
aws
DEV DAY

H - 5

セキュリティ・ガバナンス系サービスを使った安全な Sandbox 環境の作り方

Shuhei Tomita
Senior Technical Trainer
アマゾンウェブサービスジャパン合同会社

目次

- 対象と目的
- Sandbox 環境とは
- Sandbox 環境の課題
- 構築に役立つサービス
  - AWS Budget
  - AWS Cost Anomaly Detection
  - AWS Organizations
  - AWS IAM Identity Center (AWS Single Sign-On 後継)
  - AWS GuardDuty
  - AWS Cloudtrail

自己紹介

- 名前: 冨田 修平
- 所属: AWS シニアテクニカルトレーナー
- 好きな AWS のサービス: AWS Certificate Manager
  - IoT屋さん → ネット広告配信屋さん/ECサイト屋さん → 緑の不動産屋さん
- 担当しているトレーニング/好きな分野
  - Migration/Database/Architecting/Security

Sandbox 環境とは

- AWS上のリソースを実際に作成する環境
  - 公開されているチュートリアルや Workshop を行うため
- 業務システムと関係のある本番環境、開発環境とは別
- 本番環境とは接続しない、機密情報は持ち込まない（重要）
  - 個人情報、ソースコード...etc
  - 持ち込むと一気に必要なセキュリティやガバナンスレベルが上がる
  - 今回のセッションの対象外
- 個人又は会社が所有

なぜ Sandbox 環境が重要なのか

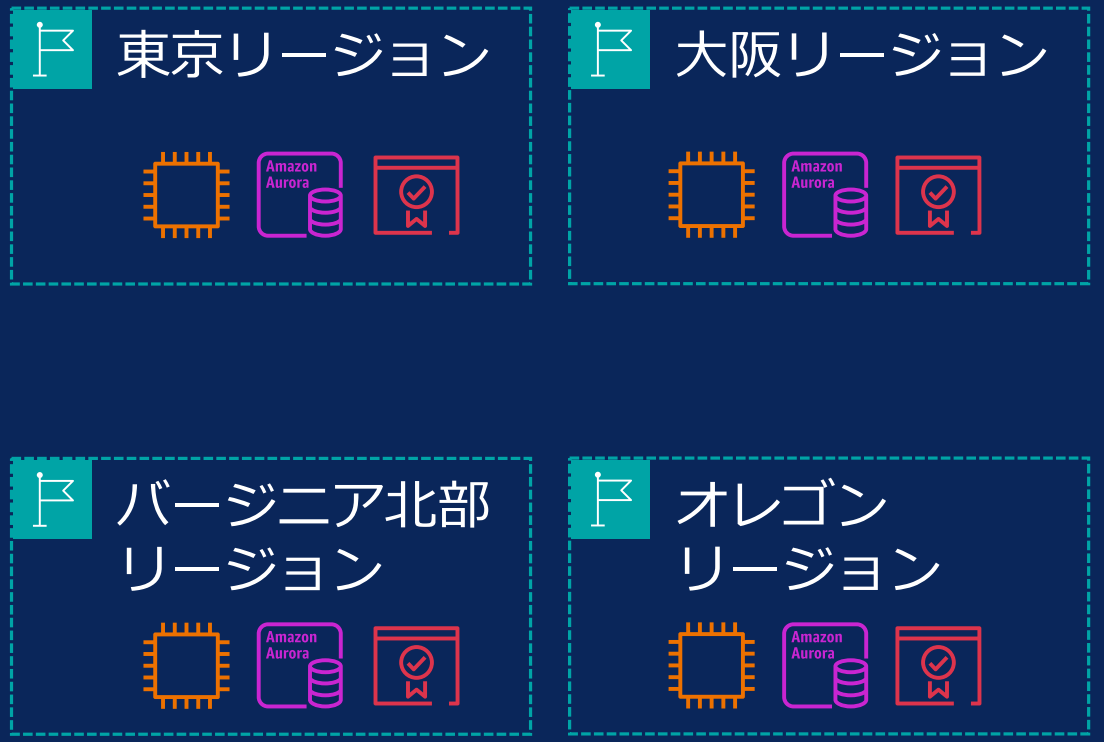
- AWS を使うためには結局実践が大事
  - AWS のサービスドキュメントを読むだけでは理解が難しい事もある
  - サービス毎のチュートリアル/ワークショップの併用がお勧め
    - 机上で分からないこともすぐ分かる
    - ドキュメントに書いてない仕様も多い
      - 各種ワークショップ AWS Workshops (https://workshops.aws/)
  - チュートリアル環境を見るとドキュメントの疑問点が解消
  - 文章だけでなく視覚のほうが情報量が多く構造化しやすい
  - 容易に実験できる

対象＆目的

- 対象
  - 好奇心旺盛な開発者
  - 組織の AWS 学習を促進したい CCoE
  - 突然セキュリティ? ガバナンス? と言われても何からやれば
わからない方
- ゴール
  - 様々な AWS サービスのチュートリアル/ワークショップを簡単かつ安全に試す環境を構築
  - Sandbox 環境の構築を通じてオペレーション、セキュリティ系サービスの基礎を学ぶ

