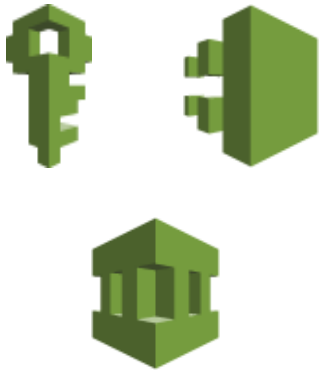
AWS Black Belt Online Seminar

【AWS Black Belt Online Seminar】 AWSサービスの権限管理



アマゾン ウェブ サービス ジャパン株式会社
プロフェッショナルサービス コンサルタント 山辺真行
2016.6.21

amazon web services

自己紹介

名前　山辺真行

所属　アマゾン ウェブ サービス ジャパン株式会社
プロフェッショナルサービス本部
コンサルタント

好きなAWSサービス　AWS Identity and Access Management (IAM)
Amazon Route 53

AWS Black Belt Online Seminar とは

- AWSJのTechメンバがAWSに関する様々な事を紹介するオンラインセミナーです

【**火曜 12:00~13:00**】
主にAWSのソリューションや
業界カットでの使いどころなどを紹介
(例：IoT、金融業界向け etc.)

【**水曜 18:00~19:00**】
主にAWSサービスの紹介や
アップデートの解説
(例：EC2、RDS、Lambda etc.)

※最新の情報は下記をご確認下さい。
オンラインセミナーのスケジュール&申し込みサイト
- http://aws.amazon.com/jp/about-aws/events/#webinar

内容についての注意点

- 本資料では2016年4月1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

- はじめに
- 権限設計の進め方
- 設計と実装例
- まとめ

Agenda

- はじめに
- 権限設計の進め方
- 設計と実装例
- まとめ

はじめに
よくある権限設計の悩み

ルールがないので使い方がばらばら。

権限を設計しようにもAPIの海に溺れる。

全員ルートアクセスで危険。

はじめに
権限設計が必要な理由

- 人はルールを完全には守れない。

- 人に頼らない仕組みが必要

- 人に頼らないルール適用の仕組み＝権限設計

はじめに
前提知識

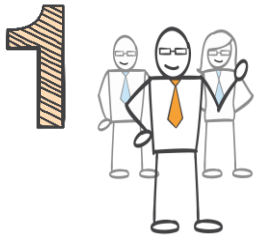
- 前提
  - IAMについて、以下の基本的な知識があること。
    - AWSアカウントとIAMアカウント
    - IAMポリシー
    - ユーザーとグループ
    - IAMベストプラクティス

- 参考：IAM Black Belt Tech Webinar
  - http://www.slideshare.net/AmazonWebServicesJapan/20150617-aws-blackbeltiam

Agenda

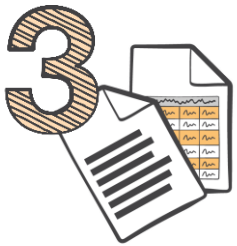
- はじめに
- 権限設計の進め方
- 設計と実装例
- まとめ

権限設計の進め方



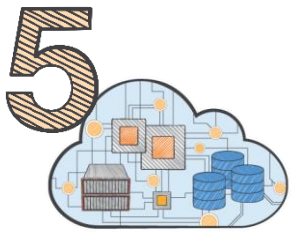
管理者の選出

関係組織の理解



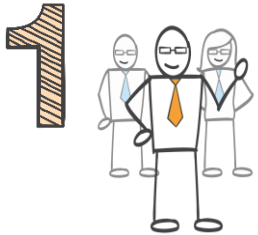
役割の整理

作業の明確化



実装

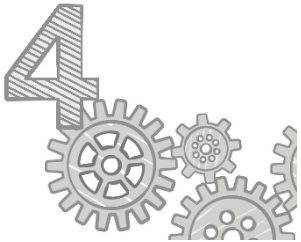
権限設計の進め方



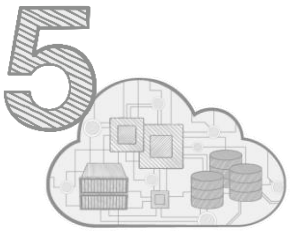
管理者の選出

関係組織の理解

役割の整理



作業の明確化



実装

権限設計の進め方

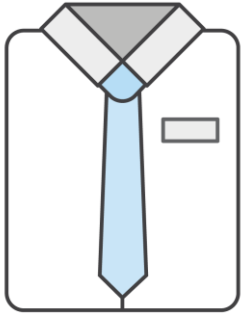
1.管理者の選出

- クラウド運営の中心を決定
  - 特定の管理者を選出
  - またはチームを編成
  - クラウド運営チーム＝**CCoE**（後述）
- 早い段階で決めることを推奨

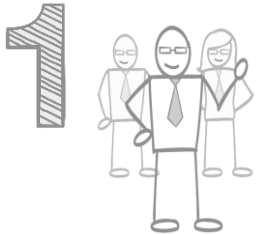
権限設計の進め方

1.管理者の選出

- CCoE(Cloud Center of Excellence)
  - クラウド導入・運営の主導チーム
  - 代表的な役割
    - クラウドの利用ルールの策定
    - 標準構成の策定
    - 社内導入コンサルティング



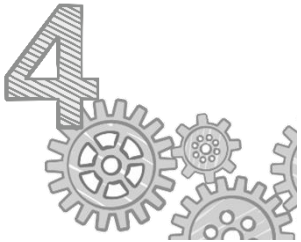
権限設計の進め方



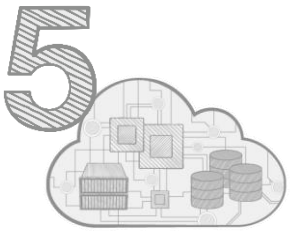
管理者の選出

関係組織の理解

役割の整理



作業の明確化



実装

権限設計の進め方

2.関係組織の理解

- 協力のための基礎
- どのような組織、人が関連しているか共有
- 書き出して相互理解を深める

権限設計の進め方

2.関係組織の理解

- 知るべき内容
  - 人数
  - スキル
  - 新技術に対する熱意、組織の文化
  - 稼働状況（AWS運営に関わる余裕度）
  - アサイン状況（専任/兼任）
  - （外部委託先）契約形態

権限設計の進め方

2.関係組織の理解　～関係組織の例～

部署・チーム名	既存の業務内容	人数	スキル	稼働状況	アサイン状況
管理者 or CCoE	(新設)	2名	2名ともAWS経験者。	(新設)	1名は専任、1名は兼任。
各事業部	サービス企画、立案、実行管理。立案時にAWSのコスト試算を行う必要あり。	不定	AWS経験はほとんどなし。	企画、立案会議にほとんどの時間を取られており常に多忙。	担当者は不定だがプロジェクト途中での離任は原則なし。
開発部及びパートナー企業	AWS上でのアプリケーション開発、リリース管理。	不定	一部にAWS経験のある人員もいる。	プロジェクトのフェーズによる。	プロジェクトごとに請負契約が基本。
ネットワーク部	既存ネットワークインフラの構築・運用。	2名	ネットワーク技術には非常に長けている。AWS経験はあまりない。	大規模ネットワーク改修が減り少し落ち着いている。	2名兼任でアサイン。
システム運用部	リソースの監視、運用、障害対応	2名	監視技術全般に詳しい。AWS経験はほとんどない。	シフト制。	年間契約で4名、パートナー企業から委任契約。
セキュリティ部	セキュリティガイドラインのレビュー、及び実環境の監査。	1名	セキュリティ技術に詳しいがAWSそのものに明るくはない。	新規プロジェクトが立ち上がる年度末・初に多忙。	1名兼任でアサイン。
経理部	月初5営業日までに請求書を受け取ることで次月支払処理が可能。	不定	経理処理全般。	通常の経理処理の一部として対応。	通常の経理処理の一部として対応。

権限設計の進め方

2.関係組織の理解　～関係組織の例～

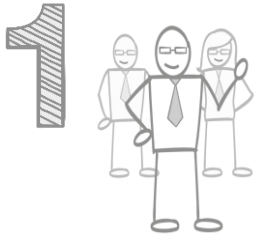
部署・チーム名	既存の業務内容	人数	スキル	稼働状況	アサイン状況
管理者 or CCoE	(新設)				
各事業部	サービス企画、立案、実行管理。立案時にAWSのコスト試算を行う必要あり。	不定			
開発部及びパートナー企業	AWS上でのアプリケーション開発、リリース管理。	不定	一部にAWS経験のある人員	プロジェクトのフェーズによ	プロジェクトごとに請負契約
ネットワーク部	既存ネットワークインフラの構築・運用。	2名			
システム運用部	リソースの監視、運用、障害対応	2名			
セキュリティ部	セキュリティガイドラインのレビュー、及び実環境の監査。	1名	セキュリティ技術に詳しいがAWSそのものに明るくはない。	新規プロジェクトが立ち上がる年度末・初に多忙。	1名兼任でアサイン。
経理部	月初5営業日までに請求書を受け取ることで次月支払処理が可能。	不定	経理処理全般。	通常の経理処理の一部として対応。	通常の経理処理の一部として対応。

