富士通PCサーバ プライマジー
PRIMERGY

FUJITSU

PRIMERGY における BitLocker™ Drive Encryption の注意事項

Windows Server 2008 版

2010 年 10 月

富士通株式会社

shaping tomorrow with you

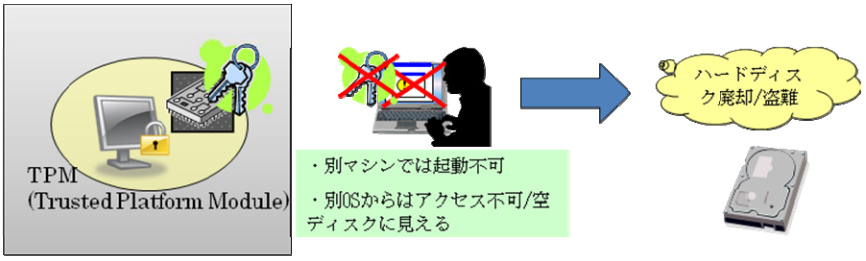
目次

はじめに

Windows Server 2008 にはシステムセキュリティ強化を目的とした BitLocker™ Drive Encryption（以降 BitLocker）機能が実装されています。当社 PC サーバ PRIMERGY では、Windows Server 2008 サポートと同期して、順次セキュリティチップ TPM(Trusted Platform Module)*1 を実装した機種*2 を出荷、BitLocker をサポートします。BitLocker では、システムボリュームおよびデータボリュームの暗号化*3を行うことができます。しかしながら、ハード保守時やシステム拡張時などに注意が必要となります。本書では、お客様が BitLocker をご使用になる場合の注意事項及びその対処方法を記載します。

*1：セキュリティチップ（TPM）とは

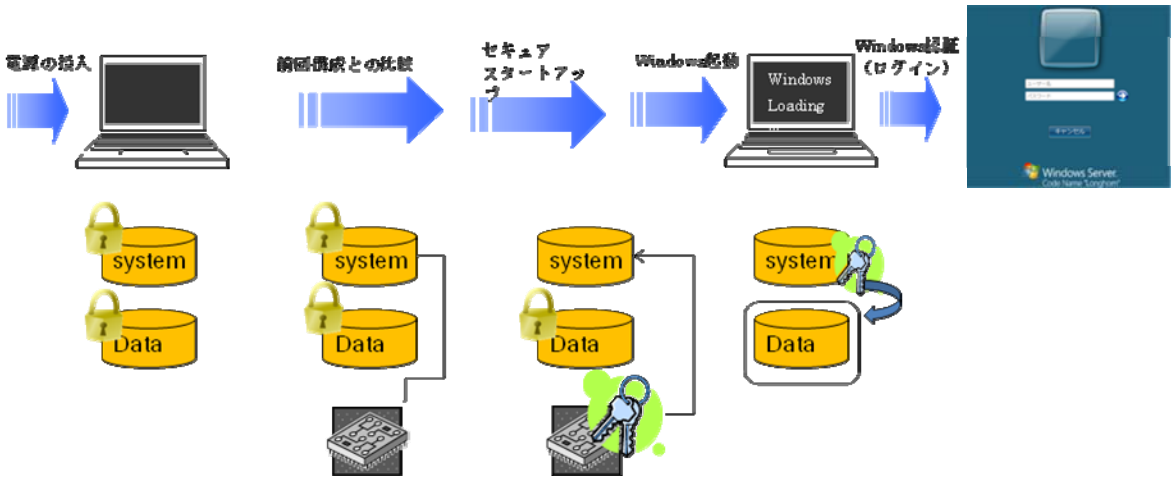
TPM とは TCG（Trusted Computing Group）が仕様を策定するセキュリティチップです。Windows Server 2008 の BitLocker 機能は、TPM と連携し、ハードウェアレベルのセキュリティ強化を実現します。



*2：各機種におけるTPM実装可否については、当社Windows Server 2008 サーバ本体動作確認状況 http://primeserver.fujitsu.com/primergy/software/windows/os/2008/hard.htmlをご参照下さい。

