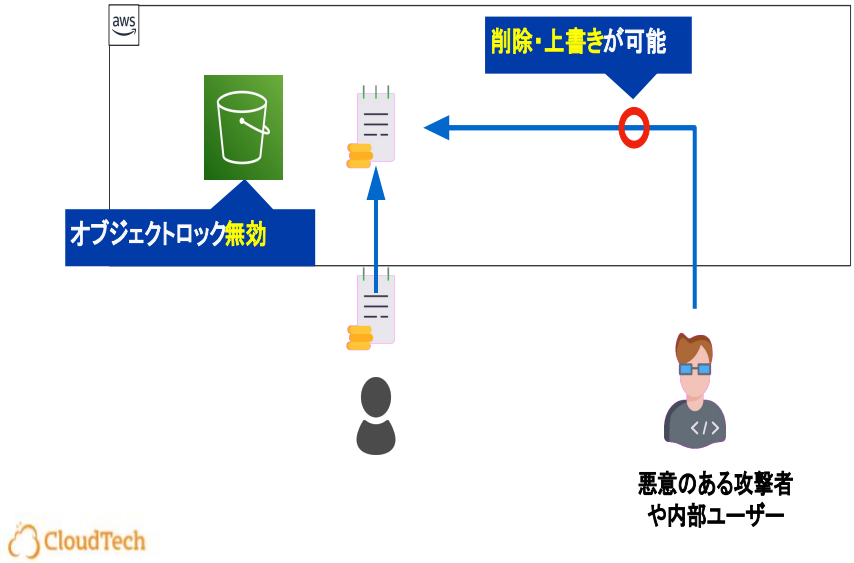
今回の講座ではS3オブジェクトロック・ボールドロックについて解説します。
どちらもS3のデータ保護に関する機能です。

S3(オブジェクトロック)



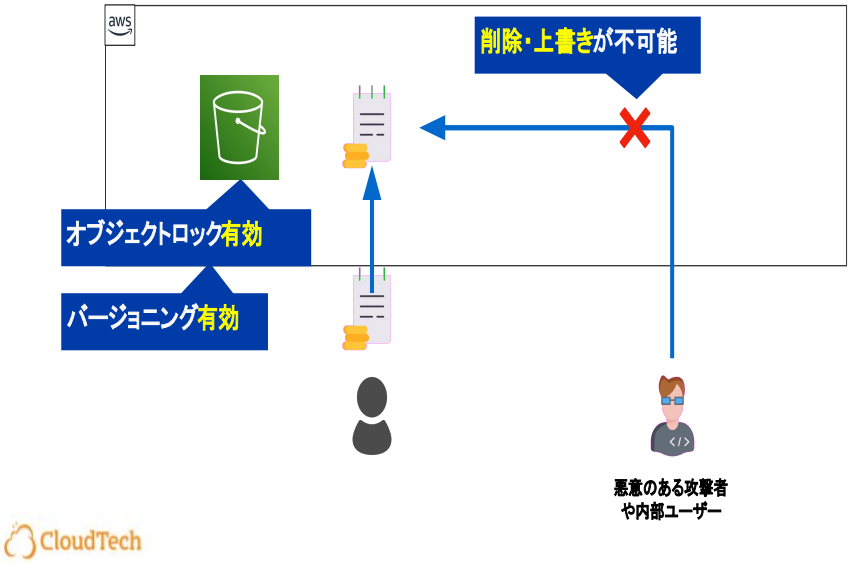
まずはS3オブジェクトロックについてです。**こちらはデフォルトでは無効となっている機能です。**
では、無効になっている場合にどのような問題があるかみてみましょう。

S3バケットに重要なデータを保存する必要があるとします。
重要なデータとは、例えばお客さんの個人情報などです。

このデータをS3バケットにアップロードします。
その後、**もし悪意のある攻撃者や内部ユーザーによってこのデータが削除や上書きをされてしまった場合、どうなるでしょう？**
データが失われるだけでなく、企業に大きな影響を与え、信頼性を損なってしまうかもしれません。

ここでオブジェクトロックが重要な役割を果たします。

S3(オブジェクトロック)

