

SystemOperations on AWS

グループディスカッション

グループディスカッションの目的

- ①運用に役立つ AWS のサービスについて知識を深める
 - 「見る＆聞く」よりも「行う＆話す」の方が知識の定着率が良い
 - 積極的に参加しましょう（マイク必須、カメラ任意）
- ②Well-Architected Frameworkの考え方を体験する
 - “なぜ”そのアーキテクチャを選択する / しないのか考える
 - 6つの柱：セキュリティ / 信頼性 / コスト / 性能 / 運用 / 持続可能性

✕ ~~正解を出すこと~~ ○ 議論して考えること

サンプルシナリオ：
既存アプリケーションを
運用にしやすいシステムに最適化しよう

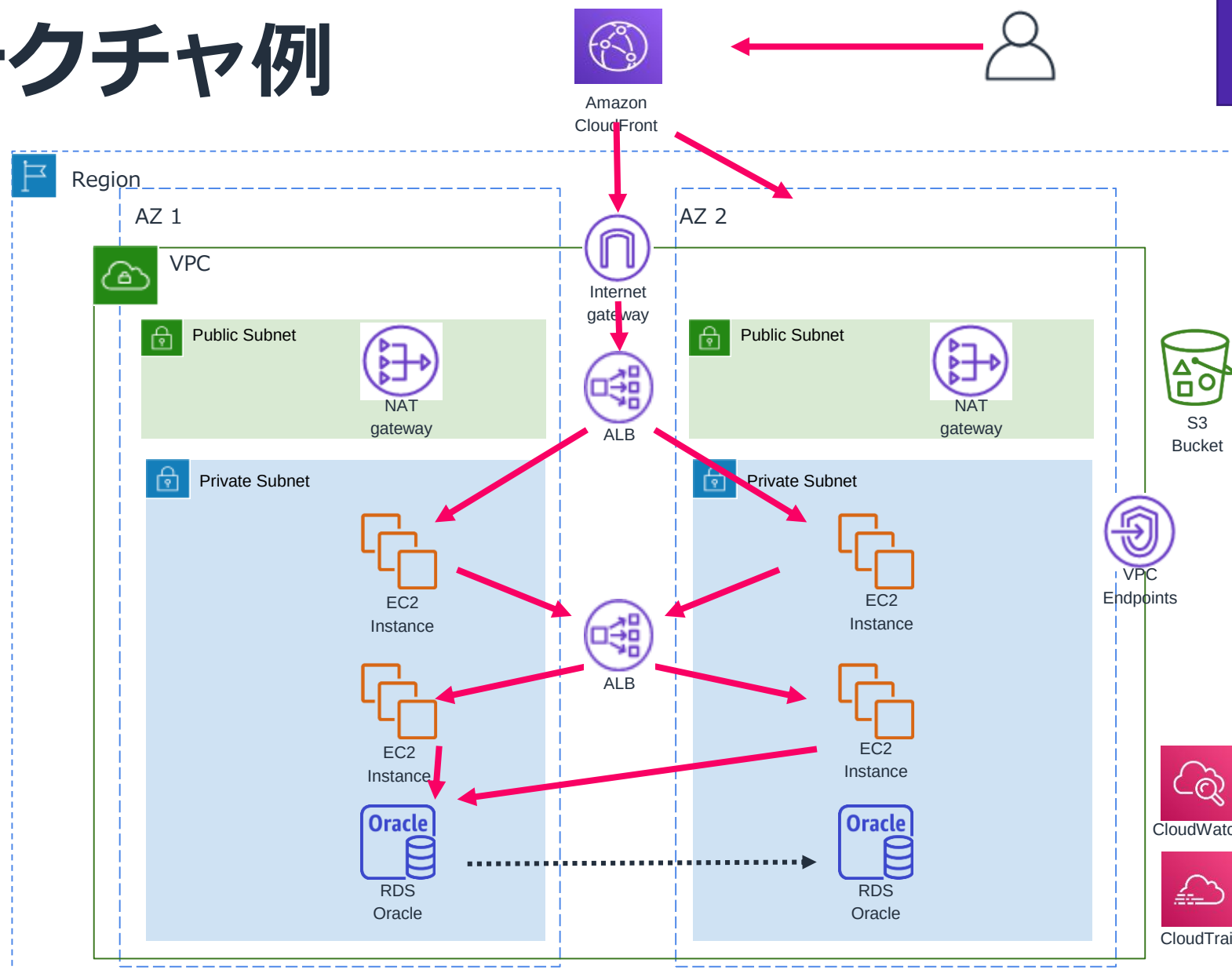
シナリオ

- 所属している会社では「**EC サイト**」をエンドユーザーに提供している
- 先月、ウェブアプリケーションをAWSに移行したばかり
- オンプレミスの頃と同じ機能をユーザに提供できるシステムはできた
- みなさんはAWSのシステム管理者を担当している

