FUJITSU Server PRIMERGY
FUJITSU Server PRIMEQUEST

PRIMERGY/PRIMEQUEST における BitLocker™ Drive Encryption の 注意事項

Windows Server 2012 版

第 1.2 版

2015 年 5 月

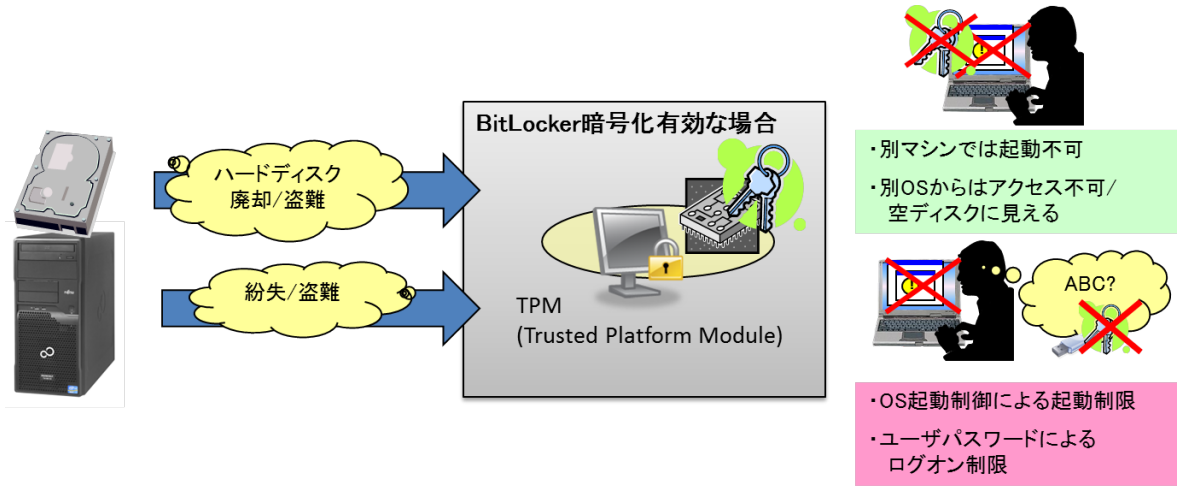
富士通株式会社

はじめに

Windows Server 2012 にはシステムセキュリティ強化を目的とした BitLocker™ ドライブ暗号化（以降 BitLocker）機能が実装されています。FUJITSU Server PRIMERGY / FUJITSU Server PRIMEQUEST では、セキュリティチップ(TPM)*1を実装した機種にて BitLocker をサポートします。
FUJITSU Server PRIMERGY 各機種における TPM 実装可否については、「FUJITSU Server PRIMERGY システム構成図」をご参照ください。
FUJITSU Server PRIMEQUEST においては、2000 シリーズのみ TPM 実装可能です。「PRIMEQUEST 2000 シリーズ ハードウェアマニュアル」をご参照ください。

BitLocker は、システムボリュームとデータボリューム、およびリムーバブルディスクの暗号化を行えますが、システムボリューム暗号化では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およ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(Trusted Platform Module)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 2012 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。



参考資料

本書以外の Windows Server 技術情報は、以下のサイトで公開しています。

・Windows システム構築ガイド(PRIMERGY)
http://jp.fujitsu.com/platform/server/primergy/technical/construct/
・Windows ガイド(PRIMEQUEST)
http://jp.fujitsu.com/platform/server/primequest/products/2000/catalog/guide/windows/

PRIMERGY の BIOS 設定に関する詳細は、以下から該当機種のマニュアルを参照してください。

・FUJITSU Server PRIMERGY マニュアル
http://jp.fujitsu.com/platform/server/primergy/manual/

PRIMEQUEST の UEFI(BIOS)設定に関する詳細は、以下のマニュアルを参照してください。

・PRIMEQUEST 2000 シリーズ ハードウェアマニュアル
http://jp.fujitsu.com/platform/server/primequest/manual/2000/

