# S3 REST API
# のサポートされる処理と制限事項
StorageGRID

NetApp
October 03, 2025

# 目次

# S3 REST API のサポートされる処理と制限事項

StorageGRID システムは Simple Storage Service API （ API バージョン 2006-03-01 ）を実装しており、ほとんどの処理をサポートしていますが、いくつかの制限事項があります。S3 REST API クライアントアプリケーションを統合するときは、実装の詳細を理解しておく必要があります。

StorageGRID システムでは、仮想ホスト形式の要求とパス形式の要求の両方がサポートされます。

## 日付の処理

S3 REST API の StorageGRID 実装では、有効な HTTP の日付形式のみをサポートしています。

StorageGRID システムでは、日付の値を設定できるすべてのヘッダーで、有効な HTTP の日付形式のみがサポートされます。日付の時刻の部分は、 Greenwich Mean Time （ GMT ；グリニッジ標準時）の形式で指定するか、タイムゾーンのオフセットなし（ +0000 を指定）の Universal Coordinated Time （ UTC ；協定世界時）の形式で指定できます。要求に「 x-amz-date 」ヘッダーを含めた場合、 Date 要求ヘッダーで指定された値よりも優先されます。AWS 署名バージョン 4 を使用する場合は、 date ヘッダーはサポートされないため、署名済み要求に x-amz-date` のヘッダーを含める必要があります。

## 代表的な要求ヘッダー

StorageGRID システムでは、で定義されている代表的な要求ヘッダーがサポートされます "Amazon Web Services （ AWS ）ドキュメント：「 Amazon Simple Storage Service API Reference"1 つの例外を除いて。

| 要求ヘッダー | 実装 |
| --- | --- |
| 承認 | AWS 署名バージョン 2 は完全にサポートされます<br><br>AWS 署名バージョン 4 は次の例外を除いてサポートされます。<br><br>• 要求の本文の SHA256 の値は計算されません。「 x-amz-content-SHA256 」ヘッダーで「 unsigned payload 」の値が指定されているかのように、ユーザが送信した値は検証なしで受け入れられます。 |
| x-amz-security-token を指定します | 実装されていませんXNotImplemented が返されます。 |

## 共通の応答ヘッダー

StorageGRID システムでは、以下の例外を除き、 _Simple Storage Service API Reference_で 定義されている共通の応答ヘッダーがすべてサポートされます。

| 応答ヘッダー | 実装 |
| --- | --- |
| x-amz-id-2 | 使用されません |

# 要求を認証します

StorageGRID システムでは、 S3 API を使用したオブジェクトへのアクセスについて、認証アクセスと匿名アクセスの両方をサポートしています。

S3 API では、 S3 API 要求の認証で署名バージョン 2 と署名バージョン 4 がサポートされます。

認証された要求は、アクセスキー ID とシークレットアクセスキーを使用して署名する必要があります。

StorageGRID システムでは、 HTTP 「 Authorization 」ヘッダーとクエリーパラメータの 2 つの認証方式がサポートされています。

## **HTTP Authorization** ヘッダーを使用します

HTTP` Authorization 」ヘッダーは、バケットポリシーで許可された匿名の要求を除き、すべての S3 API 処理で使用されます。「 Authorization 」ヘッダーには、要求を認証するために必要なすべての署名情報が格納されます。

## クエリパラメータを使用します

クエリパラメータを使用すると、 URL に認証情報を追加できます。これは署名付き URL と呼ばれ、特定のリソースへの一時的なアクセスを許可する場合に使用できます。署名付き URL を使用すると、シークレットアクセスキーを知らないユーザでもリソースにアクセスできるため、他のユーザに制限付きアクセスを提供することができます。

# サービスの処理

StorageGRID システムでは、サービスに対して次の処理をサポートしています。

| 操作 | 実装 |
| --- | --- |
| GET Service の略 | Amazon S3 REST API のすべての動作が実装されています。 |
| GET Storage Usage の略 | GET Storage Usage 要求を使用すると、アカウントで使用しているストレージの総容量とアカウントに関連付けられているバケットごとの使用容量を確認できます。これは、パス / とカスタムクエリパラメータ (`?x-ntap-sg-usage') を追加したサービス上の操作です。 |

| 操作 | 実装 |
| --- | --- |
| オプション / | クライアント・アプリケーションは ' ストレージ・ノード上の S3 ポートへの要求を ' ストレージ・ノードが使用可能かどうかを判断するために S3 認証情報を提供することなく問題 に送信できますこの要求は監視に使用できるほか、外部のロードバランサがストレージノードの停止を特定する目的でも使用できます。 |

関連情報

GET Storage Usage 要求の略

# バケットの処理

## StorageGRID システムでは、 S3 テナントアカウントあたり最大 1 、 000 個のバケットがサポートされます。

バケット名については、 AWS US Standard リージョンの制限が適用されますが、 S3 仮想ホスト形式の要求をサポートするために DNS の命名規則にも従う必要があります。

"Amazon Web Services （ AWS ）ドキュメント：「 Bucket Restrictions and Limitations"

S3 API エンドポイントのドメイン名を設定

GET Bucket （ List Objects ）処理と GET Bucket versions 処理では、 StorageGRID の整合性制御がサポートされます。

最終アクセス時間の更新が個々のバケットで有効になっているか無効になっているかを確認することができます。

次の表に、 StorageGRID での S3 REST API バケット処理の実装方法を示します。これらの処理を実行するには、アカウントに必要なアクセスクレデンシャルが付与されている必要があります。

| 操作 | 実装 |
| --- | --- |
| バケットを削除します | Amazon S3 REST API のすべての動作が実装されています。 |
| バケットの CORS を削除します | この処理は、バケットの CORS 設定を削除します。 |
| バケットの暗号化を削除 | この処理は、バケットからデフォルトの暗号化を削除します。既存の暗号化オブジェクトは暗号化されたままですが、バケットに追加された新しいオブジェクトは暗号化されません。 |
| バケットライフサイクルを削除 | この処理は、バケットからライフサイクル設定を削除します。 |

| 操作 | 実装 |
| --- | --- |
| バケットポリシーを削除 | この処理は、バケットに関連付けられているポリシーを削除します。 |
| バケットレプリケーションを削除します | この処理は、バケットに関連付けられているレプリケーション設定を削除します。 |
| バケットのタグ付けを削除します | この処理では、「 tagging 」サブリソースを使用して、バケットからすべてのタグが削除されます。 |
| GET Bucket （ List Objects ）、バージョン 1 およびバージョン 2 | この処理は、バケット内のオブジェクトの一部またはすべて（最大 1 、 000 ）を返します。オブジェクトのストレージクラスには '2 つの値のいずれかを指定できますこれは ' オブジェクトが reduced_redundancy ストレージクラスオプションを使用して取り込まれた場合でも同様です<br>• オブジェクトがストレージ・ノードで構成されるストレージ・プールに格納されていることを示す 'standard'<br>• 「 Glacier 」。オブジェクトが、クラウド・ストレージ・プールで指定された外部バケットに移動されたことを示します。<br>バケットに同じプレフィックスを持つ削除されたキーが多数含まれている場合、応答にキーを含まない「 CommonPrefixes 」がいくつか含まれることがあります。 |
| GET Bucket ACL の場合 | この処理では、バケットの所有者にバケットに対するフルアクセスがあることを示す応答が返され、所有者の ID 、表示名、および権限が表示されます。 |
| GET Bucket CORS | この処理は、バケットの「 cors 」設定を返します。 |
| GET Bucket encryption | この処理は、バケットのデフォルトの暗号化設定を返します。 |
| GET Bucket lifecycle | この処理は、バケットのライフサイクル設定を返します。 |
| GET Bucket location の各ノードで使用でき | この処理は、 PUT Bucket 要求で LocationConstraint 要素を使用して設定されたリージョンを返します。バケットのリージョンが「 us-east-1 」の場合は、リージョンに対して空の文字列が返されます。 |
| GET Bucket notification | この処理は、バケットに関連付けられている通知設定を返します。 |
| GET Bucket Object versions | バケットに対する読み取りアクセスで、「 versions 」サブリソースを使用して、バケット内のオブジェクトのすべてのバージョンのメタデータのリストが表示されます。 |
| GET Bucket policy の場合 | この処理は、バケットに関連付けられているポリシーを返します。 |
| GET Bucket replication | この処理は、バケットに関連付けられているレプリケーション設定を返します。 |

| 操作 | 実装 |
| --- | --- |
| GET Bucket tagging | この処理では、「 tagging 」サブリソースを使用して、バケットのすべてのタグが返されます。 |
| GET Bucket versioning | この実装では 'versioning サブリソースを使用して ' バケットのバージョン管理状態を返します<br><br>• *blank*: バージョン管理は有効になっていません ( バケットはバージョン管理されていません )<br>• 有効：バージョン管理が有効になっています<br>• 中断：バージョン管理は以前有効になっていて、中断されています |
| オブジェクトロック設定の取得 | この処理では、バケットのデフォルトの保持モードとデフォルトの保持期間（設定されている場合）が返されます。<br><br>を参照してください オブジェクトロック設定の取得 を参照してください。 |
| HEAD Bucket （ヘッドバケット） | この処理は、バケットが存在し、そのバケットへのアクセス権限があるかどうかを判断します。<br><br>この処理から返される情報は次の<br><br>• x-ntap-sg-bucket-id ： UUID 形式のバケットの UUID 。<br>• `x-ntap-sg-trace-id`: 関連付けられた要求の一意のトレース ID 。 |

| 操作 | 実装 |
| --- | --- |
| PUT Bucket の場合 | この処理は、新しいバケットを作成します。バケットを作成すると、そのバケットの所有者になります。<br><br>• バケット名は次のルールを満たす必要があります。<br>◦ StorageGRID システム全体で（テナントアカウント内だけではなく）一意である必要があります。<br>◦ DNS に準拠している必要があります。<br>◦ 3 文字以上 63 文字以下にする必要があります。<br>◦ 1 つ以上のラベルを連続して指定できます。隣接するラベルはピリオドで区切ります。各ラベルの先頭と末尾の文字は小文字のアルファベットか数字にする必要があり、使用できる文字は小文字のアルファベット、数字、ハイフンのみです。<br>◦ テキスト形式の IP アドレスのようにはできません。<br>◦ 仮想ホスト形式の要求でピリオドを使用しないでください。ピリオドを使用すると、サーバワイルドカード証明書の検証で原因 の問題が発生します。<br>• デフォルトではバケットは us-east-1 リージョンに作成されますが、要求の本文で LocationConstraint 要求要素を使用し、別のリージョンを指定できます。LocationConstraint 要素を使用する場合は、 Grid Manager またはグリッド管理 API を使用して定義されたリージョンの正確な名前を指定する必要があります。使用すべきリージョン名がわからない場合は、システム管理者にお問い合わせください。<br>• 注： StorageGRID で定義されていないリージョンを PUT Bucket 要求で使用すると、エラーが発生します。<br>• S3 オブジェクトロックが有効なバケットを作成するには、「 x-amz-bucket-object lock-enabled 」要求ヘッダーを含めることができます。を参照してください S3 オブジェクトロックを使用する。<br><br>バケットの作成時に S3 オブジェクトのロックを有効にする必要があります。バケットの作成後に S3 オブジェクトのロックを追加または無効にすることはできません。S3 オブジェクトロックにはバケットのバージョン管理が必要です。バケットの作成時に自動的に有効になります。 |
| PUT Bucket CORS | この処理は、バケットの CORS 設定を指定し、クロスオリジン要求を処理できるようにします。Cross-Origin Resource Sharing （ CORS ）は、あるドメインのクライアント Web アプリケーションが別のドメインのリソースにアクセスできるようにするセキュリティ機能です。たとえば、「 images 」という名前の S3 バケットを使用してグラフィックを格納するとします。「 images 」バケットに対して CORS 設定を指定することで、そのバケット内の画像を Web サイト「 + http://www.example.com+` 」に表示できます。 |

| 操作 | 実装 |
| --- | --- |
| PUT Bucket encryption | この処理は、既存のバケットのデフォルトの暗号化状態を設定します。バケットレベルの暗号化が有効な場合は、バケットに追加されたすべての新しいオブジェクトが暗号化されます。 StorageGRID では、 StorageGRID で管理されるキーによるサーバ側の暗号化がサポートされます。サーバ側の暗号化設定規則を指定する場合は 'SSEAlgorithm' パラメータを AES256 に設定し 'KMSMasterKeyID' パラメータは使用しないでください<br><br>バケットのデフォルトの暗号化設定は、オブジェクトのアップロード要求ですでに暗号化が指定されている場合は無視されます（要求に「 x-amz-server-side-encryption - * 」要求ヘッダーが含まれる場合）。 |
| PUT Bucket lifecycle の場合 | この処理は、バケットの新しいライフサイクル設定を作成するか、既存のライフサイクル設定を置き換えます。StorageGRID では、 1 つのライフサイクル設定で最大 1 、 000 個のライフサイクルルールがサポートされます。各ルールには、次の XML 要素を含めることができます。<br><br>• 有効期限（日数、日付）<br>• NoncurrentVersionExpiration （ NoncurrentDays ）<br>• フィルタ（プレフィックス、タグ）<br>• ステータス<br>• ID<br><br>StorageGRID では、次のアクションはサポートされません。<br><br>• AbortIncompleteMultipartUpload の略<br>• ExpiredObjectDeleteMarker<br>• 移行<br><br>バケット・ライフサイクルの Expiration アクションと ILM 配置手順の相互作用については ' 情報ライフサイクル管理を使用してオブジェクトを管理する手順のオブジェクトのライフサイクル全体にわたる ILM の動作を参照してください<br><br>• 注：バケットライフサイクル設定は S3 オブジェクトロックが有効なバケットで使用できますが、従来の準拠バケットではバケットライフサイクル設定がサポートされません。 |

