

## CTC Engineer's Insight # 3

金融業界の実践知から学ぶ、クラウド×オンプレの運用最適解とセキュリティ戦略  
～ハイブリッドなインフラが必要な業界に活かせるノウハウ～

# クラウドリフト&シフトについて

伊藤忠テクノソリューションズ株式会社

金融技術第2部

高橋 英一

無限の未来と、幾千のテクノロジーをつなぐ。

**CTC Financial Services Group**

# 0. はじめに

自己紹介、本日のお話について。。。。

無限の未来と、幾千のテクノロジーをつなぐ。

## CTC Financial Services Group

# 0. はじめに

## 自己紹介

- 名前：高橋 英一
- 所属：伊藤忠テクノソリューションズ株式会社  
金融技術第2部
- 経歴：開発部でアプリ開発を担当（大型案件から維持保守まで手広く）  
PMO業務（超・大型案件のテスト分析やテスト推進）  
技術部に異動（大型更改案件から維持保守まで手広く）  
今に至る。。。
- 出身：神奈川県横浜市
- 趣味：日本酒（石川県珠洲の宗玄酒造さんを応援中）



無限の未来と、幾千のテクノロジーをつなぐ。

**CTC Financial Services Group**

# 0. はじめに

## ■ 本日つたえたいこと

- オンプレ、プライベートクラウド、AWSの違いと運用の勘所
- クラウド移行時に見落とされがちなポイントとその影響
- 『クラウド化』の誤解と、オンプレとのバランス
- AWSの可用性（稼働率99%以上）の誤解と、実際に発生し得るダウンタイムの影響

AWSへの移行するシステムはまだ多いです、  
本日のSessionがヒントになれば幸いです。

無限の未来と、幾千のテクノロジーをつなぐ。

**CTC Financial Services Group**

- 
1. オンプレ、プライベートクラウド、AWSの違いと運用の勘所
- 
2. クラウド移行時に見落とされがちなポイントとその影響
- 
3. 『クラウド化』の誤解と、オンプレとのバランス
- 
4. AWSの可用性（稼働率99%以上）の誤解と、実際に発生し得るダウンタイムの影響
- 
5. まとめ

無限の未来と、幾千のテクノロジーをつなぐ。

**CTC Financial Services Group**

# 1. オンプレ、プライベートクラウド、 AWSの違いと運用の勘所

無限の未来と、幾千のテクノロジーをつなぐ。

**CTC Financial Services Group**

# 1. オンプレ、プライベートクラウド、AWSの違いと運用の勘所

## ■ オンプレ

### メリット:

- ・ 物理的なセキュリティを完全に管理可能（データセンターの選定、アクセス制御）
- ・ レイテンシーが最小限で済む（オンプレ環境内での処理）
- ・ 規制・コンプライアンスに適合しやすい（特定の監査要件に対応しやすい）

### デメリット:

- ・ インフラの維持・更新コストが高い
- ・ スケーラビリティが低い（需要変動に柔軟に対応しにくい）

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

# 1. オンプレ、プライベートクラウド、AWSの違いと運用の勘所

## ■ プライベートクラウド

### メリット:

- ・ オンプレと同様にセキュリティを確保しつつ、ある程度のスケーラビリティを実現可能
- ・ 専用リソースを確保しやすく、他のクラウドユーザと分離できる

### デメリット:

- ・ クラウドのメリット（自動化、柔軟なリソース増減）を完全には享受できない
- ・ 運用の手間はオンプレとあまり変わらないこともある

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

# 1. オンプレ、プライベートクラウド、AWSの違いと運用の勘所

## AWS

### メリット:

- ・ スケールアウト・スケールインが容易 (Auto Scaling、Elastic Load Balancing)
- ・ マネージドサービスの活用で運用負荷を軽減可能 (RDS、Lambdaなど)
- ・ 災害対策や冗長性を低コストで実現しやすい (マルチAZ・マルチリージョン)

