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

で構築する企業向け最新ファイルサーバー

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

2019年8月7日

内容

1　概要

1.1　このガイドについて

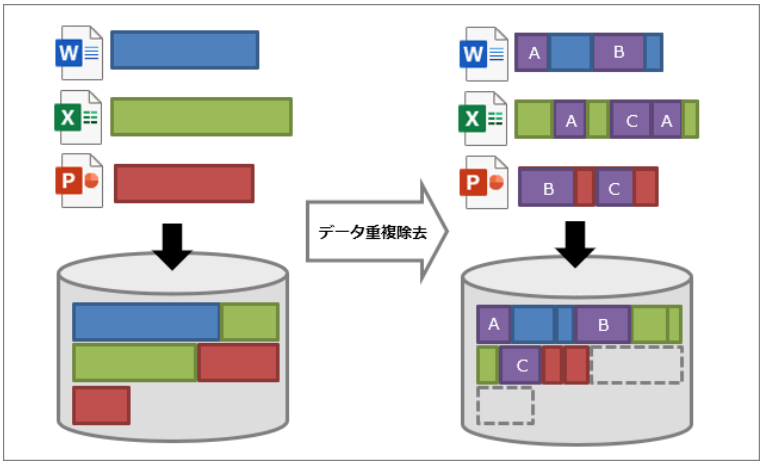
このガイドは、Windows Server IoT 2019 for Storage Standard または Workgroup を搭載する LAN DISK Z シリーズの NAS デバイスを新規に導入するにあたり、より効率的でセキュリティが高く、高速なファイル共有インフラストラクチャ（基盤）をエンドユーザーに提供するために、ストレージおよびネットワークを最適化するポイントについて解説します。

1.2　ファイルサーバーのボリュームおよびネットワークの最適化について

Windows Server IoT 2019 for Storage Standard または Workgroup を搭載する LAN DISK Z シリーズは、Windows Server 2019 と共通のファイルサーバー機能を搭載しており、Windows Server 2019 と同じ手順で構成、管理、および利用することができます。このガイドでは、インフラストラクチャ部分に関わる以下の 4 つの機能のセットアップ方法について説明します。これらの機能は運用を開始して、後になって構成することもできますが、バックグラウンドで実行されるタスクの負荷や、ネットワークの変更がエンドユーザーに影響しないように、導入後、早い段階でセットアップしておくことをお勧めします。

- データ重複除去（Standard のみ）
- NIC チーミング
- SMB マルチチャンネル
- SMB 暗号化

データ重複除去（Standard のみ）



データ重複除去（Data Deduplication）は、ストレージに格納されるデータから冗長な部分を削除し、ストレージの使用を効率化する Windows Server 2012 からの機能です。データ重複除去はファイル単位の圧縮技術ではなく、ボリューム上のファイル全体で繰り返されるパターンを特定し、個々のファイルをその繰り返されるパターンのチャンク（小さな塊）に分割して、重複するチャンクを 1 回だけ保存し、必要に応じてさらに圧縮することで、データの完全性を損なうことなく使用領域を解放し、ディスク使用を効率化します。一般的なファイル共有としての利用シナリオ（ユーザーデータ、ライブラリ、ISO/VHD イメージなどを格納）において、50～60%の重複除去率を期待できます。

データ重複除去がサポートされるのは Windows Server IoT for Storage Standard

データ重複除去機能は、OEM 製品である Windows Server 2019 IoT for Storage では、Standard エディションでサポートされる機能です。Workgroup エディションでは利用できないことに注意してください。リテール製品およびボリュームライセンス製品の Windows Server 2019 では、Standard および Datacenter エディションでサポートされる機能であり、Essentials エディションではサポートされません。

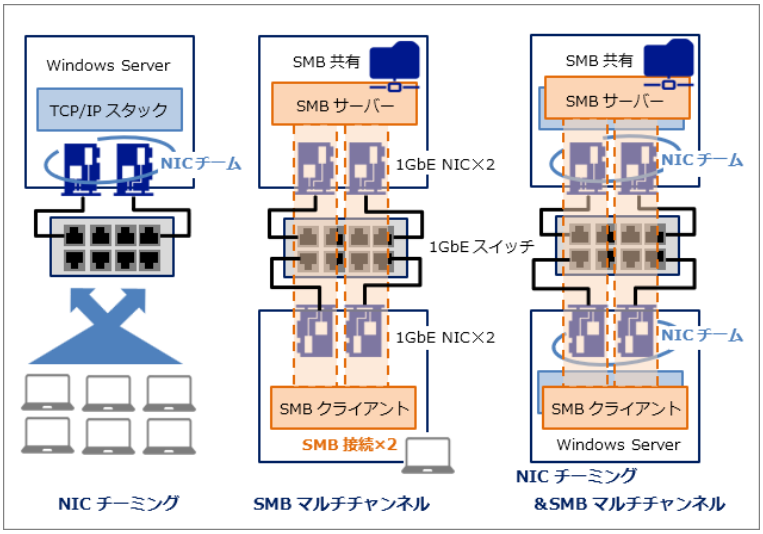
NIC チーミング

NIC チーミング（Load Balancing and Failover : LBFO とも呼ばれます）は、複数のネットワークアダプター（NIC）を束ねることで、冗長化による可用性の向上と負荷分散、および帯域幅の集約を可能にする Windows Server 2012 R2 からの OS の標準機能です。次に説明する SMB マルチチャンネルとは異なり、TCP スタックに対して複数の物理的な NIC（最大 32）を 1 つの論理的な NIC（NIC チーム）に見せるため、アプリケーションに依存することなく、さまざまな種類のネットワークトラフィックに対応できます。

SMB マルチチャンネル

Windows 8 および Windows Server 2012 から登場した Windows ファイル共有プロトコル、SMB（サーバーメッセージブロック）の最新バージョン SMB v3 は、SMB ダイレクト（SMB Direct、SMB over RDMA）、SMB マルチチャンネル（SMB MultiChannel）、SMB 暗号化など、高速化、冗長化、セキュリティのためのさまざまな機能を提供します。RDMA（Remote Direct Memory Access）を必要とする SMB ダイレクトは、10GbE ネットワークの帯域幅を最大限に活用できる高速化機能ですが、高価な NIC を必要とする、データセンター向けの機能です。これに対して、SMB マルチチャンネルは、SMB サーバー（ファイルサーバー）と SMB クライアントの両方で複数の NIC を利用可能な場合、または両方で 1 つ以上の RSS（Receive Side Scaling）対応の NIC を利用可能な場合に、複数の SMB セッションを作成して多重で通信を行う、帯域幅の集約機能です。複数の NIC が使用される場合は、1 つの経路（NIC、ケーブル、スイッチ）が障害になったとしても、残りの接続で SMB セッションを継続する SMB フェールオーバー機能も備えています。

LAN DISK Z は 2 または 4 ポートの物理 NIC を備えており、NIC チーミングと SMB マルチチャンネルの両方に対応できます。一般的に、エンドユーザーのデバイス向けには NIC チーミングが適切です。一方、複数の LAN DISK Z の NAS デバイス間、あるいは既存の Windows Server と LAN DISK Z の NAS デバイス間には SMB マルチチャンネルの利点を生かせるでしょう。



利用可能な場合、NIC チーミングと SMB マルチチャンネルの両方を同時に利用す

ることができます。エンドユーザーのデバイスが複数の物理 NIC を備えていることは一般的ではありませんが、最近の NIC は RSS 対応のものが多いため、1 つの NIC であっても SMB マルチチャンネルを利用できる場合があります（ただし、帯域幅集約機能のみ）。

SMB 暗号化

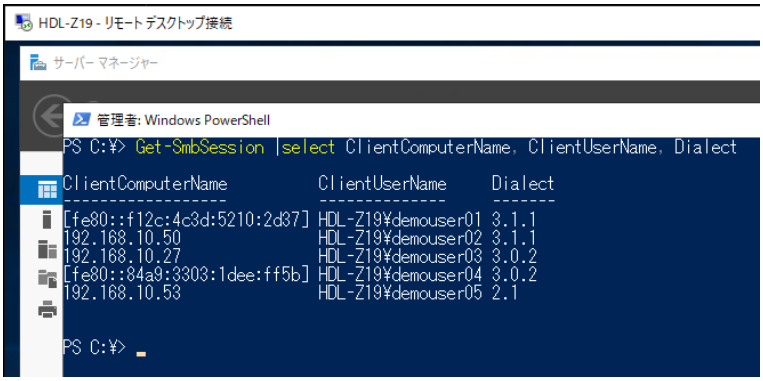
SMB 暗号化（SMB Encryption）は、SMB v3 でサポートされるファイル共有プロトコル自身が備える暗号化機能です。SMB v3 の SMB サーバーとクライアント間では、SMB 暗号化を有効化することで、ファイル共有トラフィックをエンドツーエンドで暗号化し、ネットワークの盗聴などから保護できます。SMB 暗号化は、IP パケット単位で暗号化を行う従来からのネットワーク暗号化技術である IPSec よりも圧倒的に簡単に利用できるという利点があります。なお、SMB 暗号化を有効化した共有フォルダーに SMB 暗号化に対応していない SMB v2 や SMB v1/CIFS クライアントが接続しようとすると、アクセスが拒否されます。

