進化する明日へ Continue thinking

I-O DATA

ホワイトペーパーシリーズ：

Windows Server IoT 2019 for Storage

を活用した生産性向上術

1. ファイルサービス編

2. クライアント PC 管理編

3. ドキュメント活用編

4. リモートワーク対応編

2020 年 8 月 31 日

内容

1　概要

1.1　このガイドについて

このガイドのシリーズは、Windows Server IoT 2019 for Storage Standard または Workgroup を搭載する LAN DISK Z（HDL-Z）シリーズの NAS デバイスを利用するにあたり、Windows Server IoT 2019 for Storage の能力を最大限に生かしてエンドユーザーの生産性の向上を図る、ワンランク上の活用方法について解説します。

> 参照情報
>
> このガイドのシリーズは、既に公開済みの以下のホワイトペーパーの続編です。以下のホワイトペーパーで解説済みの概念や手順については参照元として、“**前編『1. インフラ編』**” のように示します。
>
> Windows Server IoT 2019 for Storage で構築する企業向け最新ファイルサーバー（全 4 編）
> 1. インフラ編 ／ 2. 運用管理編 ／ 3. 集中管理編 ／ 4. ハイブリッドクラウド編
> https://www.iodata.jp/biz/whitepaper/

1.2　ファイルサービスへのアクセスを提供するその他の方法について

Windows Server IoT 2019 for Storage を搭載する HDL-Z シリーズは、Windows ネットワークとの親和性が特に高く、Windows Server ベースのファイルサーバーとしてワークグループ環境または Active Directory ドメイン環境で完全に機能します。

このガイドの前編『1. インフラ編』で解説したように、Windows ネットワークのファイル共有プロトコルである「サーバーメッセージブロック（SMB）」の最新バージョン SMB バージョン 3.x（SMB v3）は、SMB マルチチャンネルや SMB 暗号化機能を標準で備え、高速でセキュアなファイル共有を可能にします。SMB v3 の機能は、Windows 8 および Windows Server 2012 以降で標準で利用できるほか、主要な Linux ディストリビューションや macOS も標準で対応しています。

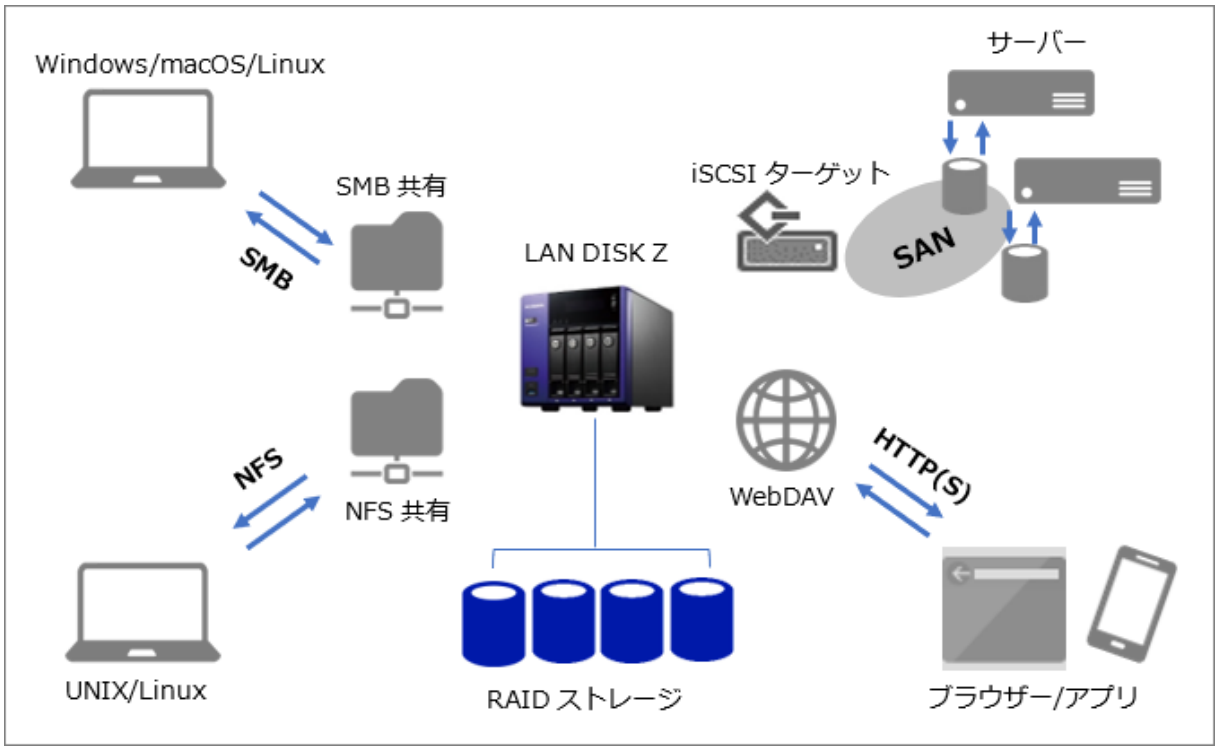
Windows Server IoT 2019 for Storage のファイルサービスは、SMB だけでなく、さまざまなプラットフォームに対して多様なアクセス手段を提供するマルチプロトコル対応です。このガイドでは、iSCSI、NFS、WebDAV の 3 つのプロトコルによるディスクまたはファイルアクセスの概要と、HDL-Z でこれらのプロトコルをサポートするための手順について説明します。

- **iSCSI（Internet Small Computer System Interface）** ･･･ IP（インターネットプロトコル）v4/v6 ネットワークを利用して「記憶域ネットワーク（Storage Area Network、SAN）」を構築するためのブロックアクセス用プロトコルです。iSCSI では、「iSCSI ターゲットサーバー」が「LUN（論理ユニット番号）」（Windows Server では「iSCSI 仮想ディスク」とも呼びます）と呼ばれる記憶域を提供し、「iSCSI イニシエーター」が IP ネットワーク上で SCSI（Small Computer System Interface）パケットを iSCSI ターゲットサーバーに送信します。iSCSI イニシエーターによって接続された LUN は、ローカルディス

クとまったく同じように扱うことができます。Windows Server IoT 2019 for Storage のファイルサービスは、iSCSI ターゲットサーバーの機能をサポートしています。HDL-Z を iSCSI ターゲットサーバーとして構成することで、1 台以上のサーバーやクライアントにアプリケーション（Hyper-V や VMware の仮想マシン、SQL Server データベースの配置先など）用のデータの記憶域やバックアップ用の記憶域を提供することができます。LUN をバックアップ用途で使用する手順については、このガイドの『2. クライアント PC 管理編』で説明します。接続元のサーバーのマザーボードが iSCSI の SAN ブートをサポートしていれば、iSCSI ターゲットサーバー上のイメージから Windows Server やその他の OS をディスクレスでブートさせることも可能です。

- **NFS（Network File System）** ･･･ NFS は UNIX で古くから使用されていたファイル共有プロトコルです。NFS クライアントは NFS サーバーに個別に認証することなしにファイルリソースにアクセスすることができます。マウントやファイル参照のアクセス制御は、UID（ユーザーID）／GID（グループ ID）で識別されます。Windows Server IoT 2019 for Storage のファイルサービスは、NFS サーバーとして NFS v2、NFS v3、NFS v4.1 をサポートしており、UNIX や Linux の NFS クライアントに対して共有サービスを提供できます。

- **WebDAV（Web-based Distributed Authoring and Versioning）** ･･･ WebDAV は古くからある HTTP（Hypertext Transfer Protocol）1.1 の拡張であり、HTTP（非推奨）または HTTPS（推奨）を使用して、Web サーバーとの間でファイルのダウンロードやアップロード、削除を可能にします。Web サーバーの CMS（コンテンツ管理システム）で利用されることが多いプロトコルですが、一般的なファイル共有目的や、ネットワークデバイス（FAX／スキャナーなど）のファイル出力先としても利用できます。Windows Server IoT 2019 for Storage で利用可能なインターネットインフォメーションサービス（IIS）の役割は、WebDAV に対応しています。

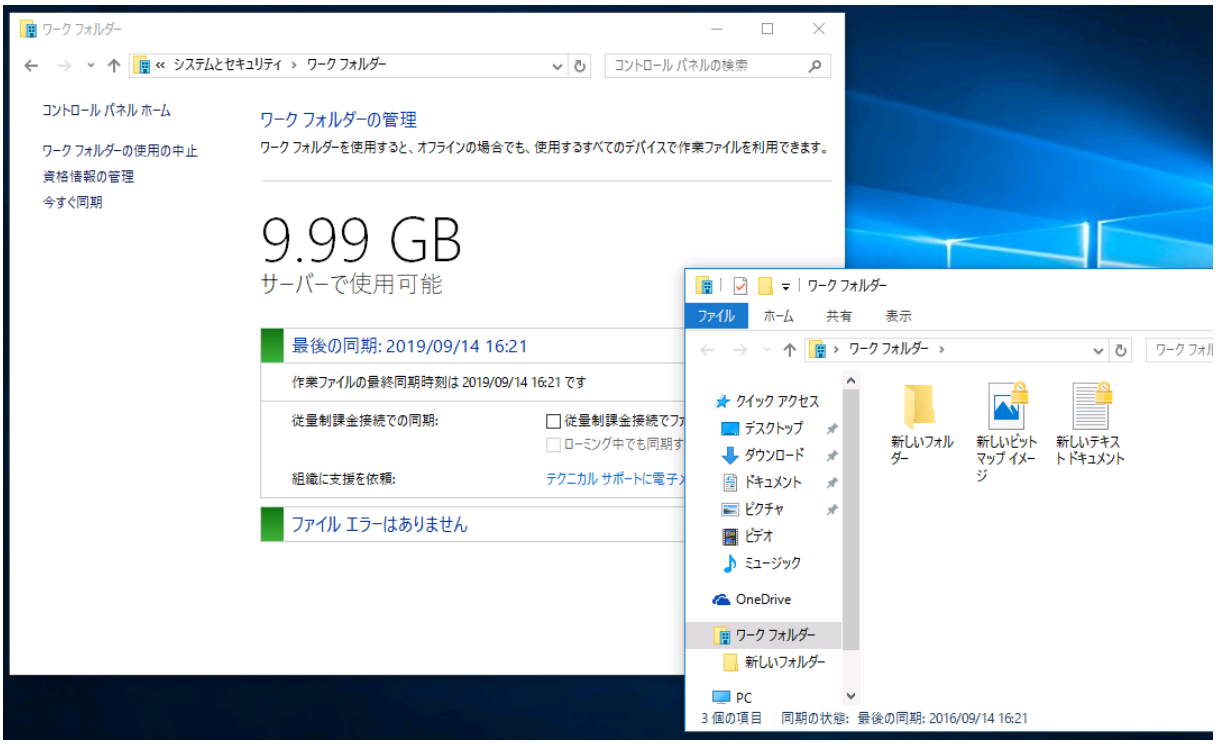


図：Windows Server IoT 2019 for Storage は、マルチプロトコル対応のファイルサービスを提供する

ワークフォルダーについて

Windows Server IoT 2019 for Storage は、HTTPS ベースのファイル共有サービスとして、Windows 10、Windows 8.1、Windows 7、Android、および iOS をクライアントとしてサポートする「ワークフォルダー（Workfolders、SyncShare とも呼ばれます）」という機能も利用可能です。

ワークフォルダーは、主に BYOD（Bring Your Own Device、個人デバイスの業務利用）を想定したもので、HTTPS によるセキュアなアクセス、ファイルの暗号化や画面ロックの強制などの機能を提供します。社内でのファイル共有という用途ではなく、コンシューマー向けの OneDrive サービスと同じように、ユーザーごとの個人データの同期を対象としています。



画面：Windows Server のワークフォルダーは、デバイス管理とユーザーデータの同期を行う、BYOD 向けの機能

社外からもアクセス可能なワークフォルダーの導入には、パブリックな IPv4 固定アドレス、Active Directory ドメイン環境や証明書サービス、厳格な証明書の管理（インターネットから証明書の検証が可能なこと）、セキュアなアクセスのためのゲートウェイの構築（例えば、Windows Server の「Web アプリケーションプロキシ」の環境構築）や追加の認証（Azure MFA）などが必要です。難易度が高い上、導入コストもかかるため、このガイドでは説明しません。このガイドの『4. リモートワーク対応編』では、より簡単に導入可能な、オンプレミスとクラウドのハイブリッドなリモートワーク環境を紹介しています。

1.3　実施環境について

このガイドで説明するネットワーク機能は、HDL-Z が接続された IPv4/IPv6 ネットワークの単一のサブネット環境、または適切にルーティングされたマルチサブネット環境に導入できます。

HDL-Z シリーズは複数の LAN インターフェイスを標準搭載しているため、NIC チーミングを構成することで冗長化と負荷分散、ネットワーク帯域幅の集約が可能です。NIC チーミングは上位のアプリケーションプロトコルの種類（ファイル共有プロトコルなど）に依存せず、IPv4/IPv6 ネットワークで利用できます。NIC チーミングのセットアップについては、このガイドの前編『1. インフラ編』を参照してください。

HDL-Z シリーズの上位モデルには 10GbE ネットワークインターフェイスを搭載しているものがあります。HDL-Z を iSCSI ターゲットサーバーとして利用する場合は、10GbE ネットワークインターフェイスを iSCSI 専用に使用して、IP SAN で高速リンクを使用できるようにし、社内クライアントからの共有へのアクセストラフィックと分離するとよいでしょう。ただし、iSCSI イニシエーター側にも追加の 10GbE ネットワークインターフェイスが必要になります。この構成は必須ではありませんが、アプリケーションデータ用の iSCSI 接続のディスクアクセス性能を最適化するために推奨します。対象となるアプリケーションとしては、高速なディスク I/O が要求される Hyper-V、VMware、SQL Server などがあります。

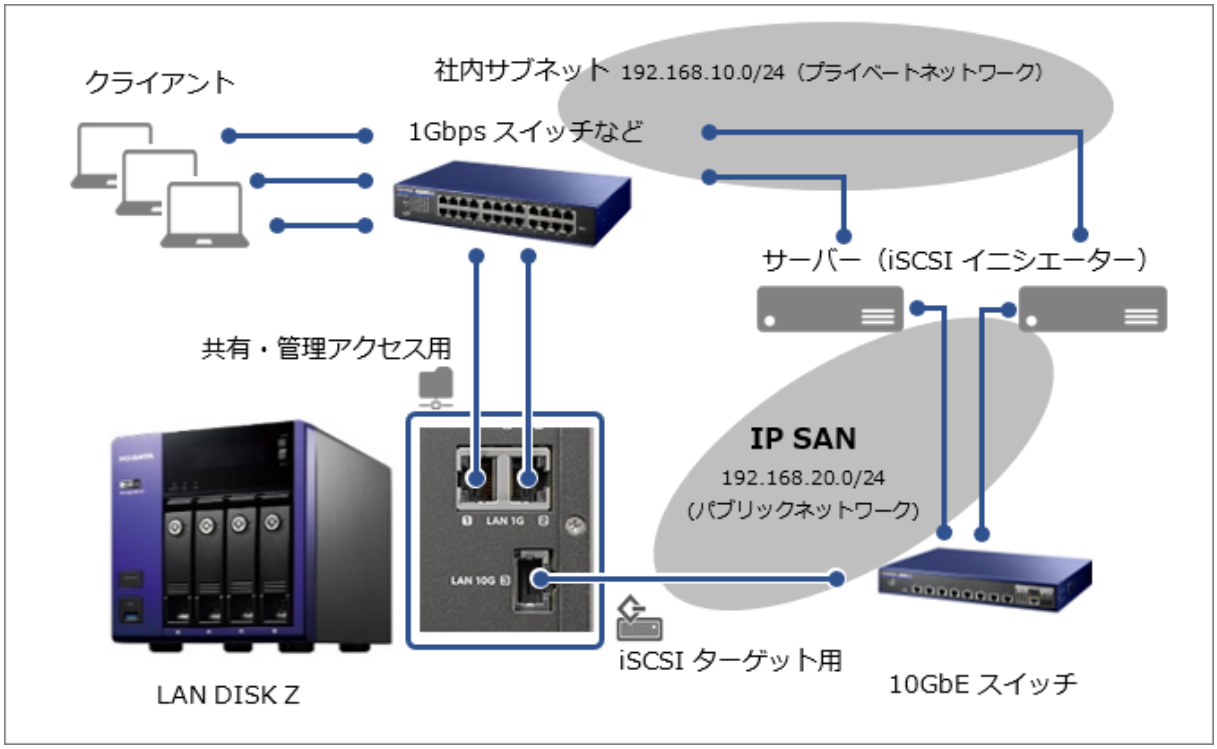


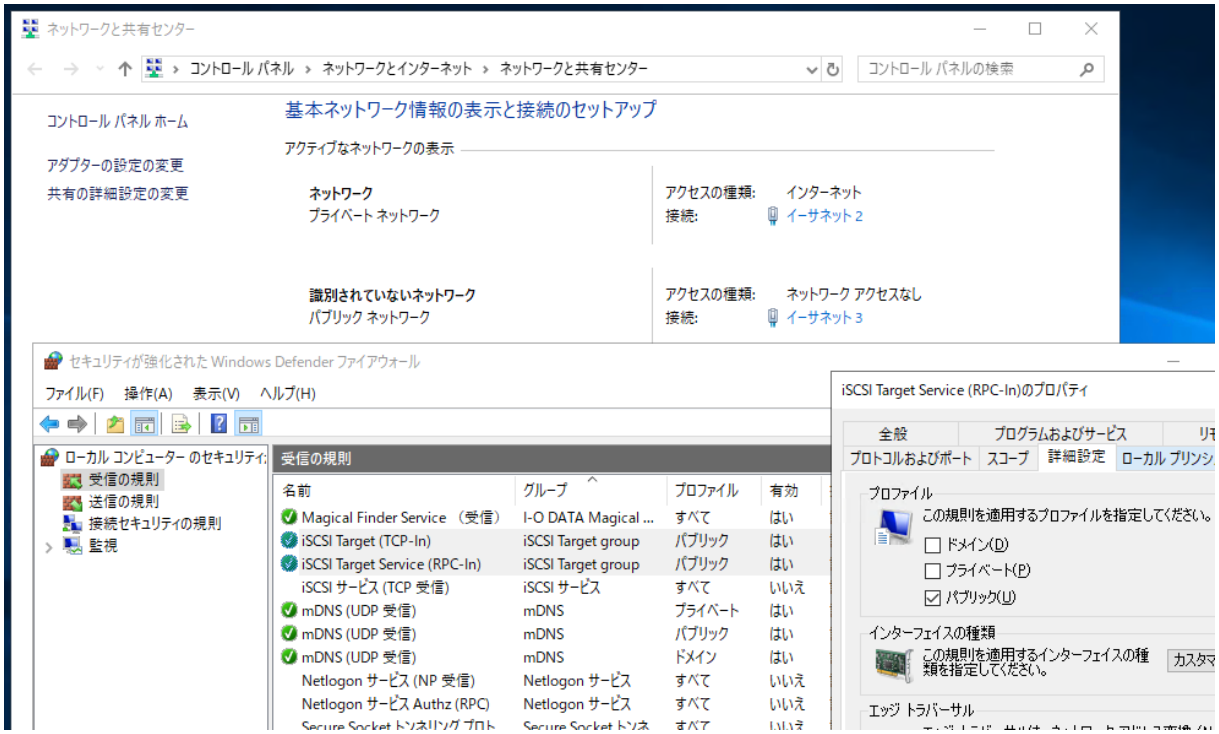
図 : HDL-Z シリーズの 10GbE ネットワークを iSCSI ベースの IP SAN 専用にする場合のネットワーク構成例（オプション）

iSCSI 専用の高速リンクのサブネットを構成する場合は、10GbE スイッチに iSCSI ターゲットサーバーと iSCSI イニシエーターのサーバーの 10GbE ネットワークを接続し、10GbE ネットワークの IP v4 アドレスとサブネットマスクを手動で静的に設定します。デフォルトゲートウェイの指定は不要です。

Windows はデフォルトゲートウェイのないネットワークを「識別されていないネットワーク」として検出

し、「パブリックネットワーク」として構成します。iSCSI 専用にするためには、HDL-Z の「セキュリティが強化された Windows Defender ファイアウォール」（WF.msc）で「iSCSI Target（TCP-in）」と「iSCSI Target Service（RPC-in）」の受信許可規則を「パブリック」プロファイルに限定します。

あるいは、IP SAN に接続されるすべての HDL-Z とサーバーで「パブリック」プロファイルのファイアウォールを無効化し、iSCSI イニシエーター側の送信の規則「iSCSI サービス」を「ドメイン」および「プライベート」プロファイルでブロックするように構成することもできます。



画面：iSCSI ネットワークの IP アドレスを手動で設定し（デフォルトゲートウェイの指定はなし）、HDL-Z のファイアウォール設定で「iSCSI Target（TCP-in）」と「iSCSI Target Service（RPC-in）」の受信許可規則を「パブリック」プロファイルに限定する

> **iSCSI 専用のサブネットの構成はオプション**
>
> iSCSI 専用のサブネットを構成してトラフィックを分離するためには、iSCSI イニシエーターとなる接続元のサーバーに追加で高速な LAN ネットワークインターフェイスが必要です。

HDL-Z のための管理用端末について

このガイドでは、Windows またはその他の OS を実行する管理用端末からリモートデスクトップ接続を使用して HDL-Z のデスクトップに管理者（ローカルまたはドメインの Administrator アカウント、またはローカル Administrators グループのメンバー）としてリモート接続して作業することを前提としています。その方法および、その他の管理方法については、このガイドの前編『2. 運用管理編』および『3. 集中管理編』で説明しています。

共有リソースにアクセスするユーザーについて

このガイドでは、HDL-Z をワークグループ環境に設置し、Windows Server IoT 2019 for Storage に作成した一般ユーザーアカウント（Users ローカルグループのメンバー）の資格情報（<HDL-Z のサーバー名>¥<ユーザー名>とそのパスワード）を使用して SMB 共有や NFS 共有にアクセスすることを想定しています。