| 操作 | 実装 |
| --- | --- |
| PUT Bucket notification | この処理は、要求の本文に含まれる通知設定 XML を使用してバケットの通知を設定します。実装に関する次の詳細事項に注意してください。<br><br>• StorageGRID では、 Simple Notification Service （ SNS ）のトピックがデスティネーションとしてサポートされます。Simple Queue Service （ SQS ）エンドポイントまたは Amazon Lambda エンドポイントはサポートされていません。<br>• 通知のデスティネーションは、 StorageGRID エンドポイントの URN として指定する必要があります。エンドポイントは、 Tenant Manager またはテナント管理 API を使用して作成できます。<br><br>通知設定が機能するためには、エンドポイントが存在している必要があります。エンドポイントが存在しない場合は '400 Bad Request' エラーがコード 'InvalidArgument とともに返されます<br><br>• 次のイベントタイプには通知を設定できません。これらのイベントタイプは * サポートされていません。<br><br>◦ `s3 ： ReducedRedundancyLostObject`<br><br>◦ `s3:ObjectRestore: Completed`<br><br>• StorageGRID から送信されるイベント通知は標準の JSON 形式を使用しますが、次のように使用されないキーおよび特定の値が使用されるキーがあります。<br>• * eventSource*<br><br>sgws ： s3`<br><br>• * awsRegion *<br><br>含まれません<br><br>• * x-amz-id-2 *<br><br>含まれません<br><br>• * arn *<br><br>urn ： sgws ： s3 ：：： bucket_name' |
| PUT Bucket policy の場合 | この処理は、バケットに関連付けられているポリシーを設定します。 |

| 操作 | 実装 |
| --- | --- |
| PUT Bucket replication | この処理では、要求の本文に含まれるレプリケーション設定 XML を使用して、バケットの StorageGRID CloudMirror レプリケーションが設定されます。CloudMirror レプリケーションについては、実装に関する次の詳細事項に注意してください。<br><br>• StorageGRID では、 V1 のレプリケーション設定のみがサポートされます。つまり、 StorageGRID では「 Filter 」要素をルールに使用することはサポートされておらず、 V1 の規則に従ってオブジェクトバージョンが削除されます。詳細については、を参照してください "レプリケーション設定に関する Amazon S3 のドキュメント"。<br>• バケットレプリケーションは、バージョン管理されているバケットでもバージョン管理されていないバケットでも設定でき<br>• レプリケーション設定 XML の各ルールで異なるデスティネーションバケットを指定できます。1 つのソースバケットを複数のデスティネーションバケットにレプリケートできます。<br>• デスティネーションバケットは、テナントマネージャまたはテナント管理 API で指定された StorageGRID エンドポイントの URN として指定する必要があります。<br><br>レプリケーション設定が機能するためには、エンドポイントが存在している必要があります。エンドポイントが存在しない場合、リクエストは「 400 Bad Request 」として失敗します。「複製ポリシーを保存できません。」というエラーメッセージが表示されます。指定されたエンドポイント URN は存在しません： *URN*<br><br>• 設定 XML で「 Role 」を指定する必要はありません。この値は StorageGRID では使用されず、送信されても無視されます。<br>• 設定 XML からストレージクラスを省略した場合、 StorageGRID はデフォルトで「 standard 」ストレージクラスを使用します。<br>• ソースバケットからオブジェクトを削除する場合、またはソースバケット自体を削除する場合、クロスリージョンレプリケーションは次のように動作します。<br>◦ レプリケートの前にオブジェクトまたはバケットを削除すると、オブジェクトまたはバケットはレプリケートされず、通知は届きません。<br>◦ レプリケートのあとにオブジェクトまたはバケットを削除すると、 StorageGRID は、 V1 のクロスリージョンレプリケーションに対する Amazon S3 の通常の削除動作に従います。 |

| 操作 | 実装 |
| --- | --- |
| PUT Bucket tagging | この処理では、「 tagging 」サブリソースを使用して、バケットの一連のタグを追加または更新します。バケットタグを追加する場合は、次の制限事項に注意してください。<br><br>• StorageGRID と Amazon S3 はどちらもバケットごとに最大 50 個のタグをサポートします。<br>• バケットに関連付けられているタグには、一意のタグキーが必要です。タグキーには Unicode 文字を 128 文字まで使用できます。<br>• タグ値には、 Unicode 文字を 256 文字以内で指定します。<br>• キーと値では大文字と小文字が区別されます。 |
| PUT Bucket versioning の場合 | この実装では、「 versioning 」サブリソースを使用して、既存のバケットのバージョン管理の状態を設定します。バージョン管理の状態は、次のいずれかの値に設定できます。<br><br>• Enabled ：バケット内のオブジェクトに対してバージョン管理を有効にします。バケットに追加されるすべてのオブジェクトに、一意のバージョン ID が割り当てられます。<br>• Suspended ：バケット内のオブジェクトに対してバージョン管理を無効にします。バケットに追加されたすべてのオブジェクトは、バージョン ID 「 null 」を受け取ります。 |
| PUT Object Lock の設定を指定します | この処理は、バケットのデフォルト保持モードとデフォルトの保持期間を設定または削除します。<br><br>デフォルトの保持期間を変更した場合、既存のオブジェクトバージョンの retain-until はそのまま残り、新しいデフォルトの保持期間を使用して再計算されることはありません。<br><br>を参照してください PUT Object Lock の設定を指定します を参照してください。 |

関連情報

整合性制御

GET Bucket last access time 要求

バケットとグループのアクセスポリシー

監査ログで追跡される S3 処理

ILM を使用してオブジェクトを管理する

テナントアカウントを使用する

# S3 ライフサイクル設定を作成する

## S3 ライフサイクル設定を作成して、特定のオブジェクトが StorageGRID システムから削除されるタイミングを制御できます。

このセクションの簡単な例では、 S3 ライフサイクル設定で特定のオブジェクトが特定の S3 バケットから削除（期限切れ）されるタイミングを制御する方法を示します。このセクションの例は、説明のみを目的としています。S3 ライフサイクル設定の作成の詳細については、を参照してください "『 Amazon Simple Storage Service Developer Guide 』：「 Object lifecycle management"。StorageGRID では、 Expiration アクションのみがサポートされ、移行アクションはサポートされません。

### ライフサイクル構成とは

ライフサイクル設定は、特定の S3 バケット内のオブジェクトに適用される一連のルールです。各ルールは、影響を受けるオブジェクトと、それらのオブジェクトの有効期限（特定の日付または日数後）を指定します。

StorageGRID では、 1 つのライフサイクル設定で最大 1 、 000 個のライフサイクルルールがサポートされます。各ルールには、次の XML 要素を含めることができます。

- Expiration ：指定した日付に達した場合、またはオブジェクトが取り込まれたときから指定した日数に達した場合にオブジェクトを削除します。
- NoncurrentVersionExpiration ：指定した日数に達したオブジェクトを削除します。これは、オブジェクトが最新でなくなったときからです。
- フィルタ（プレフィックス、タグ）
- ステータス
- ID

バケットにライフサイクル設定を適用する場合、バケットのライフサイクル設定は常に StorageGRID の ILM 設定よりも優先されます。StorageGRID は、 ILM ではなくバケットの Expiration 設定を使用して、特定のオブジェクトを削除するか保持するかを決定します。

そのため、 ILM ルールの配置手順がオブジェクトに引き続き適用されていても、オブジェクトがグリッドから削除されることがあります。あるいは、 ILM 配置手順がすべて終了したあとも、オブジェクトがグリッドに保持される場合があります。詳細については、を参照してください オブジェクトのライフサイクル全体にわたる ILM の動作。

> バケットライフサイクル設定は S3 オブジェクトロックが有効になっているバケットで使用できますが、従来の準拠バケットではバケットライフサイクル設定がサポートされません。

StorageGRID では、次のバケット処理を使用してライフサイクル設定を管理できます。

- バケットライフサイクルを削除
- GET Bucket lifecycle
- PUT Bucket lifecycle の場合

### ライフサイクル構成を作成します

ライフサイクル設定を作成するための最初の手順として、 1 つ以上のルールを含む JSON ファイルを作成します。たとえば、この JSON ファイルには次の 3 つのルールが含まれています。

1. ルール 1 は、プレフィックス「 Category1`/ 」に一致するオブジェクトと「 key2` の値」が「 tag2` のオブジェクトにのみ適用されます。「 Expiration 」パラメータは、フィルタに一致するオブジェクトの有効期限が 2020 年 8 月 22 日の午前 0 時に切れるように指定します。
2. ルール 2 は、プレフィックス「 Category2`/ 」に一致するオブジェクトにのみ適用されます。' Expiration ' パラメータを指定すると、フィルタに一致するオブジェクトの取り込みから 100 日後に期限切れになります。

> ⓘ 日数を指定するルールは、オブジェクトが取り込まれた時点を基準とした相対的なルールです。現在の日付が取り込み日と日数を超えている場合は、ライフサイクル設定の適用後すぐに一部のオブジェクトがバケットから削除される可能性があります。

3. ルール 3 は、プレフィックス「 Category3/ 」に一致するオブジェクトにのみ適用されます。Expiration パラメータを指定すると ' 最新でないすべてのバージョンの一致オブジェクトが ' 最新でない状態になってから 50 日後に期限切れになります

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

バケットにライフサイクル設定を適用

ライフサイクル設定ファイルを作成したら、 PUT Bucket lifecycle 要求を発行してバケットに適用します。

この要求は、サンプルファイル内のライフサイクル設定を、「 testbucket 」という名前のバケット内のオブジェクトに適用します。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

ライフサイクル設定がバケットに正常に適用されたことを検証するために、問題 には GET Bucket lifecycle 要求があります。例：

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

成功応答には、適用したライフサイクル設定が表示されます。

バケットライフサイクルの有効期限が環境 オブジェクトであることを検証します

PUT Object 、 HEAD Object 、または GET Object 要求の発行時に、ライフサイクル設定の有効期限ルールが環境 の特定のオブジェクトかどうかを確認できます。ルールが適用される場合、応答にはオブジェクトの有効期限と一致する有効期限ルールを示す「 Expiration 」パラメータが含まれます。

> バケット・ライフサイクルは ILM よりも優先されるため ' 表示される「 expiry-date 」は ' オブジェクトが削除される実際の日付です詳細については、を参照してください オブジェクト保持期間の決定方法。

たとえば、この PUT Object 要求は 2020 年 6 月 22 日に発行され、「 testbucket 」バケットにオブジェクトを配置します。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

成功の応答は、オブジェクトの有効期限が 100 日（ 2020 年 10 月 1 日）に切れ、ライフサイクル設定のルール 2 に一致したことを示します。

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

たとえば、この HEAD Object 要求を使用して、 testbucket バケット内の同じオブジェクトのメタデータを取得しました。

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

成功の応答にはオブジェクトのメタデータが含まれ、オブジェクトが 100 日で期限切れになり、ルール 2 に一致したことが示されます。

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

## S3 オブジェクトロックのデフォルトバケット保持を使用する

バケットで S3 オブジェクトのロックが有効になっている場合は、バケットに追加された各オブジェクトに適用されるデフォルトの保持モードとデフォルトの保持期間を指定できます。

- バケットの作成時に S3 オブジェクトロックを有効または無効にすることができます。
- バケットで S3 オブジェクトロックが有効になっている場合は、バケットのデフォルトの保持を設定できます。
- デフォルトの保持設定は次のとおりです。
  - デフォルトの保持モード： StorageGRID は「準拠」モードのみをサポートします。
  - デフォルトの保持期間（日数または年数）。

### オブジェクトロック設定の取得

GET Object Lock Configuration 要求を使用すると、バケットでオブジェクトロックが有効になっているかどうかを確認できます。有効になっている場合は、バケットにデフォルトの保持モードと保持期間が設定されているかどうかを確認できます。

オブジェクトの新しいバージョンがバケットに取り込まれる際には、デフォルトの保持モードが適用されるのは、「 x-amz-object-lock-mode 」が指定されていない場合です。デフォルトの保持期間は、「 x-amz-object-lock-retain-date 」が指定されていない場合に、 retain-until date の計算に使用されます。