全ての業務を列挙する必要はない。

AWSの運営と関係しそうな業務を記載

AWSを使った業務が明確な場合は記載

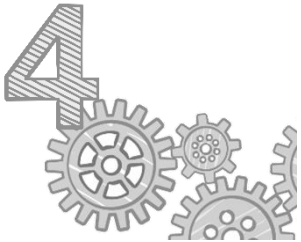
権限設計の進め方



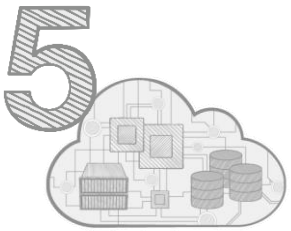
管理者の選出

関係組織の理解

役割の整理



作業の明確化



実装

権限設計の進め方

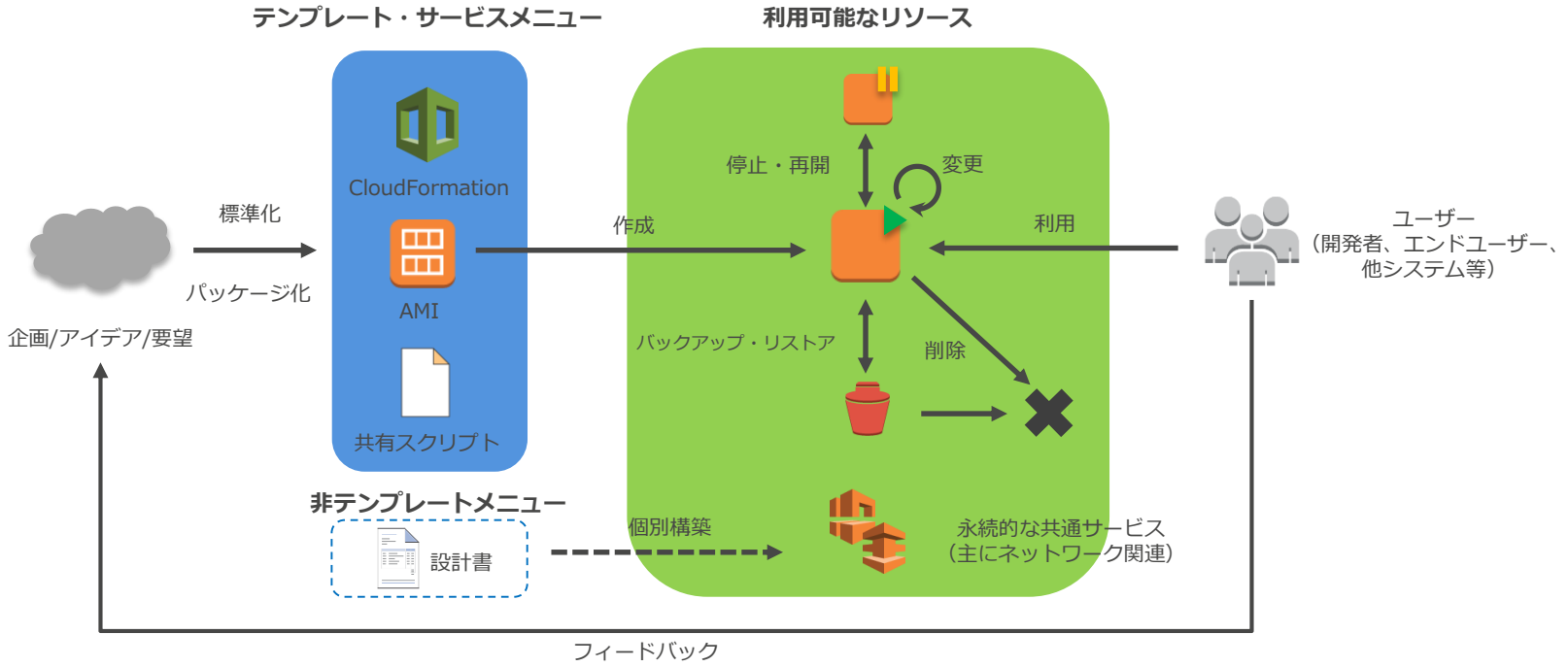
3.役割の整理

- AWSリソースの操作ポイントで役割を分割

- 操作ポイントの例
  - EC2インスタンスを**作成**する。
  - EC2インスタンスを**起動・停止**する。
  - EC2インスタンスを**削除**する。

