進化する明日へ Continue thinking

I-O DATA

ホワイトペーパーシリーズ：

はじめての Windows NAS

Windows Server IoT 2019 for Storage 版

2021 年 6 月 15 日

内容

ので、内容については一切保証を致しかねます。アイ・オー・データサポートセンターでは内容に関するお問い合わせは承っておりません。以下の内容をご了承いただいた場合のみご利用ください。(1)アイ・オー・データは、本文書によりいかなる権利の移転もしくはライセンスの許諾、またはいかなる保証を与えるものではありません。(2)アイ・オー・データは、本文書について、有用性、正確性、特定目的への適合性等のいかなる保証をするものではありません。(3)アイ・オー・データは、本文書を利用したこと、または利用しなかったことにより生じるいかなる損害についても責任を負うものではありません。(4)アイ・オー・データは、本文書の内容を随時、断りなく更新、修正、変更、削除することがあります。最新の商品情報については、https://www.iodata.jp/をご覧ください。

1. 概要

1.1 このホワイトペーパーについて

このホワイトペーパーは、Windows Server IoT 2019 for Storage Standard または Workgroup を搭載するランディスク HDL-Z シリーズの NAS（ネットワーク接続型ストレージ）をはじめて導入する新米担当者を対象に、利用開始までのステップと利用開始後の重要な運用管理タスクについて説明します。

参照情報

このホワイトペーパーは、Windows や Windows Server に慣れていない初心者にもわかるように、必要最小限の手順を説明しています。Windows Server IoT 2019 for Storage 搭載の LAN DISK Z シリーズの NAS の、より高度なセットアップや最適化、活用方法については、以下のホワイトペーパーを参考にしてください。

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/index.htm#IoT2019-04

Windows Server IoT 2019 for Storage を活用した生産性向上術（全 4 編）
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
https://www.iodata.jp/biz/whitepaper/index.htm#IoT2019-08

1.2 HDL-Z シリーズの NAS の特徴

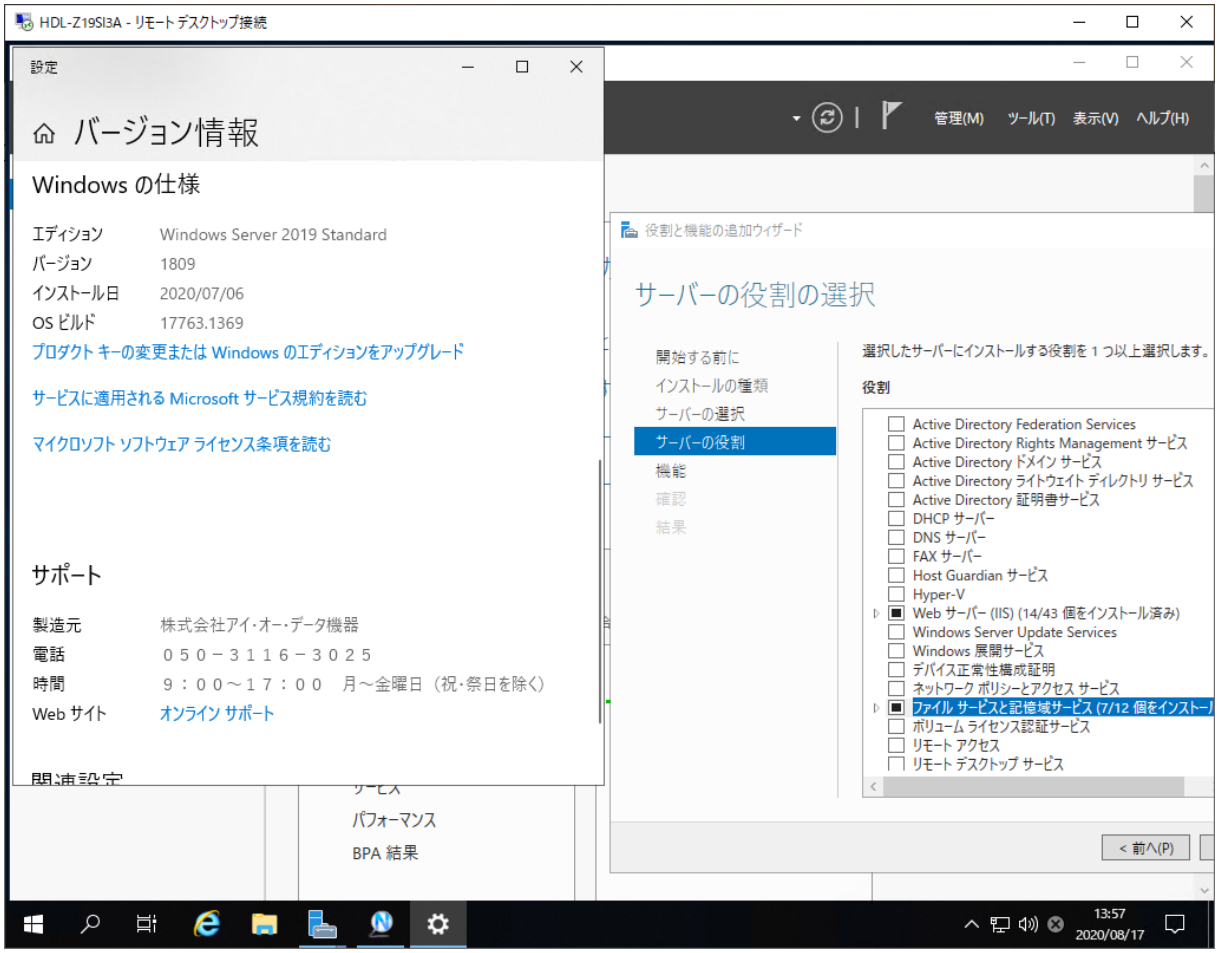
HDL-Z シリーズの NAS は、プレインストール OS として Windows Server IoT 2019 for Storage Standard または Workgroup を搭載した、Windows Server ベースの NAS です。

低価格なエントリモデルの NAS の多くは Linux ベースの OS を搭載しており、設置して電源をオンにし、Web ブラウザーで管理ツールに接続して簡単な初期設定を行うだけで使い始めることができます。

一方、Windows Server ベースの NAS の特徴は、NAS 専用の管理ツールを持たないため、Windows Server の知識や経験が無いと導入のハードルが高いと感じるかもしれません。しかし、いったん初期設定を行ってしまえば、Linux ベースの NAS と同じように小規模な環境でファイル共有を簡単に始めることもできますし、Windows Server OS の特性を生かして、企業内の既存の Windows ネットワーク環境に完全に統合され管理された Windows Server のファイルサーバーとして、高度なアクセス許可やドキュメント管理機能などとともに使用することもできます。

Windows Server IoT 2019 for Storage とは

Windows Server IoT 2019 for Storage には Standard と Workgroup の 2 つのエディションが存在します。エディションの違いは、Workgroup にはハードウェアの制約（ディスク数の上限など）やユーザー数の上限（最大 50 ユーザー）があるだけで、ソフトウェア的には通常版の Windows Server 2019 Standard エディションとまったく同じものです。



画面：Windows Server IoT 2019 Storage は専用 OS ではなく、Windows Server 2019 Standard と全く同じもの。ライセンス条項で用途や上限（Workgroup の場合）が制限されている

Windows Server IoT 2019 for Storage は Windows Server 2019 Standard と同じサーバーの役割と機能を備えていますが、ライセンス条項（EULA）によってファイルサービスの提供およびサーバーの管理目的（更新やバックアップ、ローカルサーバーのシステム管理など）のみに用途が限定されています。そのため、Active Directory ドメインサービスの役割をインストールしてドメインコントローラーとしてセットアップすることはライセンス上許可されていません。一方で、Windows Server IoT 2019 for Storage の NAS は、通常版の Windows Server の Active Directory ドメインサービスで構成された Active Directory ドメインにメンバーサーバーとして参加することは可能です。

Windows Admin Center による簡単管理

Windows Server IoT 2019 for Storage は、Windows Server 2019 と同じ手順でセットアップし、ファ

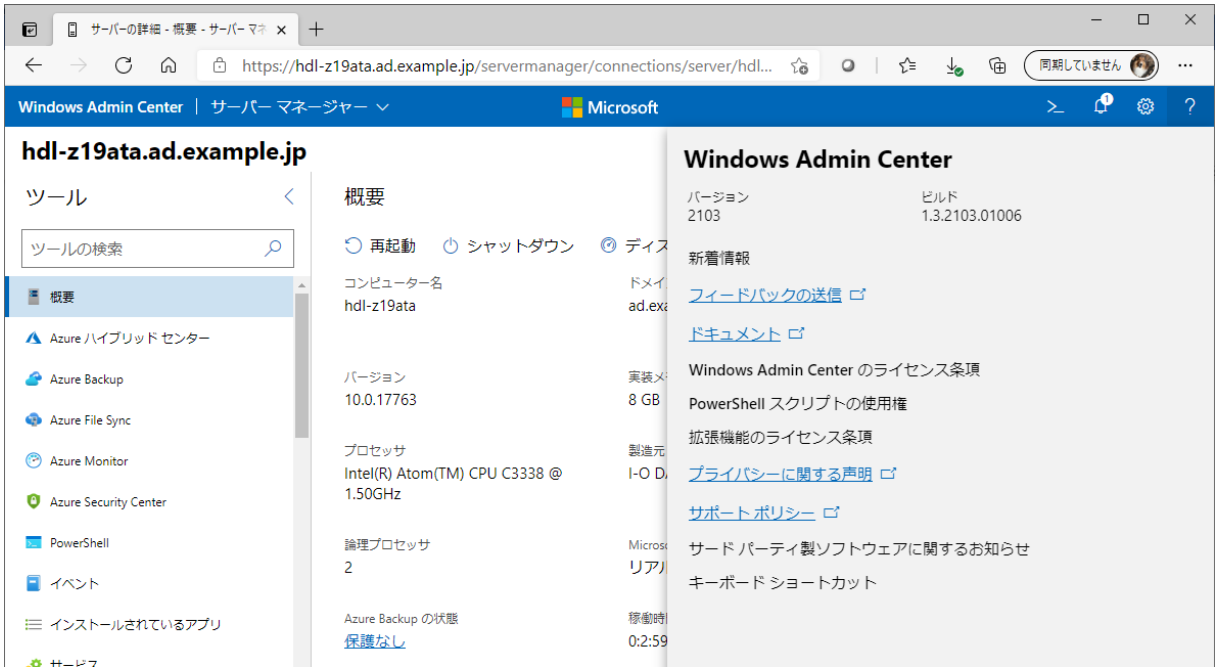
イルサーバーとして構成して利用することができます。また、Windows Server 2019 と同じ方法でバックアップ管理や更新管理が可能です。

通常、Windows Server は、「サーバーマネージャー」や各種 MMC（Microsoft 管理コンソール）スナップインの管理ツール、コマンドラインツール、Windows PowerShell などを利用して構成および管理します。さまざまな管理ツールを適材適所で使い分ける必要があるため、Windows Server の管理に慣れていない人にとっては、導入後の初期設定、共有設定、運用管理のための操作はハードルが高いと感じるかもしれません。

これは Windows Server IoT 2019 for Storage を搭載する NAS の場合も同様です。NAS はヘッドレス（キーボード、マウス、ディスプレイがない）のデバイスであるため、通常はリモートデスクトップ接続を利用して Windows Server のコンソールにリモート接続して作業することになります（主にメンテナンス作業のために、キーボード、マウス、ディスプレイを接続して使用することもできます）。

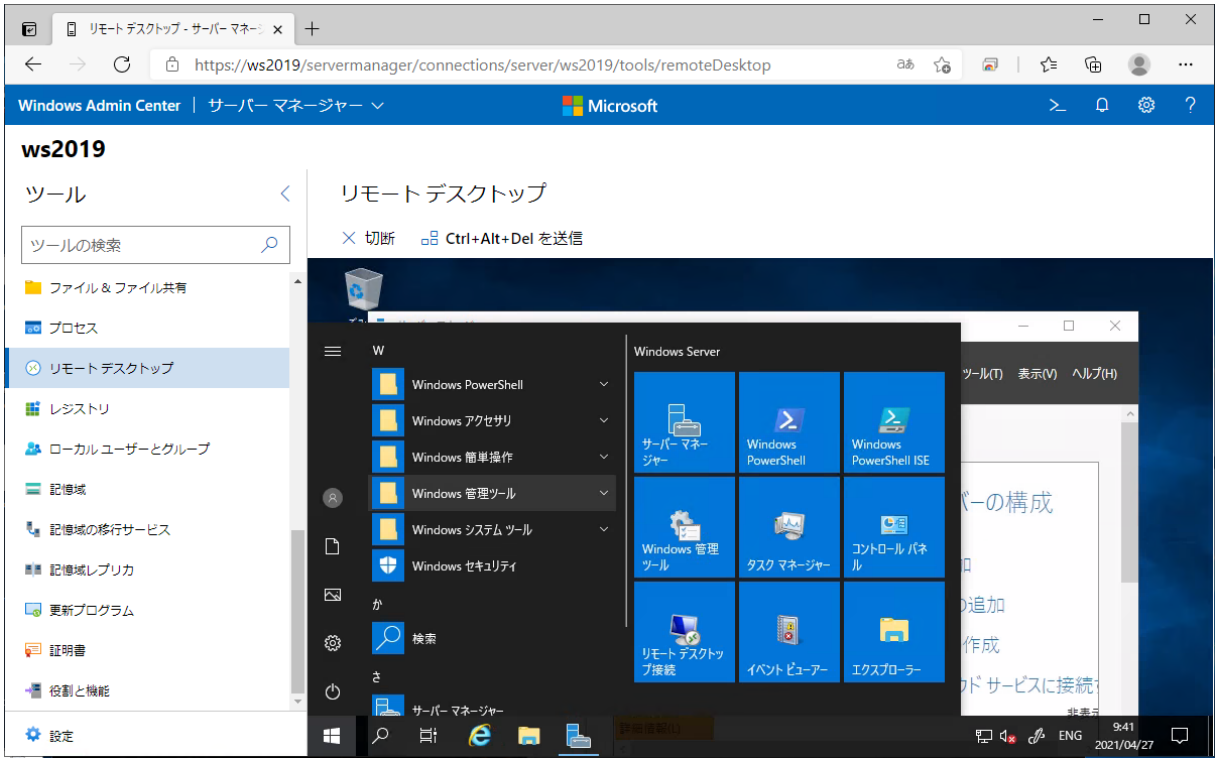
Windows はリモートデスクトップ接続クライアント（Mstsc.exe）を標準搭載していますが、Windows PC がなく、その他のプラットフォームの場合はリモートデスクトップ対応アプリ（Android および iOS 用にマイクロソフト純正アプリが提供されています）をインストールして使用する必要があります。

マイクロソフトは Windows Server のリモート管理を簡素化するために、2018 年 4 月に HTML5 ベースの管理アプリ「Windows Admin Center（WAC）」の無料提供を開始しました。Windows Admin Center は概ね半年ごとに新しいメジャーバージョンがリリースされ、機能の改善や強化が行われています（2020 年 5 月時点の最新バージョンは 2103.2）。リモートデスクトップ接続で NAS の最小限の初期設定を行い、Windows Admin Center を導入してしまえば、その後はリモートデスクトップ接続を使用せずに、手元の PC の HTML5 対応 Web ブラウザー（Internet Explorer には非対応）だけで NAS の設定や管理を行うことが可能です。



画面：Windows Admin Center の管理インターフェイス。Windows Server（IoT 2019 for Storage を含む）のリモート管理に対応

また、Windows Admin Center の［リモートデスクトップ］ツールを使用すると、Web ブラウザーだけでリモートデスクトップ接続して管理操作を行うこともできます。この機能を利用するために、リモートデスクトップ対応アプリは必要ありません。



画面：Windows Admin Center の［リモートデスクトップ］ツールを使用すると、Web ブラウザーだけでリモートのコンソールにアクセスできる

Windows Admin Center の 2 種類のインストールタイプ

Windows Admin Center は、Windows 10 のローカルアプリとしてインストールしてリモートのサーバーを登録して管理する方法と、管理対象の Windows Server（Windows Server 2016 以降、IoT 2019 for Storage を含む）にインストールして、リモートの HTML5 対応ブラウザーから Windows Server がホストする Windows Admin Center にリモート接続して管理する方法があります。前者はデスクトップモード、後者はゲートウェイモードと呼びます。

管理対象の Windows Server が 1 台の場合は、Windows Server にゲートウェイモードとして Windows Admin Center をインストールすると、同じネットワーク上のどの PC やモバイルデバイスの Web ブラウザーからでも管理できて便利です。管理対象が複数台の場合は、1 台の Windows 10 PC に Windows Admin Center をインストールして複数の管理対象のための管理用端末にすると便利です。

1.3　実施環境

このホワイトペーパーでは、Active Directory ドメインを導入していない小規模環境（ワークグループ構成のネットワーク）、Active Directory ドメインを導入済みの中・大規模環境（ドメイン構成のネットワーク）のいずれかに HDL-Z シリーズの 1 台の NAS を新規に導入することを想定し、Windows Admin Center を活用することで必要最小限の初期設定と必要最小限の管理ツールでファイル共有環境をセットアップし、利用を開始、そして運用管理するための環境を準備します。

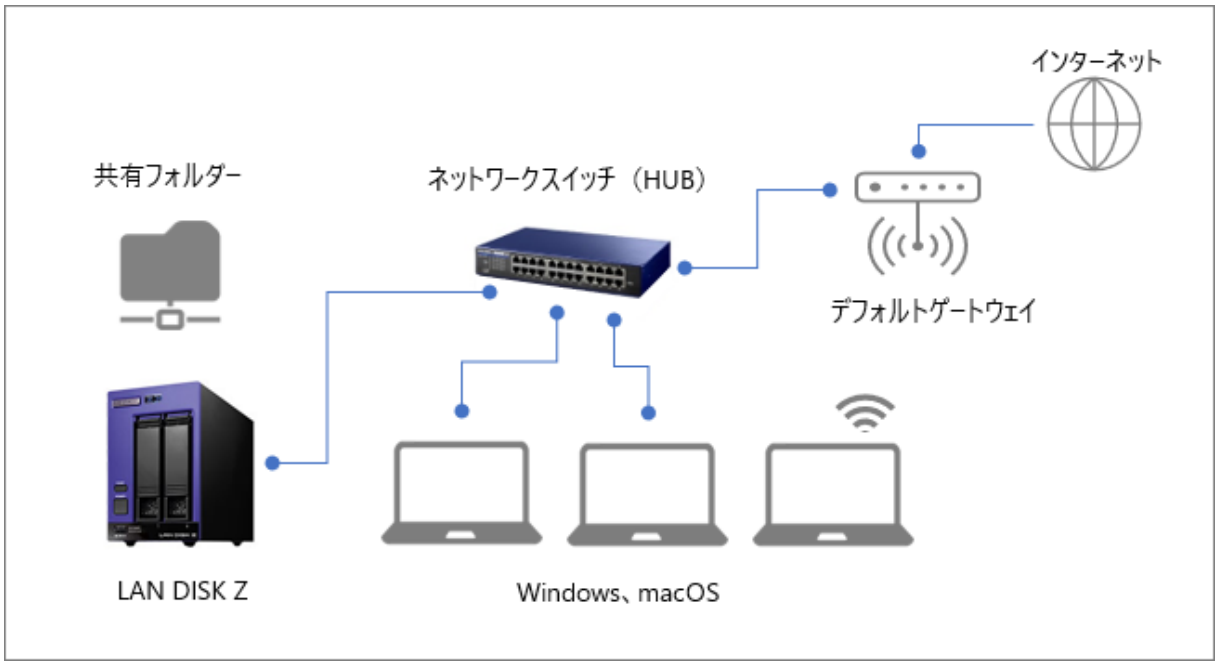
このホワイトペーパーでは、Windows Server IoT 2019 for Storage Workgroup を搭載した 2 ドライブモデル、HDL2-Z19WATA-2 を導入する手順で説明しますが、基本的な手順は HDL-Z シリーズの他のモデルでも共通です。

写真：HDL-Z シリーズ、2 ドライブモデル

小規模な環境（ワークグループ環境）への導入

企業のネットワーク構成はさまざまです。ここでは小規模な環境として、複数台のクライアント PC（Windows や macOS の PC）が有線 LAN または無線 LAN（Wi-Fi）で単一のネットワークに接続されており、ブロードバンドルーターを介してインターネットに接続されていることを想定します。

NAS は有線 LAN で接続する必要があるため、ネットワークスイッチ（ハブ）またはルーターの LAN ポートに接続します。ネットワークの IP アドレスやサブネットマスク、デフォルトゲートウェイ、DNS サーバーの情報は、DHCP（動的ホスト構成プロトコル）サーバーを兼ねるルーターから自動割り当てされることを想定します。



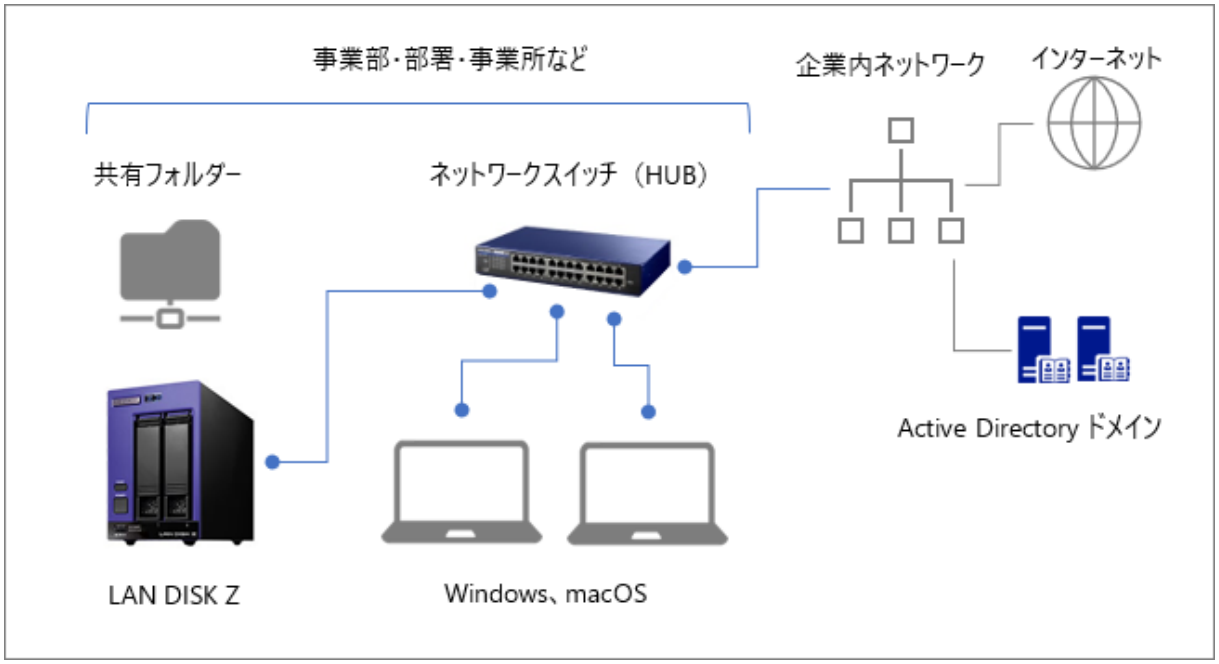
図：小規模な環境のネットワーク構成の例

固定の IP アドレスを手動で割り当てる場合は、NAS 用の以下の情報を予め決めておいてください。

設定項目	設定値
NAS のコンピューター名	（例：WINNAS01）
NAS の IP アドレス	（例：192.168.10.201）
サブネットマスク	（例：255.255.255.0）
デフォルトゲートウェイの IP アドレス	（例：192.168.10.1）
DNS サーバーの IP アドレス	（例：192.168.10.1）

中・大規模環境（ドメインネットワーク）への導入

中・大規模な Active Directory ドメインネットワークに NAS を導入する場合は、NAS に割り当てるネットワークの構成情報、Active Directory ドメインの情報を IT 部門の担当者に確認してください。管理対象として把握するために、サーバー用途のデバイスには固定の IP アドレスを割り当てるのが一般的です（DHCP による自動割り当ても可能です）。



図：中・大規模な Active Directory ドメインネットワークに NAS を導入する場合のネットワーク構成例

NAS は Active Directory ドメインのメンバーサーバーとしてドメインに参加させることを想定します。ドメインに参加させることで、ドメインのユーザーやドメインのグループによる共有フォルダーへのアクセス許可を設定できます。Active Directory ドメインの場合、DNS サーバーは通常、DNS サーバーを兼ねている 1 台以上のドメインコントローラーを参照するように構成します。ドメインユーザーの資格情報（ユーザー名とパスワード）は、ドメイン参加設定をするために必要です。