この処理を完了するには、 s3 ： GetBucketObjectLockConfiguration 権限または root アカウントが必要です。

要求例

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization string
Authorization: authorization string
```

応答例

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

**PUT Object Lock** の設定を指定します

PUT Object Lock Configuration 要求を使用すると、オブジェクトロックが有効になっているバケットのデフォルトの保持モードとデフォルトの保持期間を変更できます。以前に設定したデフォルトの保持設定を削除することもできます。

オブジェクトの新しいバージョンがバケットに取り込まれる際には、デフォルトの保持モードが適用されるのは、「 x-amz-object-lock-mode 」が指定されていない場合です。デフォルトの保持期間は、「 x-amz-object-lock-retain-date 」が指定されていない場合に、 retain-until date の計算に使用されます。

オブジェクトバージョンの取り込み後にデフォルトの保持期間が変更された場合、オブジェクトバージョンの retain-until はそのまま残り、新しいデフォルトの保持期間を使用して再計算されることはありません。

この処理を完了するには、 s3 ： PutBucketObjectLockConfiguration 権限または root アカウントが必要です。

PUT 要求では 'Content-MD5' 要求ヘッダーを指定する必要があります

要求例

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization string
Authorization: authorization string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

## バケットのカスタム処理

## StorageGRID システムでは、 S3 REST API に追加されたシステム固有のカスタムバケット処理をサポートしています。

次の表に、 StorageGRID でサポートされるカスタムバケット処理を示します。

| 操作 | 説明 | を参照してください。 |
| --- | --- | --- |
| GET Bucket consistency | 特定のバケットに適用されている整合性レベルを返します。 | GET Bucket consistency 要求を実行します |
| PUT Bucket consistency | 特定のバケットに適用される整合性レベルを設定します。 | PUT Bucket consistency 要求 |
| GET Bucket last access time の場合 | 特定のバケットで最終アクセス時間の更新が有効になっているか無効になっているかを返します。 | GET Bucket last access time 要求 |

| 操作 | 説明 | を参照してください。 |
| --- | --- | --- |
| PUT Bucket last access time のように指定します | 特定のバケットの最終アクセス時間の更新を有効または無効にできます。 | PUT Bucket last access time 要求の場合 |
| バケットのメタデータ通知設定を削除します | 特定のバケットに関連付けられているメタデータ通知設定 XML を削除します。 | DELETE Bucket metadata notification configuration 要求 |
| GET Bucket metadata notification configuration | 特定のバケットに関連付けられているメタデータ通知設定 XML を返します。 | GET Bucket metadata notification configuration 要求 |
| PUT Bucket metadata notification configuration のコマンドです | バケットのメタデータ通知サービスを設定します。 | PUT Bucket metadata notification configuration 要求 |
| 準拠設定の PUT Bucket | 廃止およびサポート終了：準拠を有効にした新しいバケットを作成できなくなりました。 | 廃止：準拠設定を指定した PUT Bucket |
| GET Bucket compliance で確認します | 廃止されましたがサポートされています：既存の古い準拠バケットに対して現在有効な準拠設定を返します。 | 廃止予定： GET Bucket compliance 要求 |
| PUT Bucket compliance で確認してください | 廃止されましたがサポートされています：既存の古い準拠バケットの準拠設定を変更できます。 | 廃止予定： PUT Bucket compliance 要求 |

関連情報

監査ログで追跡される S3 処理

# オブジェクトの処理

このセクションでは、 StorageGRID システムでオブジェクトの S3 REST API 処理を実装する方法について説明します。

すべてのオブジェクトの処理に次の条件が適用されます。

- StorageGRID 整合性制御 オブジェクトに対するすべての操作でサポートされます。ただし、次の操作はサポートされません。
  - GET Object ACL の場合
  - オプション /
  - オブジェクトのリーガルホールドを適用します
  - PUT Object retention のことです

◦ オブジェクトコンテンツを選択します

- 同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「 latest-wins 」ベースで解決されます。「 latest-wins 」評価は、 S3 クライアントが処理を開始するタイミングではなく、 StorageGRID システムが特定の要求を完了したタイミングで行われます。
- StorageGRID バケット内のオブジェクトは、匿名ユーザまたは別のアカウントが作成したオブジェクトも含めて、すべてバケット所有者によって所有されます。
- Swift を使用して StorageGRID システムに取り込まれたデータオブジェクトに S3 を使用してアクセスすることはできません。

次の表に、 StorageGRID での S3 REST API オブジェクト処理の実装方法を示します。

| 操作 | 実装 |
| --- | --- |
| オブジェクトを削除します | 多要素認証（ MFA ）と応答ヘッダー「 x-amz-MFA 」はサポートされていません。<br><br>StorageGRID は、 DELETE Object 要求を処理する際に、オブジェクトのすべてのコピーをすべての格納場所からただちに削除しようとします。成功すると、 StorageGRID はただちにクライアントに応答を返します。30 秒以内にすべてのコピーを削除できなかった場合（格納場所が一時的に使用不能などの理由で）、 StorageGRID は削除対象のコピーをキューに登録し、クライアントに処理が成功したことを通知します。<br><br>• バージョン管理 *<br><br>特定のバージョンを削除するには、バケットの所有者がリクエスタであり、「 versionId 」サブリソースを使用する必要があります。このサブリソースを使用すると、バージョンが完全に削除されます。'versionId' が削除マーカーに対応している場合 ' レスポンス・ヘッダー 'x-amz-delete-marker' は 'true' に設定されます<br><br>• バージョン管理が有効になっているバケットで「 versionID 」サブリソースを指定せずにオブジェクトを削除すると、削除マーカーが生成されます。削除マーカーの 'versionId' は 'x-amz-version-id' 応答ヘッダーを使用して返され 'x-amz-delete-marker' 応答ヘッダーは 'true' に設定されます<br>• バージョンが一時停止中のバケットで「 versionID 」サブリソースを使用せずにオブジェクトを削除すると、既存の「 null 」バージョンまたは「 null 」削除マーカーが完全に削除され、新しい「 null 」削除マーカーが生成されます。「 x-amz-delete-marker' response header 」が「 true 」に設定されて返されます。<br>• 注 * ：特定の場合、 1 つのオブジェクトに複数の削除マーカーが存在することがあります。 |
| 複数のオブジェクトを削除します | 多要素認証（ MFA ）と応答ヘッダー「 x-amz-MFA 」はサポートされていません。<br><br>同じ要求メッセージで複数のオブジェクトを削除できます。 |

| 操作 | 実装 |
| --- | --- |
| オブジェクトのタグ付けを削除します | 「 tagging 」サブリソースを使用して、オブジェクトからすべてのタグが削除されます。Amazon S3 REST API のすべての動作が実装されています。<br><br>• バージョン管理 *<br><br>要求に「 versionId 」クエリパラメータが指定されていない場合は、バージョン管理されたバケット内のオブジェクトの最新バージョンからすべてのタグが削除されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「 MethodNotAllowed 」ステータスが返され、「 x-amz-delete marker` 応答ヘッダーが「 true 」に設定されます。 |
| オブジェクトの取得 | オブジェクトの取得 |
| GET Object ACL の場合 | アカウントに必要なアクセスクレデンシャルがある場合、オブジェクトの所有者にオブジェクトに対するフルアクセスがあることを示す応答が返され、所有者の ID 、表示名、および権限が表示されます。 |
| オブジェクトのリーガルホールドを取得します | S3 オブジェクトロックを使用する |
| GET Object retention のことです | S3 オブジェクトロックを使用する |
| GET Object tagging | tagging` サブリソースを使用して、オブジェクトのすべてのタグを返します。Amazon S3 REST API のすべての動作が実装されています<br><br>• バージョン管理 *<br><br>要求に「 versionId 」クエリパラメータが指定されていない場合は、バージョン管理されたバケット内のオブジェクトの最新バージョンからすべてのタグが返されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「 MethodNotAllowed 」ステータスが返され、「 x-amz-delete marker` 応答ヘッダーが「 true 」に設定されます。 |
| HEAD Object の実行 | HEAD Object の実行 |
| POST Object restore の実行 | POST Object restore の実行 |
| PUT Object の場合 | PUT Object の場合 |
| PUT Object - Copy の各コマンドを実行します | PUT Object - Copy の各コマンドを実行します |
| オブジェクトのリーガルホールドを適用します | S3 オブジェクトロックを使用する |

| 操作 | 実装 |
| --- | --- |
| PUT Object retention のことです | S3 オブジェクトロックを使用する |
| PUT Object tagging | tagging` サブリソースを使用して、既存のオブジェクトに一連のタグを追加します。Amazon S3 REST API のすべての動作が実装されています<br><br>• オブジェクトタグの上限 *<br><br>タグは、新しいオブジェクトをアップロードするときに追加することも、既存のオブジェクトに追加することもできます。StorageGRID と Amazon S3 はどちらも、オブジェクトごとに最大 10 個のタグをサポートします。オブジェクトに関連付けられたタグには、一意のタグキーが必要です。タグキーには Unicode 文字を 128 文字まで、タグ値には Unicode 文字を 256 文字まで使用できます。キーと値では大文字と小文字が区別されます。<br><br>• タグの更新と取り込み動作 *<br><br>PUT Object tagging を使用してオブジェクトのタグを更新した場合、StorageGRID はオブジェクトを再取り込みしません。これは、一致する ILM ルールで指定されている取り込み動作が使用されないことを意味します。更新によって発生したオブジェクト配置の変更は、通常のバックグラウンド ILM プロセスで ILM が再評価されるときに実施されます。<br><br>このため、 ILM ルールの取り込み動作に Strict オプションが指定されている場合、必要なオブジェクト配置を実行できないと（たとえば、新たに必要となった場所を使用できない場合）、アクションは実行されません。更新されたオブジェクトは、必要な配置を実行可能になるまで現在の配置が維持されます。<br><br>• 衝突の解決 *<br><br>同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「 latest-wins 」ベースで解決されます。「 latest-wins 」評価は、 S3 クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングで行われます。<br><br>• バージョン管理 *<br><br>要求に「 versionId 」クエリパラメータが指定されていない場合、バージョン管理されたバケット内のオブジェクトの最新バージョンにタグが追加されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「 MethodNotAllowed 」ステータスが返され、「 x-amz-delete marker` 応答ヘッダーが「 true 」に設定されます。 |

関連情報

監査ログで追跡される S3 処理

# S3 オブジェクトロックを使用する

StorageGRID システムでグローバルな S3 オブジェクトのロック設定が有効になっている場合は、 S3 オブジェクトのロックを有効にしたバケットを作成し、バケットごとにデフォルトの保持期間を指定したり、バケットに追加する各オブジェクトバージョンに対して特定の retain-une-date および legal hold 設定を指定したりできます。

S3 オブジェクトロックでは、オブジェクトレベルの設定を指定して、一定期間または無期限にオブジェクトが削除または上書きされないようにすることができます。

StorageGRID S3 オブジェクトロック機能は、 Amazon S3 準拠モードと同等の単一の保持モードを提供します。デフォルトでは、保護されたオブジェクトバージョンは、どのユーザーでも上書きまたは削除できません。StorageGRID S3 オブジェクトのロック機能では、ガバナンスモードはサポートされず、特別な権限を持つユーザは保持設定を省略したり保護されたオブジェクトを削除したりすることはできません。

## バケットに対して S3 オブジェクトロックを有効にします

StorageGRID システムでグローバルな S3 オブジェクトのロック設定が有効になっている場合は、各バケットの作成時に S3 オブジェクトのロックを必要に応じて有効にすることができます。次のいずれかの方法を使用できます。

- Tenant Manager を使用してバケットを作成します。

  テナントアカウントを使用する

- PUT Bucket 要求で「 x-amz-bucketobject-lock-enabled 」要求ヘッダーを指定してバケットを作成します。

  バケットの処理

バケットの作成後に S3 オブジェクトのロックを追加または無効にすることはできません。S3 オブジェクトロックにはバケットのバージョン管理が必要です。バケットの作成時に自動的に有効になります。

S3 オブジェクトのロックが有効になっているバケットには、 S3 オブジェクトのロック設定があるオブジェクトとなっていないオブジェクトを組み合わせて含めることができます。StorageGRID では、 S3 オブジェクトロックバケット内のオブジェクトに対してデフォルトの保持期間をサポートしており、 PUT Object Lock Configuration バケット処理をサポートしています。`s3:object-lock-remaining-retention-days' ポリシー条件キーは ' オブジェクトの最小および最大の保持期間を設定します

## バケットで S3 オブジェクトのロックが有効になっているかどうかを確認しています

S3 オブジェクトロックが有効になっているかどうかを確認するには、を使用します オブジェクトロック設定の取得 リクエスト。

## S3 オブジェクトのロック設定を指定してオブジェクトを作成します

S3 オブジェクトロックが有効に問題 なっているバケットにオブジェクトのバージョンを追加するときに S3 オブジェクトのロック設定を指定するには、 PUT Object 、 PUT Object - Copy 、 Initiate Multipart Upload 要求のいずれかを実行します。次の要求ヘッダーを使用します。