SMB v3（3.x）対応クライアントについて

SMB サーバーと SMB クライアント間では、両方がサポートする最上位バージョンの SMB を使用して通信します。Windows 10 および Windows Server 2016 以降は最新の SMB 3.1.1、Windows 8.1 および Windows Server 2012 R2 は SMB 3.0.2、Windows Server 2012 は SMB 3.0 と、下位バージョンをサポートしています。SMB 2.1（SMB v2）が最上位バージョンである Windows 7 および Windows Server 2008 R2、およびそれ以前の Windows は SMB v3 を利用できません。

比較的新しいバージョンの macOS（OS X 10.10 Yosemite 以降）や Linux（Linux 3.11 以降、Samba 4 以降）は、SMB v3 に対応しています。ただし、Linux のディストリビューションやバージョンによっては、SMB v3 に対応させるために構成ファイルの変更や明示的なバージョン指定が必要な場合があります。

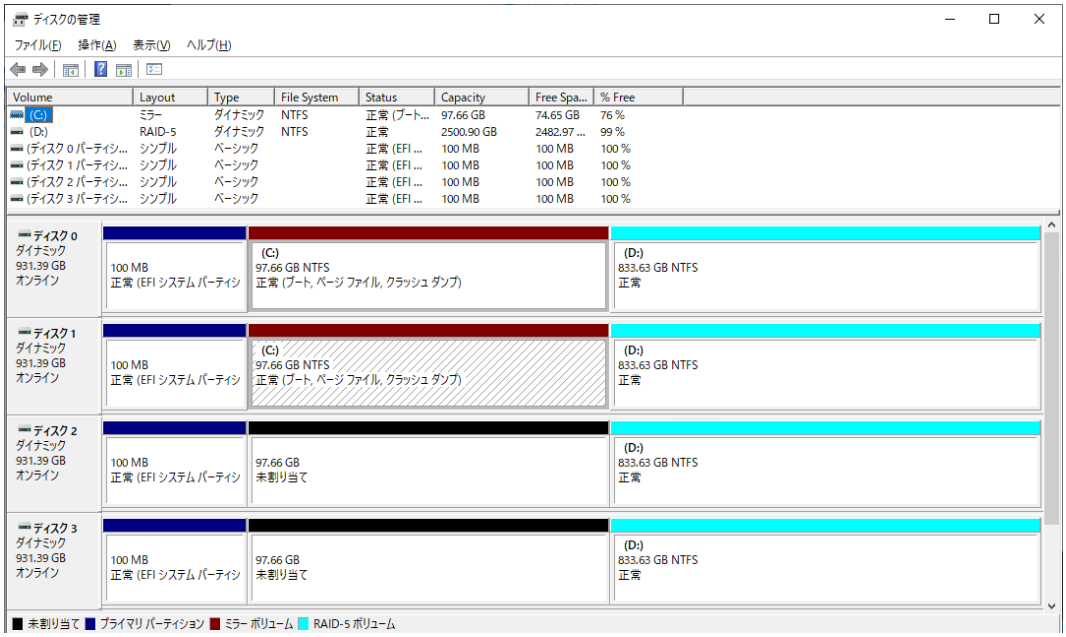
SMB サーバー側の Windows PowerShell で次のコマンドラインを実行すると、現在、SMB サーバーの共有に接続中の SMB セッションで使用されている SMB バージョン（Dialect）を確認することができます。右のスクリーンショットは、上から Windows 10、Ubuntu 18.04 LTS、macOS 10.12 Sierra、Windows 8.1、Windows 7 です。



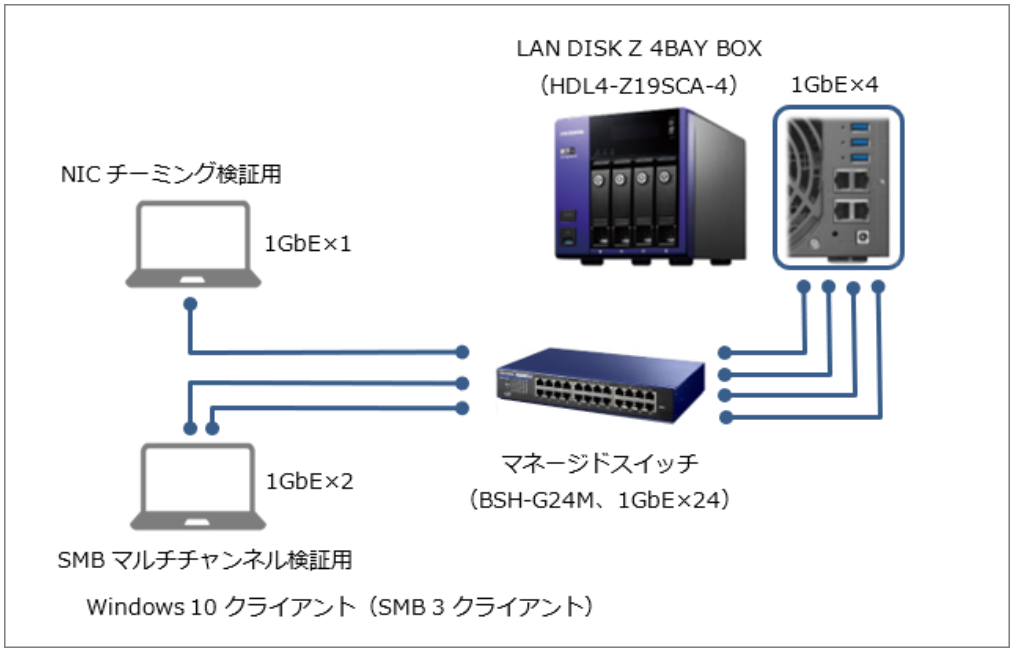

```
Get-SmbSession | Select ClientComputerName, ClientUserName, Dialect
```

1.3　実施環境について

このガイドの内容は、LAN DISK Z（商品型番：HDL4-Z19SCA-4）と 2 台の Windows 10 クライアントを、同じネットワークスイッチに接続した環境で実施しました。ディスクのパーティションは、既定の構成（OS C:／100GB NTFS／ミラー、データ D:／約 2.4TB NTFS／RAID-5）で、データ用ボリュームである D:をデータ重複除去の対象としてセットアップします。



LAN DISK Z（HDL4-Z19SCA-4）は 4 ポートの NIC を標準搭載しています。今回は 4 ポートをすべて 4 本の LAN ケーブルで LACP 対応のマネージドスイッチ（商品型番：BSH-G24M）に接続します。NIC チーミングおよび SMB マルチチャンネルのためには、少なくとも 2 ポートを 2 本の LAN ケーブルで接続してください。このガイドでは、両機能の検証用に 1 ポートの NIC と、2 ポートの NIC をそれぞれ備えたクライアント PC を同じスイッチに接続し、LAN DISK Z 側は 3 ポートの NIC でチームを構成します。



LAN DISK Z のための管理用端末について

ここでは、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 LAN DISK Z のコンソールに管理者として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、このガイドのシリーズの『2. 運用管理編』および『3. 集中管理編』で説明しています。

2　データ重複除去によるディスク使用の効率化

LAN DISK Z のデータ用ボリューム D:でデータ重複除去を有効化する手順を説明します。データ重複除去の処理にはデータ量によって時間とシステム負荷が少なからず発生するため、データ重複除去を利用する予定がある場合は LAN DISK Z を導入後、格納データが少ない早い段階に有効化することをお勧めします。

データ重複除去がサポートされるのは Windows Server IoT for Storage Standard

繰り返しますが、データ重複除去機能は、OEM 製品である Windows Server 2019 IoT for Storage では、Standard エディションでサポートされる機能です。Workgroup エディションでは利用できないことに注意してください。

