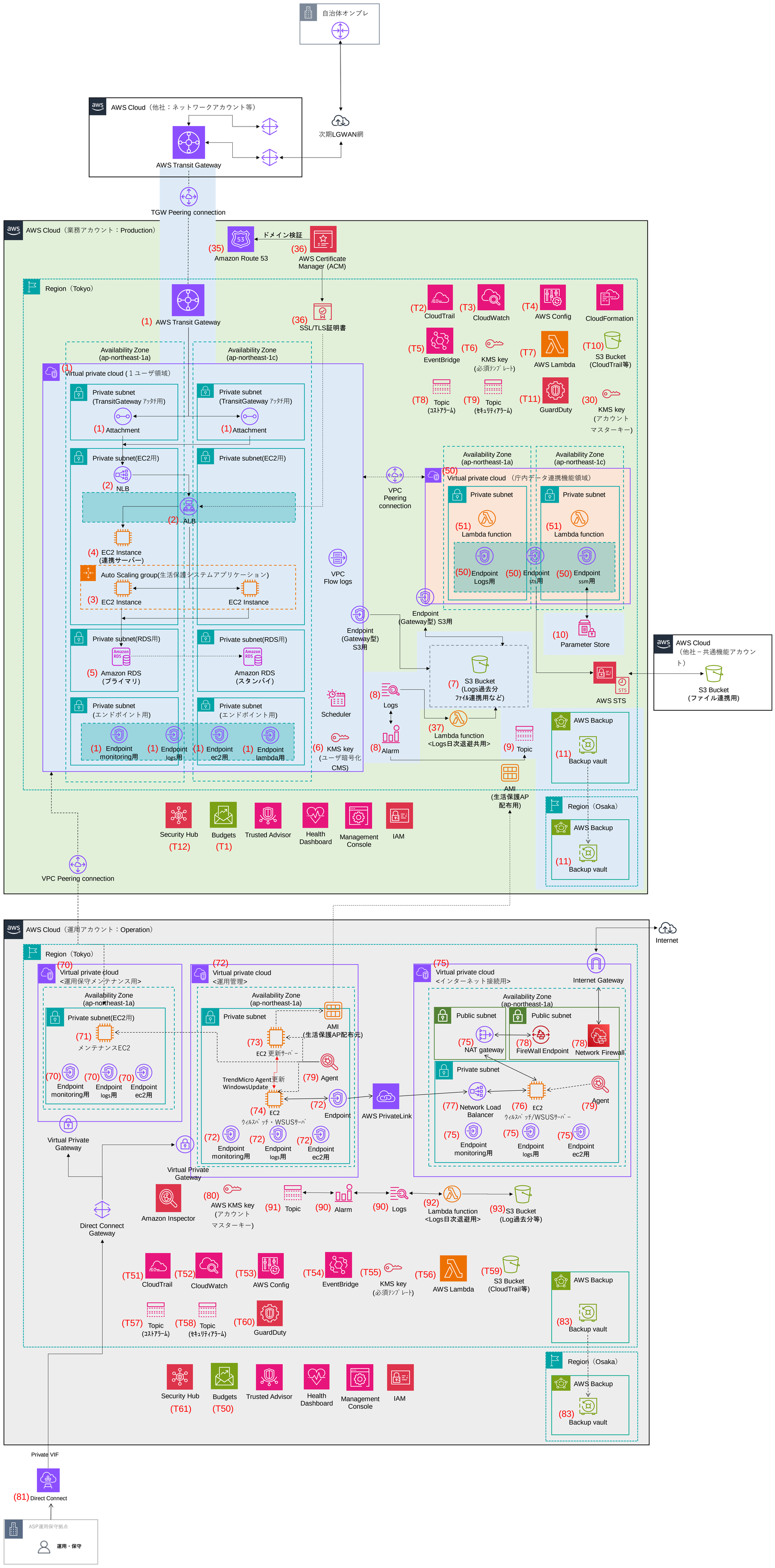
AWS構成図


自治体オンプレ
AWS Cloud（他社：ネットワークアカウント等）
AWS Transit Gateway
次期LGWAN網
TGW Peering connection
AWS Cloud（業務アカウント：Production）
(35) Amazon Route 53
ドメイン検証
(36) AWS Certificate Manager (ACM)
Region（Tokyo）
(1) AWS Transit Gateway
(36) SSL/TLS証明書
(T2) CloudTrail
(T3) CloudWatch
(T4) AWS Config
CloudFormation
(T5) EventBridge
(T6) KMS key (必須ﾃﾝﾌﾟﾚｰﾄ)
(T7) AWS Lambda
(T10) S3 Bucket (CloudTrail等)
(T8) Topic (ｺｽﾄｱﾗｰﾑ)
(T9) Topic (ｾｷｭﾘﾃｨｱﾗｰﾑ)
(T11) GuardDuty
(30) KMS key (アカウントマスターキー)
Availability Zone (ap-northeast-1a)
Availability Zone (ap-northeast-1c)
(1) Virtual private cloud (1 ユーザ領域)
Private subnet (TransitGateway ｱｯﾀﾁ用)
(1) Attachment
Private subnet(EC2用)
(2) NLB
(2) ALB
(4) EC2 Instance (連携サーバー)
Auto Scaling group(生活保護システムアプリケーション)
(3) EC2 Instance
EC2 Instance
Private subnet(RDS用)
(5) Amazon RDS (プライマリ)
Amazon RDS (スタンバイ)
Private subnet (エンドポイント用)
(1) Endpoint monitoring用
(1) Endpoint logs用
(1) Endpoint ec2用
(1) Endpoint lambda用
(50) Virtual private cloud （庁内データ連携機能領域）
VPC Peering connection
Private subnet
(51) Lambda function
(50) Endpoint Logs用
(50) Endpoint sts用
(50) Endpoint ssm用
VPC Flow logs
Endpoint (Gateway型) S3用
Endpoint (Gateway型) S3用
(10) Parameter Store
(7) S3 Bucket (Logs過去分 ﾌｧｲﾙ連携用など)
AWS STS
AWS Cloud （他社－共通機能アカウント）
S3 Bucket (ファイル連携用)
(8) Logs
(8) Alarm
Scheduler
(6) KMS key (ユーザ暗号化 CMS)
(37) Lambda function <Logs日次退避共用>
(9) Topic
AWS Backup
(11) Backup vault
AMI (生活保護AP配布用)
Region（Osaka）
