



NetApp Console アクセスロール

NetApp Console setup and administration

NetApp
January 13, 2026

目次

NetApp Consoleアクセスロール	1
NetApp Consoleのアクセスロールについて学ぶ	1
プラットフォームの役割	1
アプリケーションロール	2
データサービスの役割	2
関連リンク	3
NetApp Consoleプラットフォームアクセスロール	3
組織管理の役割	4
連盟の役割	5
パートナーシップの役割	5
スーパー管理者と閲覧者の役割	5
アプリケーションロール	6
NetApp ConsoleのGoogle Cloud NetApp Volumesロール	6
NetApp ConsoleのKeystoneアクセス ロール	7
NetApp Consoleの運用サポートアナリスト アクセス ロール	8
NetApp Consoleのストレージアクセスロール	8
データサービスの役割	11
NetApp ConsoleのNetApp Backup and Recoveryの役割	11
NetApp ConsoleのNetApp Disaster Recoveryロール	15
NetApp Consoleのランサムウェア耐性アクセス ロール	16

NetApp Console アクセスロール

NetApp Consoleのアクセスロールについて学ぶ

NetApp Consoleの ID およびアクセス管理 (IAM) では、リソース階層のさまざまなレベルにわたって組織のメンバーに割り当てることができる定義済みのロールが提供されます。これらのロールを割り当てる前に、各ロールに含まれる権限を理解しておく必要があります。ロールは、プラットフォーム、アプリケーション、データ サービスというカテゴリに分類されます。

プラットフォームの役割

プラットフォーム ロールは、ロールの割り当てやユーザー管理などのNetApp Console管理権限を付与します。コンソールにはいくつかのプラットフォーム ロールがあります。

プラットフォームの役割	責任
"組織管理者"	ユーザーは、組織内のすべてのプロジェクトとフォルダに無制限にアクセスでき、任意のプロジェクトまたはフォルダにメンバーを追加できるほか、任意のタスクを実行したり、明示的にロールが関連付けられていない任意のデータ サービスを使用したりできます。このロールを持つユーザーは、適切な資格情報を持っている場合、フォルダーとプロジェクトの作成、ロールの割り当て、ユーザーの追加、システムの管理を行うことで組織を管理します。これは、コンソール エージェントを作成できる唯一のアクセス ロールです。
"フォルダまたはプロジェクトの管理者"	割り当てられたプロジェクトとフォルダーへのユーザーの無制限アクセスを許可します。管理するフォルダーまたはプロジェクトにメンバーを追加できるほか、割り当てられたフォルダーまたはプロジェクト内のリソースに対して任意のタスクを実行したり、任意のデータ サービスやアプリケーションを使用したりすることもできます。フォルダーまたはプロジェクト管理者はコンソール エージェントを作成できません。
"連盟管理者"	ユーザーがコンソールを使用してフェデレーションを作成および管理し、シングル サインオン (SSO) を有効にすることを許可します。
"連盟ビューア"	ユーザーがコンソールを使用して既存のフェデレーションを表示できるようにします。フェデレーションを作成または管理できません。
"パートナーシップ管理者"	ユーザーがパートナーシップを作成および管理できるようにします。
"パートナーシップビューアー"	ユーザーが既存のパートナーシップを表示できるようにします。パートナーシップを作成または管理することはできません。
"スーパー管理者"	ユーザーに管理者ロールのサブセットを付与します。この役割は、コンソールの責任を複数のユーザーに分散する必要がない小規模な組織向けに設計されています。
"スーパービューアー"	ユーザーにサブセット閲覧者ロールを付与します。この役割は、コンソールの責任を複数のユーザーに分散する必要がない小規模な組織向けに設計されています。

アプリケーションロール

以下は、アプリケーション カテゴリ内のロールの一覧です。各ロールは、指定された範囲内で特定の権限を付与します。必要なアプリケーションまたはプラットフォームのロールを持たないユーザーは、それぞれのアプリケーションにアクセスできません。

