# StorageGRIDによるランサムウェア対策

## S3オブジェクトの保護

NetApp
Aron Klein
2023年12月| TR-4921

## 概要

ランサムウェア攻撃はますます増えつつあります。このドキュメントでは、StorageGRIDでオブジェクトデータを保護する方法について、いくつかの推奨事項を示します。

目次



# はじめに

今日のランサムウェアは、データセンターに常に存在する危険です。ランサムウェアは、データを暗号化し、データに依存するユーザやアプリケーションがデータを使用できないようにするように設計されています。保護対策の第一歩は、ネットワークの強化やユーザによる堅実なセキュリティ プラクティスという、ごく普通の防御を講じることです。そのうえで、データ アクセスのセキュリティ プラクティスを実践する必要があります。

# StorageGRIDのベストプラクティス

StorageGRIDのセキュリティのベストプラクティスには、管理アクセスとオブジェクトアクセスの両方に、署名付き証明書でHTTPSを使用することが含まれます。アプリケーションと個人用に専用のユーザアカウントを作成し、アプリケーションアクセスやユーザデータアクセスにテナントrootアカウントを使用しないでください。言い換えれば、最小特権の原則に従ってください。IDおよびアクセス管理（IAM）ポリシーが定義されたセキュリティグループを使用して、ユーザ権限を管理し、アプリケーションおよびユーザに固有のアカウントにアクセスします。これらの対策を実施した場合でも、データを確実に保護する必要があります。Simple Storage Service（S3）では、オブジェクトが暗号化するように変更されると、元のオブジェクトが上書きされます。

# 防御方法

S3 APIの主なランサムウェア対策メカニズムは、オブジェクトロックの実装です。すべてのアプリケーションがオブジェクトロックと互換性があるわけではありません。そのため、このレポートでは、バージョン管理が有効な別のバケットへのレプリケーションと、IAMポリシーによるバージョン管理の2つのオプションについて説明します。

# オブジェクト ロック

オブジェクトロックは、オブジェクトが削除または上書きされないようにするWORMモデルを提供します。StorageGRIDではオブジェクトロックが実装され 、規制要件を満たすためにCohassetが評価され、オブジェクト保持のリーガルホールド、コンプライアンスモード、ガバナンスモード、およびデフォルトのバケット保持ポリシーがサポートされます。バケットの作成時にオブジェクトロックを有効にし、バージョン管理を有効

にする必要があります。オブジェクトの特定のバージョンがロックされ'バージョンIDが定義されていない場合は'オブジェクトの現在のバージョンに保持が適用されます現在のバージョンに保持が設定されていて、オブジェクトを削除、変更、または上書きしようとすると、削除マーカーまたはオブジェクトの新しいリビジョンを現在のバージョンとして使用して新しいバージョンが作成されます。 ロックされたバージョンは、最新でないバージョンとして保持されます。まだ互換性がないアプリケーションでは、オブジェクトロックとバケットに配置されたデフォルトの保持設定を使用できます。設定の定義が完了すると、バケットに追加される新しいオブジェクトごとにオブジェクト保持期間が適用されます。これは、保持期間が経過する前にオブジェクトを削除または上書きしないようにアプリケーションが設定されているかぎり機能します。

オブジェクトロックAPIの使用例を次に示します。

オブジェクトロックリーガルホールドは、オブジェクトに適用される単純なオン/オフステータスです。

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal-hold Status=ON --
endpoint-url https://s3.company.com
```

リーガルホールドステータスを設定しても値は返されないため、GET処理で確認できます。

```
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt --endpoint-url
https://s3.company.com
{
    "LegalHold": {
        "Status": "ON"
    }
}
```

リーガルホールドをオフにするには、オフステータスを適用します。

```
aws s3api put-object-legal-hold --bucket mybucket --key myfile.txt --legal-hold Status=OFF --
endpoint-url https://s3.company.com
aws s3api get-object-legal-hold --bucket mybucket --key myfile.txt --endpoint-url
https://s3.company.com
{
    "LegalHold": {
        "Status": "OFF"
    }
}
```

オブジェクトの保持期間の設定には、タイムスタンプまで保持が適用されます。

