

# 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	3
2	暗号	号化の要望	3
3	実が	<b>临環境</b>	3
4	動作	乍環境	4
5	事前	↑準備	5
6	Bit	Locker の設定	9
7	暗号	<b>号化ドライブの解除方法</b> 1	6
7	.1	パスワード入力によるアンロック1	6
7	.2	<b>USB 回復キーを使ったアンロック</b> 1	8
8	Bit	<b>Locker 利用時の実測値</b> 1	9
9	Тір	s: ちょっと便利な使い方	1
9	.1	<b>装置起動時の実行指定</b>	1
9	.2	Func キー長押しでのアンロック2	5
10	Т	i <b>ps: システム領域をリカバリーしたときは・・・</b>	6
10.	1	<b>ステータスの確認</b> 2	6
10.	2	記憶域プールの復元	7
10.	3	<b>仮想ディスクの復元</b>	7
10.	4	<b>ディスクの復元</b>	8
10.	5	復元の確認	9

本文書は、株式会社アイ・オー・データ機器(以下、「アイ・オー・データ」とします。)が、アイ・オー・データの特定の商品に関 する機能・性能や技術についての説明を記述した参考資料となります。当該商品の利用という目的の範囲内で自由に使用、 複製をしていただけますが、アイ・オー・データの事前の書面による承諾なしに、改変、掲示、転載等の行為は禁止されます。 また、<u>あくまで参考資料として提供いたしますので、内容については一切保証を致しかねます。</u>以下の内容をご了承いただ いた場合のみご利用ください。

- (1) アイ・オー・データは、本文書によりいかなる権利の移転もしくはライセンスの許諾、またはいかなる保証を与えるもの ではありません。
- (2) アイ・オー・データは、本文書について、有用性、正確性、特定目的への適合性等のいかなる保証をするものでは ありません。
- (3) アイ・オー・データは、本文書を利用したこと、または利用しなかったことにより生じるいかなる損害についても責任を 負うものではありません。
- (4) アイ・オー・データは、本文書の内容を随時、断りなく更新、修正、変更、削除することがあります。最新の商品情報については、<u>http://www.iodata.jp/</u>をご覧ください。

# 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

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。

A	役割と機能の追加ウィザード
開始する前に	対象サーバー HDL-ZWMC
開始する前に インストールの種類 サーバーの選択	このウイザードを使用すると、役割、役割サービス、または機能をインストールできます。ドキュメントの共有や Web サイト のホストなどの組織のコンピューティング ニーズに応じて、インストールする役割、役割サービス、または機能を決定しま す。 役割、役割サービス、または機能を削除するには、次の手順を実行します:
サーバーの役割 機能 確認 結果	役割と機能の削除ワイサートの起勤 続行する前に、次のタスクが完了していることを確認してください。 ・管理者アカウントに弾力なパスワードが設定されている ・静的 IP アドレスなどのネットワークの設定が構成されている ・Windows Update から最新のセキュリティ更新プログラムがインストールされている
	前提条件が完了していることを確認する必要がある場合は、ウイザードを閉じて、それらの作業を完了してから、ウイザードを再度実行してください。 続行するには、「次へ」 をクリックしてください。
	□ 既定でこのページを表示しない(S)
	<前へ(P) 次へ(N) > インストール(I) キャンセル

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。

<b>a</b>	役割と機能の追加ウィザード	_ 🗆 X
インストールの種類	の選択	対象サーバー HDL-ZWMC
開始する前に <u>インストールの種類</u> サーバーの選訳 サーバーの役割 機能 確認 結果	<ul> <li>インストールの種類を選択します。役割および機能は、実行中の物理コンピューター、仮想コンピューンの仮想ハードディズク(VHD)にインストールできます。</li> <li>② 役割ペースまたは機能ペースのインストール 役割、役割サービス、および機能を追加して、1 台のサーバーを構成します。</li> <li>③ リモートデスクトップサービスのインストール 仮想デスクトップ インフラストラクチャ (VDI)に必要な役割サービスをインストールして、仮想マシション ペースのデスクトップ展開を作成します。</li> </ul>	·ター、またはオフライ ·ン ベースまたはセッ
	<前へ( <u>P</u> ) 次へ( <u>N</u> ) > インストール(	[) キャンセル