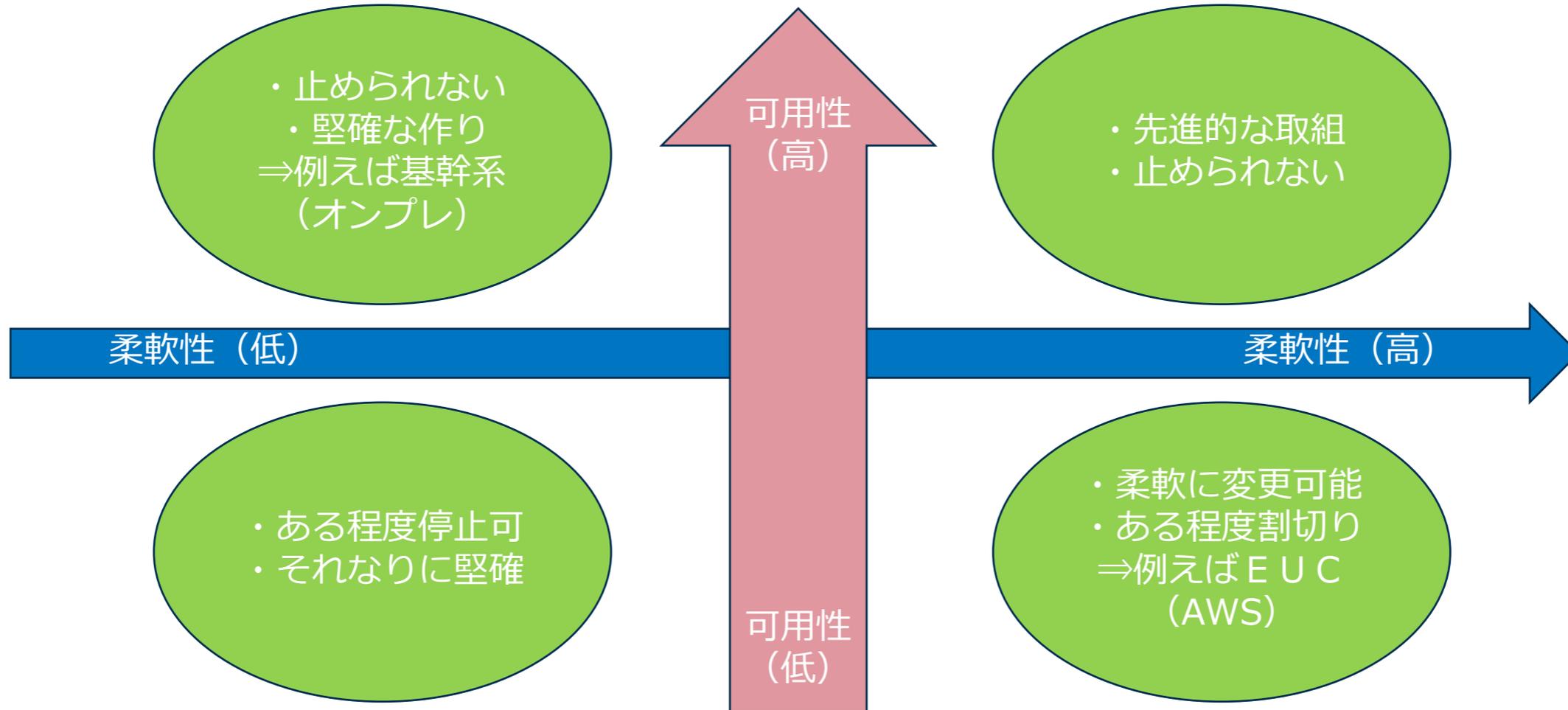
### デメリット:

- ・ コスト管理が難しい (リソース管理を怠ると予想外のコストになることも)
- ・ すべての規制に対応できるわけではなく、特定業界の厳格な基準ではオンプレ優勢
- ・ ネットワークレイテンシーの制御が難しい (Direct Connectなどが必要な場合あり)

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

# 1. オンプレ、プライベートクラウド、AWSの違いと運用の勘所



無限の未来と、幾千のテクノロジーをつなぐ。

## 2. クラウド移行時に見落とされがちな ポイントとその影響

無限の未来と、幾千のテクノロジーをつなぐ。

**CTC Financial Services Group**

## 2. クラウド移行時に見落とされがちなポイントとその影響

### ■ データ転送コスト

クラウドに移行したが、オンプレとのハイブリッド構成でデータ転送料が想定以上に増える  
(例：S3とオンプレのデータ同期)

