



ロールベースアクセス制御

ONTAP tools for VMware vSphere 9.12

NetApp
December 19, 2023

目次

ロールベースアクセス制御	1
ONTAP ツールでのロールベースアクセス制御の概要	1
vCenter Server アクセス許可の要素	1
vCenter Server のアクセス許可の割り当てと変更に関する要点	3
ONTAP ツールに付属の標準ロール	4
ONTAP toolsのタスクに必要な権限	6
ONTAP ストレージシステムおよび vSphere オブジェクトの権限	6
VMware vSphere 用の ONTAP ツール用に ONTAP の RBAC を設定する方法	8

ロールベースアクセス制御

ONTAP ツールでのロールベースアクセス制御の概要

vCenter Server の RBAC を使用すると、vSphere オブジェクトへのアクセスを制御できます。ONTAP@tools for VMware vSphereでは、vCenter Server RBACとONTAP RBACにより、特定のストレージシステムのオブジェクトに対して特定のユーザが実行できるONTAP toolsタスクが決まります。

タスクを完了するには、適切な vCenter Server RBAC アクセス許可が必要です。タスクの実行中、ONTAP toolsはユーザのvCenter Serverアクセス許可を確認してから、ユーザのONTAP権限を確認します。

vCenter Server アクセス許可をルートオブジェクト（ルートフォルダ）に対して設定することができます。その後、アクセス許可が不要な子エンティティのアクセスを禁止することでセキュリティを強化できます。

vCenter Server アクセス許可の要素

vCenter Server で認識されるのはアクセス許可で、権限ではありません。vCenter Server アクセス許可は 3 つの要素で構成されます。

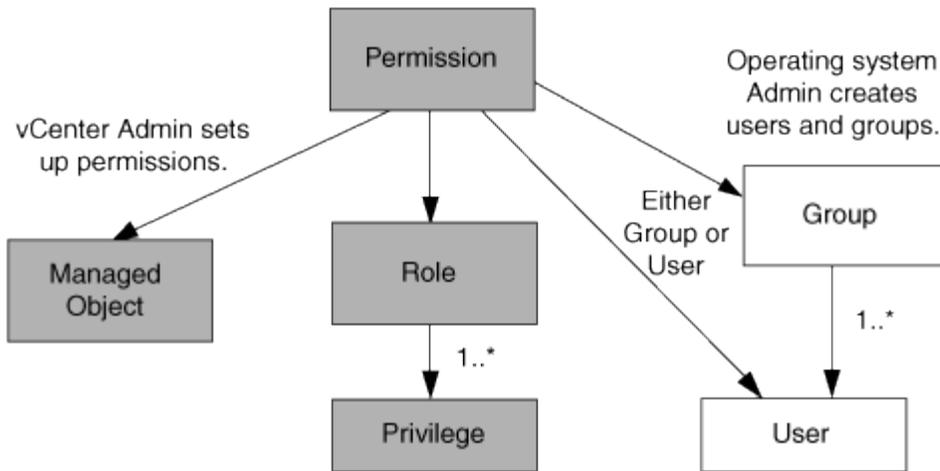
vCenter Server には次のコンポーネントがあります。

- 1 つ以上の権限（ロール）
ユーザが実行できるタスクを定義します。
- vSphere オブジェクト
タスクの対象となるオブジェクトです。
- ユーザまたはグループ
タスクを実行できるユーザまたはグループを定義します。

次の図に示すように、3 つの要素がすべて揃っていないとアクセスは許可されません。



グレーのボックスは vCenter Server 側の要素、白のボックスは vCenter Server を実行しているオペレーティングシステム側の要素を表しています。



