



# システムの保護対策

## StorageGRID 11.7

NetApp  
April 12, 2024

# 目次

システムの保護対策.....	1
システムのセキュリティ強化：概要.....	1
ソフトウェアアップグレードの強化に関するガイドライン.....	1
StorageGRID ネットワークのセキュリティ強化のガイドライン.....	2
StorageGRID ノードの保護対策のガイドライン.....	3
TLSとSSHに関するセキュリティ強化ガイドライン.....	6
その他のセキュリティ強化に関するガイドライン.....	8

# システムの保護対策

## システムのセキュリティ強化：概要

システムのセキュリティ強化とは、StorageGRID システムからできるだけ多くのセキュリティリスクを排除するプロセスです。

このドキュメントでは、StorageGRID 固有の強化ガイドラインの概要を説明します。これらのガイドラインは、システム強化に関する業界標準のベストプラクティスを補足するものです。たとえば、次のガイドラインでは、StorageGRID に強力なパスワードを使用し、HTTP ではなく HTTPS を使用し、可能な場合は証明書ベースの認証を有効にすることを前提としています。

StorageGRID をインストールして構成する際に、これらのガイドラインを使用して、情報システムの機密性、整合性、可用性に関する規定のセキュリティ目標を達成できます。

StorageGRID はに準拠しています "[NetApp Vulnerability Handling Policyの略](#)". 報告された脆弱性は、製品セキュリティインシデント対応プロセスに従って検証および解決されます。

## StorageGRID システムを強化するための一般的な考慮事項

StorageGRID システムを強化する際は、次の点を考慮する必要があります。

- 実装した 3 つの StorageGRID ネットワークのうち、どれですか。すべての StorageGRID システムでグリッドネットワークを使用する必要がありますが、管理ネットワーク、クライアントネットワーク、またはその両方を使用することもできます。ネットワークごとにセキュリティに関する考慮事項が異なります。
- StorageGRID システムの個々のノードで使用するプラットフォームのタイプ。StorageGRID ノードは、VMware 仮想マシン、Linux ホスト上のコンテナエンジン、または専用のハードウェアアプライアンスとして導入できます。プラットフォームのタイプごとに、強化に関するベストプラクティスがあります。
- テナントアカウントが信頼されている方法。テナントアカウントを信頼しないサービスプロバイダである場合は、信頼できる社内テナントのみを使用した場合はセキュリティ上の問題が異なります。
- どのセキュリティ要件および規則に準拠しているか。特定の規制や企業の要件に準拠しなければならない場合があります。

## ソフトウェアアップグレードの強化に関するガイドライン

攻撃を防御するには、StorageGRID システムおよび関連サービスを最新の状態に保つ必要があります。

### StorageGRID ソフトウェアへのアップグレード

StorageGRID ソフトウェアは、可能なかぎり、最新のメジャーリリースまたは以前のメジャーリリースにアップグレードする必要があります。StorageGRID を最新の状態に保つことで、既知の脆弱性がアクティブになる時間を短縮し、攻撃対象領域全体を削減できます。また、StorageGRID の最新リリースには、以前のリリースには含まれていないセキュリティ強化機能が含まれていることがよくあります。

を参照してください "[NetApp Interoperability Matrix Tool で確認できます](#)" (IMT) をクリックして、使用する StorageGRID ソフトウェアのバージョンを確認します。ホットフィックスが必要になったときに、ネット

アップは最新リリースの更新プログラムの作成に優先順位を付けます。一部のパッチは、以前のリリースと互換性がない場合があります。

- 最新のStorageGRID リリースとホットフィックスをダウンロードするには、に進みます ["ネットアップのダウンロード：StorageGRID"](#)。
- StorageGRID ソフトウェアをアップグレードするには、を参照してください ["アップグレード手順"](#)。
- ホットフィックスを適用するには、を参照してください ["StorageGRID ホットフィックス手順"](#)。

## 外部サービスへのアップグレード

外部サービスには、StorageGRID に間接的に影響する脆弱性が存在する場合がありますStorageGRID が依存するサービスが最新の状態で保たれていることを確認してください。LDAP、KMS（KMIP サーバ）、DNS、NTP などのサービスを利用できます。