設定項目	設定値
NAS のコンピューター名	（例：WINNAS01）
NAS の IP アドレス	（例：192.168.10.201）
サブネットマスク	（例：255.255.255.0）
デフォルトゲートウェイの IP アドレス	（例：192.168.10.1）
DNS サーバー1 の IP アドレス	（例：192.168.1.10）
DNS サーバー2 の IP アドレス	（例：192.168.1.11）
Active Directory のドメイン名	（例：ad.example.jp）
ドメインユーザーの資格情報（一般ユーザーでよい）	（例：AD¥user01）

IT 担当部門に内緒の設置（いわゆる野良 NAS）は厳禁！

その企業の規則にもよりますが、通常、IT 部門が存在する企業において、IT 部門が把握しないデバイスを社内ネットワークに接続することは許可されません。企業において適切に管理されていないデバイスが存在することは、セキュリティ侵害や情報漏洩、社内ネットワークの障害など、重大なインシデントにつながるリスクがあります。

管理用端末について

このホワイトペーパーでは、導入や管理作業を行う端末として、NAS と同じネットワーク上に Windows 10（Windows 8.1 でも可）の PC が利用できることを想定しています。

NAS の初期設定を行う際、Windows 標準の［リモートデスクトップ接続］クライアント（Mstsc.exe）を使用します。利用可能な Windows PC が無い場合は、Mac コンピューター（macOS） 、スマートフォン

やタブレット端末（Android、iOS）で利用可能なマイクロソフト純正のアプリが各デバイスのオンラインストアから無料で入手できます。

リモート デスクトップ クライアント
https://docs.microsoft.com/ja-jp/windows-server/remote/remote-desktop-services/clients/remote-desktop-clients

NAS の電源をオンにしたあとに NAS を含むネットワークデバイスを発見するツールとして、アイ・オー・データから［Magical Finder（マジカルファインダー）］というツールが無料提供されています。以下のサイトから Windows 用、macOS 用、iOS 用、Android 用のソフトウェアをダウンロードできます。

Magical Finder
https://www.iodata.jp/r/3022.htm

2. 設置から初期構成まで

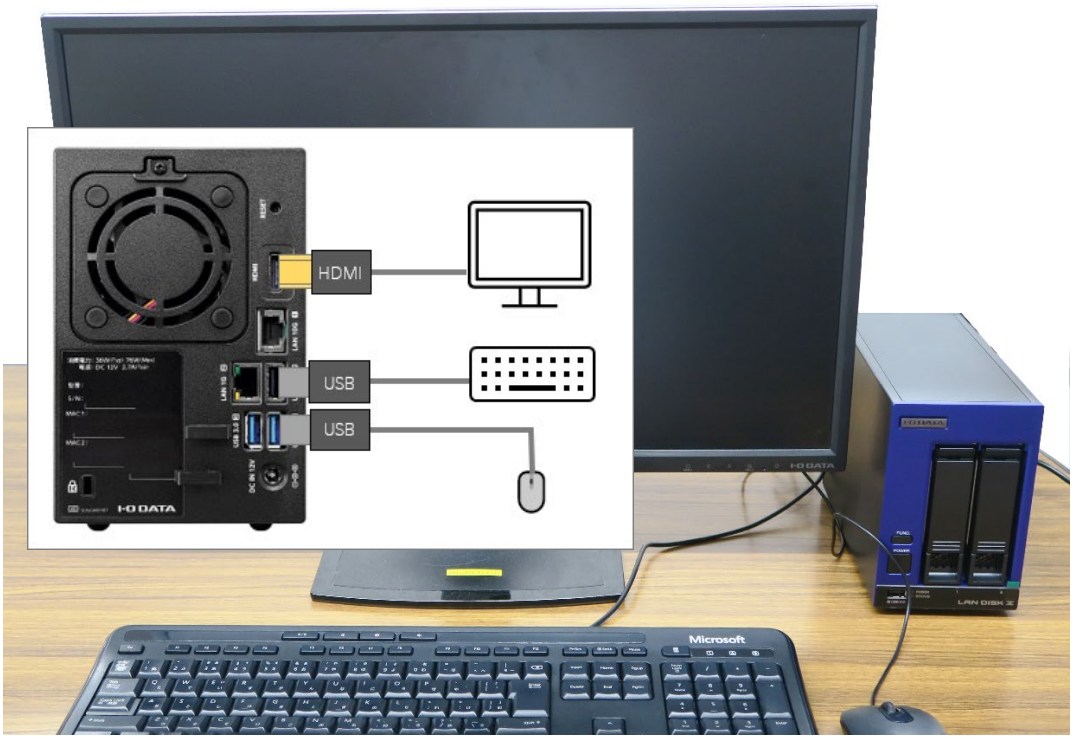
Windows Server IoT 2019 for Storage 搭載 NAS の利用を開始するために、最低限の初期設定を行います。NAS はヘッドレスのデバイスであるため、初期段階ではネットワーク上の NAS を発見し、リモートデスクトップ接続経由で NAS のコンソール（Windows Server のデスクトップ）にアクセスして作業するか、NAS に一時的にキーボード、ディスプレイ、マウスを接続してローカルコンソールを利用可能にして作業します。ここでは Windows 10 PC からのリモートデスクトップ接続経由でのセットアップ手順で説明します。

写真：NAS を LAN に接続し、リモートデスクトップ接続経由でコンソールにアクセスし初期設定を行う

ローカルコンソールの準備（推奨）

NAS の初期設定にローカルコンソールは必須ではありませんが、準備しておくことをお勧めします。ローカルコンソールは、初期設定の他、ネットワーク障害への対応 OS ディスクの障害時のミラーディスクからの起動選択、バックアップからのシステムの復元などで一時的に必要になることがあります。ローカルコンソールの目的はメンテナンス作業のためであり、常時接続することは避けてください。

ローカルコンソールのためには、HDMI コネクタ接続のディスプレイ、USB キーボード、および USB マウスが必要です。これらの機器を NAS 専用に用意する必要はありません。デスクトップ PC で利用しているものなどを一時的に代用できれば構いません。なお、D-Sub や DVI コネクタのディスプレイしか用意できない場合は、HDMI 変換アダプターや変換ケーブル（参考製品、アイ・オー・データ DA-ADH/V、GP-HDDVI）で安価に対応できます。



写真／図：NAS にキーボード、ディスプレイ、マウスを接続し、ローカルコンソールを利用可能にして作業する。必須ではないが、障害対応時にあると役立つので準備しておくことを推奨

2.1　LAN への接続

はじめて NAS を設置する場合は、まず、NAS の **LAN 10G** とラベルされた LAN ポートを、企業内の既存のネットワークスイッチ（ハブ）のポートに LAN ケーブル（カテゴリ 6 以上を推奨）で接続し、NAS の電源アダプター／ケーブルを **DC IN** に接続して、NAS 前面の電源（**POWER** ラベル）ボタンを押し、電源を

投入します。

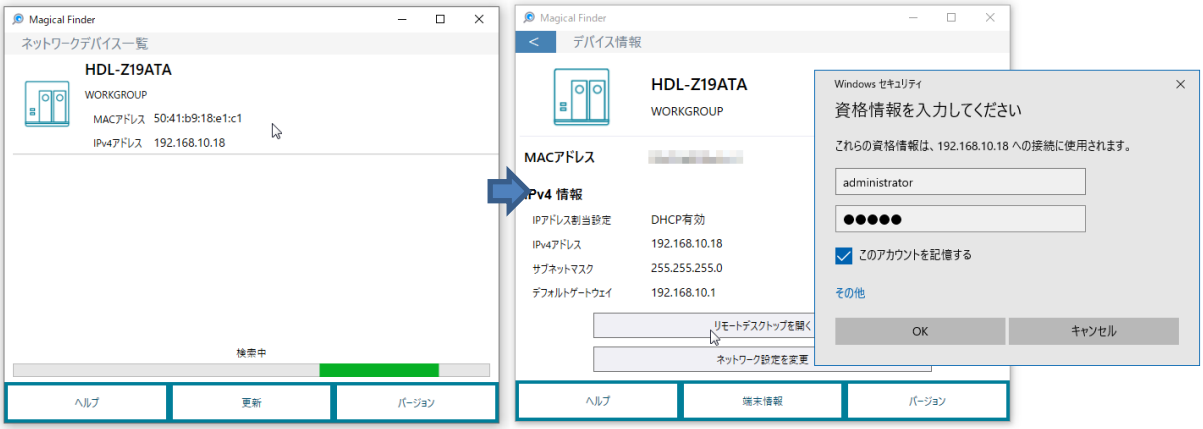
LAN 10G とラベルされた LAN ポートは 10GBASE-T、5GBASE-T、2.5GBASE-T、1000BASE-T、100BASE-TX に対応しているため、一般的なネットワークスイッチの場合はこちらのポートを使用してください。10Mbps の低速なハブを使用している場合は、もう 1 つの **LAN 1G** とラベルされた LAN ポートを使用してください。こちらは、1000BASE-T、100BASE-TX、10BASE-T に対応しています。

写真：LAN 10G ポートとネットワークスイッチ（ハブ）間を LAN ケーブル（カテゴリ 6 以上を推奨）で接続する

2.2　Magical Finder で NAS を発見する

同じネットワーク（ネットワークスイッチを介して接続される同じネットワークセグメント）にある Windows 10 PC に、ダウンロードして展開した Magical Finder（MagicalFinder.exe）を起動します。

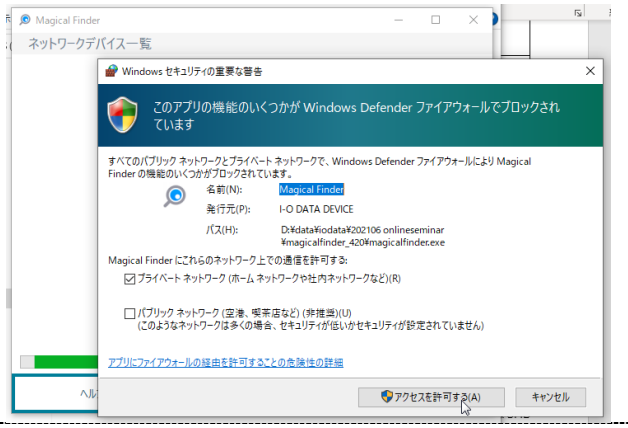
Magical Finder はネットワーク上に NAS を発見すると、[ネットワークデバイス一覧] に表示します。発見された NAS をクリックし、[リモートデスクトップを開く] をクリックして、NAS にリモートデスクトップ接続で管理者としてログオンします。工場出荷時の管理者の資格情報は、ユーザー名「Administrator」、パスワード「admin」です。



画面：Magica lFinder で NAS を発見し、リモートデスクトップ接続で Administrator としてログオンする

［Windows セキュリティの重要な警告］が表示されたら･･･

［Windows セキュリティの重要な警告］ダイアログボックスに、「このアプリの機能のいくつかが Windows Defender ファイアウォールでブロックされています」と表示され、Magical Finder の機能がブロックされる場合は、「プライベートネットワーク（ホームネットワークや社内ファイアウォールなど)」を選択して、［アクセスを許可する］をクリックします。



画面：この警告ダイアログボックスが表示されたら、［アクセスを許可する］をクリックする

2.3　リモートデスクトップ接続経由で初期設定を行う

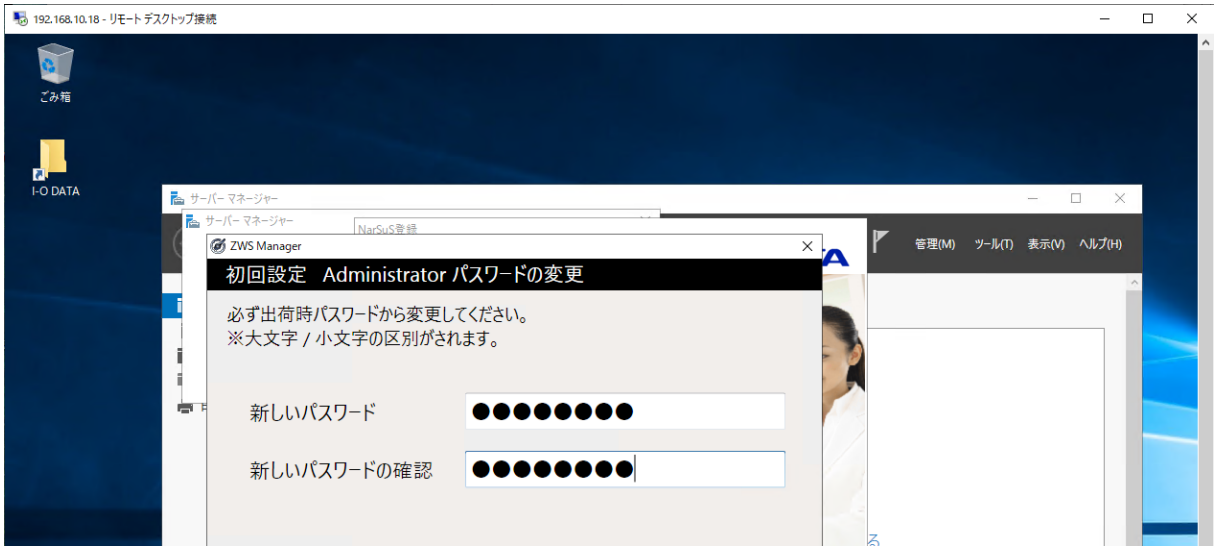
NAS にリモートデスクトップ接続経由で Administrator としてログオン（またはローカルコンソールからローカルログオン）すると、画面右側に［ネットワーク］の通知が表示され、「このネットワーク上の他の PC やデバイスがこの PC を検出できるようにしますか？」と問われる場合があります。その場合は、［はい］をクリックしてください。

画面：「このネットワーク上の他の PC やデバイスがこの PC を検出できるようにしますか？」と問われた場合は［はい］をクリックする

管理者（Administrator）パスワードの変更

NAS にログオンすると、通常版の Windows Server 2019 と共通のデスクトップ画面が表示されます。ただし、HDL-Z シリーズの NAS の場合は、通常版の Windows Server 2019 では出てこないダイアログボックスがいくつか表示されます。［ZWS Manager］が表示する［初回設定　Administrator パスワードの変更］、［初回設定　保証期間の設定］、［初回設定　起動・終了スケジュール設定（スケジュール設定 1）］ダイアログボックスの 3 つと、［NarSuS 登録］ダイアログボックスです。

これらの設定はスキップできますが、設定されるまで毎回のログオン時に表示されます。少なくとも［初回設定　Administrator パスワードの変更］は先に済ませてください。工場出荷時の既定の管理者パスワードを変更することは、セキュリティ上、極めて重要なことです。その他の設定についてはこのホワイトペーパーでは省略します。適宜、必要に応じて設定してください。



画面：Administrator のパスワードは、できるだけ速やかに変更すること

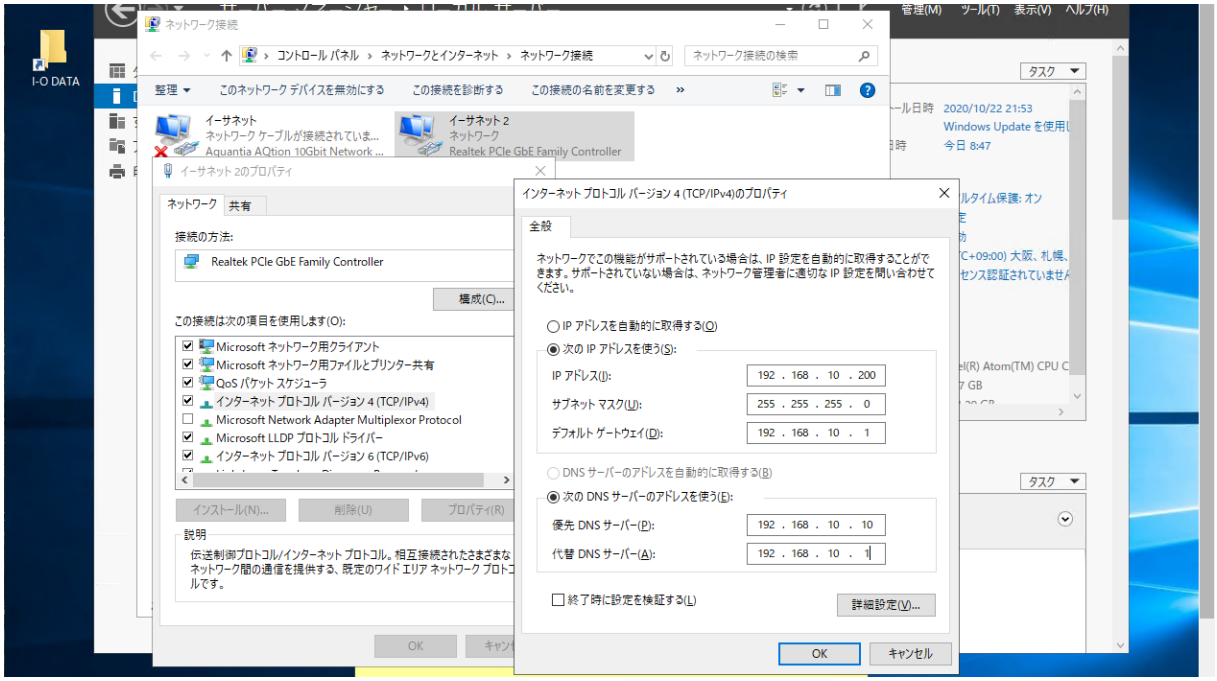
管理者パスワードを変更したら、自動開始した［サーバーマネージャー］の［ローカルサーバー］を開き、リモート管理のための最低限の初期設定を開始します。

画面：［サーバーマネージャー］で初期設定を行う

IP アドレスの設定

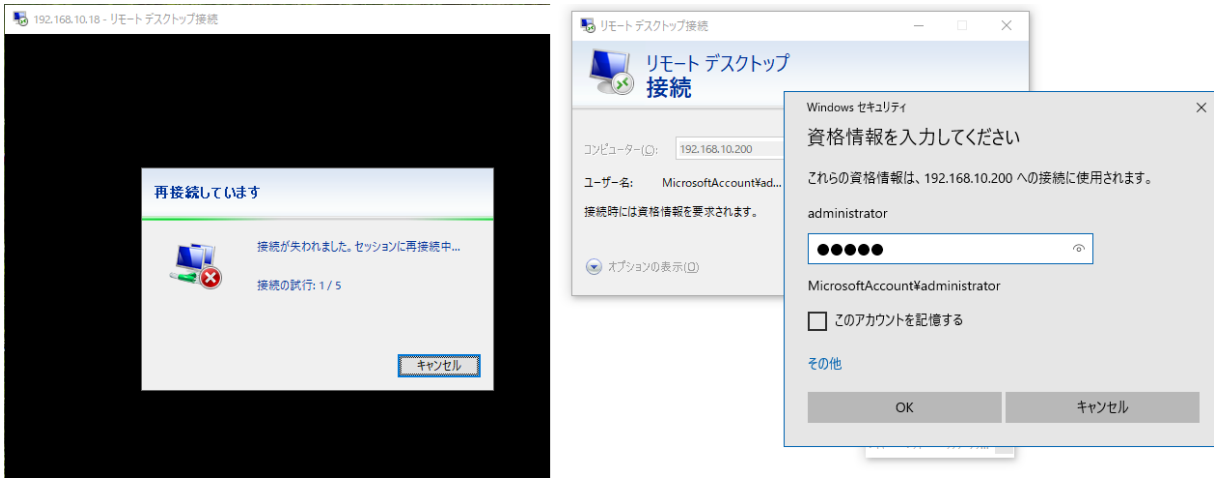
既定では、NAS は DHCP（動的ホスト構成プロトコル）によって自動的に IP ネットワークの設定が行われ、ネットワーク上で利用可能になります。そのままでも利用に支障はありませんが、固定の IP アドレスの割り当てを受け（または決定して）、手動で設定することもできます。DHCP で自動割り当てするか（既定のまま）、固定の IP アドレスを手動で設定するかは、社内のルールに従ってください。

固定の IP アドレスを手動で設定する場合は、［サーバーマネージャー］の［ローカルサーバー］を開き、DHCP で自動構成されたネットワークインターフェイス（前出の画面の［イーサネット 2］のすぐ横のリンク）の現在の設定値をクリックしてコントロールパネルの［ネットワーク接続］を開いて、対象のネットワークインターフェイスのプロパティを開きます。イーサネットプロトコルバージョン 4（TCP/IPv4）］のプロパティをさらに開いて、［次のアドレスを使う］を選択し、IP アドレス（必須）、サブネットマスク（必須）、デフォルトゲートウェイ（必須）、優先 DNS サーバー（必須）、代替 DNS サーバー（オプション）を適切に設定し、［OK］をクリックしてすべてのダイアログボックスを閉じます。



画面：固定の IP アドレスとネットワークパラメーターを適切に設定する

IP アドレスを変更すると、現在のリモートデスクトップ接続は切断されるので、Magical Finder を更新して新しい IP アドレスを再検出させ、再接続してください。または、リモートデスクトップ接続クライアント（Mstsc.exe）を起動して、新しい IP アドレスを直接指定して接続してください。

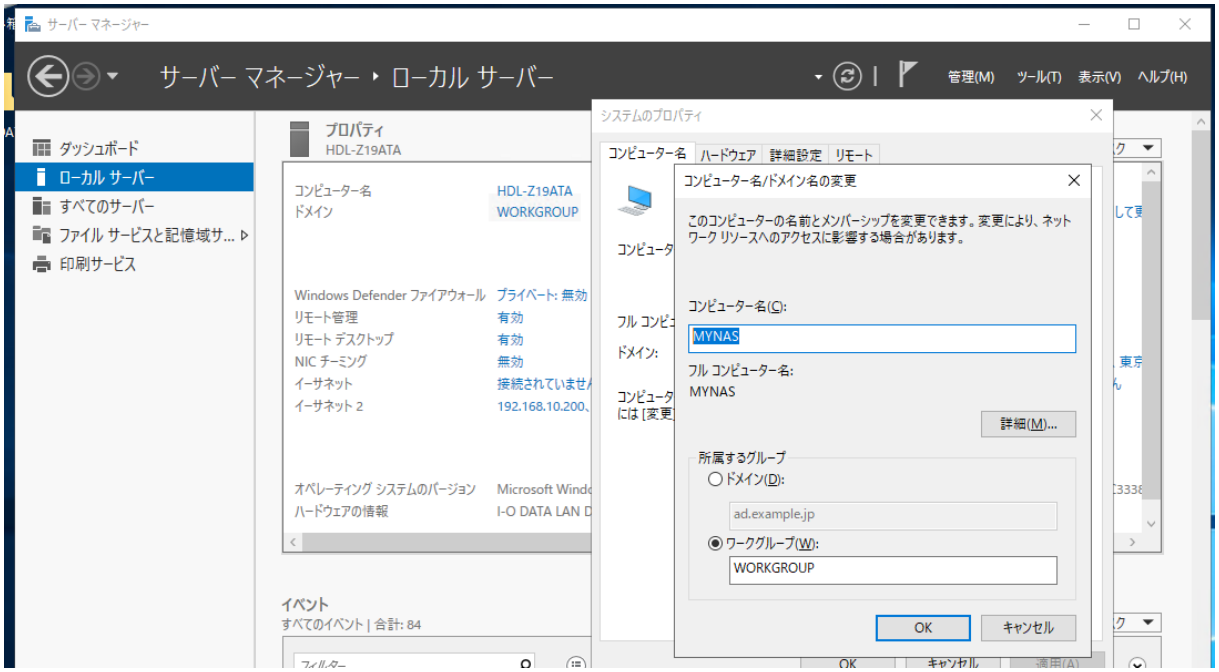


画面：IP アドレスを変更すると現在の接続は失われ、自動的に再接続されることはないので、[キャンセル] をクリックして、新しい IP アドレスで接続しなおす

コンピューター名の変更

NAS の共有フォルダーには、コンピューター名または IP アドレス（IPv4 アドレス）で接続することができます。単一のネットワークセグメントのシンプルなネットワークの場合、Windows では LLMNR（Link-Local Multicast Name Resolution）という IPv6 の名前解決が利用可能であり、ローカルネットワークに DNS の名前解決環境がなくてもコンピューター名で IPv6 アドレス（通常、自動構成される）に名前解決できます。そのため、NAS を識別できる、わかりやすいコンピューター名に変更しておくことをお勧めします。

