



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

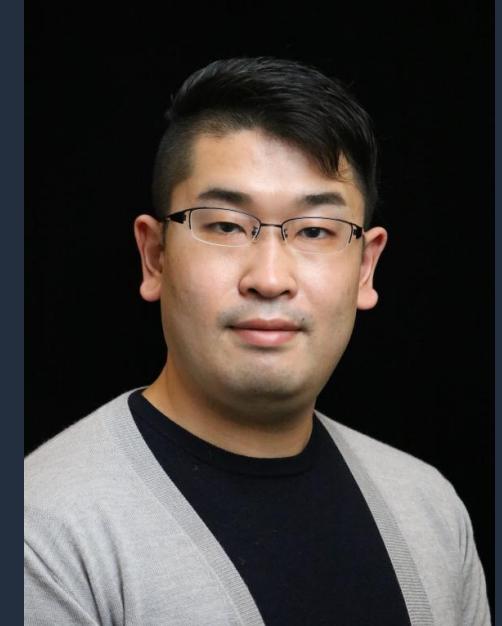
自己紹介

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

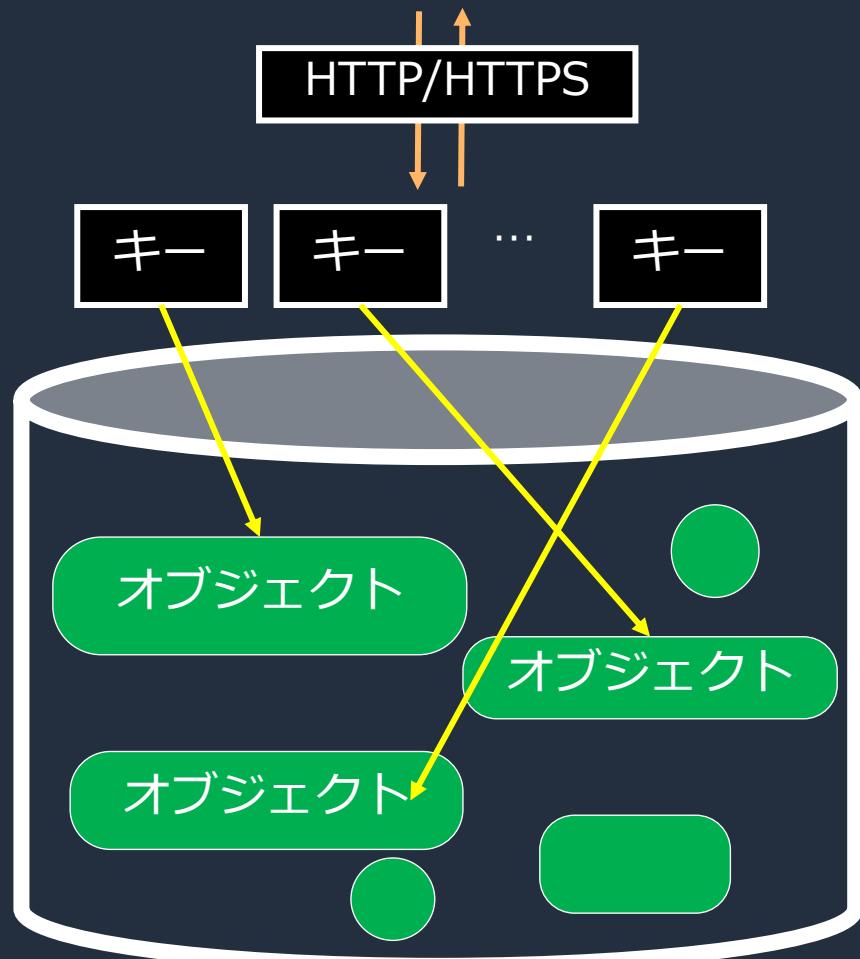
- Amazon S3 のセキュリティについて、特徴や機能を深く知りたい方

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



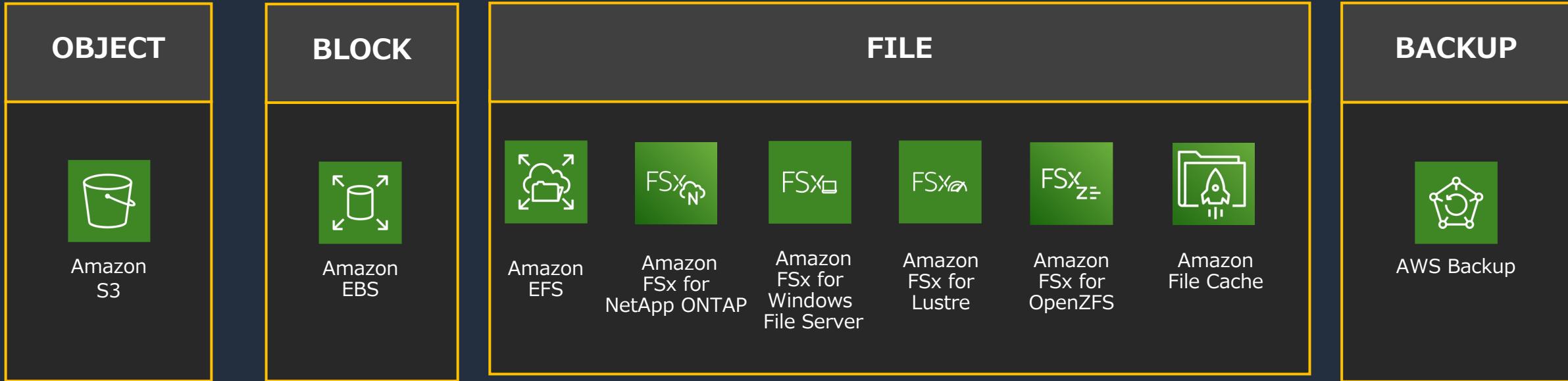
特徴

- 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

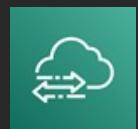
AWS のストレージサービス



DATA TRANSFER AND MIGRATION



