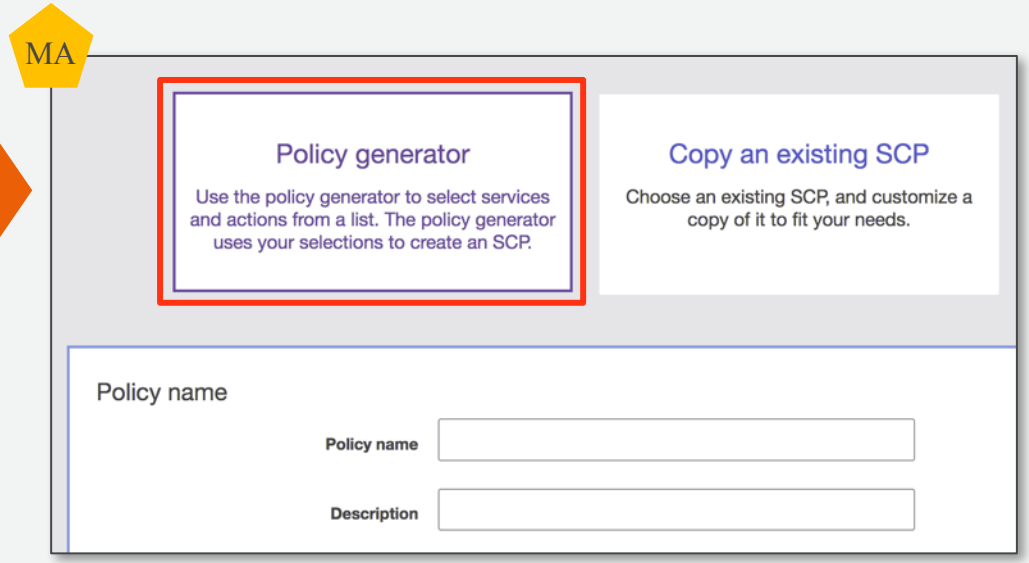
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_reference_scp-syntax.html

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



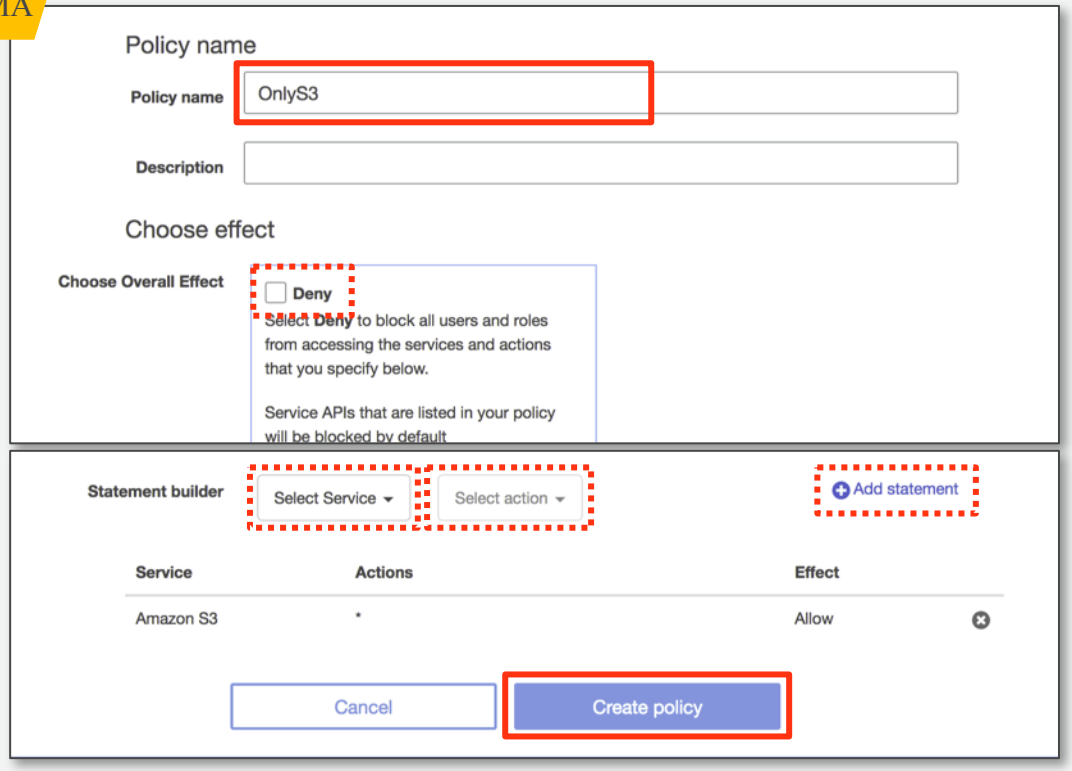
2. ポリシーの作成方法を選択する



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



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

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

  - 一括請求のみを有効

```
$ 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
```

https://docs.aws.amazon.com/cli/latest/reference/organizations/

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。

https://docs.aws.amazon.com/ja_jp/awsaccountbilling/latest/aboutv2/con-bill-blended-rates.html

