生成AIセキュリティ制御

Information Security for Workload Factory

NetApp
September 16, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/workload-infosec/ai-controls-overview.html on September 16, 2026. Always check docs.netapp.com for the latest.

目次

生成AIセキュリティ制御

NetApp Workload FactoryにおけるAIコントロールについて説明します

NetApp Workload Factoryには、モデルへのアクセス、データ範囲、および実行時動作に対するセキュリティ制御を適用しながら、診断を加速する生成AI機能が含まれています。

Workload Factoryは、デフォルトでAI診断を有効にしています。Workload Factoryの「管理」設定から、生成AI機能をいつでも無効にできます。"GenAI機能の管理方法について詳しくはこちらをご覧ください。"

セキュリティ関連のAI機能の概要

Workload Factoryは現在、生成AIを以下の機能に適用しています：

- Ask Me アシスタント（厳選された NetApp ドキュメントを用いた RAG、ソースに基づく回答）
- レイテンシ分析
- EMSイベント分析
- エラーログ分析

AI診断のためのAWS Bedrockの概要

Workload Factory は、AI推論にAmazon Bedrockを使用しています。推論処理は、お客様のAWSアカウント内で、お客様が設定した認証情報と推論プロファイルに基づいて実行されます。

関連情報

- "NetApp Workload Factory AI診断向けのAmazon Bedrockのオプトイン"
- "NetApp Workload FactoryにおけるAIツールの境界"
- "AIモデルのパラメータとNetApp Workload Factoryの課金"

NetApp Workload Factory AI診断向けのAmazon Bedrockのオプトイン

NetApp Workload FactoryのAI診断機能は、Amazon Bedrockを使用してイベントを分析し、この機能はデフォルトで有効になっています。Workload Factoryが選択したBedrockモデルを呼び出し、診断データを収集するには、IAM権限、推論プロファイル、およびSSH機能を備えた接続済みLambdaリンクを設定する必要があります。これらのコンポーネントのいずれかが欠落している場合、またはBedrock構成が削除された場合、AI診断は利用できなくなります。

AI診断はデフォルトで有効になっています。

開始する前に

- アカウントにAWS Bedrock推論プロファイルが含まれていることを確認してください。
- 診断データ収集のために、SSH機能を備えた接続済みのLambdaリンクが必要です。

手順

1. IAM ロールに Bedrock 権限を付与する：
    - `bedrock:InvokeModel`
    - `bedrock:InvokeModelWithResponseStream`
    - `bedrock:ListInferenceProfiles`
    - `bedrock:GetInferenceProfile`
2. Workload Factory の設定で、推論プロファイルの ARN を設定します。

前提条件となる要素が一つでも欠けている場合、システムは不足している具体的な要素を報告し、AI機能は非アクティブ状態のままになります。

AI診断を無効にする

AI診断を無効にするには：

- Bedrock の権限を IAM ロールから削除するか、
- Workload Factoryの設定でBedrockの設定を削除します。

AI診断は直ちに利用できなくなり、残留するデータ処理は発生しません。

地域および地域間推論プロファイル

Bedrock の推論は、推論プロファイルで指定された AWS リージョンで実行されます。リージョン間推論プロファイルを使用する場合、AWS は標準的な AWS Bedrock の動作に従って、プロファイルの設定で指定された任意のリージョンにリクエストをルーティングする可能性があります。データは AWS インフラストラクチャの外部に持ち出されません。

NetApp Workload FactoryにおけるAIツールの境界

NetApp Workload Factory は、AI 機能が AWS および ONTAP 環境とどのように連携するかについて厳格な境界を適用しているため、意図しない変更のリスクを負うことなく、AI による診断を信頼することができます。Amazon Bedrock は、変更コマンドをブロックし、サイズと実行によって出力を制限する読み取り専用の AWS CLI および ONTAP CLI 診断ツールを使用しており、使用されるデータはすべて一時的なものであり、NetApp Workload Factory または AWS によって保持されることはありません。

ツールの安全制御

ツール	機能	安全対策
AWS CLI（読み取り専用）	読み取り専用のAWS CLIコマンド（describe、list、get）を実行する	すべての変更動詞（作成、削除、変更、更新、配置、削除）をブロックします。1ステップあたり最大10個のコマンド。出力は20 KBで切り捨てられます。
ONTAP CLI（読み取り専用）	SSHを使用して読み取り専用のONTAP CLIコマンドを実行する	すべての変更動詞（削除、破壊、作成、変更、移動）をブロックします。出力は途中で途切れています。

エージェントは、リソースを変更、作成、または削除することはできません。観察と診断のみ実行できます。

データ保持とモデルトレーニングの境界

AWSのポリシーに基づき、Amazon Bedrockは、基盤モデルのトレーニングや改善のために、お客様の入力データや出力データを保存または使用することはありません。オンデマンド推論（Workload Factoryで使用）の場合、AWSはデータを一時的に処理し、レスポンスを返した後はデータを保持しません。

