W-A レビューワークショップ - **課題**

目次

1. 背景

目黒生命株式会社は、日本全国に拠点を持つ中規模の生命保険会社です。現在、目黒生命では、顧客体験の向上を目的に、保険契約を締結した顧客が契約内容の確認や給付金請求をはじめとした各種請求、顧客情報の変更手続きを Web 上で行えるよう、Web アプリケーションを開発しています。

このアプリケーションは目黒生命の開発環境(AWS 環境)にて、開発が進められてきました。開発当初、利用するクラウドプラットフォームが確定していなかったことから、どのような環境でも動作するよう、アプリケーションはコンテナ上で動作するように作られています。アプリケーションの基本機能の開発が一通り完了し、社内開発環境で一定のシステム品質が確保できたことから、本番環境の設計及び構築を計画しています。開発環境では、アプリケーションの基本機能を開発することに重点を置いていたため、本番環境で考慮すべきセキュリティの仕組みに対する検討、考慮が不足しています。

あなたは、AWS のプロフェッショナルとして、目黒生命社が設計した AWS による設計書をセキュリティの観点でレビューし、AS-IS(現状)を分析し、TO-BE(将来像)を検討してください。

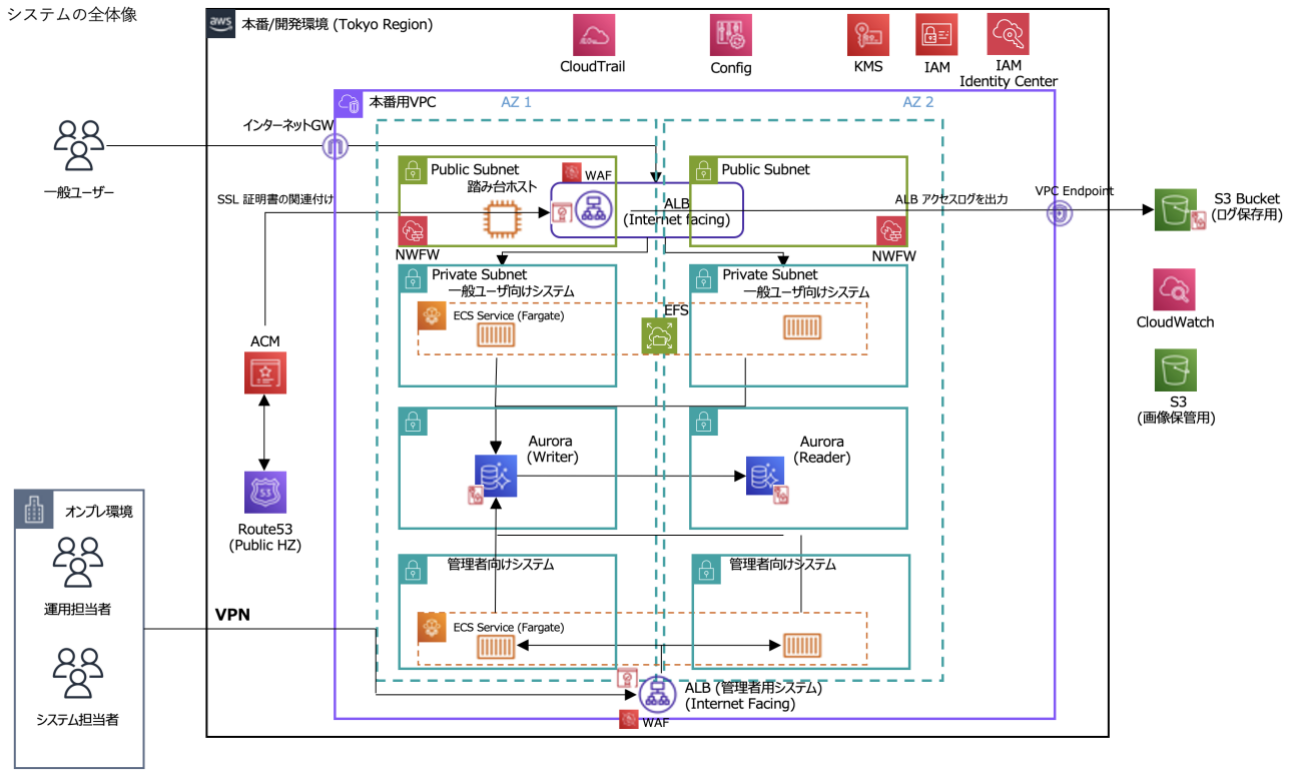
※なお、現状確認できている情報のみを掲載しています。レビューを実施する上で、情報不足により AS-IS(現状)の判断ができないポイントがあれば、その項目は W-A を満たしていないものとして判断し、TO-BE(将来像)を検討してください。