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 

料金 

を

- プロジェクト単位
- 本番環境 開発環境
- エンドユーザ 企業単位

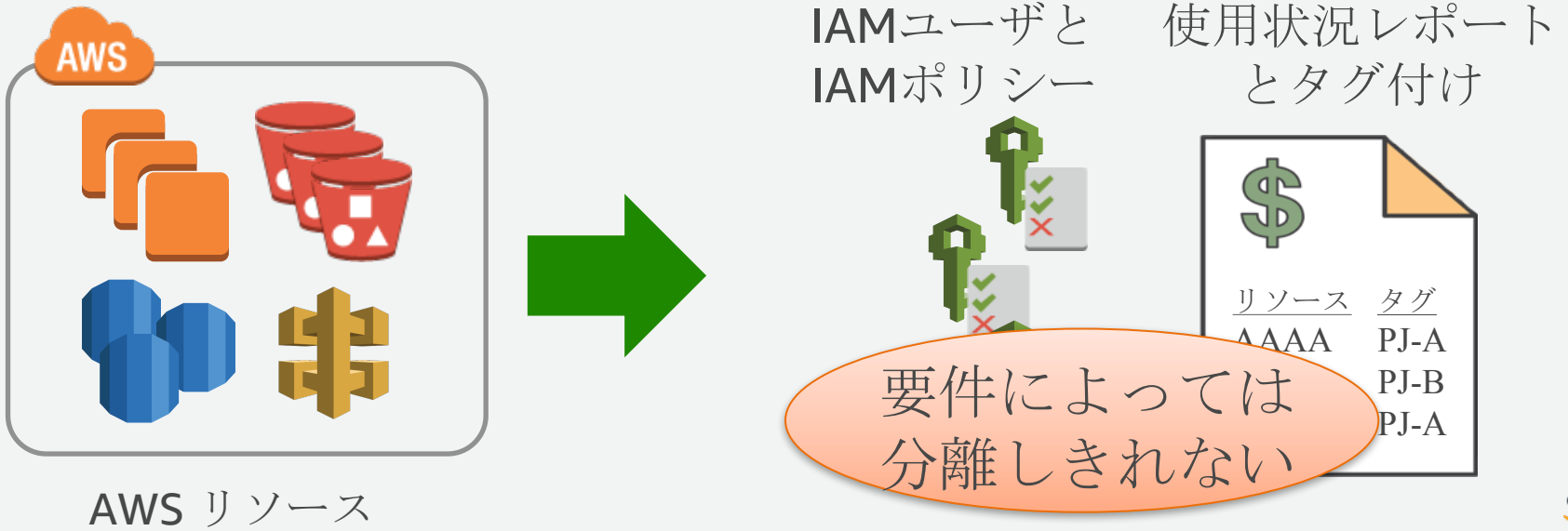
で明確に分離

など

という必要が出てくる事が多い

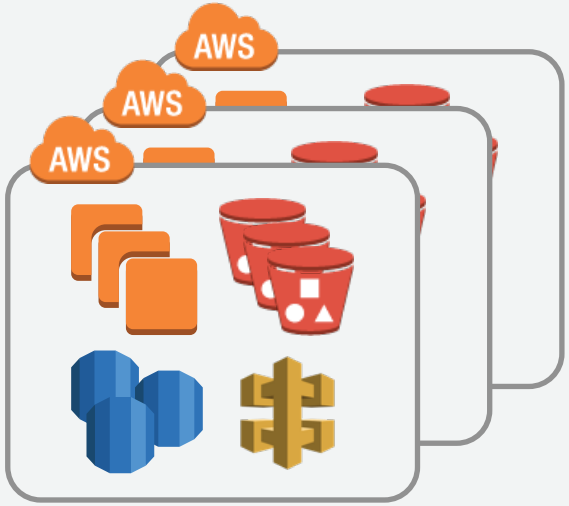
１アカウントのみで分離

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。

