

LSI MegaRAID SAS 12G Software Users Guide 追補版

1. 本書について

下記のMegaRAID SASアレイコントローラ(以下、本アレイコントローラ)のご使用にあたって、ユーザーズガイド「LSI MegaRAID SAS 12G Software Users Guide」の記載を補足するものです。

製品名	型名	アレイコントローラ名称
SAS アレイコントローラカード	PY-SR3C41 PYBSR3C41	PRAID EP400i
	PY-SR3C42 PYBSR3C42	PRAID EP420i
	PY-SR3C43 PYBSR3C43	PRAID EP420i
	PY-SR3FA PYBSR3FA	PRAID CP400i
SAS アレイコントローラモジュール	PY-SRD36A PYBSRD36A	PRAID EM400i
	PY-SRD32A PYBSRD32A	PRAID CM400i
SAS アレイコントローラカード	PY-SR3PE PYBSR3PE PYBSR3PEL	PRAID EP420e

2. 留意事項・制限事項

2.1 UEFI モード使用時の制限事項

2.1.1. 本製品を搭載した全ての PCI Slot の Option ROM を Enabled に設定する必要があります。

UEFIモードにてお使いの場合は、サーバ本体のBIOS設定より、本製品を搭載した全てのPCI SlotのOption ROMをEnabledに設定してください。設定方法詳細はサーバ本体のマニュアルをご覧ください。

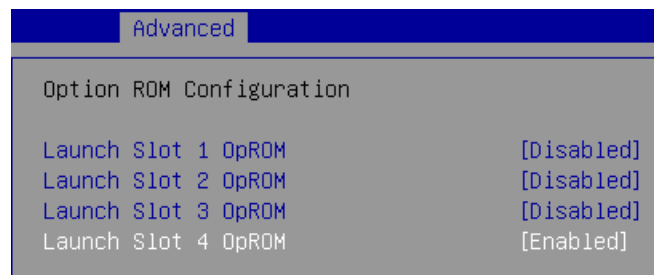


図 1: Option ROM Configuration

2.1.2. Boot Mode 設定にて Stop on errors は使用しないでください。

UEFIモードにてBoot ModeをStop on errorsに設定した場合、停止対象となるハードウェアエラーが発生した際、サーバーが起動しなくなります。本設定は工場出荷値のPause on errorsより変更しないでください。