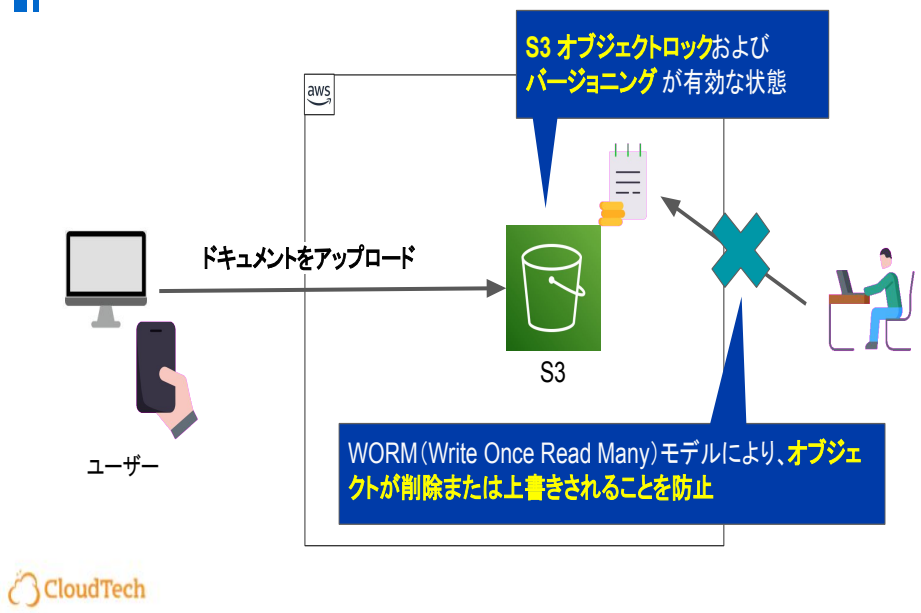


では、オブジェクトロックを有効にしてみましょう。
オブジェクトロックを有効にする際に **バージョニングも有効になります。**
バージョニングとは変更前・削除前のオブジェクトを保持する機能でしたね。

同じように重要なデータを S3バケットにアップロードします。
その後、悪意のある攻撃者や内部のユーザーが削除や上書きをしようとしますが、オブジェクトロックが有効になっているためできません。

このようにオブジェクトロックは、オブジェクトを変更や削除から保護してくれる機能となります。

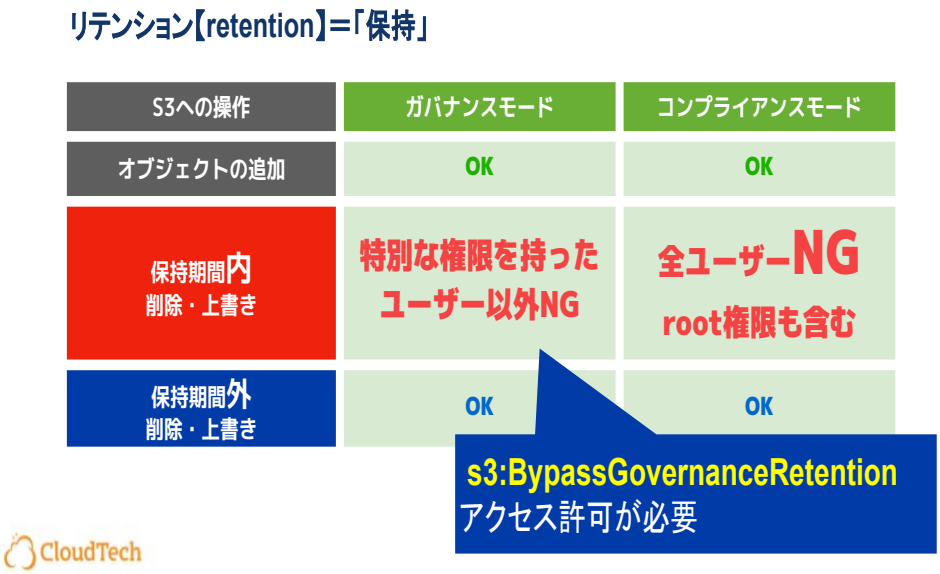
S3(オブジェクトロック)



この機能はWrite Once Read Many（WORM）モデルといったモデルに基づいています。
WORMとは文字通り、データを一度書き込むと、その後は何度でも読み取ることはできるが、書き換えることはできないという原則です。
この原則により、オブジェクトが削除または上書きされることを防止できます。

次にオブジェクトロックを有効にする時に理解しておく必要があるオプションをみていきましょう。

S3(オブジェクトロック)



まずはリテンションモードです。

リテンションには「保持」という意味があります。 つまりリテンションモードは、データを一定期間保持する設定です。
このモードには「ガバナンス」と「コンプライアンス」という二つのモードがあります。

