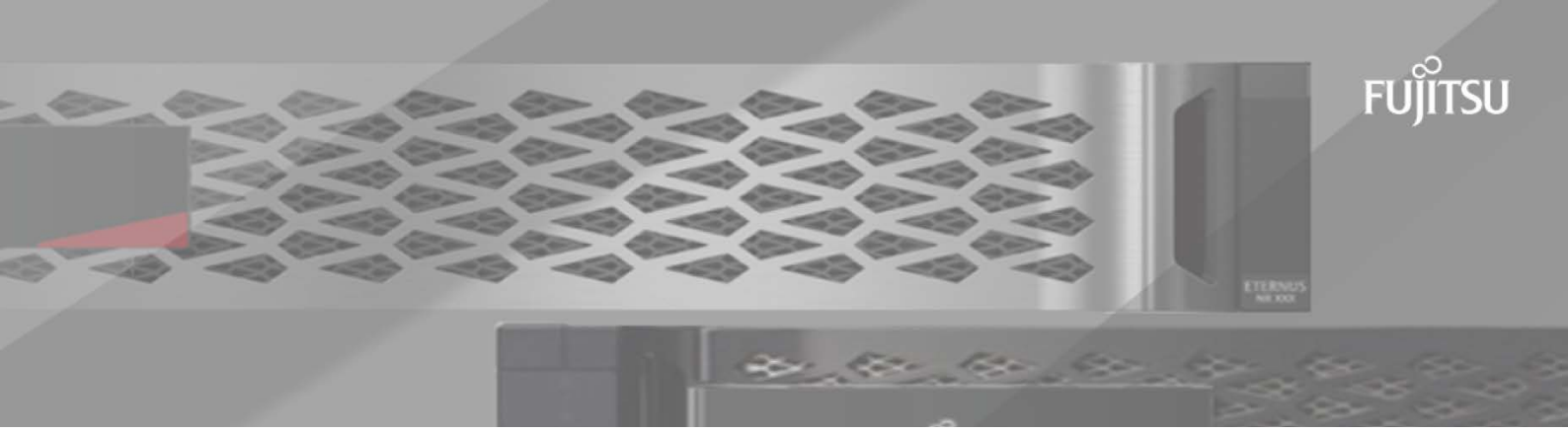


# SANtricity 11.7 Unified Manager

## *CA08871-193*

Fujitsu Limited

Version 04

# Table of Contents

# メイン画面

## Unified Managerインターフェイスの概要

Unified　ManagerはWebベースのインターフェイスであり、1つのビューで複数のストレージ システムを管理することができます。

### メイン ページ

Unified Managerにログインすると、メイン ページが開き、**[管理 - すべて]** が表示されます。このページから、ネットワーク内で検出されたストレージ システムのリストをスクロールして、そのステータスを表示し、1つのアレイまたはアレイ グループに対して処理を実行できます。

### ナビゲーション サイドバー

ナビゲーション サイドバーからUnified Managerの各機能にアクセスできます。

| 領域 | 説明 |
|---|---|
| 管理 | ネットワーク内のストレージ　システムの検出、アレイのSANtricity　System Managerの起動、1つのアレイから複数のアレイへの設定のインポート、およびアレイ グループの管理を行います。設定のインポートやアレイ グループの作成など、アレイに対する処理を実行するには、アレイ名の横にあるチェックボックスを選択します。各行の最後にある省略記号をクリックすると、1つのアレイに対する処理（アレイ名の変更など）のインライン　メニューが表示されます。 |
| 処理 | バッチ処理（アレイ間での設定のインポートなど）の進捗状況が表示されます。<br>ストレージ　システムのステータスが最適でない場合は、一部の処理は使用できません。 |
| 証明書管理 | ブラウザーとクライアント間の認証を行う証明書を管理します。 |
| アクセス管理 | Unified Managerインターフェイスのユーザー認証を確立します。 |
| サポート | 富士通のサポートのオプション、リソース、および連絡先が表示されます。 |

### 画面の設定とヘルプ

画面右上からヘルプやその他のドキュメントにアクセスできます。ログイン名の横にあるドロップダウンから管理オプションにアクセスすることもできます。

### ユーザー ログインとパスワード

システムに現在ログインしているユーザーが画面右上に表示されます。

ユーザーとパスワードの詳細については、以下を参照してください。

- 管理者パスワード保護の設定
- 管理者パスワードの変更
- ローカル ユーザー プロファイルのパスワードの変更

## サポートされるブラウザー

Unified Managerには、いくつかの種類のブラウザーからアクセスできます。

サポートされるブラウザーとバージョンを次に示します。

| ブラウザー | 最小バージョン |
|---|---|
| Google Chrome | 79 |
| Mozilla Firefox | 70 |
| Safari | 12 |
| Microsoft Edge | 79 |
| Microsoft Edge Legacy | 18 |
| Microsoft Internet Explorer（MSIE） | 11 |

Web Services Proxyがインストールされていて、ブラウザーから使用できる必要があります。

## 管理者パスワード保護の設定

Unified Managerには、不正なアクセスを防ぐために管理者パスワードを設定する必要があります。

### 管理者パスワードとユーザー プロファイル

Unified Managerを初めて起動したとき、管理者パスワードを設定するように求められます。管理者パスワードを知っているユーザーは、ストレージ システムの設定を変更することができます。

管理者パスワードに加えて、Unified Managerには、ロールが1つ以上割り当てられたユーザー プロファイルがあらかじめ設定されています。詳細については、アクセス管理の仕組みを参照してください。

ユーザーとマッピングは変更できません。変更できるのはパスワードのみです。パスワードの変更については、以下を参照してください。

- 管理者パスワードの変更
- ローカル ユーザー プロファイルのパスワードの変更

### セッション タイムアウト

1つの管理セッションでパスワードの入力を求められるのは1回のみです。デフォルトでは操作がない状態が30分続くとセッションがタイムアウトし、パスワードをもう一度入力する必要があります。セッション中に別の管理クライアントから同じソフトウェアにアクセスしている別のユーザーがパスワードを変更した場合は、次回の設定処理や表示処理でパスワードの入力を求められます。

セキュリティ上の理由から、パスワードの入力を試行できるのは5回までとなっており、この回数を超えると、ソフトウェアは「ロックアウト」状態になります。この状態のソフトウェアはその後のパスワード入力を拒否します。パスワードを再度入力するには、「通常」状態にリセットされるまで10分間待つ必要があります。

セッション　タイムアウトを調整したり、セッション　タイムアウトを無効にしたりできます。詳細については、「セッション タイムアウトの管理」を参照してください。

## 管理者パスワードの変更

Unified Managerへのアクセスに使用する管理者パスワードを変更できます。

開始する前に

- Root Adminの権限が割り当てられたローカル管理者としてログインする必要があります。
- 現在の管理者パスワードを知っている必要があります。

タスク概要

パスワードを決める際は、次のガイドラインに注意してください。

- パスワードでは大文字と小文字が区別されます。
- パスワードの末尾のスペースは削除されません。設定時に末尾にスペースを含めた場合は、入力時にスペースを含めるようにしてください。
- セキュリティを強化するため、パスワードには15文字以上の英数字を使用し、頻繁に変更してください。

手順

1. [設定] > [アクセス管理]を選択します。
2. **[ローカル ユーザ ロール]** タブを選択します。
3. **admin** ユーザーを表から選択します。

   [パスワードの変更]ボタンが使用可能な状態になります。
4. **[パスワードの変更]** を選択します。

[パスワードの変更]ダイアログ ボックスが開きます。

5. ローカル ユーザー パスワードに対して最小文字数が設定されていない場合は、システムにアクセスするユーザーにパスワードの入力を求めるチェックボックスを選択します。
6. 2つのフィールドに新しいパスワードを入力します。
7. この処理を実行する確認としてローカル管理者パスワードを入力し、**[変更]** をクリックします。

## セッション タイムアウトの管理

非アクティブな状態が一定の時間続いたユーザー　　セッションは切断されるよう、Unified Managerでタイムアウトを設定できます。

タスク概要

デフォルトでは、Unified Managerのセッション タイムアウトは30分です。この時間を調整したり、セッション タイムアウトを無効にしたりできます。

手順

1. メニュー バーで、ユーザー ログイン名の横にあるドロップダウン矢印を選択します。
2. **[セッション タイムアウトの有効化 / 無効化]** を選択します。

   [セッション タイムアウトの有効化 / 無効化]ダイアログ ボックスが開きます。
3. スピン ボックスを使用して時間（分単位）を増減します。

   設定できる最小値は15分です。

   セッション タイムアウトを無効にするには、**[セッションが非アクティブ…]** チェックボックスの選択を解除します。
4. **[保存]** をクリックします。

# ストレージ アレイ

## 検出の概要

ストレージリソースを管理するには、最初にネットワーク内のストレージシステムを検出する必要があります。

### アレイの検出方法

組織のネットワークから管理対象のストレージ システムを検索して追加するには、[追加 / 検出]ページを使用します。複数のアレイを検出することも、単一のアレイを検出することもできます。検出するためには、ネットワークIPアドレスを入力します。指定したアドレス範囲内の各IPアドレスへの接続がUnified

Managerで個別に試行されます。

詳細情報：

- アレイの検出に関する考慮事項
- 複数のストレージ システムの検出
- 単一のアレイの検出

### アレイの管理方法

アレイを検出したあと、**[管理 - すべて]** ページに移動します。このページから、ネットワーク内で検出されたストレージ　システムのリストをスクロールして、そのステータスを表示し、1つのアレイまたはアレイ グループに対して処理を実行できます。

単一のアレイを管理する場合は、そのアレイを選択してSANTricity　System　Managerを開くことができます。

詳細情報：

- System Managerへのアクセスに関する考慮事項
- 個々のストレージ システムの管理
- ストレージ システムのステータスの表示

## 概念

### アレイの検出に関する考慮事項

Unified Managerでストレージ リソースを表示して管理する前に、組織のネットワークから管理対象のストレージ システムを検出する必要があります。複数のアレイを検出することも、単一のアレイを検出することもできます。

#### 複数のストレージ システムの検出

複数のアレイを検出する場合は、ネットワークIPアドレスの範囲を入力すると、その範囲の各IPアドレスへの接続がUnified Managerで個別に試行されます。到達できたストレージ システムが[追加 / 検出]ページに表示され、管理ドメインに追加できます。

#### 単一のストレージ システムの検出

単一のアレイを検出する場合は、ストレージ　システムのいずれかのコントローラーのIPアドレスを1つ入力すると、そのストレージ システムが追加されます。

Unified　Managerは、あるコントローラーに割り当てられている1つのIPアドレスまたは範囲内のIPアドレスだけを検出して表示します。代替のコントローラーまたはそれら

のコントローラーに割り当てられているIPアドレスがあっても、この1つのIPアドレスまたはIPアドレス範囲に含まれていなければ、Unified　Managerでは検出または表示されません。ただし、いったんストレージ システムを追加すると、関連付けられているIPアドレスがすべて検出されて[管理]ビューに表示されます。

**ユーザー クレデンシャル**

検出プロセスでは、追加する各ストレージ システムの管理者パスワードが必要になります。

**Webサービスの証明書**

検出プロセスでは、検出されたストレージ　　システムに信頼できるソースからの証明書があるかどうかがUnified　Managerで確認されます。Unified　Managerでは、ブラウザーで確立するすべての接続に対して2種類の証明書ベースの認証を使用します。

- **信頼された証明書**

  Unified　Managerで検出されたアレイについては、認証局が発行する信頼された証明書が追加で必要となる場合があります。

  これらの証明書をインポートするには、**[インポート]** ボタンを使用します。このアレイに前に接続したことがある場合は、一方または両方のコントローラーの証明書が期限切れになっているか、失効しているか、証明書チェーンにルート証明書または中間証明書がない可能性があります。ストレージ　システムの管理を開始する前に、期限切れまたは失効した証明書を差し替えるか、不足しているルート証明書または中間証明書を追加する必要があります。

- **自己署名証明書**

  自己署名証明書を使用することもできます。署名済みの証明書をインポートせずにアレイを検出しようとすると、Unified　Managerにエラー　ダイアログ　ボックスが表示されます。このダイアログ　ボックスで自己署名証明書を承認することができます。自己署名証明書が信頼済みとしてマークされ、Unified Managerにストレージ システムが追加されます。

  ストレージ　システムへの接続を信頼できない場合は、**[キャンセル]** を選択し、ストレージ　システムのセキュリティ証明書の方針を確認してからUnified　Managerにストレージ　システムを追加してください。

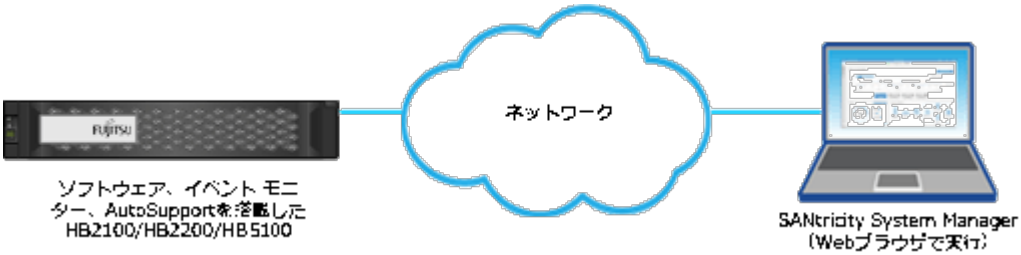
## System Managerへのアクセスに関する考慮事項

### ストレージ システムを設定および管理する場合は、1つ以上のストレージ システムを選択し、[起動]オプションを使用してSystem Managerを開きます。

System　Managerはコントローラーに組み込みのアプリケーションで、イーサネット管理ポートを介してネットワークに接続されます。System Managerにはアレイベースの機能がすべて含まれています。

System Managerにアクセスするには、以下を準備しておく必要があります。

- ETERNUS　AB/HBシリーズ　ハードウェアの概要 [https://www.fujitsu.com/jp/products/computing/storage/manual/]に記載されているアレイ モデル
- Webブラウザーを使用したネットワーク管理クライアントへのアウトオブバンド接続




# アレイの検出

## 複数のストレージ システムの検出

複数のアレイの検出では、管理サーバーが配置されているサブネット全体からすべてのストレージ システムを検出し、検出されたアレイを管理ドメインに自動的に追加します。

開始する前に

- Security Adminの権限を含むユーザー プロファイルでログインする必要があります。
- ストレージ システムのセットアップが完了し、正しく設定されている必要があります。
- ストレージ システムのパスワードがSystem Managerの[アクセス管理]タイルで設定されている必要があります。
- 信頼されていない証明書を解決するには、認証局（CA）の信頼された証明書ファイルがローカル システム上にある必要があります。

アレイの検出は複数の手順で構成されます。

### 手順 1：ネットワーク アドレスの入力

ローカルのサブネットワーク全体から検索するには、ネットワーク アドレスの範囲を入力します。到達できたストレージ システムが[追加 / 検出]ページに表示され、管理ドメインに追加できます。

何らかの理由で検出処理を中止する場合は、**[検出の中止]** をクリックします。

手順

1. [管理]ページで、**[追加 / 検出]** を選択します。

   [追加 / 検出]ダイアログ ボックスが表示されます。

2. **[ネットワーク アドレス範囲に含まれるすべてのストレージ システムを検出]** ラジオ ボタンを選択します。

3. ローカル サブネットワーク全体から検索する開始ネットワーク アドレスと終了ネットワーク アドレスを入力し、**[検出の開始]** をクリックします。

   検出プロセスが開始されます。この検出プロセスが完了するまでに数分かかることがあります。ストレージ システムが検出された順に[追加 / 検出]ページの表に表示されていきます。

   管理可能なアレイが検出されない場合は、ストレージ システムがネットワークに適切に接続されていて、割り当てられたアドレスが範囲内にあることを確認してください。**[新しい検出パラメータ]** をクリックして[追加 / 検出]ページに戻ります。

4. 検出されたストレージ システムのリストを確認します。
5. 管理ドメインに追加するストレージ システムの横にあるチェックボックスを選択し、**[次へ]** をクリックします。

   管理ドメインに追加する各アレイについて、Unified Managerでクレデンシャルのチェックが実行されます。そのアレイに関連付けられている自己署名証明書や信頼されていない証明書の解決が必要になる場合があります。

6. **[次へ]** をクリックしてウィザードの次の手順に進みます。

**手順 2：検出時の自己署名証明書の解決**

検出プロセスでは、ストレージ システムに信頼できるソースからの証明書があるかどうかが確認されます。

手順

1. 次のいずれかを実行します。
   - 検出されたストレージ システムへの接続を信頼する場合は、ウィザードの次のカードに進みます。自己署名証明書は信頼済みとしてマークされ、ストレージ システムはUnified Managerに追加されます。
   - ストレージ システムへの接続を信頼できない場合は、**[キャンセル]** を選択し、ストレージ システムのセキュリティ証明書の方針を確認してからUnified Managerにストレージ システムを追加してください。
2. **[次へ]** をクリックしてウィザードの次の手順に進みます。

**手順 3：検出時の信頼されていない証明書の解決**

信頼されていない証明書の問題は、ストレージ システムからUnified Managerへのセキュアーな接続を確立しようとしたときに、接続が安全であることが確認できないと発生します。アレイの検出時に信頼されていない証明書を解決するには、信頼できる第三者機関が発行した認証局（CA）証明書（CA署名証明書）をインポートします。

信頼された追加のCA証明書のインストールが必要になる可能性があるのは、次のいずれかに該当する場合です。

- ストレージ システムを新たに追加した。
- 一方または両方の証明書の期限が切れている。
- 一方または両方の証明書が失効している。
- 一方または両方の証明書のルート証明書または中間証明書がない。

手順

1. 信頼されていない証明書を解決するストレージ　システムの横にあるチェックボックスを選択し、**[インポート]**ボタンを選択します。

   信頼された証明書ファイルをインポートするためのダイアログ ボックスが表示されます。

2. **[参照]** をクリックし、ストレージ システムの証明書ファイルを選択します。

   ダイアログ ボックスにファイル名が表示されます。

3. **[インポート]** をクリックします。

   ファイルがアップロードされて検証されます。

   信頼されていない証明書の問題が未解決のストレージ システムはUnified Managerに追加されません。

4. **[次へ]** をクリックしてウィザードの次の手順に進みます。

#### ステップ 4：パスワードの入力

管理ドメインにストレージ システムを追加するときは、ストレージ システムのパスワードを入力する必要があります。

手順

1. Unified Managerに追加する各ストレージ システムのパスワードを入力します。
2. **オプション：** ストレージ システムをグループに関連付けます。ドロップダウン リストから、選択したストレージ システムを関連付けるグループを選択します。
3. **[完了]** をクリックします。