2. システム設計

2.1 システム全体構成

本アプリケーションのインフラ構成を以下に記載する。

図 1 インフラ構成図



「**一般ユーザ**」: 日本全国に利用ユーザが存在する。一般ユーザの登録/ログインはコンテナ上に構築された一般ユーザ向けシステムの認証機能により実現する。Application Load Balancer(ALB)を経由し、顧客向けの Web サーバへ接続する。契約内容や契約者情報はデータベース上に格納する。Web サイトで用いる静的ファイル(画像等)は Amazon S3 バケットに保管されている。

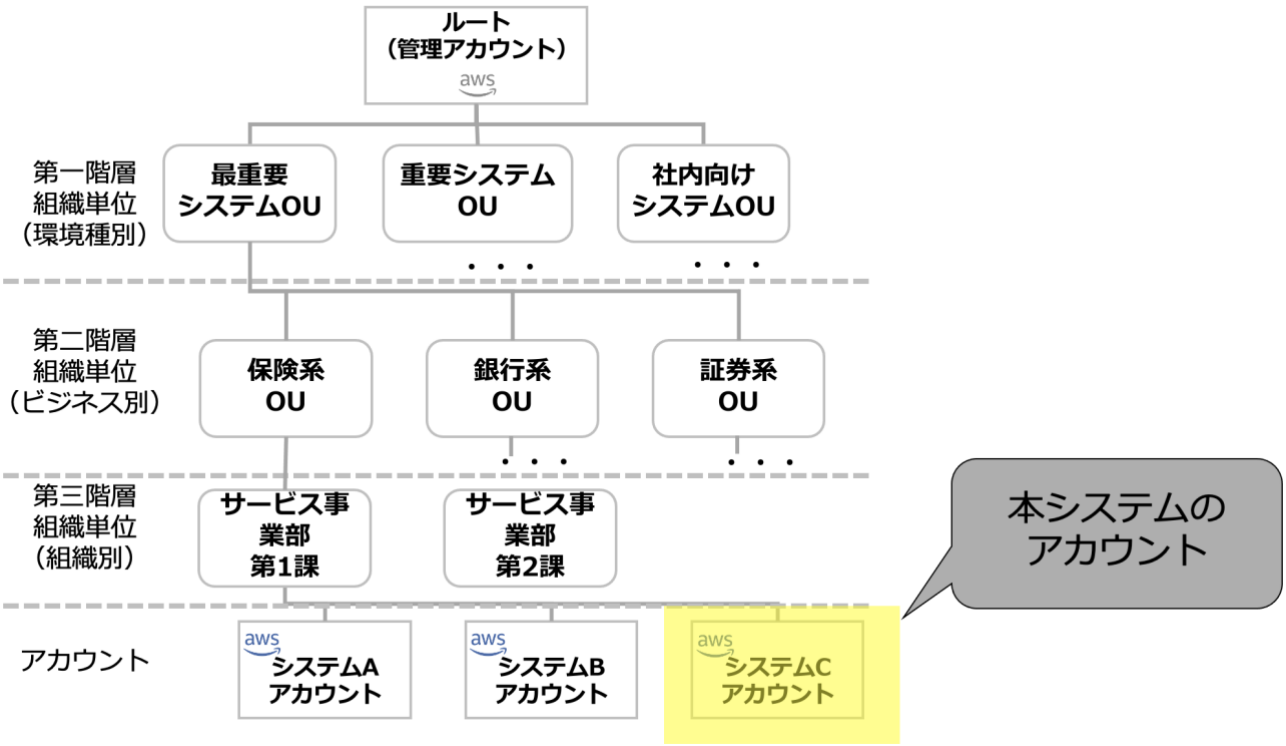
「**システム担当者**」: 目黒生命社の本システム全体を管轄する部署の担当者である。本システムに対するシステム開発、機能拡張、トラブル発生時の対応を実施する。拠点は目黒生命社の東京オフィスに存在する。システム担当者は、ALB 経由で、システム担当者用の特権ユーザで管理者用システムにログインし、管理者モードでシステムを操作することが出来る。DB に対する設定確認/変更が必要な場合には、パブリックサブネットに配置された踏み台インスタンスを経由して、操作を実施する。