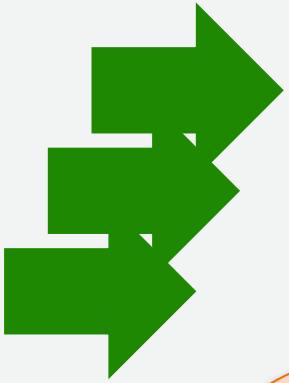


複数アカウントにして分離

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。）

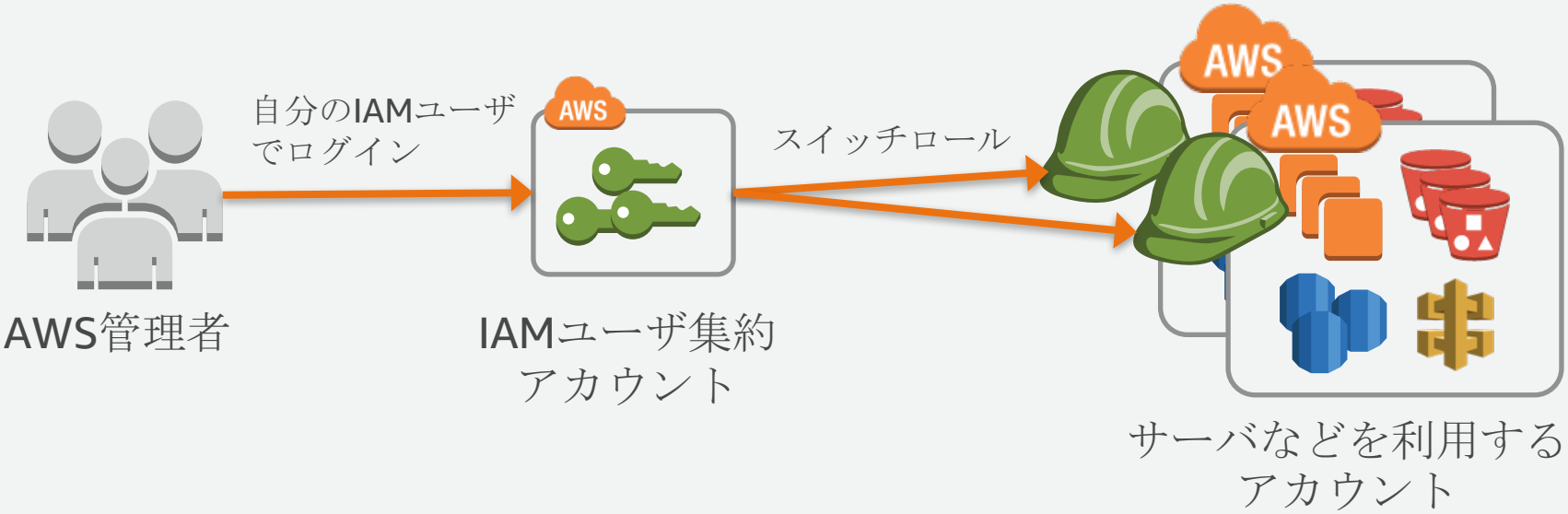
2つの方式を比較 (2/2)

	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	○	○ AWS Organizations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。

