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を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　HDL-Z 内のデータにリモートワーク環境からアクセスする手段について

企業では今、感染症のパンデミックや大規模災害発生時の事業継続性が喫緊の課題となっています。新型コロナウイルス感染症（COVID-19）の感染拡大を受けて 2020 年 4 月に発出された緊急事態宣言は、企業の規模の大小を問わず、可能な場合はリモートワーク（テレワーク）の推奨を伴うものでした。7 月に入ってからの全国的な感染の再拡大は、リモートワークのさらなる継続を求めるものでした。リモートワークを想定しておらず、何の備えもしていなかった企業にとって、突然のリモートワークの実施推奨で右往左往した IT 担当者は多かったと思います。しかも、リモート会議ができればよいというものでもありません。

HDL-Z は、中小規模から大企業の全社的な、あるいは部門用のファイルサーバーとして、社内ネットワークに設置して、別のユーザーやコンピューターを信頼できる、閉じたネットワーク内で利用することが想定されています。インターネットを介した外部からのアクセスは想定していません。

ここでは、リモートワーク環境において HDL-Z 内のデータにアクセスするという視点で、どのようなソリューションがあるのかを検討します。

直接的なリモートアクセスの課題

社内ネットワーク上の HDL-Z に保存されているデータにアクセスして参照する、あるいは HDL-Z にデータを保存することを可能にするには、一般的に次の 2 つの手段が考えられます。

- **仮想プライベートネットワーク（Virtual Private Network、VPN）によるフルアクセス** ･･･ 社内ネ

ットワークの IP サブネットにインターネット経由でのトンネル接続を許可する方式です。新規に導入する場合、VPN デバイスの設置やネットワーク帯域幅の増強などに導入コストがかかります。HDL-Z に限らず、社内ネットワーク上のリソースに制限なくアクセスできる可能性があり、通信路は安全でもエンドポイントからの不正侵入や情報漏洩に対して課題があります。特に、企業によって管理されていない、さまざまなプラットフォームが使用される可能性がある BYOD（Bring Your Own Device、個人デバイスの業務使用）での利用には適していません。

- **セキュアなプロトコルでのアクセスのみを限定的に許可** ･･･ 厳密な認証（証明書や多要素認証、デバイス認証など）に基づいて、HDL-Z 上の共有リソースに対するアクセスのみに限定したプロトコル（例えば、HTTPS）だけを許可する方式です。このガイドの『1. ファイルサービス編』で説明した WebDAV は SSL で暗号化できるとはいえ、ユーザー名とパスワードの組み合わせの基本認証に依存するため、総当たり攻撃に対して脆弱であり、セキュアなソリューションにはなり得ません。Windows Server IoT 2019 for Storage はこの方式に最適な「ワークフォルダー」機能をサポートしていますが、『1. ファイルサービス編』でも説明したように、導入のためのシステム設計や導入コストが高いハードルになります。少なくとも、HDL-Z 単体で実装できるものではありません。

このように、ファイル共有を目的としたリモートワーク環境の導入にはさまざまな課題があります。そこでこのガイドで提案するのは、Microsoft Azure のクラウドサービスと Windows Server IoT 2019 for Storage のファイルサービス機能のハイブリッドな利用環境です。この利用環境は、以下の Microsot Azure のサービスを利用します。

- **Azure ファイル共有（Azure Files）** ･･･ SMB プロトコルに対応したサーバーレスのクラウドストレージです。Azure ファイル共有は Azure リージョン内の仮想ネットワークでは SMB v2.1 または SMB v3 でのアクセスを提供し（例えば、Azure 仮想マシンのゲスト OS から Azure ファイル共有への接続）、別の Azure リージョンやインターネット経由では SMB v3 での暗号化（必須）されたアクセスを提供します。SMB v3 はプロトコルに組み込みの「SMB 暗号化」機能でエンドツーエンドで保護されるため、インターネット経由でもセキュアにアクセスすることが可能です。SMB クライアントは、ストレージアカウント名とキーの認証に基づいて Azure ファイル共有をマウントできます。また、Active Directory ドメインサービス（AD DS）や Azure Active Directory ドメインサービス（Azure AD DS）の ID に基づいた認証、および Azure MFA（多要素認証）に基づいたアクセス制御にも対応しています。

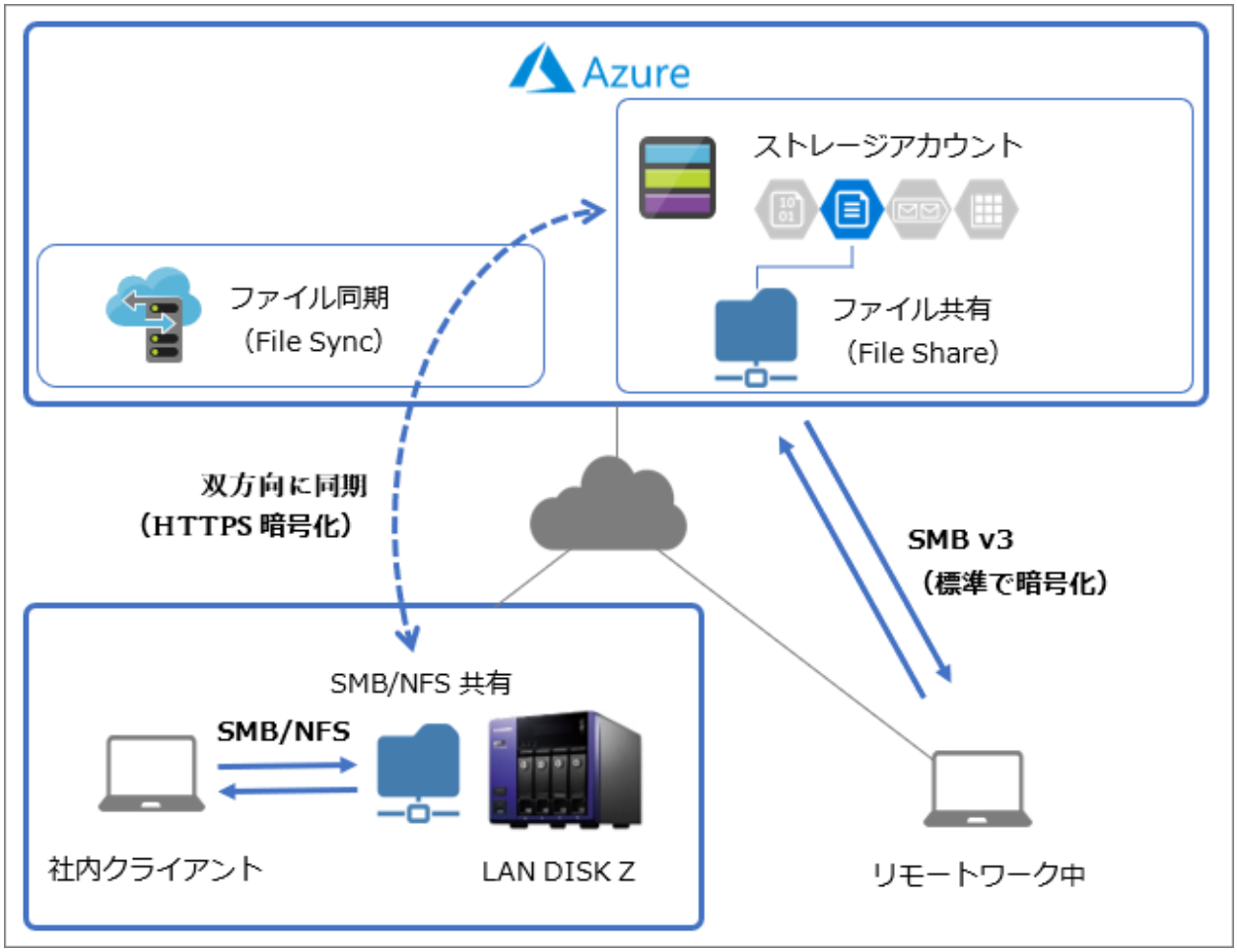
  Azure Files
  https://azure.microsoft.com/ja-jp/services/storage/files/

- **Azure ファイル同期（Azure File Sync）** ･･･ Azure ファイル共有を、エンドポイントとなるオンプレミスの Windows Server にキャッシュするファイル同期サービスです。このサービスを利用すると、オンプレミスの Windows Server のディレクトリと Azure ファイル共有を双方向に同期することができます。あるいは、SMB のみのアクセスをサポートする Azure ファイル共有に対して、マルチプロトコル（SMB v1/v2/v3、NFS、WebDAV、FTP、iSCSI など）でアクセス可能なエンドポイントをオンプレミスに用意するために使用できます。オンプレミスのファイルサーバーのバックアップとして、あるいはリモートワーク対応のためのアクセス手段を提供するために使用することもできます。

Azure ファイル共有へのアクセスは、発信方向の TCP ポート 445 経由の SMB v3 アクセスです。また、エンドポイントの Windows Server と Azure ファイル同期サービスとの通信は、Web サイトへの一般的なアクセスと同じ、発信方向の TCP ポート 443 経由の HTTPS トラフィックです。これらのトラフィックを許可するために特別なネットワーク構成やファイアウォール構成は必要ありません。

1.3　実施環境について

ここでは、HDL-Z をドキュメント共有用のファイルサーバーとして導入済みであり、クライアントである Windows 10 コンピューターと同じ IP サブネットまたは適切にルーティングされた IP サブネットに HDL-Z が接続されていることを前提とします。また、リモートワーク中のクライアントを想定し、個人が自宅の Windows 10 コンピューターからアクセスすることを想定します。社内ネットワークと自宅の両方とも、一般的な方法（ブロードバンドルーターなど）を介してインターネットに接続されているものとします。なお、社内または社外のクライアント（個人デバイスを含む）としては Windows 10 以外に、SMB v3 に対応した Windows 8.1、macOS、および Linux を使用できます。



図：Azure のサービスと連携させたハイブリッドなリモートアクセス環境

Azure 無料アカウントについて

このガイドで説明する機能は、Azure 評価用の無料アカウントで利用することができます。Azure 無料アカウントには 30 日間ほぼ機能制限なく利用できる無料クレジット枠（2020 年 8 月時点で 22,500 円分の利用が 1 か月間無料）と、12 か月間の無料サービスが提供されます。30 日の無料評価期間の終了時点でサブスクリプションを終了するか、従量課金制での継続利用に移行することができます。無料アカウントのサインアップには、以前に Azure 無料アカウントのサインアップに使用されたことのないクレジットカードの登録が必要ですが、30 日の評価期間内に課金が発生することはありません。