アプリケーションロール	責任
"Google Cloud NetApp Volumes管理者"	Google Cloud NetApp Volumesロールを持つユーザーは、Google Cloud NetApp Volumes を検出して管理できます。
"Google Cloud NetApp Volumes閲覧者"	Google Cloud NetApp Volumesユーザーロールを持つユーザーは、Google Cloud NetApp Volumes を表示できます。
"Keystone管理者"	Keystone管理者ロールを持つユーザーは、サービス リクエストを作成できます。ユーザーがアクセスしているKeystoneテナント内の使用状況、リソース、および管理の詳細を監視および表示できるようにします。
"Keystoneビューア"	Keystoneビューア ロールを持つユーザーは、サービス リクエストを作成できません。ユーザーがアクセスしているKeystoneテナント内の消費量、資産、管理情報を監視および表示できるようにします。
ONTAPメディエーターのセットアップロール	ONTAP Mediator セットアップ ロールを持つサービス アカウントは、サービス リクエストを作成できます。このロールは、サービスアカウントでインスタンスを構成するために必要です。" ONTAPクラウドメディエーター "。
"オペレーションサポートアナリスト"	アラートおよび監視ツールへのアクセスと、サポートケースの入力および管理機能を提供します。
"Storage Admin"	ストレージの健全性とガバナンス機能を管理し、ストレージ リソースを検出し、既存のシステムを変更および削除します。
"ストレージビューア"	ストレージの健全性とガバナンス機能を表示し、以前に検出されたストレージ リソースも表示します。既存のストレージ システムを検出、変更、または削除することはできません。
"システムヘルススペシャリスト"	ストレージとヘルスおよびガバナンス機能を管理します。ストレージ管理者のすべての権限がありますが、既存のシステムを変更または削除することはできません。

データサービスの役割

以下は、データ サービス カテゴリのロールの一覧です。各ロールは、指定された範囲内で特定の権限を付与します。必要なデータ サービス ロールまたはプラットフォーム ロールを持たないユーザーは、データ サービスにアクセスできません。

データサービスの役割	責任
"バックアップとリカバリのスーパー管理者"	NetApp Backup and Recoveryで任意のアクションを実行します。
"バックアップとリカバリの管理者"	ローカル スナップショットへのバックアップ、セカンダリ ストレージへの複製、オブジェクト ストレージへのバックアップを実行します。
"バックアップとリカバリの復元管理者"	バックアップとリカバリでワークロードを復元します。

データサービスの役割	責任
"バックアップとリカバリのクローン管理者"	バックアップとリカバリでアプリケーションとデータを複製します。
"バックアップとリカバリビューア"	バックアップとリカバリの情報を表示します。
"災害復旧管理者"	NetApp Disaster Recoveryサービスで任意のアクションを実行します。
"災害復旧フェイルオーバー管理者"	フェイルオーバーと移行を実行します。
"災害復旧アプリケーション管理者"	レプリケーション プランを作成し、レプリケーション プランを変更し、テスト フェイルオーバーを開始します。
"災害復旧ビューア"	情報の表示のみ。
分類ビューア	ユーザーがNetApp Data Classificationスキャン結果を表示できるようにします。このロールを持つユーザーは、コンプライアンス情報を表示し、アクセス権限を持つリソースのレポートを生成できます。これらのユーザーは、ボリューム、バケット、またはデータベース スキーマのスキャンを有効または無効にすることはできません。分類には管理者の役割がありません。
"ランサムウェア耐性管理者"	NetApp Ransomware Resilienceの「保護」、「アラート」、「回復」、「設定」、「レポート」タブでアクションを管理します。
"ランサムウェア耐性ビューア"	ランサムウェア耐性で、ワークロード データを表示し、アラート データを表示し、回復データをダウンロードし、レポートをダウンロードします。
"ランサムウェア耐性ユーザー行動管理者"	Ransomware Resilience で、疑わしいユーザー行動の検出、アラート、監視を構成、管理、表示します。
"ランサムウェア耐性ユーザー行動ビューア"	ランサムウェア耐性で疑わしいユーザー行動のアラートと分析情報を表示します。
SnapCenter管理者	NetApp Backup and Recovery for Applications を使用してオンプレミスのONTAPクラスターからスナップショットをバックアップする機能を提供します。このロールを持つメンバーは、次のアクションを実行できます。* [バックアップとリカバリ]> [アプリケーション] から任意のアクションを実行する * 権限を持つプロジェクトおよびフォルダ内のすべてのシステムを管理する * すべてのNetApp Consoleサービスを使用するSnapCenterには、閲覧者ロールはありません。

関連リンク

- ["NetApp Consoleのアイデンティティとアクセス管理について学ぶ"](#)
- ["NetApp ConsoleIAMを使い始める"](#)
- ["NetApp Consoleのメンバーとその権限を管理する"](#)
- ["NetApp ConsoleIAMのAPIについて学ぶ"](#)

NetApp Consoleプラットフォームアクセスロール

ユーザーにプラットフォーム ロールを割り当てて、NetApp Consoleの管理、ロールの割り当て、ユーザーの追加、コンソール エージェントの作成、フェデレーションの管理

を行う権限を付与します。

大規模な多国籍組織の組織役割の例

XYZ 社は、北米、ヨーロッパ、アジア太平洋の地域別にデータ ストレージ アクセスを整理し、集中管理による地域制御を実現しています。

XYZ 社のコンソールの 組織管理者 は、初期組織と各リージョンの個別のフォルダーを作成します。各リージョンの*フォルダーまたはプロジェクト管理者*は、リージョンのフォルダー内のプロジェクト (および関連するリソース) を整理します。