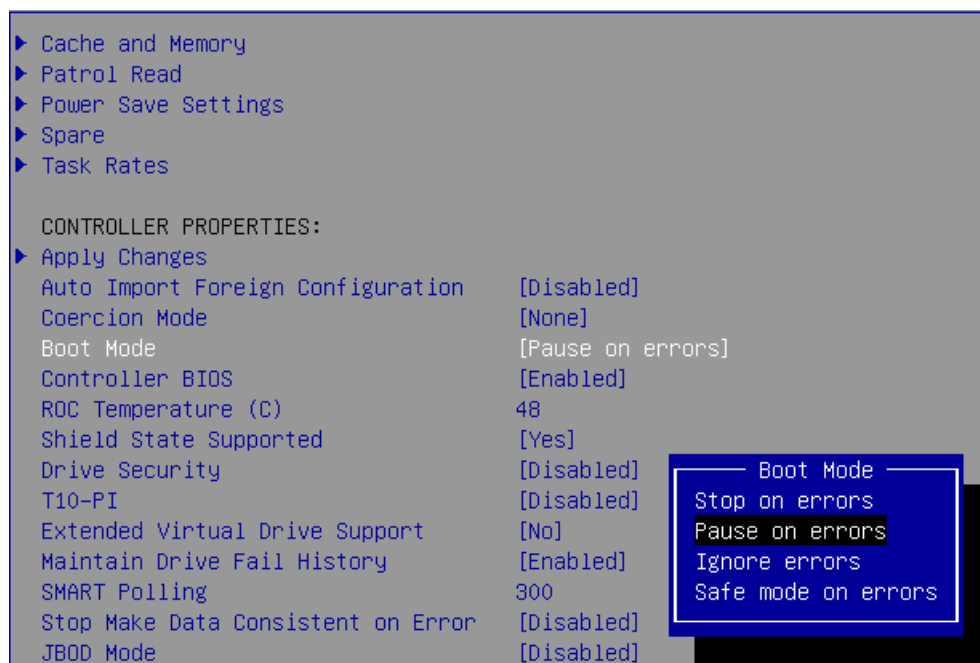


図 2: Boot Mode

2.1.3. Suggest Security Key 機能は未サポートです。

UEFIモードにてSafeStore機能によるセキュリティ設定を有効化する際、「Suggest Security Key」機能を使用してセキュリティキーを自動生成せず、キーボードから直接入力して設定してください。

2.2 SafeStore によるドライブの暗号化

2.2.1. Ctrl-R Utility の機能が一部異なります

ファームウェア版数24.7.0-0061において、ユーザーズガイドの記載と、下記の相違点があります。

- セキュリティキー識別子のSuggest(自動生成)機能は未サポートです。
- ブートパスワードの設定機能がありません。ブートパスワードは未サポートです。

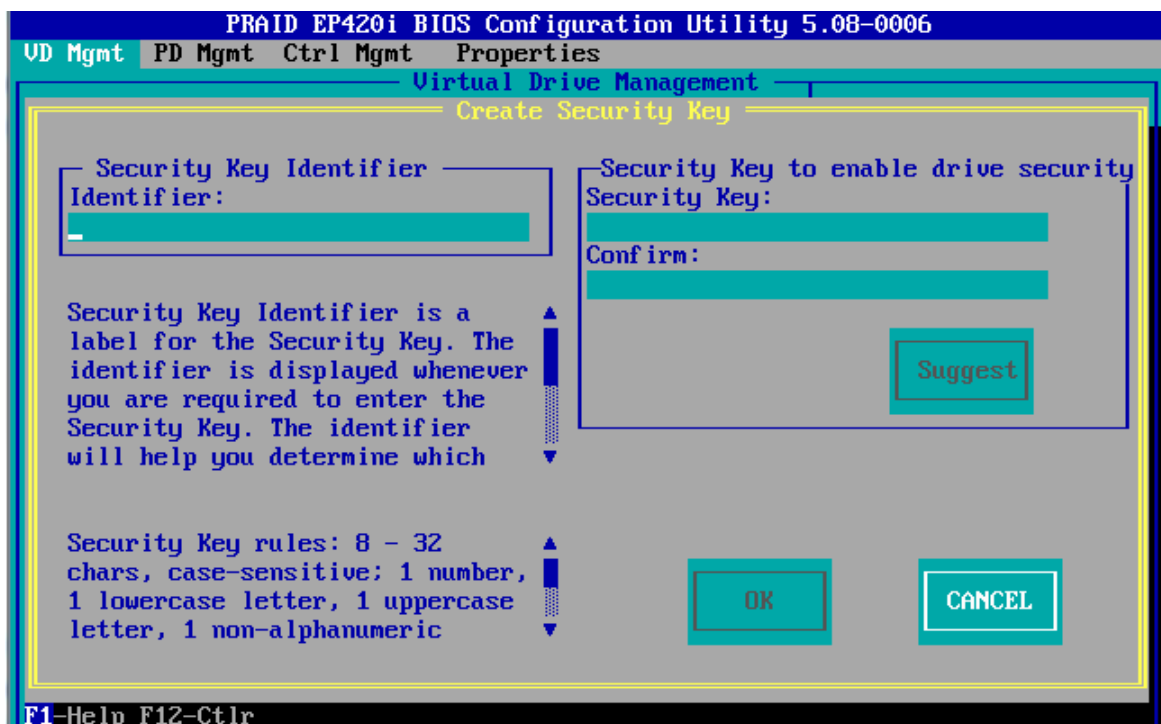


図 3: Create Security Key (FW 24.7.0-0061)

