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 6 月 30 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、ファイルサーバーとしての運用管理の基本的な環境の整備、および Windows Server の便利なファイルサーバー機能の活用について解説します。

1.2　ファイルサーバーとしての運用管理について

Windows Server IoT 2019 for Storage のファイルサーバー機能は、Windows Server 2019 とその多くが共通しており、同じ管理操作で運用管理することができます。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、Windows Server IoT 2019 for Storage 搭載の LAN DISK Z をリモート管理する環境を準備し、運用管理の一例としてファイルサーバーリソースマネージャーのいくつかの機能の活用例を示します。

- リモートデスクトップ接続
- リモートサーバー管理ツール（RSAT）
- ファイルサーバーリソースマネージャー

リモートデスクトップ接続

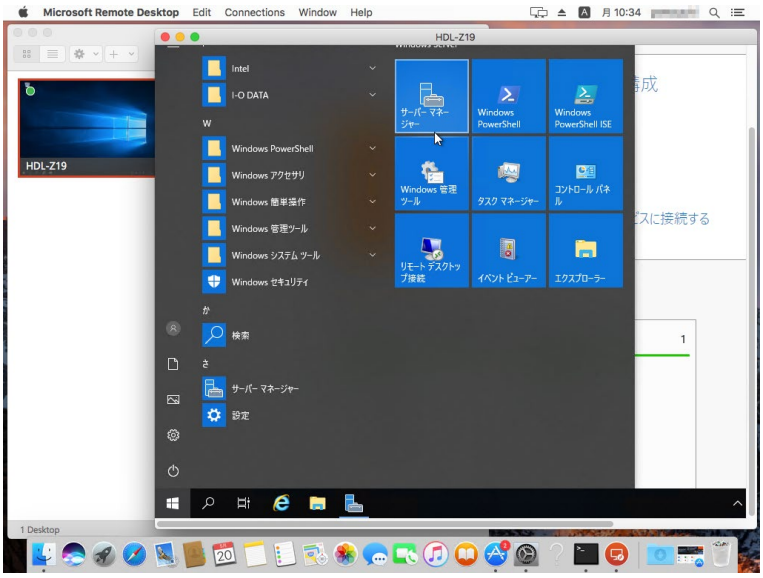
リモートデスクトップ接続は、Windows Server が標準でサポートするリモートデスクトッププロトコル（RDP）を使用するリモート管理環境です。Windows Server は、リモートデスクトップサービス（RDS）の役割を追加することなく、RDP 対応クライアントから管理目的でのリモートでストップ接続をサポートします。RDP 対応クライアントから LAN DISK Z の Windows Server IoT 2019 for Storage のセッションにリモート接続した後は、Windows Server 2019 が備えるのと共通の管理ツール、例えば、［設定］アプリや［コントロールパネル］、［サーバーマネージャー］やその他の MMC（Microsoft 管理コンソール）スナップインの管理ツールを使用して、Windows Server のシステム設定や更新管理、運用管理、ファイルサーバー機能の管理が可能です。

Windows クライアントおよびデスクトップエクスペリエンスが有効な Windows Server は、標準の RDP 接続クライアントとして［リモートデスクトップ接続］デスクトップアプリ（mstsc.exe）を備えています。Windows 8.1 および Windows 10 向けには、ストア（Windows ストア、Microsoft ストア）を通じて［リモートデスクトップ］アプリが無料提供されており、標準の［リモートデスクトップ接続］デスクトップアプリの代わりにこちらを利用することもできます。

Android や iOS、macOS に対しては、それぞれのデバイスのストアを通じて［Microsoft Remote Desktop］アプリが無料提供されています。Linux についても、FreeRDP（http://www.freerdp.com/）や Remmina（https://remmina.org/）といった無料のオープンソースソフトウェアを RDP 対応クライアントとして利用できます。この他、このガイドのシリーズの『3. 集中管理編』で説明する Windows Admin Center を導入すると、HTML5 対応ブラウザーだけでリモートデスクトップ接続を行うことができます。

マイクロソフト純正の Android、iOS、macOS 向け RDP 対応クライアント

マイクロソフトは、Windows 以外の Android、iOS、macOS に対しても、最新の RDP 対応クライアントをそれぞれのデバイスのストアを通じて無料提供しています。これらのアプリを利用すれば、Windows 端末がなくても、Andriod や iPad のタブレット端末から LAN DISK Z をリモート管理できます。



Android 向け Microsoft Remote Desktop（Google Play）
https://play.google.com/store/apps/details?id=com.microsoft.rdc.android&hl=ja

iOS 向け Microsoft リモートデスクトップ（App Store）
https://itunes.apple.com/jp/app/microsoft-remote-desktop/id714464092?mt=8

macOS 向け Microsoft Remote Desktop 10（Mac App Store）
https://itunes.apple.com/us/app/microsoft-remote-desktop/id1295203466?mt=12

リモートサーバー管理ツール（RSAT）

Windows クライアントと Windows Server の標準的な管理ツールは共通であり、Windows 10 のローカルの管理ツールを管理対象にリモート接続して管理することができます。ただし、Windows Server のサーバーの役割や機能に対応した管理ツールについては、Windows クライアントには標準では搭載されていません。

Windows 10（ただし、Home エディションを除く）を利用できる場合は、Windows 10 に「リモートサーバー管理ツール（Remote Server Administrative Tool：RSAT）」を追加することで、[サーバーマネージャー]やその他の MMC スナップイン管理ツールを LAN DISK Z の Windows Server IoT 2019 for Storage にリモート接続して管理することができます。

ファイルサーバーリソースマネージャー

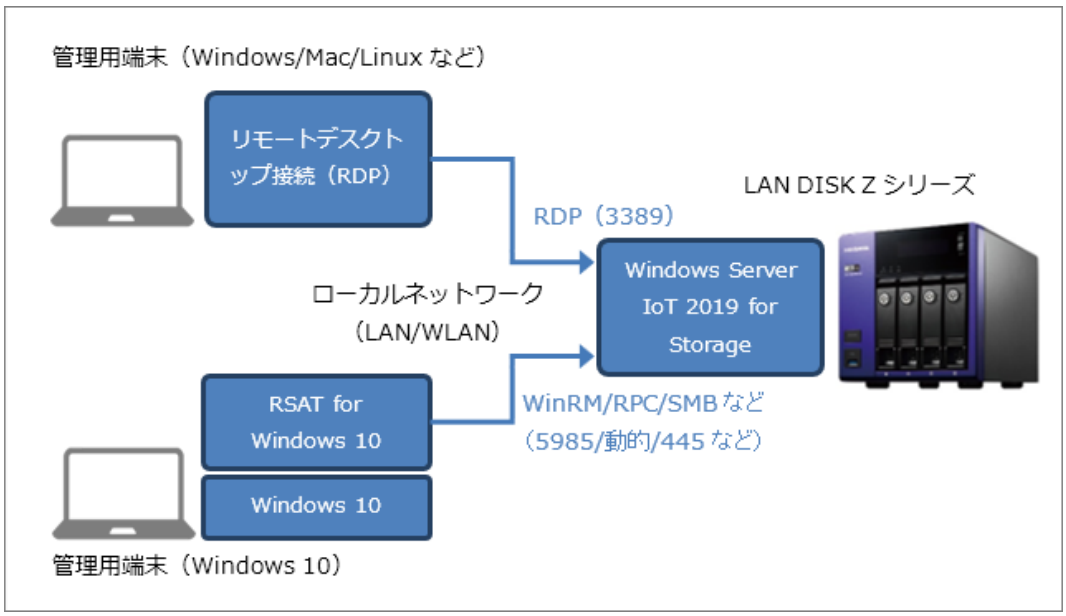
ファイルサーバーにファイルサーバーリソースマネージャーの役割サービスを追加すると、クォータの管理、ファイルスクリーンの管理、ファイル分類管理、ファイル管理タスク、記憶域レポートといった、高度なファイルサーバー機能を活用することができます。

ファイルサーバーリソースマネージャーのすべての機能を利用するには、リテール製品またはボリュームラ

イセンス製品の Windows Server で構築した Active Directory ドメイン環境や Windows Server クライアントアクセスライセンス（CAL）、その他の CAL（Active Directory Rights Management サービスによる暗号化のための RMS CAL など）、および社内のメールシステム環境が必要です。このガイドでは、ワークグループ環境でも比較的簡単に導入して利用できる機能について説明します。

1.3 実施環境について

このガイドの内容は、LAN DISK Z（HDL4-Z19SCA-4）と管理用端末を同じネットワークスイッチに接続した、ワークグループ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 ミラー、データ D: 約 2.4TB RAID-5）は変更せず、管理用端末の環境のセットアップと、ファイルサーバーリソースマネージャーの役割サービスのインストールと利用手順について説明します。ファイルサーバーリソースマネージャーの機能の検証は、管理用の Windows 10 端末で兼用して行いました。



リモートデスクトップ接続のリモート管理環境は、サーバーに対する TCP および UDP ポート 3389 の接続のみで利用できるのに対して、リモートサーバー管理ツール（RSAT）のリモート接続には、Windows Remote Management（TCP ポート 5589）、ファイル共有ポート（TCP ポート 445）、RPC（TCP ポート 135 および動的ポート）など、広範囲のポートを使用するため、クライアントとサーバーの Windows Defender ファイアウォールや経路上のファイアウォールでブロックされることがあることに留意してください。

2 標準のリモート管理環境の準備

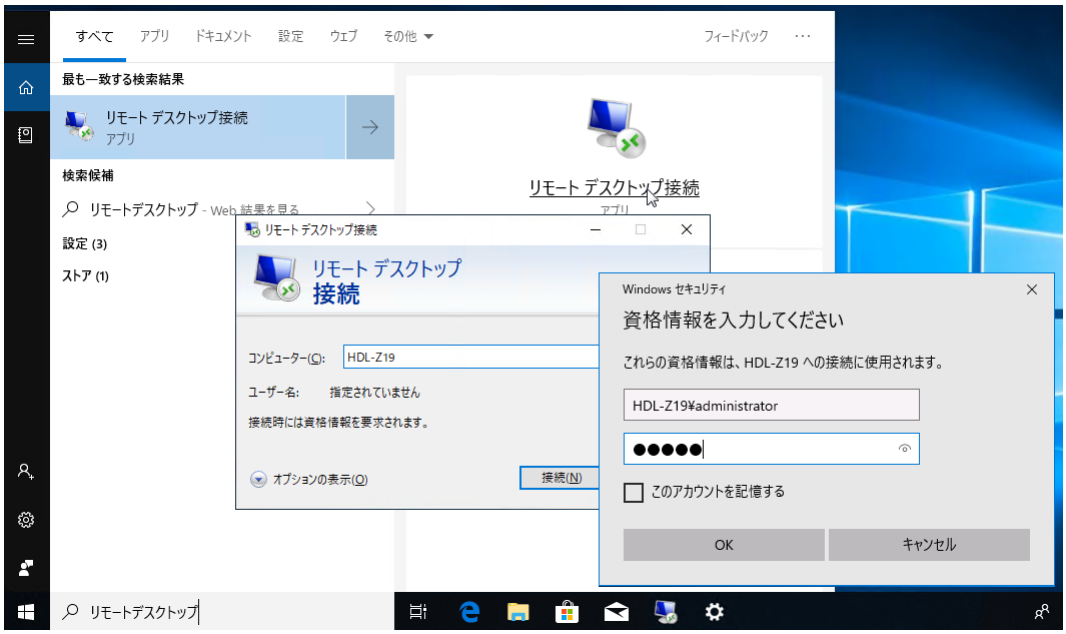
はじめに、リモートデスクトップ接続またはリモートサーバー管理ツール（RSAT）を使用した LAN DISK Z の NAS デバイスのためのリモート管理環境を準備する手順を説明します。