共有リソースにアクセスするためのローカルアカウントは、HDL-Z の［コンピューターの管理］スナップインまたは、「Windows Admin Center」の「ローカルユーザーとグループ」を使用して作成することができます。Windows Admin Center の導入については、このガイドの前編『3. 集中管理編』を参考にしてください。

HDL-Z を Active Directory ドメイン環境に設置し、ドメインのメンバーサーバーとして構成する場合は、Active Directory ドメインのユーザー／グループを使用した SMB 共有へのアクセス制御が可能です。

2 iSCSI ターゲットサーバーのセットアップとディスクアクセス

HDL-Z を iSCSI ターゲットサーバーとして構成し、データ用ボリューム D:に SAN の LUN（論理ユニット番号）となる iSCSI 仮想ディスクを配置して、iSCSI イニシエーターからの接続とディスクアクセスを実行できるようにするまでの一連の手順を説明します。

2.1 役割サービスのインストール

はじめに、Windows Server IoT 2019 for Storage で「iSCSI ターゲットサーバー」の役割サービスが有効になっていることを確認し、有効になっていない場合はインストールします。

1. ［サーバーマネージャー］の［ダッシュボード］を開き、［クイックスタート ②役割と機能の追加］をクリックして、［役割と機能の追加ウィザード］を開始します。［開始する前に］ページで［次へ］をクリックします。

2. ［インストールの種類の選択］ページで［役割ベースまたは機能ベースのインストール］を選択して［次へ］をクリックします。

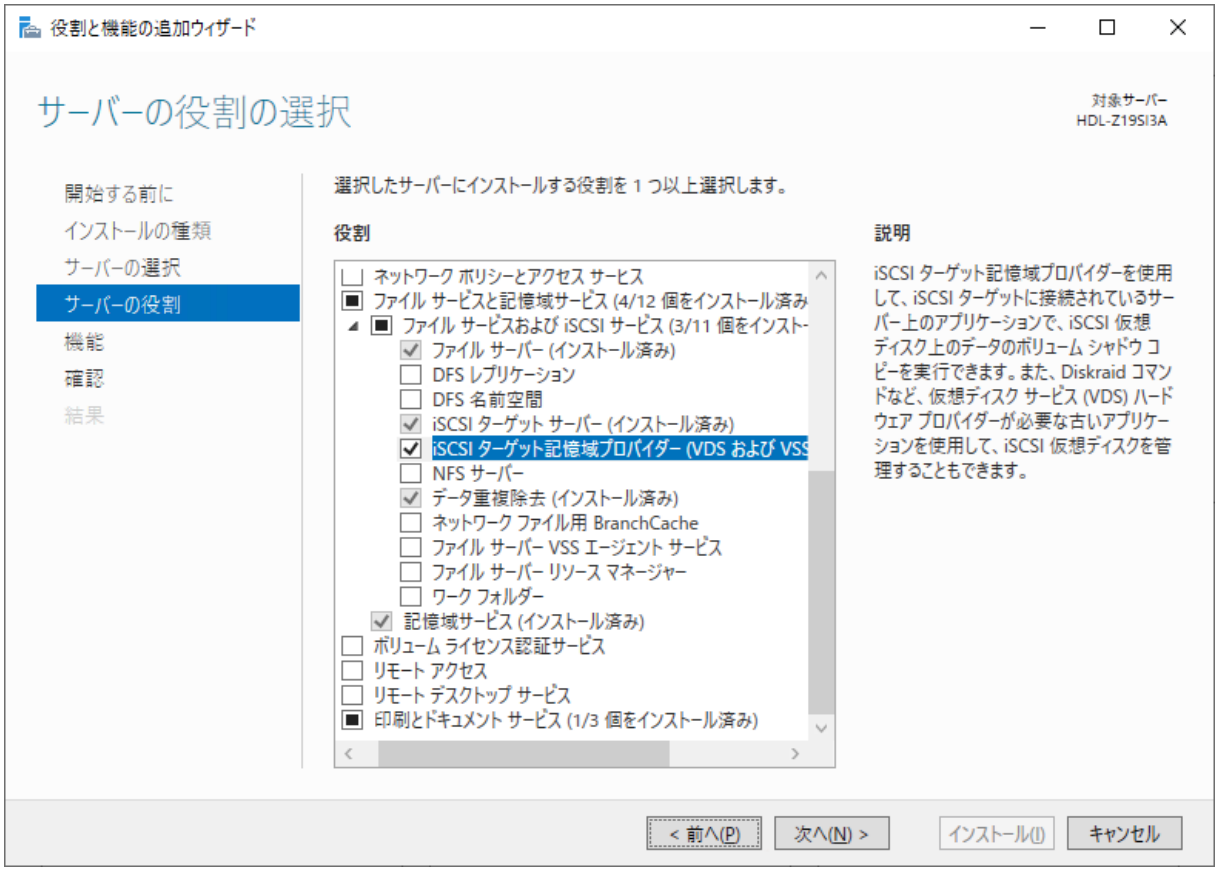
3. ［対象サーバーの選択］ページで HDL-Z を選択し、［次へ］をクリックします。

4. ［サーバーの役割の選択］ページで役割の一覧から［ファイルサービスと記憶域サービス］と［ファイルサービスおよび iSCSI サービス］を展開します。［iSCSI ターゲットサーバー（インストール済み）］となっている場合は、［キャンセル］をクリックしてウィザードを終了します。インストールされていない場合は、［iSCSI ターゲットサーバー］の役割サービスを選択し、［次へ］をクリックします。必要に応じて［iSCSI ターゲット記憶域プロバイダー（VDS および VSS）］の役割サービスも同時（または後で）選択してインストールします。

5. ［機能の選択］ページでは、そのまま［次へ］をクリックします。

6. ［インストールオプションの確認］ページで［インストール］をクリックし、役割サービスのインストールを完了させます。なお、役割サービスのインストールを完了するために、再起動は要求されません。

> 役割サービス［iSCSI ターゲット記憶域プロバイダー（VDS および VSS)］について
>
> iSCSI 仮想ディスク（LUN）を Windows Server OS や Windows デスクトップ OS のバックアップ用ディスクとして使用する場合は、［iSCSI ターゲット記憶域プロバイダー（VDS および VSS)］を追加で選択してください。この役割サービスは、iSCSI ターゲットサーバーに接続するサーバーのバックアップアプリケーションで iSCSI 仮想ディスク上のデータのボリュームシャドウコピーサービス（VSS）をサポートできるようにするものです。



画面：[iSCSI ターゲットサーバー]（必須）と［iSCSI ターゲット記憶域プロバイダー（VDS および VSS)］（オプション）をインストールする

2.2　iSCSI 仮想ディスクと iSCSI ターゲットの作成

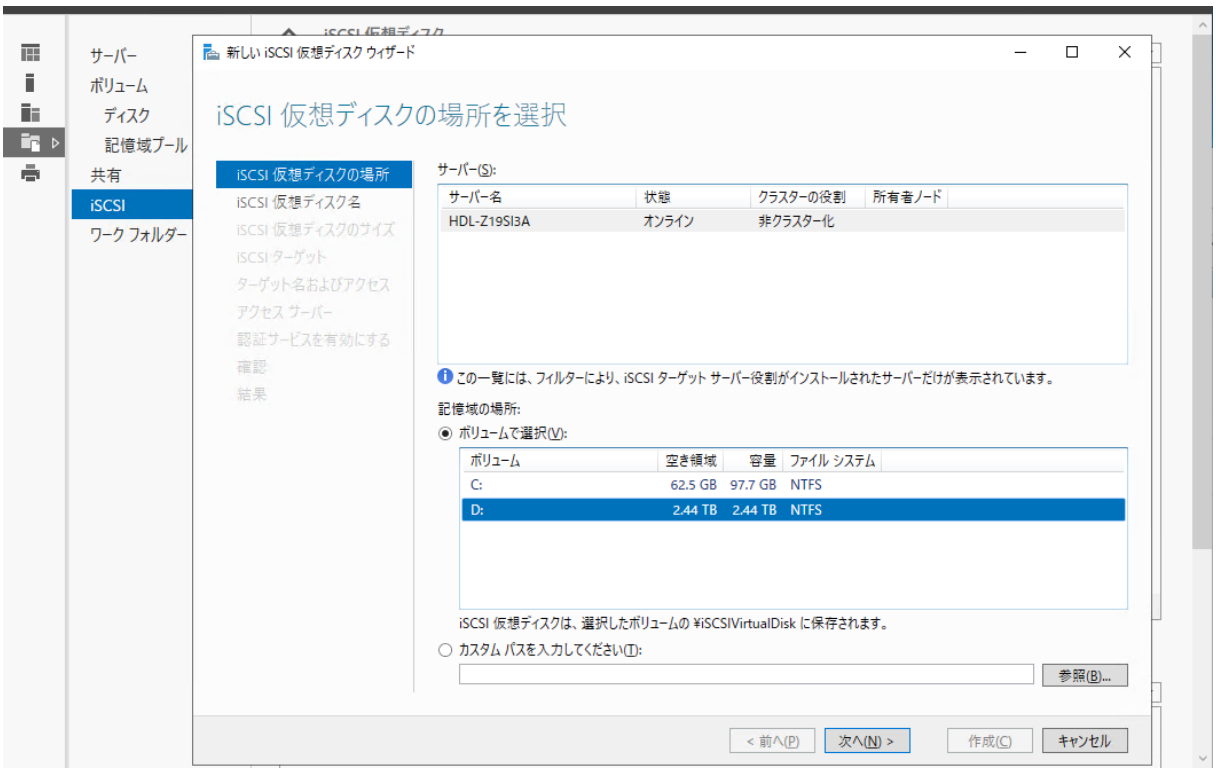
「iSCSI ターゲットサーバー」の役割サービスを有効化したら、次の手順で LUN となる iSCSI 仮想ディス

クを作成し、アクセス用の iSCSI ターゲットを作成して iSCSI イニシエーターに公開します。

> **iSCSI 仮想ディスクのファイル形式について**
>
> iSCSI 仮想ディスクは、Hyper-V の仮想マシン用の仮想ハードディスクと共通の VHDX 形式です。Hyper-V と同様に、容量固定、容量可変、および差分ディスク（親 VHDX に対する子 VHDX）をサポートします。割り当て可能なサイズは 8MB～64TB までで、最高のパフォーマンスを得るには容量固定タイプを使用します。ディスクを効率的に利用したい場合は、実際の使用とともにサイズが拡張される容量可変タイプを使用します。

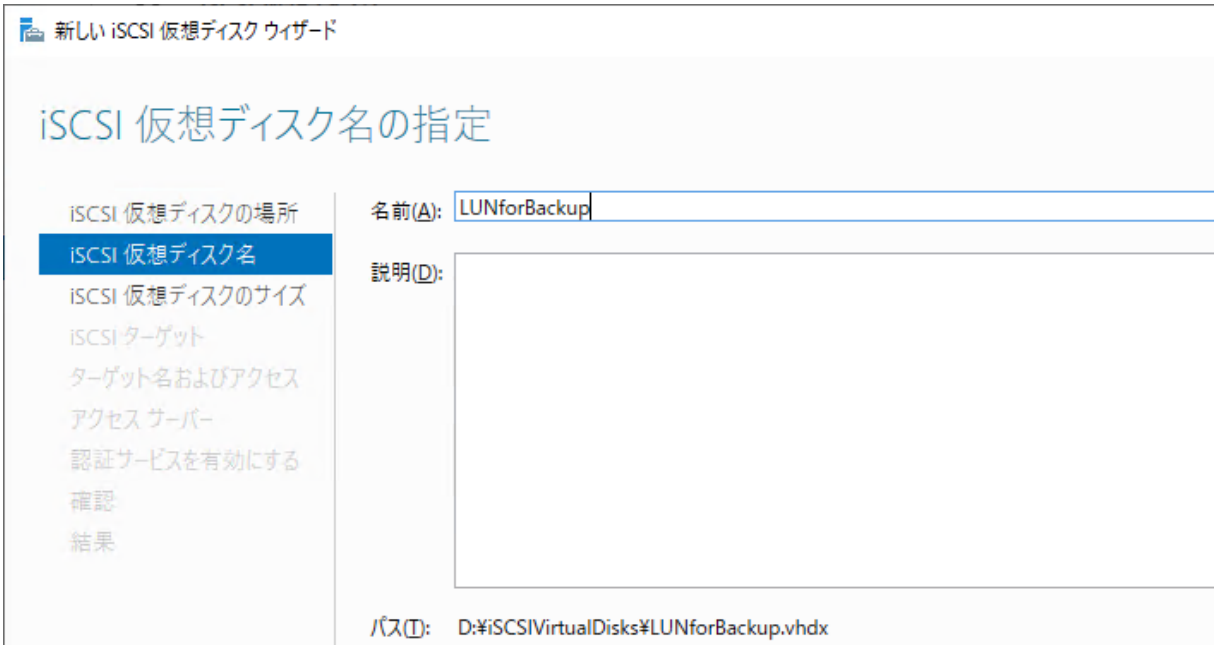
1. ［サーバーマネージャー］の［ファイルサービスと記憶域サービス］から［iSCSI］の場所を開き、［タスク▼］メニューから［新しい iSCSI 仮想ディスク］を選択して［新しい iSCSI 仮想ディスクウィザード］を開始します。

2. ウィザードの［iSCSI 仮想ディスクの場所を選択］ページで［ボリュームで選択］を選択し、［D:］ボリュームを選択して［次へ］をクリックします。この場合、「D:¥iSCSIVirtualDisks¥ファイル名.vhdx」に iSCSI 仮想ディスクが作成されます。または［カスタムパスを入力してください］を選択して、iSCSI 仮想ディスクの配置先のパスを指定します。



画面：iSCSI 仮想ディスクの作成を開始する

3. ［新しい iSCSI 仮想ディスク名の指定］ページで iSCSI 仮想ディスクのファイル名（拡張子を除く）を設定し、［次へ］をクリックします。



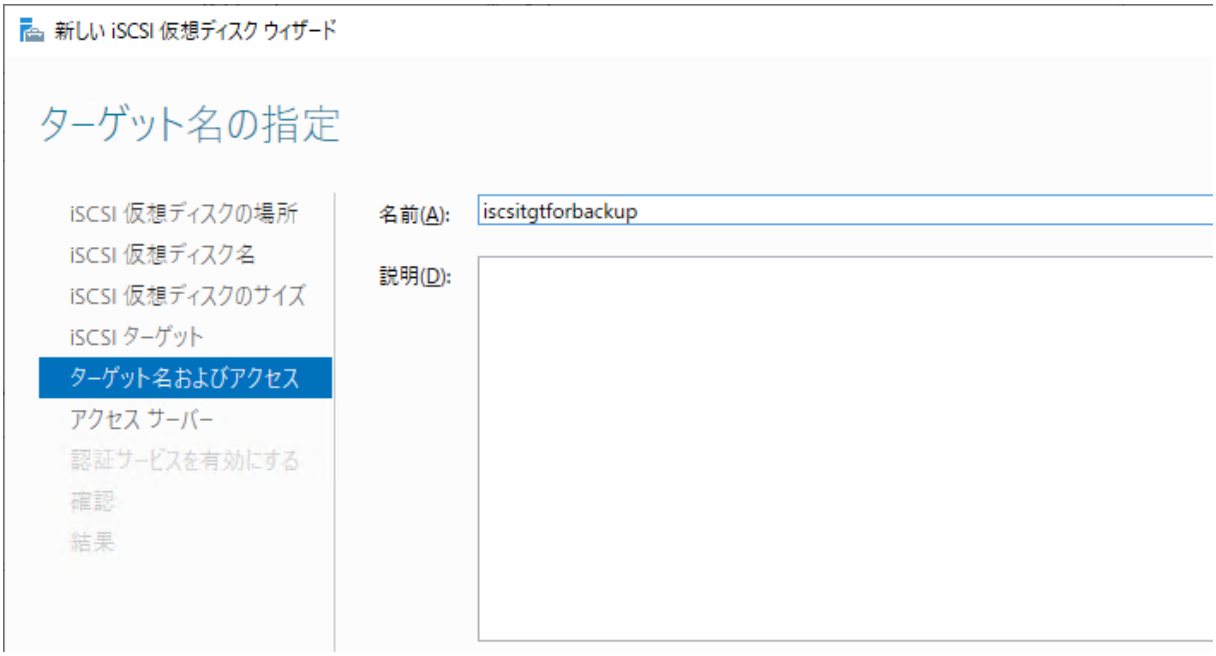
画面：VHDX ファイルのファイル名を指定する

4. ［iSCSI 仮想ディスクのサイズを指定］ページで、iSCSI 仮想ディスクに割り当てるサイズと VHDX の種類を指定します。容量可変と容量固定のどちらの種類を選択する場合でも、配置先ボリュームの現在の空き領域より小さな値を設定してください。

画面：VHDX ファイルの割り当てサイズと種類を指定する

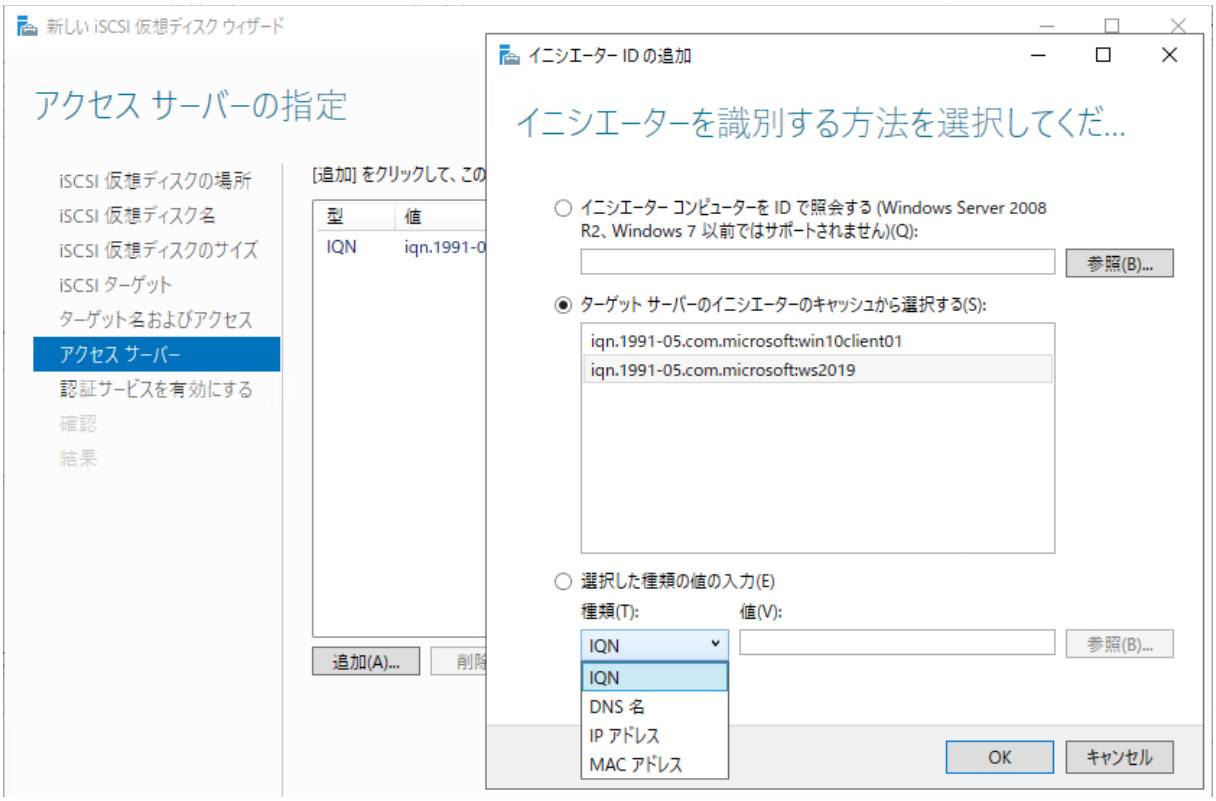
5. ［iSCSI ターゲットの割り当て］ページで［新しい iSCSI ターゲット］を選択し、［次へ］をクリックします。既に作成済みの iSCSI ターゲットが存在する場合は、選択して指定することもできます。

6. ［新しい iSCSI ターゲット］を選択した場合は、［ターゲット名の指定］ページで iSCSI ターゲットに付ける分かりやすい名前を入力して［次へ］をクリックします。



画面：iSCSI ターゲットの名前を入力する

7. ［アクセス サーバーの指定］ページで［追加］をクリックし、この iSCSI 仮想ディスクにアクセスすることを許可する iSCSI イニシエーターを指定します。



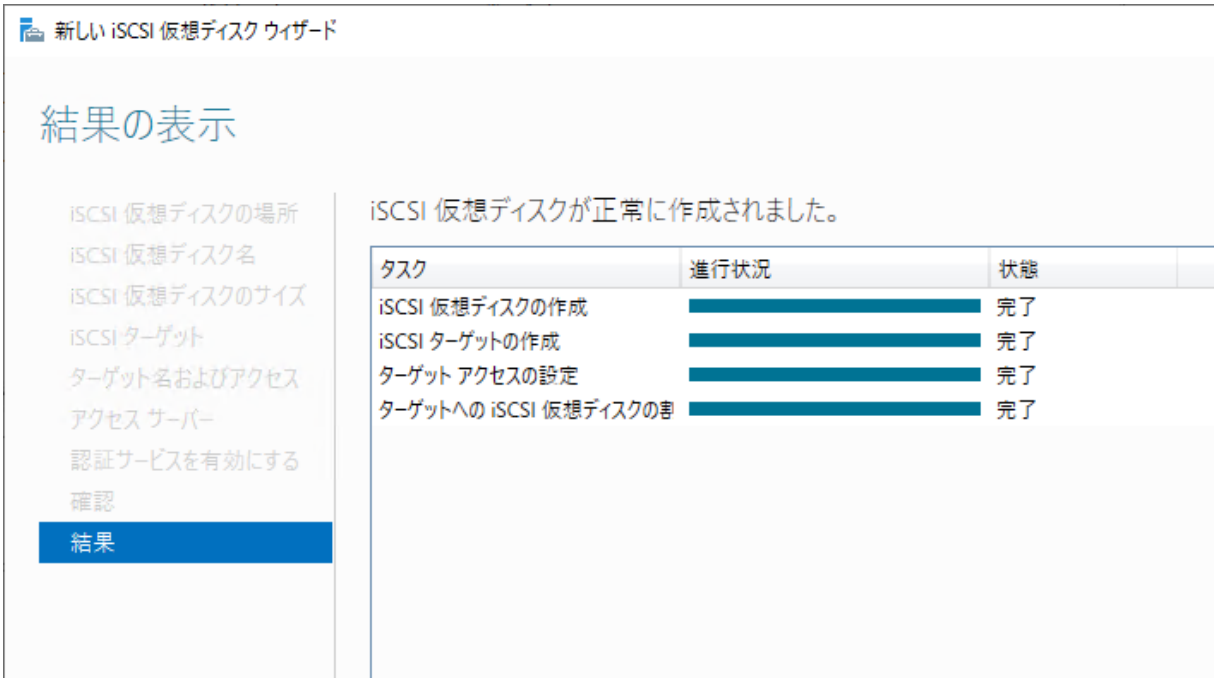
画面：この iSCSI ターゲットへの接続を許可するクライアントの IQN を指定する