2.2.2. ブートパスワード機能は未サポートです。

PY-SR3C43 / PYBSR3C43およびSED(Self-Encrypting Drive, 自己暗号化ドライブ)を使用してセキュリティ設定を有効に設定する場合、ブートパスワードは使用しないでください。

ブートパスワードを使用する設定をした場合、UEFIモードにてシステムが起動できなくなります。

◆ Ctrl-R Utility の場合

ファームウェア版数24.7.0-0061の場合、Ctrl-R Utilityにブートパスワード設定機能はありません。

ファームウェア版数24.16.0-0097以降の場合、ブートパスワードを使用しない設定でお使いください。

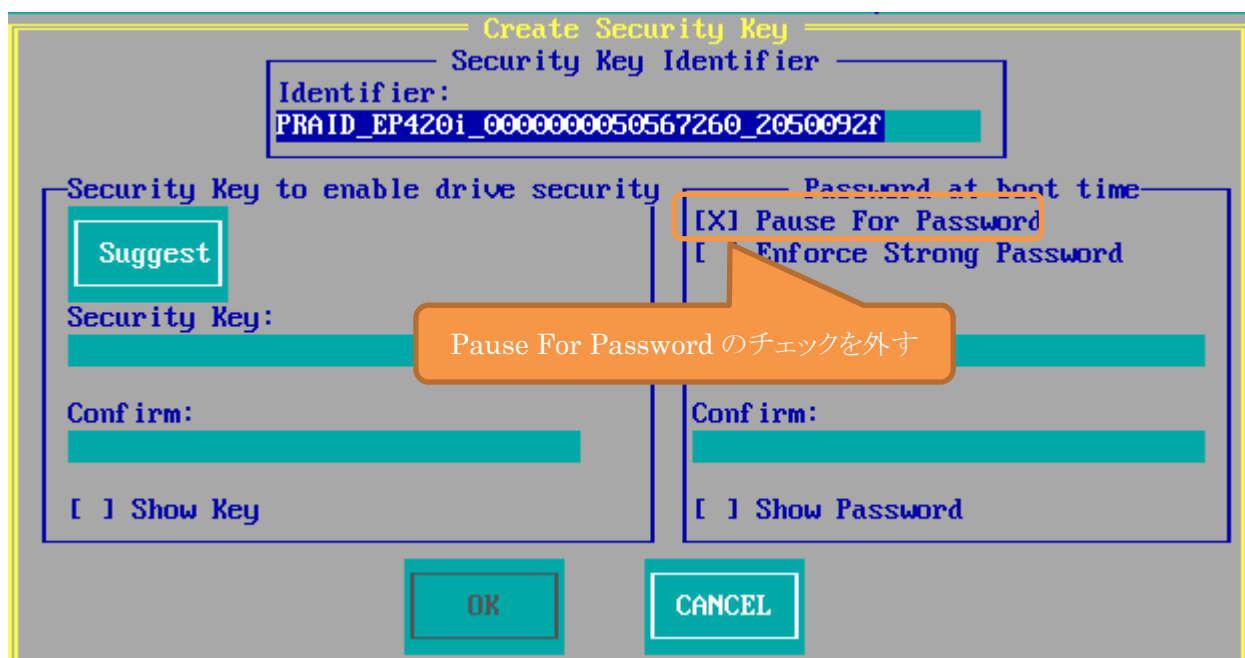


図 4: Disable Boot Password (Ctrl-R Utility, FW24.16.0-0097)