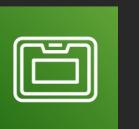
AWS Storage
Gateway



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

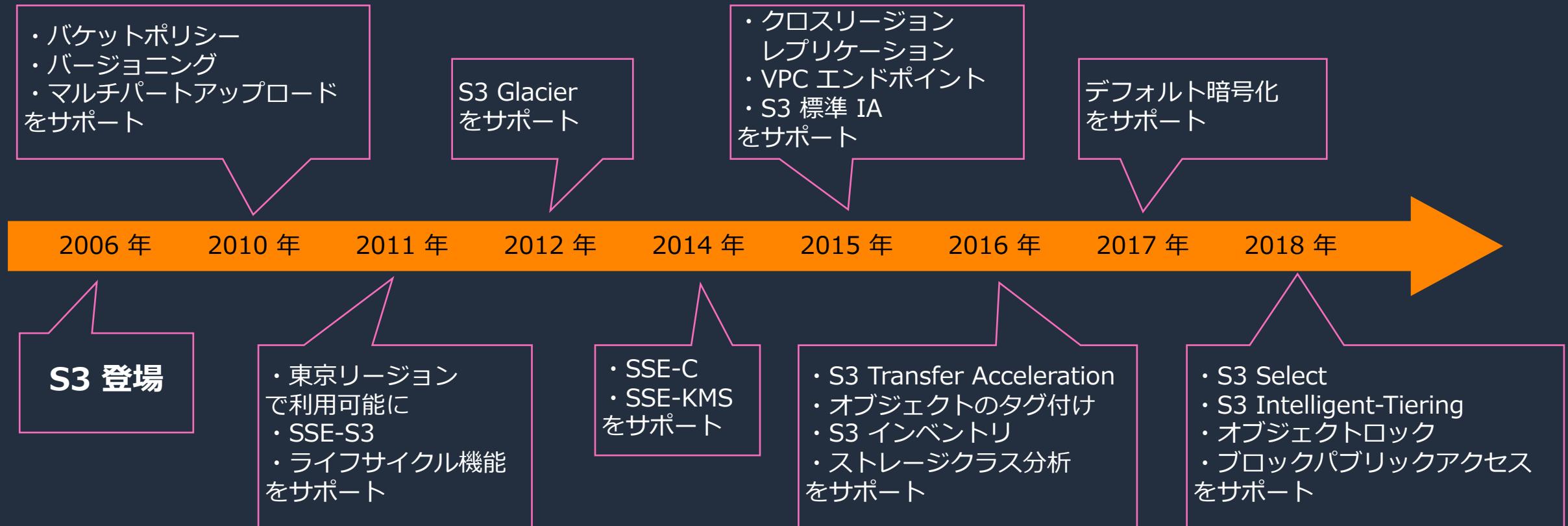


Amazon S3 の特徴などは FAQ にて詳解: <https://aws.amazon.com/jp/s3/faqs/?nc=sn&loc=7>

Amazon S3 の 2018 年までの主要アップデート



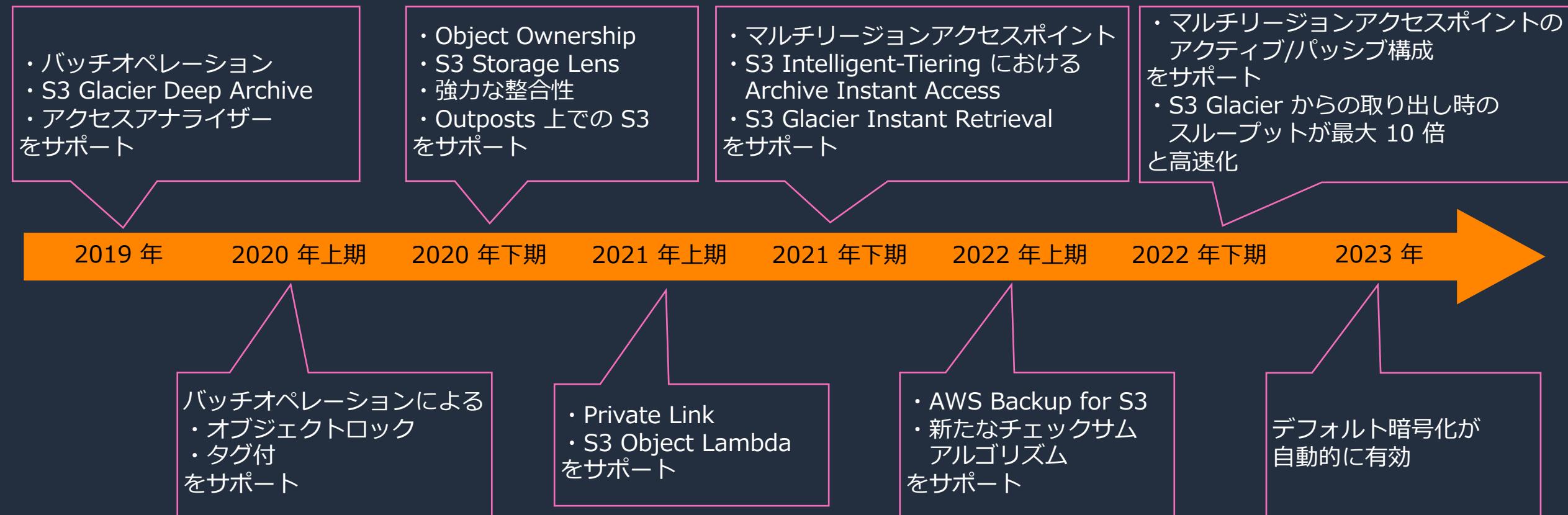
Amazon S3



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

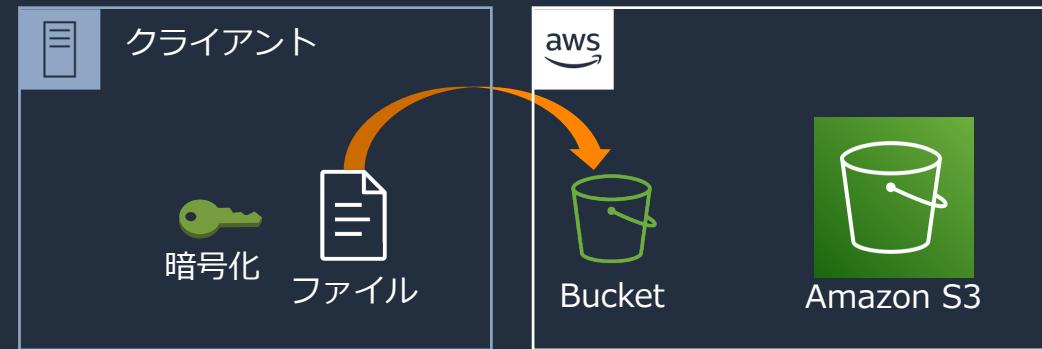
Amazon S3 における データの暗号化



S3 におけるデータ暗号化