Active Directory 環境がある場合、コンピューター名や FQDN から照会して IQN（iSCSI Qualified Name、iSCSI 修飾名）を設定することができます（ただし、Windows Server 2012 および Windows 8 以降）。この iSCSI 仮想ディスクに接続することになる iSCSI イニシエーターから接続を試みるこ

とで（iSCSI ターゲットの作成前なので失敗します）、iSCSI ターゲットに IQN の情報をキャッシュとして保存されます。このキャッシュから IQN を選択して設定するのが簡単です。IQN の代わりに、DNS 名や IP アドレス、MAC アドレスで設定することも可能です。それには［選択した種類の値の入力］を選択して、手動で入力します。

8. ［認証を有効にする］ページでオプションで追加の認証を要求するように構成します。アクセスサーバーを IQN で指定している場合、ネットワーク上の他のサーバーからは接続できないため、通常、追加の認証は必要ありません。

9. ［設定内容の確認］で［作成］をクリックします。



画面：iSCSI 仮想ディスクと iSCSI ターゲットを作成してサーバー側の準備は完了

2.3　Windows 標準の iSCSI イニシエーターからの接続

Windows および Windows Server は、iSCSI イニシエーターの機能を標準搭載しており、「iSCSI イニシエーター」（IscsiCpl.exe）ツールまたは Windows PowerShell の iSCSI モジュールのコマンドレット、または「iscsicli.exe」コマンドを使用してセットアップすることができます（iscsicli.exe については、このガイドでは説明しません）。

その他のプラットフォームについても、標準で、または iSCSI イニシエーターソフトウェアを追加することで iSCSI ターゲットサーバーに接続し、LUN をマウントすることができます。

「iSCSI イニシエーター」（IscsiCpl.exe）ツールを使用した接続

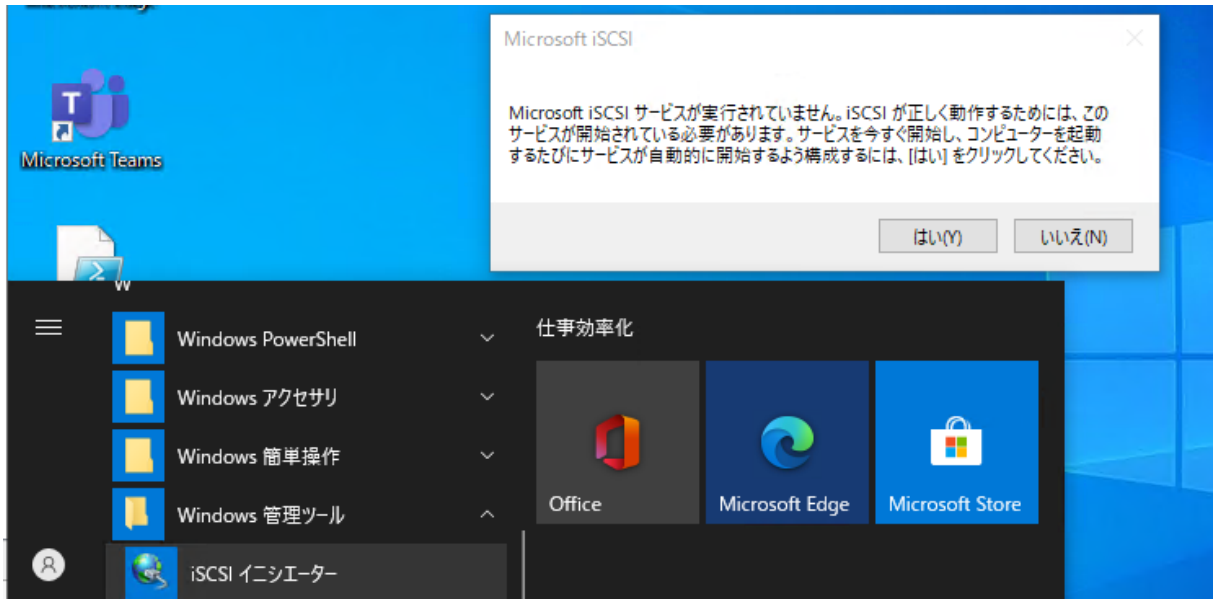
現在、サポートされているバージョンの Windows および Windows Server には、iSCSI イニシエーターの機能が標準搭載されており、Windows 管理ツールである「iSCSI イニシエーター」を使用して、GUI でセ

ットアップすることができます。このツールは Windows Server 2012 以降の Server Core インストール環境でも標準で使用できます。

1. Windows 10 の［スタート］メニューを開き、［Windows 管理ツール］から［iSCSI イニシエーター］を選択して開きます。またはコマンドプロンプトや「ファイル名を指定して実行」から「iscsicpl.exe」を実行して開始します。

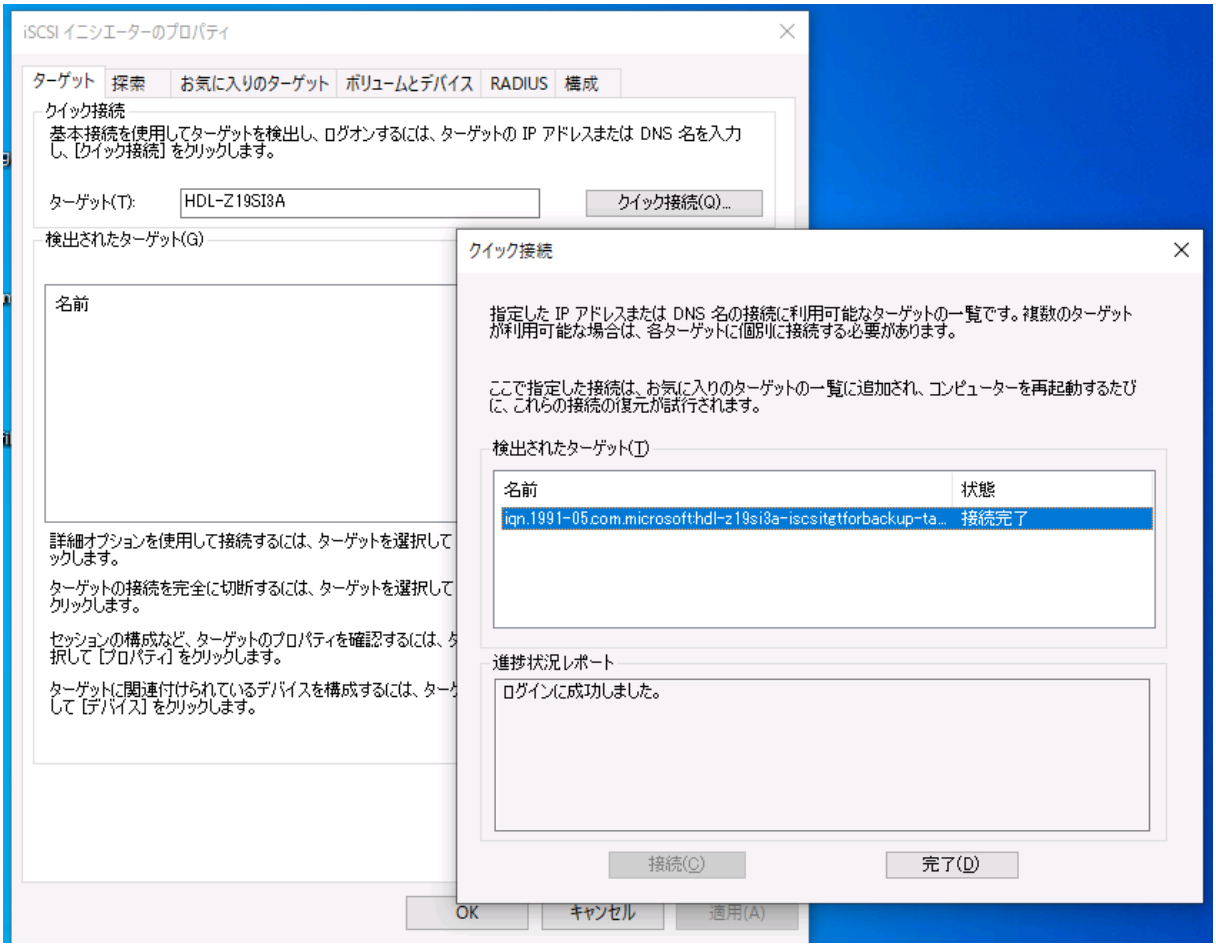
2. ［iSCSI イニシエーター］を初めて起動した場合は、次のようなメッセージが表示されるので、［はい］を選択して続行します。

   “Microsoft iSCSI サービスが実行されていません。iSCSI が正しく動作するためには、このサービスが開始されている必要があります。サービスを今すぐ開始し、コンピューターを起動するたびにサービスが自動的に開始するように構成するには、［はい］をクリックしてください。“



画面：[はい] をクリックする

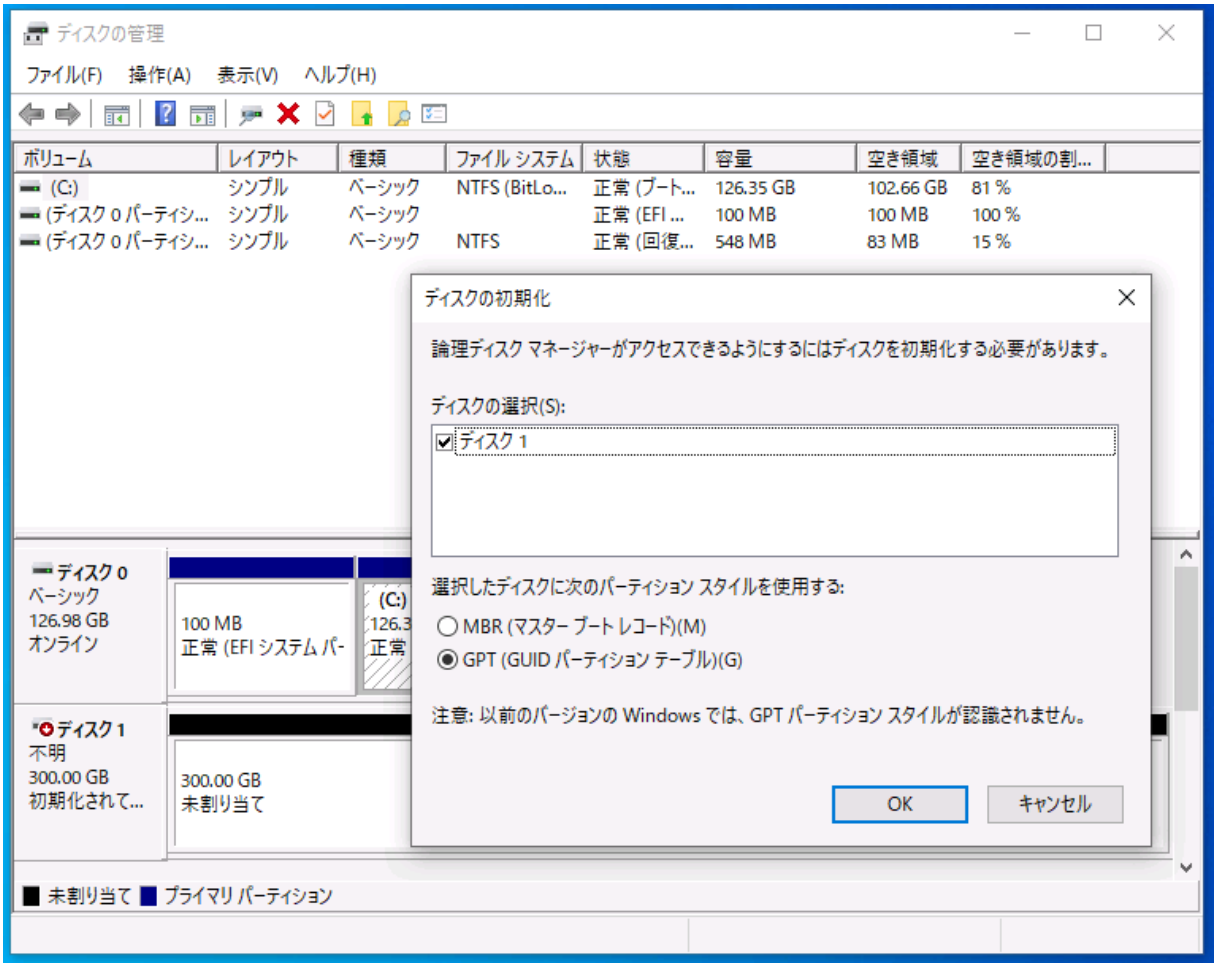
3. ［iSCSI イニシエーターのプロパティ］が表示されるので、[ターゲット] タブの [ターゲット] に iSCSI ターゲットサーバーのコンピューター名または FQDN または IP アドレスを入力し、[クイック接続] をクリックします。追加の認証を要求するように iSCSI ターゲットを構成した場合は、[クイック接続] では接続に失敗するため、[接続] をクリックして詳細オプションを指定して接続してください。



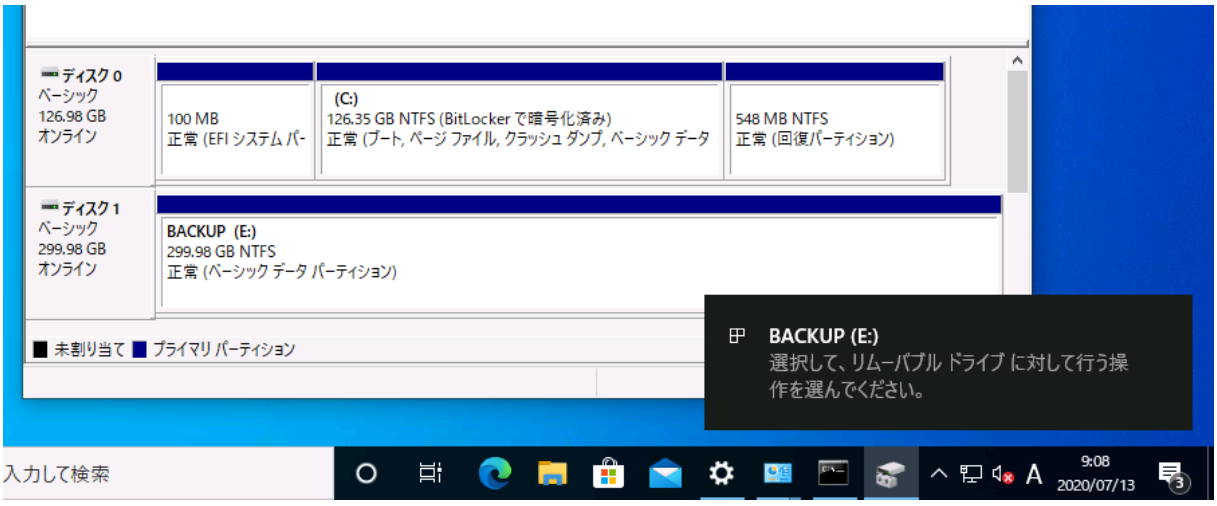
画面：iSCSI ターゲットサーバーのコンピューター名または IP アドレスを入力し、［クイック接続］をクリックして接続する

4. 接続が完了したら［iSCSI イニシエーターのプロパティ］を閉じます。これで永続的な接続がセットアップされました。永続的な接続は、コンピューターを再起動するたびに再接続されます。

5. ［ディスクの管理］（Diskmgmt.msc）を開きます。接続した iSCSI 仮想ディスクはローカルの固定ディスクとまったく同じように扱えます。未使用の iSCSI 仮想ディスクの場合はディスクを初期化し（GPT または MBR ディスクとして）、ディスク上に新しいボリュームを作成して、NTFS または ReFS 形式でフォーマットし、ローカルディスクとしてマウントします。



画面：マウントした iSCSI 仮想ディスクはローカルディスク（リムーバブルディスク）とまったく同じように扱える



画面：NTFS または ReFS 形式でフォーマットして、アプリケーションやバックアップ用のディスクとして使用する

Windows PowerShell によるコマンドラインからの接続

Windows や Windows Server では、Windows PowerShell の iSCSI モジュール（標準搭載）のコマンドレットを使用して iSCSI ターゲットサーバーへの接続をセットアップすることもできます。

永続的な接続をセットアップするには、Windows PowerShell を管理者として開き、次のコマンドラインを実行します。最初の 2 つのコマンドラインでは、「Microsoft iSCSI Initiator Service」（サービス名：MSiSCSI）のスタートアップの種類の変更とサービスの開始を行っています。

```
PS C:¥> Set-Service -Name MSiSCSI -StartupType Automatic ↲
PS C:¥> Start-Service -name MSiSCSI ↲
PS C:¥> New-IscsiTargetPortal -TargetPortalAddress <iSCSI ターゲットサーバーのコンピューター名または FQDN または IP アドレス> ↲
PS C:¥> Get-IscsiTarget ↲ （iSCSI ターゲットの NodeAddress の IQN を確認）
PS C:¥> Connect-IscsiTarget -NodeAddress <iSCSI ターゲットの IQN> -IsPersistent $true ↲
```

iSCSI ターゲットとの接続を切断し、完全に削除するには、次のコマンドラインを実行します。

```
PS C:¥> Disconnect-IscsiTarget -NodeAddress <iSCSI ターゲットの IQN> ↲
PS C:¥> Remove-IscsiTargetPortal -TargetPortalAddress <iSCSI ターゲットサーバーのコンピューター名または FQDN または IP アドレス> ↲
```

3　NFS 共有のセットアップとファイルアクセス

HDL-Z を NFS サーバーのサポートを追加し、NFS 共有を作成して NFS クライアントからのアクセスを可能にするまでの一連の手順を説明します。

3.1　役割サービスのインストール

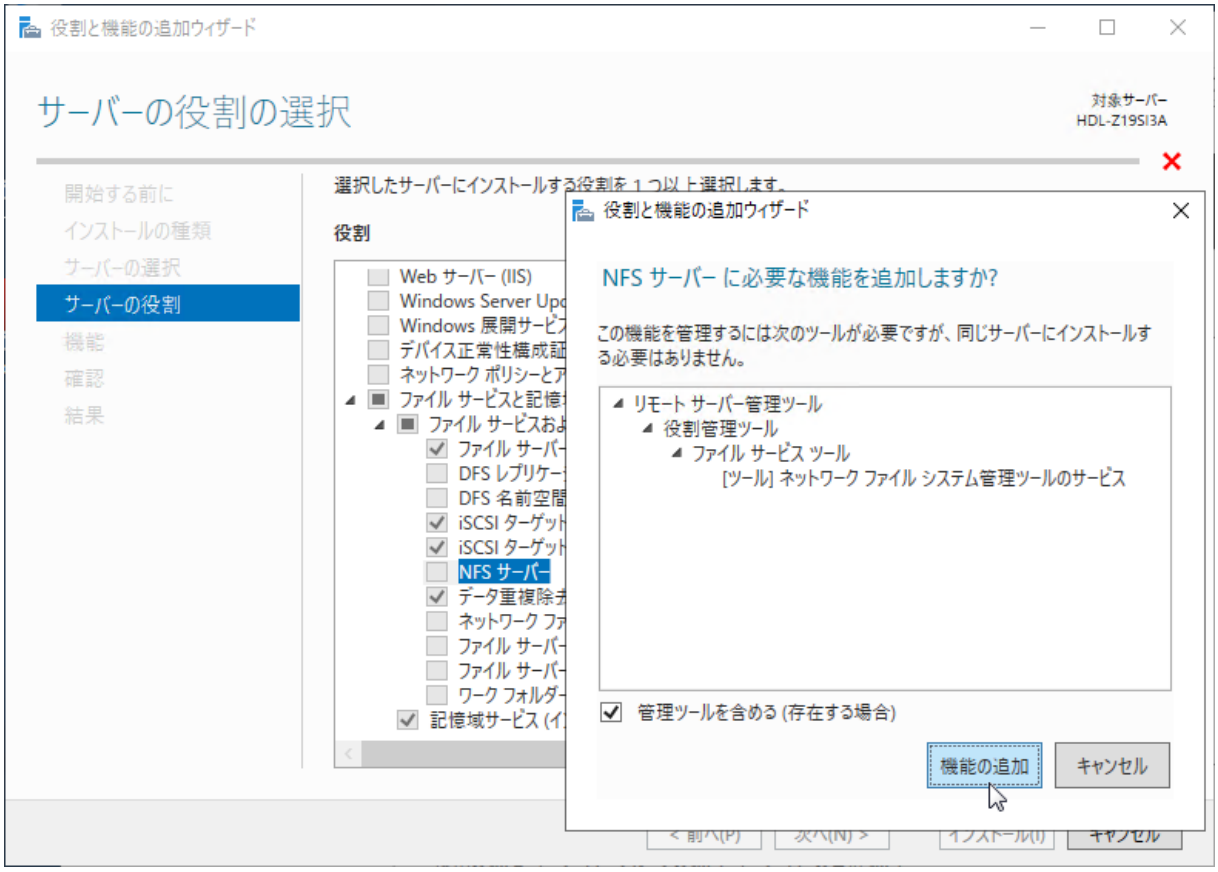
はじめに、Windows Server IoT 2019 for Storage で「NFS サーバー」の役割サービスが有効になっていることを確認し、有効になっていない場合はインストールします。