◆ HII Configuration Utility の場合

セキュリティ設定を有効にする際、ブートパスワードを使用しない設定でお使いください。

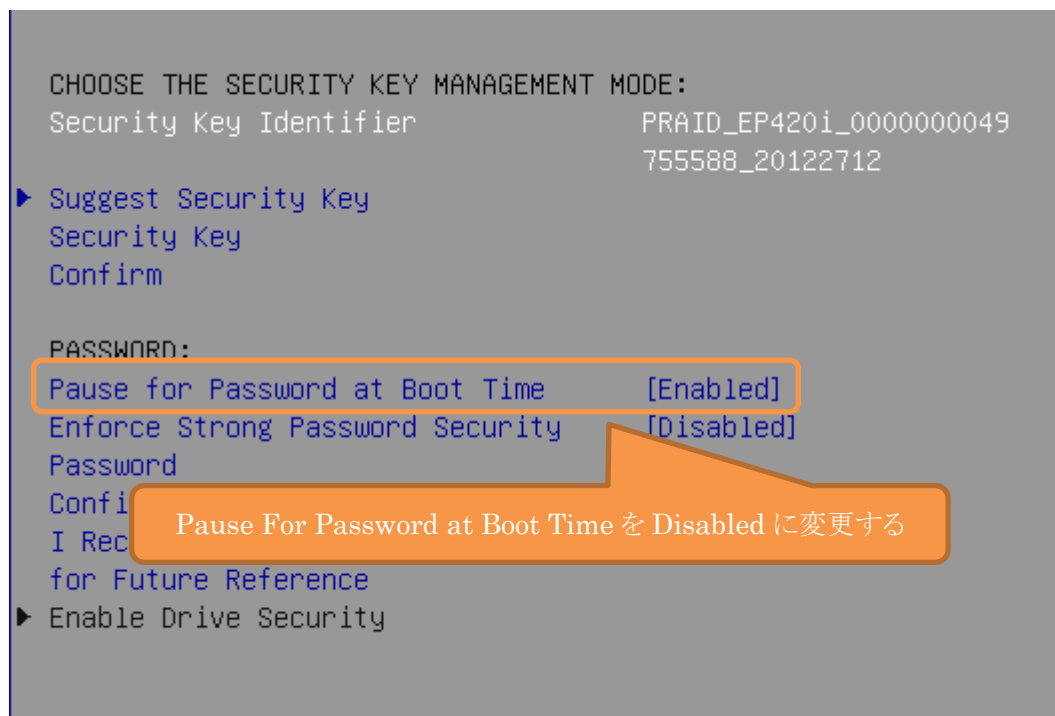


図 5: Disable Boot Password (HII Configuration Utility)

◆ **ServerView RAID Manager の場合**

セキュリティ設定を有効にする際、ブートパスワードを使用しない設定でお使いください。

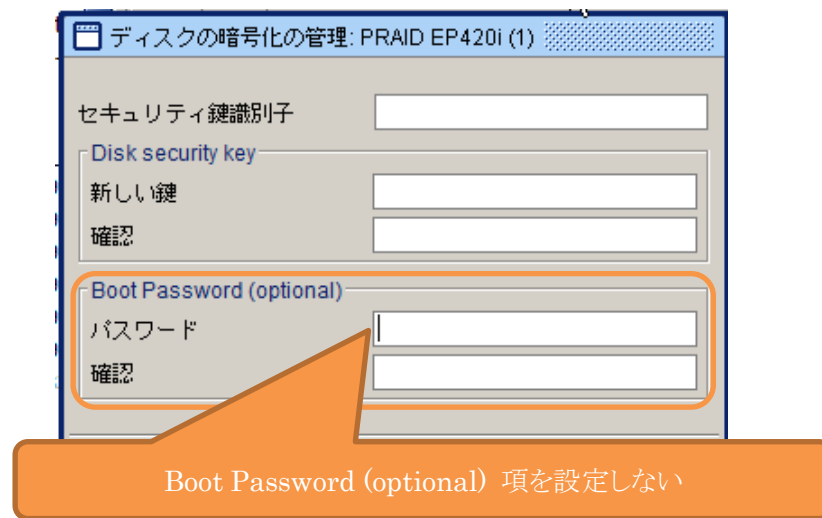


図 6: Disable Boot Password (ServerView RAID Manager)

