iStorage

Empowered by Innovation NEC

iStorage HS シリーズ

CIFS 利用の手引き

IH1907-1

輸出する際の注意事項

本製品（ソフトウェアを含む）は、外国為替及び外国貿易法で規定される規制貨物（または役務）に該当することがあります。

その場合、日本国外へ輸出する場合には日本国政府の輸出許可が必要です。

なお、輸出許可申請手続にあたり資料等が必要な場合には、お買い上げの販売店またはお近くの当社営業拠点にご相談ください。

iStorage HS シリーズについて

iStorage HS シリーズには、バックアップ/アーカイブ用途の iStorage HS3/HS8/HS Virtual Appliance とアーカイブ用途の iStorage HS6 があります。

- **iStorage HS3/HS8**

  NEC 独自のグリッド・ストレージ技術によるシステムの柔軟な拡張性、 分散冗長配置技術による高い信頼性、最先端の重複排除技術による高いデータ圧縮性を持つディスクストレージです。

  搭載する重複排除エンジンは、最も効率よく重複を検出できる可変長の知的ブロック分割方式を採用しています。

  これにより、複数世代のバックアップデータを効率的に格納し、テープ並みの容量単価を実現した製品です。

- **iStorage HS6**

  iStorage HS3/HS8 のコア技術を継承し、システムの柔軟な拡張性、分散冗長配置技術による高い信頼性、および重複排除機能を備えたディスクストレージです。

  搭載する重複排除エンジンは、リソースの消費が少ない固定長分割方式を採用しています。これにより入出力処理への影響を抑え低価格を実現しています。

- **iStorage HS Virtual Appliance**

  iStorage HS8/HS3 で培われたコア技術をベースとした iStorage HS シリーズの仮想アプライアンス製品です。

  一般的なサーバ上の仮想化環境で動作するため、サーバリソースの有効活用を行い、消費電力や運用管理コスト低減を図ることができます。また、すばやく導入することが可能なため、ビジネスや IT 環境の変化に柔軟に対応できます。

  iStorage HS Virtual Appliance を使用する場合は、はじめに「iStorage HS Virtual Appliance 導入構成ガイド」をお読みください。

本書について

本書では、CIFS の導入、設定、運用を行う際の手順を説明します。本書の各手順を実施することで、Windows クライアントから iStorage HS へのアクセスが可能になります。各章の概要は以下の通りです。画面のナビゲーションとシステム操作手順は同じです。ただし、画面上の情報は参考情報であり、使用システムで表示される実際の画面入力とは異なります。

各手順における GUI の設定項目の詳細は、「*ユーザーズガイド*」を参照してください。各手順で使用する CLI の設定項目の詳細は、「*コマンドリファレンス*」の「*第 II 編 リファレンス*」を参照してください。

第 1 章 – CIFS を初めて使用する場合の設定手順を説明します。
第 2 章 – CIFS の認証方式を変更する場合の手順を説明します。
第 3 章 – Active Directory 認証で使用できる ACL によるアクセス制御について説明します。
第 4 章 – ファイル情報に対応したファイルシステムについて説明します。
第 5 章 – クライアントの IP アドレスによるアクセス制御について説明します。
第 6 章 – CIFS 通信のセキュリティを強化する設定について説明します。

本書の手順は、iStorage HS およびクライアント、Active Directory などが以下の状態であることを前提にしています。

- iStorage HS の外部ネットワークの設定が完了していること
- iStorage HS とクライアント間で正常に通信が行えること
- iStorage HS とドメインコントローラ間で正常に通信が行えること
- Active Directory が正常に運用されていること
- 接続されるクライアントの OS は Windows Server 2003 以降のバージョンであること
  （Windows クライアント以外には対応していません。）

対象読者

本書は、Windows のファイル共有やドメインによるユーザ管理を含む Windows ネットワークに精通しているシステム管理者を対象としています。システム管理者が、ストレージ管理者やバックアップ管理者の場合もあります。管理者ユーザの役割と責任は、部門の方針によって決定されます。

２０２２年　６月　初　版

備考

(1) 本書は、iStorage HS3/HS8 バージョン5.7, iStorage HS6 バージョン2.7およびiStorage HS VirtualAppliance バージョン1.7に対応しています。

(2) 本書では、特にご注意いただく内容を以下で示しております。

シンボル	説明
Note	説明対象の追加情報です。

(3) 本書ではスケールアウトモデルを前提とした用語を使用しております。シングルノードモデルをご利用の場合は、以下の読み替えを行ってください。

本書で使用される用語		読み替え用語
管理ノード	→	ストレージノード
外部フローティング IP	→	外部 IP アドレス

目　次

第1章　認証方式の新規設定

この章では、CIFS を初めて使用する場合の設定手順について説明します。手順は使用する認証方式によって異なります。

1.1　認証方式

iStorage HS は、以下の 2 種類の認証方式をサポートしています。

1. ワークグループ（共有）認証
   パスワード認証によるアクセス制御を行います。パスワードを設定しない場合、誰でもアクセスすることが可能です。利用者は共通のユーザアカウントを使用してファイルアクセスを行うため、ユーザおよびグループによるアクセス制御はできません。
   ユーザアカウントによるアクセス制御が不要な場合には、本認証方式を使用します。

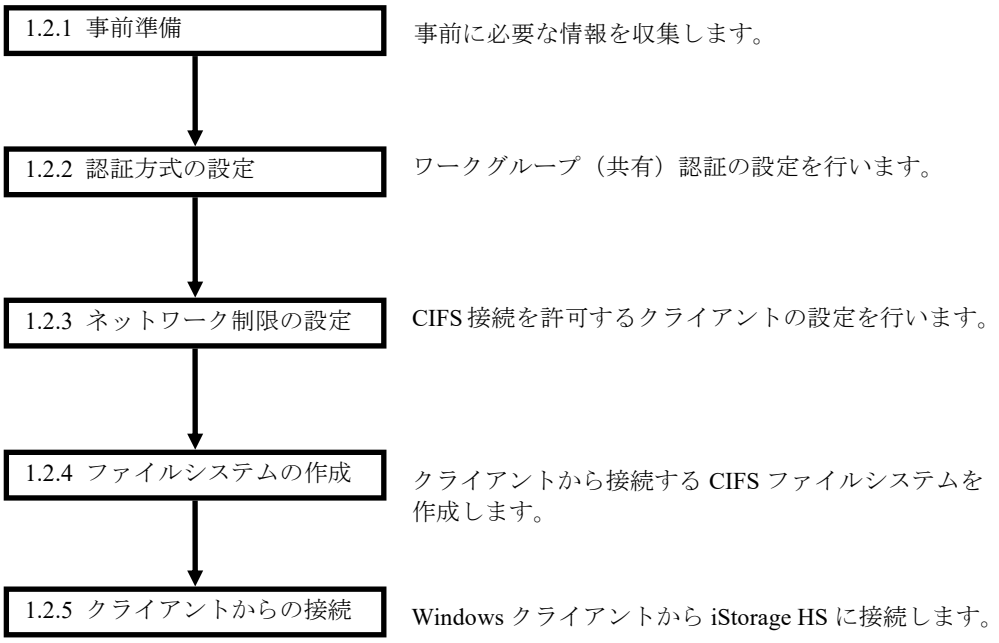
2. Active Directory 認証
   Active Directory 上のユーザアカウント認証によるアクセス制御を行います。
   使用するファイルシステムの ACL オプションが有効（既定値）であれば、NTFS と互換性のある ACL 機能を利用することができます。
   Active Directory 環境でユーザアカウントによるアクセス制御を行う場合には、本認証方式を使用します。

Note iStorage HS の初期設定時、ウィザードを使用して CIFS ファイルシステムを作成した場合、認証方式はワークグループ（共有）に設定されます。CIFS ファイルシステムを作成しなかった場合は、認証方式は設定されません。

1.2 ワークグループ（共有）認証の新規設定

本節では、認証方式にワークグループ（共有）を使用する場合の手順について説明します。

クライアントからワークグループ（共有）認証で接続するには、はじめに iStorage HS の認証方式の設定を行った後、接続するファイルシステムを作成し、クライアントから接続を行います。



1.2.1 事前準備

本手順では以下の事前準備が必要です。

- ワークグループ名
- 認証用のパスワード
- クライアントから接続するファイルシステム名

1.2.2 認証方式の設定

iStorage HS の認証方式をワークグループ（共有）認証に設定します。「*ユーザーズガイド*」の「*第5章 システム設定*」の「*認証方式にワークグループ（共有）を設定する*」を参照してください。

1.2.3 ネットワーク制限の設定

CIFS 接続を許可するクライアントを設定します。「*ユーザーズガイド*」の「*第5章 システム設定*」の「*ネットワーク制限を設定する*」を参照してください。

1.2.4 ファイルシステムの作成

Windows クライアントから使用するファイルシステムを作成します。「*ユーザーズガイド*」の「*第4章 ファイルシステム設定の管理*」の「*ファイルシステムを作成する（CIFS）*」を参照してファイルシステムの作成を行ってください。

1.2.5 クライアントからの接続

Windows OS の net use コマンドを使用して、クライアントから接続（マウント）を行います。「*付録 A クライアントからの接続*」を参照して接続を行ってください。

Note Windows OS のバージョンによっては、ネットワークドライブを指定せずに net use コマンドを実行すると、接続に失敗する場合があります。この場合は、ネットワークドライブを指定して、再度 net use コマンドを実行してください。

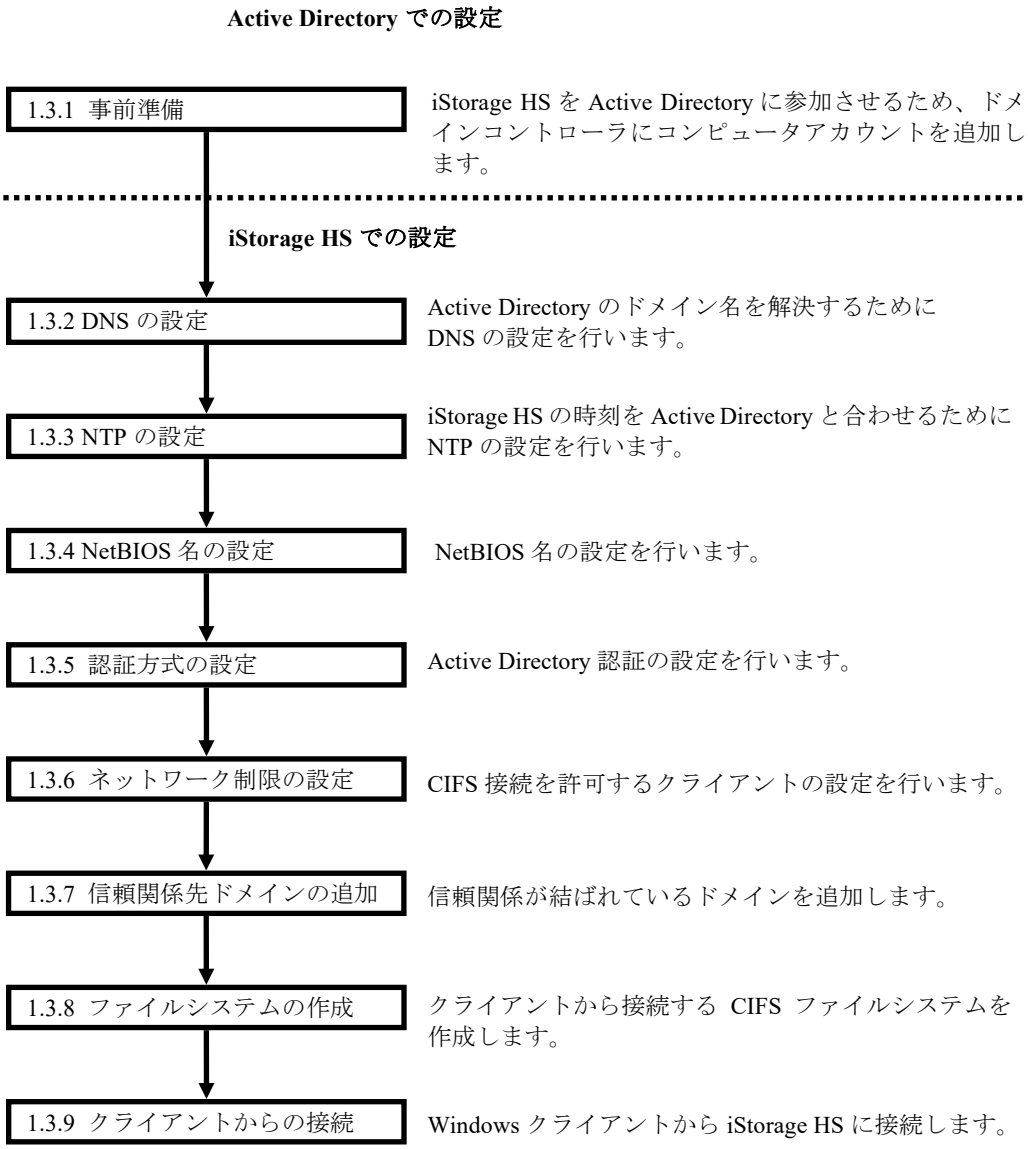
Note Windows OS のバージョンによっては、Windows OS のユーザ名を net use コマンドに指定する必要があります。以下は、ユーザ名「user01」を指定した例です。

