

AWSへのECサイト構築のご提案

前提条件

- お客様サービスは日本国内で展開されている
- サービス継続期間は1年間ごとに見直す
- 現状のECサイトの会員数は500名程
- 各種AWSサービスはスモールスタート

目次

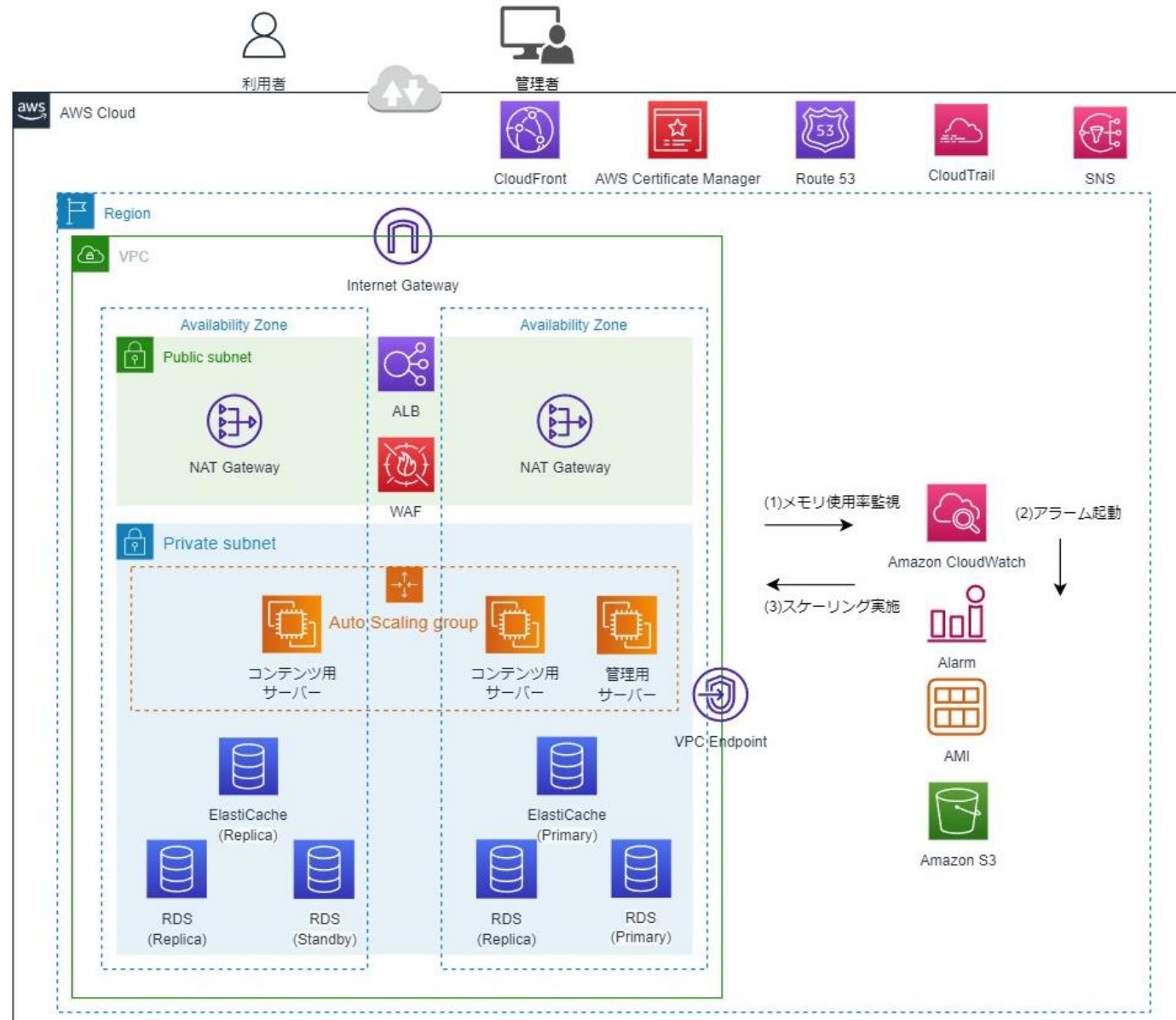
- ご要望一覧
- 構成図
- 構成図説明 ① ～ ⑥
- インスタンス選定について（EC2） ① ～ ③
- インスタンス選定について（DB） ① ～ ②

ご要望一覧

No.	ご要望	説明
1	セキュアなアーキテクチャ	構成図説明① 参照
2	攻撃者から一般的な攻撃へのアプリケーションの保護	構成図説明① 参照
3	余剰リソースを極力抑え、利用費を最適化	構成図説明② 参照
4	時間帯に応じたインフラストラクチャの柔軟性	構成図説明② 参照
5	管理用サーバ（複数台構成不可能）の耐障害性	構成図説明② 参照
6	管理用アクセス、クライアント用アクセスでサーバーを分離	構成図説明③ 参照
7	DBは更新用、参照用で分離	構成図説明④ 参照
8	更新用DBの高可用性設計	構成図説明④ 参照
9	画像コンテンツ用のストレージ拡大が可能であること	構成図説明⑤ 参照
10	サービスのレスポンス速度の向上	構成図説明⑤ 参照
11	障害・異常を即座に検知、通知	構成図説明⑥ 参照

