



このコンテンツは公開から3年以上経過しており内容が古い可能性があります
最新情報については[サービス別資料](#)もしくはサービスのドキュメントをご確認ください

[AWS Black Belt Online Seminar]

Amazon S3 / Amazon S3 Glacier

サービスカットシリーズ

アマゾンウェブサービスジャパン株式会社
ソリューションアーキテクト

焼尾 徹

2019/2/20



自己紹介

焼尾 徹

技術統括本部 レディネス&テックソリューション本部
ソリューションアーキテクト



普段の業務

個別相談会のお客様を技術的にサポート
場所にとらわれない働き方の模索

好きなAWSの取り組み

Amazon Wind Farm



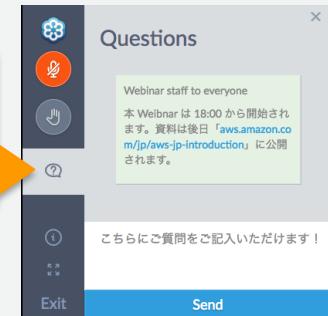
AWS Black Belt Online Seminar とは

「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分かれて、Amazon ウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです。

質問を投げることができます！

- 書き込んだ質問は、主催者にしか見えません
- 今後のロードマップに関するご質問はお答えできませんのでご了承下さい

- ①吹き出しをクリック
- ②質問を入力
- ③Sendをクリック



Twitter ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- 本資料では2019年02月19日時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(<http://aws.amazon.com>)にてご確認ください。
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。
- 価格は税抜表記となっています。日本居住者のお客様が東京リージョンを使用する場合、別途消費税をご請求させていただきます。
- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at <http://aws.amazon.com/agreement/>. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

本日の内容

- Amazon S3の位置付け
- Amazon S3の概要
- Amazon S3へのアクセス
- Amazon S3のデータ保護
- Amazon S3の管理
- Amazon S3パフォーマンス最適化
- Amazon S3の料金
- まとめ

Amazon S3の位置付け

Amazon S3の概要

Amazon S3へのアクセス

Amazon S3のデータ保護

Amazon S3のデータ管理

Amazon S3パフォーマンス最適化

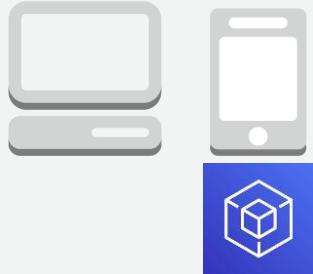
Amazon S3の料金

Amazon S3の位置付け

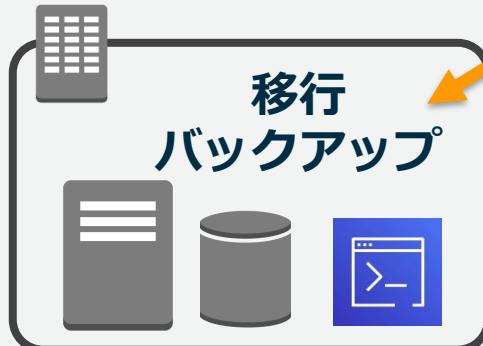
Amazon S3の位置付け



Web / モバイル
アプリケーション



移行
バックアップ

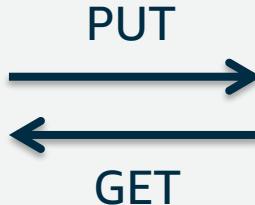


Amazon S3とは

Amazon Simple Storage Service (S3)は、ユーザがデータを安全に、容量制限なく、データ保存が可能な、クラウド時代のオブジェクトストレージです。



S3 API



S3

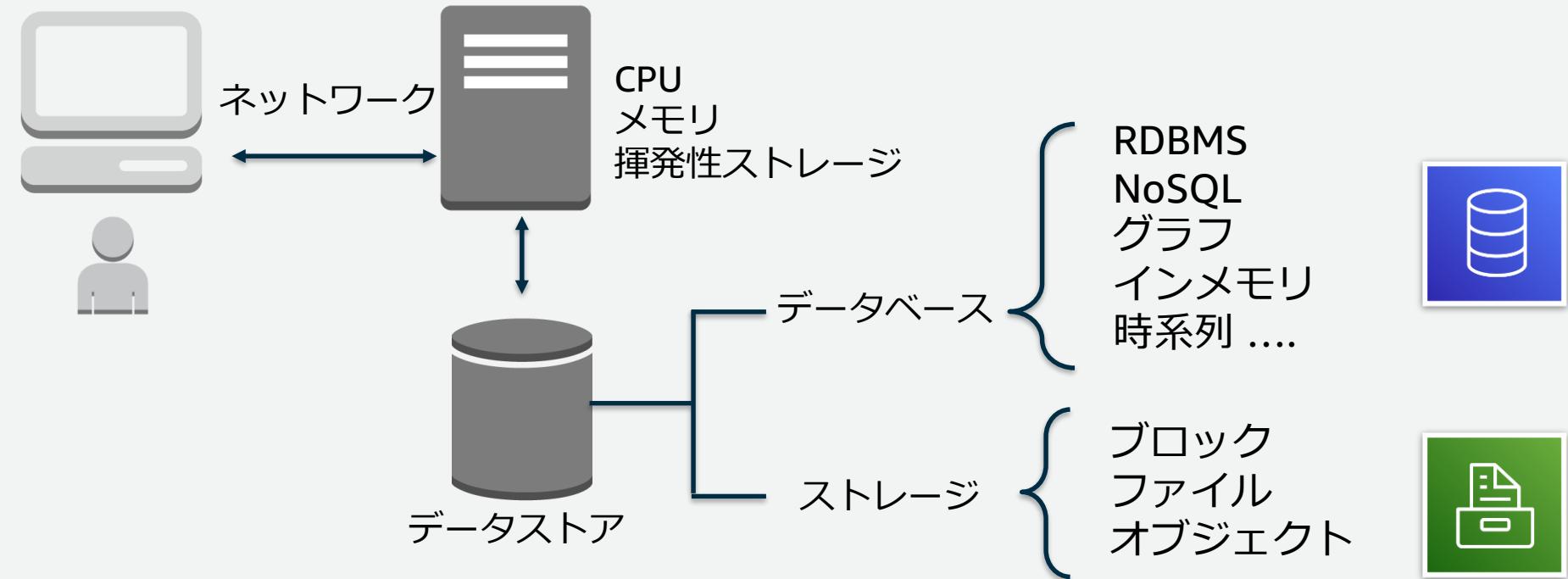
Amazon S3 及び Amazon S3 Glacier

Amazon Simple Storage Service (S3)は、ユーザがデータを安全に、容量制限なく、データ保存が可能な、クラウド時代のオブジェクトストレージです。

Amazon S3 Glacier は、安全性とコスト効率を重視したアーカイブ向けストレージです。



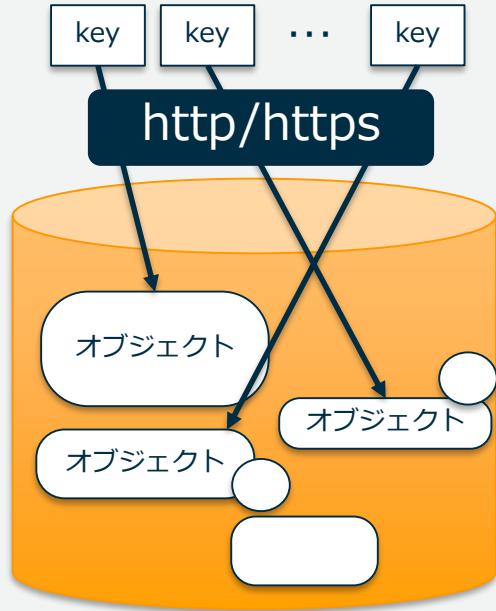
データストアの選択シーン



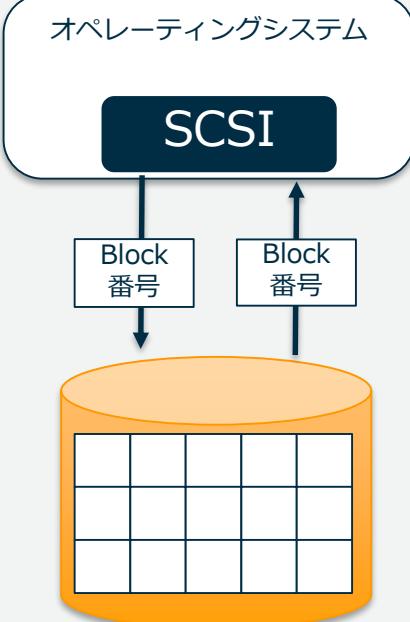
オブジェクトストレージの特徴

オブジェクトストレージ

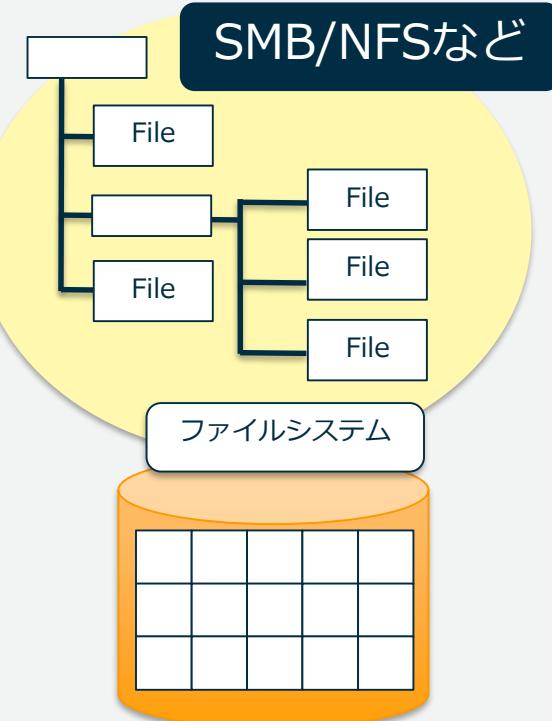
オブジェクト、それに付随するメタデータ、そのオブジェクトにアクセスするためのユニークなIDで構成されるデータの倉庫



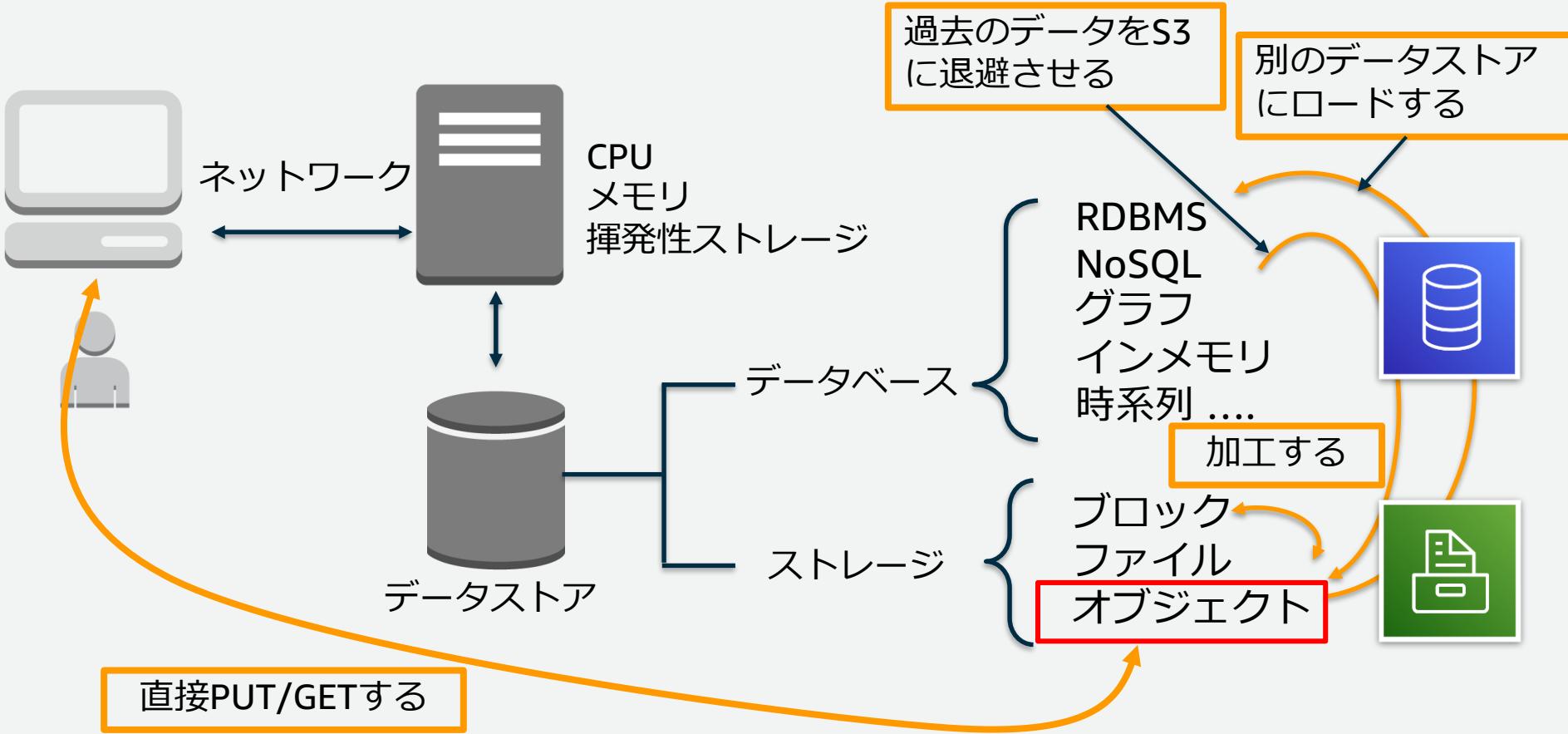
ブロックストレージ



ファイルストレージ



S3 利用シーン



ユースケース <https://aws.amazon.com/jp/blogs/news/webinar-bb-s3-usecase-2018/>



Amazon S3の位置付け

Amazon S3の概要

Amazon S3へのアクセス

Amazon S3のデータ保護

Amazon S3のデータ管理

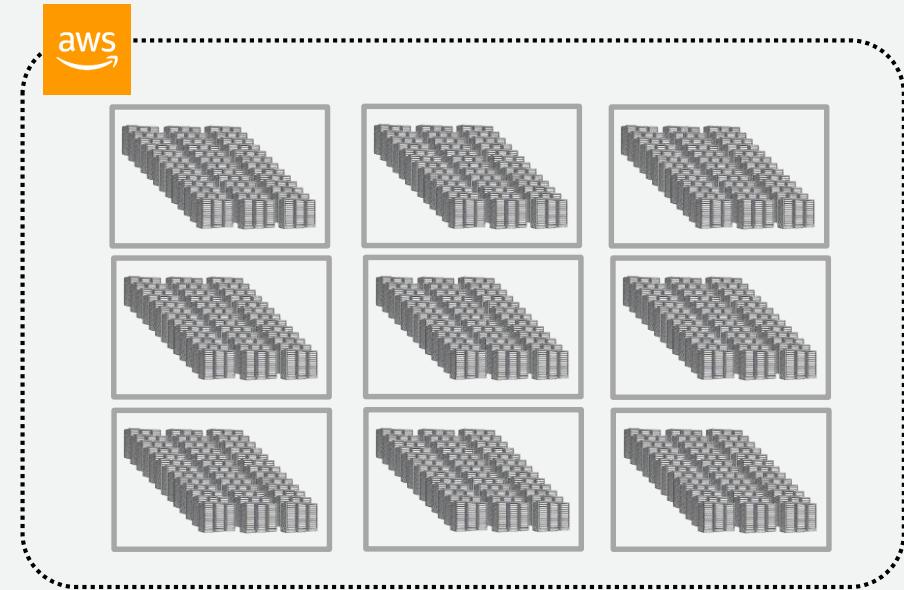
Amazon S3パフォーマンス最適化

Amazon S3の料金

Amazon S3の概要

Amazon S3 特徴

- **容量無制限**
 - 1ファイル最大5TBまで
- **高い耐久性**
 - 99.99999999%
- **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**
 - データ容量に依存しない性能（ユーザが、サーバ台数、媒体本数やRAID、RAIDコントローラを考える必要がない）



※2019年2月 <https://aws.amazon.com/jp/s3/pricing/>
東京リージョンにおけるスタンダードが、US\$0.025/GB



S3 とリージョン、アベイラビリティゾーン(AZ)



S3 標準は少なくとも3つのAvailability Zones(AZs)にデータを格納する



1つのAZは最大8つのデータセンターで構成

物理的に離れている - つまり、万一災害が起きても、1つのAZへの影響しかない

データセンター間、AZ間は低遅延のプライベートネットワークで接続されている



1つのデータセンタのダウン、または、1つのAZのダウンは、S3としての可用性に影響しない

Amazon S3の耐久性
99.99999999%



Amazon S3 用語



バケット

- オブジェクトの保存場所。各AWSアカウントにてデフォルト100個まで作成可能。**名前はグローバルでユニークな必要あり。**上限緩和申請で100以上も利用可能に。

オブジェクト

- データ本体。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。1オブジェクトサイズは0から5TBまで(1つのPUTでアップロード可能なオブジェクトの最大サイズは5GB)。

キー

- オブジェクトの格納URLパス。「バケット+キー+バージョン」が必ず一意になる。

メタデータ

- オブジェクトに付随する属性の情報。システム定義メタデータ、ユーザ定義メタデータがある。

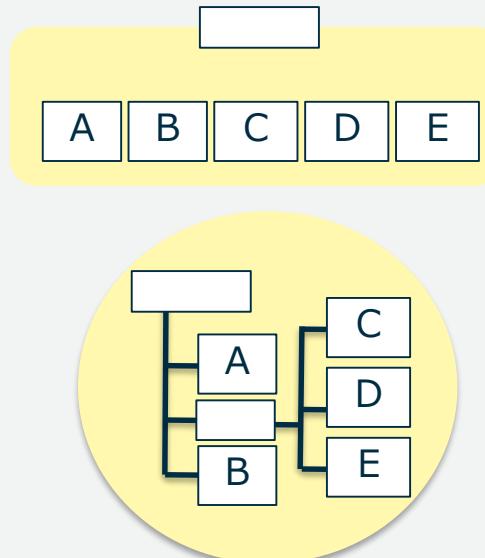
リージョン

- バケットを配置するAWSのロケーション。目的のアプリケーションと同じリージョンであると有利。



Amazon S3 の概要 - オブジェクトのネーミングスキーマ

オブジェクトはバケット内にフラットに格納される。
キーのパス指定でフォルダ階層のように表示も可能。「/」を区切り記号として、マネジメントコンソールでは、フォルダ構造を表現する。



(*) 2018.3月 バケット命名規則について、米国東部リージョンでも適用されるようになり、これで全てのリージョンにてDNS命名規則に沿って、命名する必要があります。



Amazon S3 の概要 - Data Consistency モデル

Amazon S3はデータを複数の場所に複製することで高い可用性を実現するため、データの更新・削除にはEventual Consistency Readモデル（結果整合性）が採用されている。

オペレーション	Consistencyモデル	挙動
新規登録 (New PUTs)	Consistency Read(*)	登録後、即時データが参照できる
更新 (Overwrite PUTs)	Eventual Consistency Read(結果整合性)	更新直後は、以前のデータが参照される可能性がある
削除 (DELETE)	Eventual Consistency Read (結果整合性)	削除直後は、削除前のデータが参照される可能性がある

- 同じオブジェクトへの複数同時書き込み制御のためのロック処理は行われず、最新のタイムスタンプのリクエストが優先される。
- (ロック処理があるような仕組みと比べて) 読み込みの待ち時間が小さくなるのがメリット

(*) 2015.8月 new putについて、read-after-write consistencyがUS Standard regionでもサポートされるようになり、全てのリージョンにてread-after-write-consistencyとなりました。



Amazon S3 の概要 – ストレージクラス

用途に応じて、オブジェクトを格納するS3の場所の使い分け

ストレージクラス	特徴	耐久性（設計上）	可用性（設計上）
STANDARD (スタンダード)	複数AZにデータを複製。デフォルトのストレージクラス。	99.999999999%	99.99%
STANDARD-IA (標準低頻度アクセスストレージ)	スタンダードに比べ格納コストが安価。いつでもアクセス可能だが、データの読み出し容量に対して課金。IAはInfrequent Accessの略。	99.999999999%	99.9%
INTELLIGENT_TIERING	アクセス頻度が高いオブジェクトと低いオブジェクトを自動的に最適化するストレージクラス	99.999999999%	99.9% 2018.11月
ONEZONE_IA (1ゾーン-低頻度アクセスストレージ)	Single AZにデータを格納するが、複製の考え方はスタンダード、STANDARD-IAと同じ。ただし、地震や洪水などの大災害によるアベイラビリティゾーンの物理的な損失には耐性はありません。	99.999999999%	99.5% 2018.4月
S3 Glacier (アーカイブ)	低コストだが、データの取り出しにコストと時間を要する。ライフサイクルマネジメントにて指定する。	99.999999999%	99.99% Object復元後
S3 Glacier Deep Archive (予定)	もっとも低コストなコールドストレージ。取り出しには半日から2-3日かかる。	99.999999999%	(未定)
低冗長化ストレージ(RRS)	RRS はReduced Redundancy Storageの略。Glacierから取り出したデータの置き場所として利用。	99.99%	99.99%

Amazon S3 の操作

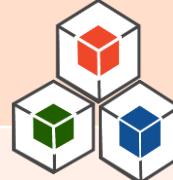
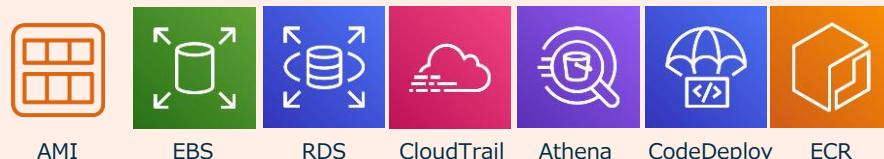
オペレーション	処理	特徴
GET	S3から任意のファイルをダウンロード	<ul style="list-style-type: none">RANGE GETに対応。S3 Glacierにアーカイブされ、RestoreされていないオブジェクトへのGETリクエストはエラー
PUT	S3に対してファイルをアップロード(新規・更新)	<ul style="list-style-type: none">シングルPUTオペレーションでは最大5GBまで、Multipart Uploadを利用すると5TBまで格納可能。
LIST	S3バケット内のオブジェクト一覧を取得	<ul style="list-style-type: none">Prefixによるパス指定での取得一覧のフィルタリングが可能。1回のリクエストでは1,000オブジェクトまで情報を取得可能。それ以上の場合は再帰的にリクエストを実施する必要がある
COPY	S3内でオブジェクトの複製を作成	<ul style="list-style-type: none">シングルCOPYオペレーションでは最大5GBまで、Multipart Uploadを利用すると5TBまでのファイルの複製が可能
DELETE	S3から任意のファイルを削除	<ul style="list-style-type: none">シングルDELETEオペレーションで最大1,000個のオブジェクトを削除可能MFA(Multi Factor Authentication)と連携した削除制御が可能
HEAD	オブジェクトのメタデータを取得	<ul style="list-style-type: none">オブジェクトそのものをGETオペレーションで取得しなくても、メタデータだけを取得可能
RESTORE	アーカイブされたオブジェクトを一時的にS3に取り出します。またはアカーブされたオブジェクトへSelectクエリが可能	<ul style="list-style-type: none">S3 Glacierからのデータの取り出し低冗長化ストレージに指定期間オブジェクトがコピーされ、その指定期間中、ダウンロードが可能になるGlacier Selectによるデータの部分的な取り出し
SELECT	ファイルへのSelect クエリをかけられる	<ul style="list-style-type: none">S3 Selectによるデータの部分的な取り出し

New
2017.11月

New
2018.4月



S3へのアクセス方法

操作	利用イメージ
アプリケーション開発	AWS SDK <pre>PutObjectRequest putObjectRequest = new PutObjectRequest(bucketName, Key, file); PutObjectResult result = this.client.putObject(putObjectRequest)</pre> 
コマンドラインやシェル	AWS CLI <pre>\$ aws s3 cp xxxx.mp4 s3://bucketName/ \$ aws s3api get-object --bucket-name <bucket-name> --key <prefix/file-name></pre>
手動、人間の操作	Management Console 3rdパーティツール 
アプリケーションやAWSサービスでのS3利用	HTTPS AWS SDK そのアプリケーションやAWSサービスが透過的にS3を活用する 



Amazon S3の位置付け
Amazon S3の概要
Amazon S3へのアクセス

Amazon S3のデータ保護
Amazon S3のデータ管理
Amazon S3パフォーマンス最適化
Amazon S3の料金

Amazon S3へのアクセス

アクセス管理

きめ細やかなバケットもしくはオブジェクトへのアクセス権の設定

デフォルトでは、S3のバケットやオブジェクトなどは全てプライベートアクセス権限
(Owner:作成したAWSアカウント)のみに設定

IAMユーザ、クロスアカウントユーザ、匿名アクセスなどバケット/オブジェクト単位で
指定可能

- **ユーザポリシー**

- IAM Userに対して、S3やバケットへのアクセス権限を設定
- 複数バケットやS3以外のものも含めて一元的にユーザ権限を指定する場合など

- **バケットポリシー**

- S3バケット毎に、アクセス権限を指定
- クロスアカウントでのS3バケットアクセス権を付与する場合など

- **ACL**

- 各バケットおよびオブジェクトのアクセス権限を指定
- バケット単位やオブジェクト単位で簡易的に権限を付与する場合など



アクセス管理(続き) - ユーザーポリシー

ユーザポリシーサンプル

```
{  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "s3>ListAllMyBuckets"  
      ],  
      "Resource": "arn:aws:s3:::*"  
    },  
    {  
      "Effect": "Allow",  
      "Action": [  
        "s3>ListBucket", "s3:GetBucketLocation"  
      ],  
      "Resource": "arn:aws:s3:::examplebucket"  
    },  
    {  
      "Effect": "Allow",  
      "Action": [  
        "s3:PutObject", "s3:GetObject", "s3:DeleteObject"  
      ],  
      "Resource": "arn:aws:s3:::examplebucket/*"  
    }  
  ]  
}
```



AWS Identity and Access Management (IAM)

「AWSにおいて、このユーザは何ができるか？」

- IAMのアイデンティティベースのポリシー
- IAMの環境において、何らかの制御を行う目的
- 全てのAWSサービスに言えることでS3に限らない

ユーザポリシーを利用して、IAMユーザに対して任意のバケットへのアクセス権限を付与

その他サンプルは下記URLを参照

http://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/example-policies-s3.html



アクセス管理(続き) - バケットポリシー

バケットポリシーサンプル

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AddPerm",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": ["s3:GetObject"],  
      "Resource": ["arn:aws:s3:::examplebucket/*"]  
    }  
  ]  
}
```



S3 バケットポリシー

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "IPAllow",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": "s3:*",  
      "Resource": "arn:aws:s3:::examplebucket/*",  
      "Condition": {  
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"}  
      }  
    }  
  ]  
}
```



S3 バケットポリシー

「このS3リソースには誰がアクセスできるのか？」

- IAMのリソースベースのポリシー
- S3環境において、何らかの制御を行う目的
- Conditionを利用してIAM User、クロスカント、IPアドレス制限、HTTP Referrer制限、CloudFront、MFA制限なども指定可能

バケットポリシーを利用して、全てのユーザに対して、任意のバケットへのGETリクエストを許可

バケットポリシーを利用して、任意のIPアドレスレンジからバケットへのアクセスを許可

その他サンプルは下記URLを参照

http://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/example-bucket-policies.html



アクセス管理(続き) - アクセスコントロールリスト(ACL)

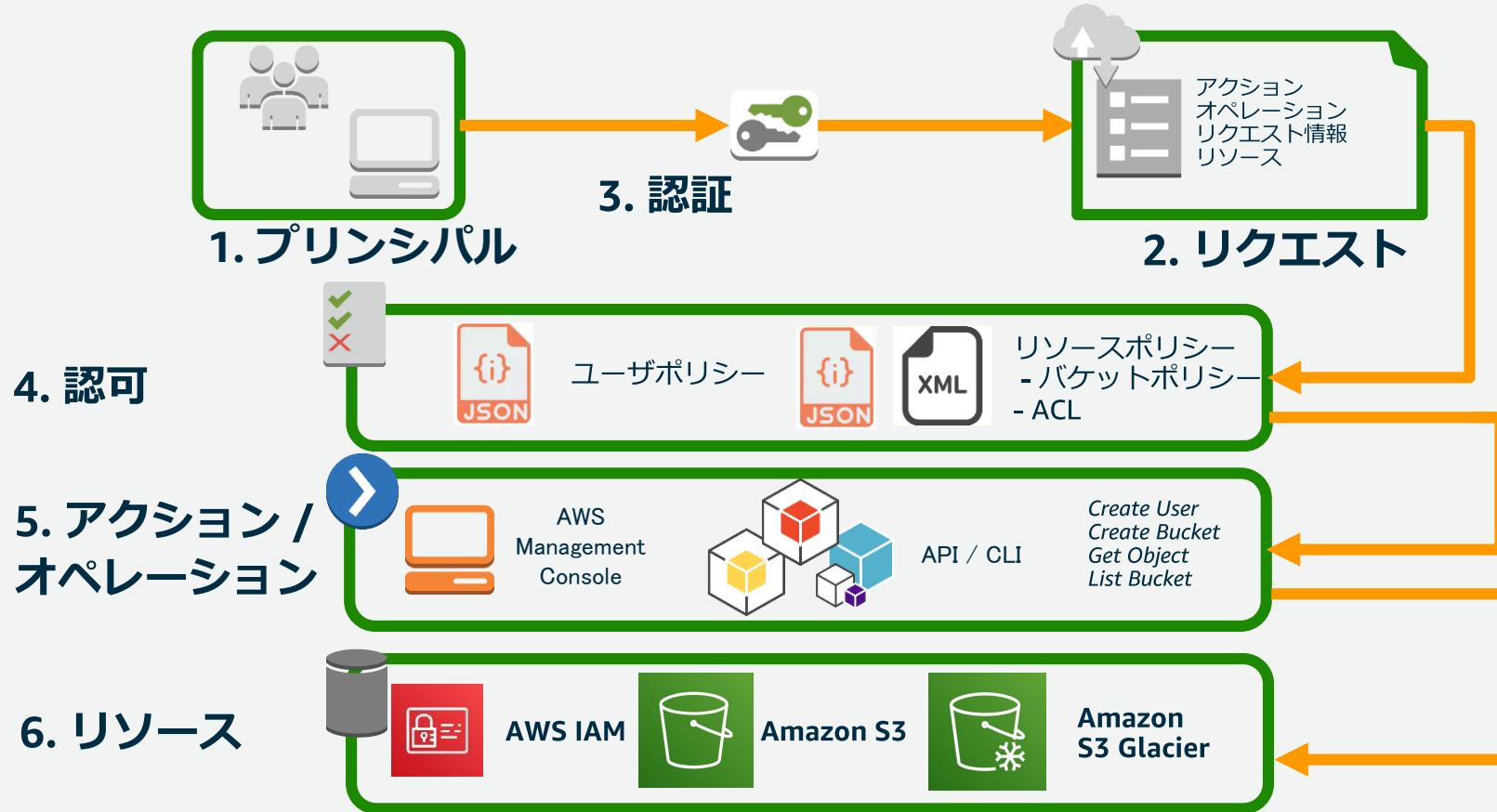
ACLはバケット単位のACLとオブジェクト単位のACLが存在

- バケットACLはバケット内のオブジェクトにも影響を与えるが、オブジェクトが個別にACLを設定している場合、オブジェクトACLが優先される
- ACLよりも、**ユーザポリシー**や**バケットポリシー**が優先される
- 例えば、違うアカウントが所有するオブジェクトのアクセス許可を管理する場合に、オブジェクトACLが有用
- バケットACLを利用するには、Amazon S3 のログ配信グループに、バケツのアクセスログオブジェクトの書き込みアクセス許可を付与する場合のみ



=> 通常は、バケットポリシーを用いましょう

S3へのアクセス、ここまで整理



意図せずバケットがパブリックアクセスになるのを抑制する

- アクセス許可チェック、S3コンソールで公開アクセスが許可されたバケットが容易に分かるようなインジケータを表示する

2017.11月

The screenshot shows the AWS S3 console with a list of 49 buckets. The columns include the bucket name, object status, location, and last modified date. Red circles highlight specific entries:

- Bucket 1: オブジェクトは公開可能 (Object is public)
- Bucket 2: 公開 (Public)
- Bucket 3: オブジェクトは公開可能 (Object is public)
- Bucket 4: オブジェクトは公開可能 (Object is public)

At the bottom of the list, there is a note: "オブジェクトは公開可能 (Object is public)" followed by "(審査)".

公開されている・
されていないがす
ぐわかる
↓
間違いがあれば
すぐ気付くことが
できる

- AWS Configにて、S3バケットがPublicにreadできたり、誰でも書き込みめるようになっていないかをチェックするマネージドルールを提供

2017.8月

<https://aws.amazon.com/jp/blogs/news/aws-config-update-new-managed-rules-to-secure-s3-buckets/>

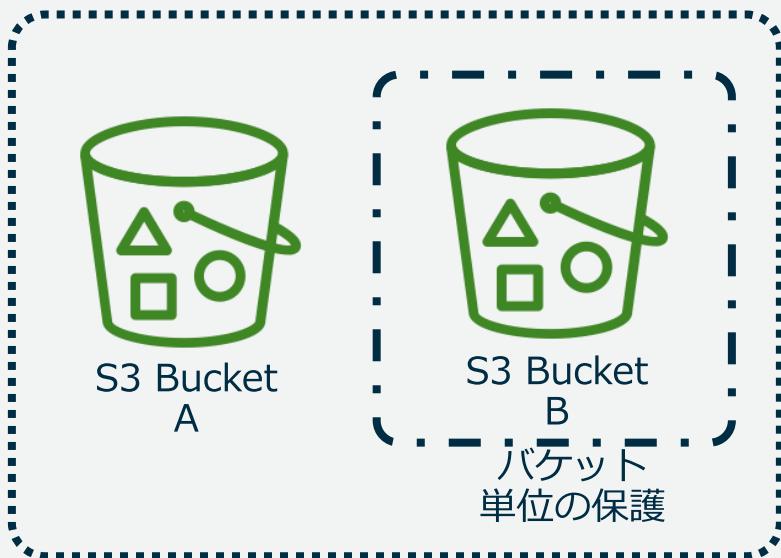


Amazon S3 Block Public Access

New 2018.11月

アカウントレベル、もしくはバケットレベルで「あらかじめ」意図せずバケットがパブリックアクセスになるのを抑制する

アカウント単位の保護



パブリックなアクセスを許すバケットポリシー

{
 "version": "2012-10-17",
 "Id": "Policy15315299",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": "*",
 "Action": "s3:GetObject",
 "Resource": "arn:aws:s3:::ex-bucket/*"
 }
]
}

A large red circular 'prohibited' symbol is overlaid on the middle section of the JSON policy code, specifically covering the 'Effect', 'Principal', 'Action', and 'Resource' fields.

- 新規で作成されるバケット、新規で作成されるアカウントにはデフォルトで適用（安全側に）



Amazon S3 Block Public Access (続き)

設定	Trueとした場合の効果	備考
BlockPublicAcls	パブリックなACL設定、パブリックなオブジェクトのアップロードをさせない	
IgnorePublicAcls	パブリックなACLの設定をしていても、それを無効化する	
BlockPublicPolicy	パブリックなバケットポリシーの設定をさせない	アカウントレベルで有効にするのが効果的。AWS Organizationsなど
RestrictPublicBuckets	パブリックなバケットポリシー設定を持つバケットに対して、パブリックなアクセス、クロスアカウントでのアクセスを無効化する	パブリックなバケットポリシー設定を持っていなければ、そのバケットへのアクセスの影響はない

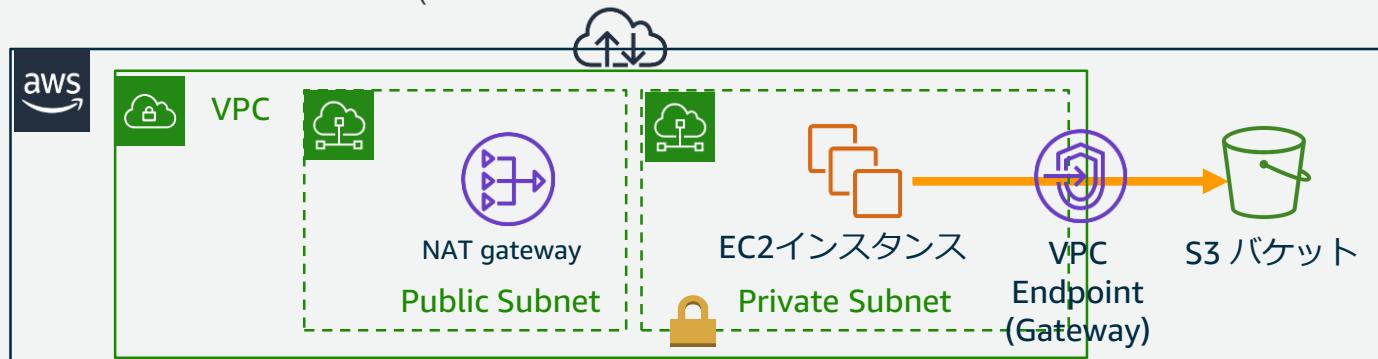
- ・ 「パブリック」の意味= どなたにもアクセスしうる状況
 - ・ ACLで、All Users Authenticated Usersへの許可
 - ・ 誰でもアクセスできるようなバケットポリシー
 - ・ https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/access-control-block-public-access.html
- ・ ブロックパブリックアクセス設定は既存のポリシーまたはACL **設定内容を変更するものではない**
 - ・ ブロックパブリックアクセス設定を削除すると、パブリックポリシーまたはACLを持つバケットまたはオブジェクトは再びパブリックにアクセス可能になる

VPC Endpoint

(*) 2015.5月より

VPC内の**Private Subnet**上で稼働するサービスから、NAT Gatewayを経由せずに、直接S3とセキュアに通信させることが可能

- 通信可能なのは同一リージョンのS3のみ
- VPC管理画面のEndpointで作成し、S3と通信したいSubnetのルートテーブルに追加
- Endpoint作成時にアクセスポリシーを定義し、通信可能なBucketや通信元のVPCの指定が可能（バケットポリシーとIAMポリシーを利用したSource IPやVPC CIDRによる制限は利用不可）
- 別のVPCやSubnetを跨いだ直接のEndpointの利用は不可
- ゲートウェイエンドポイント（PrivateLinkベースのインターフェースエンドポイントではない）



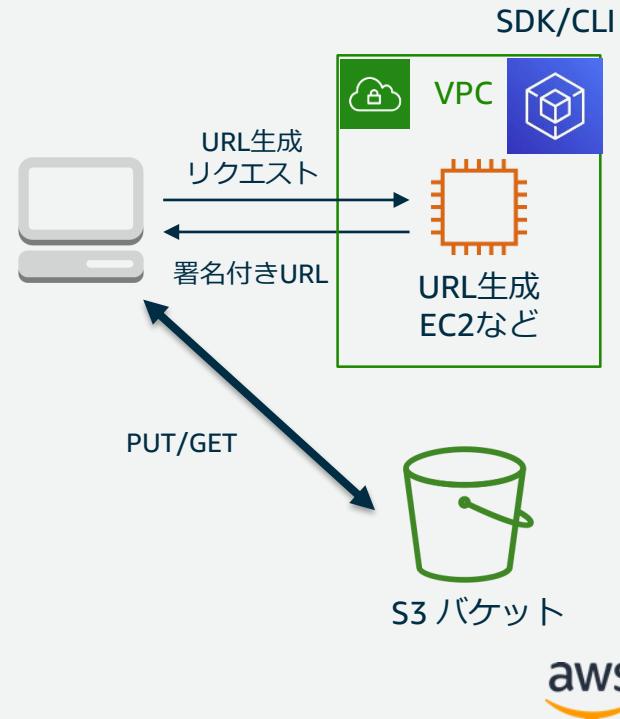
http://docs.aws.amazon.com/ja_jp/AmazonVPC/latest/UserGuide/vpc-endpoints.html
http://aws.typepad.com/aws_japan/2015/05/vpcendpointfors3.html



Pre-signed Object URL (署名付きURL)

AWS SDK (またはAWS CLI)を利用して生成される、署名されたURLを利用し、S3上のプライベートなオブジェクトに対して**一定時間の**アクセスを許可

- Pre-signed URLを利用してすることで、セキュアにS3とのデータのやり取りが可能
- GETとPUTオペレーションで利用可能
 - 任意のユーザへの一時的なオブジェクト共有
 - 任意のユーザからの一時的なS3へのオブジェクトアップロード権限の付与
- URLを生成したIAMユーザ/ロールの権限が用いられる
- バケット名、オブジェクトキー、HTTPメソッド(GETもしくはPUT)、Expire時間を指定する
- 生成されたURLはExpireする前までが有効
- 注意：そのURLで誰でもそのアクションを実行できる



Pre-signed Object URL (署名付きURL、続き)

署名URLの生成ソースサンプル (Python)

```
# Get the service client.  
s3 = boto3.client('s3')  
  
# Generate the URL to get 'key-name' from 'bucket-name'  
url = s3.generate_presigned_url(  
    ClientMethod='get_object',  
    Params={  
        'Bucket': 'sample-bucket-cf',  
        'Key': 'contents/test.txt'  
    },  
    ExpiresIn=3600  
)
```

以降でPUTもしくはGET処理を実装
:

署名付きURL生成

GET/PUTのいずれかの処理
を指定

} 対象バケットおよびオブジェ
クトの指定

URL有効期間の指定 (秒)



Webサイトホスティング

静的なWebサイトをS3のみでホスティング可能

- バケット単位で指定
 - Management Consoleで設定可能
 - パブリックアクセスを許可するため別途バケットポリシーで全ユーザにGET権限を付与
- 独自ドメインの指定
 - ドメイン名をバケット名として指定(www.example.com)
 - 通常は http://バケット名.s3-website-ap-northeast-1.amazonaws.com
 - Route53のAlias設定でドメイン名とS3のバケット名を紐付けたレコードを登録
- リダイレクト機能
 - 任意のドメインにリダイレクト設定が可能
 - x-amz-website-redirect-location(メタデータの一つ)にセットされる



Webサイトホスティング（続き）

- CORS(Cross-origin Resource Sharing)の設定
 - AJAXなどを利用して、異なるドメインからのS3アクセス時に利用
 - Management Console の場合Bucket PropertiesのPermissionより設定

```
<CORSConfiguration>
  <CORSRule>
    <AllowedOrigin>http://www.example.com</AllowedOrigin>
    <AllowedMethod>PUT</AllowedMethod>
    <AllowedMethod>POST</AllowedMethod>
    <AllowedMethod>DELETE</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
  </CORSRule>
</CORSConfiguration>
```

設定例

クロスドメインがwww.example.comの場合、
全てのリクエストを許可

CloudFrontとの連携

- WebサーバとしてS3を利用する場合は、**CloudFront経由で配信することを推奨**
- バケットポリシーを利用してCloudFrontからのHTTP/HTTPSリクエストのみを許可することも可能
 - バケットポリシーのPrincipalにCloudFrontのCanonicalUserを指定 (CloudFrontの「Origin Access Identity」のコンフィグレーション)

Amazon CloudFront



Amazon S3の位置付け
Amazon S3の概要
Amazon S3へのアクセス
Amazon S3のデータ保護
Amazon S3のデータ管理
Amazon S3パフォーマンス最適化
Amazon S3の料金

Amazon S3のデータ保護

暗号化によるデータ保護

保管時(Amazon S3 データセンター内のディスクに格納されているとき)
のデータを暗号化して保護するもの

・ サーバサイド暗号化

- AWSのサーバリソースを利用して格納データの暗号化処理を実施
- 暗号化種別
 - SSE-S3 : AWSが管理する鍵を利用して暗号化
 - SSE-KMS : Key Management Service(KMS)の鍵を利用して暗号化
 - SSE-C : ユーザが提供した鍵を利用して暗号化(AWSで鍵は管理しない)

・ デフォルト暗号化

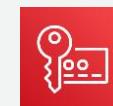
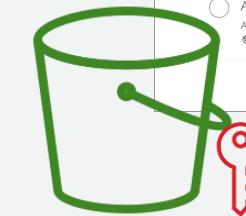
- バケットポリシーを定義することなく、バケットに格納するオブジェクトの暗号化を強制する

・ クライアントサイド暗号化

- 暗号化プロセスはユーザ管理
- クライアント側で暗号化したデータをS3にアップロード
- 暗号化種別
 - AWS KMSで管理されたカスタマーキーを利用して暗号化
 - クライアントが管理するマスターキーを利用して暗号化

2017.11月

New

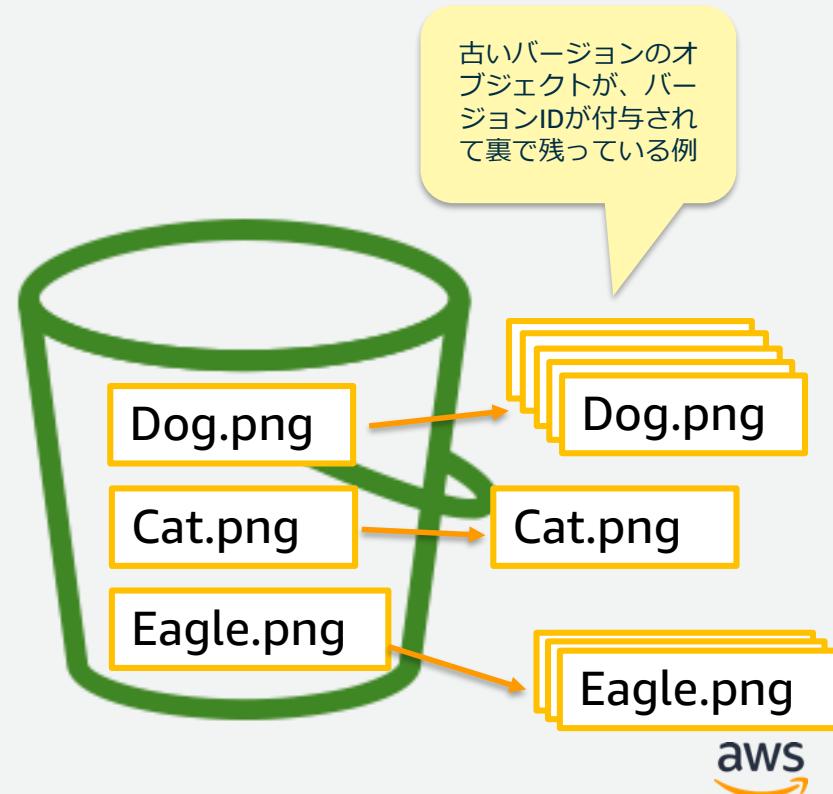


https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/UsingEncryption.html

バージョン管理機能 (Versioning)

ユーザやアプリケーションの誤操作による削除対策に有効

- バケットに対して設定(Enable/Disable)
- 同じキー名でアップロードすると前のバージョンが残る
- バージョン保管されている任意のオブジェクトを参照可能
- バージョニングにより保管されているオブジェクト分も課金
- ライフサイクル管理(後述)と連携し、保存期間(有効期限)も指定可能
- バケットを削除したい場合は、古いバージョンのオブジェクトも削除する
 - ここでも、ライフサイクル管理が便利



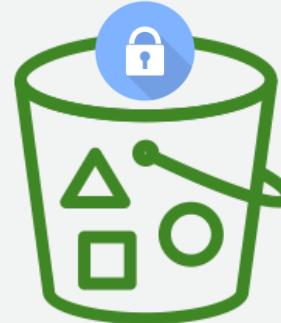
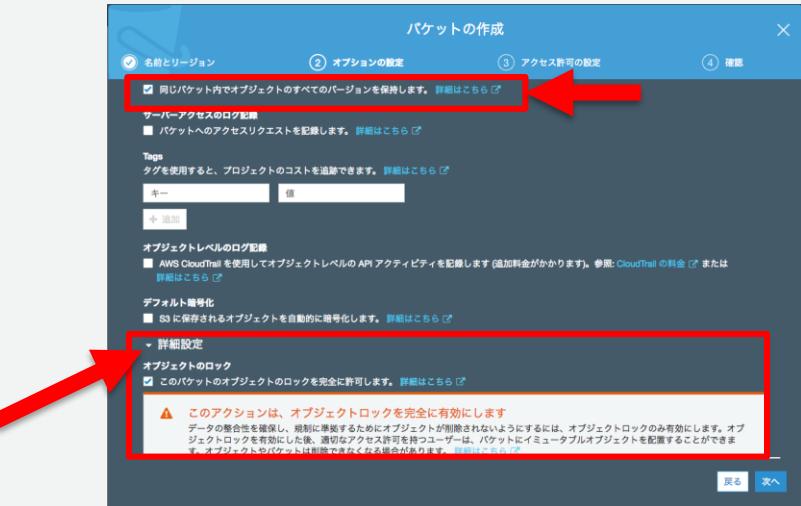
S3 Object Lock (WORM機能)

2018.11月

New

Write Once Read Many(WORM)モデルでのオブジェクト保存を提供する。そのオブジェクトに対する一定期間の上書き、または、削除ができないようロックする。

- Object Lockの有効化は、バケット単位で設定する（新規バケットのみ）
- 保護モード(Retention Mode)及び、保持期間(Retention Period)はバケット単位（デフォルトの設定になる）、または、オブジェクト格納時に明示指定する
- 保持期間とは、このロック（=削除できない状態）が有効な期間のこと
- もしくはリーガルホールド(Legal Hold)のON/OFFが可能
- バージョニングを併用するので、「見た目上の」削除や上書きの動きは妨げられない



例) 30日のRetention Period
(そのバケットに格納されるオブジェクトのデフォルトのロック保持期間が30日になる)

例) オブジェクト単位で、
60日間のロック保持期間



S3 Object Lock (WORM機能)(続き)

2種類の保護モード(Retention Mode)がある

Retention Mode	特徴
コンプライアンスマード (Compliance)	「コンプライアンス」の目的 rootアカウントですら削除ができない、また無効化ができない Cohasset Associates (*1)によるSEC 17a-4アセスメント済み
ガバナンスマード (Compliance)	ガバナンスの効いた「データ保護」 特別な権限(*2)(*3)で WORM保護されたオブジェクトの削除が可能 コンプライアンスマードに変更可能

(*1) <https://d1.awsstatic.com/r2018/b/S3-Object-Lock/Amazon-S3-Compliance-Assessment.pdf>

(*2) S3 Object Lockのアクセス許可

オペレーション	必要なアクセス許可
オブジェクトバージョンのRetention Modeや期間を作成、変更	s3:PutObjectRetention
オブジェクトバージョンに対して、Legal Holdを作成、変更	s3:PutObjectLegalHold
オブジェクトバージョンのRetention Modeや期間を取得	s3:GetObjectRetention
オブジェクトバージョンのLegal Holdの状態を取得	s3:GetObjectLegalHold
ガバナンスマードをバイパスする	s3:BypassGovernanceRetention
バケットのObject Lockの設定情報を取得	s3:GetBucketObjectLockConfiguration
バケットのObject Lockの設定を作成、変更	s3:PutBucketObjectLockConfiguration

マネジメントコンソールでの削除操作には x-amz-bypass-governance-retention:true のリクエストヘッダがつく



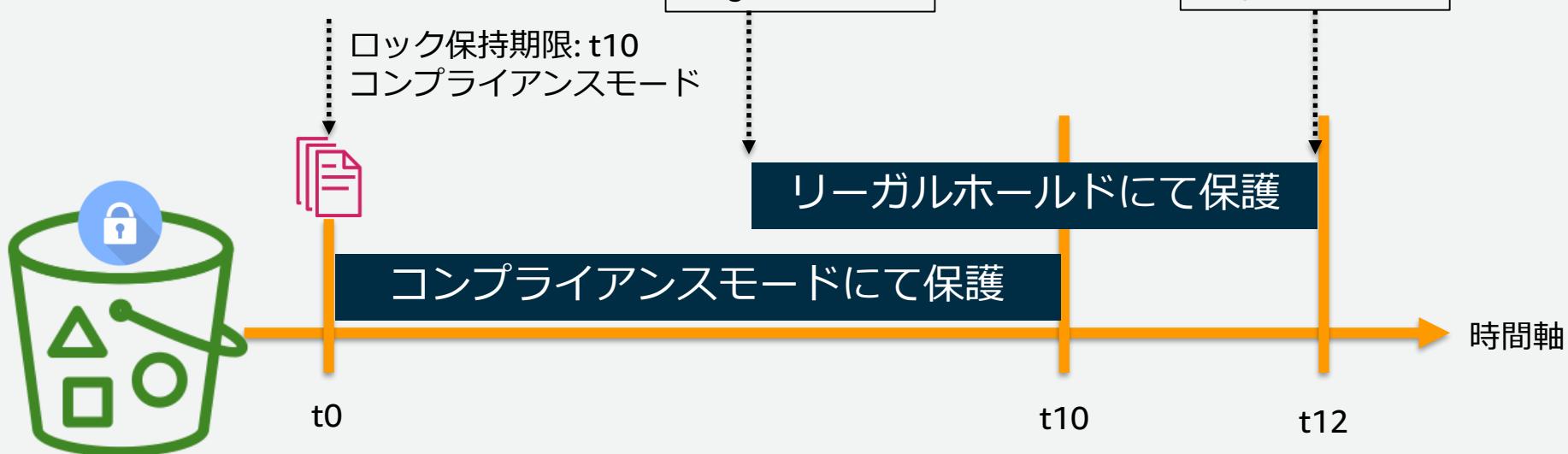
S3 Object Lock (WORM機能)(続き)

PUT Legal Hold

PUT

LegalHold=ON

LegalHold=OFF



S3 Object Lock
が有効なバケット



クロスリージョンレプリケーション

異なるリージョン間のS3バケットオブジェクトのレプリケーションを実施

- バケットに対するオブジェクトの作成、更新、削除をトリガーに非同期でレプリケーションを実行
 - 対象元バケットはバージョニングの機能を有効にする必要がある
 - バケットはそれぞれ異なるリージョンでなければならない
 - レプリケーション時は、リージョン間データ転送費用が発生
 - バケット、プレフィックス、オブジェクト単位でのレプリケーション
 - レプリケーション元、レプリケーション先でのストレージクラスの指定 ← 2018.11月
 - レプリケーション元でのObject Lockは利用できない
 - マルチアカウントでの利用（レプリケーション先でのオブジェクトオーナーの変更）

東京リージョン
S3 Standard



非同期レプリケーション

北米リージョン
S3 Glacier



New

2018.11月

Amazon S3の位置付け
Amazon S3の概要
Amazon S3へのアクセス
Amazon S3のデータ保護
Amazon S3のデータ管理

Amazon S3パフォーマンス最適化
Amazon S3の料金

Amazon S3のデータ管理

ストレージクラス

New

2018.11月

2019年予定



S3 Standard



S3 Intelligent-Tiering



S3 Standard-IA



S3 One Zone-IA



S3 Glacier



S3 Glacier Deep Archive

- ・アクティブ、頻繁にアクセスするデータ
- ・ミリ秒アクセス
- ・ ≥ 3 AZ
- ・\$0.0210/GB~

- ・変化するアクセスパターンのデータ
- ・ミリ秒アクセス
- ・ ≥ 3 AZ
- ・\$0.0210~\$0.0125/GB
- ・オブジェクト毎の管理料金
- ・最低保定期限

- ・低頻度アクセスデータ
- ・ミリ秒アクセス
- ・ ≥ 3 AZ
- ・\$0.0125/GB~
- ・GB毎の取り出し料金
- ・最低保定期限
- ・最小オブジェクトサイズ

- ・再作成可能な低頻度アクセスデータ
- ・ミリ秒アクセス
- ・1 AZ
- ・\$0.0100/GB~
- ・GB毎の取り出し料金
- ・最低保定期限
- ・最小オブジェクトサイズ

- ・アーカイブデータ
- ・分~時間アクセス
- ・ ≥ 3 AZ
- ・\$0.0040/GB~
- ・GB毎の取り出し料金
- ・最低保定期限

- ・アーカイブデータ
- ・時間アクセス
- ・ ≥ 3 AZ
- ・\$0.00099/GB~
- ・GB毎の取り出し料金
- ・最低保定期限

30日以上

30日以上、128KB以上

90日以上

いずれもできるだけサイズの「大きな」オブジェクトでの利用が良い



ライフサイクル管理

バケット内のオブジェクトに対して、ストレージクラスの変更や、削除処理に関する自動化

- バケット全体もしくはPrefixに対して、オブジェクトの更新日をベースに日単位での指定が可能
- 最大1,000までLifecycleのルールを設定可能
- 毎日0:00UTCに処理がキューイングされ順次実行
- Lifecycleを利用してIAに移動できるのは128KB以上のオブジェクトのみでそれ以外はIAに移動されない
- STANDARD-IA・アーカイブおよび削除の日程をそれぞれ指定した組み合わせも可能
- マルチアップロード処理で完了せず残った分割ファイルの削除にも対応
- MFA delete が有効なバケットにはライフサイクル設定は不可



ライフサイクルルール

① 名前とスコープ ② 移行 ③ 有効期限 ④ 確認

ストレージクラスの移行

ライフサイクルの設定にルールを追加して、別のストレージクラスにオブジェクトを移行する
ように Amazon S3 に指定できます。 詳細はこちら [\[?\]](#)

現行バージョン 以前のバージョン

オブジェクトの現行バージョン + 移行を追加する

オブジェクト作成 オブジェクト作成からの日数

標準- IA への移行の期限

標準- IA への移行の期限

インテリジェントへの移行の期限

ゾーン - IA への移行の期限

Amazon Glacier への移行の期限

30 X

戻る 次へ

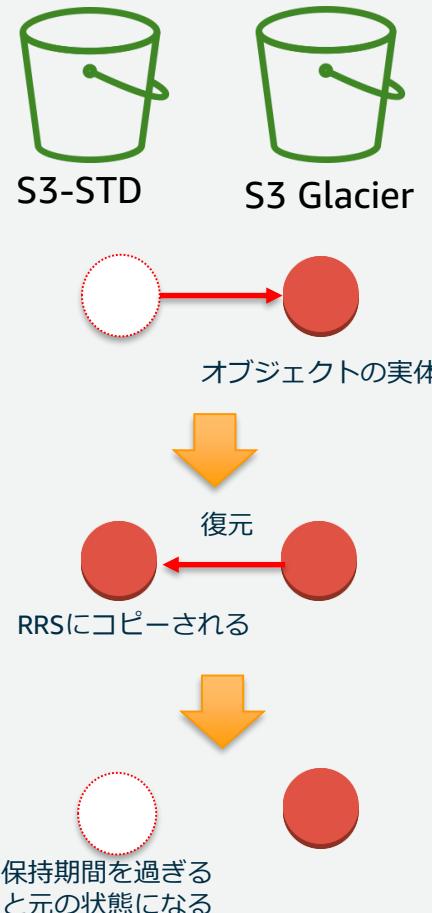
S3 Glacierへのアーカイブと復元

アーカイブ

- オブジェクトのデータはS3 Glacierに移動(アーカイブ後、マスターはS3 Glacierとなる)
- オブジェクトを S3 Glacierに直接PUTが可能 **New** 2018.11月
- S3上のデータを削除することで、S3 Glacier側のデータも削除される
- S3には8KBのオブジェクト名とメタデータのみが保管
- S3 Glacierには32KBのインデックスおよび関連メタデータが追加で保管
- アーカイブしたオブジェクトを90日以内に削除しても、90日間アーカイブされたのと同じ課金対象

オブジェクトの復元 restore

- オブジェクト毎に復元
- オブジェクト復元時(復元開始と復元完了)のNotification **New** 2018.11月
- データは一時的にS3の低冗長化ストレージに指定日数間複製される
- 復元後の、S3上での保持期間の変更も可能
- 復元にかかる時間について、3種類から選択可能
- 復元期間中は、S3の低冗長化ストレージとS3 Glacier双方で課金



S3 Glacierへのアーカイブと復元 (続き)



S3 Glacier

- 復元リクエスト時に指定できる3つの選択肢

- Expedited:** 少ない数のファイルについて、緊急のアクセスを要する場合の取得
- Standard:** 3-5時間の間にファイルを取得する標準的な取得
- Bulk:** 5-12時間の間にファイルを取得する最も低価格で、大量のデータを取得

- 復元リクエストのアップグレード

New

2018.11月

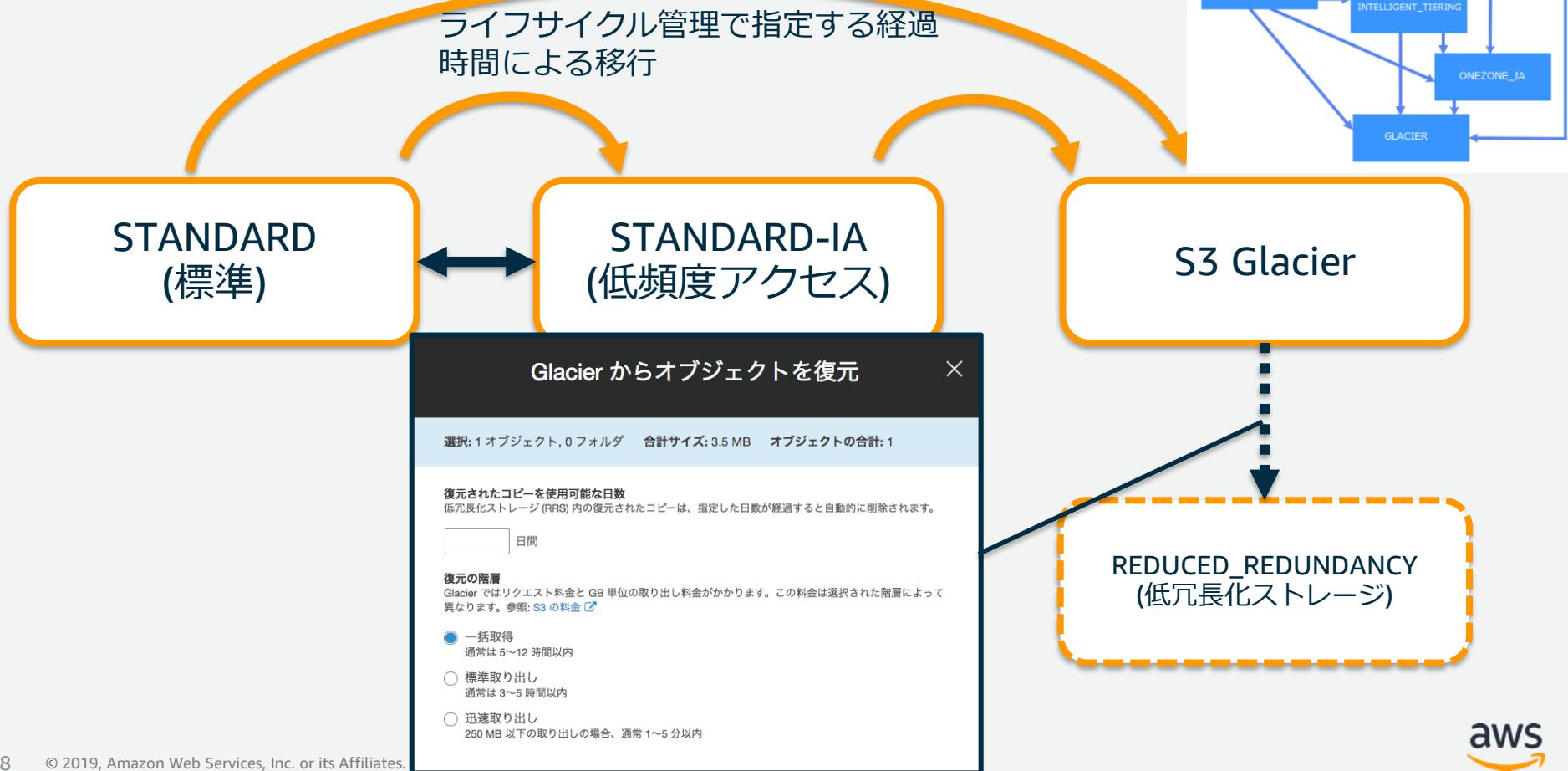
	迅速(Expedited)	標準(Standard)	大容量(Bulk)
データアクセス時間	1~5 分	3~5 時間	5~12 時間
データ復元容量	\$0.033 / GB	\$0.011 / GB	\$0.00275 / GB
復元リクエスト	オンデマンド: \$0.011 リクエストごと プロビジョンド: \$110 プロビジョンド キャパシティユニットごと(*)	\$0.0571 : 1,000 リクエストあたり	\$0.0275 : 1,000 リクエストあたり

(*)プロビジョンド=あらかじめデータを取り出すリソースを購入できる考え方
1プロビジョンドキャパシティユニット=5分間に、3回までのExpedited復元リクエスト、かつ、復元時スループットが150MB/sec以内

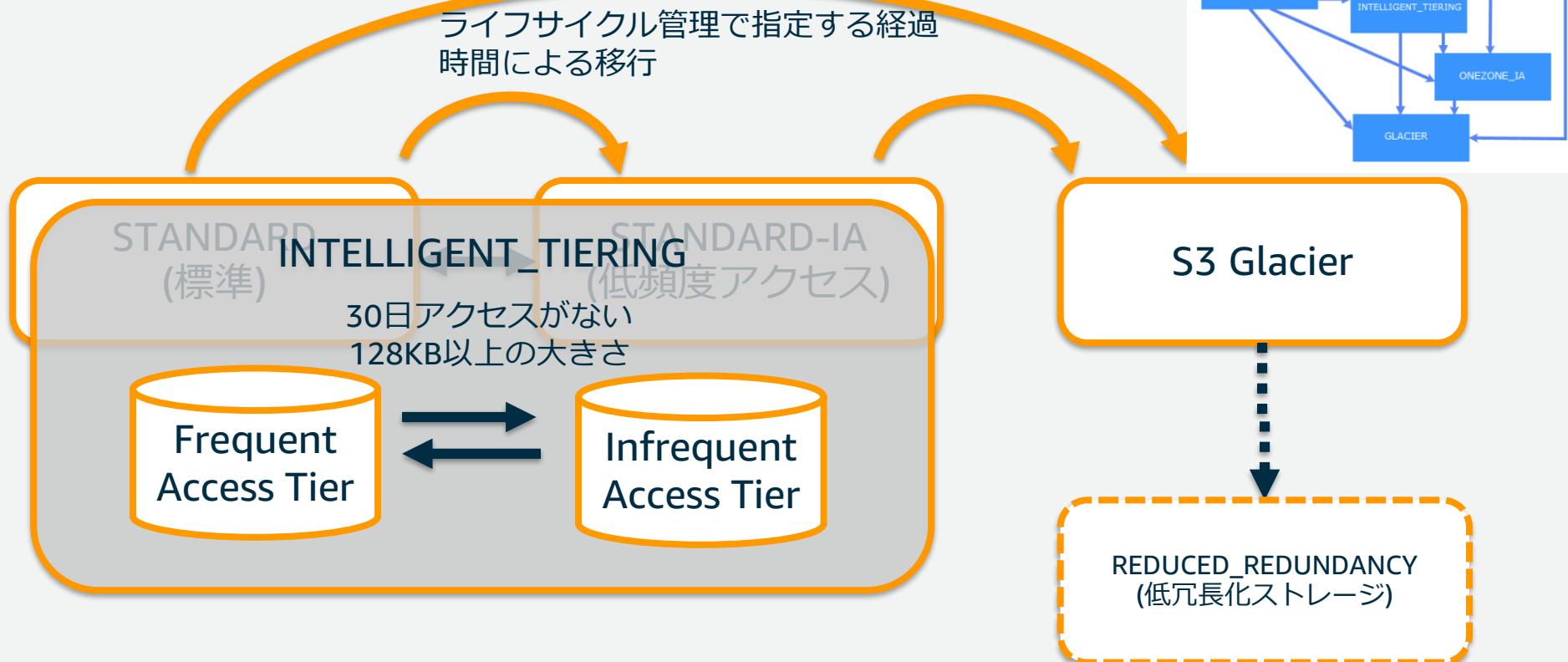
東京リージョン<https://aws.amazon.com/jp/glacier/pricing/>



ストレージクラス間のオブジェクト移動の整理



ストレージクラス間のオブジェクト移動の整理



S3 Analytics

「STANDARD-IAとS3 Glacierどちらににいつ移動すればいいのだろうか？」この疑問に応える、データのアクセスパターンの簡易可視化

開始方法

- 目的のバケットに対して、分析フィルターを定義する
- 結果がが出るまで、フィルター作成してから24~48時間ほど待つ

CSVでも結果を出力する場合→

The screenshot shows the AWS S3 Analytics console. At the top, there are tabs for 'オブジェクト', 'プロパティ', 'アクセス権限', and '管理'. The '管理' tab is highlighted with a red box. Below it, there are tabs for 'ライフサイクル', '分析' (which is also highlighted with a red box), 'メトリクス', and 'イベントリ'.