2つモードの違いは保持期間内にオブジェクトを「削除・上書き」できるかです。

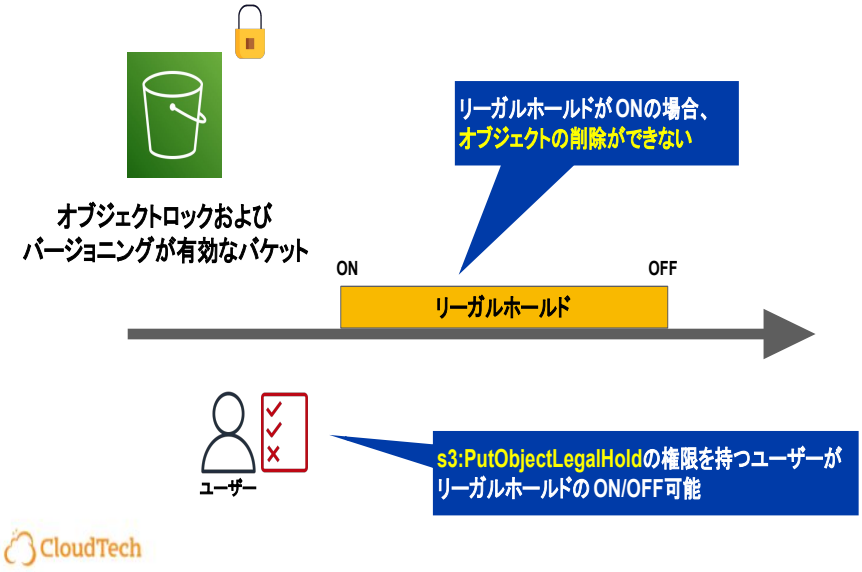
ガバナンスモードは、「s3:BypassGovernanceRetention」といった特定のアクセス権限を持つユーザー以外は削除・上書きができません。
一方、コンプライアンスモードは root権限も含む全ユーザーが削除・上書きができません。

よって、一度コンプライアンスモードでロックしてしまうと保持期間

を過ぎるまでオブジェクトの削除などができなくなります。
そのため、事前にガバナンスモードで保持期間の設定テストなどをしてからコンプライアンスモードに変更するのがいいでしょう。

なお、保持期間外であればどちらのモードも削除・上書きが可能となります。
では、無期限にオブジェクトを削除・上書きされないようにするにはどうすればいいでしょう？

S3(オブジェクトロック)

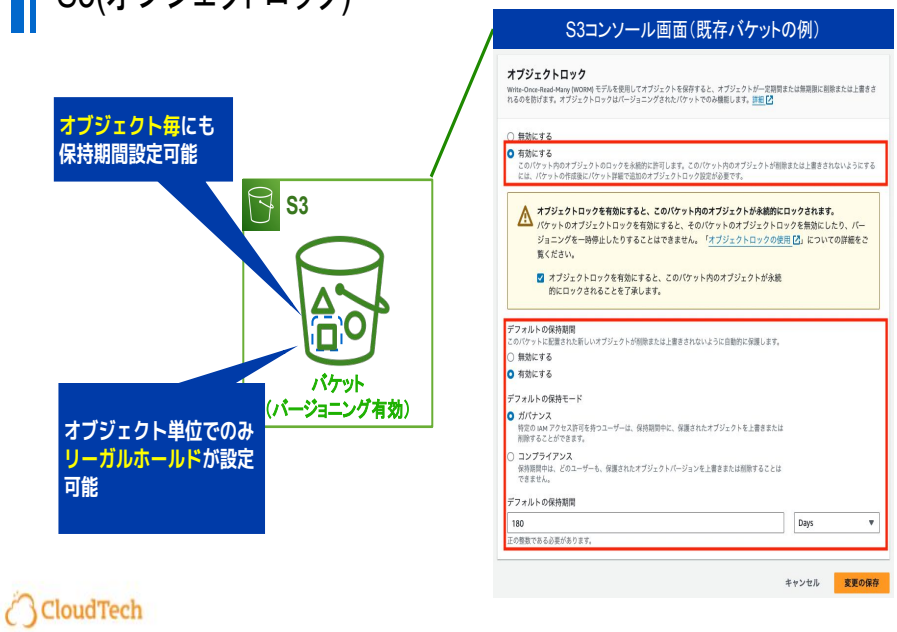


無期限にオブジェクトを削除・上書きされないようにするにはリーガルホールドという設定を使用します。

リーガルホールドがONの間は無期限にオブジェクトが削除・上書きできなくなります。
先ほどのリテンションモードと違い、リーガルホールドは保持期間を設定する必要がありません。
そのため、削除・上書きするまでの期間が未定なデータ、例えば、審査期間が決まっていない監査に使用するデータなどを保管する場合に有効です。