を使用します ["NetApp Interoperability Matrix Tool で確認できます"](#) をクリックすると、サポートされるバージョンのリストが表示されます。

## ハイパーバイザーのアップグレード

StorageGRID ノードが VMware または別のハイパーバイザーで実行されている場合は、ハイパーバイザーのソフトウェアとファームウェアが最新であることを確認する必要があります。

を使用します ["NetApp Interoperability Matrix Tool で確認できます"](#) をクリックすると、サポートされるバージョンのリストが表示されます。

## \* Linux ノードへのアップグレード\*

StorageGRID ノードで Linux ホストプラットフォームを使用している場合は、セキュリティ更新とカーネル更新がホスト OS に適用されていることを確認する必要があります。また、これらの更新プログラムが利用可能になった場合は、脆弱なハードウェアにファームウェアの更新プログラムを適用する必要があります。

を使用します ["NetApp Interoperability Matrix Tool で確認できます"](#) をクリックすると、サポートされるバージョンのリストが表示されます。

## StorageGRID ネットワークのセキュリティ強化のガイドライン

StorageGRID システムでは、グリッドノードあたり最大 3 つのネットワークインターフェイスがサポートされ、各グリッドノードのネットワークをセキュリティやアクセスの要件に応じて設定することができます。

StorageGRID ネットワークの詳細については、を参照してください ["StorageGRID のネットワークタイプ"](#)。

## グリッドネットワークのガイドライン

グリッドネットワークはすべての内部 StorageGRID トラフィック用に設定する必要があります。グリッドネットワークのグリッドノードは、いずれも他のすべてのノードと通信できなければなりません。

グリッドネットワークを設定する際は、次のガイドラインに従ってください。

- オープンインターネット上のクライアントなど、信頼できないクライアントからネットワークが保護されていることを確認します。
- 可能な場合は、グリッドネットワークを内部トラフィック専用にします。管理ネットワークとクライアントネットワークの両方に、内部サービスへの外部トラフィックをブロックするファイアウォール制限が追加されています。グリッドネットワークを使用した外部クライアントトラフィックの処理はサポートされていますが、この使用によって保護レイヤが少なくなります。
- StorageGRID 環境が複数のデータセンターにまたがっている場合は、仮想プライベートネットワーク（VPN）またはグリッドネットワーク上で同等の機能を使用して、内部トラフィックをさらに保護します。
- 一部のメンテナンス手順では、プライマリ管理ノードと他のすべてのグリッドノードの間のポート 22 で Secure Shell（SSH）アクセスが必要です。外部ファイアウォールを使用して、信頼できるクライアントへの SSH アクセスを制限します。

## 管理ネットワークのガイドライン

管理ネットワークは、通常、管理タスク（Grid Manager または SSH を使用する信頼できる従業員）および LDAP、DNS、NTP、KMS（KMIP サーバ）などの信頼された他のサービスとの通信に使用します。ただし、StorageGRID ではこの使用が内部的に適用されることはありません。

管理ネットワークを使用する場合は、次のガイドラインに従ってください。

- 管理ネットワーク上のすべての内部トラフィックポートをブロックします。を参照してください ["内部ポートのリスト"](#)。
- 信頼されていないクライアントが管理ネットワークにアクセスできる場合は、外部ファイアウォールで管理ネットワーク上の StorageGRID へのアクセスをブロックします。

## クライアントネットワークのガイドライン

クライアントネットワークは、通常、テナント、および CloudMirror レプリケーションサービスや別のプラットフォームサービスなどの外部サービスとの通信に使用されます。ただし、StorageGRID ではこの使用が内部的に適用されることはありません。

クライアントネットワークを使用する場合は、次のガイドラインに従ってください。

- クライアントネットワーク上のすべての内部トラフィックポートをブロックします。を参照してください ["内部ポートのリスト"](#)。
- 明示的に設定されたエンドポイントでのみ、インバウンドクライアントトラフィックを受け入れます。の情報を参照してください ["ファイアウォールコントロールの管理"](#)。