Security Hub (T12)
Budgets (T1)
Trusted Advisor
Health Dashboard
Management Console
IAM
VPC Peering connection
AWS Cloud（運用アカウント：Operation）
Internet
Region（Tokyo）
(70) Virtual private cloud <運用保守メンテナンス用>
(72) Virtual private cloud <運用管理>
(75) Virtual private cloud <インターネット接続用>
Internet Gateway
Availability Zone (ap-northeast-1a)
Private subnet(EC2用)
(71) メンテナンスEC2
(70) Endpoint monitoring用
(70) Endpoint logs用
(70) Endpoint ec2用
Private subnet
AMI (生活保護AP配布元)
(73) EC2 更新ｻｰﾊﾞｰ
TrendMicro Agent更新 WindowsUpdate
(79) Agent
(74) EC2 ｳｨﾙｽﾊﾟｯﾁ・WSUSｻｰﾊﾞ
(72) Endpoint
(72) Endpoint monitoring用
(72) Endpoint logs用
(72) Endpoint ec2用
AWS PrivateLink
Public subnet
(75) NAT gateway
(78) FireWall Endpoint
(78) Network Firewall
(77) Network Load Balancer
(76) EC2 ｳｨﾙｽﾊﾟｯﾁ/WSUSｻｰﾊﾞｰ
(79) Agent
(75) Endpoint monitoring用
(75) Endpoint logs用
(75) Endpoint ec2用
Virtual Private Gateway
Virtual Private Gateway
Direct Connect Gateway
Amazon Inspector
(80) AWS KMS key (アカウントマスターキー)
(91) Topic
(90) Alarm
(90) Logs
(92) Lambda function <Logs日次退避用>
(93) S3 Bucket (Log過去分等)
(T51) CloudTrail
(T52) CloudWatch
(T53) AWS Config
(T54) EventBridge
(T55) KMS key (必須ﾃﾝﾌﾟﾚｰﾄ)
(T56) AWS Lambda
(T59) S3 Bucket (CloudTrail等)
(T57) Topic (ｺｽﾄｱﾗｰﾑ)
(T58) Topic (ｾｷｭﾘﾃｨｱﾗｰﾑ)
(T60) GuardDuty
AWS Backup
(83) Backup vault
Region（Osaka）
AWS Backup
(83) Backup vault
Security Hub (T61)
Budgets (T50)
Trusted Advisor
Health Dashboard
Management Console
IAM
Private VIF
(81) Direct Connect
ASP運用保守拠点
運用・保守