コンピューター名を変更するには、[サーバーマネージャー] の [ローカルサーバー] で現在のコンピューター名をクリックします。すると、[システムのプロパティ] ダイアログボックスが表示されるので、[コンピューター名] タブにある [変更] をクリックして新しいコンピューター名を設定します。なお、コンピューター名の変更には、NAS（Windows Server）の再起動が必要です。



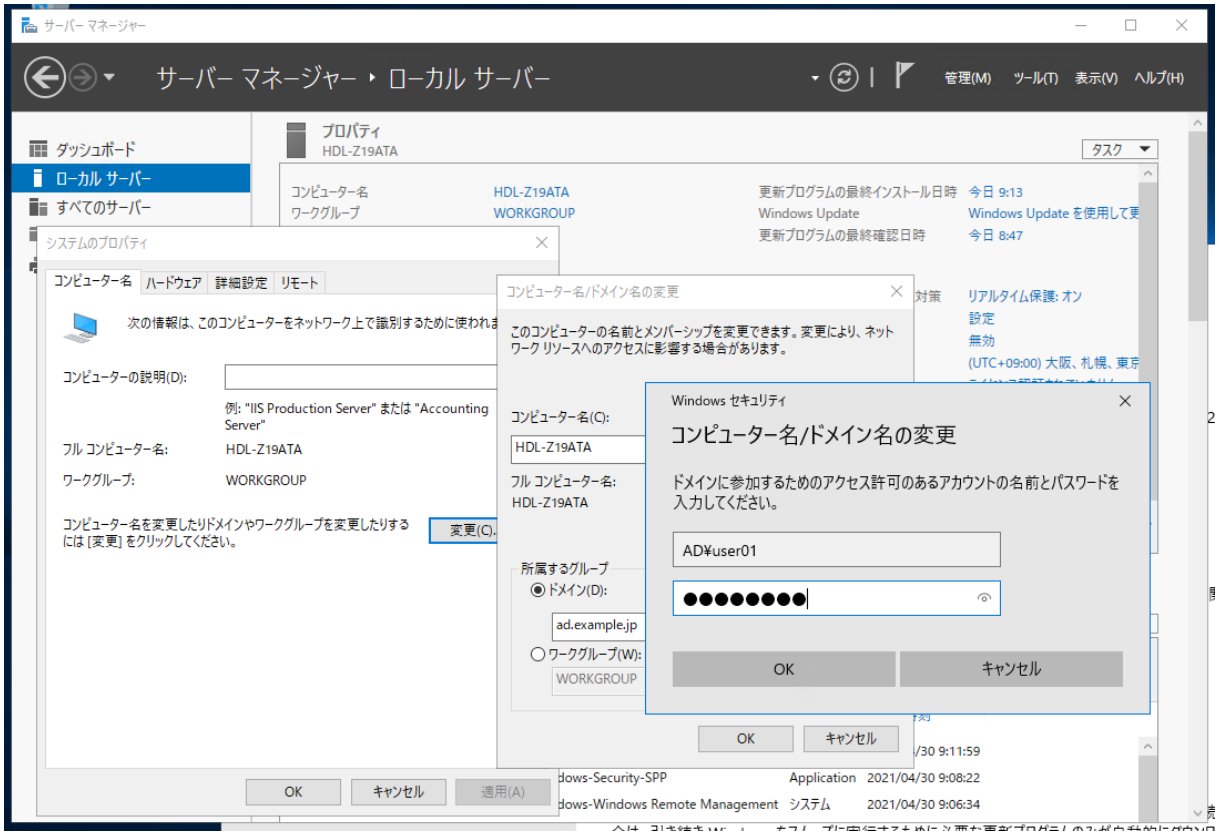
画面：NAS のコンピューター名を変更する

ドメインへの参加設定（Active Directory ドメインに導入する場合のみ）

NAS を Active Directory ドメイン環境に導入する場合は、コンピューター名の変更と同時に、ドメインへの参加設定を行います（ドメインの参加設定を後から行うこともできます）。

ドメインへの参加設定を行うには、コンピューター名の変更と同じダイアログボックスで [所属するグループ] として [ドメイン] を選択し、ドメインの FQDN ドメイン名（例：ad.example.jp）または NetBIOS ドメイン名（例：AD）を入力します。このとき、ドメイン参加時に資格情報が求められるので、有効なドメインアカウントの資格情報を入力します。ドメインアカウントは、ドメインの管理者アカウント（ドメイン名¥Administrator）である必要はなく、一般ユーザー（Domain Users グループのメンバー）で構いません。

コンピューター名の変更、およびドメインへの参加設定を完了するには、コンピューター名の変更には、NAS（Windows Server）の再起動が必要です。



画面 : NAS をドメインのメンバーとして設定する。ドメインに参加する際、ドメインアカウントによる認証が要求される

DNS サーバーに IPv4 アドレスを指定しても参照されないのは自動構成された IPv6 の可能性

最近のルーターは IPv4 と IPv6 の両方の IP スタックに対応しており、パブリックな IPv6 インターネットに接続されているかどうかに関わらず、RA（Router Advertisement）として社内ネットワークのための IPv6 ネットワークを自動構成する場合があります。Windows は IPv4 と IPv6 の両方に対応しており、既定では利用可能な場合 IPv6 を優先します。そのため、社内に IPv4 の DNS サーバーを設置して Windows や Windows Server から参照するように設定したとしても、IPv6 に構成された IPv6 の DNS サーバー（通常、ルーターの IPv6 アドレス）が名前解決に使用され、社内ネットワークの名前解決に問題が発生することがあります。

IPv6 が優先されることで名前解決の問題が発生している疑いがある場合は、以下のコマンドラインを［コマンドプロンプト（管理者として実行）］で実行し、再起動後に問題が軽減されるかどうかを確認してください。

```
C:¥> REG ADD "HKLM¥SYSTEM¥CurrentControlSet¥Services¥Tcpip6¥Parameters" /v DisabledComponents /t REG_DWORD /d 32 /f ↲

C:¥> SHUTDOWN /r /t 0 ↲
```

問題が継続する場合は別の原因の可能性があります。以下のコマンドラインを実行して再起動すると、

既定の設定（IPv6 を優先）に戻ります。

```
C:¥>  REG  ADD  "HKLM¥SYSTEM¥CurrentControlSet¥Services¥Tcpip6¥Parameters"  /v DisabledComponents /t REG_DWORD /d 32 /f ↲

C:¥> SHUTDOWN /r /t 0 ↲
```

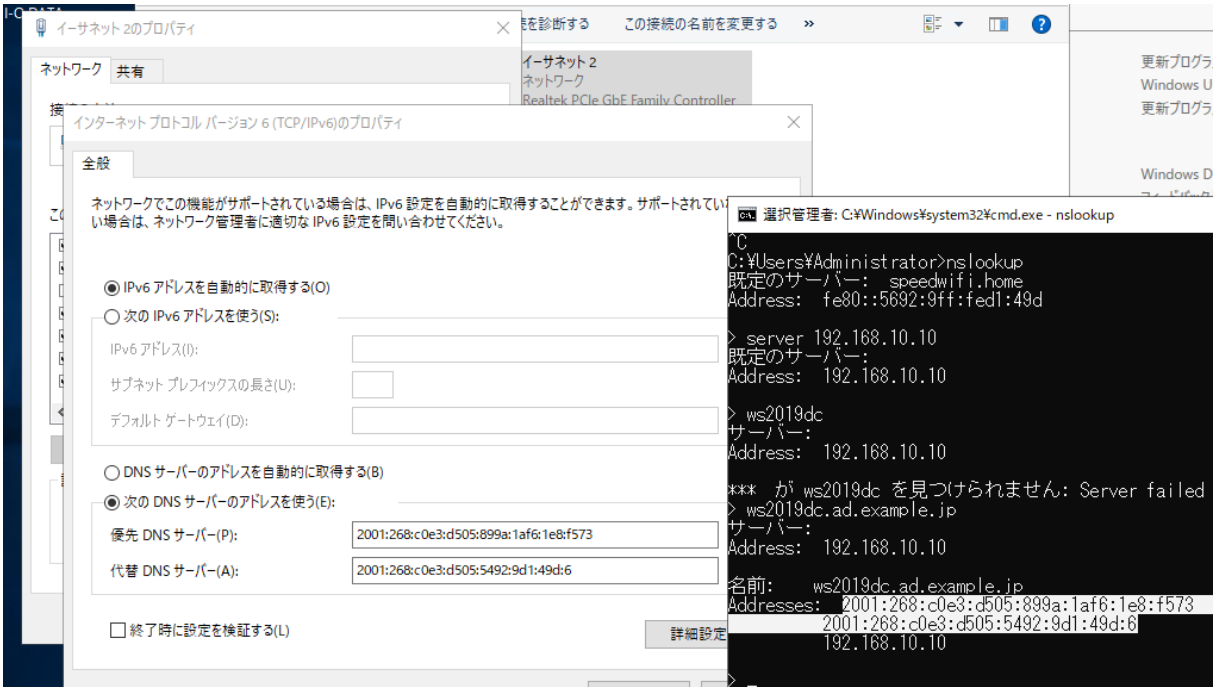
Active Directory ドメインコントローラーの IP アドレスを DNS サーバーに設定しているのにも関わらず、ドメインが見つからない、ドメインコントローラーに接続できないといったエラーが発生する場合は、ブロードバンドルーターの IPv6 アドレスを DNS サーバーの参照先として使用している場合があります。その場合は、ドメインコントローラーの IPv6 アドレスを IPv6 の DNS サーバーに手動で設定してください。

ドメインコントローラーの IPv6 アドレスを調べるには、nslookup コマンドを利用できます。

```
C:¥> nslookup ↲

> server «ドメインコントローラーの IPv4 アドレス» ↲

> «ドメインコントローラーの FQDN» ↲
```



画面：ドメインコントローラーの IPv6 アドレスを調べ、DNS サーバーの参照先に設定する

Windows Update で最新状態に更新

Windows Server IoT 2019 for Storage は、ソフトウェアとしては通常版の Windows Server 2019 と共

通です。Windows Server は、セキュリティと安定性の維持のために少なくとも毎月 1 回提供される更新プログラムをインストールして最新状態にしておくことが重要です。[サーバーマネージャー] の [ローカルサーバー] で [Windows Update] の横のリンクをクリックし、検出されたすべての更新プログラムをできるだけ速やかにインストールしてください。

更新プログラムのインストールを完了するには、NAS（Windows Server）の再起動が必要です。

画面：初回の Windows Update を実施し、すべての更新プログラムをダウンロード、インストールする

3. Windows Admin Center の導入

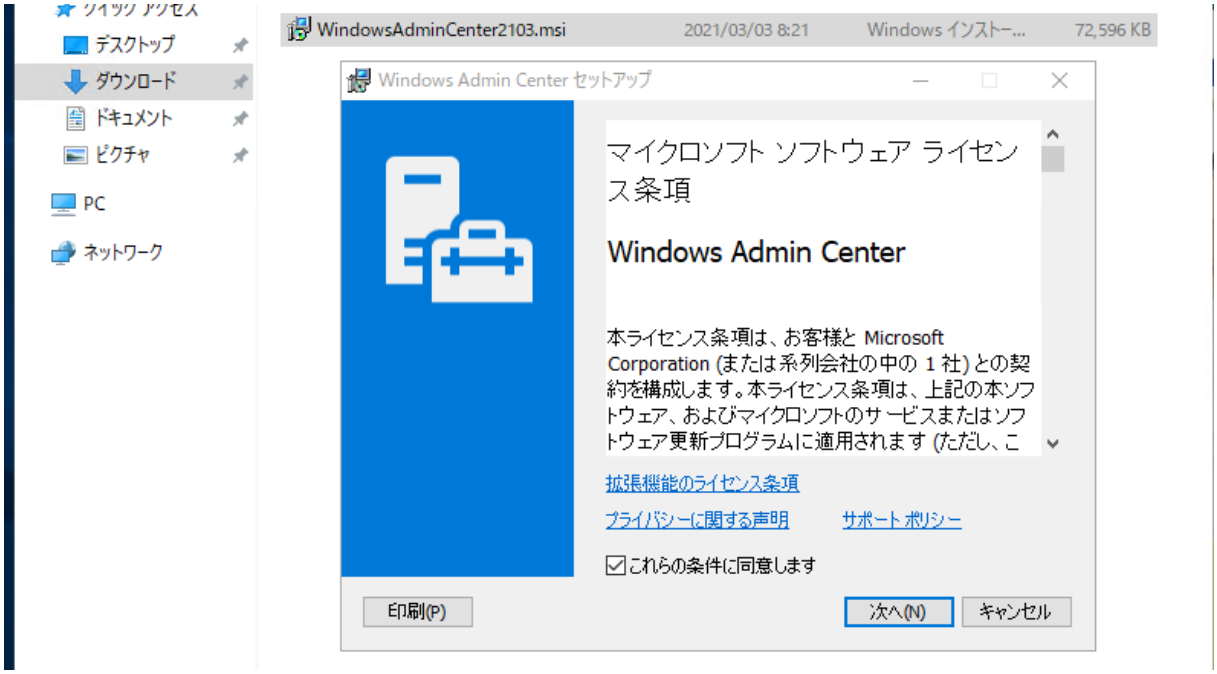
NAS の初期設定および Windows Update が完了したら、Windows Admin Center をインストールします。Windows Admin Center をインストールすると、その後の管理作業のほとんどは、クライアント PC の Web ブラウザーから Windows Admin Center に接続して実施できるようになります。

3.1 Windows Admin Center のインストール

NAS にリモートデスクトップ接続で Administrator の資格情報を使用してログオンし、以下の場所から Windows Admin Center の最新バージョンのインストーラー（Windows Admin Center バージョン 2103.2 の場合は WindowsAdminCenter2103.2.msi）をダウンロードします。

Windows Admin Center 最新バージョンのダウンロード
https://aka.ms/WACDownload

Windows Admin Center のインストーラーをダブルクリックして実行し、[Windows Admin Center のセットアップ] に従ってインストールします。

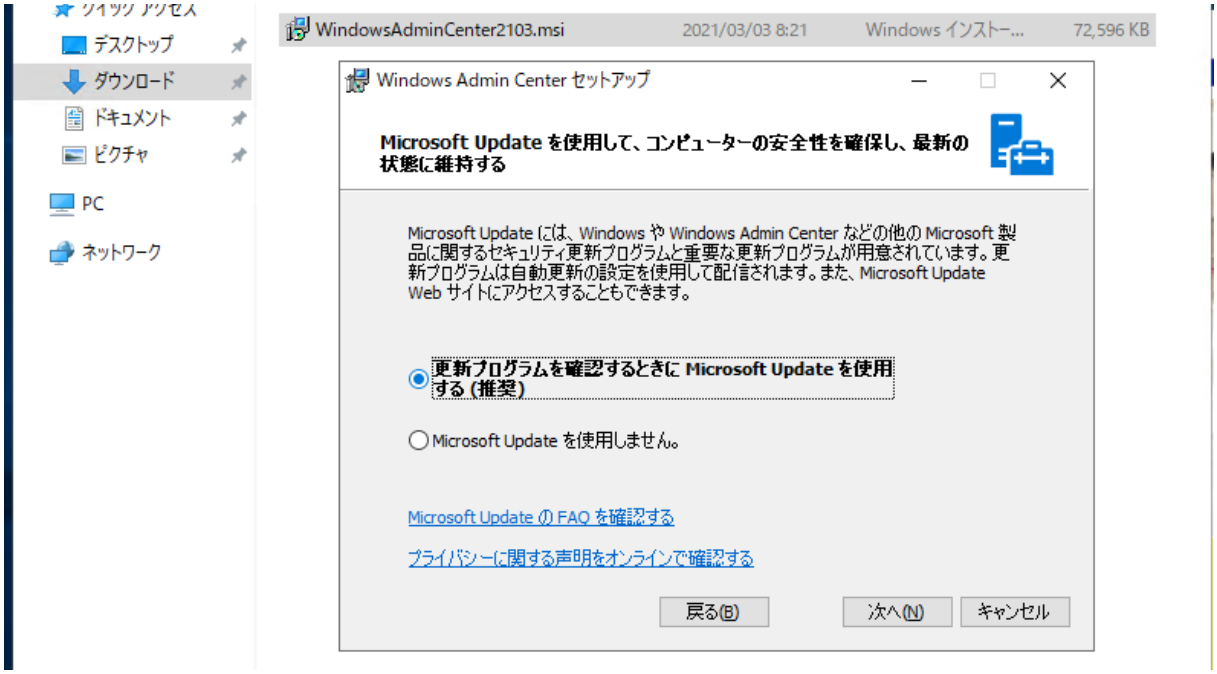


画面：Windows Admin Center のインストールを開始する

インストールでは、ほとんどの項目は既定の設定および選択のまま進んでください。以下に出てこない画面はすべて［次へ］をクリックして進んで下さい。

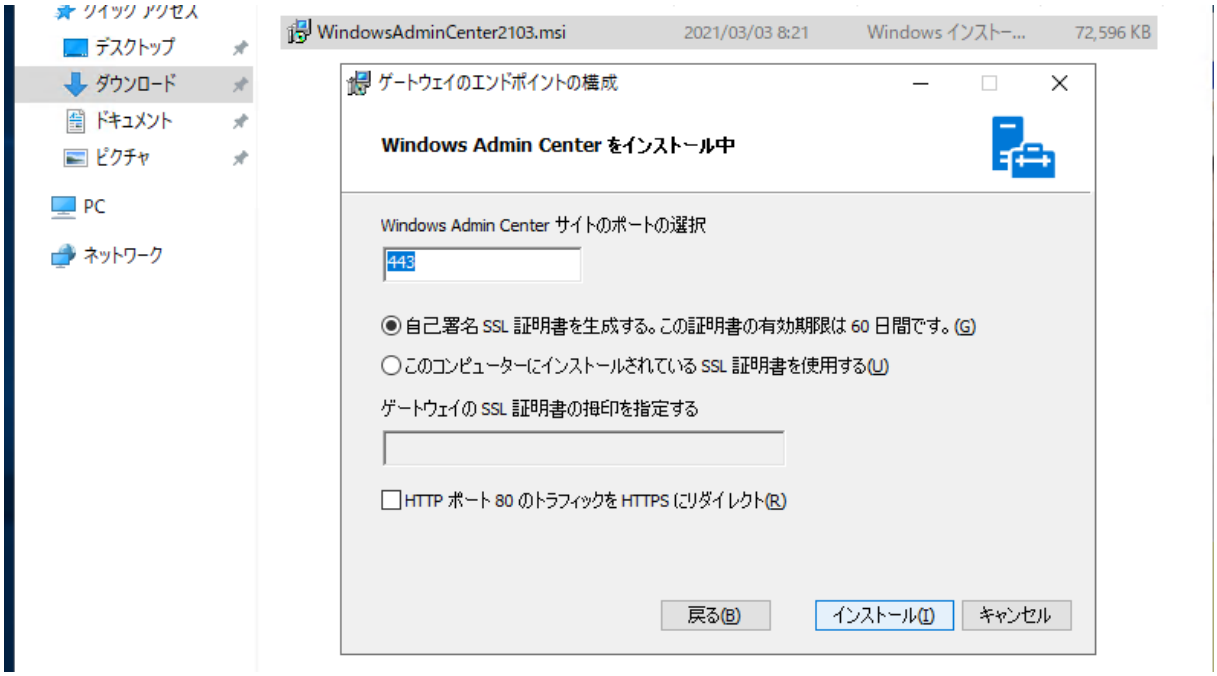
1 つだけポイントがあるとすれば、Microsoft Update を使用するかどうかの設定で［更新プログラムを確認するときに Microsoft Update を使用する（推奨）］を選択することです。

Windows Admin Center は概ね半年ごとに新メジャーバージョンがリリースされます。また、既知の問題を修正するマイナーバージョンがリリースされることもあります。Microsoft Update を使用するように構成しておくと、Windows Update を通じて新バージョンに更新できるという利点があります。なお、既に Microsoft Update を使用するように Windows Update が構成されている場合、この設定画面は表示されません。また、Microsoft Update を使用するように構成しなくても、Windows Admin Center が備える自動更新機能と通知機能により、最新バージョンに更新できます。



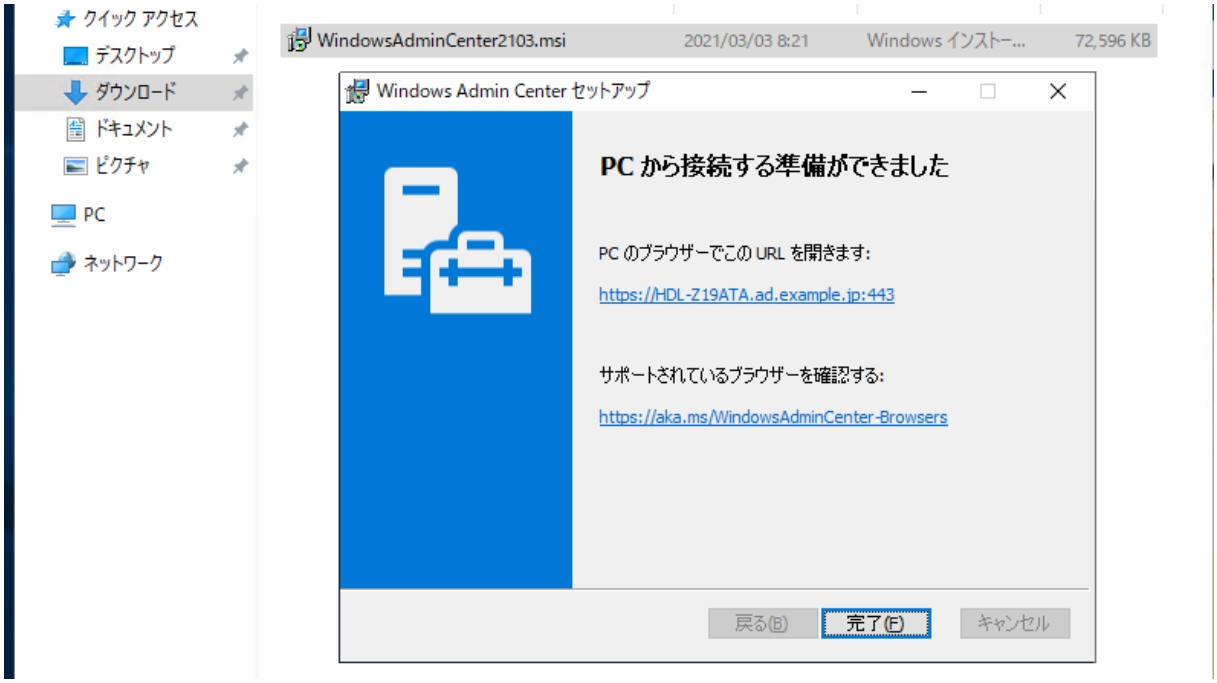
画面：Microsoft Update を使用するように選択する

Windows Admin Center はデスクトップモードとゲートウェイモードの 2 つのインストールタイプがあります。Windows Server IoT 2019 for Storage の NAS にインストールする場合、ゲートウェイモードとして適切にインストールされ、HTTPS ポート（443）で自己署名証明書を使用して Windows Admin Center のアプリがホストされることになります。



画面：NAS に Windows Admin Center をインストールする場合、HTTPS（443）ポートでホストされる

インストールが完了したら、最後の画面でアクセス先の URL を確認しておきます。ワークグループ構成の場合は **https://コンピューター名:443/**（:443 は省略可能）、Active Directory ドメインに参加している場合は **https://コンピューター名.FQDN ドメイン名:443/**（:443 は省略可能）になります。



画面：インストーラーの最後の画面でアクセス先の URL を確認する

3.2　管理用端末から Windows Admin Center に接続する

Windows 10 標準の Microsoft Edge（Chromium ベース）、その他のプラットフォームの Microsoft Edge（Chromium ベース）、Google Chrome、Mozilla Firefox（Firefox はテストされていませんが利用可能です）など、最新のモダンブラウザーから利用できます。

Windows Admin Center にアクセスするには、Windows Admin Center のインストール時に確認した URL をブラウザーで開きます。

自己署名証明書を使用しているため証明書エラーが表示されますが、エラーを無視して続行してください。Microsoft Edge の場合は、［接続がプライベートではありません］と表示されるので、［詳細設定］をクリックし、［https://･･･に進む（安全ではありません）］をクリックします。