構成図

ご提案する構成は以下になります。各要件への対応方法については次頁以降でご紹介いたします。



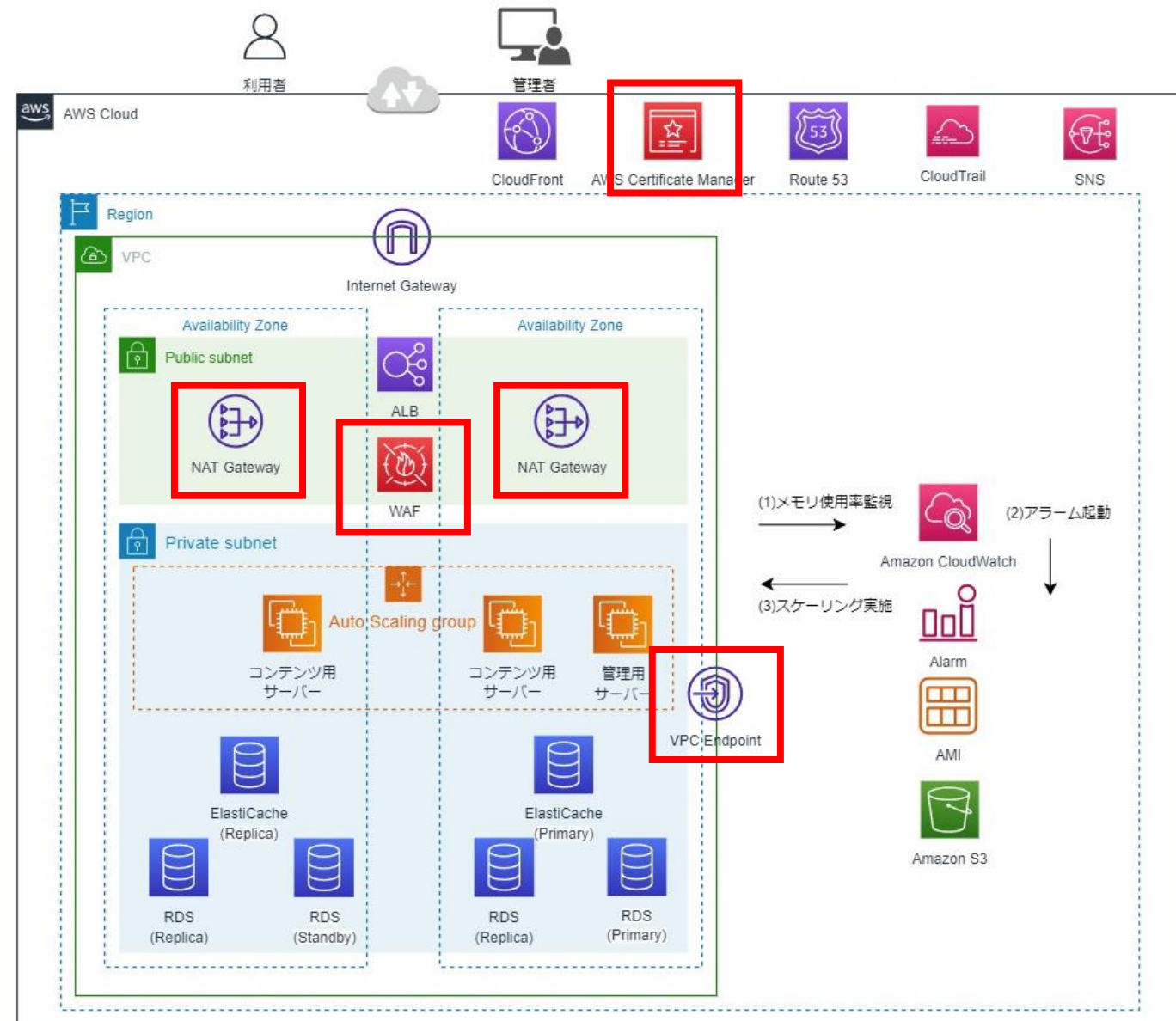
構成図説明①

1, セキュアなアーキテクチャ

- ・ NAT Gatewayを設置し EC2をPrivateサブネットに配置
 - EC2をPublicなアクセスから保護
 - 通信料金抑制の為、EC2 S3間アクセスはVPN エンドポイントを経由
- ・ ACM(AWS Certificate Manager)
 - ALBと紐づけることで、配下インスタンスの証明書を一元管理
 - 証明書の無料利用が可能

2, 攻撃者から一般的な攻撃へのアプリケーションの保護

- ・ WAFを設置
 - アサインするRules
 - Core rule set : 一般的な攻撃へのアプリケーション保護
 - Linux operating system : Linux 固有の脆弱性からの保護
 - SQL database : SQL データベースの悪用からの保護