「**運用担当者**」: 本サービスの運用を担当する。拠点は目黒生命社の東京オフィスに存在する。運用タスクとして事前に定義された操作のみを実施する。

2.2 組織/アカウント構成

- 目黒生命社は、多種多様な業界、顧客に対してシステム設計、構築、運用の支援を行う。近年、自社で管理する AWS アカウント数が 30 を超え始めており、各アカウントの位置付けを整理できるよう AWS Organizations を利用する。なお、Organizations の管理は「**情報システム部担当者**」が実施する。情報システム部担当者はアカウントの払い出しと、払い出されたアカウントに対する OU への参加処理を必ず実施し、その後に必要な操作については、各システムの担当者に一任される。目黒生命における Organizations 構成は図 2 を参照。

図 2 Organizations 組織構成



「第一階層」：システム重要度を区分できるよう、OU を分離。

「第二階層」：ビジネス業界を区別できるよう、OU を分離。

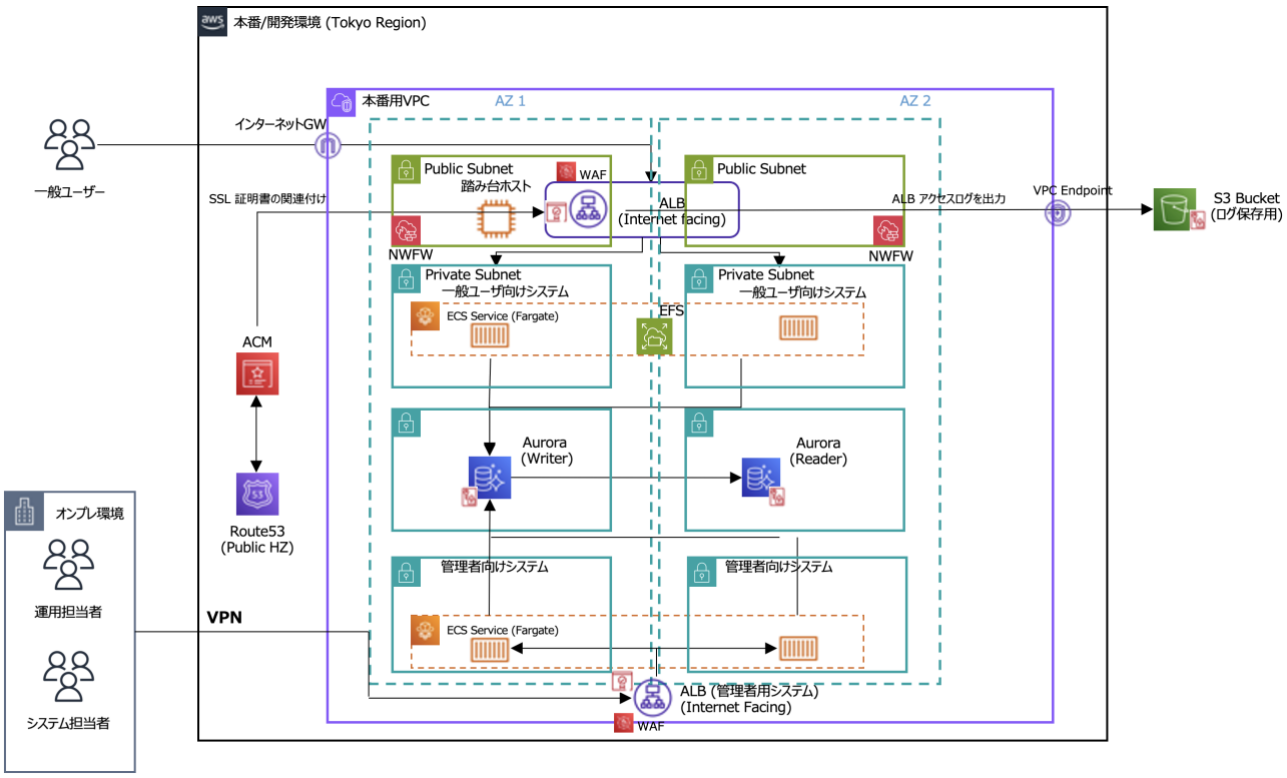
「第三階層」：組織単位を識別できるよう、OU を分離。

- 本システムは上記記載の「システム C アカウント」に構成される環境となる。なお、本システムの開発環境はシステム C アカウント内に存在する別 VPC に構築済みである。
- Organizations はアカウントの役割と位置付けを明確化するために使用しているため、SCP による

