



データガバナンス、プライバシー、ライフサイクル

Information Security for Workload Factory

NetApp
September 16, 2026

目次

データガバナンス、プライバシー、ライフサイクル	1
NetApp Workload Factoryのデータ処理とデータレジデンシー	1
Workload Factoryによって処理されるデータクラス	1
Workload Factory が保持するデータクラス	1
情報が保管される場所	1
情報の保存期間	2
VPCからどのような情報が流出するのか	2
構成およびメタデータ収集の範囲	3
NetApp Workload Factoryの暗号化と暗号化キー管理	7
FSxにおけるKMSの保存時暗号化範囲	7
認証情報保護（サービス側エンベロープ暗号化）	7
NetApp Workload Factoryアカウントの削除	8

データガバナンス、プライバシー、ライフサイクル

NetApp Workload Factoryのデータ処理とデータレジデンシー

NetApp Workload Factoryは、サービスが処理する運用データ、各データクラスがセキュリティモデルにどのように適合するか、データがどこに保存されるか、どのくらいの期間保持されるか、そしてデータが顧客環境から外部に持ち出されるかどうかを説明するカテゴリにデータ処理を整理します。主要なデータクラスには、構成情報とメタデータ、運用ログとイベント、およびテレメトリが含まれます。保持されるデータには、FSx for ONTAP構成スナップショット、認証情報参照、AIの使用状況とコストデータ、監査記録、および短期間有効な応答キャッシュが含まれる場合があります。ストレージと処理の場所はデータタイプによって異なります。一部の情報は顧客のAWSアカウントに残りますが、その他の運用データはNetAppアカウントに保存されます。

Workload Factoryによって処理されるデータクラス

NetApp Workload Factory は、以下のデータクラスを扱います。

- 設定とメタデータ
- 運用ログとイベント
- テレメトリー

Workload Factory が保持するデータクラス

Workload Factory は以下のデータを保持します：

- FSx構成スナップショット（スキャンごとに更新）
- ONTAP認証情報参照、またはKMSエンベロープ暗号化で暗号化された認証情報（選択された認証情報モードによる）
- EDAメトリクス
- CloudFormation テンプレート（7日間 Expires ヘッダー）
- AIの利用状況とコストデータ
- 監査記録
- Redis は（FSx の応答を）20 分の TTL でキャッシュします。

情報が保管される場所

AWSアカウント

- ONTAP管理者パスワードはAWS Secrets Managerに保存されます。
- Amazon Bedrock は、お客様の AWS アカウント内の STS が引き受けたロールを通じて、お客様の推論プロファイル ARN を使用して AI 推論（EMS 分析）を処理します。

NetAppアカウント

- FSx構成、バランスプラン、ARP構成、およびAI使用制限
- 一時的なAWS STS認証情報（Redisにキャッシュ）、レスポンスキャッシュ、ロック、およびデプロイメント状態
- CloudFormation/Terraformテンプレート、WAD構成記述子、および圧縮レポート
- AI使用状況計測とコレクターのパフォーマンス指標
- EDA集計指標
- アクション監査証跡
- OpenTelemetry トレース

地域に関する考慮事項

- Amazon Bedrockサービスが利用可能なリージョンに保存されます。
- NetApp 内部は `us-east-1` および `us-west-2` で動作します。

情報の保存期間

このセクションでは、保持対象となるカテゴリをまとめています。詳細な値とポリシーの動作については、リンク先のページを参照してください。

- 認証情報および一時的なAWS STS認証情報の保持：["NetApp Workload Factoryの資格情報の保持"](#)
- 運用指標およびテレメトリデータの保持：["メトリクスとテレメトリのリファレンス（NetApp Workload Factory）"](#)
- 監査記録の保持：NetApp Console の保持ポリシーによって管理されます（Workload Factory では制御されません）