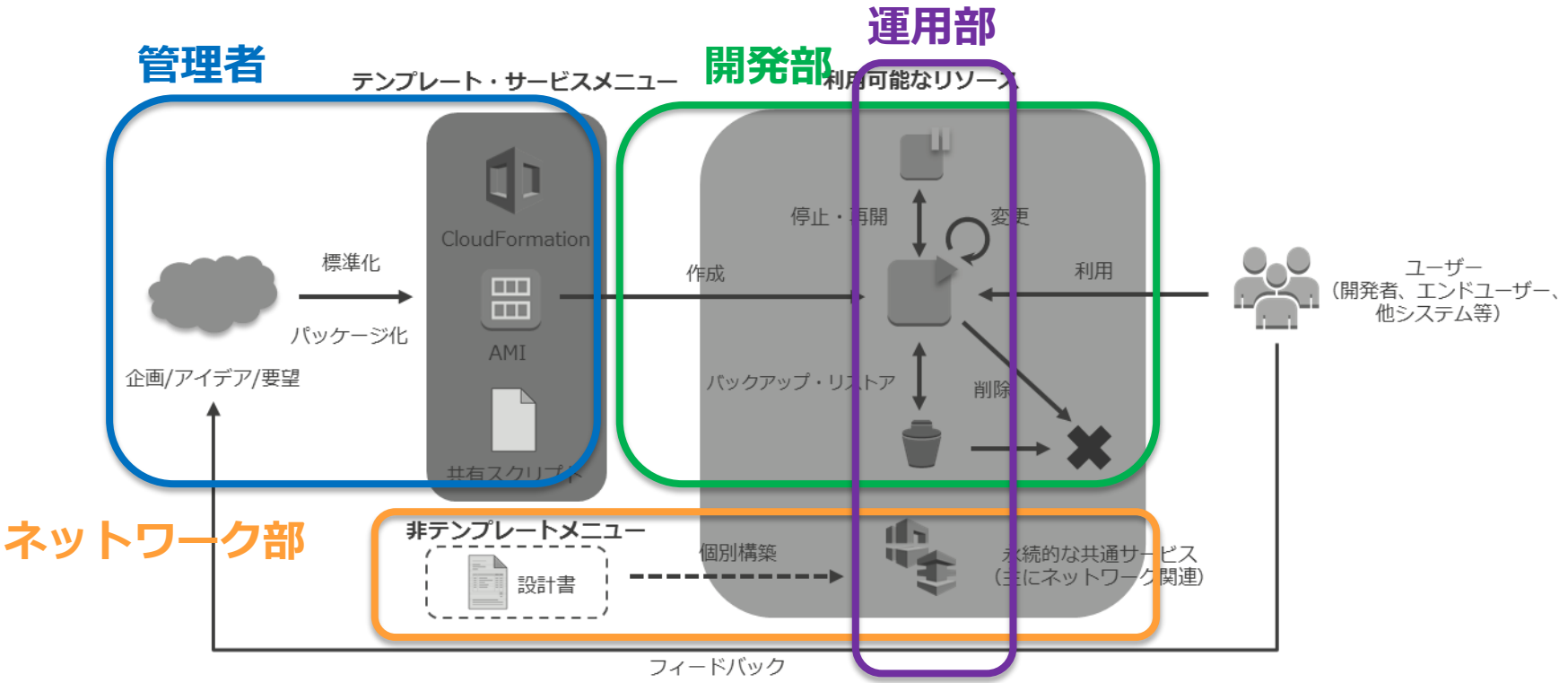
権限設計の進め方

3.役割の整理 ～AWSリソースの各操作ポイント～



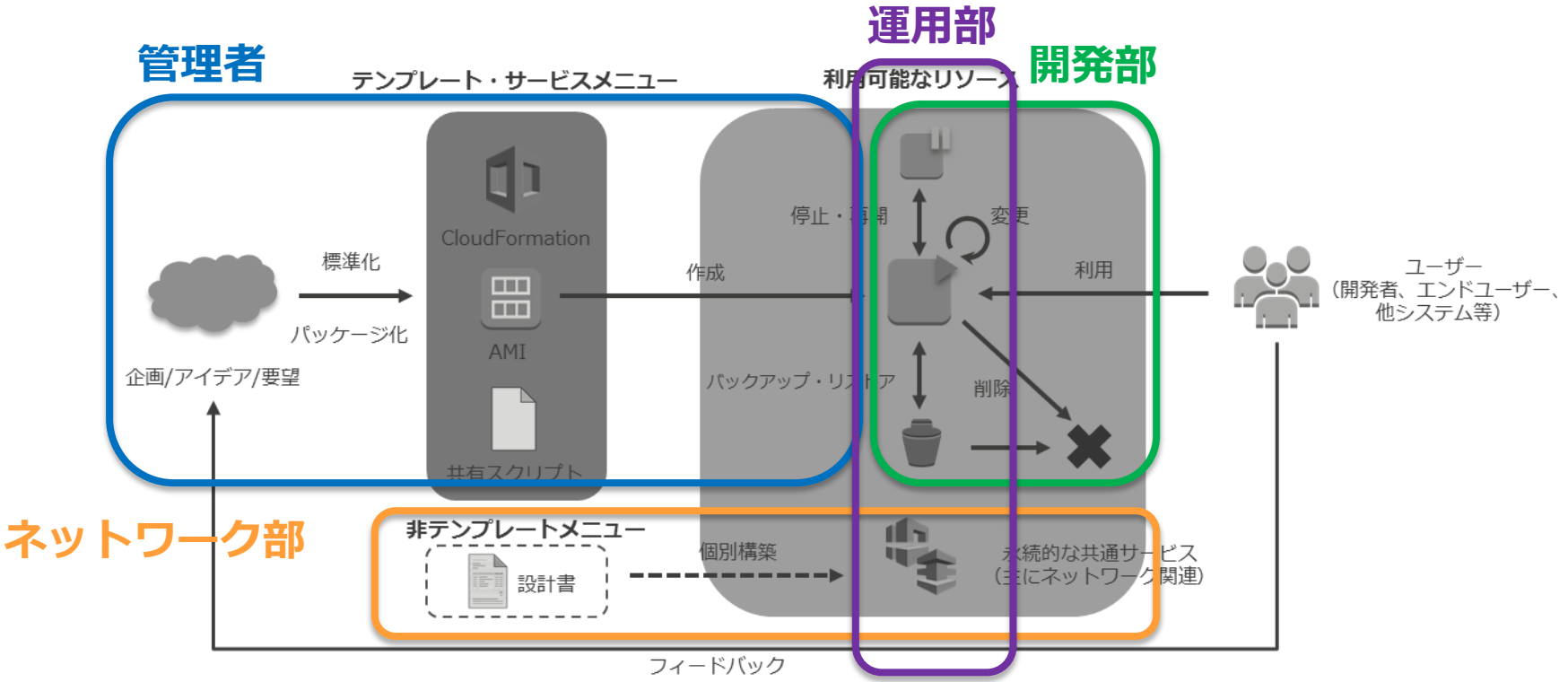
権限設計の進め方

3.役割の整理 ～例：自由にリソースを作成～



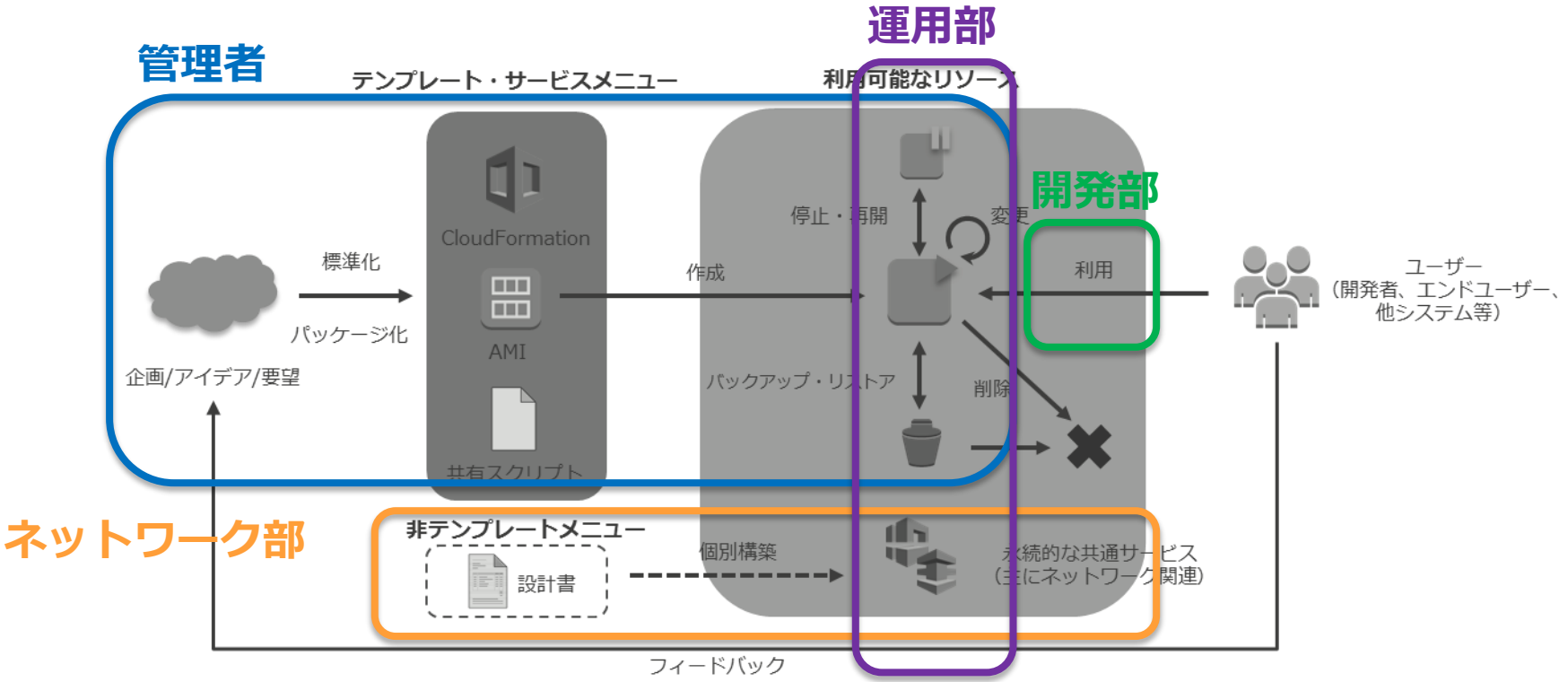
権限設計の進め方

3.役割の整理 ～例：CCoEでリソース作成～

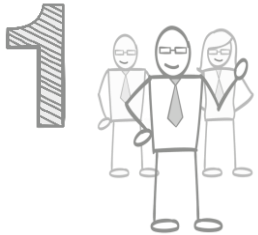


権限設計の進め方

3.役割の整理 ～例：リソースの変更は禁止～



権限設計の進め方

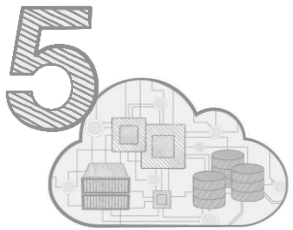


管理者の選出

関係組織の理解

役割の整理

作業の明確化



実装

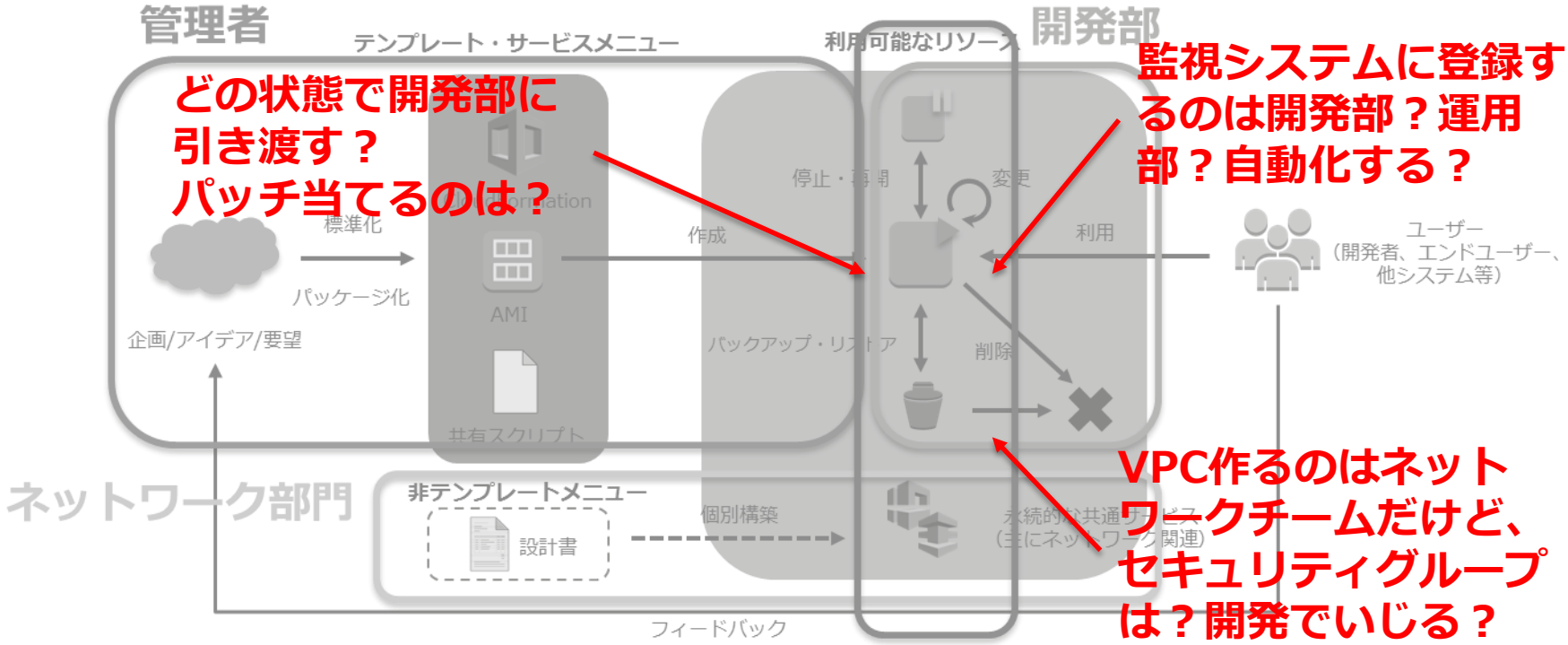
権限設計の進め方

4.作業の明確化

- 複数の組織の連携
  - 誰の担当か不明な作業（グレーゾーン）を減らす。

権限設計の進め方

4.作業の明確化　～組織間の連携例～



権限設計の進め方

4.作業の明確化　～作成ポイント～

- 記載ポイント

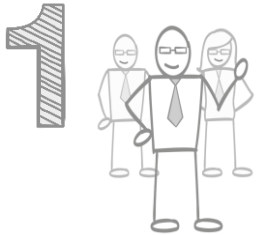
1. 誰が？
2. 何を？
3. どうする？
4. いつ？いつまでに？

権限設計の進め方

4.作業の明確化　～明確化の例～

組織名	責任	業務名	詳細
管理者 or CCoE	AWS運営全般の取りまとめ、サービス企画、利用ガイドライン、セキュリティ既定の策定。	標準イメージを作成	フィードバック、企画、アップデートなどのタイミングで標準イメージをアップデートする。半年に一度、AWSのサービスアップデートを含めて計画する。
		環境のデプロイ	依頼が来てから3営業日程度で完了する。
		利用料金を経理へ提出	毎月月初3営業日までに前月の利用料金を取りまとめて経理部に提出する。料金情報はBilling Reportを取得する。
開発部及びパートナー企業	AWS上でのアプリケーション開発、リリース管理。	EC2インスタンスの起動・停止	随時自分のチームのタグが割り当てられたインスタンスに限定して起動、停止を行う。
		バックアップ・リストア	随時自分のチームのタグが割り当てられたインスタンスに限定してバックアップ・リストアを行う。
ネットワーク部	既存ネットワークインフラの構築・運用。	IPレンジ割り当て	依頼に基づいてサブネットを払い出す。あまりに多い場合は要相談。
運用部門	リソースの監視	性能データへの読み取り	毎時AWSのリソースを情報を取得する。

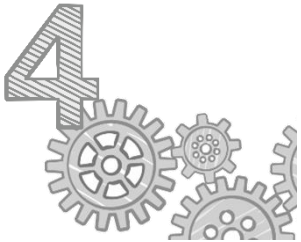
権限設計の進め方



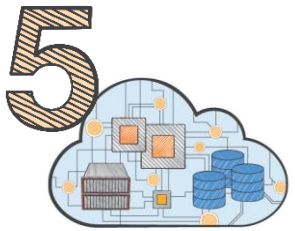
管理者の選出

関係組織の理解

役割の整理



作業の明確化



実装

権限設計の進め方

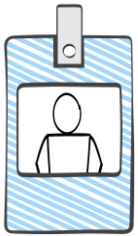
5.実装

- 認証と認可

何を？＝認可

許可・禁止を決めたルール
・IAMポリシー
・セキュリティグループ

誰？＝認証



本人かどうかを確認する手段
・パスワード
・IDカード
・セキュリティトークン

権限設計の進め方

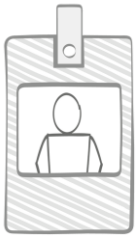
5.実装

- 認証と認可

何を？＝認可

許可・禁止を決めたルール。
- **IAMポリシー**
- セキュリティグループ

誰？＝認証



本人かどうかを確認する手段。
- パスワード
- IDカード
- セキュリティトークン

権限設計の進め方

5.実装　～作業のブレークダウン～

組織名	責任	業務内容	詳細
管理者 or CCoE	AWS運営全般の取りまとめ、サービス企画、利用ガイドライン、セキュリティ既定の策定。	標準イメージを作成	フィードバック、企画、アップデートなどのタイミングで標準イメージをアップデートする。半年に一度、AWSのサービスアップデートを含めて計画する。
		環境のデプロイ	依頼が来てから3営業日程度で完了する。
		利用料金を経理へ提出	毎月月初3営業日までに前月の利用料金を取りまとめて経理部に提出する。料金情報はBilling Reportを取得する。