1. ［サーバーマネージャー］の［ダッシュボード］を開き、［クイックスタート ②役割と機能の追加］をクリックして、［役割と機能の追加ウィザード］を開始します。［開始する前に］ページで［次へ］をクリックします。

2. ［インストールの種類の選択］ページで［役割ベースまたは機能ベースのインストール］を選択して［次へ］をクリックします。

3. ［対象サーバーの選択］ページで HDL-Z を選択し、［次へ］をクリックします。

4. ［サーバーの役割の選択］ページで役割の一覧から［ファイルサービスと記憶域サービス］と［ファイルサービスおよび iSCSI サービス］を展開します。［NFS サーバー（インストール済み）］となっている場合は、［キャンセル］をクリックしてウィザードを終了します。インストールされていない場合は、［NFS サーバー］の役割サービスを選択ます。「NFS サーバーに必要な機能を追加しますか？」と問われるので［機能を追加］をクリックし、［サーバーの役割の選択］ページで［次へ］をクリックします。



画面：「NFS サーバー」の役割サービスと関連する機能を追加する

5. ［機能の選択］ページでは、そのまま［次へ］をクリックします。

6. ［インストールオプションの確認］ページで［インストール］をクリックし、役割サービスのインストールを完了させます。なお、役割サービスのインストールを完了するために、再起動は要求されません。

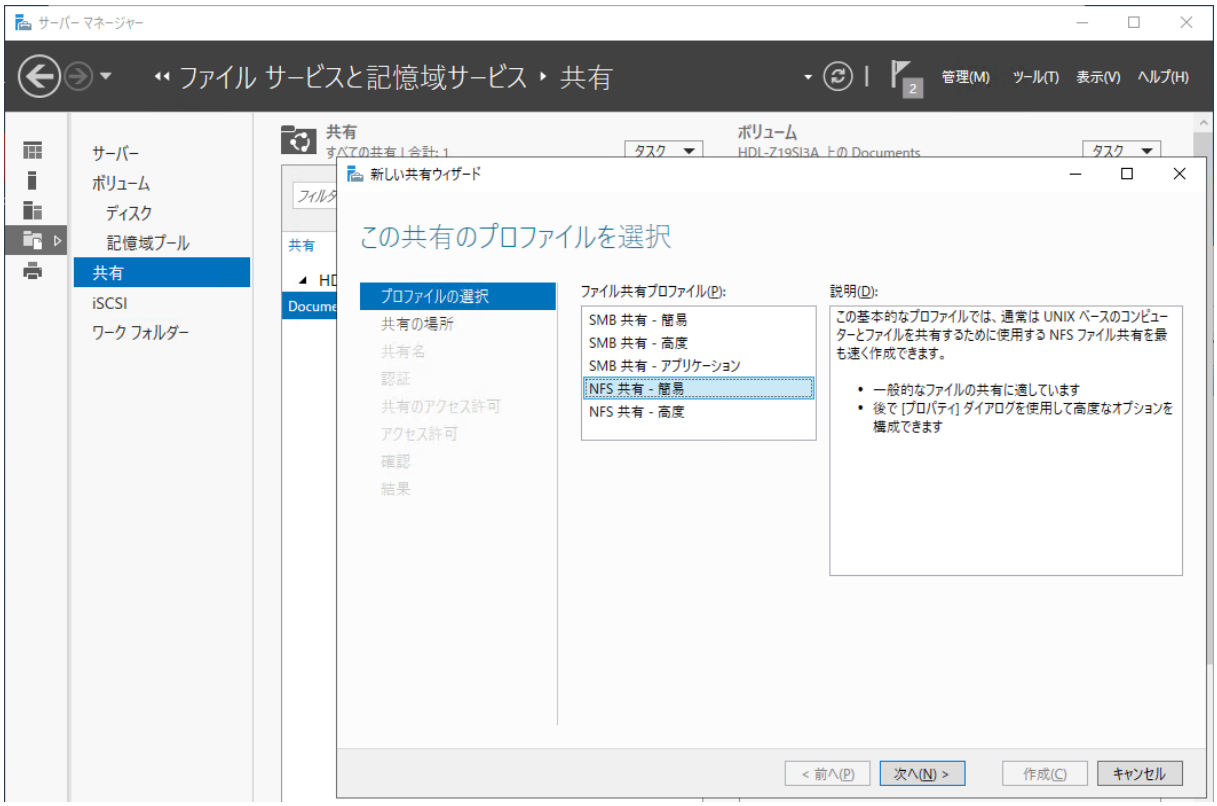
3.2 NFS 共有の作成と公開

「NFS サーバー」の役割サービスを有効化したら、次の手順で NFS 共有を作成し NFS クライアントに公開します。ここでは、読み取り/書き込みのアクセスが可能な共有用のディレクトリを新規に作成する手順で

説明します。

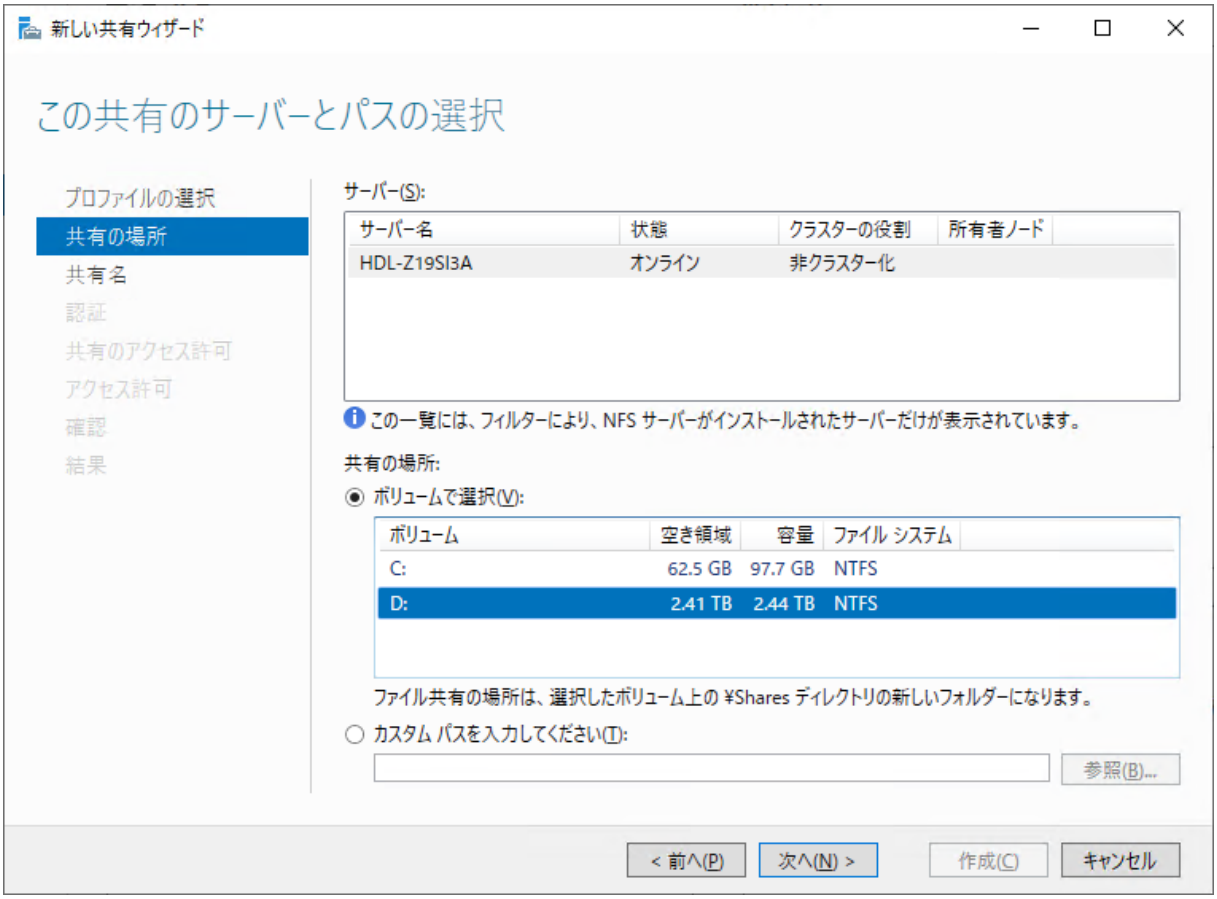
1. ［サーバーマネージャー］の［ファイルサービスと記憶域サービス］から［共有］の場所を開き、［共有］一覧の［タスク▼］メニューから［新しい共有］を選択して［新しい共有ウィザード］を開始します。

2. ウィザードの［この共有のプロファイルを選択］ページでファイル共有プロトコルとして［NFS 共有 – 簡易］を選択し、［次へ］をクリックします。



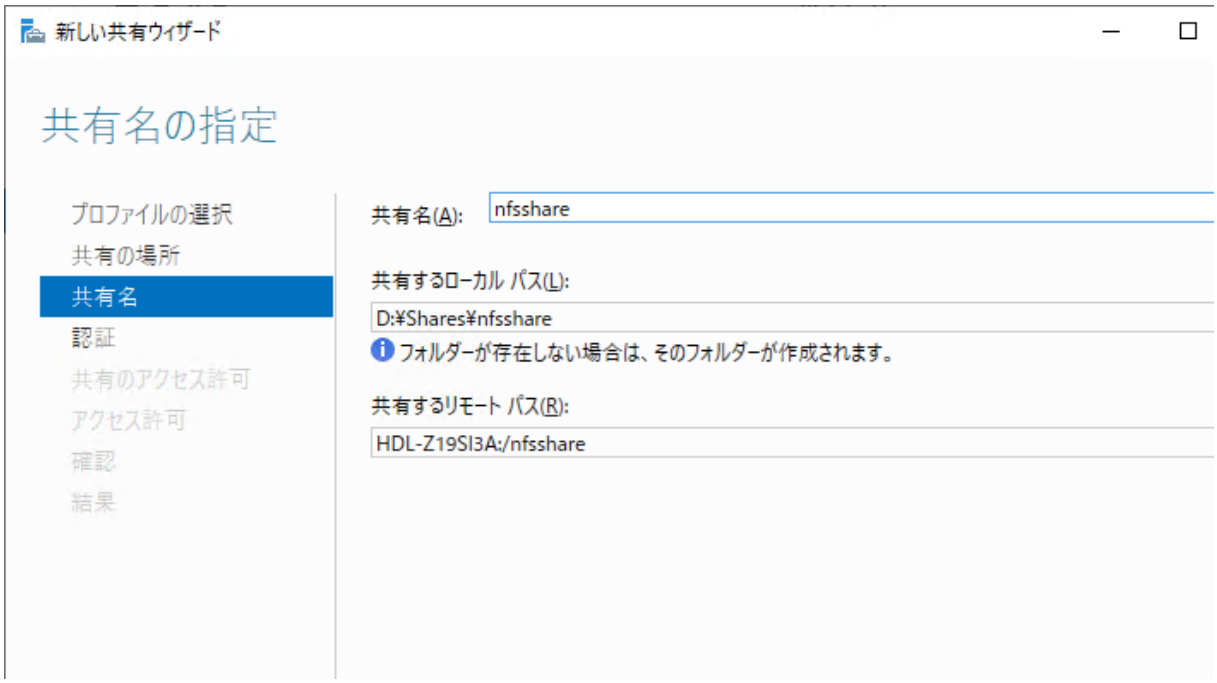
画面：［NFS 共有 – 管理］を選択して NFS 共有を作成する

3. ［この共有のサーバーとパスの選択］ページで［ボリュームで選択］を選択し、［D:］ボリュームを選択して［次へ］をクリックします。この場合、「D:¥Shares¥ディレクトリ名」が作成され、NFS による共有が構成されます。または［カスタムパスを入力してください］を選択して、共有するディレクトリのパスを指定します。既存の SMB 共有と同じディレクトリに NFS 共有設定を行う場合はカスタムパスで指定します。



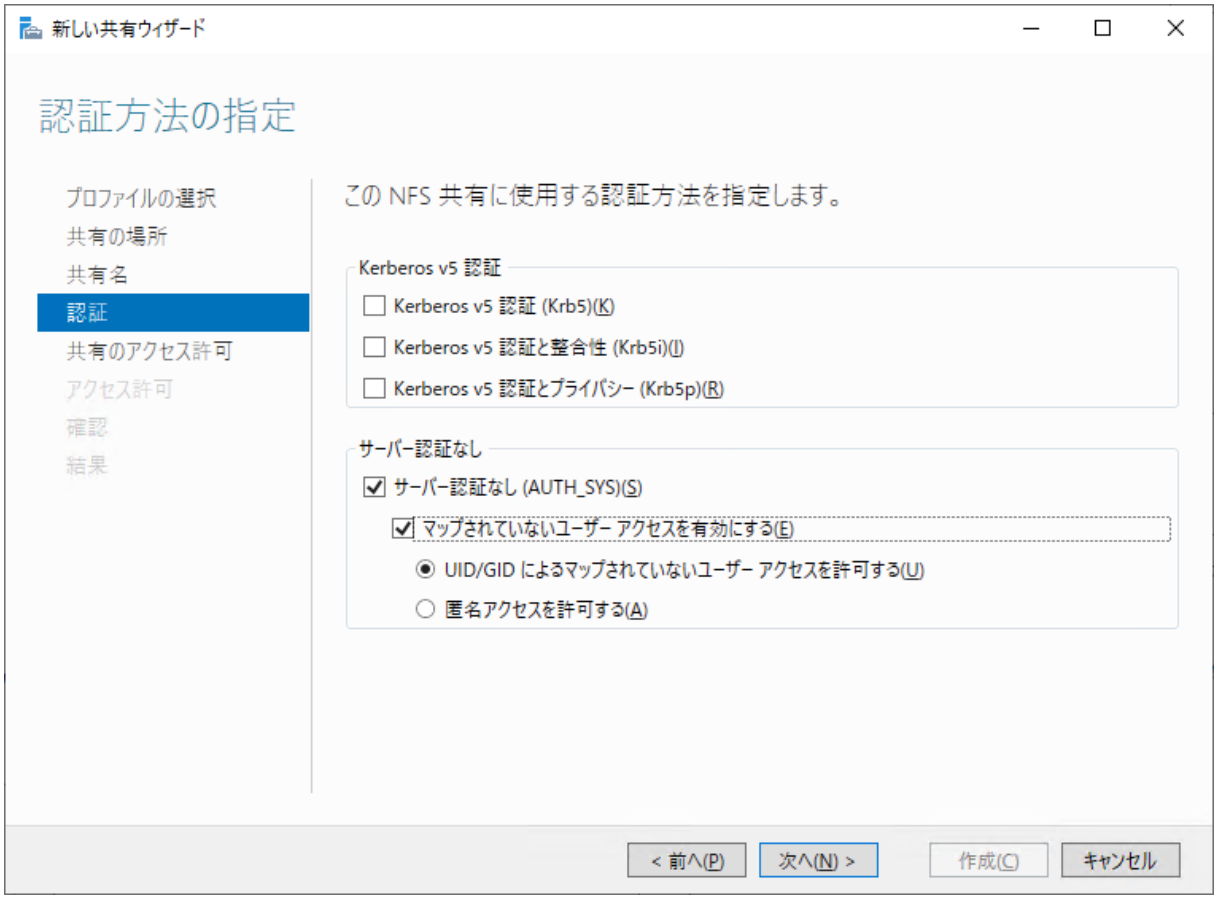
画面：新規にディレクトリを作成する場合はボリュームを選択する。既存の SMB 共有を NFS でも共有する場合はカスタムパスに既存のディレクトリパスを指定する

4. ［共有名の指定］ページで共有名を入力または確認し、リモートパスを確認して［次へ］をクリックします。



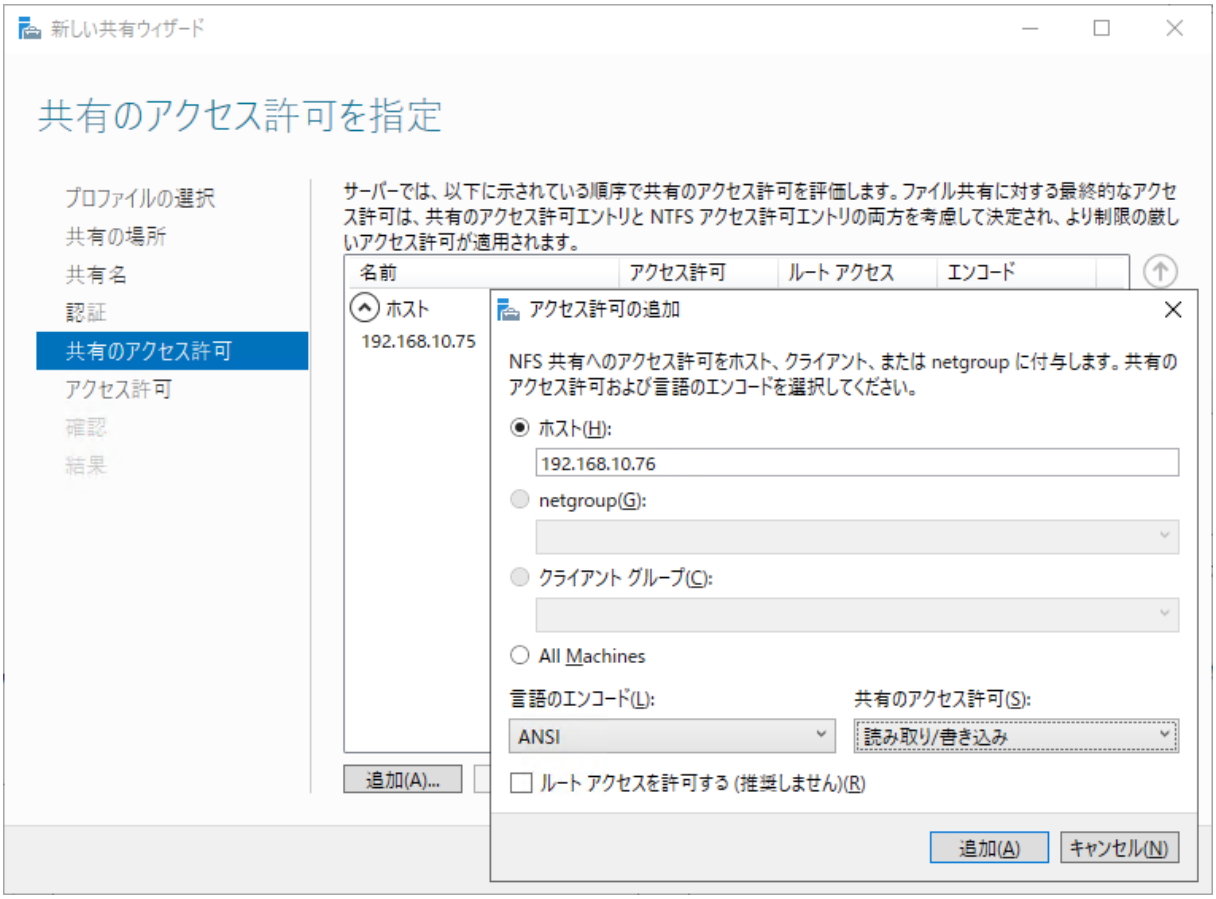
画面：共有名を入力し、リモートパスを確認する

5. ［認証方法の指定］ページで認証方法を指定します。Active Directory ドメインや Active Directory ライトウェイトディレクトリサービスの環境があり利用できる場合は［Kerberos v5 認証］の 3 つのオプションをチェックします。Kerberos v5 認証の利用環境がない場合は、［サーバー認証なし（AUTH_SYS）］をチェックし、さらに［マップされていないユーザーアクセスを有効にする］と［UID/GID によるマップされていないユーザーアクセスを許可する］の 2 つをチェックして［次へ］をクリックします。なお、Kerberos v5 認証を使用せず、かつ［マップされていないユーザーアクセスを有効にする］をオフにする方法については後述します。



画面：NFS クライアントの認証方法を選択する

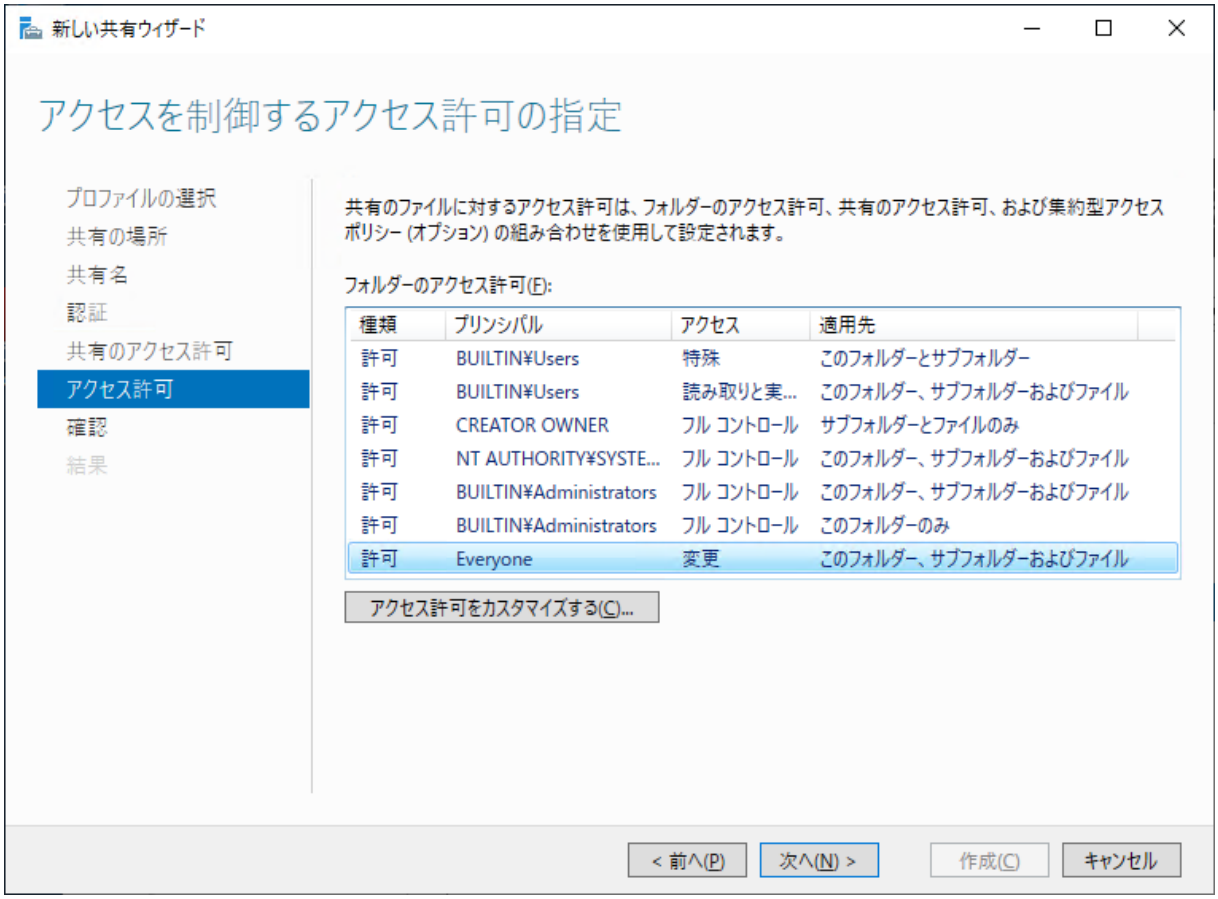
6. ［共有のアクセス許可を指定］ページで［追加］をクリックし、この NFS 共有へのアクセスを許可するクライアントのホスト名や IP アドレスを指定し、共有のアクセス許可で［読み取り/書き込み］を選択して［追加］をクリックします。複数の NFS クライアントからアクセスできるようにするには、NFS クライアントごとに設定を追加してください。なお、NFS 共有の作成後、［All Machines：アクセスなし］のエントリが自動追加されます。



