HITACHI
Inspire the Next

Account Authentication

ユーザーズガイド
（HUS100 シリーズ）

Hitachi Storage Navigator Modular 2を使ってアレイ装置を操作する場合は、必ずこのマニュアルを読み、操作手順、および指示事項をよく理解してから操作してください。
また、このマニュアルをいつでも利用できるよう、Hitachi Storage Navigator Modular 2を使用するコンピュータの近くに保管してください。

対象製品
P-002D-J517

免責事項
このマニュアルの内容の一部または全部を無断で複製することはできません。
このマニュアルの内容については、将来予告なしに変更することがあります。
このマニュアルに基づいてソフトウェアを操作した結果、たとえ当該ソフトウェアがインストールされているお客様所有のコンピュータに何らかの障害が発生しても、当社は一切責任を負いかねますので、あらかじめご了承ください。
このマニュアルの当該ソフトウェアご購入後のサポートサービスに関する詳細は、当社営業担当にお問い合わせください。

輸出時の注意
本製品を輸出される場合には、外国為替及び外国貿易法の規制ならびに米国輸出管理規則など外国の輸出関連法規をご確認のうえ、必要な手続きをお取りください。なお、ご不明な場合は、弊社担当営業にお問い合わせください。

商標類
Microsoft および Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Red Hat は、米国およびその他の国で Red Hat, Inc. の登録商標もしくは商標です。
UNIX は、The Open Group の米国ならびに他の国における登録商標です。
その他記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。
なお、本文中では、®および ™は明記しておりません。

マイクロソフト製品のスクリーンショットの使用について
Microsoft Corporation のガイドラインに従って画面写真を使用しています。

発行
2013 年 5 月（第 7 版）K6603694

著作権

目次

はじめに

このマニュアルは、HUS110/130/150アレイ装置用の「Account Authenticationユーザーズガイド」です。このマニュアルでは、Account Authenticationを初めて導入するときのインストール方法やAccount Authenticationの主な機能について簡単に説明しています。

また、このマニュアルでは特に断りのない限り、HUS110/130/150アレイ装置を「アレイ装置」と呼びます。

対象読者

このマニュアルは、次の方を対象読者として記述しています。

- システムの運用管理者
- システムエンジニア
- アレイ装置の保守員

このマニュアルの内容については、万全を期しておりますが、ご不審な点や誤りなど、お気付きのことがございましたら当社までご連絡ください。

単なる誤字・脱字などはお断りなく訂正しています。

マニュアルで使用する単位について

1 k（キロ）バイトは1,024バイト、1 M（メガ）バイトは1,024キロバイト、1 G（ギガ）バイトは1,024メガバイト、1 T（テラ）バイトは1,024ギガバイトの計算値です。

1ブロック（Block）は512バイトです。

1

Account Authentication

Account Authenticationは、アレイ装置の構成情報やユーザーデータを守ることを目的とし、管理LANインターフェースからの不正侵入・不正操作などのセキュリティ上の脅威、攻撃からアレイ装置を防御して安全性を確保するための機能です。アレイ装置に登録されたアカウントの情報によって、アレイ装置にアクセスするユーザーの認証と、アレイ装置のリソースへのアクセス（参照・設定）を制御します。

Account Authenticationは、以下の3つの機能で構成されています。

- ユーザー管理機能

  アレイ装置に、ユーザーのアカウント（ユーザーID、パスワード、ロール等）の登録・変更する機能です。

- ユーザー認証機能

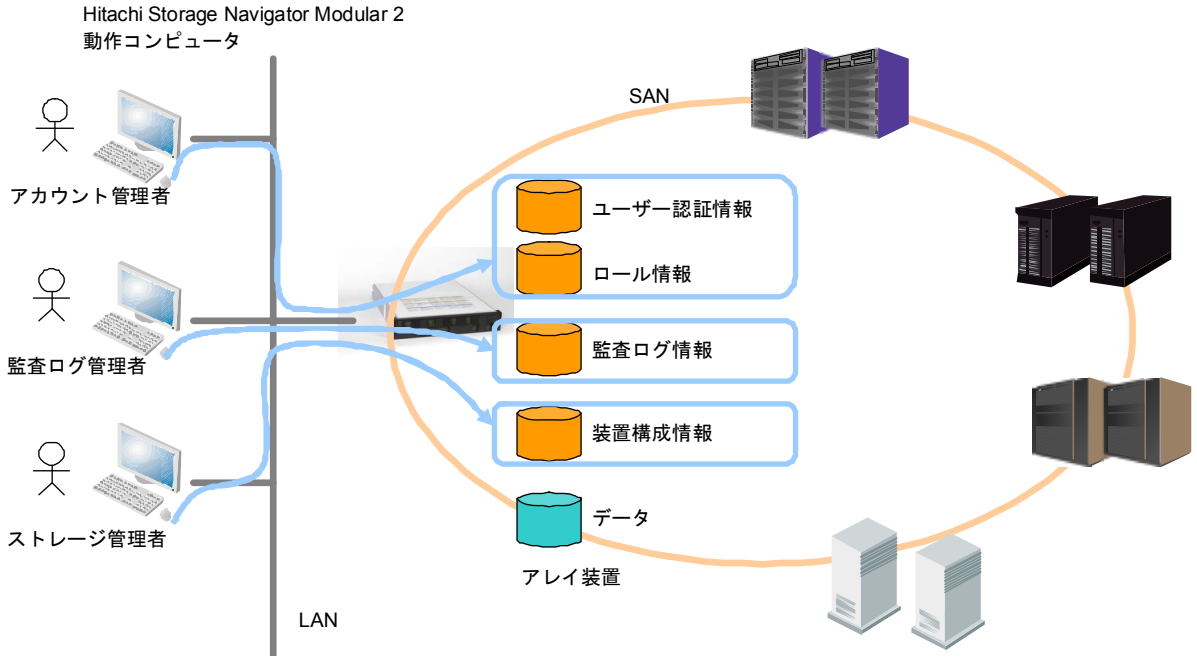
  ユーザーがアレイ装置にアクセス（ログイン）する際に、アカウントの情報によって認証する機能です。

- アクセス制御機能

  アカウントに割り当てられたロールの種別によって、アレイ装置リソースへのアクセス（リソース参照・設定更新）を制御する機能です。

図 1-1にAccount Authenticationの概要例を示します。

図 1-1　Account Authentication 概要



アレイ装置を使用するユーザーは、あらかじめ個別のアカウント（ユーザーID、パスワード等）を登録しておきます（ユーザー管理機能）。

ユーザーがアレイ装置にアクセスした際に、そのユーザーが登録されているユーザーかどうかを認証します（ユーザー認証機能）。これにより、アレイ装置を利用するユーザーの識別・制限が可能になります。

アカウントを登録したユーザーには、システムの管理目的別に参照・更新権限（ロール情報）が与えられ、その権限の範囲内においてアレイ装置の各リソースをアクセスすることができます（アクセス制御）。

アカウントを登録していないユーザーに対しては、アレイ装置へのアクセスを許可しないため、不正侵入を防ぐことができます。また、ロール情報により管理目的別に参照・更新権限を割り当てることができるため、アカウントを登録済みであるユーザーにおいても、管理目的以外の不正操作に対して制限をかけることができます。

2

準備

お客様がAccount Authenticationを使用するための準備について記載します。

本章は以下の内容で構成されています。

2.1 動作環境と必要条件

表 2-1にAccount Authenticationの動作環境と必要条件を示します。

表 2-1　Account Authentication の動作環境と必要条件

項目	用途
動作環境と前提条件	• 管理用 PC にはバージョンが 21.50 以上の Hitachi Storage Navigator Modular 2 が必要です。
注意事項	• アレイ装置保守のため、保守員も Hitachi Storage Navigator Modular 2 を使用します。Account Authentication を使用する際は、保守員用アカウントも作成し、保守作業に支障をきたさないようにしてください • Account Authentication だけでは正規にアカウントをもつユーザーによる不正操作を抑止することはできません。Audit Logging と併用することで、ユーザーによる構成変更の内容を記録することができ、ユーザーによる不正操作を抑止する効果を生み出すことができます。
制限事項	• Password Protection とは併用できません。両方インストールした場合は、先にインストールした方が有効になります。 • Password Protection から Account Authentication に変更する場合は、Password Protection を無効にしたあとで、Account Authentication を有効にしてください。 • Password Protection から Account Authentication に変更した場合または Account Authentication から Password Protection に変更した場合、登録したアカウント情報は引き継がれません。
追加インストール／構成変更	ありません。

2.2 仕様

表 2-2にAccount Authenticationの仕様を示します。

表 2-2　Account Authentication の仕様

項目	用途
アカウント作成に必要な情報	アカウント情報にはユーザーID、パスワード、ロール、およびアカウントの有効・無効を含みます。
登録可能アカウント数	最大 200 アカウントをアレイ装置に登録できます。
最大ログイン数	最大 256 ユーザーのログインが可能です（同一ユーザーによる重複ログイン含む）。
割り当て可能ロール数	下記のロールを最大 6 つ、1 アカウントに割り当てることができます。 ・ Storage Administrator（View and Modify） ・ Storage Administrator（View Only） ・ Account Administrator（View and Modify） ・ Account Administrator（View Only） ・ Audit Log Administrator（View and Modify） ・ Audit Log Administrator（View Only）
セッションタイムアウト時間	ユーザーのログイン有効時間が設定できます。 5 分単位で 20～60 分、10 分単位で 70～120 分、一日、または OFF。 無操作で上記期間を超過すると強制的にログアウトされます。
セキュリティモード	セキュリティモードには、アドバンスドセキュリティモードがあります。「2.3.8　アドバンスドセキュリティモード」を参照してください。

注意 1：パスワード設定時の最小文字数は 6 です。8 文字以上を推奨します。

注意 2：セッションと管理モードについては、「2.3.5　セッション」、「2.3.6　セッションの種別とリソース操作権限の移行」を参照してください。

注意 3：アレイ装置保守のため、保守員も Hitachi Storage Navigator Modular 2 を使用します。アカウントを作成する際は、保守員用アカウントも作成し、保守作業に支障をきたさないようにしてください。保守員用アカウントには必ず Storage Administrator（View and Modify）ロールを割り当ててください。

注意 4：アレイ装置運用のため、Hitachi Storage Navigator Modular 2 などによる障害監視を行う場合、障害監視用アカウントを作成してください。障害監視用アカウントには必ず Storage Administrator（View only）ロールを割り当ててください。

2.3 導入

2.3.1 アカウント

アカウントとは、Account Authenticationをインストールしたアレイ装置にアクセスするために、あらかじめアレイ装置に登録しておく情報（ユーザーID、パスワード、ロール、およびアカウントの有効・無効）です。アレイ装置はこの情報を元に、ログイン時の認証とログイン後のリソースへの参照・更新の可否を判断します。

アカウントには表 2-3の情報が含まれます。

アレイ装置は、これらの情報をユーザー認証、リソースへのアクセス制御を行う際に使用します。

表 2-3　アカウント仕様

項目	説明	仕様
ユーザーID	当該アカウントを識別するための識別子	文字数：1～256 使用可能文字種：ASCII コード（0-9、A-Z、a-z、! # $ % & ‘ * + - . / = ? @ ^ _ ` { | } ~）
パスワード	当該アカウントを認証するための認証情報	文字数：6～256 使用可能文字種：ASCII コード（0-9、A-Z、a-z、” ! # $ % & ‘ ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~）
ロール	当該アカウントに割り当てるロール	詳細は「2.3.3　ロール」を参照 1 アカウントに割り当て可能なロール数：1～6
アカウント有効/無効の情報	当該アカウントに対する認証機能の有効/無効情報	選択範囲：有効、無効

注意：パスワード設定時の最小文字数は 6 です。8 文字以上を推奨します。

2.3.2 アカウント種別

アカウントには、「ビルトインアカウント」と「一般アカウント」の2種類があります。

Account Authenticationのインストール後、ユーザーが任意に作成可能なアカウントは一般アカウントです。ビルトインアカウントは、はじめからアレイ装置に登録されているルートアカウントです。

ビルトインアカウントの初期ユーザーID、初期パスワード、初期割り当てロールはあらかじめ決められています。アレイ装置を運用する際は、通常使うアカウントとして一般アカウントを作成し、必要なロールを割り当てて使用してください。

表 2-4　アカウント種別

種別	初期 ユーザーID	初期 パスワード	初期割り当て ロール	説明
ビルトイン アカウント	root （変更不可）	storage （変更可）	Account Administrator (View and Modify)	Account Authentication 機能にあらかじめ登録されているアカウント。
一般 アカウント	ユーザー任意（登録後変更不可）	ユーザー任意	ユーザー任意	Account Authentication のインストール後に任意に作成可能なアカウント。

注意 1：ビルトインアカウントの初期パスワードは推測されやすいものであるため、インストール後は必ず変更してください。
注意 2：ビルトインアカウントのパスワードを紛失した場合、初期パスワードに戻すことができません。そのため、ビルトインアカウントのパスワード管理には十分注意してください。

ビルトインアカウントは上位管理者（スーパーユーザー）として利用することを目的としています。そのため、ビルトインアカウントに対しては、表 2-5の操作は実行できません。一般アカウントではすべて実行できます。

表 2-5　アカウント種類別の設定制限

種別	アカウントの削除	Account Administrator (View and Modify) ロールの削除	アカウント無効化
ビルトイン アカウント	不可	不可	不可
一般 アカウント	可	可	可

注意：ビルトインアカウントでログインした場合は、**常に更新モードのセッションでのログイン**となり、すでにログイン中のビルトインアカウントはログアウトされます（ビルトインアカウントによる 2 重ログインはできません。すでにログイン中のビルトインアカウントのセッションが破棄されます。セッションと管理モードについては「2.3.5　セッション」、「2.3.6　セッションの種別とリソース操作権限の移行」を参照してください）。

2.3.3　ロール

ロールとは、アレイ装置内のリソースへの操作権限（「参照および更新（View and Modify）」または「参照（View Only）」）を定義した情報です。アカウントにロールを割り当てることで、そのアカウントのリソースに対する操作を制限することができます。

各ロールは、アレイ装置の管理用途別に用意されています。また、ロールごとに用途に適したリソース操作権限が定義されています。

表 2-6　ロールの種別

ロールの種類	説明	用途
Storage Administrator（View and Modify）	RAID グループ、ボリュームの作成など、ストレージに関するリソースに対して参照・更新を許可する権限	ストレージを管理するユーザーに割り当てます。
Storage Administrator（View Only）	RAID グループ、ボリュームの作成など、ストレージに関するリソースに対して参照のみを許可する権限	ストレージを管理するユーザーに割り当てます。Storage Administrator の更新モードのセッションでログインできなかったユーザーが自動的に割り当てられます。
Account Administrator（View and Modify）	アカウントの作成・設定・削除など、アカウントに関するリソースに対して参照・更新を許可する権限	アカウントの情報を管理するユーザーに割り当てます。
Account Administrator（View Only）	アカウントの作成・設定・削除など、アカウントに関するリソースに対して参照のみを許可する権限	アカウントを参照するユーザーに割り当てます。Account Administrator の更新モードのセッションでログインできなかったユーザーが自動的に割り当てられます。
Audit Log Administrator（View and Modify）	監査ログの送信・エクスポートなど、監査ログに関するリソースに対して参照・更新を許可する権限	監査ログ機能を管理するユーザーに割り当てます。
Audit Log Administrator（View Only）	監査ログの送信・エクスポートなど、監査ログに関するリソースに対して参照のみを許可する権限	監査ログ機能を参照するユーザーに割り当てます。Audit Log Administrator の更新モードのセッションでログインできなかったユーザーが自動的に割り当てられます。