*3：BitLocker での暗号化とは

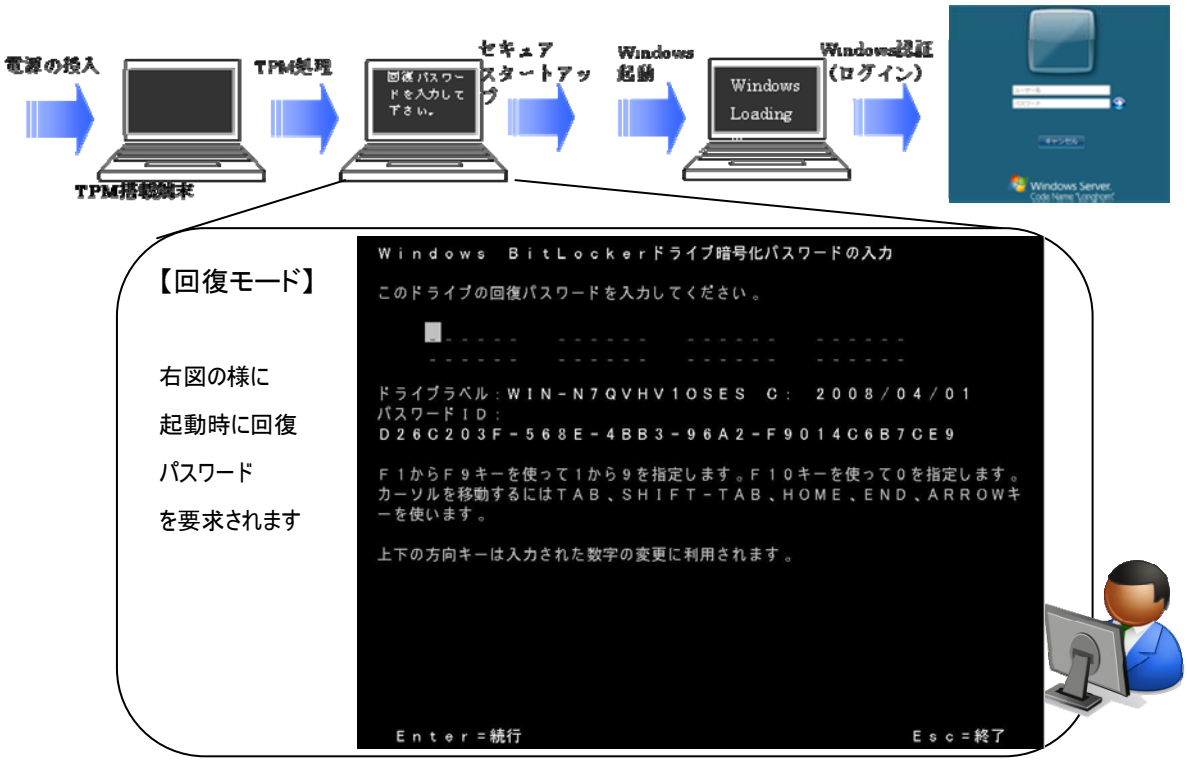
BitLocker はボリュームの暗号化を行います。システム起動時に、システム構成のチェックを行い前回起動時と同一環境からの起動が保証された場合に、TPM に格納されたキーよりシステムボリュームの復号を行い OS を起動します。



1　回復モード

BitLockerが有効なシステムでは、起動時にTPMと連動し、システム整合性チェックが行われます。ハード保守やシステム拡張後の起動時には、システム変更が検出され、回復パスワード入力を求める回復モードに移行します。システムの起動には、お客様が保持している回復パスワードを入力が必要です。

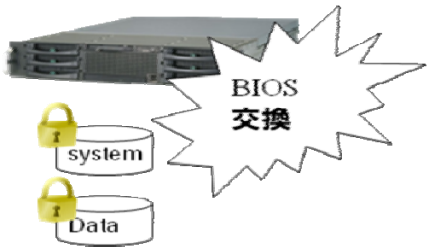
■ハード構成変更を検出し、回復モードに移行する



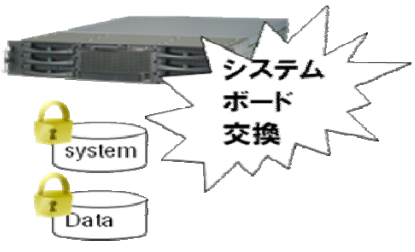
*48 桁の回復パスワードの入力が必要です。

回復モードに移行するハード構成変更の例

例1. システム BIOS の更新



例 2. TPM が搭載されている部品交換時*1



※1: TPM が搭載されている部品は機種により異なります(ベースボード、TPM モジュール等)