権限

VMware vSphere 用の ONTAP ツールには、次の 2 種類の権限が関連付けられています。

- vCenter Server 標準の権限

vCenter Server に付属している権限です。

- ONTAP tools固有の権限

これらの権限は、ONTAP toolsの特定のタスク用に定義されています。ONTAPツールに固有の機能です。

ONTAP toolsのタスクには、ONTAP tools固有の権限とvCenter Server標準の権限の両方が必要です。これらの権限は、ユーザーのロールを構成しますアクセス許可には複数の権限を含めることができます。これらの権限は、vCenter Server にログインしているユーザを対象としています。



vCenter Server RBACの使用を簡易化するために、ONTAP toolsには、ONTAP toolsのタスクの実行に必要なONTAP tools固有の権限と標準の権限をすべて含む標準ロールがいくつか用意されています。

アクセス許可に含まれる権限が変更された場合、そのアクセス許可が関連付けられたユーザは、更新されたアクセス許可を有効にするためにログアウトしてログインし直す必要があります。

* 権限 *	* 役割 *	* タスク *
NetApp ONTAP Tools Console > View の順にクリックします	<ul style="list-style-type: none"> • VSC管理者 • VSC によるプロビジョニング • VSC 読み取り専用 	ONTAPツールおよびVASA Provider固有のタスクには、いずれも表示権限が必要です。

NetApp Virtual Storage Console > Policy Based Management > Management または privilege.nvpfVSC.VASAGroup.co m.netapp.nvpf.label > Management の順にクリックします	VSC管理者	ストレージ機能プロファイルおよ びしきい値設定に関連する VSC お よび VASA Provider のタスク。
---	--------	---

vSphere オブジェクト

アクセス許可は vSphere オブジェクトに関連付けられます。vCenter Server、ESXi ホスト、仮想マシン、データストア、データセンター、とフォルダ。任意の vSphere オブジェクトに権限を割り当てることができます。vSphere オブジェクトに割り当てられたアクセス許可に基づいて、そのオブジェクトに対してどのユーザがどのタスクを実行できるかが決まります。ONTAP tools固有のタスクの場合、アクセス許可の割り当てと検証はルートフォルダレベル (vCenter Server) でのみ行われ、他のエンティティでは行われません。ただし VAAI プラグインの処理は例外で、関連する ESXi に対して権限が検証されます。

ユーザとグループ

ユーザとグループは、Active Directory (またはローカルの vCenter Server マシン) を使用して設定できます。その後、vCenter Serverアクセス許可を使用してこれらのユーザまたはグループにアクセスを許可し、特定のONTAP toolsタスクを実行できるようにすることができます。



これらのvCenter Serverアクセス許可は、ONTAP tools管理者ではなく、ONTAP tools vCenter ユーザに適用されます。デフォルトでは、ONTAP tools管理者は製品へのフルアクセス権を持ち、権限を割り当てる必要はありません。

ユーザとグループにはロールは割り当てられません。vCenter Server アクセス許可を割り当てることで、間接的にロールが適用されます。

vCenter Server のアクセス許可の割り当てと変更に関する要点

vCenter Server のアクセス許可を使用する際にはいくつかの点に注意する必要があります。VMware vSphere タスク用の ONTAP ツールを使用できるかどうかは、アクセス許可を割り当てた場所、およびアクセス許可の変更後にユーザが実行した操作によって決まります。

権限を割り当てます

vCenter Server のアクセス許可は、vSphere のオブジェクトおよびタスクへのアクセスを制限したい場合のみ設定します。それ以外の場合は、管理者としてログインできます。このログインでは、すべての vSphere オブジェクトに自動的にアクセスできます。

アクセス許可を割り当てる場所によって、ユーザが実行できるONTAP toolsタスクが決まります。

タスクによっては、完了を確認するために、ルートオブジェクトなどの上位レベルにアクセス許可を割り当てる必要があります。具体的には、特定の vSphere オブジェクトには適用されない権限 (タスクの追跡など) がタスクに必要な場合や、必要な権限環境が vSphere 以外のオブジェクト (ストレージシステムなど) に必要な場合です。

このような場合は、子エンティティに継承されるようにアクセス許可を設定できます。子エンティティには、他の権限も割り当てることができます。子エンティティに割り当てたアクセス許可は、親エンティティから継承されたアクセス許可を上書きします。したがって、子エンティティにアクセス許可を割り当てることで、ルートオブジェクトに割り当てられ、子エンティティに継承されたアクセス許可の対象を制限することができます。



