

SuitePRO V4 Windows Server® 2016 (ファイルサーバー初期設定済み) 手順書

株式会社 NTTPC コミュニケーションズ

作成日:2017年 6月 28日

更新日: 2018年 3月19日

**WebARENA® SuitePRO V4

目次

1. はじめに	3
▶ ファイルサーバーのインストール	
2. OS のインストール	5
3. 共有フォルダーヘアクセス	
→ ファイルサーバーの設定変更	
4. パスワード変更・ユーザー追加	12
5. シャドウコピーの確認・変更・削除	16
6. シャドウコピーの復元	18
7. ディスククォータの変更・削除	
8. ファイルアクセス監査の削除	
9. SMB 暗号化の解除	
y. SMD 旧与160/27中水	23

1. はじめに

本手順書は、Windows Server 2016(ファイルサーバー初期設定済み)のインストール方法と、OS インストール後の設定について解説しています。

設定項目

OS		
サーバーOS	Windows Server® 2016	Windows Server のファイルサーバー機能を
(本手順こてインストール)	Datacenter	インストール (OS インストールは手順 P.5 参照)
		▶役割
		・ファイルサーバー
		・ファイルサーバーVSS エージェントサービス
		・ファイルサーバーリソースマネージャー
		▶ ツール
		・ファイルサーバーリソースマネージャーツール
クライアント OS	Windows® 8以上	SMB 暗号化を利用しているため左記バージョン
(お客さま端末)	Windows Server® 2012以上	以上 (SMB 暗号化の無効化は手順 P.23 参照)
 オプション		
		OS インストール時(ごらかディスクを作成し、スロット(ご割り
追加ディスク	八九 沙貝	当てます(手順 P.8 参照)
		指定したアドレスのみダイレクト・ホスティング SMB
ファイアンオール	州人1世光	
		(445/tcp) を許可 (手順 P.7 参照)
バックアップ	購入推奨	1日1回、別ストレージにバックアップ

Windows Server 2016(ファイルサーバー初期設定済み)ユーザー・アクセス先				
Windows 管理者	Administrator	パスワードは初回ログイン時にお客さまにて設定		
ファイルサーバー用① ファイルの作成・変更・削除が可能	user[NIC1の第4オクテット※] (例)user29	パスワードは PROV4 コントロールパネルと同じ (パスワード変更は P.12 参照)		
ファイルサーバー用② ファイル参照のみ	user-ro[NIC1の第4オケテット※] (例)user-ro29	パスワードは PROV4 コントロールパネルと同じ (パスワード変更は P.12 参照)		
共有フォルダー	D ドライブ内の Share[NIC1 の第4 オクテット※]\$ (例) D:\Share29\$	隠し共有のため、最後に\$を追加する		
サーバーアドレス	¥¥PROV4 サーバーIP アドレス¥share [NIC1の第4オクテット※]\$ (例)¥¥203.0.113.29¥share29\$	PROV4 サーバーIP アドレスは下記 VPN オブションをご契約中の場合: NIC3 UTM オプションをご契約中の場合: NIC4 それ以外のお客さま: NIC1 (共有フォルダーへのアクセスは P.10 参照)		

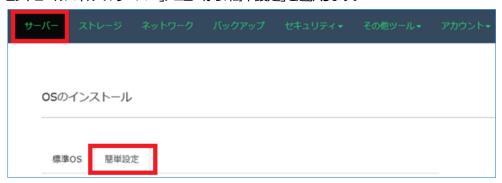
※NIC1 の第4 オクテット・・・ドットで区切られている IP アドレスの 4 番目の数字 (例) NIC1 の IP アドレスが 203.0.113.29 の場合は 29