2　サーバ運用時の影響範囲

表 1 に、システム構成が変更された場合の例と影響範囲についてまとめます。表中の●の場合に回復モードに移行します。当社では、ハード保守作業時にあらかじめ、お客様ご自身で、BitLocker をオフにし、保守員が保守作業を実施後、再度お客様にてBitLockerをオンにしていただくことをお願いしております（BitLocker をオフにすることで回復モードへの移行を抑止できます）。次章以降詳細な手順を説明します。

表 1. 保守/ハード追加作業への影響（回復モード移行への移行有無）

対象部品 / 作業内容	ベースボード	CPU	メモリ	RAID *6	SAS HBA	SCSI	NIC	Fibre channel	バックアップデバイス	FDD	ODD	TPM モジュール*8
BIOS 版数変更/拡張 BIOS 版数変更	●	N/A	N/A	N/A	●	●	N/A	●	N/A	N/A	N/A	N/A
Firmware 版数変更	×	N/A	N/A	● *7	×	×	N/A	×	N/A	N/A	N/A	N/A
BIOS 設定変更/拡張 BIOS 設定変更	● *1	N/A	N/A	×	×	×	N/A	×	N/A	N/A	N/A	N/A
Firmware 設定変更	●	N/A	N/A	×	×	×	N/A	N/A	N/A	N/A	N/A	N/A
交換 (BIOS/Firmware の同一版数へ交換)	●	× *2	× *2	×	×	×	×	×	×	×	×	●
新規追加	×	×	×	●	●	●	● *4	●	×	×	×	×
増設追加	N/A	×	×	● *4	●	●	● *4	●	N/A	N/A	N/A	N/A
削除(HW 取り外し)	N/A	× *3	× *3	●	●	●	● *4	●	×	×	● *5	N/A
ドライバ変更	×	N/A	N/A	×	×	×	×	×	N/A	N/A	N/A	N/A

凡例：●：影響あり（回復モードへ移行する）、×：影響なし(回復モードへ移行しない)、N/A：該当なし

※：整合性チェック範囲：PCR 0,1,2,3,4,5,8,9,10,11 で確認した結果

補足

*1:設定が変更されると回復モードへ移行する項目

1)ブートオーダー、2)PCI スロットの拡張 ROM スキャン,3)BIOS Password／System Password

*2:ステッピングおよびベンダが異なる場合も、影響はありません

*3:縮退時も影響はありません。

*4:回復モードに移行せず、影響なしの場合もあります。

*5:システム BIOS 設定のブートオーダーの設定に影響を受けます。

・ODD が HDD より上位の順番では、回復モードへ移行します。

・回復モードに移行せず、影響なしの場合もあります。

*6: RAID 構成変更(アレイ構成追加)に、回復モードに移行する場合があります。
もともとアレイ構成のあるカード配下にロジカルドライブを作成した場合は影響ありません。ただし、追加搭載したカード配下に新規にロジカルドライブを作成すると「回復モードへ移行」する場合があります。

*7: Firmware 版数を変更した際、変更前および変更後の版数の組み合わせによって、影響がある場合と無い場合があります。

*8:TPM モジュール対象機種のみ。

用語の説明

・SAS HBA:

Serial Attached SCSI の略 ホストバスアダプター シリアル接続方式 SCSI 規格デバイス

・Fibre Channel:

コンピュータと周辺機器を接続するための規格。

・NIC

Network Interface Card の略。

・FDD

Floppy Disk Device の略。

・ODD

Optical Disk Device の略

・PCR

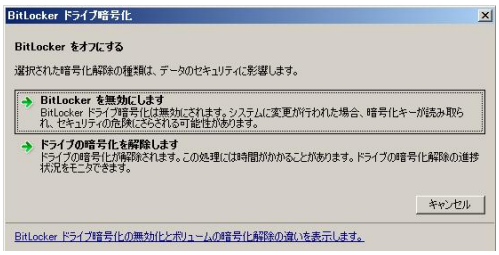
Platform Configuration Register の略 TPM 内にあるハッシュ値を保持する領域のこと。