Azure の無料アカウント
https://azure.microsoft.com/ja-jp/free/

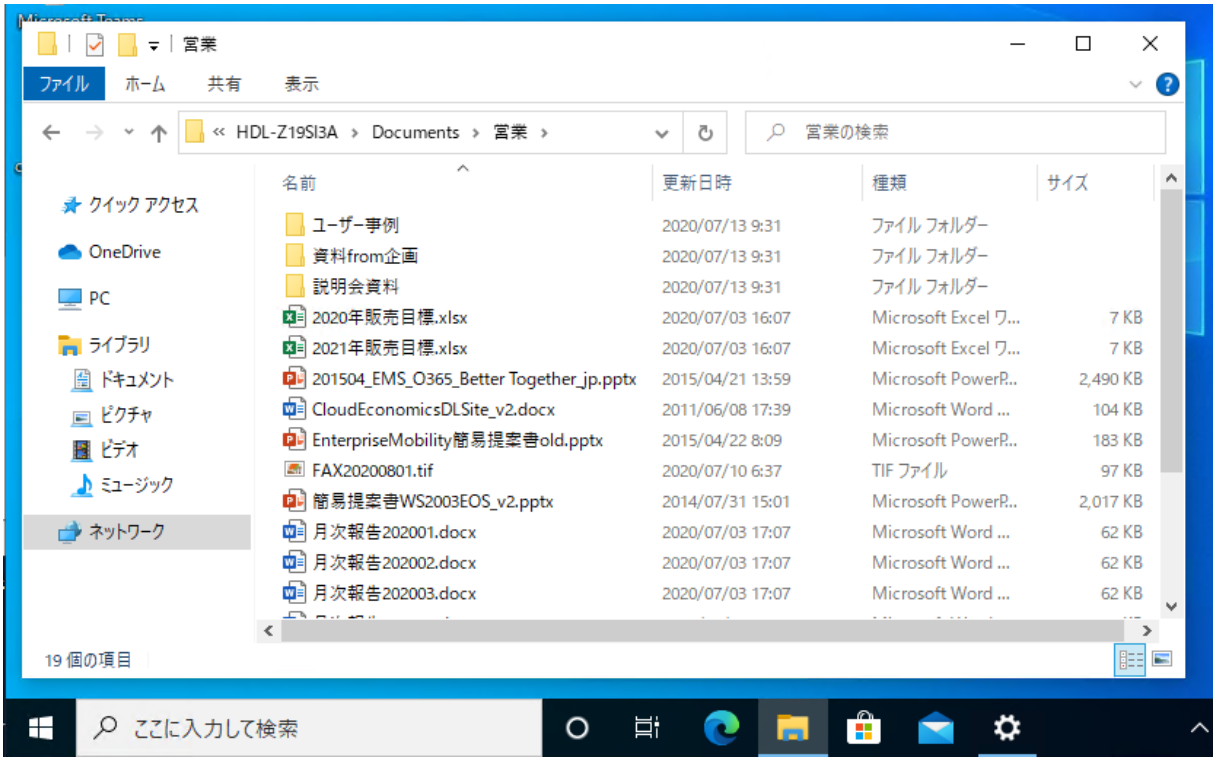
HDL-Z のための管理用端末について

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。ただし、可能な場合は「Windows Admin Center」のリモート管理環境を優先して使用してます。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。

SMB 共有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>とそのパスワードの組み合わせ）を使用して SMB 共有にアクセスすることを想定しています。SMB 共有は社内ネットワーク上で既に運用中であるものとします。

SMB 共有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。



画面：社内では SMB 共有（共有名 Documents）にアクセスできる環境が利用可能になっていることを想定

Azure ファイル共有のアクセスするユーザーについて

このガイドでは、シンプルな構成で簡単に導入できるように、Azure ファイル共有へのアクセスは、すべてのユーザーが単一のストレージアカウント名とストレージアカウントキー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ことを想定します。

シンプルに利用できるように、このガイドではストレージアカウント名とストレージアカウントキー以外に追加の認証は使用しません。そのため、ストレージアカウント名とストレージアカウントキーの取り扱いについてはユーザー各自が十分に注意する必要があります。

また、Azure ファイル共有に対するユーザーやグループによるアクセス制御は行わず、すべてのユーザーが同一権限ですべてのファイルを読み書きできる環境を構築します。厳密なアクセス許可については、次の『Windows の DACL の厳密なサポートのためには』を参照してください。

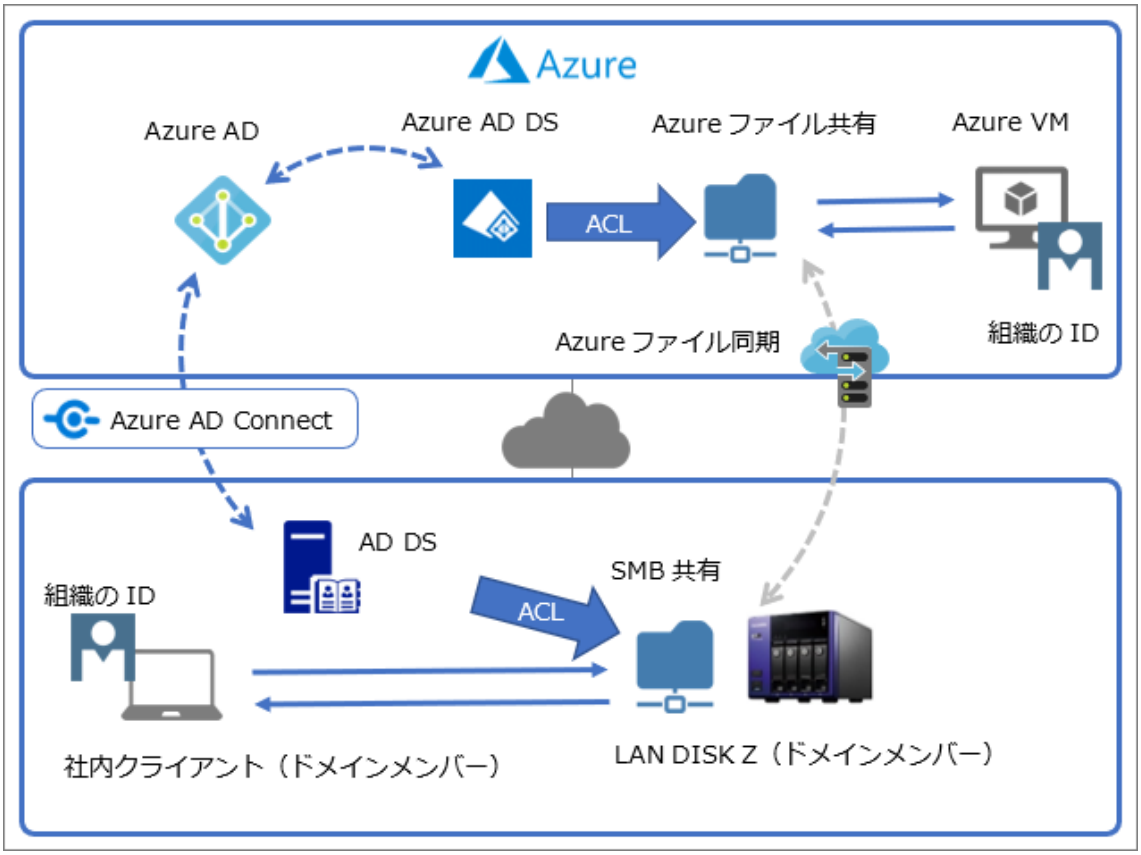
> Windows の DACL の厳密なサポートのためには
>
> Azure ファイル同期および Azure ファイル共有は、ACL（アクセス制御リスト）としても知られる Windows の DACL（随意アクセス制御リスト）を完全にサポートしています。Azure ファイル同期は同期対象の Windows Server 側の DACL を維持したまま Azure ファイル共有と同期できます。また、Azure ファイル共有はオンプレミスと「Active Directory ドメインサービス（AD DS）」またはクラウドの「Azure Active Directory ドメインサービス（Azure AD DS）」（Azure 仮想マシン向けのドメインサービス、Azure AD サービスに含まれる）を介した、SMB の ID ベースの認証とアクセス制御をサ

ポートしています（注：ドメイン認証ができないリモートワーク環境では利用できません）。

Azure ファイル共有で ID ベースの認証とアクセス制御を実現するには、オンプレミスの AD DS と「Azure Active Directory（Azure AD）」のディレクトリ同期をセットアップする必要があります。オンプレミスの Active Directory ドメイン環境および Azure 仮想マシンからは、ドメイン認証に基づいて Azure ファイル共有をマウントし、ファイルにアクセスできるため、ストレージアカウントキーを指定する必要がありません。

要件や構成が複雑になるためこのガイドでは説明しませんが、厳密なアクセス制御が必要な場合は以下のドキュメントを参考に実装してください。このガイドではリモートワーク環境を想定しているため、ストレージアカウントキーを使用したシンプルなファイル共有マウントについてのみ説明しています。

SMB アクセスの Azure Files ID ベース認証オプションの概要
https://docs.microsoft.com/ja-jp/azure/storage/files/storage-files-active-directory-overview



図：Azure ファイル共有の ID ベースの認証の展開イメージ。リモートワーク向けではない

2　リモートワーク向けのハイブリッドな共有環境の構築

HDL-Z のファイルサービスと、Azure ファイル共有および Azure ファイル同期のハイブリッド環境を構築するための一連の手順を説明します。

2.1　Azure サービスの準備

Azure ファイル共有および Azure ファイル同期を利用するには、はじめにクラウド側のサービスを準備しておきます。それには、管理用端末の Web ブラウザーを使用して Azure ポータル（https://portal.azure.com）に Azure サブスクリプションのアカウントの資格情報でサインインし、次の手順で準備します。

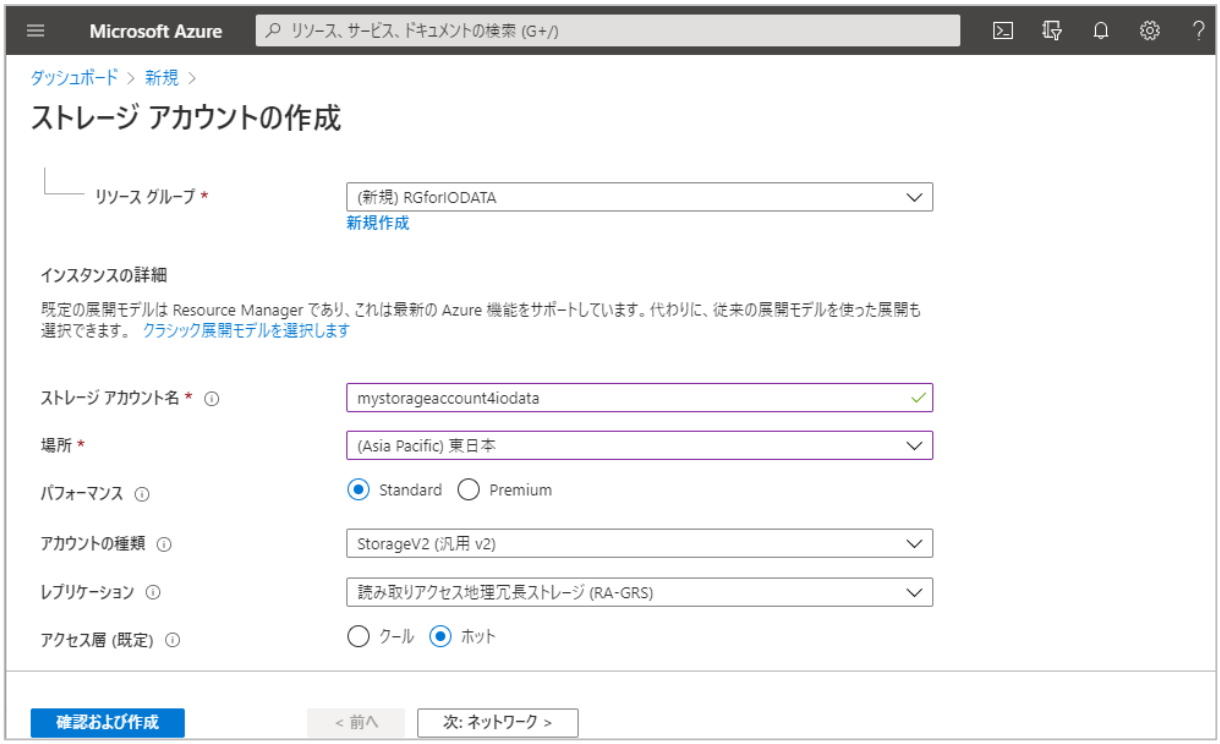
Azure ストレージアカウントの作成

Azure ファイル共有は、Azure ストレージアカウントが提供するストレージサービスの一部です。次の手順に従って、Azure ファイル共有をサポートする種類の Azure ストレージアカウントを作成します。

