ホワイトペーパーシリーズ：

BitLocker によるデータドライブの暗号化手順

2014 年 5 月

内容

1 はじめに

この手順書では、Windows Storage Server 2012 以降で搭載された『記憶域プール（Storage Spaces）』機能を利用して作成されたデータドライブを、Windows 標準機能の『BitLocker』を利用して丸ごと暗号化する手順についてご紹介します。

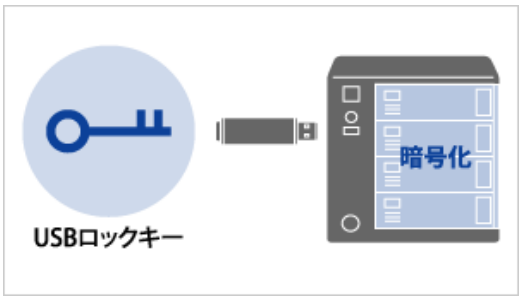
ボリュームを暗号化することにより、万一装置が盗難に遭った場合や、ハードディスクが持ち出された場合でも、鍵情報がなければ全く中身を見られる心配がありません。USB メモリに鍵情報を書き出すことで運用も容易に行えるようになりますので、不特定多数の方が出入りされるような環境や重要な機密情報を保管している場合などにおいて情報漏えいのリスクを軽減することができます。起動時に解除作業を行う以外、通常の操作と変更はありませんので、ご検討ください。

2 暗号化の要望

弊社ではこれまで NAS の暗号化として LAN DISK XR で暗号化ボリューム機能を提供していました。サテライトオフィス（例えば工事現場、仮設事務所等）や公共施設での NAS を利用される際などにご利用いただいています。

今回のホワイトペーパでは、Windows Storage Server 搭載の LAN DISK Z シリーズで利用できる BitLocker を利用した暗号化の手順をご紹介致します。

高速なパフォーマンスをもつ LAN DISK Z での暗号化を利用することにより様々なシーンで、本製品をご利用いただければ幸いです。



※ LAN DISK XR に搭載されている暗号化ボリューム機能

3 実施環境

3.1. 確認 OS

Windows Storage Server 2012 R2 Workgroup / Standard Edition
Windows Storage Server 2012 Workgroup / Standard Edition

3.2. 対応機種

Windows Storage Server 2012 R2 シリーズ

- ✧ HDL-Z2WMC2 シリーズ
- ✧ HDL-Z4WMC2 シリーズ
- ✧ HDL-Z6WLC2 / V シリーズ
- ✧ HDL-Z4WLCR2 / V シリーズ

LAN DISK Z

Windows Storage Server 2012 シリーズ

- ✧ HDL-Z4WMC シリーズ
- ✧ HDL-Z6WLC / V シリーズ

3.3. 必要なもの

BitLocker 暗号キー保存用 USB メモリ（最低 1 本）

3.4. ご注意

HDL-Z シリーズでボリューム丸ごと暗号化を行うためには、RAID モードではなく、マルチディスクモードに切り替える必要があります。その際に装置の設定情報・データは全て失われますので、あらかじめバックアップを取ったのちに初期化を実行してください。詳しい手順は装置同梱の管理者ガイドをご参照ください。

4 動作環境

HDL-Z シリーズは複数台のハードディスクで構成されており、出荷時には『RAID1』または『RAID5』で構成されています。これらの RAID モードは、ソフトウェア RAID と呼ばれ、Windows 標準機能を利用して実現しています。Windows 標準機能のソフトウェア RAID の場合、ハードディスクを『ダイナミックディスク』に変換したうえで構成します。

BitLockerでボリューム全体を暗号化する場合、ダイナミックディスクでは利用することができません。そのため、あらかじめ HDL-Z シリーズ添付のリカバリーディスクを使って、『マルチディスクモード』にて構成し、Windows Server 2012/R2 の『記憶域プール』を使って冗長構成を組んでおきます。『マルチディスクモード』ならびに『記憶域プール』の設定方法については、HDL-Z シリーズ添付の『管理者ガイド』をご参照ください。

これから BitLocker の設定方法について手順をご紹介しますが、以下の環境にて構成していますのでご参照ください。

商品型番：HDL-Z2WMC2 シリーズ

ドライブ

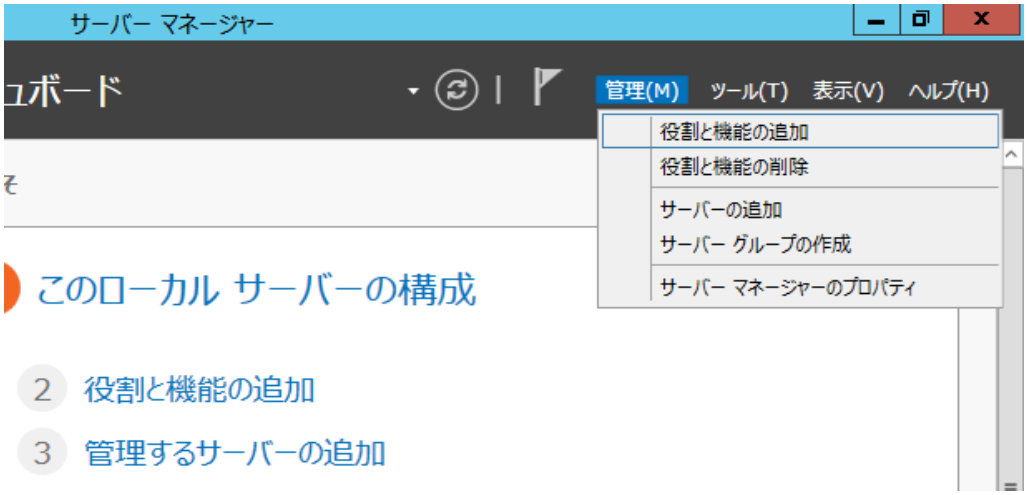
C: Windows OS インストール済
　記憶域プール：ドライブ C:以外の領域を全て記憶域プールに割り当て
D: 記憶域プール『Pool1』から切り出した 100GB/Simple 構成の仮想ディスク
E: 記憶域プール『Pool1』から切り出した 100GB/Simple 構成の仮想ディスク
F: USB フラッシュメモリ（鍵保存用）

5 事前準備

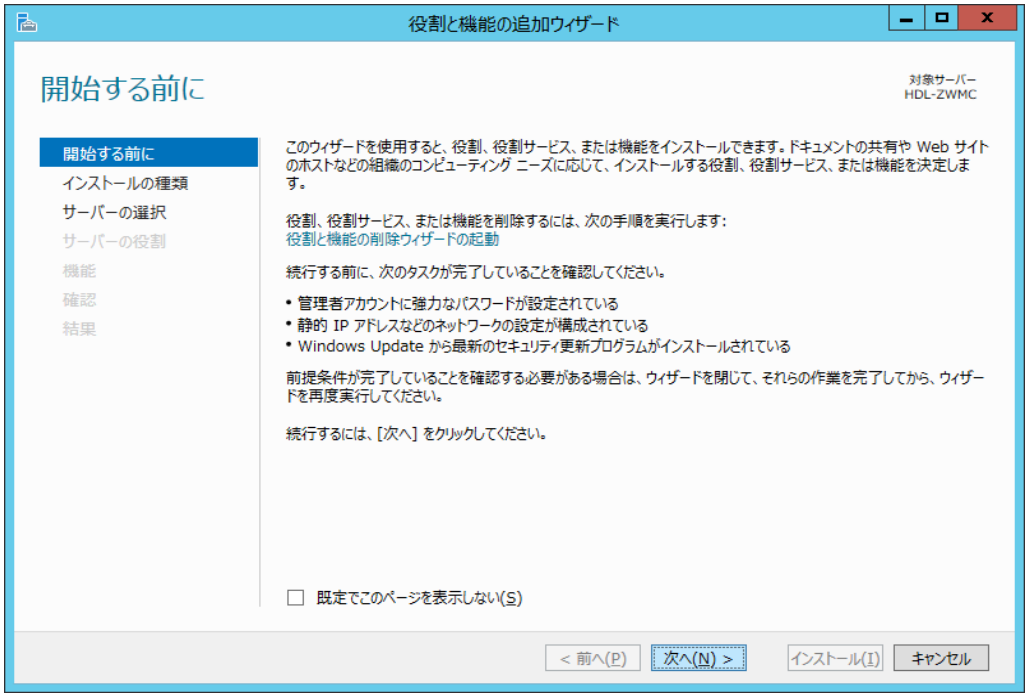
HDL-Z シリーズは出荷状態において BitLocker は組み込まれていません。ここでは HDL-Z シリーズに BitLocker を組み込む手順についてご紹介します。

（以下では Windows Storage Server 2012 R2 の設定画面を例に手順をご紹介しています。）

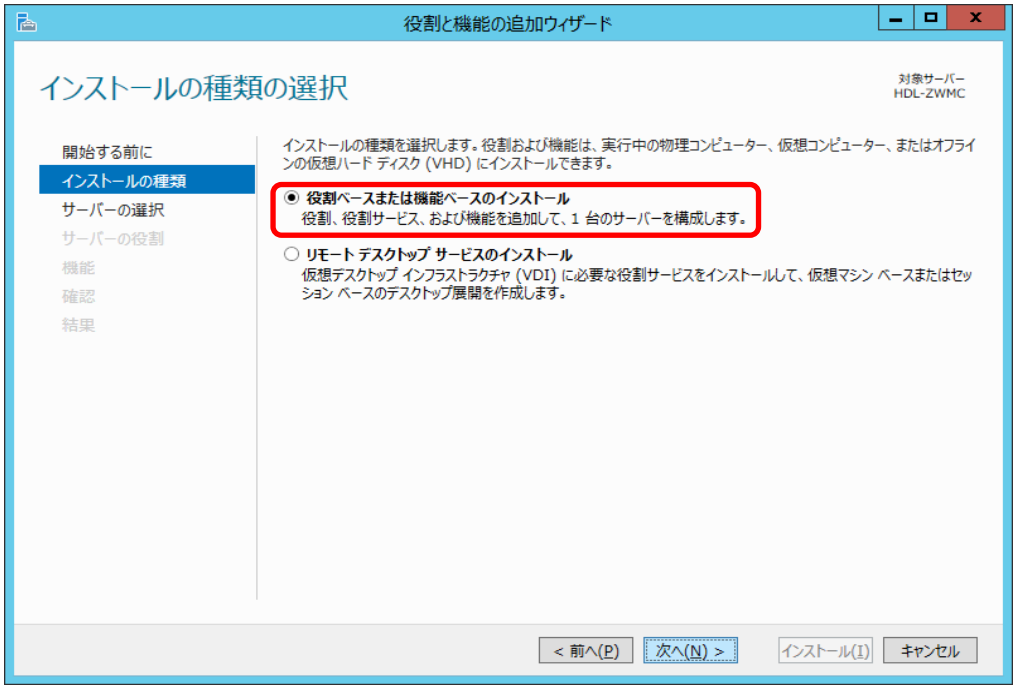
5.1 サーバーマネージャーから『管理』→『役割と機能の追加』をクリックします。



