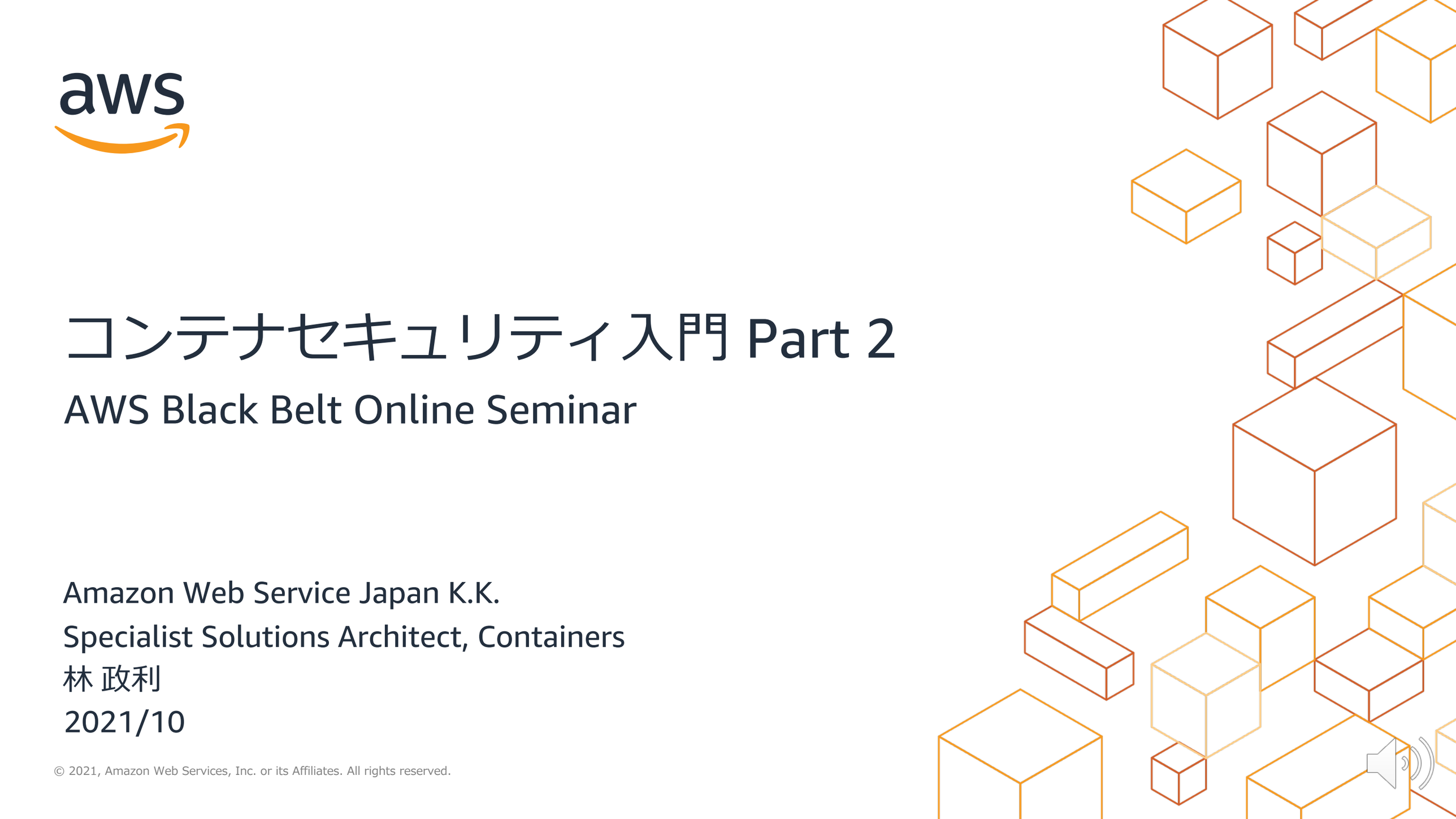