In the main area, there are two sections: '分析' and 'ストレージクラス分析'. The '分析' section contains a search bar 'フィルター/プレフィックス/タグを検索' and a 'フィルター (0)' button with a '+ 追加' button next to it. A red box highlights the '+ 追加' button. Below this, there's a 'フィルター名' input field with 'whole' typed in, and a 'モニクリングするプレフィックス/タグ (省略可)' dropdown with 'バケット全体の場合は未入力'. At the bottom of this section is a 'データのエクスポート (省略可)' button, which is also highlighted with a red box. There are '保存' and 'キャンセル' buttons at the very bottom.

To the right of the analysis section, there's a small icon of a magnifying glass over a bar chart, followed by the text 'ストレージクラス分析'. Below this, it says 'バケット全体、共有プレフィックス、またはタグに対して、ストレージクラス分析を有効にできます。Amazon S3 でアクセスパターンが分析され、オブジェクトのライフサイクルルールで標準 - IA に移行する期間の候補を提案します。' and a 'フィルターの追加' link.

http://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/analytics-storage-class.html



S3 Analytics (続き)

青が格納量、紫がどれだけそのデータが読まれたか？

この例の場合は、

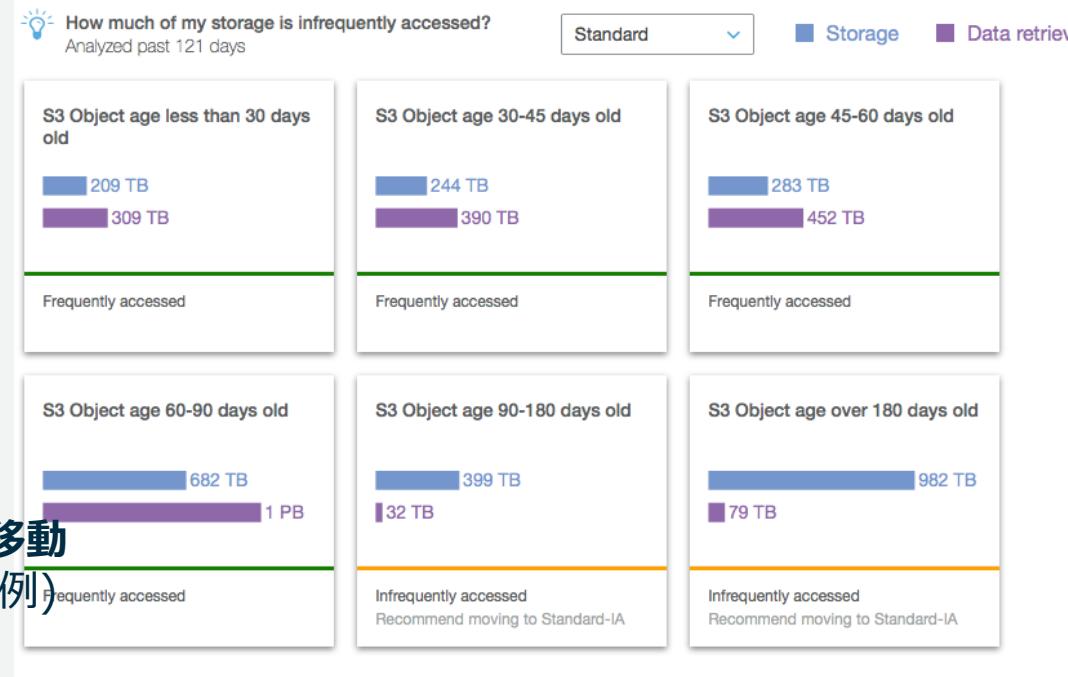
- 90日までのオブジェクトは、そこそこアクセスがある。
- 90日以降のオブジェクトのニーズが急に減っている。
- 90日以降でも、全くアクセスがないわけではない。
- 他のコンプライアンス要件などを加味したとして、、、



90日経過したデータをSTANDARD-IAへ移動

365日経過したデータをS3 Glacierへ移動(例)

5年経過したデータは削除(例)

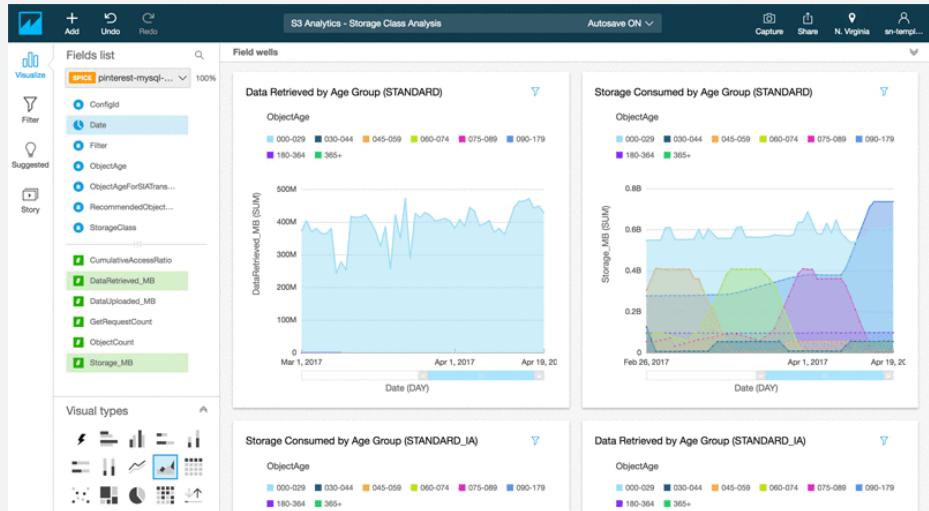




S3 Analytics を QuickSightでみる

Amazon QuickSight

S3管理コンソールの 管理->分析からたどる



もしくは、QuickSightのデータセット作成時
(New Dataset)でS3 Analyticsを選択

<https://aws.amazon.com/blogs/big-data/visualize-amazon-s3-analytics-data-with-amazon-quicksight/>



S3 インベントリ

S3に入っているオブジェクトのリストを、一気にCSVまたはORCファイルで取得する

- オブジェクトのリストを取得するにあたって、List Bucketの処理に時間や手間がかかる場合に有益
- スケジュール化（日単位・週1回）してレポートを取得
- 初回の結果が出るまで、48時間待つ
- ある時点のsnapshotとしてのPUT/DELETE（結果整合性）結果のインベントリリストとなる



http://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/storage-inventory.html



S3インベントリ (続き)

例) インベントリを取得したいバケット : sample-bucket-analytics-oregon

インベントリ名	フィルター	送信先バケット 	送信先プレフィックス	頻度
sample-inventory	プレフィックスでフィルター(省略)	redshift-bucket-toruyakio	s3inventory	週1回 

マニュフェストファイルの吐き出し先

destination-prefix/source-bucket/config-ID/YYYY-MM-DDTHH-MMZ/manifest.json
destination-prefix/source-bucket/config-ID/YYYY-MM-DDTHH-MMZ/manifest.checksum

この例の場合 :

s3://redshift-bucket-toruyakio/s3inventory/sample-bucket-analytics-oregon/sample-inventory/2017-02-14T15-02Z/manifest.json
s3://redshift-bucket-toruyakio/s3inventory/sample-bucket-analytics-oregon/sample-inventory/2017-02-14T15-02Z/manifest.checksum

インベントリリストの吐き出し先

destination-prefix/source-bucket/data/example-file-name.csv.gz

この例の場合

s3://redshift-bucket-toruyakio/s3inventory/sample-bucket-analytics-oregon/sample-inventory/data/0042fc70-0dee-4e0a-9fb5-92c639d1d93c.csv.gz

Bucket	Key	VersionID	IsLatest	IsDeleteMarker	Size	Last modified date	Etag	Storage Class	Replication Status
sample-bucket-analytics-oregon	bad_keys/00000002/2017-d2fPieFQm7		TRUE	FALSE	1024	2017-02-15T00:23:43.000Z	0f343b0931	STANDARD	COMPLETED
sample-bucket-analytics-oregon	bad_keys/00000002/2017-fnS18W.tD4h		TRUE	FALSE	1024	2017-02-15T00:24:05.000Z	0f343b0931	STANDARD	COMPLETED
sample-bucket-analytics-oregon	bad_keys/00000002/2017-sTsM3kb7E5		TRUE	FALSE	1024	2017-02-15T00:24:15.000Z	0f343b0931	STANDARD	COMPLETED
sample-bucket-analytics-oregon	bad_keys/00000002/2017-UZkmkdrqZH		TRUE	FALSE	1024	2017-02-15T00:23:54.000Z	0f343b0931	STANDARD	COMPLETED
sample-bucket-analytics-oregon	bad_keys/00000002/2017-kkxyNpUDpl8		TRUE	FALSE	1024	2017-02-15T00:25:53.000Z	0f343b0931	STANDARD	COMPLETED
sample-bucket-analytics-oregon	bad_keys/00000002/2017-Dhe37pgvHs		TRUE	FALSE	1024	2017-02-15T00:24:55.000Z	0f343b0931	STANDARD	COMPLETED
sample-bucket-analytics-oregon	bad_keys/00000002/2017-Oo8UjgBwcJ		TRUE	FALSE	1024	2017-02-15T00:25:09.000Z	0f343b0931	STANDARD	COMPLETED
sample-bucket-analytics-oregon	bad_keys/00000002/2017-ShlIN9n_agC		TRUE	FALSE	1024	2017-02-15T00:25:53.000Z	0f343b0931	STANDARD	COMPLETED
sample-bucket-analytics-oregon	bad_keys/00000002/2017-zxO8Q9dLe_		TRUE	FALSE	1024	2017-02-15T00:25:11.000Z	0f343b0931	STANDARD	COMPLETED
sample-bucket-analytics-oregon	bad_keys/00000002/2017-WaaQPOajq		TRUE	FALSE	1024	2017-02-15T00:26:17.000Z	0f343b0931	STANDARD	COMPLETED

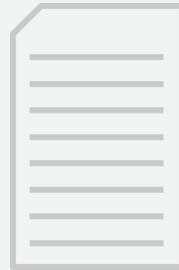


S3 バッチオペレーション(Preview)

New

数千、数百万、数十億のオブジェクトに対するAPIアクションを一括実行

オブジェクトの選択



- マニフェストファイル
- S3 インベントリ (CSV)
- CSVファイル

オペレーションの選択



- COPY (PUT Object Copy)
- S3 Glacierからのリストア
- PUT ObjectACL
- PUT Object Tagging
- Lambda関数の呼び出し



ジョブの作成

ジョブの進捗
ジョブの通知
ジョブの状態
完了レポート

S3 イベント通知



バケットにてイベントが発生した際に、Amazon SNS, SQS, Lambdaに対して通知することでシームレスなシステム連携が可能

イベントタイプ	概要
s3:ObjectCreated:*	S3バケットにオブジェクト作成された時 (PUT/POST/COPYのAPIがコールされた時)
s3:ObjectCreated:Put	
s3:ObjectCreated:Post	
s3:ObjectCreated:Copy	
s3:ObjectCreated:CompleteMultipartUpload	
s3:ObjectRemoved:*	S3バケットから、オブジェクトが削除された時 Delete = バージョニングされていないオブジェクトの削除、または バージョニングされているバケットのオブジェクトの完全な削除
s3:ObjectRemoved:Delete	
s3:ObjectRemoved:DeleteMarkerCreated	DeleteMarkerCreated = バージョニングされているオブジェクトの削除マーカ作成
s3:ObjectRestore:Post	S3 Glacierストレージクラスから復元の開始、完了した時
s3:ObjectRestore:Completed	
s3:ReducedRedundancyLostObject	低冗長化ストレージにてデータロストが発生した時

- Amazon SNS: メール送信, HTTP POST, モバイルPushなどのTopics実行
- Amazon SQS: キューメッセージの登録
- Amazon Lambda: 指定Lambda Functionの実行



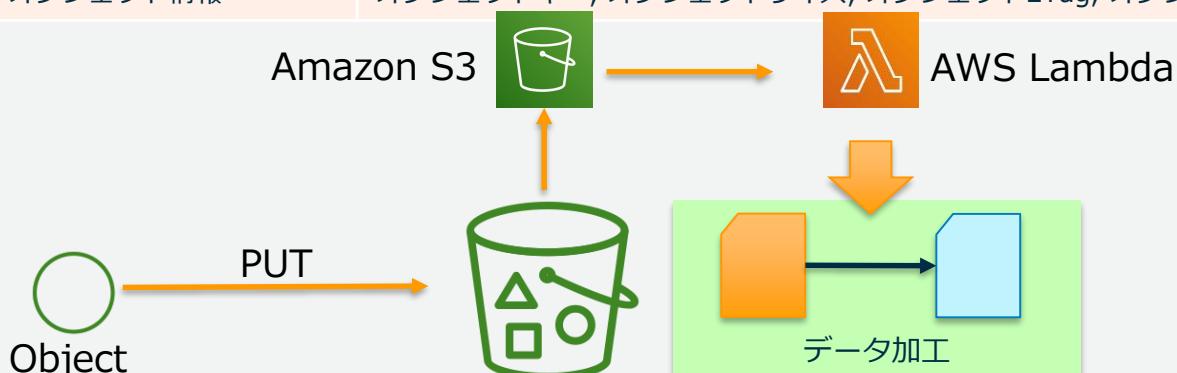
S3 イベント通知（続き）

S3からの実行権限の付与

- SNSおよびSQSはそれぞれのPolicyに対してS3からの実行権限を付与
- Lambdaに関しては、Lambdaが利用するIAM RoleにS3の権限を付与

イベントでの通知内容

	通知項目
共通情報	リージョン, タイムスタンプ, Event Type
リクエスト情報	Request Actor Principal ID, Request Source IP, Request ID, Host ID
バケット情報	Notification Configuration Destination ID, バケット名, バケットARN, バケットOwner Principal ID
オブジェクト情報	オブジェクトキー, オブジェクトサイズ, オブジェクトETag, オブジェクトバージョンID





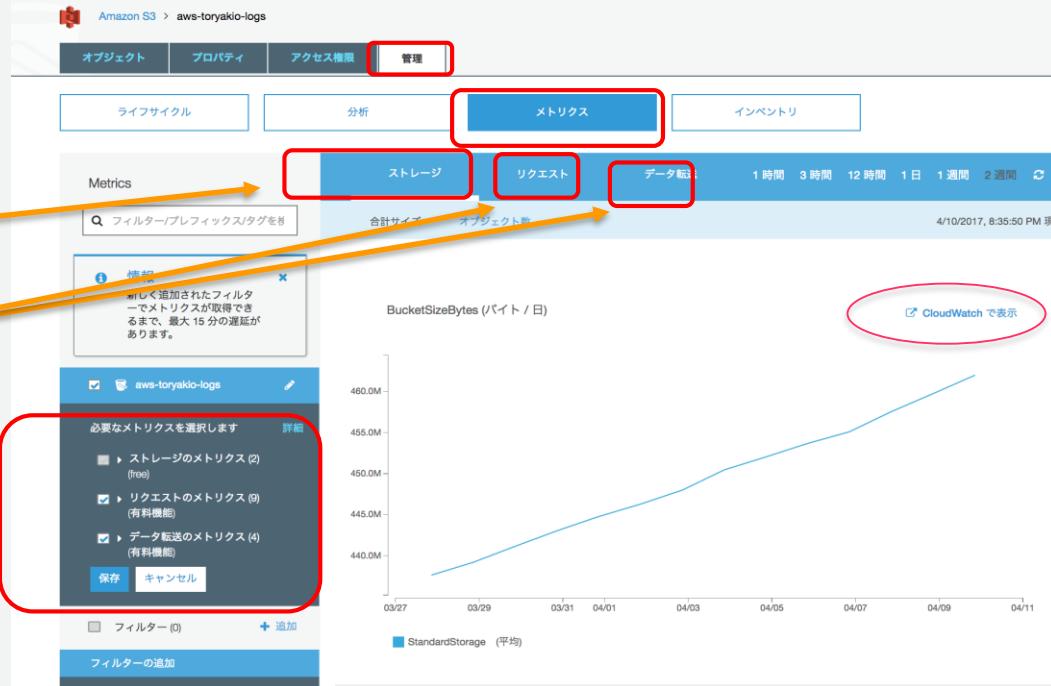
Amazon CloudWatch

Amazon CloudWatchによるメトリクス管理

- バケットに対するストレージメトリクス → 日単位
- オブジェクトに対するリクエストメトリクス → 分単位

ストレージメトリクス

リクエストメトリクス



https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/user-guide/configure-metrics.html



Amazon CloudWatchによるメトリクス管理（続き）



Amazon CloudWatch

New
S3 Glacier

ストレージメトリクス

- バケット単位および、Storage Typeごとにメトリクスを把握する
- 1日間隔でのレポート、状況把握（追加料金なし）

メトリクス	詳細
BucketSizeBytes	標準ストレージクラス、INTELLIGENT_TIERING、STANDARD IAストレージクラス、OneZone-IA、Glacier、または低冗長化ストレージ (RRS) クラスのバケットに保存されたバイト単位のデータ量
NumberOfObjects	すべてのストレージクラスのバケットに保存されたオブジェクトの総数

リクエストメトリクス

- タグやプレフィックスの指定にて細かい粒度での把握も可能
- 1分間隔でのメトリクスで、通常のCloudWatchの料金

New
S3 Select

メトリクス	単位	メトリクス	単位	メトリクス	単位
AllRequests	Count	SelectRequests	Count	BytesDownloaded	MB
PutRequests	Count	SelectScannedBytes	Bytes	BytesUploaded	MB
GetRequests	Count	SelectReturnedBytes	Bytes	4xxErrors	Count
ListRequests	Count				5xxErrors
DeleteRequests	Count				FirstByteLatency
HeadRequests	Count				ms
PostRequests	Count				TotalRequestLatency
					ms



AWS CloudTrailによるAPI管理



AWS CloudTrail

CloudTrailを有効にすることでS3への操作ログ(API Call)を収集することができる

いつ、どこから、誰がS3の操作を行ったか、コンプライアンスの目的で把握可能(S3 イベント通知との使い分けを意識)

CloudTrailでのイベント	操作
データイベント	GetObject, DeleteObject, PutObjectなどのS3のオブジェクトに対するAPI操作
管理イベント	S3のバケット操作はもちろん、その他のすべてのAPI操作

監査対象とは別のS3バケットを用意することを推奨

100,000イベントごとに、\$0.1の料金

ログに記録されるS3オペレーションは下記を参照

http://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/cloudtrail-logging.html

http://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/logging-management-and-data-events-with-cloudtrail.html



その他のモニタリングや管理に有効な機能

Logging

- ・ バケット単位でバケットに対するアクセスログの出力設定が可能
- ・ 出力先としてS3バケットを指定
- ・ ログフォーマットは下記を参照

http://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/LogFormat.html

Tag管理

- ・ バケット、オブジェクトに対してタグの指定が可能
- ・ タグ指定によりリソースグループにて関連するAWSサービスとの紐付けが可能
- ・ **オブジェクトに対してのタグ**は、ここまで紹介したライフサイクル、分析、モニタリング、クロスリージョンレプリケーション機能で活用可能



Amazon S3の位置付け
Amazon S3の概要
Amazon S3へのアクセス
Amazon S3のデータ保護
Amazon S3のデータ管理
Amazon S3パフォーマンス最適化
Amazon S3の料金

Amazon S3 パフォーマンス最適化



パフォーマンスの最適化

大きなサイズのファイルを快適に、ダウンロード、アップロード

GETリクエストについて、**RANGE GETを活用**することで、マルチスレッド環境では高速にダウンロードが可能

- マルチパートアップロード時と同じチャンクサイズを利用する



マルチパートアップロードの活用によるアップロード(PUT)オペレーションの高速化

- チャンクサイズと並列コネクション数のバランスが重要
 - 帯域が太い場合は**20MB-50MB**チャンクサイズから調整
 - モバイルや帯域が細い場合は**10MB程度**から調整





主にメディア

パフォーマンスの最適化（続き）

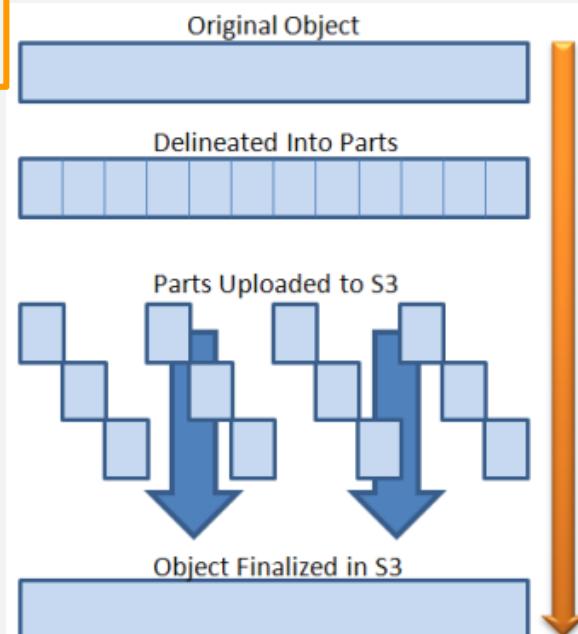
目安100MB以上のファイルのアップロードを快適にしたい場合のマルチパートアップロード機能

S3にアップロードする際に、ファイルを複数のチャunkに分割して並列アップロードを実施

- ・ ファイルが100MBを超える場合、利用することを推奨
- ・ 各チャunkは5GB以下に設定(5MB-5GB)
- ・ 全てのチャunkがアップロードされるとS3側で結合
- ・ Multipart Uploadを利用することで単一オブジェクトで5TBまで格納可能

各SDKにてMultipart Uploadの機能は実装済みAWS CLIの場合は、ファイルサイズを元に自動的に判別PUT処理を並列化することでのスループット向上を期待→広帯域ネットワークが重要

http://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/mpuoverview.html
<http://docs.aws.amazon.com/cli/latest/topic/s3-config.html>



S3 Transfer Acceleration

AWSのマネージドバックボーンネットワークを活用した高速ファイル転送手法

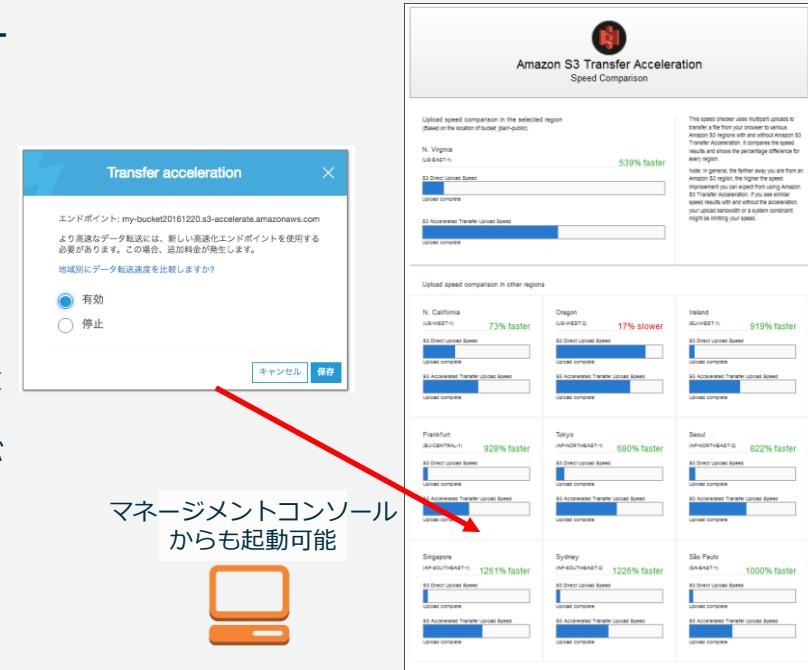
全世界149箇所(*)にあるAWSのエッジネットワークから、最適化されたAWSのネットワークを経由して、高速にAmazon S3とのデータ転送を実現

- 利用者は自動的に最短のエッジネットワークに誘導

S3 Bucketに対してAccelerationを有効化

- S3へのアクセスエンドポイントを変更するだけで利用可能
- Acceleration有効後、転送速度が高速化されるまでに最大30分かかる場合がある
- バケット名はピリオド"."が含まれない名前にする必要がある
- IPv6 (dualstack)エンドポイントも指定可能

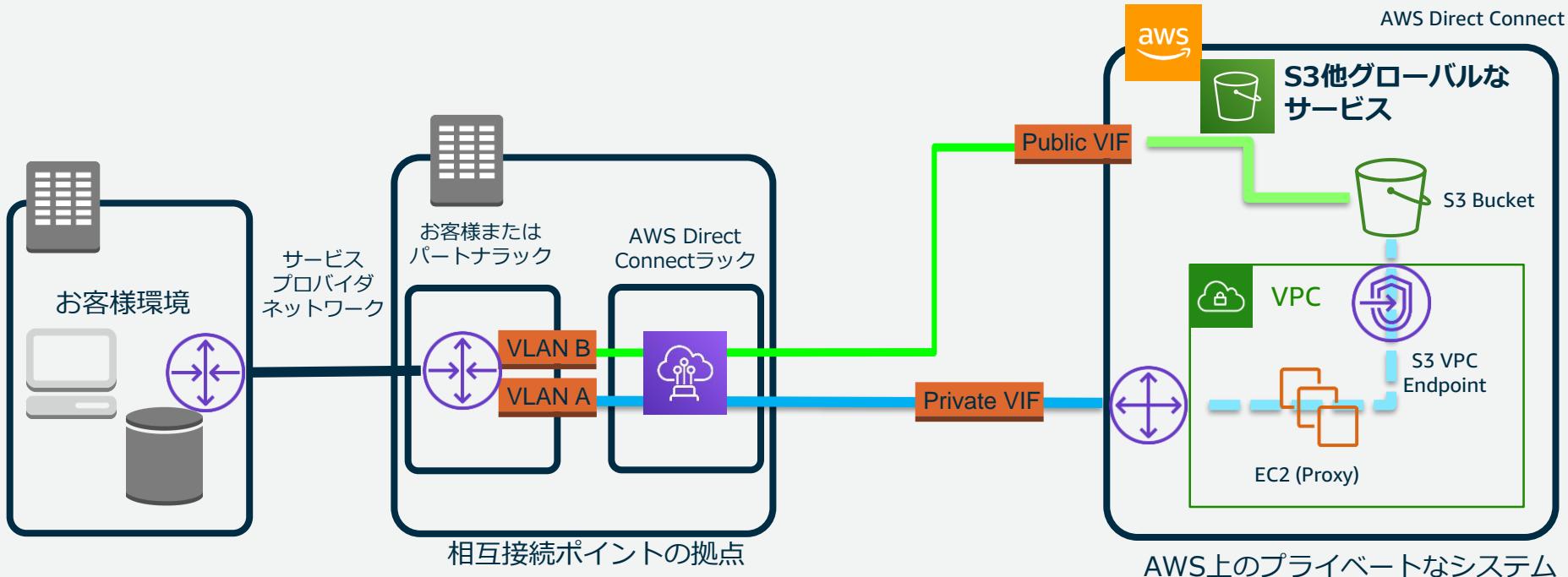
利用している端末からの無料スピード測定ツールも提供



<http://s3-accelerate-speedtest.s3-accelerate.amazonaws.com/en/accelerate-speed-comparsion.html>



S3 と Direct Connect



- 1) お客様環境と VPC への専用線による接続 (Private接続)
- 2) AWS のグローバルなサービスとの専用線による接続(Public接続)



S3 Select

Amazon S3 に格納されているオブジェクトに対して、SQL式にて、一部分のみを抽出できる



オブジェクト全体を取得して、
アプリケーションにて、
抽出する



価格、速度でのメリット

↓

アプリケーションが、S3
Select を利用して、オブ
ジェクトの一部のみを取得
する

S3 Select (続き)

- Input : フォーマットはCSV, JSON、圧縮(GZIP,BZIP3), 暗号化(SSE)
- Output: CSV, JSON
- SDK: Java, Python(boto3), Ruby, Go, .NET, JavaScript

句	データタイプ	オペレータ	関数
Select	String	Conditional	String
From	Integer, Float, Decimal	Math	Cast
Where	Timestamp	Logical	Math
	Boolean	String (Like,)	Aggregate

制約など: <https://docs.aws.amazon.com/AmazonS3/latest/dev/selecting-content-from-objects.html>

SQLリファレンス : <https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-glacier-select-sql-reference.html>

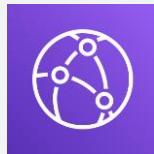


リクエストレート

Amazon S3 は、自動的にスケールするよう設計されています。データの追加操作で最大 3,500 リクエスト/秒の、データの取得操作で最大 5,500 リクエスト/秒をサポートできるようにパフォーマンスを向上させています。

重要

大量のGETリクエストが発生するワークフローの場合は、Amazon CloudFrontを併用することを推奨



Amazon
CloudFront



Amazon S3

定常的にS3バケットへのPUT/LIST/DELETEリクエストが3,500 RPSを超える、もしくはGETリクエストが5,500RPSを超える場合、キー名先頭部分の文字列をランダムにすることでレート向上が期待できるが、その必要性があるワークフローかどうかはよく見極める

```
examplebucket/2013-26-05-15-00-00/cust1234234/photo1.jpg  
examplebucket/2013-26-05-15-00-00/cust3857422/photo2.jpg  
...  
examplebucket/2013-26-05-15-00-01/cust1248473/photo4.jpg  
examplebucket/2013-26-05-15-00-01/cust1248473/photo5.jpg
```

ほとんどのユースケースでプレフィックスをハッシュする必要性はない

```
examplebucket/232a-2013-26-05-15-00-00/cust1234234/photo1.jpg  
examplebucket/7b54-2013-26-05-15-00-00/cust3857422/photo2.jpg  
...  
examplebucket/9810-2013-26-05-15-00-01/cust1248473/photo4.jpg  
examplebucket/c34a-2013-26-05-15-00-01/cust1248473/photo5.jpg  
...
```

<https://aws.amazon.com/jp/about-aws/whats-new/2018/07/amazon-s3-announces-increased-request-rate-performance/>

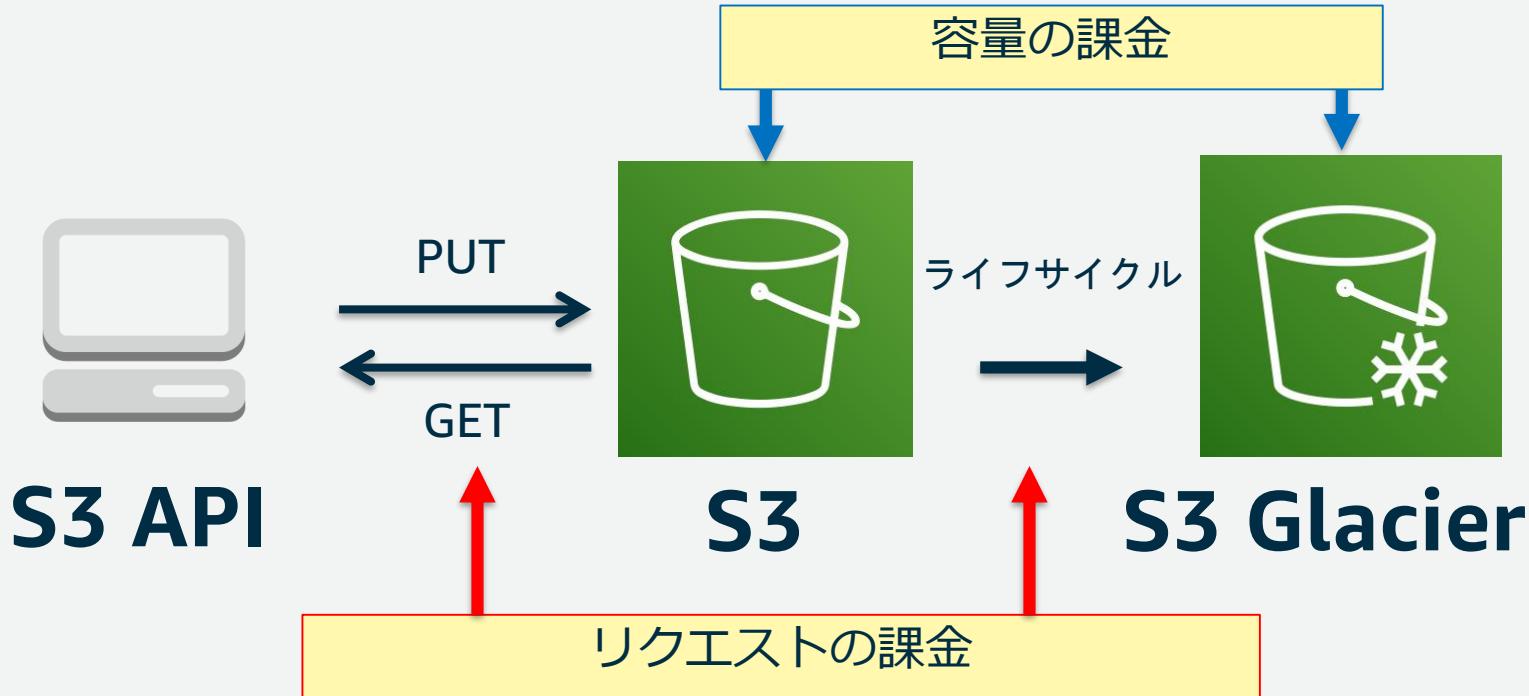


Amazon S3の位置付け
Amazon S3の概要
Amazon S3へのアクセス
Amazon S3のデータ保護
Amazon S3のデータ管理
Amazon S3パフォーマンス最適化
Amazon S3の料金



Amazon S3の料金

主に、容量の料金とオペレーションの料金



細かい多数のファイルを活用するユースケースは要注意
使用頻度が低いファイルは束ねる、など。

Amazon S3の料金

ストレージ料金

	スタンダード	STANDARD-IA(*)	S3 OneZone -IA	S3 Glacier
最初の50TB/月	\$0.025 / GB	\$0.019 / GB	\$0.0152 / GB	\$0.005 / GB
次の450TB/月	\$0.024 / GB	\$0.019 / GB	\$0.0152 / GB	\$0.005 / GB
500TB月以上	\$0.023 / GB	\$0.019 / GB	\$0.0152 / GB	\$0.005 / GB

(*) STANDARD-IAの請求対象となる最小オブジェクトサイズは 128 KB です。128 KB より小さいサイズのオブジェクトは、128 KBとして課金されます。

リクエスト料金

	スタンダード	INTELLIGENT_TIERING	STANDARD-IA	S3 OneZone -IA	S3 Glacier
PUT、COPY、POST、または LIST リクエスト	\$0.0047 : 1,000 リクエストあたり	\$0.0047 : 1,000 リクエストあたり	\$0.01 : 1,000 リクエストあたり	\$0.01 : 1,000 リクエストあたり	-
GET、SELECTおよび他のすべてのリクエスト	\$0.00037 : 1,000 リクエストあたり	\$0.00037 : 1,000 リクエストあたり	\$0.001 : 1,000 リクエストあたり	\$0.001 : 1,000 リクエストあたり	-
S3 Selectによって返されたデータ	\$0.0008 / GB	\$0.0008 / GB	\$0.01 / GB	\$0.01 / GB	Glacier Select
S3 Selectによってスキヤンされたデータ	\$0.00225 / GB	\$0.00225 / GB	\$0.00225 / GB	\$0.00225 / GB	Glacier Select
ライフサイクル移行リクエスト	-	\$0.01 : 1,000 リクエストあたり	\$0.01 : 1,000 リクエストあたり	\$0.01 : 1,000 リクエストあたり	\$0.0571 : 1,000 リクエストあたり
取り出し（容量）			\$0.01 / GB	\$0.01 / GB	Glacier取り出し料金 (slide 47)



Amazon S3 の料金(続き)

ストレージマネジメント料金

管理	料金
S3 Inventory	リストされるオブジェクト 100 万個ごとに \$0.0028
S3 Analytics Storage Class Analysis	モニターされるオブジェクト 100 万個ごとに月あたり \$ 0.10
S3 Object Tagging	10,000 タグごとに月あたりUS\$0.01
CloudWatch リクエストメトリクス	CloudWatch 料金
CloudTrail データイベント	100,000 件のイベントあたり \$0.1
S3 Intelligent-Tiering モニタリング、オート メーション	オブジェクト1,000件ごとに \$0.0025

データ転送料金

転送方向	価格
IN	\$0.000/GB
OUT (AWS Network)	同じリージョンのAmazon EC2
	別のAWSリージョン
	Amazon CloudFront
	\$0.000/GB
OUT (Internet)	最初の1GB/月
	10TBまで/月
	次の40TB/月
	次の100TB/月
	次の350TB/月
	350TB/月以上
	お問い合わせ

New
2018.9月

2019年2月時点の東京リージョン料金表
<http://aws.amazon.com/jp/s3/pricing/>



Amazon S3 の料金(続き)

S3 Transfer Acceleration料金

転送方向		価格
S3へのデータIN	米国、欧州、日本のエッジロケーションによる高速化	\$0.04/GB
	その他の国のエッジロケーションによる高速化	\$0.08/GB
S3からのデータOUT (Internet)	エッジロケーションによる高速化	\$0.04/GB
S3と別のAWSリージョン間	エッジロケーションによる高速化	\$0.04/GB

S3 Transfer Accelerationの費用は、S3のデータ転送コストとは別に加算されることに注意

S3 Transfer Accelerationを利用してデータを取り扱う場合、通常のS3との転送よりも高速であるかを確認します。通常の転送に比べTransfer Accelerationが高速でないと判断した場合は、Transfer Accelerationの料金は請求されず、Transfer Accelerationシステムをバイパスする可能性があります。

S3 無料枠(1年)

- 標準ストレージ 5GB
- 20,000 GETリクエスト / 2,000 PUTリクエスト

2019年2月時点の東京リージョン料金表
<http://aws.amazon.com/jp/s3/pricing/>



まとめ

まとめ

Amazon Simple Storage Service (S3)は、ユーザがデータを安全に、容量制限なく、データ保存が可能な、クラウド時代のオブジェクトストレージです。

- Amazon S3の位置付け
- Amazon S3の概要
- Amazon S3へのアクセス
- Amazon S3のデータ保護
- Amazon S3のデータ管理
- Amazon S3パフォーマンス最適化
- Amazon S3の料金

様々なAWSサービスと連携し、利用者のAWS利用を支えてくれるストレージ・データストア



AWS Well-Architected 個別技術相談会

毎週”W-A個別技術相談会”を実施中

- AWSのソリューションアーキテクト(SA)に
対策などを相談することも可能
- 申込みはイベント告知サイトから

(<https://aws.amazon.com/jp/about-aws/events/>)

AWS イベント で[検索]



ご視聴ありがとうございました



Amazon Simple Storage Service (Amazon S3)

入門編

佐藤 真也

Amazon Web Service Japan G.K.

Solutions Architect

2022/12

AWS Black Belt Online Seminarとは

- ・ 「サービス別」「ソリューション別」「業種別」などのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- ・ AWSの技術担当者が、AWSの各サービスやソリューションについてテーマごとに動画を公開します
- ・ 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます
- ・ 以下のURLより、過去のセミナー含めた資料などをダウンロードすることができます
 - ・ <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>

内容についての注意点

- ・ 本資料では2022年12月時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(<https://aws.amazon.com/>)にてご確認ください
- ・ 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます
- ・ 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます

自己紹介

名前：佐藤 真也 (Sato Shinya)

所属：アマゾン ウェブ サービス ジャパン合同会社
技術統括本部 金融ソリューション本部
保険ソリューション部

好きなAWSサービス：

- AWS Snowball Edge
- Amazon Simple Storage Service (S3)
- Amazon FSx シリーズ



本セミナーの対象者

前提知識

- AWS のグローバルインフラストラクチャやフルマネージドサービスの概念
- AWS IAM、Amazon VPC などの基盤となるサービスの基本的な知識

対象者

- これから AWS を利用される方
- Amazon S3 の基本を押さえたい方
- Amazon S3 を深く知るための最初の一歩を踏み出したい方

注意: Amazon S3 Glacier については本資料では紹介しません。

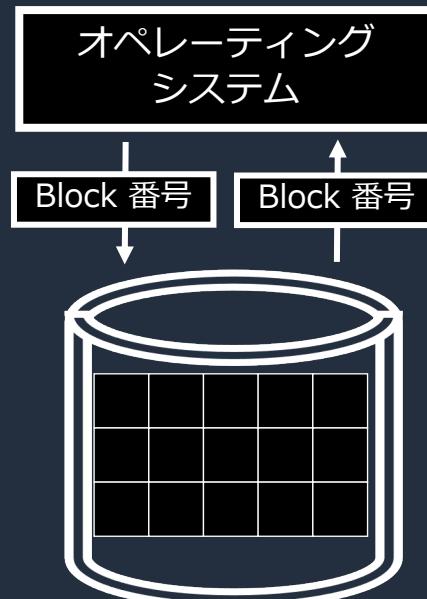
アジェンダ

1. Amazon S3 とは
2. Amazon S3 を理解するための 8 つのポイント
3. Amazon S3 にオブジェクトをアップロードする方法
4. まとめ

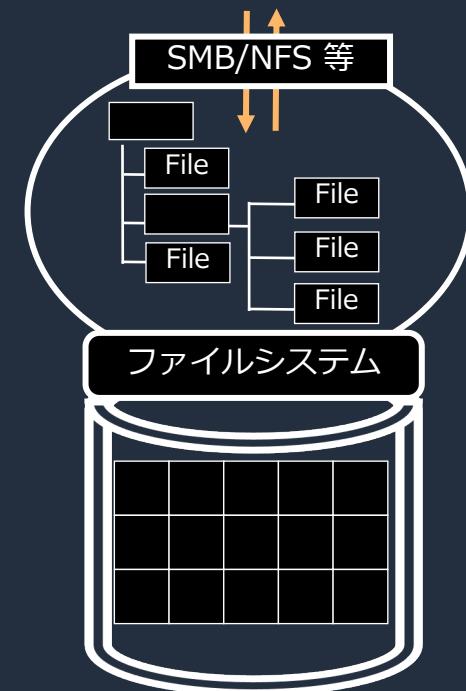
Amazon S3 とは

3つのストレージタイプ

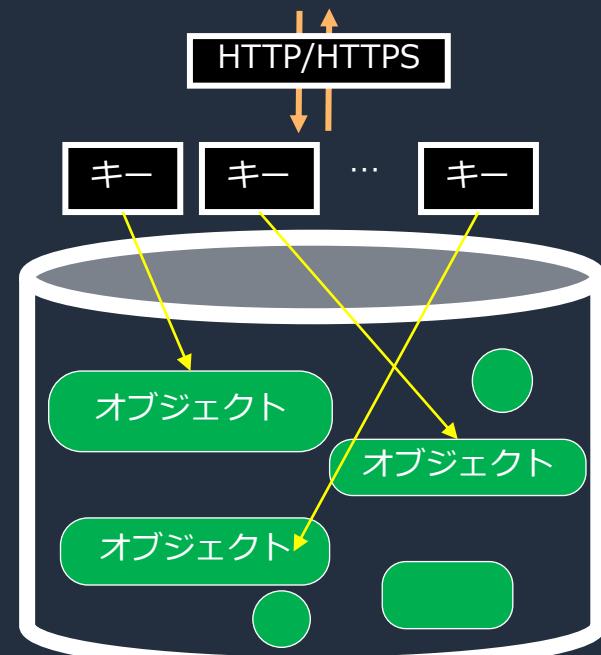
ブロックストレージ
主に SCSI でアクセス
低レイテンシ



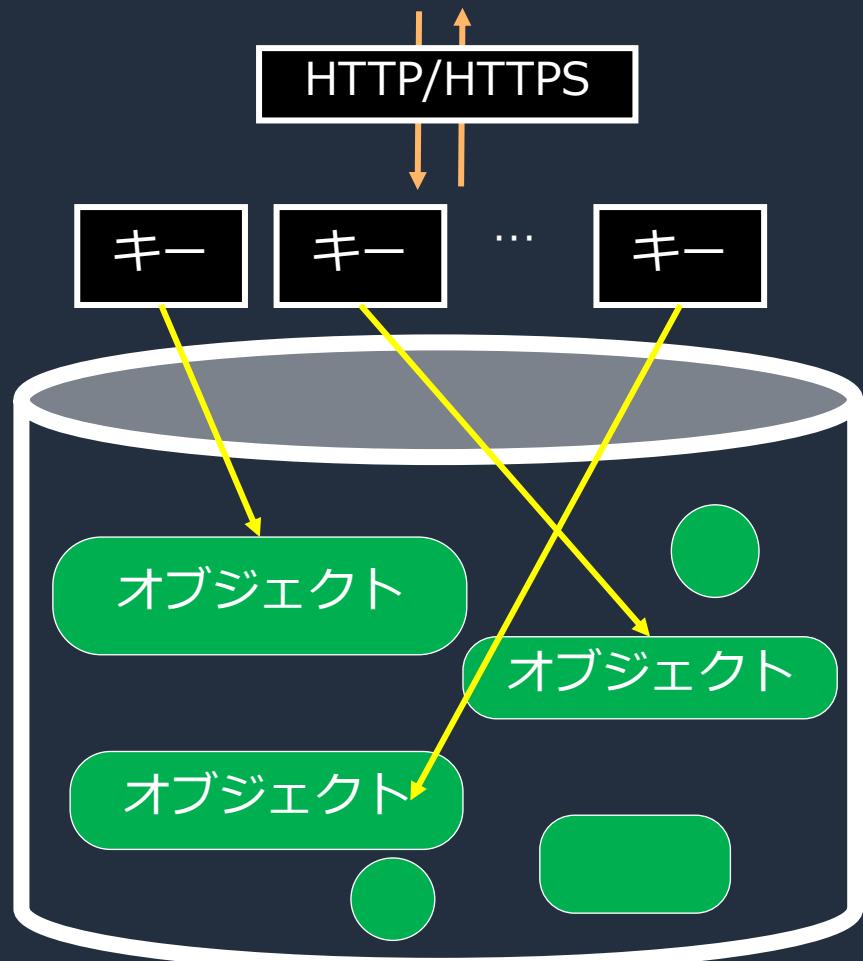
ファイルストレージ
主に SMB/NFS でアクセス
階層構造・ファイル共有システム



オブジェクトストレージ
主に HTTP/HTTPS でアクセス
大容量のデータ保存



オブジェクトストレージとは



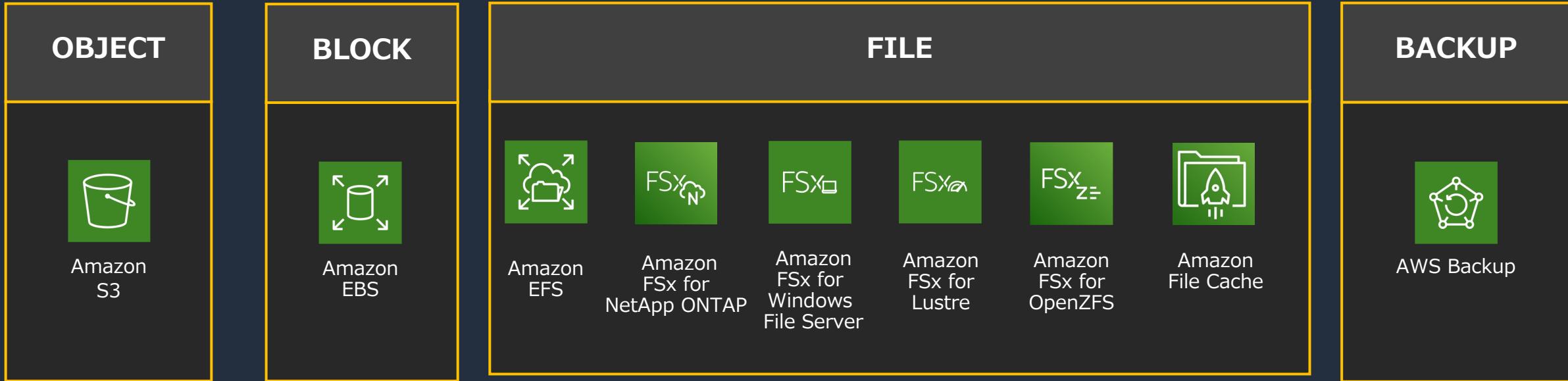
特徴

- HTTP/HTTPS でアクセス
- 一意のキーに対するオブジェクト（データ）が存在
- 階層構造を取るファイルストレージとは異なり、フラットな構造

メリット

- スケールが容易で、大容量のデータ保存が可能
- オブジェクト単位でのアクセス制御
- 高い可用性と耐障害性
- 独自にカスタマイズできるメタデータを追加可能

AWS のストレージサービス



DATA TRANSFER AND MIGRATION



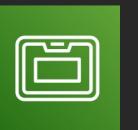
AWS Storage
Gateway



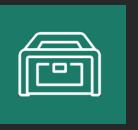
AWS DataSync



AWS Transfer
Family



AWS Snowball



AWS Snowcone

Amazon S3 とは

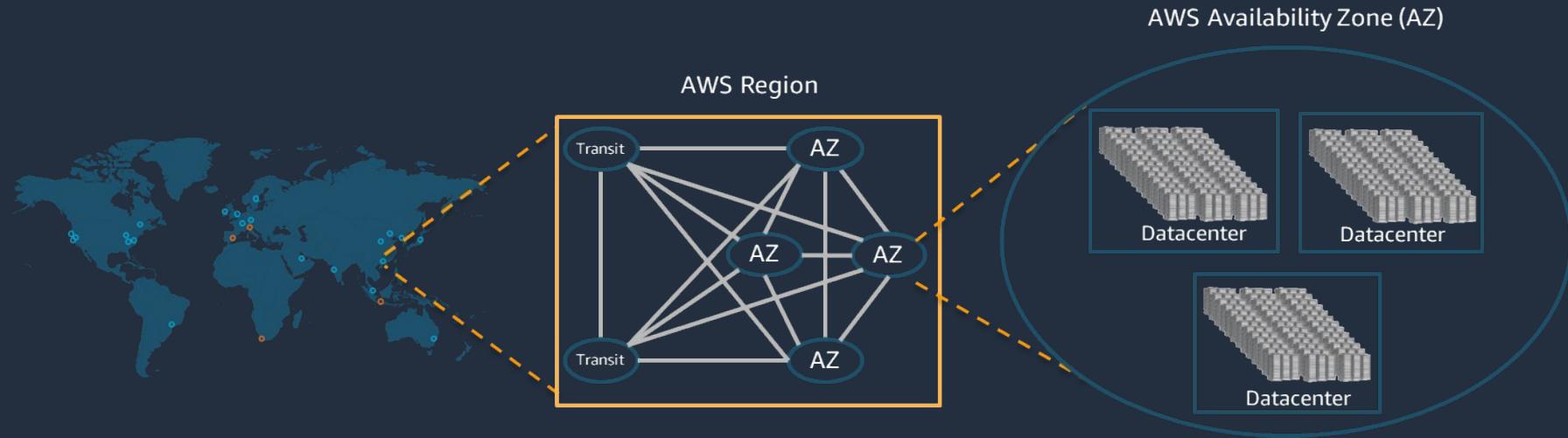
高いパフォーマンスと可用性、そして低コストが特徴なオブジェクトストレージ
2006 年に登場してから、現在に至るまでのイノベーションが積み重なった歴史あるサービス

- 耐久性
 - 99.99999999% (イレブンナイン)
 - 最低 3 つのアベイラビリティゾーン (AZ) で冗長化
- スケーラビリティ
 - 無制限のデータ保存
 - ただし、1 オブジェクトは最大 5 TB
- 低コスト
- セキュリティ
 - アクセス制御とログ監査
- データの保護
 - 誤削除から守る機能
- アクセシビリティ
 - HTTP/HTTPS でアップロード/ダウンロード/変更/削除といった操作が可能
- 様々な AWS サービスとの連携



Amazon S3 の特徴などは FAQ にて詳解: <https://aws.amazon.com/jp/s3/faqs/?nc=sn&loc=7>

Amazon S3 を支えるグローバルインフラストラクチャ



- 99.99999999% のデータ耐久性
 - 1000 万のオブジェクトが格納されている場合、1 つのオブジェクトが損失するケースは平均して 1 万年に一度
- 最低 3 つのアベイラビリティゾーン (AZ) で冗長化

Amazon S3 のセキュリティ



転送中と保管時における
データの暗号化



ユーザーベース/リソースベースの
ポリシーによるアクセス制御



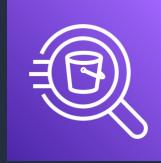
AWS CloudTrail
と連携し API コールの記録

様々な AWS サービスとの連携

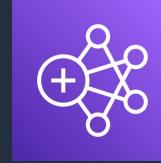


Amazon S3

分析系サービスのデータソースに使う



Amazon Athena



Amazon EMR

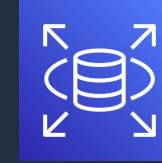


Amazon Redshift

スナップショットを S3 に保存する



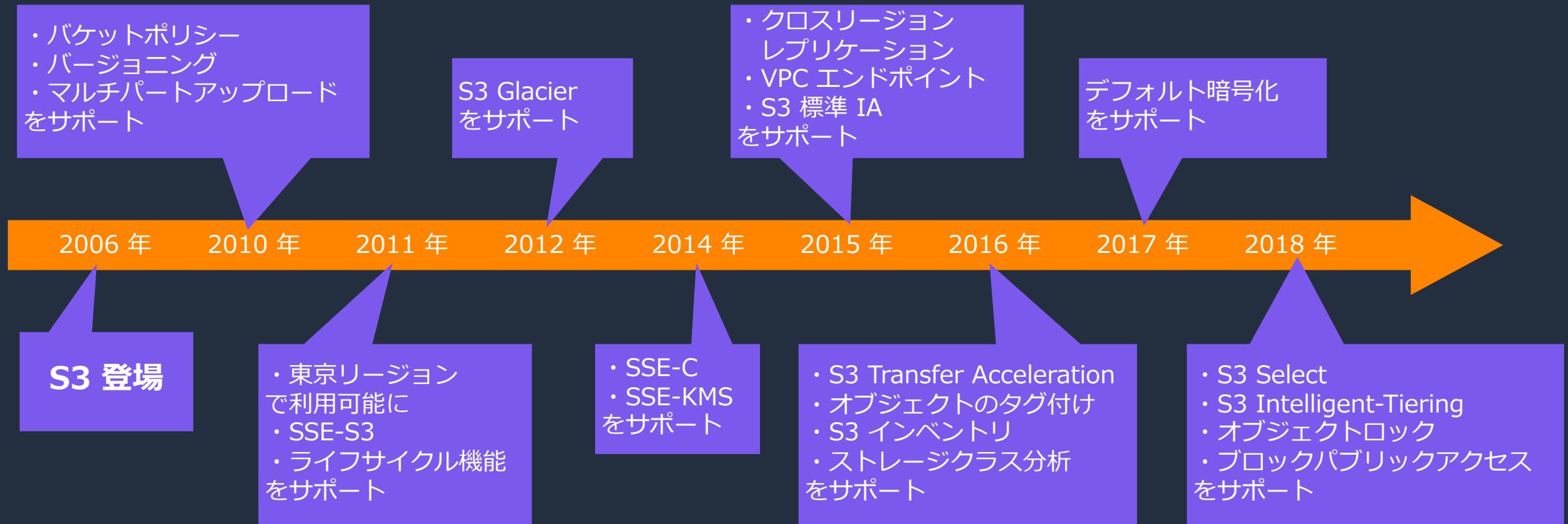
Amazon Elastic Block Store



Amazon Relational Database Service

他にも様々な AWS サービスと連携して、コンテンツ配信やデータレイクとしての活用など、多様なワークフローに利用できる

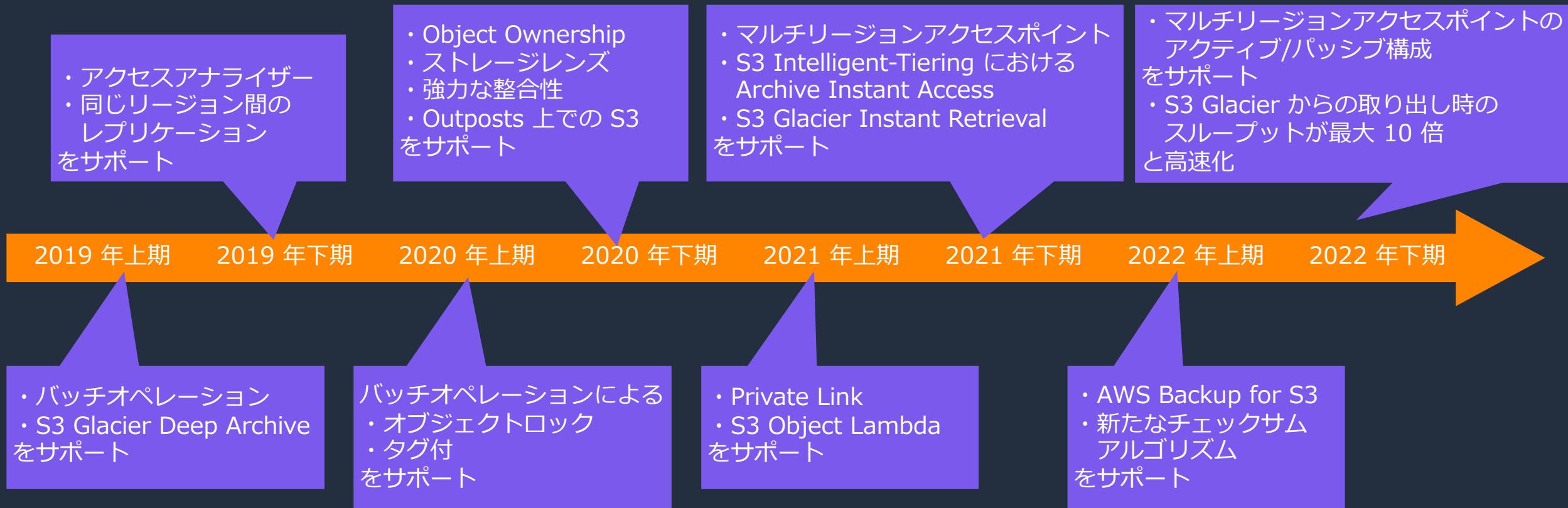
Amazon S3 の 2018 年までの主要アップデート



Amazon S3 の 2019 年以降の主要アップデート



Amazon S3



Amazon S3 を理解する ための 8 つのポイント

Amazon S3 を理解するための 8 つのポイント

1. バケット
2. オブジェクト
3. フォルダ
4. プレフィックス
5. 強力な整合性
6. Amazon S3 のストレージクラス
7. コスト
8. Amazon S3 のアーキテクチャ

1. バケット



バケットとは？

- オブジェクトを保存する入れ物
- 1つのアカウントで最大 100 個まで作成可能で、増加リクエストができる
- 中国/GovCloud リージョンを除く全てのリージョンで、バケット名は一意でなければならない
- バケットの命名規則
 - 3~63 文字で構成する
 - 小文字、数字、ドット (.) 、ハイフン (-) のみ使用できる
 - バケット名は小文字または数字で開始/終了する
 - バケット名は xn-- から開始しない
 - バケット名は -s3alias で終了しない
 - 連続する 2 つのドットを含めない
 - IP アドレスの形式 (192.168.0.2 など) にしない

バケットの命名規則の詳解やバケット名の例: https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/bucketnamingrules.html

2. オブジェクト (1)

オブジェクトとは？

- ・ ファイルとそのファイルを記述する任意のメタデータ
- ・ キーを用いてバケット内のオブジェクトを識別
- ・ 最大サイズは 5 TB

shinya-sato-bb-demo 情報

オブジェクト

オブジェクト (1)

オブジェクトは、Amazon S3 に保存された基本的なエンティティです。Amazon S3 インベントリにアクセスできるためには、明示的にアクセス権限を付与する必要があります。詳細

C S3 URI をコピー URL をコピー ダウンロード

アップロード

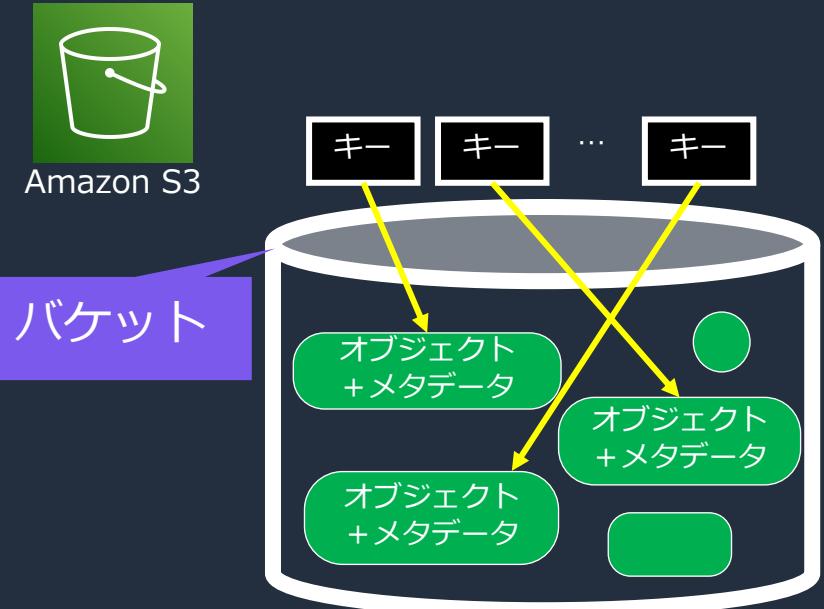
名前 プレフィックスでオブジェクトを検索

hoge/ dummy.txt fuga/

名前

dummy.txt

dummy.txt 情報



「shinya-sato-bb-demo」がバケット
hoge/dummy.txt がキー

オブジェクトの詳解: https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/UsingObjects.html
オブジェクトキーの詳解: https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/object-keys.html

2. オブジェクト (2)



オブジェクトのメタデータ

- ・アップロード時のみメタデータの設定ができる。
- ・アップロード後にメタデータを編集する場合、**更新されたメタデータを持つオブジェクトのコピーが作成され、上書きが発生する**。メタデータのみの編集であってもオブジェクトの最終更新日が更新される。

A screenshot of the AWS S3 Object Metadata configuration interface. The title bar says "メタデータ" (Metadata). Below it, a sub-header states: "メタデータは、名前-値(キーと値)のペアとして提供されるオプションの情報です。詳細" (Metadata is optional information provided as key-value pairs). The main area shows a table with columns: "タイプ" (Type), "キー" (Key), and "値" (Value). There are two rows: one row with "システム定義" (System-defined) selected in the Type dropdown, "Content-Type" in the Key dropdown, and "binary/octet-stream" in the Value input field; and another row with "タイプの選択" (Select type) in the Type dropdown, "キーの選択" (Select key) in the Key dropdown, and an empty Value input field. Buttons for "削除" (Delete) and "追加" (Add) are also visible.