	サーバー初期設定済み)	
アクセス許可設定に基づいた列挙	有効	アクセス権のないファイルを表示しない
共有のキャッシュ	有効	
キャッシュデータを他の端末でも利用する	無効	
シャドウコピー	有効	ファイル単位のスナップショット
		·1日1回取得
		・シャドウコピーの保存領域が D ドライブのディス
		ク容量の 10%を超えた場合、もしくは保存数
		が 64 世代を超えた場合は古い世代から削除
		される
		※2017年7月26日以前にOSをインストール
		した場合はシャドウコピーが無効となっているため
		設定することを推奨
		(シャドウコピー設定は手順 P.16 参照)
ディスククォータ	有効	D ドライブの 85%に使用を制限
		※シャドウコピー等 Windows で利用する容量を考慮
		(無効化、サイズ変更は手順 P.20 参照)
レポート機能	無効	
ファイルアクセス監査	有効	ユーザーの読み取り・書き込み処理を口グに記録
		(無効化は手順 P.21 参照)
Windows ファイアウォール	有効	ダイレクト・ホスティング SMB(445/tcp)を許可
SMB1.0/CIFS	無効	セキュリティ上無効にすることを推奨するが、
		運用上有効化したい場合は以下の手順を実施
		https://web.arena.ne.jp/support/suiteprov4/
		manual/smb1_cifs.html
SMB 暗号化	有効	SMB データのエンド ツー エンドの暗号化を提供
		(無効化は手順 P.23 参照)

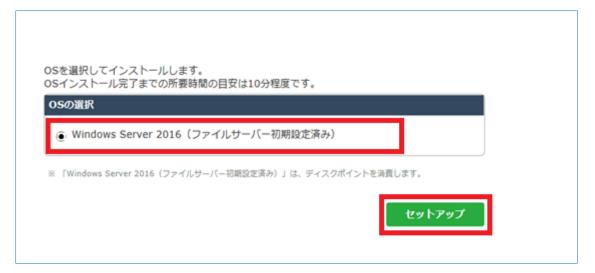
2. OS のインストール

SuitePRO V4のコントロールパネル(https://pro4.arena.ne.jp)にログインし、OSをインストールします。

1. コントロールパネルの「サーバー」メニューから「簡単設定」を選択します。



2. 「Windows Server 2016 ファイルサーバー(ファイルサーバー初期設定済み)」を選択し、「セットアップ」をクリックします。

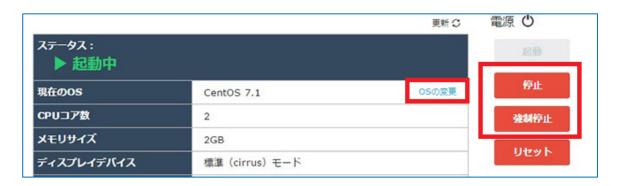


OS インストール済みの場合

「OSの変更」から、「簡単設定」にアクセス可能です。

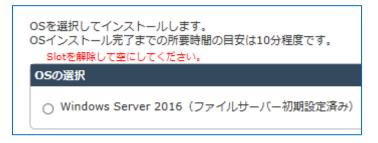
サーバーが起動している場合は、先に「電源:停止/強制停止」からサーバーを停止しておいてください。

※OS を変更することで、すべてのデータが初期化されます。作業前にあらかじめデータのバックアップをしてください。



「Slot を解除して空にしてください。」と表示された場合

ストレージから各 slot のディスクをすべて解除し、OS インストールを再実行してください。



コントロールパネルの「ストレージ」メニューから「ストレージ」を選択します。



設定されているすべてのディスクを「解除」します。



****WebARENA*** SuitePRO V4

3. OS インストールが始まります。 所要時間は 10 分程度です。



- 4. 続いてファイアウォールポリシーを設定します。 (NIC3 は VPN ご契約の場合のみ表示されます。) ファイルサーバーへのアクセスを許可したい IP アドレスを入力し、「設定」をクリックします。
 - ※ 既にファイアウォールを設定していた場合でも、本設定を行うことで全て初期化されます。 (ファイアウォールエントリーのご契約がない場合、この画面はスキップされます。