2.1 リモートデスクトップ接続

「1.2 ファイルサーバーとしての運用管理について」で説明したように、RDP 対応クライアントを使用したリモートデスクトップ接続は、Windows クライアントでは標準で利用できますが、Windows 以外の OS

においてもマイクロソフト純正の RDP クライアントアプリや、オープンソースの RDP 対応クライアントアプリを利用できます。そのため、リモートデスクトップ接続を使用する方法は、クライアントの OS を問わない、マルチプラットフォーム対応のリモート管理環境と言えます。ここでは、Windows クライアント標準の［リモートデスクトップ接続］デスクトップアプリ（Mstsc.exe）を使用する方法で説明します。

Windows 10 の場合は、タスクバーの検索ボックス（Cortana）に“**リモートデスクトップ接続**”と入力し、検索結果に表示された［リモートデスクトップ接続］をクリックします。Windows 10 およびそれ以前の Windows バージョンでは、［ファイル名を指定して実行］や［コマンドプロンプト］などから“**mstsc.exe**”を実行することで、［リモートデスクトップ接続］デスクトップアプリを開始することができます。



［リモートデスクトップ接続］デスクトップアプリのウィンドウが開いたら、［コンピューター］のテキストボックスに接続先のコンピューター名または IP アドレスを入力し、ローカル管理者の資格情報（既定は <コンピューター名>¥Administrator とそのパスワード）を入力して［接続］をクリックします。

LAN DISK Z に初めて接続する場合は MagicalFinder が便利

LAN DISK Z を設置したばかりで、そのコンピューター名や IP アドレスが不明の場合は、アイ・オー・データが Windows および macOS 向けに無料ダウンロード提供している MagicalFinder アプリを利用してください。MagicalFinder アプリを実行すると、ネットワーク上のデバイスが検出され、LAN DISK Z の場合は MagicalFinder アプリから直接にリモートデスクトップ接続を開始できます。

MagicalFinder のダウンロード（Windows および macOS 用）
https://www.iodata.jp/lib/product/m/3022.htm

ネットワークレベル認証（NLA）の無効化について（非推奨）

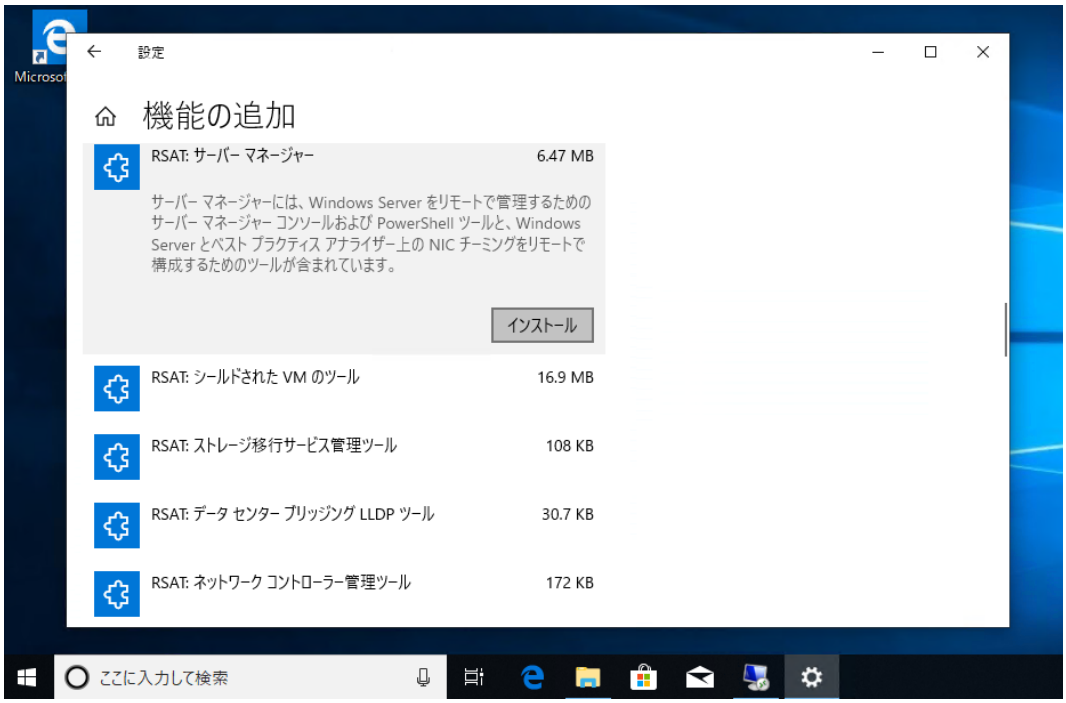
リモートデスクトップ接続のサーバー側の設定では、RDP セッションを確立する前にユーザー認証を要求するネットワークレベル認証（NLA）が有効になっていることが推奨されます。NLA が有効になっている場合、古いバージョンの RDP 対応クライアントやセキュリティパッチ（例、CVE-2018-0886 の CredSSP の脆弱性）が不足している RDP 対応クライアントからの接続は拒否されます。

セキュリティ上の問題があることを理解した上でセキュリティ設定を一時的に緩和して接続可能にするには（非推奨）、［設定］アプリの［システム］－［リモートデスクトップ］－［詳細設定］を開き、［コンピューターの接続にネットワークレベル認証の使用を求める（推奨）］をオフにします。または、コントロールパネルの［システムとセキュリティ］－［システム］－［リモートアクセスの許可］から［システムのプロパティ］の［リモート］タブを開き、［ネットワークレベル認証でリモートデスクトップを実行しているコンピューターからのみ接続を許可する（推奨）］をオフにします。

2.2　リモートサーバー管理ツール（RSAT）

管理用端末として Windows 10 コンピューターを利用できる場合は、Windows 10 に「リモートサーバー管理ツール（RSAT）」を追加することで、Windows Server 標準の管理ツールから直接リモートのサーバーを管理することができます。Windows 10 バージョン 1809（October 2018 Update）以降を実行している場合は、［設定］アプリの［アプリ］－［オプション機能の管理］を開き、［＋機能の追加］をクリックして RSAT のツールを個別に追加できます。Windows Server IoT 2019 for Storage を搭載する LAN DISK Z の管理のためには、以下の RSAT ツールを追加すればよいでしょう。

- RSAT：BitLocker ドライブ暗号化管理ユーティリティ
- RSAT：サーバーマネージャー
- RSAT：ファイルサービスツール



Windows 10 バージョン 1803（April 2018 Update）以前の RSAT

「リモートサーバー管理ツール（RSAT）」が Windows 10 のオプションの機能（オンデマンド機能）になったのは Windows 10 バージョン 1809（October 2019 Update）からであり、Windows 10 バージョン 1809 には Windows Server 2019 と同じバージョンのツールが含まれます。Windows 10 バージョン 1803（April 2018 Update）以前については、RSAT が以下の URL からダウンロード提供されています。ダウンロード提供されている RSAT は、Windows Server, version 1803、Windows Server, version 1709、または Windows Server 2016 バージョンに対応するものですが、Windows Server 2019 のリモート管理にも使用できます。ただし、古いバージョンの管理ツールは、Windows Server 2019 からの新機能の管理には対応していない場合があることに注意してください。

Windows 10 用のリモートサーバー管理ツール
https://www.microsoft.com/ja-jp/download/details.aspx?id=45520

TrustedHosts の構成（ワークグループ環境のみ）

Active Directory ドメインに参加していないワークグループ環境の場合は、RSAT のツールを使用する Windows クライアント側で Windows リモート管理（WinRM）で NTLM 認証を使用するために TrustedHosts の構成が必要です。それには、Windows クライアントの Windows PowerShell を管理者として開き、次のいずれかのコマンドラインを実行します。管理対象が複数ある場合は**"*"**を使用するか、**"<**

管理対象 1>,<管理対象 2>"のようにカンマで区切って指定してください。

```
Set-Item WSMan:¥localhost¥Client¥TrustedHosts "<管理対象のサーバー名または IP アドレス>" -Force
```

または

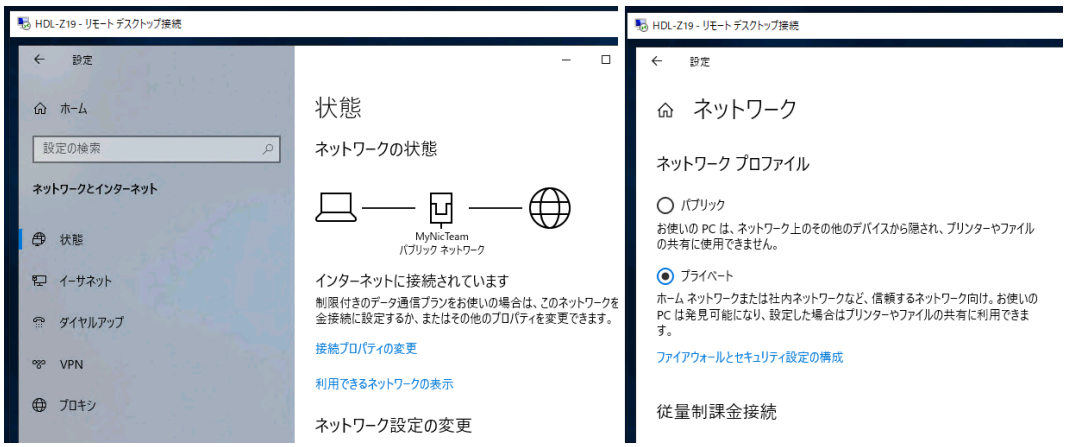
```
Set-Item WSMan:¥localhost¥Client¥TrustedHosts "*" -Force
```

この手順は Windows リモート管理（WinRM）に Kerberos 認証が使用される Active Directory ドメイン環境では不要です。

追加のファイアウォール規則の許可

RSAT のツールおよび Windows 10 にもともと含まれる MMC スナップインのツールをリモート管理に使用するには、サーバー側の［セキュリティが強化された Windows Defender ファイアウォール］で［受信の規則］の許可設定が必要なものがあります。ただしその前に、大前提としてサーバー側の現在のネットワークプロファイルを確認してください。

サーバー側（サーバーにリモートデスクトップ接続して）で、［設定］アプリの［ネットワークとインターネット］を開き、現在のネットワークプロファイルを確認します。ネットワークプロファイルが［ドメインネットワーク］（Active Directory ドメインに参加している場合）または［プライベートネットワーク］と認識されている場合は問題ありません。［パブリックネットワーク］と認識されている場合は、ほとんどの受信トラフィックがファイアウォールでブロックされる状態であり、リモート管理に影響する場合があります。そのため、［設定］アプリの［ネットワーク］－［イーサネット］を開き、ネットワーク名をクリックして［ネットワークプロファイル］を［パブリック］から［プライベート］に変更してください。