バケットの作成時に S3 オブジェクトのロックを有効にする必要があります。バケットの作成後に S3 オブジェクトのロックを追加または無効にすることはできません。

- 「 x-amz-object-lock-mode 」を指定してください。このモードは準拠している必要があります（大文字と小文字が区別されます）。

  「 x-amz-object-lock-mode 」を指定した場合は、「 x-amz-object-lock-retain-date 」も指定する必要があります。

- x-amz-object-lock-retain-until -date' のように指定します
  - retain-until の値は、「 2020-08-10T21:46:00Z」 の形式で指定する必要があります。秒数には分数を指定できますが、保持される 10 進数は 3 桁（ミリ秒単位）だけです。それ以外の ISO 8601 形式はサポートされません。
  - retain-une-date は将来の日付にする必要があります。
- 「 x-amz-object-lock-legal hold' 」のようになります

  リーガルホールドがオン（大文字と小文字が区別される）の場合、オブジェクトはリーガルホールドの対象になります。リーガルホールドがオフの場合、リーガルホールドは適用されません。それ以外の値を指定すると、 400 Bad Request （ InvalidArgument ）エラーが発生します。

次のいずれかの要求ヘッダーを使用する場合は、次の制限事項に注意してください。

- PUT Object 要求に x-amz-object-lock-*' 要求ヘッダーが含まれている場合は 'Content-MD5' 要求ヘッダーが必要ですPUT Object - Copy または Initiate Multipart Upload には 'Content-md5' は必要ありません
- バケットで S3 オブジェクトロックが有効になっておらず、「 x-amz-object-lock - * 」要求ヘッダーが存在する場合、 400 Bad Request （ InvalidRequest ）エラーが返されます。
- PUT Object 要求では、 AWS の動作に合わせて「 x-amz-storage-class ： reduced_redundancy 」を使用できます。ただし、 S3 オブジェクトのロックが有効になっているバケットにオブジェクトが取り込まれると、 StorageGRID は常にデュアルコミットの取り込みを実行します。
- 後続の GET または HEAD Object バージョンの応答には、「 x-amz-object-lock-mode 」、「 x-amz-object-lock-retain-until date 」、「 x-amz-object-lock-legal hold` 」のヘッダーが含まれます。設定されている場合、要求の送信者に「 s3 ： get * 」権限が付与されている場合のみです。
- それ以降の DELETE Object version 要求または DELETE Objects versions 要求は、 retain-until 日の前であるか、リーガルホールドがオンの場合には失敗します。

**S3** オブジェクトのロック設定を更新します

既存のオブジェクトのバージョンのリーガルホールドや保持の設定を更新する必要がある場合、次のオブジェクトサブリソース処理を実行できます。

- 「 PUT Object legal hold. 」のように指定します

  新しいリーガルホールドの値が on の場合、オブジェクトはリーガルホールドの対象になります。リーガルホールドの値がオフの場合、リーガルホールドは解除されます。

- 「 PUT Object retention 」のように指定します
  - モード値は準拠している必要があります（大文字と小文字が区別されます）。

- retain-until の値は、「 2020-08-10T21:46:00Z」 の形式で指定する必要があります。秒数には分数を指定できますが、保持される 10 進数は 3 桁（ミリ秒単位）だけです。それ以外の ISO 8601 形式はサポートされません。
- オブジェクトバージョンに既存の retain-until がある場合は、オブジェクトバージョンを増やすことはできますが、増やすことはできません。新しい値は将来の必要があります。

関連情報

ILM を使用してオブジェクトを管理する

テナントアカウントを使用する

PUT Object の場合

PUT Object - Copy の各コマンドを実行します

マルチパートアップロードを開始します

オブジェクトのバージョン管理

"『 Amazon Simple Storage Service User Guide 』：「 Using S3 Object Lock"

## S3 Select を使用する

StorageGRID では、用の AWS S3 Select 句、データ型、および演算子をサポートしています SelectObjectContent コマンド。

リストにない項目はサポートされていません。

構文については、を参照してください SelectObjectContent の順に選択します。S3 Select の詳細については、を参照してください "S3 Select に関する AWS のドキュメント"。

問題 SelectObjectContent クエリを実行できるのは、 S3 Select が有効になっているテナントアカウントのみです。を参照してください S3 Select を使用する際の考慮事項と要件。

句

- リストを選択します
- FROM 句
- WHERE 句
- Limit 句

データ型

- ブール値
- 整数
- 文字列
- 浮動小数点

- 10 進数、数値
- タイムスタンプ

### 演算子

#### 論理演算子

- および
- ありません
- または

#### 比較演算子

- <
- >
- ⇐
- >=
- =
- =
- <>
- !=
- 間（ Between ）
- インチ

#### パターンマッチング演算子

- いいね
- _
- %

#### 単一の演算子

- は NULL です
- は NULL ではありません

#### 数学演算子

- [+]
- -
- *
- /
- %

StorageGRID は、 AWS S3 Select 演算子の優先順位に従います。

集合関数

- 平均 ()
- カウント（ * ）
- 最大 ()
- 最小（）
- 合計 ()

条件付き関数

- ケース
- 集合体
- NULLIF

変換関数

- CAST （サポートされているデータタイプ用）

日付関数

- date_add
- DATE_DIFF
- 抽出（ Extract ）
- 文字列まで（ _STRING ）
- 終了タイムスタンプ
- UTCNOW

文字列関数

- char_length 、 character_length
- 低い
- サブストリング
- トリム（ Trim ）
- 上限

## サーバ側の暗号化を使用します

サーバ側の暗号化を使用して、保存中のオブジェクトデータを保護できます。StorageGRID は、オブジェクトを書き込む際にデータを暗号化し、ユーザがオブジェクトにアクセスする際にデータを復号化します。

サーバ側の暗号化を使用する場合は、暗号化キーの管理方法に基づいて、次の 2 つのオプションを同時に選択できます。

- * SSE （ StorageGRID で管理されるキーによるサーバ側の暗号化） * ：オブジェクトを格納する S3 要求を問題 で暗号化すると、 StorageGRID は一意のキーでオブジェクトを暗号化します。オブジェクトを読み出す S3 要求を問題 で実行すると、 StorageGRID は格納されているキーを使用してオブジェクトを復号化します。
- * SSE-C （ユーザ指定のキーによるサーバ側の暗号化） * ：オブジェクトを格納する S3 要求を問題 で処理するときに、独自の暗号化キーを指定します。オブジェクトを読み出すときは、同じ暗号化キーを要求に指定します。2 つの暗号化キーが一致すると、オブジェクトが復号化されてオブジェクトデータが返されます。

  オブジェクトの暗号化処理と復号化処理はすべて StorageGRID で管理されますが、指定する暗号化キーはユーザが管理する必要があります。

> ⓘ 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。

> ⓘ SSE または SSE-C で暗号化されたオブジェクトは、バケットレベルまたはグリッドレベルの暗号化設定が無視されます。

**SSE** を使用します

StorageGRID で管理される一意のキーでオブジェクトを暗号化する場合は、次の要求ヘッダーを使用します。

「 x-amz-server-side-encryption 」です

SSE 要求ヘッダーは、次のオブジェクト処理でサポートされます。

- PUT Object の場合
- PUT Object - Copy の各コマンドを実行します
- マルチパートアップロードを開始します

**SSE-C** を使用します

ユーザが管理する一意のキーでオブジェクトを暗号化する場合は、次の 3 つの要求ヘッダーを使用します。

| 要求ヘッダー | 説明 |
| --- | --- |
| x-amz-server-sideAlsebaling-smaling()- ユーザアルゴリズム | 暗号化アルゴリズムを指定します。ヘッダー値は 'AES256' でなければなりません |
| x-amz-server-sideSDebing-sotionsmokey-customer-key' のように指定します | オブジェクトの暗号化と復号化に使用する暗号化キーを指定します。キーの値は、 Base64 でエンコードされた 256 ビットであることが必要です。 |

| 要求ヘッダー | 説明 |
| --- | --- |
| x-amz-server-side-encryption | RFC 1321 に従って暗号化キーの MD5 ダイジェストを指定します。これは、暗号化キーがエラーなしで送信されたことを確認するために使用されます。MD5 ダイジェストの値は、 Base64 でエンコードされた 128 ビットであることが必要です。 |

SSE-C 要求ヘッダーは、次のオブジェクト処理でサポートされます。

- オブジェクトの取得
- HEAD Object の実行
- PUT Object の場合
- PUT Object - Copy の各コマンドを実行します
- マルチパートアップロードを開始します
- パーツをアップロードします
- パーツのアップロード - コピー

ユーザ指定のキーによるサーバ側の暗号化（ **SSE-C** ）を使用する場合の考慮事項

SSE-C を使用する場合は、次の考慮事項に注意してください。

- HTTPS を使用する必要があります。

> SSE-C を使用すると、 http 経由の要求が StorageGRID ですべて拒否されますセキュリティ上の理由から、誤って http を使用して送信したキーは漏洩する可能性があります。キーを破棄し、必要に応じてローテーションします。

- 応答内の ETag は、オブジェクトデータの MD5 ではありません。
- 暗号化キーとオブジェクトの対応関係を管理する必要があります。StorageGRID では暗号化キーは格納されません。各オブジェクトに対して指定した暗号化キーを管理する責任はユーザにあります。
- バケットのバージョン管理が有効になっている場合は、オブジェクトのバージョンごとに固有の暗号化キーが必要です。各オブジェクトバージョンで使用される暗号化キーを管理する責任はユーザにあります。
- 暗号化キーはクライアント側で管理するため、キーローテーションなどの追加の防護策もクライアント側で管理する必要があります。

> 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。

- バケットに CloudMirror レプリケーションが設定されている場合は、 SSE-C オブジェクトを取り込むことができません。取り込み処理は失敗します。

関連情報

オブジェクトの取得

HEAD Object の実行

PUT Object の場合

PUT Object - Copy の各コマンドを実行します

マルチパートアップロードを開始します

パーツをアップロードします

パーツのアップロード - コピー

"Amazon S3 開発者ガイド：「お客様が用意した暗号化キーによるサーバ側の暗号化（ SSE-C ）を使用したデータの保護」"

## オブジェクトの取得

S3 GET Object 要求を使用して、 S3 バケットからオブジェクトを読み出すことができます。

### オブジェクトとマルチパートオブジェクトを取得する

「 PartNumber 」要求パラメータを使用すると、マルチパートオブジェクトまたはセグメント化されたオブジェクトの特定の部分を取得できます。「 x-amz-mp-parts-count 」応答要素は、オブジェクトのパーツ数を示します。

セグメント化された / マルチパートオブジェクトとセグメント化されていない / 非マルチパートオブジェクトの両方に対して「 PartNumber 」を 1 に設定できますが、「 x-amz-mp-parts-count 」応答要素はセグメント化されたオブジェクトまたはマルチパートオブジェクトに対してのみ返されます。

### ユーザ指定の暗号化キーによるサーバ側の暗号化（ **SSE-C** ）の要求ヘッダー

指定した一意のキーでオブジェクトが暗号化されている場合は、 3 つのヘッダーをすべて使用します。

- 「 x-amz-server-side-encryption-customer-algorithm 」：「 AES256 」を指定します。
- x-amz-server-side-encryption-customer-key ：オブジェクトの暗号化キーを指定します。
- x-amz-server-side-encryption-customer-key-MD5 ：オブジェクトの暗号化キーの MD5 ダイジェストを指定します。

> 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に ' サーバ側の暗号化を使用の考慮事項を確認してください

### ユーザメタデータ内の **UTF-8** 文字

StorageGRID は、ユーザ定義メタデータ内のエスケープされた UTF-8 文字を解析も解釈もしません。ユーザ定義メタデータにエスケープされた UTF-8 文字が含まれているオブジェクトに対して GET 要求を実行した場合、キーの名前または値に印刷不能文字が含まれていると、「 x-amz-missing -meta 」ヘッダーが返されません。

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。指定した場合は "XNotImplemented " が返されます。

- 「 x-amz-website redirect-location 」

バージョン管理

versionId サブリソースが指定されていない場合、バージョン管理されたバケット内のオブジェクトの最新バージョンが取得されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「 Not Found 」ステータスが返され、「 x-amz-delete-marker` 応答ヘッダーは「 true 」に設定されます。

クラウドストレージプールオブジェクトに対する **GET Object** の動作

オブジェクトがクラウドストレージプールに格納されている場合（情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照）、 GET Object 要求の動作はオブジェクトの状態によって異なります。詳細については、「 head Object 」を参照してください。

> オブジェクトがクラウドストレージプールに格納され、かつそのオブジェクトのコピーがグリッドに 1 つ以上存在する場合、 GET Object 要求はクラウドストレージプールからデータを読み出す前に、グリッドからデータを読み出そうとします。

| オブジェクトの状態 | **GET Object** の動作 |
| --- | --- |
| StorageGRID に取り込まれているがまだ ILM によって評価されていないオブジェクト、または従来のストレージプールに格納されているオブジェクト、またはイレイジャーコーディングを使用しているオブジェクト | 「 200 OK 」<br><br>オブジェクトのコピーが読み出されます。 |
| クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない | 「 200 OK 」<br><br>オブジェクトのコピーが読み出されます。 |
| オブジェクトを読み出し不可能な状態に移行した | 「 403 Forbidden 」、「 InvalidObjectState 」<br><br>POST Object restore 要求を使用して、オブジェクトを読み出し可能な状態にリストアします。 |
| 読み出し不可能な状態からリストア中である | 「 403 Forbidden 」、「 InvalidObjectState 」<br><br>POST Object restore 要求が完了するまで待ちます。 |
| クラウドストレージプールへのリストアが完了している | 「 200 OK 」<br><br>オブジェクトのコピーが読み出されます。 |

クラウドストレージプール内のマルチパートオブジェクトまたはセグメント化されたオブジェクト