```
aws s3api put-object-retention --bucket mybucket --key myfile.txt --retention
'{"Mode":"COMPLIANCE", "RetainUntilDate": "2022-06-10T16:00:00"}' --endpoint-url
https://s3.company.com
```

繰り返しになりますが、成功した場合も戻り値はありません。そのため、GET呼び出しを使用して保持ステータスを同様に確認できます。

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt --endpoint-url
https://s3.company.com

{

    "Retention": {

        "Mode": "COMPLIANCE",

        "RetainUntilDate": "2022-06-10T16:00:00+00:00"

    }
```

オブジェクトロックが有効なバケットにデフォルトの保持期間を設定すると、保持期間（日と年）が使用されます。

```
aws s3api put-object-lock-configuration --bucket mybucket --object-lock-configuration '{
"ObjectLockEnabled": "Enabled", "Rule": { "DefaultRetention": { "Mode": "COMPLIANCE", "Days":
1 }}}' --endpoint-url https://s3.company.com
```

これらの処理のほとんどと同様に、成功した場合も応答が返されないため、設定を検証するGETを実行できます。

```
aws s3api get-object-lock-configuration --bucket mybucket --endpoint-url
https://s3.company.com
{
    "ObjectLockConfiguration":
        { "ObjectLockEnabled":
        "Enabled", "Rule": {
            "DefaultRetention":
                { "Mode":
                "COMPLIANCE",
                "Days": 1
            }
        }
    }
```

次に、保持設定を適用した状態でバケットにオブジェクトを配置します。

```
aws s3 cp myfile.txt s3://mybucket --endpoint-url https://s3.company.com
```

PUT処理で応答が返されます。

```
upload: ./myfile.txt to s3://mybucket/myfile.txt
```

保持オブジェクトでは、上記の例でバケットに設定されている保持期間がオブジェクトの保持タイムスタンプに変換されます。

```
aws s3api get-object-retention --bucket mybucket --key myfile.txt --endpoint-url
https://s3.company.com
{
    "Retention": {
        "Mode": "COMPLIANCE",
        "RetainUntilDate": "2022-03-02T15:22:47.202000+00:00"
    }
}
```

# バージョン管理を使用したバケットへのレプリケーション

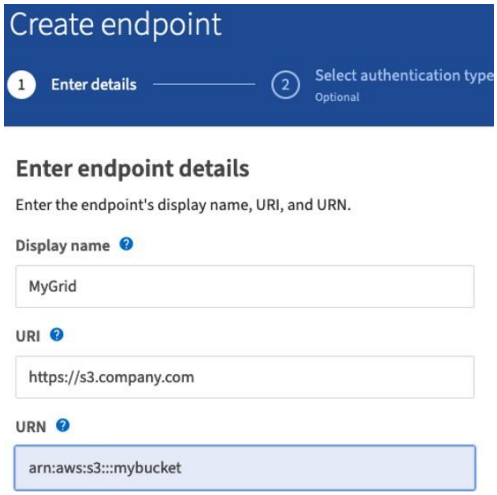
すべてのアプリケーションとワークロードがオブジェクトロックと互換性があるわけではありません。もう1つの方法は、同じグリッド内（アクセスが制限された別のテナントを推奨）、またはStorageGRIDプラットフォームサービスCloudMirrorを使用する他のS3エンドポイントのいずれかのセカンダリバケットにオブジェクトをレプリケートする方法です。

StorageGRID CloudMirrorはStorageGRIDのコンポーネントで、ソースバケットに取り込まれたオブジェクトを定義済みのデスティネーションにレプリケートするように設定できます。CloudMirrorでは削除はレプリケートされません。CloudMirrorはStorageGRIDに統合されたコンポーネントであるため、S3 APIベースの攻撃によって無効にしたり操作したりすることはできません。レプリケートされたバケットは、バージョン管理またはオブジェクトロックを有効にして設定できます。オブジェクトロックを有効にした場合は、攻撃を検出してリカバリできるように、デフォルトの保持期間を設定する必要があります。オブジェクトロックはバージョン管理に依存するため、どちらのシナリオでも、レプリケートされたバケットの古いバージョンを自動的にクリーンアップして安全に破棄する必要があります。そのためには、StorageGRID ILMポリシーエンジンを使用できます。ルールを作成して、最新でない時間（攻撃を特定してリカバリするのに十分な時間）に基づいてオブジェクトの配置を管理します。オブジェクトロックを実装する場合は、ルールの期間がデフォルトの保持期間を超えている必要があります。