### ■ IAM (Identity and Access Management) 設計

クラウドの権限管理を適切に設計しないと、不要なアクセス権限が広がる  
(特に金融業界では重要)

### ■ 可用性の誤解

クラウドサービスは落ちないという誤解 (後述)

### ■ 監査ログの管理

オンプレではSyslog中心だったが、クラウドではCloudTrailやGuardDutyなどを  
適切に設計する必要がある

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

## 2. クラウド移行時に見落とされがちなポイントとその影響

### 性能問題

クラウドに移行したが、移行前のオンプレやプライベートクラウドでの処理時間との乖離があり、パフォーマンス問題が露呈してその対応に追われまくる（ST後半やUATで初見だと致命的。。。）



- IT工程、可能であればもっと前の工程から、パフォーマンス測定を実施して、対応すべき
  - ⇒DBならSQLチューニング、DBのパラメータ変更によるチューニングなど
  - ⇒OSならI/Oスループット変更、EMRの利用による並列処理実行など追加費用が必要になるような変更もありえます

無限の未来と、幾千のテクノロジーをつなぐ。

### 3. 『クラウド化』の誤解と、 オンプレとのバランス

無限の未来と、幾千のテクノロジーをつなぐ。

**CTC Financial Services Group**

### 3. 『クラウド化』の誤解と、オンプレとのバランス

#### ■ 誤解1：クラウドに移せばすべてのコストが削減される

- 実際はオンプレと比べて運用コストは減るが、リソース利用量次第でインフラコストは増加することもある
- 例 EC2インスタンスを常時稼働させるより、サーバーレス（Lambda）に移行する方が効率的

#### ■ 誤解2：クラウドなら100%可用性が保証される

- クラウドでも障害は発生する
- 可用性を確保するにはマルチAZやマルチリージョンを考慮した設計が必須

#### ■ 誤解3：クラウドはセキュリティが弱い

- AWSのセキュリティ機能（VPC、IAM、KMSなど）を適切に使えばオンプレ以上に強固なセキュリティを実現可能
- 逆に設定ミス（S3のパブリック公開ミスなど）が発生しやすい

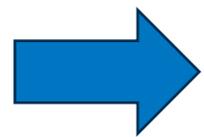
無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

### 3. 『クラウド化』の誤解と、オンプレとのバランス

#### ■ 誤解が解けたところで、、、

- AWSのコストはある程度試算可能なので、インフラコストを試算しておく
  - ⇒オンプレ、プライベートクラウドでも試算可能であるなら比較する
- 可用性は要求事項や要件をまとめる時に、どこまで必要かキッチリと詰めておく
  - ⇒完全に止めないシステムとなると、単独の環境の4倍程度にすぐなってしまうので割切る
- セキュリティーは一筋縄ではいかない
  - ⇒要件定義段階から堅固な作りを目指し、有識者などにも確認に入ってもらった方がよい



途中から予算が大きく上振れるのはかなり厳しい（金融系、公共・政府系などは特に）

無限の未来と、幾千のテクノロジーをつなぐ。

**CTC Financial Services Group**

## 4. AWSの可用性（稼働率99%以上）の誤解 と、実際に発生し得るダウンタイムの影響

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

## 4. AWSの可用性（稼働率99%以上）の誤解と、実際に発生し得るダウンタイムの影響

### AWSの代表的なSLA

- EC2のSLA : 99.99% (年間ダウンタイム約52分)
- RDSのSLA : 99.95% (年間ダウンタイム約4.3時間)
- S3のSLA : 99.9 % (年間ダウンタイム約8.76時間)

年間でみると、それなりに止まってしまう時間があることが前提

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

## 4. AWSの可用性（稼働率99%以上）の誤解と、 実際に発生し得るダウンタイムの影響

### 2019年8月23日のAWS東京リージョンにおけるAZ障害の詳細

#### 障害概要:

特定のAZで大規模な障害が発生。この障害により、該当AZ内で稼働していたEC2インスタンスやRDS（Relational Database Service）などのサービスが影響を受け、サービス停止や遅延がありました。