1. クライアントサイド暗号化

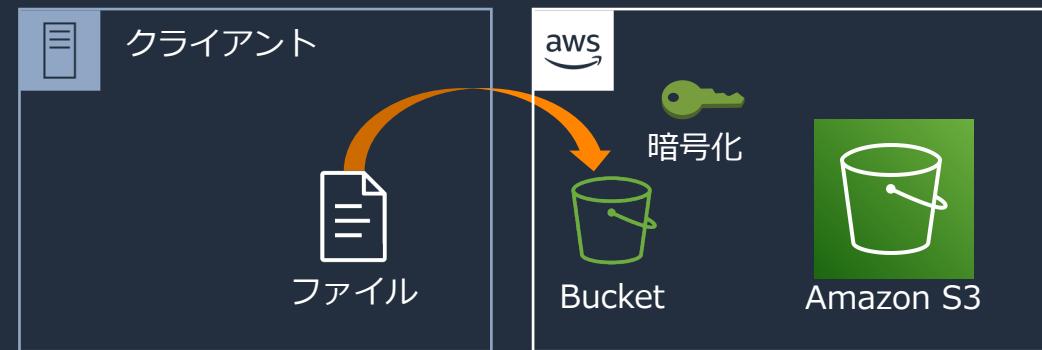
- クライアント側でデータを暗号化し、暗号化したデータを S3 へアップロード



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"  
    }  
  ]  
}
```

A screenshot of a JSON-based AWS bucket policy document. A large pink circle with a diagonal slash is overlaid on the entire policy text, indicating it should not be used.

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"  
                }  
            }  
        }  
    ]  
}
```