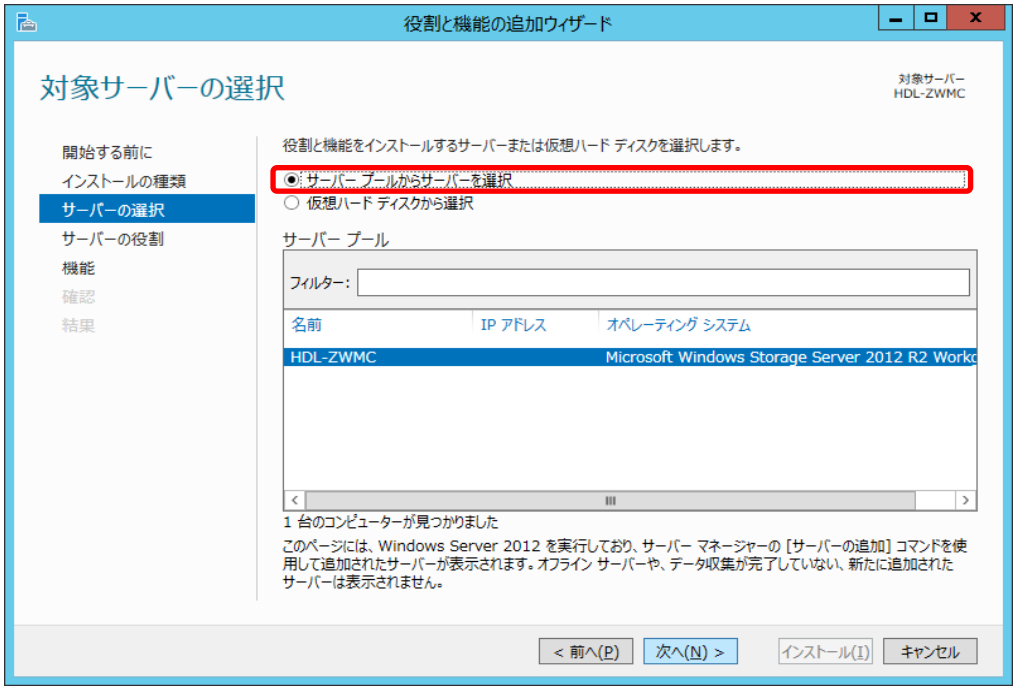
5.2 役割と機能の追加ウィザードが表示されますので、『次へ』をクリックします。



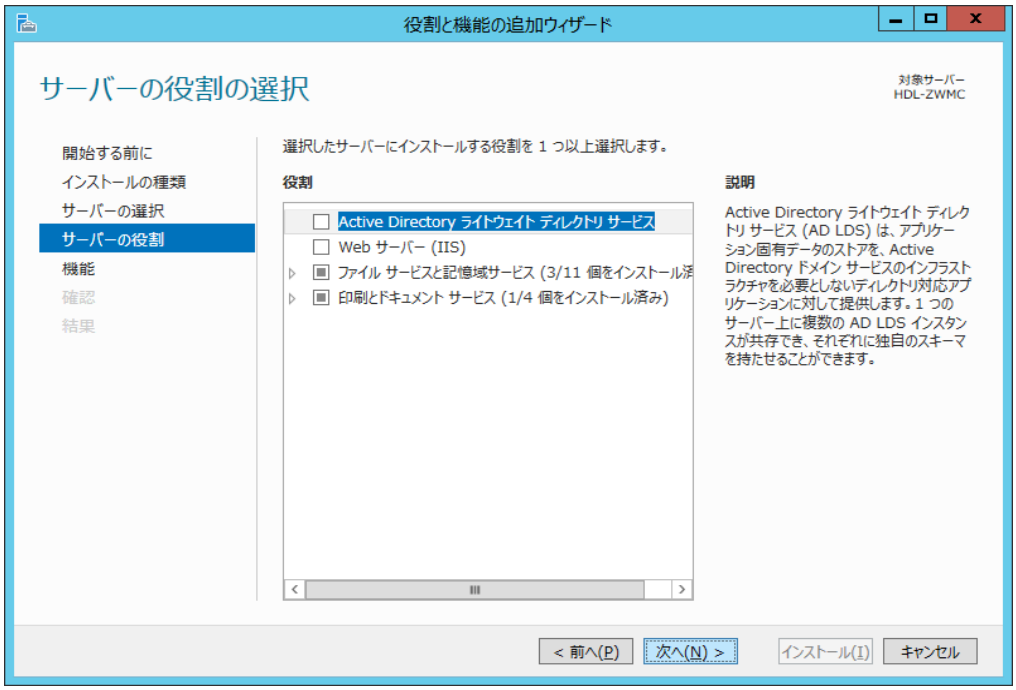
5.3 インストールの種類の選択では『役割ベースまたは機能ベースのインストール』にチェックして『次へ』をクリックします。



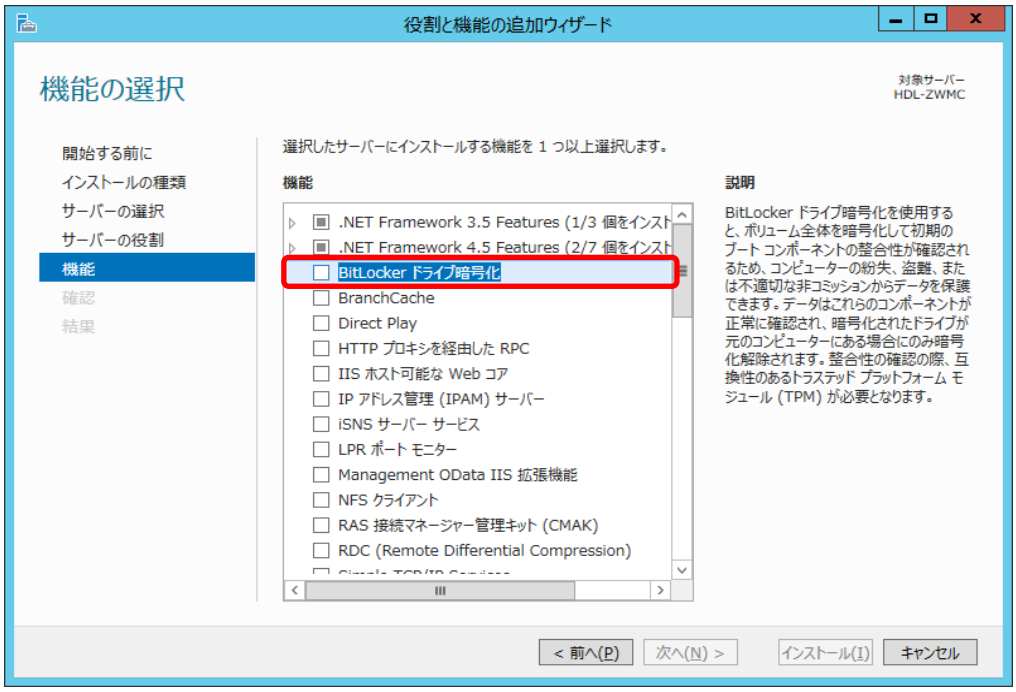
5.4『サーバープールからサーバーを選択』をチェックし、対象となる装置をサーバープールから選択して『次へ』をクリックします。



