NEC

管理者ガイド（詳細編）

iStorage

iStorage NS シリーズ

70.016.01-062.02

2026 年 6 月

商標について

Microsoft、Windows、Windows Server は米国 Microsoft Corporation の米国およびその他の国における登録商標です。
ESMPRO は日本電気株式会社の商標です。

Windows Server 2025 は、Windows Server 2025 Standard、Windows Server 2025 Datacenter、Windows Server 2025 Essentials、Windows Server IoT 2025 Standard、Windows Server IoT 2025 Datacenter、Windows Server IoT 2025 Telecommunications、Windows Server IoT 2025 for Storage Standard、Windows Server IoT 2025 for Storage Workgroup の略称です。Windows Server 2022 は、Windows Server 2022 Standard、Windows Server 2022 Datacenter、Windows Server 2022 Essentials、Windows Server IoT 2022 Standard、Windows Server IoT 2022 Datacenter、Windows Server IoT 2022 Telecommunications、Windows Server IoT 2022 for Storage Standard、Windows Server IoT 2022 for Storage Workgroup の略称です。Windows Server 2019 は、Windows Server® 2019 Standard、Windows Server® 2019 Datacenter、Windows Server® 2019 Essentials、Windows Server® IoT 2019 Datacenter、Windows Server® IoT 2019 Standard、Windows Server® IoT 2019 Essentials、Windows Server® IoT 2019 Telecommunications、Windows Server® IoT 2019 for Storage Standard、Windows Server® IoT 2019 for Storage Workgroup の略称です。Windows Server 2016 は、Windows Server® 2016 Datacenter、Windows Server® 2016 Standard、Windows Server® 2016 Essentials および Windows® Storage Server 2016 Standard の略称です。Windows 11 は、Windows 11 Pro および Windows 11 Home の略称です。

本書のサンプル画像などで使用している名称は、すべて架空のものです。実在する品名、団体名、個人名とは一切関係ありません。

記載の会社名および商品名は各社の商標または登録商標です。

ご注意

(1) 本書の内容の一部または全部を無断転載することは禁止されています。

(2) 本書の内容に関しては将来予告なしに変更することがあります。

(3) NEC の許可なく複製・改変などを行うことはできません。

(4) 本書の内容および本書を使用した結果について明示的にも黙示的にも一切の保証を行いません。

はじめに

NAS (Network Attached Storage) は、既存環境に対する変更を加えることなく、大規模ストレージシステムを提供するネットワーク接続型ストレージです。
一般的に NAS は導入が容易です。ネットワーク管理や OS に関する広範な知識がなくとも使用することができ、通常、管理業務はクライアントからリモートデスクトップ経由で行うことができます。ユーザーは NAS をネットワークに接続して電源を投入し、最小限のセットアップ作業を行うだけで運用を開始することができます。
iStorage NS シリーズは NAS アプライアンスであり、CIFS、NFS、FTP、HTTP のマルチプロトコルに対応しています。Windows や UNIX、Linux などが混在する既存のネットワーク環境に設置するだけで、簡単にそのネットワーク環境の記憶容量を拡張することができます。

管理者ガイドは、【概要編】および【詳細編】の二部で構成されています。【概要編】または【詳細編】のみに記載している内容もございますので、各ガイドの目次を参考にして、目的に応じて参照してください。

管理者ガイドは改版される場合があります。以下の Web ページを参照し、ご利用の機種の最新版をダウンロードしてください。
https://www.support.nec.co.jp/View.aspx?NoClear=on&id=3170101815（2026 年 6 月 1 日現在）

【注意】
iStorage NS シリーズは、Windows Server IoT 2025 for Storage を使用して作成されたファイルサーバー専用機です。標準の Windows Server とは違い、ファイルサーバー以外でのご利用はできませんのでご注意ください。

各操作画面の説明

iStorage NS にリモートデスクトップで接続し、サインインすると、デスクトップ画面に管理者メニューとサーバーマネージャーが自動起動します。

管理者メニュー

管理者メニューは、iStorage NS 専用のメニュー画面で管理者がよく使う機能を簡単に起動することができます。管理者メニューは、デスクトップのショートカットからも起動できます。

【補足】

管理者メニューを自動起動しないようにしたい場合は、管理者権限のコマンドプロンプトにて以下のコマンドを実行します。

del "C:¥ProgramData¥Microsoft¥Windows¥Start Menu¥Programs¥Startup¥管理者メニュー.lnk"

なお、管理者メニューを手動で起動する場合は、デスクトップ上の [管理者メニュー] アイコンをダブルクリックしてください。

サーバーマネージャー

サーバーマネージャーは、Windows Server に標準で組み込まれている管理機能です。各機能の呼び出しや、役割と機能の追加なども行うことができます。

【補足】

サーバーマネージャーを自動起動しないようにしたい場合は、右上の [管理] をクリックし、[サーバーマネージャーのプロパティ] を起動して、[ログオン時にサーバーマネージャーを自動的に起動しない] をチェックした後、[OK] をクリックします。

目次

1 iStorage NS の共有領域を作る

- **Windows** クライアントからアクセスする
- **UNIX** クライアントからアクセスする
- **FTP** クライアントからアクセスする
- **Web** クライアントからアクセスする

1.1 Windows クライアントからアクセスする

SMB（Server Message Block）共有を作成する方法については、【管理者ガイド（概要編）共有を作成する】をご覧ください。作成した共有に Windows クライアントからアクセスする方法については、【管理者ガイド（概要編）Windows クライアントからアクセスする】をご覧ください。

1.2 UNIX クライアントからアクセスする

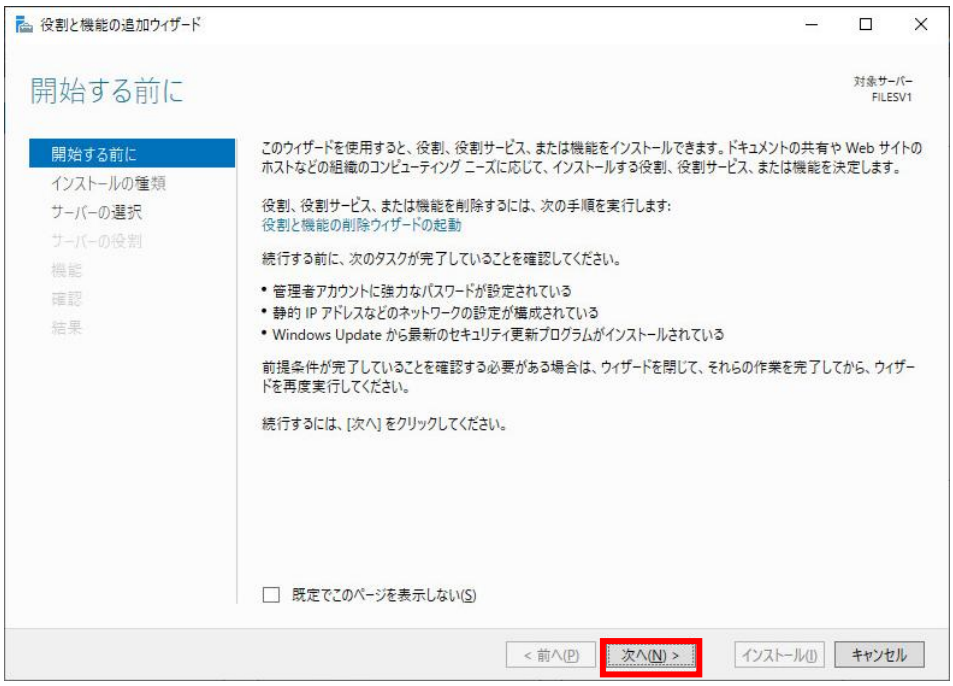
NFS 共有を使用することで、UNIX クライアントから iStorage NS 上のフォルダーやファイルへアクセスすることが可能になります。なお、Server for NFS サービスでは、NFS のバージョンは、v2、v3、v4.1 をサポートしています。

1.2.1 Server for NFS サービスの有効化

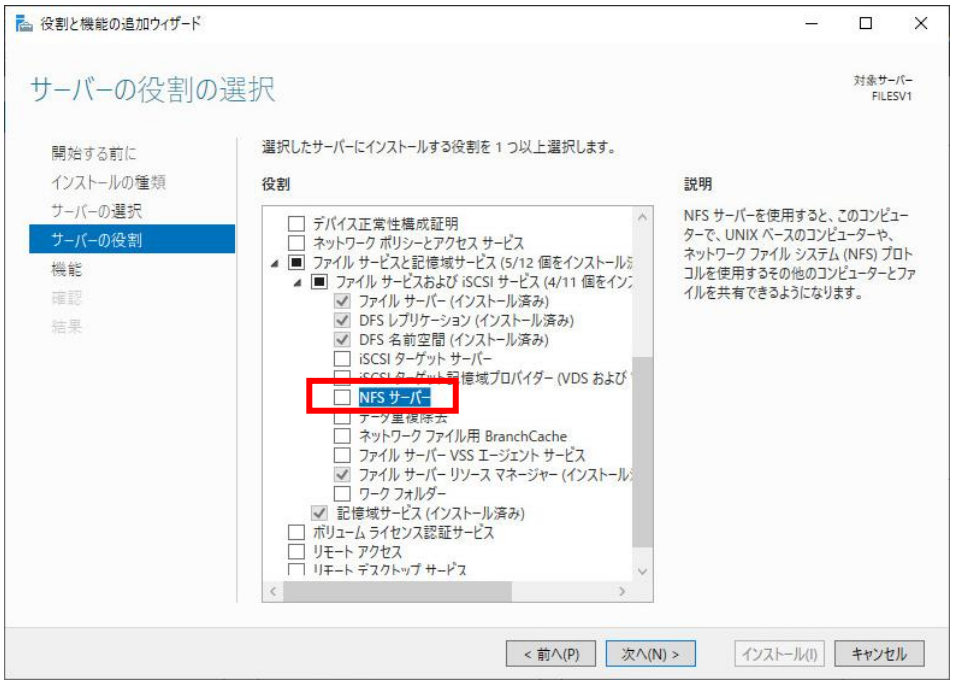
iStorage NS は工場出荷時に、Server for NFS サービスを無効化しています。
NFS アクセスを行う場合は、最初に Server for NFS サービスを下記の手順で有効化してください。

1. サーバーマネージャーを起動し [役割と機能の追加] をクリックします。

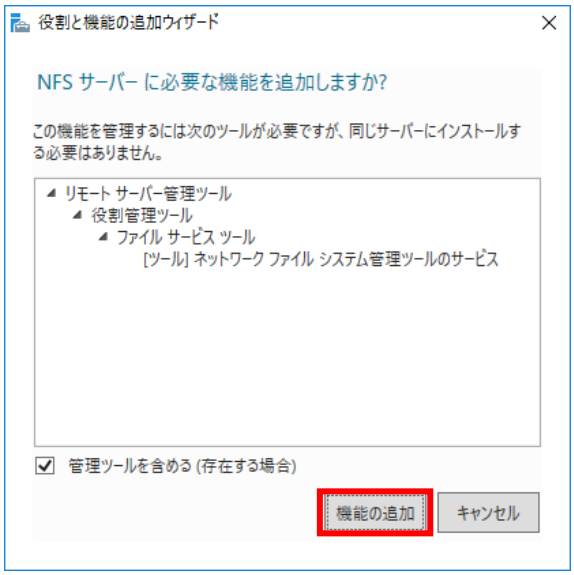
2. [開始する前に] 画面が表示されますので、デフォルト状態のまま [次へ] ボタンをクリックして、[サーバーの役割の選択] 画面まで進みます。



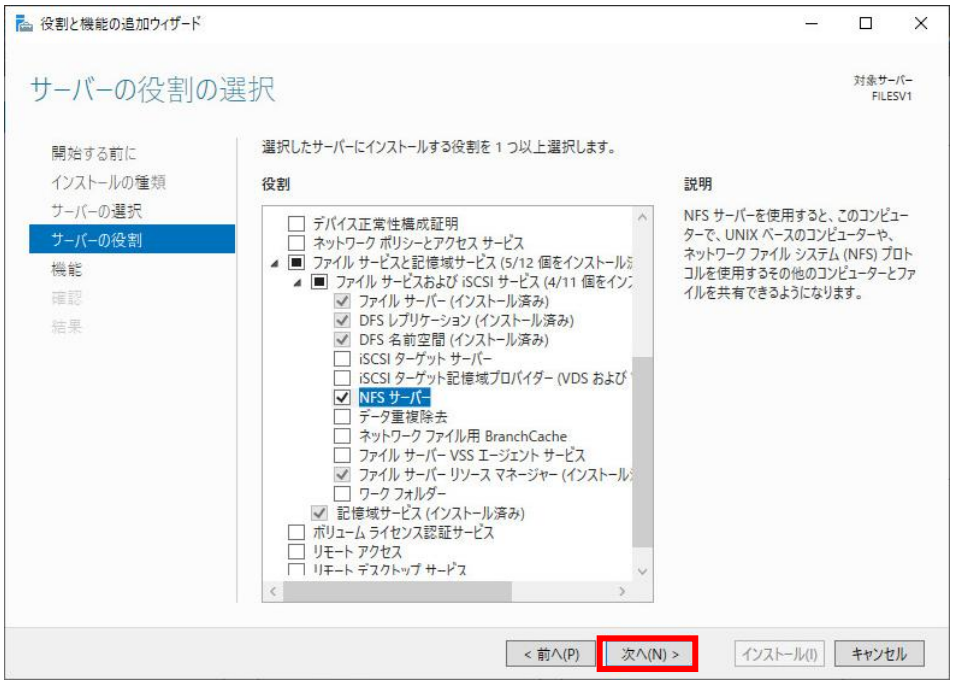
3. [サーバーの役割の選択] 画面の [ファイルサービスと記憶域サービス]、[ファイルサービスおよび iSCSI サービス] を順に展開して、 [NFS サーバー] をチェックします。



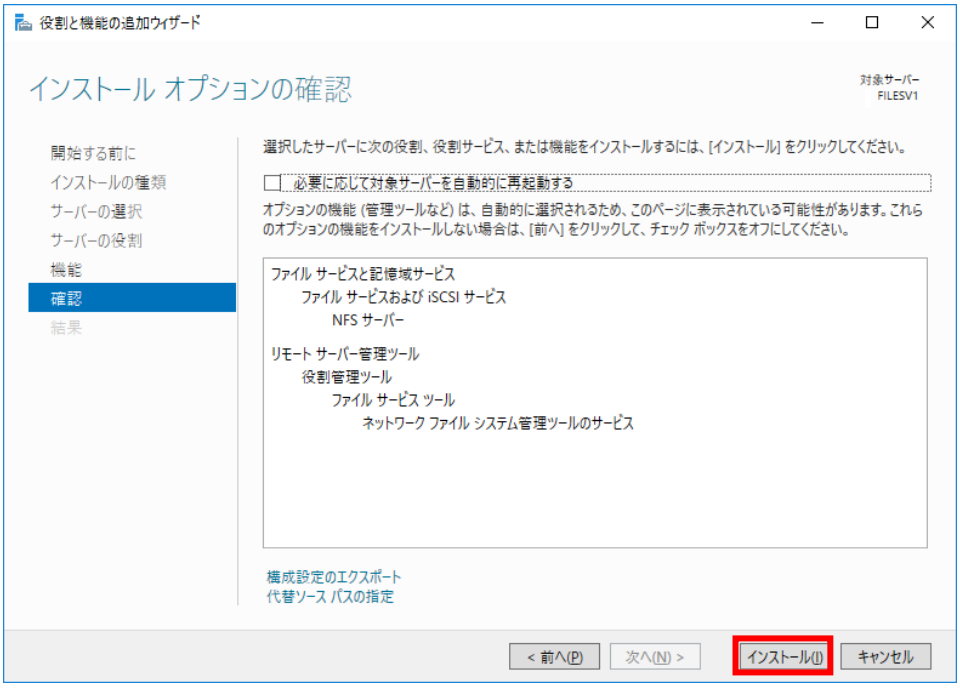
4. [NFS サーバーに必要な機能を追加しますか？] 画面が表示されますので、 [機能の追加] をクリックします。



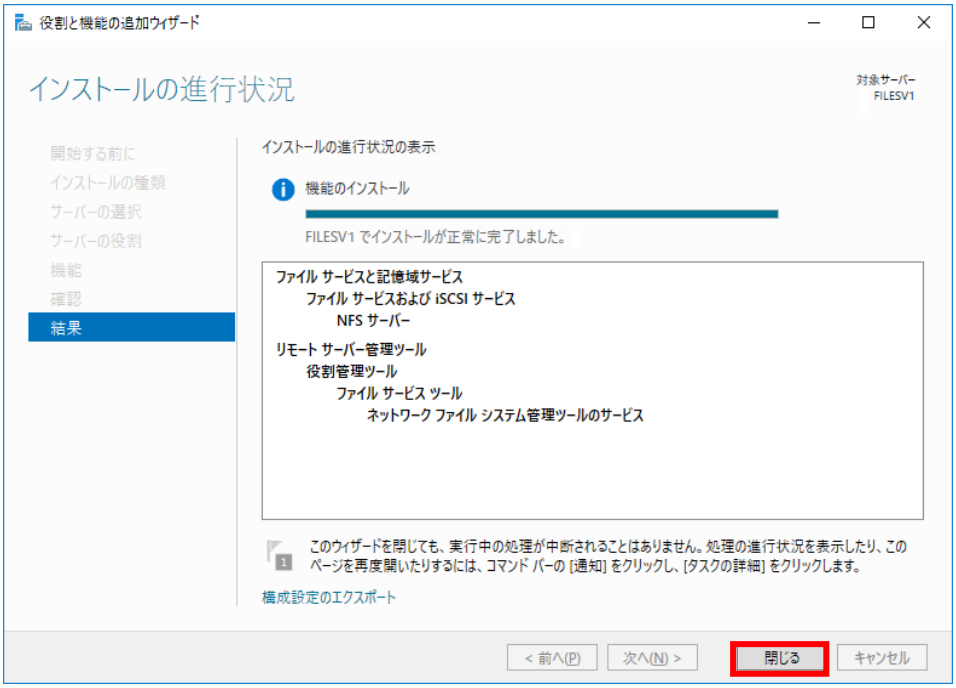
5. [サーバーの役割の選択] 画面に戻りますので、[次へ] をクリックします。



6. [機能の選択] 画面が表示されますので [次へ] をクリックして、[インストールオプションの確認] 画面に進み、[インストール] をクリックします。

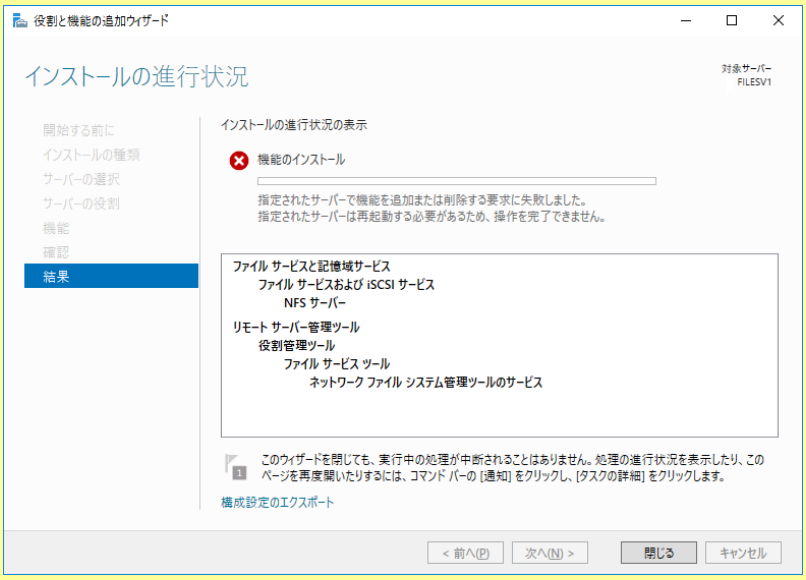


7. [インストールの進行状況] 画面が表示されますので、インストールの完了を待ち、[閉じる] をクリックします。



【注意】

Server for NFS サービスを有効化する際、以下のメッセージが表示されて、Server for NFS サービスの有効化に失敗する場合があります。



これは、Server for NFS サービスで使用する 111 番ポートを、他のアプリケーションが使用している状態でサービスの有効化を行った場合に起きる事象です。事前にアプリケーション側でポートマップ機能が使用するポート番号を変更し、再度、Server for NFS サービスを有効化してください。ポート番号の変更方法は、アプリケーション側にご確認ください。

1.2.2 ユーザー/グループのマッピングについて

UNIX クライアントが iStorage NS 上の NFS 共有にアクセスする場合、UNIX のユーザー ID およびグループ ID を使用します。しかし、iStorage NS の OS は、Windows Storage Server となっているため、Windows のユーザー ID およびグループ ID に変換しなければなりません。この変換を "ユーザーマッピング" と呼びます。

システム環境に応じて、以下のマッピング方法を使用します。
マッピングが完了した後、NFS 共有を作成します。

- ドメイン環境の場合

  ドメインコントローラーの Active Directory を使用して、ドメインユーザーと UNIX ユーザーをマッピング
- ワークグループ環境の場合

  iStorage NS 上の Active Directory ライトウェイト ディレクトリ サービス（AD LDS）を使用して、ローカルユーザーと UNIX ユーザーをマッピング

1.2.3 ドメイン環境におけるマッピング

ドメイン環境におけるマッピングを行うには、あらかじめ、UNIX アカウントとのマッピングを行う Windows アカウントをドメインコントローラーに登録しておく必要があります。
本書では、必要な Windows アカウントが既にドメインコントローラーに登録されているものとして、ユーザーマッピングの手順を説明します。

1.2.3.1 NFS ID マッピングソースの設定

Server for NFS サービスが、ユーザーマッピング情報をドメインコントローラーから参照するように設定します。

1. Windows PowerShell を起動し、以下のコマンドを実行します。
   Set-NfsMappingStore -EnableADLookup $true -ADDomainName “< AD の DNS 名>”
   例)
   Set-NfsMappingStore -EnableADLookup $true -ADDomainName “example.com”

2. 設定を反映させるため、Server for NFS サービスを再起動します。
   nfsadmin server stop
   nfsadmin server start

3. 以下のコマンドを実行して、設定内容を確認します。
   Get-NfsMappingStore

   [確認する項目]
   ADDomain : < AD の DNS 名>
   ADLookupEnabled : True

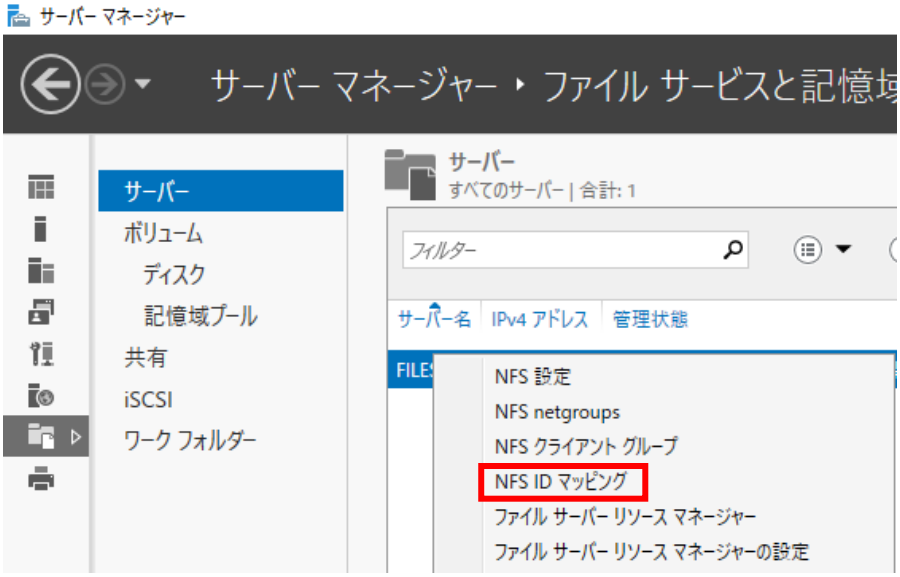
1.2.3.2 ユーザーおよびグループのマッピング設定

以下の手順で、ユーザーおよびグループのマッピングを設定します。

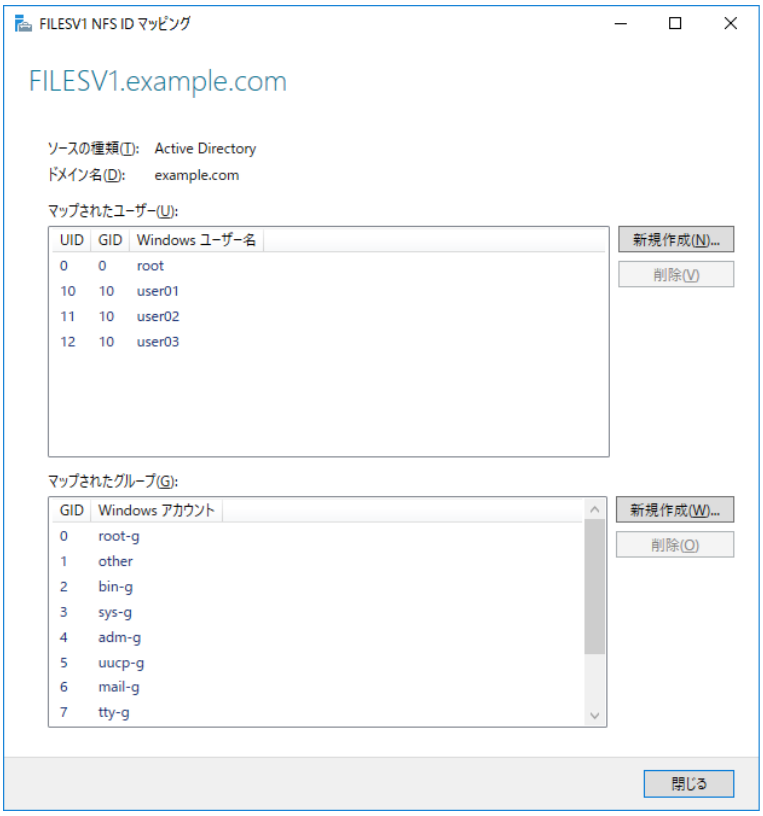
1. iStorage NS に、ドメインの Administrator でサインインします。

2. サーバーマネージャーの左ペインの [ファイル サービスと記憶域サービス] をクリックします。

3. 右ペインのサーバー一覧から該当のサーバーを選択して右クリックし、表示されるメニューの [NFS ID マッピング] をクリックします。



4. 以下のような、NFS ID マッピングの画面が表示されますので、グループ、ユーザーの順に、[新規作成] ボタンにてマッピングを追加してください。



1.2.4 ワークグループ環境におけるマッピング

iStorage NS 上のローカルアカウントと UNIX アカウントとのユーザーマッピングを実現するために、AD LDS の有効化と設定、および、NFS ID マッピングソースの設定を行う必要があります。

【注意】

- AD LDS を用いてのマッピングでは対象サーバーのローカルユーザーとのマッピングが行われます。つまり、ユーザー管理は個々のサーバーで行われますので、フェイルオーバー環境のホストにおいて同じユーザー名を作成しマッピングしたとしても、フェイルオーバーした際、それぞれで SID が異なるためアクセス権は引き継がれません。そのため、Windows クラスター環境では、ドメインコントローラーの Active Directory を使用する方法でマッピングを行ってください。
- AD LDS でユーザーマッピングを行っている環境において、Windows クライアントから作成されたファイルを NFS クライアントから参照した場合、グループ名には 4294967294 や -2 、nobody 、nogroup 等が表示される仕様です。

【注意】

ユーザーマッピングに際しては、UNIX クライアントの passwd/group ファイルを準備する必要があります。

- 本機に UNIX クライアントを 1 台のみ接続する場合は、該当の UNIX クライアントの passwd/group ファイルを準備してください。
- 複数台の UNIX クライアントを接続する場合は、それぞれの passwd/group ファイルをマージしたものを準備してください。なお、マージした passwd/group ファイルでは、ユーザーID およびグループ ID、ユーザー名、グループ名が重複しないように調整してください。

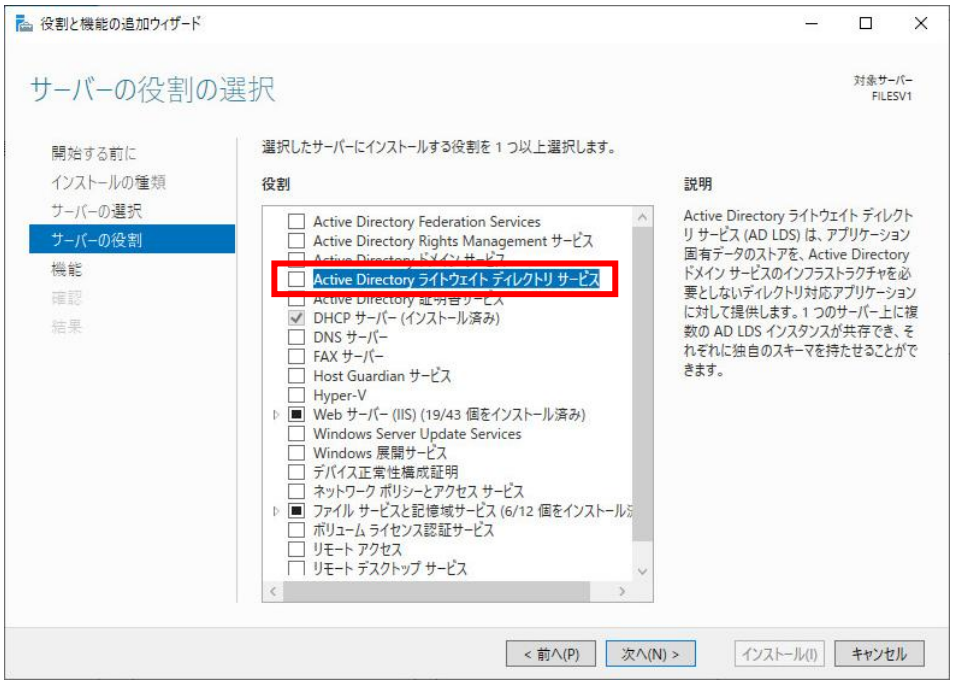
passwd / group ファイル間に重複した名前が存在する場合 （例えば、passwd ファイルと group ファイルに root が存在する場合など）はエラーとなりますので、事前に重複した名前が存在しないように名前を変更してください。

1.2.4.1 AD LDSの有効化

1. サーバーマネージャーを起動し [役割と機能の追加] をクリックします。

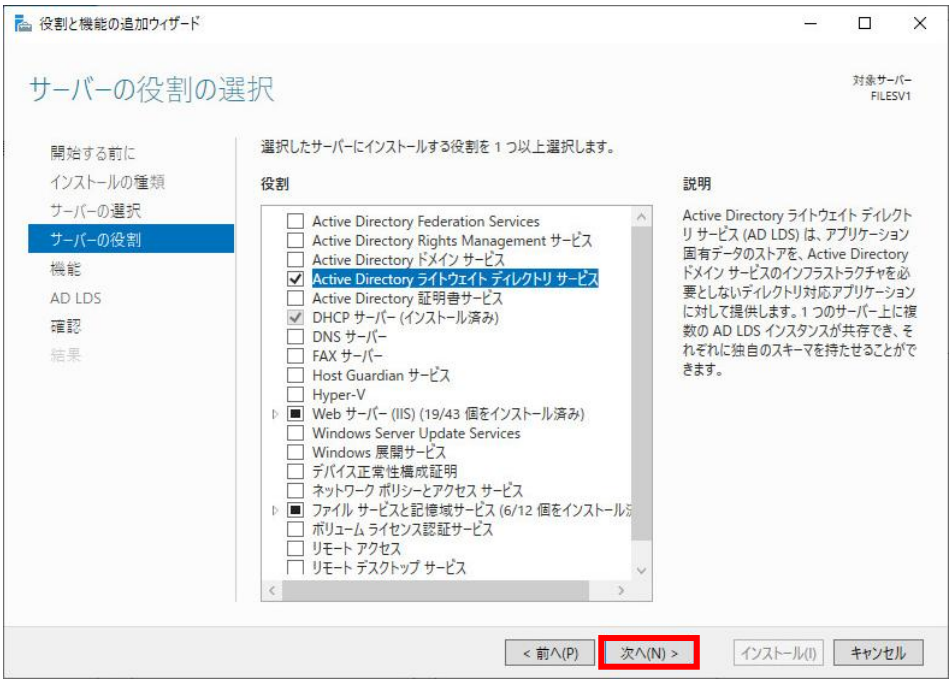
2. [開始する前に] 画面が表示されますので、デフォルト状態のまま [次へ] ボタンをクリックして、[サーバーの役割の選択] 画面まで進みます。

3. [サーバーの役割の選択] 画面の役割から、[Active Directory ライトウェイト ディレクトリ サービス] をチェックします。

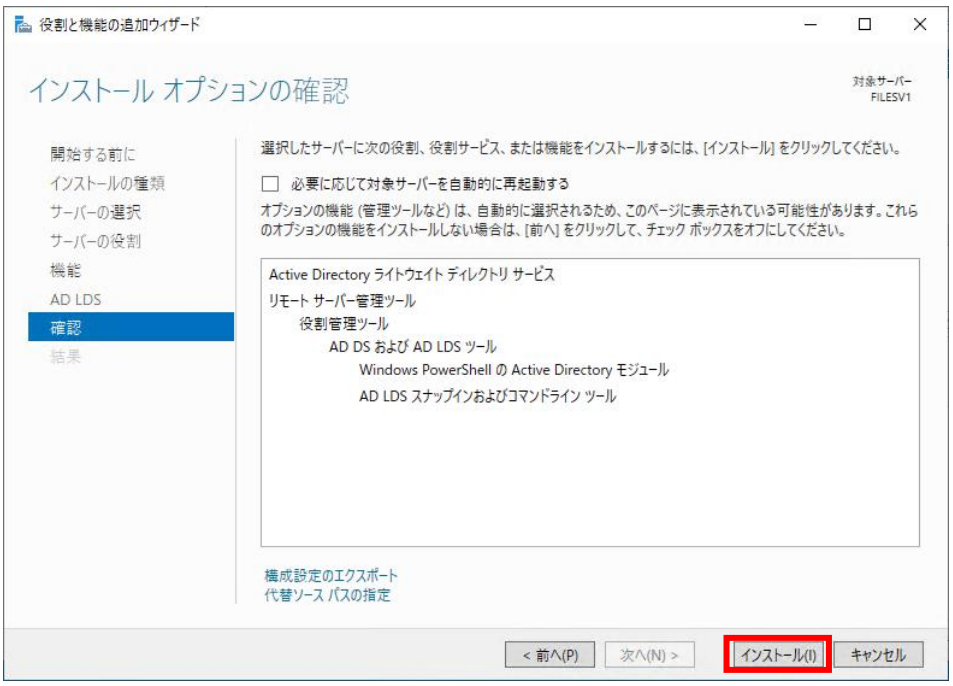


4. [Active Directory ライトウェイト ディレクトリ サービス に必要な機能を追加しますか？] 画面が表示されますので、 [機能の追加] をクリックします。

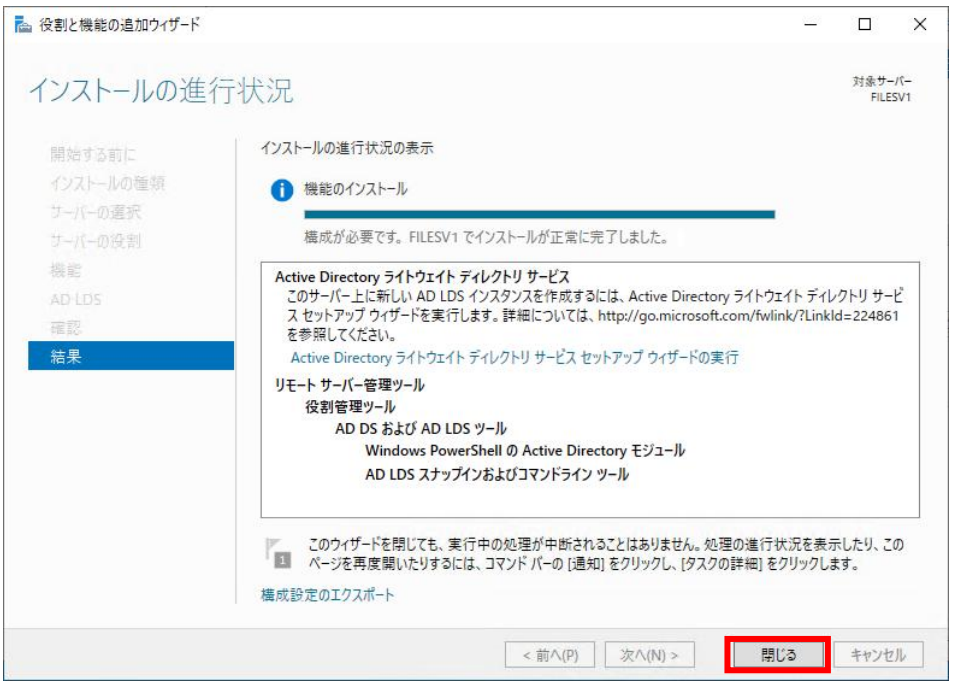
5. [サーバーの役割の選択] 画面に戻りますので、[次へ] をクリックします。



6. [機能の選択] 画面が表示されますので、デフォルト状態のまま [次へ] ボタンをクリックして、 [インストールオプションの確認] 画面まで進み、[インストール] をクリックします。



7. [インストールの進行状況] 画面が表示されますので、インストールの完了を待ち、[閉じる] をクリックします。



8. AD LDS を有効化するために、システムを再起動します。

1.2.4.2 AD LDSの設定

【補足】
手動でマッピングを追加する場合は、下記手順の 2. および 3. のみ実施後、【NFS ID マッピングソースの設定】に進み、NFS ID マッピングソースを設定してください。その後、NFS ID マッピング画面の [新規作成] ボタンにて、グループ、ユーザーの順に、手動でマッピングを追加してください。
UNIX の root ユーザーを Windows の管理者権限を持つユーザーにマッピングする際は、Windows のビルトイン Administrator は特別な位置づけのユーザーのため、管理者グループに所属する、ビルトイン Administrator 以外のユーザーをマッピングしてください。

1. 準備した passwd / group ファイルを本機の任意のフォルダーに格納します。

2. ビルトインの Administrator でサインインし、管理者メニューからコマンドプロンプトを起動します。

3. C:¥NEC¥iStorageNS¥nfs に移動し、下記コマンドを実行して、AD LDS に CN=Nfsadmin,DC=nfs のインスタンスを作成します。

   > factory-setup-adlds.cmd

4. C:¥NEC¥iStorageNS¥nfs 配下の add-map-users.cmd ファイルをメモ帳(notepad.exe)で開き、環境に合わせて環境変数に値 (以下の各行の = より右の部分) を設定し、上書き保存します。

   set PASSWD="<格納パス>¥passwd"
   set GROUP="<格納パス>¥group"
   set USERPASSWORD=Abc-123456

   [各環境変数の説明]
   PASSWD : 格納した passwd ファイルの絶対パス (記述例: D:¥work¥passwd)
   GROUP : 格納した group ファイルの絶対パス (記述例: D:¥work¥group)
   USERPASSWORD : コマンドで作成するすべての Windows ユーザーの初期パスワード。なお、初期パスワードは、6 文字以上で、英大文字、英小文字、数字、記号の文字の 4 つの種類のうち 3 つの種類が使用されている必要があります。(記述例: Abc-123456)

5. 下記コマンドを実行して、Windows ローカルユーザーの作成、および、UNIX ユーザーとのマッピングを行います。

   > add-map-users.cmd

   コマンドの実行結果は、C:¥NEC¥iStorageNS¥nfs¥configure-adlds.txt に出力されますので必ず確認してください。

6. 管理者メニューから [ローカルユーザーとグループ] を起動し、passwd ファイルに記載されているユーザーと、group ファイルに記載されているグループが作成されていることを確認します。

【補足】

- 本手順で作成される Windows ユーザーはすべて一般ユーザーです。必要に応じて管理者権限を付与してください。また、root ユーザーに関しては必ず管理者権限を付与してください。
- 本手順で作成される Windows ユーザーのパスワードは、add-map-users.cmd で指定した値で一律設定されますので、適宜、変更してください。なお、デフォルトではパスワードには有効期限が設定されており、パスワードの有効期限を過ぎてしまうと NFS 共有へのアクセスが出来なくなりますのでご注意ください。
- ユーザー/グループを再度追加する場合は、追加するユーザー/グループのみを記述した passwd / group ファイルを作成し、上記の add-map-users.cmd を必要に応じて編集した後、実行してください。
- 本手順を実施した際に、configure-adlds.txt に「指定されたアカウント名は既にグループのメンバーです。」というメッセージが記録されますが、処理は正しく行われているため、問題はありません。
- Windows 上にすでに UNIX ユーザー名/グループ名と同じ名前のユーザー/グループが存在していた場合、configure-adlds.txt に「アカウントは既に存在します。」や「指定されたローカル グループは既にあります。」というメッセージが記録されますが、マッピング自体は行われますので、その他の部分にエラーが記録されていなければ問題はありません。

1.2.4.3 NFS ID マッピングソースの設定

Server for NFS サービスが、ユーザーマッピング情報を AD LDS から参照するように設定します。

1. Windows PowerShell を起動し、以下のコマンドを実行します。なお、<対象サーバー名>には、iStorage NS のコンピューター名を指定します。

   Set-NfsMappingStore -EnableLdapLookup $true -LdapServer “<対象サーバー名>:389”

   例)

   Set-NfsMappingStore -EnableLdapLookup $true -LdapServer “FILESV1:389”

2. 設定を反映させるため、Server for NFS サービスを再起動します。

   nfsadmin server stop

   nfsadmin server start

3. 以下のコマンドを実行して、設定内容を確認します。

   Get-NfsMappingStore

   [確認する項目]

   LdapServer : <対象サーバー名>:389

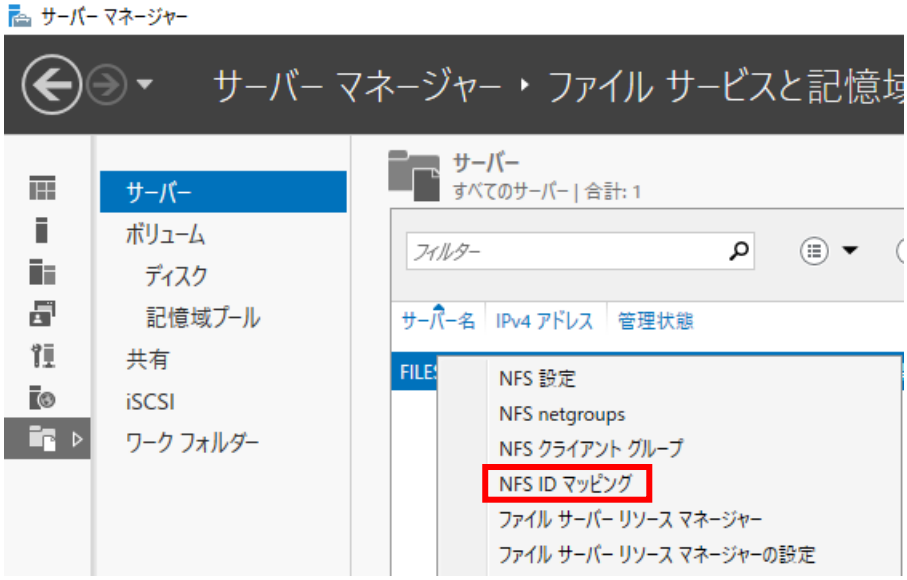
   LdapLookupEnabled : True

1.2.4.4 マッピングされたユーザーおよびグループの確認

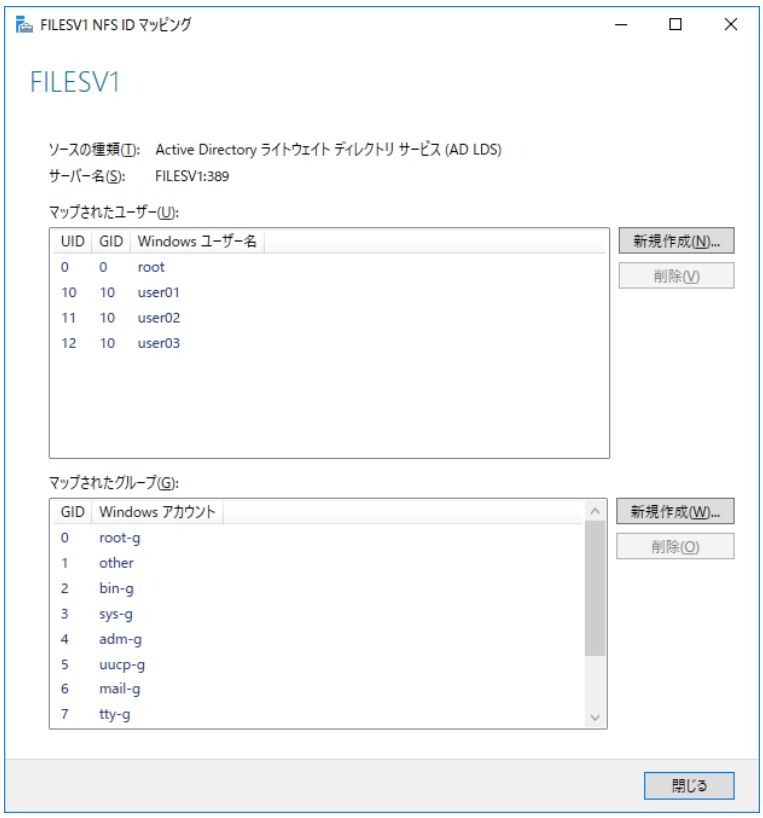
NFS ID マッピングでマッピングされたユーザーおよびグループは、以下の手順で確認することができます。

1. サーバーマネージャーの左ペインの [ファイル サービスと記憶域サービス] をクリックします。

2. 右ペインのサーバー一覧から該当のサーバーを選択して右クリックし、表示されるメニューの [NFS ID マッピング] をクリックします。



3. 以下のような、NFS ID マッピングの画面が表示されますので、[マップされたユーザー] および [マップされたグループ] に表示されている内容が、意図した通りのマッピングになっているか確認します。



1.2.5 NFS 共有を作成する

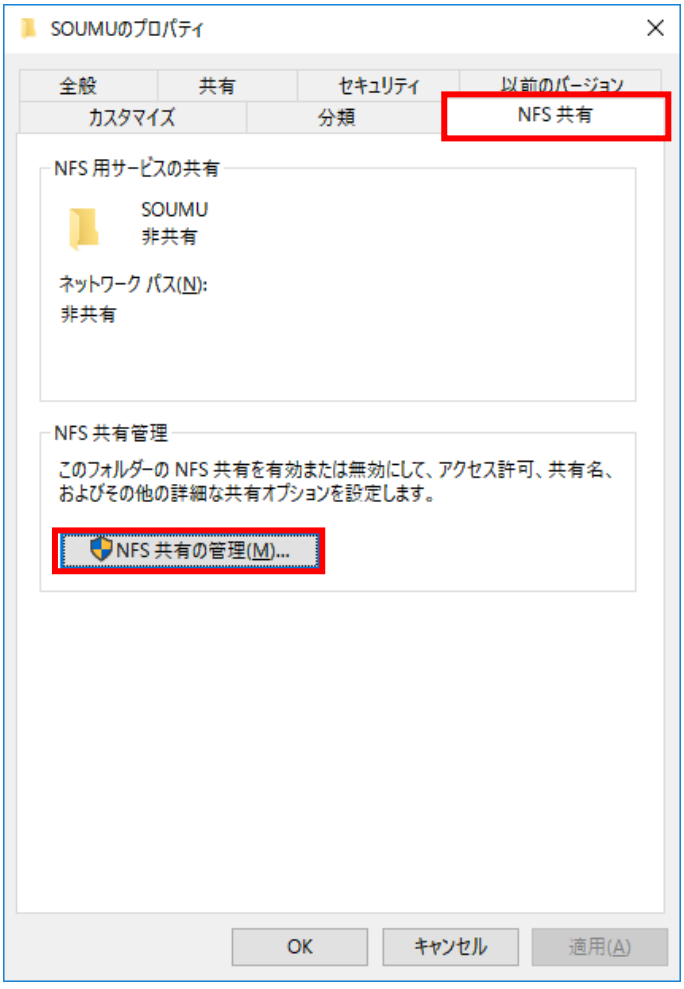
以下に、エクスプローラーより NFS 共有を作成する方法を説明します。

1.2.5.1 NFS 共有の設定方法

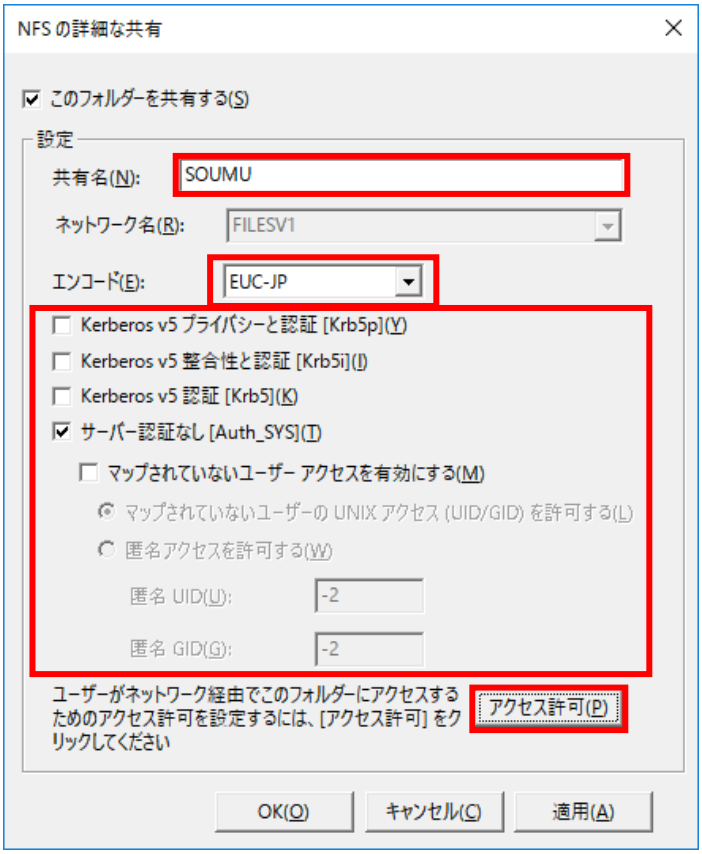
1. iStorage NS に Administrator でサインインします。

2. エクスプローラーにて、NFS 共有を行うフォルダーを新規に作成します。

3. 上記フォルダーのプロパティを開き、[NFS 共有] タブを選択して [NFS 共有の管理] ボタンをクリックします。



4. [このフォルダーを共有する] をチェックし、[共有名] に NFS 共有名を設定します。必要に応じて [エンコード] を設定し、認証方式を設定 (下記例では [サーバー認証なし [Auth_SYS]] のみチェック) して [アクセス許可] ボタンをクリックします。



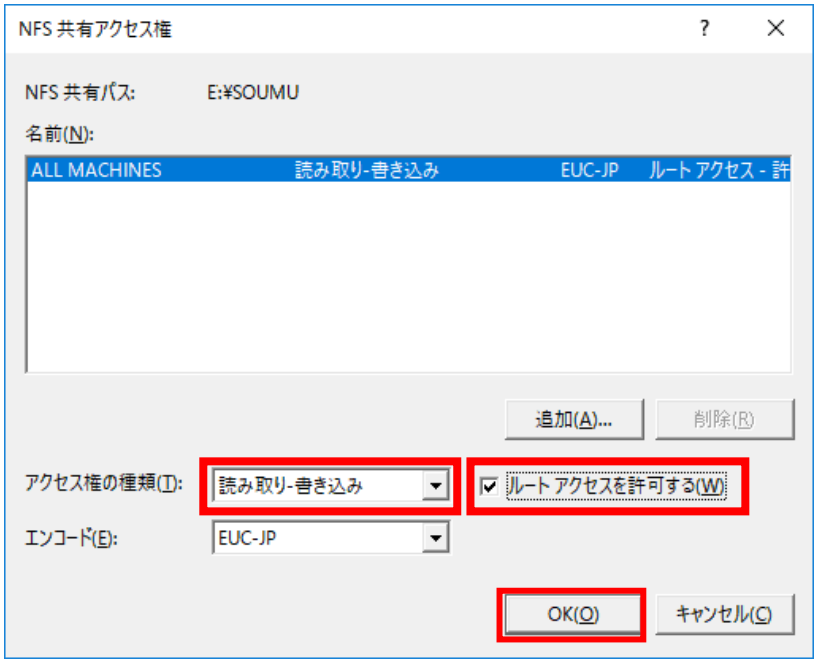
【注意】

- NFS 共有で設定する共有名に DBCS（2 バイト）文字は使用できません。
- Windows と UNIX でフォルダー/ファイル名に使用するエンコードが異なる場合、UNIX 上でフォルダー/ファイル名が文字化けすることがあります。
- 使用可能なエンコードは、クライアントからマウントする際に使用する NFS バージョンによって異なります。

NFS バージョン	v2, v3	v4.1
使用可能なエンコード	ANSI, BIG5, EUC-JP, EUC-KR, EUC-TW, GB2312-80, KSC5601, Shift-JIS	UTF-8

- [エンコード] 欄では UTF-8 は指定できません。UNIX で使用しているエンコードが UTF-8 の場合は、NFS v4.1 を使用してマウントしてください。なお、その場合、[エンコード] の値は無視されます。

5. 本共有にアクセスするすべての UNIX クライアントに対するアクセス許可を設定します。UNIX クライアントの root ユーザーにアクセス権限を与える場合は、[ルートアクセスを許可する] をチェックします。設定が完了したら、[OK] ボタンをクリックします。



【補足】

- NFS 共有にてアクセス権を設定する際には、本画面のアクセス権の種類の設定は「読み取り-書き込み」とし、NTFS のアクセス権の設定により、マッピングしたユーザーのアクセス権を設定することをお勧めします。
- 共有にアクセスするクライアントが複数あり、文字コード体系が混在している、もしくはクライアント毎にアクセス権を設定する必要がある、という場合はクライアントグループを利用します。クライアントグループを利用するには、上記画面の [追加] をクリックして、あらかじめ作成しておいたグループに対して設定を行います。クライアントグループの作成と設定方法については【クライアントグループ】を参照してください。

6. [NFS の詳細な共有] 画面に戻りますので、 [OK] ボタンをクリックします。

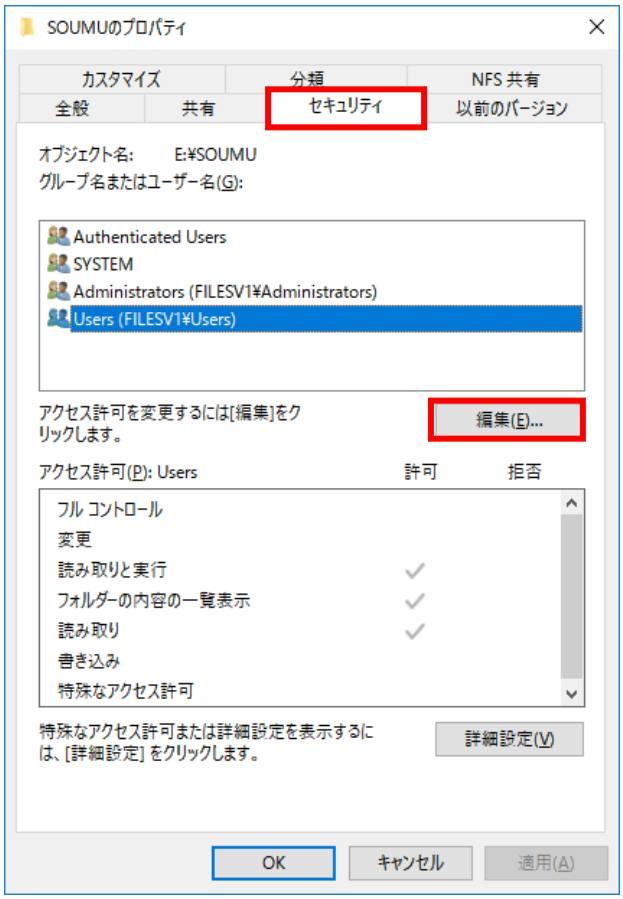
1.2.5.2 NFS 共有フォルダーのアクセス権設定

NTFS ボリュームに作成したフォルダーには、通常、上位フォルダーから引き継がれた NTFS のアクセス権が設定されています。作成したフォルダーを NFS 共有フォルダーとして設定し、NFS クライアントから UNIX ユーザーがアクセスできるようにするためには、アクセスする UNIX ユーザーをマッピングした Windows ユーザーに対して、NTFS のアクセス権を適切に設定する必要があります。

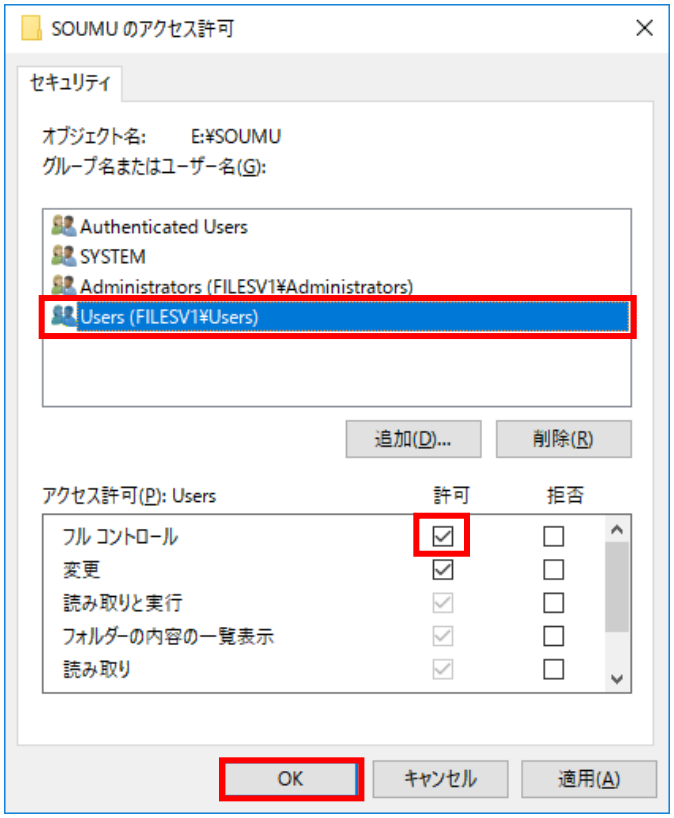
ここでは、例として、iStorage NS の出荷時のデータボリューム直下にフォルダー(*) を作成し、NFS 共有設定を行うケースにおいて、UNIX ユーザーが読み書き可能なアクセス権を設定する手順について説明します。このとき、UNIX ユーザーをマッピングした Windows ユーザーが Users グループに所属しているものとします。

(*) データボリューム直下に作成したフォルダーには、ルートフォルダーから継承した NTFS アクセス権が設定されており、Users グループには、読み取り専用のアクセス権しか設定されていません。

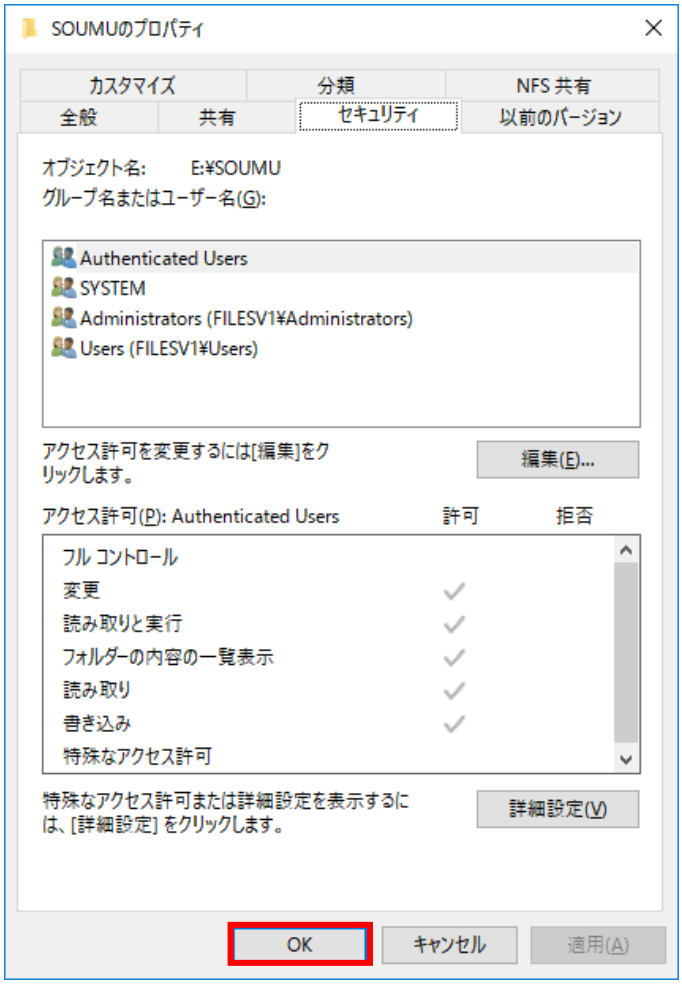
1. NFS 共有フォルダーのプロパティ画面にて、[セキュリティ] タブを選択して [編集] ボタンをクリックします。



2. アクセス許可設定画面の [グループ名またはユーザー名] の一覧にて “Users” を選択し、[アクセス許可] の一覧にて “フル コントロール” の 許可 のチェックボックスにチェックを入れ、[OK] をクリックします。



3. プロパティ画面で [OK] をクリックします。



【補足】

NFS 共有配下に NFS クライアントからフォルダー/ファイルを作成した場合、一般的な UNIX システムと同様、上位フォルダーからのアクセス権の継承は行われません。そのため、該当フォルダー/ファイルには、Windows 上の Administrators、SYSTEM、Backup Operators 等のユーザーからもアクセスができない状態となり、Windows 側にて該当フォルダー/ファイルを含むバックアップを実施するとアクセスが失敗します。

Windows システムと同様にアクセス権の継承を有効にしたい場合は、以下のレジストリを設定してください。

キー: HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥ServerforNFS¥CurrentVersion¥Mapping

名前: KeepInheritance

種類: REG_DWORD

値: 0 (上位フォルダーのアクセス権を継承しない:既定値)

1 (上位フォルダーのアクセス権を継承する)

※設定変更後は、以下のコマンドにて NFS サーバーサービスの再起動が必要です。

nfsadmin server stop

nfsadmin server start

1.2.6 クライアントグループ

1 つの共有にアクセスするクライアントが複数あり、文字コード体系が混在している、もしくはクライアント毎にアクセス権を設定する必要がある、という場合はクライアントグループを作成し、エンコードやアクセス権を設定することができます。
ここではクライアントグループの作成方法、共有フォルダーに対してクライアントグループ毎の設定を行う方法を説明します。なお、クライアントグループに対して行った設定は、共有に対する設定より優先的に動作します。

1.2.6.1 クライアントグループの作成

クライアントグループの作成は以下の手順で行います。

1. ビルトインの Administrator でサインインし、管理者メニューの [コマンドプロンプト] をクリックします。

2. nfsadmin コマンドを使用して、クライアントグループを作成します。
   以下にコマンド例を示します。詳細はコマンドヘルプ(nfsadmin server /?) を参照願います。

   【クライアントグループ名：group1 を作成する場合】
   nfsadmin server creategroup group1

3. nfsadmin コマンドを使用して、クライアントグループに登録するメンバー（クライアント） を指定します。

   【クライアントグループ名：group1 に IP アドレス：10.10.10.1 のクライアントを追加する場合】
   nfsadmin server addmembers group1 10.10.10.1

   【クライアントグループ名：group1 にコンピューター名：client1 のクライアントを追加する場合】
   nfsadmin server addmembers group1 client1

4. nfsadmin コマンドを使用して、作成したクライアントグループを確認します。

   【クライアントグループ名の一覧を表示させる場合】

   nfsadmin server listgroups

5. nfsadmin コマンドを使用して、作成したクライアントグループのメンバーを確認します。

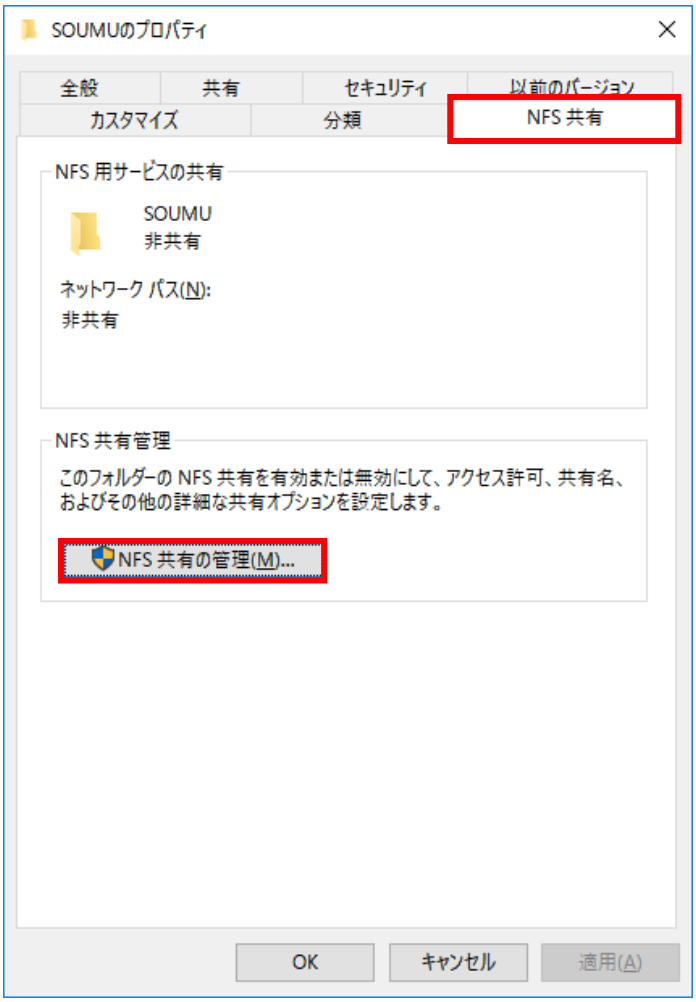
   【クライアントグループ名:group1 内の登録メンバーの一覧を表示させる場合】

   nfsadmin server listmembers group1

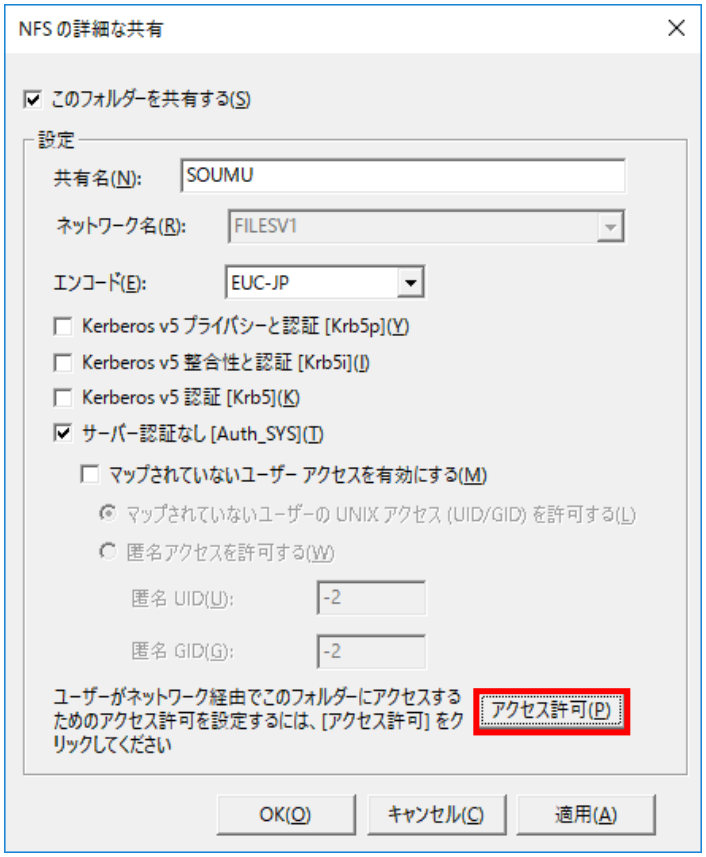
1.2.6.2 クライアントグループの割り当て

作成したクライアントグループを用いて、共有フォルダーにエンコードやアクセス権の設定を行う方法を説明します。

1. エクスプローラーにて クライアントグループの割り当てを行うフォルダーのプロパティを開き、[NFS 共有] タブを選択して [NFS 共有の管理] ボタンをクリックします。



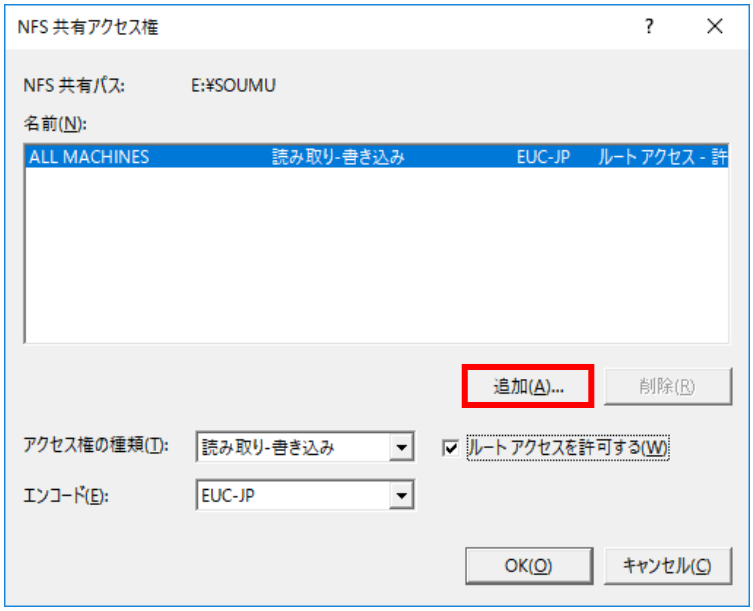
2. [アクセス許可] ボタンをクリックします。



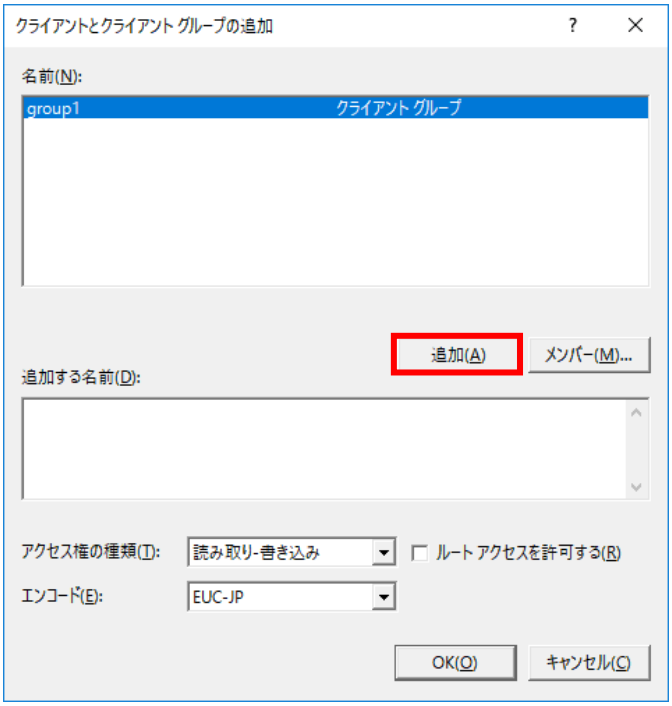
【注意】

[NFS の詳細な共有] 画面に表示されている内容は、本共有にアクセスするすべての UNIX クライアントに対するアクセス許可の設定です。クライアントグループ毎のアクセス権やエンコードの設定は、[アクセス許可] ボタン押下後に行います。

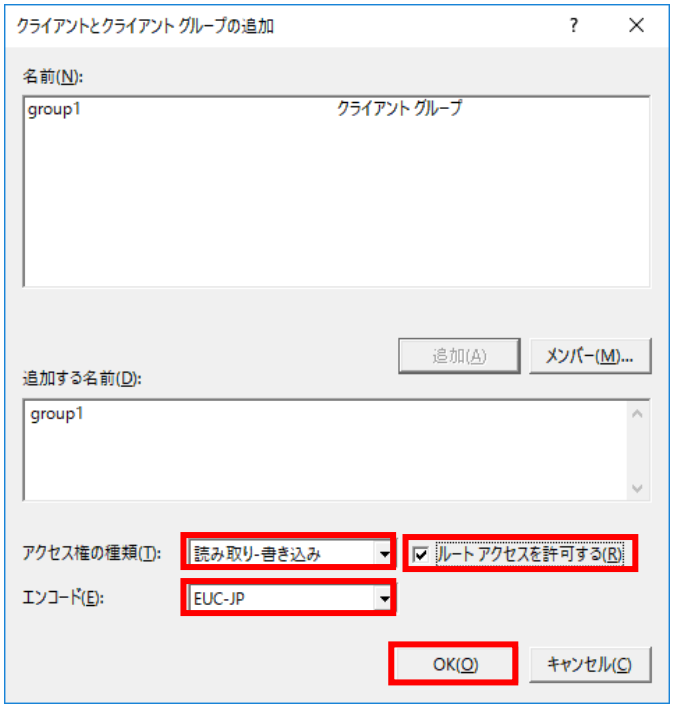
3. クライアントグループを割り当てる共有の NFS 共有アクセス権 の設定画面にて [追加] ボタンをクリックします。



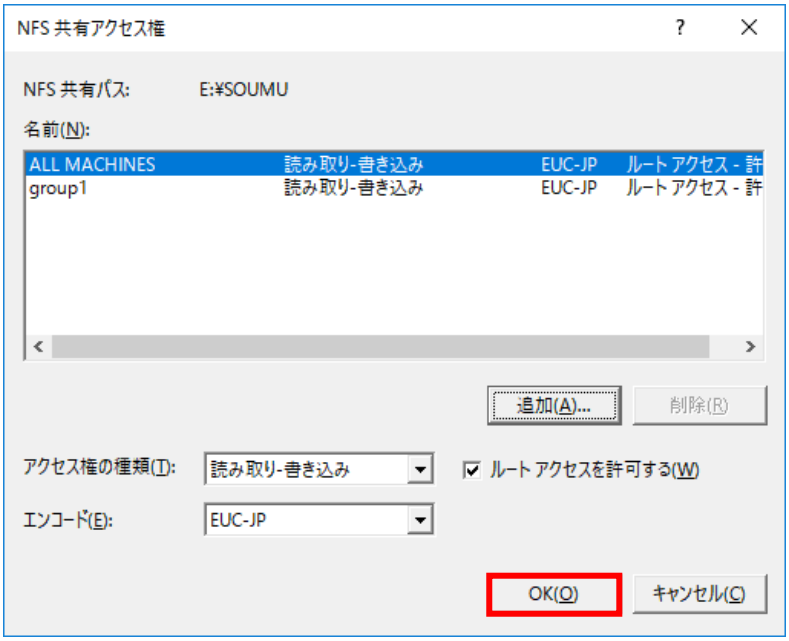
4. [クライアントとクライアントグループの追加] 画面が表示されますので、クライアントグループを選択し、[追加] ボタンをクリックします。



5. [追加する名前] にクライアントグループが表示されていることを確認し、[アクセス権の種類] と [エンコード] 、[ルートアクセスを許可する] の有無を設定し、[OK] ボタンをクリックします。



6. クライアントグループが追加されていることを確認し、[OK] ボタンをクリックします。



7. [NFS の詳細な共有] 画面に戻りますので、 [OK] ボタンをクリックします。

1.2.7 ファイルのロック時間について

UNIX よりファイルにロックを掛けた状態で Server for NFS サービスが再起動した場合、ロック状態を保持する時間が設定できます。その時間を過ぎるとファイルのロックは解除されます。
ロックの保持時間は、下記の手順で設定します。

1. Windows PowerShell を起動し、以下のコマンドを実行します。

   [NFS v2, v3 で接続しているクライアントに対して]

   Set-NfsServerConfiguration -NlmGracePeriodSec <ロック保持時間(秒)>

   [NFS v4.1 で接続しているクライアントに対して]

   Set-NfsServerConfiguration -GracePeriodSec <ロック保持時間(秒)>

   ※ LeasePeriodSec の値を変更している場合、ロック保持時間には、少なくともその 2 倍の値を設定してください。

2. 設定を反映させるため、Server for NFS サービスを再起動します。

   nfsadmin server stop

   nfsadmin server start

3. 以下のコマンドを実行して、設定内容を確認します。

   Get-NfsServerConfiguration

1.2.8 環境差異の対応

1.2.8.1 文字コードについて

Windows 環境と UNIX 環境での文字コードの違いは運用に影響を与えることがあります。iStorage NS 上に SMB 経由で日本語のファイル名でファイルを作成した場合、UNIX 環境から NFS 経由でこのファイルが存在するフォルダーを [ls –al] コマンド等で参照すると、日本語のファイル名が正しく表示されない問題が起こる可能性があります。これは、UNIX 環境で使われている文字コードと iStorage NS が標準で使用している文字コード体系が異なるためです。そのため日本語のファイル名を UNIX 環境で利用する場合は、NFS 共有のプロパティを設定する際に適切なエンコード（例えば、EUC-JP 等）を選択してください。なお、NFS v4.1 を使用してマウントしている場合は、プロパティの設定によらず、エンコードには UTF-8 が使用されます。

1.2.8.2 NFS 共有の文字変換マッピングについて

UNIX 環境では、ディレクトリ/ファイル名に以下の文字を使用することができます。しかし、これらの文字は、Windows のファイルシステムではフォルダー/ファイル名には使用できません。

使用不可文字： ¥ : * ? " < > |

NFS v2/v3 を使用して NFS 共有をマウントする場合は、設定ファイル(テキストファイル)を使って文字変換マッピングを行うことにより、UNIX クライアント側では上記使用不可文字を含むディレクトリ/ファイル名を使用できます。iStorage NS 上では、文字変換マッピングにて変換されたフォルダー/ファイル名で表示されます。

[例] コロン (:) とアルファベットの B (全角) をマッピングした場合。
－ UNIX クライアント上では aaa:bb.txt と表示されます。
－ iStorage NS 上では aaaBbb.txt と表示されます。

なお、NFS v4.1 を使用して NFS 共有をマウントする場合は、文字変換マッピングの設定を行っても変換機能は動作しないため、Windows のファイルシステムで許可されていない文字は UNIX クライアントではフォルダー/ファイル名には使用できません。

1.2.8.2.1. 設定ファイルの記述フォーマット

設定ファイルの記述フォーマットは以下です。

0xnn 0xnn : 0xnn 0xnn ; コメント
① ② ③

nn は、2 バイトの UNICODE の 1 バイト分を、16 進数で指定したものです。
①は、UNIX 環境で使用される文字の UNICODE です。
②は、Windows 環境で使用される文字の UNICODE です。
③は、コメントとなり、無視されます。

設定ファイルのサンプル

以下に設定ファイルの記述例を示します。

―――― ファイル記述例(サンプル) ――――

0x00 0x5c : 0xff 0x21 ; (¥) →（A）に変換する

0x00 0x3a : 0xff 0x22 ; (:) →（B）に変換する

0x00 0x2a : 0xff 0x23 ; (*) →（C）に変換する

0x00 0x3f : 0xff 0x24 ; (?) →（D）に変換する

0x00 0x22 : 0xff 0x25 ; (″) →（E）に変換する

0x00 0x3c : 0xff 0x26 ; (<) →（F）に変換する

0x00 0x3e : 0xff 0x27 ; (>) →（G）に変換する

0x00 0x7c : 0xff 0x28 ; (|) →（H）に変換する

――――――――――――――――――――――――――――

【補足】

- 一つの文字を、二つ以上の文字とマッピングさせないでください。
- ピリオド (.) は、マッピングの対象にしないでください。
- 変換後の文字には、NFS クライアント側で未使用の文字(全角文字など)を使用してください。
- Windows 上のフォルダー/ファイル名を UNIX クライアントで表示した場合、本マッピングルールが適用されますので、変換に際しては Windows 上で使用頻度の低い文字を設定してください。

1.2.8.2.2. 文字変換マッピングの設定ファイルの適用手順

1. あらかじめ用意した設定ファイルを、iStorage NS 上のフォルダーに格納します。 ここでは、D:¥work¥table.txt とします。

2. Windows PowerShell を起動し、以下のコマンドを実行します。

   Set-NfsServerConfiguration -CharacterTranslationFile “D:¥work¥table.txt”

3. 設定を反映させるため、Server for NFS サービスを再起動します。

   nfsadmin server stop

   nfsadmin server start

4. 以下のコマンドを実行して、設定内容を確認します。

   Get-NfsServerConfiguration

   [確認する項目]

   CharacterTranslationFile : D:¥work¥table.txt

1.2.8.3 ファイル名の大文字と小文字を区別する

Windows の既定値では、A.txt と a.txt の混在はできません。
NFS 共有で大文字と小文字を区別するためには、下記の設定を行う必要があります。

1. 管理者メニューより [ローカルセキュリティポリシー] を起動します。

2. ツリーより [セキュリティの設定] → [ローカル ポリシー] → [セキュリティオプション] を選択します。

3. 右ペインより、 [システム オブジェクト：Windows システムではないサブシステムのための大文字と小文字の区別をしないことが必須] をダブルクリックし、[無効] を選択して [OK] をクリックします。

4. システムを再起動します。

【注意】
本設定を行うと、NFS 共有領域に対してはファイルサーバーリソースマネージャー(FSRM)の機能が正常に動作しない場合があります。

1.2.8.4 隠しファイルの属性について

UNIX 環境では、ピリオドで始まる名前のファイルは隠し属性となりますが、Windows では隠し属性とはなりません。ピリオドで始まる名前のファイルを隠し属性にするには、以下の設定を行います。

1. Windows PowerShell を起動し、以下のコマンドを実行します。

   Set-NfsServerConfiguration -HideFilesBeginningInDot $true

2. 設定を反映させるため、Server for NFS サービスを再起動します。

   nfsadmin server stop

   nfsadmin server start

3. 以下のコマンドを実行して、設定内容を確認します。

   Get-NfsServerConfiguration

> 【注意】
> NFS v4.1 を使用して NFS 共有をマウントした場合は、本設定を行っても、隠しファイル属性にはならず、通常の属性のファイルとして扱われます。

1.2.8.5 UNIX/Windows のタイムスタンプの差異について

UNIX のファイルシステムでは、以下の３つのタイムスタンプ(ファイル属性に含まれる日時)を管理しています。

A. 最終アクセス日時（atime）
B. 最終更新日時（mtime）
C. メタデータの最終変更日時（ctime）

次に、Windows のファイルシステムでは、以下の4つのタイムスタンプを管理しています。

a. 最終アクセス日時（LastAccessTime）
b. 最終更新日時（LastWriteTime）（データの更新日時）
c. メタデータの最終変更日時（ChangeTime）（ファイルの属性やファイル名の更新日時。ただし、内部で管理されており、プロパティ等では表示されません）
d. 作成日時（Creation Time）

UNIX と Windows のタイムスタンプは以下のように対応しています。

UNIX	Windows
A. 最終アクセス日時（atime）	a. 最終アクセス日時（LastAccessTime）
B. 最終更新日時（mtime）	b. 最終更新日時（LastWriteTime）
C. メタデータの最終変更日時（ctime）	c. メタデータの最終変更日時（ChangeTime）
対応項目なし	d. 作成日時（CreationTime）

Windows の "a. 最終アクセス日時" と "c. メタデータの最終変更日時" は、値が設定されていないと "b. 最終更新日時" を使用します。
そのため、Windows システムで作成されたファイルを UNIX システムにて参照した場合、 "A. 最終アクセス日時" や "C. メタデータの最終変更日時" は、お客様が認識している日時と異なる場合がありますが、これは仕様の動作となります。
なお、iStorage NS シリーズの出荷時設定では、最終アクセス日時を更新しない設定になっています。

1.2.8.6 ファイルの排他制御について

ファイルの排他制御には、NFS ではアドバイザリーが使用され、SMB ではマンダトリーが使用されます。このため、NFS 共有配下のファイルに、UNIX と Windows の双方から同時アクセスした場合には、ファイルの破壊などの問題が発生することがありますので、UNIX 側の排他制御を十分考慮した上で、同時アクセスを行ってください。

1.2.9 NFS 共有における注意事項

NFS 共有における注意事項を以下に説明します。

- NFS 共有で設定する共有名に DBCS（2 バイト）文字は使用できません。

- 複数の NFS クライアントから同一ファイルにアクセスする場合は、NFS クライアント側にて適切にロック制御を行わないと、ファイルが破損することがあります。

- NFS 共有では、ポート 111 番を使用します。他のアプリケーションがポート 111 番を使用している場合は、事前にアプリケーションが使用するポート番号を変更してください。

- AD LDS でユーザーマッピングを行っている環境において、Windows クライアントから作成されたファイルを NFS クライアントから参照した場合、グループ名には 4294967294 や -2 、 nobody 、nogroup 等が表示される仕様です。

- ファイル名の大文字と小文字を区別する設定を行うと、NFS 共有領域に対してはファイルサーバーリソースマネージャー(FSRM)の機能が正常に動作しない場合があります。

- ピリオドで始まる名前のファイルを隠しファイル属性にする機能を有効にしても、NFS v4.1 を使用して NFS 共有をマウントした場合は隠しファイル属性にはならず、通常の属性のファイルとして扱われます。

- 文字変換マッピングの設定を行っても、NFS v4.1 を使用して NFS 共有をマウントした場合は、変換機能は動作しないため、Windows のファイルシステムで許可されていない文字は UNIX クライアントではフォルダー/ファイル名には使用できません。

- UNIX の root ユーザーを Windows の管理者権限を持つユーザーにマッピングする際は、Windows のビルトイン Administrator は特別な位置づけのユーザーのため、管理者グループに所属する、ビルトイン Administrator 以外のユーザーをマッピングしてください。

- Windows と UNIX では使用する文字コード体系が異なる場合があり、相互にファイルを参照すると、フォルダー/ファイル名が文字化けすることがあります。このような場合、NFS 共有設定時のエンコードにて UNIX で使用している文字コードを指定してください。

- NFS v2, v3 を使用してクライアントからマウントする場合、エンコードとして UTF-8 は使用できません。UTF-8 を使用するには NFS v4.1 を使用してマウントしてください。

- Active Directory が存在するクラスターシステム環境においては、Active Directory を使用する方法でユーザーマッピングを行ってください。

- Windows OS 標準の NFS クライアント機能を使用して NFS 共有をマウントする場合は、下記の点に注意してください。
  - Windows OS 標準の NFS クライアント機能がサポートする NFS プロトコルのバージョンは v2 および v3 のみです。v4.1 はサポートしていません。
  - mount コマンドによるマウント実行時には、NFS 共有の設定時に指定したエンコードと同じエンコードを、-o lang= オプションにより指定してください。エンコードの指定を適切に行っていない場合、NFS 共有に日本語を含むファイル名のファイルが作成できない等の問題が発生する場合があります。
  - ファイル名の大文字と小文字を区別する設定にする場合は、NFS クライアント側の mount コマンドによるマウント実行時に -o casesensitive= オプションを指定するだけでなく、事前に iStorage NS 側の設定も必要です。iStorage NS 側の設定方法については、本書の【ファイル名の大文字と小文字を区別する】を参照してください。

1.3 FTP クライアントからアクセスする

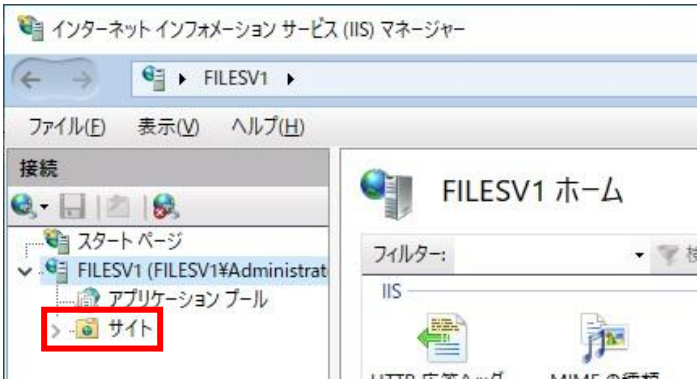
FTP（File Transfer Protocol）とは、ネットワーク上でファイルを送受信する際に使われるファイル転送プロトコルです。FTP を使用し、大容量のファイルを転送することができます。ここでは、iStorage NS 上の FTP サーバーを起動し、FTP クライアントからアクセスする手順を説明します。

1.3.1 FTP 共有を作成する

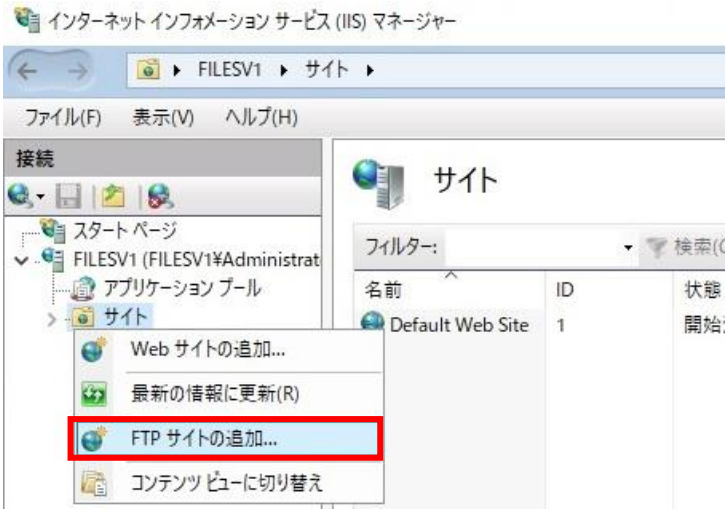
以下に、FTP 共有の作成手順について説明します。

1. 管理者メニューから[IIS マネージャー] を起動します。

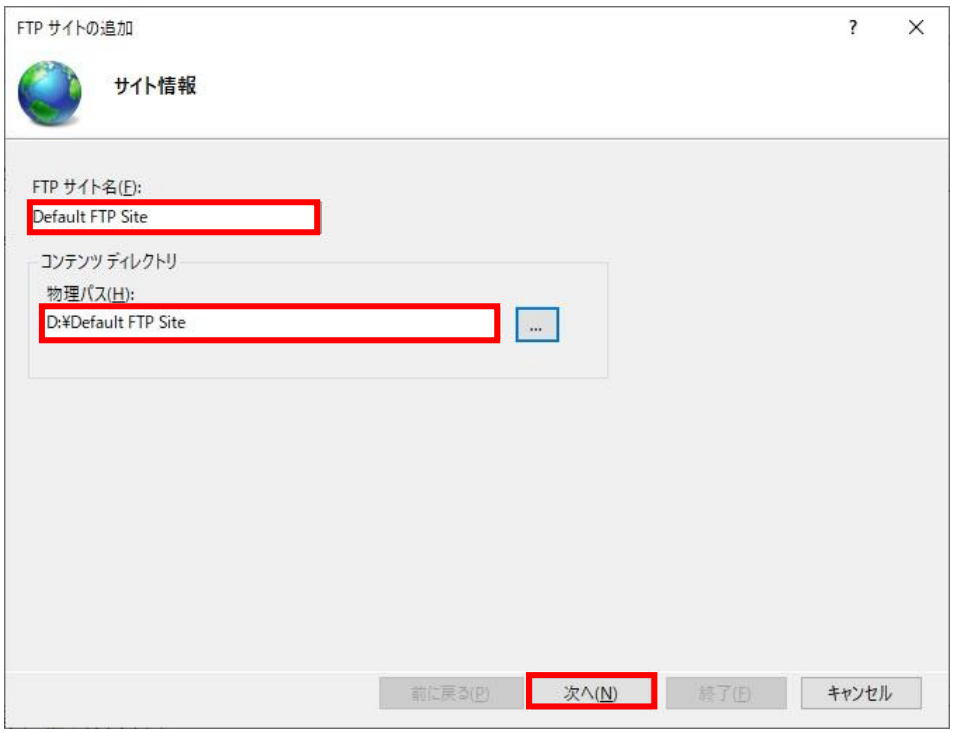
2. ツリーのコンピューター名のノードを展開し、[サイト] を表示します。



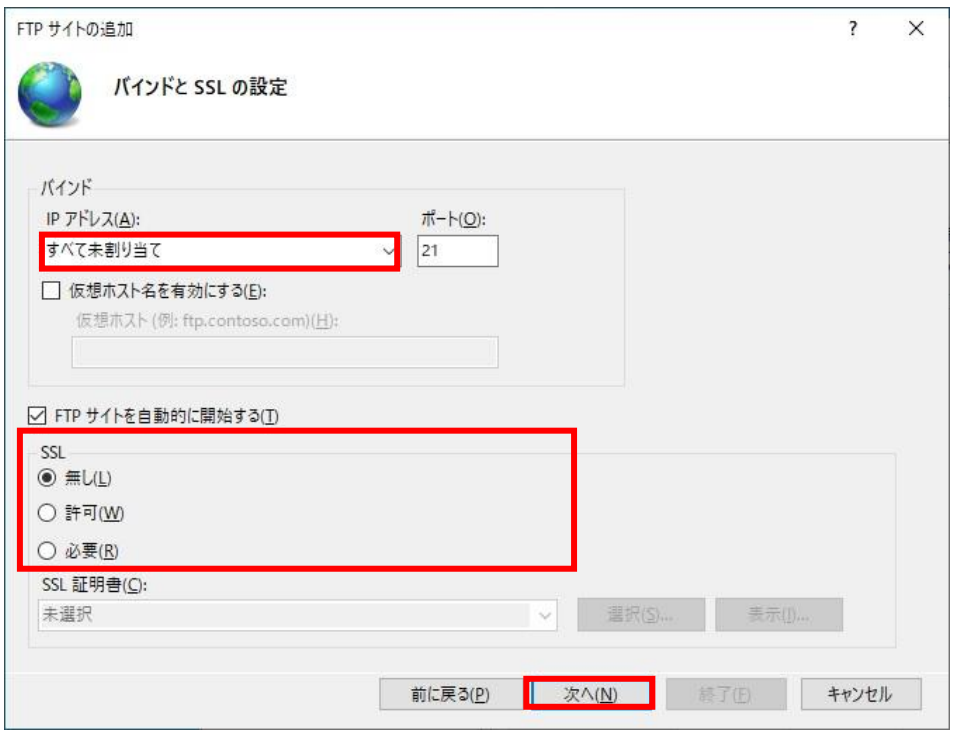
3. ツリーの [サイト] を右クリックし、[FTP サイトの追加] をクリックします。



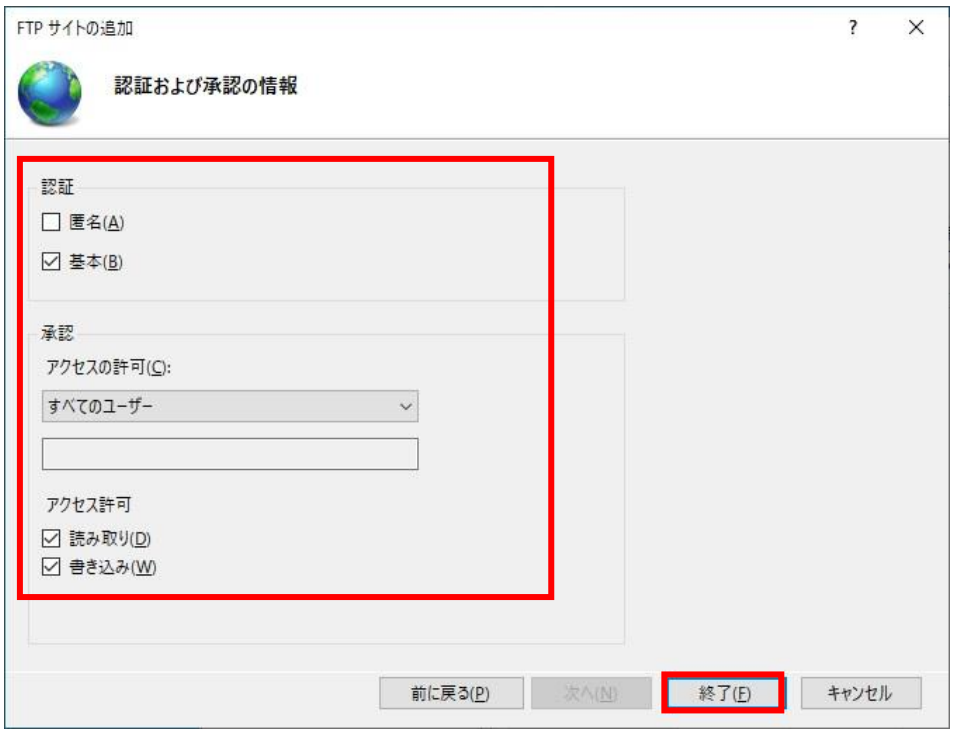
4. FTP サイト名と物理パスを指定し、[次へ] をクリックします。物理パスのフォルダーは自動作成されませんので、あらかじめ作成しておいてください。



5. [IP アドレス] で [すべて未割り当て] を選択し、SSL の項目を必要に応じて選択した後、 [次へ] ボタンをクリックします。



6. 認証および承認の情報を必要に応じて指定し、[終了] ボタンをクリックします。なお、[認証] で [基本] のみをチェックすると、本サーバーにアカウントがあるユーザーのみがアクセス可能となります。



1.3.2 FTP 共有の仮想ディレクトリを割り当てる

作成した FTP 共有配下に仮想ディレクトリを割り当てると、異なるドライブ/フォルダーなどに分散して存在する既存のフォルダーを仮想的に FTP 配下のフォルダーとして、指定したエイリアス名で見せることができます。なお、この時、既存のフォルダーに設定したファイルシステムレベルのアクセス権が FTP アクセスにも適用されます。

以下に、FTP 共有の仮想ディレクトリを割り当てる手順を説明します。

1. 管理者メニューから[IIS マネージャー] を起動します。

2. 作成した FTP 共有上で右クリックし、[仮想ディレクトリの追加] をクリックします。

3. [エイリアス] に仮想ディレクトリ名を入力し、エイリアスに割り当てる [物理パス] を指定して [OK] をクリックします。

4. 以下のように、作成した FTP 共有配下に仮想ディレクトリが割り当てられます。複数の仮想ディレクトリを割り当てたい場合、上記と同様の手順で割り当てることができます。

1.3.3 FTP のアクセス制御

ユーザーや複数のユーザーをまとめたグループに対して、各 FTP 共有へのアクセスを制御することで、セキュリティを保ったファイルアクセスの管理を行います。アクセス制御によって、必要なユーザーだけにファイルをアクセス可能にし、不必要なユーザーからのアクセスを禁止することで、不正な参照や書き換え、削除を防止します。

FTP 共有へのアクセス制御は、認証されたすべてのユーザーに対して、読み取りを許すか否か、書き込みを許すか否かのみです。これに加え、ファイルシステムレベルでのアクセス制御を併用することで、ユーザーおよびグループに対し、個々にアクセス権を設定することができます。その場合は、各フォルダーのプロパティで設定します。ファイルシステムレベルのアクセス権については【管理者ガイド（概要編）ファイルシステムレベルのアクセス許可】をご覧ください。

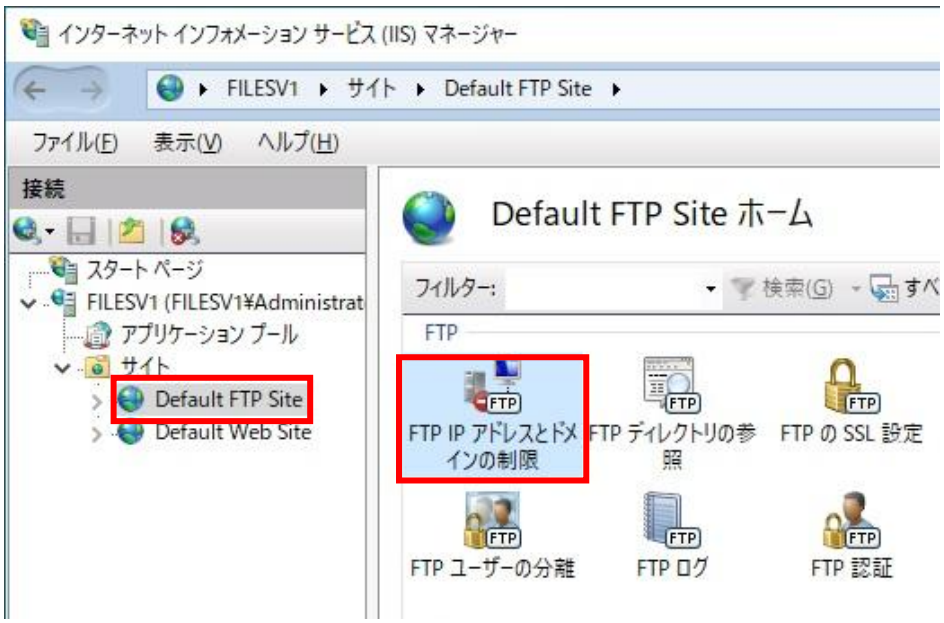
さらに、IP アドレスによるアクセス制限も可能です。デフォルトでは、すべての IP アドレスからのアクセスを許可していますが、すべての IP アドレスからのアクセスを拒否し、特定の IP アドレスや特定のネットワーク ID 内にあるコンピューターからのアクセスを許可する設定も可能です。

1.3.3.1 FTP 共有に IP アドレスのアクセス制限を設定する

ここでは、作成した FTP 共有に対し、特定の IP アドレスに限りアクセスを許可する設定を行う手順を説明します。

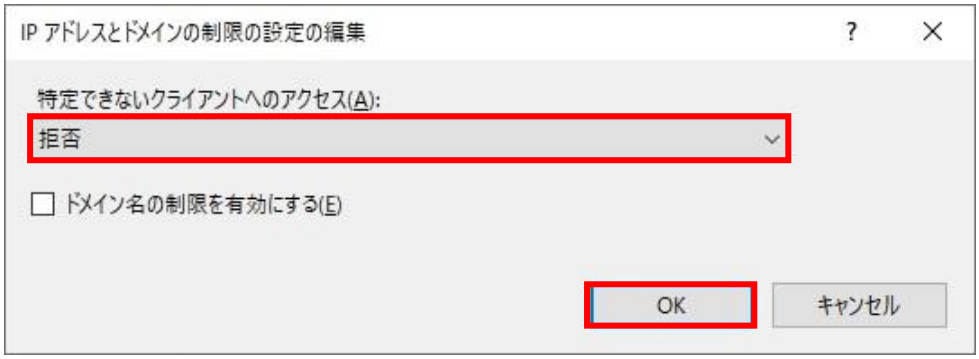
1. 管理者メニューの [IIS マネージャー] をクリックします。

2. 左ペインで作成した FTP 共有をクリックし、 [FTP IP アドレスとドメインの制限] をダブルクリックします。

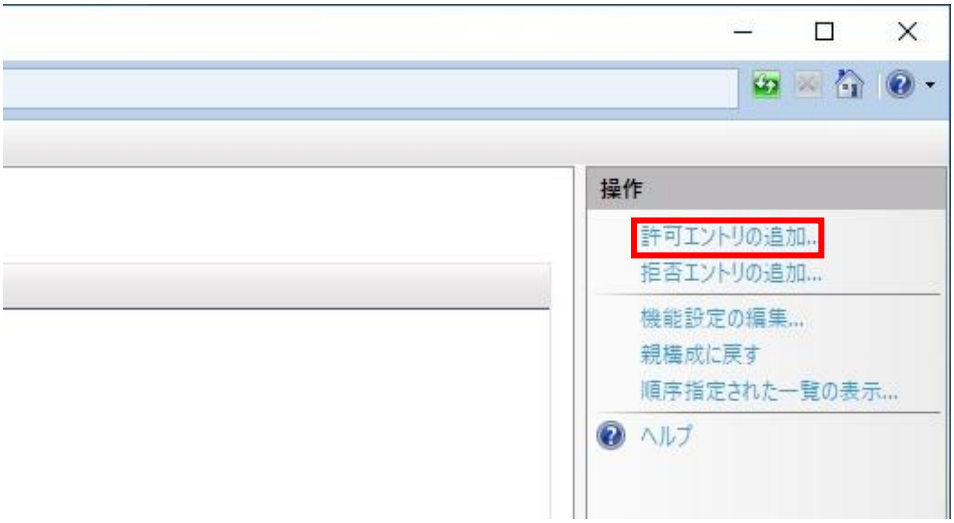


3. 右ペインで、[機能設定の編集] をクリックします。

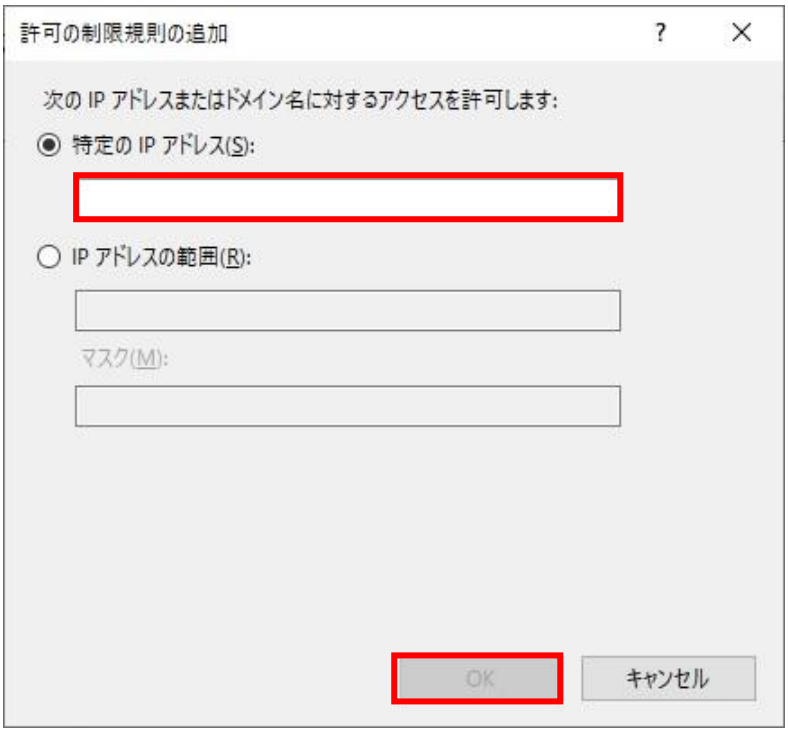
4. [特定できないクライアントへのアクセス] のプルダウンで、[拒否] を選択し [OK] をクリックします。