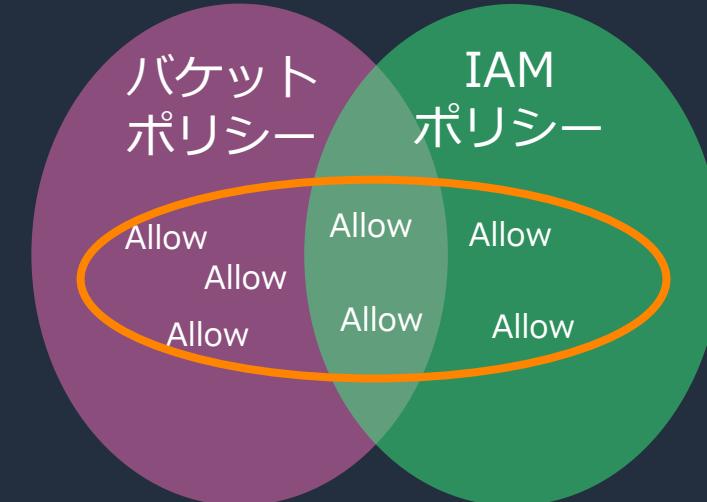
バケットポリシーと IAM ポリシーの関係 1

	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",  
    "s3GetObject",  
    "s3PutObject"  
  ],  
  "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": "s3GetObject",  
      "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

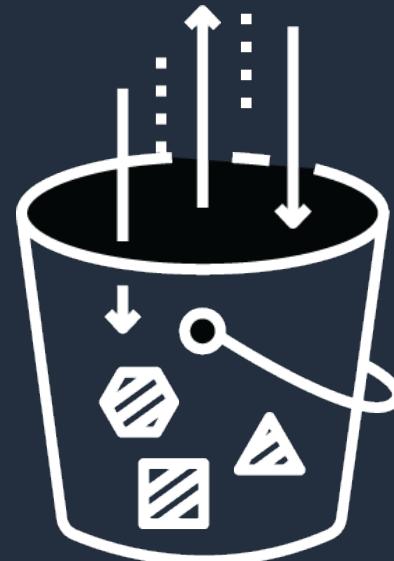
※ S3 Storage Lens の細かい仕様は本資料では解説しない

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" selected under "S3 のアクセスアナライザー". A large orange arrow points from this panel down to the middle panel.
- Middle Panel (S3 のアクセスアナライザー):** Displays the "S3 のアクセスアナライザー" page. It includes a note about the region being used and a call-to-action button "IAM アクセスアナライザーにアクセスしてアナライザーを作成する". A second large orange arrow points from this panel down to the right panel.
- Right Panel (Identity and Access Management (IAM) > Access Analyzer):** Shows the "Access Analyzer" page. It features a title "Access Analyzer リソースへのアクセスをモニタリング", a note for administrators, and three numbered steps: 1. アナライザーを作成 (Create Analyzer), 2. アクティブな結果を確認 (Review active results), and 3. アクションを実行 (Perform actions). The "Access Analyzer" button is highlighted with a blue box and an orange arrow pointing to it.