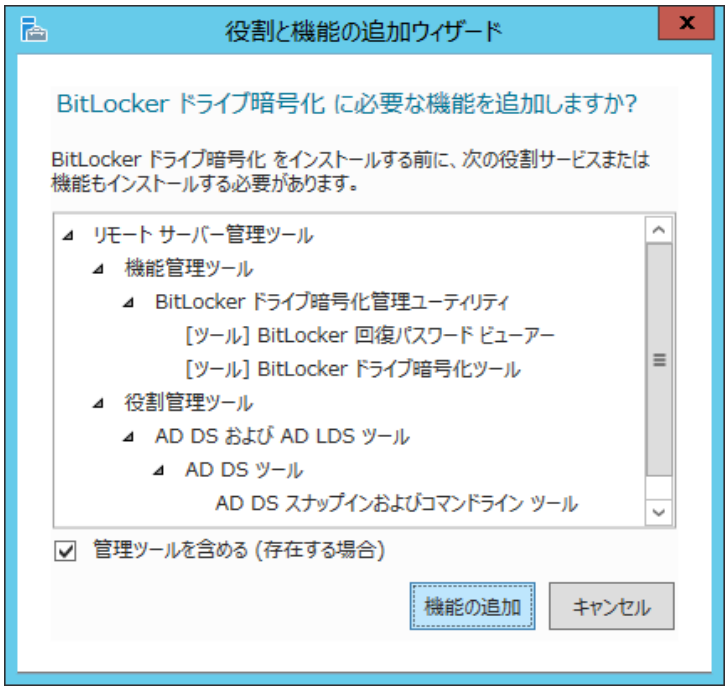
5.5 『役割』の画面ではそのまま『次へ』をクリックします。



5.6 『機能』の画面で『BitLocker ドライブ暗号化』をクリックします。

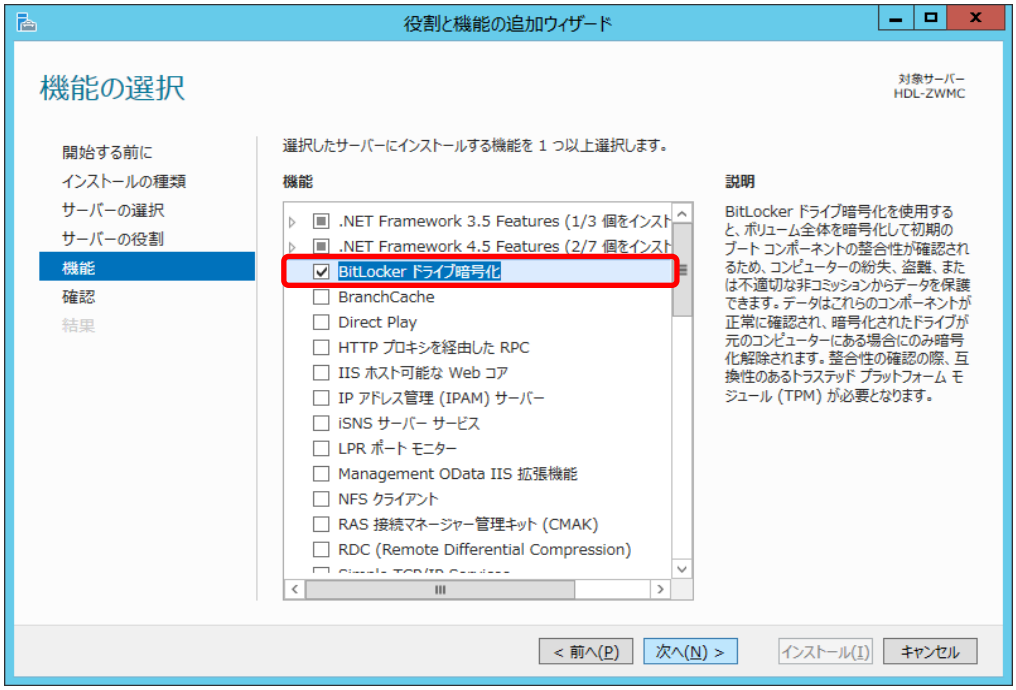


5.7 確認画面が表示されますので、『機能の追加』ボタンをクリックします。

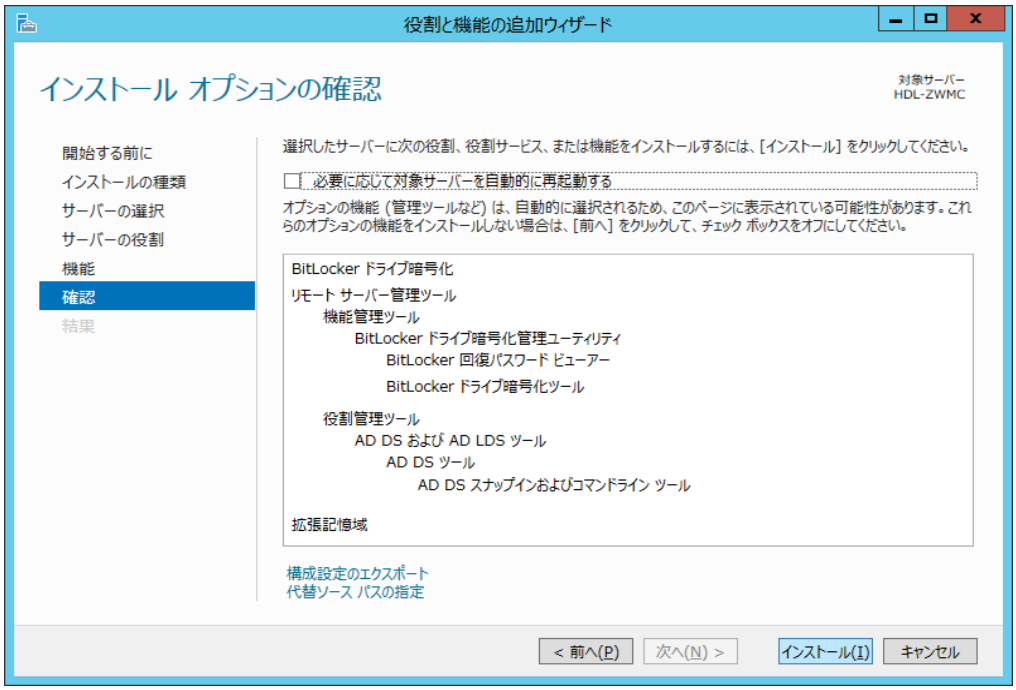


※ 役割管理ツールの『AD DS および AD LDS ツール』は関連する機能として自動的に追加されます。

5.8 『機能』画面に戻りますので、『BitLocker ドライブ暗号化』にチェックが付いているのを確認して、『次へ』をクリックします。



5.9 『インストール』ボタンをクリックすると、インストールが始まります。



インストール完了後、装置の再起動が要求されますので、再起動を行います。

以上で事前準備は完了です。

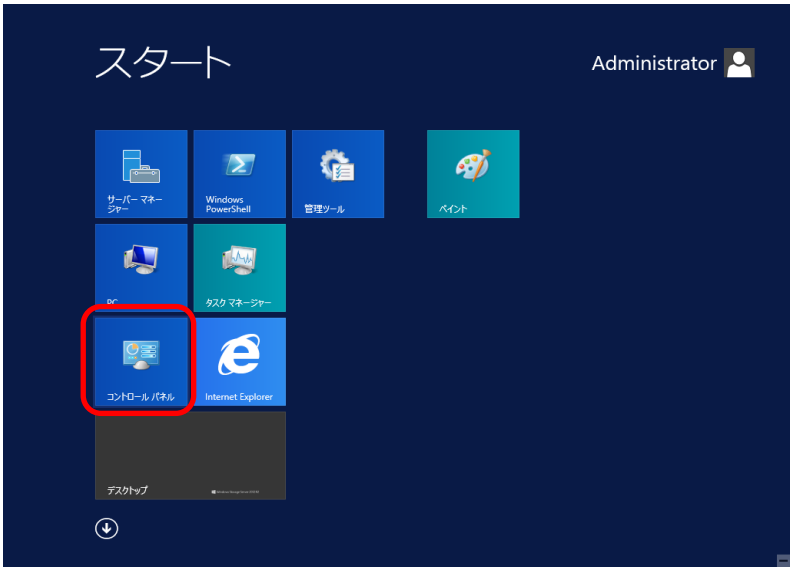
6 BitLocker の設定

それではデータドライブ D:を丸ごと暗号化します。

『記憶域プール』機能を利用して、データドライブを作成しておきます。

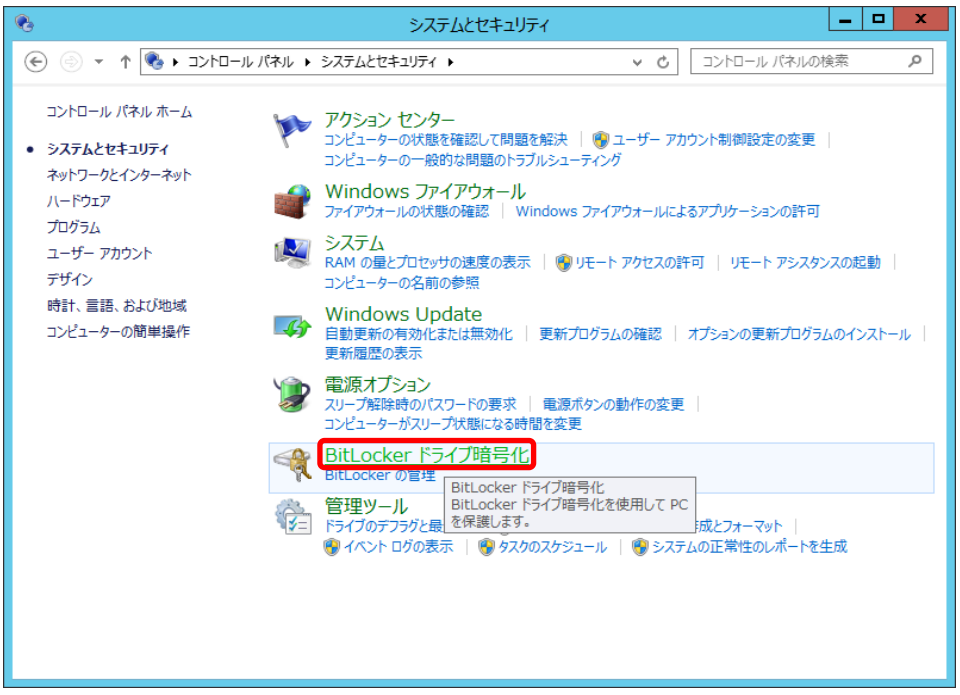
作成手順については装置同梱の『管理者ガイド』をご参照ください。

6.1 『Windows ボタン』を押し、『コントロールパネル』を開きます。



6.2 『コントロールパネル』から『システムとセキュリティ』をクリックします。

『BitLocker ドライブ暗号化』が表示されていればクリックして『6.4』へお進みください。



6.3 『Windows キー』と『Q』キーを押し、検索画面を開きます。

検索項目には『BitLocker』と入力してください。

しばらくすると検索結果が表示されますので、『BitLocker の管理』をクリックします。

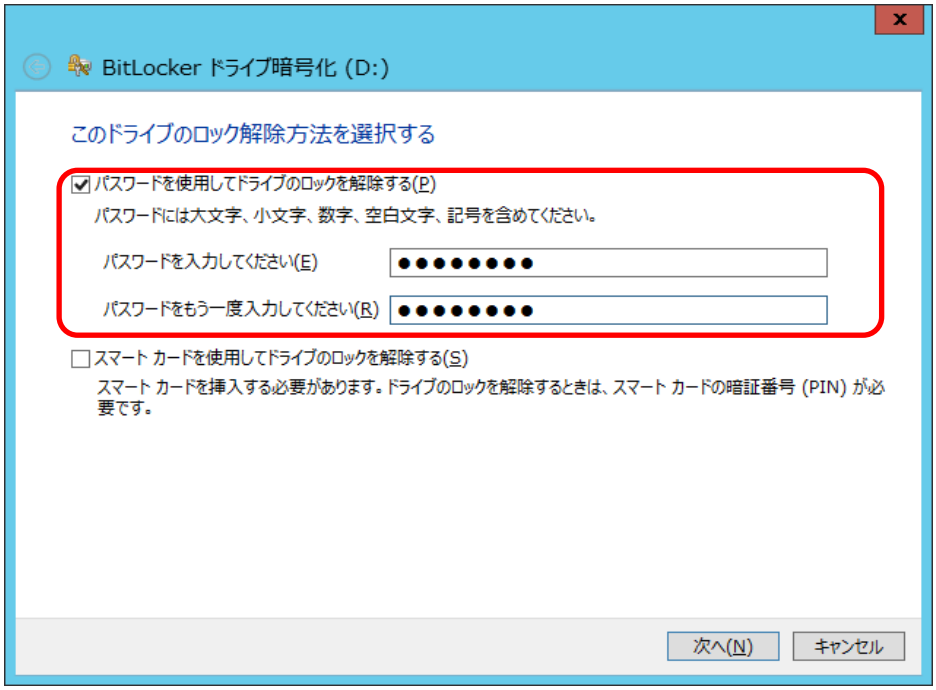
検索結果が表示されない場合は、正しく入力されているか確認して再度実行してください。
それでもうまく行かない場合は一度装置を再起動してお試しください。