3　保守作業前の対処

ハード保守作業や増設作業前に、BitLockerをオフにする手順について記載します。ただし、OS起動が出来ないような場合には、事前にオフにすることができないため、交換後回復パスワードを入力します。

注意　回復パスワードを紛失した場合、システムを再インストールする必要があります。

3.1 BitLockerをオフにする

1	[スタート]-[コントロールパネル]-[セキュリティ]-[BitLockerドライブ暗号化]　をクリックしてBitLocker の管理画面を起動します。	
2	システムボリューム（以下では　C　と想定）の[BitLocker　をオフにする]メニューをクリックします。	
3	BitLocker ドライブ暗号化のダイアログが表示されたら、[BitLocker を無効にします]を選択してください。	

Point！

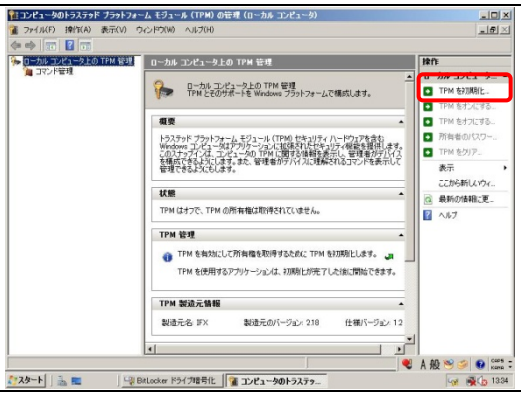
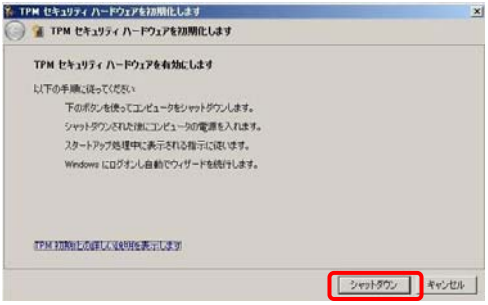
・システムボリュームの「BitLocker が有効」な場合にのみ、回復モードへ移行します。
　データボリュームの BitLocker をオフにする必要はありません。

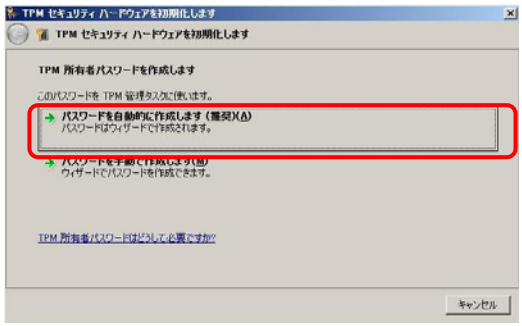
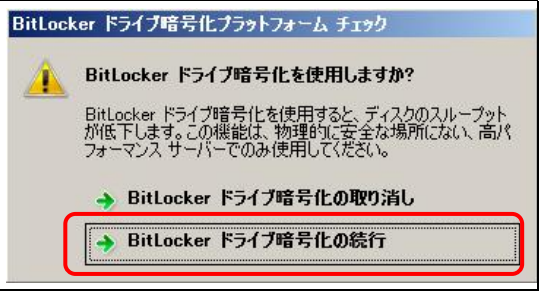
　なお、データボリュームでは、[ドライブ暗号化を解除する]のみが選択可能です。
　ドライブ暗号化を解除を選択した場合、再暗号化や回復パスワードの再取得が必要です。

4　保守作業後の復旧

ベースボードや TPM モジュール等、TPM が搭載されている部品を交換した場合は、TPM のパスワード情報がクリアされるため、PCI スロット/BIOS 交換への増設時とは復旧手順が異なり、新たに TPM 所有権を取得する必要があります。

