

S3

レクチャー	レクチャーで学ぶ内容
S3の概要	S3の基本的な機能や仕組みについて理解します。
S3の用途	S3の様々な活用方法についてユースケースを確認します。
S3バケットの作成と操作 (ハンズオン)	S3バケットを作成して、その操作方法や様々な設定方法について理解します。
S3のバージョン管理 (ハンズオン)	S3のプロパティ機能の1つであるバージョニングを利用したバージョン管理を設定します。
S3のライフサイクル管理 (ハンズオン)	S3の管理機能の1つであるライフサイクルを利用したオブジェクトのライフサイクルを設定します。



S3

レクチャー	レクチャーで学ぶ内容
EC2からのS3 ファイルの取得 (ハンズオン)	EC2インスタンスを起動して、S3に接続してデータを取得していきます。
AWS CLIの導入 (ハンズオン)	S3をコマンドラインから操作するために、AWS CLIをインストールして利用方法を確認します。
リージョン間を跨いだ レプリケーション (ハンズオン)	リージョン間を跨いでデータのレプリケーションを実行する設定を行い実行結果を確認します。
静的ホスティングの活用 (ハンズオン)	S3のプロパティ機能の1つである静的ホスティングを利用したWEBサイトを構築します。
S3のプロパティ活用 (ハンズオン)	ここまでに確認していないその他のプロパティ機能の利用方法を確認していきます。



S3

レクチャー

レクチャーで学ぶ内容

S3の外部接続

S3と外部環境とのデータ転送方法に係るサービスを理解します。



S3の概要



AWSストレージサービス

AWSは3つの形式のストレージサービスを提供

ブロックストレージ

- ✓ EC2にアタッチして活用するディスクサービス
- ✓ ブロック形式でデータを保存
- ✓ 高速・広帯域幅
- ✓ 例：EBS、インスタンスストア

オブジェクトストレージ

- ✓ 安価かつ高い耐久性をもつオンラインストレージ
- ✓ オブジェクト形式でデータを保存
- ✓ 例：S3、Glacier

ファイルストレージ

- ✓ 複数のEC2インスタンスから同時にアタッチ可能な共有ストレージサービス
- ✓ ファイル形式でデータを保存
- ✓ 例：EFS



Simple Storage Service (S3)