オブジェクトのメタデータの詳解: https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/add-object-metadata.html

3. フォルダ

- オブジェクトを階層構造に見せることができる（実際にはフラット）
- shinya-sato-bb-demo/hoge/fuga/dummy.txt の場合
 - shinya-sato-bb-demo がバケットで、hoge と fuga がフォルダ



フォルダの詳解: https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/using-folders.html

4. プレフィックス

Amazon S3 > パケット > shinya-sato-bb-demo > hoge/ > fuga/ > dummy.txt

dummy.txt 情報

S3 URI をコピー ダウンロード 開く オブジェクトアクション ▾

- ・ プレフィックスとは、オブジェクトに対するキーの先頭から任意の長さを指定可能な文字列で、**パーティションとして機能**
- ・ shinya-sato-bb-demo/hoge/fuga/dummy.txt というオブジェクトの場合、
 - ・ キーは「hoge/fuga/dummy.txt」
 - ・ プレフィックスは
 - ・ ho でも
 - ・ hoge/fug でも
 - ・ hoge/fuga/dummy.txt でも指定可能
- ・ フォルダでは"/"は配下のフォルダを示す一方、プレフィックスでは単なる文字列

プレフィックスの詳解: https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/using-prefixes.html

フォルダとプレフィックスの違いについての解説: https://aws.amazon.com/jp/premiumsupport/knowledge-center/s3-prefix-nested-folders-difference/?nc1=h_ls

5. 強力な整合性

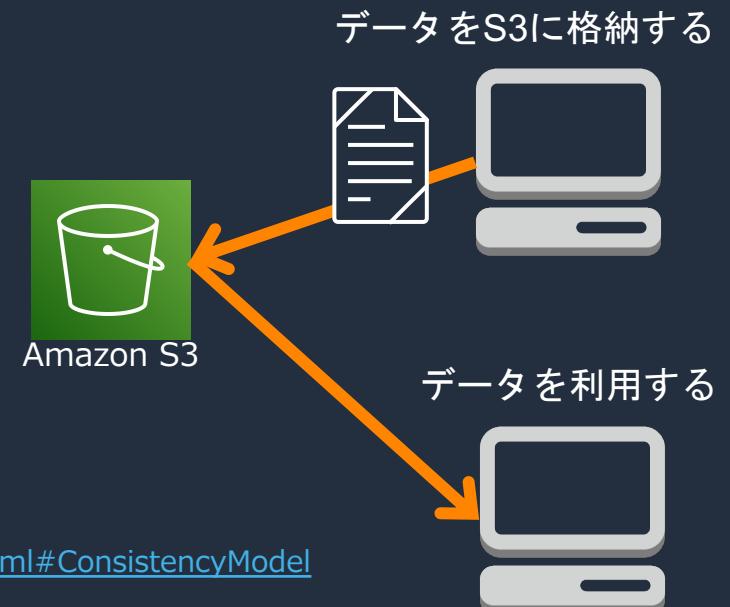
強力な整合性（現在の S3）：新しいオブジェクトの書き込みや既存のオブジェクトの上書きリクエストが成功した後、読み込みリクエストはオブジェクトの最新版を受け取ることができる



結果整合性（かつての S3）：古いバージョンのオブジェクトを受け取る可能性がある

注意点

- 同時書き込みにおけるオブジェクトのロック機能をサポートしていない
- 同時書き込みが発生した場合、最新のタイムスタンプを持つ書き込み結果となる
- 同時書き込みを制御する場合、書き込むアプリケーションでの対処する
- バケットの設定（作成/削除処理など）は結果整合性



S3 のデータ生合成モデルについての詳解: https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/Welcome.html#ConsistencyModel

6. Amazon S3 のストレージクラス

7つのストレージクラスを用途に応じて使い分けることで、コストを最適化できる

S3 Intelligent-Tiering	S3 Standard (S3 標準)	S3 Standard-IA (S3 標準-IA)	S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval	S3 Glacier Deep Archive	S3 One Zone-IA (S3 1ゾーン-IA)
AZ 配置						1 つの AZ
想定されるデータタイプ	アクセスパターンが変化するデータ	頻繁にアクセスされるアクティブデータ	アクセス頻度が低いデータ	めったにアクセスされないデータ	アーカイブデータ	長期保存のアーカイブデータ
設計上の耐久性	99.99999999%					
レイテンシー	ミリ秒単位のアクセス	ミリ秒単位のアクセス	ミリ秒単位のアクセス	ミリ秒単位のアクセス	分から時間単位のアクセス (数分 ~ 12 時間)	時間単位のアクセス (12 ~ 48 時間)
ストレージ価格 (USD/GB 月) ※	0.025 ~ 0.002	0.025 ~ 0.023	0.0138	0.005	0.0045	0.002
aws	※ 価格は 2022 年 12 月の東京リージョンに基づく。リクエストなどに応じて別途課金。					

7. コスト: S3 標準 (2022 年 12 月東京リージョン)

- ストレージ
 - S3 に存在する 1 ヶ月間の平均データ容量に対して課金
 - 最初の 50 TB/月: 0.025 USD/GB、次の 450 TB/月: 0.024 USD/GB、500 TB/月以上: 0.023 USD/GB
- HTTP リクエスト
 - PUT/COPY/POST/LIST: 1000 リクエストあたり 0.0047 USD
 - GET/SELECT/他: 1000 リクエストあたり 0.00037USD
- データ転送
 - S3 からインターネットへデータ転送
 - 最初の 10 TB/月: 0.114 USD/GB、次の 40 TB/月: 0.089 USD/GB
次の 100 TB/月: 0.086 USD/GB、150 TB/月以上: 0.084 USD/GB
 - S3 から各リージョンへのデータ転送: 0.09 USD/GB

その他の特別な処理に関する料金は下記リンクを参照

コストの詳細: <https://aws.amazon.com/jp/s3/pricing/?nc=sn&loc=4>

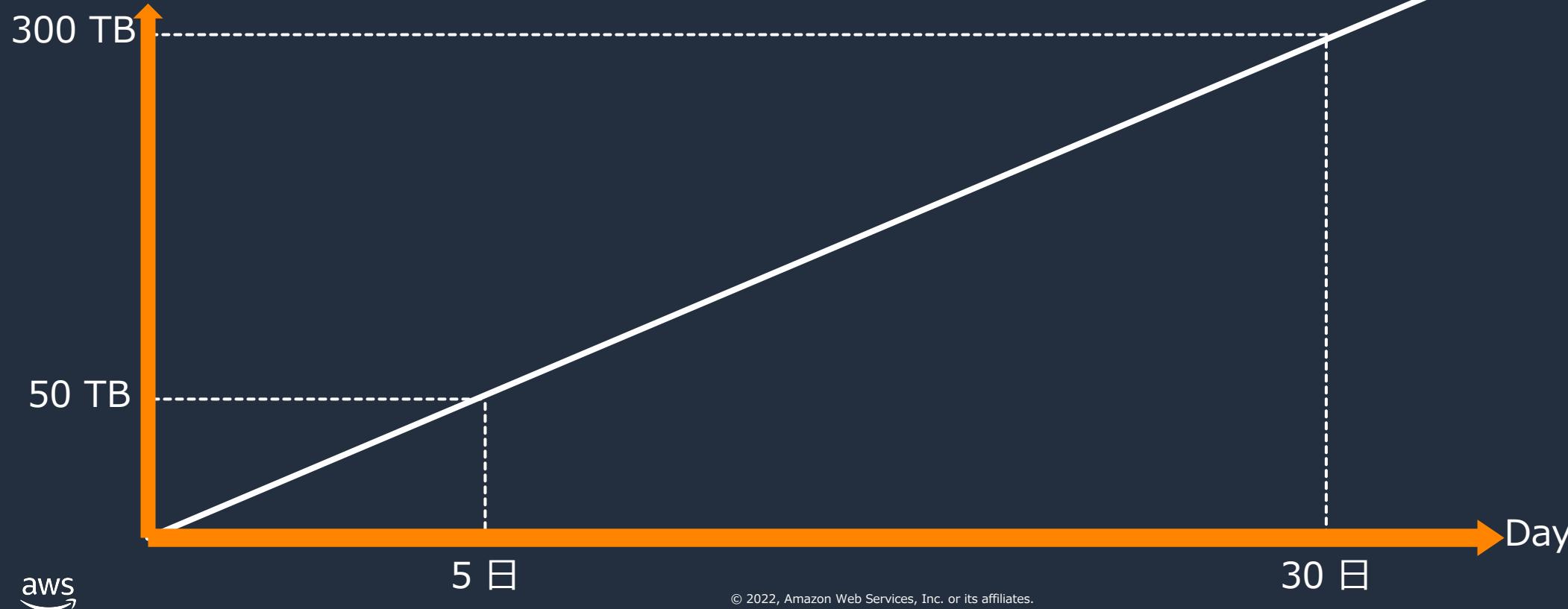


7. コストの算出: ステップ 1

保存するデータの容量と期間を把握する

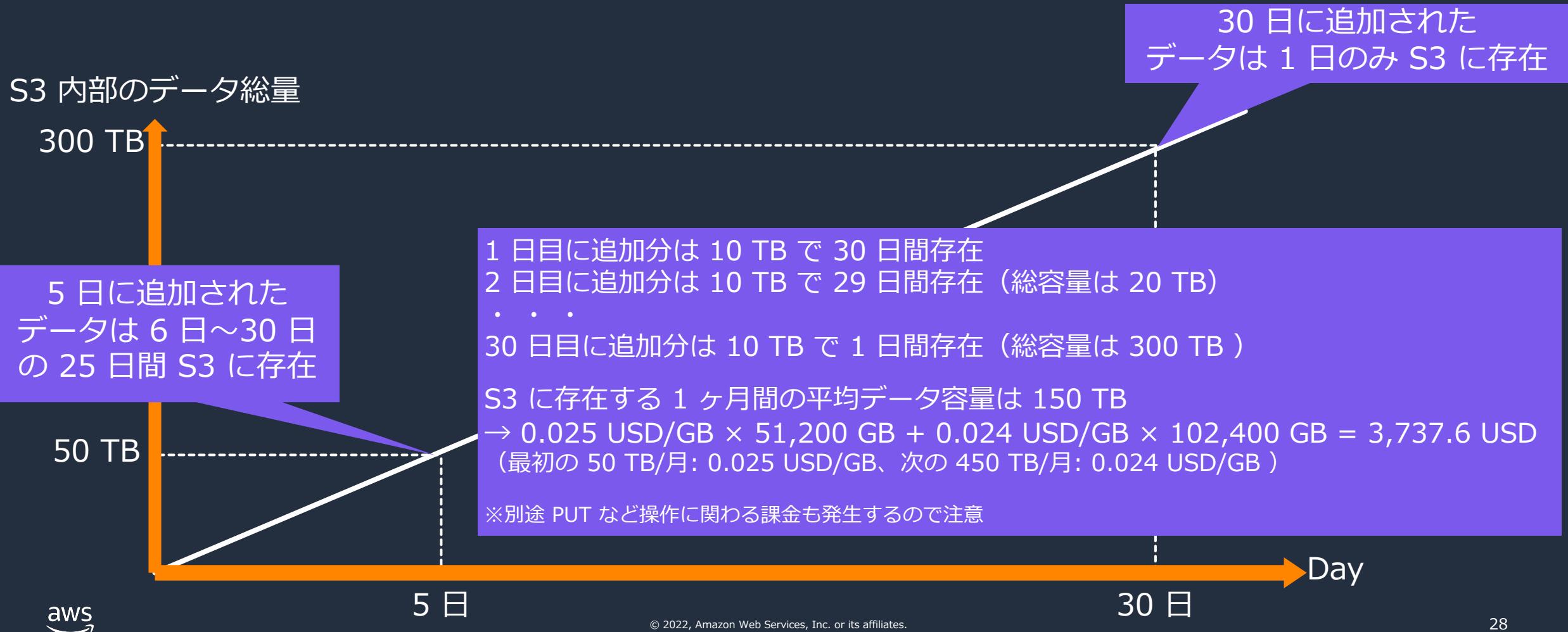
1 日ごとに 10 TB のデータを新たに S3 に保存した場合のデータ総量

S3 内部のデータ総量

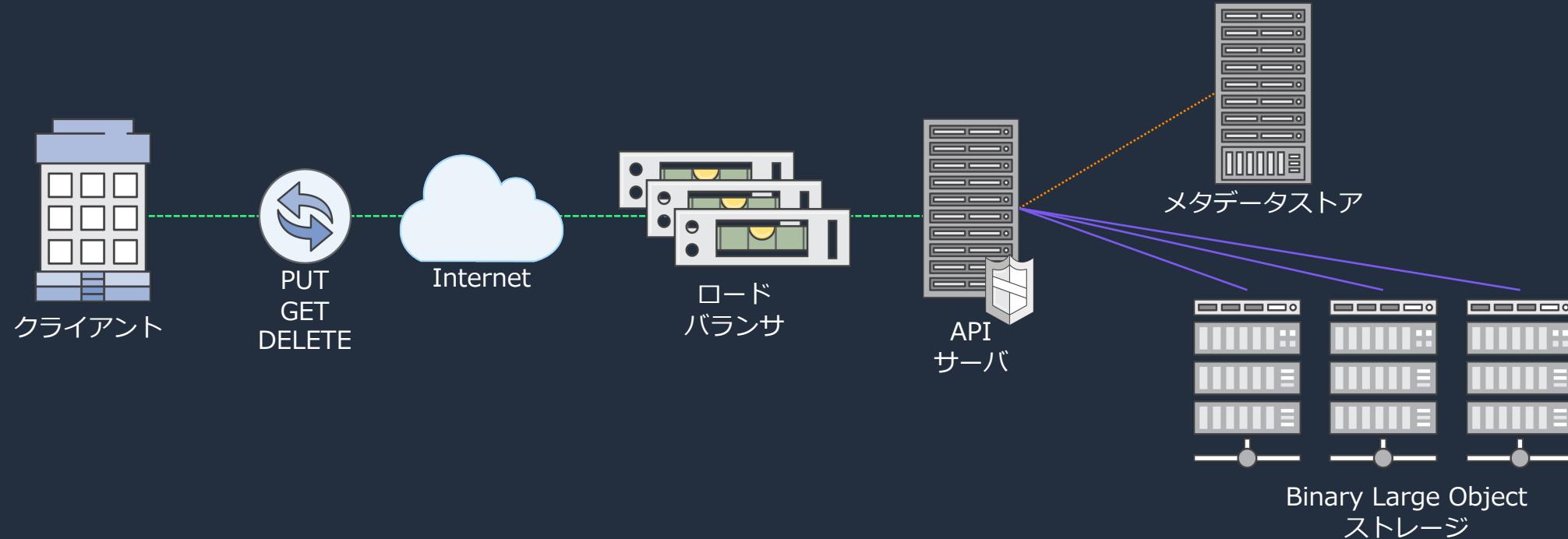


7. コストの算出: ステップ 2

データ容量と保持期間をベースに料金を算出する



8. Amazon S3 のアーキテクチャ



- HTTP/HTTPS 経由で操作を行う
- ファイルシステムとして使用する場合には、S3 File Gateway などの他のツールを利用する

※利用者がこのアーキテクチャを直接的に意識するものではありません。

Amazon S3 にオブジェクトを アップロードする方法

オブジェクトアップロードの流れ



1. Amazon S3 でバケットを作成する。バケットの作成にはマネジメントコンソール/CLI/SDK を用いることができる
2. クライアントから、マネジメントコンソール/CLI/SDK を用いて、作成したバケットへオブジェクトをアップロードする

バケットの作成

Amazon S3

Bucket

アクセスポイント

Object Lambda アクセスポイント

マルチリージョンアクセスポイント

バッチオペレーション

S3 のアクセスアナライザー

このアカウントのブロックバブ

Amazon S3 > バケット

▼ アカウントのスナップショット

最終更新日: Storage Lens による 2022/11/06。メトリクスは 24 時間ごとに生成されます。詳細は [こちら](#)

Storage Lens ダッシュボードを表示

ストレージの合計	オブジェクト数	平均オブジェクトサイズ	アドバンストメトリクスは、 [default-account-dashboard] の設定で有効にできます。
3.3 GB	931 k	3.7 KB	[default-account-dashboard]

バケット (12) 情報

バケットは S3 に保存されたデータのためのコンテナです。詳細

C ARN をコピー 空にする 削除 バケットを作成

S3 の「バケット」を選択し、「バケットを作成」をクリックする

バケット名を入力し、他の領域はデフォルトのまま（任意）スクロールダウンし、「バケットを作成」をクリックする

Amazon S3 > バケット > バケットを作成

バケットを作成 情報

バケットは S3 に保存されたデータのためのコンテナです。詳細

一般的な設定

バケット名

shinya-sato-bb

バケット名はグローバルに一意である必要があります。スペースや大文字を含めることはできません。バケットの命名規則を参照してください

AWS リージョン

米国西部 (オレゴン) us-west-2

既存のバケットから設定をコピー - オプション
次の設定のバケット設定のみがコピーされます。

バケットを選択する

オブジェクトのアップロード 1

Amazon S3 > バケット > shinya-sato-bb

shinya-sato-bb 情報

オブジェクト (0)

オブジェクトは、Amazon S3 に保存された基本的なエンティティです。Amazon S3 インベントリ を使用して、バケット内のすべてのオブジェクトのリストを取得できます。他のユーザーが自分のオブジェクトにアクセスできるためには、明示的にアクセス権限を付与する必要があります。詳細は こちら

C S3 URI をコピー URL をコピー ダウンロード 開く 削除 アクション フォルダの作成

アップロード

検索

名前 タイプ 最終更新日時 サイズ ストレージクラス

オブジェクトはありません
このバケットにはオブジェクトがありません。

アップロード



「ファイルを追加」をクリックする

作成したバケットを選択し
「アップロード」をクリックする

ファイルとフォルダ (0)

このテーブル内のすべてのファイルとフォルダがアップロードされます。

削除 ファイルを追加 フォルダの追加

名前検索

名前 タイプ サイズ

ファイルまたはフォルダがありません
アップロードするファイルまたはフォルダを選択していません。



オブジェクトのアップロード 2



アップロードの完了を確認できる

「アップロード」をクリックする



CLI/SDK でのオブジェクトのアップロード

CLI の場合

dummy.txt を shinya-sato-bb というバケットへコピー

```
[ec2-user@ip-172-31-26-56 ~]$ touch dummy.txt  
[ec2-user@ip-172-31-26-56 ~]$ aws s3 cp ./dummy.txt s3://shinya-sato-bb  
upload: ./dummy.txt to s3://shinya-sato-bb/dummy.txt
```

アップロードが完了

SDK の場合 (Python)

```
[ec2-user@ip-172-31-26-56 ~]$ python3  
Python 3.7.10 (default, Jun 3 2021, 00:02:01)  
[GCC 7.3.1 20180712 (Red Hat 7.3.1-13)] on linux  
Type "help", "copyright", "credits" or "license" for more information.  
>>> import boto3  
>>> s3 = boto3.resource('s3')  
>>> bucket = s3.Bucket('shinya-sato-bb')  
>>> bucket.upload_file('./dummy.txt', 'dummy.txt')  
>>>
```

アップロードするファイルの指定

キーの指定

バケットを指定



まとめ



まとめ

- Amazon S3 は高い耐久性を誇る低コストなオブジェクトストレージ
- AWS の様々なサービスと連携し、多くのワークフローで活用できる
- 2006 年に登場して以来、セキュリティ/データの保護/分析する機能など多くのアップデートがなされている
- マネジメントコンソールによる GUI 操作だけではなく、CLI や SDK が利用できるのでスクリプトやプログラムと親和性が高く、ロジックに組み込んで自動化し易い

本資料に関するお問い合わせ・ご感想

技術的な内容に関しましては、有料のAWSサポート窓口へ
お問い合わせください

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

料金面でのお問い合わせに関しましては、カスタマーサポート窓口へ
お問い合わせください（マネジメントコンソールへのログインが必要です）

<https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service>

具体的な案件に対する構成相談は、後述する個別相談会をご活用ください



ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt



その他コンテンツのご紹介

ウェビナーなど、AWSのイベントスケジュールをご参照いただけます

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

ハンズオンコンテンツ

<https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/>

AWS 個別相談会

AWSのソリューションアーキテクトと直接会話いただけます

<https://pages.awscloud.com/JAPAN-event-SP-Weekly-Sales-Consulting-Seminar-2021-reg-event.html>



Thank you!



Amazon Simple Storage Service (Amazon S3)

コスト最適化編

吉澤 巧

Amazon Web Service Japan G.K.

Solutions Architect

2023/06

AWS Black Belt Online Seminar とは

- ・ 「サービス別」「ソリューション別」「業種別」などのテーマに分け、
アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナー
シリーズです
- ・ AWS の技術担当者が、AWS の各サービスやソリューションについてテーマ
ごとに動画を公開します
- ・ 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も
可能、スキマ時間の学習にもお役立ていただけます
- ・ 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
- ・ <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>

内容についての注意点

- ・ 本資料では 2023 年 6 月時点のサービス内容および価格についてご説明しています。最新の情報は AWS 公式ウェブサイト(<https://aws.amazon.com/>)にてご確認ください
- ・ 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- ・ 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます

自己紹介

名前：吉澤 巧 (Yoshizawa Takumi)

所属：アマゾン ウェブ サービス ジャパン合同会社
技術統括本部
ソリューションアーキテクト

経歴：気象予報士

好きなAWSサービス：
Amazon S3、 AWS Trusted Advisor



本題に入る前に - コスト最適化のイメージ -

1 GB のオブジェクトを 1000 個格納すると仮定

本題に入る前に - コスト最適化のイメージ -

1 GB のオブジェクトを 1000 個格納すると仮定

コスト最適化前
(S3 標準を利用)

年間およそ

300 USD

ストレージ : $0.025\text{USD} \times 1000 = 25 \text{ USD} / \text{月}$

PUT リクエスト : 0.005USD

- 2023 年 6 月現在の東京リージョンの価格

本題に入る前に - コスト最適化のイメージ -

1 GB のオブジェクトを 1000 個格納すると仮定

コスト最適化前
(S3 標準を利用)

年間およそ

300 USD

ストレージ : $0.025\text{USD} \times 1000 = 25 \text{ USD} / \text{月}$

PUT リクエスト : 0.005USD

コスト最適化後
(S3 Glacier Deep Archiveを利用)

年間およそ

24.9 USD

約 91 %
OFF

ストレージ : $0.002\text{USD} \times 1000 = 2 \text{ USD} / \text{月}$

メタデータ : 0.07 USD / 月

PUT リクエスト : 0.065USD

- 2023 年 6 月現在の東京リージョンの価格
- アクセスパターン等によってコスト削減の効果は異なります

本セミナーの対象者

前提知識

- AWS の基本的な知識
- Amazon S3 入門編あるいは同等の知識※

対象者

- Amazon S3 のコスト最適化方法にご興味を持つ方
- Amazon S3 ストレージクラスの詳細にご興味を持つ方

※参考リンク:

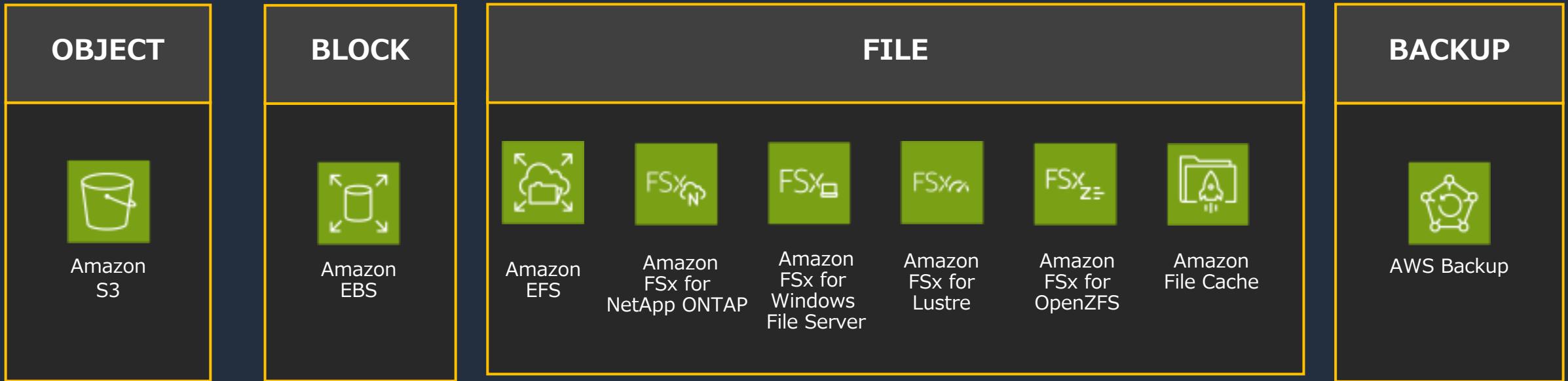
Amazon S3 入門編: <https://www.youtube.com/watch?v=wQ8ZDvoMSno>

アジェンダ

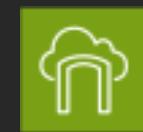
1. Amazon S3 の概要
2. Amazon S3 の料金体系
3. ストレージクラス
4. コスト最適化 4 つのポイント
5. まとめ

Amazon S3 の概要

AWS のストレージサービス



DATA TRANSFER AND MIGRATION



AWS Storage
Gateway



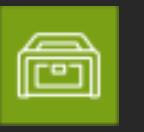
AWS DataSync



AWS Transfer
Family

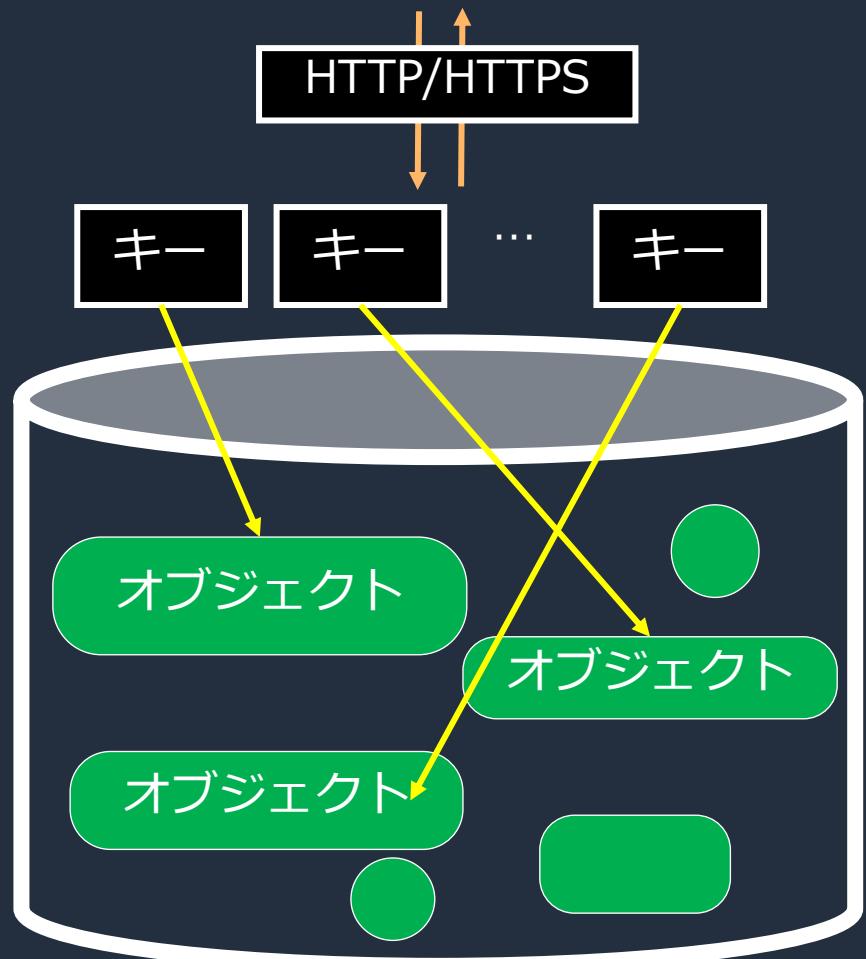


AWS Snowball



AWS Snowcone

オブジェクトストレージとは



特徴

- HTTP/HTTPS でアクセス
- 一意のキーに対するオブジェクト（データ）が存在
- 階層構造を取るファイルストレージとは異なり、
フラットな構造

メリット

- スケールが容易で、大容量のデータ保存が可能
- オブジェクト単位でのアクセス制御
- 高い可用性と耐障害性
- 独自にカスタマイズできるメタデータを追加可能

Amazon S3 とは

高いパフォーマンスと可用性、そして低コストが特徴なオブジェクトストレージ
2006 年に登場してから、現在に至るまでのイノベーションが積み重なった歴史あるサービス

- 耐久性
 - 99.99999999% (イレブンナイン)
 - 最低 3 つのアベイラビリティゾーン (AZ) で冗長化
- スケーラビリティ
 - 無制限のデータ保存
 - ただし、1 オブジェクトは最大 5 TB
- 低成本
- セキュリティ
 - アクセス制御とログ監査
- データの保護
 - 誤削除から守る機能
- アクセシビリティ
 - HTTP/HTTPS でアップロード/ダウンロード/変更/削除といった操作が可能
- 様々な AWS サービスとの連携

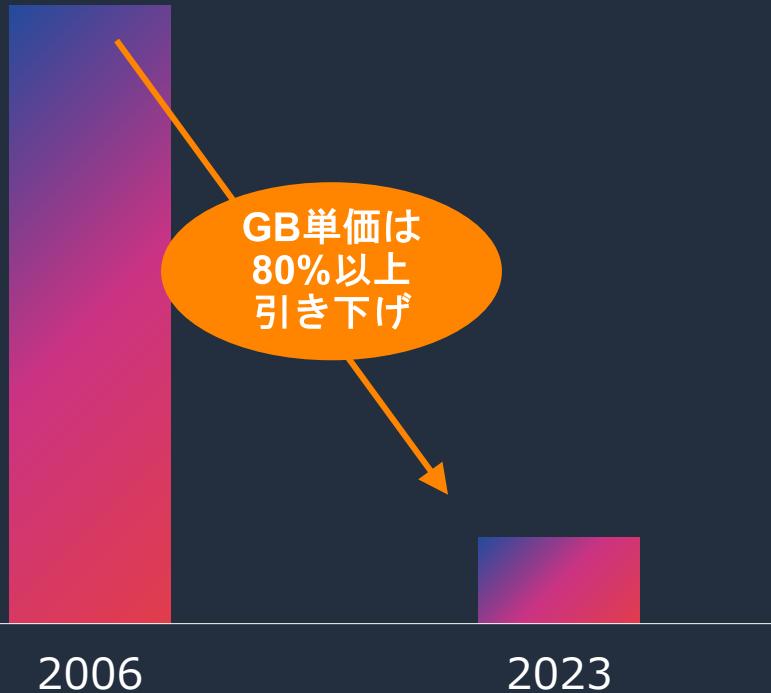


Amazon S3 の特徴などは FAQ にて詳解: <https://aws.amazon.com/jp/s3/faqs/>

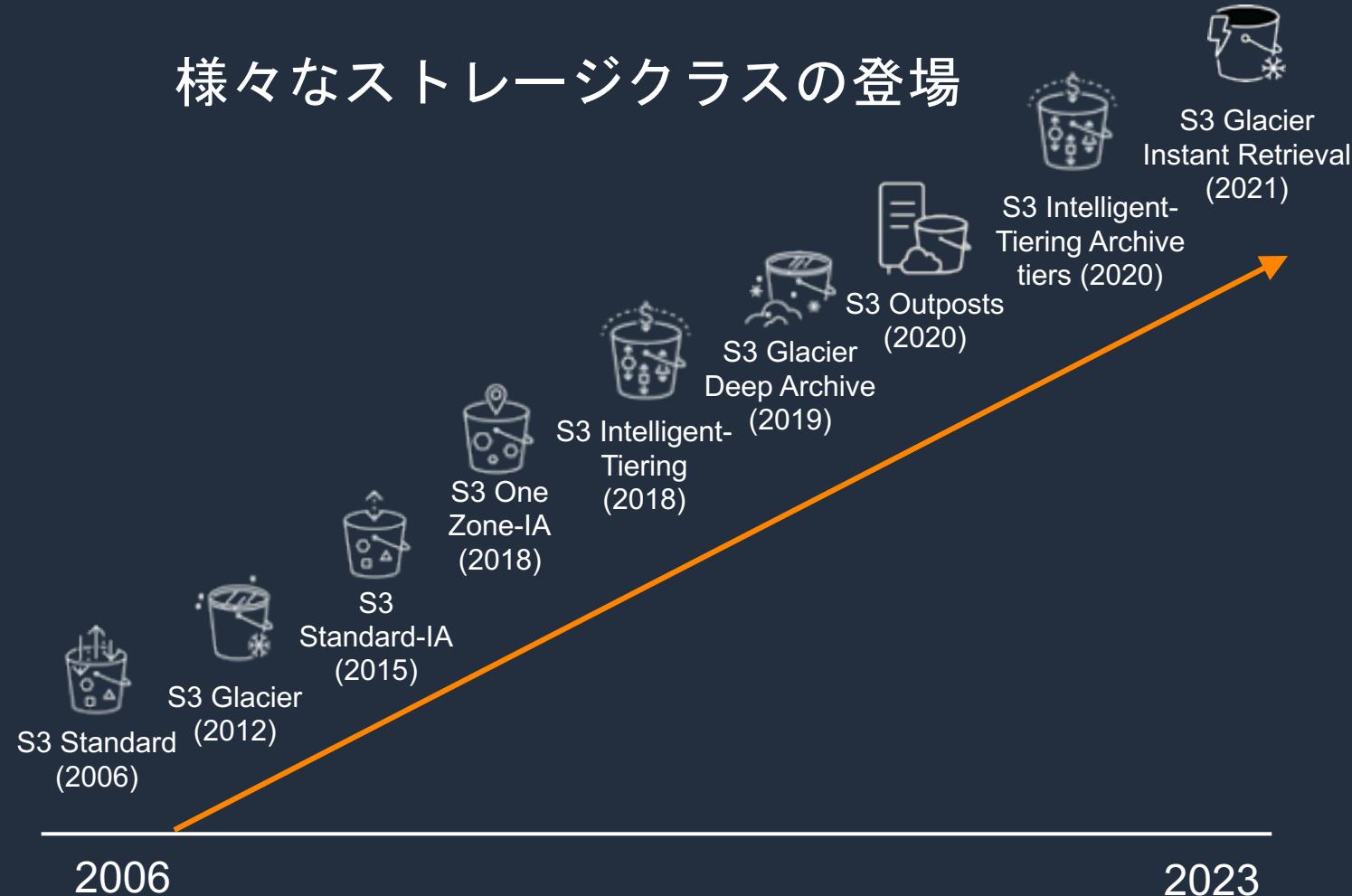


Amazon S3 のコストイノベーション

継続的な値下げ



様々なストレージクラスの登場



Amazon S3 の料金体系

Amazon S3 のコスト – 全体像

2023 年 6 月現在の東京リージョンの価格
以下のスライドについても同上

1. ストレージ
 - S3 標準の場合 : 0.025 USD/GB (S3 標準、最初の 50 TB)
2. リクエストとデータ取り出し
 - S3 標準の場合 : 0.00037 USD/1000 件 (GET)、0.00047 USD/1000 件 (PUT)
 - ライフサイクル移行リクエスト (他ストレージクラスへの移行)
 - データ取り出しリクエスト、データ取り出し (主に標準以外のストレージクラスで発生)
3. データ転送
 - S3 からインターネットや他リージョンへ転送する場合料金が発生
4. 管理と分析
 - S3 Storage Lens : オブジェクト 100 万個あたり 0.20 USD/月
 - S3 ストレージクラス分析 : オブジェクト 100 万個あたり 0.10 USD/月
 - S3 Inventory 分析 : オブジェクト 100 万個あたり 0.0028 USD/月
 - S3 オブジェクトのタグ付け : タグ 1 万個あたり 0.01 USD/月
5. レプリケーション
 - S3 Replication Time Control を使用する場合、0.015 USD/GB の追加料金
6. S3 Object Lambda
 - 戻りデータ 1 GB につき 0.01 USD/月

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

一部抜粋、詳細はこちらのリンクをご確認ください。



Amazon S3 のコスト – S3 標準で発生する代表的な料金

1. ストレージ



1 ヶ月間の平均データ容量に
対して課金

料金

最初の 50 TB : 0.025 USD/GB
次の 450 TB : 0.024 USD/GB
500 TB 以上 : 0.023 USD/GB

2. リクエスト



リクエスト数に応じて課金

料金

PUT、COPY、POST、LIST :
0.0047 USD/1000 リクエスト
GET、SELECT、他 :
0.0037 USD/1000 リクエスト
DELETE、CANCEL :
無料

3. データ転送



出入りしたネットワーク帯域幅
に応じて課金

料金 (一部抜粋)

インターネットから S3 : 無料
S3 からインターネット :
最初の 10 TB : 0.114 USD/GB
10 TB 以上の転送は割引あり
他リージョンへ : 0.09 USD/GB

Amazon S3 ストレージクラス

Amazon S3 ストレージクラス概要

ワークロードに応じてストレージクラスを選択可能、コストの最適化が可能に



AZ 間の冗長性	複数のアベイラビリティゾーン (AZ)						1つの AZ
想定されるデータタイプ	アクセスパターンが想定できない/変化するデータ	頻繁にアクセスされるアクティブデータ	アクセス頻度が低いデータ	即時取り出しが必要なアーカイブデータ	ほとんどアクセスされないアーカイブデータ	長期保存のアーカイブデータ	再生可能でアクセス頻度が低いデータ
オブジェクトの耐久性	99.999999999%	99.999999999%	99.999999999%	99.999999999%	99.999999999%	99.999999999%	99.999999999%
データの可用性	99.9%	99.99%	99.9%	99.9%	99.99%	99.99%	99.5%
レイテンシー	ミリ秒単位のアクセス	ミリ秒単位のアクセス	ミリ秒単位のアクセス	ミリ秒単位のアクセス	分から時間単位の復元 (数分～12時間)	時間単位の復元 (12～48時間)	ミリ秒単位のアクセス
取り出し料金	なし	なし	GB あたり	GB あたり	GB あたり	GB あたり	GB あたり
最小ストレージ期間 (最低保存期間)	-	-	30 日	90 日	90 日	180 日	30 日
最小オブジェクトサイズ	-	-	128 KB	128 KB	40 KB	40 KB	128 KB
ストレージ価格	0.025 ~ 0.002 USD/GB 月	0.025 ~ 0.023 USD/GB 月	0.0138 USD/GB 月	0.005 USD/GB 月	0.0045 USD/GB 月	0.002 USD/GB 月	0.011 USD/GB 月

S3 標準 - 低頻度アクセスとは

			
		S3 標準	S3 標準 - 低頻度アクセス (S3 標準 - IA)
ストレージ 料金	0.025 USD/GB-month	約 45 % 安い	0.00138 USD/GB-month
データ取り出し料金	なし		0.01 USD/GB
ライフサイクル 移行料金	なし		0.01 USD/1000 件
最低保存期間	なし		30 日
最小 オブジェクトサイズ	なし		128 KB

Amazon S3 Glacier 比較



S3 Glacier
Instant Retrieval



S3 Glacier
Flexible Retrieval



S3 Glacier
Deep Archive

ストレージ 料金

0.005 USD / GB-month

0.0045 USD / GB-month

0.002 USD / GB-month

データ取り出し 所要時間

ミリ秒単位のアクセス

迅速: 1-5 分
標準: 3-5 時間
大容量: 5-12 時間

標準: 12 時間以内
大容量: 48 時間以内

最小 オブジェクトサイズ

128 KB

オブジェクトサイズが 128 KB 以下の場合
128 KB として課金

40 KB

40 KB

40 KB のメタデータが追加される
(32 KB : 同一クラス, 8 KB : 標準クラスとして課金)

Amazon S3 Glacier - 復元

S3 Glacier Flexible Retrieval と S3 Glacier Deep Archive は取り出す際に復元をする必要あり



- S3 Glacier Flexible Retrieval
 - 1. 一括取得 (5-12 時間) : 取り出し料金なし
 - 2. 標準取り出し (3-5 時間) : 0.0571 USD/1000 リクエスト + 0.011 USD/GB
 - 3. 迅速取り出し (1-5 分、250 MBまで) : 11 USD/1000 リクエスト + 0.033 USD/GB
- S3 Glacier Deep Archive
 - 1. 一括取得 (48 時間) : 0.025 USD/1000 リクエスト + 0.005 USD/GB
 - 2. 標準取り出し (12 時間) : 0.1142 USD/1000 リクエスト + 0.022 USD/GB

ストレージクラスの選択



S3 標準



S3 標準 - IA



Glacier
Instant Retrieval



Glacier
Flexible Retrieval



Glacier
Deep Archive

ミリ秒単位のアクセス

リストア
リクエスト

日常的に
アクセス

アーカイブデータ

任意のサイズ

> 128 KB

推奨 > 256 KB

推奨 > 1 MB

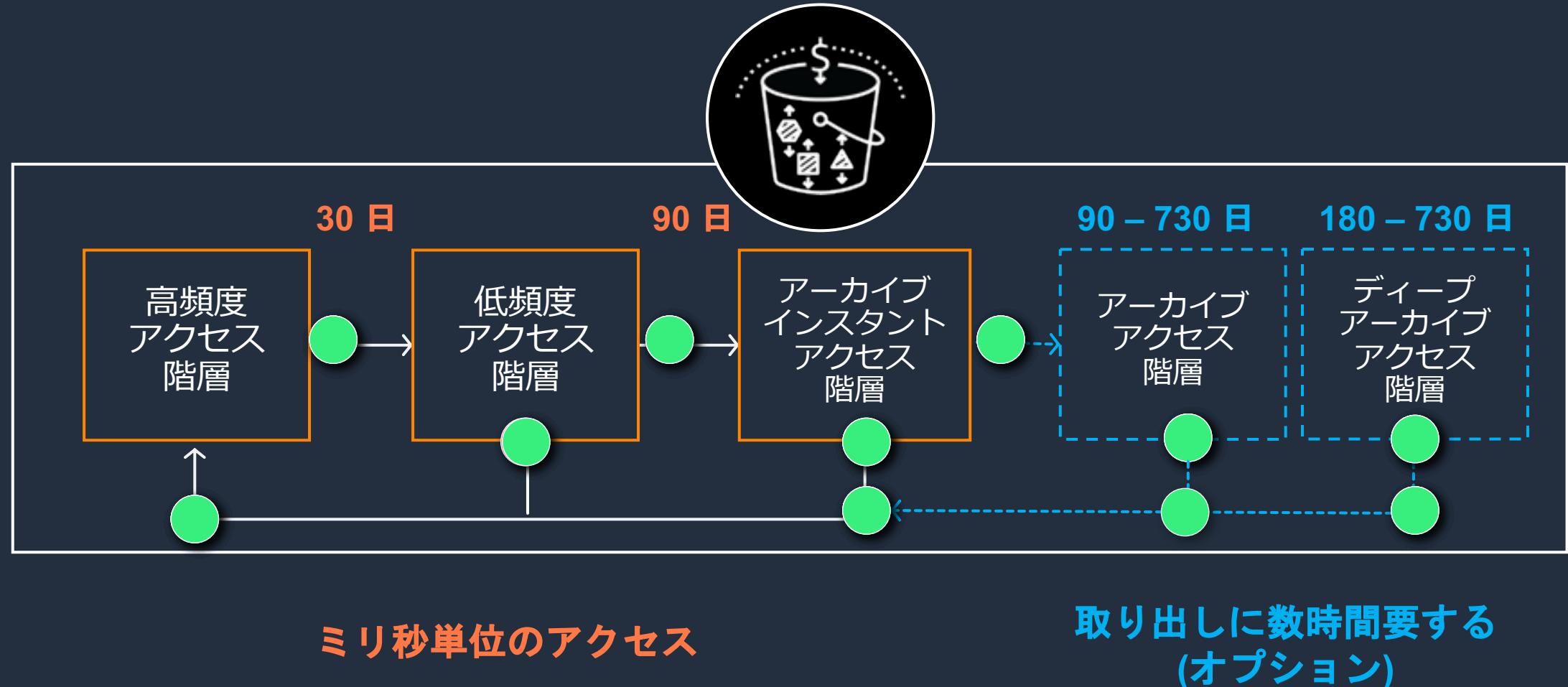
S3 Intelligent-Tiering 概要



- ストレージコストを自動で節約できる唯一の S3 ストレージ
- 毎月少額のモニタリング・オートメーション料金を支払うだけで、より低コストのアクセス階層へ自動的に移動
- 例えばアーカイブインスタントアクセス階層は、S3 標準と比べて 80 % コストが低い
- ライフサイクル移行費用や取り出し費用は不要
- 128 KB 未満のファイルは常に高頻度アクセス階層料金で保管、モニタリング料金は不要
- 99.9 % の可用性、99.999999999 % の耐久性

S3 Intelligent-Tiering の動き

一定日数連続でアクセスがないと、より低コストのアクセス階層へ自動的に移動



Amazon S3 ストレージクラス（再掲）

ワークロードに応じてストレージクラスを選択可能、コストの最適化が可能に



AZ 間の冗長性	複数のアベイラビリティゾーン (AZ)						1つの AZ
想定されるデータタイプ	アクセスパターンが想定できない/変化するデータ	頻繁にアクセスされるアクティブデータ	アクセス頻度が低いデータ	即時取り出しが必要なアーカイブデータ	ほとんどアクセスされないアーカイブデータ	長期保存のアーカイブデータ	再生可能でアクセス頻度が低いデータ
オブジェクトの耐久性	99.999999999%	99.999999999%	99.999999999%	99.999999999%	99.999999999%	99.999999999%	99.999999999%
データの可用性	99.9%	99.99%	99.9%	99.9%	99.99%	99.99%	99.5%
レイテンシー	ミリ秒単位のアクセス	ミリ秒単位のアクセス	ミリ秒単位のアクセス	ミリ秒単位のアクセス	分から時間単位の復元 (数分～12時間)	時間単位の復元 (12～48時間)	ミリ秒単位のアクセス
取り出し料金	なし	なし	GB あたり	GB あたり	GB あたり	GB あたり	GB あたり
最小ストレージ期間 (最低保存期間)	-	-	30 日	90 日	90 日	180 日	30 日
最小オブジェクトサイズ	-	-	128 KB	128 KB	40 KB	40 KB	128 KB
ストレージ価格 *	0.025 ~ 0.002 USD/GB 月	0.025 ~ 0.023 USD/GB 月	0.0138 USD/GB 月	0.005 USD/GB 月	0.0045 USD/GB 月	0.002 USD/GB 月	0.011 USD/GB 月

コスト最適化 4つのポイント

Amazon S3 におけるコスト最適化のポイント

1



アプリケーション
要件の整理

2



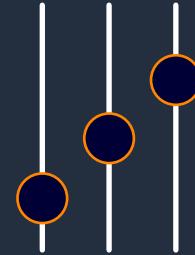
データ配置の
設計

3



ストレージ状況把握、
分析、最適化

4



継続的な
サイジング

Amazon S3 におけるコスト最適化のポイント



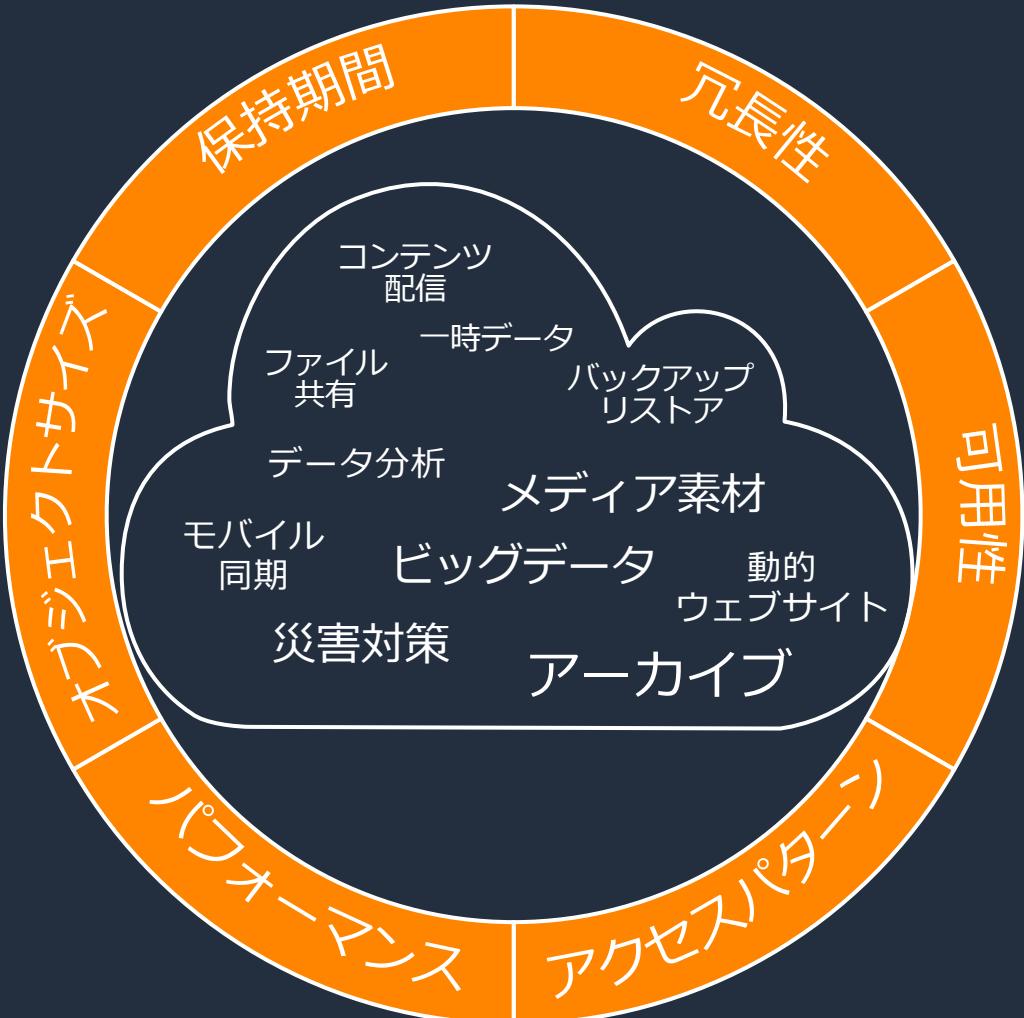
アプリケーション
要件の整理

データ配置の
設計

ストレージ状況把握、
分析、最適化

継続的な
サイジング

アプリケーション要件の整理



- ✓ 冗長性や耐久性
- ✓ 求められる可用性
- ✓ ストレージにアクセスする頻度
- ✓ 必要なパフォーマンス、例えば取得までに数時間かかることは許容できるか
- ✓ オブジェクトのサイズ
- ✓ 格納する期限

Amazon S3 におけるコスト最適化のポイント

1



アプリケーション
要件の整理

2



データ配置の
設計

3



ストレージ状況把握、
分析、最適化

4

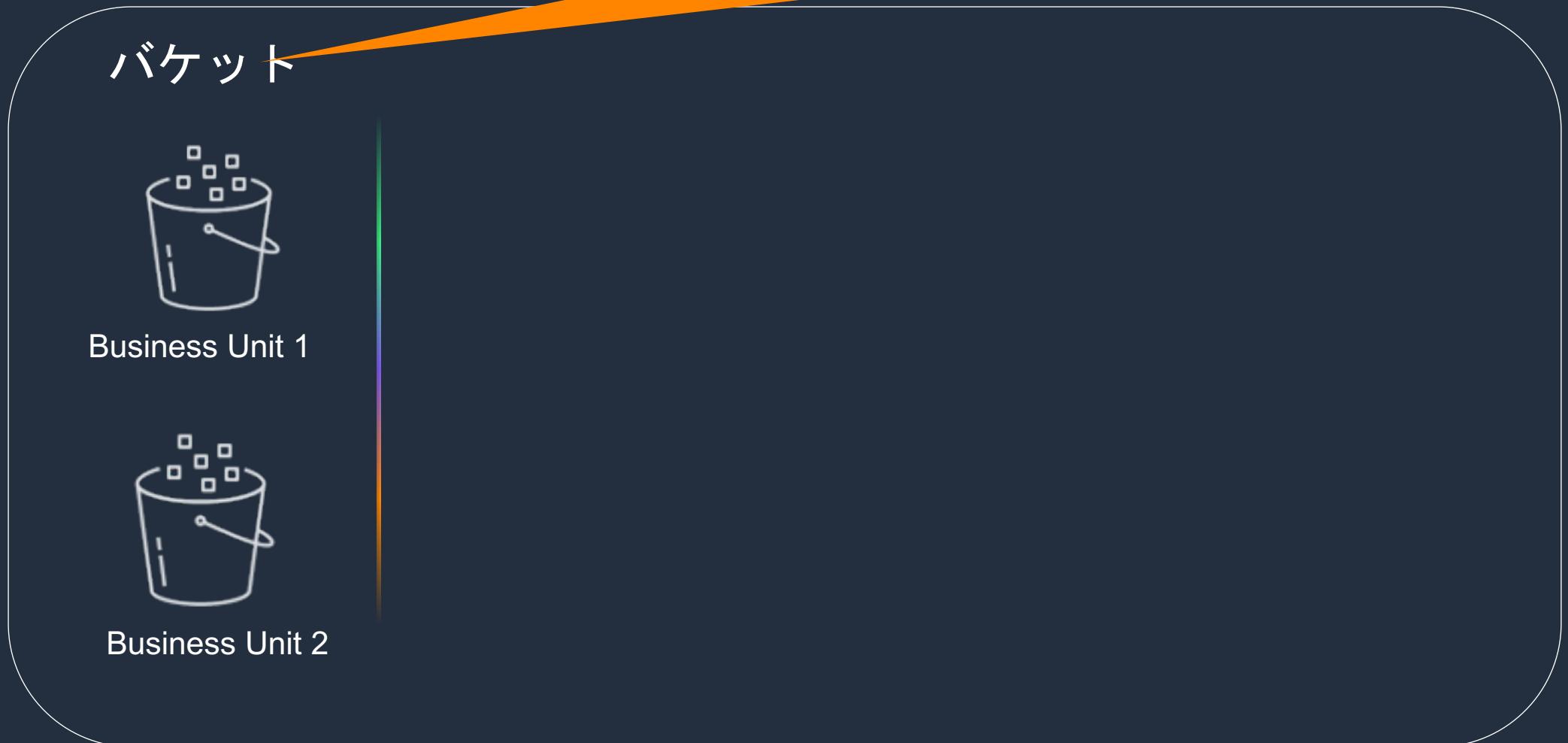


継続的な
サイジング



データ配置の設計

データを整理する最初のステップ、部署や利用目的で分割
バケット数は料金に影響しない



データ配置の設計

実際のオブジェクトを格納する「パス」のようなもの
フォルダのように管理することが可能に



AWS アカウント
IAM ユーザー

バケット



Business Unit 1



Business Unit 2

プレフィックス

Unit1/internal/usage/
Unit1/internal2/billing/usage
Unit1/internal3/free/usage

Unit2/model1/inference
Unit2/model2/inference
Unit2/predictions/prod

データ配置の設計

キーと値のペア、オブジェクト毎に最大 10 個設定可能
他 AWS サービスとの連携や請求管理にも活用可能



AWS アカウント
IAM ユーザー

バケット



Business Unit 1



Business Unit 2

プレフィックス

Unit1/internal/usage/
Unit1/internal2/billing/usage
Unit1/internal3/free/usage

Unit2/model1/inference
Unit2/model2/inference
Unit2/predictions/prod

オブジェクトタグ

Department = Finance
Team = Business Reporting
Classification = Confidential

Department = Marketing
Team = Data Science
Classification = Confidential

Amazon S3 におけるコスト最適化のポイント

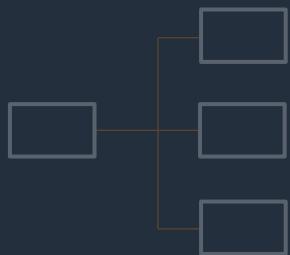
1



アプリケーション
要件の整理



2



データ配置の
設計

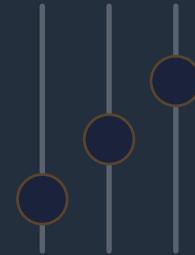


3



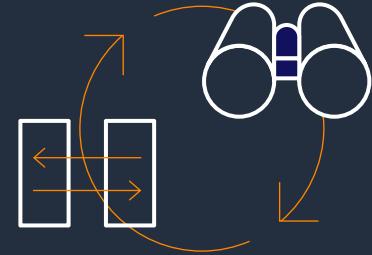
ストレージ状況把握、
分析、最適化

4



継続的な
サイジング

ストレージ状況把握、分析、最適化

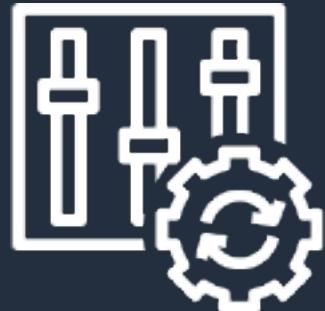


Storage Lens



コスト最適化のための
S3 使用状況の可視化と
ダッシュボード

ストレージクラス 分析



ストレージの
アクセスパターン分析

S3 Inventory



分析や監査のための
オブジェクトレベルの分析

Amazon S3 Storage Lens とは？

S3 の使用状況とアクティビティを組織全体で可視化



- ✓ 28 の無料メトリクスと 35 の追加メトリクス
- ✓ リージョン、ストレージクラス、バケット等ごとにドリルダウン分析が可能
- ✓ コスト最適やデータ保護に関するベストプラクティスを提示
- ✓ Amazon S3 に統合されたダッシュボードで確認可能
- ✓ 組織的な可視化

Amazon S3 Storage Lens 例



Amazon S3 Storage Lens 有効化

Amazon S3 Storage Lens の有効化手順を示すスクリーンショットです。

左側のナビゲーションメニューでは、**Storage Lens ダッシュボード**が選択されています。

中央部には、Storage Lens の概要と使用開始に関する情報が表示されています。

- ダッシュボードを作成**: ダッシュボードのスコープを設定し、メトリクス履歴を選択し、必要に応じてメトリクスのエクスポートを設定します。
- 日次の集約**: 毎日、ストレージメトリクスは、アカウント、リージョン、ストレージクラス、およびパケット別に事前に集約され、オプションで AWS Organization とプレフィックス別に集約されます。

右側のオレンジ色の領域には、以下の確認項目が記載されています。

- 追加メトリクスの確認
- 15ヶ月分のメトリクスを確認したい場合、ダッシュボードを別途作成

下部には、ダッシュボード一覧画面が表示されています。リスト内に **default-account-dashboard** が表示されています。

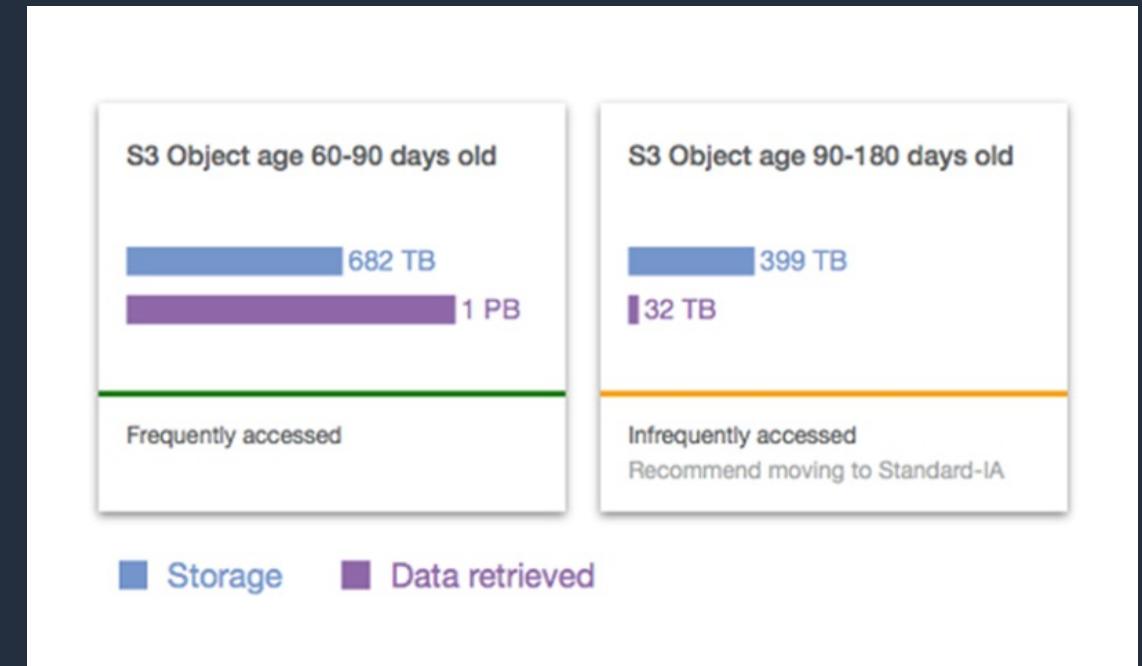
Amazon S3 ストレージクラス分析

ストレージのアクセスパターンを分析、ストレージクラス移行タイミングの決定を手助け

- ✓ストレージアクセスパターンを分析
- ✓ いつ低頻度アクセス階層に移動するべきか
レコメンデーションを提示
- ✓ プレフィックスやタグによる
絞り込みも可能
- ✓ CSV ファイルでエクスポートし、
QuickSight で可視化といったアプローチも

注意点

- 標準 or 標準 IA クラスの推奨のみが提供
- 推奨事項の表示には約 30 日の監視が必要



Amazon S3 ストレージクラス分析の有効化

The screenshot shows the Amazon S3 console. On the left, the navigation pane includes 'Amazon S3', 'パケット' (selected), 'アクセスポイント', 'Object Lambda アクセスポイント', 'マルチリージョンアクセスポイント', 'バッヂオペレーション', and 'IAM Access Analyzer for S3'. Under 'パケット', there are sections for 'このアカウントのブロックバッファーアクセス設定', 'Storage Lens' (collapsed), 'ダッシュボード', and 'AWS Organizations の設定'. Below that is '注目機能' (collapsed) with a blue badge showing '1' and 'S3 の AWS Marketplace'. The main content area shows the 'blackbelt-s3-demo' bucket details. The 'Metrics' tab is selected, indicated by an orange box and a circled '1'. The 'Metrics' section displays a line chart for storage class analysis metrics over the last 2 weeks. Below the chart is a table for 'ストレージクラス分析 (0)' (Storage Class Analysis (0)). A button '分析設定を作成' (Create analysis settings) is highlighted with an orange box and circled '2'. At the bottom of the table, there's a 'Create con...' button.