制御は特段かけていない。

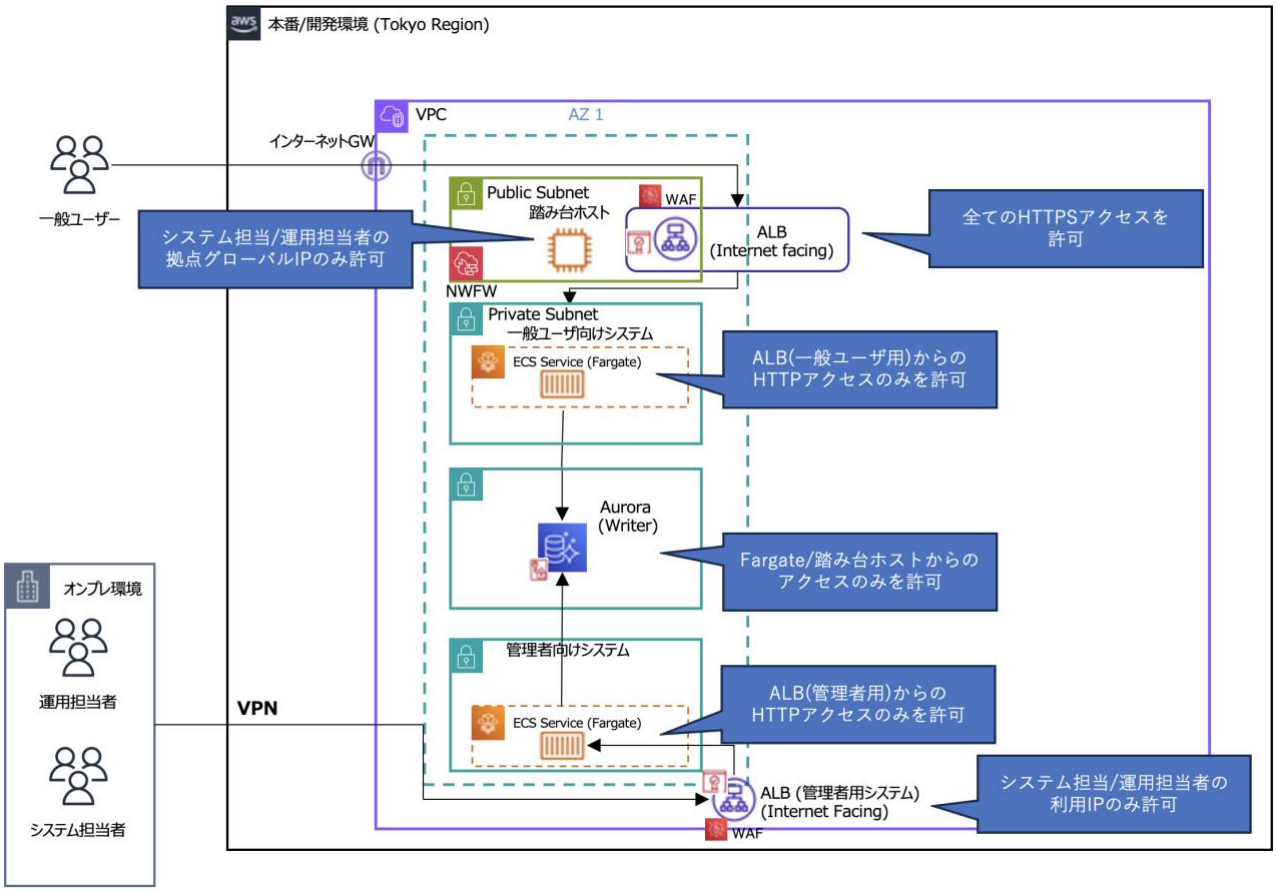
2.3 ネットワーク構成

図 3 ネットワーク構成図



- 本システムの AWS アカウント上には、本番/開発環境ごとに Amazon VPC が作成され、VPC 内では AZ が冗長化され、パブリックサブネットとプライベートサブネットを配置する。なお、コンテナで構築される Web 層と、DB 層のサブネットは分離する。パブリックサブネットにはインターネット経由でアクセスが可能な ALB と踏み台インスタンス(Windows サーバ)を配置する。
- コンピュート及び DB サービスには図 4 の方針(紙面の都合上、1AZ のみ記載)でセキュリティグループを適用する。なお、NW ACL はステートレスな定義が必要となるため、管理負荷軽減を目的に使用しない。

図 4 セキュリティグループの方針



- Fargate は NAT GW を用いたインターネットへの疎通が可能。
- ALB には HTTPS 経由で接続し、踏み台インスタンスにはリモートデスクトップ(RDP)経由で接続する。RDP の認証情報はシステム担当者が厳重に管理する。管理目的で DB にアクセスする際には、踏み台インスタンス上に保管された DB の認証情報を用いて接続する。
- VPC エンドポイントが提供されるサービスについては、原則 VPC エンドポイントを使用する。
- オフィスと AWS 環境間は IPsec VPN を用いて接続されている。

2.3 セキュリティ

- 以下のセキュリティサービスを Organizations 配下のアカウントについては有効化する。

サービス	用途
AWS CloudTrail	AWSサービスに対するAPI実行/操作履歴を記録する
AWS Security Hub	AWS Security Hub の AWS Foundational Security Best Practice(FSBP)標準で提供されているコンプライアンス基準をベースとして設定する
AWS Config	AWS上のリソースの構成情報を取得し、変更情報のトラッキングを実施する

- インフラストラクチャ保護の目的で、以下のサービスを有効化する。

サービス	用途
AWS WAF	ALBに付与し、主にL7レイヤーの攻撃の検査、保護を行う
AWS Shield Standard	主にDDoS攻撃の対策、保護を行う
AWS Network Firewall	VPCからのアウトバウンド通信を制御する