IAM アクセスアナライザーを有効



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

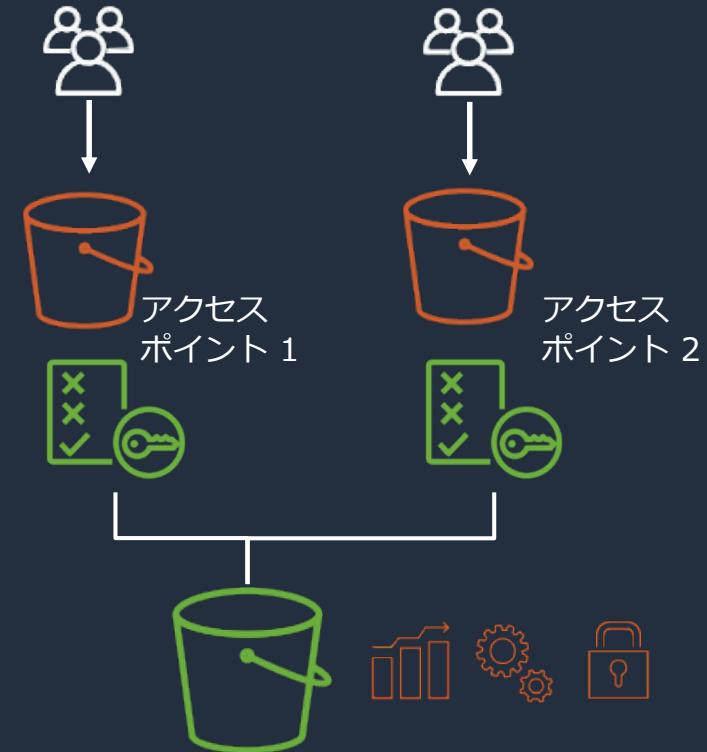
2種類のアクセス方法が選択できる

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)		

At the top, there are buttons for 'Copy Access Point Alias', 'Copy ARN', 'Edit Policy', 'Delete', and 'Create Access Point'. A search bar is also present.

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

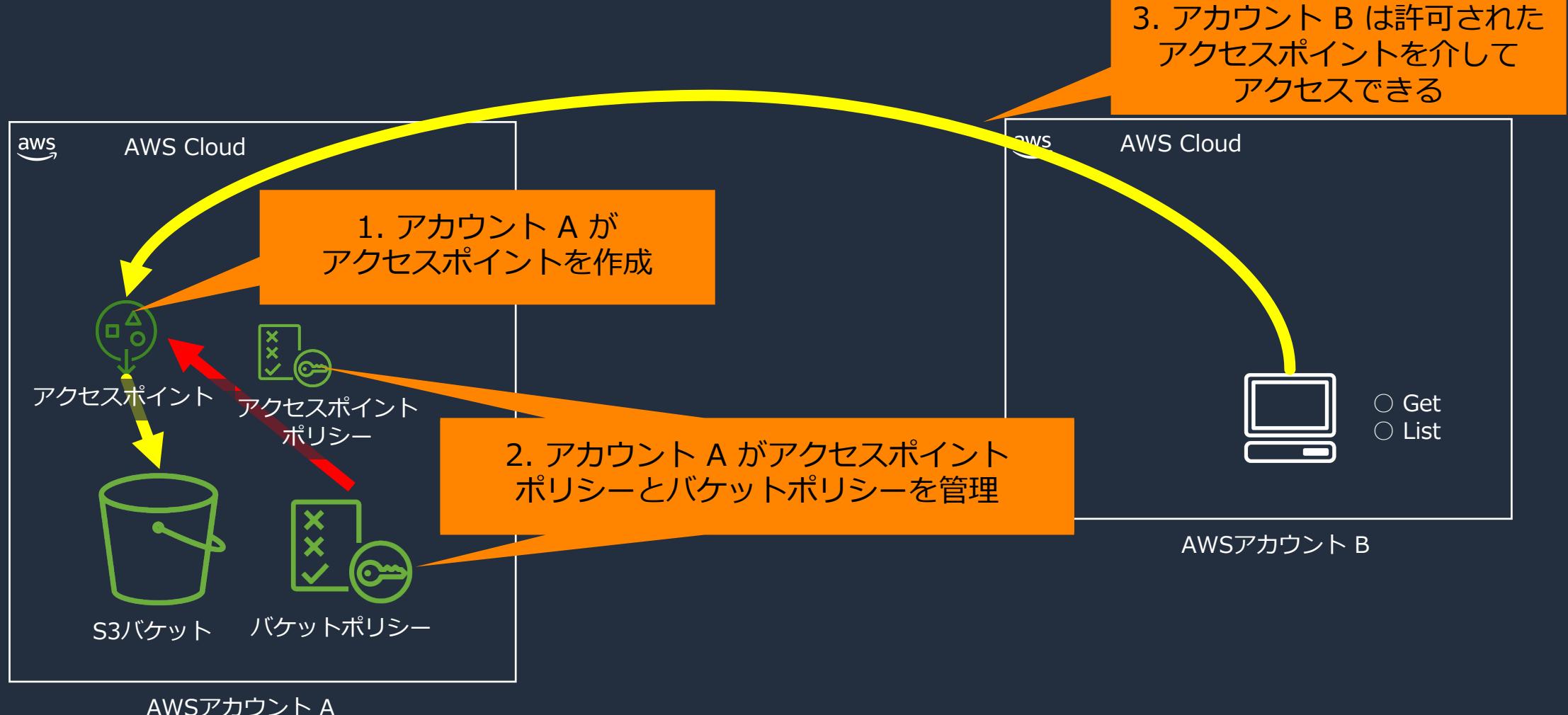
アクセスポイントを名前で検索

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)	[Redacted]	[Redacted]
accesspoint2	インターネット	[Redacted]	[Redacted]