View and Modify：参照および更新、View Only：参照のみ

注意：セッションと管理モードについては、「2.3.5　セッション」、「2.3.6　セッションの種別とリソース操作権限の移行」を参照してください。

2.3.4　リソース

ロールによる参照・更新権限の定義が可能な対象を指します。たとえば、「ボリュームを作成する機能」や「アカウントを削除する機能」がこれに当てはまります（ロールはこれらの機能に対し、参照・更新権限を定義します）。リソースは、対象とする数が多いため、アレイ装置ではリソース群とリポジトリーというグループに分類されています。

表 2-7　リソースグループの定義

リソース群	リポジトリー	説明	対応するリソース
ストレージ管理リソース群	ロール定義リポジトリー	ロールの定義、つまり、各ロールが各リソースに対して、何のアクセス権を保持しているかの情報の格納リポジトリー。 ロールの種類、リソース、操作権限の有無	付録 A 参照
	鍵リポジトリー	機器認証の認証情報（iSCSI の CHAP 認証における、認証名や、シークレット（パスワード））の格納リポジトリー	
	ストレージリソースリポジトリー	ホスト、スイッチ、ボリューム、ポートの情報や、ストレージ管理に関する機能の設定等、ストレージ管理のための格納リポジトリー	
アカウント管理リソース群	アカウントリポジトリー	各アカウントのユーザーID、パスワードなどの情報を格納するリポジトリー	
	ロール割り当てリポジトリー	各アカウントとそこに割り当てるロールとの対応関係の格納リポジトリー	
	アカウント設定リポジトリー	アカウント関連機能の情報の格納リポジトリー。セッションタイムアウト時間やパスワード最小文字等	
監査ログ管理リソース群	監査ログ設定リポジトリー	Audit Logging を設定するためのリポジトリー（転送先ログサーバの IP アドレス設定等）	
	監査ログ	アレイ装置内の監査ログを格納するファイル	

表 2-8にロールとリソースグループの関係を示します。たとえば、Storage Administrator（View and Modify）ロールを割り当てられたアカウントは、鍵リポジトリーおよびストレージの参照・更新を操作することができます。

表 2-8　ロールとリソースグループの関係

ロール名称 ＼ リソースグループ名称	ロール定義リポジトリー	鍵リポジトリー	ストレージリソースリポジトリー	アカウントリポジトリー	ロール割り当てリポジトリー	アカウント設定リポジトリー	監査ログ設定リポジトリー	監査ログ
Storage Administrator (View and Modify)	–	V/M	V/M	×	×	×	×	×
Storage Administrator (View Only)	–	V	V	×	×	×	×	×
Account Administrator (View and Modify)	–	×	×	V/M	V/M	V/M	×	×
Account Administrator (View Only)	–	×	×	V	V	V	×	×
Audit Log Administrator (View and Modify)	–	×	×	×	×	×	V/M	V
Audit Log Administrator (View Only)	–	×	×	×	×	×	V	V

V：参照可（View）、M：更新可（Modify）、V/M：参照/更新可、×：参照/更新不可、–：該当しない

2.3.5　セッション

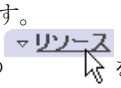
ユーザーのアレイ装置へのログインからログアウトまでをセッションとして管理しています。ログイン実行ごとにセッションを管理しているため、同一ユーザーによる複数ログインも区別されます。
アレイ装置は、ユーザーがログインに成功すると、ユーザーが操作するアプリケーションプログラムに対してセッションIDを発行します。アレイ装置によるセッションIDの最大同時発行数

は256です。つまり、単一のアレイ装置に最大256ユーザーがログインできることになります（同一ユーザーの重複ログインを含む）。

次の場合、セッションIDは削除されます。削除後はアレイ装置に対して操作することはできません。

- ログアウト時
- 強制的にログアウトされたとき
- 無操作の状態がログイン有効期間を超過したとき
- アレイ装置の計画停止時

注意：Hitachi Storage Navigator Modular 2（GUI）を使用している場合、画面右上の[ログアウト]ボタンではアレイ装置からログアウトされず、アレイ装置のセッションタイムアウト時間または Hitachi Storage Navigator Modular 2（GUI）のログイン有効時間（[ログアウト]ボタンでアプリケーションを終了した場合は最大 17 分、  ボタンまたは[閉じる]ボタンでアプリケーションを終了した場合は最大 34 分）の間、アレイ装置のログイン状態が維持されます。

ログアウト後すぐにアレイ装置の設定を変更する必要がある場合は、画面左側の 

をクリックし、アレイ選択画面に戻った後で、[ログアウト]ボタンをクリックして Hitachi Storage Navigator Modular 2（GUI）を終了させてください。

2.3.6 セッションの種別とリソース操作権限の移行

更新権限を持つ複数ユーザーによる単一リソースに対する同時更新を避ける機能です。

参照および更新（View and Modify）権限のロールを保持する複数の一般アカウントが、アレイ装置に対してログインする場合、最初にログインしたアカウントに更新モードの権限が与えられます。2番目以降にログインしたアカウントは、最初にログインした一般アカウントと重複する参照および更新（View and Modify）権限のロールを保持している場合は、参照モードの権限のみが与えられます（リソース操作権限の移行）。

表 2-9 セッションの種別

種別	許可する操作	最大発行数
更新モード	アレイ装置の参照・更新（設定）操作	3（各ロールで 1 ログインのみ）
参照モード	アレイ装置の情報参照のみ	256

たとえば、Storage Administrator (View and Modify)ロールをもつユーザーAが最初にログインしている場合、同じStorage Administrator (View and Modify)ロールを持つ別のユーザーBがログインしたとしても参照モードの権限しか与えられません。この場合、重複したロールのみ参照モードになるのではなく、ユーザーBのもつすべてのロールが参照モードになります。ユーザーBが更新モードを獲得するためには、最初にログインしたユーザーAがログアウトした後にユーザーBが再度ログインする必要があります（ユーザーAがログアウトした場合でも、自動的にユーザーBが更新モードに変更されることはありません）。

また、Storage Administrator (View and Modify)ロールをもつユーザーAが最初にログインしている場合でも、別のAccount Administrator (View and Modify)ロールを持つ別のユーザーCは、ロールが重複しないため、更新モードでログインすることができます。

表 2-10　リソース操作権限の移行

ユーザー	ログイン順	Storage Administrator (View and Modify)	Storage Administrator (View Only)	Account Administrator (View and Modify)	Account Administrator (View Only)	Audit Log Administrator (View and Modify)	Audit Log Administrator (View Only)	獲得できるモード
ユーザーA	1	○			○			更新モード
ユーザーB	2	○		○				参照モード
ユーザーC	3			○				更新モード

○：該当するロールを持つ

ただし、ビルトインアカウントはAccount Administratorロールに関していつでも更新モードのセッションIDでログインします。したがって、ビルトインアカウントのログイン後、ビルトインアカウントと同じ参照および更新（View and Modify）ロールを持ち、更新モードでログイン中の一般アカウントは強制的に参照モードになります。

注意 1：ビルトインアカウントは強力な権限を持つため、他のユーザーに対して十分な注意が必要です。どのユーザーが更新モードでログインしているかという情報については、Account Administrator (View and Modify)または Account Administrator (View Only)を持つユーザーでログインし、アカウント情報の表示を確認することで知ることができます。

注意 2：最初にログインしたアカウントのロールと重複しない種類のロール（View and Modify）をもつアカウントでログインした場合、そのアカウントには、更新モードのセッション ID が与えられます。参照および更新（View and Modify）のロールは 3 種類定義されているため（「表 2-6　ロールの種別」を参照）、最大 3 つの更新モードが発行されます。

注意 3：リソース操作権限の移行はセッション ID 発行中のみ有効です。アカウントに割り当てたロールの参照および更新（View and Modify）権限を変更するものではありません。

2.3.7　警告バナー

警告バナーとは、不正なユーザーに対してその不正アクセスを思いとどまらせるため、また不正アクセスがあった場合の法的処置を円滑に進めやすくするため、管理アプリケーションのすべての利用者に対してログイン前に警告する機能です。警告バナー機能は、Hitachi Storage Navigator Modular 2のGUIまたはCLIのログイン認証において、ログイン前にあらかじめ設定した警告文でバナー表示します。

表 2-11　警告バナー仕様

項目	説明	仕様
警告バナーメッセージ	警告バナーに表示するメッセージ	文字数：1000 文字以内（UTF-8 で 6000 バイト以下。登録する言語により、文字数は前後します。） 使用可能文字種： 0-9、A-Z、a-z、” ! # $ % & ‘ ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~が使用できます。他にも UTF-8 で表現できる文字列も使用できますが、表示するオペレーティングシステム環境によっては、文字化けが発生する場合があります。
警告バナーの有効/無効	警告バナー機能の有効/無効情報	選択範囲：有効、無効

以下に、警告バナーの文面（テンプレート）を示します。お客様のセキュリティポリシーに応じて修正し、使用してください。

和文：

警告

これは{会社名}のコンピュータシステムです．このコンピュータシステムは，承認を受けた人だけがその業務のためにのみ使用できます．承認を受けない人からのアクセスや使用があった場合，侵入者として刑事，民事，および行政上の訴訟を提起する場合があります．

犯罪捜査を含む公の目的のために，このコンピュータシステムに対するすべてのアクセスの履歴は，責任者によって傍受，記録，読み取り，複写，および開示される場合があります．アクセスした人に関する私的な機密情報についても機密性とプライバシーの要件に従って暗号化され，アクセス履歴として記録されます．このシステムを使用する人は，承認を受けているかどうかに関係なく，上記の条件に同意したものとみなします．このシステムにおいてプライバシーの権利はありません．

英文：

```
Warning Notice!

This is a {Company Name Here} computer system, which may be accessed and used
only for authorized {Company Name Here} business by authorized personnel.
Unauthorized access or use of this computer system may subject violators to
criminal, civil, and/or administrative action.

All information on this computer system may be intercepted, recorded, read, copied,
and disclosed by and to authorized personnel for official purposes, including
criminal investigations. Such information includes sensitive data encrypted to
comply with confidentiality and privacy requirements. Access or use of this
computer system by any person, whether authorized or unauthorized, constitutes
consent to these terms. There is no right of privacy in this system.
```

2.3.8 アドバンスドセキュリティモード

アドバンスドセキュリティモードとは、アレイ装置に登録されるパスワード暗号化の強度を高くする機能です。アドバンスドセキュリティモードを有効にすることにより、128ビットの強度をもつ次世代暗号方式でパスワードを暗号化します。

表 2-12　アドバンスドセキュリティモード

項目	説明	仕様
アドバンスドセキュリティモード	アレイ装置にパスワードを登録時に暗号化の強度を選択できます。	選択範囲：有効、無効（デフォルト） 操作権限：ビルトインアカウントのみ 仕様：有効時 SHA256、無効時 MD5 を使用し暗号化します。

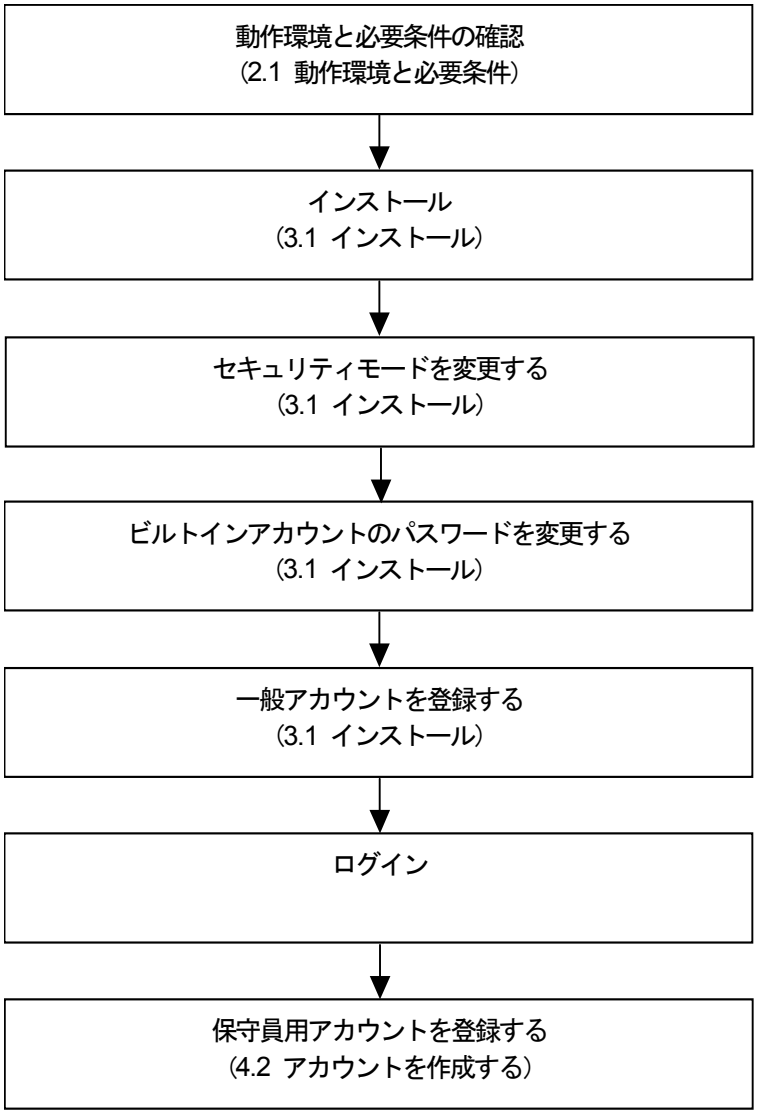
注意 1：アドバンスドセキュリティモードは、ビルトインアカウントのみ操作できます。

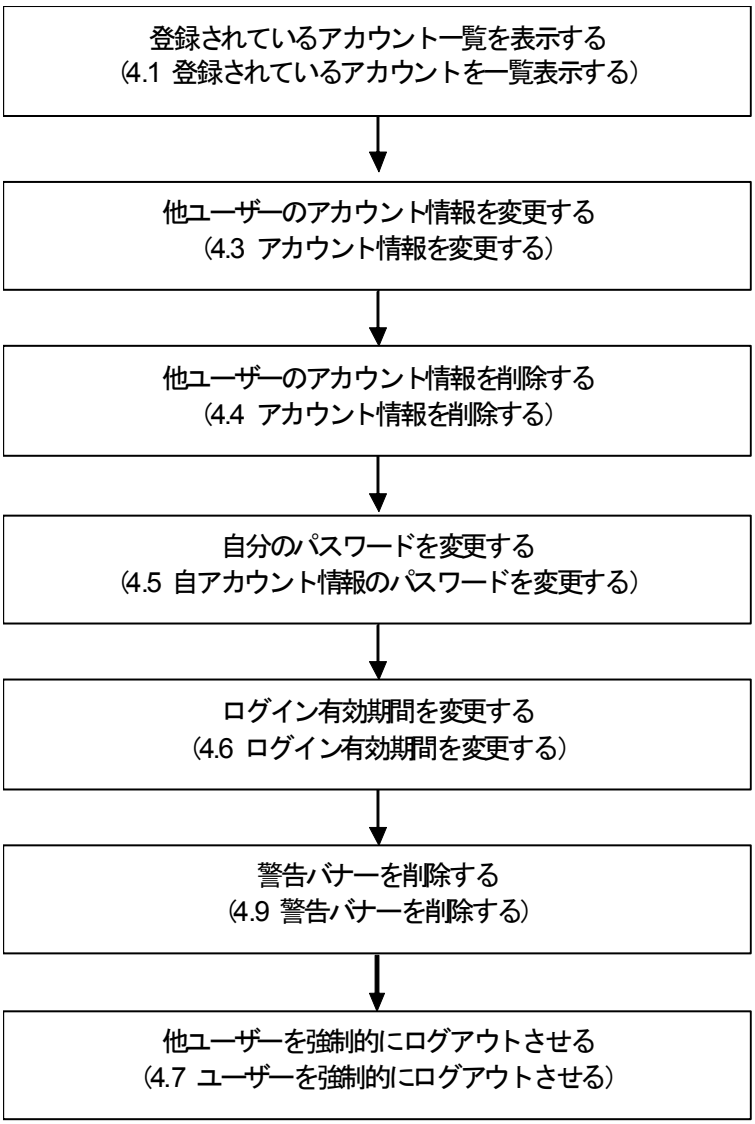
注意 2：アドバンスドセキュリティモードを変更することにより、以下の情報が削除または初期化されます。必要に応じて、設定されている情報を事前に確認し、アドバンスドセキュリティモード変更後に再度設定してください。