ユーザ名を指定する場合：
C:¥>net use Z: ¥¥<IP アドレス>¥cifs1 /user:user01 <パスワード>

1.3 Active Directory 認証の新規設定

本節では、認証方式に Active Directory を使用する場合の手順について説明します。

クライアントから Active Directory 認証で接続するには、事前に DNS、NTP サーバの設定を行い、iStorage HS の認証方式の設定を行った後、接続するファイルシステムを作成し、クライアントから接続を行います。認証方式設定には、iStorage HS が所属するドメインと所属するドメインの信頼関係先ドメインを設定する必要があります。



1.3.1 事前準備

本手順では以下の事前準備が必要です。iStorage HS が Active Directory に参加する際に必要なアカウントを、ドメインコントローラに準備します。認証に使用する Active Directory の管理者に、アカウントの作成を依頼してください。

- DNS サーバの IP アドレス
- NTP サーバの IP アドレス
- iStorage HS が所属するドメイン名と DNS ドメイン名
- 所属するドメイン名の信頼関係先 DNS ドメイン名（詳細は 1.3.7 で説明）
- iStorage HS に設定する NetBIOS 名
- クライアントから接続するファイルシステム名
- ユーザアカウント（iStorage HS のドメイン参加用に 1 アカウント）
  - アカウント名は任意
  - 既存のユーザを利用してもよい。
- コンピュータアカウント（アクセラレータノード機能を持つノード 1 台につき 1 アカウント）
  - アカウント名は iStorage HS に設定する NetBIOS 名
  - 「パスワードのリセット」と「書き込み」許可のアクセス権限を与えておくこと。

1.3.2 DNS の設定

Active Directory に参加する際、iStorage HS はドメイン名の名前解決を行う必要があります。この名前解決に使用する DNS サーバを設定します。「*ユーザーズガイド*」の「*第 5 章 システム設定*」の「*アクセラレータノード機能を持つノードの外部ネットワーク設定を有効にする*」を参照して設定を行ってください。

Note DNS の設定は、アクセラレータノード機能を持つ全ノードに対して設定してください。

Note Active Directory 認証の環境に新しいノードを追加した場合は、追加したノードに DNS を設定してください。

Note Active Directory 認証を使用する際、検索ドメインに検索ドメイン名が登録されている場合、性能が劣化する場合があります。検索ドメインは既定値（設定なし）にしておくことを推奨いたします。

1.3.3 NTP の設定

NTP サーバの設定を行います。「*ユーザーズガイド*」の「*第 5 章 システム設定*」の「*NTP サーバを設定する*」を参照して設定を行ってください。NTP サーバの設定後は、システムの再起動が必要となります。

Note CIFS 認証方式に Active Directory を使用する場合は、ドメインコントローラが参照している NTP サーバと同じ NTP サーバを指定してください。iStorage HS の時刻がドメインコントローラとずれている場合、Active Directory への参加に失敗する場合があります。

1.3.4 NetBIOS 名の設定

NetBIOS 名を設定します。「*ユーザーズガイド*」の「*第 5 章 システム設定*」の「*NetBIOS 名を設定する*」を参照して設定を行ってください。

Note 同じドメイン内に本製品が複数システムある場合、重複することがないように、それぞれ異なる NetBIOS 名を指定してください。NetBIOS 名が既定値の場合、NetBIOS 名が重複するため、Windows クライアントから本製品に接続できない場合があります。

1.3.5 認証方式の設定

iStorage HS の認証方式を Active Directory 認証に設定します。「*ユーザーズガイド*」の「*第 5 章 システム設定*」の「*認証方式に Active Directory を設定する*」を参照して設定を行ってください。

iStorage HS と Active Directory の間の LDAP 通信を暗号化する場合は、「*第 6 章 セキュリティ強化*」の「*6.1 LDAP 通信の暗号化*」を参照して設定を行ってください。

Note 本手順は NTP の設定を反映するためのシステム再起動を行った後に行ってください。再起動を行わない場合、ドメインの参加に失敗する場合があります。

Note ドメイン参加設定では、「*1.3.1 事前準備*」で指定したユーザ名とパスワードを使用してください。

1.3.6 ネットワーク制限の設定

CIFS 接続を許可するクライアントを設定します。「*ユーザーズガイド*」の「*第 5 章 システム設定*」の「*ネットワーク制限を設定する*」を参照してください。

1.3.7 信頼関係先ドメインの追加

「*1.3.5 認証方式の設定*」で設定したドメインと信頼関係が結ばれているドメインを登録します。設定方法については「*第 3 章 ファイルアクセス制御*」の「*3.4 信頼関係先ドメインの追加*」を参照してください。

Note 本設定は必須ではありません。ただし、信頼関係先ドメインの設定がされていない場合、信頼関係先ドメインに登録されたユーザ、グループは iStorage HS にアクセスできません。また、信頼関係先ドメインに登録されたユーザ、グループの ACL が含まれるファイル・フォルダは、iStorage HS への書き込み・読み込みに失敗します。

Note レプリケーションの設定を行っている場合、レプリカ側も信頼関係先ドメインの設定を行ってください。詳細は「*第 3 章 ファイルアクセス制御*」の「*3.5 レプリケーションの注意事項*」を参照してください。レプリケーションは、ディザスタリカバリソリューションとして、iStorage HS 間でファイルシステムをレプリケートする機能です。レプリケーション機能についての詳細は「*ユーザーズガイド*」の「*第 8 章 レプリケーション*」を参照してください。

1.3.8 ファイルシステムの作成

Windows クライアントから使用するファイルシステムを作成します。「*ユーザーズガイド*」の「*第 4 章 ファイルシステム設定の管理*」の「*ファイルシステムを作成する（CIFS）*」を参照して ACL オプションを有効にしたファイルシステムの作成を行ってください。Active Directory 認証を指定している場合、ACL オプションの既定値は有効となります。

1.3.9 クライアントからの接続

クライアントから接続（マウント）を行います。「*付録 A クライアントからの接続*」を参照して接続を行ってください。

第2章　認証方式の変更

この章では、認証方式を変更する手順について説明します。既存の CIFS ファイルシステムを残した状態で認証方式を変更する場合、iStorage HS では以下の図の変更をサポートしています。

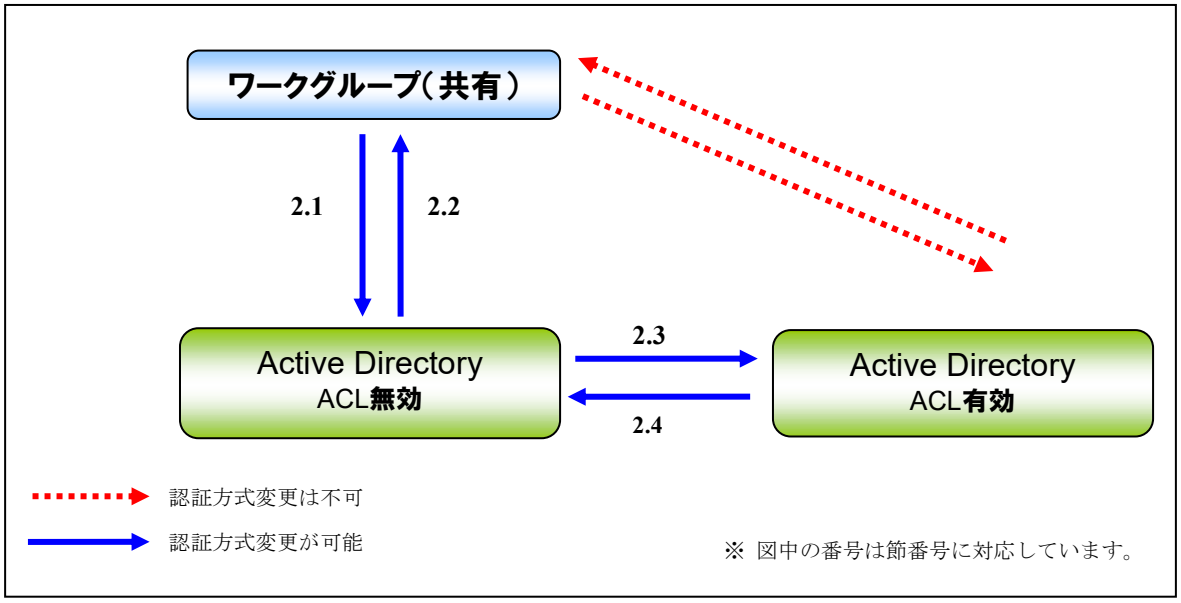
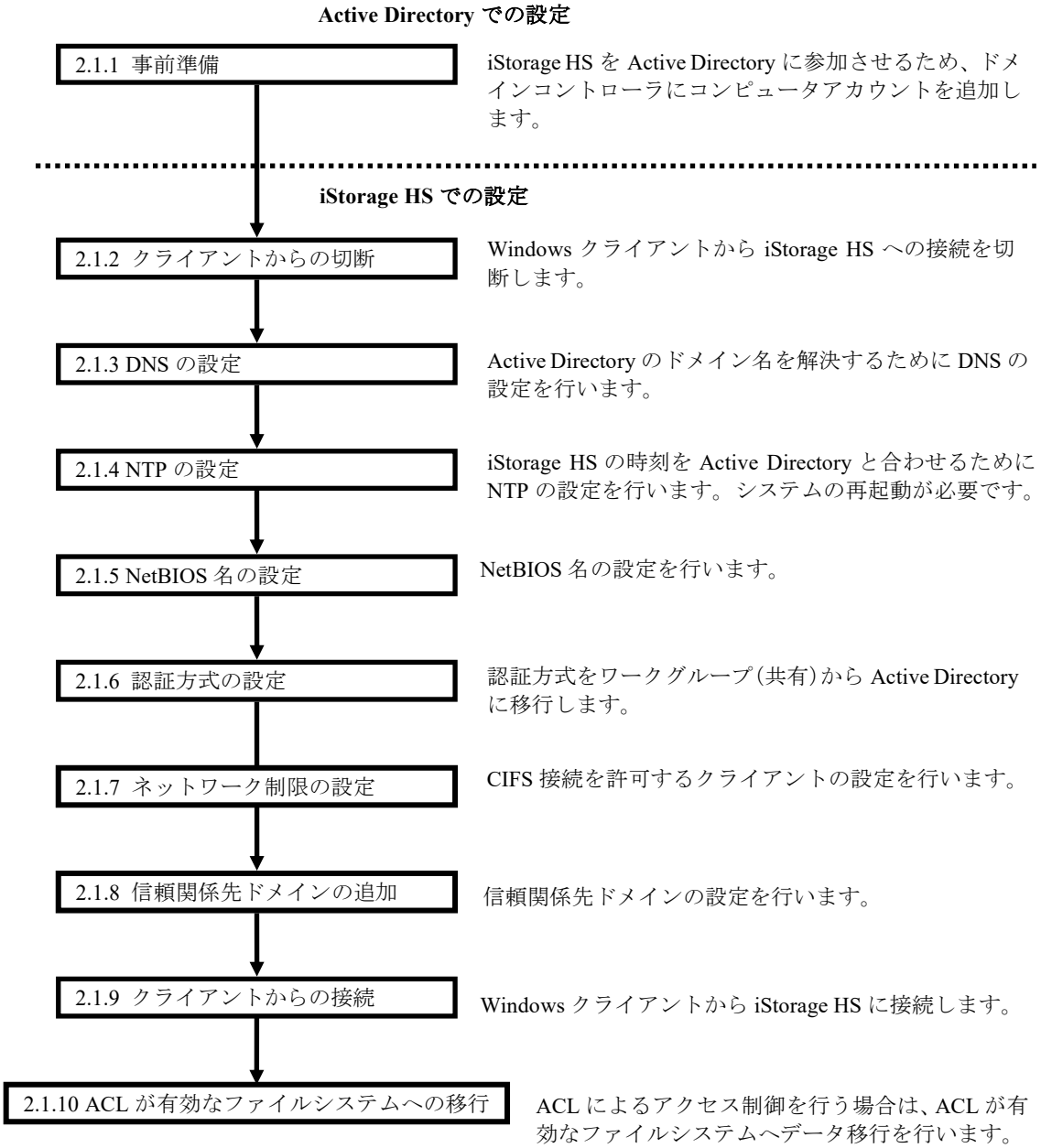