1. Azure ポータルで［＋リソースの作成］をクリックし、［ストレージ］－［ストレージアカウント］をクリックします。

2. ［ストレージアカウントの作成］ブレードが開始するので、リソースグループを新規作成するか、既存のリソースグループから選択し、［ストレージアカウント名］にグローバルに一意の名前を入力します。ストレージアカウント名に使用できるのは、小文字と数字のみで、3～24 文字である必要があります。

3. ［場所］にストレージアカウントを作成する Azure リージョン（例、西日本または東日本）を選択し、［アカウントの種類］として［StorageV2（汎用 v2)］（推奨）または［Storage（汎用 v1)］または［FileStorage］を選択します。Azure ファイル共有はこれらのいずれかの種類でサポートされます。コストとパフォーマンスの両面に柔軟に対応できるのは［StorageV2（汎用 v2)］です。［FileStorage］はコストが高いパフォーマンスレベル［Premium］のみで利用できますが、［StorageV2（汎用 v2)］は［Standard］と［Premium］のいずれかを選択できます。



画面：Azure ファイル共有用のストレージアカウントを作成する

4. その他の項目は既定のまま、［次：ネットワーク >］をクリックして［ネットワーク］タブに切り替えます。このあとの設定は既定のまま進みますが、内容を確認ながら気になるところがある場合は ⓘ をクリックして設定の意味を確認し、適宜設定してください。

5. 最後に、［確認および作成］タブにある［作成］をクリックしてサービスのデプロイを開始します。

> Azure データセンター（リージョン）の選択について
>
> Azure データセンターはグローバルに展開されており、日本国内にも東日本リージョン（東京）と西日本リージョン（大阪）の 2 つが設置されています。データを国内に置きたいという理由やネットワークの遅延を考慮すると、日本国内の企業は日本にあるいずれか（または両方）のリージョンを選択するでしょう。
>
> Azure ファイル共有に関して言えば、ネットワーク遅延を最小化したいのなら地理的に最寄りのリージョンを選択するのがよいでしょうし、大規模な災害時の事業継続性を考えれば地理的に距離のあるリージョンを選択するのがよいでしょう。なお、Azure ストレージアカウントのデータは、最もコストのかからないローカル冗長ストレージ（LRS）でも、リージョン内で 3 回同期的にレプリケートされ保護されます。

Azure ファイル共有の作成

ストレージアカウントのデプロイが完了したら、ストレージアカウントのリソースに移動し、次の手順に従ってファイル共有を作成します。

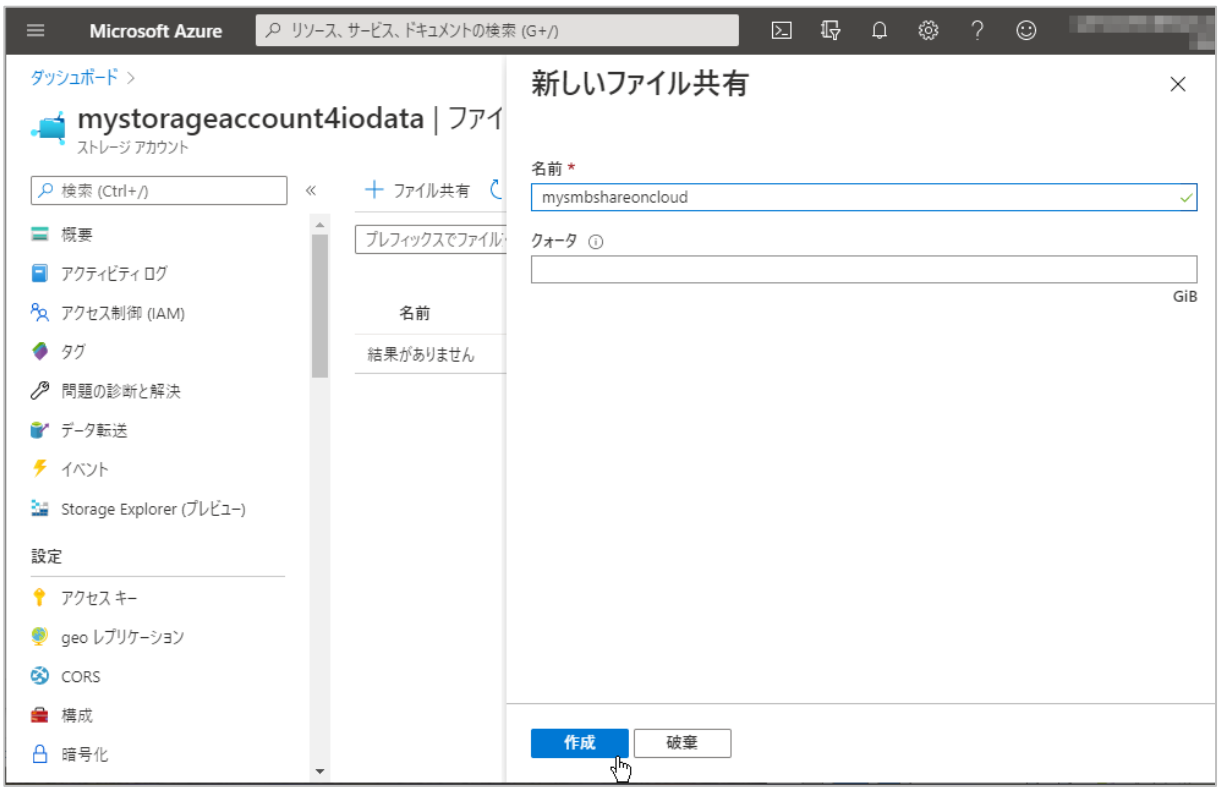
1. ストレージアカウントの［概要］ページにある［ファイル共有］をクリックします。

画面：ストレージアカウントのリソースに移動し、［ファイル共有］をクリックして開く

2. ［ストレージアカウント名｜ファイル共有］ページが開くので、［＋ファイル共有］をクリックし、［新しいファイル共有］の［名前］に共有名を入力します。共有名に使用できるのは、アルファベットの小文字、数字、ハイフンのみです。先頭と末尾はアルファベットである必要があります。また、ハイフン

を連続して使用することはできません。

3. ［作成］をクリックしてファイル共有を作成します。



画面：[＋ファイル共有］をクリックして、共有名を入力し、［作成］をクリックする。

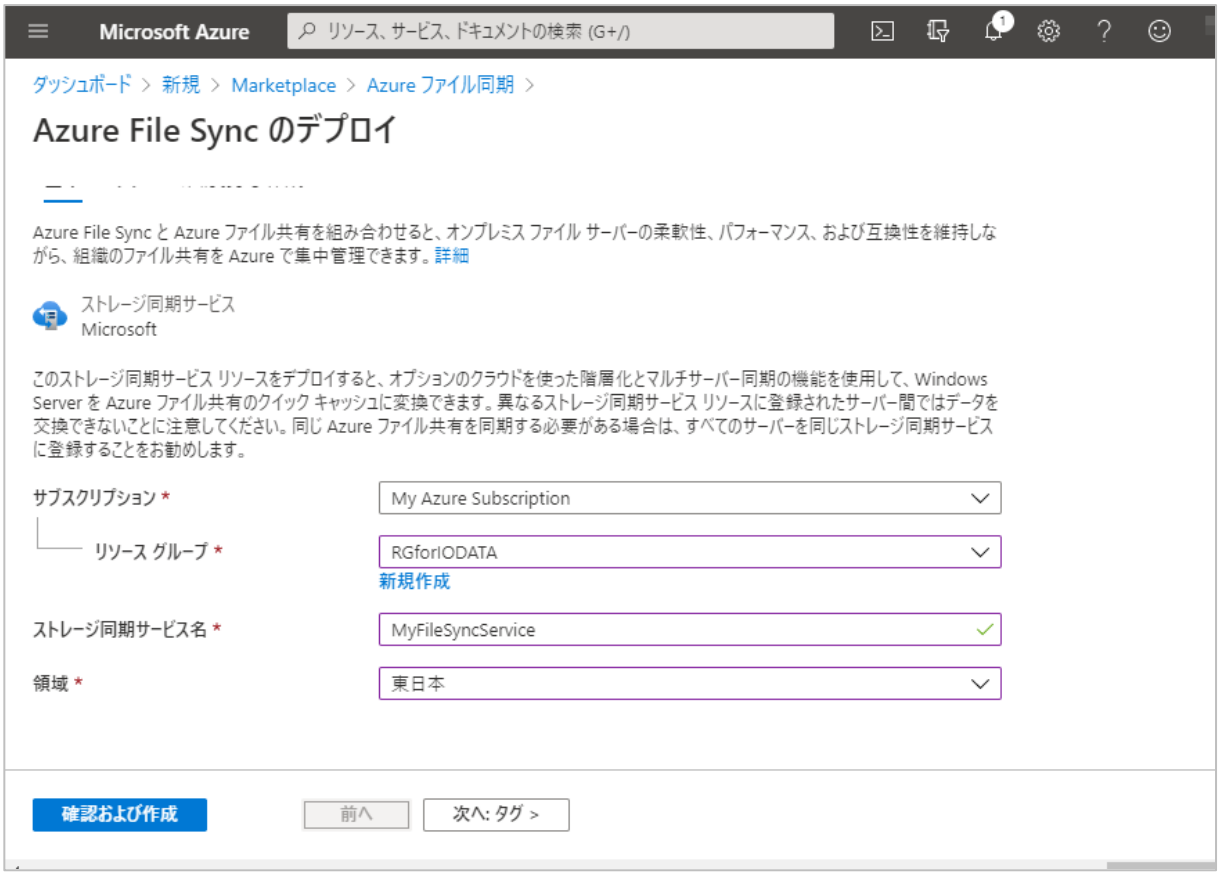
Azure ファイル同期サービスの準備

引き続き Azure ポータルを使用して、Azure ファイル同期のクラウド側サービスを準備します。次の手順に従って操作します。

1. ［＋リソースの作成］をクリックし、［ストレージ］－［Azure ファイル同期］をクリックして開き、［作成］をクリックします。サービスが見つからない場合は検索ボックス［🔍 Marketplace を検索］に「ファイル同期」と入力すれば見つかります。

2. ［Azure File Sync のデプロイ］ブレードが開始するので、リソースグループとしてストレージアカウントと同じものを選択し（必ずしも同じである必要はありません）、［ストレージ同期サービス名］に分かりやすい名前を入力します。ストレージ同期サービス名には、アルファベット、数字、スペース、ドット（.）、ハイフン（-）、アンダーバー（_）を使用でき、260 文字以内で指定できます。