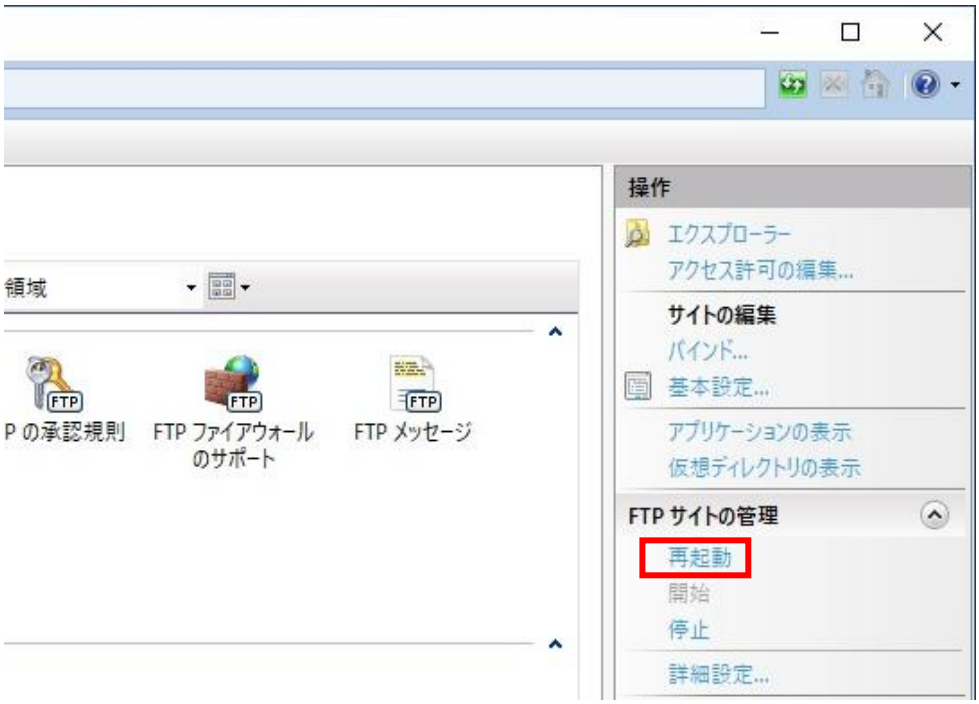
5. 右ペインで [許可エントリの追加] をクリックします。



6. [特定の IP アドレス] に許可したい IP アドレスを入力し、[OK] をクリックします。



7. 左ペインで作成した FTP 共有をクリックし、右ペインで [再起動] をクリックして、サイトを再起動します。



1.3.4 FTP 共有にアクセスする

iStorage NS 上に作成した FTP 共有に、クライアント PC から FTP プロトコルでアクセスする場合、クライアント PC の Web ブラウザに以下の URL を入力します。

ftp://<iStorage NS の IP アドレス または コンピューター名>/<仮想ディレクトリ名(エイリアス名)>

1.4 Web クライアントからアクセスする

HTTP（Web）共有では、WebDAV（Web-based Distributed Authoring and Versioning）というプロトコルを使用します。WebDAV を使用し、Web クライアントからネットワーク経由で HTTP（Web）共有にアクセスし、直接ファイルを編集したり、ファイルのアップロードやダウンロードをすることができます。ここでは、HTTP（Web）共有を公開する Web サイトを作成した後、HTTP（Web）共有を作成し、クライアント PC からアクセスする手順を説明します。

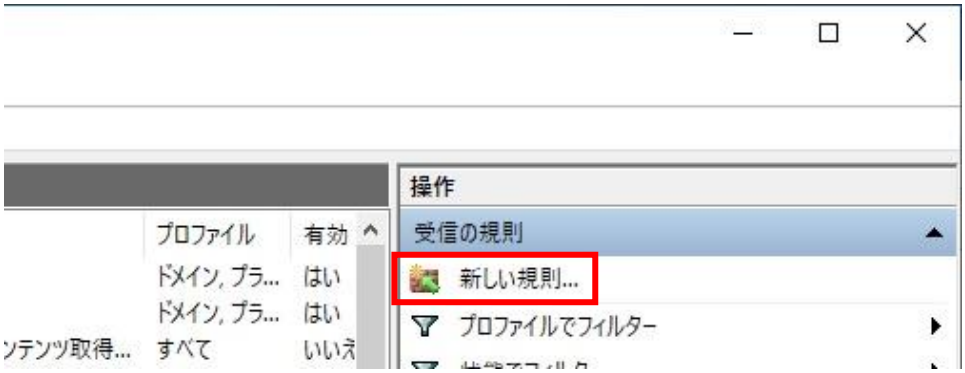
1.4.1 任意のポートを開放する

iStorage NS 上のファイアウォールを有効にしている場合、新規 Web サイトで指定するポートを開放し、接続を許可する必要があります。以下に、Windows 標準のファイアウォール設定手順を説明します。

1. 管理者メニューから [セキュリティが強化された Windows Defender ファイアウォール] を起動します。

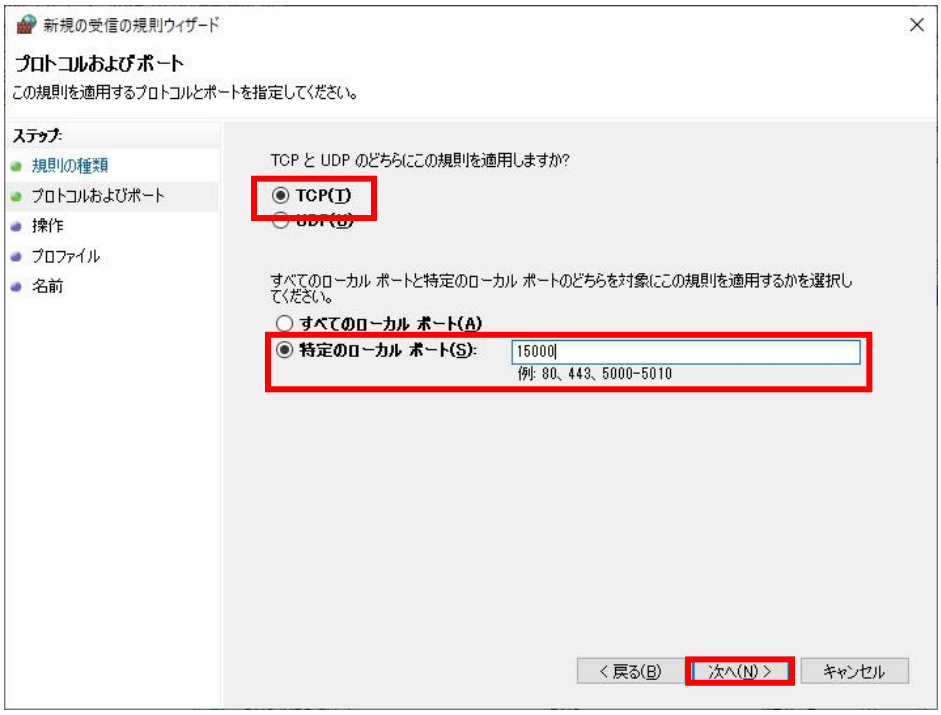
2. 左ペインの [受信の規則] をクリックします。

3. 右ペインの [新しい規則] をクリックします。



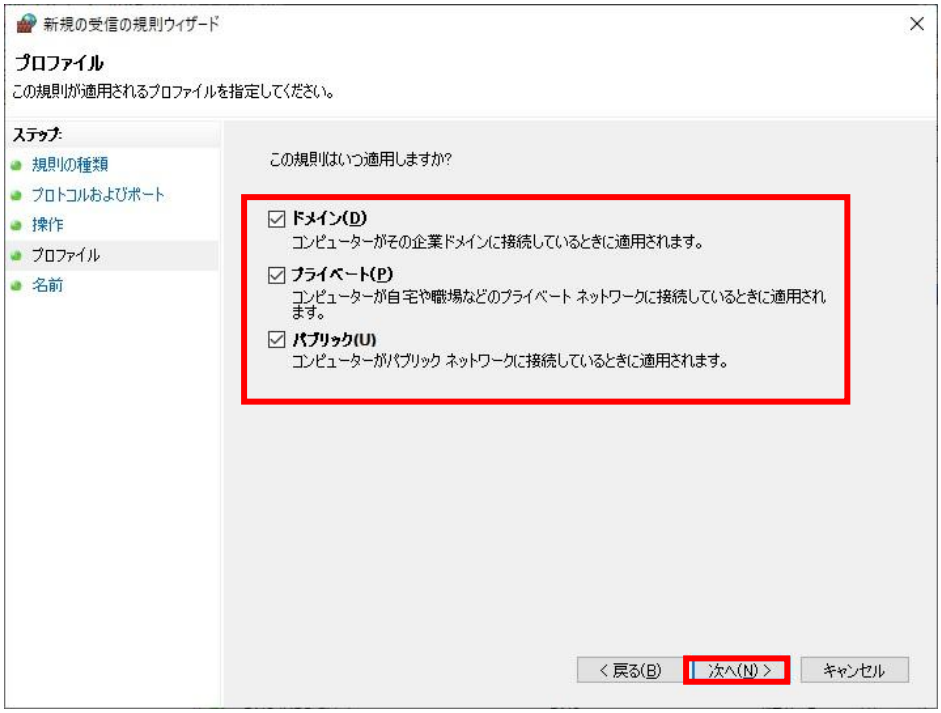
4. [新規の受信の規則ウィザード] が起動します。[ポート] を選択し、[次へ] をクリックします。

5. [TCP] を選択し、[特定のローカル ポート] に HTTP （Web）共有で使用するポート番号を入力して、[次へ] をクリックします。



6. [接続を許可する] を選択し、[次へ] をクリックします。

7. この規則が適用されるプロファイルを必要に応じて選択し、[次へ] をクリックします。



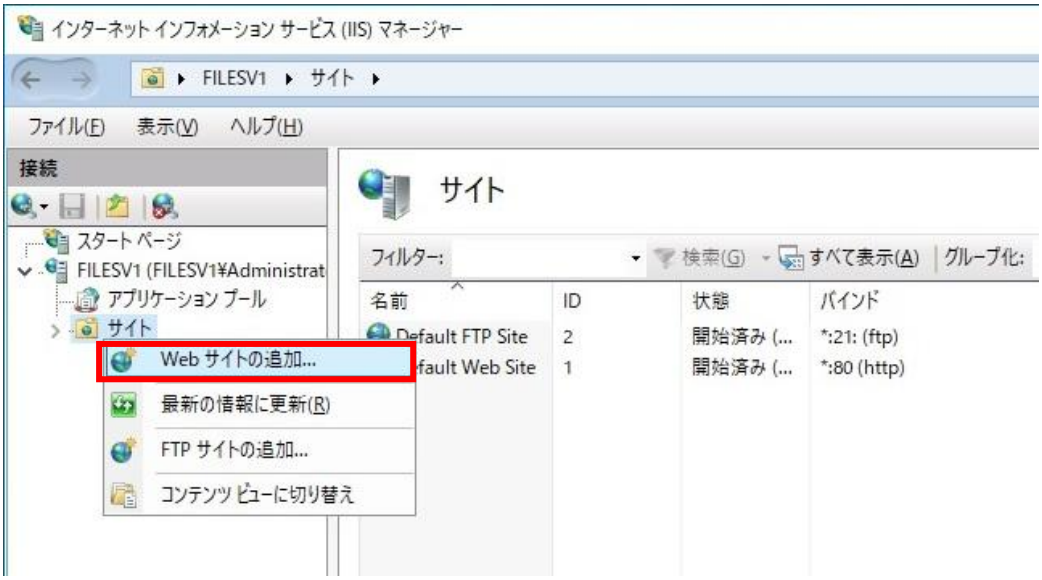
8. [名前] と [説明] （省略可能）を入力した後、[完了] をクリックします。

1.4.2 HTTP（Web）共有を作成し、WebDAV の認証方法を設定する

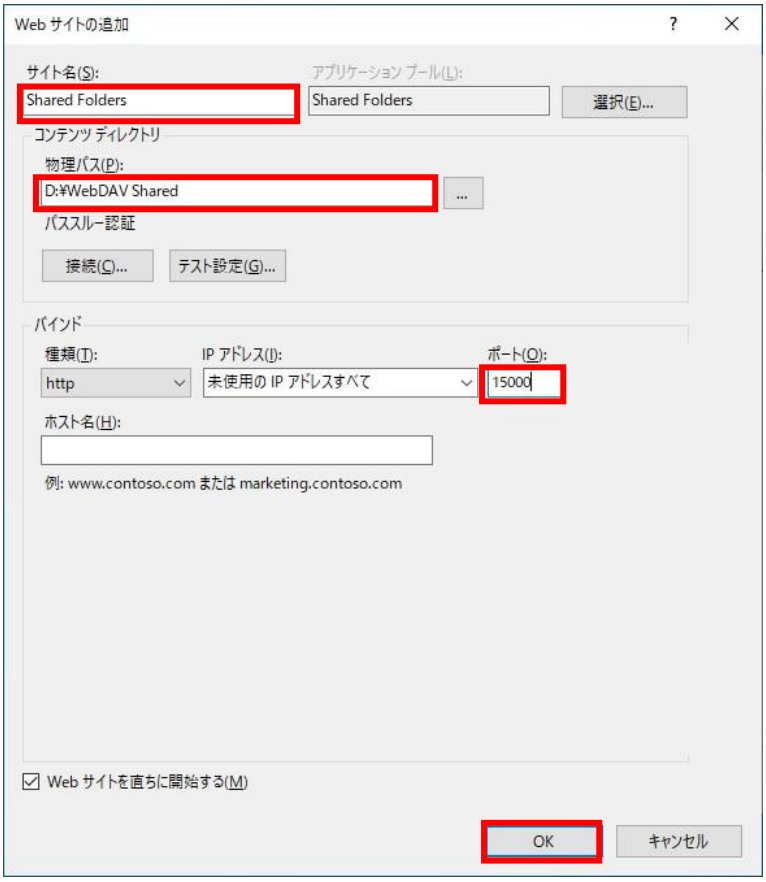
1. 管理者メニューから [IIS マネージャー] を起動します。

2. ツリーのコンピューター名のノードを展開し、[サイト] を表示します。

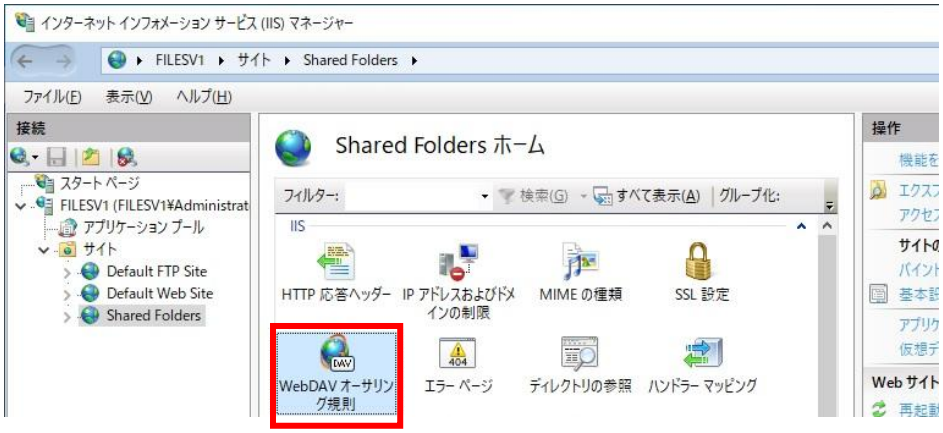
3. ツリーの [サイト] を右クリックして [Web サイトの追加] をクリックします。



4. 必要項目を設定し、[OK] ボタンをクリックします。なお、[ポート] には、本書の【任意のポートを開放する】 で指定したポート番号を入力してください。また、物理パスのフォルダーは自動作成されませんので、あらかじめ作成しておいてください。



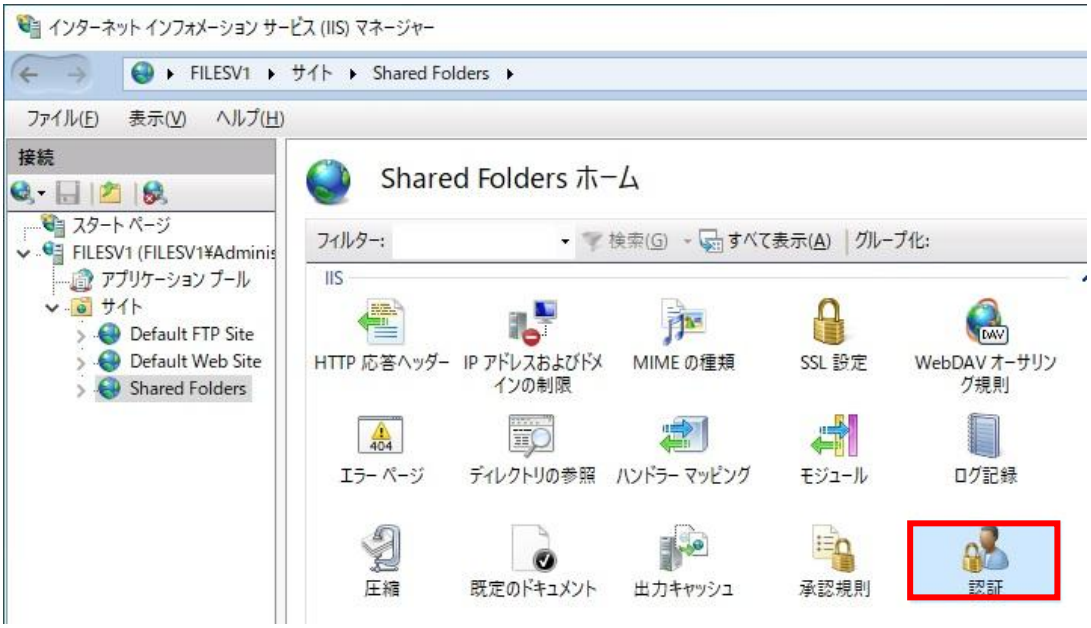
5. 作成した HTTP (Web) 共有をクリックし、中央ペインの [WebDAV オーサリング規則] をダブルクリックします。



6. [操作] 画面の [WebDAV の有効化] をクリックします。

7. [操作] 画面の [オーサリング規則の追加] をクリックし、必要に応じて設定後、[OK] ボタンをクリックします。

8. ツリーにて、作成した HTTP (Web) 共有を選択し、[認証] をダブルクリックします。



9. 必要に応じて認証方法を設定します。

【注意】

"匿名認証" が有効になっていると、ユーザー名とパスワードを求められることなく、ユーザーが WebDAV 共有にアクセス可能となります。セキュリティ上の観点から、"匿名認証" は無効に設定することをお勧めします。

1.4.3 HTTP（Web）共有の仮想ディレクトリを割り当てる

作成した HTTP（Web）共有配下に仮想ディレクトリを割り当てると、異なるドライブ/フォルダーなどに分散して存在する既存のフォルダーを仮想的に HTTP（Web）共有配下のフォルダーとして見せることができます。

仮想ディレクトリの割り当ては、IIS マネージャーを起動し、作成した HTTP（Web）共有上で右クリックして表示される [仮想ディレクトリを追加する] から行うことができます。HTTP（Web） 共有の仮想ディレクトリの割り当て手順は、FTP 共有の仮想ディレクトリの割り当て手順と同様ですので、詳細は本書の【FTP 共有の仮想ディレクトリを割り当てる】をご覧ください。

1.4.4 HTTP（Web）共有のアクセス制御

ユーザーや複数のユーザーをまとめたグループに対して、各 HTTP（Web）共有へのアクセスを制御することで、セキュリティを保ったファイルアクセスの管理を行います。アクセス制御によって、必要なユーザーだけにファイルをアクセス可能にし、不必要なユーザーからのアクセスを禁止することで、不正な参照や書き換え、削除を防止します。

HTTP（Web）共有のアクセス制御では、WebDAV 認証設定により、個々のユーザーまたはグループに対して読み取り、書き込みの許可を設定することができます。また、ファイルシステムレベルでのアクセス制御も可能です。その場合は、各フォルダーのプロパティで設定します。

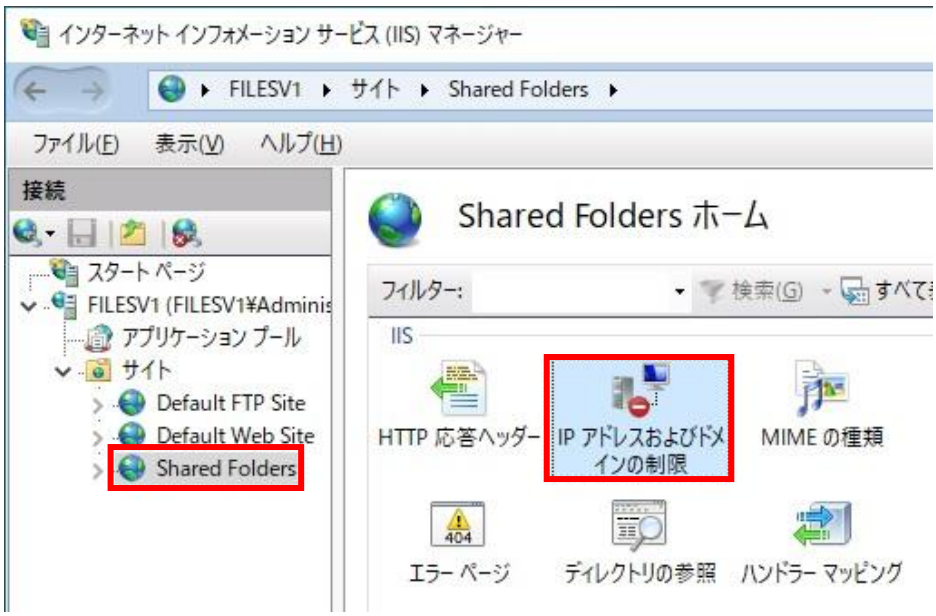
さらに、IP アドレスによるアクセス制限も可能です。デフォルトでは、すべての IP アドレスからのアクセスを許可していますが、すべての IP アドレスからのアクセスを拒否し、特定の IP アドレスや特定のネットワーク ID 内にあるコンピューターからのアクセスを許可する設定も可能です。

1.4.4.1 HTTP（Web）共有に IP アドレスのアクセス制限を設定する

ここでは、特定の IP アドレスからのアクセスを拒否する設定方法を説明します。

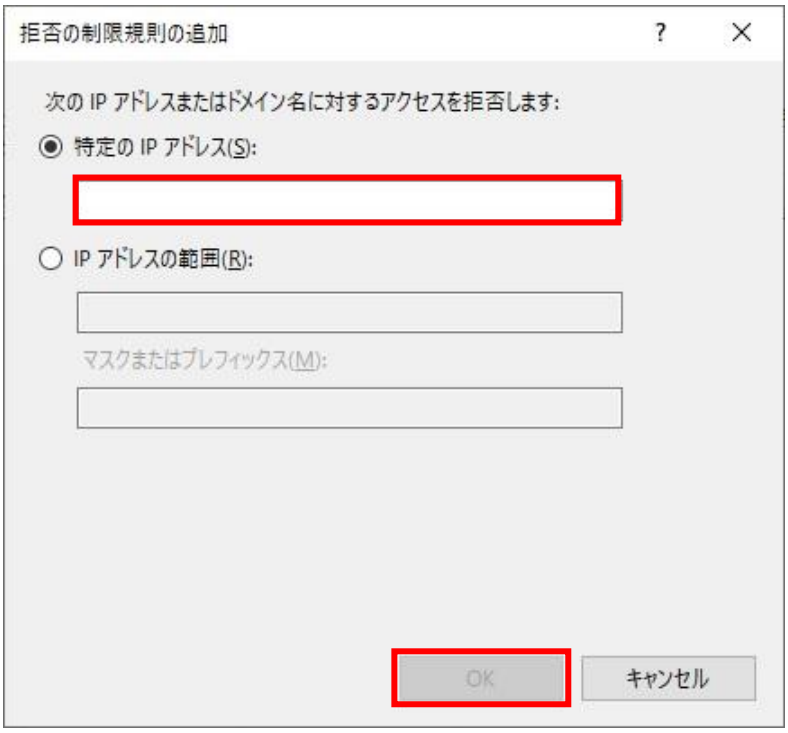
1. 管理者メニューから [IIS マネージャー] を起動します。

2. 左ペインにて、作成した HTTP（Web）共有をクリックし、 [IP アドレスおよびドメインの制限] をダブルクリックします。

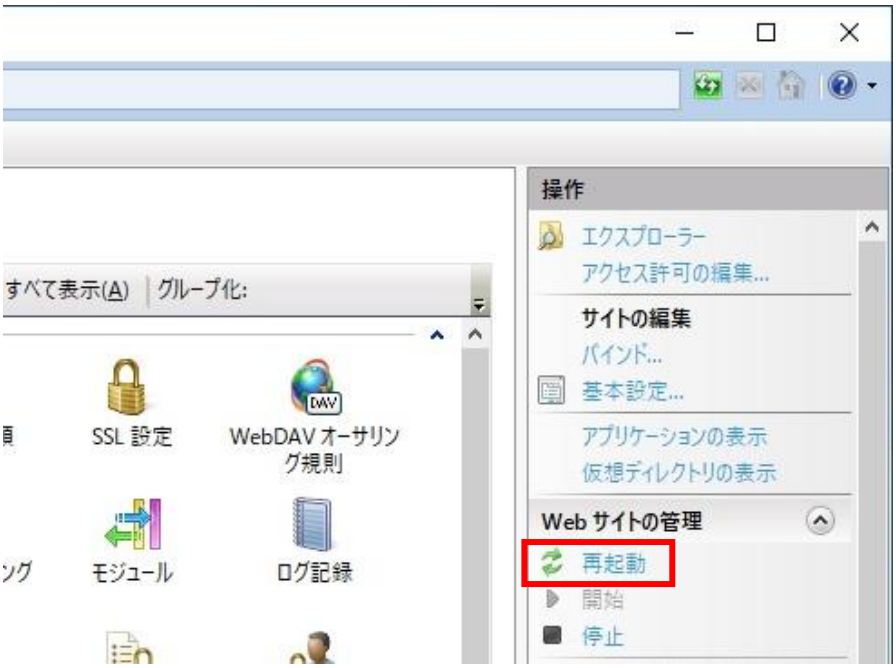


3. 右ペインで、[拒否エントリの追加] をクリックします。

4. [特定の IP アドレス] に拒否したい IP アドレスを入力し、[OK] をクリックします。



5. 左ペインにて、作成した HTTP（Web）共有をクリックし、右ペインで [再起動] をクリックして、サイトを再起動します。

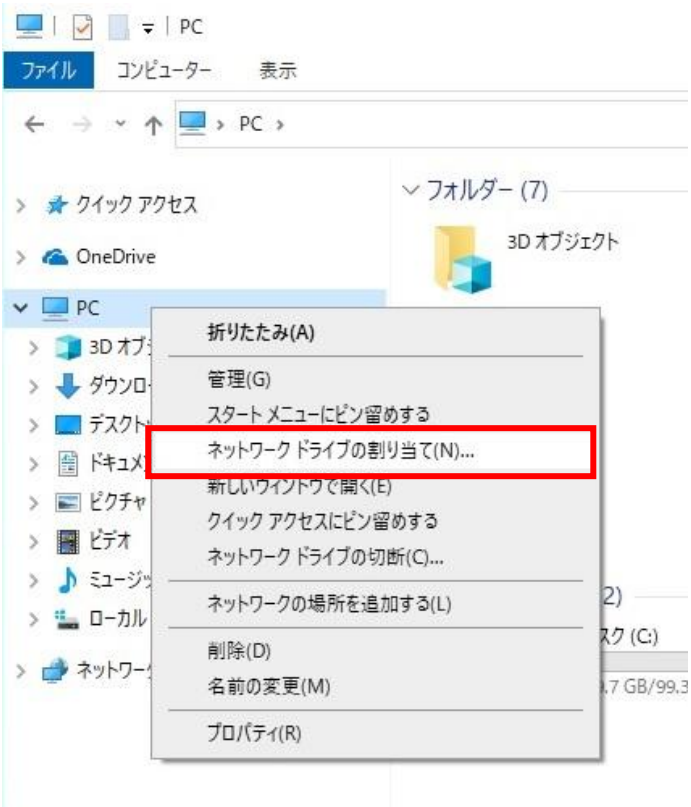


1.4.5 HTTP（Web）共有にアクセスする

iStorage NS 上の HTTP（Web）共有へアクセスするには、WebDAV に対応したクライアントソフトウェアを使用します。アクセスの方法については、各ソフトウェアの使用方法に従ってください。

ここでは、Windows クライアントにてネットワークドライブを追加し、HTTP（Web）共有フォルダーにアクセスする手順について説明します。なお、Windows クライアントの OS バージョンによっては画面表示が異なる場合があります。

1. クライアント PC の [エクスプローラー] にて[PC] を右クリックし、[ネットワークドライブの割り当て] をクリックします。



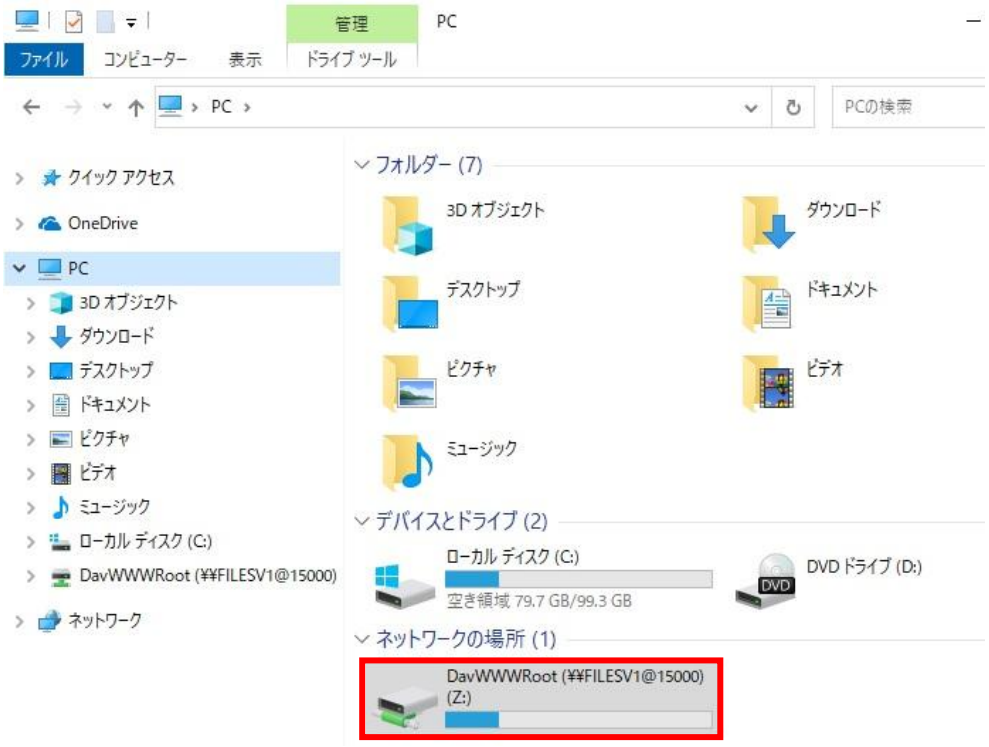
2. [ドライブ] を指定し、[フォルダー] 欄に以下のいずれかの書式を入力します。なお、ポート番号はサイト作成時に指定した値を入力します。

・¥¥iStorage NS の IP アドレス または コンピューター名@ポート番号¥DavWWWRoot
・http://iStorage NS の IP アドレス または コンピューター名:ポート番号

3. [完了] をクリックします。

4. HTTP（Web）共有へアクセス可能なユーザー名とパスワードを入力し、[OK] をクリックします。

5. [PC] の [ネットワークの場所] 配下に、HTTP（Web）共有フォルダーが追加されます。こちらをダブルクリックし、HTTP（Web）共有フォルダーにアクセスすることができます。



2 iStorage NS の共有領域を管理する

- シャドウコピー
- ファイルサーバーリソースマネージャー
- ディスククォータ
- 複数サーバーの共有フォルダーを統合する（**DFS**）

2.1 シャドウコピー

ユーザーがローカルのコンピューター上のファイルを削除した場合、削除したファイルはゴミ箱に保存されるため、ゴミ箱を空にしない限り、削除したファイルを後から元に戻すことができます。一方、ネットワーク経由でサーバー上のファイルを削除した場合、削除したファイルはゴミ箱に残らないため、ファイルを元の状態に戻すことができません。しかし、シャドウコピーサービスを使用すると、サーバー上に保存しているファイルを削除した場合、これらをある時点の状態まで戻すことが可能となります。

シャドウコピーサービスは、ある時点でのボリュームの状態を保存しておく機能です。シャドウコピーサービスを有効にしておくと、管理者の手を煩わせることなく、ユーザーがサーバー上のファイルをシャドウコピー取得時点の状態に戻すことができます。

シャドウコピーサービスはスケジューリング機能を持っており、自動的にシャドウコピーを作成することができます。なお、スケジュールで設定するシャドウコピーの作成時刻は、ご使用の環境やファイルの利用方法などに基づいて、負荷の低い時間帯に設定することを推奨します。

2.1.1 シャドウコピーの動作

シャドウコピーサービスは、サーバー上の特定のファイルに対してシャドウコピーを作成するのではなく、ボリューム全体のシャドウコピーを作成します。

シャドウコピーは、最後に作成されたシャドウコピーから変更があったブロックレベルのコピーを作成します。

シャドウコピーのデータはシャドウコピー記憶域に格納されます。シャドウコピー記憶域の最大サイズは、既定ではコピー対象であるボリュームの 10%に設定されています。シャドウコピー記憶域の使用量が最大サイズに達した場合や、シャドウコピー記憶域を設定しているボリュームに空きがなく、シャドウコピー記憶域を拡張できない場合は、最も古いシャドウコピーが削除されます。この動作はシャドウコピー記憶域に十分な空き容量が確保できるまで繰り返されるため、結果としてすべての世代が削除される場合があります。また、1 つのボリュームで作成されるシャドウコピーの世代数は、デフォルトでは最大 64 個ですので、シャドウコピー記憶域が最大値に達していなくても、65 個目のシャドウコピーが作成された場合、最も古いシャドウコピーが削除されます。

ファイルに設定されたアクセス許可も保持しますので、ファイルを復元した場合、以前と同じアクセス許可が割り当てられます。しかし、削除したファイルを別の権限を持ったフォルダーに復元する場合は、そのファイルには復元先フォルダーの既定のアクセス許可が設定されます。

【注意】

- シャドウコピーのデータは一時的なものと認識してください。シャドウコピーがシャドウコピー記憶域に入りきらない場合、もしくは、シャドウコピーの数が既定では 65 個に達した場合など、意図せずシャドウコピーが削除されることがあります。そのため、シャドウコピーはバックアップの代用とはなりませんので、通常のバックアップ作業は必要です。大切なデータについては、必ずバックアップソフトウェアを使ってバックアップするようにお願いします。
- シャドウコピーは読み取り専用です。編集はできません。

2.1.2 シャドウコピーの運用計画

シャドウコピーの設定を行う際、以下を決定する必要がありますので、運用環境やファイルの利用状況などから事前に検討してください。

- シャドウコピーを有効にするボリューム
- シャドウコピーを保存するボリューム
- シャドウコピーのために確保するディスク領域
- シャドウコピーが使用するメモリ領域
- シャドウコピー作成のスケジュール

2.1.2.1 シャドウコピーを有効にするボリューム

シャドウコピーを有効にするボリュームについて、以下の点を考慮してください。

- シャドウコピーは、データボリュームに対して有効にしてください。システム領域を含むボリューム、仮想メモリのページングファイルや休止ファイルを含むボリュームでは、シャドウコピーを有効にしないでください。
- Windows Server バックアップのバックアップ先ボリュームは、シャドウコピーを有効にしないでください。
- シャドウコピーは NTFS ボリュームのみに対応しています。FAT ボリュームでは動作しません。
- シャドウコピーを有効にするボリュームで最適化 (デフラグ) を実行する予定がある場合、フォーマット時にクラスターサイズ (アロケーション ユニットサイズ) を 16KB 以上に設定してください。なお、クラスターサイズを 16KB 以上に設定すると、NTFS 圧縮機能(＊)は使用できません。
- ＊: NTFS 圧縮機能を使用する場合は、クラスターサイズを 4KB 以下に設定する必要があります。
- シャドウコピーを有効にするボリュームの最大サイズは 64TB です。

2.1.2.2 シャドウコピーを保存するボリューム

シャドウコピーを保存するボリューム（シャドウコピー記憶域を格納するボリューム）について、以下の点を考慮してください。

- シャドウコピーを保存するボリュームは、既定ではソースボリューム (コピー対象のユーザーデータが保存されているボリューム) と同じボリュームです。同じサーバー上の別のボリュームに変更することもできます。
- I/O 負荷が高いシステムにおいては、取得済みのシャドウコピーがすべて削除される現象が発生し易くなります。I/O 負荷を緩和するために、シャドウコピーの保存先ボリュームとして、他の用途で使用しないシャドウコピー記憶域専用ボリュームを設定することを推奨します。また、物理的に異なるディスクが存在する場合は、そのディスク上のボリュームに設定すると、より効果があります。
- ソースボリュームで BitLocker が有効となっている場合、シャドウコピーを保存するボリュームはソースボリュームから変更できません。
- シャドウコピー記憶域があるボリュームに断片化が多いシステムにおいては、取得済みのシャドウコピーがすべて削除される現象が発生し易くなります。断片化発生を緩和するために、シャドウコピー記憶域を格納するボリュームのフォーマット時に、クラスターサイズ (アロケーションユニットサイズ) を 16KB 以上のできるだけ大きいサイズとすることを推奨します。
- Windows Server フェイルオーバー クラスタリングの共有ディスク上のボリュームでシャドウコピーを有効化する場合、シャドウコピーを保存するボリュームとして、同一の共有ディスク上の別ボリュームを選択できません。
- シャドウコピーを保存するボリュームの最大サイズは 64TB です。

2.1.2.3 シャドウコピーのためのディスク領域

シャドウコピーを格納する領域サイズは、既定ではコピー対象であるボリュームの 10%に設定されています。シャドウコピーの量が増え、この領域の使用率が 100% に達した場合は、新しいシャドウコピーを格納するための空き領域を確保するため、シャドウコピーの古い世代から順次自動で削除されます。したがって、ファイルに対して更新される頻度（更新量）が多い場合や保持したい世代数を多く取りたい場合は、あらかじめその領域を増やす必要があります。

【補足】

シャドウコピーを格納する領域の現在のサイズは、以下の方法で確認することができます。

1. 管理者権限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以下のコマンドを実行します。

   vssadmin list shadowstorage
3. 以下のようなコマンド実行結果が表示されますので、「シャドウ コピーの記憶域の割り当て領域」の項目を参照してください。

2.1.2.4 シャドウコピーが使用するメモリ領域

シャドウコピーでは、ボリュームサイズやファイル数に比例して、NonPagedPool、PagedPool と呼ばれるメモリ領域を使用します。それぞれのサイズは、以下での計算式で概算できます。

- シャドウコピーが使用する NonPagedPool サイズ
  シャドウコピーでは、スナップショットを作成する際、シャドウコピーを有効にするボリューム容量 1TB あたり NonPagedPool を 40MB 消費します。このため、NonPagedPool のサイズを算出する式は以下となります。

  ＜NonPagedPool サイズ＞ ＝ ＜ボリューム容量（TB）＞ × 40MB

- シャドウコピーが使用する PagedPool サイズ
  スナップショットを参照する場合、そのスナップショットに格納されているファイル数に応じて、PagedPool を消費（100 万ファイルあたり、最大 2MB）します。スナップショットから復元を行う場合は、現在から復元を行う世代までのすべてのスナップショットが参照されるため、PagedPool のサイズを算出する式は以下となります。

  ＜PagedPool サイズ＞ ＝ (＜ファイル数＞／100 万) × 2MB ×＜スナップショット世代数＞

2.1.2.5 シャドウコピー作成のスケジュール

シャドウコピーはスケジューリング機能を持っているため、定期的にシャドウコピーを作成することができます。お客様の運用に合わせてスケジュールを設定してください。

シャドウコピーを頻繁に作成すると、ユーザーが必要とする世代のシャドウコピーを復元できる可能性が高くなります。しかし、1 つのボリュームに作成できるシャドウコピーの数は既定では最大 64 個ですので、シャドウコピー作成の間隔を短くすると早い段階でシャドウコピーが削除されてしまう可能性があります。また、作成されるシャドウコピー数が多いほどシャドウコピーによる消費ディスク領域も増えますので、その旨もご考慮の上、スケジュール設定を行ってください。

【注意】

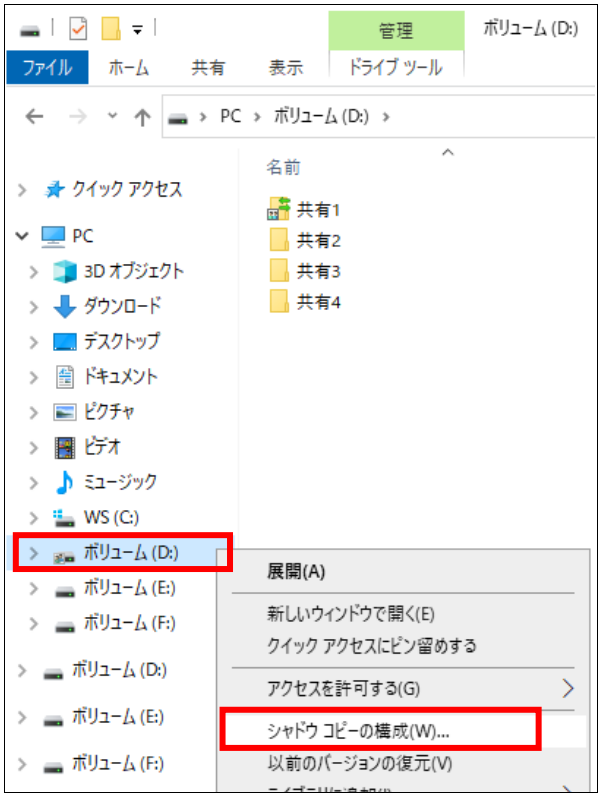
- シャドウコピーを作成する頻度の上限は、同一システム内で 1 時間につき 1 回までとしてください。
- 複数ボリュームでシャドウコピーを有効にする場合、デフォルトのスケジュール時刻（平日の 7 時と 12 時）のままでは、スケジュール時刻が重複していますので、各ボリュームのスケジュール時刻が、1 時間以上空くように設定を変更してください。
- シャドウコピーを有効にしているシステムにおいて、シャドウコピーを利用するバックアップソフトウェア製品やファイルサーバーリソースマネージャー （FSRM） 機能を使用すると、意図しないタイミング（スケジュールされたシャドウコピー処理の延長）で動作する後処理により、I/O 負荷が高くなる事象が発生します。このため、シャドウコピーのスケジュール時刻は、バックアップ処理や FSRM の記憶域レポート作成のスケジュール時刻と重ならないようにしてください。また、スケジュールされたシャドウコピー処理とその後動作する後処理により I/O 負荷が高くなっても業務に支障がない時間帯にシャドウコピーのスケジュール時刻を調整してください。

2.1.3 シャドウコピーの設定手順

シャドウコピーの設定は、以下の手順で行います。

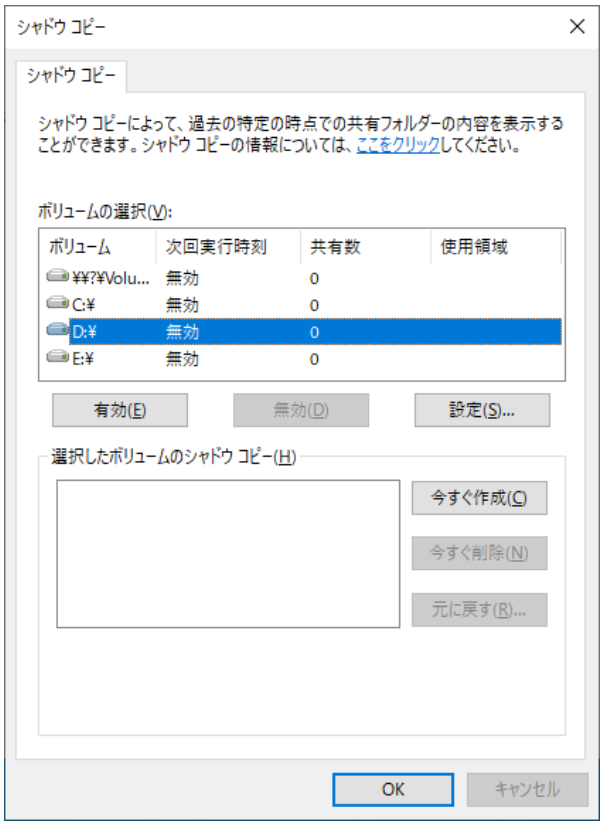
1. 管理者メニューより [エクスプローラー] を起動します。

2. エクスプローラーにて、対象のボリューム名を選択し、 右クリックメニューから [シャドウコピーの構成] をクリックします。



【注意】
シャドウコピーはデータボリュームを対象とした機能です。したがって、システム領域を含むボリューム、および、仮想メモリのページング ファイルや休止ファイルを含むボリュームを選択しないでください。

3. 下記のダイアログに従い、シャドウコピーの詳細設定を行います。



[ボリュームの選択] 欄には、下記の情報が表示されます。対象のボリュームを選択し、各操作ボタンをクリックしてください。

- **［ボリューム］**

  シャドウコピーサービスを利用できるサーバー上のボリュームがすべて表示されます。シャドウコピーは、NTFS ファイルシステムのデータボリュームのみで使用できます。シャドウコピーを管理するには、ここで対象のボリュームを選択して、実行するタスクを選択します。 C ドライブや System Reserved ボリュームを選択しないようにしてください。

- **[次回実行時刻]**

  シャドウコピーサービスが有効な場合、次にシャドウコピーを作成する日時が表示されます。

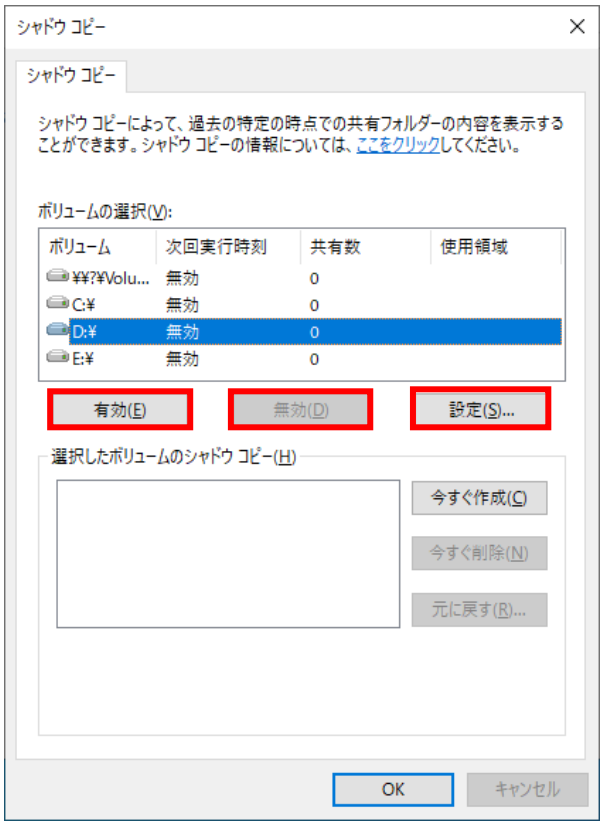
- **[共有数]**

  ボリューム上に存在する共有フォルダーの数が表示されます。

- **[使用領域]**

  シャドウコピーが現在使用しているディスク容量がボリュームごとに表示されます。

ボリュームを選択後、下記のボタンをクリックして操作を行えます。



- **[有効] ボタン**

  選択したボリュームのシャドウコピーを作成し、スケジュールを有効にします。

  以下の既定の設定で実行されます。

  - シャドウコピーの記憶域の最大値が、 ボリュームサイズの 10%に設定されます。
  - 選択したボリュームのシャドウコピーが 1 つ作成され、それに応じて使用領域が計算されます。
  - 月曜から金曜までの午前 7 時と 12 時にシャドウコピーを作成するスケジュールが新規作成されます。

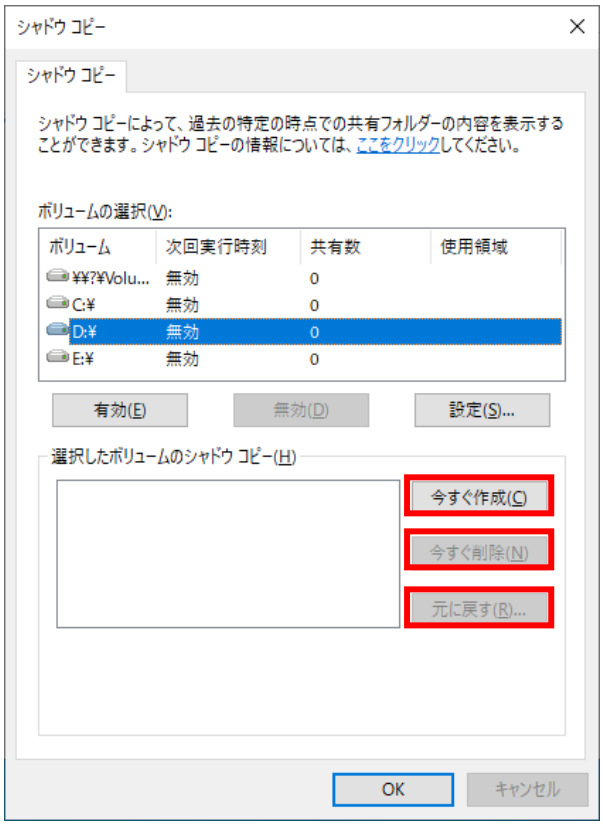
- **[無効] ボタン**

  選択したボリュームのスケジュールを無効にします。この時点で保存していたシャドウコピーはすべて削除されます。

- **[設定] ボタン**

  選択したボリュームのスケジュールやシャドウコピーのための記憶域容量の設定を行います。

画面の下半分では以下の操作が行えます。



- **[選択したボリュームのシャドウコピー]**

  保存されているシャドウコピー(作成された日時) の一覧が表示されます。

- **[今すぐ作成] ボタン**

  選択したボリュームのシャドウコピーを手動で作成します。

- **[今すぐ削除] ボタン**

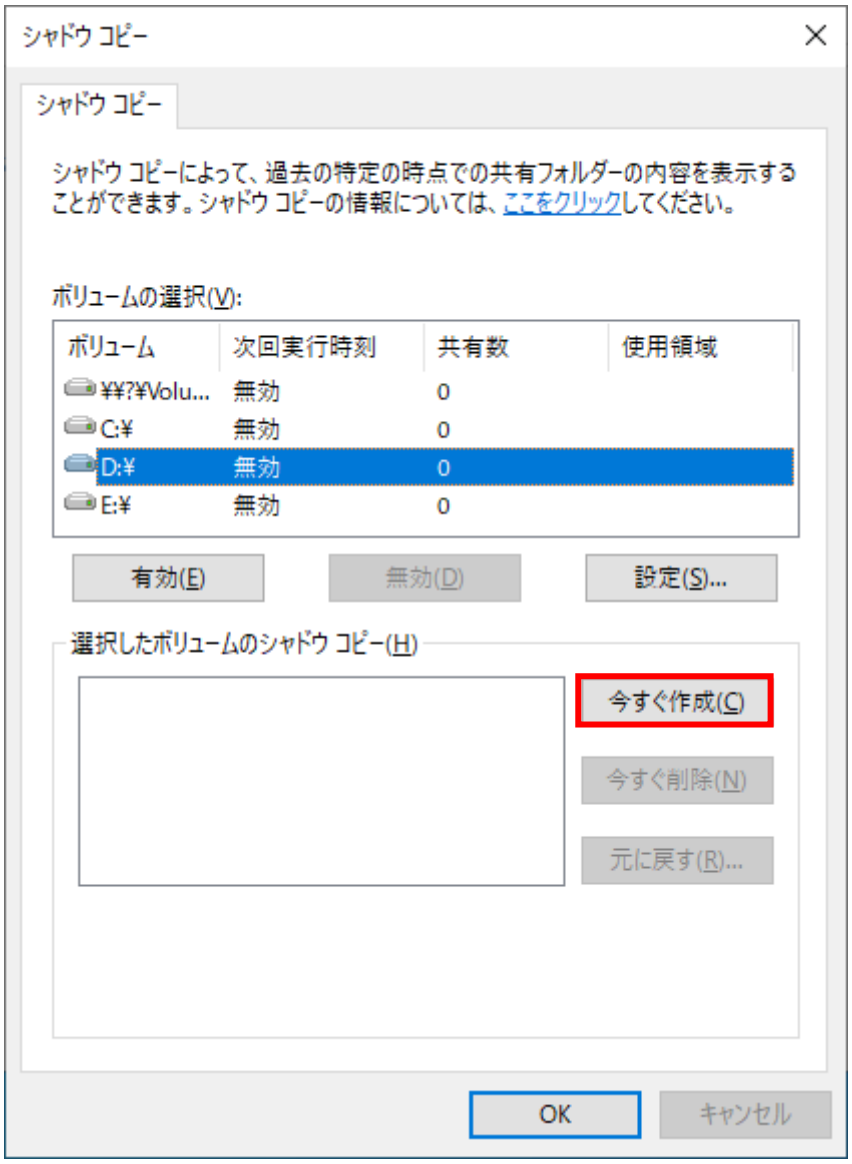
  シャドウコピーの削除を行います。保存されているシャドウコピーの一覧から削除したいシャドウコピーを選択し、[今すぐ削除] ボタンをクリックしてください。

- **[元に戻す] ボタン**

  シャドウコピーからボリュームの復元を行います。保存されているシャドウコピーの一覧から元に戻したいシャドウコピーを選択し、[元に戻す] ボタンをクリックしてください。指定したボリューム全体を元の状態に戻します。

2.1.3.1 シャドウコピーの作成

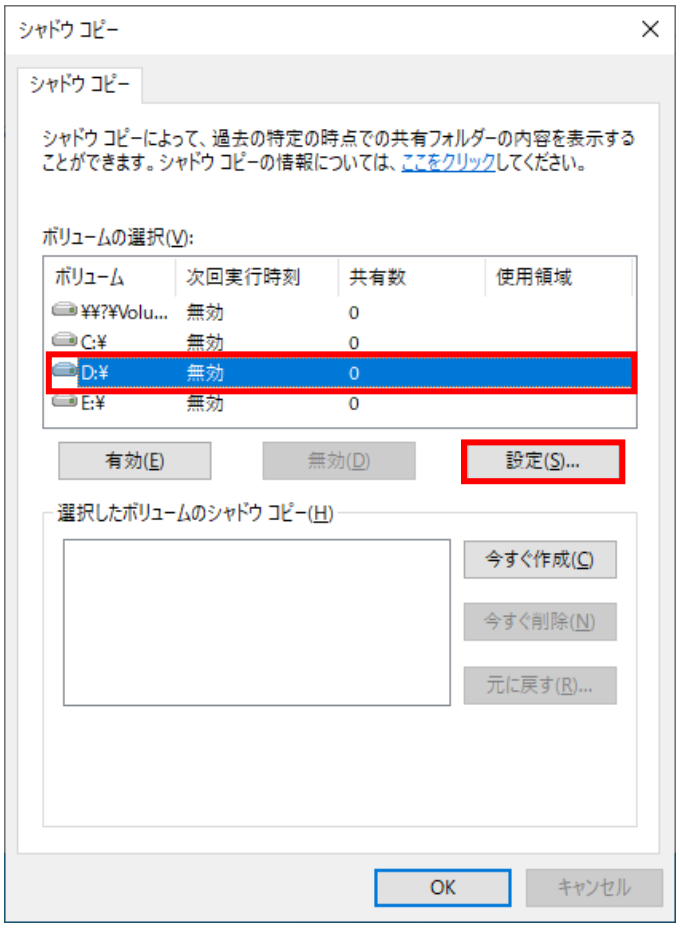
シャドウコピーの作成は、スケジューリングによる作成と手動での作成の 2 つの方法があります。手動でシャドウコピーを作成する場合は、シャドウコピー画面にて、対象のボリュームを選択し、[今すぐ作成]ボタンをクリックしてください。スケジューリングによるシャドウコピーの作成については、次項で説明します。



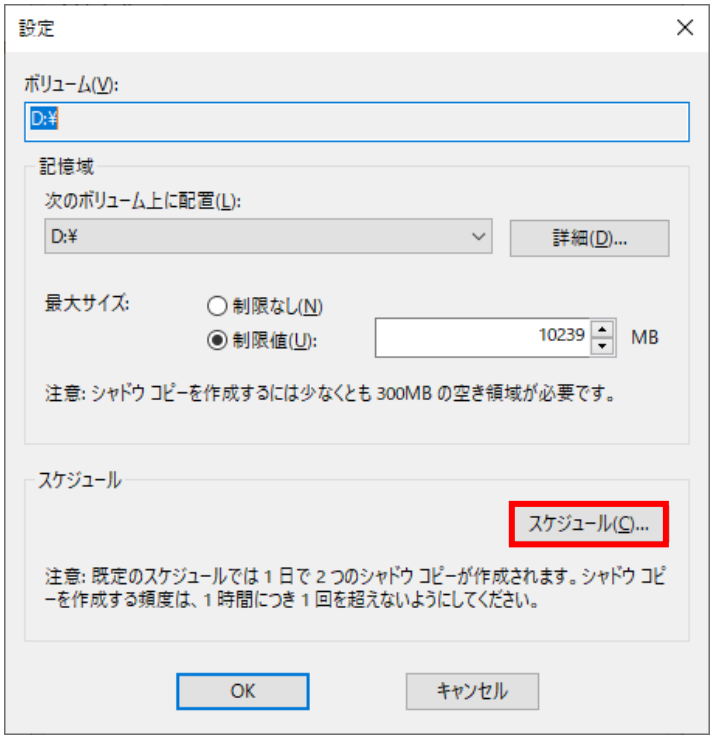
2.1.3.2 スケジュールの設定

シャドウコピーのスケジュールは、既定で 2 つのスケジュール（平日の 7:00 と 12:00）が設定されています。変更する場合は以下の手順を実施してください。

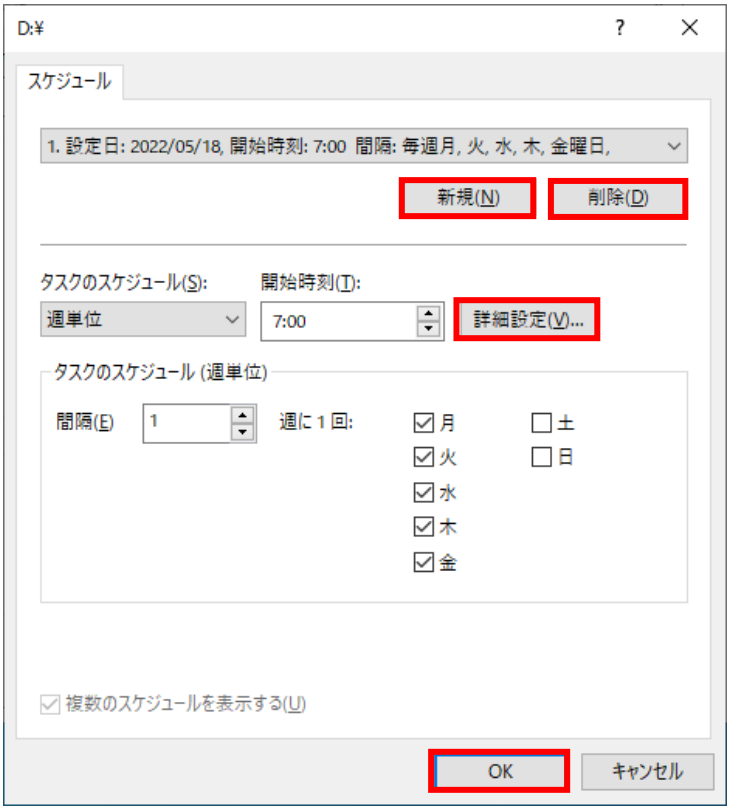
1. シャドウコピー画面にて、対象のボリュームを選択し、[設定] ボタンをクリックします。



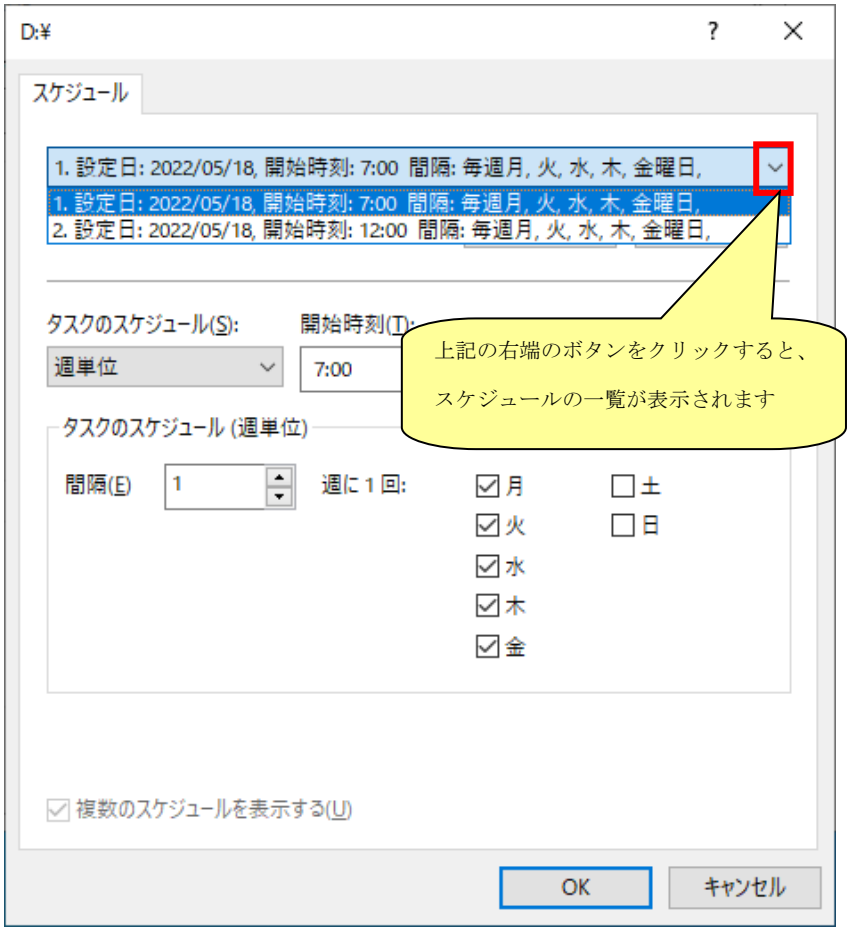
2. 設定画面が表示されるので [スケジュール] ボタンをクリックします。



3. スケジュールの設定画面が表示されます。



最上段のドロップダウンリストが、現在選択中のスケジュールです。複数のスケジュールが存在する場合、他のスケジュールに表示を切り替えることができます。



スケジュールの設定画面では次の操作を行うことができます。

1）新規作成

シャドウコピーの作成を開始する日時と、頻度を指定します。

2）削除

選択したスケジュールを削除します。

3）修正

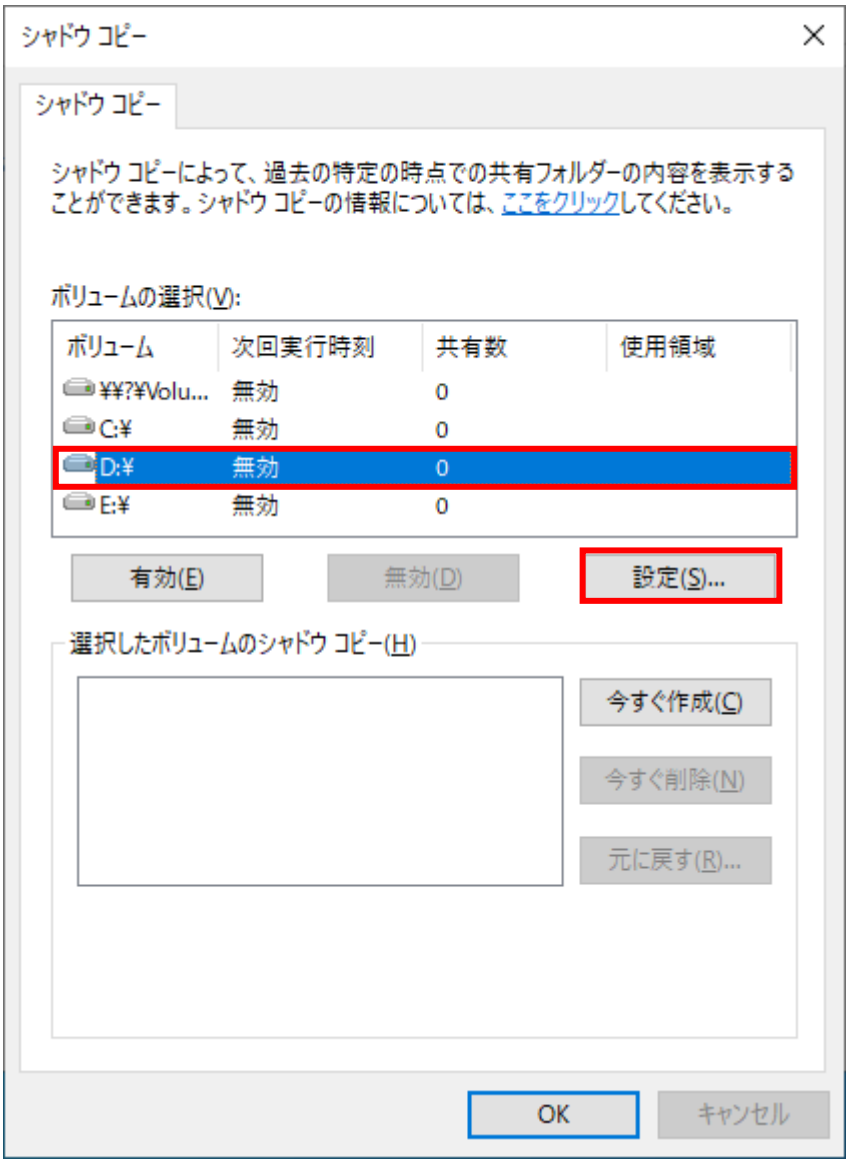
選択したスケジュールの項目を修正します。

【注意】
シャドウコピーの作成頻度は、1 時間につき 1 回までにしてください。

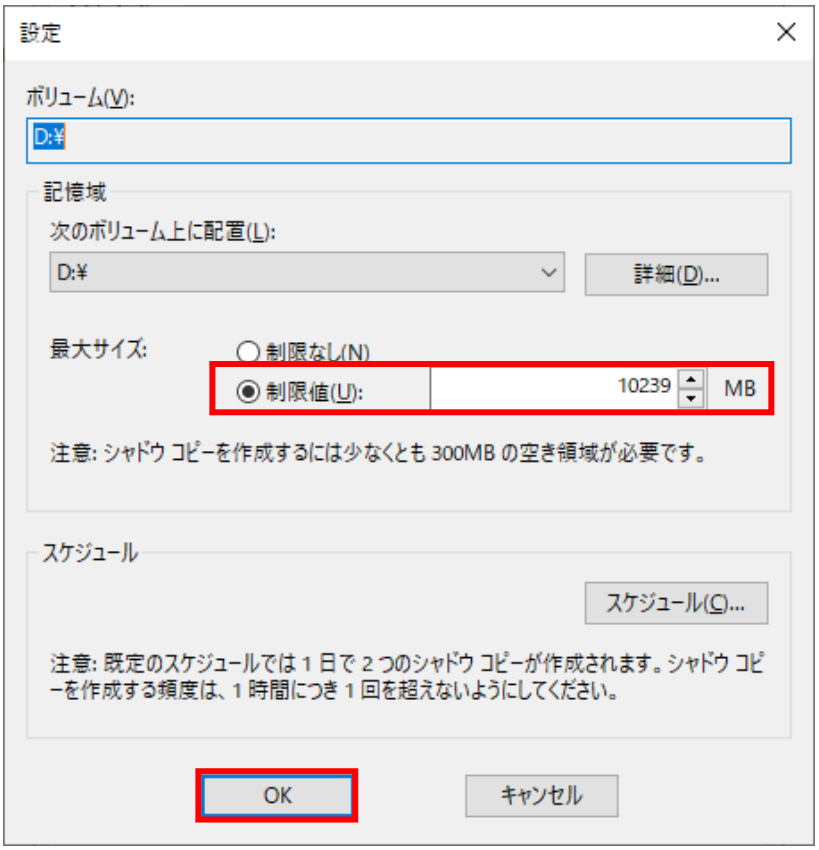
2.1.3.3 シャドウコピー記憶域の設定

シャドウコピーの記憶域は、既定ではソースボリューム (コピー対象のユーザーデータが保存されているボリューム) と同じボリュームが設定されています。また、シャドウコピーが使用できる最大ディスク容量の既定値は、ソースボリュームのサイズの 10%に設定されています。これらを変更する場合は以下の手順を実施してください。

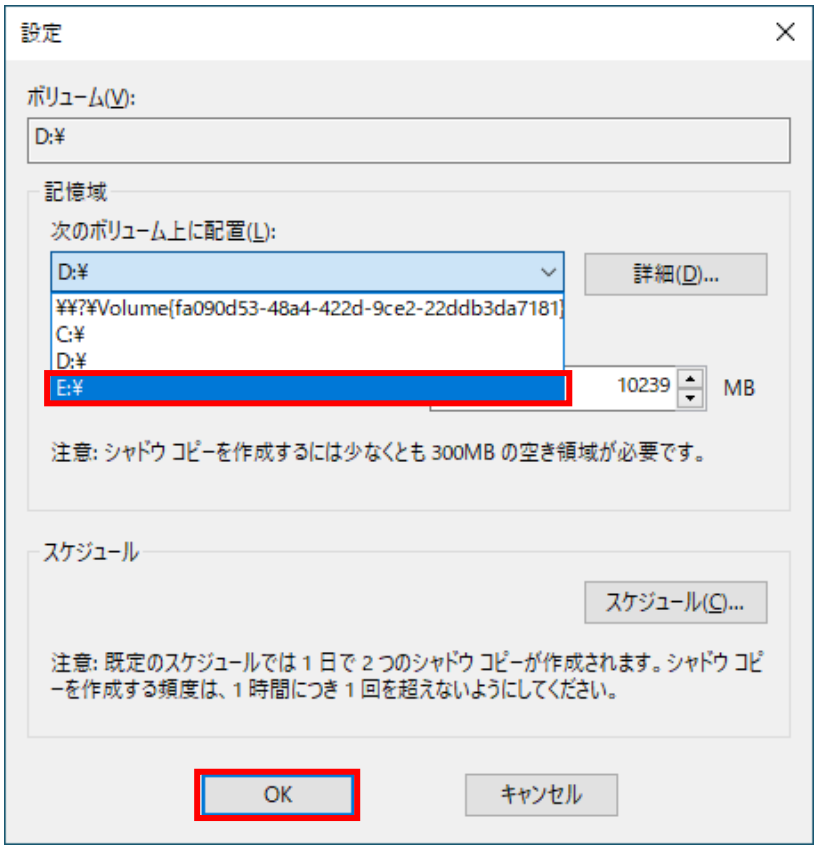
1. シャドウコピー管理画面にて、対象のボリュームを選択し、[設定] ボタンをクリックします。



2. 設定画面で、シャドウコピーの記憶域のボリューム、およびサイズを変更できます。シャドウコピーが使用できる最大ディスク容量の既定値は、ソースボリュームのサイズの 10%です。この値は変更することができますが、この値を大きくしても 1 つのボリュームに作成できるシャドウコピーの最大世代数は大きくなりません。



3. 記憶域を別ボリュームに配置する場合は、プルダウンからボリュームを選択します。なお、64TB を超えるボリュームはシャドウコピー記憶域の格納対象とはなりませんので、プルダウンに表示されません。

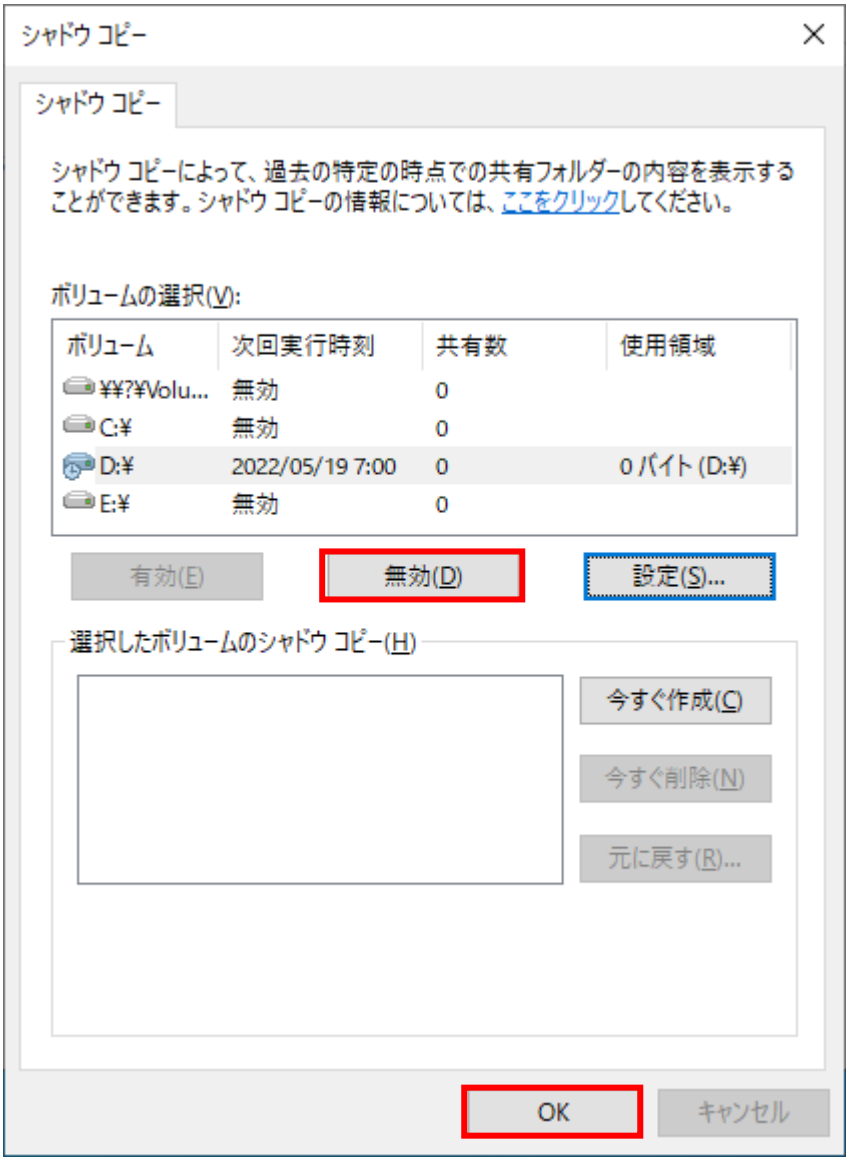


【注意】

- シャドウコピー記憶域の最大ディスク容量を現在の値よりも小さいサイズに変更する場合、新しい容量に合わせて古いシャドウコピーが削除されます。削除されたシャドウコピーは元に戻すことができません。
- シャドウコピーを有効化しているボリュームにおいて、シャドウコピー記憶域の格納先ボリュームを変更する場合、シャドウコピーを無効化し、格納先ボリュームを変更後、シャドウコピーを有効化してください。このとき、システムの再起動は不要です。なお、シャドウコピーの無効化により、取得しているシャドウコピーは全て削除されますので、ご注意ください。

2.1.3.4 シャドウコピーの無効化

該当ボリュームでのシャドウコピーの使用を停止する場合は、[無効] ボタンをクリックしてください。[無効] ボタンをクリックすると、そのボリューム上に存在するすべてのシャドウコピー、およびシャドウコピーのスケジュールが削除されます。



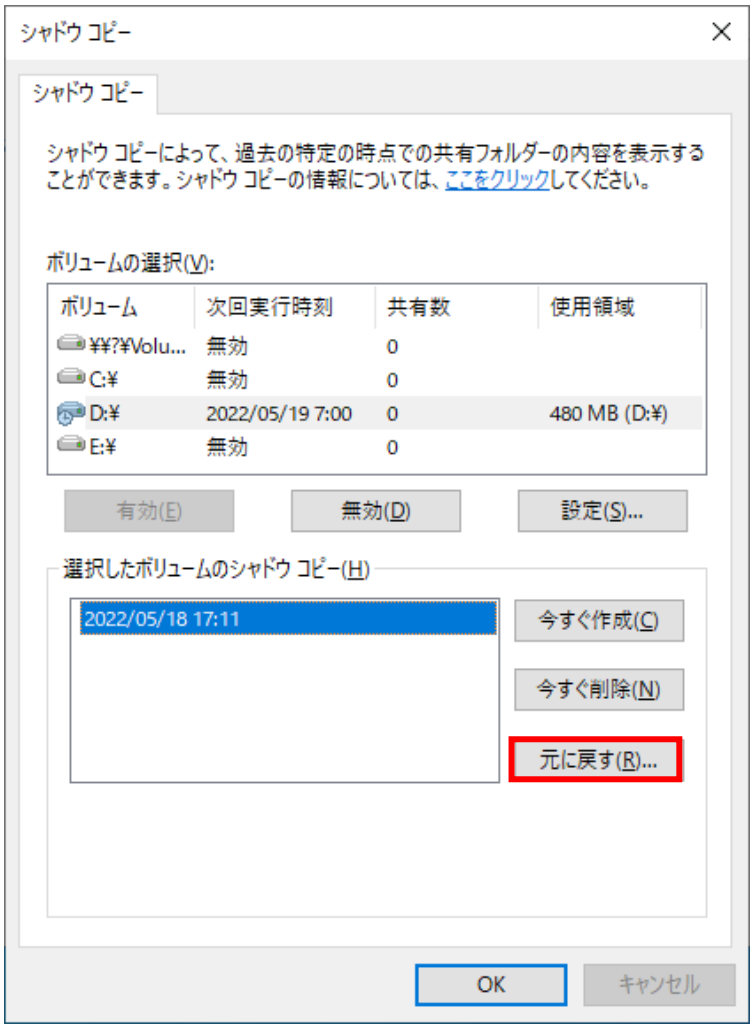
2.1.4 シャドウコピーからの復元

保存されているシャドウコピーから、ファイルやフォルダーを復元したい場合、以下の方法があります。

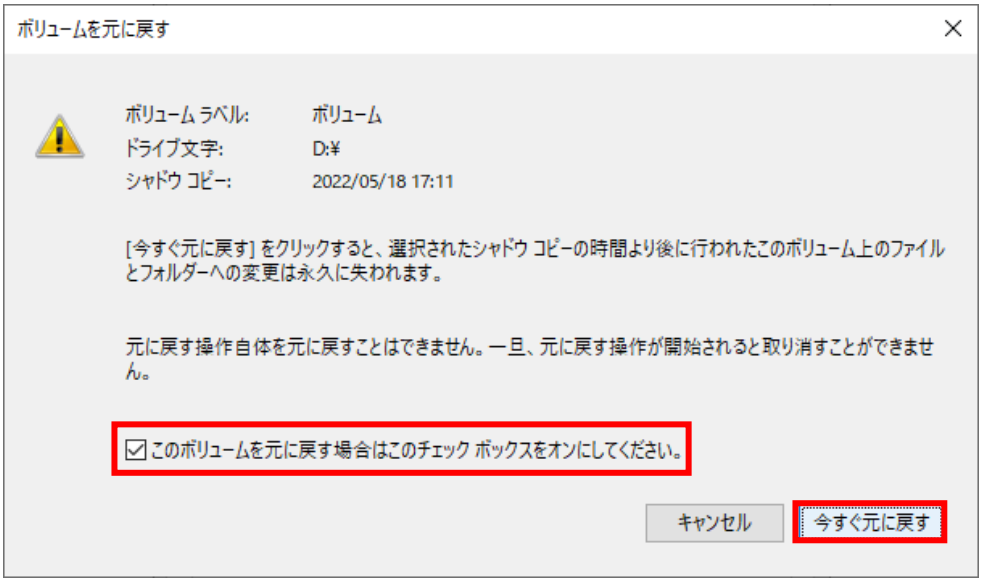
- iStorage NS 上で、ボリューム単位で実施する方法
- Windows クライアントからフォルダー／ファイル単位で実施する方法
- UNIX クライアントからフォルダー／ファイル単位で実施する方法

2.1.4.1 iStorage NS 上での復元方法

ボリューム単位での復元を行う場合、iStorage NS 上のエクスプローラーで復元したいボリュームを選択し、右クリックメニューから [シャドウコピーの構成] を選択します。下記画面の [選択したボリュームのシャドウコピー] 欄から元に戻したい世代を選択して [元に戻す] ボタンをクリックします。



下記のような警告が表示されますので、チェックを入れ、[今すぐ元に戻す] ボタンをクリックします。



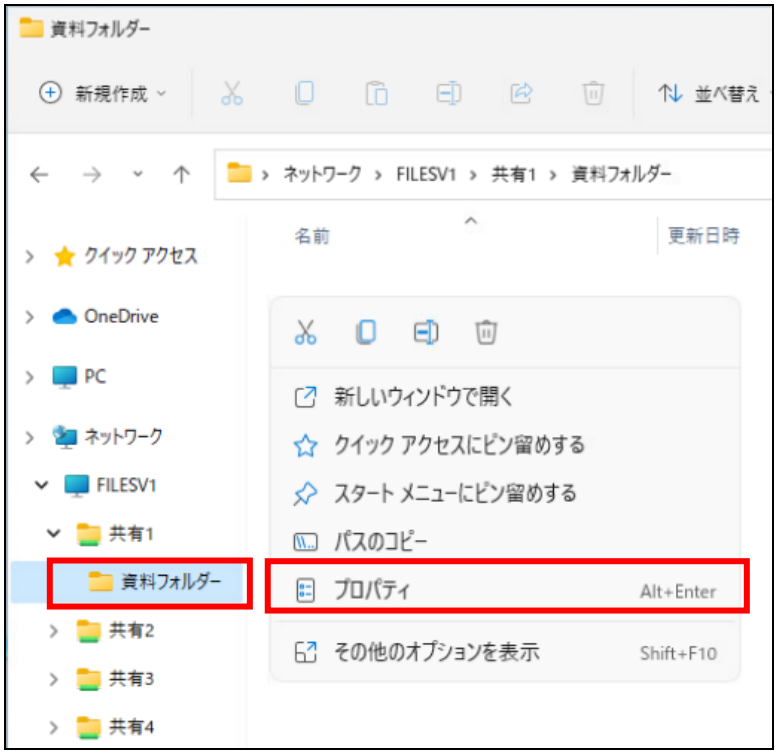
2.1.4.2 Windows クライアントからの復元方法

Windows クライアントからフォルダー／ファイル単位の復元を行う場合、クライアントコンピューター上のエクスプローラーから操作を行います。なお、Windows クライアントの OS バージョンによっては画面表示が異なる場合があります。

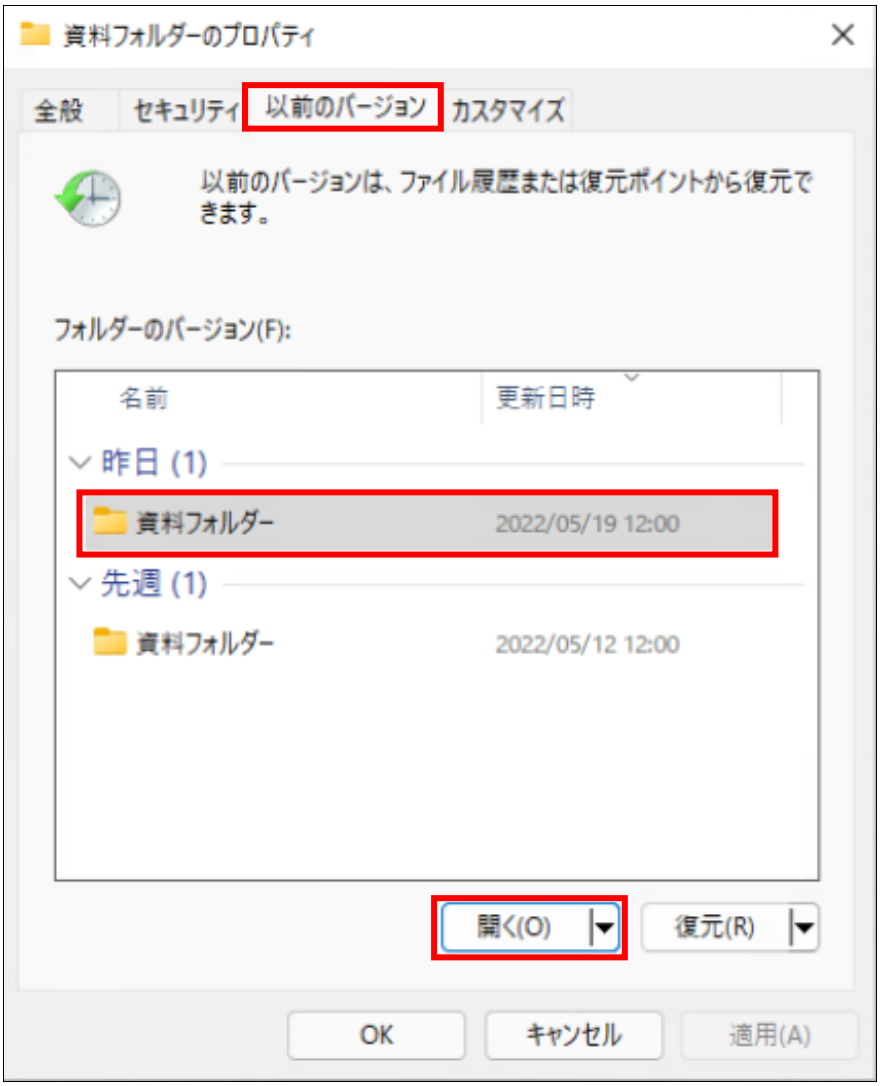
2.1.4.2.1. 削除したファイルの復元

削除したファイルを復元する場合は、以下の手順に従って、クライアント上のエクスプローラーから操作を行います。

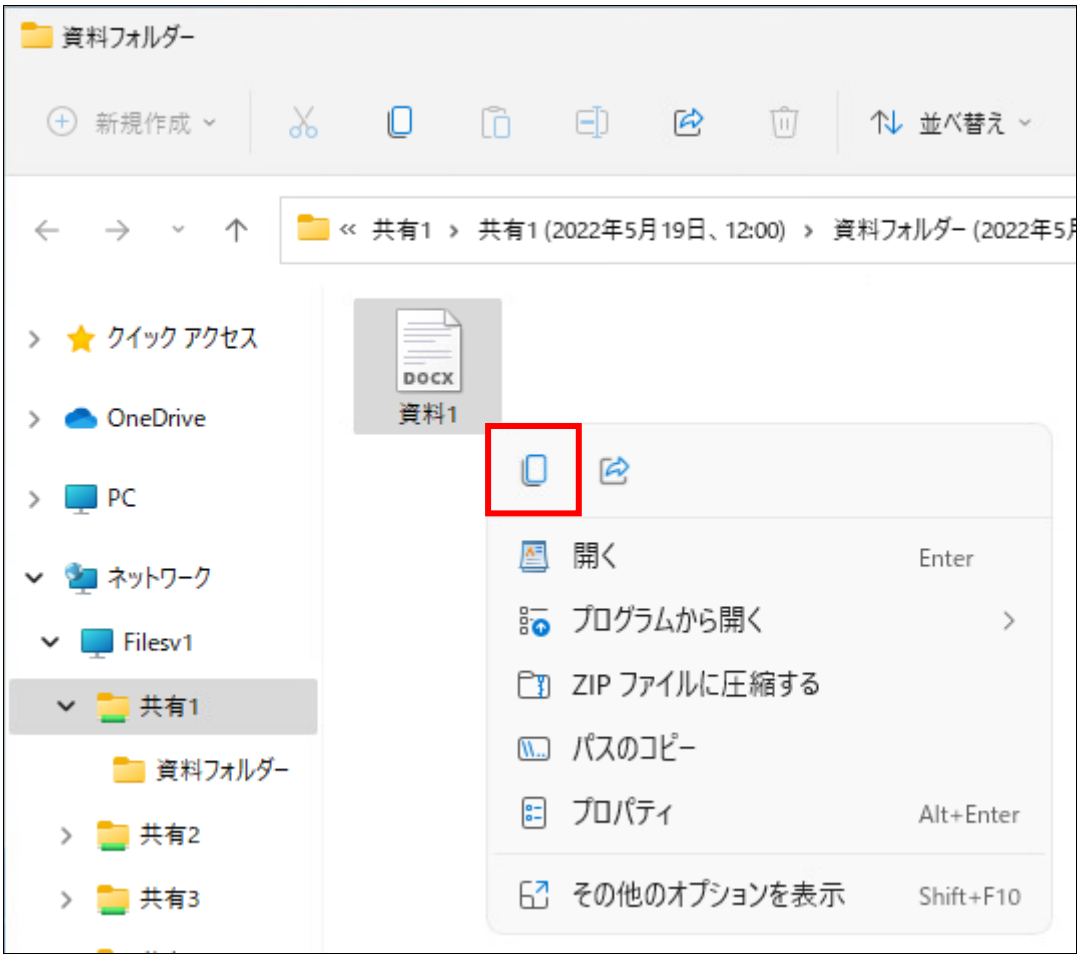
1. 削除したファイルが格納されていた共有フォルダーを選択し、右クリックメニューから[プロパティ]をクリックします。



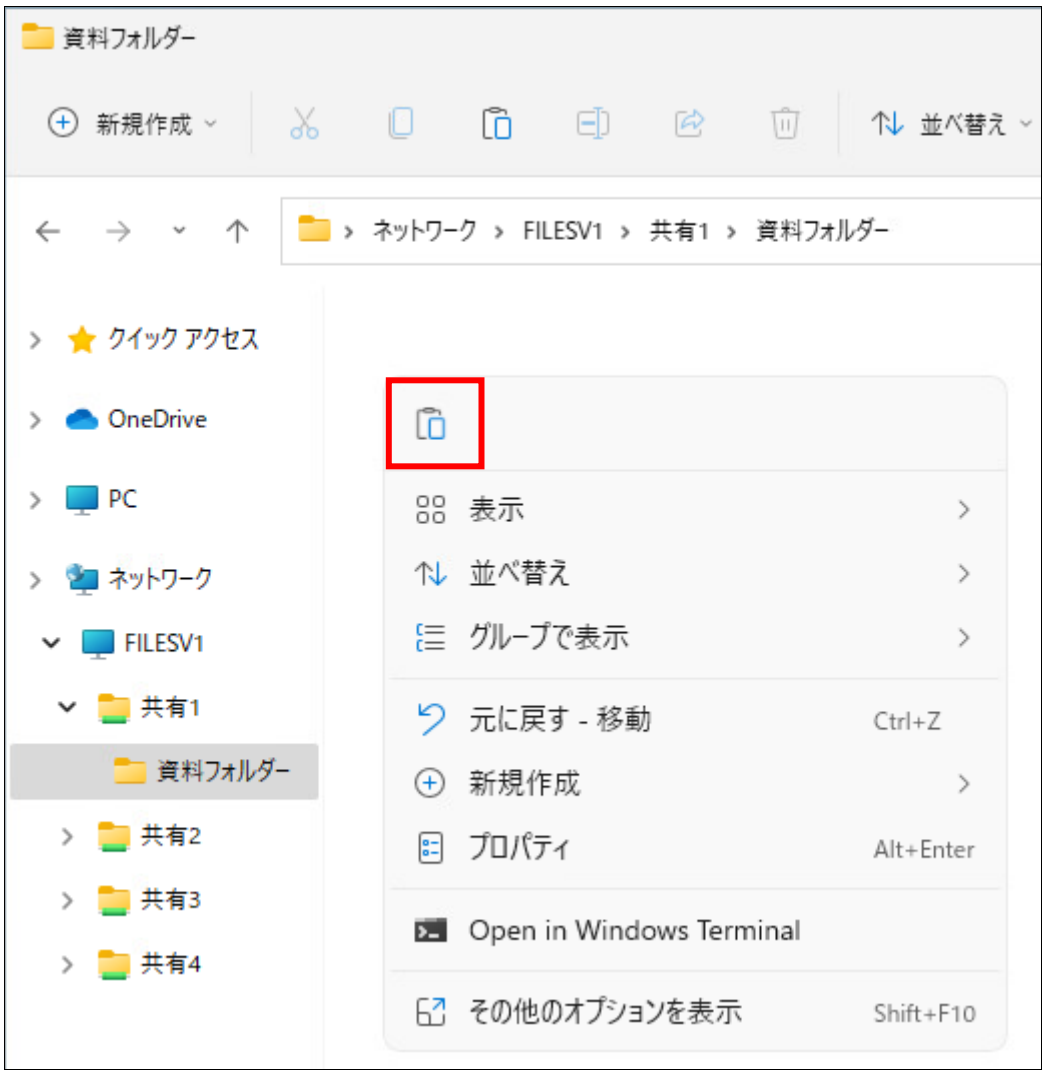
2. プロパティ画面にて [以前のバージョン] タブをクリックします。[フォルダーのバージョン] 欄にシャドウコピーの世代の一覧が表示されますので、 削除される前のファイルを含む世代を選択し、[開く] ボタンをクリックします。



3. 別のエクスプローラーの画面が新しく起動し、前項で選択した世代のフォルダー内のファイル一覧が表示されます。復元したいファイルを選択し、右クリックメニューから [コピー] アイコンを実行します。



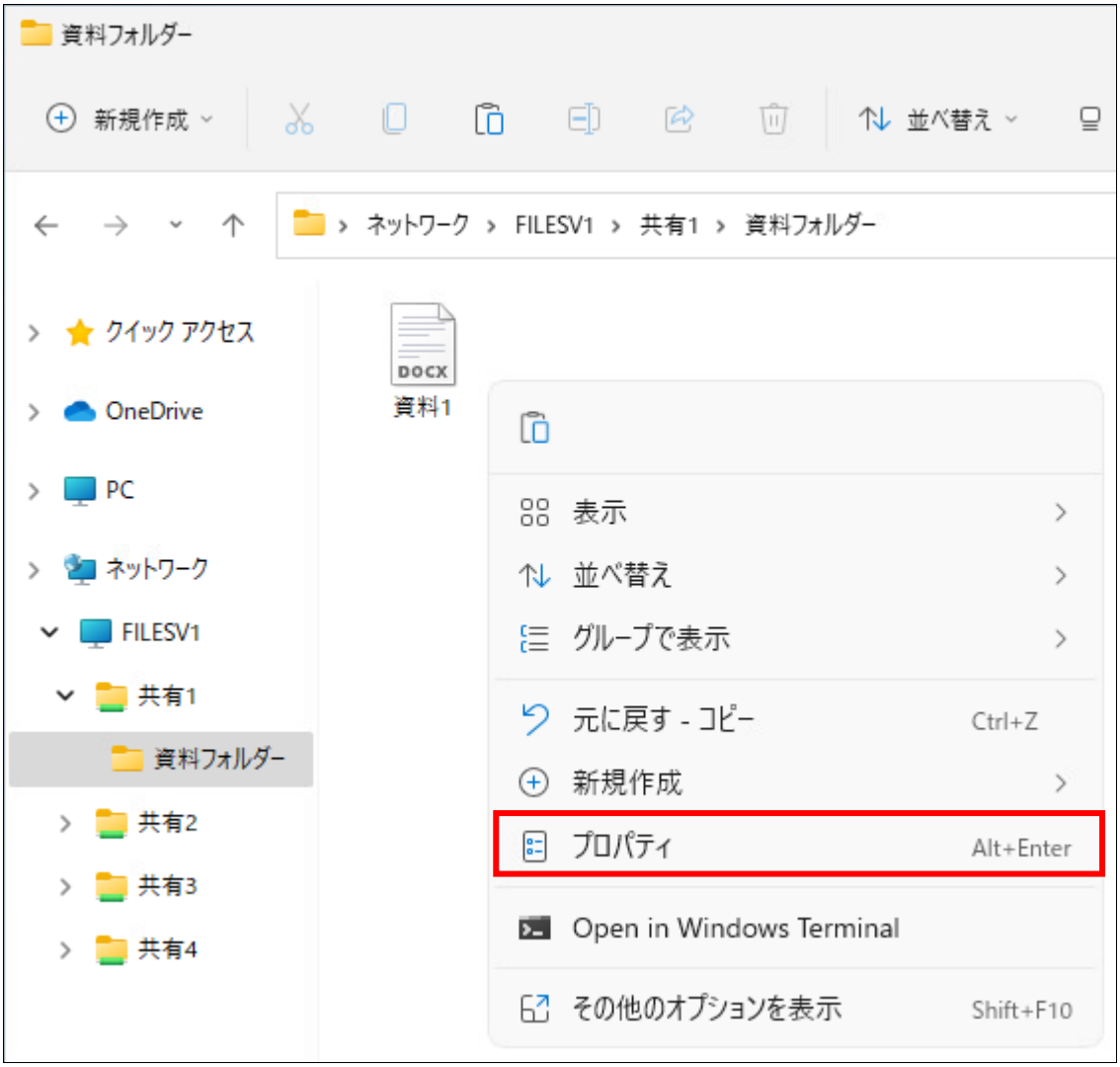
4. 表示するウィンドウを項番 2 のエクスプローラーに切り替え、復元先のフォルダーを選択し、右クリックメニューから [貼り付け] アイコンを実行すると、ファイルが復元されます。



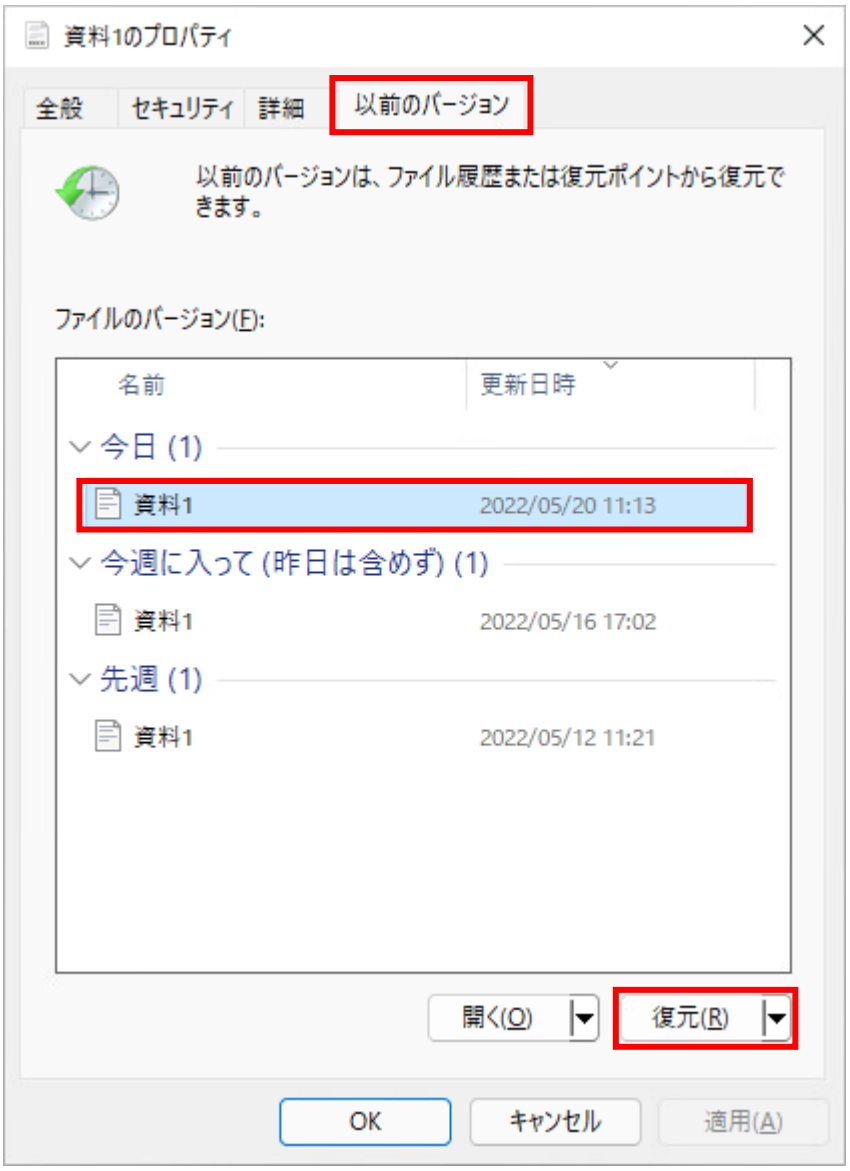
2.1.4.2.2. 更新したファイルの復元

誤って更新したファイルや壊れたファイルを復元する場合は、以下の手順に従って、クライアント上のエクスプローラーから操作を行います。

1. 誤って更新したファイル (もしくは壊れたファイル) を選択し、右クリックメニューから[プロパティ] をクリックします。



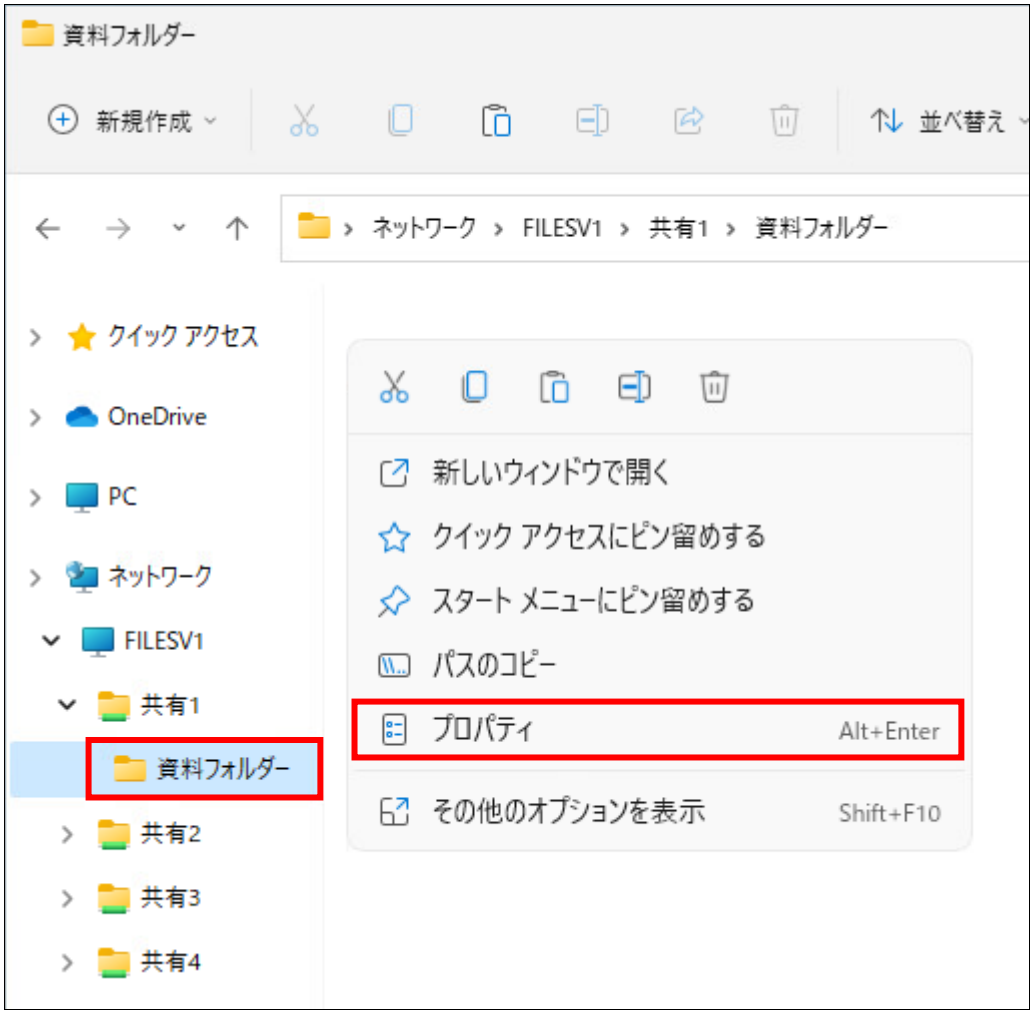
2. プロパティ画面にて [以前のバージョン] タブをクリックします。 [ファイルのバージョン] 欄から戻したい世代を選択し、[復元] ボタンをクリックすれば、元の場所へ復元ができます。また、別の場所へ復元したい場合は、[コピー] ボタンをクリックして、戻したい場所を指定します。なお、 [開く] ボタンをクリックするとファイルを開きます。