- セキュリティ監査は年に 1 回の頻度で実施する。この監査において、AWS IAM Identity Center (IIC) の認証情報でユーザに対して過度な権限を与えているものがないかどうか、チェックし、不要なものは削除する。また、IAM Access Analyzer を用いて外部からの意図せぬアクセスが可能となっていないかどうかチェックする。
- 情報システム部のセキュリティ担当者が以下を実施し、セキュリティリスクがある項目についてはシステム担当者に対して予防/対策方法を連携する。
  - CVE など、公開されている脆弱性情報の定期的な確認
  - AWS セキュリティ速報で発表されているセキュリティに関する最新情報の取得と全社で利用可能な AWS サービスの定義
  - 脅威モデリングの実施
  - 新しいセキュリティサービスの機能の確認と定期的な評価
  - アプリケーションのセキュアな開発手法のトレーニング開催

2.4 認証/認可

- システム担当者、及び、運用担当者が利用する認証情報は AWS IAM Identity Center(以下、IIC)で管理する。IIC における認証時には、MFA を有効化する。ユーザへ追加権限を与える場合はシステム管理者に申請の上で、定められた手順に沿って実施する。
- IIC では、役割ごとにグループを分け、それぞれのグループに対して許可セットを付与する。グループに所属するユーザは、メンバー毎に払い出す。グループと許可セットの紐付は以下の通り。

グループ	許可セット
システム担当者	Administrator
運用担当者	SystemAdministrator SupportUser Billing

- ルートユーザの認証情報は厳密に管理され、システム担当者以外のメンバーがルートアカウントへのログインが出来ないように管理する。ルートユーザにログインする際には MFA を有効化する。ルートユーザの連絡先はシステム担当者チームのメールアドレスを設定している。
- コンテナや EC2 など、AWS リソースに付与するアクセス権限については IAM ロールで制御する。将来的に、今後提供される様々なサービスと連携が必要となる可能性が想定されるため、Fargate および EC2 インスタンスには他 AWS サービスに対する API 実行を可能とする権限を幅広く付与する。なお、サードパーティのサービスに対して連携を行う場合には IAM 信頼ポリシーと外部 ID を用いたセキュアな連携を実現する。
- アプリケーションから DB にアクセスするため、コード上に DB の認証情報を記載する。