画面：この NFS 共有にアクセスする NFS クライアントごとにアクセス許可を設定する

> ⚠ 共有のアクセス許可は個別に
>
> NFS クライアントは NFS サーバーに個別にユーザー認証することなしにファイルリソースにアクセスすることができます。[共有のアクセス許可] の設定は、ユーザー認証の代わりになるアクセス制御の手段であり、不必要に広範囲なアクセス許可を行わないようにしてください。少なくとも、[ルートアクセスを許可する] (root 権限でのアクセス) と [All Machines] への [アクセスなし] 以外の許可設定は行わないことを強く推奨します。また、[認証方法の指定] ページでの [匿名アクセスを許可する] の設定も推奨されません。

7. [アクセススを制御するアクセス許可の指定] ページでは、共有するディレクトリパスの NTFS アクセス許可を調整します。ここでは [アクセス許可をカスタマイズする...] をクリックして、既定の設定に加えて、[Everyone：変更] のアクセス許可を追加してください。後述するユーザーのマッピングを構成すると、[Everyone：変更] のアクセス許可を削除できます。



画面：共有する NTFS アクセス許可を調整する

8. ［設定内容の確認］ページで［作成］をクリックします。

Linux ユーザーと Windows ユーザーの簡易マッピングについて

Active Directory ドメインや Active Directory ライトウェイトディレクトリサービス（つまり、Kerberos v5 認証）を利用できない場合は、Linux 側の/etc/passwd と/etc/group を使用した簡易的なマッピングが可能です。簡易的なマッピングを行うと、NFS クライアントで作成したファイルの所有者が、Windows 側ではマッピングした Windows ユーザーに紐づけられます。また、簡易マッピングを構成した場合、NFS 共有の［認証方法の指定］ページでの［サーバー認証なし（AUTH_SYS）］で［マップされていないユーザーアクセスを有効にする］をオフにし、ディレクトリの NTFS アクセス許可から［Everyone:変更］のエントリを削除することが可能です。

簡易的なマッピングを行うには、NFS クライアントである Linux コンピューターの/etc/passwd と/etc/group を Windows Server 側にコピーして編集し、NFS サーバーである Windows Server の C:¥Windows¥System32¥drivers¥etc に保存します。マッピングは NFS クライアント側で新たに作成されたファイルに対して有効になります。

次の例は、Linux の root ユーザーとグループを Windows の **Administrator** ローカルアカウントと **Administrators** ローカルグループに、Linux の **lxuser01** と **lxuser02**（UID が異なれば別の Linux マシンのユーザーでもよい）を、それぞれ Windows Server のローカルアカウント **winuser01** と **winuser02** にマッピングする例です。使用しない（あるいは用途不明の既定の）ユーザーやグループのエントリは削除

してしまって構いません。なお、設定を反映するためには、サーバー側の OS の再起動が必要です。

変更前の Linux 側の/etc/password

root:x:0:0:root:/root:/bin/bash **lxuser01**:x:1000:1000:lxuser01,,,:/home/lxuser01:/bin/bash **lxuser02**:x:1001:1001:lxuser02,,,:/home/lxuser02:/bin/bash

変更前の Linux 側の/etc/group

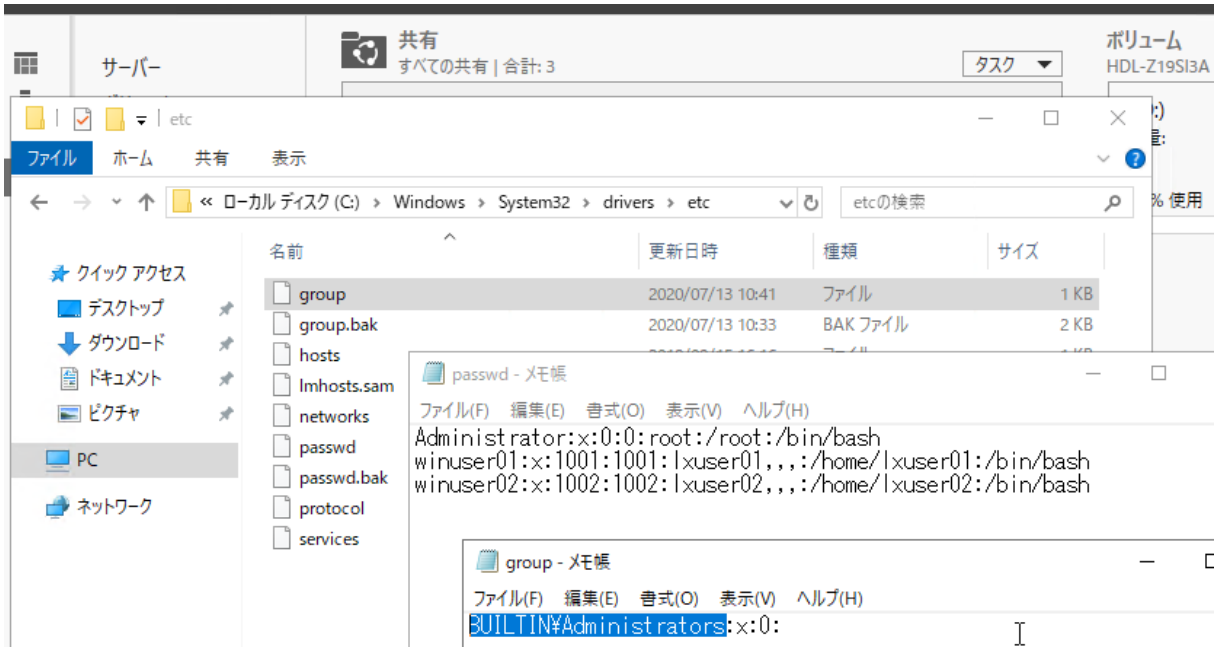
root:x:0:root

コピーおよび変更後の Windows Server 側の C:¥Windows¥System32¥drivers¥etc¥passwd

Administrator:x:0:0:root:/root:/bin/bash **winuser01**:x:1000:1000:lxuser01,,,:/home/lxuser01:/bin/bash **winuser02**:x:1001:1001:lxuser02,,,:/home/lxuser02:/bin/bash

コピーおよび変更後の Windows Server 側の C:¥Windows¥System32¥drivers¥etc¥passwd

BUILTIN¥Administrators:x:0:root



画面：Linux からコピーした passwd と group を編集して簡易マッピングを作成する。設定を反映させるために再起動が必要

詳しくは、以下の Windows プラットフォームサポートチームのアーカイブされたブログ記事を参考にしてください。

Windows Server 2012 以降の NFS 利用時のユーザーマッピングについて
https://docs.microsoft.com/ja-jp/archive/blogs/askcorejp/windows-server-2012-nfs

Active Directory ドメイン環境における Kerberos 認証と ID マッピングについては、FileCAB – Team のアーカイブされたブログ記事が参考になります。

以下の NFS Identity Mapping in Windows Server 2012
https://techcommunity.microsoft.com/t5/storage-at-microsoft/nfs-identity-mapping-in-windows-server-2012/ba-p/424602

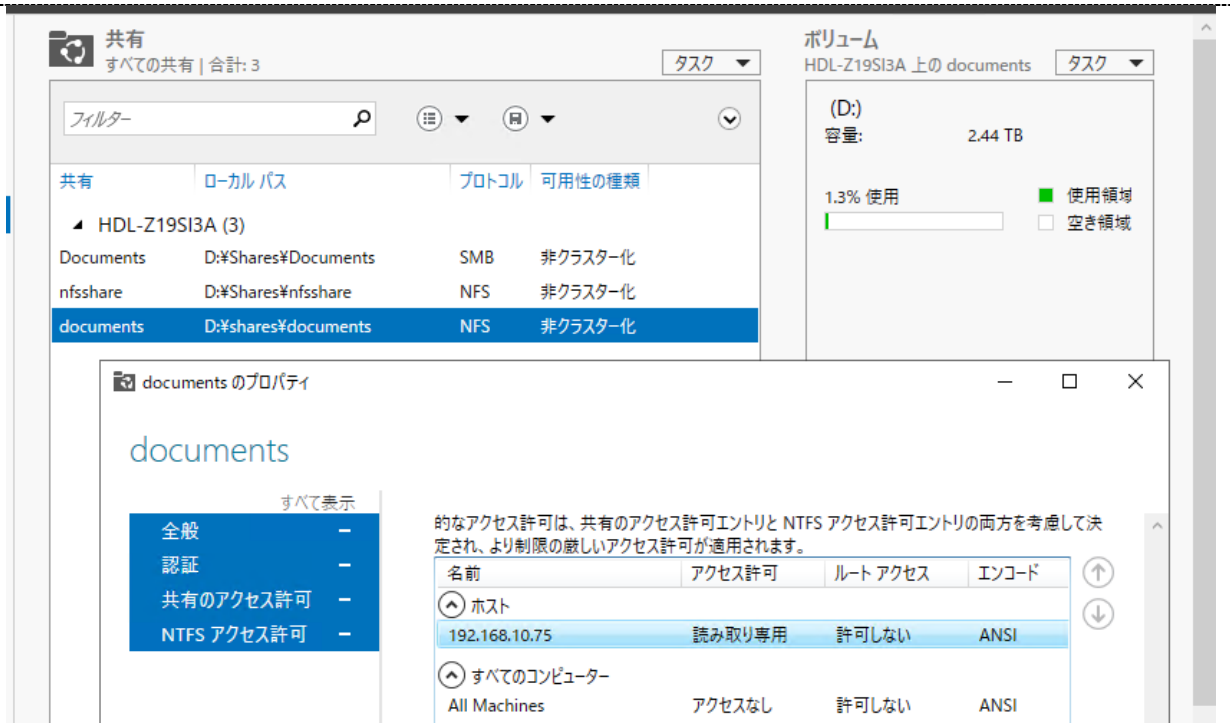
同じディレクトリを SMB と NFS で共有する際の注意点

Windows Server では、既に SMB 共有として共有済みのディレクトリで NFS 共有を有効にし、同じ共有フォルダーへのアクセスを異なるプロトコルで混在させることが可能です。ただし、Windows と UNIX/Linux のファイルシステムの違いやアクセス制御の違い、日本語のエンコードの違いに注意してください。

例えば、Windows は大文字と小文字を区別しませんが、UNIX/Linux は大文字と小文字を区別します。NFS クライアントは Windows が提供する NFS 共有において通常、大文字と小文字を区別することはありませんが、操作によっては大文字と小文字が区別され、意図しない結果が返ってくる場合があります（例：ファイル名の部分一致による検索結果など）。

また、Windows では **CON**、**AUX**、**PRN**、**NUL** といった名前は予約されており、これらのファイル名でファイルを作成することはできませんが、NFS クライアントからは作成可能です。無効な名前で作成されたファイルは、Windows 側では削除などの操作が制限されます。さらにアプリケーション（Nautilus など）によっては、エンコードの違いによりファイル名やディレクトリ名の日本語が文字化けします。

読み書き可能な SMB 共有と NFS 共有は可能な限り、別々のディレクトリで提供することをお勧めします。例えば、以下のように SMB 共有は読み取りアクセスのみで NFS 共有として公開し、書き込み可能な NFS 共有とは分けるとよいでしょう。



画面：SMB 共有は読み取りのみで NFS 共有としてもアクセスできるようにし、書き込み可能な NFS 共有と分けることを推奨

3.3 NFS クライアントからのアクセス

NFS サーバー側で NFS 共有へのアクセスを許可した NFS クライアントでの操作について、Linux を例に簡単に説明します。

Linux の標準的な NFS クライアント

Linux では、mount コマンドを使用して NFS 共有をファイルシステムにマウントすることが可能です。NFS は UNIX/Linux で古くから使用されてきたファイル共有プロトコルですが、最近の Linux ディストリビューションでは NFS クライアントのサポートが標準でインストールされていない場合があります。次のコマンドラインを実行して、/sbin/mount.nfs ファイルが存在すれば、NFS クライアントは既にサポートされています。

```
$ ls /sbin/mount.nfs ↵
```

/sbin/mount.nfs ファイルが存在しない場合は、各 Linux ディストリビューションの標準のリポジトリから追加でインストールしてください。

Ubuntu や Debian の場合は、以下のコマンドラインで NFS クライアント機能をインストールできます。

```
$ sudo apt install nfs-common ↲
```

CentOS や Fedora の場合は、以下のコマンドラインで NFS クライアント機能をインストールできます。

```
$ sudo yum install nfs-utils ↲
```

Linux シェルからのマウント

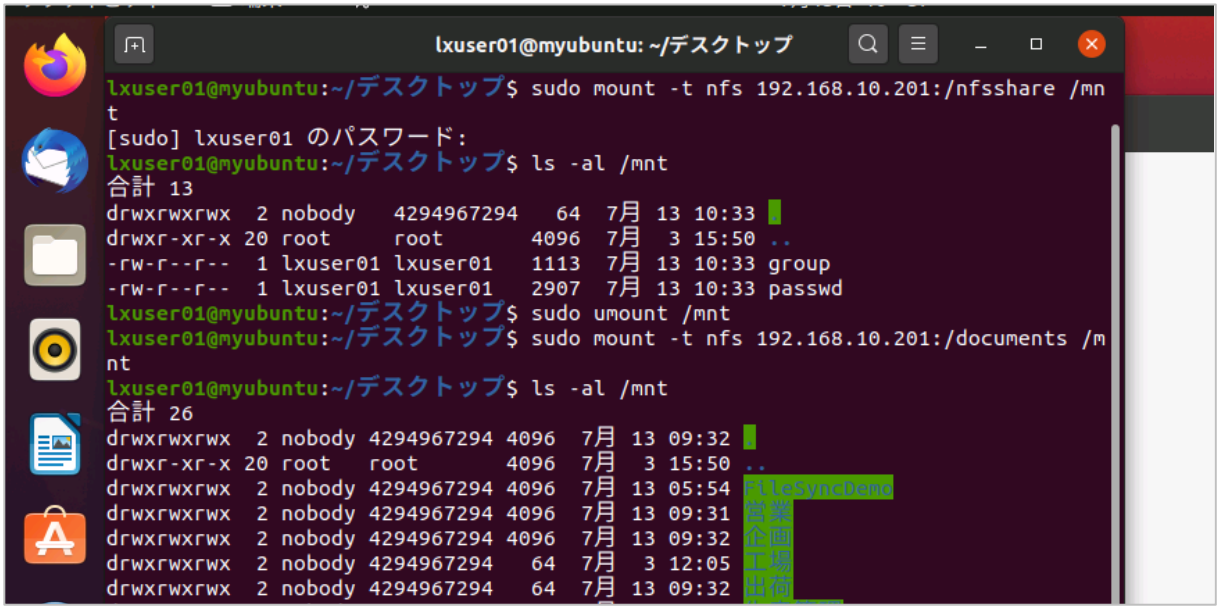
Linux シェル（/bin/bash など）から NFS 共有をマウントおよびマウントを解除するには、次のようにコマンドラインを実行します。以下の例は、/mnt にマウントする例です。sudo コマンドの初回実行時には管理者である現在のユーザーのパスワードの入力が要求されます。

```
$ sudo mount -t nfs <IP アドレスまたはコンピューター名>:/共有名  /mnt ↲

$ sudo umount /mnt ↲
```

Access denied by server while mounting...エラーの回避

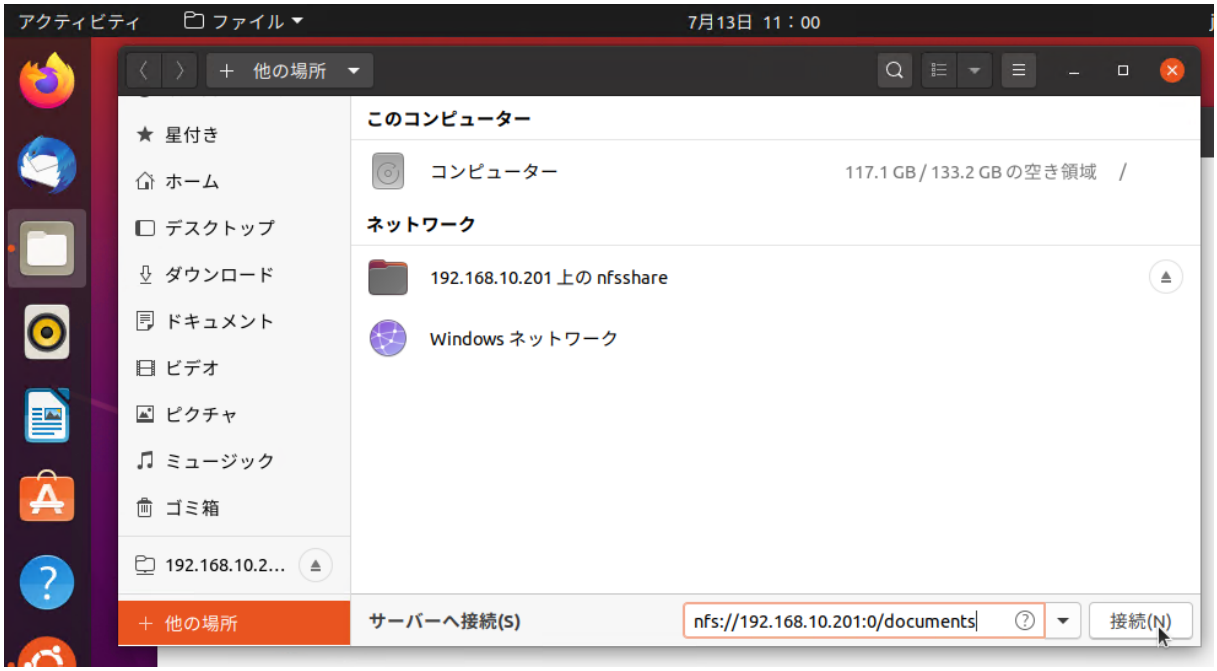
簡易マッピングを有効にして、認証方法で［マップされていないユーザーアクセスを有効にする］をオフにした場合、mount コマンドによるマウント操作が拒否される場合があります。その場合は、認証方法［マップされていないユーザーアクセスを有効にする］と NTFS アクセス許可［Everyone：変更］を有効にするか（こちらを推奨）、共有アクセス許可［ルートアクセスを許可する］を付与します。前者の場合、マウント後のファイル操作は正しく Windows ユーザーにマッピングされます。



画面：Linux の bash シェルから mount コマンドを実行して NFS 共有をマウントする

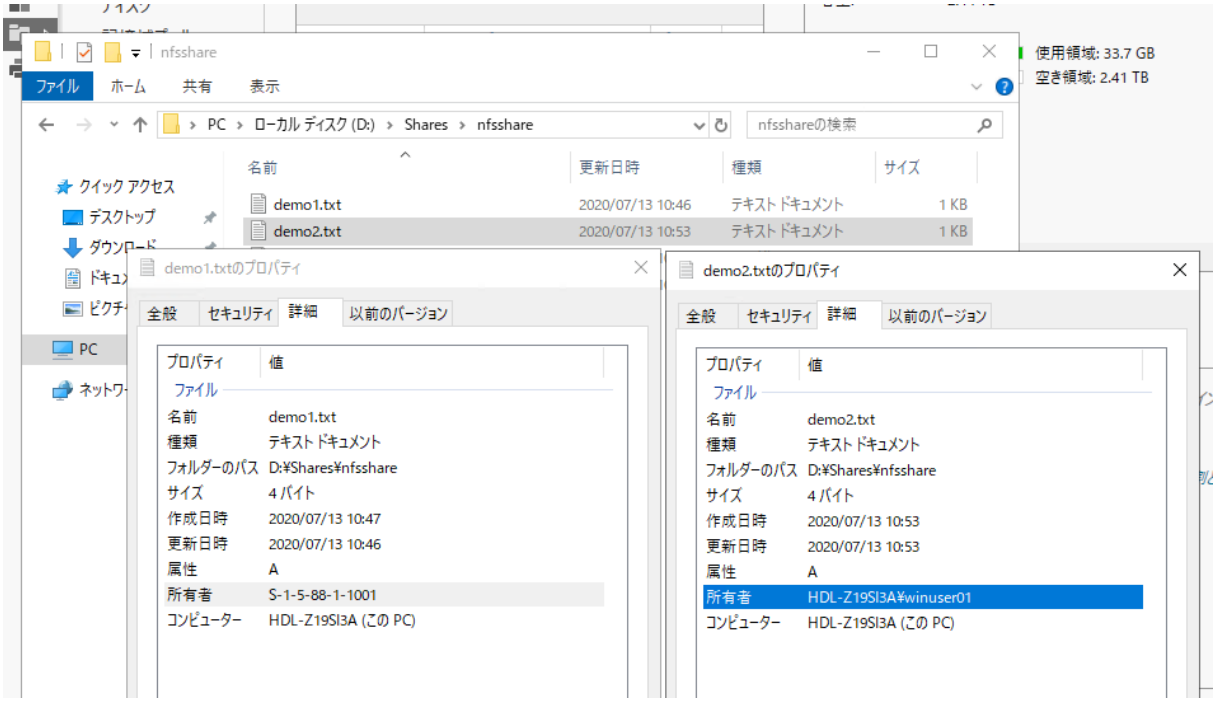
ファイル（Nautilus）アプリからのマウント

Linux のデスクトップで標準的な「ファイル（Nautilus）」アプリを使用する場合は、［＋他の場所］を開き、［サーバーへ接続］のテキストボックスに「nfs://<IP アドレスまたはコンピューター名>:/共有名」のように入力して、［接続］をクリックします。