6.4 暗号化するドライブ D:をクリックします。

続いて『BitLocker を有効にする』をクリックします。

6.5 BitLocker ドライブ暗号化設定画面が開きますので、『パスワードを使用してドライブのロックを解除する』をクリックし、パスワードを入力します。

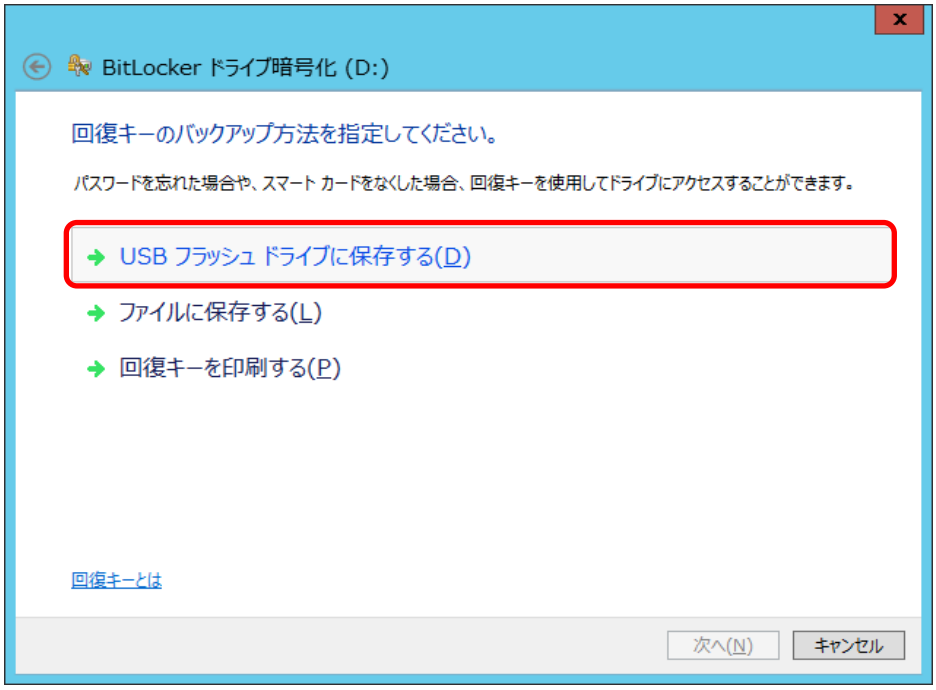
入力したら『次へ』をクリックします。



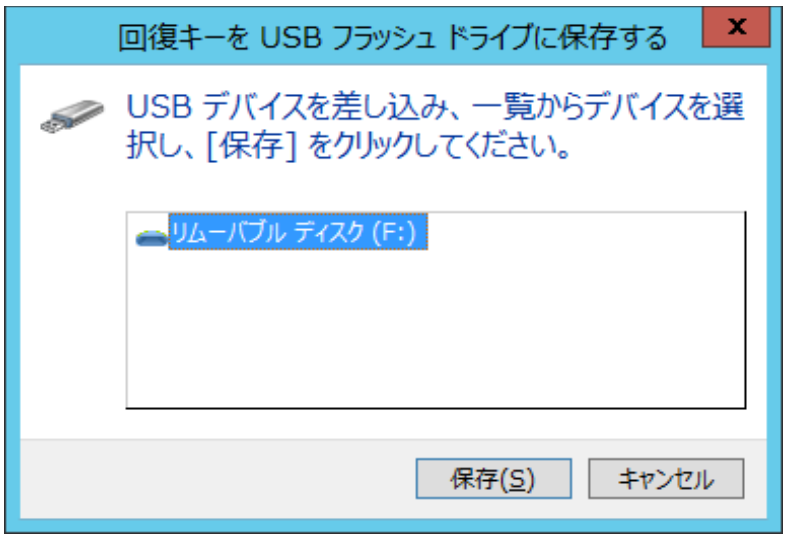
パスワードは複雑さの要件を満たすものである必要があります。8 文字以上にてアルファベット大文字・小文字、数字、記号を含んだパスワードを作成してください。

6.6 回復キーのバックアップ方法を指定します。

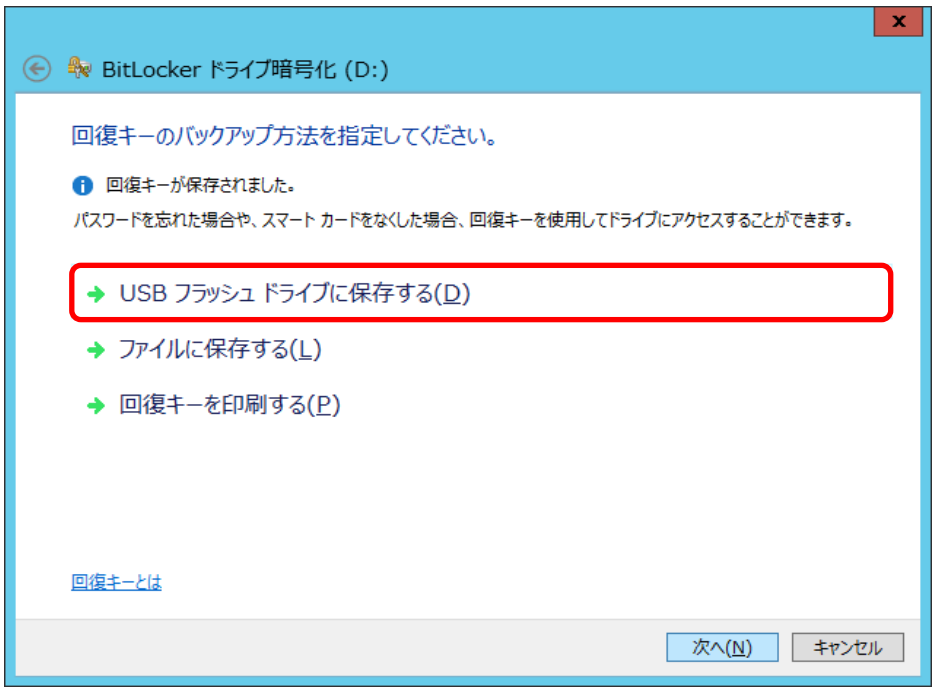
ここでは USB メモリに回復キーを保存しますので、『USB フラッシュ ドライブに保存する』をクリックします。



6.7 対象となる USB メモリを選択し、『保存』ボタンをクリックします。

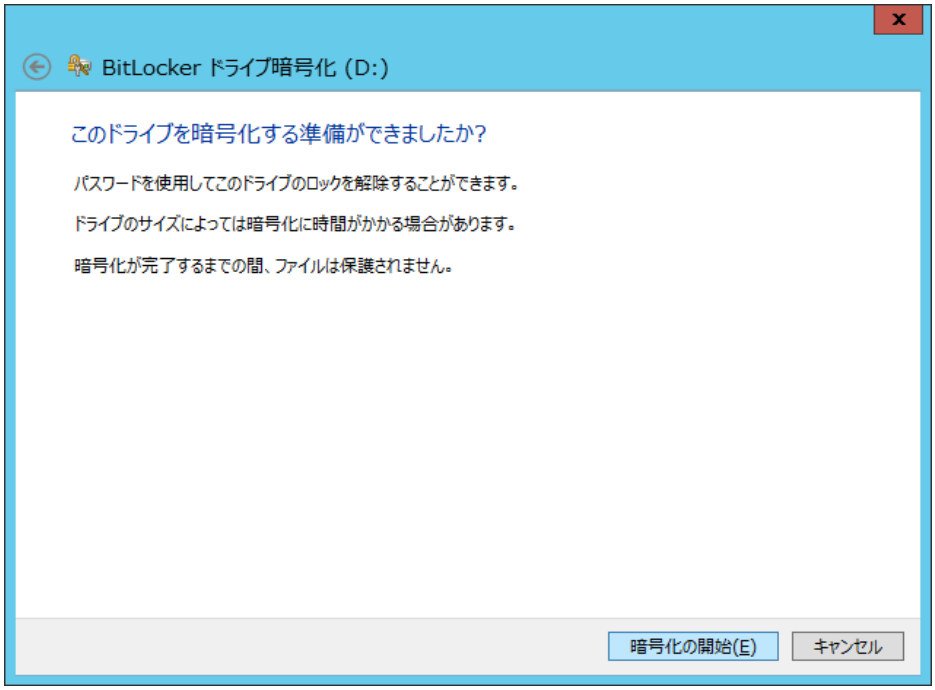


6.8『回復キーが保存されました』と標示されたら『次へ』をクリックします。



ここで作成した USB メモリ（以下、USB 回復キー）は大切に保管してください。

6.9『暗号化の開始』をクリックするとドライブの暗号化が始まります。



保存されているデータ量によって完了時間が変わりますので、データを保存する前に暗号化設定されることをお勧めします。

6.10　　完了ダイアログが表示されたら BitLocker によるドライブ暗号化は完了です。

正常に完了すると、以下のように表示されます。

7 暗号化ドライブの解除方法

BitLocker の設定が完了すると、対象ドライブは暗号化された状態となります。この状態を『ロック状態』と言います。
『ロック状態』のままでは対象ドライブへのアクセスは出来ません。（USB 回復キーを挿入していない状態で装置を再起動すると『ロック状態』で起動します。）
『ロック状態』のドライブを使用できるようにするには『アンロック』処理を実施する必要があります。
『アンロック』するには大きく以下の 2 つの方法があります。