万が一、UEFIモードにてブートパスワードを設定し、システムが起動できなくなった場合、下記手順にて復旧してください。復旧にはセキュリティ設定を有効にする際設定したセキュリティキーが必要になります。

1. システムの電源を切断します
2. ブートパスワードを設定したアレイカードを取り外します
3. システムの電源を投入します
4. 本体BIOSの設定をBIOSモードに変更します
 - I. BIOS POSTにて[F2]キーを押し、本体BIOSを起動します
 - II. [Advanced]→[CSM Configuration]を選択します
 - III. Launch CSMが[Disabled]設定だった場合は、[Enabled]に設定します

Launch Storage OpROM policyが[UEFI only]設定だった場合は、[Legacy Only]に設定します

※ 本設定は、後で復元するために記録してください

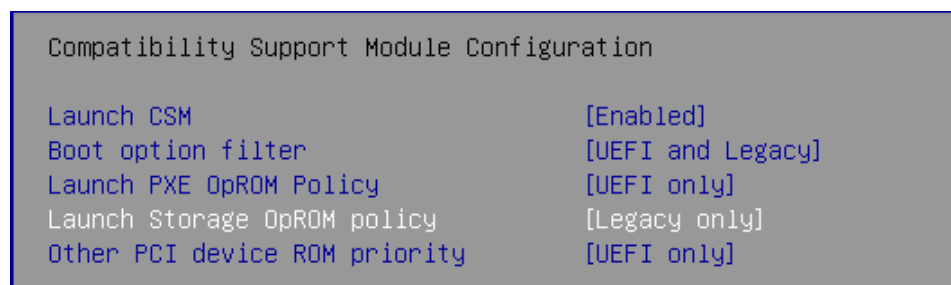


図 7: Change CSM Settings

- IV. [Save & Exit]より[Save Changeds and Exit]を選択します
5. システムの電源を切断します

6. アレイカードを再度取り付けます
7. システムの電源を投入します
8. アレイコントローラのPOST画面にて、設定済のブートパスワードを入力します

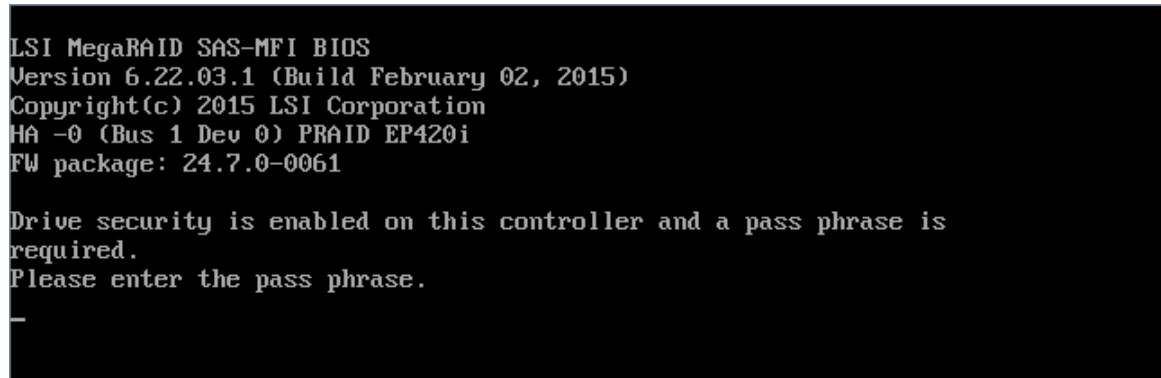


図 8: Enter Boot Password (BIOS mode)

9. Ctrl-R Utilityを起動します
10. ブートパスワードを使用しない構成にて再設定します
 - I. [VD Mgmt]を選択し、[F2]キーを押します
 - II. Drive Security→Change security settingsを選択し、[Enter]キーを押します
 - III. 下図を参照して、security key欄およびConfirm欄に、設定済のセキュリティキーを入力します