組織名	責任	業務内容	EC2	S3	VPC	コスト管理画面
管理者 or CCoE	AWS運営全般の取りまとめ、サービス企画、利用ガイドライン、セキュリティ既定の策定。	標準イメージを作成	**AMI作成**	-	-	-
		環境のデプロイ	**インスタンス作成**	**バケット作成** **ポリシー設定**	-	-
		利用料金を経理へ提出	-	-	-	**参照**

権限設計の進め方

5.実装　～IAMポリシーの記述～

ホワイトリスト方式

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ec2:CopyImage",
            "ec2:CopySnapshot",
            "ec2:CreateSnapshot",
                  .
                  .
                  .
         ],
         "Resource": [
            "*"
         ]
      }
   ]
}
```

許可する内容をすべてリストする。
（ホワイトリスト）

ブラックリスト方式

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": "ec2:*",
         "Resource": "*"
      },
      {
         "Effect": "Deny",
         "Action": "ec2:XXXXX",
         "Resource": "*"
      },

   ]
}
```

許可する内容を包括的に記述する。

許可する中でも禁止する内容を記述する。
（ブラックリスト）

権限設計の進め方

5.実装　～IAMポリシーの記述～

- メンテナンスの考慮
  - メンバーの異動や退職
  - 使われていない権限は削除
  - 他のメンバーがポリシーをメンテナンス可能であること

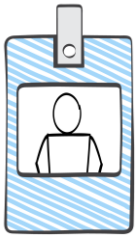
権限設計の進め方
5.実装

- 認証と認可

何を？＝認可

許可・禁止を決めたルール
・IAMポリシー
・セキュリティグループ

誰？＝認証



本人かどうかを確認する手段
・パスワード
・IDカード
・セキュリティトークン

権限設計の進め方

5.実装　～認証方式の選択～

認証方式	概要	特徴
パスワード	マネージメントコンソールへアクセスする際のパスワードをIAMユーザー単位に発行する。	パスワードはユーザーも慣れているので組織になじみやすい。パスワード管理が必要。
MFA （多要素認証）	セキュリティトークンでマネージメントコンソールへのアクセスを制御する。	パスワードだけでは不安な場合にMFAを管理することで制御ができる。物理トークンの場合は保管場所が必要。
固定Credential	AWS APIに対する認証キー。	API（またはCLI）を多用するユーザーには利便性が高い。文字列であるため漏洩に注意する必要がある。
EC2 IAMロール	EC2上のAWS APIの一時Credential。	特定のEC2インスタンスで実行できるAPIを制限できる。Credential管理が不要。
AD連携	既存のActive Directoryの認証を使ってマネージメントコンソールにログインする。	AWS側のパスワード管理が不要。 組織の人的移動（部署移動、退職）などと連携できる。

権限設計の進め方

5.実装　～認証方式の選択～

組織名	責任	業務内容	EC2	S3	VPC	コスト管理画面
管理者 or CCoE	AWS運営全般の取りまと & ナ ラ	標準イメージを作成	**AMI作成**	-	-	-
開発部及びパートナー企業	AWS上でのアプリケーション開発、リリース管理。	EC2インスタンスの起動・停止	**インスタンス起動 停止**	-	-	-
		バックアップ・リストア	**スナップショット 取得**	**オブジェクト Put Get**	-	-
ネットワーク部	既存ネットワークインフラの構築・運用。	IPレンジ割り当て	-	-	**VPC作成 サブネット作成**	-
運用部門	リソースの監視	性能データへの読み取り				