終了後の操作

ストレージ システムが管理ドメインに追加され、指定した場合は選択したグループに関連付けられます。

指定したストレージ システムへの接続がUnified Managerで確立されるまでに数分かかることがあります。

## 単一のアレイの検出

単一のストレージ　システムを手動で検出して組織のネットワークに追加するには、[単一のストレージ システムを追加 / 検出]オプションを使用します。

開始する前に

- ストレージ システムのセットアップが完了し、正しく設定されている必要があります。
- ストレージ システムのパスワードがSystem Managerの[アクセス管理]タイルで設定されている必要があります。

手順

1. [管理]ページで、**[追加 / 検出]** を選択します。

   [追加 / 検出]ダイアログ ボックスが表示されます。

2. **[単一のストレージ システムを検出]** ラジオ ボタンを選択します。
3. ストレージ システムのいずれかのコントローラーのIPアドレスを入力し、**[検出の開始]** をクリックします。

   指定したストレージ システムへの接続がUnified Managerで確立されるまでに数分かかることがあります。

   指定したIPアドレスでコントローラーに接続できない場合、「ストレージ システムにアクセスできません」というメッセージが表示されます。

4. 自己署名証明書についての確認が求められた場合は解決します。

   検出プロセスの一環として、検出されたストレージ システムに信頼できるソースからの証明書があるかどうかが確認されます。ストレージ システムのデジタル証明書が見つからない場合、承認された認証局（CA）の署名がない証明書について、セキュリティ例外を追加して解決するように求められます。

5. 信頼されていない証明書についての確認が求められた場合は解決します。

   信頼されていない証明書の問題は、ストレージ システムからUnified Managerへのセキュアーな接続を確立しようとしたときに、接続が安全であることが確認できないと発生します。信頼されていない証明書を解決するには、信頼できる第三者機関から発行された認証局（CA）証明書をインポートします。

6. **[次へ]** をクリックします。
7. **オプション：** 検出されたストレージ システムをグループに関連付けます。ドロップダウン リストから、選択したストレージ システムを関連付けるグループを選択します。

   デフォルトでは、[すべて]が選択されています。

8. 管理ドメインに追加するストレージ システムの管理者パスワードを入力し、**[OK]** をクリックします。

終了後の操作

ストレージ システムがUnified Managerに追加され、指定した場合は選択したグループにも追加されます。

サポート データの自動収集が有効になっている場合は、追加したストレージ システムのサポート データが自動的に収集されます。

# アレイの管理

## ストレージ システムのステータスの表示

Unified Managerには、検出された各ストレージ システムのステータスが表示されます。

**[管理 - すべて]** ページに移動します。このページで、Web Services Proxyとそのストレージ システムの間の接続のステータスを確認できます。

ステータス インジケータの説明を次の表に示します。

| ステータス | 説明 |
|---|---|
| 最適 | ストレージ　システムが最適な状態です。証明書の問題は存在せず、パスワードは有効です。 |
| 無効なパスワード | 無効なストレージ システム パスワードが指定されました。 |
| 信頼されていない証明書 | HTTPS証明書が自己署名証明書でインポートされていないか、またはCA署名証明書でルート証明書と中間CA証明書がインポートされていないため、ストレージ システムとの1つ以上の接続が信頼されていません。 |
| 要注意 | ストレージ システムにユーザーによる修正操作が必要な問題があります。 |
| ロックダウン | ストレージ システムがロックダウン状態です。 |
| 不明 | ストレージ システムに一度も接続していません。この状態は、Web Services Proxyが起動中でまだストレージ　システムに接続していない場合や、ストレージ システムがオフラインでWeb Services Proxyの起動後に一度も接続されていない場合に発生することがあります。 |
| オフライン | Web Services Proxyは以前にストレージ システムに接続しましたが、現在はすべての接続が失われています。 |

## 個々のストレージ システムの管理

[起動]オプションを使用すると、管理処理を実行する場合に1つ以上のストレージ　システムに対してブラウザーベースのSystem Managerを開くことができます。

手順

1. [管理]ページで、管理処理を実行する1つ以上のストレージ システムを選択します。
2. **[起動]** をクリックします。

   新しいウィンドウが開き、System Managerのログイン ページが表示されます。

3. ユーザー名とパスワードを入力し、**[ログイン]** をクリックします。

## ストレージ システムのパスワードの変更

Unified Managerでストレージ システムを表示したりアクセスしたりするときに使用するパスワードを更新できます。

開始する前に

- Storage Adminの権限を含むユーザー プロファイルでログインする必要があります。
- ストレージ システムの現在のパスワード（System Managerで設定されているパスワード）を確認しておきます。

タスク概要

このタスクでは、Unified Managerからストレージ システムにアクセスできるようにストレージ システムの現在のパスワードを入力します。これは、System Managerでアレイのパスワードが変更されたために、Unified Managerでも変更が必要になった場合などに行います。

手順

1. [管理]ページで、1つ以上のストレージ システムを選択します。
2. [一般的でないタスク] > [ストレージ システムのパスワードの入力]を選択します。
3. 各ストレージ システムのパスワードを入力し、**[保存]** をクリックします。

## SANtricity Unified Managerからのストレージ システムの削除

Unified Managerでストレージ システムを管理する必要がなくなった場合は、削除することができます。

タスク概要

削除すると、そのストレージ システムにはアクセスできなくなります。ただし、ブラウザーでIPアドレスまたはホスト名を直接指定すれば、削除したストレージ システムへの接続を確立できます。

ストレージ システムを削除しても、ストレージ システム自体やそのデータには影響はありません。ストレージ システムを誤って削除した場合は、再度追加することができます。

手順

1. **[管理]** ページを選択します。
2. 削除するストレージ システムを選択します。
3. [一般的でないタスク] > [ストレージ システムの削除]を選択します。

   ストレージ システムがSANtricity Unified Managerのすべてのビューから削除されます。

# 設定のインポート

## 設定のインポートの概要

設定のインポート機能を使用すると、1つのアレイから複数のアレイに設定をインポートするバッチ処理を実行できます。この機能により、ネットワークの複数のアレイを設定する場合に時間を短縮できます。

### どの設定をインポートできますか？

アラート方法、AutoSupport設定、ディレクトリー サービス設定、ストレージ設定（ボリューム グループやプールなど）、およびシステム設定（自動ロード バランシングなど）をインポートできます。

詳細情報：

- 設定のインポートの仕組み
- ストレージ構成のレプリケートに関する要件

### バッチ インポートを実行するにはどうすればよいですか？

ソースとして使用するストレージ システムで、System Managerを開いて希望するオプションを設定します。その後、Unified Managerの[管理]ページに移動し、設定を1つ以上のアレイにインポートします。

詳細情報：

- アラート設定のインポート
- AutoSupport設定のインポート
- ディレクトリー サービス設定のインポート
- ストレージ構成のインポート
- システム設定のインポート

## 概念

### 設定のインポートの仕組み

Unified Managerを使用して、1つのストレージ システムから複数のストレージ システムに設定をインポートできます。[設定のインポート]機能を使用して一括で処理すると、ネットワークの複数のアレイを設定する場合の時間を短縮できます。

### インポートできる設定

複数のアレイにインポートできる設定は次のとおりです。

- **アラート**
  Eメール、syslogサーバー、またはSNMPサーバーを使用して管理者に重要なイベントを送信するアラート方法です。
- **AutoSupport**
  ストレージ システムの健全性を監視し、富士通のサポートに自動ディスパッチを送信する機能です。
- **ディレクトリー サービス**
  LDAP（Lightweight Directory Access Protocol）サーバーとディレクトリー サービス（MicrosoftのActive Directoryなど）を使用してユーザー認証を管理する方法です。
- **ストレージ構成**
  次の項目に関連する設定です。
  - ボリューム（リポジトリ ボリュームでないシック ボリュームのみ）
  - ボリューム グループとプール
  - ホット スペア ドライブの割り当て
- **システム設定**
  次の項目に関連する設定です。
  - ボリュームのメディア スキャン設定
  - SSD設定
  - 自動ロード バランシング（ホスト接続レポートは含まれません）

### 設定ワークフロー

設定をインポートするワークフローは次のとおりです。

1. ソースとして使用するストレージ システムで、System Managerを使用して設定を行います。
2. ターゲットとして使用するストレージ システムで、System Managerを使用して設定をバックアップします。
3. Unified Managerで、**[管理]** ページに移動して設定をインポートします。
4. **[処理]** ページで、設定のインポート処理の結果を確認します。

## ストレージ構成のレプリケートに関する要件

ストレージ システム間でストレージ構成をインポートする前に、要件およびガイドラインを確認してください。

### シェルフ

- コントローラーが配置されているシェルフがソースとターゲットのアレイで同一である。

- シェルフIDがソースとターゲットのアレイで同一である。
- 拡張シェルフの同一のスロットに同じドライブ　タイプが搭載されている（ドライブが構成で使用されている場合、未使用ドライブの場所は問題になりません）。

**コントローラー**

- コントローラー　　タイプはソースとターゲットのアレイで同一である必要はないが、RBOD(RAID Bunch of Disks)エンクロージャのタイプは同一である必要がある。
- HIC（ホストのDA機能を含む）がソースとターゲットのアレイで同一である。
- FDE設定はインポート プロセスに含まれない。

**ステータス**

- ターゲット アレイのステータスが「最適」である。
- ソース アレイのステータスは「最適」である必要はない。

**ストレージ**

- ターゲットのボリューム容量がソースよりも大きいかぎり、ソースとターゲットのアレイでドライブ容量が違っていてもかまわない（ターゲット　アレイには容量の大きい新しいドライブが搭載されている場合、それらのドライブはレプリケーション処理によってボリュームに割り当てられない可能性があります）。
- ソース アレイのディスク プールのボリュームが64TB以上の場合、ターゲットでインポート プロセスを実行できない。
- シン ボリュームはインポート プロセスに含まれない。

# バッチ インポートの使用

## アラート設定のインポート

ストレージ　システムから別のストレージ　システムにアラート設定をインポートできます。この方法でバッチ処理すると、ネットワークの複数のアレイを設定する場合に時間を短縮できます。

開始する前に

- ソースとして使用するストレージ システムのアラート設定をSystem Manager（[設定] > [アラート]）で設定しておきます。
- ターゲット ストレージ システムの既存の設定をSystem Manager（[設定] > [システム] > [ストレージ システム構成の保存]）でバックアップしておきます。

タスク概要

インポート処理では、Eメール、SNMP、またはsyslogのいずれかのアラートを選択することができます。

インポートされる設定は次のとおりです。

- **Eメール アラート**
  メール サーバーのアドレスとアラート受信者のEメール アドレス。
- **syslogアラート**
  syslogサーバーのアドレスとUDPポート。
- **SNMPアラート**
  SNMPサーバーのコミュニティ名とIPアドレス。

手順

1. [管理]ページで、**[設定のインポート]** をクリックします。

   設定のインポート ウィザードが開きます。

2. [設定の選択]ダイアログ ボックスで、**[E メール アラート]**、**[SNMP アラート]**、または **[syslog アラート]** を選択し、**[次へ]** をクリックします。

   ソース アレイを選択するためのダイアログ ボックスが表示されます。

3. [ソースの選択]ダイアログ ボックスで、設定のインポート元のアレイを選択し、**[次へ]** をクリックします。
4. [ターゲットの選択]ダイアログ　ボックスで、新しい設定をインポートするアレイを1つ以上選択します。

   Unified　Managerが通信できないアレイ（オフラインのアレイや、証明書、パスワード、ネットワークに問題があるアレイなど）はこのダイアログ　ボックスに表示されません。

5. **[完了]** をクリックします。

   [処理]ページにインポート処理の結果が表示されます。処理に失敗した場合は、その行をクリックすると詳細を確認できます。

結果

Eメール、SNMP、またはsyslogを使用して管理者にアラートを送信するようにターゲット ストレージ システムが設定されます。

## AutoSupport設定のインポート

ストレージ システムから別のストレージ システムにAutoSupport設定をインポートできます。この方法でバッチ処理すると、ネットワークの複数のアレイを設定する場合に時間を短縮できます。

開始する前に

- ソースとして使用するストレージ システムのAutoSupport設定をSystem Manager（[サポート] > [

サポート センター]）で設定しておきます。

- ターゲット ストレージ システムの既存の設定をSystem Manager（[設定] > [システム] > [ストレージ システム構成の保存]）でバックアップしておきます。

タスク概要

インポートされる設定には、個別の機能（Basic　AutoSupport）、メンテナンス期間、配信方法、およびディスパッチ スケジュールが含まれます。ただし、Basic Autosupportのみサポート対象です。

手順

1. [管理]ページで、**[設定のインポート]** をクリックします。

   設定のインポート ウィザードが開きます。

2. [設定の選択]ダイアログ ボックスで、**[AutoSupport]** を選択し、**[次へ]** をクリックします。

   ソース アレイを選択するためのダイアログ ボックスが表示されます。

3. [ソースの選択]ダイアログで、設定のインポート元のアレイを選択し、**[次へ]** をクリックします。
4. [ターゲットの選択]ダイアログ　ボックスで、新しい設定をインポートするアレイを1つ以上選択します。

   Unified　Managerが通信できないアレイ（オフラインのアレイや、証明書、パスワード、ネットワークに問題があるアレイなど）はこのダイアログ　ボックスに表示されません。

5. **[完了]** をクリックします。

   [処理]ページにインポート処理の結果が表示されます。処理に失敗した場合は、その行をクリックすると詳細を確認できます。

結果

ターゲット ストレージ システムのAutoSupport設定がソース アレイと同じに設定されます。

## ディレクトリー サービス設定のインポート

ストレージ システムから別のストレージ システムにディレクトリー サービス設定をインポートできます。この方法でバッチ処理すると、ネットワークの複数のアレイを設定する場合に時間を短縮できます。

開始する前に

- ソースとして使用するストレージ システムのディレクトリー サービス設定をSystem Manager（[設定] > [アクセス管理]）で設定しておきます。
- ターゲット ストレージ システムの既存の設定をSystem Manager（[設定] > [システム] > [ストレージ システム構成の保存]）でバックアップしておきます。

タスク概要

インポートされる設定には、LDAP（Lightweight Directory Access Protocol）サーバーのドメイン名とURL、およびLDAPサーバーのユーザー グループとストレージ システムの定義済みロールとのマッピングが含まれます。

手順

1. [管理]ページで、**[設定のインポート]** をクリックします。

   設定のインポート ウィザードが開きます。

2. [設定の選択]ダイアログ ボックスで、**[ディレクトリ サービス]** を選択し、**[次へ]** をクリックします。

   ソース アレイを選択するためのダイアログ ボックスが表示されます。

3. [ソースの選択]ダイアログで、設定のインポート元のアレイを選択し、**[次へ]** をクリックします。
4. [ターゲットの選択]ダイアログ ボックスで、新しい設定をインポートするアレイを1つ以上選択します。

   Unified Managerが通信できないアレイ（オフラインのアレイや、証明書、パスワード、ネットワークに問題があるアレイなど）はこのダイアログ ボックスに表示されません。

5. **[完了]** をクリックします。

   [処理]ページにインポート処理の結果が表示されます。処理に失敗した場合は、その行をクリックすると詳細を確認できます。

**結果**

ターゲット ストレージ システムのディレクトリー サービスがソース アレイと同じに設定されます。

## システム設定のインポート

ストレージ システムから別のストレージ システムにシステム設定をインポートできます。この方法でバッチ処理すると、ネットワークの複数のアレイを設定する場合に時間を短縮できます。

開始する前に

- ソースとして使用するストレージ システムのシステム設定をSystem Managerで設定しておきます。
- ターゲット ストレージ システムの既存の設定をSystem Manager（[設定] > [システム] > [ストレージ システム構成の保存]）でバックアップしておきます。

タスク概要

インポートされる設定には、ボリュームのメディア スキャン設定、コントローラーのSSD設定、および自

動ロード バランシングが含まれます（ホスト接続レポートは含まれません）。

手順

1. [管理]ページで、**[設定のインポート]** をクリックします。

   設定のインポート ウィザードが開きます。

2. [設定の選択]ダイアログ ボックスで、**[システム]** を選択し、**[次へ]** をクリックします。

   ソース アレイを選択するためのダイアログ ボックスが表示されます。

3. [ソースの選択]ダイアログで、設定のインポート元のアレイを選択し、**[次へ]** をクリックします。
4. [ターゲットの選択]ダイアログ　ボックスで、新しい設定をインポートするアレイを1つ以上選択します。

   Unified　Managerが通信できないアレイ（オフラインのアレイや、証明書、パスワード、ネットワークに問題があるアレイなど）はこのダイアログ　ボックスに表示されません。

5. **[完了]** をクリックします。

   [処理]ページにインポート処理の結果が表示されます。処理に失敗した場合は、その行をクリックすると詳細を確認できます。

結果

ターゲット ストレージ システムのシステム設定がソース アレイと同じに設定されます。

## ストレージ構成のインポート

ストレージ　システムから別のストレージ　システムにストレージ構成をインポートできます。この方法でバッチ処理すると、ネットワークの複数のアレイを設定する場合に時間を短縮できます。

開始する前に

- ソースとして使用するストレージ システムのストレージをSANtricity System Managerで設定しておきます。
- ターゲット ストレージ システムの既存の設定をSystem Manager（[設定] > [システム] > [ストレージ システム構成の保存]）でバックアップしておきます。
- ソースとターゲットのアレイが次の要件を満たしている必要があります。
  - コントローラーが配置されているシェルフが同一である。
  - シェルフIDが同一である。
  - 拡張シェルフの同一のスロットに同じドライブ タイプが搭載されている。
  - RBODエンクロージャ タイプが同一である。

- HICが、ホストのData Assurance機能を含めて同一である。
- ターゲット アレイのステータスが「最適」である。
- ターゲット アレイのボリューム容量がソース アレイよりも大きい。

- 次の制限事項に留意してください。
  - ソース アレイのディスク プールのボリュームが64TB以上の場合、ターゲットでインポート プロセスを実行できない。
  - シン ボリュームはインポート プロセスに含まれない。

タスク概要

インポートされる設定には、設定済みのボリューム（リポジトリ ボリュームでないシック ボリュームのみ）、ボリューム グループ、プール、およびホット スペア ドライブの割り当てが含まれます。

手順

1. [管理]ページで、**[設定のインポート]** をクリックします。

   設定のインポート ウィザードが開きます。

2. [設定の選択]ダイアログ ボックスで、**[ストレージ構成]** を選択し、**[次へ]** をクリックします。

   ソース アレイを選択するためのダイアログ ボックスが表示されます。

3. [ソースの選択]ダイアログで、設定のインポート元のアレイを選択し、**[次へ]** をクリックします。
4. [ターゲットの選択]ダイアログ ボックスで、新しい設定をインポートするアレイを1つ以上選択します。

   Unified Managerが通信できないアレイ（オフラインのアレイや、証明書、パスワード、ネットワークに問題があるアレイなど）はこのダイアログ ボックスに表示されません。