Sandbox 環境の課題(1)

- うっかり想定よりもコストがかかる
  - インスタンス等リソースの削除漏れ
    - 特に複数リージョン使うと発生しがち
  - リージョン間の価格の差異
  - 意図せず最低コストが高いサービスを使う
    - 削除漏れと合わさると高額になりがち



Sandbox 環境の課題(2)

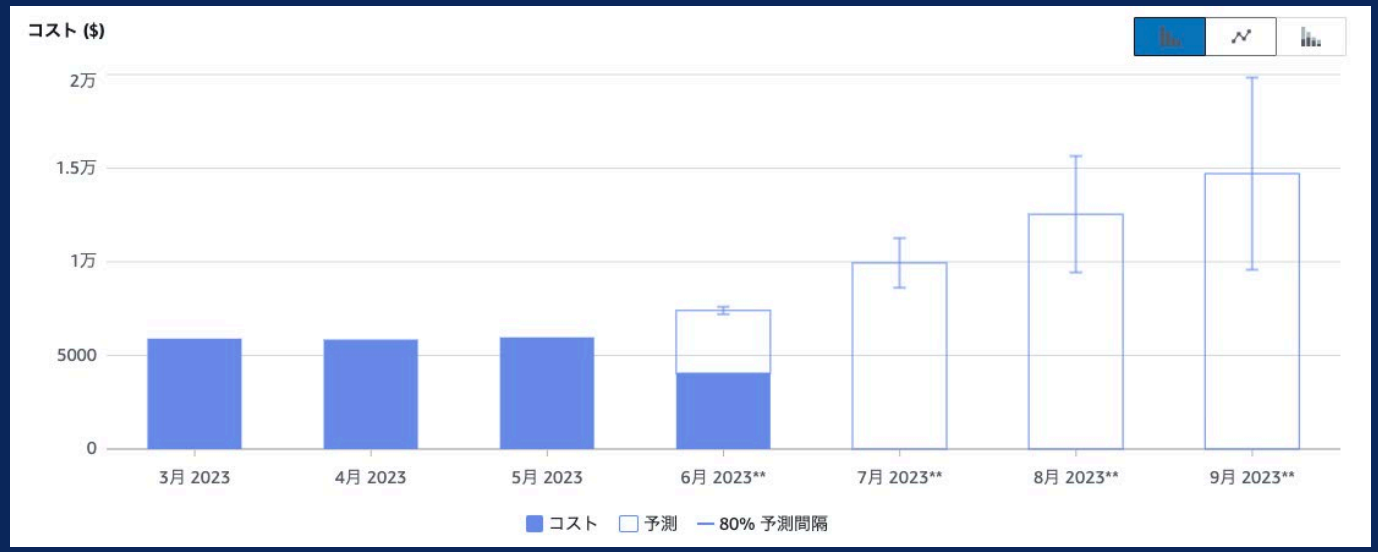
- セキュリティ
  - 不適切なサービス使用によるインシデント
    - 機密情報の漏洩には繋がらなくとも、暗号通貨の採掘などに繋がる恐れ
  - しかし予防的統制が厳密すぎると Sandbox 環境として学習ができない

  - 可用性、追跡性の確保を重視
    - 予防的統制ではなく発見的統制をメイン
    - 学習のためには自由度も大事
  - ただし学習用としても非推奨なアクション、サービスは利用不可にしておく
    - インシデントの原因になりやすいアクションなど

Sandbox 環境の構築方針

- AWS Cloudformation or AWS CLI or マネジメントコンソール？
  - 一度は AWS CLI 又は マネジメントコンソールから手動で構築することをお勧め
  - **自分で理解していないものが壊れると足かせにしかならない**
- **この環境を作る事自体がセキュリティやガバナンスの学習の機会**
  - 後回しになりがちなセキュリティ、ガバナンス面のベースラインになる
  - なるべく複雑にしない
    - 自分の Sandbox 環境を自分で作る事が重要なワークショップ、学習の課題
    - セキュリティやオペレーションのレベルが上がる
  - できれば追加費用が発生しない範囲で

AWS Budgets



- 月末になって慌てないために
- メール通知
  - 予測とアクションが便利
  - 予測：このままいくと月末には XXX USD
  - アクション：SCP などを設定してこれ以上のリソース作成等制限を行う
  - AWS Organizations と連携可能

- Xbar (旧 bitbar) AWS Cost Plugin

  - Mac 用ツールバーアプリケーション すぐ現状の数値が見える状態にする
  - マネジメントコンソールなしに簡単にコストが把握できる

AWS Budget メール文面サンプル

AWS Budget Notification
AWS Account *8235*

June 10, 2023

Dear AWS Customer,

You requested that we alert you when the **actual cost** associated with your *My Monthly Cost Budget* budget **exceeds $255.00** for the current month. The month **actual cost** associated with this budget is **$258.38**. You can find additional details below and by accessing the AWS Budgets dashboard.