2.1　役割サービスのインストール状況の確認

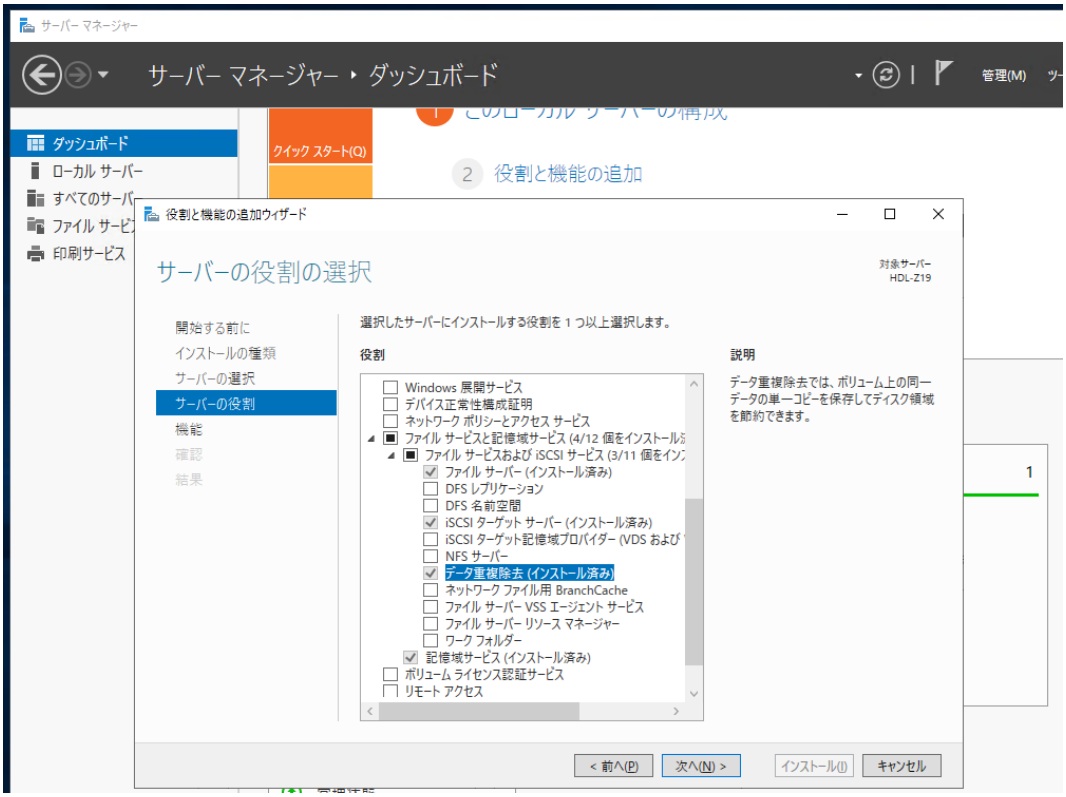
Windows Server IoT 2019 for Storage Standard では、はじめからデータ重複除去の役割サービスがインストールされ、有効になっています。インストール状況は下記より確認できます。

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 LAN DISK Z の NAS デバイスを選択し、［次へ］をクリックします。

4. ［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。［データ重複除去（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、［データ重複除去］を選択し、［次へ］をクリックしてインストールしてください。なお、役割サービスのインストールを完了するために、再起動が要求される場合があります。その場合は、指示に従って LAN DISK Z の OS を再起動してください。

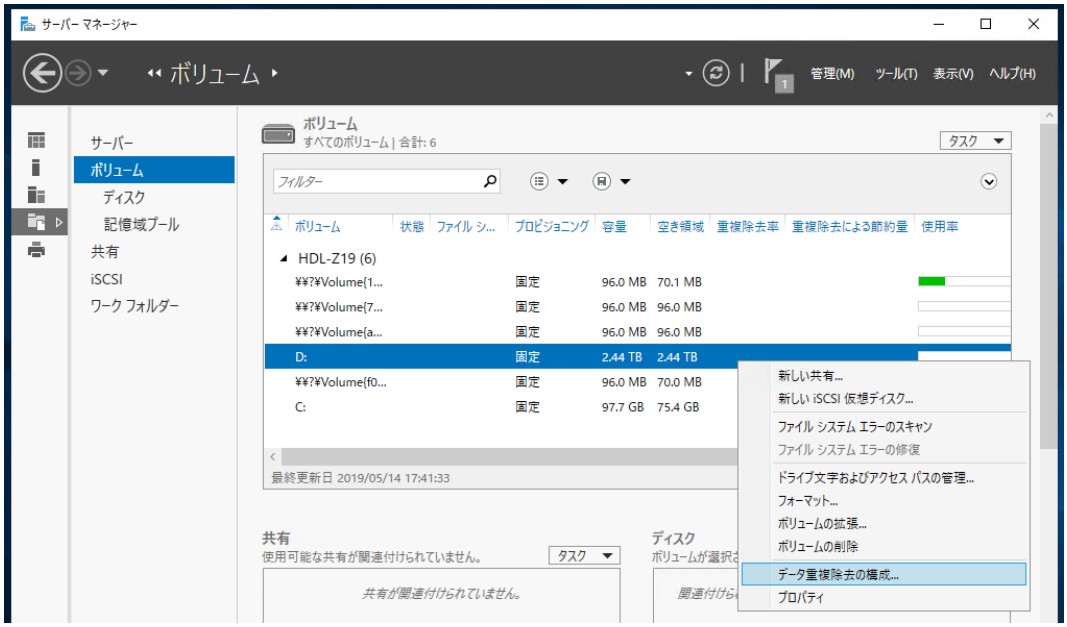


2.2　データ用ボリュームでデータ重複除去を有効にする

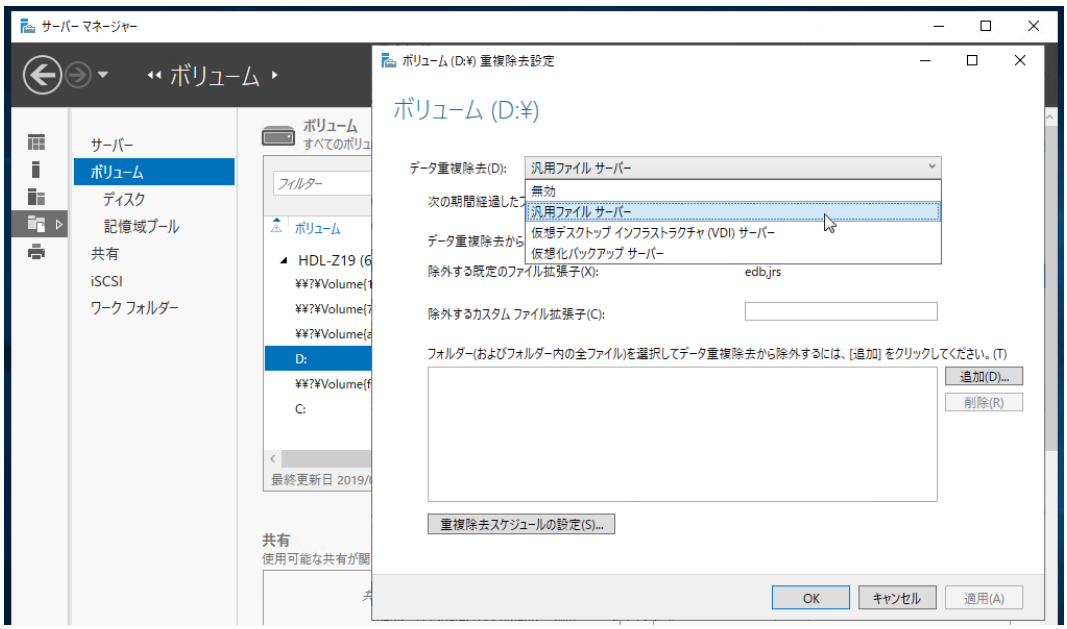
データ重複除去は、NTFS または ReFS 形式のボリューム単位で有効化できます。既定は無効です。ボリュームでデータ重複除去を有効化するには、次の手順で操作します。

> Windows Server 2019 におけるデータ重複除去の新機能
>
> Windows Server 2016 以前のデータ重複除去は、NTFS ボリュームのみをサポートしていました。Windows Server 2019 からは ReFS ボリュームについてもデータ重複除去がサポートされます。Windows Server IoT 2019 for Storage Standard も同様です。

1. ［サーバーマネージャー］で［ファイルサービスと記憶域サービス］の［ボリューム］を開きます。
2. ボリュームの一覧が表示されるので、データ重複除去を有効化するデータ用ボリューム D:を選択し、右クリックして［データ重複除去の構成...］をクリックします。