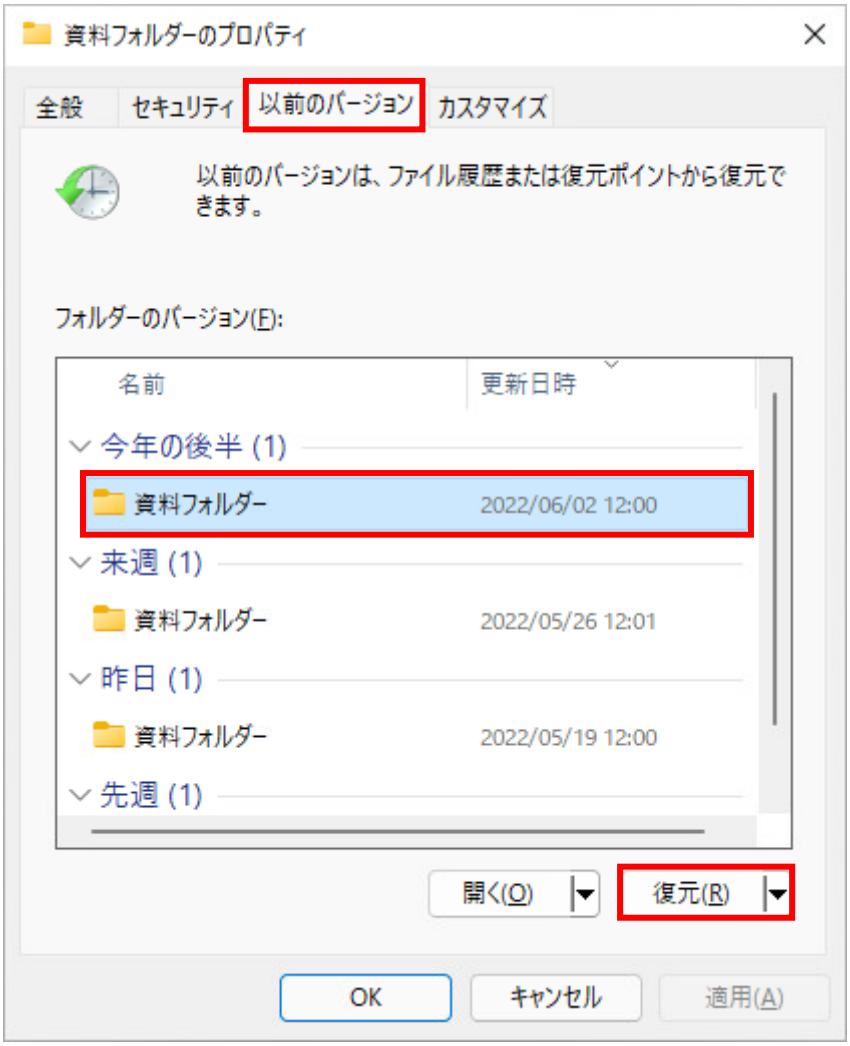
2.1.4.2.3. フォルダーの復元

指定したフォルダー配下のサブフォルダーとファイルをまとめて復元したい場合は、以下の手順に従って、クライアント上のエクスプローラーから操作を行います。

1. 復元したいフォルダーを選択し、右クリックメニューから[プロパティ] をクリックします。



2. プロパティ画面にて [以前のバージョン] タブをクリックします。[フォルダーのバージョン] 欄にシャドウコピーの世代が表示されますので、復元したい世代を選択し、元の場所に復元したい場合は [復元] ボタンをクリックします。



【注意】
以前のバージョンのフォルダーには存在していなかったファイルが、現在のフォルダーに存在する場合、フォルダー全体に対して［復元］操作を実施しても、新たに作成されたファイルは削除されません。

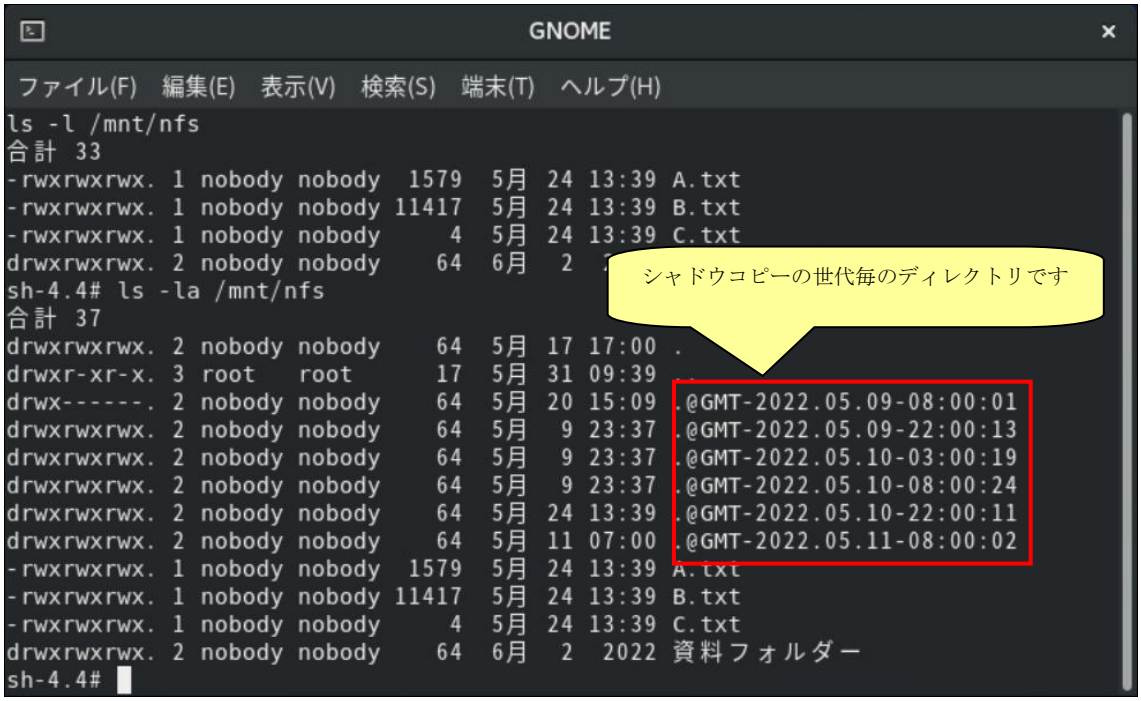
2.1.4.3 UNIXクライアントからの復元方法

UNIX クライアントからフォルダー／ファイル単位の復元を行う場合、コマンド等により、フォルダー／ファイルを復元することが可能です。

シャドウコピーは NFS 共有直下に、".@GMT-(日付)"というディレクトリとして表示されます。UNIX の ls コマンドの仕様によっては、デフォルトではドットで始まるファイル名を一覧に表示しないことがありますのでご注意ください。

UNIX クライアントからディレクトリ／ファイルの復元操作を行う場合は、該当する世代のシャドウコピーのディレクトリ／ファイルを復元したいディレクトリにコピーしてください。

ディレクトリ名に設定されている日時はグリニッジ標準時にて表示されています。



【注意】
シャドウコピーは読み取り専用です。編集はできません。

2.1.5 シャドウコピーサービスに関する注意事項

- シャドウコピーは、NTFS ファイルシステムのデータボリュームのみに対応しています。FAT ファイルシステムには対応していません。

- システム領域を含むボリューム、および、仮想メモリのページングファイルや休止ファイルを含むボリュームでは、シャドウコピーサービスを有効にしないでください。

- シャドウコピーを有効にするボリューム、およびシャドウコピーを保存するボリュームとして 64TB を超えるボリュームは指定できません。

- シャドウコピーは 1 つのボリュームにつき最大 64 個まで作成できます。それ以上シャドウコピーが作成された場合、一番古いシャドウコピーが削除されます。

- シャドウコピー記憶域の最大ディスク容量を現在の値よりも小さいサイズに変更する場合、新しい容量に合わせて古いシャドウコピーが削除されます。削除されたシャドウコピーは元に戻すことができません。

- I/O 負荷が高いシステムにおいては、取得済みのシャドウコピーがすべて削除される現象が発生し易くなります。このような場合、シャドウコピーの保存先ボリュームとしてシャドウコピーを有効化していない別ボリュームを設定することを検討してください。

- シャドウコピーを有効にするボリュームで最適化 (デフラグ) を実行する予定がある場合は、そのボリュームを 16KB 以上のアロケーションユニットサイズでフォーマットしてください。16KB 未満の場合、ボリュームを最適化すると予期せずシャドウコピーが削除されることがあります。なお、出荷状態は、アロケーションユニットサイズを 16KB でフォーマットしています。

- シャドウコピーの作成頻度は、最大 1 時間に 1 回までにしてください。

- 複数ボリュームでシャドウコピーを有効にする場合、デフォルトのスケジュール時刻（平日の 7 時と 12 時）のままではスケジュール時刻が重複しますので、各ボリュームのスケジュール時刻が重複しないように変更してください。また、シャドウコピーを利用するバックアップソフトウェア製品をご利用の際には、バックアップのスケジュール時刻がシャドウコピーのスケジュール時刻と重ならないようにしてください。

- シャドウコピーを設定していたボリュームを削除する場合、事前にそのボリュームに対するシャドウコピーを無効にしてください。シャドウコピーのスケジュール設定が残ったまま、ボリューム削除を行った場合、イベントログに大量の「ソース: VSS イベント ID:7001」のイベントが記録されます。

- シャドウコピーのデータは一時的なものと認識してください。シャドウコピーの使用ディスク容量が設定した最大ディスク容量に達した場合、もしくは、シャドウコピーの数が既定では 65 個に達した場合など、意図せずシャドウコピーが削除されることがあります。そのため、シャドウコピーはバックアップの代用とはなりませんので、通常のバックアップ作業は必要です。大切なデータについては、必ずバックアップソフトウェアを使ってバックアップするようにお願いします。

- シャドウコピーは読み取り専用です。編集はできません。

- Windows Server バックアップのバックアップデータ保存先には、シャドウコピーを設定しないでください。

- Windows クライアントからの復元操作において、復元しようとするファイルのパス長が 256 文字を超えていると、Windows OS の制限により「パス長が長い」というメッセージが表示され、復元することができません。そのような場合は、フォルダー構成のより深い階層に共有フォルダーを設定していただき、その共有に接続することで、パス長が短くなるようにしてください。

- シャドウコピー対象ボリューム(ソースボリューム)で BitLocker が有効となっている場合は、シャドウコピー記憶域の格納先ボリュームはソースボリュームから変更できません。このため、BitLocker が有効なボリュームに対するシャドウコピーの設定時には、シャドウコピー記憶域の格納先ボリュームの選択肢に、自ボリューム以外のボリュームが表示されません。

- 1 つのボリュームに対して、シャドウコピー機能とデータ重複除去機能を同時に有効にする場合、データ重複除去対象のデータ量増加に応じて、シャドウコピーの一部の世代 (または全世代) が削除されることがあります。

【補足】
通常、シャドウコピー記憶域には、過去の複数世代分の差分データが保存されており、空きが少なくなると、一番古い世代を自動的に削除します。
データ重複除去機能によるファイル再構成は、シャドウコピー機能の変更差分として収集されますので、データ重複除去対象のデータが増加すると、シャドウコピー記憶域に保存される変更差分の量が多くなります。このため、1 つのボリュームに対して、シャドウコピー機能とデータ重複除去機能を同時に有効にする場合、データ重複除去を有効化する前に比べ、保存されるシャドウコピーの世代が少なくなることがあります。

- シャドウコピーのスケジュールは、タスクスケジューラに反映され、実行されます。
  シャドウコピーのスケジュール設定は、複数のスケジュール時刻の変更差分の合計が 0 となる変更を一度に行った場合、タスクスケジューラにスケジュールの変更が反映されない場合があります。
  (例えば、3 つのスケジュールがあり、7:00→9:00(+2 時間)、12:00→11:00(-1 時間)、17:00→16:00(-1 時間)となるような変更)
  この場合、スケジュールを 1 つずつ変更してください。

- シャドウコピーを有効にしているシステムにおいて、シャドウコピーを利用するバックアップソフトウェア製品やファイルサーバーリソースマネージャー (FSRM) 機能を使用すると、意図しないタイミング (スケジュールされたシャドウコピー処理の延長) で動作する後処理により、I/O 負荷が高くなる事象が発生します。このため、シャドウコピーのスケジュール時刻は、バックアップ処理や FSRM の記憶域レポート作成のスケジュール時刻と重ならないようにしてください。また、スケジュールされたシャドウコピー処理とその後動作する後処理により I/O 負荷が高くなっても業務に支障がない時間帯にシャドウコピーのスケジュール時刻を調整してください。

- シャドウコピーを有効化しているボリュームにおいて、シャドウコピー記憶域の格納先ボリュームを変更する場合、シャドウコピーの無効化により、取得しているシャドウコピーは全て削除されます。

2.1.5.1 シャドウコピーの世代数を減らす方法について

シャドウコピーの世代数を減らす場合は、下記の手順に従いレジストリを変更してください。なお、シャドウコピーの世代数は全てのボリュームに対して同じ値が適用され、ボリューム毎に別の値を設定することはできません。

【注意】
レジストリ エディターの使い方を誤ると、深刻な問題が発生することがあります。
最悪の場合、オペレーティング システムの再インストールが必要になることがあります。 弊社ならびにマイクロソフト社は、レジストリ エディターの誤用により発生した問題に関しては、一切責任を負わないものとします。レジストリ エディターは、お客様の責任においてご使用ください。

1. iStorage NS に Administrator 権限でサインインし、レジストリエディター(regedit.exe)を起動します。
2. 次のレジストリキーを選択します。
   HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥VSS¥Settings
3. [編集] メニューの [新規] を選択し、 [DWORD 値] をクリックします。
4. 名前に **MaxShadowCopies** と入力し、Enter キーを押します。
5. [MaxShadowCopies] をダブルクリックし、10 進数を選択して指定したい値(63 以下の値)を入力します。
6. レジストリエディターを終了して、システムを再起動します。

なお、デフォルト値は 64 です。

2.1.5.2 予期せずシャドウコピーがすべて削除される現象について

シャドウコピーの対象ボリュームとシャドウコピー記憶域の格納先ボリュームが同一ボリューム（既定値）に設定されている環境で I/O 負荷が高い場合、イベントログに「ソース: Volsnap イベント ID:25」が記録され、予期せずシャドウコピーがすべて削除される現象が発生することがあります。
回避策は以下の通りです。

シャドウコピー記憶域の格納先ボリュームとして、シャドウコピーが設定されていない別のボリュームを設定する。

2.2 ファイルサーバーリソースマネージャー

2.2.1 ファイル サーバー リソース マネージャー(FSRM) の概要

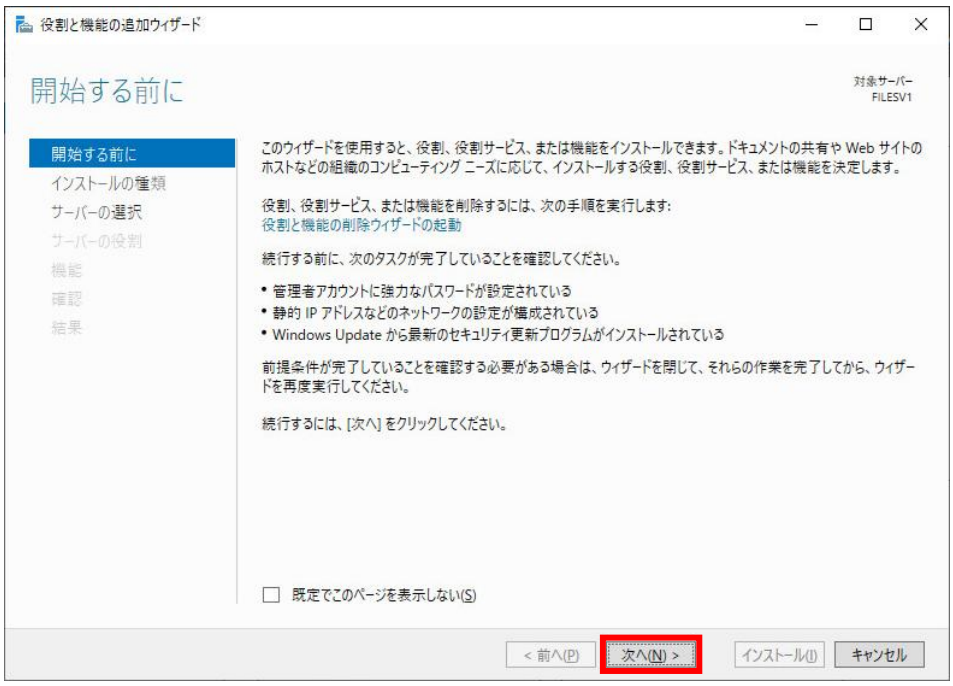
FSRM は、ファイル サーバーに保存されたデータの管理および分類を行うための機能のセットです。具体的には、クォータ、ファイルスクリーン、記憶域レポート、ファイル分類インフラストラクチャ（FCI）の機能があります。

2.2.2 FSRM のインストール

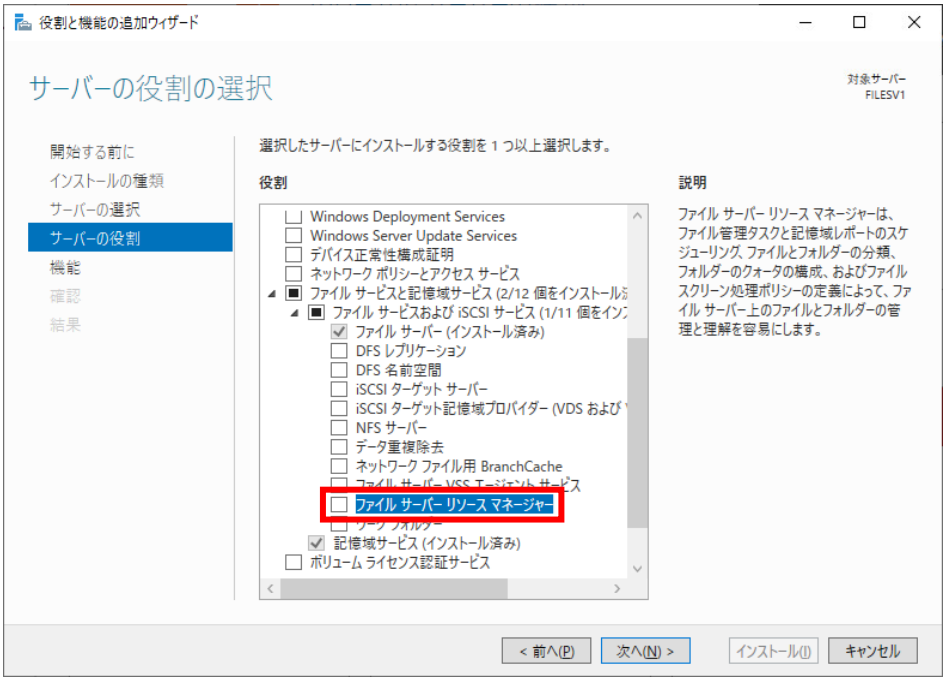
FSRM は出荷状態ではインストールされていませんので、使用に際しては、下記の手順にてインストールする必要があります。

1. サーバーマネージャーを起動し、[管理] - [役割と機能の追加] をクリックします。

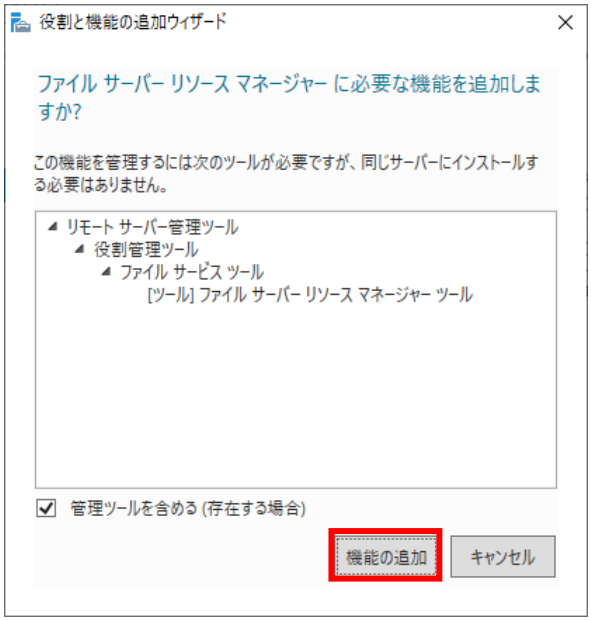
2. [開始する前に] 画面が表示されますので、デフォルト状態のまま [次へ] ボタンをクリックして、[サーバーの役割の選択] 画面まで進みます。



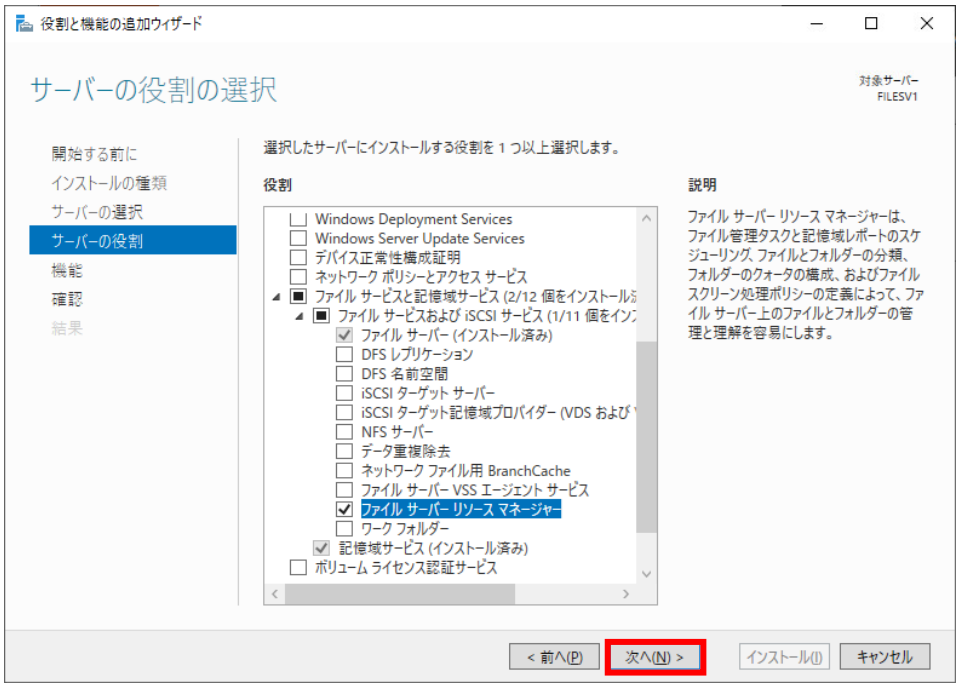
3. [サーバーの役割の選択] 画面の [ファイルサービスと記憶域サービス]、[ファイルサービスおよび iSCSI サービス] を順に展開して、[ファイル サーバー リソース マネージャー] をチェックします。



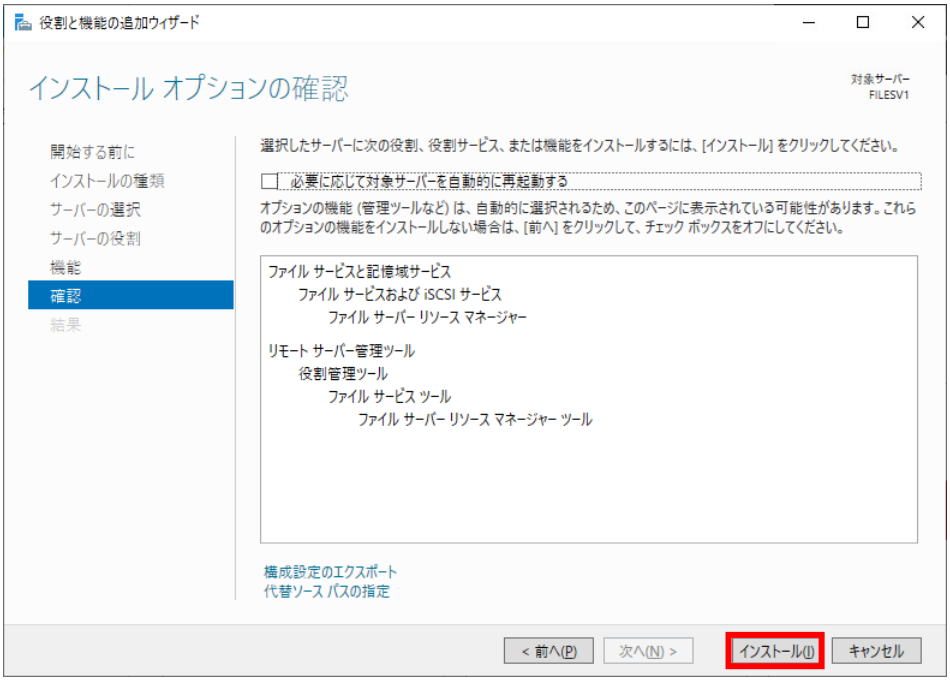
4. [ファイル サーバー リソース マネージャー に必要な機能を追加しますか？] 画面が表示されますので、 [機能の追加] をクリックします。



5. [サーバーの役割の選択] 画面に戻りますので、[次へ] をクリックします。



6. [機能の選択] 画面が表示されますので [次へ] をクリックして、[インストールオプションの確認] 画面に進み、[インストール] をクリックします。



7. [インストールの進行状況] 画面が表示されますので、インストールの完了を待ち、[閉じる] をクリックします。

2.2.3 通知設定

FSRM の各機能では、アクション実行時に様々な方法での通知を行うことができます。

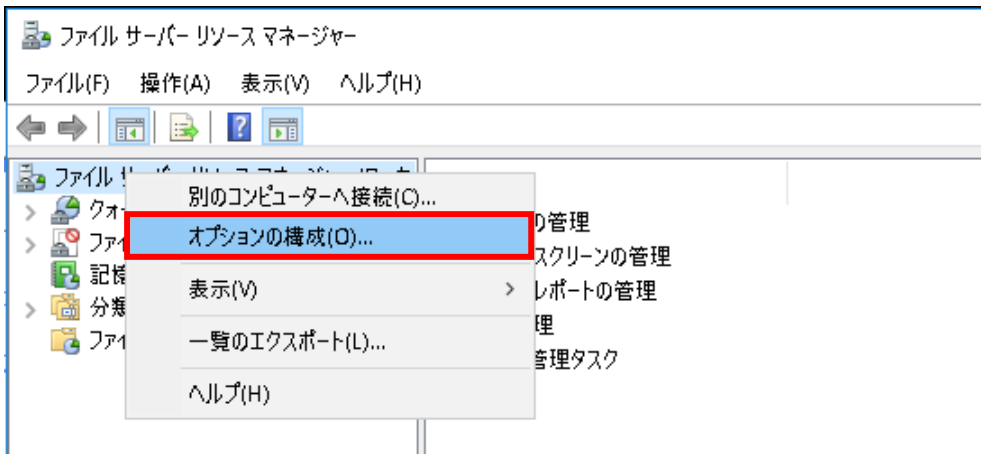
2.2.3.1 電子メール

あらかじめ「既定の電子メール」を設定しておくことで、ディスク容量がクォータの制限値を超えたときなどの通知や記憶域レポートを、メール送信することができます。

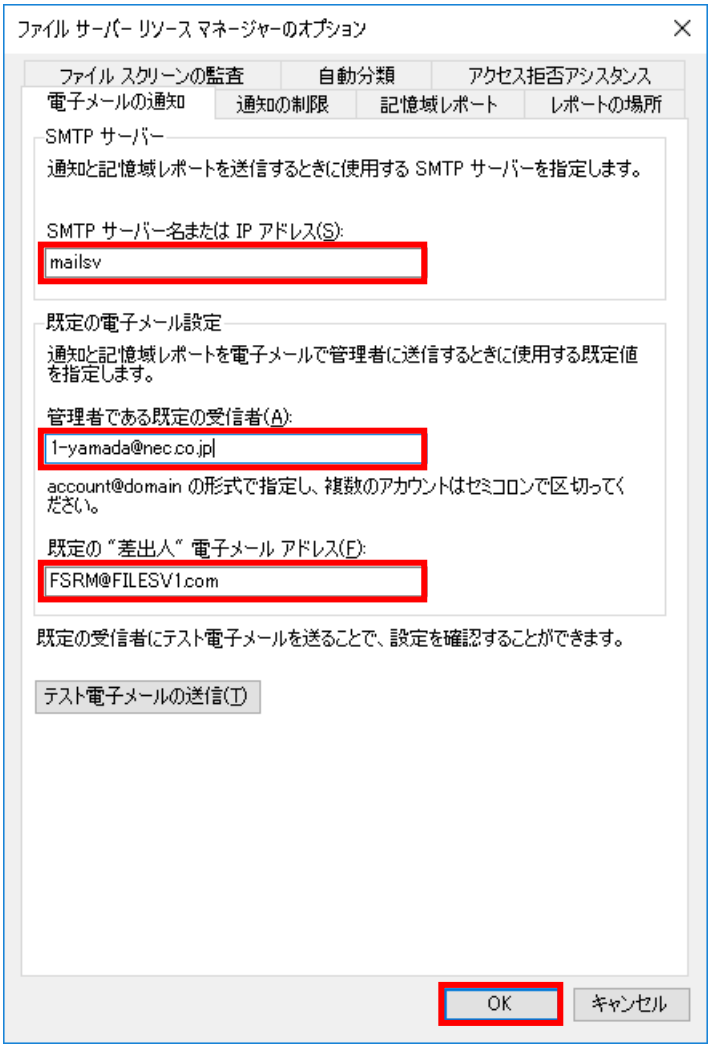
設定方法は以下の通りです。

1. 管理者メニューから [ファイル サーバー リソース マネージャー] を起動します。

2. [ファイルサーバーリソースマネージャー（ローカル）] を右クリックし、[オプションの構成] を選択します。



3. [ファイル サーバー リソース マネージャーのオプション] 画面で、メールの送信に利用する SMTP サーバー名もしくは IP アドレスと、通知メールの送信先、差出人となるメールアドレスをそれぞれ設定し、[OK] をクリックします。



【補足】

[管理者である既定の受信者] のメールアドレスは、FSRM の各機能の通知メール設定で [Admin Email] と表示され、送信先アドレスの初期値となります。

【注意】

“SMTP サーバー名または IP アドレス” に設定するメールサーバーについては、SMTP 認証機能を有していないメールサーバーを指定してください。

【注意】
“差出人”電子メールアドレスは、ご利用のメールサーバーの仕様として制限がなければ、メールアカウントとして存在しない任意の値が設定可能ですが、メールアドレスの形式（「任意の文字@任意の文字.任意の文字」）である必要があります。また、”¥”のようなメールアドレスに使用できない記号は使用できません。

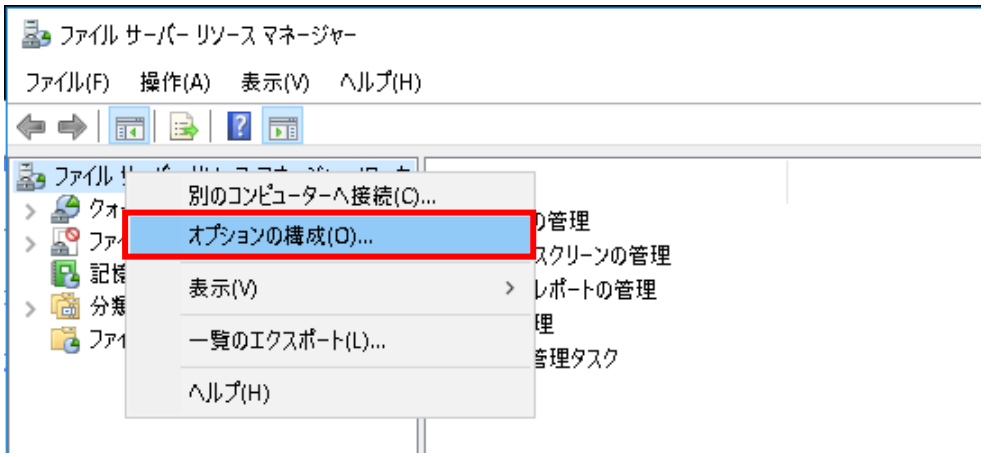
2.2.3.2 記憶域レポートの格納場所

FSRM における管理事象の発生時に、記憶域レポートを作成することもできます。
記憶域レポートはデフォルトでは「C:¥StorageReports」配下に格納されますが、格納場所は任意の場所に変更することもできます。

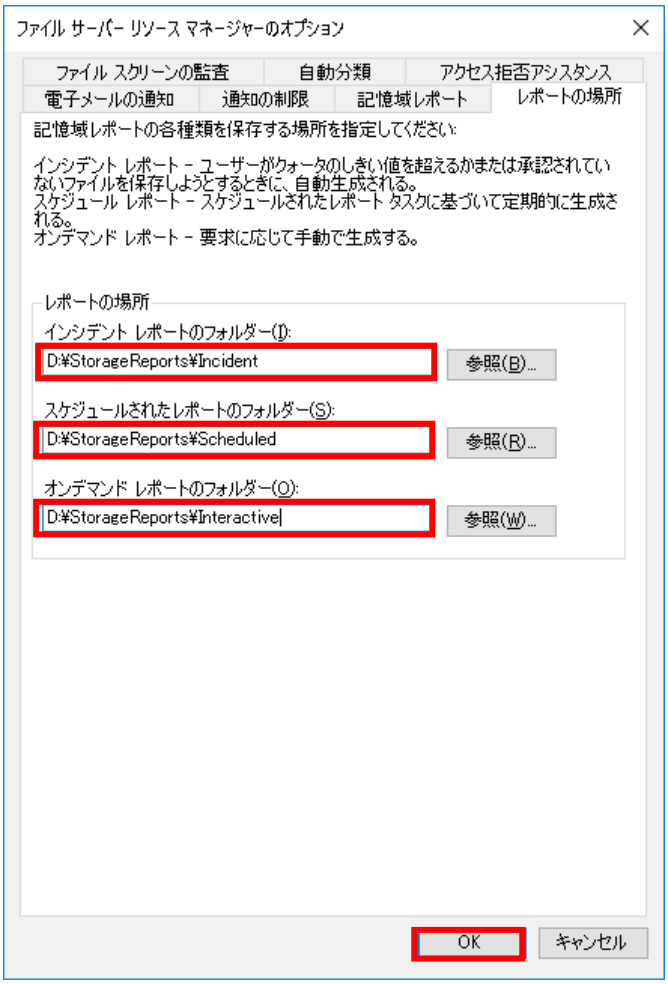
【注意】
記憶域レポートを電子メールで通知する場合においても「C:¥StorageReports」（デフォルト設定）配下の記憶域レポートは削除されませんので、お客様にて管理いただく必要があります。

記憶域レポートの格納場所の変更方法は、以下の通りとなります。

1. 管理者メニューから [ファイル サーバー リソース マネージャー] を起動して、 [ファイルサーバーリソースマネージャー（ローカル）] を右クリックし、[オプションの構成] を選択します。



2. [ファイル サーバー リソース マネージャーのオプション] 画面で、[レポートの場所] タブに移動し、インシデントレポートのフォルダー、スケジュールされたレポートのフォルダー、オンデマンドレポートのフォルダーをそれぞれ設定して、[OK] をクリックします。



2.2.3.3 その他の通知

電子メール送信や記憶域レポート送信以外にも、イベントログへの記録、任意のコマンドの実行によって、FSRM における管理事象の発生を通知することができます。

2.2.4 FSRMの機能

ここでは、FSRM の各機能について説明します。

2.2.4.1 クォータ

2.2.4.1.1. 機能概要

クォータを使用することにより、iStorage NS 上の選択したボリューム、フォルダーに対して領域の使用量を制限、監視することができます。

また、クォータでの領域の使用量の制限には以下の 2 種類の方法が存在します。

- ハードクォータ
  領域の制限に達すると、ユーザーはファイルを保存できなくなります。また、データ量が設定した各しきい値に達すると、通知が行われます。

- ソフトクォータ
  領域の制限に達してもファイルの保存は制限されません。通知が行われるのみとなります。

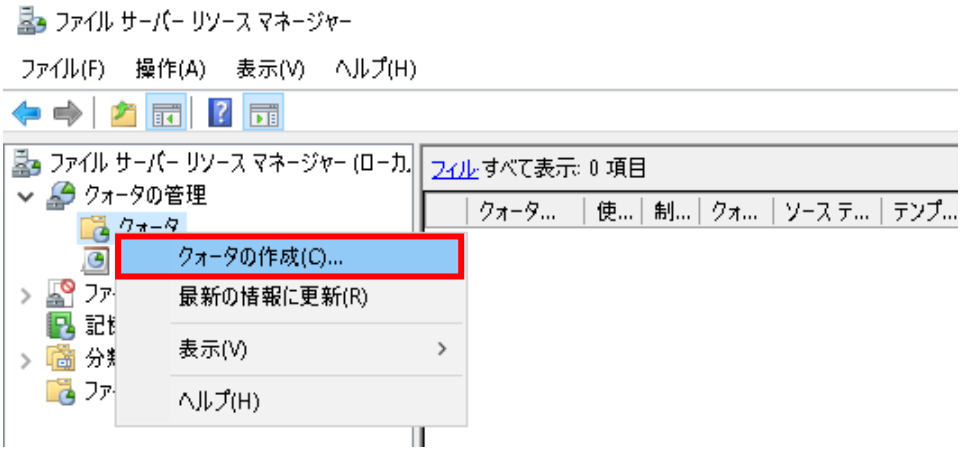
【補足】
一般的に、FSRM のクォータはフォルダー単位での監視を行う際、ディスククォータはユーザー単位での監視を行う際に利用されます。

2.2.4.1.2. 既定のテンプレートからクォータを設定する

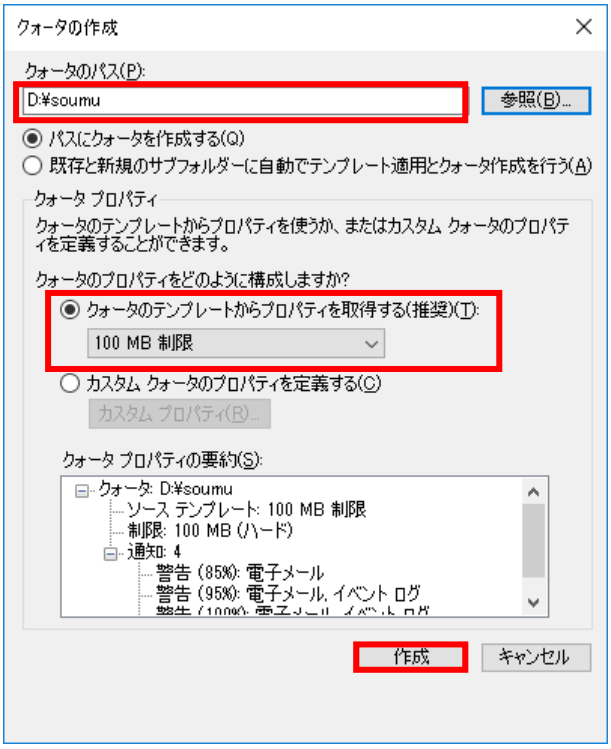
既定のテンプレートを用いてクォータを設定する手順を説明します。既定のテンプレート以外に独自のテンプレートを作成した場合も、既定のテンプレートと同様に選択することができます。独自のテンプレートの作成については本書の【クォータのテンプレートを作成する】を参照してください。

【注意】
「C:¥Windows」などのシステムフォルダーについては、ハードクォータの設定はできません。

1. 管理者メニューから [ファイル サーバー リソース マネージャー] を起動して、[クォータの管理] を展開し、[クォータ] を選択後に右クリックして表示されるメニューから、[クォータの作成] をクリックします。



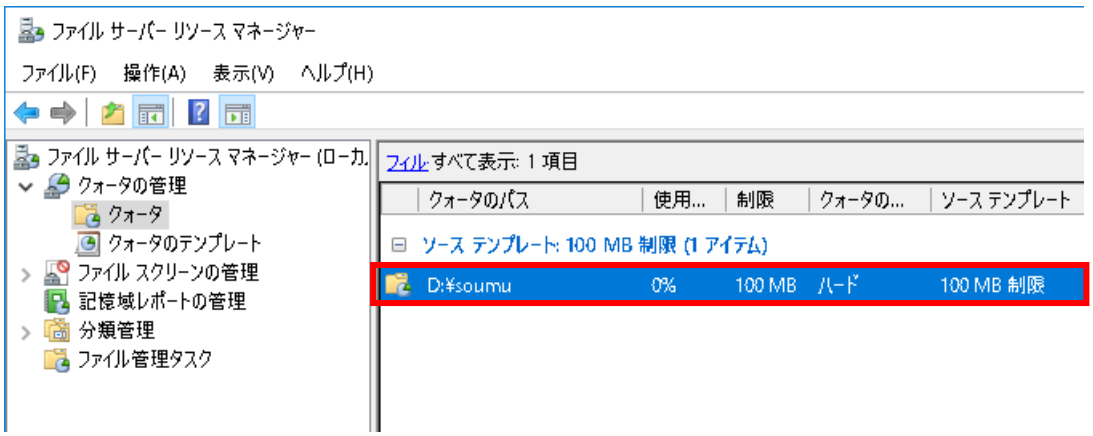
2. [クォータの作成] 画面が表示されますので、クォータを設定する場所のパス、テンプレートを設定し、 [作成] をクリックします。



【補足】

[カスタムクォータのプロパティを定義する] を選択し、[カスタムプロパティ] をクリックすると、テンプレートを利用しないクォータの設定ができます。また、既存のテンプレートの情報をコピーして一部変更して使用することも可能です。

3. 作成されたクォータを確認します。

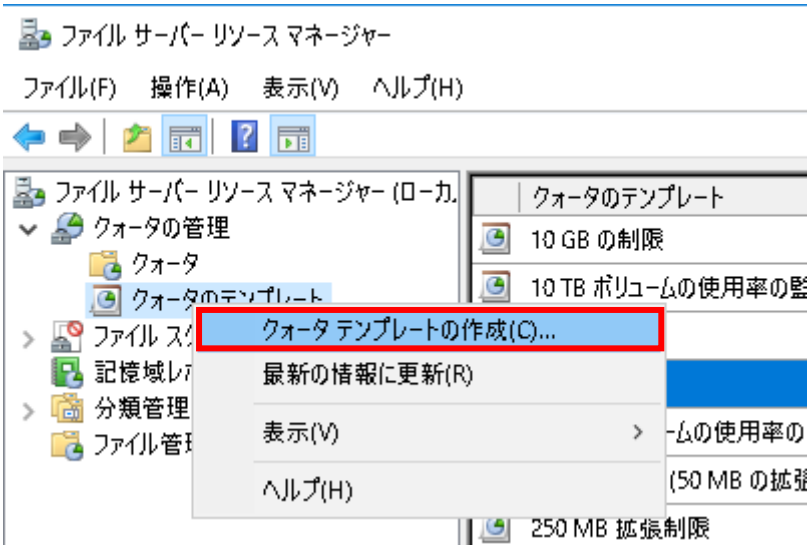


2.2.4.1.3. クォータのテンプレートを作成する

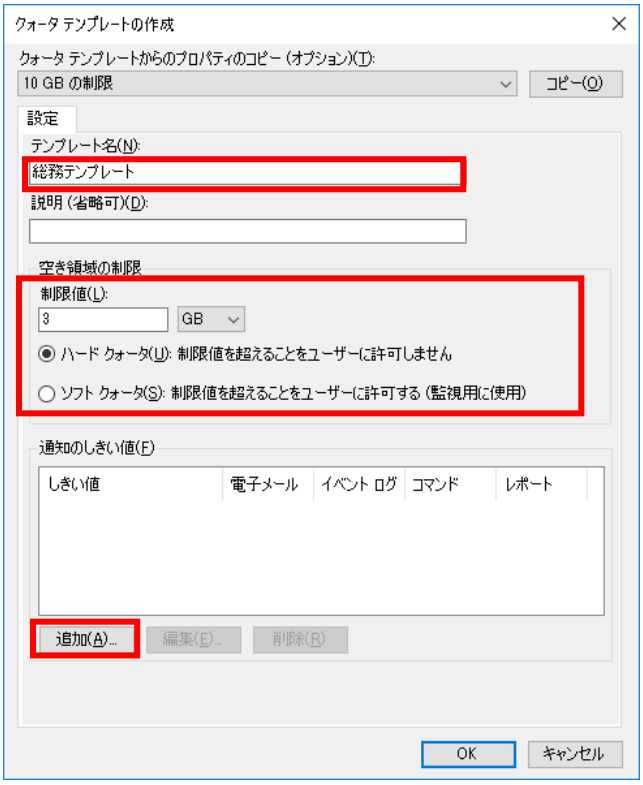
FSRM のクォータ設定で使用できるテンプレートを作成する手順について説明します。テンプレートを作成することで多数のフォルダーに同じ設定を効率的に行うことができます。
ここで作成するテンプレートの設定は以下の通りとします。

項目	設定内容
テンプレート名	総務テンプレート
制限値	3GB
クォータの種類	ハードクォータ
しきい値	使用率が 85%を超えたら、管理者とユーザーに電子メールで通知を行う。 ※ユーザーに電子メールを通知する機能を利用する場合、ドメイン環境に参加する必要があり、Active Directory のユーザー設定に電子メールアドレスを登録する必要があります。

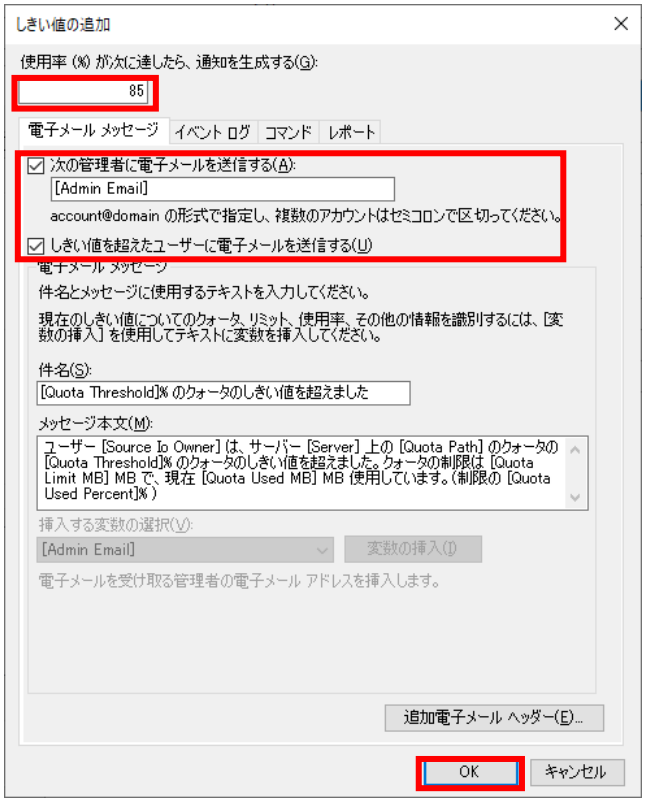
1. 管理者メニューから [ファイル サーバー リソース マネージャー] を起動して、[クォータの管理] を展開し、[クォータのテンプレート] を選択後に右クリックして表示されるメニューから、[クォータ テンプレートの作成] をクリックします。



2. [クォータ テンプレートの作成] 画面が表示されますので、テンプレート名、データ容量の制限値、クォータの種類を設定し [追加] をクリックします。しきい値を設定しない場合は [OK] をクリックして項番 5 へ進みます。

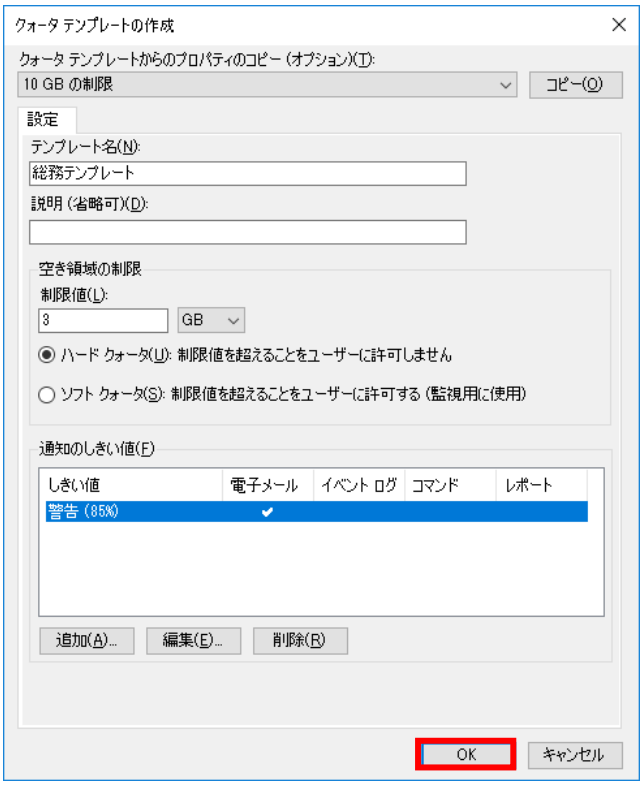


3. [しきい値の追加] 画面が表示されますので、通知を生成する使用率を入力し、[電子メール メッセージ] のタブにて [次の管理者に電子メールを送信する] と [しきい値を超えたユーザーに電子メールを送信する] をチェックして [OK] をクリックします。電子メール以外の通知の方法を利用する場合は、本画面の各タブにて設定を行います。



【補足】
メールの送信先アドレスの初期値となっている [Admin Email] は、本書【電子メール】で設定する [管理者である既定の受信者] となります。

4. 設定内容を確認し、[OK] をクリックします。



5. テンプレートが作成されていることを確認します。

2.2.4.2 ファイルスクリーン

2.2.4.2.1. 機能概要

FSRM のファイルスクリーン機能を使用すると、指定したフォルダーに対しての書き込みを、ファイルの拡張子によって制限、監視することができます。
例えば、業務に関係しない音楽や画像のファイルの書き込みを制限することでディスク容量の消費を抑制したり、実行形式ファイルの書き込みを制限することでウイルス感染などのリスクを抑制することができます。

ファイルスクリーンによる制限には、以下の 2 種類が存在します。

- アクティブスクリーン
  設定した制限に該当するファイルをディスクに保存することはできません。

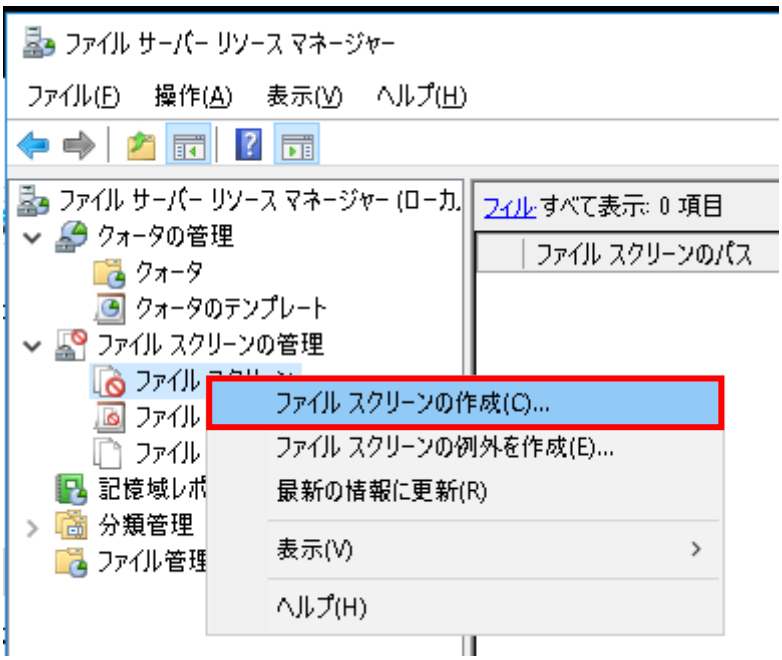
- パッシブスクリーン
  設定した制限に該当するファイルの書き込みについて、監視のみが行われ保存は制限されません。

2.2.4.2.2. 既定のテンプレートからファイルスクリーンを設定する

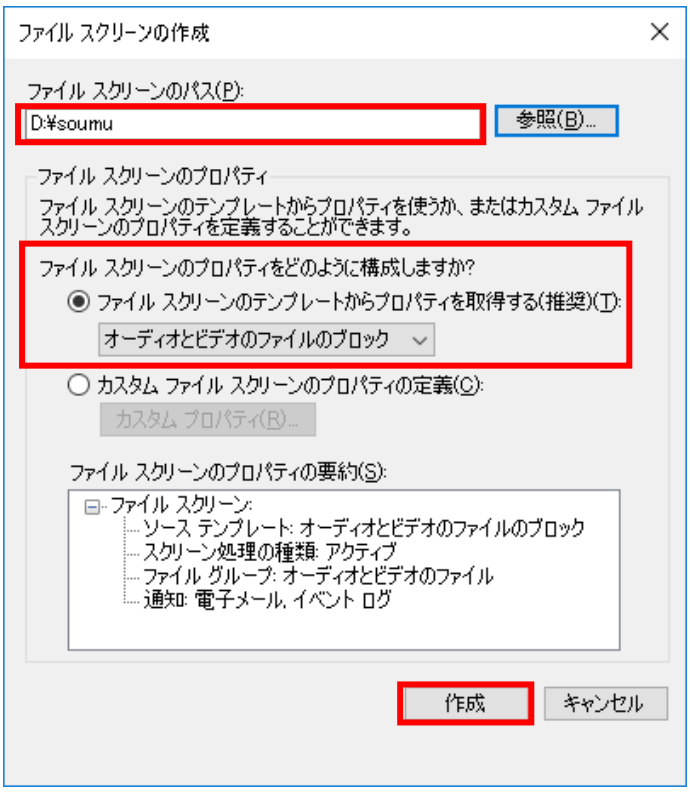
既定のテンプレートを用いて、ファイルスクリーンを設定する手順を説明します。既定のテンプレート以外に独自のテンプレートを作成した場合も、既定のテンプレートと同様に選択することができます。独自のテンプレートの作成については本書の【ファイルスクリーンのテンプレートを作成する】を参照してください。

> 【注意】
> アクティブスクリーンを「C:¥」や「C:¥Windows 」に設定することはできません。

1. 管理者メニューから [ファイル サーバー リソース マネージャー] を起動して、[ファイルスクリーンの管理] を展開し、[ファイルスクリーン] を選択後に右クリックして表示されるメニューから、[ファイルスクリーンの作成] を選択します。



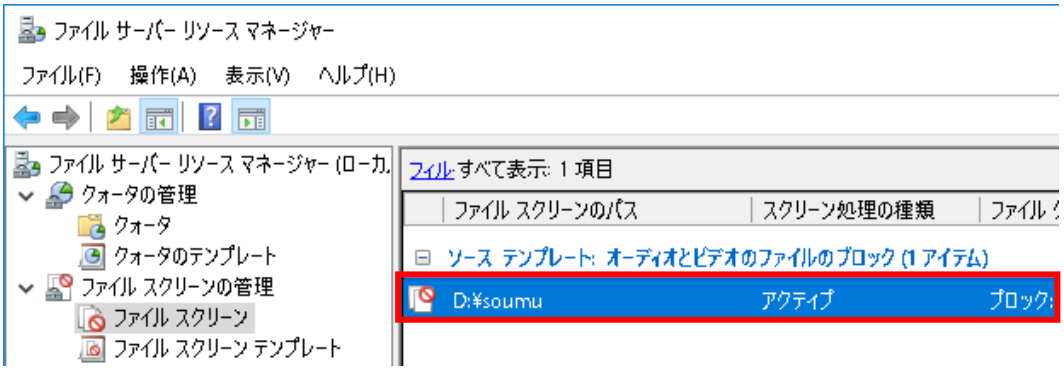
2. [ファイルスクリーンの作成] 画面が表示されますので、ファイルスクリーンを設定する場所のパス、テンプレートを設定し、 [作成] をクリックします。



【補足】

[カスタムファイルスクリーンのプロパティの定義] を選択し、[カスタムプロパティ] をクリックすると、テンプレートを利用しないファイルスクリーンの設定ができます。また、既存のテンプレートの情報をコピーして一部変更して使用することも可能です。

3. 作成されたファイルスクリーンを確認します。

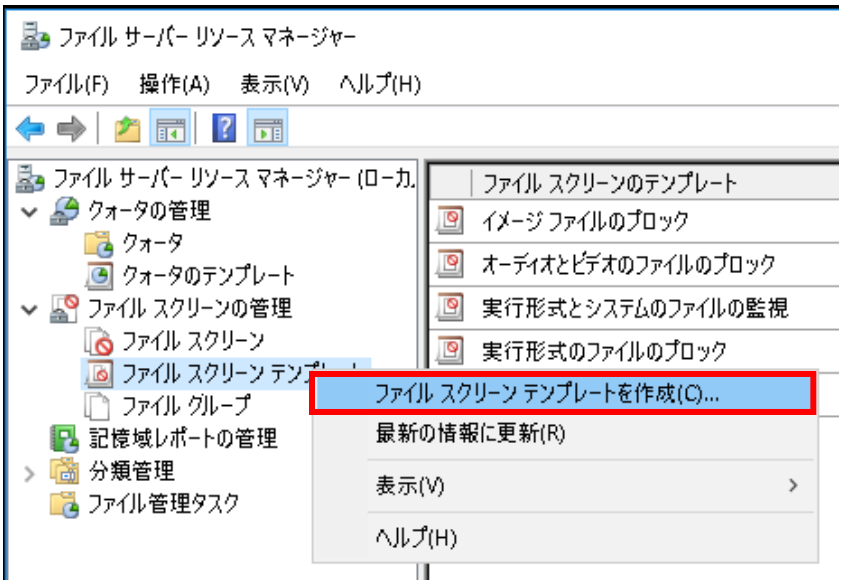


2.2.4.2.3. ファイルスクリーンのテンプレートを作成する

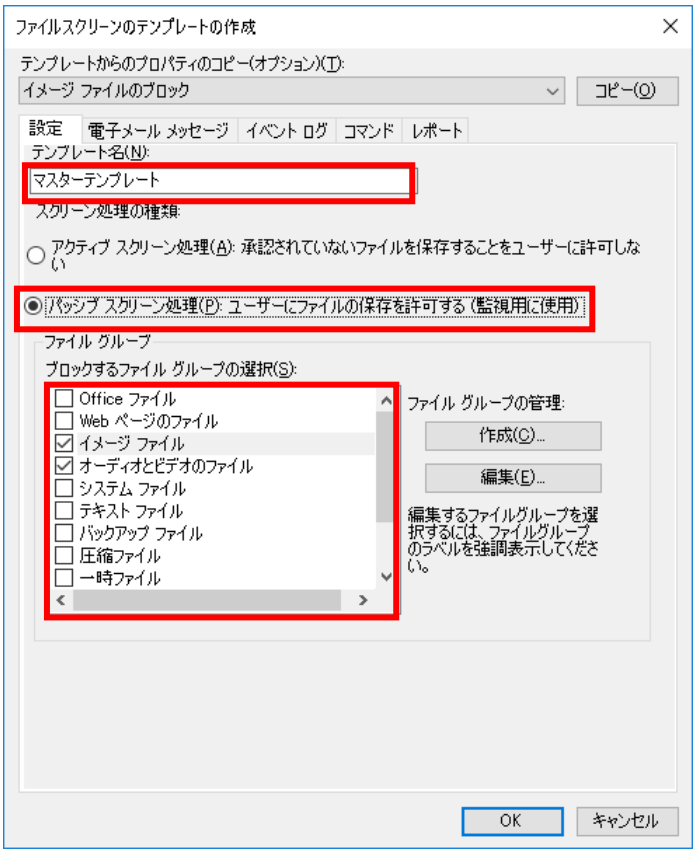
FSRM のファイルスクリーン設定で使用できるテンプレートを作成する手順について説明します。テンプレートを作成することで多数のフォルダーに同じ設定を効率的に行うことができます。
ここで作成するテンプレートの設定は以下の通りとします。

項目	設定内容
テンプレート名	マスターテンプレート
ファイルスクリーンの種類	パッシブスクリーン
ブロックするファイルグループ	イメージファイル、オーディオとビデオのファイル
通知方法	管理者とユーザーに電子メールで通知を行う。 ※ユーザーに電子メールを通知する機能を利用する場合、ドメイン環境に参加する必要があり、Active Directory のユーザー設定に電子メールアドレスを登録する必要があります。

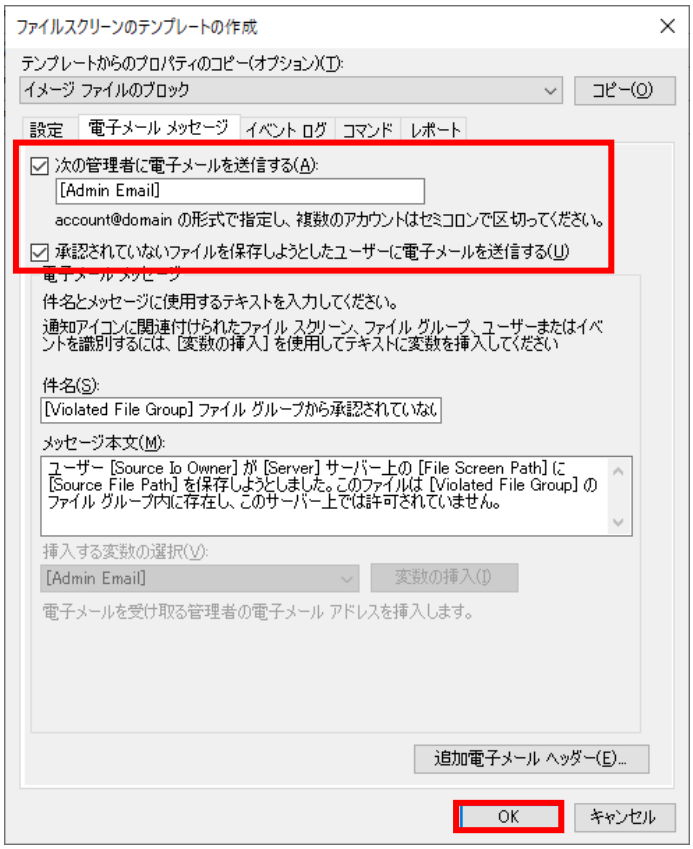
1. 管理者メニューから [ファイル サーバー リソース マネージャー] を起動して、[ファイル スクリーンの管理] を展開し、[ファイル スクリーン テンプレート] を選択後に右クリックして表示されるメニューから、[ファイル スクリーン テンプレートを作成] をクリックします。



2. [ファイルスクリーンのテンプレートの作成] 画面が表示されますので、テンプレート名、スクリーン処理の種類、ブロックするファイルグループを設定し、 [電子メールメッセージ] タブをクリックします。通知方法を設定しない場合は [OK] をクリックして項番 4 へ進みます。

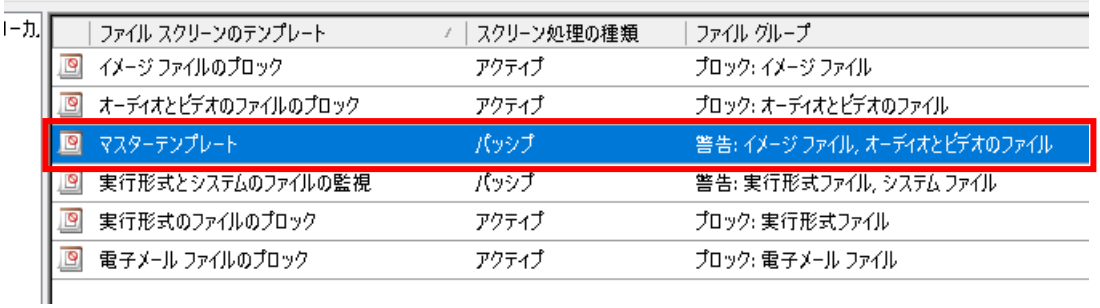


3. [次の管理者に電子メールを送信する] と [承認されていないファイルを保存しようとしたユーザーに電子メールを送信する] をチェックして [OK] をクリックします。電子メール以外の通知の方法を利用する場合は、本画面の各タブにて設定を行います。



【補足】
メールの送信先アドレスの初期値となっている [Admin Email] は、本書【電子メール】で設定した [管理者である既定の受信者] となります。

4. テンプレートが作成されていることを確認します。



2.2.4.3 記憶域レポート

2.2.4.3.1. 機能概要

FSRM の記憶域レポートは、ディスク使用状況をレポート化します。スケジュールを設定して自動的にレポートの作成を行うことや、作成したレポートをサーバー管理者にメールで送信することもできます。

記憶域レポートでは、ディスクの使用状況について以下のような内容のレポートを作成することができます。

レポート	説　　明
クォータの使用率	ディスク領域の利用状況が指定した割合を超えたクォータの一覧を表示します。このレポートを使って、クォータがまもなく制限を超えるかを効率的に判断して、適切な対処を行うことができます。
ファイルグループごとのファイル	ファイル拡張子を基に設定したファイルグループごとにファイルを一覧表示します。このレポートを使うと、ファイルグループの使用状況パターンを監視し、大量のディスク領域を占めているファイルグループを効率的に判断できます。これは、サーバーでどのようなファイルスクリーン処理ポリシーを構成するかを決定する場合に役立ちます。
ファイルスクリーン処理の監査	指定した期間におけるサーバー上のファイルスクリーン処理の監査のイベントを一覧表示します。このレポートを使って、スクリーン処理ポリシーに違反しているアプリケーションやユーザーを効率的に判断することができます。
プロパティごとのファイル	特定の分類プロパティを持つファイルの一覧を表示します。このレポートを使って、ファイルの分類状況がわかります。
プロパティ別フォルダー	セキュリティで保護されている特定の分類プロパティの値毎にフォルダーを一覧表示します。このレポートを使って、フォルダーの分類状況がわかります。
大きいサイズのファイル	指定したサイズ以上のファイル一覧を表示します。このレポートを使ってサーバー上で最も多くのディスク領域を消費しているファイルを効率的に判断できます。これは、ディスクに空き領域を確保するのに役立ちます。
所有者ごとのファイル	ファイルの所有ユーザー毎にファイルを一覧表示します。このレポートを使って、大量のディスク領域を使用しているユーザーを効率的に判断することができます。

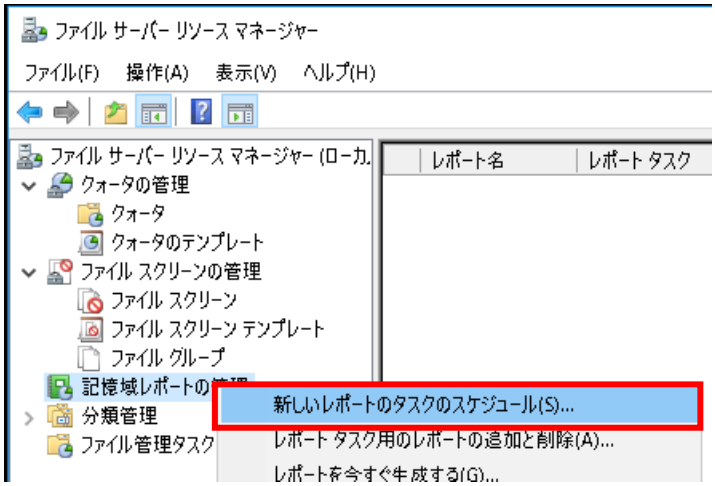
レポート	説　　明
最近アクセスされていないファイル	最近アクセスされていないファイルを一覧表示します。このレポートを使用して、削除またはアーカイブのどちらかが可能な古いファイルを効率的に特定できます。これはディスク領域の使われていない領域を空けるのに役立ちます。注意：サーバーによって最終アクセス時刻が管理されていない場合、このレポートは正しくない可能性があります。iStorage NS シリーズのデフォルト設定では、性能を優先するため最終アクセス時刻は管理していません。最終アクセス時刻を管理するように設定変更する場合は、【管理者ガイド（概要編）FAQ】の「ファイルのアクセス日時が更新されるようにする方法を教えてください。」を参照してください。
最近アクセスしたファイル	最近アクセスしたファイルを一覧表示します。このレポートを使用して、頻繁に使用されるデータ（常に使用可能にしておく必要があるデータ）を特定できます。注意：サーバーによって最終アクセス時刻が管理されていない場合、このレポートは正しくない可能性があります。iStorage NS シリーズのデフォルト設定では、性能を優先するため最終アクセス時刻は管理していません。最終アクセス時刻を管理するように設定変更する場合は、【管理者ガイド（概要編）FAQ】の「ファイルのアクセス日時が更新されるようにする方法を教えてください。」を参照してください。
重複しているファイル	重複していると思われる (名前、サイズ、最終更新日時が同じ) ファイルの一覧の作成。このレポートを使って、重複により無駄となっているディスク領域を効率的に判断し、空き領域を確保することができます。

【注意】
「プロパティごとのファイル」および「プロパティ別フォルダー」について、記憶域レポートの出力を指定した際は、それぞれに対して「パラメーターの編集」ボタンを押下し、「パラメーターのレポート設定」を指定する必要があります。

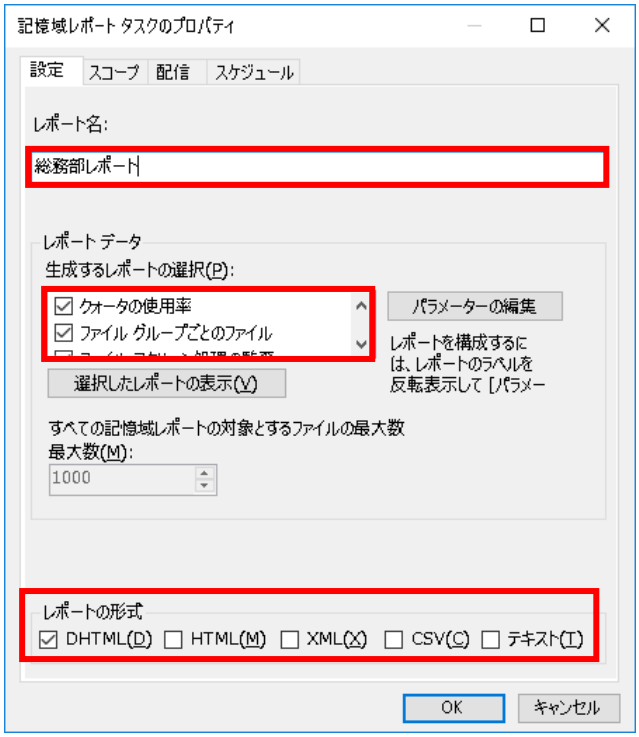
2.2.4.3.2. 記憶域レポートを設定する

ここでは、記憶域レポートを定期的に作成するためのスケジュールを設定する手順について説明します。

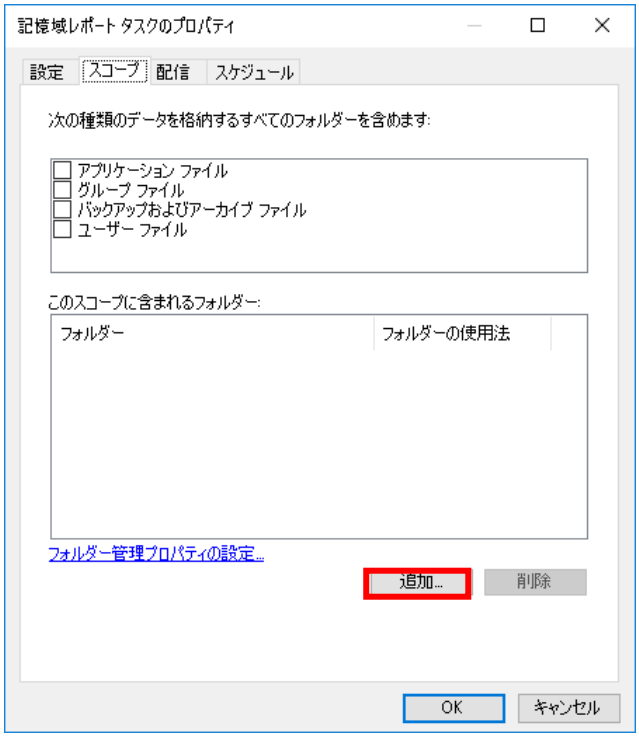
1. 管理者メニューから [ファイル サーバー リソース マネージャー] を起動して、[記憶域レポートの管理] を右クリックし、[新しいレポートのタスクのスケジュール] を選択します。



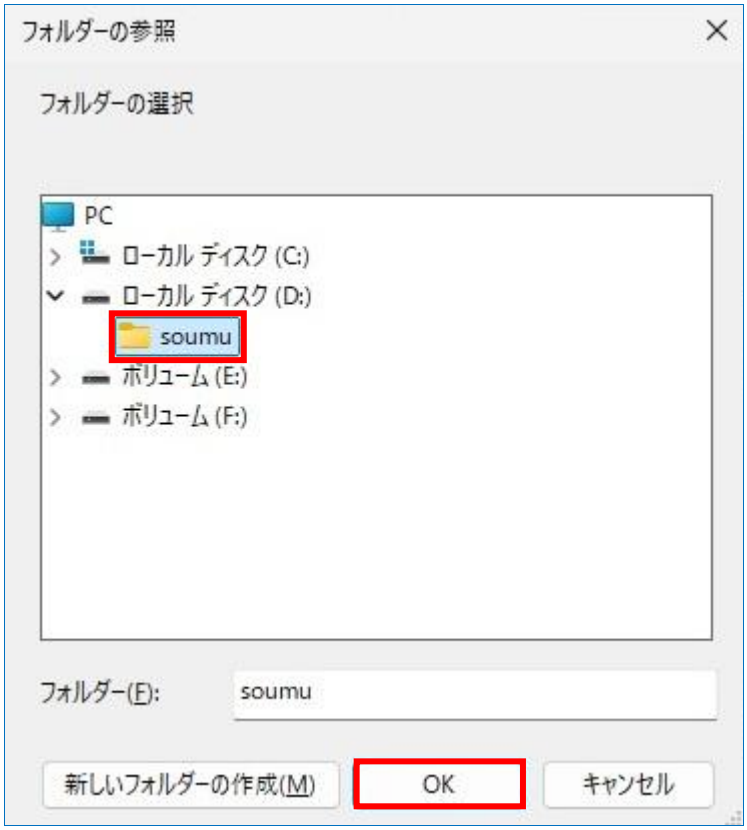
2. [記憶域レポート タスクのプロパティ] 画面で、レポート名と生成するレポートの種類、レポートの出力形式を設定し、[スコープ] タブに移動します。



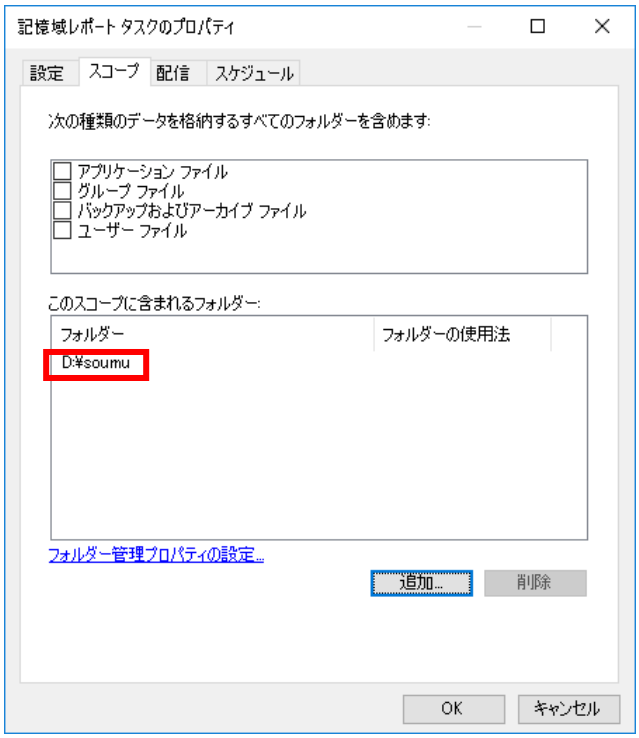
3. [追加] をクリックします。



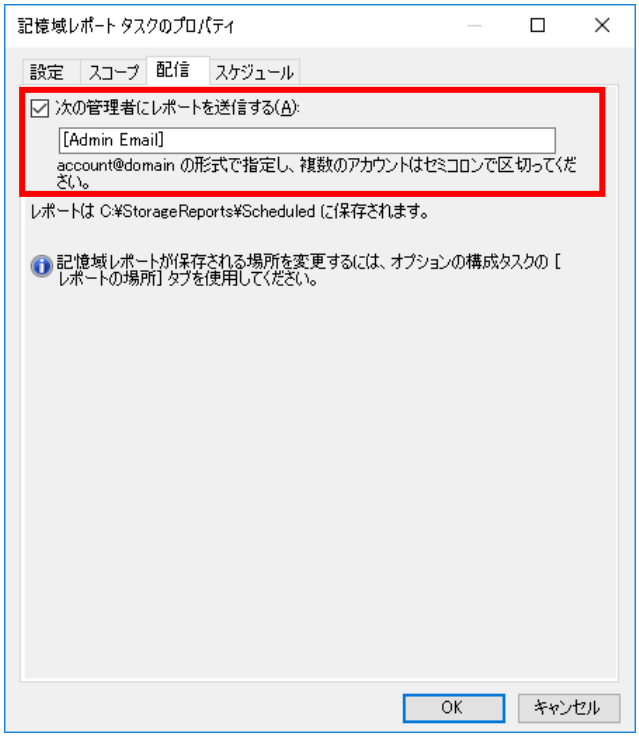
4. 分析の対象となるフォルダーを選択し、[OK] をクリックします。



5. 設定したフォルダーが [このスコープに含まれるフォルダー] に追加されていることを確認して、[配信] タブに移動します。記憶域レポートのメールでの送信を行わない場合は、[スケジュール] タブをクリックして、項番 7 に進みます。



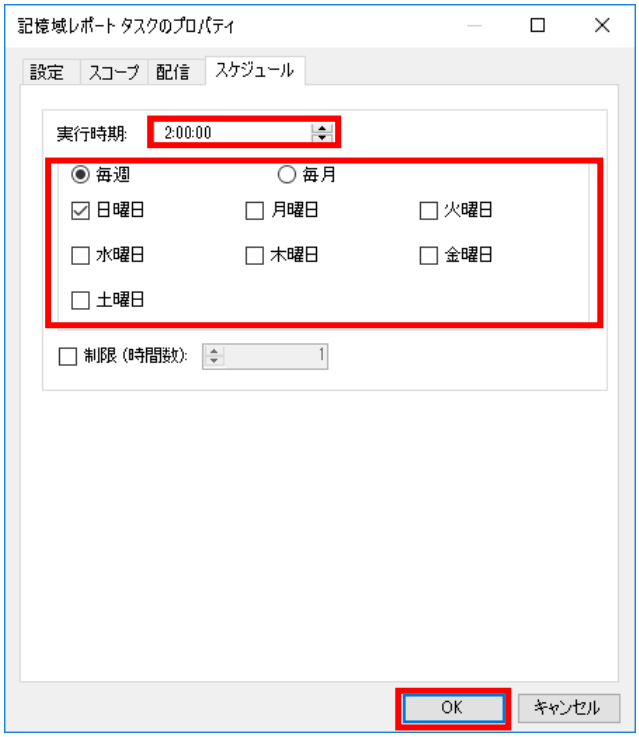
6. [次の管理者にレポートを送信する] をチェックして、[スケジュール] タブに移動します。



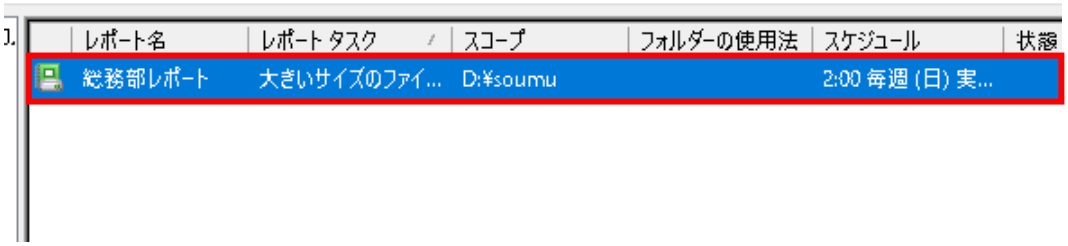
【補足】

メールの送信先アドレスの初期値となっている [Admin Email] は、本書【電子メール】で設定する [管理者である既定の受信者] となります。

7. [実行時期] にてスケジュールを設定して、[OK] をクリックします。



8. 記憶域レポートの設定が行われていることを確認します。



2.2.4.4　ファイル分類インフラストラクチャ（FCI）

2.2.4.4.1. 機能概要

FCI は、ファイル中に含まれる文字列や、ファイルの属性でファイルを分類し、その分類に基づいてタスク (格納フォルダーの移動、またはカスタムタスク) を実行する機能です。FCI は、「分類管理」と「ファイル管理タスク」という２つの機能で構成されており、それぞれの内容は以下の通りとなります。

1）　分類管理

- ローカル分類プロパティを作成する
- 値を付与する
  - 手動で付与する
  - 分類規則によって付与する

    規則を作成する

    分類処理をスケジュール（実行）する

2）　ファイル管理タスク

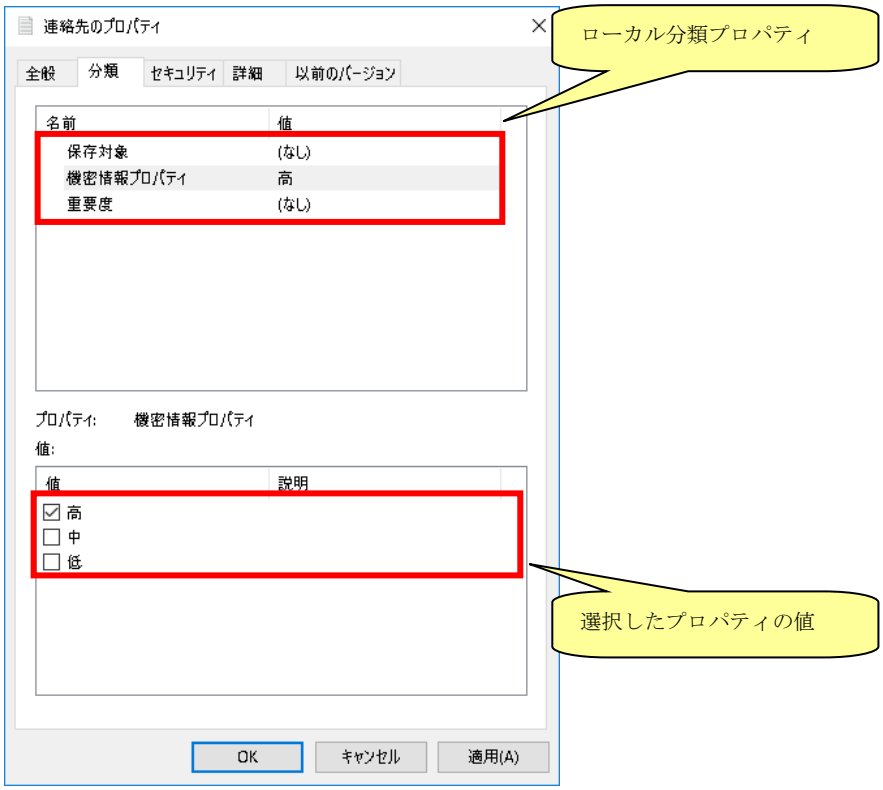
- ファイル管理タスクで処理する

  対象はカスタムプロパティや標準プロパティ

●ローカル分類プロパティを作成する

FSRM 分類管理の GUI から、独自のプロパティを作成することができます。

作成したローカル分類プロパティはファイルのプロパティからも確認することができます。



●値を付与する

ローカル分類プロパティに対して値を付与することができます。

ファイルのプロパティから直接付与する方法と、指定したフォルダー配下のファイルを対象としてユーザーにて分類規則を作成した後、規則による分類をスケジューリングすることで自動的に値を付与する方法があります。

●ファイル管理タスクで処理する

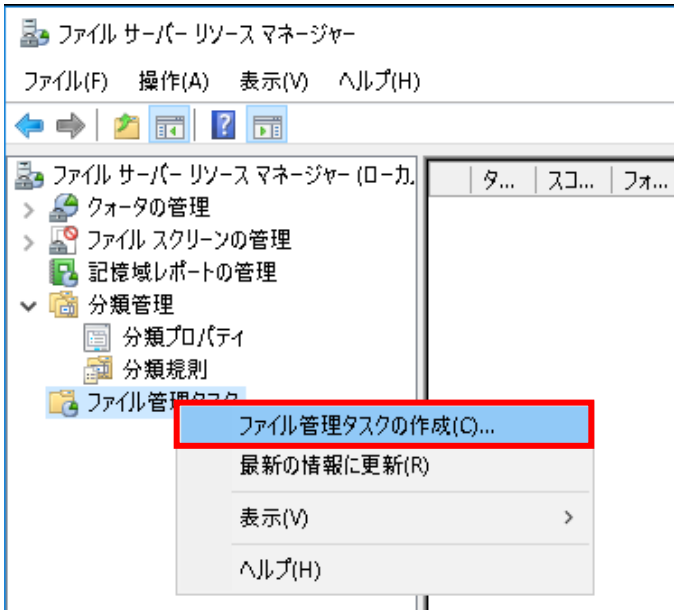
指定したフォルダー配下のファイルを対象として、標準プロパティ（ファイルの作成・更新・アクセス日時）や、ローカル分類プロパティに基づいて、指定したタスクを実行することができます。

2.2.4.4.2. 標準プロパティを利用してファイル管理タスクを実行する

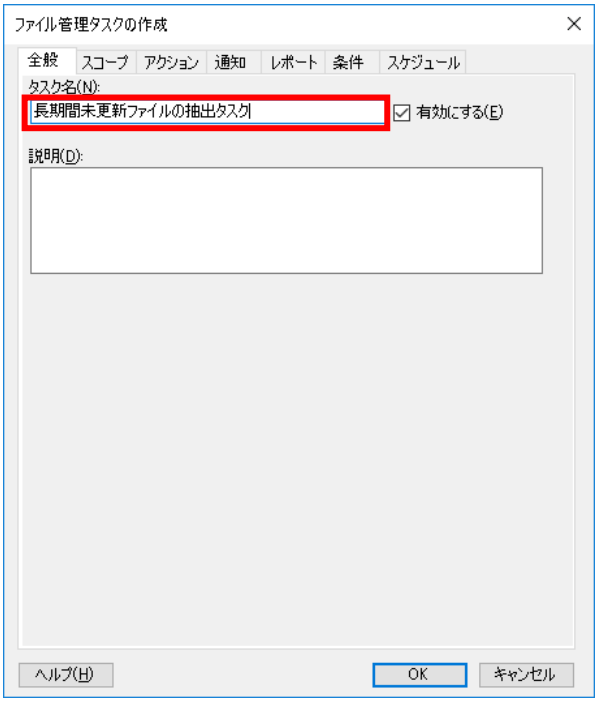
ここでは、1 年以上未更新のファイルを別のフォルダーに移動させる、という標準プロパティを利用したファイル管理タスクの実行方法を説明します。
具体的な設定内容は以下の通りとします。

項目	設定内容
タスク名	長期間未更新ファイルの抽出タスク
タスク実行対象フォルダー	D:¥soumu
アクション	D:¥古いファイルフォルダー への移動
プロパティの条件	最終更新から 365 日以上経過している
スケジュール	毎月 1 日の 4:00

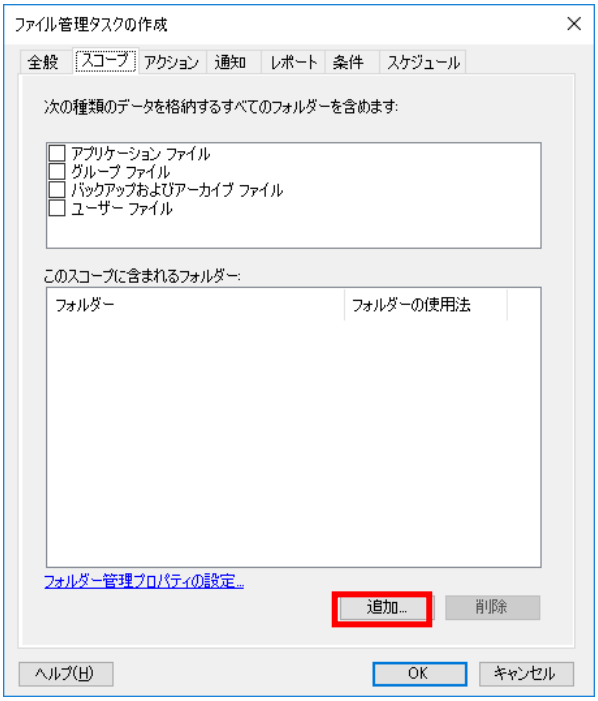
1. 管理者メニューから [ファイル サーバー リソース マネージャー] を起動して、ファイルサーバーリソースマネージャー（ローカル）を展開して、[ファイル管理タスク] を右クリックし、[ファイル管理タスクの作成] をクリックします。



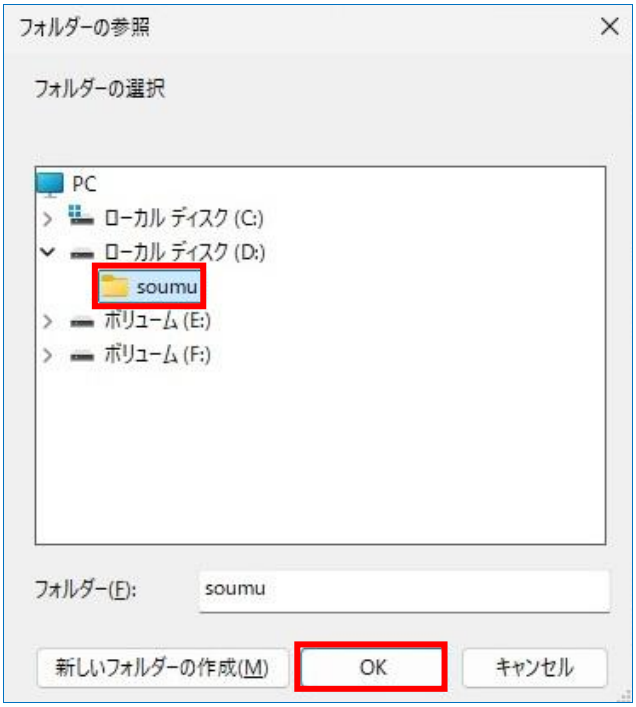
2. タスク名を入力して、[スコープ] タブに移動します。



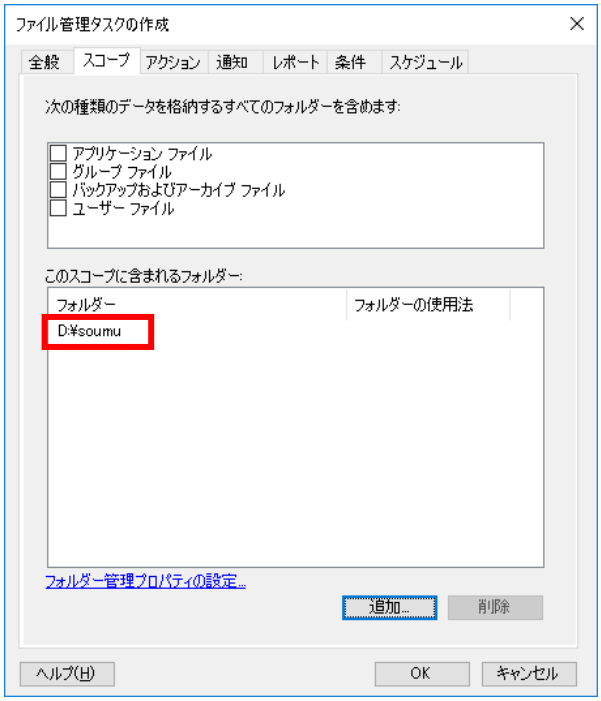
3. [追加] をクリックします。



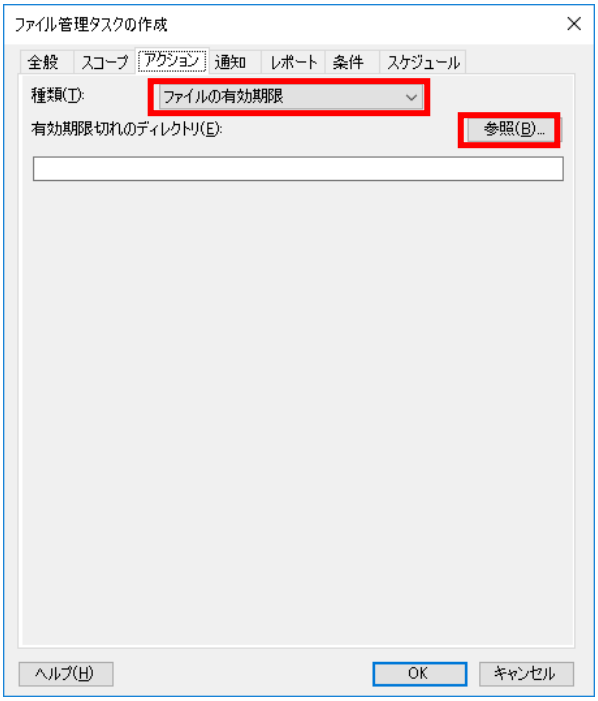
4. タスク実行対象のフォルダーを選択して、[OK] をクリックします。



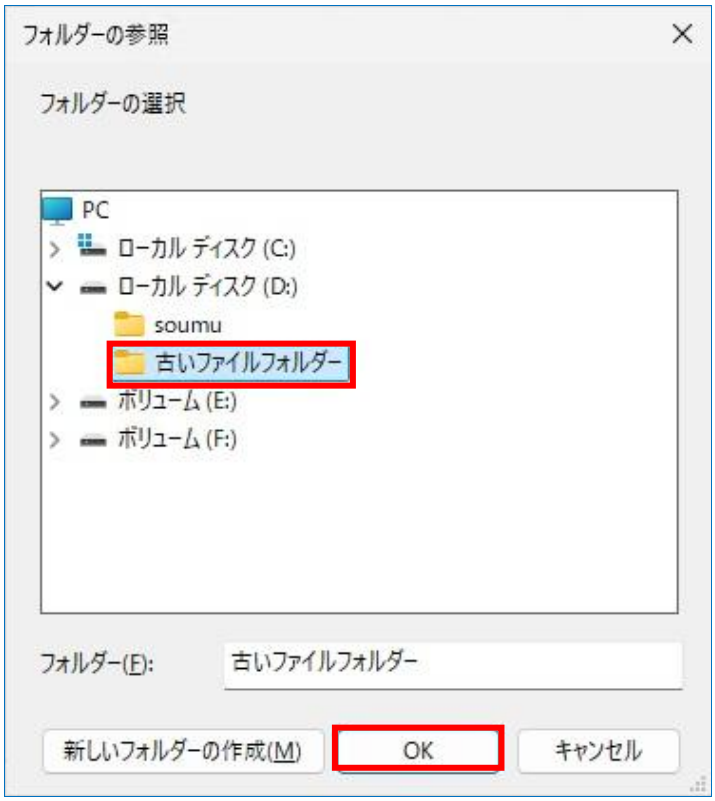
5. フォルダーが追加されたことを確認して、[アクション] タブに移動します。



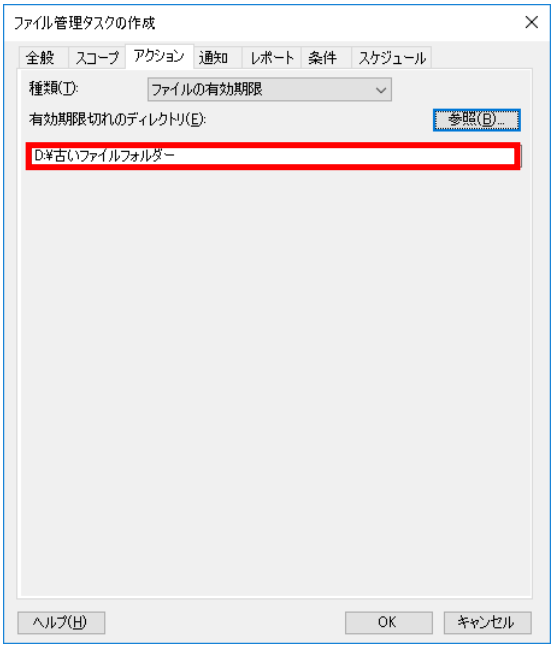
6. [ファイルの有効期限] を選択して、[参照] をクリックします。



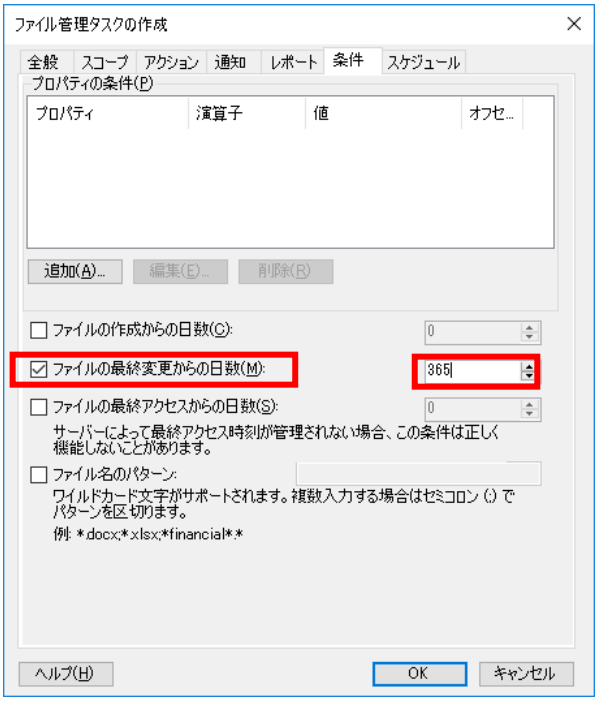
7. 移動先のフォルダーを選択して、[OK] をクリックします。



8. フォルダーが選択されたことを確認して、[条件] タブに移動します。

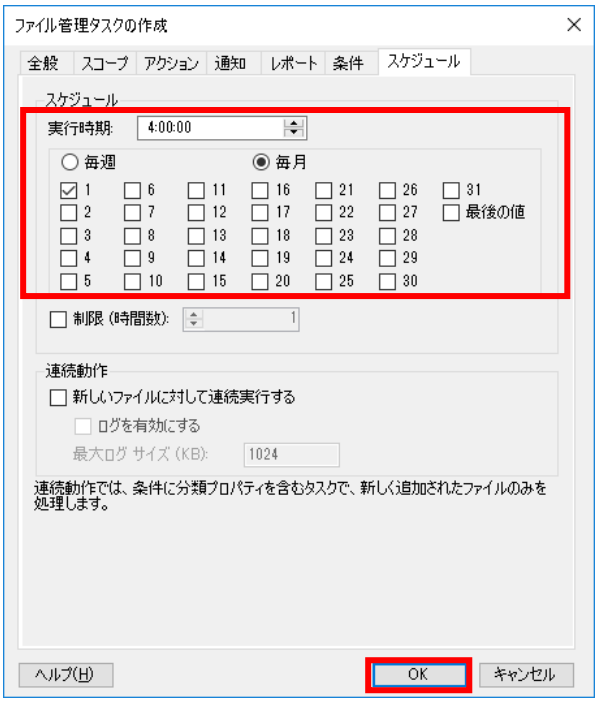


9. [ファイルの最終更新からの日数] をチェックして”365”を入力し、[スケジュール] タブに移動します。ファイル作成からの日数や、最終アクセス日からの日数など、他の標準プロパティでの条件を設定する場合は本画面で、カスタムプロパティを用いての設定を行う場合は、[追加] をクリックして設定を行います。

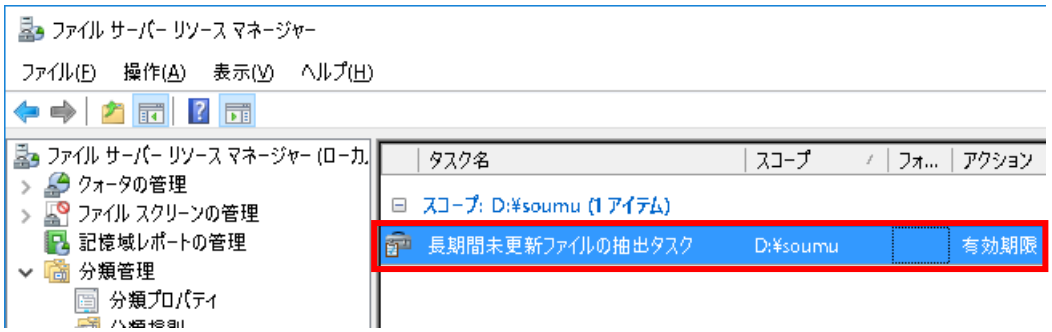


【補足】
サーバーによって最終アクセス時刻が管理されていない場合、[ファイルの最終アクセスからの日数]の標準レポートは正しく動作しない可能性があります。iStorage NS シリーズのデフォルト設定では、性能を優先するため最終アクセス時刻は管理していません。最終アクセス時刻を管理するように設定変更する場合は、【管理者ガイド（概要編）FAQ】の「ファイルのアクセス日時が更新されるようにする方法を教えてください。」を参照してください。

10. スケジュールを設定し、[OK] をクリックします。



11. 管理タスクが作成されていることを確認します。



2.2.5 注意事項

通知機能の注意事項

- “SMTP サーバー名または IP アドレス” に設定するメールサーバーについては、SMTP 認証機能を有していないメールサーバーを指定してください。
- “差出人”電子メールアドレスは、ご利用のメールサーバーの仕様として制限がなければ、メールアカウントとして存在しない任意の値が設定可能ですが、メールアドレスの形式（「任意の文字@任意の文字.任意の文字」）である必要があります。また、”¥”のようなメールアドレスに使用できない記号は使用できません。
- 記憶域レポートを電子メールで通知する場合においても「C:¥StorageReports」（デフォルト設定）配下の記憶域レポートは削除されませんので、お客様にて管理いただく必要があります。

クォータ機能の注意事項

- クォータ機能は NTFS のみサポートとなります。
- 「データ重複除去（Data Deduplication）」を利用している場合は、クォータ機能が正しくファイルのサイズを計算しない場合があります。
- 「C:¥Windows」などのシステムフォルダーについては、ハードクォータの設定はできません。
- クォータ機能のしきい値設定の [電子メール メッセージ] タブおよび [レポート] タブにおいて、「しきい値を超えたユーザーに電子メール(レポート)を送信する」機能を利用する場合、ドメイン環境に参加する必要があり、Active Directory のユーザー設定に電子メールアドレスを登録する必要があります。

ファイルスクリーン機能の注意事項

- アクティブスクリーンを「C:¥」や「C:¥Windows 」に設定することはできません。
- ファイルスクリーン機能の [電子メール メッセージ] タブおよび [レポート] タブにおいて、「承認されていないファイルを保存しようとしたユーザーに電子メール(レポート)を送信する」機能を利用する場合、ドメイン環境に参加する必要があり、Active Directory のユーザー設定に電子メールアドレスを登録する必要があります。

記憶域レポート機能の注意事項

- 「プロパティごとのファイル」および「プロパティ別フォルダー」について、記憶域レポートの出力を指定した際は、それぞれに対して「パラメーターの編集」ボタンを押下し、「パラメーターのレポート設定」を指定する必要があります。

ファイルの分類管理の注意事項

- スケジュールは、サーバーの負荷が小さい時間帯にタスクが実行されるように設定してください。
- カスタムプロパティを付加することができるのはNTFSにてフォーマットされたボリューム上のファイルのみとなります。
- 既定の動作では、一度分類処理が行われたファイルは、同じ分類規則で再度分類されることはありません。再分類が必要な場合は、分類規則を作成する際に [評価の種類] タブで、「既存のプロパティ値を再評価する」をチェックします。
- コンテンツ分類子でファイルの内容を検索可能なファイルの種類は IFilter の有無に依存します。あらかじめ対応する IFilter がインストールされていない拡張子のファイルを分類対象とするためには、別途その拡張子に対応した Microsoft IFilter のインストールが必要となります。

2.3 ディスククォータ

2.3.1 機能概要

ディスククォータを使用することにより、iStorage NS 上で選択したボリュームに対して、ユーザー単位で領域の使用量を制限、監視することができます。

また、クォータでの領域の使用量の制限には以下の 2 種類の方法が存在します。

- ハードクォータ
  領域の制限に達すると、ユーザーはファイルを保存できなくなります。また、データ量が設定した値に達すると、通知が行われます。

- ソフトクォータ
  領域の制限に達してもファイルの保存は制限されません。通知が行われるのみとなります。

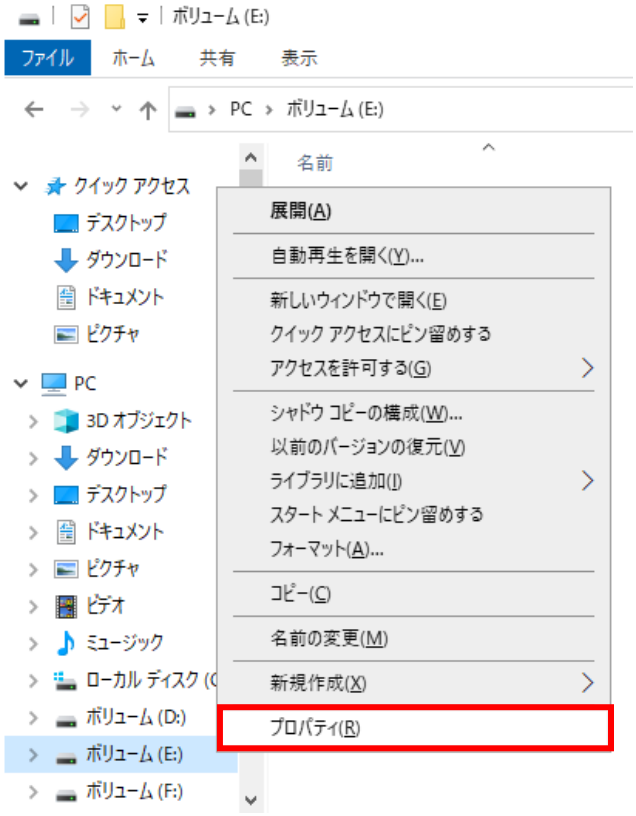
【補足】
一般的に、FSRM のクォータはフォルダー単位での監視を行う際、ディスククォータはユーザー単位での監視を行う際に利用されます。