システム上、この組織は何か？
IAMのグループか？ADのグループか？
特定のIAMユーザーか？

権限設計の進め方

5.実装　～ドキュメント例～

実装の全ステップをドキュメントにまとめた例

組織と業務

認証方式

IAMポリシー名

Operation			IAM Configuration								Policy Attachement			
				IAM Groups	IAM Roles									
						Trusted Entity (see also "Sample Trust Relationship")								
						SAML(SSO)			AWS Account	AWS Service				
							ADFS Settings(Claim rule)							
Division or Role	Tasks/ Responsibility	Environment	AWS Account ID	Group Name	Role Name	ID Provider	Claim Name	Claim Value	Trusted AWS ID	Trusted AWS Service	Billing-Admin	Support-Access	Trusted-Advisor	IAM-Admin
Billing Administrator	Review AWS Cost	Dev		-	AWS-Billing-Admin	IDP-Name	AD Group	Billing-Group	-					
		Prod	123456789012	-	AWS-Billing-Admin	IDP-Name	AD Group	Billing-Group	120987654321		✓	✓	✓	
Infrastructure Administrator	Manage AWS Infrastructure	Dev	120987654321	-	AWS-Dev-Infra-Ope	IDP-Name	AD Group	Infra-Group	-			✓		
	Deploy and monitor guest user stacks.	Prod	123456789012	-	AWS-Prod-Infra-Ope	IDP-Name	AD Group	Infra-Group	-			✓		
ID Administrators	Manage AWS ID and Roles	Dev	120987654321	-	AWS-IAM-Admin	IDP-Name	AD Group	ID-Managers	-			✓		
		Prod	123456789012	-	AWS-IAM-Admin	IDP-Name	AD Group	ID-Managers	-			✓		
Network Administrators	Manager	Dev	120987654321	-	AWS-NW-Admin	IDP-Name	AD Group	NW-Admins	-			✓		
		Prod	123456789012	-	AWS-NW-Admin	IDP-Name	AD Group	NW-Admins	-			✓		
Guest System User	Application Developer	Dev	120987654321	-	AWS-User-***SystemID***	IDP-Name	AD Group	Guest-Group-XXXX	-			✓		
		Prod	123456789012	-	AWS-User-***SystemID***	IDP-Name	AD User	Guest-Group-XXXX	-			✓		
Operator	Monitor and support	Dev	120987654321	-	AWS-Dev-Audit-Admin	-	-	-	-	EC2				
		Prod	123456789012	-	AWS-Prod-Audit-Admin	-	-	-	-	EC2				
Auditor	Audit and monitor API call	Dev	120987654321	-	AWS-Dev-Audit-Admin	IDP-Name	AD Group	-	-					
		Prod	123456789012	-	AWS-Prod-Audit-Admin	IDP-Name	AD Group	-	-					
Shared Role	AWS Support Console Access	Prod	123456789012	-	AWS-Prod-Support	-	-	-	120987654321			✓		
External contructor	Develop and monitor applications	Dev	120987654321	External-Users	-	-	-	-	-					
		Prod	123456789012	External-Users	-	-	-	-	-					

AWS上のグループ名

AWS上のロール名

AD上のグループ名

実際のポリシードキュメントは別シートで管理してもよい。

IAMポリシー割り当て

Agenda

- はじめに
- 権限設計の進め方
- 設計と実装例
- まとめ

設計と実装例

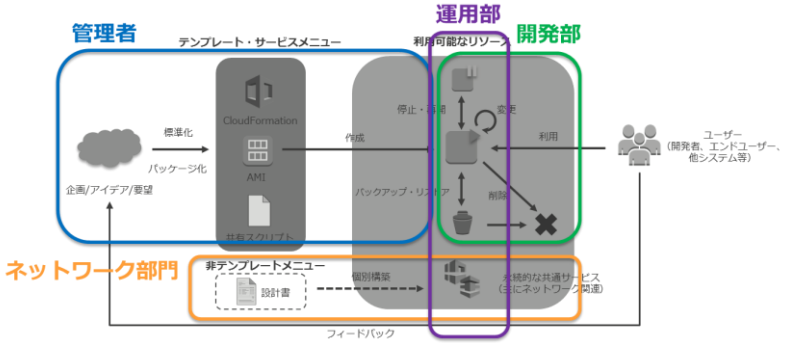
実装例

1. 中央管理型
   - CCoEがテンプレートの企画、開発、リソースの作成を担当
2. セルフサービス型
   - リソースの作成はユーザー自身が担当
3. 認証委任型
   - 依頼元が委託先（ベンダー）にIAMユーザーの作成・管理を委任
4. マネージメントコンソールへのアクセス制限
   - Federationを利用したコンソールへのアクセス制御

設計と実装例

1. 中央管理型

- シナリオ
  - CCoE
    - テンプレートの企画、開発
    - テンプレートから環境の作成
    - 不要になったリソースの削除
  - 各事業部
    - 与えられたインスタンスの起動停止
    - 所定のS3バケットへのPut/Get
    - 但し他の部門に与えられたリソースへのアクセスは禁止



設計と実装例

1. 中央管理型　～権限設計～

組織名	責任	業務内容	EC2	S3	VPC	コスト管理画面
CCoE	テンプレートの企画、開発。 テンプレートから環境の作成。 不要になったインスタンスの削除。	標準イメージを作成	**AMI作成**	-	-	-
		環境のデプロイ	**インスタンス作成**	**バケット作成** **ポリシー設定**	-	-
		利用料金を経理へ提出				**参照**
各事業部	与えられたインスタンスの起動停止 所定のS3バケットへのPut/Get 但し他の部門に与えられたリソースへのアクセスはできない。	EC2インスタンスの起動・停止	**インスタンス起動** **停止**	-	-	-
		バックアップ・リストア	-	**オブジェクト** **Put Get**	-	-
ネットワーク部	既存ネットワークインフラの構築・運用。	IPレンジ割り当て	-	-	**VPC作成** **サブネット作成**	-
運用部門	リソースの監視	性能データへの読み取り				