- ログイン中のすべてのセッション（ログイン中のアカウントはログアウトされます）
- アレイ装置に登録されているすべての一般アカウント
- ビルトインアカウントのロールとパスワード

2.4 代表的な操作例

Account Authenticationのインストールから基本設定など、代表的な使用手順について説明します。




登録されているアカウント一覧を表示する
(4.1 登録されているアカウントを一覧表示する)
他ユーザーのアカウント情報を変更する
(4.3 アカウント情報を変更する)
他ユーザーのアカウント情報を削除する
(4.4 アカウント情報を削除する)
自分のパスワードを変更する
(4.5 自アカウント情報のパスワードを変更する)
ログイン有効期間を変更する
(4.6 ログイン有効期間を変更する)
警告バナーを削除する
(4.9 警告バナーを削除する)
他ユーザーを強制的にログアウトさせる
(4.7 ユーザーを強制的にログアウトさせる)

3

インストールとアンインストール

ここでは、Hitachi Storage Navigator Modular 2を使用したインストール方法とアンインストール方法について説明します。

本章は以下の内容で構成されています。

3.1 インストール

Account Authenticationはオプション機能のため、通常は選択できない状態（施錠状態）になっています。このオプション機能を使用可能な状態に設定するには、ご購入いただいたAccount Authenticationのオプションをインストールして、機能を選択できる状態（解錠状態）にする必要があります。インストールするためには、Account Authenticationに添付されているキーファイルが必要です。

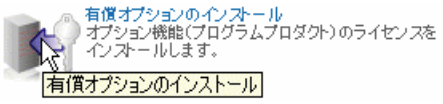
インストールとアンインストールの操作を以下に示します。

Hitachi Storage Navigator Modular 2の操作手順については、「Hitachi Storage Navigator Modular 2のオンラインヘルプ」を参照してください。

注意 1：操作するアレイ装置が正常であることを確認後、インストール／アンインストールしてください。コントローラー閉塞などの障害が発生している場合は、実行できません。

注意 2：Account Authentication は Password Protection と同時に使用することはできません。Account Authentication のインストール時には、Password Protection をアンインストールするか Password Protection を無効に設定する必要があります。

1. Hitachi Storage Navigator Modular 2 を起動してください。
2. 登録済みのユーザーID とパスワードを入力して、Hitachi Storage Navigator Modular 2 にログインしてください。
3. Account Authentication をインストールするアレイ装置を選択してください。
4. **アレイ表示/設定**ボタンをクリックしてください。
5. **コモンアレイタスク**画面から、**有償オプションのインストール**アイコンをクリックしてください。



ライセンス解錠画面が表示されます。

6. **解錠方法**で**キーファイル**のラジオボタンを選択し、**キーファイル**へのパスとキーファイル名を入力し、OK ボタンをクリックしてください。

   キーファイルへのパスの例：HUS110の場合

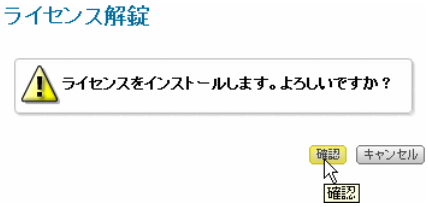
   E:\licensekey\AccountAuthentication\XS\Windows\keyfile

   EはCD-ROMまたはDVD-ROMなどのAccount Authenticationに添付されているCD-Rを装着したドライブレターです。

HUS130の場合、XSはSに置き換えてください。

HUS150の場合、XSはMHに置き換えてください。

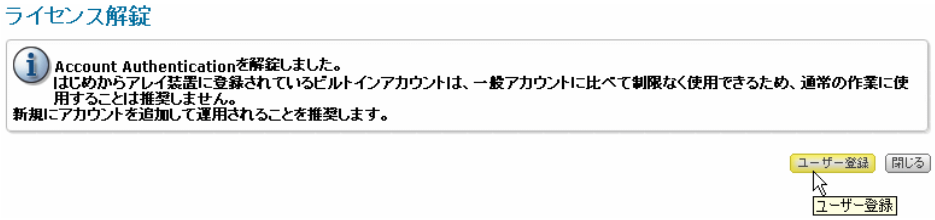
7. 確認メッセージが表示されるので、**確認**ボタンをクリックしてください。



8. 確認メッセージが表示されます。引き続きユーザーを登録する場合は、**ユーザー登録**ボタンをクリックしてください。ユーザーを登録しない場合は、**閉じる**ボタンをクリックし、アレイ装置からログアウトしてください。

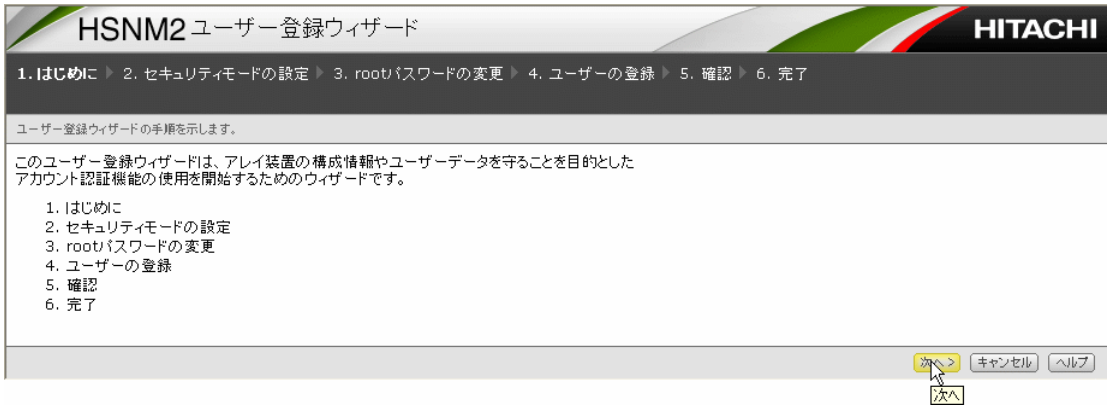
注意1：**ユーザー登録**ボタンが表示されない場合は、**閉じる**ボタンをクリックし、アレイ装置からログアウトしてください。その後ビルトインアカウントでログインし、ユーザーを追加できます。ユーザーの追加は、「4.2　アカウントを作成する」を参照してください。

注意2：ビルトインアカウントでアレイ装置にログインしているユーザーがいる場合、ユーザー登録ボタンが非活性になります。このとき、閉じるボタンをクリックし、アレイ装置からログアウトしてください。



ユーザー登録ボタンをクリックと、**ユーザー登録ウィザード**が表示されます。

注意：**ユーザー登録ウィザード**の表示と同時に、一時的に、アレイ装置にログインしています。ここでは、ビルトインアカウント（root）パスワードの変更、1名のアカウント追加を実行できます。



9. **次へ**ボタンをクリックしてください。

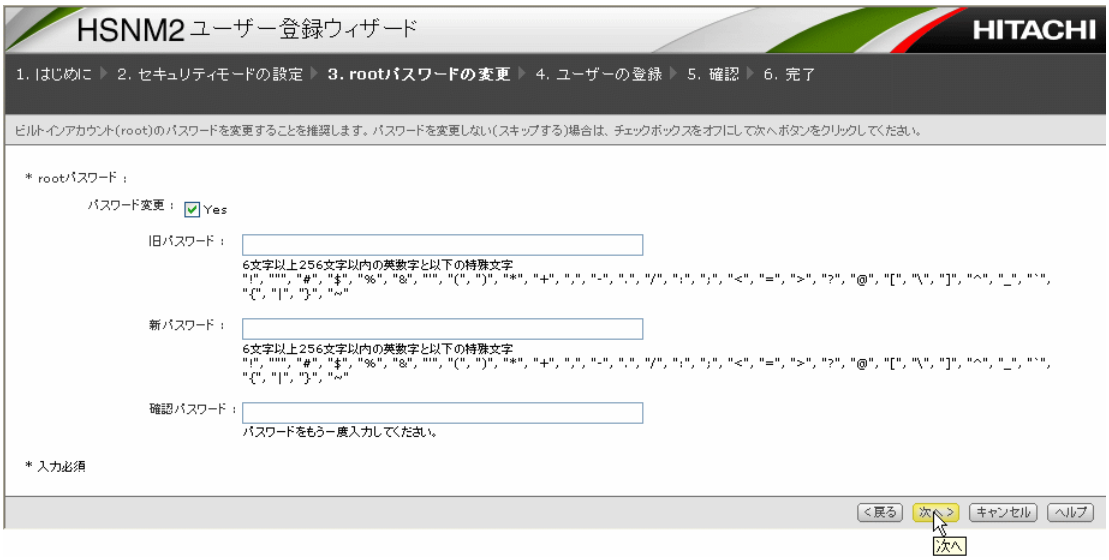
セキュリティモードの設定画面が表示されます。

10. アドバンスドセキュリティモードを有効にする場合は、有効のチェックボックスにチェックを入れ、**次へ**ボタンをクリックしてください。

    アドバンスドセキュリティモードを無効にする場合は、有効のチェックボックスのチェックを外し、**次へ**ボタンをクリックしてください。

    アドバンスドセキュリティモードは後でも変更できますが、アカウントの再登録が必要となるので、アドバンスドセキュリティモードを使用する場合は、ここで有効にすることを推奨します。

    rootパスワードの変更画面が表示されます。



11. **旧パスワード**、**新パスワード**、および**確認パスワード**を入力し、**次へ**ボタンをクリックしてください。

    新パスワードと**確認パスワード**は同じ内容を入力してください。

    パスワードの変更をスキップする場合は、**パスワード変更**のチェックボックスのチェックを外し、**次へ**ボタンをクリックしてください。

    ユーザーの登録画面が表示されます。

12. **ユーザーID**、**アカウント有効/無効**、**パスワード**、および**確認パスワード**を入力または選択してください。

    割り当て可能ロール一覧から、作成したユーザーに割り当てるロールを選択してください。ロールは1個から6個の範囲で割り当てられます。

13. **次へ**ボタンをクリックしてください。

    確認画面が表示されます。

14. 間違いなければ、**確認**ボタンをクリックしてください。間違いがある場合、**戻る**ボタンで戻り修正してください。

    処理中の画面が表示されます。

15. 完了メッセージが表示されるので、**完了**ボタンをクリックしてください。

注意：ビルトインアカウントのパスワードを紛失した場合、初期パスワードに戻すことができません。そのため、ビルトインアカウントのパスワード管理には十分注意してください。

Account Authenticationのインストールが完了しました。

3.2 アンインストール

アンインストールするためには、キーファイルが必要です。一度アンインストールすると、再度キーファイルで解錠するまではAccount Authenticationは使用できません（施錠状態）。

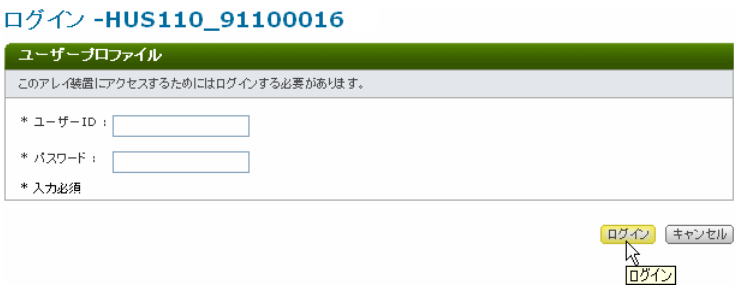
注意 1：アンインストールは、Account Administrator（View and Modify）ロールを割り当てられたアカウントのみで操作できます。

注意 2：アンインストール実行時には、自アカウントを除くログイン中の全アカウントが強制ログアウトされます。全ユーザーの強制ログアウトが完了できない場合、アンインストールは実行できません。

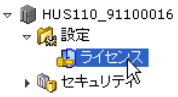
注意 3：アンインストール実行後、ビルトインアカウントを除くすべてのアカウント情報が削除され、ビルトインアカウントのパスワードとロール、セキュリティモードの設定が初期化されます。

Hitachi Storage Navigator Modular 2を使用した場合のアンインストール手順を以下に示します。

1. Hitachi Storage Navigator Modular 2 を起動してください。
2. 登録済みのユーザーID とパスワードを入力して、Hitachi Storage Navigator Modular 2 にログインしてください。
3. Account Authentication をアンインストールするアレイ装置を選択してください。
4. **アレイ表示/設定**ボタンをクリックしてください。
5. **ログイン**ダイアログが表示されるので、Account Administrator（View and Modify）ロールを割り当てたアカウントでログインしてください。



6. **設定**ツリー内の**ライセンス**アイコンをクリックしてください。



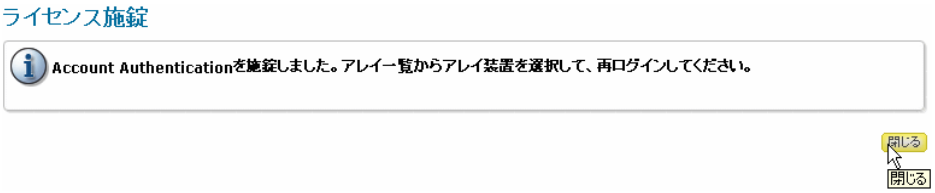
7. **ライセンス施錠**ボタンをクリックしてください。

   ライセンス施錠ダイアログボックスが表示されます。

8. **施錠方法**で**キーファイル**のラジオボタンを選択し、**キーファイル**のパスとキーファイル名を入力し、OK ボタンをクリックしてください。

   キーファイルへのパスの例：HUS110の場合
   E:\licensekey\AccountAuthentication\XS\Windows\keyfile
   EはCD-ROMまたはDVD-ROMなどのAccount Authenticationに添付されているCD-Rを装着したドライブレターです。
   HUS130の場合、XSはSに置き換えてください。
   HUS150の場合、XSはMHに置き換えてください。

9. 確認メッセージが表示されるので、**閉じる**ボタンをクリックしてください。



Account Authenticationのアンインストールが完了しました。

3.3 無効化と有効化の設定

Account Authenticationはインストールされた状態（解錠状態）で、機能の利用の有効化や無効化の設定ができます。

注意 1：機能の有効化や無効化は、Account Administrator（View and Modify）ロールを割り当てられたアカウントのみで操作できます。