⇒ **運用しやすいシステムにするにはどうしたらいいか**

アーキテクチャ例

投影のみ



一般的な設計原則

Stop guessing your capacity needs

キャパシティの予測をやめる

Test systems at production scale

本番環境と同じ規模でテストする

Automate to make architectural experimentation easier

自動化によりアーキテクチャのテストを容易にする

Allow for evolutionary architectures

アーキテクチャを進化させる

Drive architectures using data

データに基づいてアーキテクチャを駆動する

Improve through game days

ゲームデーを利用して改善する

運用上の優秀性の柱：設計原則

- ・ 運用をコードとして実行する
- ・ 小規模かつ可逆的な変更を頻繁に行う
- ・ 運用手順を頻繁に改善する
- ・ 障害を予想する
- ・ 運用上のすべての障害から学ぶ

ヒアリング(1/3)

1



システム管理者

AWSアカウントにアクセスしたいのですが、アクセス方法はどのように運用されているのでしょうか？



既存社員

最初にAWSアカウントを作成した時の初期ユーザアカウントを全員でシェアして使っています。開発チーム・インフラチームの共有Wikiページに書いてあるので見たらいいですよ。

2



システム管理者

EC2インスタンスからS3などAWSリソースへのアクセスってどうやって権限与えているのでしょうか？



既存社員

IAMユーザ？とかいうものを作成したらアクセスキー、シークレットキーができたので、アプリケーションコードに埋め込んで作成しています!!

3



システム管理者

EC2インスタンスのデータバックアップはどうしていますか？



既存社員

僕が毎日やっています！出社したらマネジメントコンソールにアクセスして必要なサーバ1台1台に対して実行しています。

4



システム管理者

各AWSリソースの操作履歴や変更履歴はどうやって管理していますか？



既存社員

作業ログをwordで作成してそこにどんな変更をしたのか、だれが行うのかを記載しています。特にAWSの設定は初期状態から変更していません。

ヒアリング(2/3)

5



既存社員

管理系サーバでは日常的な運用タスク（ビジネス上必要なレポートログの抽出タスク、動作に問題が発生した際の一次調査タスク、追加設定..etc）を行う必要があるのですが、いちいちサーバにSSH/RDPログイン&コマンド発行をしなければいけません。手間や時間がかかる上に、サイトのリニューアル後、台数も増えることが想定されています。どうしよう....

6



システム管理者

管理系サーバは追加で構築が必要になる可能性はありますか？



既存社員

サービスの規模が大きくなれば追加で構築が必要です。ただ、手作業でインストール作業を行なっているのでもう時間がかかります....

7



システム管理者

S3バケットを追加で作る場面もありそうですが、S3の「サーバ側暗号化機能」はシステム要件上、有効化が必須ですね。周知されていますか？



既存社員

はい。メンバーは認識しているはずですが、この前設定が漏れているサーバがあったので忘れてしまう場面はあるかもしれません....

8



システム管理者

アクセスの増加が見込まれる時間と処理能力の増強が必要なコンポーネントはありますか？



既存社員

TV CMやニュースサイトで紹介される予定で、毎日決まった時間帯に大幅なアクセス数の増加が見込まれていて、WEB-APP EC2の台数を増やす必要があります。私が手動でAMIを基に台数を増やす予定です。またアクセス増加の時間帯が終わったら手動でサーバを削除する予定です！

ヒアリング(3/3)

9



既存社員

S3にアップロードされたコンテンツですが、使わなくなったものを定期的に削除予定です。ただ、この間テスト作業を実施していたら、間違ったファイルを消しちゃったんです！まだ本番稼働してないので消えても大丈夫でしたが焦りました....