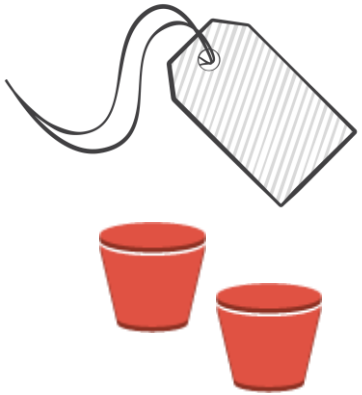
実際には複数の利用主体の集合

各事業部門が別の事業部門のリソースにアクセスできないようにするには？

設計と実装例

1. 中央管理型　～設計ポイント～

- 事業部門ごとの権限の管理
  - 互いのリソースに干渉しない権限設計
- EC2＝タグによる権限分離
- S3＝リソースによる権限分離



設計と実装例

1. 中央管理型　～リソースベースの制御ポリシー例～

EC2

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec2:RebootInstances"
         ],
         "Condition": {
            "StringEquals": {
               "ec2:ResourceTag/<タグキー>": "<タグ値>"
            }
.....
```

Start/Stop/Restartはタグを条件に指定できる。
（※すべてのEC2 APIが対応しているわけではないので注意）

S3

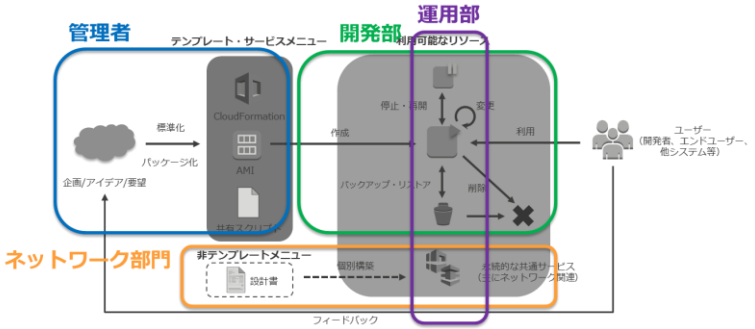
```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": "s3:ListAllMyBuckets",
         "Resource": "arn:aws:s3:::*"
      },
      {
         "Effect": "Allow",
         "Action": [
            "s3:PutObject",
            "s3:GetObject",
            "s3:DeleteObject"
         ],
         "Resource": [
            "arn:aws:s3:::<バケット名>/*"
         ]
      },
....
```

S3はリソースで対象を制限

参考:『Amazon EC2 API アクションでサポートされるリソースレベルのアクセス許可』
http://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/ec2-supported-iam-actions-resources.html

設計と実装例
2. セルフサービス型

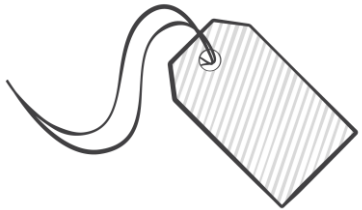
- シナリオ
  - CCoE
    - テンプレートの企画、開発
  - 各事業部
    - テンプレートから環境の作成
    - 不要になったリソースの削除
    - 与えられたインスタンスの起動停止
    - 所定のS3バケットへのPut/Get
    - 但し他の部門に与えられたリソースへのアクセスは禁止



設計と実装例
2. セルフサービス型

- 事業部門ごとの権限の管理
  - 互いのリソースに干渉しない権限設計

- タグで権限分離可能か？



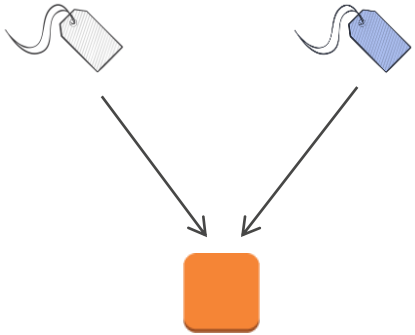
設計と実装例
2. セルフサービス型

- インスタンス作成とタグ編集を許可する場合

インスタンス作成時のタグ

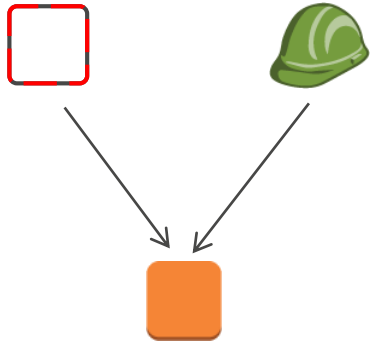
「インスタンス作成時に特定のタグをつける」という制限はできない。

タグの編集



タグの編集権限を与えると、他の事業部門のタグもつけたり、外したりできる。

他に権限が必要



インスタンス作成には実は他にも必要な権限（例えばセキュリティグループの適用等）が必要

設計と実装例

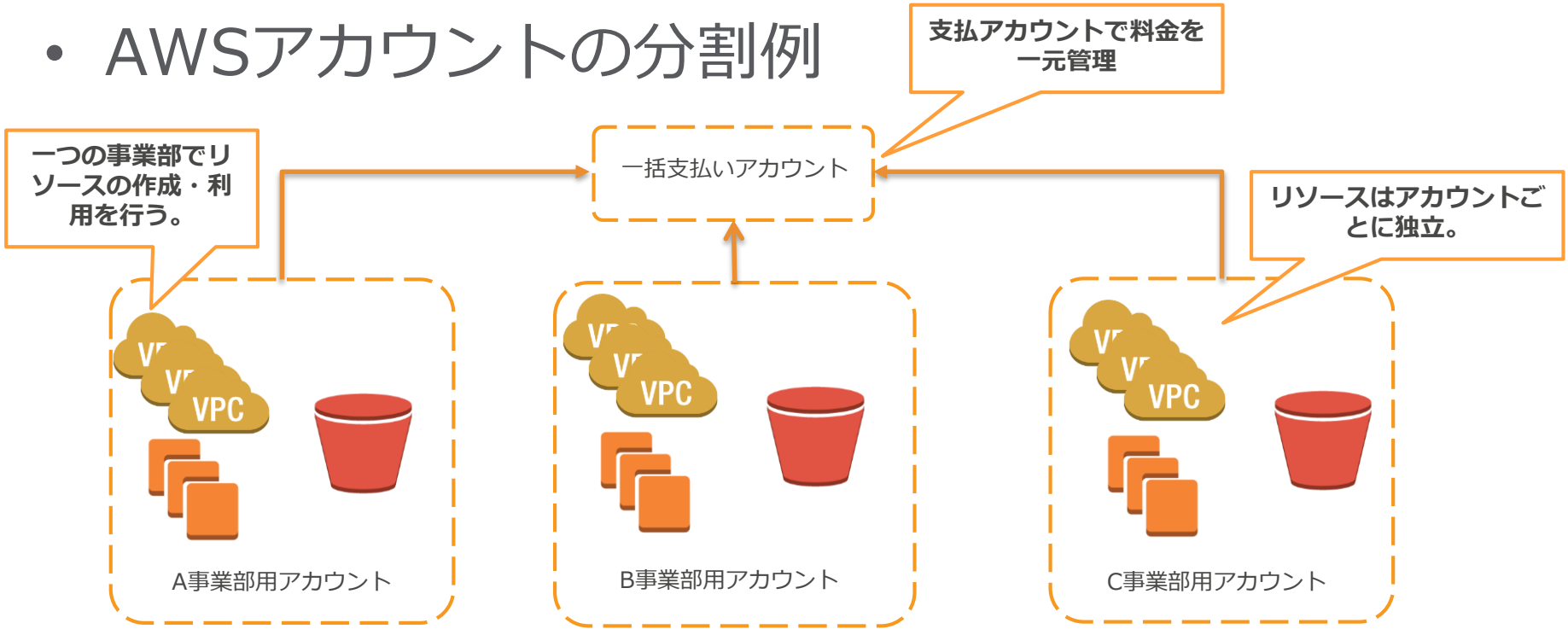
2. セルフサービス型

- AWSアカウントの分割
  - AWSアカウントを事業部ごとに分割

- AWS Service Catalogの利用
  - ユーザーのリソース作成権限が不要

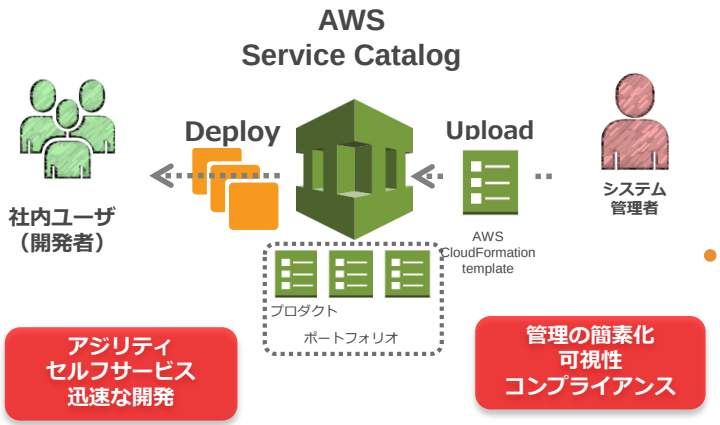
設計と実装例
2. セルフサービス型

- AWSアカウントの分割例



AWS Service Catalog

組織内サービスポータル提供サービス



- **特徴** (http://aws.amazon.com/jp/servicecatalog/)
  - シンプルな操作性のポータルを提供
  - セルフサービスで環境を準備可能
  - 環境管理の一元化が可能
  - ライセンスの管理も容易に
- **価格体系**
  - 1ポートフォリオ $5/Month
  - 1つ以上の IAM users/groups/roles を持つポートフォリオに対して課金
  - スタックの数に制限はなし

※別途カタログから起動するサービスの料金も発生します。

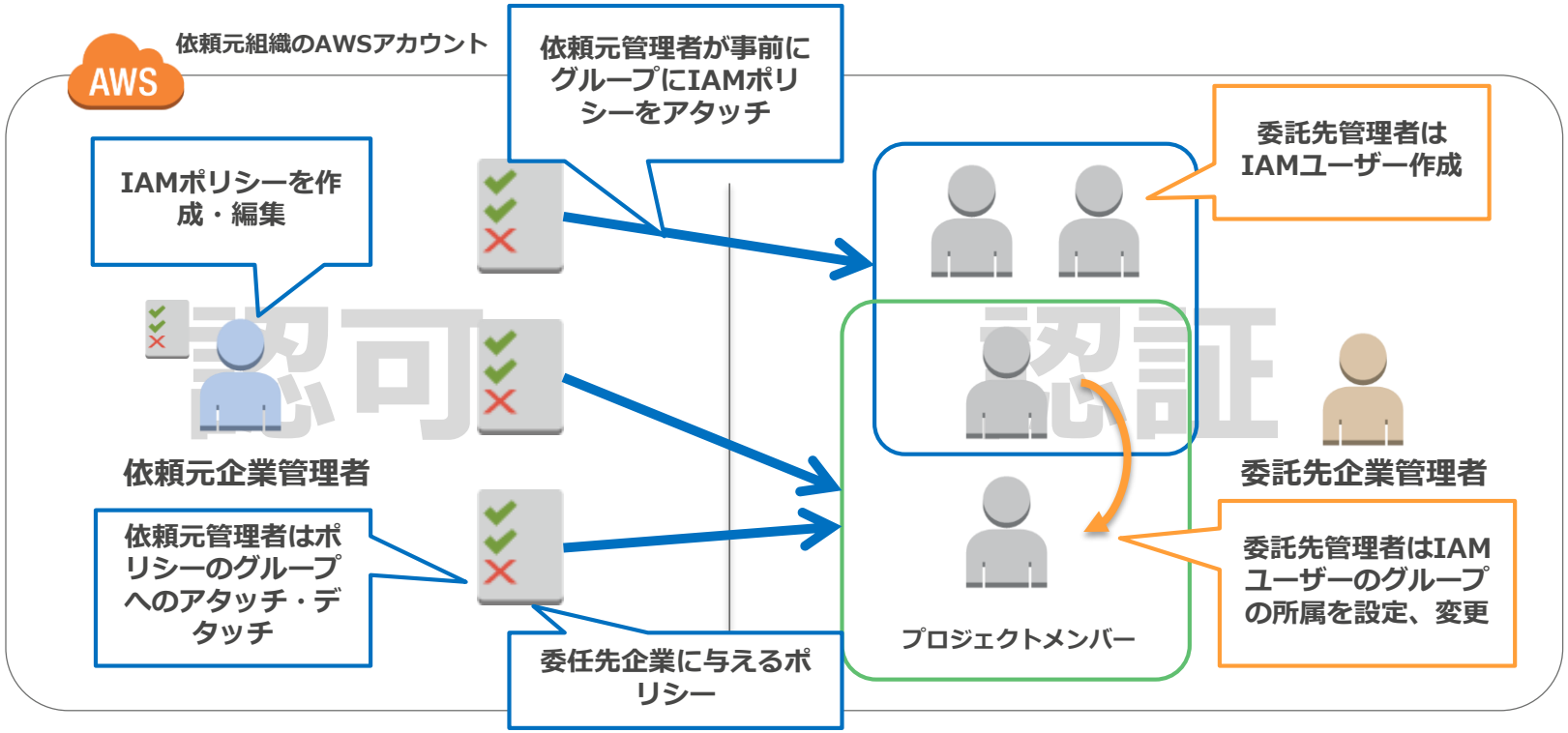
設計と実装例

3. 認証委任型

- シナリオ
  - 依頼元企業管理者
    - システムの発注元
    - IAMポリシーの作成、編集
  - 委託先企業管理者
    - システムの受託企業
    - 自社のメンバーをプロジェクトに参加、離任させる
    - IAMユーザーの作成、IAMユーザーのグループへの割当

設計と実装例

3. 認証委任型



設計と実装例

3. 認証委任型　～設計例～

依頼元企業管理者

