



バケットとグループのアクセスポリシー

StorageGRID 11.8

NetApp
March 19, 2024

目次

バケットとグループのアクセスポリシー.....	1
バケットとグループのアクセスポリシーを使用.....	1
バケットポリシーの例.....	18
グループポリシーの例.....	24

バケットとグループのアクセスポリシー

バケットとグループのアクセスポリシーを使用

StorageGRID では、Amazon Web Services (AWS) ポリシー言語を使用して、S3 テナントによるバケットおよびバケット内のオブジェクトへのアクセスを制御できます。StorageGRID システムには、S3 REST API ポリシー言語のサブセットが実装されています。S3 API のアクセスポリシーは JSON 形式で記述されます。

アクセスポリシーの概要

StorageGRID では 2 種類のアクセスポリシーがサポートされています。

- **バケットポリシー**。S3 API の GetBucketPolicy、PutBucketPolicy、および DeleteBucketPolicy の各処理を使用して管理されます。バケットポリシーはバケットに関連付けられ、バケットとそのオブジェクトへのバケット所有者アカウントやその他のアカウントのユーザによるアクセスを制御するために使用されます。バケットポリシー環境は 1 つのバケットのみで、場合によっては複数のグループに分かれています。
- *** グループポリシー ***。Tenant Manager またはテナント管理 API を使用して設定します。グループポリシーはアカウントのグループに関連付けられ、そのアカウントが所有する特定のリソースにそのグループがアクセスできるように設定されます。グループポリシー環境は 1 つのグループに限定され、場合によっては複数のバケットに適用されます。



グループポリシーとバケットポリシーの優先度に違いはありません。

StorageGRID のバケットとグループのポリシーは、Amazon が定義している特定の文法に従って記述されます。各ポリシーは一連のステートメントからなり、各ステートメントは次の要素で構成されます。

- ステートメント ID (SID) (オプション)
- 効果
- プリンシパル / NotPrincipal
- リソース / メモリソース
- アクション / NotAction
- Condition (オプション)

次の構造を使用して、権限を指定するポリシーステートメントが構築されます。<Effect> を付与して、<Condition> に該当する場合に <Principal> に <Resource> に対する <Action> の実行を許可または拒否します。

各ポリシー要素は、特定の機能に使用されます。

要素 (Element)	説明
SID	Sid 要素はオプションです。SID は、ユーザの概要としてのみ使用されます。StorageGRID システムに格納はされますが、システムで解釈されません。

要素 (Element)	説明
効果	Effect 要素では、指定した処理を許可するか拒否するかを指定します。Action 要素でサポートされるキーワードを使用して、バケットやオブジェクトで許可（または拒否）する処理を指定する必要があります。
プリンシパル / NotPrincipal	<p>ユーザ、グループ、およびアカウントに特定のリソースへのアクセスと特定の操作の実行を許可できます。要求に S3 の署名が含まれていない場合は、ワイルドカード文字（*）をプリンシパルとして指定することで匿名アクセスが許可されます。デフォルトでは、アカウントが所有するリソースへのアクセスは root アカウントにのみ許可されます。</p> <p>Principal 要素を指定する必要があるのはバケットポリシーだけです。グループポリシーの場合は、ポリシーが関連付けられたグループが暗黙的にプリンシパルになります。</p>
リソース / メモリソース	Resource 要素では、バケットとオブジェクトを指定します。Amazon リソースネーム（ARN）を使用してリソースを指定し、バケットやオブジェクトに対する権限を許可または拒否することができます。
アクション / NotAction	権限は Action 要素と Effect 要素の 2 つで構成されます。グループがリソースを要求すると、リソースへのアクセスが許可または拒否されます。権限を明示的に割り当てていないかぎりアクセスは拒否されますが、明示的な拒否を使用して別のポリシーで付与された権限を上書きすることもできます。
条件	Condition 要素はオプションです。条件を使用すると、ポリシーを適用する条件を示す式を作成できます。

Action 要素では、ワイルドカード文字（*）を使用してすべての処理または処理のサブセットを指定できます。たとえば、次の Action の値は、s3 : GetObject、s3 : PutObject、s3 : DeleteObject などの権限に一致します。

```
s3:*Object
```

Resource 要素では、ワイルドカード文字（*）および（?）を使用できます。アスタリスク（*）は 0 文字以上の文字に一致し、疑問符（?）は 0 文字以上の文字に一致します。任意の 1 文字に一致します。

