コンテナセキュリティ100

AWS Black Belt Online Seminar

AWS Container Specialist
Principal Solution Architect
荒木靖宏

2021-Jun

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

このセッションで扱うこと

- AWSでのセキュリティの考え方
- コンテナでのサービスに至る工程
- コンテナによるサービスのために考えるべき 5 つの領域

AWS クラウドセキュリティ

AWS はクラウドコンピューティングの先駆者として、セキュリティを最優先事項としてお客様のイノベーションに迅速に対応可能な
クラウドインフラストラクチャーを創造してきました。セキュリティ機能の実装や厳格なコンプライアンス要件へ対応で
お客様は最も柔軟かつセキュアなクラウドコンピューティング環境を実現可能です

AWS コンプライアンスプログラム

コンプライアンスプログラムの例

cloud security alliance
ISO 9001 International Organization for Standardization
ISO 27001 International Organization for Standardization
ISO 27017 International Organization for Standardization
ISO 27018 International Organization for Standardization
AICPA SOC
PCI Security Standards Council PARTICIPATING ORGANIZATION
TISAX ENX ASSOCIATION
FedRAMP
FIPS 140-2 FIPS CRYPTOGRAPHY

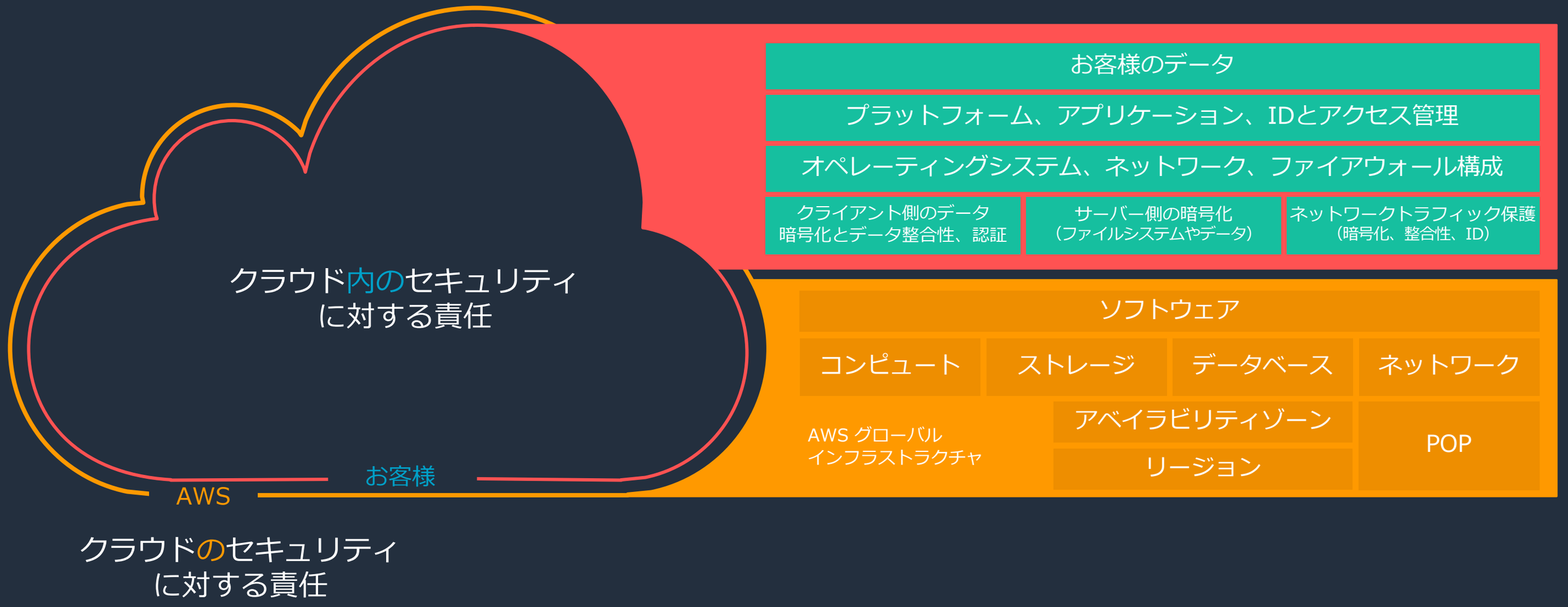
AWS コンプライアンスプログラム
https://aws.amazon.com/jp/compliance/programs/