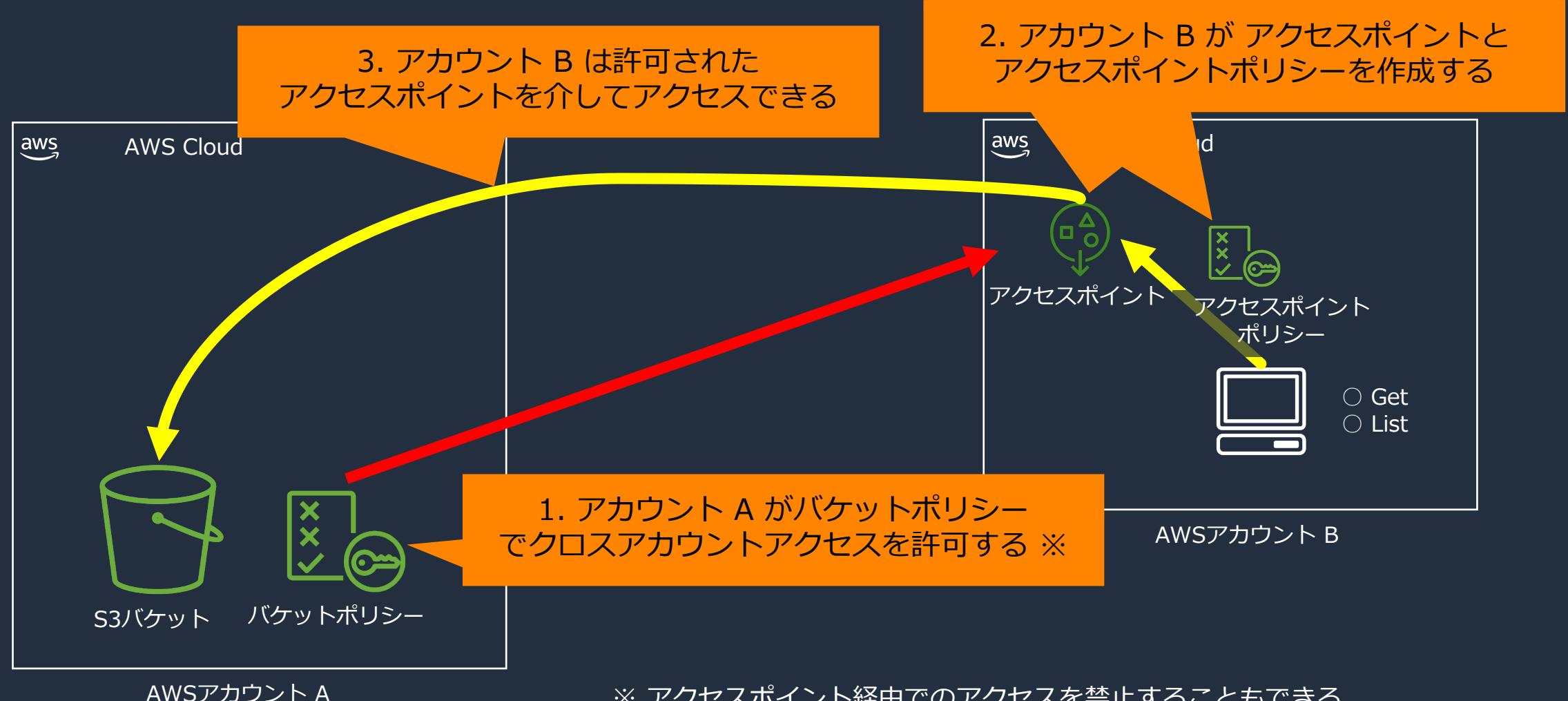
アクセスポイントを利用したクロスアカウントアクセス

アクセスポイントをバケットの所有者が管理



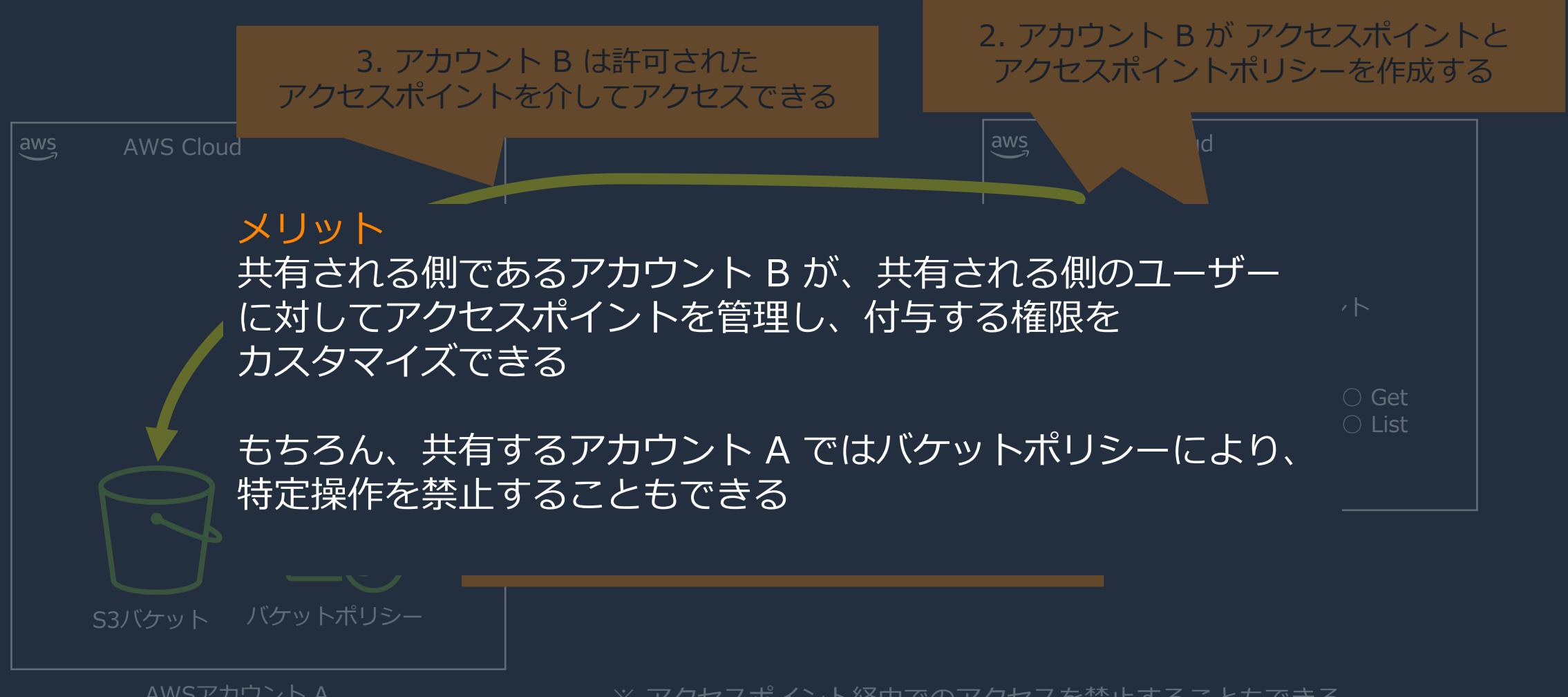
アクセスポイントを利用したクロスアカウントアクセス

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

