



# TR-4921 : 『Ransomware Defense』

## How to enable StorageGRID in your environment

NetApp  
July 05, 2024

# 目次

TR-4921：『Ransomware Defense』	1
StorageGRID S3オブジェクトをランサムウェアから保護	1
オブジェクトロックを使用したランサムウェア対策	2
レプリケートされたバケットを使用したバージョン管理によるランサムウェア対策	4
保護IAMポリシーを使用したバージョン管理を使用したランサムウェア防御	7

# TR-4921 : 『Ransomware Defense』

## StorageGRID S3オブジェクトをランサムウェアから保護

ランサムウェア攻撃と、StorageGRIDのセキュリティに関するベストプラクティスでデータを保護する方法をご紹介します。

ランサムウェア攻撃が増加しています。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。

ランサムウェアは今日、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。保護は、強化されたネットワーキングと強固なユーザーセキュリティプラクティスの通常の防御から始まります。そして、データアクセスセキュリティプラクティスに従う必要があります。

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。

### 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として、管理アクセスとオブジェクトアクセスの両方に、署名済み証明書を使用したHTTPSの使用を推奨します。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。

### 追加情報の参照先

このドキュメントに記載されている情報の詳細については、以下のドキュメントや Web サイトを参照してください。

- NetApp StorageGRIDドキュメントセンター <https://docs.netapp.com/us-en/storagegrid-118/>
- NetApp StorageGRIDイネーブルメント <https://docs.netapp.com/us-en/storagegrid-enable/>
- StorageGRIDドキュメントリソースページ <https://www.netapp.com/data-storage/storagegrid/documentation/>
- NetApp製品ドキュメント <https://www.netapp.com/support-and-training/documentation/>

# オブジェクトロックを使用したランサムウェア対策

StorageGRIDのオブジェクトロックがWORMモデルを提供してデータの削除や上書きを防止する方法や、それが規制要件をどのように満たしているかをご紹介します。

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を実装すること "[Cohasset評価済み](#)" で、規制要件への対応を支援し、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をサポートします。オブジェクトロックは、バケットの作成およびバージョン管理の一環として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、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を実行できません。

```
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"
  }
}
```

## レプリケートされたバケットを使用したバージョン管理によるランサムウェア対策

StorageGRID CloudMirrorを使用して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について説明します。

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

この方法は、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す。定義されたデスティネーションにバケットのオブジェクトがソースバケットに取り込まれたときにレプリケートされ、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。このレプリケートされたバケットは、バージョン管理を有効にして設定できます。このシナリオでは、レプリケートされたバケットの古いバージョンを破棄しても安全な自動クリーンアップが必要です。そのためには、StorageGRID ILMポリシーエンジンを使用できます。最新でない時間に基づいてオブジェクトの配置を管理するルールを作成し、攻撃を特定してリカバリします。

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、同様のソリューションで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バージョン管理が有効でオブジェクトロックが有効でない場合のもう1つの欠点は、セカンダリの場所に損傷を与える可能性がある特権アカウントが多数存在することです。長所は、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侵害さ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バージョン管理が設定されたら、次のようにレプリケーションを設定して有効にすることができます。

#### 手順

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。

# Create endpoint

1

Enter details

2

Select authentication type  
Optional

## Enter endpoint details

Enter the endpoint's display name, URI, and URN.

Display name [?](#)

MyGrid

URI [?](#)

https://s3.company.com

URN [?](#)

arn:aws:s3:::mybucket

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。



## Create ILM Rule Step 1 of 3: Define Basics

Name	MyTenant - version retention
Description	retain non-current versions for 30 days
Tenant Accounts (optional)	mytenant (26261433202363150471)
Bucket Name	contains - mybucket

## Create ILM Rule Step 2 of 3: Define Placements

Configure placement instructions to specify how you want objects matched by this rule to be stored.

MyTenant - version retention  
retain non-current versions for 30 days

A rule that uses Noncurrent Time only applies to noncurrent versions of S3 objects.  
You cannot use this rule as the default rule in an ILM policy because it does not apply to current object versions.