The screenshot shows the 'Analysis Settings' configuration page for the 'blackbelt-s3-demo' bucket. The top header says '設定スコープ' (Scope) with the sub-instruction '分析するスコープを指定します' (Specify the scope for analysis). A large orange box highlights the 'ルールスコープを選択' (Select rule scope) section, which contains two radio buttons: '1つ以上のフィルターを使用してこのルールのスコープを制限する' (Limit the rule's scope using one or more filters) (selected) and 'パケット内のすべてのオブジェクトに適用' (Apply to all objects in the bucket). A circled '3' is placed next to this section. Below this is the 'フィルタータイプ' (Filter type) section, which includes 'プレフィックス' (Prefix) and 'オブジェクトタグ' (Object tags). The 'Prefix' section has a sub-section for 'プレフィックスを入力' (Enter prefix) with the note 'プレフィックスにバケット名を含めないでください。キー名に特定の文字を使用すると、一部のアプリケーションやプロトコルで問題が発生する可能性があります' (Do not include the bucket name in the prefix. Using specific characters in key names may cause issues with some applications and protocols). The 'Object tags' section has a 'タグの追加' (Add tag) button. The entire configuration page has a light gray background.

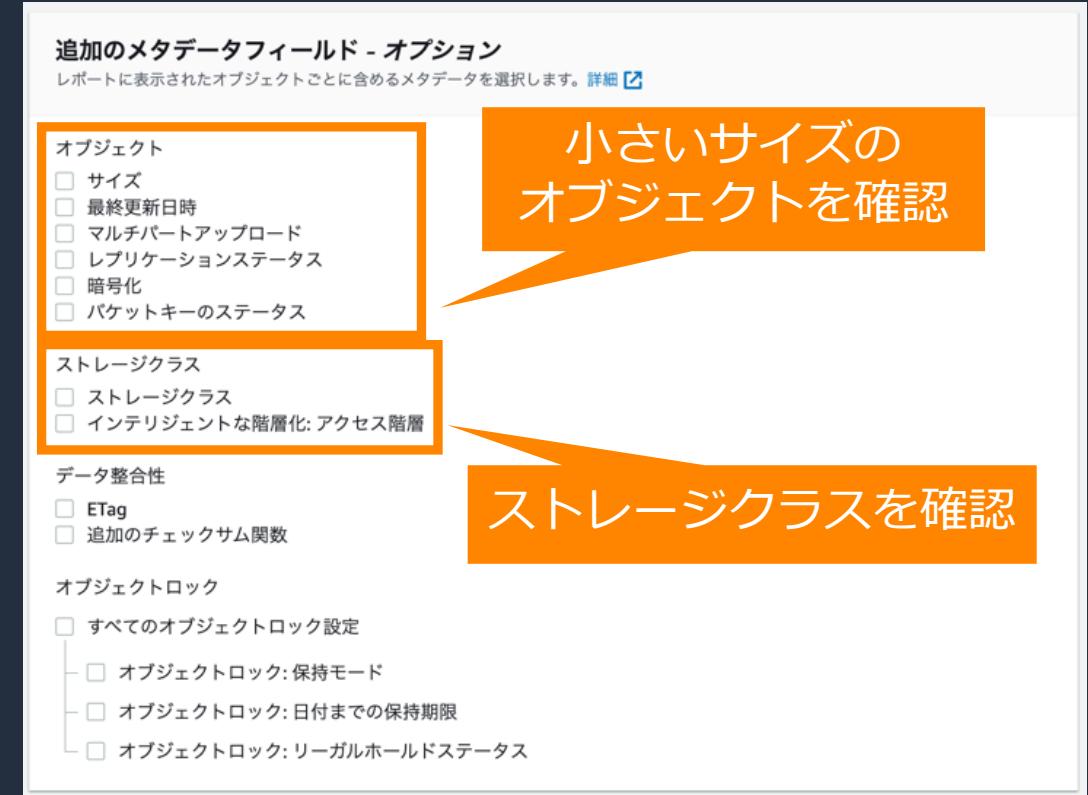
手順

1. バケットを選択→メトリクスタブ
2. ストレージクラス分析の「分析設定を作成」
3. 必要に応じて設定スコープを変更し、対象オブジェクトを絞り込む

Amazon S3 インベントリ

オブジェクトのレプリケーション状況や暗号化状況等のステータスを監査、レポートとして出力

- ✓ オブジェクトのリストを定期的に出力
- ✓ 毎日 or 每週日曜日から選択可能
- ✓ S3 List API を使用しないので
リクエストレーントに影響なし
- ✓ 出力形式は CSV, Apache ORC,
Apache Parquet から選択可能
- ✓ 出力できる情報は右画像を参照
- ✓ S3バケットごとに管理タブから設定可能

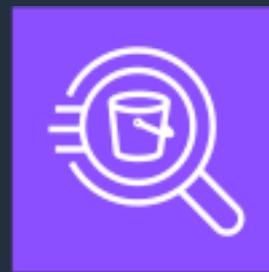
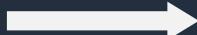


Amazon S3 インベントリの活用例

Amazon Athena により SQL を用いてオブジェクトの状況を分析する



インベントリ
レポート



Amazon
Athena

インベントリレポートに
対して SQL でクエリ

最低容量なし



S3 標準



S3 Intelligent-
Tiering



S3 標準-IA



S3 One
Zone-IA

最低 128 KB



S3 Glacier
Flexible Retrieval

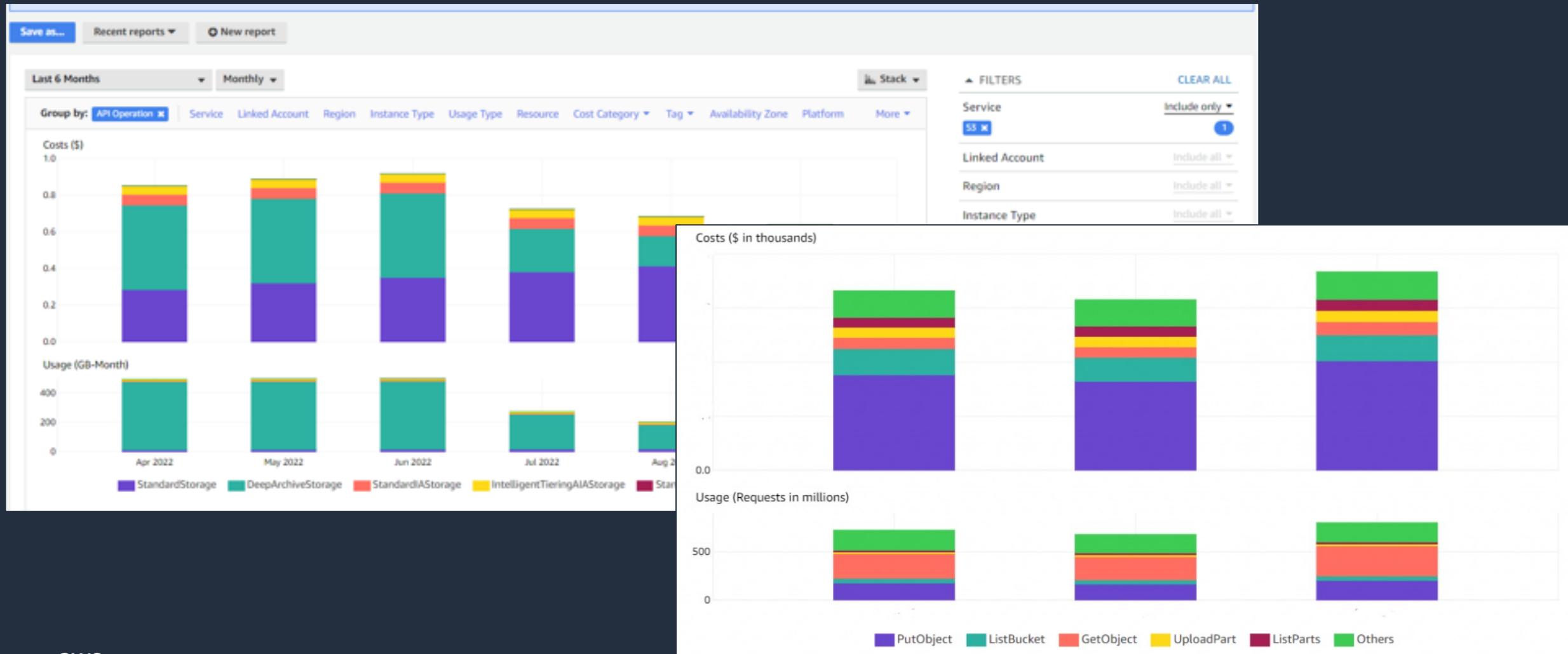


S3 Glacier
Deep Archive

推奨 1 MB 以上

AWS Cost Explorer

AWS リソースの使用量や使用料金を、可視化して確認できるツール



AWS Cost Explorer - Demo

AWS コスト管理 > Cost Explorer > 新しいコストと使用状況レポート

新しいコストと使用状況レポート

コストと使用量のグラフ 情報

合計コスト \$24.79

1 日あたりの平均コスト \$0.53

リージョン カウント 17

コスト (\$)

5月-15

リージョン	コスト (\$)
米国東部 (バージニア北部)	\$0.24
米国西部 (オレゴン)	\$0.22
アジアパシフィック (シンガポール)	\$0.09
アジアパシフィック (東京)	\$0.00
欧州 (フランクフルト)	\$0.00
欧州 (アイルランド)	\$0.00
アジアパシフィック (シドニー)	\$0.00
米国東部 (オハイオ)	\$0.00
EU (Stockholm)	\$0.00
その他	\$0.00
合計コスト	\$0.55

5月-17*

リージョン	コスト (\$)
米国東部 (バージニア北部)	\$0.00
米国西部 (オレゴン)	\$0.00
アジアパシフィック (シンガポール)	\$0.00
アジアパシフィック (東京)	\$0.00
欧州 (フランクフルト)	\$0.00
欧州 (アイルランド)	\$0.00
アジアパシフィック (シドニー)	\$0.00
米国東部 (オハイオ)	\$0.00
EU (Stockholm)	\$0.00
その他	\$0.00
合計コスト	\$0.55

レポートパラメータ

▼ 時刻

日付範囲 2023-04-01 — 2023-04-30

粒度 日別

グループ化 : リージョンを指定
リージョンごとの料金を確認が可能

▼ グループ化の条件

ディメンション クリア
リージョン

▼ フィルター 情報

適用フィルター (2) すべてをクリア

サービス クリア
サービス を含む (1)
S3 (Simple Storage Service) X

連結アカウント クリア
連結アカウント を選択

リージョン リージョン を選択

フィルター : S3を指定
S3 で発生した料金に絞り込み

参考ブログ : Optimize storage costs by analyzing API operations on Amazon S3

<https://aws.amazon.com/jp/blogs/storage/optimize-storage-costs-by-analyzing-api-operations-on-amazon-s3/>

AWS Cost Explorer

參考資料



[AWS Black Belt Online Seminar] AWS Cost Explorer

AWS Customer Service TCSA 中村一至
2020.1.29

AWS 公式 Webinar
<https://amzn.to/JPWebinar>



過去資料
<https://amzn.to/JPArchive>



© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

https://pages.awscloud.com/rs/112-TZM-766/images/20200129_BlackBelt_CostExplorer.pdf

© 2023, Amazon Web Services, Inc. or its affiliates.



Amazon S3 におけるコスト最適化のポイント

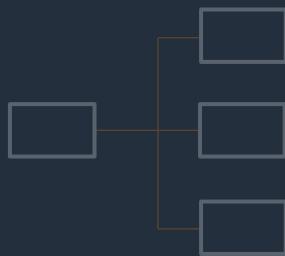
1



アプリケーション
要件の整理



2



データ配置の
設計



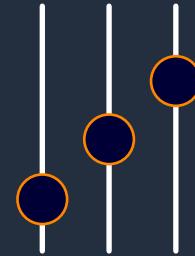
3



ストレージ状況把握、
分析、最適化



4



継続的な
サイジング

継続的なサイジング：アプローチ例

アプリケーション等から
直接アップロードする場合

例

API 経由で S3 にアップロード、
バックアップ等用途が明確な場合

データの利用頻度が
ある程度予測可能な場合

例

格納後、一定期間経過で
利用頻度が低下するような場合

データの利用頻度が
予測不可能な場合

例

データは断続的に利用、
アクセスパターンが読めない場合



ストレージクラスを指定して PUT



ライフサイクルポリシー



S3 Intelligent-Tiering



Amazon S3 ライフサイクル

ライフサイクルを使用して、他のストレージクラスにオブジェクトを移動する

ライフサイクルルールを使用することで、
保存日数を基にストレージクラスを変更できる

例



S3 標準

30 日



S3 Glacier
Instant Retrieval

150 日



S3 Glacier
Deep Archive

ライフサイクルフィルターとアクションの詳細



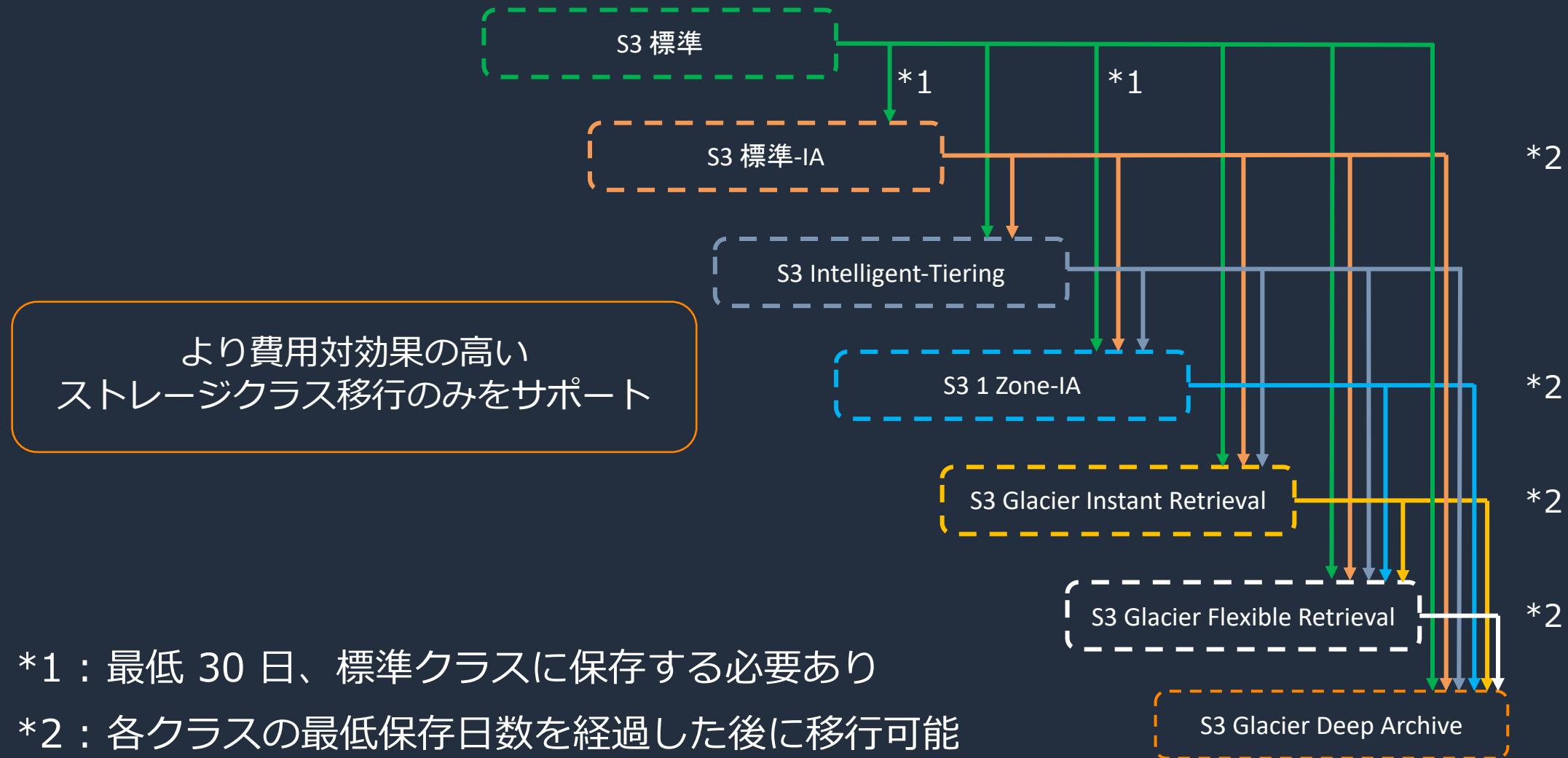
フィルター

- ✓ プレフィックス
- ✓ タグ
- ✓ 最小 or 最大オブジェクトサイズ

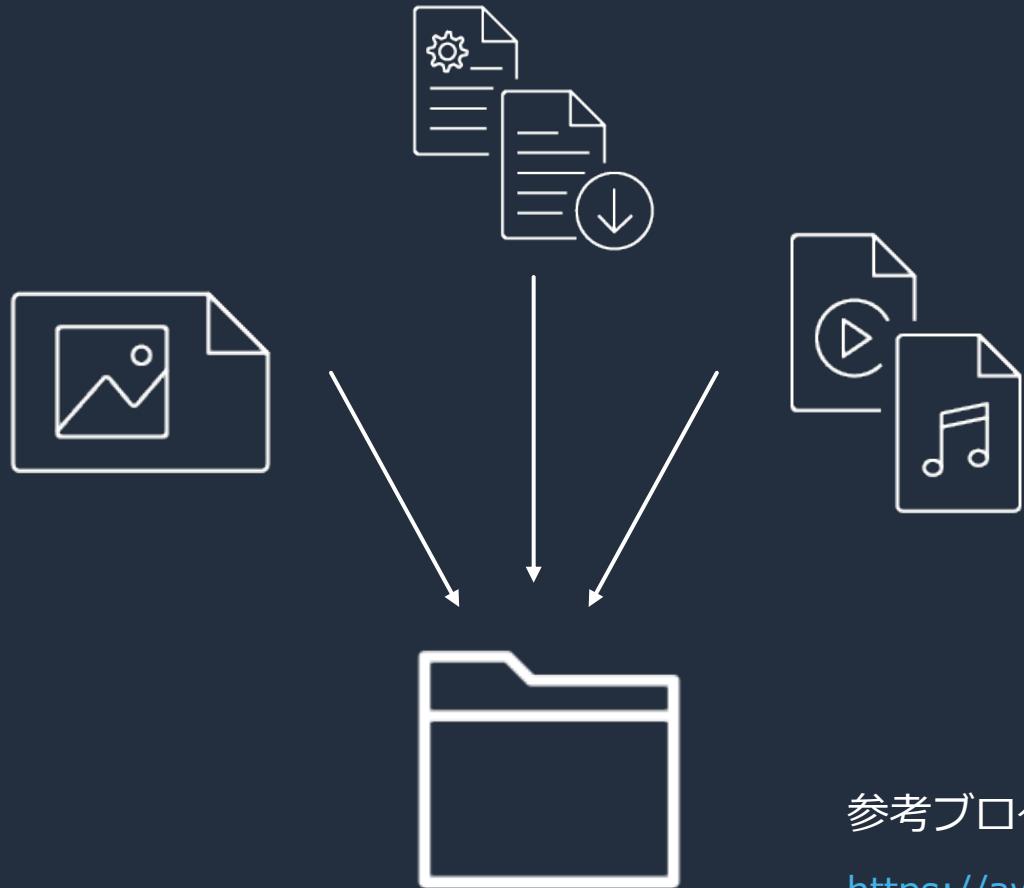
アクション

- ✓ ストレージクラスの移動
- ✓ オブジェクトの削除
- ✓ バージョニングを利用している場合
非現行バージョンのストレージクラス変更や削除
- ✓ 不完全なマルチパートアップロードを削除

ライフサイクルにおけるストレージクラスの移行先



小さいサイズのオブジェクト取り扱いについて



Glacier 等の低階層ストレージクラス
を利用する場合

- 複数のオブジェクトを束ねて圧縮
など、オブジェクトサイズを
大きくすると効果的。

参考ブログ : Amazon S3 Glacier ストレージクラスへのログの圧縮とアーカイブ

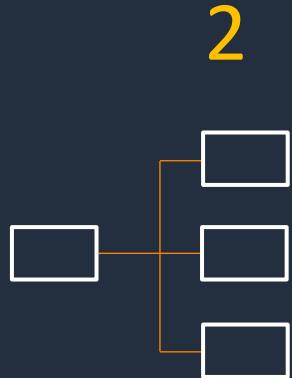
<https://aws.amazon.com/jp/blogs/news/compressing-and-archiving-logs-to-the-amazon-s3-glacier-storage-classes/>

まとめ

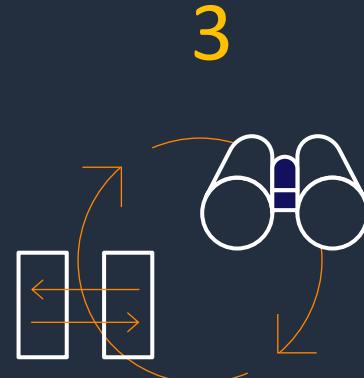
まとめ：Amazon S3 におけるコスト最適化のポイント



1
アプリケーション
要件の整理



2
データ配置の
設計



3
ストレージ状況把握、
分析、最適化



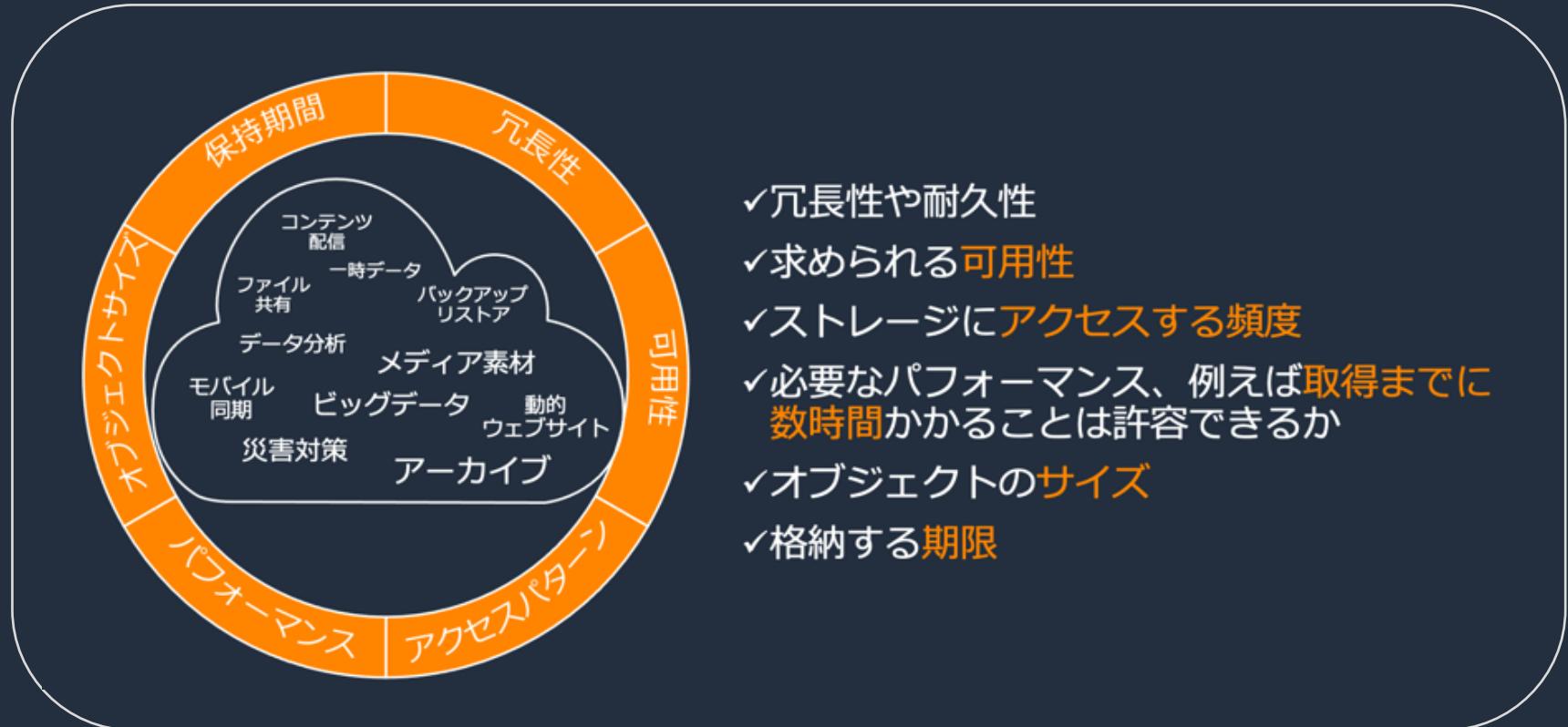
4
継続的な
サイジング

まとめ：Amazon S3 におけるコスト最適化のポイント

1

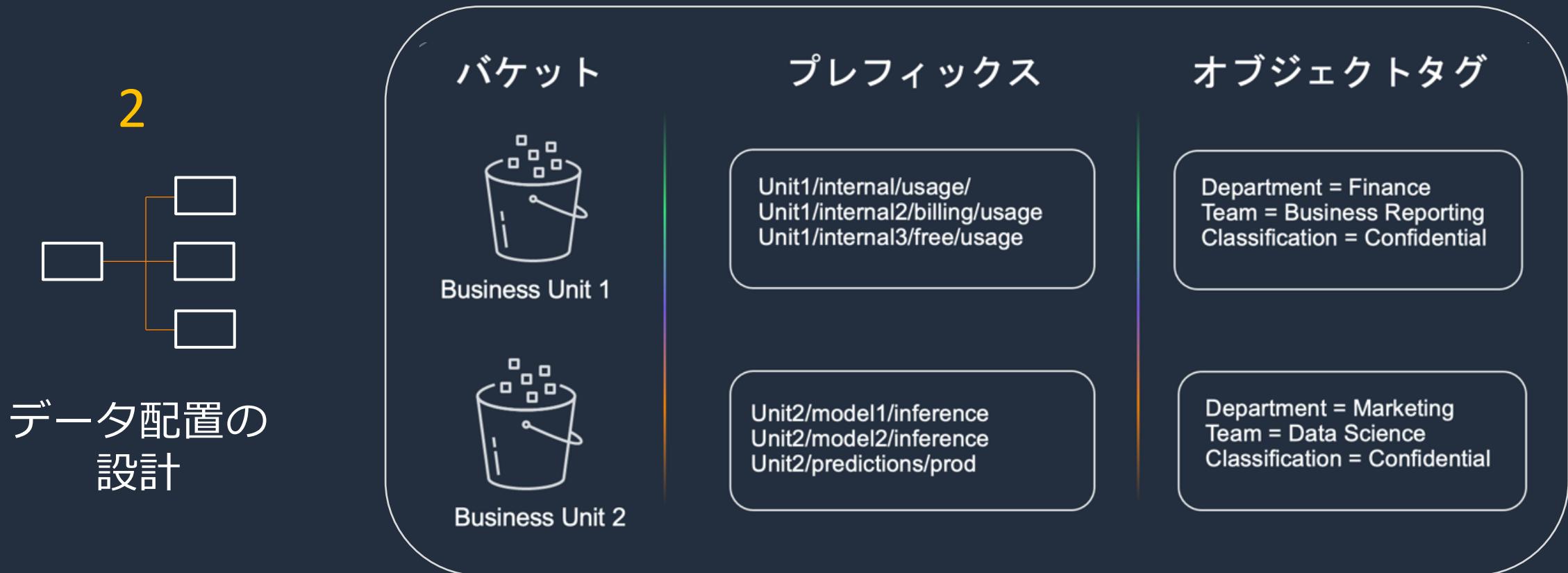


アプリケーション
要件の整理



これらの要件を整理することで、
適切なストレージクラスの選定が可能に

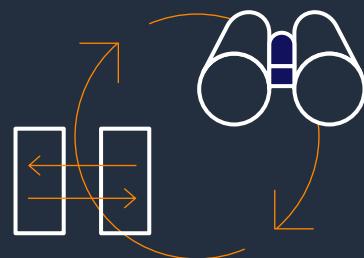
まとめ：Amazon S3 におけるコスト最適化のポイント



バケット、プレフィックス、タグを使って配置を設計
オブジェクトの利用特性を設計に反映させる

まとめ：Amazon S3 におけるコスト最適化のポイント

3



ストレージ状況把握、
分析、最適化

Storage Lens



コスト最適化のための
S3 使用状況の可視化と
ダッシュボード

ストレージクラス
分析



ストレージの
アクセスパターン分析

S3 Inventory

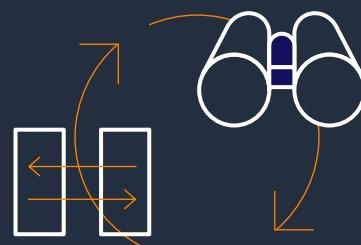


分析や監査のための
オブジェクトレベルの分析

オブジェクトの使用状況やアクセスパターンを分析

まとめ：Amazon S3 におけるコスト最適化のポイント

4



継続的な
サイジング

S3 Intelligent-Tiering	S3 Standard (S3 標準)	S3 Standard-IA (S3 標準-IA)	S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval	S3 Glacier Deep Archive	S3 One Zone-IA (S3 1 ゾーン-IA)
AZ 間の冗長性	複数のアベイラビリティゾーン (AZ)					1つの AZ
想定されるデータタイプ	アクセスパターンが想定できない/変化するデータ	頻繁にアクセスされるアクティブデータ	アクセス頻度が低いデータ	即時取り出しが必要なアーカイブデータ	ほとんどアクセスされないアーカイブデータ	長期保存のアーカイブデータ
オブジェクトの耐久性	99.999999999%	99.999999999%	99.999999999%	99.999999999%	99.999999999%	99.999999999%
データの可用性	99.9%	99.99%	99.9%	99.9%	99.99%	99.99%
レイテンシー	ミリ秒単位のアクセス	ミリ秒単位のアクセス	ミリ秒単位のアクセス	ミリ秒単位のアクセス	分から時間単位の復元(数分~12時間)	時間単位の復元(12~48時間)
取り出し料金	なし	なし	GBあたり	GBあたり	GBあたり	GBあたり
最小ストレージ期間(最低保存期間)	–	–	30日	90日	90日	180日
最小オブジェクトサイズ	–	–	128 KB	128 KB	40 KB	40 KB
ストレージ価格*	0.025 ~ 0.002 USD/GB月	0.025 ~ 0.023 USD/GB月	0.0138 USD/GB月	0.005 USD/GB月	0.0045 USD/GB月	0.002 USD/GB月
						0.011 USD/GB月

最適なストレージクラスを利用しコストを最適化
ライフサイクルポリシーによりストレージクラスを自動的に移行

本資料に関するお問い合わせ・ご感想

技術的な内容に関しましては、有料のAWSサポート窓口へ
お問い合わせください

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

料金面でのお問い合わせに関しましては、カスタマーサポート窓口へ
お問い合わせください（マネジメントコンソールへのログインが必要です）

<https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service>

具体的な案件に対する構成相談は、後述する個別相談会をご活用ください



ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt



その他コンテンツのご紹介

ウェビナーなど、AWSのイベントスケジュールをご参照いただけます

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

ハンズオンコンテンツ

<https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/>

AWS 個別相談会

AWSのソリューションアーキテクトと直接会話いただけます

<https://pages.awscloud.com/JAPAN-event-SP-Weekly-Sales-Consulting-Seminar-2021-reg-event.html>



Thank you!



Amazon Simple Storage Service (Amazon S3)

ユースケース編

宮城 康暢

Amazon Web Service Japan G.K.

Solutions Architect

2023/01

AWS Black Belt Online Seminarとは

- ・ 「サービス別」「ソリューション別」「業種別」などのテーマに分け、
アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナー
シリーズです
- ・ AWSの技術担当者が、AWSの各サービスやソリューションについてテーマご
とに動画を公開します
- ・ 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も
可能、スキマ時間の学習にもお役立ていただけます
- ・ 以下のURLより、過去のセミナー含めた資料などをダウンロードするこ
とができます
 - ・ <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>
 - ・ <https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY>

内容についての注意点

- ・ 本資料では2023年01月時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(<https://aws.amazon.com/>)にてご確認ください
- ・ 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます
- ・ 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます

自己紹介

名前：宮城 康暢 (Koyo Miyagi)

所属：アマゾン ウェブ サービス ジャパン合同会社
技術統括本部 エンタープライズソリューション本部
パートナーサクセスソリューション部

経歴：国内SI会社でエンジニアとして
ストレージサービスやIaaSの開発・運用に従事

好きなAWSサービス：
Amazon FSx シリーズ、Amazon S3



本セミナーの対象者

前提知識

- AWSの基本的な知識
- Amazon S3 入門編(※) あるいは 同等の知識

対象者

- Amazon S3の具体的なユースケースにご興味のある方
- Amazon S3を効果的に活用できていないという課題感のある方

(※) Amazon Simple Storage Service (Amazon S3) 入門編

- 資料 : https://pages.awscloud.com/rs/112-TZM-766/images/AWS-Black-Belt_2022_Amazon_S3_for_Beginner_1231_v1.pdf
- 動画 : <https://www.youtube.com/watch?v=wQ8ZDvoMSno>

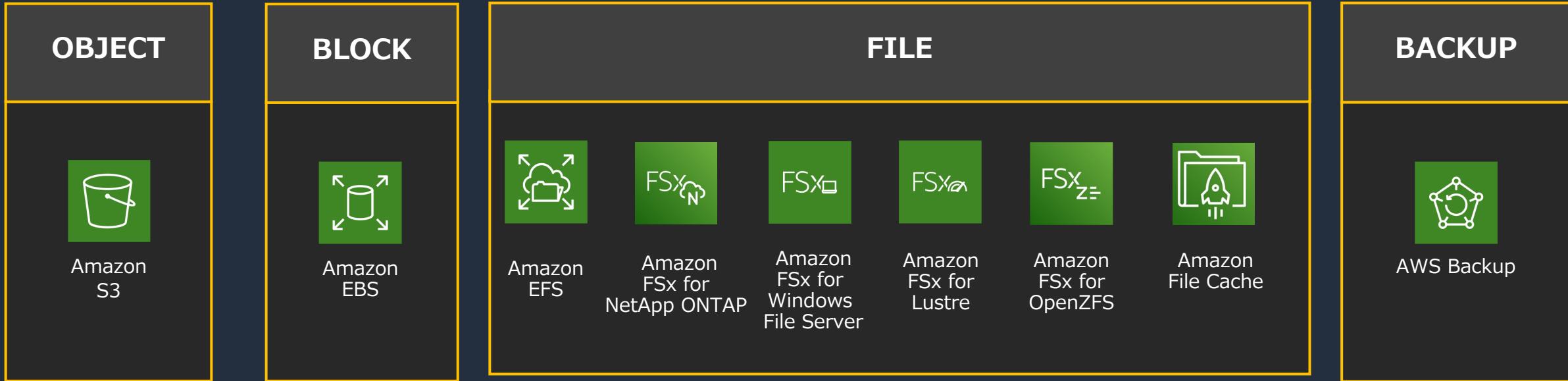


アジェンダ

- Amazon S3 の概要（おさらい）
- Amazon S3 のユースケース
 - データ保護・移行
 - データレイク
 - Webサービスのコンテンツオフロード

Amazon S3 の概要 (おさらい)

AWS のストレージサービス



DATA TRANSFER AND MIGRATION



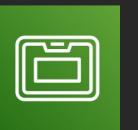
AWS Storage
Gateway



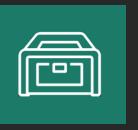
AWS DataSync



AWS Transfer
Family



AWS Snowball



AWS Snowcone

Amazon S3 とは

高いパフォーマンスと可用性、そして低コストが特徴なオブジェクトストレージ
2006 年に登場してから、現在に至るまでのイノベーションが積み重なった歴史あるサービス

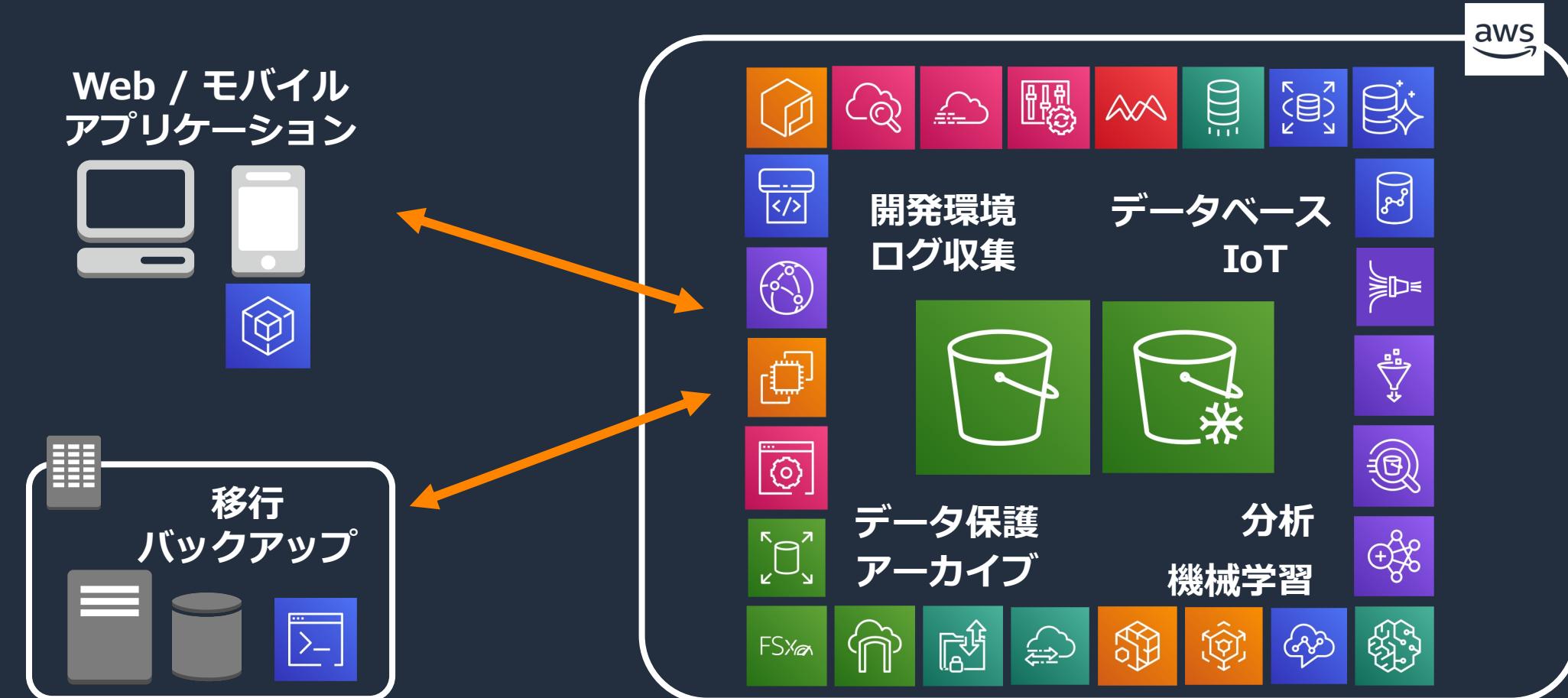
- 耐久性
 - 99.99999999% (イレブンナイン)
 - 最低 3 つのアベイラビリティゾーン (AZ) で冗長化
- スケーラビリティ
 - 無制限のデータ保存
 - ただし、1 オブジェクトは最大 5 TB
- 低コスト
- セキュリティ
 - アクセス制御とログ監査
- データの保護
 - 誤削除から守る機能
- アクセシビリティ
 - HTTP/HTTPS でアップロード/ダウンロード/変更/削除といった操作が可能
- 様々な AWS サービスとの連携



Amazon S3 の特徴などは FAQ にて詳解: <https://aws.amazon.com/jp/s3/faqs/?nc=sn&loc=7>

Amazon S3 にデータが格納されるシーン

高度な特徴・豊富な機能により、さまざまなシーンでデータが格納される
AWSサービスのデータ保管場所の1つとしても利用されている

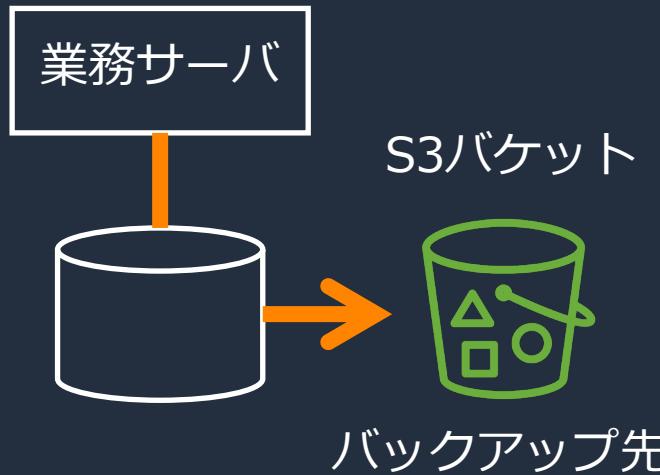


Amazon S3 へのアクセス方法

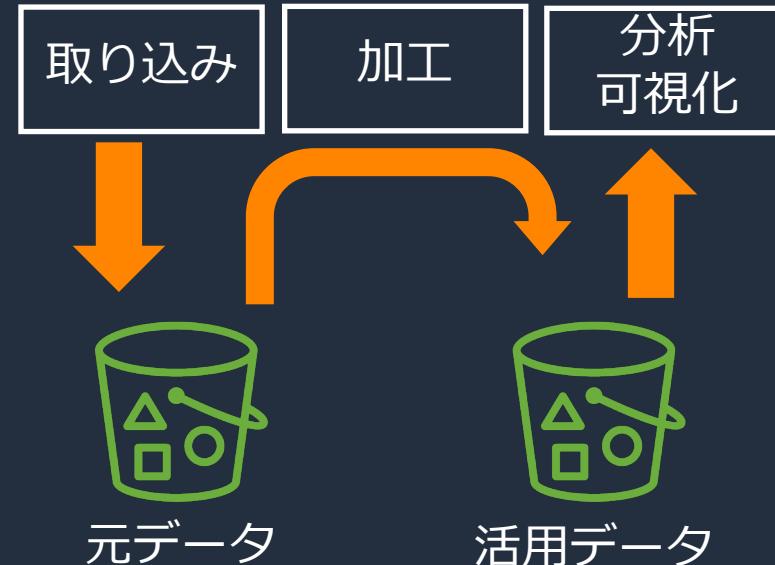
アクセス方法	説明・利用イメージ			
Management Console			AWSクラウドにアクセスして管理するためのウェブインターフェイス 	
AWS CLI		<pre>\$ aws s3 cp xxxx.mp4 s3://bucketName/ \$ aws s3api get-object --bucket-name <bucket-name> --key <prefix/file-name></pre>		
AWS SDK		<pre>PutObjectRequest putObjectRequest = new PutObjectRequest(bucketName, Key, file); PutObjectResult result = this.client.putObject(putObjectRequest)</pre>		
AWSサービス (S3と連携)			S3へのデータコピー機能を提供するサービス 	S3への追加のアクセス方法(読み込み、または書き込み)を提供するサービス
3 rd Party Tools		S3連携機能を備えたソフトウェア・ツール バックアップソフトウェアによるバックアップ・リストア等		

Amazon S3 のユースケースの分類

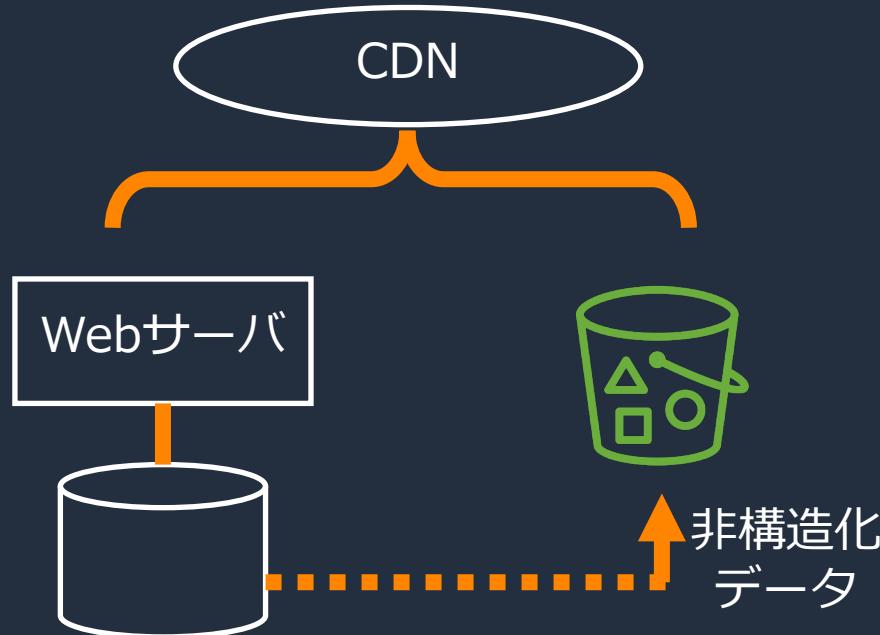
データ保護・移行



データレイク



Webサービスのコンテンツオフロード



- ・アーカイブ、バックアップによる活用
- ・データ移行

- ・データ分析基盤
- ・機械学習・IoT
- ・HPC・映像処理

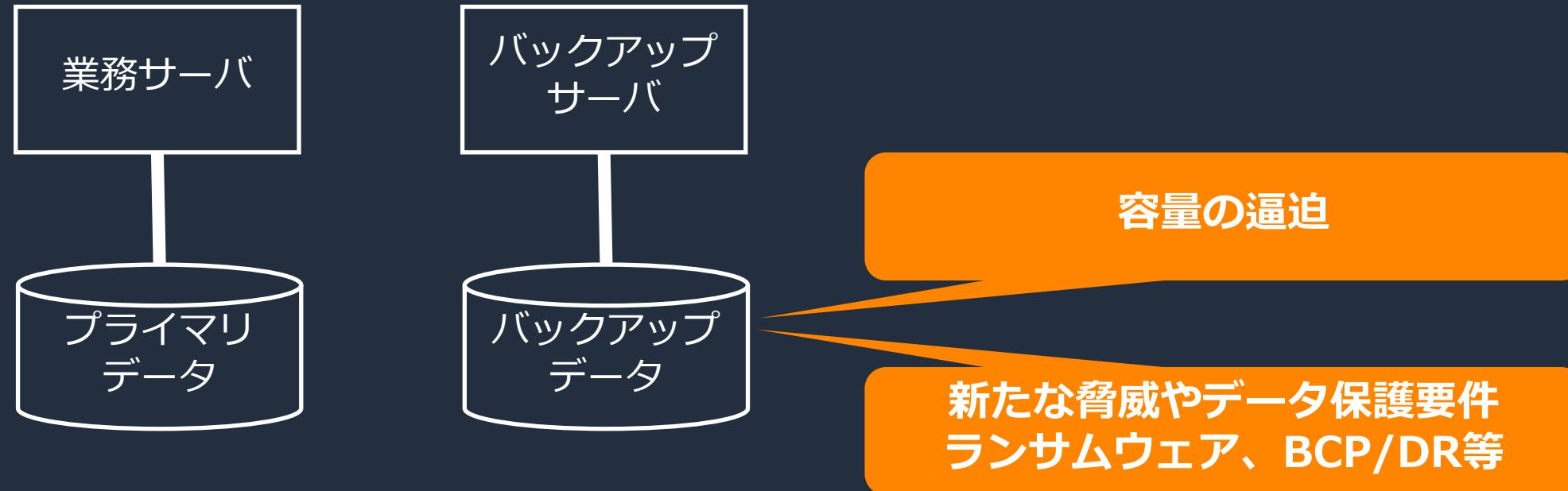
- ・写真管理サイト
- ・動画サイト
- ・ECサイト

Amazon S3のユースケース

①データ保護・移行

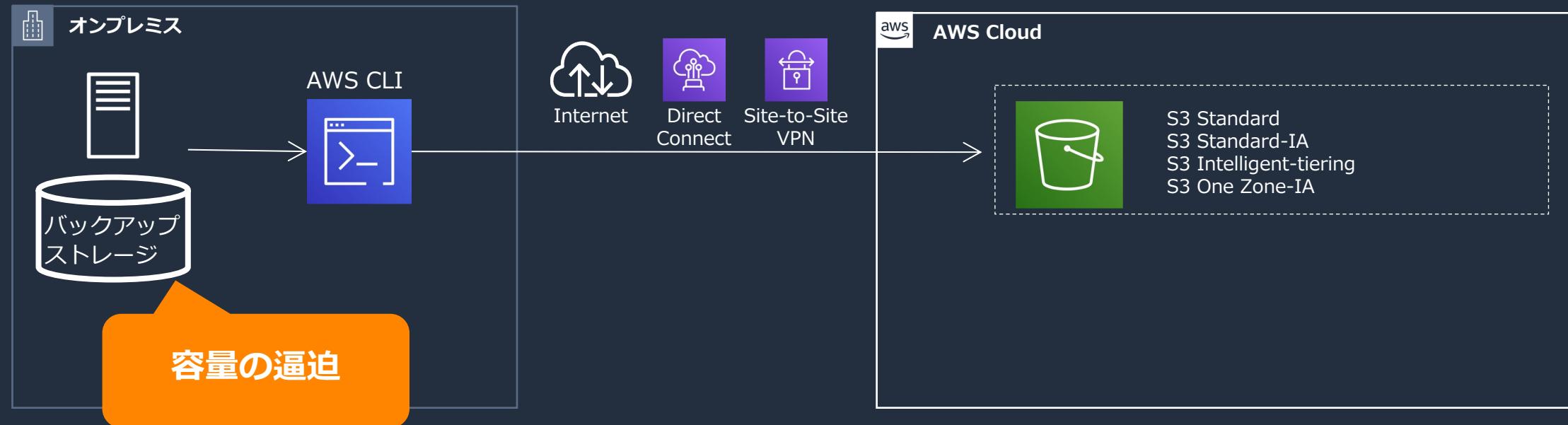
データ保護・移行における課題

- ・ オンプレミスのストレージ容量が逼迫している
- ・ 新たなデータ保護の要件（ランサム対策、BCP/DR等）にインフラ整備が間に合わない



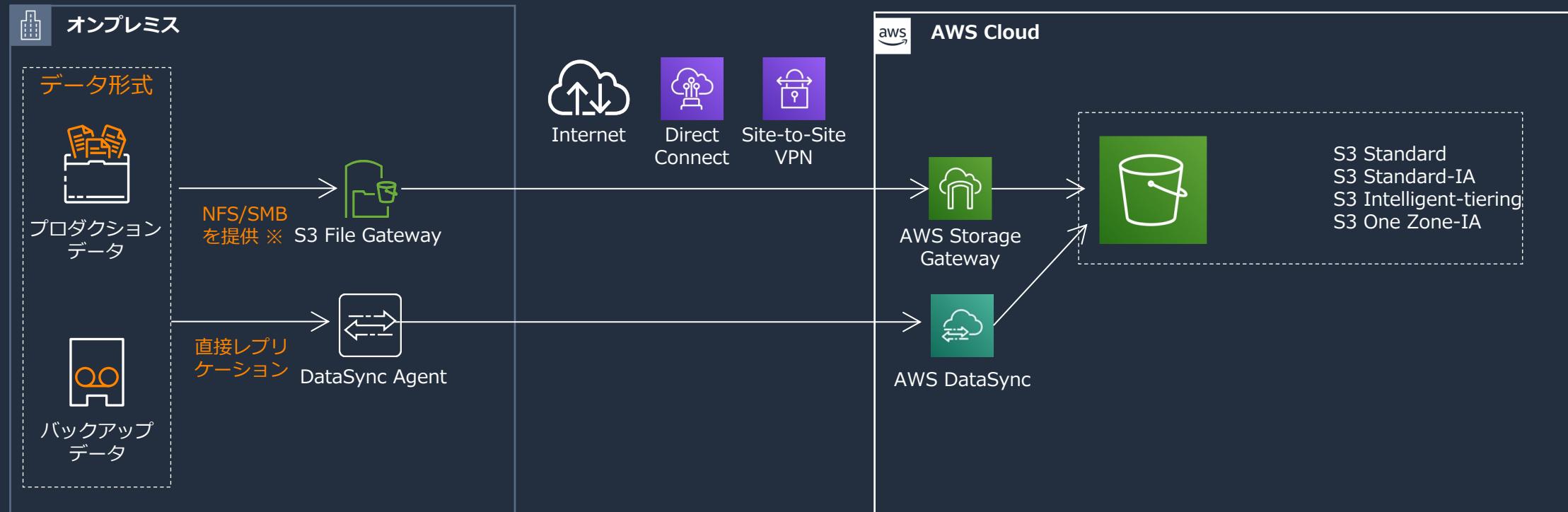
AWS CLIを使用してバックアップデータをS3へコピー

- ・バックアップサーバのストレージ容量逼迫を解消
- ・AWS CLI（要インストール）を使用することで構成変更も最小化



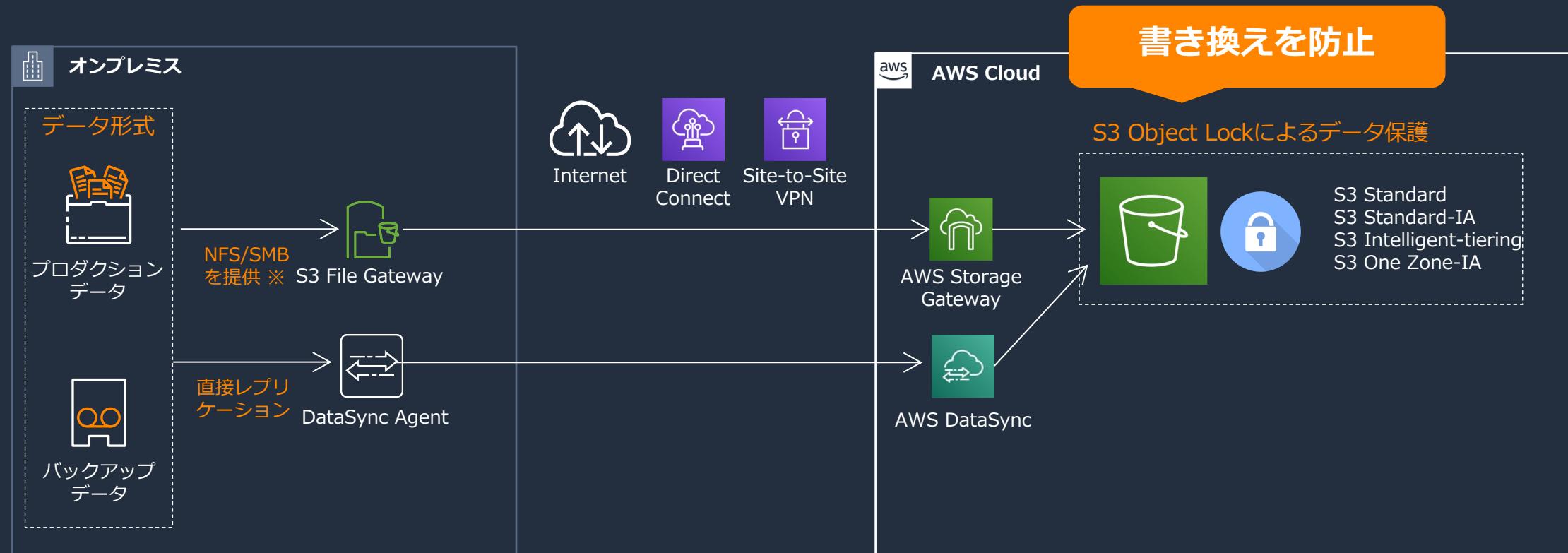
既存環境の要件に応じて、S3への書き込み手段を選択

- S3 File Gatewayを使用して、NFS/SMB(OS標準プロトコル)を利用して
- AWS DataSyncを使用して、データ同期を自動化・省力化



バックアップデータに対して、S3 Object Lockを有効化

- ・S3 Object Lockを使用して、データの書き換えを防止
- ・ランサムウェアのリスクを軽減



※ Storage Gateway はデータをS3にコピーする目的、バックアップやアーカイブする目的で利用します。
一般的なオフィスアプリケーション用のファイルサーバとしてのご利用には適しません。