- 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。

<b>a</b>	役割と機能の追加ウィザード
対象サーバーの達	刻衆サーバー HDL-ZWMC
開始する前に	役割と機能をインストールするサーバーまたは仮想ハード ディスクを選択します。
インストールの種類	● サーバー ブールからサーバーを選択
サーバーの選択	○ 仮想ハード ディスクから選択
サーバーの役割	サーバー プール
機能	フィルター:
確認	
結果	名前 IP アドレス オペレーティング システム
	HDL-2WMC MICLOSOIL WINDOWS Storage Server 2012 K2 Work
	< III > 1 かのついどっ カーが目つかりました
	コーロップクロージー・デーデル・プリンス CLC このページには、Windows Server 2012 を実行しており、サーバー マネージャーの [サーバーの追加] コマンドを使 用して追加されたサーバーが表示されます。 オフライン サーバーや、データ収集が完了していない、新たに追加された サーバーは表示されません。
	<前へ(P) 次へ(N) > インストール(I) キャンセル

P	役割と機能の追加ウィザード	_ <b>□</b> X
サーバーの役割の	選択	対象サーバー HDL-ZWMC
開始する前に	選択したサーバーにインストールする役割を 1 つ以上選択します。	
インストールの種類	役割	説明
サーバーの選択 サーバーの役割 機能 確認 結果	<ul> <li>Active Directory ライトウェイト ディレクトリ サービス</li> <li>Web サーバー (IIS)</li> <li>■ ファイル サービスと記憶域サービス (3/11 個をインストール済)</li> <li>■ 印刷とドキュメント サービス (1/4 個をインストール済み)</li> </ul>	Active Directory ライトウェイト ディレク トリ サービス (AD LDS) は、アリケー ション回有データのストアを、Active Directory ドメイン サービスのインフラスト ラクチャを必要としないディレクトリ対応アプ リケーションに対して提供します。1 つの サーバー上に複数の AD LDS インスタン スが共存でき、それぞれに独自のスキーマ を持たせることができます。
	< III >	
	<前へ(P) 次へ(N)	)> インストール(I) キャンセル

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

<b>b</b>	役割と機能の追加ウィザード	_ <b>D</b> X
機能の選択 開始する前に インストールの種類 サーバーの選択 サーバーの役割 機能	役割と機能の追加ウイザード 選択したサーバーにインストールする機能を 1 つ以上選択します。 機能 ▶ ■ .NET Framework 3.5 Features (1/3 個をインスト ▶ ■ .NET Framework 4.5 Features (2/7 個をインスト ■ .NET Framework 4.5 Features (2/7 個をインスト ■ BranchCache □ Direct Play □ HTTP プロキシを経由した RPC □ IS ホスト可能な Web コア □ IP アドレス管理 (IPAM) サーバー □ iSNS サーバー サーゼス □ LPR ポート モニター Management OData IIS 拡張機能 □ NFS クライアント □ SAS 198572 - ジャー 等調 t-ub (CMAY)	<ul> <li>ユ ロ メ         メ             メ             メ</li></ul>
	RDC (Remote Differential Compression)	
	<b>&lt;前へ(P)</b> 次へ(N	) > インストール( <u>I</u> ) <b>キャンセル</b>

