OCIjp#20 LT

「ネットワーク・ソース」によるアクセス元IP制限

小畑 知義

2021/7/20

NRI

Share the Next Values!

自己紹介

小畑 知義（おばた ともよし）

■ 経歴

・NRI
・アプリ開発　約７年
・基盤　　約５年

■ OCIとの関わり

・2019年5月の**東京リージョン開設をきっかけに、OCIを利用開始**
・**インフラエンジニアとして、IaaS (PaaS) を利用**した環境構築を担当

■ 資格

・Oracle Cloud Infrastructure 2019 Certified Architect Professional
・Oracle Cloud Infrastructure Foundations 2020 Certified Associate
・Oracle Cloud Infrastructure 2020 Certified Architect Associate
・Oracle Cloud Infrastructure 2020 Certified Cloud Operations Associate

■ 最近の個人的なトピック

・技術書オンラインイベント「技術書典11」に出展（自己出版）
・自身は**OCI担当**として、AWS/Azure/GoogleCloud各担当と共著
・**優劣をつけることなく**、OCIのこの機能ってAWSだと何ていうの？どう違うの？
などの**特徴や思想の違いにフォーカスした内容**

技術書典：https://techbookfest.org/product/4867756493111296
BOOTH　：https://cloud-quadrant.booth.pm/items/3094507