注意事項

本ドキュメントを輸出または第三者へ提供する場合は、お客様が居住する国および米国輸出管理関連法規等の規制をご確認のうえ、必要な手続きをおとりください。

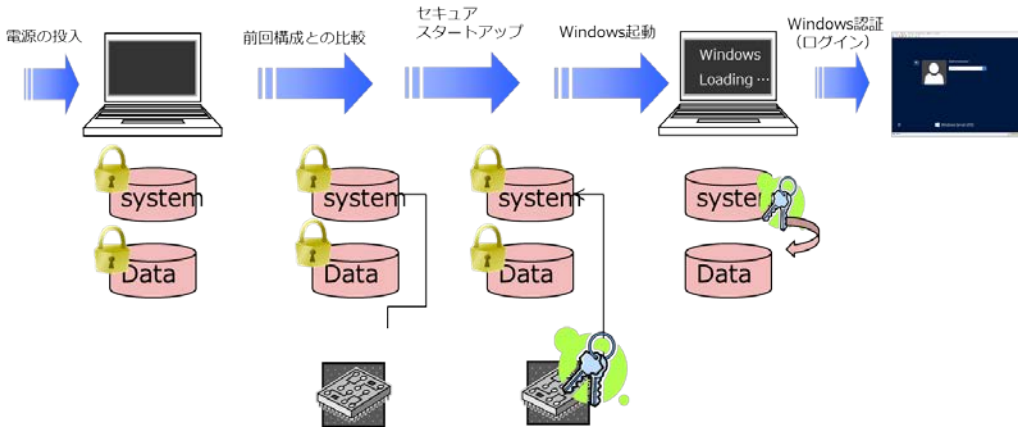
改版履歴

改版日時	版数	改版内容
2012.11	1.0	・新規作成
2014.6	1.1	・PRIMEQUEST 情報を追加
2015.5	1.2	・OS インストール手順に ServerView Installation Manager 情報追加 ・BitLocker 構築手順に再起動の手順を追加

目次

1　BitLocker による暗号化と復号化

BitLocker が有効なシステムでは、システム起動時にシステム整合性チェックが行われます。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 に格納された暗号化キーによりシステムボリュームの復号を行い Windows を起動します。また、データボリュームの復号は、Sysvol 内に保存されたキーを利用して自動解除されます*2。



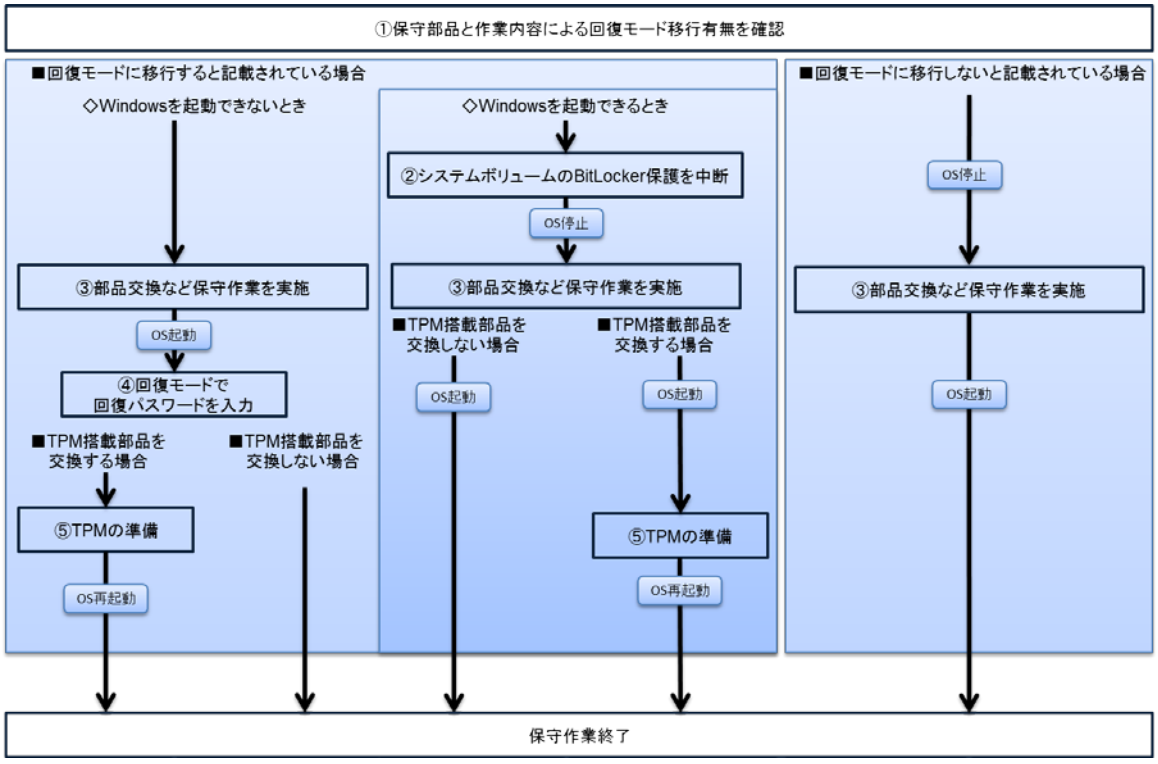
2 パスワードやスマートカードを利用した暗号化の解除も可能です。

2　保守手順

2.1 手順概要

保守作業の流れは下図のとおりです。保守部品の種類と作業内容や、Windows が起動する状態かどうか、システムボリュームの暗号化が解除/中断されているかどうか、あるいは、TPM が搭載されている部品を交換するのかどうかで、以下のように保守手順が異なります。

なお、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 保護を中断し、保守員が保守作業を実施後、再度お客様にて BitLocker 保護を再開していただくことをお願いしています。作業の詳細は次項で説明します。



2.2 保守部品と作業内容による回復モードへの移行有無の確認

まず最初に、保守部品と作業内容について、回復モードへの移行があるかないかを下表を参照して確認してください。表中の●の場合に回復モードへ移行します。回復モードについては「2.4 回復モードにおける回復パスワードの入力」を参照してください。