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

	役割と機能の追加ウィザード	
<ul> <li>機能の選択</li> <li>開始する前に インストールの種類 サーバーの選択 サーバーの役割</li> <li>機能</li> <li>確認</li> <li>結果</li> </ul>	選択したサーバーにインストールする機能を 1 つ以上選択します。 機能 ▶ ■ .NET Framework 3.5 Features (1/3 個をインスト ▶ ■ .NET Framework 4.5 Features (2/7 個をインスト ♥ BitLocker ドライブ暗号化 ■ BranchCache ■ Direct Play ■ HTTP プロキシを経由した RPC ■ IIS ホスト可能な Web コア ■ IP アドレス管理 (IPAM) サーバー	対象サーバー HDL-ZWMC 説明 BitLocker ドライブ暗号化を使用する と、ポリューム全体を暗号化して初期の ブートコンポーネントの整合性が確認され るため、コンビューターの紛失、盗難、また は不適切な非コミッションからデータを保護 できます。データはこれたドライブが 元のコンビューターにある場合にのみ暗号 化解除されます。整合性の確認の際、互 換性のあるトラステッドプラットフォーム モ シュール (TPM) が必要となります。
	は SNS 9-パー 9-EX LPR ポート モニター Management OData IIS 拡張機能 NFS クライアント RAS 接続マネージャー管理キット (CMAK) RDC (Remote Differential Compression) Classic TO/TD Contents く Ⅲ > < 前へ( <u>P</u> ) 次へ( <u>N</u> )	> (1)XI-1/(I) +r>t1/

認して、『次へ』をクリックします。

<b>a</b>	役割と機能の追加ウィザード	_ 🗆 🗙
インストール オプシ		対象サーバー HDL-ZWMC
開始する前に	選択したサーバーに次の投資制、投資制サービス、または1機能を1 ノストール9 るには、「1 ノストール	」をクリックしてください。
インストールの種類	○ 必要に応じて対象サーバーを目動的に再起動する	
サーバーの選択	オプションの機能(管理ツールなど)は、自動的に選択されるため、このページに表示されている。 らのオプションの機能をインストールしない場合は、「前へ」をクリックして、チェック ボックスをオフに	可能性があります。これ してください。
サーバーの役割		
機能	BitLocker ドライブ暗号化	
確認	リモート サーバー管理ツール	
結果	機能管理ツール BitLocker ドライブ暗号化管理ユーティリティ BitLocker 回復パスワード ビューアー BitLocker ドライブ暗号化ツール	
	AD DS および AD LDS ツール	
	AD DS ツール	
	AD DS スナップインおよびコマンドライン ツール	
	拡張記憶域	
	構成設定のエクスポート 代替ソース バスの指定	
	<前へ( <u>P</u> ) 次へ( <u>N</u> ) > インストー	·ル(I) キャンセル

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。





『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。

すべての場所 ~	
BitLocker 🔎	

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。

SitLocker の管理	
1 個の設定	

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。

<b>4</b>	BitLocker ドライブ暗号化	_ <b>D</b> X
🔄 💿 🔻 🕈 🏘 « 527548t	Zキュリティ → BitLocker ドライブ暗号化 v	C コントロール パネルの検索 P
コントロール パネル ホーム	BitLocker ドライブ暗号化 BitLocker ドライブ暗号化によりドライブを保護することで、ファイルお ちます。	<b>②</b> はびフォルダーの承認されないアクセス防止に役立
	オペレーティング システム ドライブ	
	C: BitLocker が無効です	$\odot$
	BitLock	er を有効にする
	固定データ ドライブ	
	新しいボリューム (D:) BitLocker が無効です	$\odot$
	新しいポリューム (E:) BitLocker が無効です	$\odot$
関連項目 TPM の管理 ディスクの管理 プライバミーに関する実用	リムーバブル データ ドライブ - BitLocker To Go F: BitLocker が無効です	$\odot$
フラコバラ (日知970)年1月		

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。

	x
○ 🎭 BitLocker ドライブ暗号化 (D:)	
このドライブのロック解除方法を選択する	
『アスワードを使用してドライブのロックを解除する(P) パスワードには大文字、小文字、数字、空白文字、記号を含めてください。	
パスワードを入力してください( <u>E</u> ) ●●●●●●●●	
パスワードをもう一度入力してください(R)	
□ スマート カードを使用してドライブのロックを解除する( <u>S</u> ) スマート カードを挿入する必要があります。ドライブのロックを解除するときは、スマート カードの暗証番号 (PIN) が必要です。	
次へ(N) キャンセル	