また、現在のファイアウォールポリシーに「445/tcp」の通信許可設定が既にある場合も同様にスキップされます。)



ファイアウォールの設定は後でも変更できます。

https://web.arena.ne.jp/support/suiteprov4/manual/fw_entry_settings.html

***WebARENA** SuitePRO V4

5. 次にディスクを作成します。

ディスクプランを選択し、「作成」をクリックします。ディスクの作成が完了すると、自動的に次の画面に進みます。 (ディスクが既に作成されている場合、この画面はスキップされます。)



6. ディスクを slot1 に割り当てます。ディスクを選択し、「設定」をクリックします。
ここで割り当てたディスクは初期化され、データは全て消去されます。
別のディスクを使用したい場合は、右上の「ディスク新規作成」から、新しいディスクを作成してください。



**WebARENA* SuitePRO V4

7. 設定がおわると、サーバーを起動する画面が表示されるので「起動」をクリックします。



8. サーバーが起動したら「コンソールを開く」をクリックします。 別画面でコンソールが開くので、Administratorのパスワードを設定してください。



パスワード設定後、画面に何も表示されない状態が数分続きます。Windows 設定処理を行っていますので、電源を切らずにしばらくお待ちください。(処理中にサーバーを停止した場合、再度 OS をインストールし直す必要があります。) 以上で OS のインストールは完了です。

3. 共有フォルダーヘアクセス

クライアント端末から、共有フォルダーにアクセスします。

Windows® 8以上、Windows Server® 2012以上の端末を準備してください。MAC の場合は MAC OS X v10.10以上となります。

※SMB 暗号化を利用しているため上記バージョン以上が必要となります。(SMB 暗号化の無効化は本手順 P.23 参照)

Windows の場合

1. エクスプローラーや、ブラウザ等で下記のようにファイルサーバーのアドレスを入力し、Enterを押します。 隠し共有のため、最後に\$を追加する必要があります。



2. ユーザー名、PROV4コントロールパネルのパスワードを入力し、ログインできることを確認してください。

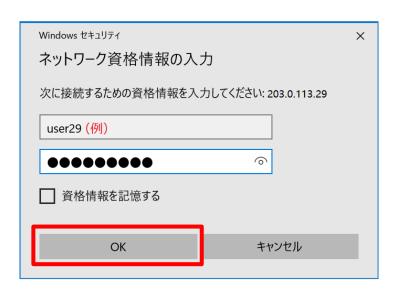
user【NIC1 の第4オクテット※】

ファイルの作成・変更・削除が可能

user-ro【NIC1 の第4オクテット※】

ファイルの参照のみ

※NIC1 の第4オクテット・・・ドットで区切られている IPアドレスの4番目の数字 NIC1のIPアドレスが203.0.113.29の場合は29

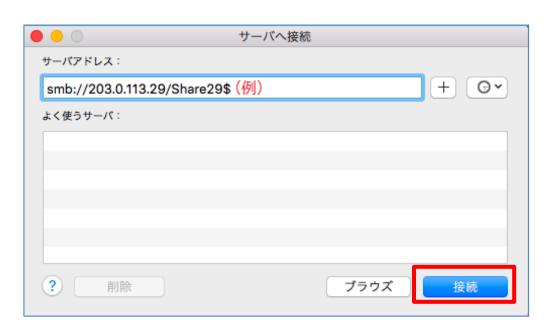


以上でファイルサーバーとして使用できるようになりました。 次のページを参考に、パスワードの変更をしてください。



MACの場合

1. 「Finder」を起動し、メニューの「移動」から「サーバーへ接続」を選択します。
下記のように smb://のあとにファイルサーバーのアドレスを入力し「接続」をグリックします。隠し共有のため、最後に\$を追加する必要があります。