AIモデルのパラメータとNetApp Workload Factoryの課金

NetApp Workload Factoryは、AIガバナンスに関連するモデル構成、使用範囲、および課金範囲を定義します。設定されたモデルは決定論的なパラメータを使用し、一貫性のある分析結果をサポートするために構造化されたJSONを返します。AWSはAmazon Bedrockの推論処理費用をお客様のアカウントに請求しますが、Workload FactoryはAIの使用状況を追跡し、アカウントごとの月額コストを可視化します。これらのセクションでは、モデルのパラメータと、AIの利用に適用される制限について説明します。

モデルとパラメータ

パラメータ	**Value**
モデル	Anthropic Claude （クロスリージョン推論プロファイルを使用）
温度	0（決定論的、ランダム性なし）
最大出力トークン数	2,048
最大推論ステップ数	分析1件あたり15
出力形式	構造化JSON（概要、重大度、根本原因、是正措置）

請求および使用制限

- AWS は Bedrock の推論処理費用をお客様のアカウント（お客様の推論プロファイル、お客様の認証情報）に請求します。
- Workload Factoryは、AIの使用状況を内部で追跡します。
- Workload Factoryは、アカウントごとの月間コストを可視化します。

  "NetApp Workload Factoryでストレージコストを追跡する"

Ask Me AIアシスタント

NetApp Workload Factory の Ask Me セキュリティアーキテクチャ

Ask Me は、NetApp Workload Factory に組み込まれた生成AI搭載アシスタントです。Amazon FSx for NetApp ONTAP および Workload Factory のトピックに関するリアルタイムの会話サポートを提供します。回答は検証済みのNetAppドキュメントに基づいており、Ask Me は公開インターネットにアクセスしたり、顧客データを使用してモデルをトレーニングしたりすることはできません。複数のセキュリティ層により、悪意のあるクエリをブロックし、応答をサポート対象ドメインに限定し、ユーザー入力がシステム命令を上書きするのを防ぎます。Ask Me がツールを使用する場合、認証境界、読み取り専用クエリの強制、一時的なサンドボックス、および監査ログが、実行の制限と監視に役立ちます。

Workload Factory の 管理 設定からいつでも Ask Me を無効にできます。これにより、ユーザーアカウントのアシスタント機能が無効になります。"GenAI機能の管理方法について詳しくはこちらをご覧ください。"

Ask MeにおけるRAGアーキテクチャ

Ask Meは、検索拡張生成（RAG）を使用しています。

- 厳選されたナレッジベース：回答は、検証済みで公開された NetApp ドキュメントの管理されたコーパスに基づいています。
- 検索スコアリングとフィルタリング：モデルのコンテキストには、十分に関連性の高いコンテンツのみが含まれます。
- インターネットアクセスなし：モデルは外部コンテンツの取得、閲覧、またはスクレイピングができません。
- 出典の明記：回答には、使用した出典資料への参照が含まれます。

多層プロンプトセキュリティ

- レイヤー1：セキュリティ分類器（LLM-as-a-judge）は、悪意のあるクエリ（プロンプトインジェクション、権限昇格、データ漏洩、ソーシャルエンジニアリング、ポリシー違反）をブロックします。

  システムはブロックされたクエリをログに記録しますが、生成モデルはそれらを認識しません。

- レイヤー2：システムプロンプトの強化により、ユーザー入力がシステム命令を上書きすることを防止します。
- レイヤー 3：ドメインスコープにより、FSx ONTAP および Workload Factory のトピックへの応答が制限されます。
- レイヤー4：ツール使用ガバナンスはパラメータを検証し、強化されたサンドボックス内でクエリを実行します。モデルは任意の操作を実行できません。

モデルデータの分離とプライバシー

- 顧客データに基づくモデルトレーニングは行いません。

- リクエストレベルの分離（テナント間のデータ漏洩なし）
- セッションスコープの会話コンテキストと限定された履歴
- 永続的なモデルメモリはありません
- マネージド推論インフラストラクチャ

ツールの使用とエージェントのセキュリティ

- 認可スコープ付きツール（ユーザー権限の境界が適用される）
- 厳格なツール実行タイムアウト
- 取得したデータのための、一時的なセッションスコープのサンドボックス
- 許可リストによる読み取り専用クエリの強制
- 機密パラメータのスクラビングによるツール呼び出しの監査可能性

NetApp Workload Factory のアクセス制御について質問する

NetApp Workload Factory の Ask Me アクセスセキュリティは、認証済みセッション、ユーザーレベルの責任、および実行時操作中の保護された秘密情報の取り扱いに重点を置いています。認証制御は各セッションを検証し、操作を特定のユーザーに関連付けます。機密性の高い認証情報は、実行時に管理対象のシークレット保管庫から取得され、ログから削除されます。このサービスは、非ルートコンテナの実行や制限付き CORS 許可リストなど、インフラストラクチャ制御も適用します。