なおリーガルホールドは誰でも設定を ON/OFFできる訳ではありません。
OFFにする場合は、**「s3:PutObjectLegalHold」**のIAMポリシー権限を持つ必要があります。

S3(オブジェクトロック)



CloudTech

次にオブジェクトロックの設定方法について解説します。
S3コンソール、AWS CLIどちらでも設定可能ですが、**今回はS3コンソールでの設定方法をみてみましょう。**

新規の場合は作成時の「詳細設定」から、既存の場合は S3バケットの「プロパティ」タブをから設定できます。画面は既存バケットの例です。
オブジェクトロックを有効後、デフォルトの保持期間を設定します。なおバージョニングが有効になっていない場合は、設定時に合わせて有効にします。

ここで覚えておくポイントとしては、2点あります。

- **オブジェクト毎にも保持期間が設定可能**
    - デフォルトの保持期間はS3バケット全体のオブジェクトに対して設定される保持期間となっており、特定のオブジェクトのみ期間を変更することも可能です。

- **オブジェクト単位でのみリーガルホールドが設定可能**
    - リーガルホールドはS3バケット全体に対しては設定できません。

なお自分で既存のS3バケットに対してオブジェクトロックを設定できるようになったのは、2023年11月からです。
それより前はAWSサポートに連絡する必要がありました。
このように設定方法は常に変わっていく可能性があるので、最新の公式ドキュメントを参照し、手順を確認するようにしましょう。

では、オブジェクトロックについてまとめます。

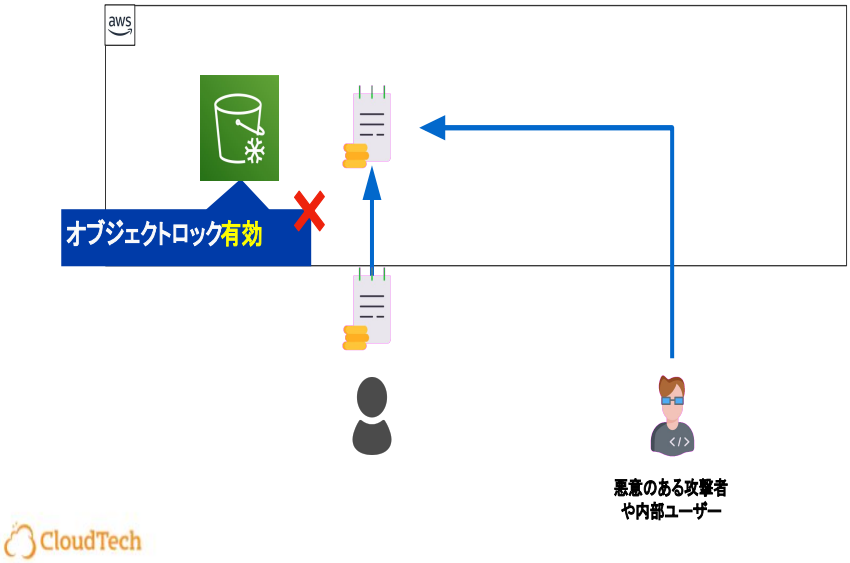
- オブジェクトを一定期間または無期限で削除や上書きから保護する機能
- Write Once Read Many（WORM）モデルを採用し、バージョンニング機能も有効
- リテンションモードを使用して、一定期間オブジェクトを削除や上書きから保護
- リーガルホールドを使用して、無期限でオブジェクトを削除や上書きから保護

気になる料金ですが、Amazon S3オブジェクトロック機能自体の使用に追加料金は発生しません。
しかし、オブジェクトロックを利用するためには S3バージョニングが自動的に有効になります。
バージョニングの講座で解説したように、保存されるオブジェクト

のバージョンが増えると、それに伴ってストレージの使用量が増加し、結果的にストレージコストが増加する可能性がありま す。
そのため、オブジェクトロックを設定する際には低コストのストレージクラスに保管するなど、コスト効率良く使うのが良いでしょう。