2.3.2 設定手順

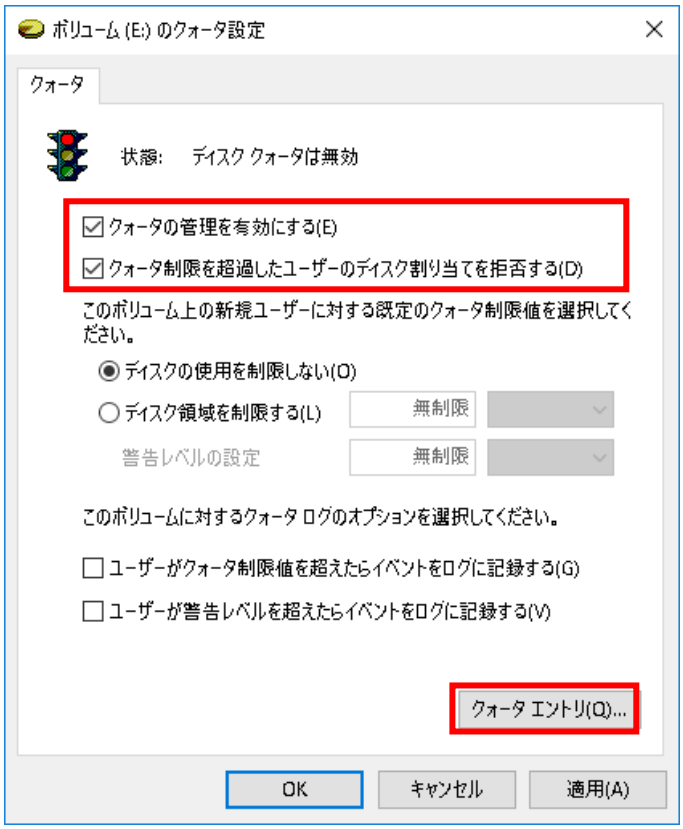
ここでは、ディスククォータを設定してボリューム毎にユーザー単位でディスク使用量を制限（ハードクォータ）する手順について説明します。

1. 管理者メニューから [エクスプローラー] を起動します。

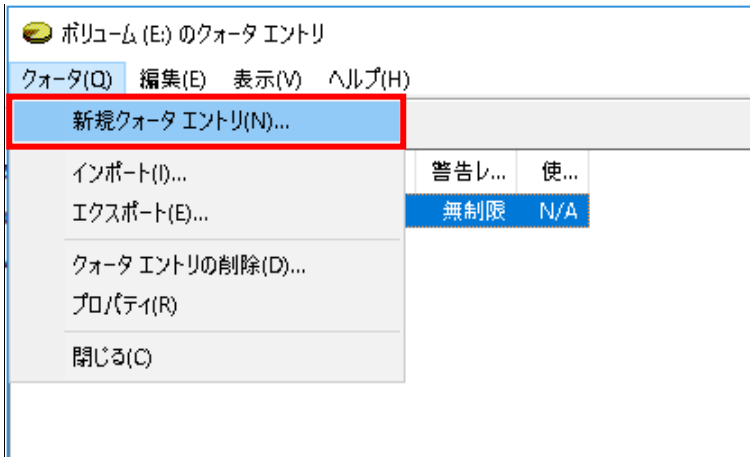
2. 対象ボリュームを右クリックし、[プロパティ] を選択します。



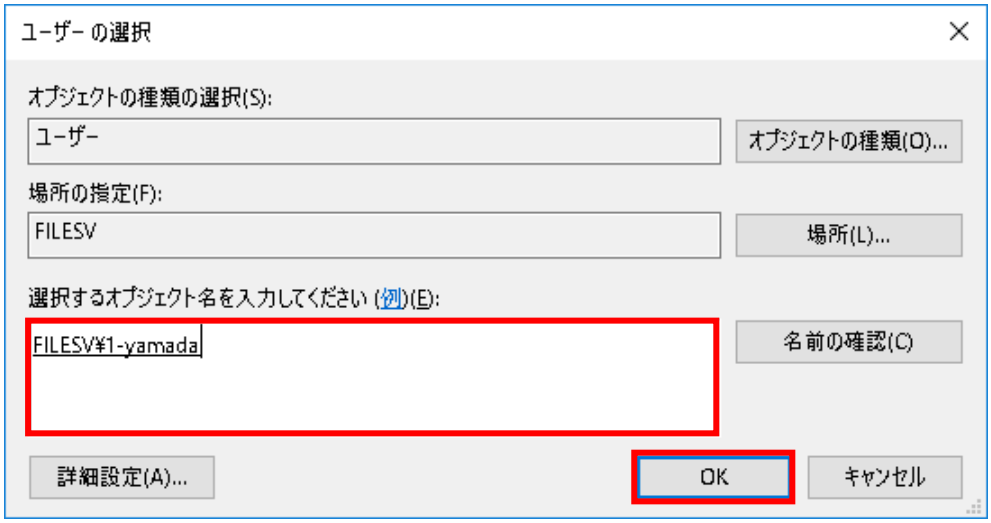
3. プロパティ画面で [クォータ] タブを開いて [クォータの管理を有効にする] をチェック後、[クォータ制限を超過したユーザーのディスク割り当てを拒否する] をチェックし、[クォータエントリ...] をクリックします。ユーザー毎ではなく一括で設定を行う場合は、[ディスク領域を制限する]、[警告レベルの設定] に適切な値を入力し [OK] をクリックして終了します。



4. [クォータエントリ] 画面にて、[クォータ] – [新規クォータエントリ] をクリックします。

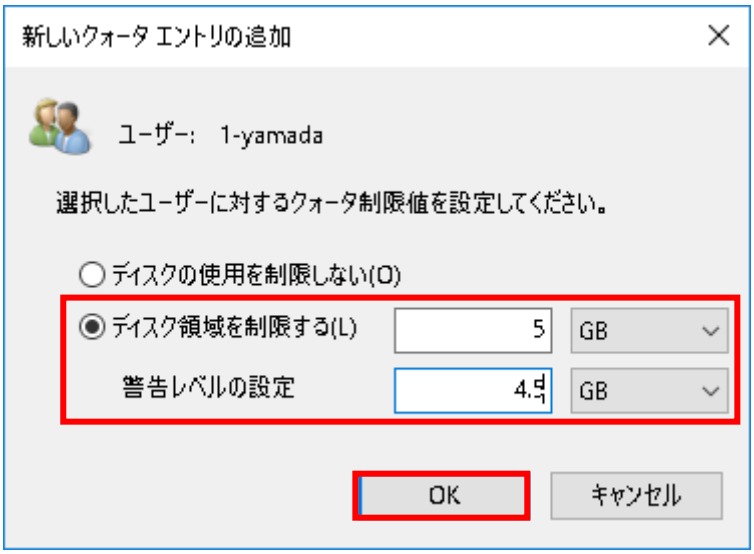


5. [選択するオブジェクト名を入力してください] に制限を行うユーザー名を入力して、[名前の確認] をクリックします。その後、[OK] をクリックします。

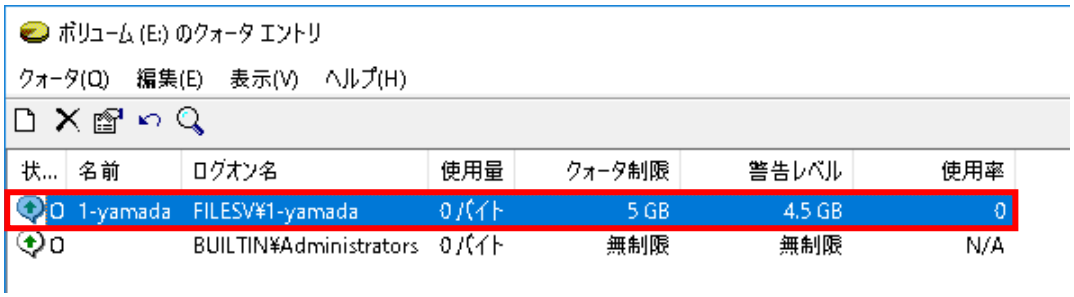


【補足】
[詳細設定] をクリックすると、ユーザー名を検索して選択指定することができます。

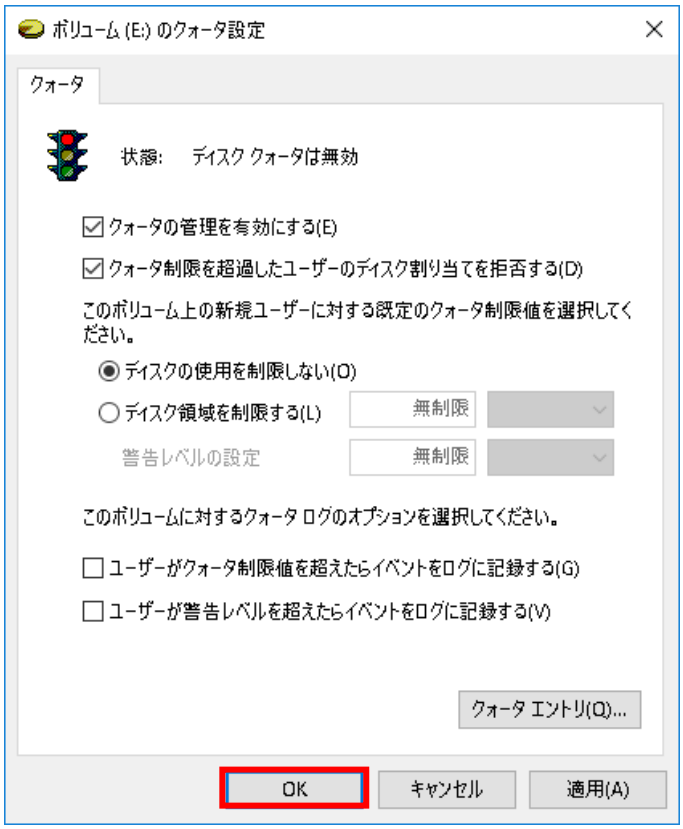
6. ユーザーに適用する制限を入力し、[OK] をクリックします。



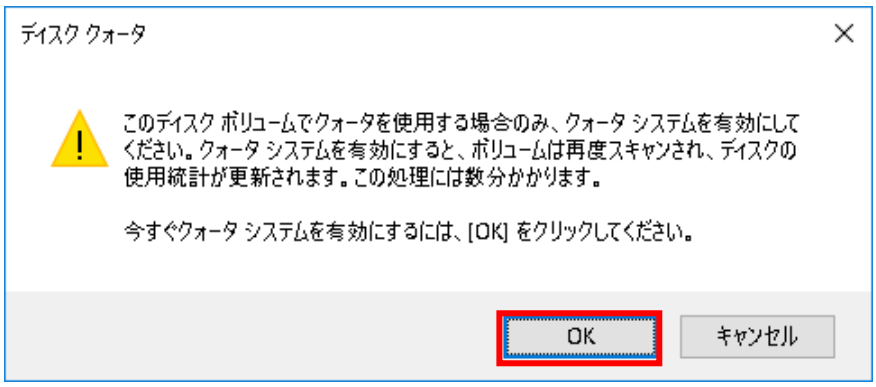
7. クォータエントリが追加されていることを確認し、メニューの [クォータ] – [閉じる] をクリックします。



8. [OK] をクリックします。



9. 以下の画面が表示された場合は、[OK] をクリックします。



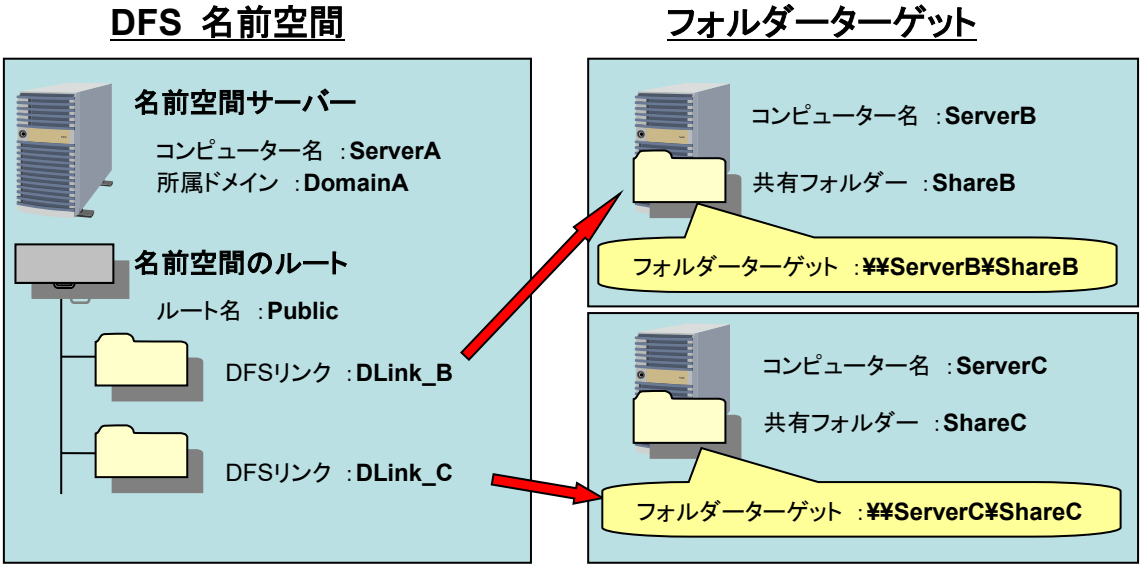
2.4 複数サーバーの共有フォルダーを統合する (DFS)

システム管理者が分散ファイルシステム (DFS : Distributed File System) を使用すると、ネットワーク上に物理的に分散しているファイルサーバーへのアクセスと、それらの共有フォルダーの管理を仮想的に統合した環境としてユーザーに提供できます。複数のサーバーに分散しているファイルが、ネットワーク上の 1 つの場所に配置されているように見えます。ユーザーは、ファイルの物理的な場所を指定しなくても、目的のファイルにアクセスできます。

2.4.1 DFS 名前空間

2.4.1.1 DFS 名前空間の機能概要

DFS 名前空間により、散在するファイルサーバーを統一された名前空間の配下にまとめることができます。代表となるサーバーのフォルダー配下に複数のファイルサーバーの共有フォルダーを配することにより、それぞれのファイルサーバーの物理的な位置を意識せずにアクセスすることが可能になります。



【補足】
フォルダーターゲットとして、名前空間サーバー自身の共有フォルダーを指定することもできます。

上記の図の例の場合、クライアント PC からは、以下のどちらかの形式の共有パスを指定し、DFS 名前空間経由で共有フォルダー(ShareB)にアクセスすることができます。

- ¥¥DomainA¥Public¥DLink_B (先頭が¥¥ドメイン名 / ドメインモードのDFS の場合のみ)
- ¥¥ServerA¥Public¥DLink_B (先頭が¥¥サーバー名)

つまり、クライアント PC から ¥¥DomainA¥Public¥DLink_B の配下のファイル一覧を参照すると ¥¥ServerB¥ShareB の配下のファイル一覧が、¥¥DomainA¥Public¥DLink_C の配下のファイル一覧を参照すると ¥¥ServerC¥ShareC の配下のファイル一覧が見えます。

なお、ワークグループ環境にて DFS 経由で別サーバーの共有フォルダーにアクセスする場合、名前空間のルートとなるフォルダー、フォルダーターゲットとなる共有フォルダーのそれぞれに適切なアクセス権を設定しておく必要があります。しかし、フォルダーターゲット間（異なるサーバー間）において、アクセス権を含むデータコピーを行った場合は、該当ファイルのアクセス権は引き継がれません。このため、コピー前のアクセス権でアクセスできないことがあります。
ドメイン環境であれば、ドメインのユーザーに適切なアクセス権を設定することで DFS リンク先のフォルダーにもスムーズにアクセス可能となり、フォルダーターゲット間でのデータコピー時のアクセス権の問題も発生しなくなりますので、名前空間機能はドメイン環境にて利用することを推奨いたします。

名前空間の作成には以下が必要となります。

(1) 名前空間サーバー

DFS 名前空間を作成する際には、名前空間を代表するサーバーである名前空間サーバー（上記の例の ServerA）が必要となります。

> 【補足】
> ドメイン環境では、名前空間の情報はアクティブディレクトリに格納されますので、名前空間を作成する場合は、名前空間サーバーをドメインコントローラーに作成することを推奨いたします。なお、iStorage NS はドメインコントローラーとすることはできません。

(2) 名前空間のルート

DFS 名前空間にアクセスする際には、ドメイン名もしくは名前空間サーバーのサーバー名に続けて、名前空間のルート名を指定します。なお、設定時は『名前空間の名前』として指定します。

(3) 名前空間

名前空間には以下の 2 種類が存在します。

① ドメインベースの名前空間

ドメイン環境にて利用することができる名前空間です。共有フォルダーへのアクセスは、ドメイン名もしくは名前空間サーバーのサーバー名を用いて行います。また、1 つの名前空間に複数の名前空間サーバーを設定することができ、共有フォルダーに「¥¥（ドメイン名）¥Public¥DLink_B」の形式でアクセスすることで、1 つの名前空間サーバーが停止しても、クライアント PC からのアクセスが引き続き可能となり、耐障害性が向上します。

名前空間作成時に Windows Server 2008 モードを指定した場合、アクセスベースの列挙 (ABE) 機能を利用することができます。DFS 名前空間内の DFS リンク (ターゲットを持つフォルダー) に設定されたアクセス許可 (ACL) によって、アクセス権がない DFS リンクをユーザーに見せなくすることができます。

【注意】
ドメインベースの DFS 名前空間を利用する場合、名前空間サーバー、フォルダーターゲットのサーバー、クライアント PC は同じドメインに属する必要があります。

② スタンドアロンの名前空間

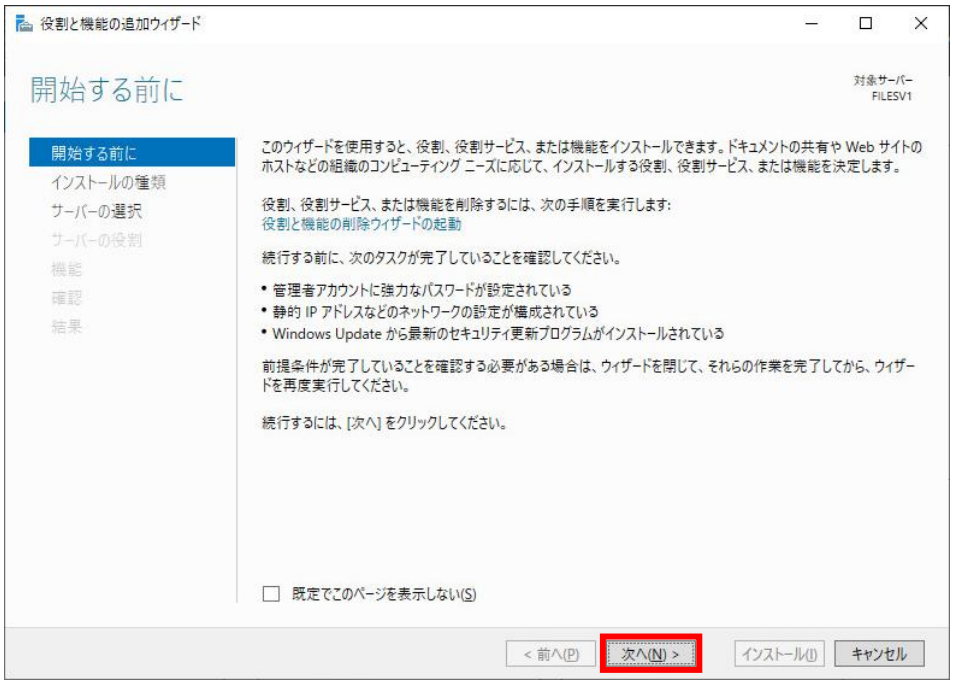
名前空間サーバーを 1 台のみ設定できます。共有フォルダーへのアクセスは、名前空間サーバーのサーバー名を用いて行います。名前空間サーバーが停止すると、名前空間にアクセスできません。

2.4.1.2 DFS 名前空間のインストール

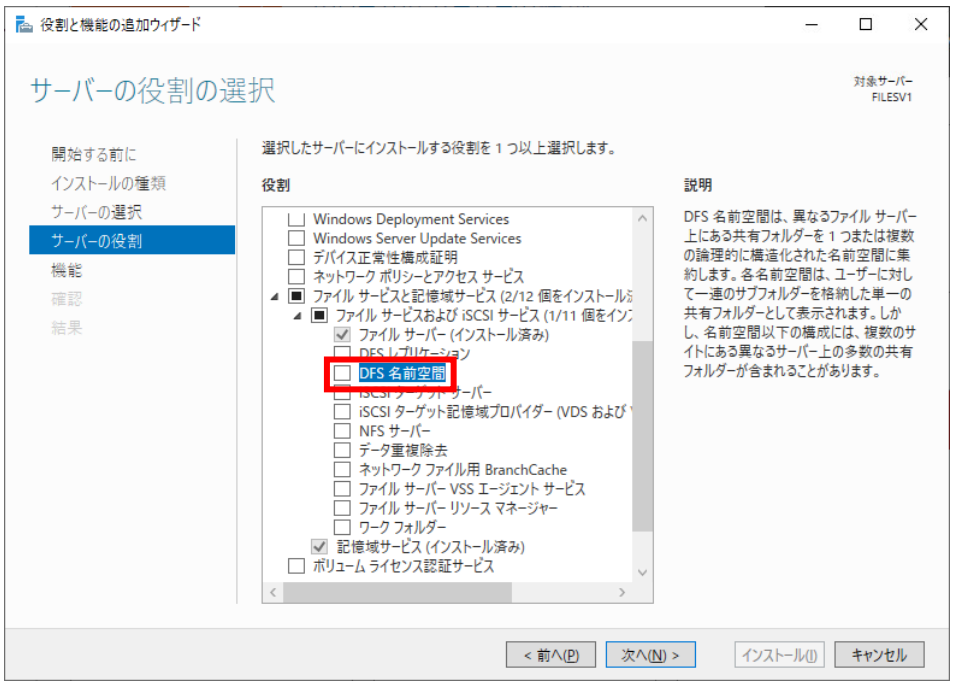
DFS 名前空間 は出荷状態ではインストールされていませんので、使用に際しては、下記の手順にてインストールする必要があります。

1. サーバーマネージャーを起動し、[管理] - [役割と機能の追加] をクリックします。

2. [開始する前に] 画面が表示されますので、デフォルト状態のまま [次へ] ボタンをクリックして、[サーバーの役割の選択] 画面まで進みます。

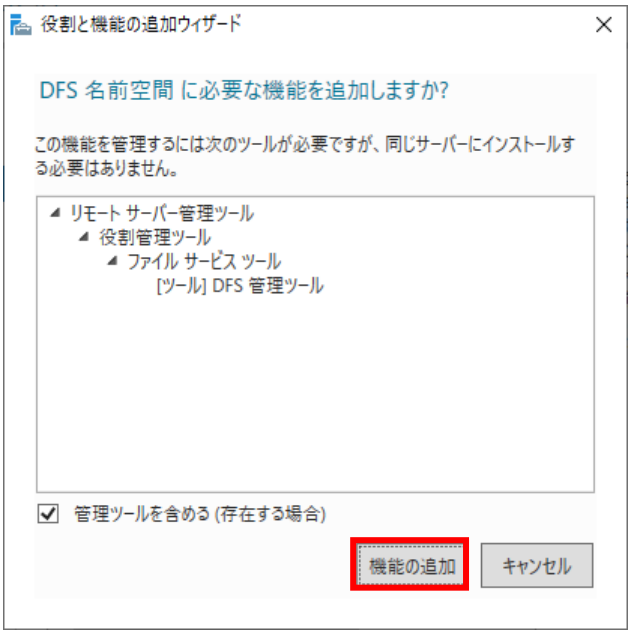


3. [サーバーの役割の選択] 画面の [ファイルサービスと記憶域サービス]、[ファイルサービスおよび iSCSI サービス] を順に展開して、 [DFS 名前空間] をチェックします。

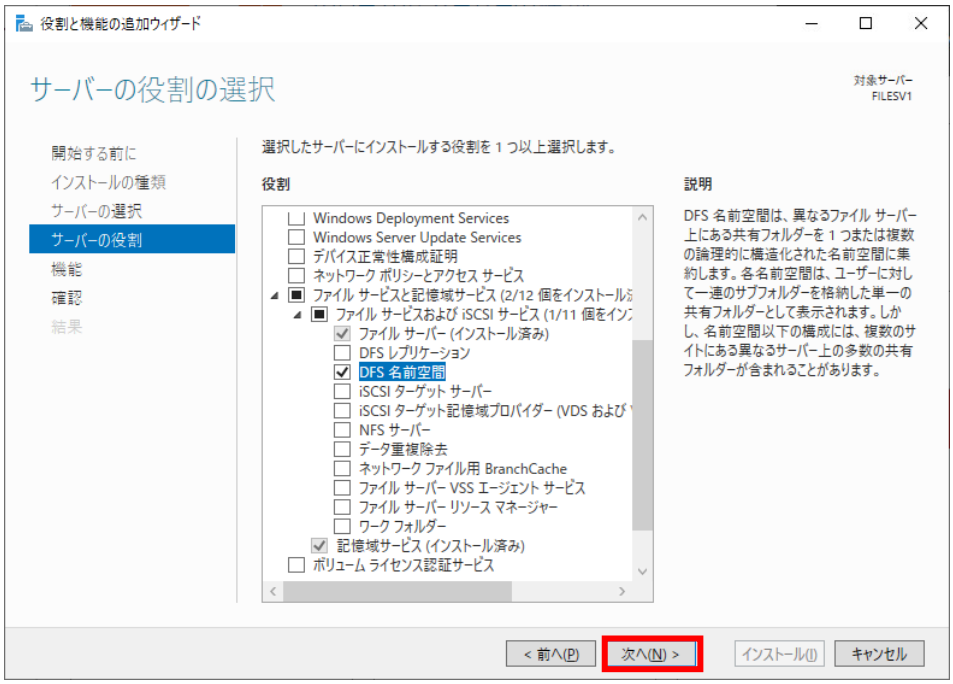


4. [DFS 名前空間 に必要な機能を追加しますか？] 画面が表示されますので、 [機能の追加] をクリックします。

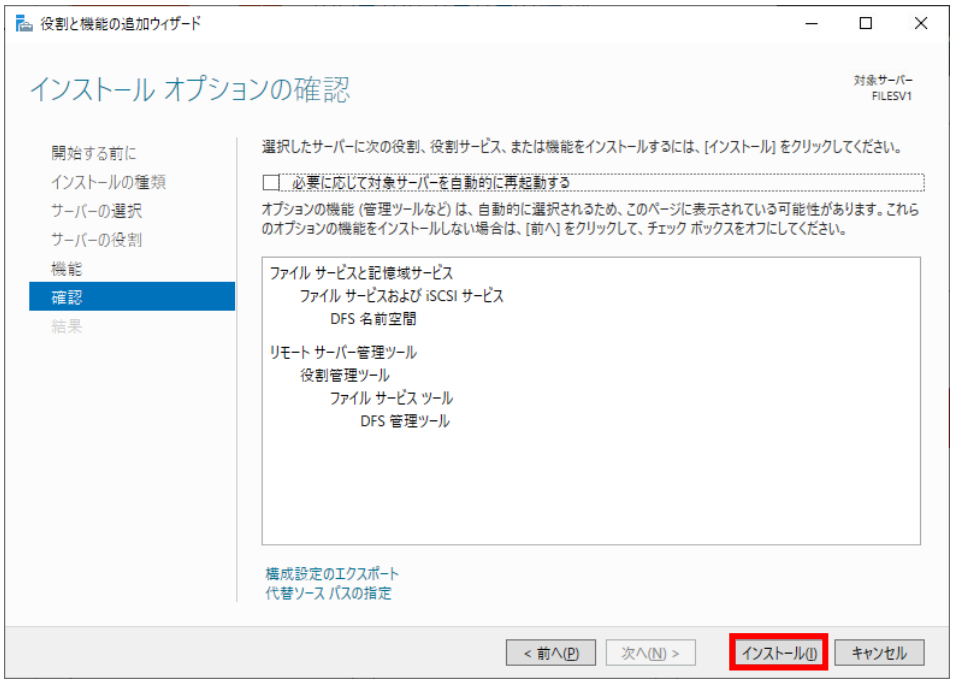
※すでに [DFS 管理ツール] がインストールされている場合、本画面は表示されません。



5. [サーバーの役割の選択] 画面に戻りますので、[次へ] をクリックします。



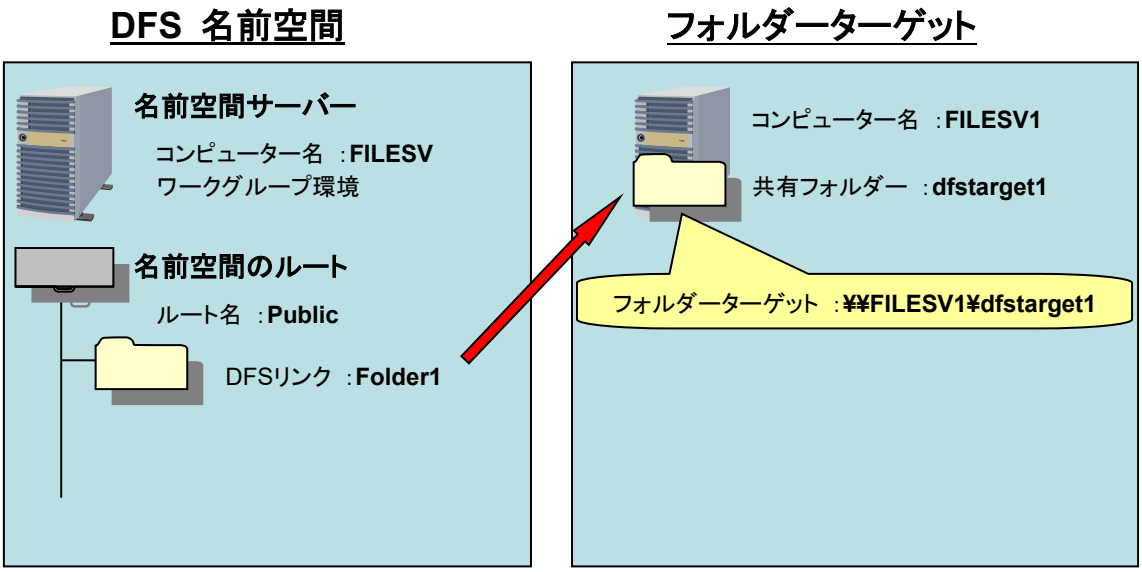
6. [機能の選択] 画面が表示されますので [次へ] をクリックして、[インストールオプションの確認] 画面に進み、[インストール] をクリックします。



7. [インストールの進行状況] 画面が表示されますので、インストールの完了を待ち、[閉じる] をクリックします。

2.4.1.3 名前空間の新規作成

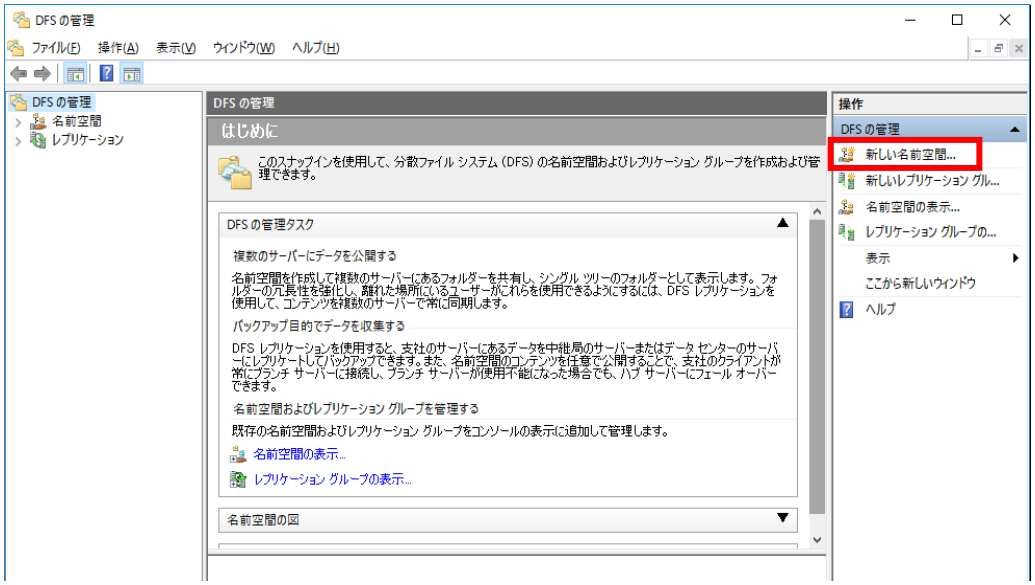
ここでは、ワークグループ環境で名前空間を新規作成する手順を説明します。名前空間サーバーは iStorage NS （サーバー名：FILESV）とし、フォルダーターゲットサーバーは別の iStorage NS （サーバー名：FILESV1）とします。具体的な設定内容は以下のとおりです。



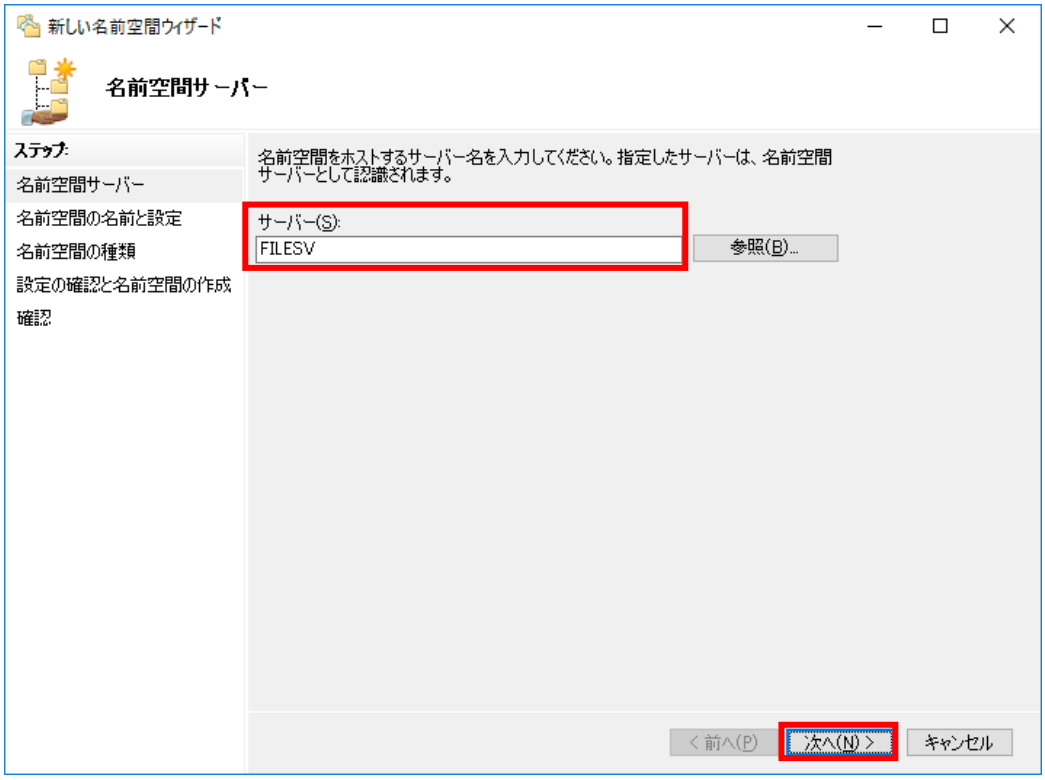
項目	設定内容
名前空間サーバー	FILESV
名前空間の種類	スタンドアロン(ワークグループ環境)
名前空間のルート	Public
DFS リンク	Folder1
フォルダーターゲット サーバー	FILESV1
フォルダーターゲットとする 共有フォルダー	¥¥FILESV1¥dfstarget1
名前空間経由での共有パス	¥¥FILESV¥Public¥Folder1

1. 管理者メニューから [DFS の管理] を起動します。

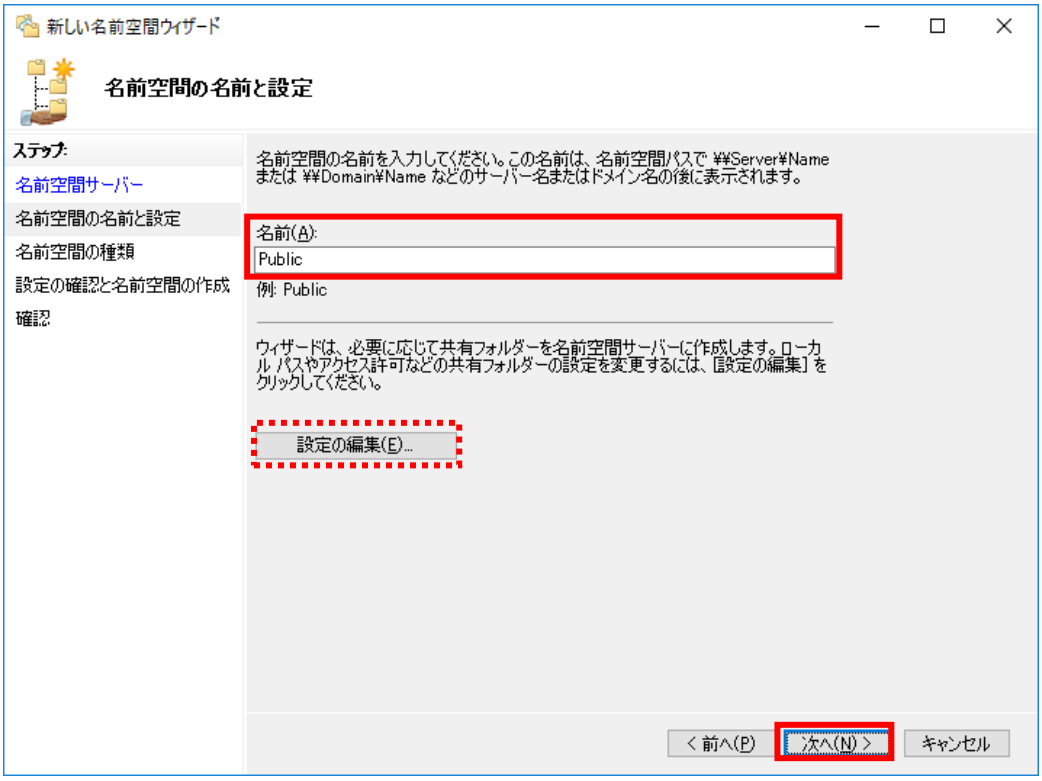
2. [新しい名前空間] をクリックします。



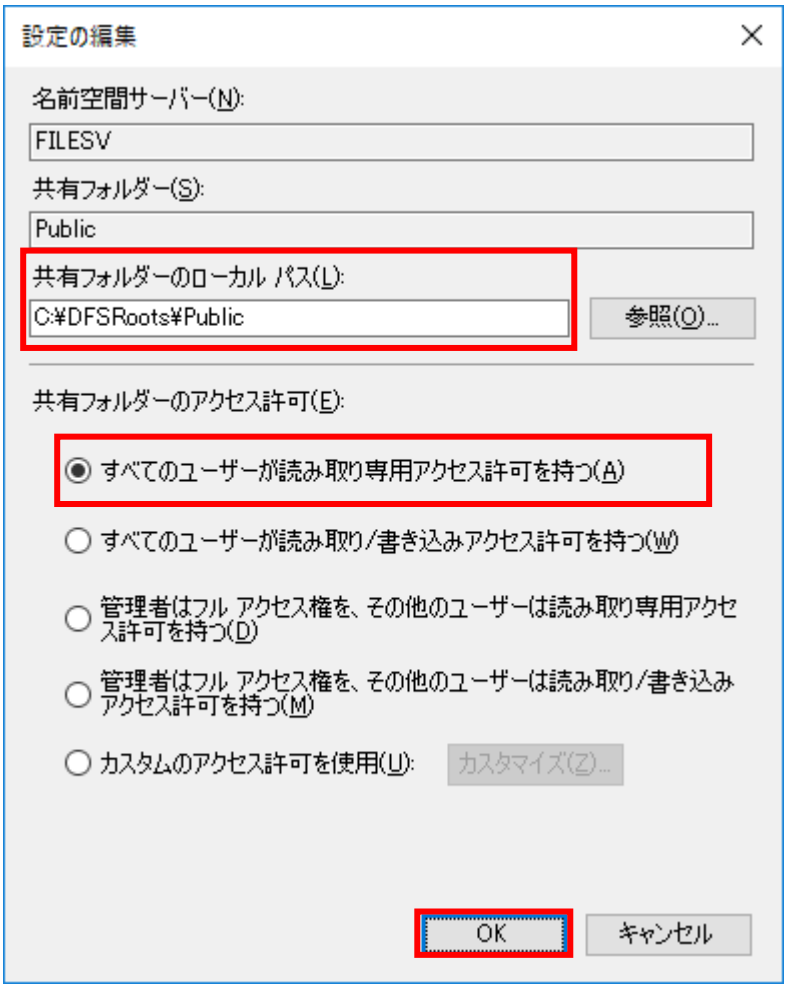
3. [新しい名前空間ウィザード] の [サーバー] に名前空間サーバーとなるサーバー名を入力し、[次へ] をクリックします。



4. [名前空間の名前と設定] 画面にて、 [名前] に新規作成する名前空間の名前を入力して、[次へ] をクリックします。ローカルパスやアクセス許可の設定を変更する場合には、[設定の編集] をクリックします。



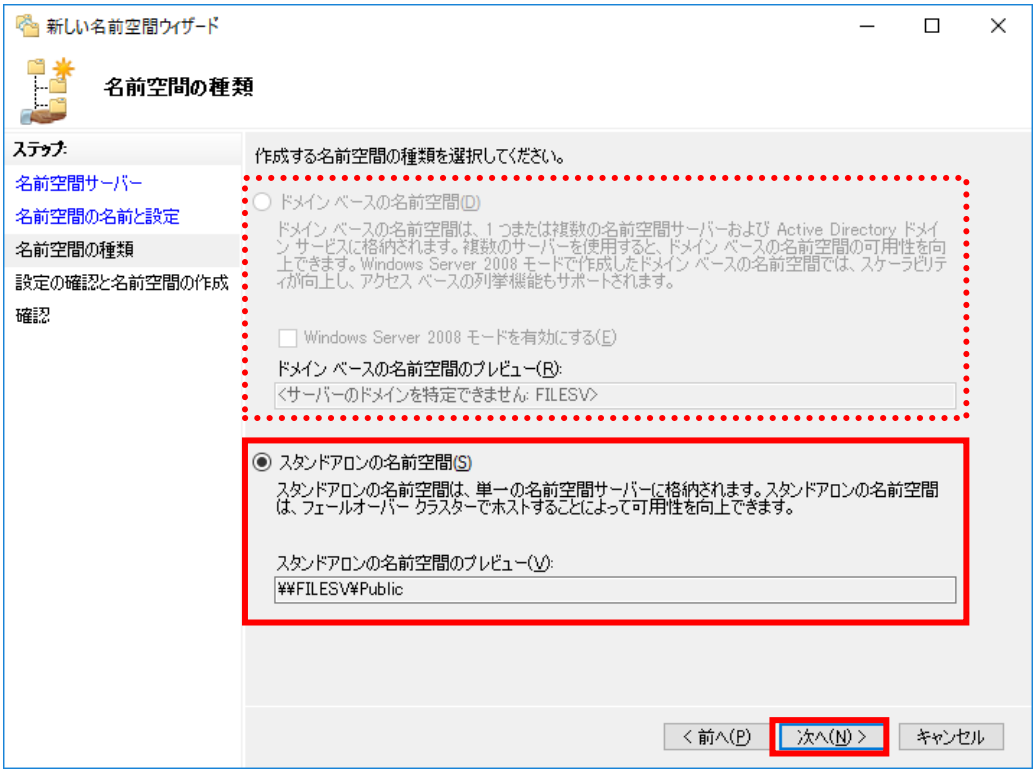
[設定の編集] をクリックした場合は、下記の画面が表示されます。



デフォルトでは [共有フォルダーのローカルパス] は、「C:¥DFSRoots¥"名前空間の名前"」に割り当てられており、[共有フォルダーのアクセス許可] は、[すべてのユーザーが読み取り専用アクセス許可を持つ] となっています。必要に応じて設定を変更し、[OK] をクリックしてください。

[名前空間の名前と設定] 画面に戻ります。

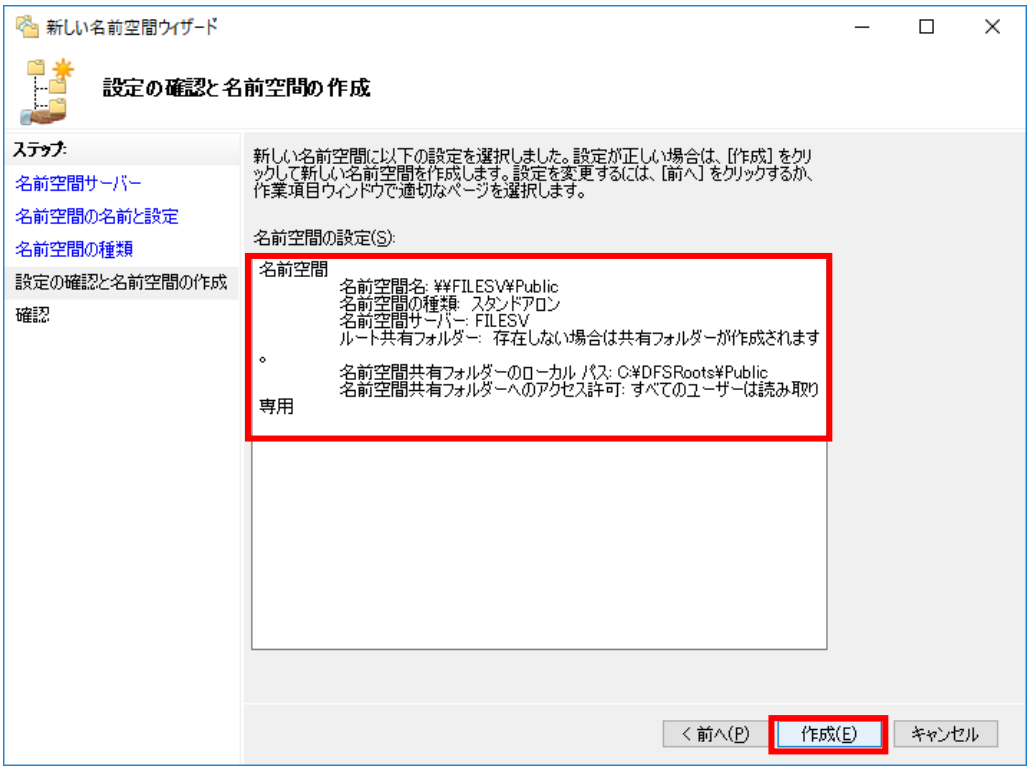
5. [名前空間の種類] 画面にて、作成する名前空間の種類を選択します。 [ドメインベースの名前空間] は、サーバーがドメインに参加していないと選択できません。[Windows Server 2008 モードを有効にする] をチェックすると、DFS 名前空間でアクセスベースの列挙を使用できます。
ここでは [スタンドアロンの名前空間] を選択し、[次へ] ボタンをクリックします。



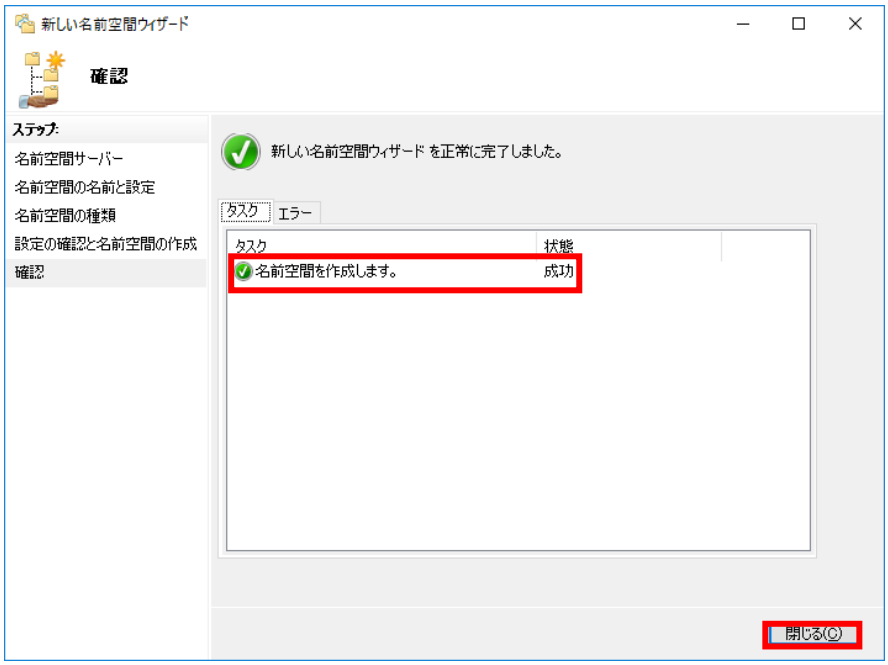
【注意】
ドメインベースの名前空間で Windows Server 2008 モードを使用するには、ドメインと名前空間で次の要件を満たす必要があります。

- フォレストの機能レベル：Windows Server 2003 以上のフォレスト機能レベル
- ドメインの機能レベル：Windows Server 2008 以上のドメイン機能レベル
- すべての名前空間サーバーが、Windows Storage Server 2008 以降、または Windows Server 2008 以降の OS であること

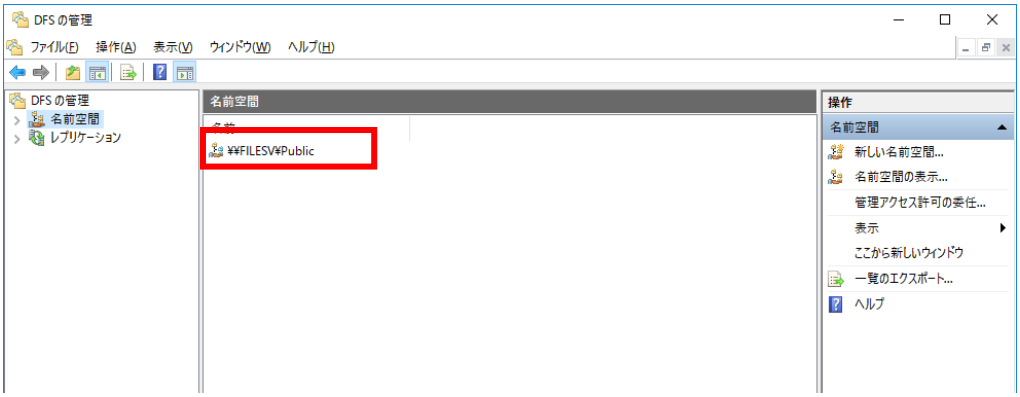
6. [設定の確認と名前空間の作成] 画面にて、[名前空間の設定] に設定した内容が表示されていることを確認して、[作成] をクリックします。



7. [確認] 画面に切り替わり、名前空間が作成されます。正常に作成が完了すると、[タスク] タブの画面の項目にチェックマークが表示されますので、[閉じる] をクリックします。作成がエラーとなった場合は、[エラー] タブの画面に、詳細なエラー内容が表示されます。内容を確認の上、設定を見直し、再度作成してください。



8. 作成された名前空間を確認します。

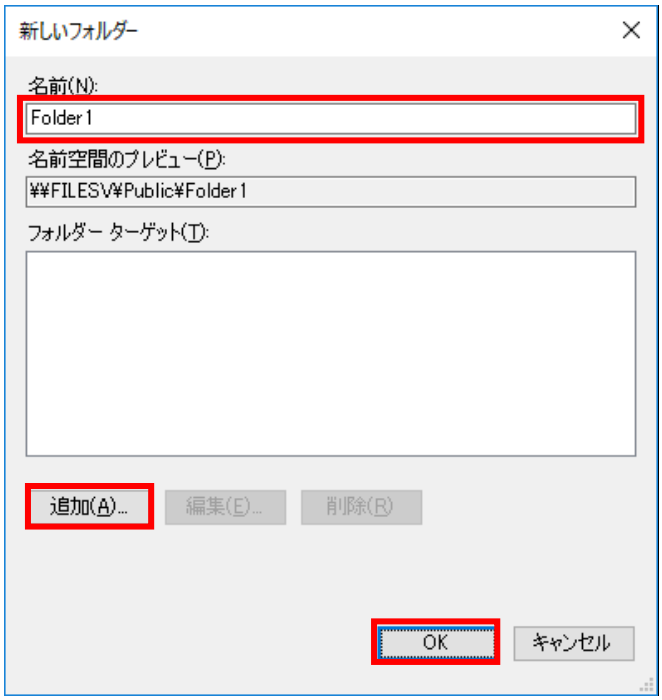


2.4.1.4 名前空間でのフォルダーの新規作成

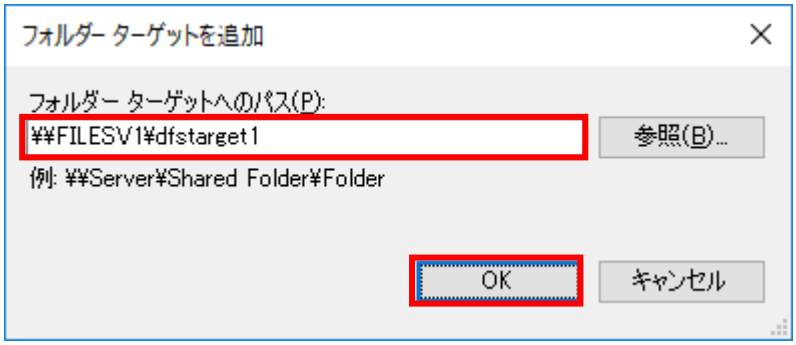
作成した名前空間にフォルダーを新規作成してフォルダーターゲットを設定する方法を説明します。ここでは、フォルダーターゲットとして、名前空間サーバーとは別の iStorage NS 上にあらかじめ適切なアクセス権を設定した共有フォルダーを作成しておきます。共有フォルダーのパスは「¥¥FILESV1¥dfstarget1」とします。

1. DFS の管理画面にて、ツリーに表示されている名前空間を選択し、右ペインの [新しいフォルダー] をクリックします。

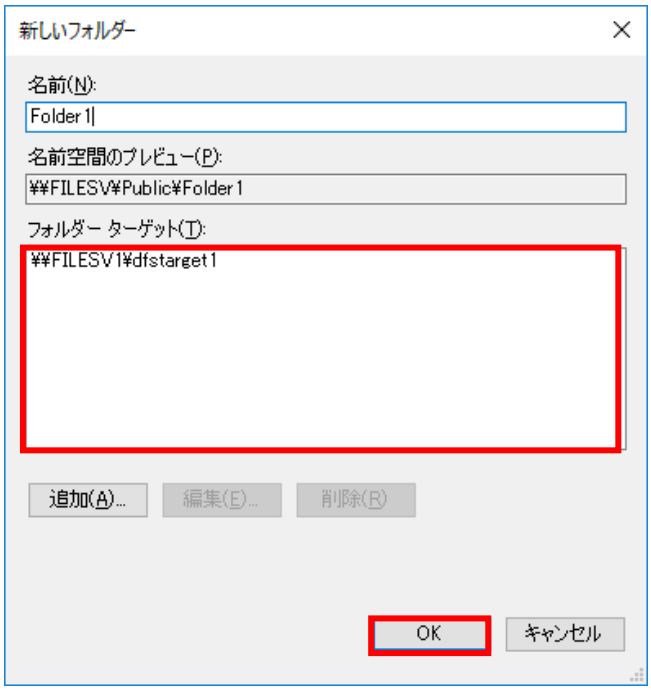
2. [新しいフォルダー] 画面にて、フォルダーの名前を入力し、[追加] をクリックします。



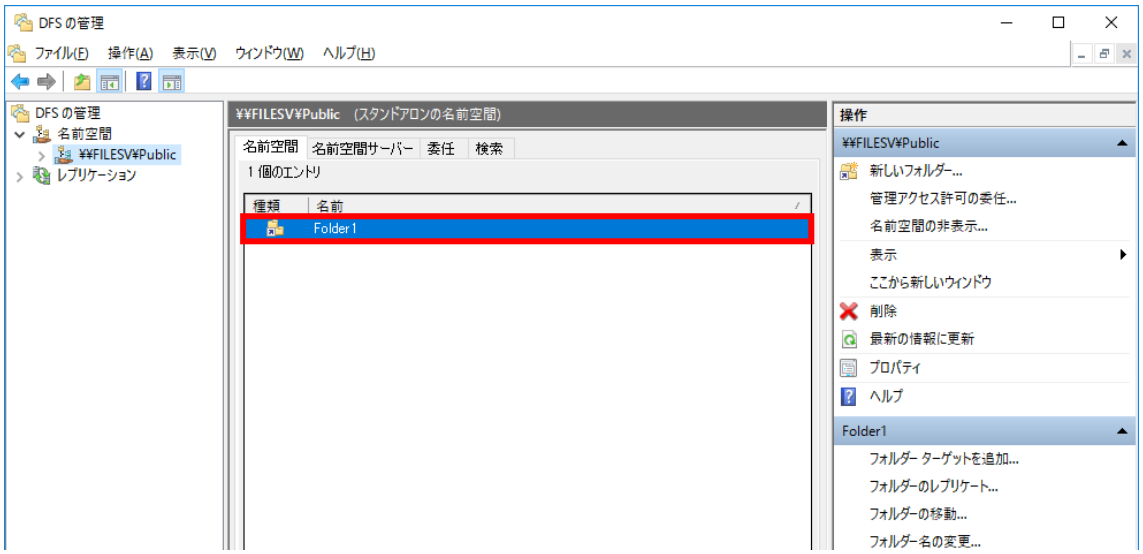
3. [フォルダー ターゲットを追加] 画面にて、 [フォルダー ターゲットへのパス] にターゲットのパスを入力し、[OK] をクリックします。



4. [新しいフォルダー] 画面に戻りますので、 [フォルダー ターゲット] にフォルダーが追加されたことを確認し、[OK] をクリックします。



5. DFS の管理画面で、中央ペインの [名前空間] タブにて、フォルダーが追加されたことを確認します。



2.4.1.5 DFS 名前空間の注意・制限事項

- ドメインベースの DFS 名前空間を利用する場合、名前空間サーバー、フォルダーターゲットのサーバー、クライアント PC は同じドメインに属する必要があります。

- ドメインベースの名前空間で Windows Server 2008 モードを使用するには、ドメインと名前空間で次の要件を満たす必要があります。
  - フォレストの機能レベル：Windows Server 2003 以上のフォレスト機能レベル
  - ドメインの機能レベル：Windows Server 2008 以上のドメイン機能レベル
  - すべての名前空間サーバーが、Windows Storage Server 2008 以降、または Windows Server 2008 以降の OS であること

2.4.2 DFS レプリケーション

2.4.2.1 DFS レプリケーションの機能概要

DFS レプリケーションは、ドメイン環境でのみ利用可能な機能で、複数のサーバー間のフォルダー／ファイルを双方向に複製・同期するマルチマスタ レプリケーション エンジンです。レプリケーションの設定を行ったサーバー上で生じた変更は、ステージングフォルダーに蓄積後、レプリケーション グループの他のすべてのサーバーに複製されます。

レプリケーショングループを構成する各サーバーの同一ファイルに対して同時に更新処理を行うと、サーバー間のレプリケーション時に競合が発生し、最も新しい更新以外は破棄されます（破棄された更新内容は ConflictAndDeleted フォルダーに一定期間保存されます)。更新処理を行った利用者の観点では、意図しない内容に更新されている場合があります。この動作はマルチマスタ レプリケーションを行う DFS レプリケーションの仕様の動作です。

このため、DFS レプリケーションの運用においては、ファイル更新処理の衝突に十分ご注意ください。

また、読み取り専用のレプリケートフォルダーも作成することができますので、ファイルを更新するサーバー1 台を除き、他のサーバーすべてのレプリケートフォルダーを読み取り専用にすることで、ファイル更新処理の衝突を回避することが可能です。なお、これを利用して、「センターのサーバー上にあるファイルを、拠点のサーバー上に展開し参照のみを許可する。」といった運用が可能です。

【注意】

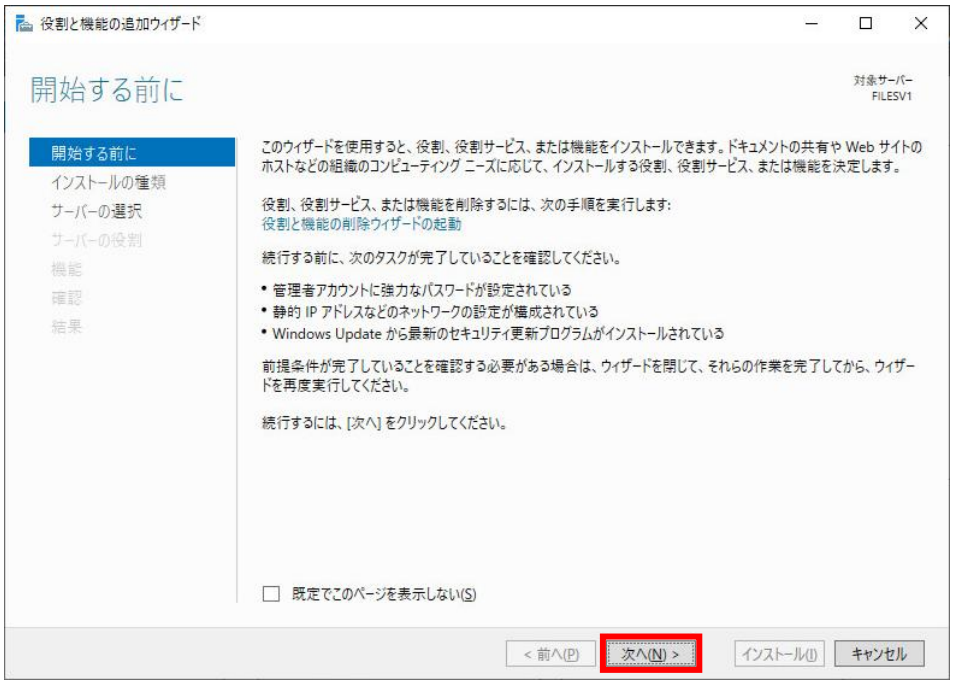
- DFS レプリケーションの設定を行う際は、必ずドメインの管理者アカウントで実施してください。
- 読み取り専用のレプリケートフォルダーを利用する場合は、ドメインコントローラーのアクティブディレクトリに Windows Server 2008 以降のスキーマが必要となります。

2.4.2.2 DFS レプリケーションのインストール

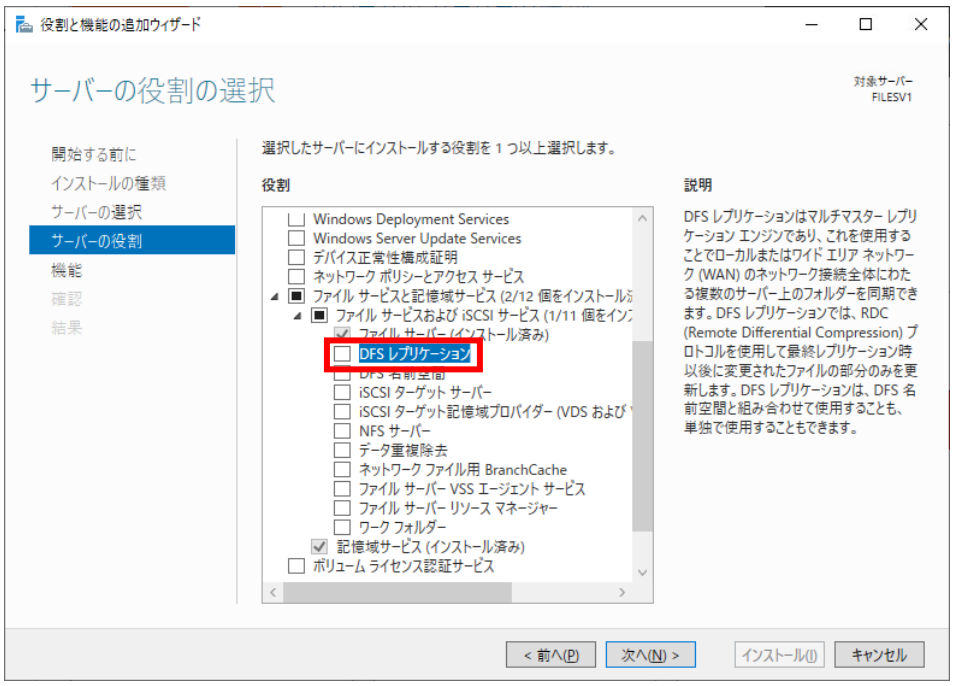
DFS レプリケーション は出荷状態ではインストールされていませんので、使用に際しては、下記の手順にてインストールする必要があります。

1. サーバーマネージャーを起動し、[管理] - [役割と機能の追加] をクリックします。

2. [開始する前に] 画面が表示されますので、デフォルト状態のまま [次へ] ボタンをクリックして、[サーバーの役割の選択] 画面まで進みます。

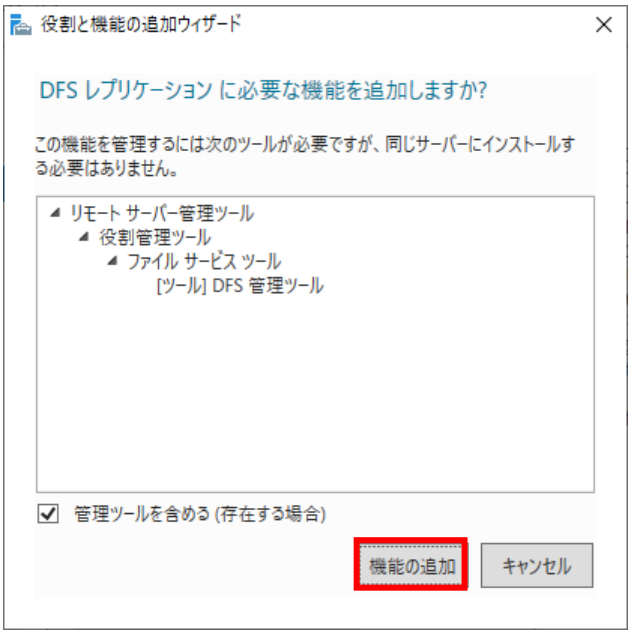


3. [サーバーの役割の選択] 画面の [ファイルサービスと記憶域サービス]、[ファイルサービスおよび iSCSI サービス] を順に展開して、 [DFS レプリケーション] をチェックします。

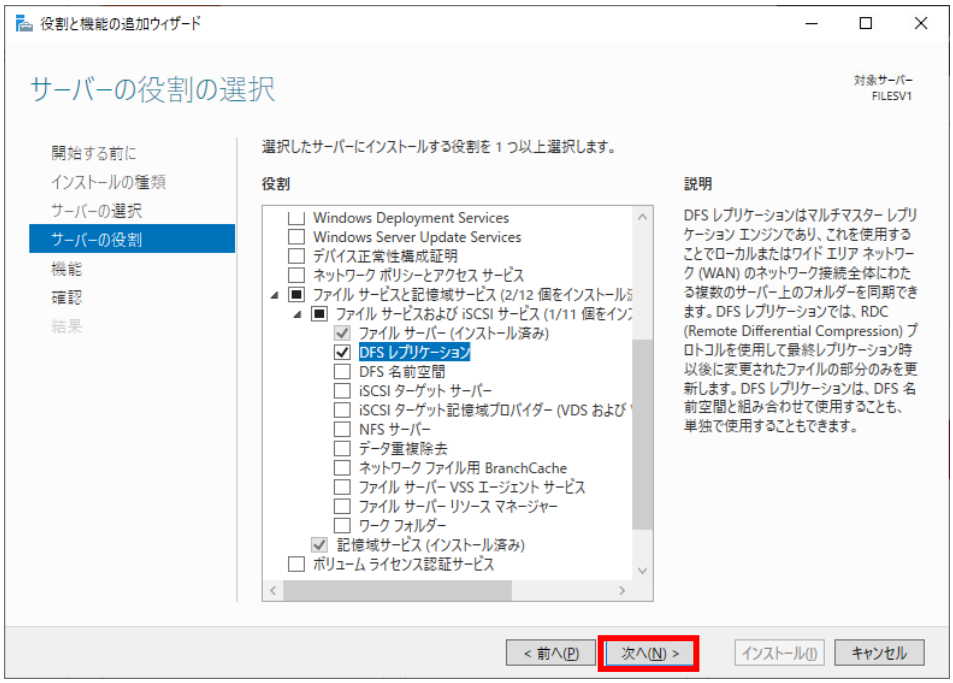


4. [DFS レプリケーション に必要な機能を追加しますか？] 画面が表示されますので、 [機能の追加] をクリックします。

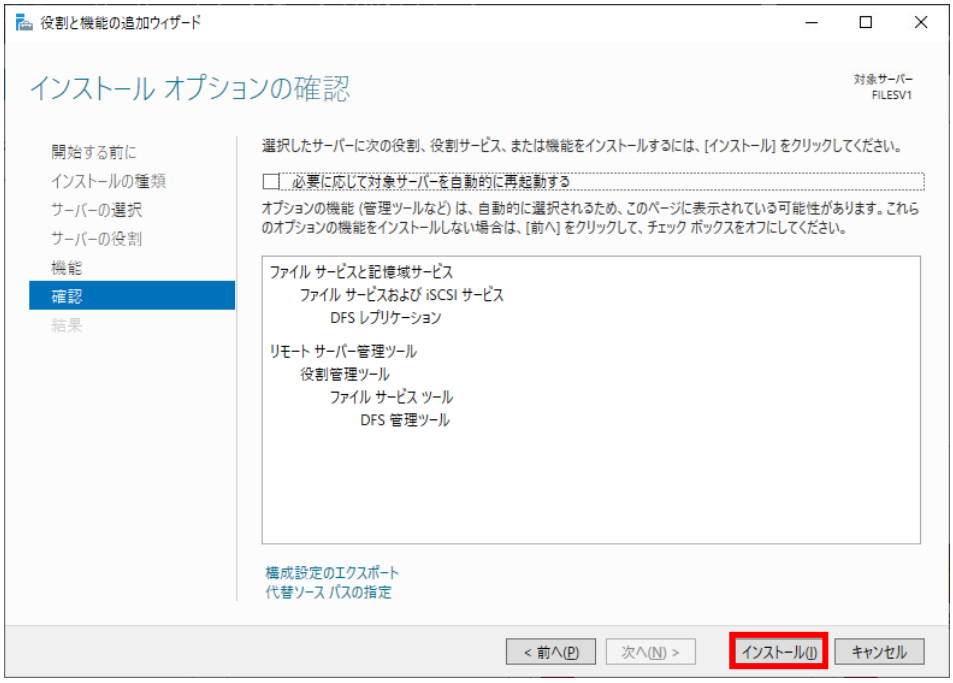
※すでに [DFS 管理ツール] がインストールされている場合、本画面は表示されません。



5. [サーバーの役割の選択] 画面に戻りますので、[次へ] をクリックします。



6. [機能の選択] 画面が表示されますので [次へ] をクリックして、[インストールオプションの確認] 画面に進み、[インストール] をクリックします。



7. [インストールの進行状況] 画面が表示されますので、インストールの完了を待ち、[閉じる] をクリックします。

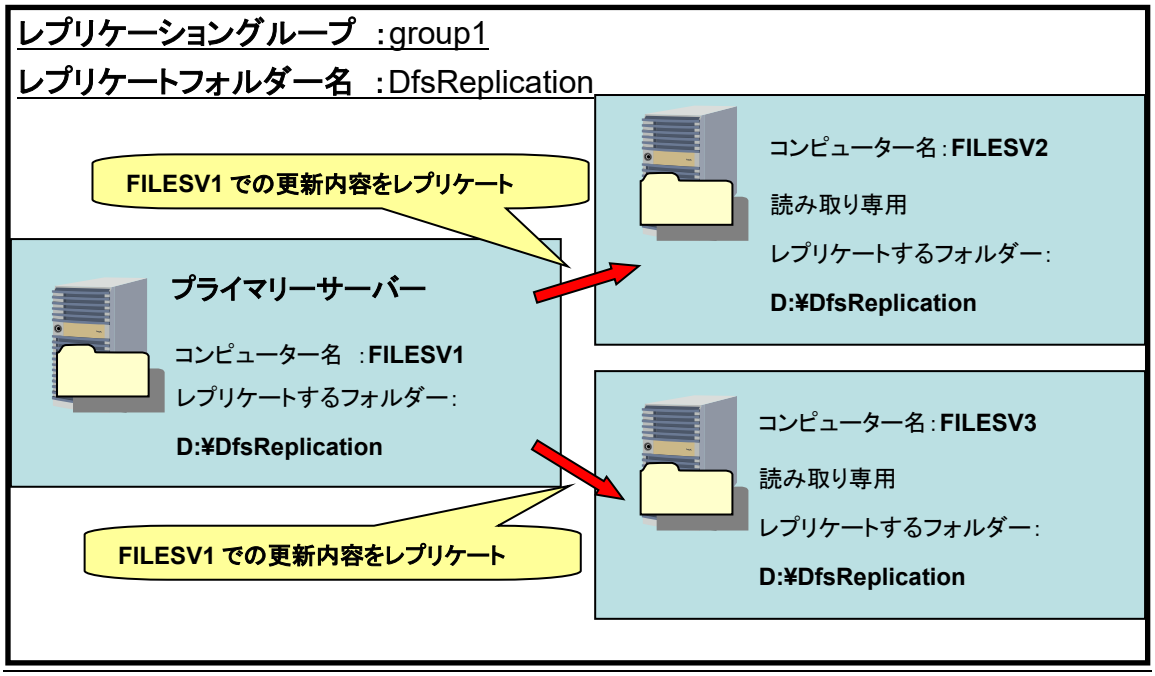
【注意】
DFS レプリケーションのインストール後、イベントログに「ソース: DFSR イベント ID:6104」が記録される場合があります。このイベントが記録された場合、DFS レプリケーション サービスを再起動する必要があります。DFS レプリケーション サービスを再起動後、「ソース: DFSR イベント ID:6102」が記録されることを確認してください。

2.4.2.3 レプリケーショングループの設定

2.4.2.3.1. レプリケーショングループの新規作成

ここでは、レプリケーショングループの新規作成方法について説明します。なお、レプリケーショングループの設定が完了すると、レプリケーションが自動的に実行されますので、システム負荷を考慮し、設定作業を行ってください。

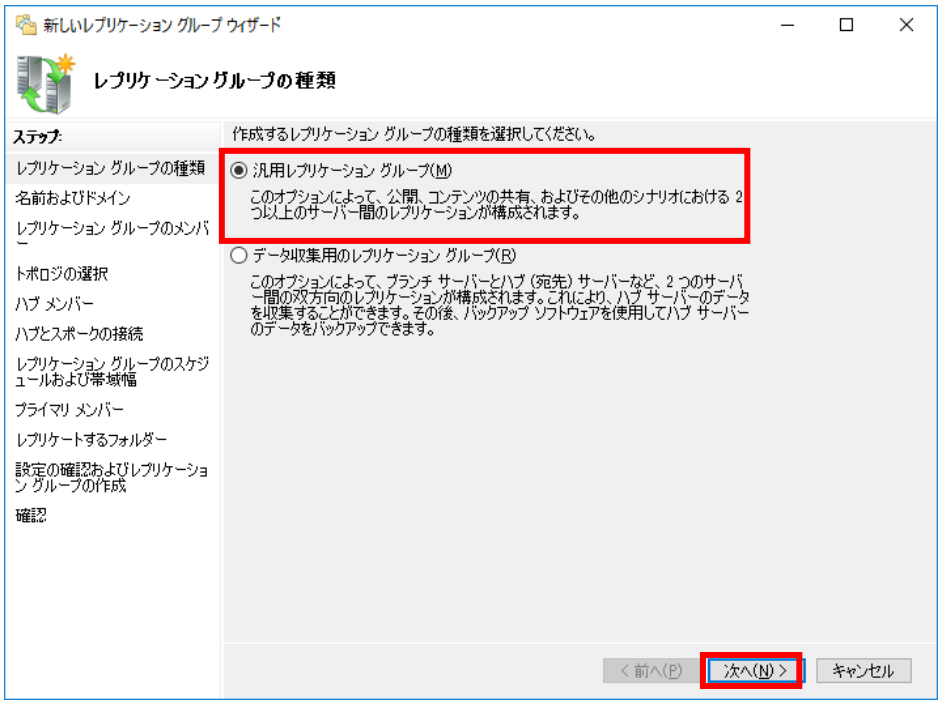
以下の設定例では、3 台の iStorage NS に存在するフォルダー間で、汎用レプリケーショングループを作成、更新可能なサーバーは 1 台のみとし、残りの 2 台は読み取り専用とします。



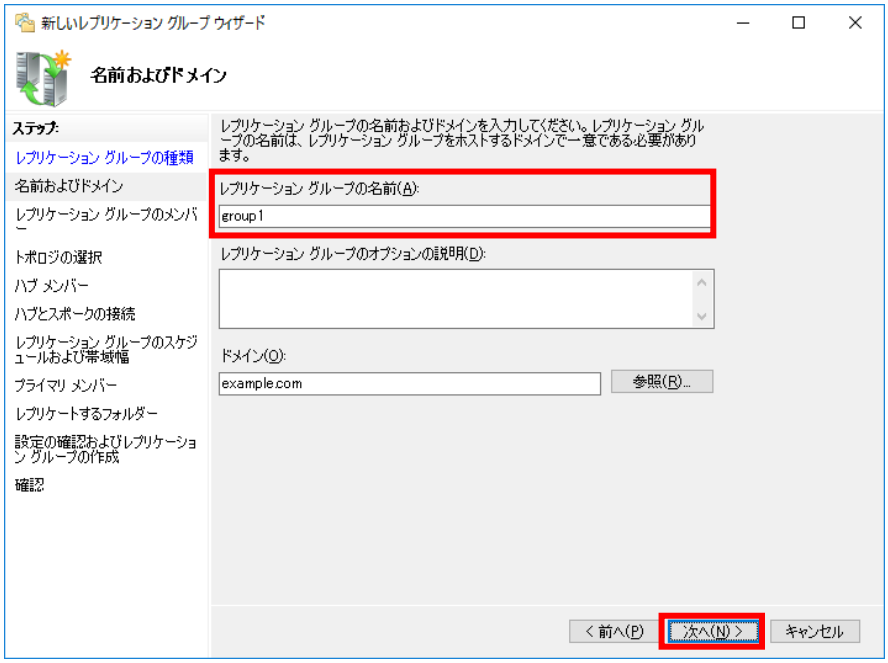
項目	設定内容
レプリケーショングループのメンバー	FILESV1 FILESV2 FILESV3
レプリケートフォルダーのローカルパス	各サーバーの「D:¥DfsReplication」 FILESV2 と FILESV3 のフォルダーは読み取り専用レプリケートフォルダーとする。
プライマリメンバー	FILESV1

1. FILESV1 にドメインの管理者アカウントでサインインします。管理者メニューから [DFS の管理] を起動して、ツリーの [レプリケーション] をクリックします。その後、右ペインの [新しいレプリケーショングループ] をクリックします。

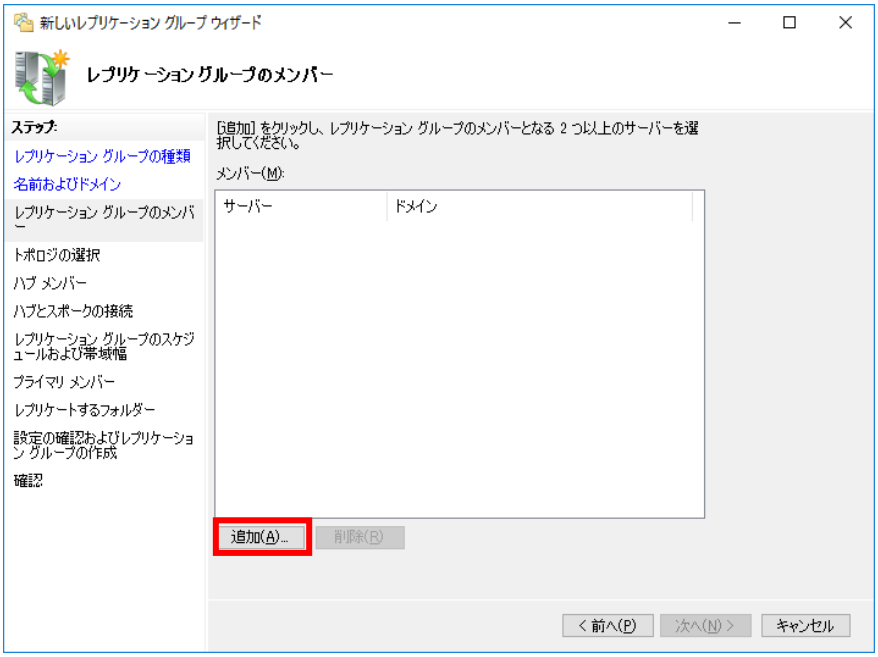
2. [新しいレプリケーショングループウィザード] が起動します。作成するレプリケーショングループの種類を選択し [次へ] をクリックします。



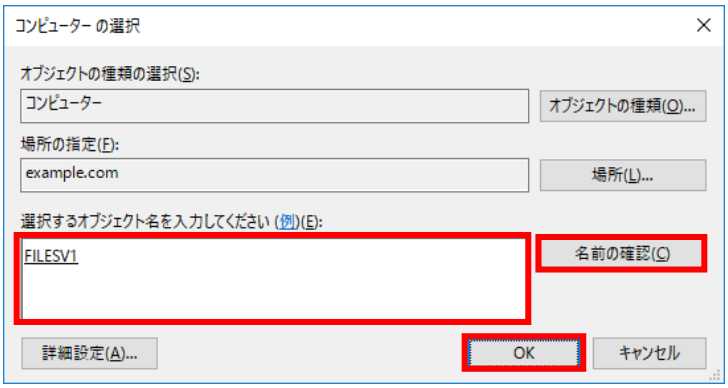
3. [名前およびドメイン] 画面にて、[レプリケーショングループの名前] を入力し、[次へ] をクリックします。



4. [レプリケーショングループのメンバー] にて、レプリケーショングループのメンバーとなるサーバーを追加するため、[追加] をクリックします。

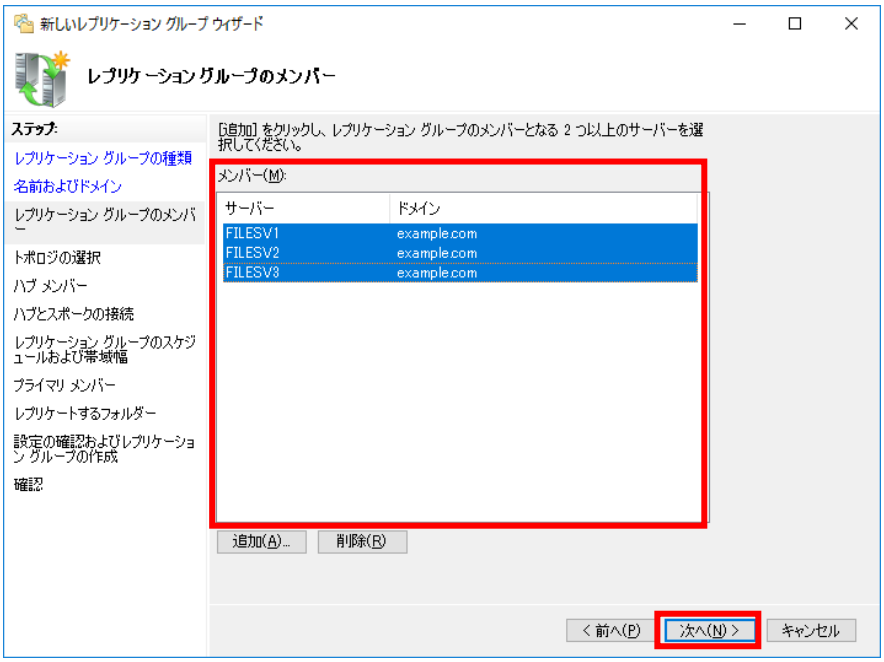


5. [選択するオブジェクト名を入力してください] にて、レプリケーショングループのメンバーとなるサーバー名を入力して、[名前を確認] をクリックします。その後、[OK] をクリックします。

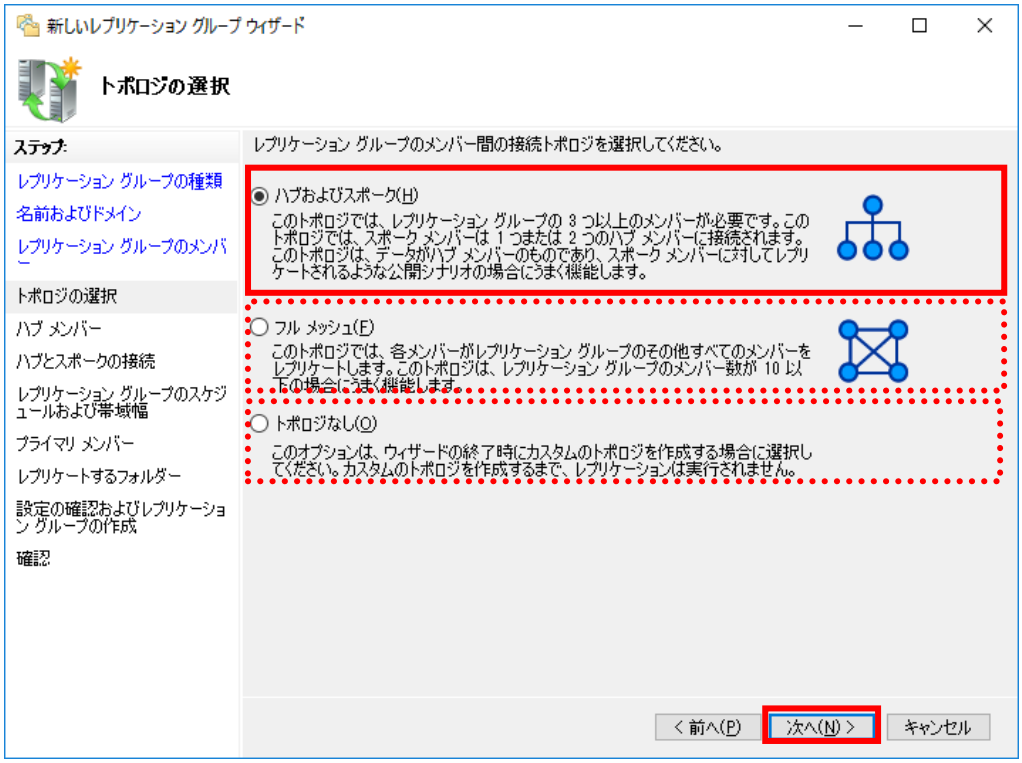


【補足】
[名前を確認] をクリックする際、ドメインの管理者権限を持つユーザー名とパスワードを要求される場合があります。

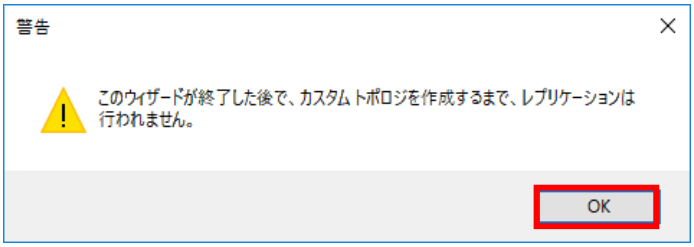
6. サーバーが追加されたことを確認します。レプリケーショングループのメンバーとなるサーバーは 2 台以上必要となりますので、サーバーの数だけ [追加] ボタンをクリックして項番 5 を繰り返し、すべてのサーバーを追加したら、 [次へ] をクリックします。



7. [トポロジの選択] 画面にて、[ハブおよびスポーク] を選択し、[次へ] をクリックします。

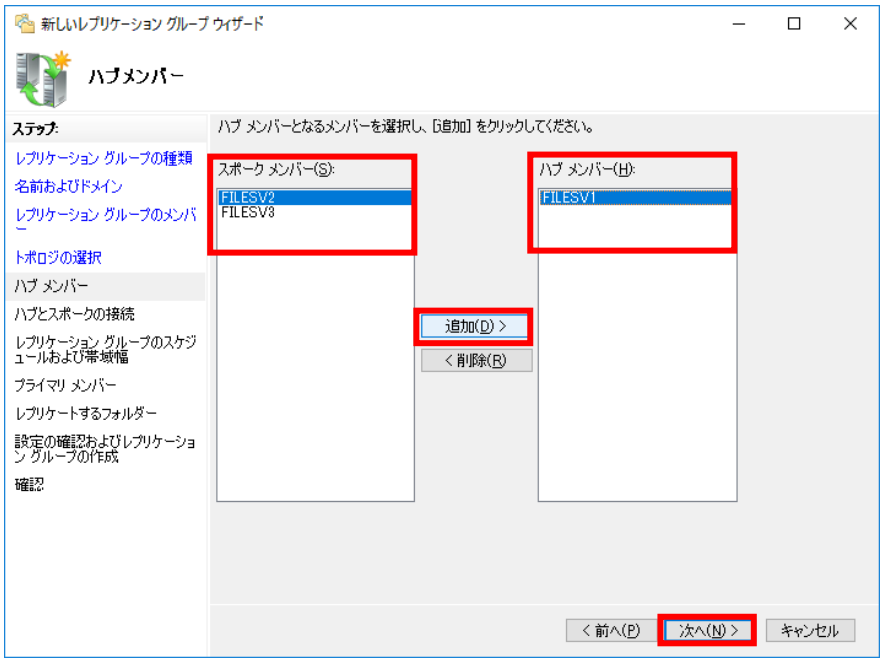


- [フルメッシュ] を選択した場合は、項番 10 [レプリケーショングループのスケジュールおよび帯域幅] 画面に進んでください。
- [トポロジなし] を選択した場合、項番 11 [プライマリメンバー] 画面に進んでください。なお、レプリケーショングループの作成完了後に別途トポロジを設定する必要があります。また、[次へ] をクリックした後に以下の [警告] 画面が表示されますので、[OK] をクリックしてください。

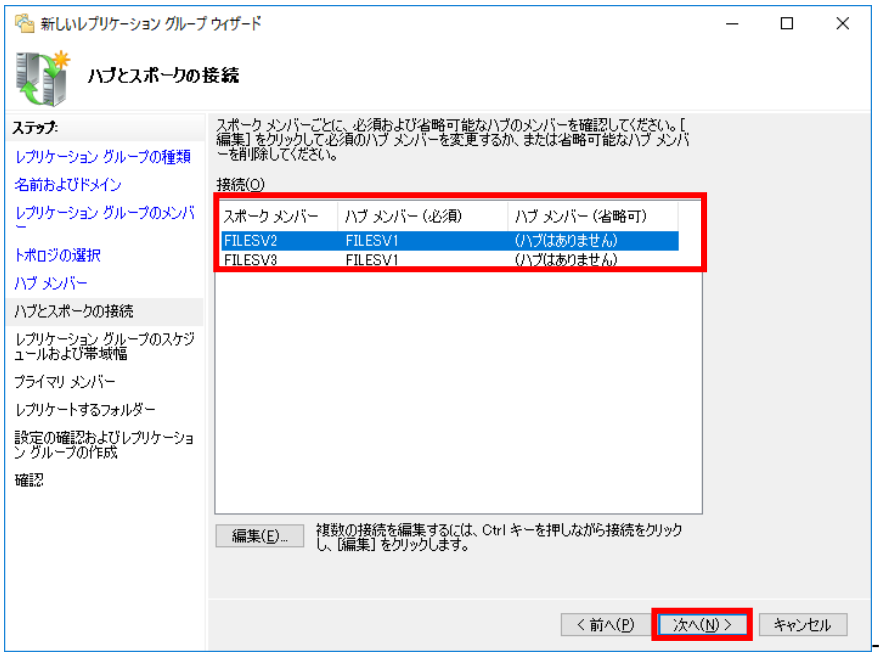


【補足】
[ハブおよびスポーク] は、メンバーが 3 台以上の場合のみ選択できます。また、[フル メッシュ] はメンバーが 10 台以下の場合に選択することが推奨されます。

8. [ハブメンバー] 画面で、[スポークメンバー] 欄より、ハブメンバーにするサーバーを選択し、[追加] をクリックします。選択したサーバーがハブメンバーとして登録されたことを確認し、 [次へ] をクリックします。

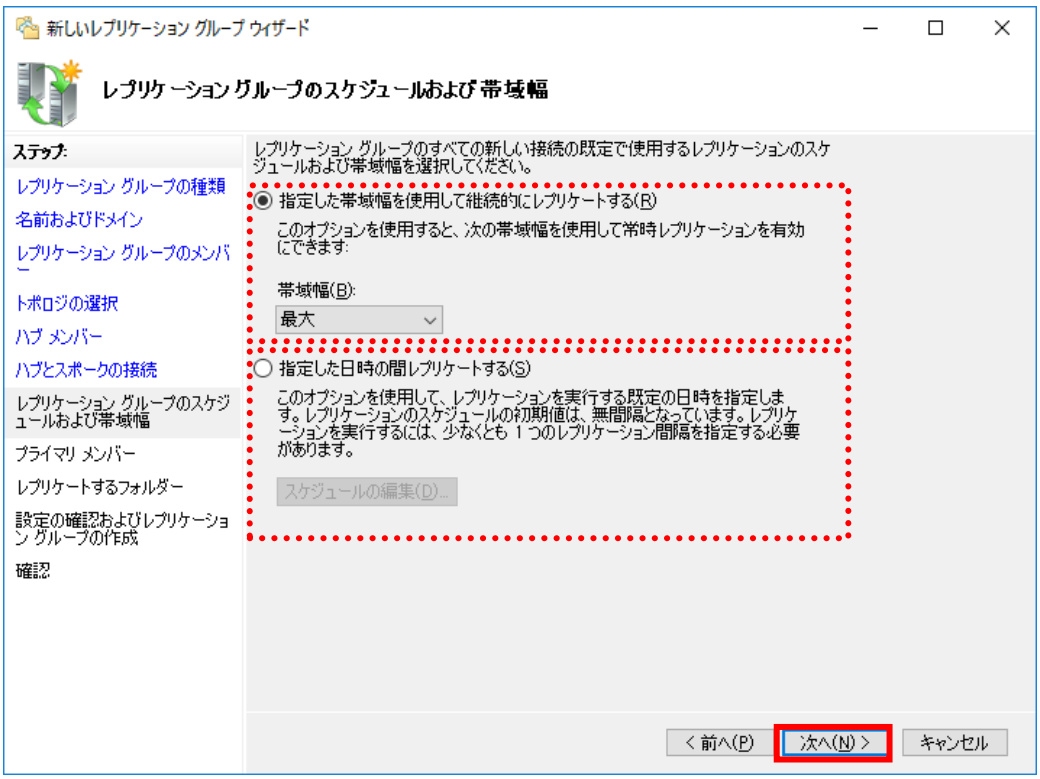


9. [ハブとスポークの接続] 画面にて、ハブメンバーを確認し、[次へ] をクリックします。

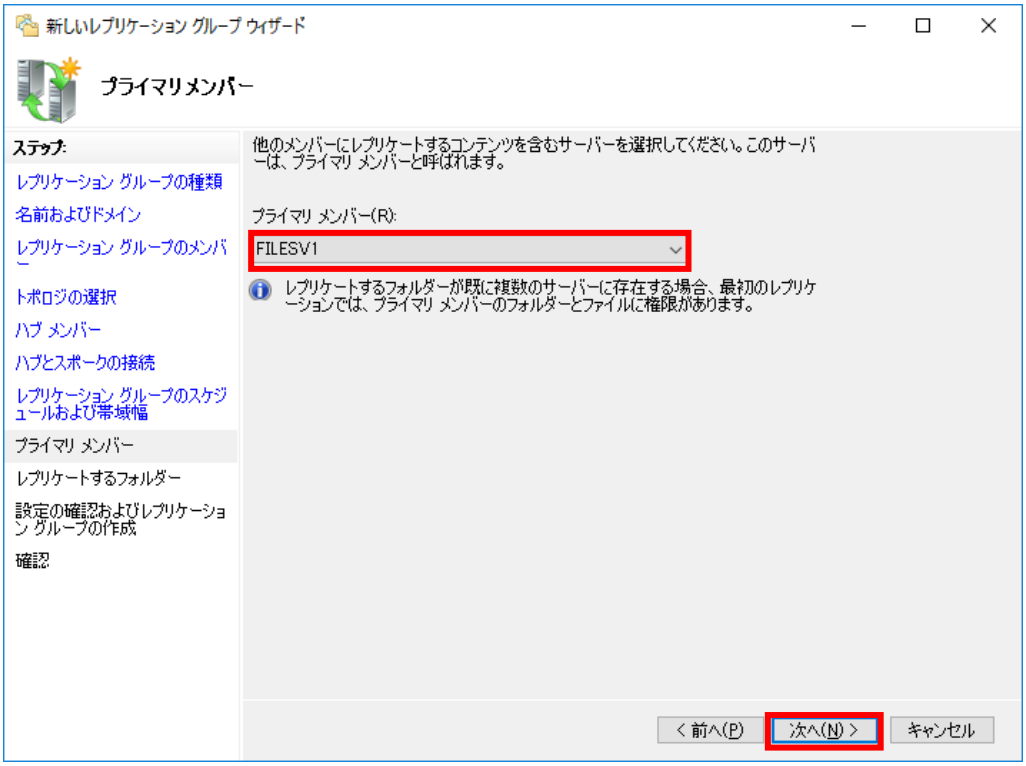


10. [レプリケーショングループのスケジュールおよび帯域幅] 画面にて、レプリケーションのスケジュールと帯域幅を設定してください。常時レプリケーションを行う場合は、[指定した帯域幅を使用して継続的にレプリケートする] を選択して使用する帯域幅を指定します。日時を指定したレプリケーションを行う場合は、[指定した日時の間レプリケートする] を選択します。なお、[指定した日時の間レプリケートする] を選択した場合、[スケジュールの編集] ボタンをクリックするとスケジュールの設定を行うことができます。詳細は、本書の【レプリケーションのスケジュール】の項番 2 以降を参照してください。

    設定が完了したら、[次へ] をクリックしてください。



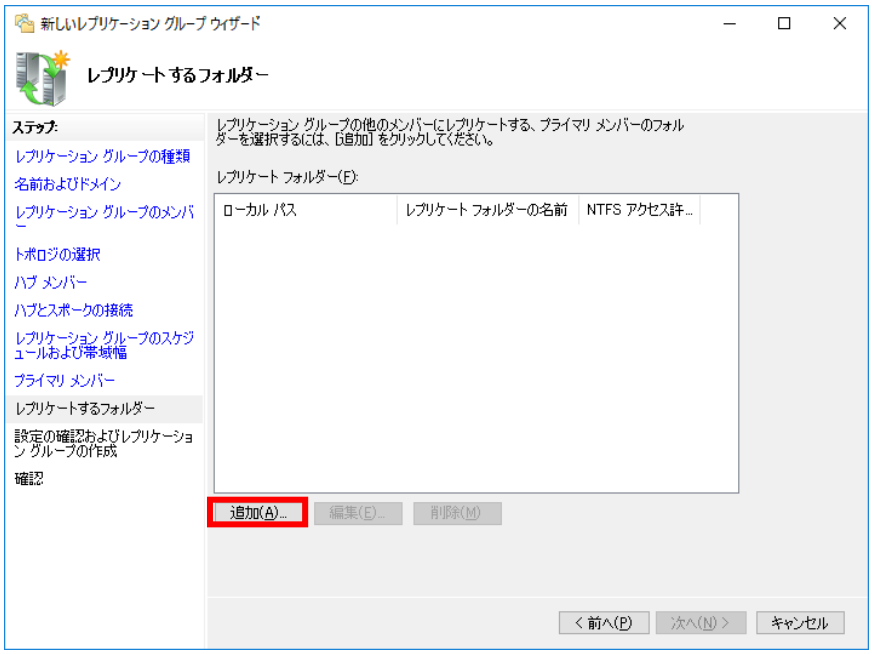
11. [プライマリメンバー] 画面にて、プルダウンメニューからプライマリメンバーにするサーバーを選び、[次へ] をクリックします。



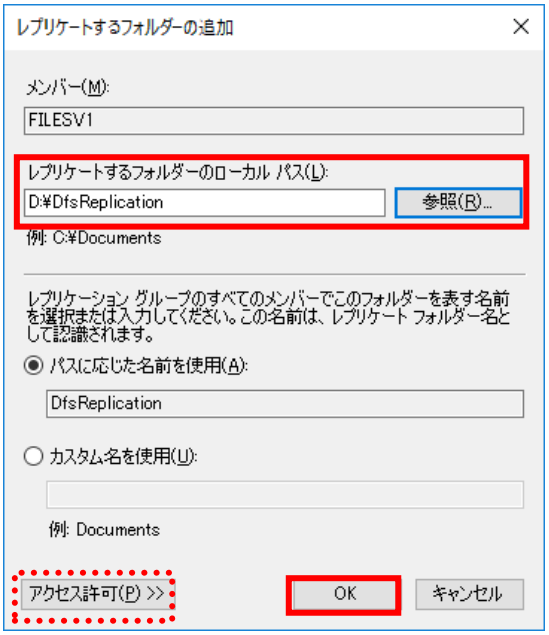
【補足】

プライマリメンバーの設定は、初期レプリケーション時のみ利用されます。初期レプリケーションが完了後、プライマリメンバーと他のメンバーの区別はなくなります。新規レプリケーショングループの初期レプリケーションの際、プライマリメンバー上のファイルは他のメンバーサーバー上のファイルよりも優先されます。初期レプリケーション時にプライマリメンバー以外のメンバーサーバーにファイルが存在すると、ファイル消失が発生することがありますので、あらかじめ別フォルダーに移動しておく等の処置が必要です。

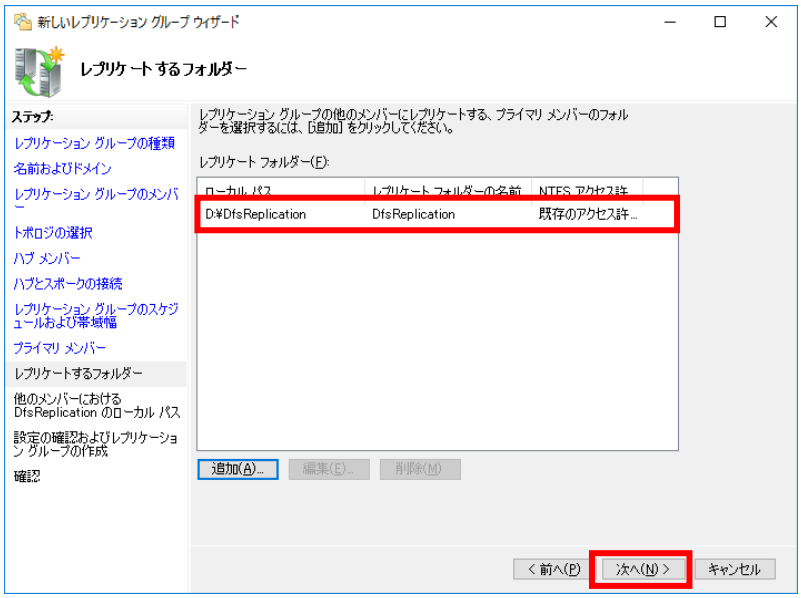
12. [レプリケートするフォルダー] 画面にて、 [追加] をクリックして、プライマリメンバーのフォルダーを選択します。



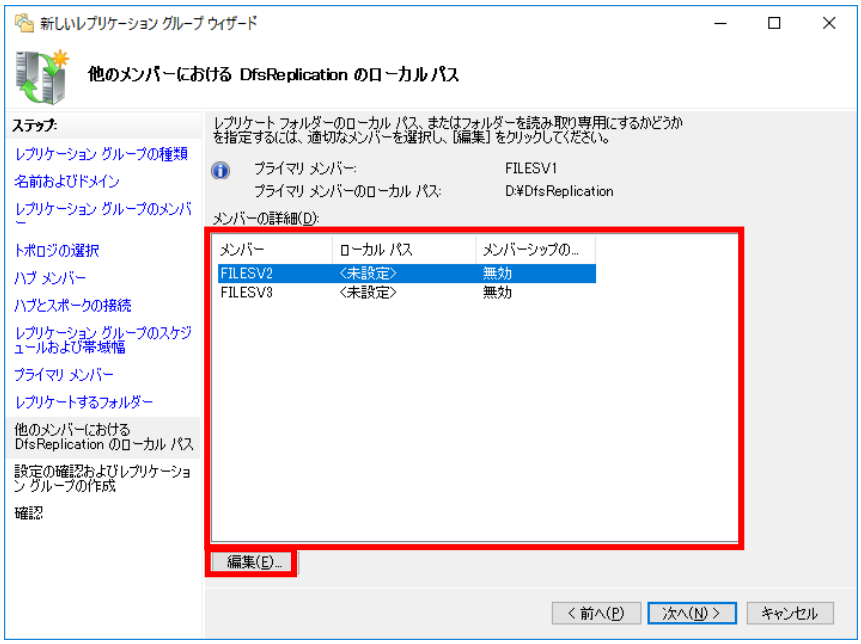
13. [レプリケートするフォルダーを追加] 画面にて、 [レプリケートするフォルダーのローカルパス] を入力します。フォルダーの NTFS のアクセス許可を変更する場合は、 [アクセス許可] をクリックします。