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。

¢	× 影itLocker ドライブ暗号化 (D:)
	回復キーのバックアップ方法を指定してください。 パスワードを忘れた場合や、スマートカードをなくした場合、回復キーを使用してドライブにアクセスすることができます。
	◆ USB フラッシュ ドライブに保存する(D)
	→ ファイルに保存する(L)
	→ 回復キーを印刷する(P)
_	回復キーとは
	次へ(12) キャンセル

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。

回復キーを USB フラッシュ ドライブに保存する		
USB デバイスを差し込み、一覧からデバイスを選     択し、[保存] をクリックしてください。		
ー リムーバブル ディスク (F:)		
保存( <u>S</u> ) キャンセル		

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。

	x
📀 🎭 BitLocker ドライブ暗号化 (D:)	
回復キーのバックアップ方法を指定してください。	
→ USB フラッシュ ドライブに保存する( <u>D</u> )	
→ ファイルに保存する(L)	
→ 回復キーを印刷する(P)	
回復キーとは	
次へ(N) キャンセ	IL

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。

	x
📀 🎭 BitLocker ドライブ暗号化 (D:)	
このドライブを暗号化する準備ができましたか?	
パスワードを使用してこのドライブのロックを解除することができます。	
ドライブのサイズによっては暗号化に時間がかかる場合があります。	
暗号化が完了するまでの間、ファイルは保護されません。	
	暗号化の開始(E) キャンセル

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。

<b>₽</b> e	BitLocker ドライブ暗	号化	_ 🗆 🗙
🔄 💿 🔻 🕈 🏘 « 5276202	Fユリティ 🕨 BitLocker ドライブ暗号化	✓ C コントロール //	ペネルの検索  ク
コントロール パネル ホーム	BitLocker ドライブ暗号化 BitLocker ドライブ暗号化によりドライブを保護 役立ちます。	することで、ファイルおよびフォルダーの承認さ	
	オペレーティング システム ドライブ		
	C: BitLocker が無効です		$\bigcirc$
	<b>~</b>	🜍 BitLocker を有効にする	=
	固定データドライブ		
	新しいボリューム (D:) BitLocker	- が有効です	$\bigcirc$
朗海道日		<ul> <li>         ・         ・         ・</li></ul>	
国建境日 予 TPM の管理		🚱 自動ロック解除の有効化 🚱 BitLocker を無効にする	
ディスクの管理 プライバシーに関する声明	新しいボリューム (E:) BitLocker	が無効です	<ul> <li>✓</li> </ul>

# 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。

19   🕞 🔝 🖛	PC	_ <b>D</b> X
ファイル コンピューター	表示	~ <b>(</b> )
\ominus 🔿 - 🕇 💌 F	۲ ک ک ک	YCの検索 <b>ク</b>
<ul> <li>☆ お気に入り</li> <li>※ ダウンロード</li> <li>※ デスクトップ</li> <li>※ 最近表示した場所</li> <li>※ グウンロード</li> <li>※ デスクトップ</li> <li>※ ゲウンロード</li> <li>※ デスクトップ</li> <li>※ ドキュメント</li> <li>※ ビクチャ</li> <li>※ ビデオ</li> <li>※ ミュージック</li> <li>※ ローカル ディスク (C:)</li> <li>※ ローカル ディスク (C:)</li> <li>※ ローカル ディスク (C:)</li> <li>※ ローカル ディスク (C:)</li> <li>※ 新しいボリューム (E:)</li> </ul>	<ul> <li>▲ フォルダー(6)</li> <li>▲ ジウンロード</li> <li>● デスクトップ</li> <li>● デスクトップ</li> <li>● デスクトップ</li> <li>● デスクトップ</li> <li>● デスクトップ</li> <li>● ジウンロード</li> <li>● ジローボーズク(C:)</li> <li>● ジローボル ディスク(C:)</li> <li>● ジローボル ディスク(</li></ul>	)
9個の項目		8==