会社のセキュリティポリシーでアクセス許可を厳しく制限することが求められる場合を除き、ルートオブジェクト（ルートフォルダとも呼ばれる）にアクセス許可を割り当てることを推奨します。

アクセス許可と非 vSphere オブジェクト

作成したアクセス許可は、vSphere 以外のオブジェクトに適用されます。たとえば、ストレージシステムは vSphere オブジェクトではありません。ストレージシステムの権限環境の場合は、その権限を含むアクセス許可を ONTAP tools のルートオブジェクトに割り当てる必要があります。これは、ストレージシステムを割り当てることができる vSphere オブジェクトがないためです。

たとえば、ONTAP tools の「Add/Modify/Skip storage systems」などの権限を含むすべての権限は、ルートオブジェクトレベルに割り当てる必要があります。

アクセス許可の変更

一度に変更できるアクセス許可は 1 つです。

アクセス許可に含まれる権限が変更された場合、そのアクセス許可が関連付けられたユーザは、更新されたアクセス許可を有効にするためにログアウトしてログインし直す必要があります。

ONTAP ツールに付属の標準ロール

vCenter Server の権限と Role-Based Access Control (RBAC ; ロールベースアクセス制御) を簡単に使用できるように、ONTAP tools には、主要な ONTAP ツールタスクを実行できる標準の ONTAP tools ロールが用意されています。タスクを実行せずに情報を表示できる読み取り専用ロールもあります。

標準の ONTAP tools ロールには、ユーザが ONTAP tools タスクを実行するために必要な ONTAP tools 固有の権限と vCenter Server 標準の権限の両方が含まれています。また、サポートされるどのバージョンの vCenter Server でも必要な権限が付与されるように設定されています。

管理者は、必要に応じてこれらのロールをユーザに割り当てることができます。



ONTAP tools を最新バージョンにアップグレードすると、新しいバージョンのツールで使用できるように標準ロールが自動的にアップグレードされます。

ONTAP tools の標準ロールを表示するには、vSphere Client の [ホーム] ページで *[ロール]* をクリックします。

ONTAP tools のロールで実行できるタスクは次のとおりです。

* 役割 *	* 概要 *
--------	--------

VSC管理者	すべてのONTAP toolsタスクを実行するために必要なvCenter Server標準の権限とONTAP tools固有の権限がすべて含まれています。
VSC 読み取り専用	ONTAP toolsへの読み取り専用アクセスを許可します。これらのユーザは、アクセス制御されたONTAP toolsアクションを実行できません。
VSC によるプロビジョニング	ストレージのプロビジョニングに必要なvCenter Server標準の権限とONTAP tools固有の権限がすべて含まれています。次のタスクを実行できます。 <ul style="list-style-type: none"> • 新しいデータストアを作成する • データストアを削除 • ストレージ機能プロファイルに関する情報を表示する

ONTAP toolsの標準ロールの使用に関するガイドライン

VMware vSphere の標準的な ONTAP ツールを使用する場合は、一定のガイドラインに従う必要があります。

標準ロールは直接変更しないでください。このオプションを選択すると、アップグレードするたびにONTAP toolsによって変更が上書きされます。ONTAP toolsをアップグレードするたびに、インストーラによって標準ロール定義が更新されます。これにより、使用しているバージョンのONTAP toolsだけでなく、サポートされるすべてのバージョンのvCenter Serverでロールが最新の状態に維持されます。

ただし、標準のロールを使用して環境に合わせたロールを作成することもできます。これを行うには、ONTAP toolsの標準ロールをコピーしてから、コピーしたロールを編集する必要があります。新しいロールを作成すると、ONTAP tools Windowsサービスを再起動またはアップグレードしても、このロールを維持できます。