本題です

OCI操作の「アクセス元IPを制限しよう」という話になることってありませんか？

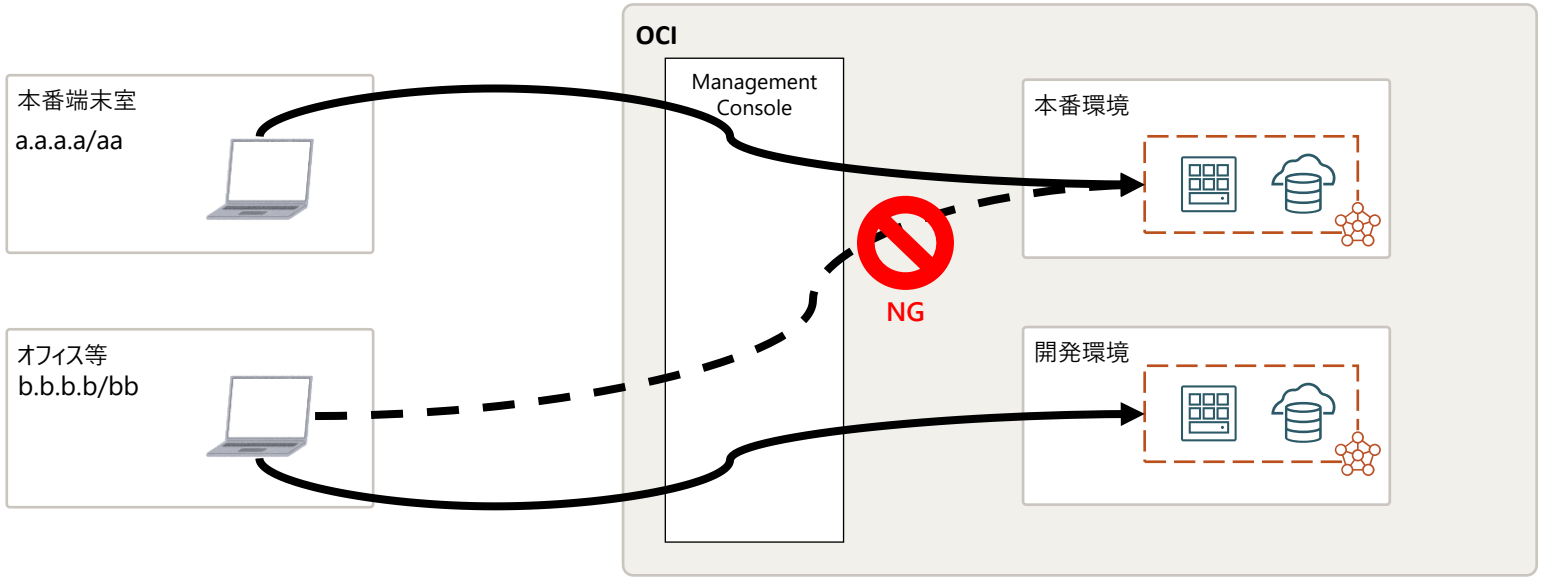
VMへのログインではなく、
マネジメントコンソール等からの
OCI操作の話

様々な事情で苦労した点、
工夫した点などをご紹介します

今回、私が達成する必要のあるお題目は以下でした

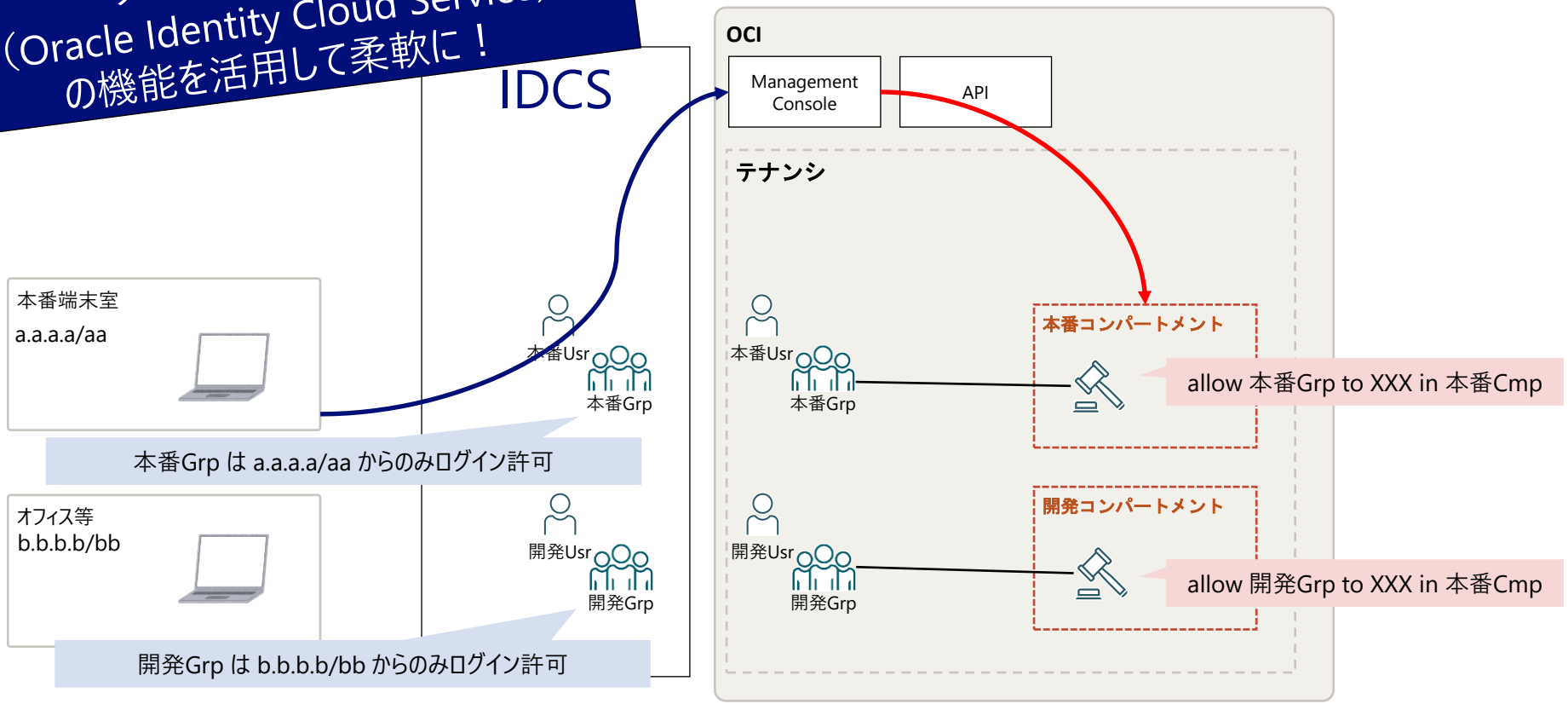
本番環境、開発環境それぞれで
OCIに対する操作が可能な端末を限定すること

<イメージ>



当初案はこちら

ソースIP制限はIDCS
（Oracle Identity Cloud Service）
の機能を活用して柔軟に！



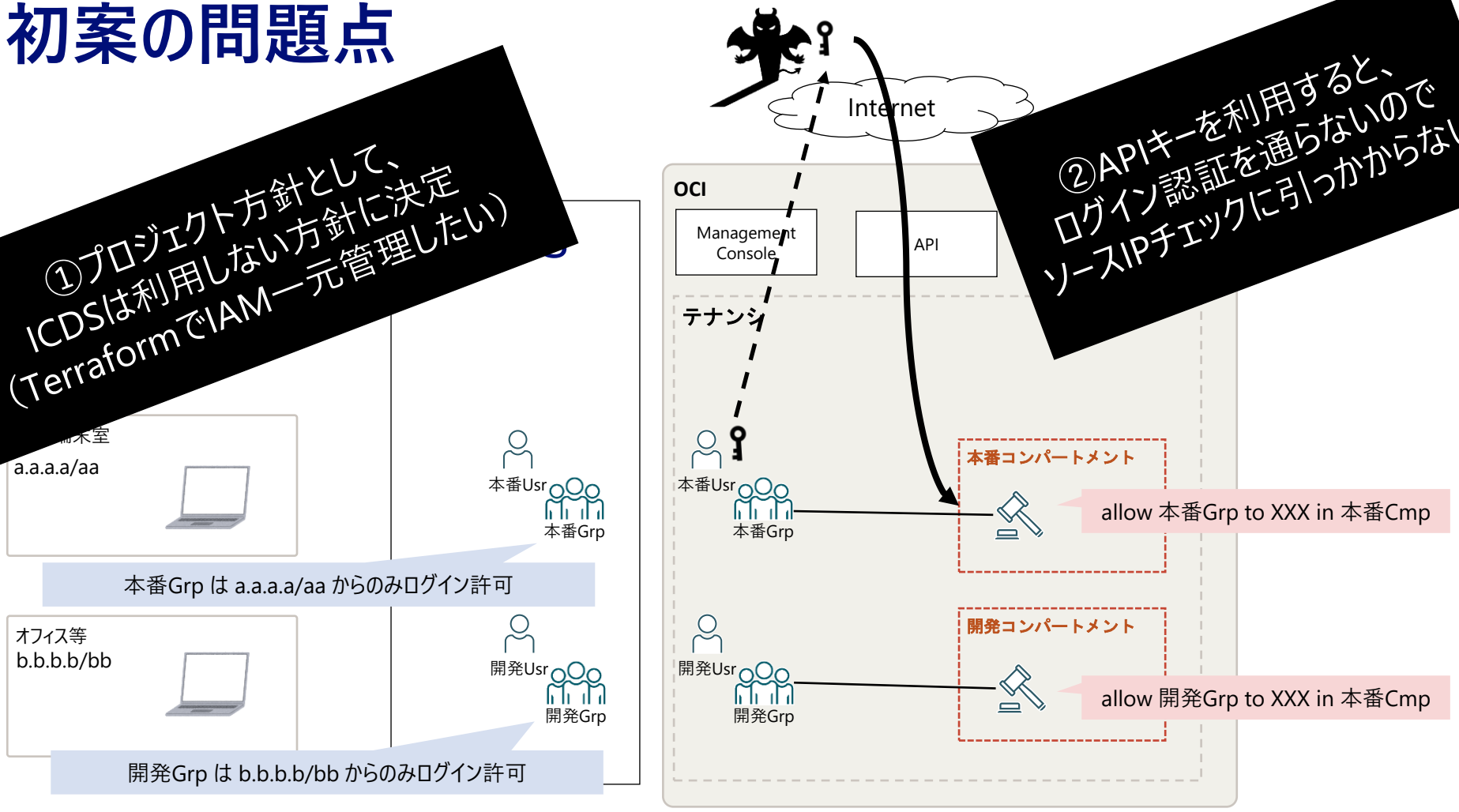
ログイン（認証）の時点で
グループ別に**ソースIP制限**
※IDCSを活用

ポリシー（認可）で
グループ別に操作対象を限定

当初案の問題点

①プロジェクト方針として、
ICDSは利用しない方針に決定