画面：「nfs://<IP アドレスまたはコンピューター名>:/共有名」と入力して［接続］をクリックする

> **ユーザーマッピングの効果について**
>
> マップされていないユーザーアクセスの場合、Linux 側では問題ありませんが、Windows 側から見ると所有者が「不明なアカウント（S-1-5-88-1-Linux のユーザーID）」と認識されます。一方、Windows Server の NFS サーバー側でユーザーマッピングが作成済みであり、マップされたユーザーでアクセスした場合は、Linux 側で作成されたファイルの所有者は Windows 側ではマップされた Windows ユーザーとして識別されます。



画面 : demo1.txt はユーザーマッピング前に NFS クライアント側で作成したファイル、demo2.txt はユーザーマッピング後に NFS クライアント側で作成したファイル

4　WebDAV 共有のセットアップとファイルアクセス

HDL-Z にインターネットインフォメーションサービス（IIS）の役割を追加し、WebDAV をサポートする仮想ディレクトリを作成して公開するまでの一連の手順を説明します。

> **WebDAV アクセスのセキュリティ**
>
> WebDAV は http または https で構成できますが、IIS の基本認証を利用することになるため、セキュアなアクセスのためには SSL 証明書を必要とする、暗号化された https アクセスのみで許可することを推奨します。ここでは、自己署名証明書を利用した方法で説明します。社内で利用するには自己署名証明書でも問題はないでしょう（社内限定で自己署名証明書を信頼するという前提での利用となります）。

4.1　役割サービスのインストール

はじめに、Windows Server IoT 2019 for Storage で「Web サーバー（IIS）」の役割と WebDAV サポートに関連する役割サービスをインストールします。

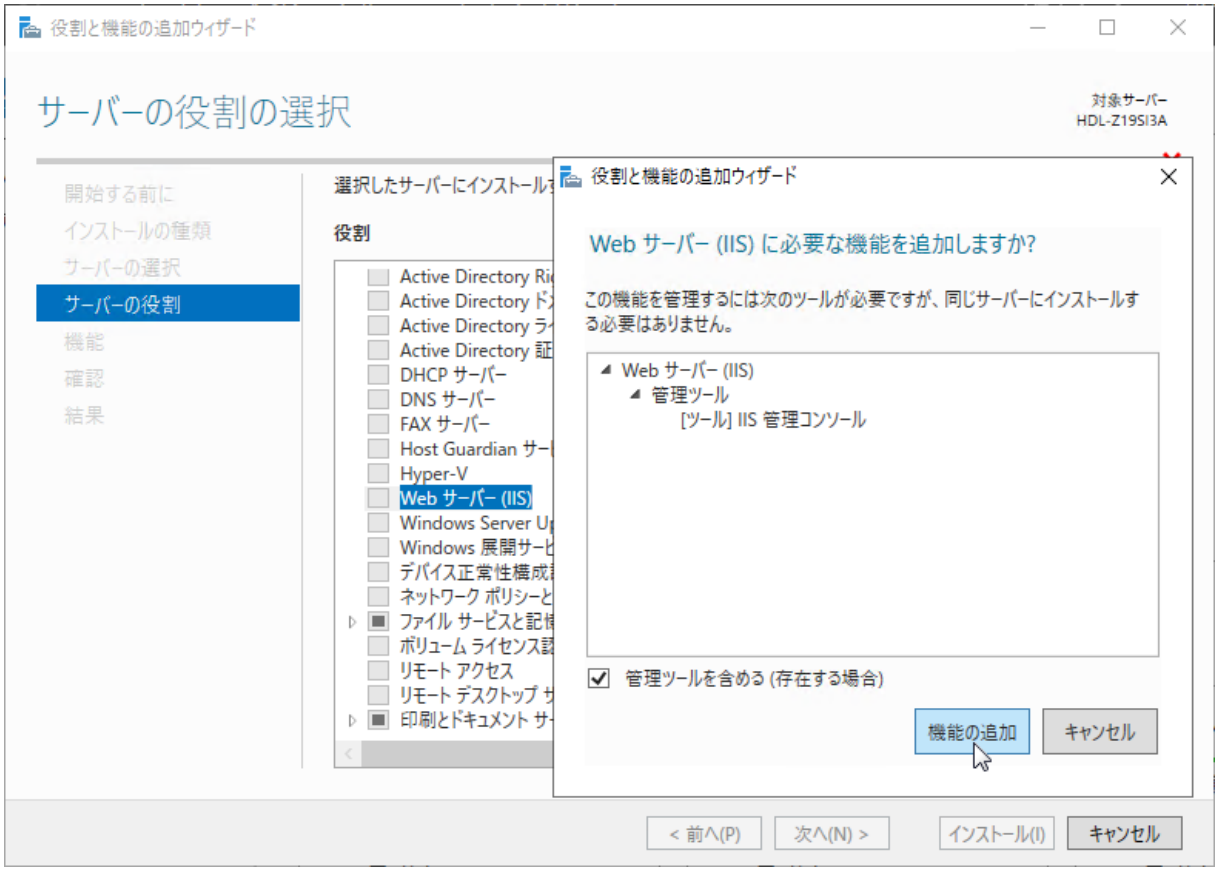
1.　［サーバーマネージャー］の［ダッシュボード］を開き、［クイックスタート ②役割と機能の追加］を

クリックして、[役割と機能の追加ウィザード] を開始します。[開始する前に] ページで [次へ] をクリックします。

2. [インストールの種類の選択] ページで [役割ベースまたは機能ベースのインストール] を選択して [次へ] をクリックします。

3. [対象サーバーの選択] ページで HDL-Z を選択し、[次へ] をクリックします。

4. [サーバーの役割の選択] ページで役割の一覧で [Web サーバー (IIS)] をチェックします。がチェックされていない場合はチェックします。[Web サーバー (IIS) に必要な機能を追加しますか？] と表示されるので、[管理ツールを含める (存在する場合)] がチェックされていることを確認し、[機能の追加] をクリックします。[サーバーの役割の選択] ページに戻るので [次へ] をクリックします。



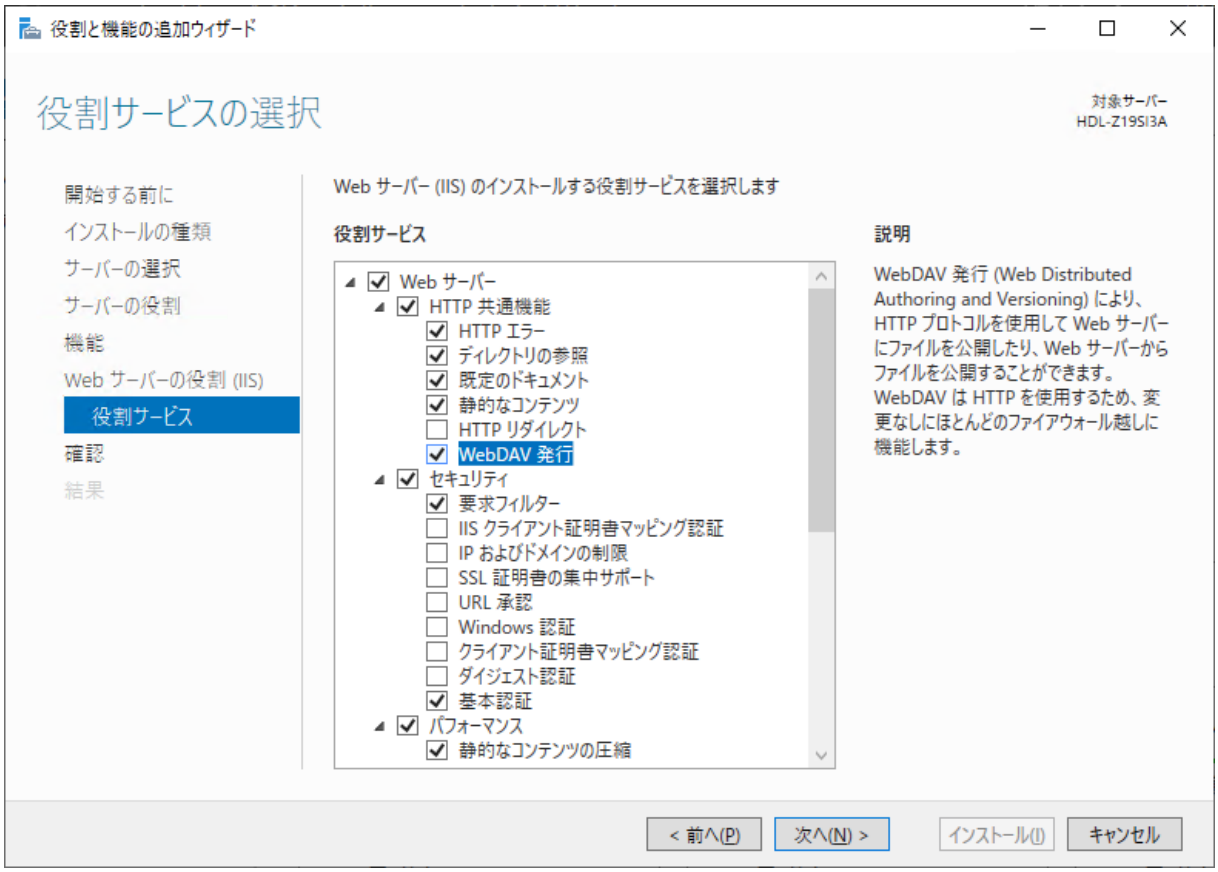
画面：[Web サーバー (IIS)] の役割と管理ツールを追加する

5. [機能の選択] ページでは、そのまま [次へ] をクリックします。

6. [Web サーバーの役割 (IIS)] ページで [次へ] をクリックし、[役割サービスの選択] ページで既定で選択されている役割サービスに加えて、以下の場所にある [WebDAV 発行] と [基本認証] の 2 つの役割サービスをチェックして追加します。

Web サーバー
- ├ HTTP 共通機能
  - ├ ☑ WebDAV 発行
- ├ セキュリティ

├ ☑ 基本認証



画面：既定の選択に加えて、［WebDAV 発行］と［基本認証］を追加する

7. ［インストールオプションの確認］ページで［インストール］をクリックします。なお、役割サービスのインストールを完了するために、再起動は要求されません。

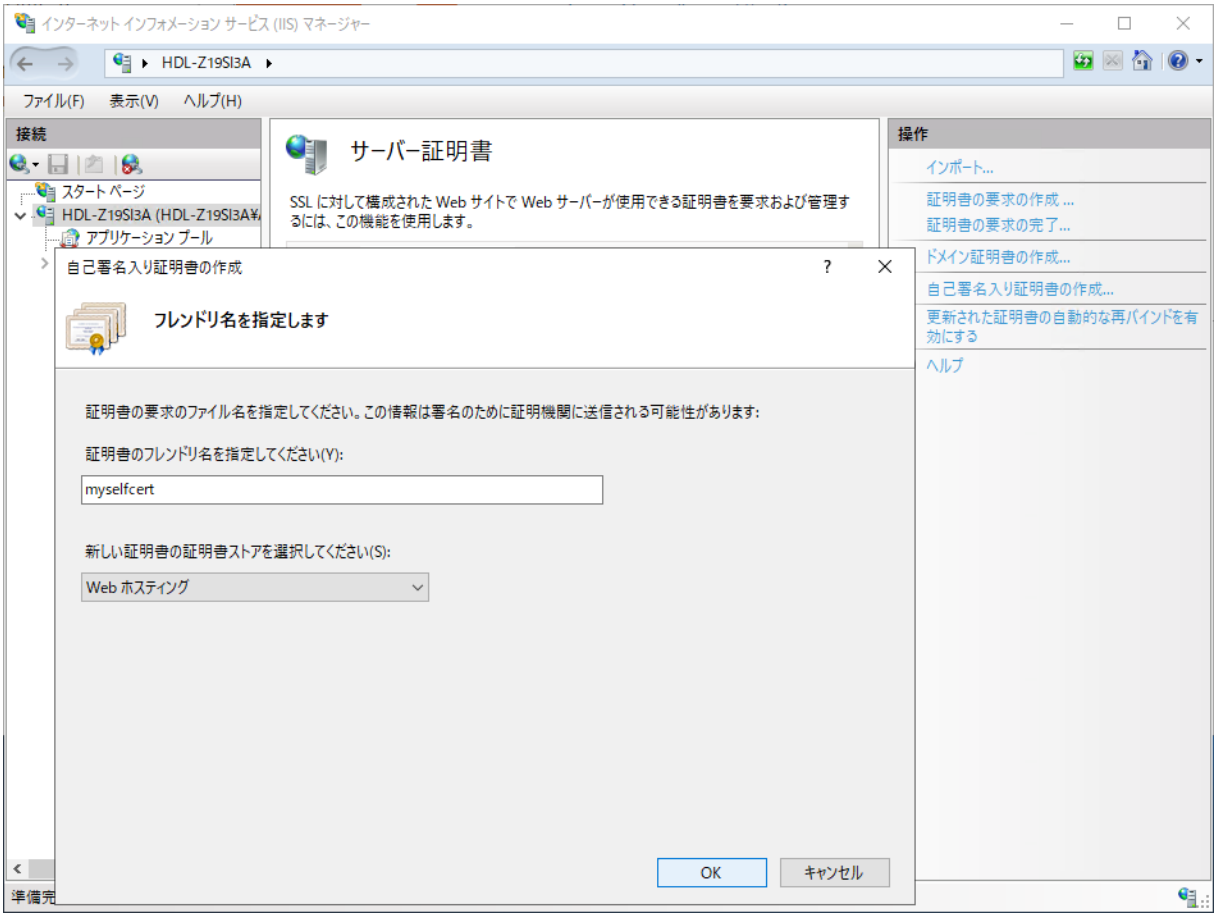
4.2　WebDAV 仮想ディレクトリの作成と公開

次に、WebDAV で公開する仮想ディレクトリを作成し、セキュリティの保護と WebDAV のサポートを有効化して公開します。

自己署名証明書の作成とバインド

WebDAV で公開するディレクトリは、基本認証の保護とダウンロード／アップロードトラフィックの保護のために SSL を要求するように構成することを強く推奨します。このガイドでは自己署名証明書を作成して使用します。

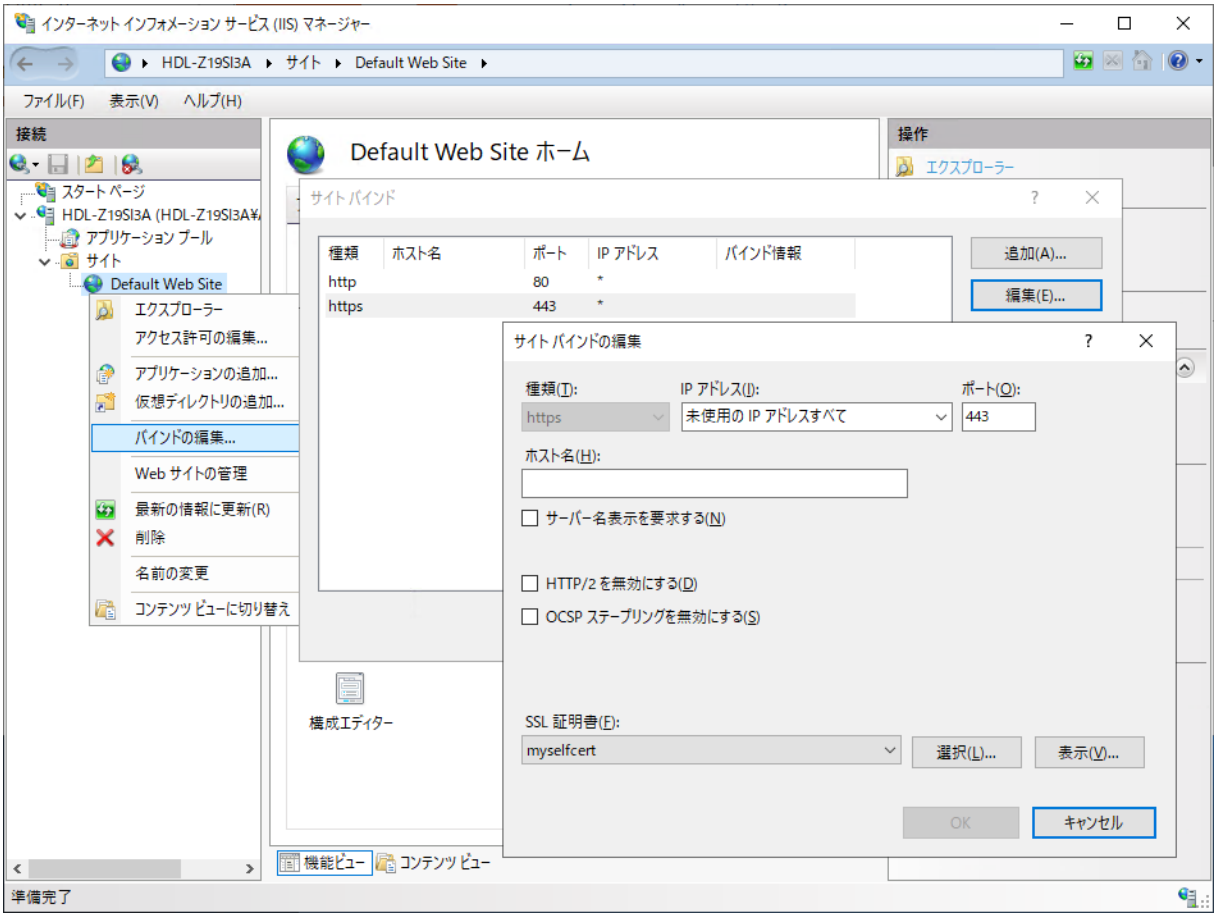
1. Windows 管理ツールの［インターネットインフォメーションサービス（IIS）マネージャー］を開き、［接続］ペインでサーバーを選択して［<サーバー名>ホーム］を開きます。さらに［サーバー証明書］をクリックして開きます。［操作］ペインから［自己署名入り証明書の作成...］をクリックして、証明書のフレンドリ名に分かりやすい名前を入力し、証明書ストアとして［Web ホスティング］を選択して［OK］をクリックします。



画面：WebDAV 用に自己署名証明書を作成する

2. 作成した自己署名証明書を配布できるように、作成された証明書を選択し、[操作] メニューから [表示...] をクリックして証明書のプロパティを開きます。[詳細] タブに切り替え、[ファイルにコピー...] をクリックします。[証明書のエクスポートウィザード] が開始するので、秘密キーをエクスポートしないことを選択し、[DER encoded binary X.509（.CER)] 形式で任意のパスにファイルとして保存します。Windows クライアントの場合はこのファイルから証明書をローカルコンピューターの証明書ストアの [信頼されたルート証明機関] にインポートすることで、自己署名証明書の警告を回避できます。

3. [接続] ペインで [サイト] を展開し [Default Web Site] を右クリックして [バインドの編集...] をクリックします。[サイトバインド] ダイアログボックスを開くので、[追加...] をクリックして、[https | 未使用の IP アドレスすべて | 443] と選択し、[SSL 証明書] ドロップダウンリストから先ほど作成した自己署名証明書を選択して、[OK] をクリックします。



画面：TCP ポート 443 に自己署名証明書を割り当ててバインドする

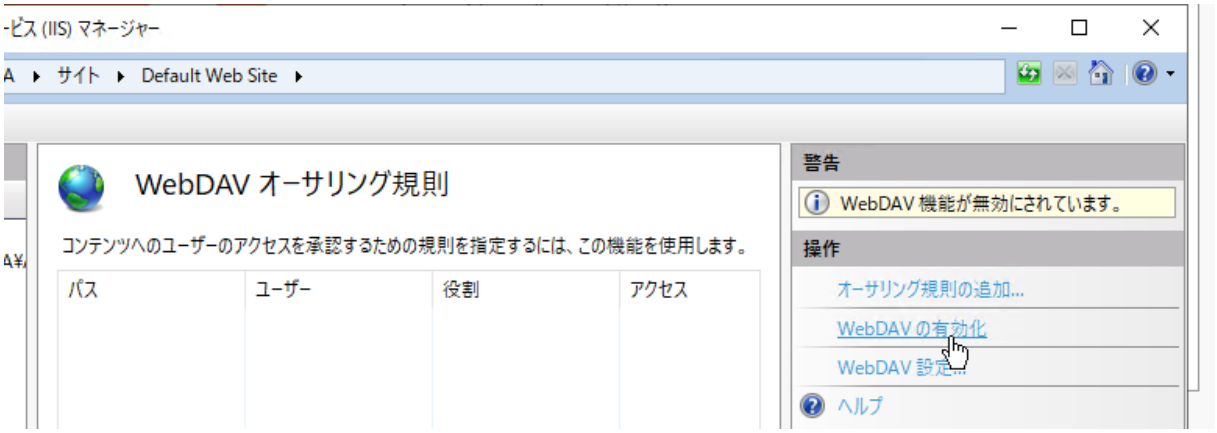
4. ［サイトバインド］ダイアログボックスに戻るので、［閉じる］をクリックしてダイアログボックスを閉じます。