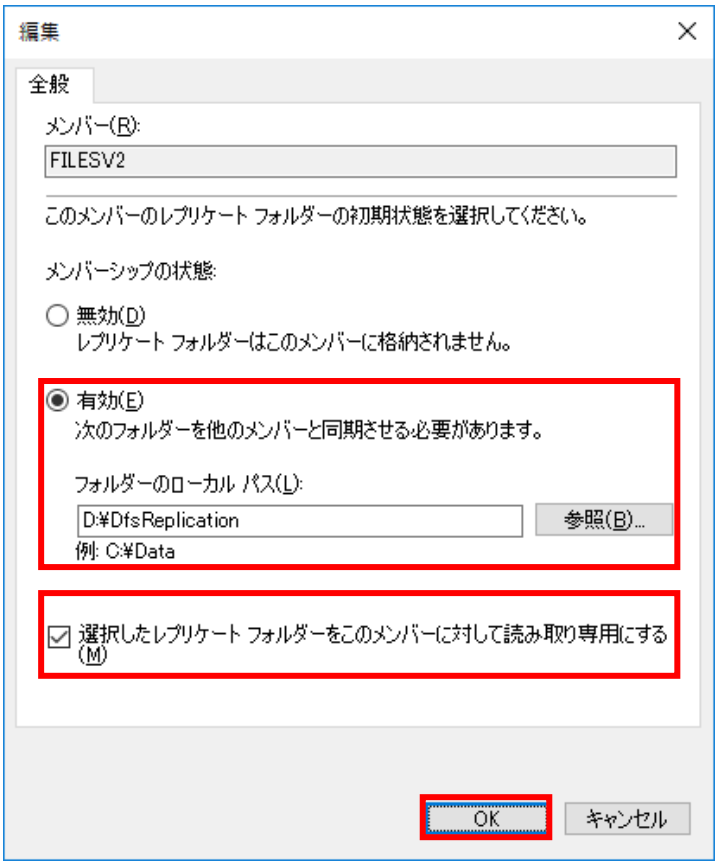
14. [レプリケートするフォルダー] 画面にて、 [レプリケートフォルダー] に設定した内容が表示されていることを確認し、[次へ] をクリックします。



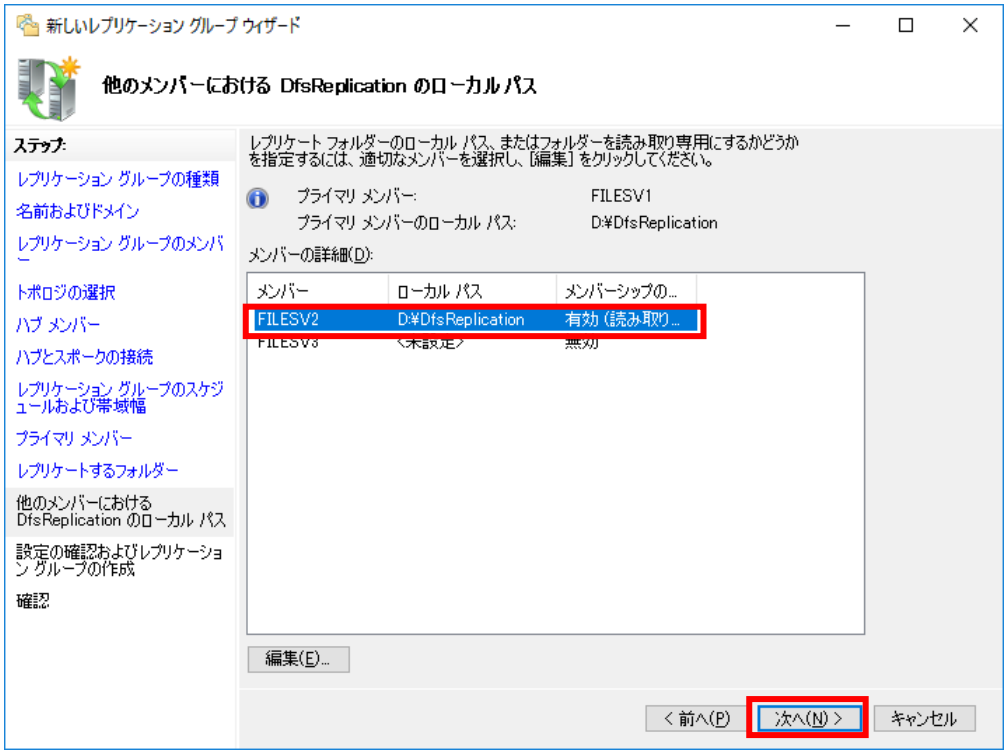
15. [他のメンバーにおける"レプリケートフォルダー名"のローカルパス] 画面にて、 [メンバーの詳細] にプライマリメンバー以外のメンバーのサーバー名が表示されていることを確認します。 [ローカルパス] が“<未設定>”になっているメンバーを選択し、 [編集] をクリックします。



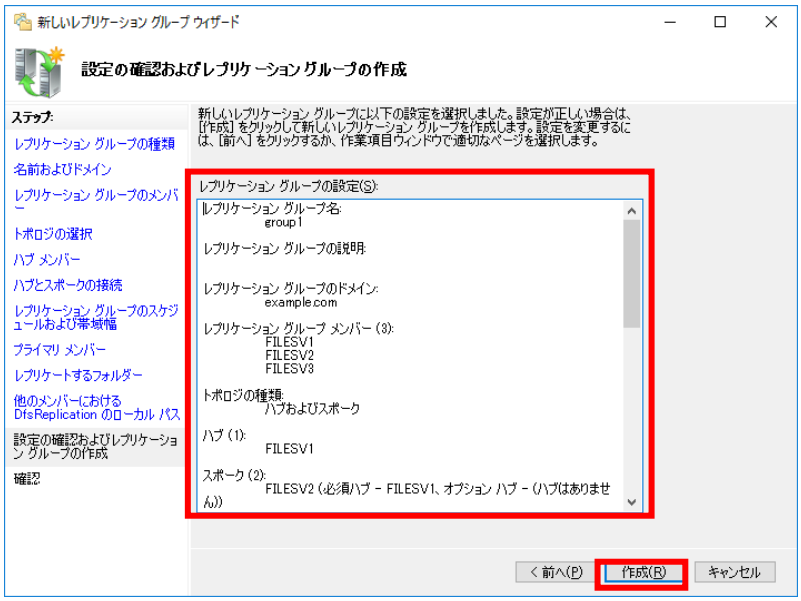
16. [編集] 画面にて、 [メンバーシップの状態] の [有効] を選択し、[フォルダーのローカルパス] を入力します。このフォルダーを読み取り専用のレプリケート フォルダーにする場合は、[選択したレプリケートフォルダーをこのメンバーに対して読み取り専用にする] チェックボックスにチェックを入れ、[OK] をクリックします。



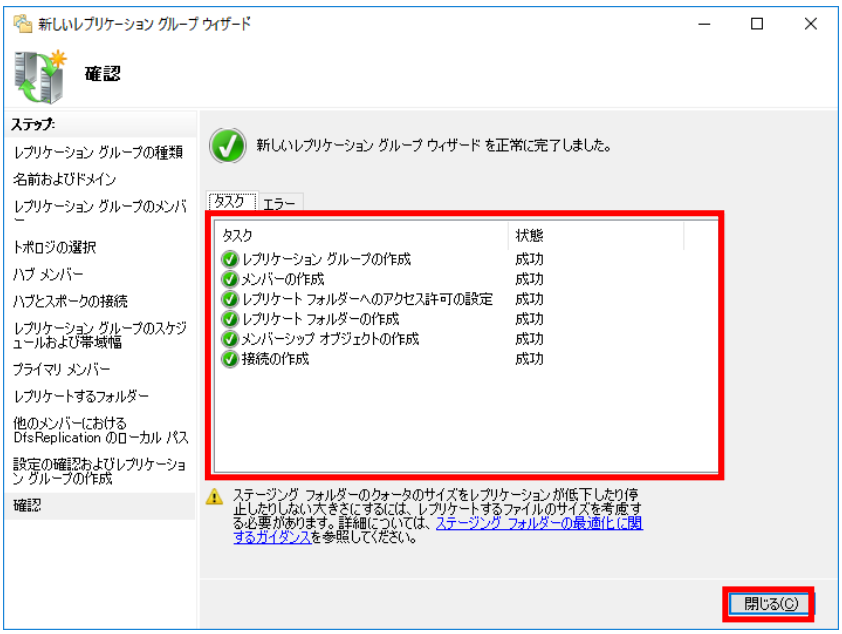
17. [他のメンバーにおける"レプリケートフォルダー名"のローカルパス] 画面に戻り、[メンバーの詳細] にローカルパスが表示され、[メンバーシップの状態] が "有効（読み取り専用）" になっていることを確認します。その後、[ローカルパス] が "<未設定>" になっている他の全てのメンバーについても、同様にローカルパスを設定して、 [次へ] をクリックします。



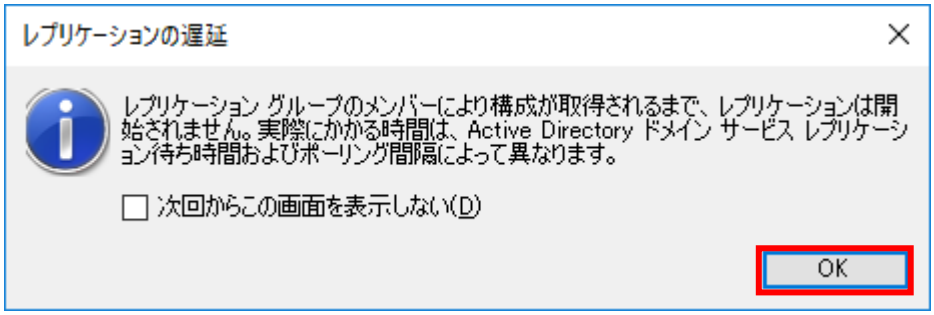
18. [設定の確認およびレプリケーショングループの作成] 画面にて、設定内容を確認し、[作成] をクリックします。



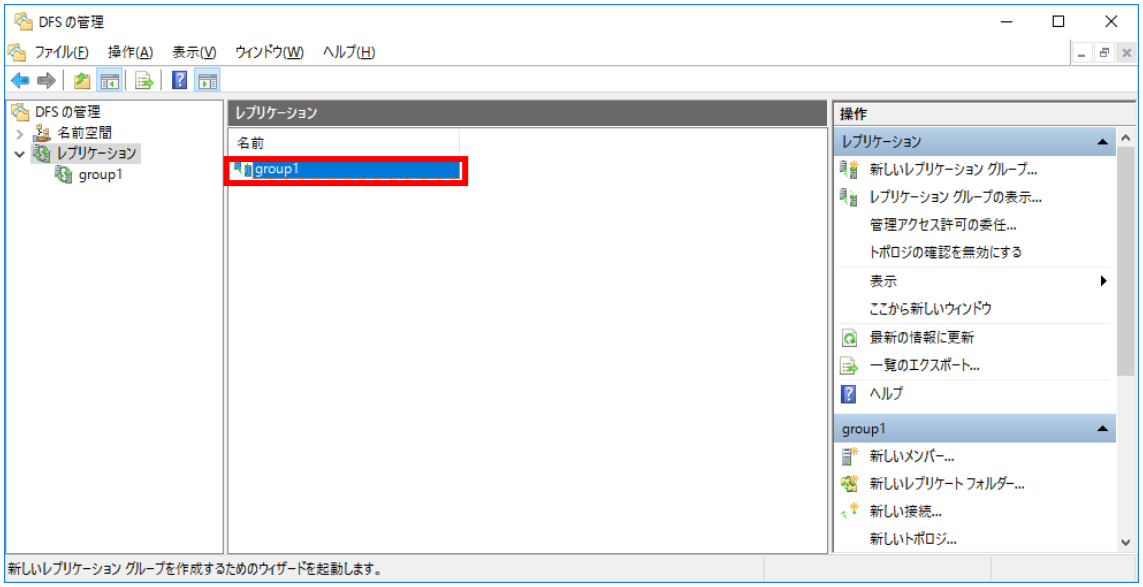
19. [確認] 画面に切り替わり、レプリケーショングループが作成されます。正常に作成されると、[タスク] タブの画面の全項目の状態が "成功" になりますので、[閉じる] をクリックします。作成がエラーとなった場合は、[エラー] タブの画面に、詳細なエラー内容が表示されます。内容を確認の上、設定を見直し、再度作成してください。



20. [閉じる] をクリックすると、下記の [レプリケーションの遅延] 画面が表示されます。[OK] ボタンをクリックして画面を閉じます。



21. [DFS の管理] 画面に、作成したレプリケーショングループが表示されていることを確認してください。初期レプリケーションが自動的に実行されます。

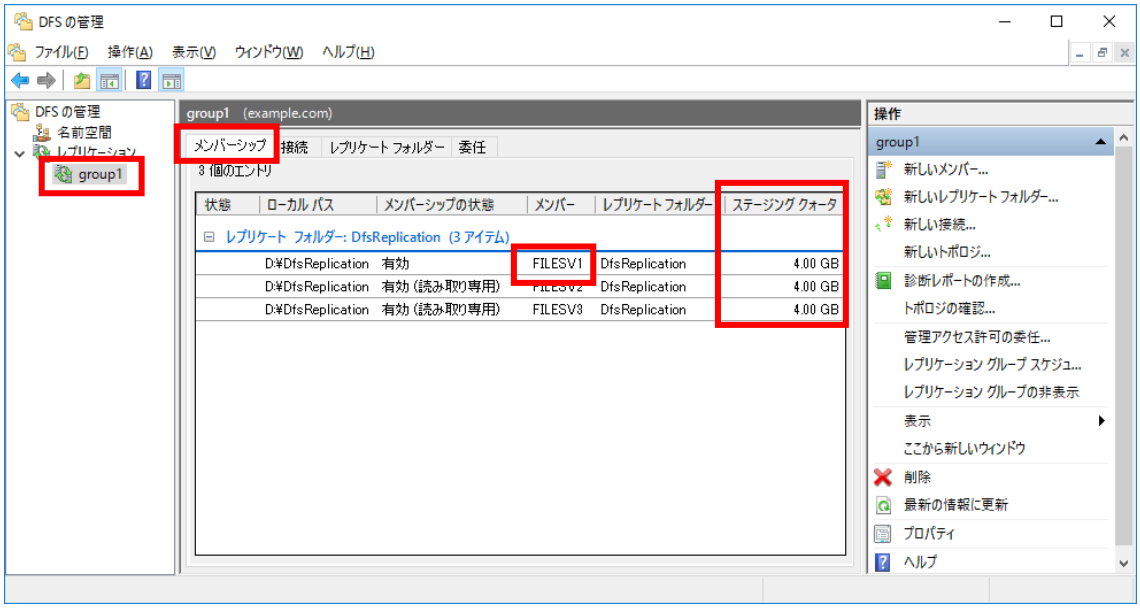


2.4.2.3.2. ステージングフォルダーの設定

DFS レプリケーションでは、レプリケーショングループの他サーバーへのファイル更新反映のために一時的な作業領域としてステージングフォルダーを使用します。

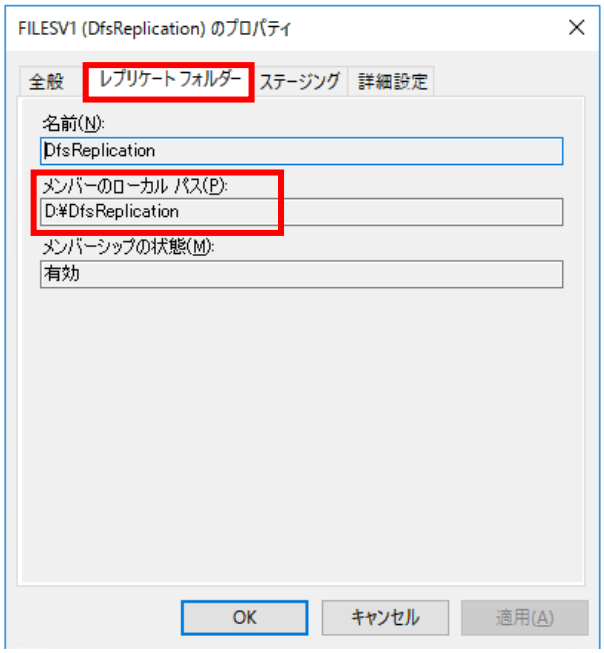
DFS レプリケーションサービスは、ファイルやフォルダーの新規作成や更新が行われた際に、レプリケーション対象のファイルやフォルダーを一旦ステージングフォルダーにコピーします。ステージングフォルダーのサイズは既定値で 4GB となっていますが、レプリケーション対象に非常に大きなファイルが存在する場合など、環境に合わせて最適なパフォーマンスを維持するためにステージングフォルダーのサイズを拡張することができます。
ここではお客様環境に適したステージングフォルダーのサイズを算出し、変更する手順を説明します。

1. FILESV1 にドメインの管理者アカウントでサインインし、管理者メニューから [DFS の管理] を起動します。左ペインより、レプリケーショングループ "group1" を選択した後、中央ペインの [メンバーシップ] タブを選択し、レプリケートフォルダーの一覧を表示します。次にメンバー "FILESV1" を右クリックし、プロパティを表示します。



【補足】
レプリケートフォルダーの一覧にて、現在のステージングフォルダーのサイズが ”ステージングクォータ” の欄に表示されています。

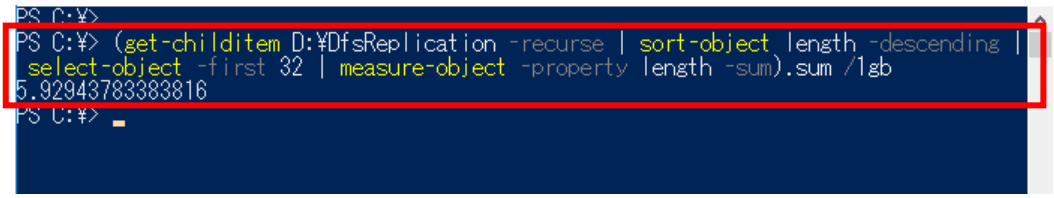
2. プロパティ画面にて、[レプリケート フォルダー] タブをクリックし、”メンバーのローカルパス” に設定されているパスを確認します。



3. FILESV1 の管理者メニューから [Windows PowerShell] を起動して、ステージングフォルダーの情報を取得するために下記のコマンドを実行します。コマンド内の ”メンバーのローカルパス” は、「2.」で確認したパスを指定してください。

> (get-childitem “メンバーのローカルパス” -recurse | sort-object length -descending | select-object -first 32 | measure-object -property length -sum).sum /1gb

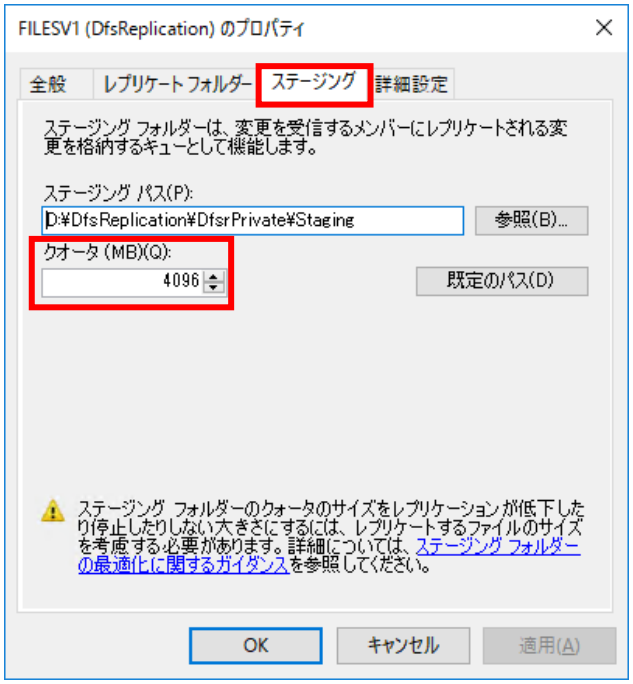
コマンドの実行結果として、お客様環境で必要となるステージングフォルダーのサイズ(GB 単位)が小数値で表示されますので、小数点以下を切り上げて整数値に読み替えてください。
(例：5.92943783383816 → 6 に読み替えます)



上記コマンドで得られた値が、現状のステージングフォルダーのサイズ(GB)よりも小さい場合は、変更は不要のため、これ以降の手順を実施する必要はありません。

4. 「2.」で表示しているプロパティ画面にて、[ステージング] タブを選択します。クォータの設定値に、PowerShell コマンドで取得した整数値×1024 (MB 単位)を設定します。(例:整数値が 6 の場合は 6144 を設定します)

   設定が終わったら、[OK] をクリックし、プロパティ画面を閉じます。

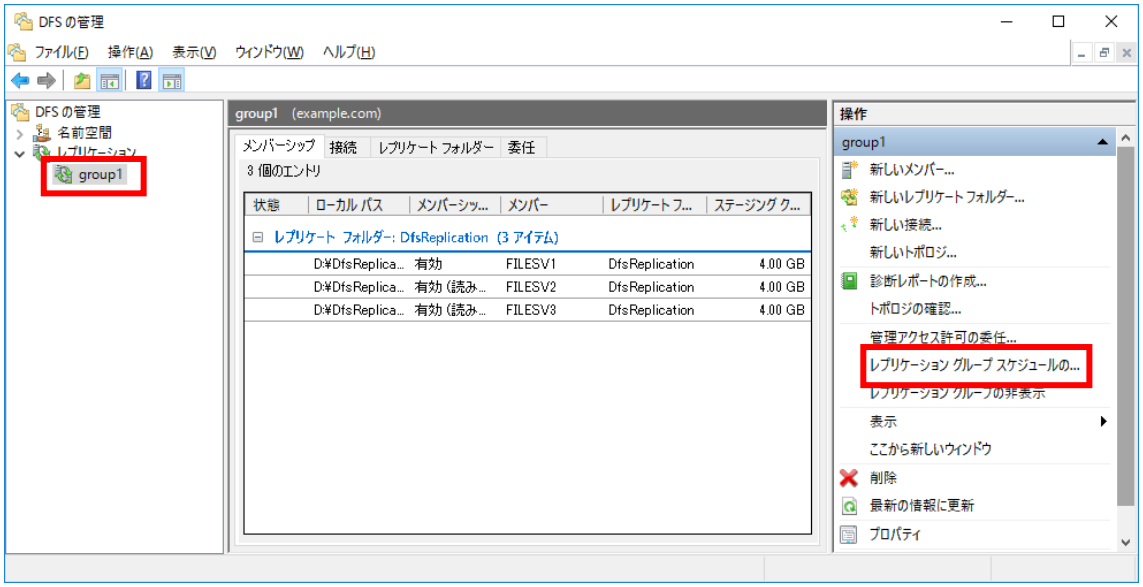


FILESV1 のステージングフォルダーのサイズを変更した場合は、同一のレプリケーショングループに属する各サーバーのステージングフォルダーサイズを合わせてください。なお、FILESV2、FILESV3 のステージングフォルダーのサイズ変更についても、本サーバーのレプリケートフォルダーの一覧画面からメンバーサーバーを選択することにより実施可能です。

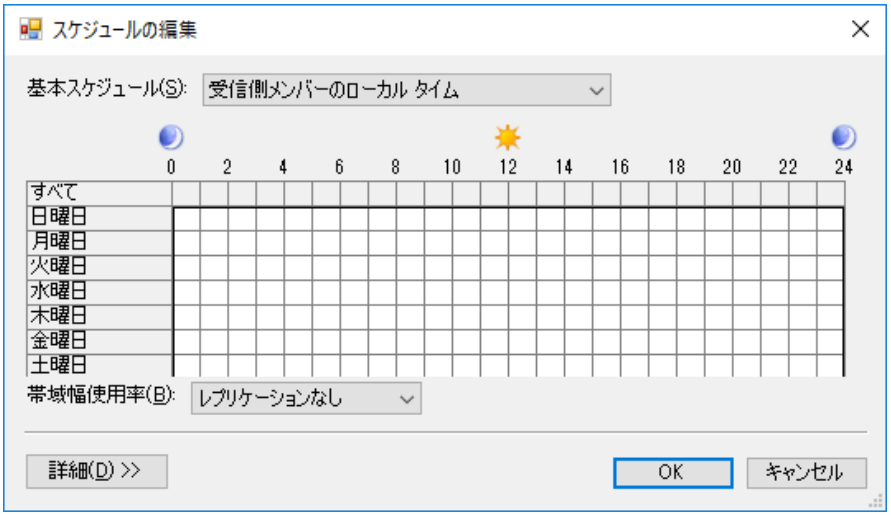
2.4.2.4 レプリケーションのスケジュール

スケジュールにしたがってレプリケーションを実行する場合の設定方法を説明します。

1. FILESV1 の [DFS の管理] 画面にて、ツリーより、スケジュールを編集するレプリケーショングループをクリックし、右ペインの [レプリケーショングループスケジュールの編集] をクリックします。



2. [スケジュールの編集] 画面が表示されますので、スケジュールを設定します。

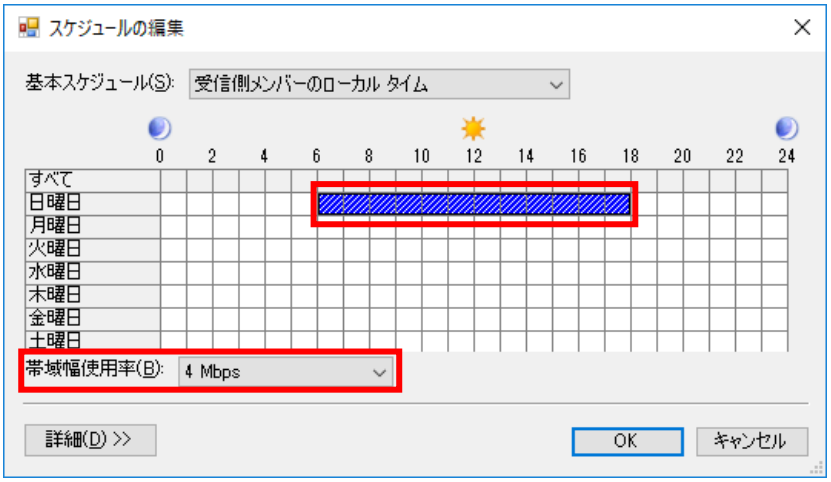


【注意】

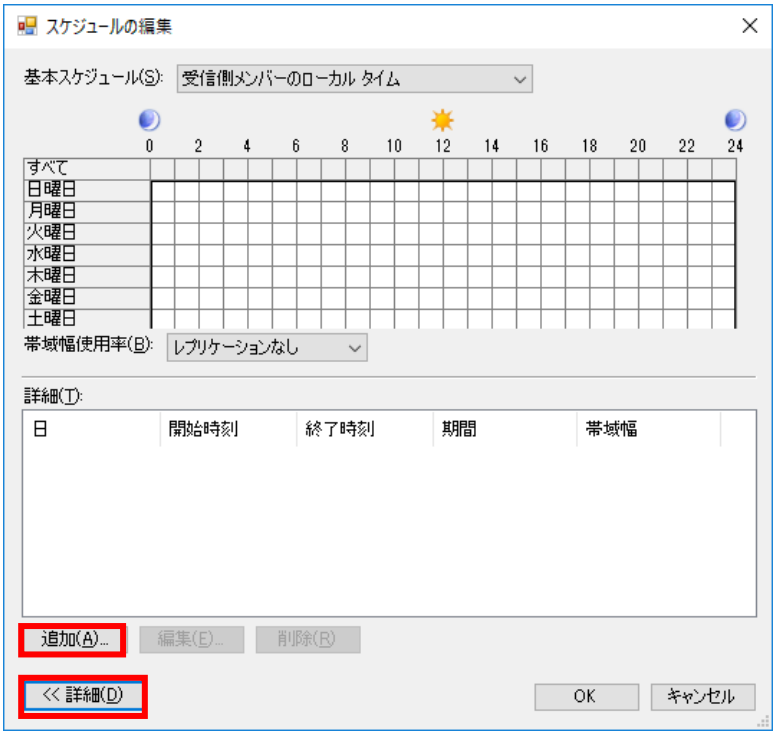
レプリケーショングループの作成ウィザードから直接スケジュールの編集を実行する場合の初期状態は、上記のとおりレプリケーションが全く行われない設定ですが、レプリケーショングループ作成時に [指定した帯域幅を使用して継続的にレプリケートする] を選択した場合の初期値は、すべての曜日の 24 時間に対して最大の帯域を使用する設定となっています。

設定を変更する場合は、すべての曜日に対して適切な設定を行うよう注意してください。

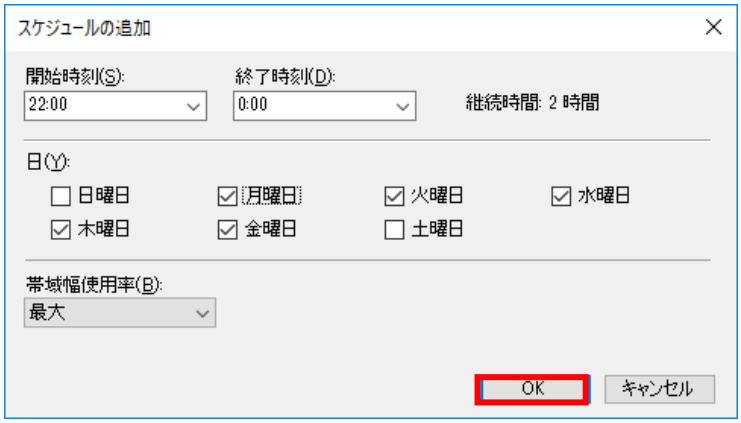
カレンダー表示からレプリケーションを実行するスケジュールを設定する場合は、曜日と時間が表示されているマス目を選択もしくはドラッグして範囲指定をし、 その範囲における帯域使用率を [帯域幅使用率] のプルダウンメニューから選択します。

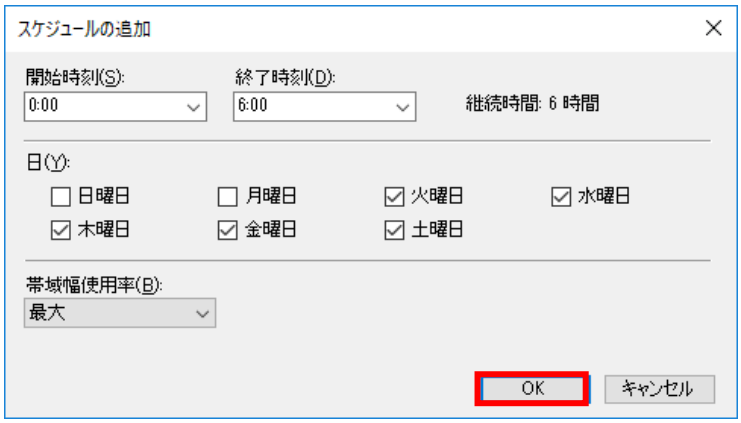


数値の入力にて設定する場合は、[詳細(D) >>] をクリックしてから、[追加] をクリックします。

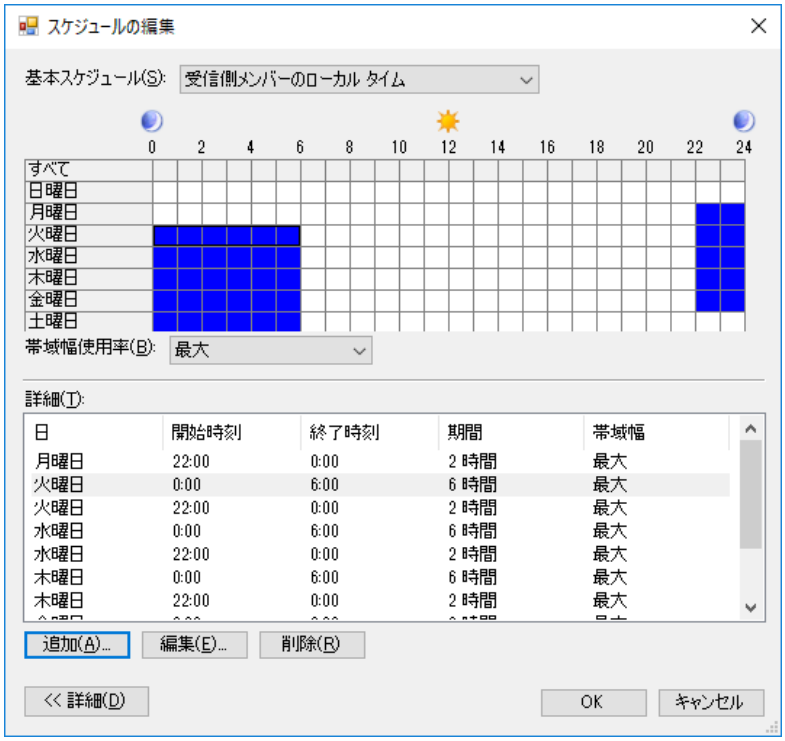


必要に応じて設定を行い、[OK] をクリックして [スケジュールの編集] 画面に戻ります。たとえば、平日の 22 時から翌 6 時までレプリケーションを行う設定とする場合は、以下のように 2 つのスケジュールを追加します。





追加すると、以下のようにカレンダーと詳細画面に設定したスケジュールが表示されます。



3. 設定が終わったら、[OK] をクリックして [スケジュールの編集] 画面を閉じます。

2.4.2.5 DFS レプリケーションの注意事項

- DFS レプリケーションのインストール後、イベントログに「ソース: DFSR イベント ID:6104」が記録される場合があります。このイベントが記録された場合、DFS レプリケーション サービスを再起動する必要があります。DFS レプリケーション サービスを再起動後、「ソース: DFSR イベント ID:6102」が記録されることを確認してください。

- DFS レプリケーションはワークグループ環境では利用できません。必ずドメインに参加した状態でご利用ください。

- DFS レプリケーションの設定を行う際は、必ずドメインの管理者アカウントで実施してください。

- ウイルス対策ソフトウェアやバックアップソフトウェアを使用する場合は、各ソフトウェア ベンダーに問い合わせて、DFS レプリケーションをサポートしていることを必ず確認してください。
  DFS レプリケーションと互換性がないソフトウェアを使用すると、様々な問題が発生する可能性があります。

- レプリケートフォルダーは、NTFS 上に作成する必要があります。

- レプリケーショングループのメンバーサーバーは、同じフォレスト内であれば同じドメイン内でなくてもかまいませんが、異なるフォレストに属するサーバーを設定することはできません。

- ハードリンクとリパースポイントは複製されません。

- データベースファイルのように継続的にオープンされ続けているファイルは複製されません。ファイルがクローズされた後に複製が開始されます。

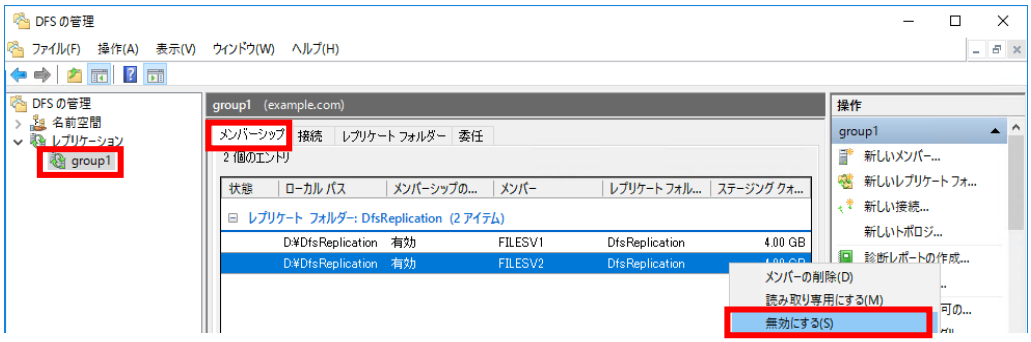
- 読み取り専用のレプリケートフォルダーを有効にすると、レプリケートフォルダーが存在するボリュームの全てのファイルの書き込みオープンおよび新規作成の操作が監視されます。このため、該当ファイルサーバーの性能が低下する可能性があります。

- 新規レプリケーショングループの初期レプリケーションの際、プライマリメンバー上のファイルは他のメンバーサーバー上のファイルよりも優先されます。初期レプリケーション時にプライマリメンバー以外のメンバーサーバーのレプリケートフォルダーにファイルが存在すると、ファイル消失が発生することがありますので、あらかじめ別フォルダーに移動して、空にしておく等の処置が必要です。

- クォータやファイルスクリーンとの共存は可能ですが、レプリケートによってクォータやファイルスクリーンの矛盾が発生すると、複製が失敗し、その後、継続的に複製をリトライするために、システムの性能に問題が発生します。このため、以下の点に注意してください。
  - レプリケートフォルダーにある DfsrPrivate 隠しフォルダーには、レプリケート時の競合やファイル削除による退避ファイルが格納され、フォルダー容量が増大する可能性がありますので、これを考慮してクォータの設定を行ってください。
  - DfsrPrivate 隠しフォルダーには、レプリケート時の競合やファイル削除による退避ファイルが格納されますので、この格納を妨げるようなファイルスクリーンの設定は行わないようにしてください。レプリケートフォルダーにファイルスクリーンを設定する必要がある場合、DfsrPrivate 隠しフォルダーを除外してください。
  - レプリケーションサーバー間では、クォータやファイルスクリーンの設定を一致させる必要があります。

- 計画停電・保守等によりレプリケーショングループに属するサーバーのうち 1 台もしくは複数台をシャットダウンする必要がある場合、特にレプリケーションの停止操作は必要ありません。そのままサーバーのシャットダウンを実行してください。

  DFS の管理画面には以下のようなレプリケーションを無効化するメニューが存在しますが、本操作はレプリケーションの運用を中止する場合に実行します。この操作を行った場合、再度有効化すると初期レプリケーションから実行されますので、使用環境によっては初期レプリケーションが完了するまで非常に長い時間を要すことがあります。



2.4.2.6 DFS レプリケーションの制限事項

- DFS レプリケーションを運用する上で、推奨される各容量は以下となっています。
  ・サーバー上でレプリケートされるすべてのファイルサイズ： 100 TB (テラバイト)
  ・ボリューム毎にレプリケートされるファイル数： 7,000 万ファイル
  ・１ファイルの最大サイズ： 250 GB (ギガバイト)

- 同時に (または短時間内に)、複製されている複数サーバー上の同じファイルに更新処理を行う運用は避けてください。そのような運用では、サーバー間のレプリケーション時に競合が発生し、最も新しい更新以外は破棄されます。この動作はマルチマスタレプリケーションを行う DFS レプリケーションの仕様の動作となりますが、更新が破棄されたプログラム (または利用者) の観点では、意図しないファイル破損に見えることがあります。
  なお、破棄されたファイルはレプリケートフォルダーの配下に存在する『DfsrPrivate¥ConflictAndDeleted』フォルダーに移動されますが、ファイル名は変更されます。元のファイル名との対応は、『DfsrPrivate¥ConflictAndDeletedManifest.xml』ファイルに記録されています。また、『ConflictAndDeleted』フォルダー内に保持できるファイルサイズは、デフォルトで 4096MB になっていますので、破棄されたファイルの合計が上限の 90%を超えた場合『ConflictAndDeleted』フォルダー内のファイルはすべて削除されます。本フォルダーの上限値を変更する場合は、下記【補足】を参照してください。

  このとき、破棄されたファイルは、PowerShell から Restore-DfsrPreservedFiles コマンドを使用してリストアすることもできます。以下に、衝突によって破棄されたファイルすべてを指定のフォルダーにリストアするコマンド例を示します。

  Restore-DfsrPreservedFiles -Path "<レプリケーションフォルダーのパス>
  ¥DfsrPrivate¥ConflictAndDeletedManifest.xml" -RestoreToPath "<リストア先のパス>"

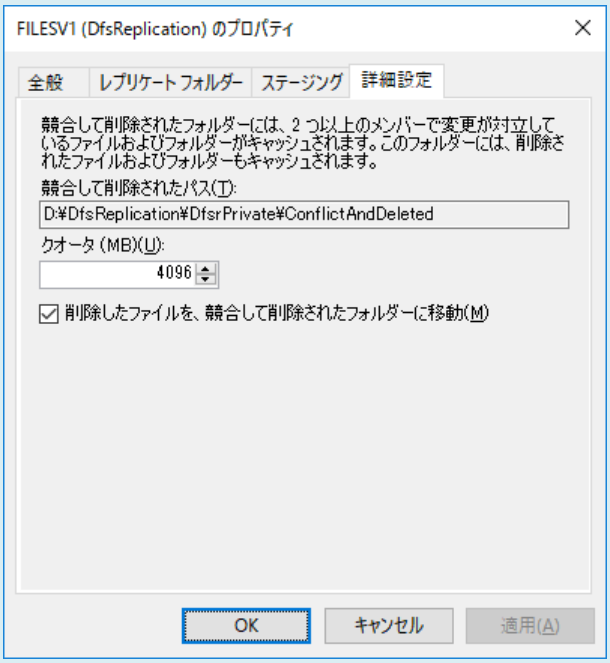
  コマンドの詳細な利用方法については、マイクロソフト社の Web サイトをご参照ください。

  Restore-DfsrPreservedFiles
  http://technet.microsoft.com/ja-jp/library/dn296582.aspx（2026 年 6 月 1 日現在）

【補足】

『ConflictAndDeleted』フォルダー内に保持できる容量は、以下の手順で変更できます。なお、本設定変更は、レプリケーショングループの作成後に実施してください。

1. 管理者メニューから[DFS の管理]を起動します。
2. ツリーに表示される[レプリケーション]を展開し、対象のレプリケーショングループをクリックします。
3. 中央ペインで[メンバーシップ]タブをクリックし、レプリケートフォルダーを表示します。
4. 中央ペインから、『ConflictAndDeleted』フォルダーの容量を変更したいレプリケートフォルダーを右クリックし、[プロパティ]を選択します。
5. プロパティ画面の[詳細設定]タブにて、拡張した『ConflictAndDeleted』フォルダーの容量を入力後、OK をクリックします。



・ 変更後の値が有効になるまでに時間を要すことがあります。直ちに設定を有効にしたい場合は、DFS Replication サービスを再起動してください。

- システムファイルは複製しないでください。
- Encrypting File System (EFS) で暗号化されたファイルは複製できません。

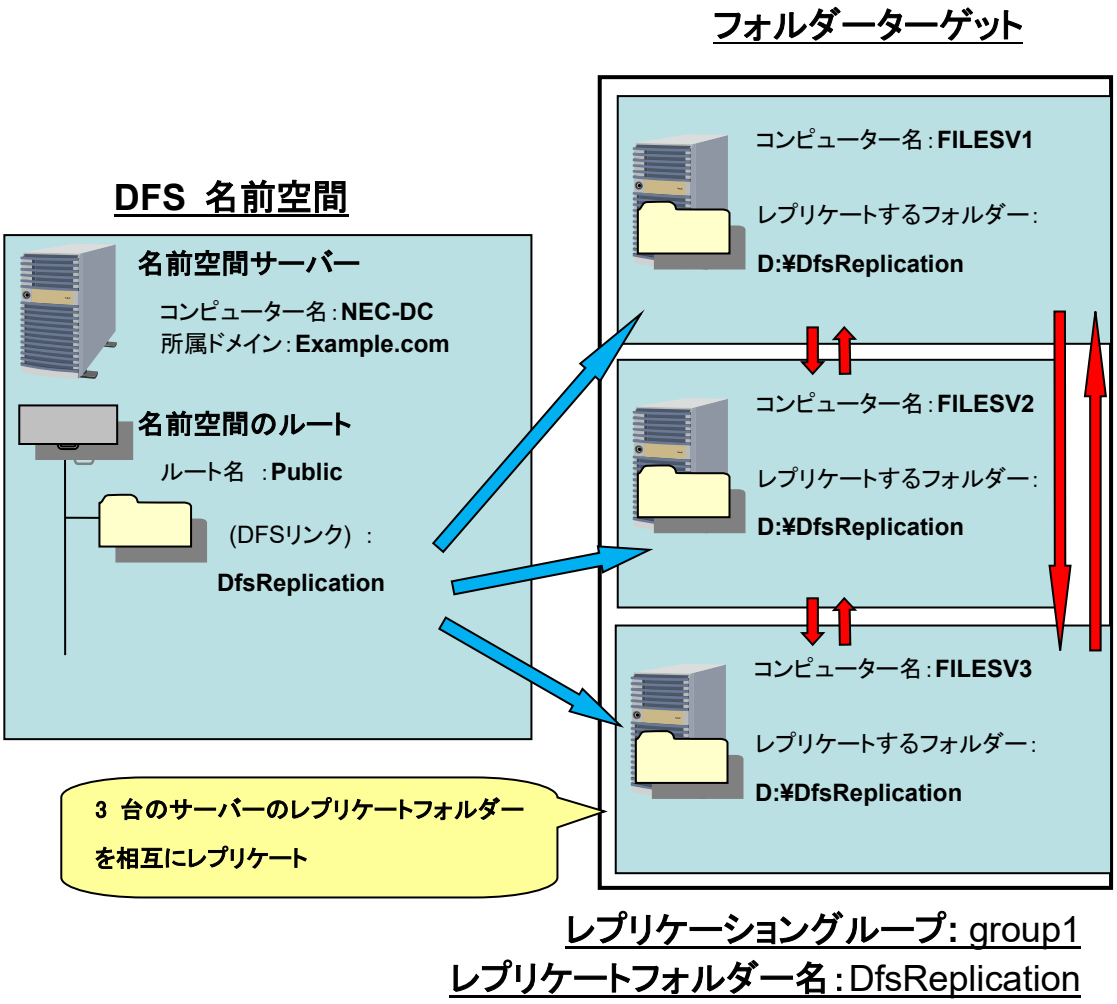
2.4.3 DFS 名前空間と DFS レプリケーションの連携

2.4.3.1 機能概要

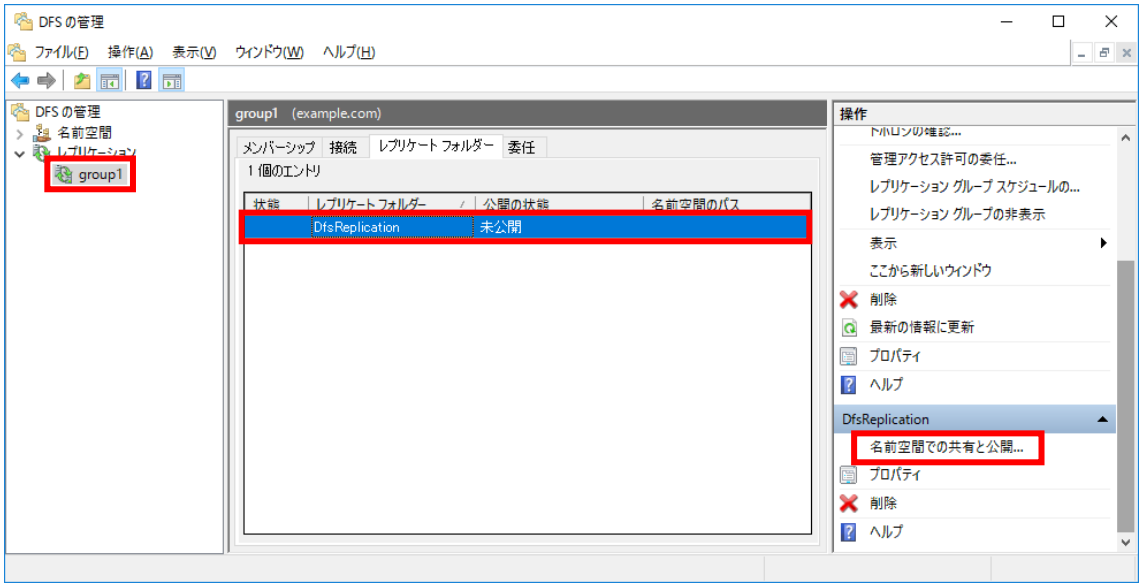
DFS レプリケーションによって相互のレプリケーションが行われているレプリケーショングループのレプリケートフォルダーを共有し、DFS 名前空間にて公開することができます。この設定を行った状態でクライアント PC から DFS 名前空間に公開したレプリケートフォルダーにアクセスすると、ターゲットサーバーを意識することなくアクセスが可能となります。これによって 1 つのターゲットサーバーがダウンしている状況においても他のターゲットサーバーに対して共有名を用いてのアクセスが実現されますので、ファイルサーバーの冗長性を向上させることができます。ただし、1 つのターゲットサーバーのレプリケートフォルダーのみ更新可能とし、他のターゲットサーバーのレプリケートフォルダーを読み取り専用にしている環境では、本設定により読み取り専用のレプリケートフォルダーにアクセスが割り当てられる場合がありますので、ファイルの更新が必須となる運用を行う場合、本設定との共存は推奨いたしません。

2.4.3.2 名前空間での共有と公開

レプリケーショングループのレプリケートフォルダーを共有し、DFS 名前空間にて公開する方法を説明します。ここでは、あらかじめ FILESV1、FILESV2、FILESV3 のそれぞれのサーバーに存在する D:¥DfsReplication フォルダーを相互にレプリケートするレプリケーショングループ（group1）と、ドメインベースの DFS 名前空間（¥¥Example.com¥Public）が存在している環境を、例に説明します。



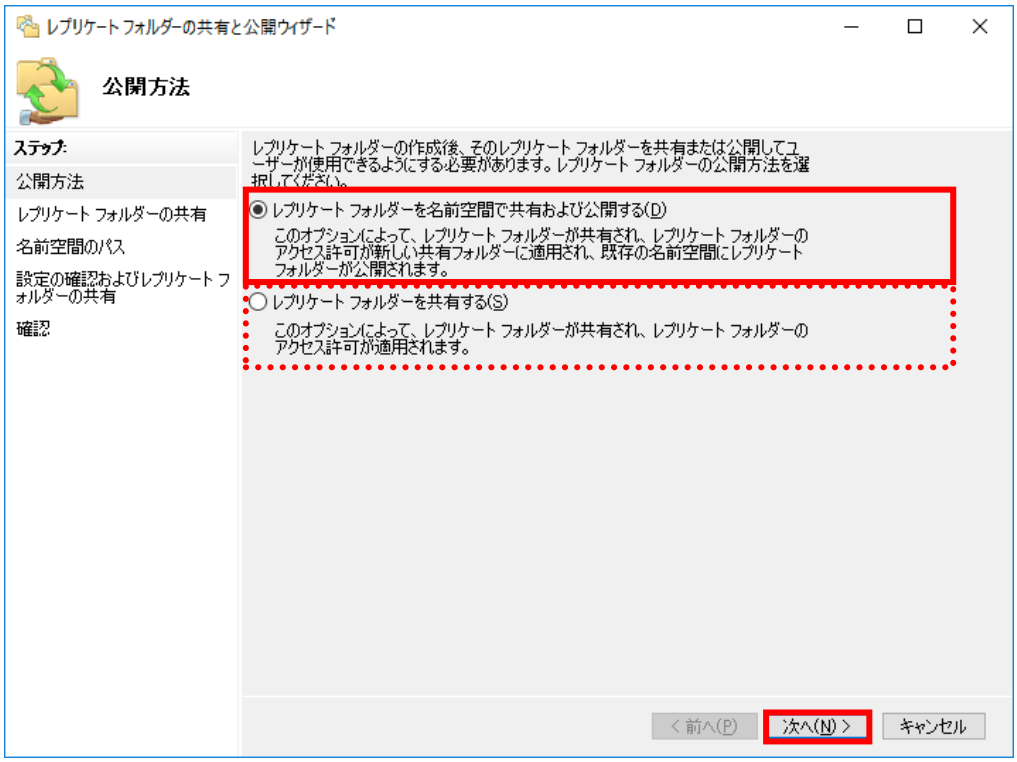
1. FILESV1 の [DFS の管理] 画面にて、ツリーより、レプリケーショングループをクリックします。中央ペインで [レプリケートフォルダー] タブをクリックし、[レプリケートフォルダー] が「DfsReplication」 となっているエントリを選択します。右ペインの [名前空間での共有と公開] をクリックします。



2. [レプリケートフォルダーの共有と公開ウィザード] が起動します。レプリケートフォルダーの公開方法として、以下のいずれかを選択して、[次へ] をクリックします。

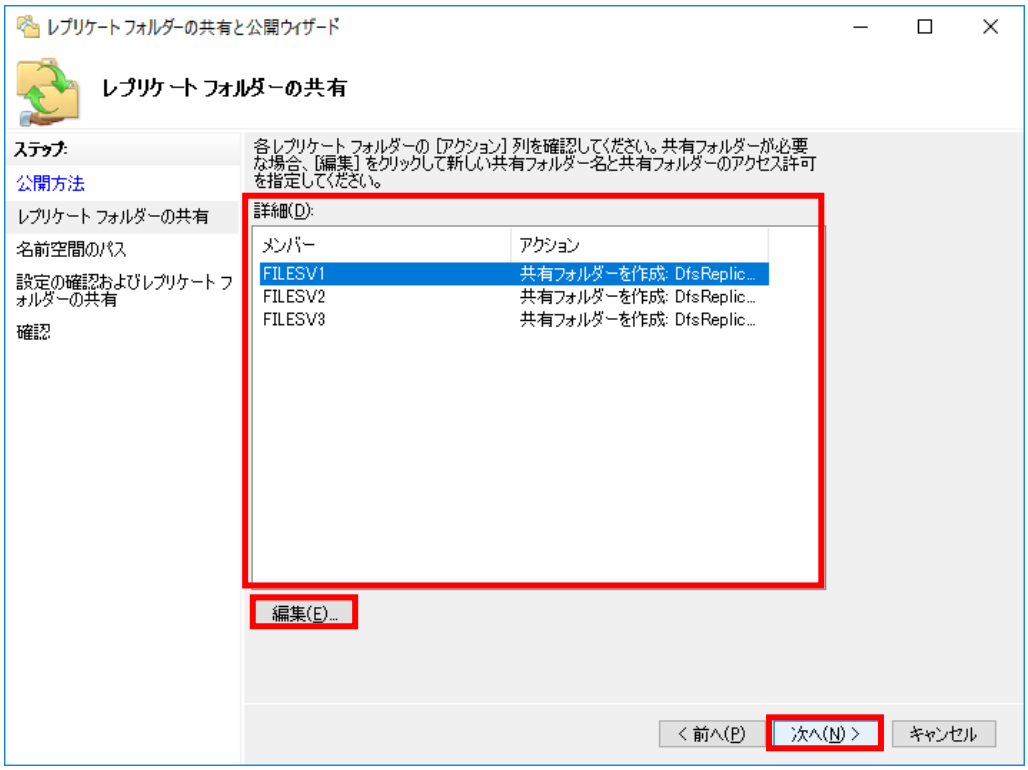
   - **[レプリケートフォルダーを名前空間で共有および公開する]** :
     レプリケートフォルダーを共有し、DFS 名前空間にも公開します。
   - **[レプリケートフォルダーを共有する]** :
     レプリケートフォルダーの共有のみを行い、DFS 名前空間には公開しません。

   ここでは、[レプリケートフォルダーを名前空間で共有および公開する] を選択します。

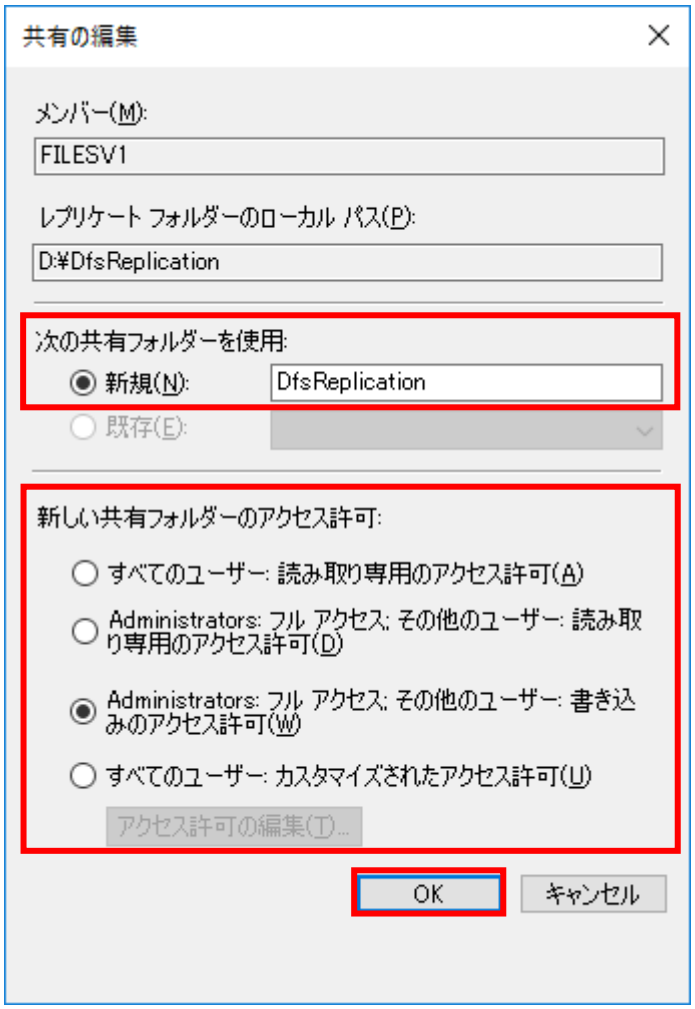


3. [レプリケートフォルダーの共有] 画面にて、 [詳細] の [アクション] 列を確認してください。 [共有フォルダーを作成] となっている場合は、現在共有フォルダーは作成されておらず本操作にて作成が行われますので、それぞれのメンバーに対して [編集] をクリックし、新しい共有フォルダー名と共有フォルダーのアクセス許可を設定します。

   設定が完了したら、[次へ] をクリックしてください。



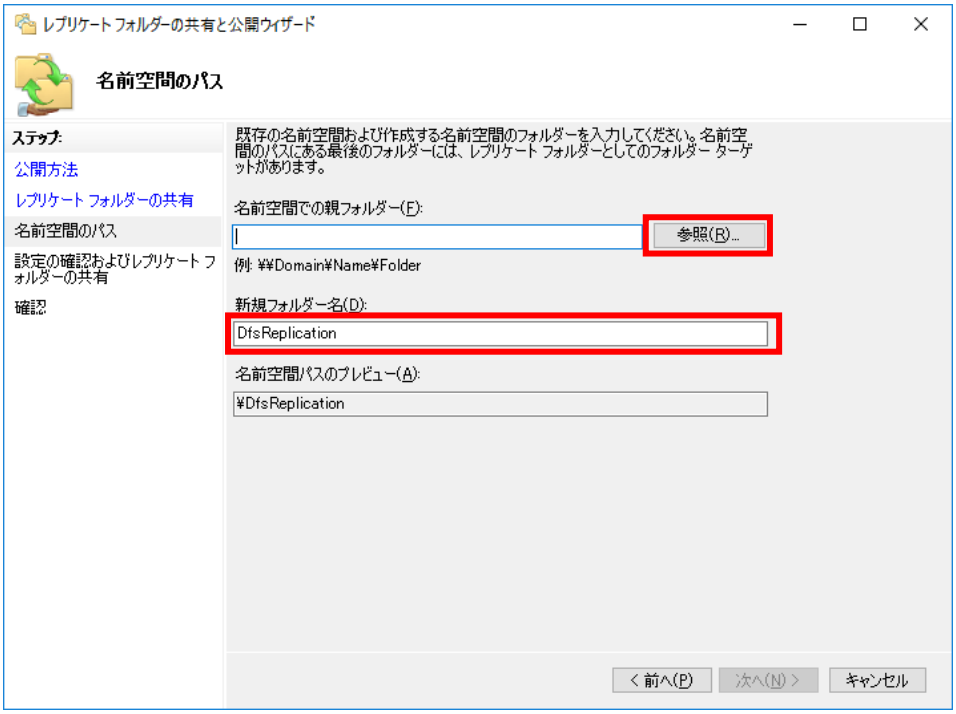
[編集] をクリックすると、[共有の編集] 画面が表示されます。[次の共有フォルダーを使用] は [新規] が選択されていますので、必要に応じて共有フォルダー名を入力します。



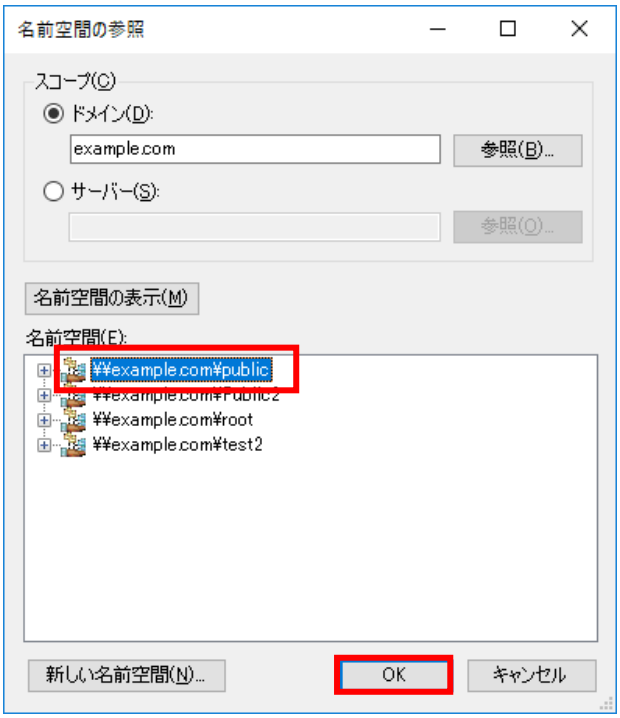
[新しい共有フォルダーのアクセス許可] にてアクセス許可をカスタマイズする場合は、[すべてのユーザー: カスタマイズされたアクセス許可] を選択し、[アクセス許可の編集] をクリックします。[共有のアクセス許可] 画面が表示されますので、アクセス許可を編集してください。

編集が終了したら [OK] をクリックしてください。[レプリケートフォルダーの共有] 画面に戻ります。

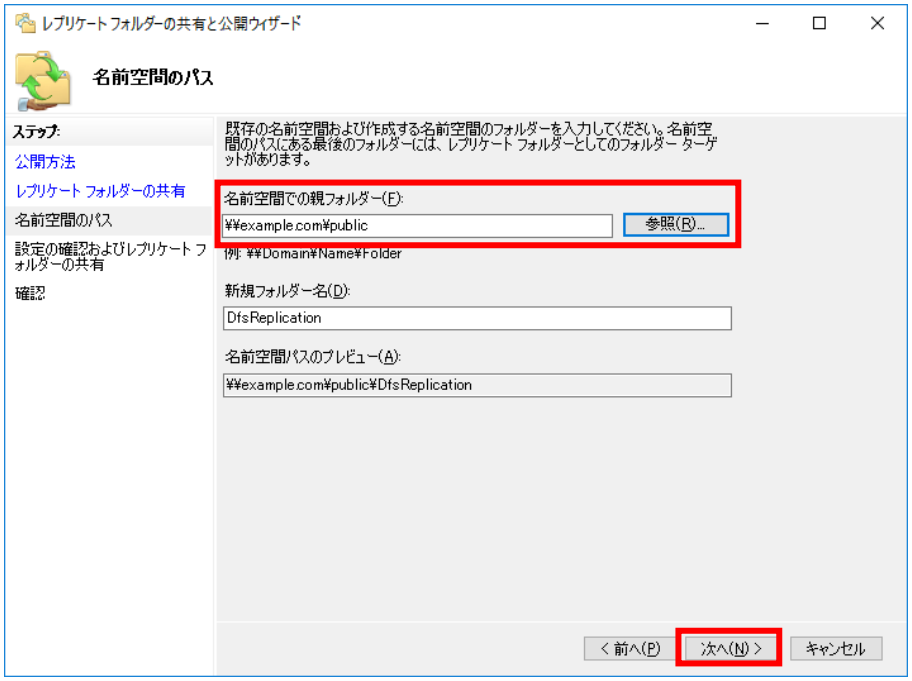
4. [名前空間のパス] 画面にて、名前空間における DFS リンク名を [新規フォルダー名] に指定します。その後、 [参照] をクリックし、名前空間におけるルートを指定します。



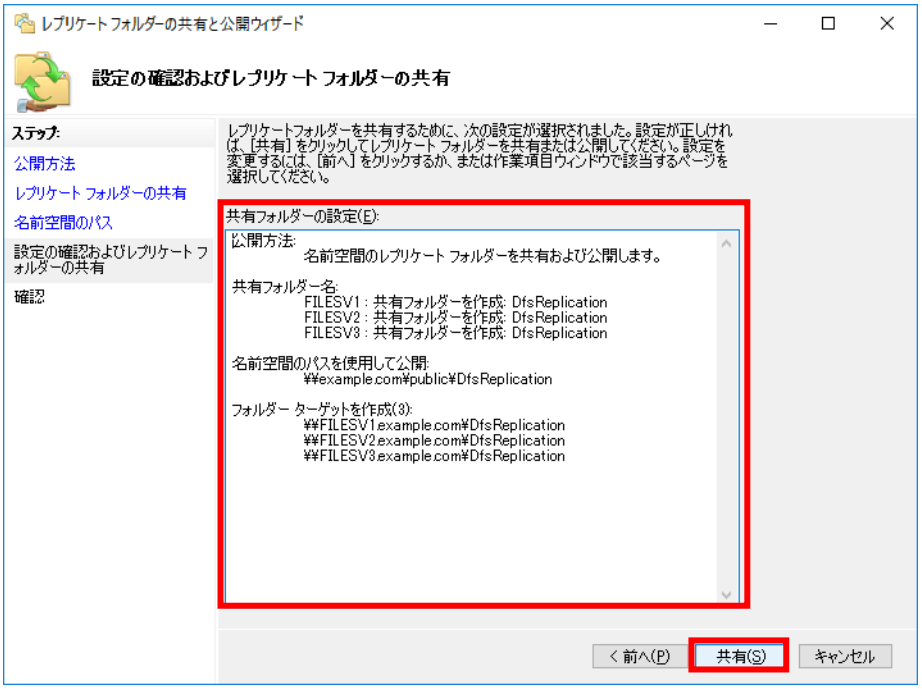
5. [名前空間の参照] 画面の [名前空間] にて、レプリケートフォルダーを公開する名前空間を選択して、[OK] をクリックします。



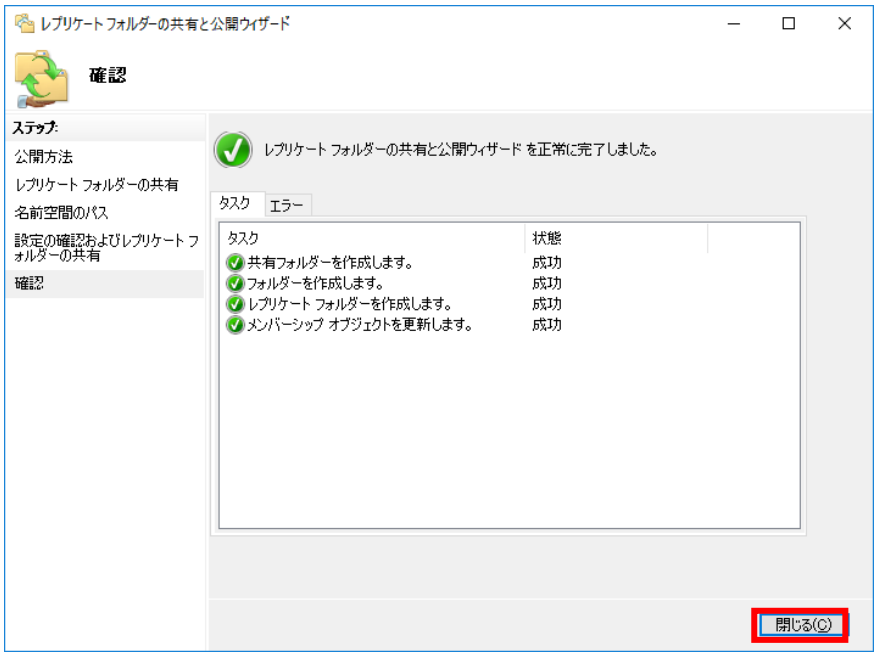
6. [名前空間のパス] 画面に戻りますので、 [名前空間での親フォルダー] の表示内容を確認し、 [次へ] をクリックします。



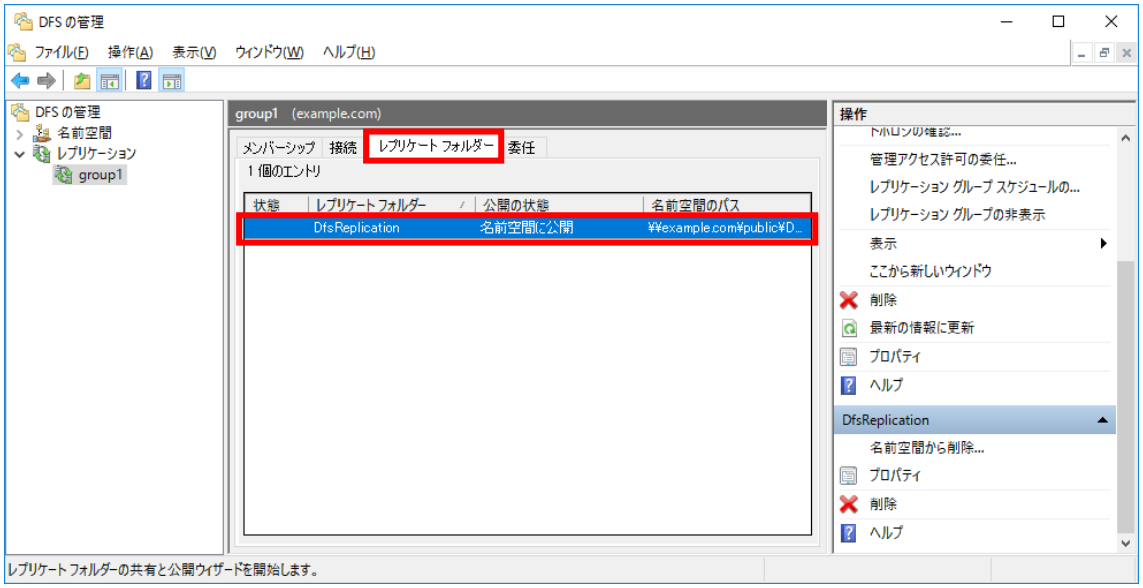
7. [設定の確認およびレプリケートフォルダーの共有] 画面を確認し、設定内容が正しい場合は、[共有] をクリックします。



8. [確認] 画面に切り替わり、レプリケートフォルダーの共有と公開が行われます。正常に完了すると、[タスク] タブの画面の全項目の状態が "成功" になりますので、[閉じる] をクリックします。共有や公開がエラーとなった場合は、[エラー] タブの画面に、詳細なエラー内容が表示されます。内容を確認の上、設定を見直し、再度設定してください。



9. [DFS の管理] 画面にて、中央ペインの [レプリケートフォルダー] タブの [公開の状態] が "名前空間に公開" と表示されていることを確認します。



3 iStorage NS を運用する

- **iStorage NS** の管理
- 運用中の設定変更について
- **NIC** チーミングを設定する
- **Windows Server** バックアップ

3.1 iStorage NS の管理

iStorage NS を管理する方法について説明します。

3.1.1 共有フォルダーのログオン監視

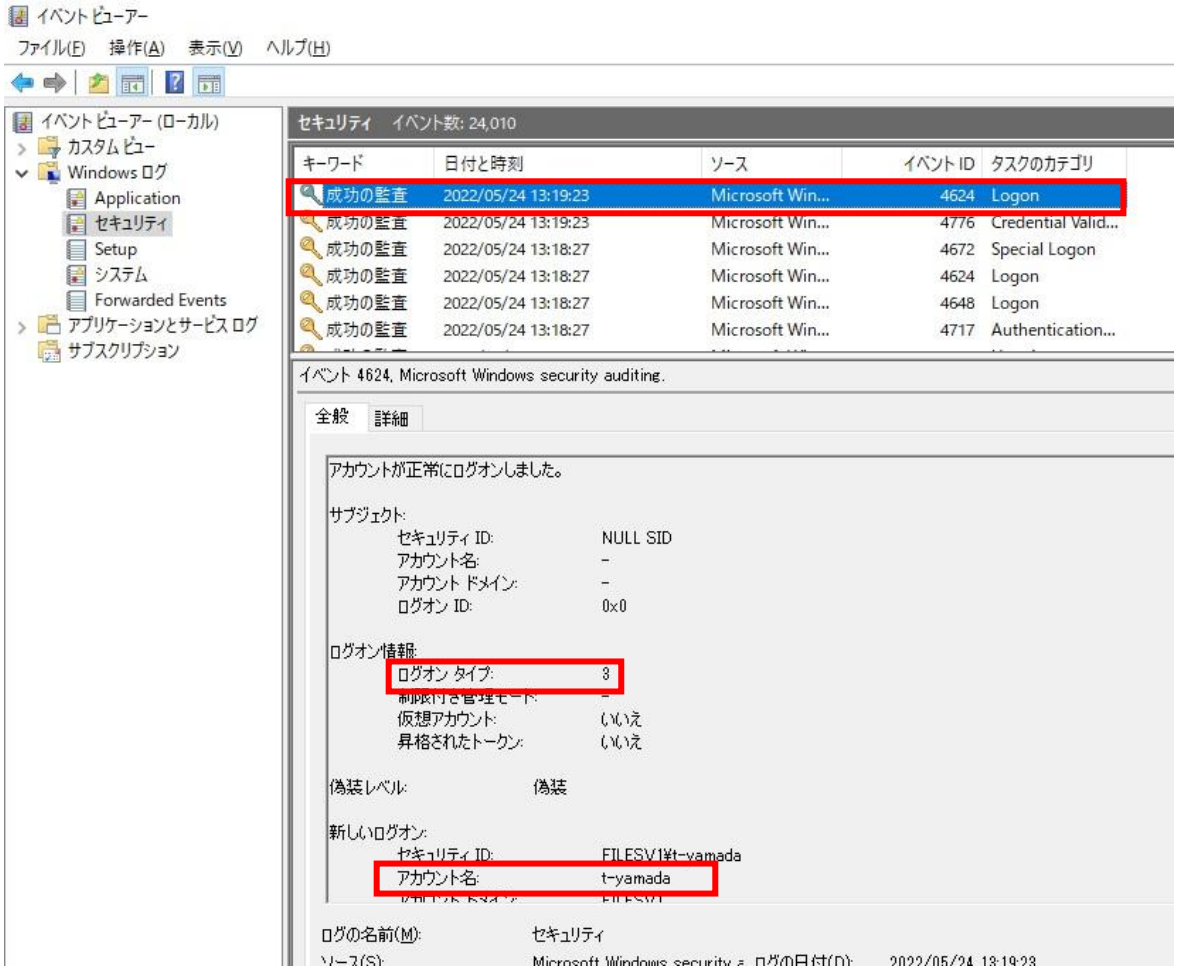
iStorage NS に記録されたセキュリティのイベントログから、どのユーザーが、いつ共有フォルダーにアクセス（ログオン）したかを監視することができます。以下に、ログオン監視の確認手順を説明します。

1. 管理者メニューの [イベントビューアー] をクリックします。

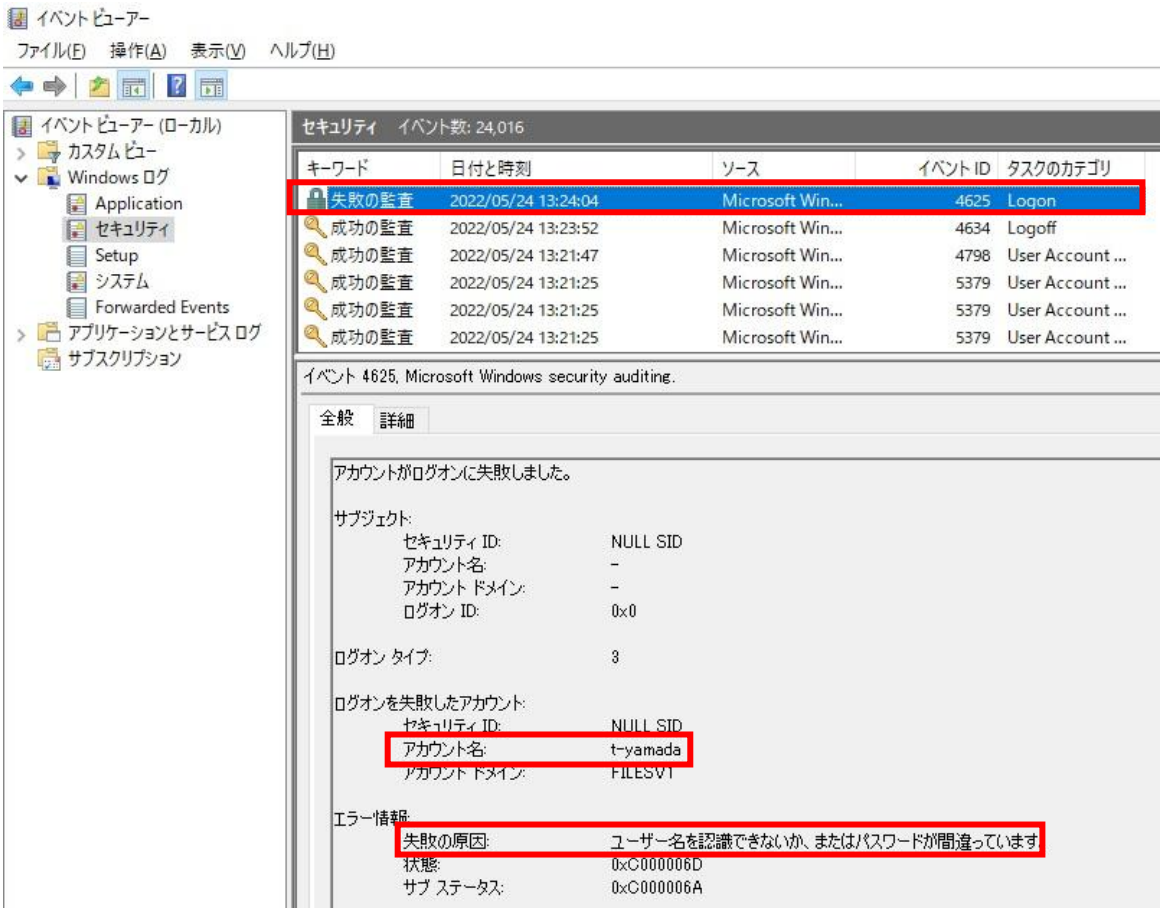
2. イベントビューアー左ペインの [Windows ログ] を展開し、[セキュリティ] をクリックします。

3. 中央ペインに表示されるログオンのイベントログをクリックし、 [全般] タブに表示される、共有フォルダーへのアクセス（ログオン）の記録を確認します。

   下記の例では、t-yamada というユーザーが、2022/05/24 13:19:23 に共有フォルダーへアクセス（ログオン）したことを示しています。ネットワーク経由でアクセスした場合は、ログオンタイプ 3 が記録されます。



また、下記の例では、t-yamada というユーザーが、誤ったパスワードを入力したため、2022/05/24 13:24:04 に共有フォルダーへのアクセス（ログオン）に失敗したことを示しています。誤ったパスワードを入力した場合、またはサーバーが認識できないユーザーアカウントでログオンしようとした場合は、「失敗の原因： ユーザー名を認識できないか、またはパスワードが間違っています。」というエラー情報が記録されます。



3.1.2 共有フォルダーのファイルアクセス監視

企業内に設置されたファイルサーバー上には、重要な機密情報が格納されたファイルが存在しています。通常、企業内では内部統制として、ファイルサーバーにはアクセス許可の設定が行われており、業務上で必要な従業員にのみ許可されています。
しかしながら、業務上でファイルの閲覧・更新・削除の操作が許可されている従業員が悪意を持つと、ファイルの情報漏えい、改ざん、あるいは、ファイル削除などの不正行為を防ぐことができません。
このため、ファイルサーバーの運用において、誰が・いつ・どのファイルにアクセスしたかの証跡を日々記録しておき、前述のような事故が発生した場合に、証跡情報から該当ファイルへのアクセスを特定できるように備えておくことが重要になります。また、従業員に対し、ファイルサーバー上のファイルアクセスが常に監視されていることを周知することで、従業員の不正行為を未然に抑止する効果も期待できます。

iStorage NS に搭載されているオペレーティングシステムは、共有フォルダー経由でのファイルアクセスを監視し、誰が・いつ・どのファイルにアクセスしたかをログファイルに残す、監査ログ機能を有しています。

iStorage NS の出荷時設定では、上記のような記録を残す監査ログは有効化しておりません。これは、監査ログの書き込みによるディスク負荷や、システムドライブ容量の圧迫等によりシステムの基本動作に影響を与える可能性が考えられるためです。このため、監査ログ採取が必要なお客様は、システムへの影響を考慮し、必要に応じて監査ログを有効化してください。これにより、Windows のセキュリティイベントログに、下記のファイルアクセスの監査ログを記録することができます。

- Windows クライアント PC から SMB 共有へのファイルアクセス
- iStorage NS 上のプログラムからローカル HDD へのファイルアクセス

なお、NFS クライアントから NFS 共有へのファイルアクセスについては監査ログの採取ができませんので、ご注意ください。また、ファイルシステムが FAT32 の場合は、監査ログの設定に必要となる、システムアクセス制御リスト (SACL) をサポートしていないため、監査ログの採取ができません。

Windows のセキュリティイベントログに記録された監査ログは、イベントビューアーにて確認してください。また、市販の監査ログ管理アプリケーションを利用すると、効率よく監査ログの確認・管理が可能です。

3.1.2.1 監査ログの有効化

監査ログの有効化は、下記①～④の手順にて実施します。

① イベントログの設定変更
② 監査ポリシーのバックアップ
③ 監査ポリシーの設定
④ システムアクセス制御リスト (SACL) の作成

なお、各手順は、リモートデスクトップ経由、または、コンソールにて、管理者権限を持つユーザーでサインインして実行してください。

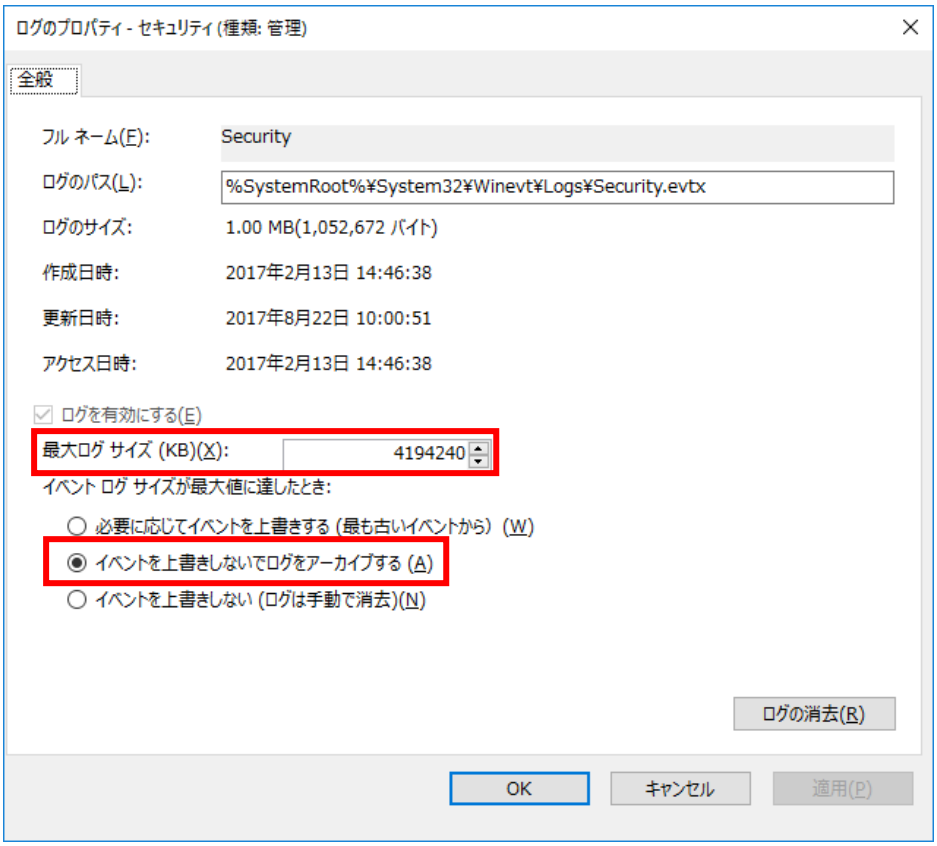
① イベントログの設定変更

セキュリティイベントログの出荷時設定のサイズは 20MB (20480KB) です。監査ログを有効化すると、セキュリティイベントログが大量に記録されます。このため、ログファイルのサイズの拡大を実施してください。推奨サイズは、4GB (4194240 KB) ですが、イベントログをテキストファイル形式や CSV 形式でファイルに出力し、テキストエディタ等で参照する場合につきましては、ツールによっては大きなファイルを読み込めないことがありますので、ツールで読み込める程度のサイズとしてください。(OS 付属のメモ帳で参照する場合、100MB を目安にしてください)

また、必要に応じて、古いイベントログファイルを上書きせずに別ファイルに残す (アーカイブする) 設定を実施してください。

【ログサイズ拡大とアーカイブ設定の手順】

1. [管理者メニュー] から [イベントビューアー] を開きます。
2. [Windows ログ] - [セキュリティ] を右クリックし、[プロパティ] をクリックします。
3. [最大ログサイズ(KB)] 欄にファイルサイズを入力します。4GB にする場合は 4194240 (KB)と記入します。100MB にする場合は、102400(KB)と記入します。(64KB 単位で入力してください)
4. ログファイルを古い方から上書きせずに別ファイルに残す（アーカイブする）場合は、[イベントログサイズが最大値に達したとき] 欄を、デフォルトの [必要に応じてイベントを上書きする (最も古いイベントから)] から、[イベントを上書きしないでログをアーカイブする] に変更してください。



アーカイブされたファイルは、C:¥Windows¥System32¥Winevt¥Logs フォルダー配下に下記のような名前で作成されます。ファイル名には年月日時分秒の値が含まれます。

Archive-Security-YYYY-MM-DD-HH-MM-SS-NNN.evtx

【注意】
アーカイブされたファイルは自動的に削除されず、増える一方になります。 放置すると C ドライブの空き容量が無くなり運用に支障が発生します。このため、アーカイブする設定を実施した場合は、定期的に古いファイルを削除する、もしくは、別の場所に移動するようにしてください。

② 監査ポリシーのバックアップ

ファイルアクセス監視を実施するためには監査ポリシー設定を出荷時状態から変更する必要があります。しかしながら、監査ポリシーを一括で出荷時状態に復元する方法は用意されていません。
このため、監査ポリシーの変更作業を開始する前に、下記の手順で、出荷時状態の監査ポリシー設定のバックアップを実施してください。バックアップデータを作成しておくと、後で監査ポリシーを簡単に復元することができます。

【バックアップ手順】

1. 管理者権限の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下記のコマンドを実行します。

```
auditpol /backup /file:c:¥NEC¥auditpol_default.csv
```

上記コマンドの“/file:”の後ろはバックアップファイルの出力先のファイルパスです。本ファイルに監査ポリシーのバックアップデータが保存されます。出力先ファイルパスには、任意のパス名を指定できます。

③ 監査ポリシーの設定

ファイルアクセスの監査を行うには、監査ポリシーの [オブジェクトアクセス] カテゴリの配下にある 2 つのサブカテゴリ [ファイル システム] と [ハンドル操作] を有効化する必要があります。

【監査ポリシーの設定手順】

1. 管理者権限のコマンドプロンプトを起動します。
2. 現在の監査ポリシーの設定状況を確認するため、下記のコマンドを実行します。

```
auditpol /get /category:*
```

3. 上記 2 のコマンドの結果表示を確認します。出荷時状態では下記の赤文字のように [ファイル システム] と [ハンドル操作] が 「監査なし」になっています。

```
------------------------------   --------
カテゴリ/サブカテゴリ             設定
------------------------------   --------
(中略)
オブジェクト アクセス
  ファイル システム               監査なし
  レジストリ                     監査なし
  カーネル オブジェクト           監査なし
  SAM                           監査なし
  証明書サービス                 監査なし
  生成されたアプリケーション     監査なし
  ハンドル操作                   監査なし
(後略)
```

4. 監査ポリシーを変更するため、下記２つのコマンドを実行します

   auditpol /set /subcategory:"ファイル システム" /success:enable /failure:enable

   auditpol /set /subcategory:"ハンドル操作" /success:enable /failure:enable

   各コマンドが成功すると「コマンドは正常に実行されました。」と表示されます。

5. 監査ポリシーの変更結果を確認するため、再度上記 2 と同じコマンドを実行し、下記のような結果表示になることを確認します。[ファイル システム] と [ハンドル操作] が 「**成功および失敗**」になっている場合は、正しく設定変更が行われています。

```
------------------------------  --------
カテゴリ/サブカテゴリ            設定
------------------------------  --------
(中略)
オブジェクト アクセス
  ファイル システム             成功および失敗
  レジストリ                    監査なし
  カーネル オブジェクト         監査なし
  SAM                           監査なし
  証明書サービス                監査なし
  生成されたアプリケーション    監査なし
  ハンドル操作                  成功および失敗
(後略)
```

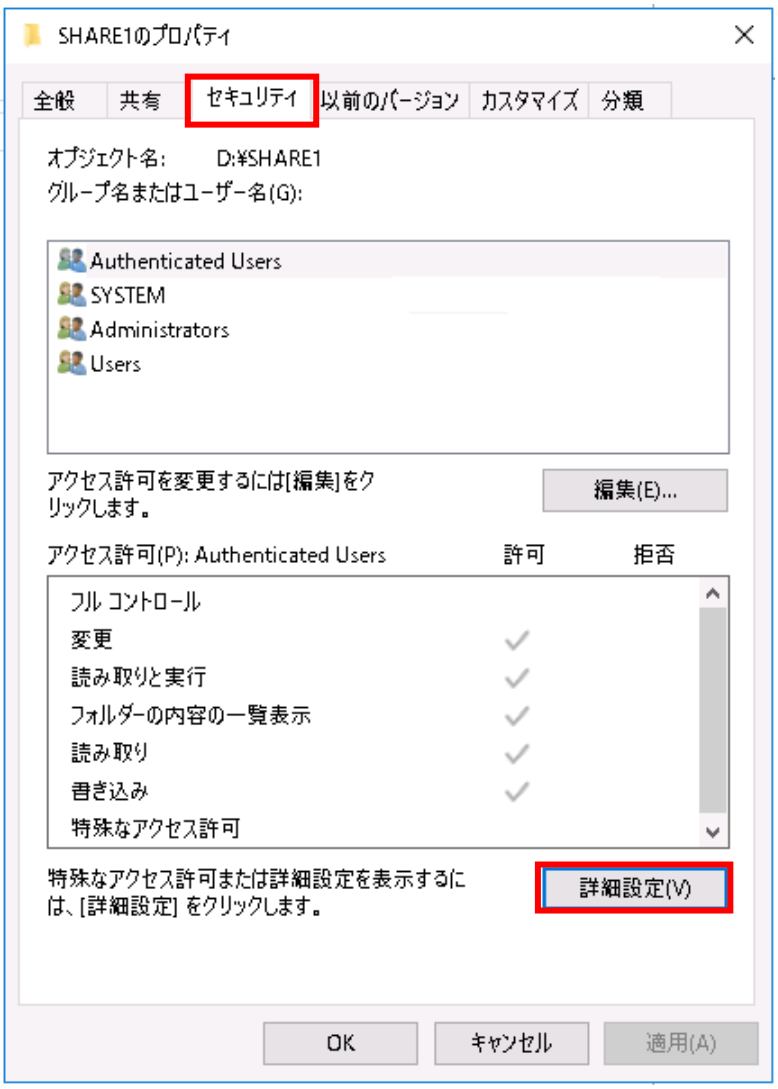
④ システムアクセス制御リスト (SACL) の作成

ファイルアクセス監視を行うには、③の監査ポリシーの設定に加え、監視対象のファイル/フォルダーに対して、システムアクセス制御リスト(SACL) の作成を行う必要があります。設定手順は下記の通りです。なお、複数のファイルに対して監査設定を行う必要がある場合は、上位のフォルダーに監査設定を行い、継承設定を行うことをお勧めします。

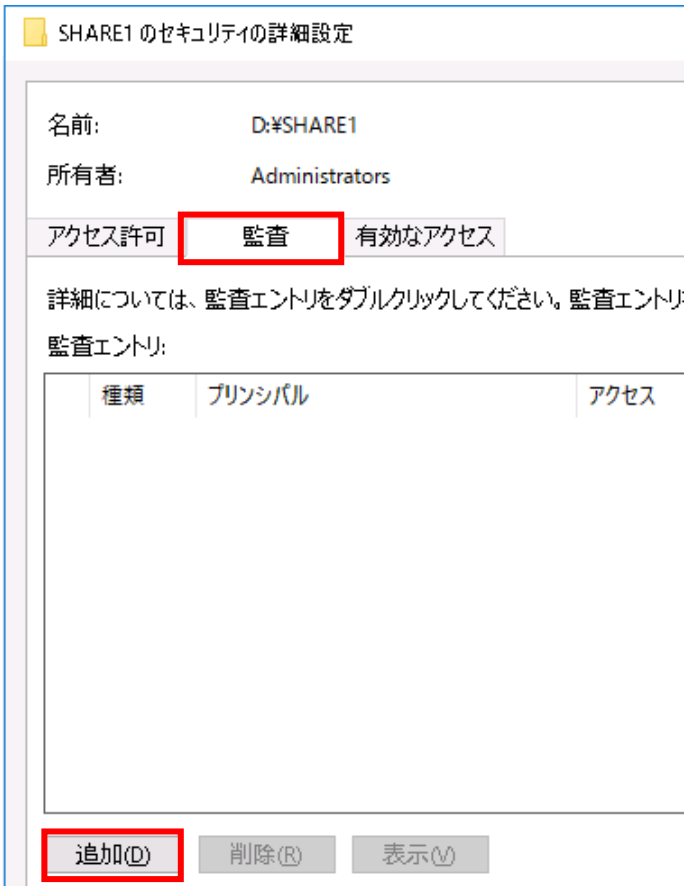
【システムアクセス制御リスト (SACL) の作成手順】

1. [管理者メニュー] よりエクスプローラーを起動し、ファイルアクセス監視の対象とするフォルダーまたはファイルを右クリックして、[プロパティ] をクリックします。

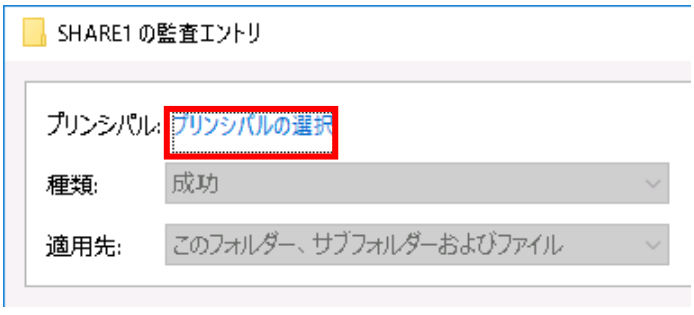
2. [～のプロパティ] 画面で [セキュリティ] タブをクリックし、[詳細設定] ボタンをクリックします。



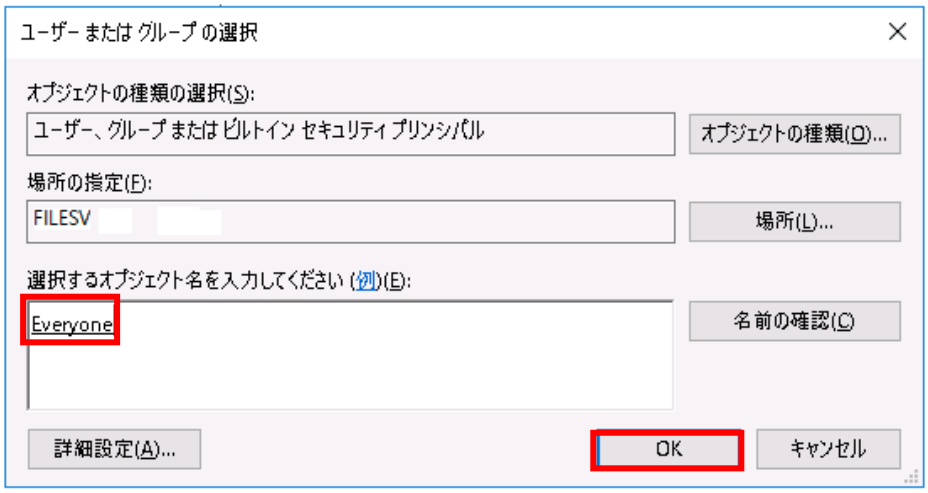
3. [～のセキュリティの詳細設定] 画面で、[監査] タブをクリックし、[追加] ボタンを押します。



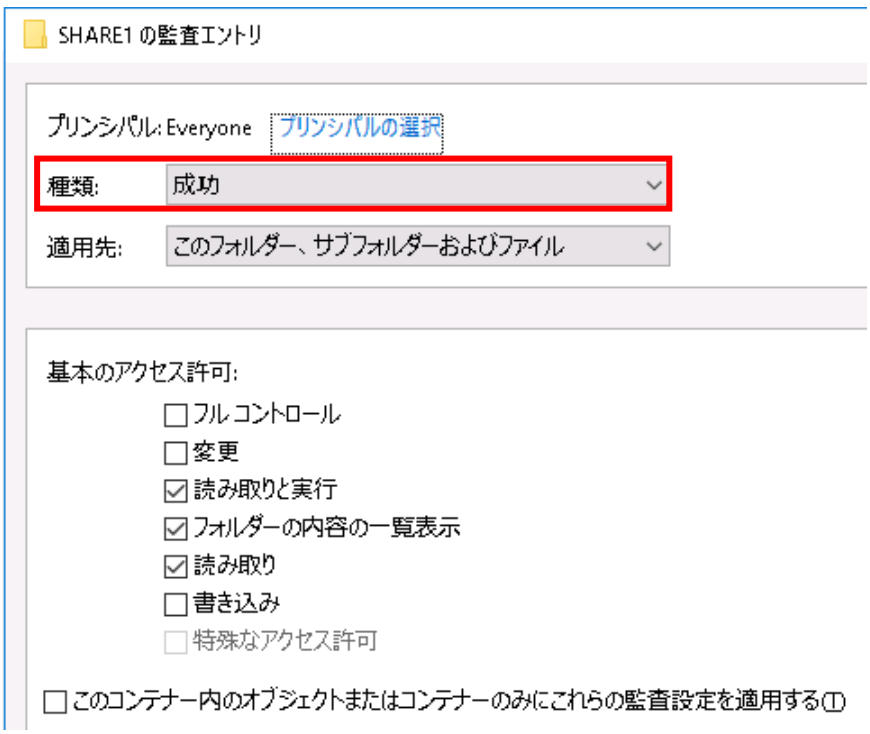
4. [～の監査エントリ] 画面で、[プリンシパルの選択] をクリックします。



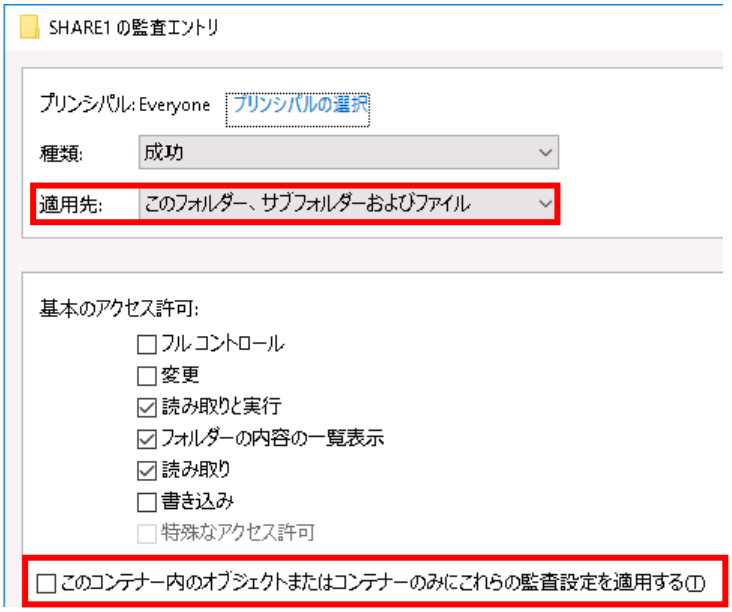
5. [ユーザーまたはグループの選択] 画面で、”Everyone”と記入し、[OK] をクリックします。ここでは、記録対象のユーザー/グループを指定します。”Everyone” は全ユーザーを意味し、Administrator も含みます。代わりに、特定のユーザー/グループを指定することもできます。



6. [種類] 欄 は既定では [成功] が選択されていますが、成功した操作だけではなく、失敗した操作についても監視する必要がある場合は、本欄を [すべて] に変更します。失敗した操作だけを監視する場合は、本欄を [失敗] に変更します。
情報漏えい者、ファイル改ざん者、ファイル削除者を特定する場合は [成功] を、不正アクセスを監視する場合は [失敗] を選択します。

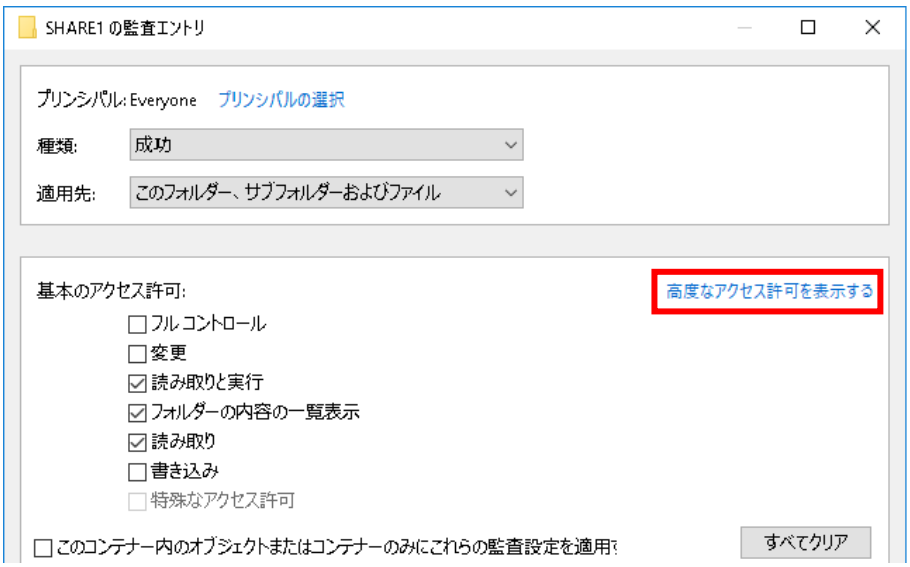


7. (フォルダーの場合のみ) [～の監査エントリ] 画面に、[適用先] 欄が存在します。本欄は、監査エントリをこのフォルダー配下のどの範囲に適用するかの選択となり、既定では、このフォルダー配下の全てに継承する [このフォルダー、サブフォルダーおよびファイル] が選択されています。



画面下部の [このコンテナー内のオブジェクトまたはコンテナーのみにこれらの監査設定を適用する] 欄のチェックボックスは、直下のファイル／サブフォルダーのみに本監査エントリを適用し、それより下への継承を行わない場合にチェックします。

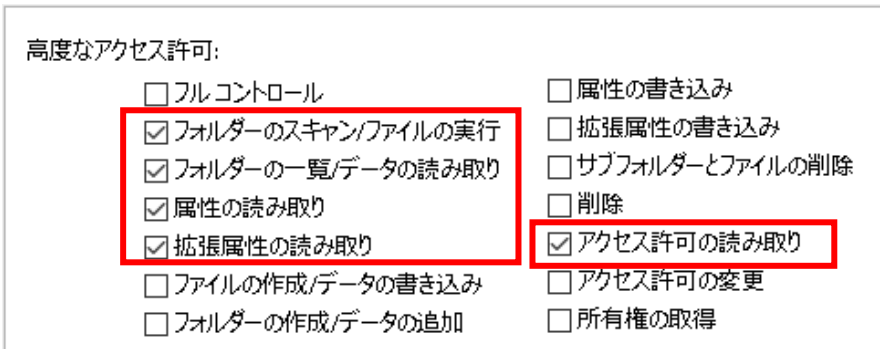
8. [～の監査エントリ] 画面に、[基本のアクセス許可] 欄があります。本欄は、どのような操作を行った場合に監査ログに記録するのか指定します。 [基本のアクセス許可] は、一部の表示が省略された簡易的な表示となりますので、全ての項目を表示するために [高度なアクセス許可を表示する] をクリックしてください。



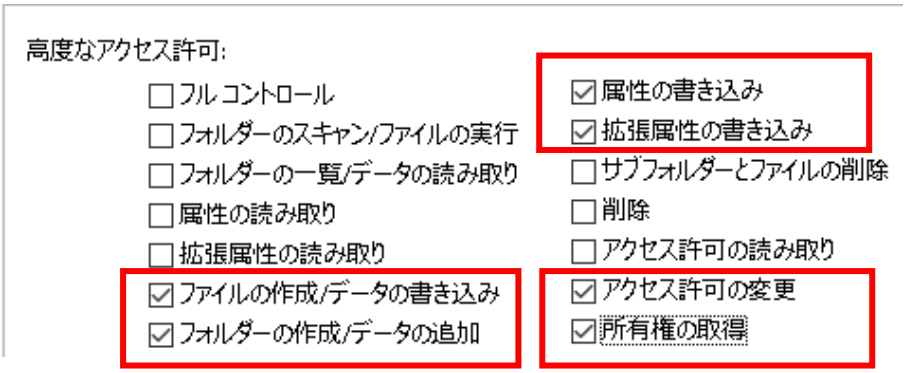
[高度なアクセス許可] 欄のチェックボックス一覧に、監査の必要があるファイル操作に応じて、チェックを入れてください。
以下に、下記４つの設定例を記載します。

・読み込み系操作の監査（情報漏えい者を特定する場合）
・書き込み系操作の監査 (ファイル改ざん者を特定する場合)
・削除操作の監査 (ファイル削除者を特定する場合)
・全ファイル操作の監査 (上記３つの全ての情報含む)