なお、ハード構成変更前にシステムボリュームの BitLocker 保護を中断しておくことで、回復モードへの移行を抑止できます。BitLocker 保護の中断については「2.3 システムボリュームの BitLocker 保護を中断」を参照してください。

表 1. PRIMERGY での保守/ハード追加作業への影響（回復モードへの移行有無）

部品 / 作業内容	ﾍﾞｰｽﾎﾞｰﾄﾞ変更	CPU	ﾒﾓﾘ	RAID *3	SAS HBA	SCSI	NIC	Fibre channel	ﾊﾞｯｸｱｯﾌﾟﾃﾞﾊﾞｲｽ	ODD	TPM ﾓｼﾞｭｰﾙ
BIOS版数変更/拡張 BIOS 版数変更	●	N/A	N/A	N/A	●	●	●	●	N/A	N/A	N/A
Firmware 版数変更	×	N/A	N/A	● *4	×	×	×	×	×	×	N/A
BIOS設定変更/拡張 BIOS 設定変更	● *5	N/A	N/A	×	×	×	●	● *6	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
交換(BIOS/Firmware の同一版数へ交換)	●	× *7	× *7	×	×	×	×	×	×	×	●
新規追加	×	×	×	●	●	●	● *6	● *6	● *8	● *8	×
増設追加	N/A	×	×	● *6	●	●	● *6	● *6	N/A	N/A	N/A
削除(HW 取り外し)	N/A	× *9	× *9	●	●	●	● *6	● *6	×	● *8	●
ドライバ変更	×	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

3 RAID 構成を変更した際に回復モードに移行する場合があります。

4 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。

5 次の項目は、設定が変更されると回復モードへ移行します。
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
ただし、2)、3)については搭載カードの種類や装置により、回復モードに移行せず、影響なしの場合もあります

6 回復モードに移行せず、影響がない場合もあります。

7 ステッピングおよびベンダーが異なる場合も、影響はありません。

8 システム BIOS 設定のブートオーダの設定で、HDD より優先度が高いと回復モードへ移行します。

9 縮退時も影響はありません。

表 2. PRIMEQUEST における保守/ハード追加作業への影響（回復モードへの移行有無）

部品 / 作業内容	SB					IOU_1GbE /IOU_10GbE		DU		PCI Box		MMB
		CPU	メモリ	BMC	RAID *10		PCI Card		RAID *10		PCI Card	
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	●	N/A
BIOS 設定変更/拡張 BIOS 設定変更	● *11	N/A	N/A	N/A	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	N/A	×	● *12	N/A	● *12	N/A	● *12	N/A	● *12	×
Firmware 設定変更	N/A	N/A	N/A	×	×	N/A	×	N/A	×	N/A	×	● *13
交換 (BIOS/Firmware の同一版数へ交換)	● *14	× *15	× *15	N/A	×	N/A	×	N/A	×	N/A	×	N/A
新規追加	● *16	×	×	N/A	●	● *16	● *16	N/A	●	● *16	● *16	×
増設追加	● *16	×	×	N/A	N/A	● *16	● *16	N/A	●	● *16	● *16	×
削除(HW 取り外し)	● *16	× *17	× *17	N/A	●	● *16	● *16	N/A	●	● *16	● *16	×
ドライバ変更	×	N/A	N/A	N/A	×	N/A	×	N/A	×	N/A	×	N/A

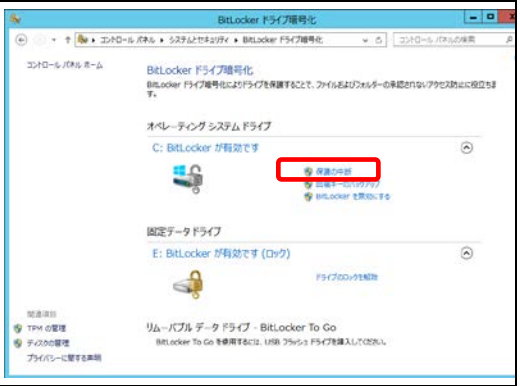
凡例：●：影響あり（回復モードへ移行する）、×：影響なし（回復モードへ移行しない）、N/A：該当なし

10 RAID 構成を変更した際に回復モードに移行する場合があります。
11 次の項目は、設定が変更されると回復モードへ移行します。
1)ブートオーダー、2)PCI スロットの拡張 ROM スキャン
ただし、2)については搭載カードの種類や装置により、回復モードに移行せず、影響なしの場合もあります。
12 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。
13 MMB Firmware で対象 Partition に以下の作業を行った場合に回復モードに移行します。
1)Partition 構成変更(SB や I/O リソースの追加/削除)、2)Backup/Restore BIOS Configuration
14 Home SB が対象で、以下の事象が発生した時(TPM チップそのものが変更された時)に回復モードに移行します。
1)Home SB の交換、2)Home SB 指定変更
また、BitLocker 利用時においては Reserved SB 機能は利用不可です。
15 ステッピングおよびベンダーが異なる場合も、影響はありません。
16 回復モードに移行せず、影響がない場合もあります。
17 縮退時も影響はありません。