3. Azure リージョン（領域）として、必ずストレージアカウントと同じリージョン（例、西日本または東日本）を選択して、［確認および作成］をクリックします。



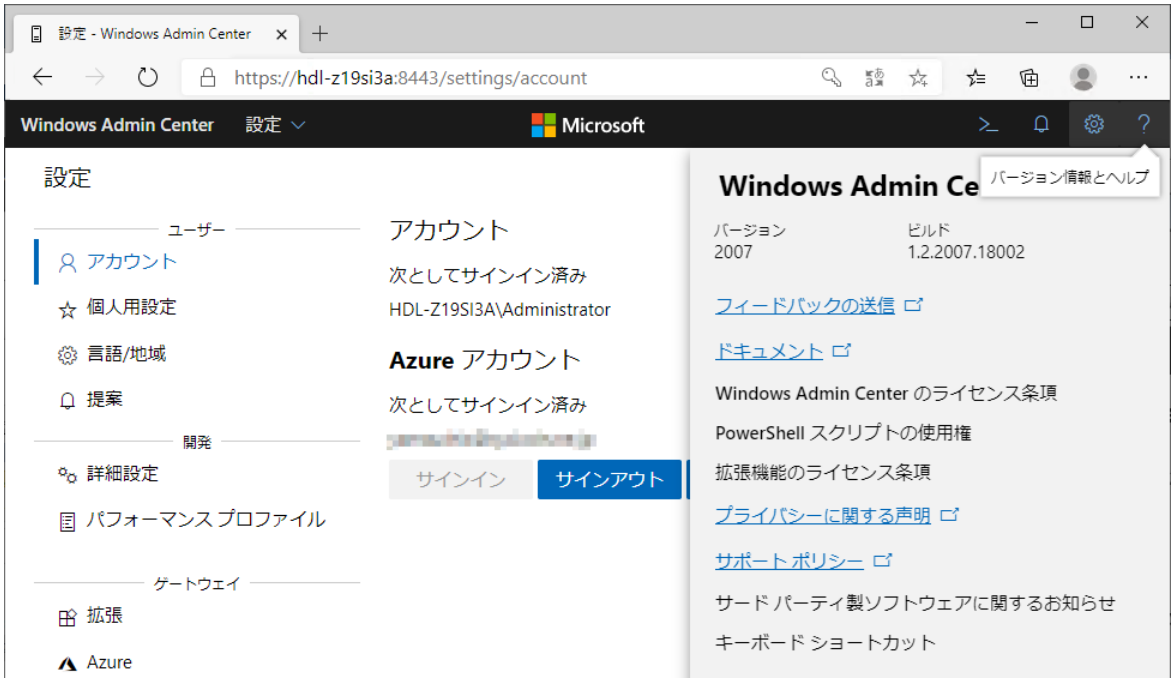
画面：ストレージアカウントと同じリージョンにストレージ同期サービスをデプロイする

4. 最後に、［確認および作成］タブにある［作成］をクリックしてサービスのデプロイを開始します。

2.2 Azure ファイル同期の構成

次に、HDL-Z で Azure ファイル同期を構成します。ここでの作業は、主に Windows Admin Center を使用します。Windows Admin Center を使用しない方法もありますが、Windows Admin Center を使用するほうが簡単です。

Windows Admin Center は、既にゲートウェイとして Azure に登録され、統合構成になっていることを前提とします。Windows Admin Center を Azure と統合する手順については、このガイドの前編『4. ハイブリッドクラウド編』で説明しています。



画面：Windows Admin Center の最新 GA バージョンがインストール済みであり、Azure との統合はセットアップ済み

> このガイドの前編『4. ハイブリッドクラウド編』の手順との違いについて
>
> 手順が異なる理由は、Windows Admin Center のバージョンの違いと、拡張機能「Azure File Sync」の機能改善によるものです。以前のバージョンに比べ、より多くのセットアップ作業を Windows Admin Center 側でできるようになりました。
>
> Windows Admin Center は、概ね半期に 1 回のサイクルで GA（一般提供）バージョンがリリースされます。このガイドの前編『3. 集中管理編』および『4. ハイブリッドクラウド編』は当時の最新 GA バージョンである 1904 に基づいています。今回のガイドは 2019 年 11 月にリリースされた GA バージョン 1910 のマイナーアップデート 1910.2 および 2020 年 7 月にリリースされた GA バージョン 2007 に基づいています。
>
> Windows Admin Center release history
> https://support.microsoft.com/en-us/help/3204979/

サーバーのシステム要件

Azure ファイル同期サービスは、Windows Server 2012 R2 以降の Windows Server、Windows Storage Server、および Windows Server IoT をサポートしています。サーバーには少なくとも 1 つの CPU と、2GB 以上のメモリが必要です。Windows Server IoT 2019 for Storage を搭載する HDL-Z は、これらすべてのシステム要件を満たしています。

また、Azure ファイル共有はローカルに直接接続された NTFS ボリュームのみでサポートされています。

Azure ファイル同期の互換性評価

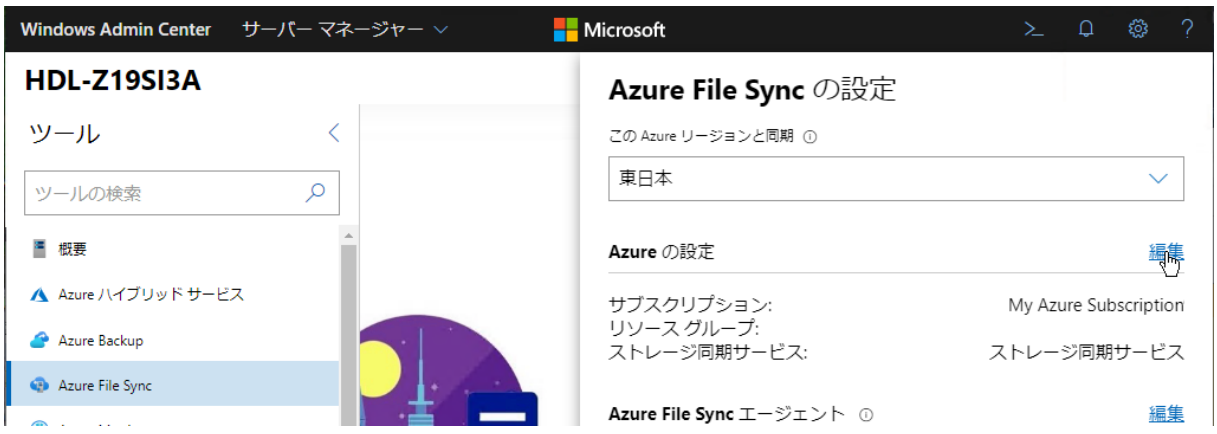
Azure ファイル同期を導入する前に、Azure PowerShell が提供する Azure ファイル共有用評価コマンドレットを使用して、システム情報と同期対象のデータの互換性をテストすることができます。HDL-Z のデスクトップで Windows PowerShell を開き、次の 2 行のコマンドレットを実行します（1 行目は Azure PowerShell がインストールされていない場合のみ）。

```
PS C:¥> Install-Module -Name Az -AllowClobber -Scope CurrentUser ↲

PS C:¥> Invoke-AzStorageSyncCompatibilityCheck -Path D:¥Share¥Documents ↲

Environment validation results:
Computer name: localhost
OS version check: Passed.
File system check: Passed.
Namespace validation results:
Path: D:¥Share¥Documents
Number of files scanned: 6012
Number of directories scanned: 368
There were no compatibility issues found with your files.
```

Azure ファイル同期のセットアップ

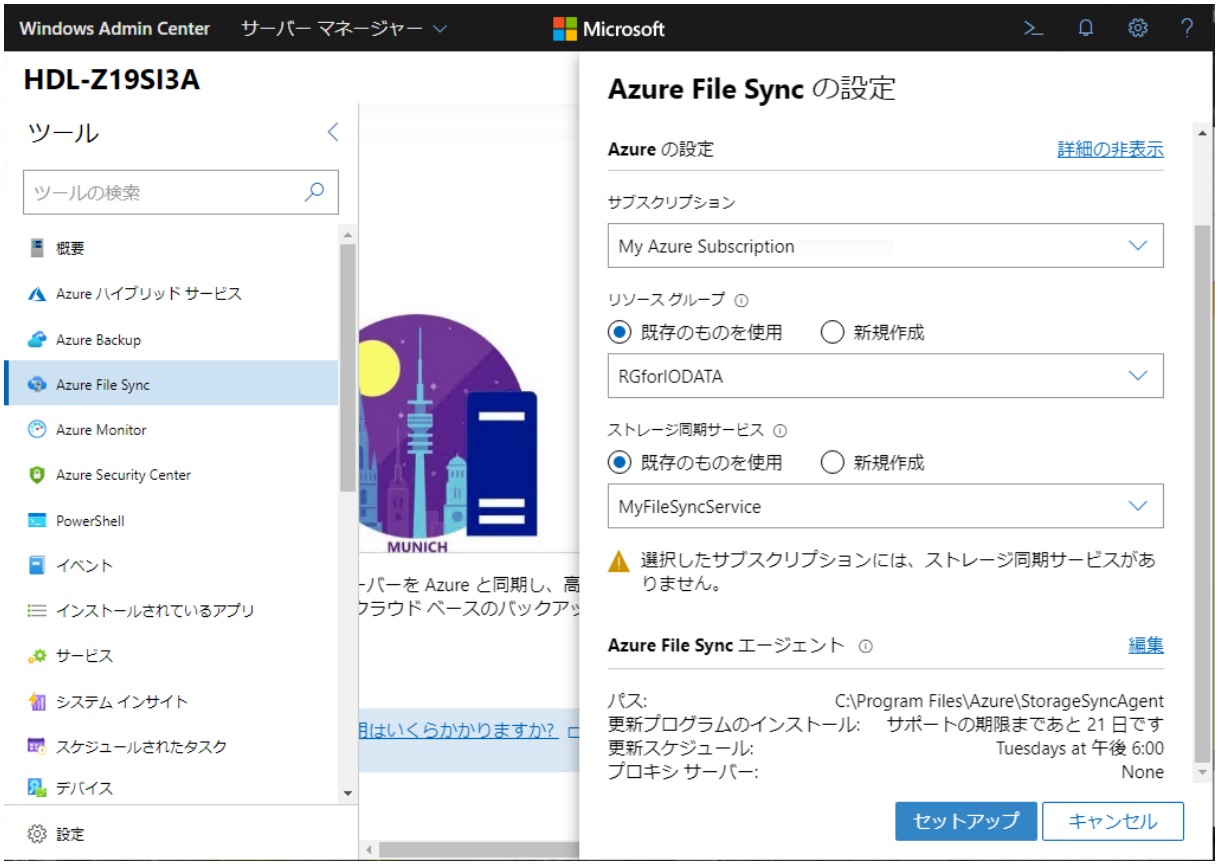
Windows Admin Center で HDL-Z にリモート接続し、次の手順に従って Azure ファイル同期のオンプレミス側の設定を行います。

1. Windows Admin Center の［Azure File Sync］ページを開き、［セットアップ］をクリックします。
2. ［Azure File Sync の設定］が開くので、［この Azure リージョンと同期］ドロップダウンリストから、Azure ファイル同期サービスを準備したのと一致するリージョン（例、西日本または東日本）を選択します。リージョンを選択できない場合は、次の手順に進んで［Azure の設定］を編集します。