10



システム管理者

システムの運用や現状の課題についての情報共有はいつ行われていますか？



既存社員

特に行われていませんね...コレすごくまずいなって思った人がいたら都度チャットなどで共有されています。

11



既存社員

現在は本番用とテスト用の2つの環境のみです。ですが今後は、各開発者に自由に触れるAWSアカウントを個別に与えて、自分専用の環境上で開発を進めてもらいたいと思っています。ただ、開発者自身でVPC,ELB,EC2,RDS,IAMロールなど、一式の環境を作成するのは、かなり難しい&手間と思うのですが何か良い方法はありますか？

12



既存社員

システムのセキュリティを高めるために、何かできそうなことはありますか？
各サーバでセキュリティグループを使用する、パブリックサブネット、プライベートサブネットを使い分けることは意識しているのですが、他にもできそうなことがあれば...

ワークの進め方

個人ワーク（10 分）

課題を解釈し、運用の提案を考える

チームワーク（40 分）

役割を決めてディスカッションする

ファシリテータ：グループのディスカッションが円滑になるようサポートする

書記(全員)：提案内容と理由などを記録する

相互フィードバック（オプション）

自チームで作成した構成図について、発表をお願いします。

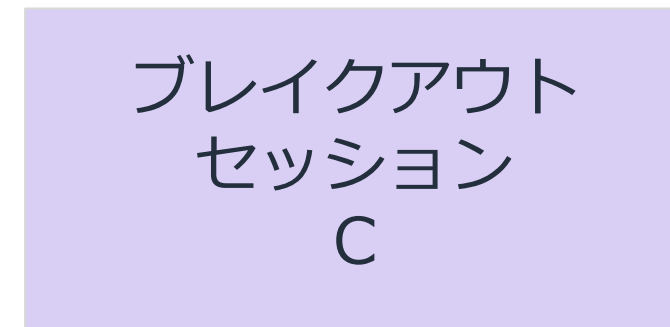
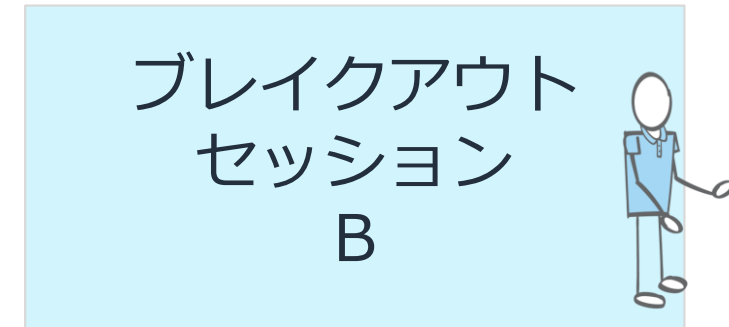
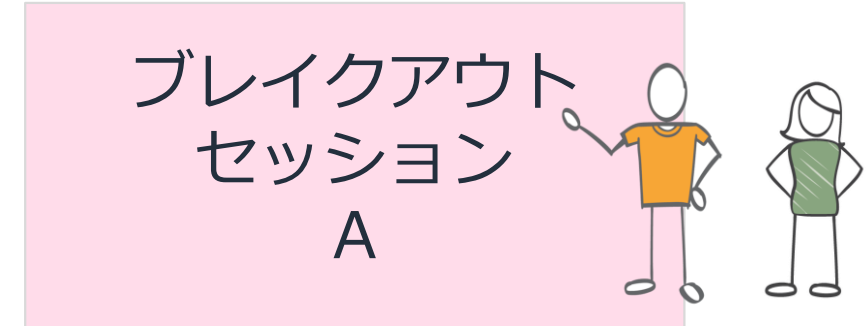
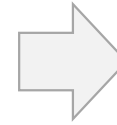
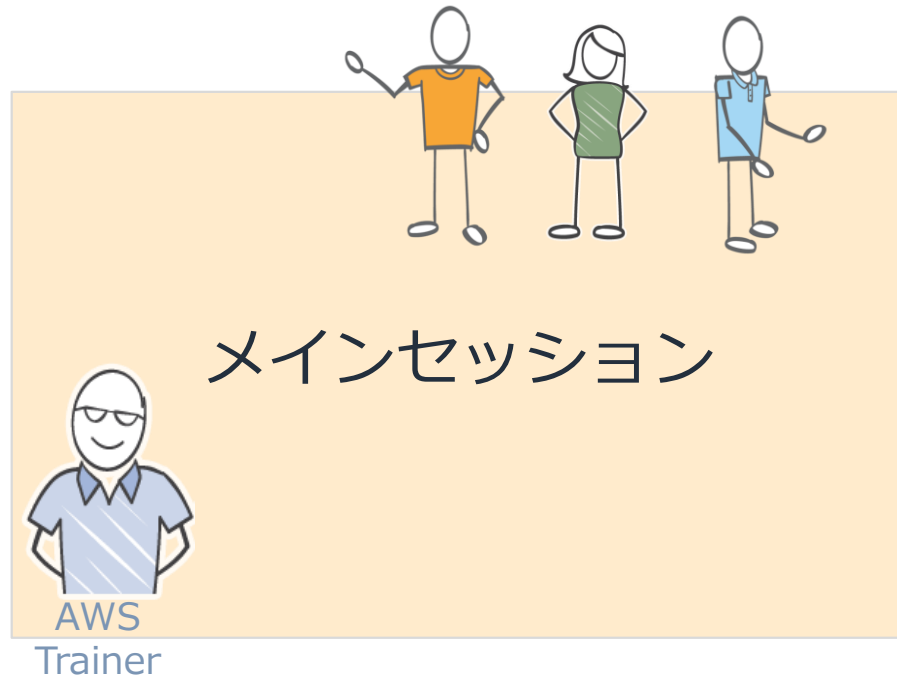
ほかの受講者は、質問や感想をお願いします。