2. ユーザー名、PROV4 コントロールパネルのパスワードを入力し、ログインできることを確認してください。

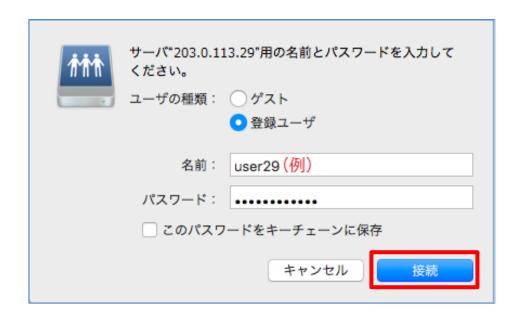
user【NIC1 の第4オクテット※】

ファイルの作成・変更・削除が可能

user-ro【NIC1 の第4オクテット※】

ファイルの参照のみ

※NIC1 の第4 オクテット・・・ドットで区切られている IP アドレスの 4番目の数字 NIC1 の IP アドレスが 203.0.113.29 の場合は 29

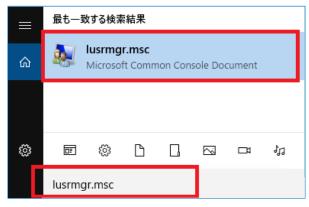


以上でファイルサーバーとして使用できるようになりました。 次の章を参考に、パスワードの変更をしてください。

4. パスワード変更・ユーザー追加

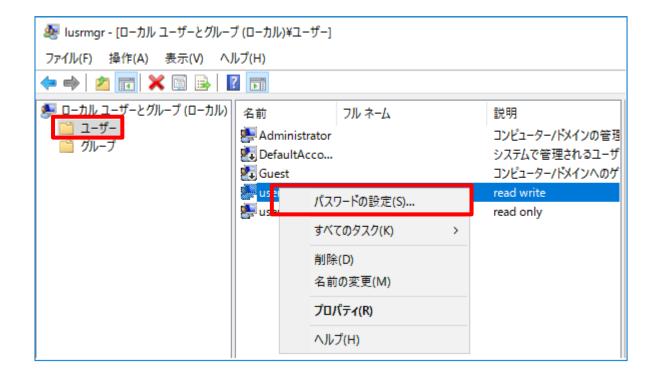
ローカル ユーザーとグループ (ローカル)を起動します。検索ボックスに「lusrmgr.msc」と入力してください。





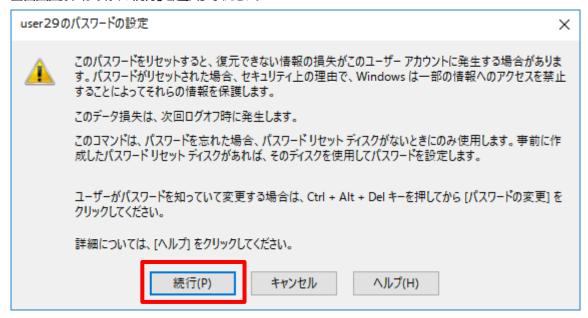
パスワード変更

1. ローカル ユーザーとグループ (ローカル)からファイルサーバー用ユーザーの初期パスワードを変更します。「ユーザー」から、パスワードを変更したいユーザーを選択し、右クリックして「パスワードの設定」を選択してください。