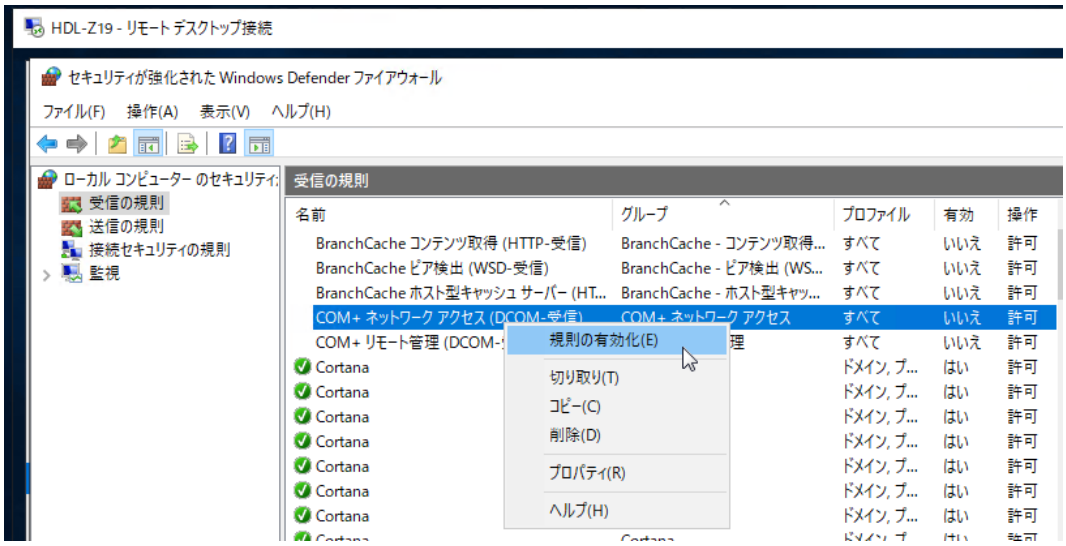


次に、サーバー側で［スタート］メニューの［Windows 管理ツール］から［セキュリティが強化された Windows Defender ファイアウォール］を開き、［受信の規則］の以下の規則またはグループに含まれる規則を有効化します。

- ［COM＋ネットワークアクセス（DCOM-受信）］の規則

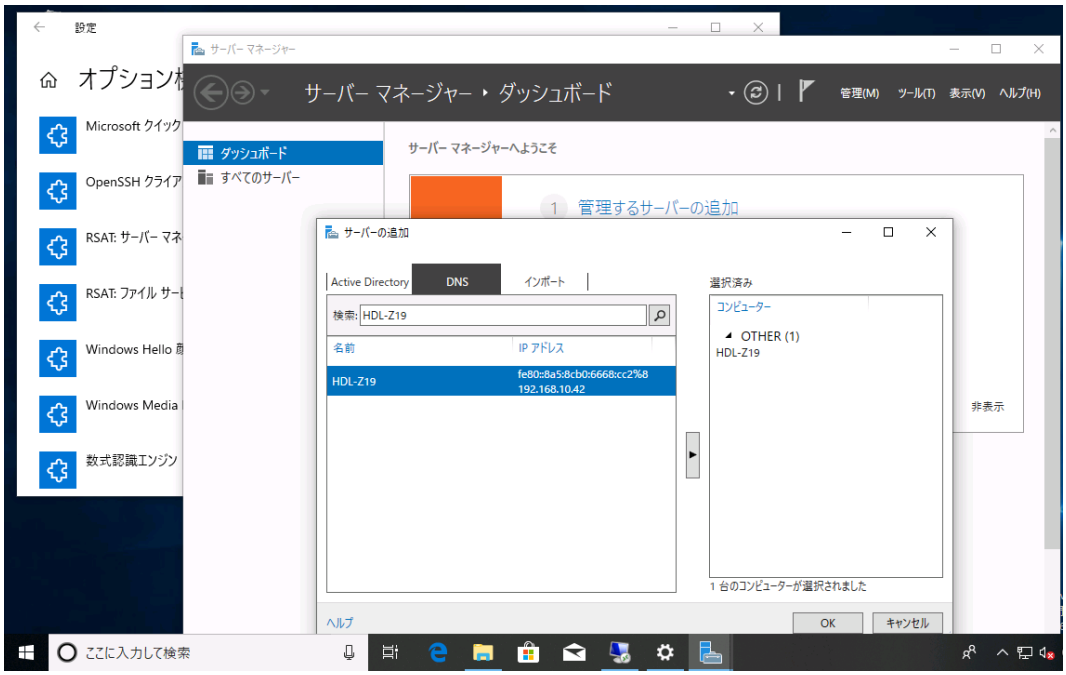
- ［リモートイベントログ管理］グループのすべての規則
- ［リモートボリューム管理］グループのすべての規則

なお、［リモートボリューム管理］グループの規則は、接続元の Windows クライアント側の［セキュリティが強化された Windows Defender ファイアウォール］の［受信の規則］でも有効化する必要があります。

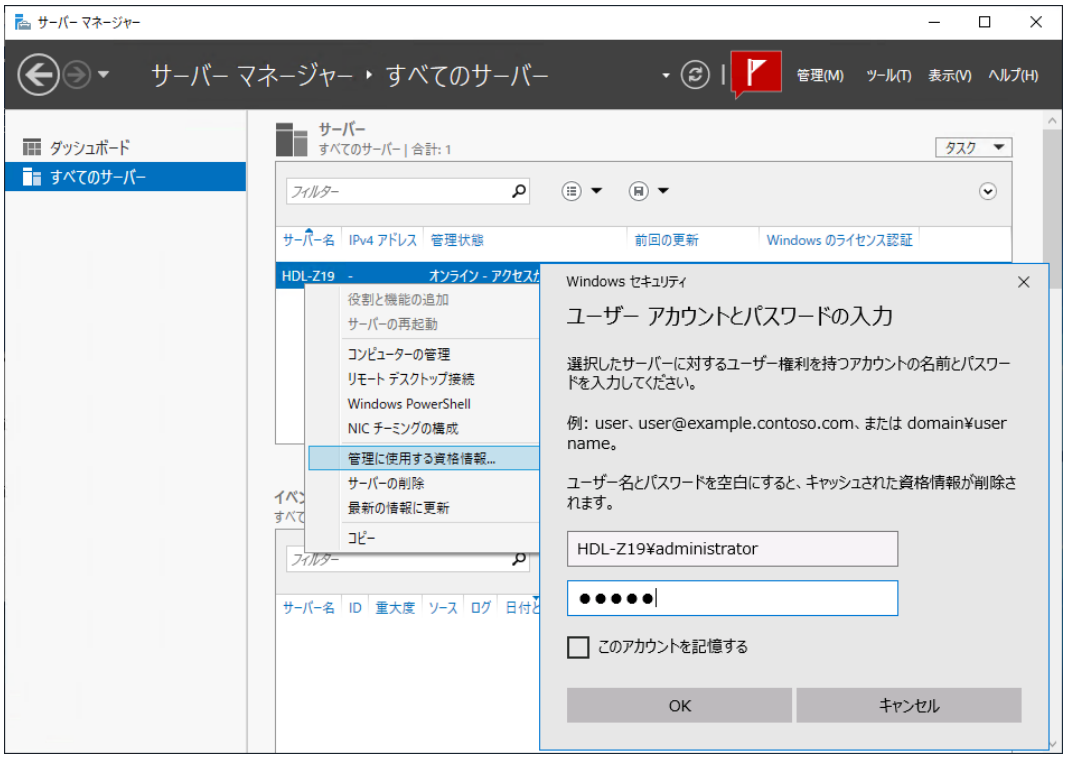


管理対象のサーバーの追加

以上の事前準備ができたら、Windows 10 の［スタート］メニューに追加された［Server Manager］をクリックして［サーバーマネージャー］を開始します。［ダッシュボード］にある［①管理するサーバーの追加］をクリックすると、［サーバーの追加］ダイアログボックスが開くので、［DNS］タブに切り替え、LAN DISK Z のコンピューター名または IP アドレスを検索し、［▶］をクリックして管理対象に追加して、［OK］をクリックします。



［サーバーマネージャー］は、Windows 10 のサインインに使用している資格情報を使用してリモートのサーバーに接続を試みます。しかし、管理対象のサーバーの資格情報（ユーザー名とパスワード）と一致しないため、アクセスが拒否されて失敗するはずです。そこで、［サーバーマネージャー］の［すべてのサーバー］を開き、追加したサーバーを右クリックして［管理に使用する資格情報］をクリックし、サーバーの管理者の資格情報（<コンピューター名>¥Administrator とそのパスワード）を入力し、［OK］をクリックします。



以上の設定により、アクセス拒否のエラーが解消され、［サーバーマネージャー］による管理や、［サーバーマネージャー］から起動する［コンピューターの管理］や［Windows PowerShell］、その他の操作を使用したリモートサーバーの管理が可能になります。

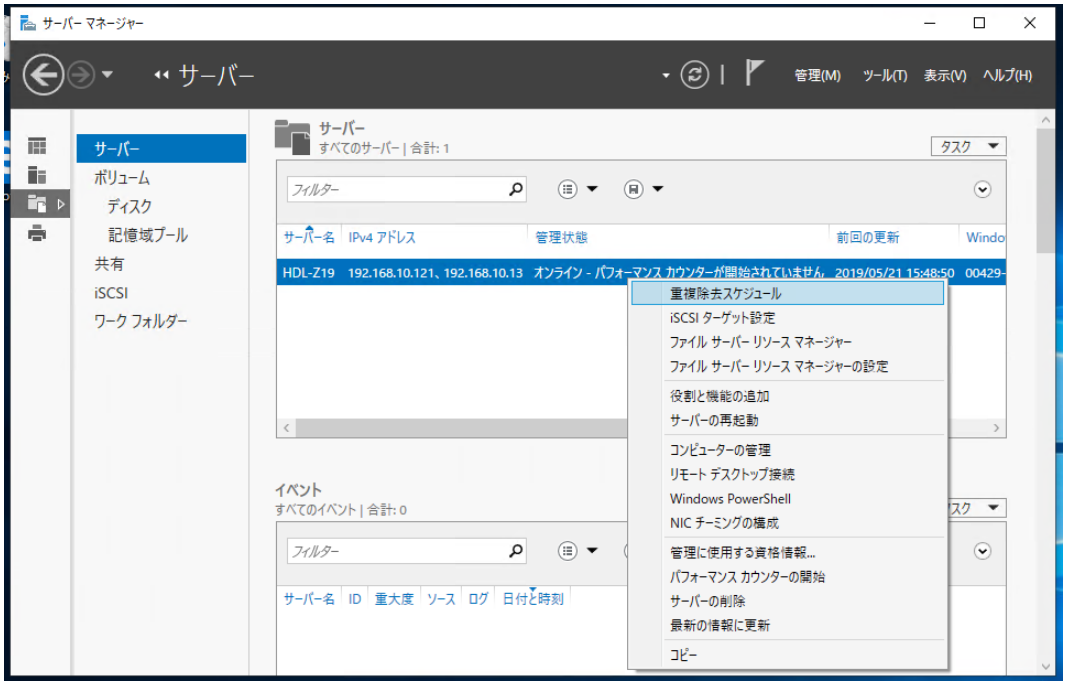
> **リモート管理に利用できないツールは、リモートデスクトップ接続で代替**
>
> ［コンピューターの管理］に含まれるほとんどのツールは、このガイドで説明した方法で利用できるはずです。ただし、［デバイスマネージャー］と［ディスクの管理］は、リモート管理に対応していないため使用できません。これらのツールを使用する場合は、リモートデスクトップ接続を利用してください。
>
> また、管理ツールの中には、追加のファイアウォール許可設定やセキュリティ設定が必要な場合や、ドメイン管理者アカウント（またはサーバーのローカル管理者と同じ名前、同じパスワード）による Windows 10 へのサインインが要求されるものもあります。これらはリモートデスクトップ接続で完全に代替できるため、個別のツールについては説明を省略します。