図 1 認証方式の変更

上図の点線の矢印に対応する認証方式の変更は、ファイルシステムを残したまま行うことはできません。認証方式を変更するには、NFS を除く CIFS ファイルシステムを削除した後、認証方式を設定してください。認証方式変更前のファイルシステムのデータが必要な場合、認証方式変更前のファイルシステムのデータをバックアップし、認証方式移行後の新規ファイルシステムにリストアするデータ移行の検討が必要となります。

2.1 ワークグループ(共有)認証から Active Directory 認証への移行

本節では、ワークグループ（共有）認証から Active Directory 認証への移行手順について説明します。ワークグループ（共有）認証時に作成した CIFS ファイルシステムは ACL が無効であるため、ACL によるアクセス制御を行う場合は、認証方式を Active Directory 認証へ変更した後、ACL が有効なファイルシステムへデータを移行する必要があります。



2.1.1 事前準備

本手順では以下の事前準備が必要です。iStorage HS が Active Directory に参加する際に必要なアカウントを、ドメインコントローラに準備します。認証に使用する Active Directory の管理者に、アカウントの作成を依頼してください。

- DNS サーバの IP アドレス
- NTP サーバの IP アドレス
- iStorage HS が所属するドメイン名と DNS ドメイン名
- 所属するドメイン名の信頼関係先 DNS ドメイン名（詳細は 2.1.8 で説明）
- iStorage HS に設定する NetBIOS 名
- クライアントから接続するファイルシステム名
- ユーザアカウント（iStorage HS のドメイン参加用に 1 アカウント）
  - アカウント名は任意。
  - 既存のユーザを利用してもよい。
- コンピュータアカウント（アクセラレータノード機能を持つノード 1 台につき 1 アカウント）
  - アカウント名は iStorage HS に設定する NetBIOS 名
  - 「パスワードのリセット」と「書き込み」許可のアクセス権限を与えておくこと。

2.1.2 クライアントからの切断

クライアントから iStorage HS を切断します。切断する前にファイルシステムにアクセスしていないことを確認してください。「*付録 B クライアントからの切断*」を参照してください。

2.1.3 DNS の設定

Active Directory に参加する際、iStorage HS はドメイン名の名前解決を行う必要があります。この名前解決に使用する DNS サーバを設定します。「*ユーザーズガイド*」の「*第 5 章 システム設定*」の「*アクセラレータノード機能を持つノードの外部ネットワーク設定を有効にする*」を参照して設定を行ってください。

Note DNS の設定は、アクセラレータノード機能を持つ全ノードに対して設定してください。

Note Active Directory 認証を使用する際、検索ドメインに検索ドメイン名が登録されている場合、性能が劣化する場合があります。検索ドメインは既定値（設定なし）にしておくことを推奨いたします。

2.1.4 NTP の設定

NTP サーバの設定を行います。「*ユーザーズガイド*」の「*第 5 章 システム設定*」の「*NTP サーバを設定する*」を参照して設定を行ってください。システムの再起動が必要となります。

Note CIFS 認証方式に Active Directory を使用する場合は、ドメインコントローラが参照している NTP サーバと同じ NTP サーバを指定してください。iStorage HS の時刻がドメインコントローラとずれている場合、Active Directory への参加に失敗する場合があります。

2.1.5 NetBIOS 名の設定

NetBIOS 名を設定します。「*ユーザーズガイド*」の「*第 5 章 システム設定*」の「*NetBIOS 名を設定する*」を参照して設定を行ってください。

Note 同じドメイン内に本製品が複数システムある場合、重複することがないように、それぞれ異なる NetBIOS 名を指定してください。NetBIOS 名が既定値の場合、NetBIOS 名が重複するため、Windows クライアントから本製品に接続できない場合があります。

2.1.6 認証方式の設定

iStorage HS の認証方式を Active Directory 認証に設定します。「*ユーザーズガイド*」の「*第 5 章 システム設定*」の「*認証方式に Active Directory を設定する*」を参照して設定を行ってください。

Note 本手順は、NTP の設定を反映するためのシステム再起動を行った後に行ってください。再起動を行わない場合、ドメインの参加に失敗する場合があります。

Note ドメイン参加設定では、「*2.1.1 事前準備*」で指定したユーザ名とパスワードを使用してください。

2.1.7 ネットワーク制限の設定

CIFS 接続を許可するクライアントを設定します。「*ユーザーズガイド*」の「*第 5 章 システム設定*」の「*ネットワーク制限を設定する*」を参照してください。

2.1.8 信頼関係先ドメインの追加

「*2.1.6 認証方式の設定*」で設定したドメインと信頼関係が結ばれているドメインを登録します。設定方法については「*第 3 章 ファイルアクセス制御*」の「*3.4 信頼関係先ドメインの追加*」を参照してください。

Note 本設定は必須ではありません。ただし、信頼関係先ドメインの設定がされていない場合、信頼関係先ドメインに登録されたユーザ、グループは iStorage HS にアクセスできません。また、信頼関係先ドメインに登録されたユーザ、グループの ACL が含まれるファイル・フォルダは、iStorage HS への書き込み・読み込みに失敗します。

Note レプリケーションの設定を行っている場合、レプリカ側も信頼関係先ドメインの設定を行ってください。詳細は「*第 3 章 ファイルアクセス制御*」の「*3.5 レプリケーションの注意事項*」を参照してください。レプリケーションは、ディザスタリカバリソリューションとして、iStorage HS 間でファイルシステムをレプリケートする機能です。レプリケーション機能についての詳細は「*ユーザーズガイド*」の「*第 8 章 レプリケーション*」を参照してください。

2.1.9 クライアントからの接続

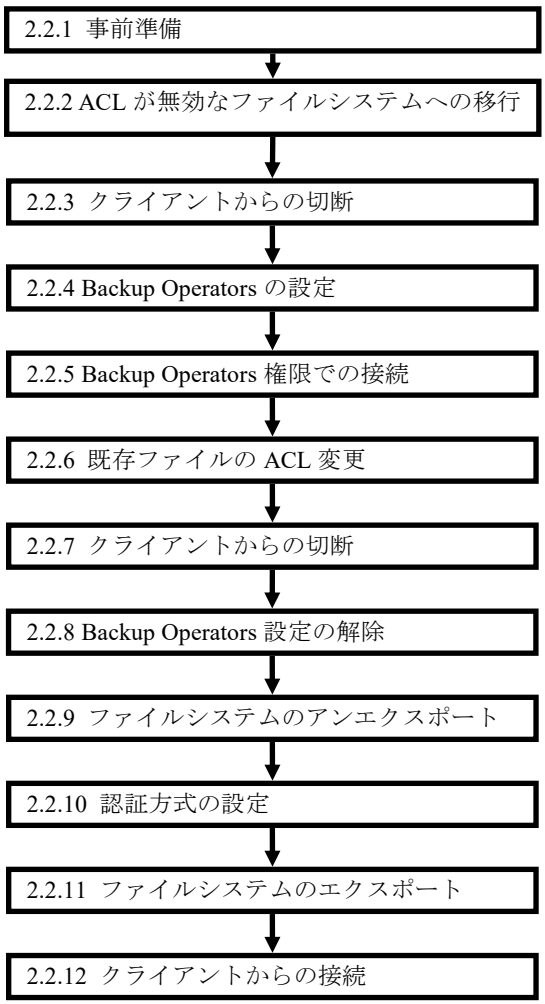
クライアントから接続（マウント）を行います。「*付録 A クライアントからの接続*」を参照して接続を行ってください。

2.1.10 ACL が有効なファイルシステムへの移行

認証方式がワークグループ（共有）に設定されていたときに作成されたファイルシステムは ACL が無効になっています。ACL を使用する場合は ACL が有効なファイルシステムへのデータ移行が必要です。「*2.3 ACL が有効なファイルシステムへの移行*」を参照してデータ移行を行ってください。

2.2 Active Directory 認証からワークグループ（共有）認証への移行

本節では、Active Directory 認証からワークグループ（共有）認証への移行手順について説明します。ワークグループ（共有）認証では ACL が有効なファイルシステムはエクスポートできません。そのため、ACL が有効なファイルシステムに、認証方式変更後もクライアントから接続する必要がある場合は、事前に ACL が無効なファイルシステムにデータを移行する必要があります。このデータ移行時、ACL により通常のユーザではアクセスできないデータがある場合があるため、アクセス制御を無視する特権ユーザを使用して ACL が無効なファイルシステムへデータを移行することが必要となります。また、ACL が有効なファイルシステムがない場合でも、ACL が無効な既存のファイルシステムのデータに接続が必要な場合は、ワークグループ（共有）認証でアクセス可能となるように、既存のファイル、フォルダへ必要なアクセス権の設定を変更する必要があります。



事前に必要な情報を収集します。

ACL が有効なファイルシステムがある場合、無効なファイルシステムに移行します。

Windows クライアントから iStorage HS への接続を切断します。

既存ファイルの ACL を変更するために、特権ユーザでアクセスする設定を行います。

設定した特権ユーザで Windows クライアントから iStorage HS に接続します。

認証方式の移行後も既存ファイルにアクセスできるよう、既存ファイルの ACL を変更します。

Windows クライアントから iStorage HS への接続を切断します。

特権ユーザでアクセスする設定を解除します。

認証方式を移行するために、CIFS ファイルシステムをアンエクスポートします。

認証方式を Active Directory からワークグループ（共有）に移行します。

クライアントから接続する CIFS ファイルシステムをエクスポートします。

Windows クライアントから iStorage HS に接続します。

2.2.1 事前準備

本手順では以下の事前準備が必要です。

- ワークグループ名
- 認証用のパスワード
- クライアントから接続するファイルシステム名

2.2.2 ACL が無効なファイルシステムへの移行

ACL が有効なファイルシステムが存在しない場合、本手順は不要です。

ACL が有効なファイルシステムを認証方式変更後も使用する場合は、ACL が無効なファイルシステムへのデータ移行が事前に必要です。「*2.4 ACL が無効なファイルシステムへの移行*」を参照してデータ移行を行ってください。

2.2.3 クライアントからの切断

クライアントから iStorage HS を切断します。切断する前にファイルシステムにアクセスしていないことを確認してください。「*付録 B クライアントからの切断*」を参照してください。

2.2.4 Backup Operators の設定

認証方式の移行前に作成したファイルは、Active Directory 認証での接続時に利用されるユーザがファイル所有者となる ACL が付与されています。ワークグループ（共有）認証ではこのユーザを利用できないため、これらの既存ファイルのアクセス許可の変更ができません。認証方式の移行後に作成するファイルと同様にアクセス許可の変更を可能にするには、ワークグループ（共有）認証でもファイルに所有者としてアクセスできるようにする必要があります。そのため、既存ファイルの所有者をワークグループ（共有）認証で利用するユーザに変更する必要があります。

所有者でないファイルの ACL も変更するために、ACL のチェックを受けない Backup Operators 権限を持つユーザで iStorage HS に接続します。「*2.2.4 Backup Operators の設定*」～「*2.2.8 Backup Operators 設定の解除*」の手順はファイル・フォルダが存在するすべての CIFS ファイルシステムに対して行ってください。