注意 2：機能の有効化や無効化実行時には、自アカウントを除くログイン中の全アカウントが強制ログアウトされます。全ユーザーの強制ログアウトが完了できない場合、有効化や無効化は実行できません。

注意 3：機能を無効化すると、認証されなくなります。

注意 4：機能を無効化しても、すべてのアカウント情報は削除されず、そのままアレイ装置に残ります。

注意 5：Account Authentication は Password Protection と同時に使用することはできません。Account Authentication を有効に設定するには、Password Protection を無効に設定する必要があります。

Account Authenticationの利用を有効または無効に設定する手順を次に示します。

Hitachi Storage Navigator Modular 2を使用した場合の設定手順を以下に示します。

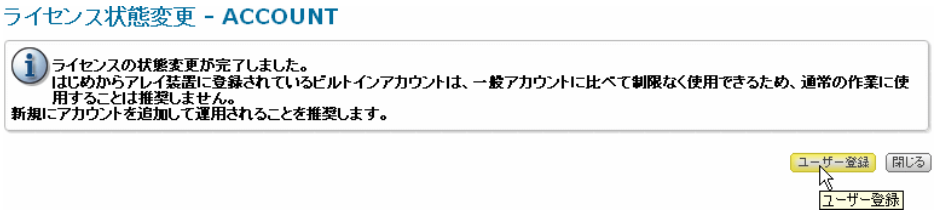
1. Hitachi Storage Navigator Modular 2 を起動してください。
2. 登録済みのユーザーID とパスワードを入力して、Hitachi Storage Navigator Modular 2 にログインしてください。
3. Account Authentication を設定するアレイ装置を選択してください。
4. **アレイ表示/設定**ボタンをクリックしてください。
5. **ログイン**ダイアログが表示されるので、Account Administrator（View and Modify）ロールを割り当てたアカウントでログインしてください。
6. **設定**ツリー内の**ライセンス**アイコンをクリックしてください。
7. **オプション名**内の ACCOUNT を選択し、**状態変更**ボタンをクリックしてください。

   ライセンス状態変更ダイアログボックスが表示されます。

8. 有効化する場合はチェックボックスにチェックを入れ、無効化する場合はチェックボックスのチェックを外し、OK ボタンをクリックしてください。

9. 無効化した場合は、下記のメッセージが表示されるので、**閉じる**ボタンをクリックしてください。

有効化した場合は、下記のメッセージが表示されます。



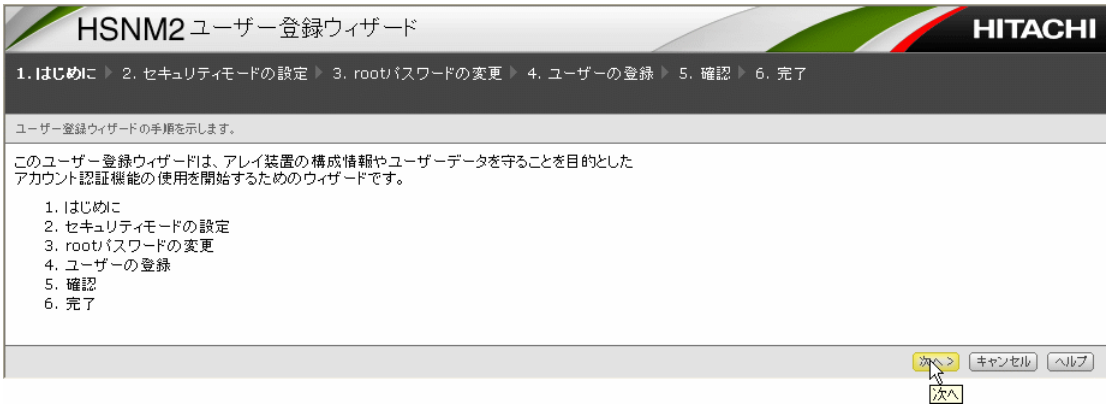
引き続きユーザーを登録する場合は、**ユーザー登録**ボタンをクリックしてください。ユーザーを登録しない場合は、**閉じる**ボタンをクリックし、アレイ装置からログアウトしてください。

注意1：すでにユーザーが登録されている場合など、**ユーザー登録**ボタンが非活性になる場合があります。この場合、**閉じる**ボタンをクリックし、登録済みのユーザーでアレイ装置にログインしてください。

注意2：**ユーザー登録**ボタンが表示されない場合は、**閉じる**ボタンをクリックし、アレイ装置からログアウトしてください。その後ビルトインアカウントでログインし、ユーザーを追加できます。ユーザーの追加は、「4.2　アカウントを作成する」を参照してください。

ユーザー登録ボタンをクリックすると、**ユーザー登録ウィザード**が表示されます。

注意：**ユーザー登録ウィザード**の表示と同時に、一時的に、アレイ装置にログインしています。ここでは、1名のアカウントのみを追加できます。



10. **次へ**ボタンをクリックしてください。

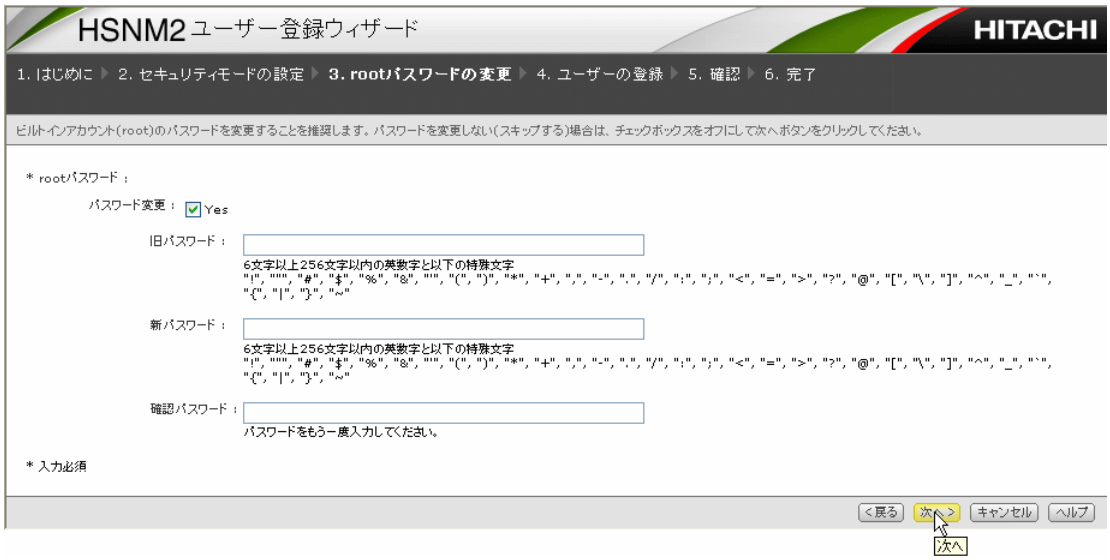
セキュリティモードの設定画面が表示されます。

11. アドバンスドセキュリティモードを有効にする場合は、有効のチェックボックスにチェックを入れ、**次へ**ボタンをクリックしてください。

    アドバンスドセキュリティモードを無効にする場合は、有効のチェックボックスのチェックを外し、**次へ**ボタンをクリックしてください。

    アドバンスドセキュリティモードは後でも変更できますが、アカウントの再登録が必要となるので、アドバンスドセキュリティモードを使用する場合は、ここで有効にすることを推奨します。

    rootパスワードの変更画面が表示されます。



12. **旧パスワード**、**新パスワード**、および**確認パスワード**を入力し、**次へ**ボタンをクリックしてください。

    新パスワードと**確認パスワード**は同じ内容を入力してください。

    パスワードの変更をスキップする場合は、**パスワード変更**のチェックボックスのチェックを外し、**次へ**ボタンをクリックしてください。

    ユーザーの登録画面が表示されます。

13. **ユーザーID**、**アカウント有効/無効**、**パスワード**、および**確認パスワード**を入力または選択してください。

    割り当て可能ロール一覧から、作成したユーザーに割り当てるロールを選択してください。ロールは1個から6個の範囲で割り当てられます。

14. **次へ**ボタンをクリックしてください。

    確認画面が表示されます。

15. 間違いなければ、**確認**ボタンをクリックしてください。間違いがある場合、**戻る**ボタンで戻り修正してください。

    処理中の画面が表示されます。

16. 完了メッセージが表示されるので、**完了**ボタンをクリックしてください。

Account Authenticationの利用の有効化/無効化の設定が完了しました。

4

設定手順

ここではHitachi Storage Navigator Modular 2を使用したアカウントの作成・変更・削除の手順について説明します。

本章は以下の内容で構成されています。

4.1 登録されているアカウントを一覧表示する

アレイ装置に登録されているアカウント情報を表示します。

注意 1：この操作は、Account Administrator（View and Modify）または Account Administrator（View Only）ロールを割り当てられたアカウントのみで操作できます。

注意 2：Hitachi Storage Navigator Modular 2（GUI）を使用している場合、アレイ装置へ Hitachi Storage Navigator Modular 2 をインストールしたサーバを経由して通信するため、セッション情報にはサーバの IP アドレスが表示されます。これにより、別々のクライアントから同じサーバを経由してアレイ装置にログインしている場合には、セッション情報にはログインしているクライアント数のサーバの IP アドレスが表示されます。

注意 3：ネットワークがアドレス変換機能を使用して構成されている場合、ルータ等で送信元 IP アドレスは書き換えられます。これにより、セッション情報には本来の送信元 IP アドレスが表示されない場合があります。

Hitachi Storage Navigator Modular 2を使用した場合の表示手順を以下に示します。

1. Hitachi Storage Navigator Modular 2 を起動してください。
2. 登録済みのユーザーID とパスワードを入力して、Hitachi Storage Navigator Modular 2 にログインしてください。
3. アカウント情報を表示したいアレイ装置を選択してください。
4. **アレイ表示/設定**ボタンをクリックしてください。
5. **ログイン**ダイアログが表示されるので、Account Administrator（View and Modify）ロールを割り当てたアカウントでログインしてください。
6. **セキュリティ**ツリー内の**アカウント認証**アイコンを選択してください。

   登録されているアカウント情報が表示されます。

図 4-1　アカウント認証情報の表示

表 4-1　アカウント情報の表示内容

項目	内容	説明
ユーザーID	root	ビルトインアカウント
	User001	一般アカウント
アカウントタイプ	ビルトイン	ビルトインアカウント
	一般	一般アカウント
アカウント有効/無効	有効	アカウントが有効な状態
	無効	アカウントが無効な状態
セッション数	1	セッション数が 1
	0	セッション数が 0
更新権限	有	セッション ID が更新モード（更新権限がある）
	---	セッション ID が参照モード（更新権限がない）

7. セッション数が 1 以上の場合には、セッション一覧を参照できます。セッション数の数字をクリックしてください。ログインされているセッション情報が表示されます。

図 4-2　セッション情報の表示

表 4-2　セッション情報の表示内容

項目	内容	説明
更新権限	有	セッション ID が更新モード（更新権限がある）
	無	セッション ID が参照モード（更新権限がない）
IP アドレス	IPv4 アドレス	IPv4 アドレス
	IPv6 アドレス	IPv6 アドレス

4.2 アカウントを作成する

アカウント情報の作成手順について説明します。

注意 1：この操作は、Account Administrator（View and Modify）ロールを割り当てられたアカウントのみで操作できます。Account Authentication 機能のインストール直後はビルトインアカウントでログインし、アカウント情報を作成してください。

注意 2:アカウント情報作成時は､任意のユーザーID とパスワードを登録する必要があります。ユーザーID とパスワードは推測されにくい文字列を登録することを推奨します。

以下に示す文字列は、特に、推測され易いので、できる限り使用しないよう、
ISO/IEC 17799 (BS 7799)に規定されています。
Built_in_user、Admin、Administrator、Administrators、root、Authentication、Authentications、Guest、Guests、Anyone、Everyone、System、Maintenance、Developer、Supervisor

注意 3：アカウントを利用するユーザーは、作成後に直ちにログインし、パスワードを変更することを推奨します（アカウント作成者が初期パスワードを記憶し、不正にログインしてしまう可能性があるため)。

注意 4：パスワードは 8 文字以上を推奨します。(6 文字以上 256 文字の範囲で指定できます。)

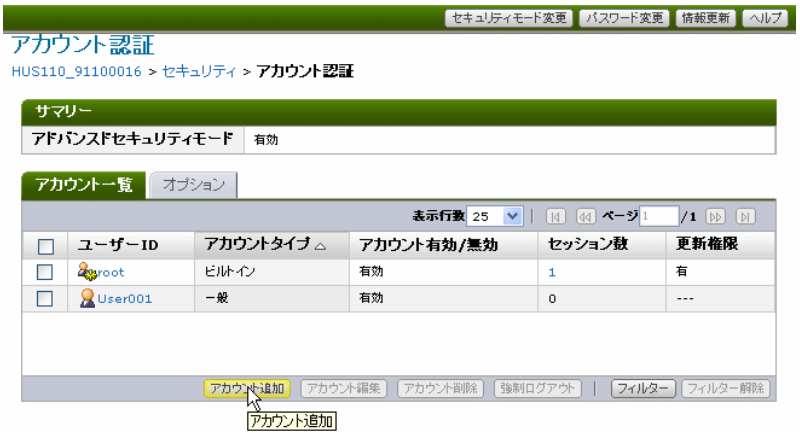
注意 5：Hitachi Storage Navigator Modular 2 を使用して障害を監視する場合、アカウント管理用対象装置は、ログインしないと障害監視ができないため、障害監視時に使用する共通の監視用ユーザーID とパスワードを登録してください。アカウント管理が有効な各装置には、あらかじめ障害監視用のユーザーID とパスワードを作成しておく必要があります。

注意 6:Hitachi Storage Navigator Modular 2 とアレイ装置に同一ユーザーID のアカウントを作成する場合、Hitachi Storage Navigator Modular 2 のアカウントを使用してアレイ装置にログインを試みます。そのため、異なるパスワードを登録している場合にはログインに失敗します。同一ユーザーID のアカウントを作成する場合、同じパスワードを登録してください。この際、サポートされている文字数および文字種を確認してから指定してください。具体的には、文字数は 6 文字以上が必要であり、8 文字以上を推奨します。

Hitachi Storage Navigator Modular 2を使用した場合のアカウント情報の作成手順を以下に示します。

1. Hitachi Storage Navigator Modular 2 を起動してください。
2. 登録済みのユーザーID とパスワードを入力して、Hitachi Storage Navigator Modular 2 にログインしてください。
3. アカウント情報を作成したいアレイ装置を選択してください。
4. **アレイ表示/設定**ボタンをクリックしてください。
5. **ログイン**ダイアログが表示されるので、Account Administrator（View and Modify）ロールを割り当てたアカウントでログインしてください。
6. **セキュリティ**ツリー内の**アカウント認証**アイコンを選択してください。