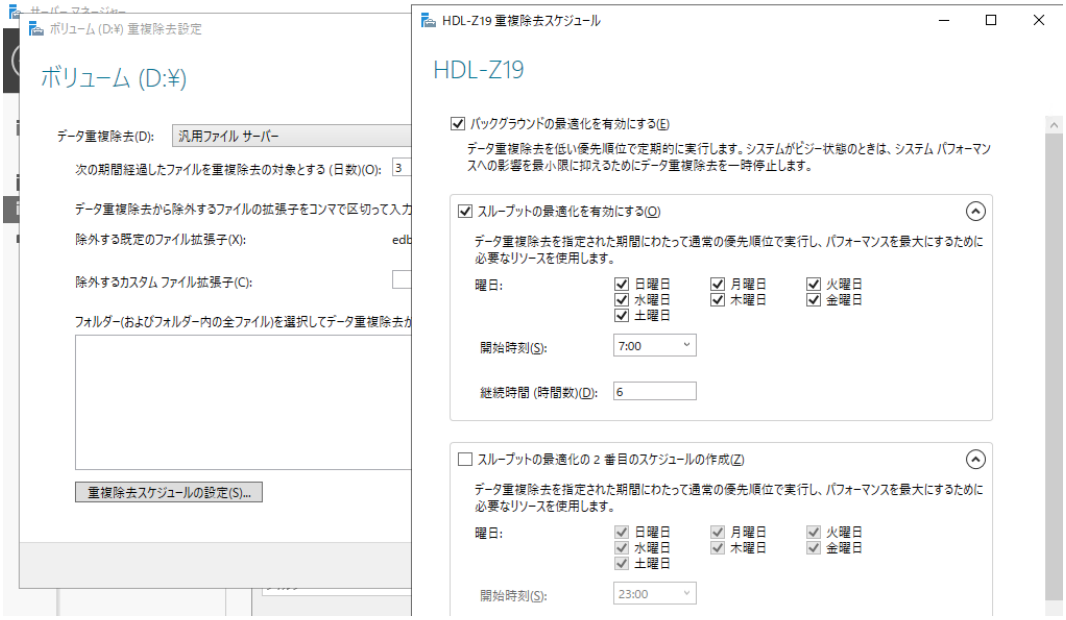


3. ［ボリューム（D:¥）重複除去設定］ダイアログボックスが開くので、［データ重複除去］のドロップダウンリストから［汎用ファイルサーバー］を選択します。データ重複除去は、ボリュームごとに［汎用ファイルサーバー］［仮想デスクトップインフラストラクチャ（VDI）サーバー］［仮想バックアップサーバー］のいずれかの利用シナリオを選択して簡単にセットアップできます。［汎用ファイルサーバー］を選択すると、既定で 3 日経過したファイルがデータ重複除去の対象になり、edb と jrs の拡張子（Windows や Exchange が使用するデータベース関連ファイル、ウイルス対策ソフトのスキャン対象やデータ重複除去の対象としては互換性に問題があります）のファイルが除外されるように設定されています。その他に除外したいファイルの種類がある場合は［追加］をクリックして設定してください。他の 2 つの利用シナリオは、LAN DISK Z では想定されていません。



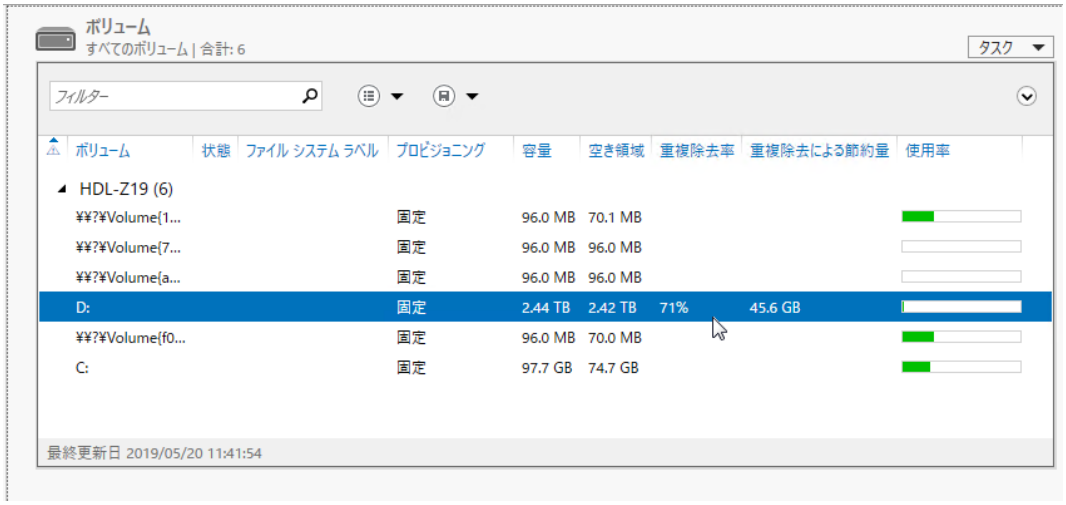
4. ［ボリューム（D:¥）重複除去設定］ダイアログボックスで［OK］をクリックすると、ボリュームのデータ重複除去の有効化は完了です。既定ではバックグラウンドで最適化処理が行われますが、夜間など業務時間外に集中的に最適化タスクを実行させたい場合は、［ボリューム（D:¥）重複除去設定］ダイア

ログボックスの［重複除去スケジュールの設定］をクリックして、［スループットの最適化を有効にする］をチェックし、曜日と開時間、継続時間を設定します。追加のスケジュールは最大 2 つまで設定できます。なお、最適化は Windows のタスクとして¥Microsoft¥Windows¥Deduplication に登録され、自動実行されます。既定のバックグラウンドタスクは BackgroundOptimization タスクとして、追加のスケジュール設定は ThroughputOptimization タスクおよび ThroughputOptimization-2 タスクとしてそれぞれ自動実行されます。これらのタスクの他に、週次で自動実行される WeeklyGarbageCollection タスクおよび WeeklyScrubbing タスクがあります。

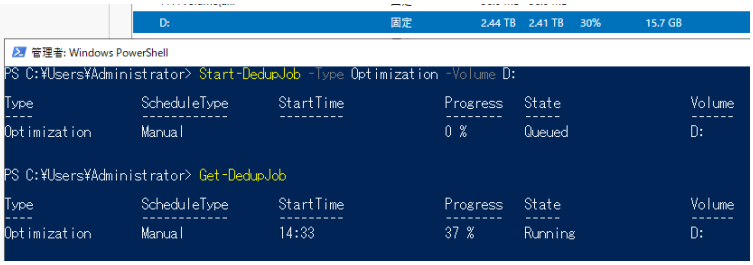


2.3　除去率の確認

データ重複除去を有効化してしばらくすると（通常、3 日以上経過後）、最適化処理が実施され、その結果が［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］の［ボリューム］の一覧に反映されます。該当ボリュームの［重複除去率］および［重複除去による節約量］列で確認してください。



データ重複除去の最適化処理を直ちに手動開始するには



Windows PowerShell の Start-DedupJob コマンドレットを使用すると、データ重複除去の最適化処理をすぐに開始できます。例えば、D:ドライブの最適化処理を開始するには、Windows PowerShell ウィンドウを開いて次のコマンドラインを実行します。

```
Start-DedupJob -Type Optimization -Volume D:
```

進行中の最適化タスクの状況を確認するには、次のコマンドラインを実行します。ジョブが終了した直後は、Progress 100 %、State Completed を出力しますが、その後は何も出力しません。

```
Get-DedupJob
```

2.4　データ重複除去の制約・注意点

Windows Server のほとんどの機能は、データ重複除去と互換性があります。例えば、最適化されたファイルが SMB クライアントから要求された場合、ファイルシステムレベルで再解析が行われ、ネットワークを介して最適化されていない状態のファイルとしてダウンロードされます。SMB サーバーはそのファイルが最適化されているかどうかを識別することはありません。ただし、データ重複除去を有効化した場合の以下の制約には注意してください。

ボリュームルートに対するハードクォータの作成不可

データ重複除去が有効になっているボリュームのルートディレクトリ（例えば、D:ドライブの D:¥）にハードクォータを作成することはできません。これは、ボリュームの実際の空き領域とクォータで制限された領域が一致しなくなり、データ重複除去の最適化ジョブが失敗する可能性があるからです。データ重複除去が有効になっているボリュームのルートディレクトリに対するソフトクォータの作成、サブフォルダーに対するハードクォータおよびソフトクォータの作成は可能です。これらのクォータでは、ファイルの論理サイズに基づいてクォータ使用率が計算されます。そのため、データ重複除去によりファイルが最適化されている場合でも、ユーザーのクォータの使用率やしきい値には影響せず、通常どおりに機能します。

なお、ボリュームのルートディレクトリに対するハードクォータは、NTFS ボリュームでサポートされるディスク毎のクォータ（ディスククォータ）およびファイルサーバーリソースマネージャーのクォータの管理で作成可能です。この制約は、ファイルサーバーリソースマネージャーのクォータの管理によるサブフォルダーごとにクォータには影響しません。

