



ある日「DRやって？」と言われたら

開発・運用現場が始める DR の第一歩

2023年11月16日

エムオーテックス株式会社 サービス開発1部

立古 佳大

立古 佳大
りゅうご よしひろ

エムオーテックス株式会社
開発本部 サービス開発1部 サービス開発1課 SREグループ

業務:

LANSCOPE Endpoint Manager クラウド版
SRE業務
コンプライアンス対応業務
PSIRT

(過去には開発業務、オンプレミス製品の担当業務も)

AWS認定資格:

AWS Certified Solutions Architect - Professional
AWS Certified DevOps Engineer - Professional
AWS Certified Security - Specialty
AWS Certified Advanced Networking - Specialty



会社概要

会社名	エムオーテックス株式会社 (MOTEX)
代表取締役社長	宮崎 吉朗
設立	1990年7月
従業員数	413名 (2022年4月現在)
株主	京セラコミュニケーションシステム株式会社 (2012年から資本参加)
事業内容	自社製品の開発・販売、サイバーセキュリティのコンサルティング・ソリューション導入・運用監視サービス

拠点

本社	大阪市淀川区西中島5-12-12 エムオーテックス新大阪ビル
東京本部	東京都港区三田 3-5-19 住友不動産東京三田ガーデンタワー 22階
名古屋支店	名古屋市中区錦1-11-11 名古屋インターシティ 3F
九州営業所	福岡市博多区博多駅前1-15-20 NMF博多駅前ビル2階
長崎 Innovation Lab	長崎県長崎市出島町1-41 クレインハーバー長崎ビル3F

“LANSCOPE”を通して、お客様の“Secure Productivity”（安全と生産性向上の両立）を支援

統合エンドポイント管理



Endpoint Manager

組織のIT資産管理・内部不正対策・ウイルス対策をオールインワンでカバーします。発売当初からご提供している「オンプレミス版」に加え、スマホ管理が可能な「クラウド版」も提供しており、国内2万社を超えるお客様にご利用いただいています。

AI アンチウイルス



Cyber Protection

AI を活用したアンチウイルスで、既知のマルウェアはもちろん、未知・亜種のマルウェアからもデバイスを防御します。高性能な AI アンチウイルス「CylancePROTECT」や「Deep Instinct」を、MOTEX の安心サポートと共に提供するマネージドサービスです。

クラウドセキュリティ監査

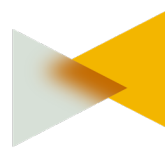


Security Auditor

Microsoft 365 の監査ログを収集し、利用状況の見える化や、情報漏洩などのインシデントにつながる操作の

把握を可能とします。また、レビュープラットフォーム「ITreview」では、サービスデスク・インシデント管理の部門でLeaderを獲得するなど、お客様からも高い評価をいただいています。

リモートサポート・ヘルプデスク



Remote Desktop

遠隔地にあるサーバーや PC・スマホへの「リモート操作」や「画面共有」を可能とする組織向けのリモートコント

ロールツールです。Windows・macOS・iOS・Android に対応しています。

セキュリティ診断・ソリューション



Professional Service

サイバーセキュリティのさまざまな領域に対し、セキュリティプロフェッショナルの知見を活かした「セキュリティ診

断」と「セキュリティ製品・ソリューション」で、巧妙化するサイバー攻撃などのリスクから組織を守ります。

クラウド版 の提供開始から10年以上。安心の実績でデバイス管理を支援します。

サービス提供実績

導入実績 **9,000** 社

サービス提供 **10年** 以上

2012年よりサービス提供開始。
以来 9,000 社以上のお客様に導入。

顧客満足度No.1



運用管理・仮想化ソフト/サービス
(クライアント)部門

エムオーテックスとして
日経コンピュータ 2023 年 8 月 31 日号
顧客満足度調査 2023-2024
運用管理・仮想化ソフト/サービス
(クライアント) 部門1位を獲得