#### 障害原因:

具体的な原因はAWSから公式には公開されていませんが、一般的にAZ障害はサーバやネットワーク機器の物理的な故障が原因と考えられています。

#### 影響範囲:

特に、単一のAZに依存していたシステムはサービス停止となりました。また、マルチAZ構成を採用していた一部のユーザでも、ロードバランサーが正常に機能せず、トラフィックの切り替えが適切に行われないケースもあったとのこと。

無限の未来と、幾千のテクノロジーをつなぐ。

## 4. AWSの可用性（稼働率99%以上）の誤解と、 実際に発生し得るダウンタイムの影響

### 2017年3月1日：米国東部リージョンのS3サービス障害

#### 障害概要：

オペレーションミスにより、S3（Simple Storage Service）が利用不可となりました。

#### 障害原因：

通常メンテナンス作業中に、S3の多数のサーバーが誤ってシャットダウンされ、アクセス不能となりました。これにより、EBSスナップショットやLambdaなどの他のサービスにも影響が及びました。

#### 影響範囲：

Imgur、IFTTT、Zapier、Slack、Trelloなど、多くのサービスが影響を受けました。ダウンタイムは約5時間。

無限の未来と、幾千のテクノロジーをつなぐ。

**CTC Financial Services Group**

## 4. AWSの可用性（稼働率99%以上）の誤解と、 実際に発生し得るダウンタイムの影響

### 2016年6月4日：アジアパシフィックリージョンのEC2サービス障害

#### 障害概要：

豪雨による停電が発生し、EC2（Elastic Compute Cloud）インスタンスが利用不可となりました。

#### 障害原因：

豪雨により電力供給が不安定となり、UPS（無停電電源装置）への切り替え時に異常な電圧低下が発生。これにより、多数のEC2インスタンスが停止しました。

#### 影響範囲：

シドニーリージョン内の複数のサービスが影響を受けました。ダウンタイムは約1.5時間。

## 4. AWSの可用性（稼働率99%以上）の誤解と、 実際に発生し得るダウンタイムの影響

### 2015年9月20日：米国東部リージョンのDynamoDBサービス障害

#### 障害概要：

新機能追加に伴い、DynamoDBが利用不可となりました。

#### 障害原因：

DynamoDBにグローバルセカンダリインデックス（GSI）機能が追加され、ユーザ数が想定を上回ったことで、内部メタデータが急増。これにより、メタデータのパーティショニングが発生し、DynamoDBのエラー率が増加しました。

影響範囲：Netflix、Redditなどの主要サービスが影響を受けました。ダウンタイムは約5時間。

無限の未来と、幾千のテクノロジーをつなぐ。

**CTC Financial Services Group**

## 4. AWSの可用性（稼働率99%以上）の誤解と、実際に発生し得るダウンタイムの影響

### 2012年12月24日：米国東部リージョンのELBサービス障害

障害内容：

オペレーションミスにより、ELB（Elastic Load Balancing）が利用不可となりました。

障害下人：

オペレーションミスにより、ELBの設定に問題が生じ、サービスが利用不可となりました。

影響範囲：

複数のサービスが影響を受けました。詳細なダウンタイムの時間は報告されていませんが、数時間程度にわたる影響があったとされています。

無限の未来と、幾千のテクノロジーをつなぐ。

**CTC Financial Services Group**

## 5. まとめ

無限の未来と、幾千のテクノロジーをつなぐ。

**CTC Financial Services Group**

## 5. まとめ

- 規制や運用面でオンプレ、プライベートクラウド、AWSの使い分けが重要  
(特に規制が厳しい業界は注意が必要)
- クラウド移行時には、コスト・ネットワーク・権限管理・性能などの落とし穴に注意
- 「クラウド化=完全なコスト削減」や「AWSは絶対に落ちない」といった誤解に注意
- AWSの99.99%可用性を過信せず、設計でダウンタイムを最小限にする検討は必須

⇒実際に、HW障害で自動でAZ切替が起こったりすることはそれなりにあります。

無限の未来と、幾千のテクノロジーをつなぐ。

**CTC Financial Services Group**

無限の未来と、  
幾千のテクノロジーをつなぐ。

# CTC Financial Services Group