Budget Name	Budget Type	Budgeted Amount	Alert Type	Alert Threshold	ACTUAL Amount
My Monthly Cost Budget	Cost	$300.00	ACTUAL	> $255.00	$258.38

Go to the AWS Budgets dashboard

AWS Cost Anomaly Detection

- どこにコストがかかっているのか、いつから発生したのか
- 機械学習（異常検知）を使って検知することでコスト超過原因を通知
- 閾値(% or USD)を設定し検知した異常の幅が閾値に達するとアラート
- AWS Organizations と連携可能

閾値
% or USD

AWS Cost Anomaly Detection
メール文面サンプル

AWS Cost Management: Anomaly Detection 2023-06-06
AWS Account:

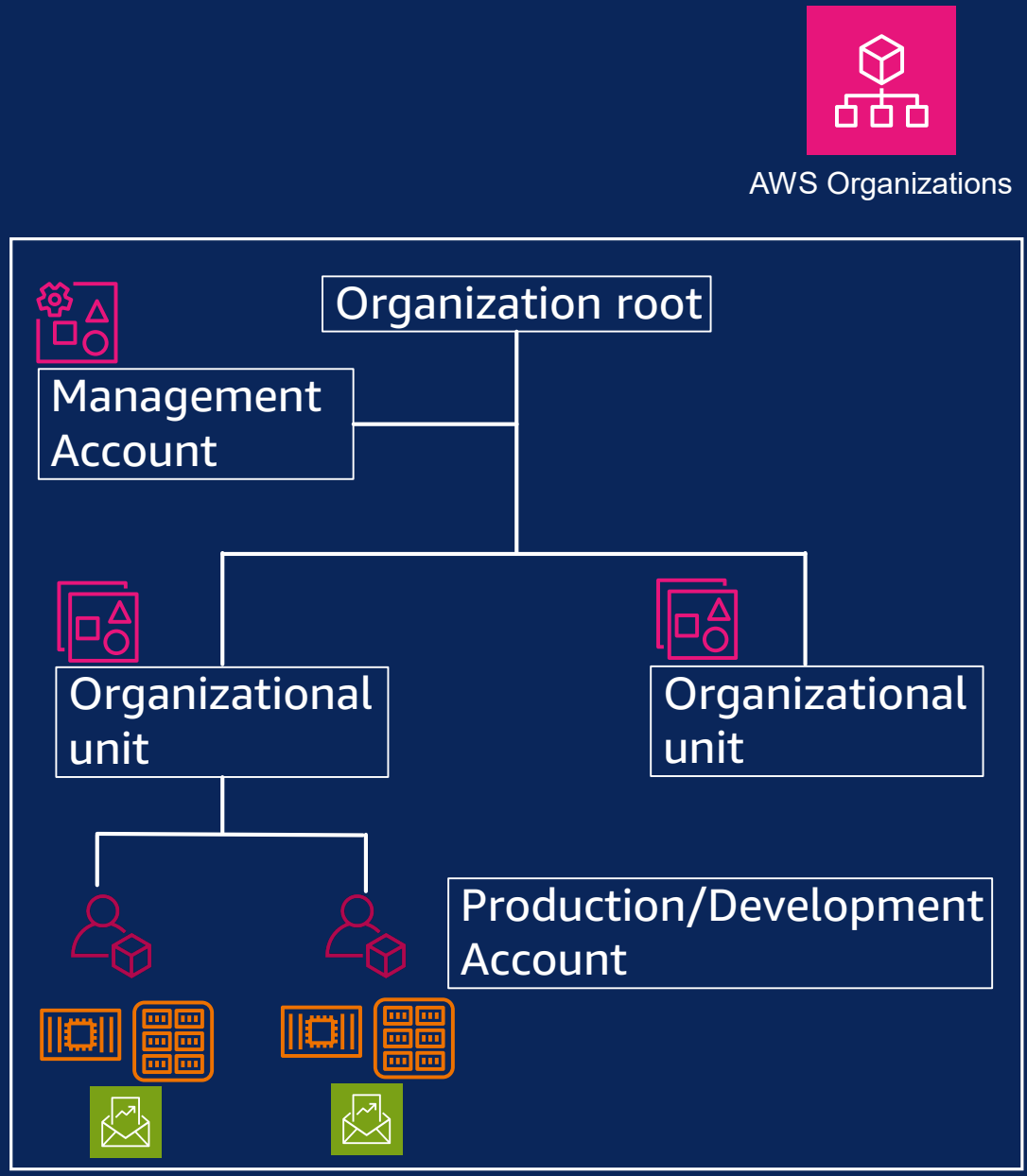
Dear AWS Customer,

You are receiving this alert because you asked us to provide you with a summary of unusual AWS usage patterns for accounts in your AWS organization with payer account id number above. Below is a recent list of anomalies that have been detected up until 2023-06-06 with corresponding root cause(s).