2.3 システムボリュームのBitLocker保護を中断

Windows が起動する場合には、回復モードでのパスワードの入力作業を省略するため、ハード保守作業や増設作業前に、BitLocker 保護を中断することをお勧めします。システムボリュームの BitLocker 保護を中断する手順について、GUI による手順と PowerShell による手順を示します。

2.3.1 BitLocker の保護を中断する[GUI による手順]

1	検索チャームで“コントロール パネル”と入力します。コントロール パネルで、[システムとセキュリティ]-[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	システムボリューム（以下では C と想定）の[保護の中断]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、[はい]をクリックします。	

Point！

システムボリュームの「BitLocker が有効」な場合に回復モードへ移行します。不要なトラブルを避けるためにも保守作業前には、システムボリュームの BitLocker 保護を中断することをお勧めします。また、BitLocker 保護を中断することで、BitLocker の無効化と有効化に要する時間を節約するメリットもあります。なお、保守作業時にはデータボリュームの BitLocker 暗号化を解除する必要はありません。

2.3.2 BitLocker の保護を中断する［PowerShell による手順］

1　管理者の PowerShell で Get-BitLockerVolume コマンドを実行し、Protection Status が On 表示されていることを確認します。

```
PS C:¥Users¥Administrator> Get-BitLockerVolume


   ComputerName: WIN-8ALL0A8S2LS

VolumeType      Mount Point CapacityGB VolumeStatus          Encryption Percentage KeyProtector            AutoUnlock Enabled Protection Status
----------      ----------- ---------- ------------          ---------- ----------- ------------            ------------------ ----------
Data            E:            99.87 FullyDecrypted        0                      {}                                        Off
OperatingSystem C:           226.93 FullyEncrypted        100                    {Tpm, RecoveryPassword}                   On
```

Protection Status が On 表示の場合、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 の保護を中断します。

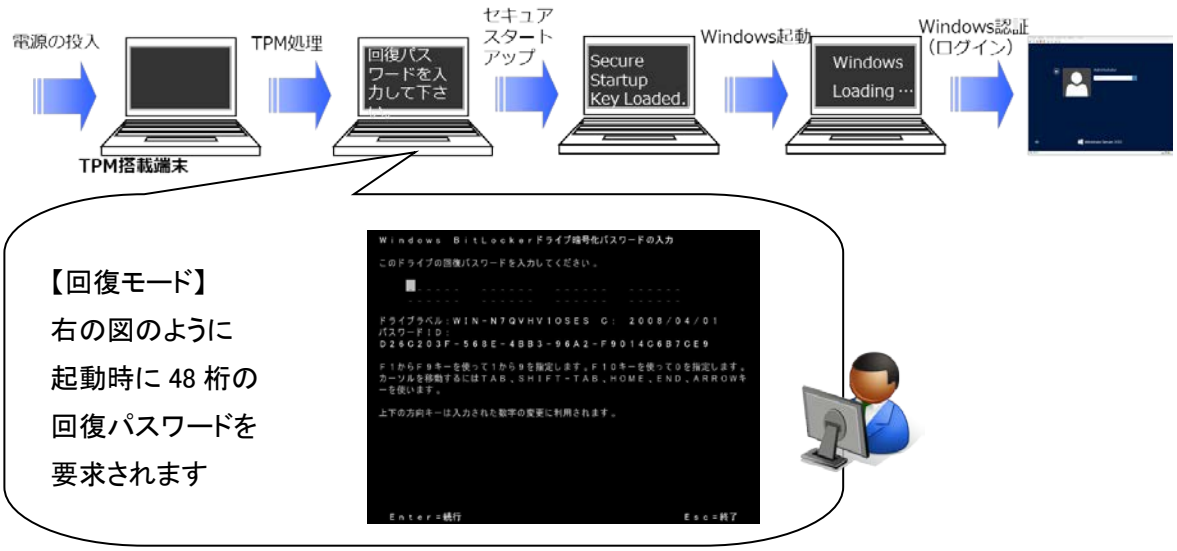
Suspend-BitLocker C:

2.4 回復モードにおける回復パスワードの入力

システム起動時のシステム整合性チェックで不整合が見つかったり、「2.2 保守部品と作業内容による回復モードへの移行有無の確認」で回復モードへの移行がみとめられる作業を行う場合には、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の入力が必要です。