Windows Search サービスは非サポート

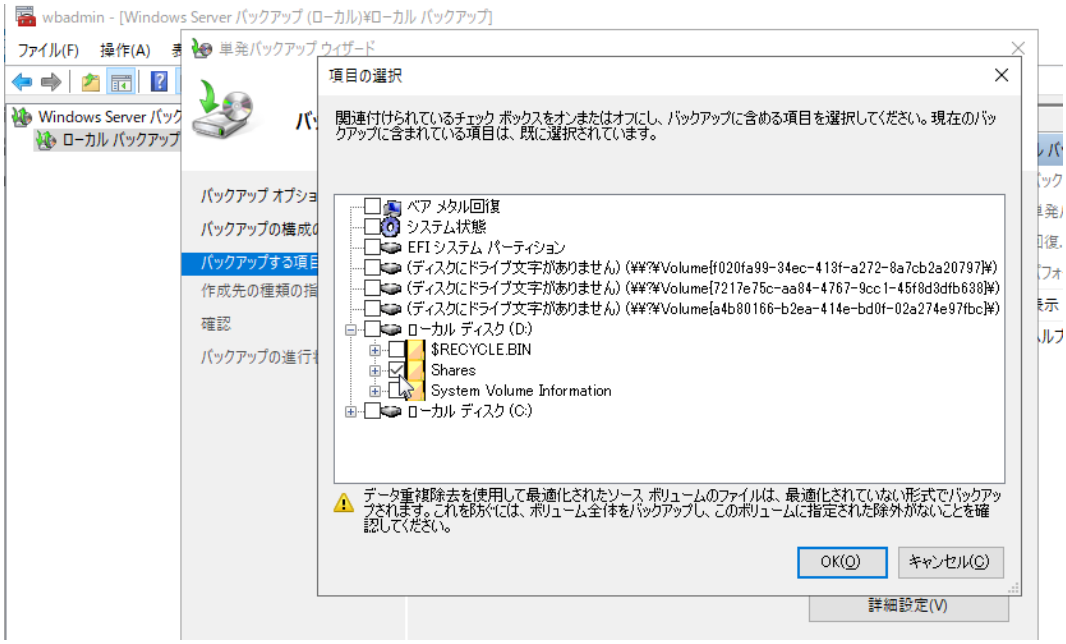
Windows Search サービスはデータ重複除去をサポートしていません。データ重複除去により最適化されたファイルの再解析ポイントを Windows Search サービスはインデックスできないため、最適化されたファイルはインデックスから除外されてしまいます。

ROBOCOPY コマンドの使用は非推奨

Windows 標準のコピーツールである ROBOCOPY コマンドは、データ重複除去が有効なボリュームと共に使用しないでください。ROBOCOPY コマンドの一部は、データ重複除去と互換性がなく、データ重複除去のチャンクストア（ボリュームの System Volume Information ディレクトリに存在します）に不整合を発生させ、ボリュームを破損させる危険性があります。

Windows Server バックアップにおける注意事項

Windows Server バックアップは、データ重複除去で最適化されたボリュームを、データ重複除去された状態を維持したままバックアップすることが可能です。ただし、それはボリューム単位でバックアップおよびリストアする場合に限られます。フォルダーやファイル単位のバックアップやリストアを行う場合、データ重複除去の状態が解除されてバックアップまたはリストアされることに注意してください。ファイルやフォルダー単位のバックアップが制限されるわけではありませんが、バックアップに含まれるデータは最適化されていない状態であるため、バックアップサイズは当然のことですが大きくなります。



3　ネットワークトラフィックの最適化とセキュリティ

LAN DISK Z で NIC チーミング、SMB マルチチャンネル、SMB 暗号化をセットアップする手順について説明します。NIC チーミングと SMB マルチチャンネルについては、「1.2　ファイルサーバーのボリュームおよびネットワークの最適化について」を参照し、NIC チーミングを使用するのか、SMB マルチチャンネルを使用するのか、あるいは NIC チーミングと SMB マルチチャンネルの両方を使用するのかを検討した上

で、どちらか一方を構成するか、両方を構成してください。

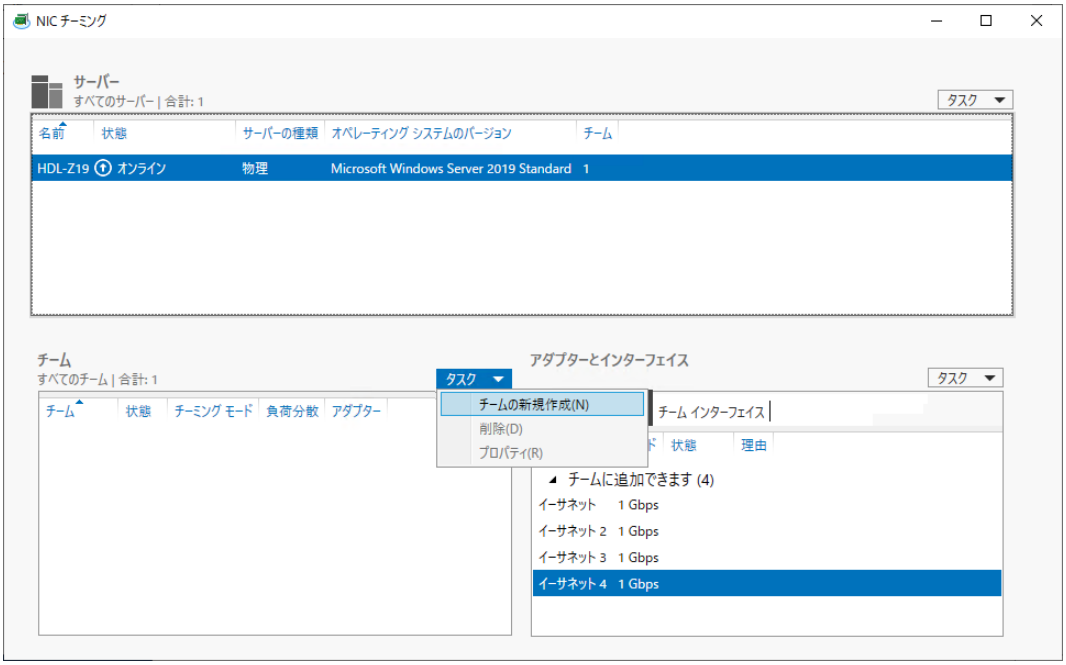
3.1　NIC チーミングの作成

LAN DISK Z の 2 または 4 ポートの NIC を使用して、NIC チーミングをセットアップするには次の手順で操作します。ここでは、4 ポートのうち 3 ポートの NIC を使用してチームを作成する例で説明します。NIC のポートとスイッチの間は LAN ケーブルですべて接続されており、チームに含める NIC は DHCP 割り当てで構成されているものとします。

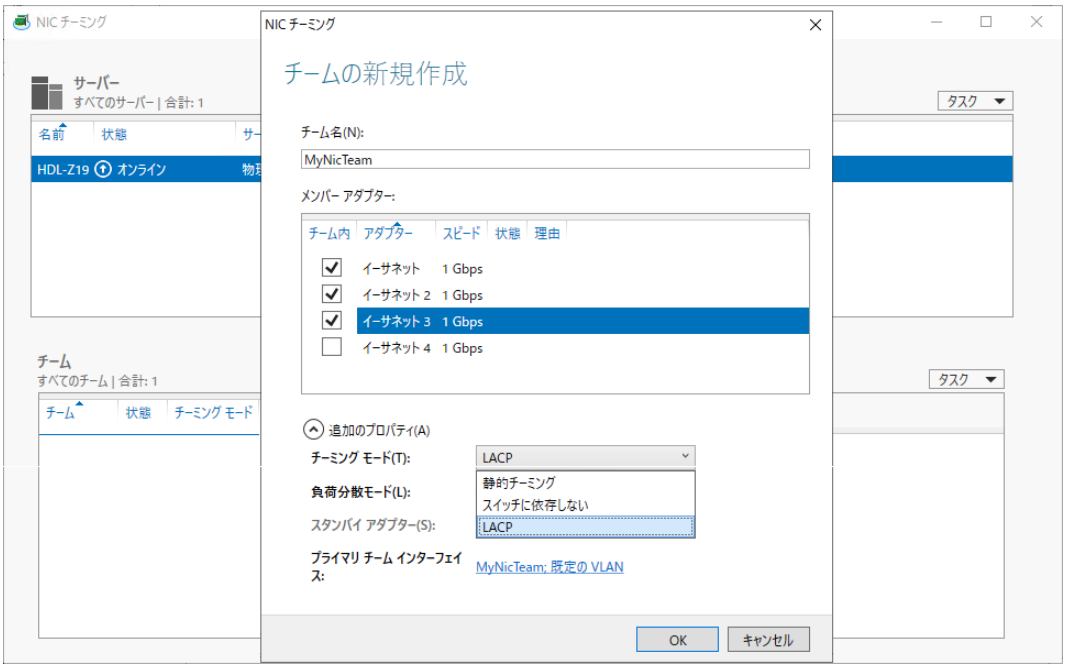
> **チーム作成時の一時オフライン状態に注意してください**
>
> NIC チーミングは、1 つ以上の物理 NIC を束ねて作成することができます。可用性の向上と帯域幅の集約の利点を得るには、2 つ以上の物理 NIC でチームを作成してください。ただし、LAN DISK Z の場合、リモート管理による NIC チームのセットアップが前提となります。LAN DISK Z が備える 2 つまたは 4 つの NIC すべてを選択してチームを作成すると、一時的にオフライン状態になり、DHCP により自動構成された（または静的に割り当てた）IP アドレスがチームに対する新たな割り当てにより変更される可能性があります。4 つの NIC を利用できるモデルの場合は、1 つの NIC をリモート管理用に確保し、残りの 3 つの NIC でチームを作成するとよいでしょう。2 つまたは 4 つの NIC でチームを作成する場合は、1 つまたは 3 つの NIC で先にチームを作成し、チームに割り当てられた IP アドレスまたは静的に割り当てた IP アドレスを確認し、その IP アドレスでリモート管理用に接続し、残りの NIC をチームに追加します。