フォルダーまたはプロジェクト管理者 の役割を持つ地域管理者は、リソースとユーザーを追加することでフォルダーを積極的に管理します。これらの地域管理者は、管理するフォルダやプロジェクトを追加、削除、または名前変更することもできます。組織管理者 は新しいリソースの権限を継承し、組織全体のストレージ使用状況の可視性を維持します。

同じ組織内で、1 人のユーザーに フェデレーション管理者 ロールが割り当てられ、組織の企業 IdP とのフェデレーションを管理します。このユーザーはフェデレーション組織を追加または削除できますが、組織内のユーザーまたはリソースを管理することはできません。組織管理者 は、フェデレーション ステータスを確認し、フェデレーション組織を表示するための フェデレーション ビューアー ロールをユーザーに割り当てます。

次の表は、各コンソール プラットフォーム ロールが実行できるアクションを示しています。

組織管理の役割

Task	組織管理者	フォルダまたはプロジェクトの管理者
エージェントを作成する	はい	いいえ
コンソールからシステムを作成、変更、または削除する (システムの追加または検出)	はい	はい
フォルダとプロジェクトの作成 (削除を含む)	はい	いいえ
既存のフォルダとプロジェクトの名前を変更する	はい	はい
役割を割り当ててユーザーを追加する	はい	はい
リソースをフォルダとプロジェクトに関連付ける	はい	はい
エージェントをフォルダとプロジェクトに関連付ける	はい	いいえ
フォルダとプロジェクトからエージェントを削除する	はい	いいえ
エージェントの管理 (証明書、設定などの編集)	はい	いいえ
管理 > 資格情報から資格情報を管理する	はい	はい
フェデレーションの作成、管理、表示	はい	いいえ
コンソールからサポートに登録し、ケースを送信します	はい	はい
明示的なアクセス ロールに関連付けられていないデータ サービスを使用する	はい	はい
監査ページと通知を表示する	はい	はい

連盟の役割

Task	連盟管理者	連盟ビューア
連盟を作成する	はい	いいえ
ドメインを確認する	はい	いいえ
フェデレーションにドメインを追加する	はい	いいえ
フェデレーションを無効化および削除する	はい	いいえ
テスト連盟	はい	いいえ
連盟とその詳細を表示する	はい	はい

パートナーシップの役割

Task	パートナーシップ管理者	パートナーシップビューアー
パートナーシップを構築できる	はい	いいえ
パートナーメンバーに役割を割り当てる	はい	いいえ
パートナーシップにメンバーを追加できます	はい	いいえ
組織のパートナーシップの詳細を表示できます	はい	はい

スーパー管理者と閲覧者の役割

スーパー管理者 ロールには、コンソールの機能、ストレージ、およびデータ サービスを管理するための完全なアクセス権が付与されます。この役割は、管理とガバナンスを監督する人に適しています。対照的に、スーパー ビューアー ロールは読み取り専用アクセスを提供するため、変更を加えずに可視性を必要とする監査人や関係者に最適です。

組織は、セキュリティ リスクを最小限に抑え、最小権限の原則に従うために、スーパー管理者 アクセスを控えるために使用する必要があります。ほとんどの組織では、リスクを軽減し、監査可能性を向上させるために、必要な権限のみを持つきめ細かいロールを割り当てる必要があります。

スーパーロールの例

ABC コーポレーションには、データ サービスとストレージ管理にNetApp Consoleを活用する 5 人の小規模なチームがあります。複数の役割を配分する代わりに、ユーザー管理やリソース構成などのすべての管理タスクを担当する 2 人の上級チーム メンバーにスーパー管理者 の役割を割り当てます。残りの 3 人のチーム メンバーにはスーパー ビューアー ロールが割り当てられており、設定を変更する権限なしで、ストレージの健全性とデータ サービスの状態を監視できます。

ロール	継承された役割
スーパー管理者	<ul style="list-style-type: none"> • 組織管理者 • フォルダまたはプロジェクトの管理者 • 連盟管理者 • パートナーシップ管理者 • ランサムウェア耐性管理者 • 災害復旧管理者 • バックアップスーパー管理者 • Storage Admin • Keystone管理者 • Google Cloud NetApp Volumes 管理者
スーパービューアー	<ul style="list-style-type: none"> • 組織閲覧者 • 連盟ビューア • パートナーシップビューアー • ランサムウェア耐性ビューア • 災害復旧ビューア • バックアップビューア • ストレージビューア • Keystoneビューア • Google Cloud NetApp Volumes 閲覧者