Service*	Date	Cost Impact	Root Cause(s)	Monitor	Next Steps
Amazon Relational Database Service	Start Date: 2023-06-02T00:00:00Z Last Detected Date: 2023-06-05T00:00:00Z Duration: 4 day(s)	Max Daily Impact: $49.92 Total Impact: $192.92	Member Account: 0362 Member Account Name: advarch-child3 Region: us-east-1 AWS Service: Amazon Relational Database Service Usage Type: InstanceUsage:db.r6g.2xl	Name: kobetu-service Type: AWS services	View In Anomaly Detection

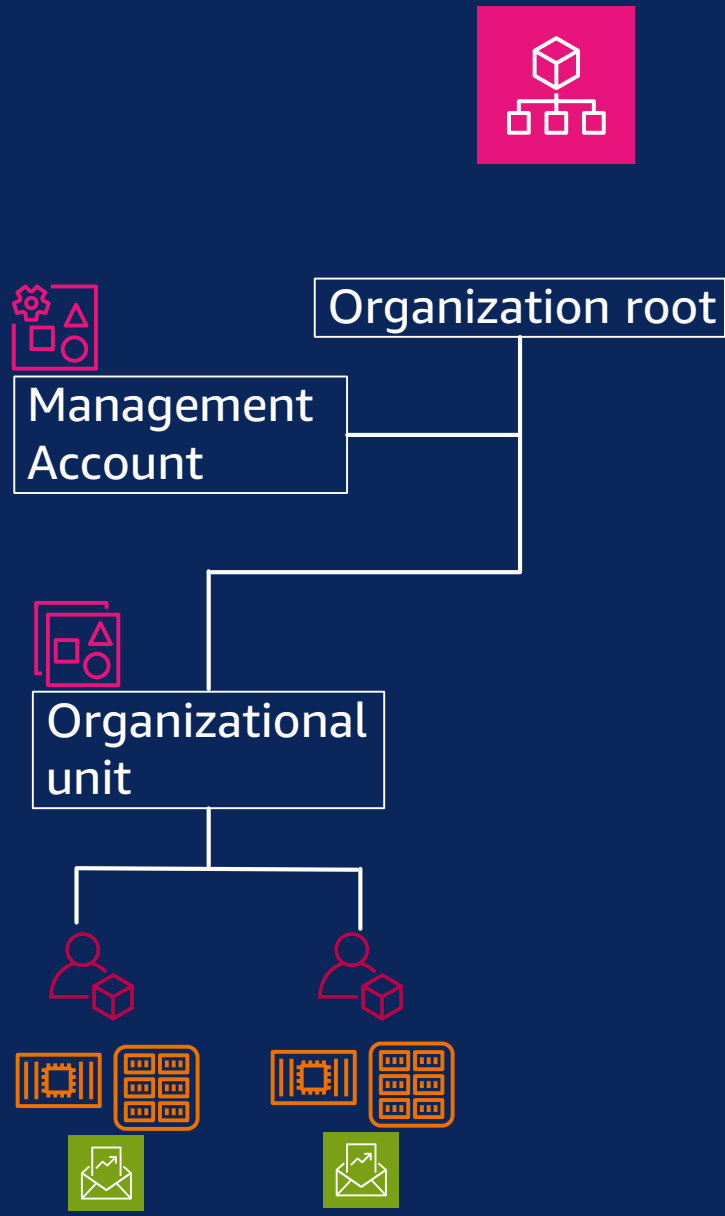
AWS Organizations とは

- 複数のアカウントをまとめるサービス
  - マルチアカウント管理の重要な構成要素
  - 本番/開発環境の論理的な分離等が可能
  - 管理アカウントと実験用アカウントの分離
    - 削除すべきリソースとそうでないリソースの見分け
    - Organizations 自体は無料
- 管理アカウント側での集中制御
  - トレーサビリティ
  - ガバナンス
    - マルチアカウント構成



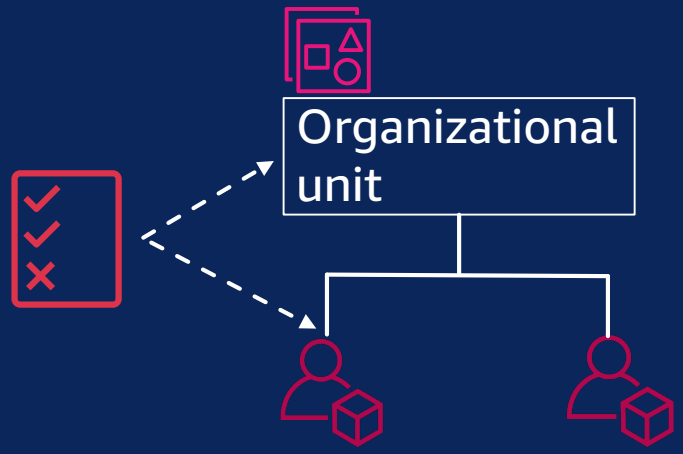
AWS Organizations のガバナンスモデル(1)

- 管理アカウント
  - Organization 又はメンバーアカウントを作成/削除/変更/招待するために使用するアカウント
  - Organization 内の全ての請求は管理アカウント側に一括請求される
  - Organization の管理専用に使用することを推奨
- OU (組織単位)
  - Organization 内のアカウントのコンテナ、ネストさせることも可能
  - ツリー構造が構築できる