ONTAP toolsの標準ロールを使用する方法には、次のようなものがあります。

- ONTAP toolsのすべてのタスクには、標準のONTAP toolsロールを使用します。

このシナリオでは、標準ロールには、ONTAP toolsタスクを実行するために必要なすべての権限が含まれています。

- 複数のロールを組み合わせることでユーザが実行できるタスクを拡張する。

ONTAP toolsの標準ロールの方が細かすぎる場合は、複数のロールを含む上位レベルのグループを作成してロールを拡張できます。

ユーザがvCenter Server標準の追加権限を必要とするONTAP tools以外のタスクを実行する必要がある場合は、それらの権限を提供するロールを作成してグループに追加できます。

- より細分化されたロールを作成します。

標準のONTAP toolsロールよりも制限の厳しいロールを実装する必要がある場合は、ONTAP toolsロールを使用して新しいロールを作成できます。

この場合は、必要なONTAP toolsロールのクローンを作成し、そのクローンロールを編集してユーザーに必要な権限のみを付与します。

ONTAP toolsのタスクに必要な権限

ONTAP Tools for VMware vSphereのタスクごとに、ONTAP Tools固有の権限とvCenter Server標準の権限の組み合わせが異なります。

ONTAP toolsのタスクに必要な権限については、NetAppの技術情報アーティクル1032542を参照してください。

["Virtual Storage Console 用の RBAC の設定方法"](#)

VMware vSphere 用の ONTAP ツールで必要な製品レベルの権限

ONTAP tools for VMware vSphere GUIにアクセスするには、製品レベルのONTAP tools固有のView権限が、適切なvSphereオブジェクトレベルで割り当てられている必要があります。この権限なしでログインすると、NetAppアイコンをクリックしたときにONTAP toolsにエラーメッセージが表示され、ONTAP toolsにアクセスできなくなります。

View *権限では、ONTAPツールGUIにアクセスできます。ONTAP tools内でタスクを実行することはできません。ONTAP toolsのタスクを実行するには、タスクに対して適切なONTAP tools固有の権限とvCenter Server標準の権限が必要です。

割り当てレベルによって、表示できる UI の部分が決まります。ルートオブジェクト（フォルダ）でView権限を割り当てると、NetAppアイコンをクリックしてONTAP toolsにアクセスできるようになります。

別のvSphereオブジェクトレベルにView権限を割り当てることもできますが、その場合は表示および使用できるONTAP toolsメニューが制限されます。

View 権限を含むアクセス許可は、ルートオブジェクトに割り当ててることを推奨します。

ONTAP ストレージシステムおよび vSphere オブジェクトの権限

ONTAP の RBAC を使用すると、特定のストレージシステムへのアクセスとそれらのストレージシステムで実行できる操作を制御できます。ONTAP®tools for VMware vSphere では、ONTAP RBACとvCenter Server RBACにより、特定のストレージシステムのオブジェクトに対して特定のユーザーが実行できるONTAP toolsタスクが決まります。

ONTAP toolsでは、ONTAP toolsで設定したクレデンシャル（ユーザー名とパスワード）を使用して各ストレージシステムを認証し、そのストレージシステムで実行できるストレージ操作を判別します。ONTAP toolsでは、ストレージシステムごとに1組のクレデンシャルが使用されます。このクレデンシャルによって、そのストレージシステムで実行できるONTAP toolsタスクが決まります。つまり、このクレデンシャルはONTAP toolsのクレデンシャルであり、個々のONTAP toolsユーザーのクレデンシャルではありません。

ONTAP RBACは、ストレージシステムへのアクセスとストレージ関連のONTAP toolsタスク（仮想マシンのプロビジョニングなど）の実行にのみ適用されます。それぞれのストレージシステムに対する適切な ONTAP RBAC 権限がないと、そのストレージシステムでホストされる vSphere オブジェクトに対してタスクを実行

することはできません。ONTAP RBACとONTAP tools固有の権限を組み合わせると、ユーザが実行できるONTAP toolsタスクを制御できます。

- ストレージまたはストレージシステムに格納されている vCenter Server オブジェクトの監視と設定
- ストレージシステムに格納されている vSphere オブジェクトのプロビジョニング