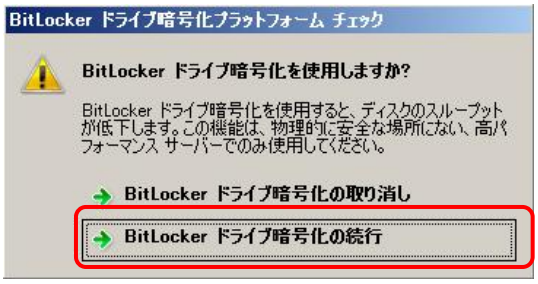
4.1 TPMが搭載されている部品を交換した時 ※1

1	サーバを起動します。 BitLocker をオフにしているため回復モードには移行せず、システムが起動します。	
2	[スタート]-[コントロールパネル]-[セキュリティ]-[BitLocker ドライブ暗号化]をクリックします。 [BitLocker ドライブ暗号化]の画面を表示されます。	
3	左下の[TPM の管理]をクリックします。 [コンピュータのトラステッドプラットフォームモジュール（TPM）の管理（ローカル コンピュータ）]の管理画面が表示されます。	
4	右ペインの[TPM を初期化]をクリックします。	
5	[TPM セキュリティハードウェアを初期化します]のダイアログより、[シャットダウン]をクリックし、システムをシャットダウンします。	

6	電源切断後、処理を続行するために電源を再投入します。 TPM が搭載されている部品を交換した場合、回復モードへ移行します。	
7	起動時にBIOS画面にて、TPMの初期化処理を続行するか確認されるので、[Execute]を選択します。	
8	OS ログイン後、[TPM セキュリティハードウェアを初期化します]ダイアログが再度表示されます。	
9	[パスワードを自動的に作成します]を選択し、TPM 所有者パスワードを保存します。	
	Point ・BitLocker ドライブ暗号化では、初期化プロセスを自動的に行っています。 初めて BitLocker ドライブ暗号化を有効にする場合に、TPM 所有者パスワードは自動的に作成され、BitLocker 回復パスワードと同じ場所に保存されています。 ・TPM 所有者パスワードのみ更新されます。[回復パスワード]は変更されません。	
10	[スタート]-[コントロールパネル]-[セキュリティ]-[BitLockerドライブ暗号化] をクリックします。 [BitLockerドライブ暗号化]の画面を表示されます。	
11	システムボリューム(C)の[BitLocker をオンにする]をクリックしてドライブを暗号化を再度有効にします。	
12	[BitLocker ドライブ暗号化プラットフォームチェック]のダイアログが表示されるので、[BitLocker ドライブ暗号化の続行]をクリックします。	

※1: TPM が搭載されている部品は機種により異なります(ベースボード、TPM モジュール等)

4.2 その他（PCIスロット増設時、BIOSブートオーダー変更時など）

1	[スタート]-[コントロールパネル]-[セキュリティ]-[BitLockerドライブ暗号化] をクリックします。 [BitLockerドライブ暗号化]の画面が表示されます。	
2	システムドライブ（C）の BitLocker 状態を[BitLocker をオンにする]をクリックしてドライブ暗号化を再度有効にします。	
3	[BitLockerドライブ暗号化プラットフォームチェック]のダイアログが表示されるので、[BitLockerドライブ暗号化の続行]をクリックします。	