2.3　サーバーマネージャーによるファイルサーバーの管理

リモートデスクトップ接続から起動する［サーバーマネージャー］、または Windows 10 に追加した RSAT の［サーバーマネージャー］を使用すると、LAN DISK Z の Windows Server IoT 2019 for Storage が提供するファイルサーバーの主要な機能を単一の GUI で管理することができます。

ファイルサービスと記憶域サービス

［サーバーマネージャー］にファイルサーバー機能を持つサーバーを管理対象として追加すると、［ファイルと記憶域サービス］にそのサーバーが分類され、ここからボリュームや共有、iSCSI ターゲットなどの管理ができるようになります。

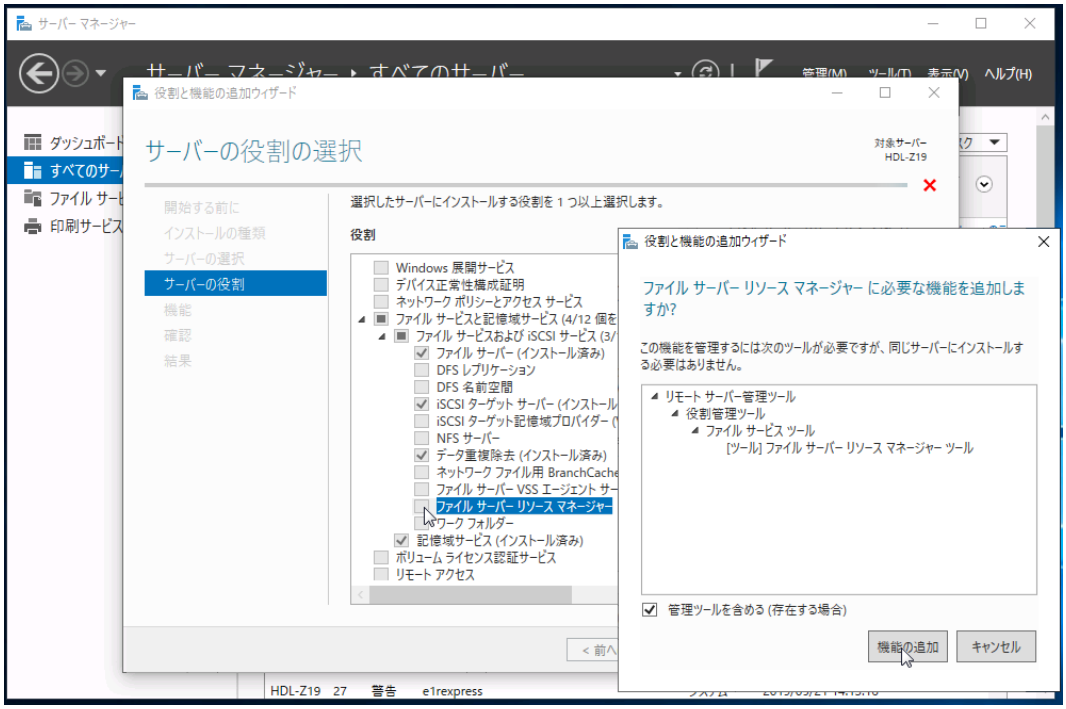


ファイルサーバーリソースマネージャーの役割サービスの追加

このガイドの次に説明するファイルサーバーリソースマネージャーの役割サービスは、LAN DISK Z の Windows Server IoT 2019 for Storage には既定でインストールされていません。［サーバーマネージャー］の［すべてのサーバー］で管理対象のサーバーを右クリックし、［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］を開始して追加してください。［ファイルサーバーリソースマネージャー］の役割サービスは、［ファイルサービスと記憶域サービス］－［ファイルサービスおよび iSCSI サービス］の下にあります。この役割サービスとともに、関連する管理ツールをインストールします。インストールを完了するために、通常、サーバーの再起動は求められません。

役割サービスを追加したら、ファイルサーバーリソースマネージャーのリモート管理を可能にするために、［Windows Defender ファイアウォール］の［例外の規則］で以下のグループの規則を有効化します。

- ［リモートファイルサーバーリソースマネージャー管理］グループのすべての規則



［ファイルサーバーリソースマネージャー］スナップインで使用される資格情報

Windows 10 に追加した RSAT の［サーバーマネージャー］から開始する［ファイルサーバーリソースマネージャー］スナップインや、［ファイルサーバーリソースマネージャー］スナップインの［別のコンピューターに接続］によるリモートサーバーのファイルサーバーリソースマネージャーの接続には、Windows 10 にサインイン中の資格情報（ローカルアカウント、Microsoft アカウント、または Active Directory ドメインアカウント）が使用されます。［サーバーマネージャー］に指定した別の資格情報が使用されることはありません。

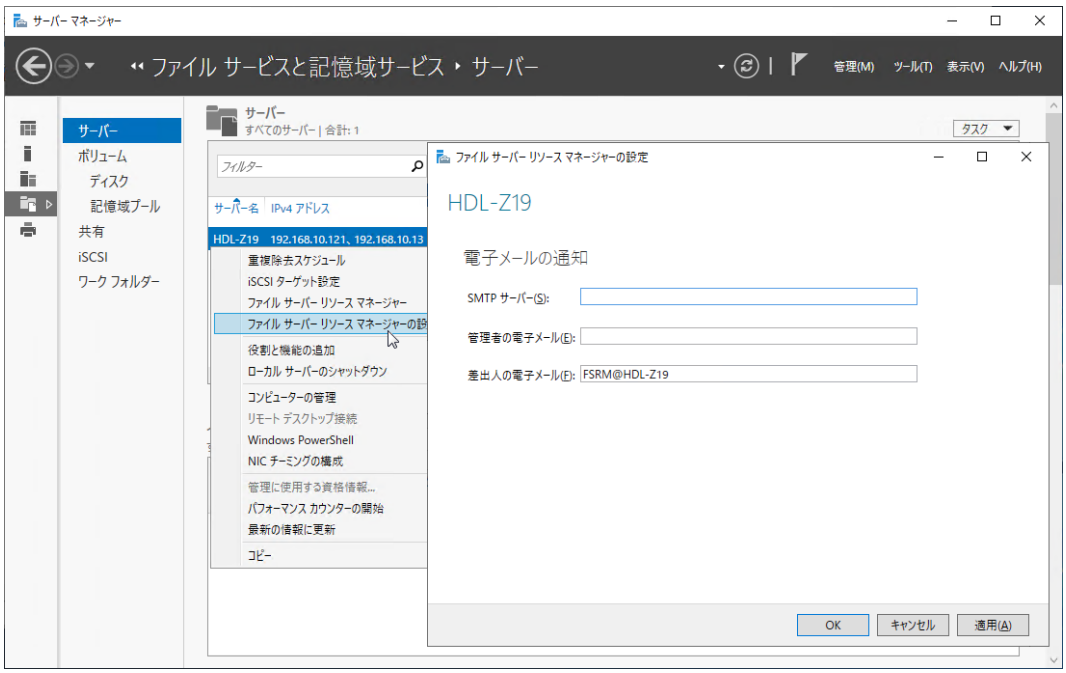
そのため、ファイルサーバーリソースマネージャーをリモートから管理するには、通常、サーバーの管理者アカウント（ローカル Administrators グループのメンバー）となっている、Active Directory ドメインアカウントでサインインしていることが前提となります。この要件は、Windows 10 のローカルアカウントして、サーバー側に作成したローカル管理者アカウントと同じ名前（Administrator の使用は非推奨）、同じパスワードのユーザーを作成し、そのユーザーで Windows 10 にサインインすることで回避することができます。

ファイルサーバーリソースマネージャーの全体設定

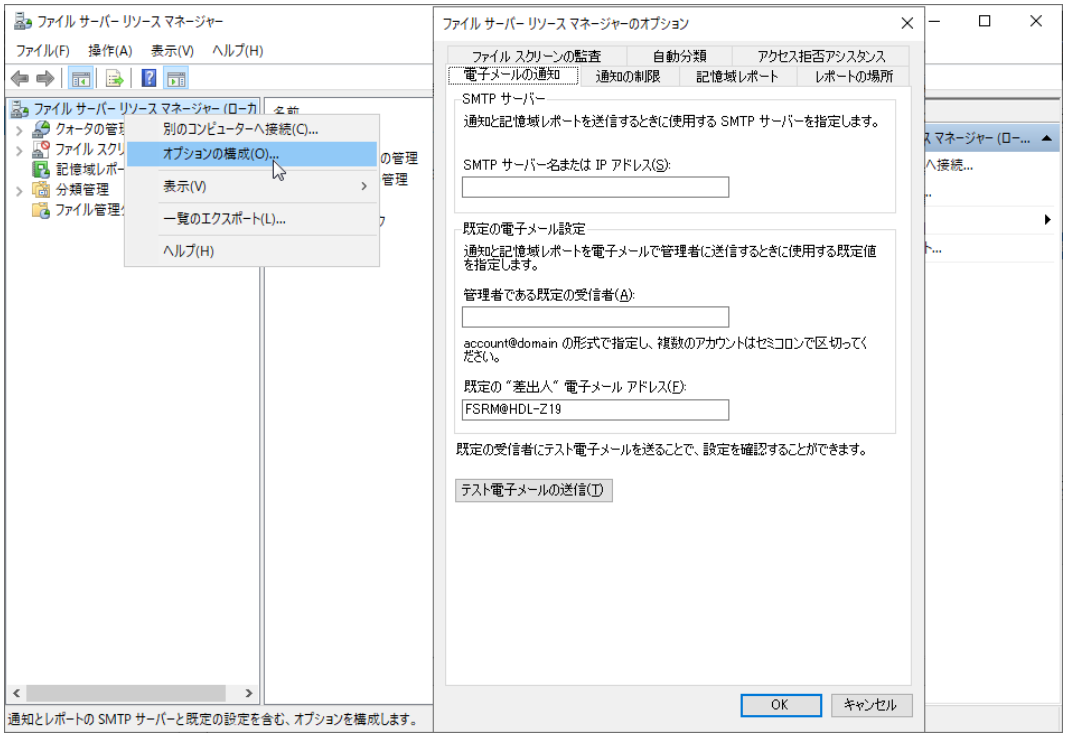
ファイルサーバーリソースマネージャーには、電子メールによる管理者やユーザーへの通知機能があります。この通知機能を利用するためには、少なくとも SMTP ポート 25、匿名アクセスでメールの転送が可能な SMTP メールサーバーが社内ネットワーク上で利用できる必要があります。