VPCからどのような情報が流出するのか

このセクションでは、送信データのカテゴリをまとめています。プロトコルレベルおよび機能レベルの詳細については、リンク先のページを参照してください。

Workload Factoryサービスへの管理プレーントラフィック

管理操作においては、FSx構成、ボリュームメタデータ、リソース識別子、および操作コマンドはHTTPS経由でWorkload Factoryサービス層に送信されます。

NetApp Console 監査サービスへの監査レコード

追跡対象となるすべての操作は、以下の情報を送信します。

- accountId
- actionName
- status
- resourceId

- userId
- requestData
- responseData
- timestamps
- IP address
- workspaceId

AI分析トラフィック

FSx for ONTAP のAI診断のために送信される緊急管理システム（EMS）イベント、レイテンシデータ、およびエラーログは、設定済みの推論プロファイルを使用してAWSアカウント経由でAmazon Bedrockに転送されるため、このトラフィックはNetAppシステムに到達することなく、お客様の環境内に留まります。

AI分析トラフィックに関する詳細については、以下を参照してください。

- ["NetApp Workload FactoryのAI制御の概要"](#)
- ["Bedrock の NetApp Workload Factory AI 診断へのオプトイン"](#)
- ["NetApp Workload FactoryにおけるAIツールの境界"](#)

AWSサービスAPIトラフィック

["NetApp Workload Factoryの接続性と信頼パス"](#)を参照してください。

テレメトリとメトリクスの収集

["メトリクスとテレメトリのリファレンス"](#)を参照してください。

構成およびメタデータ収集の範囲

ファイルシステムレベル

- ファイルシステム構成（展開タイプ Gen1/Gen2、スループット容量、ストレージ容量、ストレージタイプ）
- 優先サブネット、セキュリティグループ、VPC構成
- KMS暗号化キーメタデータ
- ファイルシステムタグ
- ファイルシステムのライフサイクルステータス
- メンテナンスウィンドウの設定

ボリュームレベル（包括的）

- ID と状態：ボリューム名、UUID、タイプ（rw/dp/ls）、スタイル（FlexVol/FlexGroup）、状態（オンライン/オフライン/制限付き）、作成時間
- 容量：合計サイズ、使用済み、利用可能、物理的に使用済み、使用率、SSD フットプリント、容量プール

フットプリント、非アクティブ データ バイト/パーセント

- 階層化：ポリシー（すべて/自動/なし/スナップショットのみ）、最低冷却日数
- QoS：割り当てられたQoSポリシー名
- NAS構成：ジャンクションパス、エクスポートポリシーの割り当て、UNIXパーミッション、セキュリティスタイル（unix/ntfs/mixed）
- スナップショット：スナップショットの予約サイズ/割合/使用率、自動削除設定
- データ効率：圧縮タイプ／状態、重複排除、コンパクション、スペース削減
- 自動サイズ調整：モード（grow/grow_shrink/off）、最小／最大サイズ、拡大／縮小しきい値
- SnapLock：タイプ（コンプライアンス/エンタープライズ/non_snaplock）、保持期間（最小/最大/デフォルト）、自動コミット期間
- クローン：親ボリューム / スナップショット / ストレージ VM、FlexCloneであるか、スプリット ステータス
- iノード/ファイル数：最大可能数、最大設定数、使用数
- 暗号化：有効/無効の状態
- アクセス時間：atime更新の有効/無効と更新期間
- SnapMirror：保護ステータス、デスティネーションタイプ（クラウド/ONTAP）
- FlexGroup リバランス：不均衡率、最大しきい値
- ボリューム移動：デスティネーションアグリゲート、移動状態
- FlexCacheエンドポイントタイプ：none/cache/origin
- タグ：ONTAPレベルのボリュームタグ

スナップショットデータ

- スナップショット名、UUID、作成日時、有効期限
- サイズ（バイト）
- SnapMirrorラベル
- SnapLock 有効期限とロック状態
- 状態（有効／無効／部分的）
- ユーザーコメント
- スナップショット ポリシー：名前、有効状態、スケジュール コピー（カウント、保持期間、スケジュール名、プレフィックス、SnapMirror ラベル）

