



ONTAP運用とLambdaリンク（顧客VPCコンポーネント）

Information Security for Workload Factory

NetApp
September 16, 2026

目次

ONTAP運用とLambdaリンク（顧客VPCコンポーネント）	1
NetApp Workload Factory の Lambda リンクについて	1
リンクセキュリティアーキテクチャ	1
Lambda link対NetApp Console agent	2
関連情報	2
NetApp Workload Factory向けのLambdaリンクのポートと呼び出し	3
リクエストの種類	3
アウトバウンドネットワーク境界	3
Workload FactoryがLambdaリンクを呼び出します	3
関連情報	4
Lambda リンクの IAM 権限（NetApp Workload Factory 用）	4
Lambda実行ロールの権限	4
Workload Factory の呼び出し権限	4
NetApp Workload FactoryのLambdaリンクのライフサイクル	4
ライフサイクル管理ポイント	5

ONTAP運用とLambdaリンク（顧客VPCコンポーネント）

NetApp Workload Factory の Lambda リンクについて

NetApp Workload Factory は、VPC にデプロイされた AWS Lambda 関数である *link* を使用して、Amazon FSx for NetApp ONTAP API がこれらの操作を公開していない場合でも、ONTAP ネイティブ操作を AWS アカウント境界内に保持します。このリンクはお客様のサブネットとセキュリティグループ内で実行されるため、実行コンポーネントはお客様の AWS 環境内に留まります。Workload Factory は、利用可能な AWS サービス API ではなく、ONTAP への直接アクセスが必要な操作に対してのみリンクを呼び出します。リンクのアーキテクチャを、NetApp Console エージェントのセキュリティおよび運用プロファイルと比較します。