## StorageGRID ノードの保護対策のガイドライン

StorageGRID ノードは、VMware 仮想マシン、Linux ホスト上のコンテナエンジン、または専用のハードウェアアプライアンスとして導入できます。プラットフォームのタイプとノードのタイプにはそれぞれ、強化に関するベストプラクティスがあります。

### ファイアウォールの設定

システム強化プロセスの一環として、外部ファイアウォールの設定を確認し、IP アドレスとそれが厳密に必要なポートからのみトラフィックが許可されるように変更する必要があります。

StorageGRID には、各ノードに内部ファイアウォールがあります。このファイアウォールを使用すると、ノードへのネットワークアクセスを制御できるため、グリッドのセキュリティが強化されます。お勧めします "[内部ファイアウォールコントロールを管理します](#)" 特定のグリッド環境に必要なポート以外のすべてのポートでネットワークアクセスを禁止する。[Firewall]コントロールページで行った設定変更は、各ノードに展開されます。

具体的には、次の領域を管理できます。

- 特権アドレス：[外部アクセスの管理]タブの設定によって閉じられたポートに、選択したIPアドレスまたはサブネットがアクセスできるようにすることができます。
- 外部アクセスの管理：デフォルトで開いているポートを閉じるか、以前閉じていたポートを再度開くことができます。
- 信頼されていないクライアントネットワーク：ノードがクライアントネットワークからのインバウンドトラフィックを信頼するかどうか、および信頼されていないクライアントネットワークが設定されている場合に開く追加ポートを指定できます。

この内部ファイアウォールは、一部の一般的な脅威に対する追加の保護レイヤを提供しますが、外部ファイアウォールの必要性は排除されません。

StorageGRID で使用されるすべての内部ポートと外部ポートのリストについては、を参照してください "[ネットワークポートのリファレンス](#)"。

## 未使用のサービスを無効にします

すべての StorageGRID ノードについて、未使用のサービスへのアクセスを無効化またはブロックする必要があります。たとえば、NFSの監査共有へのクライアントアクセスを設定する予定がない場合は、これらのサービスへのアクセスをブロックまたは無効にします。

## 仮想化、コンテナ、共有ハードウェア

すべての StorageGRID ノードで、信頼されていないソフトウェアと同じ物理ハードウェア上で StorageGRID を実行しないでください。StorageGRID とマルウェアの両方が同じ物理ハードウェア上に存在する場合、ハイパーバイザーの保護によってStorageGRIDで保護されたデータへのマルウェアのアクセスが防止されるとは限りません。たとえば、Meltdown と Specter 攻撃は、最新のプロセッサに存在する重要な脆弱性を悪用し、プログラムが同じコンピュータ上のメモリにデータを盗むことを可能にします。

## インストール中にノードを保護

ノードがインストールされているときに、信頼されていないユーザがネットワーク経由でStorageGRID ノードにアクセスできないようにします。ノードは、グリッドに参加するまで完全にセキュアになりません。

## 管理ノードのガイドライン

管理ノードは、システムの設定、監視、ロギングなどの管理サービスを提供します。Grid Manager または Tenant Manager にサインインすると、管理ノードに接続されます。

StorageGRID システムで管理ノードを保護するには、次のガイドラインに従います。

- 開いているインターネット上の管理ノードなど、信頼されていないクライアントからすべての管理ノードを保護します。グリッドネットワーク上、管理ネットワーク上、またはクライアントネットワーク上のどの管理ノードにも、信頼されていないクライアントがアクセスできないようにします。

- StorageGRID グループは Grid Manager とテナントマネージャの機能へのアクセスを制御します。各ユーザグループにロールに最低限必要な権限を付与し、読み取り専用アクセスモードを使用してユーザによる設定変更を防止します。
- StorageGRID ロードバランサエンドポイントを使用する場合は、信頼されないクライアントトラフィックに管理ノードの代わりにゲートウェイノードを使用します。
- 信頼されていないテナントがある場合は、そのテナントにTenant Managerまたはテナント管理APIへの直接アクセスを許可しないでください。代わりに、信頼されていないテナントがテナントポータルまたはテナント管理APIと連動する外部テナント管理システムを使用するようにします。
- 必要に応じて、管理プロキシを使用して、管理ノードからネットアップサポートへのAutoSupport 通信を詳細に制御します。の手順を参照してください ["管理プロキシの作成"](#)。
- 必要に応じて、制限された 8443 ポートと 9443 ポートを使用して Grid Manager と Tenant Manager の通信を分離します。共有ポート 443 をブロックして、テナント要求をポート 9443 に制限して追加の保護を確保します。
- 必要に応じて、グリッド管理者とテナントユーザには別々の管理ノードを使用します。

