7.AWS Security Configuration Summary

🔵 AWS Security Configuration Summary

（英語版 / *Based on your PDF*）

💚 1. Overview

This document summarizes the key security configurations implemented in the AWS environment, including IAM, Security Groups, Network settings, encryption, and logging.

It clarifies the consistency of the architecture and the overall security level.

💙 2. IAM (Users / Roles / Permissions)

🧩 2.1 IAM Users

User Name	Permission	MFA	Notes
*****	AdministratorAccess	Enabled	Primary admin account (MFA required)
viewer-ops	ReadOnlyAccess	Optional	Monitoring / read-only access

🧩 2.2 IAM Roles

Role Name	Attached Policies	Purpose
EC2InstanceRole-Web	AmazonS3ReadOnlyAccess / CloudWatchAgentServerPolicy	S3 access + EC2 log forwarding
LambdaExecutionRole (optional)	AWSLambdaBasicExecutionRole	Reserved for future Lambda use

🧩 2.3 Custom IAM Policies

Policy Name	Description	Purpose
S3AssetAccessPolicy (optional)	Restricts access to specific S3 buckets	Scoped bucket access

💛 3. Security Groups (SG)

🧩 3.1 ALB-SG

Inbound: 80/443 (0.0.0.0/0)

Outbound: All allowed

Purpose: Public-facing ALB

🧩 3.2 Web-SG (EC2)

Inbound:

- 80 (from ALB-SG)
- 22 (from admin workstation)

Outbound:

- 3306 (to DB-SG)

Purpose: Web / Application Server

🧩 3.3 DB-SG (RDS)

Inbound:

- 3306 (from Web-SG)

Outbound:

- Default allowed

Purpose: MySQL Database

💜 4. Network (VPC / Route / ACL)

🧩 4.1 VPC Settings

Item	Value
CIDR	10.10.0.0/16

Item	Value
Public Subnet	10.10.0.0/24 (1a), 10.10.1.0/24 (1c)
Private-App	10.10.10.0/24 (1a), 10.10.11.0/24 (1c)
Private-DB	10.10.20.0/24 (1a), 10.10.21.0/24 (1c)

🧩 4.2 NAT / IGW / Route Tables

Component	Setting
IGW	Attached to VPC
NATGW	ap-northeast-1a only
Public Route	0.0.0.0/0 → IGW
Private Route	0.0.0.0/0 → NATGW

🧩 4.3 Network ACL (if needed)

- **Public:** Default (security managed via SGs)
- **Private:** Default (kept simple intentionally)

💙 5. Encryption

Resource	Method	Status
S3	SSE-S3 or SSE-KMS	Enabled
RDS	AES-256	Enabled
EC2 EBS	AES-256 (AWS-managed key)	Enabled
ACM	TLS 1.2/1.3 certificates	Active

💚 6. Logging (CloudWatch / S3)

Log Type	Destination	Status
EC2 Nginx Access Logs	CloudWatch Logs	Enabled
EC2 PHP Error Logs	CloudWatch Logs	Enabled
RDS Error Logs	CloudWatch Logs	Enabled
ALB Access Logs	S3 (optional)	Optional
CloudTrail	Optional	OFF or ON depending on requirements

💛 7. Audit Checklist (Minimum Baseline)

Item	Status	Notes
MFA for admin	✅	Enabled for admin-fuu
SG port minimization	✅	Only 22 / 80 / 443 / 3306
Network segmentation	✅	Public / Private / DB
Least-privilege IAM	✅	S3 + CloudWatch only
Encryption	✅	EBS / RDS / S3 enabled

💜 8. Recommended Security Enhancements

Recommendation	Benefit	Priority
Enable AWS WAF	Protects from SQLi, XSS	High
Migrate to SSM Session Manager	Remove SSH, central logging	Medium
Enable IAM Access Analyzer	Detects excessive privileges	Medium
Fully enable CloudTrail	Audits config changes	Medium