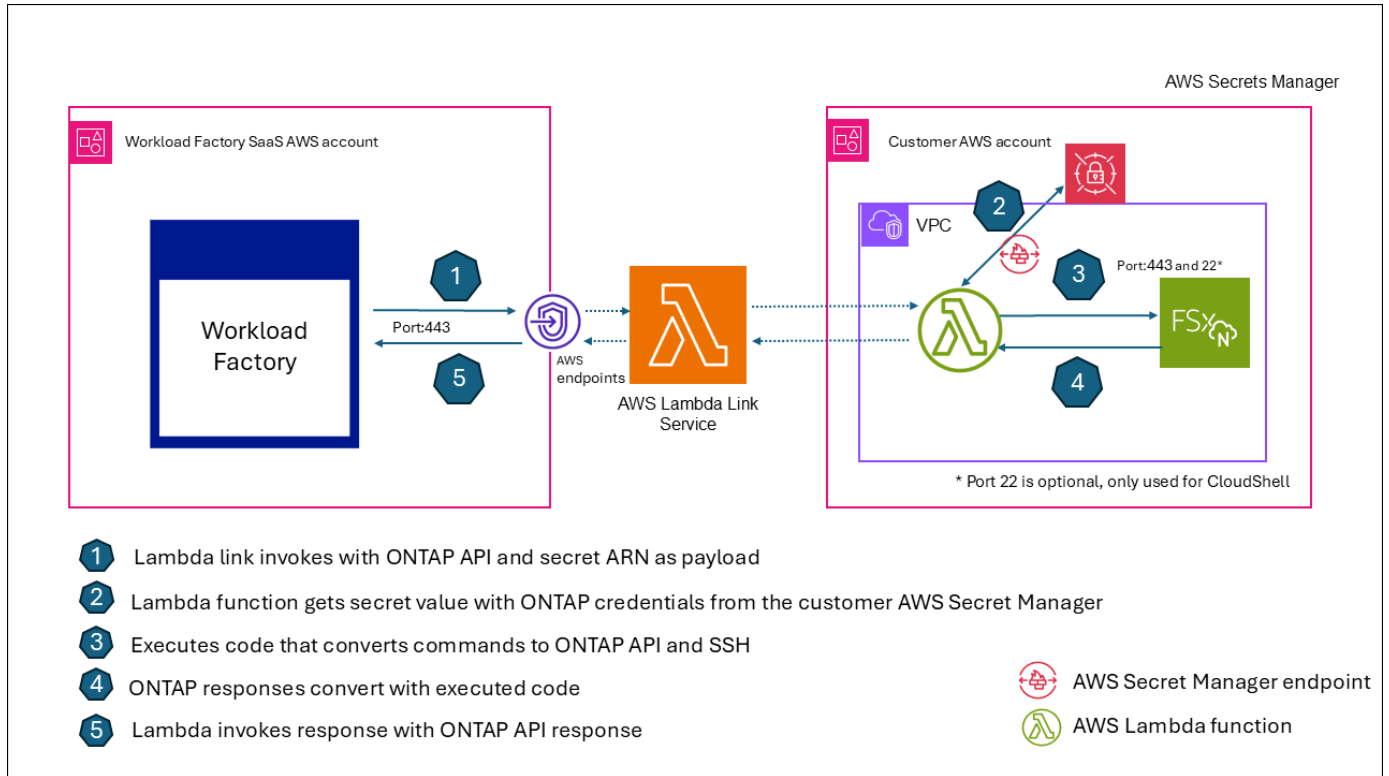
リンクセキュリティアーキテクチャ

Workload Factory リンクは、Workload Factory アカウントと 1 つ以上の FSx for ONTAP ファイルシステムとの間に信頼関係と間接的な接続を作成します。

以下の表は、Lambdaリンクのセキュリティアーキテクチャの概要を示しています。この情報を使用して、AWSアカウントにおけるLambda関数のデプロイおよび実行方法（ネットワーク構成、実行環境、運用上の制限など）を理解してください。

プロパティ	詳細
コンピューティング	AWS Lambda（コンテナイメージ）
ランタイム	Node.js 22
導入	CloudFormation AWS アカウントのスタック
VPCの配置	お客様のサブネット、お客様のセキュリティグループ
Timeout	呼び出しごとに10秒
呼び出し	同期（RequestResponse）
パッケージの種類	コンテナイメージ（NetApp ECR）

以下の図は、Lambdaリンクのセキュリティアーキテクチャを示しています。



Lambda link対NetApp Console agent

LambdaリンクとNetApp Consoleエージェントは、異なる目的を果たし、セキュリティおよび運用上の影響もそれぞれ異なります。

寸法	リンク（Lambdaベース）	NetApp コンソールエージェント（VM/Pods ベース）
ランタイムモデル	サーバーレス（AWS Lambda）、顧客によるデプロイ	顧客がデプロイしたVM/コンテナ。NetApp コンソールサービスポッドを実行します。
主な範囲	コントロールプレーン ONTAP REST 操作 （AWS API が当該操作をサポートしていない場合のみ）	データサービスのオーケストレーションと サポート
データサービスサポ ート	データサービスは提供していません	データサービスをホストできます （NetApp コンソールサービスポッドを実 行します）
運営上の諸経費	常時稼働のVMはありません	VMライフサイクル管理とアップグレード

関連情報

システム間の接続性マップ全体については、"[NetApp Workload Factory の接続性と信頼パス](#)"を参照してください。

NetApp Workload Factory向けのLambdaリンクのポートと呼び出し

NetApp Workload Factory は、Lambda リンク要求とポート境界を使用して、必要なアウトバウンド接続と IAM 認証済み呼び出しを定義します。このリンクは、ONTAP 管理エンドポイントへの HTTPS リクエスト、診断用の読み取り専用 SSH コマンド、およびヘルスチェックをサポートします。すべての接続は VPC 内のリンクからアウトバウンドで行われるため、インバウンド接続や公開エンドポイントは必要ありません。Workload Factory は、IAM ベースの認証を使用して AWS Lambda API 経由でリンクを呼び出します。

リクエストの種類

- HTTPS (ONTAP REST API) : HTTPS 呼び出しをボリューム、ストレージ VM、およびクラスタ操作のための ONTAP 管理エンドポイント (ポート 443) にプロキシします。
- SSH (ONTAP CLI) : 診断およびパフォーマンスデータ取得のため、ポート22で読み取り専用の ONTAP CLI コマンドを実行します。
- ヘルスチェック: ステータスとサポートされている機能を返します。