マルチパートオブジェクトをアップロードした場合や StorageGRID が大きなオブジェクトをセグメントに分割した場合、 StorageGRID はオブジェクトのパーツまたはセグメントのサブセットをサンプリングすることでクラウドストレージプール内のオブジェクトが使用可能かどうかを判断します。オブジェクトの一部の部分がすでに読み出し不可能な状態に移行されている場合、またはオブジェクトの一部がまだリストアされていない場合、 GET Object 要求が誤って「 200 OK 」を返すことがあります。

このような場合は、次のよう

- GET Object 要求がデータの一部を返し、転送の途中で停止することがあります。
- 後続の GET Object 要求では、「 403 Forbidden 」が返される場合があります。

関連情報

サーバ側の暗号化を使用します

ILM を使用してオブジェクトを管理する

POST Object restore の実行

監査ログで追跡される S3 処理

## HEAD Object の実行

S3 HEAD Object 要求を使用すると、オブジェクト自体を返さずにオブジェクトからメタデータを読み出すことができます。オブジェクトがクラウドストレージプールに格納されている場合は、 HEAD Object を使用してオブジェクトの移行状態を特定できます。

### HEAD オブジェクトおよびマルチパートオブジェクト

「 PartNumber 」要求パラメータを使用すると、マルチパートオブジェクトまたはセグメント化されたオブジェクトの特定の部分のメタデータを取得できます。「 x-amz-mp-parts-count 」応答要素は、オブジェクトのパーツ数を示します。

セグメント化された / マルチパートオブジェクトとセグメント化されていない / 非マルチパートオブジェクトの両方に対して「 PartNumber 」を 1 に設定できますが、「 x-amz-mp-parts-count 」応答要素はセグメント化されたオブジェクトまたはマルチパートオブジェクトに対してのみ返されます。

### ユーザ指定の暗号化キーによるサーバ側の暗号化（ SSE-C ）の要求ヘッダー

指定した一意のキーでオブジェクトが暗号化されている場合は、次の 3 つのヘッダーをすべて使用します。

- 「 x-amz-server-side-encryption-customer-algorithm 」：「 AES256 」を指定します。
- x-amz-server-side-encryption-customer-key ：オブジェクトの暗号化キーを指定します。
- x-amz-server-side-encryption-customer-key-MD5 ：オブジェクトの暗号化キーの MD5 ダイジェストを指定します。

指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に ' サーバ側の暗号化を使用の考慮事項を確認してください

ユーザメタデータ内の **UTF-8** 文字

StorageGRID は、ユーザ定義メタデータ内のエスケープされた UTF-8 文字を解析も解釈もしません。ユーザ定義メタデータにエスケープされた UTF-8 文字が含まれているオブジェクトに対して HEAD 要求を実行した場合、キーの名前または値に印刷不能文字が含まれていると、「 x-amz-missing -meta 」ヘッダーが返されません。

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。指定した場合は "XNotImplemented " が返されます。

- 「 x-amz-website redirect-location 」

クラウドストレージプールオブジェクトの応答ヘッダー

オブジェクトがクラウドストレージプールに格納されている場合（情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照）、次の応答ヘッダーが返されます。

- x-amz-storage-class ： Glacier
- x-amz-restore のように指定します

応答ヘッダーは、オブジェクトがクラウドストレージプールに移動され、必要に応じて読み出し不可能な状態に移行されてリストアされるときの状態に関する情報を提供します。

| オブジェクトの状態 | **HEAD Object** への応答 |
| --- | --- |
| StorageGRID に取り込まれているがまだ ILM によって評価されていないオブジェクト、または従来のストレージプールに格納されているオブジェクト、またはイレイジャーコーディングを使用しているオブジェクト | '200 OK' ( 特別な応答ヘッダーは返されません ) |
| クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない | 「 200 OK 」<br><br>x-amz-storage-class ： Glacier<br><br>x-amz-restore ： Ongoing - request="false" 、 expiry-date ="Sat 、 23 July 20 20203000:00:00:00GMT<br><br>オブジェクトが読み出し不可能な状態に移行されるまで、「 expiry-date 」の値は将来の日時に設定されます。移行の正確な時間は、 StorageGRID システムでは制御されません。 |

| オブジェクトの状態 | **HEAD Object** への応答 |
| --- | --- |
| オブジェクトが読み出し不可能な状態に移行したが、少なくとも 1 つのコピーがグリッドに存在する | 「 200 OK 」<br><br>x-amz-storage-class ： Glacier<br><br>x-amz-restore ： Ongoing - request="false" 、 expiry-date ="Sat 、 23 July 20 20203000:00:00:00GMT<br><br>「 expiry-date 」の値は、将来の日時に設定されます。<br><br>• 注：グリッド上のコピーを取得できない場合（ストレージノードが停止している場合など）は、オブジェクトを読み出す前に、問題 a POST Object restore 要求を実行してクラウドストレージプールからコピーをリストアする必要があります。 |
| 読み出し不可能な状態に移行しており、グリッドにコピーが存在しない | 「 200 OK 」<br><br>x-amz-storage-class ： Glacier |
| 読み出し不可能な状態からリストア中である | 「 200 OK 」<br><br>x-amz-storage-class ： Glacier<br><br>x-amz-restore ： Ongoing -request="true"` |
| クラウドストレージプールへのリストアが完了している | 「 200 OK 」<br><br>x-amz-storage-class ： Glacier<br><br>x-amz-restore ： ongoing -request="false" 、 expiry-date ="Sat, 23 July 20 2018 00:00:00:00 ： 00 GMT<br><br>「 expiry-date 」は、クラウドストレージプール内のオブジェクトが読み出し不可能な状態に戻るタイミングを示します。 |

クラウドストレージプール内のマルチパートオブジェクトまたはセグメント化されたオブジェクト

マルチパートオブジェクトをアップロードした場合や StorageGRID が大きなオブジェクトをセグメントに分割した場合、 StorageGRID はオブジェクトのパーツまたはセグメントのサブセットをサンプリングすることでクラウドストレージプール内のオブジェクトが使用可能かどうかを判断します。オブジェクトの一部のパートがすでに読み出し不可能な状態に移行されている場合や、オブジェクトの一部のパートがまだリストアされていない場合は、 HEAD Object 要求が誤って「 x-amz-restore ： ongoing-request="false" 」を返すことがあります。

バージョン管理

versionId サブリソースが指定されていない場合、バージョン管理されたバケット内のオブジェクトの最新バ

ージョンが取得されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「 Not Found 」ステータスが返され、「 x-amz-delete-marker` 応答ヘッダーは「 true 」に設定されます。

関連情報

サーバ側の暗号化を使用します

ILM を使用してオブジェクトを管理する

POST Object restore の実行

監査ログで追跡される S3 処理

## POST Object restore の実行

S3 POST Object restore 要求を使用して、クラウドストレージプールに格納されているオブジェクトをリストアできます。

### サポートされている要求タイプ

StorageGRID では、オブジェクトのリストアに POST Object restore 要求のみがサポートされます。SELECT タイプのリストアはサポートされていませんSELECT 要求は 'XNotImplemented を返します

### バージョン管理

バージョン管理されているバケット内のオブジェクトの特定のバージョンをリストアするには 'versionId' を指定します「 versionId 」を指定しない場合、オブジェクトの最新バージョンがリストアされます

### クラウドストレージプールオブジェクトでの **POST Object restore** の動作

オブジェクトがクラウドストレージプールに格納されている場合（情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照）、 POST Object restore 要求はオブジェクトの状態に基づいて次のように動作します。詳細については、「 head Object 」を参照してください。

> オブジェクトがクラウドストレージプールに格納され、かつそのオブジェクトのコピーがグリッドに 1 つ以上存在する場合は、 POST Object restore 要求を実行してオブジェクトをリストアする必要はありません。GET Object 要求を使用してローカルコピーを直接読み出すことができます。

| オブジェクトの状態 | **POST Object restore** の動作 |
| --- | --- |
| StorageGRID に取り込まれているがまだ ILM によって評価されていない、またはオブジェクトがクラウドストレージプールにない | 「 403 Forbidden 」、「 InvalidObjectState 」 |
| クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない | 「 200 OK 」変更は行われません。<br>• 注：オブジェクトが取得不可能な状態に移行される前に ' その 'expiry-date ' を変更することはできません |

| オブジェクトの状態 | **POST Object restore** の動作 |
| --- | --- |
| オブジェクトを読み出し不可能な状態に移行した | 「 202 Accepted 」は、要求の本文で指定された日数、オブジェクトの読み出し可能なコピーを Cloud Storage Pool にリストアします。この期間が終了すると、オブジェクトは読み出し不可能な状態に戻ります。<br><br>リストア・ジョブを完了するのにかかる時間（「 Expedited 」、「 Standard 」、または「 Bulk 」）を指定するには、「 Tier 」要求要素を使用します。Tier を指定しない場合 ' Standard 階層が使用されます<br><br>• 注意： S3 Glacier Deep Archive またはクラウドストレージプールに移行されたオブジェクトや、 Azure Blob Storage を使用するクラウドストレージは、「 Expedited 」階層を使用してリストアできません。次のエラーが返されます「 403 Forbidden 」 'InvalidTier ：このストレージクラスでは Retrieval オプションはサポートされていません」 |
| 読み出し不可能な状態からリストア中である | 409 Conflict`, RestoreAlreadyInProgress |
| クラウドストレージプールへのリストアが完了している | 「 200 OK 」<br><br>• 注意：オブジェクトが読み出し可能な状態にリストアされた場合は 'days' の新しい値で POST Object restore 要求を再発行することにより 'expiry-date を変更できます要求が実行された日時に基づいてリストア日が更新されます。 |

関連情報

ILM を使用してオブジェクトを管理する

HEAD Object の実行

監査ログで追跡される S3 処理

## PUT Object の場合

S3 PUT Object 要求を使用すると、オブジェクトをバケットに追加できます。

競合を解決します

同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「 latest-wins 」ベースで解決されます。「 latest-wins 」評価は、 S3 クライアントが処理を開始するタイミングではなく、 StorageGRID システムが特定の要求を完了したタイミングで行われます。

### オブジェクトのサイズ

単一 PUT Object 処理の maximum_recommended_size は 5GiB （ 5 、 368 、 709 、 120 バイト）です。5GB より大きいオブジェクトがある場合は、マルチパートアップロードを使用してください。

> StorageGRID 11.6 では、単一 PUT Object 処理の maximum_supported_size は 5TiB （ 5 、 497 、 558 、 138 、 880 バイト）です。ただし、 5GiB を超えるオブジェクトをアップロードしようとすると、 * S3 PUT Object size too large * アラートがトリガーされます。

### ユーザメタデータのサイズ

Amazon S3 では、各 PUT 要求ヘッダー内のユーザ定義メタデータのサイズが 2KB に制限されます。StorageGRID では、ユーザメタデータが 24KiB に制限されます。ユーザ定義のメタデータのサイズは、各キーと値の UTF-8 エンコードでのバイト数の合計で測定されます。

### ユーザメタデータ内の **UTF-8** 文字

要求のユーザ定義メタデータのキー名または値に（エスケープされていない） UTF-8 文字が含まれている場合、 StorageGRID の動作は定義されていません。

ユーザ定義メタデータのキー名または値に含まれているエスケープされた UTF-8 文字は、 StorageGRID で解析も解釈もされません。エスケープされた UTF-8 文字は ASCII 文字として扱われます。

- ユーザ定義メタデータにエスケープされた UTF-8 文字が含まれている場合、 PUT 、 PUT Object-Copy 、 GET 、 HEAD の各要求は正常に実行されます。
- キーの名前または値の解釈後の値に印刷不能文字が含まれている場合、 StorageGRID は「 x-amz-missing-meta 」ヘッダーを返しません。

### オブジェクトタグの制限

タグは、新しいオブジェクトをアップロードするときに追加することも、既存のオブジェクトに追加することもできます。StorageGRID と Amazon S3 はどちらも、オブジェクトごとに最大 10 個のタグをサポートします。オブジェクトに関連付けられたタグには、一意のタグキーが必要です。タグキーには Unicode 文字を 128 文字まで、タグ値には Unicode 文字を 256 文字まで使用できます。キーと値では大文字と小文字が区別されます。

### オブジェクトの所有権

StorageGRID では、非所有者アカウントまたは匿名ユーザによって作成されたオブジェクトを含むすべてのオブジェクトが、バケット所有者アカウントによって所有されます。

### サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- 「 Cache - Control 」を選択します
- 「 Content-Disposition 」
- 「コンテンツエンコーディング」

  「 Content-Encoding 」に「 aws-chunked 」を指定すると、次の項目が検証されません。

- StorageGRID では ' チャンク・シグネチャとチャンク・データの照合は行われません
- StorageGRID では、「 x-amz-decoded-content-length 」に指定した値がオブジェクトに対して検証されません。

- 「 Content - Language 」
- 「 Content-Length 」
- 「 Content-md5` 」
- 「 Content-Type 」
- 'expires'
- 「 Transfer-Encoding 」

  「 aws-chunked 」ペイロード署名も使用すると、チャンク転送エンコーディングがサポートされます。

- x-amz-meta- 。後ろに、ユーザ定義のメタデータを含む名前と値のペアを付加。

  ユーザ定義メタデータの名前と値のペアを指定する場合、一般的な形式は次のとおりです。

