セキュリティモデルと責任
Information Security for Workload Factory

NetApp
September 16, 2026

目次

セキュリティモデルと責任

NetApp Workload Factory のセキュリティモデルについて

NetApp Workload Factoryは、AWS環境でAmazon FSx for NetApp ONTAP上で実行されるワークロードの管理と最適化を支援するSaaSコントロールプレーンです。セキュリティの成果は、NetApp、AWS、およびお客様の組織間での責任共有によって決まります。

高レベルのセキュリティモデル

- Workload Factoryは、IAMのassume-roleモデルを使用して、お客様のアカウント内のAWS APIを呼び出すための一時的なAWS STS認証情報を取得します。
- ワークフローによっては、AWS API を通じて公開されていない ONTAP ネイティブの操作が必要となる場合があります。そのような操作は、お客様がデプロイした実行コンポーネント（Lambda リンクなど）を使用して、VPC 内で実行できます。
- 観測可能性シグナル（メトリクス、テレメトリ、運用記録）は、運用監視および調査をサポートします。

重要な復習問題

- Workload Factoryは、お客様のAWSアカウントに対してどのようなアクセス権限（ロールの信頼＋アクセス許可）を必要としますか？
- 想定されるワークフロー（AWS APIのみの操作、またはVPCコンポーネントを介したONTAPネイティブ操作）には、どの実行パスが適用されますか？
- どのようなデータカテゴリ（設定/メタデータ、運用ログ/イベント、テレメトリ）が処理され、それらはどこに保存されますか？
- どのような監視シグナルが存在し、それらの保持特性はどのようなものですか？

次の手順

- "NetApp Workload Factoryの共同責任の境界"
- "NetApp Workload Factory の接続性と信頼パス"
- "NetApp Workload Factoryの最小権限のアクセス許可階層"

NetApp Workload Factoryの共同責任の境界

NetApp Workload Factory のセキュリティ責任は、NetApp （SaaS運用）、AWS （クラウドインフラストラクチャおよびマネージドサービス）、およびお客様（顧客設定）の間で共有されます。各当事者の責任範囲を理解することで、AWS環境を正しく構成し、セキュリティ上のギャップを回避することができます。これらの境界線は、NetApp が運用するもの、AWS が保護するもの、およびお客様自身が設定・維持する必要があるものを明確にします。

NetAppの責任範囲（サービス側）

NetAppは、Workload Factory SaaSプラットフォームの運用とセキュリティ確保を担当しています。これには、保存された構成参照と運用データのサービス側での処理が含まれます。

AWSの責任範囲（クラウドプラットフォーム）

AWS は、デプロイメントやワークフローで使用されるクラウドインフラストラクチャとマネージドサービス（例：IAM/STS、FSx for ONTAP、CloudWatch、KMS、Secrets Manager、CloudFormation、Lambda、およびネットワークプリミティブ）のセキュリティに責任を負います。

お客様の責任（お客様の設定）

お客様は以下の責任を負います：

- AWS IAMロール、信頼ポリシー、および最小権限のアクセス許可
- VPCの制御（サブネット、セキュリティグループ、ルーティング、エンドポイント、およびエグレス）
- クレデンシャル管理（ワークフローで必要な場合は ONTAP クレデンシャルを含む）
- 暗号化とキー管理の決定（たとえば、FSx for ONTAP のオプションのカスタマー管理 KMS キー）
- 監視、アラート、データ保持ポリシー、およびインシデント対応プロセス

収集する証拠

- IAMロールの信頼関係（外部ID条件を含む）
- IAM権限階層の選択とポリシー成果物
- ネットワーク境界の決定（AWS APIのみか、LambdaリンクなどのVPC実行コンポーネントか）
- 可観測性に関する決定と保持に関する期待
- AI有効化の決定（AI診断は、明示的に無効化されない限り、デフォルトで有効になります）

NetApp Workload Factory オンボーディングセキュリティワークフロー

NetApp Workload Factoryへのオンボーディングは、製品の使用を開始する前に、お客様のAWS環境への安全なアクセスを確立します。このプロセスは、AWSの信頼設定、権限スコープの設定、接続性のセットアップ、可観測性の検証、およびオプションのAI診断の有効化を組み合わせたものです。

ステップ1：オンボーディングの方針を決定する

- AWSアカウントと環境境界（例：本番環境と非本番環境の分離）を特定します。
- 必要なワークフロー（読み取り専用の検出、プロビジョニング、ONTAPネイティブ操作）を特定します。
- ワークフローのニーズに基づいて、VPC実行コンポーネント（例：Lambda リンク）をデプロイするかどうかを決定します。

- AI診断を有効にするかどうかを決定します（デフォルトでは有効）。

関連情報

- "認証情報の種類"
- "Lambdaリンクの概要"
- "AI制御の概要"

ステップ2：AWSの信頼関係とアクセスを確立する

1. AWSアカウントにIAMロールをデプロイします。
2. 信頼ポリシーで外部IDを使用したゲートロールの引き受けを行います。
3. Workload Factory にロール ARN と外部 ID を登録します。

関連情報

"AWSアカウントの統合"

ステップ3：最小権限のアクセス許可を適用する

1. 想定するワークフローをサポートする最小限の権限レベルを選択してください。
2. リクエストごとのセッションポリシーによって、実行される操作に対するアクションが制限されていることを確認します。

関連情報

"NetApp Workload Factoryの最小権限のアクセス許可階層"。

ステップ4：接続性とVPC境界の設定（必要に応じて）

1. AWSエンドポイントへの必要なネットワークパスを検証します。
2. ONTAPネイティブ操作が必要な場合は、VPC内で適切な実行オプションをデプロイして検証してください。

関連情報

- "NetApp Workload Factory の接続性と信頼パス"
- "NetApp Workload FactoryにおけるONTAPの実行オプション"

ステップ5：可観測性の検証

1. メトリクスとテレメトリが想定どおりに収集および保持されていることを確認してください。
2. トラブルシューティングや調査に必要な運用記録にアクセスできることを確認してください。

関連情報

- "NetApp Workload Factoryの可観測性の概要"
- "NetApp Workload Factoryのメトリクスとテレメトリ"

ステップ6：AI診断を有効にする（オプション）

AI診断はデフォルトで有効になっています。これらを有効にする場合は、前提条件を満たしていること、および必要な最小限の権限範囲であることを確認してください。

関連情報

- "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"

NetApp Workload Factoryのコンプライアンスとセキュリティ体制

NetApp Workload Factoryは、コンプライアンスとセキュリティを最優先事項として構築されています。Workload Factory のすべてのワークロードは、Amazon FSx for NetApp ONTAP上で実行されます。"AWSセキュリティ機能"に加えて、NetApp Workload Factoryには"SOC2 Type 1、SOC2 Type 2、およびHIPAA準拠"があります。

Amazon FSx for NetApp ONTAP for NetApp Workload Factory は"エンタープライズアプリケーションをデプロイするためのAWSソリューション"であり、AWS Well-Architected のベストプラクティスに準拠しています。

著作権に関する情報

商標に関する情報