画面：ストレージアカウントと Azure ファイル同期サービスをデプロイしたリージョンを選択する

3. ［Azure の設定］の［編集］をクリックし、［リソースグループ］と［ストレージ同期サービス］で［既存のものを使用］を選択し、ドロップダウンリストから事前に準備しておいた Azure ファイル同期サービスを選択して指定し、［セットアップ］をクリックします。



画面：Azure 側に事前に準備しておいたリソースグループと Azure ファイル同期サービスのストレージ同期サービスを選択する

4. Azure ファイル同期サービスのセットアップが完了したら、［閉じる］をクリックします。

画面：設定が完了したら［閉じる］をクリックする

同期グループの作成

最後に、オンプレミスのエンドポイント（ファイルサーバー）とクラウドのエンドポイント（Azure ファイル共有）の同期ペアを定義する同期グループを作成します。

この手順も、引き続き Windows Admin Center の［Azure File Sync］ページにある［フォルダーの同期］を使用してきるように見えますが、Windows Admin Center バージョン 2007（および以前のバージョン 1910.2）では Azure ファイル共有の情報の取得が失敗して機能しませんでした。Windows Admin Center の拡張機能「Azure File Sync」はプレビュー版であるため、プレビュー版の問題である可能性があります。そこで、このガイドの前編『4. ハイブリッドクラウド編』で説明したのと同様に、Azure ポータルで同期グループを作成する手順を説明しています。

1. Azure ポータルで［ストレージ同期サービス］を開き、事前に作成しておいたサービスのリソースに移動します。

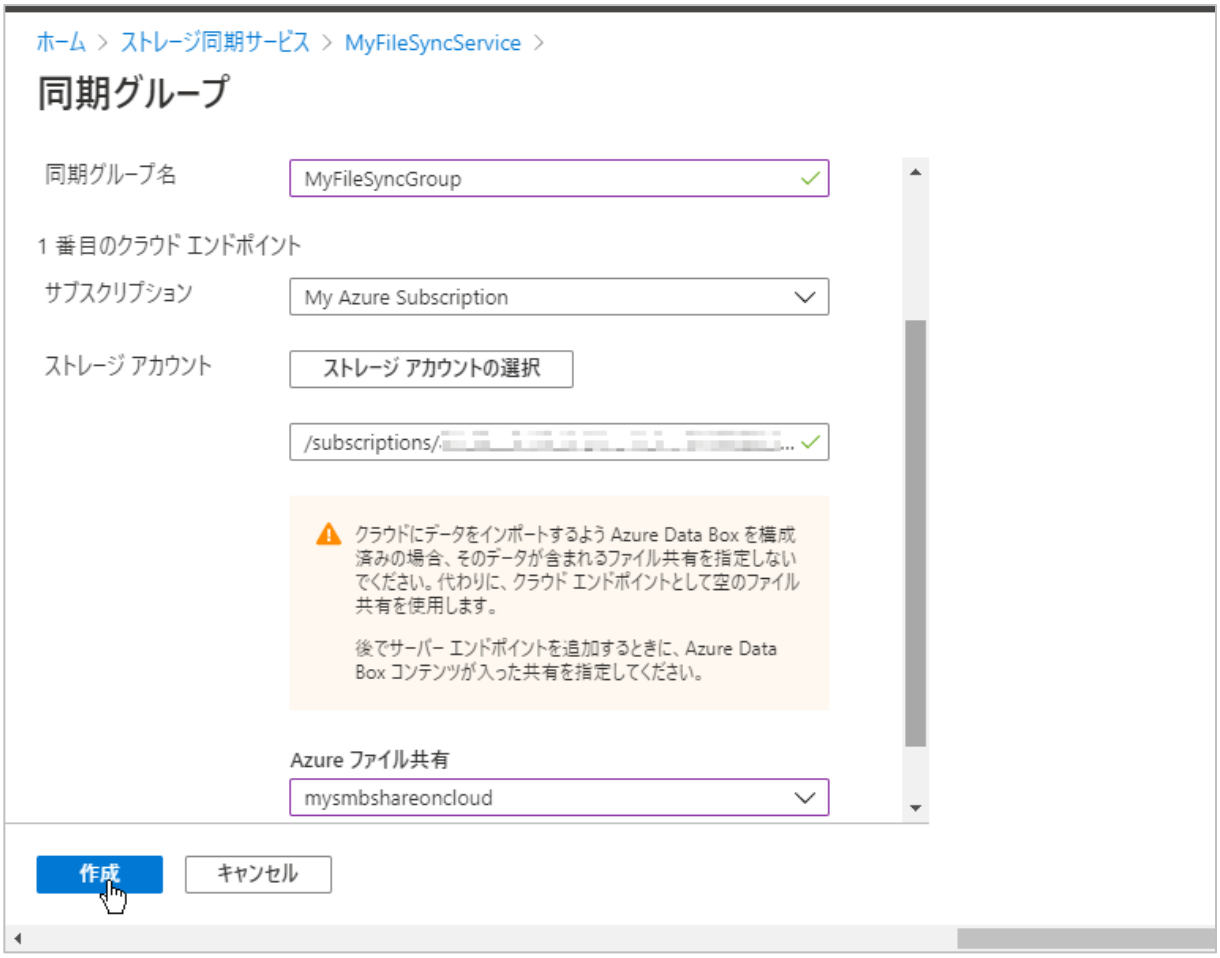
2. サービスの［概要］ページを開き、［＋同期グループ］をクリックします。

画面：Azure ポータルでストレージ同期サービスを開き、［＋同期グループ］をクリックする

3. ［同期グループ名］の名前を入力します。同期グループ名は、ストレージ同期サービス名と同様に、アルファベット、数字、スペース、ドット（.）、ハイフン（-）、アンダーバー（_）を使用できます。

4. ［ストレージアカウントの選択］をクリックし、同じ Azure リージョンに準備した Azure ファイル共有用のストレージアカウントを選択します。

5. ［Azure ファイル共有］ドロップダウンリストから事前に準備しておいた Azure ファイル共有の共有名を選択し、［作成］をクリックします。



画面：同期グループを作成し、クラウドエンドポイントとして Azure ファイル共有の共有を指定する

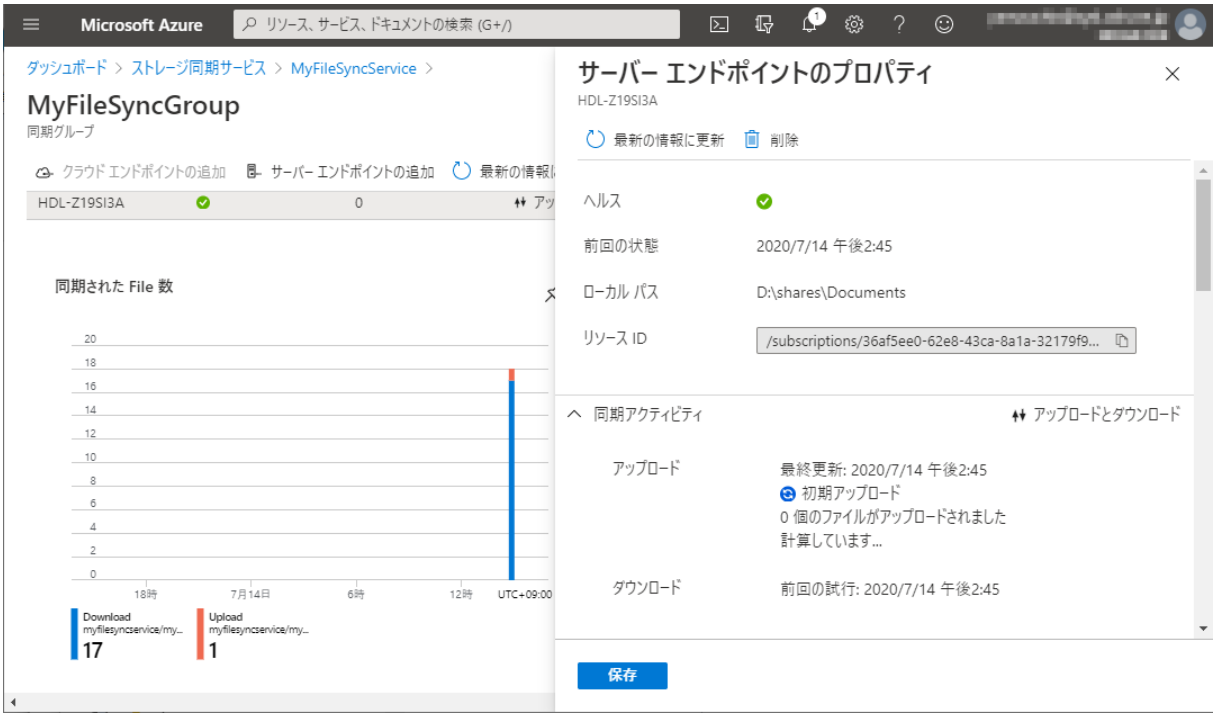
6. 同期グループの作成が完了したら、同期グループのページを開きます。この時点ではまだ、同期グループにはクラウド側のエンドポイントしかありません。そこで、[サーバーエンドポイントの追加] をクリックし、[登録済みサーバー] のドロップダウンリストから Windows Admin Center でセットアップしたサーバーを選択します。また、[パス] に同期対象のディレクトリパスを入力します。

7. [作成] をクリックし、サーバーエンドポイントの作成が完了すると、サーバーエンドポイントとクラウドエンドポイント間の同期がスタートします。

画面：サーバーエンドポイントとして登録済みサーバー（Windows Admin Center でセットアップしたもの）を選択し、同期対象のディレクトリパス（例、D:¥Shares¥Documents）を指定する

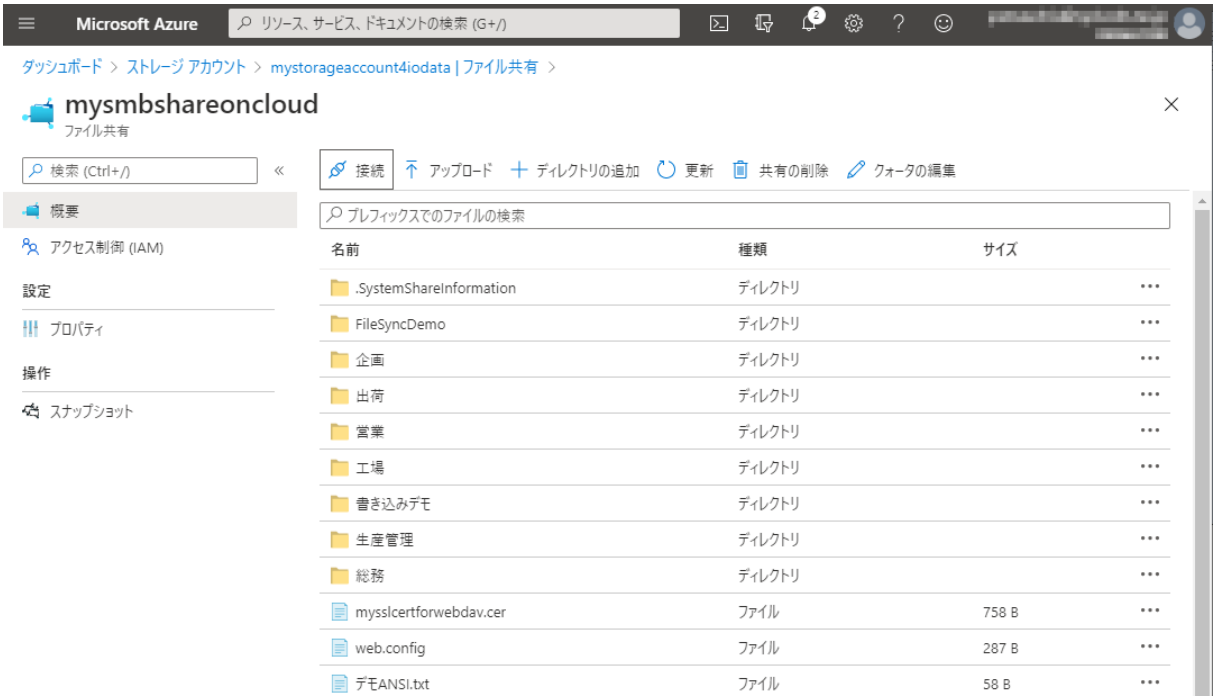
8. 同期グループのセットアップが完了すると、Windows Admin Center の［Azure File Sync］ページにも同期グループが表示されます。サーバーエンドポイントの同期の状態は、同期グループのサーバーエンドポイントの［ヘルス］列や［同期アクティビティ］列、グラフ（同期された File 数／同期したバイト数）およびエンドポイントのプロパティで確認することができます。なお、最新状態の反映までにはタイムラグがあります。また、初期の同期が完了するまでにはしばらく時間がかかります。