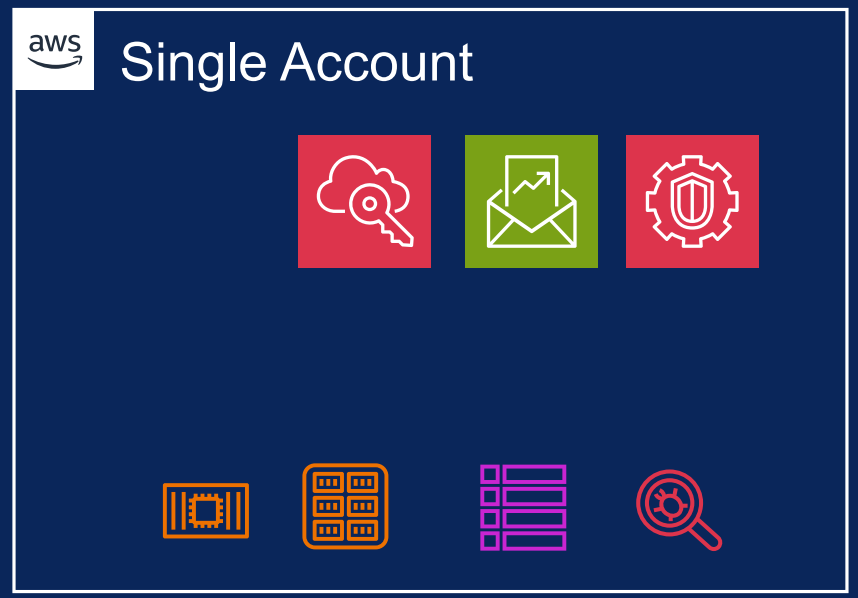
AWS Organizations のガバナンスモデル(2)

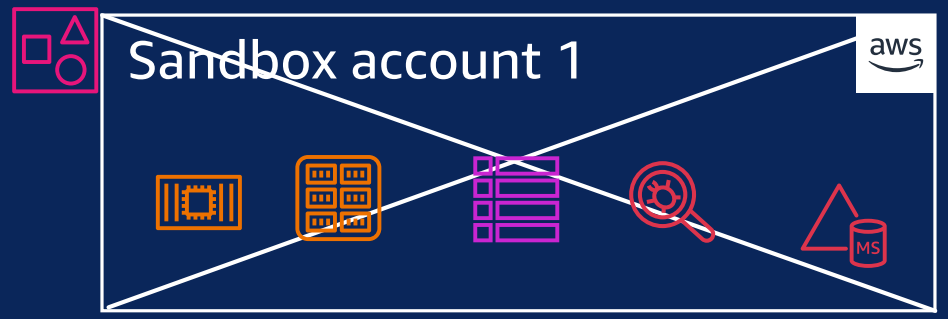
- メンバーアカウント
  - Organization によって管理されるアカウント
- ポリシー
  - Service Control Policy (SCP)
    - アカウント又は OU にアタッチするポリシー
    - アカウント内のユーザやロールが使用可能なアクションやサービスを制御する
      - 実際に可能なアクションは IAM ユーザやロールのポリシーと SCP の両方で許可されているもの(and)
    - 許可リスト又は拒否リスト戦略が利用可能
      - 上階層のOUにアタッチした SCP は下階層の OU 又はアカウントに継承される
    - 注意：管理アカウントから実行するアクションは制御しない



アカウントの閉鎖による不要リソースの削除

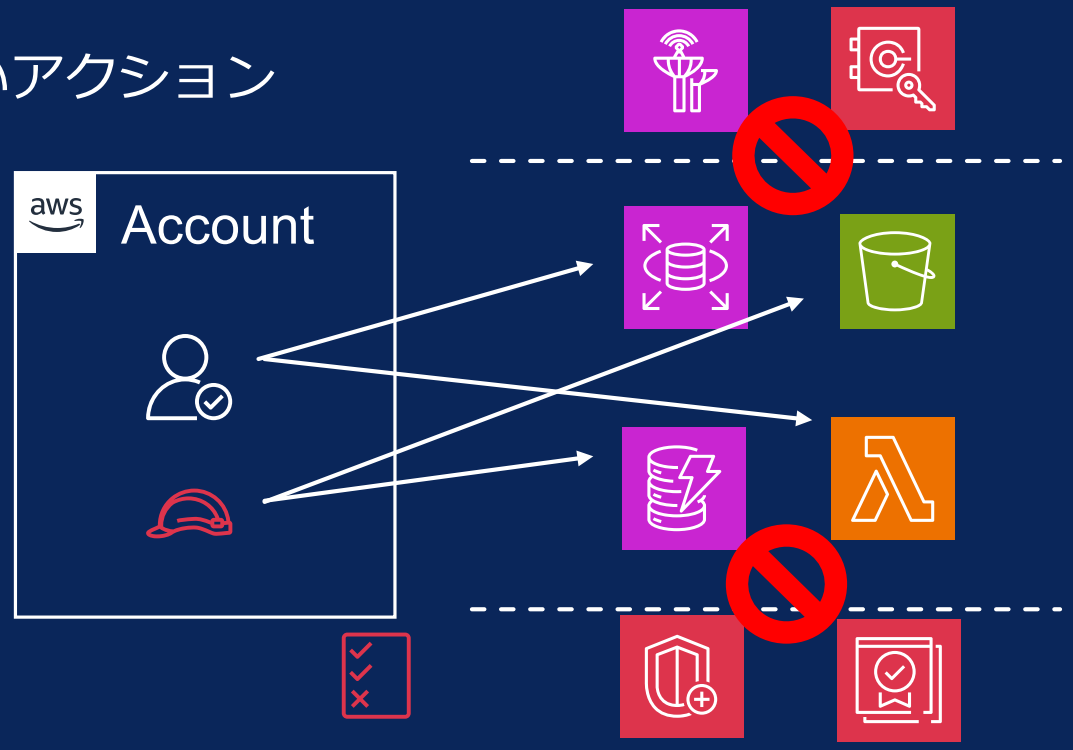
- AWS Organizations を使う事でアカウントの作成閉鎖が容易
  - アカウントを閉鎖することで不要リソースをまとめて削除可能(条件あり)
  - aws-nuke も利用可能
  - 注意：アクティブなサブスクリプションがある場合には請求が継続