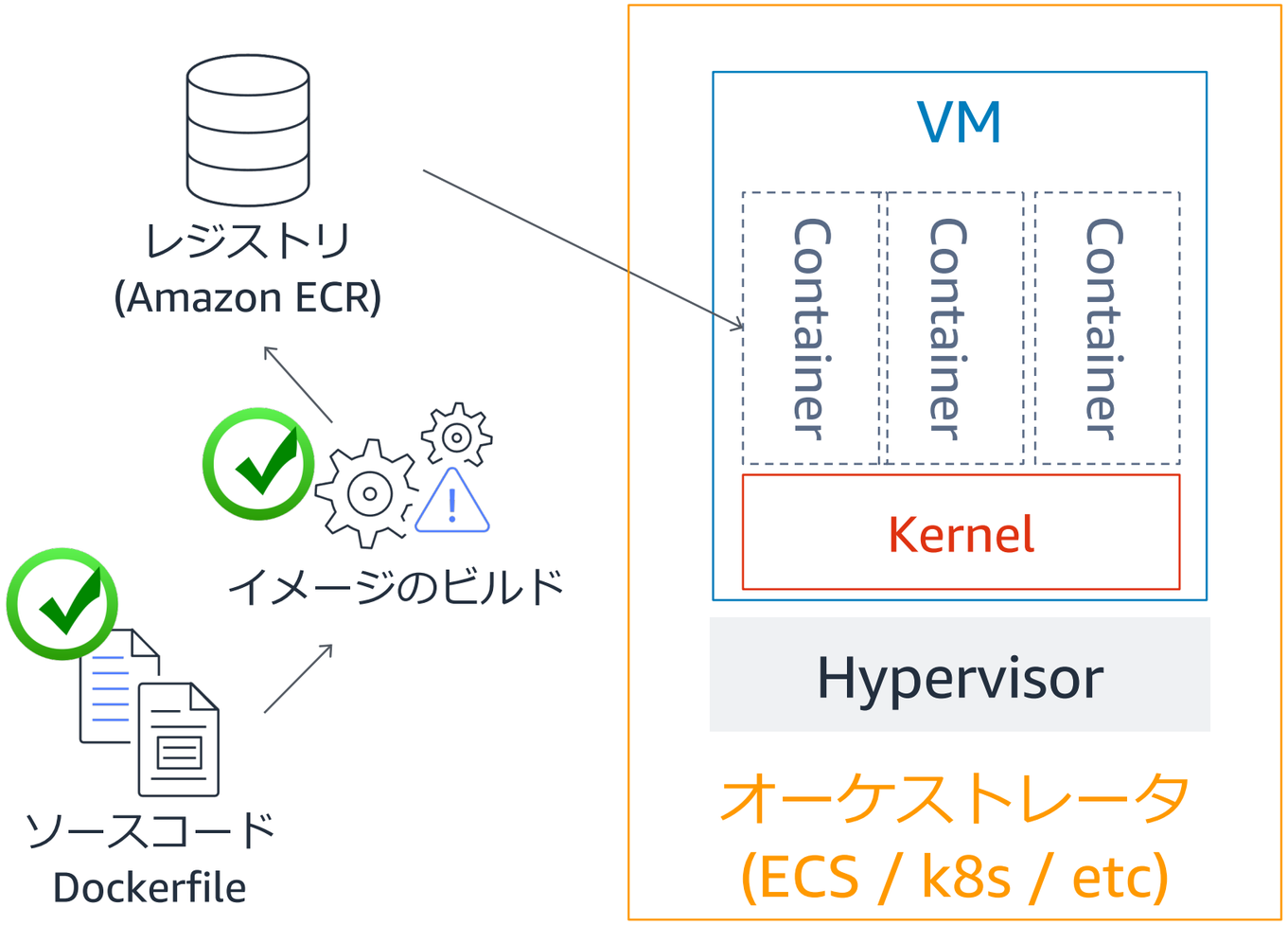