システム管理者のユーザ名（既定値は sysadmin）で管理ノードに CLI ログインし、以下のコマンドを実行してください。管理ノードに接続する際には、接続先として外部フローティング IP アドレスを指定してください。
Backup Operators 権限を与えるユーザには、iStorage HS が所属するドメインの任意のユーザを指定してください。コマンドに関する詳細は「*コマンドリファレンス*」の「*cifs*」を参照してください。

```
# cifs modify name=<ファイルシステム名> ¥
        backup-operators=<Backup Operators 権限を与えるユーザ名>
```

2.2.5 Backup Operators 権限での接続

既存ファイルの所有者を変更して、ワークグループ（共有）認証時に上書きやアクセス許可の変更を可能にするために、「*2.2.4 Backup Operators の設定*」で Backup Operators 権限を与えたユーザとして iStorage HS に接続します。「*付録 A クライアントからの接続*」を参照して接続を行ってください。Backup Operators 権限を持った sample01 ユーザで接続する場合は以下のようになります。

```
C:¥>net use Z: ¥¥<IP アドレス>¥cifs1 /user:ccc¥sample01 password01
コマンドは正常に終了しました。


C:¥>
```

2.2.6 既存ファイルの ACL 変更

ワークグループ（共有）認証でも使用できるように、ファイルシステム上の全ファイルの ACL を一括変更します。

1. クライアント側で iStorage HS の共有を割り当てたネットワークドライブのプロパティを開いてください。以下のような画面が表示されます。

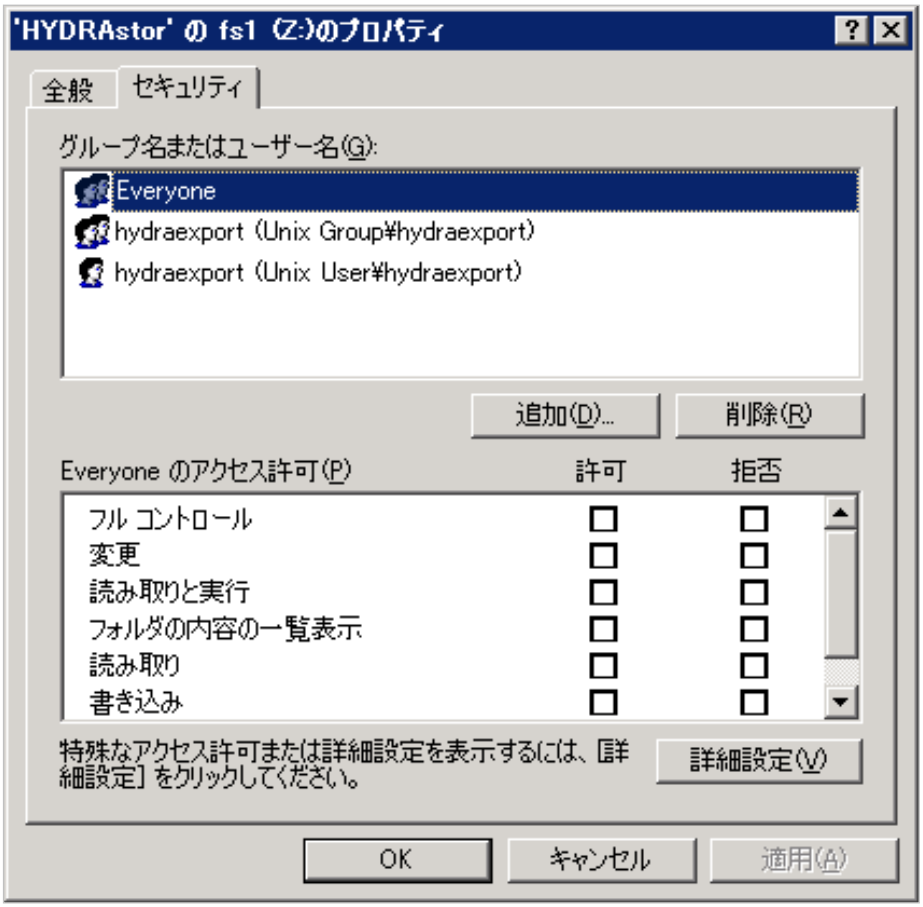


図 2 ネットワークドライブのプロパティ

2. 「セキュリティ」タブをクリックします。
3. 「グループ名またはユーザ名」から「Everyone」を選択します。
4. 「フル コントロール」の許可のチェックボックスを選択します。
5. 「詳細設定」をクリックします。

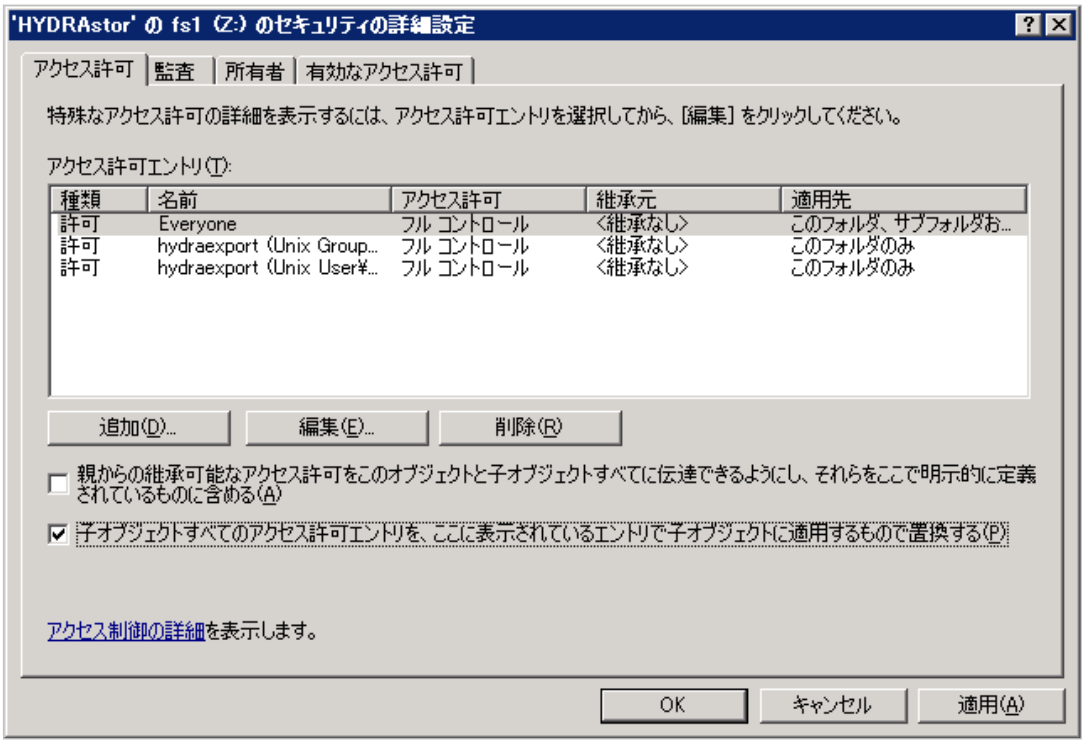


図 3　セキュリティの詳細設定

6. Everyone の「適用先」を「このフォルダ、サブフォルダおよびファイル」に変更します。
7. 「子オブジェクトすべてのアクセス許可エントリを、ここに表示されているエントリで子オブジェクトに適用するもので置換する」のチェックボックスを選択します。
8. 「OK」をクリックします。

2.2.7　クライアントからの切断

Backup Operators 権限で接続しているクライアントから iStorage HS を切断します。切断する前にファイルシステムにアクセスしていないことを確認してください。「*付録 B クライアントからの切断*」を参照してください。

2.2.8 Backup Operators 設定の解除

システム管理者のユーザ名（既定値は sysadmin）で管理ノードに CLI ログインし、以下のコマンドを実行してください。管理ノードに接続する際には、接続先として外部フローティング IP アドレスを指定してください。コマンドに関する詳細は「*コマンドリファレンス*」の「*cifs*」を参照してください。

```
# cifs modify name=<「2.2.4 Backup Operators の設定」で指定したファイルシステム名> backup-operators=none
```

2.2.9 ファイルシステムのアンエクスポート

CIFS ファイルシステムをすべてアンエクスポートします。「*ユーザーズガイド*」の「*第 4 章 ファイルシステム設定の管理*」の「*ファイルシステムをアンマウントする*」を参照して設定を行ってください。

2.2.10 認証方式の設定

iStorage HS の認証方式をワークグループ（共有）認証に設定します。
システム管理者のユーザ名（既定値は sysadmin）で管理ノードに CLI ログインし、以下のコマンドを実行してください。管理ノードに接続する際には、接続先として外部フローティング IP アドレスを指定してください。コマンドに関する詳細は「*コマンドリファレンス*」の「*cifs config*」を参照してください。

```
# cifs config clear
# cifs config set authmethod=share ¥
      workgroup=<ワークグループ名> ¥
      auth={yes(パスワード認証を行う) | no(パスワード認証を行わない)}
# cifs config show
```

2.2.11 ファイルシステムのエクスポート

CIFS ファイルシステムをエクスポートします。「*ユーザーズガイド*」の「*第 4 章 ファイルシステム設定の管理*」の「*CIFS でファイルシステムを使用できるようにする*」を参照して設定を行ってください。

2.2.12 クライアントからの接続

Windows OS の net use コマンドを使用して、クライアントから接続（マウント）を行います。「*付録 A クライアントからの接続*」を参照して接続を行ってください。

Note Windows OS のバージョンによっては、ネットワークドライブを指定せずに net use コマンドを実行すると、接続に失敗する場合があります。この場合は、ネットワークドライブを指定して、再度 net use コマンドを実行してください。

Note Windows OS のバージョンによっては、Windows OS のユーザ名を net use コマンドに指定する必要があります。以下は、ユーザ名「user01」を指定した例です。

```
ユーザ名を指定する場合：
C:¥>net use Z: ¥¥<IP アドレス>¥cifs1 /user:user01 <パスワード>
```

2.3 ACL が有効なファイルシステムへの移行

本節では、ACL オプションが無効なファイルシステムを有効なファイルシステムに移行するための手順について説明します。ACL オプションが無効なファイルシステムから有効なファイルシステムに移行するためには、新規に作成した ACL が有効なファイルシステムにデータを移行します。

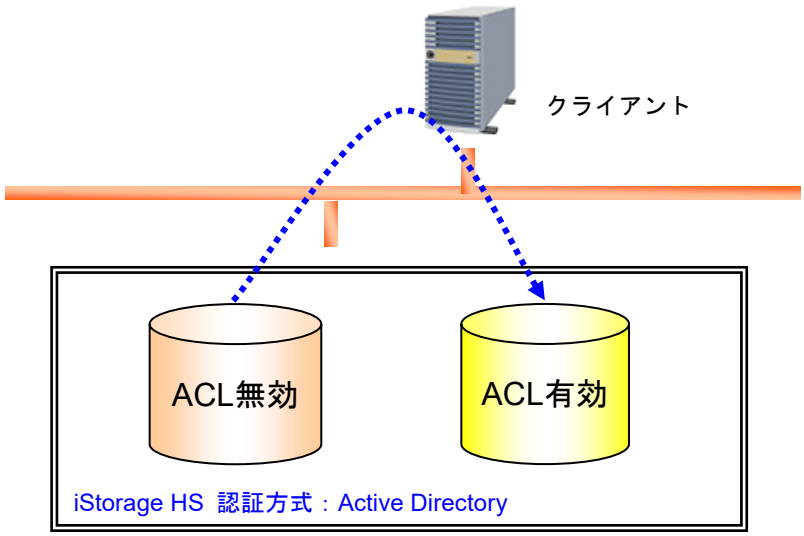


図 4 ACL が無効なファイルシステムと有効なファイルシステム間のデータ移行

2.3.1 ファイルシステムの作成

データ移行先になる ACL が有効なファイルシステムを作成します。移行するデータの格納先として十分な空き容量があることを確認してください。「*ユーザーズガイド*」の「*第 4 章 ファイルシステム設定の管理*」の「*ファイルシステムを作成する（CIFS）*」を参照して ACL オプションを有効にしたファイルシステムを作成してください。