このアプローチの欠点は、バケットの完全な2つ目のコピーを作成し、オブジェクトの複数のバージョンをしばらくの間保持することで、より多くのストレージを消費することです。また、プライマリバケットから意図的に削除されたオブジェクトは、レプリケートされたバケットから手動で削除する必要があります。NetApp CloudSyncなど、製品以外にも、同様の解決策の削除をレプリケートできるレプリケーションオプションがあります。セカンダリバケットのもう1つの欠点は、バージョン管理が有効でオブジェクトロックが有効ではないことです。複数の権限付きアカウントが存在し、セカンダリサイトで原因が破損する可能性があります。その利点は、そのエンドポイントまたはテナントバケットに対して一意のアカウントである必要があり、プライマリロケーションのアカウントへのアクセスやプライマリロケーションのアカウントへのアクセスが含まれない可能性があることです。

ソースバケットとデスティネーションバケットが作成され、デスティネーションでオブジェクトロックまたはバージョン管理が設定されたら、次のようにCloudMirrorレプリケーションを設定して有効にできます。

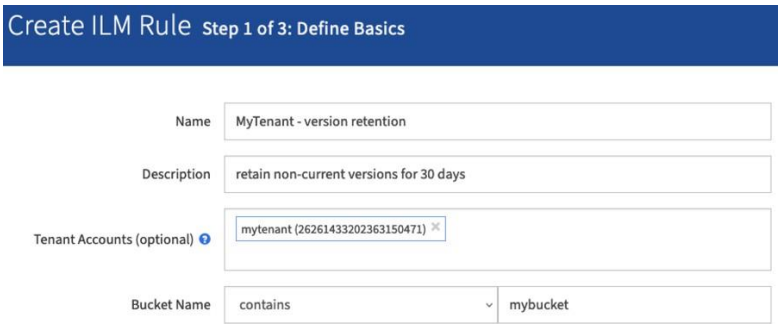
1. CloudMirrorを設定するには、S3デスティネーション用のプラットフォームサービスエンドポイントを作成します。