> **HTTPS ポートの競合に注意**
>
> HDL-Z で TCP ポート 443 を使用する別のアプリケーションを既に導入している、または今後導入する予定がある場合は、WebDAV のポートとの競合に注意してください。WebDAV の HTTPS を別のポート（8443 など）で構成するか、別のアプリケーションの方のポートを変更してください。例えば、このガイドの前編『3. 集中管理編』で説明した「Windows Admin Center」のサイトの既定のポートは 443 です。

仮想ディレクトリの作成と構成

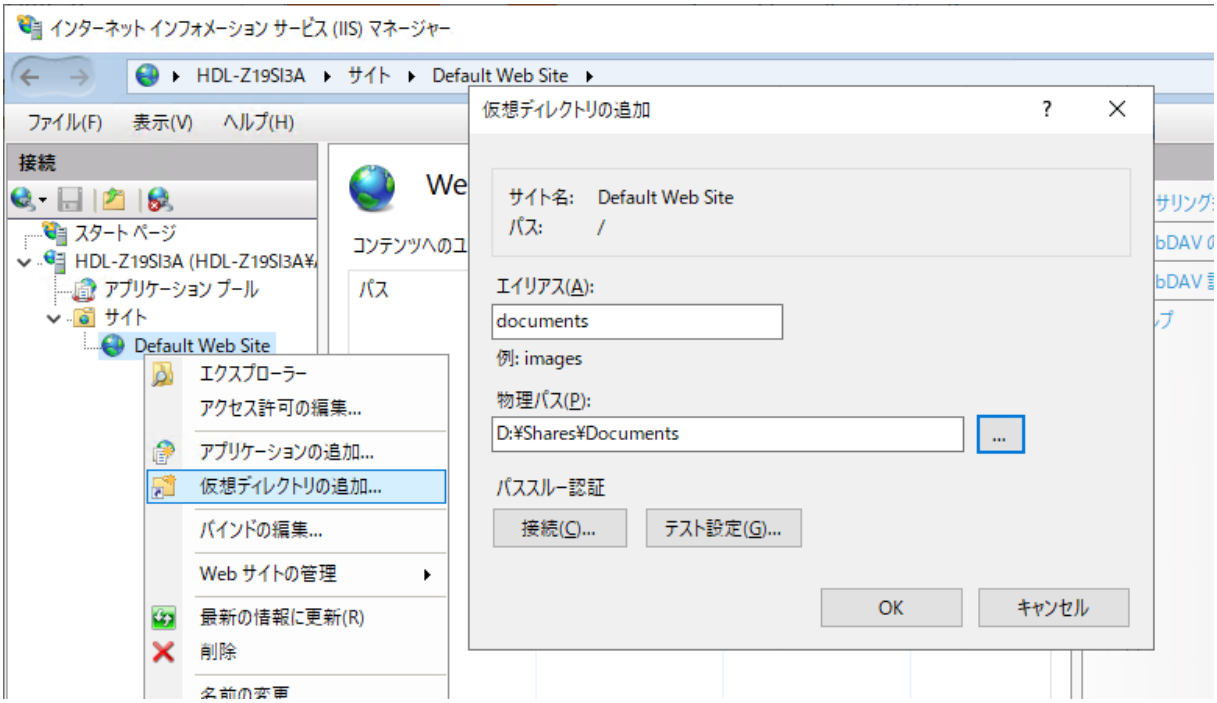
ここまでの時点で既定の Web サイト「Default Web Site」に対する http および https アクセスが可能になりました。次に WebDAV で公開するための仮想ディレクトリを作成して公開します。

1. ［インターネットインフォメーションサービス（IIS）マネージャー］の［接続］ペインで［Default Web Site］を選択して［Default Web Site ホーム］を開き、［WebDAV オーサリング規則］をクリックして開きます。［操作］ペインの［WebDAV の有効化］をクリックして WebDAV を有効化します。



画面：[WebDAV の有効化] をクリックする

2. [インターネットインフォメーションサービス (IIS) マネージャー] の [接続] ペインで [Default Web Site] を右クリックし、[仮想ディレクトリの追加...] をクリックします。[仮想ディレクトリの追加] ダイアログボックスが開くので、エイリアスに仮想ディレクトリ名（例：documents）と入力し、物理パスとして WebDAV で公開する既存のディレクトリパスを選択して [OK] をクリックします。既存のディレクトリパスの代わりに、新しいディレクトリを作成して指定することもできます。

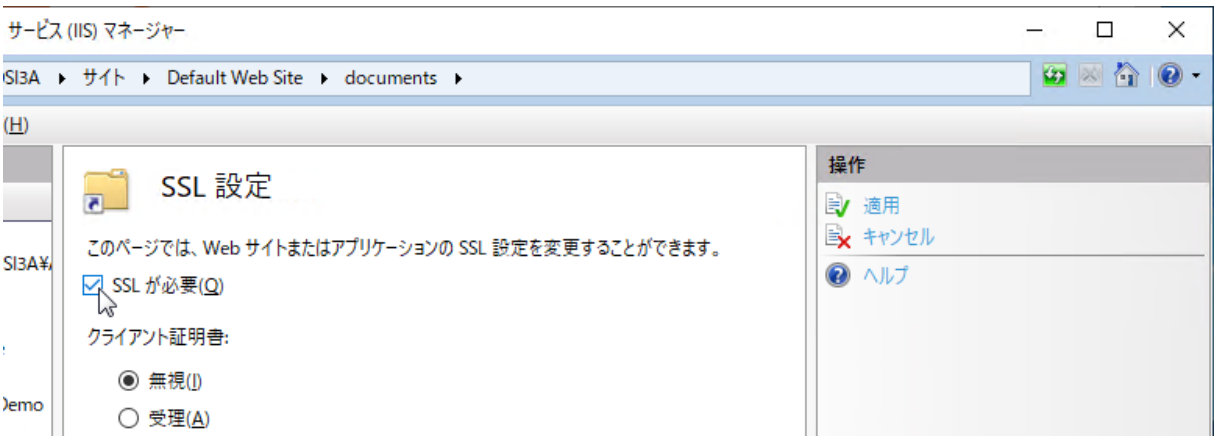


画面：共有用のディレクトリ（新規または既存の SMB 共有）を IIS の仮想ディレクトリとして追加する

3. [接続] ペインで追加された仮想ディレクトリ（例：documents）を右クリックして [アクセス許可の編集] をクリックします。ディレクトリのプロパティダイアログボックスが開くので、[セキュリティ] タブに切り替え、NTFS アクセス許可を調整します。例えば、一般ユーザーに読み書きを許可するには、[Users：変更] のアクセス許可が必要です。

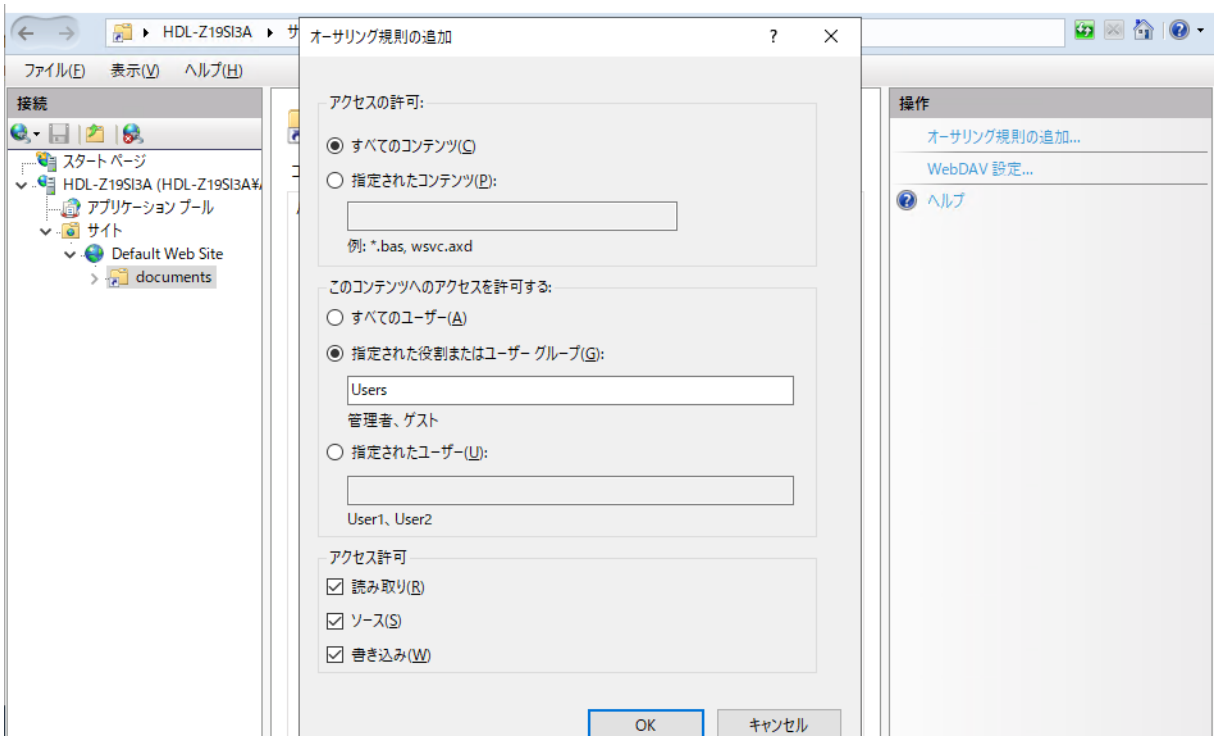
4. [接続] ペインで仮想ディレクトリ（例：documents）を選択し、[<仮想ディレクトリ名>ホーム] を

開きます。[SSL 設定] をクリックして開き、[SSL が必要] をチェックして [操作] ペインの [適用] をクリックします。安全ではない http を許可する（非推奨）場合はこの手順は不要です。



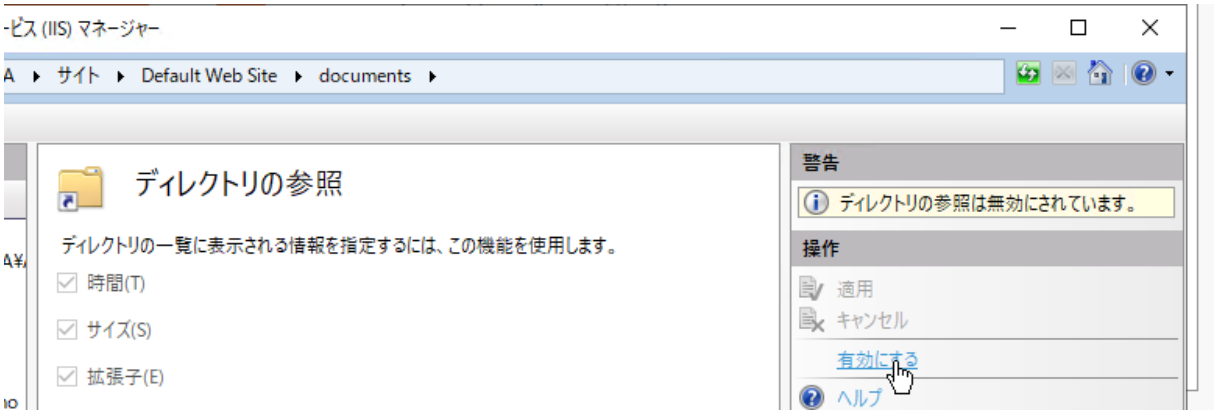
画面：https のみでのアクセスを許可するには、[SSL が必要] をチェックし、[適用] をクリックする

5. [接続] ペインで仮想ディレクトリ（例：documents）を選択し、[<仮想ディレクトリ名>ホーム] を開きます。さらに [WebDAV オーサリング規則] をクリックして開きます。[操作] ペインの [WebDAV オーサリング規則の追加...] をクリックして [WebDAV オーサリング規則の追加] ダイアログボックスを開き、アクセス許可を設定し、[OK] をクリックします。例えば、[すべてのコンテンツ] に対して [Users] グループに対して [読み取り／ソース／書き込み] のアクセス許可を与えます。



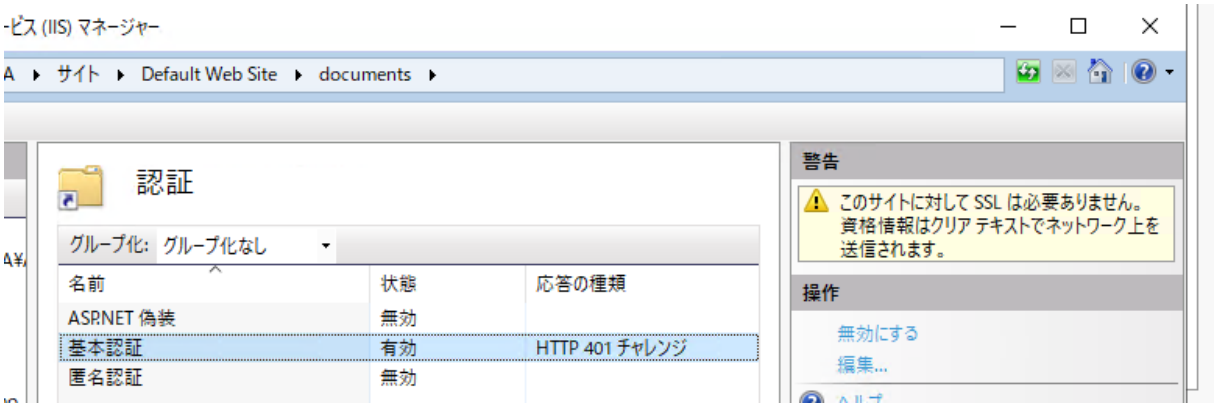
画面：Users グループに対して [読み取り] [ソース] [書き込み] のアクセスを許可する

6. [接続] ペインで仮想ディレクトリ（例：documents）を選択し、[<仮想ディレクトリ名>ホーム] を開きます。[ディレクトリの参照] をクリックして開き、[操作] ペインの [有効にする] をクリックします。



画面：仮想ディレクトリで「ディレクトリの参照」機能を有効にする

7. ［接続］ペインで仮想ディレクトリ（例：documents）を選択し、［<仮想ディレクトリ名>ホーム］を開きます。［認証］をクリックして開き、［基本認証］を選択して［操作］ペインの［有効にする］をクリックします。また、［匿名認証］を選択して［操作］ペインの［無効にする］をクリックします。この設定により、WebDAV アクセスでは基本認証が必須になります。



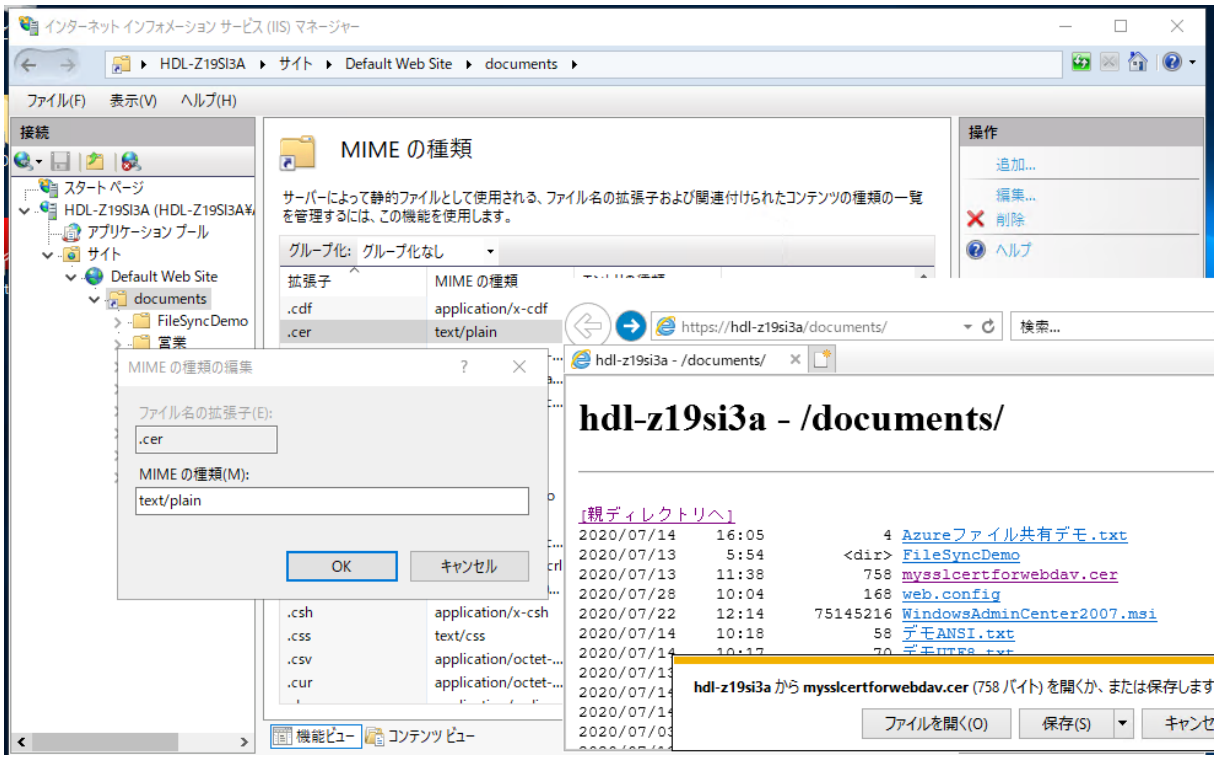
画面：認証方法として「基本認証」だけを有効にする

ダウンロードできないファイルがある場合の回避方法について

WebDAV で公開した仮想ディレクトリからファイルをダウンロードしようとした際に 404 HTTP エラー（例：404 – ファイルまたはディレクトリが見つかりません」）が表示される場合は、不明な MIME の種類であることが原因の可能性があります。

その場合は［インターネットインフォメーションサービス（IIS）マネージャー］の［接続］ペインで仮想ディレクトリ（例：documents）を選択し、［<仮想ディレクトリ名>ホーム］を開きます。［MIME の種類］をクリックして開き、問題のファイルの拡張子に対して「text/plain」や「application/octet-stream」を設定してみてください。

画面：ファイルの種類（拡張子）によってはダウンロードできない場合がある



画面：ダウンロードできないファイルの種類を「MIME の種類」に追加登録する

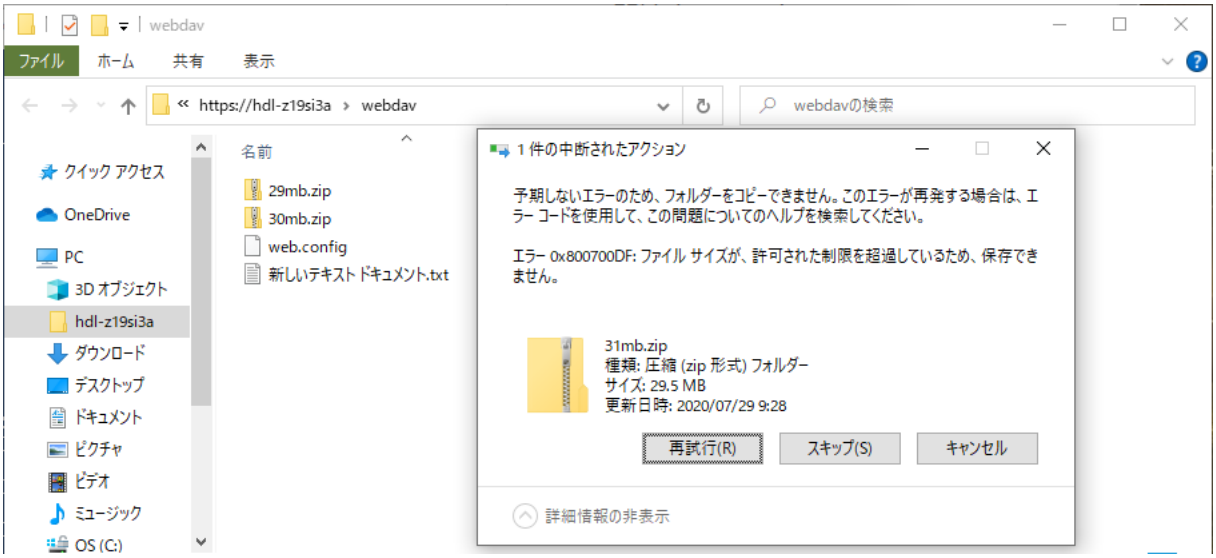
MIME の種類の追加は、C:¥Inetpub¥wwwroot（Default Web Site のルートパス）または仮想ディレクトリのルートにある「web.config」に、次の太字部のように記述して追加することもできます。