5. **[完了]** をクリックします。

   [処理]ページにインポート処理の結果が表示されます。処理に失敗した場合は、その行をクリックすると詳細を確認できます。

結果

ターゲット ストレージ システムのストレージ構成がソース アレイと同じに設定されます。

# FAQ

## どの設定がインポートされますか？

設定のインポート機能は、1つのストレージ システムから複数のストレージ システムに設定をロードするバッチ処理です。この処理でインポートされる設定は、System

Managerでソース ストレージ
システムがどのように設定されているかによって異なります。

複数のストレージ システムにインポートできる設定は次のとおりです。

- **Eメール アラート**
  メール サーバーのアドレスとアラート受信者のEメール アドレスが含まれます。
- **syslogアラート**
  syslogサーバーのアドレスとUDPポートが含まれます。
- **SNMPアラート**
  SNMPサーバーのコミュニティ名とIPアドレスが含まれます。
- **AutoSupport**
  個別の機能（Basic AutoSupport、AutoSupport OnDemand、Remote Diagnostics）、メンテナンス期間、配信方法、およびディスパッチ スケジュールが含まれます。ただし、Basic Autosupportのみサポート対象とする。
- **ディレクトリー サービス**
  LDAP（Lightweight Directory Access Protocol）サーバーのドメイン名とURL、およびLDAPサーバーのユーザー グループとストレージ システムの定義済みロールとのマッピングが含まれます。
- **ストレージ構成**
  ボリューム（リポジトリ ボリュームでないシック ボリュームのみ）、ボリューム グループ、プール、およびホット スペア ドライブの割り当てが含まれます。
- **システム設定**
  ボリュームのメディア スキャン設定、コントローラーのSSDキャッシュ、および自動ロード バランシングが含まれます（ホスト接続レポートは含まれません）。

### ストレージ システムが一部表示されないのはなぜですか？

設定のインポート処理の際、ターゲットの選択ダイアログ ボックスに一部のストレージ システムが表示されないことがあります。

ストレージ システムが表示されない理由は次のとおりです。

- ストレージ システムがオフラインになっている。
- システムがアレイと通信できない（アレイに証明書、パスワード、ネットワークの問題がある場合など）。

# アレイ グループ

## グループの概要

[グループの管理]ページでストレージ
システムのグループを作成すると管理が簡単になります。

### アレイ グループとは何ですか？

一連のストレージ　システムを1つのグループにまとめて物理インフラや仮想インフラを管理することができます。ストレージ システムをグループ化すると、ジョブの監視やレポートが簡単になります。

グループには次の2種類があります。

- **すべて**
  デフォルトのグループで、組織で検出されたすべてのストレージ　システムが含まれます。[すべて]グループにはメイン ビューからアクセスできます。
- **ユーザーが作成したグループ**
  ユーザーが手動で選択して追加したストレージ　システムが含まれます。ユーザーが作成したグループにはメイン ビューからアクセスできます。

### グループを設定するにはどうすればよいですか？

[グループの管理]ページで、グループを作成し、そのグループにアレイを追加できます。

詳細情報：

- ストレージ システム グループの設定

# ストレージ システム グループの設定

ストレージ グループを作成し、そのグループにストレージ システムを追加します。

グループの設定は2つの手順で構成されます。

### 手順 1：グループを作成する

最初にグループを作成します。ストレージ グループでは、ボリュームを構成するストレージをどのドライブから提供するかを定義します。

手順

1. [管理]ページで、[グループの管理] > [ストレージ システム グループの作成]を選択します。
2. **[名前]** フィールドに新しいグループの名前を入力します。
3. 新しいグループに追加するストレージ システムを選択します。
4. **[作成]** をクリックします。

### 手順 2：グループへのストレージ システムの追加

ユーザーが作成したグループにストレージ システムを追加することができます。

手順

1. メイン ビューで **[管理]** を選択し、ストレージ システムを追加するグループを選択します。
2. [グループの管理] > [グループへのストレージ システムの追加]を選択します。
3. グループに追加するストレージ システムを選択します。
4. **[追加]** をクリックします。

## グループからのストレージ システムの削除

管理対象のストレージ システムを特定のストレージ グループで管理する必要がなくなった場合は、それらのストレージ システムをグループから削除することができます。

タスク概要

グループからストレージ システムを削除しても、ストレージ システム自体やそのデータには影響はありません。ストレージ システムをSystem Managerで管理している場合は、引き続きブラウザーを使用して管理できます。ストレージ システムをグループから誤って削除した場合は、再度追加することができます。

手順

1. [管理]ページで、[グループの管理] > [グループからのストレージ システムの削除]を選択します。
2. 削除するストレージ システムが含まれているグループをドロップダウンから選択し、グループから削除する各ストレージ システムの横にあるチェックボックスをクリックします。
3. **[削除]** をクリックします。

## ストレージ システム グループの削除

不要になった1つ以上のストレージ システム グループを削除することができます。

タスク概要

この処理で削除されるのは、ストレージ システム グループだけです。削除したグループに関連付けられているストレージ システムには、[すべて管理]ビューや関連付けられている他のグループから引き続きアクセスできます。

手順

1. [管理]ページで、[グループの管理] > [ストレージ システム グループの削除]を選択します。
2. 削除するストレージ システム グループを1つ以上選択します。

3. **[削除]** をクリックします。

# ストレージ システム グループの名前の変更

現在の名前が適切でない場合は、ストレージ システム グループの名前を変更することができます。

タスク概要

次のガイドラインに注意してください。

- 名前には、アルファベット、数字、アンダースコア（_）、ハイフン（-）、シャープ記号（#）を使用できます。それ以外の文字を使用しようとすると、エラー メッセージが表示され、別の名前を入力するように求められます。
- 名前は30文字以内で指定します。名前の先頭と末尾のスペースは削除されます。
- すぐに思い出せるような、わかりやすい一意の名前を使用します。
- わかりにくい名前は使用しないでください。

手順

1. メイン ビューで **[管理]** を選択し、名前を変更するストレージ システム グループを選択します。
2. [グループの管理] > [ストレージ システム グループの名前変更]を選択します。
3. **[グループ名]** フィールドにグループの新しい名前を入力します。
4. **[名前変更]** をクリックします。

# アップグレード

## アップグレード センターの概要

アップグレード センターでは、複数のストレージ システムのSANtricity OSソフトウェアとNVSRAMのアップグレードを管理できます。

### アップグレードはどのように行いますか？

最新のOSソフトウェアをダウンロードしてから、アレイをアップグレードします。

#### アップグレード ワークフロー

ソフトウェアのアップグレードを実行する手順の大まかなワークフローを以下に記載します。

1. サポート サイトから最新のSANtricity OSソフトウェア ファイルをダウンロードします。管理ホスト システム（ブラウザーでUnified Managerにアクセスするホスト）にファイルを保存し、ファイルを解凍します。

2. Unified Managerで、SANtricity OSソフトウェア ファイルとNVSRAMファイルをリポジトリ（ファイルが格納されているWeb Services Proxyサーバーの領域）にロードします。[アップグレード センター] > [SANtricity OS ソフトウェアのアップグレード]または[アップグレード センター] > [ソフトウェア リポジトリの管理]からファイルを追加できます。
3. リポジトリにファイルをロードしたら、そのファイルを選択してアップグレードに使用できます。[SANtricity OS ソフトウェアのアップグレード]ページ（[アップグレード センター] > [SANtricity OS ソフトウェアのアップグレード]）で、SANtricity OSソフトウェア ファイルとNVSRAMファイルを選択します。ソフトウェア ファイルを選択すると、互換性があるストレージ システムのリストがこのページに表示されます。新しいソフトウェアにアップグレードするストレージ システムをリストから選択します（互換性がないアレイは選択できません）。
4. ソフトウェアの転送とアクティブ化をすぐに開始するか、ファイルをステージングしてあとでアクティブ化するかを選択できます。アップグレード プロセスを実行すると、Unified Managerで次の処理が実行されます。
   a. ストレージ システムの健全性チェックが実行され、アップグレードの完了の妨げとなる状況がないかどうかが確認されます。健全性チェックでいずれかのアレイに問題が見つかった場合、そのアレイをスキップして他のアレイのアップグレードを続行するか、プロセス全体を中止して該当するアレイのトラブルシューティングを行うことができます。
   b. 各コントローラーにアップグレード ファイルが転送されます。
   c. コントローラーが一度に1台ずつリブートされ、新しいSANtricity OSソフトウェアがアクティブ化されます。アクティブ化では、既存のSANtricity OSファイルが新しいファイルに置き換えられます。

   ソフトウェアをあとでアクティブ化するように指定することもできます。

**即時アップグレードと段階的アップグレード**

アップグレードはただちにアクティブ化することも、ステージングしてあとでアクティブ化することもできます。あとでアクティブ化する理由は次のとおりです。

- **時間帯**
  ソフトウェアのアクティブ化には時間がかかることがあるため、I/O負荷の低い時間帯に実行できます。I/O負荷とキャッシュ サイズに応じて、コントローラーのアップグレードには通常15～25分かかります。アクティブ化の際にはコントローラーがリブートしてフェイルオーバーするため、アップグレードが完了するまではパフォーマンスが通常よりも低下する可能性があります。
- **パッケージのタイプ**
  新しいソフトウェアとファームウェアを1つのストレージ システムでテストしてから、他のストレージ システムでファイルをアップグレードできます。

ステージング済みソフトウェアをアクティブ化するには、[サポート] > [アップグレード センター]に移動し、[SANtricity OS コントローラ ソフトウェアのアップグレード]で **[アクティブ化]** をクリックします。

**健全性チェック**

健全性チェックはアップグレード プロセスの一環として実行されますが、開始前に別途実行することもできます（[アップグレード センター] > [アップグレード前の健全性チェック]を選択）。

健全性チェックでは、ストレージ システムのすべてのコンポーネントについて、アップグレードを実行できる状態であるかがチェックされます。次の状況に該当する場合、アップグレードを実行できないことがあります。

- 割り当てドライブに障害が発生している
- ホット スペアを使用中である
- 不完全なボリューム グループがある
- 同時に実行できない処理を実行中である
- ボリュームが見つからない
- コントローラーのステータスが最適でない
- イベント ログのイベント数が多すぎる
- 構成データベースの検証にエラーがある
- ドライブのDACstoreのバージョンが古い

## アップグレードするときは、どのような点に注意する必要がありますか？

複数のストレージ システムをアップグレードする場合に、計画段階で確認が必要な考慮事項を以下に記載します。

**現在のバージョン**

検出された各ストレージ システムについて、Unified Managerの[管理]ページでSANtricity OSの現在のバージョンを確認できます。バージョンは、[SANtricity OSソフトウェア]列に表示されます。各行のSANtricity OSのバージョンをクリックするとポップアップ ダイアログ ボックスが表示され、コントローラーのファームウェアとNVSRAMの情報を確認できます。

**アップグレードが必要な他のコンポーネント**

アップグレード プロセスの一環として、ホストがコントローラーと正しく連携するように、ホストのマルチパス / フェイルオーバー ドライバーやHBAドライバーのアップグレードも必要になることがあります。

手順については、使用するオペレーティング システムに対応したエクスプレス ガイドを参照してください。エクスプレス ガイドは、ETERNUS AB/HBシリーズ 富士通マニュアルサイト [https://www.fujitsu.com/jp/products/computing/storage/manual/]から入手できます。

**コントローラー**

ストレージ システムにコントローラーが2台あり、マルチパス ドライバーがインストールされている場合

は、アップグレードの実行中もストレージ
システムでI/Oの処理を継続できます。アップグレードのプロセスは次のとおりです。

1. コントローラーAのすべてのLUNがコントローラーBにフェイルオーバーされます。
2. コントローラーAでアップグレードが実行されます。
3. コントローラーAにLUNが戻され、コントローラーBのLUNもすべて移されます。
4. コントローラーBでアップグレードが実行されます。

アップグレードの完了後、所有権のある正しいコントローラーにボリュームが配置されるように、コントローラー間で手動でのボリュームの再配置が必要になることがあります。

# ソフトウェアとファームウェアのアップグレード

## アップグレード前の健全性チェックの実行

健全性チェックは、アップグレード プロセスの一環として実行されますが、開始前に別途実行することもできます。健全性チェックでは、ストレージ システムのコンポーネントについて、アップグレードを実行できる状態であるかがチェックされます。

手順

1. メイン ビューから **[管理]** を選択し、[アップグレード センター] > [アップグレード前の健全性チェック]を選択します。

   [アップグレード前の健全性チェック]ダイアログ ボックスが開き、検出されたすべてのストレージ システムが表示されます。

2. 必要に応じて、ストレージ　システムのリストをフィルターまたはソートして、状態が現在「最適」でないすべてのシステムを確認します。
3. 健全性チェックを実行するストレージ システムのチェック ボックスを選択します。
4. **[開始]** をクリックします。

   健全性チェックの実行中、ダイアログ ボックスに進捗状況が表示されます。

5. 健全性チェックが完了したら、各行の右側にある省略記号（…）をクリックして、詳細情報を表示したり他のタスクを実行したりできます。

> 健全性チェックでいずれかのアレイに問題が見つかった場合、そのアレイをスキップして他のアレイのアップグレードを続行するか、プロセス全体を中止して該当するアレイのトラブルシューティングを行うことができます。

## SANtricity OSのアップグレード

ストレージ　システムのソフトウェアとNVSRAMをアップグレードして、最新の機能

とバグ修正をすべて適用します。コントローラーNVSRAMは、コントローラーのデフォルト設定を指定するコントローラー ファイルです。

開始する前に

- 最新のSANtricity OSファイルは、SANtricity Web Services ProxyとUnified Managerが実行されているホスト システムに格納しておきます。
- ソフトウェアのアップグレードをすぐにアクティブ化するか、あとでアクティブ化するかを決めておきます。

  あとでアクティブ化する理由は次のとおりです。

  - **時間帯**
    ソフトウェアのアクティブ化には時間がかかることがあるため、I/O負荷の低い時間帯に実行できます。アクティブ化の際にはコントローラーがフェイルオーバーするため、アップグレードが完了するまではパフォーマンスが通常よりも低下する可能性があります。
  - **パッケージのタイプ**
    新しいOSソフトウェアを1つのストレージ システムでテストしてから、他のストレージ システムでファイルをアップグレードできます。

タスク概要

データ損失のリスク、ストレージ システムの損傷のリスク
アップグレードの実行中にストレージ システムに対する変更を行わないでください。ストレージ システムへの電源を維持してください。

手順

1. マルチパス　ドライバーを使用していない場合は、アプリケーション　エラーを防ぐためにストレージ システムに対するI/Oアクティビティを停止します。マルチパス　ドライバーがインストールされている場合は、I/Oアクティビティを停止する必要はありません。
2. メイン ビューから **[管理]** を選択し、アップグレードする1つまたは複数のストレージ システムを選択します。
3. [アップグレード センター] > [SANtricity OS ソフトウェアのアップグレード]を選択します。

   [SANtricity OSソフトウェアのアップグレード]ページが表示されます。
4. 富士通サポートサイトよりローカル マシンに最新のSANtricity OSソフトウェア パッケージをダウンロードします。

   バージョン8.60以降のデジタル署名されたファームウェアが必要です。署名のないファームウェアをダウンロードしようとすると、エラーが表示されてダウンロードが中止されます。
5. コントローラーのアップグレードに使用するOSソフトウェア　ファイルとNVSRAMファイルを選択し

ます。

a. **[SANtricity OS ソフトウェア ファイルを選択]** ドロップダウンで、ローカル マシンにダウンロードしたOSファイルを選択します。

使用可能なファイルが複数ある場合は、日付が新しい順にファイルがソートされます。

ソフトウェア リポジトリには、Web Services Proxyに関連付けられているすべてのソフトウェア　ファイルが表示されます。使用するファイルが表示されない場合は、**[ソフトウェア リポジトリに新しいファイルを追加]** リンクをクリックし、追加するOSファイルが格納されている場所を参照できます。

b. **[NVSRAM　ファイルを選択]**　ドロップダウンで、使用するコントローラー　ファイルを選択します。

ファイルが複数ある場合は、日付が新しい順にファイルがソートされます。

6. [互換性があるストレージ　システム]の表で、選択したOSソフトウェア　ファイルと互換性があるストレージ システムを確認し、アップグレードするアレイを選択します。
   - [互換性があるストレージ　システム]の表では、[管理]ビューで選択したストレージ　システムのうち、選択したファームウェア ファイルと互換性があるアレイがデフォルトで選択されます。
   - [互換性があるストレージ　システム]の表では、選択したファームウェア　ファイルで更新できないストレージ システムについては選択できない状態になり、ステータスが **[互換性なし]** と表示されます。
7. ソフトウェア　ファイルをアクティブ化せずにストレージ　システムに転送する場合は、**[OS　ソフトウェアをストレージ　システムに転送してステージング済みとマークし、あとでアクティブ化します]** チェック ボックスを選択します。
8. **[開始]** をクリックします。
9. すぐにアクティブ化するかあとでアクティブ化するかに応じて、次のいずれかを実行します。
   - アップグレード対象として選択したアレイに推奨バージョンのOSソフトウェアを転送する場合は、確認のために「**転送**」と入力し、**[転送]** をクリックします。

     転送したソフトウェアをアクティブ化するには、[アップグレード　センター] > [ステージング済み OS ソフトウェアのアクティブ化]を選択します。
   - アップグレード対象として選択したアレイに推奨バージョンのOSソフトウェアを転送してアクティブ化する場合は、確認のために「**アップグレード**」と入力し、**[アップグレード]**　をクリックします。

     アップグレード対象として選択した各ストレージ　システムにソフトウェア　ファイルが転送され、ストレージ システムがリブートされてファイルがアクティブ化されます。

アップグレード処理では、次の処理が実行されます。

- アップグレード　プロセスの一環として、アップグレード前の健全性チェックが実行されます。ア

ップグレード前の健全性チェックでは、ストレージ
システムのすべてのコンポーネントについて、アップグレードを実行できる状態であるかがチェックされます。

- いずれかの健全性チェックでストレージ　システムに問題が見つかった場合、アップグレードが停止します。省略記号（…）をクリックして **[ログの保存]** を選択すると、エラーを確認することができます。健全性チェックのエラーを無視し、**[続行]**　をクリックしてアップグレードを続行することもできます。
- アップグレード前の健全性チェックのあとに、アップグレード処理をキャンセルすることができます。

10. **オプション：**　アップグレードの完了後、省略記号（…）をクリックして　**[ログの保存]**　を選択すると、特定のストレージ システムについてのアップグレード状況のリストを確認できます。

    ブラウザーのDownloadsフォルダーに、`upgrade_log-<date>.json`　という名前でファイルが保存されます。

## ステージング済みOSソフトウェアのアクティブ化

ソフトウェア ファイルはただちにアクティブ化することも、都合のいいタイミングでアクティブ化することもできます。ここでは、ソフトウェア ファイルをあとでアクティブ化するように選択した場合の手順を示します。

