暗号化されたボリュームでのデータのセキュアパージ

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/ontap/encryption-at-rest/secure-purge-data-encrypted-volume-concept.html on February 12, 2026. Always check docs.netapp.com for the latest.

目次

暗号化されたボリュームでのデータのセキュア パージ . . . 1

暗号化されたONTAPボリュームからデータを安全に消去する方法について説明します。 . . . 1

セキュア パージを使用する場合の考慮事項 . . . 1

暗号化されたONTAPボリュームからSnapMirror関係なしでデータを消去する . . . 2

SnapMirror非同期関係を持つ暗号化された ONTAP ボリュームからデータをスクラブする . . . 3

SnapMirror同期関係を持つ暗号化された ONTAP ボリュームからデータをスクラブする . . . 5

暗号化されたボリュームでのデータのセキュア パージ

暗号化された**ONTAP**ボリュームからデータを安全に消去する方法について説明します。

ONTAP 9.4以降では、セキュアパージを使用して、NVE対応ボリューム上のデータを無停止でスクラブできます。暗号化されたボリューム上のデータをスクラブすることで、例えばブロックの上書き時にデータの痕跡が残ってしまう「スピレッジ」が発生した場合や、退去するテナントのデータを安全に削除する場合など、物理メディアからのデータの復元を不可能にすることができます。

セキュア パージの対象となるのは、NVE対応ボリューム上で以前に削除されたファイルだけです。暗号化されていないボリュームはスクラビングできません。キーの提供には、オンボード キー マネージャではなく、KMIPサーバを使用する必要があります。

セキュア パージを使用する場合の考慮事項

- NetApp Aggregate Encryption（NAE）が有効になっているアグリゲートに作成されたボリュームでは、セキュア パージがサポートされません。
- セキュア パージの対象となるのは、NVE対応ボリューム上で以前に削除されたファイルだけです。
- 暗号化されていないボリュームはスクラビングできません。
- キーの提供には、オンボード キー マネージャではなく、KMIPサーバを使用する必要があります。

セキュア パージの動作は、ONTAPのバージョンによって異なります。

ONTAP 9.8以降

- セキュア パージはMetroClusterとFlexGroupでサポートされます。
- パージするボリュームがSnapMirror関係のソースである場合、セキュア パージを実行するためにSnapMirror関係を解除する必要はありません。
- 再暗号化の方法は、SnapMirrorデータ保護（DP）を使用するボリュームと使用しないボリューム、またはSnapMirror拡張データ保護を使用するボリュームとで異なります。
  - SnapMirrorデータ保護（DP）モードを使用するボリュームでは、デフォルトでボリューム移動方式を使用してデータが再暗号化されます。
  - SnapMirrorデータ保護を使用しないボリュームまたはSnapMirror拡張データ保護（XDP）モードを使用するボリュームでは、インプレース再暗号化方式がデフォルトで使用されます。
  - これらのデフォルトは `secure purge re-encryption-method [volume-move|in-place-rekey]`コマンドを使用して変更できます。
- デフォルトでは、FlexVolボリューム内のすべてのスナップショットは、セキュアパージ操作中に自動的に削除されます。デフォルトでは、FlexGroupボリューム内のスナップショットおよびSnapMirrorデータ保護を使用しているボリューム内のスナップショットは、セキュアパージ操作中に自動的に削除されません。これらのデフォルトは、 `secure purge delete-all-snapshots [true|false]` コマンドを使用して変更できます。

ONTAP 9.7以前

- 次の機能ではセキュア パージがサポートされません。
  - FlexClone
  - SnapVault
  - FabricPool
- パージするボリュームがSnapMirror関係のソースである場合、ボリュームをパージする前にSnapMirror関係を解除する必要があります。

  ボリューム内に使用中のスナップショットがある場合は、ボリュームをパージする前にスナップショットを解放する必要があります。たとえば、FlexCloneボリュームを親ボリュームから分割する必要がある場合などです。
- セキュア パージ機能を呼び出すと、ボリューム移動がトリガーされ、パージされない残りのデータが新しいキーで再度暗号化されます。