注意　回復モードが起動した状態において、回復パスワードを紛失していた場合、システムを再インストールする必要があります。

■ハード構成変更を検出し、回復モードに移行する

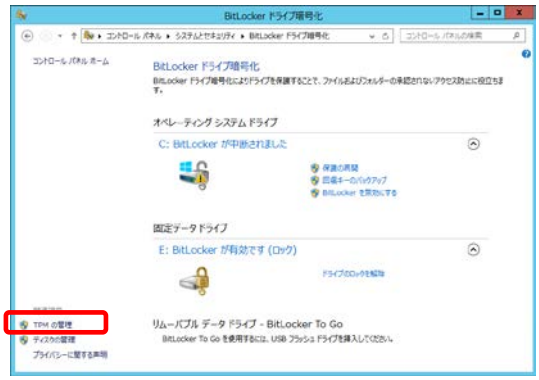
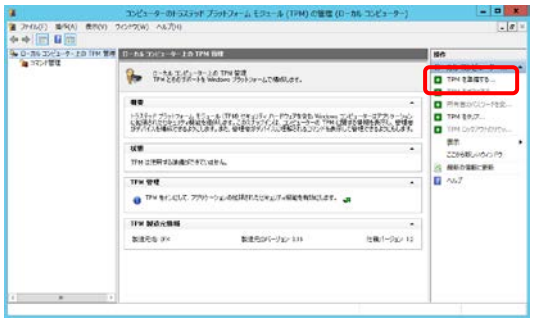


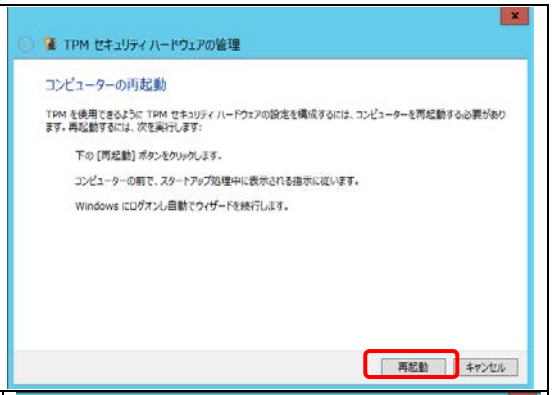
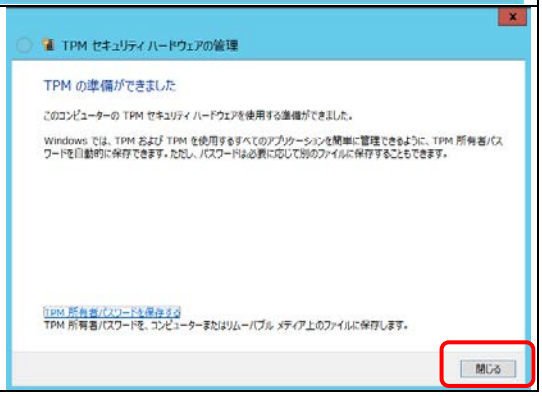
2.5 TPMの準備

PCI スロットのカード増設や BIOS ブートオーダー変更時には、『2.3 システムボリュームの BitLocker 保護を中断』の手順後に、Windows Server 2012 が再起動すると、自動的に保護が再開されます。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、新たに TPM 所有権を取得する必要があります。

以下に GUI による手順と PowerShell による手順を示します。なお、本手順の後に、システムボリュームの BitLocker 保護は自動的に再開されます。

2.5.1 TPM が搭載されている部品を交換した場合[GUI による手順]

1	サーバを起動します。 BitLocker を中断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	検索チャームで“コントロール パネル”と入力します。コントロール パネルで、[システムとセキュリティ]-[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。	
3	左下の[TPM の管理]をクリックします。	
4	右ペインの[TPM を準備する]をクリックします。	

5	[TPM セキュリティハードウェアの管理]のダイアログが表示されたら、[再起動]をクリックします。*18	
6	OS ログイン後、[TPM セキュリティハードウェアの管理]ダイアログが表示されたら、[閉じる]をクリックします。 自動的に BitLocker 保護が再開されます。	

Point！

・TPM 所有者パスワードのみ更新されます。この時、[回復パスワード]は更新されないため、既存の回復パスワードをそのまま利用できます。

[18] 機種によっては再起動時の POST 画面上で BitLocker を有効にするかを確認する画面が表示される場合があります。【F10】キーを押下し、お進みください。

2.5.2 TPM が搭載されている部品を交換した場合[PowerShell による手順]

1　管理者の PowerShell 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。

Initialize-TPM -AllowPhysicalPresense

以下のような画面が表示されます。

```
-------------------------------------------
TpmReady                    :False
RestartRequired             :True
ShutdownRequired            :False
ClearRequired               :False
PhysicalPresenceRequired    :True
-------------------------------------------
```

2　以下のコマンドを実行し、システムを再起動します。*[19]

shutdown /r /t 0

3　再起動します。

4　ログイン後、管理者の PowerShell 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。

ConvertTo-TPMOwnerAuth xxxxxx | Set-TPMOwnerAuth

以下のような画面が表示されます。

```
-------------------------------------------
TpmReady              :True
TpmPresent            :True
ManagedAuthLevel      :Full
OwnerAuth             :yyyyyyyyyyyyyyy
OwnerClearDisabled    :True
AutoProvisioning      :  Enabled
LockedOut             :False
SelfTest              :  {191, 191, 245, 191...}
-------------------------------------------
```

xxxxxxxx には、8 文字以上の任意のパスワードを指定します。

yyyyyyyyyyyyyyy には、xxxxxxxx から生成された文字列が表示されます。

[19] 機種によっては再起動時の POST 画面上で BitLocker を有効にするかを確認する画面が表示される場合があります。【F10】キーを押下し、お進みください。