タスク概要

ファームウェア ファイルは、アクティブ化せずに転送できます。あとでアクティブ化する理由は次のとおりです。

- **時間帯**
  ソフトウェアのアクティブ化には時間がかかることがあるため、I/O負荷の低い時間帯に実行できます。アクティブ化の際にはコントローラーがリブートしてフェイルオーバーするため、アップグレードが完了するまではパフォーマンスが通常よりも低下する可能性があります。
- **パッケージのタイプ**
  新しいソフトウェアとファームウェアを1つのストレージ　システムでテストしてから、他のストレージ システムでファイルをアップグレードできます。

> 一度開始したアクティブ化プロセスは停止できません。

手順

1. メイン　ビューから　**[管理]**　を選択します。必要に応じて、ページ上部の[ステータス]列をクリックしてソートし、ステータスが「OS　ソフトウェア　アップグレード完了（アクティブ化待ち）」であるすべてのストレージ システムを確認します。
2. ソフトウェアをアクティブ化する1つまたは複数のストレージ システムを選択し、[アップグレード センター] > [ステージング済み OS ソフトウェアのアクティブ化]を選択します。

   アップグレード処理では、次の処理が実行されます。

- アクティブ化プロセスの一環として、アップグレード前の健全性チェックが実行されます。アップグレード前の健全性チェックでは、ストレージ　システムのすべてのコンポーネントについて、アクティブ化を実行できる状態であるかがチェックされます。
- いずれかの健全性チェックでストレージ　システムに問題が見つかった場合、アクティブ化が停止します。省略記号（…）をクリックして **[ログの保存]** を選択すると、エラーを確認することができます。健全性チェックのエラーを無視し、**[続行]**　をクリックしてアクティブ化を続行することもできます。
- アップグレード前の健全性チェックのあとに、アクティブ化処理をキャンセルすることができます。
  アップグレード前の健全性チェックが正常に完了すると、アクティブ化が実行されます。アクティブ化にかかる時間は、ストレージ　システムの構成とアクティブ化しているコンポーネントによって異なります。

3. **オプション：** アクティブ化の完了後、省略記号（…）をクリックして **[ログの保存]** を選択すると、特定のストレージ システムについてのアクティブ化状況のリストを確認できます。

   ブラウザーのDownloadsフォルダーに、`activate_log-<date>.json` という名前でファイルが保存されます。

## ソフトウェア リポジトリの管理

ソフトウェア リポジトリには、Web Services Proxyに関連付けられているすべてのソフトウェア ファイルが表示されます。

使用するファイルが表示されない場合は、[ソフトウェア リポジトリの管理]オプションを使用して、Web Services ProxyとUnified Managerが実行されているホスト システムにSANtricity OSファイルをインポートできます。ソフトウェア リポジトリにあるSANtricity OSファイルを削除することもできます。

開始する前に

SANtricity OSファイルを追加する場合は、ローカル システム上にOSファイルを用意しておきます。

手順

1. メイン ビューから **[管理]** を選択し、[アップグレード センター] > [ソフトウェア リポジトリの管理]を選択します。

   [ソフトウェア リポジトリの管理]ダイアログ ボックスが表示されます。

2. 次のいずれかを実行します。

| オプション | 手順 |
| --- | --- |
| インポート | a. **[インポート]** をクリックします。<br>b. **[参照]** をクリックし、追加するOSファイルの場所に移動します。<br>OSファイルの名前は `N2800-830000-000.dlp` などです。<br>c. 追加するOSファイルを選択し、**[インポート]** をクリックします。 |
| 削除 | a. ソフトウェア リポジトリから削除するOSファイルを選択します。<br>b. **[削除]** をクリックします。 |

結果

インポートを選択した場合は、ファイルがアップロードされて検証されます。削除を選択した場合は、ファイルがソフトウェア リポジトリから削除されます。

### ステージング済みOSソフトウェアのクリア

保留中のバージョンがあとで誤ってアクティブ化されないように、ステージング済みのOSソフトウェアを削除することができます。ステージング済みOSソフトウェアを削除しても、ストレージ システムで実行されている現在のバージョンには影響しません。

手順

1. メイン ビューから **[管理]** を選択し、[アップグレード センター] > [ステージング済み OS ソフトウェアのクリア]を選択します。

   [ステージング済みOSソフトウェアのクリア]ダイアログ ボックスが開き、保留中のソフトウェアまたはNVSRAMがあるストレージ システムがすべて検出されて表示されます。

2. 必要に応じて、ストレージ　システムのリストをフィルターまたはソートして、ソフトウェアがステージング済みのすべてのシステムを確認します。
3. 保留中のソフトウェアをクリアするストレージ システムのチェック ボックスを選択します。
4. **[クリア]** をクリックします。

   処理のステータスがダイアログ ボックスに表示されます。

# ミラーリング

## ミラーリングの概要

ミラーリング機能を使用して、ローカル ストレージ システムとリモート ストレージ

システムの間でデータを非同期または同期的にレプリケートします。

この機能はAB6100またはAB3100ストレージ　　システムでは使用できません。また、HB1000 seriesは同期ミラーリングを使用できません。

### ミラーリングとは何ですか？

SANtricityアプリケーションには2種類のミラーリング（非同期と同期）があります。非同期ミラーリングでは、データ ボリュームをオンデマンドで、またはスケジュールに基づいてコピーします。これにより、データの破損や損失が原因で発生するダウンタイムを回避または最小限に抑えることができます。同期ミラーリングでは、データ ボリュームをリアルタイムでレプリケートして、継続的な可用性を確保します。

詳細情報：

- ミラーリングの仕組み
- ミラーリングに関する用語

### ミラーリングを設定するにはどうすればよいですか？

Unified Managerで非同期ミラーリングまたは同期ミラーリングを設定し、System Managerを使用して同期を管理します。

詳細情報：

- ミラーリングの設定ワークフロー
- ミラーリングを使用するための要件
- 非同期ミラー ペアの作成
- 同期ミラー ペアの作成

## 概念

### ミラーリングの仕組み

Unified　Managerには、SANtricityのミラーリング機能の設定オプションが用意されており、管理者は2つのストレージ　システム間でデータをレプリケートすることでデータを保護できます。

この機能はAB6100またはAB3100ストレージ　　システムでは使用できません。また、HB1000 seriesは同期ミラーリングを使用できません。

#### ミラーリングのタイプ

SANtricityアプリケーションには2種類のミラーリング（非同期と同期）があります。

非同期ミラーリングでは、データ
ボリュームをオンデマンドで、またはスケジュールに基づいてコピーします。これにより、データの破損や損失が原因で発生するダウンタイムを回避または最小限に抑えることができます。非同期ミラーリングは、特定の時点におけるプライマリー　ボリュームの状態をキャプチャーし、前回のイメージ　キャプチャー以降に変更されたデータのみをコピーします。プライマリー サイトはただちに更新でき、セカンダリー サイトは帯域幅に余裕があれば更新できます。情報はキャッシュされ、あとからネットワーク リソースが利用可能になったときに送信されます。このタイプのミラーリングは、バックアップやアーカイブなどの定期的なプロセスに最適です。

同期ミラーリングでは、データ ボリュームをリアルタイムでレプリケートして、継続的な可用性を確保します。目的は、2つのストレージ　システムのいずれかで災害が発生した場合に重要なデータのコピーを確保しておくことにより、データ損失ゼロの目標復旧時点（RPO）を達成することです。プライマリー ボリュームに書き込みが行われるたびにセカンダリー ボリュームにも書き込みが行われるため、どの時点においてもコピーは本番環境のデータと同一です。プライマリー　ボリュームで行われた変更でセカンダリー ボリュームが更新されるまで、ホストは書き込みが成功したという確認応答を受信しません。このタイプのミラーリングは、ディザスタ リカバリーなどのビジネス継続性の確保に最適です。

**ミラーリングのタイプの違い**

次の表は、2種類のミラーリングの主な違いを示しています。

| 属性 | 非同期 | 同期 |
|---|---|---|
| レプリケーション方法 | ポイントインタイム<br>ミラーリングはオンデマンドで、またはユーザー定義のスケジュールに従って自動的に行われます。 | 連続<br>ミラーリングは継続して自動的に実行され、ホストに書き込みがあるたびにデータがコピーされます。 |
| 距離 | 地理的に離れたアレイをサポートします。通常、この距離はネットワークとチャネル拡張テクノロジの機能によってのみ制限されます。 | アレイ間の距離は短い距離に制限されます。レイテンシおよびアプリケーション　パフォーマンスの要件を満たすために、通常はローカル　ストレージ　システムから約10km（6.2マイル）以内の距離にする必要があります。 |
| 通信手段 | iSCSIまたはFibre　Channelネットワーク。 | Fibre　Channelネットワークのみ。 |
| ボリューム タイプ | 標準またはシン。 | 標準のみ。 |

## ミラーリングの設定ワークフロー

Unified　Managerで非同期ミラーリングまたは同期ミラーリングを設定し、System Managerを使用して同期を管理します。

### 非同期ミラーリングのワークフロー

非同期ミラーリングのワークフローは次のとおりです。

1. Unified Managerで初期設定を実行します。
   a. データ転送元としてローカル ストレージ システムを選択します。
   b. ミラー整合性グループを作成するか、または既存のミラー整合性グループを選択します。ミラー整合性グループは、ローカル アレイのプライマリー ボリュームとリモート アレイのセカンダリー ボリュームのコンテナです。プライマリー ボリュームとセカンダリー ボリュームは「ミラー ペア」と呼ばれます。ミラー整合性グループを初めて作成する場合は、実行する同期方法（手動またはスケジュール）を指定します。
   c. ローカル ストレージ システムからプライマリー ボリュームを選択し、リザーブ容量を確認します。リザーブ容量は、コピー処理に使用される物理割り当て容量です。
   d. 転送先としてリモート ストレージ システムを選択し、セカンダリー ボリュームを選択して、リザーブ容量を確認します。
   e. プライマリー ボリュームからセカンダリー ボリュームへの初回のデータ転送を開始します。ボリューム サイズによっては、この初回転送に数時間かかることがあります。
2. 初期同期の進捗状況を確認します。
   a. Unified Managerで、ローカル アレイのSystem Managerを起動します。
   b. System Managerで、ミラーリング処理のステータスを確認します。ミラーリングが完了すると、ミラー ペアのステータスは「最適」になります。
3. 必要に応じて、System Managerで後続のデータ転送のスケジュールを再設定したり、手動で実行したりできます。新しいブロックと変更されたブロックだけがプライマリー ボリュームからセカンダリー ボリュームに転送されます。

非同期レプリケーションは定期的に行われるため、システムでは変更されたブロックを統合し、ネットワーク帯域幅を節約できます。書き込みスループットと書き込みレイテンシへの影響は最小限に抑えられます。

### 同期ミラーリングのワークフロー

同期ミラーリングのワークフローは次のとおりです。

1. Unified Managerで初期設定を実行します。
   a. データ転送元としてローカル ストレージ システムを選択します。
   b. ローカル ストレージ システムからプライマリー ボリュームを選択します。
   c. データ転送先としてリモート ストレージ システムを選択し、セカンダリー ボリュームを選択します。
   d. 同期と再同期の優先度を選択します。
   e. プライマリー ボリュームからセカンダリー ボリュームへの初回のデータ転送を開始します。ボリ

ューム サイズによっては、この初回転送に数時間かかることがあります。

2. 初期同期の進捗状況を確認します。
   a. Unified Managerで、ローカル アレイのSystem Managerを起動します。
   b. System Managerで、ミラーリング処理のステータスを確認します。ミラーリングが完了すると、ミラー ペアのステータスは「最適」になります。2つのアレイは、通常の処理を通じて同期状態が維持されます。新しいブロックと変更されたブロックだけがプライマリー ボリュームからセカンダリー ボリュームに転送されます。
3. 必要に応じて、System Managerで同期設定を変更できます。

同期レプリケーションは継続的に行われるため、2つのサイト間のレプリケーション リンクで十分な帯域幅を提供する必要があります。

## ミラーリングに関する用語

ストレージ システムに関連するミラーリングの用語を次に示します。

| 用語 | 説明 |
|---|---|
| ローカル ストレージ システム | ローカル ストレージ システムは、操作の対象となるストレージ システムです。 |
| ミラー整合性グループ | ミラー整合性グループは、1つ以上のミラー ペアのコンテナです。非同期ミラーリング処理では、ミラー整合性グループを作成する必要があります。グループ内のすべてのミラー ペアが同時に再同期されるため、一貫したリカバリー ポイントが維持されます。<br><br>同期ミラーリングではミラー整合性グループを使用しません。 |
| ミラー ペア | ミラー ペアは、プライマリー ボリュームとセカンダリー ボリュームの2つのボリュームで構成されます。<br><br>非同期ミラーリングでは、ミラー ペアは必ずミラー整合性グループに属します。書き込み処理はまずプライマリー ボリュームに対して実行され、その後セカンダリー ボリュームにレプリケートされます。ミラー整合性グループ内の各ミラー ペアには同じ同期設定が適用されます。 |
| プライマリー ボリューム | ミラー ペアのプライマリー ボリュームは、ミラーリングするソース ボリュームです。 |
| リモート ストレージ システム | 通常はリモート ストレージ システムがセカンダリー サイトで、ミラーリング構成においてデータのレプリカが格納されます。 |

| 用語 | 説明 |
| --- | --- |
| リザーブ容量 | リザーブ容量は、コピー サービス処理やストレージ オブジェクトに使用される物理割り当て容量です。ホストから直接読み取ることはできません。<br><br>ミラーリングの動作状態を維持するために必要な情報をコントローラーが永続的に保存できるようにするには、これらのボリュームが必要です。これらのボリュームには、差分ログやコピーオンライトデータなどの情報が格納されます。 |
| セカンダリー　ボリューム | ミラー ペアのセカンダリー ボリュームは通常はセカンダリー サイトに配置され、データのレプリカが格納されます。 |
| 同期 | 同期は、ローカル ストレージ システムとリモート ストレージ システムの間の初期同期で実行されます。また、通信が中断されてプライマリー　ボリュームとセカンダリー　ボリュームが同期されていない状態になったときにも実行されます。通信リンクが再確立されると、レプリケートされていないデータがセカンダリー ボリュームのストレージ システムに同期されます。 |

## ミラーリングを使用するための要件

ミラーリングを設定する場合は、次の要件に注意してください。

### Unified Manager

- Web Services Proxyサービスが実行されている必要があります。
- Unified ManagerがHTTPS接続経由でローカル ホストで実行されている必要があります。
- Unified　Managerにストレージ　システムの有効なSSL証明書が表示されている必要があります。証明書については、Unified　Managerの[証明書] > [証明書管理]で、自己署名証明書を受け入れるか独自のセキュリティ証明書をインストールできます。

### ストレージ システム

AB6100またはAB3100ストレージ　　システムではミラーリングを使用できません。また、HB1000 seriesは同期ミラーリングを使用できません。

- 2つのストレージ システムが必要です。
- 各ストレージ システムに2台のコントローラーが必要です。
- Unified Managerで2つのストレージ システムが検出されている必要があります。
- プライマリー アレイとセカンダリー アレイ内の各コントローラーにイーサネット管理ポートが設定されていて、各コントローラーがネットワークに接続されている必要があります。
- ストレージ　システムに必要なファームウェアの最小バージョンは7.84です（ストレージ　システムごとに異なるバージョンのOSを実行できます）。
- ローカルとリモートのストレージ システムのパスワードを確認しておく必要があります。

- リモート ストレージ システムにセカンダリー ボリュームを作成するための十分な空き容量（ミラーリングするプライマリー ボリュームと同等以上）が必要です。
- 非同期ミラーリングはFibre Channel（FC）またはiSCSIホスト ポートを備えたコントローラーでサポートされますが、同期ミラーリングはFCホスト ポートを備えたコントローラーでのみサポートされます。

**接続要件**

FCインターフェイスでのミラーリング（非同期または同期）には次の要件が適用されます。

- ストレージ システムの各コントローラーでは、**最も番号が大きいFCホスト ポート** がミラーリング処理の専用ポートとして使用されます。
- ベースのFCポートとホスト インターフェイス カード（HIC）のFCポートの両方があるコントローラーでは、HICの **最も番号が大きいポート** が使用されます。専用ポートにログオンしたホストはログアウトされ、ホスト ログイン要求は許可されません。このポートに対しては、ミラーリング処理の対象となるコントローラーからのI/O要求のみが許可されます。
- 専用のミラーリング ポートは、ディレクトリー サービスとネーム サービスのインターフェイスをサポートするFCファブリック環境に接続されている必要があります。特に、FC-ALおよびポイントツーポイントはミラー関係が確立されたコントローラー間の接続オプションとしてサポートされないことに注意してください。

iSCSIインターフェイスでのミラーリング（非同期のみ）には次の要件が適用されます。

- FCとは異なり、iSCSIでは専用のポートを必要としません。iSCSI環境で非同期ミラーリングを使用する場合、ストレージ システムのどのフロントエンドiSCSIポートも非同期ミラーリング専用にする必要はありません。これらのポートは、非同期ミラーリングのトラフィックとホスト / アレイ間のI/O接続で共有されます。
- コントローラーはリモート ストレージ システムのリストを管理しており、iSCSIイニシエータはこのリストを使用してセッションの確立を試みます。iSCSI接続が確立されると、接続に最初に成功したポートがリモート ストレージ システムとの以降のすべての通信に使用されます。通信に失敗すると、使用可能な残りのポートを使用して新しいセッションの確立が試行されます。
- iSCSIポートはアレイレベルでポート単位で設定されます。設定の通知やデータ転送などのコントローラー間の通信には、次の設定を含むグローバル設定が使用されます。
  - VLAN：ローカルとリモートのシステムが通信するためには、両方のシステムでVLAN設定を同じにする必要があります。
  - iSCSIリスン ポート
  - ジャンボ フレーム
  - イーサネットの優先順位

コントローラー間のiSCSI通信には、管理イーサネット ポートではなくホスト接続ポートを使用する必要があります。

**ミラー ボリュームの候補**

- ミラー ペアのプライマリー ボリュームとセカンダリー ボリュームでは、RAIDレベル、キャッシング パラメーター、およびセグメント サイズが異なる場合があります。
- セカンダリー ボリュームには、プライマリー ボリュームと同等以上のサイズが必要です。
- ボリュームに設定できるミラー関係は1つだけです。
- 同期ミラー ペアの場合、プライマリー ボリュームとセカンダリー ボリュームは標準ボリュームである必要があります。シン ボリュームやSnapshotボリュームは使用できません。
- 同期ミラーリングの場合、特定のストレージ システムでサポートされるボリュームの数に制限があります。お使いのストレージ システムに設定されているボリュームの数がサポートされている制限よりも少ないことを確認してください。同期ミラーリングがアクティブな場合は、作成済みの2個のリザーブ容量ボリュームがボリュームの制限に含まれます。
- 非同期ミラーリングの場合、プライマリー ボリュームとセカンダリー ボリュームでドライブ セキュリティ機能が同じである必要があります。
  - プライマリー ボリュームがFIPS対応である場合、セカンダリー ボリュームもFIPS対応である必要があります。
  - プライマリー ボリュームがFDE対応である場合、セカンダリー ボリュームもFDE対応である必要があります。
  - プライマリー ボリュームがドライブ セキュリティを使用していない場合、セカンダリー ボリュームもドライブ セキュリティを使用していない必要があります。