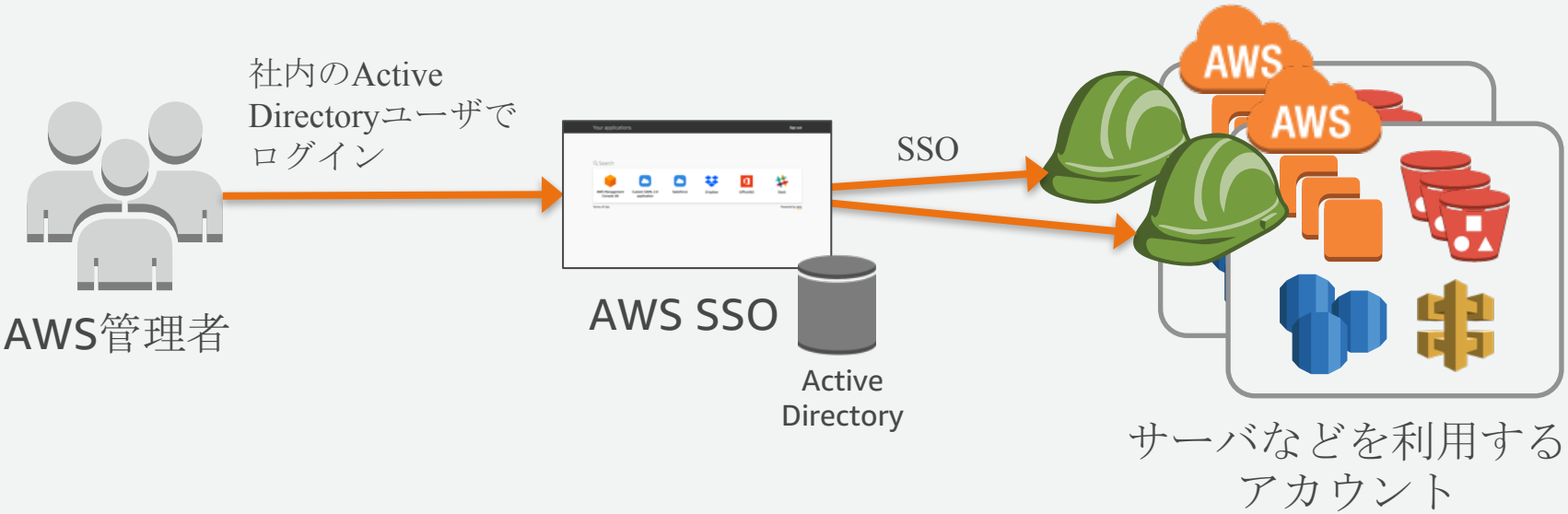
- IAMユーザを1アカウントに集約しスイッチロール



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アカウントのマネー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

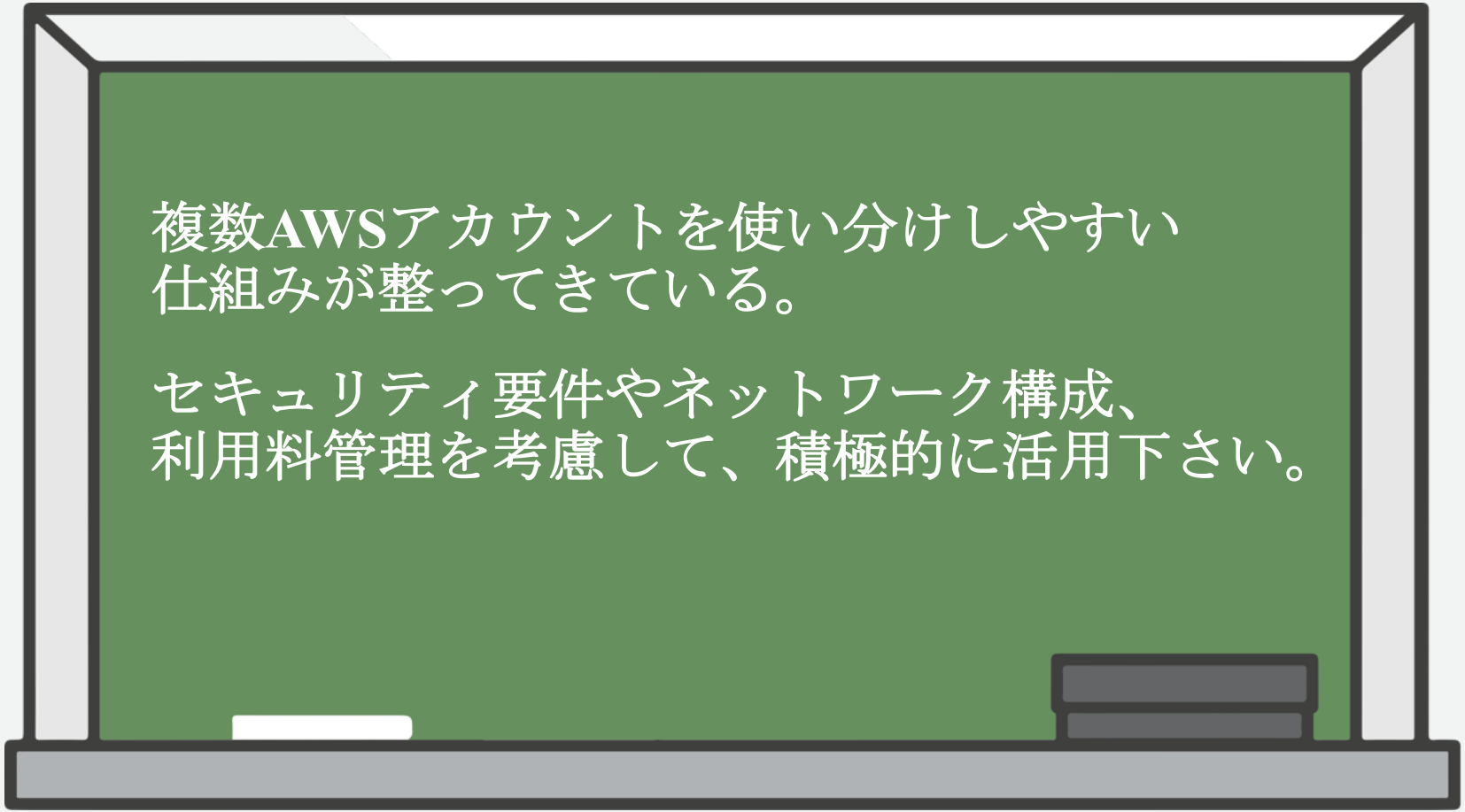
AWS SSO

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場合があるため注意。

- 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/

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

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/

※「AWS 問い合わせ」で検索してください


aws