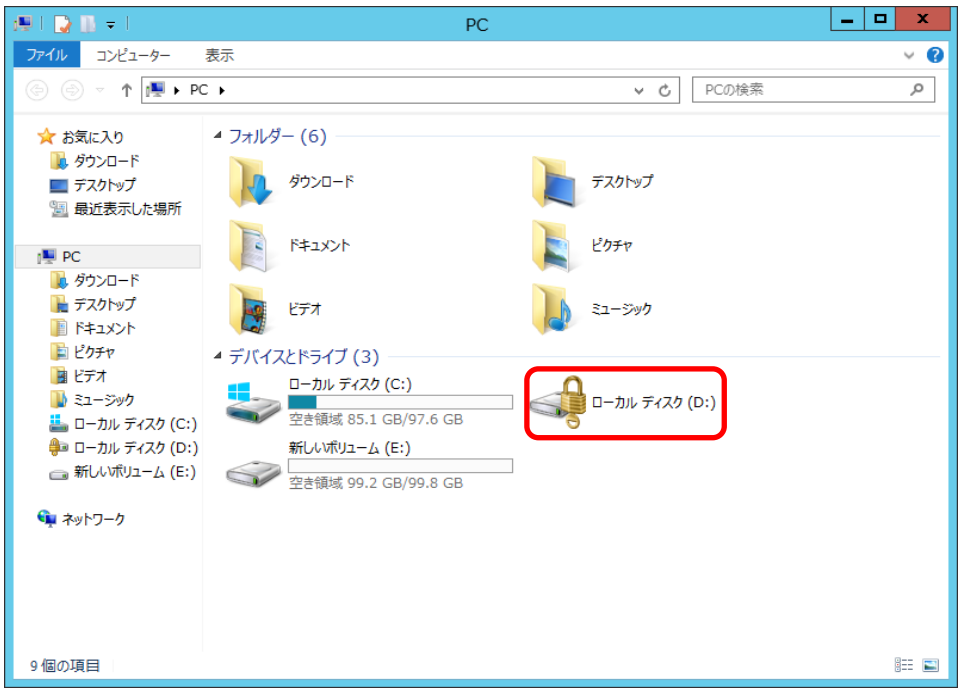
1.パスワード入力によるアンロック

2.USB 回復キーを使ったアンロック

それぞれの手順についてご紹介します。

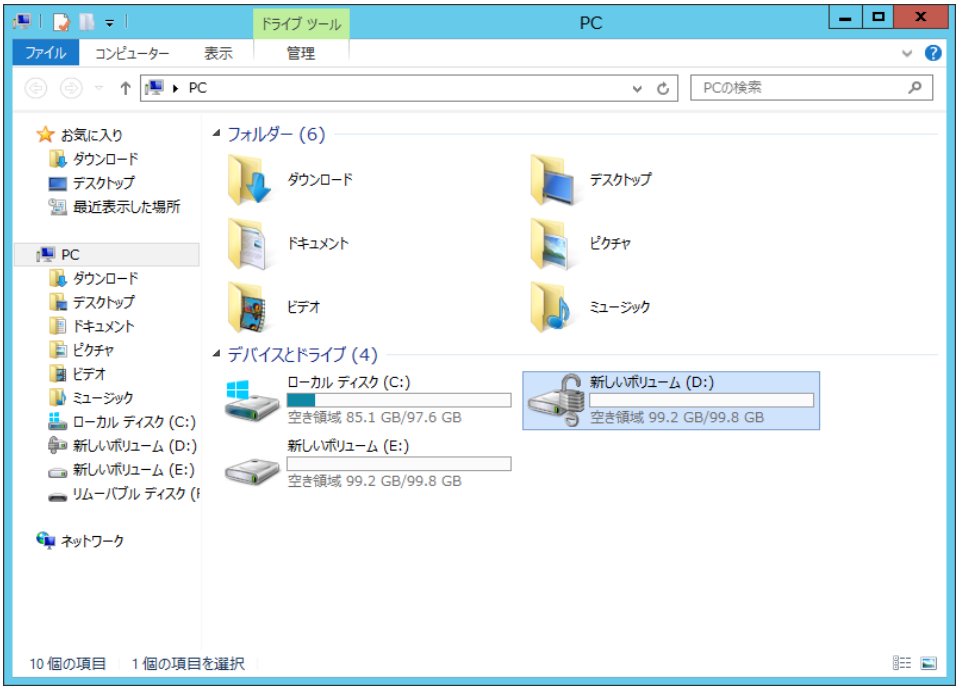
7.1 パスワード入力によるアンロック

7.1.1 エクスプローラーを開きます。



アンロックするドライブをダブルクリックすると、パスワード入力画面が開きます。

7.1.2 正しくパスワードを入力すると、対象ドライブはアンロック状態となります。



以上でアンロック処理は完了です。

7.2 USB 回復キーを使ったアンロック

7.2.1 USB 回復キーを装置に接続します。

7.2.2 Windows Power Shell を起動して、以下のように入力します。

（管理者モードで起動してください。）

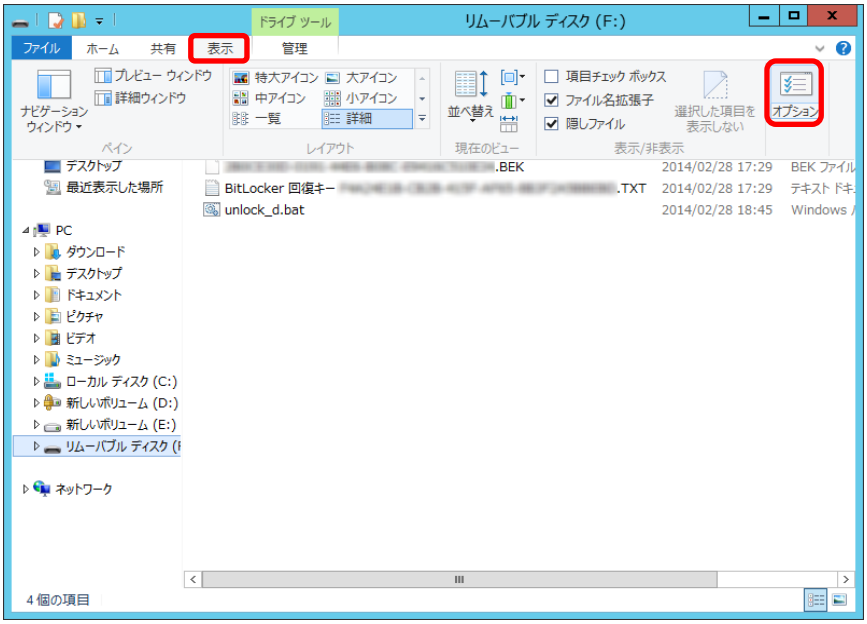
PSC:¥Users¥Administrator>**manage-bde -unlock D: -recoverykey F:¥xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx.BEK**

D: アンロック対象の BitLocker で暗号化されたドライブ

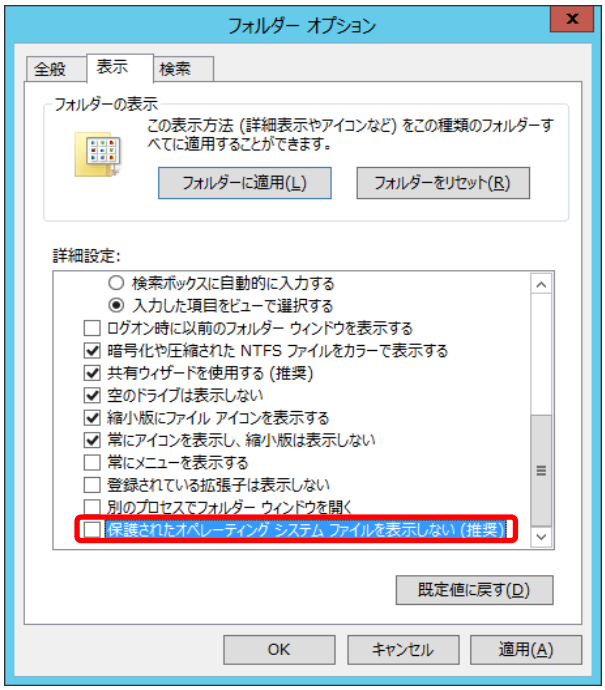
F: USB 回復キーが挿入されているドライブ

xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx.BEK 回復キー

通常、回復キーはファイル一覧に表示されません。そのため回復キーを確認するにはフォルダーオプションの設定を変更します。エクスプローラーを開き、『表示』をクリックします。メニューが表示されますので、右端にある『オプション』をクリックしてください。



『フォルダーオプション』が表示されますので、『表示』タブをクリックし、一番下にある『保護されたオペレーティングシステムファイルを表示しない(推奨)』をクリックしてチェックを外します。



以上で回復キーファイルが表示できるようになります。回復キーファイルは『～.BEK』というファイル拡張子で登録されています。

8 BitLocker 利用時の実測値

BitLocker を設定した状態と通常 RAID モードでの速度の差を測定しました。

測定方法

- 対象 NAS とクライアント PC を 1 対 1 で接続
- 1 ファイル転送：4GB サイズ 1 ファイルの読み書きを測定
- 4096 ファイル転送：1MB サイズ、1024 ファイル x4 フォルダーの読み書きを測定
- 上記測定を 5 回行った結果の平均を記載

対象 NAS：HDL-Z2WMC2 シリーズ

Windows storage server 2012 R2 搭載 NAS

1. Storage Pool Simple BitLocker 有
2. Storage Pool Simple BitLocker 無
3. RAID 0

注意事項：今回ホワイトペーパ作成の為、Storage Pool Simple および RAID 0 で評価・測定しておりますが、NAS の冗長性を損なうため、通常運用では上記モードでのご利用は推奨しておりません。

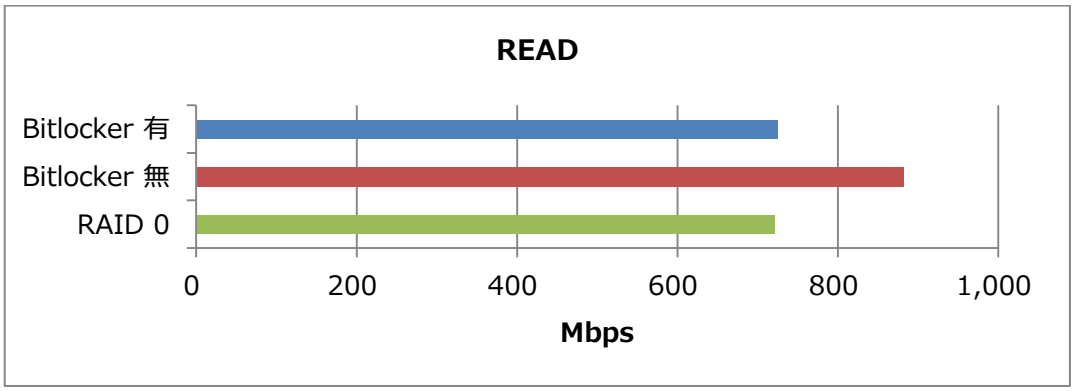
クライアント PC

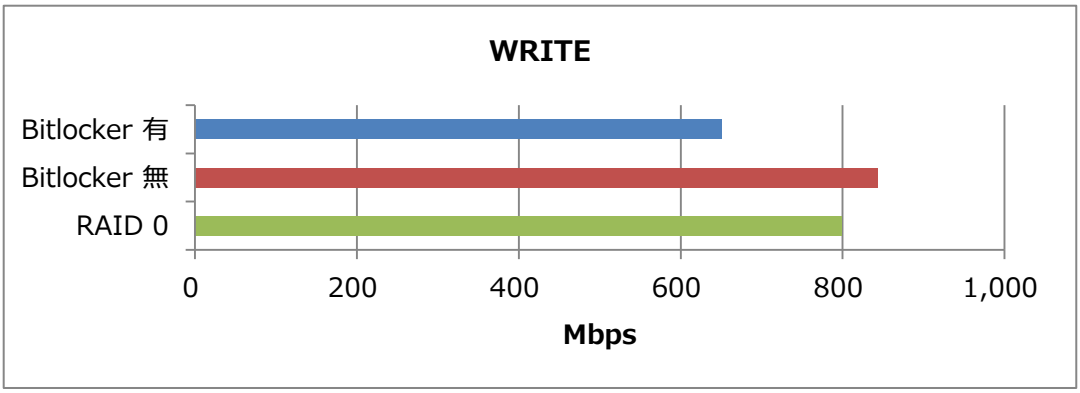
OS：Window 7 Home Premium（64bit）

CPU：Intel Core 2 Quad CPU Q8200 2.34GHz

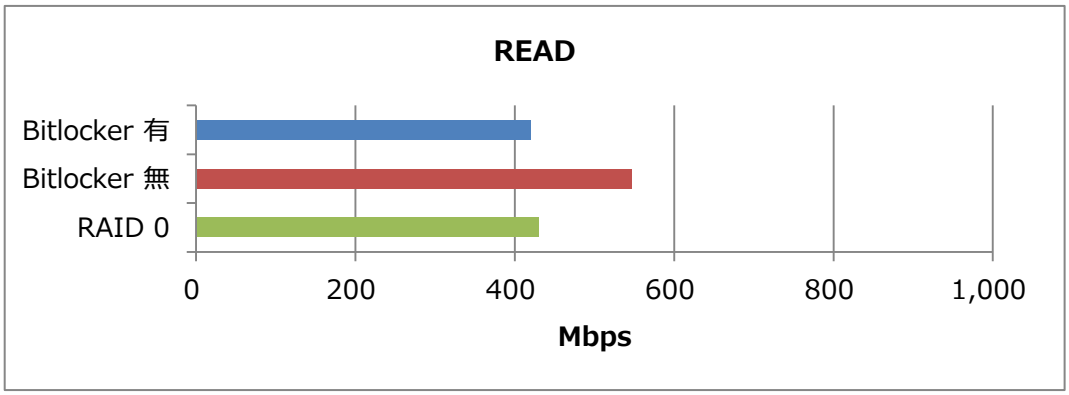
メモリ：4.0GB

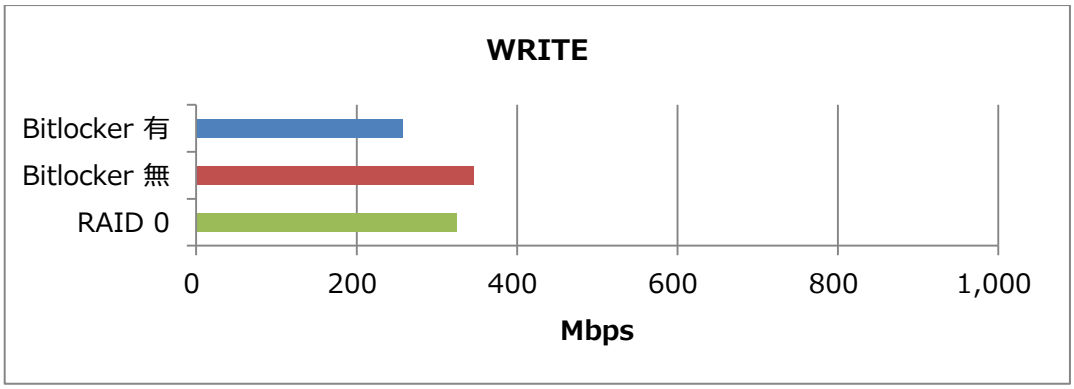
【1 ファイル転送： 1 ファイル 4GB サイズの読み書き】





【4096 ファイル転送： 1 ファイル 1GB サイズの読み書き】





BitLocker を設定して暗号化を有効にしても、大きな速度低下は見受けられませんでした。暗号化環境でも高いパフォーマンスを保っていることがわかります。

9　Tips：　ちょっと便利な使い方

実際の利用シーンでは、起動するたびにパスワードを入力したり、コマンドを入力するのは大変です。そのため、USB 回復キーを使ったアンロックを行うバッチファイルを作成し、装置起動時に実行するよう設定します。
また、HDL-Z シリーズでは『Func キー』を使って特定のプログラムを実行させることができます。『Func キー』を長押ししたらアンロックするよう設定します。