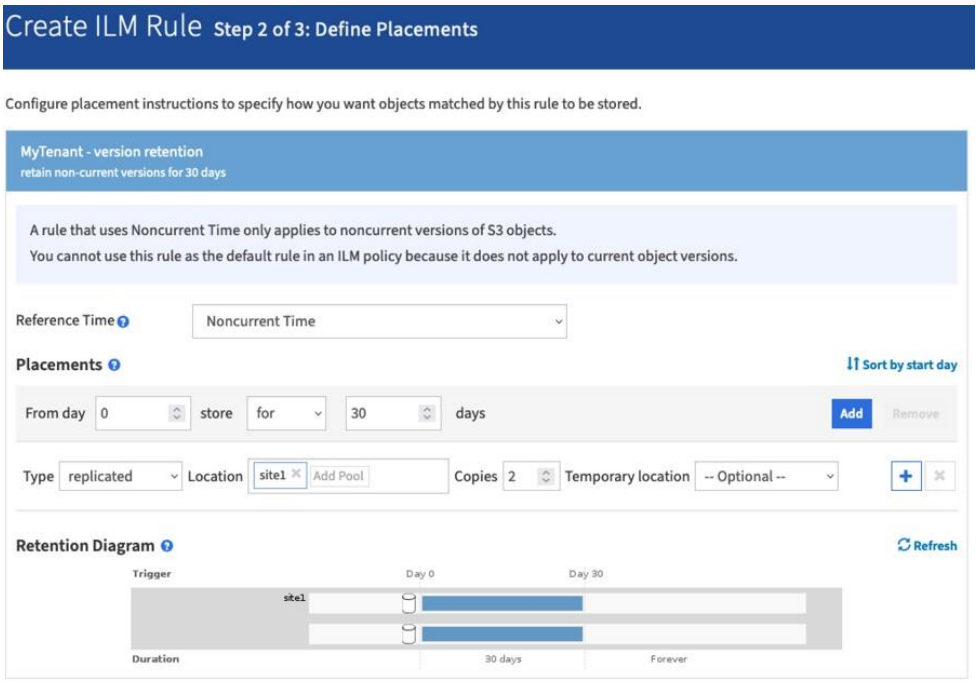



2. ソースバケットで、設定されているエンドポイントを使用するようにレプリケーションを設定します。

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Bucket>arn:aws:s3:::mybucket</Bucket>
            <StorageClass>STANDARD</StorageClass>
        </Destination>
    </Rule>
</ReplicationConfiguration>
```

3. ストレージの配置とバージョンのストレージ期間を管理するILMルールを作成します。この例では、格納するオブジェクトの最新でないバージョンが設定されています。



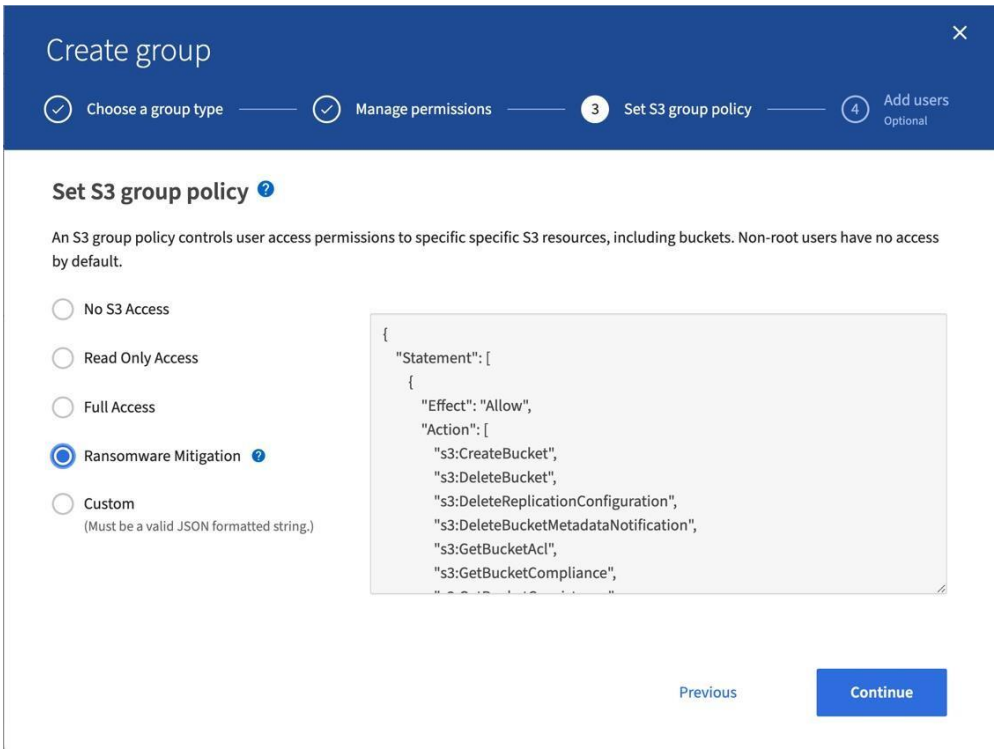



サイト1にコピーが2つあり、30日間保持されます。また、ILMルールの取り込み時間をソースバケットのストレージ期間に一致させるための参照時間として使用することに基づいて、オブジェクトの現在のバージョンのルールを設定します。オブジェクトバージョンのストレージ配置は、イレイジャーコーディングまたはレプリケートが可能です。

# 保護されたIAMポリシーを使用したバージョン管理

オブジェクトロックやレプリケーションを使用せずにデータを保護するには、バケットでバージョン管理を有効にし、ユーザセキュリティグループにIAMポリシーを実装して、ユーザによるオブジェクトのバージョン管理を制限します。攻撃が発生した場合、データの新しい不正なバージョンが現在のバージョンとして作成され、最新でないバージョンが安全なクリーンデータになります。データにアクセスするために侵害されたアカウントは、削除したり、最新でないバージョンを変更したりすることができず、以降のリストア処理のために保護されています。前のシナリオと同様に、最新でないバージョンの保持期間を選択してILMルールによって管理されます。欠点は、不正なアクター攻撃のために特権アカウントが存在する可能性がまだあることですが、すべてのアプリケーションサービスアカウントとユーザーは、より制限的なアクセスを設定する必要があります。制限付きグループポリシーでは、ユーザまたはアプリケーションに許可する各アクションを明示的に許可し、許可しないアクションを明示的に拒否する必要があります。NetAppでは、今後新しいアクションが導入される可能性があり、許可するか拒否するかを制御する必要があるため、ワイルドカードAllowの使用は推奨されていません。この解決策では、ユーザによる変更やプログラムによる変更からバケットとオブジェクトのバージョン設定を保護するために、拒否リストにDeleteObjectVersion、PutBucketPolicy、DeleteBucketPolicy、PutLifecycleConfiguration、およびPutBucketVersioningを含める必要があります。

StorageGRID 11.7では、この解決策の実装を簡易化するために、S3グループポリシーオプションである「Ransomware Mitigation」が新たに導入されました。テナントでユーザグループを作成するときに、グループ権限を選択すると、この新しいオプションのポリシーが表示されます。




次に、グループポリシーの内容を示します。このグループポリシーには、明示的に許可された処理と、最低限必要な処理が含まれています。