転送用のメールサーバーを利用できる場合は、［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］－［サーバー］で管理対象のサーバーを右クリックして［ファイルサーバーリソースマネージャーの設定］をクリックし、［SMTP サーバー］にメールサーバーの FQDN または IP アドレスを設定します。ま

た、[管理者の電子メール] に通知先となる管理者の電子メールアドレスを、[差出人の電子メールアドレス] に送信元となる電子メールアドレスを入力します。



上記の設定は、[ファイルサーバーリソースマネージャー] スナップインの [オプションの構成] の [電子メール] タブで設定することもできます。



メール転送サーバーのセキュリティについて

SMTP ポート 25、匿名アクセスでメール転送を許可するようなメール環境は、マルウェアによって踏

み台に使用されるリスクがあるため、高いセキュリティが要求される現代のメール環境としては不適切なものです。このセキュリティ上のリスクを理解した上で、必要な対策（転送元 IP アドレスや転送先アドレスの制限など）を講じたメールサーバーを用意できる場合に限り、ファイルサーバーリソースマネージャーのメール通知環境をセットアップしてください。

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やファイルスクリーンの管理でユーザーごとの通知を行う場合は、さらに Active Directory ドメイン環境が必要になります。ファイルサーバーリソースマネージャーは、通知先のユーザーのメールアドレスとして、Active Directory のドメインユーザーアカウントの［電子メール（mail)］属性を使用します。つまり、ユーザーごとの通知機能は、LAN DISK Z の NAS デバイスとクライアントの両方が Active Directory ドメインのメンバーとしてセットアップされており、NAS デバイスの共有フォルダーへのアクセスが Active Directory のドメインユーザーアカウントで行われる環境でのみ利用できます。

このガイドの「付録　外部メールサービスを利用したメール通知の実現」では、ファイルサーバーリソースマネージャーのメール通知機能を使用せずに、Outlook.com や Office 365 といった外部メールサービスを使用して通知する方法について説明しています。ユーザーごとの通知には利用できませんが、管理者への固定メッセージの通知に応用することができます。

3　ファイルサーバーリソースマネージャーの活用

ファイルサーバーリソースマネージャーの機能の一部は、［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］に統合されています。すべての機能は［ファイルサーバーリソースマネージャー］スナップインで管理できます。

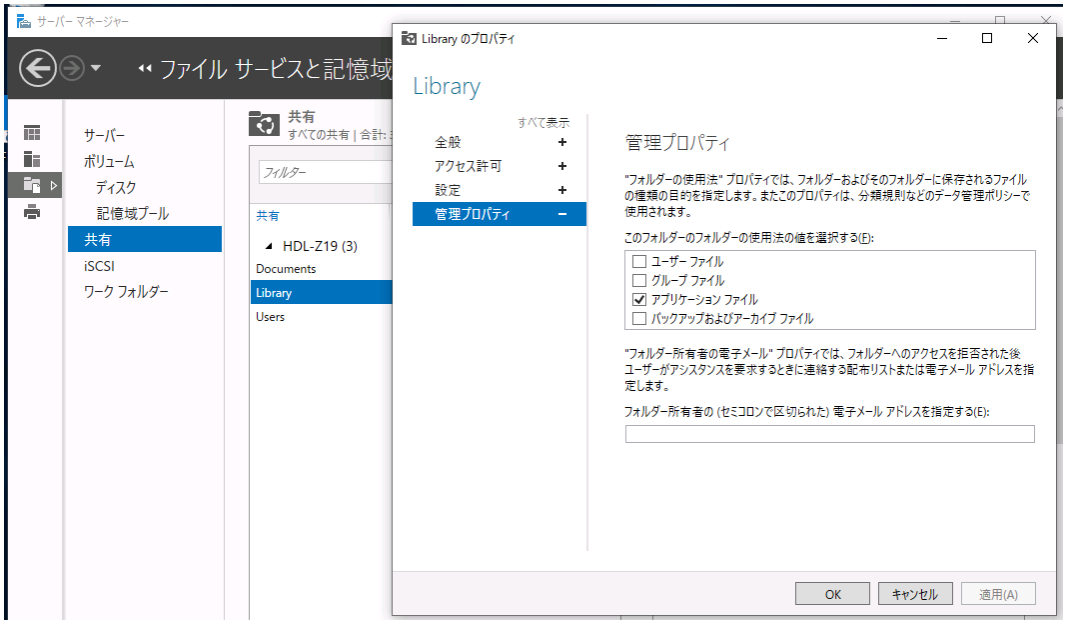
3.1　フォルダーの使用法（分類プロパティ）

ファイルサーバーリソースマネージャーには分類プロパティという概念があります。既定では［フォルダーの使用法］というローカルプロパティに次の 4 つの値が設定済みで利用可能な状態になっています。共有フォルダーに対して［フォルダーの使用法］を設定しておくこと、ファイルサーバーリソースマネージャーの他の機能においてフォルダーの対象化のために利用できます。例えば、個別のフォルダーごとに指定する代わりに、［ユーザーファイル］ローカルプロパティが設定されたすべてのフォルダーを対象化できます。

- ユーザーファイル（User Files）
- グループファイル（Group Files）
- アプリケーションファイル（Application Files）
- バックアップおよびアーカイブファイル（Backup and Archival Files）

［フォルダーの使用法］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］－［共有］から開始する［新しい共有ウィザード］でファイル共有プロファイル［SMB 共有－高度］を選択した際に、［管理プロパティ］のページで選択できるようになっています。ファイル共有プロファイル［SMB 共有－簡易］を選択した場合は、分類プロパティを設定する場面はありませんが、作成済みの共有のプロパティの［管

理プロパティ］を使用して後から選択することができます。



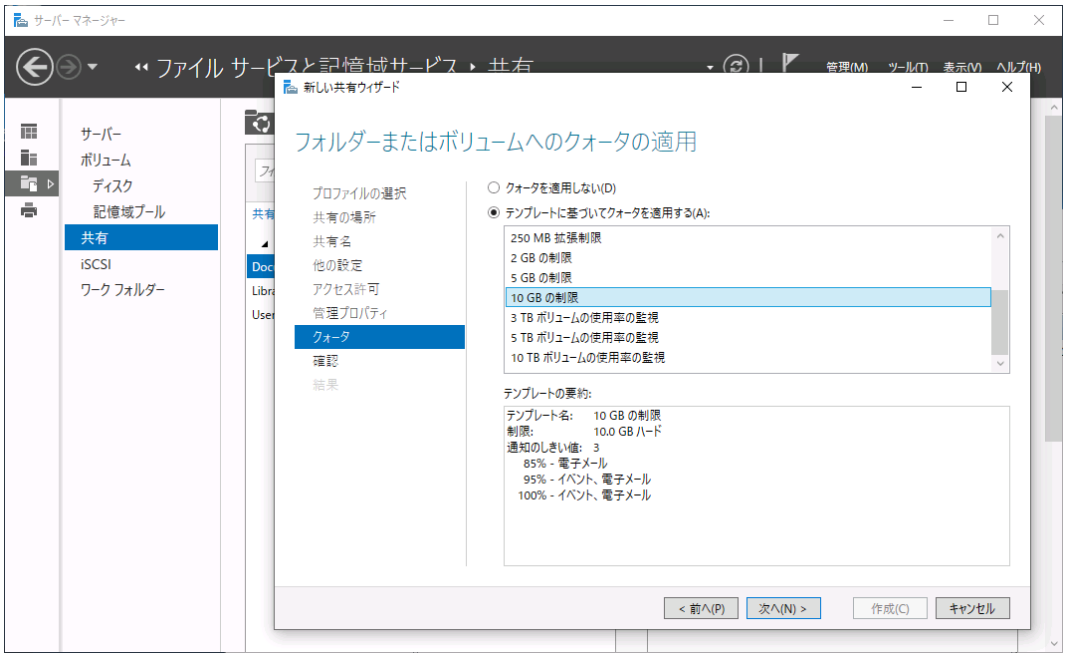
［フォルダーの使用法］ローカルプロパティは、［ファイルサーバーリソースマネージャー］スナップインの［分類管理］－［分類プロパティ］で編集することができます。例えば、独自の値を追加することができます。また、［操作］メニューの［フォルダー管理プロパティの設定］を使用して、フォルダーに対してプロパティを設定することもできます。

> ［フォルダーの使用法］の表示名と値
>
> ［サーバーマネージャー］や［ファイルサーバーリソースマネージャー］スナップインは、［フォルダーの使用法］ローカルプロパティが実際の値ではなく、ローカライズされた表示名（例：ユーザーファイル）で表示します。［ファイルサーバーリソースマネージャー］スナップインを使用して［フォルダーの使用法］ローカルプロパティの編集画面を開くと、値を追加や変更をしなくても、日本語の表示名から英字の値（例：User Files、Application Files）に変わってしまうことに注意してください。これは表示上の問題であり、実際の分類に影響することはありません。

3.2　クォータの管理

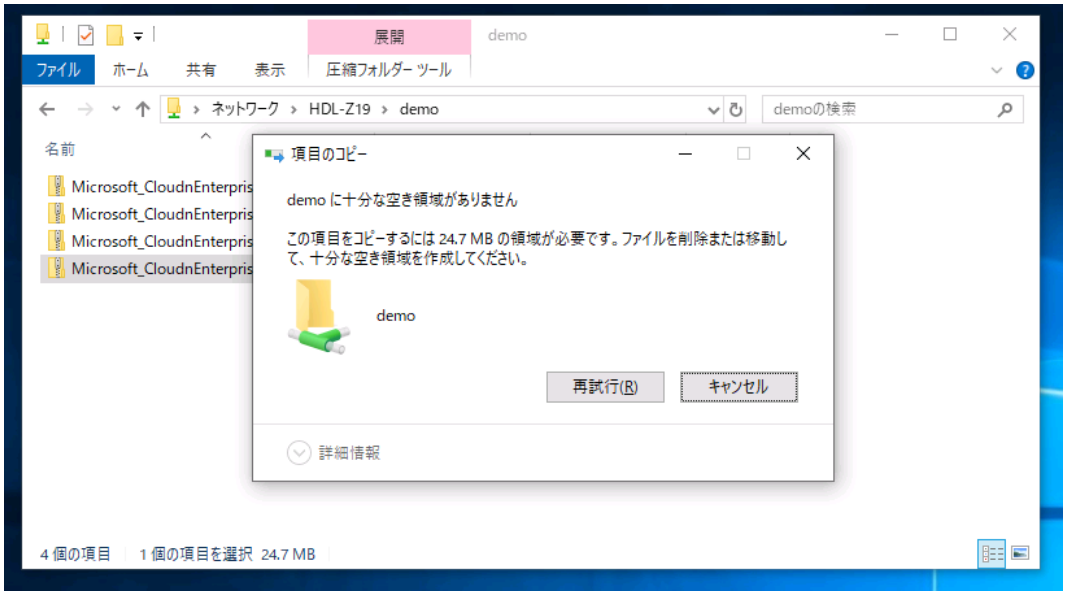
ファイルサーバーリソースマネージャーを使用すると、ファイルサーバーの共有フォルダーのディレクトリパス内でユーザーが使用できるディスク領域に上限を設定することができます。クォータには、制限を超えてのファイルの保存を拒否する「ハードクォータ」と、使用量の計測だけ行い実際の制限は行わない「ソフトクォータ」の 2 種類があり、制限値に対するしきい値を設定して、管理者やユーザーへの電子メールによる警告の通知やイベントログへの記録、コマンドの実行などの処理を自動化することができます。Windows は標準で、NTFS ボリュームでディスククォータを作成することができますが（エクスプローラーでボリュームのプロパティを開き［クォータ］タブからクォータを作成できます）、これはディスク単位のクォータ制限であり、ファイルサーバーリソースマネージャーのような高度な管理機能は備えていません。