一定期間経過後、安価なストレージクラスへ移動

- リストアの要件に応じたストレージクラスを活用し、コストを最適化



※ Storage Gateway はデータをS3にコピーする目的、バックアップやアーカイブする目的で利用します。
一般的なオフィスアプリケーション用のファイルサーバとしてのご利用には適しません。

既存バックアップシステムのS3連携機能を活用

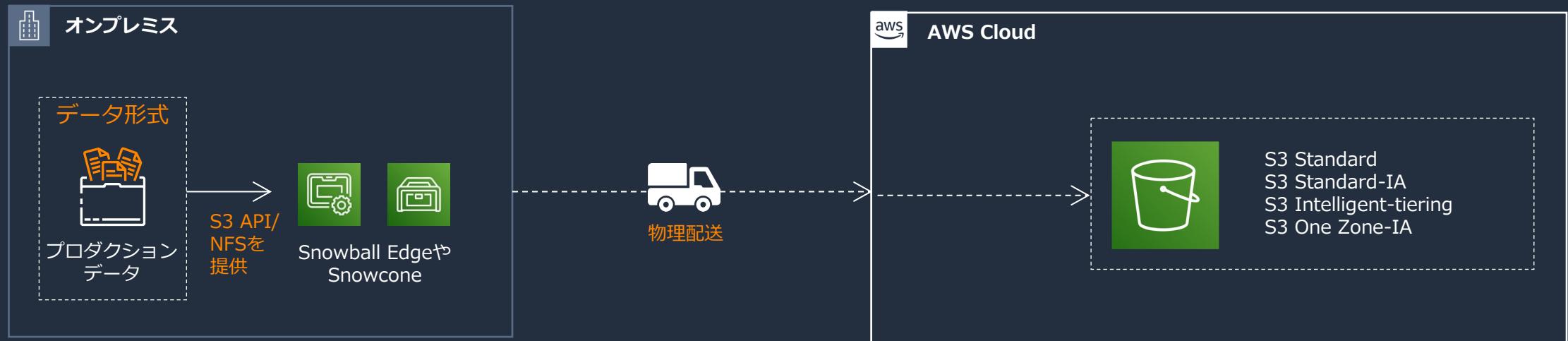
- ・ バックアップソフトのS3連携機能により、バックアップデータをS3へ保管
- ・ 既存バックアップソフトの高度なバックアップ・リカバリを踏襲
 - 有事の際にクラウドへシステムを復元するなど（※）



※ バックアップソリューションによって、構成、提供できる機能は違います。
※ 詳しくはバックアップベンダーにお問い合わせください。

コピー対象のデータ量が膨大な場合、オフライン移行も検討

- AWS Snow ファミリーを手配してオフラインでデータ移行、S3 ヘインポート
 - オンプレミス環境とAWS Cloud間の回線帯域が少ない
 - コピー対象データの更新・追加が発生しない（または限定的である）

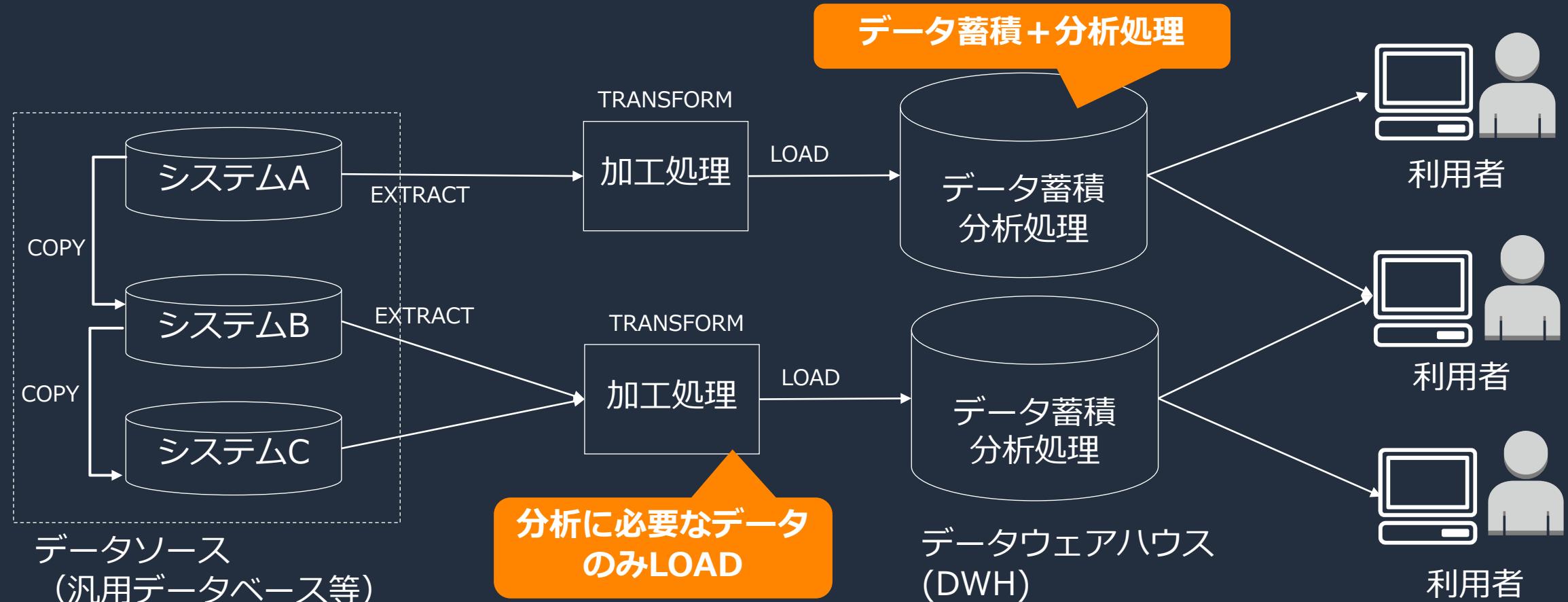


AWS Snow ファミリー : <https://aws.amazon.com/jp/snow/>

Amazon S3のユースケース ②データレイク

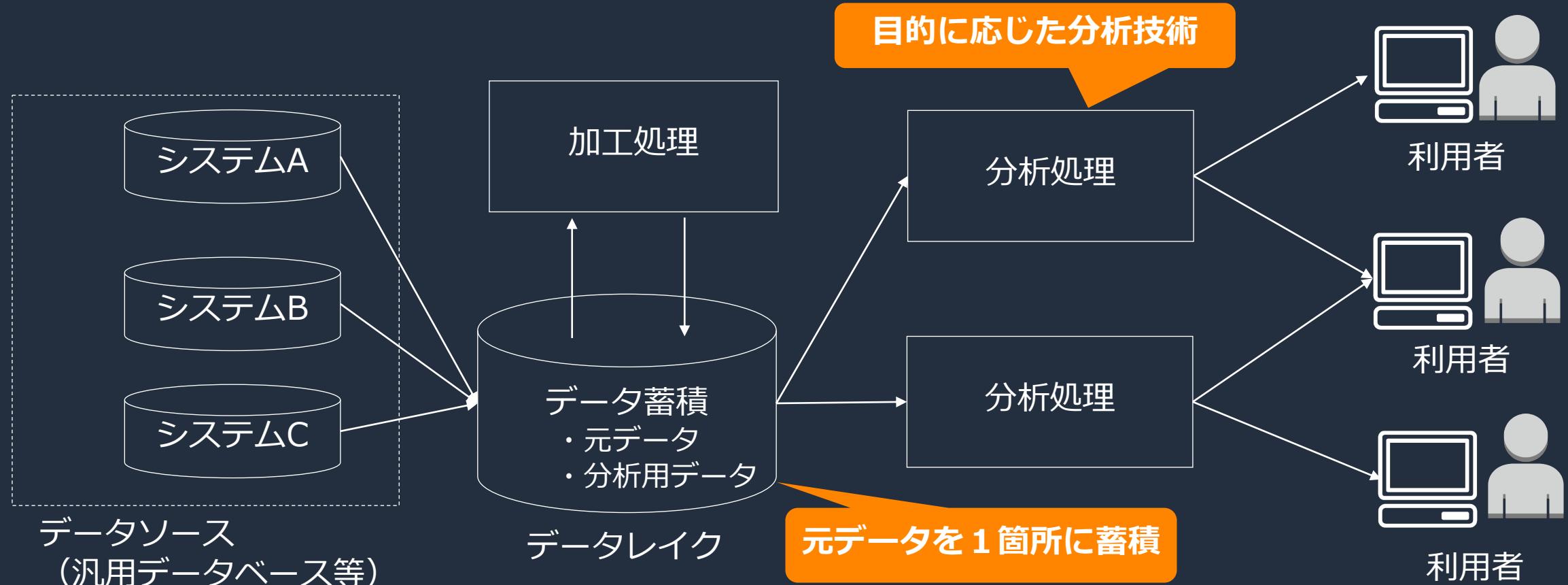
データ分析基盤における課題

- 各システムでデータを所有(サイロ化)、統合した分析が困難
- 分析に必要なデータのみDWHへ格納、新しい分析ニーズへの対応が困難



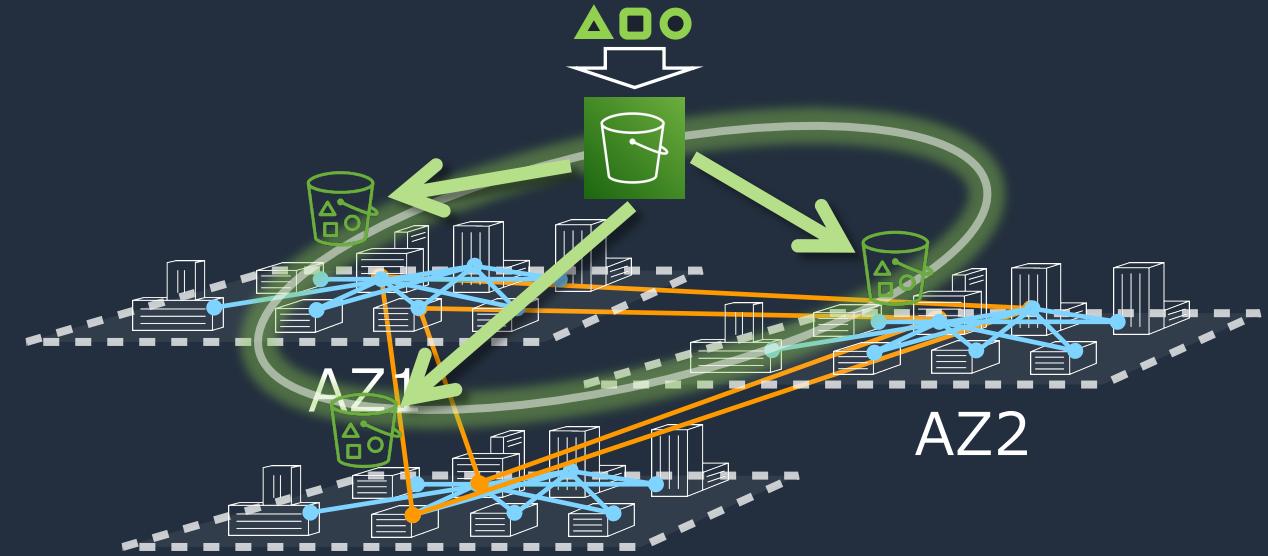
分析の高度化に向けたデータレイクのアプローチ

- ・元データをデータレイクに蓄積し、将来的なニーズに対応
- ・分析・可視化といった活用部分は取り替え可能な構成



S3 がデータレイクのストレージに最適な理由

- 高い耐久性
 - 99.99999999%の耐久性
- スケーラビリティ
 - 容量：無制限（1ファイル最大5TBまで）
 - 性能：データ容量に依存しない性能 ※1
- 安価なストレージ
 - 容量単価：月額1GBあたり約3円 ※2
 - コスト最適化：ライフサイクル機能、豊富なストレージクラス
- 豊富なアクセス手段、データ管理機能
 - AWSのさまざまなサービスとシームレスに連携
 - APIの提供により、多くのソフトウェアやサービスでS3との連携をサポート
 - セキュリティに関する機能（アクセス制御やログ監査など）、追加のデータ保護機能を提供



(※1) https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/optimizing-performance.html

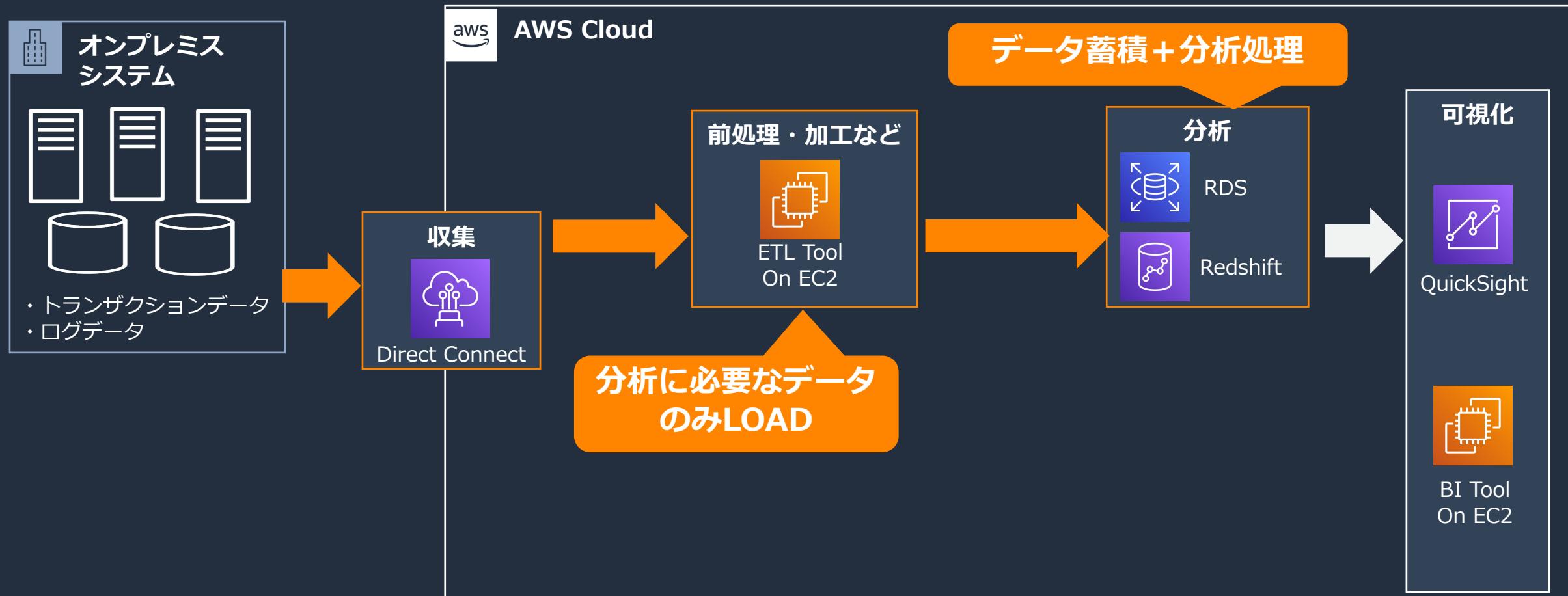
aws (※2) <https://aws.amazon.com/jp/s3/pricing/>

Amazon S3 は様々なサービスと連携



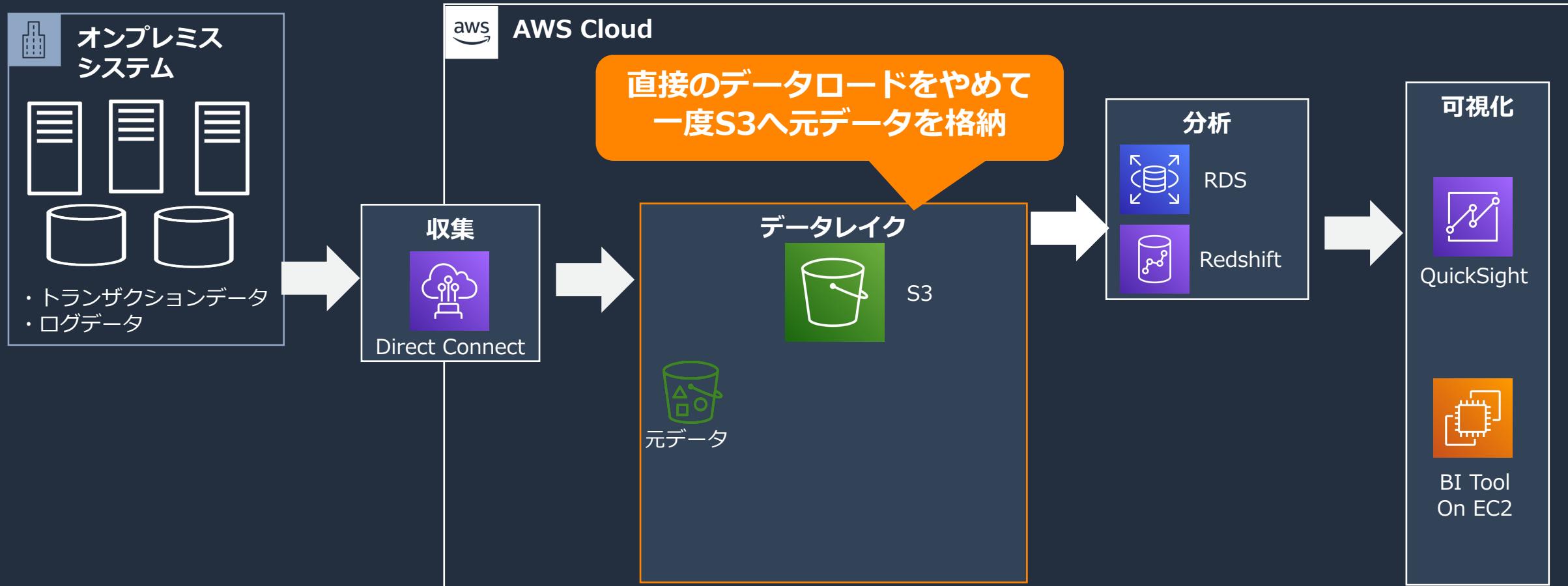
データ分析基盤における課題（再掲）

- 各システムでデータを所有(サイロ化)、統合した分析が困難
- 分析に必要なデータのみDWHへ格納、新しい分析ニーズへの対応が困難



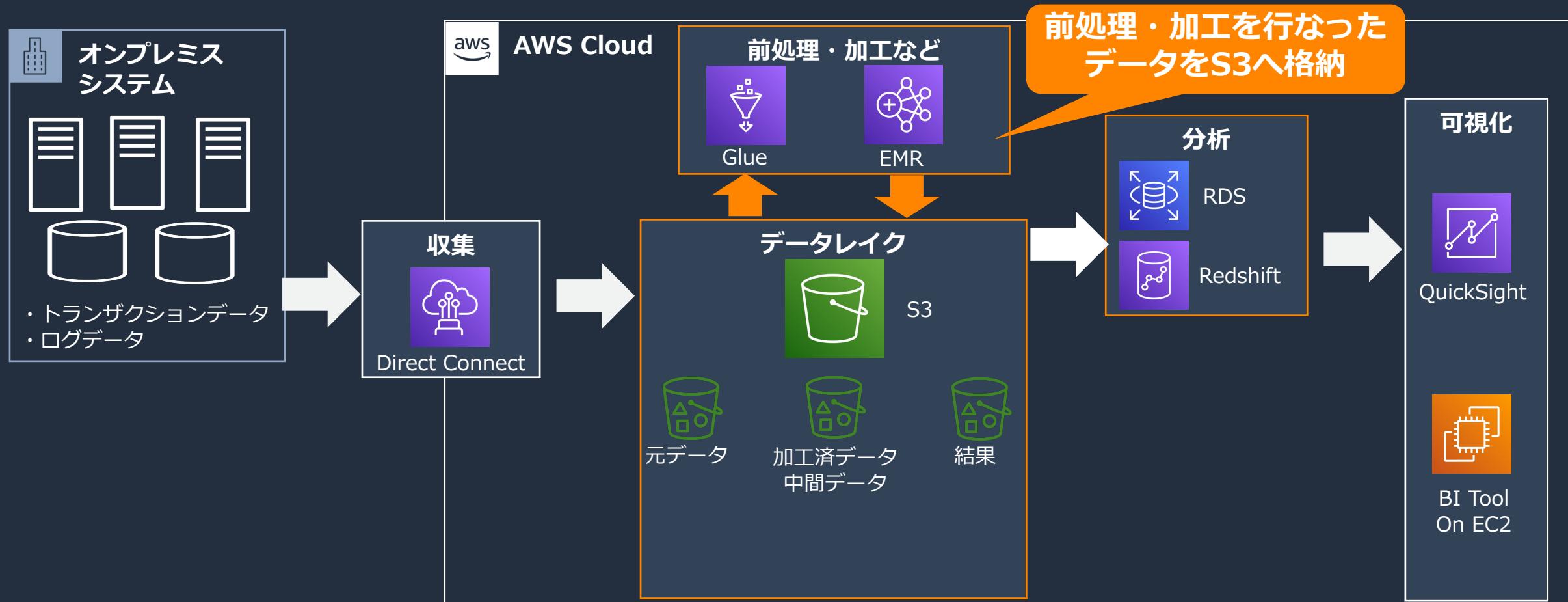
元データを S3 へアップロード・蓄積

- ・データ蓄積と分析処理を疎結合化することで、分析の柔軟性を向上
- ・元データを1箇所へ蓄積することで、将来の分析ニーズに対応



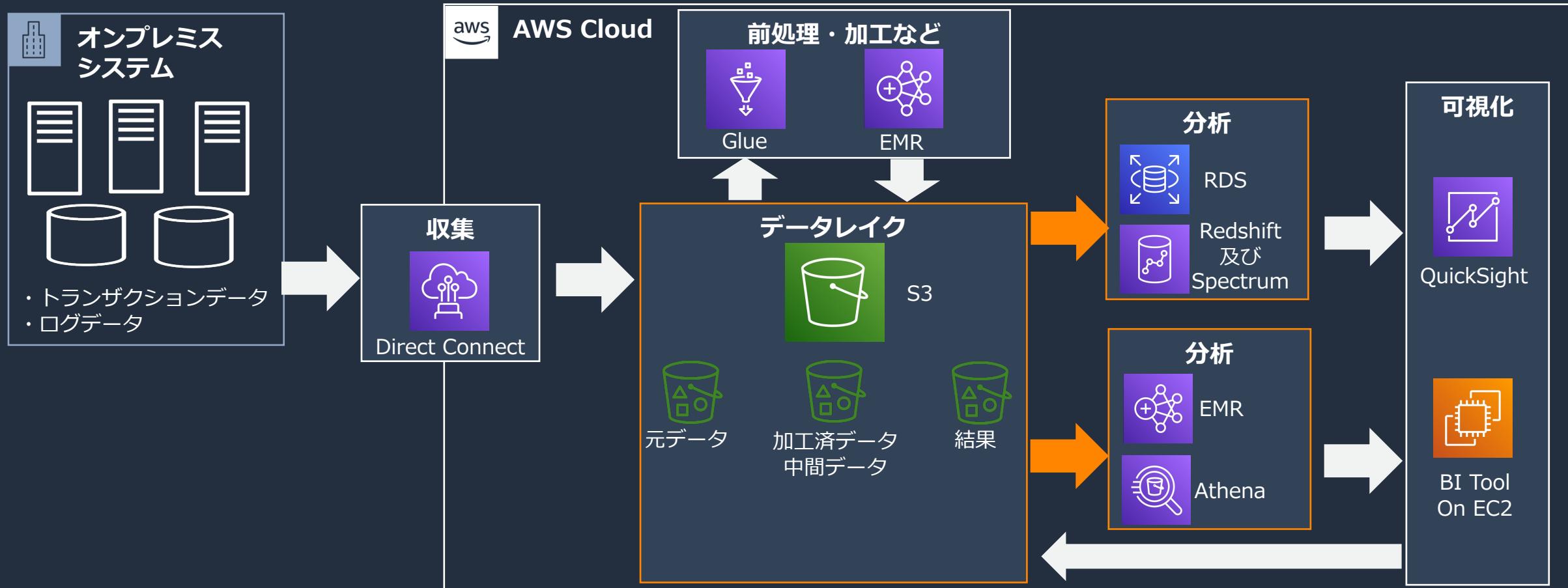
前処理・加工したデータもS3へ保管し、分析に活用

- 元データは分析に最適なフォーマットへ加工
- 加工済データはS3に戻すことで、"加工"と"分析"の処理系を疎結合化



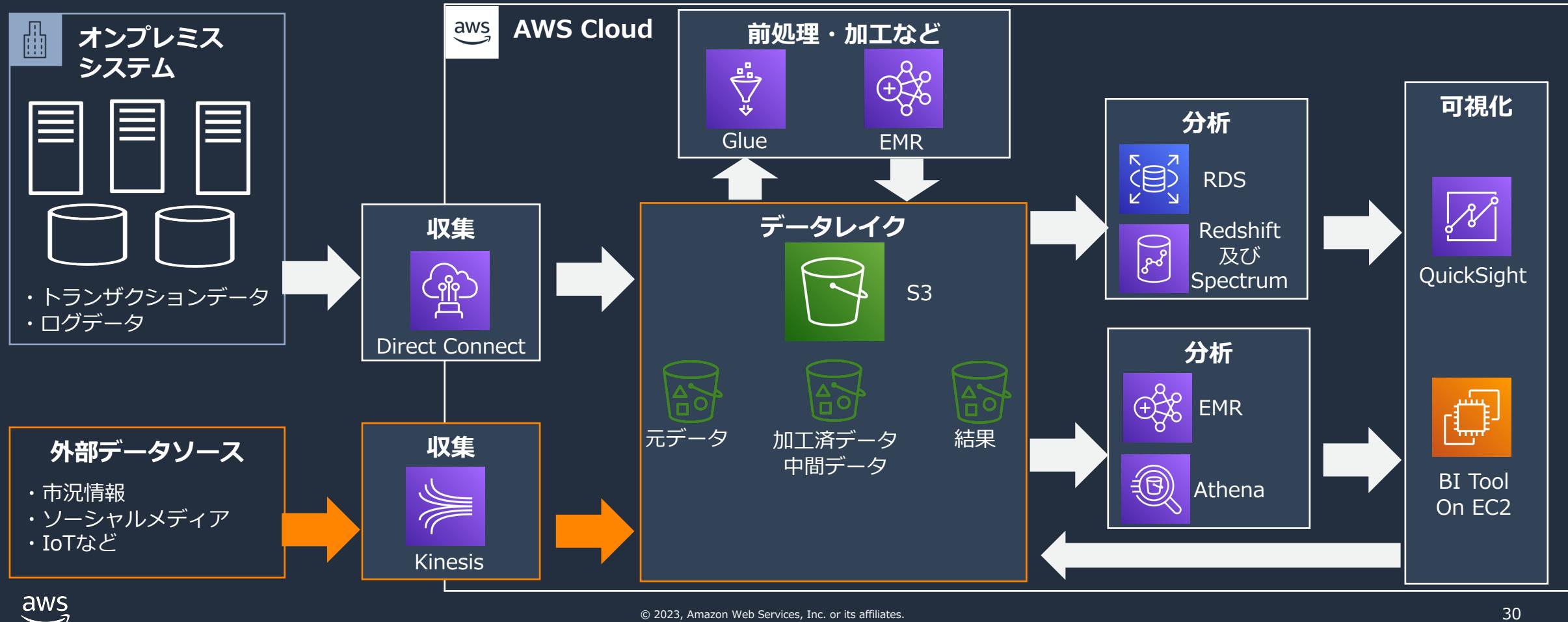
分析ニーズに応じて、最新の分析技術を迅速に適用

- データをS3へ分離したことでの、分析技術の取り替えが容易に
- 蓄積された元データにより、過去データも含めて分析可能



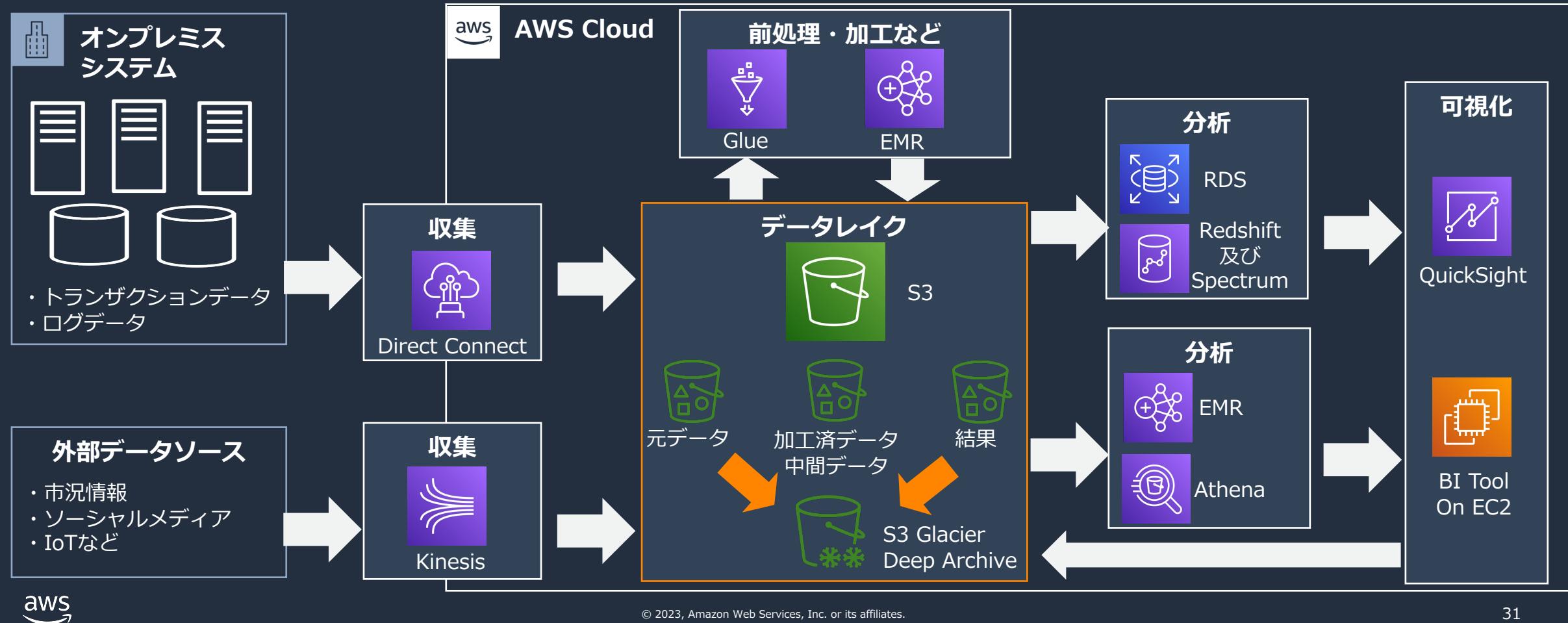
異なる目的のデータも、適切なツールを活用してS3へ保管

- ・データ蓄積と分析処理を疎結合化することで、収集の処理を単純化
- ・S3の豊富な書き込み手段・連携サービスから、要件に応じて収集方法を選択



利用頻度の低いデータを、安価なストレージクラスへ移動

- ・データが増えても、S3ライフサイクルを用いたアーカイブが可能
- ・アクセス頻度に応じたストレージクラスを活用し、コストを最適化

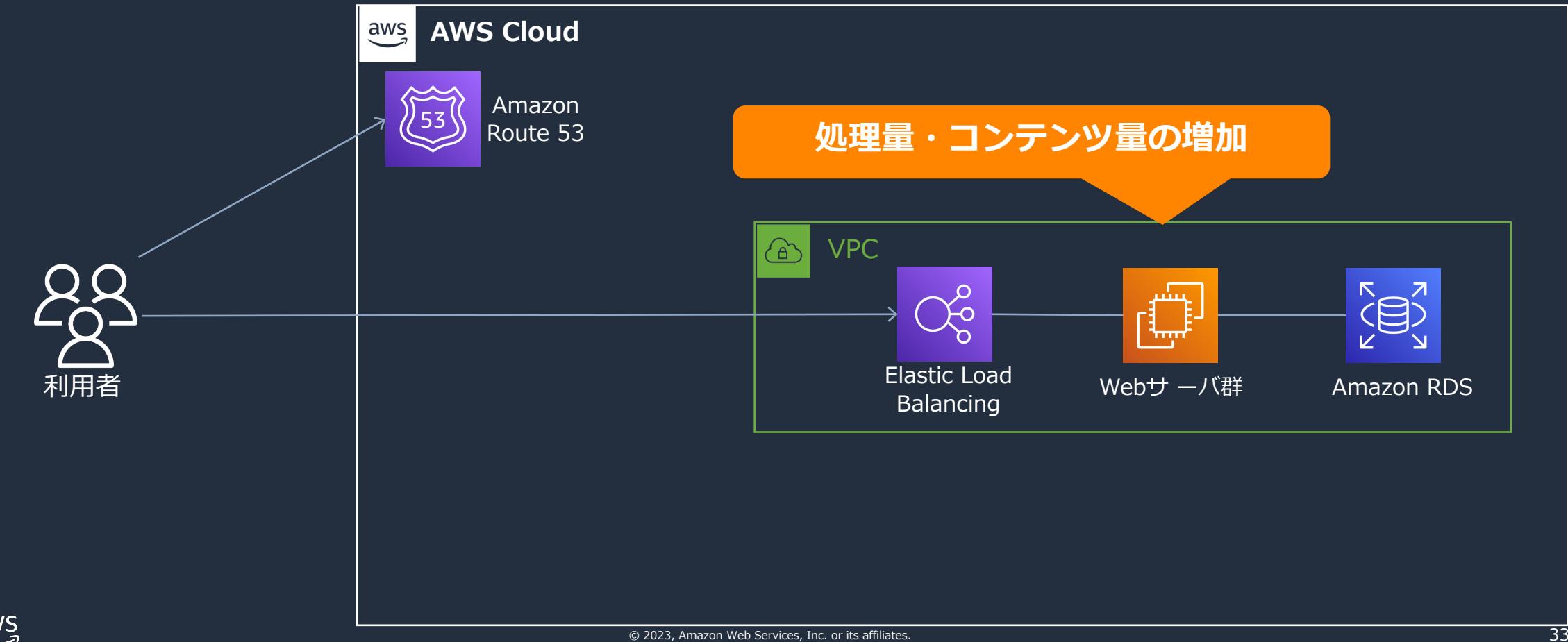


Amazon S3のユースケース

③Webサービスの コンテンツオフロード

Webサーバにおける課題

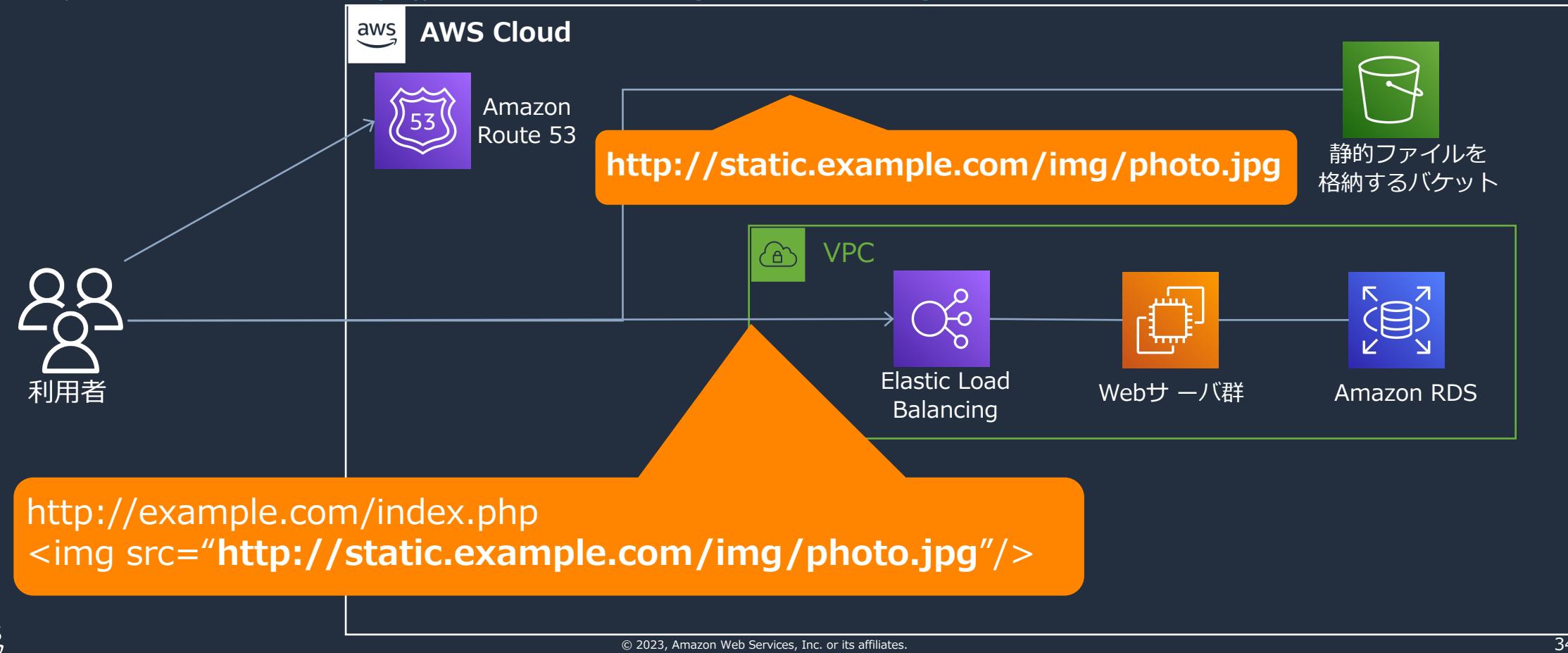
- Webサーバの処理量がビジネスの成長とともに増加してきた
 - Webへのアクセス数、Webコンテンツ量のいずれも増加している
 - Webコンテンツには、変化しない静的なデータ（画像、動画、HTML/CSSなど）が多い



静的コンテンツの処理をS3へオフロード

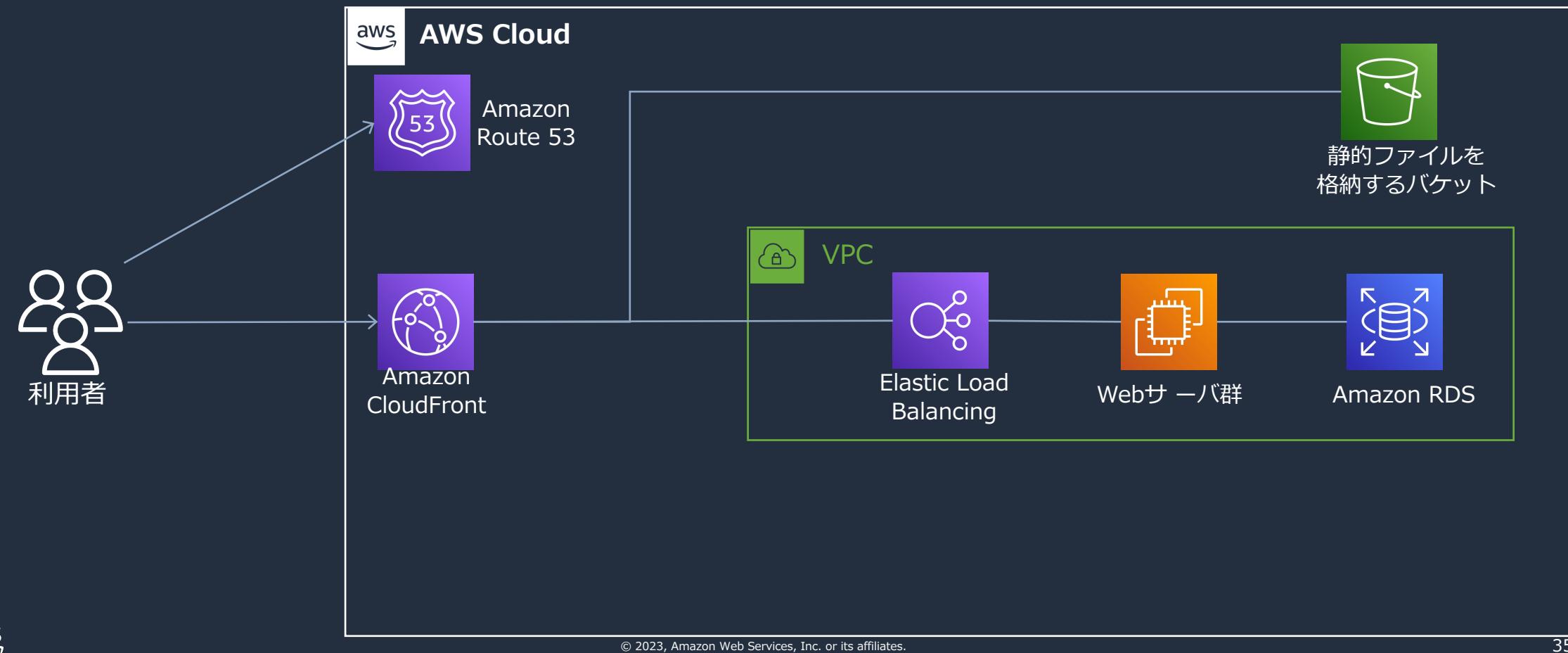
- ・ S3で静的ウェブサイトをホスティングし、バックエンドの負荷も軽減
 - S3のスケーラビリティ（容量・性能）により、負荷のスパイクへの耐性を強化
 - HTTPSは未サポート、HTTPS必要時は次ページの構成でCloudFrontを活用

https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/WebsiteHosting.html



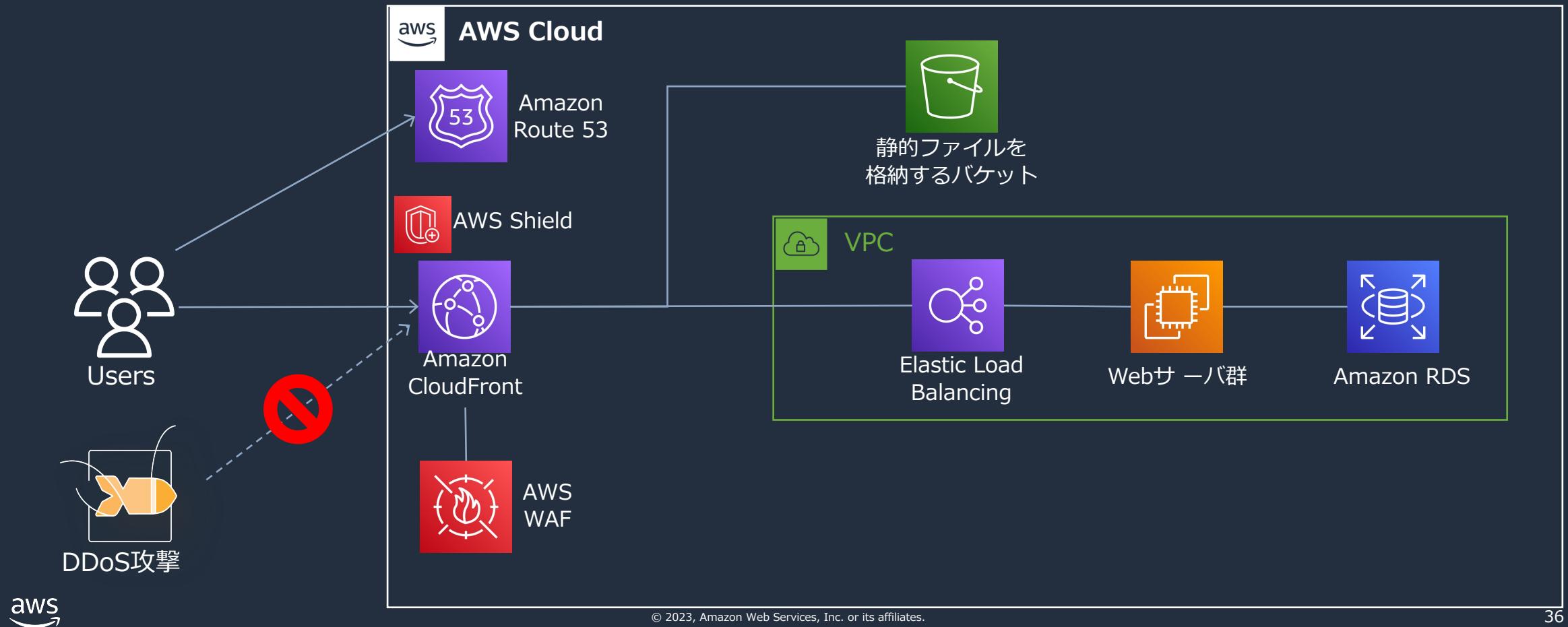
一度取得したコンテンツをCloudFrontへキャッシュ

- 同じデータの取得を抑え、バックエンドの負荷を軽減
 - CDN(Contents Delivery Network)のサービスにより、サイトの高速化、サーバの負荷軽減
 - 世界中のエッジロケーション（利用者に近い場所）からコンテンツを高速配信



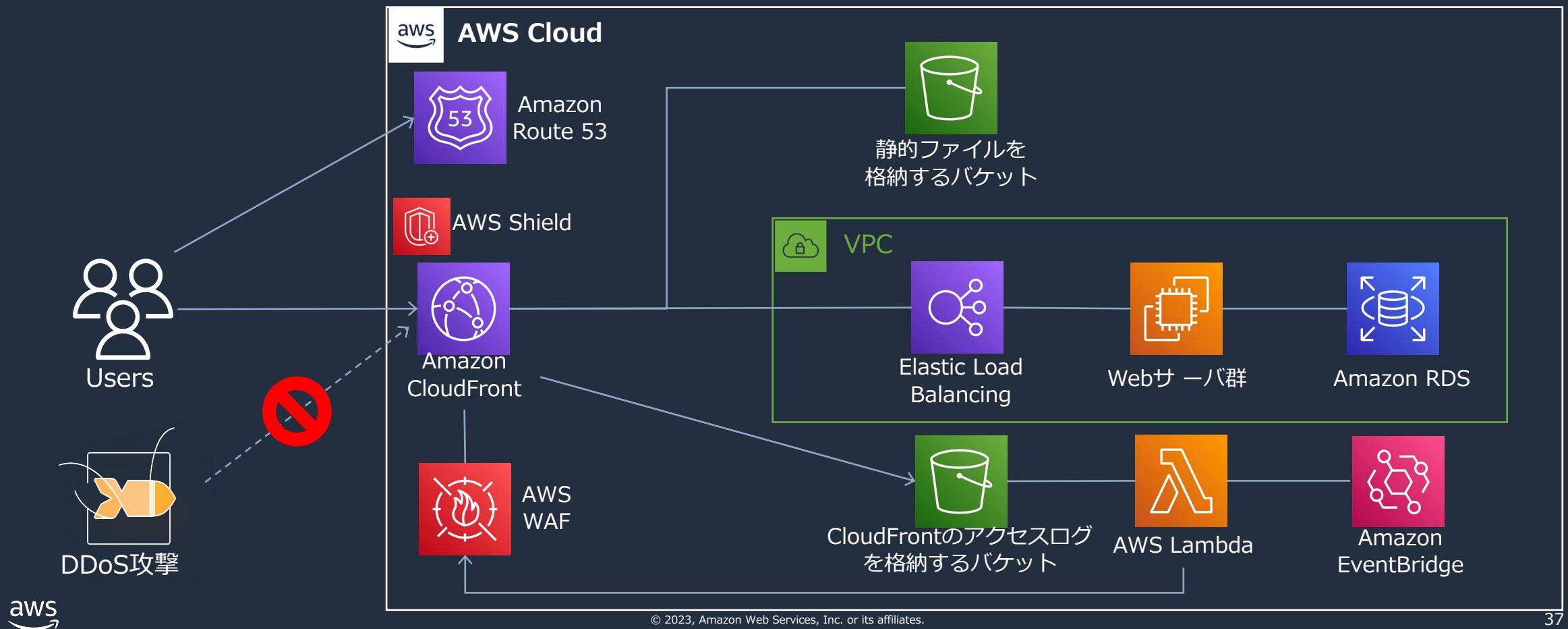
CloudFrontのセキュリティ対策を活用

- AWS Shield Standardでの保護
- AWS WAFによるアプリケーションレイヤの保護



AWS WAFのセキュリティ設定を自動化

- CloudFrontアクセスログを分析し、AWS WAFのルールへ反映
- 外部から脅威に関する情報を定期取得し、AWS WAFのルールへ反映



まとめ



まとめ

Amazon S3は高い耐久性・拡張性を誇るコスト最適なオブジェクトストレージ

＜代表的なユースケース＞

- データ保護・移行
 - 豊富な管理機能・アクセス手段を備え、AWSの多数のサービスと連携
様々なデータ保護・移行要件（オフライン／オンライン）、環境条件に対応
- データレイク
 - データをS3に保管することで、データ分析基盤を疎結合化
データ分析基盤の拡張性・柔軟性を高め、将来的なニーズに対応
- Webサービスのコンテンツオフロード
 - 静的コンテンツをS3へオフロードすることで、Webサーバの負荷を軽減
 - Amazon CloudFrontの活用により、サイトの高速化とセキュリティの向上を実現

本資料に関するお問い合わせ・ご感想

技術的な内容に関しましては、有料のAWSサポート窓口へ
お問い合わせください

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

料金面でのお問い合わせに関しましては、カスタマーサポート窓口へ
お問い合わせください（マネジメントコンソールへのログインが必要です）

<https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service>

具体的な案件に対する構成相談は、後述する個別相談会をご活用ください



ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt



その他コンテンツのご紹介

ウェビナーなど、AWSのイベントスケジュールをご参照いただけます

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

ハンズオンコンテンツ

<https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/>

AWS 個別相談会

AWSのソリューションアーキテクトと直接会話いただけます

<https://pages.awscloud.com/JAPAN-event-SP-Weekly-Sales-Consulting-Seminar-2021-reg-event.html>



Thank you!



Amazon Simple Storage Service (Amazon S3)

データ保護編

佐藤 真也

Amazon Web Service Japan G.K.

Solutions Architect

2023/04

AWS Black Belt Online Seminar とは

- ・ 「サービス別」「ソリューション別」「業種別」などのテーマに分け、
アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナー
シリーズです
- ・ AWS の技術担当者が、AWS の各サービスやソリューションについてテーマ
ごとに動画を公開します
- ・ 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も
可能、スキマ時間の学習にもお役立ていただけます
- ・ 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
- ・ <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>

内容についての注意点

- ・ 本資料では 2023 年 4 月時点のサービス内容および価格についてご説明しています。最新の情報は AWS 公式ウェブサイト(<https://aws.amazon.com/>)にてご確認ください
- ・ 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- ・ 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます

自己紹介

名前：佐藤 真也 (Sato Shinya)

所属：アマゾン ウェブ サービス ジャパン合同会社
技術統括本部 金融ソリューション本部
保険ソリューション部

好きなAWSサービス：

- AWS Snowball Edge
- Amazon Simple Storage Service (S3)
- Amazon FSx シリーズ



本セミナーの対象者

前提知識

- AWS のグローバルインフラストラクチャやフルマネージドサービスの概念
- AWS IAM、Amazon VPC などの基盤となるサービスの知識
- Amazon S3 入門編あるいは同等の知識※

対象者

- Amazon S3 でどのようにデータを保護するか気になる方

※参考リンク:

Amazon S3 入門編: <https://www.youtube.com/watch?v=wQ8ZDvoMSno>

Amazon S3 セキュリティ編: <https://www.youtube.com/watch?v=VutHE2vSvFo&t=1s>

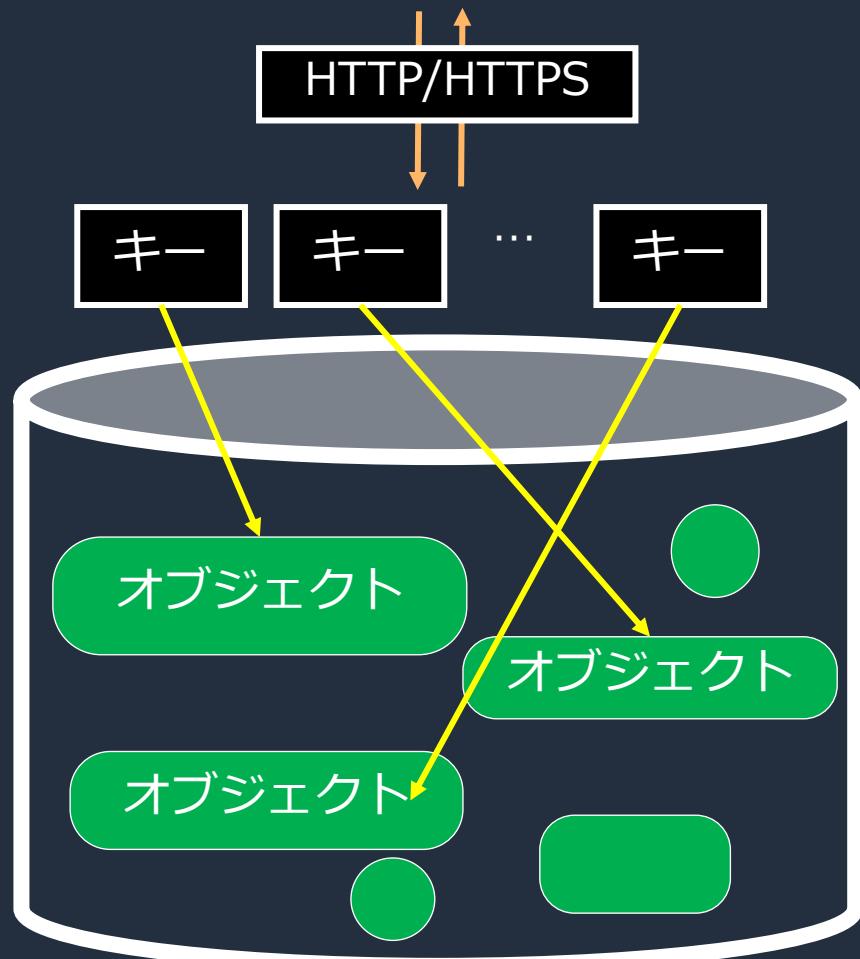
Amazon S3 ユースケース編: <https://www.youtube.com/watch?v=uuK-VaQLrzq>

アジェンダ

1. Amazon S3 の概要
2. オブジェクトのバージョニングとロック機能
3. AWS Backup の利用
4. レプリケーションによるデータ保護
5. データの整合性の検証
6. まとめ

Amazon S3 の概要

オブジェクトストレージとは



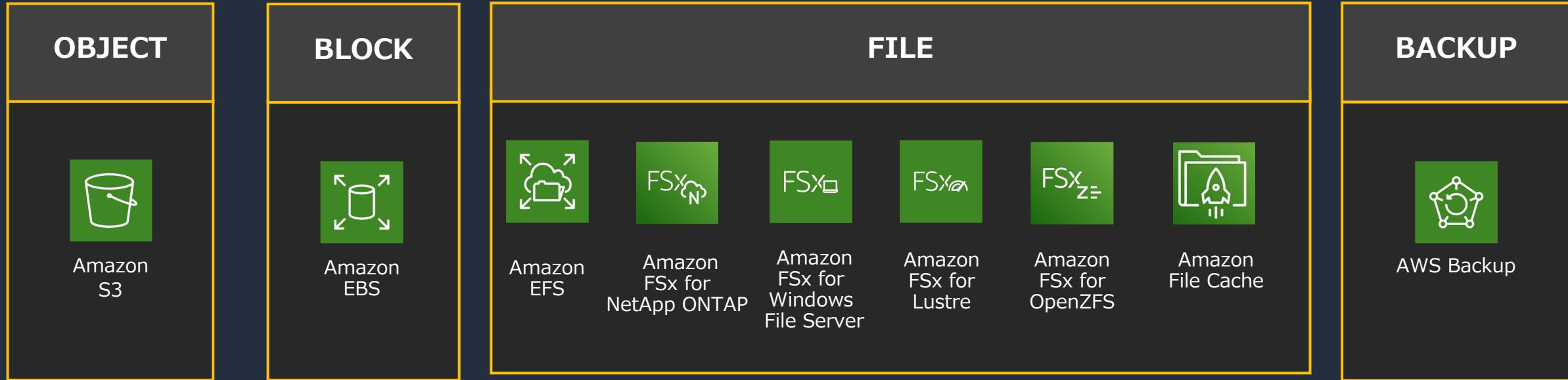
特徴

- HTTP/HTTPS でアクセス
- 一意のキーに対するオブジェクト（データ）が存在
- 階層構造を取るファイルストレージとは異なり、フラットな構造

メリット

- スケールが容易で、大容量のデータ保存が可能
- オブジェクト単位でのアクセス制御
- 高い可用性と耐障害性
- 独自にカスタマイズできるメタデータを追加可能

AWS のストレージサービス



DATA TRANSFER AND MIGRATION



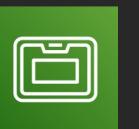
AWS Storage
Gateway



AWS DataSync



AWS Transfer
Family



AWS Snowball



AWS Snowcone

Amazon S3 とは

高いパフォーマンスと可用性、そして低コストが特徴なオブジェクトストレージ
2006 年に登場してから、現在に至るまでのイノベーションが積み重なった歴史あるサービス

- 耐久性
 - 99.99999999% (イレブンナイン)
 - 最低 3 つのアベイラビリティゾーン (AZ) で冗長化
- スケーラビリティ
 - 無制限のデータ保存
 - ただし、1 オブジェクトは最大 5 TB
- 低成本
- セキュリティ
 - アクセス制御とログ監査
- データの保護
 - 誤削除から守る機能
- アクセシビリティ
 - HTTP/HTTPS でアップロード/ダウンロード/変更/削除といった操作が可能
- 様々な AWS サービスとの連携