アプリケーションロール

NetApp ConsoleのGoogle Cloud NetApp Volumesロール

ユーザーに次のロールを割り当てて、NetApp ConsoleでGoogle Cloud NetApp Volumesにアクセスできるようにすることができます。

Google Cloud NetApp Volumes は次のロールを使用します。

- * Google Cloud NetApp Volumes管理者*: コンソールでGoogle Cloud NetApp Volumes を検出し、管理します。
- * Google Cloud NetApp Volumes閲覧者*: コンソールでGoogle Cloud NetApp Volumesを表示します。

NetApp ConsoleのKeystoneアクセス ロール

Keystoneロールは、Keystoneダッシュボードへのアクセスを提供し、ユーザーがKeystoneサブスクリプションを表示および管理できるようにします。Keystone の役割には、Keystone管理者とKeystoneビューアの 2 つがあります。2 つのロールの主な違いは、Keystoneで実行できるアクションです。Keystone管理者ロールは、サービス リクエストの作成やサブスクリプションの変更が許可される唯一のロールです。

NetApp ConsoleのKeystoneロールの例

XYZ 社には、Keystoneサブスクリプション情報を閲覧できる、さまざまな部門のストレージ エンジニアが 4 人います。これらのユーザー全員がKeystoneサブスクリプションを監視する必要がありますが、サービス リクエストを作成できるのはチーム リーダーのみです。チーム メンバーのうち 3 名に * Keystoneビューア* ロールが付与され、チーム リーダーには * Keystone管理者* ロールが付与されるため、会社のサービス リクエストを制御できるようになります。

次の表は、各Keystoneロールが実行できるアクションを示しています。

特徴とアクション	Keystone管理者	Keystoneビューア
次のタブを表示します: サブスクリプション、資産、モニター、管理	はい	はい
* Keystoneサブスクリプションページ*:		
サブスクリプションを表示	はい	はい
サブスクリプションの修正または更新	はい	いいえ
* Keystoneアセット ページ*:		
アセットを表示	はい	はい
資産管理	はい	いいえ
* Keystoneアラートページ*:		
アラートを表示	はい	はい
アラートを管理する	はい	いいえ
自分用のアラートを作成する	はい	はい
Licenses and subscriptions:		
ライセンスとサブスクリプションを表示できます	はい	はい
* Keystoneレポートページ*:		
レポートをダウンロード	はい	はい

特徴とアクション	Keystone管理者	Keystoneビューア
レポートを管理する	はい	はい
自分用のレポートを作成する	はい	はい
サービスリクエスト:		
サービスリクエストを作成する	はい	いいえ
組織内の任意のユーザーが作成したサービスリクエストを表示する	はい	はい

NetApp Consoleの運用サポートアナリスト アクセス ロール

ユーザーに運用サポートアナリストの役割を割り当てて、アラートと監視へのアクセスを許可することができます。この役割を持つユーザーはサポートケースを開くこともできます。

運用サポートアナリスト

Task	実行できる
設定 > 資格情報から自分のユーザー資格情報を管理します	はい
発見されたリソースを表示する	はい
コンソールからサポートに登録し、ケースを送信します	はい
監査ページと通知を表示する	はい
アラートの表示、ダウンロード、設定	はい

NetApp Consoleのストレージアクセスロール

ユーザーに次のロールを割り当てて、NetApp Consoleのストレージ管理機能へのアクセスを許可できます。ユーザーに、ストレージを管理するための管理者ロールまたは監視するための閲覧者ロールを割り当てることができます。



これらのロールは、NetApp Consoleパートナーシップ API から使用できません。

管理者は、次のストレージ リソースと機能についてユーザーにストレージ ロールを割り当てることができます。

ストレージ リソース:

- オンプレミスのONTAPクラスタ

- StorageGRID
- Eシリーズ

コンソールのサービスと機能:

- デジタルアドバイザー
- ソフトウェアアップデート
- ライフサイクルプランニング
- 持続可能性

NetApp Consoleのストレージロールの例

多国籍企業である XYZ 社には、大規模なストレージ エンジニアとストレージ管理者のチームが存在します。これにより、このチームは、ユーザー管理、エージェントの作成、ライセンス管理などのコアコンソールタスクへのアクセスを制限しながら、担当リージョンのストレージ資産を管理できるようになります。

12 人のチーム内で、2 人のユーザーに ストレージ閲覧者 ロールが付与され、割り当てられたコンソール プロジェクトに関連付けられたストレージ リソースを監視できるようになります。残りの 9 人には、ソフトウェア更新の管理、コンソール経由のONTAP System Manager へのアクセス、ストレージ リソースの検出 (システムの追加) などの機能を含む **Storage admin** ロールが付与されます。チームの 1 人に システム ヘルス スペシャリスト の役割が付与され、担当リージョン内のストレージ リソースのヘルスを管理できるようになります。システムを変更または削除することはできません。このユーザーは、割り当てられたプロジェクトのストレージ リソースに対してソフトウェア更新を実行することもできます。