Principal要素では、匿名アクセスを設定してすべてのユーザに権限を付与する場合を除き、ワイルドカード文字はサポートされません。たとえば、Principal の値としてワイルドカード（*）を設定します。

```
"Principal": "*" 
```

```
"Principal":{"AWS": "*" }
```

次の例では、Effect、Principal、Action、およびResourceの各要素を使用して記述します。次の例は、「許可」の効果を使用してプリンシパル、adminグループを指定したバケットポリシーのステートメントを示しています federated-group/admin 財務グループなどです federated-group/finance、アクションを実行する権限 s3:ListBucket をバケットにインストールします mybucket そしてアクション s3:GetObject そのバケット内のすべてのオブジェクト。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:iam:s3:::mybucket",
        "arn:aws:iam:s3:::mybucket/*"
      ]
    }
  ]
}
```

バケットポリシーのサイズの上限は 20、480 バイトで、グループポリシーのサイズの上限は 5、120 バイトです。

ポリシーノセイコウセイ

デフォルトでは、グループポリシーに対するすべての更新の整合性レベルは結果整合性です。グループポリシーの整合性が取れた場合、ポリシーキャッシュのために変更が有効になるまでにさらに15分かかることがあります。デフォルトでは、バケットポリシーに対する更新の整合性は非常に高くなります。

バケットポリシーの更新の整合性保証は必要に応じて変更できます。たとえば、サイトが停止しているときにバケットポリシーを変更できるようにすることができます。

この場合は、を設定できます Consistency-Control PutBucketPolicy要求のヘッダー、またはPUT Bucket consistency要求を使用できます。バケットポリシーの整合性が確保されると、ポリシーキャッシュのために変更が有効になるまでにさらに8秒かかることがあります。



一時的な状況を回避するために整合性の値を別の値に設定する場合は、完了後にバケットレベルの設定を元の値に戻してください。そうしないと、以降のすべてのバケット要求で変更後の設定が使用されます。

ポリシーステートメントでは **ARN** を使用します

ポリシーステートメントでは、Principal 要素と Resource 要素で ARN を使用します。

- S3 リソースの ARN の指定には次の構文を使用します。

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- アイデンティティリソースの ARN (ユーザおよびグループ) の指定には次の構文を使用します。

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

その他の考慮事項：

- オブジェクトキーの一部にワイルドカードとしてアスタリスク (*) を使用すると、0 文字以上の文字に一致します。
- オブジェクトキーで指定できる国際文字は、JSON UTF-8 形式または JSON \u エスケープシーケンスを使用してエンコードする必要があります。パーセントエンコーディングはサポートされていません。

"RFC 2141 の URN 構文"

PutBucketPolicy処理のHTTP要求の本文は、charset=UTF-8でエンコードする必要があります。

ポリシー内のリソースを指定します

ポリシーステートメントでは、Resource 要素を使用して、権限を許可または拒否するバケットやオブジェクトを指定できます。

- Resource 要素はポリシーの各ステートメントに必要です。ポリシーでは、リソースは要素で示されます Resource または、`NotResource` 除外のため。
- リソースは S3 リソースの ARN で指定します。例：

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- オブジェクトキーの内部でポリシー変数を使用することもできます。例：

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- グループポリシーの作成時は、まだ存在しないバケットもリソースの値で指定することができます。

ポリシーでプリンシパルを指定します

ポリシーステートメントでリソースへのアクセスを許可または拒否するユーザ、グループ、またはテナントアカウントを指定するには、Principal 要素を使用します。

- バケットポリシーの各ポリシーステートメントには、Principal 要素を含める必要があります。グループはプリンシパルとみなされるため、グループポリシーのポリシーステートメントではPrincipal要素は必要ありません。
- ポリシーでは、「Principal」要素または「NotPrincipal」要素（除外の場合）でプリンシパルを指定します。
- ID または ARN を使用してアカウントベースのアイデンティティを指定する必要があります。

```
"Principal": { "AWS": "account_id" }
"Principal": { "AWS": "identity_arn" }
```

- 次の例では、テナントアカウント ID 27233906934684427525 を使用しています。この場合、root アカウントとそのすべてのユーザが含まれます。