参考 1　PRIMERGY での BitLocker の構築手順

1　当該機種の電源を投入し、BIOS の設定を行います*[20]。

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)　「Advanced」メニュー配下の「Trusted Computing」サブメニューを表示します。

4)　「TPM State」を「Enabled」に設定します。

5)　【F4】キーを押して、Save ＆ Exit に対して「yes」にカーソルを合わせて【Enter】キーを押します。

6)　再起動します。*[21]

2　OS をインストールします。

ServerView Installation Manager または手動インストールマニュアルを利用して、OS インストール作業を行ってください。

3　OS インストール完了後、BitLocker を追加します。

1)　サーバー マネージャーの起動

検索チャームで“サーバー マネージャー”と入力します。

2)　BitLocker を追加

サーバー マネージャーのダッシュボードから[役割と機能の追加]をクリックし、役割と機能の追加ウィザードを起動します。ウィザードの[機能の選択]画面にて[BitLocker ドライブ暗号化]をクリックします。この時、関連する役割サービスまたは機能もインストールしてウィザードを終了します。

3)　システム再起動

4)　もう一度、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。

4　BitLocker を有効にして、ディスクを暗号化します。

1)　BitLocker ドライブ暗号化の起動

検索チャームで“コントロール パネル”と入力します。コントロール パネルで、[システムとセキュリティ]-[BitLocker ドライブ暗号化]をクリックします。

2)　システムボリュームの暗号化

---

[20] 機種によっては BIOS メニューの名称が異なる場合があります。詳細は各機種の「BIOS セットアップユーティリティリファレンスマニュアル」を参照ください。対象のマニュアルは PRIMERGY サーバに付属の ServerView Suite DVD 2 または以下の URL から入手できます。
http://jp.fujitsu.com/platform/server/primergy/manual/

[21] 機種によっては再起動時の POST 画面上で BitLocker を有効にするかを確認する画面が表示される場合があります。【F10】キーを押下し、お進みください。

システムボリュームの[BitLocker を有効にする]をクリックします。

3) 回復キーの保存

[回復キーのバックアップ方法を指定してください]の画面にて、なるべく複数の方法で回復キーを保存し、[次へ]をクリックします。

4) 暗号化範囲の選択

[ドライブを暗号化する範囲]の画面にて、使用済の領域のみを暗号化するか、ドライブ全体を暗号化するかを選択します。

- 使用済の領域を暗号化する場合
  新しいドライブや新しい PC を暗号化する場合に適しています。新しいデータを追加すると、BitLocker によって自動的に暗号化されます。
- ドライブ全体を暗号化する場合
  運用中のドライブを暗号化する場合に適しています。ドライブ全体を暗号化すると、削除したにもかかわらず復旧可能な情報が残っているデータを含め、すべてのデータが暗号化されます。

5) システムチェック実行の選択

[このドライブを暗号化する準備ができましたか？]の画面にて、BitLocker システムチェックを実行する場合は、画面の指示に従ってください。

回復キーと暗号化キーが正しく読み取れることを確認する処理なため、実行することをお勧めします。

6) データボリュームの暗号化

データボリュームの[BitLocker を有効にする]をクリックします。

7) ロック解除方法の選択

[スタートアップ時にドライブのロックを解除する方法を選択する]の画面にて、データボリュームのロックの解除方法を選択します。

8) 回復キーの保存

[回復キーのバックアップ方法を指定してください]の画面にて、なるべく複数の方法で回復キーを保存し、[次へ]をクリックします。

9) 暗号化範囲の選択

[ドライブを暗号化する範囲]の画面にて、使用済の領域のみを暗号化するか、ドライブ全体を暗号化するかを選択します。

10) システムを再起動します。

Point！

・使用済みの領域を暗号化する場合

BitLocker を初めて有効にするとき、暗号化処理の初期化が行われます。このため、使用済の領域が多ければ初期化完了までに時間がかかり、使用済の領域が少なければ短時間で初期化が完了します。

・ドライブ全体を暗号化する場合
ディスクの回転数や構成などにも依存しますが、100GB のパーティションの暗号化に 25 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、「暗号化無効」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。

参考 2　PRIMEQUEST での BitLocker 構築手順

1　当該機種の電源を投入し、BIOS の設定を行います*[22]。

1)　パーティションの電源を投入します。

2)　POST 中、画面に Fujitsu ロゴが表示されたら、Fujitsu ロゴが表示されている間に何かキーを押します。

3)　「DeviceManager」メニュー配下の「Security Configuration」サブメニューを表示します。

4)　「TPM Support」を「Enabled」に設定します。

5)　「TPM State」を「Enabled」に設定します。

6)　「Commit Changes and Exit」にカーソルを合わせて【Enter】キーを押します。

7)　再起動します。*[23]