作成するバッチファイル

7.2 USB 回復キーを使ったアンロックで入力したコマンドをそのままバッチファイルとして記述します。

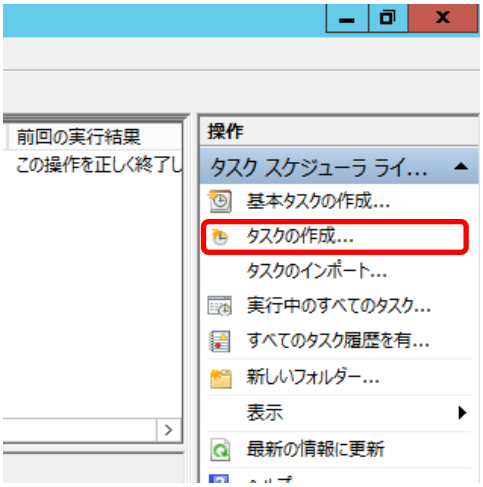
例）　C:¥unlock_d.bat
manage-bde -unlock D: -recoverykey F:¥xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx.BEK

9.1　装置起動時の実行指定

装置起動時に USB 回復キーを挿しておけば、自動的にアンロックする設定を行います。

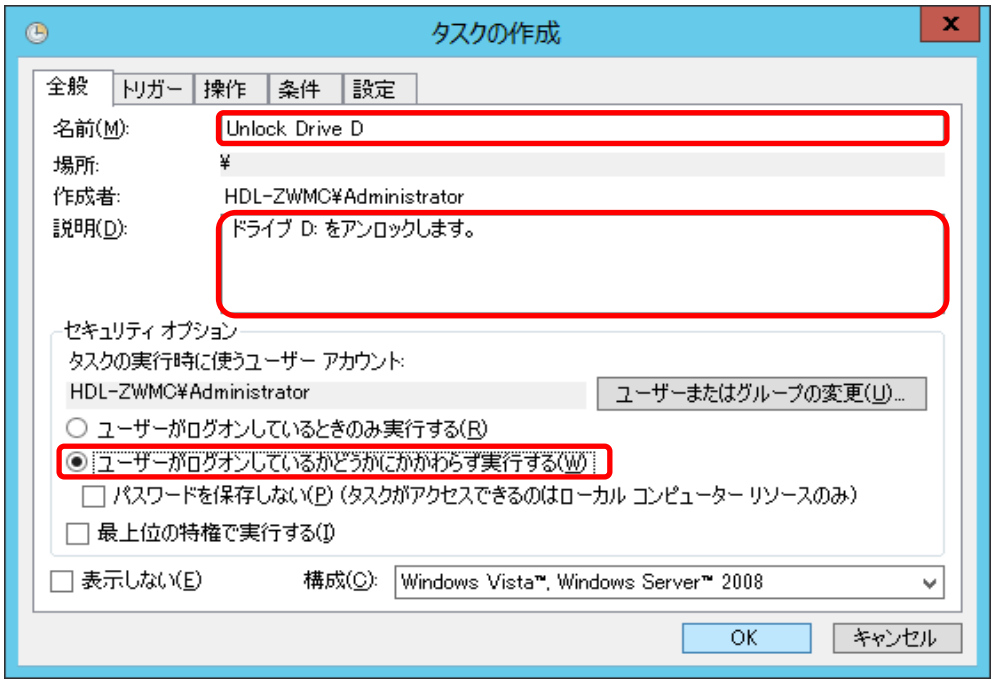
9.1.1　**ダッシュボード**から『ツール』→『タスク スケジューラー』を起動します。

9.1.2 タスクスケジューラの『操作』から『タスクの作成…』をクリックします。



9.1.3 タスクの作成ダイアログが開きます。

『全般』タブでは以下の項目を入力します。

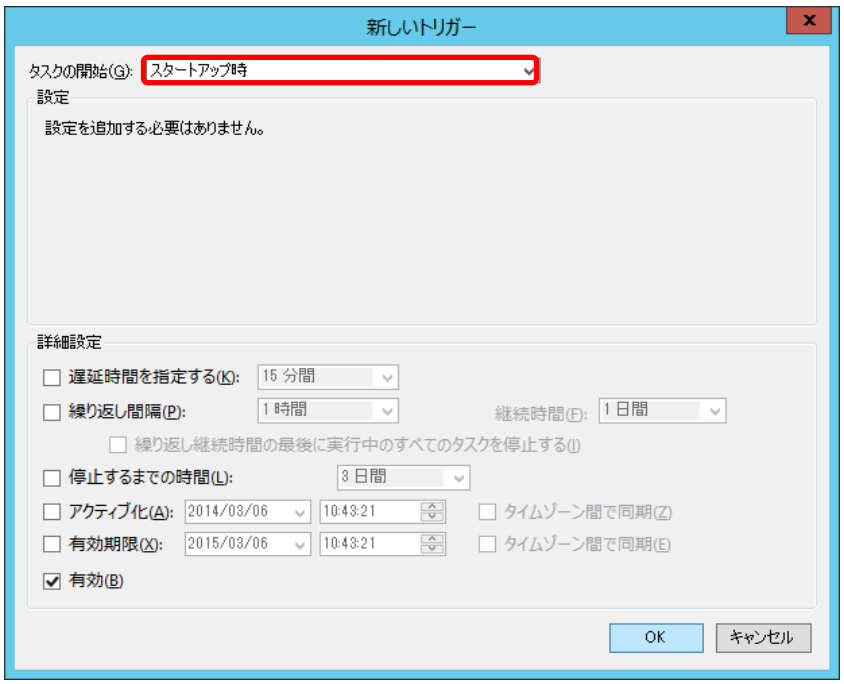


名前：任意の名前を入力します。

説明：（任意）タスクの説明文を記述します。

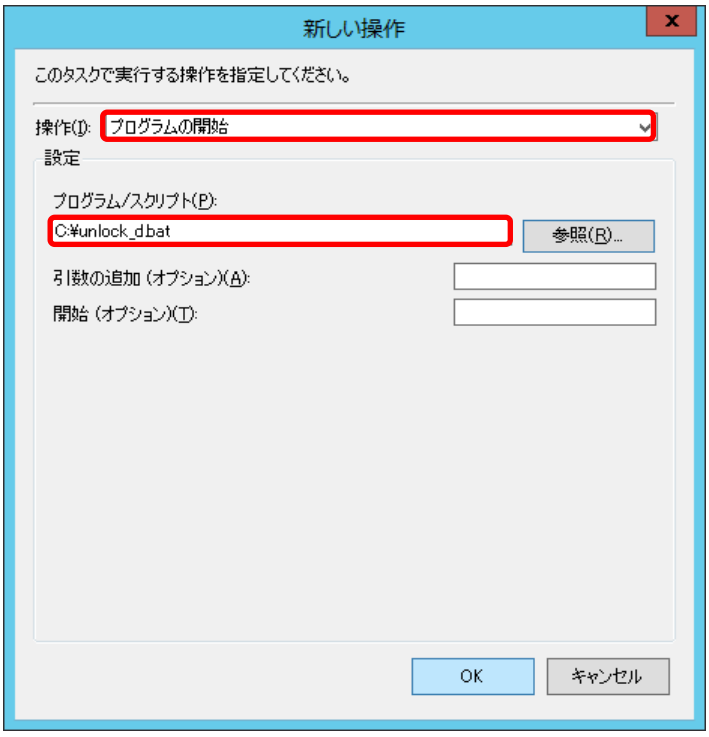
セキュリティオプション：『ユーザーがログオンしているかどうかにかかわらず実行する』にチェックします。

9.1.4 『トリガー』タブでは『新規』ボタンをクリックし、以下の項目を入力します。



タスクの開始：『スタートアップ時』を選択します。

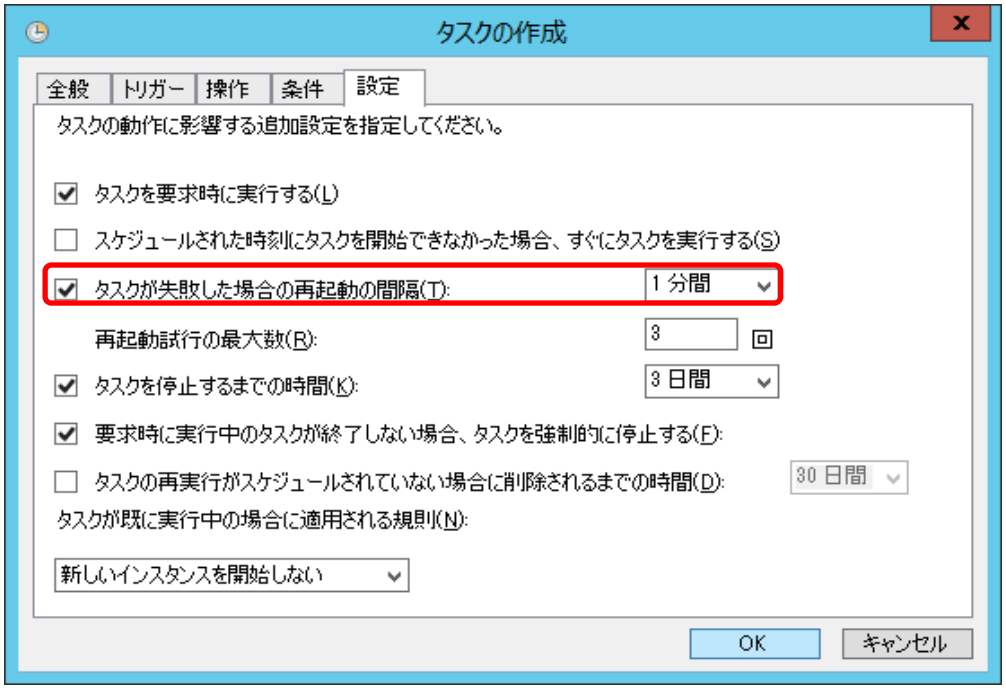
9.1.5 『操作』タブでは『新規』ボタンをクリックし、以下の項目を入力します。