Reference Time

Placements

From day  store for  days

Type  Location  Add Pool Copies  Temporary location

Retention Diagram

Trigger: site1  
Day 0  
Day 30  
Duration: 30 days, Forever

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。

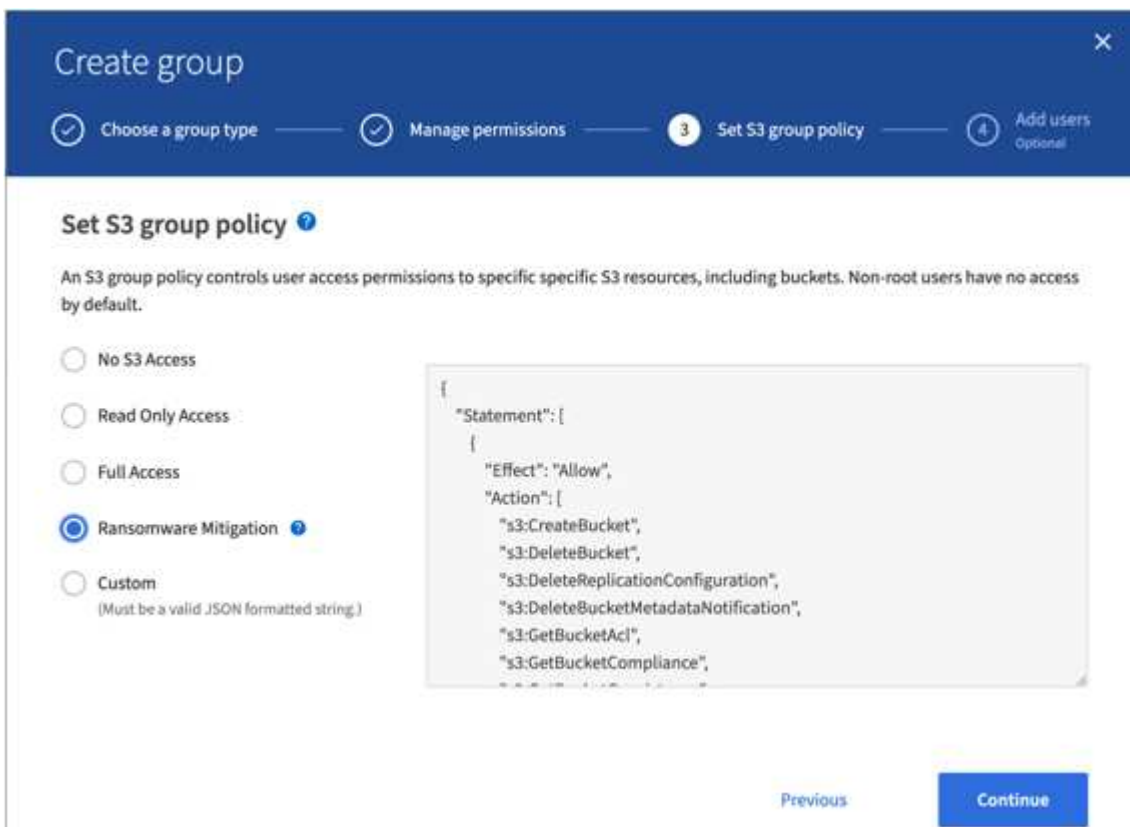
## 保護IAMポリシーを使用したバージョン管理を使用したランサムウェア防御

バケットのバージョン管理を有効にし、StorageGRIDのユーザセキュリティグループにIAMポリシーを実装して、データを保護する方法について説明します。

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。このソリューションでは、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、このソリューションの実装を容易にするために、新しいS3グループポリシーオプション「Ransomware Mitigation」が導入されました。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"
    ],
    "Resource": "arn:aws:s3:::*"
},
{
    "Effect": "Deny",
    "Action": [
        "s3:DeleteObjectVersion",
        "s3:DeleteBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning"
    ],
    "Resource": "arn:aws:s3:::*"
}
]
}

```

## 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。