```
{
   "Statement": [
      {
         "Effect": "Allow"、
         "Action": [
            "s3:CreateBucket",
            "s3:DeleteBucket",
            "s3:DeleteReplicationConfiguration",

"s3:DeleteBucketMetadataNotification",
            "s3:GetBucketAcl",
            "s3:GetBucketCompliance",
            "s3:GetBucketConsistency",
            "s3:GetBucketLastAccessTime",
            "s3:GetBucketLocation",
            "s3:GetBucketNotification",

"s3:GetBucketObjectLockConfiguration",
            "s3:GetBucketPolicy",
            "s3:GetBucketMetadataNotification",
            "s3:GetReplicationConfiguration",
            "s3:GetBucketCORS",
            "s3:GetBucketVersioning",
            "s3:GetBucketTagging",
            "s3:GetEncryptionConfiguration",
            "s3:GetLifecycleConfiguration",
            "s3:ListBucket",
            "s3:ListBucketVersions",
            "s3:ListAllMyBuckets",
            "s3:ListBucketMultipartUploads",
            "s3:PutBucketConsistency",
            "s3:PutBucketLastAccessTime",
            "s3:PutBucketNotification",

"s3:PutBucketObjectLockConfiguration",
            "s3:PutReplicationConfiguration",
            "s3:PutBucketCORS",
            "s3:PutBucketMetadataNotification",
            "s3:PutBucketTagging",
            "s3:PutEncryptionConfiguration",
            "s3:AbortMultipartUpload",
            "s3:DeleteObject",
            "s3:DeleteObjectTagging",
            "s3:DeleteObjectVersionTagging",
            "s3:GetObject",
            "s3:GetObjectAcl",
            "s3:GetObjectLegalHold",
            "s3:GetObjectRetention",
            "s3:GetObjectTagging",
            "s3:GetObjectVersion",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectVersionTagging",
            "s3:ListMultipartUploadParts",
```

```
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectLegalHold",
                "s3:PutObjectRetention",
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging",
                "s3:RestoreObject",
                "s3:ValidateObject",
                "s3:PutBucketCompliance",
                "s3:PutObjectVersionAcl"
            ],
            "リソース": " arn:aws：s3:::*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "s3:DeleteObjectVersion",
                "s3:DeleteBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketVersioning"
            ],
            "リソース": " arn:aws:s3:::*"
        }
    ]
}
```

# まとめ

ランサムウェアは、今日の最大級のセキュリティ脅威の1つです。NetApp StorageGRIDチームは、これらの脅威に先手を打つためにお客様と協力しています。オブジェクトロックとバージョン管理を使用すると、不要な変更から保護し、悪意のある攻撃からリカバリできます。データセキュリティは多層的な取り組みであり、オブジェクトストレージはデータセンターの一部にすぎません。

# バージョン履歴

| バージョン | 日付 | ドキュメントの改訂履歴 |
|---|---|---|
| バージョン1.0 | 2022年4月 | 初版リリース |
| バージョン2.0 | 2023年12月 | イメージを修正し、11.7グループポリシーオプション用に更新します。 |

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで Interoperability Matrix Tool (IMT)を参照してください。NetApp IMT には、NetApp がサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

**機械翻訳に関する免責事項**

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

**著作権に関する情報**



**商標に関する情報**