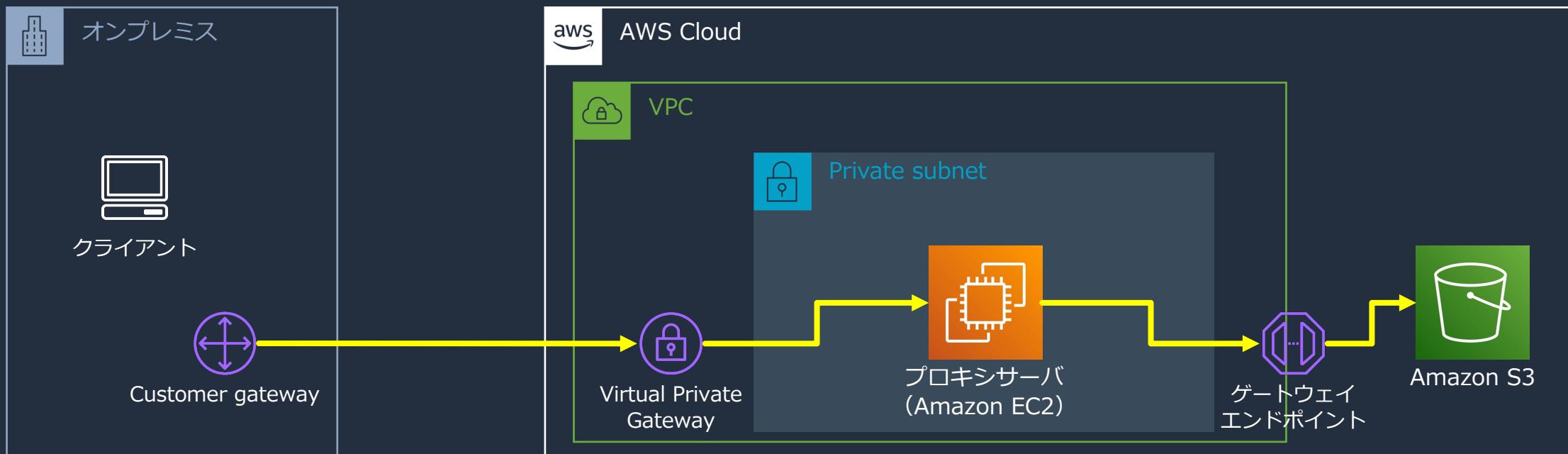
- ・ ゲートウェイエンドポイント
 - ・ VPC から AWS ネットワーク経由で S3 にアクセスする際、ルートテーブルで指定するゲートウェイ
- ・ インターフェイスエンドポイント (AWS PrivateLink)
 - ・ VPC 内部、オンプレミス、VPC ピアリングや Transit Gateway と紐づく別の VPC から、プライベート IP を利用してアクセス