［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］－［共有］から開始する［新しい共有ウィザード］では、ファイル共有プロファイル［SMB 共有－高度］を選択した場合に、［クォータ］ページでクォータのテンプレートを選択できるようになっています。［ファイルサービスと記憶域サービス］－［共有］で既存の共有フォルダーを右クリックして［クォータの構成］を開き、あとから設定または変更することもできます。

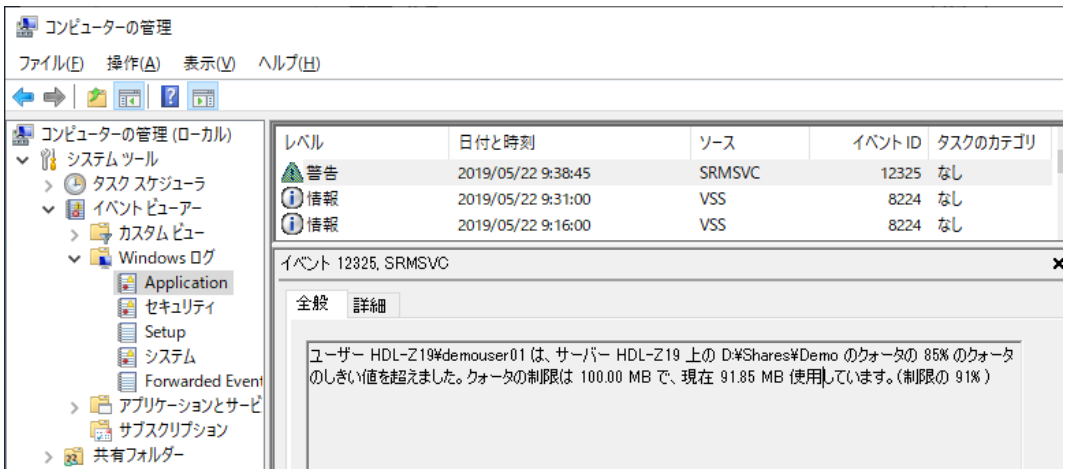


ユーザーがクォータのしきい値を超えた場合

ユーザーが共有フォルダーにファイルを保存したときに、ハードまたはソフトクォータのしきい値を超えた場合、しきい値に定義されている操作が自動実行され、管理者やユーザーへの通知やイベントログへの記録が行われます。また、ファイルを保存する際にハードクォータの 100%に達する場合は、空き領域不足で保存はブロックされます。

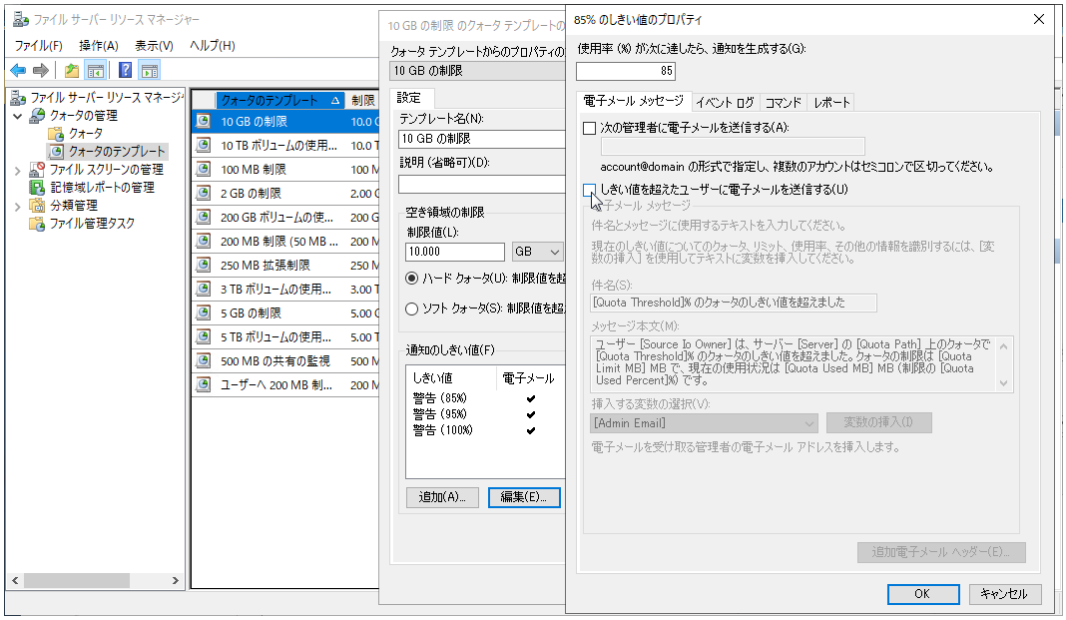


クォータ設定でイベントログに記録するように設定した場合、サーバーの［Application］ログにソース［SRMSVC］からのイベントが記録されます。



クォータのテンプレートの編集

ファイルサーバーリソースマネージャーには既定でハードとソフトの 12 のクォータのテンプレートが定義済みになっています。いずれもユーザー（Active Directory ドメイン環境が必要）や管理者への電子メール通知が設定されています。そのため、メール環境が利用できない場合、既定のクォータのテンプレートをそのまま利用することはできません（メール通知が機能しません）。メール環境が利用できない場合は、使用するクォータのテンプレートの管理者やユーザーへの電子メール通知設定をオフにするか、電子メール通知設定を含まない独自のクォータのテンプレートを作成して使用してください。



電子メール通知の代替策について

電子メール通知機能を利用できる環境が無い場合、管理者はハードクォータに達したユーザーからのクレームや、イベントログの監視、ソフトクォータと記憶域レポートの結果に基づいて、ユーザーに対し

て不要なファイルの削除の依頼を行ったり、クォータの制限を増やしたりといったマニュアルの対応で運用できるでしょう。最も重要なことは、サーバーのストレージを使い果たしてしまう前に対処することです。

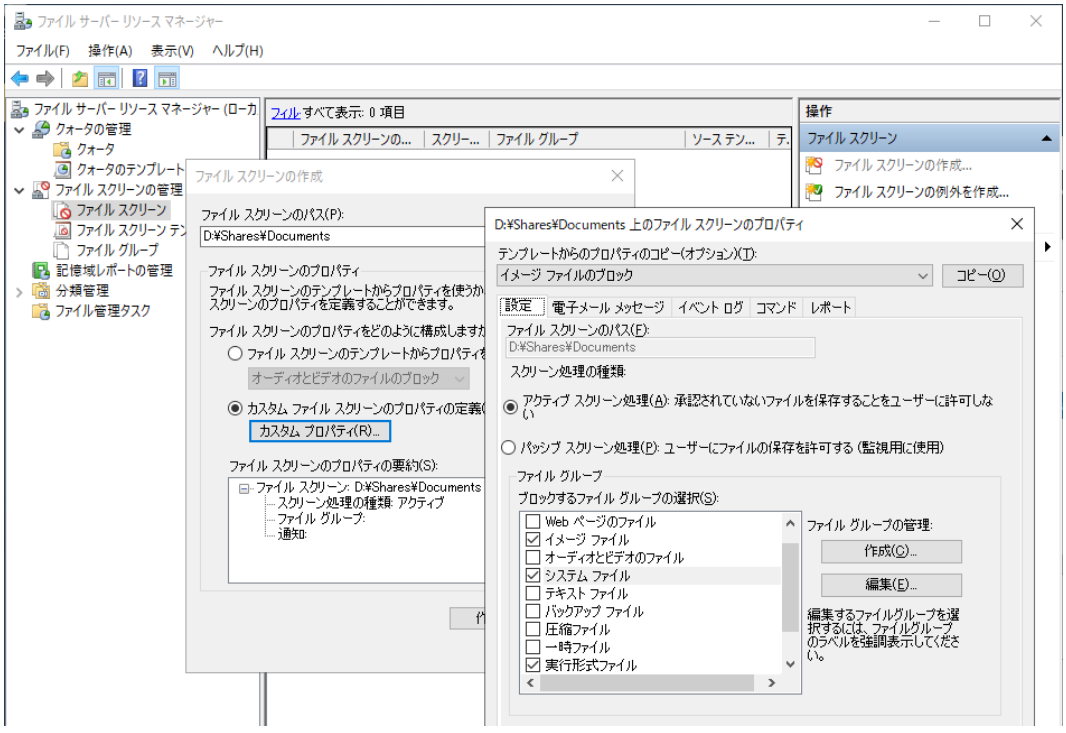
管理者への固定メッセージの通知については、このガイドの「付録　外部メールサービスを利用したメール通知の実現」の方法をクォータのテンプレートのコマンド実行機能（しきい値のプロパティの［コマンド］タブ）に応用することで実装可能です。

3.3　ファイルスクリーンの管理

ファイルサーバーリソースマネージャーのファイルスクリーンの管理は、ファイルの種類（拡張子）に基づいて、指定したディレクトリパスへの保存をブロック、または警告やイベントログへの記録で監視する機能を提供します。ファイルスクリーン処理には、該当するファイルの種類の保存を許可しない「アクティブ」と、監視のみで保存を許可する「パッシブ」の 2 種類あり、フォルダーに対するカスタム設定またはファイルスクリーンのテンプレートによる設定が可能です。

ファイルスクリーンの作成

ファイルスクリーンの管理は、［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］には統合されていません。この機能を利用するには、［ファイルサーバーリソースマネージャー］スナップインの［ファイルスクリーンの管理］－［ファイルスクリーン］の［操作］ペインから［ファイルスクリーンの作成］をクリックし、ディレクトリパス（例えば、共有フォルダーのローカルパス）に対してスクリーン処理設定を作成します。