コンテナセキュリティ入門 Part 2

AWS Black Belt Online Seminar

Amazon Web Service Japan K.K.
Specialist Solutions Architect, Containers
林 政利
2021/10

アジェンダ



- イメージの開発とビルド
- サプライチェーン
- オーケストレータの保護
- ホストのセキュリティ
- 実行時のセキュリティ

サプライチェーンの保護

安全なイメージを安全な経路でコンテナとして届ける

イメージレジストリの保護

イメージレジストリを不正なアクセスから保護する

イメージレジストリのホワイトリスト化

安全なイメージレジストリのみを使う

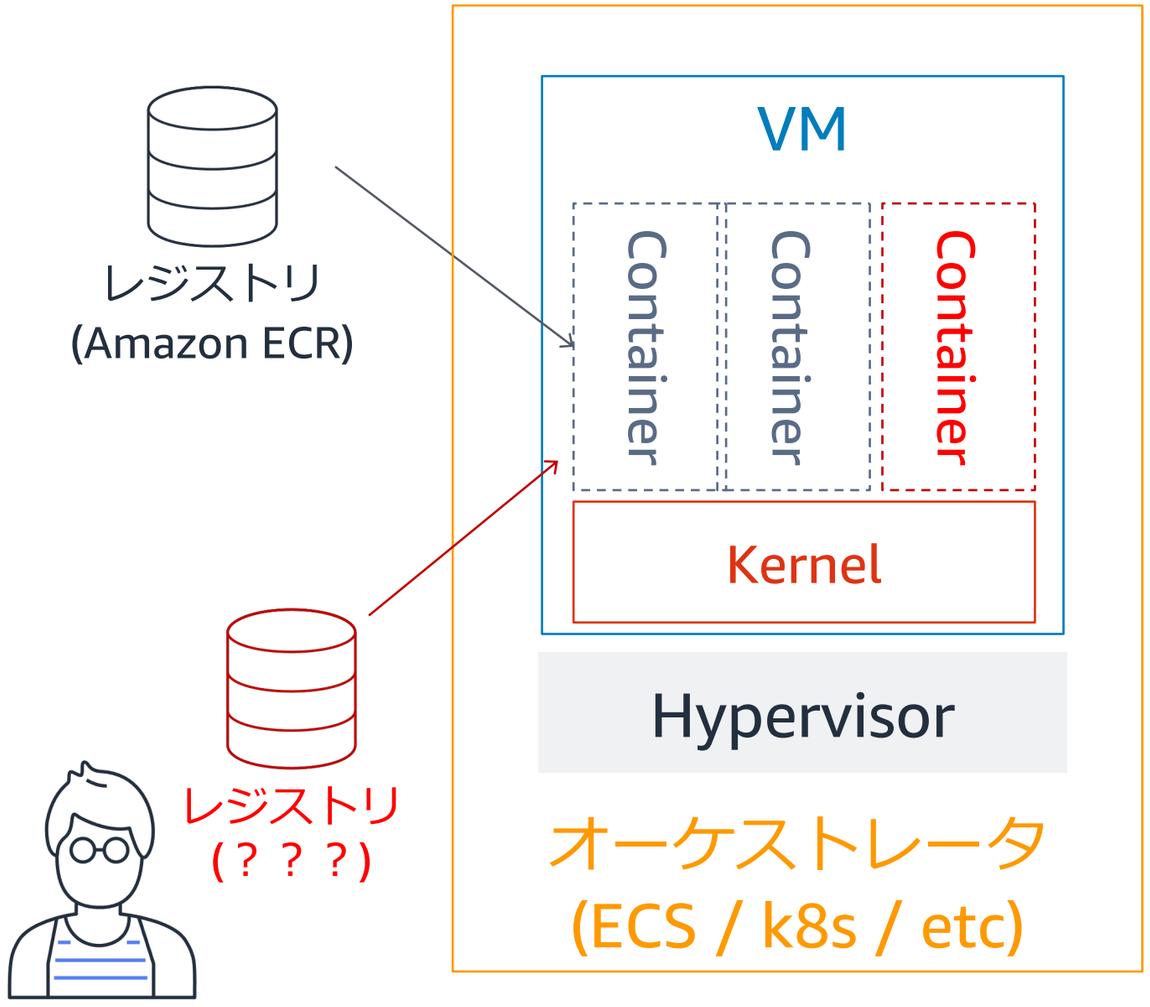
コンテナレジストリのアクセス保護

アカウント内の運用で、特定のチームのみECRリポジトリアクセスを許可する例

```
{
  "Statement": [{
    "Sid": "AllowPushPull",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::123456789012:role/<team_a_role_name>"
    },
    "Action": [ "ecr:GetDownloadUrlForLayer", "ecr:BatchGetImage",...],
    "Resource": [ "arn:aws:ecr:region:123456789012:repository/team-a/*"
```

https://aws.github.io/aws-eks-best-practices/security/docs/image/#create-iam-policies-for-ecr-repositories