認証

- 暗号化検証（オーディエンス、発行者、RS256などのアルゴリズムチェックを含む）を備えた署名付きJWT認証
- サービス境界におけるミドルウェアによる認証
- ユーザーIDスコープにより、インタラクションを特定のユーザーに帰属させることができます

認証情報の保護と機密情報の取り扱い

- 安全な保管庫ストレージ：サービスで使用される機密性の高い認証情報は、管理されたシークレット保管庫に保存され、実行時に取得されます。アプリケーションコード、設定ファイル、またはコンテナイメージには、シークレットは一切保存されません。
- ログのスクラビング：機密情報（認証情報、トークン、パスワード、アクセスキー、証明書）は、ログに書き込まれる前に削除されます。

インフラストラクチャセキュリティ

- 非ルートコンテナの実行
- CORSは信頼できるNetAppドメインの明示的な許可リストに制限されています

Ask Me の実行モード（NetApp Workload Factory）

NetApp Workload Factoryは、Ask Meに対して複数の実行モードを提供しており、それぞれ異なるセキュリティおよびプライバシー特性を備えています。Ask Meがツール統合を使用する場合、例えばお客様自身のWorkload Factoryリソースにクエリを実行する場合、ツールの実行は多層的な安全対策によって制御されます。ツールによる実行は、認証されたユーザーの権限の範囲内で行われ、各操作の期間と範囲に制限が適用されます。取得されたデータは、外部からのアクセスを遮断する一時的なセッションサンドボックス内に保持され、セッションが終了すると破棄されます。独立したプロンプトとコード制御により読み取り専用のクエリが強制され、監査記録には機密値が削除されたツールアクティビティが記録されます。

ツール実行時の安全対策

- 認証済みユーザーの権限の範囲内で動作する、認可スコープ付きツールです。
- ツールの実行タイムアウトは、長時間実行される操作を制限します。
- 一時的なデータサンドボックスは、ツールによって取得されたデータをセッションスコープ内に保存し、エンジンレベルでの外部アクセス、ファイル I/O、ネットワーク呼び出し、および拡張機能の読み込みをブロックし、セッションが終了すると破棄されます。
- 読み取り専用クエリの強制適用は、厳格な許可リストを通じて生成されたクエリを検証します。
- プロンプトによるセキュリティとコードによるセキュリティは、それぞれ独立して適用されます。
- ツール呼び出しの監査可能性ログには、ツール名、パラメータ、タイムスタンプ、および結果ステータスが記録され、機密性の高い値はスクラビングされます。

出力制御

- トークン制限の適用
- 分類/セキュリティ上重要な操作のための決定論的出力（温度0）
- 早期終了とクリーンアップ機能を備えたストリーミング配信

NetApp Workload Factoryにおける「Ask Me」のプライバシーと可用性

NetApp Workload Factory の Ask Me プライバシー制御は、データ損失を制限し、セッション処理を分離して、ユーザーとのやり取りにおけるプライバシー境界を維持します。お客様の入力は、基盤モデルのトレーニングや改善には使用されない管理 AI サービスによって処理されます。取得された運用データは、セッション期間中、一時的なインメモリストレージに保持され、永続化または共有されることはありません。複数のクラウドリージョンにまたがるマルチモデルのフォールバックチェーンは、プライマリモデルが制限されたり利用できなくなったりした場合の可用性をサポートし、同じセキュリティ制御がフォールバックモデル全体に適用されます。

データ処理とプライバシー

- プロンプト内のユーザーデータ：管理されたAIサービスによって処理されますが、そのサービスはお客様の入力を基盤モデルのトレーニングや改善には使用しません。

- ナレッジベースコンテンツ：厳選・公開されたNetAppドキュメントのみ。お客様のデータは含まれません。
- 運用データ：ユーザーが自身のリソースを照会した場合にのみ取得され、セッション期間中は一時的なインメモリストレージに保持され、永続化または共有されることはありません。
- 監査ログ：クエリのメタデータ（匿名化されたユーザーID、タイムスタンプ、期間）がログに記録され、機密性の高いフィールドは削除されます。
- フィードバックデータ：匿名化されたユーザーID以外の個人を特定できる情報ではなく、クエリIDに紐づけられて別に保存されます。

可用性および隔離制御

Ask Meは、複数のクラウドリージョンにまたがるマルチモデルフォールバックチェーンを採用しています。

プライマリモデルがスロットリングされているか利用できない場合、システムは代替モデルにフェイルオーバーできます。

すべてのモデルは、同じセキュリティ管理、システムプロンプトの強化策、および隔離保証の対象となります。

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。