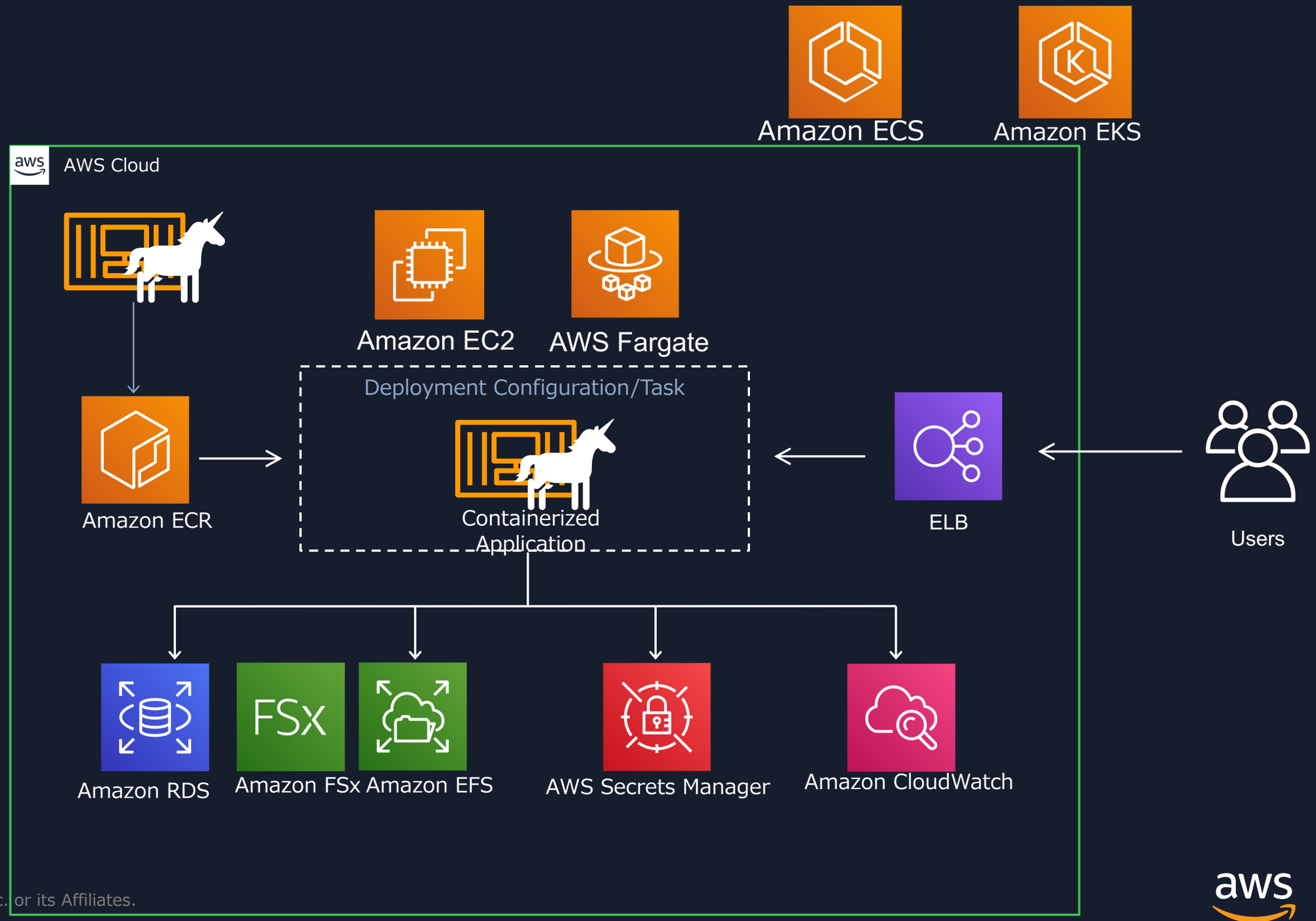
クラウドセキュリティのためのサービス

- アイデンティティ & アクセス管理
- 脅威の検出と継続的なモニタリング
- インフラストラクチャとデータの保護
- インシデントへの対応
- コンプライアンス