```
"Principal": { "AWS": "27233906934684427525" }
```

- root アカウントのみを指定する場合は次のようになります。

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- 特定のフェデレーテッドユーザ（「Alex」）を指定する場合は次のようになります。

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- 特定のフェデレーテッドグループ（「Managers」）のみを指定する場合は次のようになります。

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers" }
```

- 匿名プリンシパルを指定する場合は次のようになります。

```
"Principal": "*" 
```

- あいまいさを排除するために、ユーザ名の代わりに UUID を使用できます。

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-eb6b9e546013
```

たとえば、Alexが組織とユーザ名を退職するとします Alex が削除されました。新しいAlexが組織に参加し、同じが割り当てられている場合 Alex ユーザ名。元のユーザに付与された権限が、新しいユーザに意図せず継承されることがあります。

- バケットポリシーの作成時は、まだ存在しないグループ/ユーザの名前もプリンシパルの値で指定することができます。

ポリシーで権限を指定します

ポリシーでは、Action 要素を使用してリソースに対する権限を許可または拒否します。ポリシーには、「Action」要素で示される一連の権限、または除外する「NotAction」要素で指定できる一連の権限があります。それぞれが特定の S3 REST API 処理に対応しています。

次の表に、バケットに適用される権限とオブジェクトに適用される権限を示します。



Amazon S3では、PutBucketReplicationとDeleteBucketReplicationの両方のアクションにs3:PutReplicationConfiguration権限が使用されるようになりました。StorageGRID では、元の Amazon S3 仕様に一致する個別の権限が各アクションに使用されます。



DELETEは、PUTを使用して既存の値を上書きした場合に実行されます。

バケットに適用される権限

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : CreateBucket を指定します	CreateBucketを選択します	はい。 注：グループポリシーでのみ使用します。
S3 : DeleteBucket	DeleteBucketの場合	
S3 : DeleteBucketMetadataNotification	バケットのメタデータ通知設定を削除します	はい。
S3 : DeleteBucketPolicy	DeleteBucketPolicyのようになります	
S3 : DeleteReplicationConfiguration	DeleteBucketReplication	○ (PUTとDELETEに別々の権限を設定)
S3 : GetBucketAcl	GetBucketAcl	

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : GetBucketCompliance	GET Bucket compliance (廃止)	はい。
S3 : GetBucketConsistency	GET Bucket consistency	はい。
S3 : GetBucketCORS	GetBucketCors	
S3 : GetEncryptionConfiguration	GetBucketEncryptionの略	
S3 : GetBucketLastAccessTime	GET Bucket last access time の場合	はい。
S3 : GetBucketLocation	GetBucketLocation	
S3 : GetBucketMetadataNotification	GET Bucket metadata notification configuration	はい。
S3 : GetBucketNotification	GetBucketNotificationConfigurationを参照してください	
S3 : GetBucketObjectLockConfiguration	GetObjectLockConfigurationの略	
S3 : GetBucketPolicy	GetBucketPolicyのようになります	
S3 : GetBucketTagging	GetBucketTagging	
S3 : GetBucketVersioning	GetBucketVersioningの各ノードの設定	
S3 : GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
S3 : GetReplicationConfiguration	GetBucketReplicationの略	
S3 : ListAllMyBuckets	<ul style="list-style-type: none"> • ListBuckets • GET Storage Usage の略 	<p>○ (GET Storage Usage) 。</p> <p>注：グループポリシーでのみ使用します。</p>
S3 : ListBucket	<ul style="list-style-type: none"> • ListObjects • ヘッドバケット • RestoreObject 	

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : ListBucketMultipartUploads	<ul style="list-style-type: none"> ListMultipartUploads RestoreObject 	
S3 : ListBucketVersions	GET Bucket versions (バケットバージョンの取得)	
S3 : PutBucketCompliance	PUT Bucket compliance (廃止)	はい。
S3 : PutBucketConsistency	PUT Bucket consistency	はい。
S3 : PutBucketCORS	<ul style="list-style-type: none"> DeleteBucketCors† PutBucketCorsの略 	
S3 : PutEncryptionConfiguration	<ul style="list-style-type: none"> DeleteBucketEncryption PutBucketEncryptionの略 	
S3 : PutBucketLastAccessTime	PUT Bucket last access time のように指定します	はい。
S3 : PutBucketMetadataNotification	PUT Bucket metadata notification configuration のコマンドです	はい。
S3 : PutBucketNotification	PutBucketNotificationConfigurationの略	