組織には、ユーザー管理、エージェント作成、ライセンス管理など、コンソールのあらゆる側面を管理できる組織管理者 ロールを持つ 2 人の追加ユーザーと、割り当てられているフォルダーとプロジェクトのコンソール管理タスクを実行できる フォルダーまたはプロジェクト管理者 ロールを持つ複数のユーザーがいます。

次の表は、各ストレージ ロールが実行するアクションを示しています。

特徴とアクション	Storage Admin	システムヘルススペシャリスト	ストレージビューア
ストレージ管理:			
新しいリソースを発見する (システムを作成する)	はい	はい	いいえ
検出されたシステムを表示	はい	はい	いいえ
コンソールからシステムを削除する	はい	いいえ	いいえ
システムを変更する	はい	いいえ	いいえ
エージェントを作成する	いいえ	いいえ	いいえ
デジタルアドバイザー			
すべてのページと機能を表示	はい	はい	はい
Licenses and subscriptions			

特徴とアクション	Storage Admin	システムヘルススペシャリスト	ストレージビューア
すべてのページと機能を表示	いいえ	いいえ	いいえ
ソフトウェアアップデート			
ランディングページと推奨事項を表示	はい	はい	はい
潜在的なバージョンの推奨事項と主な利点を確認する	はい	はい	はい
クラスターの更新の詳細を表示する	はい	はい	はい
更新前のチェックを実行し、アップグレードプランをダウンロードする	はい	はい	はい
ソフトウェアアップデートをインストールする	はい	はい	いいえ
ライフサイクルプランニング			
キャパシティプランニングの状況を確認する	はい	はい	はい
次のアクションを選択する（ベストプラクティス、階層）	はい	いいえ	いいえ
コールドデータをクラウドストレージに階層化してストレージを解放する	はい	はい	いいえ
リマインダーを設定する	はい	はい	はい
持続可能性			
ダッシュボードと推奨事項を表示する	はい	はい	はい
レポートデータをダウンロード	はい	はい	はい
炭素削減率を編集	はい	はい	いいえ
修正の推奨事項	はい	はい	いいえ
推奨を延期する	はい	はい	いいえ
システム管理者アクセス			
資格情報を入力できます	はい	はい	いいえ
資格			
ユーザ クレデンシャル	はい	はい	いいえ

データサービスの役割

NetApp ConsoleのNetApp Backup and Recoveryの役割

コンソール内でNetApp Backup and Recoveryにアクセスできるように、ユーザーに次のロールを割り当てることができます。バックアップとリカバリのロールにより、組織内でユーザーが実行する必要があるタスクに固有のロールを柔軟に割り当てることができます。ロールの割り当て方法は、独自のビジネスおよびストレージ管理の実践によって異なります。

このサービスは、NetApp Backup and Recoveryに固有の次のロールを使用します。

- バックアップおよびリカバリ スーパー管理者: NetApp Backup and Recoveryであらゆるアクションを実行します。
- バックアップとリカバリ バックアップ管理者: NetApp Backup and Recoveryで、ローカル スナップショットへのバックアップ、セカンダリ ストレージへの複製、オブジェクト ストレージへのバックアップ アクションを実行します。
- バックアップおよびリカバリの復元管理者: NetApp Backup and Recoveryを使用してワークロードを復元します。
- バックアップおよびリカバリ クローン管理者: NetApp Backup and Recoveryを使用してアプリケーションとデータをクローンします。
- バックアップおよびリカバリ ビューア: NetApp Backup and Recoveryの情報を表示しますが、アクションは実行しません。

NetApp Consoleのアクセスロールの詳細については、["コンソールのセットアップと管理に関するドキュメント"](#)。

一般的なアクションに使用されるロール

次の表は、すべてのワークロードに対して各NetApp Backup and Recoveryロールが実行できるアクションを示しています。

特徴とアクション	バックアップとリカバリのスーパー管理者	バックアップとリカバリのバックアップ管理者	バックアップとリカバリの復元管理者	バックアップとリカバリのクローン管理者	バックアップとリカバリビューア
ホストを追加、編集、または削除する	はい	いいえ	いいえ	いいえ	いいえ
プラグインをインストールする	はい	いいえ	いいえ	いいえ	いいえ
資格情報を追加する (ホスト、インスタンス、vCenter)	はい	いいえ	いいえ	いいえ	いいえ
ダッシュボードとすべてのタブを表示	はい	はい	はい	はい	はい