画面：自己署名証明書のエラーが表示される

画面：自己署名証明書のエラーを無視して続行する

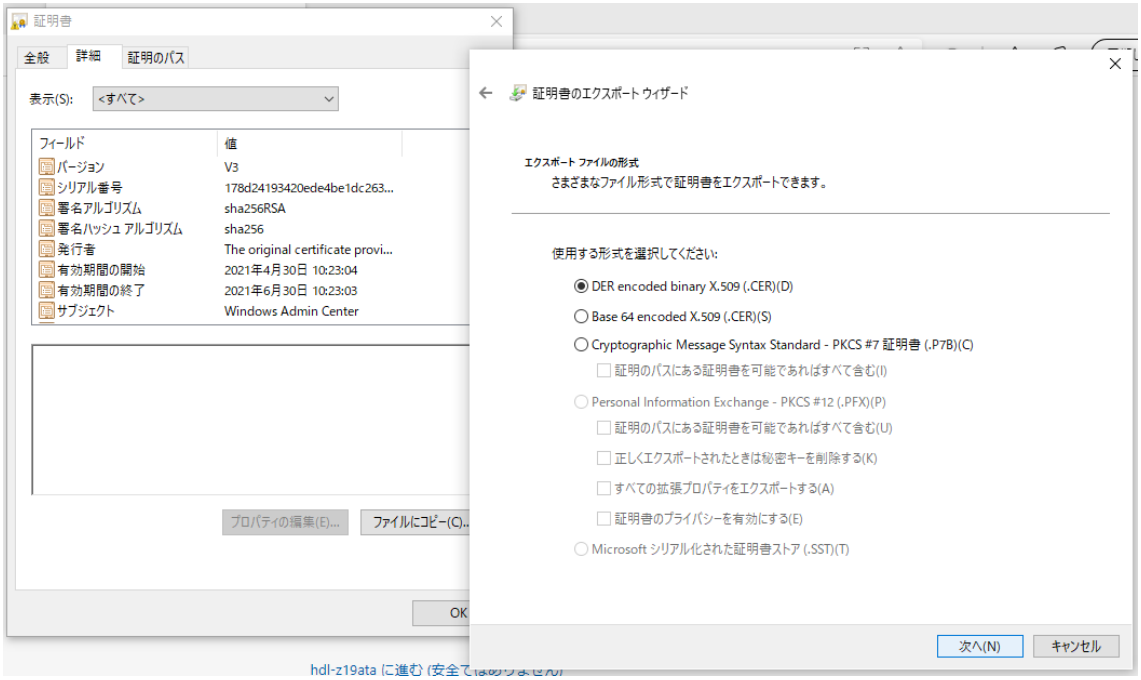
証明書のエラーを回避するには

ゲートウェイモードの Windows Admin Center を自己署名証明書でセットアップした場合、証明書エラーが表示されますが、使用される自己署名証明書をローカル（現在のユーザーまたはコンピューター）の［信頼されたルート証明機関］にインストールすることで、自己署名証明書を信頼し、証明書エラーを回避することができます。

Windows 10 の Microsoft Edge の場合は、次の手順で証明書をインストールします。

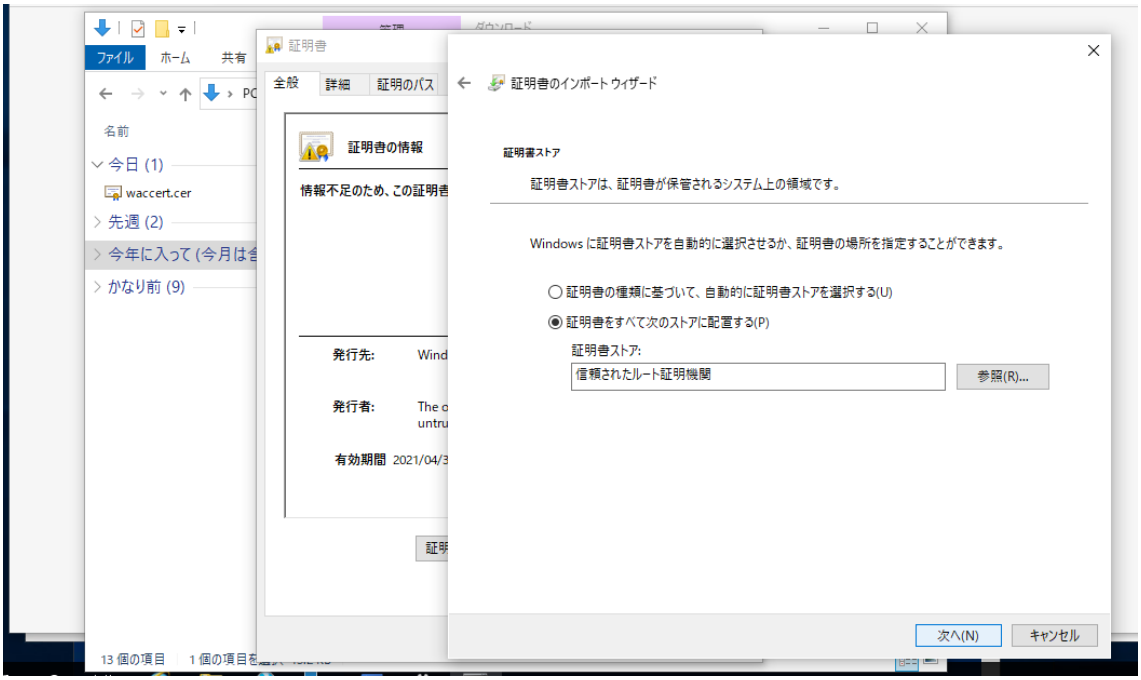
1. Windows Admin Center サイトに接続し、アドレスバーにある［証明書エラー］をクリックして、［証明書の表示］をクリックします。

2. ［証明書情報］が表示されるので、［ファイルにエクスポート］をクリックして、デスクトップまたは任意の場所に X.509 証明書ファイル形式（.cer）でエクスポートします。



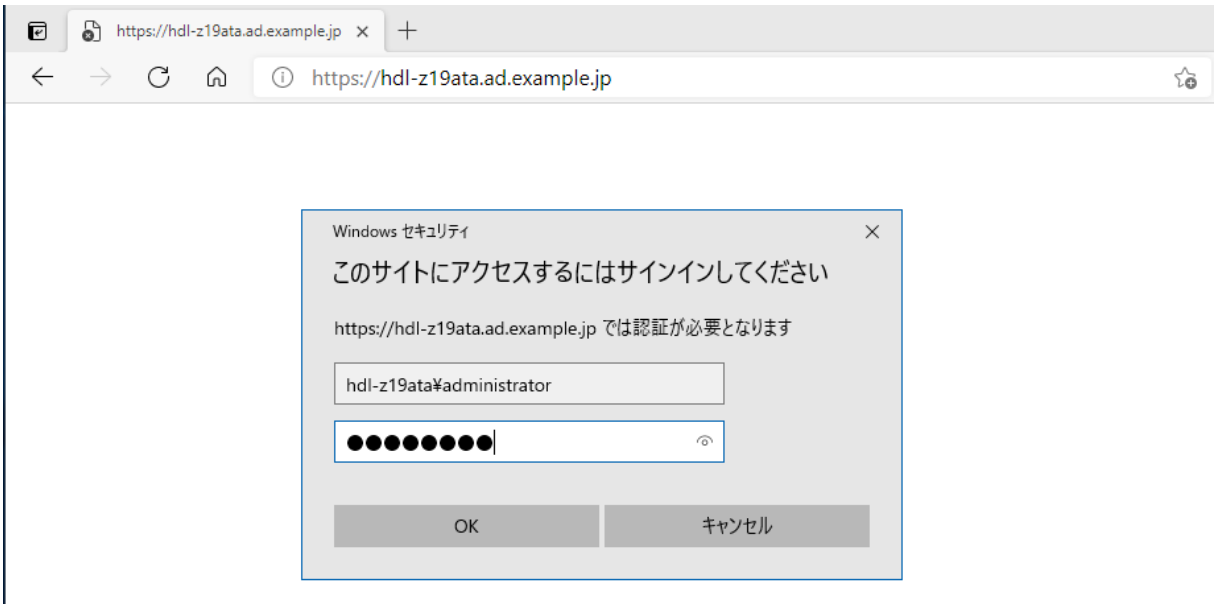
3. エクスポートした証明書ファイルをダブルクリックして開き、［証明書のインストール］をクリックします。

4. ［証明書のインポートウィザード］が開始するので、保存場所として［現在のユーザー］を選択し、証明書ストアとして［信頼されたルート証明機関］を選択して証明書をインストールします。



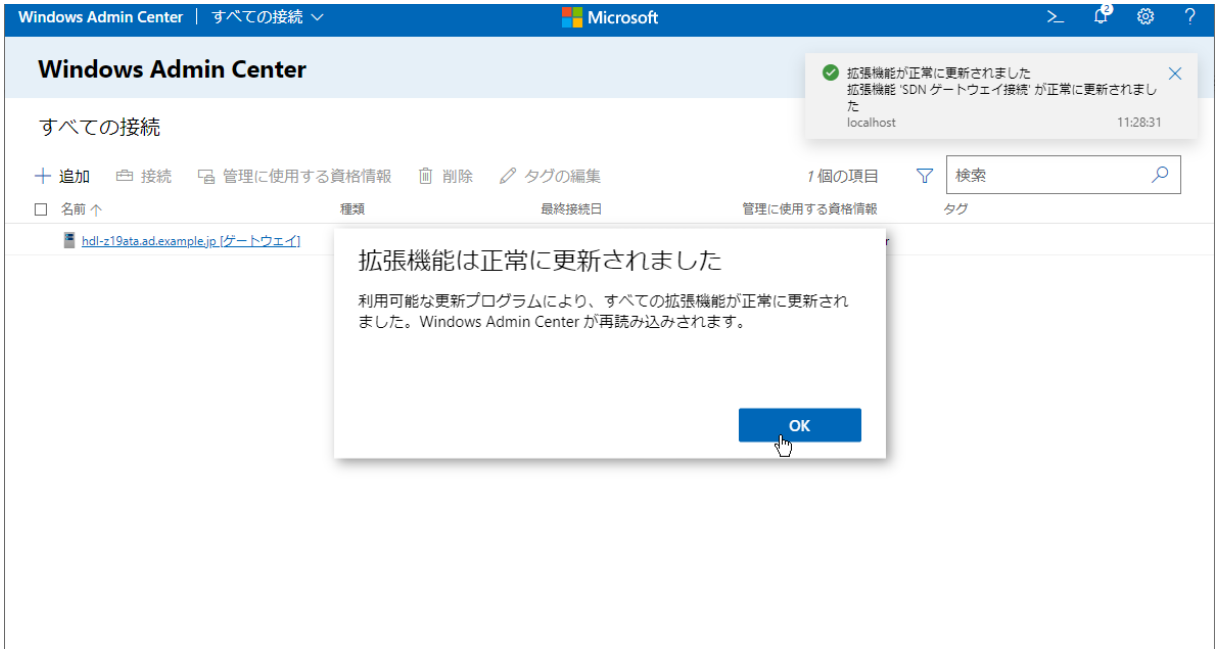
5. Web ブラウザーをいったん閉じ、再び開始して、Windows Admin Center サイトに接続し、証明書エラーが解消されたことを確認します。ページの再読み込みだけでは証明書エラーは解消しないので、必ず Web ブラウザー（参照中の他のタブを含めて）をいったん終了してください。

初回接続時に［Windows セキュリティ］ダイアログボックスがポップアップするので、NAS の管理者アカウント（Administrator）の資格情報を入力してください。



画面：初回接続時、NAS の管理者アカウントの資格情報を入力する

Windows Admin Center をインストール後にはじめてアクセスする場合、拡張機能が自動的に更新され、最新状態になります（再読み込みされます）。NAS を管理するには、［すべての接続］の一覧から「NAS のコンピューター名または FQDN（ゲートウェイ）」をクリックして開きます。



画面：Windows Admin Center のトップ画面

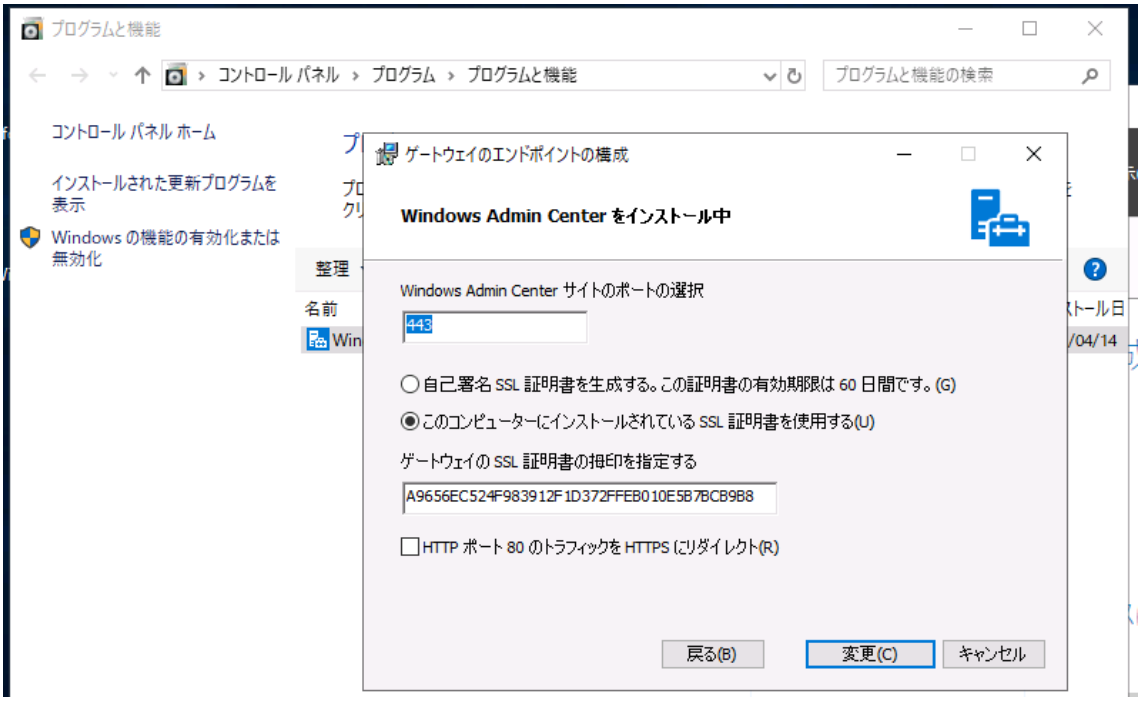
なお、Windows Server IoT 2019 for Storage に標準搭載されている Internet Explorer を使用して Windows Admin Center にアクセスすることはできません。Microsoft Edge や Google Chrome、Mozilla Firefox などのモダンブラウザーを NAS にインストールすればアクセスできますが、NAS へのアプリの追加はそのアプリを最新に維持するための更新作業を増やすことになり、現実的ではありません。

自己署名証明書の更新

Windows Admin Center のインストール時に生成される自己署名証明書の有効期限は 60 日です。有効期限が切れると、HTTPS 接続は証明書エラーになります。有効期限切れの証明書エラーを解消するには、次の手順に従って新たな有効期限を持つ自己署名証明書を再生成します。

それには、コントロールパネルの［プログラムと機能］にある［プログラムのアンインストールまたは変更］を開き、インストール済みの Windows Admin Center を選択して［変更］をクリックします。

1. ［Windows Admin Center セットアップ］ウィザードが開くので、最初の画面で［次へ］をクリックします。
2. ［インストールの変更、修復、または削除］の画面で［変更］をクリックします。
3. ［Windows Admin Center をインストール中］の画面で［自己署名 SSL 証明書を生成する。この証明書の有効期限は 60 日間です。］を選択します。その他の項目はそのままで［変更］をクリックします。



4. 最後の画面で［完了］をクリックしてウィザードを閉じます。

4. 共有フォルダーのセットアップ

NAS の主な機能は、NAS の大きな記憶域を活用したファイル共有です。言い換えれば、共有フォルダーをセットアップして初めて NAS としての利用価値が生まれます。

Windows Server IoT 2019 for Storage における共有フォルダーのセットアップには、通常版の Windows Server 2019 と同じであり、［サーバーマネージャー］、［エクスプローラー］、NET SHARE コマンド、PowerShell（New-SmbShare コマンドレットなど）など、さまざまな手段を利用できます。しかし、Windows Server に慣れていない人にとって、これらの方法ははどれもハードルの高い手順です。

ここでは直観的に簡単に、そして完全にリモートから実施できる、Windows Admin Center を利用した手順で説明します。

4.1 ユーザーとグループの準備

ファイル共有環境では、ユーザー認証によるアクセス制御が重要です。共有フォルダーを作成する前に、共有フォルダーを利用するユーザーとグループを準備します。

ユーザーは共有されたファイルやフォルダーに誰がアクセスできるのか、できないかを決めるアクセス制御（読み取り、変更）の基本要素です。共有フォルダーにアクセスする利用者ごとに個別のユーザーを用意しておくことで、細かなアクセス制御が可能になり、セキュリティ侵害や情報漏洩時の調査にも役立ちます。なお、NAS を Active Directory ドメインに参加させている場合は、NAS でのユーザー（ローカルユーザー）の作成は不要です。

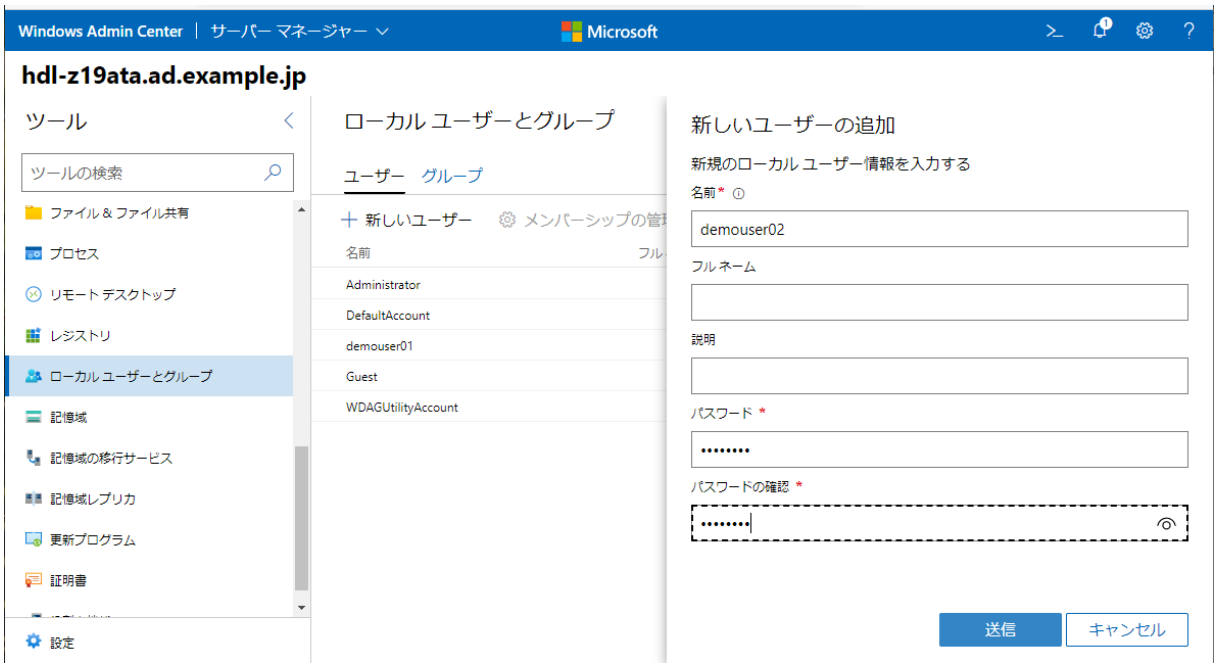
グループはアクセス制御のためのアクセス許可の効率的な設定を可能にします。個別ユーザーに対する許可を設定するよりも、特定の範囲（部署や役職）のユーザーをまとめたグループによる一括設定の方が管理しやすくなります。なお、NAS を Active Directory ドメインに参加させている場合は、NAS 側に準備したグループ（ローカルグループ）に Active Directory のドメインユーザーアカウントまたはドメイングループを追加して、グループでアクセス制御を行います。共有フォルダーのアクセス許可をドメイングループに対して直接設定することもできます。

すべての利用者が単一のユーザーアカウントを使用して共有フォルダーにアクセスできるようにしたり、ユーザー認証なしで（匿名アクセスで）共有フォルダーを利用可能にしたりすることも不可能ではありませんが、セキュリティ上するべきではありません。逆に Windows Server と Windows クライアントで匿名アクセスを可能にする設定のほうが複雑です。また、セキュリティ上の理由から、Windows 10 バージョン 1709 以降の Enterprise/Education エディション、および Windows Server 2019 では SMB クライアントの匿名アクセスは既定で無効化されました。

ローカルユーザーの作成（非ドメイン環境のみ）

NAS にローカルユーザーを作成するには、Windows Admin Center で［ローカルユーザーとグループ］ツールを開き、［＋新しいユーザー］をクリックします。［新しいユーザーの追加］で［名前］と［パスワード］、［パスワードの確認］を入力して［送信］をクリックします。

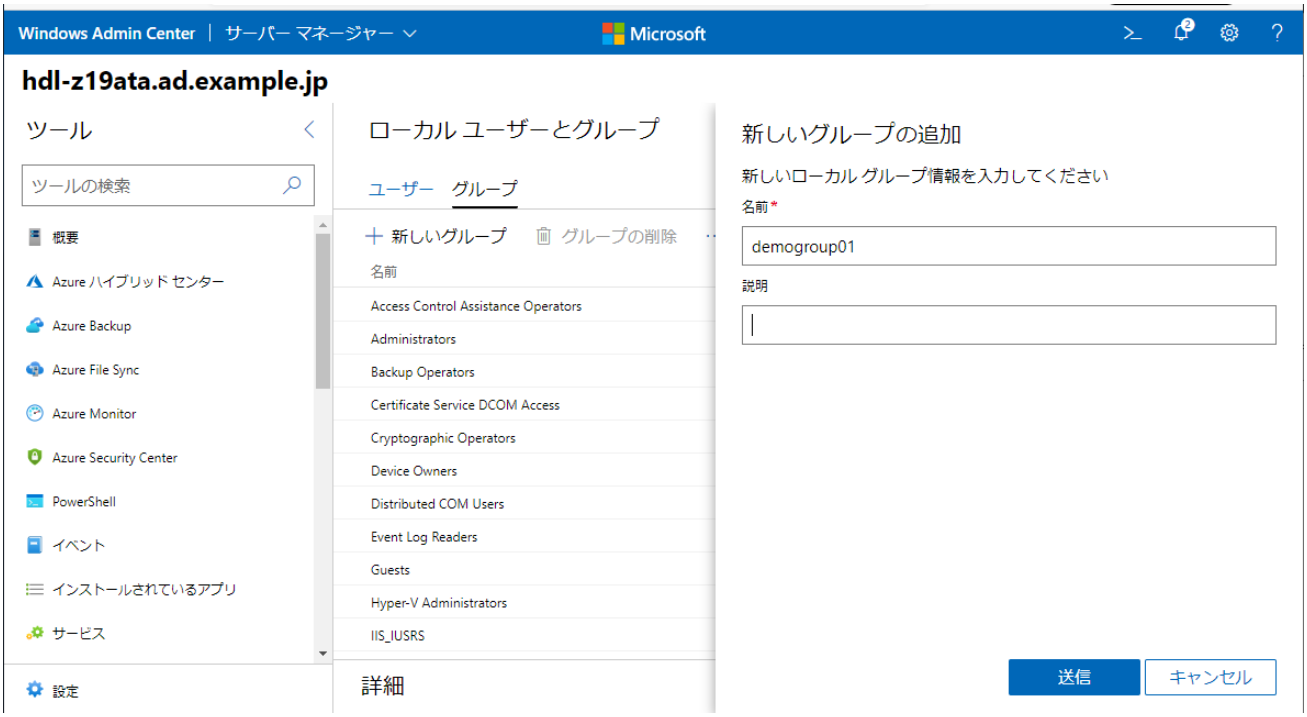
Active Directory ドメイン環境の場合、既存のドメインユーザーアカウントによる認証でアクセス制御ができるので、NAS 側にローカルユーザーの作成は不要です。