```
…
"Statement": [
      {
         "Effect": "Allow",
         "Action": "iam:*",
         "Resource": "*"
      }
   ]
….
```

注）IAM全権限付与はルート権限とほぼ同等と考えるべき

AWSルートアカウントと同等の管理を検討する。
例）MFAデバイスによる認証管理

設計と実装例

3. 認証委任型　～設計例～

委託先企業管理者

```
・・・{
        "Effect": "Allow",
        "Action": "iam:*",
        "Resource": "*"
    },
    {
        "Effect": "Deny",
        "Action": [
            “iam:Attache*”,
            “iam:Detache**”,
            "iam:CreatePolicy",
            "iam:DeletePolicy",
            "iam:PutGroupPolicy",
            "iam:PutRolePolicy",
            "iam:PutUserPolicy",
            "iam:DeleteUserPolicy",
            "iam:DeleteRolePolicy",
            "iam:DeleteGroupPolicy“,
    ],
・・・
```

アタッチ・デタッチを禁止する理由
依頼元企業の管理者が作成していない、強力なAWS管理ポリシーを勝手にアタッチさせないため。
（IAMFullAccessポリシーを委託先管理者が自分にアタッチできると何でもできてしまう。）

ポリシーのアタッチ、デタッチを禁止。

IAMポリシーを操作する権限をすべて禁止。

インラインポリシーの操作を禁止。

設計と実装例

4. マネージメントコンソールへのアクセス制限

- シナリオ
  - 社内でAWSを利用しているが、マネージメントコンソールのアクセスは社内に限定したい。
  - 機密データを扱うAWSアカウントのマネージメントコンソールに自宅などからログインしてほしくない。

設計と実装例

4. マネージメントコンソールへのアクセス制限

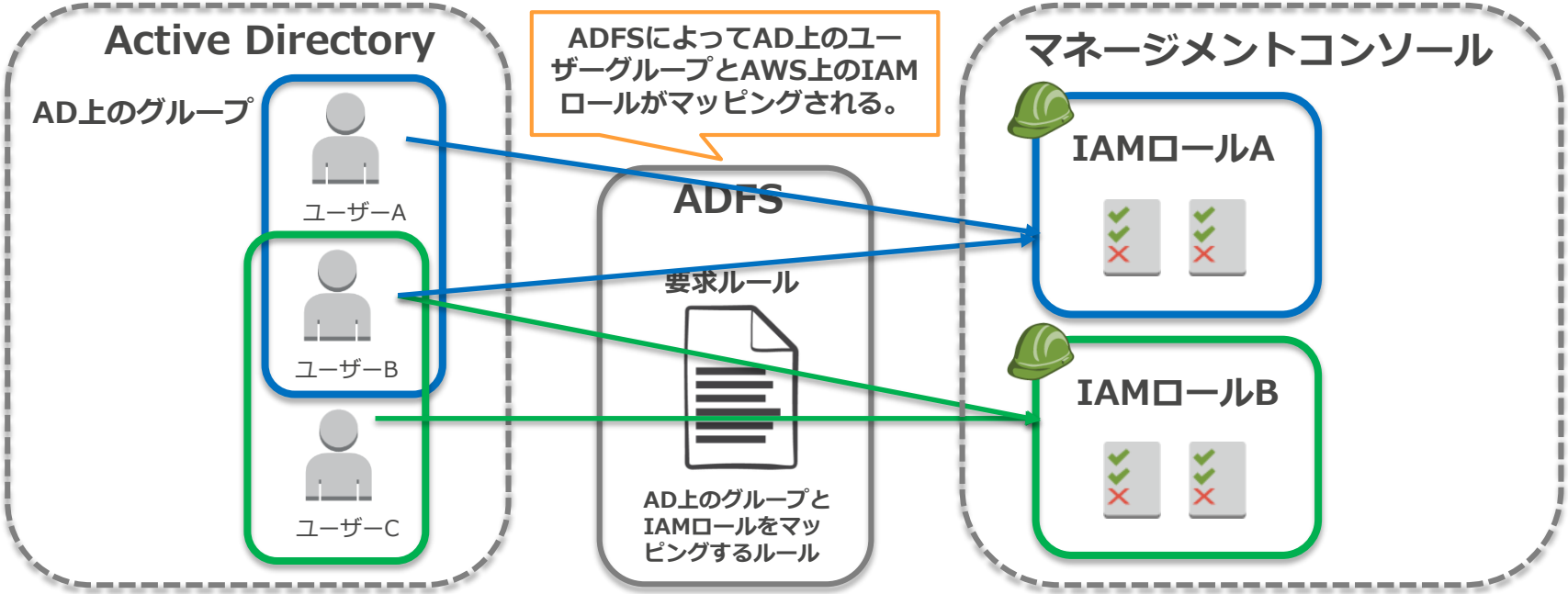
- 認証を利用して実現
  - 固定パスワードをユーザーに渡さなければログインできない
  - 社内の認証機構を利用
  - Active Directoryの認証と連携

発信元IPアドレスによる制限も可能だが、CloudFormationなどAWSのIPアドレスからAPIが呼び出される場合には注意が必要
http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/access_policies_examples.html#iam-policy-example-deny-source-ip-address

設計と実装例

4. マネージメントコンソールへのアクセス制限

- ADFSとAWSの連携



設計と実装例

4. マネージメントコンソールへのアクセス制限

- ADへのアクセスを社内からに限定

- ADFS連携ではユーザーはマネージメントコンソールのログインパスワードを持たない。

- **コンソールログインを社内に限定！**

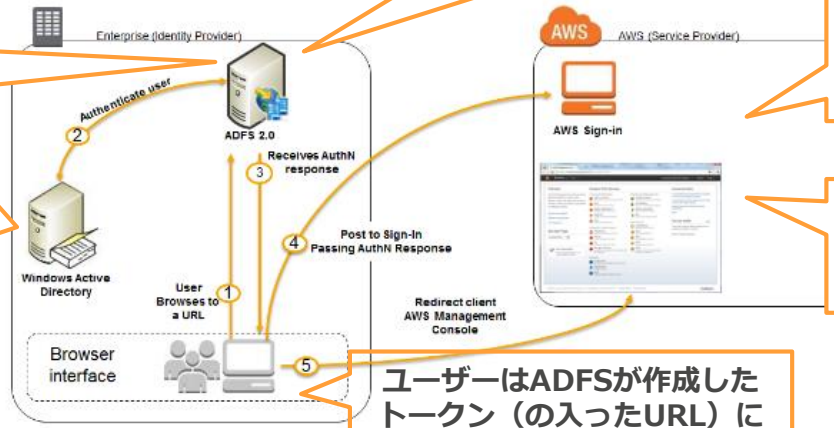
設計と実装例

4. マネージメントコンソールへのアクセス制限

要求ルールを記述

ADFSサーバーはAWS上でもオンプレミスでも利用可能
（ADにアクセスさえできれば利用可能）

対象のAWSアカウントに、事前にトークン発行元のADFSを登録



AD上のユーザー認証を管理すればAWSのID管理はほとんど不要

AWSには設定したロールでアクセス

ユーザーはADFSが作成したトークン（の入ったURL）にリダイレクト

<参考：ADFS設定手順>
http://blogs.aws.amazon.com/security/post/Tx71TWXXJ3UI14/Enabling-Federation-to-AWS-using-Windows-Active-Directory-ADFS-and-SAML-2-0

amazon web services

設計と実装例
4. マネージメントコンソールへのアクセス制限

設計と実装例

4. マネージメントコンソールへのアクセス制限

- CloudTrailによる監査

Agenda

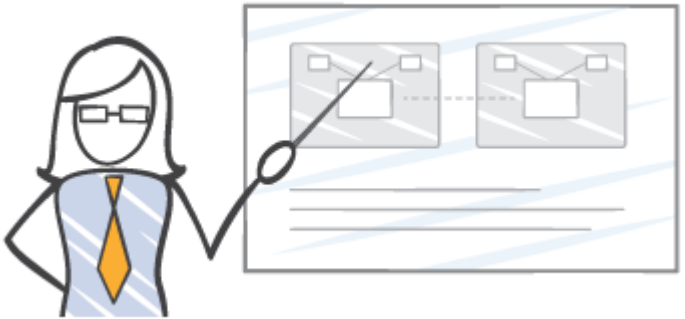
- はじめに