操作：『プログラムの開始』を選択します。

プログラム／スクリプト：作成したバッチファイルを指定します。

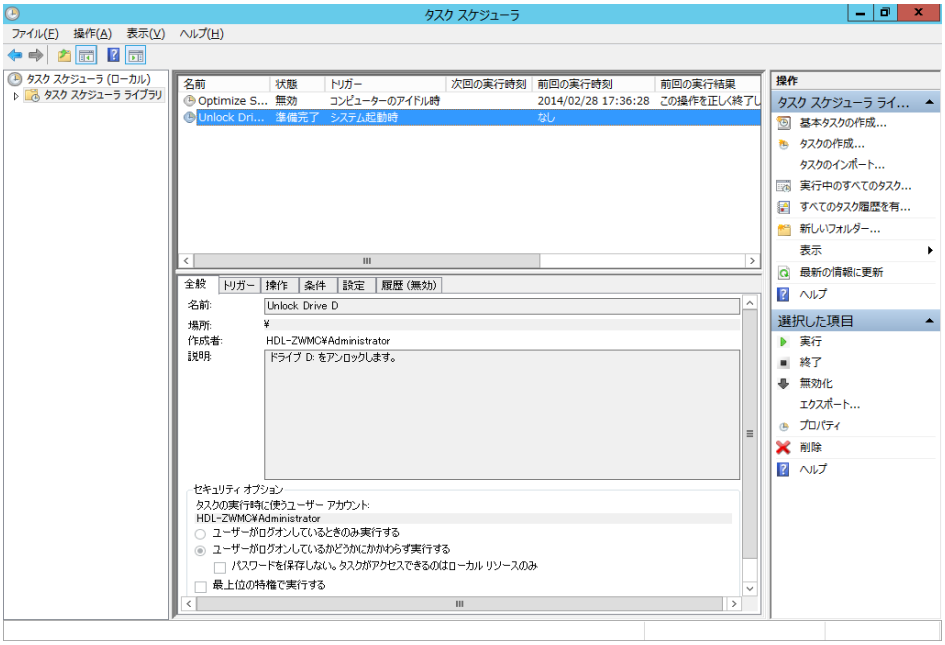
9.1.6 『設定』タブでは以下の項目を設定します。



『タスクが失敗した場合の再起動の間隔』にチェックし、『1 分間』を選択します。
通常、正常処理する場合は必要ありませんが、万一何かトラブルがありうまく起動できないときにリトライを行えるようになります。

9.1.7 『OK』ボタンをクリックすると実行権限者情報の入力画面が開きますので、管理者名（Administrator）とパスワードを入力します。

9.1.8　以上で設定は完了です。



これにより、装置起動時に USB 回復キーを挿しておけば、自動的にドライブ D:がアンロックされるようになります。

9.2 Func キー長押しでのアンロック

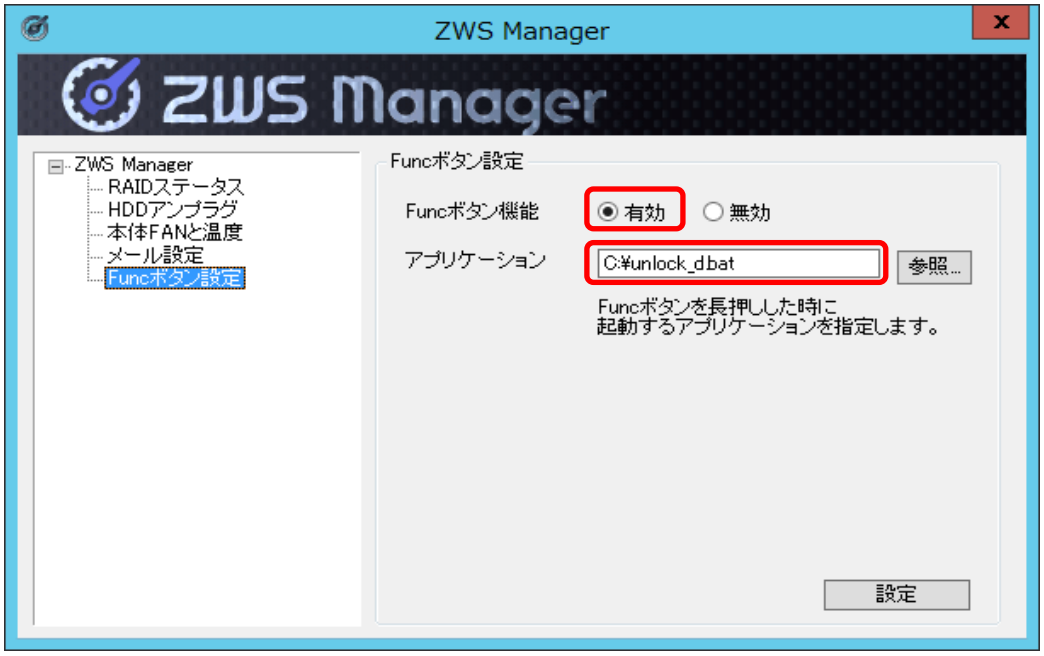
HDL-Z シリーズには『Func キー』があり、『ZWS Manager』で制御可能です。

9.1 装置起動時の実行指定で起動時設定をしておいても、うっかり接続し忘れて起動することも考えられます。

起動後に簡単にアンロックできるよう、ZWS Manager を利用してみましょう。

ZWS Manager を起動します。

画面左側の『Func ボタン設定』をクリックし、以下の項目を入力します。



Func ボタン設定：有効

アプリケーション：作成したバッチファイルを指定します。

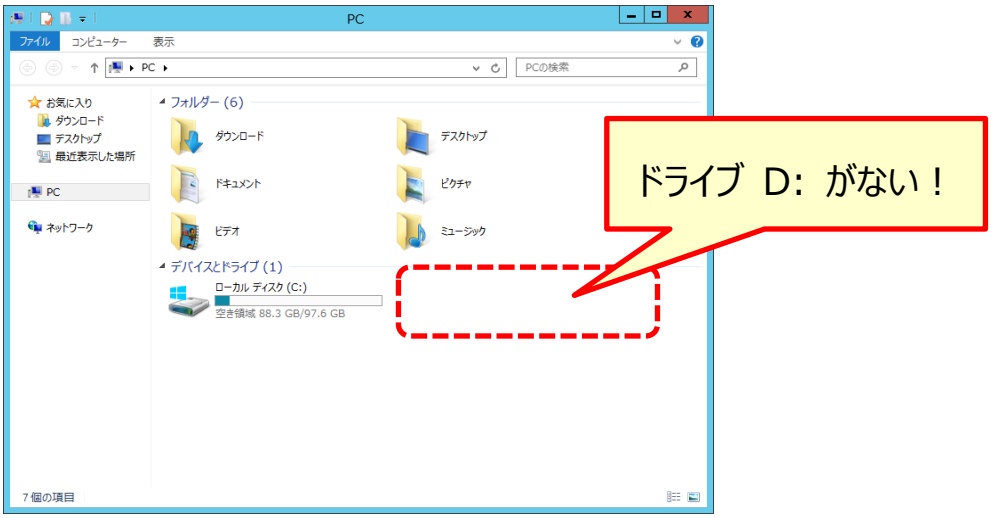
『設定』ボタンをクリックすると設定は完了です。

アンロックしたい時は、USB 回復キーを HDL-Z シリーズに挿し、『Func』ボタンを長押ししてください。

10　Tips：　システム領域をリカバリーしたときは・・・

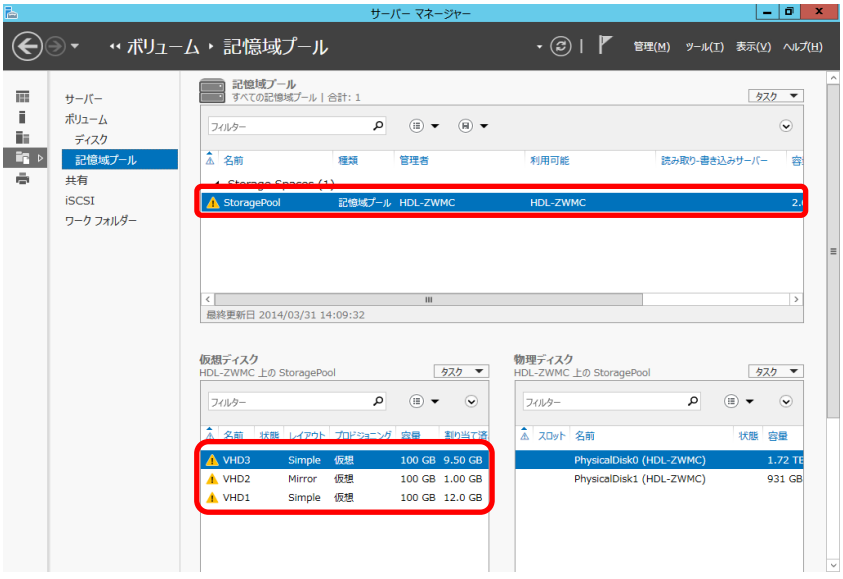
システムが何らかの要因で不安定になり、システム領域のみリカバリーしなければならない場合があります。Windows Storage Server 2012/R2 の記憶域プールはシステム領域を初期化すると、そのままでは利用不可能な状態になってしまいます。

※ あらかじめサーバーマネージャーから『役割と機能の追加』にて『BitLocker ドライブ暗号化』機能を追加しておいてください。



10.1　ステータスの確認

サーバーマネージャーから『ファイルサービスと記憶域プール』→『ボリューム』→『記憶域プール』をクリックし、状況を確認します。

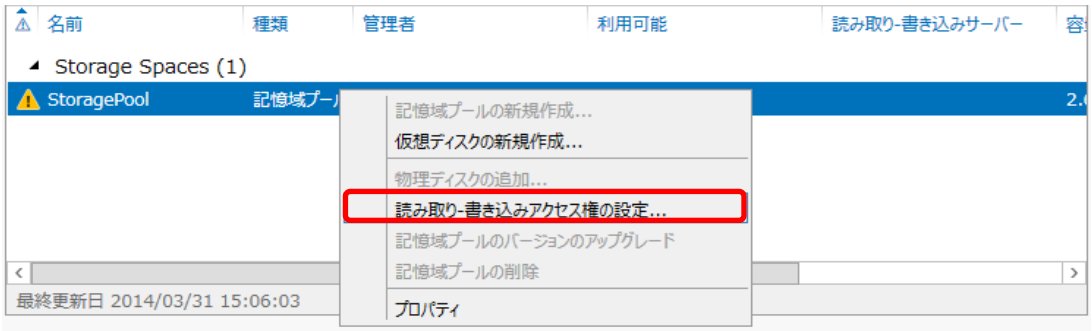


システム領域の復元直後は上記のように記憶域プール、仮想ディスクとも作成したはずの領域に『△』が付いています。これらを再び有効化することにより、見えなくなった領域を復元することができます。