2.5 データ保護

- ALB には TLS1.2 を用いた HTTPS で接続が可能。
- 証明書管理には ACM を使用し、ドメイン検証(DV)証明書を利用する。
- データベース、Amazon EFS など、データが保管されるサービスに対しては、AWS KMS による暗号化を実施する。デフォルトで暗号化を有効化できるものはデフォルト有効化する。各データに対する暗号化および重要度の詳細は以下に記載する。

保護対象データ	格納先	暗号化 (サーバーサイド)	重要度	保持期間
DBデータ (機密)	Auroraストレージ	KMS※2	高	ユーザ登録が 削除されるまで
アプリケーション関連 ファイル (機密)	EFS	KMS※2	高	ユーザ登録が 削除されるまで
S3格納データ(画像)	S3※1	SSE-S3	高	サービス提供中は永久 保持
監査ログ	CloudWatch Logs S3※1	KMS※2 SSE-S3	中	5年
システムログ	CloudWatch Logs	KMS※2	低	3年

※1：バケットポリシーを用いて、アクセス制御を実施する。また、S3 アクセスログを有効化する。

※2：KMS キーはアカウントに一つ KMS カスタムキーを払い出し、それを使用する。

2.6 監視

- Amazon CloudWatch ダッシュボードを作成し、本システムで取得され、監視が必要なメトリクスについてはダッシュボードで一元管理する。
- セキュリティ系サービス(Config)の情報は Security Hub に統合し、一元管理する。

- セキュリティ系サービスで検知された情報はシステム管理者及び運用者に通知する。

2.7 ログ

- 本システムで利用する AWS サービスに対して、以下のログを取得する。

大分類	分類	ログ	保管期限※2	保管場所※3
監査ログ	AWSサービス	CloudTrailログ※1	5年	S3
		Configログ(設定履歴、設定スナップショット)	5年	S3
		VPCフローログ	5年	S3
		S3アクセスログ/データイベントログ	5年	S3
		ELBアクセスログ	5年	S3
		WAF ログ	5年	S3
		Network Firewall ログ	5年	S3
	環境固有のログ	OS監査ログ(ログイン)	5年	CloudWatch Logs
		DB監査ログ	5年	CloudWatch Logs
システムログ	環境固有のログ	OSログ	3年	CloudWatch Logs
		APログ	3年	CloudWatch Logs
		DBログ	3年	CloudWatch Logs