特徴とアクション	バックアップとリカバリのスーパー管理者	バックアップとリカバリのバックアップ管理者	バックアップとリカバリの復元管理者	バックアップとリカバリのクローン管理者	バックアップとリカバリビューア
無料トライアルを始める	はい	いいえ	いいえ	いいえ	いいえ
ワークロードの検出を開始する	いいえ	はい	はい	はい	いいえ
ライセンス情報を表示	はい	はい	はい	はい	はい
ライセンスを有効化	はい	いいえ	いいえ	いいえ	いいえ
ホストを表示	はい	はい	はい	はい	はい
スケジュール:					
スケジュールをアクティブ化	はい	はい	はい	はい	いいえ
スケジュールを中断	はい	はい	はい	はい	いいえ
ポリシーと保護:					
保護プランを見る	はい	はい	はい	はい	はい
保護プランを作成、変更、または削除する	はい	はい	いいえ	いいえ	いいえ
ワークロードを復元する	はい	いいえ	はい	いいえ	いいえ
クローンを作成、分割、または削除する	はい	いいえ	いいえ	はい	いいえ
ポリシーの作成、変更、または削除	はい	はい	いいえ	いいえ	いいえ
レポート:					
レポートを表示	はい	はい	はい	はい	はい
レポートを作成する	はい	はい	はい	はい	いいえ
レポートを削除する	はい	いいえ	いいえ	いいえ	いいえ
* SnapCenterからインポートしてホストを管理する*:					
インポートされたSnapCenterデータを表示する	はい	はい	はい	はい	はい

特徴とアクション	バックアップとリカバリのスーパー管理者	バックアップとリカバリのバックアップ管理者	バックアップとリカバリの復元管理者	バックアップとリカバリのクローン管理者	バックアップとリカバリビューア
SnapCenterからデータをインポートする	はい	はい	いいえ	いいえ	いいえ
ホストの管理（移行）	はい	はい	いいえ	いいえ	いいえ
設定を構成する:					
ログ ディレクトリを設定	はい	はい	はい	いいえ	いいえ
インスタンス資格情報の関連付けまたは削除	はい	はい	はい	いいえ	いいえ
バケツ:					
バケツを表示	はい	はい	はい	はい	はい
バケツを作成、編集、または削除する	はい	はい	いいえ	いいえ	いいえ

ワークロード固有のアクションに使用されるロール

次の表は、各NetApp Backup and Recoveryロールが特定のワークロードに対して実行できるアクションを示しています。

Kubernetes ワークロード

この表は、Kubernetes ワークロードに固有のアクションに対して各NetApp Backup and Recoveryロールが実行できるアクションを示しています。

特徴とアクション	バックアップとリカバリのスーパー管理者	バックアップとリカバリのバックアップ管理者	バックアップとリカバリの復元管理者	バックアップとリカバリビューア
クラスター、名前空間、ストレージ クラス、API リソースを表示する	はい	はい	はい	はい
新しいKubernetesクラスターを追加する	はい	はい	いいえ	いいえ
クラスタ構成を更新する	はい	いいえ	いいえ	いいえ
管理からクラスタを削除する	はい	いいえ	いいえ	いいえ
アプリケーションを表示する	はい	はい	はい	はい

特徴とアクション	バックアップとリカバリのスーパー管理者	バックアップとリカバリのバックアップ管理者	バックアップとリカバリの復元管理者	バックアップとリカバリビューア
新しいアプリケーションの作成と定義	はい	はい	いいえ	いいえ
アプリケーション構成を更新する	はい	はい	いいえ	いいえ
管理からアプリケーションを削除する	はい	はい	いいえ	いいえ
保護されたリソースとバックアップステータスを表示する	はい	はい	はい	はい
バックアップを作成し、ポリシーでアプリケーションを保護する	はい	はい	いいえ	いいえ
アプリの保護を解除し、バックアップを削除する	はい	はい	いいえ	いいえ
リカバリポイントとリソースビューアの結果を表示する	はい	はい	はい	はい
リカバリポイントからアプリケーションを復元する	はい	いいえ	はい	いいえ
Kubernetes バックアップ ポリシーを表示する	はい	はい	はい	はい
Kubernetes バックアップ ポリシーを作成する	はい	はい	はい	いいえ
バックアップポリシーを更新する	はい	はい	はい	いいえ
バックアップポリシーを削除する	はい	はい	はい	いいえ
実行フックとフックソースを表示する	はい	はい	はい	はい
実行フックとフックソースを作成する	はい	はい	はい	いいえ
実行フックとフックソースを更新する	はい	はい	はい	いいえ
実行フックとフックソースを削除する	はい	はい	はい	いいえ
実行フックテンプレートを表示する	はい	はい	はい	はい
実行フックテンプレートを作成する	はい	はい	はい	いいえ

特徴とアクション	バックアップとリカバリのスーパー管理者	バックアップとリカバリのバックアップ管理者	バックアップとリカバリの復元管理者	バックアップとリカバリビューアー
実行フックテンプレートを更新する	はい	はい	はい	いいえ
実行フックテンプレートを削除する	はい	はい	はい	いいえ
ワークロードの概要と分析ダッシュボードを表示する	はい	はい	はい	はい
StorageGRIDバケットとストレージターゲットを表示する	はい	はい	はい	はい