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。

BitLocker (D:)
このドライブのロックを解除するためにパスワードを入力して ください。
<b>^</b>
その他のオプション
ロック解除

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。

1 💭 l 🔁 👔 = l	ドライブ ツール	PC	_ 🗆 X
ファイル コンピューター	表示  管理		~ <b>?</b>
(a) (b) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c		✓ C PCの検索	م
<ul> <li>☆ お気に入り</li> <li>※ ダウンロード</li> <li>デスクトップ</li> <li>※ 厨」 展示表示した場所</li> <li>● PC</li> <li>● ダウンロード</li> <li>● デスクトップ</li> <li>● ドキュメント</li> <li>● ビクチャ</li> <li>● ビデオ</li> <li>● ミュージック</li> <li>▲ ローカル ディスク (C:)</li> <li>● 新しいボリューム (D:)</li> <li>■ 新しいボリューム (E:)</li> <li>■ リムーパブル ディスク (F</li> </ul>	<ul> <li>              オオルダー(6)             ダウンロード             ダウンロード             ダウンロード             ドキュメント             ビデオ             ビデオ</li></ul>	デスクトップ レクチャ レクチャ ミュージック S:) B/97.6 GB S:) B/99.8 GB	
10 個の項目 1 個の項目	を選択		: 🖿

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:¥xxxxxxx-xxxx-xxxx-xxxx-xxxx.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-xxxxxxxxxxx.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。

フォルダー オプション	x
全般表示検索	
フォルダーの表示 この表示方法 (詳細表示やアイコンなど) をこの種類のフォルダーす べてに適用することができます。 フォルダーに適用(L) フォルダーをリセット(R)	
<ul> <li>○ 検索ボックスに自動的に入力する</li> <li>◎ 入力した項目をビューで選択する</li> <li>□ ログオン時に以前のフォルダー クインドウを表示する</li> <li>▽ 暗号化や圧縮された NTFS ファイルをカラーで表示する</li> <li>▽ 共有ウィザードを使用する(推奨)</li> <li>◇ 空のドライブは表示しない</li> <li>○ 確心板にファイル アイコンを表示する</li> <li>▽ 常にアイコンを表示しない</li> <li>○ 常にアイコンを表示する</li> <li>○ 常は、ニューを表示する</li> <li>○ 登録されている拡張子は表示しない</li> <li>○ 別のプロセスでフォルダー ウィンドウを開く</li> <li>□ 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)</li> </ul>	
既定値に戻す(D)	
OK キャンセル 適用(A)	)

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: ¥xxxxxxx-xxxx-xxxx-xxxx-xxxx-xxxx.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。

サーバー マネージャー	
ボード ・ ②	)   🚩 管理(M) <mark>ツール(T)</mark> 表示(V) ヘルプ(H)
	Active Directory サイトとサービス
	Active Directory ドメインと信頼関係
	Active Directory ユーザーとコンピューター
	ADSI IT19-
このローカル サーバーの構成	
	ODBC 7-9 9-X (64 EVF)
2 役割と機能の追加	Windows PowerShell (v.9.0)
	Windows PowerShell (X86)
3 管理するサーバーの追加	Windows PowerShell ISE
	Windows Sorver Jud Zud
4 9 A 900 JOI FUX	Windows VELIS
	イベントドューアー
	コンピューターの管理
	コンポーネント サービス
	サービス
	システム構成
数:1   サーバーの合計数:1	システム情報
- 1	セキュリティが強化された Windows ファイアウォール
1 🛛 📥 印刷サービス	セキュリティの構成ウィザード
	タスク スケジューラ
1 管理状態	ドライブのデフラグと最適化
イベント	パフォーマンス モニター