【読み込み系操作の監査】
情報漏えい者の特定のために、読み取り系操作を監査する場合は、下記のようにチェックを入れます。

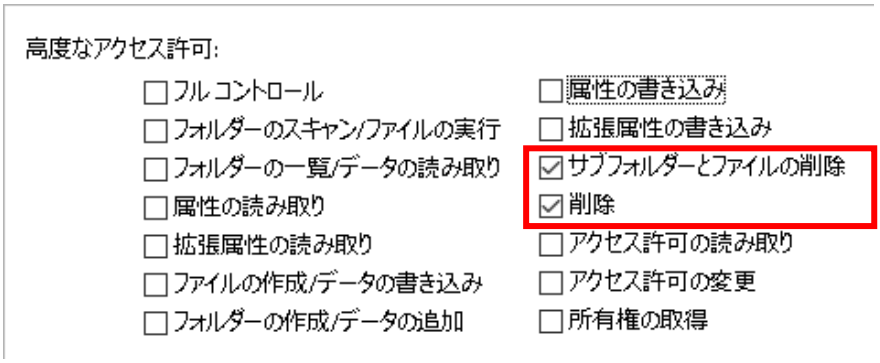


【書き込み系操作の監査】
ファイル改ざん者の特定のために、書き込み系操作のみを監査する場合は、下記のようにチェックを入れます。



【削除操作の監査】

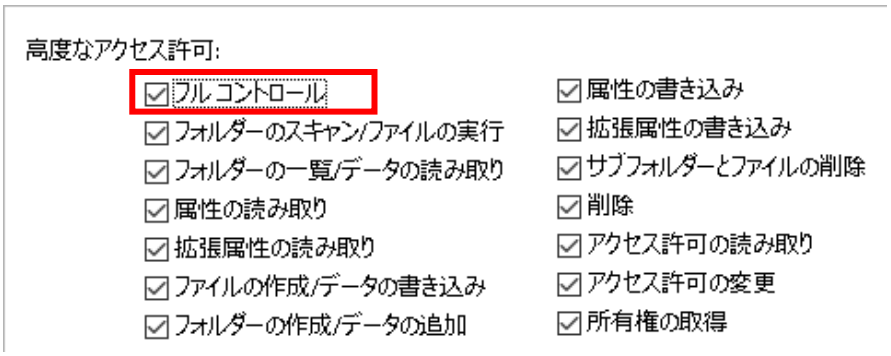
ファイル削除者の特定のために、削除操作のみを監査する場合は、下記のようにチェックを入れます。



※対象がファイルの場合、上記の[サブフォルダーとファイルの削除] は表示されません。

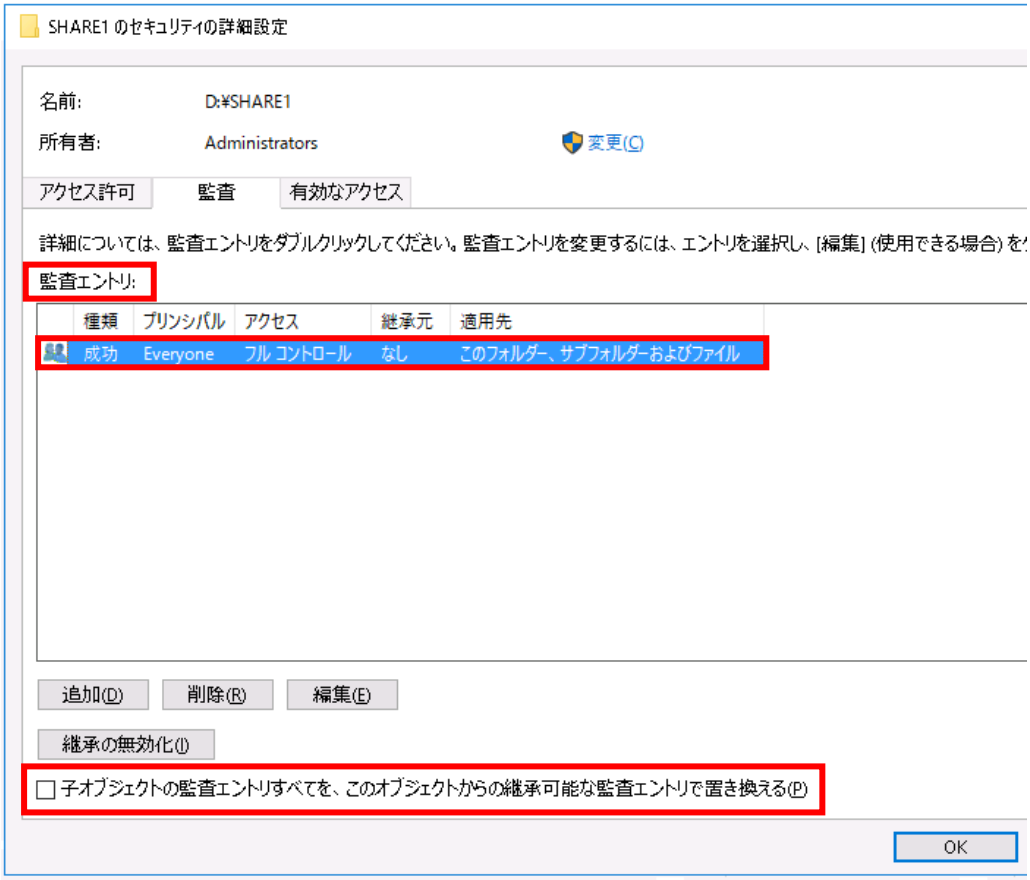
【全ファイル操作の監査】

全てのファイル操作を監査する場合は、下記のように [フルコントロール] にチェックを入れます。[フルコントロール] をチェックすると、他の全項目もチェックされます。



9. [～の監査エントリ] 画面で、[OK]をクリックします。

10. [～のセキュリティの詳細設定] 画面で、[監査エントリ] の一覧に、手順 3～9 の操作で追加した監査エントリが追加されていることを確認してください。

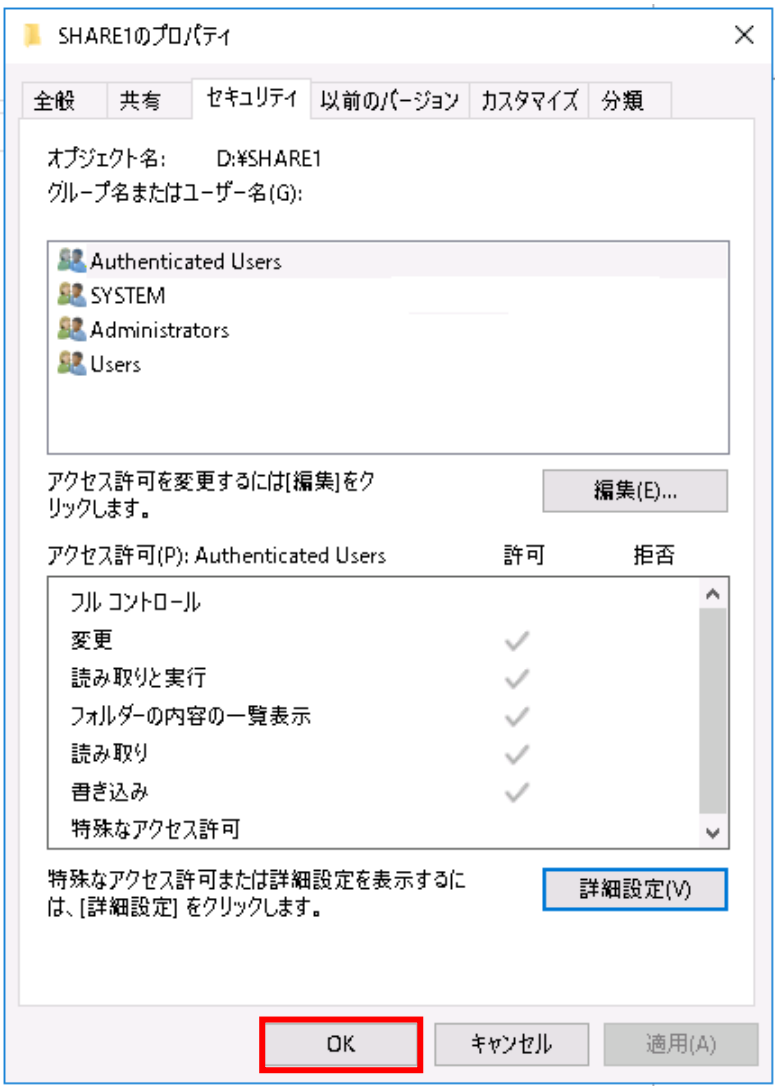


画面下部に [子オブジェクトの監査エントリすべてを、このオブジェクトからの継承可能な監査エントリで置き換える] のチェックボックスがあります。既存の監査エントリを置換する場合は、チェックを入れてください。

他の監査エントリを追加する場合は、手順 3～9 を繰り返し実行します。

監査エントリの追加を終了する場合は、[OK] をクリックします。

11. [～のプロパティ] 画面に戻るので、[OK] をクリックします。



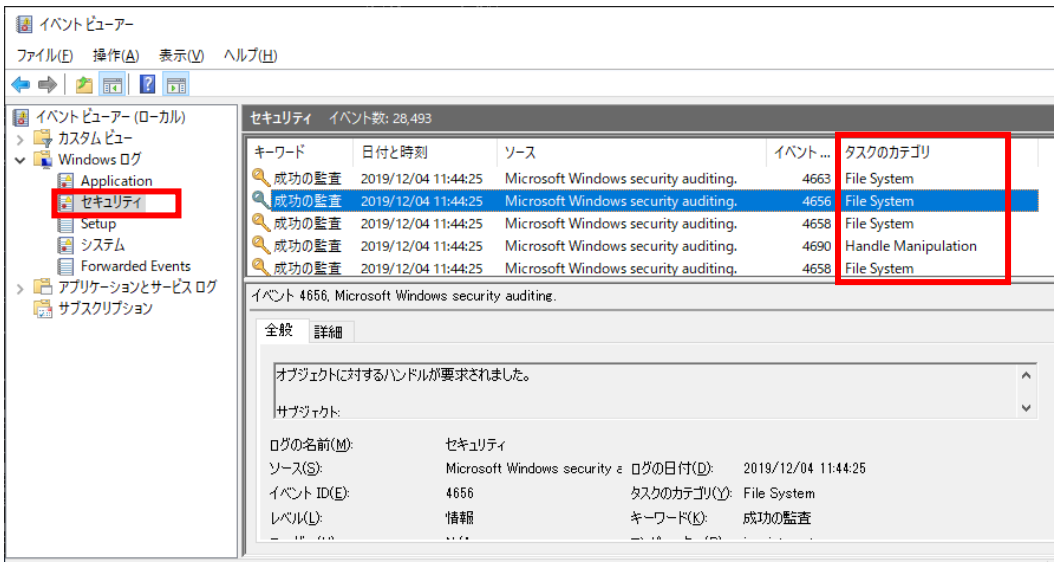
以上で、システムアクセス制御リスト (SACL) の作成が完了 (再起動不要) となります。
これ以降、システムアクセス制御リスト (SACL) が設定されているフォルダー／ファイルにアクセスが発生すると、セキュリティイベントログに監査ログが記録されます。

3.1.2.2 監査ログの参照方法

監査ログの参照方法について説明します。
各手順は、リモートデスクトップ経由、または、コンソールにて、管理者権限を持つユーザーでサインインして実行してください。

① 監査ログの参照方法について

監査ログは、Windows OS のセキュリティイベントログに記録されます。確認するには、[管理者メニュー] から [イベントビューアー] を起動し、ツリー部の [Windows ログ] – [セキュリティ] をクリックします。



上記のイベント一覧のうち、 [タスクのカテゴリ] 欄が 「File System」と「Handle Manipulation」になっているイベントが、記録された監査ログとなります。
なお、イベント一覧には、監査対象のファイル名が表示されません。パスを確認するには、各イベントのメッセージ内容を参照してください。
また、各イベントのメッセージには、「どのユーザーが、どのファイル に、どのようなファイル操作を実施した」というような整理された情報は記録されておらず、「ファイルオープンのイベント」、「ファイルアクセス（読み取り/書き込み/削除、等）のイベント」「ファイルクローズのイベント」等が異なるイベント ID で記録されており、このような複数のイベントについてファイルパス名やファイルハンドル ID をキーに組み合わせて、ファイルアクセス状況を解析する必要があります。

② イベント ID について

前項で説明したイベント ID は、下記の表のとおりとなります。

イベント ID	操作	メッセージ内の情報		
		ユーザー名	ファイルパス名	ファイル ハンドル ID
4656	オープン	○	○	○
4663	アクセス(Read/Write/削除等)	○	○	○
4658	クローズ	○	× (※)	○
4659	削除	○	○	×
4660	削除	○	× (※)	○

上記の表の右側は、そのイベントのメッセージ内に、ユーザー名、ファイルのパス名、ファイルのハンドル ID が記録されるかどうかを示しています。

上記の表のとおり、削除のイベントは 4659 と 4660 の２つがあります。OS 内に削除方法が２つ用意されており、削除プログラムがどちらの削除方法を選択するかにより、いずれかのイベントが記録されます。両イベントが混在することがありますが、どちらが記録されても削除された結果に違いはありません。

上記の表の※印の箇所、クローズイベント 4658、および、削除イベント 4660 には、メッセージ内にファイルのパス名が記録されません。対象ファイルのパスを特定するには、イベントに記録されているファイルハンドル ID をキーにして、イベントを解析してください。なお、ファイルハンドル ID は、システムが一時的に割り当てる値のため、別タイミングにおいては、同じ ID が別のファイルに割り当てられることがあるので注意が必要です。

上記の表以外の監査ログのイベント ID に関する詳細な情報につきましては、【参考情報】に記載しているマイクロソフト社のイベント ID 一覧の資料をご覧ください。

③ 監査ログの参照例

監査ログの参照例として、下記の３つを記載します。

(1) 情報漏えい者を特定する場合

(2) ファイル改ざん者を特定する場合

(3) ファイル削除者を特定する場合

(1) 情報漏えい者を特定する場合

情報漏えいが行われ、その被疑者を特定する場合は、監査ログの一覧から、該当ファイルへの読み込みを行った際のイベントを参照します。

ファイル読み込み時は、下記のイベントが記録されますので、該当ファイルのファイルパス名を持つアクセスイベント (4663) を探します。該当イベントが複数存在する場合には、被害を受けたと思われる時間帯のイベントを確認してください。

【イベント 4663（アクセス)】

ファイルに読み込みのアクセスを行うと、下記のようなイベント 4663 が記録されます。

```
オブジェクトへのアクセスが試行されました。

サブジェクト:
    セキュリティ ID:        FILESV¥Administrator
    （中略）

オブジェクト:
    （中略）
    オブジェクト名:        D:¥SHARE1¥test.txt
    （中略）

プロセス情報:
    （中略）

アクセス要求情報:
    アクセス:        ReadData（または ListDirectory）

    （後略）
```

- [セキュリティ ID] 欄：アクセスを行ったユーザー名
- [オブジェクト名] 欄：アクセス対象のファイル名
- [アクセス] 欄：ファイルにどのようなアクセスを行ったか記録されます。ファイル読み込み操作を実行した場合、ReadData と記録されます。

(2) ファイル改ざん者を特定する場合

不正なファイル改ざんが行われ、その被疑者を特定する場合は、監査ログの一覧から、該当ファイルへの書き込みを行った際のイベントを参照します。

ファイル書き込み時は、下記のイベントが記録されますので、該当ファイルのファイルパス名を持つアクセスイベント (4663) を探します。該当イベントが複数存在する場合には、被害を受けたと思われる時間帯のイベントを確認してください。

【イベント 4663（アクセス)】

ファイルに書き込みのアクセスを行うと、下記のようなイベント 4663 が記録されます。

```
オブジェクトへのアクセスが試行されました。

サブジェクト:
    セキュリティ ID:        FILESV¥Administrator
    （中略）

オブジェクト:
    （中略）
    オブジェクト名:        D:¥SHARE1¥test.txt
    （中略）

プロセス情報:
    （中略）

アクセス要求情報:
    アクセス:        WriteData (または AddFile)
    （後略）
```

- [セキュリティ ID] 欄：アクセスを行ったユーザー名
- [オブジェクト名] 欄：アクセス対象のファイル名
- [アクセス] 欄：ファイルにどのようなアクセスを行ったか記録されます。ファイル書き込み操作を実行した場合、WriteData と記録されます。

(3) ファイル削除者を特定する場合

不正なファイル削除が行われ、その被疑者を特定する場合は、監査ログの一覧から、該当ファイルを削除した際のイベントを参照します。

ファイル削除時は、イベント 4659 もしくは 4660 が記録されますので、以下の手順で、イベントの参照を行います。

イベント 4659 の確認手順は、下記のとおりです。

該当ファイルのファイルパス名を持つ削除イベント (4659) を探します。該当イベントが複数存在する場合には、被害を受けたと思われる時間帯のイベントを確認してください。

【イベント 4659（削除)】

```
オブジェクトに対するハンドルが削除を目的として要求されました。

サブジェクト:
    セキュリティ ID:        FILESV¥Administrator
    （中略）

オブジェクト:
    （中略）
    オブジェクト名:        D:¥SHARE1¥test.txt
    （後略）
```

- [セキュリティ ID] 欄：ファイル削除を行ったユーザー名
- [オブジェクト名] 欄：削除したファイル名

削除イベント 4660 の確認手順は、下記のとおりです。

1. 該当ファイルのファイルパス名を持つオープンイベント (4656) を探します。
   該当イベントが複数存在する場合には、被害を受けたと思われる時間帯のイベントを確認してください。
2. 特定したオープンイベントのメッセージ中のハンドル ID を確認し、以降に記録されているイベントから、同じハンドル ID を持つ削除イベント (4660) を探します。

【イベント 4656（オープン）】

削除イベント 4660 にはファイルパス名が記録されないため、オープンイベント中のファイルパス名からハンドル ID を紐付けすることで、削除イベントを探します。

```
オブジェクトに対するハンドルが要求されました。

サブジェクト:
    （中略）

オブジェクト:
    （中略）
    オブジェクト名:        D:¥SHARE1¥test.txt
    ハンドル ID:        0x1324
    （中略）

アクセス要求情報:
    （後略）
```

- [オブジェクト名] 欄：オープンしたファイル名
- [ハンドル ID] 欄： オープンした結果として得られたファイルハンドル ID

【イベント 4660（削除）】

特定したファイルハンドル ID を持つ、以下のような削除イベント (4660) を探します。

```
オブジェクトが削除されました。

サブジェクト:
    セキュリティ ID:        FILESV¥Administrator
    （中略）

オブジェクト:
    （中略）
    ハンドル ID:    0x1324

プロセス情報:
    （後略）
```

- [セキュリティ ID] 欄：ファイル削除を行ったユーザー名

3.1.2.3 監査ログの無効化

監査ログを無効化する場合は、下記①～③の手順を実施します。

① システムアクセス制御リスト (SACL) の削除
② 監査ポリシーの無効化設定
③ イベントログの設定変更

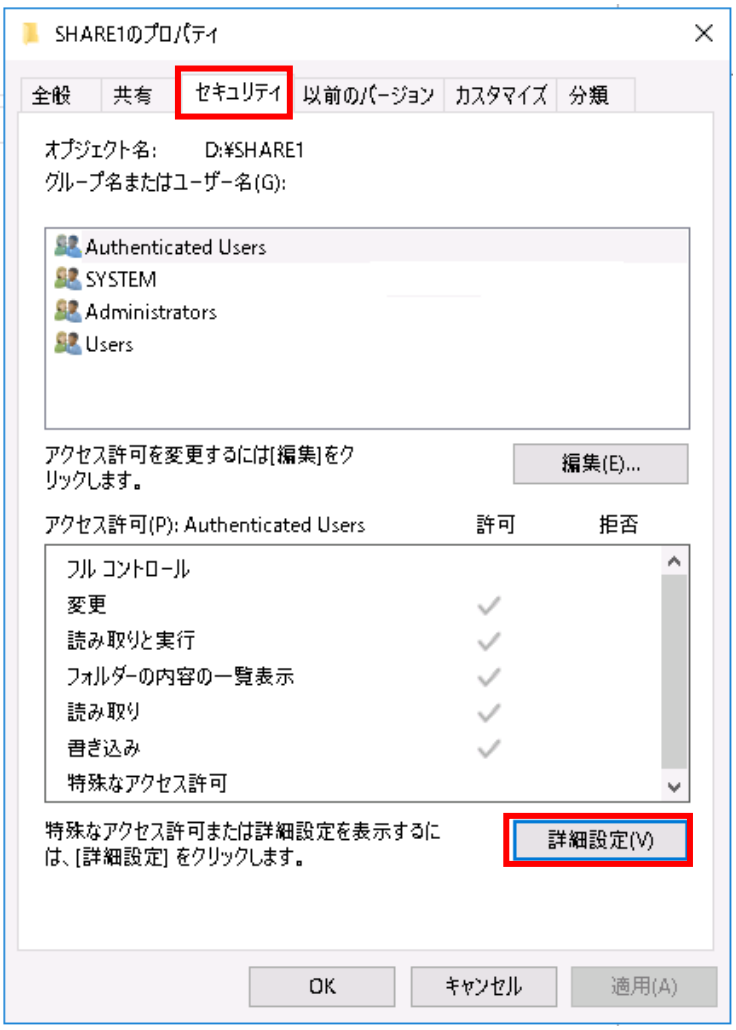
なお、各手順は、リモートデスクトップ経由、または、コンソールにて、管理者権限を持つユーザーでサインインして実行してください。

① システムアクセス制御リスト (SACL) の削除

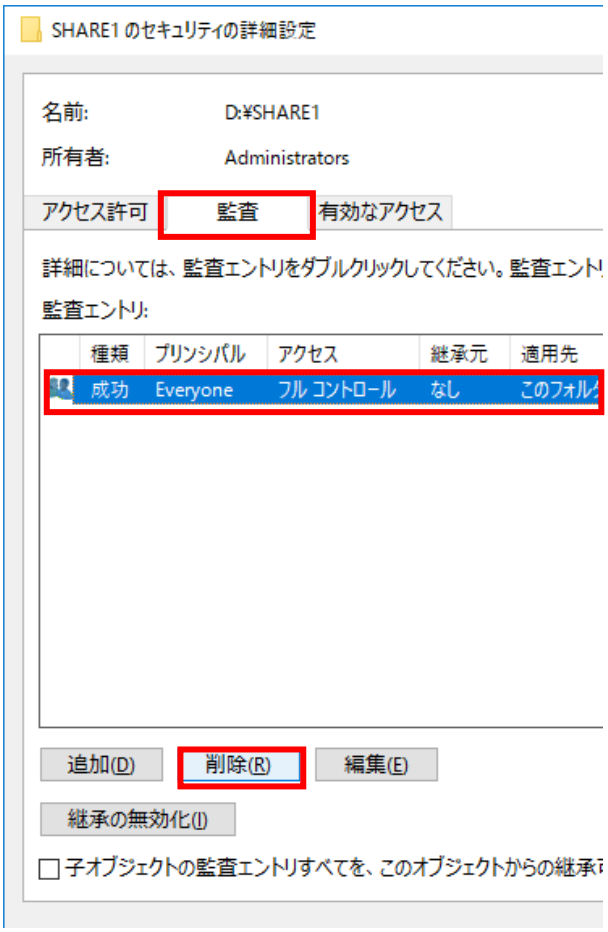
監視対象のファイル/フォルダーの、システムアクセス制御リスト (SACL) の削除を行います。
複数のファイル/フォルダーに対して監査設定を行っている場合、本操作を繰り返し実行します。

1. iStorage NS 上でエクスプローラーを起動し、ファイルアクセス監視の対象となっているフォルダーまたはファイルを右クリックして、[プロパティ] をクリックします。

2. [～のプロパティ] 画面で [セキュリティ] タブをクリックし、[詳細設定] ボタンをクリックします。



3. [～のセキュリティの詳細設定] 画面で、[監査] タブをクリックし、[監査エントリ] 欄の項目を選択して、[削除] ボタンを押します。
   監査エントリに項目が複数ある場合は、対象の監査エントリを選択し、削除します。



以上で、システムアクセス制御リスト (SACL) の削除が完了となります。

② 監査ポリシーの無効化設定

ファイルアクセス監視の監査ポリシーの無効化は、下記の２つの手順のいずれかを実施します。

- 監査ポリシーのバックアップから出荷時状態に復元
- auditpol コマンドにてファイルアクセス監視の監査項目を無効化

各手順について以下に記載します。

【監査ポリシーのバックアップから出荷時状態に復元する手順】

本手順は、事前に【監査ログの有効化】の「② 監査ポリシーのバックアップ」にてバックアップを作成しておく必要があります。

1. 管理者権限の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下記のコマンドを実行します。

```
auditpol /restore /file:c:¥NEC¥auditpol_default.csv
```

上記コマンドの“/file:”の後ろは、実体に合わせてバックアップファイルのファイルパスを指定してください。

【auditpol コマンドにてファイルアクセス監視の監査ポリシーを無効化する手順】

1. 管理者権限のコマンドプロンプトを起動します。
2. 現在の監査ポリシーの設定状況を確認するため、コマンドプロンプトにて下記のコマンドを実行します。

```
auditpol /get /category:*
```

3. 上記 2 のコマンドの結果表示を確認します。下記の赤文字のように [ファイル システム] と [ハンドル操作] が「監査なし」以外の値になっている場合は、ファイルアクセス監視の監査ポリシーが有効になっていますので、次項の手順で無効化を行います。

```
------------------------------   --------
カテゴリ/サブカテゴリ             設定
------------------------------   --------
(中略)
オブジェクト アクセス
  ファイル システム              成功および失敗
  レジストリ                     監査なし
  カーネル オブジェクト          監査なし
  SAM                            監査なし
  証明書サービス                 監査なし
  生成されたアプリケーション     監査なし
  ハンドル操作                   成功および失敗
(後略)
```

4. 監査ポリシーを無効化するため、下記２つのコマンドを実行します。

auditpol /set /subcategory:"ファイル システム" /success:disable /failure:disable

auditpol /set /subcategory:"ハンドル操作" /success:disable /failure:disable

各コマンドが成功すると「コマンドは正常に実行されました。」と表示されます。

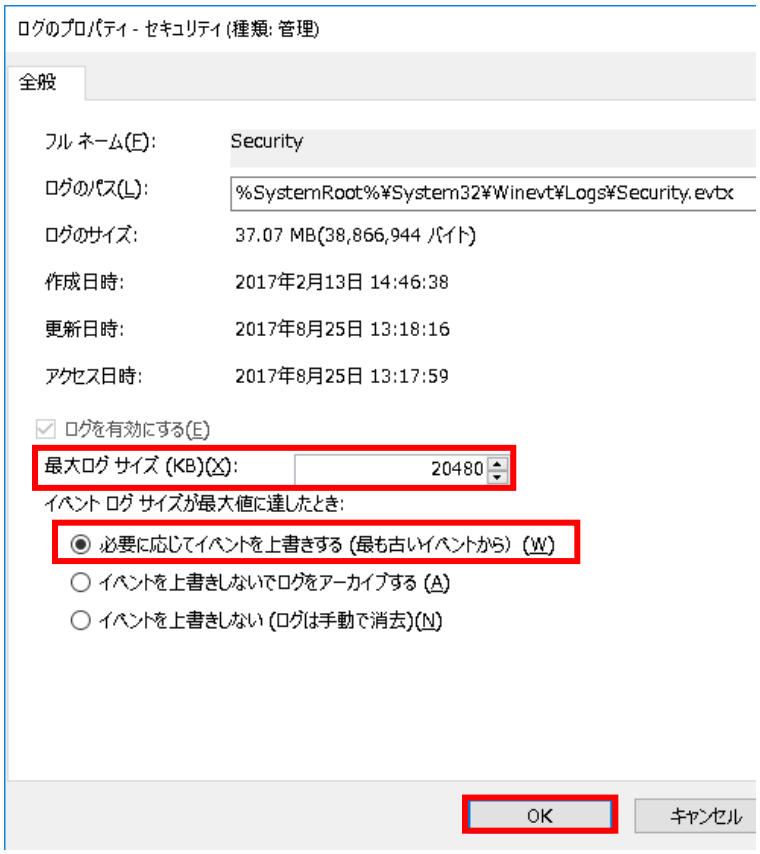
5. 監査ポリシーの変更結果を確認するため、再度上記 2 と同じコマンドを実行し、下記のような結果表示になることを確認します。[ファイル システム] と [ハンドル操作] が 「監査なし」になっている場合は、正しく無効化が実施されています。

```
------------------------------  --------
カテゴリ/サブカテゴリ            設定
------------------------------  --------
(中略)
オブジェクト アクセス
  ファイル システム             監査なし
  レジストリ                    監査なし
  カーネル オブジェクト         監査なし
  SAM                           監査なし
  証明書サービス                監査なし
  生成されたアプリケーション    監査なし
  ハンドル操作                  監査なし
(後略)
```

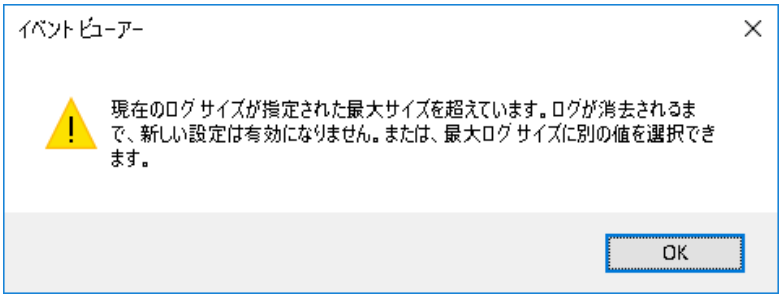
③ イベントログの設定変更

【監査ログの有効化】の設定手順にて、セキュリティイベントログのログサイズの拡大、および、アーカイブの設定を行っていますので、必要に応じて元の状態に戻してください。以下に出荷時状態に戻す手順を記載します。

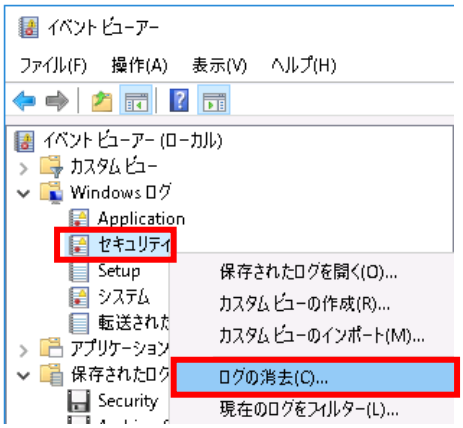
1. [管理者メニュー] から [イベントビューアー] を起動します。
2. [Windows ログ] - [セキュリティ] を右クリックし、[プロパティ] をクリックします。
3. [最大ログサイズ(KB)] 欄に 20480 (KB) を入力します。
4. [イベントログサイズが最大値に達したとき] 欄を、[必要に応じてイベントを上書きする(最も古いイベントから)] に変更します。
5. [OK] をクリックします。



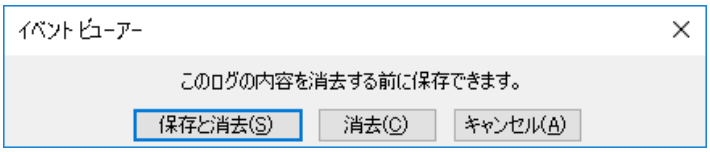
6. [最大ログサイズ(KB)] 欄に記入した値が、現在のログサイズよりも小さい場合は、下記の警告が表示されます。



上記の警告が表示された場合、新しいサイズを反映するためには、ログの消去を実施する必要があるので、[セキュリティ] を右クリックし、[ログの消去] をクリックします。



下記の選択肢が表示されますので、ログの保存が必要な場合は [保存と消去] をクリックしてください。ログの保存が必要ない場合は、[消去] をクリックしてください。



なお、アーカイブ設定をしていた場合は、C:¥Windows¥System32¥Winevt¥Logs フォルダー配下に下記のようなファイル名のアーカイブされたセキュリティイベントログが残っていますので、不要であれば削除してください。

Archive-Security-YYYY-MM-DD-HH-MM-SS-NNN.evtx

※ファイル名には年月日時分秒の値が含まれます。

3.1.2.4 注意事項

- NFS 共有経由のファイルアクセスについて
  NFS 共有経由のファイルアクセスについては、本章で記載した監査ログ機能ではファイルアクセスを監視することができません。

- FAT32 ファイルシステムについて
  FAT32 ファイルシステムでは、監査ログの設定に必要となる、システムアクセス制御リスト (SACL) をサポートしていないため、監査ログの採取ができません。

- 監査ログのアーカイブについて
  監査ログを削除せずに残す（アーカイブする）設定を行った場合、C ドライブがディスクフルとなり、システム動作が不安定となりますので、定期的にアーカイブされた監査ログを削除する、あるいは、別のドライブに移動するようにしてください。

3.1.2.5 参考情報

- 監査ログのイベント ID 一覧について
  マイクロソフト社が下記の URL にて、監査ログのイベント ID 一覧と、各イベントの詳細な説明を記述した資料 (Microsoft Word の DOCX 形式) を提供しております。

  Windows 10 and Windows Server 2016 security auditing and monitoring reference
  https://www.microsoft.com/en-us/download/details.aspx?id=52630
  (2026 年 6 月 1 日現在)

- 監査ログ解析用の市販アプリケーションについて
  【監査ログの参照方法】に記載しましたように、監査ログの解析は、大量のイベントの確認と、複数のイベントを組み合わせた煩雑な解析が必要となるため、市販アプリケーションを利用することもご検討ください。

3.2 運用中の設定変更について

iStorage NS の運用中に、諸設定を変更する手順を説明します。

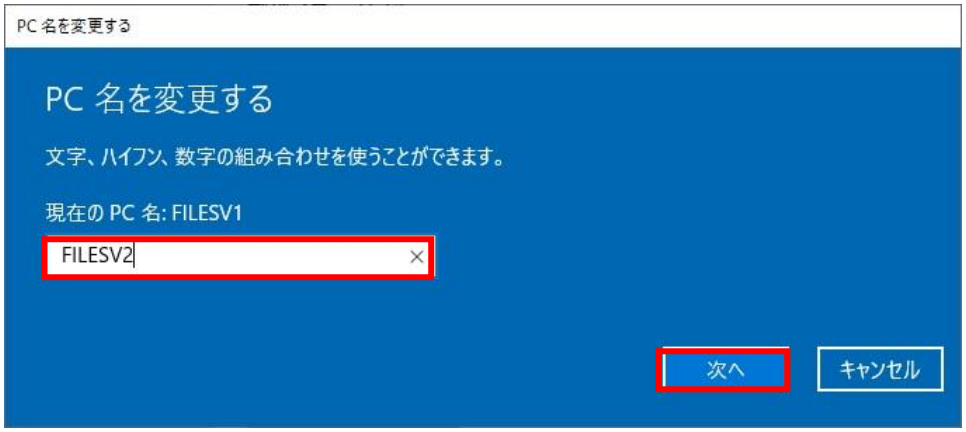
3.2.1 コンピューター名を変更する

既に運用しているサーバーのコンピューター名を変更する場合、以下の手順で行うことができます。なお、コンピューター名を変更した場合には、システムの再起動が必要となります。

1. [管理者メニュー] より [バージョン情報] をクリックします。

2. [この PC の名前を変更] をクリックします。

3. 変更するコンピューター名を入力して、[次へ]をクリックします。



4. 変更後のコンピューター名を確認する画面が表示されるので、間違いがなければ [今すぐ再起動する] をクリックします。再起動に際しては、【管理者ガイド（概要編）iStorage NS をシャットダウンまたは再起動する】の補足をご参照ください。

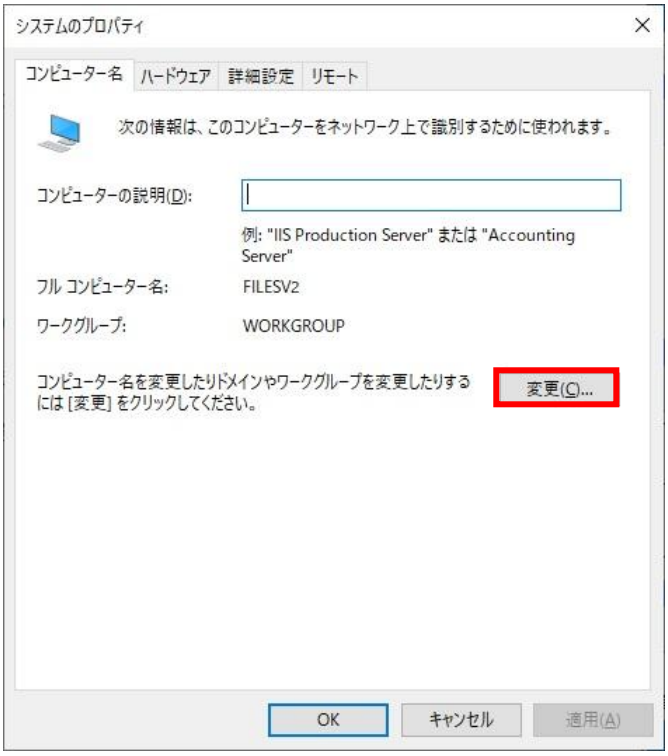
3.2.2 ドメインに参加するまたはドメインを変更する

ワークグループで運用していたサーバーをドメインに参加させる、または参加しているドメインを変更する場合、以下の手順で行うことができます。このとき、ドメインの変更にはドメインコントローラーの管理者アカウントおよびパスワードが必要となります。なお、ドメインを変更した場合には、システムの再起動が必要となります。

1. [管理者メニュー] より [バージョン情報] をクリックします。

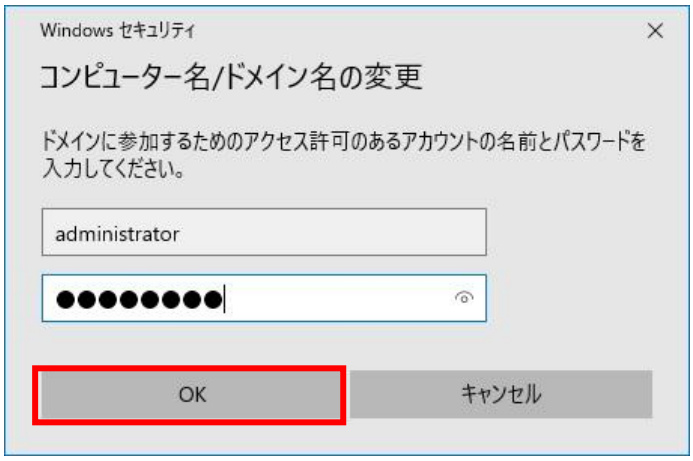
2. [システムの詳細設定] をクリックします。

3. [コンピューター名] タブを選択し、[変更] ボタンをクリックします。



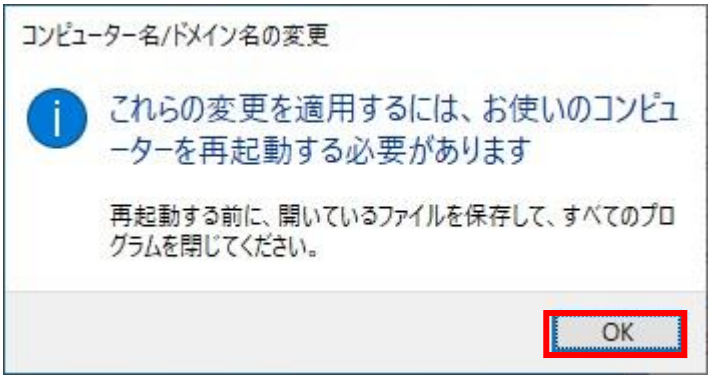
4. 新たに参加するドメイン名、もしくは変更するドメイン名を入力して、[OK] ボタンをクリックします。

5. 参加したドメインの管理者名とパスワードの入力画面が表示されたら、それぞれを入力し、[OK] ボタンをクリックします。

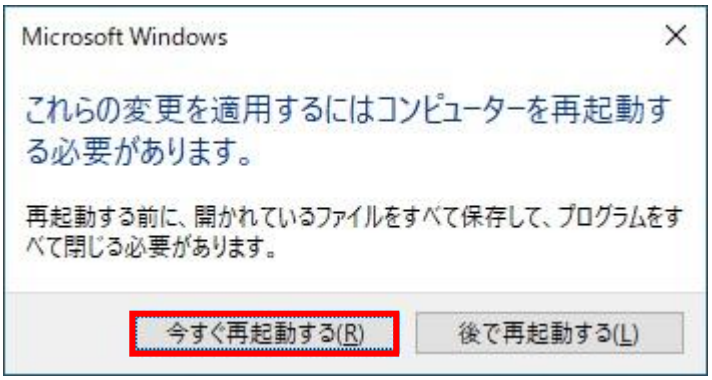


6. 以下のメッセージが表示されたら、[OK] ボタンをクリックします。

7. 再起動するようメッセージが表示されたら、[OK] ボタンをクリックします。



8. システムのプロパティ画面を閉じると、以下の画面が表示されますので、[今すぐ再起動する] を選択して iStorage NS を再起動します。再起動に際しては、【管理者ガイド（概要編）iStorage NS をシャットダウンまたは再起動する】の補足をご参照ください。



3.2.3 管理者のパスワードを変更する

iStorage NS のローカル管理者のパスワード変更は、iStorage NS にディスプレイ、キーボード、マウスを接続して行うか、または管理 PC よりリモートデスクトップ経由で行うこともできます。それぞれの方法を以下に記載します。

【注意】

- パスワードの有効期限は初期設定では 42 日になっておりますので、お客様のポリシーに合わせて有効期限を適宜変更してください。
- パスワードの文字数は 6 文字以上である必要があります。また、パスワードには、英大文字、英小文字、数字、記号の文字の 4 つの種類のうち 3 つの種類が使用されていなければなりません。なお、記号には以下の文字を使用することが可能です。

  ` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] ¥ | : ; " ' < > , . ? /

3.2.3.1 ディスプレイ、キーボード、マウスを接続して行う場合

1. iStorage NS にローカル管理者のアカウントでサインインします。
2. [Ctrl+Alt+Del] を押下します。
3. [パスワードの変更] をクリックします。
4. [古いパスワード]、[新しいパスワード]、[パスワードの確認入力] にそれぞれ入力し、[Enter] キーを押下します。
5. [パスワードは変更されました] と表示されるので、[OK] をクリックします。

3.2.3.2 リモートデスクトップ経由で行う場合

1. 管理 PC からリモートデスクトップ経由で、 iStorage NS にローカル管理者のアカウントでサインインします。

2. [Ctrl+Alt+End] を押下し、[パスワードの変更] をクリックします。

3. [古いパスワード]、[新しいパスワード]、[パスワードの確認入力] にそれぞれ入力し[Enter] キーを押下します。

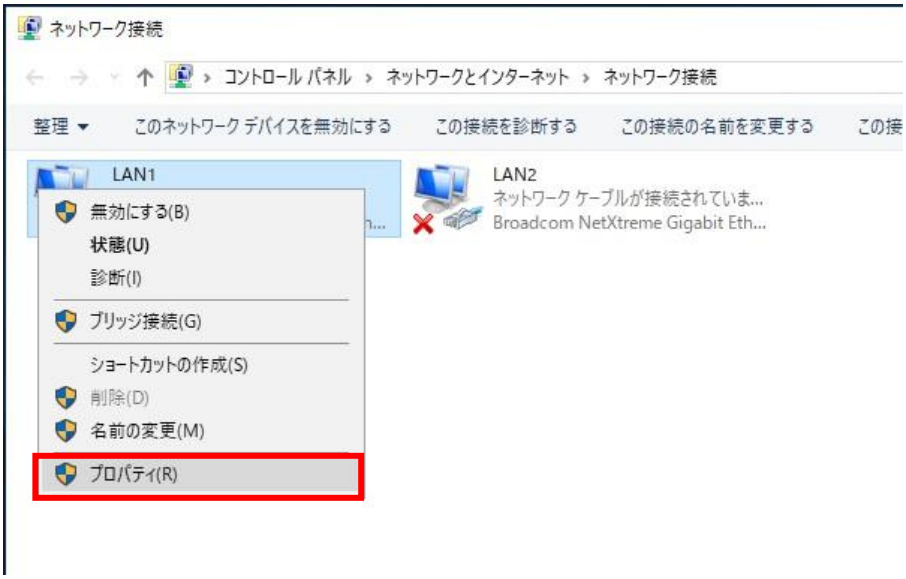
4. [パスワードは変更されました] と表示されますので、[OK] ボタンをクリックします。

3.2.4 IP アドレスを変更する

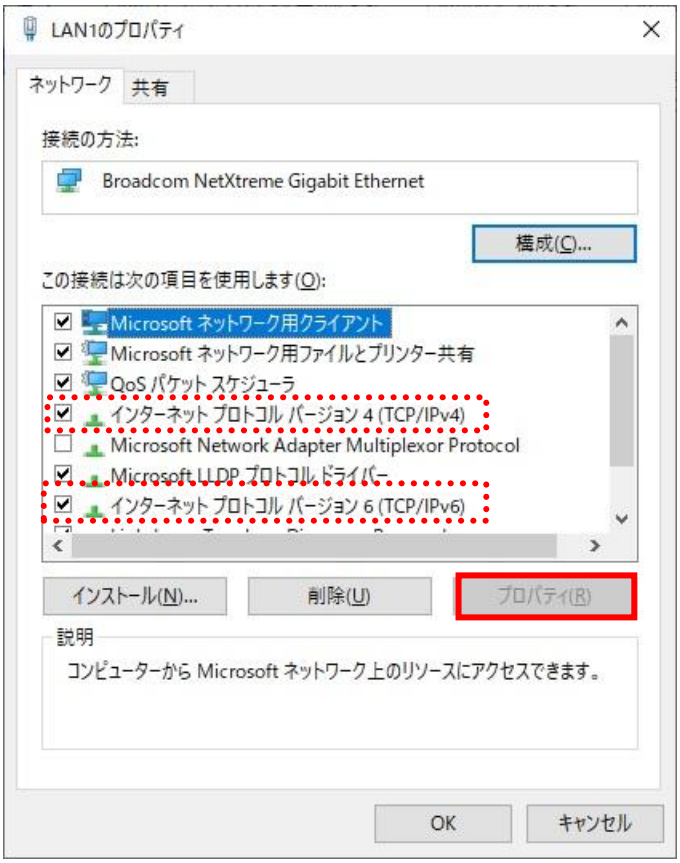
iStorage NS の運用中に、IP アドレスを変更する手順を以下に説明します。なお、接続中のクライアント PC が存在する場合は、あらかじめアクセスを切断し、IP アドレス変更後しばらくして、再接続を行ってください。

1. 管理者メニューの [ネットワーク接続] をクリックします。

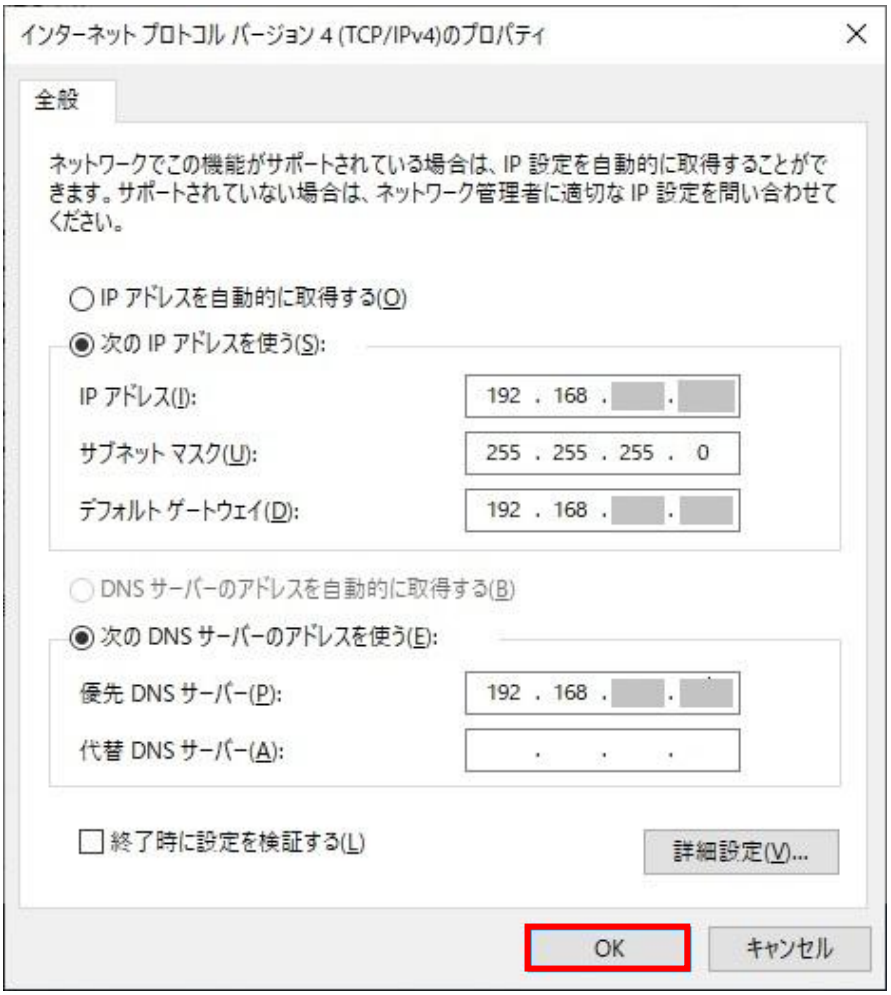
2. IP アドレスを変更するネットワークアダプターを右クリックし、[プロパティ] をクリックします。



3. お客様環境に応じ、[インターネットプロトコルバージョン 4（TCP/IPv4）] または [インターネットプロトコルバージョン 6（TCP/IPv6）] を選択して [プロパティ] ボタンをクリックします。



4. 必要に応じて IP アドレス等を設定し、[OK] ボタンをクリックします。（下図は IPv4 アドレスの設定例です。）



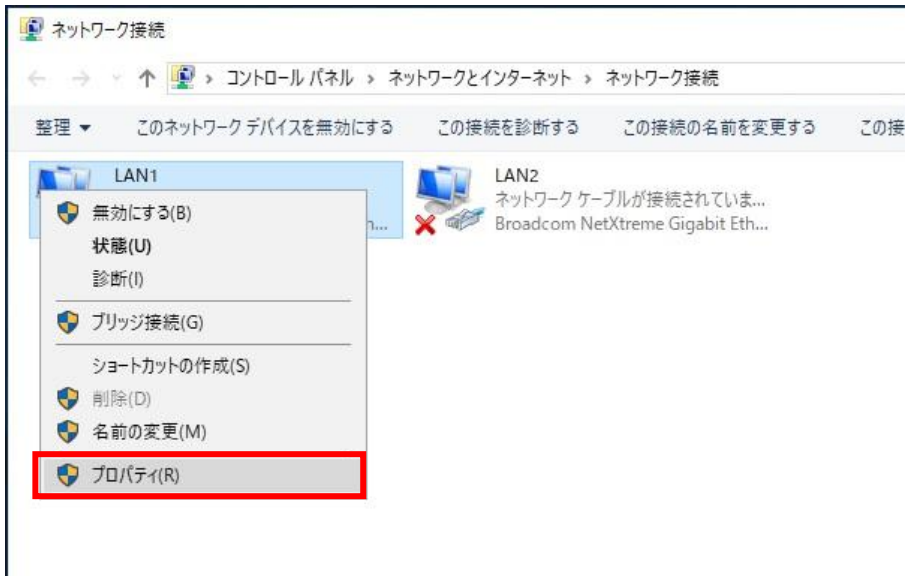
5. [閉じる] ボタンをクリックしてプロパティ画面を閉じます。

3.2.5 ネットワークインターフェイスの優先順位を変更する

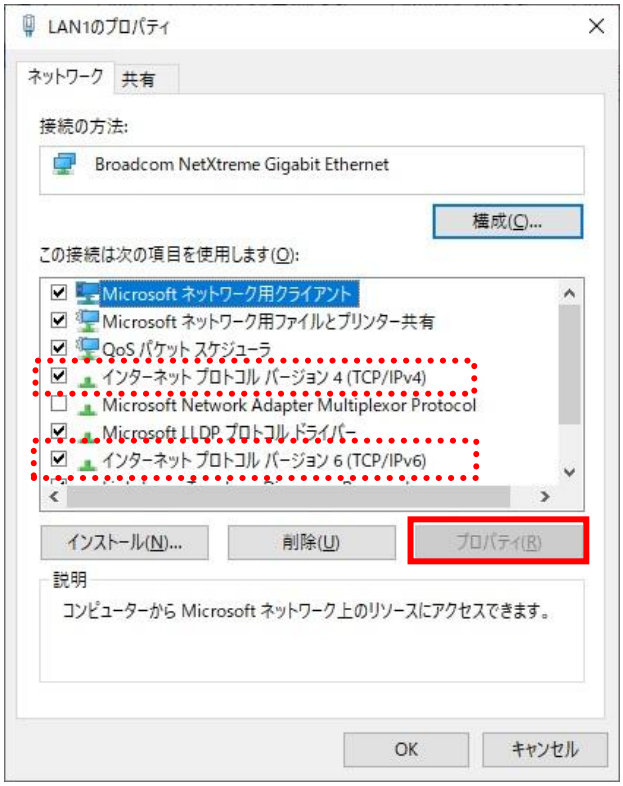
iStorage NS において複数のネットワークインターフェイスを使用している環境では、以下の手順でネットワークインターフェイスの優先順位を変更することができます。ネットワークインターフェイスに優先順位を付けて運用を行いたい場合は、使用可能な各ネットワーク接続すべてについて、下記手順の 2. ～ 5. を行ってください。

1. 管理者メニューの [ネットワーク接続] をクリックします。

2. 使用可能なネットワーク接続が表示されるので、設定を変更するネットワークアダプターを右クリックし、[プロパティ] をクリックします。

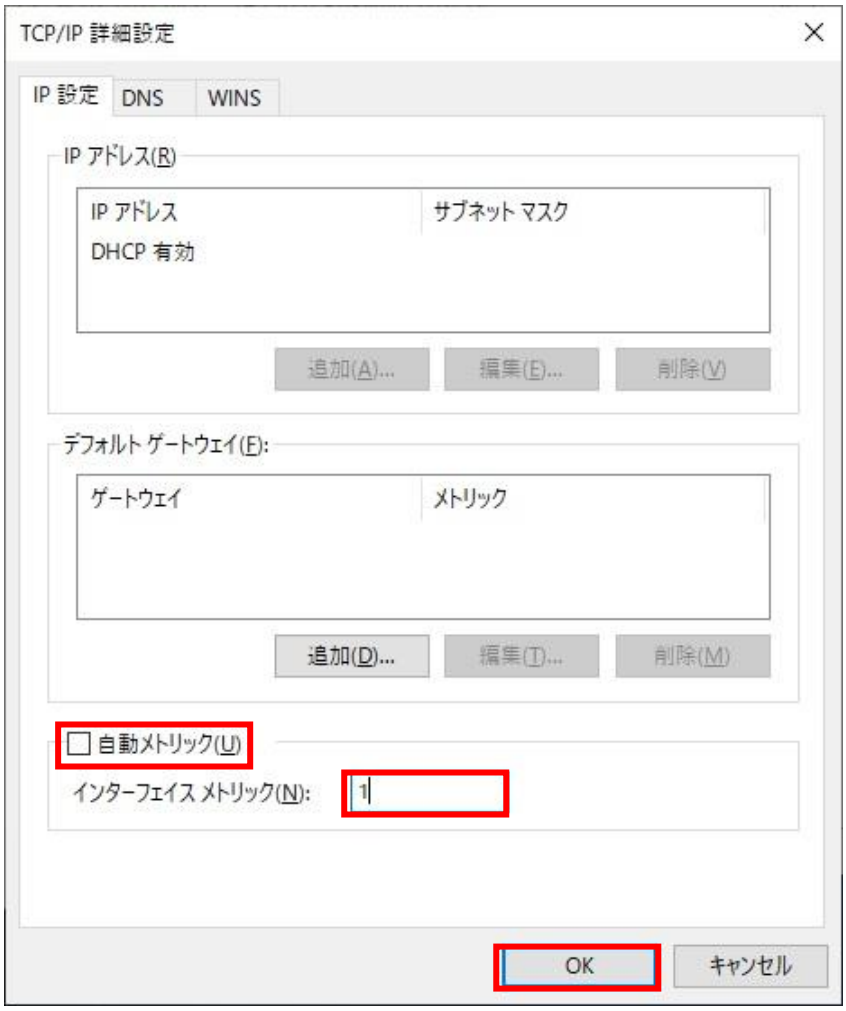


3. お客様環境に応じ、[インターネットプロトコルバージョン 4（TCP/IPv4）] または [インターネットプロトコルバージョン 6（TCP/IPv6）] を選択して [プロパティ] ボタンをクリックします。



4. [全般] タブの [詳細設定] をクリックします。（下図は IPv4 アドレスの画面です。）

5. [IP 設定] タブの [自動メトリック] チェック ボックスをオフにし、[インターフェイス メトリック] ボックスに値を入力して [OK] をクリックします。 このメトリック値は通信先への経路が複数存在する場合に、どの経路を利用するかの優先付けとなります。メトリック値には 1 以上の整数値が指定でき、値の小さい経路が優先的に利用されます。



3.3 NIC チーミングを設定する

NIC チーミングとは、サーバー上の複数のネットワークアダプターを 1 つにまとめて運用する機能です。NIC チーミングの設定を行うことで、1 つのネットワークアダプターに障害が発生しても他のネットワークアダプターで処理を継続することができます。また、ネットワークアダプターの帯域幅を仮想的に集約することもできるようになります。

3.3.1 NIC チーミングの機能概要

3.3.1.1 チーミングモード

NIC チーミングでは、以下の 3 種類のチーミングモードを選択することができます。

- **スイッチに依存しない**

  OS で送信時の負荷分散処理を実施します。静的リンクアグリケーションや動的リンクアグリケーションに対応したスイッチングハブは必須ではありません。また、チームを構成するネットワークアダプターをそれぞれ別のハブに接続することもできます。

- **静的チーミング**

  ネットワークアダプターとスイッチングハブのポート双方を、Link Aggregation Static Mode に設定し、チーム内の全ネットワークアダプターを使用して送受信を行います。静的リンクアグリケーション対応のスイッチングハブが必要となります。なお、チームを構成するネットワークアダプターはすべて同じスイッチングハブに接続します。

- **LACP(Link Aggregation Control Protocol)**

  ネットワークアダプターとスイッチングハブの双方で LACP を有効化し、チーム内の全ネットワークアダプターを使用して送受信を行います。動的リンクアグリケーション対応のスイッチングハブが必要となります。なお、チームを構成するネットワークアダプターはすべて同じスイッチングハブに接続します。

3.3.1.2 負荷分散モード

負荷分散モードとして、以下の３種類を選択することができますが、既定値（動的）で運用いただくことを推奨します。

- **アドレスのハッシュ**
  IP アドレス、ポート番号、MAC アドレスによる負荷分散となります。

- **Hyper-V ポート**
  VM が使用するポート番号による負荷分散で、Hyper-V サーバーにて有効となります。

- **動的**
  ネットワーク使用率を重視した負荷分散で、デフォルトの設定値となります。

3.3.1.3 スタンバイアダプター

チーミングモードを「スイッチに依存しない」とした場合のみ、スタンバイアダプターを設定することができます。

スタンバイアダプターを「なし（すべてのアダプターがアクティブ）」とした場合は、常にすべてのネットワークアダプターを用いて通信が行われます。
チームのメンバーのいずれかをスタンバイアダプターに設定した場合は、そのアダプターはスタンバイ状態となり、正常な状態での通信には利用されず、アクティブアダプターの 1 つに障害が発生した際にアクティブ状態となります。その後、障害が発生したアクティブアダプターが復旧した場合、30 秒後にアクティブアダプターがアクティブ状態となり、スタンバイアダプターに設定したアダプターはスタンバイ状態に戻ります。この動作は仕様であり、変更することはできません。

3.3.2 NIC チーミングを作成する

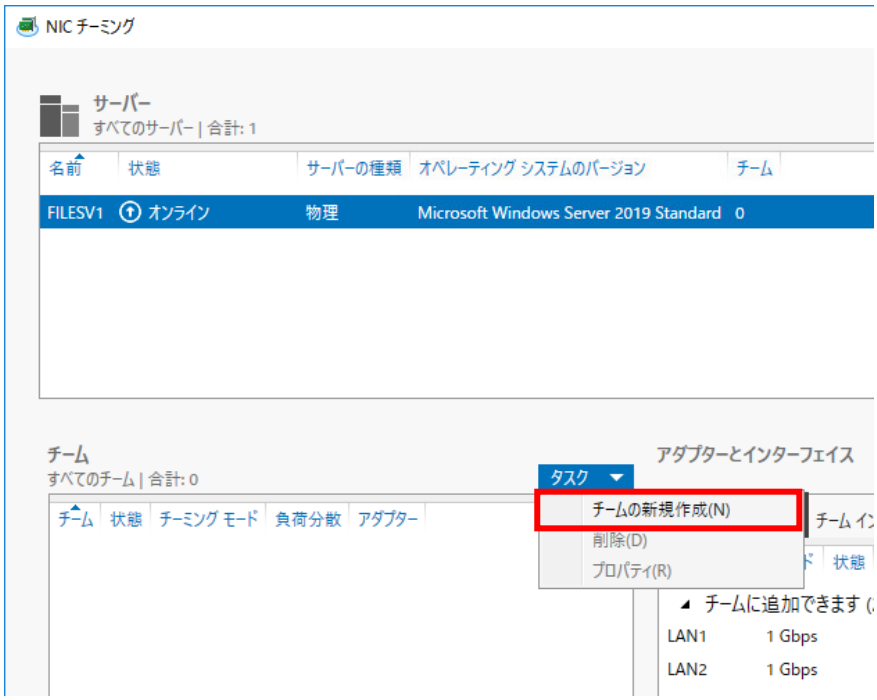
NIC チーミングを新規に設定する手順について説明します。

【注意】
チームを作成する際には、一時的にネットワークが切断され、IP アドレスの再設定も必要となります。
このため、NIC チーミングを設定する場合は、本機にコンソールを接続して設定を行ってください。

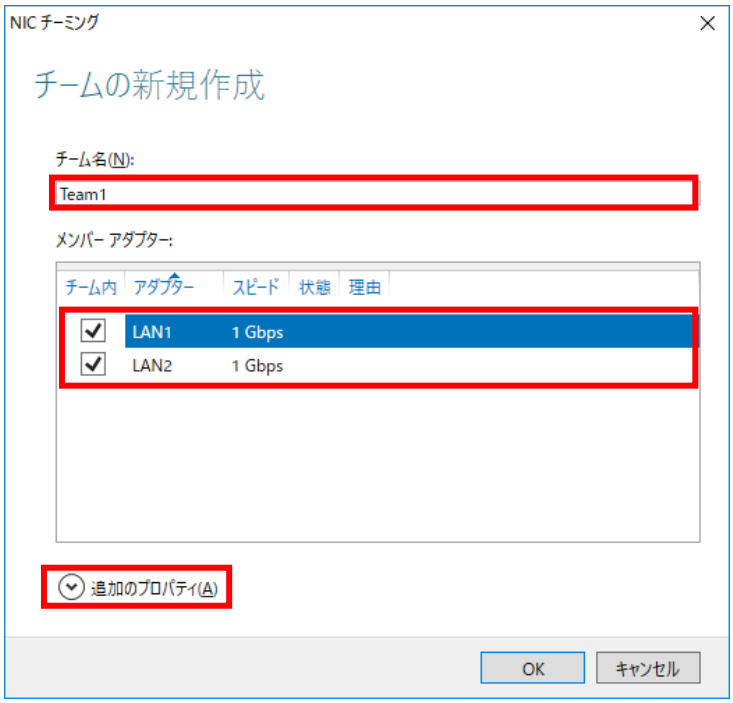
1. サーバーマネージャーを起動して、[ローカルサーバー] をクリックします。

2. ローカルサーバーのプロパティから [NIC チーミング] の [無効] をクリックします。

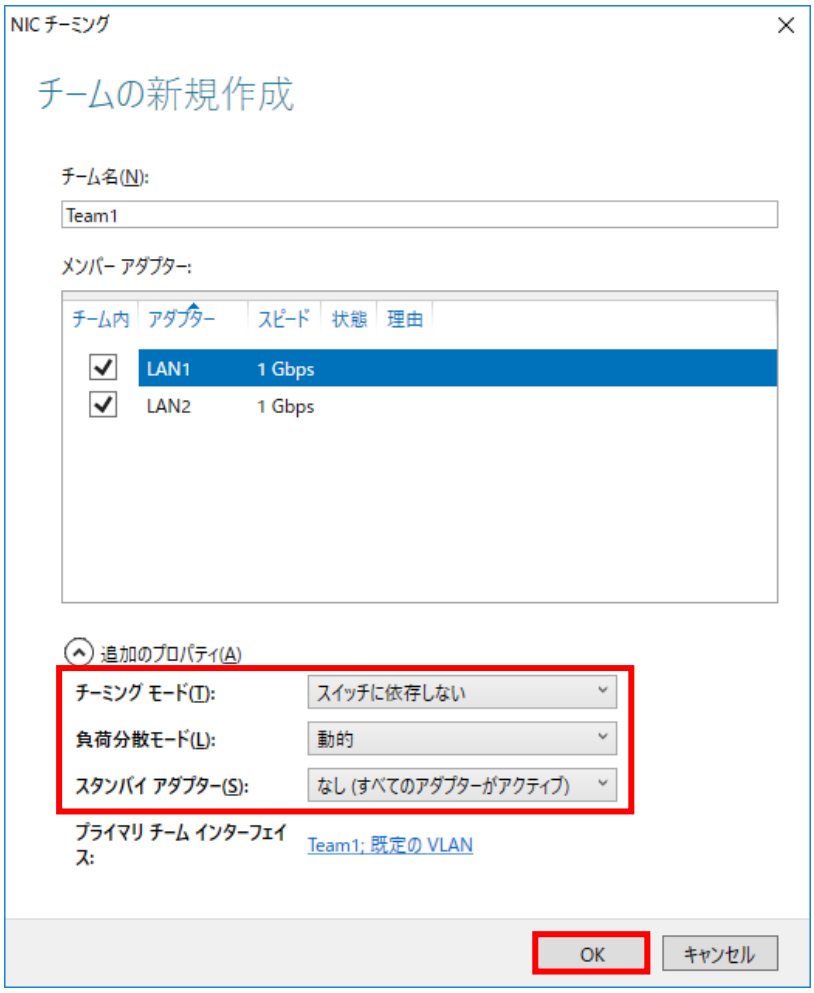
3. [NIC チーミング] の画面が表示されますので、チームの [タスク] – [チームの新規作成] をクリックします。



4. [チームの新規作成] の画面が表示されますので、[チーム名] を入力し、[メンバーアダプター] からチームを構成するアダプターを選択して、[追加のプロパティ] をクリックします。



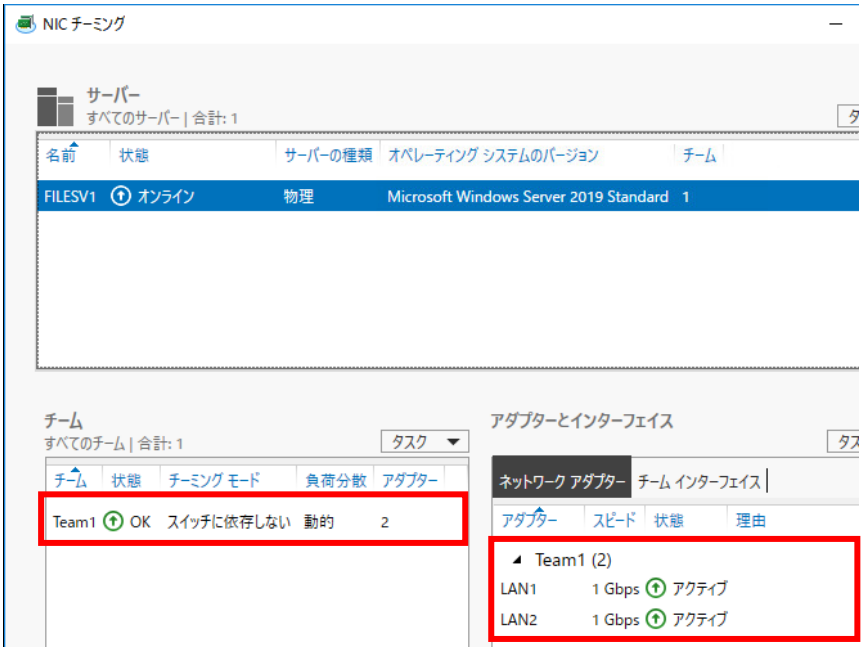
5. [チーミングモード] [負荷分散モード] [スタンバイアダプター] を設定し、[OK] をクリックします。



【注意】

チーミングモードとして、静的チーミング、LACP を指定する場合は別途スイッチングハブ側でも適切な設定が必要となります。

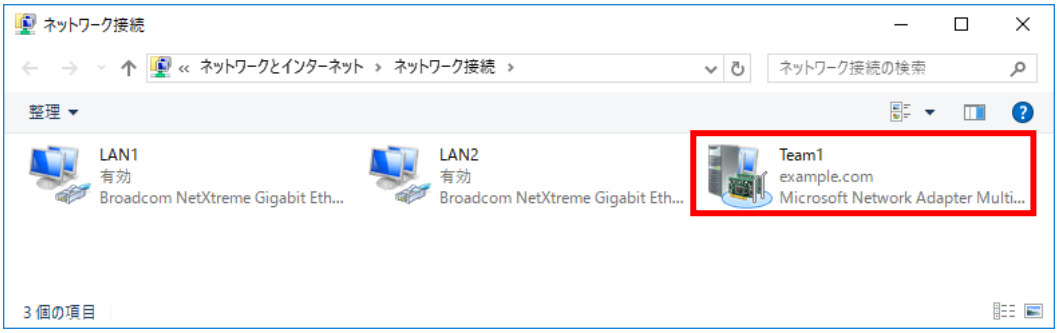
6. 設定が完了するとネットワーク接続が回復しますので、[チーム] の [状態] が [OK] になり、[アダプターとインターフェイス] の [状態] が [アクティブ] になっていることを確認します。



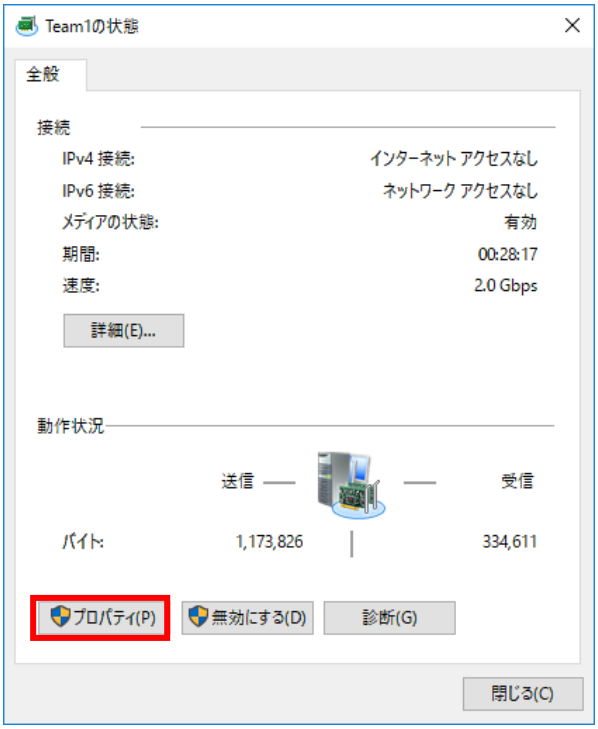
7. サーバーマネージャーに戻り、[NIC チーミング] の状態が [有効] に変化していることを確認します。

なお、作成したチームの IP アドレスはデフォルトでは [IP アドレスを自動的に取得する] 設定となっています。チームに静的 IP アドレスを設定する場合は、作成したチームの状態（画像中では [IPv4 アドレス（DHCP により割り当て）、IPv6（有効）]）をクリックして項番 8、9、10 の操作を行います。

8. [ネットワーク接続] の画面が表示されますので、作成したチーム名（画像中では [Team1] ）をダブルクリックします。



9. [プロパティ] をクリックして、静的 IP アドレスを設定します。



10. 設定後、サーバーマネージャーに戻って、作成したチームの IP アドレスが設定した静的 IP アドレスになっていることを確認します。

3.3.3 NIC チーミング利用時の注意事項

- 以下の機能は NIC チーミングと互換性がありません。

  - SR-IOV
  - リモート ダイレクト メモリ アクセス (RDMA)
  - TCP Chimney

  SR-IOV および RDMA の場合、データはネットワーク スタックを経由せずにネットワークアダプターに直接送信されます。したがって、NIC チーミングモジュールがデータを確認、または別のパスにデータをリダイレクトすることはできません。また、TCP Chimney は NIC チーミングでサポートされていません。

- NIC チーミングを構成している場合、OS 再起動後に、チーミングアダプターの MAC アドレス、IP アドレスが変わる場合があります。

  チーミングアダプターに割り当てられる MAC アドレスは、チームに含まれている物理 NIC のうち、OS 起動時に最初に認識された物理 NIC の MAC アドレスとなります。
  そのため、NIC チーミングを構成していると、何らかの要因で最初に認識する物理 NIC が異なることがあり、チーミングアダプターに割り当てられる MAC アドレスは変わる可能性があります。
  MAC アドレスが変わることが運用上の問題となる場合は、NIC チーミングは使用しないでください。

  また、NIC チーミング設定を行った iStorage NS の IP アドレスを DHCP により取得する環境においては、チーミングアダプターの MAC アドレスが変わることにより、DHCP サーバーから払い出される IP アドレスが変わる可能性があります。問題となる場合は、iStorage NS の IP アドレスを固定割り当てに変更してください。

3.4 Windows Server バックアップ

Windows Server バックアップは、OS に標準で組み込まれているイメージバックアップソフトウェアです。

3.4.1 Windows Server バックアップの機能概要

3.4.1.1 バックアップ

Windows Server バックアップでは、システムおよびユーザーデータを、ローカルボリュームやネットワーク上の共有フォルダーにバックアップすることが可能です。「ベアメタル回復」を指定することにより、システム回復に必要なボリューム及び情報をまとめてバックアップすることもできます。

> 【注意】
> Starter Pack の適用が必要な機種の場合、Starter Pack 適用ごとに「ベアメタル回復」のバックアップを取得していなければ、バックアップ DVD を用いてシステムの回復(バックアップからのリストア)に使用できません。Windows Server バックアップにて、システム回復を予定している場合は、Starter Pack の適用後に必ずベアメタル回復用のバックアップデータを取得してください。

このバックアップはイメージ形式で行われるため、ファイルの総数が多い環境でも高速なバックアップが可能となります。
また、バックアップは手動、もしくは、スケジュール設定により自動で実行されます。
保存場所やバックアップ方法によって、保存できる世代数が異なりますので以下の表をご確認ください。

保存場所	専用の ローカルディスク（※）	ローカルボリューム	共有フォルダー
手動 バックアップ	—（選択不可）	複数世代の保存可	最新状態のみ保存可
スケジュール バックアップ	複数世代の保存可	複数世代の保存可	最新状態のみ保存可

※ 専用のローカルディスクには、通常ドライブレターの付与されていない未使用のローカルディスクを割り当てます。このため、iStorage NS の出荷時設定ではご利用になれません。

バックアップの運用については、【Windows Server バックアップ利用時の留意点】にも留意事項を記述していますので、ご参照ください。

3.4.1.2 リストア

すべてのユーザーボリューム、選択したユーザーボリューム、または特定のファイルやフォルダーなどを指定して、GUI から簡単にリストアを実行することができます。

※ なお、システムそのものに問題が発生した場合にも、「ベアメタル回復」のバックアップを取得していれば、バックアップ DVD を用いてシステムの復旧(バックアップからのリストア)が可能です。

ボリューム単位のリストアでは、バックアップ元のボリュームとは異なるボリュームをリストア先とすることもできますが、バックアップ元のボリュームより小さいサイズのボリュームを指定することはできません。
ファイル・フォルダー単位のリストアを選択した場合は、リストア対象のデータが格納できる空き容量が存在していれば、ボリュームの大小は問いません。

3.4.2 Windows Server バックアップによるバックアップ

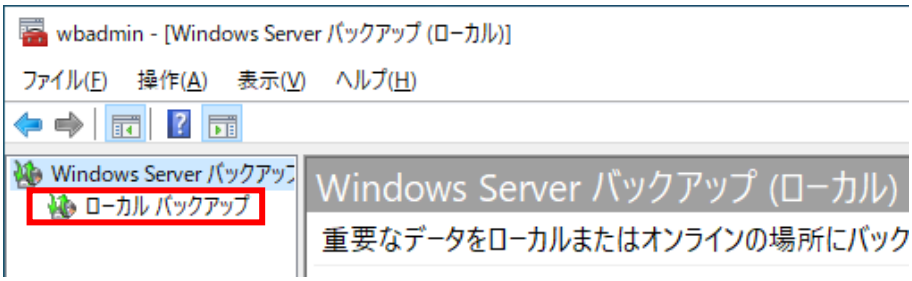
ここでは、Windows Server バックアップを用いて、手動で iStorage NS の全ボリュームのバックアップをネットワーク上の共有フォルダーに作成する方法を説明します。

なお、バックアップデータをネットワーク上の共有フォルダーに格納する場合は、以下の情報を事前に準備しておく必要があります。

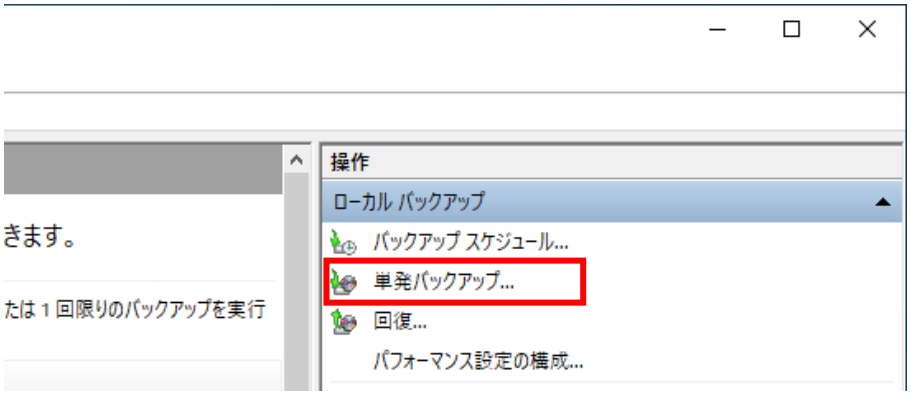
- バックアップデータ保存先サーバーのコンピューター名または IP アドレス
- バックアップデータ保存先共有名
- 共有アクセス用アカウント名
- 共有アクセス用パスワード

1. 管理者メニューから [Windows Server バックアップ] を起動します。

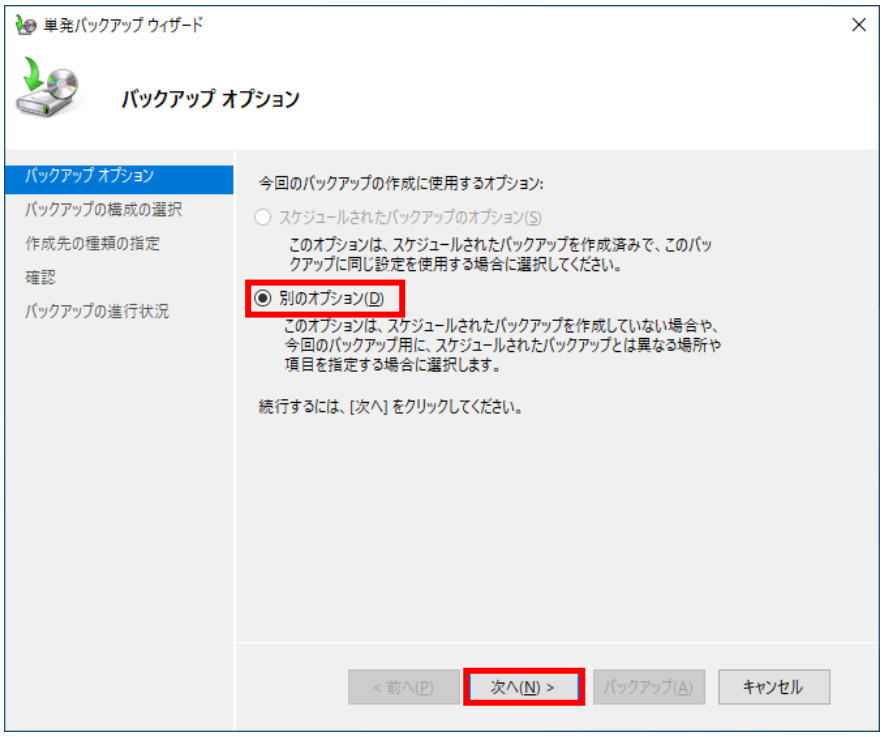
2. [ローカルバックアップ] をクリックします。



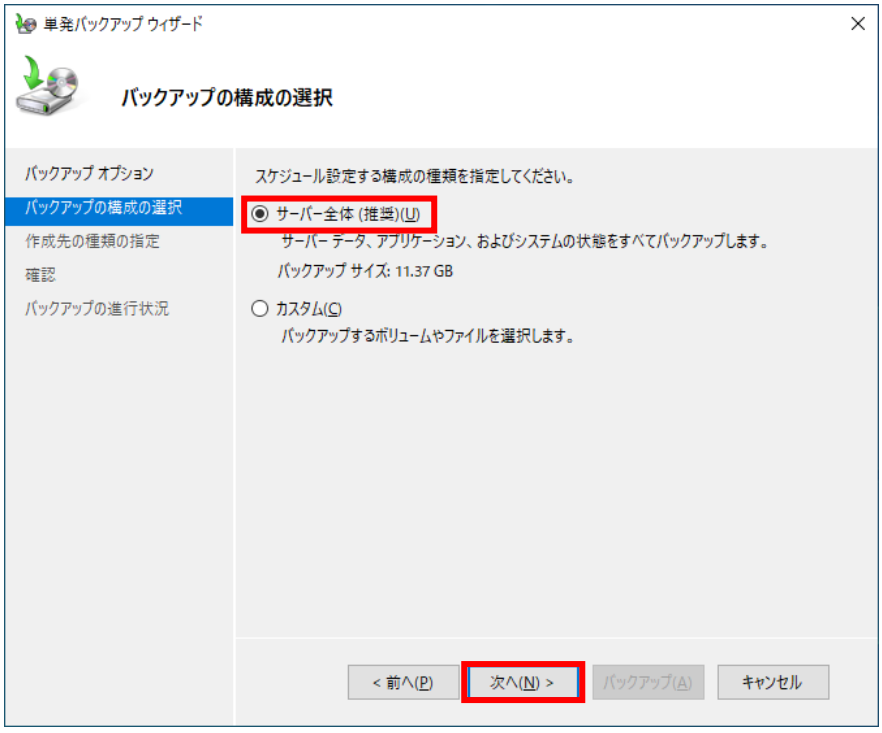
3. [単発バックアップ…] をクリックします。



4. [別のオプション] を選択して、[次へ] をクリックします。

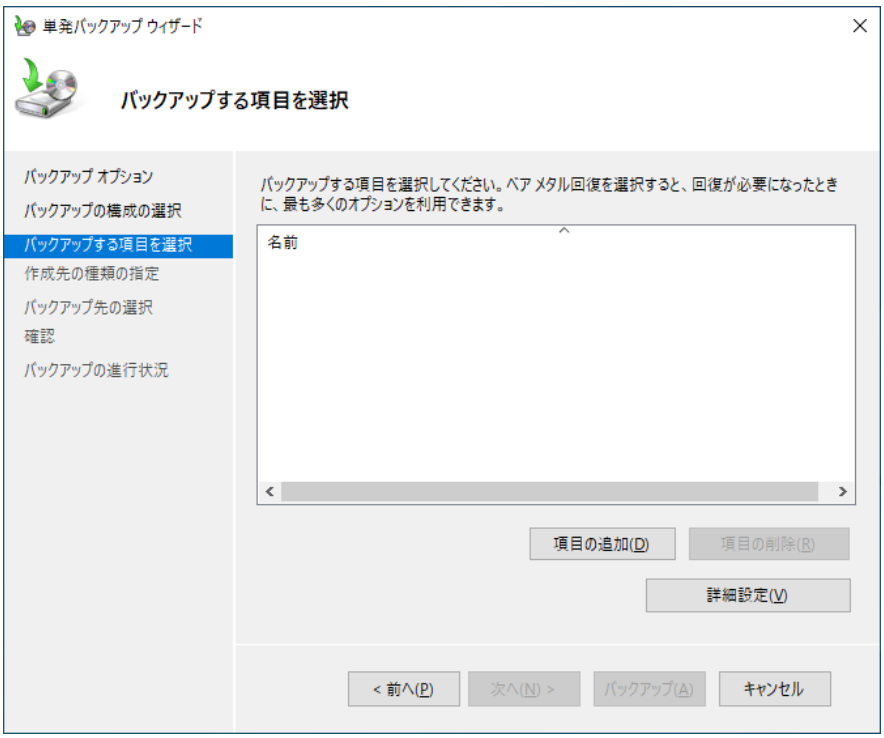


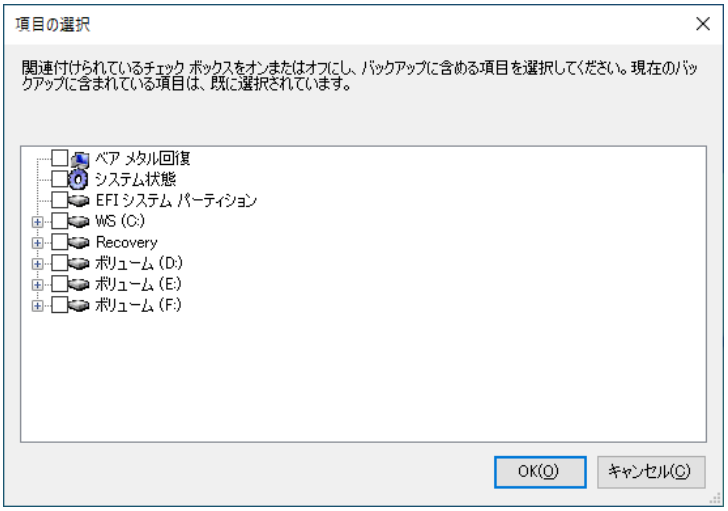
5. [サーバー全体（推奨）] を選択して、[次へ] をクリックします。



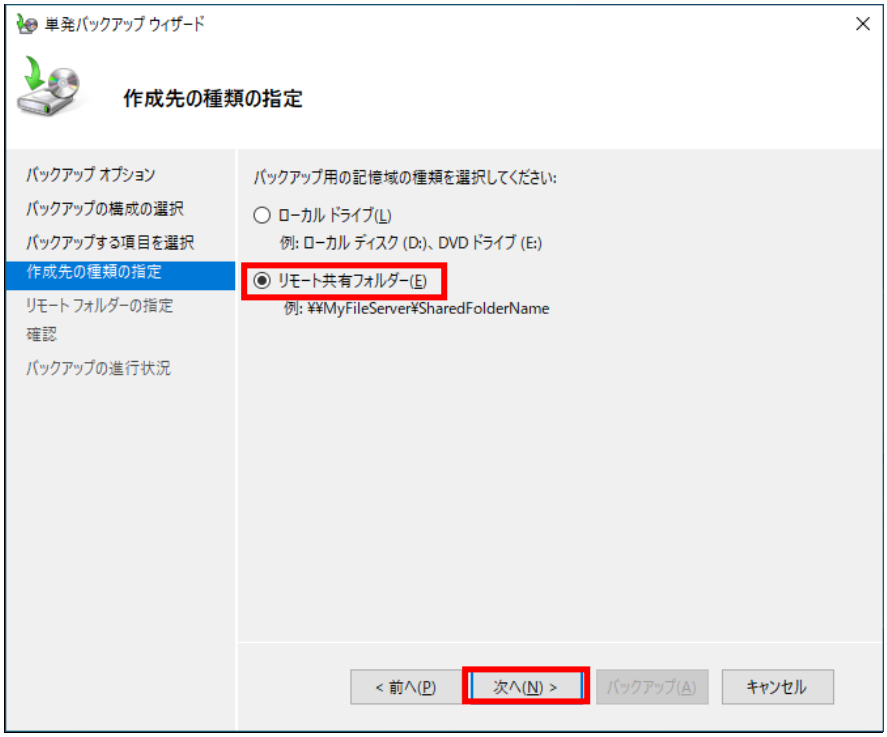
ここで、[カスタム] を選択して [次へ] をクリックすると、バックアップ対象を個別に選択することができます。
[項目の追加] をクリックしてバックアップしたい対象をチェックし追加してください。

なお、問題が発生した際に OS をバックアップ実行時点に復旧したい場合は、必ず [ベアメタル回復] を追加してください。

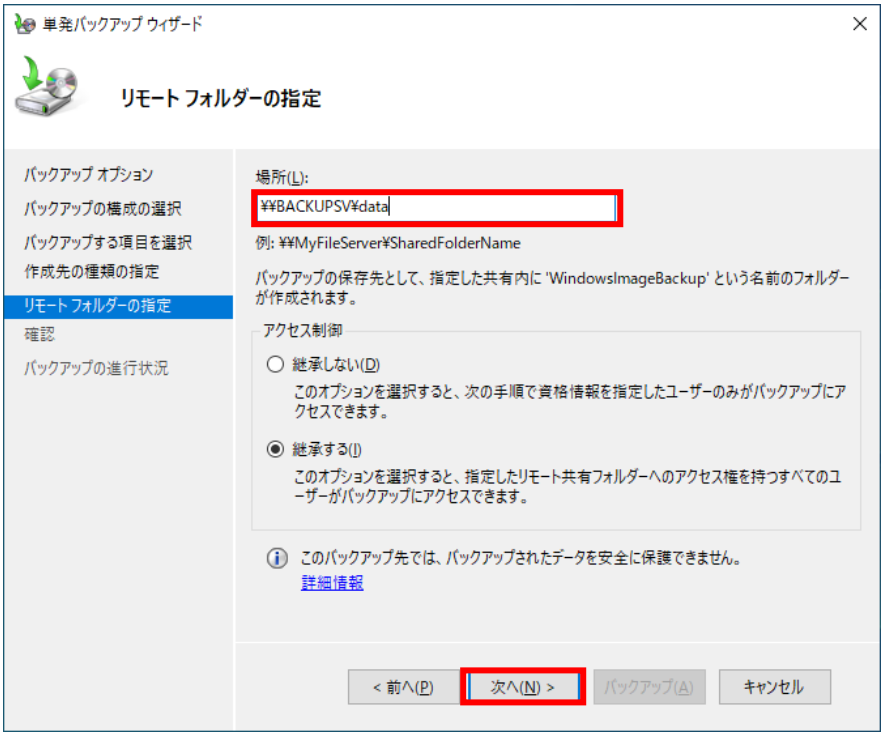




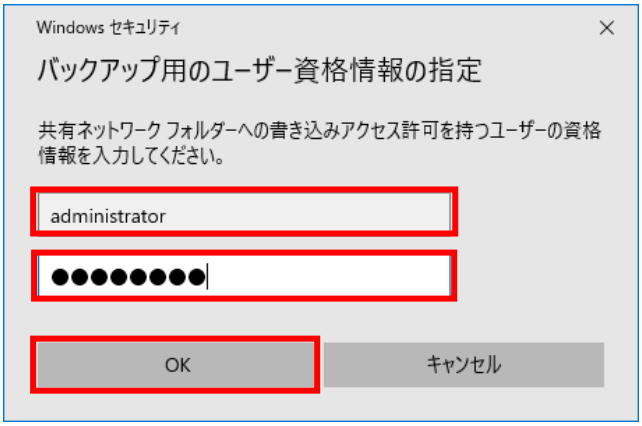
6. バックアップデータ保存先を選択して、[次へ] をクリックします。



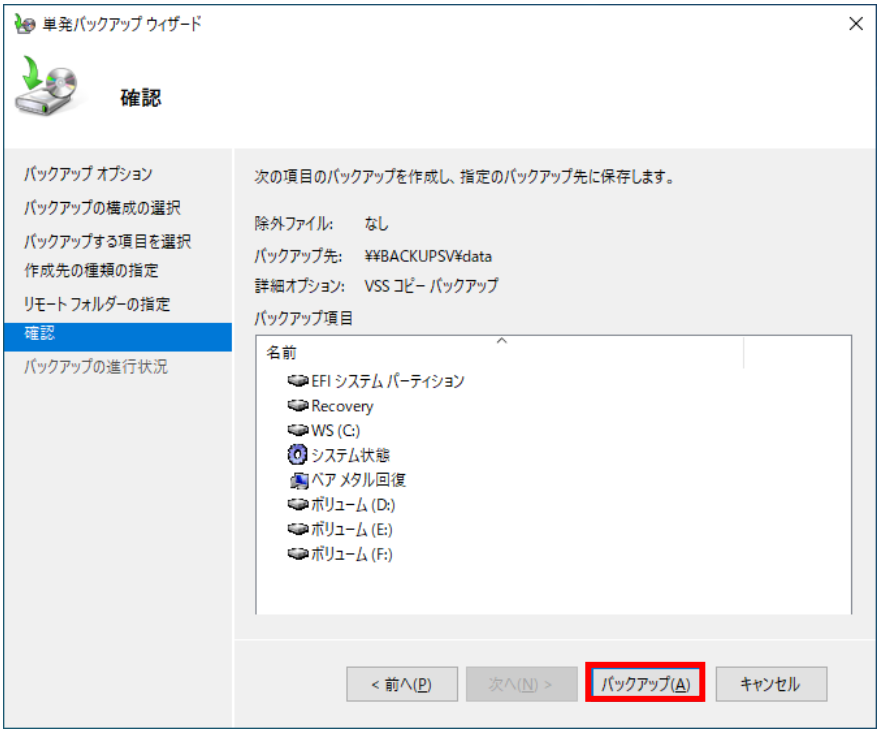
7. [場所] にバックアップデータ保存先の共有フォルダーのパスを入力して、[次へ] をクリックします。



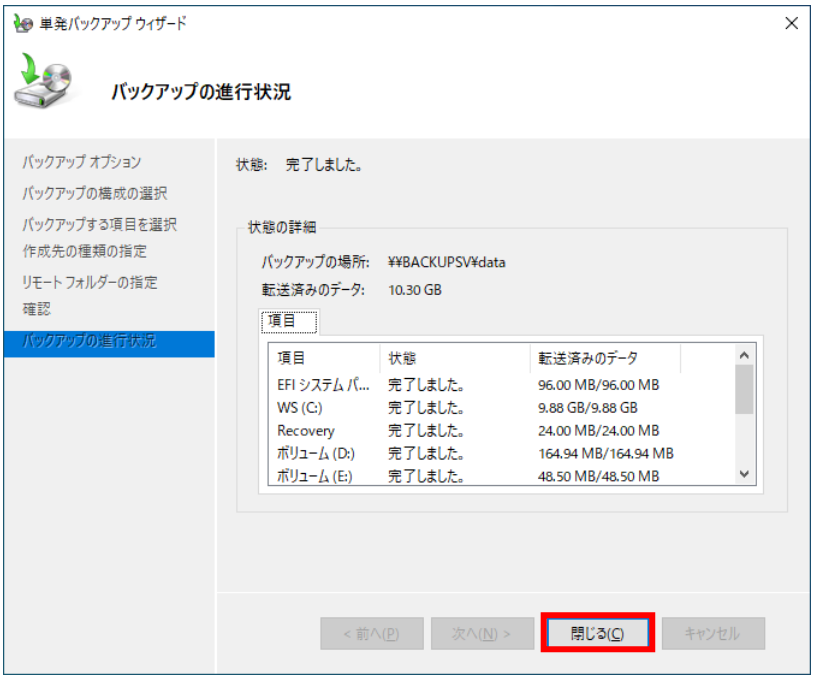
8. バックアップデータ保存先へのアクセスに利用するユーザー名とパスワードを入力して、[OK] をクリックします。



9. 選択した内容を確認し、[バックアップ] をクリックします。



10. バックアップが完了すると、以下の画面が表示されますので、[閉じる] をクリックします。



【補足】

バックアップ時にエラーが発生してバックアップが失敗した場合、[Windows Server バックアップ] 画面から失敗していることが確認できますが、Microsoft-Windows-Backup ログを確認すると、より詳細なエラー原因を確認できる場合があります。

Microsoft-Windows-Backup ログは、イベントビューアーの以下の場所から確認できます。

[イベントビューアー（ローカル）] – [Windows ログ] –

[アプリケーションとサービスログ] – [Microsoft] – [Windows] – [Backup] – [Operational]

3.4.3 Windows Server バックアップによるリストア

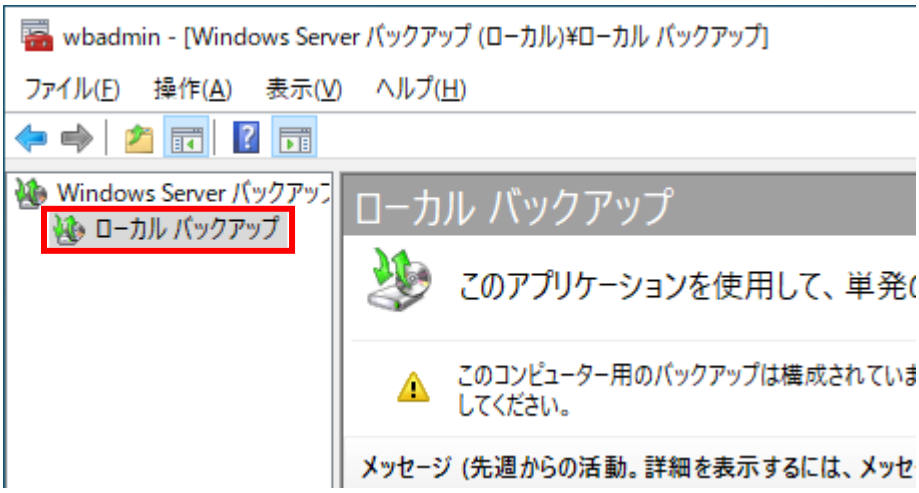
ここでは Windows Server バックアップを用いて、ネットワーク上の共有フォルダーに格納されたバックアップデータから、iStorage NS のデータボリュームをボリューム単位でリストアする方法を説明します。システムをリストア（ベアメタル回復）する場合は、メンテナンスガイドを参照してください。

なお、バックアップデータをネットワーク上の共有フォルダーに格納している場合は、以下の情報を事前に準備しておく必要があります。

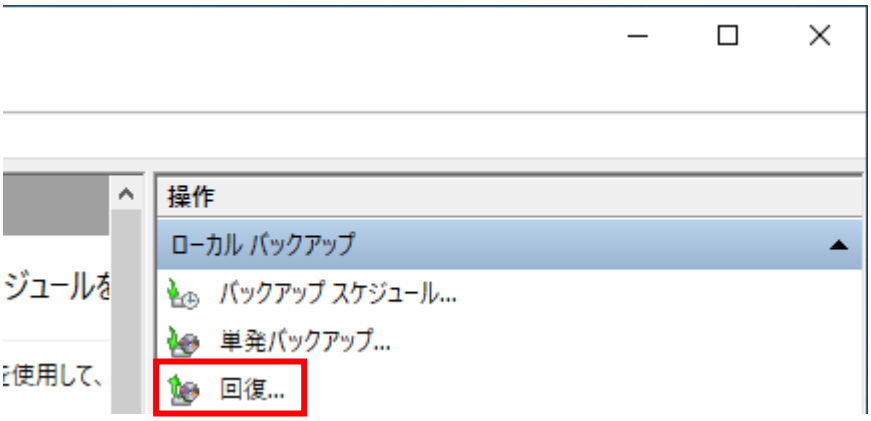
- バックアップデータ保存先サーバーのコンピューター名または IP アドレス
- バックアップデータ保存先共有名
- 共有アクセス用アカウント名
- 共有アクセス用パスワード

1. 管理者メニューから [Windows Server バックアップ] を起動します。

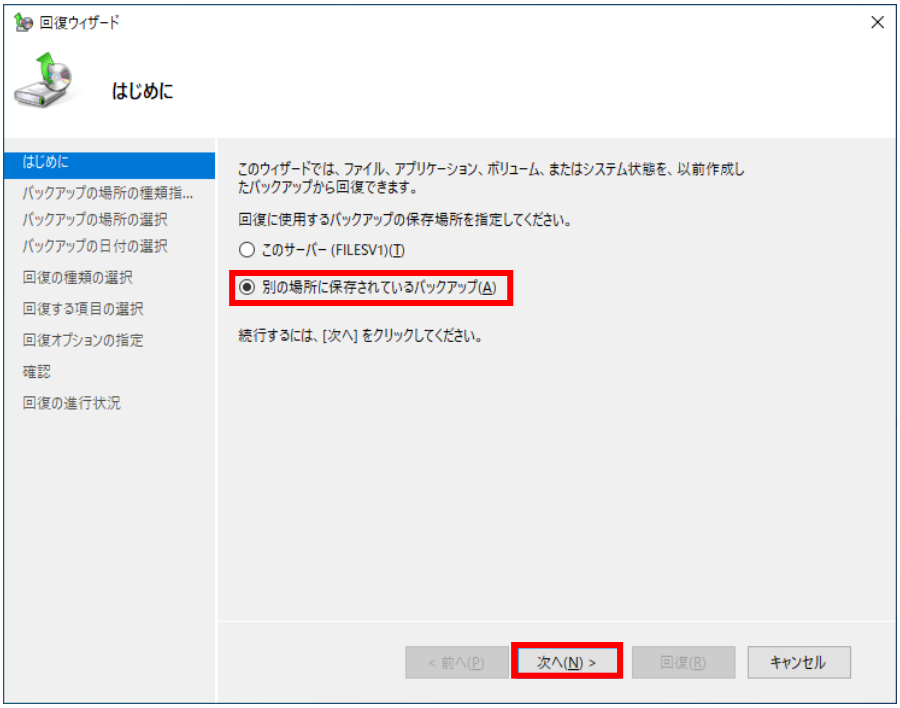
2. [ローカルバックアップ] をクリックします。



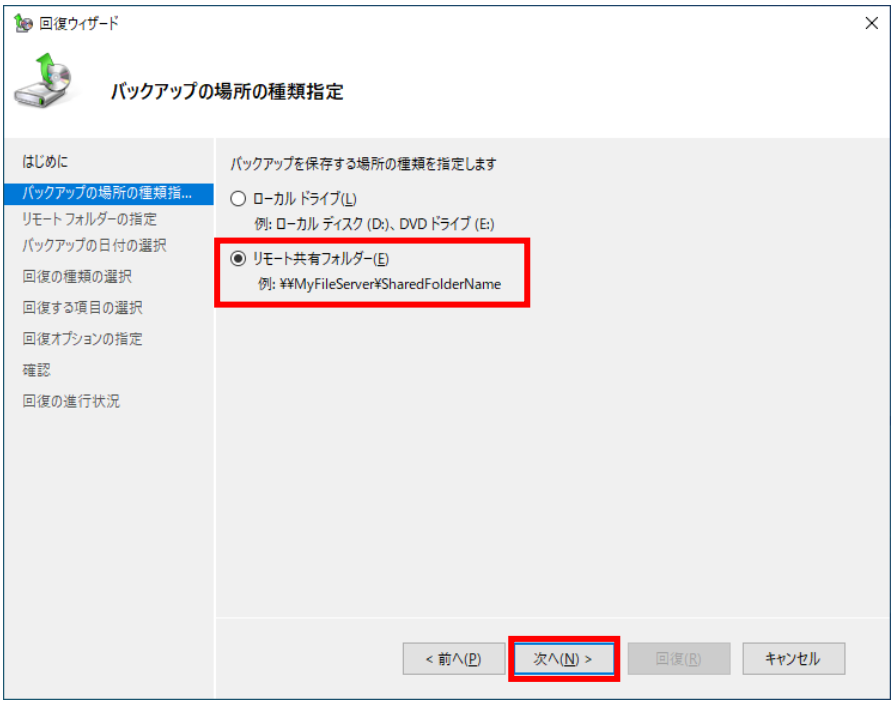
3. [回復…] をクリックします。



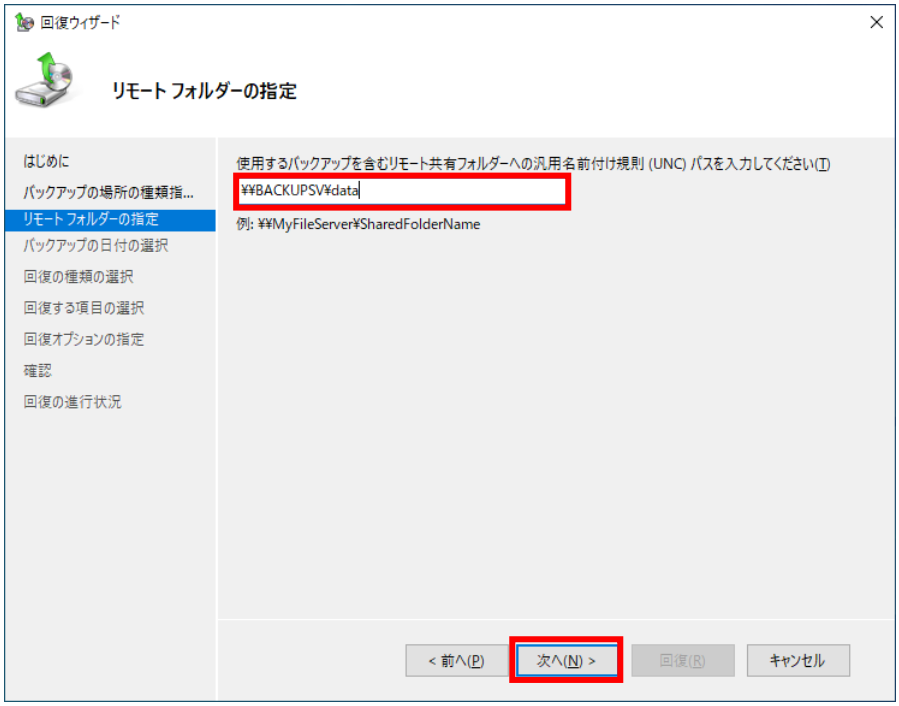
4. バックアップデータ保存先を選択して、[次へ] をクリックします。バックアップデータ保存先としてバックアップ専用のディスクを利用している場合は [このサーバー] を、ドライブ文字が付与されたローカルドライブやネットワーク上の共有フォルダーが保存先の場合は [別の場所に保存されているバックアップ] を選択します。