  ```
  x-amz-meta-name: value
  ```

  ILM ルールの参照時間として * User Defined Creation Time * オプションを使用する場合は、オブジェクトの作成時に記録されるメタデータの名前として「 creation-time 」を使用する必要があります。例：

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  'creation-time' の値は '1970 年 1 月 1 日以降の秒数として評価されます

  > ILM ルールで、参照時間に * User Defined Creation Time * と取り込み動作に Balanced オプションまたは Strict オプションの両方を使用することはできません。ILM ルールの作成時にエラーが返されます。

- x-amz-tagging`
- S3 Object Lock 要求のヘッダー
  - 「 x-amz-object-lock-mode 」です
  - x-amz-object-lock-retain-until -date' のように指定します
  - 「 x-amz-object-lock-legal hold' 」のようになります

    これらのヘッダーがない状態で要求を送信した場合、バケットのデフォルトの保持設定を使用して、オブジェクトバージョンの retain-date が計算されます。

  S3 オブジェクトロックを使用する

- SSE 要求ヘッダー：
  - 「 x-amz-server-side-encryption 」です

- 「 x-amz-server-side-encryption-customer-key-MD5 」
- 「 x-amz-server-side-encryption-customer-key 」
- 「 x-amz-server-side-encryption-customer-algorithm 」を実行します

  を参照してください [サーバ側の暗号化を行うための要求ヘッダー]

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。

- x-amz-acl' 要求ヘッダーはサポートされていません
- 「 x-amz-website redirect-location 」要求ヘッダーはサポートされていません。「 XNotImplemented 」を返します。

ストレージクラスのオプション

x-amz-storage-class' 要求ヘッダーがサポートされています。x-amz-storage-class で送信される値は StorageGRID が取り込み中にオブジェクトデータを保護する方法に影響し、 StorageGRID システムに格納されるオブジェクトの永続的コピーの数（ ILM で決定）には影響しません。

取り込まれたオブジェクトに一致する ILM ルールの取り込み動作が Strict オプションに指定されている場合、x-amz-storage-class ヘッダーの値は無視されます。

x-amz-storage-class には次の値を使用できます。

- 'standard' （デフォルト）
  - * Dual commit * ： ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み直後にオブジェクトの 2 つ目のコピーが作成されて別のストレージノードに配置されます（デュアルコミット）。ILM が評価されると、この初期中間コピーがルールの配置手順を満たしているかどうかを StorageGRID が判断します。満たしていない場合は、新しいオブジェクトコピーを別の場所に作成し、初期中間コピーを削除することが必要になる可能性があります。
  - * Balanced * ： ILM ルールで Balanced オプションが指定されていて、ルールで指定されたすべてのコピーを StorageGRID がただちに作成できない場合、 StorageGRID は 2 つの中間コピーを別々のストレージノードに作成します。

    StorageGRID が ILM ルールで指定されたすべてのオブジェクトコピーをただちに作成できる（同期配置）場合、「 x-amz-storage-class 」ヘッダーは無視されます。
- 「 reduced_redundancy 」
  - * Dual commit * ： ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み時に StorageGRID が中間コピーを 1 つ作成します（シングルコミット）。
  - * Balanced * ： ILM ルールで Balanced オプションが指定されている場合、 StorageGRID は、ルールで指定されたすべてのコピーをただちに作成できない場合にのみ、中間コピーを 1 つ作成します。StorageGRID で同期配置を実行できる場合、このヘッダーは効果がありません。オブジェクトに一致する ILM ルールが単一のレプリケートコピーを作成する場合は、「 reduced_redundancy 」オプションの使用を推奨します。この場合 'reduced_redundancy</1> を使用すると ' すべての取り込み操作で余分なオブジェクト・コピーを不要に作成および削除する必要がなくなります

  他の状況では 'reduced_redundancy</1> オプションを使用することは推奨されません「

reduced_redundancy 」を使用すると、取り込み中にオブジェクトデータが失われるリスクが高まります。たとえば、 ILM 評価の前にコピーが 1 つだけ格納されていたストレージノードに障害が発生すると、データが失われる可能性があります。

- 注意 * ：一定期間にレプリケートされたコピーを 1 つだけ保持すると、データが永久に失われる危険があります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

「 reduced_redundancy 」を指定した場合は、オブジェクトを最初に取り込むときに作成されるコピー数のみに影響します。オブジェクトがアクティブな ILM ポリシーで評価される際に作成されるオブジェクトのコピー数には影響せず、 StorageGRID システムでデータが格納されるときの冗長性レベルが低下することもありません。

- 注 * ： S3 オブジェクトロックが有効な状態でオブジェクトをバケットに取り込む場合、「 REDUCED_REDUNDANCY 」オプションは無視されます。オブジェクトをレガシー準拠バケットに取り込む場合、「 reduced_redundancy 」オプションはエラーを返します。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

サーバ側の暗号化を行うための要求ヘッダー

オブジェクトをサーバ側の暗号化で暗号化するには、次の要求ヘッダーを使用します。SSE オプションと SSE-C オプションを同時に指定することはできません。

- * SSE * ： StorageGRID で管理される一意のキーでオブジェクトを暗号化するには、次のヘッダーを使用します。
  - 「 x-amz-server-side-encryption 」です
- * SSE-C * ：ユーザが指定および管理する一意のキーでオブジェクトを暗号化する場合は、次の 3 つのヘッダーをすべて使用します。
  - 「 x-amz-server-side-encryption-customer-algorithm 」：「 AES256 」を指定します。
  - x-amz-server-side-encryption-customer-key ：新しいオブジェクトの暗号化キーを指定します。
  - x-amz-server-side-encryption-customer-key-MD5 ：新しいオブジェクトの暗号化キーの MD5 ダイジェストを指定します。
- 注意： * 指定した暗号化キーは保存されません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に ' サーバ側の暗号化を使用の考慮事項を確認してください
- 注： SSE または SSE-C で暗号化されたオブジェクトは、バケットレベルまたはグリッドレベルの暗号化設定が無視されます。

バージョン管理

バケットでバージョン管理が有効になっている場合、格納されるオブジェクトのバージョンごとに一意の「 versionID 」が自動的に生成されます。この 'versionId' は 'x-amz-version-id' 応答ヘッダーを使用した応答でも返されます

バージョン管理が一時停止されている場合、オブジェクトのバージョンは null の「 versionID 」で格納され、 null のバージョンがすでに存在する場合は上書きされます。

関連情報

ILM を使用してオブジェクトを管理する

バケットの処理

監査ログで追跡される S3 処理

サーバ側の暗号化を使用します

クライアント接続の設定方法

## PUT Object - Copy の各コマンドを実行します

S3 PUT Object - Copy 要求を使用すると、すでに S3 に格納されているオブジェクトのコピーを作成できます。PUT Object - Copy 処理は、 GET を実行してから PUT を実行する処理と同じです。

### 競合を解決します

同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「 latest-wins 」ベースで解決されます。「 latest-wins 」評価は、 S3 クライアントが処理を開始するタイミングではなく、 StorageGRID システムが特定の要求を完了したタイミングで行われます。

### オブジェクトのサイズ

単一 PUT Object 処理の maximum_recommended_size は 5GiB （ 5 、 368 、 709 、 120 バイト）です。5GB より大きいオブジェクトがある場合は、マルチパートアップロードを使用してください。

> StorageGRID 11.6 では、単一 PUT Object 処理の maximum_supported_size は 5TiB （ 5 、 497 、 558 、 138 、 880 バイト）です。ただし、 5GiB を超えるオブジェクトをアップロードしようとすると、 * S3 PUT Object size too large * アラートがトリガーされます。

### ユーザメタデータ内の **UTF-8** 文字

要求のユーザ定義メタデータのキー名または値に（エスケープされていない） UTF-8 文字が含まれている場合、 StorageGRID の動作は定義されていません。

ユーザ定義メタデータのキー名または値に含まれているエスケープされた UTF-8 文字は、 StorageGRID で解析も解釈もされません。エスケープされた UTF-8 文字は ASCII 文字として扱われます。

- ユーザ定義メタデータにエスケープされた UTF-8 文字が含まれている場合、要求は正常に実行されます。
- キーの名前または値の解釈後の値に印刷不能文字が含まれている場合、 StorageGRID は「 x-amz-missing-meta 」ヘッダーを返しません。

### サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- 「 Content-Type 」
- 「 x-amz-copy-source 」

- x-amz-copy-source-if-match
- x-amz-copy-source-if-none-match
- 「 x-amz-copy-source-if-unmodified-since 」です
- x-amz-copy-source-if-modified-since
- x-amz-meta- 。後ろに、ユーザ定義のメタデータを含む名前と値のペアを付加
- x-amz-metadata-directive ：デフォルト値は「 copy 」です。この場合、オブジェクトおよび関連するメタデータをコピーできます。

  オブジェクトのコピー時に既存のメタデータを上書きする場合は 'replace' を指定し ' オブジェクトのメタデータを更新する場合は 'replace' を指定します

- x-amz-storage-class'
- x-amz-tagging-directive ：デフォルト値は「 copy 」です。この場合、オブジェクトとすべてのタグをコピーできます。

  オブジェクトをコピーするときに既存のタグを上書きする場合 ' またはタグを更新する場合は 'replace' を指定できます

- S3 オブジェクトロック要求のヘッダー：
  - 「 x-amz-object-lock-mode 」です
  - x-amz-object-lock-retain-until -date' のように指定します
  - 「 x-amz-object-lock-legal hold' 」のようになります

    これらのヘッダーがない状態で要求を送信した場合、バケットのデフォルトの保持設定を使用して、オブジェクトバージョンの retain-date が計算されます。

  S3 オブジェクトロックを使用する

- SSE 要求ヘッダー：
  - x-amz-copy-sourcemalse-server-sideAlgorithme-encryption.Algorithmy-customer-algorithm 」のように指定します
  - x-amz-copy-sourceSourcedming-ser-encryption-customer-key のようになります
  - x-amz-copy-source Sourcedmings-server-side-encryption-customer-key-MD5
  - 「 x-amz-server-side-encryption 」です
  - 「 x-amz-server-side-encryption-customer-key-MD5 」
  - 「 x-amz-server-side-encryption-customer-key 」
  - 「 x-amz-server-side-encryption-customer-algorithm 」を実行します

    を参照してください [サーバ側の暗号化を行うための要求ヘッダー]

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。

- 「 Cache - Control 」を選択します
- 「 Content-Disposition 」
- 「コンテンツエンコーディング」
- 「 Content - Language 」
- 'expires'
- 「 x-amz-website redirect-location 」

ストレージクラスのオプション

x-amz-storage-class' 要求ヘッダーがサポートされています。一致する ILM ルールで取り込み動作に Dual commit または Balanced が指定されている場合に StorageGRID で作成されるオブジェクトコピーの数に影響します

- 「 standard 」

  （デフォルト） ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、デュアルコミットの取り込み処理を指定します。

- 「 reduced_redundancy 」

  ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、シングルコミットの取り込み処理を指定します。

  S3 オブジェクトロックが有効な状態でオブジェクトをバケットに取り込む場合、「 REDUCED_REDUNDANCY 」オプションは無視されます。オブジェクトをレガシー準拠バケットに取り込む場合、「 reduced_redundancy 」オプションはエラーを返します。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

**PUT Object - Copy** で **x-amz-copy-source** を使用しています

「 x-amz-copy-source 」のヘッダーで指定されたソースのバケットおよびキーがデスティネーションのバケットおよびキーと異なる場合は、ソースのオブジェクトデータのコピーがデスティネーションに書き込まれます。

ソースとデスティネーションが一致し、「 x-amz-metadata-directive 」ヘッダーで「 replace 」が指定されている場合は、要求で指定されたメタデータの値がオブジェクトのメタデータに更新されます。この場合、StorageGRID はオブジェクトを再取り込みしません。これには 2 つの重要な結果があります。