画面：NAS にローカルユーザーを作成する

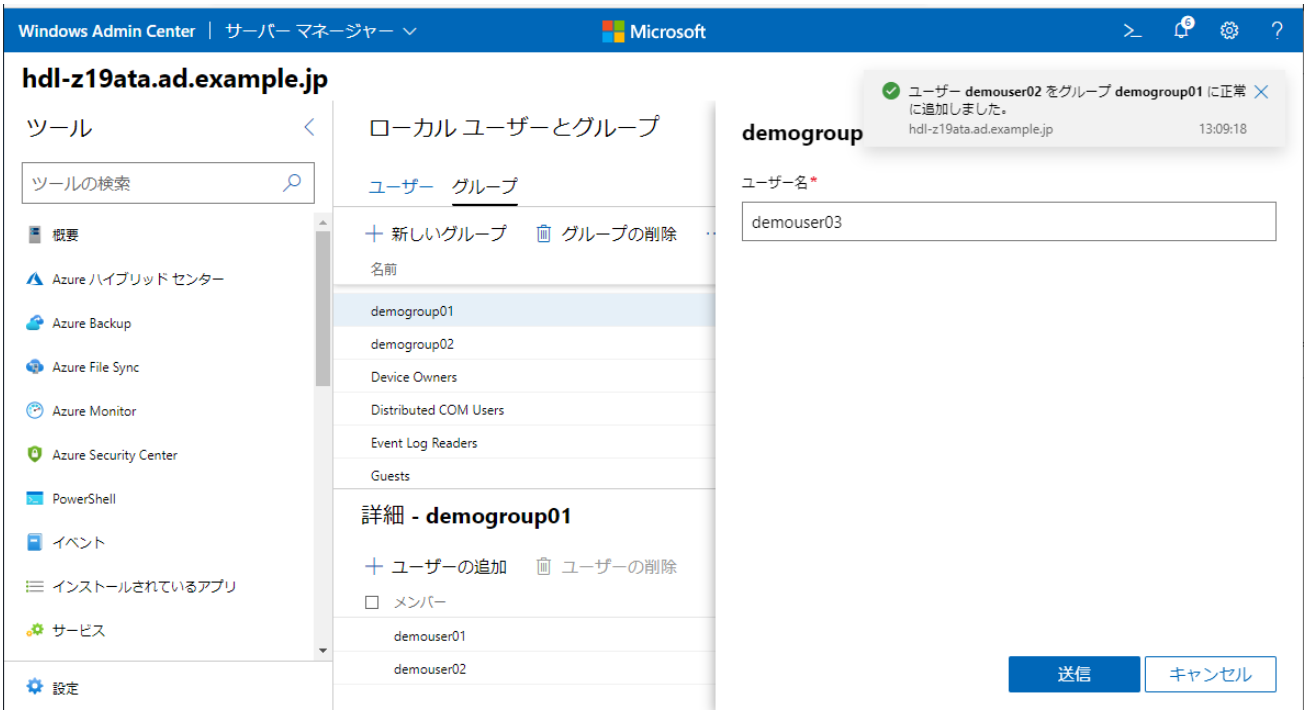
グループの作成

NAS にグループを作成するには、［ローカルユーザーとグループ］の［グループ］タブに切り替え、［＋新しいグループ］をクリックします。［新しいグループの追加］で［名前］を入力し、［送信］をクリックします。



画面：NAS にグループを作成する

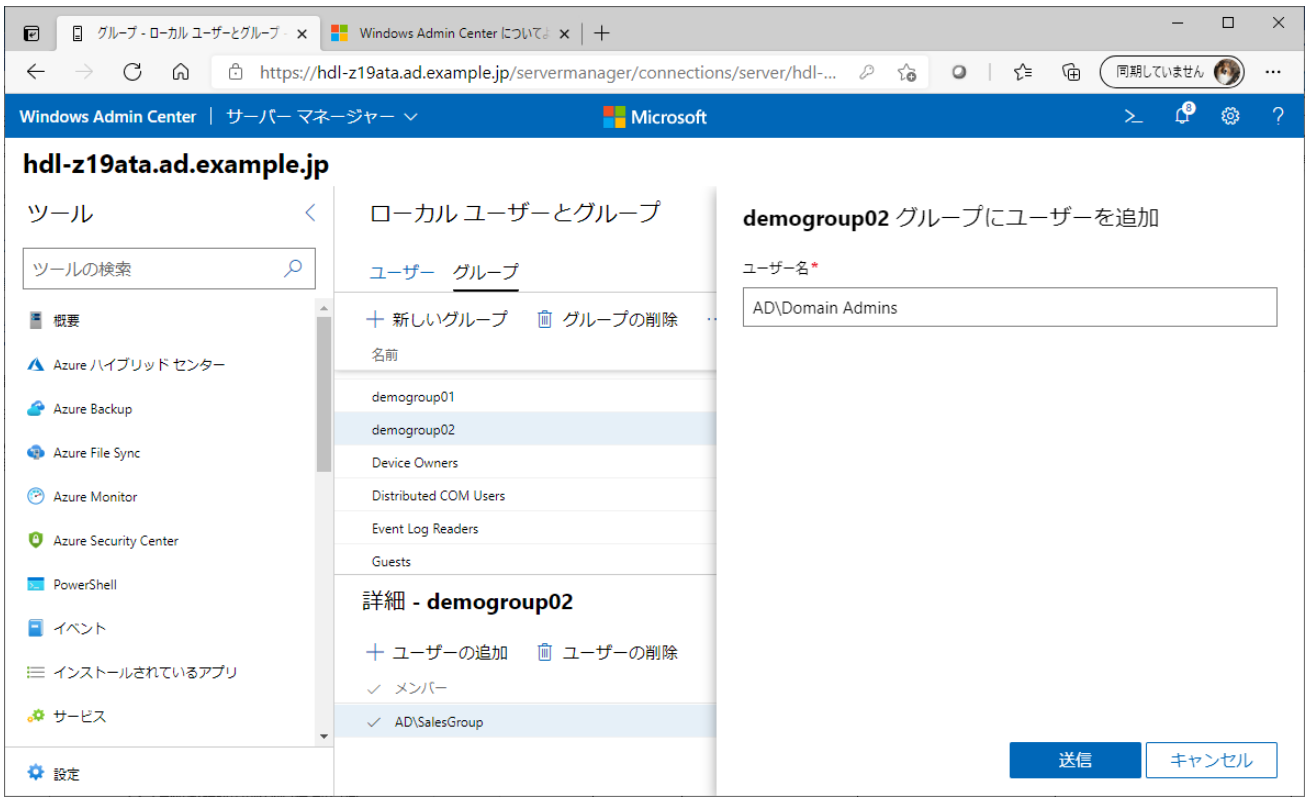
非ドメイン環境の場合は、[グループ] タブの一覧から今作成したグループを選択し、[＋ユーザーの追加] をクリックして、グループに含めるローカルユーザーを追加します。



画面：作成したグループにローカルユーザーを追加する

Active Directory ドメイン環境の場合は、[グループ] タブの一覧から今作成したグループを選択し、[＋ユーザーの追加] をクリックして、グループに含める Active Directory のドメインユーザーアカウントまたはドメイングループを追加します。ドメインアカウントを指定するには **NetBIOS ドメイン名¥アカウント名**

（AD¥GroupName）または**アカウント名@FQDN ドメイン名**（例：username@ad.example.jp）の形式で入力します。



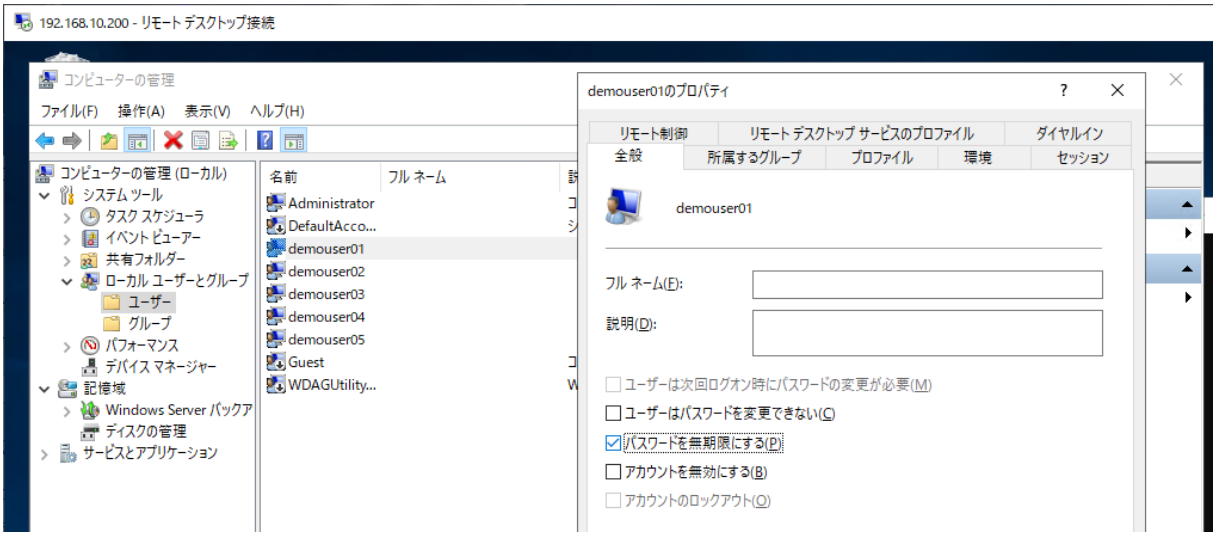
画面：NAS 側のグループに Active Directory のドメイングループまたはドメインユーザーを追加する

パスワードの有効期限を無期限にするには･･･

Windows Admin Center でローカルアカウントを作成した場合、指定したパスワードは 42 日後に有効期限が切れ、パスワードの変更が要求されます。しかし、サーバーにローカルログオンせずに自身のパスワードを変更するためには NAS 側で追加のセキュリティ設定が必要です（「4.4　ワークグループ環境におけるセルフパスワード管理」を参照）。一般ユーザーはリモートデスクトップ接続でのログオンは許可されません。

パスワードの有効期限 42 日は Windows の既定の設定です。有効期限を無期限に設定することで、パスワードの有効期限切れの問題を回避することができます。それには 2 つの方法があります。

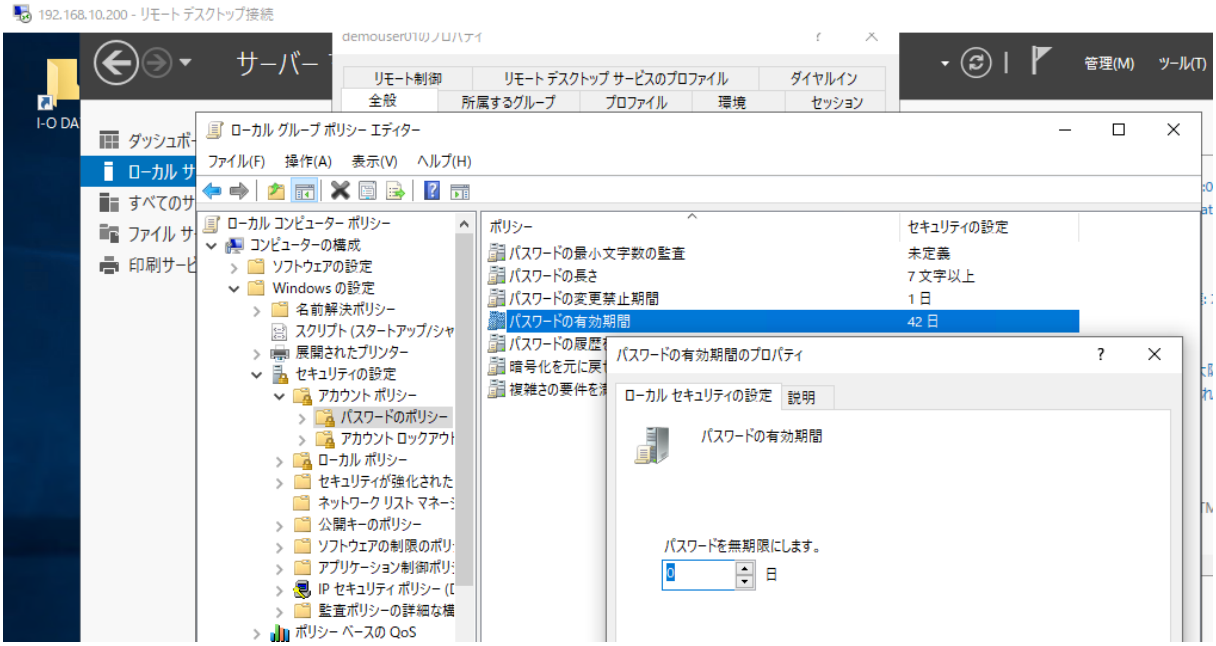
1 つ目の方法は、NAS の［コンピューターの管理］スナップインの［ローカルユーザーとグループ］で各ユーザーのプロパティを開き、［パスワードを無期限にする］をチェックする方法です。そのためには、NAS にリモートデスクトップ接続経由でログオンして作業する必要があります。



画面：各ユーザーのプロパティで［パスワードを無期限にする］をチェックする。ユーザーごとに行う必要がある

2 つ目の方法は、すべてのユーザーのパスワードの有効期限を無期限にする方法です。こちらも NAS にリモートデスクトップ接続経由でログオンして作業する必要があります。［ローカルグループポリシーエディター］スナップイン（Gpedit.msc）を使用して、［コンピューターの構成¥Windows の設定¥セキュリティの設定¥パスワードのポリシー］にある［パスワードの有効期限］を既定の 42 日から **0** 日（無期限）に変更します。この設定により、既に作成済みのユーザーとこれから作成するユーザーの両方でパスワードの有効期限が無期限になります。

なお、Active Directory ドメイン環境の場合は、ドメインのグループポリシー（Default Domain Policy）で［パスワードの有効期限］を設定する必要があります。

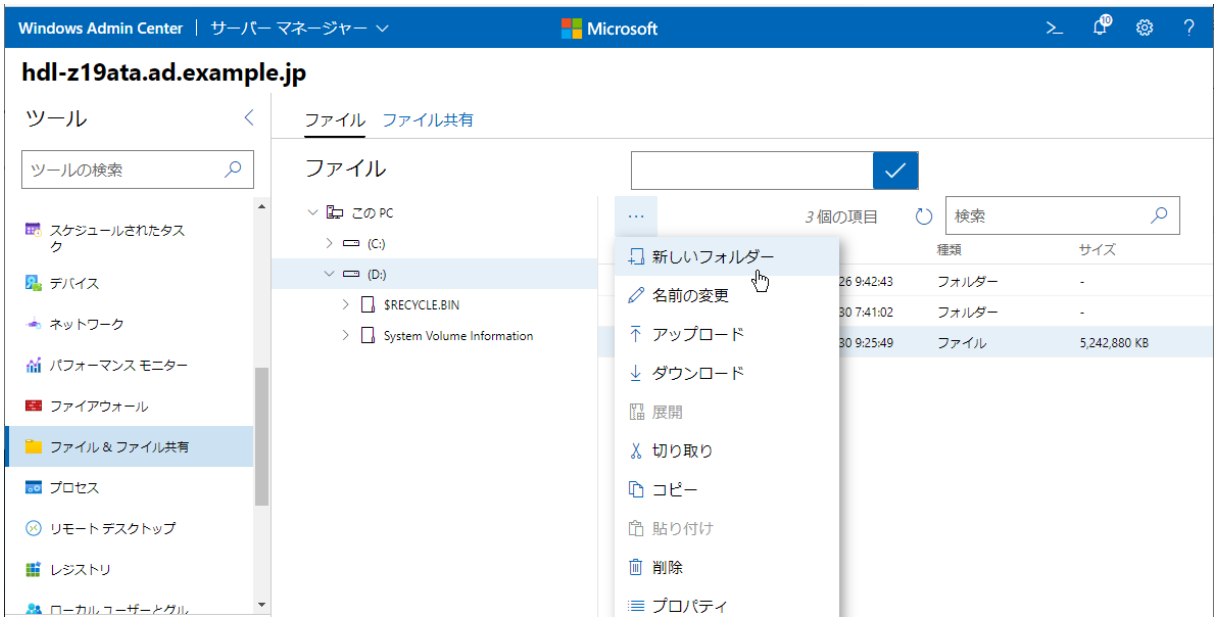


画面：パスワードポリシーでパスワードの有効期限を無期限（0 日）に設定する

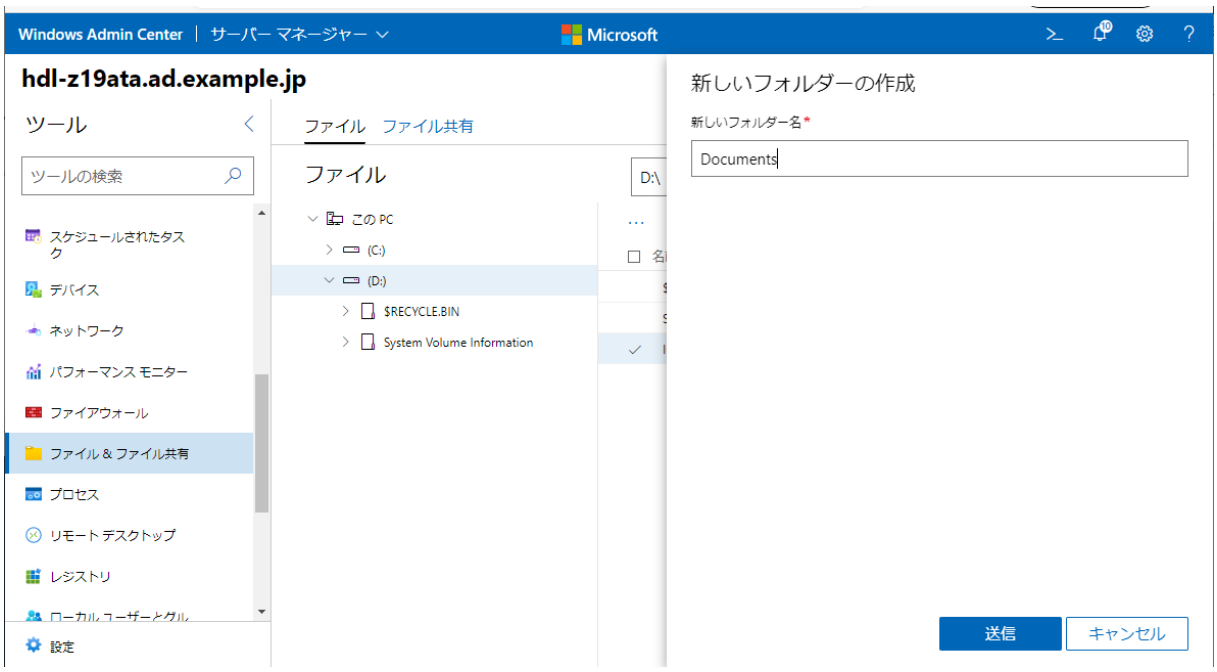
4.2　共有フォルダーの作成

ユーザーとグループを準備したら、続いて共有フォルダーを作成します。ここでは、一例として NAS のデータ用ボリュームである D:ドライブに Documents（D:¥Documents）というフォルダーを作成し、このフォルダーを共有名 Documents として、DemoGroup01 グループのユーザーがフルコントロール（または変更）の権限でアクセスできるようにします。

Windows Admin Center の［ファイル＆ファイル共有］ツールを開きます。［ファイル］タブで D:ドライブを選択し、［･･･｜新しいフォルダー］をクリックし、［新しいフォルダーの作成］で［新しいフォルダー名］に Documents と入力して、［送信］をクリックします。

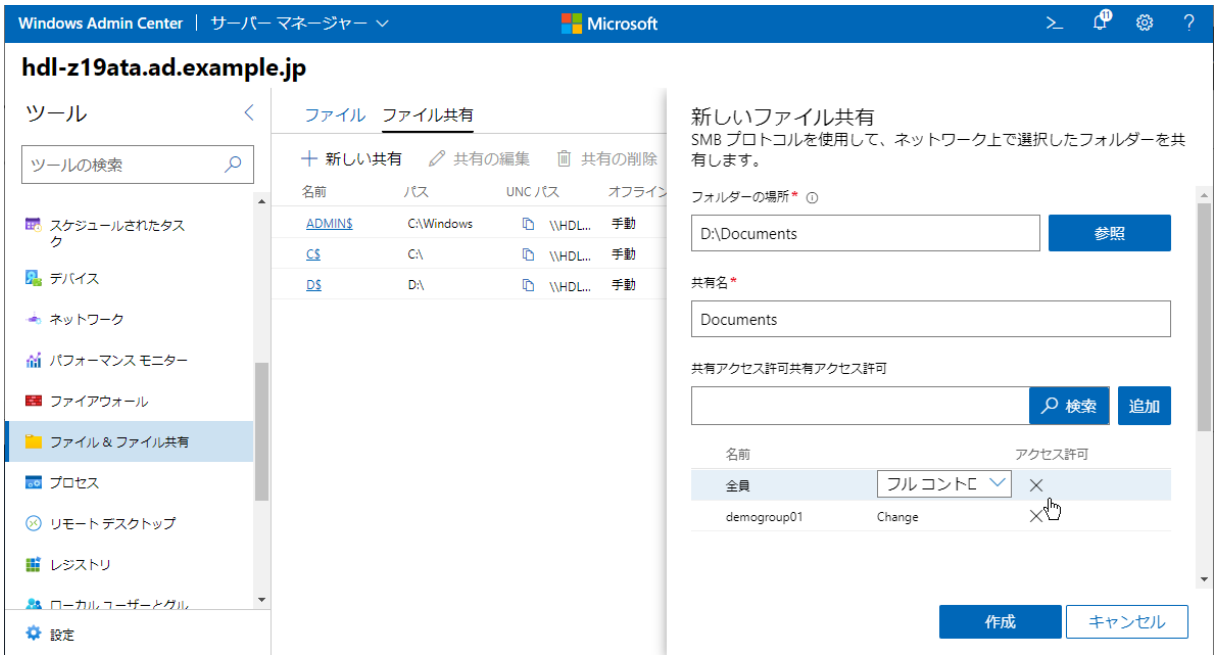


画面：D:ドライブ上に新しいフォルダーを作成する



画面：D:ドライブに Documents フォルダーを作成する

次に、[ファイル＆ファイル共有] ツール [ファイル共有] タブに切り替え、[＋新しい共有] をクリックします。[新しいファイル共有] では、[参照] をクリックして [フォルダーの場所] に D:¥Documents を設定します。すると、[共有名] に Documents が自動設定されます。[共有アクセス許可] のテキストボックスに DemoGroup01 と入力し、[追加] をクリックしたら、既定で設定されているアクセス許可の [全員：フルコントロール（Full-Control）] を削除し、追加した DemoGroup のアクセス許可を [フルコントロール（Full-Control）] または [変更（Change）] に設定して [作成] をクリックします。



画面：DemoGroup にフルコントロールまたは変更の共有アクセス許可を設定して Documents フォルダーを共有する

4.3　共有フォルダーへの接続

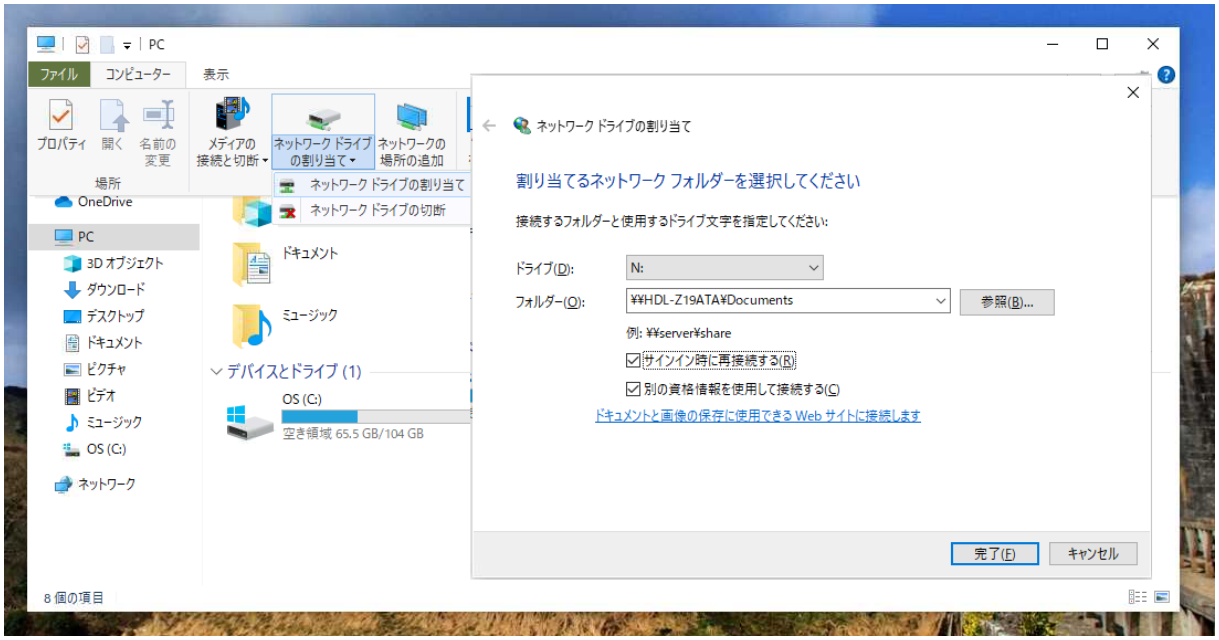
NAS の共有フォルダーには、Windows クライアントから UNC パス「**¥¥コンピューター名¥共有名**」（例：¥¥WINNAS01¥Documents）または「**¥¥IP アドレス共有名**」（例：¥¥192.168.10.201¥Documents）または「**¥¥NAS の FQDN ドメイン名¥共有名**」（例：¥¥WINNAS01.ad.example.jp¥Documents）、NAS のローカルアカウントまたはドメインユーザーアカウントの資格情報でアクセスすることができます。共有フォルダーへのアクセスに慣れている人であれば、それが分かれば事足りるでしょう。ここでは初心者向けに、Windows 10 の［エクスプローラー］（ファイルエクスプローラー）および Mac の［Finder］を使用して、ネットワークドライブとしてマウントして利用する方法を説明します。