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
```

```
    <system.webServer>
        <directoryBrowse enabled="true" />
        <staticContent>
            <mimeMap fileExtension=".cer" mimeType="text/plain" />
        </staticContent>
    </system.webServer>
</configuration>
```

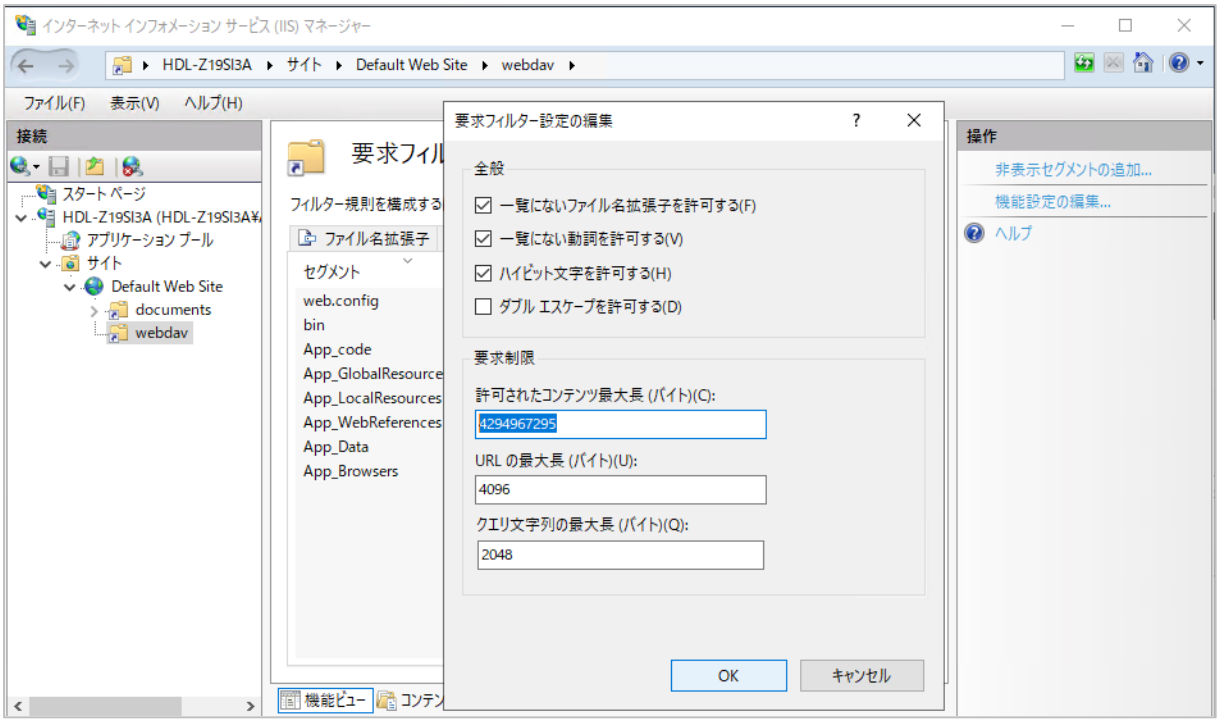
大きなファイル（30MB 以上）のアップロードについて

IIS の既定では、仮想ディレクトリにアップロード可能なファイルの最大サイズは約 28.6MB（30,000,000B）までになります。このサイズを超えたファイルをアップロードしようとした場合、制限の超過により失敗します。



画面：IIS の既定の最大アップロードサイズは約 28.6MB

最大アップロードサイズは 4GB 未満（4,294,967,295B）まで拡大することができます。それには、［インターネットインフォメーションサービス（IIS）マネージャー］で「Default Web Site」または仮想ディレクトリの［要求フィルター］機能を開き、［操作］ペインの［機能設定の編集...］をクリックして［許可されたコンテンツ最大長（バイト）］にバイト長を指定します。既定値は **3000000** で、**0**～**4294967295** の範囲で指定することができます。



画面：[許可されたコンテンツ最大長（バイト）] で最大アップロードサイズのバイト長を変更する

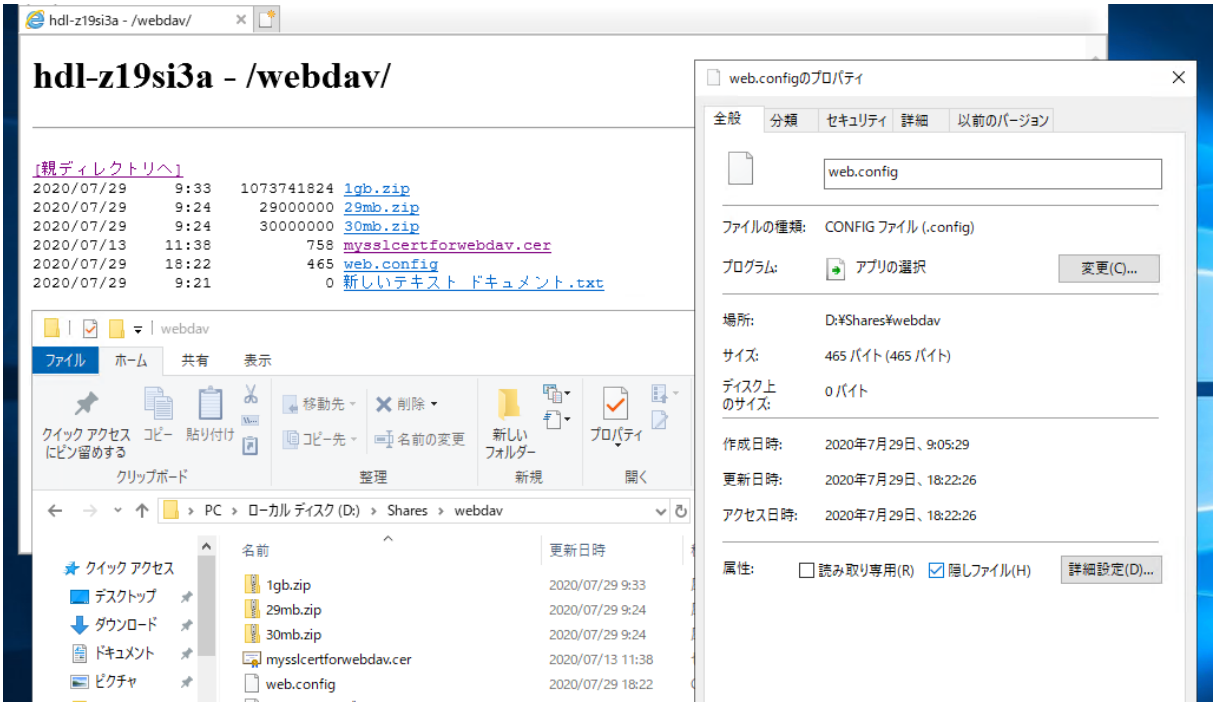
最大アップロードサイズは、C:¥Inetpub¥wwwroot（Default Web Site のルートパス）または仮想ディレクトリのルートにある「web.config」に、次の太字の部分のように requestLimits の maxAllowedContentLength 設定を追加することで変更することもできます。

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
        <directoryBrowse enabled="true" />
        <security>
            <requestFiltering>
                <requestLimits maxAllowedContentLength="4294967295" />
            </requestFiltering>
        </security>
    </system.webServer>
</configuration>
```

web.config を非表示にする方法

IIS の仮想ディレクトリを構成すると、物理パスのルートに「web.config」ファイルが配置されます。この仮想ディレクトリを WebDAV で公開した場合、および SMB や NFS の共有フォルダーとして構成した場合、一般ユーザーは「web.config」にアクセスできてしまいますし、ファイルの NTFS アクセス許可によっては削除や内容の変更ができてしまいます。

故意または操作ミスから「web.config」ファイルを保護するには、NTFS アクセス許可を適切に設定して、一般ユーザーが変更できないようにしてください。IIS 用には IIS_USERS グループに対する読み取りアクセス許可があれば問題ありません。また、「web.config」ファイルのプロパティで「隠しファイル」属性を設定することで、WebDAV や共有フォルダーで非表示にすることができます。



画面：「web.config」の NTFS アクセス許可を適切に設定し、「隠しファイル」属性を設定する

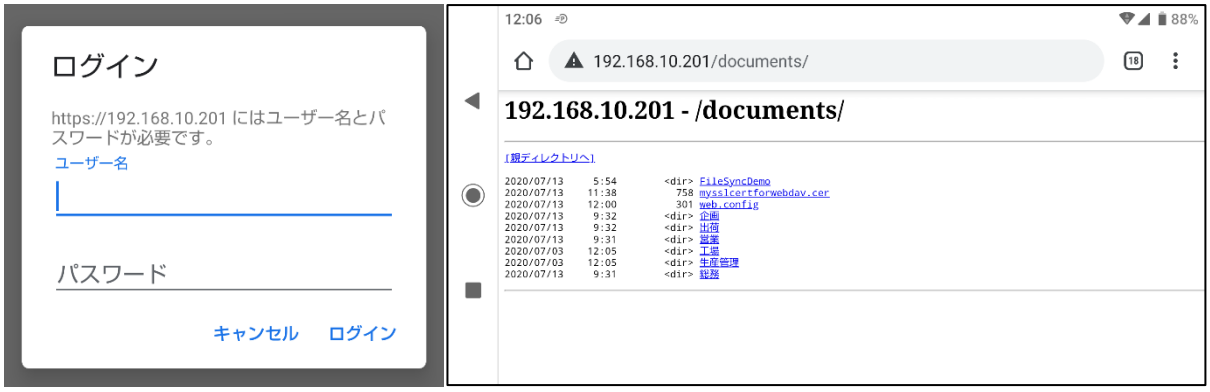
4.3 WebDAV クライアントからのアクセス

WebDAV で公開した仮想ディレクトリには、一般的な Web ブラウザーまたは WebDAV 対応アプリを使用してアクセスすることができます。

Web ブラウザーからのアクセス

Web ブラウザーを使用して仮想ディレクトリに WebDAV でアクセスするには、単純に Web ブラウザーを使用して http または https から始まる仮想ディレクトリの URI（Uniform Resource Identifier）に接続します。例えば、Web ブラウザーで「https://コンピューター名/仮想ディレクトリ名/」に接続します。アクセスするために基本認証が要求されるので、サーバーのローカルユーザーの資格情報を入力して接続します。WebDAV を既定のポート番号以外で構成した場合は、「https://コンピューター名**:ポート番号**/仮想ディレクトリ名/」のように指定してください。

この方法ではディレクトリの移動やファイルのダウンロード（読み取り）操作のみが可能ですが、Windows、Linux、macOS、iOS、Android といった Web ブラウザーを利用可能なすべての環境で利用できます。



画面：Web ブラウザーで WebDAV で公開した仮想ディレクトリの URL にアクセスする（Android の Google Chrome から接続した例）

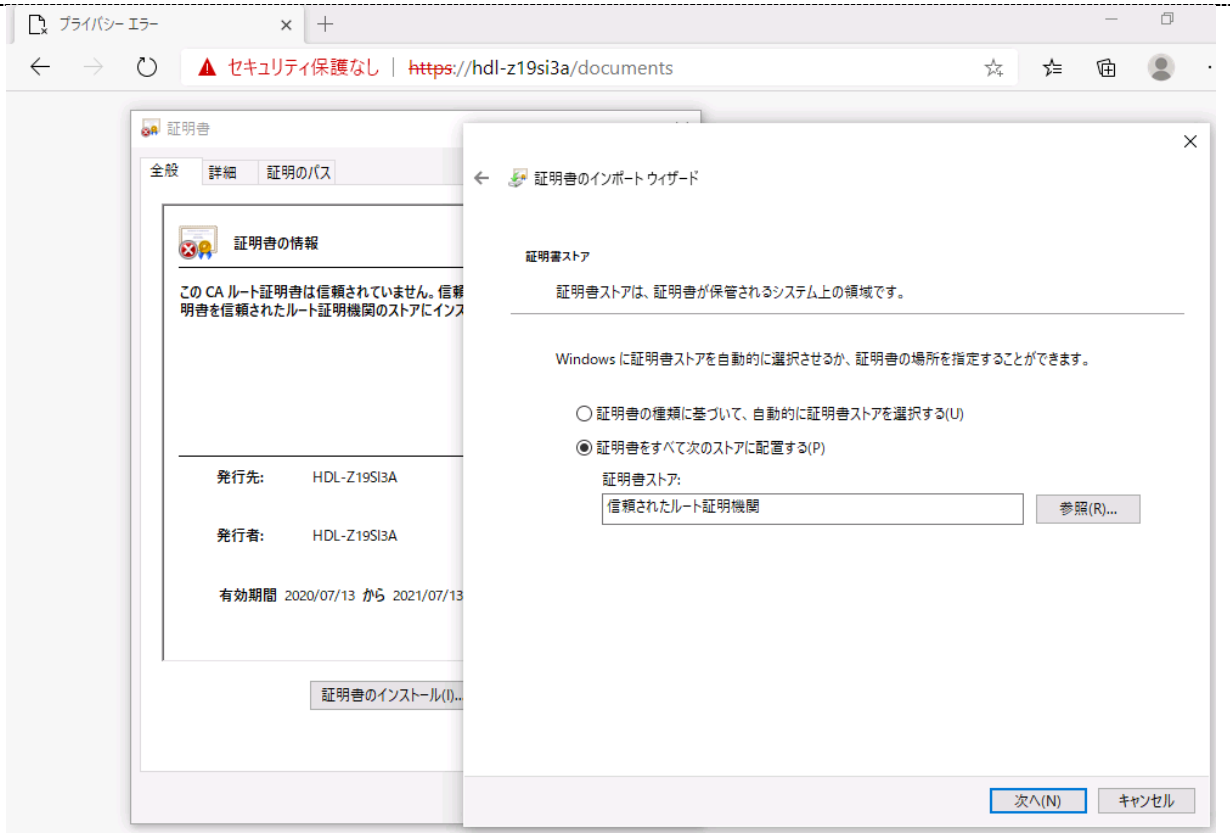
証明書エラーの回避

使用する Web ブラウザーによっては、Web ブラウザーが備えるセキュリティ機能が自己署名証明書のサイトを信頼できないものとしてブロックします。例えば、Internet Explorer や Microsoft Edge（EdgeHTML ベース）は「このサイトは安全ではありません」、Microsoft Edge（Chromium ベース）は「接続がプライベートではありません」と警告します。エラーとなっている証明書を Web ブラウザーで開き、［証明書のインストール］をクリックすることでも警告を無視して先に進むこともできますが、その場合、Web ブラウザーには警告が表示され続けます。

証明書エラーを回避するには、「4.2　WebDAV 仮想ディレクトリの作成と公開」で自己署名証明書を作成した際にエクスポートしておいた自己署名証明書のファイル（.cer）をダブルクリックして開き、［全般］タブの［証明書のインストール］をクリックして現在のユーザーまたはローカルコンピューターの［信頼されたルート証明機関］にインストールします。

または、エラーとなっている証明書を Web ブラウザーから直接開き、［詳細］タブの［ファイルにコピー］をクリックして証明書をファイルにエクスポートします。エクスポートしたファイルをダブルクリックして証明書を開き、［全般］タブの［証明書のインストール］をクリックして現在のユーザーまたはローカルコンピューターの証明書ストアの［信頼されたルート証明機関］にインストールします。

なお、証明書エラーを回避するためには、IP アドレスではなく、証明書に含まれるサブジェクト名と一致するコンピューター名を使用する必要があります。



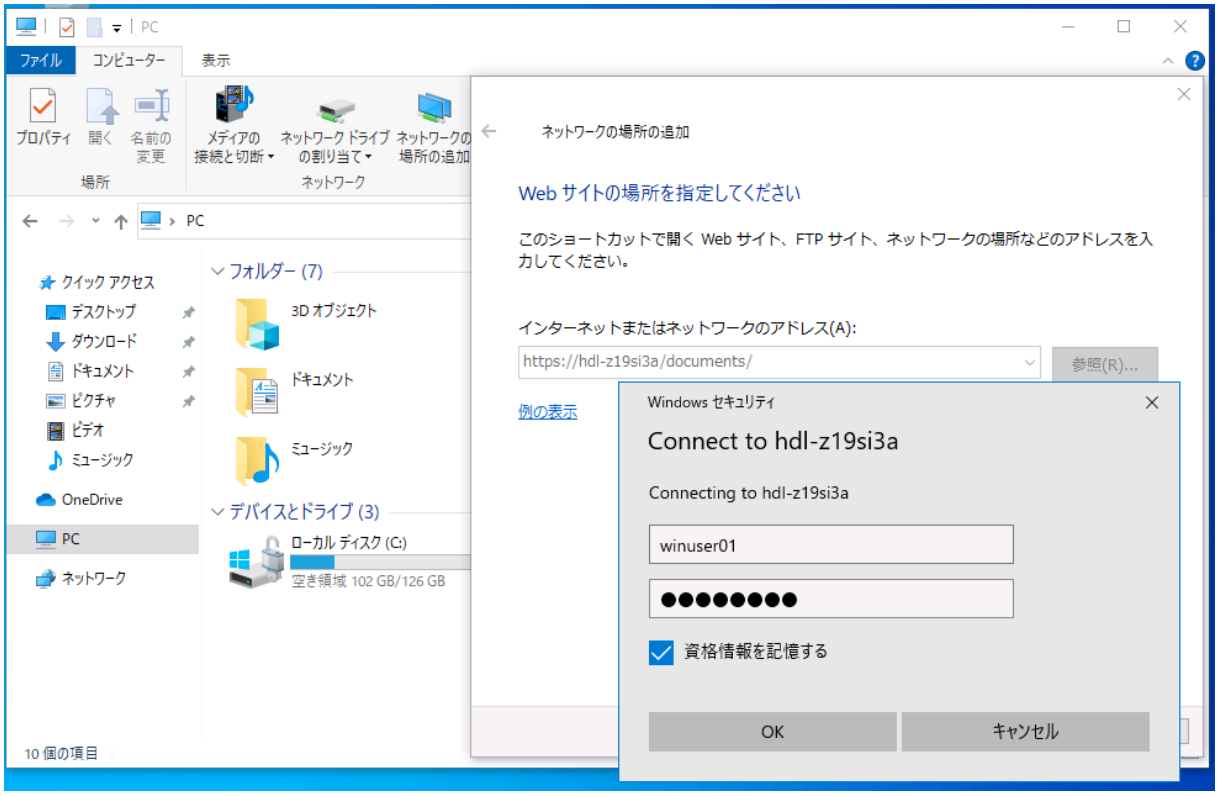
画面：自己署名証明書を「信頼されたルート証明機関」にインストールする

WebDAV 対応アプリからのアクセス

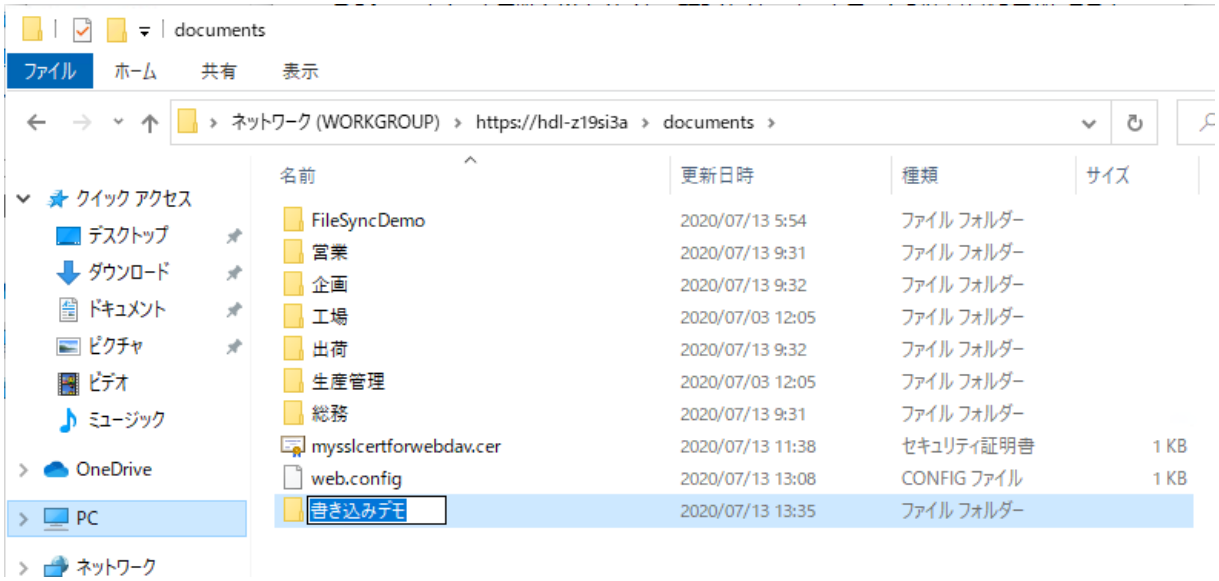
WebDAV アクセスでファイルのアップロード（書き込み）や削除操作を行うには、WebDAV プロトコルに対応したクライアントアプリが必要です。

例えば、Windows の［エクスプローラー］、Ubuntu の［ファイル］（Nautilus）、macOS の［Finder］は WebDAV クライアント機能を備えています。

Windows の［エクスプローラー］の場合は、［PC］を選択して［コンピューター］タブの［ネットワークの場所の追加］をクリックし、［ネットワークの場所の追加ウィザード］を使用して、［カスタムネットワークの場所を選択］を繰KKうし、**http://**または **https://**から始まる仮想ディレクトリの URI を指定して接続します。すると、［エクスプローラー］の中でローカルディスクや SMB 共有上のファイルと同じようにファイル操作が可能です。



画面：[ネットワークの場所の追加] ウィザードで WebDAV 共有に接続する



画面：WebDAV 対応アプリからはファイルのアップロード（書き込み）や削除操作も可能

Linux の場合は、[ファイル] を開き、[＋他の場所] を開き、[サーバーへ接続] のテキストボックスに **dav://**（http の場合）または **davs://**（https の場合）から始まる URI を入力して接続します。

macOS の場合は、[Finder] の [移動] メニューから [サーバへ接続...] を開き、[サーバアドレス] に **http://** または **https://**から始まる URI を入力して接続します。

スマートフォンデバイスの場合は、公式のオンラインストア（Google Play や Apple App Store）で "**WebDAV**" と検索すれば、WebDAV 対応の有料または無料アプリが簡単に見つかります。アプリの評価を

参考に、好みのアプリをインストールして使用してください。

画面：Android 用の WebDAV クライアントアプリの例（CX ファイルエクスプローラ）

著者紹介

山内 和朗（やまうち かずお）

2020-2021 Microsoft MVP - Cloud and Datacetner Management
https://mvp.microsoft.com/ja-jp/PublicProfile/4021785

略歴

フリーランスのテクニカルライター。大手 SIer のシステムエンジニア、IT 専門誌の編集者、地方の中堅企業のシステム管理者を経て、2008 年にフリーランスに。「山市良」の筆名で IT 専門誌や IT 系 Web メディアへの寄稿、IT ベンダーの Web コンテンツの制作、技術文書（ホワイトペーパー）の執筆、Windows 系技術書の執筆や翻訳を行う。2008 から現在まで Microsoft MVP Award を毎年受賞。岩手県花巻市在住。

近著

『Windows 版 Docker＆Windows コンテナー テクノロジ入門』（日経 BP 社、2020 年）

『Windows Server 2016 テクノロジ入門 改訂新版』（日経 BP 社、2019 年）

『Windows トラブル解決コマンド＆テクニック集』（日経 BP 社、2018 年）

『インサイド Windows 第 7 版 上』（訳書、日経 BP 社、2018 年）

『Windows Sysinternals 徹底解説 改訂新版』（訳書、日経 BP 社、2017 年）

ブログ

山市良のえぬなんとかわーるど
https://yamanxworld.blogspot.com/