1. ［サーバーマネージャー］で［ローカルサーバー］ページを開き、［NIC チーミング 無効］のリンクをクリックします。

2. ［NIC チーミング］のウィンドウが開くので、［チーム］にある［タスク▼］から［チームの新規作成］をクリックします。

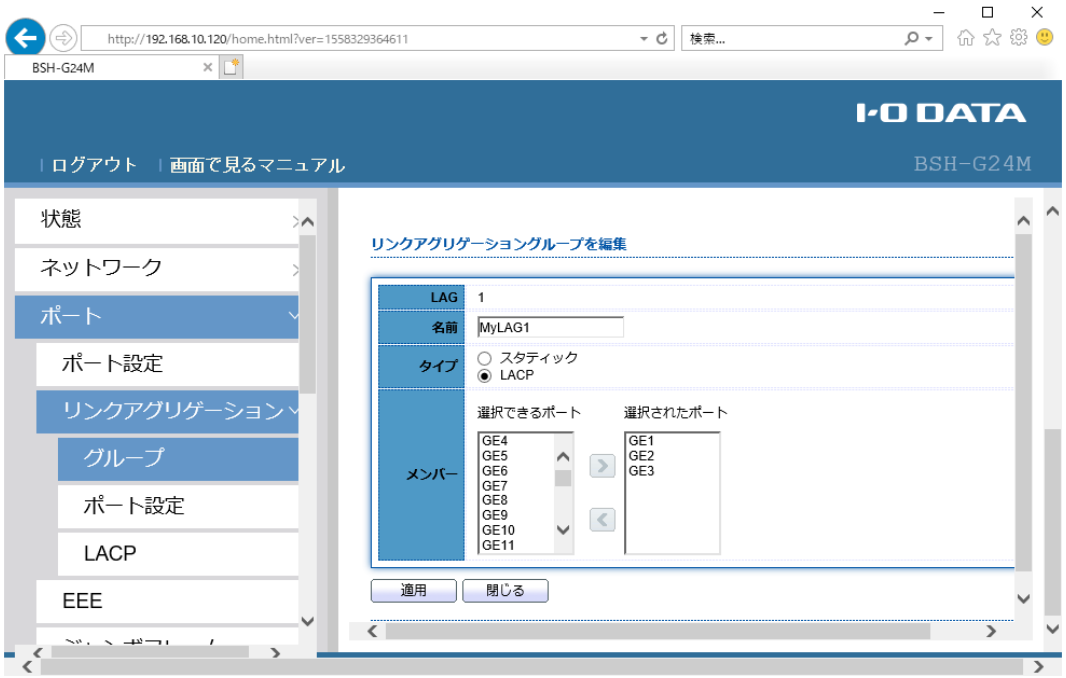


3. ［チームの新規作成］ウィンドウが開くので、［チーム名］に分かりやすいチームの名前を入力し、チームに含める NIC を選択します。また、［⓪追加のプロパティ］をクリックして［チーミングモード］として［スイッチに依存しない］または［LACP］を、負荷分散モードとして［動的］を、［スタンバイアダプター］として［なし（すべてのアダプターがアクティブ）］を選択します。［チーミングモード］は接続先のスイッチの種類と構成に応じて選択します。

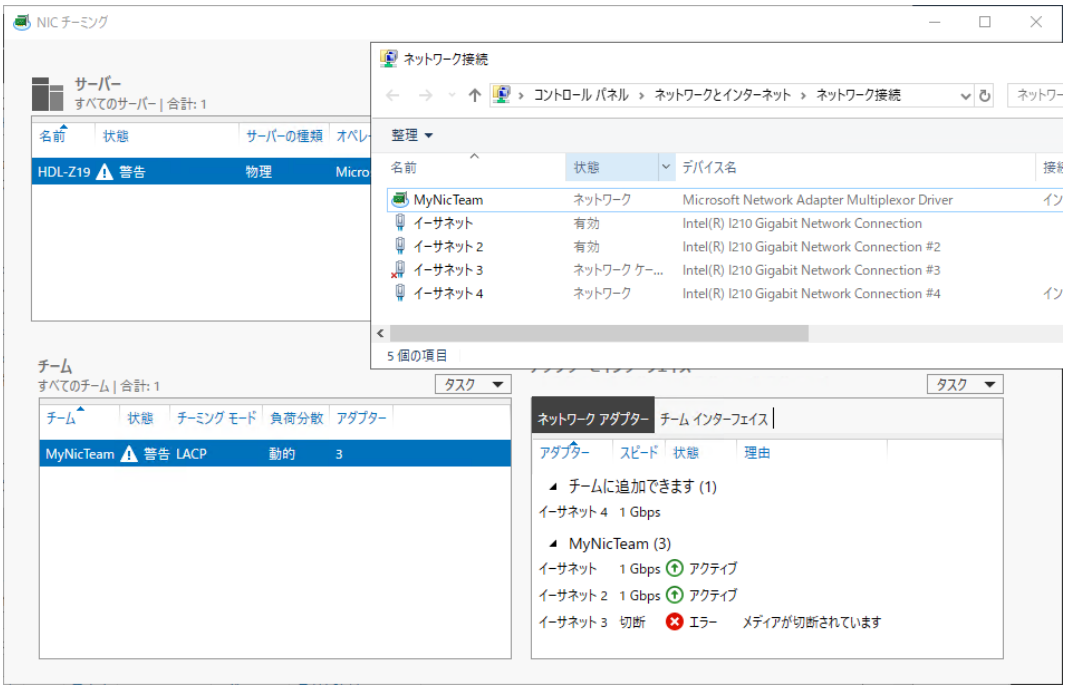


接続先がアンマネージドスイッチの場合は［スイッチに依存しない］を選択します。接続先 LACP（Aggregation Control Protocol）対応のマネージドスイッチに接続されている場合は、スイッチの接続先のポートが同じ LACP グループになるように構成し、［チーミングモード］として［LACP］を選択してください。次の画面は、アイ・オー・データのマネージドスイッチ（商品型番：BSH-G24M）の管理ポータルを使用して 3 つのポートを含む LACP グループ（リンクアグリゲーショングループ）を作成

する例です。設定方法については、実際に使用するマネージドスイッチのマニュアルに従ってください。



4. ［チームの新規作成］ウィンドウで［OK］をクリックし、チームを作成します。作成が完了すると、指定したチーム名でデバイス名 Microsoft Network Adapter Multiplexor Driver の単一の論理的な NIC が作成され、アクティブになります。この論理的な NIC は、既定で DHCP による自動構成となりますが、固定の IP アドレスを静的に設定することも可能です。また、2 つ以上の NIC からなるチームでは、チーム内の物理 NIC の経路（LAN ケーブルの切断など）に障害があったとしても、ネットワークトラフィックは残りのアクティブな物理 NIC にフェールオーバーされるため、通信が切断されることはありません。