画面：Windows Admin Center に表示された同期グループ。リンク先は Azure ポータル



画面：サーバーエンドポイントのプロパティで同期のステータスを確認する

9. サーバーエンドポイントのデータが Azure ファイル共有に実際に同期されていることを確認するには、Azureポータルでストレージアカウントのファイル共有のページを開きます。なお、初期同期の完了後、オンプレミスのサーバーに対する変更は直ちに Azure ファイル共有に同期されますが、Azure ファイル共有に対して行われた変更はオンプレミスのサーバーに同期されるまで最大 24 時間かかります（その理由については最後に説明します）。



画面：Azure ポータルを使用して、Azure ファイル共有を参照する。ここからファイルのダウンロードやアップロードも可能

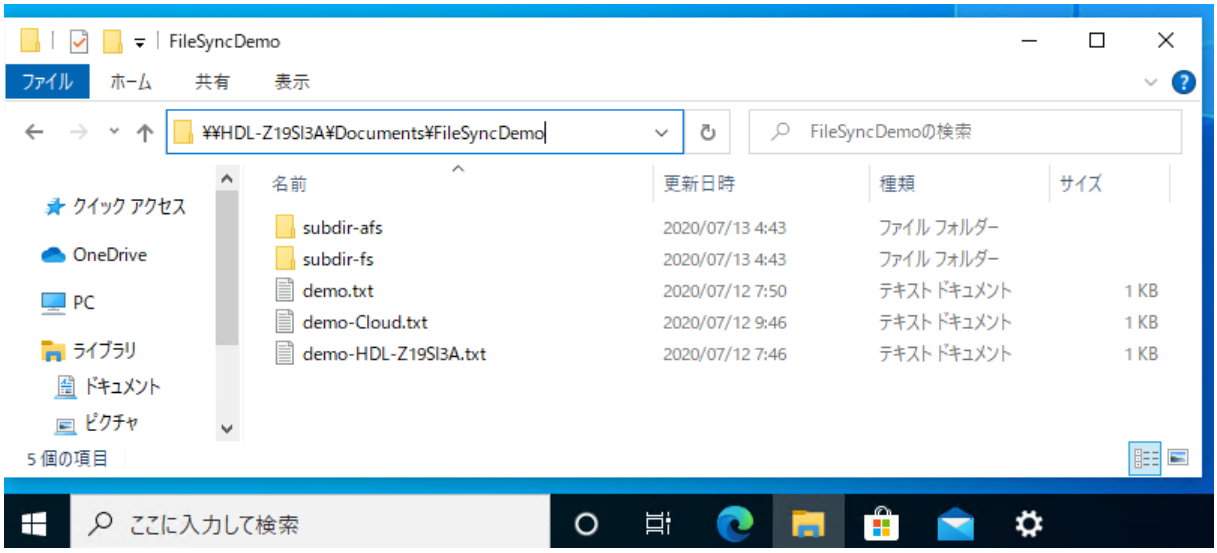
3　リモートワーク環境からのデータアクセス

リモートワーク中の社員が、Azure ファイル共有を介して HDL-Z に保存されたデータにアクセスしたり、データをアップロードしたりする方法について説明します。

データの競合やタイムラグについての考慮事項

このガイドで説明しているのは、ストレージアカウントキーを使用したシンプルな Azure ファイル共有の利用方法です。ユーザーごとに個別に認証を求めたり、ユーザーごとのアクセス制御を行うことは想定していません。

同時期にオンプレミスと Azure ファイル共有の両方で同じファイルが変更された場合、競合を回避するためにファイル名にサフィックスが付与され、別ファイルとして保持されます。例えば、オンプレミスと Azure ファイル共有の両方で「demo.txt」が更新されると、オンプレミス側の変更は同期後に「demo-<サーバーエンドポイントのコンピューター名>.txt」という名前で別のファイルに保存されます。Azure ファイル共有側での変更は、同期後に「demo-Cloud.txt」という名前で別のファイルに保存されます。



画面：競合が発生する場合、ファイル名にサフィックスが付与されて別ファイルとして保存され、競合が回避される。

また、Azure ファイル共有に対して SMB 経由で直接的に行われた変更は、オンプレミスのサーバーに同期されるまで最大 24 時間かかる場合があることにも留意してください（その理由については最後に説明します）。

Azure ファイル共有と Azure ファイル同期のソリューションはこのような制約やタイムラグがあるため、出社した社員とリモートワーク中の社員に対してリアルタイム性のある共同作業を提供できるわけではないことに注意してください。

3.1　クライアントのシステム要件

Windows 8.1 以降（Windows 8 はサポートが終了しています）の Windows、および Windows Server 2012 以降の Windows Server は、SMB v3 に対応しており、インターネット経由で Azure ファイル共有に接続できます。

macOS および Linux についても、最近のバージョンでは SMB v3 をサポートしており、Azure ファイル共有に接続可能です。詳細なシステム要件および Azure ファイル共有の接続方法については、以下のドキュメントで確認してください。

macOS を使用して SMB 経由で Azure ファイル共有をマウントする
https://docs.microsoft.com/ja-jp/azure/storage/files/storage-how-to-use-files-mac

Linux で Azure Files を使用する
https://docs.microsoft.com/ja-jp/azure/storage/files/storage-how-to-use-files-linux

このガイドでは Windows 10 での手順についてのみ説明します。

Azure ファイル共有にアクセスするためのファイアウォール要件

Azure ファイル共有に SMB クライアントからアクセスするためには、経由するネットワークデバイスで出力方向の TCP ポート 445（Direct Hosting of SMB）の通信が許可されている必要があります。利用中のネットワークデバイスによっては（特に、一般家庭でも利用されるブロードバンドルーター）、TCP ポート 445 を含むインターネットへの SMB トラフィックの発信方向のトラフィックをブロックする設定がされていることがあるので留意してください。

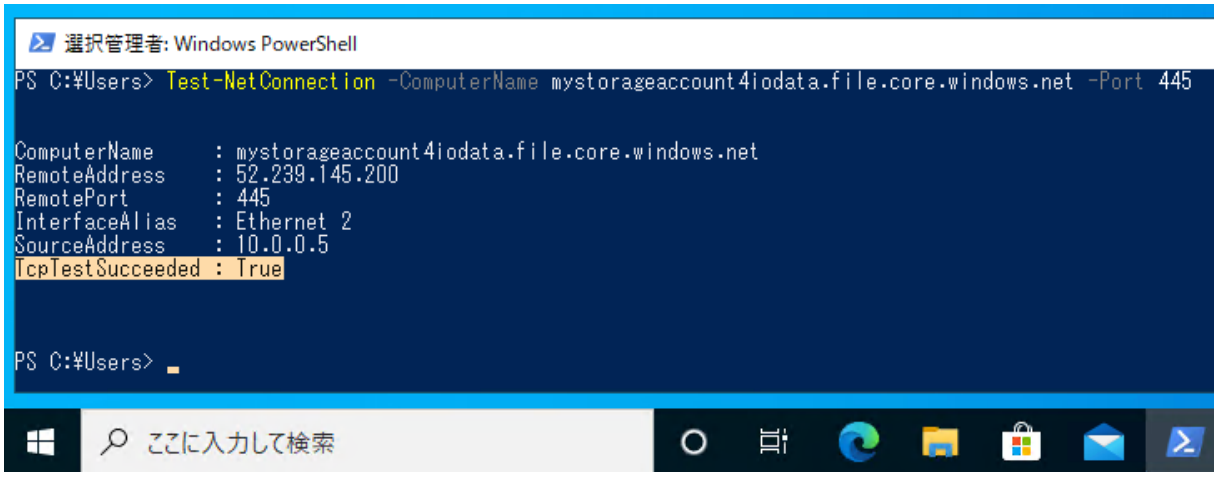
ネットワークデバイスで TCP ポート 445（Direct Hosting of SMB）の発信トラフィックをブロックするファイアウォールルールが存在する場合は削除します。なお、SMB のレガシなプロトコルである NetBIOS over TCP/IP（NBT）の TCP/UDP ポート 135～139 の発信はブロックすることが推奨されており、許可するべきではありません。

画面：TCP ポート 445 の発信トラフィックをブロックするブロードバンドルーターの設定例

インターネットサービスプロバイダー（ISP）が SMB をブロックしている場合や、マンションなどの共同のインターネット設備で SMB をブロックしている場合は、残念ながらそのインターネット環境からは Azure ファイル共有に接続することはできません。その場合、スマートフォンの Wi-Fi デザリングなど、別のインターネット接続を検討してください。

Windows PowerShell で Test-NetConnetion コマンドレットを実行すると、ローカルのエンドポイントから Azure ファイル共有へのネットワークの接続性を検査することができます。

```
PS C:¥> Test-NetConnection -ComputerName <ストレージアカウント名
>.file.core.windows.net -Port 445 ↲

...

TcpTestSucceeded        :True（成功）または False（失敗）
```