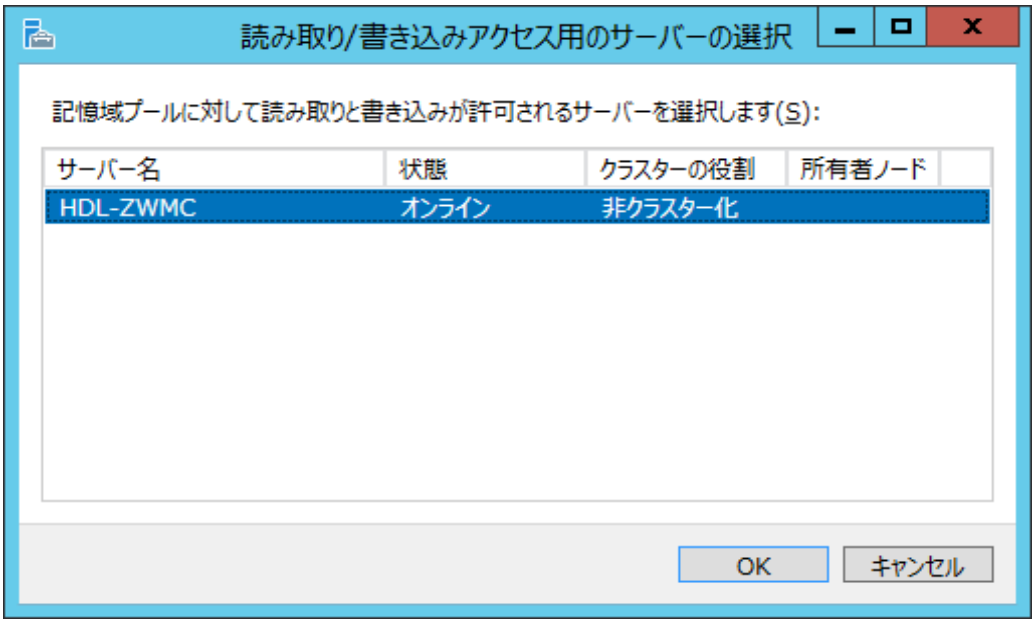
10.2　記憶域プールの復元

まずは記憶域プールから復元します。

記憶域プール欄の『StoragePool』上でマウスを右クリックし、『読み取り-書き込みアクセス権の設定…』をクリックします。



対象のサーバー確認ダイアログが表示されますので、目的のサーバーを選択し『OK』をクリックします。



以上で記憶域プールが復元されました。

10.3　仮想ディスクの復元

続いて仮想ディスクを復元します。

仮想ディスクもサーバーマネージャーから復元できますが、再起動すると再び見えなくなってしまいますので、以下のように Power Shell から復元します。

画面下にある Power Shell のアイコンをクリックします。

管理者以外でログオンしている場合は、Power Shell アイコンを右クリックして『管理者として実行』を選択します。

まずは、以下のコマンド（太字部分）を入力して、登録されている仮想ディスクの一覧を表示します。

PS C:¥Users¥Administrator> **Get-VirtualDisk**

次に登録されている仮想ディスクそれぞれについて、以下のコマンドを入力します。

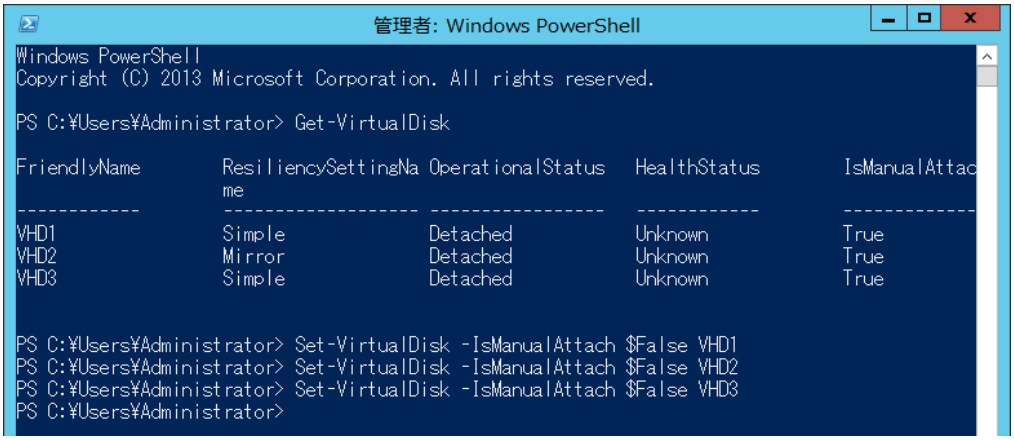
PS C:¥Users¥Administrator> **Set-VirtualDisk -IsManualAttach $False [仮想ディスク名]**

この例の場合、『VHD1』、『VHD2』、『VHD3』の 3 つの仮想ディスクがありますので、以下のように入力します。

PS C:¥Users¥Administrator> **Set-VirtualDisk -IsManualAttach $False VHD1**

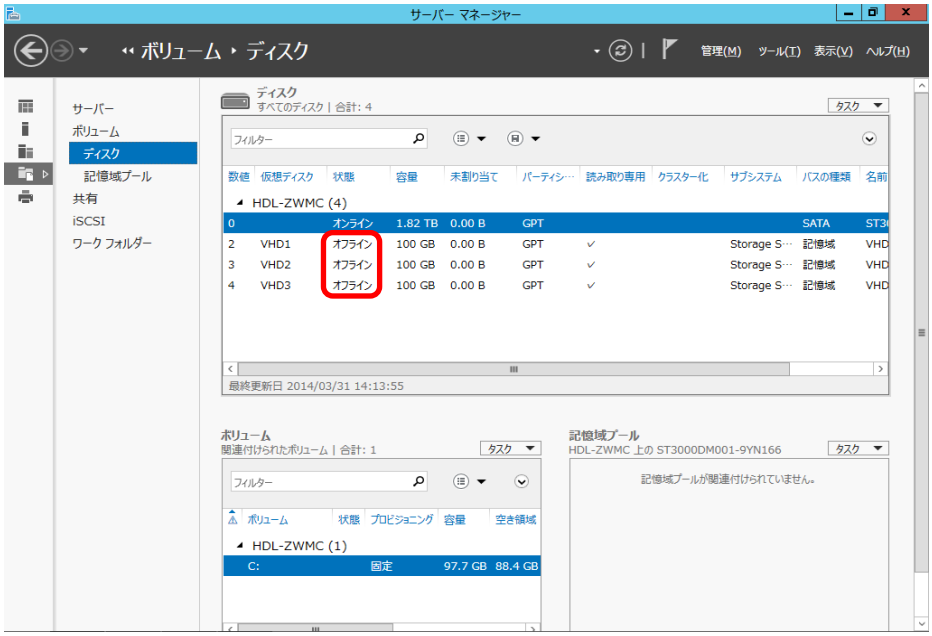
PS C:¥Users¥Administrator> **Set-VirtualDisk -IsManualAttach $False VHD2**

PS C:¥Users¥Administrator> **Set-VirtualDisk -IsManualAttach $False VHD3**

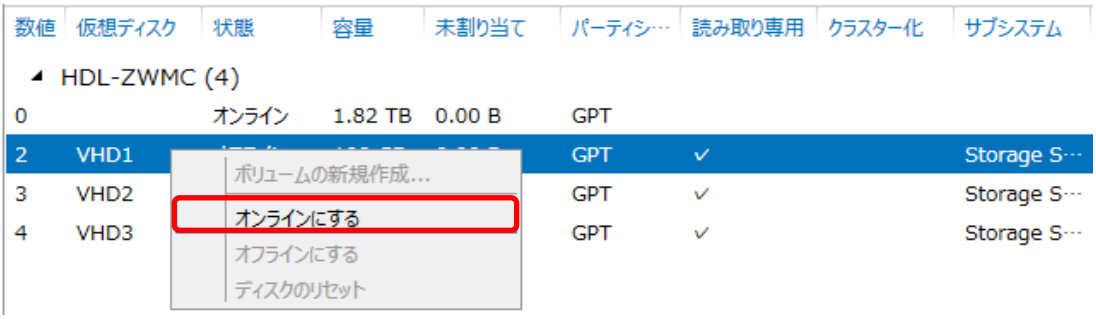


10.4 ディスクの復元

これで準備が整いました。再びサーバーマネージャーに戻り、『ファイルサービスと記憶域プール』→『ボリューム』→『ディスク』をクリックします。

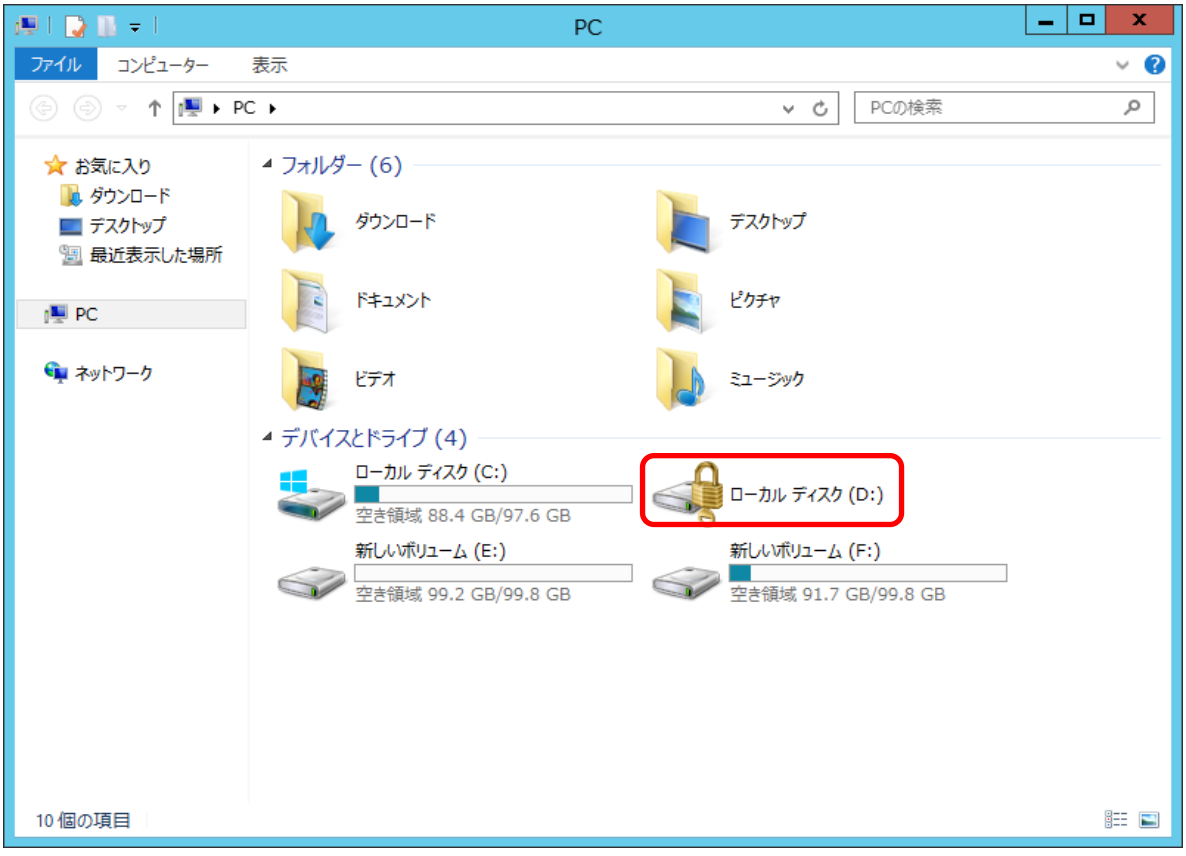


ディスク欄を見てみると、それぞれの仮想ディスクが『オフライン』となっています。
これらを利用可能な状態である『オンライン』に切り替えます。
それぞれの仮想ディスク上で右クリックし、『オンラインにする』をクリックします。



10.5 復元の確認

以上で復元は完了です。
エクスプローラーをクリックして、仮想ディスクが見えてきているか確認してください。



全てのディスクが復元できたのを確認したら完了です。