S3 : PutBucketObjectLockConfiguration	<ul style="list-style-type: none"> を使用してCreateBucketを作成します。 x-amz-bucket-object-lock-enabled: true 要求ヘッダー (s3 : CreateBucket権限も必要) PutObjectLockConfigurationの略 	
S3 : PutBucketPolicy	PutBucketPolicyのように指定します	
S3 : PutBucketTagging	<ul style="list-style-type: none"> DeleteBucketTagging† PutBucketTaggingの略 	
S3 : PutBucketVersioning	PutBucketVersioningの各ノードの設定	
S3 : PutLifecycleConfiguration	<ul style="list-style-type: none"> DeleteBucketLifecycle† PutBucketLifecycleConfigurationの略 	

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : PutReplicationConfiguration	PutBucketReplicationの略	○ (PUTとDELETEに別々の権限を設定)

オブジェクトに適用される権限

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : AbortMultipartUpload	<ul style="list-style-type: none"> • AbortMultipartUpload の略 • RestoreObject 	
S3 : Bypassガバナー 保持	<ul style="list-style-type: none"> • deleteObject • オブジェクトを削除します • PutObjectRetentionの略 	
S3 : DeleteObject	<ul style="list-style-type: none"> • deleteObject • オブジェクトを削除します • RestoreObject 	
S3 : DeleteObjectTagging	DeleteObjectTagging の場合	
S3 : DeleteObjectVersionTagging	DeleteObjectTagging (オブジェクトの特定のバージョン)	
S3 : DeleteObjectVersion	deleteObject (オブジェクトの特定のバージョン)	
S3 : GetObject	<ul style="list-style-type: none"> • GetObject • HeadObject (ヘッドオブジェクト) • RestoreObject • SelectObjectContent の順に選択します 	
S3 : GetObjectAcl	GetObjectAcl	
S3 : GetObjectLegalHold	GetObjectLegalHold	
S3 : GetObjectRetention	GetObjectRetentionの略	

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : GetObjectTagging	GetObjectTagging の 2 つの機能を	
S3 : GetObjectVersionTagging	GetObjectTagging (オブジェクトの特定のバージョン)	
S3 : GetObjectVersion	GetObject (オブジェクトの特定のバージョン)	
S3 : ListMultipartUploadParts	ListParts、RestoreObject	
S3 : PutObject	<ul style="list-style-type: none"> • PutObject • CopyObject • RestoreObject • CreateMultipartUpload を実行します • CompleteMultipartUpload • UploadPart のアップロード • UploadPartCopyをクリックします 	
S3 : PutObjectLegalHold	PutObjectLegalHold	
S3 : PutObjectRetention	PutObjectRetentionの略	
S3 : PutObjectTagging	PutObjectTagging の 2 つのグループが	
S3 : PutObjectVersionTagging	PutObjectTagging (オブジェクトの特定のバージョン)	
S3 : PutOverwriteObject	<ul style="list-style-type: none"> • PutObject • CopyObject • PutObjectTagging の 2 つのグループが • DeleteObjectTagging の場合 • CompleteMultipartUpload 	はい。
S3 : RestoreObject	RestoreObject	

PutOverwriteObject 権限を使用します

s3 : PutOverwriteObject 権限は、オブジェクトの作成または更新を行う環境 処理のカスタムの StorageGRID 権限です。この権限の設定により、オブジェクトのデータ、ユーザ定義メタデータ、または S3 オブジェクトのタグをクライアントが上書きできるかどうかが決まります。

この権限で可能な設定は次のとおりです。

- * allow * : クライアントはオブジェクトを上書きできます。これがデフォルト設定です。
- **Deny**: クライアントはオブジェクトを上書きできません。PutOverwriteObject 権限が Deny に設定されている場合の動作は次のとおりです。
 - 同じパスで既存のオブジェクトが見つかった場合は、次の手順を実行します。
 - オブジェクトのデータ、ユーザ定義メタデータ、またはS3オブジェクトのタグを上書きすることはできません。
 - 実行中の取り込み処理はすべてキャンセルされ、エラーが返されます。
 - S3のバージョン管理が有効になっている場合は、Denyに設定すると、PutObjectTagging処理またはDeleteObjectTagging処理によってオブジェクトとその最新でないバージョンのTagSetが変更されなくなります。
 - 既存のオブジェクトが見つからない場合は、この権限の設定は影響しません。
- この権限がない場合、Allow が設定されたものと同じ結果になります。



現在のS3ポリシーで上書きが許可されていて、PutOverwriteObject権限がDenyに設定されている場合、オブジェクトのデータ、ユーザ定義メタデータ、またはオブジェクトのタグをクライアントが上書きすることはできません。また、**[Prevent client modification]***チェックボックスが選択されている場合（configuration > Security settings > Network and objects *）、この設定はPutOverwriteObject権限の設定よりも優先されます。

ポリシーの条件を指定します

条件は、ポリシーが有効になるタイミングを定義します。条件は演算子とキーと値のペアで構成されます。

条件はキーと値のペアを使用して評価されます。Condition 要素には複数の条件を指定でき、各条件には複数のキーと値のペアを含めることができます。条件ブロックの形式は次のとおりです。