画面：Test-NetConnection コマンドレットで Azure ファイル共有の TCP ポート 445 への接続性を確認する

3.2　Azure ファイル共有のローカルマウント

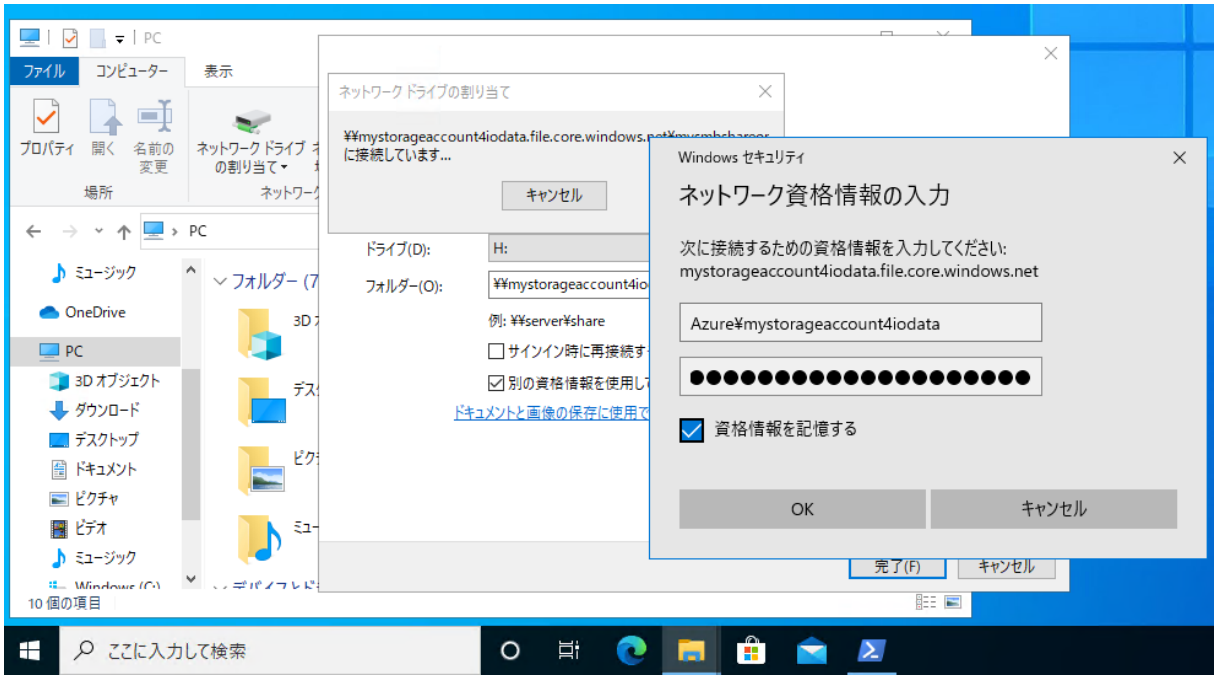
Azure ファイル共有に接続するために必要なのは、簡単に言ってしまえば「ストレージアカウント名」と「アクセスキー」だけです。これらの情報は、Azure サブスクリプションの管理者であれば、Azure ポータルのストレージアカウントの［アクセスキー］ページで確認できます。管理者はユーザーに対してこれらの情報と手順を伝えて、指示してあげればよいのです。もちろん、ユーザーに対しては、セキュリティ上、極めて重要な情報であって、決して漏れてはいけない情報であることを伝えてください。

画面：ストレージアカウントのアクセスキーを確認する

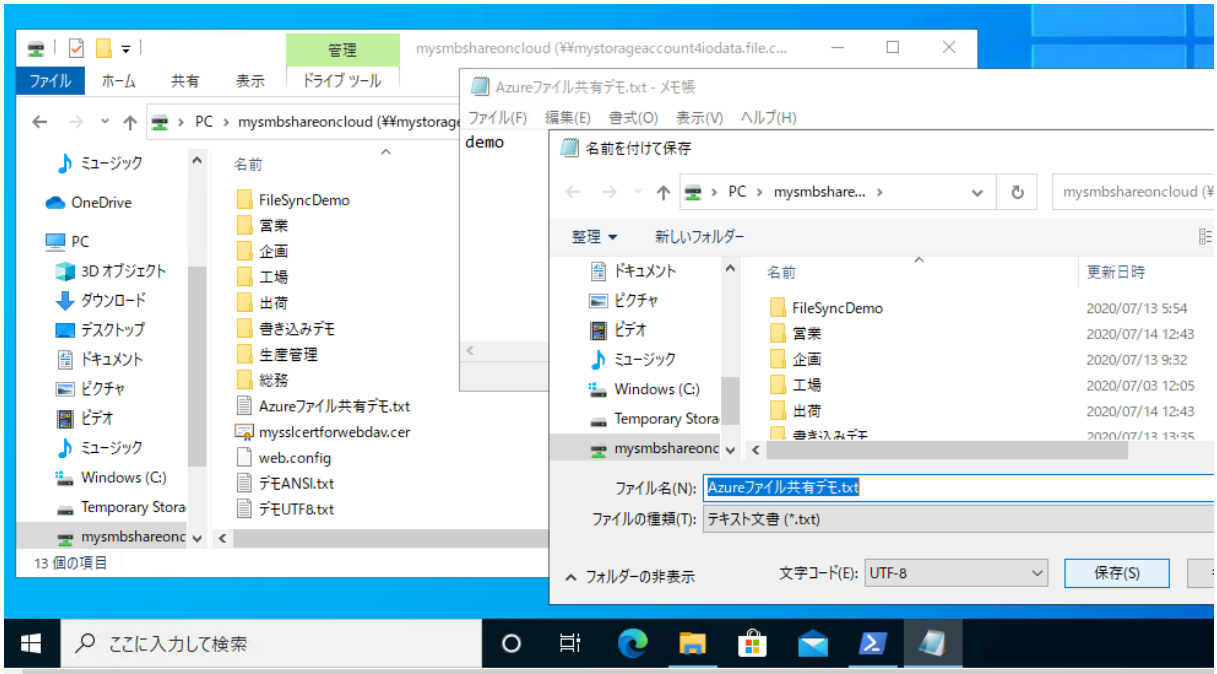
エクスプローラーでマウントする

Azure ファイル共有に接続するには、［エクスプローラー］の［ネットワークドライブの割り当て］または［ネットワークの場所の追加］を使用して、次の情報を指定して接続します。

UNC 名	¥¥<ストレージアカウント名>.file.core.windows.net¥<Azure ファイル共有名>
ユーザー名	Azure¥<ストレージアカウント名>
パスワード	<ストレージアカウントのアクセスキー>



画面：Azure ファイル共有をストレージアカウント名とアクセスキーの資格情報でマウントする

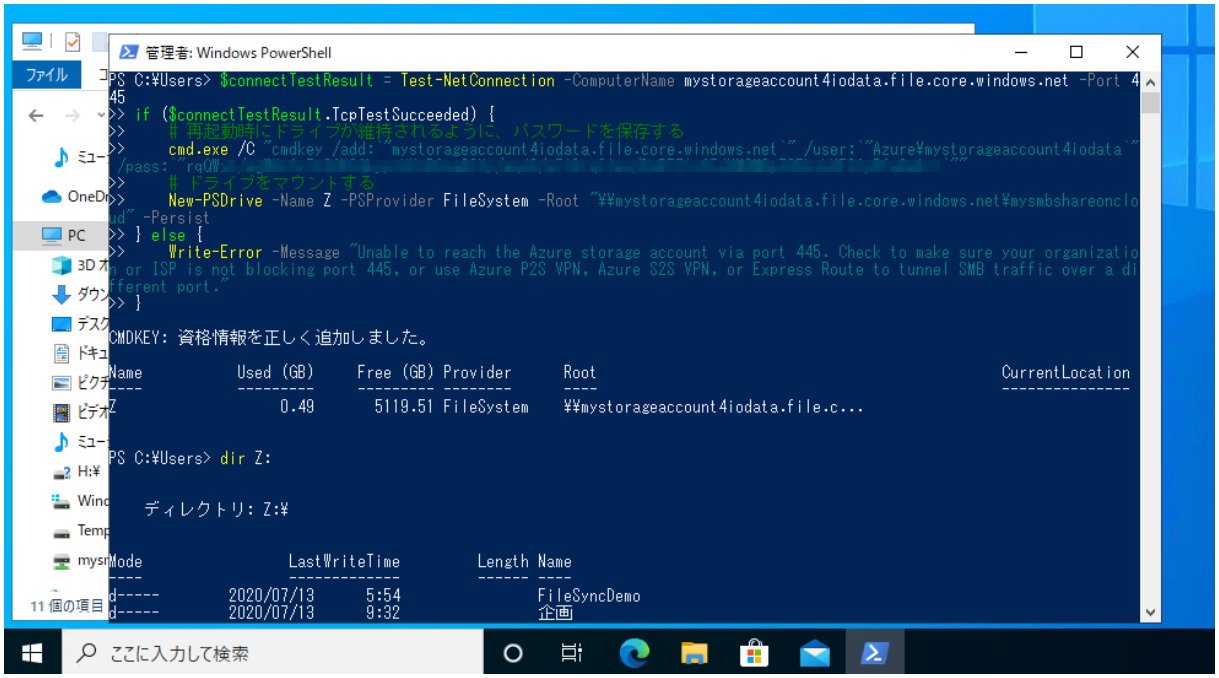


画面：Azure ファイル共有に接続後は通常のファイル操作で読み書きできる

スクリプトを利用してマウントする

Azure ポータルのストレージアカウントの［ファイル共有］のページを開き、［接続］をクリックすると、Windows、Linux、macOS の各プラットフォーム用に、コマンドラインで接続するためのスクリプトを自動生成してくれます。例えば、Windows の場合は、Windows PowerShell のコマンドライン（一般ユーザーとして実行）を入手できます。このスクリプトをコピーして利用者に渡し、実行してもらうこともできます。

画面：ドライブ文字にマウントするスクリプトを自動生成



画面：Windows PowerShell（非管理者）でコマンドラインを実行してネットワークドライブにマウントする

SMB 経由で Azure ファイル共有に加えられた変更がサーバーエンドポイントに反映されるまでに最大 24 時間かかることについて

サーバーエンドポイントに対してオンプレミスで行われた変更は、Azure ファイル同期エージェントによって直ちに検出され、Azure ファイル共有にアップロード同期されます。

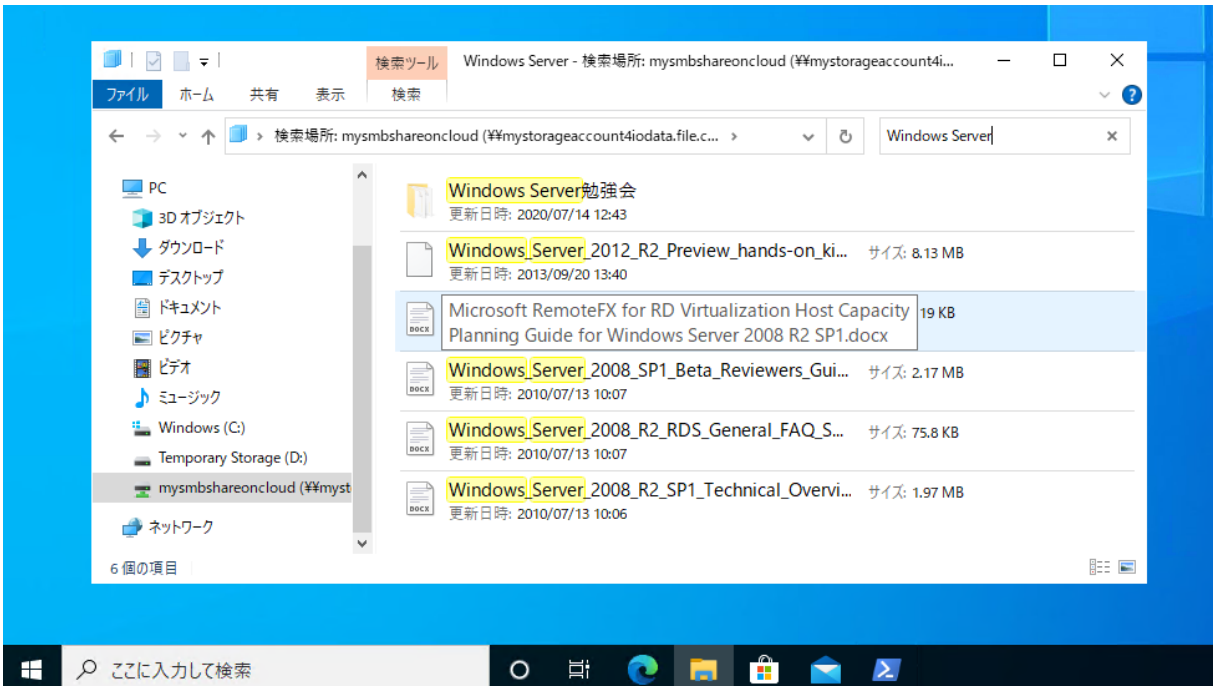
一方、SMB v3 経由、または Azure ポータル経由（Storage Explorer などを使用）で Azure ファイル共有に対して直接的に行われた変更は、サーバーエンドポイントにダウンロード同期されるまでには最大で 24 時間がかかる場合があります（ファイル数が多い場合はそれ以上かかる可能性もあります）。これは、Azure ファイル共有に対する変更検出ジョブが 24 時間ごとに実行されるからです。ただし、同じファイルに対する変更の競合状態は、サーバーエンドポイントからのアップロード同期時に検出され、即座にダウンロード同期されます。