詳細については、の手順を参照してください ["StorageGRID の管理"](#)。

## ストレージノードに関するガイドライン

ストレージノードは、オブジェクトデータとメタデータを管理および格納します。StorageGRID システムでストレージノードを保護するには、次のガイドラインに従います。

- 信頼されていないクライアントがストレージノードに直接接続することを許可しないでください。ゲートウェイノードまたはサードパーティのロードバランサによって処理されるロードバランサエンドポイントを使用します。
- 信頼されていないテナントに対してアウトバウンドサービスを有効にしないでください。たとえば、信頼されていないテナントのアカウントを作成する場合は、テナントに独自のアイデンティティソースの使用やプラットフォームサービスの使用を許可しないでください。の手順を参照してください ["テナントアカウントを作成する"](#)。
- 信頼されないクライアントトラフィックには、サードパーティのロードバランサを使用します。サードパーティ製のロードバランシングにより、攻撃に対する制御性が向上し、追加の保護レイヤが提供されます。
- 必要に応じて、ストレージプロキシを使用して、クラウドストレージプールとプラットフォームサービスのストレージノードから外部サービスへの通信をより細かく制御します。の手順を参照してください ["ストレージプロキシを作成します"](#)。
- 必要に応じて、クライアントネットワークを使用して外部サービスに接続します。次に、\* configuration > Security > Firewall control > Untrusted Client Networks \*を選択し、ストレージノード上のクライアントネットワークが信頼されていないことを指定します。ストレージノードはクライアントネットワーク上の受信トラフィックを受け入れなくなりますが、プラットフォームサービスへのアウトバウンド要求は引き続き許可します。

## ゲートウェイノードのガイドライン

ゲートウェイノードは、クライアントアプリケーションが StorageGRID への接続に使用できるオプションのロードバランシングインターフェイスです。StorageGRID システムにゲートウェイノードを保護するには、次のガイドラインに従います。

- ロードバランサエンドポイントを設定して使用する。を参照してください ["ロードバランシングに関する"](#)

## 考慮事項

- クライアントとゲートウェイノードまたはストレージノードの間で、信頼されていないクライアントトラフィックにサードパーティのロードバランサを使用します。サードパーティ製のロードバランシングにより、攻撃に対する制御性が向上し、追加の保護レイヤが提供されます。サードパーティのロードバランサを使用する場合でも、内部のロードバランサエンドポイントを経由するようにネットワークトラフィックを設定したり、ストレージノードに直接送信したりすることができます。
- ロードバランサエンドポイントを使用している場合は、必要に応じてクライアントネットワーク経由で接続します。次に、\* configuration > Security > Firewall control > Untrusted Client Networks \*を選択し、ゲートウェイノード上のクライアントネットワークが信頼されていないことを指定します。ゲートウェイノードは、ロードバランサエンドポイントとして明示的に設定されたポートのインバウンドトラフィックのみを受け入れます。

## ハードウェアアプライアンスノードのガイドライン

StorageGRID ハードウェアアプライアンスは、StorageGRID システム専用に設計されています。一部のアプライアンスはストレージノードとして使用できます。その他のアプライアンスは、管理ノードまたはゲートウェイノードとして使用できます。アプライアンスノードをソフトウェアベースのノードと組み合わせることも、自社開発の全アプライアンスグリッドを導入することもできます。