安心のサービス提供基盤



基盤に採用している AWS の認定、
クラウドサービスに関するガイドライン
規格の ISO27017 を取得。

本日のアジェンダ

DRって何から始めたらいいの？ という開発・運用担当者の皆様へ



DR対策の具体化



具体的な施策の実施



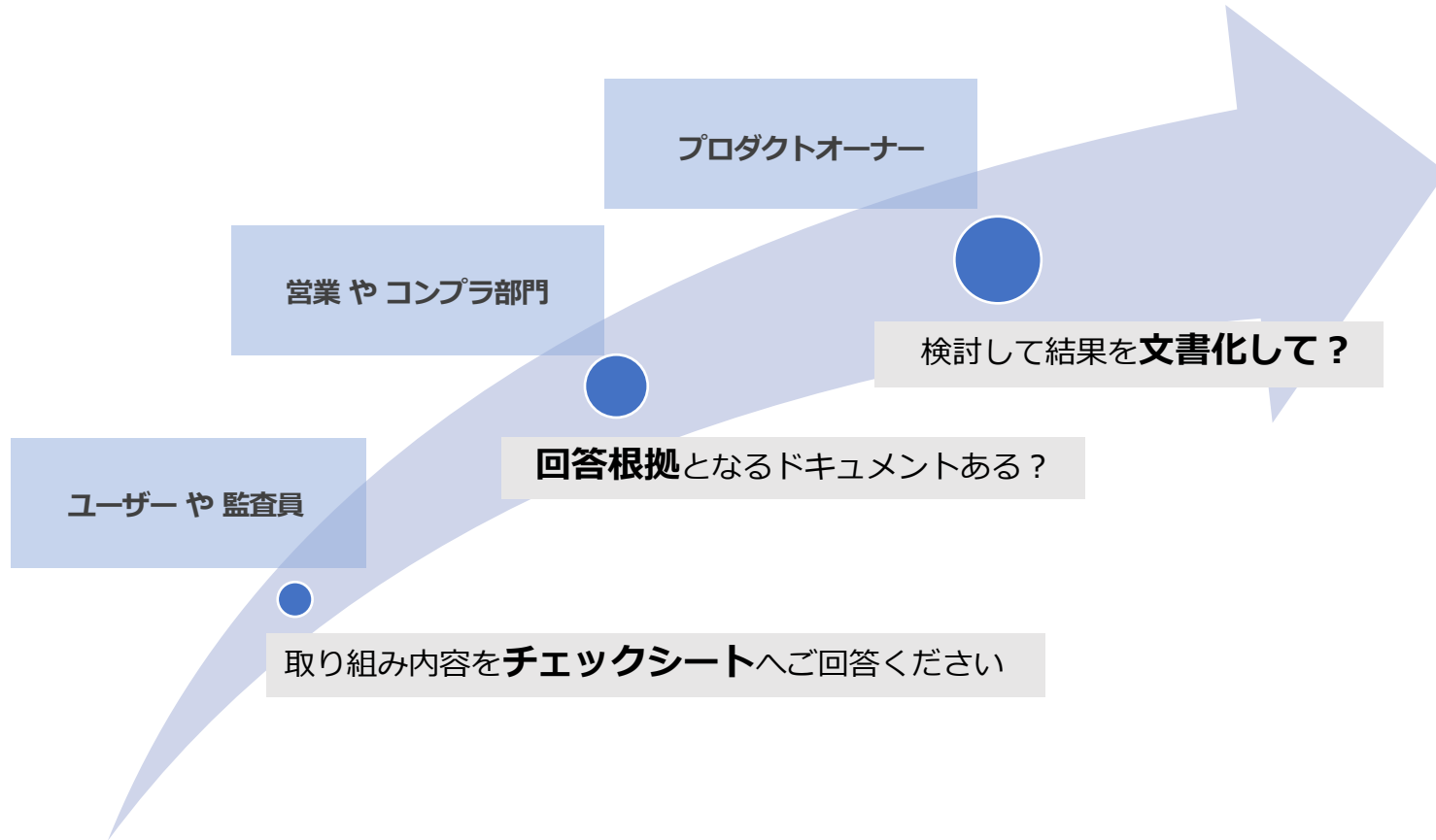
DR制定後の動き

なぜ開発・運用現場が？

開発でやってくれとは言われるんだけど…やるべきことが**具体的に**ならない



要求：「適切な対策を検討して文書化しなさい」



「検討」って何を？

なぜ開発・運用現場が？

開発でやってくれと言われるんだけど…やるべきことが具体的ににならない



要求：「適切な対策を検討して文書化しなさい」

具体的なところは内部の設計にもよるし、結果を文書化して？

開発現場でうまいこと考えてよ…

ユーサ

取り組み内容のチェックシートへて回答ください



「検討」って何を？

DR対策を具体化するには

ここから始めましょう



プロダクトの**ゴール**を定める

DR で守らなくてはいけないものは何か、はっきりさせる。



外部のベンチマークを活用する

自社内だけで悩まず、客観的なアドバイスを参照する。

「プロダクト」を「社内システム」等へ読み替えていただいてもOK

プロダクトのゴールを定める

SLO/RTO/RPO を決めてみましょう



SLO (Service Level Objective: **サービスレベル目標**)

例えば: 月間の **ダウン時間は 10分以内** に抑える



RTO (Recovery Time Objective: **目標復旧時間**)

例えば: 災害によるデータベース破損時は **2時間以内に復旧作業完了** する



RPO (Recovery Point Objective: **目標復旧地点**)