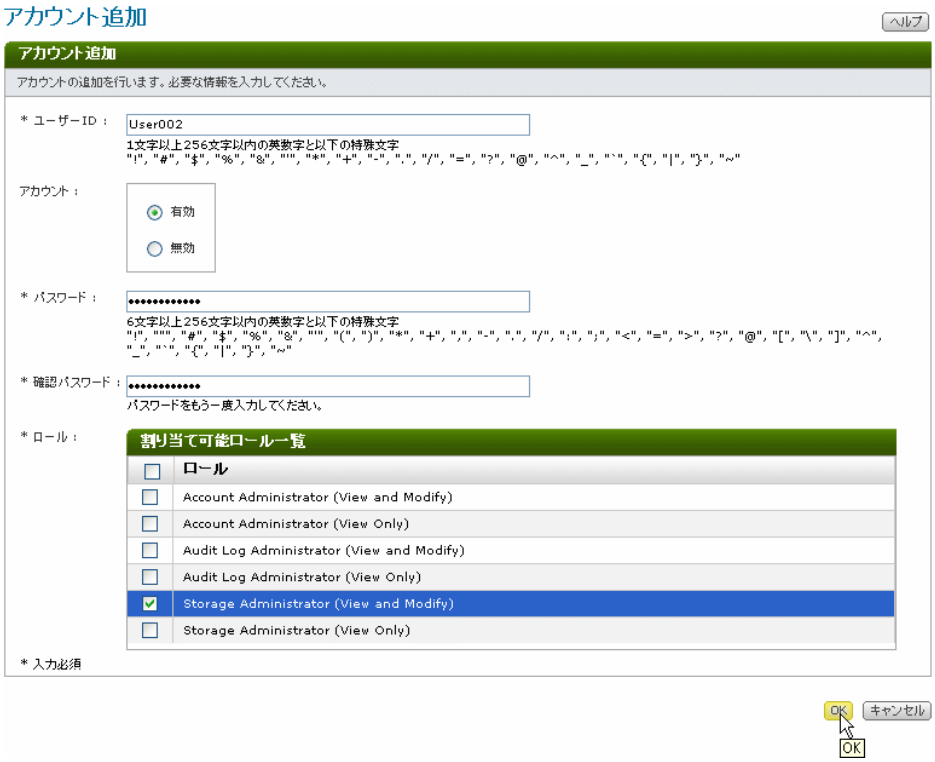
図 4-3　アカウント情報の作成



7. **アカウント追加**ボタンをクリックしてください。

   アカウント追加画面が表示されます。

図 4-4　アカウント追加画面



8. **ユーザーID**、**アカウント有効/無効**、**パスワード**、および**確認パスワード**を入力または選択してください。

9. **割り当て可能ロール一覧**から、作成したユーザーに割り当てるロールを選択してください。ロールは 1 個から 6 個の範囲で割り当てられます。

10. OK ボタンをクリックしてください。

11. 確認メッセージが表示されるので、**閉じる**ボタンをクリックしてください。

作成したアカウント情報が表示されます。

4.3 アカウント情報を変更する

アレイ装置に登録されているアカウント情報を変更します。変更できるアカウント情報は、以下の3つです。

- パスワード
- ロールの割り当て
- アカウントの有効/無効

注意 1：この操作は、Account Administrator（View and Modify）ロールを割り当てられたアカウントのみで操作できます。

注意 2：ここで説明するアカウント情報の変更手順は、他ユーザーのアカウントに対して実行できます。自アカウント情報は変更できません。ただし、ビルトインアカウントは自アカウント情報を変更できます。

注意 3：変更したアカウント情報は、当該アカウントの次回ログイン時から適用されます。

注意 4：一般アカウントはビルトインアカウント情報を変更できません。

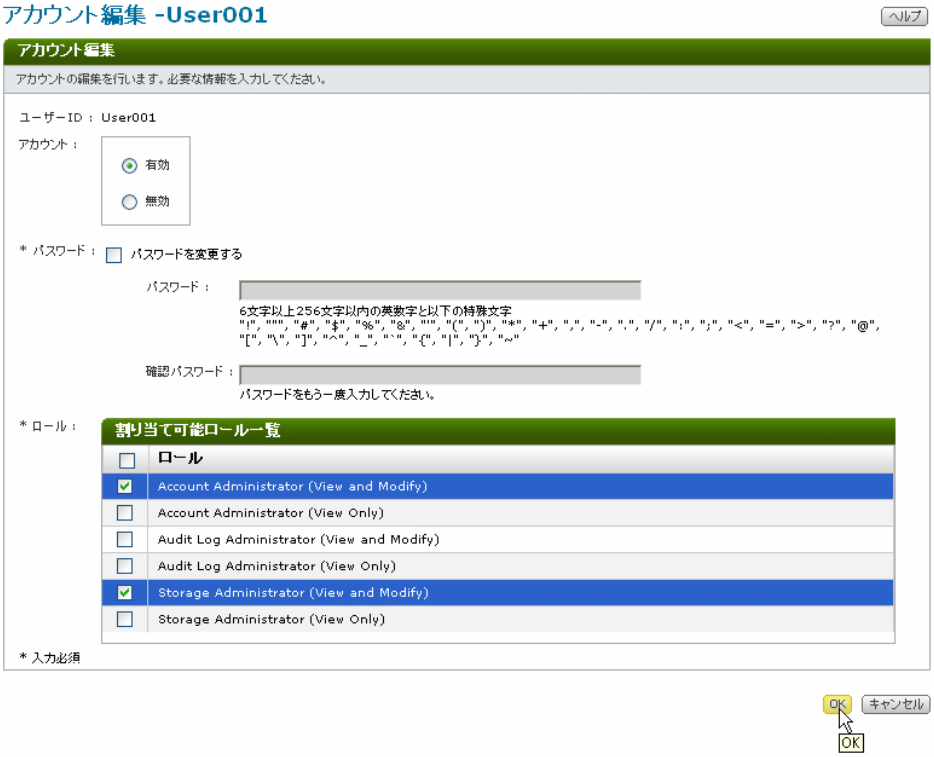
注意 5：一般アカウント、ビルトインアカウントともユーザーID の変更はできません。

Hitachi Storage Navigator Modular 2を使用した場合のアカウント情報の変更手順を以下に示します。

1. Hitachi Storage Navigator Modular 2 を起動してください。
2. 登録済みのユーザーID とパスワードを入力して、Hitachi Storage Navigator Modular 2 にログインしてください。
3. アカウント情報を変更したいアレイ装置を選択してください。
4. **アレイ表示/設定**ボタンをクリックしてください。
5. **ログイン**ダイアログが表示されるので、Account Administrator（View and Modify）ロールを割り当てたアカウントでログインしてください。
6. **セキュリティ**ツリー内の**アカウント認証**アイコンを選択してください。
7. **アカウント一覧**から変更したいアカウントを選択し、**アカウント編集**ボタンをクリックしてください。

   アカウント編集画面が表示されます。

図 4-5　アカウント編集画面



8. **アカウント有効/無効**または**パスワード**、および**確認パスワード**を入力または選択してください。

9. **割り当て可能ロール一覧**から、選択したユーザーに割り当てるロールを選択してください。

10. OK ボタンをクリックしてください。

11. 確認メッセージが表示されるので、**確認**ボタンをクリックしてください。

12. 確認メッセージが表示されるので、**閉じる**ボタンをクリックしてください。

変更したアカウント情報が表示されます。

4.4 アカウント情報を削除する

アカウント情報の削除手順について説明します。

注意 1：この操作は、Account Administrator（View and Modify）ロールを割り当てられたアカウントのみで操作できます。

注意 2：自アカウントとビルトインアカウントは削除できません。

注意 3：ログイン中のユーザーアカウントを削除すると、そのユーザーは直ちに強制ログアウトとなります。

Hitachi Storage Navigator Modular 2を使用した場合のアカウント情報の削除手順を以下に示します。

1. Hitachi Storage Navigator Modular 2 を起動してください。
2. 登録済みのユーザーID とパスワードを入力して、Hitachi Storage Navigator Modular 2 にログインしてください。
3. アカウント情報を削除したいアレイ装置を選択してください。
4. **アレイ表示/設定**ボタンをクリックしてください。
5. **ログイン**ダイアログが表示されるので、Account Administrator（View and Modify）ロールを割り当てたアカウントでログインしてください。
6. **セキュリティ**ツリー内の**アカウント認証**アイコンを選択してください。
7. **アカウント一覧**から削除したいアカウントを選択し、**アカウント削除**ボタンをクリックしてください。
8. 確認メッセージが表示されるので、**確認**ボタンをクリックしてください。
9. 確認メッセージが表示されるので、**閉じる**ボタンをクリックしてください。

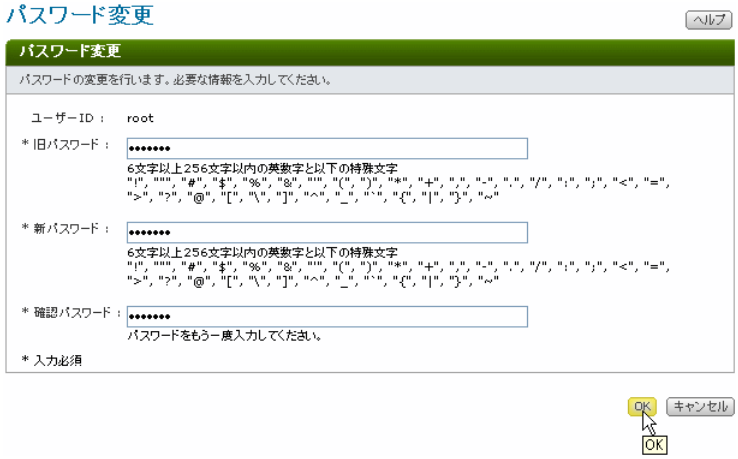
削除したアカウント情報が表示されなくなります。

4.5 自アカウント情報のパスワードを変更する

Hitachi Storage Navigator Modular 2を使用した場合のパスワードの変更手順を以下に示します。

1. Hitachi Storage Navigator Modular 2 を起動してください。
2. 登録済みのユーザーID とパスワードを入力して、Hitachi Storage Navigator Modular 2 にログインしてください。
3. パスワードを変更したいアレイ装置を選択してください。
4. **アレイ表示/設定**ボタンをクリックしてください。
5. **ログイン**ダイアログが表示されるので、パスワードを変更したいアカウントでログインしてください。
6. **セキュリティ**ツリー内の**アカウント認証**アイコンを選択してください。
7. **アカウント一覧**から**パスワード変更**ボタンをクリックしてください。

   パスワード変更画面が表示されます。



8. **旧パスワード**、**新パスワード**、および**確認パスワード**を入力し、OK ボタンをクリックしてください。

   新パスワードと**確認パスワード**は同じ内容を入力してください。**新パスワード**と**確認パスワード**に入力できる文字数と文字種については、「表 2-3　アカウント仕様」を参照してください。

9. 確認メッセージが表示されるので、**閉じる**ボタンをクリックしてください。

4.6 ログイン有効期間を変更する

アレイ装置に登録されているログイン有効期間を変更します。

注意：この操作は、Account Administrator（View and Modify）ロールを割り当てられたアカウントのみで操作できます。

Hitachi Storage Navigator Modular 2を使用した場合の表示手順を以下に示します。

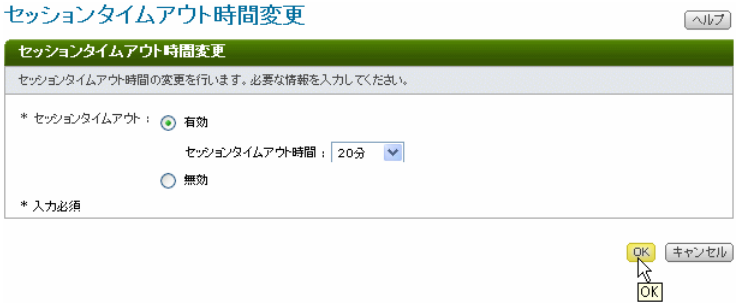
1. Hitachi Storage Navigator Modular 2 を起動してください。
2. 登録済みのユーザーID とパスワードを入力して、Hitachi Storage Navigator Modular 2 にログインしてください。
3. ログイン有効期間を変更したいアレイ装置を選択してください。
4. **アレイ表示/設定**ボタンをクリックしてください。
5. **ログイン**ダイアログが表示されるので、Account Administrator（View and Modify）ロールを割り当てられたアカウントでログインしてください。
6. **セキュリティ**ツリー内の**アカウント認証**アイコンを選択してください。
7. **オプション**タブをクリックしてください。

図 4-6　セッションタイムアウト時間の変更

8. **セッションタイムアウト時間変更**ボタンをクリックしてください。

   セッションタイムアウト時間変更画面が表示されます。

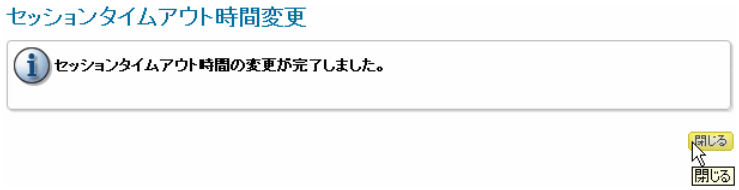
図 4-7　セッションタイムアウト時間の変更



9. **セッションタイムアウト**の有効・無効を選択します。**セッションタイムアウト時間**をドロップダウンリストから選択し、OK ボタンをクリックしてください。

セッションタイムアウト時間：20分、25分、30分、35分、40分、45分、50分、55分、60分、70分、80分、90分、100分、110分、120分、24時間

10. 確認メッセージが表示されるので、**閉じる**ボタンをクリックしてください。



4.7 ユーザーを強制的にログアウトさせる

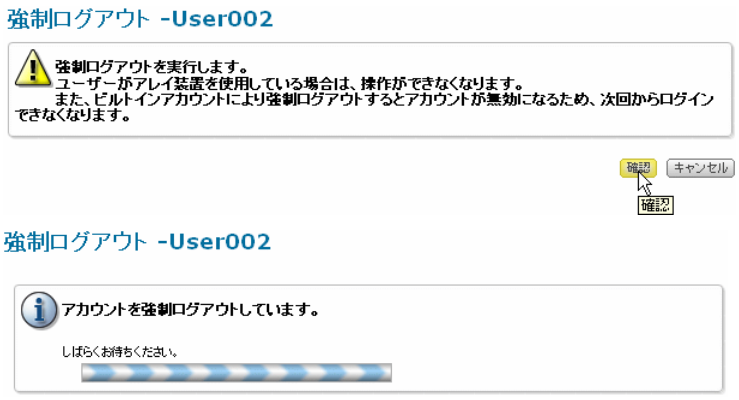
アレイ装置にログインしているビルトインアカウントを除く他のユーザーを強制的にログアウトさせます。主に、不正なユーザーに対して強制的にログアウトさせます。

注意 1：アカウントのログイン中に、アレイ装置のコントローラー障害が発生した場合、ログイン中のセッション ID がアレイ装置内に残ってしまう場合があります。
したがって、コントローラー障害が発生した場合、Account Administrator（View and Modify）ロールを割り当てられたアカウントで、セッション ID の残っているアカウントをすべて強制ログアウトしてください。

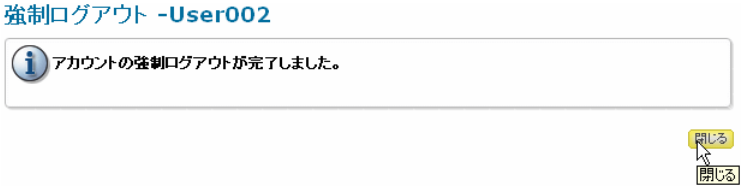
注意 2：強制ログアウトされたアカウントは無効になります。Account Administrator（View and Modify）ロールを割り当てられたアカウントで有効にしない限り、当該アカウントでの再ログインはできません。一般アカウントによる強制ログアウトでは無効になりません。