```
Condition: {
  condition_type: {
    condition_key: condition_values
```

次の例では、IpAddress 条件で SourceIp 条件キーを使用しています。

```
"Condition": {
  "IpAddress": {
    "aws:SourceIp": "54.240.143.0/24"
    ...
  },
  ...
}
```

サポートされる条件演算子は次の

条件演算子は次のように分類されます。

- 文字列
- 数値
- ブール値
- IP アドレス
- Null チェック

条件演算子	説明
StringEquals	キーを文字列値と比較し、完全一致であるかを確認します（大文字と小文字の区別あり）。
StringNotEquals	キーを文字列値と比較し、不一致であるかを確認します（大文字と小文字の区別あり）。
StringEqualsIgnoreCase	キーを文字列値と比較し、完全一致であるかを確認します（大文字と小文字の区別なし）。
StringNotEqualsIgnoreCase	キーを文字列値と比較し、不一致であるかを確認します（大文字と小文字の区別なし）。
StringLike	キーを文字列値と比較し、完全一致であるかを確認します（大文字と小文字の区別あり）。含めることができる * と ? ワイルドカード文字を使用できます。
StringNotLike	キーを文字列値と比較し、不一致であるかを確認します（大文字と小文字の区別あり）。含めることができる * と ? ワイルドカード文字を使用できます。
NumericEquals (数値機器)	キーを数値と比較し、完全一致であるかを確認します。
NumericNotEquals	キーを数値と比較し、不一致であるかを確認します。
NumericGreaterThan	キーを数値と比較し、「より大きい」の一致であるかどうかを確認します。
NumericGreaterThanEquals	キーを数値と比較し、「以上」の一致であるかどうかを確認します。
NumericLessThan	キーを数値と比較し、「より小さい」一致であるかを確認します。
NumericLessThanEquals	キーを数値と比較し、「小なり」の一致であるかを確認します。

条件演算子	説明
ブール値	キーをブール値と比較し、「trueまたはfalse」の一致であるかを確認します。
IP アドレス	キーを IP アドレスまたは IP アドレスの範囲と比較します。
NotIpAddress	キーを IP アドレスまたは IP アドレスの範囲と比較し、不一致であるかを確認します。
null	現在の要求コンテキストに条件キーが存在するかどうかを確認します。

サポートされている条件キー

Conditionキー	アクション	説明
AWS : sourceIP	IP 演算子	<p>要求の送信元の IP アドレスと比較します。バケットまたはオブジェクトの処理に使用できます。</p> <ul style="list-style-type: none"> 注： S3 要求が管理ノードおよびゲートウェイノード上のロードバランササービスを介して送信された場合は、ロードバランササービスのアップストリームの IP アドレスと比較します。 注*：サードパーティ製の非透過型ロードバランサを使用する場合は、そのロードバランサの IP アドレスと比較します。任意 X-Forwarded-For ヘッダーの有効性を確認できないため、ヘッダーは無視されます。
AWS : ユーザ名	リソース / ID	要求の送信者のユーザ名と比較します。バケットまたはオブジェクトの処理に使用できます。
S3 : デリミタ	S3 : ListBucket と S3 : ListBucketVersions 権限	ListObjects要求またはListObjectVersions要求で指定されたdelimiterパラメータと比較します。

Conditionキー	アクション	説明
S3 : ExistingObjectTag /<tag-key>	S3 : DeleteObjectTagging S3 : DeleteObjectVersionTagging S3 : GetObject S3 : GetObjectAcl S3 : GetObjectTagging S3 : GetObjectVersion S3 : GetObjectVersionAcl S3 : GetObjectVersionTagging S3 : PutObjectAcl S3 : PutObjectTagging S3 : PutObjectVersionAcl S3 : PutObjectVersionTagging	既存のオブジェクトに特定のタグキーと値が必要になります。
S3 : max-keys	S3 : ListBucket と S3 : ListBucketVersions 権限	ListObjects要求またはListObjectVersions要求で指定されたmax-keysパラメータと比較します。
S3 : object-lock-remaining-retention-days	S3 : PutObject	で指定されたretain-until-dateと比較します x-amz-object-lock-retain-until-date 次の要求について、これらの値が許容範囲内であることを確認するために、要求ヘッダーまたはバケットのデフォルト保持期間から計算されます。 <ul style="list-style-type: none"> • PutObject • CopyObject • CreateMultipartUpload を実行します
S3 : object-lock-remaining-retention-days	S3 : PutObjectRetention	は、PutObjectRetention要求で指定されたretain-until-dateと比較して、許容範囲内であることを確認します。

Conditionキー	アクション	説明
S3 : プレフィックス	S3 : ListBucket と S3 : ListBucketVersions 権限	ListObjects要求またはListObjectVersions要求で指定されたprefixパラメータと比較します。
S3 : RequestObjectTag /<tag-key>	S3 : PutObject S3 : PutObjectTagging S3 : PutObjectVersionTagging	オブジェクト要求にタグ付けが含まれている場合は、特定のタグキーと値が必要になります。

ポリシーで変数を指定します

ポリシーで変数を使用すると、該当するポリシーの情報を設定できます。でポリシー変数を使用できます Resource の要素と文字列比較 Condition 要素 (Element) :

この例では、変数を使用しています `${aws:username}` はResource要素の一部です。

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

この例では、変数を使用しています `${aws:username}` は、条件ブロックの条件値の一部です。