例えば: 災害によるデータベース破損時は **過去1時間以内のデータ** へ切り戻す

さらに、
RLO(Recovery Level Objective: **目標復旧レベル**)を入れてもOK

SLO/RTO/RPO を決めてみましょう

👉 SLO/RTO/RPO を議題に据えると、ステークホルダーから**具体的要求**がどんどん出てきます。



SLO/RTO/RPO を決めてみましょう

👉 SLO/RTO/RPO を議題に据えると、ステークホルダーから**具体的な要求**がどんどん出てきます。



外部のベンチマークを活用する

自社で考えても煮詰まるなら **外部** に手掛かりを求めてみましょう



AWS Trusted Advisor

AWS が DR をはじめとした **推奨対応** を教えてくれる！



外部のセキュリティ認証規格

セキュリティ要求事項の一角として、DR 対応が含まれていることも

社内検討に留まらず
客観的な情報を活用



Trusted Advisor × [Trusted Advisor](#) > 耐障害性

耐障害性

すべてのチェックを更新 | すべてのチェックをダウンロード

チェック名を選択すると、AWS アプリケーションの可用性と冗長性を高めるための推奨事項が表示されます。Trusted Advisor では、Auto Scaling、ヘルスチェック、複数のアベイラビリティゾーン、バックアップ機能などのリソースの使用を推奨する場合があります。

概要

0 推奨されるアクション 情報	3 調査が推奨されます 情報	32 問題が検出されなかったチェック項目 情報	0 除外された項目があるチェック 情報
-----------------------	----------------------	-------------------------------	---------------------------

▼ 詳細設定
Trusted Advisor を管理
通知

aws

製品 ソリューション 料金 ドキュメント 学ぶ パートナーネットワーク AWS Marketplace カスタマーサポート イベント さらに詳しく見る

AWS サポート サポートプラン テクノロジーとプログラム 料金 リソース ナレッジセンター よくある質問 お客様

AWS Trusted Advisor

コストを削減、パフォーマンスを向上、セキュリティを強化

[AWS Trusted Advisor を始めましょう](#) [ステップバイステップガイド](#)

AWS Innovate 登録開始！モダンアプリ開発と運用の最新手法を 4 時間で学ぶ - 10/26 (木) 開催 [今すぐ登録 >](#)

AWS Trusted Advisor は、お客様が AWS のベストプラクティスをフォローするためのレコメンデーションを提供いたします。Trusted Advisor は、チェックを使ってお客様のアカウントを評価します。これらのチェックは、お客様の AWS インフラストラクチャを最適化し、セキュリティとパフォーマンスを向上し、コストを削減し、サービスをモニタリングします。そしてレコメンデーションに従って、サービスやリソースを最適化することができます。

AWS ベーシックサポートと [AWS デベロッパーサポート](#) をご利用のお客様は、コアセキュリティチェックとサービスオータチェックにアクセスできます。 [AWS ビジネスサポート](#) と [AWS エンタープライズサポート](#) にご契約のお客様は、すべてのチェック (コスト最適化、セキュリティ、耐障害性、パフォーマンス、サービスの範囲など) と推奨事項にアクセスできます。チェックの一覧と説明については、 [Trusted Advisor Best Practices](#) をご覧ください。

[AWS Trusted Advisor の使用を開始する方法 \(11:45\)](#)

実際のリソースを見て 推奨事項を教えてくれる！

耐障害性の **課題となりそうな設定** を改善提案してくれる

Trusted Advisor

優先度

- レコメンデーション
- コスト最適化
- パフォーマンス
- セキュリティ
- 耐障害性**
- サービスの制限

Engage

▼ 詳細設定

- Trusted Advisor を管理
- 通知

Amazon S3 バケットバージョンニング

最終更新: 5分前

バージョンニングが有効化されていない、またはバージョンニングが停止されている Amazon Simple Storage Service バケットをチェックします。バージョンニングを使用すると、意図しないユーザーアクションとアプリケーション障害の両方から簡単に復旧することができます。バージョンニングは、バケットに保存された任意のオブジェクトの任意のバージョンを保存、取得、および復元できるようにします。Glacier ストレージクラスへのオブジェクトのアーカイブ、または指定された期間後のオブジェクトの削除を自動的に行うことによって、オブジェクトの全バージョン、およびそれらに関連するコストを管理するために、ライフサイクルルールを使用することができます。オブジェクトの削除、またはバケットへの設定変更に対して Multi-Factor Authentication (MFA) を義務付けることも選択できます。

バージョンニングを有効にした後で無効化することはできませんが、停止することは可能です。停止することによって、オブジェクトの新しいバージョンの作成が阻止されます。バージョンニングの使用は、オブジェクトの複数バージョンのストレージに料金を支払うことになるため、Amazon S3 のコストを増加させる場合があります。

アラート基準

緑: バケットでバージョンニングが有効化されています。
Yellow: バケットでバージョンニングが有効化されていません。
Yellow: バケットでバージョンニングが停止されています。

