7.セキュリティ設定一覧

🟦 AWSセキュリティ設定一覧

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. 概要

本ドキュメントでは、AWS環境の主要セキュリティ項目（IAM / Security Group / ネットワーク / 暗号化 / ログ管理）を一覧化し、

構成の整合性とセキュリティレベルを明確にする。

💙 2. IAM（ユーザー / ロール / 権限）一覧

🧩 2.1 IAMユーザー

ユーザー名	権限	MFA	用途 / 備考
*****	AdministratorAccess	有効	管理者アカウント（MFA必須）
viewer-ops	ReadOnlyAccess	任意	監視・参照用

🧩 2.2 IAMロール

ロール名	アタッチポリシー	用途
EC2InstanceRole-Web	AmazonS3ReadOnlyAccess / CloudWatchAgentServerPolicy	EC2からS3アクセス・ログ送信
LambdaExecutionRole（任意）	AWSLambdaBasicExecutionRole	将来Lambda使用時

🧩 2.3 IAMポリシー（カスタム）

ポリシー名	内容	用途
S3AssetAccessPolicy（任意）	バケット単体のアクセス制御	限定バケットアクセス

💛 3. Security Group（SG）一覧

🧩 3.1 ALB-SG

設定	内容
Inbound	80/443（0.0.0.0/0）
Outbound	全許可
用途	外部公開用ALB

🧩 3.2 Web-SG（EC2）

設定	内容
Inbound	80（ALB-SG から）22（管理端末から）
Outbound	3306（DB-SG へ）
用途	Web/APサーバ

🧩 3.3 DB-SG（RDS）

設定	内容
Inbound	3306（Web-SG から）
Outbound	（デフォルト許可）
用途	MySQL データベース

💜 4. ネットワーク（VPC / Route / ACL）

🧩 4.1 VPC設定

項目	内容
CIDR	10.10.0.0/16
Public Subnet	10.10.0.0/24 / 1a 10.10.1.0/24 / 1c
Private-App	10.10.10.0/24 / 1a10.10.11.0/24 / 1c
Private-DB	10.10.20.0/24 / 1a10.10.21.0/24 / 1c

🧩 4.2 NAT / IGW / Route Table

コンポーネント	設定
IGW	vpcにアタッチ
NATGW	ap-northeast-1a のみ
Public Route	0.0.0.0/0 → IGW
Private Route	0.0.0.0/0 → NATGW

🧩 4.3 Network ACL（必要に応じて）

サブネット	ルール	備考
Public	デフォルト	今回はSG中心で管理
Private	デフォルト	ACLはシンプル維持

💙 5. 暗号化（Encryption）

対象	暗号化方式	状態
S3	SSE-S3（またはSSE-KMS）	有効
RDS	AES-256	有効
EC2 EBS	AES-256	有効（AMAZON管理キー）
ACM	SSL証明書（TLS 1.2/1.3）	有効

💚 6. ログ管理（CloudWatch / S3）

ログ種類	送信先	状態
EC2 Nginx Access Log	CloudWatch Logs	有効
EC2 PHP Error Log	CloudWatch Logs	有効
RDS エラーログ	CloudWatch Logs	有効
ALB アクセスログ	必要に応じてS3へ	任意
CloudTrail	任意（必要なら有効化）	OFFまたはON

💛 7. 監査項目（最低ライン）

項目	状態	コメント
MFA必須（管理者）	✅	admin-fuu に適用済み

項目	状態	コメント
セキュリティグループのポート最小化	✅	22, 80, 443, 3306 のみ
VPC内の通信分離	✅	Public / Private / DB
IAM最小権限	✅	S3 / CloudWatch のみ
暗号化	✅	EBS / RDS / S3 すべて有効

💜 8. 今後強化すべきセキュリティ項目

提案内容	効果	優先度
AWS WAF導入	主要攻撃（SQLi・XSS）防止	高
SSM Session Managerへ完全移行	SSH不要・ログ保存可	中
IAM Access Analyzer設定	過剰権限検出	中
CloudTrail全有効化	設定変更の監査	中