構成図説明②

3, 余剰リソースを極力抑え、利用費を最適化

4, 時間帯に応じたインフラストラクチャの柔軟性

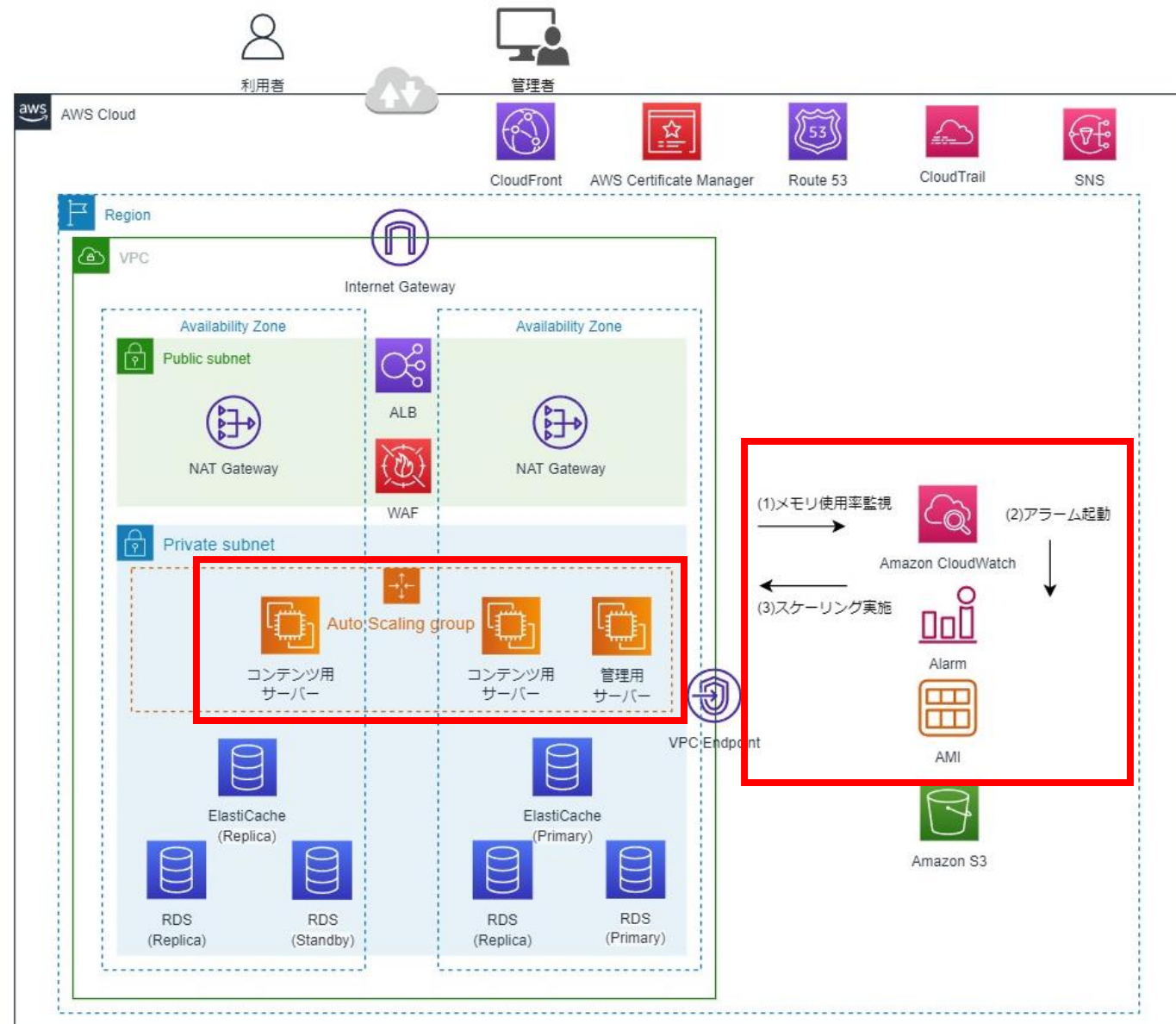
- Auto Scaling

- CloudWatchを利用したターゲット追跡トラッキング
 - カスタムメトリクスを設定しメモリ使用率50%以内を維持
- スケジュールスケーリング
 - イベントなどに備えて、希望台数スケーリングの開始、終了タイミングを設定可能