2　OS をインストールします。

ServerView Installation Manager または手動インストールマニュアルを利用して、OS インストール作業を行ってください。

3　OS インストール完了後、BitLocker を追加します。

1)　サーバー マネージャーの起動

検索チャームで“サーバー マネージャー”と入力します。

2)　BitLocker を追加

サーバー マネージャーのダッシュボードから[役割と機能の追加]をクリックし、役割と機能の追加ウィザードを起動します。ウィザードの[機能の選択]画面にて[BitLocker ドライブ暗号化]をクリックします。この時、関連する役割サービスまたは機能もインストールしてウィザードを終了します。

3)　システム再起動

4)　もう一度、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。

4　BitLocker を有効にして、ディスクを暗号化します。

1)　BitLocker ドライブ暗号化の起動

---

[22] 機種によっては BIOS メニューの名称が異なる場合があります。詳細は、PRIMEQUEST2000 シリーズのハードウェアマニュアル「運用管理ツールリファレンス」を参照してください。対象のマニュアルは以下の URL から入手できます。

http://jp.fujitsu.com/platform/server/primequest/manual/2000/

[23] 機種によっては再起動時の POST 画面上で BitLocker を有効にするかを確認する画面が表示される場合があります。【F10】キーを押下し、お進みください。

検索チャームで“コントロール パネル”と入力します。コントロール パネルで、[システムとセキュリティ]-[BitLocker ドライブ暗号化]をクリックします。

2) システムボリュームの暗号化
システムボリュームの[BitLocker を有効にする]をクリックします。

3) 回復キーの保存
[回復キーのバックアップ方法を指定してください]の画面にて、なるべく複数の方法で回復キーを保存し、[次へ]をクリックします。

4) 暗号化範囲の選択
[ドライブを暗号化する範囲]の画面にて、使用済の領域のみを暗号化するか、ドライブ全体を暗号化するかを選択します。
- 使用済の領域を暗号化する場合
新しいドライブや新しい PC を暗号化する場合に適しています。新しいデータを追加すると、BitLocker によって自動的に暗号化されます。
- ドライブ全体を暗号化する場合
運用中のドライブを暗号化する場合に適しています。ドライブ全体を暗号化すると、削除したにもかかわらず復旧可能な情報が残っているデータを含め、すべてのデータが暗号化されます。

5) システムチェック実行の選択
[このドライブを暗号化する準備ができましたか？]の画面にて、BitLocker システムチェックを実行する場合は、画面の指示に従ってください。
回復キーと暗号化キーが正しく読み取れることを確認する処理なため、実行することをお勧めします。

6) データボリュームの暗号化
データボリュームの[BitLocker を有効にする]をクリックします。

7) ロック解除方法の選択
[スタートアップ時にドライブのロックを解除する方法を選択する]の画面にて、データボリュームのロックの解除方法を選択します。

8) 回復キーの保存
[回復キーのバックアップ方法を指定してください]の画面にて、なるべく複数の方法で回復キーを保存し、[次へ]をクリックします。

9) 暗号化範囲の選択
[ドライブを暗号化する範囲]の画面にて、使用済の領域のみを暗号化するか、ドライブ全体を暗号化するかを選択します。

10) システムを再起動します。

Point！

・使用済みの領域を暗号化する場合

BitLocker を初めて有効にするとき、暗号化処理の初期化が行われます。このため、使用済の領域が多ければ初期化完了までに時間がかかり、使用済の領域が少なければ短時間で初期化が完了します。

・ドライブ全体を暗号化する場合

ディスクの回転数や構成などにも依存しますが、100GB のパーティションの暗号化に 25 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、「暗号化無効」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。

・Home SB が対象で、以下の事象が発生した時(TPM チップそのものが変更された時)に回復モードに移行します。

1)Home SB の交換、2)Home SB 指定変更

また、BitLocker 利用時においては Reserved SB 機能は利用不可です。

参考 3　PRIMERGY での TPM クリア手順

以下に TPM 設定を工場出荷時の状態する手順を示します。最初に BitLocker による暗号化を解除または中断してください。その後、以下の手順を実施してください*[24]。

1　サーバ本体の電源を投入します。
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　「Advanced」メニュー配下の「Trusted Computing」サブメニューを表示します。
4　「TPM State」を「Clear」に設定します。
5　【F4】キーを押して、Save & Exit に対して「yes」にカーソルを合わせて【Enter】キーを押します。
6　TPM がクリアされ、サーバが再起動されます。

[24] 機種によっては BIOS メニューの名称が異なる場合があります。詳細は各機種の「BIOS セットアップユーティリティリファレンスマニュアル」を参照ください。対象のマニュアルは PRIMERGY サーバに付属の ServerView Suite DVD 2 または以下の URL から入手できます。
http://jp.fujitsu.com/platform/server/primergy/manual/