  移動されたボリュームは現在のアグリゲートに残ります。パージされたデータをストレージ メディアからリカバリできないように、古いキーは自動的に破棄されます。

暗号化されたONTAPボリュームからSnapMirror関係なしでデータを消去する

ONTAP 9.4 以降では、 secure-purge を使用して、 NVE 対応ボリューム上のデータを中断せずに「スクラブ」することができます。

タスク概要

セキュアパージは、削除されたファイルのデータ量に応じて、数分から数時間かかる場合があります。 `volume encryption secure-purge show`コマンドを使用して、操作のステータスを表示できます。 `volume encryption secure-purge abort`コマンドを使用して、操作を終了できます。

> SANホストでセキュアパージを実行するには、パージ対象のファイルを含むLUN全体を削除するか、パージ対象のファイルに属するブロックのLUNにパンチホールを作成できる必要があります。LUNを削除できない場合、またはホストOSがLUNのパンチホール作成をサポートしていない場合は、セキュアパージを実行できません。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクを実行するにはadvanced権限が必要です。

手順

1. セキュア パージを実行するファイルまたはLUNを削除します。
   - NASクライアントで、セキュア パージを実行するファイルを削除します。
   - SANホストで、セキュア パージを実行するLUNを削除するか、パージするファイルに属するブロックに対してLUNでホール パンチングを実行します。
2. ストレージ システムで、advanced権限レベルに切り替えます。

   `set -privilege advanced`

3. セキュア パージを実行するファイルがSnapshotに含まれている場合は、Snapshotを削除します。

   `snapshot delete -vserver` *SVM_name* `-volume` *volume_name* `-snapshot`

4. 削除したファイルのセキュア パージを実行します。

   `volume encryption secure-purge start -vserver` *SVM_name* `-volume` *volume_name*

   次のコマンドは、SVM`vs1`上の `vol1`で削除されたファイルを安全に消去します：

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

5. セキュア パージ処理のステータスを確認します。

   `volume encryption secure-purge show`

SnapMirror非同期関係を持つ暗号化された ONTAP ボリュームからデータをスクラブする

ONTAP 9.8 以降では、セキュア パージを使用して、SnapMirror 非同期関係にある NVE 対応ボリューム上のデータを中断することなく「スクラブ」することができます。

開始する前に

* このタスクを実行するには、クラスタ管理者である必要があります。
* このタスクを実行するにはadvanced権限が必要です。

タスク概要

セキュアパージは、削除されたファイルのデータ量に応じて、数分から数時間かかる場合があります。 `volume encryption secure-purge show`コマンドを使用して、操作のステータスを表示できます。 `volume encryption secure-purge abort`コマンドを使用して、操作を終了できます。

> SANホストでセキュアパージを実行するには、パージ対象のファイルを含むLUN全体を削除するか、パージ対象のファイルに属するブロックのLUNにパンチホールを作成できる必要があります。LUNを削除できない場合、またはホストOSがLUNのパンチホール作成をサポートしていない場合は、セキュアパージを実行できません。

手順

1. ストレージ システムで、advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. セキュア パージを実行するファイルまたはLUNを削除します。
   * NASクライアントで、セキュア パージを実行するファイルを削除します。
   * SANホストで、セキュア パージを実行するLUNを削除するか、パージするファイルに属するブロックに対してLUNでホール パンチングを実行します。

3. 非同期関係のデスティネーション ボリュームでセキュア パージを準備します。

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   SnapMirror非同期関係の各ボリュームに対してこの手順を繰り返します。

4. セキュア パージを実行するファイルがSnapshotに含まれている場合は、Snapshotを削除します。

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. セキュア パージを実行するファイルがベースSnapshotに含まれている場合は、次の手順を実行します。

   a. SnapMirror非同期関係の宛先ボリュームにSnapshotを作成します：

   ```
   volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
   volume_name
   ```

   b. SnapMirrorを更新してベーススナップショットを前進させる：

   ```
   snapmirror update -source-snapshot snapshot_name -destination-path
   destination_path
   ```