推奨されるアクション

過失による削除または上書き防くため、ほとんどのバケットでバケットバージョンニングを有効化します。「[バージョンニングの使用](#)」、および [プログラムを使用したバージョンニングの有効化](#) について参照してください。

バケットバージョンニングが停止されている場合は、バージョンニングの再有効化を検討します。バージョンニングが停止されたバケットでのオブジェクトの取扱いについての情報は、「[バージョンニングが停止されたバケットのオブジェクトを管理する](#)」を参照してください。

バージョンニングが有効化または停止されている場合、所定のオブジェクトバージョンを有効期限切れとしてマークする、または不必要なオブジェクトバージョンを恒久的に削除するためのライフサイクル設定ルールを定義できます。詳細については、「[オブジェクトのライフサイクル管理](#)」を参照してください。

MFA Delete では、バケットのバージョンニングステータスが変更される、またはオブジェクトのバージョンが削除されるときに、追加の認証が必要になります。ユーザーには、認証情報と、承認された認証デバイスからのコードの入力が求められます。詳細については、「[MFA Delete](#)」を参照してください。

追加のリソース

[S3 バケットの作成と設定](#)

Amazon S3 バケットバージョンニング (1)

1個のバケットのうち1個でバージョンニングが有効化されていないかバージョンニングが停止されています。

非表示 & 更新 表示可能な項目 ▼

< 1 > ⚙️

<input type="checkbox"/>	リージョン ▼	バケット名 ▼	バージョンニング ▼	MFA Delete 有効 ▼	ステータス ▼
<input type="checkbox"/>			有効化されていない		⚠️

客観的な指摘事項 = 説得力



思ってもみなかった 観点への気づきも

Trusted Advisor

レコメンデーション
コスト最適化
パフォーマンス
セキュリティ
耐障害性
サービスの制限
Engage

詳細設定
Trusted Advisor を管理
通知

▼ ⚠ NAT ゲートウェイ AZ インディペンデンス

NAT ゲートウェイがアベイラビリティゾーン (AZ) インディペンデンスに設定されているかどうかをチェックします。

アラート基準

赤色: ある AZ 内のサブネットからのトラフィックが、別の AZ 内の NATGW を経由してルーティングされています
緑色: ある AZ 内のサブネットからのトラフィックが、同じ AZ 内の NATGW を経由してルーティングされています

推奨されるアクション

サブネットの AZ を確認して、同じ AZ の NAT ゲートウェイを経由してトラフィックをルーティングしてください。
AZ に NATGW がない場合は、NATGW を作成してから、それを経由してサブネットにトラフィックをルーティングします。

その他のリソース

以下の AWS 公開ドキュメントを参照してください。

- [NAT ゲートウェイの作成](#)
- [ハブの概念を使用し、NAT ゲートウェイのさまざまなユースケースに応じてルートを設定する方法](#)
- [AWS サポートに問い合わせで追加のサポートを得る](#)

NAT ゲートウェイ AZ インディペンデンス (6)
2 / 6 のリソースが、このチェックでフラグが付けられました。

<input type="checkbox"/>	ステータス	リージョン	NAT アベイラビリティゾーン	サブネットアベイラビリティゾーン
<input type="checkbox"/>	⚠	ap-northeast-1	apne1-az4	apne1-az1
<input type="checkbox"/>	⚠	ap-northeast-1	apne1-az1	apne1-az4
<input type="checkbox"/>	✔	ap-northeast-1	apne1-az2	apne1-az2

ネットワーク経路 の冗長化
忘れがち



耐障害性の課題となりそうな設定を改善提案してくれる … 採用するかは自社のポリシー次第

The screenshot shows the AWS Trusted Advisor interface. On the left is a navigation menu with categories like '優先度' (Priority), 'レコメンデーション' (Recommendations), 'コスト最適化' (Cost Optimization), 'パフォーマンス' (Performance), 'セキュリティ' (Security), '耐障害性' (High Availability), 'サービスの制限' (Service Limits), 'Engage', '詳細設定' (Advanced Settings), 'Trusted Advisor を通知' (Notify Trusted Advisor), and '通知' (Notifications). The main content area displays a warning for 'Amazon S3 バケットバージョンニング' (Amazon S3 bucket versioning). The warning text explains that versioning is not enabled or is disabled for some buckets, which can lead to data loss and application downtime. It describes how versioning allows for easy recovery and provides features like MFA Delete and lifecycle rules. Below the text is a table with one entry for a bucket where versioning is not enabled.