**リザーブ容量**

非同期ミラーリングの場合：

- コントローラーのリセットおよびその他の一時的な中断からリカバリーするための書き込み情報をログに記録するには、ミラー ペアのプライマリー ボリュームとセカンダリー ボリュームにリザーブ容量ボリュームが必要です。
- ミラー ペアのプライマリー ボリュームとセカンダリー ボリュームには追加のリザーブ容量が必要であるため、ミラー関係にある両方のストレージ システムに空き容量が確保されていることを確認してください。

同期ミラーリングの場合：

- コントローラーのリセットおよびその他の一時的な中断からリカバリーするための書き込み情報をログに記録するには、プライマリー ボリュームとセカンダリー ボリュームにリザーブ容量が必要です。
- 同期ミラーリングがアクティブ化されると、リザーブ容量ボリュームが自動的に作成されます。ミラー ペアのプライマリー ボリュームとセカンダリー ボリュームにはリザーブ容量が必要であるため、同期ミラー関係にある両方のストレージ システムに十分な空き容量が確保されていることを確認してください。

**ドライブ セキュリティ機能**

- セキュリティ対応ドライブを使用する場合、プライマリー ボリュームとセカンダリー ボリュームのセキュリティ設定に互換性がある必要があります。この制限は強制的には適用されないため、自分で確認する必要があります。
- セキュリティ対応ドライブを使用する場合、プライマリー ボリュームとセカンダリー ボリュームで同じタイプのドライブを使用する必要があります。この制限は強制的には適用されないため、自分で確認する必要があります。
- Data Assurance（DA）を使用する場合、プライマリー ボリュームとセカンダリー ボリュームでDA設定を同じにする必要があります。

# ミラーリングの設定

## 非同期ミラー ペアの作成

非同期ミラーリングを設定するには、ローカル アレイのプライマリー ボリュームとリモート アレイのセカンダリー ボリュームを含むミラー ペアを作成します。

この機能はAB6100またはAB3100ストレージ システムでは使用できません。

開始する前に

ミラー ペアを作成する前に、Unified Managerに関する次の要件を満たしている必要があります。

- Web Services Proxyサービスが実行されている必要があります。
- Unified ManagerがHTTPS接続経由でローカル ホストで実行されている必要があります。
- Unified Managerにストレージ システムの有効なSSL証明書が表示されている必要があります。証明書については、Unified Managerの[証明書] > [証明書管理]で、自己署名証明書を受け入れるか独自のセキュリティ証明書をインストールできます。

また、ストレージ システムとボリュームに関する次の要件を満たしていることも確認してください。

- Unified Managerで2つのストレージ システムが検出されている必要があります。
- プライマリー アレイとセカンダリー アレイ内の各コントローラーにイーサネット管理ポートが設定されていて、各コントローラーがネットワークに接続されている必要があります。
- ローカルとリモートのストレージ システムのパスワードを確認しておく必要があります。
- リモート ストレージ システムにセカンダリー ボリュームを作成するための十分な空き容量（ミラーリングするプライマリー ボリュームと同等以上）が必要です。
- ローカルとリモートのストレージ システムをFibre ChannelファブリックまたはiSCSIインターフェイスを介して接続します。
- 非同期ミラー関係で使用するプライマリー ボリュームとセカンダリー ボリュームの両方を作成しておきます。

- セカンダリー ボリュームには、プライマリー ボリュームと同等以上のサイズが必要です。

タスク概要

非同期ミラー ペアを作成するプロセスは複数の手順で構成されます。

**手順 1：ミラー整合性グループを作成または選択する**

この手順では、新しいミラー整合性グループを作成するか既存のグループを選択します。ミラー整合性グループは、プライマリー ボリュームとセカンダリー ボリューム（ミラー ペア）のコンテナであり、グループ内のすべてのペアに対して必要な再同期方法（手動または自動）を指定します。

手順

1. **[管理]** ページで、ソースとして使用するローカル ストレージ システムを選択します。
2. [操作] > [非同期ミラー ペアの作成]を選択します。

   非同期ミラー ペアの作成ウィザードが開きます。

3. 既存のミラー整合性グループを選択するか、新規に作成します。

   既存のグループを選択するには、**[既存のミラー整合性グループ]** が選択されていることを確認し、表からグループを選択します。整合性グループには複数のミラー ペアを含めることができます。

   新しいグループを作成するには、次の手順を実行します。

   a. **[新しいミラー整合性グループ]** を選択し、**[次へ]** をクリックします。

   b. 2つのストレージ システム間でミラーリングするボリュームのデータを表す、一意のわかりやすい名前を入力します。名前に使用できる文字は、アルファベット、数字、アンダースコア（_）、ダッシュ（-）、ハッシュ記号（#）だけです。最大文字数は30文字で、スペースは使用できません。

   c. ローカル ストレージ システムとの間でミラー関係を確立するリモート ストレージ システムを選択します。

      リモート ストレージ システムがパスワードで保護されている場合は、パスワードを入力するように求められます。

   d. ミラー ペアの同期を手動で行うか自動で行うかを選択します。

      - **手動**
        このオプションは、グループ内のすべてのミラー ペアの同期を手動で開始する場合に選択します。再同期をあとから実行する場合は、プライマリー ストレージ システムのSystem Managerを起動して、[ストレージ] > [非同期ミラーリング]に移動し、**[ミラー整合性グループ]** タブからグループを選択して、[さらに表示] > [手動で再同期]を選択します。
      - **自動**
        **[分]**、**[時間]**、**[日]** で目的の間隔（前回の更新が開始されてから次回の更新を開始するまでの間隔）を選択します。たとえば、同期間隔が30分に設定されていて、同期プロセスが午後4時に開始する場合、次回のプロセスは午後4時30分に開始されます。

e. 必要なアラート設定を選択します。

- 手動同期の場合は、アラートを受信するときのしきい値（残りの容量の割合によって定義）を指定します。
- 自動同期の場合は、3つのアラート方法として、特定の時間内に同期が完了していない場合、リモート アレイのリカバリー ポイント データが特定の期限よりも古くなった場合、およびリザーブ容量が特定のしきい値（残りの容量の割合によって定義）に近づいている場合を設定できます。

4. **[次へ]** を選択し、手順 2：プライマリー ボリュームを選択するに進みます。

新しいミラー整合性グループを定義した場合は、Unified Managerによって、最初にローカル ストレージ システムに、続いてリモート ストレージ システムにミラー整合性グループが作成されます。各アレイのSystem Managerを起動すると、ミラー整合性グループを表示および管理できます。

Unified Managerによるミラー整合性グループの作成がローカル ストレージ システムで成功したあと、リモート ストレージ システムで失敗した場合は、ローカル ストレージ システムからミラー整合性グループが自動的に削除されます。Unified Managerによるミラー整合性グループの削除でエラーが発生した場合は、手動で削除する必要があります。

**手順 2：プライマリー ボリュームを選択する**

この手順では、ミラー関係で使用するプライマリー ボリュームを選択し、リザーブ容量を割り当てます。ローカル ストレージ システムのプライマリー ボリュームを選択する画面には、そのミラー ペアに対応するすべてのボリュームのリストが表示されます。使用できないボリュームはリストに表示されません。

ローカル ストレージ システムのミラー整合性グループに追加するボリュームには、ミラー関係のプライマリー ロールが割り当てられます。

手順

1. 対応するボリュームのリストから、プライマリー ボリュームとして使用するボリュームを選択し、**[次へ]** をクリックしてリザーブ容量を割り当てます。
2. 対応する候補のリストから、プライマリー ボリュームのリザーブ容量を選択します。

次のガイドラインに注意してください。

- リザーブ容量のデフォルト設定はベース ボリュームの容量の20%であり、通常はこの容量で十分です。割合を変更した場合は、**[候補を更新]** をクリックします。
- 必要な容量は、プライマリー ボリュームに対するI/O書き込みの頻度とサイズ、およびその容量を維持する必要がある期間によって異なります。
- 一般に、次のいずれかまたは両方に該当する場合は、リザーブ容量を大きくします。
  - ミラー ペアを長期にわたって維持する場合。
  - 大量のI/Oアクティビティにより、プライマリー ボリュームのデータ ブロックの大部分で変更が発生する場合。プライマリー ボリュームに対する一般的なI/Oアクティビティを判断するに

は、過去のパフォーマンス データやその他のオペレーティング システム ユーティリティーを使用します。

3. **[次へ]** を選択し、手順 3：セカンダリー ボリュームを選択するに進みます。

**手順 3：セカンダリー ボリュームを選択する**

この手順では、ミラー関係で使用するセカンダリー ボリュームを選択し、リザーブ容量を割り当てます。リモート ストレージ システムのセカンダリー ボリュームを選択する画面には、そのミラー ペアに使用できるすべてのボリュームが表示されます。使用できないボリュームはリストに表示されません。

リモート ストレージ システムのミラー整合性グループに追加するボリュームには、ミラー関係のセカンダリー ロールが割り当てられます。

手順

1. 対応するボリュームのリストから、ミラー ペアのセカンダリー ボリュームとして使用するボリュームを選択し、**[次へ]** をクリックしてリザーブ容量を割り当てます。
2. 対応する候補のリストから、セカンダリー ボリュームのリザーブ容量を選択します。

   次のガイドラインに注意してください。

   - リザーブ容量のデフォルト設定はベース ボリュームの容量の20%であり、通常はこの容量で十分です。割合を変更した場合は、**[候補を更新]** をクリックします。
   - 必要な容量は、プライマリー ボリュームに対するI/O書き込みの頻度とサイズ、およびその容量を維持する必要がある期間によって異なります。
   - 一般に、次のいずれかまたは両方に該当する場合は、リザーブ容量を大きくします。
     - ミラー ペアを長期にわたって維持する場合。
     - 大量のI/Oアクティビティにより、プライマリー ボリュームのデータ ブロックの大部分で変更が発生する場合。プライマリー ボリュームに対する一般的なI/Oアクティビティを判断するには、過去のパフォーマンス データやその他のオペレーティング システム ユーティリティーを使用します。
3. **[終了]** を選択して非同期ミラーリングの手順を完了します。

結果

Unified Managerは次の処理を実行します。

- ローカル ストレージ システムとリモート ストレージ システムの間で初期同期を開始します。
- ローカル ストレージ システムとリモート ストレージ システムにミラー ペア用のリザーブ容量を作成します。

ミラーリングしているボリュームがシン ボリュームの場合、初期同期では、プロビジョニングされたブロック（レポート容量ではなく割り当て容量）のみがセカンダリー ボリュームに転送されます。これにより、初期同期で転送する必要があるデータの量が削減されます。

## 同期ミラー ペアの作成

同期ミラーリングを設定するには、ローカル アレイのプライマリー ボリュームとリモート アレイのセカンダリー ボリュームを含むミラー ペアを作成します。

この機能はAB6100またはAB3100ストレージ システムでは使用できません。また、HB1000 seriesは同期ミラーリングを使用できません。

開始する前に

ミラー ペアを作成する前に、Unified Managerに関する次の要件を満たしている必要があります。

- Web Services Proxyサービスが実行されている必要があります。
- Unified ManagerがHTTPS接続経由でローカル ホストで実行されている必要があります。
- Unified Managerにストレージ システムの有効なSSL証明書が表示されている必要があります。証明書については、Unified Managerの[証明書] > [証明書管理]で、自己署名証明書を受け入れるか独自のセキュリティ証明書をインストールできます。

また、ストレージ システムとボリュームに関する次の要件を満たしていることも確認してください。

- ミラーリングに使用する2つのストレージ システムがUnified Managerで検出されている必要があります。
- プライマリー アレイとセカンダリー アレイ内の各コントローラーにイーサネット管理ポートが設定されていて、各コントローラーがネットワークに接続されている必要があります。
- ローカルとリモートのストレージ システムのパスワードを確認しておく必要があります。
- ローカルとリモートのストレージ システムをFibre Channelファブリックを介して接続します。
- 同期ミラー関係で使用するプライマリー ボリュームとセカンダリー ボリュームの両方を作成しておきます。
- プライマリー ボリュームは標準ボリュームである必要があります。シン ボリュームやSnapshotボリュームは使用できません。
- セカンダリー ボリュームは標準ボリュームである必要があります。シン ボリュームやSnapshotボリュームは使用できません。
- セカンダリー ボリュームには、プライマリー ボリュームと同等以上のサイズが必要です。

タスク概要

同期ミラー ペアを作成するプロセスは複数の手順で構成されます。

### 手順 1：プライマリー ボリュームを選択する

この手順では、同期ミラー関係で使用するプライマリー ボリュームを選択します。ローカル ストレージ システムのプライマリー ボリュームを選択する画面には、そのミラー ペアに対応するすべてのボリュームのリストが表示されます。使用できないボリュームはリストに表示されません。選択するボリュームには、ミラー関係のプライマリー ロールが割り当てられます。

手順

1. **[管理]** ページで、ソースとして使用するローカル ストレージ システムを選択します。
2. [操作] > [同期ミラー ペアの作成]を選択します。

   同期ミラー ペアの作成ウィザードが開きます。

3. 対応するボリュームのリストから、ミラーのプライマリー　ボリュームとして使用するボリュームを選択します。
4. **[次へ]** を選択し、手順 2：セカンダリー ボリュームを選択するに進みます。

### 手順 2：セカンダリー ボリュームを選択する

この手順では、ミラー関係で使用するセカンダリー ボリュームを選択します。リモート ストレージ システムのセカンダリー　ボリュームを選択する画面には、そのミラー　ペアに使用できるすべてのボリュームが表示されます。使用できないボリュームはリストに表示されません。選択するボリュームには、ミラー関係のセカンダリー ロールが割り当てられます。

手順

1. ローカル ストレージ システムとの間でミラー関係を確立するリモート ストレージ システムを選択します。

   リモート ストレージ システムがパスワードで保護されている場合は、パスワードを入力するように求められます。

   - ストレージ システムは、リストに名前で表示されます。ストレージ システムに名前を付けていない場合は、「名前なし」と表示されます。
   - 使用するストレージ システムがリストにない場合は、Unified Managerでそのストレージ システムが検出されていることを確認してください。

2. 対応するボリュームのリストから、ミラーのセカンダリー　ボリュームとして使用するボリュームを選択します。

   選択したセカンダリー ボリュームの容量がプライマリー ボリュームよりも大きい場合、使用可能な容量はプライマリー ボリュームのサイズまでに制限されます。

3. **[次へ]** をクリックし、手順 3：同期設定を選択するに進みます。

### 手順 3：同期設定を選択する

この手順では、通信中断後のデータの同期方法に関する設定を選択します。通信が中断した場合に、プライマリー　ボリュームの所有コントローラーがセカンダリー　ボリュームとの間でデータを再同期する優先度を設定できます。また、再同期ポリシーとして、手動または自動のどちらかを選択する必要があります。

手順

1. スライダ バーを使用して同期優先度を設定します。

同期優先度は、I/O要求の処理と比較して、初期同期および通信中断後の再同期処理を完了するためにどの程度のシステム リソースが使用されるかを決定するものです。

このダイアログで設定した優先度は、プライマリー ボリュームとセカンダリー ボリュームの両方に適用されます。プライマリー ボリュームの優先度は、System Managerの[ストレージ] > [同期ミラーリング] > [さらに表示] > [設定の編集]を選択してあとで変更できます。

同期優先度は5段階で設定できます。

- 最低
- 低
- 中
- 高
- 最高

同期優先度を[最低]に設定すると、I/Oアクティビティが優先され、再同期処理にかかる時間が長くなります。同期優先度を[最高]に設定すると、再同期処理が優先されますが、ストレージ　システムのI/Oアクティビティに影響する可能性があります。

2. リモート ストレージ システムのミラー ペアの再同期を手動で行うか自動で行うかを選択します。
   - **手動**（推奨オプション）
     ミラー　ペアとの通信が回復したあとに同期を手動で再開する場合に選択します。このオプションを選択すると、最適なタイミングでデータをリカバリーすることができます。
   - **自動**
     ミラー ペアとの通信が回復したあとに再同期を自動で開始する場合に選択します。

     同期を手動で再開するには、System Managerに移動して、[ストレージ] > [同期ミラーリング]の表でミラー ペアを選択し、**[さらに表示]** の **[再開]** を選択します。
3. **[終了]** をクリックして同期ミラーリングの手順を完了します。

結果

ミラーリングがアクティブ化されると、システムは次の処理を実行します。

- ローカル ストレージ システムとリモート ストレージ システムの間で初期同期を開始します。
- 同期優先度と再同期ポリシーを設定します。
- コントローラーのHICで **最も大きい番号のポート** をデータ送信のミラーリング用に予約します。

  このポートで受信したI/O要求は、ミラー　ペアに含まれるセカンダリー　ボリュームのリモートの優先コントローラー所有者からのみ承認されます（プライマリー　ボリュームにおける予約が許可されます）。

- 2個のリザーブ容量ボリューム（各コントローラーに1個ずつ）を作成します。これらのボリュームは、コントローラーのリセットおよびその他の一時的な中断からリカバリーするための書き込み情報

をログに記録するために使用されます。

各ボリュームの容量は128MiBです。ただし、ボリュームがプールに配置されている場合は、ボリュームごとに4GiBが予約されます。

終了後の操作

System Managerに移動し、[ホーム] > [実行中の処理を表示]を選択して、同期ミラーリング処理の進捗状況を確認します。この処理には時間がかかることがあり、システムのパフォーマンスに影響する可能性があります。

# FAQ

## ミラー整合性グループを作成するときは、どのような点に注意する必要がありますか？

ミラー整合性グループを作成する際は、次のガイドラインに従ってください。

Unified Managerに関する次の要件を満たしている必要があります。

- Web Services Proxyサービスが実行されている必要があります。
- Unified ManagerがHTTPS接続経由でローカル ホストで実行されている必要があります。
- Unified Managerにストレージ システムの有効なSSL証明書が表示されている必要があります。証明書については、Unified Managerの[証明書] > [証明書管理]で、自己署名証明書を受け入れるか独自のセキュリティ証明書をインストールできます。

また、ストレージ システムに関する次の要件を満たしていることも確認してください。

- Unified Managerで2つのストレージ システムが検出されている必要があります。
- プライマリー アレイとセカンダリー アレイ内の各コントローラーにイーサネット管理ポートが設定されていて、各コントローラーがネットワークに接続されている必要があります。
- ローカルとリモートのストレージ システムのパスワードを確認しておく必要があります。
- ローカルとリモートのストレージ システムをFibre ChannelファブリックまたはiSCSIインターフェイスを介して接続します。