Service Control Policy (SCP)

- アカウント単位で利用可能なサービス、アクション、条件を制御
  - 誤って使用しないよう Sandbox 環境では不要な機能を必要に応じて禁止できる
    1. 高価なサービス、インスタンスタイプ
    2. 継続的なサブスクリプション型サービス
    3. Sandbox であってもセキュリティ上推奨されないアクション
    4. 価格差の大きいリージョン



Service Control Policy の制御対象(1)

- アカウント単位で利用可能なサービス、アクションを制御
  1. 意図せず高価になりがちなサービス、インスタンスタイプ
     - AWS CloudHSM
     - AWS Shield Advanced
     - AWS Outposts
     - 大きなサイズの各種インスタンス/ボリューム
     - Amazon Redshift (Redshift Serverless 除く)
     - Amazon EC2 Dedicated Hosts / ベアメタルサーバ
       - 等々
  2. 一定期間のサブスクリプション又はコミットメントを伴うサービス
     - Reserved Instance / Savings Plan / AWS Marketplace サブスクリプション

Service Control Policy の制御対象(2)

- アカウント単位で利用可能なサービス、アクションを制御
  3. Sandbox であってもセキュリティ、ガバナンス上あまり推奨されないアクション
     - organizations:LeaveOrganization
     - iam:CreateAccessKey
     - ルートユーザによるオペレーション
  4. 価格差の大きいリージョン
     - 例：リージョン毎の価格差

	バージニア北部（米国）	オレゴン（米国）	東京（アジア）	サンパウロ（南米）
S3 標準(1GBあたり)	0.023 USD	0.023 USD	0.025 USD	0.0405 USD
EC2 t3.micro (1時間あたり)	0.0104 USD	0.0104 USD	0.0136 USD	0.0168 USD

本資料では2023年6月時点のサービス価格に基づいています

サンプル SCP ポリシー(1)

- 特定のリージョン以外の利用を禁止するポリシー(抜粋)

```
"Effect": "Deny",
"NotAction": ["a4b:*","route53","pricing","iam","sts","waf"(中略)],
"Resource": "*",
"Condition": {
        "StringNotEquals": {"aws:RequestedRegion":
                ["us-west-2","us-east-2"]
        },
```

サンプル SCP ポリシー(2)

- 特定のインスタンスタイプ以外の起動を禁止するポリシー(抜粋)

```
"Effect": "Deny",
"Action": ["ec2:RunInstances","ec2:startInstances"],
"Resource": [ "arn:aws:ec2:*:*:instance/*"],
"Condition": {"StringNotEquals": {"ec2:InstanceType": "t2.micro"}}
```

"StringNotLike": { "ec2:InstanceType": "t3.*" }
なども可能

サンプル SCP ポリシー(3)

- 特定のサービス/アクションの使用を禁止するポリシー(抜粋)

```
"Effect": "Deny",
"Resource":"*"
"Action": [
        "cloudhsmv2:*",
        "ec2:allocateHosts",
        "outposts:*",
        "iam:CreateAccessKey",
        "organizations:LeaveOrganization" ]
```

サンプル SCP ポリシー(4)

- 一定期間のコミットメントを伴うサービス/アクションを禁止するポリシー(抜粋)

```
"Effect": "Deny",
"Resource":"*"
"Action": [
        "savingsplans:*",
        "ec2:PurchaseReservedInstancesOffering",
        "shield:CreateSubscription" ]
```

サンプル SCP ポリシー(5)