チーミングモードと負荷分散モードについて

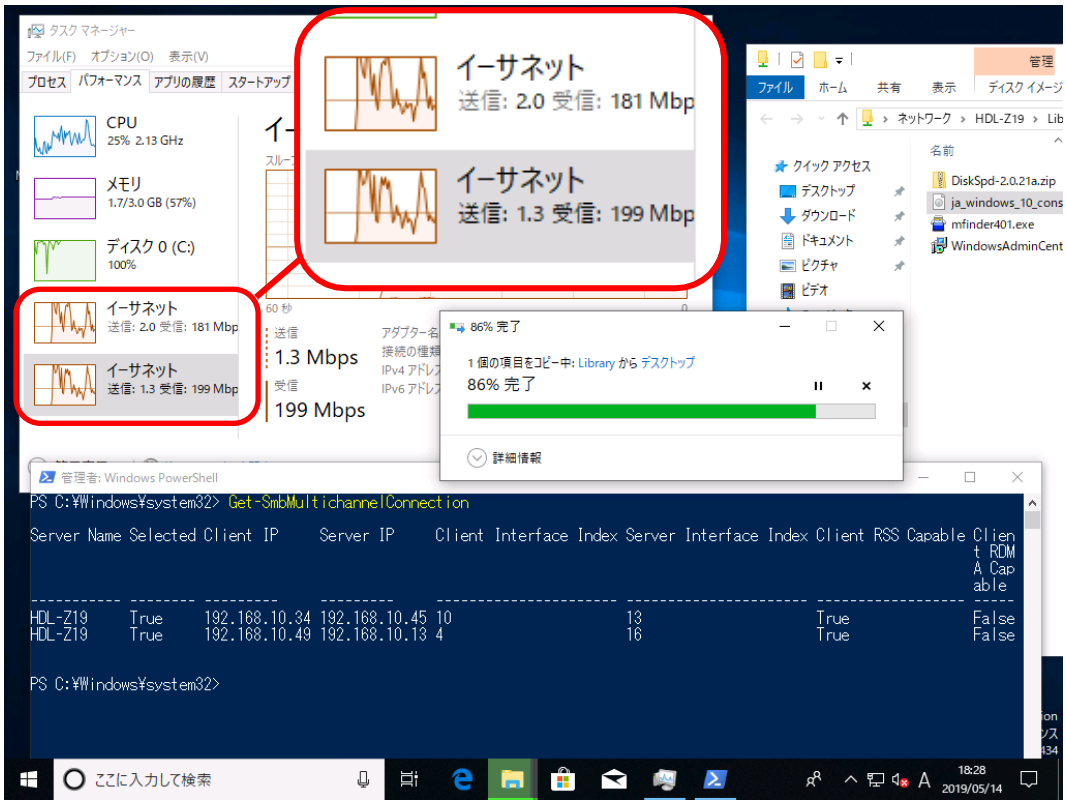
NIC チーミングは複数のチーミングモードと負荷分散モードをサポートしていますが、一般的に LACP 対応のマネージドスイッチを利用できる場合は、チーミングモード [LACP] および負荷分散モード [動的] を、アンマネージドスイッチを利用する場合は、チーミングモード [スイッチに依存しない] および負荷分散モード [動的] を選択すればよいでしょう。スイッチの LACP とともに動作する前者の場合、送受信トラフィックの両方が負荷分散されます。スイッチに依存しない後者の場合、サーバーからスイッチへの送信トラフィックのみが負荷分散されますが、経路上のスイッチを分けてスイッチのハードウェア障害や電源障害に備えることが可能です。

その他のモード設定については、以下のドキュメントで確認してください。

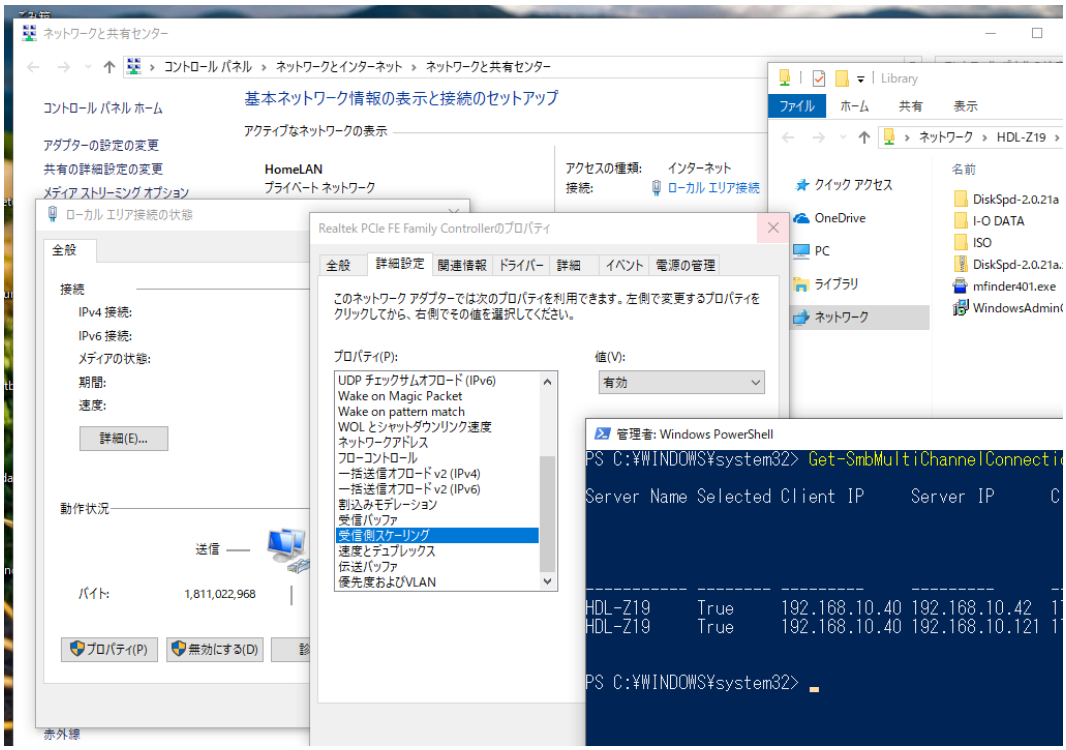
NIC Teaming settings
https://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming/nic-teaming-settings

3.2 SMB マルチチャンネルの利用

SMB マルチチャンネルは、SMB サーバーと SMB クライアントの両方で、同じ速度の複数の NIC を利用できる場合に使用されます。SMB マルチチャンネルの機能は SMB サーバーと SMB クライアントの両方で既定で有効になっており、利用可能な状況下では自動的に SMB マルチチャンネルが使用されます。



SMB サーバーと SMB クライアントの両方の NIC が RSS 対応の場合は、1 つの NIC しかなくても SMB マルチチャンネルが使用され、帯域幅の集約の利点を得られます（経路障害に対するフェールオーバー機能は利用できません）。LAN DISK Z に搭載されている NIC は、RSS 対応です。クライアントの NIC が RSS に対応しているかどうかは、NIC のプロパティの［詳細設定］タブで［Receive Side Scaling（または受信側スケーリング）］が［Enabled（または有効）］になっているかどうかで確認することができます。



SMB マルチチャンネルが使用されているかどうかは、共有リソースへの接続中に Windows PowerShell を管理者として開き、次のコマンドラインを実行することで確認できます。

```
Get-SmbMultiChannelConnection
```

SMB マルチチャンネルの設定の確認と変更について

SMB サーバーと SMB クライアントで SMB マルチチャンネルの機能が有効になっているかどうかは、SMB サーバーと SMB クライアントのそれぞれで次のコマンドラインを実行して True（既定）が返されるかどうかで確認できます。

```
(Get-SmbServerConfiguration).EnableMultiChannel

(Get-SmbClientConfiguration).EnableMultiChannel
```

次のコマンドラインを実行すると、SMB サーバーと SMB クライアントのそれぞれで、SMB マルチチャンネルの機能を有効化または無効化することもできます。

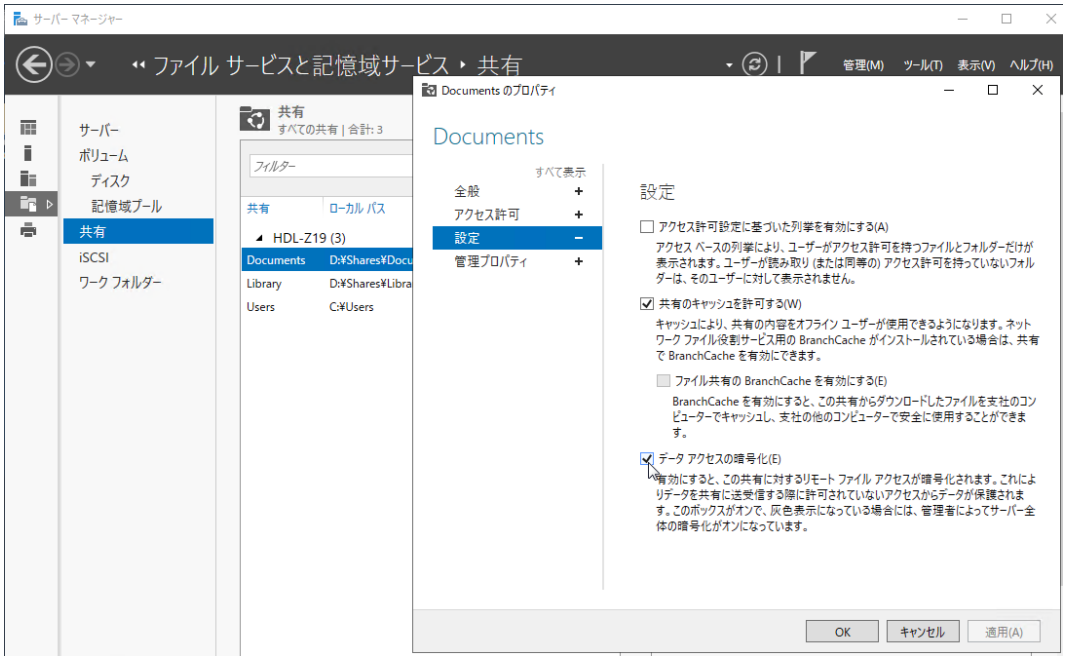
```
Set-SmbServerConfiguration -EnableMultiChannel $true または$false

Set-SmbClientConfiguration -EnableMultiChannel $true または$false
```