- PUT Object - Copy を使用して既存のオブジェクトを暗号化したり、既存のオブジェクトの暗号化を変更したりすることはできません。「 x-amz-server-side-encryption' ヘッダーまたは「 x-amz-server-side-encryption-customer-algorithm 」ヘッダーを指定した場合、 StorageGRID は要求を拒否し、「 XNotImplemented 」を返します。
- 一致する ILM ルールで指定されている取り込み動作のオプションが使用されません。更新によって発生したオブジェクト配置の変更は、通常のバックグラウンド ILM プロセスで ILM が再評価されるときに実施されます。

  このため、 ILM ルールの取り込み動作に Strict オプションが指定されている場合、必要なオブジェクト配置を実行できないと（たとえば、新たに必要となった場所を使用できない場合）、アクションは実行され

ません。更新されたオブジェクトは、必要な配置を実行可能になるまで現在の配置が維持されます。

サーバ側の暗号化を行うための要求ヘッダー

サーバ側の暗号化を使用する場合は、ソースオブジェクトが暗号化されているかどうか、およびターゲットオブジェクトを暗号化するかどうかによって、指定する要求ヘッダーが異なります。

- ソースオブジェクトがユーザ指定のキーを使用して暗号化されている場合（ SSE-C ）は、オブジェクトを復号化してコピーできるように、 PUT Object - Copy 要求に次の 3 つのヘッダーを含める必要があります。
  - x-amz-copy-sourcemalgebals-server-sideAlgorithmebals-encryptedユーザ ・アルゴリズム「 AES256 」を指定します。
  - x-amz-copy-source Sourcedming-ser-encryption-customer-key 「ソースオブジェクトの作成時に指定した暗号化キーを指定します。
  - x-amz-copy-source Sourcedgals-server-side-encryption-customer-key-MD5 ：ソースオブジェクトの作成時に指定した MD5 ダイジェストを指定します。
- ユーザが指定および管理する一意のキーでターゲットオブジェクト（コピー）を暗号化する場合は、次の 3 つのヘッダーを含めます。
  - 「 x-amz-server-side-encryption-customer-algorithm 」：「 AES256 」を指定します。
  - x-amz-server-side-encryption-customer-key ：ターゲットオブジェクト用の新しい暗号化キーを指定します。
  - x-amz-server-side-encryption-customer-key-MD5 ：新しい暗号化キーの MD5 ダイジェストを指定します。
- 注意： * 指定した暗号化キーは保存されません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に ' サーバ側の暗号化を使用の考慮事項を確認してください
- StorageGRID で管理される一意のキーでターゲットオブジェクト（コピー）を暗号化する（ SSE ）には、 PUT Object - Copy 要求に次のヘッダーを含めます。
  - 「 x-amz-server-side-encryption 」です
- 注意： * オブジェクトの「 server-side-encryption 」の値は更新できません。代わりに 'x-amz-metadata-directive: 'replace' を使用して ' 新しい 'server-side-encryption' 値をコピーします

バージョン管理

ソースバケットでバージョン管理が有効になっている場合は、「 x-amz-copy-source 」ヘッダーを使用してオブジェクトの最新バージョンをコピーできます。オブジェクトの特定のバージョンをコピーするには、コピーするバージョンを versionId サブリソースを使用して明示的に指定する必要があります。デスティネーションのバケットでバージョン管理が有効になっている場合は、生成されたバージョンが「 x-amz-version-id 」応答ヘッダーで返されます。ターゲットバケットのバージョン管理が一時停止されている場合 'x-amz-version-id' は Null 値を返します

関連情報

ILM を使用してオブジェクトを管理する

サーバ側の暗号化を使用します

監査ログで追跡される S3 処理

PUT Object の場合

## SelectObjectContent の順に選択します

S3 SelectObjectContent 要求を使用すると、シンプルな SQL ステートメントに基づいて S3 オブジェクトのコンテンツをフィルタリングできます。

詳細については、を参照してください "SelectObjectContent に関する AWS ドキュメント"。

必要なもの

- テナントアカウントには S3 Select 権限が割り当てられます。
- 照会するオブジェクトの 's3:GetObject' のアクセス権があります
- 照会するオブジェクトは CSV 形式であるか、 CSV 形式のファイルを含む GZIP または bzip2 圧縮ファイルです。
- SQL 式の最大長は 256KB です。
- 入力または結果のすべてのレコードの最大長は 1MiB です。

要求の構文例

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

**SQL** クエリの例

このクエリは、州名、 2010 年人口、 2015 年推定人口、米国の人口調査データからの変化率を取得します。状態以外のファイル内のレコードは無視されます。

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

照会するファイルの最初の数行「 sub-est2020_all.csv 」は、次のようになります。

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

**AWS- CLI** の使用例

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

出力ファイルの最初の数行である「 changes.csv 」は、次のようになります。

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

# マルチパートアップロードの処理

## このセクションでは、 StorageGRID でのマルチパートアップロードの処理のサポートについて説明します。

マルチパートアップロードのすべての処理に、次の条件と注意事項が適用されます。

- 1 つのバケットに対して同時に実行するマルチパートアップロードが 1 、 000 件を超えないようにしてください。 1 、 000 件を超えると、そのバケットに対する List Multipart Uploads のクエリで完全な結果が返されないことがあります。
- StorageGRID は、マルチパートに AWS のサイズ制限を適用します。S3 クライアントは次のガイドラインに従う必要があります。
  - マルチパートアップロードの各パートのサイズは 5MiB （ 5 、 242 、 880 バイト）と 5GiB （ 5 、 368 、 709 、 120 バイト）の間にする必要があります。
  - 最後の部分は 5MiB （ 5,242,880 バイト）より小さくできます。
  - 一般に、パーツサイズはできるだけ大きくする必要があります。たとえば、 100GiB オブジェクトの場合、 5GB のパートサイズを使用します。各パートは固有のオブジェクトとみなされるため、大きなパートサイズを使用すると、 StorageGRID のメタデータのオーバーヘッドが軽減されます。
  - 5GB 未満のオブジェクトでは、マルチパートではないアップロードの使用を検討してください。
- ILM ルールの取り込み動作が Strict または Balanced に指定されている場合は、マルチパートオブジェクトの各パートが取り込まれるときに ILM が評価され、マルチパートアップロードが完了したときにオブジェクト全体に対して ILM が評価されます。これがオブジェクトとパートの配置にどのように影響するかに注意する必要があります。
  - S3 マルチパートアップロードの進行中に ILM が変更されると、マルチパートアップロードが完了した時点でオブジェクトの一部のパートが現在の ILM 要件を満たしていないことがあります。正しく配置されていないパートは ILM ルールによる再評価の対象としてキューに登録され、あとで正しい場所に移動されます。
  - パートに対して ILM を評価する際、 StorageGRID はオブジェクトのサイズではなくパートのサイズでフィルタリングします。つまり、オブジェクト全体としては ILM 要件を満たしていない場所にオブジェクトのパーツが格納される可能性があります。たとえば、 10GB 以上のオブジェクトをすべて DC1 に格納し、それより小さいオブジェクトをすべて DC2 に格納するルールの場合、 10 パートからなるマルチパートアップロードの 1GB の各パートは取り込み時に DC2 に格納されます。オブジェクト全体に対して ILM が評価されると、オブジェクトのすべてのパートが DC1 に移動されます。
- マルチパートアップロードでは、すべての処理で StorageGRID の整合性制御がサポートされます。
- マルチパートアップロードでは、必要に応じてサーバ側の暗号化を使用できます。SSE （ StorageGRID で管理されるキーによるサーバ側の暗号化）を使用するには、 Initiate Multipart Upload 要求にのみ「 x-amz-server-side-encryption 」要求ヘッダーを指定します。SSE-C （ユーザ指定のキーによるサーバ側の

暗号化）を使用する場合は、 Initiate Multipart Upload 要求と後続の各 Upload Part 要求に、同じ 3 つの暗号化キー要求ヘッダーを指定します。

| 操作 | 実装 |
| --- | --- |
| マルチパートアップロードをリストします | を参照してください マルチパートアップロードをリストします |
| マルチパートアップロードを開始します | を参照してください マルチパートアップロードを開始します |
| パーツをアップロードします | を参照してください パーツをアップロードします |
| パーツのアップロード - コピー | を参照してください パーツのアップロード - コピー |
| Complete Multipart Upload の実行 | を参照してください Complete Multipart Upload の実行 |
| マルチパートアップロードを中止します | Amazon S3 REST API のすべての動作が実装されています |
| パーツをリストします | Amazon S3 REST API のすべての動作が実装されています |

関連情報

- 整合性制御
- サーバ側の暗号化を使用します

## マルチパートアップロードをリストします

List Multipart Uploads 処理では、バケットの進行中のマルチパートアップロードがリストされます。

次の要求パラメータがサポートされています。

- 「 encoding-type 」
- 「 max-uploads 」を参照してください
- 「キーマーカー」
- 「 prefix 」
- 「 upload-id - marker 」のように指定します

「 delimiter 」要求パラメータはサポートされていません。

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。Complete Multipart Upload 処理が実行されると、オブジェクトが作成される時点（およびバージョン管理されている場合）になります。

## マルチパートアップロードを開始します

## Initiate Multipart Upload 処理は、オブジェクトのマルチパートアップロードを開始し、アップロード ID を返します。

x-amz-storage-class' 要求ヘッダーがサポートされています。x-amz-storage-class で送信される値は StorageGRID が取り込み中にオブジェクトデータを保護する方法に影響し、 StorageGRID システムに格納されるオブジェクトの永続的コピーの数（ ILM で決定）には影響しません。

取り込まれたオブジェクトに一致する ILM ルールの取り込み動作が Strict オプションに指定されている場合、x-amz-storage-class ヘッダーの値は無視されます。

x-amz-storage-class には次の値を使用できます。

- 'standard' （デフォルト）
  - * Dual commit * ： ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み直後にオブジェクトの 2 つ目のコピーが作成されて別のストレージノードに配置されます（デュアルコミット）。ILM が評価されると、この初期中間コピーがルールの配置手順を満たしているかどうかを StorageGRID が判断します。満たしていない場合は、新しいオブジェクトコピーを別の場所に作成し、初期中間コピーを削除することが必要になる可能性があります。
  - * Balanced * ： ILM ルールで Balanced オプションが指定されていて、ルールで指定されたすべてのコピーを StorageGRID がただちに作成できない場合、 StorageGRID は 2 つの中間コピーを別々のストレージノードに作成します。

    StorageGRID が ILM ルールで指定されたすべてのオブジェクトコピーをただちに作成できる（同期配置）場合、「 x-amz-storage-class 」ヘッダーは無視されます。
- 「 reduced_redundancy 」
  - * Dual commit * ： ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み時に StorageGRID が中間コピーを 1 つ作成します（シングルコミット）。
  - * Balanced * ： ILM ルールで Balanced オプションが指定されている場合、 StorageGRID は、ルールで指定されたすべてのコピーをただちに作成できない場合にのみ、中間コピーを 1 つ作成します。StorageGRID で同期配置を実行できる場合、このヘッダーは効果がありません。オブジェクトに一致する ILM ルールが単一のレプリケートコピーを作成する場合は、「 reduced_redundancy 」オプションの使用を推奨します。この場合 'reduced_redundancy</1> を使用すると ' すべての取り込み操作で余分なオブジェクト・コピーを不要に作成および削除する必要がなくなります

  他の状況では 'reduced_redundancy</1> オプションを使用することは推奨されません「 reduced_redundancy 」を使用すると、取り込み中にオブジェクトデータが失われるリスクが高まります。たとえば、 ILM 評価の前にコピーが 1 つだけ格納されていたストレージノードに障害が発生すると、データが失われる可能性があります。
- 注意 * ：一定期間にレプリケートされたコピーを 1 つだけ保持すると、データが永久に失われる危険があります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生した

り、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

「 reduced_redundancy 」を指定した場合は、オブジェクトを最初に取り込むときに作成されるコピー数のみに影響します。オブジェクトがアクティブな ILM ポリシーで評価される際に作成されるオブジェクトのコピー数には影響せず、 StorageGRID システムでデータが格納されるときの冗長性レベルが低下することもありません。

- 注 * ： S3 オブジェクトロックが有効な状態でオブジェクトをバケットに取り込む場合、「 REDUCED_REDUNDANCY 」オプションは無視されます。オブジェクトをレガシー準拠バケットに取り込む場合、「 reduced_redundancy 」オプションはエラーを返します。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

次の要求ヘッダーがサポートされています。

- 「 Content-Type 」
- x-amz-meta- 。後ろに、ユーザ定義のメタデータを含む名前と値のペアを付加

  ユーザ定義メタデータの名前と値のペアを指定する場合、一般的な形式は次のとおりです。