アウトバウンドネットワーク境界

送受信方向	ポート	デスティネーション	目的
アウトバウンド	443	ONTAP管理用IPアドレス (VPC内)	REST API操作
アウトバウンド	22	ONTAP管理用IPアドレス (VPC内)	SSH CLIコマンド
アウトバウンド	443	AWS Secrets Managerエンドポイント (オプション)	Secrets Manager使用時の認証情報の取得

受信接続は不要です。このリンクはエンドポイントを公開していません。Workload Factory はAWS `lambda:InvokeFunction` APIを使用してそれを呼び出します。

Workload FactoryがLambdaリンクを呼び出します

Workload Factory は、IAM ベースの認証を使用して、AWS Lambda API (`lambda:InvokeFunction`) を介して Lambda リンクを呼び出します。

呼び出しペイロードには以下が含まれます：

- ターゲットONTAP管理エンドポイント (IPアドレス／ホスト名)
- 実行する操作 (REST APIパスまたはSSHコマンド)
- 認証情報 (インライン認証情報またはSecrets Manager ARN参照)

関連情報

システム間の接続性マップ全体については、"[NetApp Workload Factoryの接続性と信頼パス](#)"を参照してください。

Lambda リンクの IAM 権限（NetApp Workload Factory 用）

NetApp Workload Factory は、Lambda リンクのアクセス許可境界を使用して、Lambda の実行および Workload Factory の呼び出しに必要な IAM アクセスを定義します。これらの権限は任意ですが、ONTAP ネイティブ操作には必須です。Secrets Manager サポートを設定すると、リンクは実行時に AWS Secrets Manager から ONTAP 認証情報を直接取得し、パスワードは VPC 内でのみ転送されます。Secrets Manager から Lambda 関数、そして ONTAP エンドポイントへと転送されます。

リクエストパスとポートの要件については、"[Lambdaリンクポートと呼び出し](#)"を参照してください。

Lambda実行ロールの権限

VPC内にリンクをデプロイする際、Lambda実行ロールには以下の権限が必要です：

アクセス許可	目的
ec2:CreateNetworkInterface / ec2:DescribeNetworkInterfaces / ec2:DeleteNetworkInterface	標準のVPC接続型Lambdaネットワーク
ec2:AssignPrivatelPAddresses / ec2:UnassignPrivatelPAddresses	VPC ENI IP管理
secretsmanager:GetSecretValue (FSxSecret* にスコープ設定)	ONTAP 認証情報の取得（Secrets Manager が有効になっている場合のみ）
CloudWatch ログ（管理ポリシー）	Lambda実行ログ

Workload Factory の呼び出し権限

Lambda リンクのリソースベースポリシーは、NetApp Workload Factory のサービスプリンシパルに次の権限を付与します：

アクセス許可	目的
lambda:InvokeFunction	Lambda関数を実行する
lambda:GetFunction	健康状態とステータスの確認
lambda:UpdateFunctionCode	バージョンアップグレード（イメージ更新）
lambda:GetFunctionConfiguration	構成検証

NetApp Workload FactoryのLambdaリンクのライフサイクル

NetApp Workload Factoryは、Lambdaリンクのライフサイクル制御を利用して、運用上

のリスクを最小限に抑えながら、デプロイメント、ヘルスマニタリング、および制御されたイメージ更新を管理します。Amazon CloudFormationスタックを再デプロイすることなく、`lambda:UpdateFunctionCode`権限を使用して、Lambdaリンクコンテナイメージを更新し、改善点やセキュリティパッチをデプロイできます。ライフサイクル制御では、リンクの状態を監視する方法や、Lambdaリンクとその関連リソースが不要になったときに削除する方法も定義されます。

ライフサイクル管理ポイント

- デプロイ：Amazon CloudFormation または Terraform スタックのデプロイを介して自動化
- 監視：ヘルスチェックで接続の問題を検出し、障害カウンターで信頼性を追跡します。
- 削除：CloudFormation スタックを削除すると、AWS アカウントから Lambda と関連リソースが削除されます。

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。