- 権限設計の考慮事項
- 権限設計の進め方
- 設計と実装例
- まとめ

まとめ

- 権限設計は組織のルールを適用する仕組み
- ルールは組織によって様々
- 権限は組織の役割に基づいて設計・管理

まとめ

お悩みの場合はAWSソリューションアーキテクトやプロフェッショナルサービス、もしくはAWSコンサルティングパートナーにご相談いただくのも一案です！



Appendix
他の権限設計の考え方

- 予防的
  - 不正な行為を**制限**
- 主なAWSサービス

IAM

本資料の実装のメインテーマ

- 発見的
  - 不正な行為を**検出**
- 主なAWSサービス

AWS CloudTrail

AWS Config

AWS CloudTrailとAWS ConfigについてはBlack Beltシリーズをご参照ください！
http://www.slideshare.net/AmazonWebServicesJapan/aws-black-belt

Appendix
最小権限

- 最小権限の難しさ
  - 最初から実装することは困難
    - 設計者が業務を完全に知ることは困難
    - 最小権限はビジネス・業務により変化

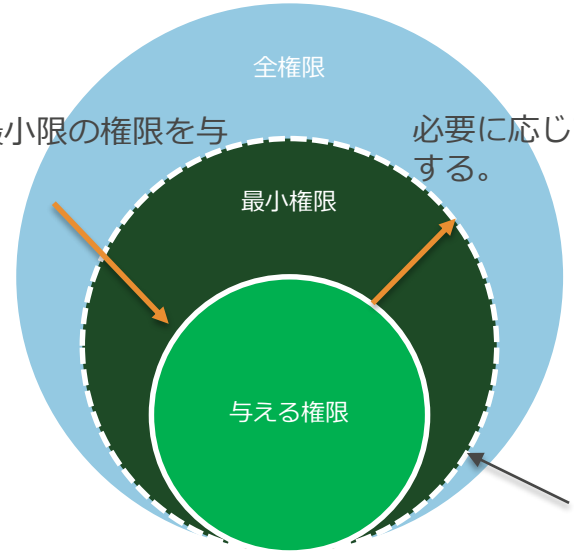
- 運用で最小権限に近づける
  - 最初に与えた権限を管理・修正することで最小権限に近づける

Appendix
最小権限

ホワイトリスト方式

必要な最小限の権限を与える。

必要に応じて権限を付与する。

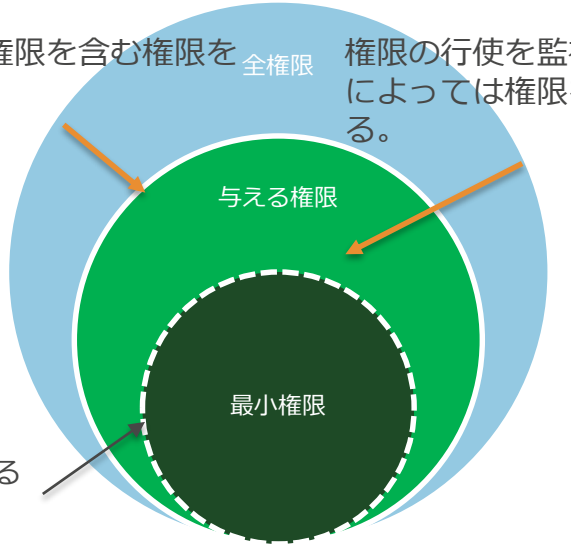


最小権限を完全に特定することは困難。

ブラックリスト方式

必要な権限を含む権限を与える。

権限の行使を監視、場合によっては権限を剥奪する。



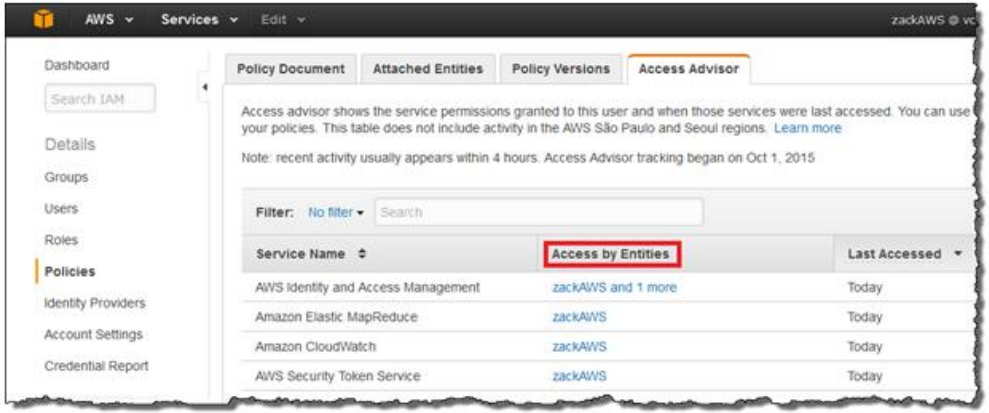
参考資料

- AWS IAM
  - AWS IAMドキュメント
  - http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/introduction.html
- AWS Service Catalog
  - 管理者ガイド
  - http://docs.aws.amazon.com/ja_jp/servicecatalog/latest/adminguide/introduction.html

お知らせ

New

- IAMのメンテナンスがしやすくなりました
  - アクセスした最終時刻をAWSサービスごとに一覧可能に！



2016年6月14日リリース：Now Available: Get Even More Details from Service Last Accessed Data
http://blogs.aws.amazon.com/security/post/Tx3C1P1UVB7WQ6E/Now-Available-Get-Even-More-Details-from-Service-Last-Accessed-Data

Q&A

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 Black Belt Online Seminar

- 6月の配信予定
  - **6月22日(水) 18:00～19:00** Amazon Inspector

- 申し込みサイト
  - http://aws.amazon.com/jp/about-aws/events/#webinar
    (もしくは「AWS イベント」で検索)

AWS Black Belt Online Seminar

- 7月の配信予定
  - **7月　5日(火) 12:00-13:00** Parse.comからAWSへのモバイルアプリの移行
  - **7月　6日(水) 18:00-19:00** Amazon CloudWatch
  - **7月13日(水) 18:00-19:00** AWS Certificate Manager
  - **7月19日(火) 12:00-13:00** コストの観点から見る AWS アカウント管理
  - **7月20日(水) 18:00-19:00** Amazon Redshift
  - **7月26日(火) 12:15-13:00** 公共分野でAWSを活用する方法－事例紹介を中心に
  - **7月29日(金) 18:00-19:00** Amazon Aurora

- 申し込みサイト
  - http://aws.amazon.com/jp/about-aws/events/#webinar
    (もしくは「AWS イベント」で検索)

amazon web services

ご参加ありがとうございました


amazon
web services