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。

・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・			
全般 トリガー 操作 条件 設定			
名前( <u>M</u> ): Unlock Drive D			
場所: ¥			
作成者: HDL-ZWMC¥Administrator			
説明( <u>D</u> ): ドライブ D: をアンロックします。			
セキュリティ オプション			
タスクの実行時に使うユーザー アカウント:			
HDL-ZWMC¥Administrator ユーザーまたはグループの変更(U)			
○ ユーザーがログオンしているときのみ実行する(R)			
● 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(W)			
パスワードを保存しない(P) (タスクがアクセスできるのはローカル コンピューター リソースのみ)			
□ 最上位の特権で実行する①			
□ 表示しない(E) 構成(C): Windows Vista™, Windows Server™ 2008 ✓			
OK         キャンセル			

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。

新しいトリガー	x
タスクの開始(G): スタートアップ時	
設定	
設定を追加する必要はありません。	
詳細設定	
□ 遅延時間を指定する(K): 15 分間 ∨	
□ 繰9返し間隔(P): 1時間 V 継続時間(F): 1日間 V	
□ 繰り返し継続時間の最後に実行中のすべてのタスクを停止する(!)	
□ 停止するまでの時間(L): 3 日間 ∨	
□ アクティブ化(A): 2014/03/06 ↓ 10:43:21 ラ □ タイムゾーン間で同期(Z)	
□ 有効期限(X): 2015/03/06 V 10:43:21 🔄 □ タイムゾーン間で同期(E)	
✓ 有効(B)	
OK ++v>1	211

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。

新しい操作	x
このタスクで実行する操作を指定してください。	
操作(J): プログラムの開始	y
設定	
プログラム/スクリプト( <u>P</u> ):	
C:¥unlock_dbat	参照( <u>R</u> )
引数の追加 (オプション)( <u>A</u> ):	
開始 (オプション)(工):	
	ОК <i>キャンセル</i>

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。

P         タスクの作成	×
全般 トリガー 操作 条件 設定 タスクの動作に影響する追加設定を指定してください。	
▼ タスクを要求時に実行する(L)	
□ スケジュールされた時刻にタスクを開始できなかった場合、すぐにタ	スクを実行する( <u>S</u> )
✓ タスクが失敗した場合の再起動の間隔(T):	1 分間 🗸
再起動試行の最大数(图):	3 🛛
☑ タスクを停止するまでの時間(K):	3日間 🗸
■ 要求時に実行中のタスクが終了しない場合、タスクを強制的に停	▶止する( <u>F</u> ):
タスクの再実行がスケジュールされていない場合に削除されるまで タスクが既に実行中の場合に適用される規則(N):	(0時間(0): 30日間 ↓
新しいインスタンスを開始しない ✓	
	ОК <b>++&gt;</b> セル

『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。

	タスク スケジューラ ? ×
	G S
このタスクを実行するユーサ	fー アカウント情報を入力してください。
ユーザー名( <u>U</u> ):	😰 HDL-ZWMC¥Administrator 🗸 💷
パスワード <u>(P</u> ):	
	OK キャンセル

	タスク スケジューラ	_ 0	2
ファイル(E) 操作(A) 表示(⊻)	ヘルプ( <u>H</u> )		
Þ 🔿 🙎 🖬 🚺 🖬			
タスク スケジューラ (ローカル)	名前 状態 トリガー 次回の実行時刻 前回の実行時刻 前回の実行結果	果 操作	
> 🔀 タスク スケジューラ ライブラリ	④ Optimize S 無効 コンビューターのアイドル時 2014/02/28 17:36:28 この操作を正しく	〈終了し タスク スケジューラ ライ	
	Onlock Dri 準備完了 システム起動時 なし	💿 基本タスクの作成	_
		🔈 タスクの作成	
		タスクのインポート	
		実行中のすべてのタス	ŋ
		■ すべてのタスク履歴を有	á
		新しいフォルダー	
		表示	
	< III	> 品新の情報に更新	
	全般 トリガー 操作 条件 設定 履歴(無効)		
	名前: Unlock Drive D		
	場所: ¥	選択した項目	
	作成者: HDL-ZWMC¥Administrator	▶ 実行	
	130% トライブ D: をアンロックします。	終了	
		- ● 無効化	
		エクスポート	
		・ プロパティ     ・	
		- 🗙 削除	
		2 ∧ルプ	
	ช่ายปราก สวีบัยช่ว		
	タスクの実行時に使うユーザーアカウント		
	HDL-ZWMC#Administrator つ フーザーがロガオンルアにるときのみ実行する		
	□ パスワードを保存しない。タスクがアクセスできるのはローカル リソースのみ		
	最上位の特権で実行する	~	
	۲ III III III III III III III III III I	>	