リージョン	バケット名	バージョンニング	MFA Delete 有効	ステータス
		有効化されていない		⚠️



このバージョンニングは RPO1時間 に必要？

 提案を採用するか判断に SLO/RTO/RPOが必要！

例えば: **AWS Foundational Technical Review (FTR)** も活用できる

Item ID	Requirement	Compliance Status	Notes
DR-001	Define a Recovery Point Objective (RPO) according to your organizational needs.	Compliant	定義が適切に設定されています。RPOは「業務継続性」に基づいて決定されています。
DR-002	Define a Recovery Time Objective (RTO) according to your organizational needs.	Compliant	定義が適切に設定されています。RTOは「業務継続性」に基づいて決定されています。
DR-003	Provide your RPO or 'Recovery Point' column of the assessment template.	Compliant	レポートに適切に記載されています。
DR-004	Define a Recovery Time Objective (RTO) to meet business needs and operations. This should be on the order of minutes for all components that are critical for providing service to your customers, but should never exceed 24 hours. Recovery Time Objective (RTO) defines your tolerance for downtime. The RTO requirement is for the RTO to be no less than 24 hours for critical components providing service to customers.	Compliant	RTOは「業務継続性」に基づいて決定されています。RTOは24時間を超えてはなりません。
DR-005	Recovery Time Objective (RTO) defines your tolerance for downtime. The RTO requirement is for the RTO to be no less than 24 hours for critical components providing service to customers.	Compliant	RTOは「業務継続性」に基づいて決定されています。RTOは24時間を超えてはなりません。
DR-006	Provide your RTO or 'Recovery Point' column of the assessment template.	Compliant	レポートに適切に記載されています。
DR-007	Perform testing.	Compliant	テストが適切に実施されています。
DR-008	Test regularly to ensure that RPO and RTO are met, and periodically increment and test and after major updates. The test plan must include restoration data loss, restore, and availability tests and should be tested and verified for the RPO and RTO requirements must be completed prior to RPO testing.	Compliant	テストが適切に実施されています。RPOとRTOの要件を満たす必要があります。
DR-009	Provide the test log and test or 'Recovery Point' column of the assessment template.	Compliant	レポートに適切に記載されています。

The screenshot shows the AWS Foundational Technical Review (FTR) page. It features the AWS logo at the top left, navigation links for 'お問い合わせ', 'サポート', '日本語', 'アカウント', and 'コンソールにサインイン' at the top right. Below the navigation is a search bar and a list of links: '製品', 'ソリューション', '料金', 'ドキュメント', '学ぶ', 'パートナーネットワーク', 'AWS Marketplace', 'カスタマーサポート', 'イベント', 'さらに詳しく見る'. The main heading is 'AWS パートナーになるには' followed by 'AWS ファンデーションルテクニカルレビュー'. Below this is the sub-heading 'AWS パートナーによる AWS を利用したソフトウェアの評価の実現'. There are two call-to-action buttons: 'AWS パートナーネットワークに参加する >>' and 'APN アカウントをお持ちですか? ログイン >>'. The main content area contains a detailed description of the FTR, stating that it is used to assess the security and availability of SaaS solutions. It mentions that FTR is a free, 2-year valid service that helps reduce risk and improve security. The text is followed by three columns of benefits: 'リスクの緩和', 'セルフサービスプロセス', and 'パートナーの特典へのアクセス'. The 'リスクの緩和' column states that FTR is defined by the AWS Well-Architected Framework and helps reduce risk by adopting best practices. The 'セルフサービスプロセス' column states that FTR is a self-service process that allows partners to assess their solutions. The 'パートナーの特典へのアクセス' column states that FTR provides access to various AWS partner benefits, including the AWS ISV Accelerate Program. The '「Reviewed by AWS」バッジの獲得' column states that partners who pass the FTR can earn the 'Reviewed by AWS' badge, which is a valuable asset for their business.

<https://aws.amazon.com/jp/partners/foundational-technical-review/>

利用するAWSサービスによって 対応パターンが変わってきます

👉 フルマネージド

👉 自動化可能

👉 要手動メンテナンス

クラウドって
全部おまかせじゃないの？



本当の意味でクラウド任せできるサービス: 例えば **Amazon S3** や **Amazon DynamoDB**

aws お問い合わせ サポート 日本語 アカウント [コンソールにサインイン](#)

製品 ソリューション 料金 ドキュメント 学ぶ パートナーネットワーク AWS Marketplace カスタマーサポート イベント さらに詳しく見る

Amazon S3 [概要](#) [特徴](#) [ストレージクラス](#) [料金](#) [セキュリティ](#) [リソース](#) [よくある質問](#)

Amazon S3

どこからでも簡単に、お好みの量のデータを取得できるオブジェクトストレージ

[Amazon S3 の使用を開始](#) [Amazon S3 スペシャリストに連絡する](#)

5 GB の S3 Standard ストレージ
(AWS 無料利用枠 12 か月間)

- 99.999999999% (11 9s) のデータ耐久性で、変動するニーズに合わせてストレージリソースをスケールします。
- Amazon S3 のストレージクラスにまたがってデータを保存することで、先行投資やハードウェアの更新サイクルなしにコストを削減できます。
- 卓越したセキュリティ、コンプライアンス、および監査機能により、データを保護します。
- 堅牢なアクセスコントロール、柔軟なレプリケーションツール、組織全体の可視性により、あらゆる規模のデータを容易に管理できます。

<https://aws.amazon.com/jp/s3/>

クラウド特有の サービスに限定される傾向



オンプレミスを踏襲した設計では
利用困難なシーンも



Key-value ってなに??