エクスポート ポリシー

- ポリシー名、ID、関連付けられたストレージVM
- ルール：プロトコルリスト（NFS/CIFS/FlexCache）、クライアントのマッチパターン、読み取り専用ルール、読み取り / 書き込みルール、スーパーユーザールール、ルールインデックス/優先度
- SUID、デバイス作成、chownモード、匿名ユーザーマッピング、NTFS UNIXセキュリティ設定

S3アクセスポイント

- ライフサイクル状態（利用可能／作成中／削除中／失敗／設定ミス）
- 作成日時、ARN、エイリアス、名前
- ファイル所有者ユーザーと種類（UNIX/WINDOWS）
- ネットワーク構成（インターネットアクセスとVPCアクセス、VPC ID）
- AWSタグ
- メタデータスキャン有効化、ジャーナリング有効化、CloudTrail ARN

ランサムウェア対策（ARP）

Workload Factoryは、構成ステータスとイベントの詳細の両方を収集します。

- ボリュームごとの状態（有効／無効／dry_run／一時停止）
- 攻撃される可能性（なし／低い／中程度／高い）
- タイムスタンプ付き攻撃レポート
- 検出パラメータ：ファイル拡張子のしきい値、名前変更率の急増 %、エントロピー率の急増 %、ファイル作成 / 削除率の急増 %
- 疑わしいファイル：ファイルパス、ファイル名、ファイル形式、疑わしい時刻、関連ボリューム

レプリケーション / SnapMirror

- リレーションシップUUID、状態、正常性ステータス
- ソースと宛先（ストレージVM、パス、クラスタ）
- 転送統計情報（転送バイト数、所要時間、終了時刻、状態）
- ポリシー（名前、タイプ：非同期/同期/継続的）
- スロットル設定
- 遅延時間
- 異常の理由（メッセージとコード）
- 現在の転送エラー

igroup

- 名前、UUID、プロトコル（FCP/iSCSI/混合）、OSタイプ
- イニシエータ（IQN/WWPN）、接続状態、最終確認時刻
- LUNマッピング（論理ユニット番号、LUNの詳細）

LUN

- 名前、UUID、シリアル番号、OSの種類、有効状態
- サイズ、使用容量、シンプロビジョニング設定
- 場所（ボリューム、ノード、論理ユニットパス）

- 自動削除設定
- コンテナの状態、マッピングされた状態、読み取り専用状態
- QoSポリシー
- パフォーマンス指標（IOPS、レイテンシ、読み取り / 書き込み / 合計別スループット）
- 整合性グループのメンバーシップ

FlexCache

- 元のボリューム/ストレージVM/クラスター、キャッシュサイズ、パス
- ライトバック有効、DRキャッシュステータス
- 相対サイズ設定
- ディレクトリパスを事前入力する
- キャッシュとオリジン間の接続状態

ストレージVMレベル

- 名前、UUID、状態（実行中／停止中）、サブタイプ
- 有効/許可されているプロトコル（NFS、CIFS、iSCSI、FCP、NVMe、S3）
- DNSサーバーとドメイン
- 名前サービススイッチの設定（passwd、group、hostsなど）
- IPインターフェース（名前、IPアドレス、サービス）
- 割り当て済みアグリゲート
- ランサムウェア対策のデフォルトボリューム状態
- スペース適用設定
- ピア関係（アプリケーション、状態、リモートクラスター／ストレージVM）

アグリゲート / ストレージレベル

- 集約名、UUID、状態、RAID状態
- ブロックストレージ：ディスク数、RAIDサイズ、使用可能/使用済み/合計容量、物理使用済み
- クラウドストレージの使用
- 効率：比率、論理使用量、削減量
- 暗号化、ミラー、SnapLock 設定
- パフォーマンス指標（IOPS、レイテンシ、スループット）