5, 管理用サーバ（複数台構成不可能）の耐障害性

- Auto Scaling

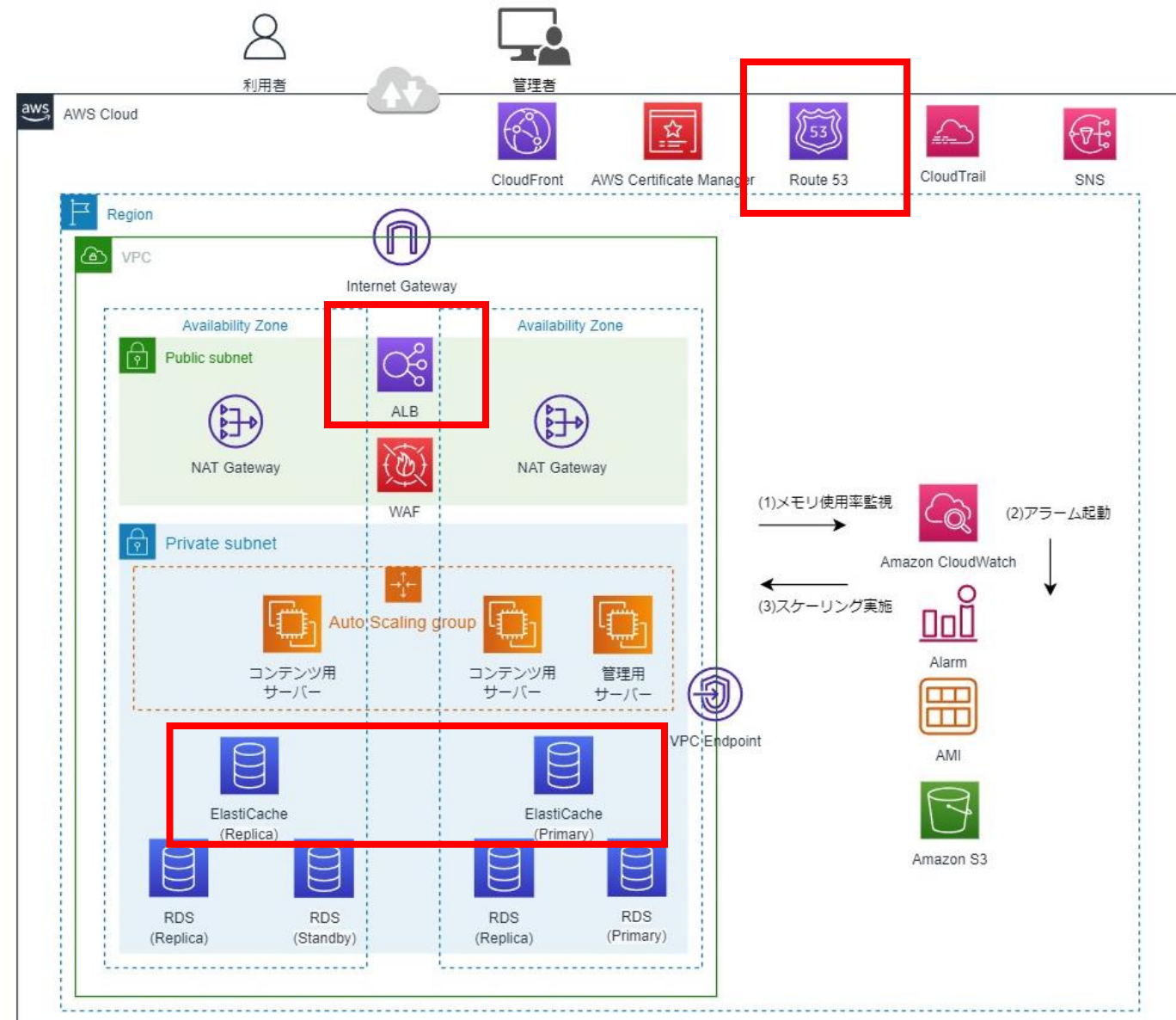
- 希望台数を1台にすることで、単体で自動リカバリを実現



構成図説明③

6, 管理用アクセス、クライアント用アクセスでサーバーを分離

- ALB
 - パスベースルーティングの導入
 - 任意のパスとターゲットグループを紐づけルーティングが可能
- Route 53
 - エイリアスレコードの登録
 - ドメインをALBのDNS名と紐づける
 - ※ ALBのスケールアウト時など、IPアドレス変更のため
- ElastiCache
 - セッション情報をストア
 - Auto Scalingでサーバがスケールしても
共通のセッション情報を参照できる
 - Primaryがダウンした際、参照用のReplicaが
Primaryとして自動フェイルオーバー