Windows からの接続

Windows 10 の［エクスプローラー］を開き、ナビゲーションウィンドウの［PC］を選択します。すると、［エクスプローラー］のメニューバーに［コンピューター］タブが表示されるので、［コンピューター］タブに切り替え、［ネットワークドライブの割り当て｜ネットワークドライブの割り当て］を選択します。

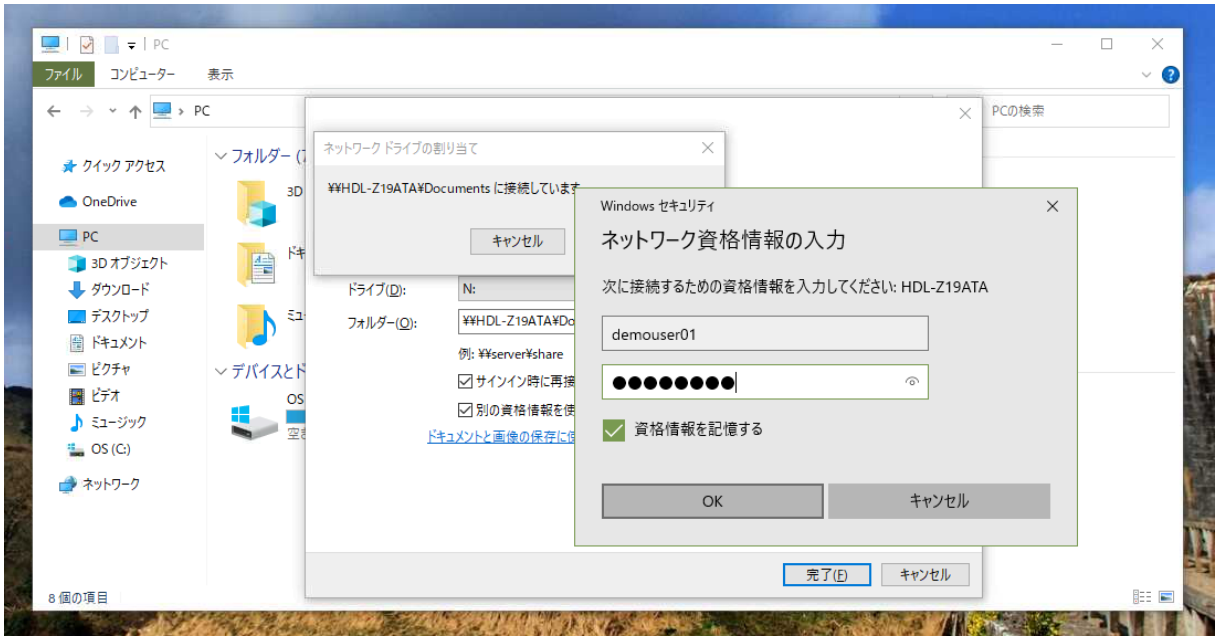
［ネットワークドライブの割り当て］ウィザードが開始するので、［ドライブ］にマウント先のドライブ文字を選択し、［フォルダー］に共有フォルダーの UNC パスを入力します。

常時マウントした状態で利用する場合は、[サインイン時に再接続する] オプションをチェックします。また、非ドメイン環境（ワークグループ環境）で利用している場合は、[別の資格情報を使用して接続する] オプションをチェックします。



画面：[ネットワークドライブの割り当て] ウィザードにマウント先と UNC パスを指定する

[完了] ボタンをクリックすると、[Windows セキュリティ] ダイアログボックスにネットワーク資格情報の入力が求められるので、ユーザー名（またはコンピューター名¥ユーザー名）とパスワードを入力し、[資格情報を記憶する] をチェックして［OK］をクリックします。

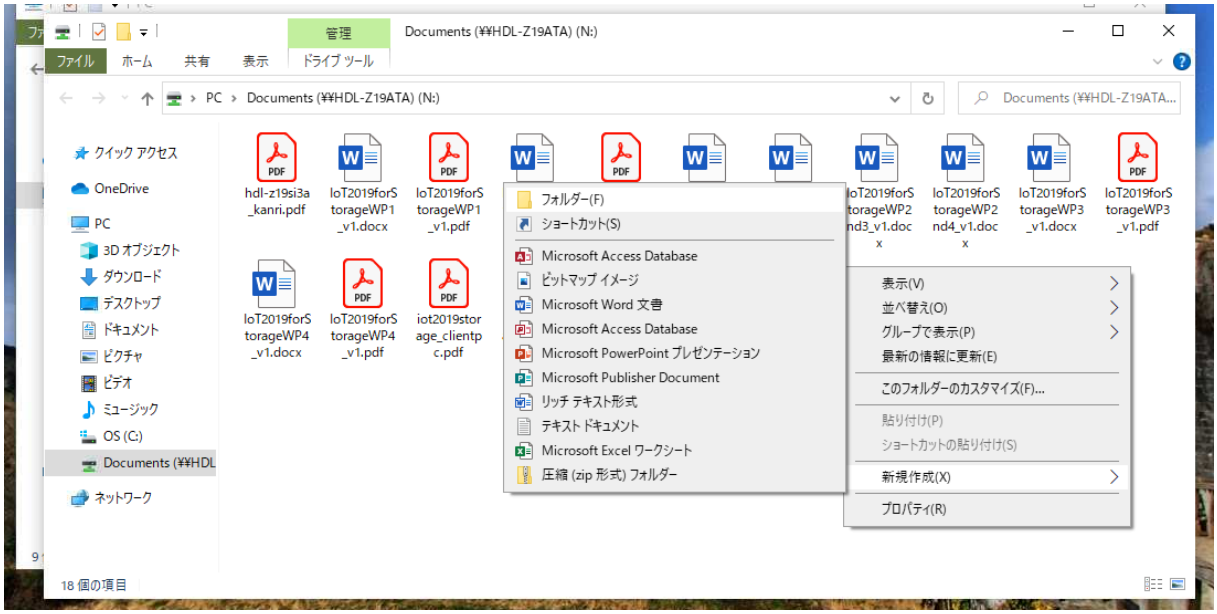


画面：ネットワーク資格情報として、NAS のローカルユーザーの資格情報を入力する（非ドメイン環境の場合）

なお、アクセス元の Windows クライアントがドメインに参加しており、現在、ドメインユーザーアカウン

トでログオン（サインイン）している場合は、［別の資格情報を使用して接続する］オプションのチェックは不要です。ネットワーク資格情報の入力が求められることなく、現在ログオンしているユーザーの資格情報で共有フォルダーにアクセスすることができます。

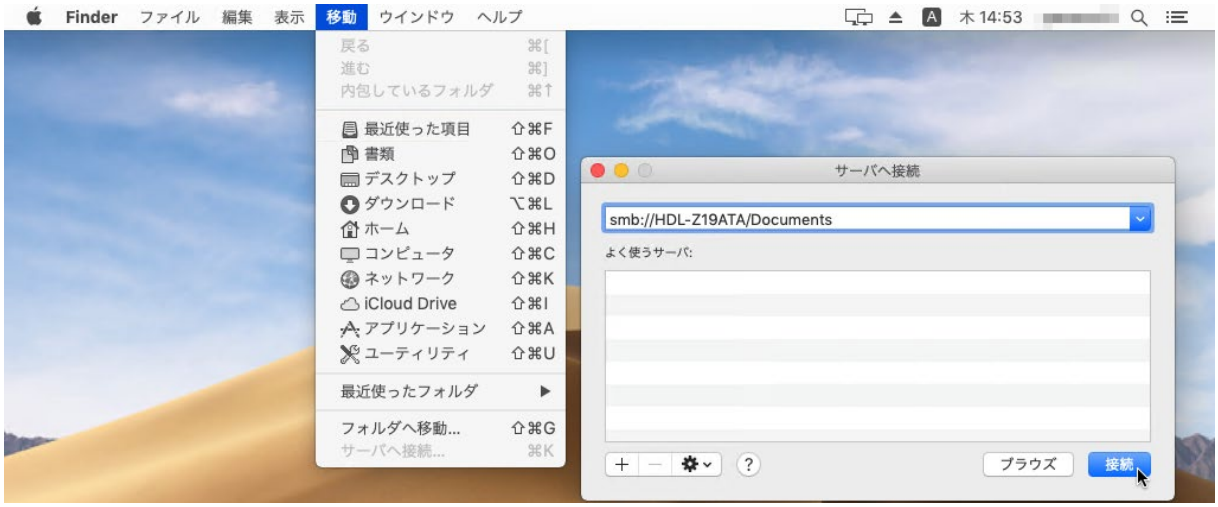
指定したドライブ文字にネットワークドライブがマウントされ、設定されたアクセス許可の範囲でファイルの作成や読み取り、削除、フォルダーの作成や削除が可能になります。また、この共有フォルダーを介して、別のユーザーとファイル共有を行うことができます。



画面：指定したドライブ文字に NAS の共有フォルダーがマウントされる

Mac からの接続

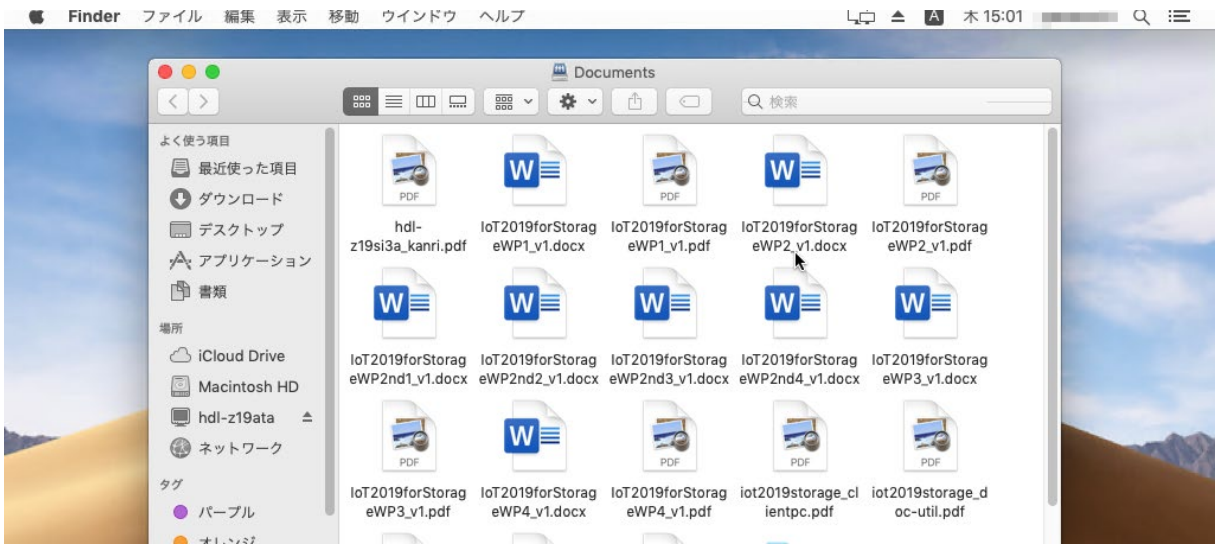
最近の Mac は最新の SMB バージョン 3 を標準でサポートしています（10.9 Mavericks から SMB バージョン 2、10.10 Yosemite から SMB バージョン 3 に対応）。Mac から NAS の共有（SMB 共有）に接続するには、［Finder］の［移動｜サーバへ接続］を選択し、［サーバーへ接続］ダイアログボックスに「smb://コンピューター名/共有名」の形式で共有フォルダーのパスを指定し、［接続］をクリックします。



画面：［サーバーへ接続］で「smb://コンピューター名/共有名」の形式でパスを指定し接続する

資格情報の入力が求められるので、[ユーザの種類：登録ユーザ] を選択し、共有フォルダーに接続するための資格情報を入力します。ユーザー名とパスワードの指定で認証が失敗する場合は、「**ユーザー名@コンピューター名**」（例：username@MYNAS01）または「**ユーザー名@FQDN ドメイン名**」（Active Directory ドメインユーザーアカウントの場合、例：username@ad.example.jp）の形式で入力してください。

画面：共有フォルダーにアクセスするための資格情報を入力する



画面：NAS の共有フォルダーが SMB プロトコルを使用してマウントされる

共有アクセス許可とファイルシステムのアクセス許可

このホワイトペーパーの例では、D:¥Documents フォルダーを共有名 Documents で共有設定し、DemoGroup01 グループにフルコントロール（または変更）のアクセス許可を付与しました。このアクセス許可設定では、DemoGroup01 グループのあるユーザーは Documents 共有にファイルやフォルダーを作成、変更、削除できますが、DemoGroup01 グループの別のユーザーが作成した（所有する）ファイルやフォルダーは読み取り専用でアクセスできます。

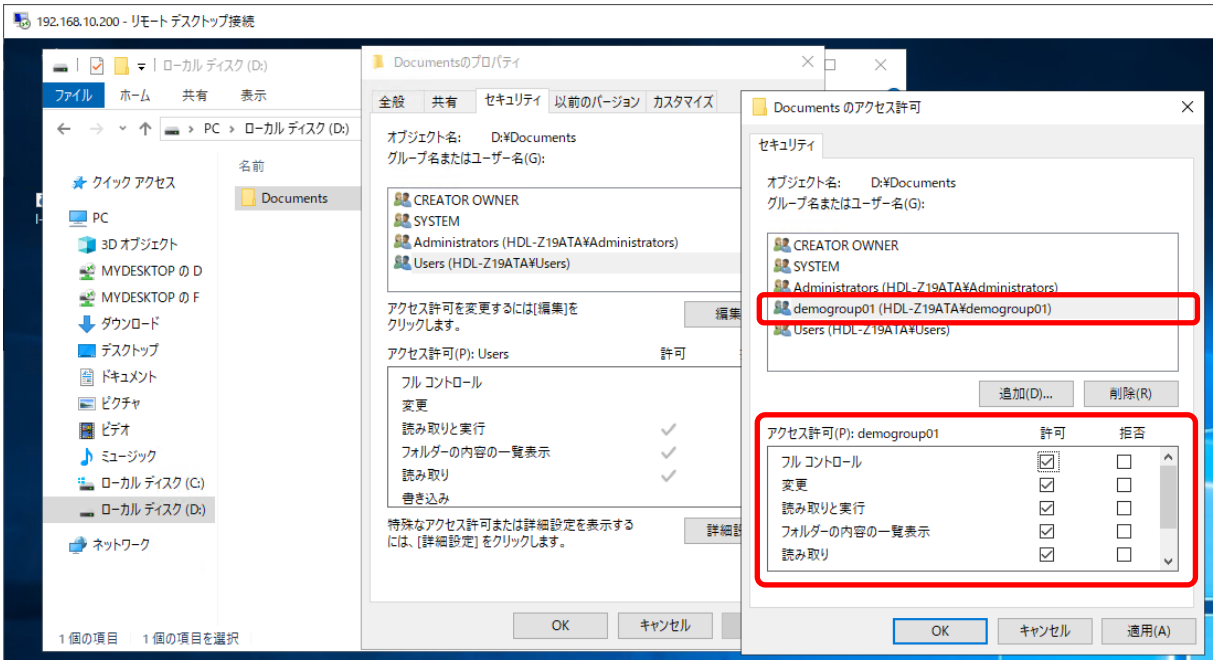
DemoGroup01 グループのユーザーであれば誰もが同じ権限で Documents 共有内のファイルやフォ

ルダーにアクセスできると期待するかもしれませんが、実際にはフルコントロール（または変更）の権限を持つのはそのファイルやフォルダーの作成者／所有者に制限されます。これは、ファイルシステム（NTFS または ReFS）レベルで設定される既定でアクセス許可の影響があるからです。

D:¥Documents フォルダーのファイルシステムレベルでは、CREATOR OWENER（作成者／所有者）、SYSTEM（システム）、Administrators グループはフルコントロールのアクセス許可を持ちますが、一般ユーザーが含まれる Users グループは読み取り（と実行）のアクセス許可しか持ちません。

作成者／所有者のみが最大のアクセス許可を持つことは予期した設定とは異なるかもしれませんが、ファイル共有環境での同一ファイルに対する同時更新といった競合を回避できますし、同じグループのユーザーは他のユーザーのファイルをコピーしてコピーに対して変更を加えることができる（オリジナルは残る）ため、適切なアクセス許可設定と言うこともできます。

作成者／所有者に関係なく、同じグループのユーザーに対して同じファイルに同じアクセス許可を与えたいというニーズがある場合は、ファイルシステムレベルで対象のグループにフルコントロール（または変更）のアクセス許可を追加します。Windows Admin Center は現状、ファイルシステムレベルのアクセス許可の参照や編集の機能を持ちません。そのため、ファイルシステムレベルのアクセス許可を変更するには NAS にリモートデスクトップ接続経由でログオンし、[エクスプローラー] で対象のフォルダーのプロパティの［セキュリティ］タブを開いて設定する必要があります。



画面：ファイルシステムのアクセス許可に必要なアクセス許可を追加する

4.4　ワークグループ環境におけるセルフパスワード管理

小規模なワークグループ環境（Active Directory ドメインを導入していない環境）では、ユーザーは NAS に登録したローカルユーザーとパスワードで共有フォルダーにアクセスします。初期パスワードは管理者が

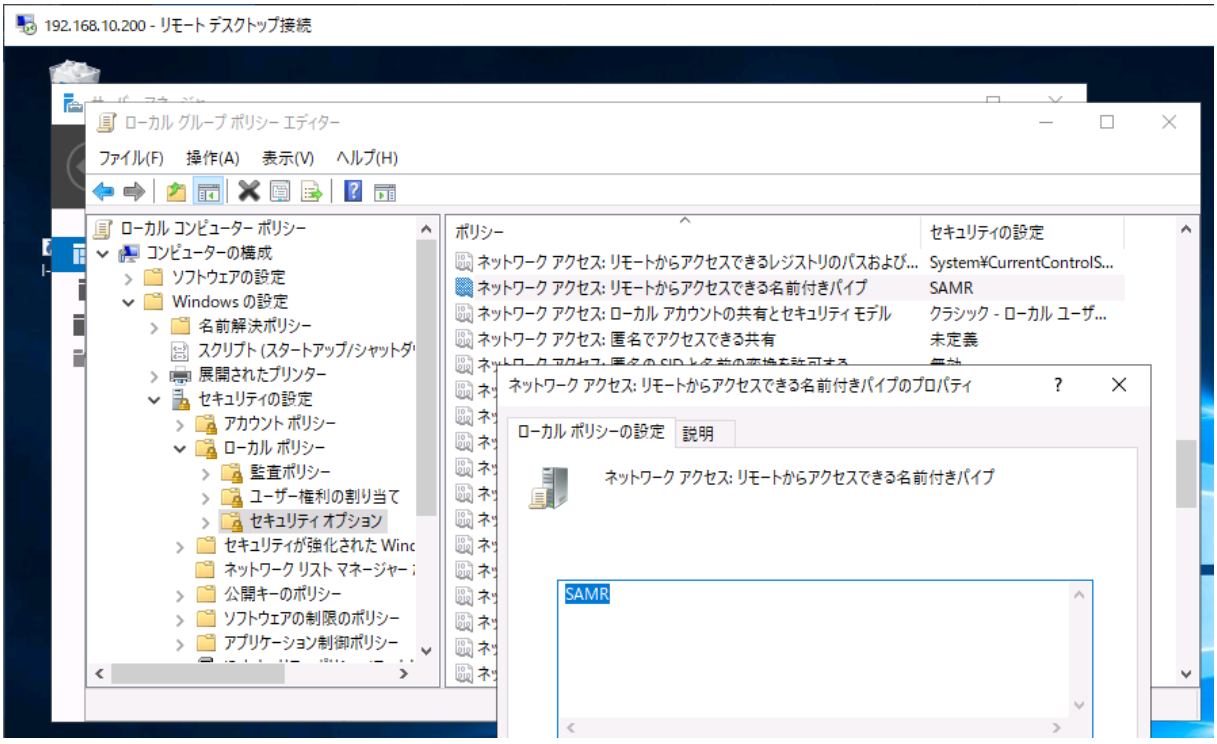
設定しますが、Windows クライアントでは次の方法でサーバー上の自分のローカルユーザーのパスワードを変更できます。

NAS 側の準備

Windows Server（特に Windows Server 2016 以降）や Windows 10 のセキュリティ強化の影響などで、リモートからのローカルユーザーのパスワード変更操作は、既定でブロック（アクセス拒否）されます。リモートからのローカルユーザーのパスワード変更操作を可能にするには、NAS にリモートデスクトップ接続で管理者としてログオンし、次の設定を行います。

1. ［ローカルグループポリシーエディター］（Gpedit.msc）を開き、次のポリシーに「SAMR」と設定します。

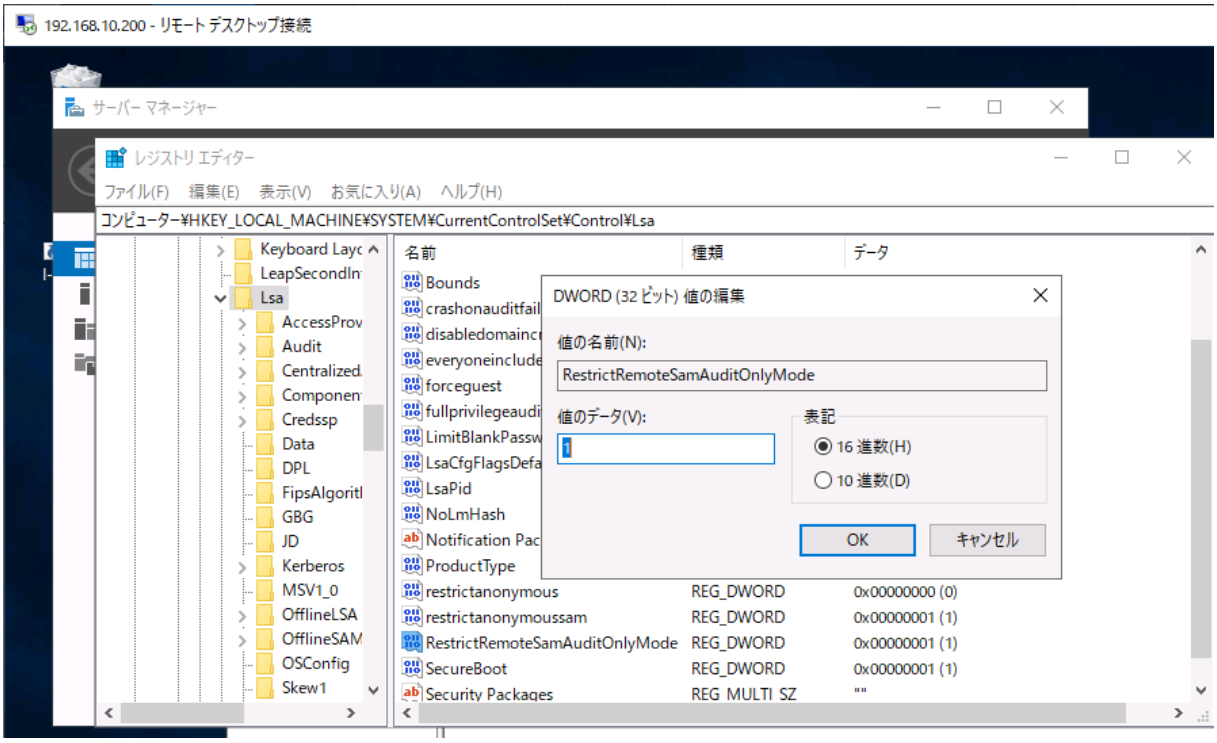
ポリシーの場所	コンピューターの構構成¥Windows の設定¥セキュリティの設定¥ローカルポリシー¥セキュリティ オプション
ポリシーの名前	ネットワーク アクセス: リモートからアクセスできる名前付きパイプ
セキュリティの設定	SAMR