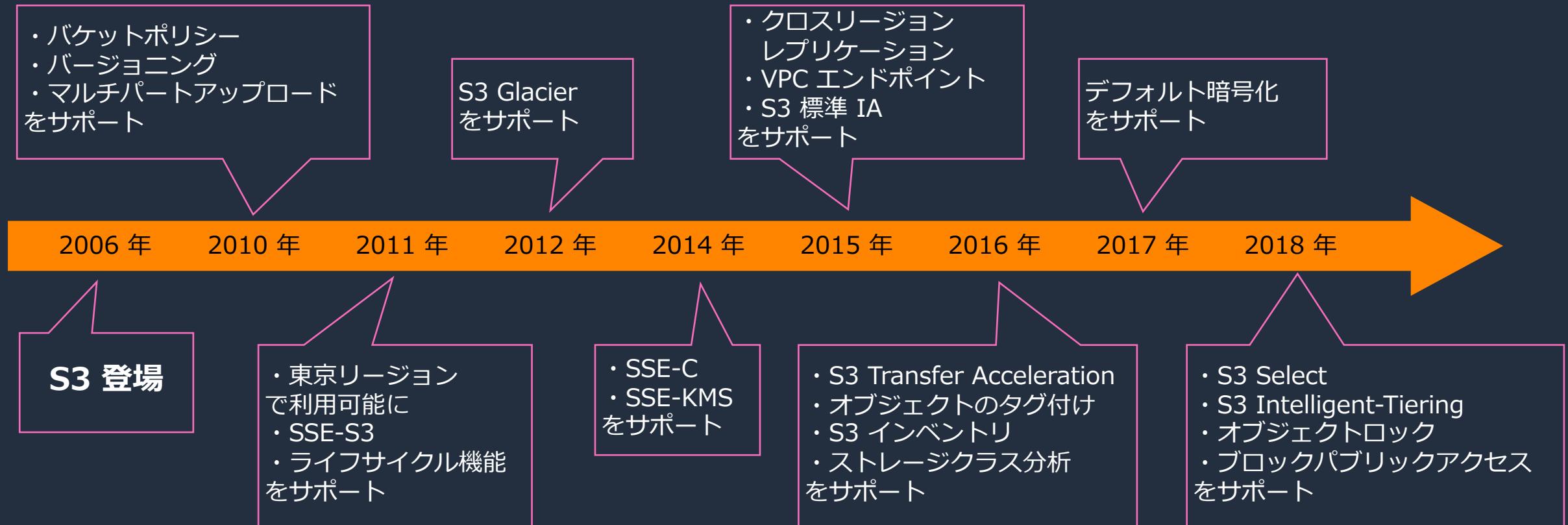


Amazon S3 の特徴などは FAQ にて詳解: <https://aws.amazon.com/jp/s3/faqs/>

Amazon S3 の 2018 年までの主要アップデート



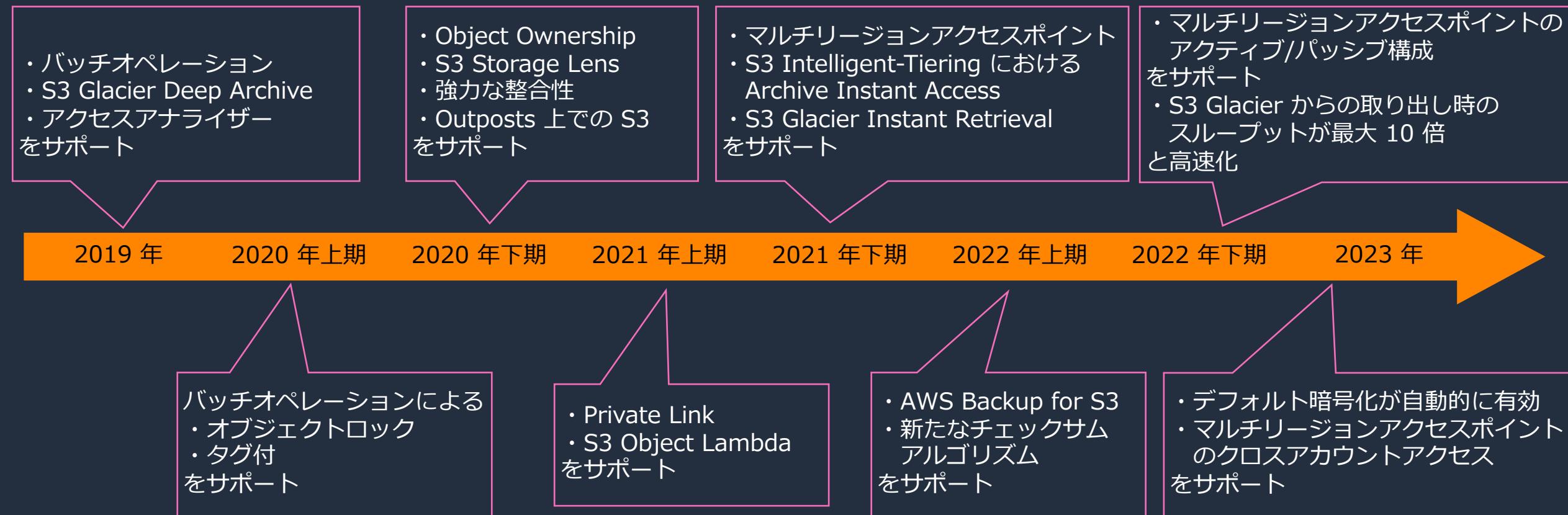
Amazon S3



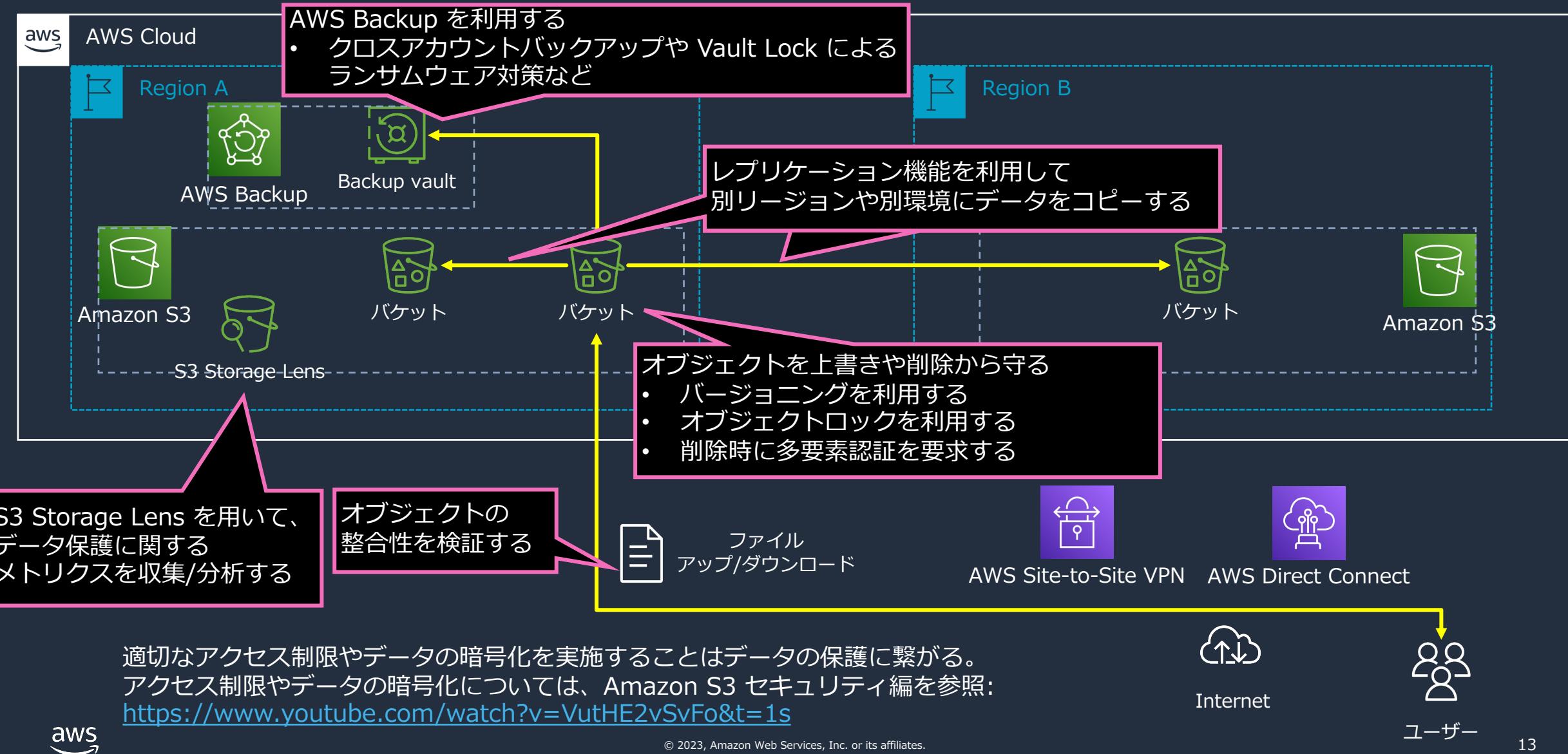
Amazon S3 の 2019 年以降の主要アップデート



Amazon S3



S3 におけるデータ保護のポイント



オブジェクトのバージョニングと ロック機能

バージョニングとは

同じバケット内部でオブジェクトの複数のバージョンを保持する方法。バケットレベルで設定し、設定以降に作成/上書きされたオブジェクトはバージョン ID が付与される※

メリット

- オブジェクトを削除/上書きした場合にも、復元ができる
 - 削除処理を行なった場合、オブジェクトが削除されるのではなく、代わりに削除マーカーが挿入される。削除マーカーが最新のオブジェクトのバージョンとなる
 - 上書きされると、上書きしたもののが最新のオブジェクトのバージョン

注意

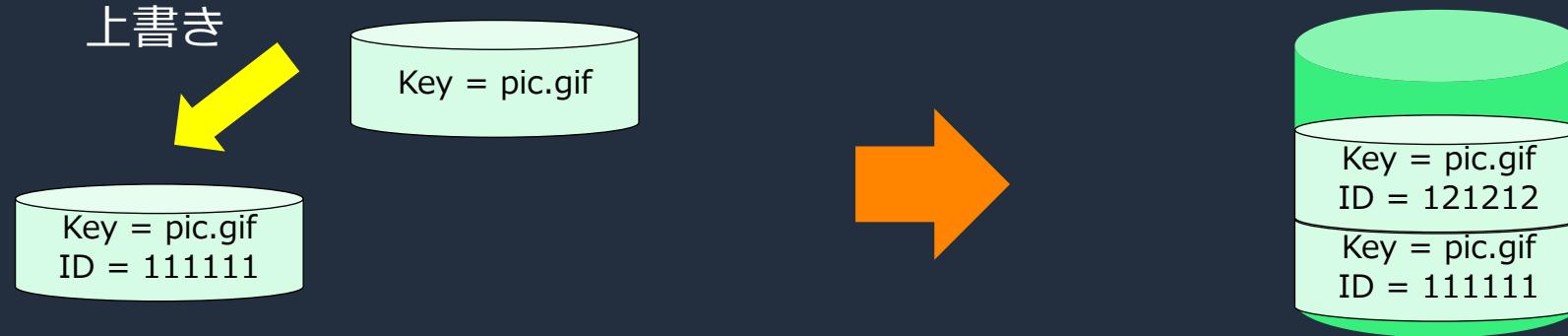
- オブジェクトのバージョン分が課金の対象となる
 - 3 つのバージョンを保持していた場合、3 つのオブジェクトに対して課金される。
 - バージョン 1/2/3 がそれぞれ 10/20/30 KB の場合、合計 60 KB 課金される。
これは各バージョンは以前のバージョンとの差分ではなく、完全なオブジェクトであるため

※バージョニング設定前に存在したオブジェクトのバージョン ID は null



バージョニングの仕組み

バージョニングを有効にすると、一意のバージョン ID を自動的に生成する



バージョニングが有効でない場合、バージョン ID は存在するが値は null となる
バージョン ID の生成は S3 のみができる、編集はできない
COPY コマンドやメタデータの編集でも新しいバージョンが作成される

COPY ※

メタデータ編集

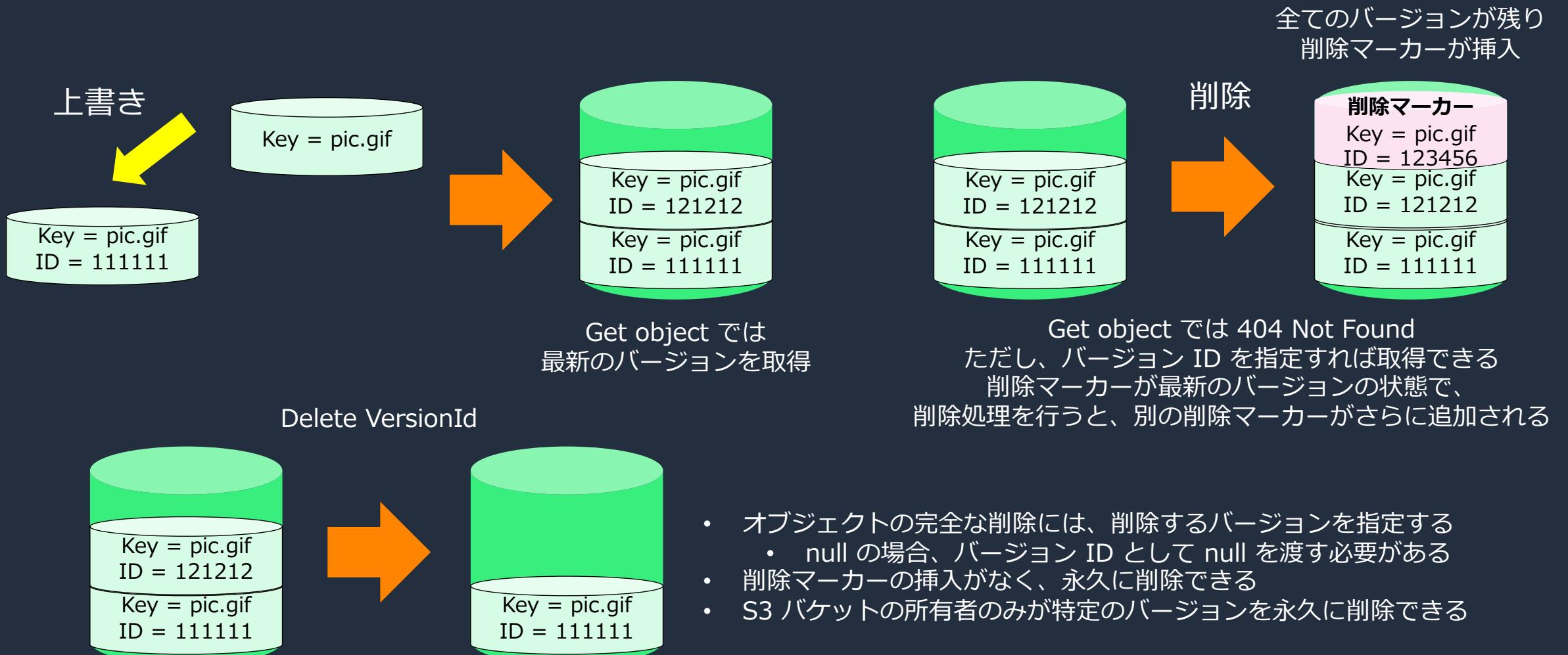
最初の version

バージョン ID	タイプ	最終更新日時	サイズ	ストレージクラス
6T8f4BqQ_dsRovpxfBZDttyQUKjFLMdZ (現行バージョン)	txt	2023/02/07 11:23:32 AM JST	0 B	スタンダード
F78el1S.J_Fyst3cetUqZ7wZPs7ZEunP	txt	2023/02/07 11:22:21 AM JST	0 B	スタンダード
yNeOus65NaKyaXmvfVXoJS7jlRf28LDG	txt	2023/02/07 11:21:48 AM JST	0 B	スタンダード

※ 同一バケット内で同一名でコピー

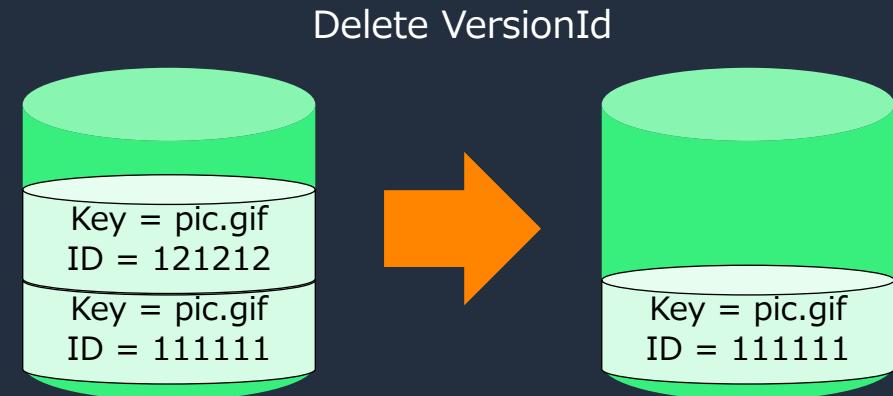
```
% aws s3 cp s3://shinya-sato-bb/dummy.txt s3://shinya-sato-bb/  
copy: s3://shinya-sato-bb/dummy.txt to s3://shinya-sato-bb/dummy.txt
```

バージョニングのワークフロー

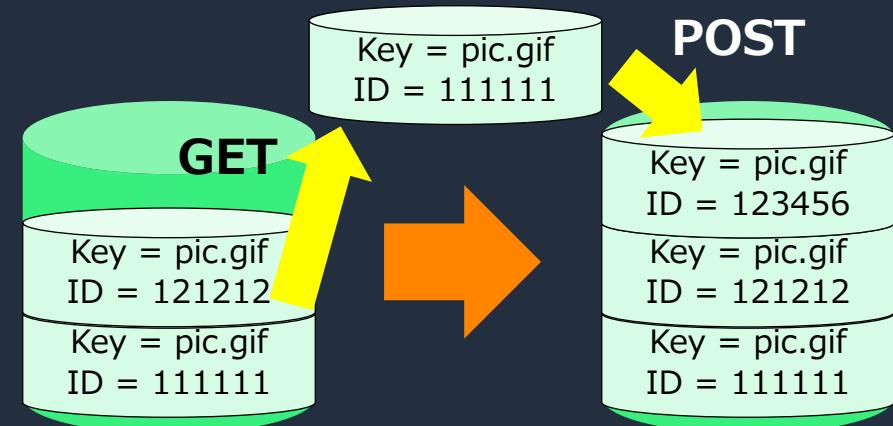


以前のバージョンの復元方法

- オブジェクトの新しいバージョンを完全に削除する
 - 以前のバージョンが最新のバージョンになる

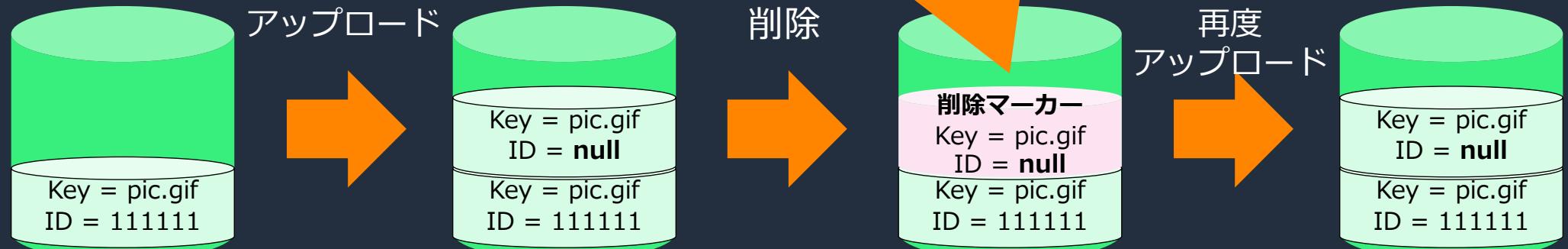


- 以前のバージョンを取得し、同じバケットにアップロードする
 - コピーされたオブジェクトが最新となり、全てのオブジェクトバージョンが保持される



バージョニングを停止した時の挙動

バージョニングを停止した後の流れ



バージョン ID は null として管理される。バージョニングを停止した後にアップロード/削除/再度アップロードしたオブジェクトは同一の null ID として管理される

アップロード

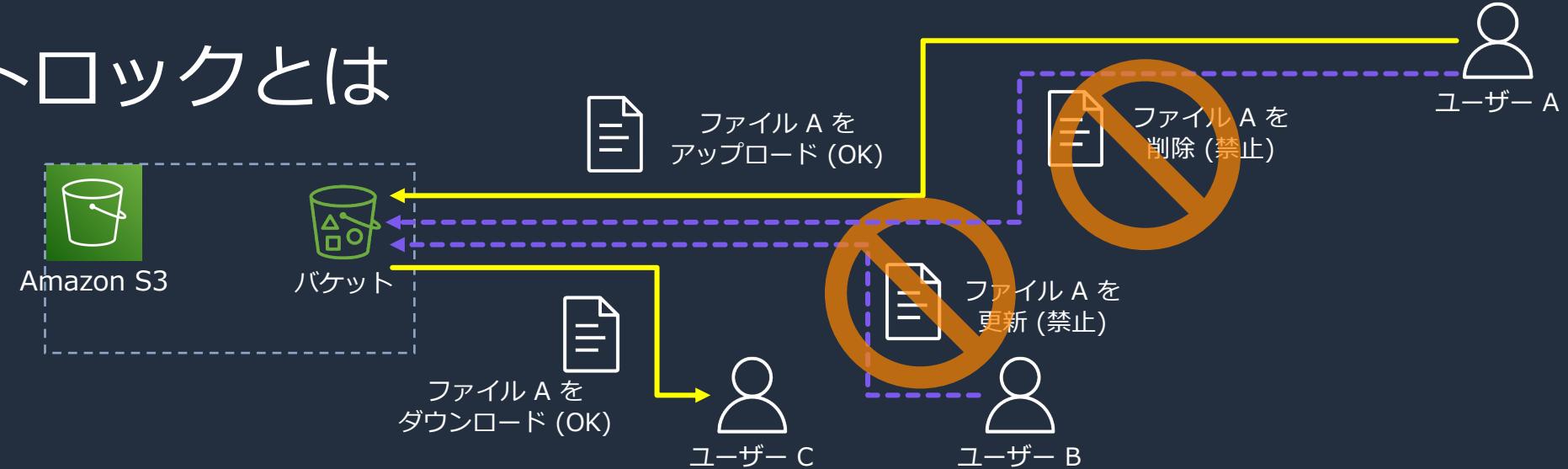
バージョン ID	タイプ
null (現行バージョン)	txt
6T8f4BqQ_dsRovpxfBZDttyQUKjFLMdZ	txt
F78eI1S.J_Fyst3cetUqZ7wZPs7ZEunP	txt
yNeOus65NaKyaXmvfVXoJS7jlRf28LDG	txt

削除し、再度アップロード

バージョン ID	タイプ
null (現行バージョン)	txt
6T8f4BqQ_dsRovpxfBZDttyQUKjFLMdZ	txt
F78eI1S.J_Fyst3cetUqZ7wZPs7ZEunP	txt
yNeOus65NaKyaXmvfVXoJS7jlRf28LDG	txt



オブジェクトロックとは



オブジェクトロックはバージョニングされたバケットのみに適用できる Write Once Read Many (WORM) 機能で、削除/上書きを一定期間/無期限に防止できる※

※変更/削除処理を反映するよう見えるが、実際にはバージョニングにより保存されている

2つのリテンションモードがある

- ガバナンスモード
 - s3:BypassGovernanceRetention の権限を持ち、かつ、x-amz-bypass-governance-retention:true のヘッダーを含む場合を除き、上書き/削除/設定の変更ができない
 - 特定権限があれば、削除/設定変更ができるため、コンプライアンスモードのテストとしても利用できる
- コンプライアンスモード
 - いかなるユーザーも上書き/削除/設定の変更を行うことができない

保持期間とリーガルホールド

保持期間

- ・個々のオブジェクトバージョンに対して適用される
- ・この期間、ガバナンス/コンプライアンスマードが適用され、オブジェクトを上書き/削除できない
- ・保持期間の終了後、リーガルホールドを適用しない限り、オブジェクトを上書き/削除できる

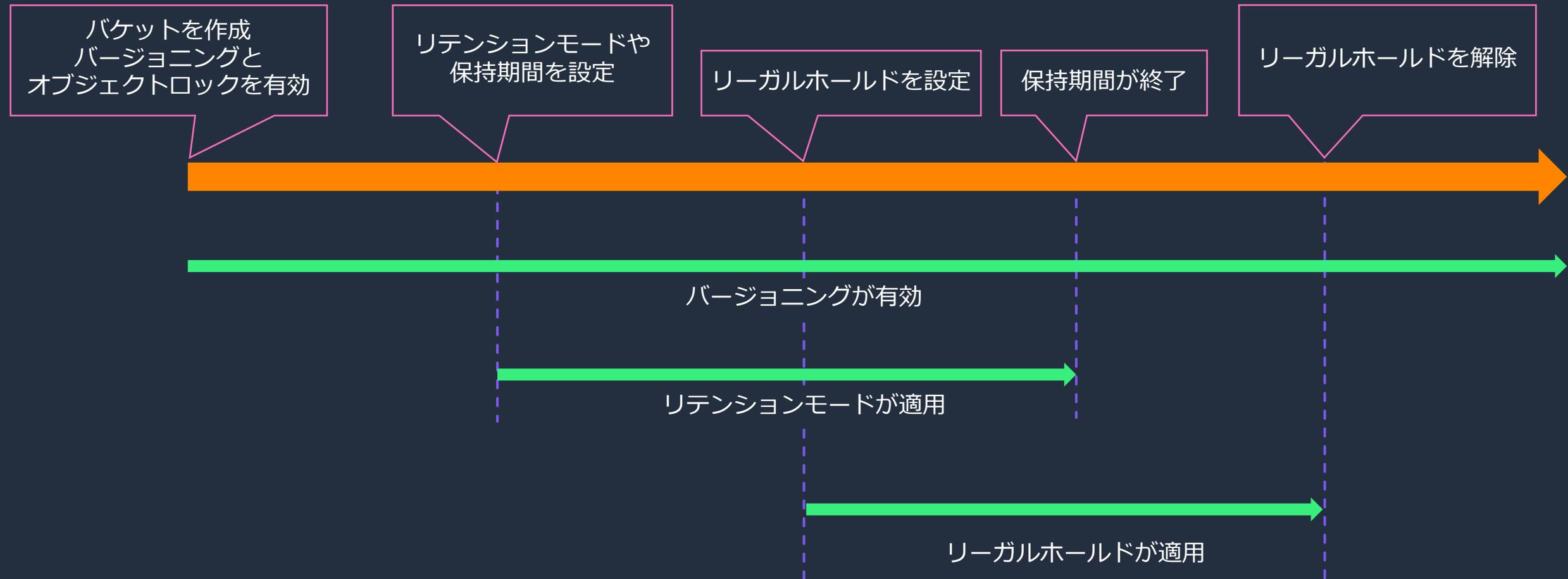
リーガルホールド

- ・オブジェクトの上書きと/削除を防止する
- ・保持期間とは独立に設定され有効期間はない。s3:PutObjectLegalHold 許可を持つ任意のユーザーが自由に適用/解除できる
- ・オブジェクトロックが有効になっているバケットに対して設定ができるが、リテンションモードや保持期間とは独立に設定される
- ・保持期間中はリテンションモードが適用され、保持期間後はリーガルホールドが適用される

保持期間とリーガルホールドの関係

	リーガルホールドを適用する	リーガルホールドを適用しない
保持期間終了前	<ul style="list-style-type: none">ガバナンス/コンプライアンスマードが適用されるs3:PutObjectLegalHold 許可を持つ任意のユーザーは自由にリーガルホールドを設定できる	
保持期間終了後	s3:PutObjectLegalHold 許可を持つ任意のユーザーが自由に解除するまで WORM 機能が引き続き適用される	自由にオブジェクトを操作できる

有効になるデータ保護機能



オブジェクトロックでの挙動: 削除処理

オブジェクトロックを有効にした状態でテスト

オブジェクトをアップロード

	バージョン ID	タイプ	最終更新日時
□	NTDMXt21RE3vxRd96UX9FQsVWat4PaNj (現行バージョン)	txt	2023/02/07 11:38:49 AM JST

オブジェクトを削除すると、マネジメントコンソールからはオブジェクトが非表示になり、削除処理が反映されているように見える。しかし、再度アップロードして確認すると、削除処理時には削除マークーが追加され、実際には以前のバージョンは保持されていることが確認できる

	バージョン ID	タイプ	最終更新日時
□	5qMRCgFW47NPsdB1SLTllyMSr5W34m8 (現行バージョン)	txt	2023/02/07 11:41:05 AM JST
□	OkYaye1PNpXHmo6YgKAcVBPrzrVI5RXZP	削除マークー	2023/02/07 11:40:51 AM JST
□	NTDMXt21RE3vxRd96UX9FQsVWat4PaNj	txt	2023/02/07 11:38:49 AM JST

バージョンを指定して削除（完全削除）はできない

⊗ 削除に失敗しました (1 オブジェクト, 0 B)

名前	フォルダ	バージョン ID	タイプ	最終更新日時	サイズ	エラー
dummy.txt	-	5qMRCgFW47NPsdB1SLTllyMSr5W34m8	txt	2023/02/07 11:41:05 AM JST	0 B	⊗ アクセスが拒否されました

オブジェクトロックでの挙動: リーガルホールドの変更

オブジェクトロックのリーガルホールド

ホールドが明示的に削除されるまで、オブジェクトの削除または上書きが実行されないようにします。リーガルホールドは、特定の IAM アクセス許可を持つ AWS アカウントで有効または無効にすることができます。[詳細](#)

リーガルホールド

無効にする
 有効にする

指定されたオブジェクト

名前	バージョン ID	タイプ	最終更新日時	サイズ
dummy.txt	-	txt	2023/02/07 11:41:05 AM JST	0 B

キャンセル **変更の保存**



オブジェクトロックのリーガルホールド

ホールドが明示的に削除されるまで、オブジェクトの削除または上書きが実行されないようにします。リーガルホールドは、特定の IAM アクセス許可を持つ AWS アカウントで有効または無効にすることができます。[詳細](#)

リーガルホールド

有効

リーガルホールドの変更は反映される

オブジェクトロックのリーガルホールド

ホールドが明示的に削除されるまで、オブジェクトの削除または上書きが実行されないようにします。リーガルホールドは、特定の IAM アクセス許可を持つ AWS アカウントで有効または無効にすることができます。[詳細](#)

リーガルホールド

無効にする
 有効にする

指定されたオブジェクト

名前	バージョン ID	タイプ	最終更新日時	サイズ
dummy.txt	-	txt	2023/02/07 11:41:05 AM JST	0 B

キャンセル **変更の保存**



リーガルホールド
無効

リーガルホールドの設定は
リテンションモードや保持期間とは独立
に適用することや設定変更できる



オブジェクトロックの注意点

- オブジェクトロックはバケット作成時に設定し、作成後の有効化/無効化はできない
- バケット作成後に、保持期間の有効化/無効化/変更やリテンションモードの変更はできる
これらの設定は個々のオブジェクトに適用される
 - 保持期間やリテンションモードを変更した場合には、既存のオブジェクトは従来の設定に従う一方で、新規のオブジェクトには変更後の設定が反映される
- オブジェクトロックの有効にはバケットのバージョニングが必須
 - バージョニングはオブジェクトロックが有効になっているバケットでは無効化できない
- AWS KMS キーでサーバーサイド暗号化を行う場合には、キーの保護も検討する
 - キーを破棄することで、オブジェクトは保持され続けるものの復号できなくなる
(自動キーローテーションのように暗号化マテリアルを保存する必要がある)

オブジェクトロックのユースケース

- オブジェクト単位で一定期間、上書き/削除を防止する
 - 監査やコンプライアンス目的
 - ランサムウェア対策
- リーガルホールドを適用することで、保持期間の終了後も解除するまで無制限で「監査やコンプライアンス目的」/「ランサムウェア対策」のため、オブジェクトを上書き/削除から保護する

AWS Backup の利用

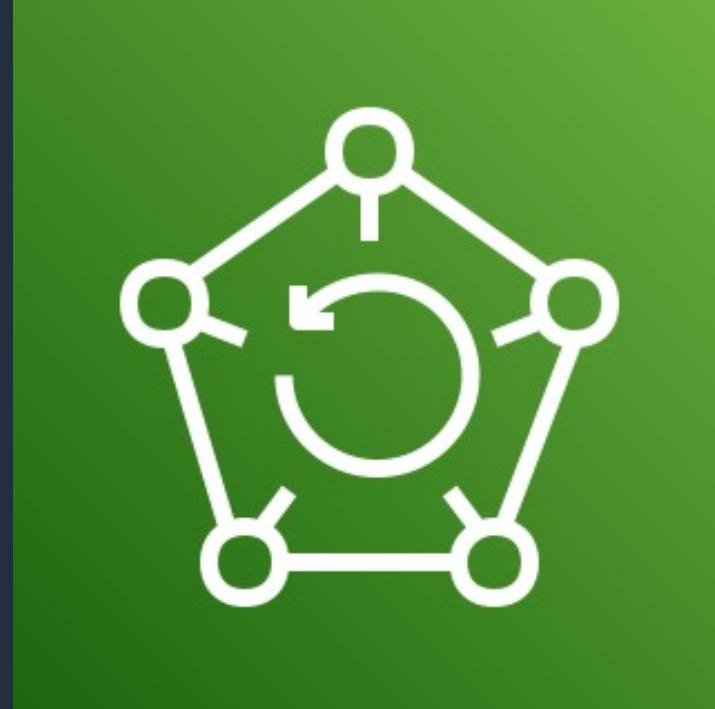
AWS Backup とは

AWS の各サービスのバックアップの実行と
バックアップデータの一元的な管理を提供

集中型の管理

バックアップの自動化

コンプライアンス



AWS Backup



「バックアッププラン」、
「バックアップルール」、
「Backup Vault」を定義



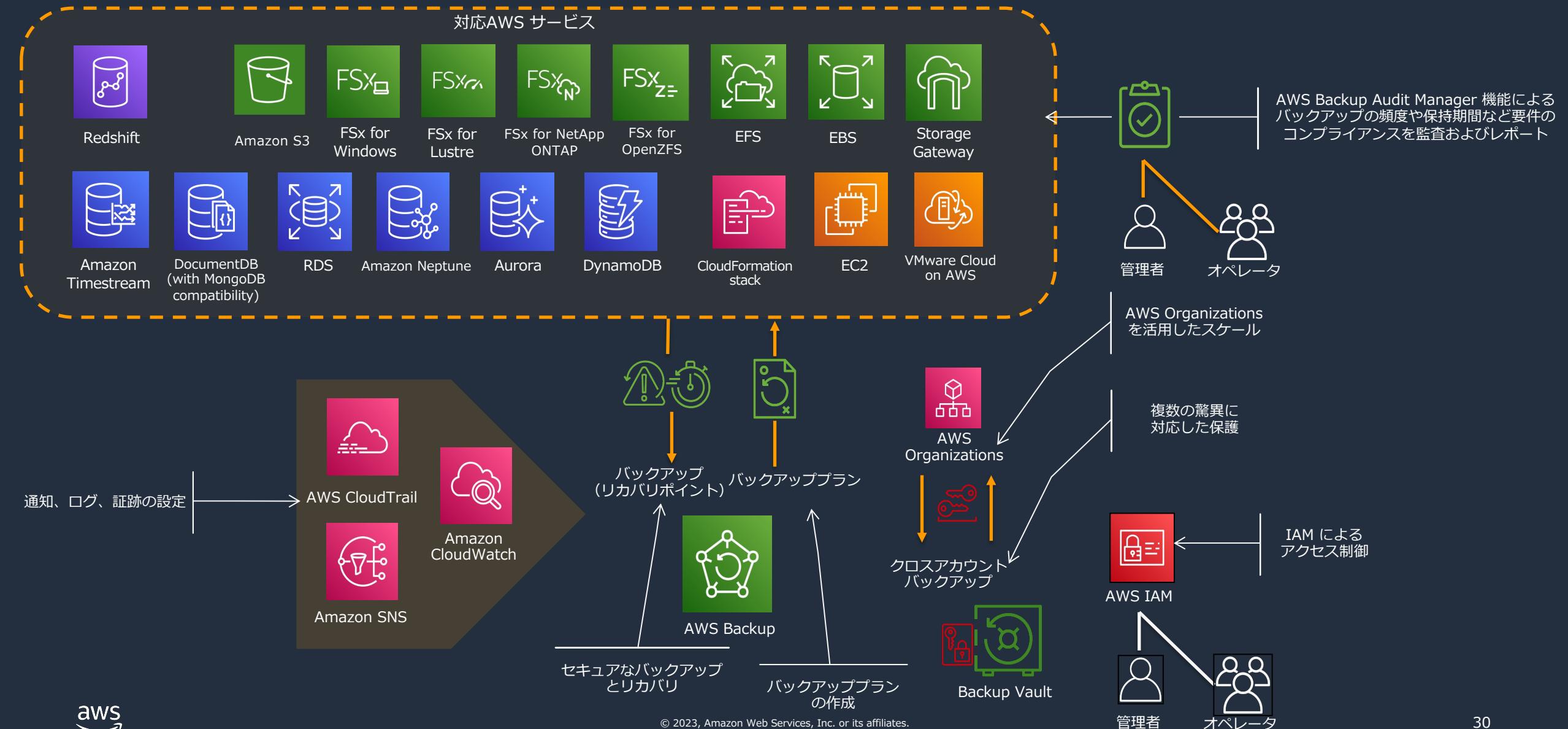
- 「バックアップスケジュール」を定義
- CloudTrail や SNS と連携



- IAM でアクセス権限を管理
- 複数のコンプライアンス標準に準拠 (PCI-DSS 含む)

- クラウドネイティブなバックアップと AWS Storage Gateway を統合したハイブリッドなバックアップを提供
- ポリシーベースおよびタグベースのバックアップ
- 自動化されたバックアップスケジューリング
- バックアップの暗号化
- クロスアカウント、クロスリージョンのバックアップ
- 自動バックアップリテンション管理

AWS Backup 全体像



AWS Backup for S3: バケットの保護

AWS Backup を利用して、S3 バケットをバケット単位で Vault へとバックアップできる

1. リソース選択を定義 [情報](#)
すべてのリソースを保護するか、タイプまたは ID でリソースを指定します。

すべてのリソースタイプを含める
アカウントで有効になっているすべてのリソースタイプを保護します。

特定のリソースタイプを含める
タイプ別にリソースを選択するか、ID で個別のリソースを指定します。

2. 特定のリソースタイプを選択 [情報](#)
このバックアップ計画で保護する特定のリソースタイプを選択します。特定のリソース ID を選択から除外することもできます。

リソースタイプを選択 ▾

リソースタイプ バケット名

S3 リソースを選択 削除

S3 バケットでバージョニングを有効にする必要があります。詳細は [こちら](#)

すべてのバケット X

特定のバケットのみ選択できる



特定のバケットのみ対象外とする

3. 選択したリソースタイプから特定のリソース ID を除外する - オプション [情報](#)
この割り当てから除外する特定のリソース ID を選択します。

リソースタイプを選択 ▾

4. タグを使用して選択を絞り込む - オプション [情報](#)
タグでリソースをフィルタリングします。タグが複数ある場合、リソースはすべてのタグ条件を満たす場合にのみバックアッププランに割り当てられます。

キー	値の条件	値
Q キーを入力	条件を選択 ▾	Q 値を入力 削除

タグでの絞り込み



AWS Backup for S3: バケットのリストア

AWS Backup を利用して、S3 バケットをバケット単位/オブジェクト単位でリストアできる

The screenshot shows the AWS Backup console interface. At the top, there's a search bar labeled "復旧ポイント ID でフィルタリング". Below it is a table with columns: "復旧ポイント ID", "ステータス", and "バックアップタイプ". A single row is selected, showing "s3-bb-shinyasato-[REDACTED]" in the ID column, "完了しました" (Completed) in the status column, and "バックアップ" (Backup) in the type column. An orange callout box highlights this row with the text: "バケット全体またはオブジェクト/フォルダ単位でのリストアができる". At the bottom of the table, another orange callout box highlights the "バージョニング" (Versioning) link with the text: "同じリージョンでバージョニングが有効になっている既存のバケットへのリストアができる".

The screenshot shows the "設定" (Settings) screen for a restore operation. It includes sections for "リストアタイプ" (Restore Type), "復元先" (Restore Target), "オブジェクト暗号化の復元" (Object Encryption Decryption), and "AWS KMS 密钥" (AWS KMS Key). The "リストアタイプ" section has two options: "バケット全体を復元する" (Restore the entire bucket) and "アイテムレベルの復元" (Restore at the item level). The "復元先" section has three options: "ソースバケットに復元する" (Restore to the source bucket), "既存のバケットを使用" (Use existing bucket), and "新しいバケットを作成する" (Create new bucket). The "オブジェクト暗号化の復元" section has two options: "元の暗号化キーを使用 (デフォルト)" (Use original encryption key (Default)) and "S3アマゾンキー (SSE-S3)" (S3 Amazon Key (SSE-S3)). The "AWS KMS 密钥" section lists "AWS KMS 密钥" (AWS KMS Key) and "AWS Lambda 密钥" (AWS Lambda Key). An orange callout box highlights the "バケット全体を復元する" option with the text: "バケット全体またはオブジェクト/フォルダ単位でのリストアができる".

AWS Backup for S3: 特徴と注意点

- ・ バックアップの対象となるバケットはバージョニングを有効化する必要がある
- ・ オブジェクト単位での増分（インクリメンタル）バックアップ
 - ・ 1 GB のオブジェクトのうち、1 KB 分だけ変更された場合にも、1 GB の新しいバックアップが作成される
- ・ 定期的なバックアップとポイントインタイムリカバリ用の継続的なバックアップが選択できる
- ・ クロスリージョン/アカウントバックアップが利用できる
 - ・ ポイントインタイムリカバリと併用はできない

その他参考情報: https://docs.aws.amazon.com/ja_jp/aws-backup/latest/devguide/s3-backups.html



AWS Backup Vault Lock

- S3 のオブジェクトロック同様に、ガバナンスモードとコンプライアンスマードが設定できる
 - コンプライアンスマードでは適用開始までの猶予期間を設定できる
- S3 同様にリーガルホールドを設定できる
- Vault 単位で設定することができ、復旧ポイントが削除されることを防止する
- 最小保持期間と最大保持期間
 - 範囲内の保持期間となる復旧ポイントを保護する
 - 例、最小保持期間が 2 日で、最大保持期間が 2 週間の場合、保持期間が 2 日から 2 週間の復旧ポイントのみ保護される

The screenshot shows the 'Vault Lock Mode' configuration page. It includes sections for 'Mode' (Governance Mode or Compliance Mode selected), 'Retention Period' (Minimum and Maximum), and 'Start Date' (Set to March 30, 2023). A note at the bottom explains the impact on existing backups and new copy jobs.

ボールトロックモード 情報

ガバナンスマード
ロックは、特定の IAM 許可を持つユーザーが管理または削除できます。

コンプライアンスマード
ロックは、ルートユーザー(アカウント所有者)や AWS を含め、いかなるユーザーも管理または削除できません。

保持期間 情報
ボールトロックは、最小保持期間と最大保持期間内のバックアップの保護に役立ちます。

最小保持期間 - オプション 情報
保持期間が入力した値以上であるバックアップは保護されます。デフォルトは 1 日です。

1 日数 ▾

最大保持期間 - オプション 情報
保持期間が入力した値以下であるバックアップは保護されます。

最大保持期間を入力 日数 ▾

① ボールト内の既存のバックアップ、およびボールトに追加された新しいバックアップまたはコピージョブはすべて保護されます。このボールトを管理または削除できるのは、特定の IAM 許可を持つユーザーのみです。 詳細 はこちる

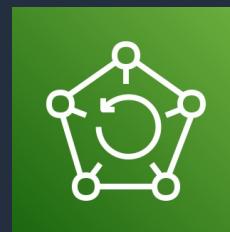
コンプライアンスマードの開始日 情報
ボールトが永続的にロックされる日付を指定します。それまでは、設定を編集または削除できます。最小猶予期間は 3 日 (72 時間) です。

2023/03/30

① ボールトは 2023年3月30日, 17:19 (UTC+09:00) にイミュータブルになります。ボールトがイミュータブルになる前に、ボールトロックを管理または削除するために 3 日 の猶予期間が設けられています。この間、特定の IAM 許可を持つユーザーのみが変更できます。

AWS Backup for S3: ユースケース

- S3 バケット/フォルダ単位でバックアップ/リストアできる
 - 復旧地点を選択することで、素早くリストアできる
- Vault 単位で、WORM 機能を利用できる
 - ランサムウェアなどの脅威への対策
 - コンプライアンス要件を満たす



Vault 単位で、WORM 機能が利用できる



オブジェクト 単位で、WORM 機能が利用できる

- 単一のバックアップポリシーを使用して、S3 を含めたサービスのバックアップを一元的に管理できる
- AWS Backup Audit Manager により、バックアップ頻度や保持期間などの要件を監査できる

レプリケーションによる データ保護

オブジェクトのレプリケーション 1

- S3 バケット間でオブジェクトを非同期にコピーできる
 - レプリケーションを設定した後に追加、変更、削除されたオブジェクトがレプリケーションされる
 - 非同期コピーであるため、即座にレプリケートされるわけではない
 - オブジェクトの作成時刻やバージョン ID などの全てのメタデータを保持しながらレプリケートする
- ソースバケットとターゲットバケットは、アカウント/リージョンは同じ/異なる場合でも利用できる
 - つまり、クロスアカウント/クロスリージョンレプリケーションができる

必要な準備

- ソースとターゲットバケットは共にバージョニングを有効化する
- レプリケーションルールには適切な権限を付与する
 - SSE-KMS の場合には、レプリケーションルールにアタッチするロールには、ソース/ターゲットで使用するキーへのアクセスを許可する。また、キーポリシーを確認し、レプリケーションルールにアタッチするロールへのアクセス許可を確認する
- クロスアカウントレプリケーションの場合、ターゲットバケットのバケットポリシーで、ソースバケットの所有者にアクセス許可を与える



オブジェクトのレプリケーション 2

レプリケーションのオプションを追加で設定することや、ターゲットバケットは別のストレージクラスを選択できる

追加のレプリケーションオプション

99.99% のオブジェクトを 15 分以内
のレプリケーションすることも
オプションで設定できる※

レプリケーション時間のコントロール (RTC)

レプリケーション時間の制御により、新しいオブジェクトの 99.99% が 15 分以内にレプリケートされ、レプリケーションのメトリクスと通知が提供されます。追加料金が適用されます。[詳細はこちら](#)

レプリケーションメトリクスと通知

Cloudwatch メトリクスを使用してレプリケーションルールの進行状況をモニタリングします。Cloudwatch メトリクスの料金が適用されます。[詳細](#)、または [Amazon Cloudwatch の料金](#) を参照してください。

削除マーカーのレプリケーション

S3 削除オペレーションによって作成された削除マーカーはレプリケートされます。ライフサイクルルールによって作成された削除マークーはレプリケートされません。[詳細](#)

レプリカ変更の同期

このバケットのレプリカに行われたメタデータの変更をレプリケート先バケットにレプリケートします。[詳細はこちら](#)

※レプリケーションデータの転送速度が 1 Gbps を超えた期間には適用されない。



別のストレージクラスを選択できる

ストレージクラス	用に設計	アベイラビリティーゾーン
スタンダード	ミリ秒単位のアクセスが可能で、アクセス頻度の高いデータ (1か月に 1 回以上)	≥ 3
Intelligent-Tiering	アクセスパターンが変化したり不明であるデータ	≥ 3
標準 - IA	ミリ秒単位のアクセスが可能で、アクセス頻度の低いデータ (1か月に 1 回)	≥ 3
1 ゾーン - IA	1 つのアベイラビリティーゾーンに保存され、ミリ秒単位のアクセスが可能な再利用可能なアクセス頻度の低いデータ (1 か月に 1 回)	1
Glacier Instant Retrieval	ミリ秒単位で瞬時に取得可能で、アクセスが四半期に一度の存続期間が長いアーカイブデータ	≥ 3
Glacier Flexible Retrieval (旧 Glacier)	取得時間が数分から数時間で、アクセスが 1 年に一度の存続期間が長いアーカイブデータ	≥ 3
Glacier Deep Archive	取得時間が数時間で、アクセスが 1 年に 1 回未満の存続期間が長いアーカイブデータ	≥ 3
低冗長化	非クリティカルでアクセス頻度の高い、ミリ秒単位のアクセスが可能なデータ (S3 標準はコスト効率が高いため、推奨されません)	≥ 3

バッチレプリケーションとは

- レプリケーションの設定を行われる前に存在するオブジェクト、以前にレプリケートされたオブジェクト、レプリケーションに失敗したオブジェクトをレプリケートできる
 - 新しいレプリケーションルールを設定して実行する
 - 既存のレプリケーションルールを用いて実行する
- フィルターを用いて、オブジェクトの作成日などを指定しレプリケートする対象を制限できる
- 注意点
 - ソースバケットにオブジェクトと削除マークの複数のバージョンがあるとき、削除マークを先にレプリケートする可能性がある。ライフサイクルポリシーによっては、削除マークが期限切れとしてマークされた時点で、**レプリケート前にターゲットバケットからオブジェクトが削除される**
 - ターゲットバケットからバージョン ID を指定して削除されたオブジェクトは再度レプリケーションできない

フィルター

フィルタを指定して、レプリケートされるオブジェクトの範囲を減らすことができます。これらのフィルタは、レプリケーション設定の既存のフィルタと連動して機能します。フィルタを指定しない場合、レプリケーション設定で定義されているすべてのオブジェクトがレプリケートされます。

オブジェクト作成開始日 - オプション オブジェクト作成の開始時刻
YYYY/MM/DD hh:mm:ss (UTC+09:00)
形式: YYYY/MM/DD

オブジェクト作成終了日 - オプション オブジェクト作成の終了時刻
YYYY/MM/DD hh:mm:ss (UTC+09:00)
形式: YYYY/MM/DD

レプリケーションステータス - オプション
レプリケーションステータスの選択します

完了済み
 ソースオブジェクトは正常にレプリケーションを完了しました。

レプリカ
 レプリケートされたオブジェクト。

失敗
 ソースオブジェクトがレプリケーションに失敗しました。

なし
 ソースオブジェクトがレプリケートされたことがありません。

レプリケーションステータスの選択します



レプリケーションの考慮事項 1

- ターゲットバケットへレプリケートされないオブジェクト
 - 別のソースバケットからレプリケートされたオブジェクト
 - S3 Glacier Flexible Retrieval/S3 Glacier Deep Archive に保存されているオブジェクト

多段レプリケーションはできない



複数のバケットへレプリケートする



レプリケーションの考慮事項 2

- デフォルト設定では削除マークはレプリケートされない。特にソース/ターゲットバケットのライフサイクル設定が異なる場合には注意する。たとえば、ソースバケットでは削除マークが挿入されている一方で、ターゲットバケットでは、削除マークが挿入されずバケット間に差異が生じる可能性がある。
- Object Ownership を有効化する。
 - 有効にしている場合、デフォルトではレプリケート元のオブジェクトの所有者もレプリカの所有者になる
- レプリケーションが完了しオブジェクトが利用可能になるまでの時間は、サイズにより異なる
 - ライフサイクルルールは、ターゲットバケットで利用可能になった時間ではなく、作成時間が適用される

レプリケーションのユースケース

- クロスリージョンレプリケーション
 - 遠く離れた地域にデータをレプリケートすることで、コンプライアンス要件を満たす
 - Disaster Recovery
 - エンドユーザーが地理的に分散している時、レイテンシを小さくすることができる
- クロスアカウントレプリケーション
 - ログを 1 つのバケットに集約することができる
 - 本番/分析/テスト環境などといった環境をまたがり、データだけをレプリケートすることができる

データの整合性の検証

チェックサムの利用

チェックサムは、デジタルフィンガープリントの一種（コンテンツの一意性を確認するための値）
チェックサムを利用することで、アップロード/ダウンロードするデータの整合性を検証できる

押さえておくべき用語

- MD5
- ETag
- 追加のチェックサム

MD5 を利用したデータの整合性の検証 1

1. MD5 のダイジェスト（ハッシュ）値を計算する
2. Content-MD5 ヘッダーとして、アップロード時に MD5 ダイジェスト値を引き渡す
3. アップロードされたオブジェクトの整合性を S3 が確認する

ファイルの MD5 ダイジェスト値を計算
バイナリ形式で出力したものを、base16 でエンコード

```
[ec2-user@ip-10-0-12-31 ~]$ echo "Hello World!" >> dummy.txt
[ec2-user@ip-10-0-12-31 ~]$ openssl md5 -binary dummy.txt | base64
jd2L5LF5pSmvpfL/rkuYWA==
[ec2-user@ip-10-0-12-31 ~]$ aws s3api put-object --bucket s3-bb-shinyasato --key dummy.txt --body dummy.txt --content-md5 jd2L5LF5pSmvpfL/rkuYWA==
{
    "ETag": "\"8ddd8be4b179a529afa5f2ffae4b9858\"",
    "ServerSideEncryption": "AES256"
}
```

アップロードを確認
ETag は 16 進数形式の MD5 ダイジェスト値

```
[ec2-user@ip-10-0-12-31 ~]$ openssl md5 -hex dummy.txt
MD5(dummy.txt)= 8ddd8be4b179a529afa5f2ffae4b9858
```

※ ETag はオブジェクトの特定のバージョンの識別子を示す
レスポンスヘッダーで、オブジェクト自体の変更を反映し、
メタデータの変更時には反映されない

MD5 を利用したデータの整合性の検証 2

MD5 ダイジェスト値が異なる場合にはエラーが発生する

今回は、引き渡す MD5 ダイジェスト値を意図的に変更し、擬似的なファイルの改竄を発生させた

```
[ec2-user@ip-10-0-12-31 ~]$ echo "Hello World!" >> dummy.txt
[ec2-user@ip-10-0-12-31 ~]$ openssl md5 -binary dummy.txt | base64
jd2L5LF5pSmvpfL/rkuYWA==
[ec2-user@ip-10-0-12-31 ~]$ aws s3api put-object --bucket s3-bb-shinyasato --key dummy.txt --body dummy.txt --content-md5 jd2L
5LF5pSmvpfL/rkuYWA==
{
    "ETag": "\"8ddd8be4b179a529afa5f2ffae4b9858\"",
    "ServerSideEncryption": "AES256"
}
```

```
[ec2-user@ip-10-0-12-31 ~]$ aws s3api put-object --bucket s3-bb-shinyasato --key dummy.txt --body dummy.txt --content-md5 jd2L
5LF5pSmvpfL/rkuYWA==1
```

An error occurred (InvalidDigest) when calling the PutObject operation: The Content-MD5 you specified was invalid.

MD5 を利用したデータの整合性の検証 3

アップロードすると、自動的に ETag が MD5 の値になる

```
[ec2-user@ip-10-0-12-31 ~]$ aws s3api head-object --bucket s3-bb-shinyasato --key dummy.txt
{
    "AcceptRanges": "bytes",
    "LastModified": "2023-03-24T05:11:20+00:00",
    "ContentLength": 13,
    "ETag": "\"8ddd8be4b179a529afa5f2ffae4b9858\"",
    "ContentType": "text/plain",
    "ServerSideEncryption": "AES256",
    "Metadata": {}
}
```

- ETag は PUT Object/POST Object/Copy や マネジメントコンソール上でオブジェクトが作成されたとき、MD5 ハッシュ値となる。この場合、保存または計算された MD5 ハッシュ値と ETag を比較することで、**整合性を検証することができる**
- ただし、マルチパートアップロードを用いた場合や、SSE-C/SSE-KMS を設定時には、ETag は MD5 ハッシュではない。この場合には、“--metadata md5=” などのコマンドを用いて、MD5 ハッシュを別途保存することでデータの整合性の検証ができる

マルチパートアップロードを利用した場合の例

マルチアップロードの対象となるサイズのファイルを作成

```
[ec2-user@ip-10-0-12-31 ~]$ dd if=/dev/zero of=./dummy.txt bs=1M count=512
512+0 records in
512+0 records out
536870912 bytes (537 MB, 512 MiB) copied, 5.33334 s, 101 MB/s
[ec2-user@ip-10-0-12-31 ~]$ openssl md5 -hex dummy.txt
MD5(dummy.txt)= aa559b4e3523a6c931f08f4df52d58f2
[ec2-user@ip-10-0-12-31 ~]$ aws s3 cp ./dummy.txt s3://s3-bb-shinyasato/ --metadata md5=aa559b4e3523a6c931f08f4df52d58f2
upload: ./dummy.txt to s3://s3-bb-shinyasato/dummy.txt
[ec2-user@ip-10-0-12-31 ~]$ aws s3api head-object --bucket s3-bb-shinyasato --key dummy.txt
{
  "AcceptRanges": "bytes",
  "LastModified": "2023-03-24T05:28:04+00:00",
  "ContentLength": 536870912,
  "ETag": "\"6d1954a8c7d6f09434c1ba4745a86869-64\"",
  "ContentType": "text/plain",
  "ServerSideEncryption": "AES256",
  "Metadata": {
    "md5": 'aa559b4e3523a6c931f08f4df52d58f2'
  }
}
```

MD5 ダイジェスト値を計算

MD5 ダイジェスト値を
メタデータを引き渡す

ETag は MD5 ダイジェスト値とは異なる

メタデータとして MD5 ダイジェスト値を保存

MD5 以外のチェックサムを利用した整合性の検証

- CRC32/CRC32C/SHA-1/SHA-256 をサポート

追加のチェックサム

チェックサム関数は、新しいオブジェクトの追加のデータ整合性検証を行うために使用されます。詳細は[こちら](#)

追加のチェックサム

オフ
Amazon S3 では、MD5 チェックサムと ETag を組み合わせてデータ整合性が検証されます。

オン
追加のデータ整合性検証用に、チェックサム関数を指定します。

チェックサム関数

チェックサム値を計算するために使用するチェックサム関数を選択します。

SHA-256

事前計算された値 - オプション

16 MB 未満の単一のオブジェクトのために事前に計算された値を指定すると、S3 は、その値を、選択されたチェックサム関数を使用して計算した値と比較します。値が一致しない場合、アップロードは開始されません。詳細は[こちら](#)

aaa

事前に計算したダイジェスト値を提供できる

ダイジェスト値が異なると
アップロードに失敗する

⚠ お客様が用意したこのオブジェクトの事前計算済みの値が、選択されたチェックサム関数の予期されるチェックサム値と一致しません。
値を確認してからもう一度試してください。または、フィールドを空白のままにすると S3 によりチェックサム値が計算されます。

追加のチェックサム

チェックサム関数は、新しいオブジェクトの追加のデータ整合性検証を行うために使用

追加のチェックサム

オン

チェックサム関数

SHA-256

チェックサムの値

47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU=

アップロードに成功するとチェックサムが保存される
注意: マルチパートアップロードを利用した場合、オブジェクトの
ダイジェスト値とは異なる値が保存される※

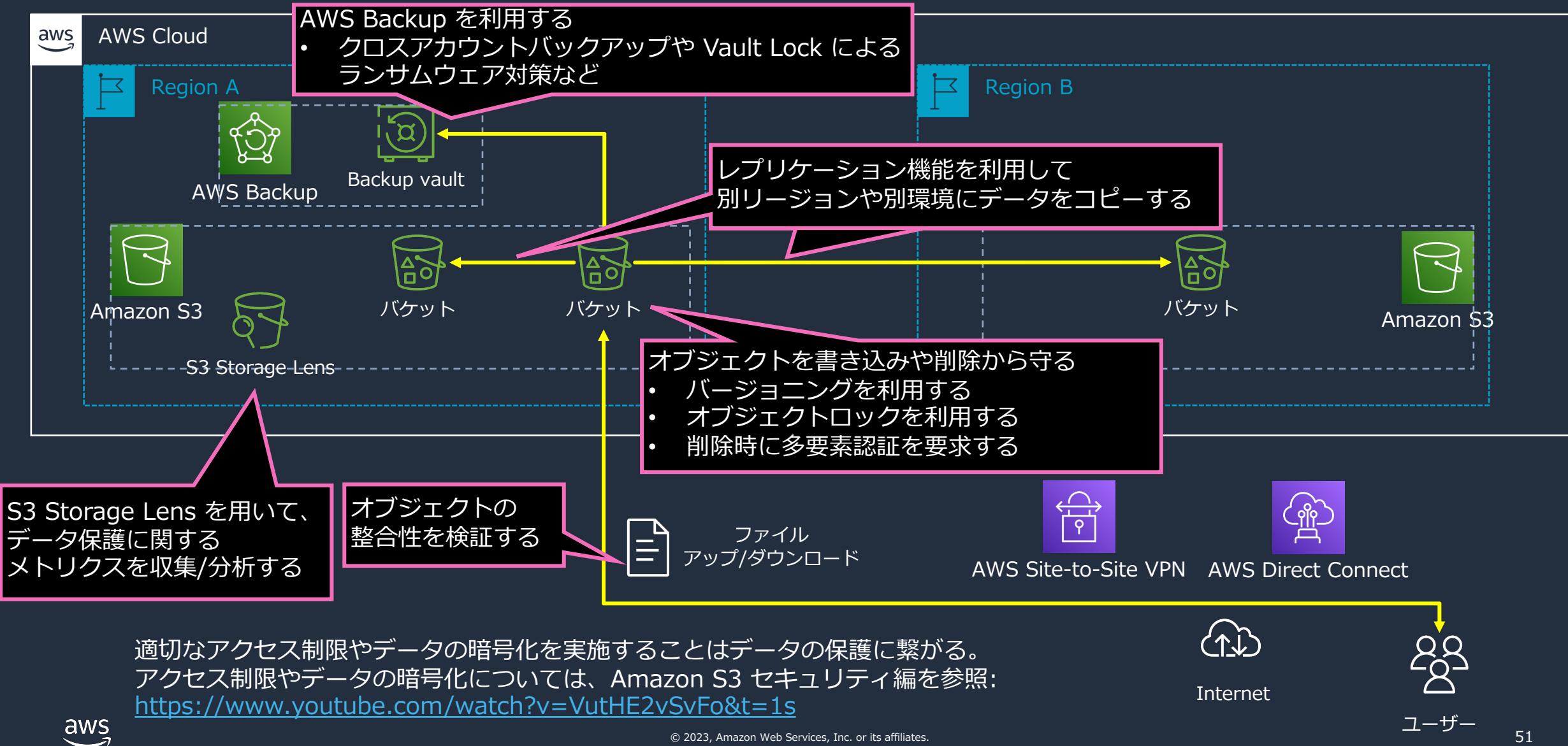
※参考:

https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/checking-object-integrity.html

まとめ



S3 におけるデータ保護のポイント（再掲）



まとめ

- Amazon S3 は高い耐久性/低コスト/セキュアなオブジェクトストレージ
- データのバージョンニングとオブジェクトロックを使い、データの誤削除や上書きを防ぐ。特に WORM 機能を提供するオブジェクトロックはランサムウェアに対して有効となる
- AWS Backup を利用することで、バケット/フォルダ単位でバックアップ/リストア/保護できる
- レプリケーション機能を利用して、コンプライアンス要件を満たすことや DR に利用できる
- チェックサム機能を利用することで、データの改竄を検知することができる
- アクセス制御を適切に設定することで、データの保護はさらに強力になる

本資料に関するお問い合わせ・ご感想

技術的な内容に関しましては、有料のAWSサポート窓口へ
お問い合わせください

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

料金面でのお問い合わせに関しましては、カスタマーサポート窓口へ
お問い合わせください（マネジメントコンソールへのログインが必要です）

<https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service>

具体的な案件に対する構成相談は、後述する個別相談会をご活用ください



ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt



その他コンテンツのご紹介

ウェビナーなど、AWSのイベントスケジュールをご参照いただけます

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

ハンズオンコンテンツ

<https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/>

AWS 個別相談会

AWSのソリューションアーキテクトと直接会話いただけます

<https://pages.awscloud.com/JAPAN-event-SP-Weekly-Sales-Consulting-Seminar-2021-reg-event.html>



Thank you!



Amazon Simple Storage Service (Amazon S3)

セキュリティ編

佐藤 真也

Amazon Web Service Japan G.K.