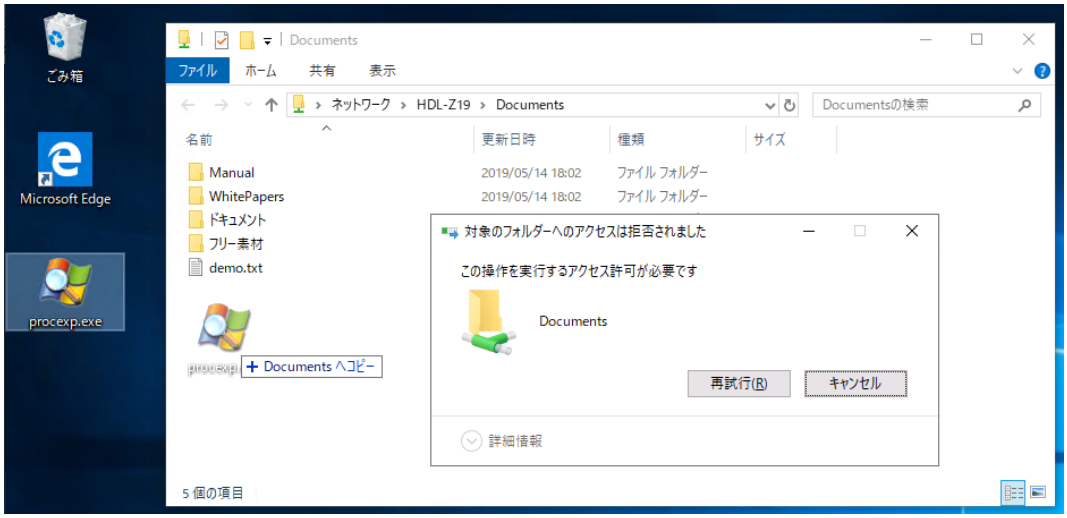


例えば、ドキュメント用の共有フォルダーに実行可能形式のファイル（.exe、.bat、.inf など）やシステム

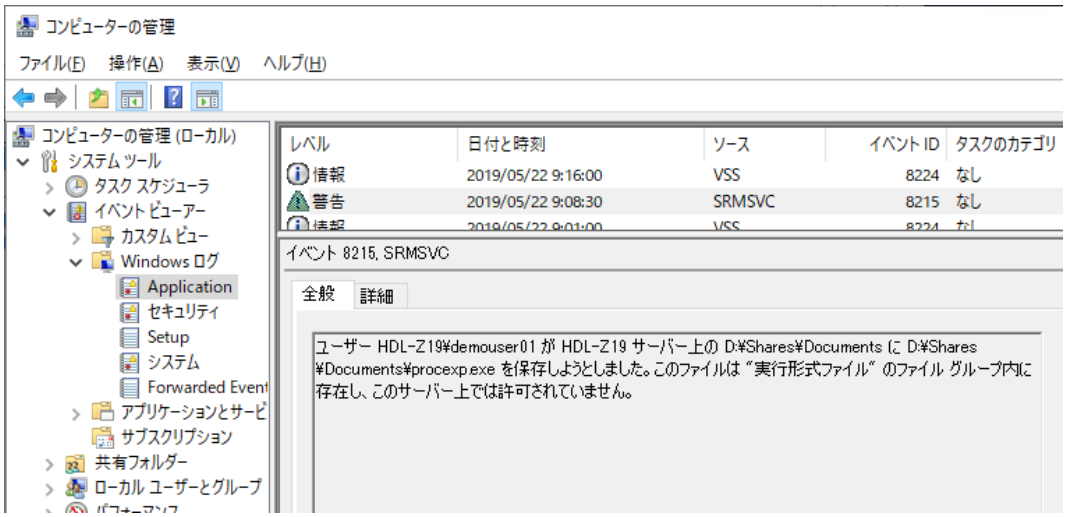
ファイル（.dll、.sys など）が保存されるのをブロックするには、カスタム設定でファイルグループの［実行形式ファイル］と［システムファイル］をチェックし、［アクティブスクリーン処理］を選択します。スクリーン処理が発生した際に通知やイベントログへの記録を行うには、［電子メールメッセージ］タブや［イベントログ］タブを設定します。

ファイルスクリーン処理

ユーザーがドキュメント用の共有フォルダーに実行可能形式やシステムファイルの種類のファイルを保存しようとすると、アクセスが拒否されます。



イベントログに記録するように設定した場合、サーバーの［Application］ログにソース［SRMSVC］からのイベントが記録されます。



ファイルスクリーンのテンプレートの編集

既定で以下の 4 つのファイルスクリーンのテンプレートが定義済みになっており、［ファイルサーバーリソースマネージャー］スナップインの［ファイルスクリーンの管理］－［ファイルスクリーンテンプレート］で確認および編集することができます。

- イメージファイルのブロック（アクティブ）
- オーディオとビデオのファイルのブロック（アクティブ）
- 実行形式とシステムのファイルの監視（パッシブ）
- 実行形式のファイルのブロック（アクティブ）

クォータのテンプレートと同様に、ファイルスクリーンのテンプレートにもユーザー（Active Directory ドメイン環境が必要）や管理者への電子メール通知が設定されています。そのため、メール環境が利用できない場合、既定のクォータのテンプレートをそのまま利用することはできません（メール通知が機能しません）。メール環境が利用できない場合は、使用するファイルスクリーンのテンプレートの管理者やユーザーへの電子メール通知設定をオフにするか、電子メール通知設定を含まない独自のファイルスクリーンのテンプレートを作成して使用してください。あるいは、その都度、カスタム設定を行います。

電子メール通知の代替策について

電子メール通知機能を利用できる環境が無い場合は、アクセスが拒否されたユーザーからのクレームや、イベントログの監視、記憶域レポートの結果に基づいて、ユーザーにマニュアルで対応することができるでしょう。

管理者への固定メッセージの通知については、このガイドの「付録　外部メールサービスを利用したメール通知の実現」の方法をファイルスクリーン処理のコマンド実行機能（プロパティの［コマンド］タブ）に応用することで実装可能です。

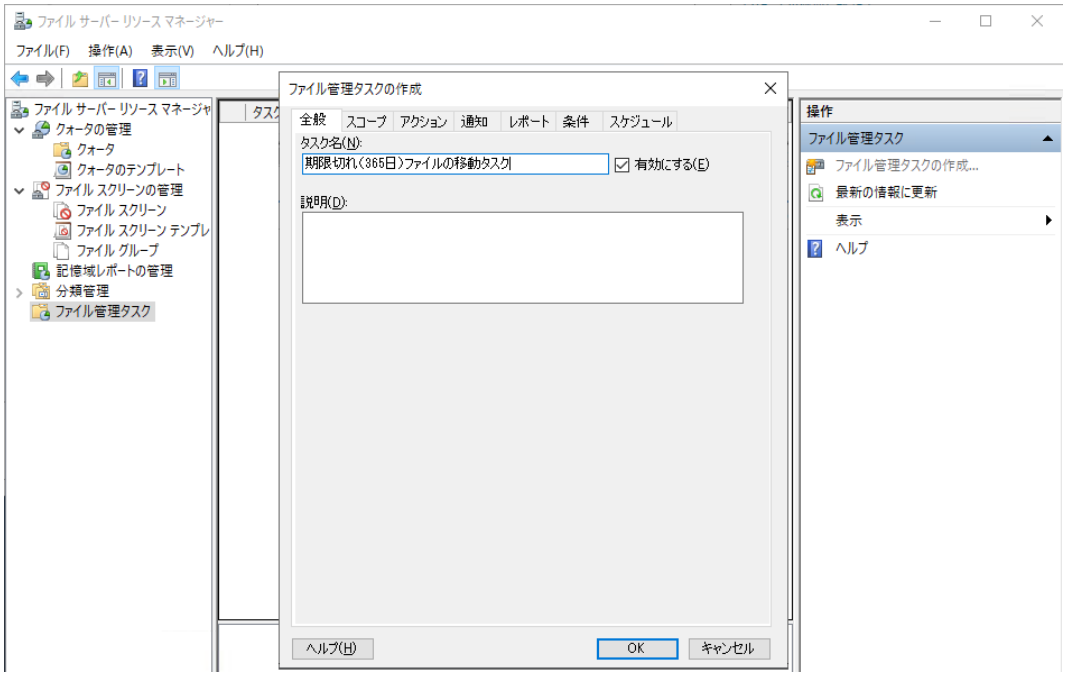
3.4　ファイル管理タスク

ファイルサーバーリソースマネージャーの分類管理とファイル管理タスクは FCI（File Classification Infrastructure）とも呼ばれ、ファイルのアーカイブやセキュリティ（自動暗号化や動的アクセス制御）を実現する柔軟なカスタマイズ機能を提供します。自動暗号化や動的アクセス制御は Active Directory ドメイン環境が前提で、高度なカスタマイズは構成が複雑になり、正常性の監視やメンテナンス作業の負担が大きくなってしまうでしょう。

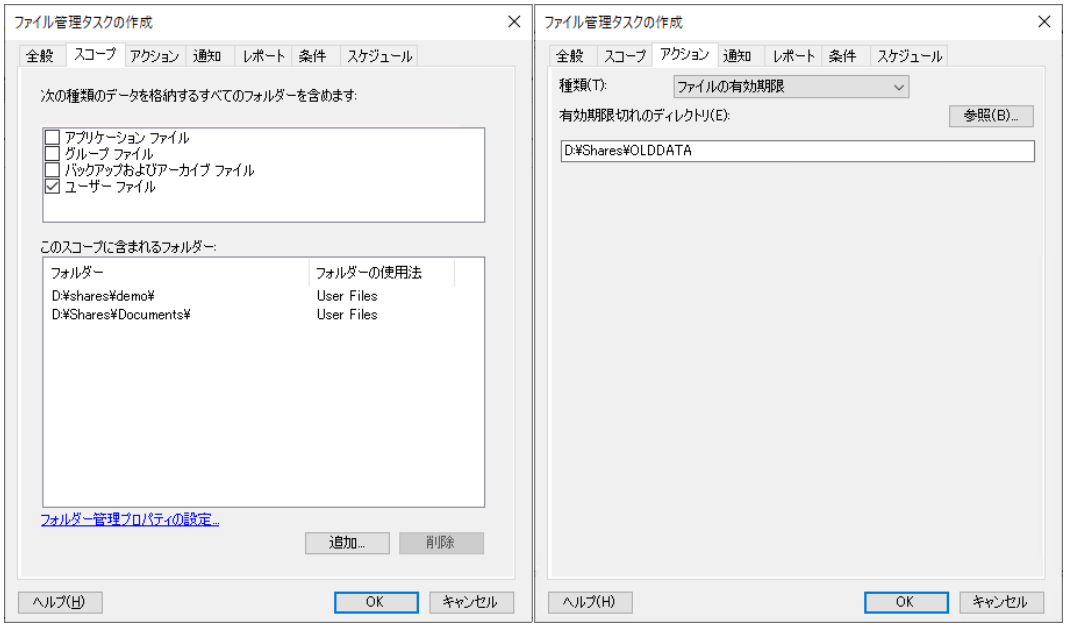
ここでは、ファイルのアーカイブについての簡単な活用例を紹介します。ユーザーのドキュメント用フォルダーに格納されていて長期間アクセスされていないファイルを、ファイル管理タスクのスケジュール実行を使用してアーカイブ用のディレクトリに移動するという利用シナリオです。管理者は、事前にユーザーに対して長期間アクセスのないファイルは自動的に特定の場所（アーカイブ用の共有フォルダーなど）に移動する旨を事前に周知しておき、目的のファイルが見つからない場合はユーザー自身で移動先のパスから探してもらって、不要なファイルを削除する、あるいは元の場所に戻す（最終アクセス日が更新されます）など、対処を要請することができます。