5 【参考 1】PRIMERGYでのBitLockerの構築手順

1. 当該機種にて TPM をサポートの有無を確認します。
   http://primeserver.fujitsu.com/primergy/software/windows/os/2008/hard.html
2. 当該機種の電源を投入し、BIOS の設定を行います。
   1. サーバ本体の電源を入れます。
   2. POST 中、画面に「<F2> BIOS Setup / <F12> Boot Menu」と表示されたら、メッセージが表示されている間に【F2】キーを押します。
   3. 「Security」メニュー配下の「TPM (Security Chip) Setting」サブメニューを表示します。
   4. 「Security Chip」を「Enabled」に設定します。「Change TPM State」が表示されます。
   5. 「Change TPM State」を「Enable & Activate」に設定します。
   6. 「Exit」メニューを表示します。
   7. 「Save Changes & Exit」にカーソルを合わせて【Enter】キーを押します。
   8. 「Save configuration changes and exit now?」というメッセージが表示されたら「Yes」にカーソルを合わせて【Enter】キーを押します。
   9. 再起動後 BIOS セットアップユーティリティが自動的に起動します。
   10. 「Physical Presence operations」メニューで「Execute」を実行します。
3. 区画の準備をします。
   1. インストールディスクで起動します。
   2. アレイモデルをお使いの場合は、必要に応じてアレイコントローラのデバイスドライバをロードします。
      詳細は下記ドキュメントの Windows Server 2008 の「インストール手順」をご覧ください。
      http://primeserver.fujitsu.com/primergy/manual/pdf/common/ca92276-8158-04.pdf
   3. OS インストール画面で[コンピュータを修復する]を選択します。
   4. システム回復オプションで OS を選択せずに、[次へ]をクリックします
   5. [コマンドプロンプト]をクリックします。
   6. 下記コマンドを入力します
      1. diskpart
      2. select disk 0
      3. Clean
      4. create partition primary size = 1500
      5. assign letter = S
      6. Active
      7. create partition primary size = 20000

8 assign letter = C
9 Exit
10 format C: /y /q /fs:NTFS
11 format S: /y /q /fs:NTFS
12 Exit

上記の手順では区画は以下のように構成されています。

区画構成	
第一区画	Sドライブ（NTFS） 1.5GB アクティブに設定されています。 ここにブートローダなどが配置されます。
第二区画	Cドライブ（NTFS） 20GB

*サーバの用途や、ディスクの量に鑑み追加区画の作成や区画のサイズ変更をご検討ください。

7 画面右上の×ボタンを押し、画面を閉じます（シャットダウン、再起動はしない）。
8 [今すぐインストール]からインストール処理を続行します。
9 上記システム用のパーティション（Cドライブ,20GB）を指定しインストールします。

4 OS インストール完了後、BitLocker を有効にします。
1 サーバーマネージャの起動
[すべてのプログラム]→[管理ツール]→[サーバー マネージャ]をクリックします。
サーバーマネージャが起動します。
2 BitLocker を有効にします
サーバーマネージャの左ペインから[機能]をクリックし、機能の追加から[BitLockerドライブ暗号化]をチェックし、機能を有効（インストール）にします。
3 システム再起動
システム再起動後、BitLocker 機能が有効になります。

5 BitLocker をオンにして、ディスクを暗号化します。
1 [コントロールパネル]-[セキュリティ]-[BitLocker ドライブ暗号化]をダブルクリックします。BitLockerドライブ暗号化設定画面が表示されます。
2 システムボリュームを暗号化する場合、システムボリュームの[BitLocker をオンにする]をクリックします。
3 [回復パスワード]の画面にて、なるべく複数の方法で回復パスワードを保存し、[次へ]をクリックしてください。
4 データボリュームを暗号化する場合、データボリュームの[BitLocker をオンにする]をクリックします。
5 [回復パスワード]の画面にて、なるべく複数の方法で回復パスワードを保存し、[次へ]をクリックします。

Point

・BitLocker を初めてオンにする場合、暗号化処理の初期化が行われます。このため、ディスクの容量および利用頻度によっては初期化完了までに時間がかかります。ディスクの回転数や構成などにも依存しますが、10GB の空パーティションの暗号化に 10 分程度かかる場合があります。

・暗号化処理は複数のドライブに対して同時実行可能です。

・暗号化/解除の処理を中断した場合、「暗号化オフ」の状態になります。

・BitLocker の暗号化を解除する場合も、完了までに時間がかかります。ディスクの構成などに依存しますが、暗号化の解除には、暗号化を実行する場合と同等かそれ以上の時間がかかる場合があります。