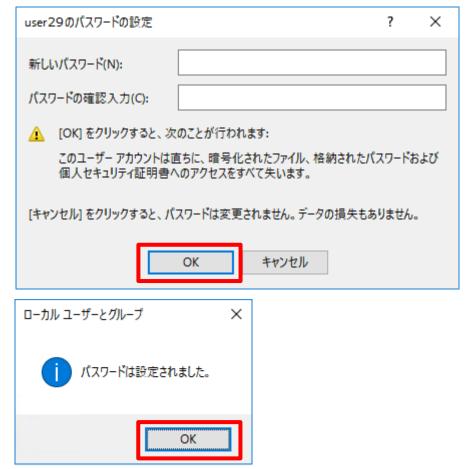


***WebARENA** SuitePRO V4

2. 警告画面が出ますが、「続行」を選択してください。



3. パスワードを二回入力します。



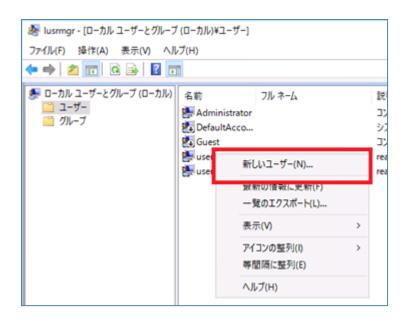
以上でパスワードの変更は完了です。再度ログインできることを確認してください。 有効期限は、Windows サーバーのデフォルト値の 42 日ですので、定期的にパスワードを変更してください。 また、必要に応じて有効期限の変更を行ってください。

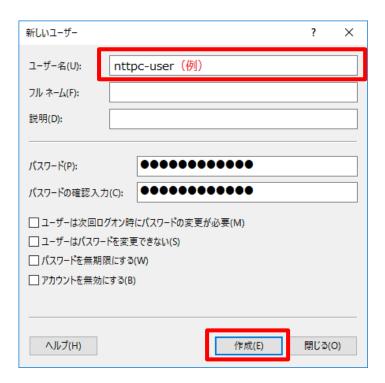




ユーザー追加

1. 新しいユーザーを作成する場合は、ローカル ユーザーとグループ (ローカル)の右画面にて右クリックをし「新しいユーザー」を選択します。既存ユーザーを選択せずに、何もないところで右クリックしてください。







**WebARENA® SuitePRO V4

2. 続いて作成したユーザーのアクセス権を設定します。パワーシェル(管理者権限で起動)にて下記のようにコマンドを入力してください。

ファイルの作成・変更・削除を許可する場合

下記の例ではユーザー「nttpc-user」に「D:\Share29」以下のフォルダーに権限を付与しています。

> icacls D:\forall Share29\forall /grant:r "nttpc-user:(OI)(CI)(M)" /T

ファイルの参照を許可する場合

下記の例ではユーザー「nttpc-user」に「D:\Share29」以下のフォルダーに権限を付与しています。

> icacls D:\forall Share29\forall /grant:r "nttpc-user:(OI)(CI)(R)" /T

以上でアクセス権の設定は完了です。

アクセス権限は、icalcsコマンドで確認できます。

権限:R=読み取り専用/M=編集権限/F=フルコントロール

> icacls D:\Share29\\$

D:\forall Share 29\forall WIN-IJM5SJ35KAH \entropy \text{inttpc-user:(OI)(CI)(R)}

WIN-IJM5SJ35KAH¥user29:(OI)(CI)(**M**)

WIN-IJM5SJ35KAH¥user-ro29:(OI)(CI)(R)

略



5. シャドウコピーの確認・変更・削除

シャドウコピー機能を利用することで、削除してしまったファイルを復活させるなど、ファイルの自動バックアップが可能となります。 シャドウコピーは初期状態で1日1回取得します。

※2017年7月26日以前にOSをインストールした場合はシャドウコピーが無効となっているため、下記手順を参考に有効にすることを推奨します。

シャドウコピーのスケジュールを確認

下記の例では、AM2:44 にシャドウコピーが実行されます。

> Get-ScheduledTask -TaskName ShadowCopy | Get-ScheduledTaskInfo | where {\$_.nextruntime}
-ne \$null} | select taskpath,taskname,nextruntime

taskpath taskname nextruntime

YMSFT_TaskDailyTrigger¥ ShadowCopy 2017/07/26 2:44:44

上記でシャドウコピーのスケジュール設定がない場合は、以降の手順で設定することが可能です。

シャドウコピー設定

シャドウコピーの設定をする場合は、パワーシェル(管理者権限で起動)にて下記のようにコマンドを入力してください。本手順では、Dドライブの 10%で設定しています。

- > \$ShadowSize=[math]::round((gwmi Win32_LogicalDisk | ? {\$_.DeviceID -eq "D:"}).Size * 0.1,0)
- > vssadmin add shadowstorage /for=D: /on=D: /maxsize=\$ShadowSize

vssadmin 1.1 - ボリューム シャドウ コピー サービス管理コマンド ライン ツール

(C) Copyright 2001-2013 Microsoft Corp.