NetApp ConsoleのNetApp Disaster Recoveryロール

コンソール内でNetApp Disaster Recoveryにアクセスできるように、ユーザーに次のロールを割り当てることができます。災害復旧ロールを使用すると、組織内でユーザーが実行する必要があるタスクに固有のロールを柔軟に割り当てることができます。ロールの割り当て方法は、独自のビジネスおよびストレージ管理の実践によって異なります。

災害復旧では次のロールが使用されます。

- 災害復旧管理者: あらゆるアクションを実行します。
- 災害復旧フェールオーバー管理者: フェールオーバーと移行を実行します。
- 災害復旧アプリケーション管理者: レプリケーション プランを作成します。レプリケーション プランを変更します。テストフェールオーバーを開始します。
- 災害復旧ビューアー: 情報の表示のみ。

次の表は、各ロールが実行できるアクションを示しています。

特徴とアクション	災害復旧管理者	災害復旧フェールオーバー管理者	災害復旧アプリケーション管理者	災害復旧ビューアー
ダッシュボードとすべてのタブを表示	はい	はい	はい	はい
無料トライアルを始める	はい	いいえ	いいえ	いいえ
ワークロードの検出を開始する	はい	いいえ	いいえ	いいえ
ライセンス情報を表示	はい	はい	はい	はい
ライセンスを有効化	はい	いいえ	はい	いいえ
サイトタブ:				

特徴とアクション	災害復旧管理者	災害復旧フェイルオーバー管理者	災害復旧アプリケーション管理者	災害復旧ビューアー
サイトを表示	はい	はい	はい	はい
サイトの追加、変更、削除	はい	いいえ	いいえ	いいえ
レプリケーション プラン タブで:				
レプリケーションプランの表示	はい	はい	はい	はい
レプリケーションプランの詳細を表示する	はい	はい	はい	はい
レプリケーションプランを作成または変更する	はい	はい	はい	いいえ
レポートを作成する	はい	いいえ	いいえ	いいえ
スナップショットを表示	はい	はい	はい	はい
フェイルオーバーテストを実行する	はい	はい	はい	いいえ
フェイルオーバーを実行する	はい	はい	いいえ	いいえ
フェイルバックを実行する	はい	はい	いいえ	いいえ
移行を実行する	はい	はい	いいえ	いいえ
リソース グループ タブで:				
リソース グループを表示する	はい	はい	はい	はい
リソース グループの作成、変更、または削除	はい	いいえ	はい	いいえ
ジョブ監視タブで:				
ジョブの表示	はい	いいえ	はい	はい
ジョブをキャンセルする	はい	はい	はい	いいえ

NetApp Consoleのランサムウェア耐性アクセス ロール

ランサムウェア レジリエンス ロールは、ユーザーにNetApp Ransomware Resilienceへのアクセスを提供します。ランサムウェア耐性は次の役割をサポートします。

ベースラインロール

- ・ランサムウェア耐性管理者 - ランサムウェア耐性設定を構成し、暗号化アラートを調査して対応します
- ・ランサムウェア耐性ビューア - 暗号化インシデント、レポート、検出設定を表示

ユーザー行動アクティビティの役割"不審なユーザーアクティビティの検出"アラートは、ファイル アクティビティ イベントなどのデータの可視性を提供します。これらのアラートには、ファイル名と、ユーザーが実行したファイル アクション (読み取り、書き込み、削除、名前の変更など) が含まれます。このデータの可視性を制限するために、これらのロールを持つユーザーのみがこれらのアラートを管理または表示できます。

- ・ランサムウェア耐性ユーザー行動管理者 - 疑わしいユーザーアクティビティの検出を有効にし、疑わしいユーザーアクティビティのアラートを調査して対応します
- ・ランサムウェア耐性ユーザー行動ビューア - 疑わしいユーザーアクティビティアラートを表示



ユーザー ビヘイビア ロールはスタンドアロン ロールではなく、ランサムウェア レジリエンス 管理者ロールまたは閲覧者ロールに追加されるように設計されています。詳細については、[\[ユーザーの行動の役割\]](#)。

各ロールの詳細な説明については、次の表を参照してください。

ベースラインロール

次の表は、ランサムウェア耐性管理者および閲覧者ロールで使えるアクションを示しています。

特徴とアクション	ランサムウェア耐性管理者	ランサムウェア耐性ビューア
ダッシュボードとすべてのタブを表示	はい	はい
ダッシュボードで推奨事項のステータスを更新する	はい	いいえ
無料トライアルを始める	はい	いいえ
ワークロードの検出を開始する	はい	いいえ
ワークロードの再検出を開始する	はい	いいえ
[保護]タブで:		
暗号化ポリシーの保護プランを追加、変更、または削除する	はい	いいえ
ワークロードを保護する	はい	いいえ
データ分類で機密データへの露出を特定	はい	いいえ
保護プランと詳細を一覧表示する	はい	はい
保護グループの一覧	はい	はい