ONTAP RBACとONTAP tools固有の権限を使用すると、ストレージ主体のセキュリティレイヤをストレージ管理者が管理できるようになります。これにより、ONTAP RBAC または vCenter Server RBAC のどちらか一方のアクセス制御だけを使用した場合に比べ、よりきめ細かい制御が可能になります。たとえば、vCenter Server RBAC を使用して、ネットアップストレージでのデータストアのプロビジョニングを vCenterUserB には許可し、vCenterUserA には許可しないように設定したとします。この場合、特定のストレージシステムのクレデンシャルに対してストレージの作成を禁止すれば、vCenterUserB と vCenterUserA のどちらもそのストレージシステムでデータストアのプロビジョニングを実行することはできません。

ONTAP toolsタスクを開始すると、最初にそのタスクに対する正しいvCenter Serverアクセス許可があるかどうかONTAP toolsによって検証されます。タスクを実行するための十分なvCenter Serverアクセス許可がない場合、最初のvCenter Serverセキュリティチェックをパスしなかったため、ONTAP toolsでそのストレージシステムのONTAP権限を確認する必要はありません。そのため、ストレージシステムにアクセスできません。

十分なvCenter Serverアクセス許可がある場合、ONTAP toolsは次に、ストレージシステムのクレデンシャル（ユーザ名とパスワード）に関連付けられているONTAP RBAC権限（ONTAPロール）を確認します。ONTAP toolsタスクに必要なストレージ操作をそのストレージシステムで実行するための十分な権限があるかどうかを確認する。適切なONTAP権限があれば、ストレージシステムにアクセスしてONTAP toolsのタスクを実行できます。ストレージシステムで実行できるONTAP toolsタスクは、ONTAPロールによって決まります。

各ストレージシステムには、一連の ONTAP 権限が関連付けられます。

ONTAP RBAC と vCenter Server RBAC の両方を使用すると、次のような利点があります。

- セキュリティ

どのユーザがどのタスクを実行できるかを、vCenter Server オブジェクトレベルおよびストレージシステムレベルで制御できます。

- 監査情報

多くの場合、ONTAPツールはストレージシステムに関する監査証跡を提供します。これにより、ストレージに対して変更を行ったvCenter Serverユーザまでさかのぼってイベントを追跡できます。

- 使いやすさ

コントローラのクレデンシャルをすべて集約して一元管理できます。

VMware vSphere 用の ONTAP ツールを使用する際に推奨される ONTAP ロール

VMware vSphere および Role-Based Access Control (RBAC ; ロールベースアクセス制御) 用の ONTAP ® ツールを使用する際に推奨される ONTAP ロールをいくつか設定できます。これらのロールには、ONTAP toolsタスクで実行するストレージ処理に必要なONTAP権限が含まれています。

新しいユーザロールを作成するには、ONTAP を実行しているストレージシステムに管理者としてログインす

する必要があります。ONTAP System Manager 9.8P1以降を使用してONTAP ロールを作成できます。を参照してください ["ユーザーロールと権限を設定"](#) を参照してください。

各 ONTAP ロールには、ロールのクレデンシャルを構成するユーザ名とパスワードのペアが関連付けられています。このクレデンシャルを使用してログインしないと、ロールに関連付けられたストレージ処理にアクセスできません。

セキュリティ対策として、ONTAP tools固有のONTAPロールは階層構造になっています。最初のロールは最も制限のあるロールで、ONTAP toolsの最も基本的なストレージ処理に関連する権限だけが含まれます。次のロールには、そのロール独自の権限と、前のロールに関連付けられているすべての権限が含まれます。以降、上位のロールほど制限が少なく、より多くのストレージ処理をサポートします。

ONTAP toolsを使用する際に推奨されるONTAP RBACロールの一部を次に示します。ロールを作成したら、仮想マシンのプロビジョニングなど、ストレージに関するタスクを実行する必要があるユーザにそのロールを割り当てることができます。