シャドウ コピーの記憶域製連付けが正しく追加されました

容量を変更するには下記のコマンドを実施 (例) 1GB に変更

vssadmin resize shadowstorage /for=D: /on=D: /maxsize=1GB

シャドウコピー取得

シャドウコピーを取得する場合は、パワーシェル(管理者権限で起動)にて下記のようにコマンドを入力してください。



シャドウコピーのスケジュール設定

シャドウコピーのスケジュールを設定する場合は、パワーシェル(管理者権限で起動)にて下記のようにコマンドを入力してください。 下記の例では毎日午前2時に設定しています。

- > \$Action=new-scheduledtaskaction -execute "c:\five windows\for=D:"
- > \$trigger=New-ScheduledTaskTrigger -daily -At 2AM
- > Register-ScheduledTask -TaskName ShadowCopy -Trigger \$trigger -Action \$Action \$trigger -Description "ShadowCopy" -Force

シャドウコピーのスケジュール停止

シャドウコピーのスケジュールを停止する場合は、パワーシェル(管理者権限で起動)にて下記のようにコマンドを入力してください。

> schtasks / Delete /TN YMSFT_TaskDailyTriggerYShadowCopy /F

成功: スケジュール タスク "¥MSFT_TaskDailyTrigger¥ShadowCopy" は正しく削除されました。

取得したシャドウコピーの削除

シャドウコピーを削除する場合は、パワーシェル(管理者権限で起動)にて下記のようにコマンドを入力してください。

> vssadmin Delete Shadows /For=D:

vssadmin 1.1 - ボリューム シャドウ コピー サービス管理コマンド ライン ツール

(C) Copyright 2001-2013 Microsoft Corp.

2 個のシャドウ コピーを削除しますか (Y/N): [N]? Y

2 個のシャドウ コピーが正しく削除されました。

対話形式にしない場合は、/Quiet を付け加えて実行します。 vssadmin Delete Shadows /For=D: /Quiet

シャドウコピー設定の削除

シャドウコピーの設定を削除する場合は、パワーシェル(管理者権限で起動)にて下記のようにコマンドを入力してください。 ※シャドウコピー設定の削除をする前に、これまで取得したシャドウコピーを削除する必要があります。

> vssadmin Delete ShadowStorage /for=D: /on=D:

vssadmin 1.1 - ボリューム シャドウ コピー サービス管理コマンド ライン ツール

(C) Copyright 2001-2013 Microsoft Corp.

シャドウ コピーの記憶或料連付けが正しく削除されました

「エラー: オプションの値が無効です。」と表示された場合は、取得したシャドウコピーが残っている可能性があります。 先に「vssadmin Delete Shadows /For=D:」にて削除を実行してください。