The screenshot shows the AWS website page for Amazon DynamoDB features. The page is in Japanese and includes the following sections:

- 無限のスケラビリティを備えたサーバーレスのパフォーマンス**
 - Key-value およびドキュメントデータモデル**

Amazon DynamoDB では Key-value およびドキュメントデータモデルのいずれもサポートされています。NoSQL データベースである Amazon DynamoDB には柔軟なスキーマがあるため、各項目にさまざまな属性を持たせることができます。柔軟なスキーマにより、ビジネス要件の変化に合わせて、簡単に対応させることができます。リレーショナルデータベースと同様にテーブルスキーマを再定義する必要はありません。
 - ゼロまでスケールできるサーバーレス**

Amazon DynamoDB には、プロビジョニングやパッチ、管理用のサーバーだけでなく、インストール、メンテナンス、または運用するソフトウェアもありません。Amazon DynamoDB にはバージョン (メジャー、マイナー、パッチ) がなく、メンテナンスウィンドウもありません。また、Amazon DynamoDB はダウンタイムなしのメンテナンスを提供します。Amazon DynamoDB のオンデマンド料金体系は従量制料金で、ゼロまでスケールでき、自動的にテーブルをスケールして容量を調整し、管理なしでパフォーマンスを維持できます。
 - ACID トランザクション**

Amazon DynamoDB は、複雑なビジネスロジックを必要とするアプリケーションの不可分性、一貫性、独立性、永続性 (ACID) トランザクションのサポートなど、ミッションクリティカルなワークロード向けに構築されています。Amazon DynamoDB は、トランザクション向けにサーバー側のネイティブサポートを提供しているため、テーブル内およびテーブル間の複数の項目を調整したり、変更しないといった、開発者のエクスペリエンスを簡素化します。

Amazon DynamoDB はトランザクションあたり 100 のアクションをサポートするようになり、開発者の生産性が向上しました。トランザクションのサポートにより、開発者は、Amazon DynamoDB のスケール、パフォーマンス、およびエンタープライズの利点を、より広範なミッションクリティカルなワークロードにスケールすることができます。
 - グローバルテーブルによるアクティブ/アクティブレプリケーション**

Amazon DynamoDB グローバルテーブルでは、99.999% の可用性で、選択した AWS リージョン間にデータをアクティブ/アクティブ

<https://aws.amazon.com/jp/dynamodb/features/>

作ってさえしまえば サービス側に任せることができる: 例えば Amazon EC2

aws お問い合わせ サポート 日本語 アカウント [コンソールにサインイン](#)

製品 ソリューション 料金 ドキュメント 学ぶ パートナーネットワーク AWS Marketplace カスタマーサポート イベント さらに詳しく見る

Amazon EC2 [概要](#) [特徴](#) [料金](#) [インスタンスタイプ](#) よくある質問 [開始方法](#) [リソース](#)

Amazon EC2

事実上すべてのワークロードに対応するセキュアでサイズ変更が可能なコンピューティング性能

[Amazon EC2 の使用を開始](#) [Amazon EC2 スペシャリストに連絡する](#)

信頼性が高く、スケーラブルなオンデマンドのインフラストラクチャにアクセスできます。99.99% の可用性の SLA コミットメントにより、数分で容量をスケールできます。

アプリケーションのセキュアなコンピューティングを提供します。セキュリティは、AWS Nitro System によって Amazon EC2 の基盤に組み込まれています。

AWS Graviton ベースのインスタンス、Amazon EC2 スポットインスタンス、および AWS Savings Plans などの柔軟なオプションで、パフォーマンスとコストを最適化します。

AWS 移行ツール、AWS マネージドサービス、または Amazon Lightsail を使用して、アプリケーションの移行と構築を簡単に行うことができます。AWS がサポートできることをご覧ください。

Amazon Elastic Compute Cloud (Amazon EC2) は、極めて幅広い、詳細な機能を提供するコンピューティングプラットフォームを提供します。また、ロックロ

<https://aws.amazon.com/jp/ec2/>

Amazon EC2 Auto Scaling を適切に設計すれば、サービス側に任せることができる。

The screenshot shows the Amazon EC2 Auto Scaling console. The breadcrumb navigation is "EC2 > Auto Scaling グループ > [Redacted] AutoScalingGroup-[Redacted]". The main title is "[Redacted] AutoScalingGroup-[Redacted]". There are tabs for "詳細", "アクティビティ", "オートスケーリング", "インスタンス管理", "モニタリング", and "インスタンスの更新". The "グループの詳細" section shows:

Auto Scaling グループ名	希望するキャパシティ	ステータス
[Redacted] AutoScalingGroup-[Redacted]	3	-
作成日	最小キャパシティ	
Tue Mar 02 2021 18:12:57 GMT+0900 (日本標準時)	3	
	最大キャパシティ	
	3	

The "起動設定" section is partially visible at the bottom.