1. Hitachi Storage Navigator Modular 2 を起動してください。
2. 登録済みのユーザーID とパスワードを入力して、Hitachi Storage Navigator Modular 2 にログインしてください。
3. 強制的にログアウトさせたいユーザーが登録されているアレイ装置を選択してください。
4. **アレイ表示/設定**ボタンをクリックしてください。
5. **ログイン**ダイアログが表示されるので、Account Administrator（View and Modify）ロールを割り当てたアカウントでログインしてください。
6. **セキュリティ**ツリー内の**アカウント認証**アイコンを選択してください。
7. **アカウント一覧**から強制的にログアウトさせたいアカウントを選択し、**強制ログアウト**ボタンをクリックしてください。
8. 確認メッセージが表示されるので、**確認**ボタンをクリックしてください。

図 4-8　強制ログアウト



9. 確認メッセージが表示されるので、**閉じる**ボタンをクリックしてください。

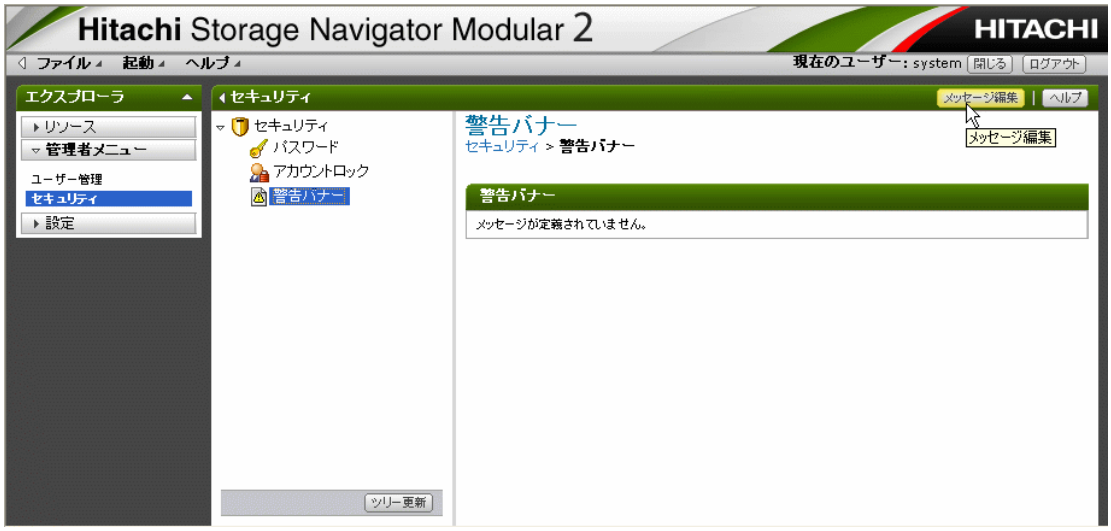


4.8 警告バナーを設定する

Hitachi Storage Navigator Modular 2の警告バナーを設定します。

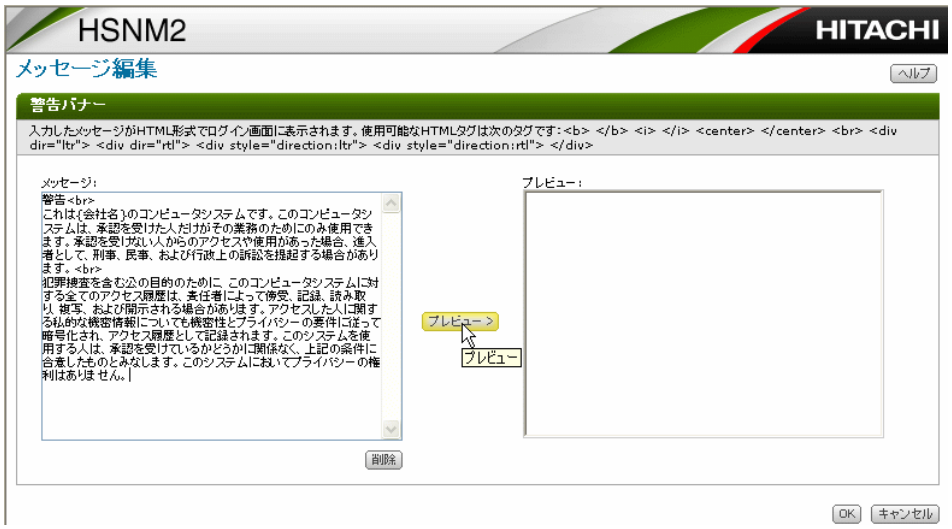
1. Hitachi Storage Navigator Modular 2 を起動してください。
2. 登録済みのユーザーID とパスワードを入力して、Hitachi Storage Navigator Modular 2 にログインしてください。
3. **エクスプローラ**内の**管理者メニュー**から**セキュリティ**を選択してください。
4. **セキュリティ**メニュー内の**警告バナー**を選択してください。
5. **メッセージ編集**ボタンをクリックしてください。

図 4-9　警告バナーの設定



メッセージ編集画面が表示されます。

図 4-10　警告バナーの編集



6. **メッセージ**フレームに適切なテキストを入力し、**プレビュー**ボタンをクリックしてください。
7. **プレビュー**フレームに表示された内容を確認し、OK ボタンをクリックしてください。

8. 図 4-9 に設定した内容が表示されるので、ログアウトボタンをクリックしてください。

9. 再度、Hitachi Storage Navigator Modular 2 を起動してください。

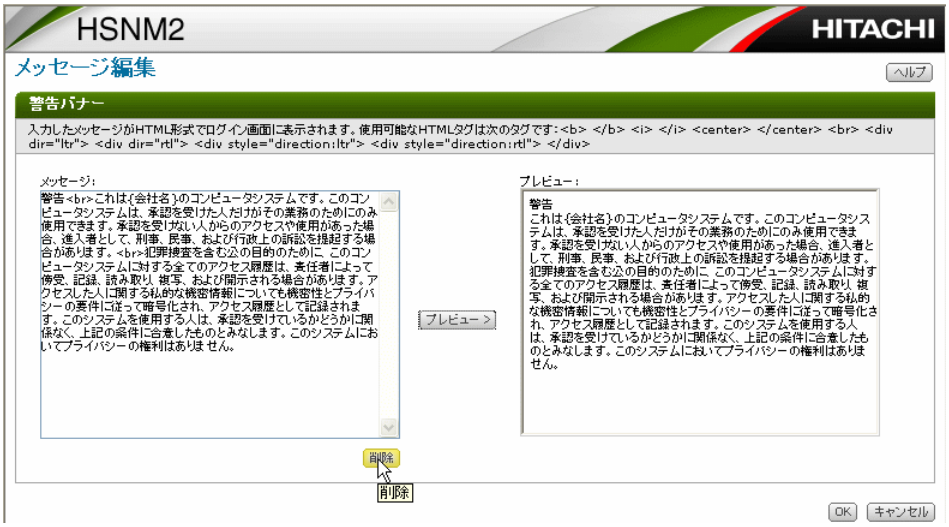
   ログイン画面に変更した警告バナーが表示されます。

4.9 警告バナーを削除する

Hitachi Storage Navigator Modular 2の警告バナーを削除します。

1. Hitachi Storage Navigator Modular 2 を起動してください。
2. 登録済みのユーザーID とパスワードを入力して、Hitachi Storage Navigator Modular 2 にログインしてください。
3. **エクスプローラ**内の**管理者メニュー**から**セキュリティ**を選択してください。
4. **セキュリティ**メニュー内の**警告バナー**を選択してください。
5. **メッセージ編集**ボタンをクリックしてください。

   メッセージ編集画面が表示されます。



6. **削除**ボタンをクリックしてください。
7. OK ボタンをクリックしてください。
8. ログアウト ボタンをクリックしてください。
9. 再度、Hitachi Storage Navigator Modular 2 を起動してください。
10. ログイン画面に警告バナーが表示されないことを確認してください。

4.10 アドバンスドセキュリティモードを変更する

アドバンスドセキュリティモードを変更します。

注意 1：アドバンスドセキュリティモードは、ビルトインアカウントのみ操作できます。

注意 2：アドバンスドセキュリティモードを変更することにより、以下の情報が削除または初期化されます。必要に応じて、設定されている情報を事前に確認し、アドバンスドセキュリティモード変更後に再度設定してください。

- ログイン中のすべてのセッション（ログイン中のアカウントはログアウトされます）
- アレイ装置に登録されているすべての一般アカウント
- ビルトインアカウントのロールとパスワード

Hitachi Storage Navigator Modular 2を使用した場合の変更手順を以下に示します。

1. Hitachi Storage Navigator Modular 2 を起動してください。
2. 登録済みのユーザーID とパスワードを入力して、Hitachi Storage Navigator Modular 2 にログインしてください。
3. アドバンスドセキュリティモードを変更したいアレイ装置を選択してください。
4. **アレイ表示/設定**ボタンをクリックしてください。
5. **ログイン**ダイアログが表示されるので、ビルトインアカウントでログインしてください。
6. **セキュリティ**ツリー内の**アカウント認証**アイコンを選択してください。
7. 画面右上にある**セキュリティモード変更**ボタンをクリックしてください。

   セキュリティモード変更画面が表示されます。

図 4-11　セキュリティモードの変更

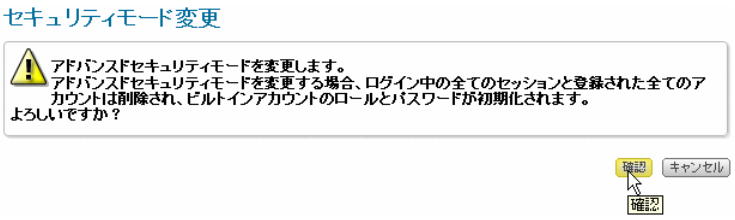
8. **アドバンスドセキュリティモード**の有効・無効を変更します。

   有効にする場合は、有効のチェックボックスにチェックを入れ、OKボタンをクリックしてください。

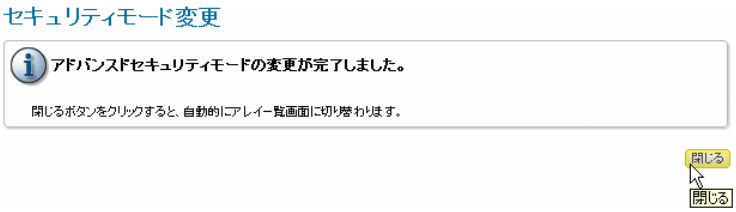
   無効にする場合は、有効のチェックボックスのチェックを外し、OKボタンをクリックしてください。

9. 確認メッセージが表示されるので、承認する場合は、**確認**ボタンをクリックしてください。

   承認しない場合は、**キャンセル**ボタンをクリックしてください。



10. 確認メッセージが表示されるので、**閉じる**ボタンをクリックしてください。


セキュリティモード変更
アドバンスドセキュリティモードの変更が完了しました。
閉じるボタンをクリックすると、自動的にアレイ一覧画面に切り替わります。
閉じる
閉じる

5

トラブルシューティング

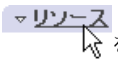
本章は以下の内容で構成されています。

5.1 トラブルシューティング

5.1.1 更新権限（View and Modify）を取れない場合

（1）更新権限（View and Modify）をもつユーザーでHitachi Storage Navigator Modular 2（GUI）にログインし、画面右上の ログアウト ボタン、 ボタン、または 閉じる ボタンでアプリケーションを終了させ、続けてログインした場合、更新権限（View and Modify）を確保できず参照権限（View Only）となる場合があります。

この問題が発生した場合、アレイ装置のセッションタイムアウト時間（初期値:20分）またはHitachi Storage Navigator Modular 2（GUI）のログイン有効時間（ ログアウト ボタンでアプリケーションを終了した場合は最大17分、 ボタンまたは 閉じる ボタンでアプリケーションを終了した場合は最大34分）の間、アレイ装置のログイン状態が維持されます。

ログアウト後すぐに続けてアレイ装置の設定を変更する必要がある場合は、画面左側の 

をクリックし、アレイ選択画面に戻った後で、 ログアウト ボタンをクリックしてHitachi Storage Navigator Modular 2（GUI）を終了させ、続けてログインしてください。

（2）「4.1　登録されているアカウントを一覧表示する」を参照し、更新権限を持つアカウントを確認してください。また、セッション数が1以上の場合には、セッションごとに更新権限とIPアドレスを確認できます。
更新権限を持つアカウントを使用しているユーザーを特定できない等により、当該アカウントを強制的にログアウトさせるには、「4.7　ユーザーを強制的にログアウトさせる」を参照してください。

5.1.2 更新権限（View and Modify）のはく奪が頻発する場合

更新権限（View and Modify）をもつユーザーでHitachi Storage Navigator Modular 2（GUI）にログインし、操作中に更新権限のはく奪（DMED1F0029: 更新権限がありません。アカウント管理者に連絡して、権限を確認してください。）が頻発する場合、以下の原因が考えられます。

- Hitachi Storage Navigator Modular 2 などによる障害監視をビルトインアカウントで実施している。
- 他の管理用 PC から、アレイ装置にビルトインアカウントでログインを実施した。

ビルトインアカウントでログインした場合、更新権限がビルトインアカウントに移り、ログイン中の一般アカウントの更新権限ははく奪されます。ビルトインアカウントは上位管理者（スーパーユーザー）として利用することが目的であるため、日常的な使用においては、必要な操作権限を持つ一般アカウントを作成し、使用してください。

障害監視を行う場合は、Storage Administrator（View Only)の権限のみを持つ障害監視用アカウントを作成することを推奨します。

5.1.3 セッションタイムアウトが頻発する場合

ビルトインアカウントでHitachi Storage Navigator Modular 2（GUI）にログインし、操作中にセッションタイムアウト（DMEG100013 セッションタイムアウトが発生しました。アレイ画面に戻り、再度アレイ装置を選択してください。）が頻発する場合、以下の原因が考えられます。

- Hitachi Storage Navigator Modular 2 などによる障害監視をビルトインアカウントで実施している。
- 他の管理用 PC から、アレイ装置にビルトインアカウントでログインを実施した。

ビルトインアカウントでログイン中に、さらにビルトインアカウントで同じアレイ装置にログインした場合、すでにログイン中のビルトインアカウントのセッションは破棄され、後からログインしたビルトインアカウントのセッションが有効になります。ビルトインアカウントは上位管理者（スーパーユーザー）として利用することが目的であるため、日常的な使用においては、必要な操作権限を持つ一般アカウントを作成し、使用してください。

障害監視を行う場合は、Storage Administrator（View Only）の権限のみを持つ障害監視用アカウントを作成することを推奨します。

5.2 お問い合わせ先

サポートサービス利用ガイドに記載された連絡先にお問い合わせください。

A

ロールとリソースの操作権限

ロール	Storage Administrator				Account Administrator						Audit Log Administrator			
リポジトリー	鍵		ストレージリソース		アカウント		ロール割り当て		アカウント設定		監査ログ設定		監査ログ	
リソース	V/M	V	V/M	V	V/M	V	V/M	V	V/M	V	V/M	V	V/M	V
ライセンスキー設定														
解錠			○								○			
施錠			○						○		○			
有効/無効			○						○		○			
ストレージ設定														
RAID Group/ボリュームなどの参照			○	○										
RAID Group/ボリュームなどの設定			○											
アカウント設定														
強制ログアウト					○		○							
アカウント作成					○		○							
アカウント変更					○		○							
アカウント削除					○		○							
自パスワード変更	○	○	○	○	○	○	○	○	○	○	○	○	○	○
アカウント情報表示					○	○	○	○						
監査ログ設定														
内部保存ログの初期化													○	
内部保存ログのエクスポート													○	○
Syslog サーバの設定											○			
内部保存ログの有効/無効											○			