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。

ø	ZWS Manager X
<ul> <li>ZWS Manager</li> <li>RAIDステータス</li> <li>HDDアンブラヴ</li> <li>本体FANと温度</li> <li>メール設定</li> </ul>	WS Manager Funcボタン設定 Funcボタン機能 アブリケーション C¥unlock_dbat Funcボタンを長押しした時に 起動するアブリケーションを指定します。

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。

💭 l 🕞 🏢 = l	PC		_ <b>_</b> ×
ファイル コンピューター	表示		~ 0
🔄 🕘 = 🕇 🌉 🕨 F	РС <b>•</b>	✓ C PCの検索	م
★ お気に入り ダウンロード デスクトップ 最近表示した場所	<ul> <li>▲ フォルダー (6)</li> <li>Øウンロード</li> </ul>	720147	
j∰ PC	٩< </td <td>ピカチャ</td> <td>ドライブ D: がない!</td>	ピカチャ	ドライブ D: がない!
<b>€</b> 79r7-2	<ul> <li>         ・ デバイスとドライブ (1)         <ul> <li>                  ーカル ディスク (C:)</li></ul></li></ul>	) 2501	
7個の項目			

#### 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。

Ъ			サー	バー マネージャー			_ 0 ×	¢
E		ム・記憶域プー	IL		• 🕲   🏲 🗑	哩(M) ツ−ル(工) 表	示(⊻) へレプ(且)	)
	サーバー ボリューム ディスク 記憶域プール 共有 iSCSI	<ul> <li>記憶域ブール すべての記憶域ブーパ</li> <li>フィルター</li> <li>名前</li> <li>StoragePool</li> </ul>	レ 合計:1 ク 種類 (1) 記憶域プール	<ul> <li>(副 ▼ (用) ▼</li> <li>管理者</li> <li>/ HDL-ZWMC</li> </ul>	利用可能 HDL-ZWMC	読み取り・書き込みサ	<u>\$75</u> ▼ ⊙ -/(- 審 2,	~
	-אוגע ע-ע	く 最終更新日 2014/03/33 仮想ディスク HDL-ZWMC 上の Storage	14:09:32 Pool	111 ( \$7.7) •	物理ディスク HDL-ZWMC上の StoragePoot	l	> \$7.5 •	
		フィルター え 冬前 状態 レイア・ ▲ VHD3 Simp ▲ VHD2 Mirro ▲ VHD1 Simp	ク ウト プロピジョング le 仮想 le 仮想	(畫) ▼ ● 2 会母 和約当て孫 100 GB 9.50 GB 100 GB 1.00 GB 100 GB 12.0 GB	スロット 名前 ▲ スロット 名前 PhysicalDisk0( PhysicalDisk1(	P (E)	▼	

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。

▲ 名前	種類	管理者	利用可能	読み取り-書き込みサーバー 容!
<ul> <li>Storage Spaces (1)</li> </ul>	)			
🛕 StoragePool	記憶域プーノ	記憶域プールの新規作成.		2.(
		仮想ディスクの新規作成		
		物理ディスクの追加		
		読み取り-書き込みアクセス	権の設定	
		記憶域プールのバージョンの	)アップグレード	
<		記憶域プールの削除		>
最終更新日 2014/03/31 15	:06:03	プロパティ		