```
"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}
```

変数 (Variable)	説明
<code>\${aws:SourceIp}</code>	SourceIp キーを指定の変数として使用します。
<code>\${aws:username}</code>	username キーを指定の変数として使用します。
<code>\${s3:prefix}</code>	サービス固有のプレフィックスキーを指定の変数として使用します。
<code>\${s3:max-keys}</code>	サービス固有の max-keys キーを指定の変数として使用します。
<code>\${*}</code>	特殊文字です。文字をリテラル * 文字として使用します。

変数 (Variable)	説明
<code>\${?}</code>	特殊文字です。文字をリテラル文字として使用しますか? を押します。
<code>\$\$\$</code>	特殊文字です。文字「\$」をリテラル文字として使用します。

特別な処理を必要とするポリシーを作成します

ポリシーで付与される権限によって、アカウントの root ユーザがロックアウトされるなど、セキュリティや継続的な運用に支障が生じることがあります。StorageGRID の S3 REST API の実装では、ポリシーの検証時の制限は Amazon よりも厳しくありませんが、評価時は同等の制限が適用されます。

Policy 概要 の略	ポリシータイプ	Amazon の動作	StorageGRID の動作
自身に対し、root アカウントに対するすべての権限を拒否する	バケット	有効で適用されるが、S3 バケットのすべてのポリシー処理に対する権限は引き続き root ユーザアカウントに付与される	同じ
自身に対しユーザ / グループに対するすべての権限を拒否する	グループ	有効で適用されます	同じ
外部アカウントグループに対し任意の権限を許可します	バケット	無効なプリンシパルです	有効だが、S3 バケットのすべてのポリシー処理に対する権限をポリシーで許可すると 405 Method Not Allowed エラーが返されます
外部アカウントの root またはユーザに任意の権限を許可します	バケット	有効だが、S3 バケットのすべてのポリシー処理に対する権限をポリシーで許可すると 405 Method Not Allowed エラーが返されます	同じ
すべてのユーザにすべての処理に対する権限を許可します	バケット	有効だが、外部アカウントの root およびユーザについては、S3 バケットのすべてのポリシー処理に対する権限で 405 Method Not Allowed エラーが返されます	同じ
すべてのユーザに対してすべての処理に対する権限を拒否する	バケット	有効で適用されるが、S3 バケットのすべてのポリシー処理に対する権限は引き続き root ユーザアカウントに付与される	同じ

Policy 概要 の略	ポリシータイプ	Amazon の動作	StorageGRID の動作
プリンシパルとして新規のユーザまたはグループを指定します	バケット	無効なプリンシパルです	有効
リソースとして新規の S3 バケットを指定する必要があります	グループ	有効	同じ
プリンシパルとしてローカルグループを指定します	バケット	無効なプリンシパルです	有効
ポリシーは、オブジェクトをPUTするための非所有者アカウント（匿名アカウントを含む）権限を付与します。	バケット	有効。オブジェクトは作成者アカウントによって所有され、バケットポリシーは適用されません。作成者アカウントは、オブジェクトのACLを使用してオブジェクトにアクセス権限を付与する必要があります。	有効。オブジェクトはバケット所有者アカウントによって所有され、バケットポリシーが適用される。

Write-Once-Read-Many (WORM) による保護

データ、ユーザ定義オブジェクトのメタデータ、S3 オブジェクトのタグを保護するために、Write-Once-Read-Many (WORM) バケットを作成することができます。新しいオブジェクトの作成を許可し、既存のコンテンツの上書きや削除を防止するように WORM バケットを設定します。ここで説明するいずれかの方法を使用します。

上書きを常に拒否するには、次の操作を実行します。

- Grid Managerで、* configuration > Security > Security settings > Network and objects の順に選択し、Prevent client modification *チェックボックスを選択します。
- 次のルールと S3 ポリシーを適用します。
 - S3 ポリシーに PutOverwriteObject DENY 処理を追加します。
 - S3 ポリシーに DeleteObject DENY 処理を追加します。
 - S3ポリシーにPutObject Allow処理を追加します。



S3ポリシーでDeleteObjectをDENYに設定しても、「zero copies after 30 days」などのルールが存在する場合はILMによってオブジェクトが削除されます。



これらのルールとポリシーがすべて適用されても、同時書き込みからは保護されません（状況Aを参照）。保護の対象になるのはシーケンシャルな上書きです（状況 B を参照）。

- 状況 A * : 同時書き込み（保護対象外）

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -----> OK
```