ユーザがデータを容量制限なく保存可能なマネージド型で提供されるオブジェクト型ストレージ

特徴

■高い耐久性

99.999999999%

■安価なストレージ

容量単価:月額1GB / 約3円

■スケーラブルで安定した性能

データは冗長化されて保存されデータ容量に依存しない性能がAWS側で保証される

■暗号化

転送中や保存時にデータを暗号化可能

データ保存形式

■バケット

オブジェクトの保存場所。名前はグローバルでユニークな必要あり

■オブジェクト

S3に格納されるファイルでURLが付与される。バケット内オブジェクト数は無制限

■データサイズ

データサイズは0KBから5TBまで保存可能



S3のオブジェクト構成

S3のオブジェクトは以下のような要素で構成されている

■ Key

オブジェクトの名前であり、バケット内のオブジェクトは一意に識別する

■ Value

データそのものであり、バイト値で構成される

■ バージョンID

バージョン管理に用いるID

■ メタデータ

オブジェクトに付随する属性の情報

■ サブリソース

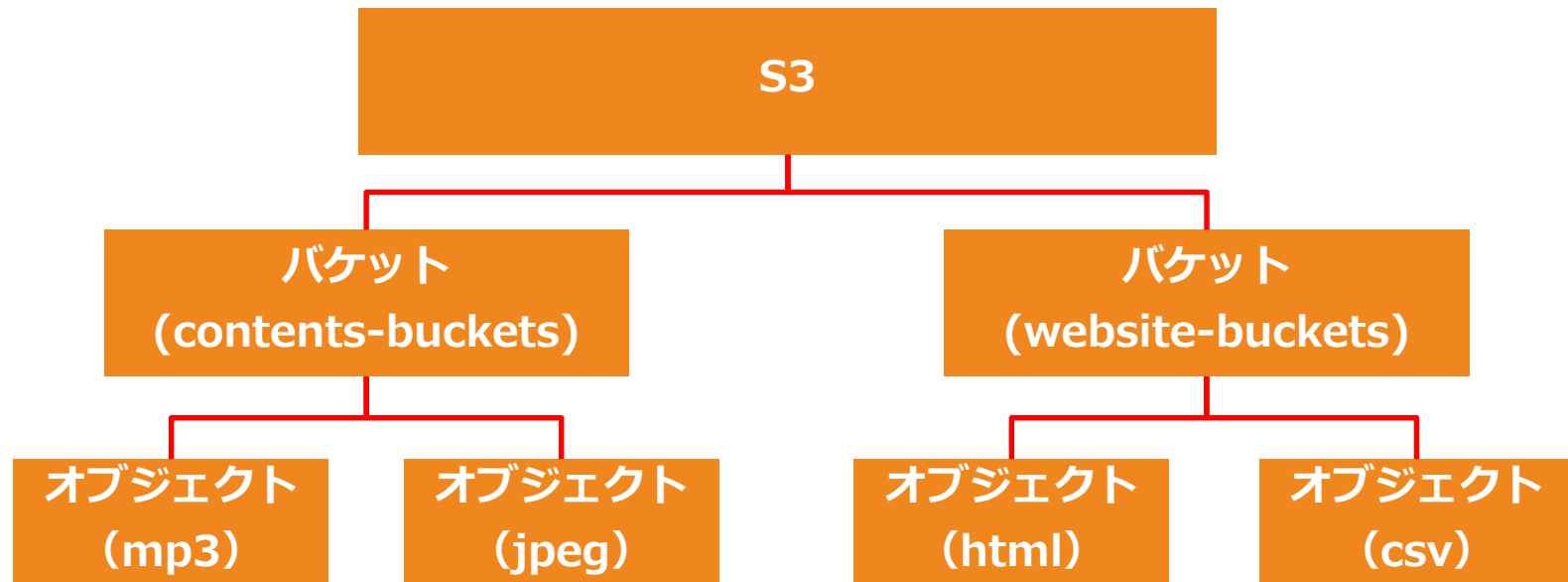
バケット構成情報を保存および管理するためのサポートを提供

例：アクセス制御リスト（ACL）



S3のデータ構造

S3はバケット単位で保存スペースを区分し、オブジェクトでデータを格納する



AWSストレージサービス

S3の用途に応じてストレージタイプを選択する

タイプ	特徴	性能
STANDARD	✓ 複数個所にデータを複製するため耐久性が非常に高い	■ 耐久性 99.999999999% ■ 可用性 99.99%
STANDARD-IA	✓ スタンダードに比べて安価 ✓ データの読み出し容量に応じた課金	■ 耐久性 99.999999999% ■ 可用性 99.9%
One Zone-IA	✓ アクセス頻度は低いが、必要に応じてすぐに取り出すデータ向け	■ 耐久性 99.999999999% ■ 可用性 99.5%
RRS	✓ Reduced Redundancy Storage 低冗長化ストレージ ✓ Glacierから取り出したデータ配置等	■ 耐久性 99.99% ■ 可用性 99.99%
Amazon Glacier	✓ 最安のアーカイブ用ストレージ ✓ データ抽出にコストと時間（3~5時間）を要する ✓ ライフサイクルマネジメントで指定 ✓ ボールロック機能でデータを保持	■ 耐久性 99.999999999% ■ 可用性 N/A



S3の整合性モデル

S3は高い可用性を実現するため、データ更新・削除には結果整合性モデルを採用。同時書込みはタイムスタンプ処理を実施

データ処理	整合性モデル
新規登録	<ul style="list-style-type: none">✓ Consistency Read✓ 登録後即時にデータが反映される
更新	<ul style="list-style-type: none">✓ Eventual Consistency Read✓ 更新直後はデータ反映に時間がかかる
削除	<ul style="list-style-type: none">✓ Eventual Consistency Read✓ 削除直後はデータ反映に時間がかかる



S3のアクセス管理

S3のアクセス管理は用途に応じて方式を使い分ける

管理方式	特徴
ユーザポリシー	<ul style="list-style-type: none">✓ IAMユーザーに対してアクセス権限を設定✓ 一元的にユーザー権限を管理
バケットポリシー	<ul style="list-style-type: none">✓ S3バケット毎にアクセス権限を設定✓ クロスアカウントでのアクセス権限管理を実施するケース向け
ACL	<ul style="list-style-type: none">✓ バケットとオブジェクトへのアクセス権限を設定✓ 簡易的に権限管理を実施
署名付きURL	<ul style="list-style-type: none">✓ AWS SDKで生成した署名付きURLでS3のオブジェクトへの一定時間アクセスを許可