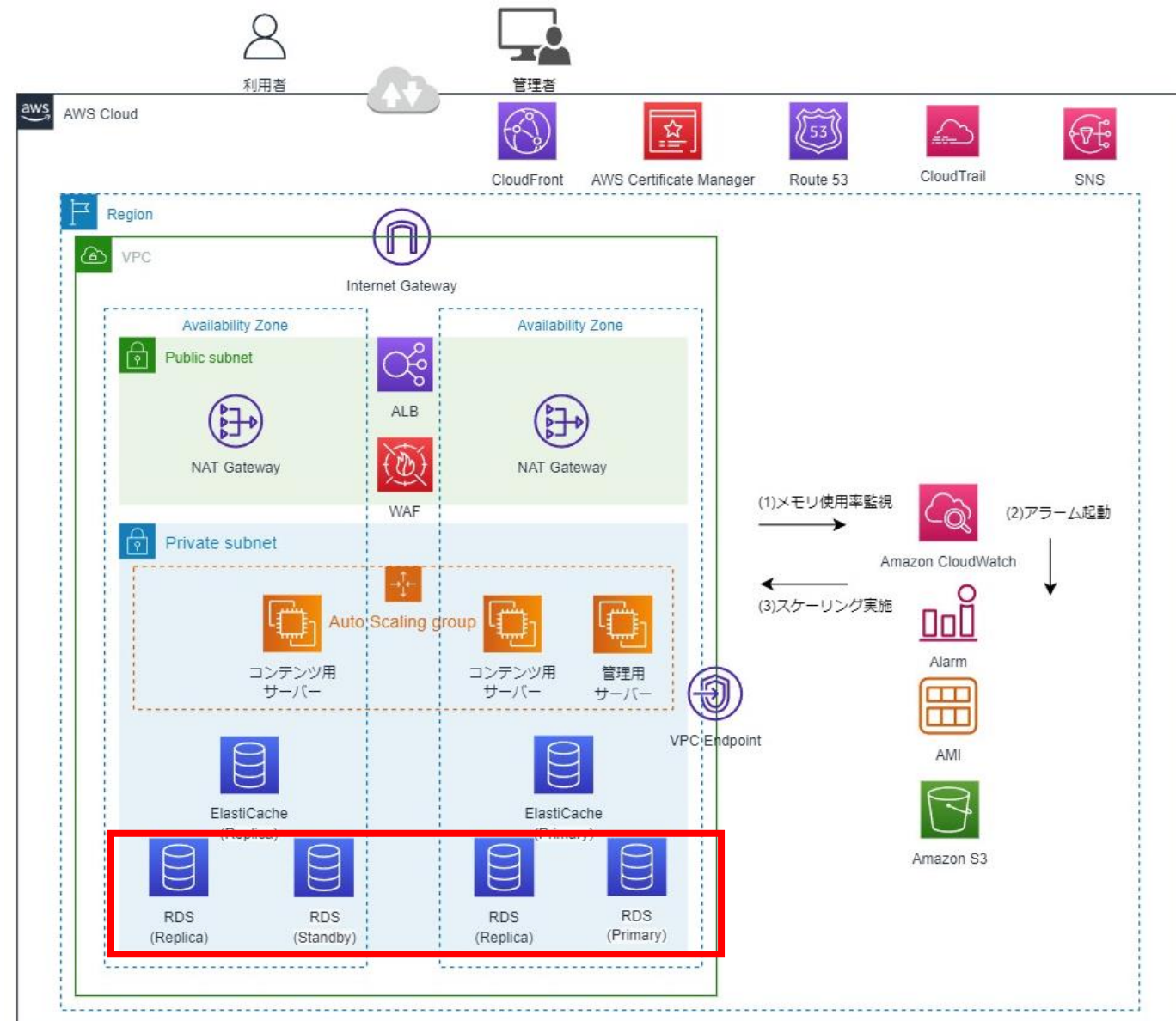
構成図説明④

7, DBは更新用、参照用で分離

- ・ 参照系DB用にリードレプリカを設置
 - 更新系のDBのレプリカを作成
 - 更新系DBに変更がある場合、リードレプリカが更新される

8, 更新用DBの高可用性設計

- ・ RDSをマルチAZ配置
 - 別AZにスタンバイレプリカを配置
 - 60秒で自動フェイルオーバー



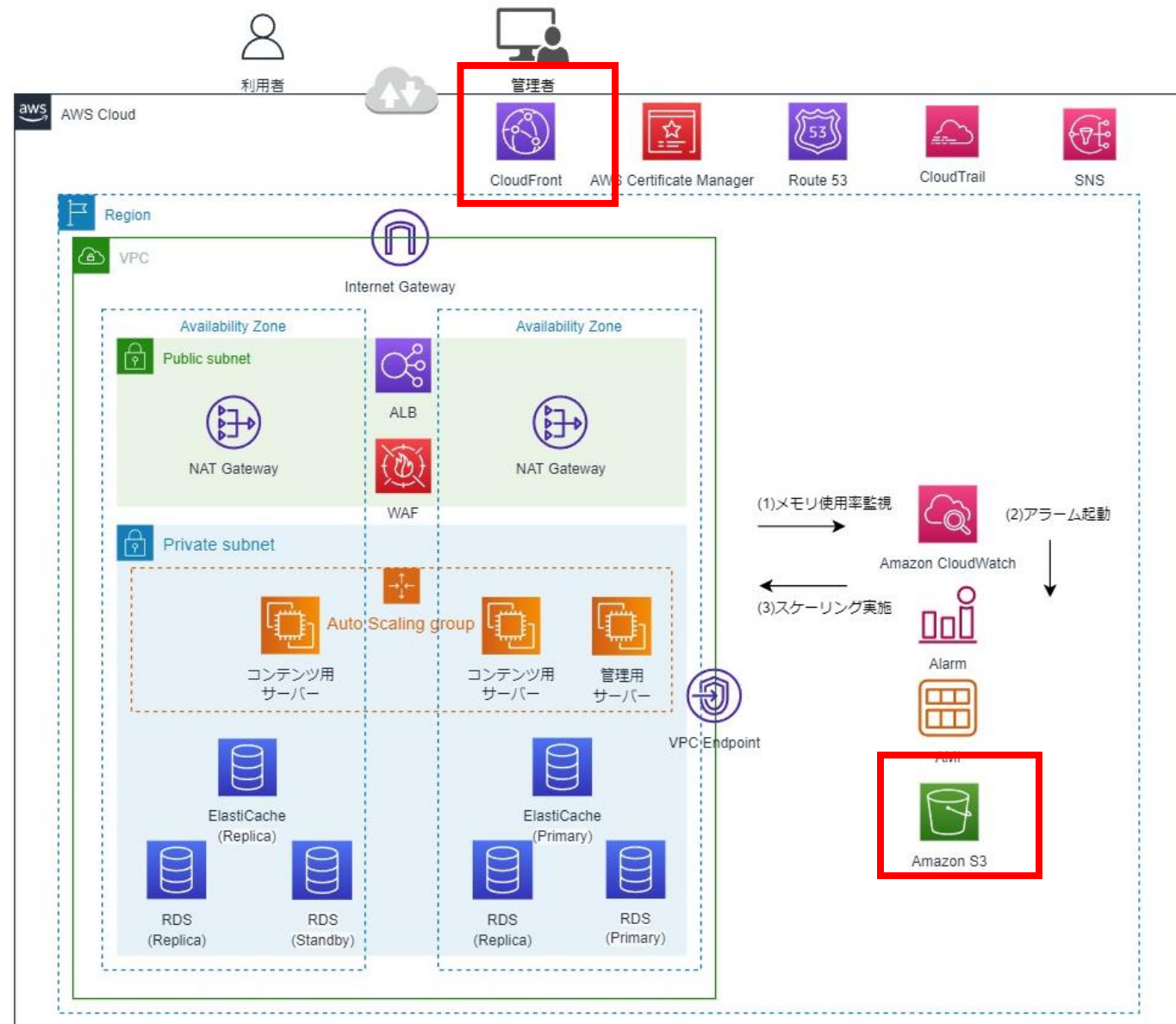
構成図説明⑤

9, 画像コンテンツ用のストレージ拡大が可能であること

- ・ S3にコンテンツを保存
 - 理論上の容量制限が無い
 - 1オブジェクトあたり5TB
 - オブジェクトの暗号化も可能

10, サービスのレスポンス速度の向上