StorageGRID システムにハードウェアアプライアンスノードを固定するには、次のガイドラインに従います。

- アプライアンスでストレージコントローラの管理に SANtricity System Manager を使用している場合は、信頼されていないクライアントからネットワーク経由で SANtricity System Manager にアクセスできないようにします。
- アプライアンスに Baseboard Management Controller (BMC ; ベースボード管理コントローラ) が搭載されている場合は、BMC 管理ポートで下位レベルのハードウェアアクセスが許可されることに注意してください。BMC 管理ポートは、信頼されているセキュアな内部管理ネットワークにのみ接続してください。該当するネットワークがない場合は、テクニカルサポートから BMC 接続の要請があった場合を除き、BMC 管理ポートを接続しないか、またはブロックしたままにしてください。
- アプライアンスが Intelligent Platform Management Interface (IPMI) 標準を使用したイーサネット経由でのコントローラハードウェアのリモート管理をサポートする場合は、ポート 623 での信頼されていないトラフィックをブロックします。



管理APIのプライベートエンドポイントPUT /private/bmcを使用して、BMCを含むすべてのアプライアンスに対してリモートIPMIアクセスを有効または無効にできます。

- アプライアンスのストレージコントローラに FDE または FIPS ドライブが搭載されていて、ドライブセキュリティ機能が有効になっている場合は、SANtricity を使用してドライブセキュリティキーを設定します。を参照してください "[SANtricity システムマネージャの設定 \(SG6000およびSG5700\)](#)"。
- FDE または FIPS ドライブが搭載されていないアプライアンスの場合は、Key Management Server (KMS) を使用してノード暗号化を有効にします。を参照してください "[オプション：ノード暗号化を有効にします](#)"。

## TLSとSSHに関するセキュリティ強化ガイドライン

インストール時に作成されるデフォルトの証明書を置き換え、TLS接続とSSH接続に適切なセキュリティポリシーを選択する必要があります。



## 証明書に関するセキュリティ強化ガイドライン

インストール時に作成されたデフォルトの証明書を独自のカスタム証明書に置き換える必要があります。

多くの組織では、StorageGRID Web アクセス用の自己署名デジタル証明書が、情報セキュリティポリシーに準拠していません。本番システムでは、StorageGRID の認証に使用する CA 署名デジタル証明書をインストールする必要があります。

具体的には、次のデフォルト証明書ではなくカスタムサーバ証明書を使用する必要があります。

- \* 管理インターフェイス証明書 \* : Grid Manager、Tenant Manager、Grid 管理 API、およびテナント管理 API へのアクセスを保護するために使用します。
- \* S3 および Swift API 証明書 \* : ストレージノードおよびゲートウェイノードへのアクセスを保護するために使用します。これらのノードは、S3 および Swift クライアントアプリケーションがオブジェクトデータのアップロードとダウンロードに使用します。

を参照してください ["セキュリティ証明書を管理する"](#) を参照してください。



StorageGRID では、ロードバランサエンドポイントに使用する証明書は別に管理されます。ロードバランサ証明書を設定するには、[を参照してください "ロードバランサエンドポイントを設定する"](#)。

カスタムサーバ証明書を使用する場合は、次のガイドラインに従ってください。

- 証明書には必要です `subjectAltName` StorageGRID の DNS エントリと同じです。詳細については、のセクション 4.2.1.6 「Subject Alternative Name」を参照してください ["RFC 5280: PKIX 証明書と CRL プロファイル"](#)。
- 可能であれば、ワイルドカード証明書は使用しないでください。ただし、S3 仮想ホスト形式のエンドポイントの証明書は例外です。この証明書では、バケット名が事前にわからない場合にワイルドカードを使用する必要があります。
- 証明書にワイルドカードを使用する必要がある場合は、リスクを軽減するために追加の手順を実行する必要があります。などのワイルドカードパターンを使用します `*.s3.example.com`` を使用しないでください ``s3.example.com` その他のアプリケーションのサフィックス。このパターンは、などのパス形式の S3 アクセスでも機能します `dc1-s1.s3.example.com/mybucket`。
- 証明書の有効期限を短く（2 カ月など）設定し、グリッド管理 API を使用して証明書のローテーションを自動化します。これは、ワイルドカード証明書で特に重要です。