- 状況 B * : シーケンシャルな上書き (保護対象)

```
/mybucket/important.doc
PUT#1 -----> PUT#2 ---X (denied)
```

関連情報

- ["StorageGRID の ILM ルールによるオブジェクトの管理"](#)
- ["バケットポリシーの例"](#)
- ["グループポリシーの例"](#)
- ["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"](#)

バケットポリシーの例

このセクションの例を使用して、バケットのStorageGRID アクセスポリシーを作成します。

バケットポリシーでは、そのポリシーが関連付けられたバケットに対するアクセス権限を指定します。バケットポリシーは、S3 PutBucketPolicy API を使用して設定します。を参照してください ["バケットの処理"](#)。

バケットポリシーを設定するには、AWS CLI で次のコマンドを使用します。

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

例：すべてのユーザにバケットへの読み取り専用アクセスを許可する

この例では、匿名ユーザを含むすべてのユーザにバケット内のオブジェクトのリストとバケット内のすべてのオブジェクトのGetObject処理を許可しています。それ以外の処理はすべて拒否されます。バケットへの書き込み権限がrootアカウント以外に付与されていないため、このポリシーは特に有用ではない場合があります。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
        ["arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

例：あるアカウントのすべてのユーザにフルアクセスを許可し、別のアカウントのすべてのユーザにバケットへの読み取り専用アクセスを許可する

この例では、指定したアカウントのすべてのユーザにバケットへのフルアクセスを許可しています。さらに、アカウントをもう1つ指定し、そのアカウントのすべてのユーザには、で始まるバケットのオブジェクトのList処理とGetObject処理のみを許可しています shared/ オブジェクトキープレフィックス。



StorageGRID では、非所有者アカウント（匿名アカウントを含む）によって作成されたオブジェクトが、バケット所有者アカウントによって所有されます。バケットポリシーで、これらのオブジェクトの環境を設定します。