2.3.2 クライアントからの接続

クライアントから ACL が有効なファイルシステムを接続（マウント）します。「*付録 A クライアントからの接続*」を参照して接続を行ってください。

2.3.3 ファイルシステムの ACL の設定

ACL が有効なファイルシステムにデータを格納した場合、すべてのデータに Everyone に対するフルコントロール許可の ACL が付与されます。データ格納時に付与される ACL を変更する場合は、「*第 3 章 ファイルアクセス制御*」の「*3.2 ACL の既定値*」および「*3.3 ACL の既定値の変更*」を参照して設定を行ってください。

2.3.4 データ移行

ACL が無効なファイルシステムから ACL が有効なファイルシステムへデータをコピーします。Windows クライアントから xcopy コマンド、robocopy コマンドなどを用いてデータを移行してください。データ移行したファイルの ACL には「*2.3.3 ファイルシステムの ACL の設定*」で設定した既定値が設定されます。

Note データ移行前の ACL が無効なファイルシステム上にあるデータの ACL は引き継ぐことはできません。そのため、xcopy では“/o”オプションを指定することはできません。robocopy では、“/copy:SOU”オプションを指定することはできません。

Note iStorage HS は監査機能についてはサポートしておりません。xcopy ではファイルの監査の設定をコピーするための“/x”オプションを指定することはできません。また、robocopy では“/copy:U”オプションを指定することはできません。

2.4 ACL が無効なファイルシステムへの移行

本節では、ACL オプションが有効なファイルシステムを無効なファイルシステムに移行するための手順について説明します。ACL オプションが有効なファイルシステムから無効なファイルシステムに移行するためには、新規に作成した ACL が無効なファイルシステムにデータを移行します。

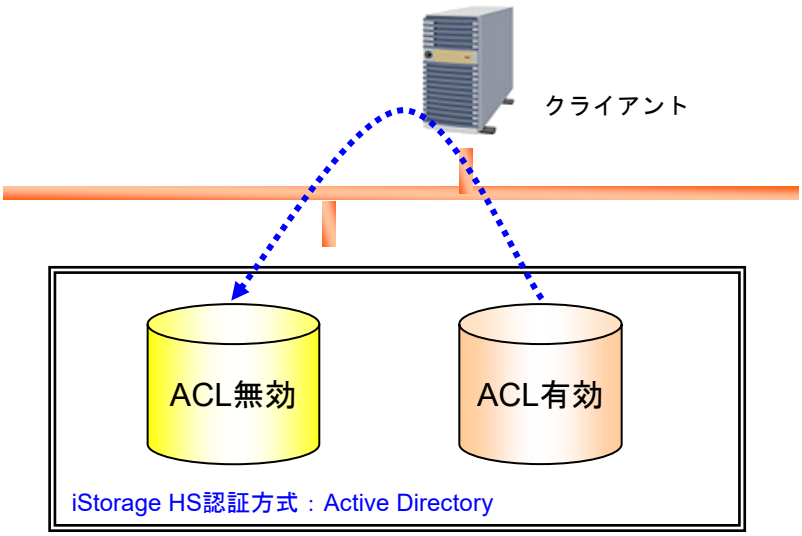


図 5 ACL が無効なファイルシステムと有効なファイルシステム間のデータ移行

2.4.1 ファイルシステムの作成

データ移行先になる ACL が無効なファイルシステムを作成します。移行するデータの格納先として十分な空き容量があることを確認してください。「*ユーザーズガイド*」の「*第 4 章 ファイルシステム設定の管理*」の「*ファイルシステムを作成する（CIFS）*」を参照して ACL オプションを無効にしたファイルシステムを作成してください。

2.4.2 クライアントからの切断

クライアントから iStorage HS を切断します。切断する前にファイルシステムにアクセスしていないことを確認してください。「*付録 B クライアントからの切断*」を参照してください。

2.4.3 Backup Operators の設定

ACL のチェックを受けない Backup Operators 権限を持つユーザで iStorage HS に接続します。

システム管理者のユーザ名（既定値は sysadmin）で管理ノードに CLI ログインし、以下のコマンドを実行してください。管理ノードに接続する際には、接続先として外部フローティング IP アドレスを指定してください。

Backup Operators 権限を与えるユーザには、Active Directory の任意のユーザを指定してください。コマンドに関する詳細は「*コマンドリファレンス*」の「*cifs*」を参照してください。

```
# cifs modify name=<ファイルシステム名> ¥
          backup-operators=<Backup Operators 権限を与えるユーザ名>
```

2.4.4 Backup Operators 権限での接続

「*2.4.3 Backup Operators の設定*」で Backup Operators 権限を与えたユーザとして、ACL が無効なファイルシステムを接続（マウント）します。「*付録 A クライアントからの接続*」を参照して接続を行ってください。Backup Operators 権限を持った sample01 ユーザで接続する場合は以下のようになります。

```
C:¥>net use Z: ¥¥<IP アドレス>¥cifs1 /user:ccc¥sample01 password01
コマンドは正常に終了しました。

C:¥>
```

2.4.5 データ移行

ACL が有効なファイルシステムから ACL が無効なファイルシステムへデータをコピーします。Windows クライアントから xcopy コマンド、robocopy コマンドなどを用いてデータを移行してください。

Note データ移行前の ACL が有効なファイルシステム上にあるデータの ACL は引き継ぐことはできません。そのため、xcopy では“/o”オプションを指定することはできません。robocopy では、“/copy:SOU”オプションを指定することはできません。

Note iStorage HS は監査機能についてはサポートしておりません。xcopy ではファイルの監査の設定をコピーするための“/x”オプションを指定することはできません。また、robocopy では“/copy:U”オプションを指定することはできません。

第3章　ファイルアクセス制御

この章では、Active Directory 認証で使用できる ACL によるアクセス制御について説明します。

3.1　ACL の概要

本節では、ACL の概要について説明します。ACL を利用することにより、ファイル、フォルダごとに「誰に対して」「どのような操作を許可するか」という属性を定義することができるようになります。 具体的には iStorage HS は以下の操作をサポートしています。

- アクセス可能なユーザ、グループの追加、削除、およびアクセス許可の設定（図 6）
- 所有者の変更（図 **7**）

Note ACL には Active Directory に登録されたグループ／ユーザのみ設定できます。Active Directory に登録されていないローカルグループ／ユーザを含めることはできません。

Note Enterprise Admins グループのメンバを使用して本製品に接続した場合、管理者特権は利用できません。

Note ビルトイングループを利用したファイル／フォルダのアクセス制御はできません。ビルトイングループの詳細については Microsoft のサポートページを参照してください。

Note 監査エントリの設定および参照はサポートしていません。本製品上のファイルに対して監査エントリを設定した場合、アクセスが拒否されます。

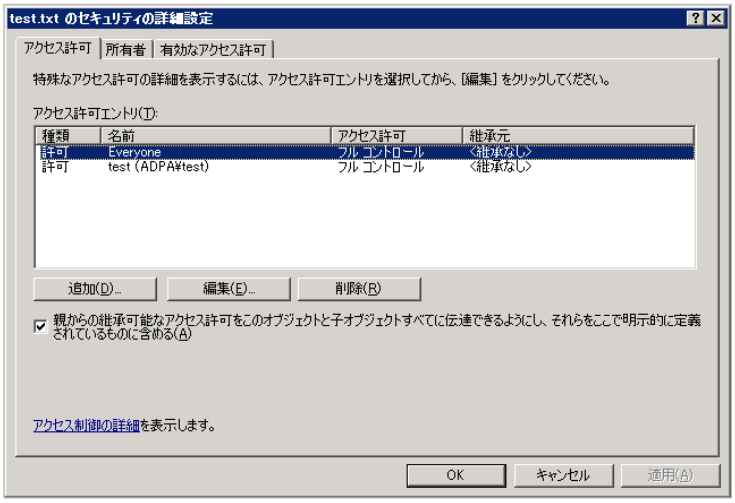


図 6　ACL の追加、編集、削除

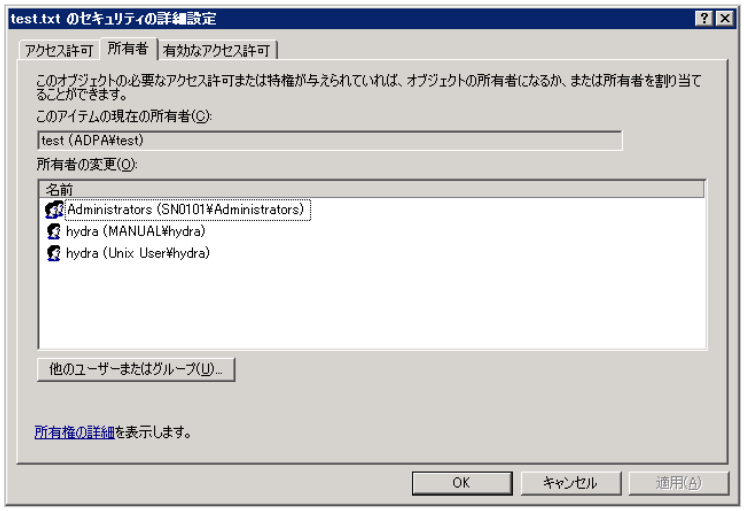

test.txt のセキュリティの詳細設定
アクセス許可
所有者
有効なアクセス許可
このオブジェクトの必要なアクセス許可または特権が与えられていれば、オブジェクトの所有者になるか、または所有者を割り当てることができます。
このアイテムの現在の所有者(O):
test (ADPA¥test)
所有者の変更(O):
名前
Administrators (SN0101¥Administrators)
hydra (MANUAL¥hydra)
hydra (Unix User¥hydra)
他のユーザーまたはグループ(U)...
所有権の詳細を表示します。
OK
キャンセル
適用(A)

図 7　所有者の変更

3.2 ACL の既定値

本節では、ファイル・フォルダに付与される ACL の既定値について説明します。
ファイル、フォルダに既定値として設定されるアクセス許可は以下の図のように Everyone グループに対するフルコントロールの許可のみとなります。また、ファイル、フォルダの所有者はファイル、フォルダの作成者となります。ファイル、フォルダの作成者が Domain Admins に属する場合は、所有者は Administrators グループとなります。

Note ファイルシステムのトップディレクトリの ACL は既定値の Everyone グループに対するフルコントロールの許可から変更しないでください。

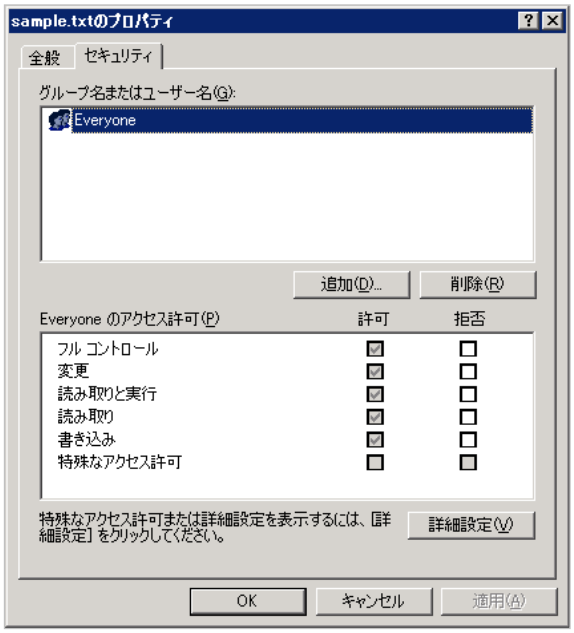


図 8 ファイルのアクセス許可

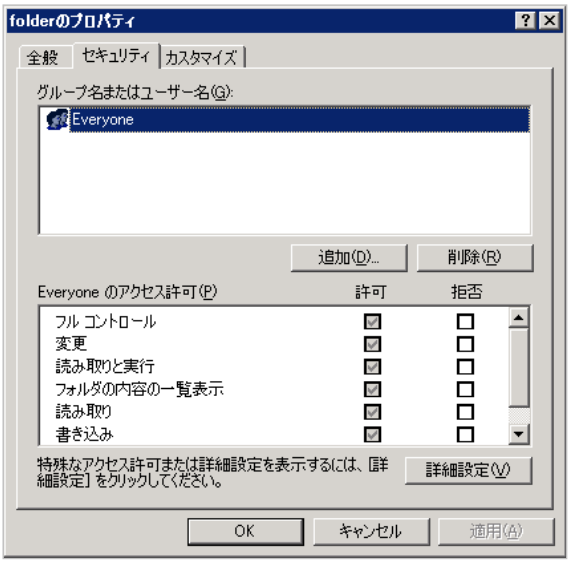


図 9 フォルダのアクセス許可

3.3 ACL の既定値の変更

本節では、ACL の既定値の変更方法について説明します。

ACL の既定値は、iStorage HS に接続する Windows クライアントからフォルダに ACL を設定することで、設定後に該当フォルダ配下に作成されるファイル、フォルダが上位フォルダの ACL を継承します。