Solutions Architect

2023/01

AWS Black Belt Online Seminarとは

- ・ 「サービス別」「ソリューション別」「業種別」などのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- ・ AWSの技術担当者が、AWSの各サービスやソリューションについてテーマごとに動画を公開します
- ・ 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます
- ・ 以下のURLより、過去のセミナー含めた資料などをダウンロードすることができます
 - ・ <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>

内容についての注意点

- ・ 本資料では 2023 年 1 月時点のサービス内容および価格についてご説明しています。最新の情報は AWS 公式ウェブサイト(<https://aws.amazon.com/>)にてご確認ください
- ・ 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- ・ 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます

自己紹介

名前：佐藤 真也 (Sato Shinya)

所属：アマゾン ウェブ サービス ジャパン合同会社
技術統括本部 金融ソリューション本部
保険ソリューション部

好きなAWSサービス：

- AWS Snowball Edge
- Amazon Simple Storage Service (S3)
- Amazon FSx シリーズ



本セミナーの対象者

前提知識

- AWS のグローバルインフラストラクチャやフルマネージドサービスの概念
- AWS IAM、Amazon VPC などの基盤となるサービスの知識
- Amazon S3 入門編あるいは同等の知識

対象者

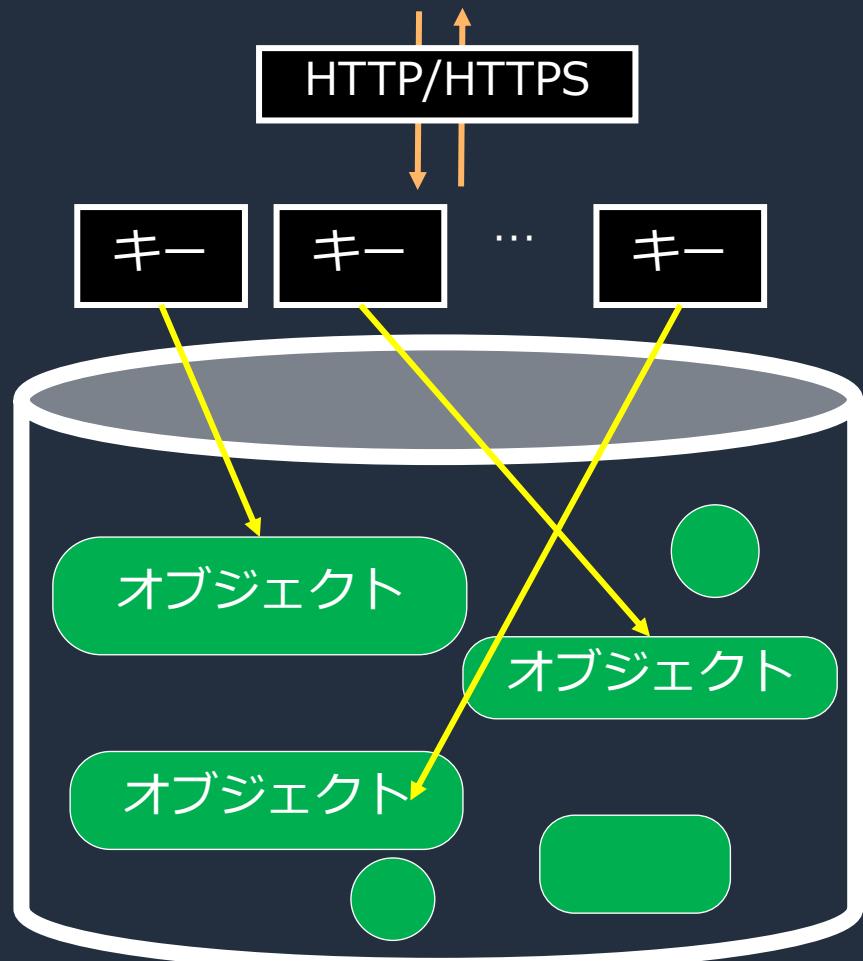
- Amazon S3 のセキュリティについて、特徴や機能を深く知りたい方

アジェンダ

1. Amazon S3 の概要
2. Amazon S3 におけるデータの暗号化
3. Amazon S3 でのアクセス制御
4. Amazon S3 へのアクセス方法
5. Amazon S3 におけるログ監査
6. まとめ

Amazon S3 の概要

オブジェクトストレージとは



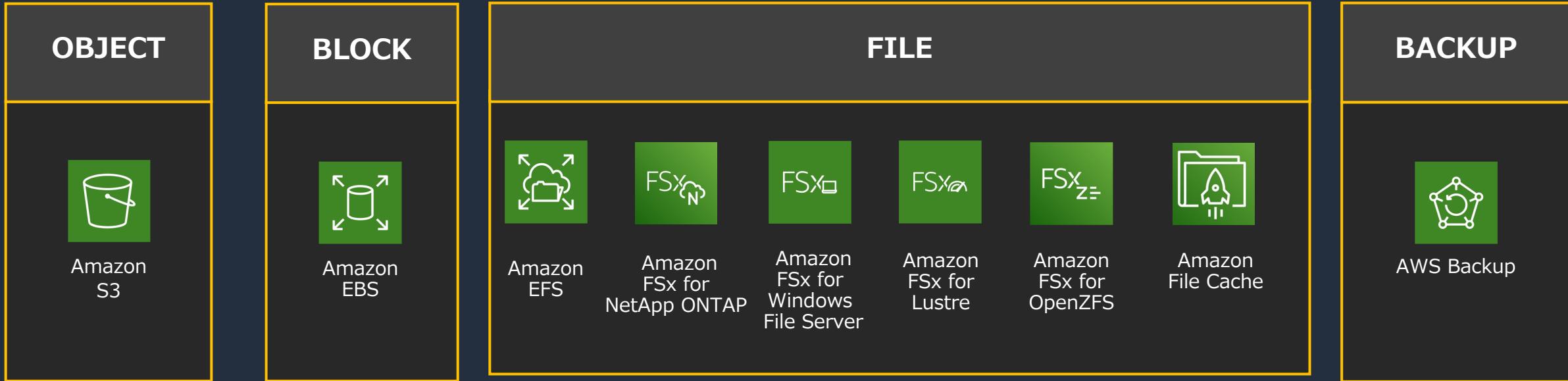
特徴

- HTTP/HTTPS でアクセス
- 一意のキーに対するオブジェクト（データ）が存在
- 階層構造を取るファイルストレージとは異なり、フラットな構造

メリット

- スケールが容易で、大容量のデータ保存が可能
- オブジェクト単位でのアクセス制御
- 高い可用性と耐障害性
- 独自にカスタマイズできるメタデータを追加可能

AWS のストレージサービス



DATA TRANSFER AND MIGRATION



AWS Storage
Gateway



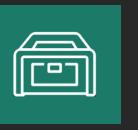
AWS DataSync



AWS Transfer
Family



AWS Snowball



AWS Snowcone

Amazon S3 とは

高いパフォーマンスと可用性、そして低コストが特徴なオブジェクトストレージ
2006 年に登場してから、現在に至るまでのイノベーションが積み重なった歴史あるサービス

- 耐久性
 - 99.99999999% (イレブンナイン)
 - 最低 3 つのアベイラビリティゾーン (AZ) で冗長化
- スケーラビリティ
 - 無制限のデータ保存
 - ただし、1 オブジェクトは最大 5 TB
- 低コスト
- セキュリティ
 - アクセス制御とログ監査
- データの保護
 - 誤削除から守る機能
- アクセシビリティ
 - HTTP/HTTPS でアップロード/ダウンロード/変更/削除といった操作が可能
- 様々な AWS サービスとの連携

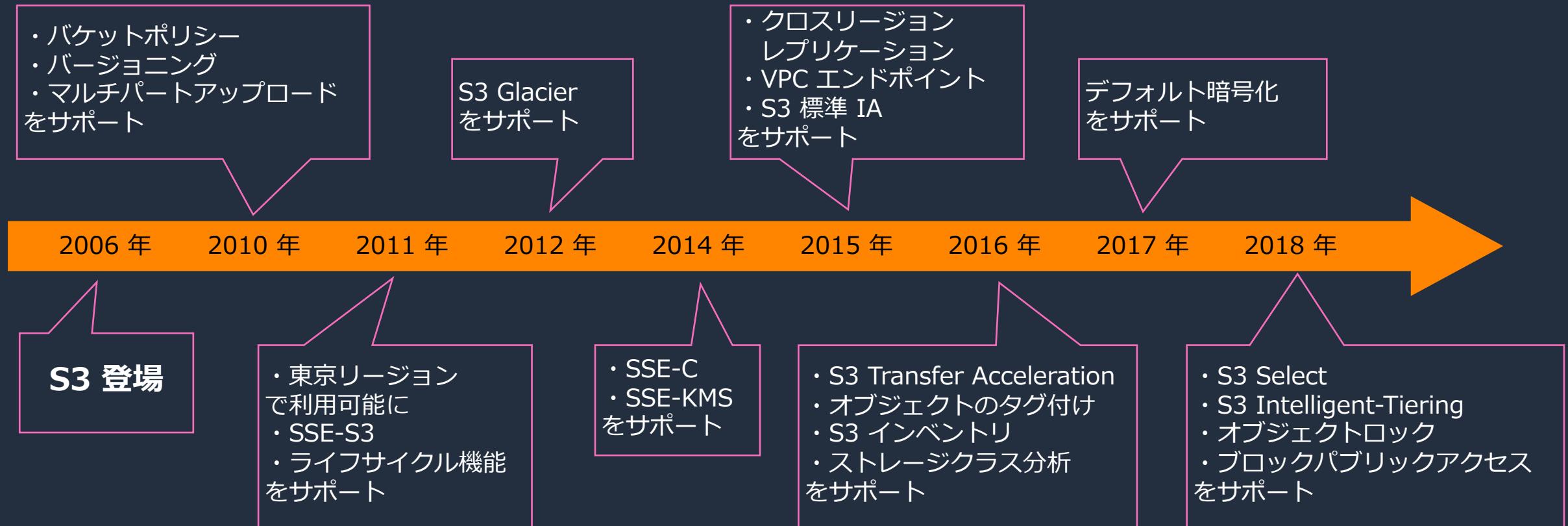


Amazon S3 の特徴などは FAQ にて詳解: <https://aws.amazon.com/jp/s3/faqs/?nc=sn&loc=7>

Amazon S3 の 2018 年までの主要アップデート



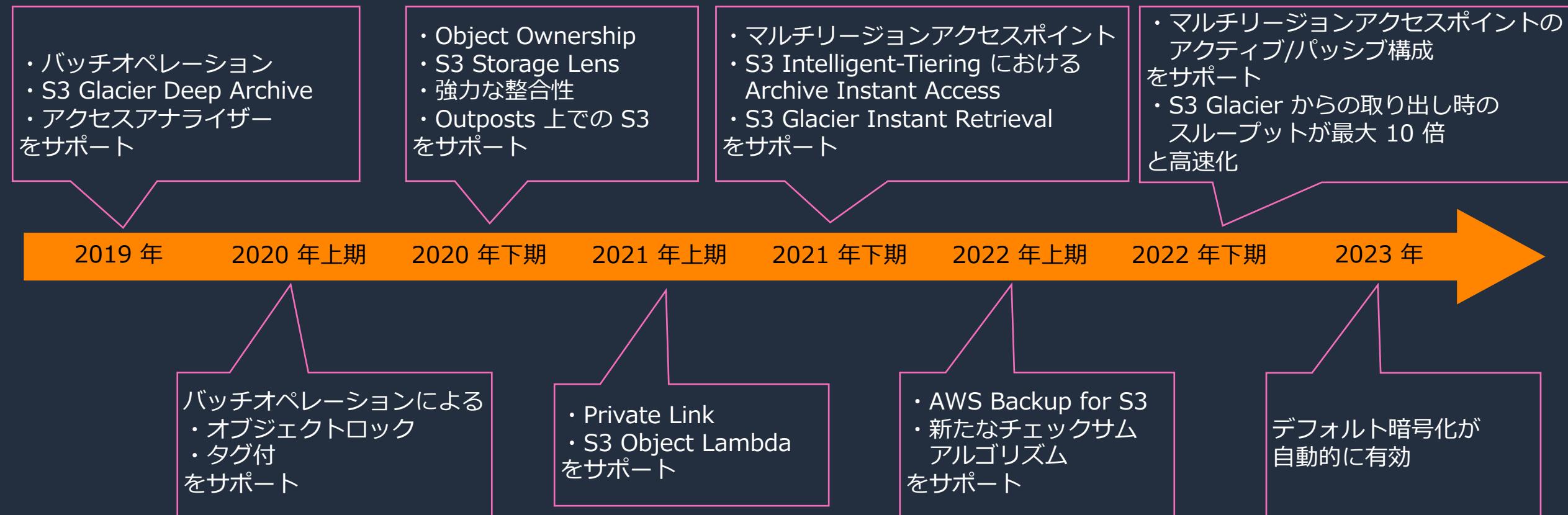
Amazon S3



Amazon S3 の 2019 年以降の主要アップデート



Amazon S3



S3 におけるセキュリティのポイント

バケットに対する操作をどう制限するか？（予防的統制）

- ・ ポリシー（バケットポリシー、VPC エンドポリシー、アクセスポイントポリシー、IAM ポリシー、サービスコントロールポリシー、KMS キーポリシーなど）で制限する
- ・ 例：特定操作に対するアクセス元 IP 制限や多要素認証（MFA）を実施するバケットポリシー
- ・ 例：アプリケーションごとに可能な操作を制限するアクセスポイントポリシー

※ 本資料の Amazon S3 でのアクセス制御、Amazon S3 へのアクセス方法で紹介

アクセス経路をどう制限するか？

（予防的統制から抜粋）

- ・ ブロックパブリックアクセスの有効化
- ・ バケットポリシーで特定の VPC からのアクセスに制限する

※ 本資料の Amazon S3 でのアクセス制御で紹介



ファイルをどこで暗号化するか？

クライアント/通信経路/S3 で暗号化を行う

※ 本資料の Amazon S3 におけるデータの暗号化で紹介

意図しないアクセスや操作をどう調査するか？

- ・ AWS Config で構成管理情報を取得する
- ・ AWS CloudTrail や S3 サーバーアクセスログを用いてログを取得する
- ・ S3 Storage Lens でメトリクスを監視する
- ・ Access Analyzer for S3 を用いて、アクセス許可を付与しているバケットを確認する

※ 本資料の Amazon S3 でのアクセス制御、Amazon S3 におけるログ監査で紹介

そして、これらをどう検知するか？（発見的統制）

- ・ 例：AWS Config と Amazon EventBridge を利用して、意図しない設定がなされた時、Amazon SNS 経由で管理者に通知する

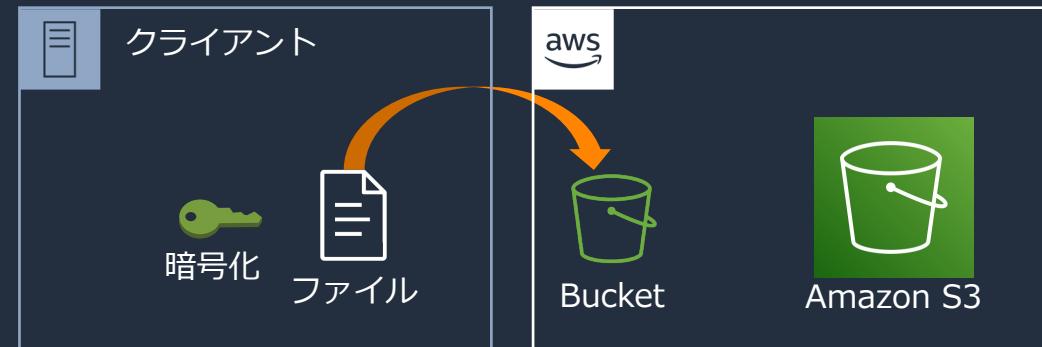
Amazon S3 における データの暗号化



S3 におけるデータ暗号化

1. クライアントサイド暗号化

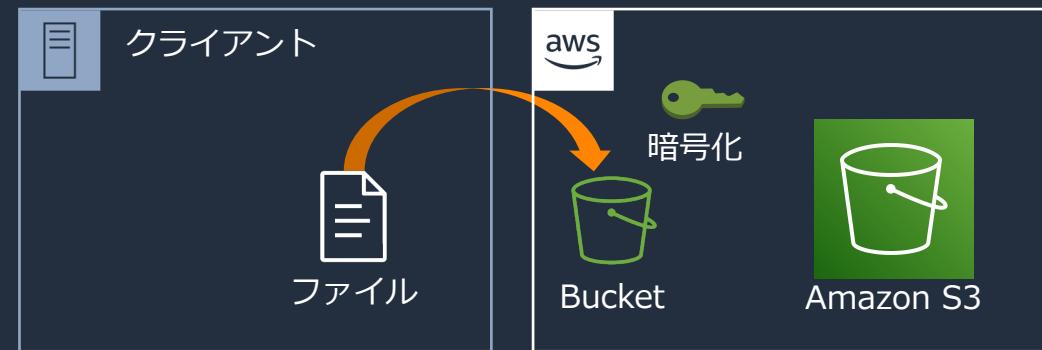
- クライアント側でデータを暗号化し、暗号化したデータを S3 へアップロード



2. クライアントと S3 の通信中のデータを暗号化 (HTTPS)

3. サーバーサイド暗号化

- オブジェクトを S3 へ保存する前に暗号化
 - データをオブジェクトレベルで暗号化、メタデータは暗号化されない
 - オブジェクトをダウンロードするときに復号
 - 現在はデフォルトで有効化
- 3 つの方法が存在
 - S3 が管理するキーによる暗号化 (**SSE-S3**)
 - AWS Key Management Service (KMS) に保存されているキーによる暗号化 (**SSE-KMS**)
 - カスタマーが指定したキーによる暗号化 (**SSE-C**)
- 異なる種類のサーバーサイド暗号化を同時に同じオブジェクトに指定はできない



サーバーサイド暗号化における注意点

- デフォルト暗号化で SSE-KMS を設定したバケットは、S3 サーバーアクセスログの送信先として指定することはできない。サーバーアクセスログの送信先バケットには、SSE-S3 を設定したバケットを選択する必要がある。
- SSE-C を使う場合の注意
 - デフォルト暗号化はできず、アップロード時には暗号化キーをリクエストに加える
 - ダウンロード時には、暗号化キーをリクエストに加える
 - コンソールでは、SSE-C を利用したアップロードはできず、SDK または S3 REST API 経由でアップロードを行う
 - HTTPS を使用する
 - ETag は オブジェクトの MD5 のダイジェスト値と異なる
 - データの整合性に ETag は利用できないので、additional checksum 機能を利用する

注意点の参考: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-encryption.html>
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/ServerSideEncryptionCustomerKeys.html>



SSE-KMS に Dive Deep 1

- 使用可能なキーから選択できる aws/s3 は AWS が管理するマネージドキー
- KMS で作成したカスタマーマネージドキーも使用可能
 - 対称鍵のみサポート

デフォルトの暗号化 情報
サーバー側の暗号化は、このパケットに保存された新しいオブジェクトに自動的に適用されます。

暗号化キータイプ 情報
 Amazon S3 マネージドキー (SSE-S3)
 AWS Key Management Service キー (SSE-KMS)

AWS KMS キー 情報
 AWS KMS キーから選択する
 AWS KMS キー ARN を入力する

使用可能な AWS KMS キー

AWS KMS キーを選択する

暗号化の流れ

1. S3 は、「平文のデータキー」と「指定の KMS キーで暗号化されたキーのコピー」をリクエスト
2. AWS KMS は、データキーを生成し、KMS キーで暗号化し、平文と暗号化されたデータキーを S3 に送信
3. データキーを使用してデータを暗号化し、使用後に平文のデータキーを削除
4. 暗号化されたデータキーを、暗号化されたデータのメタデータとして保存

復号の流れ

1. S3 は暗号化されたデータキーを AWS KMS へ送信
2. KMS キーで復号、平文のデータキーを S3 に送信
3. 暗号化されたデータを復号し、平文のデータキーを削除

SSE-KMS の暗号化と複合の流れ: https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/UsingKMSEncryption.html

SSE-KMS に Dive Deep 2

注意点

- ・ アクセスするリソースに対して、次の許可を与える。KMS キーのポリシーにおける許可も確認する
 - ・ アップロードの際: 「kms:Decrypt」と「kms:GenerateDataKey」
 - ・ ダウンロードの際: 「kms:Decrypt」
- ・ 別途 KMS キーを使用するための料金が必要
 - ・ アップロード/ダウンロードごとに KMS ヘリクエストが送信される
- ・ 利用するキーはバケットと同じリージョンでなければならない

ユースケース

- ・ KMS キーの使用方法を制御するポリシーを独自に定義したい
- ・ KMS キーの使用状況を監視したい



SSE-KMS に Dive Deep 3

S3 バケットキー

- KMS キーの使用に対する料金が発生するため、KMS へのリクエストが多い場合に注意が必要 この場合、S3 バケットキーを利用することで解決できる。
 - バケットレベルのキーが生成される
 - 追加されるオブジェクトに対して、一意のデータキーを作成するために使用される
 - KMS へのリクエストは減少する



デフォルト暗号化の注意点

- アップロード時に暗号化の方法 (SSE-S3/KMS/C) を明示的に指定すると、デフォルト暗号化 (SSE-S3 or SSE-KMS) の設定は上書きされる（下表の太字部分）

デフォルト暗号化設定とアップロード時の暗号化の方法を指定した場合の結果まとめ

アップロード時の暗号化の方法を指定

デフォルト 暗号化設定	アップロード時に 明示的に 指定しない	アップロード時に SSE-S3 を指定	アップロード時に SSE-KMS を指定	アップロード時に SSE-C を指定
SSE-S3	SSE-S3	SSE-S3	SSE-KMS	SSE-C
SSE-KMS	SSE-KMS			

デフォルト暗号化設定とアップロード時の暗号化方法をした場合の挙動について: <https://repost.aws/ja/knowledge-center/s3-aws-kms-default-encryption>

デフォルト暗号化の違い

	SSE-S3	SSE-KMS AWS KMS で作成したキー	SSE-KMS AWS が管理するキー: aws/s3
キーポリシーの管理	(-) できない	(+) できる	(-) できない
AWS CloudTrail でのログギング	(-) できない	(+) できる	(+) できる
キーローテーション	(+) S3 が実施する	利用者が実施する	(+) AWS が実施する
データの共有	(+) できる	(+) できる	(-) できない

参考: https://d1.awsstatic.com/events/Summits/reinvent2022/STG301_Amazon-S3-security-and-access-control-best-practices.pdf (23P)

Amazon S3 でのアクセス制御

S3 のアクセス制御の概要

前提として、デフォルトでは S3 のバケット/オブジェクトなど全てのリソースはプライベートで、リソースを作成したアカウントのみがリソースへのアクセスができる

押さえておくべき要素

- ブロックパブリックアクセス
- IAM ポリシー/ロール、バケットポリシー
- バケット/オブジェクトアクセスコントロールリスト (ACL) 、S3 Object Ownership
- Access Analyzer for S3

ブロックパブリックアクセス

パブリックアクセス可能な状態とは:

署名付き URL などを用いず、インターネット経由で任意のユーザーからアクセスできる状態
→ブロックパブリックアクセスを設定することで、インターネット経由での意図しないユーザーからのアクセスや意図しないアクセスを許可する権限設定を拒否することができる

ブロックパブリックアクセスは利用することはセキュリティのベストプラクティス

ブロックパブリックアクセスの設定

アカウント単位の保護



パブリックアクセスを許可するバケットポリシー

```
{  
  "Version": "2012-10-17",  
  "Id": "Policy1531309205299",  
  "Statement": [  
    {  
      "Sid": "Allow get object by any",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": "s3:GetObject",  
      "Resource": "arn:aws:s3:::blackbelt"  
    }  
  ]  
}
```

ロックパブリックアクセス

アカウントレベルでの保護

パケット
アクセスポイント
Object Lambda アクセスポイント
マルチリージョンアクセスポイント
バッチオペレーション
S3 のアクセスアナライザー

このアカウントのロックパブリックアクセス設定

このアカウントのロックパブリックアクセス設定

データへのパブリックアクセスを許可する設定を制御するには、Amazon S3 ロックパブリックアクセス設定を使用します。

パブリックアクセスをすべてブロック

オン

- 新しいアクセスコントロールリスト (ACL) を介して付与されたバケットとオブジェクトへのパブリックアクセスをブロックする
- 任意のアクセスコントロールリスト (ACL) を介して付与されたバケットとオブジェクトへのパブリックアクセスをブロックする
- 新しいパブリックバケットポリシーまたはアクセスポイントポリシーを介して付与されたバケットとオブジェクトへのパブリックアクセスをブロックする
- 任意のパブリックバケットポリシーまたはアクセスポイントポリシーを介したバケットとオブジェクトへのパブリックアクセスとクロスアカウントアクセスをブロックする

編集

パブリックアクセスできる設定行為を防止する

このアカウントのロックパブリックアクセス設定

パブリックアクセス可能な設定がなされても
アクセスをブロックする

S3 の AWS Marketplace

バケットポリシー

バケット単位のリソースベースのポリシーで、バケットとオブジェクトへのアクセスを管理できる JSON で記述し、IAM ポリシー同様 Principal/Action/Resource/Condition などを指定できる

ユースケース

- バケットへのアクセス許可/拒否を条件に応じて付与したい
 - 特定の VPC/IP/アクセスポイント（後述）以外からのアクセスを制限
 - 削除リクエストの際には、MFA を要求
 - 複数のアカウントへのアクセス許可の付与
 - HTTPS 以外のリクエストを拒否する
 - …

アクセスの際に MFA を要求するバケットポリシー

```
{  
    "Version": "2012-10-17",  
    "Id": "123",  
    "Statement": [  
        {  
            "Effect": "Deny",  
            "Principal": "*",  
            "Action": "s3:*",  
            "Resource": "arn:aws:s3:::shinya-sato-bb-demo/*",  
            "Condition": {  
                "Null": {  
                    "aws:MultiFactorAuthAge": "true"  
                }  
            }  
        }  
    ]  
}
```



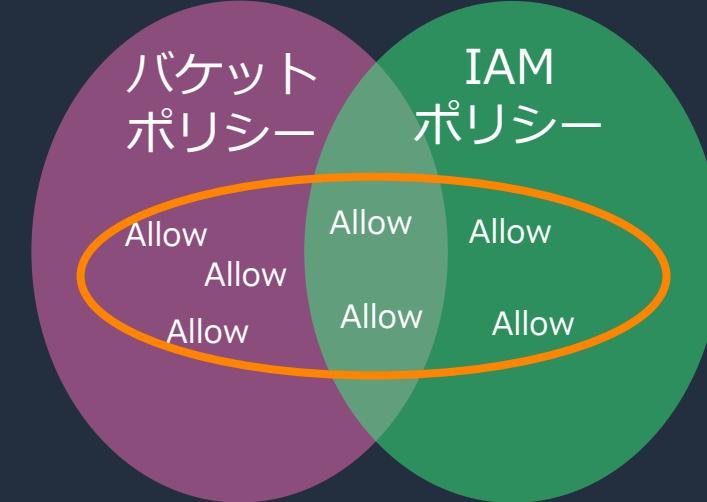
バケットポリシーと IAM ポリシーの関係 1

	バケットポリシー	IAM ポリシー
ポリシーの適用対象	S3 バケット 操作対象のリソース	IAM ロールをアタッチした EC2 や IAM ユーザーなどの操作を行うリソース
ポリシーの適用単位	Amazon Resource Name (ARN)	ARN またはタグ
ユースケース	特定のバケットごとに、条件に応じて アクセスを制限したい	ユーザー や ロール ごとに、特定の バケットへのアクセスを制限したい

バケットポリシーと IAM ポリシーを組み合わせてアクセス制御を行う場合もある

バケットポリシーと IAM ポリシーの関係 2

同一アカウントの S3 が操作対象



「同一」アカウントの S3 が操作対象

明示的な拒否がない操作は、

- IAM ポリシー
- バケットポリシー

のいずれかで許可することでアクセス権を付与できる

「別の」アカウントの S3 が操作対象

明示的な拒否がない操作は、次のいずれかでアクセスを許可する

- バケットポリシーとアクセス元のアカウントの IAM ポリシーの両方で許可する
- バケットを所有するアカウント（アクセス先）がアクセスを許可する IAM ロールを作成する。
その後、アクセス元のアカウントに対して提供する。

参考: <https://aws.amazon.com/jp/premiumsupport/knowledge-center/cross-account-access-s3/>

アクセス制御の例

バケットポリシー

```
{
  "Version": "2012-10-17",
  "Id": "123",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::blackbelt",
                  "arn:aws:s3::: blackbelt/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:SourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

VPC エンドポイント経由
以外のリクエストを全て拒否

VPC エンドポリシー

```
{
  "Effect": "Allow",
  "Principal": "*",
  "Action": [
    "s3>ListBucket",
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::blackbelt",
    "arn:aws:s3::: blackbelt/*"
  ],
  "Condition": {
    "StringEquals": {
      "aws:ResourceOrgID": "o-xxxxxxxxxxxx"
    }
  }
}
```

blackbelt バケットに対して
特定組織からの特定操作のみ許可

IAM ポリシー

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3::: blackbelt/*"
    }
  ]
}
```

blackbelt バケット内の
オブジェクトに対して GET のみ許可

この場合、該当する IAM ポリシーに対応する権限が付与された特定組織内のリソースは、
VPC エンドポイントを経由して blackbelt バケット内部のオブジェクトに対する GET のみできる

VPC エンドポイントポリシーは、IAM ポリシーやサービス固有のポリシー (S3 バケットポリシーなど) を上書き、または置き換えない:
https://docs.aws.amazon.com/ja_jp/vpc/latest/privatelink/vpc-endpoints-access.html



S3 Object Ownership と ACL

S3 Object Ownership (推奨かつデフォルト)

- ACL を無効にし、バケット内のリソースは全て、バケットの所有者が管理可能
- バケットポリシーや IAM ポリシーを利用して、他者へアクセス権を付与できる

ACL とは

- S3 Object Ownership を設定しない場合、オブジェクトをアップロードしたアカウントがそのオブジェクトの所有者になる場合がある
- オブジェクトの所有者へのフルアクセス許可を与える ACL が作成され、ACL を用いて他者へアクセス権を付与できる

オブジェクトごとにアクセスを制御する必要があるケースを除き、ACL を無効にすることを推奨
IAM ポリシー/バケットポリシーを利用し、他者からのアクセスを管理する

※ 新しいバケットも既存のバケットも S3 Object Ownership により ACL を無効化できる
S3 Object Ownership は解除できるが、以前に定めた ACL 設定が適用されるので注意

オブジェクト所有者 情報
他の AWS アカウントからこのバケットに書き込まれたオブジェクトの所有権と、アクセスコントロールリスト (ACL) の使用を管理します。オブジェクトの所有権は、オブジェクトへのアクセスを指定できるユーザーを決定します。

ACL 無効 (推奨)
このバケット内のすべてのオブジェクトは、このアカウントによって所有されます。このバケットとそのオブジェクトへのアクセスは、ポリシーのみを使用して指定されます。

ACL 有効
他の AWS アカウントがこのバケット内のオブジェクトの所有者となることができます。このバケットとそのオブジェクトへのアクセスは、ACL を使用して指定できます。

オブジェクト所有者

希望するバケット所有者
このバケットに書き込まれた新しいオブジェクトが `bucket-owner-full-control` 既定 ACL を指定する場合、その所有者はバケット所有者となります。それ以外の場合は、オブジェクトライターが所有者となります。

オブジェクトライター
オブジェクトライターが引き続きオブジェクト所有者となります。

① 新しいオブジェクトにのみオブジェクトの所有権を強制する場合、バケットポリシーは、オブジェクトのアップロードに `bucket-owner-full-control` 既定 ACL が必須であることを指定する必要があります。[詳細ははこちら](#)

ACL が有効なバケットの確認方法

ACL が有効になっているバケットへの
リクエストを確認したい場合



S3 サーバーアクセスログ
または AWS CloudTrail を利用する



S3 の ACL 活用に関するリクエストレベルの情報が
S3 サーバーアクセスログまたは
AWS CloudTrail で記録される

※ S3 サーバーアクセスログと AWS CloudTrail については後ほど解説

どのバケットで S3 Object Ownership が
有効/無効かを確認したい場合



S3 Storage Lens
を利用する



S3 Storage Lens のダッシュボードで
S3 Object Ownership が無効化されている
バケットを確認できる

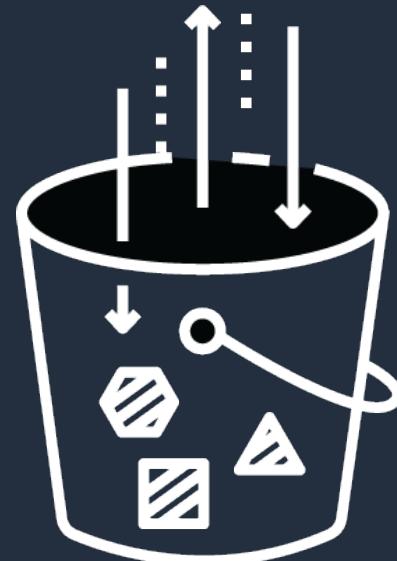
※ S3 Storage Lens の細かい仕様は本資料では解説しない

ACL が有効になっているバケットへのリクエストを確認

- S3 サーバーアクセスログと AWS CloudTrail のイベントフィールドとして aclRequired がある
 - S3 リクエストの承認に ACL が必要な場合 (=ACL が有効)
 - additionalEventData の aclRequired = Yes を記録
 - S3 リクエストの承認に ACL が不要な場合
 - サーバーアクセスログ: “-”
 - AWS CloudTrail: 出力なし



実環境での ACL 利用状況についてのインサイトが得られる
ACL からバケットポリシーへ権限設定の移行を検討する際に
有益な判断材料となる



ACL が有効なバケットを特定する方法

- S3 Storage Lens を活用

Object Ownership が有効 (=ACL が無効)							Object Ownership が無効 (=ACL が有効)		
アクセス管理 X	オブジェクトの所有者は バケットの所有者			"bucket-owner-full-control" と共に書き込んだ場合のみ、 オブジェクトの所有者は バケットの所有者			オブジェクトの所有者は アップロードした者		
バケット名	Object Ownership バ ケット所有者によって 強制されたバケット数	% (Object Ownership バケット所有者によっ て強制されたバッ ケット)	Object Ownership バ ケット所有者が優先す るバケット数	% (Object Ownership バケット所有者が優先 するバケット)	Object Ownership オ ブジェクトライバ ケット数	% (Object Ownership オブジェクトライバ ケット)	Object Ownership オ ブジェクトライバ ケット数	% (Object Ownership オブジェクトライバ ケット)	
[REDACTED]	1	100.00%	-	-	-	-	-	-	
[REDACTED]	1	100.00%	-	-	-	-	-	-	
[REDACTED]	1	100.00%	-	-	-	-	-	-	
[REDACTED]	-	-	-	-	-	-	1	100.00%	

Access Analyzer for S3 とは

任意のユーザー（インターネット含む）や他の AWS アカウントからのアクセス許可を付与している S3 バケットを一覧表示する
意図しないバケットやオブジェクトの公開を検知できる

The screenshot shows the AWS Access Analyzer for S3 interface. It displays two main sections: 'buckets with public access' and 'buckets with access from other AWS accounts'. A large orange callout box points to the top section, containing text about granting public access and a link to detailed information. Another orange callout box points to the bottom section, detailing policy types like Bucket Policy, ACL, and Access Point Policy, along with permissions for List/Read/Write and Tagging. A third orange callout box at the bottom right highlights the status 'Active (未確認)' and 'Archived (確認済み)'. The interface includes various filters and sorting options.

パブリックアクセスまたは他の AWS アカウントからのアクセスを許可するバケットを表示

パブリックアクセスを備えたバケット

検出結果を表示 アクティブとしてマーク アーカイブ パブリックアクセスをすべてブロック

これらのバケットには、インターネット上の誰でもアクセスできます。特定の検証済みのユースケースにパブリック設定が必要な場合を除き、AWS はバケットへのすべてのパブリックアクセスをブロックすることをお勧めします。詳細は[こちら](#)

ステータス: すべて < 1 > ⚙️

バケット名 Access Analyzer によって検出済み 次を介して共有: ステータス アクセスレベル

次にパブリックバケットがありません: 米国西部 (オレゴン) us-west-2
表示するパブリックバケットがありません

他の AWS アカウント (サードパーティーの AWS アカウントを含む) からのアクセスを備えたバケット (1)

検出結果を表示 アクティブとしてマーク アーカイブ

これらのバケットは、条件付きで他の AWS アカウントと共有されます。確実にアクセスが意図したアカウントにのみ付与されるべき場合は、このバケットを削除するか、バケットポリシーを更新してバケット ACL を推奨しています。

ステータス: すべて < 1 > ⚙️

バケット名 Access Analyzer によって検出済み 次を介して共有: ステータス アクセスレベル

s3-bb-shinyasato a minute ago Bucket policy Active Write, Permissions

バケットポリシー、バケット ACL、アクセスポイントポリシー

List/Read/Write/Permissions (アクセス許可の編集) / Tagging (タグ付)

Active (未確認)
Archived (確認済み)

aws

© 2023, Amazon Web Services, Inc. or its affiliates.

34

Access Analyzer for S3 の設定方法 1

The screenshot illustrates the step-by-step setup of Access Analyzer for S3. It consists of three main panels:

- Left Panel (Amazon S3):** Shows the navigation menu with "S3 のアクセスアナライザー" highlighted.
- Middle Panel (Amazon S3 > S3 のアクセスアナライザー):** Displays information about the Access Analyzer and a note that it is not active in the current region. An orange arrow points from this panel down to the IAM console.
- Right Panel (Identity and Access Management (IAM) > Access Analyzer):** Shows the "Access Analyzer" page with a large orange arrow pointing from the previous panel here. It includes sections for "Access Analyzer" and "リソースへのアクセスをモニタリング".

IAM アクセスアナライザーを有効

S3 のアクセスアナライザー 情報

以下にリストされているパケットは、組織外の AWS ユーザーを含め、インターネットを利用するすべてのユーザーまたは認証された AWS ユーザーによるアクセスを許可するように設定されています。AWS は、すぐにアクセスを制限することをお勧めします。各パケットを確認して、アクセスを確認します。IAM コンソールで詳細な結果を表示します。パケットポリシー、アクセスポイントポリシー、または ACL が追加または変更されると、Access アナライザーは 30 分以内に変更に基づいて結果を生成および更新します。アカウントレベルのブロックパブリックアクセス設定またはマルチリージョンアクセスポイントの設定に関連する結果は、設定を変更してから最大 6 時間生成または更新されない場合があります。詳細はこちら

このリージョンではアクセスアナライザーが有効になっていません
このリージョンでアクセスアナライザーを有効にするには、IAM アクセスアナライザーにアクセスし、信頼ゾーンとしてアカウントを持つアナライザーを作成します。S3 のアクセスアナライザーは、アカウントレベルのアナライザーを必要とします。別のリージョンを選択するには、リージョンフィルターを使用します。

Identity and Access Management (IAM)

ダッシュボード

▼ アクセス管理

- グループ
- ユーザー
- ロール
- ポリシー
- ID プロバイダー
- アカウント設定

▼ アクセスレポート

Access Analyzer

- アーカイブルール
- アナライザー
- 設定
- 認証情報レポート
- 組織活動
- サービスコントロールポリシー (SCP)

AWS account ID: 803661502912

米国西部 (オレゴン) us-west-2 レポートをダウンロード

Access Analyzer

リソースへのアクセスをモニタリング

ご利用開始にあたって

- Access Analyzer とは
- Access Analyzer ユーザーガイド

① アナライザーを作成

② アクティブな結果を確認

③ アクションを実行

aws

Access Analyzer for S3 の設定方法 2

アナライザーを作成 [情報](#)

アナライザーは信頼ゾーン内のリソースをスキャンします。

リージョン
米国西部 (オレゴン)
AWS リソースを使用する各リージョンで Access Analyzer を有効にする必要があります。

名前
 最大 255 文字数

信頼ゾーン [情報](#)
信頼ゾーン内でサポートされているすべてのリソースのポリシーが分析され、信頼ゾーン外から許可されたアクセスを特定します。
 現在の組織 現在のアカウント

タグ [情報](#)
オプションで、タグをアナライザーに追加します。タグは、AWS リソースを識別して整理するためのメタデータとして機能する単語またはフレーズです。各タグは、キーと 1 つのオプションの値で構成されています。

リソースに関連付けられたタグはありません。

タグ付けする
最大 50 のタグを追加できます。

Access Analyzer を有効にすると、サービスにリンクされたロールが現在のアカウントに作成されます。サービスにリンクされたロールは、ユーザーに代わって AWS リソースとやり取りするために Access Analyzer にアクセス許可を付与します。 [詳細はこちちら](#)

[キャンセル](#) [アナライザーを作成](#)

Amazon S3 > S3 のアクセスアナライザー

S3 のアクセスアナライザー [情報](#)

米国西部 (オレゴン) us-west-2 [レポートをダウンロード](#)

以下にリストされているパケットは、組織外の AWS ユーザーを含め、インターネットを利用するすべてのユーザーまたは認証された AWS ユーザーによるアクセスを許可するよう設定されています。AWS は、すぐにアクセスを制限することをお勧めします。各パケットを確認して、アクセスを確認します。IAM コンソール [で詳細な結果を表示します。](#) パケットポリシー、アクセスポイントポリシー、または ACL が追加または変更されると、Access アナライザーは 30 分以内に変更に基づいて結果を生成および更新します。アカウントレベルのブロックパブリックアクセス設定またはマルチリージョンアクセスポイントの設定に関連する結果は、設定を変更してから最大 6 時間生成または更新されない場合があります。詳細はこちら

リージョンにパブリックパケットがありません
他のリージョンのパブリックパケットを識別するには、リージョンフィルターを使用します。

パブリックアクセスを備えたパケット [検出結果を表示](#) [アクティブとしてマーク](#) [アーカイブ](#) [パブリックアクセスをすべてブロック](#)

これらのパケットには、インターネット上の誰でもアクセスできます。特定の検証済みのユースケースにパブリック設定が必要な場合を除き、AWS はパケットへのすべてのパブリックアクセスをブロックすることをお勧めします。詳細はこちら

ステータス: **すべて**

パケット名	Access Analyzer によって検出済み	次を介して共有:	ステータス	アクセスレベル

次にパブリックパケットがありません: 米国西部 (オレゴン) us-west-2
表示するパブリックパケットがありません

S3 アクセスアナライザーを設定

- 名前
- 組織 (AWS Organizations) 単位かアカウント単位か

Access Analyzer for S3 の動作確認

パケットポリシー

JSON で記述されたアクセスポイントポリシーは、パケットに保存されたオブジェクトへのアクセスを提供します。パケットポリシーは、他のアカウントが所有するオブジェクトには適用されません。[詳細](#)

編集

削除

 このアカウントとパケットに対してブロックパブリックアクセス設定が有効になっているため、パブリックアクセスはブロックされています
有効になっている設定を確認するには、[このアカウントのブロックパブリックアクセス設定](#)、このパケットのブロックパブリックアクセス設定を確認します。詳細については、「[Amazon S3 ブロックパブリックアクセスの使用](#)」をご覧ください

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AddCannedAcl",  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": "a*****"  
      },  
      "Action": [  
        "s3:PutObject",  
        "s3:PutObjectAcl"  
      ],  
      "Resource": "arn:aws:s3:::s3-bb-shinyasato/*"  
    }  
  ]  
}
```

□ コピーする

他のアカウントからのアクセスを許可する
パケットポリシーを設定する

他の AWS アカウント (サードパーティの AWS アカウントを含む) からのアクセスを備えたパケット (1)

検出結果を表示

アクティブとしてマーク

アーカイブ

これらのパケットは、条件付きで他の AWS アカウントと共有されます。確実にアクセスが意図したアカウントにのみ付与されるようにするために、AWS では、これらのパケットへのアクセスを確認することを推奨しています。

ステータス: すべて ▾

< 1 > 

パケット名	Access Analyzer によって検出済み	次を介して共有:	ステータス	アクセスレベル
s3-bb-shinyasato	a minute ago	Bucket policy	Active	Write, Permissions



Amazon S3 へのアクセス方法

押さえておくべきポイント

アクセスする方法

- 既存のエンドポイント: S3 のバケット名や Amazon Resource Name (ARN)
- アクセスポイント
- マルチリージョンアクセスポイント
- VPC エンドポイント

今回はアクセスポイントと VPC エンドポイントについて説明し、マルチリージョンアクセス
ポイントは「Amazon S3 マルチリージョン編」にて説明する（予定）

アクセスポイント

- バケットに対するネットワークエンドポイントで、既存のバケット名や ARN でアクセスした時の動作は変わらない
 - アクセスポイントに対してもアクセス制限ができる。
- アクセスポイントを利用する場合には、バケットポリシーとアクセスポイントの両方でリクエストを許可するポリシーを設定しなければならない
 - アクセスポイントを使用しない場合には、アクセスポイントのポリシーは適用されない

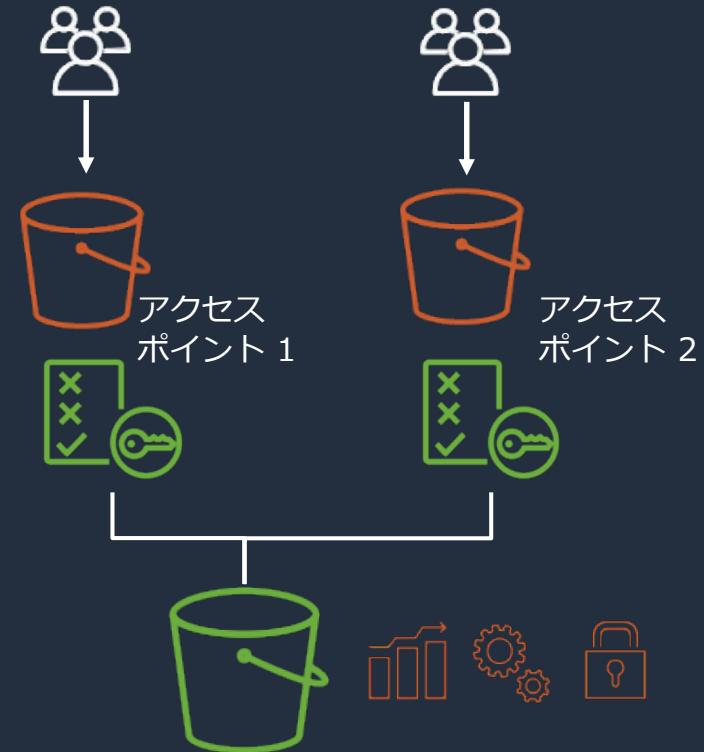
2種類のアクセス方法が選択できる

VPC 経由でのアクセス

- 特定の VPC 経由のみ操作ができるといった制限ができる
- アクセスポイント作成時のみエンドポイントが存在する VPC を指定できる

インターネット経由でのアクセス

- バケット単位でのロックパブリックアクセスとアクセスポイント単位のロックパブリックアクセスを明示的に無効にしなければ、インターネット経由のアクセスは全て拒否される
- アクセスポイント単位のロックパブリックアクセス設定の変更は作成後できない



アクセスポイントのユースケース

- 特定のアプリケーション向けのポリシーが必要
→ アプリケーションが多数存在する場合には、バケットポリシーでの記述が長大化
- アプリケーションに合わせて、S3 バケットへのアクセス許可を付与するポリシーをアタッチしたアクセスポイントを作成する

使用例

- バケットポリシーでアクセスポイント以外からのアクセスを拒否
- アプリケーションごとにアクセスポイントを作成

The screenshot shows the AWS S3 Access Points console for the bucket 'shinya-sato-bb-demo'. The 'Access Points' tab is selected. There are two entries listed:

名前	ネットワークオリジン	アクセス	アクセスポイントエイリアス
accesspoint-for-app1	Virtual private cloud (VPC)		
accesspoint-for-app2	Virtual private cloud (VPC)		

Below the table, there is a search bar labeled 'アクセスポイントを名前で検索'.

アクセスポイントの設定 1

アクセスポイント (0) 情報

Amazon S3 アクセスポイントは、S3 内の共有データセットに対する大規模なデータアクセスの管理を簡素化します。アクセスポイントは、S3 オブジェクトオペレーションの実行に使用できるバケットにアタッチされたネットワークエンドポイントの名前です。アクセスポイントのエイリアスは、アクセスポイント ARN と同じ機能を提供し、S3 バケット名がデータアクセスに通常使用されるあらゆる場所で使用するために置き換えることができます。詳細 [\[リンク\]](#)

アクセスポイントエイリアスのコピー ARN をコピー ポリシーを編集 削除 アクセスポイントの作成

検索: アクセスポイントを名前で検索 リージョン: 米国東部(バージニア北部) us-east-1

名前 ネットワークオリジン パケット アクセス アクセスポイントエイリアス

アクセスポイントなし
このリージョンにはアクセスポイントがあります

プロパティ

アクセスポイント名: [入力欄]
アクセスポイント名は、このリージョンのアカウント内で一意である必要があります。[アクセスポイントの命名規則](#)に準拠しなければなりません。

バケット名: [入力欄]
アカウントで S3 バケットを指定します。

AWS リージョン:
リージョンは、バケットの場所によって決まります。
米国西部(オレゴン) us-west-2

ネットワークオリジン:

Virtual private cloud (VPC)
インターネットアクセスがありません。リクエストは、指定された VPC でのみ行われます。

インターネット

① S3 コンソールでは、Virtual Private Cloud (VPC) アクセスポイントを使用したバケットリソースへのアクセスはサポートされていません。VPC アクセスポイントからバケットリソースにアクセスするには、AWS CLI、AWS SDK、または Amazon S3 REST API を使用する必要があります。[詳細はこちら](#)

VPC ID: vpc-[入力欄]
VPC ID は vpc- で始まる必要があります。

アクセスポイントの設定 2

ポリシー

このアカウントとアクセスポイントに対してブロックパブリックアクセス設定が有効になっているため、パブリックアクセスはブロックされています
有効になっている設定を確認するには、[このアカウントのブロックパブリックアクセス設定](#)
[このアクセスポイントのブロックパブリックアクセス設定](#)
を確認します。詳細については、「[Amazon S3 ブロックパブリックアクセスの使用](#)」をご覧ください

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Effect": "Allow",  
6             "Principal": {  
7                 "AWS": "arn:aws:  
8             },  
9             "Action": "s3>ListBucket",  
10            "Resource": "arn:aws:s3:us-west-2:  
11        }  
12    ]  
13 }
```

オブジェクト プロパティ アクセス許可 メトリクス 管理 アクセスポイント

アクセスポイント (2)
Amazon S3 アクセスポイントは、S3 内の共有データセットに対する大規模なデータアクセスの管理を簡素化します。アクセスポイントは、S3 オブジェクトオペレーションの実行に使用できるバケットにアタッチされたネットワークエンドポイントの名前です。アクセスポイントのエイリアスは、アクセスポイント ARN と同じ機能を提供し、S3 バケット名がデータアクセスに通常使用されるあらゆる場所で使用するために置き換えることができます。[詳細](#)

アクセスポイントエイリアスのコピー ARN をコピー ポリシーを編集 削除 アクセスポイントの作成

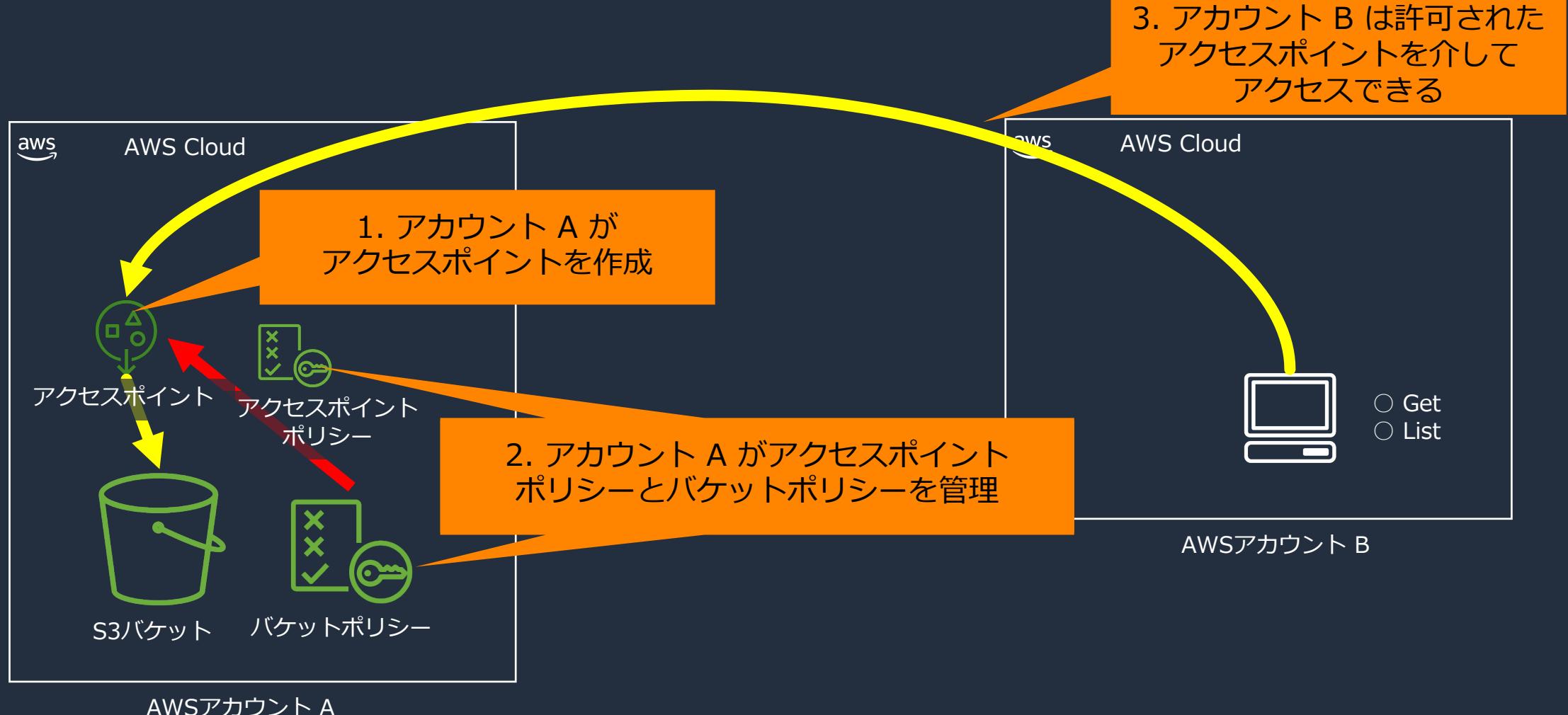
アクセスポイントを名前で検索

名前	ネットワークオリジン	アクセス	アクセスポイントエイリアス
accesspoint1	Virtual private cloud (VPC)		
accesspoint2	インターネット		



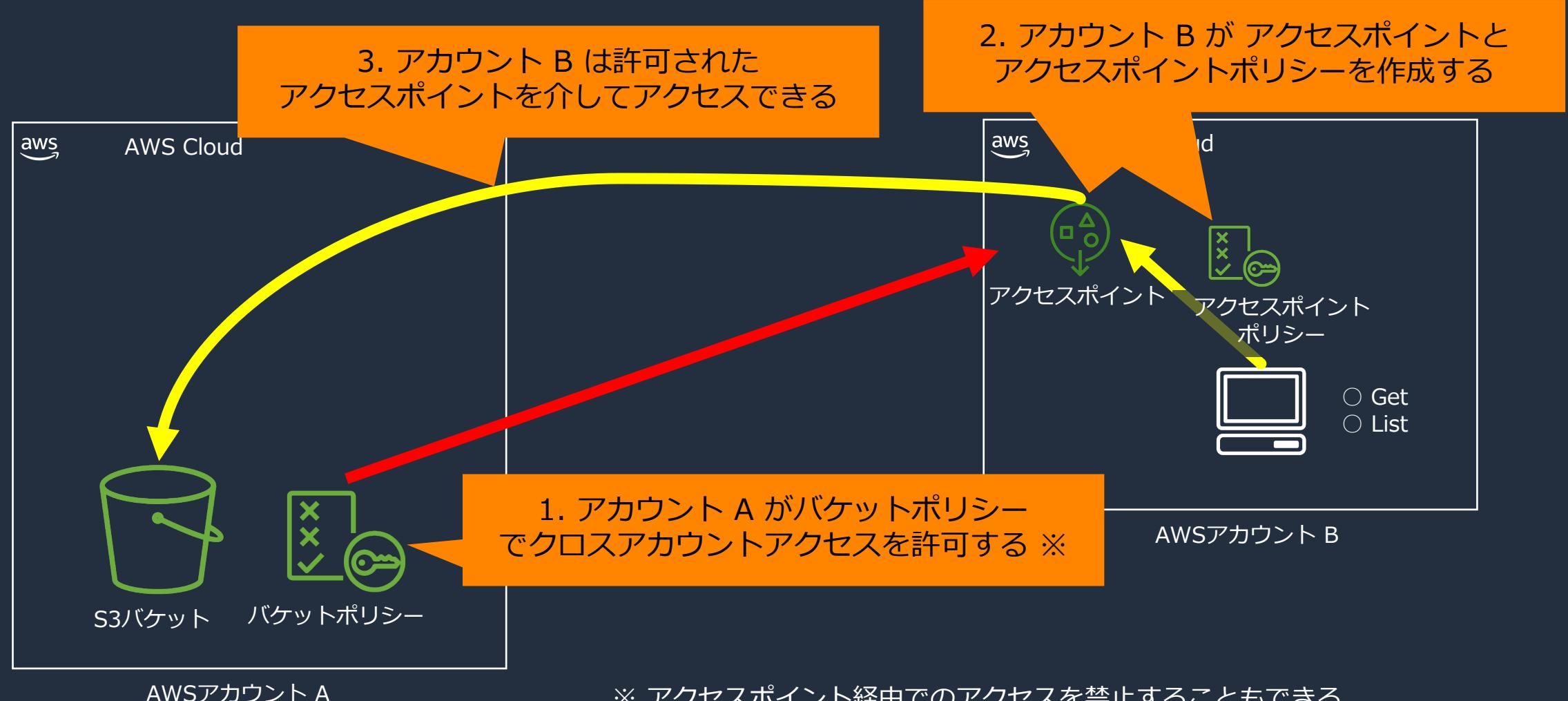
アクセスポイントを利用したクロスアカウントアクセス

アクセスポイントをバケットの所有者が管理



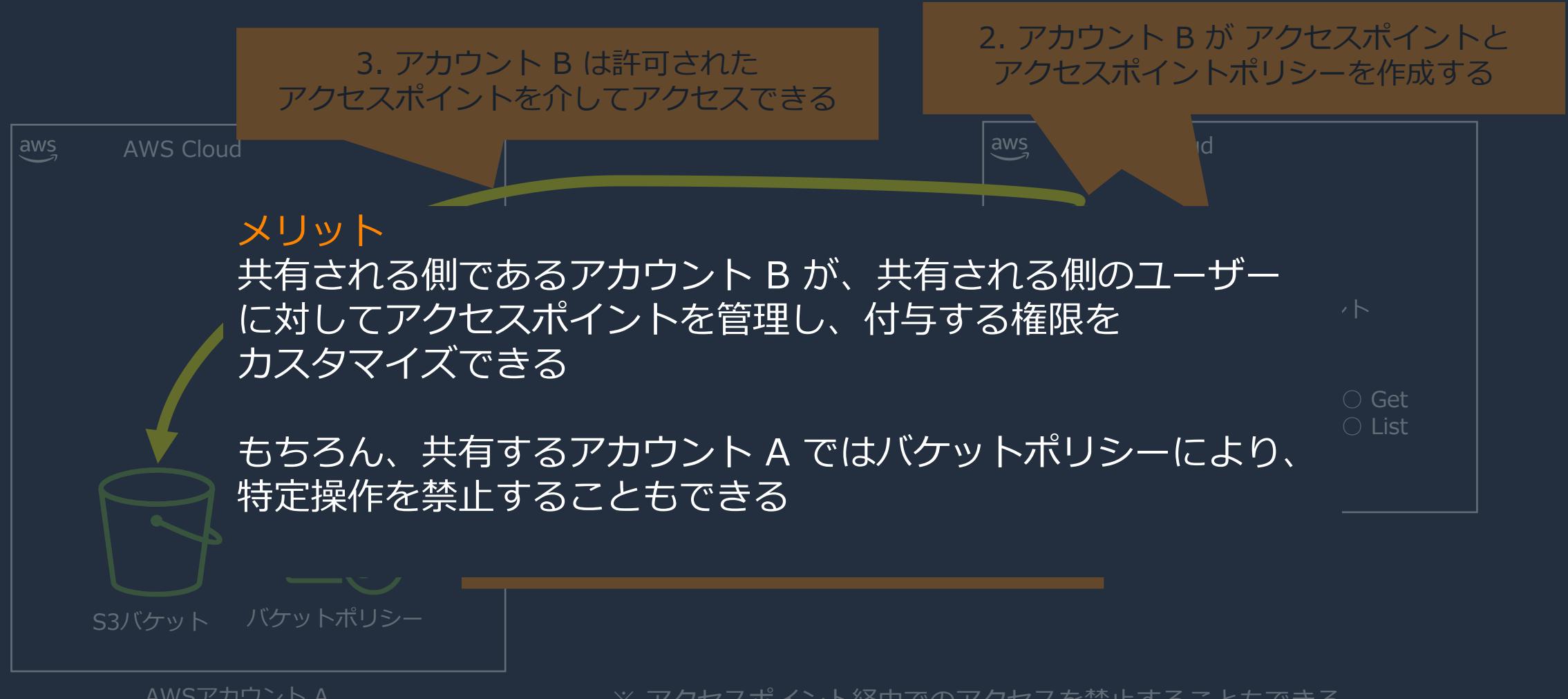
アクセスポイントを利用したクロスアカウントアクセス

アクセスポイントをアクセスするアカウントが管理



アクセスポイントを利用したクロスアカウントアクセス

アクセスポイントをアクセスするアカウントが管理



S3 の VPC エンドポイント

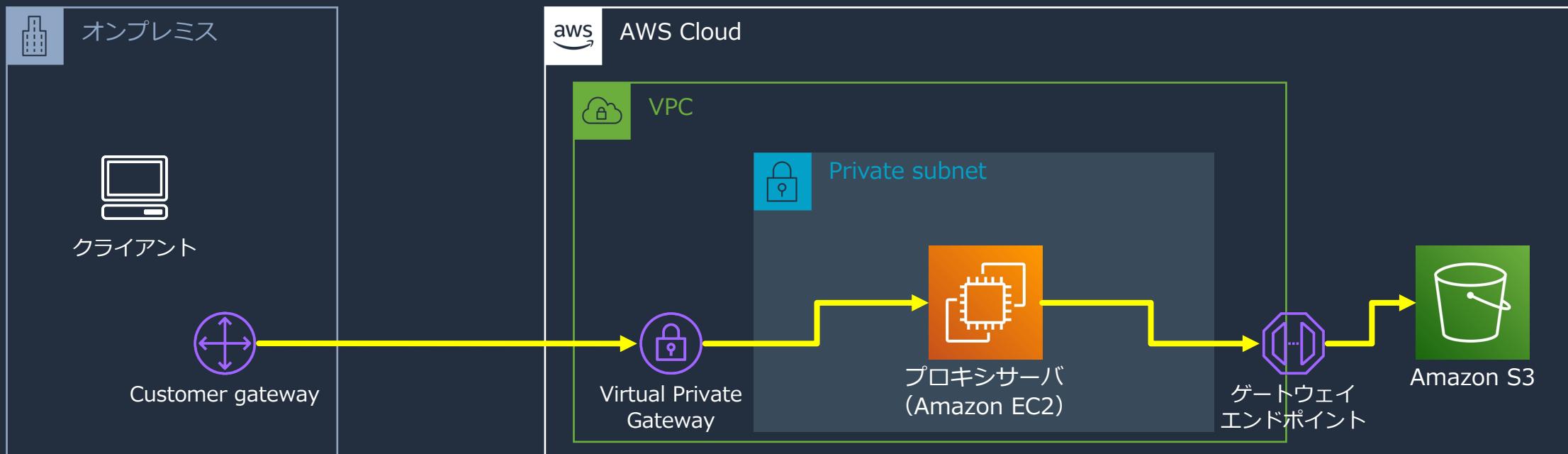
- ・ ゲートウェイエンドポイント
 - ・ VPC から AWS ネットワーク経由で S3 にアクセスする際、ルートテーブルで指定するゲートウェイ
- ・ インターフェイスエンドポイント (AWS PrivateLink)
 - ・ VPC 内部、オンプレミス、VPC ピアリングや Transit Gateway と紐づく別の VPC から、プライベート IP を利用してアクセス