   SnapMirror非同期関係の各ボリュームに対してこの手順を繰り返します。

   a. 手順（a）と（b）を、ベースSnapshotの数に1を加えた回数だけ繰り返します。

たとえば、ベースSnapshotが2つある場合は手順（a）と（b）を3回繰り返します。

b. ベーススナップショットが存在することを確認します：+ `snapshot show -vserver` *`SVM_name`* `-volume` *`volume_name`*

c. ベーススナップショットを削除します：+ `snapshot delete -vserver` *`svm_name`* `-volume` *`volume_name`* `-snapshot snapshot`

6. 削除したファイルのセキュア パージを実行します。

   `volume encryption secure-purge start -vserver` *`svm_name`* `-volume` *`volume_name`*

   SnapMirror非同期関係の各ボリュームに対してこの手順を繰り返します。

   次のコマンドは、SVM “vs1” 上の “vol1” 上の削除されたファイルを安全に消去します：

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

7. セキュア パージ処理のステータスを確認します。

   `volume encryption secure-purge show`

関連情報

- "snapmirror update"

SnapMirror同期関係を持つ暗号化された ONTAP ボリュームからデータをスクラブする

ONTAP 9.8以降では、セキュア パージを使用して、SnapMirror同期関係にあるNVE対応ボリュームのデータを無停止で「スクラビング」できます。

タスク概要

セキュアパージは、削除されたファイルのデータ量に応じて、完了までに数分から数時間かかる場合があります。 `volume encryption secure-purge show`コマンドを使用して操作のステータスを確認できます。 `volume encryption secure-purge abort`コマンドを使用して操作を終了できます。

> ⓘ SANホストでセキュアパージを実行するには、パージ対象のファイルを含むLUN全体を削除するか、パージ対象のファイルに属するブロックのLUNにパンチホールを作成できる必要があります。LUNを削除できない場合、またはホストOSがLUNのパンチホール作成をサポートしていない場合は、セキュアパージを実行できません。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクを実行するにはadvanced権限が必要です。

手順

1. ストレージ システムで、advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. セキュア パージを実行するファイルまたはLUNを削除します。
   - NASクライアントで、セキュア パージを実行するファイルを削除します。
   - SANホストで、セキュア パージを実行するLUNを削除するか、パージするファイルに属するブロックに対してLUNでホール パンチングを実行します。

3. 非同期関係のデスティネーション ボリュームでセキュア パージを準備します。

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   -prepare true
   ```

   SnapMirror同期関係のもう一方のボリュームに対してこの手順を繰り返します。

4. セキュア パージを実行するファイルがSnapshotに含まれている場合は、Snapshotを削除します。

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```

5. 対象ファイルがベースSnapshotまたは共通Snapshotに含まれている場合は、SnapMirrorを更新して共通Snapshotを最新の状態にします。

   ```
   snapmirror update -source-snapshot <snapshot_name> -destination-path
   <destination_path>
   ```

   共通Snapshotは2つあるため、このコマンドは2回実行する必要があります。

6. セキュア パージ ファイルがアプリケーション整合性スナップショット内にある場合は、SnapMirror 同期関係にある両方のボリューム上のスナップショットを削除します：

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```

   この手順は両方のボリュームで実行します。

7. 削除したファイルのセキュア パージを実行します。

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   ```

   SnapMirror同期関係の各ボリュームに対してこの手順を繰り返します。

   次のコマンドは、SVM "`vs1`"上の"`vol1`"上の削除されたファイルを安全に消去します。

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

8. セキュア パージ処理のステータスを確認します。

   ```
   volume encryption secure-purge show
   ```

関連情報

- "snapmirror update"

著作権に関する情報

Copyright © 2026 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権を有し、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権については、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。