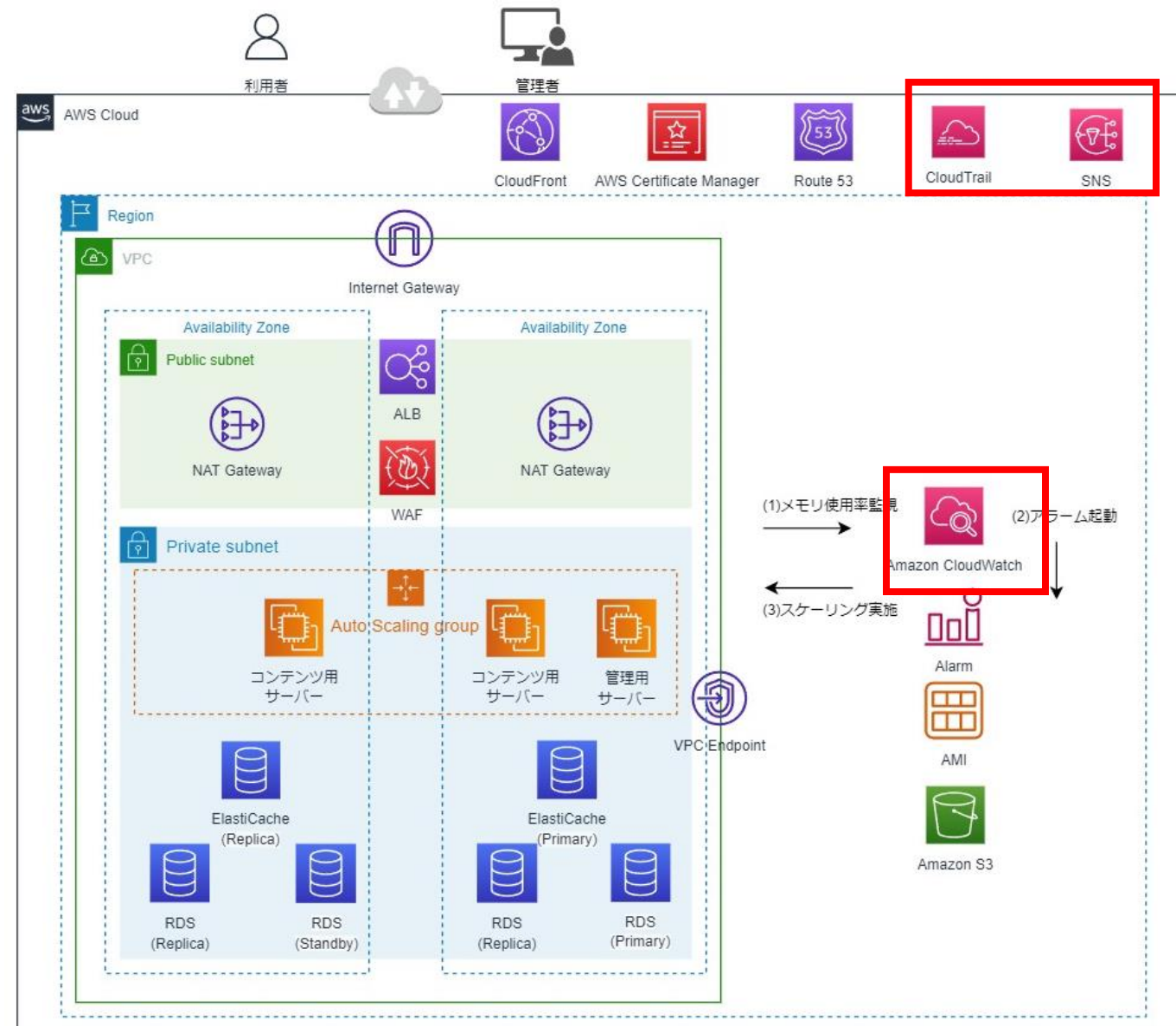
- ・ CloudFront
 - S3をオリジンとして、コンテンツをキャッシュ
 - クライアントからのリクエストに即時レスポンスが可能
 - サーバーへの負荷軽減



構成図説明⑥

11, 障害・異常を即座に検知、通知

- CloudTrail
 - AWSアカウント内のリソースに対して実行される管理操作（管理イベント）の監視
 - CloudWatchLogsを使用した異常時の通知が可能
- CloudWatch
 - インスタンスの死活監視
 - CloudWatchメトリクス
 - 対象インスタンスの何を監視するか設定(CPU、データ通信量等)
 - CloudWatchAlarms
 - メトリクス等に対しての閾値&アクションを設定
 - 閾値を超えた場合の通知が可能