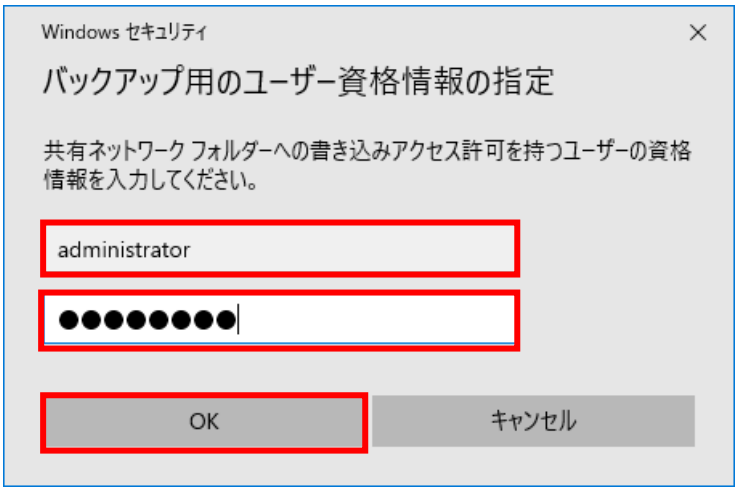
5. バックアップデータ保存先を選択して、[次へ] をクリックします。



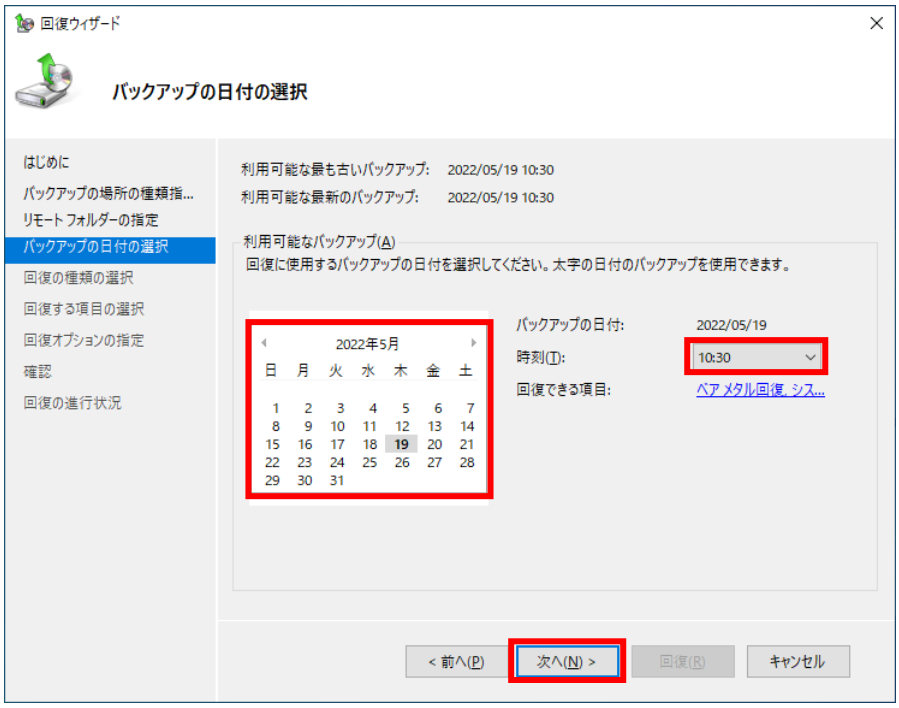
6. バックアップデータ保存先の共有フォルダーのパスを入力して、[次へ] をクリックします。



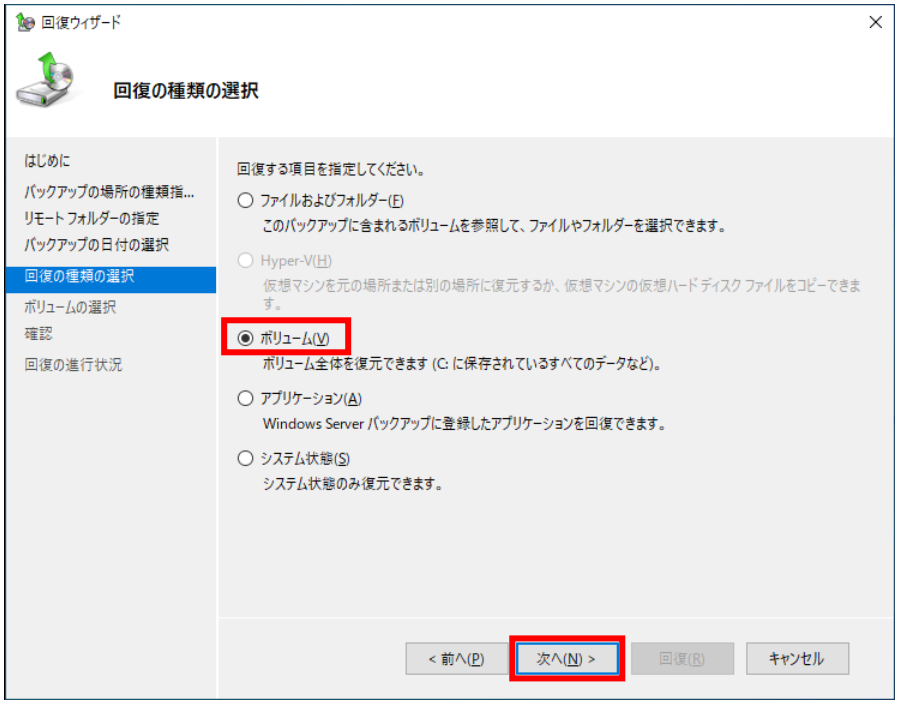
7. バックアップデータ保存先へのアクセスに利用するユーザー名とパスワードを入力して、[OK] をクリックします。



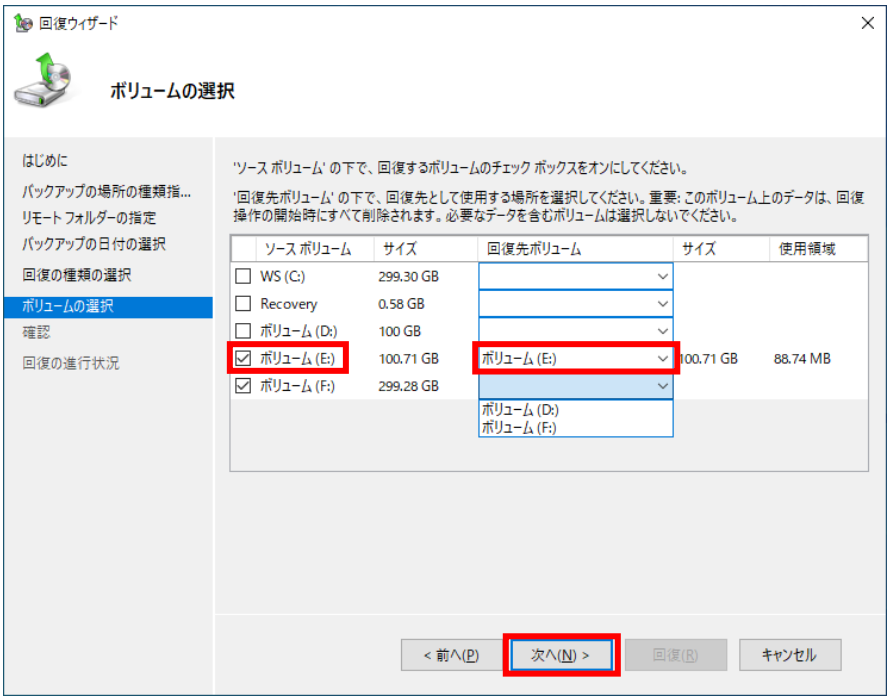
8. リストアしたいバックアップを選択して、［次へ］をクリックします。



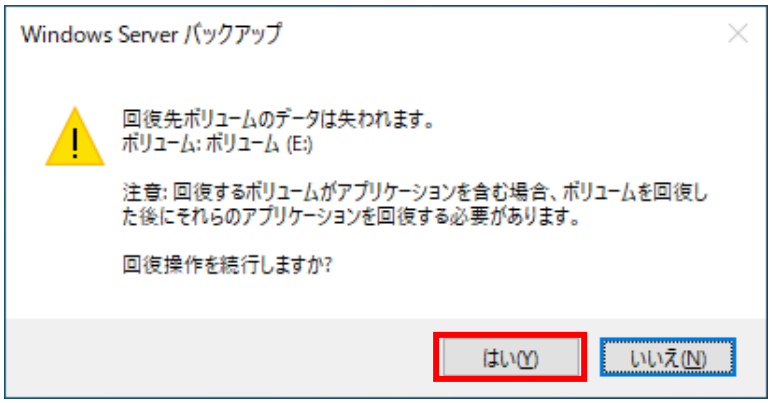
9. 回復の種類を選択して、[次へ] をクリックします。なお、ボリューム単位のバックアップから、ファイル・フォルダー単位でのリストアを選択することも可能です。



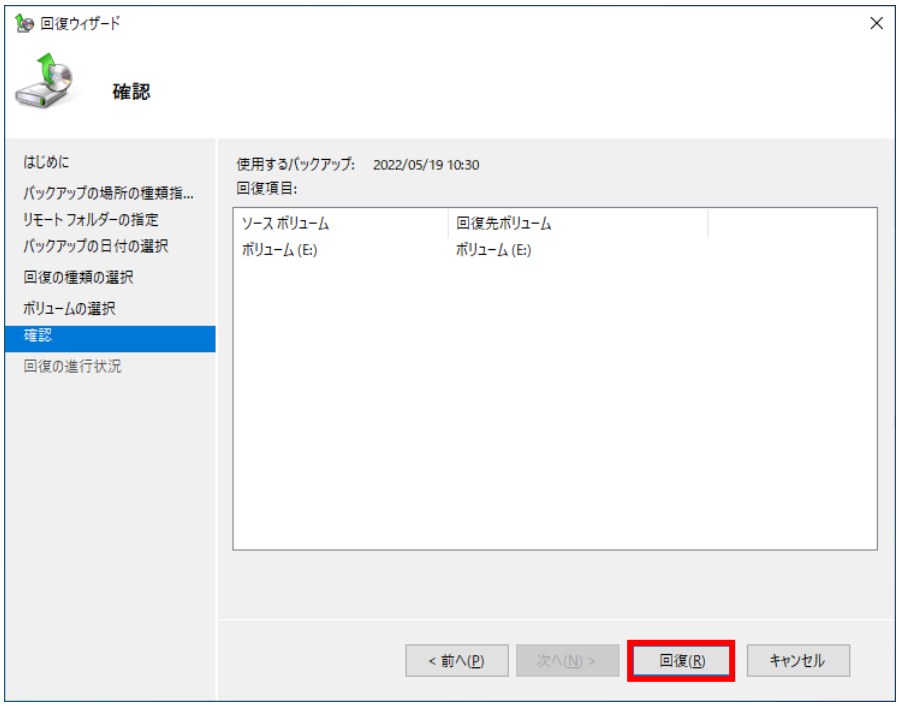
10. リストア対象ボリューム毎に回復先ボリュームを指定して、[次へ] をクリックします。



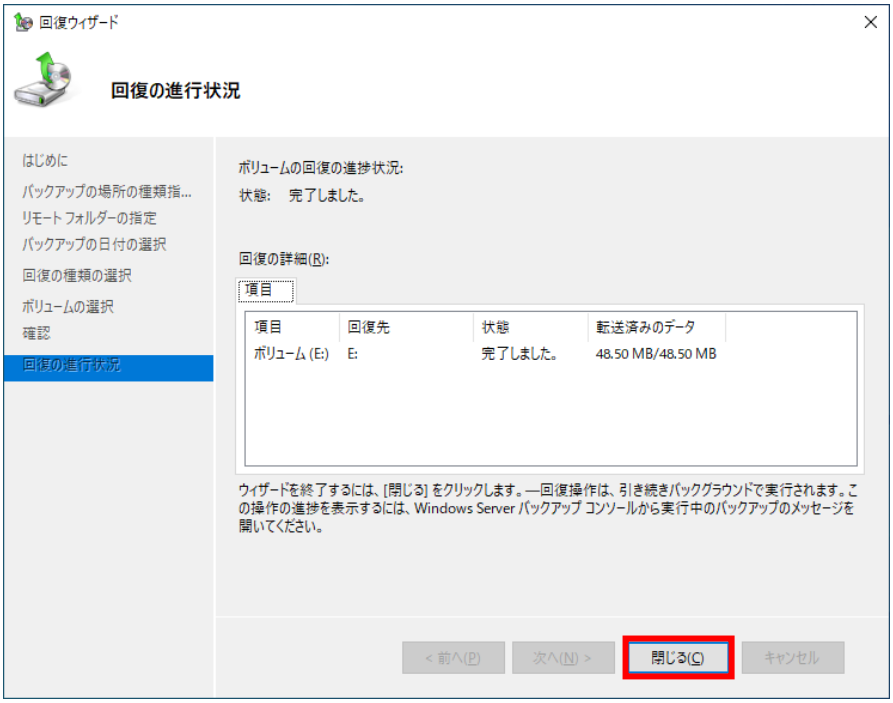
11. 記述内容を確認して、[はい] をクリックします。



12. 選択した内容を確認して、[回復] をクリックするとリストアが開始します。



13. リストアが完了すると以下の画面が表示されますので、[閉じる] をクリックします。



3.4.4 Windows Server バックアップ利用時の留意点

- バックアップをスケジュール設定にて実行する場合は、バックアップの所要時間を考慮し、できるだけシステムの負荷が少ない時間（業務が行われていない時間）にバックアップが行われるようにしてください。

- バックアップ対象のボリュームと、バックアップデータを保存するボリュームが物理的に同じディスクの場合、ディスクの障害によって実データとバックアップデータの両方が同時に破損する恐れがあります。このため、バックアップデータ保存先は、以下を推奨いたします。
  - 本機のバックアップ対象とは物理的に異なるディスク
  - 本機の固定ディスクモードの RDX ドライブ
  - 本機以外のネットワーク共有フォルダー

- バックアップデータ保存先をローカルボリュームとし、スケジュールバックアップを設定した場合は、バックアップデータを複数世代保存することができますが、空き容量が十分でない場合、期待する世代を格納できない、または、バックアップが失敗する場合がありますので、保存先ローカルディスクの空き容量については十分に配慮してください。

- バックアップデータ保存先をローカルボリュームとし、バックアップを実行すると連動するシャドウコピー機能がスナップショットを作成します。シャドウコピー機能を一度も有効にしていないローカルボリュームを保存先とした場合、シャドウコピー領域の最大サイズを独自に設定します。この状態で、バックアップ運用を継続するとボリュームサイズの最大 30%がシャドウコピー領域として使用されます。バックアップデータ保存先のボリュームサイズが大容量の場合、ボリュームの空き容量が意図せず減少することになりますので必要に応じて、手動で最大値を変更してください。変更方法は、本書の【シャドウコピー記憶域の設定】を参照してください。

- ボリュームを指定し、バックアップを行う場合、指定できるボリュームの最大サイズは 16TB です。

- ドメインに参加している iStorage NS のバックアップデータ保存先をネットワーク上の共有フォルダーに設定してバックアップを行う場合は、バックアップデータ保存先のサーバーを同一のドメインに参加させてください。

- ベアメタル回復時に使用する WinRE では、VLAN ID を設定できません。ベアメタル回復を目的としたバックアップイメージのデータ保存先をネットワーク上の共有フォルダーに設定する場合は、VLAN ID が設定されていない共有フォルダーを設定してください。

- iStorage NS に、新しいバージョンの Starter Pack を適用すると、適用前に取得したベアメタル回復のバックアップデータは使用できません。ベアメタル回復にて、システムを回復する必要がある場合は、Starter Pack の適用後に必ずベアメタル回復用のバックアップデータを取得してください。

- バックアップデータは以下の手順により削除できます。

  1. 管理者権限でコマンドプロンプトを開き、以下のコマンドを実行します。

     wbadmin get versions

     保存しているバックアップのリストが表示されますので、削除したいバックアップの 「バージョン識別子:」を確認してください。

     >バージョン識別子: 08/29/2020-03:30

  2. 「1.」で確認したバージョン識別子を使用し、以下のコマンドを実行します。

     wbadmin delete backup -version:08/29/2020-03:30 –quiet

     ※「バージョン識別子:」の内容を"-version:"の後ろに指定します。

     実行後、削除されたことを示す以下のメッセージが表示されます。

     > バックアップを削除する操作が完了し、

     > 1 個のバックアップが削除されました。

- バックアップ時にエラーが発生してバックアップが失敗した場合、[Windows Server バックアップ] 画面から失敗していることが確認できますが、Microsoft-Windows-Backup ログを確認すると、より詳細なエラー原因を確認できる場合があります。

  Microsoft-Windows-Backup ログは、イベントビューアーの以下の場所から確認できます。

  [イベントビューアー（ローカル）] – [Windows ログ] – [アプリケーションとサービスログ] – [Microsoft] – [Windows] – [Backup] – [Operational]

3.4.5 注意・制限事項

- バックアップを実行するユーザーは Administrators グループまたは Backup Operators グループに所属している必要があります。

- バックアップデータ保存先をネットワーク上の共有フォルダーとした場合は、バックアップデータを複数世代保存することはできません。毎回上書き保存されます。

- Windows Server バックアップ の GUI 画面から、完了 （警告あり） となっているバックアップの詳細を表示しようとすると、[スナップインのエラーが MMC により検出されたので、スナップインがアンロードされます。] というエラーが発生して内容が確認できないことがあります。
  本現象が発生した場合、C:¥Windows¥Logs¥WindowsServerBackup¥ 配下の [Backup_Error-dd-mm-yyyy_hh--mm--ss.log] という形式で保存されているログをメモ帳等で直接開くことで、警告の詳細を確認することができます。

- 自動マウント機能を無効にした状態で、バックアップすることはできません。
  例えば、iStorage NS シリーズに iStorage M シリーズを接続し、「iStorage DynamicDataReplication（DDR）」を使用している環境において、自動マウント機能を無効にしている場合、Windows Server バックアップによるバックアップはご利用いただけません。

  自動マウント機能が無効か否かについては、以下の手順で確認できます。
  1. 管理者権限でコマンドプロンプトを起動します。
  2. diskpart を実行します。
  3. automount コマンドを実行し、自動マウントの状態を確認します。
     DISKPART> automount
     新しいボリュームの自動マウントが無効（有効）です。
  4. exit コマンドにて、diskpart を終了します。

  自動マウントが無効の場合は、管理者権限のコマンドプロンプトにて、以下のコマンドを実行することにより、有効に変更できます。
  mountvol /E

【補足】
・ 変更後は、再度手順 2～4 を行い、有効となったことを確認してください。
・ 自動マウント機能は、有効の状態で出荷しています。無効となっている場合は、有効に変更する前に、導入しているアプリケーションなどに影響がないか確認してください。

- FAT 形式でフォーマットされたボリュームにバックアップを保存することはできません。
- 特定の拡張子をもったファイルだけをバックアップすることはできません。
- バックアップしたデータに対してアクセス制限を行うことはできません。バックアップデータを格納したフォルダーのアクセス制限にてご対応ください。
- スケジュールバックアップの際、バックアップの日付指定や祝日を考慮した設定はできません。一旦、バックアップウィザードで設定後、タスクスケジューラにて日付指定に変更することは可能です。
- テープ装置へのバックアップはサポートしていません。
- コールドバックアップ（OS を起動していない状態でのバックアップ）はできません。
- バックアップデータ保存先のボリュームには、シャドウコピーは設定しないでください。
- バックアップデータのフォルダー（WindowsImageBackup）のフォルダー名を変更すると、リストア時に Windows Server バックアップがバックアップデータを認識出来なくなるため、フォルダー名は変更しないでください。また、同様の理由により、本フォルダーをボリュームまたは共有フォルダーのルートフォルダー以外のフォルダーに移動しないでください。
- Windows Server バックアップにて世代を管理する場合、バックアップデータの差分をシャドウコピー機能によって管理しています。このため、バックアップ専用ディスク上ではないローカルボリュームをバックアップデータ保存先とした場合、以下の 2 点に注意が必要です。

  - バックアップデータ保存先ボリュームで I/O 高負荷状態が発生すると、 シャドウコピーによる差分収集が行えなくなり、その結果、最新以外のバックアップ世代が破棄される場合があります。このとき、システムイベントログにエラーイベント Volsnap/25 が記録されます。
  - バックアップデータ保存先ボリュームにバックアップデータ以外のデータを格納していると、バックアップ時に作成されるスナップショットにそのデータ差分も含まれます。
    このため、バックアップデータが消費する容量の見積もりが難しくなり、想定していた世代を残せない場合があります。

- シャドウコピー領域をバックアップすることはできません。
- Windows Update 履歴はバックアップされません。バックアップしたシステムボリュームを回復すると、Windows Update 履歴はクリアされた状態で復元されます。

4 iStorage NS のその他の使い方

- 削除済みのファイルを完全に消去する
- **iStorage NS** 上のファイルを高速検索する
- **iSCSI** を利用する

4.1 削除済みのファイルを完全に消去する

ファイルやフォルダーをゴミ箱から消去したり、パーティションを削除しても、ディスク領域への割り当て解除が行われるだけでデータ自体はディスク上に残るため、特殊なツールを使用するとファイルの内容を復活させることが可能です。情報漏えいを防止するためにも、不要となったデータは完全に消去しておく必要があります。

iStorage NS では、ボリューム内の空き領域（ファイルやフォルダーが割り当てられていない領域）を特定のデータで上書きすることでディスク上のファイルデータを消去する、ディスク・ワイプと呼ばれる機能が標準で用意されています。ディスク・ワイプには cipher コマンドの /w オプションを使用します。例として以下に、D ドライブ内の削除済みデータを消去する場合の手順を説明します。

1. 管理者メニューから [コマンドプロンプト] を起動します。

2. 以下の構文でコマンドを実行します。
   cipher /w:d:　　（d はドライブ文字）

処理が完了すると、プロンプトに戻ります。既存のファイルおよびフォルダーを残して空き領域が上書きされ、データが消去されます。

【注意】
- cipher /w コマンドでは、ボリュームの空き領域のみを上書きします。実行前には不要なファイルやフォルダーを削除しておいてください。
- 対象のボリュームにシャドウコピーを使用している場合、コマンド実行前にシャドウコピーを解除してください。解除しない場合、シャドウコピーから以前のファイルが復元できる可能性があります。
- 上書きする領域が大きい場合は、処理に時間がかかることがあります。
- NTFS ボリュームのみで実行可能です。
- 正しく消去されたことを確認する方法はありません。

4.2 iStorage NS 上のファイルを高速検索する

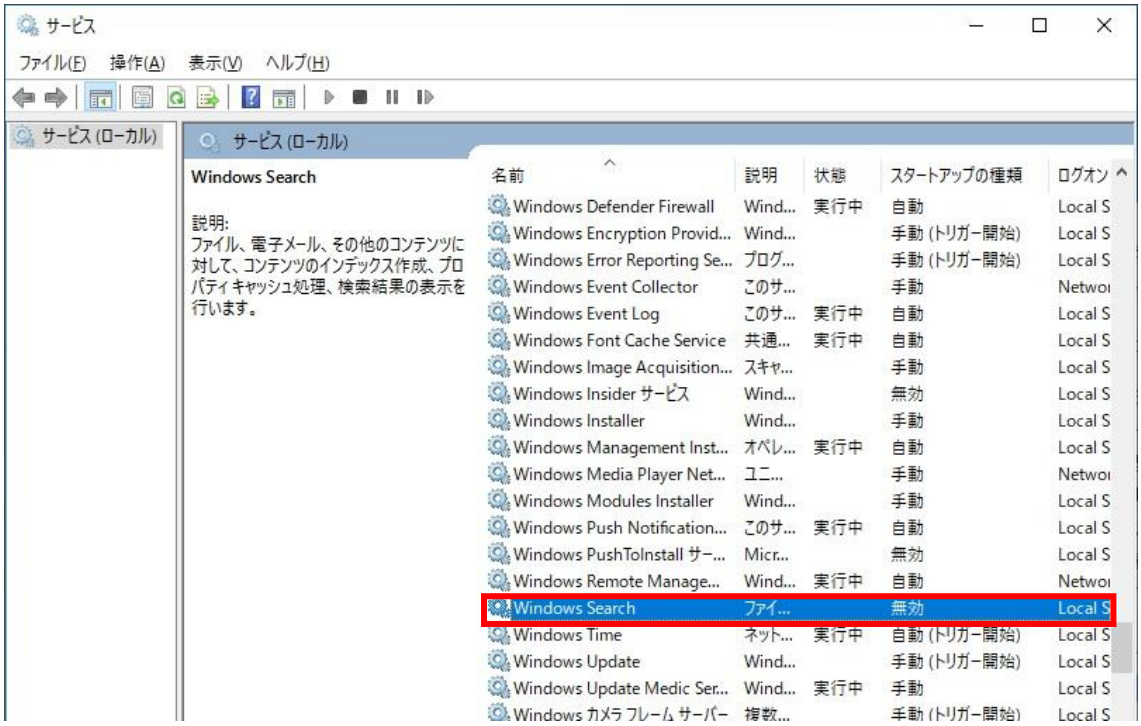
Windows サーチサービスは、iStorage NS 上のファイルのインデックスを作成し、クライアント PC からのファイル検索を高速化する機能です。なお、Windows サーチサービスは出荷状態では停止されていますので、ご利用になる場合はサービスを開始してください。ここでは、Windows サーチサービスを特定のフォルダーに対して有効とし、高速検索を行う手順を説明します。

【注意】

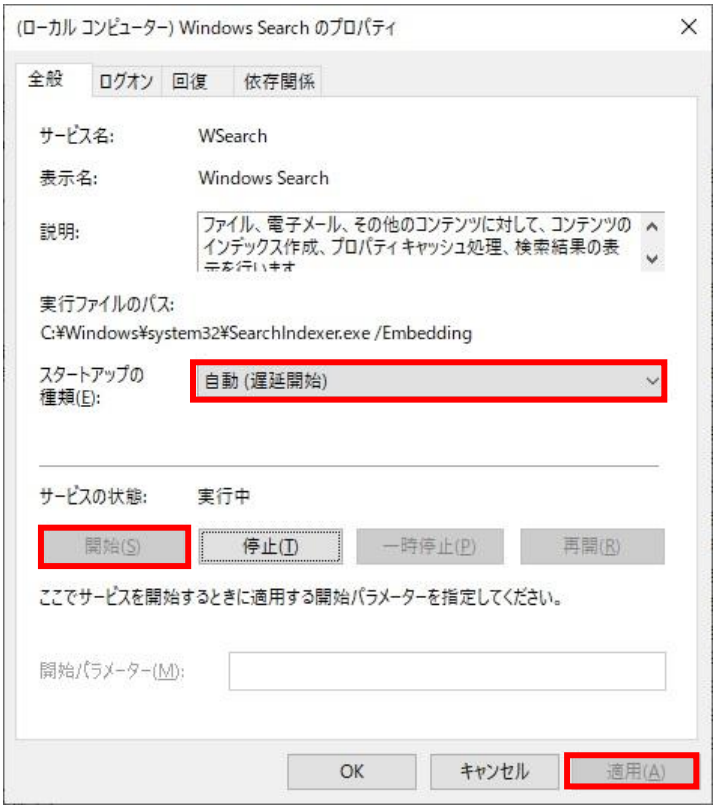
- Windows サーチサービスを開始すると、導入時や定期的な検索テーブル更新時、CPU に高い負荷がかかることが予想されますので、ご注意ください。
- iStorage NS シリーズのリモートデスクトップやコンソールからの実行を含め、同時に 4 件を超えるファイル検索を実行すること、100 万ファイル以上を対象にファイル検索を実行することは、iStorage NS シリーズのパフォーマンスを著しく低下させる可能性がありますので、その様な運用は推奨しておりません。
- データ重複除去を設定しているドライブに対して、Windows サーチを実行すると、結果が正しく表示されない場合があります。
- マイクロソフト社では分散ファイルシステム (DFS) 環境やクラスター環境での Windows サーチ 機能の使用を推奨しておりませんので、導入に際しては十分にご注意ください。

1. 管理者メニューの [サービス] をクリックします。

2. [Windows Search] をダブルクリックします。



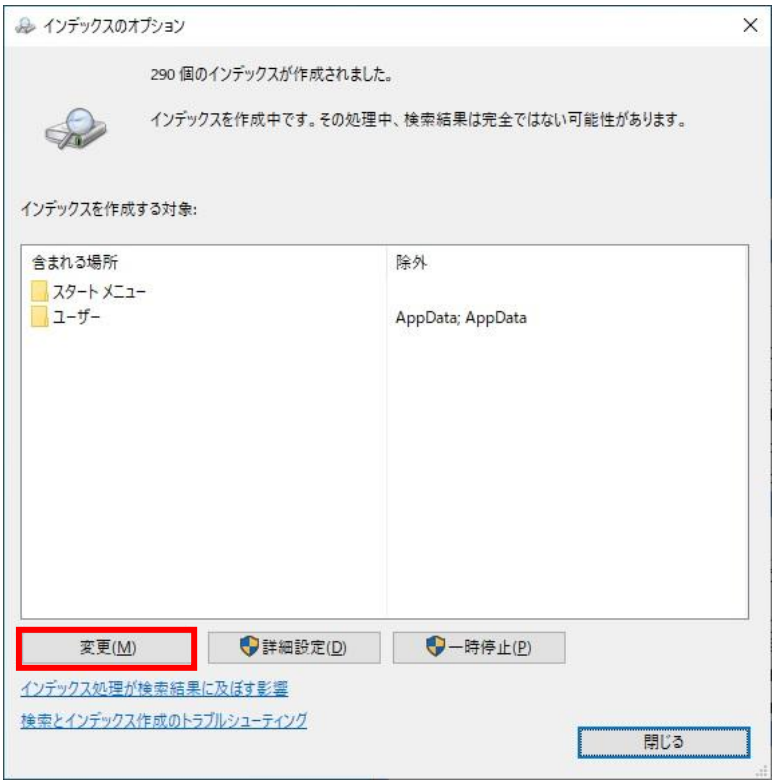
3. [全般] タブの [スタートアップの種類] で [自動(遅延開始)] を選択し、[適用] をクリックした後、[開始] をクリックします。



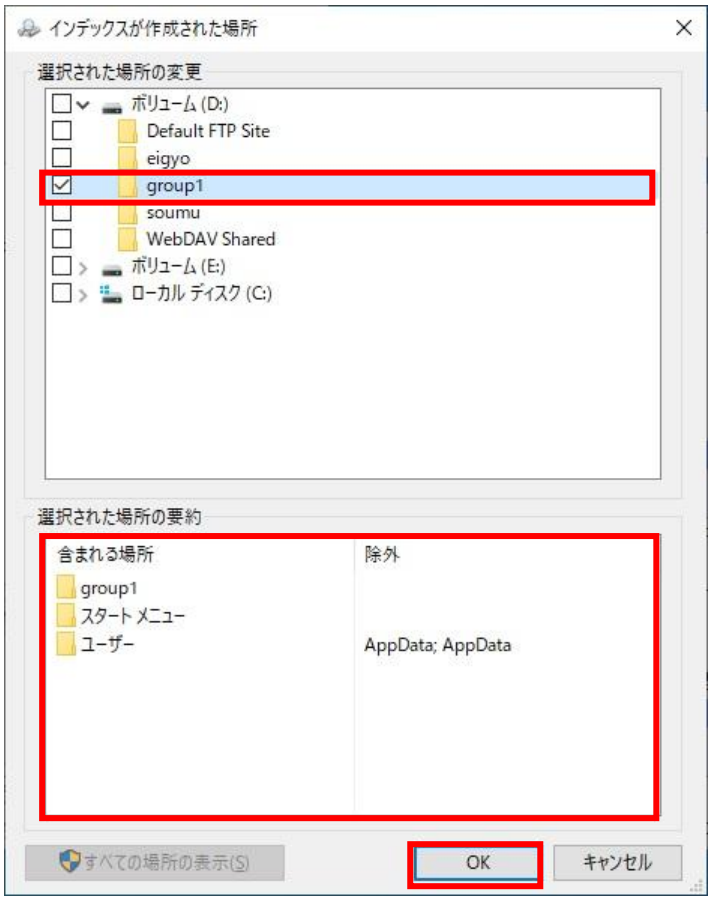
4. [OK] をクリックし、プロパティを閉じます。

5. 管理者メニューの [インデックスのオプション] をクリックします。

6. [変更] ボタンをクリックします。



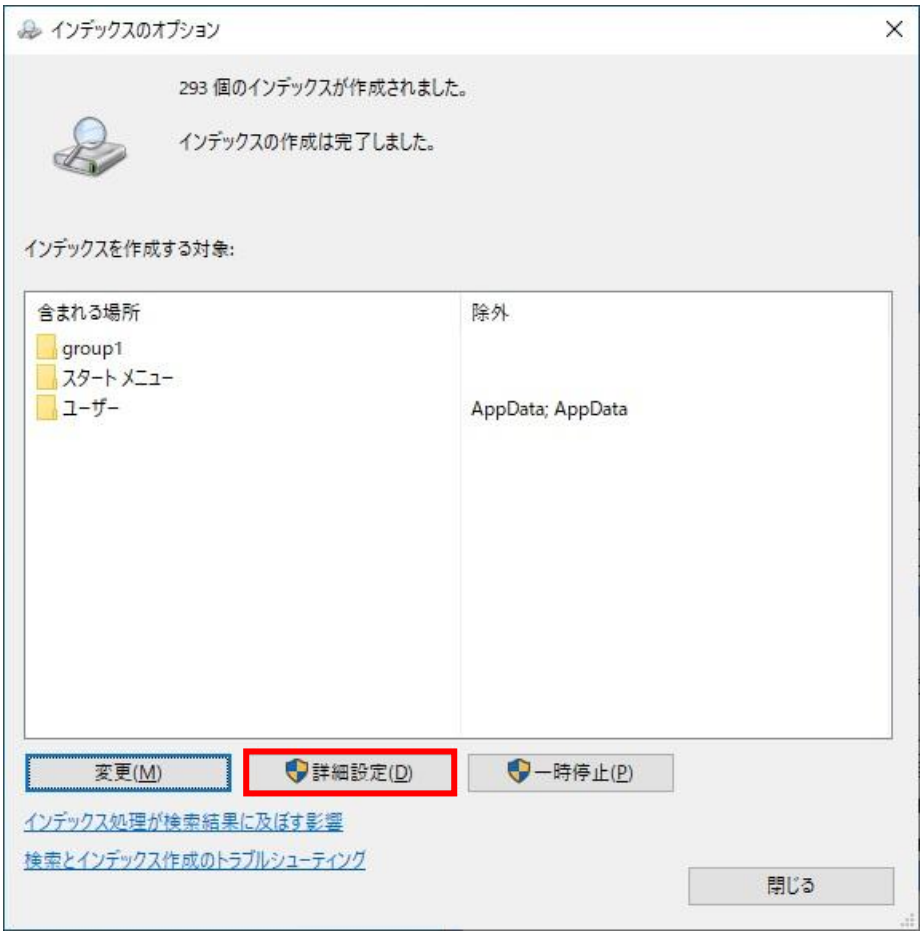
7. [選択された場所の変更] で、Windows サーチ機能を有効とするフォルダーを選択します。[選択された場所の要約] に選択したフォルダーが追加されたことを確認して [OK] ボタンをクリックします。



【注意】

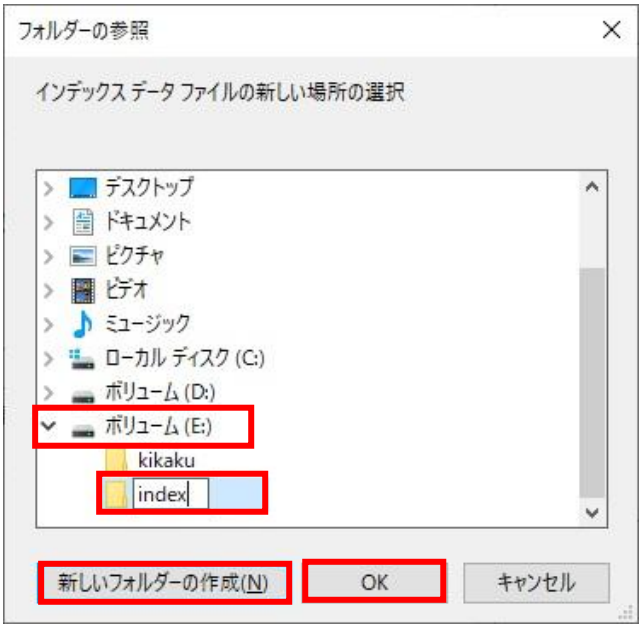
Windows サーチサービスのインデックスは、既定ではシステムドライブに作成されます。このため Windows サーチサービスの対象として追加したフォルダー内に多数のファイルが存在する場合、システム領域を圧迫しシステムの動作に支障を及ぼすことが予想されます。項番 8、9、10、11 の操作にて、インデックスの作成先を変更してください。

8. [インデックスのオプション] 画面で [詳細設定] をクリックします。



9. [インデックスの場所] の [新しい場所の選択] をクリックします。

10. システムドライブ以外のドライブを選択し、[新しいフォルダーの作成] をクリックします。作成された新しいフォルダーに任意の名前を入力して [OK] をクリックします。



11. [詳細オプション] 画面で [OK] をクリックします。サービスが再起動し、インデックスの作成先が上記で設定した新しいインデックスの場所に変更されます。

【注意】

既に Windows サーチサービスを有効にしていた場合、上記の項番 8、9、10、11 の操作を行っても以前使用していたインデックスファイルは自動削除されませんので、システムドライブに存在するインデックスフォルダーを手動で削除してください。

12. [閉じる] ボタンをクリックして、[インデックスのオプション] 画面を閉じます。

4.3 iSCSI を利用する

4.3.1 iSCSI の概要

ローカルの SCSI デバイスへアクセスするには、SCSI コマンドを使用します。
iSCSI（Internet Small Computer Systems Interface）では、SCSI コマンドを TCP/IP プロトコルに包み込んでネットワークに転送し、リモートにあるストレージデバイスへのアクセスを実現します。
これにより、統合された記憶域の実装や集中管理が容易になります。
iStorage NS シリーズに iSCSI ターゲットを導入することで、NAS としての利用だけでなくブロックストレージデバイスとしての利用も可能になります。ディスク容量の不足したコンピューター (iSCSI イニシエーター) に対して、ブロックデバイスを安価に提供することができます。
なお、iSCSI プロトコルはブロックデバイスアクセスのため排他制御は行われません。このため、1 つの iSCSI 仮想ディスクには複数の iSCSI イニシエーターから同時にアクセスしないように設計してください。

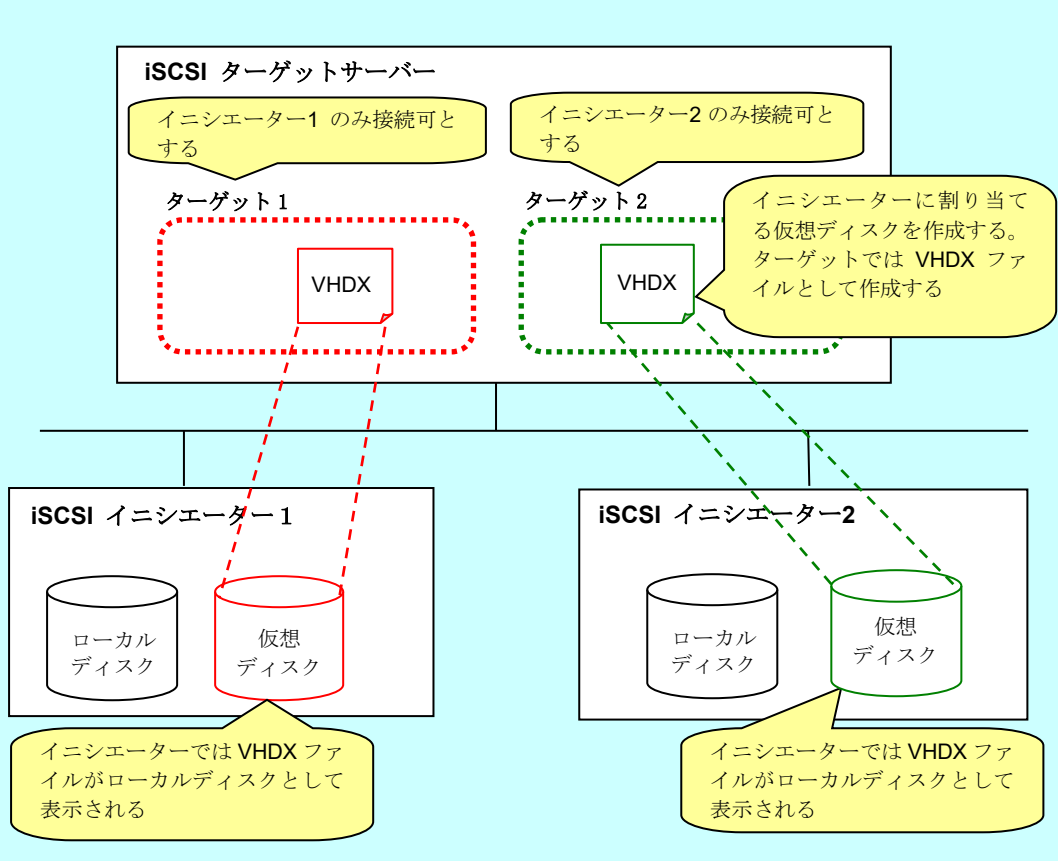
- **iSCSI ターゲット**
  iSCSI ターゲット は、iSCSI イニシエーターに記憶域を提供します。

- **iSCSI イニシエーター**
  iSCSI イニシエーター は、iSCSI ターゲットによって提供されるリモートの記憶域をローカルドライブと同等にアクセスできる機能を提供します。Windows Server 2008 以降の Windows OS には標準で iSCSI イニシエーターが搭載されています。

以下に、代表的な構成例を記載します。

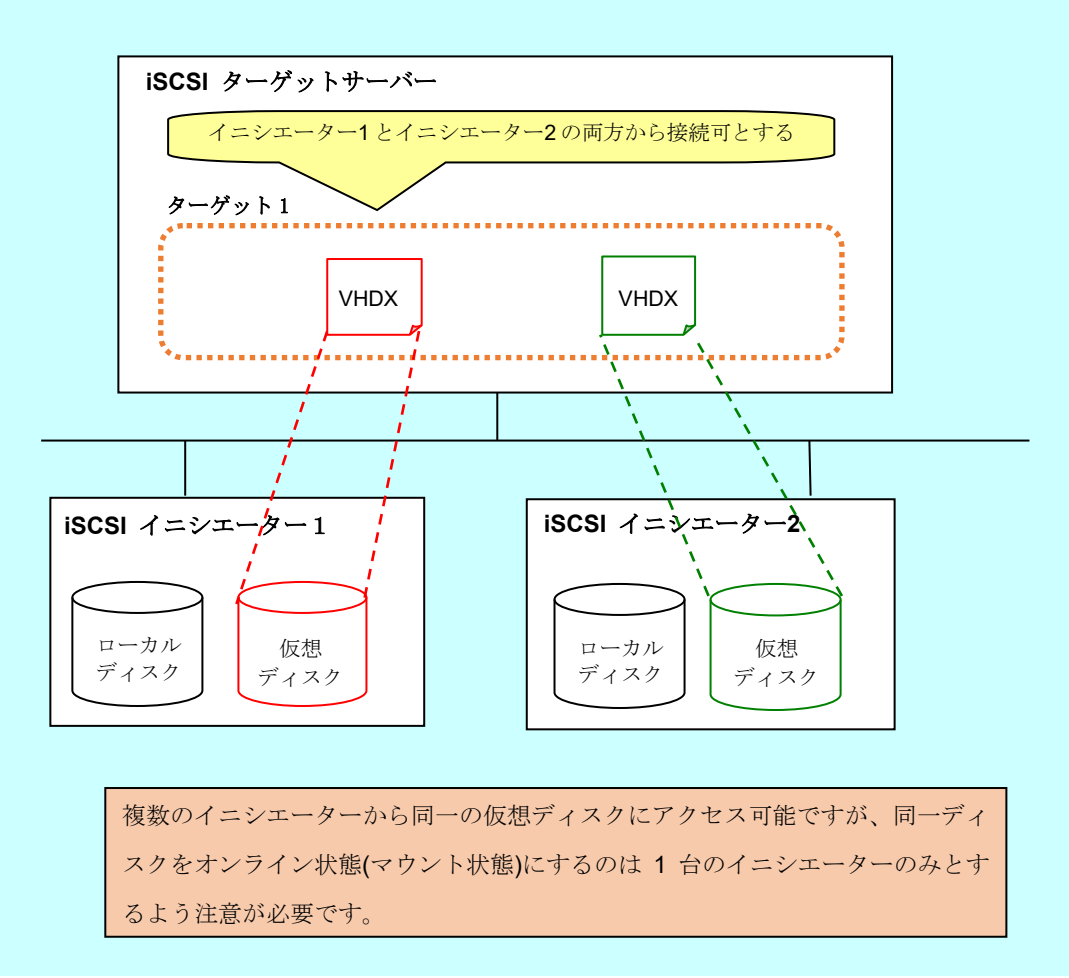
【各イニシエーターに対応する専用のターゲットを作成 (推奨設定) 】

下記の図のように、iSCSI ターゲットサーバー上にイニシエーター数分のターゲットを作成し、それぞれに VHDX ファイル(仮想ディスク)を作成します。各ターゲット毎に接続可能なイニシエーターを 1 つ設定することで、各イニシエーターからは、自サーバー専用の仮想ディスクを利用可能になります。
イニシエーター数分のターゲットを複数作成する作業が必要となりますが、各イニシエーター毎にアクセス可能な VHDX ファイル(仮想ディスク) が分離され、1 つの VHDX ファイルに複数のイニシエーターからアクセスされる可能性がありません。

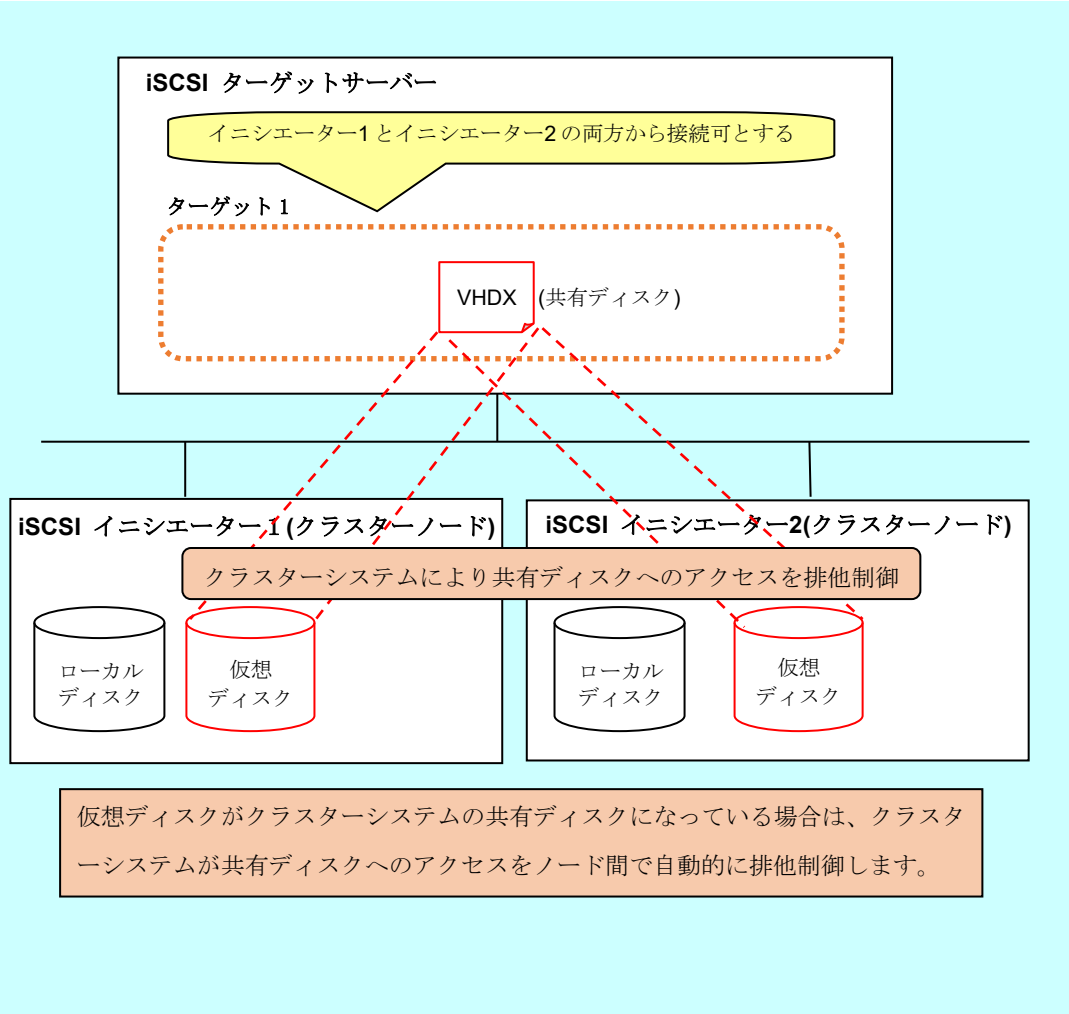


【複数のイニシエーターから接続可能なターゲットを 1 つ作成(共有ディスク)】

下記の図のように、iSCSI ターゲットサーバー上にターゲットを 1 つ作成し、VHDX ファイル(仮想ディスク)をイニシエーター数分作成します。ターゲットに接続可能なイニシエーターを複数設定することで、自サーバー専用の仮想ディスクを利用可能になります。本構成では、ターゲットを複数作成する作業が必要ありませんが、設定に誤りがあった場合、後述のようにディスクが破壊されるリスクがあります。
iSCSI ターゲット上の仮想ディスクを、クラスターシステムの共有ディスクとして利用する場合は、どのクラスターノード(iSCSI イニシエーター)からでも同じ共有ディスクに接続可能にする必要があります。
ただし、複数のイニシエーターから同一の仮想ディスクを同時にオンライン状態（マウント状態）にすると、ターゲット側では排他制御が行われませんので、仮想ディスク上のファイルシステムが破損します。
このため、クラスターシステム等によって各ノードから共有ディスクへのアクセスが排他制御されない環境では、複数のイニシエーターから同じ仮想ディスクを同時にオンライン状態にしないようにしてください。



クラスターシステムで iSCSI ターゲット上の VHDX ファイル(仮想ディスク)を共有ディスクとして使用する場合のイメージは下記のようになります。

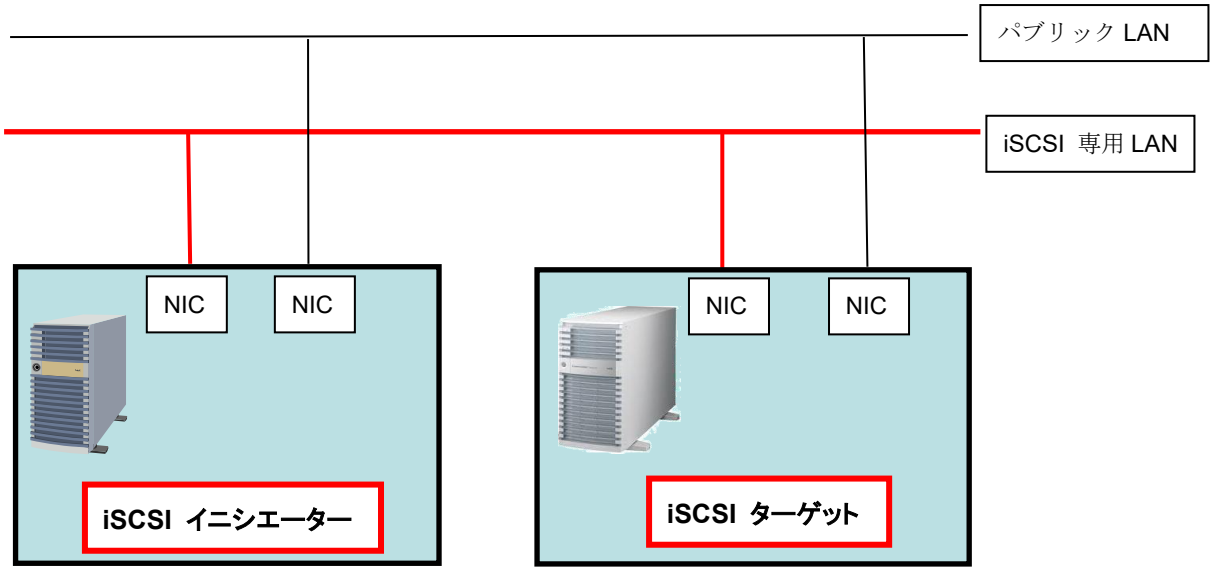


4.3.2 ネットワーク構成

iSCSI ターゲットと iSCSI イニシエーターの接続方式には、シングルパスおよびマルチパスがあります。運用形態および信頼性を考慮した上で、いずれかを選択してください。なお、接続方式としてマルチパスを使用する場合、イニシエーター側の装置上にてマルチパス I/O 機能のインストールおよび設定を実施する必要があります。マルチパス I/O 機能はイニシエーター側で動作する機能であるため、ターゲット側の装置上では、マルチパス I/O 機能のインストールは不要です。

【注意】
本機は、NIC チーミング(LBFO)の NIC(仮想 NIC)を使用した iSCSI 接続/通信をサポートしておりません。iSCSI 接続の二重化につきましては、マルチパス I/O をご利用ください。

【シングルパス構成例】



【注意】
iSCSI イニシエーターと iSCSI ターゲットとの間の通信には自動プライベート IP アドレス指定(169.254.x.x) を使用しないでください。

4.3.3 セキュリティ

iSCSI ターゲットは、iSCSI イニシエーターと iSCSI ターゲットの間で転送されるデータのセキュリティを確保するために、暗号化と認証の両方をサポートしています。

暗号化（IPsec）

iSCSI ターゲットでは、インターネット プロトコル セキュリティ (IPsec) を使用してデータを暗号化しています。

認証（CHAP 認証およびリバース CHAP 認証）

iSCSI ターゲットでは、CHAP 認証とリバース CHAP 認証を使用できます。既定では、CHAP 認証もリバース CHAP 認証も有効になっていません。利用する場合には iSCSI ターゲットと iSCSI イニシエーターの双方で設定する必要があります。

4.3.4 諸元

iSCSI ターゲットの各種諸元値につきましては、下記のマイクロソフト社の公開情報をご確認ください。

タイトル： iSCSI ターゲット サーバーのスケーラビリティ制限
URL ： https://docs.microsoft.com/ja-jp/windows-server/storage/iscsi/iscsi-target-server-limits
(2026 年 6 月 1 日現在)

なお、上記は機械翻訳のため、表現がわかりにくい場合は下記の英語の原文にてご確認ください。

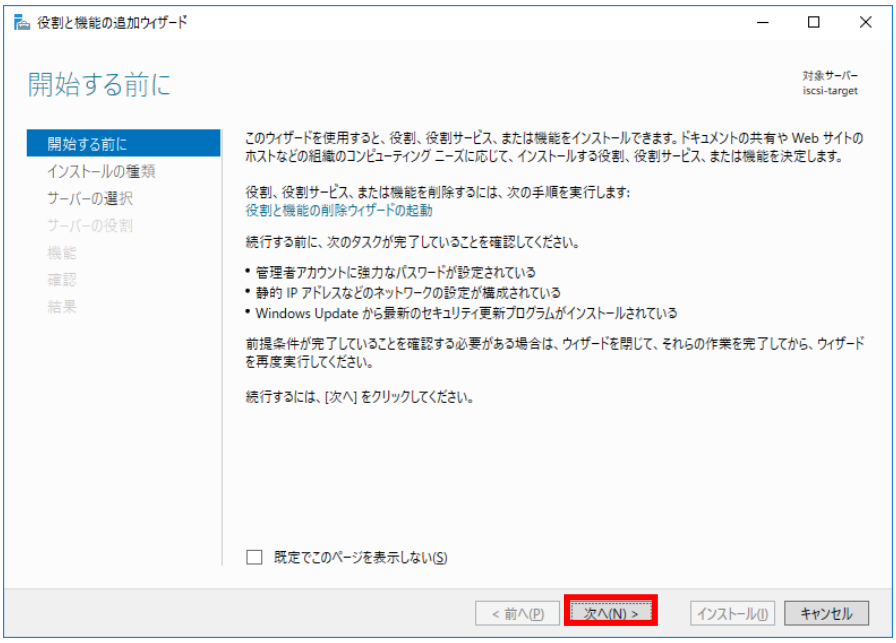
タイトル： iSCSI Target Server Scalability Limits
URL ： https://docs.microsoft.com/en-us/windows-server/storage/iscsi/iscsi-target-server-limits
(2026 年 6 月 1 日現在)

4.3.5 iSCSI ターゲットのインストール

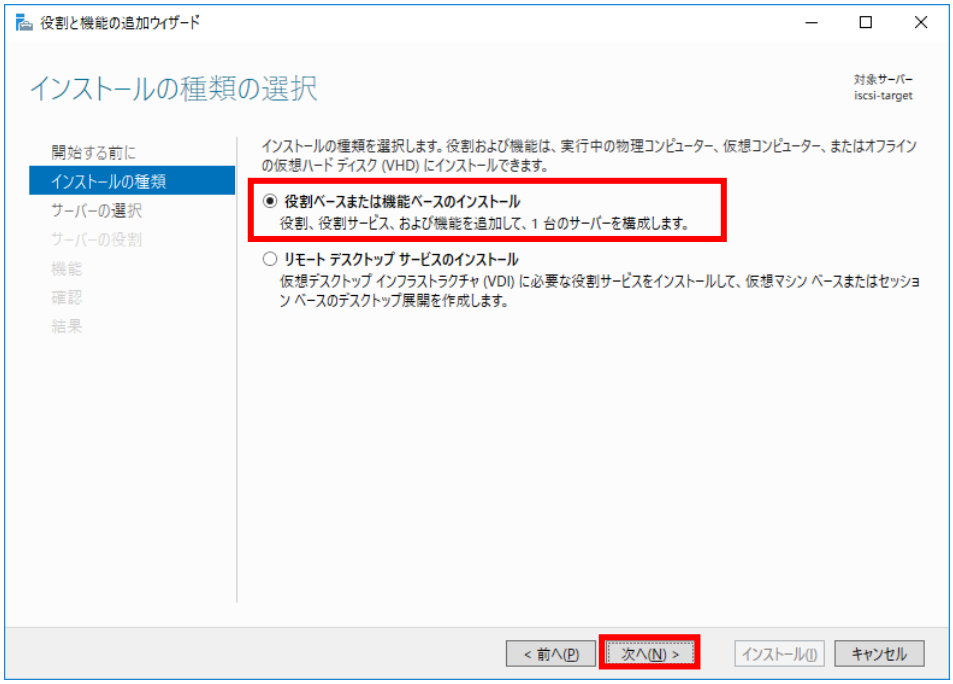
iSCSI ターゲットは出荷状態ではインストールされていませんので、使用に際しては、下記の手順にてインストールする必要があります。

1. サーバーマネージャーの [管理] - [役割と機能の追加] をクリックします。

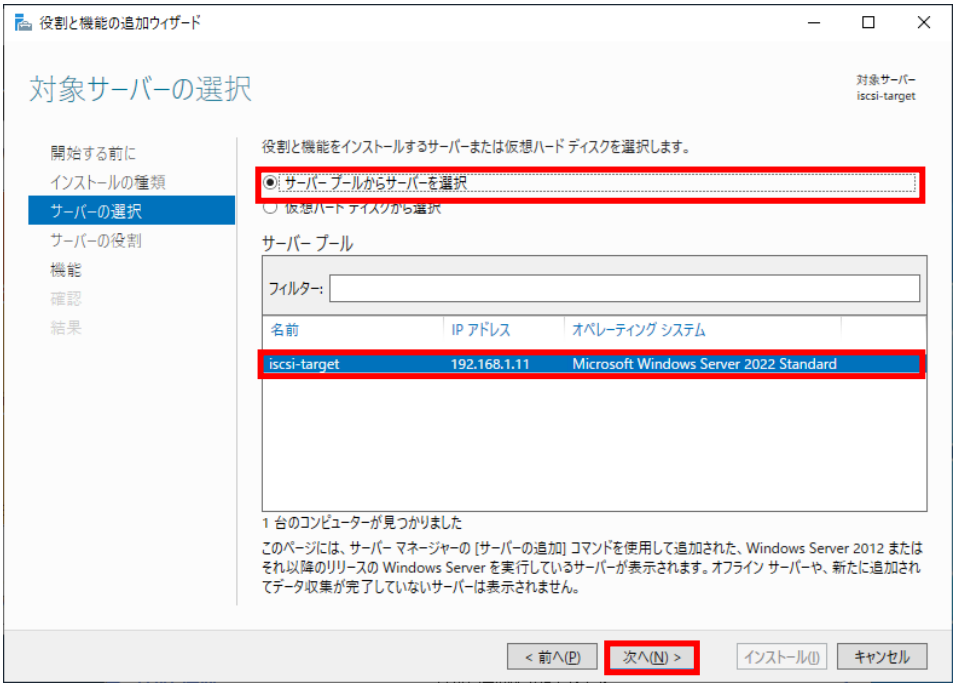
2. [役割と機能の追加ウィザード] が起動して、[開始する前に] が表示されます。 [次へ] ボタンをクリックします。



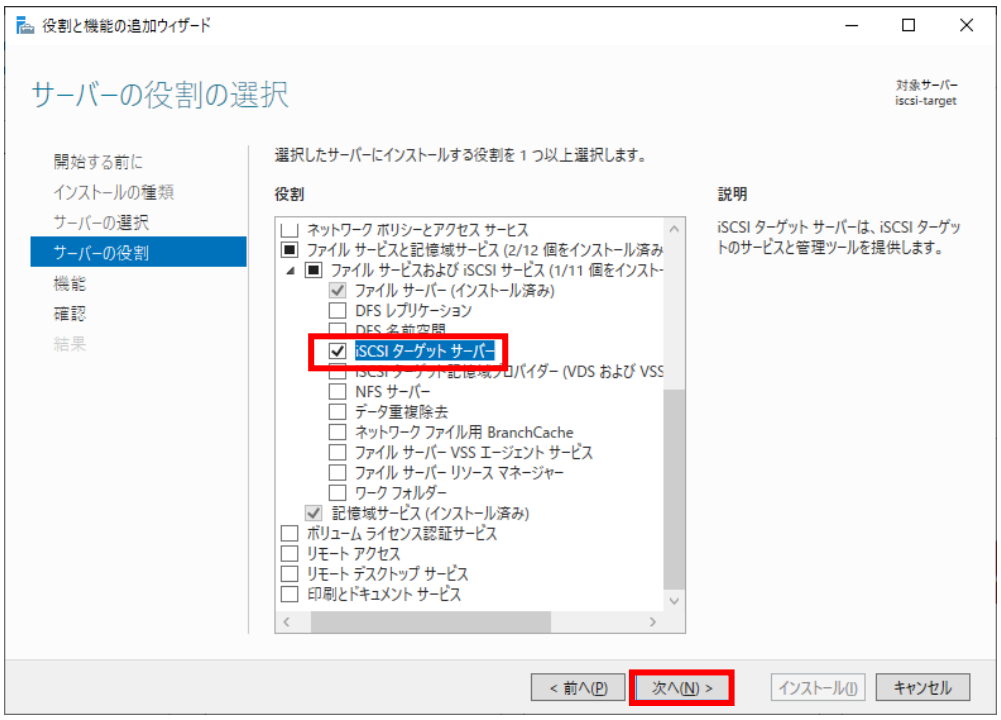
3. [役割ベースまたは機能ベースのインストール] を選択し、[次へ] ボタンをクリックします。



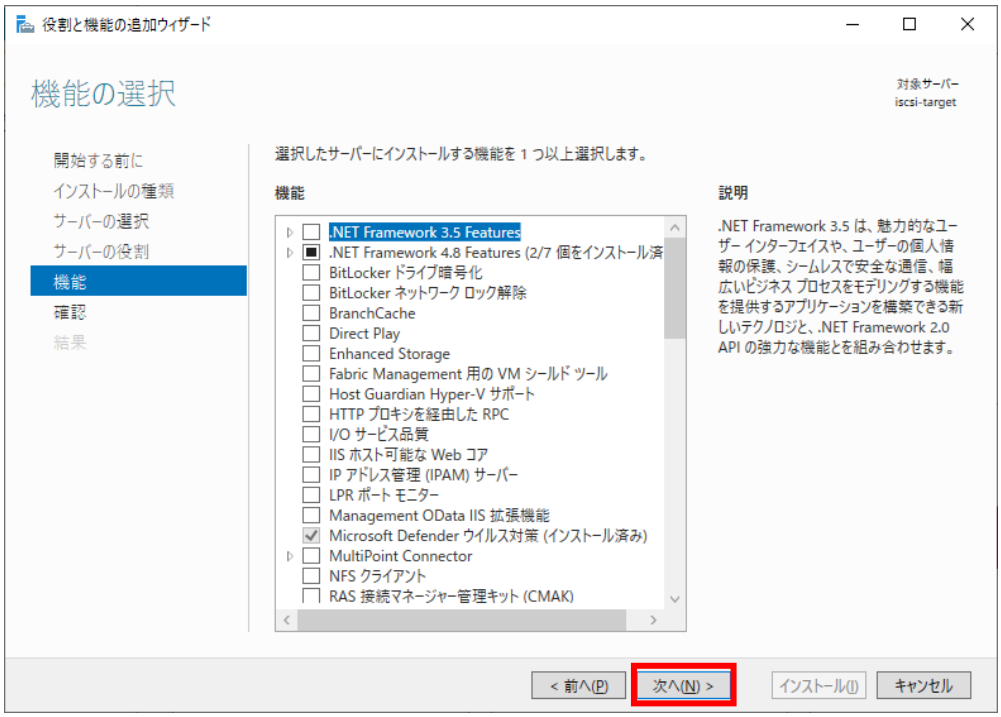
4. [サーバープールからサーバーを選択] を選択し、サーバープールから iSCSI ターゲットをインストールするサーバーをクリックして、[次へ] ボタンをクリックします。



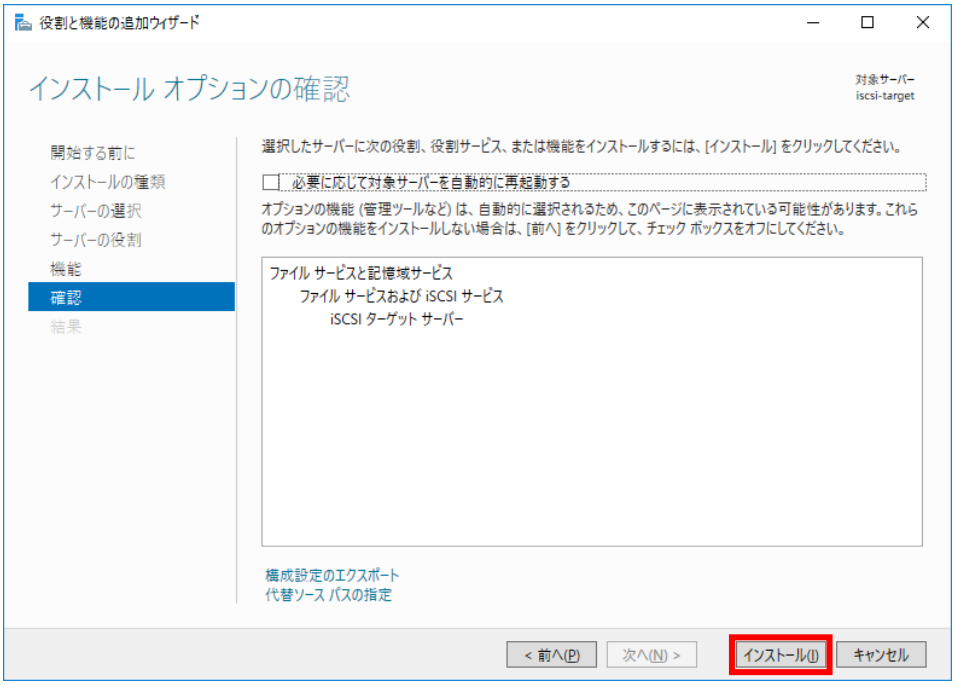
5. [役割] の [ファイルサービスと記憶域サービス] を展開し、さらに[ファイルサービスおよび iSCSI サービス] を展開して、[iSCSI ターゲットサーバー] をチェックして、[次へ] ボタンをクリックします。



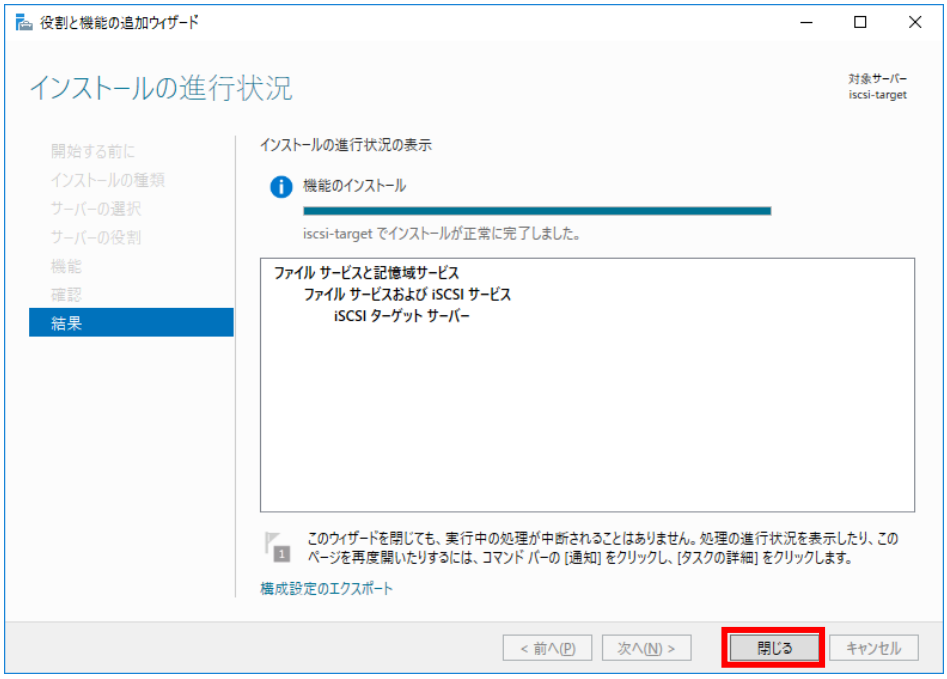
6. [次へ] ボタンをクリックします。



7. 設定内容を確認して、 [インストール] ボタンをクリックすると、インストールを開始します。

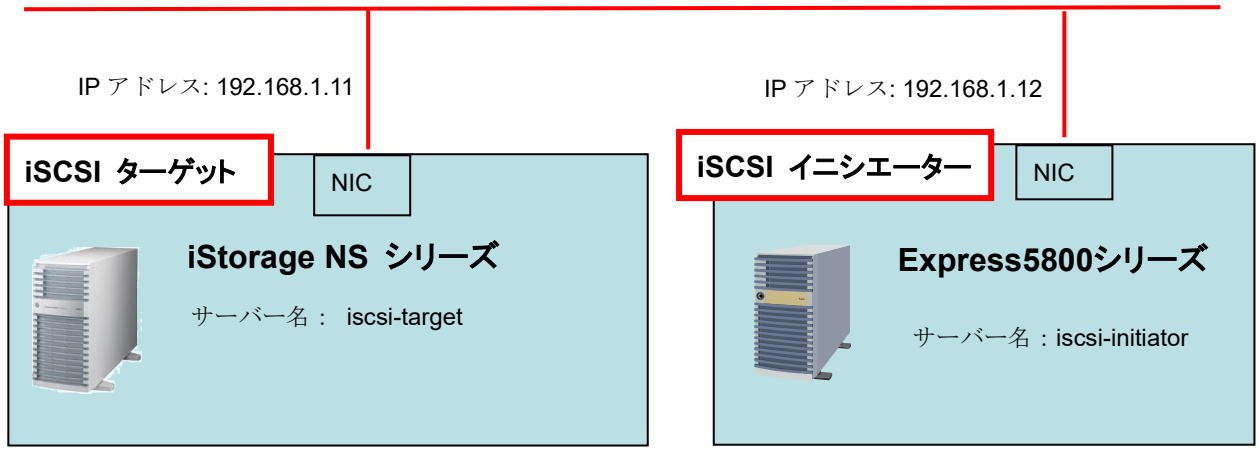


8. インストールが完了すると、以下の画面が表示されますので、[閉じる] ボタンをクリックします。なお、システムの再起動は不要です。



4.3.6 iSCSI 環境の構築

下記の環境を例に、iSCSI ターゲットおよび iSCSI イニシエーターの環境構築（設定）について説明します。



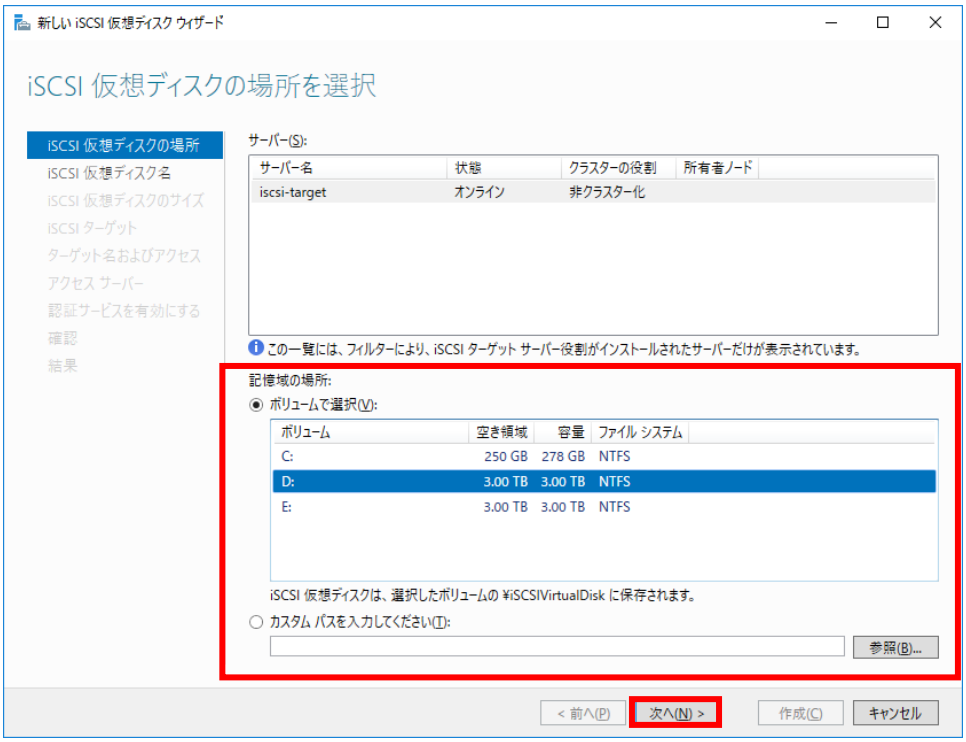
項目	設定
iSCSI 接続のパス	シングルパス
インターネット記憶域ネームサービス（iSNS）	使用しない
iSCSI ターゲットおよび iSCSI イニシエーターの識別子	IP アドレス
CHAP 認証	使用しない
iSCSI イニシエーターの起動時に iSCSI ターゲットに自動的に接続する	自動接続する
作成する iSCSI ターゲットの名前	Target01
作成する iSCSI 仮想ディスクの名前	VirtualDisk01

4.3.6.1 iSCSI 仮想ディスクの作成

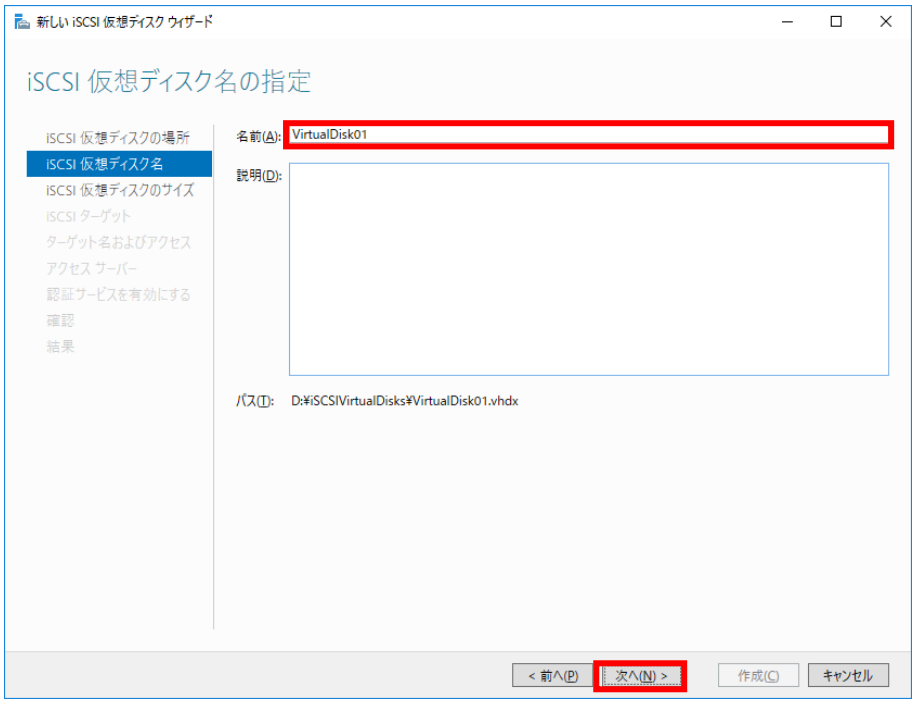
iSCSI ターゲットサーバー上にて、iSCSI 仮想ディスクを作成します。iSCSI 仮想ディスク作成のウィザードでは、iSCSI 仮想ディスクの作成、iSCSI ターゲットの作成、および iSCSI イニシエーターの割り当てを行います。

1. サーバーマネージャーの [ファイルサービスと記憶域サービス] - [iSCSI] をクリックして、iSCSI 仮想ディスクの [タスク] – [新しい iSCSI 仮想ディスク…] をクリックします。

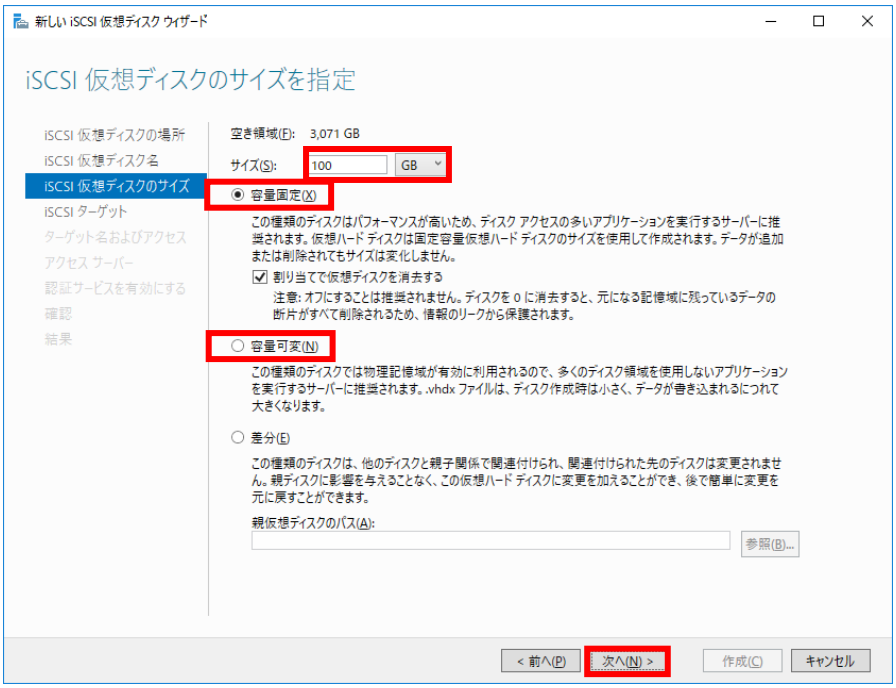
2. iSCSI 仮想ディスクを作成するボリュームを選択するか、カスタムパスを入力して、[次へ] をクリックします。



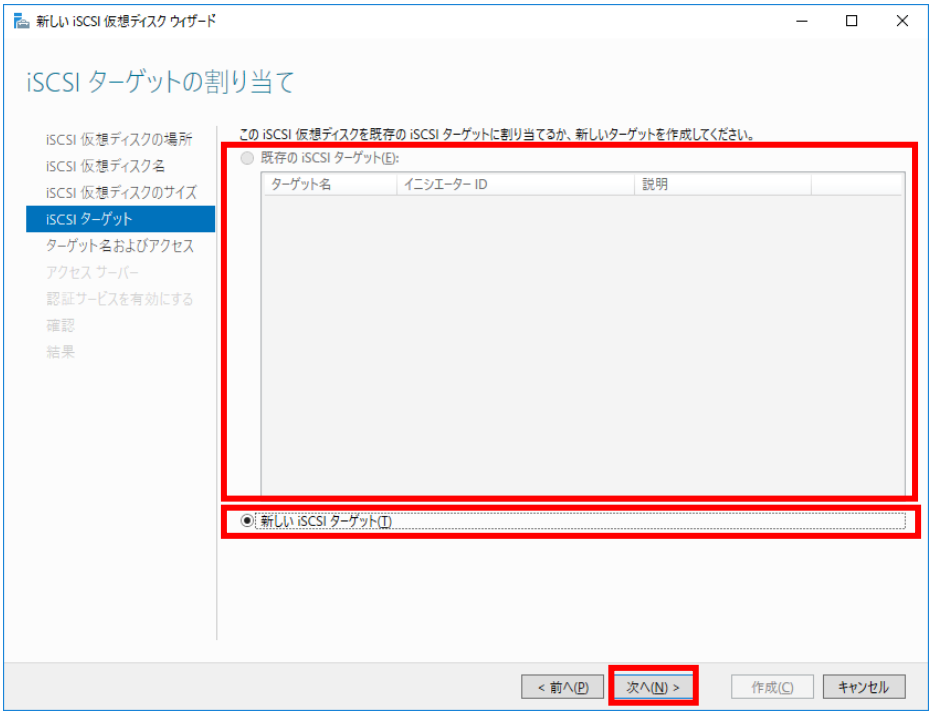
3. [名前] に 作成する iSCSI 仮想ディスクの名前を入力して、[次へ] ボタンをクリックします。



4. iSCSI 仮想ディスクの種類を選択します。[容量固定] または [容量可変] を選択した場合は [サイズ] に iSCSI 仮想ディスクの最大サイズ(8MB～64TB)を入力後、[次へ] ボタンをクリックします。



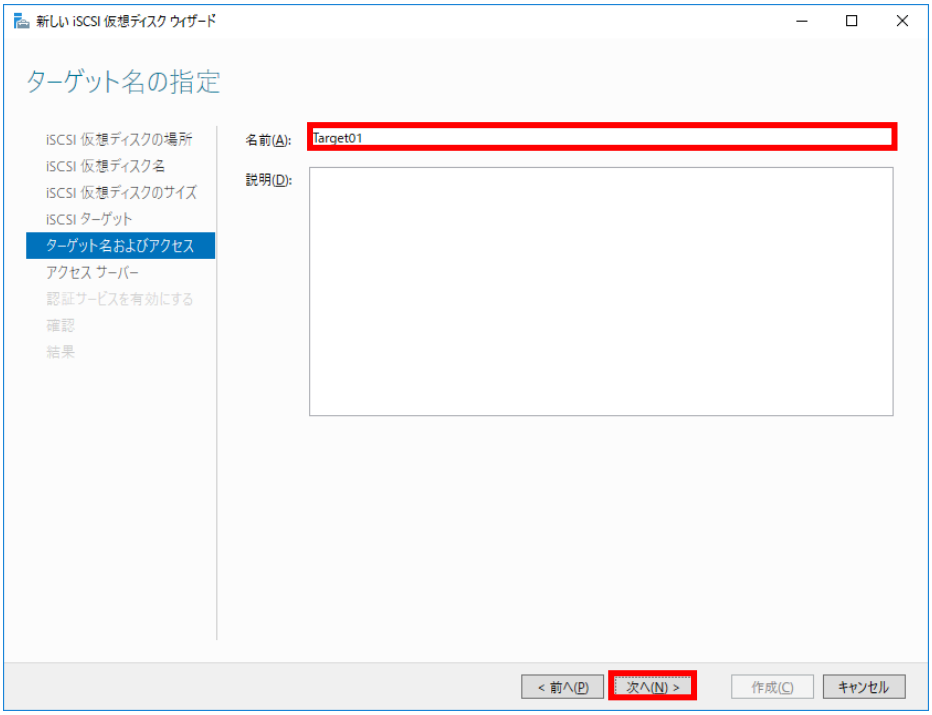
5. iSCSI 仮想ディスクを割り当てる iSCSI ターゲットを選択して、[次へ] ボタンをクリックします。



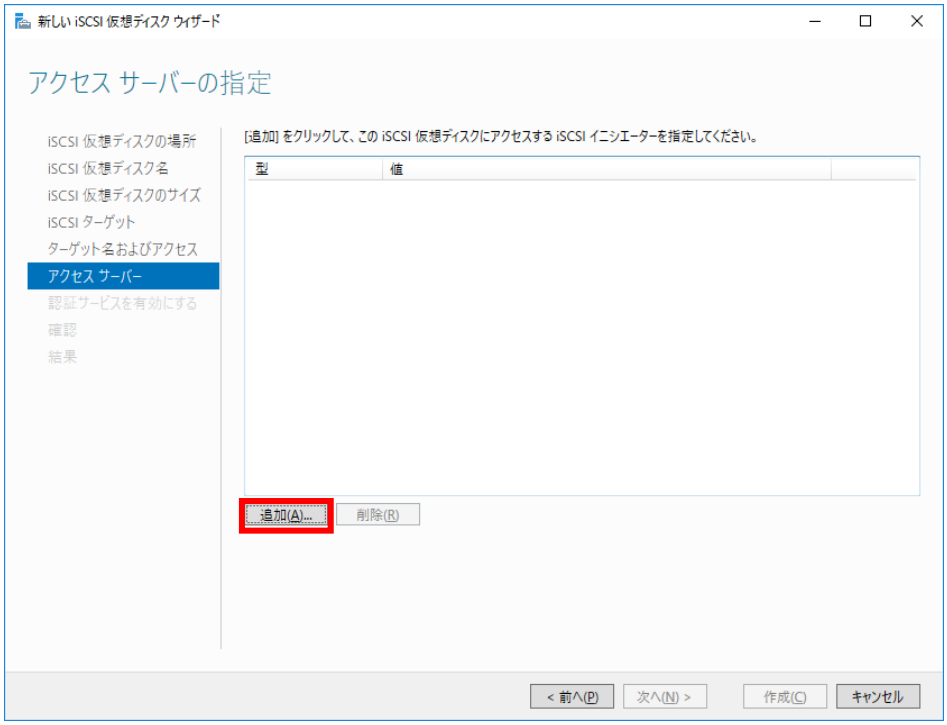
【補足】

iSCSI 仮想ディスクを初めて作成する場合は、[新しい iSCSI ターゲット] のみ選択可能です。2 回目以降の iSCSI 仮想ディスクの作成では、既存の iSCSI ターゲットに割り当てることもできます。この場合は、項番 11. に進みます。

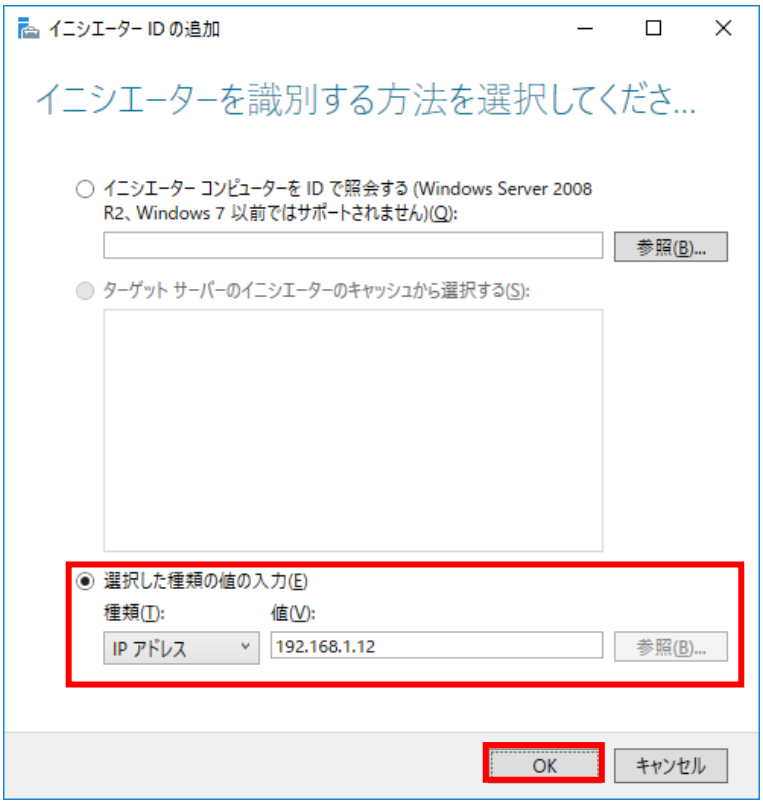
6. [名前] に作成する iSCSI ターゲットの名前を入力して、[次へ] ボタンをクリックします。



7. [アクセスサーバーの指定] 画面で、[追加] ボタンをクリックして、iSCSI ターゲットに割り当てる iSCSI イニシエーターを指定します。



8. [イニシエーターID の追加] 画面にて、[選択した種類の値の入力] を選択して、[種類] で IP アドレスを選択し、[値] に iSCSI イニシエーターの IP アドレス “192.168.1.12” を入力して、[OK] ボタンをクリックします。



IP アドレスの他に、イニシエーターを識別する識別子として、以下も使用できます。

- **IQN 名**

  iSCSI イニシエーターの IQN 名。本書の【iSCSI イニシエーターの設定】の項番 2 で確認することができます。

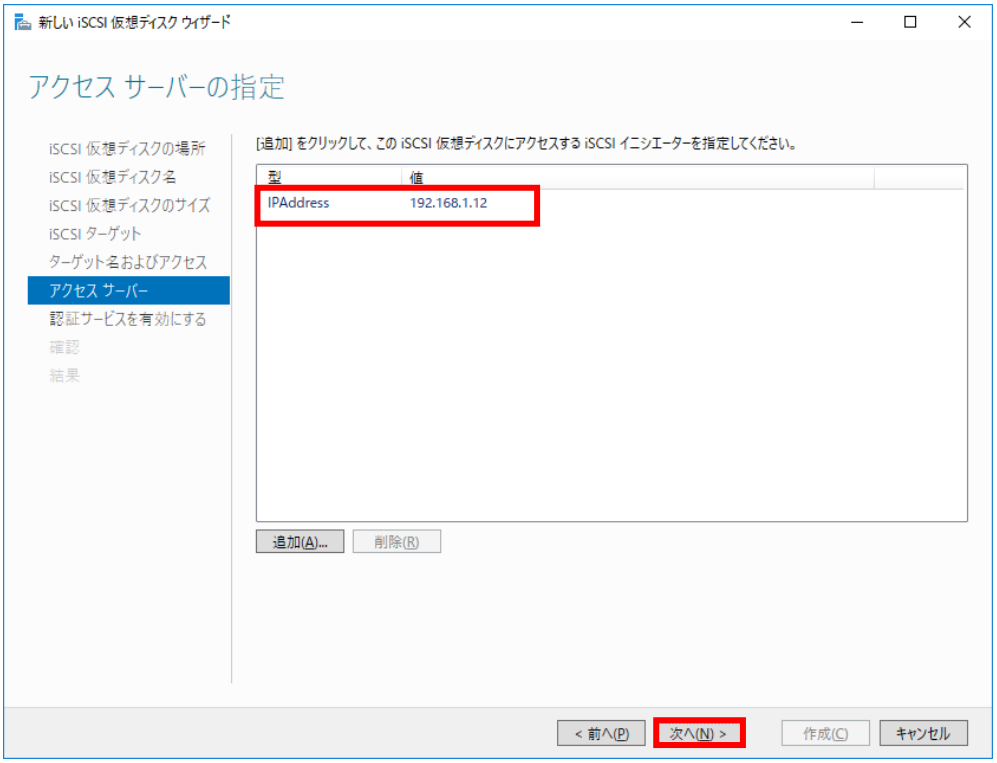
- **DNS ドメイン名**

  iSCSI イニシエーターの完全修飾ドメイン名（FQDN）

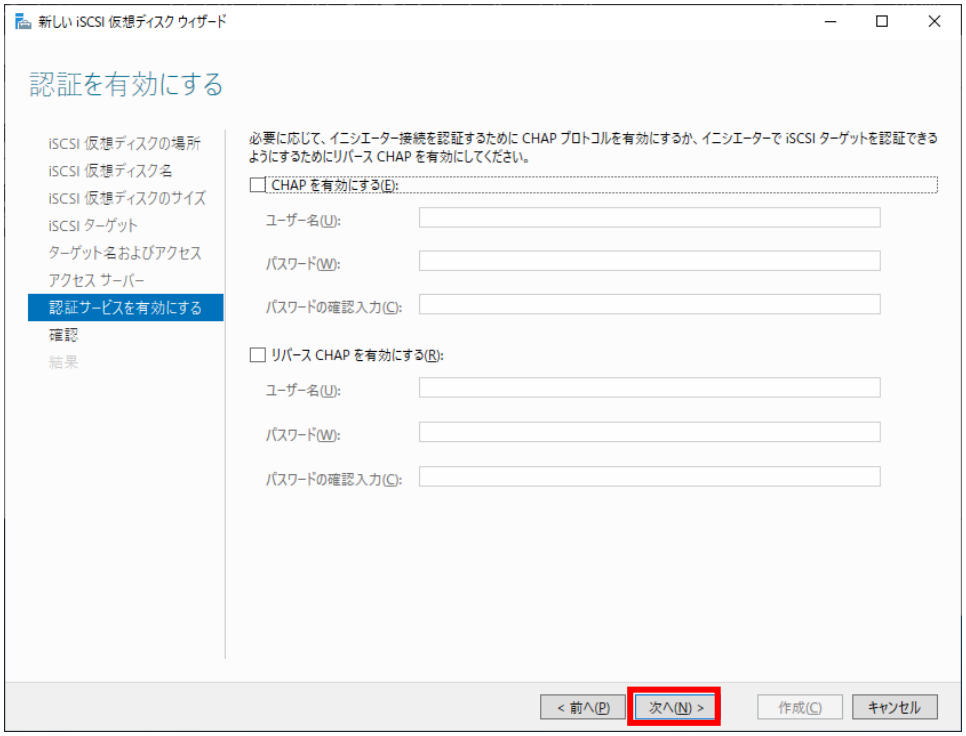
- **MAC アドレス**

  iSCSI イニシエーターの MAC アドレス

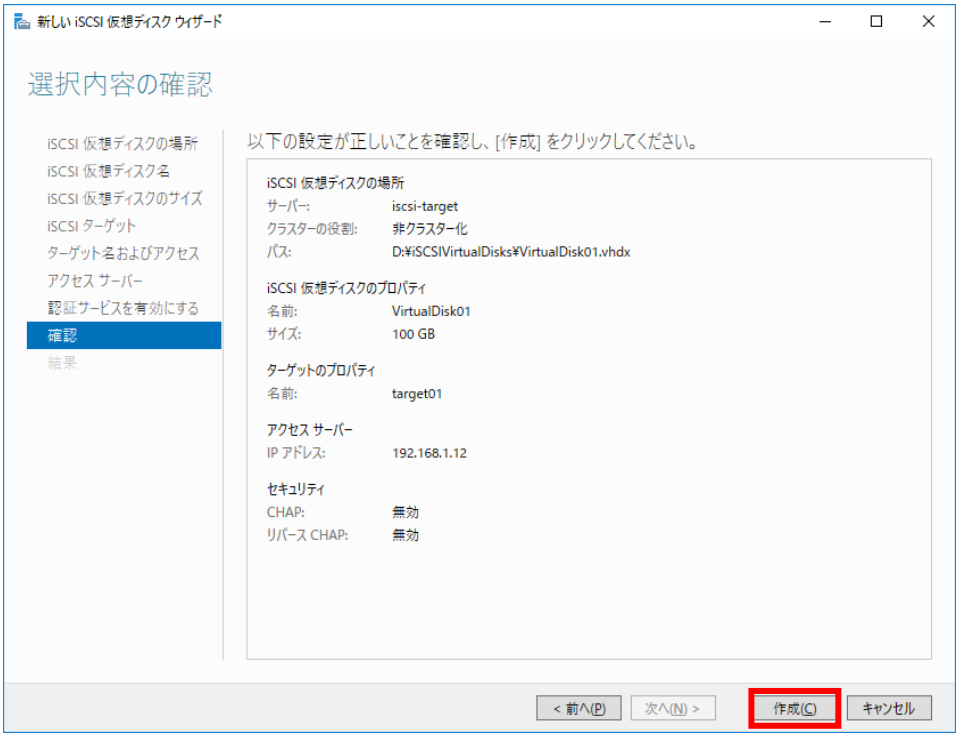
9. [アクセスサーバーの指定] に戻ります。iSCSI イニシエーターが一覧に追加されたことを確認して、[次へ] ボタンをクリックします。



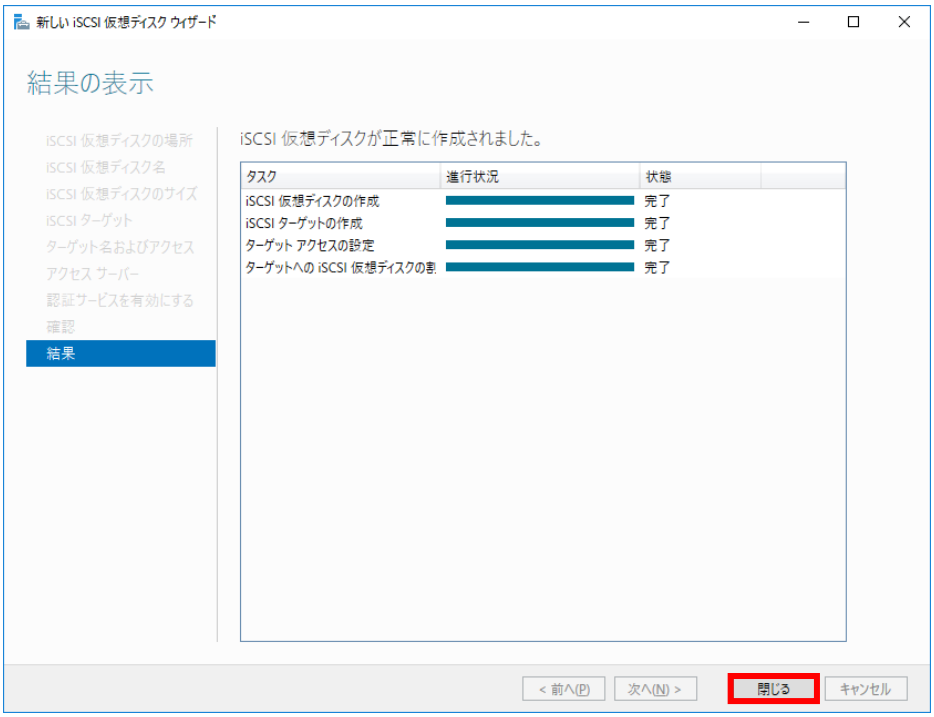
10. [認証を有効にする] 画面にて、必要に応じて認証設定をチェックし、 [次へ] ボタンをクリックします。



11. 設定内容が正しいことを確認して、[作成] ボタンをクリックします。



12. [結果の表示] 画面で、[閉じる] ボタンをクリックします。



以上で iSCSI ターゲットの設定は完了です。 iSCSI イニシエーターをiSCSI 仮想ディスクに割り当てる設定は、iSCSI イニシエーター側 (iSCSI イニシエーターの設定) にて行います。

4.3.6.2 iSCSI イニシエーターの設定

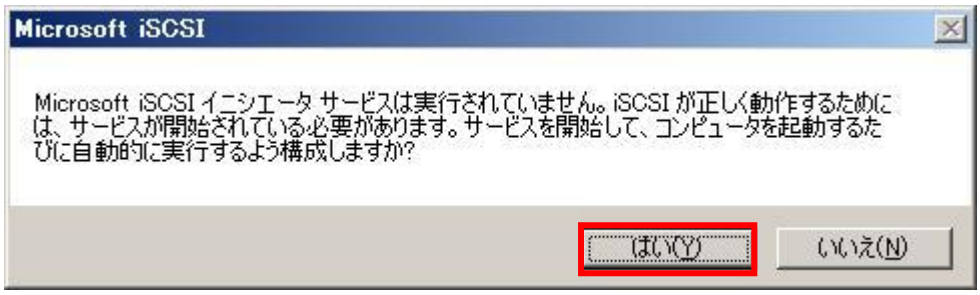
ここでは、Windows Server OS に標準でインストールされている iSCSI イニシエーターでの設定について説明します。なお、下記手順の画面イメージは例であり、実際とは異なっている場合があります。

【注意】

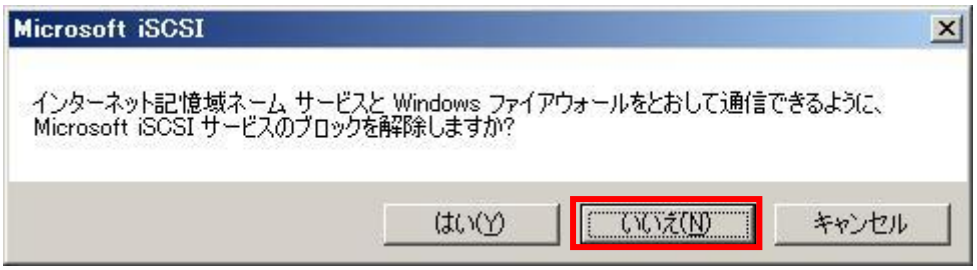
- 1 つの iSCSI 仮想ディスクに複数の iSCSI イニシエーターから同時にアクセスすると、iSCSI 仮想ディスク内のデータが破壊される恐れがあります。クラスターシステムのように iSCSI イニシエーター側で iSCSI 仮想ディスクの排他制御が行える環境を除いて、1 つの iSCSI 仮想ディスクには 1 台の iSCSI イニシエーターからのみアクセスできるよう設定してください。

1. iSCSI イニシエーターを設定するコンピューターにおいて、[スタート] - [管理ツール] - [iSCSI イニシエーター] をクリックします。

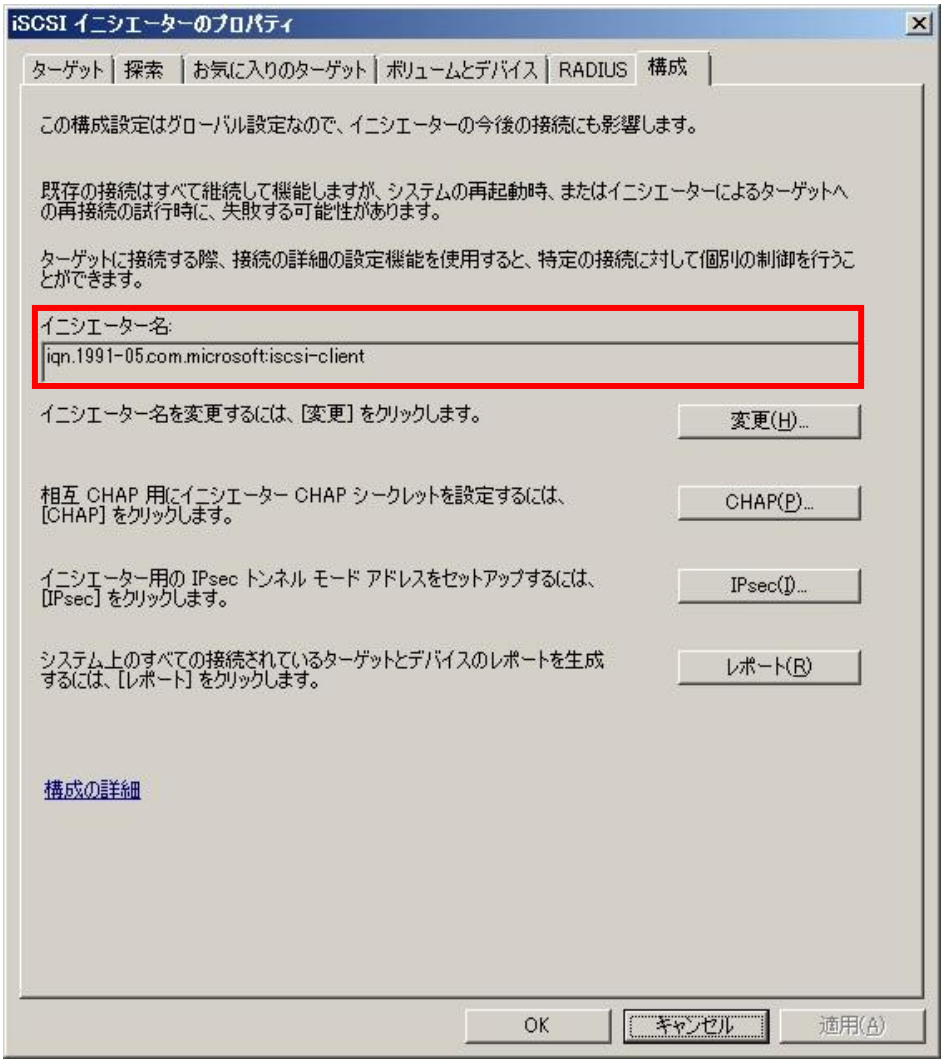
iSCSI イニシエーターのサービスが起動していない場合は、iSCSI イニシエーターのサービスを起動するメッセージが表示されますので [はい] ボタンをクリックしてください。