勝手に復旧してくれる！

The screenshot shows the "アクティビティ履歴 (56)" section. There is a search bar with the text "Q アクティビティ履歴をフィルタリングする". Below is a table with columns "ステータス", "説明", and "原因".

ステータス	説明	原因
成功	Launching a new EC2 instance: i-[Redacted]	At 2023-[Redacted]Z an instance was launched in response to an unhealthy instance needing to be replaced.
成功	Terminating EC2 instance: i-[Redacted]	At 2023-[Redacted]Z an instance was taken out of service in response to an EC2 health check indicating it has been terminated or stopped.

設計時点で考慮しておかなければならないことも



処理における文脈依存の排除 (べき等化)



アベイラビリティゾーンの定義・ネットワーク経路設計



ヘルスチェックの方法・タイミング

ヘルスチェックの設定				編集
プロトコル HTTP	パス [REDACTED]	ポート [REDACTED]	正常のしきい値 2ヘルスチェックの連続的な成功	
非正常のしきい値 10ヘルスチェックの連続的な失敗	タイムアウト 15秒	間隔 30秒	成功コード 200-499	

例えば Amazon Relational Database Service (RDS) … オンプレミス時代のハードウェア保守管理作業などは取り除けるが

<https://aws.amazon.com/jp/rds/>

非常時には人の手を介する必要があるシーンも: **手順書 訓練** ...

Amazon RDS

- ダッシュボード
- データベース
- クエリエディタ
- Performance insights
- スナップショット
- Amazon S3 ヘクスポート
- 自動バックアップ
- リザーブドインスタンス
- プロキシ

- サブネットグループ
- パラメータグループ
- オプショングループ
- カスタムエンジンバージョン
- ゼロの ETL 統合 [新規](#)

- イベント
- イベントサブスクリプション

レコメンデーション **11**

バックアップ

自動バックアップ 有効 (7 日)	最も早い復元可能な時刻 September 08, 2023, [REDACTED]	最も遅い復元可能な時刻 September 15, 2023, [REDACTED]
スナップショットにタグをコピー 無効		バックアップウィンドウ [REDACTED]

バックトラック

バックトラックウィンドウ
無効

スナップショット (7)

復元 削除 スナップショットの取得

Q フィルター条件 スナップショット

スナップショット名	スナップショットの作成時刻	ステータス	スナップショットのタイプ	スナップショットデータベース時間
<input checked="" type="checkbox"/> rds:[REDACTED] 2023-09-08-[REDACTED]	September 09, 2023, [REDACTED]	✔ 利用可能	自動	-
<input type="checkbox"/> rds:[REDACTED] 2023-09-09-[REDACTED]	September 10, 2023, [REDACTED]	✔ 利用可能	自動	-
<input type="checkbox"/> rds:[REDACTED] 2023-09-10-[REDACTED]	September 11, 2023, [REDACTED]	✔ 利用可能	自動	-
<input type="checkbox"/> rds:[REDACTED] 2023-09-11-[REDACTED]	September 12, 2023, [REDACTED]	✔ 利用可能	自動	-

データ破損が疑われますが
いつ時点で切り戻しますか?



非常時には人の手を介する必要があるシーンも: **手順書 訓練** ...

Amazon
ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)

ダッシュボード
データベース
クエリエディタ
パフォーマンス
スナップショット
Amazon
自動バックアップ
リザーブ
プロキシ

サブネット
パラメータグループ
オプション
カスタム
ゼロの
イベント
イベント
レコメン

1. 新しいDBクラスター/インスタンスを自動バックアップから起動する
2. Route53の [redacted]
3. 復元状況を確認する
4. 当日集計レポートデータがRDSに登録されているか確認
5. 4. で登録されていない場合は [redacted]
6. 新しいDBクラスター/インスタンスを [redacted]

1. 新しいDBクラスター/インスタンスを自動バックアップから起動する

- [] 実施

1. AWSコンソール -> RDS -> データベース を開く
2. [redacted] cluster のチェックボックスにチェックを入れる
3. 「アクション」 -> 「特定地点への復元」を選択
4. 「復元時刻」で「復元可能な最新時刻」を選択する
- 実際のリストアでは適切な時刻の選択を行う
5. 「設定」の「DB インスタンス識別子」に「[redacted]」を入力
6. 「設定」の「パラメータグループ」から「[redacted]」を選択
7. 「設定」の「DB クラスターのパラメータグループ」から「[redacted]」を選択
8. 「DBインスタンスの起動」を押下
9. 新しいクラスターとインスタンスが立ち上がるのを待つ