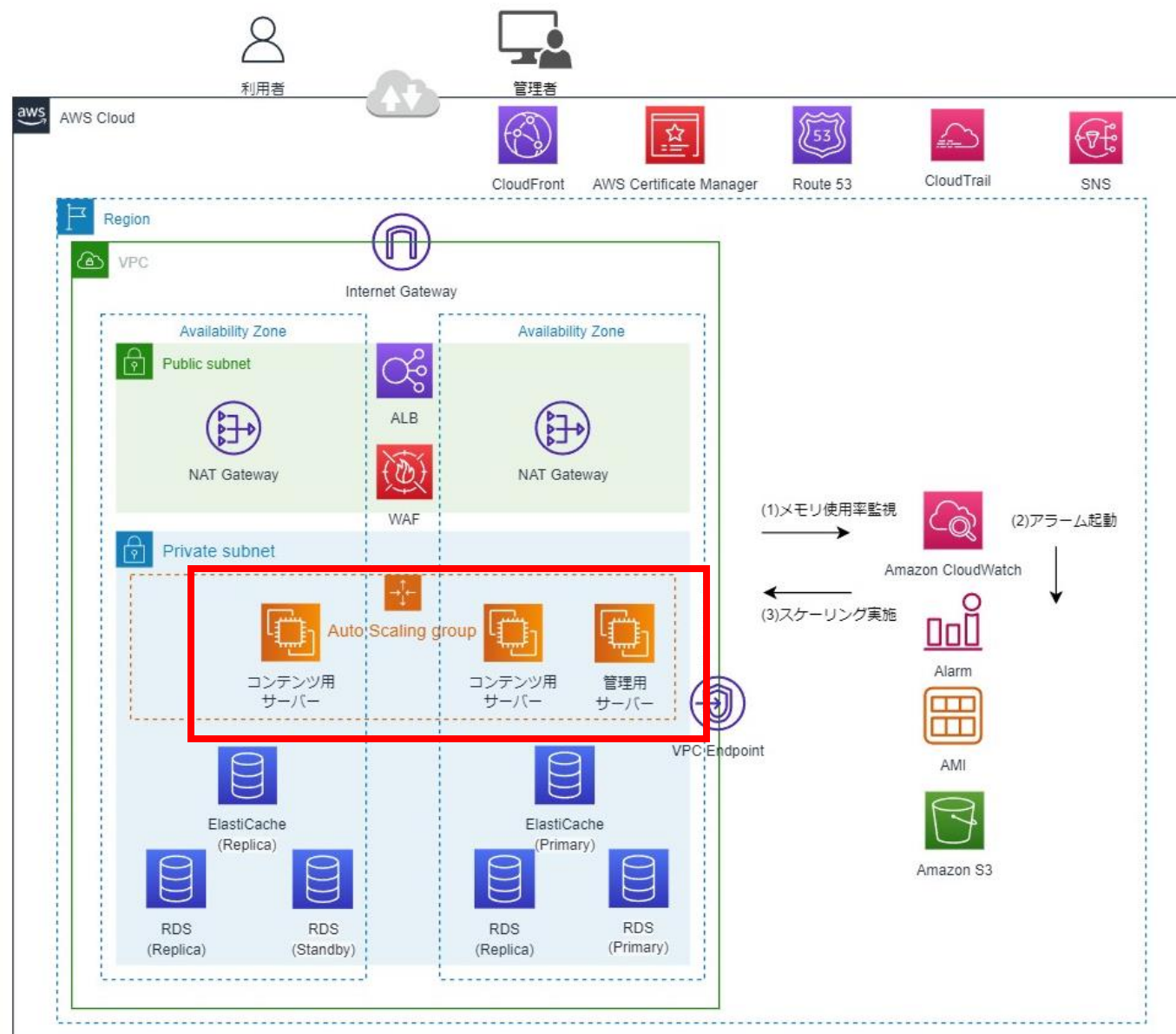
インスタンス選定について (EC2) ①

EC2

- ・ インスタンスの種類
 - コンバーティブルインスタンス (1年)
- ・ インスタンスタイプ
 - t3.medium (2 vCPU / 4 GB メモリ)
 - ※ 選定根拠は次ページに記載
- ・ ストレージ
 - 汎用SSD (gp2) ボリューム 50 GB
 - 静的コンテンツをS3に保存する為、100 GBでなくてもよいと判断
- ・ OS
 - CentOS6 64bit (on Amazon Linux 2)
- ・ Webサーバー
 - Apache2.2

Auto Scaling

- ・ グループサイズ
 - 最低2台 希望2台 最高7台
 - ※ 選定根拠は次ページに記載



インスタンス選定について（EC2）②

・条件

サーバーOS：CentOS6 64bit

Webサーバー：Apache2.2

※軽いホームページ、アクセス数の少ない状態

・平均メモリ使用率

28.42MB/1閲覧

```
# ps aux | head -1 && ps aux | grep httpd | grep -v grep
```

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	17114	0.0	0.3	470980	13232	?	Ss	Apr26	1:36	/usr/sbin/httpd
apache	21111	0.0	0.7	474796	27956	?	S	May12	0:38	/usr/sbin/httpd
apache	21115	0.0	0.8	479880	32376	?	S	May12	0:38	/usr/sbin/httpd
apache	21116	0.0	0.7	475104	28968	?	S	May12	0:38	/usr/sbin/httpd
apache	21871	0.0	1.0	486060	39480	?	S	May12	0:39	/usr/sbin/httpd
apache	21872	0.0	0.6	474152	26568	?	S	May12	0:38	/usr/sbin/httpd
apache	21873	0.0	0.8	479540	31920	?	S	May12	0:38	/usr/sbin/httpd
apache	21874	0.0	0.7	476468	29380	?	S	May12	0:38	/usr/sbin/httpd
apache	21875	0.0	0.7	475956	28348	?	S	May12	0:38	/usr/sbin/httpd
apache	21876	0.0	0.7	475900	29120	?	S	May12	0:36	/usr/sbin/httpd
apache	21877	0.0	0.7	477232	29192	?	S	May12	0:38	/usr/sbin/httpd
apache	21878	0.0	0.8	479540	32736	?	S	May12	0:37	/usr/sbin/httpd

インスタンス選定について（EC2）③

2022/9/1時点での価格

インスタンス名	RI の前払いの料金	RI の月額料金	RI の実質的な時間単位の料金	オンデマンドと比較した費用節減	オンデマンド料金
t3a.nano	0 USD	3.50 USD	0.005 USD	21%	0.0061 USD
t3.nano	0 USD	3.87 USD	0.005 USD	22%	0.0068 USD
t3a.micro	0 USD	7.01 USD	0.010 USD	21%	0.0122 USD
t3.micro	0 USD	7.81 USD	0.011 USD	21%	0.0136 USD
t3a.small	0 USD	14.02 USD	0.019 USD	22%	0.0245 USD
t3.small	0 USD	15.62 USD	0.021 USD	21%	0.0272 USD
t3a.medium	0 USD	28.11 USD	0.039 USD	21%	0.0490 USD
t3.medium	0 USD	31.17 USD	0.043 USD	22%	0.0544 USD
t3a.large	0 USD	56.14 USD	0.077 USD	21%	0.0979 USD
t3.large	0 USD	62.42 USD	0.086 USD	21%	0.1088 USD
t3a.xlarge	0 USD	112.35 USD	0.154 USD	21%	0.1958 USD
t3.xlarge	0 USD	124.83 USD	0.171 USD	21%	0.2176 USD
t3a.2xlarge	0 USD	224.62 USD	0.308 USD	21%	0.3917 USD
t3.2xlarge	0 USD	249.59 USD	0.342 USD	21%	0.4352 USD
m5a.large	0 USD	65.70 USD	0.090 USD	20%	0.1120 USD
m5.large	0 USD	72.27 USD	0.099 USD	20%	0.1240 USD
m5ad.large	0 USD	78.11 USD	0.107 USD	20%	0.1340 USD
m5d.large	0 USD	85.41 USD	0.117 USD	20%	0.1460 USD

※コンバーティブルインスタンスの場合

※東京リージョン

※1年間での購入

※前払いオプションなし

※料金参考 <https://aws.amazon.com/jp/ec2/pricing/reserved-instances/pricing/>

t3.mediumの場合、閲覧数MAX500に対して2台～7台のインスタンスで稼働可能のため、柔軟性・コストでが最も優れていると判断

	台数	コンバーティブル		オンデマンド（AutoScaling用）				
		1	2	3	4	5	6	7
t3.medium（4G メモリ）	閲覧数	72	144	216	288	360	432	504
	EC2月料金	31.17	62.34	114.06	152.08	190.1	228.12	266.14
	EBS月料金	5.00	10.00	15.00	20.00	25.00	30.00	35.00
	月合計(USD)	36.17	72.34	129.06	172.08	215.10	258.12	301.14
t3.large（8G メモリ）	閲覧数	144	288	432	576	720	864	1008
	EC2月料金	62.42	124.84	226.56	302.08	377.6	453.12	528.64
	EBS月料金	5.00	10.00	15.00	20.00	25.00	30.00	35.00
	月合計(USD)	67.42	134.84	241.56	322.08	402.60	483.12	563.64
m5.large（8G メモリ）	閲覧数	144	288	432	576	720	864	1008
	EC2月料金	72.27	144.54	260.16	346.88	433.6	520.32	607.04
	EBS月料金	5.00	10.00	15.00	20.00	25.00	30.00	35.00
	月合計(USD)	77.27	154.54	275.16	366.88	458.60	550.32	642.04