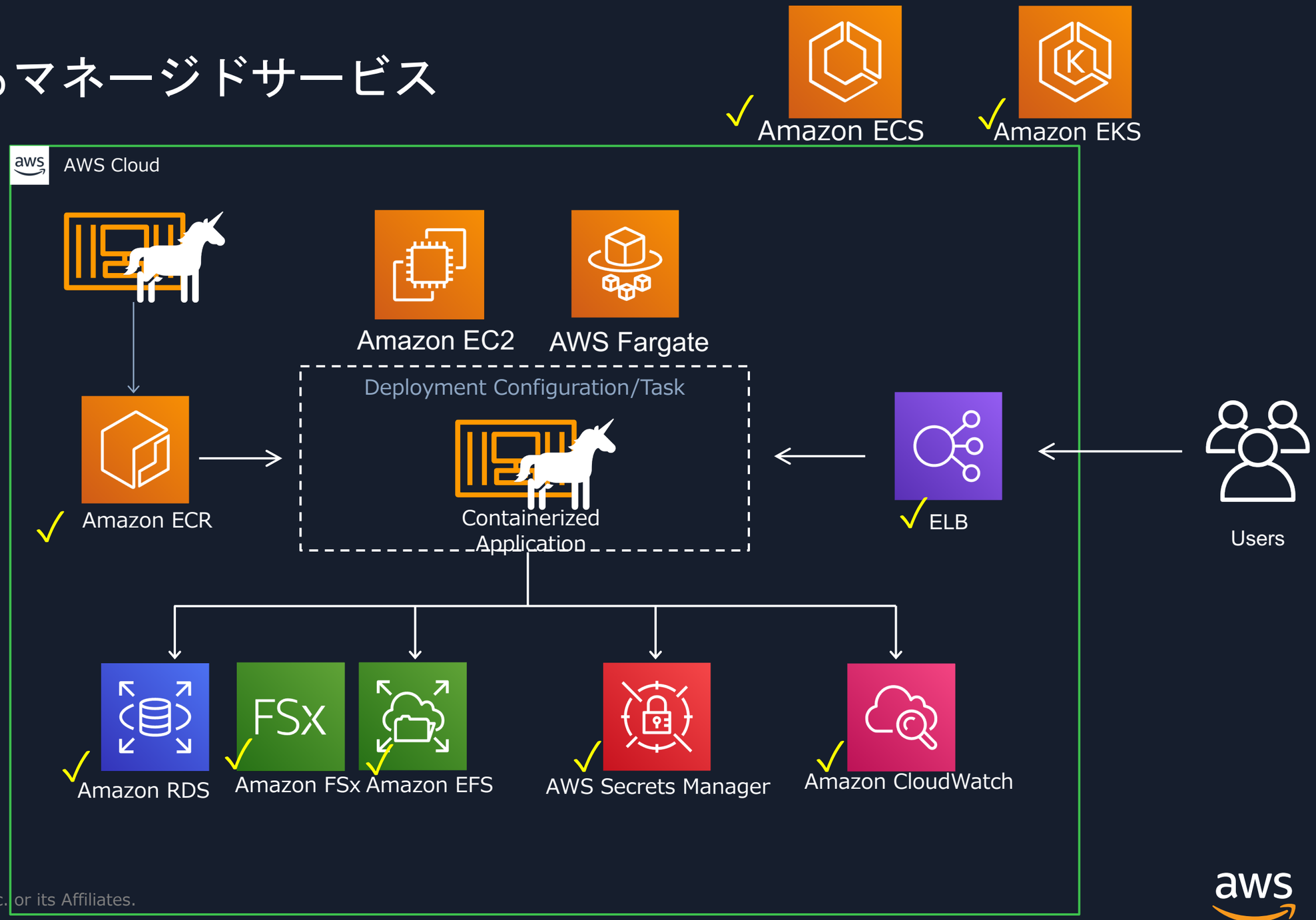
aws

AWS における責任共有モデル

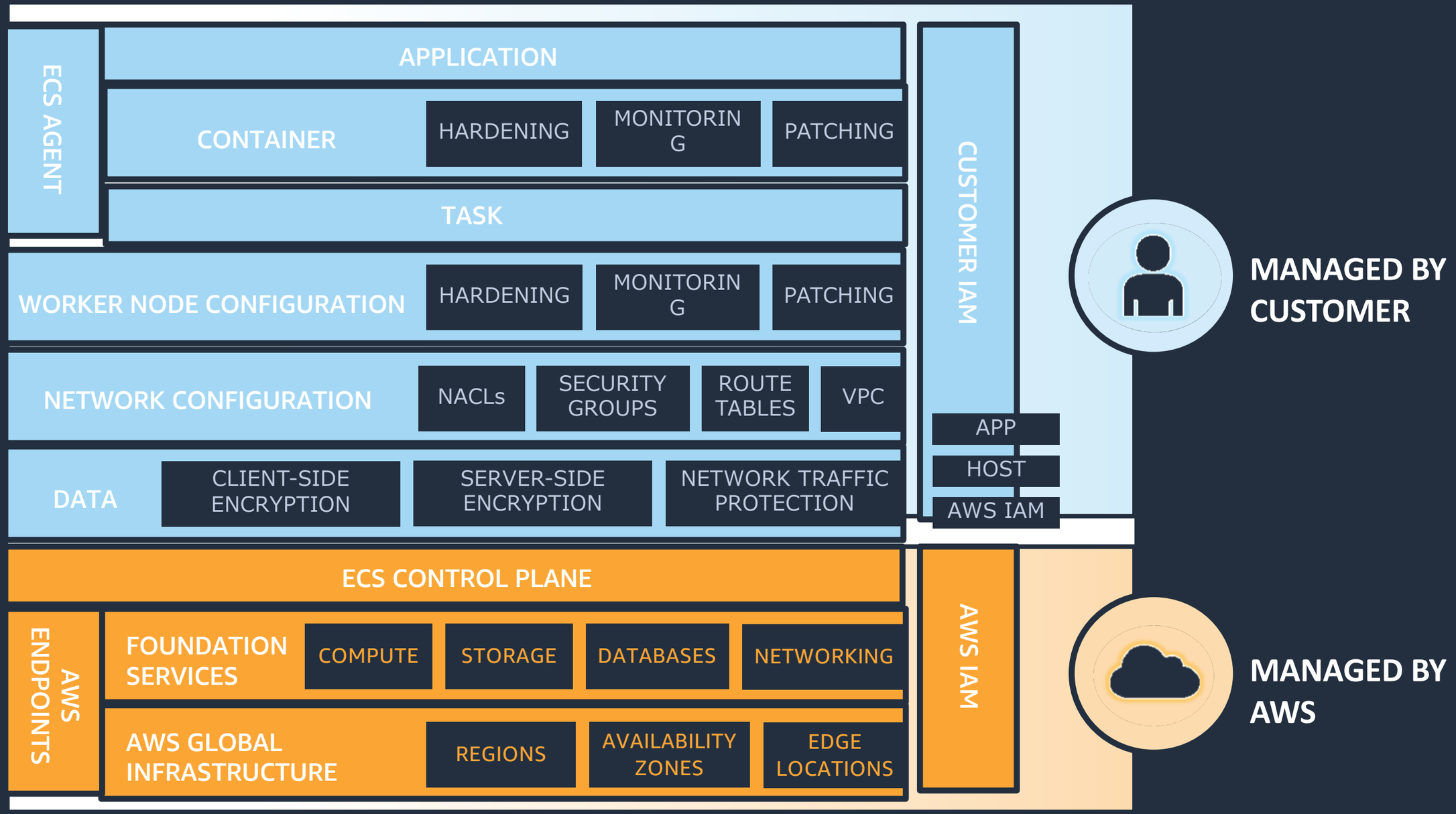




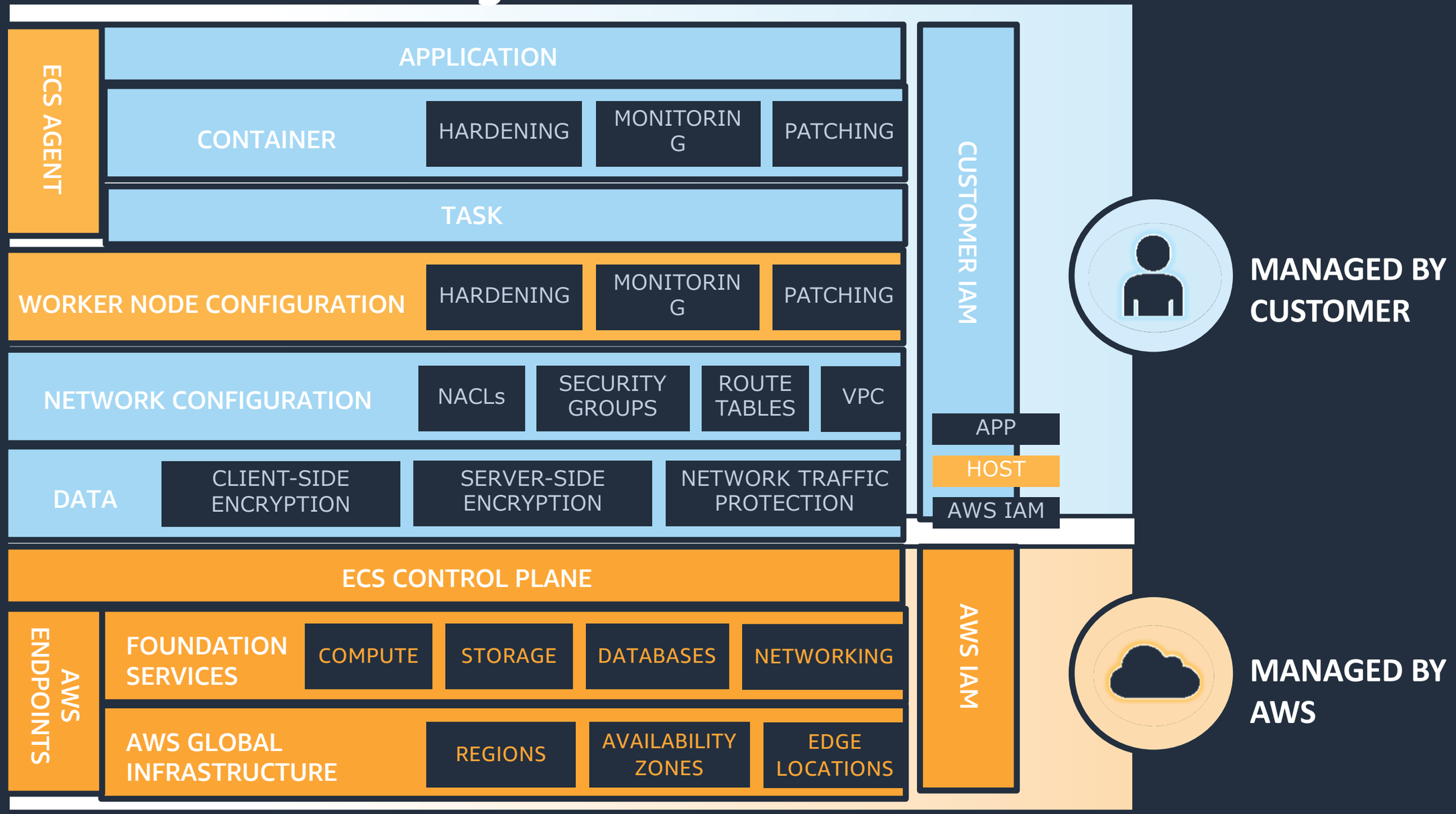
✓ AWSによるマネージドサービス



Amazon ECS on EC2

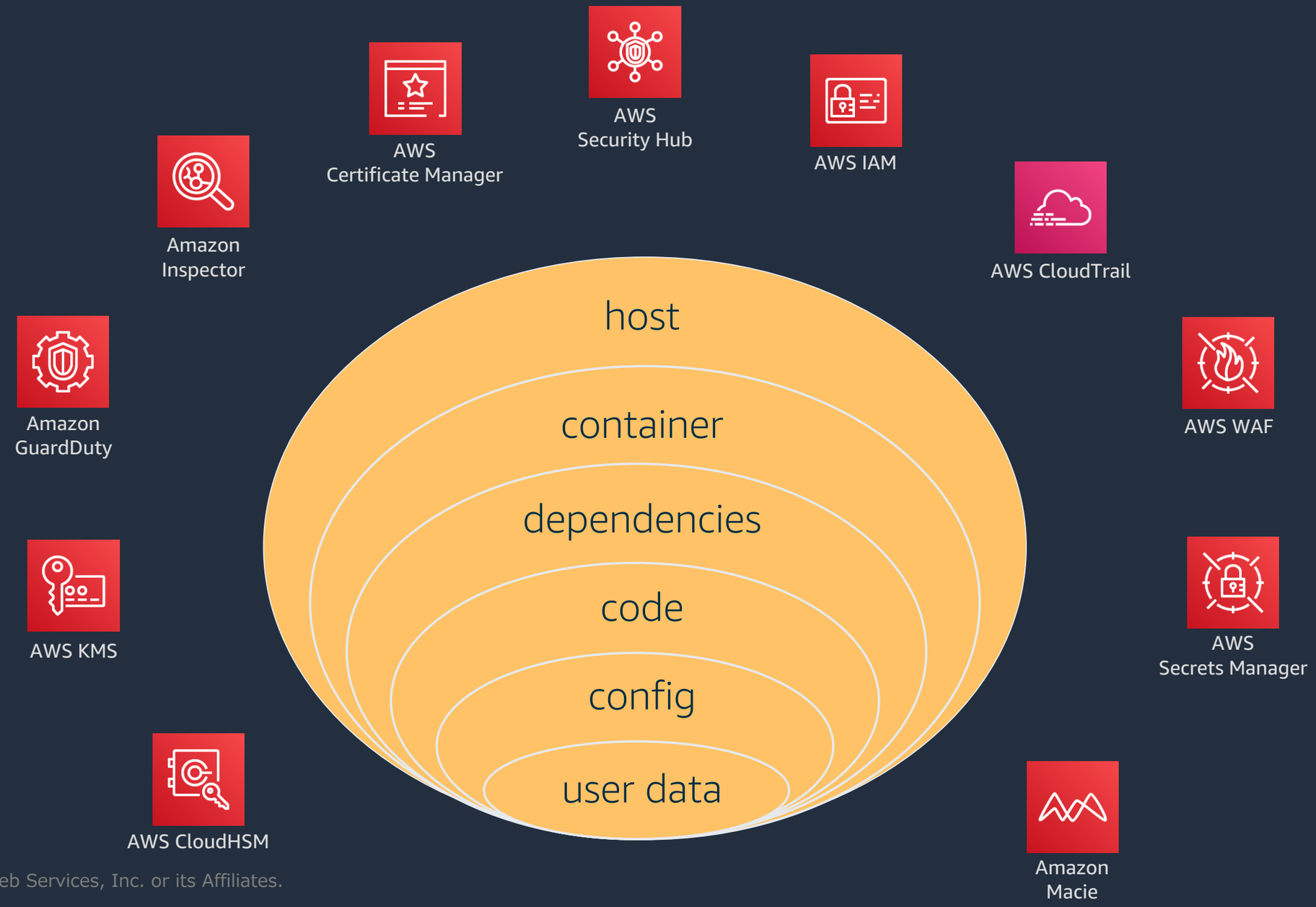


Amazon ECS on Fargate



aws

AWSにおけるセキュリティ関連サービス



コンテナのセキュリティのために

Identity and Access Management

コンテナホストとコンテナへのユーザー権限を制限

ネットワーク

ネットワークセグメンテーションによるアクセス制限
転送データの暗号化

ログ・モニタリング

コンテナ、ホスト、およびネットワークレイヤーでイベントログを実装

コンテナ・コンテナイメージ

コンテナホストとコンテナイメージを強化

機密情報の管理

シークレットプロバイダの利用

aws

コンテナのセキュリティのために：今後詳細を取り扱います

Identity and Access Management