ツールの使い方

Webex ブレイクアウトセッションの概要

投影のみ

ブレイクアウトセッションに移動して、
ディスカッション



終わったら戻れます

Webex ブレイクアウトセッションに参加

投影のみ

メインセッション



"参加者"
を表示

ブレイクアウトセッション

ブレイクアウトセッションは開始されています。参加するセッションを選択します。

- ▽ ブレイクアウトセッション 1 (0)
- ▽ ブレイクアウトセッション 2 (0)
- ▽ ブレイクアウトセッション 3 (0)
- ▽ ブレイクアウトセッション 4 (0)

参加
参加
参加
参加

参加するセッ
ションを選択

ブレイクアウトセッション



グループのメンバー
のみ参加

退出すると
メインセッションへ戻る

Webex ブレイクアウトセッションで対話

投影のみ

The screenshot shows a Webex Breakout Session window. At the top, the title bar reads "Webex ミーティング情報 ブレイクアウトセッション1 メニューバーを非表示にする ヘ". Below it is a menu bar with options: "ファイル(F) 編集(E) 共有(S) 表示(V) 音声とビデオ(A) 参加者(P) ミーティング(M) ブレイクアウトセッション(B) ヘルプ(H)". The main area is split into two video feeds: a grey one on the left labeled "AWS_Suzuki3" and a green one on the right. On the right side, there is a sidebar with a "参加者 (2)" (Participants 2) section. It contains a message: "あなたはブレイクアウトセッション1のセッションに接続されています。" (You are connected to the session 1 of the breakout session.), the session time "セッション時間: 10:57", and a link "他のブレイクアウトセッションを表示" (Show other breakout sessions). Below this is a search bar labeled "検索" (Search). The participant list shows two users: "AWS_Suzuki2" (自分, self) and "AWS_Suzuki3". At the bottom of the window is a toolbar with buttons: "ミュート" (Mute), "ビデオの停止" (Stop video), "共有" (Share), and icons for chat, help, and a red "X" button. Three pink annotations with arrows point to these buttons: "「ミュート解除」で音声会話出来ます" (You can have a voice conversation by unmute) points to the "ミュート" button; "ビデオを有効にして、お互いに顔を見ながら話すことを推奨" (We recommend enabling video and talking while looking at each other's faces) points to the "ビデオの停止" button; "グループ内だけのチャット" (Chat only within the group) points to the chat icon in the toolbar.

Webex ミーティング情報 ブレイクアウトセッション1 メニューバーを非表示にする ヘ

ファイル(F) 編集(E) 共有(S) 表示(V) 音声とビデオ(A) 参加者(P) ミーティング(M) ブレイクアウトセッション(B) ヘルプ(H)

AWS_Suzuki3

参加者 (2)

あなたはブレイクアウトセッション1のセッションに接続されています。

セッション時間: 10:57

[他のブレイクアウトセッションを表示](#) サポートを...

検索

AWS_Suzuki2
自分

AWS_Suzuki3

「ミュート解除」で音声会話出来ます

ビデオを有効にして、お互いに顔を見ながら話すことを推奨

グループ内だけのチャット

ミュート

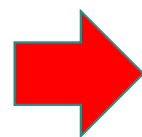
ビデオの停止

共有

チャット

Webex 画面共有する

投影のみ



コンテンツを共有

あなたが共有を開始すると、Tetsuo Nobe のコンテンツ共有が終了します。

キャンセル

共有