また、クライアントは StorageGRID との通信に厳密なホスト名チェックを使用する必要があります。

## TLS および SSH ポリシーに関するセキュリティ強化ガイドライン

セキュリティポリシーを選択して、クライアントアプリケーションとのセキュアな TLS 接続の確立や内部 StorageGRID サービスへのセキュアな SSH 接続に使用するプロトコルと暗号を決定できます。

セキュリティポリシーは、TLS と SSH による移動中のデータの暗号化方法を制御します。ベストプラクティスとして、アプリケーションの互換性に必要ない暗号化オプションを無効にすることを推奨します。システムが情報セキュリティ国際評価基準に準拠している必要がある場合や、他の暗号を使用する必要がある場合を除き、最新のデフォルトポリシーを使用します。

を参照してください ["TLS および SSH ポリシーを管理します"](#) を参照してください。

# その他のセキュリティ強化に関するガイドライン

StorageGRID ネットワークおよびノードに対する強化ガイドラインに加えて、StorageGRID システムの他の領域に対する強化ガイドラインに従う必要があります。

## ログと監査メッセージ

StorageGRID ログおよび監査メッセージ出力は必ず安全な方法で保護してください。StorageGRID のログと監査メッセージは、サポートやシステム可用性の観点から非常に重要な情報を提供します。また、StorageGRID のログおよび監査メッセージの出力に含まれる情報や詳細情報は、一般に機密性が高いため、

セキュリティイベントを外部 syslog サーバに送信するように StorageGRID を設定します。syslog エクスポートを使用する場合は、トランスポートプロトコルに対して TLS と RELP/TLS を選択します。

を参照してください "[ログファイル参照](#)" StorageGRID ログの詳細については、を参照してください。を参照してください "[監査メッセージ](#)" StorageGRID 監査メッセージの詳細については、を参照してください。

## NetApp AutoSupport

StorageGRID のAutoSupport 機能を使用すると、システムの健全性をプロアクティブに監視し、ネットアップテクニカルサポート、組織内のサポートチーム、またはサポートパートナーにメッセージと詳細を自動的に送信できます。ネットアップテクニカルサポートへのAutoSupport メッセージの送信は、StorageGRID の初回設定時にデフォルトで有効になります。

AutoSupport 機能は無効にすることができます。ただし、StorageGRID システムで問題に障害が発生した場合には、AutoSupport を使用して迅速に問題を識別し解決できるため、ネットアップではこの機能を有効にすることを推奨しています。

AutoSupport は、転送プロトコルとして HTTPS、HTTP、SMTP をサポートしています。AutoSupport メッセージは機密性が高いため、ネットアップサポートにAutoSupport メッセージを送信する際のデフォルトの転送プロトコルとしてHTTPSを使用することを強く推奨します。

## Cross-Origin Resource Sharing (CORS)

S3バケットとバケット内のオブジェクトに他のドメインにあるWebアプリケーションからアクセスできるようにするには、そのバケットにCross-Origin Resource Sharing (CORS) を設定します。一般的に、CORSは必要でない限り有効にしないでください。CORSが必要な場合は、信頼できるオリジンに制限します。

の手順を参照してください "[Cross-Origin Resource Sharing \(CORS\) の設定](#)".

## 外部セキュリティデバイス

完全なセキュリティ強化解策は、StorageGRID 以外のセキュリティメカニズムに対応する必要があります。StorageGRID へのアクセスをフィルタリングおよび制限するために追加のインフラデバイスを使用すると、厳格なセキュリティ体制を確立し、維持するための効果的な方法となります。これらの外部セキュリティデバイスには、ファイアウォール、Intrusion Prevention System (IPS ; 侵入防御システム)、およびその他のセキュリティデバイスが含まれます。

信頼されないクライアントトラフィックには、サードパーティのロードバランサを使用することを推奨します。サードパーティ製のロードバランシングにより、攻撃に対する制御性が向上し、追加の保護レイヤが提供されます。

## ランサムウェアの軽減

の推奨事項に従って、ランサムウェア攻撃からオブジェクトデータを保護しましょう ["StorageGRID によるランサムウェア対策"](#)。

## 著作権に関する情報

Copyright © 2024 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。