（TerraformでIAM一元管理したい）

②APIキーを利用すると、
ログイン認証を通らないので
ソースIPチェックに引っかからない



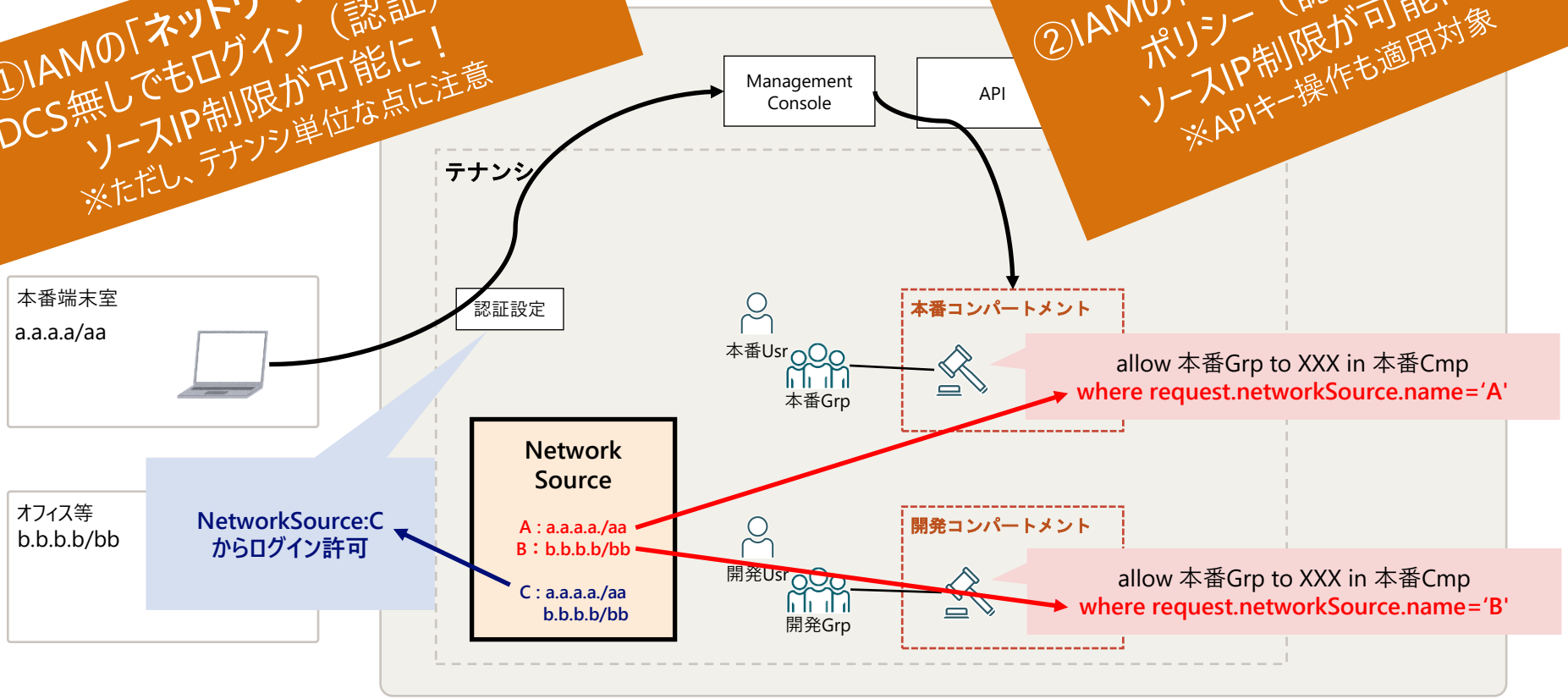
ログイン（認証）の時点で
グループ別に**ソースIP制限**
※IDCSを活用

ポリシー（認可）で
グループ別に操作対象を限定

最終案

①IAMの「**ネットワーク・ソース**」なら
IDCS無しでもログイン（認証）時の
ソースIP制限が可能に！
※ただし、テナンシ単位な点に注意

②IAMの「**ネットワーク・ソース**」なら
ポリシー（認可）でも
ソースIP制限が可能に！
※APIキー操作も適用対象



ログイン（認証）の時点で
テナンシで**ソースIPを広めに制限**
※Management Consoleの場合

ポリシー（認可）でも
コンパートメント別に**ソースIPを制限**

まとめ

IAMの「ネットワーク・ソース」機能なら

認証時(ログイン) に **テナンシ単位で** ソースIP制限が可能

→今回は1テナンシ内でコンパートメントによる環境分離という前提だったが、
認証段階から制限したい場合はテナンシごと分割するという選択もある。

** ルート・コンパートメントのリソース（認証設定、IAMユーザ/グループ、Audit保持期間、サービス制限など）はテナンシ内で共通となるため、これらを共有できる場合は同一テナンシで複数コンパートメントの方が管理負荷は少ない*

認可時(ポリシー) に **コンパートメント単位で** ソースIP制限が可能

→APIキーを利用をしたいなら、この設定が必須となる。APIキー流出は
セキュリティ・インシデントの代表例なので、APIキー自体の利用を禁止
するという選択もある。

** 正確にはコンパートメント単位だけではなく、Policyで指定できるレベルで制御が可能（サービス、OCID、タグなど）*
** CLIの利用自体は Cloud Shell や Instance Principal を活用することでも可能*
** 現時点ではポリシーによるネットワーク・ソース制限に未対応のサービスもあるため、利用サービスについては確認が必要*