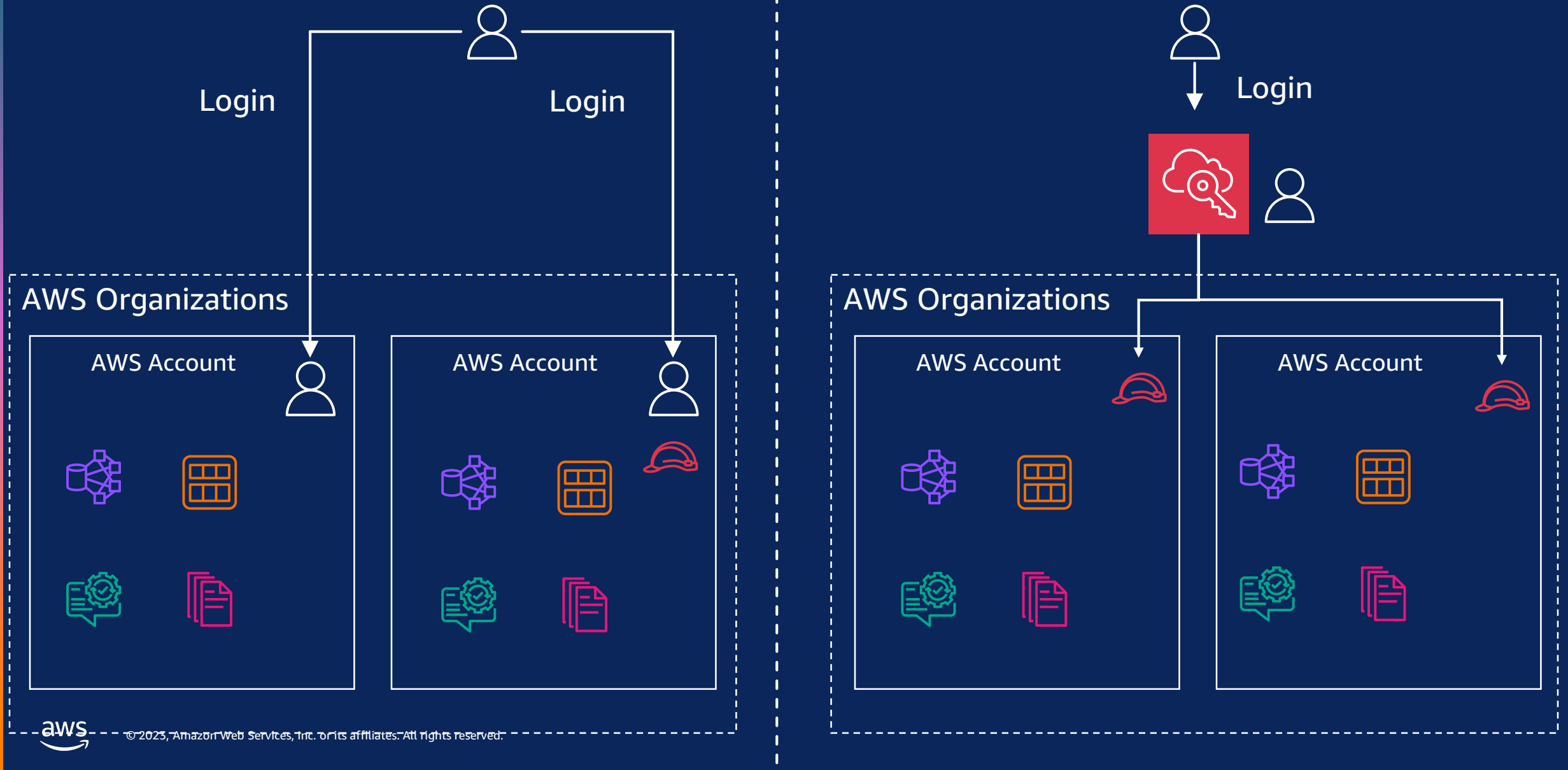
- ルートユーザによるオペレーションを禁止する(抜粋)

```
"Effect": "Deny",
"Action": ["ec2:*"],
"Resource": ["*"],
"Condition": {
        "StringLike": {"aws:PrincipalArn": ["arn:aws:iam::*:root"]}
}
```

AWS IAM Identity Center (AWS Single Sign-On 後継)

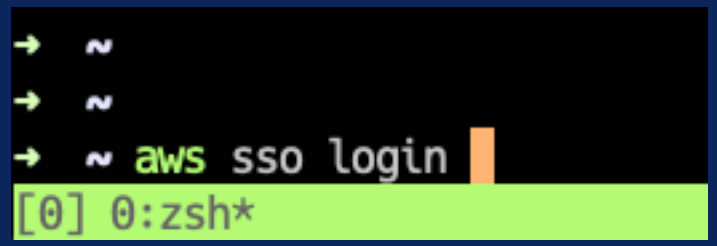
- AWS IAM Identity Center を使いマルチアカウント環境へ SSO が可能
  - Organization 内の複数アカウントに対してシングルサインオンが可能
  - AWS アカウント側のIAM ユーザは基本作らない方針での運用が可能
    - IAM Identity Center 側でのユーザ管理や 外部 IDP が利用可能
    - 単体では無料
  - WebAuthn 対応の TouchID / Windows Hello カメラ などの MFA も可能
    - コンテキストアウェア認証にも対応
- AWS CLI は AWS IAM Identity Center と連携可能
  - CLIのための永続的アクセスキーは発行不要