特徴とアクション	ランサムウェア耐性管理者	ランサムウェア耐性ビューア
保護グループの詳細を表示する	はい	はい
保護グループの作成、編集、または削除	はい	いいえ
データをダウンロード	はい	はい
アラートタブ:		
暗号化アラートとアラートの詳細を表示する	はい	はい
暗号化インシデントステータスの編集	はい	いいえ
回復のために暗号化アラートをマークする	はい	いいえ
暗号化インシデントの詳細を表示	はい	はい
暗号化インシデントを無視または解決する	はい	いいえ
暗号化イベントで影響を受けるファイルの完全なリストを取得します	はい	いいえ
暗号化イベントアラートデータをダウンロードする	はい	はい
ユーザーをブロックする (Workload Securityエージェント構成を使用)	はい	いいえ
【回復】タブで:		
暗号化イベントから影響を受けるファイルをダウンロードする	はい	いいえ
暗号化イベントからのワークロードの復元	はい	いいえ
暗号化イベントから回復データをダウンロードする	はい	はい
暗号化イベントからのレポートをダウンロード	はい	はい
設定タブで:		
バックアップ先を追加または変更する	はい	いいえ
バックアップ先の一覧	はい	はい
接続されたSIEMターゲットを表示する	はい	はい

特徴とアクション	ランサムウェア耐性管理者	ランサムウェア耐性ビューア
SIEMターゲットの追加または変更	はい	いいえ
準備訓練を構成する	はい	いいえ
準備訓練を開始、リセット、または編集する	はい	いいえ
準備訓練の状況を確認する	はい	はい
検出構成の更新	はい	いいえ
検出構成の表示	はい	はい
レポートタブ:		
レポートをダウンロード	はい	はい

ユーザーの行動の役割

疑わしいユーザーの行動設定を構成し、アラートに応答するには、ユーザーは Ransomware Resilience ユーザー行動管理者ロールを持っている必要があります。疑わしいユーザー行動アラートのみを表示するには、ユーザーは Ransomware Resilience ユーザー行動閲覧者ロールを持っている必要があります。

ランサムウェア耐性の管理者または閲覧者権限を持つユーザーで、アクセスが必要なユーザーには、ユーザー行動ロールを付与する必要があります。["不審なユーザーアクティビティの設定とアラート"](#)。たとえば、ランサムウェア耐性管理者ロールを持つユーザーには、ユーザー アクティビティ エージェントを構成し、ユーザーをブロックまたはブロック解除するための、ランサムウェア耐性ユーザー動作管理者ロールが付与される必要があります。ランサムウェア耐性ユーザー動作管理者ロールは、ランサムウェア耐性ビューアに付与しないでください。



不審なユーザー アクティビティの検出を有効にするには、コンソール組織管理者のロールが必要です。

次の表は、ランサムウェア耐性ユーザー動作の管理者および閲覧者ロールで可以使用アクションを示しています。

特徴とアクション	ランサムウェア耐性ユーザー行動管理者	ランサムウェア耐性ユーザー行動ビューア
設定タブで:		
ユーザーアクティビティエージェントの作成、変更、または削除	はい	いいえ
ユーザーディレクトリコネクタの作成または削除	はい	いいえ
データコレクターを一時停止または再開する	はい	いいえ

特徴とアクション	ランサムウェア耐性ユーザー行動管理者	ランサムウェア耐性ユーザー行動ビューア
データ侵害対策訓練を実施する	はい	いいえ
【保護】タブで:		
「疑わしいユーザー行動」ポリシーの保護プランを追加、変更、または削除する	はい	いいえ
アラートタブ:		
ユーザーアクティビティアラートとアラートの詳細を表示する	はい	はい
ユーザーアクティビティインシデントステータスの編集	はい	いいえ
回復のためにユーザーアクティビティアラートをマークする	はい	いいえ
ユーザーアクティビティインシデントの詳細を表示する	はい	はい
ユーザーアクティビティインシデントを無視または解決する	はい	いいえ
疑わしいユーザーによる影響を受けたファイルの完全なリストを取得する	はい	はい
ユーザーアクティビティイベントアラートデータをダウンロードする	はい	はい
ユーザーをブロックまたはブロック解除する	はい	いいえ
【回復】タブで:		
ユーザーアクティビティイベントの影響を受けるファイルをダウンロードする	はい	いいえ
ユーザーアクティビティイベントからワークロードを復元する	はい	いいえ
ユーザーアクティビティイベントから回復データをダウンロードする	はい	はい
ユーザーアクティビティイベントからレポートをダウンロードする	はい	はい

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。