Note ACL に設定をしていたユーザ・グループがドメインから削除されるなどにより、意図せずファイル・フォルダへのアクセスができなくなった場合、Domain Admins グループの権限を持ったユーザで接続して所有者を変更した後、所有者の権限で接続して ACL を適切に変更してください。通常、Domain Admins の権限はドメイン管理者が持っています。Domain Admins 権限での接続ができない場合、cifs acl コマンドを利用することで、指定したファイル・フォルダの ACL を Everyone グループに対するフルコントロール許可のみに変更し、アクセス可能にすることができます。コマンドに関する詳細は「*コマンドリファレンス*」の「*cifs acl*」を参照してください。

1. クライアントからエクスプローラを開きます。
2. 既定値を変更するフォルダを右クリックします。
3. プロパティを選択します。
4. 「セキュリティ」タブを選択します。

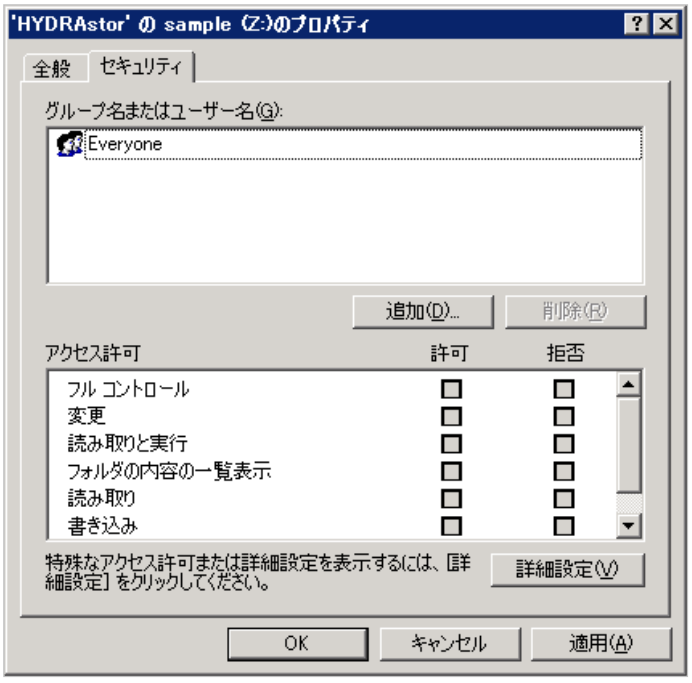


図 10 ACL の既定値の変更

5. 既定値となるユーザまたはグループを追加・削除します。
6. 既定値となるユーザ名またはグループ名のアクセス許可を設定します。
7. 「OK」をクリックします。

3.4 信頼関係先ドメインの追加

本節では、iStorage HS の所属するドメインと信頼関係が結ばれている信頼関係先ドメインの登録方法について説明します。

Note 本設定は必須ではありません。ただし、信頼関係先ドメインの設定がされていない場合、信頼関係先ドメインに登録されたユーザ、グループは iStorage HS にアクセスできません。また、信頼関係先ドメインに登録されたユーザ、グループの ACL が含まれるファイル・フォルダは、iStorage HS への書き込み・読み込みに失敗します。

Note レプリケーションの設定を行っている場合、レプリカ側も信頼関係先ドメインの設定を行ってください。詳細は「*3.5 レプリケーションの注意事項*」を参照してください。レプリケーションは、ディザスタリカバリソリューションとして、iStorage HS 間でファイルシステムをレプリケートする機能です。レプリケーション機能についての詳細は「*ユーザーズガイド*」の「*第8章 レプリケーション*」を参照してください。

具体例として、以下の図のようなドメイン A、ドメイン B、ドメイン C、ドメイン D、のドメインツリーがあり、iStorage HS がドメイン C に所属している場合の、信頼関係先ドメインの調査方法とその設定方法について説明します。

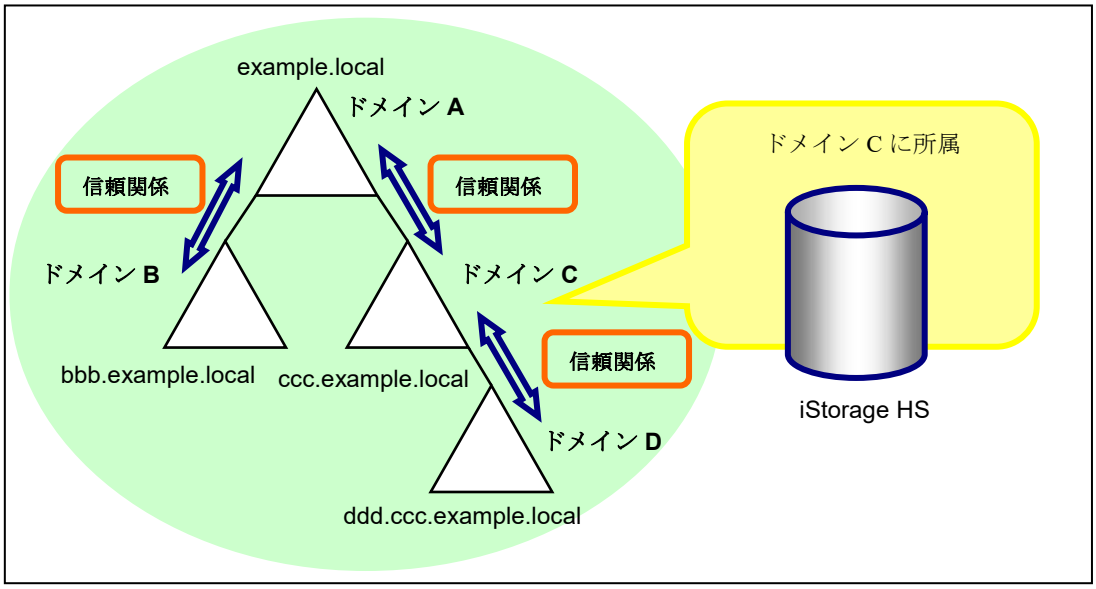


図 11 信頼関係先ドメインの設定

1. ドメイン C に所属している Windows サーバにドメイン C に所属しているユーザでログインします。

2. 所属するドメインの信頼関係先ドメインを調べるため、コマンドプロンプトから netdom コマンドを実行します。netdom コマンドは、Windows Server 2003 ではサポートツールに含まれています。Windows Server 2008 以降では標準でインストールされています。書式と実行例は以下のようになります。

（書式）

```
netdom query /Domain:<iStorage HS に設定した Active Directory の DNS ドメイン名>
     TRUST
```

（実行例）

```
C:¥>netdom query /Domain:c.example.local TRUST
信頼の方向¥信頼する側のドメイン                                    信頼の種類
========== ====================                                    ==========
<->      example.local
直接

<->      ddd.ccc.example.local
直接

<->      bbb.example.local
間接

コマンドは正しく完了しました。

C:¥>
```

3. コマンドの実行結果の「信頼する側のドメイン」に表示されるドメイン名が、設定する信頼関係先の DNS ドメイン名になります。信頼関係先 DNS ドメイン名を設定する cifs config modify コマンドは以下のようになります。「*コマンドリファレンス*」の「*cifs config*」を参照して設定を行ってください。

（実行例）

```
# cifs config modify trustdom-add=¥
     1/example.local,¥
     2/ddd.ccc.example.local,¥
     3/bbb.example.local
# cifs config show
```

3.5 レプリケーションの注意事項

本節では、CIFS でレプリケーションを作成する際の注意事項について説明します。

CIFS ファイルシステムをレプリケーションする場合、事前にマスタ側とレプリカ側のシステムが同じ認証方式になるように設定してください。また、認証方式に Active Directory を指定する場合、ドメイン環境によって設定方法が異なります。

- マスタ側とレプリカ側で所属するドメインが同じ。
  - ドメインごとに一意となる識別番号を決めてください。cifs config modify コマンドの trustdom-add パラメータで<number>を指定する際に使用します。詳細は「*コマンドリファレンス*」の「*cifs*」を参照してください。
  - マスタ側システムの信頼関係先ドメインの設定と同じ設定をレプリカ側システムに適用する場合は、マスタ側システムで cifs config show trustdomain-command コマンドを実行し、出力されるコマンドをレプリカ側システムで実行してください。詳細は「*コマンドリファレンス*」の「*cifs config*」を参照してください。

- マスタ側とレプリカ側で所属するドメインが異なる。
  - マスタ側とレプリカ側のドメインは信頼関係を結んでいる必要があります。
  - ドメインごとに一意となる識別番号を決めてください。cifs config set コマンドの domain-number パラメータの<number>および cifs config modify コマンドの trustdom-add パラメータの<number>を指定する際に使用します。詳細は「*コマンドリファレンス*」の「*cifs*」を参照してください。
  - マスタ側とレプリカ側では、iStorage HS の所属するドメインが異なるため、iStorage HS が所属するドメインの識別番号もそれぞれ異なります。しかし、GUI では iStorage HS の所属するドメインの識別番号を指定することができません（既定値の 0 が適用されます）。そのためレプリカ側での認証方式の設定には、cifs config set コマンドの domain-number パラメータでレプリカ側システムの所属するドメインの識別番号を指定してください。
  - 信頼関係先ドメインの設定には cifs config show trustdomain-command コマンドの出力結果を使用せず、cifs config modify コマンドを直接使用してください。cifs config show trustdomain-command コマンドはマスタ側とレプリカ側で所属するドメインが同じ場合に使用するコマンドです。誤って使用した場合、マスタ側とレプリカ側の ACL が不整合となります。

- レプリカ側で所属するドメインがない。
  - レプリケーションセットの作成はできますが、レプリカ側のシステムがドメインに参加するまでレプリカ側のファイルシステムにはアクセスできません。
  - ドメインごとに一意となる識別番号を決めてください。cifs config set コマンドの domain-number パラメータの<number>および cifs config modify コマンド の trustdom-add パラメータの<number>を指定する際に使用します。詳細は「*コマンドリファレンス*」の「*cifs*」を参照してください。
  - cifs config set コマンド、cifs config modify コマンドに force オプションを指定することでマスタ側と同じ認証方式を指定することができます。ドメインが存在しない環境で GUI を使用して認証方式を設定することはできません。

3.5.1 マスタとレプリカでドメインが同じ場合

レプリケーションを作成する際、マスタ側とレプリカ側で同じドメインに所属する場合のドメイン環境の設定方法について具体例で説明します。

- 以下の図のようなドメイン A、ドメイン B、ドメイン C、ドメイン D、のドメインツリーがあり、iStorage HS はドメイン C に所属している。
- ドメインの識別番号はそれぞれドメイン A が 1、ドメイン B が 3、ドメイン C が 0、ドメイン D が 2 と決定されているものとする。
- マスタ側およびレプリカ側の認証方式に Active Directory が指定されている。
- マスタ側の信頼関係先ドメインの設定はすでに行っている。