※EC2台数当たりの消費メモリと価格（メモリ使用率 50%を想定）

※汎用 SSD (gp2) ボリューム 1 か月にプロビジョニングされたストレージ 1 GB あたり 0.10USD

※サーバーOS：CentOS6 64bit

Webサーバー：Apache2.2

上記条件でのメモリ負荷

28.42MB/1閲覧

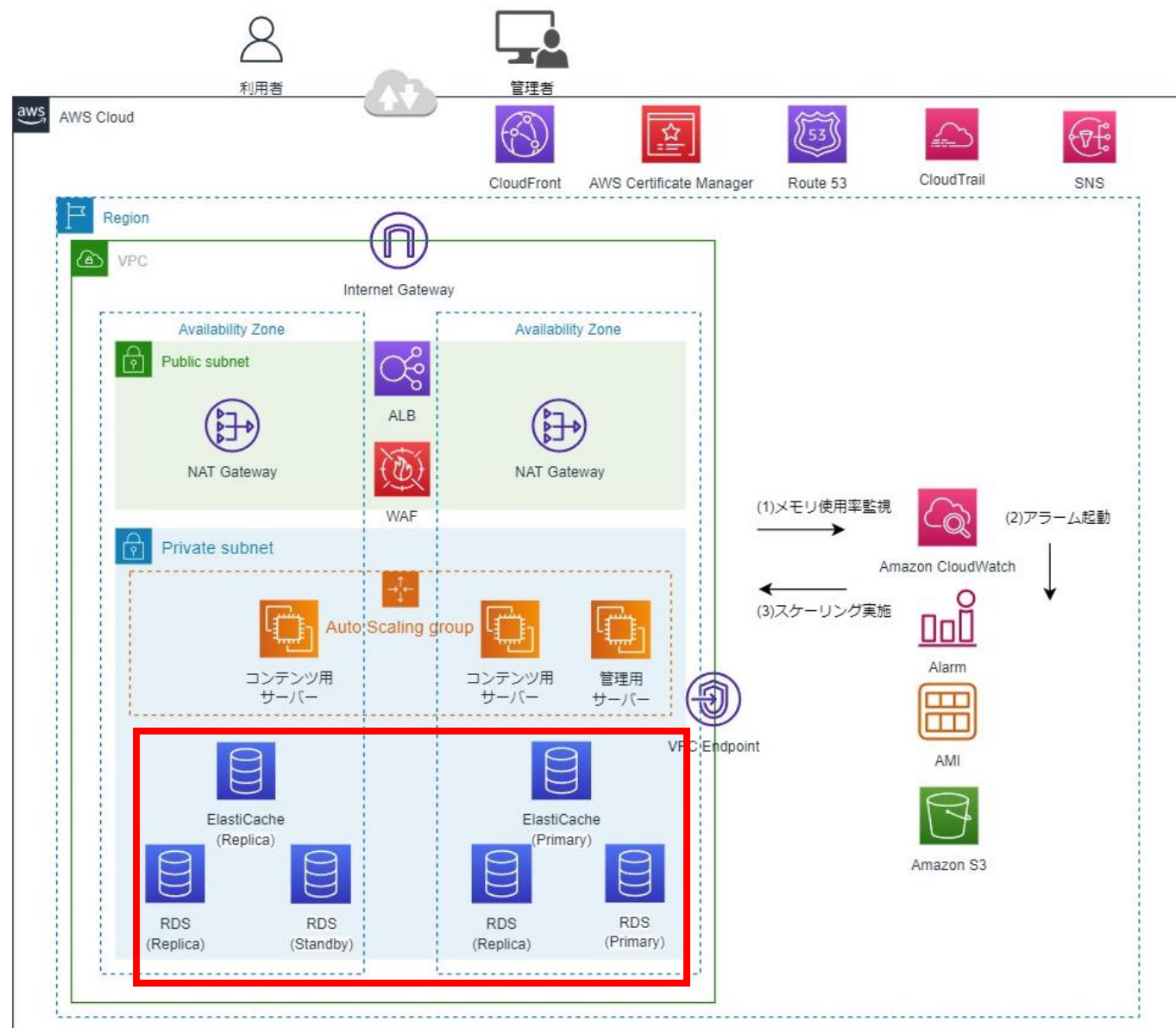
インスタンス選定について (DB) ①

RDS

- ・ インスタンスの種類
 - リザーブドインスタンス (1年)
- ・ インスタンスタイプ
 - db.m5.large (2 vCPU / 8 GB メモリ)
 - ※ 選定根拠は次ページに記載
- ・ ストレージ
 - 汎用SSD (gp2) ボリューム 100 GB
- ・ DBエンジン
 - MySQL

ElastiCache

- ・ インスタンスの種類
 - リザーブドインスタンス (1年)
- ・ インスタンスタイプ
 - cache.m5.large (2 vCPU / 6.38 GB メモリ)



インスタンス選定について (DB) ②

- ・ MySQL max_connections計算式

$\{\text{DBInstanceClassMemory} / 12582880\}$

- ・ メモリあたりのmax_connections (許可されるクライアントの同時接続数)

4Gメモリ (medium size) : 341 connections

8Gメモリ (large size) : 682 connections

※理論値の為、実際の値は10~20前後減る

参考

※https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Limits.html#RDS_Limits.MaxConnections