

1.AWS構築設計書

AWS構築設計書

案件名：中小企業向けコーポレートサイトAWS移行プロジェクト

作成者：ふうま

作成日：2025/11/22

バージョン：v1.0

1. プロジェクト概要

項目	内容
目的	オンプレ環境からAWSへ移行し、可用性と保守性を向上させる。
背景	現在のオンプレ環境では、老朽化やアクセス不安定、バックアップ運用の課題が発生。AWSを利用して高可用・低コスト化を図る。
スコープ	Web/DB構築、データ移行、監視設定、バックアップ設計
利用者想定	一般公開向けWebサイト（企業顧客・取引先）
目標コスト	月額20,000～25,000円

2. 要件定義

機能要件

- Web公開（HTTPS対応 / ALB経由）
- データベース（RDS MySQL）
- ファイル保管（S3）
- 監視（CloudWatch）
- ログ管理（CloudWatch Logs収集）

非機能要件

- 可用性：AZ冗長構成（Web/DB）
- コスト：月25,000円以内
- 拡張性：将来CI/CD導入可能
- セキュリティ：IAM最小権限・SG分離・TLS通信

3. クライアント確認事項（想定）

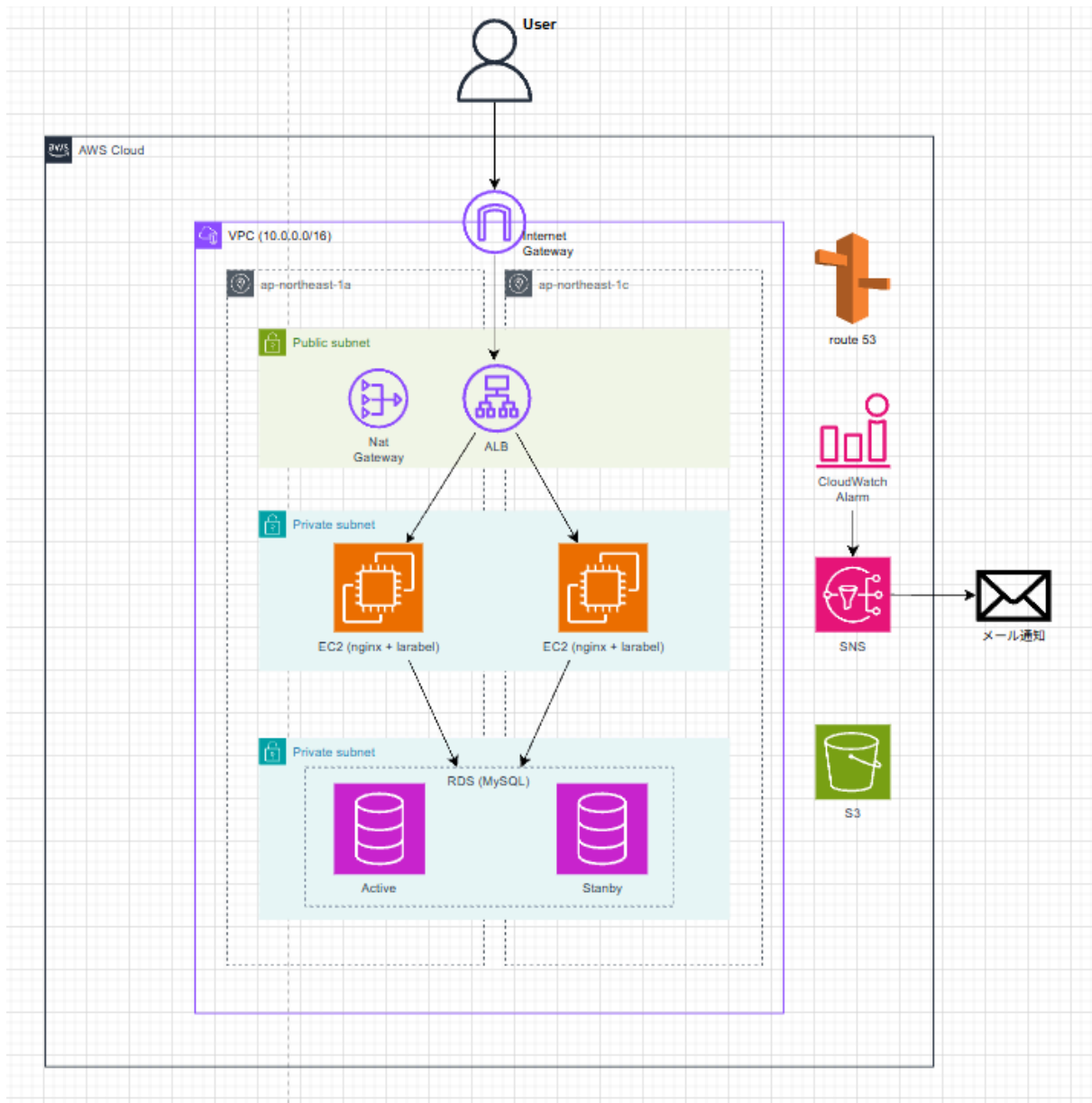
No	質問内容	回答方針
1	S3のバージョニング／ライフサイクル設定要否	バージョニングON・90日後にIA移行を提案
2	RDSスナップショットを任意取得するか	自動バックアップ＋手動スナップ提案
3	OS・ミドルウェアのパッチ適用運用	手動更新、SSM Patch Manager導入を提案
4	CloudWatchでのログ収集範囲	メトリクス＋Nginx/Laravelログを収集
5	NAT Gateway冗長化の要否	コスト重視で単一構成、HAは提案扱い
6	CI/CD導入計画	将来的にCodePipeline導入を検討