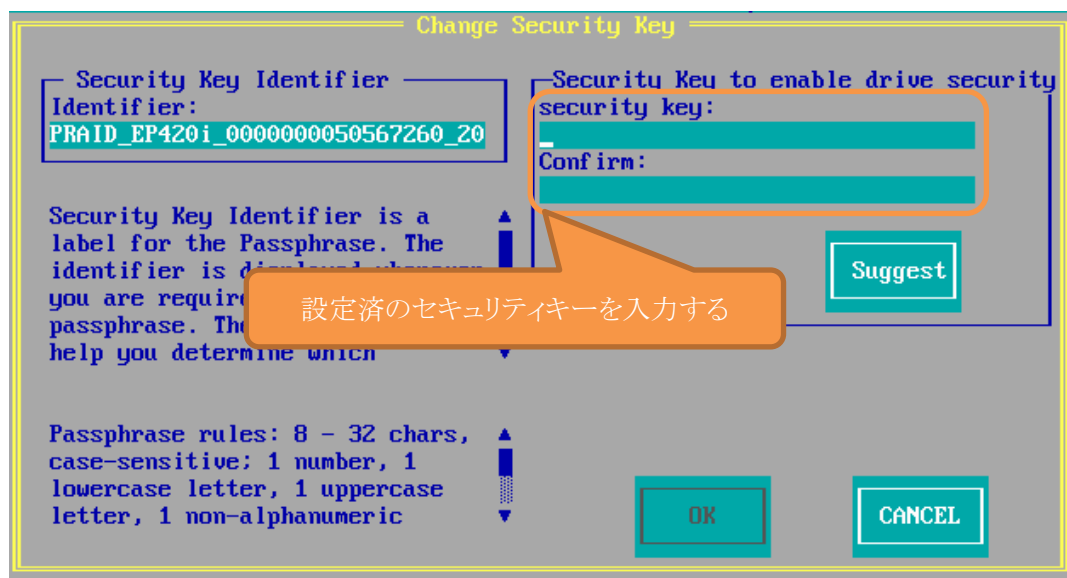


図 9: Change Security Key(Ctrl-R Utility FW: 24.7.0-0061)

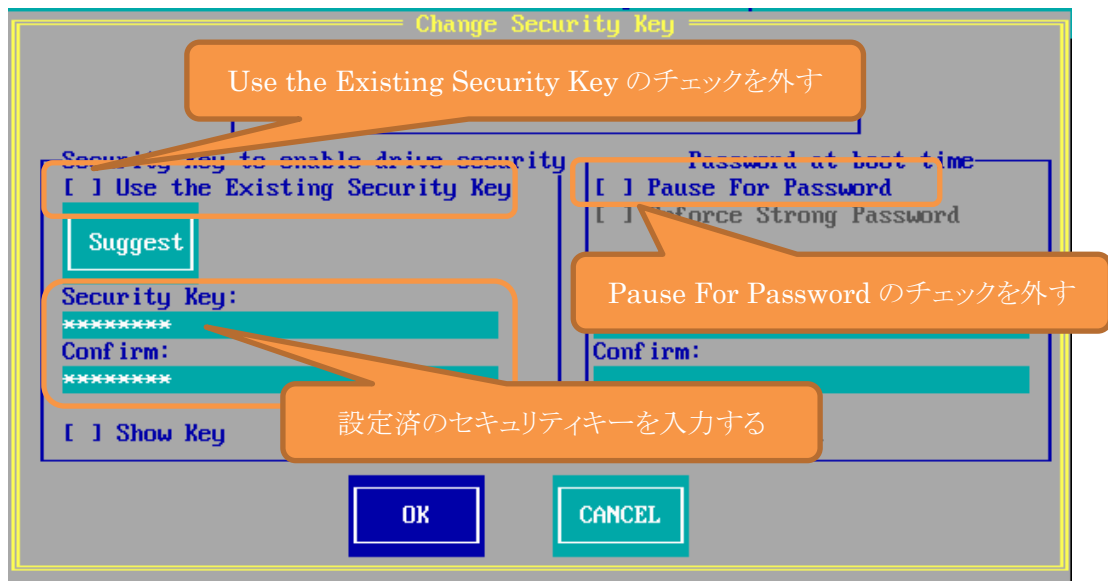


図 10 Change Security Key(Ctrl-R Utility FW: 24.16.0-0097)