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}

```

例：すべてのユーザにバケットへの読み取り専用アクセスを許可し、指定したグループにフルアクセスを許可する

この例では、グループに属するユーザのみがバケットのList処理とバケット内のすべてのオブジェクトのGetObject処理を実行できるように匿名ユーザを含むすべてのユーザに許可しています。Marketing 指定したアカウントでは、フルアクセスが許可されています。

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket", "s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

例：クライアントの IP 範囲を限定して、すべてのユーザにバケットへの読み取り / 書き込みアクセスを許可する

この例では、指定した IP 範囲（54.240.143.0~54.240.143.255 で 54.240.143.188 を除く）からの要求についてのみ、匿名ユーザを含むすべてのユーザにバケットの List 処理とバケット内のすべてのオブジェクトの全処理を許可しています。それ以外の処理はすべて拒否され、IP 範囲外の要求はすべて拒否されます。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

例：指定したフェデレーテッドユーザにのみバケットへのフルアクセスを許可します

この例では、フェデレーテッドユーザのAlexがへのフルアクセスを許可しています examplebucket バケットとそのオブジェクト。'root' を含む他のすべてのユーザは 'すべての操作を明示的に拒否されますただし、「root」による Put/Get/DeleteBucketPolicy は拒否されません。


```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

例：PutOverwriteObject 権限

この例では、を使用しています Deny PutOverwriteObjectとDeleteObjectの効果は、オブジェクトのデータ、ユーザ定義メタデータ、S3オブジェクトのタグを上書きまたは削除できないようにします。

```

{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}

```

グループポリシーの例

このセクションの例を使用して、グループのStorageGRID アクセスポリシーを作成します。

グループポリシーは、そのポリシーが関連付けられたグループに対するアクセス権限を指定します。はいません Principal 要素は暗黙的であるため、ポリシーに含まれます。グループポリシーは Tenant Manager または API を使用して設定します。

例：Tenant Manager を使用してグループポリシーを設定します

Tenant Managerでグループを追加または編集するときに、グループポリシーを選択して、このグループのメンバーに付与するS3アクセス権限を決定できます。を参照してください "[S3 テナント用のグループを作成します](#)"。

- * No S3 Access * : デフォルトオプション。バケットポリシーでアクセスが許可されていないかぎり、このグループのユーザはS3リソースにアクセスできません。このオプションを選択すると、デフォルトでは root ユーザにのみ S3 リソースへのアクセスが許可されます。
- * 読み取り専用アクセス * : このグループのユーザには、S3 リソースへの読み取り専用アクセスが許可されます。たとえば、オブジェクトをリストして、オブジェクトデータ、メタデータ、タグを読み取ることができます。このオプションを選択すると、テキストボックスに読み取り専用グループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
- * フルアクセス * : このグループのユーザには、バケットを含む S3 リソースへのフルアクセスが許可されます。このオプションを選択すると、テキストボックスにフルアクセスグループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
- ランサムウェアの軽減: このサンプルポリシーは、このテナントのすべてのバケットを環境します。このグループのユーザは共通の操作を実行できますが、オブジェクトのバージョン管理が有効になっているバケットからオブジェクトを完全に削除することはできません。

Manage All Buckets権限を持つTenant Managerユーザは、このグループポリシーよりも優先できます。[すべてのバケットを管理]権限を信頼できるユーザに制限し、可能な場合は多要素認証 (MFA) を使用します。

- * カスタム * : グループ内のユーザーには、テキストボックスで指定した権限が付与されます。

例：グループにすべてのバケットへのフルアクセスを許可する

この例では、バケットポリシーで明示的に拒否されている場合を除き、グループのすべてのメンバーにテナントアカウントが所有するすべてのバケットへのフルアクセスが許可されます。

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

例：グループにすべてのバケットへの読み取り専用アクセスを許可する

この例では、バケットポリシーで明示的に拒否されている場合を除き、グループのすべてのメンバーに S3 リソースへの読み取り専用アクセスが許可されます。たとえば、オブジェクトをリストして、オブジェクトデータ、メタデータ、タグを読み取ることができます。

```

{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}

```

例：グループメンバーにバケット内の「フォルダ」へのフルアクセスのみを許可する

この例では、指定したバケット内の特定のフォルダ（キープレフィックス）のリストおよびアクセスのみがグループのメンバーに許可されます。これらのフォルダのプライバシー設定を決めるときは、他のグループポリシーやバケットポリシーのアクセス権限を考慮する必要があります。

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。