4. システム構成

アーキテクチャ概要

- VPC（10.10.0.0/16）
- Public Subnet：ALB, NATGW
- Private Subnet：EC2（Web/AP）
- Private DB Subnet：RDS（MySQL）
- S3, Route53, CloudWatch

構成図



5. ネットワーク設計

要素	内容
VPC	10.10.0.0/16
Subnet	Public(10.10.0.0/24, 10.10.1.0/24), Private-App(10.10.10.0/24, 10.10.11.0/24), Private-DB(10.10.20.0/24, 10.10.21.0/24)
AZ構成	ap-northeast-1a / 1c
IGW / NATGW	IGW:1, NATGW:1台 (1a)
DNS	Route53 Public Hosted Zone
SSL証明書	ACM: *.example.com

6. サービス構成

層	サービス	設定内容
Web/AP	EC2 (Amazon Linux 2023)	Nginx + PHP (Laravel)
DB	RDS (MySQL)	マルチAZ・自動バックアップ7日
ストレージ	S3	静的ファイル・バックアップ保存、バージョニングON
ロードバランサ	ALB	HTTP→HTTPSリダイレクト、ACM適用
監視	CloudWatch	メトリクス・ログ・SNS通知
セキュリティ	IAM / SG	最小権限設計・SG分離管理

7. セキュリティ設計

IAM設計

種別	名称	権限
管理者	*****	AdministratorAccess (MFA必須)
閲覧専用	viewer-ops	ReadOnlyAccess
ロール	EC2InstanceRole-Web	S3ReadOnly, CloudWatchAgentServerPolicy

Security Group設計

SG名	用途	Inbound	Outbound
ALB-SG	外部公開	80/443 (0.0.0.0/0)	全許可
Web-SG	Webサーバ	80 from ALB-SG / 22 from 管理端末IP	3306 to DB-SG
DB-SG	RDS	3306 from Web-SG	デフォルト許可

8. バックアップ・運用設計

項目	設定内容
RDSバックアップ	自動7日＋手動スナップ提案
S3バックアップ	バージョニングON、90日後IAへ移行

項目	設定内容
ログ管理	CloudWatch Logs + S3転送
監視通知	CloudWatch Alarm → SNSメール
パッチ適用	手動更新（将来SSM導入予定）

9. コスト試算

サービス	構成	想定月額
EC2	t3.small ×2	39.17 USD
RDS	db.t3.micro	43.48 USD
S3	50GB	1.25 USD
NATGW	1台	45.26 USD
Route53	1 Hosted Zone	0.8 USD
CloudWatch	メトリクス+ログ	1.5 USD
合計		約150USD/月（=約23,000円）

10. 構築手順概要

- 1 VPC・サブネット・ルートテーブル作成
- 2 EC2構築（Nginx+PHP）
- 3 RDS構築・接続確認
- 4 S3作成・アップロード確認
- 5 ALB設定（ターゲット登録）
- 6 Route53 + ACM設定
- 7 CloudWatch監視・SNS通知確認

 詳細は「構築手順書」ページで管理。

https://www.notion.so/AWS-2b042340756080049fe3f5bcd8e833e2?source=copy_link

11. テスト結果

テスト項目	結果	備考
Webアクセス（HTTPS）	✔ OK	ALB経由で接続成功
RDS接続確認	✔ OK	Laravelから接続OK
CloudWatch監視	✔ OK	CPUアラート発報確認
S3バックアップ	✔ OK	ファイル保存・取得成功

12. 改善提案

分野	提案内容
冗長化	NATGWのマルチAZ化
運用	Patch Manager導入
自動化	TerraformによるIaC化
デプロイ	CodePipeline導入（CI/CD）
セキュリティ	AWS WAF有効化（CommonRuleSet）

13. まとめ

今回の構築で以下を達成：

- 高可用・低コストなAWS 3層構成を実現
- 運用負担を軽減し、監視・バックアップを自動化
- 将来的なIaC・AI自動化の拡張基盤を確保