この機能はAB6100またはAB3100ストレージ システムでは使用できません。また、HB1000 seriesは同期ミラーリングを使用できません。

## ミラー ペアを作成するときは、どのような点に注意する必要がありますか？

ミラー ペアを作成する際は、次のガイドラインに従ってください。

- 2つのストレージ システムが必要です。
- Unified Managerで2つのストレージ システムが検出されている必要があります。

- プライマリー アレイとセカンダリー アレイ内の各コントローラーにイーサネット管理ポートが設定されていて、各コントローラーがネットワークに接続されている必要があります。
- ローカルとリモートのストレージ システムのパスワードを確認しておく必要があります。
- リモート ストレージ システムにセカンダリー ボリュームを作成するための十分な空き容量（ミラーリングするプライマリー ボリュームと同等以上）が必要です。
- 非同期ミラーリングはFibre Channel（FC）またはiSCSIホスト ポートを備えたコントローラーでサポートされますが、同期ミラーリングはFCホスト ポートを備えたコントローラーでのみサポートされます。

この機能はAB6100またはAB3100ストレージ システムでは使用できません。

### この割合を変更するのはどのような場合ですか？

非同期ミラーリング処理用のリザーブ容量は、一般にベース ボリュームの20%です。通常はこの容量で十分です。

必要な容量は、ベース ボリュームへの書き込みI/Oの頻度とサイズ、およびストレージ オブジェクトのコピー サービス処理を使用する期間によって異なります。一般に、次のいずれかまたは両方に該当する場合は、リザーブ容量の割合を大きくします。

- 特定のストレージ オブジェクトのコピー サービス処理の期間が非常に長い場合。
- 大量のI/Oアクティビティにより、ベース ボリュームのデータ ブロックの大部分で変更が発生する場合。ベース ボリュームに対する一般的なI/Oアクティビティを判断するには、過去のパフォーマンス データやその他のオペレーティング システム ユーティリティーを使用します。

### リザーブ容量の候補が複数表示されるのはなぜですか？

プールまたはボリューム グループ内にストレージ オブジェクトに対して選択した容量の割合（%）を満たす複数のボリュームがある場合は、複数の候補が表示されます。

ベース ボリューム上でコピー サービス処理用にリザーブする物理ドライブ スペースの割合を変更すると、推奨される候補の一覧が更新されます。選択内容に基づいて、最適な候補が表示されます。

### ボリュームが一部表示されないのはなぜですか？

ミラー ペアのプライマリー ボリュームを選択すると、対応するすべてのボリュームのリストが表示されます。

使用できないボリュームはリストに表示されません。次のいずれかの理由で、ボリュームが対象外になっている可能性があります。

- 最適状態でない。

- すでにミラー関係に参加している。
- 同期ミラーリングの場合、ミラー ペアのプライマリー ボリュームとセカンダリー ボリュームは標準ボリュームである必要があります。シン ボリュームやSnapshotボリュームは使用できません。
- 非同期ミラーリングの場合は、シン ボリュームで自動拡張が有効になっている必要があります。

### リモート ストレージ システムのボリュームが一部表示されないのはなぜですか？

リモート ストレージ システム上のセカンダリー ボリュームを選択すると、そのミラー ペアに対応するすべてのボリュームのリストが表示されます。

使用に適さないボリュームはリストには表示されません。次のいずれかに該当するボリュームは対応しない場合があります。

- 標準以外のボリューム（Snapshotボリュームなど）である。
- 最適状態でない。
- すでにミラー関係に参加している。
- （非同期ミラーリングの場合）シン ボリューム属性が、プライマリー ボリュームとセカンダリー ボリュームで一致しない。
- Data Assurance（DA）を使用する場合、プライマリー ボリュームとセカンダリー ボリュームでDA設定を同じにする必要があります。
  - プライマリー ボリュームでDAを有効にする場合、セカンダリー ボリュームでもDAを有効にする必要があります。
  - プライマリー ボリュームでDAを有効にしない場合、セカンダリー ボリュームでもDAを無効にする必要があります。
- 非同期ミラーリングの場合、プライマリー ボリュームとセカンダリー ボリュームでドライブ セキュリティ機能が同じである必要があります。
  - プライマリー ボリュームがFIPS対応である場合、セカンダリー ボリュームもFIPS対応である必要があります。
  - プライマリー ボリュームがFDE対応である場合、セカンダリー ボリュームもFDE対応である必要があります。
  - プライマリー ボリュームがドライブ セキュリティを使用していない場合、セカンダリー ボリュームもドライブ セキュリティを使用していない必要があります。

### 同期優先度は同期のレートにどのような影響がありますか？

同期優先度は、システム パフォーマンスと比較して同期アクティビティに割り当てられる処理時間を決定します。

プライマリー ボリュームのコントローラー所有者は、この処理をバックグラウンドで実行します。同時にコントローラー所有者は、プライマリー ボリュームへのローカルのI/O書き込みと、対応するセカンダリ

ー
ボリュームへのリモートの書き込みを処理します。再同期には、I/Oアクティビティに使用されるはずのコントローラーの処理リソースが使用されるため、再同期がホスト アプリケーションのパフォーマンスに影響する可能性があります。

同期優先度に応じた所要時間や、同期優先度がシステム パフォーマンスに与える影響を特定する際には、次のガイドラインを参考にしてください。

指定できる優先度は次のとおりです。

- 最低
- 低
- 中
- 高
- 最高

最低ではシステム パフォーマンスが優先されますが、再同期化に時間がかかります。最高では再同期化が優先されますが、システム パフォーマンスが低下する可能性があります。

次のガイドラインは、各優先度の大まかな違いを示しています。

| 完全同期の優先度 | 「最高」との所要時間の比較 |
|---|---|
| 最低 | 約8倍 |
| 低 | 約6倍 |
| 中 | 約3.5倍 |
| 高 | 約2倍 |

同期の所要時間には、ボリューム サイズとホストのI/O速度が影響します。

### 手動同期ポリシーの使用が推奨されるのはなぜですか？

手動再同期が推奨されるのは、データがリカバリーされる可能性が最も高い方法で再同期プロセスを管理できるためです。

自動再同期ポリシーを使用していて、再同期中に通信が中断する問題が発生した場合は、セカンダリー ボリューム上のデータが一時的に破損する可能性があります。再同期が完了すると、データは修正されます。

# 証明書

# 証明書の概要

証明書管理では、証明書署名要求（CSR）の作成、証明書のインポート、および既存の証明書の管理を行うことができます。

## 証明書とは何ですか？

証明書は、Webサイトやサーバーなどのオンライン エンティティを識別するデジタル ファイルであり、インターネット上のセキュアーな通信を実現します。証明書には2種類あります。署名済み証明書は認証局（CA）によって検証され、自己署名証明書は第三者ではなくエンティティの所有者によって検証されます。

詳細情報：

- 証明書の仕組み
- 証明書の用語

## 証明書を設定するにはどうすればよいですか？

証明書管理では、Unified Managerをホストする管理ステーションの証明書を設定できるほか、アレイ内のコントローラーの証明書をインポートすることもできます。

詳細情報：

- 管理システムのCA署名証明書の使用
- アレイの証明書のインポート

# 概念

## 証明書の仕組み

証明書は、Webサイトやサーバーなどのオンライン エンティティを識別するデジタル ファイルであり、インターネット上のセキュアーな通信を実現します。

#### 署名済み証明書

証明書を使用すると、指定したサーバーとクライアント間でのみ、Webでの通信が非公開かつ変更されずに、暗号化された形式で送信されます。Unified Managerを使用すると、ホスト管理システムのブラウザーおよび検出されたストレージ システムのコントローラーの証明書を管理できます。

証明書には信頼できる認証局が署名した証明書と自己署名の証明書があります。「署名」とは、第三者が所有者のIDを検証し、そのデバイスが信頼できると確認したことを意味します。ストレージ システムの各コントローラーには、自動生成された自己署名証明書が付属しています。自己署名証明書を引き続き使用することも、CA署名証明書を取得してコントローラーとホスト システム間のよりセキュアーな接続を実

現することもできます。

CA署名証明書ではセキュリティ保護が強化されますが（中間者攻撃を阻止するなど）、大規模なネットワークの場合はコストがかかる可能性があります。一方、自己署名証明書の場合、安全性は低くなりますが無料です。したがって、自己署名証明書は本番環境ではなく内部テスト環境で最もよく使用されます。

署名済み証明書は、信頼できる第三者機関である認証局（CA）によって検証されます。署名済み証明書には、エンティティ（通常、サーバーまたはWebサイト）の所有者に関する詳細、証明書の発行日と有効期限、エンティティの有効なドメイン、およびアルファベットと数字で構成されるデジタル署名が含まれています。

ブラウザーを開いてWebアドレスを入力すると、証明書チェック　プロセスがバックグラウンドで実行され、有効なCA署名証明書を含むWebサイトに接続しているかどうかが確認されます。通常、署名済み証明書で保護されたサイトのアドレスには、鍵のアイコンとhttpsの指定が含まれます。CA署名証明書が含まれていないWebサイトに接続しようとすると、サイトがセキュリティで保護されていないことを示す警告がブラウザーに表示されます。

CAは、申請プロセス中にユーザーの身元を確認するための手順を実行します。登録済みの会社にEメールを送信し、会社の住所を確認して、HTTPまたはDNSの検証を実行する場合があります。申請プロセスが完了すると、ホスト管理システムにロードするデジタル　ファイルがCAから送信されます。通常、これらのファイルには次のような信頼チェーンが含まれます。

- **ルート**
  階層の最上位にあるのはルート証明書です。この証明書には、他の証明書への署名に使用する秘密鍵が含まれています。ルートは特定のCA組織を識別します。すべてのネットワーク　デバイスで同じCAを使用する場合は、ルート証明書が1つだけ必要です。
- **中間**
  ルートからの分岐は中間証明書です。CAは、保護されたルート証明書とサーバー証明書の間の証明書として機能する、1つ以上の中間証明書を発行します。
- **サーバー**
  チェーンの最下位にあるのはサーバー証明書です。この証明書は、Webサイトや他のデバイスなど、特定のエンティティを識別します。ストレージ　システムの各コントローラーには個別のサーバー証明書が必要です。

### 自己署名証明書

ストレージ システムの各コントローラーには、自己署名証明書が事前にインストールされています。自己署名証明書はCA署名証明書と似ていますが、第三者ではなくエンティティの所有者によって検証される点が異なります。CA署名証明書と同様に、自己署名証明書には独自の秘密鍵が含まれており、サーバーとクライアントの間でHTTPS接続を介してデータが暗号化および送信されることも保証されます。

自己署名証明書はブラウザーでは「信頼」されません。自己署名証明書のみを含むWebサイトに接続しようとするたびに、ブラウザーには警告メッセージが表示されます。Webサイトに進むには、警告メッセージ内のリンクをクリックする必要があります。これにより、基本的には自己署名証明書が受け入れられま

す。

### Unified Managerの証明書

Unified Managerインターフェイスは、ホスト システムにWeb Services Proxyとともにインストールされます。ブラウザーを開き、Unified Managerに接続しようとすると、ホストが信頼できるソースであるかどうかを確認するためにデジタル証明書がチェックされます。ブラウザーでサーバーのCA署名証明書が見つからない場合は、警告メッセージが表示されます。そこからWebサイトにアクセスして、そのセッションの自己署名証明書を受け入れることができます。または、CAから署名入りのデジタル証明書を取得して、警告メッセージが表示されないようにすることもできます。

### コントローラーの証明書

Unified Managerセッション中に、CA署名証明書のないコントローラーにアクセスしようとすると、追加のセキュリティ メッセージが表示されることがあります。この場合、自己署名証明書を永続的に信頼するか、コントローラーのCA署名証明書をインポートして、Web Services Proxyサーバーがこれらのコントローラーから受信するクライアント要求を認証できるようにすることができます。

## 証明書の用語

証明書管理に関連する用語を次に示します。

| 用語 | 説明 |
|---|---|
| CA | 認証局（CA）は、インターネット セキュリティに関するデジタル電子文書（証明書と呼ばれる）を発行する信頼されたエンティティです。証明書でWebサイトの所有者を識別することにより、クライアントとサーバーの間のセキュアーな接続が確立されます。 |
| CSR | 証明書署名要求（CSR）は、申請者から認証局（CA）に送信するメッセージです。CSRは、CAが証明書を発行するために必要な情報を検証します。 |
| 証明書 | 証明書はセキュリティ上の目的でサイトの所有者を識別する文書で、攻撃者による偽装を防止します。証明書には、サイトの所有者に関する情報と、その情報について証明（署名）する信頼されたエンティティの識別情報が格納されます。 |
| 証明書チェーン | 証明書にセキュリティ レイヤを追加するファイルの階層。通常、チェーンには1つのルート証明書（階層の最上位）、1つ以上の中間証明書、およびエンティティを識別するサーバー証明書が含まれています。 |
| 中間証明書 | 証明書チェーンのルートから1つ以上の中間証明書が分岐します。CAは、保護されたルート証明書とサーバー証明書の間の証明書として機能する、1つ以上の中間証明書を発行します。 |
| キーストア | キーストアはホスト管理システム上のリポジトリであり、秘密鍵とそれに対応する公開鍵および証明書が格納されています。これらの鍵と証明書によって、コントローラーなどの独自のエンティティが識別されます。 |

| 用語 | 説明 |
| --- | --- |
| ルート証明書 | ルート証明書は、証明書チェーンの階層の最上位にあります。この証明書には、他の証明書への署名に使用する秘密鍵が含まれています。ルートは特定のCA組織を識別します。すべてのネットワーク デバイスで同じCAを使用する場合は、ルート証明書が1つだけ必要です。 |
| 署名済み証明書 | 認証局（CA）によって検証される証明書。このデータ ファイルには秘密鍵が含まれており、サーバーとクライアントの間でHTTPS接続を介してデータが暗号化された形式で送信されることが保証されます。また、署名済み証明書には、エンティティ（通常、サーバーまたはWebサイト）の所有者に関する詳細およびアルファベットと数字で構成されるデジタル署名が含まれています。署名済み証明書は信頼チェーンを使用するため、本番環境で最もよく使用されます。「CA署名証明書」または「管理証明書」とも呼ばれます。 |
| 自己署名証明書 | 自己署名証明書は、エンティティの所有者によって検証されます。このデータ ファイルには秘密鍵が含まれており、サーバーとクライアントの間でHTTPS接続を介してデータが暗号化された形式で送信されることが保証されます。また、アルファベットと数字で構成されるデジタル署名も含まれています。自己署名証明書はCA署名証明書と同じ信頼チェーンを使用しないため、テスト環境で最もよく使用されます。「事前にインストールされている」証明書とも呼ばれます。 |
| サーバー証明書 | サーバー証明書は、証明書チェーンの最下位にあります。Webサイトや他のデバイスなど、特定のエンティティを識別します。ストレージ システムの各コントローラーには個別のサーバー証明書が必要です。 |
| 信頼ストア | 信頼ストアは、信頼できる第三者（CAなど）からの証明書を格納するリポジトリです。 |

## 管理システムのCA署名証明書の使用

Unified Managerをホストする管理システムへのセキュアーなアクセスを確立するために、CA署名証明書を取得してインポートできます。

開始する前に

Security Adminの権限を含むユーザー プロファイルでログインする必要があります。そうしないと、証明書関連の機能は表示されません。

タスク概要

CA署名証明書を使用するには、次の3つの手順を実行します。

**手順 1：CSRファイルを生成する**

最初に証明書署名要求（CSR）ファイルを生成する必要があります。CSRファイルは組織、およびWeb Services ProxyとUnified Managerがインストールされているホスト システムを識別します。

CSRファイルは、OpenSSLなどのツールを使用して生成することもできます。その場合は、手順　2：CSRファイルを送信するに進みます。OpenSSLのCAで認証した証明書の利用も可能です。

手順

1. **[証明書管理]** を選択します。
2. [管理]タブで、**[CSR の生成]** を選択します。
3. 次の情報を入力して、**[次へ]** をクリックします。
   - **組織**
     会社または組織の完全な正式名称。Inc.やCorp.などの接尾辞も含めて入力してください。
   - **組織単位（オプション）**
     証明書を使用する組織の部門。
   - **市区町村**
     ホスト システムまたは事業の所在地である市区町村。
   - **都道府県（オプション）**
     ホスト システムまたは事業の所在地である都道府県。
   - **ISO の国コード**
     自国を表す2桁のISO（国際標準化機構）コード（USなど）。
4. Web Services Proxyがインストールされているホスト システムについて、次の情報を入力します。
   - **共通名**
     Web Services Proxyがインストールされているホスト システムのIPアドレスまたはDNS名。このアドレスが正しいことを確認します（ブラウザーでUnified Managerにアクセスする際に入力するアドレスと正確に一致している必要があります）。「http://」または「https://」は含めないでください。DNS名の1文字目にワイルドカードを使用することはできません。
   - **代替 IP アドレス**
     共通名がIPアドレスの場合は、ホスト　システムの追加のIPアドレスまたはエイリアスをオプションで入力できます。複数指定する場合は、カンマで区切って入力します。
   - **代替 DNS 名**
     共通名がDNS名の場合は、ホスト　システムの追加のDNS名を入力します。複数指定する場合は、カンマで区切って入力します。代替DNS名がない場合は、最初のフィールドに入力したDNS名をここにコピーします。DNS名の1文字目にワイルドカードを使用することはできません。
5. ホスト情報が正しいことを確認します。正しくないと、CAから受け取った証明書をインポートできません。
6. **[完了]** をクリックします。
7. 手順 2：CSRファイルを送信するに進みます。

**手順 2：CSRファイルを送信する**

証明書署名要求（CSR）ファイルを作成したら、そのファイルを認証局（CA）に送信して、Unified

ManagerとWeb Services Proxyをホストするシステムの署名済み管理証明書をリクエストします。

ETERNUS AB/HB Series には、PEM形式（Base64 ASCIIエンコード）の署名済み証明書が必要です。該当するファイル形式は.pem、.crt、.cer、または.keyです。

手順

1. ダウンロードしたCSRファイルの場所を確認します。

   ダウンロード フォルダーの場所は、ブラウザーによって異なります。

2. CSRファイルをCA（VerisignやDigiCertなど）に送信し、PEM形式の署名済み証明書を要求します。

   **CSRファイルをCAに送信したあとに、別のCSRファイルを再生成しないでください。**CSRを生成すると、秘密鍵と公開鍵のペアが作成されます。公開鍵はCSRの一部であり、秘密鍵はシステムのキーストアに保持されます。署名済み証明書を受け取ってインポートすると、システムは秘密鍵と公開鍵の両方がオリジナルのペアであることを確認します。キーが一致しないと署名済み証明書は機能せず、CAに新しい証明書を要求する必要があります。

3. CAから署名済み証明書を受け取ったら、手順 3：管理証明書のインポートに進みます。

**手順 3：管理証明書のインポート**

認証局（CA）から署名済み証明書を受け取ったら、Web Services ProxyとUnified Managerインターフェイスがインストールされているホスト システムに証明書をインポートします。