利用状況指標（EDA）

- データ収集頻度：容量/スループットは12時間ごと、レイテンシは20分ごと
- 粒度：時間範囲ごとに約 60 データポイントに正規化
- 保持および保管に関する詳細：["メトリクスとテレメトリのリファレンス"](#)

NetApp Workload Factoryの暗号化と暗号化キー管理

NetApp Workload Factoryは保存データの暗号化を使用し、Workload FactoryとAWSサービス全体にわたる明確なキー管理責任を定義しています。Amazon FSx for NetApp ONTAPファイルシステムの場合、独自のAWS KMSキーを選択するか、AWSが管理するデフォルトのキーを使用できます。また、FSx for ONTAPはそのキーを使用して暗号化操作を実行します。Workload Factoryは、保存されたONTAPクレデンシャルを保護するためにエンベロープ暗号化も使用しています。

FSxにおけるKMSの保存時暗号化範囲

Workload Factory を使用して FSx for ONTAP ファイルシステムを作成する場合、保存データの暗号化用に独自の AWS KMS キーをオプションで指定できます。キーを指定しない場合、Workload Factory は AWS が管理するデフォルトの FSx キーを使用します。

暗号化されるもの

基盤となる EBS ボリュームに保存されているすべてのデータは、FSx for ONTAP ファイルシステムをバックアップします（AWS FSx による保存時の暗号化）。

鍵の所有権

KMSキーはAWSアカウント内に存在します。

キーの選択と使用に必要な権限

Workload Factory には以下が必要です：

- kms:DescribeKey
- kms:ListKeys
- kms:ListAliases
- kms>CreateGrant (FSx for ONTAP サービスがキーを使用できるようにするため)

キーアクセスパターン

Workload Factoryは、お客様のKMSキーを使用してデータを直接暗号化または復号化することはありません。ファイルシステム作成時に、Amazon FSx for NetApp ONTAP APIにキーIDを渡します。暗号化処理はAmazon FSx for NetApp ONTAPが実行します。

認証情報保護（サービス側エンベロープ暗号化）

Workload Factory を使用して ONTAP クレデンシャル（管理者パスワード）を保存すると、永続化する前にエンベロープ暗号化を使用して保護されます。

暗号化方式

資格情報レコードごとに一意のデータ暗号化キー（DEK）を使用したAES-256-CBC。

エンベロープ暗号化フロー

1. 認証情報ごとに固有の256ビットDEKが生成されます。
2. DEKは認証情報（パスワード）を暗号化します。

3. DEK自体はルートキーで暗号化され、暗号化された認証情報とともに保存されます。
4. 平文のDEKは保存されません。

暗号化コンテキスト

各データキーは、特定の認証情報レコードに暗号学的に紐付けられており、レコード間でキーが再利用されるのを防いでいます。

代替案：AWS Secrets Manager

サービスに暗号化されたパスワードを保存する代わりに、ONTAP 認証情報をご自身のアカウントの AWS Secrets Manager に保存できます。Workload Factory はパスワードを一切認識したり保存したりしません。Secrets Manager の ARN を Lambda リンクに渡し、Lambda が実行時にお客様の VPC 内でパスワードを取得します。



AWS Secrets Manager は、GovCloud アカウントに必要です。

NetApp Workload Factory アカウントの削除

アカウントの削除はセルフサービス操作ではありません。これは、Workload Factory サービスとAWSアカウント内のリソースの両方が関わるオフボーディングワークフローです。クリーンアップには、Workload Factory アカウント、FSx for ONTAP ファイルシステム、認証情報、リンク、通知チャンネル、および関連するIAM、AWS Lambda、Amazon CloudWatch リソースに関連するデータの安全な削除が含まれます。この操作は元に戻すことができません。

Workload Factory アカウントを削除する必要がある場合は、"[NetAppサポートにお問い合わせください。](#)"

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。