コンテナレジストリのホワイトリスト化



信頼できるレジストリのみを使う

レジストリに安全なイメージを登録しても、そのイメージが使われなければ意味がない

悪意あるイメージによる侵害例

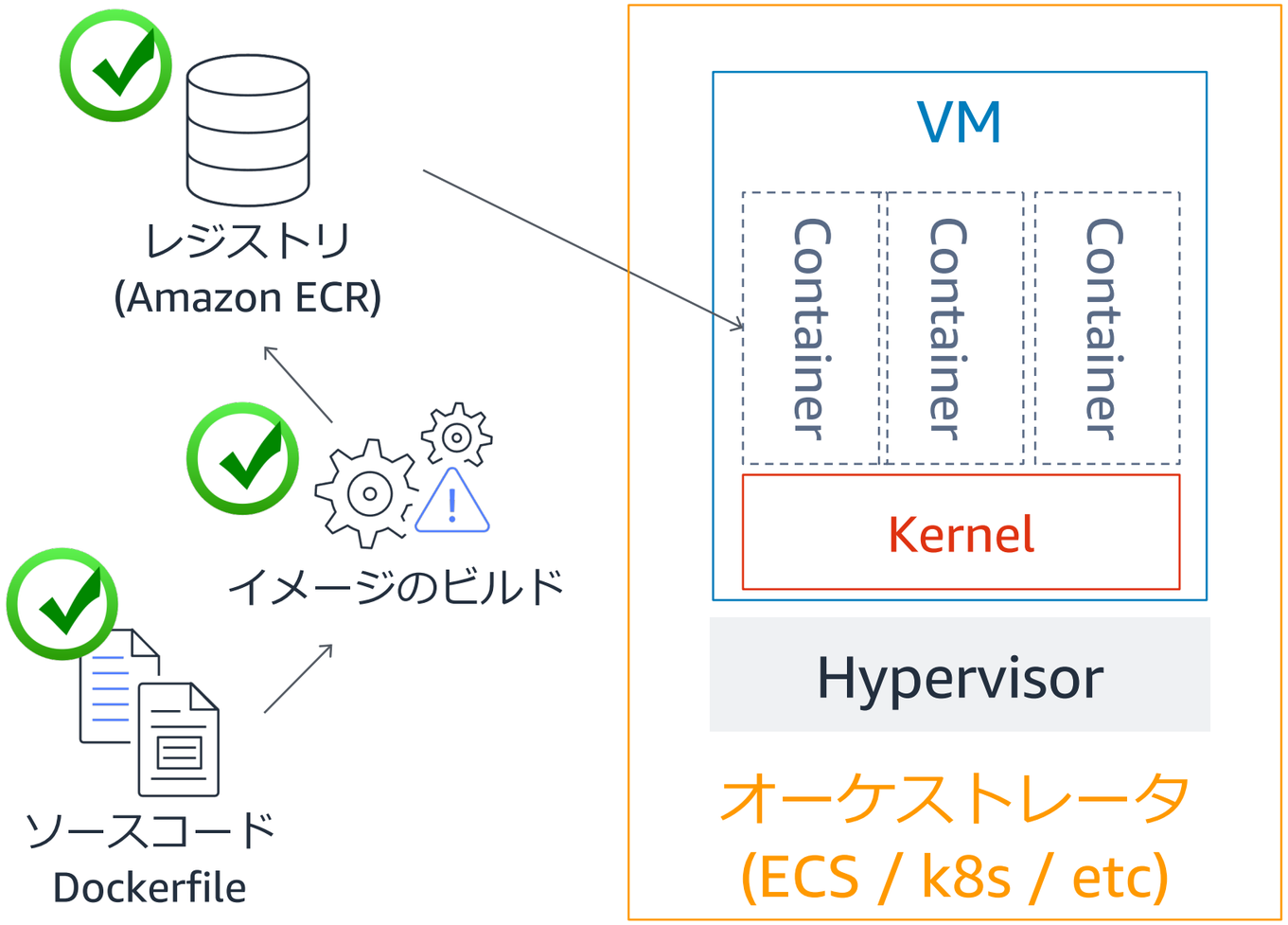
CVE-2019-5736 (runc 権限昇格 脆弱性)
悪意あるコンテナイメージの実行により侵害