開始する前に

- CAから署名済み証明書を受け取っておきます。これらのファイルには、ルート証明書、1つ以上の中間証明書、およびサーバー証明書が含まれます。
- CAからチェーン証明書ファイル（たとえば、.p7bファイル）が提供された場合は、チェーン　ファイルを個々のファイル（ルート証明書、1つ以上の中間証明書、サーバー証明書）に展開する必要があります。Windows certmgr ユーティリティーを使用すると、ファイルを展開できます（右クリックして、[すべてのタスク] > [エクスポート]を選択）。Base-64エンコード方式を推奨します。エクスポートが完了すると、チェーン内の証明書ファイルごとに1つのCERファイルが表示されます。
- Web Services Proxyが実行されているホスト システムに証明書ファイルをコピーしておきます。

手順

1. **[証明書管理]** を選択します。
2. [管理]タブで、**[インポート]** を選択します。

   証明書ファイルをインポートするためのダイアログ ボックスが表示されます。

3. **[参照]** をクリックして最初にルート証明書と中間証明書のファイルを選択してから、サーバー証明書を選択します。外部ツールからCSRを生成した場合は、CSRと一緒に作成された秘密鍵ファイルもインポートする必要があります。

ファイル名がダイアログ ボックスに表示されます。

4. **[インポート]** をクリックします。

結果

ファイルがアップロードされて検証されます。[証明書管理]ページに証明書の情報が表示されます。

### 管理証明書のリセット

管理証明書を工場出荷時の自己署名証明書の状態に戻すことができます。

開始する前に

Security Adminの権限を含むユーザー プロファイルでログインする必要があります。そうしないと、証明書関連の機能は表示されません。

タスク概要

このタスクでは、Web Services ProxyとUnified Managerがインストールされているホスト システムから現在の管理証明書を削除します。証明書をリセットすると、ホスト システムでは自己署名証明書が再び使用されるようになります。

手順

1. **[証明書管理]** を選択します。
2. [管理]タブで、**[リセット]** を選択します。

   [管理証明書のリセットの確認]ダイアログ ボックスが開きます。

3. フィールドに「リセット」と入力し、**[リセット]** をクリックします。

   ブラウザーをリフレッシュしたあとに、サイトがHTTP Strict Transport Securityを使用しているという理由でデスティネーション サイトへのアクセスがブロックされる場合があります。この状況は自己署名証明書に戻した場合に発生します。問題を解決するには、ブラウザーから閲覧データを削除する必要があります。

結果

システムでサーバーの自己署名証明書が再び使用されるようになります。そのため、セッションの自己署名証明書を手動で承認するよう求められます。

## アレイ証明書の使用

### アレイの証明書のインポート

必要に応じて、Unified Managerをホストするシステムで認証できるように、ストレージ システムの証明書をインポートすることができます。証明書には認証局（CA）が署名した証明書と自己署名の証明書があります。

開始する前に

- Security Adminの権限を含むユーザー プロファイルでログインする必要があります。そうしないと、証明書関連の機能は表示されません。
- 信頼された証明書をインポートする場合は、System Managerを使用してストレージ システムのコントローラーの証明書をインポートする必要があります。

手順

1. **[証明書管理]** を選択します。
2. **[信頼済み]** タブを選択します。

   このページには、ストレージ システムについて報告されたすべての証明書が表示されます。

3. CA証明書をインポートする場合は[インポート] > [証明書]、自己署名証明書をインポートする場合は[インポート] > [自己署名ストレージ システム証明書]を選択します。

   表示される証明書を絞り込むには、**[表示する証明書の条件を選択…]** フィルター フィールドを使用するか、いずれかの列見出しをクリックして行をソートします。

4. ダイアログ ボックスで、証明書を選択して **[インポート]** をクリックします。

   証明書がアップロードされて検証されます。

## 信頼された証明書の削除

期限切れになった証明書など、不要になった証明書を削除することができます。

開始する前に

古い証明書を削除する前に新しい証明書をインポートします。

ルート証明書または中間証明書を削除する場合は、同じ証明書ファイルが共有されていることがあるため、複数のストレージ システムに影響する可能性があることに注意してください。

手順

1. **[証明書管理]** を選択します。
2. **[信頼済み]** タブを選択します。
3. 証明書を表から選択し（複数可）、**[削除]** をクリックします。

   **[削除]** 機能は、あらかじめインストールされている証明書には使用できません。

   [信頼された証明書の削除の確認]ダイアログ ボックスが開きます。

4. 処理を確認し、**[削除]** をクリックします。

   証明書が表から削除されます。

## 信頼されていない証明書の解決

信頼されていない証明書の問題は、ストレージ システムからUnified Managerへのセキュアーな接続を確立しようとしたときに、接続が安全であることが確認できないと発生します。

[証明書]ページで信頼されていない証明書を解決するには、ストレージ システムの自己署名証明書をインポートするか、信頼できる第三者機関が発行した認証局（CA）証明書をインポートします。

開始する前に

- Security Adminの権限を含むユーザー プロファイルでログインする必要があります。
- CA署名証明書をインポートする場合は次の準備が必要です。
  - ストレージ システムの各コントローラーの証明書署名要求（.CSRファイル）を生成してCAに送信しておく必要があります。
  - 信頼された証明書ファイルをCAから受け取っておきます。
  - 証明書ファイルがローカル システム上にある必要があります。

タスク概要

信頼された追加のCA証明書のインストールが必要になる可能性があるのは、次のいずれかに該当する場合です。

- ストレージ システムを新たに追加した。
- 一方または両方の証明書の期限が切れている。
- 一方または両方の証明書が失効している。
- 一方または両方の証明書のルート証明書または中間証明書がない。

手順

1. **[証明書管理]** を選択します。
2. **[信頼済み]** タブを選択します。

   このページには、ストレージ システムについて報告されたすべての証明書が表示されます。

3. CA証明書をインポートする場合は[インポート] > [証明書]、自己署名証明書をインポートする場合は[インポート] > [自己署名ストレージ システム証明書]を選択します。

   表示される証明書を絞り込むには、**[表示する証明書の条件を選択…]** フィルター フィールドを使用するか、いずれかの列見出しをクリックして行をソートします。

4. ダイアログ ボックスで、証明書を選択して **[インポート]** をクリックします。

   証明書がアップロードされて検証されます。

# 証明書の管理

## 証明書の表示

証明書を使用している組織、発行元の機関、有効期間、フィンガープリント（一意の識別子）など、証明書の概要情報を表示できます。

開始する前に

Security Adminの権限を含むユーザー プロファイルでログインする必要があります。そうしないと、証明書関連の機能は表示されません。

手順

1. **[証明書管理]** を選択します。
2. 次のいずれかのタブを選択します。
   - **管理**
     Web Services Proxyをホストしているシステムの証明書が表示されます。管理証明書には、自己署名の証明書と認証局（CA）によって承認された証明書があります。この証明書によって、Unified Managerへのセキュアーなアクセスを確立することができます。
   - **信頼済み**
     Unified Managerがアクセスできるストレージ システムおよびその他のリモート サーバー（LDAPサーバーなど）の証明書が表示されます。認証局（CA）から発行された証明書と自己署名の証明書が含まれます。
3. 証明書の詳細を参照するには、該当する行を選択し、行の最後にある省略記号を選択して **[表示]** または **[エクスポート]** をクリックします。

## 証明書のエクスポート

証明書をエクスポートして詳細を確認することができます。

開始する前に

エクスポートしたファイルを開くには、証明書ビューア アプリケーションが必要です。

手順

1. **[証明書管理]** を選択します。
2. 次のいずれかのタブを選択します。
   - **管理**
     Web Services Proxyをホストしているシステムの証明書が表示されます。管理証明書には、自己署名の証明書と認証局（CA）によって承認された証明書があります。この証明書によって、Unified Managerへのセキュアーなアクセスを確立することができます。
   - **信頼済み**
     Unified Managerがアクセスできるストレージ システムおよびその他のリモート サーバー

（LDAPサーバーなど）の証明書が表示されます。認証局（CA）から発行された証明書と自己署名の証明書が含まれます。

3. 証明書をページから選択し、行の最後にある省略記号をクリックします。
4. **[エクスポート]** をクリックし、証明書ファイルを保存します。
5. 証明書ビューア アプリケーションでファイルを開きます。

# アクセス管理

## アクセス管理の概要

アクセス管理は、Unified Managerでのユーザー認証を設定する手段です。

### 使用可能な認証方式にはどのようなものがありますか？

次の認証方式を使用できます。

- **ローカル ユーザー ロール**
  RBAC（ロールベース アクセス制御）機能を使用して認証を管理します。ローカル ユーザー ロールには、事前定義のユーザー プロファイルと、特定のアクセス権限を持つロールが含まれます。
- **ディレクトリー サービス**
  認証は、LDAP（Lightweight Directory Access Protocol）サーバーとディレクトリー サービス（MicrosoftのActive Directoryなど）を通じて管理されます。

詳細情報：

- アクセス管理の仕組み
- アクセス管理の用語
- マッピングされたロールの権限

### アクセス管理を設定するにはどうすればよいですか？

SANtricityソフトウェアは、ローカル ユーザー ロールを使用するように事前に設定されています。LDAPを使用する場合は[アクセス管理]ページで設定できます。

詳細情報：

- ローカル ユーザー ロールを使用したアクセス管理
- ディレクトリー サービスを使用したアクセス管理

## 概念

## アクセス管理の仕組み

アクセス管理を使用してUnified　Managerでのユーザー認証を確立することができます。

### 設定ワークフロー

アクセス管理設定は次のように行います。

1. Security Adminの権限を含むユーザー プロファイルでUnified Managerにログインします。

初回ログイン時は、自動的に **admin** というユーザー名が表示され、変更することはできません。**admin** ユーザーには、システムのすべての機能を使用できるフル アクセスが付与されています。初回ログイン時にパスワードを設定する必要があります。

2. ユーザー　インターフェイスでアクセス管理に移動します。事前に設定されているローカル　ユーザー ロールが表示されます。これらのロールはRBAC（ロールベース アクセス制御）機能の実装です。
3. 次の認証方式を1つ以上設定します。
   - **ローカル ユーザー ロール**
     RBAC機能を使用して認証を管理します。ローカル　ユーザー　ロールには、事前定義のユーザーと、特定のアクセス権限を持つロールが含まれます。これらのローカル ユーザー ロールのみを認証方式として使用することも、ディレクトリー　　サービスと組み合わせて使用することもできます。ユーザーのパスワードを設定する以外に特別な設定は不要です。
   - **ディレクトリー サービス**
     認証は、LDAP（Lightweight Directory Access Protocol）サーバーとディレクトリー サービス（MicrosoftのActive　Directoryなど）を通じて管理されます。管理者がLDAPサーバーに接続し、ローカル ユーザー ロールにLDAPユーザーをマッピングします。
4. Unified Managerのログイン クレデンシャルをユーザーに割り当てます。
5. ユーザーが自身のクレデンシャルを入力してシステムにログインします。ログイン時には、次のバックグラウンド タスクが実行されます。
   - ユーザー名とパスワードがユーザー アカウントと照合して認証されます。
   - 割り当てられたロールに基づいてユーザーの権限が決定されます。
   - ユーザー インターフェイスの機能にユーザーがアクセスできるようになります。
   - 上部のバナーにユーザー名が表示されます。

### Unified Managerで使用できる機能

アクセスできる機能は、ユーザーに割り当てられたロールによって次のように異なります。

- **Storage Admin**
  アレイのストレージ オブジェクトに対する読み取り / 書き込みのフル アクセスが付与されます。セ

キュリティ設定にはアクセスできません。

- **Security Admin**
  アクセス管理と証明書管理のセキュリティ設定へのアクセスが付与されます。
- **Support Admin**
  ストレージ システムのすべてのハードウェア リソース、障害データ、およびMELイベントへのアクセスが付与されます。ストレージ オブジェクトやセキュリティ設定にはアクセスできません。
- **Monitor**
  すべてのストレージ　オブジェクトに対する読み取り専用のアクセスが付与されます。セキュリティ設定にはアクセスできません。

使用できない機能は、ユーザー インターフェイスではグレー表示されるか、非表示になります。

## アクセス管理の用語

Unified Managerに関連するアクセス管理の用語を次に示します。

| 用語 | 説明 |
|---|---|
| Active Directory | Active　Directory（AD）は、MicrosoftのWindowsドメイン　ネットワーク用のLDAPを使用したディレクトリー サービスです。 |
| バインド | バインド処理は、ディレクトリー　サーバーに対するクライアントの認証に使用されます。通常はアカウントとパスワードのクレデンシャルが必要ですが、匿名のバインド処理が可能なサーバーもあります。 |
| CA | 認証局（CA）は、インターネット　セキュリティに関するデジタル電子文書（証明書と呼ばれる）を発行する信頼されたエンティティです。証明書でWebサイトの所有者を識別することにより、クライアントとサーバーの間のセキュアーな接続が確立されます。 |
| 証明書 | 証明書はセキュリティ上の目的でサイトの所有者を識別する文書で、攻撃者による偽装を防止します。証明書には、サイトの所有者に関する情報と、その情報について証明（署名）する信頼されたエンティティの識別情報が格納されます。 |
| LDAP | Lightweight Directory Access Protocol（LDAP）は、分散型のディレクトリー情報サービスへのアクセスと管理に使用されるアプリケーション　プロトコルです。LDAPを使用して、さまざまなアプリケーションやサービスがLDAPサーバーに接続し、ユーザーを検証することができます。 |
| RBAC | ロールベース　アクセス制御（RBAC）は、コンピュータやネットワーク　リソースへのアクセスを個々のユーザーのロールに基づいて制御する手法です。Unified Managerには事前定義されたロールが用意されています。 |
| SSO | シングル　サインオン（SSO）は、1組のログイン　クレデンシャルで複数のアプリケーションにアクセスできるようにする認証サービスです。 |

| 用語 | 説明 |
| --- | --- |
| Web Services Proxy | Web Services Proxyは標準のHTTPSメカニズムによるアクセスを提供するプロキシで、管理者にストレージ　システムの管理サービスの設定を許可します。このプロキシはWindowsホストまたはLinuxホストにインストールできます。Unified Managerインターフェイスは Web Services Proxyとともに提供されます。 |

## マッピングされたロールの権限

ロールベース　アクセス制御（RBAC）機能には、1つ以上のロールがマッピングされた事前定義済みのユーザーが含まれています。各ロールには、Unified　Managerのタスクにアクセスするための権限が含まれています。

各ロールは、次のタスクへのアクセスを提供します。

- **Storage Admin**
  アレイのストレージ オブジェクトに対する読み取り / 書き込みのフル アクセスが付与されます。セキュリティ設定にはアクセスできません。
- **Security Admin**
  アクセス管理と証明書管理のセキュリティ設定へのアクセスが付与されます。
- **Support Admin**
  ストレージ システムのすべてのハードウェア リソース、障害データ、およびMELイベントへのアクセスが付与されます。ストレージ オブジェクトやセキュリティ設定にはアクセスできません。
- **Monitor**
  すべてのストレージ　オブジェクトに対する読み取り専用のアクセスが付与されます。セキュリティ設定にはアクセスできません。

ユーザーに特定の機能に対する権限がない場合、その機能は選択できない状態になるか、ユーザー インターフェイスに表示されません。

## ローカル ユーザー ロールを使用したアクセス管理

Unified Managerで適用されるRBAC（ロールベース アクセス制御）機能を使用して認証を管理することができます。これらの機能のことを「ローカル　ユーザー　ロール」と呼びます。

### 設定ワークフロー

ローカル ユーザー ロールはシステムで事前に設定されています。認証にローカル ユーザー ロールを使用するための手順は次のとおりです。

1. Security Adminの権限を含むユーザー プロファイルでUnified Managerにログインします。

admin ユーザーには、システムのすべての機能を使用できるフル アクセスが付与されています。

2. ユーザー プロファイルを確認します。ユーザー プロファイルは事前に定義されており、変更できません。
3. 必要に応じて、各ユーザー プロファイルに新しいパスワードを割り当てます。
4. ユーザーは各自に割り当てられたクレデンシャルでシステムにログインします。

#### 管理

認証にローカル ユーザー ロールのみを使用する場合、管理者は次の管理タスクを実行できます。

- パスワードを変更する。
- パスワードの最小文字数を設定する。
- パスワードなしでログインできるようにユーザーに許可する。

## ディレクトリー サービスを使用したアクセス管理

LDAP（Lightweight Directory Access Protocol）サーバーとディレクトリー サービス（MicrosoftのActive Directoryなど）を使用して認証を管理することができます。

#### 設定ワークフロー

ネットワークでLDAPサーバーとディレクトリー　サービスを使用している場合の設定は次のようになります。

1. Security Adminの権限を含むユーザー プロファイルでUnified Managerにログインします。

admin ユーザーには、システムのすべての機能を使用できるフル アクセスが付与されています。

2. LDAPサーバーの設定を入力します。これには、ドメイン名、URL、バインド　アカウント情報が含まれます。
3. LDAPサーバーでセキュアーなプロトコル（LDAPS）を使用している場合、LDAPサーバーとホスト システム（Web　Services　Proxyがインストールされているシステム）の間の認証に使用する認証局（CA）証明書チェーンをアップロードします。
4. サーバー接続が確立されたら、ユーザー グループをローカル ユーザー ロールにマッピングします。これらのロールは事前に定義され、変更することはできません。
5. LDAPサーバーとWeb Services Proxyの間の接続をテストします。
6. ユーザーは各自に割り当てられたLDAP / ディレクトリー サービスのクレデンシャルでシステムにログインします。

**管理**

認証にディレクトリー サービスを使用する場合、管理者は次の管理タスクを実行できます。

- ディレクトリー サーバーを追加する。
- ディレクトリー サーバーの設定を編集する。
- LDAPユーザーをローカル ユーザー ロールにマッピングする。
- ディレクトリー サーバーを削除する。
- パスワードを変更する。
- パスワードの最小文字数を設定する。
- パスワードなしでログインできるようにユーザーに許可する。

# ローカル ユーザ ロールの使用

## ローカル ユーザー ロールの表示

[ローカル ユーザ ロール]タブでは、ユーザーとデフォルト ロールのマッピングを表示できます。これらのマッピングは、Unified ManagerのWeb Services Proxyで適用されるRBAC（ロールベース アクセス制御）の一部です。

開始する前に

Security Adminの権限を含むユーザー プロファイルでログインする必要があります。そうしないと、アクセス管理の機能は表示されません。

タスク概要

ユーザーとマッピングは変更できません。変更できるのはパスワードのみです。

手順

1. **[アクセス管理]** を選択します。
2. **[ローカル ユーザ ロール]** タブを選択します。

   表にユーザーが表示されます。

   - **admin**
     システムのすべての機能を使用できるスーパー管理者。このユーザーには、すべてのロールが含まれています。
   - **storage**
     すべてのストレージ プロビジョニングを担当する管理者。このユーザーには、Storage Admin、Support Admin、Monitorの各ロールが含まれています。
   - **security**
     アクセス管理や証明書管理など、セキュリティ設定を担当するユーザー。このユーザーに