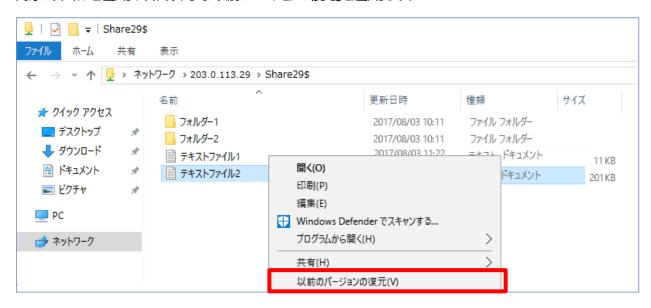
※この手順は、必要に応じて変更してください。

6. シャドウコピーの復元

シャドウコピー機能を利用している場合、上書き/削除してしまったファイルやフォルダーを元に戻すことができます。

ファイルのコピー・復元

1. 対象のファイルを選択し、右クリックして「以前のバージョンの復元」を選択します。



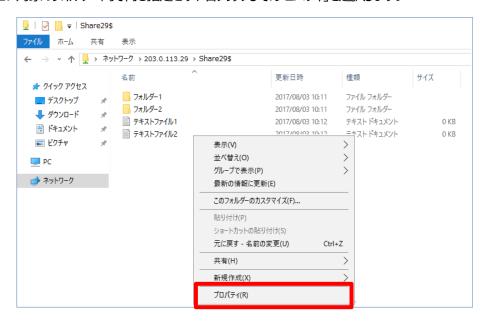
2. シャドウコピー一覧が表示されますので、対象のバージョンを選択し、「開く」をクリックしてください。ファイルを開いたら、「名前を付けて保存」を選択し、別名で保存してください。



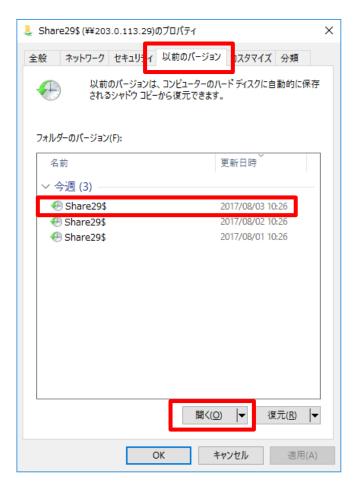
※「開く」と「復元」の違い 「復元」を選択すると、ファイルが以前 のバージョンに上書きされますのでご注 意ください。

フォルダーのコピー・復元

1. 対象のフォルダー内で何も指定せず、右クリックして「プロパティ」を選択します。



2. 「以前のバージョン」タブをクリックするとシャドウコピー一覧が表示されます。対象のバージョンを選択し、「開く」をクリックしてください。以前のバージョンのフォルダーが開くので、復元したいファイルをコピーして、別の場所に保存してください。



※「開く」と「復元」の違い 「復元」を選択すると、フォルダー内の すべてのファイルが以前のバージョンに 上書きされますのでご注意ください。 ※この手順は、必要に応じて変更してください。

7. ディスククォータの変更・削除

初期設定ではディスククォータを D ドライブの 85%で設定しています。(シャドウコピー等、Windows で利用する容量を考慮しています。)

サイズ変更

サイズを変更する場合は、パワーシェル(管理者権限で起動)にて下記のようにコマンドを入力してください。

例: 100GB に変更する場合

※NIC1 の第4 オクテット・・・ドットで区切られている IP アドレスの 4 番目の数字 NIC1 の IP アドレスが 203.0.113.29 の場合は 29

> Set-FsrmQuota -Path d:\#Share[NICの第4オクテット※]\$ -Size 100GB

> Get-FsrmQuota | select size

size

107374182400

削除

制限を削除する場合は、パワーシェル(管理者権限で起動)にて下記のようにコマンドを入力してください。

※NIC1 の第4オクテット・・・ドットで区切られている IP アドレスの4番目の数字 NIC1 の IP アドレスが203.0.113.29 の場合は29

> Remove-FsrmQuota -Path d:\frac{NICの第4オクテット※}\$

確認

この操作を実行しますか?