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。

高 読み取	り/書き込みアクセス	マ用のサーバーの選択	× 🗖 – 5						
記憶域プールに対して読み取りと書き込みが許可されるサーバーを選択します( <u>S</u> ):									
サーバー名	状態	クラスターの役割	所有者ノード						
HDL-ZWMC	オンライン	非クラスター化							
		OK	キャンセル						

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**

Σ	管理者	ă: Windows PowerSh	ell	_ <b>□</b> X				
₩indows PowerShell Copyright (C) 2013	Microsoft Corporation	n. All rights reserv	ved.	<u>^</u>				
PS C:¥Users¥Administrator> Get-VirtualDisk								
FriendlyName	ResiliencySettingNa me	OperationalStatus	HealthStatus	IsManua Attac				
VHD1 VHD2 VHD3	Simple Mirror Simple	Detached Detached Detached	Unknown Unknown Unknown	True True True				
PS C:¥Users¥Admini PS C:¥Users¥Admini PS C:¥Users¥Admini PS C:¥Users¥Admini	strator> Set-VirtualD strator> Set-VirtualD strator> Set-VirtualD strator>	isk -IsManualAttach isk -IsManualAttach isk -IsManualAttach	\$False VHD1 \$False VHD2 \$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。

i de la companya de l	サーバーマネージャー								_	0	x
$ \mathbf{E} $		ーム・ディスク				• 🕲		里( <u>M) ツール(</u> I	〕 表示(⊻)	へいブ	(日)
	サーバー ボリューム デ <i>イスク</i> 記憶域ブール 共有 iSCSI ワークフォルダー	ディスク すべてのディスク   会計: 4 フィルター 整健 仮想ディスク 秋期 4 HDL-ZWMC (4) 0 オンライン 2 VHD1 オフライン 3 VHD2 オフライン	ク 容量 1.82 TB 100 GB 100 GB	(Ⅲ) ▼ 未割り当て 0.00 B 0.00 B	<ul> <li>用 ▼</li> <li><i>J(−¬¬+&gt;···</i></li> <li>GPT</li> <li>GPT</li> <li>GPT</li> </ul>	読み取り専用 <i>×</i> <i>×</i>	クラスター化	サブシステム Storage S… Storage S…	 パスの種類 SATA 記憶域 記憶域	マ 名前 ST3( VHD VHD	~
			::55 。 ア ビジョニング 定		■ 7 ▼ 計 ※ 計 結領域	<mark>2億域プール</mark> DL-ZWMC上の 証	) ST3000DM 増増成プールが限	001-9YN166 連付けられていまけ		>	
		C									~

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。

数値	仮想ディスク	1	犬態	容量	未割り当て	パーティシー	読み取り専用	クラスター化	サブシステム
▲	HDL-ZWM	1C (4	4)						
0		7	オンライン	1.82 TB	0.00 B	GPT			
2	VHD1		· //   ポリュー <i>レ</i> /			GPT	$\checkmark$		Storage S…
3	VHD2	_	MOT-TO	刀利7为311FDX。。		GPT	$\checkmark$		Storage S…
4	VHD3		オンライン	こする		GPT	V		Storage S…
			オフラインに	こする					-
			ディスクの	ノセット					

#### 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。

💻 l 🕞 🔝 = l	PC		_ 🗆 X
ファイル コンピューター	表示		~ 🕐
😔 🔿 🔻 🖬 🕨 P	C •	▼ C PCの検索	Q
☆ お気に入り ダウンロード デスクトップ 漫 最近表示した場所	▲ フォルダー (6) ↓ ダウンロード	デスクトップ	
PC	٩-٢٢ ا	ピクチャ	
📬 ネットワーク	र्टन	الروح التعاريق	
	▲ デバイスとドライブ (4) ローカル ディスク (C:) 空き領域 88.4 GB/97.6 GB 新しいポリューム (E:) 空き領域 99.2 GB/99.8 GB	ローカル ディスク (D:) 新しいポリューム (F:) 空き領域 91.7 GB/99.8 GB	
10 個の項目			HII 📰

全てのディスクが復元できたのを確認したら完了です。