ゲートウェイエンドポイント		インターフェイスエンドポイント
トラフィック		トラフィックは AWS の内部ネットワークを通る
IP アドレス	S3 のパブリック IP を使用	VPC のプライベート IP を使用
DNS 名	S3 DNS 名を使用	エンドポイント固有の S3 DNS 名を使用
オンプレミスからのアクセス	オンプレミスからのアクセスはできない*	オンプレミスからのアクセスができる
別のリージョンからのアクセス	別のリージョンからのアクセスはできない	VPC ピアリング/Transit Gateway と紐づく別のリージョンにある VPC からアクセスできる
料金	課金されない	課金される

* EC2 でプロキシサーバを構築することで利用することは可能

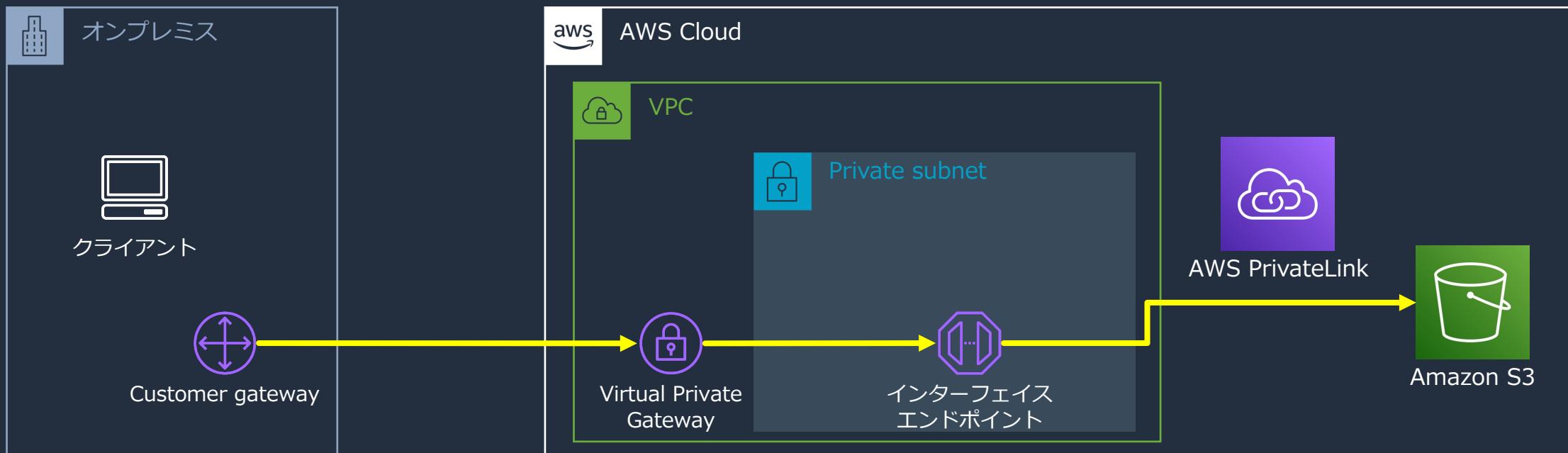
S3 のゲートウェイエンドポイントでのアクセスパス オンプレミスから閉じたネットワーク経由で S3 を利用する場合

EC2 などを利用したプロキシサーバを用意する必要がある



S3 のインターフェイスエンドポイントでのアクセスパス オンプレミスから閉じたネットワーク経由で S3 を利用する場合

プロキシサーバを用意する必要がなく、インターフェイスエンドポイントを利用して S3 へアクセスできる



インターフェイスエンドポイントの作成 1

VPC のマネジメントコンソールを開き、左側の項目から「エンドポイント」→「エンドポイントを作成」

エンドポイントの設定

名前タグ - オプション
「Name」のキーと、ユーザーが指定する値でタグを作成します。
pl-for-s3-bb

サービスカテゴリ
サービスカテゴリを選択

AWS のサービス
Amazon が提供するサービス

PrivateLink Ready パートナーのサービス
[準備が完了している AWS のサービス] の表示があるサービス

AWS Marketplace サービス
AWS Marketplace を通じて購入したサービス

その他のエンドポイントサービス
サービス名で共有されているサービスを検索

サービス (1/3)
サービスのフィルター
サービス名: com.amazonaws.us-west-2.s3 X フィルターをクリア

サービス名	所有者	タイプ
com.amazonaws.us-west-2.s3	amazon	Interface
com.amazonaws.us-west-2.s3	amazon	Gateway
com.amazonaws.us-west-2.s3-outposts	amazon	Interface

VPC
エンドポイントを作成する VPC を選択

VPC
エンドポイントを作成する VPC。
vpc-

▶ 追加設定

サブネット (4/4) 情報

アベイラビリティーゾーン	サブネット ID
us-west-2a (usw2-az2)	subnet-[REDACTED]
us-west-2b (usw2-az1)	subnet-[REDACTED]
us-west-2c (usw2-az3)	subnet-[REDACTED]
us-west-2d (usw2-az4)	subnet-[REDACTED]

IP アドレスタイプ
 IPv4
 IPv6
 デュアルスタック

インターフェイスエンドポイントの作成 2

セキュリティグループ (1/4) 情報

セキュリティグループのフィルター

グループ ID	グループ名	VPC ID
sg-[REDACTED]	[REDACTED]	vpc-[REDACTED]
sg-[REDACTED]	[REDACTED]	vpc-[REDACTED]
sg-[REDACTED]	[REDACTED]	vpc-[REDACTED]
<input checked="" type="checkbox"/> sg-[REDACTED]	[REDACTED]	vpc-[REDACTED]

sg-[REDACTED]

タグ

キー	値 - オプション
Name	pl-for-s3-bb

新しいタグを追加

さらに 49 個の タグ を追加できます。

キャンセル エンドポイントを作成

ポリシー 情報

VPC エンドポイントポリシーはサービスへのアクセスを管理します。

フルアクセス

VPC 内のユーザーまたはサービスが、Amazon ウェブ サービスのアカウントの認証情報を使用して、このAmazon ウェブ サービスのサービスの任意のリソースにアクセスすることを許可します。すべてのポリシー (IAM ユーザーポリシー、VPC エンドポイントポリシー、および Amazon ウェブ サービスのサービス固有のポリシー (Amazon S3 バケットポリシー、S3 ACL ポリシーなど)) は、正常にアクセスするために必要な許可を付与する必要があります。

カスタム

[ポリシー作成ツール](#)を使用してポリシーを生成し、作成されたポリシーを以下に貼り付けてください。

インターフェイスエンドポイントの作成 3

Name	VPC エンドポイント ID	VPC ID	サービス名	エンドポイントタイプ	ステータス
pl-for-s3-bb	vpce-[REDACTED]	vpc-[REDACTED]	com.amazonaws.us-west-2.s3	Interface	使用可能

エンドポイント ID: vpce-[REDACTED]
VPC ID: vpc-[REDACTED]
DNS レコードの IP タイプ: ipv4
IP アドレスタイプ: ipv4

5つの DNS 名が作成※
リージョナル DNS
AZ 障害発生時も耐障害性を高めることができる

ゾーナル DNS
特定の AZ に接続したい場合に利用できる

ステータス: 使用可能
ステータスマッセージ: -
作成時刻: 2022年10月19日水曜日 10:55:09 JST
サービス名: com.amazonaws.us-west-2.s3
DNS 名:

- *.vpce-[REDACTED].s3.us-west-2.vpce.amazonaws.com
- ([REDACTED])
- *.vpce-[REDACTED]-us-west-2b.s3.us-west-2.vpce.amazonaws.com
- ([REDACTED])
- *.vpce-[REDACTED]-us-west-2d.s3.us-west-2.vpce.amazonaws.com
- ([REDACTED])
- *.vpce-[REDACTED]-us-west-2a.s3.us-west-2.vpce.amazonaws.com
- ([REDACTED])
- *.vpce-[REDACTED]-us-west-2c.s3.us-west-2.vpce.amazonaws.com
- ([REDACTED])

エンドポイントタイプ: Interface
プライベート DNS 名が有効になっています
いいえ

※ 選択したサブネット数（ゾーナル DNS）プラス 1 つ（リージョナル DNS）となる

インターフェイスエンドポイントに関する注意点

- ・ インターフェイスエンドポイントを利用して S3 へアクセスする場合には、エンドポイントが作成した DNS 名を使用しなければならない
- ・ オンプレミスや別のリージョンの VPC など様々な場所からアクセスが可能であるため、セキュリティグループの設定に注意する

Amazon S3 におけるログ監査

Amazon S3 におけるログ概要

ログで押さえておくべきサービス

- AWS CloudTrail
 - API コールを記録
- S3 サーバーアクセスログ

AWS CloudTrail の注意点

管理イベント

- ・ リソース自体に対してなされる管理オペレーション
- ・ S3 のバケットを作成などをとらえる

データイベント

- ・ リソース内部で実行されたオペレーション
- ・ S3 のバケット内部のオブジェクトを作成/削除する

CloudTrail を有効化しただけでは、管理イベントのみ記録される。データイベントであるオブジェクトの削除などは検知できない

データイベントの有効化 1

The screenshot shows the AWS CloudTrail Dashboard. At the top left, it says "CloudTrail > ダッシュボード". Below that, the title "ダッシュボード" has a "情報" link. On the left, there's a sidebar with "証跡" and "情報" tabs, and a "名前" field containing "CloudTrailAudit" with an orange arrow pointing to it. To the right of the sidebar are buttons for "ステータス" and "ログ記録" (with a green checkmark icon), and a "証跡の作成" button. The main area is titled "データイベント" and contains the message "この証跡に対してデータイベント収集が設定されていません". On the far right, there's an "編集" button with an orange border.

A modal dialog box is open, titled "イベント 情報". It says "個々のリソース、または AWS アカウントの現在および将来のすべてのリソースの API アクティビティを記録します。追加料金が適用されます" with a link icon. Below this, it says "イベントタイプ" and "ログ記録するイベントのタイプを選択します。". A checkbox labeled "データイベント" is checked, with an orange arrow pointing to it. The description below says "リソース上またはリソース内で実行されたリソース操作をログに記録します。". At the bottom right of the dialog are "キャンセル" and "変更の保存" buttons.

データイベントの有効化 2

データイベント 情報
追加料金が適用されます データイベントは、リソース上またはリソース内で実行されたリソースオペレーションについての情報を表示します。

基本イベントセレクタは有効になっています
証跡でキャプチャされたデータイベントをきめ細かく制御には、高度なデータイベントセレクターに切り替えます。

データイベント: S3 情報

削除

データイベントソース
ログ記録するデータイベントのソースを選択

S3

S3 バケット
すべてのバケットの読み取り/書き込みイベントをログに記録することを選択できます。また、個々のバケットを選択することもできます。

現在および将来のすべての S3 バケット 読み取り 書き込み

個々のバケットの選択
[参照] を選択して複数のバケットを選択し、選択したすべてのバケットで [読み取り]、[書き込み]、または両方のイベントタイプを記録することを選択します。

shinya-sato-bb 参照 読み取り 書き込み

バケットの追加 GET/LIST PUT/DELETE

データイベントタイプの追加

キャンセル 変更の保存

特定のバケットのみ監査する場合

ファイルとフォルダ (1 合計, 0 B)
このテーブル内のすべてのファイルとフォルダがアップロードされます。

削除 ファイルを追加 フォルダの追加

名前で検索 < 1 >

名前	フォルダ	タイプ	サイズ
dummy.txt	-	text/plain	0 B

送信先 アップロード

送信先
s3://shinya-sato-bb

▶ 送信先の詳細
指定された宛先に保存された新しいオブジェクトに影響するパケット設定。

▶ アクセス許可
他の AWS アカウントへのパブリックアクセスとアクセス権を付与します。

▶ プロパティ
ストレージクラス、暗号化設定、タグなどを指定します。

キャンセル アップロード

オブジェクトのアップロードを検知

CloudTrail による記録の例

```
eventTime: "2022-11-16T08:34:49Z"
eventSource: "s3.amazonaws.com" PutObject を検知
eventName: "PutObject"
awsRegion: "us-west-2"
sourceIPAddress: "205.251.233.55" Source IP
▼ userAgent:
  ...
▼ requestParameters:
  X-Amz-Date: "20221116T083449Z" バケット名
  bucketName: "shinya-sato-bb"
  X-Amz-Algorithm: "AWS4-HMAC-SHA256"
  x-amz-acl: "bucket-owner-full-control"
  ▼ X-Amz-SignedHeaders:
    Host: "shinya-sato-bb.s3.us-west-2.amazonaws.com"
    X-Amz-Expires: "300"
    key: "dummy.txt" オブジェクト名
    x-amz-storage-class: "STANDARD"
  responseElements: null
```

S3 サーバーアクセスログ

バケットに対するリクエストの詳細を記録し、ログをターゲットバケットへ配信する
アクセス特性を理解するために利用できる

- ・ ソースバケットの所有者の正規ユーザー ID
- ・ リクエストを処理するバケット名
- ・ リクエストの時間

などを記録、詳細は下記リンク

https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/LogFormat.html

複数のソースバケットを同じターゲットバケットへ
配信することもできる。その場合、ログオブジェクト
はソースバケットごとに生成。



S3 サーバーアクセスログの注意点 1

- ソースバケットとターゲットバケットは同じリージョン/アカウント
 - ソースとターゲットを同じバケットを指定できるが、ロギングに関する追加のログも発生
- S3 のコンソール上でサーバーアクセスログを有効化すると、ターゲットのバケットポリシーは自動的に更新される



S3 サーバーアクセスログの注意点 2

- サーバーアクセスログの用途はバケットに対するトラフィックの特性を理解することで、ログの配信は**ベストエフォート型**となる
 - リアルタイム配信は約束されない
 - 全てのリクエストが完全に記録される訳ではない
- サーバーアクセスログを有効後、しばらくはリクエストが記録されないことがある

まとめ



まとめ

- Amazon S3 は高い耐久性/低コスト/セキュアなオブジェクトストレージ
- アップロードされるデータはデフォルトで暗号化される
 - 別途、クライアントサイドで暗号化してアップロードすることもできる
 - AWS KMS へのリクエストが多い場合には、バケットキーを利用する
- 厳格なアクセス制御をおこなう
 - ブロックパブリックアクセスを設定する
 - バケット/IAM ポリシーを利用し、バケット内部のオブジェクトへのアクセス制御をおこなう
 - ACL は無効化する
- アクセスポイントや VPC エンドポイントを利用してすることで、特定のアプリケーション向けのネットワークエンドポイントや AWS 内部にトラフィックを閉じた形でのアクセスが可能となる
- AWS CloudTrail での API コールの記録し、S3 サーバーアクセスログを用いてトラフィックを監視する

本資料に関するお問い合わせ・ご感想

技術的な内容に関しましては、有料のAWSサポート窓口へ
お問い合わせください

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

料金面でのお問い合わせに関しましては、カスタマーサポート窓口へ
お問い合わせください（マネジメントコンソールへのログインが必要です）

<https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service>

具体的な案件に対する構成相談は、後述する個別相談会をご活用ください



ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt



その他コンテンツのご紹介

ウェビナーなど、AWSのイベントスケジュールをご参照いただけます

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

ハンズオンコンテンツ

<https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/>

AWS 個別相談会

AWSのソリューションアーキテクトと直接会話いただけます

<https://pages.awscloud.com/JAPAN-event-SP-Weekly-Sales-Consulting-Seminar-2021-reg-event.html>



Thank you!



AWS Black Belt Online Seminar

AWS SAW

セルフサービスなトラブルシューティング

Amazon Simple Storage Service (Amazon S3) + AWS Lambda 編

石川 直哉 / 藤原 弘樹

Cloud Support Engineer
2024/03

AWS Black Belt Online Seminar とは

- ・ 「サービス別」「ソリューション別」「業種別」などのテーマに分け、
アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- ・ AWS の技術担当者が、AWS の各サービスやソリューションについてテーマごとに動画を公開します
- ・ 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
 - ・ <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>
 - ・ <https://www.youtube.com/playlist?list=PLzWGOASvSx6FlwIC2X1nObr1KcMCBBlqY>



ご感想は X (Twitter) へ！ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- ・ 本資料では 2024 年 2 月時点のサービス内容および価格についてご説明しています。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (<https://aws.amazon.com/>) にてご確認ください
- ・ 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- ・ 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます
- ・ 技術的な内容に関しましては、有料の [AWS サポート窓口](#)へお問い合わせください
- ・ 料金面でのお問い合わせに関しましては、[カスタマーサポート窓口](#)へお問い合わせください (マネジメントコンソールへのログインが必要です)

本セミナーの概要

- 本セミナーの対象者
 - Amazon S3 や AWS Lambda を利用した運用を実施されている方
 - Amazon S3 や AWS Lambda、Amazon S3 と AWS Lambda を組み合わせて使用する際のトラブルシューティングの効率化に興味のある方
- 本セミナーの Goal
 - Amazon S3、AWS Lambda 向けに利用可能な4つの AWS Support Automation Workflows(SAW) について利用ユースケース及び概要を理解する
- 本セミナーの前提知識
 - AWS Black Belt Online Seminar (Amazon S3) 入門編 ([PDF](#)/[YouTube](#))
 - AWS Black Belt Online Seminar (AWS Lambda) ([PDF](#)/[YouTube](#))
 - AWS Black Belt Online Seminar AWS SAW - セルフサービスなトラブルシューティングと運用の自動化 入門編 ([PDF](#)/[YouTube](#))

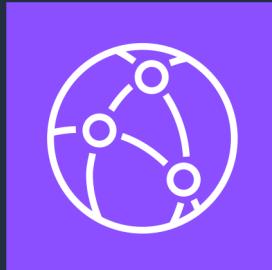
自己紹介

名前：石川 直哉 (Naoya Ishikawa)

所属：アマゾン ウェブ サービス ジャパン合同会社
技術支援本部 クラウドサポートエンジニア



好きな AWS サービス：



Amazon
CloudFront

自己紹介

名前：藤原 弘樹 (Hiroki Fujiwara)

所属：アマゾン ウェブ サービス ジャパン合同会社
技術支援本部 クラウドサポートエンジニア



好きな AWS サービス：



AWS Lambda



AWS IoT Core

アジェンダ

- Amazon S3 のよくあるお問い合わせと SAW の紹介
 - S3 バケットへのパブリックアクセスが許可されているかを判定する
 - AWSSupport-TroubleshootS3PublicRead
 - S3 バケットに対して、同一アカウントの IAM ユーザー/ロールがアクセスを行うことができるかを判定する
 - AWSSupport-TroubleshootS3AccessSameAccount
 - S3 イベントに指定した AWS Lambda 関数がトリガーされない原因を特定・修正する
 - AWSSupport-RemediateLambdaS3Event
 - VPC に接続した Lambda 関数からインターネットアクセスができない原因を特定する
 - AWSSupport-TroubleshootLambdaInternetAccess
- まとめ

Amazon S3 と AWS Lambda の よくあるお問い合わせと SAW の紹介

Amazon S3 と AWS Lambda でよくあるお問い合わせ

- 機能について
 - Amazon S3 の各種機能、ストレージクラス、ライフサイクルルール、レプリケーション、オブジェクトロック、S3イベントなどについてのお問い合わせ
- トラブルシューティング
 - Amazon S3 へのリクエスト 403 (AccessDenied) が発生する
 - S3 イベントに指定した AWS Lambda 関数がトリガーされない
 - VPC 接続した Lambda 関数からインターネット経由のアクセスができない

Amazon S3 と AWS Lambda でよくあるお問い合わせ

- 機能について
 - Amazon S3 の各種機能、ストレージクラス、ライフサイクル、オブジェクトロック、S3イベントなどについての SAW によって解析や関連情報収集ができる範囲
- トラブルシューティング
 - Amazon S3 へのリクエスト 403 (AccessDenied) が発生する
 - S3 イベントに指定した AWS Lambda 関数がトリガーされない
 - VPC 接続した Lambda 関数からインターネット経由のアクセスができない

Amazon S3 と AWS Lambdaで利用可能な SAW(ランブック)

名称	概要
AWSSupport-TroubleshootS3PublicRead	S3 バケットへのパブリックアクセスが許可されているかを判定する
AWSSupport-TroubleshootS3AccessSameAccount	S3 バケットに対して、同一アカウントの IAM ユーザー/ロールがアクセスを行うことができるかを判定する
AWSSupport-RemediateLambdaS3Event	S3 イベントに指定した AWS Lambda 関数がトリガーされない原因を特定・修正
AWSSupport-TroubleshootLambdaInternetAccess	VPC に接続した Lambda 関数からインターネットアクセスができない原因を特定する

*パブリック：アクセス許可の対象を IAM ユーザー/ロールや AWS プリンシパル、特定の IP アドレス等に限定していない状態。

AWS Support - Troubleshoot S3 Public Read



© 2024, Amazon Web Services, Inc. or its affiliates.



AWSSupport-TroubleshootS3PublicRead

- 利用ユースケース
 - S3 バケットに対するパブリックアクセスが可能かを確認したいとき
 - 具体例
 - S3 バケット内のオブジェクトを公開したい
 - オブジェクト URL を使用した S3 バケット内のオブジェクトへのアクセスに失敗する
 - 403 エラー (Access Denied) が発生

AWSSupport-TroubleshootS3PublicRead

- SAW(ランブック)が確認するポイント
 - バケットポリシーが設定されているか
 - バケットポリシーでパブリックアクセスが許可されているか
 - ACL でパブリックアクセスが許可されているか
 - バケットレベルのブロックパブリックアクセス設定
 - アカウントレベルのブロックパブリックアクセス設定

SAW(ランブック)入力パラメーター (1/3)

- `AutomationAssumeRole` : 操作しているユーザとは別にランブックのアクションを実行する IAM ロールを指定したい場合に使用
- `S3BucketName`(必須) : S3 バケット名
- `S3PrefixName` : プレフィックス
- `StartAfter` : オブジェクトの分析を開始するオブジェクトキー名
- `MaxObjects`(必須) : 分析対象とするオブジェクトの数 (デフォルト 5 個で 1 - 25 個を指定可能)
- `IgnoreBlockPublicAccess`(必須) : 対象 S3 バケットのパブリックアクセスブロック設定を無視するかどうか

SAW(ランブック)入力パラメーター (2/3)

- `HttpGet`(必須) : Range リクエストを行なって最初のバイトのみを返すかどうか
- `Verbose` (必須) : Warning や Error メッセージ以外の詳細な情報を返すかどうか
- `CloudWatchLogGroupName` : 出力を送信するロググループ
- `CloudWatchLogStreamName` : 出力を送信するログストリーム
- `ResourcePartition` (必須) : S3 バケットのあるパーティション
`aws/aws-us-gov/aws-cn`

SAW(ランブック)入力パラメーター (3/3)

- 赤枠の項目が必須パラメーター

Input parameters

AutomationAssumeRole
(Optional) The ARN of the role that allows Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses your IAM permissions to execute this document.

S3PrefixName
(Optional) Specify the prefix or name of the object key(s) residing in your Amazon S3 bucket. E.g: keyname, key*, level1/, or level1/keyname.

MaxObjects
Maximum number of objects returned for analysis (between 1 and 25).

HttpGet
Specify if you want the automation document to perform a partial HTTP GET request of the object. The document only retrieves the first 100 bytes using the Range HTTP header.

CloudWatchLogGroupName
(Optional) CloudWatch Log Group Name you want to send the analysis result and log data. If you specify a name and it does not exist, the SSM Automation document will try to create it on your behalf.

ResourcePartition
(Required) The partition in which the S3 bucket is located. The partition is used for the bucket policy simulation.

S3BucketName
(Required) Specify the name of your Amazon S3 bucket.

StartAfter
(Optional) StartAfter is the key name where you want the document to start listing from. StartAfter can be any key in the bucket.

IgnoreBlockPublicAccess
Specify if you want to ignore the account and bucket block public access settings. Changing this option is not recommended. Changing this option to 'true', causes the document analysis to not consider public access settings that might be blocking public read access to your objects.

Verbose
Specify if you want to see detailed information during the analysis or only warning and error messages.

CloudWatchLogStreamName
(Optional) CloudWatch Log Stream Name you want to send the analysis result and log data. If does not exist, the SSM Automation document will try to create it on your behalf. If you leave this input parameter empty, the document will use the SSM Automation execution Id as the name.

SAW(ランブック)実行例1

- 状況
 - バケットポリシー/ACL: パブリックアクセスを許可
 - バケット・アカウントレベルのロックパブリックアクセス設定: オフ



SAW(ランブック)実行例1

▼ 出力

AnalyzeObjects.bucket

AnalyzeObjects.objects

[info] [I09] HTTP GET request status:206, reason:Partial Content.

[info] [I09] HTTP GET request status:206, reason:Partial Content.

[info] [I09] HTTP GET request status:206, reason:Partial Content.

[info] [I09] HTTP GET request status:206, reason:Partial Content.

[info] [I09] HTTP GET request status:206, reason:Partial Content.

実行ステータス

全体的なステータス	実行されたすべてのステップ	# 成功
④ 成功	11	11
# 失敗	# キャンセル済み	# TimedOut
0	0	0

実行されたステップ (11)

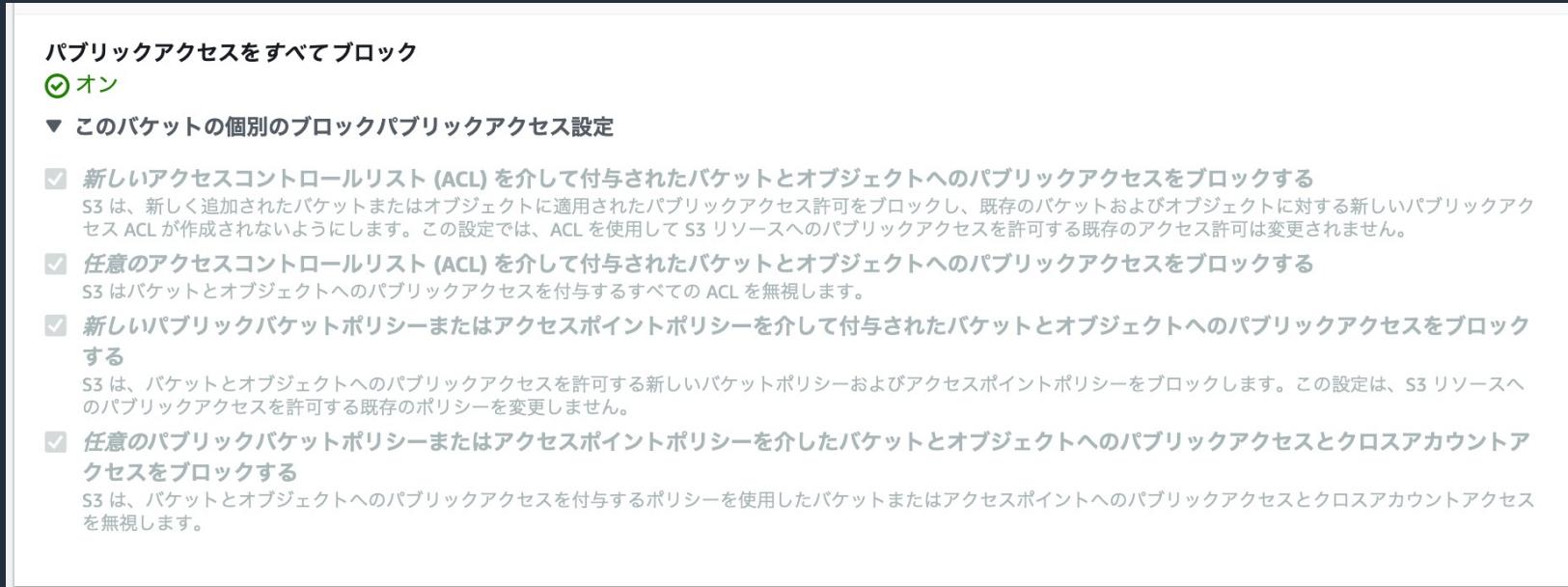
Find Steps < 1 2 >

ステップ ID	ステップ番号	ステップ名	アクション	ステータス
1	TestBucketAccess	aws:assertAwsResourceProperty	④ 成功	
2	GetBucketInformation	aws:executeScript	④ 成功	
3	GetBlockPublicAccess	aws:executeScript	④ 成功	
4	CheckBucketPayer	aws:assertAwsResourceProperty	④ 成功	
5	GetBucketPolicyStatus	aws:executeScript	④ 成功	
6	GetBucketPolicy	aws:executeAwsApi	④ 成功	
7	GetContextKeys	aws:executeAwsApi	④ 成功	
8	SimulateBucketPolicy	aws:assertAwsResourceProperty	④ 成功	
9	GetBucketAcl	aws:executeAwsApi	④ 成功	
10	CreateLogandStream	aws:executeScript	④ 成功	

SAW(ランブック)実行例2

- 状況

- バケットポリシー/ACL : パブリックアクセスを許可
- バケット・アカウントレベルのロックパブリックアクセス設定 : オン



SAW(ランブック)実行例2

▼ 出力

AnalyzeObjects.objects

-

AnalyzeObjects.bucket

[warn] [W13] S3 bucket block public access settings are configured to ignore public ACLs.
[warn] [W14] S3 bucket block public access settings are configured to ignore any public bucket policy.
[error] [E01] S3 bucket or account block public access settings are configured to ignore public ACLs and any public bucket policy.

(参考訳) S3 バケットまたはアカウントブロックのパブリックアクセス設定は、パブリック ACL とパブリックバケットポリシーを無視するように設定されています。

実行ステータス

全体的なステータス 実行されたすべてのステップ
④ 成功 11

失敗 # キャンセル済み
1 0

実行されたステップ (11)

ステップ ID	ステップ番号	ステップ名	アクション	ステータス
1	TestBucketAccess	aws:assertAwsResourceProperty	④ 成功	
2	GetBucketInformation	aws:executeScript	④ 成功	
3	GetBlockPublicAccess	aws:executeScript	④ 失敗	
4	CheckBucketPayer	aws:assertAwsResourceProperty	④ 成功	
5	GetBucketPolicyStatus	aws:executeScript	④ 成功	
6	GetBucketPolicy	aws:executeAwsApi	④ 成功	
7	GetContextKeys	aws:executeAwsApi	④ 成功	
8	SimulateBucketPolicy	aws:assertAwsResourceProperty	④ 成功	
9	GetBucketAcl	aws:executeAwsApi	④ 成功	
10	CreateLogandStream	aws:executeScript	④ 成功	

SAW(ランブック)実行例2

オートメーションステップ3: GetBlockPublicAccess

ステータス ✖ 失敗	アクション aws:executeScript	開始時刻 [遮蔽]	終了時刻 [遮蔽]
ステップ実行 ID [遮蔽]	onFailure Continue	最大試行数 -	(参考訳) 例外: パブリックアクセス設定は、パブリック ACL とパブリックバケットポリシーの両方を無視するように設定されています。

▶ 入力パラメータ

出力

OutputPayload
[]

失敗の詳細

✖ 失敗メッセージ
Step fails when it is Poll action or Lambda function execution. Exception: Public access settings are configured to ignore both public ACLs and any public bucket policy. For more information about this exception, see the Troubleshooting Guide for more diagnosis details.

FailureType
Verification

FailureStage
PostVerification

VerificationErrorMessage
Exception: Public access settings are configured to ignore both public ACLs and any public bucket policy.
Exception - Public access settings are configured to ignore both public ACLs and any public bucket policy.

その他

- 留意点
 - 対象リソースとしては S3 バケット名を入力
 - ARN 形式ではない

AWS Support - Troubleshoot S3 Access Same Account

AWS Support - Troubleshoot S3 Access Same Account

- 利用ユースケース
 - 同一アカウントの IAM ユーザー/ロールで S3 に対するアクションが拒否される場合
 - 具体例
 - IAM ユーザーに対して IAM ポリシーで GetObject 権限を付与したが、S3 オブジェクトのダウンロードに失敗する
 - バケットポリシーに変更を加えたところ、以前はできていた操作ができなくなった

AWS Support - Troubleshoot S3 Access Same Account

- SAW(ランブック)が確認するポイント
 - IAM ユーザー/ロールが持つ権限
 - S3 バケットの ACL 設定
 - 対象リソースの暗号化設定
 - バケットポリシー
 - VPC エンドポイントポリシー
 - KMS キーのキーポリシー
 - サービスコントロールポリシー (SCP)

SAW(ランブック)入力パラメーター (1/3)

- AutomationAssumeRole : ランブックのアクションを実行する IAM ロール
- S3ResourceArn(必須) : 対象の S3 リソース (バケット/オブジェクト) の ARN
- S3Action(必須) : 評価の対象とする S3 アクション
- RequesterArn(必須) : アクセス権の有無を確認したい IAM ユーザー/ロールの ARN
- RequesterRoleSessionName : RequesterArn にて IAM ロールを指定した際に、ロールを引き受ける際のセッション名

SAW(ランブック)入力パラメーター (2/3)

- S3ObjectVersionId : S3 オブジェクトのバージョン ID
- KmsKeyArn : 対象リソースの暗号化に使用している KMS キーの ARN
- VpcEndpointId : VPC エンドポイントの ID
- ContextKeyList : 評価において必要な条件キーとそれに対する値
- SCPPolicy : AWS Organizations にて設定されている SCP

SAW(ランブック)入力パラメーター (3/3)

- 赤枠の項目が必須パラメーター

Input parameters	
AutomationAssumeRole (Optional) The ARN of the role that allows the Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses your user context IAM permissions to run this document.	S3ResourceArn (Required) The ARN of your Amazon S3 resource (bucket or key). For object operations such as PutObject or GetObject, please provide the ARN of the object. Example: arn:aws:s3:::bucket_name, or arn:aws:s3:::bucket_name/key_name.
S3Action (Required) The S3 Action for which you want the runbook to evaluate the access context for. Make sure you provide the corresponding S3 resource type (bucket or object) for the specific action.	String
RequesterRoleSessionName (Optional) The session name of the assumed role, in case the IAM ARN is a role and you want to provide a specific session name.	RequesterArn (Required) The IAM Principal (user or role) ARN for which you want to find the access level on the specific S3 resource. For example: arn:aws:iam::123456789012:user/user_name or arn:aws:iam::123456789012:role/example-role.
KmsKeyArn (Optional) The KMS Key ARN if it is relevant to the action, example: 'CompleteMultipartUpload','CopyObject','CreateMultipartUpload','PutObject', etc., and the type of resource (bucket or object) for which you want to evaluate the access context.	S3ObjectVersionId (Optional) If the object has multiple versions, this parameter allows you to specify the specific version of the object you want to evaluate the access context.
ContextKeyList (Optional) Condition keys list and corresponding values with respect to the policy evaluation. For example: [{"ContextKeyName":"aws:PrincipalArn","ContextKeyValue":["arn:aws:iam::123456789012:root"]}, {"ContextKeyType":"string"}, {"ContextKeyName":"aws:SourceIp","ContextKeyValue":["54.240.143.0/24"]}, {"ContextKeyType":"ip"}] (Please remove any new lines, tabs, or white spaces when you input a value) For more information please see the context-entries parameter in https://docs.aws.amazon.com/cli/latest/reference/iam/simulate-principal-policy.html	VpcEndpointId (Optional) The virtual private cloud (VPC) endpoint ID related to the access evaluation. Amazon S3 bucket policies can control access to buckets from specific virtual private cloud (VPC) endpoints.
<input type="button" value=""/>	SCPPolicy (Optional) The AWS Organizations Service Control Policy (SCP) in case you want the runbook to evaluate the input against a particular SCP policy. This is not needed and ignored when you run this runbook from the organization's management account. (Please remove any new lines, tabs, or white spaces when you input a value).
	{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action": "*","Resource": "*"}]}

SAW(ランブック)実行例1

- 状況
 - バケットポリシーにて IAM ユーザーからのGetObject/PutObject を許可
 - IAM ユーザーの IAM ポリシーでは S3 に関する記述はなし
 - S3 バケットの ACL は無効
 - S3 バケット内のオブジェクトに対するGetObject に成功するかを評価

SAW(ランブック)実行例1

▼ 出力

```
EvaluatePolicy.denied_statements_array
-
EvaluatePolicy.allowed_statements_array
{
  "Decision": "Bucket Policy",
  "MatchedStatement": {
    "Sid": "Statement1",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::XXXXXXXXXXXX"
      ]
    },
    "Action": [
      "s3:GetObject",
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::"
    ]
  }
}

EvaluatePolicy.final_decision
- allowed for S3 action **The output policy will be similar to a statement in your policy, but may not be exact. Please check the Actions and the Sid of your policy to match the exact statement. The Resource section of the IAM Policy and the Principal & Resource sections of the Resource Policy may be a little differing from the actual statement in the policy.**
```

実行ステータス			
全体的なステータス	実行されたすべてのステップ	# 成功	# 失敗
④ 成功	14	14	# 失敗
			# キャンセル済み
0	0	0	# TimedOut

EvaluatePolicy.final_decision – allowed for S3 action (許可)

SAW(ランブック)実行例2

- 状況
 - バケットポリシーにて IAM ユーザーからのGetObject/PutObject を許可
 - IAM ユーザーの IAM ポリシーで対象リソースに対するアクションを拒否
 - S3 バケットの ACL は無効
 - S3 バケット内のオブジェクトに対するGetObject に成功するかを評価

SAW(ランブック)実行例2

▼ 出力

```
EvaluatePolicy.allowed_statements_array
```

```
{  
  "Decision": "Bucket Policy",  
  "MatchedStatement": {  
    "Sid": "Statement1",  
    "Effect": "Allow",  
    "Principal": {  
      "AWS": [  
        "arn:aws:iam::XXXXXXXXXXXX:  
      ]  
    },  
    "Action": [  
      "s3:GetObject",  
      "s3:PutObject"  
    ],  
    "Resource": [  
      "arn:aws:s3:::  
    ]  
  }  
}
```

```
EvaluatePolicy.denied_statements_array
```

```
{  
  "Decision": "IAM Policy",  
  "MatchedStatement": {  
    "Sid": "Statement1",  
    "Effect": "Deny",  
    "Action": [  
      "s3:*"  
    ],  
    "Resource": [  
      "arn:aws:s3:::  
    ]  
  }  
}
```

```
EvaluatePolicy.final_decision
```

- explicitDeny for S3 action **The output policy will be similar to a statement in your policy, but may not be exact. Please check the Actions and the Sid of your policy to match the exact statement. The Resource section of the IAM Policy and the Principal & Resource sections of the Resource Policy may be a little differing from the actual statement in the policy.**

実行ステータス

全体的なステータス

✓ 成功

実行されたすべてのステップ

14

成功

14

失敗

0

キャンセル済み

0

TimedOut

0

EvaluatePolicy.final_decision - explicitDeny for S3 action
(明示的な拒否)

その他

- 留意点
 - 対象リソースは ARN で入力する必要がある
 - オブジェクトレベルのアクションについて評価を行う場合には、対象リソースもオブジェクトレベルで指定する必要がある
 - `GetObject/PutObject` の評価を行う場合には、S3 オブジェクトの ARN を指定する必要がある

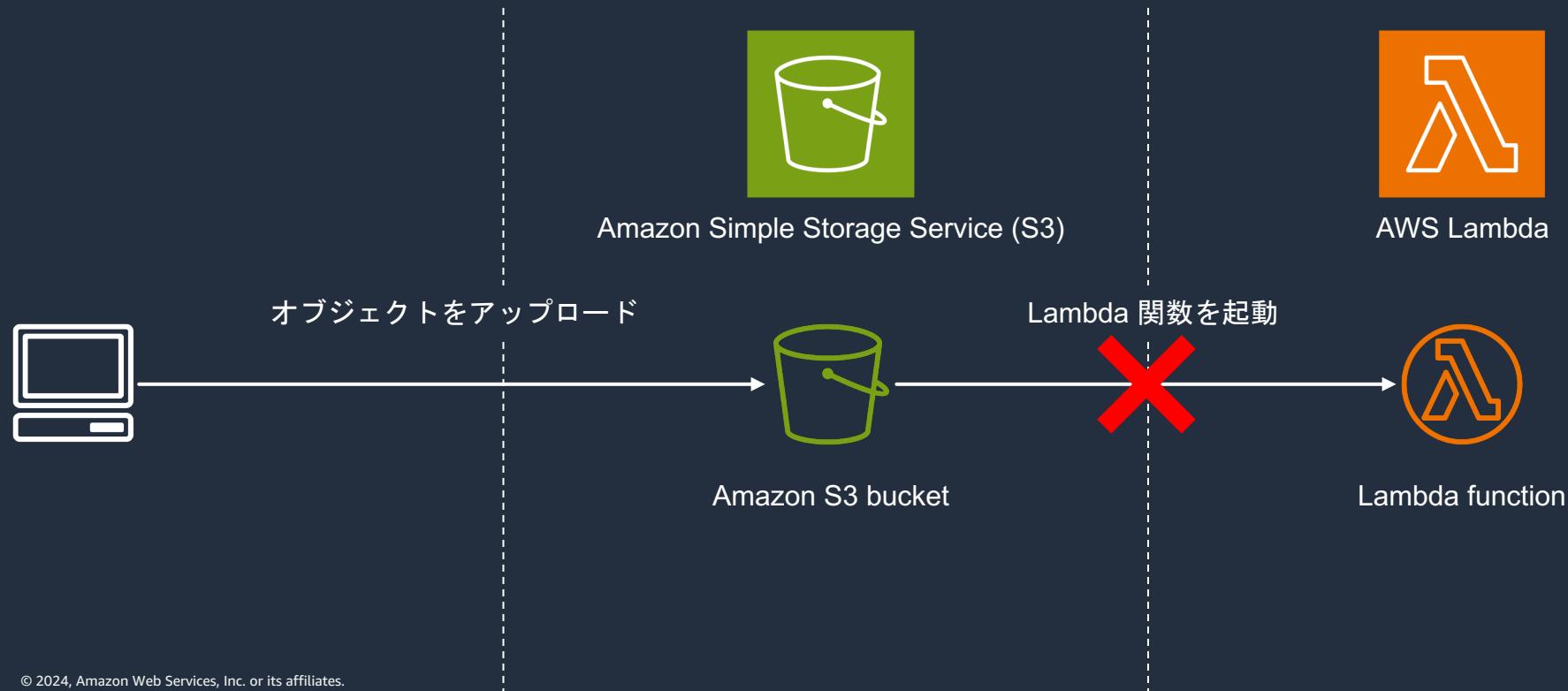
AWSSupport- RemediateLambdaS3Event

AWSSupport-RemediateLambdaS3Event

- 利用ユースケース

- S3 イベントを用いて、Lambda 関数を起動するように設定したが、対象の Lambda 関数が起動しない

S3 イベントを利用した Lambda 関数の起動 (イメージ)



AWSSupport-RemediateLambdaS3Event

- 利用ユースケース

- AWSSupport-RemediateLambdaS3Event ランブックは、AWS ナレッジセンターの記事で説明されている手順を自動化するソリューションを提供します。
 - [Lambda を呼び出すように Amazon S3 イベント通知を設定する | AWS re:Post](#)
 - [Amazon S3 イベント通知を作成する際のエラーのトラブルシューティング | AWS re:Post](#)
- S3 のイベント通知が、設定した Lambda 関数をトリガーできなかつた理由を特定して修正するのに役立ちます。

AWS Support - Remediate Lambda S3 Event

- 問題事象確認方法
 - S3 イベントを設定し、ファイルをバケットにアップロード

The screenshot shows the AWS Lambda console interface. On the left, there's a sidebar with navigation links like 'Lambda Functions', 'AWS Lambda Metrics', 'AWS Lambda Metrics Insights', 'AWS Lambda Metrics Dashboards', and 'AWS Lambda Metrics Data'. The main area displays the 'Event通知 (1)' section. A blue arrow points from the bottom of the sidebar towards the central content area.

Event通知 (1)
バケットで特定のイベントが発生したときに通知を送信します。詳細 [?] 編集 削除 イベント通知を作成

名前	イベントタイプ	フィルター	送信先タイプ	送信先
blackbelt-sample	すべてのオブジェクト作成イベント	-	Lambda 関数	SampleFunction [?]

Amazon EventBridge
追加の機能については、Amazon EventBridge を使用して、S3 イベント通知を使用するイベント駆動型アプリケーションを大規模に構築してください。

このバケット内のすべてのイベントについて Amazon EventBridge に通知を送信する
オフ

アップロード: ステータス

このページから移動すると、以下の情報は利用できなくなります。

概要	成功しました	失敗
送信先	成功しました 1 ファイル, 5.0 B (100.00%)	失敗 0 個のファイル, 0 B (0%)

ファイルとフォルダ (1 合計: 5.0 B)

名前	フォルダ	タイプ	サイズ	ステータス	エラー
sample.txt	-	text/plain	5.0 B	成功しました	-

AWSSupport-RemediateLambdaS3Event

- 問題事象確認方法
 - 設定したイベントタイプに該当する操作を行ったにも関わらず、Lambda 関数が呼び出されていない
 - 対象の Lambda 関数のログ出力がない
 - Invoke メトリクスが記録されない

The screenshot shows the AWS CloudWatch Log Groups interface. At the top, there is an orange header bar with the message: "ロググループが存在しません" (The specified log group does not exist) and "特定のロググループ: /aws/lambda/SampleFunction はこのアカウントまたはリージョンに存在しません。" (The specific log group /aws/lambda/SampleFunction does not exist in this account or region). Below the header, the URL is shown as "CloudWatch > ロググループ > /aws/lambda/SampleFunction". The main content area has a title "aws/lambda/SampleFunction" and a section titled "ロググループの詳細". This section contains the following details:

ARN	保存されているバイト数	寄稿者インサイトのルール
arn:aws:logs:ap-northeast-1:123456789012:log-group:/aws/lambda/SampleFunction*	-	-
Account	メトリクスフィルター	KMS キー ID
-	-	-
作成時刻	サブスクリプションフィルター	データ保護
-	0	-
保持	機密データの数	データ保護
失効しない	-	-

At the bottom of the page, a footer message reads: "The specified log group does not exist."

AWSSupport-RemediateLambdaS3Event

- SAW(ランブック)が確認するポイント
 - S3 イベントの有無
 - Lambda 関数のリソースベースのポリシー

SAW(ランブック)入力パラメーター

- LambdaFunctionArn (必須)
 - 調査対象の Lambda 関数の ARN
 - S3BucketName (必須)
 - 調査対象の S3 バケット名
 - アクション [Troubleshoot or Remediate] (必須)
 - Troubleshoot: 問題の検出のみを行う
 - Remediate: 問題の修正もを行う
 - AutomationAssumeRole
 - Automation が各種 API を呼び出す際に利用するロール名
 - 必要な権限はドキュメント参照
 - 指定しない場合、ランブックを利用した IAM ユーザーの権限を利用
- https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/automation-awssupport-remediate-lambda3event.html

SAW(ランブック)実行例1 (Lambda関数のポリシー誤りの検出)

- 状況
 - S3 イベントの設定を行い、S3 バケットで対応する操作を行ったが、Lambda 関数が起動しない

SAW(ランブック)実行例1 (Lambda関数のポリシー誤りの検出)

- ・ランブック実行のためのパラメーター指定

入力パラメータ

AutomationAssumeRole	LambdaFunctionArn
Choose IAMRole	Enter Arn of the Lambdafunction in the format - arn:aws:lambda:<aws-region>:<account-id>:function:<functionName>:<version -optional>
S3BucketName	arn:aws:lambda:ap-northeast-1: [REDACTED] :function:SampleFunction
Action	Troubleshoot

検出のみ行う場合は、Action で「Troubleshoot」を選択

SAW(ランブック)実行例1 (Lambda関数のポリシー誤りの検出)

- ・ランブック実行結果
 - Lambda 関数のリソースベースのポリシーに S3 向けの権限が不足している旨が出力される
 - 必要な権限をポリシーに追加するための AWS CLI コマンドも出力される

... Resource policy for the Lambda function with s3 permissions is missing. Please add below Resourcepolicy to lambda using CLI command or alternatively use Lambda console for adding the Resource Policy. Try testing if the s3 trigger works after adding the below policy ...

```
No output available.
```

```
checkoutoutput.Output
S3 events for the event blackbelt-sample and the function SampleFunction are:['s3:ObjectCreated:*'] Event Configuration for the bucket exists Event filters are: blackbelt-sample : [{"Name": "Prefix", "Value": ""}, {"Name": "Suffix", "Value": ""}] No Special Character found in Prefix for the event blackbelt-sample No Special Character found in Suffix for the event blackbelt-sample Resource policy for the Lambda function with s3 permissions is missing. Please add below Resourcepolicy to lambda using CLI command or alternatively use Lambda console for adding the Resource Policy. Try testing if the s3 trigger works after adding the below policy ----- aws lambda add-permission --function-name SampleFunction --action lambda:InvokeFunction --statement-id [REDACTED] _event_permissions_from_aws-support-remediate-lambda-s3-event-sample-bucket_for_SampleFunction --principal s3.amazonaws.com --source-arn arn:aws:s3:::aws-support-remediate-lambda-s3-event-sample-bucket --source-account [REDACTED] -----
```

SAW(ランブック)実行例2 (Lambda関数ポリシーの自動修正)

- 状況
 - S3 イベントの設定を行い、S3 バケットで対応する操作を行ったが、Lambda 関数が起動しない
 - Action 「Troubleshoot」でランブックを実行し、Lambda 関数のリソースベースのポリシーに問題があることが分かった
 - ランブックから、対象の Lambda 関数のリソースベースのポリシーを自動で修正したい

SAW(ランブック)実行例2 (Lambda関数ポリシーの自動修正)

- ・ランブック実行のためのパラメーター指定

入力パラメータ

AutomationAssumeRole	LambdaFunctionArn
Choose IAMRole	Enter Arn of the Lambdafunction in the format - arn:aws:lambda:<aws-region>:<account-id>:function:<functionName>:<version -optional>
S3BucketName	arn:aws:lambda:ap-northeast-1: [REDACTED]:function:SampleFunction
Action	Remediate

修正も行う場合は、Action で「Remediate」を選択

SAW(ランブック)実行例2 (Lambda関数ポリシーの自動修正)

- ・ランブック実行結果
 - 必要な権限が対象の Lambda 関数のリソースポリシーに追加される

▼ 出力

```
checkoutoutput.Output
No output available yet because the step is not successfully executed

remediatelambda3event.output
No Event configuration exists for the mentioned S3 bucket and lambda function Event filters are: No Event Filters as no Event configuration exists Resource policy for the Lambda function with s3 permissions was missing. Added Resourcepolicy to lambda to mitigate the issue.
```



ポリシーステートメントの詳細

Statement ID: [REDACTED]_event_permissions_from_s3-event-sample-bucket_for_SampleFunction

Principal: s3.amazonaws.com

Effect: Allow

Action: lambda:InvokeFunction

Conditions:

```
{
  "StringEquals": {
    "AWS:SourceAccount": "[REDACTED]"
  },
  "ArnLike": {
    "AWS:SourceArn": "arn:aws:s3:::[REDACTED]"
  }
}
```

[編集](#)

[閉じる](#)

© 2024, Amazon Web Services, Inc. or its affiliates.

閉じる

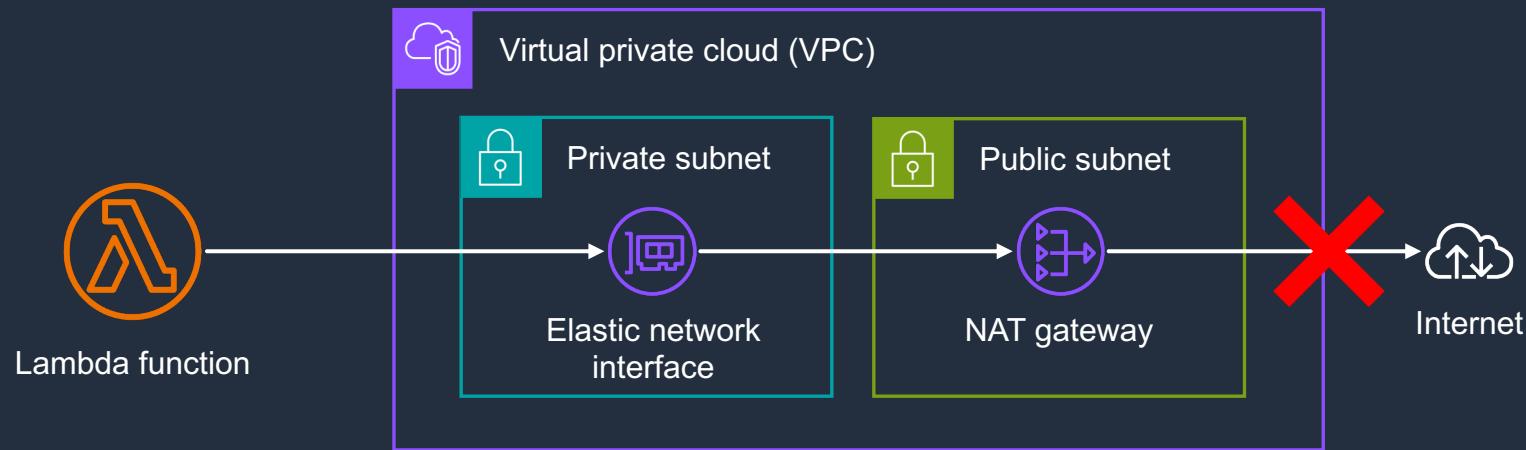
その他

- 留意点
 - S3 イベントの設定内容に起因する問題は範囲外
 - 例えば、下記のパターンは非対応
 - s3:ObjectCreated:CompleteMultipartUpload が指定されておらず、マルチパートアップロードされた場合に Lambda 関数が起動しない
 - S3 イベントでプレフィックスを指定したが、アップロード対象のオブジェクトが該当せず、Lambda 関数が起動しない
 - 例) プレフィックスに .jpg を指定し、example.png がアップロードされた場合

AWS Support - Troubleshoot Lambda Internet Access

AWSSupport-TroubleshootLambdaInternetAccess

- 利用ユースケース
 - VPC に接続された Lambda 関数において、インターネットアクセスができない



AWS Support - Troubleshoot Lambda Internet Access

- 問題事象確認方法
 - インターネット経由で通信を行うコードを VPC に接続した Lambda 関数で実行

```
import requests

def lambda_handler(event, context):
    res = requests.get('https://example.com', timeout=10)
    print(res.status_code)
```

- 設定に問題があり、インターネット経由で `example.com` にアクセスする際

```
START RequestId: 63e269e6-7301-4cc3-8ae3-8caf0a2cec5b Version: $LATEST
[ERROR] ConnectTimeout: HTTPSConnectionPool(host='example.com', port=443): Max retries exceeded with url: / (Caused by ConnectTimeoutError(<urllib3.connection.HTTPConnection to example.com timed out. (connect timeout=10)'))PSConnection object at 0x7fa46bf08150>,
```

AWSSupport-TroubleshootLambdaInternetAccess

- SAW(ランブック)が確認するポイント
 - セキュリティグループ
 - サブネットのネットワークACL
 - サブネットのルートテーブル

SAW(ランブック)入力パラメーター

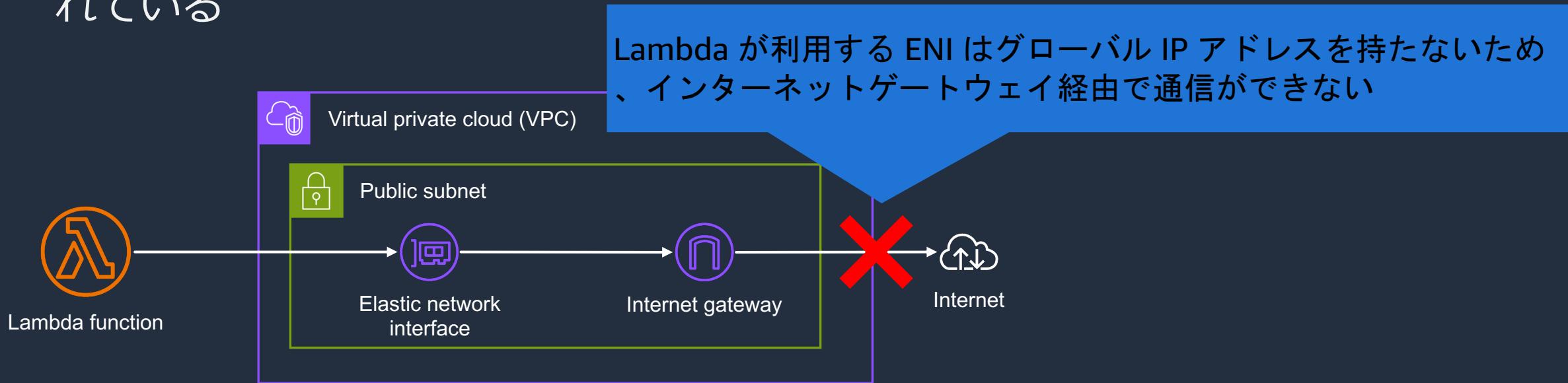
- FunctionName (必須)
 - 調査対象の Lambda 関数名
- destinationIp (必須)
 - Lambda 関数のアクセス先 IP アドレス
- destinationPort
 - Lambda 関数のアクセス先ポート番号
- AutomationAssumeRole
 - 「AWSSupport-RemediateLambdaS3Event」と同様

https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/AWSSupport-TroubleshootLambdaInternetAccess.html



ランブック実行例

- 状況
 - ルートテーブルのデフォルトルートにインターネットゲートウェイが指定されている



送信先	ターゲット
10.0.0.0/1	local
6	
0.0.0.0/0	インターネットGW

ランブック実行例

- ・ランブック実行のためのパラメーター指定

入力パラメータ

AutomationAssumeRole (Optional) The ARN of the role that allows Automation to perform the actions on your behalf. <input type="button" value="Choose IAMRole"/>	FunctionName (Required) The function name whose connectivity needs to be validated. <input type="text" value="VPCLambda"/>
destinationIp (Required) The destination Ip where you want to initiate an outbound internet access. <input type="text" value=""/>	destinationPort (Optional) The destination port where you want to initiate an outbound internet access. <input type="text" value="443"/>

ランブック実行例1 (Lambda関数のポリシー誤りの検出)

- ランブック実行結果

```
▼ 出力

checkVpc.securityGroups
sg-[REDACTED], sg-[REDACTED]

checkVpc.vpc
vpc-[REDACTED]

checkNACL.NACL
[{"subnet-[REDACTED]": {"NACL": "acl-[REDACTED]", "destinationIp_Egress": "Allowed", "destinationIp_Ingress": "Allowed", "Analysis": "This NACL has both Egress and Ingress rule allowing your desired destination IP / destination port"}}

checkSecurityGroups.secgrps
[{"sg-[REDACTED]": {"Status": "Allowed", "Analysis": "This security group has allowed destination IP and port"}, {"sg-[REDACTED]": {"Status": "Allowed", "Analysis": "This security group has allowed destination IP and port in its outbound rule."}}]

checkSubnet.subnets
[{"subnet-[REDACTED]": {"Route": {"DestinationCidrBlock": "0.0.0.0/0", "GatewayId": "igw-[REDACTED]", "Origin": "CreateRoute", "State": "active"}, "Analysis": "This Route Table has an internet gateway route for your destination. However, route should be pointed to NAT gateway. Correct this route entry to NAT gateway.", "RouteTable": "rtb-[REDACTED]"}]

ルートテーブルにインターネットゲートウェイの経路があること、
インターネットゲートウェイではなく、NAT ゲートウェイを利用すべきである点が出力される
```

その他

- 留意点
 - 名前解決に関する問題は範囲外

まとめ

まとめ

- SAW を使うことでお客様自身でトラブルシューティングを行うことができる
 - 自動化された分析によってヒューマンエラーの削減および作業の効率化
 - 問題解決までの時間を削減
- 問題解決しない場合には通常通り、サポートケースを起票いただき、AWS サポートまでお問い合わせください
- SAW を実行しても問題解決しなかった場合、実行頂いた SAW のランブック名、関連する SSM Automation の実行 ID、SAW の実行結果なども通常起票時に必要な情報と併せて記載頂けますと幸いです



Thank you!