コンテナ実行定義をチェックする

AWS Config による ECS タスク定義のチェック

Kyverno や Open Policy Agent で Kubernetes のマニフェストをチェック

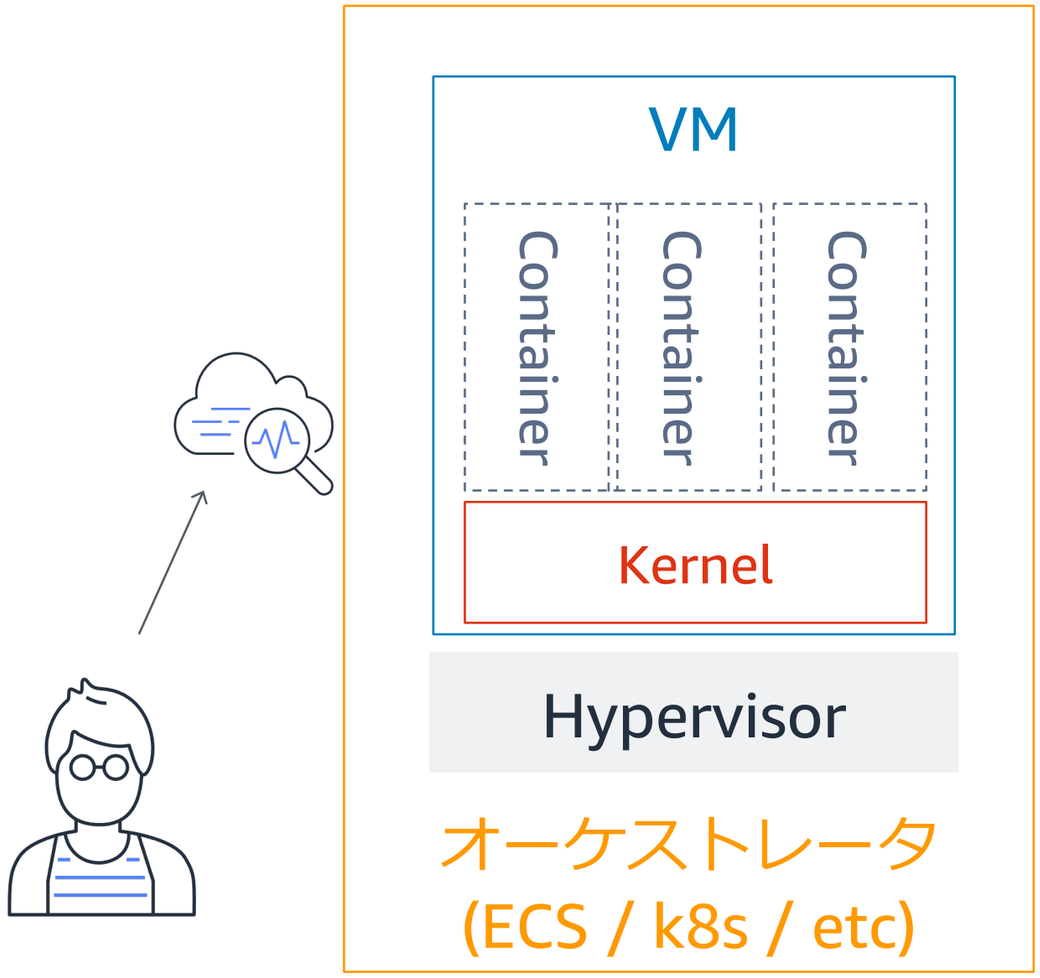
アジェンダ



- イメージの開発とビルド
- サプライチェーン
- オーケストレータの保護
- ホストのセキュリティ
- 実行時のセキュリティ

オーケストレータの保護

オーケストレータへの管理アクセスの保護



ネットワークの制限

許可したネットワークからのみアクセスする

ユーザーの管理

アクセスできるユーザーを適切に割り当てる
SSO などでユーザー管理を簡素化する

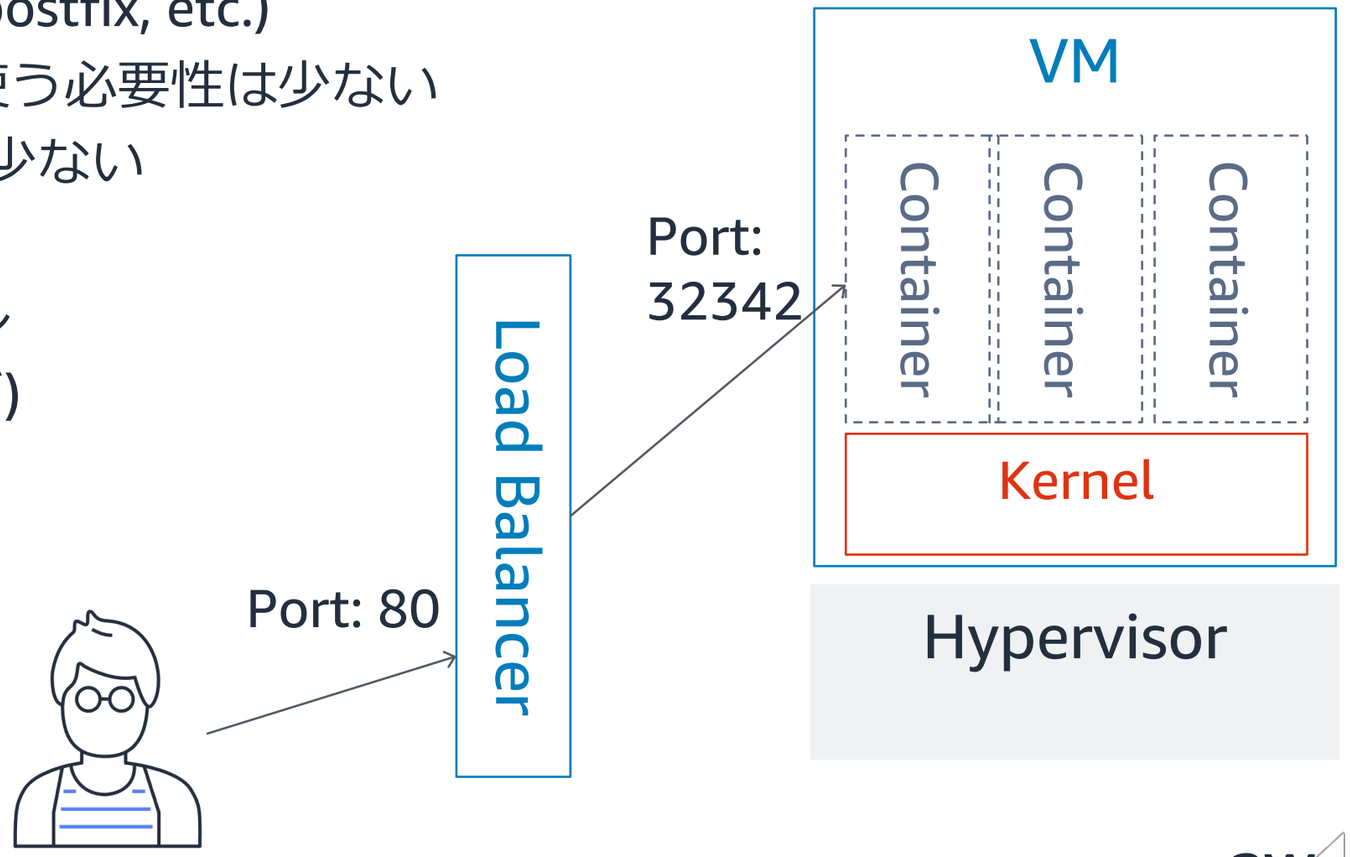
権限の管理

ユーザーに与える権限を絞る

起動するコンテナの設定: root 権限

オーケストレータがコンテナを実行する際の実行ユーザーについて

- 一般的に USER 未指定の場合はデフォルトで root 権限がコンテナプロセスの実行に利用される
- root で動くようになっているコンテナイメージは多い
  - 特権ポートを使うためなど(nginx, postfix, etc.)
  - オーケストレータで特権ポートを使う必要性は少ない
- コンテナで root は必要になるケースは少ない
  - カーネルを変更
  - 実行中にパッケージをインストール
  - ホストパスのマウント(fluentd など)



起動するコンテナの設定: Privileged、特権コンテナ

特権コンテナ ≠ root で稼働するコンテナ

- コンテナ内のプロセスは Linux Capabilities が制限
  - 脆弱性がなければコンテナから
    ホストを攻撃されることはない
- 特権コンテナ
  - 全ての Linux Capabilities が有効になっている
  - コンテナからホストに root でアクセスできる
    - ホストのデバイスをコンテナにマウントなど
- **必要な Capabilities だけを有効化する**

```
kind: Pod
spec:
  containers:
  - image: busybox
...
    securityContext:
      privileged: true
```

このセッションで扱うこと・学べること

コンテナについての一般的なセキュリティの考え方

サプライチェーン、オーケストレーターの保護

本セッションの担当: 林　政利

Specialist Solutions Architect, Containers

好きなサービス

Amazon Elastic Kubernetes Service (Amazon EKS)
AWS Certificate Manager

SIer

フリーランス
受託開発

Web系企業
サービス開発・運用

外資ベンダー
コンテナ担当SA・
サポートエンジニア

AWS Japan
コンテナ担当SA