V/M: View and Modify　V: View Only　○：実行可能

注意：Account Authentication がインストール済みである場合、ロールごとのライセンスキー設定には以下の制限があります。

- Storage Administrator は Account Authentication と Audit Logging 以外のライセンスキー設定が可能です。
- Account Administrator は Account Authentication のみのライセンスキー設定が可能です。ただし、解錠はできません（Account Authentication インストール前であるため）。
- Audit Log Administrator は Audit Logging のみのライセンスキー設定が可能です。

B

CLIでの操作

ここでは、Hitachi Storage Navigator Modular 2のCLIを使用した場合の、次に示すAccount Authenticationの操作方法を説明します。

B.1　インストール

Account Authenticationはオプション機能のため、通常は選択できない状態（施錠状態）になっています。このオプション機能を使用可能な状態に設定するには、ご購入いただいたAccount Authenticationのオプションをインストールして、機能を選択できる状態（解錠状態）にする必要があります。インストールするためには、Account Authenticationに添付されているキーファイルが必要です。Hitachi Storage Navigator Modular 2の操作手順については、「Hitachi Storage Navigator Modular 2ユーザーズガイド（for CLI）」を参照してください。

注意 1：操作するアレイ装置が正常であることを確認後、インストール／アンインストールしてください。コントローラー閉塞などの障害が発生している場合は、実行できません。
注意 2：Account Authentication は Password Protection と同時に使用することはできません。Account Authentication のインストール時には、Password Protection をアンインストールするか Password Protection を無効に設定する必要があります。

Account Authenticationをインストールする手順を次に示します。

1. コマンドプロンプト上で、Account Authentication をインストールしたいアレイ装置を登録し、さらにそのアレイ装置に接続してください。
2. auopt コマンドを実行してオプションを解錠してください。入力例および結果を次に示します。

   キーファイルへのパスの例：HUS110の場合
   E:\licensekey\AccountAuthentication\XS\Windows\keyfile
   EはCD-ROMまたはDVD-ROMなどのAccount Authenticationに添付されているCD-Rを装着したドライブレターです。
   HUS130の場合、XSはSに置き換えてください。
   HUS150の場合、XSはMHに置き換えてください。

```
% auopt -unit 装置名 -lock on -licensefile CD-R のキーファイルへのパス\キーファイル名
番号  オプション名称
  1  Account Authentication
解錠するオプションの番号を指定してください。
複数のオプションを解錠する場合はスペース区切りで指定してください。すべて解錠する場合は all を入力してください。終了する場合は q を入力してください。
解錠するオプションの番号 (番号/all/q [all]): 1
オプションを解錠します。
よろしいですか? (y/n [n]): y

オプション名称                                  結果
Account Authentication                          解錠

処理が完了しました。
%
```

3. auopt コマンドを実行してオプションが解錠されたかどうか確認してください。入力例、および結果を次に示します。ユーザ ID に root、パスワードに storage を入力してください（下記は出力項目のイメージです）。

```
% auopt -unit 装置名 -refer
Account Authentication が有効です。ログインしてください。
ユーザ ID: root
パスワード:
オプション名称                  種別        有効期限  状態      使用メモリ再構築状態
ACCOUNT                         Permanent   ---       有効      N/A
%
```

注意 1：ビルトインアカウントの初期パスワードは推測されやすいものであるため、インストール後は必ず変更してください。
注意 2：ビルトインアカウントのパスワードを紛失した場合、初期パスワードに戻すことができません。そのため、ビルトインアカウントのパスワード管理には十分注意してください。

Account Authenticationのインストールが完了しました。

B.2　アンインストール

アンインストールするためには、キーファイルが必要です。一度アンインストールすると、再度キーファイルで解錠するまではAccount Authenticationは使用できません（施錠状態）。

注意 1：アンインストールは、Account Administrator（View and Modify）ロールを割り当てられたアカウントのみで操作できます。

注意 2：アンインストール実行時には、自アカウントを除くログイン中の全アカウントが強制ログアウトされます。全ユーザーの強制ログアウトが完了できない場合、アンインストールは実行できません。

注意 3：アンインストール実行後、ビルトインアカウントを除くすべてのアカウント情報が削除され、ビルトインアカウントのパスワードとロール、セキュリティモードの設定が初期化されます。

Account Authenticationをアンインストールする手順を次に示します。

1. コマンドプロンプト上で、Account Authentication をアンインストールしたいアレイ装置を登録し、さらにそのアレイ装置に接続してください。

2. auopt コマンドを実行してオプションを施錠してください。入力例、および結果を次に示します。

   キーファイルへのパスの例：HUS110の場合
   E:\licensekey\AccountAuthentication\XS\Windows\keyfile
   EはCD-ROMまたはDVD-ROMなどのAccount Authenticationに添付されているCD-Rを装着したドライブレターです。
   HUS130の場合、XSはSに置き換えてください。
   HUS150の場合、XSはMHに置き換えてください。

```
% auopt -unit 装置名 -lock on -licensefile CD-R のキーファイルへのパス\キーファイル名
Account Authentication が有効です。ログインしてください。
ユーザ ID: root
パスワード:
番号  オプション名称
  1  Account Authentication
施錠するオプションの番号を指定してください。
終了する場合は q を入力してください。
施錠するオプションの番号 (番号/q [q]): 1
オプションを施錠します。
よろしいですか? (y/n [n]): y

オプション名称                                  結果
Account Authentication                          施錠

処理が完了しました。
%
```

3. auopt コマンドを実行してオプションが施錠されたかどうか確認してください。入力例および結果を次に示します。

```
% auopt -unit 装置名 -refer
DMEC002015:表示する情報がありません。
%
```

Account Authenticationのアンインストールが完了しました。

B.3　無効化と有効化の設定

Account Authenticationはインストールされた状態（解錠状態）で、機能の利用の有効化や無効化の設定ができます。

注意 1：機能の有効化や無効化は、Account Administrator（View and Modify）ロールを割り当てられたアカウントのみで操作できます。

注意 2：機能の有効化や無効化実行時には、自アカウントを除くログイン中の全アカウントが強制ログアウトされます。全ユーザーの強制ログアウトが完了できない場合、有効化や無効化は実行できません。

注意 3：機能を無効化すると、認証されなくなります。

注意 4：機能を無効化しても、すべてのアカウント情報は削除されず、そのままアレイ装置に残ります。

注意 5：Account Authentication は Password Protection と同時に使用することはできません。Account Authentication を有効に設定するには、Password Protection を無効に設定する必要があります。

Account Authenticationの使用を有効または無効に設定する手順を次に示します。

1. コマンドプロンプト上で、Account Authentication の有効/無効を設定したいアレイ装置を登録し、さらにそのアレイ装置に接続してください。

2. auopt コマンドを実行して有効/無効を設定してください。

   有効状態を無効状態に変更する場合の入力例および結果を次に示します。反対に、無効状態を有効状態に変更する場合は、-stオプションの後にenableと入力してください。

```
% auopt -unit 装置名 -option ACCOUNT -st disable
Account Authentication が有効です。ログインしてください。
ユーザ ID: root
パスワード:
オプションを無効にします。
よろしいですか? (y/n [n]): y
オプション設定が終了しました。
%
```

3. auopt コマンドを実行してオプションの状態を確認してください。入力例および結果を次に示します（下記は出力項目のイメージです）。

```
% auopt -unit 装置名 -refer
オプション名称                  種別        有効期限  状態      使用メモリ再構築状態
ACCOUNT                         Permanent   ---       無効      N/A
%
```

Account Authenticationの利用の有効化/無効化の設定が完了しました。

B.4　アカウント情報の表示

アレイ装置に登録されているアカウント情報を表示します。

注意 1：この操作は、Account Administrator（View and Modify）または Account Administrator（View Only）ロールを割り当てられたアカウントのみで操作できます。

注意 2：Hitachi Storage Navigator Modular 2（GUI）を使用している場合、アレイ装置へ Hitachi Storage Navigator Modular 2 をインストールしたサーバを経由して通信するため、セッション情報にはサーバの IP アドレスが表示されます。これにより、別々のクライアントから同じサーバを経由してアレイ装置にログインしている場合には、セッション情報にはログインしているクライアント数のサーバの IP アドレスが表示されます。

注意 3：ネットワークがアドレス変換機能を使用して構成されている場合、ルータ等で送信元 IP アドレスは書き換えられます。これにより、セッション情報には本来の送信元 IP アドレスが表示されない場合があります。

Account Authentication情報の表示手順を次に示します。

1. コマンドプロンプト上で、Account Authentication 情報を表示したいアレイ装置を登録し、さらにそのアレイ装置に接続してください。

2. auaccount コマンドを実行して Account Authentication 情報を表示してください。

   入力例および結果を次に示します。

```
% auaccount -unit 装置名 -refer
Account Authentication が有効です。ログインしてください。
ユーザ ID: root
パスワード:
ユーザ ID              : root
アカウントタイプ       : ビルトイン
アカウント有効/無効    : 有効
セッション数           : 1
更新権限               : 有
ロール                 : Storage Administrator (View and Modify)
                         Storage Administrator (View Only)
                         Account Administrator (View and Modify)
                         Account Administrator (View Only)
                         Audit Log Administrator (View and Modify)
                         Audit Log Administrator (View Only)
セッション
  更新権限         IP アドレス
  有               40.143.121.240

ユーザ ID              : User001
アカウントタイプ       : 一般
アカウント有効/無効    : 無効
セッション数           : 0
更新権限               : 無
ロール                 : Storage Administrator (View and Modify)
セッション
  更新権限         IP アドレス
%
```

B.5　アカウント情報の作成

アカウント情報の作成手順について説明します。

注意 1：この操作は、Account Administrator（View and Modify）ロールを割り当てられたアカウントのみで操作できます。Account Authentication 機能のインストール直後はビルトインアカウントでログインし、アカウント情報を作成してください。

注意 2:アカウント情報作成時は､任意のユーザーID とパスワードを登録する必要があります。ユーザーID とパスワードは推測されにくい文字列を登録することを推奨します。

以下に示す文字列は、特に、推測され易いので、できる限り使用しないよう、
ISO/IEC 17799 (BS 7799)に規定されています。
Built_in_user、Admin、Administrator、Administrators、root、Authentication、Authentications、Guest、Guests、Anyone、Everyone、System、Maintenance、Developer、Supervisor

注意 3：アカウントを利用するユーザーは、作成後に直ちにログインし、パスワードを変更することを推奨します（アカウント作成者が初期パスワードを記憶し、不正にログインしてしまう可能性があるため)。

注意 4：パスワードは 8 文字以上を推奨します。(6 文字以上 256 文字の範囲で指定できます。)

注意 5：Hitachi Storage Navigator Modular 2 を使用して障害を監視する場合、アカウント管理用対象装置は、ログインしないと障害監視ができないため、障害監視時に使用する共通の監視用ユーザーID とパスワードを登録してください。アカウント管理が有効な各装置には、あらかじめ障害監視用のユーザーID とパスワードを作成しておく必要があります。

Account Authentication情報の作成手順を次に示します。

1. コマンドプロンプト上で、Account Authentication 情報を作成したいアレイ装置を登録し、さらにそのアレイ装置に接続してください。

2. auaccount コマンドを実行して Account Authentication 情報を作成してください。

   入力例および結果を次に示します。

```
% auaccount -unit 装置名 -add -uid User001 -account enable -rolepattern 000001
Account Authentication が有効です。ログインしてください。
ユーザ ID: root
パスワード:
割り当てロール
  Storage Administrator (View and Modify)
アカウントを追加します。
よろしいですか? (y/n [n]): y
パスワードを入力してください。
パスワード:User001 用パスワード
確認パスワード:User001 用パスワード
アカウントを追加しました。
%
```

-rolepatternに指定する値は以下のとおりです。各ビットでロールの種類を指定します。たとえば、Storage Administrator (View and Modify)とAccount Administrator (View Only)を割り当てるには、000001+000100→000101を-rolepatternに指定します。

100000: Audit Log Administrator (View Only)
010000: Audit Log Administrator (View and Modify)
001000: Account Administrator (View Only)
000100: Account Administrator (View and Modify)
000010: Storage Administrator (View Only)
000001: Storage Administrator (View and Modify)

注意：-uidオプションに! # $ & ' * ? ` { | ~を使用する場合は、-uidオプションの代わりに-uidfileオプションを使用して、ファイル設定をしてください。-uidオプションに! # $ & ' * ? ` { | ~を使用した場合は、コマンドが異常終了したり、不当なユーザーIDが設定される場合があります。

B.6　アカウント情報の変更

アレイ装置に登録されているアカウント情報を変更します。変更できるアカウント情報は、以下の3つです。

- パスワード
- ロールの割り当て
- アカウントの有効/無効

注意 1：この操作は、Account Administrator（View and Modify）ロールを割り当てられたアカウントのみで操作できます。

注意 2：ここで説明するアカウント情報の変更手順は、他ユーザーのアカウントに対して実行できます。自アカウント情報は変更できません。ただし、ビルトインアカウントは自アカウント情報を変更できます。

注意 3：変更したアカウント情報は、当該アカウントの次回ログイン時から適用されます。

注意 4：一般アカウントはビルトインアカウント情報を変更できません。

注意 5：一般アカウント、ビルトインアカウントともユーザーID の変更はできません。

注意 6：-uid オプションに! # $ & ' * ? ` { | ~を使用する場合は、-uid オプションの代わりに -uidfile オプションを使用して、ファイル設定をしてください。

Account Authentication情報の変更手順を次に示します。

1. コマンドプロンプト上で、Account Authentication 情報を変更したいアレイ装置を登録し、さらにそのアレイ装置に接続してください。

2. auaccount コマンドを実行して Account Authentication 情報を変更してください。

   入力例および結果を次に示します。

```
% auaccount -unit 装置名 -chg -uid User001 -account enable -rolepattern 000101
Account Authentication が有効です。ログインしてください。
ユーザ ID: root
パスワード:
変更前の割り当てロール
  Storage Administrator (View and Modify)
変更後の割り当てロール
  Storage Administrator (View and Modify)
  Account Administrator (View and Modify)
アカウントを変更します。
よろしいですか? (y/n [n]): y
アカウントを変更しました。
%
```

B.7　アカウント情報の削除

アカウント情報の削除手順について説明します。

注意 1：この操作は、Account Administrator（View and Modify）ロールを割り当てられたアカウントのみで操作できます。

注意 2：自アカウントとビルトインアカウントは削除できません。

注意 3：ログイン中のユーザーアカウントを削除すると、そのユーザーは直ちに強制ログアウトとなります。

注意 4：-uid オプションに!#$&'*?`{|~を使用する場合は、-uid オプションの代わりに -uidfile オプションを使用して、ファイル設定をしてください。