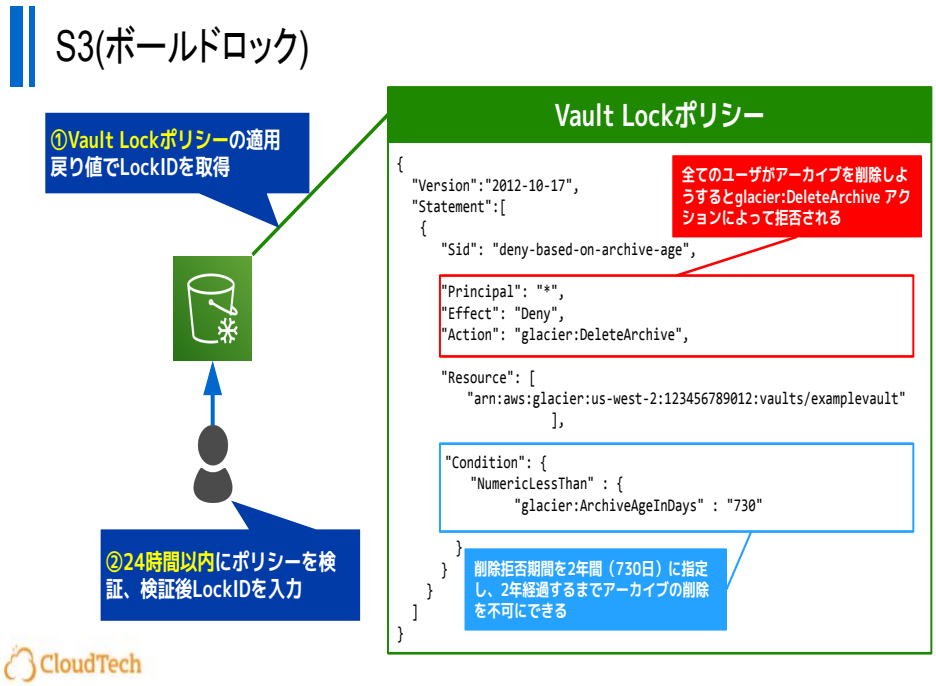
次にボールドロックについてです。

S3(ボールドロック)



先ほどはS3バケットを対象としていましたが、S3 Glacierに保存されたデータを同じように削除・上書きから保護するにはどのようにすればいいでしょう？
S3 Glacierは低コストのストレージであるため、監査や法的に保持が必要なデータを保存している場合が多く、データ保護が重要になってきます。

しかし、S3 GlacierではS3と同じようにオブジェクトロックを設定することはできません。
そこでボールドロックという機能を使用します。



ボールドロック機能はS3 Glacierに保存されたデータを削除保護する機能です。
ボールドロックは一度設定すると変更ができないため、設定には2段階プロセスを踏みます。

まずはじめに、Vault Lockポリシーを適用します。
ポリシーはこのように記述します。

- **"Principal": "*",**
- **"Effect": "Deny",**
- **"Action": "glacier:DeleteArchive",**

これにより、全ユーザーがアーカイブを削除しようするとglacier:DeleteArchive アクションによって拒否されるようになります。

"Resource"には対象のボールドを設定します。

そして、"Condition"でアーカイブの削除拒否期間を設定します。
ここでは、削除拒否期間を2年間（730日）に指定し、2年経過するまでアーカイブの削除を不可にできるよう設定しました。

このポリシーをGlacierの画面上で実行すると、テスト状態になります。
実行後に戻り値として返ってくるLockIDをメモします。

次にVault Lock ポリシーを検証します。
24時間テスト状態となるため、この間に保持期間やアクセス許可などの条件が正しいか検証します。
問題なければ、LockIDをかけて本格的に稼働させます。

以上で設定は完了です。
なお24時間を過ぎると、自動的にVault Lockポリシーは削除されます。

このようにして、ボールドロック機能により保存したアーカイブの削除を確実に防ぐことが可能となります。

S3(オブジェクトロック・ボールドロックの違い)

最後にオブジェクトロック・ボールドロックの違いについて解説します。

- サービス対象
  - オブジェクトロックはS3バケット内のオブジェクト
  - ボールトロックはS3 Glacierのアーカイブデータ
- 設定方法
  - オブジェクトロックはバケット全体または個別のオブジェクト毎に設定可能
  - ボールトロックはボールト全体にポリシーを設定、一度ロックされると変更不可
- 主な用途
  - オブジェクトロックはデータ保護、監査、法的保持要件の遵守
  - ボールトロックは長期アーカイブ、コンプライアンス要件の遵守

なおどちらもWORMモデルを使用したデータ保護機能です。
AWS SAA試験ではバージョニング機能やライフサイクル管理と合わせて出題されることが多いので、覚えておきましょう。

【公式ドキュメント】
https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/object-lock.html
https://docs.aws.amazon.com/ja_jp/amazonglacier/latest/dev/vault-lock.html