は、Security AdminとMonitorの各ロールが含まれています。

- **support**
  ハードウェア リソース、障害データ、ファームウェア アップグレードを担当するユーザー。このユーザーには、Support AdminとMonitorの各ロールが含まれています。
- **monitor**
  システムへの読み取り専用アクセスが付与されたユーザー。このユーザーには、Monitorロールのみが含まれています。
- **rw**（読み取り / 書き込み）
  このユーザーには、Storage Admin、Support Admin、Monitorの各ロールが含まれています。
- **ro**（読み取り専用）
  このユーザーには、Monitorロールのみが含まれています。

## ローカル ユーザー プロファイルのパスワードの変更

[アクセス管理]で各ユーザーのユーザー パスワードを変更できます。

開始する前に

- Root Adminの権限が割り当てられたローカル管理者としてログインする必要があります。
- ローカル管理者のパスワードを確認しておきます。

タスク概要

パスワードを決める際は、次のガイドラインに注意してください。

- 新しいローカル ユーザー パスワードは現在の最小文字数の設定（[設定の表示 / 編集]）以上にする必要があります。
- パスワードでは大文字と小文字が区別されます。
- パスワードの末尾のスペースは削除されません。設定時に末尾にスペースを含めた場合は、入力時にスペースを含めるようにしてください。
- セキュリティを強化するため、パスワードには15文字以上の英数字を使用し、頻繁に変更してください。

手順

1. **[アクセス管理]** を選択します。
2. **[ローカル ユーザ ロール]** タブを選択します。
3. 表からユーザーを選択します。

   [パスワードの変更]ボタンが使用可能な状態になります。
4. **[パスワードの変更]** を選択します。

   [パスワードの変更]ダイアログ ボックスが開きます。

5. ローカル ユーザー パスワードに対して最小文字数が設定されていない場合は、システムにアクセスするユーザーにパスワードの入力を求めるチェックボックスを選択できます。
6. 選択したユーザーの新しいパスワードを2つのフィールドに入力します。
7. この処理を実行する確認としてローカル管理者パスワードを入力し、**[変更]** をクリックします。

結果

ユーザーが現在ログインしている場合、パスワードを変更するとユーザーのアクティブなセッションが終了します。

## ローカル ユーザー パスワードの設定の変更

すべての新規または更新されるローカル ユーザー パスワードの最小文字数を設定できます。また、ローカル ユーザーがパスワードを入力せずにシステムにアクセスできるようにすることもできます。

開始する前に

Root Adminの権限が割り当てられたローカル管理者としてログインする必要があります。

タスク概要

ローカル ユーザー パスワードの最小文字数を設定する際には、次のガイドラインに注意してください。

- 設定を変更しても既存のローカル ユーザー パスワードには影響しません。
- ローカル ユーザー パスワードの最小文字数は、0～30文字にする必要があります。
- 新しいローカル ユーザー パスワードは、現在の最小文字数の設定以上にする必要があります。
- ローカル ユーザーがパスワードを入力せずにシステムにアクセスできるようにする場合は、パスワードの最小文字数を設定しないでください。

手順

1. **[アクセス管理]** を選択します。
2. **[ローカル ユーザ ロール]** タブを選択します。
3. **[設定の表示 / 編集]** を選択します。

   [ローカル ユーザ パスワードの設定]ダイアログ ボックスが開きます。

4. 次のいずれかを実行します。
   - ローカル ユーザーがパスワードを入力せずにシステムにアクセスできるようにするには、[すべてのローカル ユーザ パスワードに対して最低文字数を設定する]チェック ボックスをオフにします。
   - すべてのローカル ユーザー パスワードを対象にパスワードの最小文字数を設定するには、[すべてのローカル ユーザ パスワードに対して最低文字数を設定する]チェック ボックスをオンにし、スピン ボックスで最小文字数を設定します。

新しいローカル ユーザー パスワードは、現在の設定以上の長さにする必要があります。

5. **[保存]** をクリックします。

# ディレクトリ サービスの使用

## ディレクトリー サーバーの追加

アクセス管理用の認証を設定するには、LDAPサーバーとUnified　ManagerのWeb Services　Proxyを実行するホストの間の通信を確立します。その後、LDAPユーザーグループをローカル ユーザーロールにマッピングします。

開始する前に

- Security　Adminの権限を含むユーザープロファイルでログインする必要があります。そうしないと、アクセス管理の機能は表示されません。
- ユーザー グループがディレクトリーサービスに定義されている必要があります。
- LDAPサーバーのクレデンシャルを確認しておく必要があります。ドメイン名とサーバーのURLのほか、場合によってはバインド アカウントのユーザー名とパスワードも必要になります。
- セキュアーなプロトコルを使用するLDAPSサーバーの場合は、LDAPサーバーの証明書チェーンがローカルマシンにインストールされている必要があります。

タスク概要

ディレクトリーサーバーの追加は2段階のプロセスです。最初に、ドメイン名とURLを入力します。サーバーでセキュアーなプロトコルを使用していて、認証に使用するCA証明書が標準の署名機関によって署名されていない場合、その証明書もアップロードする必要があります。バインドアカウントのクレデンシャルがある場合は、そのアカウント名とパスワードも入力できます。その後、LDAPサーバーのユーザー　グループをローカルユーザーロールにマッピングします。

手順

1. **[アクセス管理]** を選択します。
2. **[ディレクトリ サービス]** タブで、**[ディレクトリ サーバの追加]** を選択します。

   [ディレクトリサーバーの追加]ダイアログボックスが開きます。

3. **[サーバの設定]** タブで、LDAPサーバーのクレデンシャルを入力します。

   ▼ フィールドの詳細

| 設定 | 説明 |
| --- | --- |
| **構成設定** | |

| | |
|---|---|
| ドメイン | LDAPサーバーのドメイン名を入力します。ドメインを複数入力する場合は、カンマで区切って入力します。ドメイン名は、ログイン情報（*username*@*domain*）で使用され、認証するディレクトリーサーバーを指定します。 |
| サーバー URL | LDAPサーバーにアクセスするためのURLを `ldap[s]://host: port` の形式で入力します。 |
| 証明書のアップロード（オプション） |  このフィールドは、上記の[サーバ　URL]フィールドでLDAPSプロトコルを指定した場合にのみ表示されます。<br><br>**[参照]** をクリックし、アップロードするCA証明書を選択します。これは、LDAPサーバーの認証に使用される信頼された証明書または証明書チェーンです。 |
| バインドアカウント（オプション） | LDAPサーバーに対する検索クエリやグループ内の検索で使用する読み取り専用のユーザーアカウントを入力します。アカウント名はLDAPタイプの形式で入力します。たとえば、バインドユーザーの名前が「bindacct」であれば、「`CN=bindacct,CN=Users,DC=cpoc,DC=local`」などと入力します。 |
| バインドパスワード（オプション） |  このフィールドは、バインドアカウントを入力した場合に表示されます。<br><br>バインドアカウントのパスワードを入力します。 |
| 追加する前にサーバー接続をテストする | 入力したLDAPサーバーの設定でシステムと通信できるかどうかを確認するには、このチェックボックスを選択します。テストは、ダイアログボックスの一番下の **[追加]** をクリックしたあとに実行されます。<br><br>このチェックボックスを選択した場合、テストに失敗すると設定は追加されません。設定を追加するには、エラーを解決するか、チェックボックスを選択解除してテストをスキップする必要があります。 |
| **権限設定** | |
| 検索ベースDN | ユーザーを検索するLDAPコンテキストを入力します。通常は、`CN=Users, DC=cpoc, DC=local` の形式で入力します。 |
| ユーザー名属性 | 認証用のユーザーIDにバインドされた属性を入力します。次に例を示します。<br>`sAMAccountName` |
| グループ属性 | グループとロールのマッピングに使用される、ユーザーの一連のグループ属性を入力します。次に例を示します。<br>`memberOf, managedObjects` |

4. **[ロールのマッピング]** タブをクリックします。
5. 事前定義されたロールにLDAPグループを割り当てます。1つのグループに複数のロールを割り当てる

ことができます。

▼ フィールドの詳細

| 設定 | 説明 |
| --- | --- |
| **マッピング** | |
| グループDN | マッピングするLDAPユーザーグループの識別名（DN）を指定します。正規表現を使用できます。次の特殊文字を正規表現のパターン以外で使用する場合は、バックスラッシュ（¥）でエスケープする必要があります。<br>¥.[]{}()<>*+-=!?^$\| |
| ロール | フィールド内をクリックし、グループDNにマッピングするローカル　ユーザー　ロールを選択します。グループにマッピングするロールを1つずつ選択する必要があります。MonitorロールはSANtricity　Unified Managerにログインするために必要なロールであり、他のロールと一緒に指定する必要があります。各ロールの権限は次のとおりです。<br>• **Storage Admin**<br>ストレージシステムのストレージオブジェクトに対する読み取り　/　書き込みのフルアクセスが付与されます。セキュリティ設定にはアクセスできません。<br>• **Security Admin**<br>アクセス管理と証明書管理のセキュリティ設定へのアクセスが付与されます。<br>• **Support Admin**<br>ストレージシステムのすべてのハードウェアリソース、障害データ、およびMELイベントへのアクセスが付与されます。ストレージオブジェクトやセキュリティ設定にはアクセスできません。<br>• **Monitor**<br>すべてのストレージオブジェクトに対する読み取り専用のアクセスが付与されます。セキュリティ設定にはアクセスできません。 |

Monitorロールは、管理者を含むすべてのユーザーに必要です。

6. 必要な場合は、**[別のマッピングを追加]** をクリックしてグループとロールのマッピングをさらに指定します。
7. マッピングが終了したら、**[追加]** をクリックします。

ストレージシステムとLDAPサーバーが通信できるかどうかの検証がシステムによって実行されます。エラーメッセージが表示された場合は、ダイアログ　ボックスで入力したクレデンシャルを確認し、必要に応じて情報を再入力します。

## ディレクトリー サーバー設定とロール マッピングの編集

アクセス管理でディレクトリーサーバーを設定済みの場合、その設定をいつでも変更することができます。設定には、サーバー接続情報とグループとロールのマッピングが含まれます。

開始する前に

- Security Adminの権限を含むユーザープロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- ディレクトリサーバーが定義されている必要があります。

手順

1. **[アクセス管理]** を選択します。
2. **[ディレクトリサービス]** タブを選択します。
3. 複数のサーバーが定義されている場合は、編集するサーバーを表から選択します。
4. **[設定の表示 / 編集]** を選択します。

   [ディレクトリサーバーの設定]ダイアログボックスが開きます。

5. **[サーバの設定]** タブで、必要に応じて設定を変更します。

▼ フィールドの詳細

| 設定 | 説明 |
|---|---|
| **構成設定** | |
| ドメイン | LDAPサーバーのドメイン名。ドメインを複数入力する場合は、カンマで区切って入力します。ドメイン名は、ログイン情報（*username* @*domain*）で使用され、認証するディレクトリーサーバーを指定します |
| サーバーURL | LDAPサーバーにアクセスするためのURL（`ldap[s]://host: port` の形式）。 |
| バインドアカウント（オプション） | LDAPサーバーに対する検索クエリやグループ内の検索で使用する読み取り専用のユーザーアカウント。 |
| バインドパスワード（オプション） | バインドアカウントのパスワード（このフィールドはバインドアカウントを入力した場合に表示されます）。 |
| 保存する前にサーバー接続をテストする | システムがこの設定でLDAPサーバーと通信できることを確認します。このテストは、**[保存]** をクリックしたあとに実行されます。このチェックボックスを選択した場合、テストに失敗すると設定は変更されません。設定を編集するには、エラーを解決するか、チェックボックスを選択解除してテストをスキップする必要があります。 |
| **権限設定** | |

| 設定 | 説明 |
| --- | --- |
| 検索ベースDN | ユーザーを検索するLDAPコンテキスト。通常は、`CN=Users, DC=cpoc, DC=local` の形式で入力します。 |
| ユーザー名属性 | 認証用のユーザーIDにバインドされた属性。次に例を示します。<br>`sAMAccountName` |
| グループ属性 | グループとロールのマッピングに使用される、ユーザーの一連のグループ属性。次に例を示します。<br>`memberOf, managedObjects` |

6. **[ロールのマッピング]** タブで、必要に応じてマッピングを変更します。

▼ フィールドの詳細

| 設定 | 説明 |
| --- | --- |
| **マッピング** | |
| グループDN | マッピングするLDAPユーザー　グループのドメイン名。正規表現を使用できます。次の特殊文字を正規表現のパターン以外で使用する場合は、バックスラッシュ（¥）でエスケープする必要があります。<br><br>¥.[]{}()<>*+-=!?^$\| |
| ロール | グループDNにマッピングするロール。このグループに含めるロールを個別に選択する必要があります。MonitorロールはSANtricity　Unified Managerにログインするため必要なロールであり、他のロールと一緒に指定する必要があります。ロールには次のものがあります。<br><br>• **Storage admin**<br>ストレージシステム上のストレージオブジェクトに対する読み取り/書き込みのフルアクセスが付与されます。セキュリティ設定にはアクセスできません<br>• **Security admin**<br>アクセス管理と証明書管理のセキュリティ設定へのアクセスが付与されます。<br>• **Support admin**<br>ストレージシステムのすべてのハードウェアリソース、障害データ、およびMELイベントへのアクセスが付与されます。ストレージオブジェクトやセキュリティ設定にはアクセスできません。<br>• **Monitor**<br>すべてのストレージオブジェクトに対する読み取り専用のアクセスが付与されます。セキュリティ設定にはアクセスできません。 |

Monitorロールは、管理者を含むすべてのユーザに必要です。

7. 必要に応じて、*別のマッピングを追加*をクリックして、グループとロールのマッピングをさらに入力します。
8. [ 保存（ Save ） ] をクリックします。

このタスクを完了すると、アクティブなユーザーセッションはすべて終了されます。現在のユーザーセッションのみが保持されます。

### ディレクトリー サーバーの削除

ディレクトリー サーバーとWeb Services Proxyの間の接続を切断するには、[アクセス管理]ページでサーバー情報を削除します。このタスクは、新しいサーバーの設定が完了して古いサーバーを削除する場合などに実行します。

開始する前に

Security Adminの権限を含むユーザー プロファイルでログインする必要があります。そうしないと、アクセス管理の機能は表示されません。

タスク概要

このタスクを完了すると、アクティブなユーザー セッションはすべて終了されます。現在のユーザー セッションのみが保持されます。

手順

1. **[アクセス管理]** を選択します。
2. **[ディレクトリ サービス]** タブを選択します。
3. 削除するディレクトリー サーバーをリストから選択します。
4. **[削除]** をクリックします。

   [ディレクトリ サーバの削除]ダイアログ ボックスが開きます。

5. フィールドに「削除」と入力し、**[削除]** をクリックします。

   ディレクトリー サーバー設定、権限設定、ロール マッピングが削除されます。ユーザーは、以降このサーバーからのクレデンシャルを使用してログインすることはできません。

## FAQ

### ログインできない理由は何ですか？

ログインする際にエラーが表示される場合は、次の問題がないか確認してください。

ログイン エラーは、次のいずれかが原因の可能性があります。

- 入力したユーザー名またはパスワードが間違っている。

- 必要な権限がない。
- ログインが複数回失敗したために、ロックアウトされた。この場合は、10分待ってから再度ログインしてください。

## ディレクトリー サーバーを追加するときは、どのような点に注意する必要がありますか？

アクセス管理でディレクトリー サーバーを追加する際は、一定の要件を満たしている必要があります。

- ユーザー グループがディレクトリー サービスに定義されている必要があります。
- LDAPサーバーのクレデンシャルを確認しておく必要があります。ドメイン名とサーバーのURLのほか、場合によってはバインド アカウントのユーザー名とパスワードも必要になります。
- セキュアーなプロトコルを使用するLDAPSサーバーの場合は、LDAPサーバーの証明書チェーンがローカル マシンにインストールされている必要があります。

## ストレージ システムのロールをマッピングするときは、どのような点に注意する必要がありますか？

グループをロールにマッピングする際は、次のガイドラインに注意してください。

RBAC（ロールベース アクセス制御）機能には次のロールがあります。

- **Storage Admin**
  アレイのストレージ オブジェクトに対する読み取り / 書き込みのフル アクセスが付与されます。セキュリティ設定にはアクセスできません。
- **Security Admin**
  アクセス管理と証明書管理のセキュリティ設定へのアクセスが付与されます。
- **Support Admin**
  ストレージ システムのすべてのハードウェア リソース、障害データ、およびMELイベントへのアクセスが付与されます。ストレージ オブジェクトやセキュリティ設定にはアクセスできません。
- **Monitor**
  すべてのストレージ オブジェクトに対する読み取り専用のアクセスが付与されます。セキュリティ設定にはアクセスできません。

  Monitorロールは、管理者を含むすべてのユーザーに必要です。

LDAP（Lightweight Directory Access Protocol）サーバーとディレクトリー サービスを使用する場合は、次の点を確認してください。

- ディレクトリー サービスでユーザー グループを定義しておきます。
- LDAPユーザー グループのグループ ドメイン名を確認しておきます。

## ローカル ユーザーとは何ですか？

ローカル ユーザーは、システムに事前に定義されたユーザーで、特定の権限が含まれています。

ローカル ユーザーには次のものがあります。

- **admin**
  システムのすべての機能を使用できるスーパー管理者。このユーザーには、すべてのロールが含まれています。初回ログイン時にパスワードを設定する必要があります。
- **storage**
  すべてのストレージ　　プロビジョニングを担当する管理者。このユーザーには、Storage Admin、Support　Admin、Monitorの各ロールが含まれています。このアカウントは、パスワードが設定されるまで無効です。
- **security**
  アクセス管理や証明書管理など、セキュリティ設定を担当するユーザー。このユーザーには、Security　AdminとMonitorの各ロールが含まれています。このアカウントは、パスワードが設定されるまで無効です。
- **support**
  ハードウェア リソース、障害データ、ファームウェア アップグレードを担当するユーザー。このユーザーには、Support　AdminとMonitorの各ロールが含まれています。このアカウントは、パスワードが設定されるまで無効です。
- **monitor**
  システムへの読み取り専用アクセスが付与されたユーザー。このユーザーには、Monitorロールのみが含まれています。このアカウントは、パスワードが設定されるまで無効です。
- **rw**（読み取り / 書き込み）
  このユーザーには、Storage Admin、Support Admin、Monitorの各ロールが含まれています。このアカウントは、パスワードが設定されるまで無効です。
- **ro**（読み取り専用）
  このユーザーには、Monitorロールのみが含まれています。このアカウントは、パスワードが設定されるまで無効です。

# 奥付

Fujitsu Storage ETERNUS AB/HB Series
SANtricity 11.7 Unified Manager
CA08871-193-04
発行日: 2023 年 4 月
発行責任: 富士通株式会社