ファイル管理タスクの作成

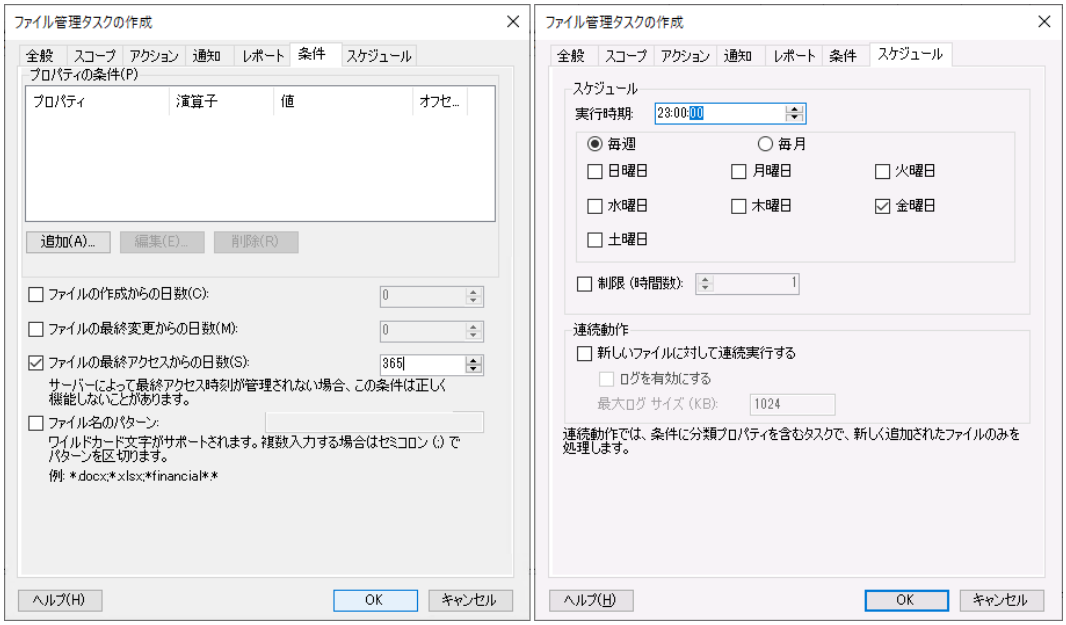
ファイル管理タスクは、[ファイルサーバーリソースマネージャー] スナップインの [ファイル管理タスク] の [操作] ペインから [ファイル管理タスクの作成] をクリックして作成します。[ファイル管理タスクの作成] ダイアログボックスの [全般] タブで [タスク名] に分かりやすい名前を指定したら、[スコープ] タブに切り替えます。



[スコープ] タブでは、「3.1　フォルダーの使用法（分類プロパティ）」で説明した分類プロパティに基づいて対象のフォルダーを選択させることができます。[追加] をクリックして個別のパスを指定することもできます。続いて [アクション] タブに切り替え、ドロップダウンリストボックスから [ファイルの有効期限] を選択し、[有効期限切れのディレクトリ] にファイルの移動先のパスを指定します。



［条件］タブに切り替えると、［ファイルの作成からの日数］、［ファイルの最終変更からの日数］、［ファイルの最終アクセスからの日数］、またはこれらの組み合わせで有効期限を設定します。最後に［スケジュール］タブに切り替え、実行スケジュールを調整します。電子メール通知環境がある場合は、［通知］タブを構成してファイルの移動をユーザーに通知するように設定することもできます。



3.5　記憶域レポートの管理

ファイルサーバーリソースマネージャーは、以下に示す 10 種類の記憶域レポートの作成機能を持ちます。これらのレポートは［ファイルサーバーリソースマネージャー］スナップインを使用してスケジュールまたは手動で作成することができます。また、クォータやファイルスクリーン処理、ファイル管理タスクと連動してレポートを生成させることもできます。

- クォータの使用率
- ファイルグループごとのファイル
- ファイルスクリーン処理の監査
- プロパティごとのファイル
- プロパティ別フォルダー
- 最近アクセスされていないファイル
- 最近アクセスしたファイル
- 重複しているファイル
- 所有者ごとのファイル
- 大きいサイズのファイル

［ファイルスクリーン処理の監査］レポートについて

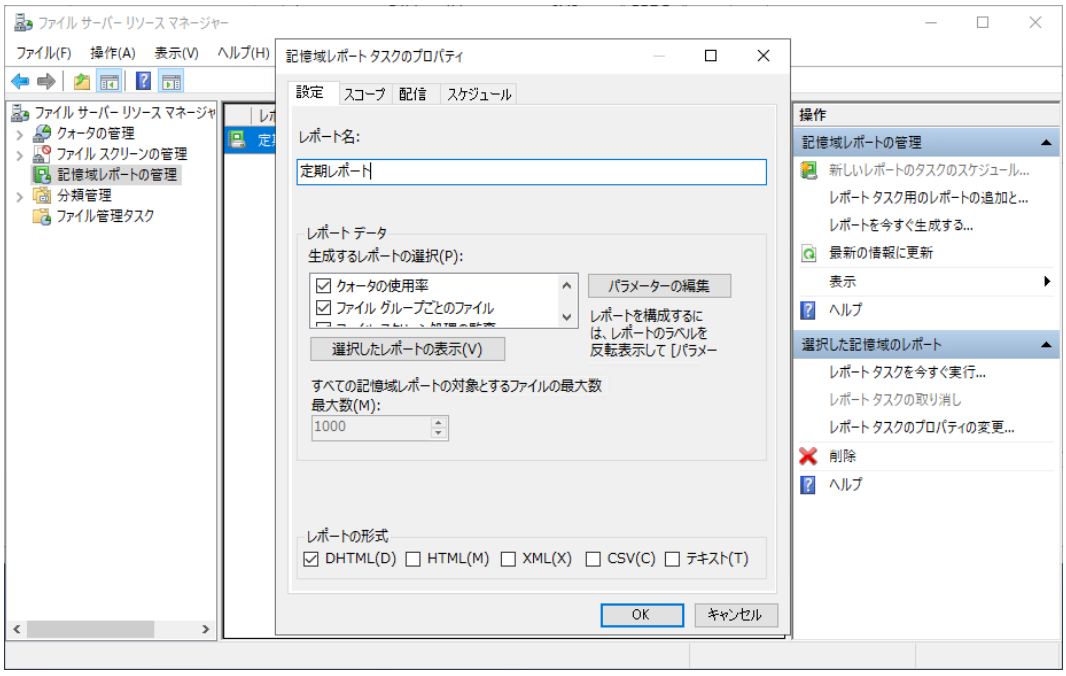
［ファイルスクリーン処理の監査］レポートを生成するには、ファイルサーバーリソースマネージャーの全体設定である［オプションの構成］の［ファイルスクリーンの監査］タブで［監査データベースにファイルスクリーン処理の動作状況を記録する］をチェックしておく必要があります。

このオプションは既定で無効です。無効の場合、または有効であっても監査データベースが空の状態の場合、［ファイルスクリーン処理の監査］レポートの生成はエラーで失敗します。このレポートを含む同じスケジュールまたは手動タスクはエラーが発生すると途中でレポートの生成を停止するため、他のレポートの生成に影響することに注意してください。

スケジュール生成と今すぐ生成

［ファイルサーバーリソースマネージャー］スナップインの［記憶域レポートの管理］の［操作］ペインで［新しいレポートのタスクのスケジュール］をクリックすると、記憶域レポートをスケジュールに従って自動生成させることができます。［レポート名］を入力し、生成するレポートを選択したら、［スコープ］タブで分類プロパティまたは個別のパス設定で対象のフォルダーを指定し、［スケジュール］タブでスケジュールを調整します。［設定］タブの［パラメーターの編集］では、各レポートでカスタマイズ可能なパラメーター（最終アクセス日からの日数や、大きなファイルのサイズなど）を変更できます。

スケジュールタスクで生成されたレポートは、既定で C:¥Storage¥Reports¥Scheduled ディレクトリに DHTML 形式で格納されます。



［操作］ペインの［レポートを今すぐ生成する］をクリックすると、指定したレポートを即時に生成させ、表示させることができます。この方法で生成したレポートは、C:¥Storage¥Reports¥Interactive ディレクトリに格納されます。

付録　外部メールサービスを利用したメール通知の実現

ファイルサーバーリソースマネージャーが備える電子メール通知機能は、SMTP ポート 25、匿名アクセスが可能な、セキュアではない転送用の SMTP メールサーバーを必要とします。メールシステムに高いセキュリティが求められる現代、そのようなメールサーバーの存在や設置はセキュリティ上のリスクになるため、ファイルサーバーリソースマネージャーの電子メール通知機能のためにそのような環境を用意するのは推奨される方法ではありません。

代替策として、Windows PowerShell の Send-MailMessage コマンドレットを利用した方法を紹介します。Send-MailMessage コマンドレットは、現代のセキュアなメールシステム環境に対応できるオプション（ポート番号の設定、SMTP 認証、TLS/StartTLS の対応など）をサポートしています。オプションの詳細については、以下の公式ドキュメントを参照してください。

Send-MailMessage
https://docs.microsoft.com/ja-jp/powershell/module/Microsoft.PowerShell.Utility/Send-MailMessage

例えば、Microsoft アカウント（Outlook.com）や Office 365 のメールアカウントを利用できる場合は、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やファイルスクリーンの管理、ファイル管理タスクが備えるコマンド実行機能で Send-MailMessage のコマンドラインを実行することで、特定のメールアドレス（管理者のメールアドレス）に固定メッセージを送信することが可能です。具体的には、該当する設定の［コマンド］タブで次のように設定します。

コマンドまたはスクリプトの実行：

C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe

コマンド引数：

-Command "& {$mailuser = メールアカウント名; $mailpass = ConvertTo-SecureString メールアカウントのパスワード -asplaintext -force; $mailcred = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $mailuser, $mailpass; Send-MailMessage -From メールアカウントのメールアドレス -To 通知先のメールアドレス -Subject 件名 -Body メッセージ本文 -Encoding ([System.Text.Encoding]::UTF8) -SmtpServer smtp.office365.com -Port 587 -Credential $mailcred -UseSSL}"

Outlook.com および Office 365 のメール送信設定は共通であり、SMTP サーバー「smtp.office365.com」、SMTP ポート「587」、TLS/StartTLS「有効」、およびメールボックスの資格情報を指定することで、任意の宛先にメール送信が可能です。これらの設定は、Send-MailMessage コマンドレットの-Port、-SmtpServer、-UseSSL でそれぞれ対応することができます。その他の外部メールサービスにも応用できる場合があります。