※1：CloudTrail 整合性検証機能を有効化する。

※2：S3 ライフサイクルポリシー及び CloudWatch Logs の保管期限を設定することで保持期間を過ぎたログファイルは自動削除する。

※3：S3 バケットポリシー、IIC の認可ポリシーによりアクセス権を制御する。

- 取得されたログは CloudWatch Logs 標準の検索機能及び、Athena によるログ検索を用いた分析が行える状態とする。

2.8 運用

運用担当当者は、以下の運用タスクを実施する。

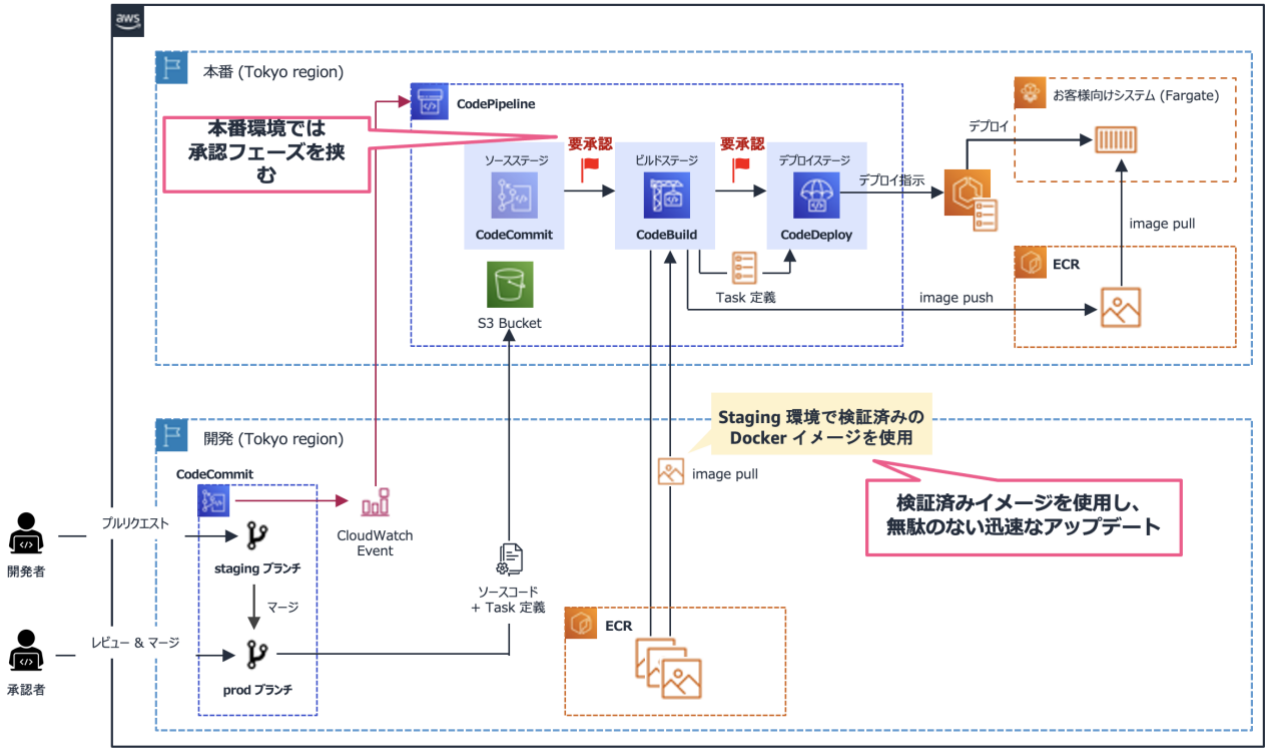
- AWS Trusted Advisor を活用し、赤色のアラートが発砲されているもの(不要なアクセス許可等)に対して、対処を実行する。
- 作成された AMI のソフトウェアが最新版にアップデートされるよう、管理する。
- 社員の退職・異動に伴い、IIC からユーザ情報を削除する。
- セキュリティインシデント発生時への備えとして以下を実施する。
  - IIC の障害発生時にはシステム担当者と連携の上で、ルートユーザを用いて Administrator 権限を持つ IAM ユーザを作成する。なお、問題解消後に緊急用の IAM ユーザを削除する。
  - セキュリティインシデント発生時に連携をとるべき担当者リストとパートナーを定義する。
  - 想定されるインシデントを挙げ、ビジネス分類ごとに整理している。また各インシデントについて発生時の対応計画を定める。
  - インシデント発生時の情報を外部へリリースする際の広報計画を定める。

- インシデント対応のトレーニングを受講する。

2.9 アプリケーション開発/デプロイ

- インフラ構築/運用は管理メンバーのスキルレベルに合わせ、マネジメントコンソール経由で実施する。AWS CloudFormation をはじめとした IaC(Infrastructure as Code)は利用しない。
- コンテナアプリのデバッグが必要な場合は、ECS Exec を使用する。
- ソフトウェア開発では、以下に留意の上で開発を行なう。
  - セキュリティ部門によって規定されたバージョンを利用する。
  - アプリケーション開発段階で不要なパッケージ(ライブラリ、コンポーネント、ユーティリティ等)をインターネット経由で組み込まないよう、考慮されている。情報システム部がベースとなるテスト済みのソフトウェアパッケージを一元化しているため、これを使用する。
  - コードを記述した以外の開発者が手動でコードレビューを行う。
  - セキュリティ部門の担当者がアプリケーションのセキュアな開発方法に関するトレーニングを実施し、プロジェクト参画前に開発者が受講する。その内容に沿って開発を実施する。開発チームがセキュアな開発手法に関してセキュリティチームからのフィードバックをもらう仕組みがある。
- 本番環境におけるコンテナ上のアプリケーションデプロイについては、CI/CD パイプラインを用いて実装する。CI/CD パイプラインの実装イメージは図 5 を参照。

図 5 CI/CD パイプラインの構成



- ✧ CI/CD パイプラインに対するセキュリティレビューはシステム担当者によって実施される。
- ✧ CI/CD パイプラインに対するアクセス制御は IAM ロールを用いて必要最小限の権限を付与する。