2. ［レジストリエディター］（Regedit.exe）を開き、次のレジストリ値を作成します。

レジストリ キー	HKEY_LOCAL_MACHINE¥¥SYSTEM¥CurrentControlSet¥Control¥Lsa

値の名前	RestrictRemoteSamAuditOnlyMode
値の種類	DWORD（32 ビット）値（REG_DWORD）
値のデータ	1



3. NAS の OS を再起動します。

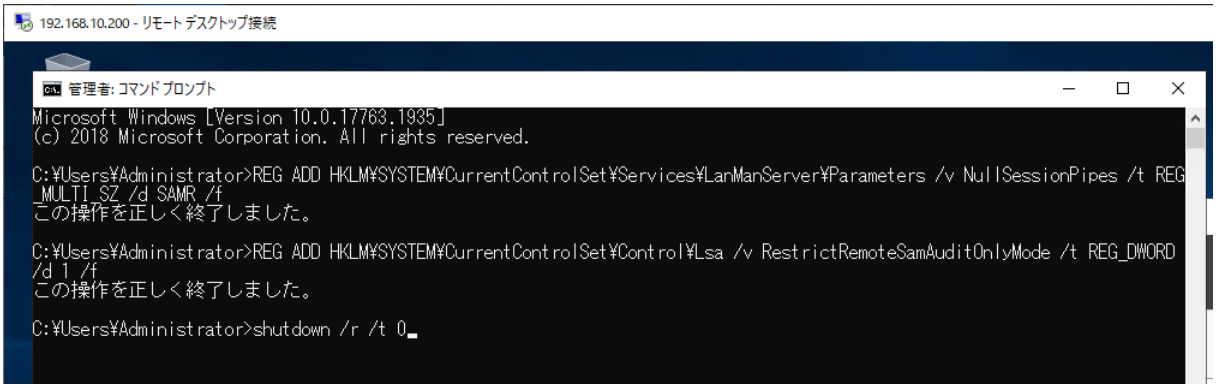
リモートからのローカルユーザーのパスワード変更操作をコマンドラインから許可する

［ローカルポリシーエディター］や［レジストリエディター］を使用せずに、コマンドプロンプト（cmd.exe）で次の 3 行のコマンドラインを実行することで、必要な設定を行うこともできます。

```
C:¥> REG ADD HKLM¥SYSTEM¥CurrentControlSet¥Services¥LanManServer¥Parameters /v NullSessionPipes /t REG_MULTI_SZ /d SAMR /f ↲

C:¥> REG ADD HKLM¥SYSTEM¥CurrentControlSet¥Control¥Lsa /v RestrictRemoteSamAuditOnlyMode /t REG_DWORD /d 1 /f ↲

C:¥> shutdown /r /t 0 ↲
```

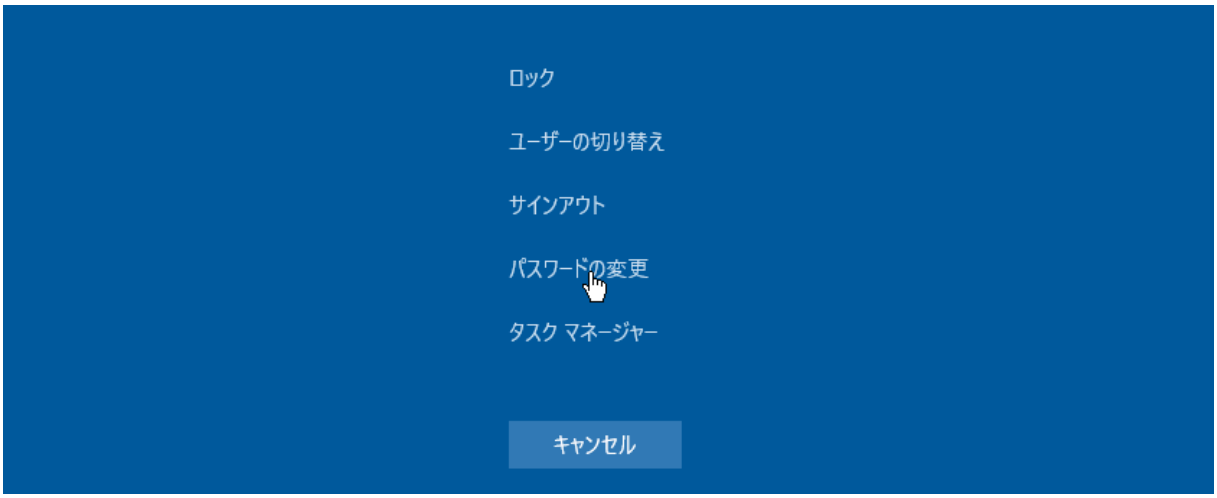


画面：リモートからのローカルユーザーのパスワード変更操作をコマンドラインから許可する

クライアントからのパスワード変更操作

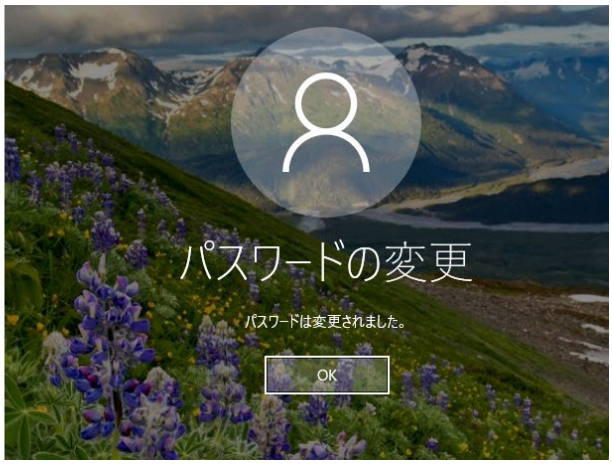
Windows 10 や Windows 8.1 を実行するクライアントからは、次の手順で NAS 上のローカルユーザーのパスワードを変更できます。

1. ［Ctrl］＋［Alt］＋［Del］キーを押して、Windows のセキュリティオプションの画面に切り替え、「パスワードの変更」を選択します。



2. ［パスワードの変更］画面が表示されるので、現在のユーザー名が表示されているテキストボックスにカーソルを移動し、「NAS のコンピューター名¥ローカルユーザー名」に書き換えます。古いパスワードと新しいパスワードを 2 回入力したら、［送信］をクリックします。

3. パスワードが変更されたことを確認します。



この方法は、ユーザーのパスワードの有効期限が切れた状態、あるいは［ユーザーは次回ログオン時にパスワード変更が必要］オプションがチェックされている場合でも利用できます。

なお、Microsoft アカウントでサインインして利用している場合は、「パスワードの変更」画面を利用できないことに注意してください。その場合は、管理者にパスワードの変更を依頼してください。

5. これだけはやっておきたい、Windows NAS の運用管理

NAS は設置して初期設定を行い、共有フォルダーを作成したらあとは放置というわけにはいきません。繰り返しますが、Windows Server IoT 2019 for Storage は、ソフトウェア的には通常版の Windows Server 2019 と共通であり、通常版の Windows Server 2019 で構築したファイルサーバーと同じように運用、管理する必要があります。セキュリティ、安定性、およびシステムとユーザーデータを保護するために、最低限、行うべき管理タスクについて説明します。

5.1 毎月 1 回のセキュリティ更新

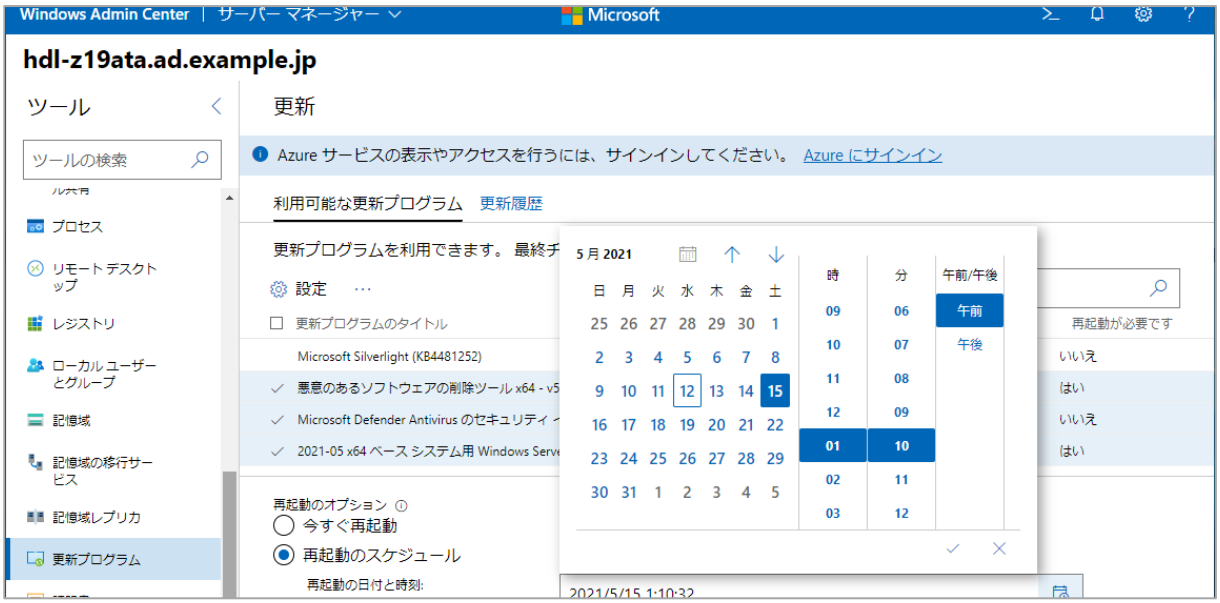
Windows や Windows Server と同様に、適切なタイミングで更新プログラムをインストールして、セキュリティ問題と不具合に対処し続けることが重要な管理作業になります。

マイクロソフトは、Windows、Windows Server について、米国時間の毎月第 2 火曜日（時差の関係で日本では翌水曜日）にセキュリティ修正を含む品質更新プログラム（累積的な更新プログラム）をリリースし、Windows Update や Windows Server Update Services（WSUS）を通じて提供しています。Windows Server IoT 2019 for Storage のための品質更新プログラムは、通常版の Windows Server 2019 用の品質更新プログラムとまったく同じものです。

Windows Server IoT 2019 for Storage（および Windows Server 2019）の Windows Update の既定の設定は、「Windows Update を使用して更新プログラムのダウンロードのみを行う」（Windows Admin Center のインストール時の選択によっては「Microsoft Update を使用して･･･」）です。NAS は長期運用前提のサーバーであるため、自動的に再起動される可能性のある自動更新（更新プログラムを自動的にインストールする）の設定は適切ではありません。自動更新以外のオプションにしておくべきです。「更新プログラムを確認しない（非推奨）」、つまり手動更新もサーバーでは推奨される選択肢の 1 つです。

更新プログラムの設定

Windows Admin Center の［更新プログラム］ツールを使用すると、Windows Update の設定を簡単に確認、設定することができます。［更新プログラム］ツールの［設定］をクリックすると、［更新プログラムの設定］で 4 つのオプションから選択することができるので、自動更新の設定である［更新プログラムを自動的にインストールする（おすすめ）］以外のオプションに設定してください。



画面：［更新プログラムを自動的にインストールする（おすすめ）］以外に設定する

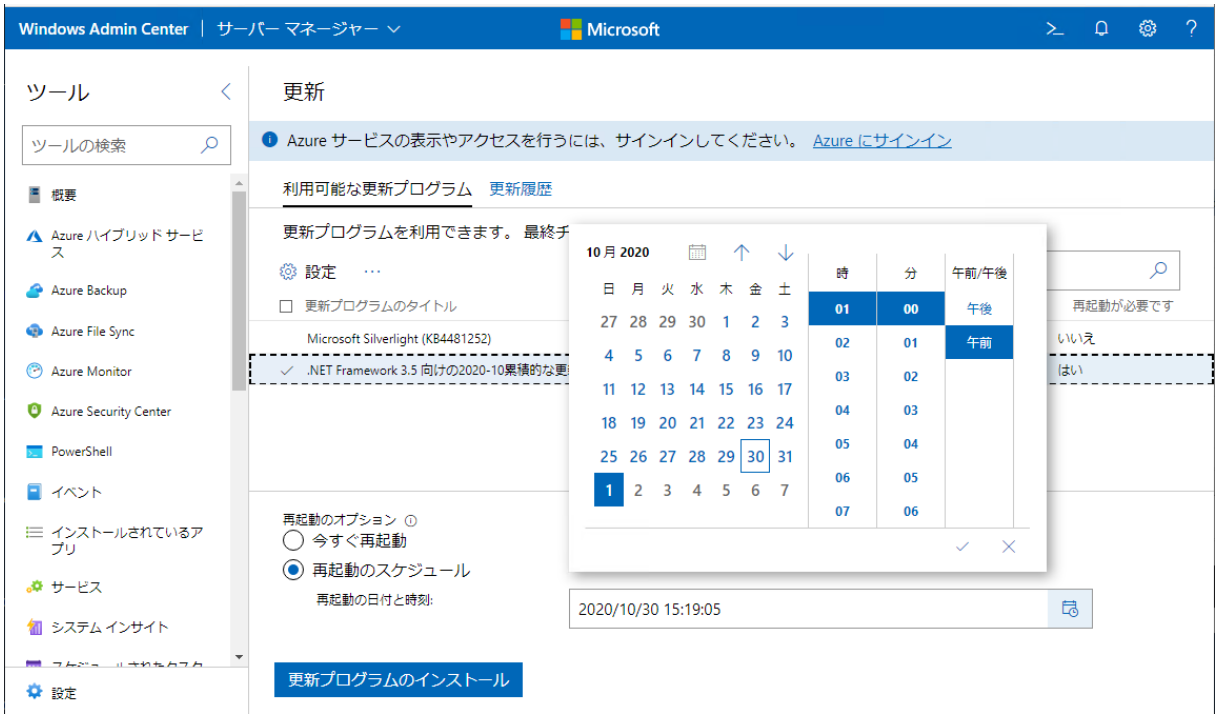
Windows Update の手動実行

毎月の更新プログラムには重大な不具合が含まれる場合があります。安定運用のためには、更新プログラムのリリース後、すぐにインストールすることはせずに、数日間様子を見て、メッセージセンターや更新履歴で既知の問題が報告されていないかどうかを確認してからインストールしてください。

メッセージセンター
https://docs.microsoft.com/ja-jp/windows/release-health/windows-message-center

Windows 10 および Windows Server 2019 の更新履歴
https://support.microsoft.com/ja-jp/help/4464619

Windows Admin Center の［更新プログラム］ツールを使用すると、利用可能な更新プログラムの確認を開始し、検出された更新プログラムを選択的にインストールすることができます。また、再起動が必要な更新プログラム（通常、累積的な更新プログラムのインストールには必要）がある場合、再起動の日時を指定して更新プログラムのインストールを開始できます。この機能は、Windows Server の Windows Update には用意されていない、Windows Admin Center が提供する便利な機能です。Windows Server の標準機能で Windows Update を実行した場合、更新プログラムのインストールを開始してそのまま放置しておくと、Windows 10 の場合と同じようにアクティブ時間外に自動的な再起動が行われてしまいます。



画面：Wndows Admin Center の［更新プログラム］ツールを利用すると、再起動をスケジューリングした上で更新プログラムのインストールを開始できる

5.2　システム構成変更時のシステムイメージのバックアップ

HDL-Z シリーズの 2 ドライブモデルの NAS は、OS ボリューム（C:ドライブ）およびデータボリューム（D:ドライブ）が 2 台のディスク間でミラー化されています。そのため、1 台のドライブに障害が発生しても、システムの稼働や起動は引き続き可能であり、ユーザーデータが失われることもありません。また、障害が発生したドライブを新しいドライブに交換することで再同期して自動的に復旧することができます。

このように標準でシステムおよびデータが保護されていますが、フルバックアップ、少なくともシステムのバックアップを取得しておくことをお勧めします。このバックアップの目的は、システムが起動不能になったとき、システムが原因不明で復旧不可能な異常な状態になったときに、システムをバックアップ時点までの状態に戻して短時間で復旧できるようにすることです。NAS に付属するリカバリーメディア（DVD また

は USB メモリ）で工場出荷時の状態に戻して復旧することもできますが、その場合、システム設定やデータの復旧など、追加の手順に多くの時間を要します。

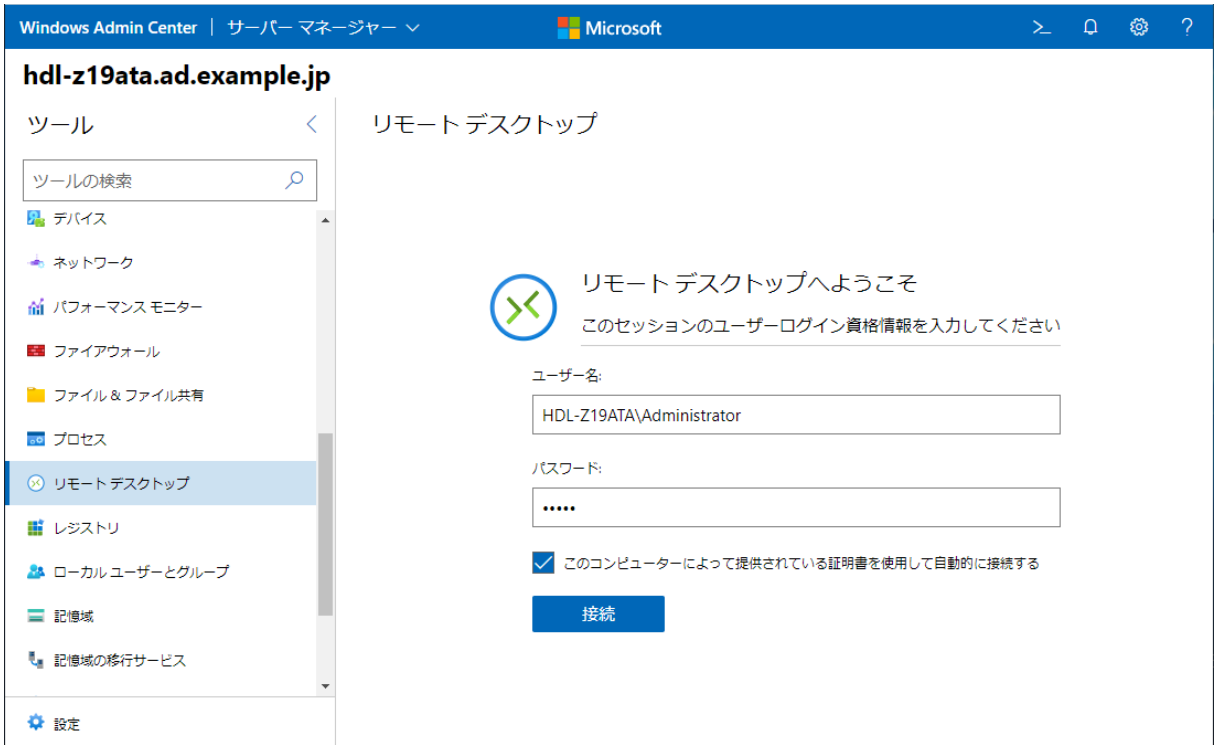
システムのバックアップはシステム設定を大きく変更したとき、その都度、行うとよいでしょう。ハードウェアの障害の影響を受けないように、USB 外付けハードディスクなど、外部メディアにバックアップを作成することをお勧めします（USB ポートから給電するセルフパワータイプのデバイスは推奨しません）。バックアップ時間を短縮するためには、USB 3.0 対応のディスクを使用することと、バックアップにはユーザーデータ（D:ドライブ）は含めないことです。ユーザーデータのバックアップについては、より頻繁なサイクルで自動化された、別の方法を検討してください（後述します）。

写真 : バックアップ用メディアとして、NAS の USB ポートに USB 外付けハードディスクを接続する（USB 3.0 対応デバイスを USB 3.0 ポートに接続することを推奨）

Windows Admin Center からのリモートデスクトップ接続

Windows Server IoT 2019 for Storage のシステムのバックアップには、［Windows Server バックアップ］を使用します。この機能は、Windows Server IoT 2019 for Storage に既定でインストールされていますが、Windows Admin Center には現状、統合されていません（［役割と機能］ツールでインストール状況の確認や変更は可能です）。リモートデスクトップ接続経由でコンソールにログオンして実施する必要があります。

Windows Admin Center の［リモートデスクトップ］ツールを使用すると、Web ブラウザーだけで NAS のコンソールにリモートデスクトップ接続することができます。もちろん、Windows 標準のリモートデスクトップ接続クライアント（Mstsc.exe）やその他のプラットフォーム用のリモートデスクトップ接続アプリを使用しても構いません。

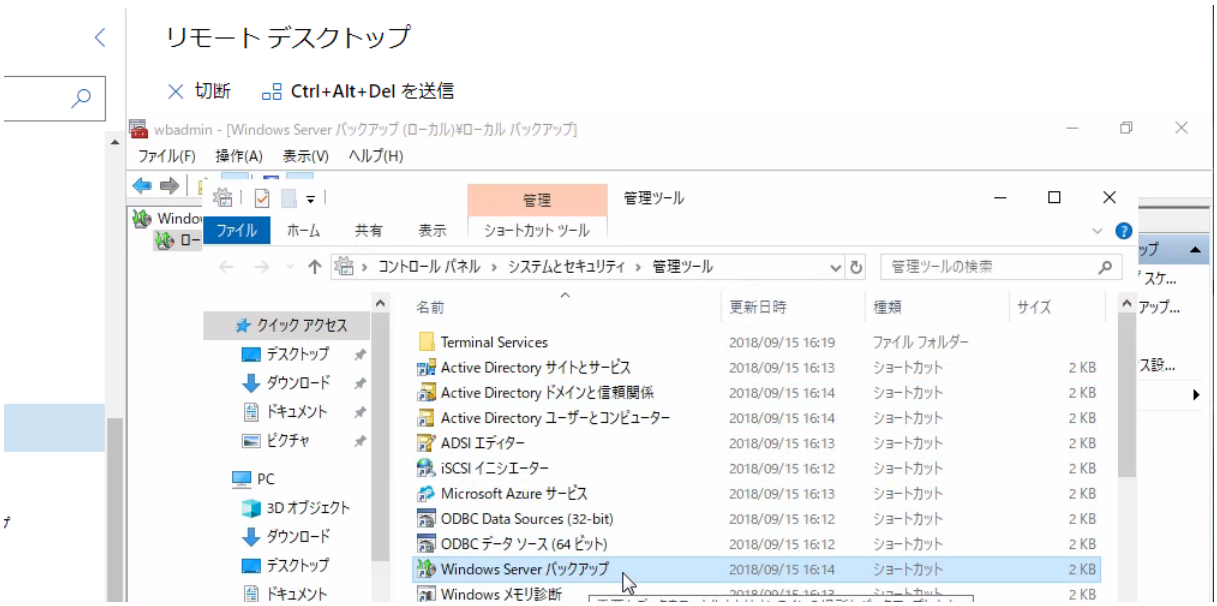


画面：Windows Admin Center を利用すると、クライアントアプリなしでリモートデスクトップ接続が可能

ベアメタル回復用のバックアップの作成

NAS にリモートデスクトップ接続経由でログオンしたら、次の手順でベアメタル回復用のバックアップを USB 外付けハードディスクに作成します。ベアメタル回復用のバックアップとは、まっさらな（ベアメタル）ディスクに対して、OS の起動に必要なボリュームだけを復元し、システムをすばやく復旧するためのバックアップです。