  ```
  x-amz-meta-_name_: `value`
  ```

  ILM ルールの参照時間として * User Defined Creation Time * オプションを使用する場合は、オブジェクトの作成時に記録されるメタデータの名前として「 creation-time 」を使用する必要があります。例：

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  'creation-time' の値は '1970 年 1 月 1 日以降の秒数として評価されます

  > レガシーコンプライアンスが有効になっているバケットにオブジェクトを追加する場合 ' ユーザー定義のメタデータとして 'creation-time' を追加することはできませんエラーが返されます。

- S3 オブジェクトロック要求のヘッダー：
  - 「 x-amz-object-lock-mode 」です
  - x-amz-object-lock-retain-until -date' のように指定します
  - 「 x-amz-object-lock-legal hold' 」のようになります

    これらのヘッダーがない状態で要求を送信した場合、バケットのデフォルトの保持設定を使用して、オブジェクトバージョンの retain-date が計算されます。

  S3 オブジェクトロックを使用する

- SSE 要求ヘッダー：
  - 「 x-amz-server-side-encryption 」です

- 「 x-amz-server-side-encryption-customer-key-MD5 」
- 「 x-amz-server-side-encryption-customer-key 」
- 「 x-amz-server-side-encryption-customer-algorithm 」を実行します

[サーバ側の暗号化を行うための要求ヘッダー]

StorageGRID での UTF-8 文字の処理については、 PUT Object に関するドキュメントを参照してください。

サーバ側の暗号化を行うための要求ヘッダー

マルチパートオブジェクトをサーバ側の暗号化で暗号化するには、次の要求ヘッダーを使用します。SSE オプションと SSE-C オプションを同時に指定することはできません。

- * SSE * ： StorageGRID で管理される一意のキーでオブジェクトを暗号化する場合は、 Initiate Multipart Upload 要求で次のヘッダーを使用します。Upload Part 要求ではこのヘッダーを指定しないでください。
  - 「 x-amz-server-side-encryption 」です
- * SSE-C * ：ユーザが指定および管理する一意のキーでオブジェクトを暗号化する場合は、 Initiate Multipart Upload 要求（および後続の各 Upload Part 要求）で、次の 3 つのヘッダーをすべて使用します。
  - 「 x-amz-server-side-encryption-customer-algorithm 」：「 AES256 」を指定します。
  - x-amz-server-side-encryption-customer-key ：新しいオブジェクトの暗号化キーを指定します。
  - x-amz-server-side-encryption-customer-key-MD5 ：新しいオブジェクトの暗号化キーの MD5 ダイジェストを指定します。
- 注意： * 指定した暗号化キーは保存されません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に ' サーバ側の暗号化を使用の考慮事項を確認してください

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていませんまた 'XNotImplemented が返されます

- 「 x-amz-website redirect-location 」

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。Complete Multipart Upload 処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

関連情報

ILM を使用してオブジェクトを管理する

サーバ側の暗号化を使用します

PUT Object の場合

## パーツをアップロードします

### Upload Part 処理では、オブジェクトのマルチパートアップロード内のパートがアップロードされます。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- 「 Content-Length 」
- 「 Content-md5` 」

サーバ側の暗号化を行うための要求ヘッダー

Initiate Multipart Upload 要求に SSE-C 暗号化を指定した場合は、各 Upload Part 要求に次の要求ヘッダーも含める必要があります。

- 「 x-amz-server-side-encryption-customer-algorithm 」：「 AES256 」を指定します。
- x-amz-server-side-encryption-customer-key ： Initiate Multipart Upload 要求で指定した暗号化キーを指定します。
- x-amz-server-side-encryption-customer-key-MD5 ： Initiate Multipart Upload 要求で指定した MD5 ダイジェストを指定します。

> ⓘ 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に ' サーバ側の暗号化を使用の考慮事項を確認してください

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。Complete Multipart Upload 処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

関連情報

サーバ側の暗号化を使用します

## パーツのアップロード - コピー

### Upload Part - Copy 処理は、データソースとしての既存のオブジェクトからデータをコピーすることで、オブジェクトのパートをアップロードします。

Upload Part - Copy 処理には、すべての Amazon S3 REST API の動作が実装されています。

この要求は、 StorageGRID システム内の「 x-amz-copy-source-range 」で指定されたオブジェクトデータの読み取りと書き込みを行います。

次の要求ヘッダーがサポートされています。

- x-amz-copy-source-if-match
- x-amz-copy-source-if-none-match
- 「 x-amz-copy-source-if-unmodified-since 」です
- x-amz-copy-source-if-modified-since

サーバ側の暗号化を行うための要求ヘッダー

Initiate Multipart Upload 要求に SSE-C 暗号化を指定した場合は、各 Upload Part - Copy 要求に次の要求ヘッダーも含める必要があります。

- 「 x-amz-server-side-encryption-customer-algorithm 」：「 AES256 」を指定します。
- x-amz-server-side-encryption-customer-key ： Initiate Multipart Upload 要求で指定した暗号化キーを指定します。
- x-amz-server-side-encryption-customer-key-MD5 ： Initiate Multipart Upload 要求で指定した MD5 ダイジェストを指定します。

ソースオブジェクトがユーザ指定のキーを使用して暗号化されている場合（ SSE-C ）は、オブジェクトを復号化してコピーできるように、 Upload Part - Copy 要求に次の 3 つのヘッダーを含める必要があります。

- x-amz-copy-sourcemalgebals-server-sideAlgorithmebals-encryptionmed-center-algorithm ：「 256 」を指定します。
- x-amz-copy-source Sourcedming-ser-encryption-customer-key ：ソースオブジェクトの作成時に指定した暗号化キーを指定します。
- x-amz-copy-source Sourcedgals-server-side-encryption-customer-key-MD5 ：ソースオブジェクトの作成時に指定した MD5 ダイジェストを指定します。

> 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に ' サーバ側の暗号化を使用の考慮事項を確認してください

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。Complete Multipart Upload 処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

## Complete Multipart Upload の実行

Complete Multipart Upload 処理では、以前にアップロードされたパートをアセンブルすることで、オブジェクトのマルチパートアップロードを完了します。

競合を解決します

同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「 latest-wins 」ベースで解決されます。「 latest-wins 」評価は、 S3 クライアントが処理を開始するタイミングではなく、 StorageGRID システムが特定の要求を完了したタイミングで行われます。

要求ヘッダー

x-amz-storage-class' 要求ヘッダーがサポートされています。一致する ILM ルールで取り込み動作に Dual commit または Balanced が指定されている場合に StorageGRID で作成されるオブジェクトコピーの数に影響します

- 「 standard 」

  （デフォルト） ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、デュアルコミットの取り込み処理を指定します。

- 「 reduced_redundancy 」

  ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、シングルコミットの取り込み処理を指定します。

  S3 オブジェクトロックが有効な状態でオブジェクトをバケットに取り込む場合、「 REDUCED_REDUNDANCY 」オプションは無視されます。オブジェクトをレガシー準拠バケットに取り込む場合、「 reduced_redundancy 」オプションはエラーを返します。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

マルチパートアップロードが 15 日以内に完了しないと、非アクティブな処理としてマークされ、関連するすべてのデータがシステムから削除されます。

返される「 ETag 」の値は、データの MD5 サムではなく、 Amazon S3 API のマルチパートオブジェクト用の「 ETag 」値の実装に従います。

バージョン管理

マルチパートアップロードは、この処理で完了します。バケットでバージョン管理が有効になっている場合は、マルチパートアップロードの完了時にオブジェクトのバージョンが作成されます。

バケットでバージョン管理が有効になっている場合、格納されるオブジェクトのバージョンごとに一意の「 versionID 」が自動的に生成されます。この 'versionId' は 'x-amz-version-id' 応答ヘッダーを使用した応答でも返されます

バージョン管理が一時停止されている場合、オブジェクトのバージョンは null の「 versionID 」で格納され、null のバージョンがすでに存在する場合は上書きされます。

バケットでバージョン管理が有効になっているときは、同じオブジェクトキーで同時に複数のマルチパートアップロードが実行されている場合でも、マルチパートアップロードが完了するたびに常に新しいバージョンが作成されます。バケットでバージョン管理が有効になっていないときは、マルチパートアップロードの開始後に、同じオブジェクトキーで別のマルチパートアップロードが開始されて先に完了することがあります。バージョン管理が有効になっていないバケットでは、最後に完了したマルチパートアップロードが優先されます。

レプリケーション、通知、またはメタデータ通知に失敗しました

マルチパートアップロードが行われるバケットでプラットフォームサービスが設定されている場合、関連する

レプリケーション操作や通知操作が失敗してもマルチパートアップロードは正常に実行されます。

この状況が発生すると、 Total Events （ SMTT ）のアラームがグリッドマネージャで生成されます。Last Event メッセージに、通知が失敗した最後のオブジェクトについて、「 Failed to publish notifications for bucket-name object key 」と表示されます。（このメッセージを表示するには、 * nodes * > * _ Storage Node_* > * Events * を選択します。表の一番上に Last Event が表示されます）。 イベント・メッセージは /var/local/log/bycast-err.log にも表示されます

テナントでは、オブジェクトのメタデータまたはタグを更新することで、失敗したレプリケーションまたは通知をトリガーできます。テナントでは、既存の値を再送信し、不要な変更を回避できます。

関連情報

ILM を使用してオブジェクトを管理する

# エラー応答

StorageGRID システムでは、該当する S3 REST API の標準のエラー応答をすべてサポートしています。また、 StorageGRID の実装では、カスタム応答もいくつか追加されています。

## サポートされている **S3 API** のエラーコード

| 名前 | **HTTP** ステータス |
| --- | --- |
| アクセスが拒否されました | 403 禁止 |
| BadDigest の略 | 400 不正な要求です |
| BucketAlreadyExists のようになりました | 409 競合 |
| BucketNotEmpty のように入力します | 409 競合 |
| IncompleteBody | 400 不正な要求です |
| 内部エラー | 500 Internal Server Error （内部サーバエラー） |
| InvalidAccessKeyId | 403 禁止 |
| アンヴァリッドドキュメント | 400 不正な要求です |
| InvalidBucketName の略 | 400 不正な要求です |
| InvalidBucketState の場合 | 409 競合 |
| InvalidDigest の略 | 400 不正な要求です |

| 名前 | **HTTP** ステータス |
| --- | --- |
| InvalidEncryptionAlgorithmError | 400 不正な要求です |
| InvalidPart | 400 不正な要求です |
| InvalidPartOrder | 400 不正な要求です |
| InvalidRange ：無効な範囲 | 416 リクエストされた範囲が適合しません |
| InvalidRequest | 400 不正な要求です |
| InvalidStorageClass | 400 不正な要求です |
| InvalidTag | 400 不正な要求です |
| InvalidURI | 400 不正な要求です |
| KeyTooLong の 2 つのグループがあります | 400 不正な要求です |
| MalformedXML の場合 | 400 不正な要求です |
| MetadataTooLarge | 400 不正な要求です |
| MethodNotAllowed のように入力します | 405 メソッドは許可されていません |
| MissingContentLength （ MissingContentLength ） | 411 長さが必要です |
| MissingRequestBodyError | 400 不正な要求です |
| MissingSecurityHeader | 400 不正な要求です |
| NoSuchBucket | 404 が見つかりません |
| NoSuchKey | 404 が見つかりません |
| NoSuchUpload | 404 が見つかりません |
| 実装なし | 501 は実装されていません |
| NoSuchBucketPolicy のようになります | 404 が見つかりません |
| ObjectLockConfigurationNotFoundError | 404 が見つかりません |

| 名前 | **HTTP** ステータス |
| --- | --- |
| PreconditionalFailed | 412 事前条件が失敗しました |
| RequestTimeTooSkewed | 403 禁止 |
| サービスを利用できません | 503 Service Unavailable （ 503 サービスが利用でき |
| SignatureDoesNotMatch のように指定します | 403 禁止 |
| TooManyBuckets | 400 不正な要求です |
| UserKeyMustBeSpecified | 400 不正な要求です |

## StorageGRID カスタムのエラーコード

| 名前 | 説明 | **HTTP** ステータス |
| --- | --- | --- |
| XBucketLifecycleNotAllowed のようになりました | バケットライフサイクル設定は従来の準拠バケットには適用されません | 400 不正な要求です |
| XBucketPolicyParseException | 受信したバケットポリシー JSON を解析できませんでした。 | 400 不正な要求です |
| XCompliConflict | 準拠設定が古いため、処理が拒否されました。 | 403 禁止 |
| XCompliReducedRedundancyForbidden | レガシー準拠バケットでは冗長性の低下は許可されません | 400 不正な要求です |
| XMaxBucketPolicyLengthExceeded （ XMaxBucketLengthExceeded ） | ポリシーが許容される最大バケットポリシー長を超えています。 | 400 不正な要求です |
| XMissingInternalRequestHeader | 内部要求のヘッダーがありません。 | 400 不正な要求です |
| XNoSuchBucketCompliance です | 指定したバケットで従来の準拠が有効になっていません。 | 404 が見つかりません |
| XNotAcceptable | 要求に含まれている Accept ヘッダーの 1 つ以上を満たすことができませんでした。 | 406 は許容されません |

| 名前 | 説明 | **HTTP** ステータス |
| --- | --- | --- |
| XNotImplemented | 指定した要求の処理には、実装されていない機能が含まれます。 | 501 は実装されていません |

## 著作権に関する情報



## 商標に関する情報