参考 4　PRIMEQUEST での TPM クリア手順

以下に TPM 設定を工場出荷時の状態する手順を示します。最初に BitLocker による暗号化を解除または中断してください。その後、以下の手順を実施してください*[25]。

1　パーティションの電源を投入します。
2　POST 中、画面にFujitsuロゴが表示されたら、Fujitsu ロゴが表示されている間に何かキーを押します。
3　「Device Manager」メニュー配下の「Security Configuration」サブメニューを表示します。
4　「Pending TPM operation」を「TPM Clear」に設定します。*[26]
5　「Commit Changes and Exit」にカーソルを合わせて【Enter】キーを押します。
6　再起動します。
7　BIOS 画面にて、TPM のクリア処理を行うために、【F12】キーを押します。
8　TPM がクリアされ、サーバが再起動されます。

[25] 機種によっては BIOS メニューの名称が異なる場合があります。詳細は、PRIMEQUEST 2000 シリーズのハードウェアマニュアル「運用管理ツールリファレンス」を参照してください。対象のマニュアルは以下の URL から入手できます。
http://jp.fujitsu.com/platform/server/primequest/manual/2000/

[26] 「Pending TPM operation」がグレーアウトして選択出来ない場合は、「参考 2 PRIMEQUEST での BitLocker 構築手順」の手順 1 を実施後に本手順を実施して下さい。

PC サーバ FUJITSU Server PRIMERGY につきましては、以下の技術情報を参照願います。

・PC サーバ FUJITSU Server PRIMERGY（プライマジー）
http://jp.fujitsu.com/platform/server/primergy/
・FUJITSU Server PRIMERGY 機種比較表
http://jp.fujitsu.com/platform/server/primergy/products/lineup/select-spec/
・FUJITSU Server PRIMERGY サーバ選定ガイド
http://jp.fujitsu.com/platform/server/primergy/products/lineup/select-model/

PC サーバ FUJITSU Server PRIMERGY のお問い合わせ先。

・PC サーバ FUJITSU Server PRIMERGY お問い合わせ
http://jp.fujitsu.com/platform/server/primergy/contact/

基幹 IA サーバ FUJITSU Server PRIMEQUEST につきましては、以下の技術情報を参照願います。

・基幹 IA サーバ FUJITSU Server PRIMEQUEST（プライムクエスト）
http://jp.fujitsu.com/platform/server/primequest/
・FUJITSU Server PRIMEQUEST 製品ラインナップ
http://jp.fujitsu.com/platform/server/primequest/products/

基幹 IA サーバ FUJITSU Server PRIMEQUEST のお問い合わせ先。

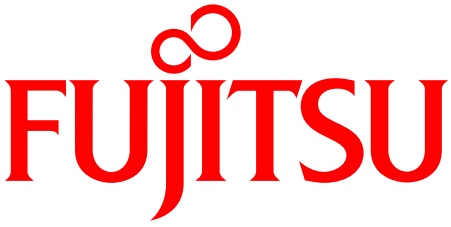
・本製品のお問い合わせ
http://jp.fujitsu.com/platform/server/primequest/contact/

商標登記について

- Intel、インテル、Pentium、Intel Core、Xeon、Celeron は、米国インテル社の登録商標または商標です。
- Microsoft、Windows、Windows Server、Hyper-V は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- Ethernet は、米国ゼロックス社の登録商標です。
- Linux は、Linus Torvalds 氏の米国およびその他の国における登録商標または商標です。
- Red Hat、RPM および Red Hat をベースとした全ての商標とロゴは、Red Hat Inc.の米国およびその他の国における登録商標または商標です。
- VMware、vSphere は、VMware,Inc.の米国およびその他の国における登録商標または商標です。
- PowerChute は、Schneider Electric の米国およびその他の国における商標です。
- ARCserve は、米国 CA, Inc.社の商標です。
- SPEC®およびベンチマーク名の SPEC® int®は、米国およびその他の国における Standard Performance Evaluation Corporation（SPEC）の商標または登録商標です。
- 記載されている会社名、製品名は各社の登録商標または商標です。
- 記載されている会社名、製品名等の固有名詞は各社の商号、登録商標または商標です。
- その他、本資料に記載されている会社名、システム名、製品名等には必ずしも商標表示を付記しておりません。

免責事項

このドキュメントは単に情報として提供され、内容は予告なしに変更される場合があります。また、発行元の許可なく、本書の記載内容を複写、転載することを禁止します。
このドキュメントに誤りが無いことの保証や、商品性又は特定目的への適合性の黙示的な保証や条件を含め明示的又は黙示的な保証や条件は一切無いものとします。富士通株式会社は、このドキュメントについていかなる責任も負いません。また、このドキュメントによって直接又は間接にいかなる契約上の義務も負うものではありません。このドキュメントを形式、手段（電子的又は機械的）、目的に関係なく、富士通株式会社の書面による事前の承諾なく、複製又は転載することはできません。


FUJITSU