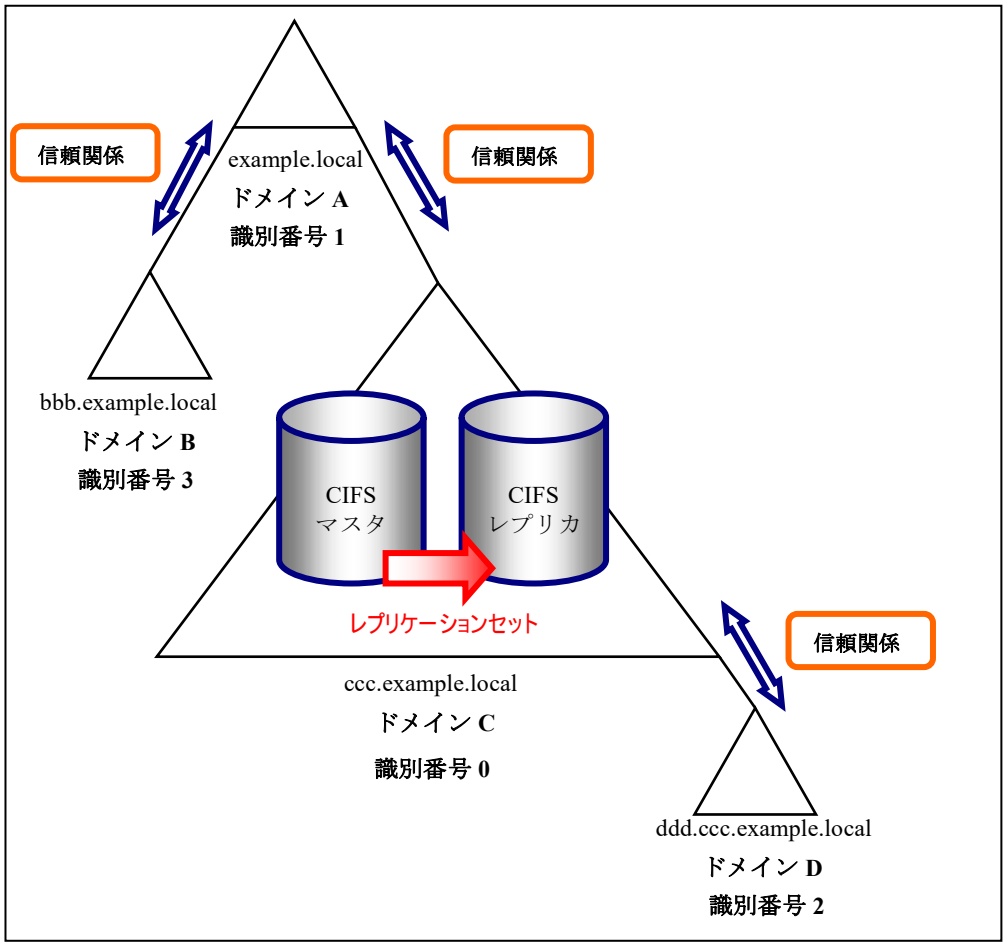


図 12 認証方式が Active Directory の場合のレプリケーション

1. マスタ側で cifs config show trustdomain-command コマンドを実行します。

```
# cifs config show trustdomain-command
CIFS Configuration
------------------------------------------------------------------------
cifs config modify trustdom-
add=1/example.local,2/ddd.ccc.example.local,3/bbb.example.local -----------
------------------------------------------------------------------
ExitStatus:0
```

2. 手順 1 の出力結果を使用してレプリカ側で cifs config modify コマンドを実行します。

```
# cifs config modify ¥
  trustdom-add=1/example.local,2/ddd.ccc.example.local,3/bbb.example.local
```

3. マスタ側とレプリカ側で cifs config show コマンドを実行し、DNS ドメイン名、信頼関係先 DNS ドメイン名に差分がないことを確認します。ドメインとドメインの識別番号の対応関係が、マスタとレプリカ側で差異がないことを確認します。

マスタ側

```
# cifs config show
CIFS Configuration
------------------------------------------------------------------------
CIFS_Config_Node               HN0101
CIFS_Config_NETBIOS            MASTER0101
CIFS_Config_Authmethod         ads
CIFS_Config_Allow              192.168.1.10
CIFS_Config_Deny               192.168.1.0/255.255.255.0
CIFS_Config_Domain             ccc
CIFS_Config_Dnsdomain          ccc.example.local
CIFS_Config_DomainNumber       0
CIFS_Config_DomainController   *
CIFS_Config_TrustDomain1       example.local
CIFS_Config_TrustDomain2       ddd.ccc.example.local
CIFS_Config_TrustDomain3       bbb.example.local
------------------------------------------------------------------------
ExitStatus:0
```

レプリカ側

```
# cifs config show
CIFS Configuration
------------------------------------------------------------------------
CIFS_Config_Node               HN0101
CIFS_Config_NETBIOS            REPLI0101
CIFS_Config_Authmethod         ads
CIFS_Config_Allow              192.168.1.10
CIFS_Config_Deny               192.168.1.0/255.255.255.0
CIFS_Config_Domain             ccc
CIFS_Config_Dnsdomain          ccc.example.local
CIFS_Config_DomainNumber       0
CIFS_Config_DomainController   *
CIFS_Config_TrustDomain1       example.local
CIFS_Config_TrustDomain2       ddd.ccc.example.local
CIFS_Config_TrustDomain3       bbb.example.local
------------------------------------------------------------------------
ExitStatus:0
```

3.5.2 マスタとレプリカでドメインが異なる場合

レプリケーションを作成する際、マスタ側とレプリカ側で異なるドメインに所属する場合のドメイン環境の設定方法について具体例で説明します。

- 以下の図のようなドメイン A、ドメイン B、ドメイン C、ドメイン D、のドメインツリーがあり、マスタ側はドメイン B、レプリカ側はドメイン C に所属している。
- ドメインの識別番号はそれぞれドメイン A が 1、ドメイン B が 0、ドメイン C が 2、ドメイン D が 3 と決定されているものとする。
- マスタ側の認証方式に Active Directory が指定されている。レプリカ側は認証方式の設定がされていない。
- マスタ側の信頼関係先ドメインの設定はすでに行っている。

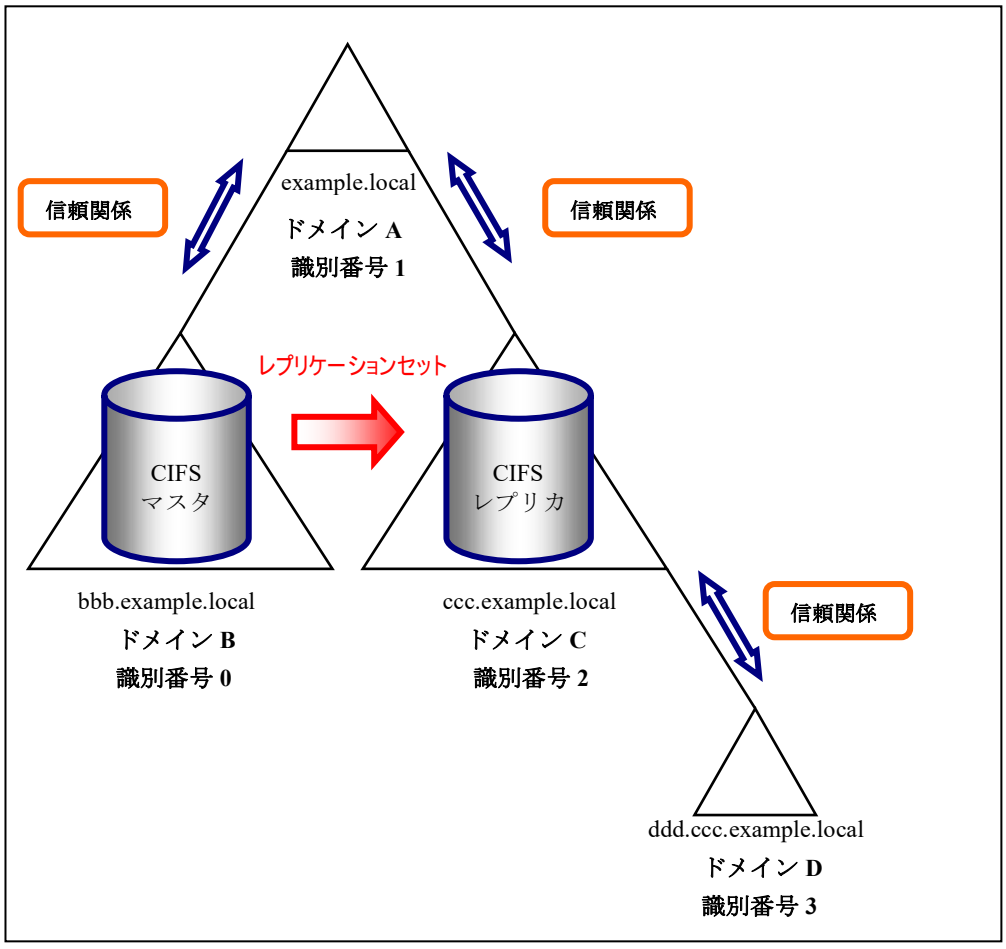


図 13 認証方式が Active Directory の場合のレプリケーション

1. マスタ側の認証方式の設定を確認します。

マスタ側

```
# cifs config show
CIFS Configuration
------------------------------------------------------------------------------
CIFS_Config_Node               HN0101
CIFS_Config_NETBIOS            MASTER0101
CIFS_Config_Authmethod         ads
CIFS_Config_Allow              192.168.1.10
CIFS_Config_Deny               192.168.1.0/255.255.255.0
CIFS_Config_Domain             bbb
CIFS_Config_Dnsdomain          bbb.example.local
CIFS_Config_DomainNumber       0
CIFS_Config_DomainController   192.168.1.3
CIFS_Config_TrustDomain1       example.local
CIFS_Config_TrustDomain2       ccc.example.local
CIFS_Config_TrustDomain3       ddd.ccc.example.local
------------------------------------------------------------------------------
ExitStatus:0
```

2. レプリカ側の認証方式を設定します。（所属するドメインの識別番号を指定するため、GUI で設定を行うことはできません。）

レプリカ側

```
# cifs config set authmethod=ads ¥
  netbios-name=REPLI ¥
  domain=ccc ¥
  dnsdomainname=ccc.example.com ¥
  domain-number=2 ¥
  dc=auto
  Please wait for a while.
  ExitStatus:0
# cifs join user=XXXXX passwd=XXXXXXXX
ExitStatus:0
```

3. レプリカ側で信頼関係先ドメインの設定を行います。

レプリカ側

```
# cifs config modify trustdom-add=
   0/bbb.example.local, ¥
   1/example.local, ¥
   3/ddd.ccc.example.local
   Please wait for a while.
   ExitStatus:0
```

4. レプリカ側で cifs config show コマンドを実行し、ドメインとドメインの識別番号の対応関係が、マスタとレプリカ側で差異がないことを確認します。

レプリカ側

```
# cifs config show
CIFS Configuration
------------------------------------------------------------------------
CIFS_Config_Node               HN0101
CIFS_Config_NETBIOS            REPLI0101
CIFS_Config_Authmethod         ads
CIFS_Config_Allow              192.168.1.10
CIFS_Config_Deny               192.168.1.0/255.255.255.0
CIFS_Config_Domain             ccc
CIFS_Config_Dnsdomain          ccc.example.local
CIFS_Config_DomainNumber       2
CIFS_Config_DomainController   *
CIFS_Config_TrustDomain0       bbb.example.local
CIFS_Config_TrustDomain1       example.local
CIFS_Config_TrustDomain3       ddd.ccc.example.local
------------------------------------------------------------------------
ExitStatus:0
```

第4章　ファイル情報

この章では、Windows と互換性のあるファイル属性およびタイムスタンプに対応したファイルシステムについて説明します。

4.1　機能概要

本製品では CIFS ファイルシステムのオプションを指定することで、Windows のファイルシステム（NTFS）と互換性のある以下のファイル情報を、保持することが可能です。

1. ファイル属性
2. タイムスタンプ

Note 代替データストリーム、監査機能についてはサポートしておりません。監査エントリを設定した場合、アクセスが拒否されます。

4.1.1 ファイル属性

本製品はファイル情報オプションのうちファイル属性対応のオプションを有効にすることで、以下のファイル属性を保持できます。

1. 読み取り専用
2. 隠しファイル
3. システムファイル
4. アーカイブ

ファイル属性対応オプションとファイル属性の対応は以下の表の通りです。

表 1 ファイル属性対応オプション

ファイル属性	ファイル属性対応オプション 無効	ファイル属性対応オプション 有効
読み取り専用	○	○
隠しファイル	×	○
システムファイル	×	○
アーカイブ	○	○

Note ファイル属性対応オプションが無効の場合、本製品に格納したファイル・ディレクトリに対して隠しファイル属性とシステムファイル属性の設定はできません。また各属性が付与されたファイルを本製品に格納した場合、隠しファイル属性、システムファイル属性の情報が破棄されます。