インターネット記憶域ネームサービス（iSNS）のメッセージが表示されたら、[はい]、または [いいえ] を選択します。

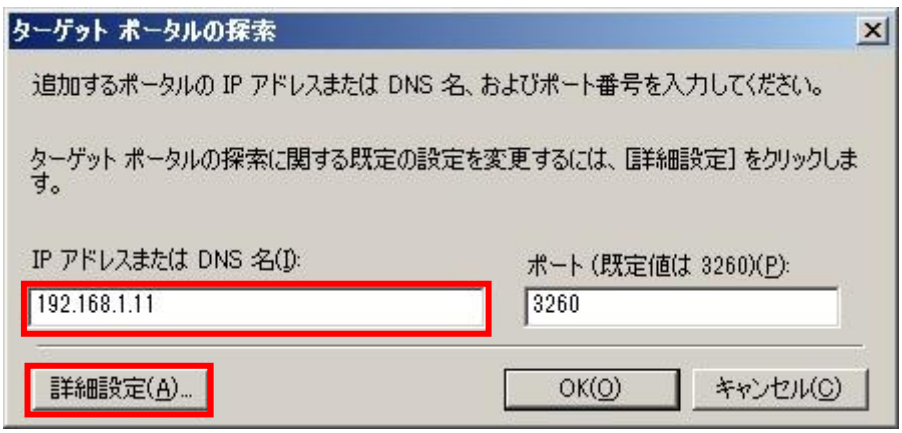


2. [構成] タブにイニシエーター名が表示されていることを確認します。表示されている値が iSCSI イニシエーター のイニシエーター名(IQN)です。

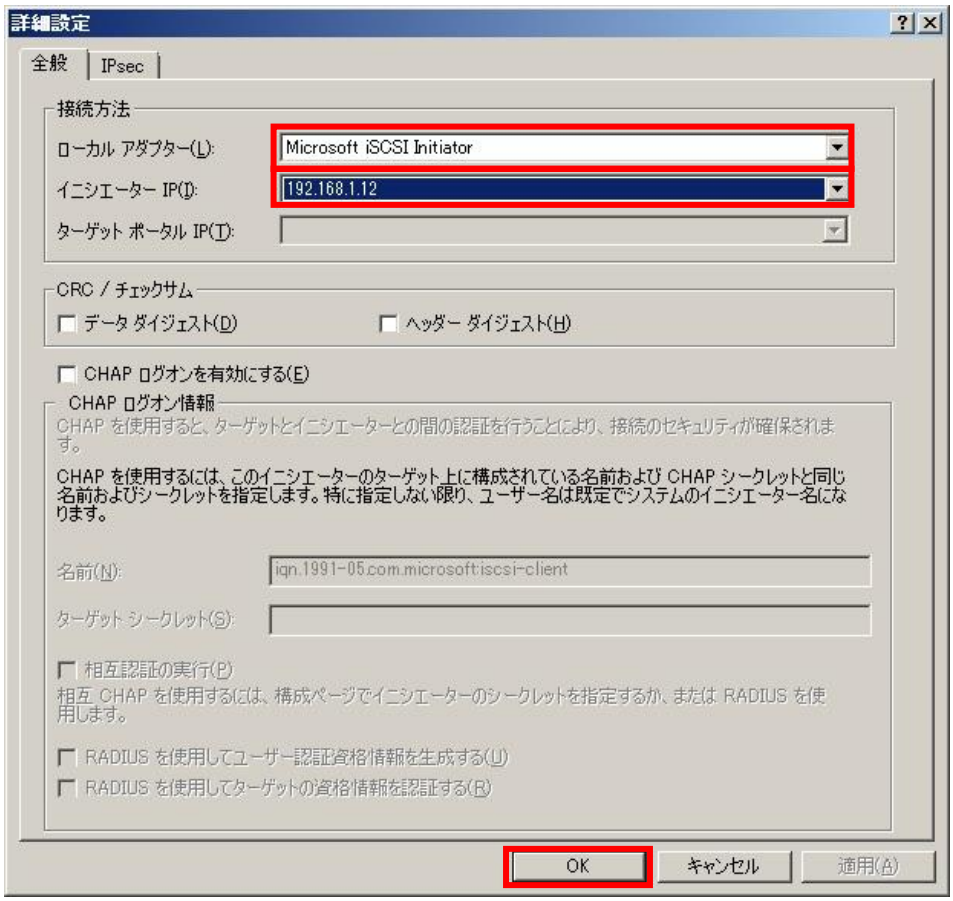


3. [探索] タブで [ポータルの探索] ボタンをクリックします。

4. [IP アドレスまたは DNS 名] に iSCSI ターゲットの IP アドレスまたは DNS 名を入力して、[詳細設定] ボタンをクリックします。

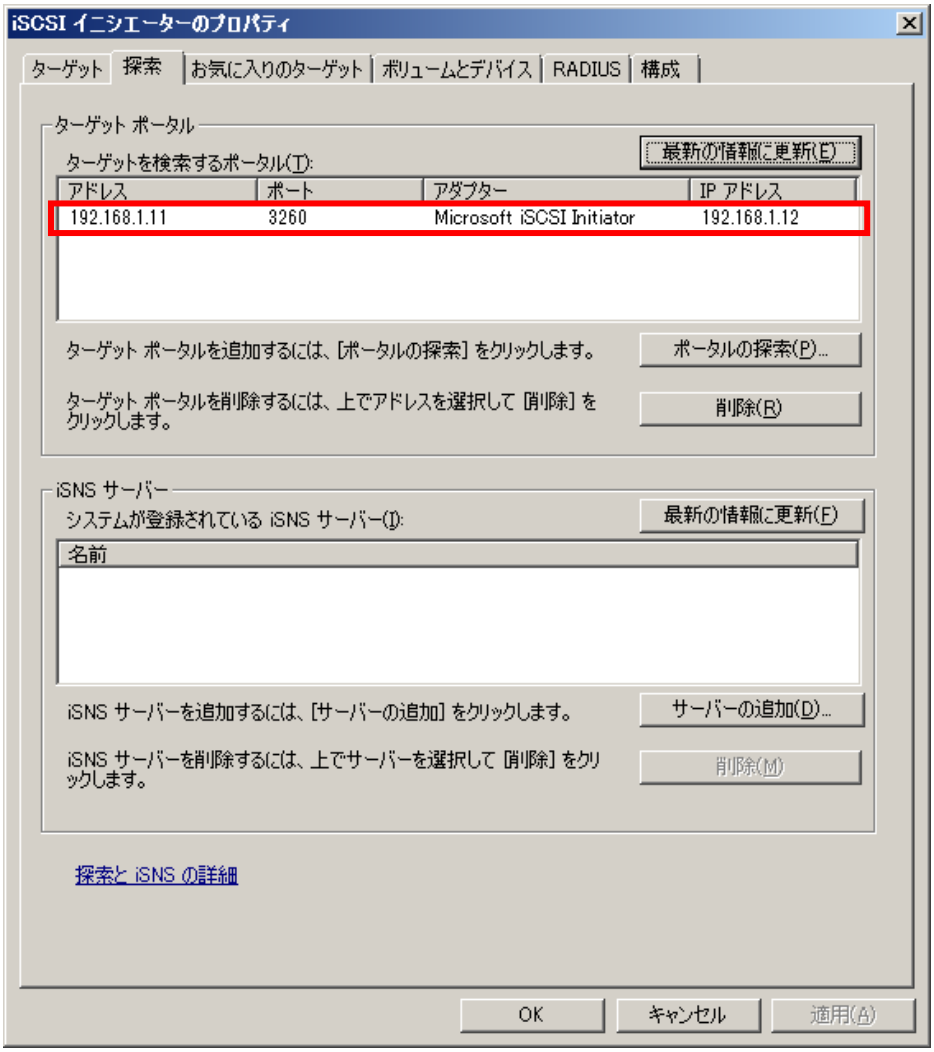


5. [詳細設定] 画面の[全般] タブにて、 [接続方法] 欄の [ローカルアダプター] で [Microsoft iSCSI Initiator] を選択し、[イニシエーター IP] で iSCSI ターゲットと通信するための自身の IP アドレスを選択後、[OK] ボタンをクリックします。

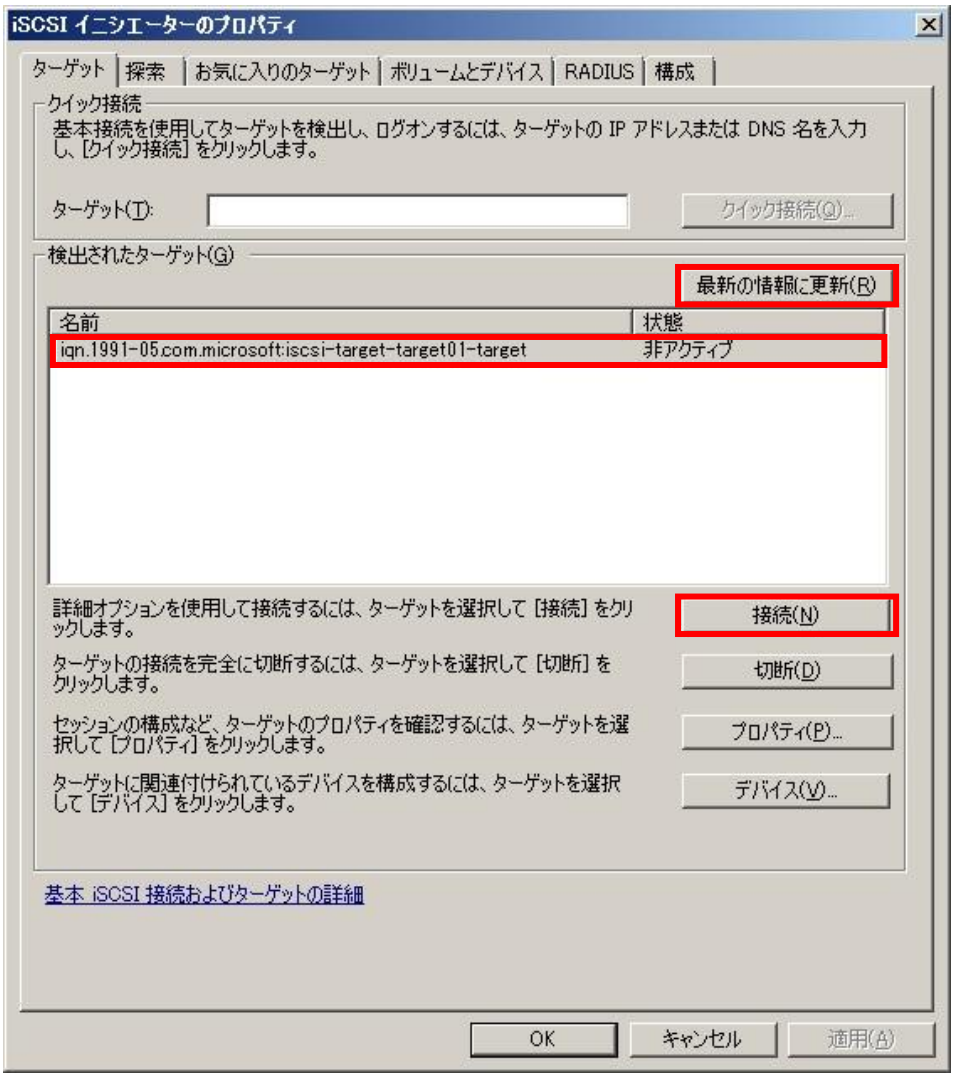


6. [ターゲットポータルの探索] に戻りますので、[OK] ボタンをクリックします。

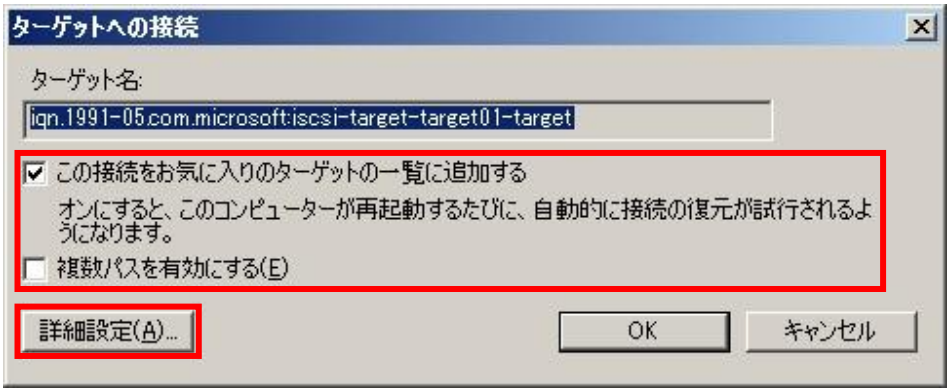
7. [iSCSI イニシエーターのプロパティ] の [探索] タブにて、[ターゲットを検索するポータル] に iSCSI ターゲットの IP アドレスが追加されたことを確認します。



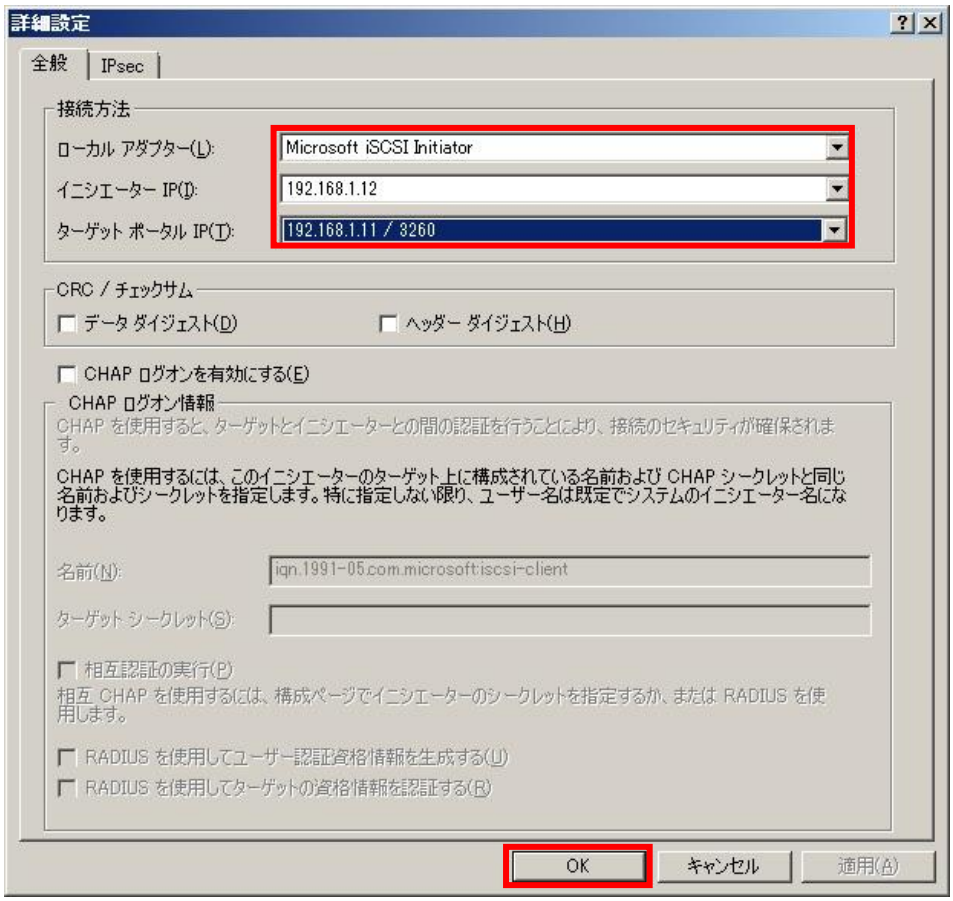
8. [ターゲット] タブをクリックします。iSCSI ターゲットの IQN が表示され、状態が [非アクティブ] になっています。表示されていない場合は、[最新の情報に更新] ボタンをクリックします。目的の iSCSI ターゲットの IQN を選択し、[接続] ボタンをクリックします。



9. [ターゲットへの接続] 画面で、 [この接続をお気に入りのターゲット一覧に追加する] をチェックして、[詳細設定] ボタンをクリックします。なお、[複数パスを有効にする] をチェックすると、iSCSI ターゲットへのアクセス経路を複数確保することができます。ただし、事前に iSCSI 用に複数の NIC と、マルチパス I/O 機能を追加しておく必要があります。本書では、イニシエーター側の装置上でのマルチパス I/O 機能の追加手順は省略します。

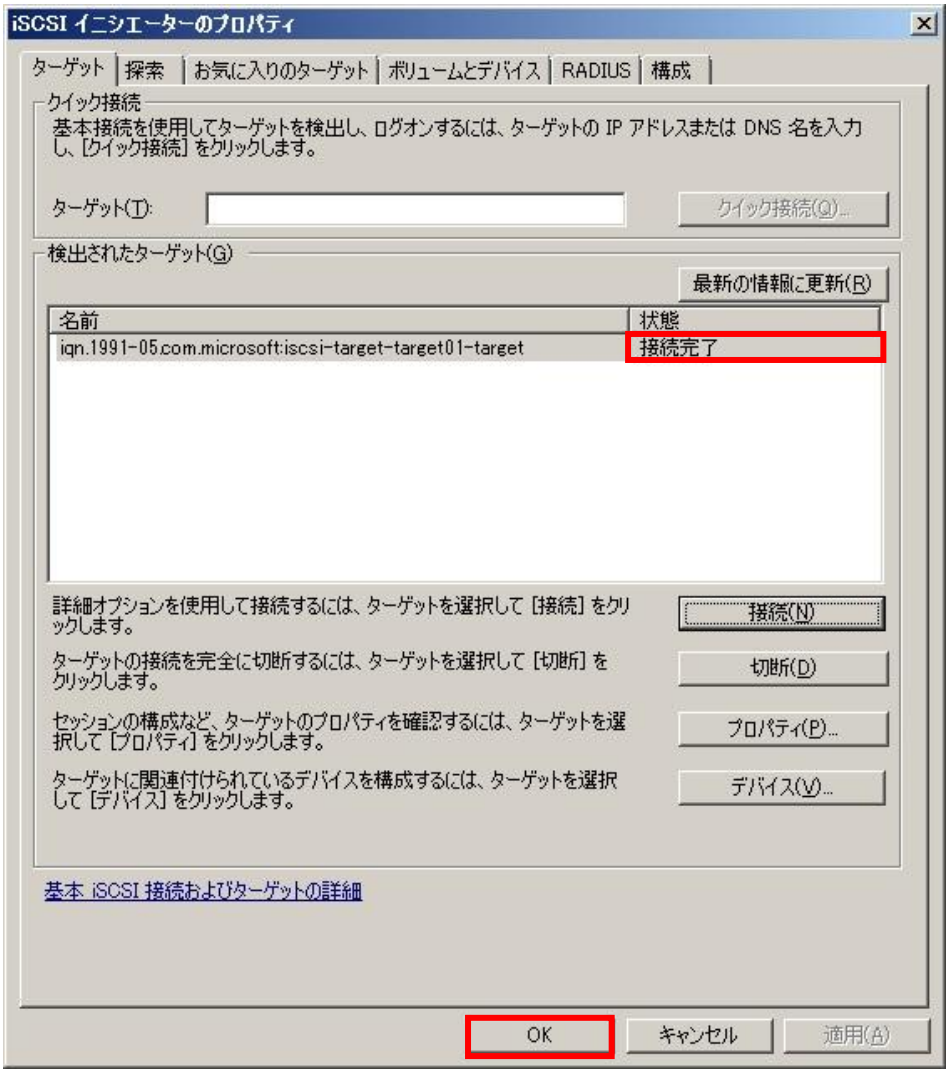


10. [詳細設定] 画面の [全般] タブの [接続方法] 欄にて、[ローカルアダプター] を [Microsoft iSCSI Initiator]、[イニシエーター IP] を iSCSI 接続に使用する自身の IP アドレス、[ターゲットポータル IP] に iSCSI ターゲットの IP アドレスを選択し、[OK] ボタンをクリックします。



11. [ターゲットへのログオン] 画面に戻りますので、[OK] をクリックします。

12. 対象の iSCSI ターゲットの状態が [接続完了] と表示されたことを確認し、[OK] ボタンをクリックして画面を閉じます。



これにより、iSCSI ターゲットへの接続は完了しました。iSCSI イニシエーター側にディスクが追加されていますので、【管理者ガイド（概要編）ボリュームを作成する】を参照し、iSCSI イニシエーター側にてボリュームの作成やフォーマットを行ってください。

4.3.7 iSCSI ターゲットの運用

iSCSI ターゲットの運用時に必要となる各種手順について説明します。

【注意】
- iSCSI ターゲットの設定を変更する場合、iSCSI イニシエーターからのすべてのアクセスを切断してください。iSCSI イニシエーターからの切断方法については、【iSCSI ターゲットとの切断】を参照してください。
- iSCSI ターゲットや iSCSI 仮想ディスクの設定変更を行った場合は、iSCSI イニシエーター側にて設定の見直しを行ってください。

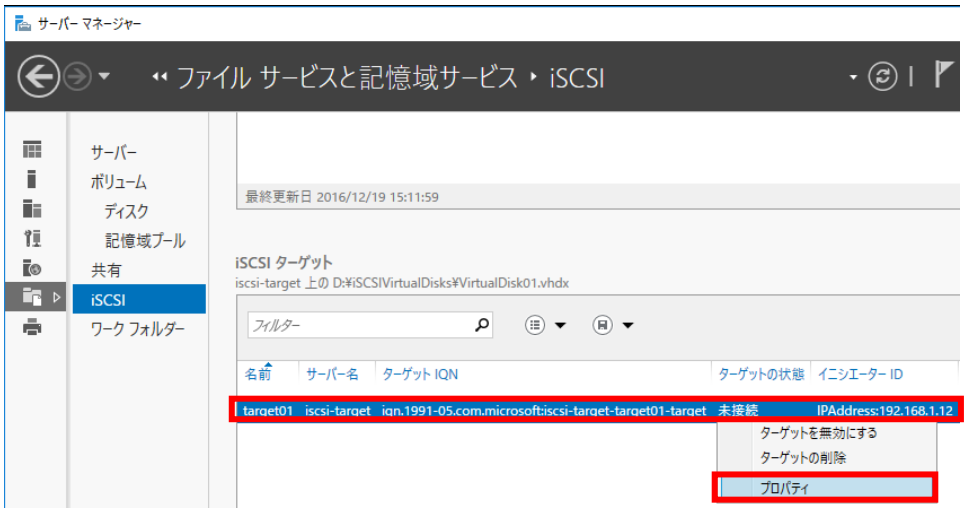
4.3.7.1 iSCSI ターゲットの IQN の変更

ここでは iSCSI ターゲットの IQN を変更する方法を説明します。

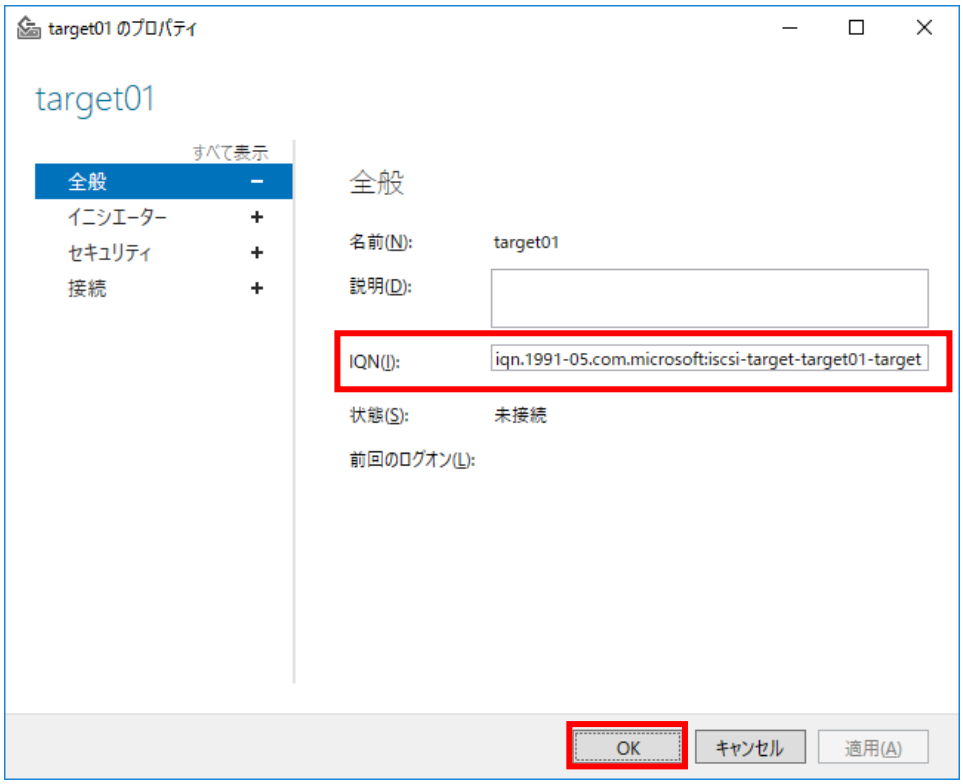
【注意】
- iSCSI ターゲット IQN はお客様環境で他と重複しないようにしてください。
- iSCSI ターゲット IQN の変更後は、iSCSI イニシエーターで接続設定を変更する必要があります。接続設定については、【iSCSI ターゲットへの接続】を参照してください。

1. サーバーマネージャーの [ファイルサービスと記憶域サービス] - [iSCSI] をクリックします。

2. 変更する iSCSI ターゲットを右クリックして [プロパティ] をクリックします。



3. iSCSI ターゲットの IQN を変更して、[OK] ボタンをクリックします。

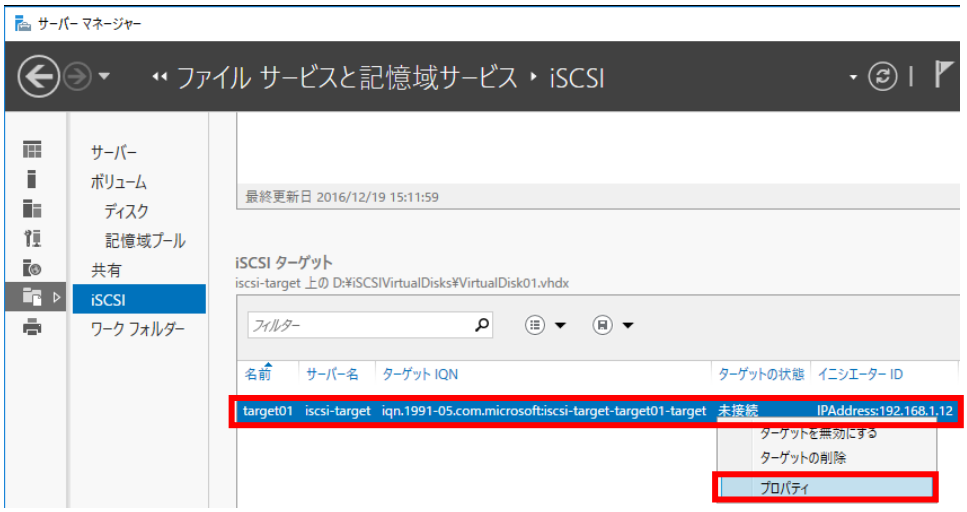


4.3.7.2 iSCSI ターゲットへアクセスする iSCSI イニシエーターの変更

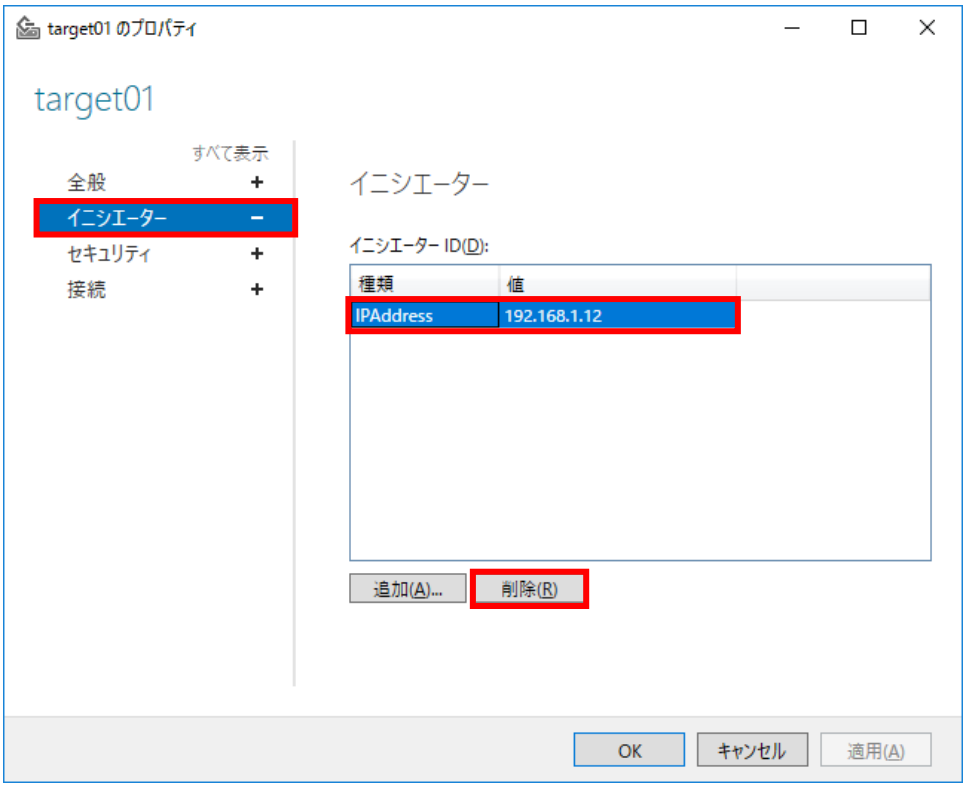
ここでは、iSCSI ターゲットへアクセスする iSCSI イニシエーターの変更方法を説明します。なお、現在設定されているイニシエーター情報を直接編集することはできませんので、現在の設定を一旦削除し、新しい設定を追加することで変更します。

1. サーバーマネージャーの [ファイルサービスと記憶域サービス] - [iSCSI] をクリックします。

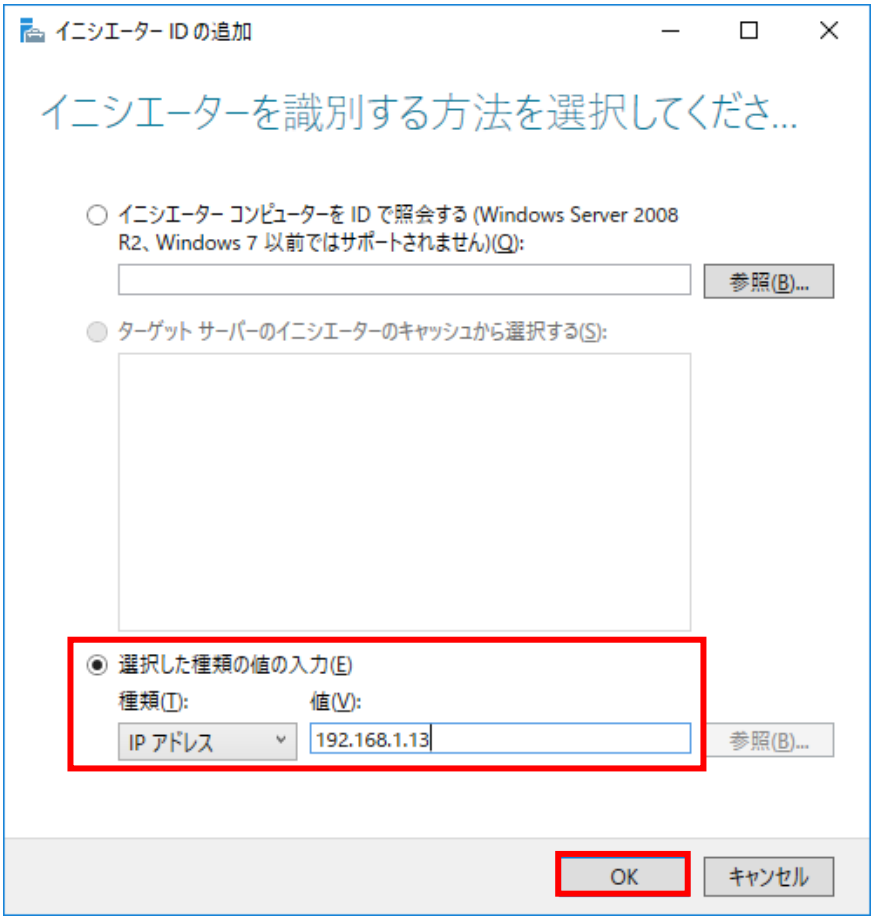
2. 変更する iSCSI ターゲットを右クリックして [プロパティ] をクリックします。



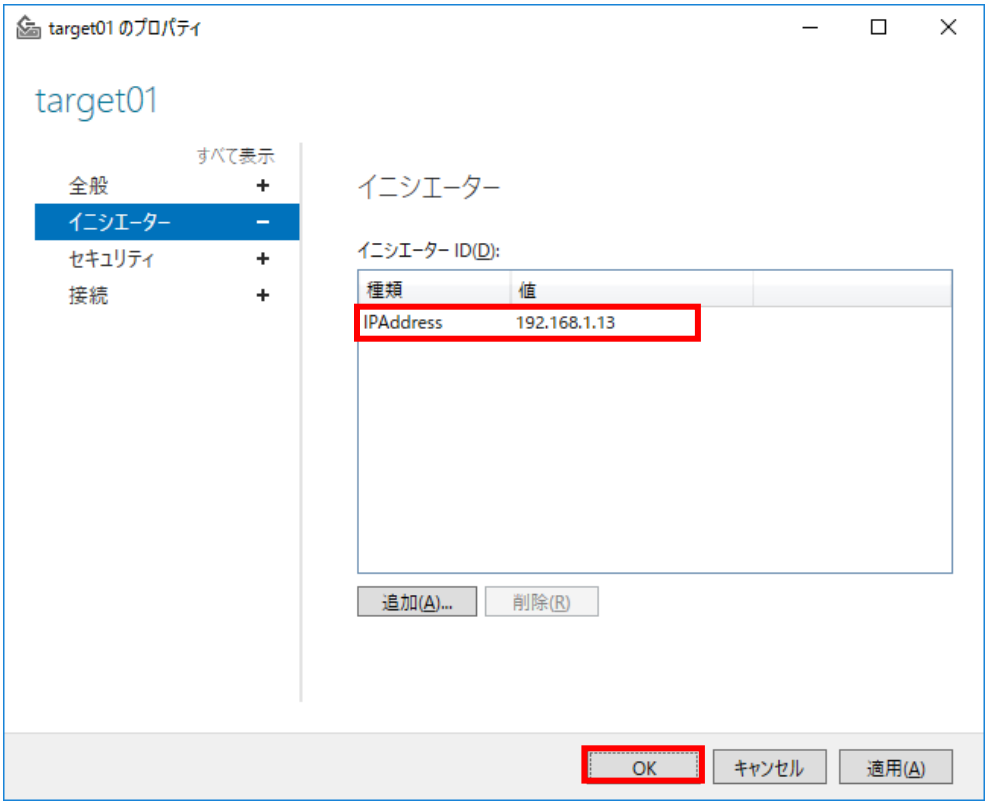
3. ツリーの [イニシエーター] をクリックし、変更する iSCSI イニシエーターをクリックして、[削除] ボタンをクリックします。



4. [追加] ボタンをクリックして、[イニシエーター ID の追加]で、変更先の iSCSI イニシエーターの識別子の種類を選択して適切な値を指定します。ここでは [選択した種類の値の入力] を選択して、[種類] で [IP アドレス] を選択し、[値] の欄に変更先の iSCSI イニシエーターの IP アドレスを入力して [OK] ボタンをクリックします。



5. 変更後の iSCSI イニシエーターの IP アドレスが表示されていることを確認して [OK] ボタンをクリックします。

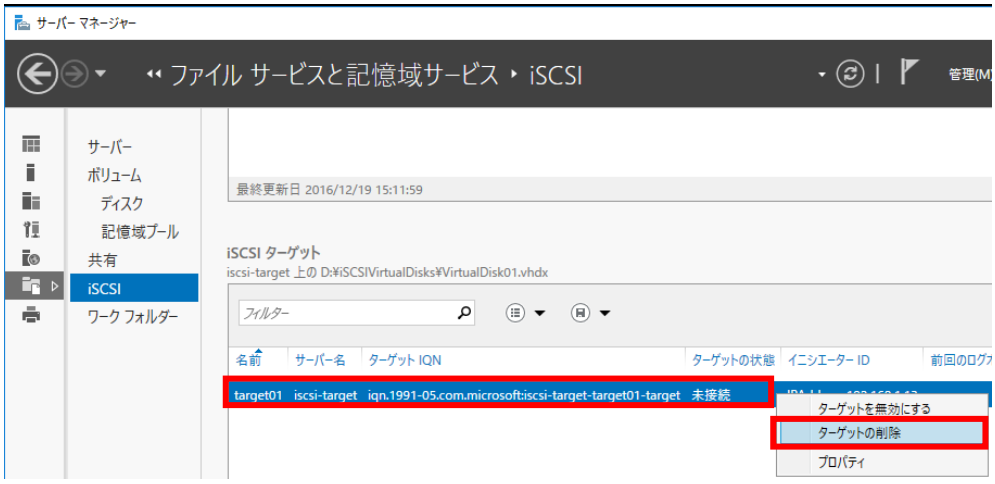


4.3.7.3 iSCSI ターゲットの削除

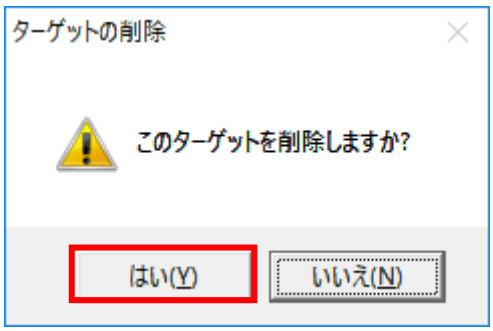
ここでは iSCSI ターゲットの削除方法を説明します。なお、iSCSI ターゲットを削除しても iSCSI 仮想ディスクは削除されません。iSCSI 仮想ディスクを削除する場合は【iSCSI 仮想ディスクの削除】を参照してください。

1. サーバーマネージャーの [ファイルサービスと記憶域サービス] - [iSCSI] をクリックします。

2. 削除する iSCSI ターゲットを右クリックして [ターゲットの削除] をクリックします。



3. 削除の確認のメッセージが表示されたら、[はい] ボタンをクリックします。



4.3.7.4 iSCSI 仮想ディスクの拡張

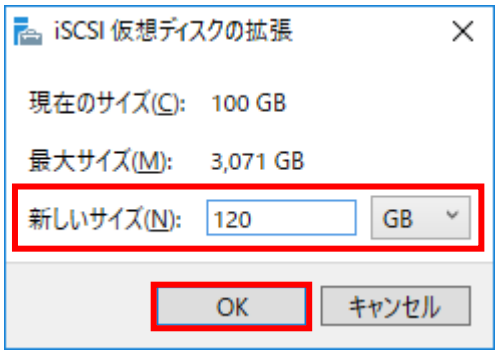
iSCSI 仮想ディスクのサイズは、動的に増やすことができます。これにより格納済みのデータが失われることはなく、iSCSI ターゲットを再起動する必要もありません。ただし、拡張した領域を iSCSI イニシエーターで使用するには、iSCSI イニシエーターでの設定変更が必要です。詳細は【iSCSI イニシエーター側の仮想ディスクの拡張】を参照してください。なお、物理ディスクの容量を超えた設定や、諸元に記載している最大サイズを設定している場合は、拡張することができません。

ここでは、iSCSI 仮想ディスクを拡張する手順について説明します。

1. サーバーマネージャーの [ファイルサービスと記憶域サービス] - [iSCSI] をクリックします。

2. 拡張する iSCSI 仮想ディスクを右クリックして [iSCSI 仮想ディスクの拡張] をクリックします。

3. [新しいサイズ] に値を入力して [OK] ボタンをクリックします。このとき、[最大サイズ] は物理ディスクの空き容量 (指定可能な最大サイズ) を示しています。



4.3.7.5 iSCSI 仮想ディスクの割り当て変更

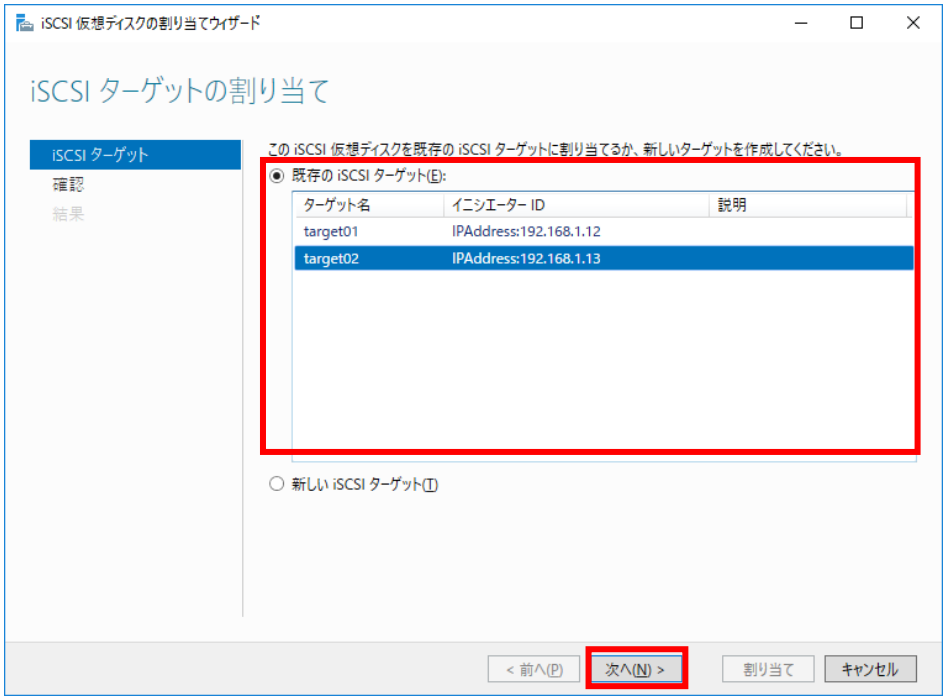
ある iSCSI ターゲットに割り当てられている iSCSI 仮想ディスクを、他の iSCSI ターゲットに割り当てます。既存の iSCSI ターゲットだけでなく、新規に作成する iSCSI ターゲットへの割り当ても可能です。

ここでは、iSCSI ターゲット(target01)に割り当てられている iSCSI 仮想ディスク(VirtualDisk01.vhdx)を iSCSI ターゲット(target02)に割り当てる手順について説明します。

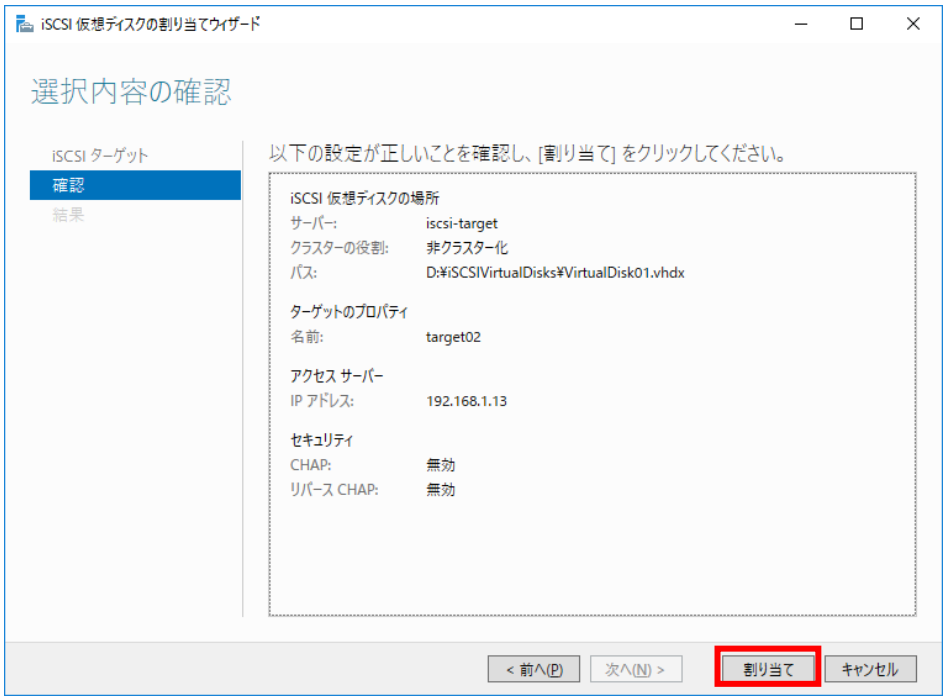
1. サーバーマネージャーの [ファイルサービスと記憶域サービス] - [iSCSI] をクリックします。

2. iSCSI 仮想ディスクの一覧から、iSCSI ターゲットを変更する iSCSI 仮想ディスクを右クリックして [iSCSI 仮想ディスクの割り当て] をクリックします。

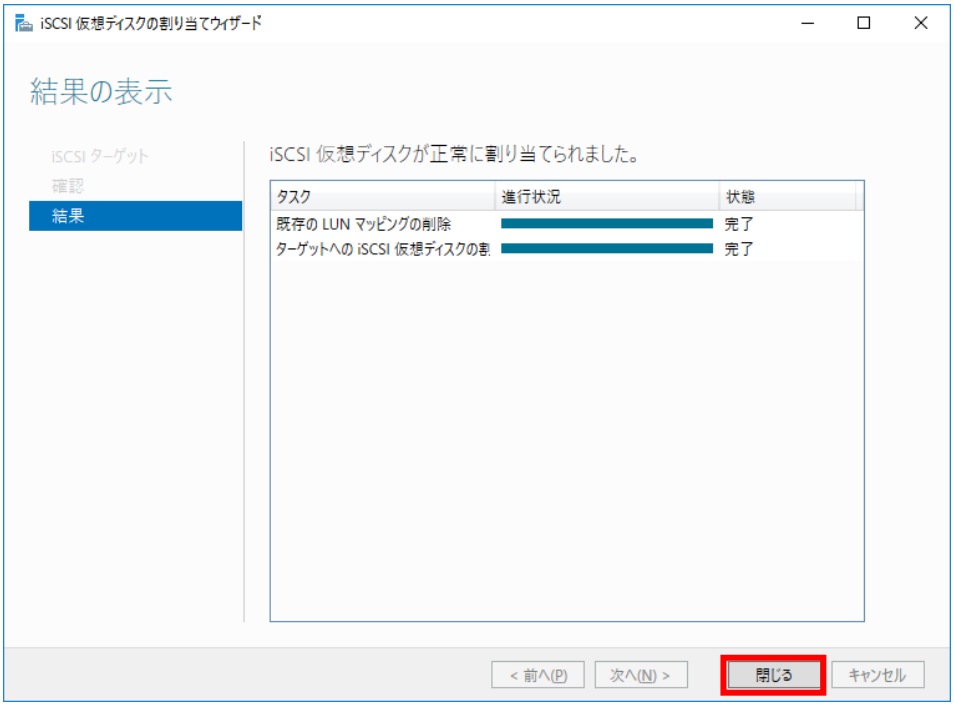
3. [iSCSI ターゲットの割り当て] 画面 で、[既存の iSCSI ターゲット] の一覧から、割り当てる iSCSI ターゲットを選択し、 [次へ] ボタンをクリックします。



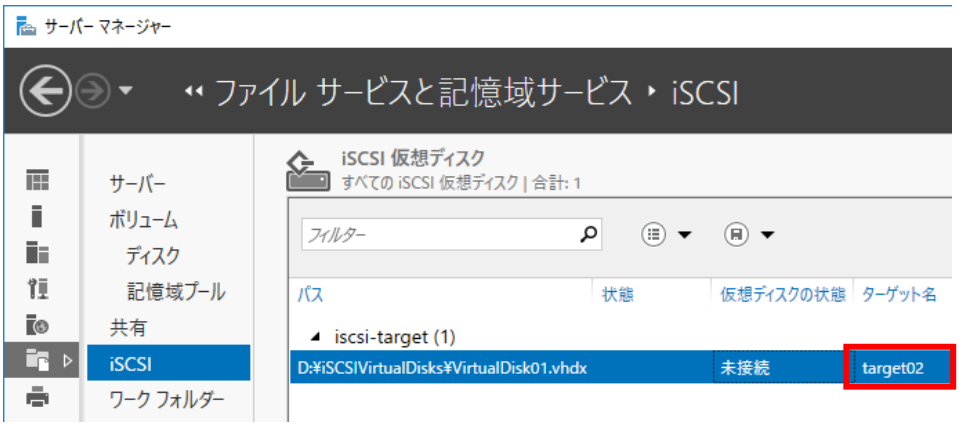
4. [選択内容の確認] 画面で、変更後の内容が表示されますので、確認して [割り当て] ボタンをクリックします。



5. [結果の表示] で、 [閉じる] ボタンをクリックします。



6. iSCSI 仮想ディスクの一覧で、変更した iSCSI 仮想ディスクの [ターゲット名] が、項番 3 で選択した iSCSI ターゲットになっていることを確認します。



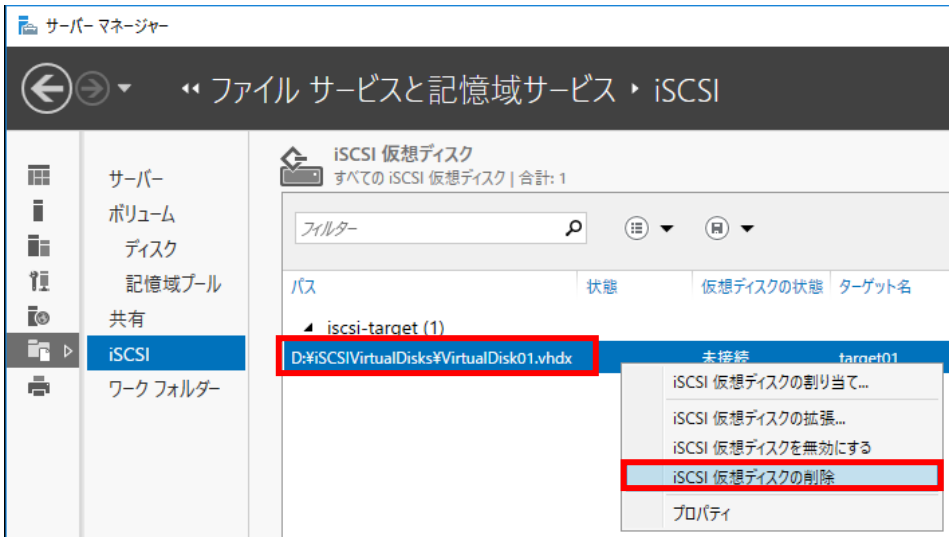
4.3.7.6 iSCSI 仮想ディスクの削除

iSCSI 仮想ディスクの削除とは iSCSI ターゲットとの関連付けを切断することを意味します。このとき、明示的に iSCSI 仮想ディスクの削除を指定することで、物理的な削除を行うことも可能です。

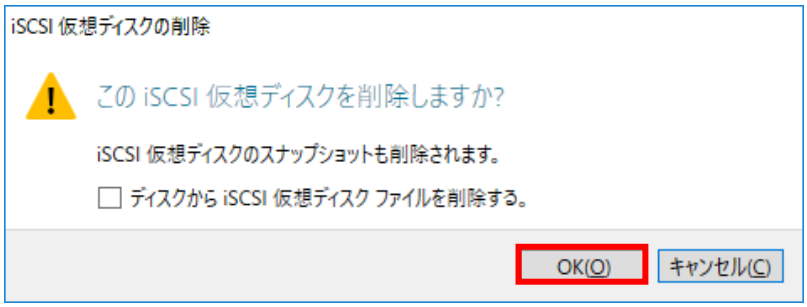
ここでは、物理的な削除は行わず、iSCSI 仮想ディスクの関連付けを切断する手順を説明します。

1. サーバーマネージャーの [ファイルサービスと記憶域サービス] - [iSCSI] をクリックします。

2. iSCSI 仮想ディスクの一覧から、削除する iSCSI 仮想ディスクを右クリックして [iSCSI 仮想ディスクの削除] をクリックします。



3. 以下のメッセージが表示されたら、[OK] ボタンをクリックします。
   なお、iSCSI 仮想ディスクを物理的に削除する場合は、本画面のチェックボックスを選択後、[OK] ボタンをクリックします。物理的に削除しなかった iSCSI 仮想ディスクは、インポートすることで再利用が可能です。



4.3.7.7 iSCSI 仮想ディスクのインポート

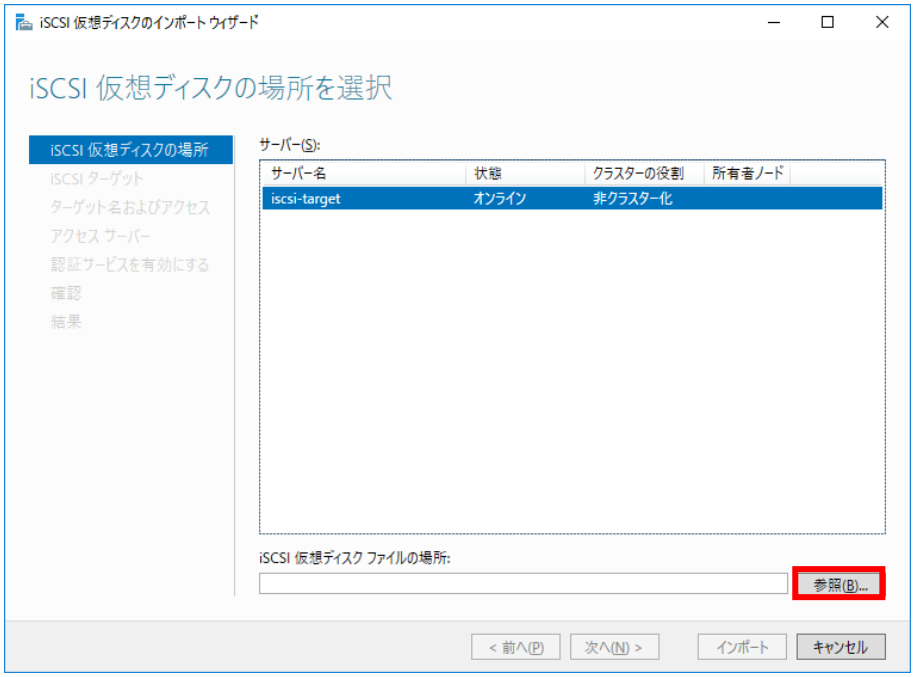
iSCSI 仮想ディスクのインポートを行うと、以前使用していた VHD ファイルを iSCSI 仮想ディスクとして再利用することができます。インポート後、iSCSI イニシエーターでの設定変更(【iSCSI イニシエーター側の仮想ディスクの追加】参照)することで、iSCSI イニシエーターから iSCSI 仮想ディスクへのアクセスが可能になります。

ここでは、未使用の iSCSI 仮想ディスク(VirtualDisk02.vhdx)をインポートし、iSCSI ターゲット(target02)に割り当てる手順を説明します。

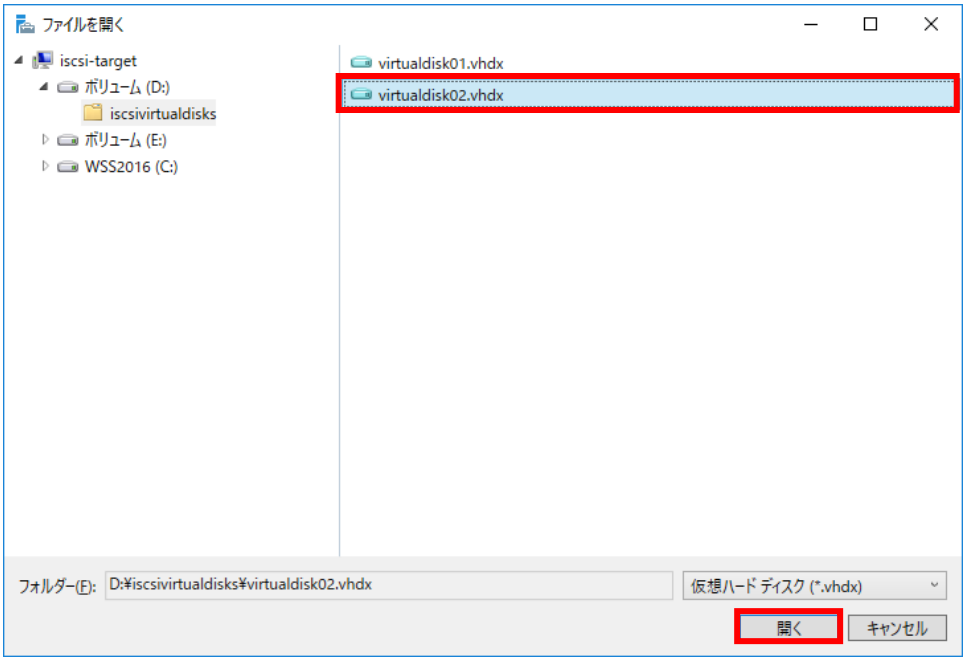
1. サーバーマネージャーの [ファイルサービスと記憶域サービス] - [iSCSI] をクリックします。

2. iSCSI 仮想ディスクの [タスク] – [iSCSI 仮想ディスクのインポート] をクリックします。

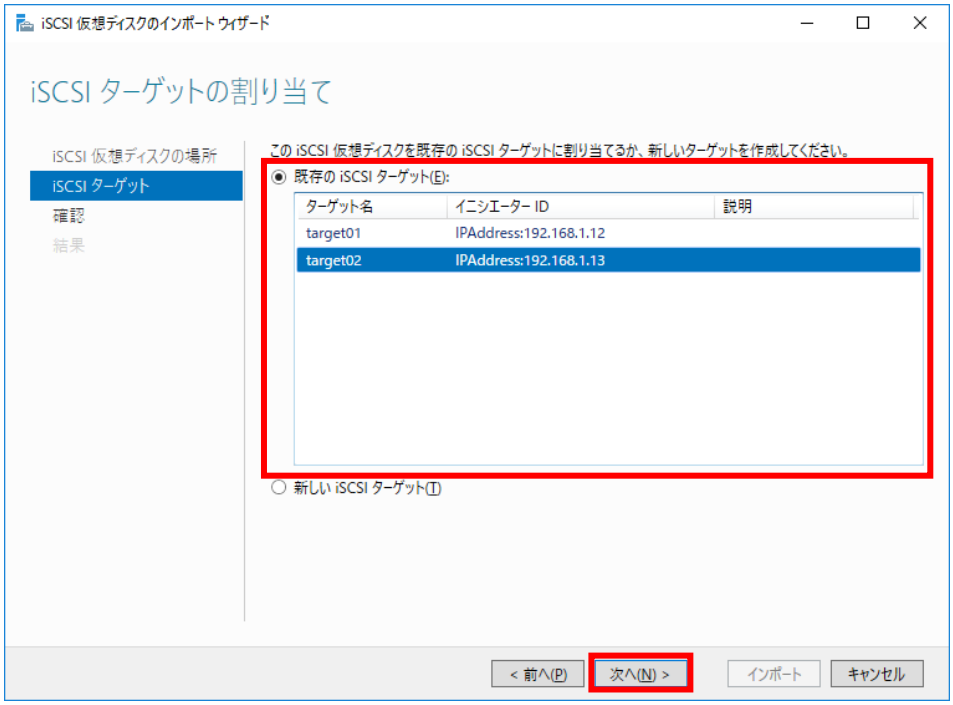
3. [iSCSI 仮想ディスクの場所を選択] で、[参照] ボタンをクリックします。



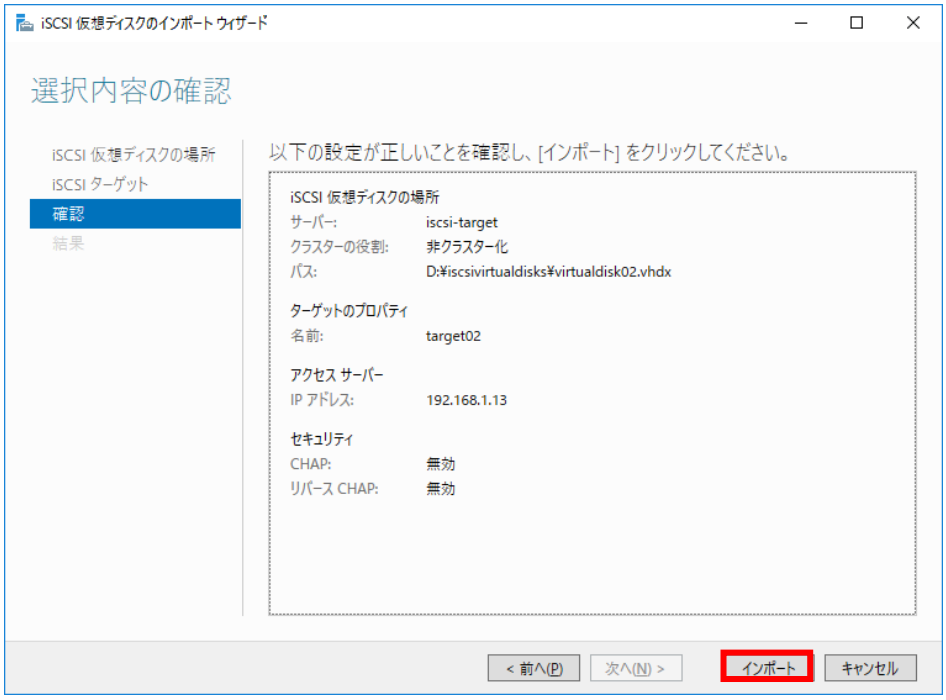
4. [ファイルを開く] 画面で、インポートする VHD ファイルを選択して、[開く] ボタンをクリックします。[3.]の画面に戻りますので [次へ] をクリックします。



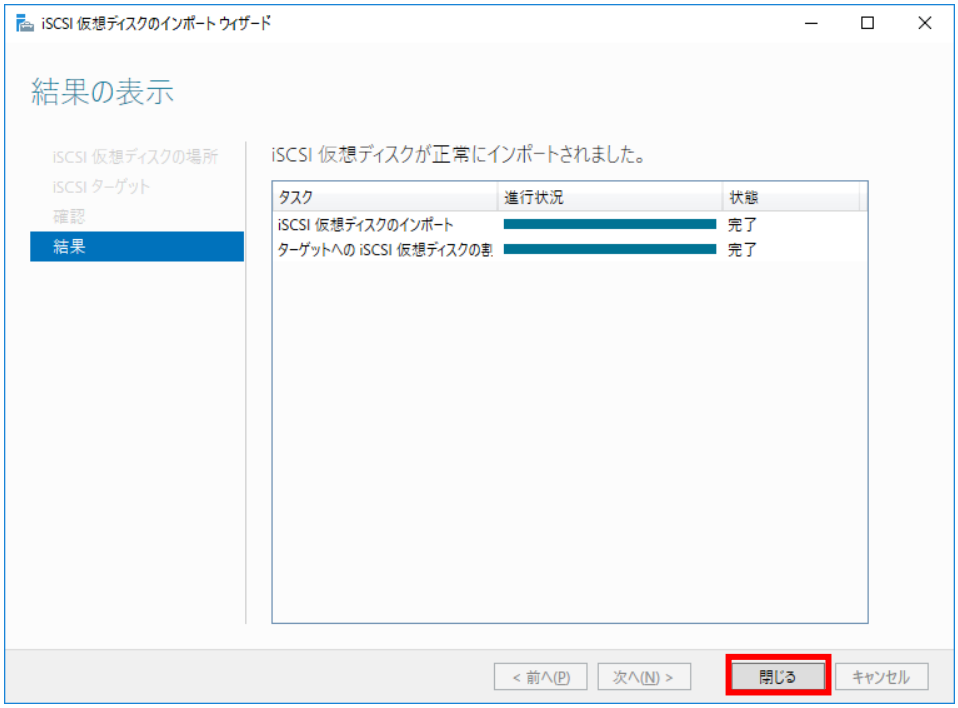
5. [iSCSI ターゲットの割り当て] 画面で、[既存の iSCSI ターゲット] の一覧から、割り当てる iSCSI ターゲットを選択し、[次へ] ボタンをクリックします。



6. [選択内容の確認] 画面で、変更内容を確認して [インポート] ボタンをクリックします。



7. [結果の表示] 画面で、 [閉じる] ボタンをクリックします。

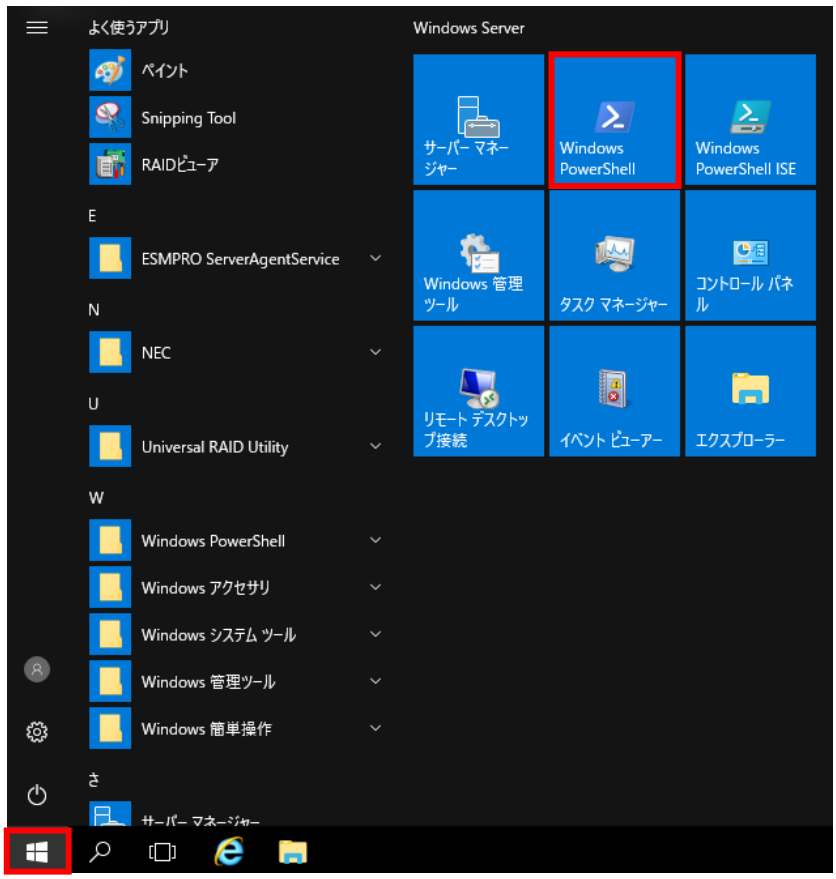


4.3.7.8 iSCSI 仮想ディスクのスナップショットの作成

iSCSI 仮想ディスクのスナップショットを作成していれば、スナップショット作成時点の状態に戻すことができます。iSCSI ターゲットサーバー上に iSCSI 仮想ディスクのスナップショットをエクスポートし、iSCSI ターゲットに割り当てることで iSCSI イニシエーターからアクセスすることが可能になります。

ここでは、iSCSI 仮想ディスクのスナップショットを iSCSI ターゲットサーバー上で作成する手順を説明します。

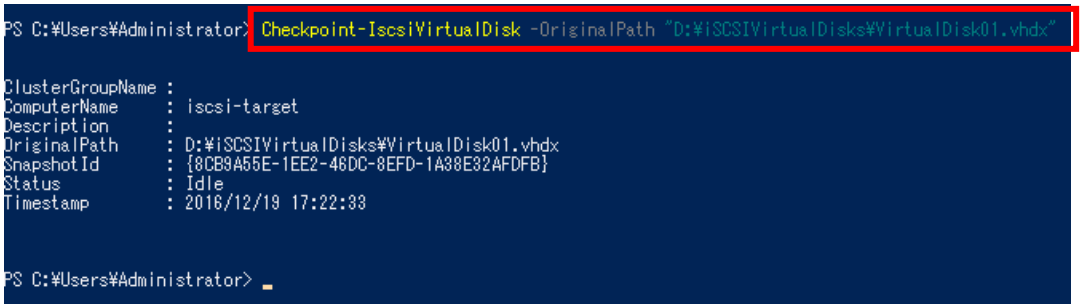
1. デスクトップ画面のタスクバーより、左端の Windows ボタンを押下後、[Windows PowerShell] を起動します。



2. PowerShell にて、

   Checkpoint-IscsiVirtualDisk -OriginalPath “iSCSI 仮想ディスクのパス”

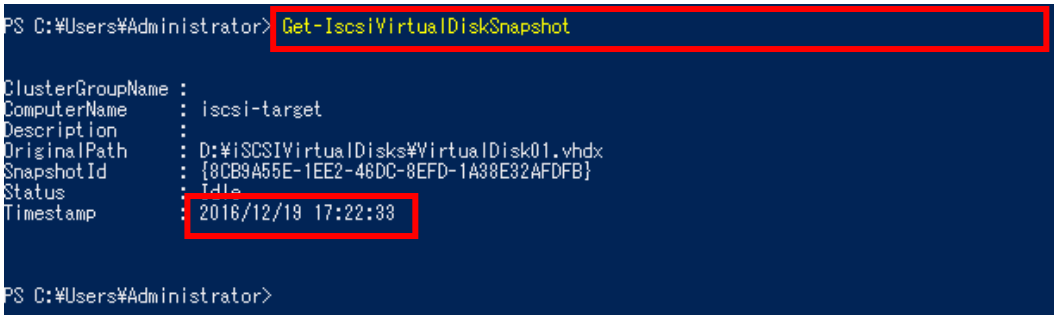
   を実行することで iSCSI 仮想ディスクのスナップショットを作成できます。



3. PowerShell にて、

   Get-IscsiVirtualDiskSnapshot

   を実行することで 取得済みの iSCSI 仮想ディスクのスナップショット一覧が表示されます。複数表示される場合、スナップショットの世代は Timestamp の値にて識別してください。



4.3.7.9 iSCSI 仮想ディスクのスナップショットの取り込み

取得した iSCSI 仮想ディスクのスナップショットは、PowerShell コマンドにより、サーバーマネージャーに取り込むことで、iSCSI イニシエーターからアクセス可能となります。

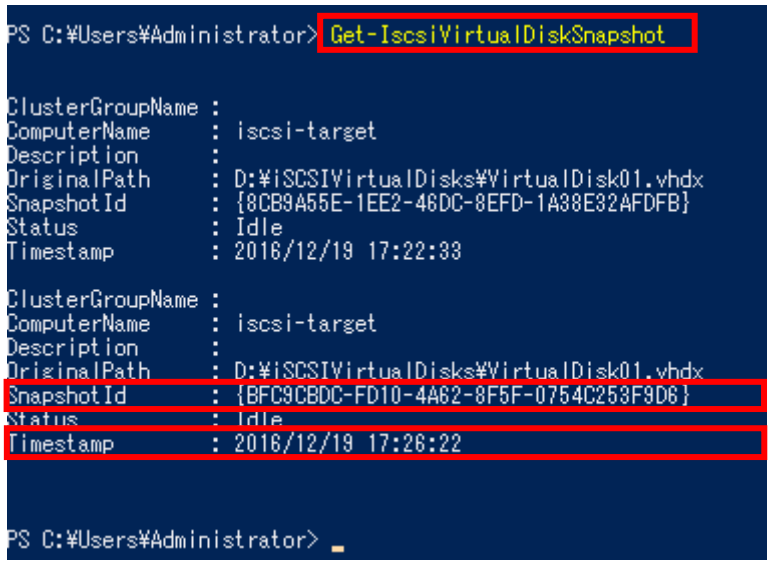
ここでは、取得済みの iSCSI 仮想ディスクのスナップショットをサーバーマネージャーに取り込む手順を説明します。

1. デスクトップ画面のタスクバーより、左端の Windows ボタンを押下後、[Windows PowerShell] を起動します。

2. PowerShell にて、

   Get-IscsiVirtualDiskSnapshot

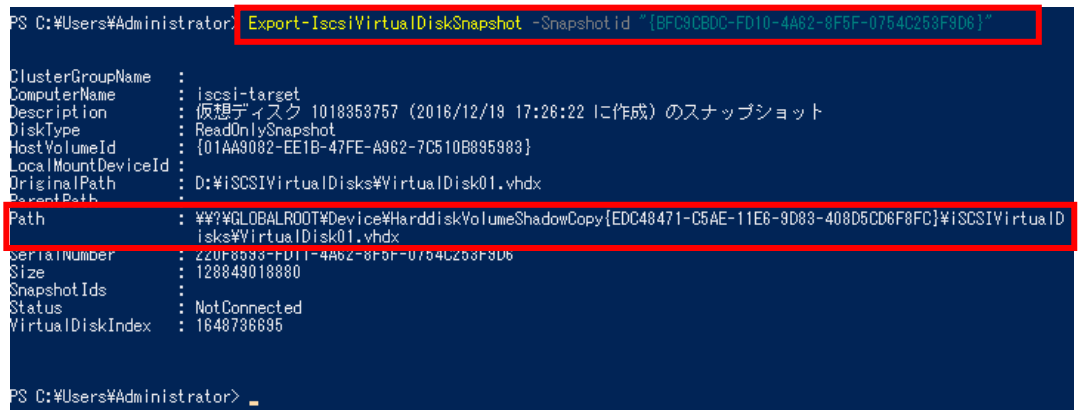
   を実行して、iSCSI 仮想ディスクのスナップショットの一覧から Timestamp を参照し、取り込みたいスナップショットの SnapshotId を確認します。



3. PowerShell にて、上記で確認した SnapshotId を指定した

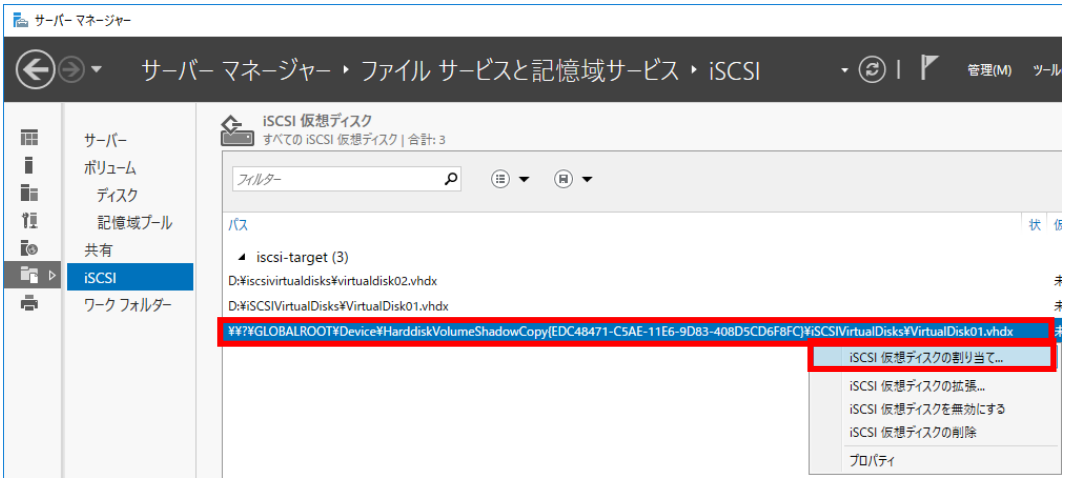
   Export-IscsiVirtualDiskSnapshot -SnapshotId “SnapshotId”

   を実行して、iSCSI 仮想ディスクのスナップショットを取り込みます。



上記のコマンド実行結果の「Path」欄に表示されているパスが、次項で表示されます。

4. サーバーマネージャーに iSCSI 仮想ディスクのスナップショットを取り込むと、iSCSI 仮想ディスクの一覧に前項で取り込んだ iSCSI 仮想ディスクのスナップショットのパスが表示されます。この iSCSI 仮想ディスクに iSCSI ターゲットを割り当て（【iSCSI 仮想ディスクの割り当て変更】参照）、iSCSI イニシエーターでの設定変更(【iSCSI イニシエーター側の仮想ディスクの追加】参照)することで、iSCSI イニシエーターから iSCSI 仮想ディスクのスナップショットにアクセスすることが可能になります。



4.3.7.10　iSCSI 仮想ディスクのスナップショットの削除

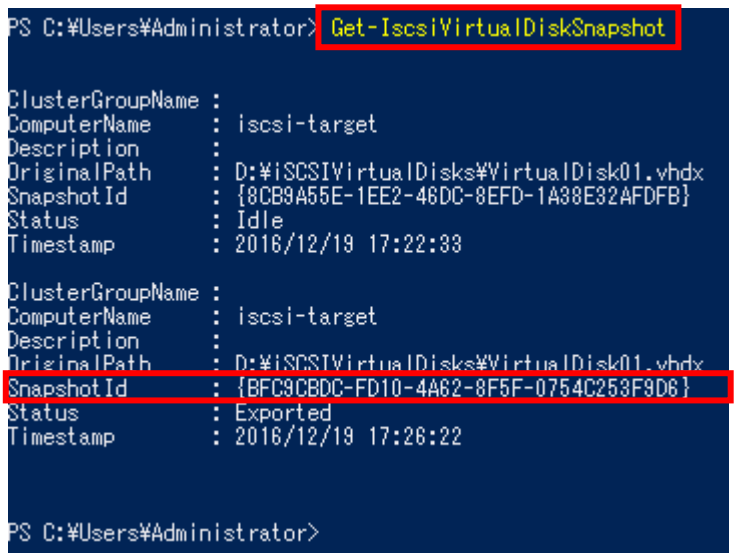
ここでは、作成した iSCSI 仮想ディスクのスナップショットを削除する方法について説明します。

1. デスクトップ画面のタスクバーより、左端の Windows ボタンを押下後、[Windows PowerShell] を起動します。

2. PowerShell にて、

   Get-IscsiVirtualDiskSnapshot

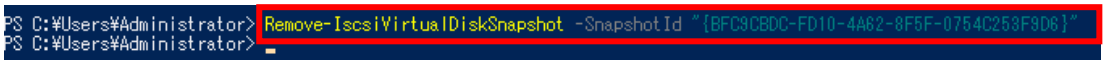
   を実行して、iSCSI 仮想ディスクのスナップショットの一覧を表示し、削除したい SnapshotId を確認します。



3. PowerShell にて、上記で確認した SnapshotId を指定した

   Remove-IscsiVirtualDiskSnapshot -SnapshotId “SnapshotId”

   を実行して、iSCSI 仮想ディスクのスナップショットを削除します。



4.3.8 iSCSI イニシエーターの運用

ここでは、iStorage NS の iSCSI ターゲットに接続する、iSCSI イニシエーターの運用に関して、Windows Server OS を例に説明します。なお、下記手順の画面イメージは例であり、実際とは異なっている場合があります。

4.3.8.1 iSCSI ターゲットとの切断

通常のイニシエーター側装置の運用におきましては、OS の起動と共に iSCSI 接続ディスクに自動接続し、OS のシャットダウンと共に iSCSI 接続ディスクの切断を行います。このため、手動による iSCSI ターゲットとの切断操作は、通常は実施不要です。
しかしながら、iSCSI 仮想ディスクの構成変更時などで、iSCSI イニシエーター側装置の OS が起動中のままで、iSCSI ターゲットへの接続を切断する必要が生じる場合があります。その場合は、以下の手順で iSCSI ターゲットとの接続を切断してください。

【切断前の事前準備】

1. 切断対象の iSCSI 接続ディスク上にある全てのパーティションのドライブに対し、現在アクセスを実施していないことを確認します。
2. より安全な切断準備を行う場合、切断対象の iSCSI 接続ディスク上に存在する全てのパーティションの各ドライブに対し、管理者権限のコマンドプロンプトにて下記のコマンドを順次実行し、マウント解除(アンマウント)します。マウント解除すると、ファイルシステムが該当ドライブにアクセスしなくなります。

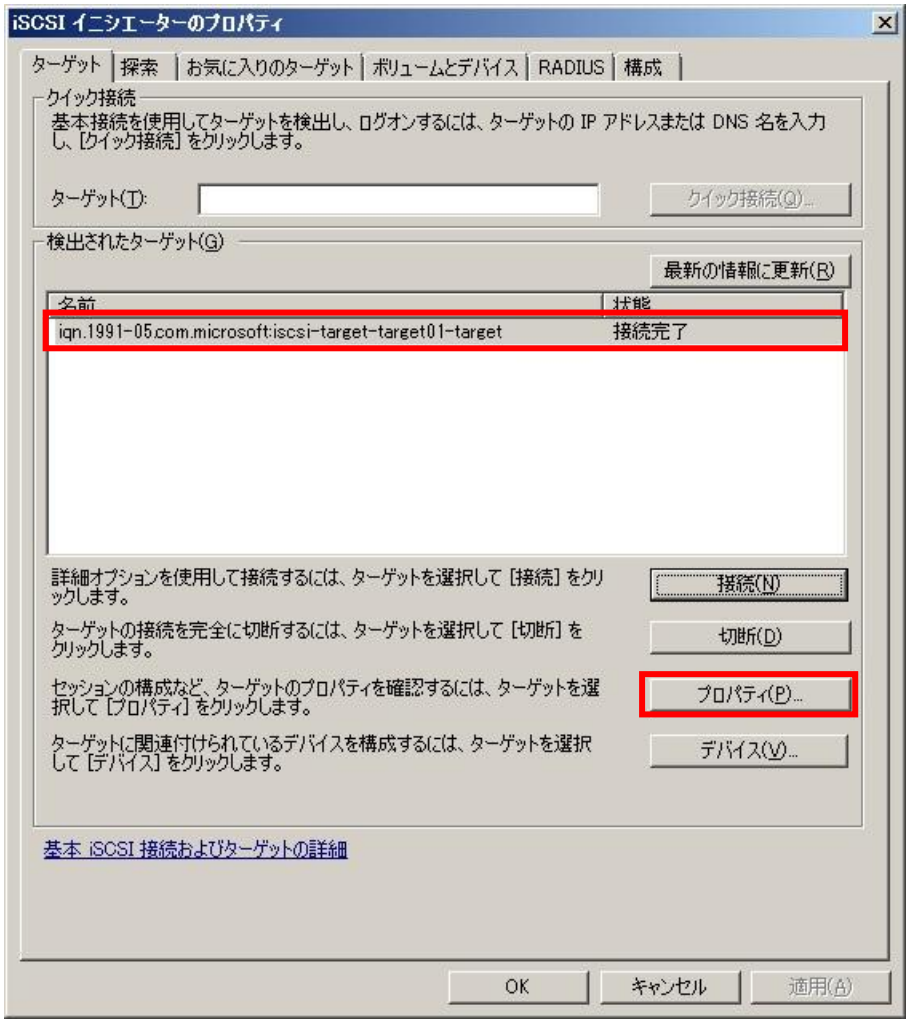
   mountvol <ドライブ文字>: /P

   なお、本マウント解除操作を実施した場合は、次回 iSCSI 接続ディスクをオンラインにした際に、iSCSI 接続ディスク上の各ボリュームにドライブ文字が自動付与されませんので、手動にてドライブ文字の割り当て操作が必要になります。
3. [ディスクの管理] ツールを起動し、iSCSI 接続ディスクを右クリックし、[オフライン] を選択します。

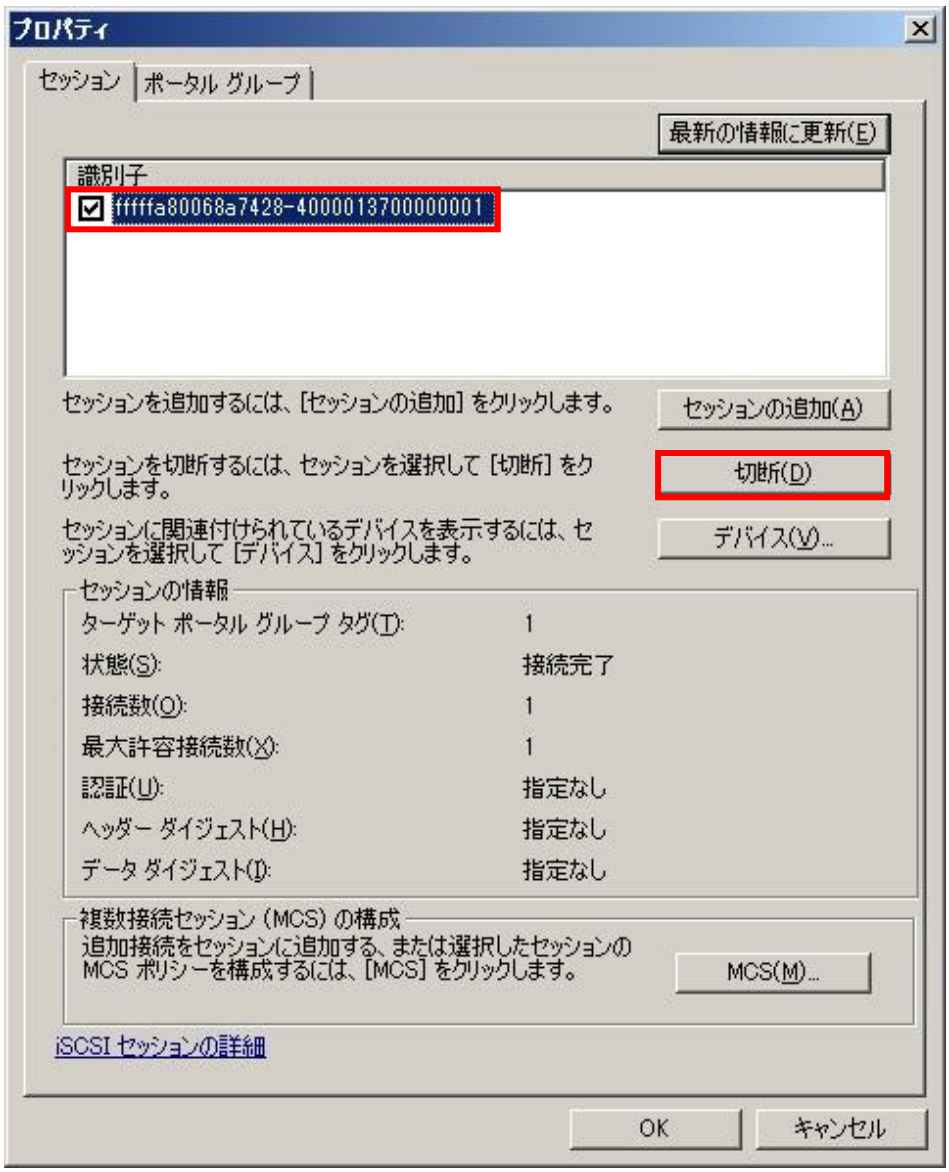
【iSCSI ターゲットとの切断手順】

1. iSCSI イニシエーターで [スタート] - [管理ツール] - [iSCSI イニシエーター] をクリックします。

2. [ターゲット] タブをクリックし、切断する iSCSI ターゲットの IQN を選択して [プロパティ] ボタンをクリックします。



3. [セッション] タブの [識別子] から、切断するパスを選択し、[切断] ボタンをクリックします。マルチパス I/O 環境の場合は、複数の識別子を選択し、切断してください。



4. [OK] ボタンをクリックして、ターゲットのプロパティおよび iSCSI イニシエーターのプロパティ画面を閉じます。

【注意】

iSCSI イニシエーターの再起動時に iSCSI ターゲットとの接続を自動的に行っており、今後 iSCSI ターゲットと接続しない場合には、[お気に入りのターゲット] からこの iSCSI ターゲットの IQN を削除してください。

iSCSI ターゲットへの接続を切断すると iSCSI 仮想ディスクは表示されなくなります。

切断前

切断後

【注意】

iSCSI ターゲットに再接続を行った場合、同じ iSCSI 仮想ディスクへの接続を行った場合においても、割り当てられるドライブ文字が変更される可能性がありますので注意してください。

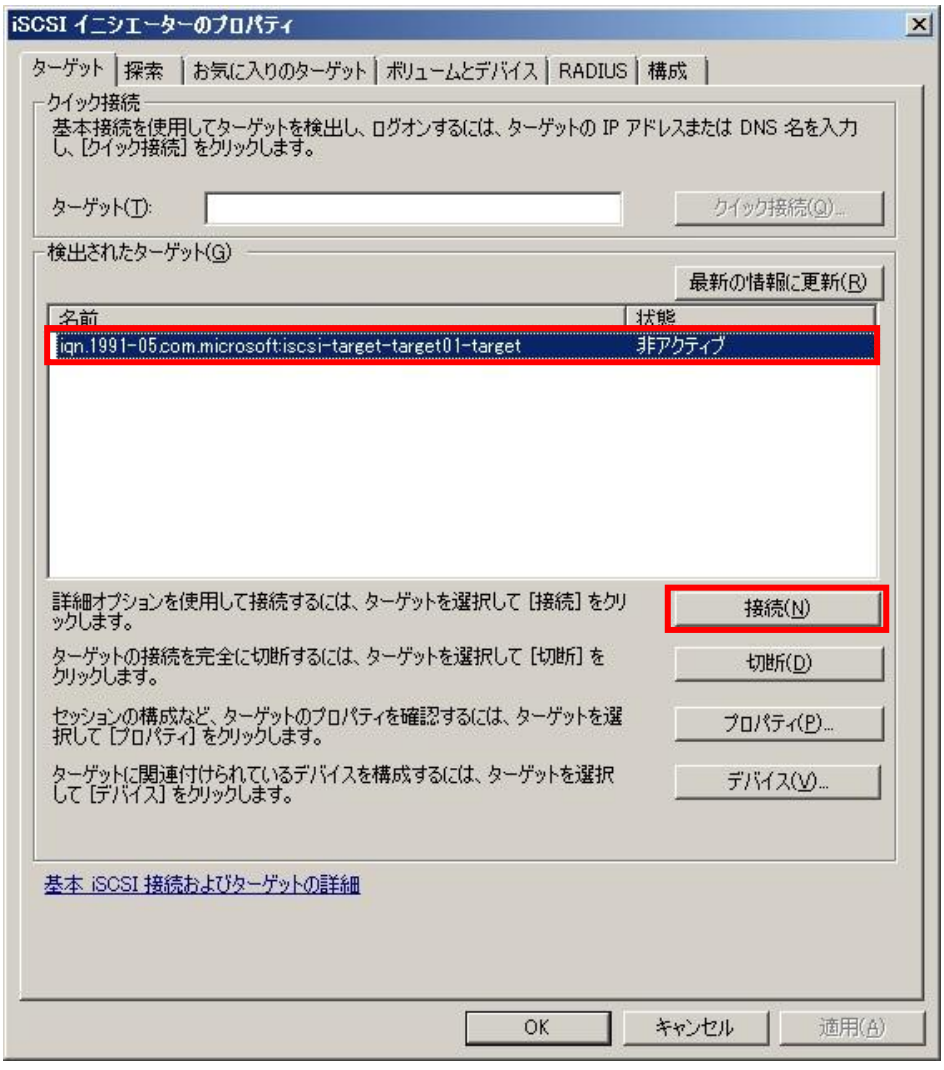
4.3.8.2 iSCSI ターゲットへの接続

ここでは、iSCSI ターゲットへ接続する手順について説明します。

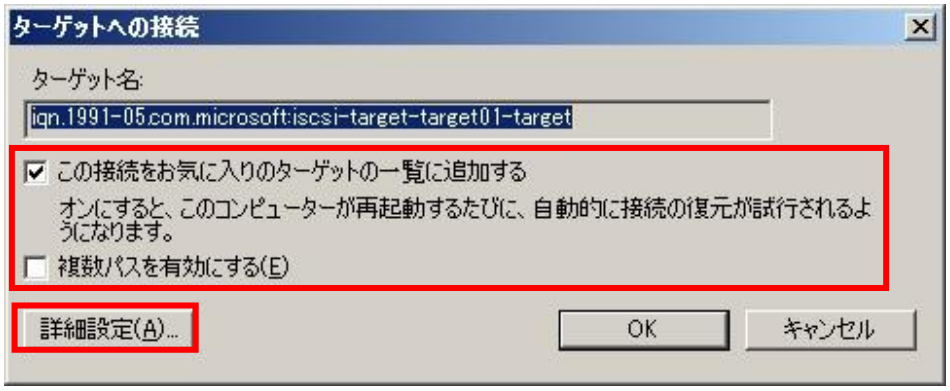
1. iSCSI イニシエーターで [スタート] - [管理ツール] - [iSCSI イニシエーター] をクリックします。

2. [ターゲット] タブをクリックします。iSCSI ターゲットの IQN が表示され、状態が [非アクティブ] になっています。表示されていない場合は、[最新の情報に更新] ボタンをクリックします。

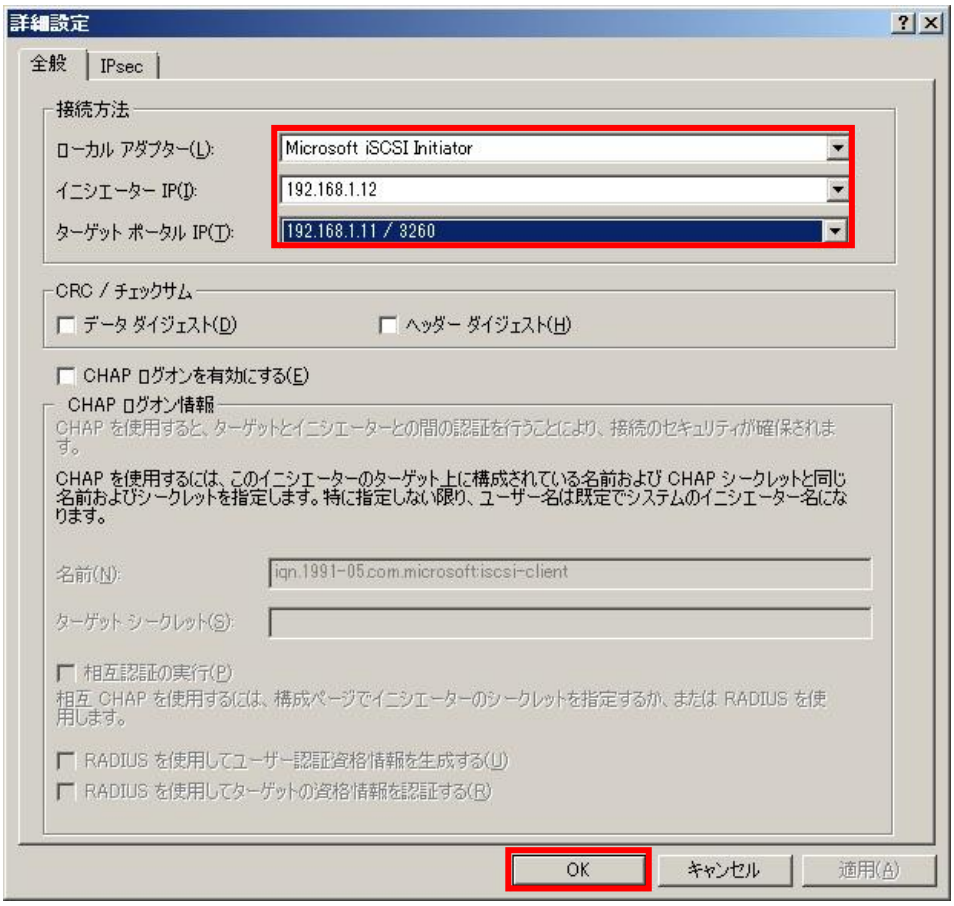
3. 接続する iSCSI ターゲットの IQN を選択し、[接続] ボタンをクリックします。なお、検出済みのターゲットではなく、新規のターゲットに接続する場合は、【iSCSI イニシエーターの設定】の手順で探索を実施してください。



4. [ターゲットへの接続] 画面で、 [この接続をお気に入りのターゲット一覧に追加する] をチェックして、[詳細設定] ボタンをクリックします。なお、[複数パスを有効にする] をチェックすると、iSCSI ターゲットへのアクセス経路を複数確保することができます。ただし、事前に iSCSI 用に複数の NIC と、マルチパス I/O 機能を追加しておく必要があります。本書では、イニシエーター側の装置上でのマルチパス I/O 機能の追加手順は省略します。

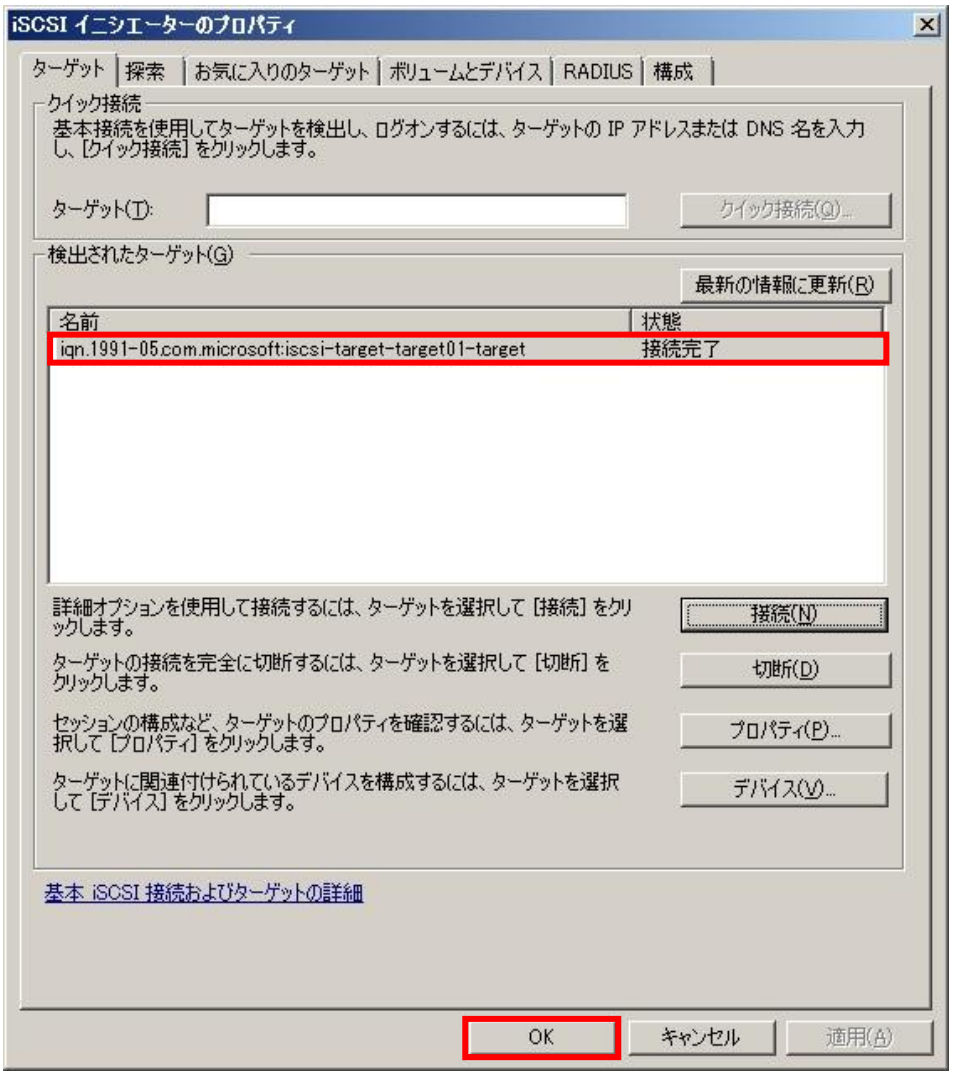


5. [全般] タブの [接続方法] 欄で、[ローカルアダプター] を [Microsoft iSCSI Initiator]、[イニシエーター IP] を iSCSI 接続に使用する自身の IP アドレス、[ターゲットポータル IP] で iSCSI ターゲットの IP アドレスを選択し、[OK] ボタンをクリックします。



6. [ターゲットへの接続] 画面に戻りますので、[OK] ボタンをクリックします。

7. 対象の iSCSI ターゲットの状態が [接続完了] と表示されたことを確認し、[OK] ボタンをクリックして画面を閉じます。



4.3.8.3 iSCSI イニシエーター側の仮想ディスクの追加

iSCSI イニシエーターで使用可能な iSCSI 仮想ディスクの追加は、iSCSI ターゲットで行います。追加方法については、【iSCSI 仮想ディスクの作成】を参照してください。ここでは、iSCSI ターゲット側でディスクの追加を行った後、iSCSI イニシエーターで行うべき手順や注意を説明します。

- iSCSI ターゲットで既存の iSCSI ターゲットに新規の iSCSI 仮想ディスクを追加した場合は、iSCSI イニシエーターにて、追加した iSCSI 仮想ディスクのフォーマット、ボリュームの作成を行う必要があります。手順は、【管理者ガイド（概要編）ボリュームを作成する】を参照してください。

既存の iSCSI 仮想ディスク

追加した iSCSI 仮想ディスク

- 新規にiSCSI ターゲットと iSCSI 仮想ディスクを作成した場合は、iSCSI イニシエーターにて、作成した iSCSI ターゲットへの接続設定を行う必要があります。【iSCSI ターゲットへの接続】を参照して、新たに作成した iSCSI ターゲットに接続してください。その後、iSCSI イニシエーターにて、追加した iSCSI 仮想ディスクのフォーマット、ボリュームの作成を行ってください。手順は、【管理者ガイド（概要編）ボリュームを作成する】を参照してください。

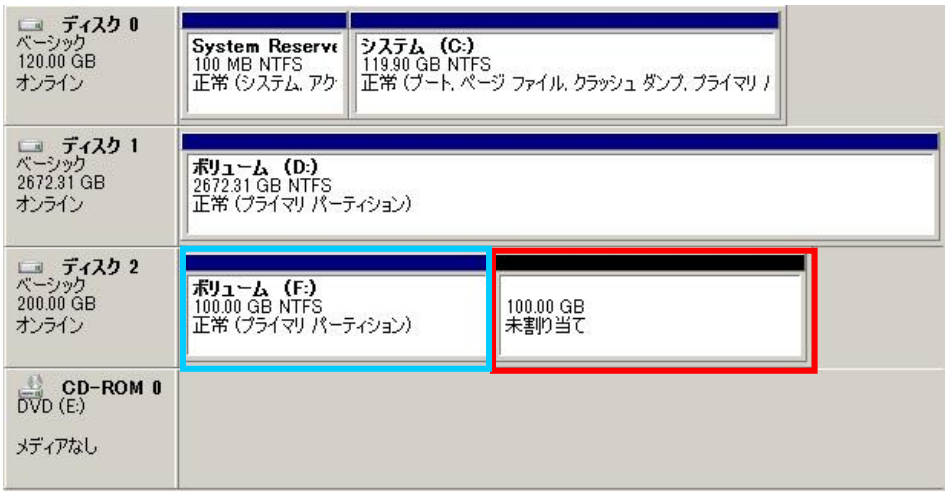
既存の iSCSI 仮想ディスク

追加した iSCSI 仮想ディスク

4.3.8.4 iSCSI イニシエーター側の仮想ディスクの拡張

iSCSI イニシエーターで使用可能な iSCSI 仮想ディスクの拡張は、iSCSI ターゲットで行います。拡張方法については、【iSCSI 仮想ディスクの拡張】を参照してください。ここでは、iSCSI ターゲット側でディスクの拡張を行った後、iSCSI イニシエーターで行うべき手順や注意を説明します。

- 既存の iSCSI 仮想ディスクを拡張したい場合は、iSCSI イニシエーターの [ディスクの管理] 画面で、ボリュームの拡張を行ってください。詳細は iSCSI イニシエーターの OS のヘルプをご確認ください。



既存の iSCSI 仮想ディスク

拡張可能な iSCSI 仮想ディスク

4.3.9 注意・制限事項

4.3.9.1 注意事項

- iSCSI イニシエーターと iSCSI ターゲットとの間の通信には自動プライベート IP アドレス (169.254.x.x) を使用しないでください。

- 1 つの iSCSI 仮想ディスクに複数の iSCSI イニシエーターから同時にアクセスすると、iSCSI 仮想ディスク内のデータが破壊される恐れがあります。クラスターシステムのように iSCSI イニシエーター側で iSCSI 仮想ディスクの排他制御が行える環境を除いて、1 つの iSCSI 仮想ディスクには 1 台の iSCSI イニシエーターからのみアクセスするように設定してください。

- iSCSI ターゲットにて、iSCSI イニシエーターとの接続に影響を与えるような変更を実施する場合、変更前に iSCSI イニシエーター側で iSCSI ターゲットへのアクセスを切断してください。

- iSCSI ターゲットの IQN を変更する際、iSCSI ターゲットの IQN が他と重複しないようにしてください。

- iSCSI ターゲットの IQN 変更後は、iSCSI イニシエーターで接続設定を変更する必要があります。

- iSCSI ターゲット側で iSCSI 仮想ディスクのサイズを拡張すると、iSCSI イニシエーターでは、元のボリュームサイズが自動的に増えることはなく、未使用領域が既存のボリュームの後ろに追加されますので、iSCSI イニシエーター側にて設定の変更を行ってください。

- [新しい iSCSI 仮想ディスクウィザード]を使って、iSCSI 仮想ディスクを作成した場合、このウィザードが完了しても、バックグラウンドでは iSCSI 仮想ディスクの初期化が行われている場合があります。iSCSI 仮想ディスクの初期化状況はサーバーマネージャー画面で確認することができますので、初期化が完了するのを待って、イニシエーターからの接続を行ってください。なお、iSCSI 仮想ディスクの初期化が完了していない状態ではイニシエーターから、iSCSI 仮想ディスクは見えません。

- 1 つの LAN ポートを、通常用途（ファイル共有等）と、iSCSI 用途の両方で使用することは可能ですが、iSCSI の通信性能が求められる場合は、iSCSI 専用の LAN ポートを設置することをご検討ください。

- 業務要件に必要な iSCSI の通信性能が得られるかについて、事前に十分に検証を実施してください。

- iSCSI はオープンなプロトコルのため、iSCSI の接続元 (イニシエーター) は Microsoft 製品に限定されませんが、他社製品からの接続時には相性問題が発生する可能性が考えられます。このため、接続元の製品観点で、Windows Server OS 付属の iSCSI ターゲットへの接続が検証済みとなっているかご確認ください。

4.3.9.2 制限事項

- 本機は、NIC チーミング(LBFO)の NIC(仮想 NIC)を使用した iSCSI 接続/通信はサポートしておりません。複数の NIC を使用して冗長構成とする場合は、マルチパス I/O（MPIO）を使用してください。なお、本制限は、本機が iSCSI ターゲット側装置となる場合だけではなく、iSCSI イニシエーター側装置となる場合も同様となります。

- iSCSI ターゲットの iSCSI 接続に NIC ベンダーが提供する NIC チーミングを使用しないでください。