- 共通: ユーザーに付与する AWS リソースへのアクセス権限を最小に
- 共通: アプリケーションに付与する権限は IAM ロールで管理
    - ECS: タスク用の IAM ロールを使用
    - EKS: IAM roles for service accounts (IRSA) を使用
- 共通: インスタンスメタデータへのアクセスを制限
- 共通: IAM Access Advisor を利用して権限を整理する

ネットワーク

- 共通: コンテナ実行環境をプライベートサブネットに配置
- ECS: ネットワークモードで awsvpc を利用する
- EKS: Pod のセキュリティグループを利用する
- EKS: EKS クラスターエンドポイントをプライベートに設定する
- 共通: 必要に応じてプライベートなクラスターを構築する

ログ・モニタリング

- 共通: CloudTrail を利用したモニタリング
- EKS: コントロールプレーンのログを有効にする
- 共通: VPC フローログの解析

コンテナ・コンテナイメージ

- 共通: コンテナイメージの定期的な静的スキャンを行う
- 共通: 特権コンテナの実行を避ける
    - ECS: 特権コンテナを含むタスクの実行を制限する
    - EKS: 特権コンテナを含む Pod の実行を制限する

機密情報の管理

- ECS: コンテナへの機密情報の配布に AWS Secrets Manager または AWS Systems Manager Parameter Store を利用する
- EKS: コンテナへの機密情報の配布に外部のシークレットプロバイダーを利用する

aws

このセッションで扱ったこと

- AWSでのセキュリティの考え方
  クラウド内のセキュリティに対する責任が利用者にある

- コンテナでのサービスに至る工程
  ECSやEKSといったサービスの周辺、AWSで広く使えるセキュリティ関連サービスの存在

- コンテナによるサービスのために考えるべき 5 つの領域
  IAM, ネットワーク、ログ・モニタリング、コンテナ・コンテナイメージ、機密情報の管理

本セッションの担当：荒木靖宏

AWSコンテナスペシャリスト
　プリンシパルソリューションアーキテクト

2011年からAWSのソリューションアーキテクトです

好きなサービスはAWS DirectConnectとEC2 Spot

AWS Black Belt Online Seminar とは

「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分け、アマゾン ウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです。

- AWSの技術担当者が、AWSの各サービスについてテーマごとに動画を公開します
- お好きな時間、お好きな場所でご受講いただけるオンデマンド形式です
- 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます

内容についての注意点

- 本資料では2021年6月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には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.

本資料に関するお問い合わせ・ご感想

- 技術的な内容に関しましては、有料のAWSサポート窓口へお問い合わせください
- https://aws.amazon.com/jp/premiumsupport/

- 料金面でのお問い合わせに関しましては、カスタマーサポート窓口へお問い合わせください（マネジメントコンソールへのログインが必要です）
- https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service

- 具体的な案件に対する構成相談は、後述する個別技術相談会をご活用ください

ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt

AWS の日本語資料の場所「AWS 資料」で検索

https://amzn.to/JPArchive

AWS のハンズオン資料の場所「AWS ハンズオン」で検索

https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/

AWS Well-Architected 個別技術相談会

毎週”W-A個別技術相談会”を実施中

- **AWSのソリューションアーキテクト(SA)に対策などを相談することも可能**
- **申込みはイベント告知サイトから**

(https://aws.amazon.com/jp/about-aws/events/)

AWS イベント で[検索]

ご視聴ありがとうございました

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive