リファレンスマニュアル - 日本語

FUJITSU Server BIOS セットアップユーティリティ

PRIMEQUEST 4000 シリーズ

リファレンスマニュアル

08/2023

CA92344-5401-02

ISO 9001 および ISO 27001 に準拠したドキュメントの作成

高い品質と情報セキュリティ基準に確保されるように、このマニュアルは、ISO 9001 および ISO 27001 に準拠した cognitas の品質管理システムの規定と情報セキュリティマネジメントシステムを満たすように作成されました。

cognitas.Gesellschaft für Technik-Dokumentation mbH www.cognitas.de/en/

著作権および商標

お届けまでの日数は在庫状況によって異なります。技術的修正の権利を有します。

使用されているハードウェア名およびソフトウェア名は、各社の商標です。

- 本書の内容は、改善のため事前連絡なしに変更することがあります。
- 本書に記載されたデータの使用に起因する、第三者の特許権およびその他の権利の侵害については、当社はその責を負いません。
- このマニュアルのいかなる部分も Fujitsu の書面による事前の許可なしにいかなる形体でも複製することを禁じます。

Microsoft、Windows、Windows Server、および Hyper-V は、米国およびその他の国における Microsoft Corporation の商標または登録商標です。

Intel および Xeon は、米国およびその他の国における Intel Corporation またはその子会社の商標または登録商標です。

本書をお読みになる前に

お客様の安全のために

このマニュアルには、この製品を安全かつ正しくご使用いただくための重要な情報が記載されています。

この製品を使用する前に、マニュアルをよくお読みください。付属の『安全上のご注意』マニュアルをよくお読みになり、安全上の注意事項をご理解されたうえで製品を使用してください。このマニュアルと『安全上のご注意』マニュアルは、この製品の使用中にすぐに参照できる安全な場所に保管してください。

電波障害対策について

この製品は、「クラス A」の情報技術装置（ITE : Information Technology Equipment）です。この製品を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合にはユーザーが適切な対策を取る必要のあることがあります。

VCCI-A

アルミ電解コンデンサについて

製品のプリント基板アセンブリとマウスおよびキーボードに使用されているアルミニウム電解コンデンサは、寿命のあるコンポーネントです。動作寿命を超えてこれらのコンポーネントを使用すると、電解質漏出や電解質減少が発生し、悪臭や煙が排出されることがあります。

ガイドラインとして、通常のオフィス環境（25 °C）では、保守サポート期間（5 年）以内に動作寿命に達することはないと予想されます。ただし、製品を高温の環境で使用した場合などに、動作寿命が短くなることがあります。動作寿命を超えた交換可能なコンポーネントの交換コストはお客様にご負担いただきます。これらは単なるガイドラインですので、保守サポート期間中のトラブルフリーの動作を保証するものではありません。

ハイセイフティ用途での使用について

この製品は、商業地域および工業地域でサーバとして使用するように設計および製造されています。

本製品は、職場規制の第 2 項に従ったビジュアルディスプレイワークプレースでの使用には適していません（TX サーバシステムを除いて、すべてのサーバシステムに該当します）。

ビジュアルディスプレイワークプレースとして使用する場合は、不便に感じる反射を避けるために、直接視野に入る場所に設置しないでください（TX サーバシステムにのみ該当します）。

このデバイスは、極端に高度な安全性が要求される用途や、そのような安全性を保証できない限り生命や人体に直接および重大な危険を及ぼす用途向けに設計および製造されていません。

この製品の用途には、原子力発電所での核反応、自動飛行機の飛行制御、航空管制、公共交通機関の交通管制、生命維持用の医療機器、兵器システムのミサイル誘導コントロールなどが含まれます（以後、「高安全用途」とします）。お客様は、高安全用途に必要とされる安全性のレベルを保証するための措置が取られない限り、このような高安全用途にこの製品を使用してはなりません。高安全用途にこの製品を使用する予定がある場合は、弊社営業担当者にご相談ください。

瞬時電圧低下対策について

この製品は、雷によって生じた電源ユニットの瞬時電圧低下により影響を受ける可能性があります。瞬時電圧低下を防ぐために、AC 無停電電源装置の使用を推奨します。

（この注記は、JEITA（社団法人電子情報技術産業協会）が発行したガイドライン『パーソナルコンピュータの瞬時電圧低下対策』に従っています。）

日本の外為法、外国為替および外国貿易管理法によって規制されるテクノロジーについて

弊社が発行したドキュメントには、日本の外為法、外国為替および外国貿易管理法によってコントロールされるテクノロジーが含まれることがあります。このようなテクノロジーは、上記法律に従って最初に許可を受けずに、日本から国外に持ち出したり、日本の非居住者に譲渡してはなりません。

高調波電流規格について

この製品は高調波電流規格 JIS C 61000-3-2 に準拠しています。

日本のみ : SATA HDD について

このサーバの SATA バージョンは、SATA/BC-SATA ストレージインターフェースを搭載した HDD をサポートしています。ご使用の HDD のタイプによって使用方法と動作条件が異なりますので、ご注意ください。

使用できるタイプの HDD の使用方法と動作条件の詳細は、以下の Web サイトを参照してください。
https://jp.fujitsu.com/platform/server/primergy/harddisk/

日本のみ :

この製品には遮蔽 LAN ケーブルを使用してください。

英国の輸入業者情報

Fujitsu Services Limited

22 Baker Street, London, W1U 3BW, United Kingdom

バージョン履歴

版番号	発行日	説明
V 1.0	2023 年 06 月	初版リリース（ドラフト）
V 1.1	2023 年 07 月	初版リリース
V 2.0	2023 年 08 月	新しい項を追加 ● 画面遷移 ● 複数のディスクを持つダンプデバイスの作成 以下の項を更新 ● BIOS セットアップを開く ● Configuration メニュー ● ブートオプション ● Device Path ● sadump Configuration ツール ● 設定項目の一覧

目次

1 はじめに

1.1 この BIOS リファレンスマニュアルについて

BIOS セットアップユーティリティでは、ご使用のシステムのシステム機能とハードウェア構成を設定します。行った変更は、設定を保存して BIOS セットアップユーティリティを終了すると有効になります。

BIOS セットアップユーティリティの各メニューで、以下の項目の設定を行います。

- 「**Information**」 – システム機能
- 「**Configuration**」 – システム構成
- 「**Management**」 – サーバ管理
- 「**Security**」 – セキュリティ機能
- 「**Boot**」 – 起動順位の設定
- 「**Exit**」 – 機能の終了

設定オプションは、システムのハードウェア構成によって異なります。

そのため、ご使用のシステムの BIOS セットアップユーティリティではメニューや特定の設定オプションが使用できない場合や、BIOS バージョンによってメニューの場所が異なる場合があります。

1.2 表記規定

このマニュアルでは以下の表記規則を使用します。

太字のテキスト およびかぎ括弧（「 」）	インターフェース要素の名前を示します。
等幅フォントのテキスト	コマンドを示します。
かぎ括弧（「 」） 二重かぎ括弧（『 』）	かぎ括弧（「 」）は、章の名前を示します。 二重かぎ括弧（『 』）は、他のマニュアル名などを示しています。

►	記載されている順序で行う必要がある作業です。
 **注意**	この記号が付いている文章には、特に注意してください。この表示を無視して、誤った取り扱いをすると、生命が危険にさらされたり、システムが破壊されたり、データが失われる可能性があります。
	追加情報、注記、ヒントを示しています。

2 BIOS セットアップユーティリティの操作方法

2.1 BIOS セットアップユーティリティを開く

POST ウィンドウから BIOS セットアップユーティリティを開く

▶ システムを起動して、画面に出力が表示されるまで待ちます。

▶ ファンクションキー [F2] を押します。

「**Information**」メニューが表示されない場合：

▶ ファンクションキー [F2] を押しても「**Information**」メニューが表示されない場合は、[Ctrl] + [Alt] + [Delete] キーを同時に押してシステムを再起動してから、BIOS セットアップユーティリティを起動します。

iRMC S6 Web インターフェースから BIOS セットアップユーティリティを開く

▶ iRMC S6 Web インターフェースに移動します。

▶「**設定**」メニューの「**システム**」ページを選択します。

▶「**ブートオプション**」グループを選択します。

▶「**ブートメディアの選択**」で「**BIOS セットアップ**」を選択します。

▶「**適用**」をクリックして変更内容を適用します。

i iRMC 設定の詳細は、『Fujitsu Server PRIMEQUEST 4000 Series iRMC S6 Web インターフェイス取扱説明書』を参照してください。

2.2 「Boot」メニューを直ちに開く

「**Boot**」メニューで設定した最初のドライブからシステムを起動しない場合に、この機能を使用します。

- ▶ システムを起動して、画面に出力が表示されるまで待ちます。
- ▶ ファンクションキー [F12] を押します。
  「**Boot**」メニューが、ポップアップウィンドウとして表示されます。
- ▶ カーソルキー [↑]または [↓] を使用して OS を起動するドライブを選択します。選択オプションは、「**Boot**」メニューと同じです。

  選択したオプションは、現在のシステムの起動に適用されます。次回のシステム起動時には、「**Boot**」メニューで行った設定が再び適用されます。

- ▶ 選択内容を [[Enter]] キーで確定します。

2.3 画面設計

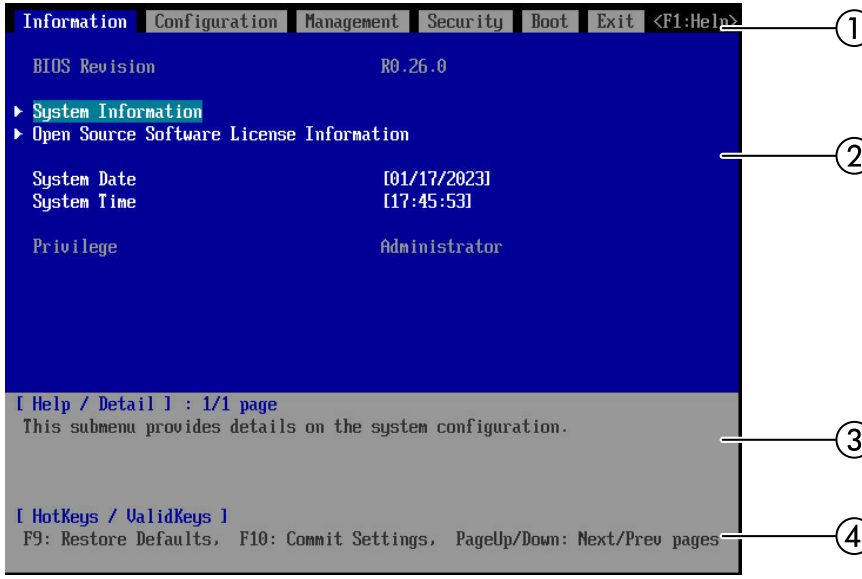

図 1: BIOS セットアップ画面の例

1	タブ領域	3	ヘルプ領域
2	メニュー領域	4	キーヘルプ領域

BIOS セットアップ画面は、以下の領域に分かれています。

タブ領域（1）

タブ領域バーは、さまざまな BIOS セットアップユーティリティメニューの選択に使用されます。

メニュー領域（2）

メニュー領域には、選択したメニューのパラメータが現在の値と共に表示されます。パラメータ値は要件に従って変更できます（適切なフィールドがグレー表示されていない場合）。

► サブメニューがあるパラメータを示します。

ヘルプ領域（3）

ヘルプ領域には、簡単な情報が表示されます。

キーヘルプ領域（4）

キーヘルプ領域には、キーの意味が表示されます。

2.4 画面遷移

電源投入からブートまでの画面遷移を次の図に示します。POST 画面表示中に特定のキーを押すと、そのキーに対応する画面に画面が移動します。

PRIMEQUEST 4000E では認証画面は表示されません。

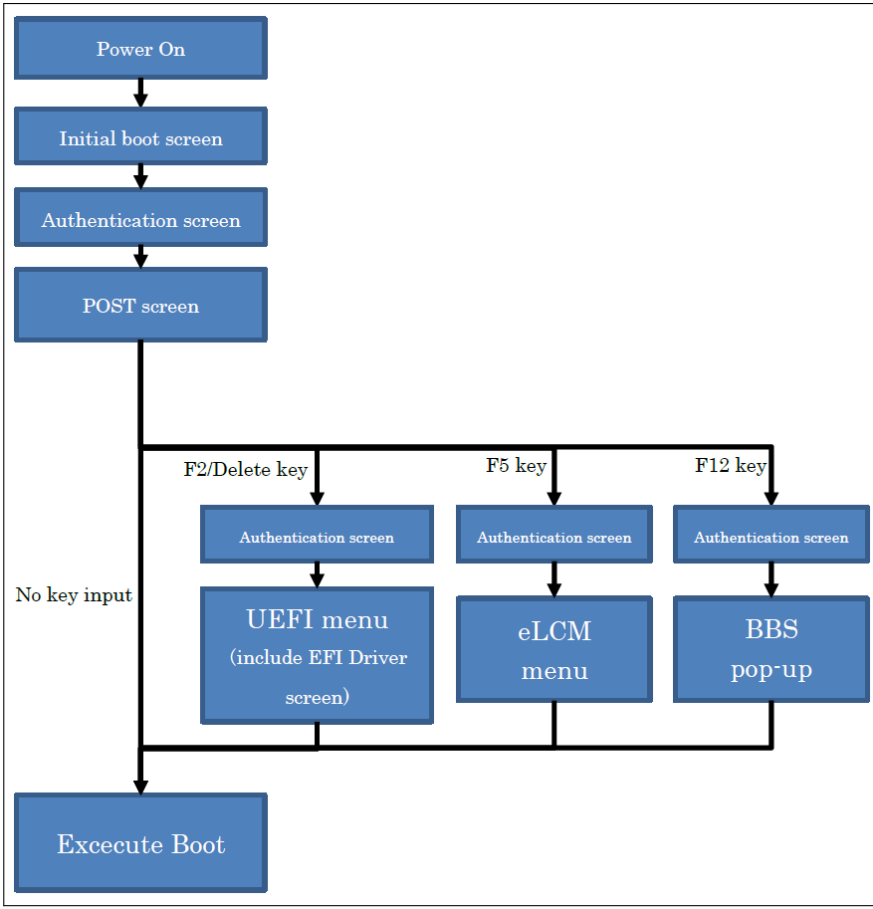

図 2: PRIMEQUEST 4000 画面遷移

キー	機能
F2	UEFI メニューの「**Information**」メニューウィンドウを表示します。
削除	UEFI メニューの「**Information**」メニューウィンドウを表示します。
F5	「**eLCM**」メニューウィンドウを表示します。

キー	機能
F12	「**BBS**」ポップアップメニューを表示します。

2.5 キー操作とキー入力

キー操作

各メニューのキー操作は次のようになります。

表示項目	説明
↑	カーソルを次に選択可能な上の項目または設定値に移動します。
↓	カーソルを次に選択可能な下の項目または設定値に移動します。
←	カーソルを 1 つ左のタブに移動します。 あるいは、カーソルを時間（HH:MM:SS）または日付フィールド（DOW （day of week)/MM/DD/YYYY）内で移動します。
→	カーソルを 1 つ右のタブに移動します。 あるいは、カーソルを時間（HH:MM:SS）または日付フィールド（DOW （day of week)/MM/DD/YYYY）内で移動します。
+	値を増加するか、選択内容を上に移動します。
-	値を減少させるか、選択内容を下に移動します。
Enter	エントリを選択します。
Esc	前のメニューに戻るか、BIOS セットアップユーティリティを終了します。
F1	メニュー選択ヘルプと操作ヘルプの表示または非表示の設定を切り替えます。
F9	すべてのメニューにあるすべての構成をデフォルト値にリセットします。

表示項目	説明
F10	前回の保存以降の変更を保存します。
PageUp	操作ヘルプ表示が設定されている場合、前のヘルプページに戻ります。
PageDown	操作ヘルプ表示が設定されている場合、次のヘルプページに移動します。

キー入力

BIOS セットアップユーティリティのキー入力は、US キーボード同じように扱われます。このため、日本語キーボードを使用する場合、キーボードに表示されるキーコードは実際のキーコード出力とは異なる文字があります。

実際のキーコード出力と示されている出力キーコードの異なる、すべての入力キーコード（キーボードキーラベル）を一覧で示します。

入力キーコード	出力キーコード
^	=
@	[
[	]
:	'
]	\
Shift + 2	@
Shift + 6	^
Shift + 7	&
Shift + 8	*
Shift + 9	（
Shift + 0	）
Shift + -	_
Shift + ^	+
Shift + @	{
Shift + [	}

入力キーコード	出力キーコード
Shift + ;	:
Shift + :	"
Shift +]	|

以下のキーコードは無視されます。

入力キーコード
¥
\
Shift + ¥
Shift + \

2.6 BIOS セットアップユーティリティを終了する

▶「**Exit**」メニューで、必要なパラメータを選択し、[Enter] キーを押します。

3 「Information」メニュー

このメニューには、システム情報が表示されます。オプションの一部は、特定の条件でのみ使用できる設定があります。

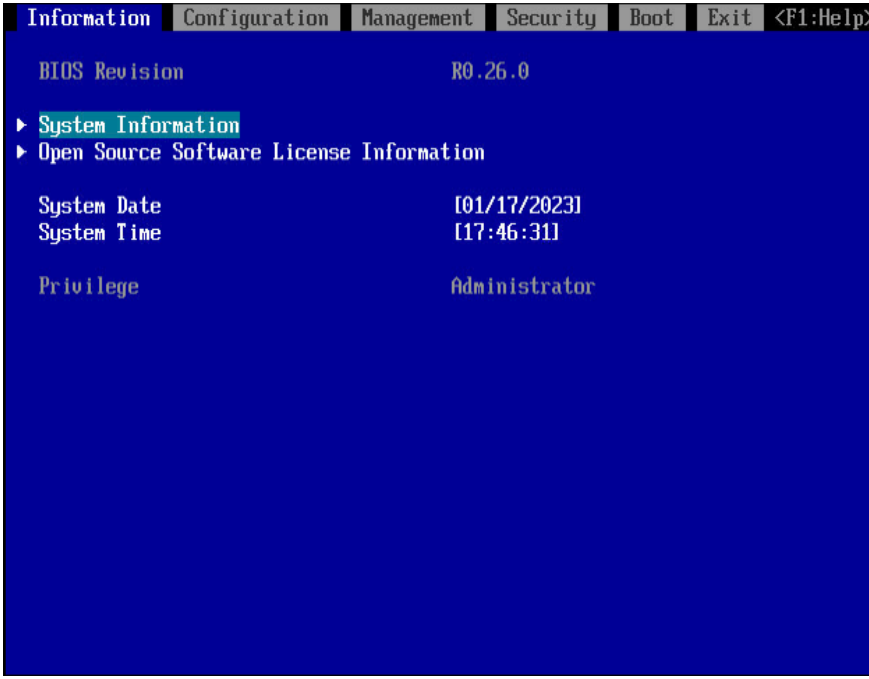

図 3: 「**Information**」メニューの例

System Information

システム構成の概要を表示します。これには、CPU、メモリ、および LAN の構成データが含まれます。

Open Source Software License Information

このシステムボードで使用されるオープンソースソフトウェアのライセンス情報が表示されます。

ライセンスの詳細は、次の Web ページを参照してください。
https://support.ts.fujitsu.com/content/3rdparty_license_info.asp

System Time / System Date

システムに設定されている現在の日付および時刻が表示されます。

システム時刻の形式は「**HH:MM:SS**」で、システム日付の形式は「**DOW (day of week)/MM/DD/YYYY**」です。

現在の時刻と日付設定を変更するには、「**System Time**」および「**System Date**」フィールドに、それぞれ新しい時刻と日付を入力します。「**System Time**」および「**System Date**」フィールド内のカーソル移動には [<-] および [->] キーを使用します。

システムの電源を切ってから再度投入した後、システム時刻および日付が失われる場合は、リチウムバッテリーが切れていますので交換が必要です。
リチウムバッテリーの交換方法については、『Fujitsu Server PRIMEQUEST 4000 アップグレード＆メンテナンスマニュアル』を参照してください。

Privilege

BIOS セットアップユーティリティの現行の「**Privilege**」を表示します。

Administrator

Privilege は、常に **Administrator** です。

4 「Configuration」 メニュー

注意

このメニューの設定が正しくない場合、コンピュータが誤動作することがあります。

► デフォルト設定は、特殊な用途に必要な場合のみ変更してください。

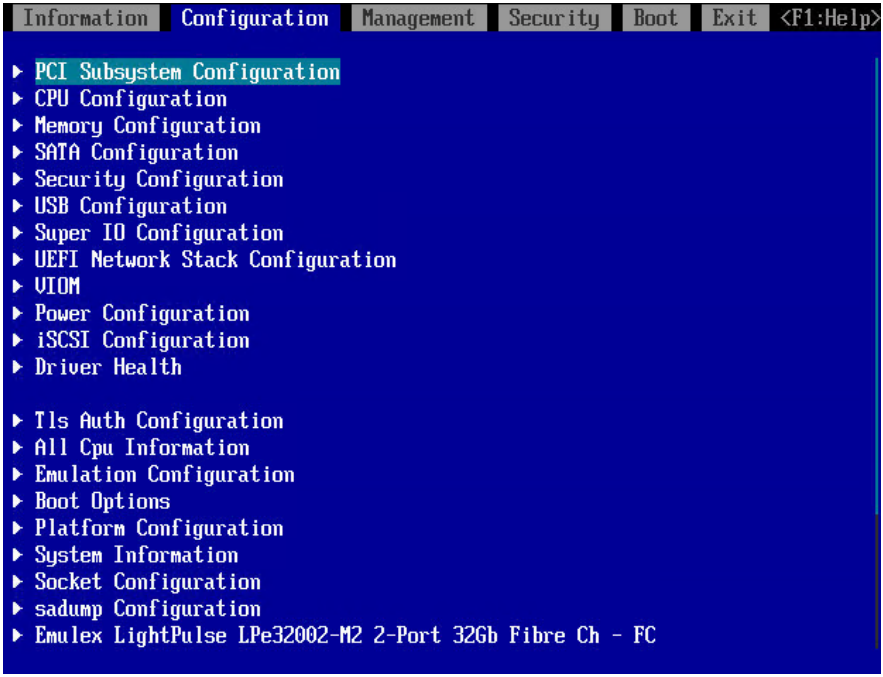

図 4: 「**Configuration**」メニューの例

Application Profile Configuration

特殊用途向けのプロファイルを選択するために使用するサブメニューを呼び出します（25 ページの「Application Profile Configuration」を参照）。

PCI Subsystem Settings

システムの PCI スロット および PCI コンポーネントの設定に使用するサブメニューを呼び出します（26 ページの「PCI Subsystem Configuration」を参照）。

CPU Configuration

追加の CPU 設定に使用するサブメニューを呼び出します（29 ページの「CPU Configuration」を参照）。

このサブメニューで利用できる調整オプションは、使用する CPU によって異なります。

Memory Configuration

メモリサブシステムのセットアップに使用するサブメニューを呼び出します（52 ページの「Memory Configuration」を参照）。

SATA Configuration

該当する SATA コントローラの設定が表示されるサブメニューを呼び出します（55 ページの「SATA Configuration」を参照）。

Security Configuration

セキュリティ関連のデータを安全に保存できるサブメニューを呼び出します（56 ページの「Security Configuration」を参照）。
このサブメニューは、TPM 2.0 がインストールされている場合にのみ表示されます。

USB Configuration

システムボードの USB コンポーネントの設定に使用するサブメニューを呼び出します（58 ページの「USB Configuration」を参照）。

Super IO Configuration

システムスーパー IO チップパラメータの設定に使用するサブメニューを呼び出します（59 ページの「Super IO Configuration」を参照）。

UEFI Network Stack Configuration

UEFI ネットワークスタックのセットアップに使用するサブメニューを呼び出します（60 ページの「UEFI Network Stack Configuration」を参照）。

VIOM

Virtual IO-Manager を無効にすることができ、状態が報告されます（61 ページの「VIOM」を参照）。

Power Configuration

ウェイクアップリソースの設定に使用するサブメニュー（62 ページの「Power Configuration」を参照）を呼び出します。

iSCSI Configuration

iSCSI 設定に使用するサブメニューを呼び出します（63 ページの「iSCSI Configuration」を参照）。

Driver Health

Driver Health インターフェースをサポートする UEFI ドライバのステータスを表示するために使用するサブメニューを呼び出します（63 ページの「Driver Health」を参照）。

Tls Auth Configuration

このサブメニューで、Transport Layer Security（TLS）設定を構成できます（63 ページの「Tls Auth Configuration」を参照）。

Network Device List

インストールされているネットワークカードの表示に使用するサブメニューを呼び出します（63 ページの「Network Device List」を参照）。

UEFI Device Driver Setup

UEFI FW セットアップへのインターフェースをサポートする UEFI デバイスドライバの情報を指定するために使用するサブメニューを呼び出します（65 ページの「UEFI Device Driver Setup」を参照）。

sadump Configuration

sadump の設定に使用するサブメニューを呼び出します（65 ページの「sadump Configuration」を参照）。

4.1 Application Profile Configuration

このメニューでは、ユーザーが予想する作業負荷に対応する最適な設定をまとめて設定することができます。

Application Profile

ユーザーがシステムの使用方法を選択すると、BIOS によって選択した用途に最適な設定がロードされます。これらの設定はメモリにロードされます。ユーザーが確定するまで、これらの設定が今後のブートに影響を及ぼすことはありません。

可能な値は以下のとおりです。

- **Custom**
- **Total Throughput Performance**
- **Single Thread Performance**
- **Energy Efficiency**
- **Virtualization Performance**
- **Low Latency**
- **Online Transaction Processing**
- **Decision Support**
- **I/O Throughput**
- **HPC (memory bandwidth)**
- **HPC (computing)**

4.2 PCI Subsystem Configuration

このサブメニューでは、以下のパラメータを設定できます。一部、特定の条件でのみ使用できる設定があります。

ASPM Support

PCI Express リンクの電源管理に Active State Power Management（ASPM）が使用されます。ASPM はこの設定によって全般的に有効になっていても、該当する PCI Express 拡張カードまたはオンボードコントローラも ASPM をサポートしている場合にのみ特定のリンクに対して有効になります。

Disabled

ASPM は無効です。PCI Express リンクの消費電力は低下しません。互換性は最大です。

Auto

該当する PCI Express 拡張カードまたはオンボードコントローラがサポートする特定のリンクに対して ASPM が有効になります。

ASPM が無効になっていない場合、PCI Express デバイスのレイテンシが長くなることがあります。複数の拡張カードを使用した場合、この機能は正しくサポートされず、未定義のシステム動作が発生することがあります。

PCIe 10-bit Tag

PCI Express のタグフィールドのビット幅を 8 ビットまたは 10 ビットに設定します。

Disabled

PCI Express のタグフィールドのビット幅を 8 ビットに設定します。

Auto

PCI Express パケットのタグフィールドのビット幅を、ハードウェアのデフォルト値に維持します。

PCIe Latency Tolerance Reporting (LTR)

PCI Express LTR 機能を有効または無効にします。

Disabled

PCI Express LTR 機能を無効にします。

Auto

PCI Express LTR 機能をハードウェアのデフォルト値に維持します。

SR-IOV Support

システムに SR-IOV 対応の PCIe デバイスが搭載されている場合、このオプションで Single Root IO Virtualization Support を有効/無効にします。

Disabled
Single Root IO Virtualization Support が無効です。

Enabled
Single Root IO Virtualization Support が有効です。

4.2.1 OpROM Scan Configuration

IOU#n-Slot#n OpROM
このスロットに取り付けられている LAN/CNA カードの Option ROM を起動するかどうかを制御します。

Disabled
このスロット内の LAN/CNA カードの Option ROM を起動しません。

Enabled
このスロット内の LAN/CNA カードの Option ROM を起動します。

PCI Box#n-Slot#n OpROM
このスロットに取り付けられている LAN/CNA カードの Option ROM を起動するかどうかを制御します。

Disabled
このスロット内の LAN/CNA カードの Option ROM を起動しません。

Enabled
このスロット内の LAN/CNA カードの Option ROM を起動します。

4.2.2 I/O Space Assignment Configuration

このサブメニューで、システム内の各種 I/O デバイスの I/O スペース割り当てを設定できます。

I/O スペースを割り当てることができるデバイス数は制限されているため、I/O スペースも割り当てられていないデバイスもあります。

4.3 CPU Configuration

Hyper-Threading

ハイパースレッディングテクノロジによって、1 つの物理プロセッサコアを複数の論理プロセッサに見せかけることができます。このテクノロジにより、OS は内蔵プロセッサリソースの利用率を向上でき、さらにはパフォーマンスを向上できます。このテクノロジの利点は、ACPI をサポートする OS でのみ使用できます。この設定は、ACPI をサポートしない OS では効果がありません。

Disabled

ACPI OS は、プロセッサコアの最初の論理プロセッサのみを使用できます。この設定は、ハイパースレッディングテクノロジが ACPI OS で正しく実装されていない場合にのみ使用してください。

Enabled

ACPI OS は、物理コア内のすべての論理プロセッサを使用できます。

Active Processor Cores

複数のプロセッサコアが含まれているプロセッサの場合は、有効なプロセッサコアの数を制限できます。無効なプロセッサコアは使用されず、OS に表示されなくなります。

Intel® Speed Select Technology - Core Power/Turbo Frequency（Intel® SST-CP/TF）機能を使用する場合は、この設定を「**0**」に変更します。

0

使用可能なすべてのプロセッサコアが有効になり、使用できます。

1 ... n

選択した数のプロセッサコアのみが有効になります。残りのプロセッサコアは無効になります。

この選択を行うことで、特定のソフトウェアパッケージやシステムライセンスに関する問題が解決される場合があります。

Dynamic SST-PP

パラメータを **Enabled** に設定した場合、次の設定が影響を受けます。

– 「**Active Processor Cores**」は無視されます。

– 「**HWPM Support** を **Disabled** に設定した場合、**Native Mode** として動作します。

Disabled

「**Dynamic SST-PP**」を無効にします。

Enabled

「**Dynamic SST-PP**」を有効にします。

Hardware Prefetcher

有効になっている場合、メモリバスが非アクティブになったときに、必要になる可能性のあるメモリ内容が自動的にキャッシュにプリロードされます。メモリではなくキャッシュから内容を読み出すことによって、特にデータへのリニアアクセスを使用するアプリケーションの場合にレイテンシが短縮されます。

このパラメータで、非標準アプリケーションのパフォーマンス設定を変更できます。標準アプリケーションについては、デフォルト設定のままにすることを推奨します。

Disabled

CPU のハードウェアプリフェッチャを無効にします。

Enabled

CPU のハードウェアプリフェッチャを有効にします。

Adjacent Cache Line Prefetch

プロセッサのキャッシュ要求時に追加の隣接する 64 バイトキャッシュラインをロードするためのメカニズムがプロセッサに備わっている場合に、このパラメータを使用できます。これによって、空間局所性の高いアプリケーションのキャッシュヒット率が高まります。

このパラメータで、非標準アプリケーションのパフォーマンス設定を変更できます。標準アプリケーションについては、デフォルト設定のままにすることを推奨します。

Disabled
プロセッサは要求されたキャッシュラインを読み込みます。

Enabled
プロセッサは要求されたキャッシュラインと隣接したキャッシュラインを読み込みます。

DCU Streamer Prefetcher
有効になっている場合、メモリバスが非アクティブになったときに、必要になる可能性のあるデータ内容が自動的に L1 データキャッシュにプリロードされます。メモリではなくキャッシュから内容を読み出すことによって、特にデータへのリニアアクセスを使用するアプリケーションの場合にレイテンシが短縮されます。


このパラメータで、非標準アプリケーションのパフォーマンス設定を変更できます。標準アプリケーションについては、デフォルト設定のままにすることを推奨します。

Disabled
CPU の「**DCU Streamer Prefetcher**」を無効にします。

Enabled
CPU の「**DCU Streamer Prefetcher** 」を有効にします。

DCU IP Prefetcher
コードがシーケンシャルに編成され、メモリに連続的に格納される場合、パフォーマンスの向上が期待されます。


このパラメータで、非標準アプリケーションのパフォーマンス設定を変更できます。標準アプリケーションについては、デフォルト設定のままにすることを推奨します。

Disabled
CPU の「**DCU IP Prefetcher**」を無効にします。

Enabled
CPU の「**DCU IP Prefetcher** 」を有効にします。

Intel Virtualization Technology

仮想コンピュータを使用して複数のソフトウェア環境の使用をサポートするための VMX（Virtual Machine Extensions）に基づいて、プラットフォームのハードウェアおよび複数のソフトウェア環境の仮想化をサポートします。仮想化テクノロジーにより、16 ビット/32 ビット保護モード、および EM64T（Intel® Extended Memory 64 Technology）モードでの仮想化を目的としてプロセッササポートを拡張します。

Disabled

VMM（Virtual Machine Monitor）は追加のハードウェア機能を使用できません。

Enabled

VMM（Virtual Machine Monitor）は追加のハードウェア機能を使用できます。

Intel (R) VT-d

VT-d (Virtualization Technology for Directed I/O) で、複数の仮想マシン間の共有 I/O デバイスに対してハードウェアサポートを提供します。
VMM（Virtual Machine Monitor）で VT-d を使用して、同じ物理 I/O デバイスにアクセスする複数の仮想マシンを管理することができます。

Disabled

VT-d が無効になり、VMM で使用できません。

Enabled

VMM の VT-d が有効になります。

Pre-boot DMA Protection

「**Intel (R) VT-d**」が有効な場合に、プリブート環境で Direct Memory Access（DMA）保護機能を指定します。

このパラメータを「**Enabled**」に設定した場合、BIOS はプリブート環境ですべての DMA 対応デバイスから意図しない DMA をブロックします。

Disabled

プリブート環境での DMA 保護は無効です。

Enabled

プリブート環境での DMA 保護は有効です。

Intel TXT Support

Trusted Execution Technology（TXT）サポートをアクティブ化します。

次の CPU と TPM の条件を満たす場合、Intel®TXT を使用できます。

- 取り付けられている CPU が Secure Mode Extensions（SMX）をサポートしている
- Intel® Virtualization Technology（VT）と Intel® VT-d が「**CPU Configuration**」サブメニューで有効になっている
- TPM が取り付けられている
- **TPM Support** が「**Security Configuration**」サブメニューで有効になっている

Intel® TXT サポートは、システム BIOS アップデートを開始する前に無効にしておく必要があります。

Disabled

TXT は非アクティブ化されます。

Enabled

TXT はアクティブ化されます。

Total Memory Encryption (TME)

TME 機能は、メモリスペース全体を暗号化します。

Disabled

TME 機能が無効になります。

Enabled

TME 機能が有効になります。

TME Bypass

「Ttal Memory Encryption（TME）をバイパスするかどうかを指定します。

このパラメータを「**Enabled**」に設定した場合、メモリ暗号化に使用されるメモリ領域（TME-MT、SGX など）は暗号化されますが、TME 機能がバイパスされるため、その他のメモリ領域は暗号化されません。

TME Bypass は、次のすべての条件が満たされる場合に表示されます。

- 搭載された CPU が TME 機能に対応している。
- このサブメニューで「**Total Memory Encryption (TME)**」が「**Enabled**」に設定されている。

Auto

TME 機能は、ハードウェア構成に応じて自動的にバイパスされます。

第 4 世代 Intel® Xeon® Scalable CPU が搭載されている場合、システムは「**Disabled**」（TME 機能はバイパスされません）に設定されているものとして動作します。

Disabled

TME 機能はバイパスされません。

Enabled

TME 機能はバイパスされます。

Total Memory Encryption Multi-Tenant (TME-MT)

TME-MT 機能は、OS と VMM で指定された複数のキーを使用してメモリスペースを暗号化します。

Disabled

TME-MT 機能は無効です。

Enabled

TME-MT 機能は有効です

TME-MT Keys

OS と VMM で指定できる TME-MT キーの数を表示します。キーの数は、取り付けられている CPU の数によって異なります。

Memory integrity

メモリ整合性をグローバルに有効または無効にします。

「**Memory integrity**」は、次のすべての条件が満たされる場合は表示されません。

- メモリ構成と状態が TME 機能と一致しない。
- 「**Limit CPU Physical Address to 46 bits**」が無効ではない。

Disabled

メモリ整合性をグローバルに無効にします。

Enabled

メモリ整合性をグローバルに有効にします。

SGX Reset

これは、BIOS が次の POST 時にすべての SGX 登録データを削除するかどうか決定する 1 スクリーンショットのオプションです。

注意

「SGX Reset」から「Enabled」の変更

「**SGX Reset**」から「**Enabled**」に変更した場合、現在の SGX キーのすべてのエクスポートした暗号化データを復号化することはできません。

► 「**SGX Reset**」から「**Enabled**」に必要な場合のみ変更してください。

CPU を追加または交換する場合は、このオプションを一部の OS で有効にする必要があります。詳細については、OS の取扱説明書またはマニュアルを参照してください。

Disabled

SGX をリセットしません。

Enabled

BIOS が次の POST 時に SGX キーを含む、すべての SGX 登録データを削除します。このとき、このオプションは「**Disabled**」に変更されます。

SW Guard Extensions (SGX)

サポートされるアプリケーションの保護されたメモリ領域を提供する SGX 機能を有効または無効にします。このこの機能は、NVM / LRDIMM と同時には使用できません。この機能を NVM/LRDIMM が取り付けられている場合に有効にすると、NVM/LRDIMM は自動的に無効になります。

次の条件を満たす場合は、Intel® SGX を使用できます。

- 取り付けられている 各 CPU の各チャンネルに、1 つ以上の DIMM を取り付ける必要があります。
- このサブメニューの「**Total Memory Encryption (TME)**」を「**Enabled**」に設定する必要があります。
- このサブメニューの「**Local x2APIC**」を「**Enabled**」に設定する必要があります。
- 「**Memory Configuration**」サブメニューの「**Memory Mode**」を「**Independent**」に設定する必要があります。
- 「**Memory Configuration**」サブメニューの「**ADDDC Sparing**」を「**Disabled**」に設定する必要があります。
- 「**Memory Configuration**」サブメニューの「**NUMA**」を「**Enabled**」に設定する必要があります。

1 つ以上の条件を満たしていない場合は、BIOS に「**SGX cannot be enabled due to unsupported configuration**」、「**SGX cannot be enabled due to unsupported memory configuration**」「**Memory population does not meet SGX memory requirements**」のいずれかが表示されるか、この設定がグレー表示されます。

POST 中に SGX 関連のエラーにより Intel® SGX が使用できない場合、BIOS が「**SW Guard Extensions (SGX)**」オプションを自動的に「**Disabled**」に変更されるか、指定された UEFI 変数を使用して OS/VMM にエラーコードをレポートします。

Disabled
SGX 機能は無効です。

Enabled
SGX 機能は有効です。

SGX Package Info In-Band Access
OS および VMM のエージェントアプリケーションによる SGX 情報への内部アクセスを有効または無効にします。

Disabled
SGX 情報が無効になります。

Enabled
SGX 情報が有効になります。

SGX PRM Size
SGX 機能の CPU ごとに保護されるメモリ範囲（PRM）のサイズを指定します。

可能な値 :
128M、256M、512M、1G、2G、4G、8G、16G、32G、64G、128G、256G、512G

SGX QoS
「**SGX QoS**」機能を有効または無効にします。QoS 機能が有効な場合に他の作業負荷での安全なエンクレーブのパフォーマンスを向上します。

Disabled
SGX QoS 機能が無効になります。

Enabled
SGX QoS 機能が有効になります。

Select Owner EPOCH input type

2 つの「Owner EPOCHs」の入力方法を設定します。設定を「**Change to New Random Owner EPOCHs**」に変更して保存すると、次のブートのときに設定が自動的に「**Manual User Defined Owner EPOCHs**」に変更されます。

注意

Intel® SGX で保護されるすべての永続データは、この設定が自動的に「**SGX Owner EPOCH activated**」に設定された後に「Owner EPOCHs」を変更して保存すると失われます。

SGX Owner EPOCH activated

EPOCHs は変更されません。この入力方法は、SGX 機能を有効にした後、または、指定した「**Change to New Random Owner EPOCHs**」または「**Manually User Defined Owner EPOCHs**」で EPOCHs を変更した後、次の POST 時にシステムによって自動的に設定されます。

Change to New Random Owner EPOCHs

EPOCHs がシステムによって生成されるランダム値に変更されます。この入力方法を指定すると、この設定は「**Manually User Defined Owner EPOCHs**」に変更され、生成されたランダム値が「**Software Guard Extensions Epoch 0**」と「**Software Guard Extensions Epoch 1**」に自動的に入力されます。

Manually User Defined Owner EPOCHs

EPOCHs がユーザーが必要とする値に変更されます。

Software Guard Extensions Epoch 0

0x0 ... 0xFFFFFFFFFFFFFFFF

最初の Owner EPOCH 値を表示して設定します。
SGX Epoch 0（Epoch バイト 7-0）。Epoch 値を使用して EGETKEY 命令でエンクレーブキーを生成します。

Software Guard Extensions Epoch 1

0x0 ... 0xFFFFFFFFFFFFFFFF
2 つ目の Owner EPOCH 値を表示して設定します。
SGX Epoch 1（Epoch バイト 15-8）。Epoch 値を使用して EGETKEY 命令でエンクレーブキーを生成します。

SGX Launch Control Policy
IA32_SGXLEPUBKEYHASH MSRs をロックするかロック解除するかを指定します。これらの MSRs は「SGX Launch Enclave」と「Flexible Launch Control (FLC)」機能に関連します。

Intel Locked
BIOS は、デフォルト値によりこれらの MSRs をロックします。デフォルト値は、Intel の署名鍵のダイジェストです。

Unlocked
BIOS は、OS/VMM による書き込みのために、これらの MSRs のロックを解除します。

Locked
BIOS は、このサブメニューの「**SGXLEPUBKEYHASH0**」-「**SGXLEPUBKEYHASH0**」からの指定されたダイジェスト値によって、これらの MSRs をロックします。

SGXLEPUBKEYHASH0

0x0 ... 0xFFFFFFFFFFFFFFFF
SGX Launch Enclave Public Key Hash バイト 7-0。
SGXLEPUBKEYHASH の 1 ～ 8 バイトを表示して設定します。

SGXLEPUBKEYHASH1

0x0 ... 0xFFFFFFFFFFFFFFFF
SGX Launch Enclave Public Key Hash バイト 15-8。
SGXLEPUBKEYHASH の 9 ～ 16 バイトを表示して設定します。

SGXLEPUBKEYHASH2

0x0 ... 0xFFFFFFFFFFFFFFFF
SGX Launch Enclave Public Key Hash バイト 23-16。
SGXLEPUBKEYHASH の 17 ～ 24 バイトを表示して設定します。

SGXLEPUBKEYHASH3

0x0 ... 0xFFFFFFFFFFFFFFFF
SGX Launch Enclave Public Key Hash バイト 31-24。
SGXLEPUBKEYHASH の 25 ～ 32 バイトを表示して設定します。

SGX Auto MP Registration
OS ブート時の自動実行による「Multi-Package Registration Agent (MPA)」を有効または無効にします。

Disabled
MPA は OS ブート時に自動的に実行されません。

Enabled
MPA は OS ブート時に自動的に実行されます。

Enhanced SpeedStep
プロセッサの電圧と周波数を定義します。EIST（Enhanced Intel SpeedStep® Technology）は省電力機能です。


プロセッサの電圧は、各システム要件に調節されます。クロック周波数を下げると、システムで必要な電力が減少します。


Intel® Speed Select Technology - Core Power/Turbo Frequency（Intel® SST-CP/TF）機能を使用する場合は、この設定を「**Enabled**」に変更します。

Disabled
Enhanced SpeedStep 機能が無効になります。

Enabled
Enhanced SpeedStep 機能が有効になります。

Turbo Mode

最高のパフォーマンス状態（P0）が OS によって要求される場合に、プロセッサの動作周波数を上げることができます。この機能は、Intel® Turbo Boost Technology とも呼ばれています。

Intel® Speed Select Technology - Core Power/Turbo Frequency（Intel® SST-CP/TF）機能を使用する場合は、この設定を「**Enabled**」に変更します。

Disabled

「**Turbo Mode**」が無効になります。

Enabled

「**Turbo Mode**」が有効になります。

Optimized Power Mode

電力最適化モードを有効または無効にします。

パラメータを「**Enabled**」に設定した場合、次の設定を行う必要があります。

- 「**Energy Perfomance**」が、「**Performance**」に設定されます。
- 「**Override OS Energy Performance**」が、「**Enabled**」に設定されます。
- 「**CPU C1E Support**」が、「**Enabled**」に設定されます。
- 「**Uncore Frequency Scaling**」が、「**Auto**」に設定されます。

Disabled

「**Optimized Power Mode**」は無効です。

Enabled

「**Optimized Power Mode**」は無効です。

Energy Performance

非レガシーオペレーティングシステムでの CPU のエネルギー効率ポリシー。これは、電力消費とパフォーマンスを調整するための CPU への入力です。

Intel® Speed Select Technology - Core Power/Turbo Frequency（Intel® SST-CP/TF）機能を使用する場合は、この設定を「**Performance**」に変更します。

Performance

エネルギー効率を犠牲にしても、パフォーマンスを得る方向に強く最適化します。

Balanced Performance

エネルギーを節約しながら、パフォーマンスを得る方向にウェイトを置きます。

Balanced Energy

良好なパフォーマンスを得ながら、エネルギーを節約する方向にウェイトを置きます。

Energy Efficient

パフォーマンスを犠牲にしても、エネルギー効率を得る方向に強く最適化します。

この電力ポリシーによって、OS がセットアップで選択されたモードを使用しないように決定することもあります。また、セットアップが上書きされ、代わりに他のモードのいずれかが選択されることもあります。

Override OS Energy Performance

OS がセットアップのエネルギー効率ポリシーの設定を上書きしないように防止します。

Disabled

「**Override OS Energy Performance**」が無効になります。

Enabled

「**Override OS Energy Performance**」が有効になります。

Utilization Profile

エネルギーとパフォーマンスの割合が、システムに従って最適化されます。

Even

エネルギーとパフォーマンスがバランスの取れたシステム利用のために最適化されます。

Unbalanced

パフォーマンスを優先したシステム利用に最適化されます。

P-State Coordination

OS Power Management（OSPM）に渡されるプロセッサパフォーマンス調整モデル。

Intel® Speed Select Technology - Core Power/Turbo Frequency（Intel® SST-CP/TF）機能を使用する場合は、この設定を「**HW_ALL**」に変更します。

HW_ALL

プロセッサハードウェアが、すべての論理プロセッサ間のパフォーマンス状態を調整します（推奨）。

SW_ALL

OSPM が、すべての論理プロセッサ間のパフォーマンス状態を調整します。パフォーマンスの推移は、すべての論理プロセッサで開始される必要があります（推奨しません）。

HWPM Support

HWPM（Hardware Power Management）は、パフォーマンスおよび省電力を管理する柔軟なプロセッサインターフェースです。以前オペレーティングシステム（OS）に搭載されていた周波数制御機能は現在、CPU ファームウェアに組み込まれています。

Intel® Speed Select Technology - Core Power/Turbo Frequency（Intel® SST-CP/TF）機能を使用する場合は、この設定を「**Native Mode**」または「**Native Mode with no legacy**」に変更します。

Disabled
HWPM 機能は使用できません。P ステートは、従来のプロセッサの世代と同様に制御されます。

Native Mode
HWPM は、ソフトウェアインターフェース経由でオペレーティングシステムと協調動作します。OS は、動的に追加の制約とヒントを提供することができます。

OOB Mode
CPU は周波数を自動的に制御します。OS の制約およびヒントは使用しません。

Native Mode with no legacy
HWPM は、ソフトウェアインターフェース経由でオペレーティングシステムと協調動作します。レガシー OS は制約およびヒントを周波数制御に提供できません。

CPU C1E Support
オペレーティングシステムでサポートされている場合、電力の節約が可能なときにプロセッサが停止されます。

Disabled
C1E Power State 機能は無効です。

Enabled
C1E Power State 機能は有効です。

CPU C6 Report
プロセッサの C6 状態を ACPI C-2 状態として OSPM に渡して、プロセッサの Deep Power Down Technology を有効にします。

Disabled
「**CPU C6 Report**」は ACPI C-2 状態として OSPM に提供されません。

Enabled
「**CPU C6 Report**」は ACPI C-2 状態として OSPM に提供されます。

Package C State limit

プロセッサパッケージのアイドル時の電力消費を最小限に抑えるには、「**Package C State limit**」を指定して、このメニュー項目の選択肢として使用します。

C0

「**Package C state limit**」は、「**C0**」に設定されます。

C2

「**Package C state limit**」は、「**C2**」に設定されます。

C6

「**Package C state limit**」は、「**C6**」に設定されます。

C6 (Retention)

「**Package C state limit**」は、「**C6 (Retention)**」に設定されます。

No Limit

Package C state limit なし

CPU C1 auto demotion

CPU の C1 への自動的なデモートを有効または無効にします。

Disabled

「**CPU C1 auto demotion**」が無効になります。

Enabled

「**CPU C1 auto demotion**」が有効になります。

CPU C1 auto undemotion

CPU の C1 からの自動的なアンデモートを有効または無効にします。

Disabled

「**CPU C1 auto undemotion**」が無効になります。

Enabled

「**CPU C1 auto undemotion**」が有効になります。

UPI Link Frequency Select

UPI 周波数を、CPU の共通してサポートされる周波数に設定できます。

Auto

BIOS から、システムに存在する CPU とチップセットに基づいて最大速度が検出されます。

12.8GT/s、14.4GT/s、16.0GT/s

（CPU に依存）

使用可能な速度設定は CPU とチップセットによってさまざまであるため、システムによって異なる値が表示されます。いずれかの値を選択して、UPI リンクが動作する速度を明示的に設定します。

UPI Link L0p

UPI L0p 電源状態を CPU 間のリンク上で使用できるかどうかを指定して、消費電力を低減します。

Disabled

UPI L0p 電源状態をリンク上で使用できません。

Enabled

UPI L0p 電源状態がリンク上で有効になります。

UPI Link L1

UPI L1 電源状態を CPU 間のリンク上で使用できるかどうかを指定して、消費電力を低減します。

Disabled

UPI L1 電源状態をリンク上で使用できません。

Enabled

UPI L1 電源状態がリンク上で有効になります。

Local x2APIC

「**Local x2APIC**」を有効または無効にします。

Disabled

「**Local x2APIC**」を無効にします。

Enabled

「**Local x2APIC**」を有効にします。

IODC Configuration

IODC（IO ダイレクトキャッシュ）の有効化または無効化: リモート InvItoM（IIO）や WCiLF に対してメモリルックアップの代わりにスヌープを生成します。

可能な値は以下のとおりです。

Disabled

Auto

Enable for Remote InvItoM Hybrid Push

Enable for Remote InvItoM AllocFlow

Enable for Remote InvItoM Hybrid AllocFlow

Enable for Remote InvItoM and Remote WCiLF

Uncore Frequency Scaling

CPU のアンコア周波数を設定します。

Auto

事前に定義された範囲で CPU が自律的に周波数を制御します。

Maximum

周波数は常に事前に定義された最大値に設定されます。そのため、消費電力が増加することがあります。

Power Balanced

電力とパフォーマンスのバランスを最適化するために、事前に定義された範囲で CPU が自律的に周波数を制御します。

Stale AtoS

Caching Agent で陳腐化したデータのディレクトリ最適化を指定します。これによりシステムパフォーマンスは影響を受けます。

Disabled

ディレクトリ最適化が無効になります。

Enabled
ディレクトリ最適化が有効になります。

Auto
ディレクトリ最適化が自動的に有効になります。

LLC Dead Line Alloc
LLC（Last Level Cache）のデッドラインの処理を指定します。これによりシステムパフォーマンスは影響を受けます。

Disabled
LLC のデッドラインを満たしません。

Enabled
便宜的に LLC のデッドラインを満たします。

AVX ICCP pre-grant level
AVX レベルをコアに付与します。基本周波数がアップデートしません。次の値が有効です。

Intel® Speed Select Technology - Core Power/Turbo Frequency（Intel® SST-CP/TF）機能を使用する場合は、この設定を「**no override**」に変更します。

no override

128 Heavy

256 Light

256 Heavy

512 Light

512 Heavy

L2 RFO Prefetch
L2 キャッシュ内のデータのプリフェッチャ（**L2 RFO Prefetch**）を有効または無効にします。

Disabled
「**L2 RFO Prefetch**」は使用できません。

Enabled
「**L2 RFO Prefetch**」は使用できます。

Monitor MWAIT
CPU の Monitor 命令および MWAIT 命令を有効または無効にします。

Disabled
「**Monitor MWAIT**」機能を無効にします。

Enabled
「**Monitor MWAIT**」 機能を有効にします。

LLC Prefetch
Last Level Cache（LLC）プリフェッチ機構を選択します。

Disabled
LLC Prefetch　機構を使用しません。

Enabled
LLC Prefetch　機構が LLC にデータを直接ロードで使用します。

Homeless Prefetch
「**Homeless Prefetch**」を有効または無効にします。

Disabled
Homeless Prefetch を使用しません。

Enabled
Homeless Prefetch を使用します。

Auto
Homeless Prefetch は、ハードウェア構成に応じて自動的に使用されます。

FB Thread Slicing
スレッドごとのデータキャッシュユニット（DCU）フィルバッファ（FB）スライシングを有効または無効にします。

Disabled
「**FB Thread Slicing**」は無効です。

Enabled
「**FB Thread Slicing**」は有効です。

LMCE Support
Local Machine Check Exception（LMCE）機能を BIOS でサポートするかどうかを切り替えます。LMCE 機能は、この項目が有効で、対応する OS を組み合わせた場合のみ使用できます。

Disabled
ローカル MCE ファームウェアのサポートを無効にします。

Enabled
ローカル MCE ファームウェアのサポートを有効にします。

Limit CPU Physical Address to 46 bits
CPU の物理アドレスを 46 ビットに制限します。「**Limit CPU Physical Address to 46 bits**」を有効に設定した場合、「**Total Memory Encryption Multi-Tenant (TME-MT)**」は自動的に無効になります。

Disabled
CPU の物理アドレスを制限しません。

Enabled
CPU の物理アドレスを 46 ビットに制限します。TME-MT オプションは自動的に無効になります。

DBP-F
「DBP-for-F」を有効または無効にします。この機能はマルチスレッドのワークロードに役に立ちますが、シングルスレッドのワークロードではパフォーマンスが低下する可能性があります。

Disabled
「**DBP-F**」は無効です。

Enabled
「**DBP-F**」は有効です。

4UPI

「**4UPI**」を有効または無効にします。

「**4UPI**」は、CPU に 4 UPI ポートがない場合は非表示になります。

Enabled

この機能が有効な場合、CPU は 4 UPI ポートで接続されます。

この設定では CPU の最高パフォーマンスが可能ですが、以下のことが IOU#1 の スロット 5 に適用されます。

- PCIe Gen5 はサポートされません（PCIe Gen4 のみサポートされています）。
- CXL カードはサポートされていません。

Disabled

この機能を無効にすると、CPU は 3 UPI ポートで接続されます。

この設定では CPU の最高パフォーマンスが可能ですが、以下のことが IOU#1 の スロット 5 に適用されます。

- PCIe Gen5 はサポートされています
- CXL カードはサポートされています

CPU Performance Boost

消費電力を増加させて CPU のパフォーマンスを向上します。

Disabled

この機能は無効です。

Moderate

消費電力を増加させて CPU のパフォーマンスを向上できます。

Aggressive

CPU のパフォーマンスを **Moderate** よりも大幅に向上できますが、消費電力が増加するおそれがあります。

4.4 Memory Configuration

このサブメニューでは、以下のパラメータを設定できます。一部、特定の条件でのみ使用できる設定があります。

Virtual NUMA

物理 NUMA ノードを、ACPI テーブルで同じサイズの仮想 NUMA ノードに分割します。これにより、論理プロセッサが 64 を超える CPU で Windows のパフォーマンスが向上します。

Disabled

「**Virtual NUMA**」は無効です。

Enabled

「**Virtual NUMA**」は有効です。

SNC (Sub NUMA)

Sub NUMA Clustering (SNC) は、アドレス範囲に基づいて、ラストレベルキャッシュ（LLC）を分離されたクラスタに分解するための機能です。各クラスタはシステム内のメモリコントローラのサブセットに結び付けられています。SNC は LLC からローカルメモリに平均レイテンシを向上します。

Disabled

「**SNC (Sub Numa)** 」は 1 つのクラスタをサポートします。

Enable SNC2

「**SNC (Sub Numa)**」は 2 つのクラスタをサポートします。

Enable SNC4

「**SNC (Sub Numa)**」は 4 つのクラスタをサポートします。

「**Enable SNC4**」は、CPU でサポートされない場合は非表示になります。

DDR Performance

メモリモジュールは互いに異なる速度（周波数）で動作できます。高速になるほどパフォーマンスが向上し、低速になるほど省電力になります。使用可能なメモリ速度は、取り付けられているメモリモジュールの構成によって異なります。

Energy optimized

省電力で可能な限り最も低速な設定。

Performance optimized

最高のパフォーマンスを得るために可能な最も高速な設定。

PPR Type

Post Package Repair（PPR）タイプを選択します。

PPR Disabled

リペアプロセスは開始されません。

Hard PPR

リペアプロセスは永続的に行われます。故障した行は、リセットしたり電源を切っても使用できるようになりません。

Soft PPR

リペアプロセスは一時的にのみ行われます。リセットするか電源を切ると、以前の構成が再び復元されます。

Patrol Scrub

全メモリをバックグラウンドで定期的にスクリーニングするかどうかを指定します。修正可能なメモリエラーが蓄積して修正不可能なメモリエラーになる前に、修正可能なメモリエラーが検出され、修正されます。

Disabled

バックグラウンドメモリスクリーニングが実行されないため、パフォーマンスが向上します。

Enabled

バックグラウンドメモリスクリーニングが実行されるため、信頼性が向上します。

修正可能なメモリエラーの原因としては、使用環境（高温など）が不適切であることが考えられます。

DDR5 ECS

この機能を使用して、「DDR5 Error Check and Scrub (ECS)」を有効または無効にすることができます。

「**DDR5 ECS**」が有効な場合、メモリはバックグラウンドで定期的にスクリーニングされます。これにより、パフォーマンスが低下することがあります。

Disabled

「**DDR5 ECS**」は無効です。

Enabled

「**DDR5 ECS**」は有効です。

FastBoot Mode

「**FastBoot Mode**」を有効または無効にします。

Enabled

「**FastBoot Mode**」が有効になります。

Disabled

「**FastBoot Mode**」が無効になります。

Volatile Memory Mode

「**1LM**」と「**2LM**」のどちらの「**Volatile Memory Mode**」をアクティブにするかを選択します。

1LM

システムが「**1LM**」モードです。

2LM

「**2LM Volatile Memory Mode**」がアクティブな場合、BIOS は「**2LM**」を構成しようとします。BIOS が「**2LM**」を構成できない場合は、揮発性メモリモードは「**1LM**」にフォールバックします。

4.4.1 Address Range Mirroring Configuration

メモリの初期化モードを選択します。

Mirror Memory Below 4GB

4 GB 未満のメモリのミラーリングを有効または無効にします

この項目を設定するには、最初に関連する SB の「**SB#x メモリモード**」パラメータを iRMC Web インターフェースの「**アドレス範囲ミラー**」に設定する必要があります。

Disabled

4 GB 未満のメモリ領域はミラーリングされません。

Enabled

4 GB 未満のメモリ領域はミラーリングされています。

Mirrored Amount Above 4GB

ミラーリングする 4 GB 以上のメモリの割合を指定します。

この項目を設定するには、最初に関連する SB の「**SB#x メモリモード**」パラメータを iRMC Web インターフェースの「**アドレス範囲ミラー**」に設定する必要があります。

0

4 GB 以上のメモリ領域はミラーリングされません。

1 ... 5000

ベーシスポイント（百分率の 12.75% = 1275）で測定して、ミラーする必要のある 4 GB を超える使用可能なメモリ容量。5000（= 50%）まで指定できます。

4.5 SATA Configuration

このサブメニューでは、以下のパラメータを設定できます。一部、特定の条件でのみ使用できる設定があります。

SATA Mode

SATA コントローラの動作方法を指定します。

AHCI
SATA インターフェースは AHCI モードです。

RAID
SATA インターフェースは RAID モードです。

SATA Controller 2
SATA コントローラ 2 の機能を定義します。

Disabled
SATA コントローラ 2 は使用できません。

Enabled
SATA コントローラ 2 を使用できます。

4.6 Security Configuration

このセットアップメニューが表示される場合は、TCG 2.0 仕様に準拠したセキュリティおよび暗号化（TPM - Trusted Platform Module）チップが、システムボードに搭載されています。このチップはセキュリティ関連のデータ（パスワードなど）を安全に保存できます。TPM の使用は標準化され、Trusted Computing Group（TCG）で規定されています。

TPM Support
TPM（Trusted Platform Module）ハードウェアを使用できるかどうかを指定します。

TPM が無効の場合、システムは TPM ハードウェアのないシステムと同様に動作します。

Disabled
Trusted Platform Module を無効にします。

Enabled
Trusted Platform Module を有効にします。

Pending TPM operation
TPM 処理を次回起動時に実行するようにスケジュールします。

None
TPM 処理は実行されません。

TPM Clear
TPM は出荷時のデフォルトにリセットされます。TPM 内のすべてのキーはクリアされます。

TPM の状態を変更するために、コンピュータが再起動されます。

Set NoPPIClear flag to FALSE
「BIOS TPM Management」フラグに含まれる「NoPPIClear」フラグを「FALSE」に設定します。

Set NoPPIClear flag to TRUE
「BIOS TPM Management」フラグに含まれる「NoPPIClear」フラグを「TRUE」に設定します。

Active PCR Banks
有効な PCR Bank を表示します。

TPM 2.0 から有効な PCR Bank の情報を取得できない場合は、**N/A** と表示されます。

TPM Support が **Disabled** から **Enabled** に変更された場合、有効な PCR Bank 情報をリセット前に取得することはできません。**N/A** と表示されます。

Change active PCR Bank

この 1 回限りのメニューは有効な PCR Bank を変更します。このメニューは、1 回限りのメニューであるため、次の POST 時に **No change** に戻ります。ただし、変更または有効にされた PCR Bank はメニューが「**No change**」に戻っても有効なままとなります。

取り付けた TPM チップが選択した PCR Bank をサポートしていない場合、BIOS は選択した PCR Bank に切り替わらず、現在有効な PCR Bank を維持します。

一部の TPM チップでは、同時に有効にできる PCR Bank は 1 つのみです。**All** の場合、BIOS は SHA256 PCR Bank のみ有効にします。

No change

PCR Bank は変更されません。

SHA256

SHA256 PCR Bank のみ有効にします。

SHA384

SHA384 PCR Bank のみ有効にします。

All

サポートされるすべての PCR Bank を有効にします。

Firmware Version

TPM ファームウェアバージョンを表示します。TPM が無効な場合、またはファームウェアバージョンを取得できない場合は、**N/A** と表示されます。

4.7 USB Configuration

USB 構成を設定するサブメニューが開きます。一部のパラメータ、特定の条件でのみ使用できる設定があります。

USB Devices

使用できる USB デバイス、USB キーボード、USB マウス、USB ハブの数を表示します。

4.7.1 USB Port Security

USB Port Security を設定するサブメニューが開きます。

USB Port Control
USB ポートの使用方法を設定します。無効にされた USB ポートは、POST 中に使用できず、OS でも使用できません。

Enable all ports
すべての USB ポートが有効です。

Disable all ports
すべての USB ポートが無効です。

Enable used ports
すべての未使用の USB ポートが無効です。

USB Device Control
「**USB Device Control**」で行った設定は、デバイスクラスに応じて追加設定できます。

Enable all devices
すべての USB ポートが有効です。

Enable Keyboard and Mouse only
キーボードとマウスが接続されている USB ポートのみを使用できます。キーボードとマウスが接続されているポート以外は、すべて無効にされます。

Enable all devices except mass storage devices / Hubs
ハブまたはストレージデバイスが使用しているポートも無効になります。

4.8 Super IO Configuration

システムスーパー IO チップのパラメータを表示します。

Super IO Chip
「**Super IO Chip**」の情報を表示します。

4.9 UEFI Network Stack Configuration

Network Stack

UEFI Network Stack を UEFI でネットワークアクセスに使用できるかどうかを設定します。たとえば、UEFI ネットワークスタックを使用できない場合、PXE 経由で UEFI インストールを実行できません。

Disabled

UEFI ネットワークスタックは使用できません。

Enabled

UEFI ネットワークスタックは使用できます。

Ipv4 PXE Support

OS のインストールに、IPv4 による PXE UEFI Boot を使用できるかどうかを指定します。

Disabled

IPv4 による PXE UEFI Boot は使用できません。

Enabled

IPv4 による PXE UEFI Boot は使用できます。

Ipv4 HTTP Support

OS のインストールに、IPv4 による HTTP UEFI Boot を使用できるかどうかを指定します。

Disabled

IPv4 による HTTP UEFI Boot は使用できません。

Enabled

IPv4 による HTTP UEFI Boot は使用できます。

Ipv6 PXE Support

OS のインストールに、IPv6 による PXE UEFI Boot を使用できるかどうかを指定します。

Disabled

IPv6 による PXE UEFI Boot は使用できません。

Enabled
IPv6 による PXE UEFI Boot は使用できます。

Ipv6 HTTP Support
OS のインストールに、IPv6 による HTTP UEFI Boot を使用できるかどうかを指定します。

Disabled
IPv6 による HTTP UEFI Boot は使用できません。

Enabled
IPv6 による HTTP UEFI Boot は使用できます。

4.10 VIOM

VIOM-flag
Virtual IO-Manager フラグは、IO 仮想化を有効または無効にするために使用します。有効にすると、Virtual IO-Manager ソフトウェアでプロファイルを提供できるようになり、IO アドレス（WWN および MAC）を仮想化し､既知のオンボード IO デバイスおよび拡張カードの構成と構成解除を実行できます。これらのプロファイルを適用して、必要に応じてブートシーケンスを上書きすることもできます。

Disabled
Virtual IO-Manager で仮想化できません。Virtual IO-Manager は BIOS で設定できます。

Enabled
Virtual IO-Manager で仮想化を行えます。Virtual IO-Manager は Virtual IO-Manager でしか設定できません。

この機能はセットアップ時にのみ無効にできます。無効にした場合、OS ベースの Virtual IO-Manager ソフトウェアを使用して、再度有効にする必要があります。

4.11 Power Configuration

Wake-up Resources
ウェイクアップリソースの設定に使用するサブメニュー（62 ページの「Wake-Up Resources」を参照）を呼び出します。

4.11.1 Wake-Up Resources

LAN
LAN コントローラ（拡張カード上）を経由してシステムの電源を入れられるかどうかを指定します。

Disabled
LAN コントローラを経由してシステムの電源を入れることはできません。

Enabled
LAN コントローラを経由してシステムの電源を入れることができます。

Wake On LAN boot
ネットワーク信号によって電源を入れた場合のシステム動作を指定します。

Boot Sequence
システムは LAN 経由で電源を入れた場合、「**Boot**」メニューで指定されたデバイスシーケンスに従って起動します。

Force LAN Boot
システムは LAN 経由で電源を入れた場合、リモートで LAN から起動します。

4.12 iSCSI Configuration

LAN/CNA コントローラ用の UEFI ドライバ（PCIe カード）がロードされる場合は、iSCSI 経由でのブート用のパラメータをここで設定できます。

4.13 iSCSI Configuration

LAN/CNA コントローラ用の UEFI ドライバ（オンボード CNA または PCIe カード）がロードされる場合は、iSCSI 経由でのブート用のパラメータをここで設定できます。

4.14 Driver Health

PCI エクスプレスデバイスの UEFI ドライバが Driver Health Protocol をサポートしている場合は、UEFI ファームウェアは、UEFI ファームウェアが管理しているデバイスのヘルス状態を UEFI ドライバに問い合わせることができます。

このメニューに、Driver Health をサポートしている UEFI ドライバのヘルスステータスが表示されます。

4.15 TIs Auth Configuration

[Enter]を押して「**TIs Auth Configuration**」を選択します。

4.16 Network Device List

このサブメニューには、MAC アドレスを持つ PCIe カードの設定メニューへのリンクが表示されます。このリンクは、PCIe カードの各 MAC アドレスとして表示されます。

図 5: 「**Network Device List**」の例

4.16.1 MAC:XX:XX:XX:XX:XX:XX

サブメニュー項目の名前に表示される MAC アドレス（**XX:XX:XX:XX:XX:XX**）に対応する NIC ポートの設定画面を表示します。

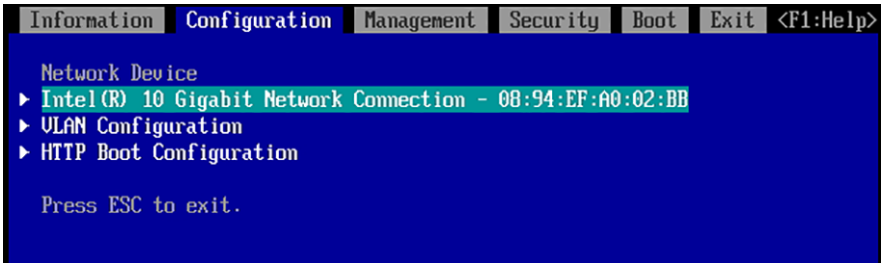

図 6: MAC:XX:XX:XX:XX:XX:XX の例

UEFI Device Driver Setup

インストールされているネットワークカードの EFI ドライバのメニューへのリンクを表示します。メニューは各ネットワークカードのマニュアルを参照してください。

表示内容は、ベンダーに提供された EFI ドライバによって異なります。

VLAN Configuration

NIC ポートに対応する「**VLAN Configuration**」メニューを表示します。

HTTP Boot Configuration

HTTP ブートパラメータを設定します。NIC ポートに対応する HTTP 設定メニューを表示します。

この項目は、「**UEFI Network Stack Configuration**」サブメニューで「**Ipv4 HTTP Support**」または「**Ipv6 HTTP Support**」が有効な場合に表示されます。

4.17 UEFI Device Driver Setup

UEFI デバイスドライバは UEFI FW セットアップへのインターフェースをサポートできる可能性があり、情報およびコントロールアイテムのリストを提供します。利用できる UEFI デバイスドライバは、例えば PRAID 680i です。

4.18 sadump Configuration

この機能で「**sadump Configuration**」ツールを管理できます。

詳細は、89 ページの「sadump Configuration ツール」を参照してください。

4.18.1 Set up Manager

「**sadump セットアップ**」メニューが開きます。

sadump

sadump 機能を有効または無効にします。

Enable

sadump 機能は有効です。

Disable

sadump 機能は無効です。

COMPRESS

システムメモリをダンプデバイスに書き込む形式を指定します。

この設定は「**Uncompress**」に固定されています。

Uncompress

システムメモリは圧縮されません。

RECYCLE

RECYCLE 機能を有効または無効にします。この機能を有効にすると、ダンプデバイス内で最も古いダンプが上書きされます。

Enable

RECYCLE 機能は有効です。

Disable

RECYCLE 機能は無効です。

REBOOT

ダンプ後の sadump 機能の動作を指定します。

0

システムは停止します。

1 ... 3600

選択した時間（秒単位）が経過した後、システムはリブートされます。

SKIPZEROPAGE

Skip Zero Page を有効または無効にします。この機能が有効な場合、"0" しか含まれないメモリページはダンプデバイスに書き込まれません。

Enable

Skip Zero Page は有効です。

Disable

Skip Zero Page は無効です。

TIMEOUT

タイムアウト値を指定します。

0

タイムアウトは無効です。sadump プロセスの中断はありません。

1 ... 255
sadump プロセスが指定された時間（時間単位）以内に完了しなかった場合、強制的に停止されます。

Only Address Mirrored Region
有効な場合、「**Address Range Mirroring**」によってミラーリングされないメモリページはダンプデバイスに書き込まれません。

Enable
「**Only Address Mirrored Region** 」は有効です。

Disable
「**Only Address Mirrored Region** 」は無効です。

Restore to factory settings
すべての項目をデフォルトの工場出荷時の設定に設定します。

Commit Changes and Exit
変更を保存して終了します。

Discard Changes and Exit
変更を破棄して終了します。

4.18.2 Dump device Manager

ダンプデバイスのメンテナンスメニューが開きます。

Maintain the dump device
すでに作成されているダンプデバイスの数と、すでに設定されているダンプデバイスの数を表示します。

Number of created dump device: n

Number of dump device in use: n

Create a dump device
ダンプデバイスの設定メニューが表示されます。

Create mode
ダンプデバイスのモードを選択します。

- **Single**：1 つのディスクまたは 1 つのパーティションでダンプデバイスを作成します。冗長性を設定するには、この値を選択して複数の sadump デバイスを構成します。
- **Multiple**：複数のディスクでダンプデバイスを作成します。システムメモリが大きく 1 つのディスクでは不十分な場合に、この値を使用します。

Disk selection
「**Select device**」メニューを呼び出します。

Exit
このメニューを終了します。

Select device
このサブメニューは、「**Create a dump device** 」メニューで「**Create mode**」が「**Single**」に設定されている場合に表示されます。

<ディスク/ディスクパーティションの ACPI 名>
ディスクまたはディスクパーティションを選択して、ダンプデバイスを作成します。

Exit
このメニューを終了します。

Select a dump device
「**Select the dump device used**」メニューが表示されます。

[1]
最初のダンプデバイスを選択します。選択されていない場合、「**[1]**」のみ表示されます。

[2]
2 つ目のダンプデバイスを選択します。選択されていない場合、「**[2]**」のみ表示されます。

[3]
3 つ目のダンプデバイスを選択します。選択されていない場合、「**[3]**」のみ表示されます。

Clear setting
現在のすべての設定をクリアします。

Commit Changes and Exit
変更を保存して、このメニューを終了します。

設定を変更する場合は、「**Commit Changes and Exit**」でメニューを終了する必要があります。[Esc] でメニューを終了しないでください。

Discard Changes and Exit
変更せずにこのメニューを終了します。

Discard a dump device
不要なダンプデバイスを破棄するためのメニューが表示されます。

Discard all dump device and Exit
すべてのダンプデバイスを破棄して、このメニューを終了します。

Exit
選択したダンプデバイスを破棄せずに、このメニューを終了します。

<ダンプデバイスの ACPI 名>
ダンプデバイスを選択します。

Exit
ダンプデバイスのメンテナンスメニューを終了します。

4.18.3 終了

sadump Configuration ツールを終了します。

5 「Management」 メニュー

このメニューでは、以下のパラメータを設定できます。一部、特定の条件でのみ使用できる設定があります。

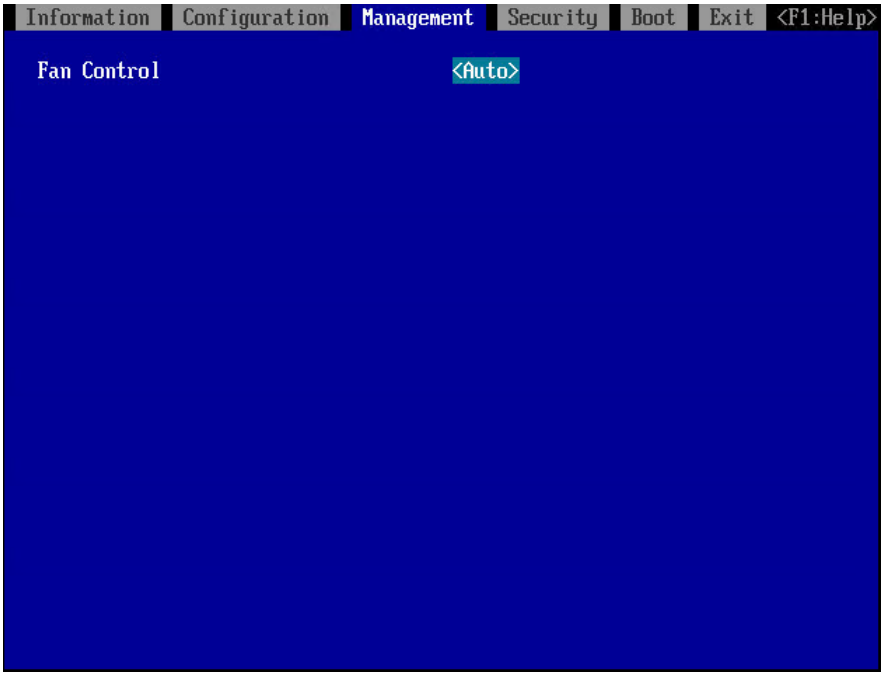

図 7: 「**Management**」メニューの例

Fan Control

ファン速度を制御します。使用するシステム構成とアプリケーションによっては、あらかじめ設定されているモードを変更できます。

Auto

ファン速度が自動的に調整されます。システム温度と CPU パフォーマンスの片方を犠牲にして片方を向上させます。

Full

すべてのファンがフルスピードに設定されます。

6 「Security」メニュー

このメニューでは、以下のパラメータを設定できます。一部、特定の条件でのみ使用できる設定があります。

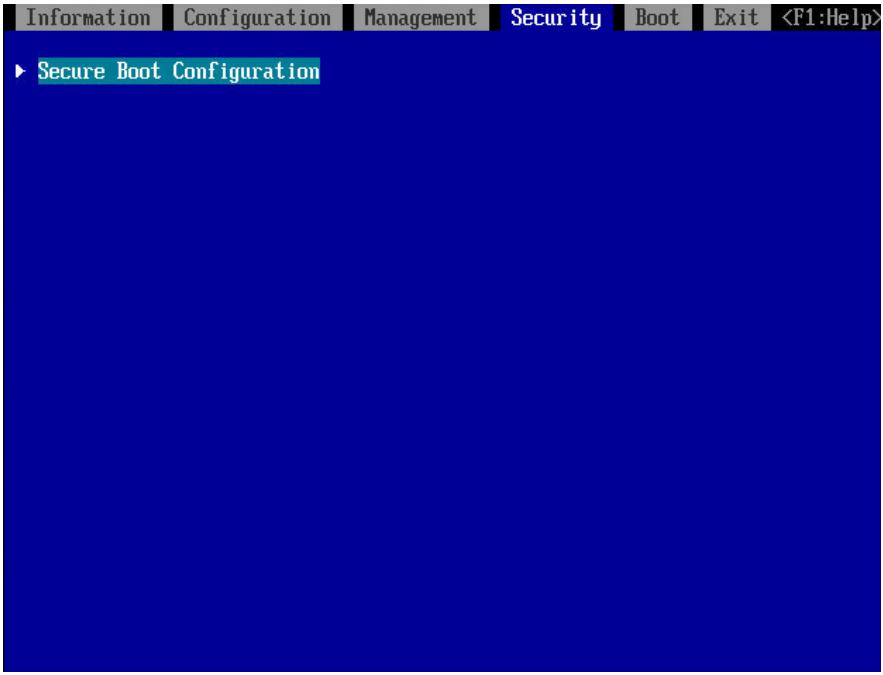

図 8: 「**Security**」メニューの例

Secure Boot Configuration

ファームウェア実行認証プロセスを定義するサブメニューを呼び出します（73 ページの「Secure Boot Configuration」を参照）。

6.1 Secure Boot Configuration

Current Secure Boot State

「**Secure Boot**」機能が有効かどうかを示します。

Enabled
「**Secure Boot**」がアクティブです。

Disabled
「**Secure Boot**」が非アクティブです。

このサブメニューで「**Reset Secure Boot Keys**」を選択し、「**Attempt Secure Boot**」が有効の場合、初期キーがロードされ、「**Secure Boot**」が「**Enabled**」になります。

「**Attempt Secure Boot**」の設定が無効の場合に PK を削除すると、「**Secure Boot**」が「**Disabled**」になります。

Attempt Secure Boot
プラットフォームのリセットの後、「**Secure Boot**」機能を有効または無効にします。

この項目はチェックボックスです。

[ ]
「**Secure Boot**」が非アクティブです。

[X]
「**Secure Boot**」がアクティブです。

Secure Boot Mode
「**Custom Secure Boot Options**」サブメニューを使用可能にするかどうかを指定します。

Standard Mode
「**Custom Secure Boot Options**」サブメニューは使用できません。

Custom Mode
「**Custom Secure Boot Options**」は使用できます。

6.1.1 Reset Secure Boot Keys

デフォルト変数のデータでキーを登録します。

6.1.2 Custom Secure Boot Options

「**Secure Boot**」に必要な鍵と署名のデータベースを削除、変更、追加するサブメニュー。

PK Options
PK を登録または削除します（75 ページの「PK Options」を参照）。

KEK Options
KEK を登録または削除します（75 ページの「KEK Options」を参照）。

DB Options
署名を登録または削除します（75 ページの「DB Options」を参照）。

DBX Options
DBX を登録または削除します（76 ページの「DBX Options」を参照）。

DBT Options
DBT を登録または削除します（76 ページの「DBT Options」を参照）。

6.1.2.1 PK Options

Enroll PK
PK フォームの登録に移行します。

Delete PK
PK を削除または維持します。

6.1.2.2 KEK Options

Enroll KEK
KEK フォームの登録に移行します。

Delete KEK
KEK フォームの削除に移行します。

6.1.2.3 DB Options

Enroll Signature
署名を登録します。

Delete Signature
署名を削除します。

6.1.2.4 DBX Options

Enroll Signature
署名を登録します。

Delete Signature
署名を削除します。

6.1.2.5 DBT Options

Enroll Signature
署名を登録します。

Delete Signature
署名を削除します。

7 「Boot」メニュー

このメニューでは、以下のパラメータを設定できます。一部、特定の条件でのみ使用できる設定があります。

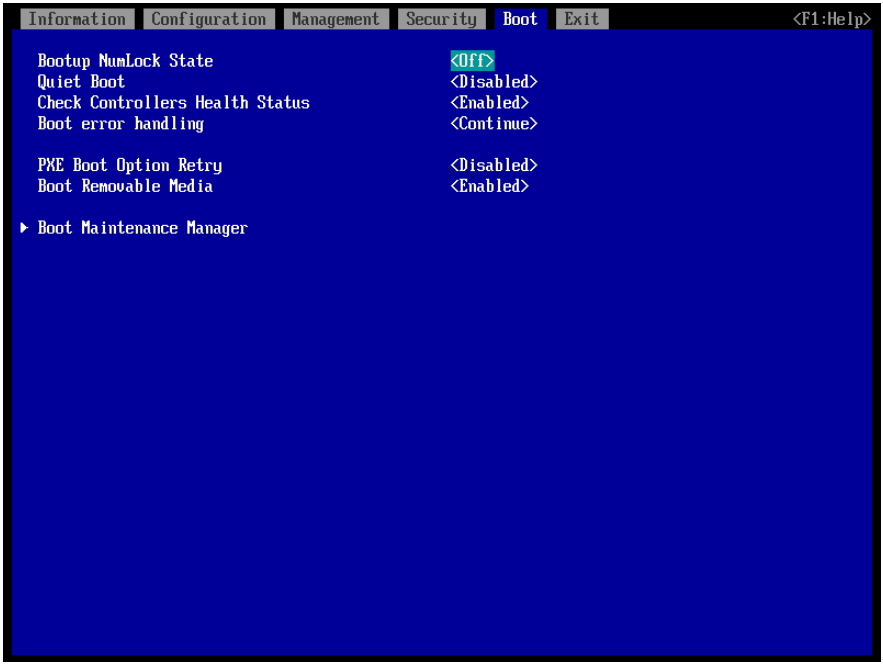

図 9: 「**Boot**」メニューの例

このメニューおよび「**Boot Maintenance Manager**」サブメニューを使用して、システムを起動するドライブのシーケンスを定義できます。

操作については、このメニューのヘルプ領域を参照してください。

Bootup NumLock State

システムが起動したときに NumLock 機能の設定を指定します。NumLock はキーボードのテンキーの使用方法を制御します。

On

NumLock は有効で、キーボードのテンキーを使用できます。

Off

NumLock は無効で、キーボードのテンキーのカーソル機能を使用できます。

キーボードの Num 表示ランプは現在の「**Bootup NumLock State**」を報告します。キーボードの [Num] キーで、On / Off の切り替えができます。

Quiet Boot

POST 起動時の情報ではなく、ブートロゴが画面に表示されます。

Disabled

POST 起動時の情報が画面に表示されます。

Enabled

ブートロゴが表示されます。

Check Controllers Health Status

PCIe デバイスの UEFI ドライバオプション ROM が Controller Health インターフェースをサポートしている場合は、UEFI FW は、UEFI FW が管理しているデバイスのヘルス状態を UEFI ドライバオプション ROM に問い合わせることができます。

Disabled

コントローラのヘルス状態は、UEFI FW でチェックされません。

Enabled

UEFI FW は、コントローラのヘルス状態をチェックします。

Boot error handling

エラーの検出時にシステムのブートプロセスを一時停止し、システムを停止するかどうかを指定します。

Continue

システムブートは一時停止しません。エラーは可能な限り無視されます。

Pause and wait for key

エラーが POST 中に検出された場合、システムブートは一時停止します。

PXE Boot Option Retry
EFI ベースの PXE ブートオプションを無限に再試行するかどうかを指定します。

Disabled
PXE ブートオプションは再試行されません。

Enabled
PXE ブートオプションは無限に再試行されます。

Boot Removable Media
USB スティックなどのリムーバブルデバイスからのブートのサポートが可能かどうかを指定します。

Disabled
リムーバブルデバイスからのブートは無効化されます。

Enabled
リムーバブルデバイスからのブートは有効化されます。

7.1 Boot Maintenance Manager

このサブメニューでは、次のブートオプション設定を行うことができます。

- 「**Boot Options**」の順序の追加または削除または変更。
- ブートローダーファイルからのブート。
- POST 画面でのキー入力の待機時間。

7.1.1 Boot Options

Add Boot Option
EFI アプリケーションまたはリムーバブルファイルシステムをブートオプションとして追加します（80 ページの「Add Boot Option」を参照）。

Delete Boot Option
ブートオプションを削除します（80 ページの「Delete Boot Option」を参照）。

Change Boot Order
ブート順位を変更します（80 ページの「Change Boot Order」を参照）。

7.1.1.1 Add Boot Option

Device Path
UEFI で認識されるストレージデバイス内にある OS のブートローダーファイルを指定して、ブートオプションを追加します。

7.1.1.2 Delete Boot Option

Boot Option
指定されたブートオプションをブート順位から削除します。

Commit Changes and Exit
変更を保存して終了します。

Discard Changes and Exit
変更を破棄して終了します。

7.1.1.3 Change Boot Order

Change the order
ブート順位を変更します。

Commit Changes and Exit
変更を保存して終了します。

Discard Changes and Exit
変更を破棄して終了します。

7.1.2 Boot From File

Device Path

UEFI で認識されるストレージデバイス内にある OS のブートローダーファイルを指定して、即座にブートします。

7.1.3 Set Time Out Value

Auto Boot Time-out

タイムアウトの時間を指定します。

0 ... 65535

0 は待機時間なし、65535 はシステムがキーを待機することを意味します。

Commit Changes and Exit

変更を保存して終了します。

Discard Changes and Exit

変更を破棄して終了します。

7.1.4 Reset System

Reset System

システムをリセットします。

8 「Exit」 メニュー

このメニューでは、以下のパラメータを設定できます。

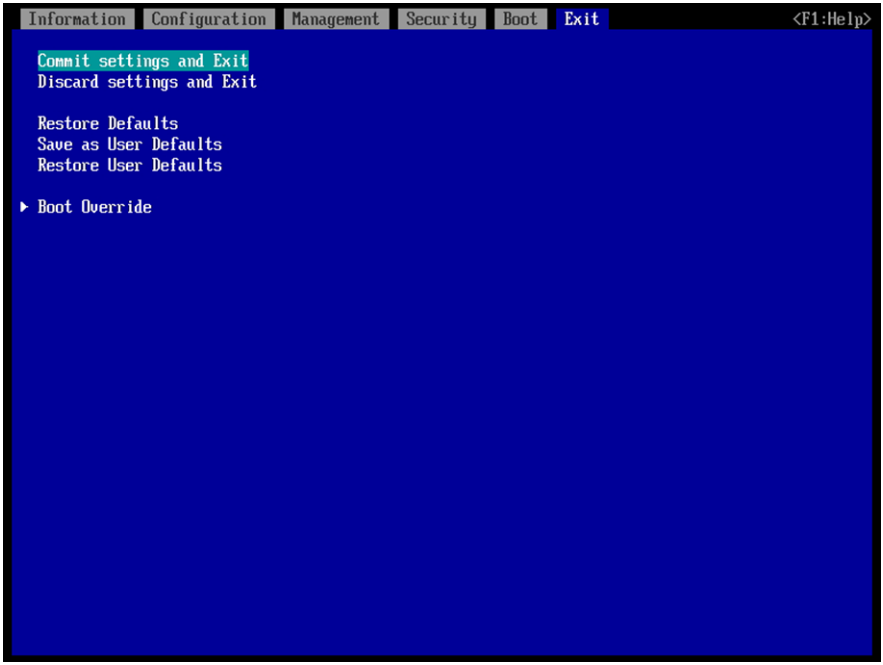

図 10: 「**Exit**」メニューの例

Commit settings and Exit

現在のメニューエントリを保存し、BIOS セットアップユーティリティを終了するには、「**Commit settings and Exit**」を選択し、「**Yes**」を選択します。

新しい設定が有効になり、変更されたオプションでリセットが不要であれば POST が継続します。

Discard settings and Exit

「**Discard settings and Exit**」を選択し、「**Yes**」を選択すると、BIOS セットアップユーティリティの起動後、または「**Save Changes**」の呼び出し後に行った変更が破棄されます。
BIOS セットアップユーティリティが閉じられ、POST が継続します。

Restore Defaults

すべての BIOS セットアップユーティリティメニューをリセットしてデフォルト値を使用するには、「**Restore Defaults**」を選択し、「**Yes**」を選択します。
これらの設定で BIOS セットアップユーティリティを終了するには、「**Commit settings and Exit**」を選択し、「**Yes**」を選択します。

Save as User Defaults

「**Save as User Defaults**」を選択した後「**Yes**」を選択して、これまで行った変更をユーザデフォルトとして保存します。

Restore User Defaults

すべての BIOS セットアップユーティリティメニューをリセットしてユーザデフォルト値を使用するには、「**Restore User Defaults** 」を選択し、「**Yes**」を選択します。これらの設定で BIOS セットアップユーティリティを終了するには、「**Commit settings and Exit**」を選択し、「**Yes**」を選択します。

Boot Override

ブートプロセスを定義するサブメニューを呼び出します（84 ページの「Boot Override」を参照）。

8.1 Boot Override

Boot Device Name

[Enter] を押して、選択したドライブからブートを開始します。設定が維持されないと、以下のメッセージが表示されます。

```
Settings have not committed. Commit Settings and exit?.
```

[Y] を押して確定、[N] を押して変更を破棄して終了します。[ESC] を押してキャンセルします。

9 デバイスパス

デバイスパスには、デバイスの物理的な接続と、PCI Route Bridge への接続の関係が表示されます。

9.1 デバイスパスのパラメータ

表示されるデバイスパスの各パラメータは、以下の表に記載されています。

画面	説明
PcieRoot (UID)	PCI express Root Bridge UID とは、Unique ID の略です。
Pci（Device、Function）	PCI デバイス Device とは、PCI デバイスのデバイス番号のことです。0-31 を 16 進数で表します。 Function とは、PCI デバイスのファンクション番号のことです。PCI デバイスのファンクション番号は 0-7 で示されます。
Scsi（PUN、LUN）	Scsi コントローラ PUN とは、Physical Unit Number の略です。SCSI ID の意。0-65535 を 16 進数で表します。 LUN とは、Logical Unit Number の略です。0-65535 を 16 進数で表します。
Fibre（WWN、LUN）	Fibre コントローラ WWN とは、World Wide Name の略です。World Wide Name は 64 bit 数値で表します。 LUN とは、Logical Unit Number の略です。Logical Unit Number は 64 bit 数値で表します。
MAC (MACAddr、IfType)	Network MacAddr とは、Mac Address の略です。 IfType とは、Interface Type の略です。0-255 を 16 進数で表します。

画面	説明
HD （Partition、Type、Signature、Start、Size）	Hard Drive Partition とは、パーティション番号を表します。 Type とは、パーティションタイプを表します。（省略可）以下のタイプがあります。 ● GPT とは、GUID Partition Table の略です。 ● MBR とは、Master Boot Record の略です。 Signature は、パーティションタイプにより以下のような意味を持ちます。 ● GPT：GUID を表します。 ● MBR：数値です。 Start は、パーティションの先頭位置を示します。パーティションの先頭位置は 64bit 数値で表します。 Size は、パーティションのサイズを示します。パーティションサイズは 64bit 数値で表します。
CDROM （Entry、Start、Size）	CD/DVD メディア Entry は、ブートエントリ番号を表します。（省略可）通常は 0 を示します。 Start に、ブートエントリの先頭セクタを表します。ブートエントリの先頭セクタは 64bit 数値で表します。 Size はパーティションサイズを示します。パーティションサイズは 64bit 数値で表します。
USB（Port、Interface）	USB Port は、USB のポート番号を示します。0-255 を 16 進数で表します。 Interface は、インターフェース番号を示します。0-255 を 16 進数で表します。
Ctrl（Controller）	コントローラ Controller には整数が入ります。

9.2 デバイスパスの識別

DU_SAS 内の SAS ディスク、Fibre カード経由のディスク、および LAN のデバイスパスの識別方法について、以下に説明し ます。

DU_SAS 内蔵 SAS ディスク

例として、DU_SAS に内蔵された SAS ディスクの特定方法について説明します。

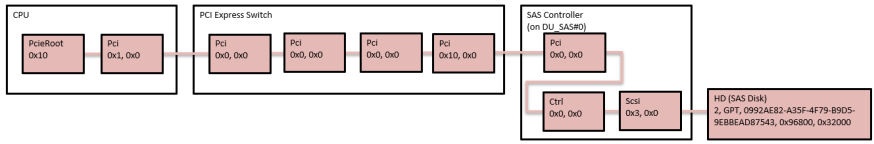

図 11: DU_SAS に内蔵された SAS ディスクの特定

デバイスパスは以下のとおりです。

PcieRoot(0x10)/Pci(0x1,0x0)/Pci(0x0,0x0)/Pci(0xC,0x0)/Pci(0x0,0x0)/
Pci(0x10,0x0)/Pci(0x0,0x0)/Ctrl(0x0,0x0)/Scsi (0x3,0x0)/HD(2, GPT,
0992AE82-A35F-4F79-B9D5-9EBBEAD87543, 0x96800, 0x32000)

Fibre カードからのディスクの特定

例として､IOU の PCIe スロットに Fibre カードを挿した場合の Fibre 接続からのディスク特定方法について説明します。

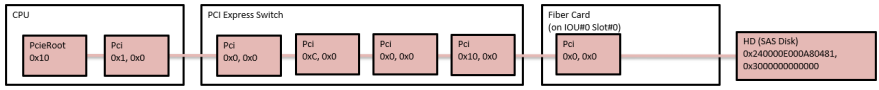

図 12: Fibre カードのディスクの特定

デバイスパスは以下のとおりです。

PcieRoot(0x10)/Pci(0x1,0x0)/Pci(0x0,0x0)/Pci(0xC,0x0)/Pci(0x0,0x0)/
Pci(0x10,0x0)/Pci(0x0,0x0)/Fibre(0x240000E000A80481,0x3000000000000)

LAN カードからの LAN の特定方法

例として、IOU の PCIe スロットに LAN カードを挿した場合の LAN の特定方法について説明します。

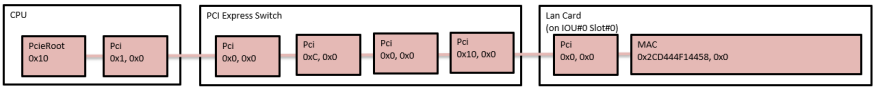

図 13: LAN の特定

LAN のデバイスパスは以下のとおりです。

PcieRoot(0x10)/Pci(0x1,0x0)/Pci(0x0,0x0)/Pci(0xC,0x0)/Pci(0x0,0x0)/
Pci(0x10,0x0)/Pci(0x0,0x0) MAC(2CD444F14458,0x0)

10 付録 A

10.1 sadump Configuration ツール

sadump Configuration ツールでは、sadump の環境を設定できます。

sadump 環境の設定は、UEFI 構成情報に保存されます。設定内容を復元するには、バックアップを実施して ください。

sadump Configuration ツールを開く

▶「**Configuration**」メニューを選択します。

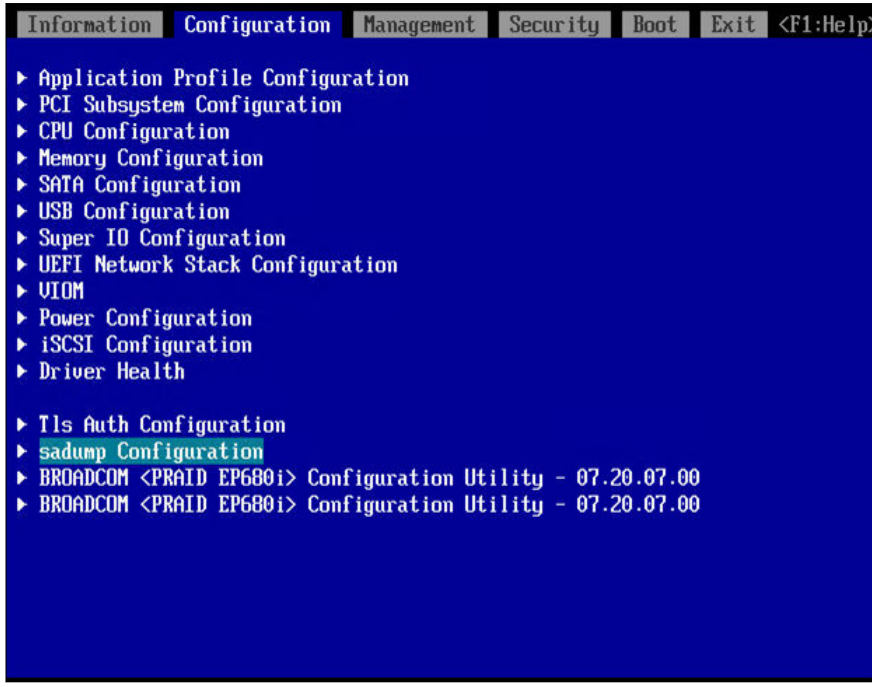

図 14:「**Configuration**」メニュー

▶「**Configuration**」メニューで「**sadump Configuration**」を選択して、sadump メインメニューを開きます。

10.1.1 sadump メインメニュー

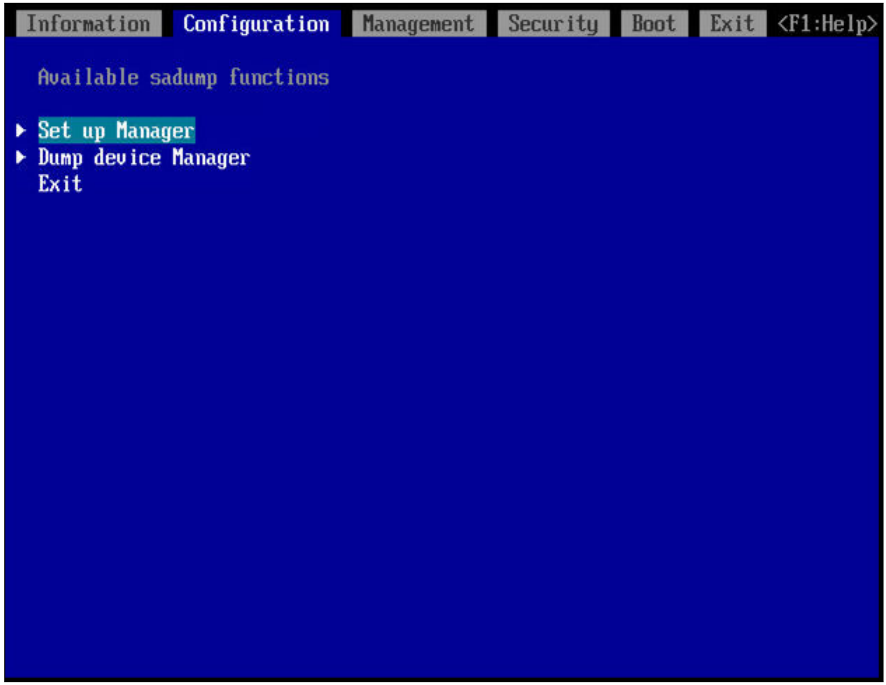

図 15: sadump メインメニュー

このメニューでは、sadump またはダンプデバイスのセットアップを開始できます。

Set up Manager

「**sadump セットアップ**」メニューを開きます。

Dump device Manager

「**ダンプデバイスのメンテナンス**」メニューを開きます。

Exit

sadump メインメニューを閉じます。

[Esc]、[F9]、[F10] を操作しないでください。

10.1.2 Set up Manager

▶ sadump メインメニューから「**Set up Manager**」メニューを選択します。
sadamp セットアップメニューが表示されます。

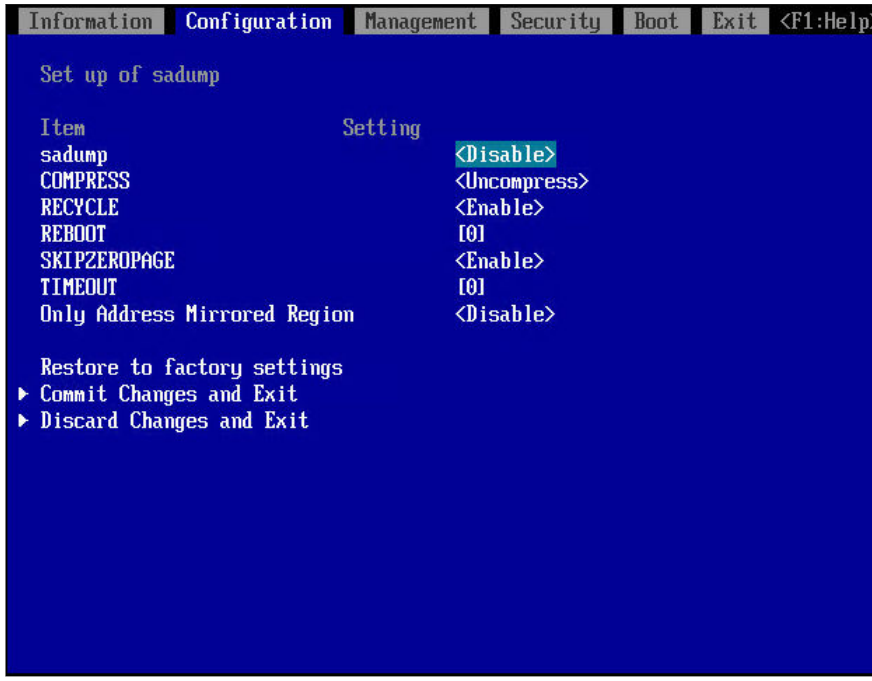

図 16: 「**Set up of sadump** 」メニュー

このメニューには、sadump 環境の設定項目がリストされます。sadump が設定されていない初期状態では、 以下のように表示されます。

▶ sadamp の以下の項目を設定します。

- sadump 機能を有効または無効にします。
- sadump がダンプデバイスに書きこむ際の形式を指定します。
- ダンプデバイスの再利用を有効または無効にします。**Enable** を指定した場合、最も古いダンプが上書きされます。
- ダンプ後の sadump の動作を指定します。
- Skip Zero Page を有効または無効にします。
- sadump の収集を中断する時間を指定します。
- 「ミラーリングされた領域のみアドレス」機能を有効または無効にします。

▶「**Restore to factory settings**」をクリックして、すべての値をデフォルトの工場出荷時の設定にリセットします。

▶「**Commit Changes and Exit**」で、変更を保存してこのメニューを終了します。

「**Discard Changes and Exit**」で、変更を保存せずにこのメニューを終了します。

[Esc]、[F9]、[F10] を操作しないでください。

10.1.3 Dump device Manager

▶ sadump メインメニューから「**Dump device Manager**」を選択します。
「**Maintain the dump device**」メニューが表示されます。

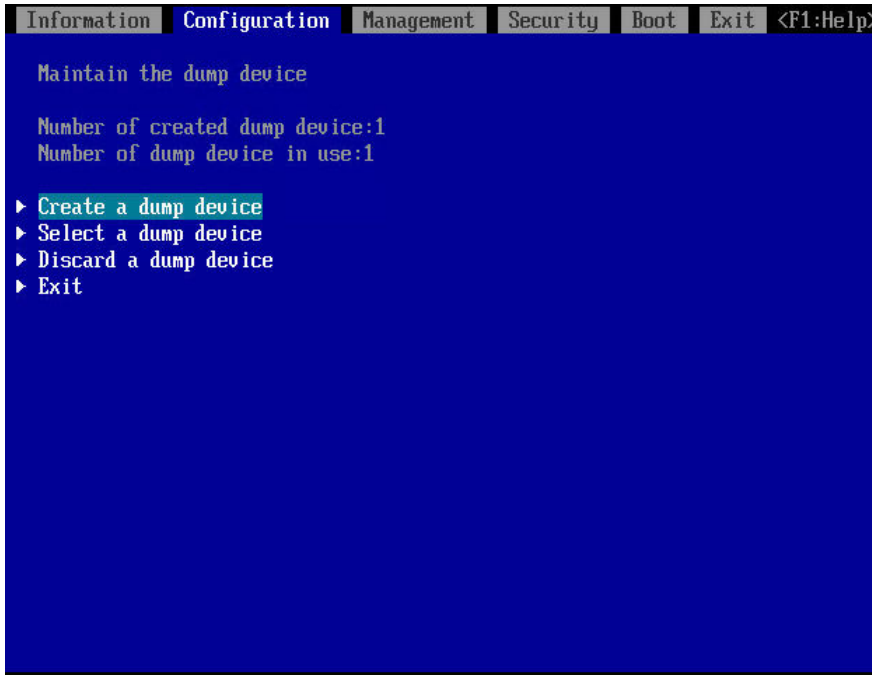

図 17: 「**Maintain the dump device** 」メニュー

「**Maintain the dump device**」に、すでに作成されているダンプデバイスの数と、すでに設定されているダンプデバイスの数が表示されます。

このメニューでは、ダンプデバイスを作成、セットアップ、破棄できます。

[Esc]、[F9]、[F10] を操作しないでください。

10.1.3.1 1 つのディスクまたは 1 つのパーティションでダンプデバイスを作成します。

OS 上から sadump デバイスを初期化することを推奨します。

▶「**Maintain the dump device**」メニュー内の「**Create a dump device**」メニューを選択します。

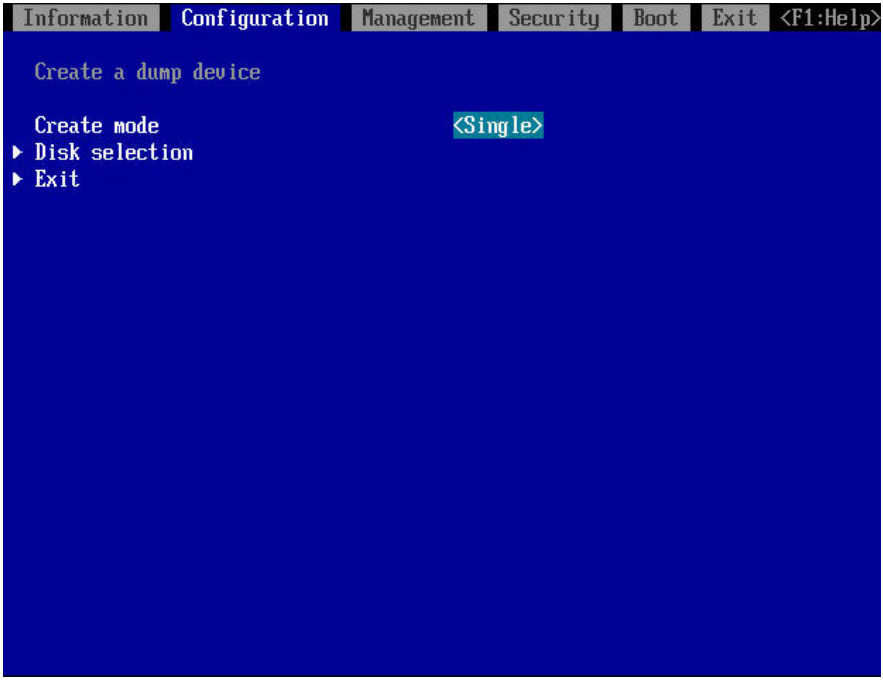

図 18: **Create a dump device** メニュー（シングルモード）

「**Create a dump device**」メニューが表示されます。

▶ ダンプデバイスのモードを選択します。1 つのディスクまたは 1 つのパーティションでダンプデバイスを作成するには、「**Create mode**」を「**Single**」に設定します。

1 つのディスクまたは 1 つのパーティションでダンプデバイスを作成して冗長に設定するには、「**Single**」を選択して、複数の sadump デバイスを構成します。

▶「**Disk selection**」をクリックします。

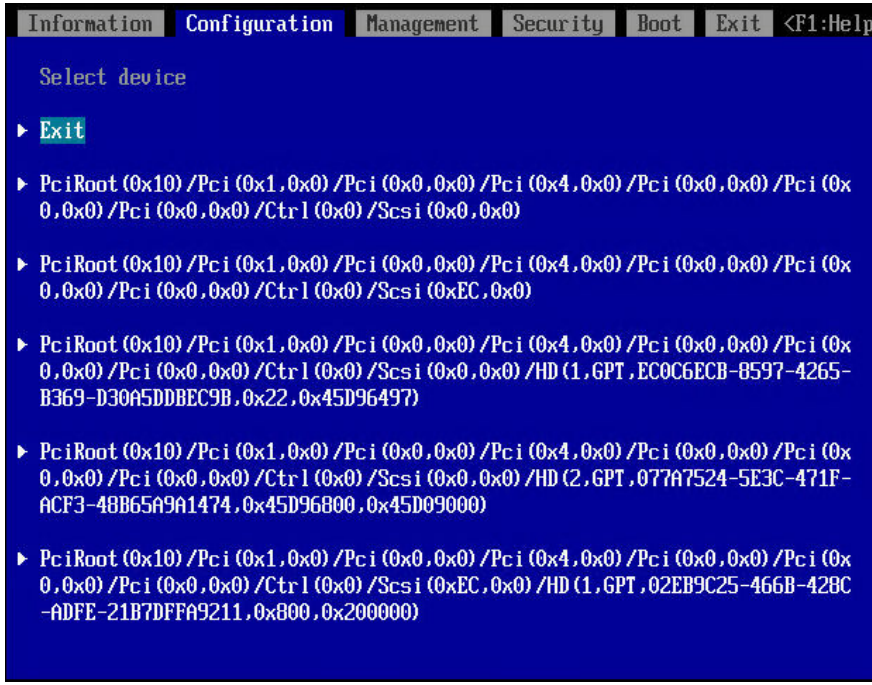

図 19:「**Select device** 」メニュー

「**Select device**」メニューが表示されます。

▶ ディスクまたはディスクパーティションの ACPI 名を選択して、ダンプデバイスを作成します。

ディスクまたはディスクパーティションに使用される ACPI 名については、85 ページの「デバイスパス」 を参照してください。

▶ [Enter] を押してダンプデバイスを作成し、「**Create a dump device**」メニューに戻ります。

「**Exit**」をクリックして、ダンプデバイスを作成せずに「**Create a dump device**」メニューに戻ります。

注意

データの破損

ダンプデバイスを選択するときに、正しいハードディスクが選択されていることを再度確認します。正しくないドライブが選択されると、データディスクは破損します。

備考：ディスクまたはディスクパーティションを表示する ACPI 名については、85 ページの「デバイスパス」を参照してください。

ETERNUS のデバイスをダンプデバイスとして使用するには、事前に UEFI ドライバのセットアップが必要です。

ダンプデバイスは作成時に初期化されます。選択したディスクまたはディスクパーティションの大きさに応じて、ダンプデバイスの初期化に時間がかかる場合があります。場合によっては、次のウィンドウに移動するまで、ダンプの初期化に数分以上かかることがあります。

10.1.3.2 複数のディスクを持つダンプデバイスの作成

OS 上から sadump デバイスを初期化することを推奨します。

システムメモリが大容量でディスクが 1 つでは十分でない場合、複数のディスクを持つダンプデバイスを作成します。

▶「**Maintain the dump device**」メニュー内の「**Create a dump device**」メニューを選択します。

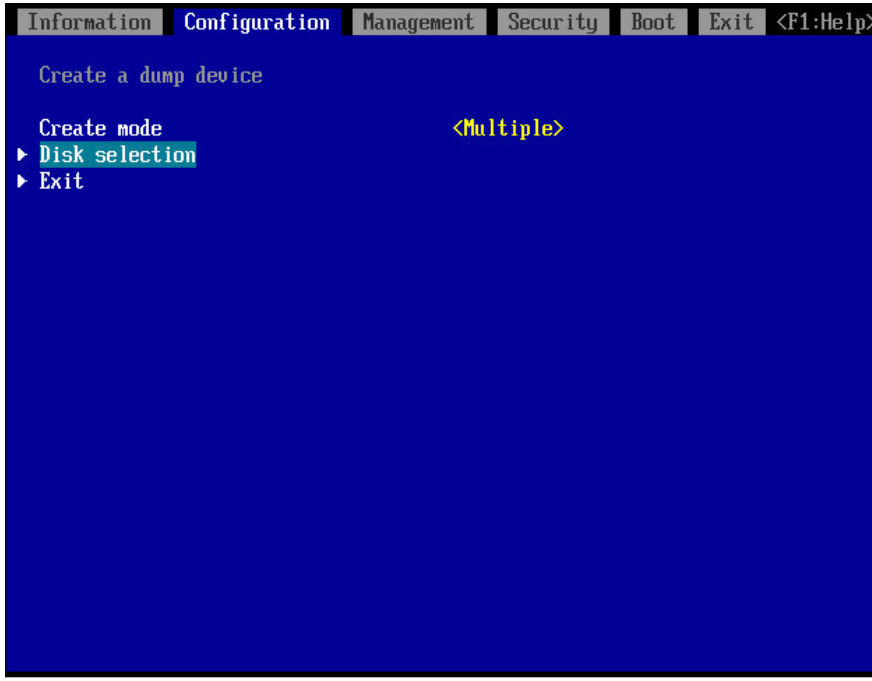

図 20: **Create a dump device** メニュー（マルチモード）

「**Create a dump device**」メニューが表示されます。

▶ ダンプデバイスのモードを選択します。複数のディスクを持つダンプデバイスを作成するには、「**Create mode**」を「**Multiple**」に設定します。

▶「**Disk selection**」をクリックします。

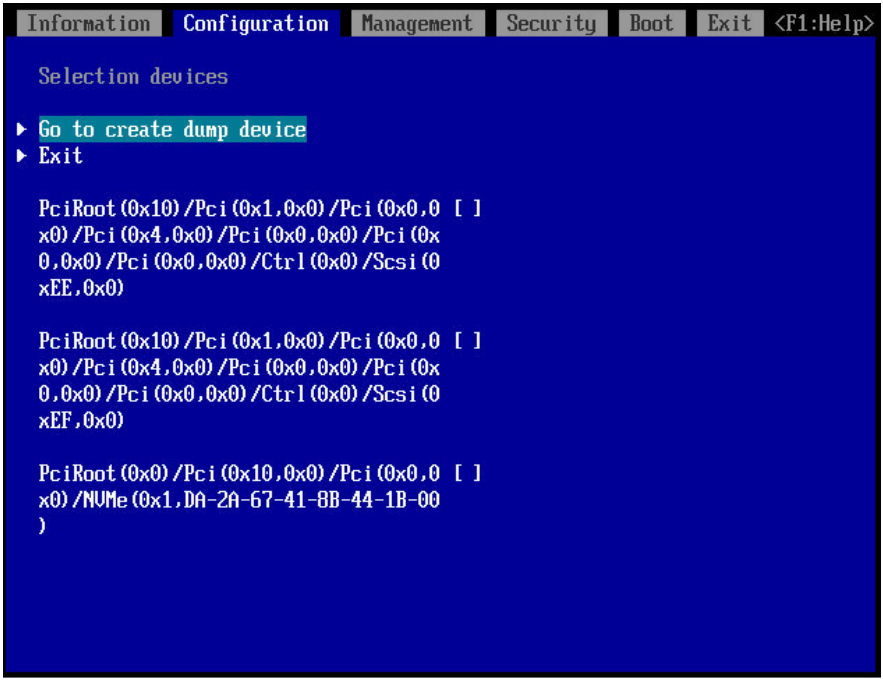

図 21: **Selection devices** メニュー（複数のデバイス）

「**Selection devices**」メニューが表示されます。

▶ ディスクまたはディスクパーティションの ACPI 名を選択して、ダンプデバイスを作成します。

ディスクまたはディスクパーティションに使用される ACPI 名については、85 ページの「デバイスパス」 を参照してください。

▶「**Go to create dump device** 」をクリックしてダンプデバイスを作成します。「**Confirmation**」メニューが開きます。

▶「**Create dump device and Exit**」をクリックして、ダンプデバイスの構成を保存し、「**Confirmation**」メニューを終了します。

または、「**Exit**」をクリックして、いずれのダンプデバイスも保存せずこのメニューを終了します。

10.1.3.3 ダンプデバイスのセットアップ

▶「**Maintain the dump device**」メニュー内の「**Select a dump device**」メニューを選択します。

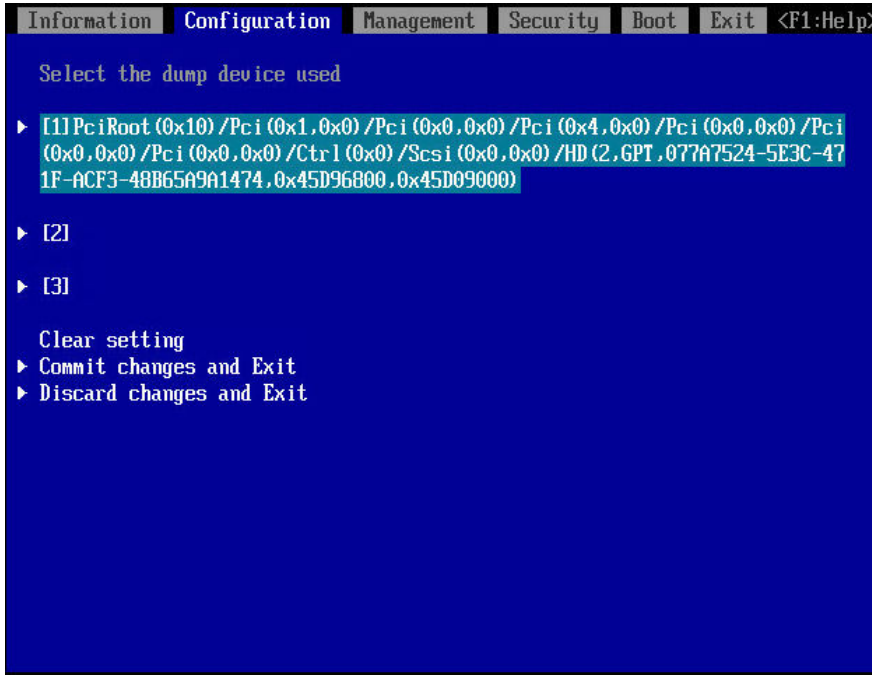

図 22:「**Select the dump device used** 」メニュー

「**Select the dump device used**」メニューが表示されます。

▶「**[1]**」、「**[2]**」、または「**[3]**」をクリックして、1 つ目、2 つ目、または 3 つ目のダンプデバイスを選択します。

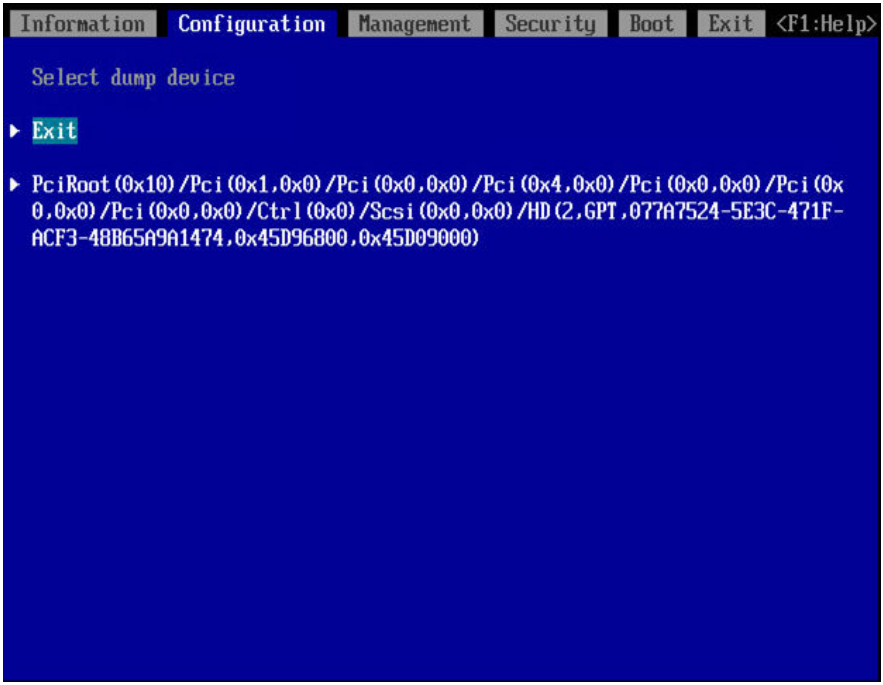

図 23: 「**Select dump device** 」メニュー

「**Select dump device**」メニューが表示されます。

- ▶ 1 つ目、2 つ目、または 3 つ目のダンプデバイスに対して、ディスクまたはディスクパーティションの ACPI 名を選択します。
- ▶ [Enter] キーを押して「**Select the dump device used**」メニューに戻ります。

  「**Exit**」をクリックして、ダンプデバイスを作成せずに「**Select the dump device used**」メニューに戻ります。
- ▶ 「**Commit Changes and Exit**」で、変更を保存してこのメニューを終了します。

  「**Discard Changes and Exit**」で、変更を保存せずにこのメニューを終了します。

10.1.3.4 ダンプデバイスの破棄

▶「**Maintain the dump device**」メニューで「**Discard a dump device**」を選択し、不要なダンプデバイスを破棄します。

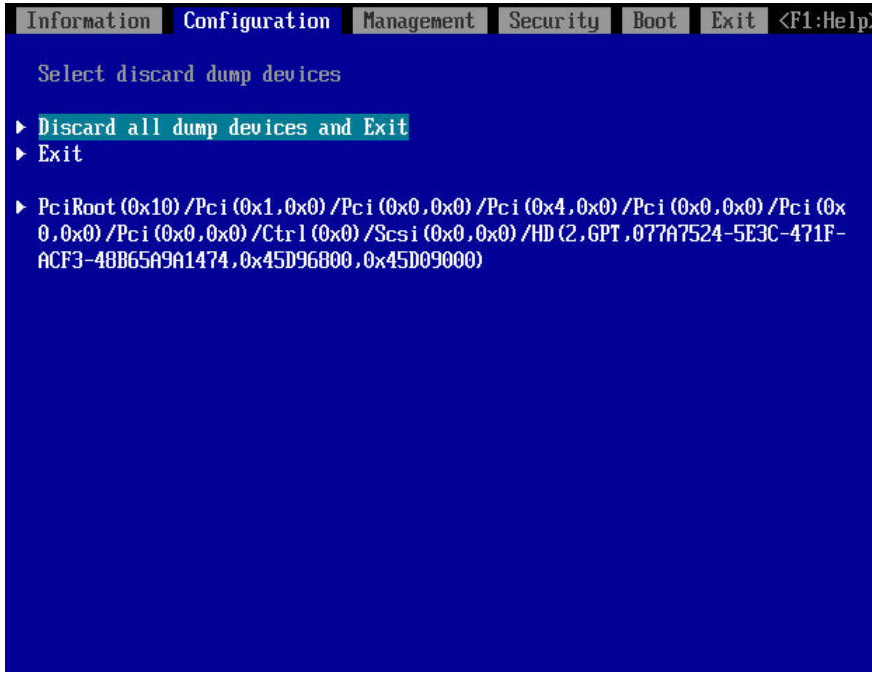

図 24:「**Select discard dump devices** 」メニュー

「**Select discard dump devices**」メニューが表示されます。

▶ ダンプデバイスの ACPI 名を選択します。

▶ [Enter] キーを押して選択したダンプデバイスを破棄しこのメニューを終了します。

▶「**Discard all dump devices and Exit** 」をクリックして、すべてのダンプデバイスを破棄しこのメニューを終了します。

「**Exit**」をクリックして、いずれのダンプデバイスも破棄せずこのメニューを終了します。

10.2 ブートオプションの取り扱い方法

ブートオプションの追加または削除とブート優先順位レベルの変更は、**Boot Maintenace Manager** の「**Boot Options**」メニューで行うことができます。操作するメニューにカーソルを置いて [Enter] キーを押すと、各メニューを表示できます。

10.2.1 ブートオプションの追加

Add Boot Option で **Boot Options** メニューに新しいブートオプションを追加できます。OS ブートローダがブートオプションとして追加、登録されている場合、登録されたブートオプションは **Boot Options** メニューに表示されます。

新しく追加および登録されたブートオプションは、「**Boot Options**」メニューのタグの末尾に追加されます。

- ▶「**Boot**」メニューを選択します。
- ▶ ブートオプションを取り扱うには、「**Boot**」メニューで「**Boot Maintenance Manager**」サブメニューを選択します。

►「**Add Boot Option**」を選択して、追加のブートオプションを **Boot Options** メニューに追加します。「**Add Boot Option**」メニューが表示されます。

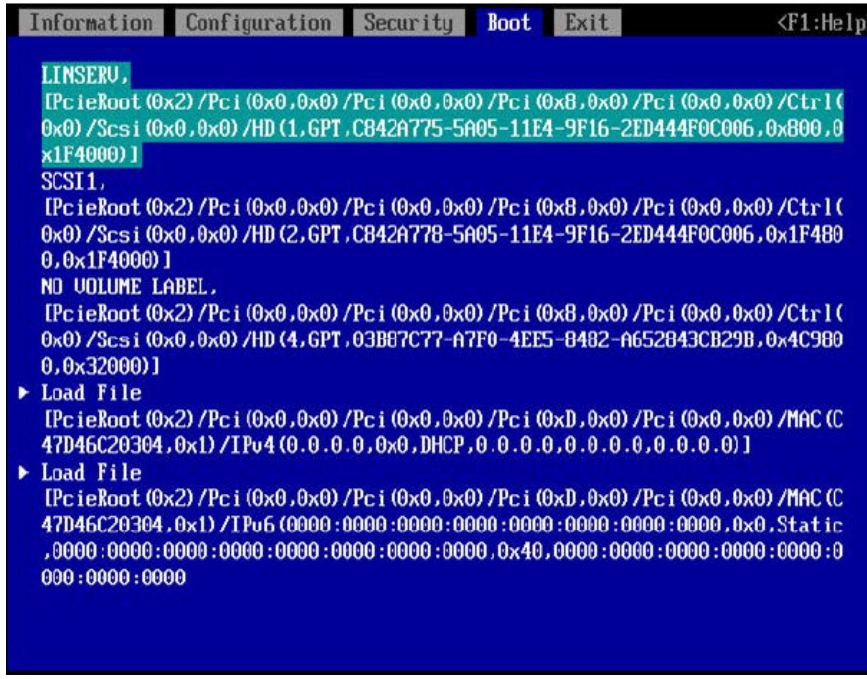

図 25: ブートオプションの追加

▶ デバイスリストから起動ファイルを追加し、保存するストレージデバイスを選択します。

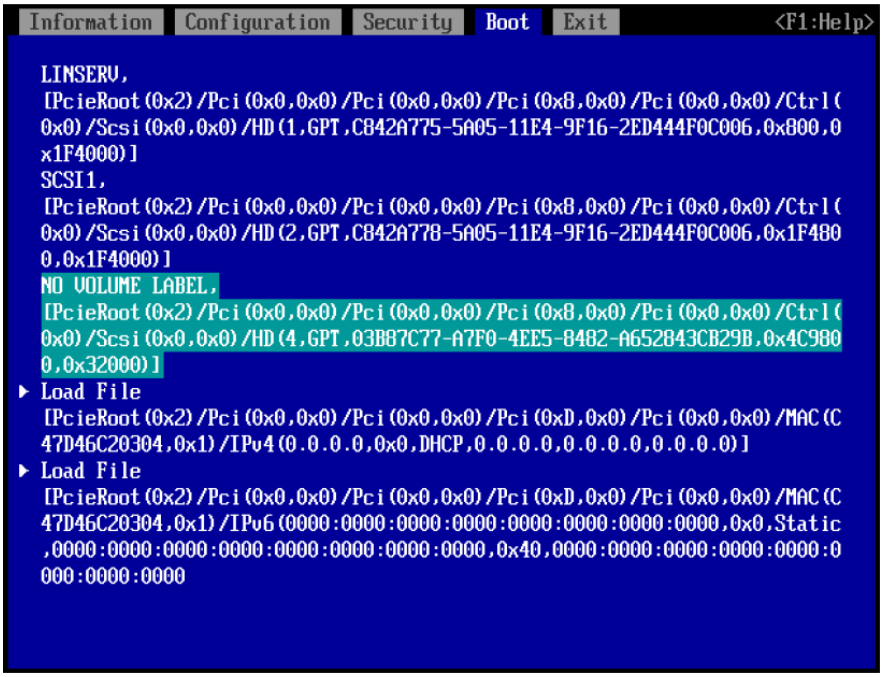

図 26: デバイスの選択（例）

► [Enter] を押します。

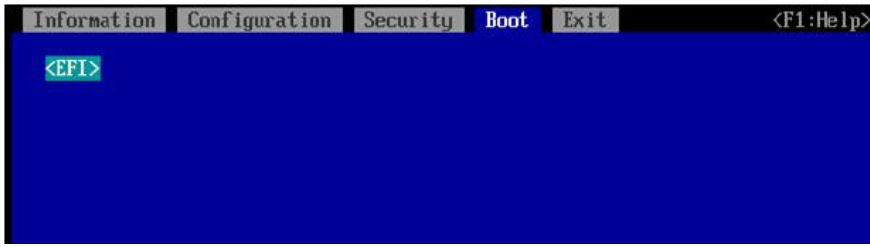

図 27: 「**File Selection**」メニュー内のファイルのリスト（例）

選択したストレージデバイスのファイルのリストが表示されます。< >で囲まれた内容はディレクトリです。たとえば、Windows Server 2016 によってインストールされたディスクが選択されている場合は、<EFI>と表示されます。

► ディレクトリ構造に従います。

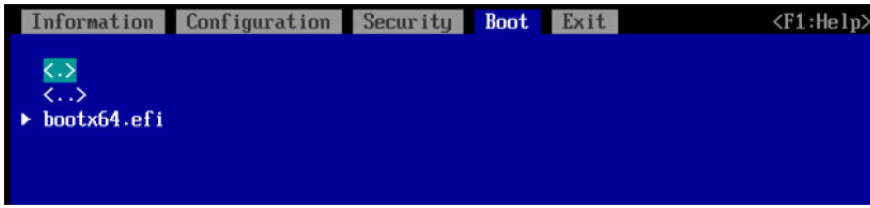

図 28: ファイル選択メニュー（Windows Server 2016 Installed Disk Window の例）

以下のファイルは OS のブートローダです。

- Windows の場合は、**\EFI\Boot\bootx64.efi** を参照してください。
- Red Hat Enterprise Linux の場合は、 **/EFI/redhat/shim.efi** を参照してください。
- SUSE Linux Enterprise Server の場合は、**/EFI/sles/shim.efi** を参照してください。

▶ 例えば、追加登録された OS ローダーとして、**bootx64.efi** を選択します。

▶ [Enter] を押します。

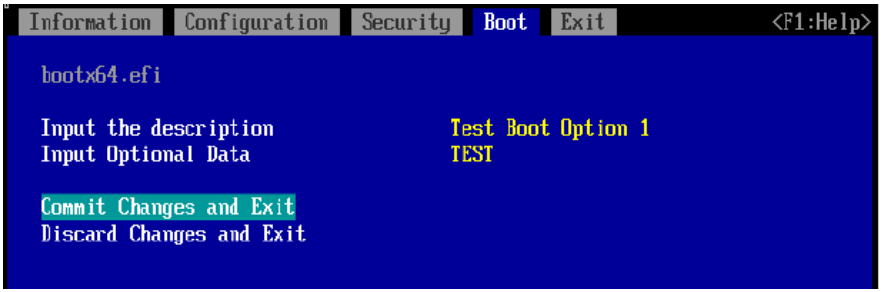

図 29: ブートオプション名とオプションの変更の例

このメニューでは、ブート時にブートオプション名とオプションを設定できます。

▶ ブートオプション名を設定するには、カーソルを「**Input the description**」に設定し、[Enter] を押します。ポップアップウィンドウが開き、ブートオプション名を入力できます。

入力できる文字数と文字の種類の詳細は、107 ページの「入力できる文字数と文字の種類」 を参照してください。

▶ ブート時にオプションを設定するには、**Input Optional Data** にカーソルを置き、[Enter] を押します。ポップアップウィンドウが開き、名前を入力できます。

入力できる文字数と文字の種類の詳細は、107 ページの「入力できる文字数と文字の種類」 を参照してください。

▶「**Commit Changes and Exit**」で、変更を保存してこのメニューを終了します。

または、「**Discard Changes and Exit**」で、変更を保存せずにこのメニューを終了します。。

入力できる文字数と文字の種類

項目	文字数	文字の種類
Input the description	6 ～ 75	0 ～ 9、A ～ Z、a ～ z、 ! " # $ % & ' ( ) * + -/ : ; < = > ? @ [¥] ^ _ ` { | } ~
Input Optional Data	0 ～ 120	0 ～ 9、A ～ Z、a ～ z、 ! " # $ % & ' ( ) * + -/ : ; < = > ? @ [¥] ^ _ ` { | } ~

文字数が制限値を超えた場合は入力できません。制限値を超えるキーが一時的に入力されても無視され、ウィンドウに表示されなくなります。

上記以外の文字タイプは入力できません。一時的に入力されても、無視され、ウィンドウに表示されなくなります。

Input the description の文字数が 0 ～ 5 の範囲の場合は、ポップアップウィンドウが開き、「**Please enter enough characters**.というメッセージが表示されます。続けるには、[Enter] を押します。

ブートオプションが正しく追加されたことを確認する

ブートオプションが正しく追加されたことを確認するには、次の手順に従います。

- ▶「**Boot Options**」メニューから「**Change Boot Order**」メニューを開きます。
- ▶ 追加したブートオプションがリストの最後に表示されることを確認します。
- ▶「**Discard Changes and Exit**」を選択して [Enter] を押します。

10.2.2 ブートオプションの削除

Delete Boot Option を使用して、指定したブートオプションをブート順位から削除できます。

▶「**Boot**」メニューを選択します。

▶ ブートオプションを取り扱うには、「**Boot** 」メニューで「**Boot Maintenance Manager**」サブメニューを選択します。

▶「**Delete Boot Option**」を選択します。

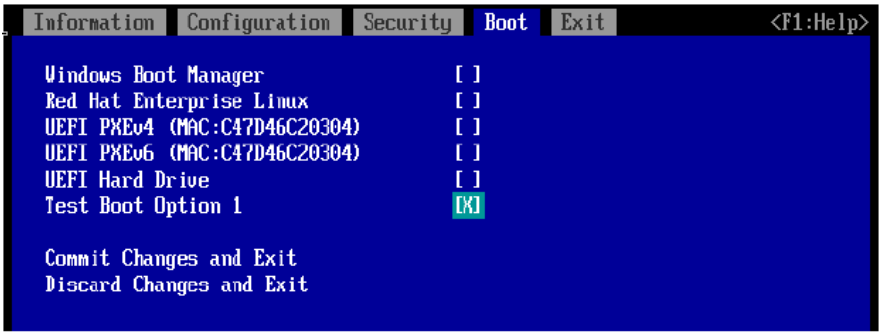

図 30:「**Delete Boot Option**」メニュー

「**Delete Boot Options**」メニューが表示されます。

▶ ブート順位から削除するブートオプションにカーソルを合わせます。

▶ [スペース] を押してブートオプションを選択します[ ] は [X] に変更されました。

選択をキャンセルするには、もう一度 [スペース] を押します。[X] は [ ] に変更されました。
[スペース] を再び押すと [ ] が [X] に戻ります。

▶ 変更した設定を保存してこのメニューを終了するには、「**Commit Changes and Exit**」を選択して [Enter] を押します。選択されたブートオプションは、**Boot Options** メニューから削除されます。

変更した設定を保存せずにこのメニューを終了するには、「**Discard Changes and Exit**」を選択して [Enter] を押します。

ブートオプションが正しく削除されたことを確認する

ブートオプションが正しく削除されたことを確認するには、次の手順に従います。

▶「**Boot Options**」メニューから「**Change Boot Order**」メニューを開きます。

▶ 削除されたブートオプションがリストにもう存在しないことを確認します。

▶「**Discard Changes and Exit**」を選択して [Enter] を押します。

10.2.3 ブートオプションの順位の変更

「**Change Boot Order**」でブート順位を変更できます。

▶「**Boot**」メニューを選択します。

▶ ブートオプションを取り扱うには、「**Boot**」メニューで「**Boot Maintenance Manager**」サブメニューを選択します。

▶「**Change Boot Order**」を選択します。

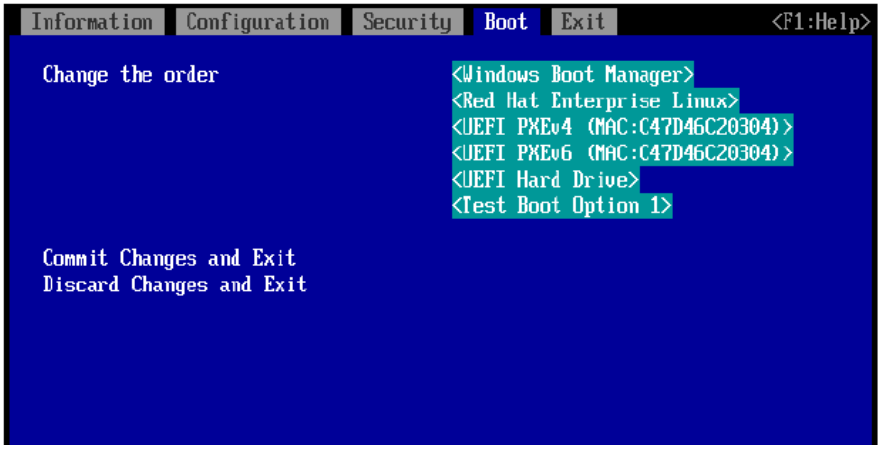

図 31:「**Change Boot Order**」メニュー（1）

「**Change Boot Order**」メニューが表示されます。

▶ **Change the order** の後ろに表示されるブートオプションにカーソルを置き、[Enter] を押します。

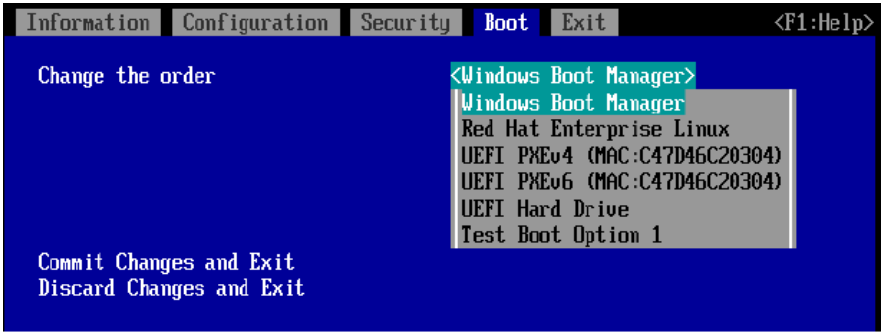

図 32: 「**Change Boot Order**」メニュー（2）

ポップアップウィンドウが開きます。

▶ 順位を変更したいブートオプションにカーソルを置きます。

▶ 優先順位を変更するには、[+] キーを押して優先順位を上げるか、または [-] キーを押して優先順位を下げます。

▶ [Enter] を押して変更した設定を保存し、ポップアップウィンドウを閉じます。

または [Esc] キーを押して変更した設定を破棄し、ポップアップウィンドウを閉じます。

▶ 変更されたブート順位を保存してこのメニューを終了するには、「**Commit Changes and Exit**」を選択して [Enter] を押します。

または、変更したブート順位を保存せずにこのメニューを終了するには、「**Discard Changes and Exit**」を選択して [Enter] を押します。

11 付録 B

11.1 設定項目の一覧

11.1.1 Information メニューの設定項目

このメニューには、システム情報が表示されます。一部のオプションは、特定の条件でのみ使用できます。

設定項目	初期値	設定可能値
System Date / System Time	パーティションの時計の日付/時刻	System Time (HH:MM:SS) ● HH：時間 ● MM：分 ● SS：秒 System Date (MM/DD/YYYY) ● MM：月 ● DD：日 ● YYYY：西暦

11.1.2 「Configuration」メニューの設定項目

11.1.2.1 「PCI Subsystem Configuration」メニューの設定項目

「**PCI Subsystem Configuration**」メニューの項目設定に使用できる初期値と設定可能値を一覧で示します。

設定項目	初期値	設定可能値
ASPM Support	Disabled	Disabled L1 Only
PCIe 10-bit Tag	Auto	Disabled Auto

設定項目	初期値	設定可能値
PCIe Latency Tolerance Reporting (LTR)	Auto	Disabled Auto
SR-IOV Support	Enabled	Disabled Enabled

11.1.2.2 「CPU Configuration」メニューの設定項目

「**CPU Configuration**」メニューの項目設定に使用できる初期値と設定可能値を一覧で示します。

設定項目	初期値	設定可能値
Hyper-Threading	Enabled	Disabled Enabled
Active Processor Cores	0	0-28
Dynamic SST-PP	Disabled	Disabled Enabled
Hardware Prefetcher	Enabled	Disabled Enabled
Adjacent Cache Line Prefetch	Enabled	Disabled Enabled
DCU Streamer Prefetcher	Enabled	Disabled Enabled
DCU IP Prefetcher	Enabled	Disabled Enabled
Intel Virtualization Technology	Enabled	Disabled Enabled
Intel (R) VT-d(3)	Enabled	Disabled Enabled
Pre-boot DMA Protection	Disabled	Disabled Enabled

設定項目	初期値	設定可能値
Intel TXT Support (1)	Disabled	Disabled Enabled
Total Memory Encryption (TME)	Disabled	Disabled Enabled
TME Bypass	Auto	Auto Disabled Enabled
Total Memory Encryption Multi-Tenant (TME-MT)	Disabled	Disabled Enabled
Memory integrity	Disabled	Disabled Enabled
SGX Reset	Disabled	Disabled Enabled
SW Guard Extensions (SGX)	Disabled	Disabled Enabled
SGX Package Info In-Band Access	Disabled	Disabled Enabled
SGX PRM Size	1G	128M 256M 512M 1G 2G 4G 8G 16G 32G 64G 128G 256G 512G
SGX QoS	Enabled	Disabled Enabled

設定項目	初期値	設定可能値
Select Owner EPOCH input type	Manual User Defined Owner EPOCHs	SGX Owner EPOCH activated Change to New Random Owner EPOCHs Manual User Defined Owner EPOCHs
Software Guard Extensions Epoch 0	0	0...FFFFFFFFFFFFFFFF
Software Guard Extensions Epoch 1	0	0...FFFFFFFFFFFFFFFF
SGX Launch Control Policy	Unlocked	Intel Locked Unlocked Locked
SGXLEPUBKEYHASH0	0	0...FFFFFFFFFFFFFFFF
SGXLEPUBKEYHASH1	0	0...FFFFFFFFFFFFFFFF
SGXLEPUBKEYHASH2	0	0...FFFFFFFFFFFFFFFF
SGXLEPUBKEYHASH3	0	0...FFFFFFFFFFFFFFFF
SGX Auto MP Registration	Disabled	Disabled Enabled
Enhanced SpeedStep	Enabled	Disabled Enabled
Turbo Mode	Enabled	Disabled Enabled
Optimized Power Mode	Disabled	Disabled Enabled
Energy Performance	Performance	Performance Balanced Performance Balanced Energy Energy Efficient

設定項目	初期値	設定可能値
Override OS Energy Performance(2)	Disabled	Disabled Enabled
Utilization Profile (2) (5)	Even	Even Unbalanced
P-State Coordination	HW_ALL	HW_ALL SW_ALL
HWPM Support	Native Mode	Disabled Native Mode OOB Mode Native Mode with no legacy
CPU C1E Support	Enabled	Disabled Enabled
CPU C6 Report	Enabled	Disabled Enabled
Package C State limit	C0	C0 C2 C6 C6 (Retention) No Limit
CPU C1 auto demotion	Enabled	Disabled Enabled
CPU C1 auto undemotion	Enabled	Disabled Enabled
UPI Link Frequency Select	Auto	Auto 12.8GT/s 14.4GT/s 16.0GT/s
UPI Link L0p	Enabled	Disabled Enabled
UPI Link L1	Enabled	Disabled Enabled
Local x2APIC (3)	Disabled	Disabled Enabled

設定項目	初期値	設定可能値
IODC Configuration	Auto	Disabled Auto Enable for Remote InvItoM Hybrid PushEnable for Remote InvItoM AllocFlow Enable for Remote InvItoM Hybrid AllocFlow Enable for Remote InvItoM and Remote WCiLF
Uncore Frequency Scaling	Auto	Auto Maximum Power Balanced
Stale AtoS	Auto	Disabled Enabled Auto
LLC Dead Line Alloc	Enabled	Disabled Enabled
AVX ICCP pre-grant level	no override	no override 128 Heavy 256 Light 256 Heavy 512 Light 512 Heavy
L2 RFO Prefetch	Enabled	Disabled Enabled
Monitor MWAIT	Enabled	Disabled Enabled
LLC Prefetch	Disabled	Disabled Enabled
Homeless Prefetch	Auto	Disabled Enabled Auto
FB Thread Slicing	Disabled	Disabled Enabled

設定項目	初期値	設定可能値
LMCE Support (4)	Disabled	Disabled Enabled
Limit CPU Physical Address to 46 bits	Enabled	Disabled Enabled
DBP-F	Disabled	Disabled Enabled
4UPI	Enabled	Disabled Enabled
CPU Performance Boost	Disabled	Disabled Moderate Aggressive

(1) **Intel Vt-d** で **Disabled** を選択した場合、あるいは、**Security Configuration** で **TPM Support** を選択した場合、この設定項目は表示されるのみで、変更することはできません。

(2) **HWPM Support** で **OOB mode** を選択した場合、この設定項目は表示されるのみで、変更することはできません。

(3) **Local x2APIC** が **Enabled** の場合、 **Intel VT-d** は設定にかかわらず、有効になります。

(4) **Enabled** を選択し、OS が Local Machine Check Exception (LMCE)機能をサポートしている場合のみ、LMCE 機能を使用できます。

(5) **Override OS Energy Performance** で **Disabled** を選択している場合、この設定項目は表示されるのみで、変更することはできません。

11.1.2.3 「Memory Configuration」メニューの設定項目

「**Memory Configuration**」メニューの項目設定に使用できる初期値と設定可能値を一覧で示します。

設定項目	初期値	設定可能値
Virtual NUMA	Disabled	Disabled Enabled
SNC (Sub NUMA)	Disabled	Disabled Enable SNC2 (2-clusters) Enable SNC4 (4-clusters)
DDR Performance	Performance optimized	Performance optimized Energy optimized
PPR Type	Soft PPR	PPR Disabled Hard PPR Soft PPR
Patrol Scrub	Disabled	Disabled Enabled
DDR5 ECS	Disabled	Disabled Enabled
FastBoot Mode	Disabled	Disabled Enabled
Volatile Memory Mode	1LM	1LM 2LM

「Address Range Mirroring Configuration」メニューの設定項目

「**Address Range Mirroring Configuration**」メニューの項目設定に使用できる初期値と設定可能値を一覧で示します。

設定項目	初期値	設定可能値
Mirror Memory Below 4GB (1)	Disabled	Disabled Enabled
Mirrored Amount Above 4GB (1)	0	0 … 5000

(1) この項目は、UEFI ブート搭載 VMware ESXi でのみ使用できます。

これらの項目を設定するには、最初に関連する SB の「**SB#x メモリモード**」パラメータを iRMC Web インターフェースの「**アドレス範囲ミラー**」に設定する必要があります。

11.1.2.4 「SATA Configuration」メニューの設定項目

「**SATA Configuration**」メニューの設定項目の初期値と設定可能値を一覧で示します。

設定項目	初期値	設定可能値
SATA Mode	AHCI	AHCI RAID
SATA Controller 2	Enabled	Disabled Enabled

11.1.2.5 「Security Configuration」メニューの設定項目

設定項目	初期値	設定可能値
TPM Support	Disabled	Disabled Enabled
Pending TPM operation	None	None TPM Clear Set NoPPIClear flag to FALSE
有効な PCR バンクの変更	No change	No change SHA256 SHA384 All

11.1.2.6 「USB Configuration」メニューの設定項目

「USB Port Security」メニューの設定項目

設定項目	初期値	設定可能値
USB Port Control (1)	Enable all ports	Enable all ports Disable all ports Enable used ports
USB Device Control	Enable all devices	Enable all devices Enable Keyboard and Mouse only Enable all devices except mass storage devices/ Hubs

11.1.2.7 「UEFI Network Stack Configuration」メニューの設定項目

設定項目	初期値	設定可能値
Network Stack	Enabled	Disabled Enabled
Ipv4 PXE Support	Disabled	Disabled Enabled
Ipv4 HTTP Support	Disabled	Disabled Enabled
Ipv6 PXE Support	Disabled	Disabled Enabled
Ipv6 HTTP Support	Disabled	Disabled Enabled

設定項目 **Ipv4 PXE Support**、**Ipv4 HTTP Support**、**Ipv6 PXE Support** および **Ipv4 HTTP Support** は、**Network Stack** が **Enabled** の場合に表示されます。

11.1.2.8 「VIOM」メニューの設定項目

設定項目	初期値	設定可能値
VIOM-flag	Disabled	Disabled Enabled

11.1.3 「Management」メニューの設定項目

設定項目	初期値	設定可能値
Fan Control	Auto	Auto Full

11.1.4 「Security」メニューで項目の設定

11.1.4.1 「Secure Boot Configuration」メニューの設定項目

設定項目	初期値	設定可能値
Attempt Secure Boot	「 」	「 」 O
Secure Boot Mode	Standard Mode	Standard Mode Custom Mode

[ ]は、**Secure Boot** が有効でないことを意味しています。
[x] は、**Secure Boot** が有効であることを意味します。

11.1.5 「Boot」メニューの設定項目

設定項目	初期値	設定可能値
Bootup NumLock State	Off	On Off
Quiet Boot	Disabled	Disabled Enabled

設定項目	初期値	設定可能値
Check Controllers Health Status	Enabled	Disabled Enabled
Boot error handling	Continue	Continue Pause and wait for key
PXE Boot Option Retry	Disabled	Disabled Enabled
Boot Removable Media	Enabled	Disabled Enabled

11.1.5.1 「Boot Maintenance Manager」メニューの設定項目

設定項目	初期値	設定可能値
Auto Boot Time-out	15	0～65535

11.2 推奨設定

Fujitsu サーバ PRIMEQUEST 4000 は工場出荷時点で最も一般的なアプリケーションシナリオ向けにパフォーマンスとエネル ギー効率の最適な比率を提供する標準 BIOS 設定で構成されています。ただし、可能な限り最大のスループット (パフォー マンス)、可能な限り最小のレイテンシ (低レイテンシ)、または可能な限り最大の省エネ (エネルギー効率)という要件 に応じて、サーバを設定する際に標準設定からの逸脱が必要な状況になる可能性があります。

BIOS セットアップユーティリティの推奨設定については、以下のマニュアルを参照してください。
https://docs.ts.fujitsu.com/dl.aspx?id=cbcdbe16-0a73-49ce-8765-355602fb16d1

ここに記載されていない BIOS オプションは、パフォーマンス、レイテンシ、電力に影響しないので、初期値のままにしてください。

多くの BIOS オプションは互いに依存関係があります。これらの依存関係によって、特定のオプションを変更した場合に望ましくないシステム動作を発生させる可能性や、さらに同時に他のオプションが変更されたときのみ、目的が達成される可能性があります。BIOS オプションの設定を変更する前に、本 マニュアルの説明を確認することをお勧めします。すべての変更を実 稼動環境に

適用する前に、必要な効果が有効かどうかテスト環境で検証することをお勧めします。

一部の BIOS オプションは、特定の条件下またはサーバモデルにのみ使用できます。表示されない BIOS オプションについては、推奨設定に変更する必要はありません。

11.3 保守モードでの動作

PRIMEQUEST 4000 が保守モードの場合、システムブートプロセスは BIOS セットアップユーティリティの最初のページ（**Information** menu）で停止します。

PRIMEQUEST 4000 が保守モードの場合、設定に関係なく、以下の BIOS メニューまたはパラメータが特別な動作を示します。

USB Port Control

設定に関係なく、システムは **Enable all ports** で一時的に起動します。

USB Device Control

設定に関係なく、システムは **Enable all devices** で一時的に起動します。

「Secure Boot Configuration」サブメニュー

設定に関係なく、システムは **Secure Boot** で一時的に起動します。

Boot Removable Media

設定に関係なく、システムは **Enabled** で一時的に起動します。

索引

R

S

T

U

V

W