6 【参考 2】TPMクリア手順

下記に TPM 設定を工場出荷時の状態する手順を示します。BitLocker による暗号化機能の運用中は、作業を実施しないでください。

1 サーバ本体の電源を入れます。
2 POST 中、画面に「<F2> BIOS Setup / <F12> Boot Menu」と表示されたら、メッセージが表示されている間に【F2】キーを押します。
3 「Security」メニュー配下の「TPM (Security Chip) Setting」サブメニューを表示します。
[Current TPM Status] の項目に[Enabled & Activated] 以外が表示されている場合は、ご購入時の状態に戻すことはできません。TPM を有効にしてから行ってください。
4 「Change TPM State」を「Clear」に設定します。
5 「Exit」メニューを表示します。
6 「Save Changes & Exit」にカーソルを合わせて【Enter】キーを押します。
7 「Save configuration changes and exit now?」というメッセージが表示されたら「Yes」にカーソルを合わせ【Enter】キーを押します。
8 再起動後 BIOS セットアップユーティリティが自動的に起動します。
9 「Physical Presence operations」メニューで「Execute」を実行します。
TPM がクリアされ、サーバが再起動されます。

7 【参考 3】保守作業前の対処（Server Coreインストールの場合）

7.1 BitLockerをオフにする。

1 管理者のコマンドプロンプトで以下のコマンドを実行し、状態を確認します。

cscript manage-bde.wsf –status

以下のような画面が表示されることを確認します。

BitLocker ドライブ暗号化で保護可能なディスク ボリューム:

ボリューム C: []

[OS ボリューム]

サイズ: xx.xx GB

変換状態: 完全に暗号化されました

暗号化された割合: 100%

暗号化の方法: ディフューザ付き AES 128

保護状態: 保護はオンです

ロック状態: ロックは解除されています

キーの保護機能:

外部キー

数字パスワード

TPM

保護状態(下線)がオンの場合、BitLocker がオンの状態であることを示します。

2 以下のコマンドを実行し、BitLocker をオフにします。

cscript manage-bde.wsf –protectors –disable C:

8 【参考 4】保守作業後の復旧（Server Coreインストールの場合）

8.1 TPMが搭載されている部品を交換した時 ※1

1 管理者のコマンドプロンプトにて、以下のコマンドを実行し、TPM を有効/アクティブ化します。

cscript manage-bde.wsf –tpm –TurnOn

以下のような画面が表示されます、画面の手順に従い作業を進めます。

TPM を有効にするには、次の手順に従う必要があります。

1. コンピュータをシャットダウンします。
   (手順については、コマンド ラインに「shutdown /?」と入力してください。)
2. コンピュータを手動で再起動します。
3. ブート画面に表示される指示に従います。

---

2 以下のコマンドを実行し、システムをシャットダウンします。

shutdown /s /t 0

3 起動時に BIOS 画面にて、TPM の初期化処理を続行するか確認されるので、[Execute]を選択します。

4 ログイン後、管理者のコマンドプロンプトから、以下のコマンドを実行し、TPM パスワードの設定と、TPM の所有権の取得を行います。

cscript manage-bde.wsf –tpm –TakeOwnerShip XXXXX

XXXX には、8 文字以上の任意のパスワードを指定します。

Server Core インストールでは、TPM パスワードの OS 自動生成はオプションはありません。必ず任意の 8 文字以上のパスワードを指定してください。

5 以下のコマンドを実行し、暗号化を有効にします。

cscript manage-bde.wsf –protectors –enable C:

TPM が搭載されている部品の交換時以外の場合は、手順 5 のみを行います。

※1: TPM が搭載されている部品は機種により異なります(ベースボード、TPM モジュール等)

富士通 PC サーバ PRIMERGY につきましては、以下にて技術情報を参照できます。

・PC サーバ PRIMERGY
http://primeserver.fujitsu.com/primergy/

・PC サーバ PRIMERGY 機種比較表
http://primeserver.fujitsu.com/primergy/catalog/select-spec/

・サーバ選定ガイド
http://primeserver.fujitsu.com/primergy/technical/select-model/

富士通 PC サーバ PRIMERGY のお問い合わせ先。

・PC サーバ PRIMERGY（プライマジー）のお問い合わせ
http://primeserver.fujitsu.com/primergy/contact/

本コンテンツの記載内容は、掲載時点での情報をもとに構成されています。あらかじめご了承ください。 最新の機器情報は PRIMERGY サイトで、ご確認ください。 また、本書の利用に起因するいかなるトラブル・損害が発生しても、富士通株式会社はその責を負いません。