1. 検出

ストレージシステムを追加できます。

2. ストレージを作成します

ストレージを作成できます。また、Discovery ロールに関連付けられているすべての権限が含まれます。

3. ストレージを変更します

ストレージを変更できます。また、Discovery ロールと Create Storage ロールに関連付けられているすべての権限が含まれます。

4. ストレージを破棄します

ストレージを破棄できます。また、Discovery ロール、Create Storage ロール、Modify Storage ロールに関連付けられているすべての権限が含まれます。

VASA Provider for ONTAP を使用する場合は、Policy-Based Management (PBM ; ポリシーベース管理) ロールも設定します。ストレージポリシーを使用してストレージを管理できます。このロールを使用するには、「検出」ロールも設定する必要があります。

VMware vSphere 用の ONTAP ツール用に ONTAP の RBAC を設定する方法

VMware vSphere 用の ONTAP ツールでロールベースアクセス制御を使用する場合は、ストレージシステムで ONTAP RBAC を設定する必要があります。ONTAP RBAC 機能を使用すると、アクセス権限を制限したカスタムユーザアカウントを 1 つ以上作成できます。

ONTAP toolsとSRAは、クラスタレベルまたはStorage Virtual Machine (SVM) レベルでストレージシステムにアクセスできます。クラスタレベルでストレージシステムを追加する場合、必要なすべての機能を使用するには、管理者ユーザのクレデンシャルを指定する必要があります。SVM の詳細を直接追加してストレージシステムを追加する場合は、「vsadmin」ユーザには特定のタスクを実行するために必要なすべてのロールと機能が付与されるわけではないことに注意してください。

VASA Provider は、クラスタレベルでのみストレージシステムにアクセスできます。特定のストレージコントローラで VASA Providerが必要な場合は、ONTAP ツールまたは SRA を使用している場合でも、クラスタレベルでストレージシステムを ONTAP tools に追加する必要があります。

新しいユーザを作成し、クラスタまたは SVM を ONTAP ツールに接続するには、次の作業を行う必要があります。

- ONTAP System Manager 9.8P1以降を使用して、クラスタ管理者または SVM 管理者ロールを作成します。を参照してください "[ユーザロールと権限を設定](#)" を参照してください。
- ONTAP を使用して、ロールが割り当てられ、適切なアプリケーションが設定されたユーザを作成します

作成したストレージシステムのクレデンシャルは、ONTAP tools用にストレージシステムを設定する際に必要になります。ONTAP tools用にストレージシステムを設定するには、ONTAP toolsでクレデンシャルを入力します。これらのクレデンシャルを使用してストレージシステムにログインすると、クレデンシャルの作成時に ONTAP で設定した ONTAP tools 機能に対する権限が付与されます。
- ONTAP tools にストレージシステムを追加し、作成したユーザのクレデンシャルを指定します

ONTAP tools のロール

ONTAP tools では、ONTAP の権限を次の ONTAP tools ロールに分類します。

- 検出

接続されているすべてのストレージコントローラを検出できます
- ストレージを作成します

ボリュームおよび論理ユニット番号（LUN）を作成できます
- ストレージを変更します

ストレージシステムのサイズ変更と重複排除を実行できます
- ストレージを破棄します

ボリュームおよび LUN を破棄できます

VASA Provider ロール

クラスタレベルで作成できるのは Policy Based Management のみです。ストレージ機能プロファイルを使用してポリシーベースでストレージを管理できます。

SRA ロール

SRA では、ONTAP 権限をクラスタレベルまたは SVM レベルで SAN または NAS ロールに分類します。これにより、ユーザは SRM 処理を実行できるようになります。

クラスタを ONTAP tools に追加するときに、ONTAP ツールで ONTAP RBAC ロールの権限の初期検証が実行されます。直接接続の SVM ストレージ IP を追加した場合、ONTAP tools では初期検証は実行されません。ONTAP tools では、タスクワークフローの後半で権限がチェックされて適用されます。

著作権に関する情報

Copyright © 2023 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。