現在、Windows Server のような変更検出を Azure ファイル共有にむけて調査が行われています。ユーザーからの要望が多ければ、優先的に開発が勧められるとのことです。

Azure Files に関してよく寄せられる質問（FAQ）
https://docs.microsoft.com/ja-jp/azure/storage/files/storage-files-faq

Azure ファイル共有の検索について

Azure ファイル共有に接続したクライアントは、「エクスプローラー」の検索機能を利用してファイル名やフォルダー名による検索が可能です。フルテキスト検索のためのインデックスは持たないため、ドキュメントのコンテンツ（内容）に基づいた検索はできません。



画面：Azure ファイル共有ではファイル名やフォルダー名の部分一致による検索が可能

Azure ファイル共有のインデックス検索については、ユーザーからのフィードバックに基づいて現在、開発中とのことです。

Indexer for Azure File shares
https://feedback.azure.com/forums/263029-azure-search/suggestions/14274261-indexer-for-azure-file-shares

Microsoft Azure には、「Azure Cognitive Search（旧称、Azure Search）」サービスというストレージアカウントのフルテキスト検索にも対応したサービスもあります。このサービスは企業のプライベートな Web アプリ／サービスに対して、異種コンテンツに対する高度な検索機能を追加するための REST API とツールを開発者に対して提供するものです。「エクスプローラー」の検索機能（Windows Search）に検索機能を提供するような目的では使用できません。

Azure Cognitive Search（製品サイト）
https://azure.microsoft.com/ja-jp/services/search/

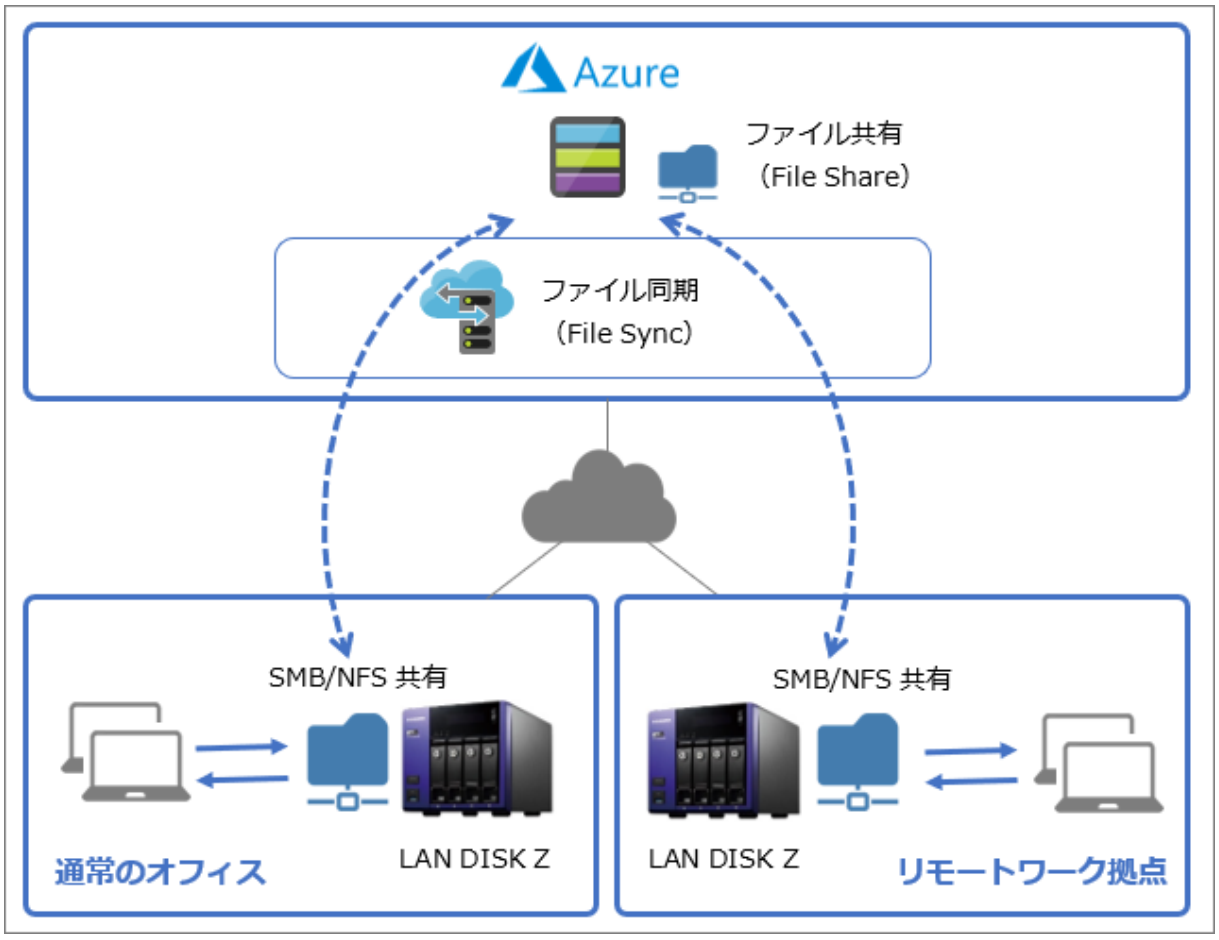
Azure Cognitive Search とは（ドキュメント）
https://docs.microsoft.com/ja-jp/azure/search/search-what-is-azure-search

4 ［応用例］リモートワーク拠点のファイルサーバーとして

リモートワーク対応のための Azure ファイル共有／ファイル同期サービスの応用例を紹介します。

例えば、パンデミック対策として、感染リスクの少ない地方に新たなオフィスの拠点を用意し、複数の社員で利用するファイルサーバーとして新規に HDL-Z を導入するとします。会社のオフィスのファイルサーバー（または HDL-Z）にある大量の大容量のドキュメント群を、新規の HDL-Z でも利用可能にするために、Azure ファイル共有と Azure ファイル同期サービスを活用することができます。

Azure ファイル同期サービスは、1 つの Azure ファイル共有を含む同じ同期グループに、複数のサーバーエンドポイントを追加することができます。Azure ファイル共有を仲介して、サーバーエンドポイント間のファイルの双方向レプリケーションを実現できるのです。



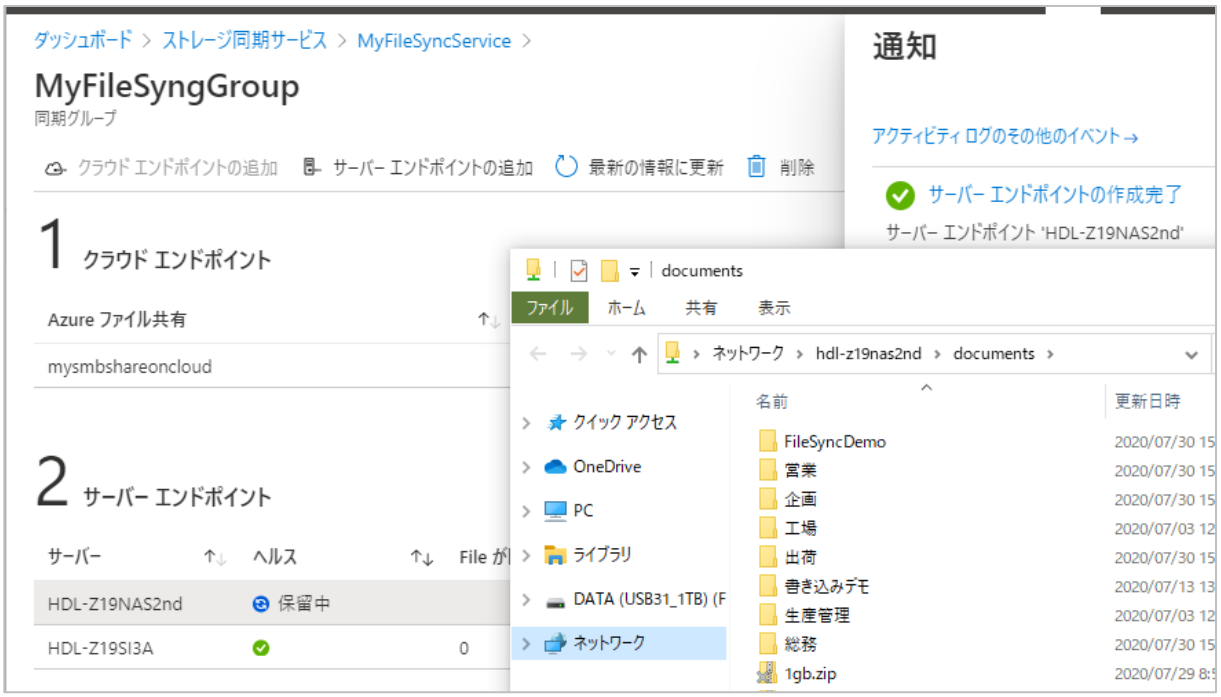
図：Azure のサービスを介して 2 台の HDL-Z の共有フォルダーを拠点間で同期する

この方法は、特別なネットワーク環境を用意することなく、簡単に実現できることがポイントです。会社のオフィスとリモート拠点の両方とも、インターネット接続があればよく、オフィスとリモート拠点間を仮想プライベートネットワーク（VPN）などでつなぐ必要はありません。なお、同じ拠点内での 2 台の HDL-Z 間のレプリケーションについては、このガイドの前編『4. ハイブリッドクラウド編』で説明した「クローン for Windows」の利用をお勧めします。

この方法を実装するために、難しい作業は一切ありません。1 台目のファイルサーバー（HDL-Z）と Azure

ファイル共有を Azure ファイル同期サービスで同期するようにセットアップしてあれば、同じ同期グループ内に 2 台目のファイルサーバー（HDL-Z）をサーバーエンドポイントとして追加すればよいのです。

画面：2 台目の HDL-Z をサーバーエンドポイントとして同期グループに追加する



画面：Azure ファイル同期により、Azure ストレージアカウントを介して 2 台の HDL-Z 間で共有フォルダーのコンテンツが双方向に同期される

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/