Account Authentication情報の削除手順を次に示します。

1. コマンドプロンプト上で、Account Authentication 情報を削除したいアレイ装置を登録し、さらにそのアレイ装置に接続してください。

2. auaccount コマンドを実行して Account Authentication 情報を削除してください。

   入力例および結果を次に示します。

```
% auaccount -unit 装置名 -rm -uid User001
Account Authentication が有効です。ログインしてください。
ユーザ ID: root
パスワード:
ユーザ[User001]を削除します。
よろしいですか? (y/n [n]): y
ログイン中のアカウントを削除すると、そのユーザはログアウトされます。
続けますか? (y/n [n]): y
アカウントを削除しました。
%
```

B.8　自アカウント情報のパスワード変更

自アカウント情報のパスワード変更手順を次に示します。

1. コマンドプロンプト上で、自アカウント情報のパスワードを変更したいアレイ装置を登録し、さらにそのアレイ装置に接続してください。

2. auaccount コマンドを実行して自アカウント情報のパスワードを変更してください。

   入力例および結果を次に示します。

```
% auaccount -unit 装置名 -chgownpwd
Account Authentication が有効です。ログインしてください。
ユーザ ID: root
パスワード:
パスワードを変更します。
よろしいですか? (y/n [n]): y
旧パスワード:
新パスワード:
確認パスワード:
パスワードを変更しました。
%
```

B.9　ログイン有効期間の変更

ログイン有効期間の変更手順を次に示します。

1. コマンドプロンプト上で、ログイン有効期間を変更したいアレイ装置を登録し、さらにそのアレイ装置に接続してください。

2. auaccountopt コマンドを実行してログイン有効期間を変更してください。

   入力例および結果を次に示します。ここでは、ログイン有効期間を30分に設定する例を示します。

```
% auaccountopt -unit 装置名 -set -timeout 30
Account Authentication が有効です。ログインしてください。
ユーザ ID: root
パスワード:
アカウントオプションを設定します。
よろしいですか? (y/n [n]): y
アカウントオプションを設定しました。
%
```

B.10　警告バナーの設定

Hitachi Storage Navigator Modular 2に警告バナーを設定します。ここで設定する警告バナーは、Hitachi Storage Navigator Modular 2のGUIとは独立してアレイ装置に登録されます。

1. コマンドプロンプト上で、警告バナーを設定したいアレイ装置を登録し、さらにそのアレイ装置に接続してください。

2. auaccountopt コマンドを実行して警告バナーを設定してください。

   入力例および結果を次に示します。最初に、テキストファイルを使って警告バナーを設定し、その後警告バナーを表示します。

```
% auaccountopt -unit 装置名 -set -bannerfile c:\banner.txt
Account Authentication が有効です。ログインしてください。
ユーザ ID: root
パスワード:
アカウントオプションを設定します。
よろしいですか? (y/n [n]): y
アカウントオプションを設定しました。
%
% auaccountopt -unit 装置名 -refer -banner
Account Authentication が有効です。ログインしてください。
ユーザ ID: root
パスワード:
バナー:有効
警告
これは{会社名}のコンピュータシステムです。このコンピュータシステムは、承認を受けた人だけがその業務のためにのみ使用できます。承認を受けない人からのアクセスや使用があった場合、進入者として、刑事、民事、および行政上の訴訟を提起する場合があります。
犯罪捜査を含む公の目的のために、このコンピュータシステムに対する全てのアクセス履歴は、責任者によって傍受、記録、読み取り、複写、および開示される場合があります。
アクセスした人に関する私的な機密情報についても機密性とプライバシーの要件に従って暗号化され、アクセス履歴として記録されます。このシステムを使用する人は、承認を受けているかどうかに関係なく、上記の条件に合意したものとみなします。このシステムにおいてプライバシーの権利はありません。
%
```

B.11　アドバンスドセキュリティモードの変更

アドバンスドセキュリティモードの変更手順を次に示します。

1. コマンドプロンプト上で、アドバンスドセキュリティモードを変更したいアレイ装置を登録し、さらにそのアレイ装置に接続してください。

2. auaccountopt コマンドを実行してアドバンスドセキュリティモードを変更してください。

   入力例および結果を次に示します。ここでは、アドバンスドセキュリティモードを有効に設定する例を示します。

```
% auaccountopt -unit 装置名 -set -advancedsecuritymode enable
Account Authentication が有効です。ログインしてください。
ユーザ ID: root
パスワード:
アカウントオプションを設定します。
よろしいですか? (y/n [n]): y
アカウントオプションを設定しました。
%
```

B.12　操作手順

ここではHitachi Storage Navigator Modular 2を使用したログイン・ログアウト・強制ログアウトの操作手順について説明します。

注意：アカウントが登録されているのにもかかわらず、本節の手順でログインができない場合は、Account Administrator（View and Modify）ロールのアカウントを管理するユーザーに問い合わせてください（ユーザ ID、パスワードが間違っているか、強制ログアウトによりアカウントが無効になっている可能性があります）。

B.12.1　ログイン

1. たとえば、RAID グループを参照するコマンド（aurgref）を発行すると、ログイン要求プロンプトが表示されるので、登録済みのユーザ ID とパスワードを入力してください。

   入力例および結果を次に示します（下記は出力項目のイメージです）。

```
% aurgref -unit 装置名 -t
Account Authentication が有効です。ログインしてください。
ユーザ ID: User001
パスワード:
RAID   RAID    Parity
Group  Level   Groups  Type  Total Capacity  Free Capacity  Priority  Status Reconstruction Progress
    0   6( 9D+2P)  1  SAS    1.3 TB        1.3 TB (84.1%) RAID Group  Expansion  Normal  N/A
%
```

B.12.2　ログアウト

ログアウトは各コマンドの実行が完了した時点で、自動的に発行されます。

B.12.3　強制ログアウト

アレイ装置にログインしているビルトインアカウントを除く他のユーザーを強制的にログアウトさせます。

注意 1：アカウントのログイン中に、アレイ装置のコントローラー障害が発生した場合、ログイン中のセッション ID がアレイ装置内に残ってしまう場合があります。
したがって、コントローラー障害が発生した場合、Account Administrator（View and Modify）ロ

ールを割り当てられたアカウントで、セッション ID の残っているアカウントをすべて強制ログアウトしてください。

注意 2：強制ログアウトされたアカウントは無効になります。Account Administrator（View and Modify）ロールを割り当てられたアカウントで有効にしない限り、当該アカウントでの再ログインはできません。一般アカウントによる強制ログアウトでは無効になりません。

注意 3：-uid オプションに! # $ & ' * ? ` { | ~を使用する場合は、-uid オプションの代わりに -uidfile オプションを使用して、ファイル設定をしてください。

1. コマンドプロンプト上で、強制ログアウトしたいアレイ装置を登録し、さらにそのアレイ装置に接続してください。

2. auaccount コマンドを実行して強制的にログアウトしてください。

   入力例および結果を次に示します。

```
% auaccount -unit 装置名 -forcelogout -uid User001
Account Authentication が有効です。ログインしてください。
ユーザ ID: root
パスワード:
ユーザ[User001]を強制ログアウトします。
よろしいですか? (y/n [n]): y
ユーザ装置を使用している場合、操作ができなくなります。
また、強制ログアウトするとアカウントが無効になるため、次回からログインできなくな
ります。
よろしいですか? (y/n [n]): y
ユーザ[User001]を強制ログアウトしました。
%
```

B.13　スクリプト対応アカウント情報設定/削除

注意：-uid オプションに! # $ & ' * ? ` { | ~を使用する場合は、-uid オプションの代わりに -uidfile オプションを使用して、ファイル設定をしてください。-uid オプションに! # $ & ' * ? ` { | ~を使用した場合は、コマンドが異常終了したり、不当なユーザーID が設定される場合があります。

1. コマンドプロンプト上で、アカウント情報を設定したいアレイ装置を登録し、さらにそのアレイ装置に接続してください。

2. auaccountenv コマンドを実行してアカウント情報を設定してください。

   ここでは、アカウント情報を設定した後削除する入力例および結果を次に示します。

```
% auaccountenv -set -uid User001
アカウント情報を設定します。
よろしいですか? (y/n [n]): y
設定するパスワードを入力してください。
パスワード:
アカウント情報を設定しました。
%
% auaccountenv -rm
アカウント情報を削除します。
よろしいですか? (y/n [n]): y
アカウント情報を削除しました。
%
```

3. 環境変数を設定してください。ここで環境変数を設定することにより、設定したアカウント情報を用いたスクリプト運用が可能になります。実行するスクリプト内限定で有効にする場合は、スクリプトの先頭に定義します。

Account Authentication有効時

STONAVM_ACT=on

STONAVM_ACT環境変数をonに設定することで、Account Authenticationのユーザ IDとパスワードの入力要求をauaccountenvで設定したユーザ IDとパスワードで実行します。

STONAVM_RSP_PASS=on

STONAVM_RSP_PASS環境変数をonに設定することで、コマンドの確認に対する入力要求をすべて“y”で応答したことになります。

Windows用のスクリプト例

```
% set STONAVM_ACT=on
% set STONAVM_RSP_PASS=on
```

Red Hat LinuxおよびUNIX用のスクリプト例（Cシェルの場合）

```
% setenv STONAVM_ACT=on
% setenv STONAVM_RSP_PASS=on
```

Account Authentication無効時

STONAVM_RSP_PASS=on

STONAVM_RSP_PASS環境変数をonに設定することで、コマンドの確認に対する入力要求をすべて“y”で応答したことになります。

Windows用のスクリプト例

```
% set STONAVM_RSP_PASS=on
```

Red Hat LinuxおよびUNIX用のスクリプト例（Cシェルの場合）

```
% setenv STONAVM_RSP_PASS=on
```

なお、auaccountenvコマンドを使用して設定されたアカウント情報がどのアレイ装置に対して使用可能かどうかを、設定時および任意のタイミングで確認することができます。

最初に、アカウント情報設定時の入力例および結果を示します。

```
% auaccountenv -set -uid User001 -authentication -unit Array1
アカウント情報の認証テストをします。
よろしいですか? (y/n [n]): y
設定するパスワードを入力してください。
パスワード:
装置名                                                  結果
Array1                                                   成功
アカウント情報を設定します。
よろしいですか? (y/n [n]): y
アカウント情報を設定しました。
%
```

また、複数のアレイ装置を指定することができます。

```
% auaccountenv -set -uid User001 -authentication -unit Array1 Array2
アカウント情報の認証テストをします。
よろしいですか? (y/n [n]): y
設定するパスワードを入力してください。
パスワード:
装置名                                                  結果
Array1                                                   成功
Array2                                                   成功
アカウント情報を設定します。
よろしいですか? (y/n [n]): y
アカウント情報を設定しました。
%
```

アレイ装置の指定を省略すると、登録されているすべてのアレイ装置に対して確認できます。

```
% auaccountenv -set -uid User001 -authentication
アカウント情報の認証テストをします。
よろしいですか? (y/n [n]): y
設定するパスワードを入力してください。
パスワード:
装置名                                                  結果
Array1                                                   成功
Array2                                                   成功
Array3                                                   成功
アカウント情報を設定します。
よろしいですか? (y/n [n]): y
アカウント情報を設定しました。
%
```

次に、auaccountenvコマンドを使用して設定されたアカウント情報をあとで確認するための入力例および結果を示します。

```
% auaccountenv -test -authentication -unit Array1
アカウント情報の認証テストをします。
よろしいですか? (y/n [n]): y
装置名                                                  結果
Array1                                                   成功
%
```

また、複数のアレイ装置を指定することができます。

```
% auaccountenv -test -authentication -unit Array1 Array2
アカウント情報の認証テストをします。
よろしいですか? (y/n [n]): y
装置名                                                  結果
Array1                                                   成功
Array2                                                   成功
%
```

アレイ装置の指定を省略すると、登録されているすべてのアレイ装置に対して確認できます。

```
% auaccountenv -test -authentication
アカウント情報の認証テストをします。
よろしいですか? (y/n [n]): y
装置名                                                  結果
Array1                                                   成功
Array2                                                   成功
Array3                                                   成功
%
```

B.14　スクリプト対応セッション維持

ここでは、スクリプトでのセッション維持の操作方法について説明します。セッション維持とは、スクリプト処理中に他のユーザーにリソース操作権限をはく奪または他のユーザーにスクリプト内で変更する予定のリソースに変更が加えられた等によりスクリプト処理が中断やエラーにならないために、セッションをスクリプト処理中に維持することです。

注意：セッションのタイムアウト時間はスクリプト開始コマンドからカウントされます。スクリプトの処理時間を想定して、スクリプト実行前に適切なセッションタイムアウト時間を設定してください。

操作例：

1. auaccountenv コマンドを実行してアカウント情報を設定してください。

   ここでは、アカウント情報を設定した後削除する入力例および結果を次に示します。

```
% auaccountenv -set -uid User001
アカウント情報を設定します。
よろしいですか? (y/n [n]): y
設定するパスワードを入力してください。
パスワード:
アカウント情報を設定しました。
%
% auaccountenv -rm
アカウント情報を削除します。
よろしいですか? (y/n [n]): y
アカウント情報を削除しました。
%
```

2. 環境変数を設定してください。ここで環境変数を設定することにより、設定したアカウント情報を用いたスクリプト運用が可能になります。実行するスクリプト内限定で有効にする場合は、スクリプトの先頭に定義します。

Account Authentication有効時

STONAVM_ACT=on

STONAVM_ACT環境変数をonに設定することで、Account AuthenticationのユーザIDとパスワードの入力要求をauaccountenvで設定したユーザIDとパスワードで実行します。

STONAVM_RSP_PASS=on

STONAVM_RSP_PASS環境変数をonに設定することで、コマンドの確認に対する入力要求をすべて“y”で応答したことになります。

Windows用のスクリプト例

```
% set STONAVM_ACT=on
% set STONAVM_RSP_PASS=on
```

Red Hat LinuxおよびUNIX用のスクリプト例（Cシェルの場合）

```
% setenv STONAVM_ACT=on
% setenv STONAVM_RSP_PASS=on
```

Account Authentication無効時

STONAVM_RSP_PASS=on

STONAVM_RSP_PASS環境変数をonに設定することで、コマンドの確認に対する入力要求をすべて“y”で応答したことになります。

Windows用のスクリプト例

```
% set STONAVM_RSP_PASS=on
```

Red Hat LinuxおよびUNIX用のスクリプト例（Cシェルの場合）

```
% setenv STONAVM_RSP_PASS=on
```

3. バッチファイルを実行してください。バッチファイル内には下記の記述が必要です。

最初に、環境変数を記述します。

STONAVM_ACT_SCRIPT =xxxxxxxxxx　　32文字以内の半角英数字

Windows用のスクリプト例

```
% set STONAVM_ACT_SCRIPT=SerialNumber93010001
```

Red Hat LinuxおよびUNIX用のスクリプト例（Cシェルの場合）

```
% setenv STONAVM_ACT_SCRIPT=SerialNumber93010001
```

その次にスクリプト開始コマンドを記述します。更新権限がない場合には、参照モードでスクリプトが動作するので、設定するコマンドはエラーになります。

```
auaccountscript -unit 装置名 -start
```

なお、更新権限をチェックしてからスクリプトを開始したい場合には、下記を記述します。更新権限がない場合には、スクリプトを開始する前にエラーを応答します。

```
auaccountscript -unit 装置名 -start -modifyperm
```

その後、スクリプトで処理したいコマンドを記述し、最後にスクリプト終了コマンドを記述します。

```
auaccountscript -unit 装置名 -finish
```

索引