Note ACL 有効ファイルシステムの場合、ファイル属性対応のオプションは強制的に有効となります。

4.1.2 タイムスタンプ

タイムスタンプに対応するためのオプションとして、タイムスタンプオプションとアクセス日時オプションの 2 つがあります。

タイムスタンプオプション

オプション無効時、更新日時のみが保持されます。オプションを有効にすることで、作成日時とアクセス日時を保持することが可能となり、各タイムスタンプが 1μs から 100ns 単位に精度が向上します。

アクセス日時オプション

タイムスタンプオプション有効、かつ、アクセス日時オプション無効時、アクセス日時はクライアントからの更新処理要求があった場合のみ更新します。タイムスタンプオプション有効、かつ、アクセス日時オプションを有効時は、クライアントからの要求に関係なく、ファイル読み取りアクセスした場合、アクセス日時を更新します。

タイムスタンプオプション無効時、作成日時とアクセス日時は更新日時と同じ値になります。

各オプションとタイムスタンプの関係は以下の表の通りです。

表 2 ファイル属性対応オプション

タイムスタンプ	タイムスタンプオプション無効（既定値） アクセス日時オプション無効（既定値）	タイムスタンプオプション有効 アクセス日時オプション無効（既定値）	タイムスタンプオプション有効 アクセス日時オプション有効
作成日時	×	○	○
更新日時	○	○	○
アクセス日時	×	△	○

Note アクセス日時オプションを有効にした場合、ファイル読み込み時にタイムスタンプが更新されるため、オプション無効時と比較してファイルアクセス性能が劣化します。また、読み取りアクセスでタイムスタンプが更新されるため、更新していないファイルがレプリケーションにおいてレプリカ先システムへのコピー対象となります。

4.2 設定方法

CIFS ファイルシステムを作成する際に、ファイルシステム作成画面の高度なオプションで有効にするファイル情報オプションのチェックボックスを選択します。ACL の有効チェックボックスを選択した場合、ファイル属性は自動的に選択されます。また、タイムスタンプのチェックボックスを選択しない場合、アクセス日時のチェックボックスは選択できません。エクスポートタイプで NFS を指定した場合、ファイル情報オプションは選択できません。

Note ファイルシステム作成後はファイル情報オプションの変更はできません。

図 14 ファイル情報オプションの設定

第5章　接続制限

この章では、Windows クライアントの IP アドレスによるアクセス制御について説明します。

5.1　システム単位の設定

cifs config コマンドの allow/deny パラメータでシステム単位に Windows クライアントの接続可否を設定できます。
GUI の場合は、CIFS 画面からネットワーク制限を選択して設定してください。

allow パラメータに all を指定して deny パラメータに none を指定した場合はすべてのクライアントから接続できます。

deny パラメータに all を指定して allow パラメータを指定しない場合は、すべてのクライアントから接続ができなくなります。deny パラメータに all を指定した場合、allow パラメータに all を指定してもすべてのクライアントから接続できません。deny パラメータに all を指定して allow パラメータに IP アドレスを指定した場合は、allow パラメータに指定した IP アドレスのクライアントだけが接続できます。

allow パラメータに IP アドレスを指定して deny パラメータを指定しない場合は、allow パラメータに指定した IP アドレスのクライアントだけが接続できます。特定のクライアントからだけ接続を許可するシステムを構築する場合はこの方式を採用してください。

特定のクライアントからの接続を拒否するシステムを構築する場合は、deny パラメータに接続を拒否するクライアントの IP アドレスを指定して、allow パラメータは指定しません。

allow パラメータと deny パラメータに同じ IP アドレスを指定することは矛盾となり、機能が無効になります。
また異なる IP アドレスを、allow パラメータと deny パラメータに設定することも管理の煩雑さを増すだけであり有効ではありません。接続を許可したいクライアントの方が少なければ allow パラメータで制限し、拒否したいクライアントが少なければ deny パラメータで制限することが管理を簡単にするコツです。

管理が煩雑になるので、ファイルシステム単位に接続を制限したい場合はシステムの設定は既定値で利用することを推奨します。

5.2 ファイルシステム単位の設定

cifs export コマンドおよび cifs modify コマンドでファイルシステム単位に Windows クライアントの接続可否を設定できます。

allow パラメータに all を指定して deny パラメータに none を指定した場合はすべてのクライアントから接続できます。

deny パラメータに all を指定して allow パラメータを指定しない場合は、すべてのクライアントから接続ができなくなります。deny パラメータに all を指定した場合、allow パラメータに all を指定してもすべてのクライアントから接続できません。deny パラメータに all を指定して allow パラメータに IP アドレスを指定した場合は、allow パラメータに指定した IP アドレスのクライアントだけが接続できます。

allow パラメータに IP アドレスを指定して deny パラメータを指定しない場合は、allow パラメータに指定した IP アドレスのクライアントだけが接続できます。ファイルシステムに、特定のクライアントからだけ接続を許可したい場合はこの方式を採用してください。

特定のクライアントからの接続を拒否するファイルシステムを作成する場合は、deny パラメータに接続を拒否するクライアントの IP アドレスを指定して、allow パラメータは指定しません。

allow パラメータと deny パラメータに同じ IP アドレスを指定することは矛盾となり、機能が無効になります。
また異なる IP アドレスを、allow パラメータと deny パラメータに設定することも管理の煩雑さを増すだけであり有効ではありません。接続を許可したいクライアントの方が少なければ allow パラメータで制限し、拒否したいクライアントが少なければ deny パラメータで制限することが管理を簡単にするコツです。

第6章　セキュリティ強化

この章では、CIFS 通信のセキュリティを強化する設定について説明します。

6.1　LDAP 通信の暗号化

本節では、Active Directory 認証の使用時に、iStorage HS と Active Directory 間の LDAP 通信を暗号化する手順を説明します。

6.1.1　ルート証明書の転送

Active Directory のルート証明書を iStorage HS に転送します。転送された証明書を利用して、iStorage HS は Active Directory との LDAP 通信路を暗号化します。

FTP で iStorage HS の管理ノードに証明書を置いてください。

```
# ftp <iStorage HS の外部フローティング IP アドレス>
User: ←システム管理者のユーザ名を入力
Password:     ←システム管理者のパスワードを入力

ftp> bin
ftp> put <証明書のファイル名>
ftp> bye
```

6.1.2　認証方式の設定

FTP 接続時に指定したシステム管理者で管理ノードに CLI ログインし、以下のコマンドを実行してください。

StartTLS で暗号化する場合

```
# cifs config set authmethod=ads domain=<ドメイン名> ¥
        dnsdomainname=<DNS ドメイン名> ¥
        dc=auto ¥
        ldap-encryption=start_tls ¥
        certificate=<証明書のファイル名>
```

LDAPS で暗号化する場合

```
# cifs config set authmethod=ads domain=<ドメイン名> ¥
        dnsdomainname=<DNS ドメイン名> ¥
        dc=auto ¥
        ldap-encryption=ldaps ¥
        certificate=<証明書のファイル名>
```

付録 A クライアントからの接続

本付録では、クライアントから iStorage HS に接続する手順について説明します。

1. クライアントで、コマンドプロンプトを起動します。
2. コマンドプロンプトで net use コマンドを実行し、共有フォルダに接続します。

・ 認証方式がワークグループ（共有）の場合

ワークグループのパスワードを指定して以下のコマンドを実行し、共有フォルダ「cifs1」に接続します。

ネットワークドライブ(例「Z:」)の割り当てを行う場合：

```
C:¥>net use Z: ¥¥<IP アドレス>¥cifs1 <パスワード>
```

ネットワークドライブの割り当てを行わない場合：

```
C:¥>net use ¥¥<IP アドレス>¥cifs1 <パスワード>
```

Note Windows OS のバージョンによっては、ネットワークドライブを指定せずに net use コマンドを実行すると、接続に失敗する場合があります。この場合は、ネットワークドライブを指定して、再度 net use コマンドを実行してください。

Note Windows OS のバージョンによっては、Windows OS のユーザ名を net use コマンドに指定する必要があります。以下は、ユーザ名「user01」を指定した例です。

ユーザ名を指定する場合：

```
C:¥>net use Z: ¥¥<IP アドレス>¥cifs1 /user:user01 <パスワード>
```

・ 認証方式が Active Directory の場合

Active Directory ドメインのドメイン名、ユーザ名、およびパスワードを指定して以下のコマンドを実行し、共有フォルダ「cifs1」に接続します。

Note cifs config show コマンドで表示される CIFS_Config_Domain の値をドメイン名に指定してください。

ネットワークドライブ(例「Z:」)の割り当てを行う場合：

```
C:¥>net use Z: ¥¥<IP アドレス>¥cifs1 /user:<ドメイン名>¥<ユーザ名> <パスワード>
```

ネットワークドライブの割り当てを行わない場合：

```
C:¥>net use ¥¥<IP アドレス>¥cifs1 /user:<ドメイン名>¥<ユーザ名> <パスワード>
```

付録 B クライアントからの切断

本付録では、クライアントから iStorage HS を切断する手順について説明します。

1. クライアントで、コマンドプロンプトを起動します。
2. コマンドプロンプトで net use コマンドを実行し、接続中の共有フォルダを表示します。

```
C:¥>net use
新しい接続は記憶されます。

ステータス  ローカル名  リモート名                    ネットワーク名
-------------------------------------------------------------------------
OK          Z:        ¥¥<IP アドレス>¥cifs1      Microsoft Windows Network
OK                    ¥¥<IP アドレス>¥cifs2      Microsoft Windows Network
```

3. net use コマンドで接続中の共有フォルダを切断します。

・ ネットワークドライブの割り当てを行っている場合、以下のようにドライブ文字を指定して切断します。

```
C:¥>net use /d Z:
```

・ ネットワークドライブの割り当てを行っていない場合、共有フォルダのパスを指定して切断します。

```
C:¥>net use /d ¥¥<IP アドレス>¥cifs2
```

4. net use コマンドで切断されたことを確認します。

```
C:¥>net use
新しい接続は記憶されません。

一覧にエントリが存在しません。
```

付録 C 未サポート機能

本付録では、Windows でサポートされているが iStorage HS ではサポートしていない主な機能について説明します。

表 3　未サポート機能一覧

項番	機能		サポート状況	備考
1	認証方式	WORKGROUP	△	システムで 1 つ設定したパスワードのみで認証（ユーザは使用しない）
		Active Directory	○	
2	ACL		△	・ CIFS 認証方式が Active Directory の場合のみ ACL を設定可能 ・ ドメインに所属していないローカルグループ／ユーザの ACL を設定することはできない ・ 本製品が所属しているドメイン以外のドメインのユーザを設定することはできない ・ 監査エントリを設定することはできない ・ ファイル属性については「*4.1.1 ファイル属性*」を参照
3	日本語		△	以下の項目に日本語を使用することはできない ・ ユーザ名 ・ グループ名 ・ NetBIOS 名 ・ ファイルシステム名 ・ コメント
4	ファイル名の大文字小文字を区別しない		△	1 バイト文字のみ対応
5	フォルダリダイレクト		×	
6	移動プロファイル		×	
7	オフラインファイル		×	
8	シャドウコピー		×	
9	スナップショット		×	

項番	機能	サポート状況	備考
10	代替データストリーム	×	
11	タイムスタンプ	△	・ Windows と互換性のあるタイムスタンプ機能は WORM 機能と同時使用できない ・ 「*4.1.2 タイムスタンプ*」を参照

○：サポート

△：一部サポート

×：未サポート

付録 D CIFS 接続で使用するポート番号

本付録では、CIFS 接続時に使用するポートについて説明します。

Windows クライアントから iStorage HS へ接続する際、以下のポート番号を使用します。

表 4　Windows クライアントから iStorage HS へ接続する際に使用するポート番号

サービス	プロトコル	iStorage HS 側 ポート番号
NetBIOS	UDP	137
NetBIOS	UDP	138
NetBIOS	TCP	139
SMB	TCP	445
Kerberos	TCP/UDP	88

Note　割り当てられるポートは、ユーザの環境によって異なる場合があります。

索 引

iStorage HS シリーズ
CIFS 利用の手引き

ＩＨ１９０７－１
２０２２年　６月　初　版

日　本　電　気　株　式　会　社
東京都港区芝五丁目７番１号
TEL(03)3454-1111（大代表）