2. Route53の [redacted]

[] 実施

サービスの選択は DR だけを考慮して行われているわけではない

👉 アプリケーション開発チームに DR を理解してもらう難しさ

開発者が使い慣れた
SQL で書きたいんだ

短納期なんだから
オンプレミスの資産をなるべく使いたい

こっちのサービスのほうが
月額費用が安いじゃないか

運用作業のマニュアルって…
我々は運用現場知らないし…



データの安全性を考慮して
DynamoDB を使いましょう

べき等性を考慮して開発すれば
Autoscaling を使えるんです

オンプレを踏襲するなら
緊急時の作業マニュアルを
作ってもらわなきゃ困る

サービスの選択は DR だけを考慮して行われているわけではない

👉 アプリケーション開発チームに DR を理解してもらう難しさ

開発者が使い慣れた
SQL で書きたいんだ

短納期なんだから
オンプレミスの資産をなるべく使いたい

こっちのサービスの方が
月額費用が安いじゃ

運用作業のマニュアルって…
我々は運用現場知らないし…

なにを注意すればいいかハッキリしてよ…

データの安全性を考えて
DynamoDB を使いましょう

クラウドで開発すれば
楽なんです

オンプレを踏襲するなら
緊急時の作業マニュアルを
作ってもらわなきゃ困る

観点表・手順テンプレートの提供 … 具体的な成果物をイメージしてもらう

設定項目	設定内容	備考
冗長化(マルチAZなど)	新規でDBクラスターを構築する場合はマルチAZ構成とする	
バックアップ	バックアップ頻度： 日次でバックアップを取得する バックアップ保持期間： 7日間保持する	



コレを作ればいいのね

```
## DR  
## シナリオ  
1. フェイルオーバー実施  
  1. マスターとレプリカが置き換わり復旧する事を確認する  
2. インスタンス障害  
  1. インスタンス再起動がかかり復旧する事を確認する  
3. レプリカインスタンス障害  
  1. インスタンス再起動がかかり復旧する事を確認する  
4. ディスク障害  
  1. レプリカがマスターに昇格し復旧する事を確認する  
## 事前準備  
- [] クラスタにレプリカを1台起動しておく  
  - AWSコンソール -> RDS を開く  
  - クラスタを選択する  
  - 「アクション」から「リーダーの追加」を押下
```

チェックリストの提供・プロセスへの組み込み … **開発者が常に確認できるように**

0. 確認項目				2. 回答
No	分類	確認項目	補足	回答状況
21	バックアップ	定期的なスケジュールと重要な変更ごとの両方で、リカバリをテストする	<p>新規リソース作成の際は、まずリカバリテストの手順書を作成してください。</p> <p>リカバリテスト手順に変更が入るような大きな構成変更がある場合、変更後のテスト手順でリカバリテストを再実施しましょう。</p> <p>定期的なテストに関しては、作成されたリカバリテスト手順書に基づき、BCP管理テストとして実施されます。</p>	
22	DR	偶発的なデータ損失、インスタンス障害、AZ障害からの回復をDR計画	バックアップ、リカバリが必要と思われる場合は、開発BCP	
23	DR	定期的なスケジュールと重要な変更ごとの両方で、DRをテスト		

作成者			
作成日			
リソース内容			未対応/対応中/完了/
フェーズ	成果物の名称	ステータス	
調査	DB設計書	完了	
調査	セキュリティ設計チェックリスト	完了	
開発	コードレビュー記録	完了	
開発	単体・非機能テスト結果評価基準	完了	
開発	LANSCOPE_EM_クラウド版_バックアップリストア_DR_管理表	完了	
開発	バックアップリストア_DR手順書	完了	
開発	バックアップリストア_DRテスト	対応中	
テスト設計	テスト計画書	対応中	
テスト実施	テスト仕様書	未対応	



DR対応 は テスト実施 などと同列

定期的な訓練・見直しの実施



特に忘れがち
カレンダー登録 する

件名	担当者	29	30	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
[FY24]年次_ [REDACTED]	[REDACTED]																		
月次_ [REDACTED]	[REDACTED]																		
月次_ [REDACTED]	[REDACTED]																		
[REDACTED]	[REDACTED]																		
[FY24]_バックアップリストア_DRの定期実施	[REDACTED]																		
月次_ [REDACTED]	[REDACTED]																		
四半期_ [REDACTED]	[REDACTED]																		

DRって何から始めたらいいの？ という開発・運用担当者の皆様へ



DR対策の具体化

まず **SLO/RTO/RPO** を定める
AWS Trusted Advisor も活用



具体的な施策の実施

利用サービス による責任範囲の違いを意識
開発部隊への浸透 にも一工夫



DR制定後の動き

定期的な訓練・見直し をスケジュール

MOTEX