操作: 削除、オブジェクト: クォータ、オブジェクト識別子 (Path): d:\Share161\$

[Y] はい(Y) [A] すべて続行(A) [N] いいえ(N) [L] すべて無視(L) [S] 中断(S) [?] へルプ (既定値は "Y"): Y

NTTPCCOMMUNICATIONS

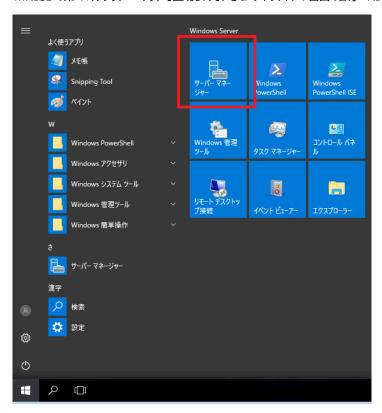


※この手順は、必要に応じて変更してください。

8. ファイルアクセス監査の削除

初期設定では、ファイルアクセス監査が有効になっています。この設定により、ユーザーの読み取り・書き込み処理をログに記録しています。ファイルアクセス監査を有効にしておくことを推奨しますが、停止する場合は下記手順を実施してください。

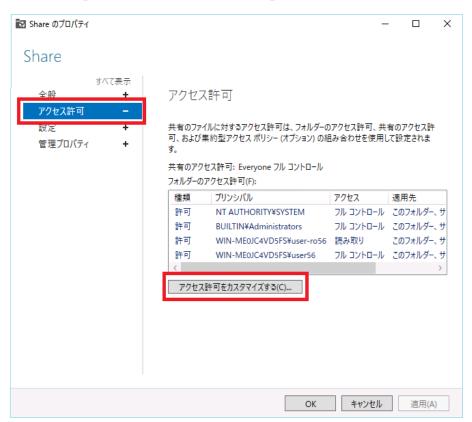
1. サーバーマネージャーを起動し「共有」から Share 【NIC1 の第4オクテット※】 \$を選択し、右クリックしてプロパティを開きます。 ※NIC1 の第4オクテット・・・ドットで区切られている IP アドレスの4番目の数字 NIC1 の IP アドレスが 203.0.113.29 の場合は 29





**WebARENA® SuitePRO V4

2. 「アクセス許可」から「アクセス許可をカスタマイズする」をクリックします。



3. 「監査」タブを開き、現状の設定を選択し、「削除」をクリックします。削除したら「OK」をクリックします。



以上でファイルアクセス監査の設定が削除されました。





※この手順は、必要に応じて変更してください。

9. SMB 暗号化の解除

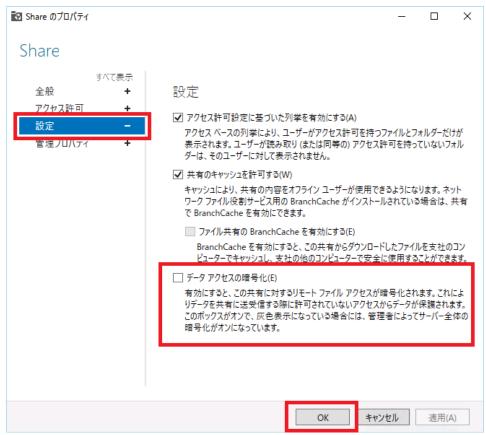
SMB 暗号化は、SMB データのエンド ツー エンドの暗号化を提供するため、本機能を有効にした状態でのご利用を推奨します。Windows® 8、Windows Server® 2012以上の OS をクライアントとしてご利用ください。
Windows® 7 等、SMB 暗号化に対応していない OS は、SMB 暗号化を解除することでご利用いただけますが、ファイル

Windows® 7 等、SMB 暗号化に対応していない OS は、SMB 暗号化を解除することでご利用いただけますが、ファイル 転送時の暗号化が無効になりますので、解除する場合はお客さまの判断と責任において実施してください。

1. サーバーマネージャーを起動し「共有」から Share 【NIC1 の第4オクテット※】 \$を選択し、右クリックしてプロパティを開きます。 ※NIC1 の第4オクテット・・・ドットで区切られている IP アドレスの4番目の数字 NIC1 の IP アドレスが 203.0.113.29 の場合は 29



2. 「設定 |を開き、「データアクセスの暗号化 |のチェックを外し、「OK |をクリックします。



以上で SMB 暗号化が解除されました。