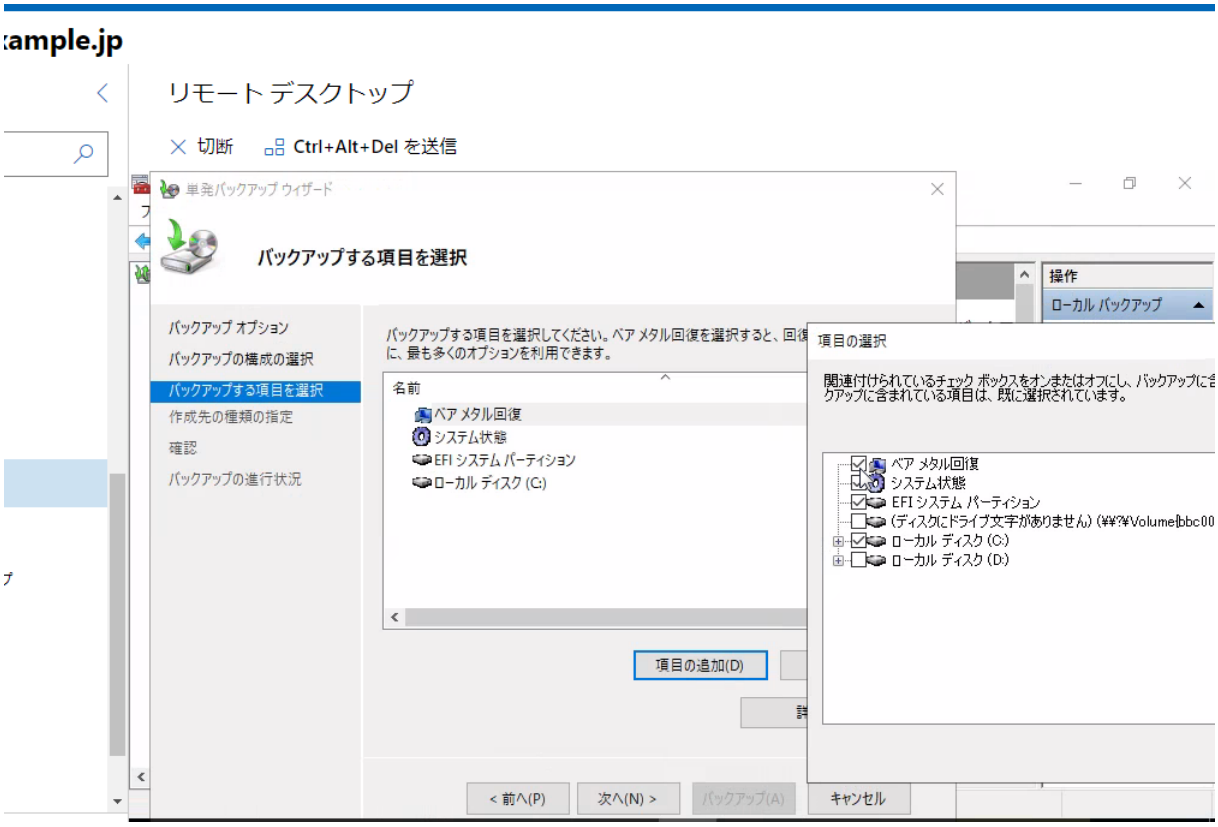
1. スタートメニューの［Windows 管理ツール］を開き、［Windows Server バックアップ］スナップイン（wbadmin.msc）を開始します。



2. ［Windows Server バックアップ］スナップインの［操作］ペインにある［単発バックアップ］をクリックし、［単発バックアップウィザード］を開始します。最初の［バックアップオプション］の画面では［別のオプション］を選択して［次へ］をクリックします。

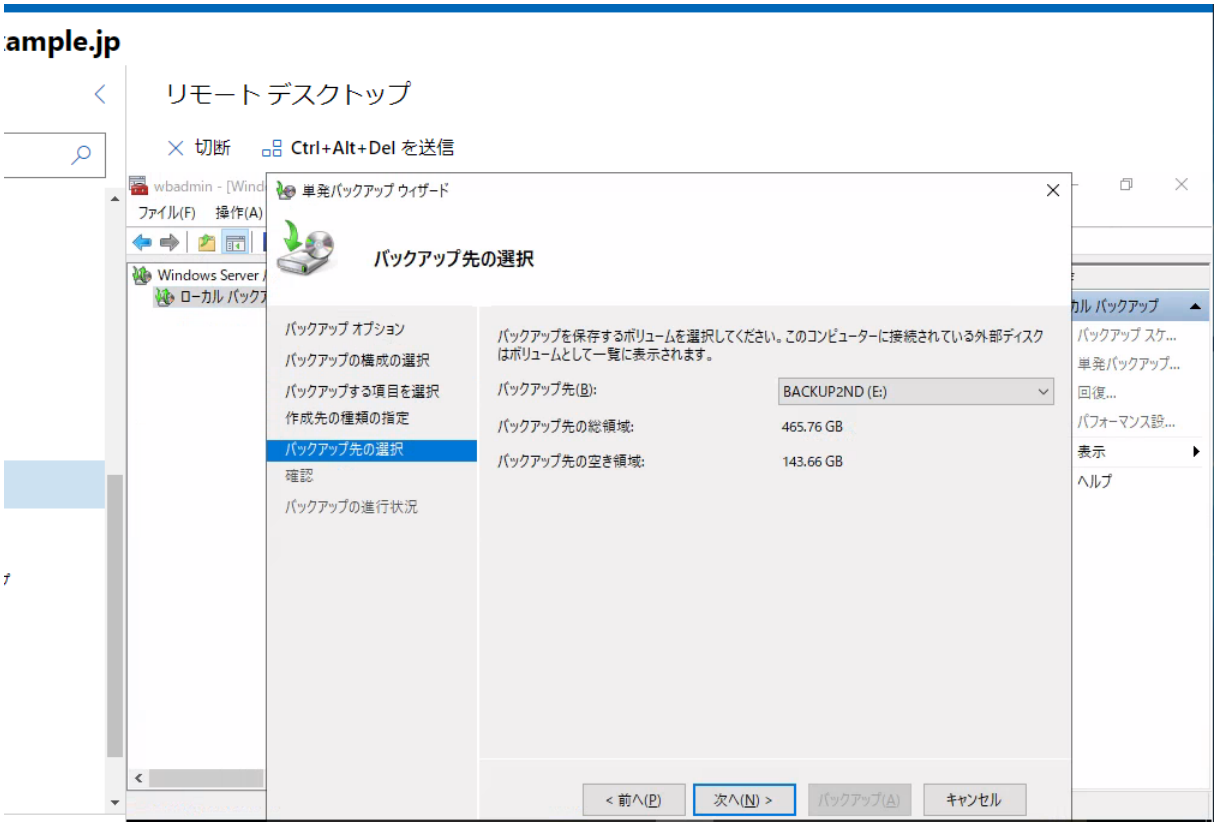
3. ［バックアップの構成の選択］の画面では［カスタム］を選択して［次へ］をクリックします。

4. ［バックアップする項目を選択］の画面では、［項目の追加］をクリックし、［項目の選択］ダイアログボックスで［ベアメタル回復］をチェックします。すると、OS の起動と稼働に必要な［システム状態］、［EFI システムパーティション］、［ローカルディスク（C:）］が自動選択されるので［OK］をクリックします。［バックアップする項目を選択］の画面に戻り、［次へ］をクリックします。

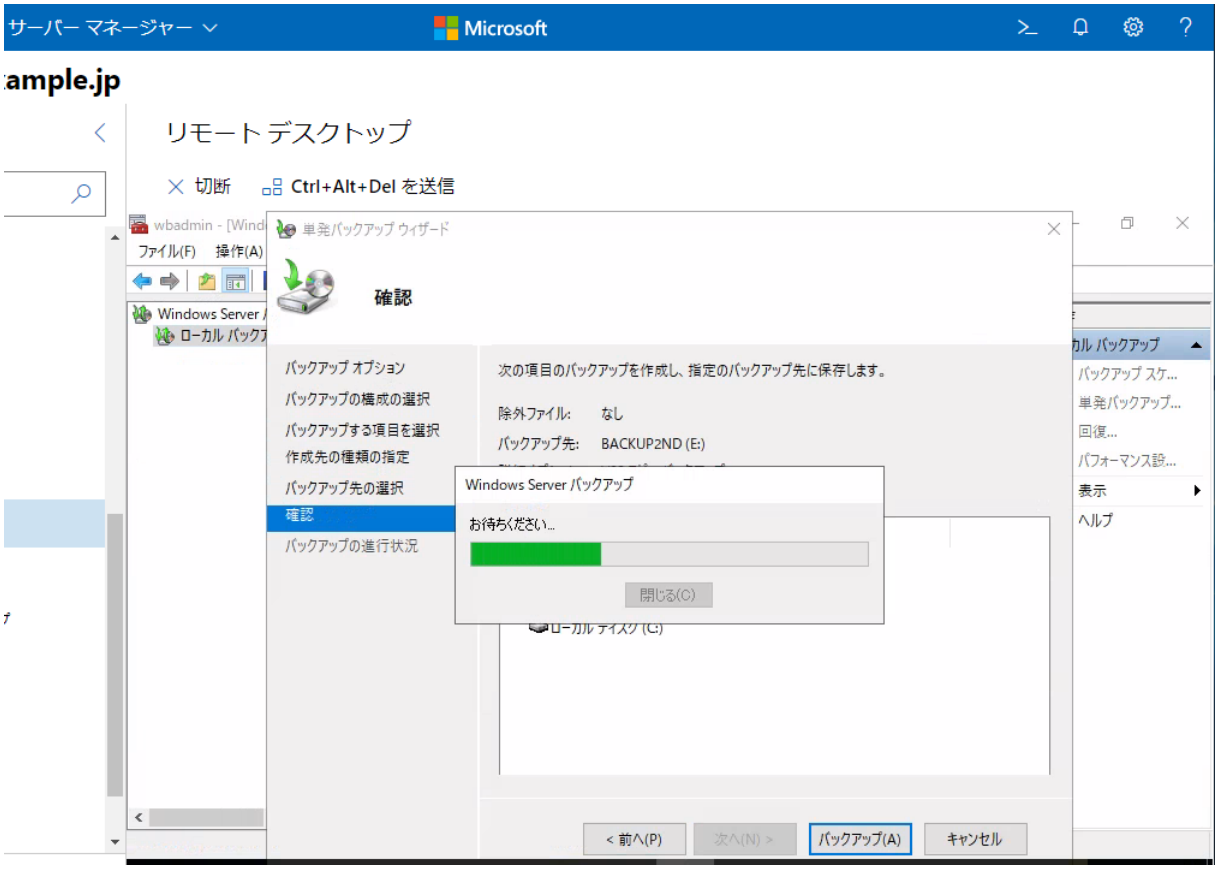


5. ［作成先の種類の指定］の画面で［ローカルドライブ］を選択し、［次へ］をクリックします。

6. ［バックアップ先の選択］の画面でバックアップ先として USB 外付けハードディスクのドライブ（NTFS または exFAT 形式でフォーマットしておくこと）を選択し、［次へ］をクリックします。



7. ［確認］の画面で[バックアップ]をクリックし、バックアップの作成を開始します。バックアップが完了したら、USB 外付けハードディスクを取り外してください。



ベアメタル回復について

ベアメタル回復用のバックアップの作成は、万が一に備えてのものであり、このバックアップを使用したベアメタル回復による復旧の手順については省略します。バックアップが適切に取得できていることが重要だからです。

ベアメタル回復のバックアップからシステムを復元すると、ディスク構成（RAID 構成を含む）も復元されるので、データボリュームの最新のバックアップをさらに復元することで、短時間でシステムとデータを正常な状態に戻すことができます。

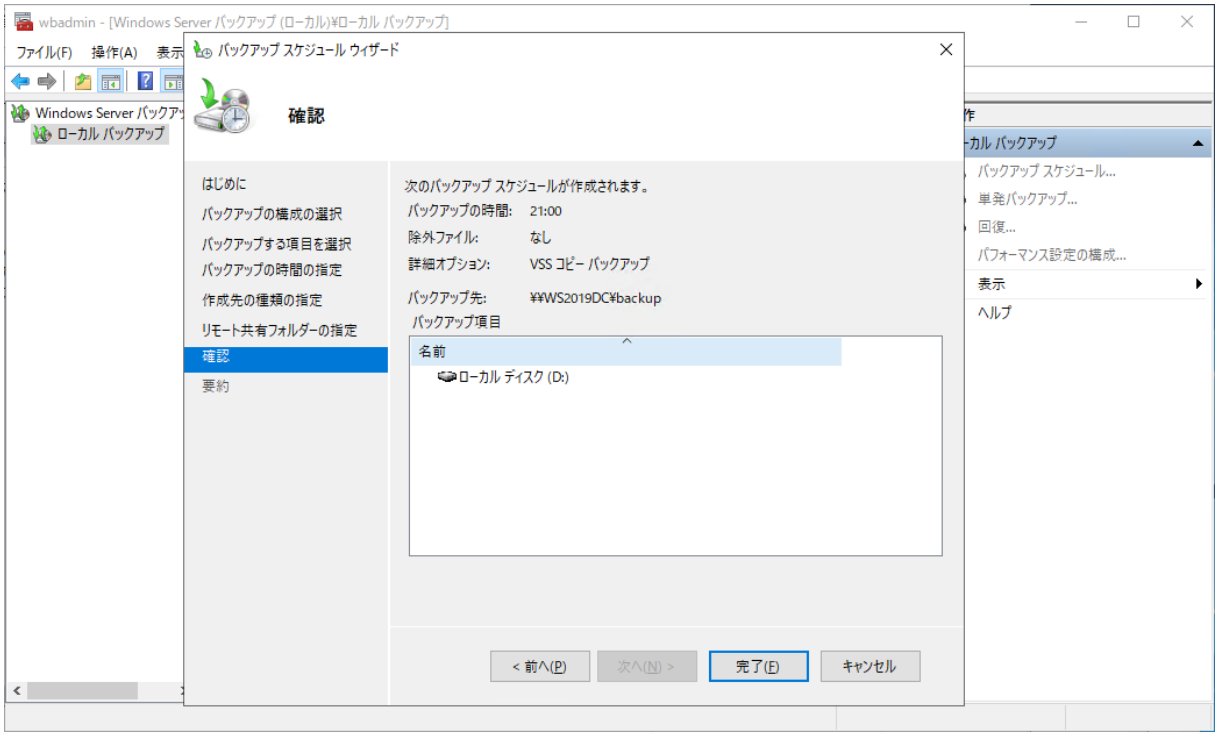
バックアップからの復旧手順については、NAS 製品の管理マニュアルの『故障時の対応｜システムをリカバリーする｜バックアップデータから復元する場合』を参照してください。

LAN DISKZ 管理マニュアル
https://www.iodata.jp/lib/manual/pdf2/hdl-z19sata_kanri.pdf

5.3　データの継続的なバックアップ保護の計画

データ用の D:ドライブに格納されるユーザーデータについては、日次や週次など、より短いサイクルで継続的かつ自動的にバックアップすることを検討してください。継続的かつ自動的なデータのバックアップ方法としては、次の方法があります。ハードウェアやサービスのコストなどを含めて検討してください。

- **［Windows Server バックアップ］を使用した自動化された継続的なバックアップ**･･･ USB 外付けハードディスク（バックアップ専用ディスクを推奨）や SMB 共有へのスケジュールバックアップ

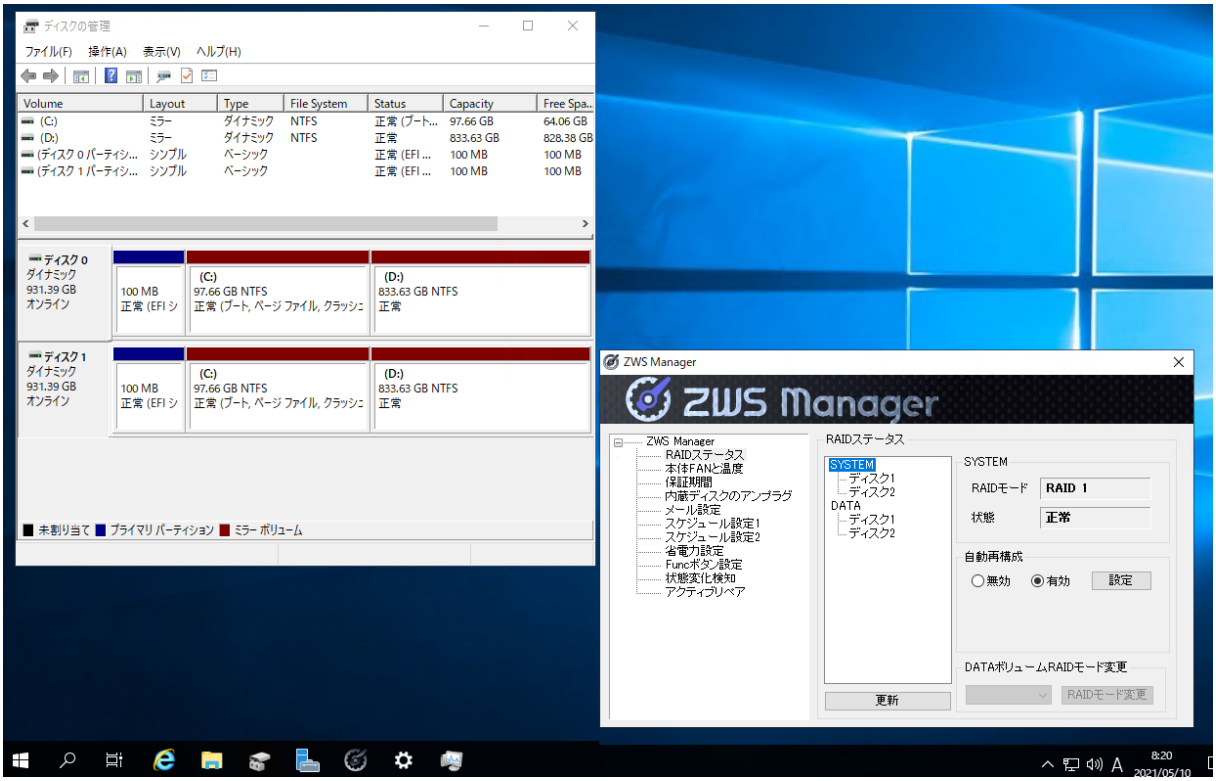


- **Azure Backup を使用したディスク･ツー･クラウドの自動化された継続的なバックアップ** ･･･ Azure のサブスクリプション契約、およびサービスの利用料金が必要
- **Azure File Sync による Azure ファイル共有との双方向同期**･･･ Azure のサブスクリプション契約、およびサービスの利用料金が必要
- **クローン for Windows（アイ・オー・データ）を使用した NAS 間のリレー同期** ･･･ ソフトウェアは無料であり、NAS の切り替えにより最も短時間で復旧可能だが、同容量の NAS がもう 1 台必要

Azure Backup およびクローン for Windows については、ホワイトペーパー『最新ファイルサーバー 3.集中管理編／4. ハイブリッドクラウド編』で、Azure File Sync および Azure ファイル共有についてはホワイトペーパー『生産性向上術 4. リモートワーク対応編』で詳しく説明しています。

HDL-Z シリーズ、2 ドライブモデルの冗長性について

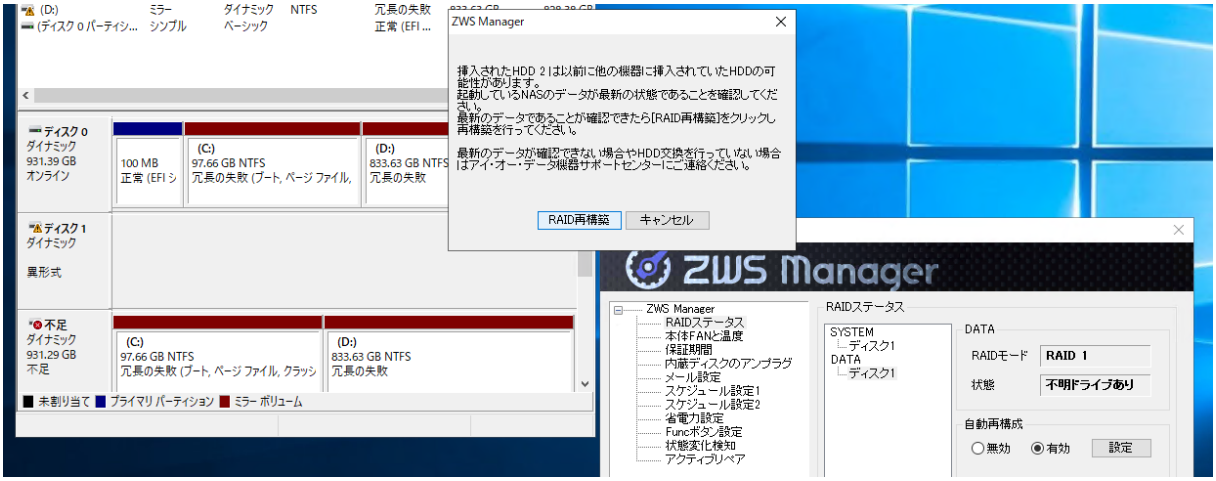
HDL-Z シリーズ、2 ドライブモデルは、工場出荷時の既定の構成で、OS ボリューム（C:ドライブ）およびデータボリューム（D:ボリューム）が RAID-1 のミラーリング構成になっています。これにより、2 ドライブのうち一方のドライブに障害が発生した場合でも、正常なドライブで稼働し続けることができ、システムやデータが破損することなく保護され、ファイルの読み書きに影響することもありません。



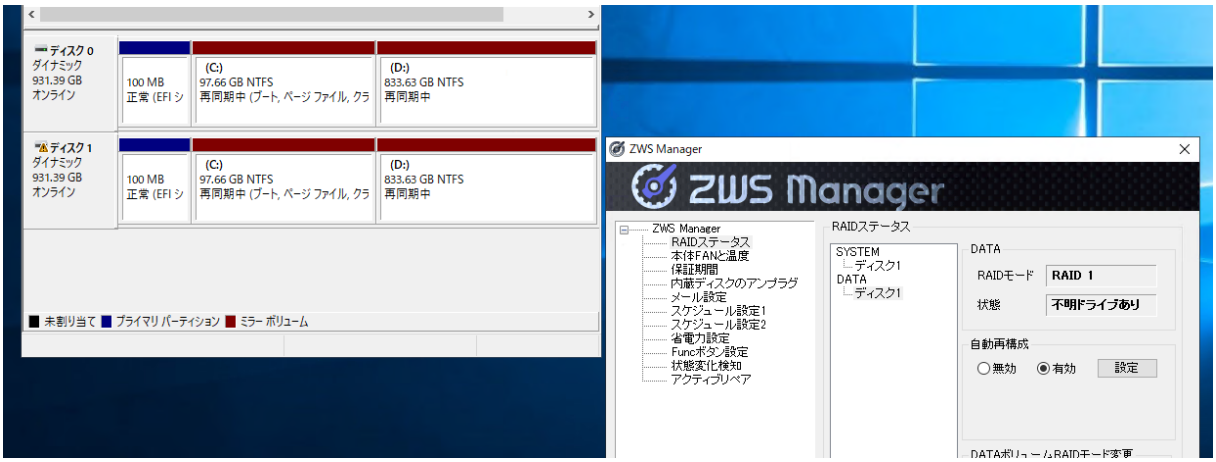
画面：2 ドライブモデルは OS とデータ用のドライブがミラー化されており、変更は両方のディスクに書き込まれ、同期される

1 台のディスクに障害が発生した場合でも、稼働中に新しいディスクカートリッジに交換することがで

きます。アイ・オー・データの ZWS Manager が新しいディスクを検知し、通知します。管理者は［RAID 再構築］をクリックするだけでよく、ZWS Manager が新しいディスクを RAID 用に準備し、RAID の再構成を開始します。



画面：ZWS Manager が新しいディスクを検知するので、管理者は［RAID 再構築］をクリックして正常な状態（冗長化された状態）に復旧させることができる



画面：同期が完全に完了するまでには数時間かかる場合がある

HDL-Z シリーズの 2 ドライブモデルの NAS は、既定で 1 台目のディスクから OS を起動します。2 台目のディスクに障害が発生し、認識しない場合でも、1 台目のディスクだけで起動できます。OS とデータのボリュームの冗長性は失われますが（ミラーリングされていない状態）、ファイルシステムの読み書きに影響はありません。

１台目のディスクに障害が発生し読み取れない場合、NAS は 2 台目のディスクから起動しようとします。この場合、［Windows ブートマネージャー］の［Windows Server – セカンダリ プレックス］を選択して起動することで、2 台目のディスクだけで起動することができます。ただし、起動直後の［Windows ブートマネージャー］に対話する必要があるため、HDMI 接続のディスプレイ、USB キーボード、および USB マウスを接続してローカルコンソールを一時的に利用可能にして操作する必要があります。

写真：：1 台目のドライブが故障した場合、2 台目のドライブから起動するにはローカルコンソールで「Windows Server – セカンダリ プレックス」を選択して起動する

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/