3.3　SMB 暗号化

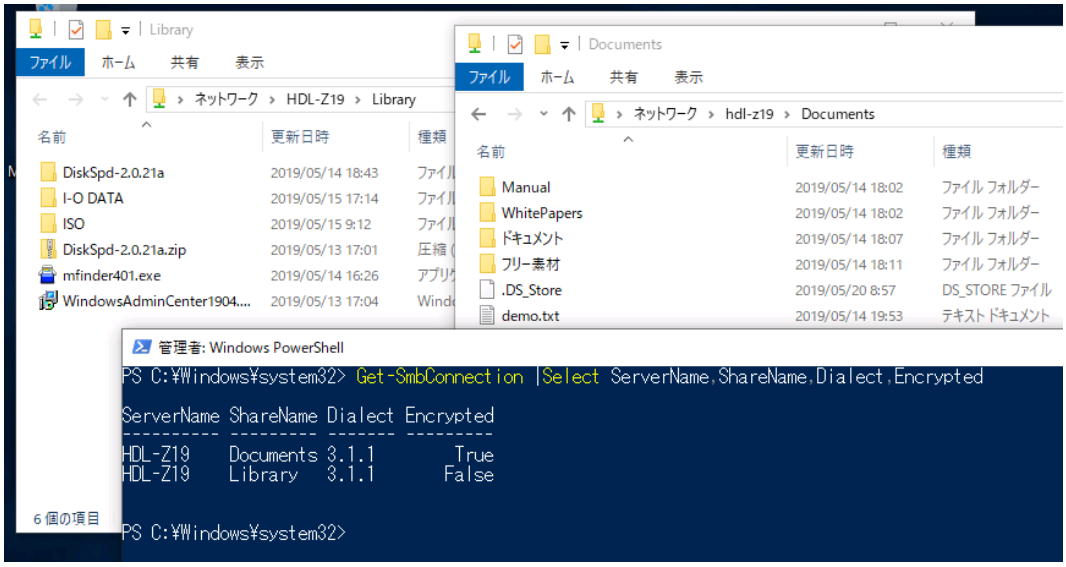
SMB クライアントのすべて SMB v3 を利用可能な場合、共有フォルダーで SMB 暗号化を有効化することで、エンドツーエンドの通信トラフィックを暗号化して保護できます。

共有フォルダーごとの SMB 暗号化の有効化は、[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] の [共有] から SMB 共有を作成する際、または作成済みの SMB 共有のプロパティの設定の 1 つとして、[データアクセスの暗号化] をチェックすることで簡単に有効化できます。なお、SMB 暗号化は通信を暗号化するものであり、SMB 暗号化の有効化、無効化が共有フォルダー内の既存のファイルや新規のファイルに影響することはありません。

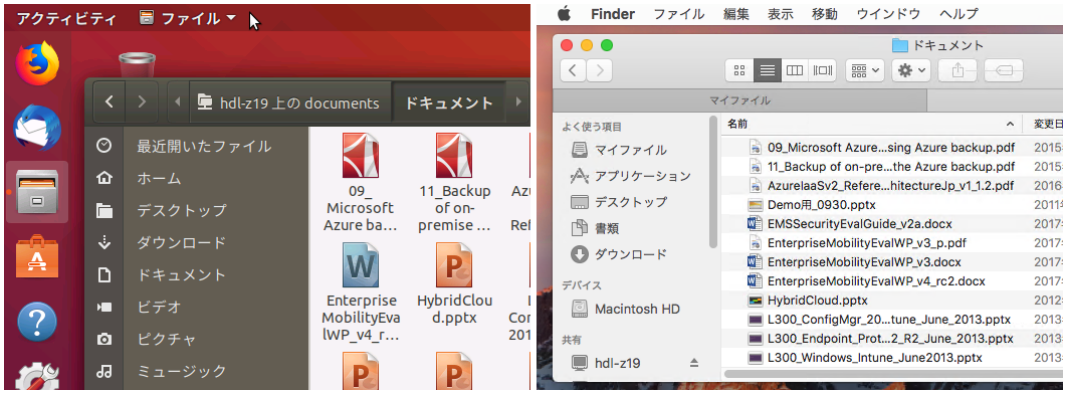


SMB v3 対応クライアントから SMB 暗号化が有効な共有フォルダーへの接続と、有効でない共有フォルダーへの接続のエクスペリエンスに何の違いもありません。SMB v3 対応の Windows クライアント（Windows 8.1 や Windows 10）の場合は、Windows PowerShell を管理者として開いて、次のコマンドラインを実行することで、SMB バージョン（Dialect）や暗号化状態（Encrypted）を確認することができます。

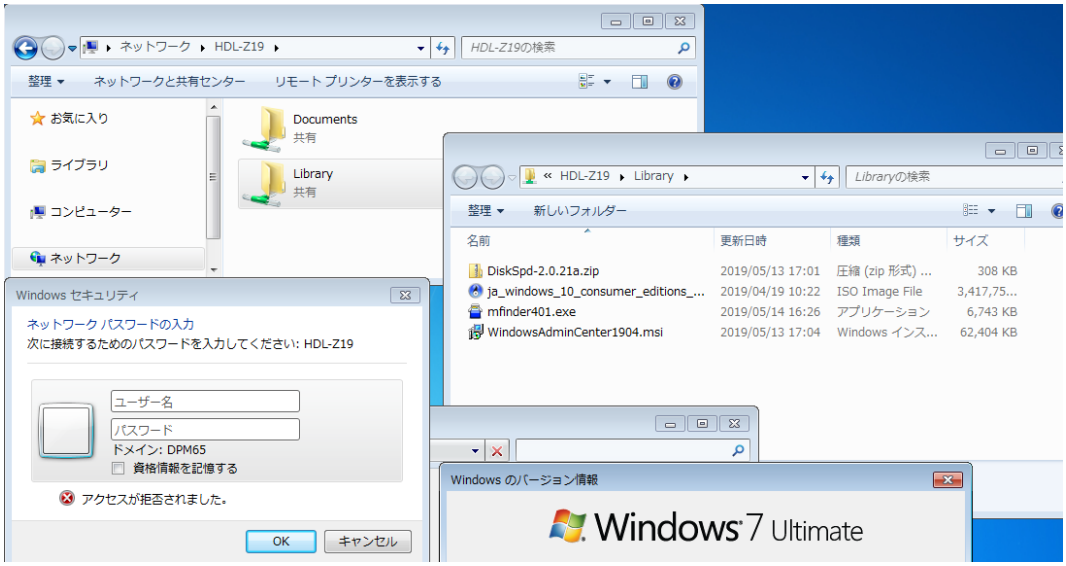
```
Get-SmbConnection | Select ServerName, ClientName, Dialect, Encrypted
```



Linux や macOS クライアントの場合も、SMB v3 がサポートされている比較的新しいバージョンであれば、SMB 暗号化が有効な共有フォルダーに接続することができます。



一方、SMB v3 をサポートしていないクライアント（例えば、SMB v2.1 の Windows 7）からの接続は、アクセスが拒否されます。SMB v3 をサポートしていないクライアントが、SMB 暗号化が有効な共有フォルダーに接続する手段はありません。



ファイルサーバー全体で SMB 暗号化を有効化するには

ファイルサーバーでは、Windows PowerShell で次のコマンドラインを実行することで、ファイルサーバー全体で SMB 暗号化を有効化することもできます。既定では、サーバー全体での SMB 暗号化は無効です。

```
Set-SmbServerConfiguration -EncryptData $true
```

ファイルサーバー全体で SMB 暗号化を有効化した場合、SMB 共有のプロパティの設定の［データアクセスの暗号化］はグレー表示となり、既定ですべての SMB 共有で SMB 暗号化が有効化されます。

ファイルサーバー全体で SMB 暗号化を有効化する場合は、ファイルサーバーにアクセスするすべてのクライアントが SMB v3 対応であることを確認してください。