S3の暗号化

S3へのデータ保管時の暗号化形式は2つ

暗号化方式	特徴
サーバーサイド 暗号化	<ul style="list-style-type: none">✓ AWSのサーバーリソースを利用して格納データの暗号化を実施✓ 暗号化タイプ : SSE-S3 / SSE-KMS / SSE-C
クライアントサイド 暗号化	<ul style="list-style-type: none">✓ 暗号化プロセスをユーザ側で管理する✓ 暗号化タイプ AWS KMSで管理されたカスタマーキーで暗号化 クライアントが管理するマスターキーで暗号化



レプリケーション

リージョン間を跨ぐクロスリージョンレプリケーションにより
耐障害性を高める

レプリケーションのトリガー

□ バケットに対するオブジェクト作成・更新・削除をトリガーにレプリケーションを実行する

設定

- バージョニング機能を有効にする
- バケットは各別リージョンを指定
- 双方向レプリケーションも可能
- データ転送費用が発生



バージョン管理

ユーザーによる誤操作でデータ削除などが発生してもバージョンから復元できる

設定

- バケットをバージョン管理する
- バージョン保管されたオブジェクトを参照可能
- ライフサイクル管理によって保存する期間の指定も可能
- バケット削除時に古いバージョンの別途削除が必要

【現在】
バージョンID
00011

データA

データB

データC

【過去分】
バージョンID
00010

データA

データB

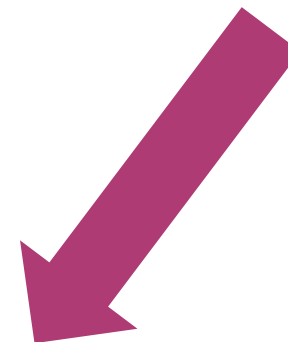
データC

バージョンID
00012

データA

データB

データC



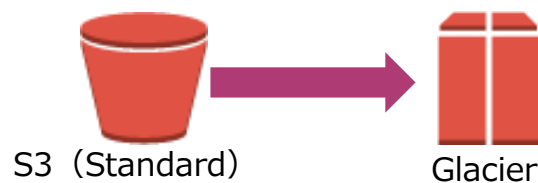
ライフサイクル管理

バケット内のオブジェクト単位でストレージクラスの変更や削除時期などを設定することで実行を自動化する

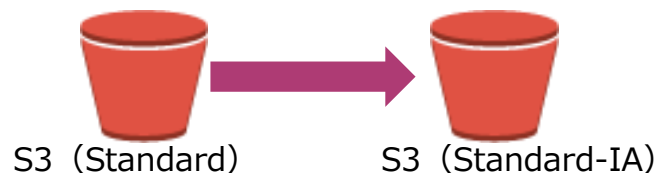
設定方法

- バケット全体やPrefixに設定
- オブジェクト更新日を基準にして日単位で指定し、毎日0:00UTCにキューを実行
- 最大1000ルール
- IAに移動できるのは128KB以上のオブジェクト
- MFA Deleteが有効だと設定不可

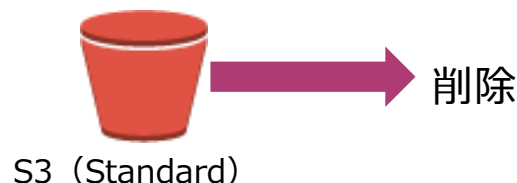
一定期間で自動アーカイブ



一定期間で自動で安価な保存場所へ



一定期間で自動で削除



バックアップ

Glacierを利用してバックアップと復元が実施可能

アーカイブ

- S3オブジェクトデータをGlacierに移動
- S3データを削除するとGlacier側も削除される

【データ紐づけ】

- S3 : 8KBオブジェクト/メタデータ
- Glacier : 32KBオブジェクト/メタデータ

リストア

- オブジェクト毎に復元が可能
- 一時的にRRSに指定日数間複製する
- 復元に要する時間を選択
- 復元期間はRRSとGlacierで課金



利用状況の確認

S3の利用状況やS3のイベント発生を確認することができる

S3の分析

- データのアクセスパターンの簡易可視化
- CSV形式で出力可能
- バケット内の分析を実施
- アクセス頻度の低いデータや保存期間を確認して、ライフサイクルポリシー設定に活かしていく

S3のイベント通知

- バケット内イベントの発生をトリガーにして、SNS/SQS/Lambdaに通知設定が可能
- シームレスなシステム連携処理を実現