AWS IAM Identity Center (AWS Single Sign-On)



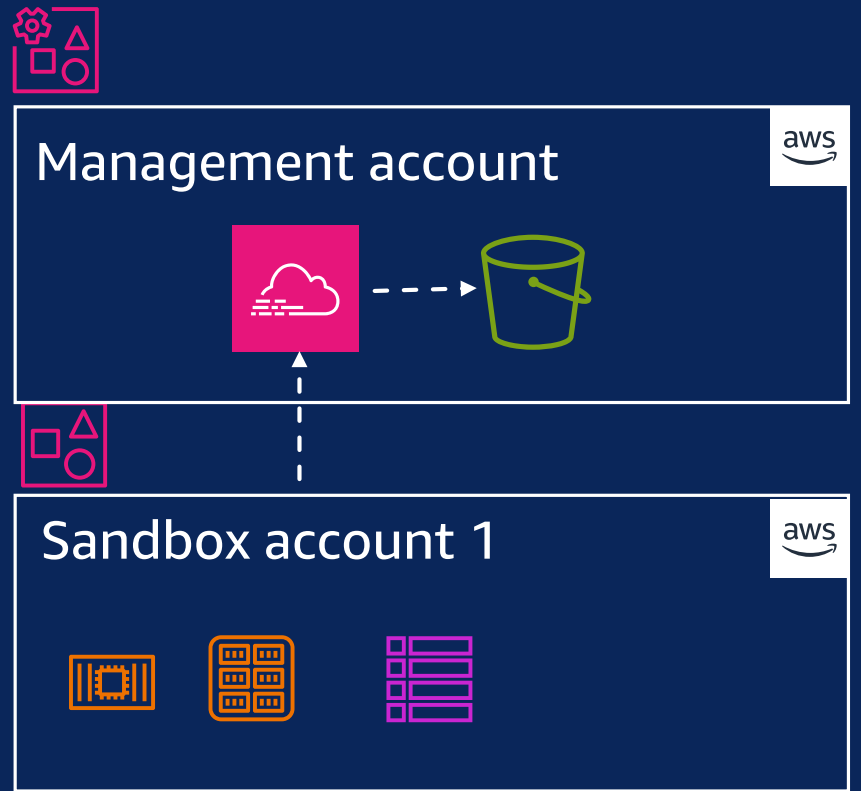
AWS CLI と AWS IAM Identity Center の連携

- AWS CLI の実行には認証情報(アクセスキー)が必要
  - アクセスキーの発行は外部への漏洩によるインシデントに繋がりやすい
  - AWS IAM Identity Center と AWS CLI の連携により、一時的な認証情報の使用が可能
    - 認証情報はデフォルト8時間有効
    - aws sso login コマンドを実行すると Web ブラウザが起動し、認証を行う
    - マネジメントコンソールと CLI の間でも SSO できる



AWS CloudTrail の活用

- ユーザーアクティビティと AWS API 使用状況の追跡
- Sandbox 環境全体のトレーサビリティを確保するためのサービス
- 管理アカウント側から Organization 全体の証跡を設定可能
  - メンバーアカウント側への設定は不要



Amazon GuardDuty の活用

- AWS アカウントの脅威を様々な情報ソースから機械学習を使って検知
- Organization 全体に有効化できる
- 管理又は委任管理者アカウントで Organization 全体の Finding を確認
  - メンバーアカウント側への設定は不要

その他のAWSセキュリティガバナンス系サービス

- AWS Config
  - リソースを継続的にルールに従って適切なリソース構成になっているかを監査
- AWS Security Hub
  - セキュリティアラートを集約し、ベストプラクティスに沿っていることを確認
- Amazon Macie
  - 機械学習とパターンマッチを利用してS3バケット内の機密データを検出
- AWS Cloudformation StackSets
  - 複数リージョン、アカウントにリソースを簡単に作成
- AWS Control Tower
  - 安全なマルチアカウント AWS 環境のセットアップと管理

まとめ

- AWS サービスの理解や組織内での AWS 利用促進には Sandbox 環境が重要
  - 運用には本番環境とも共有する課題がある
  - オペレーション、セキュリティ、ガバナンス系のサービスが利用可能
  - Sandbox 環境の構築自体が学習の機会
  - 本番環境の運用にも役立つ
- まずは AWS Budgets AWS Organization のセットアップから

- おまけ：お気に入りワークショップ
  - AWS Well-Architected Labs https://wellarchitectedlabs.com/

AWS 認定取得: Associate チャレンジ実施中！

Associate レベルの認定取得を応援するキャンペーンを実施中（英語）

https://pages.awscloud.com/GLOBAL-ln-GC-Traincert-Associate-Certification-Challenge-Registration-2023.html　***7 月より日本語でも展開予定**

チャレンジ参加メリット

- 効率よく認定取得するためのコンテンツを集めた**リソースハブの利用**
- Associate レベルの認定資格 **50% 割引バウチャー**獲得

期間

- チャレンジ登録： 9 月 30 日 午前 10 時まで
- 認定受験期限：10 月 31 日まで

皆様のチャレンジ参加登録お待ちしています！