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

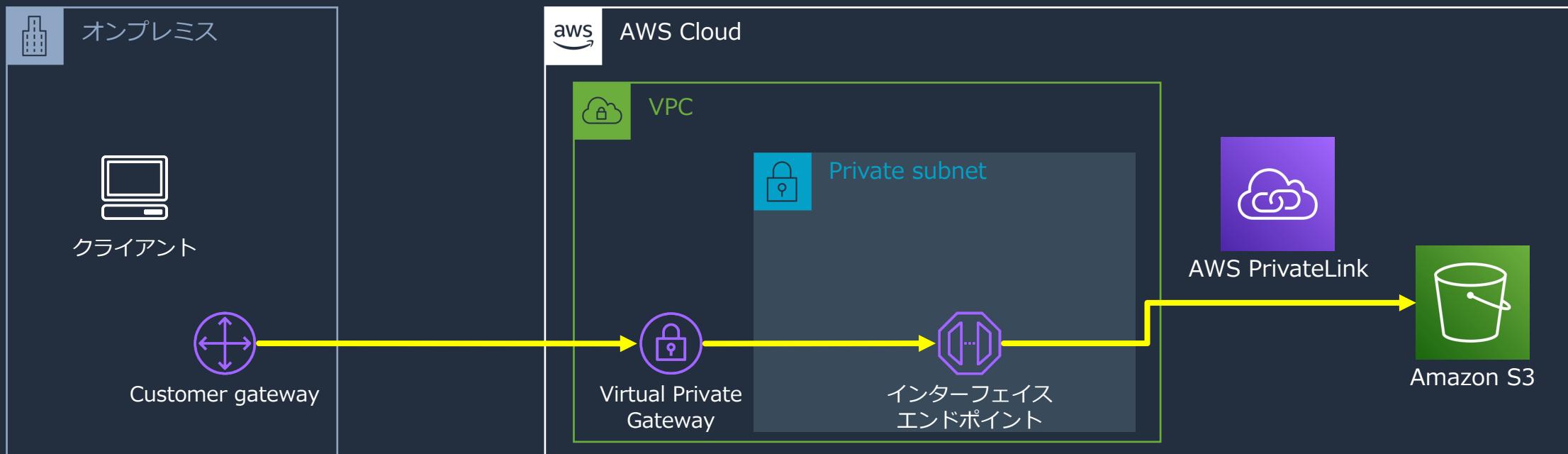
S3 のゲートウェイエンドポイントでのアクセスパス オンプレミスから閉じたネットワーク経由で S3 を利用する場合

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]

タグ

キー 値 - オプション

Name pl-for-s3-bb 削除

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

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
-

IP アドレスタイプ
ipv4

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, there's a breadcrumb navigation "ダッシュボード 情報". On the left, there's a sidebar with tabs "証跡" (selected) and "情報". The main area has tabs "名前" (with an orange arrow pointing to the input field containing "CloudTrailAudit"), "ステータス", and "ログ記録". A "ログ記録" tab is selected, showing a "データイベント" section with 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 right, there's a "編集" button with an orange border.

A modal dialog titled "イベント 情報" is open. 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" (Individual resources or all resources in your AWS account will be recorded. Additional charges apply). It has a section for "イベントタイプ" (Event Type) with the sub-instruction "ログ記録するイベントのタイプを選択します" (Select the type of events to log). There is a checkbox labeled "データイベント" (Data Events) with the description "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" (Logs resource operations performed on or within a resource). At the bottom right of the dialog are "キャンセル" (Cancel) and "変更の保存" (Save changes) 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!