- ※ 設定済のものと同一のセキュリティキーを入力してください。異なるセキュリティキーを入力する場合は、必ず入力したセキュリティキーを記録してください。セキュリティキーは、アレイカードの交換時および、セキュリティ設定の変更時に必ず必要となります
- ※ セキュリティキー識別子(Security Key Identifier)は、設定済のものが自動的に入力されます
- ※ [Show Key]にチェックを入れると、入力中のセキュリティキーを画面上に表示することができます
- ※ ファームウェア版数24.7.0-0061のCtrl-R Utilityにはセキュリティキー設定機能がない為、本手順にてセキュリティキーを使用しない構成で設定を上書きすることができます

IV. [OK]を選択し、[Enter]キーを押します

- V. 確認画面にて、設定済のセキュリティキーを再度入力します

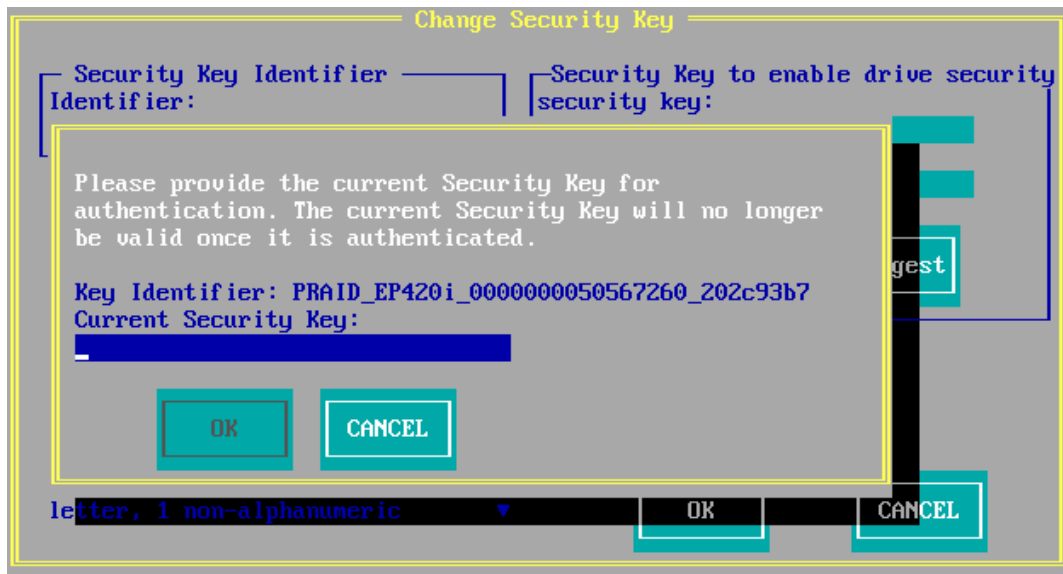


図 11: Enter Current Security key

- VI. [OK]を選択し、[Enter]キーを押します
11. 本体BIOSにてuEFIモードに変更します
- I. BIOS POSTにて[F2]キーを押し、本体BIOSを起動します
 - II. [Advanced]→[CSM Configuration]を選択します
 - III. Launch Storage OpROM policyが[UEFI only]に復元するか、またはLaunch CSMを[Disabled]に復元します
※ 手順4. で記録した設定を復元してください
 - IV. [Save & Exit]より[Save Changeds and Exit]を選択します

2.3 Ctrl-R Utility の表示が一部異なります

ファームウェア版数24.7.0-0061において、ユーザーズガイドの記載と、下記の相違点があります。

- ロジカルドライブ作成画面のレイアウトが一部異なります。機能上の相違はありません。

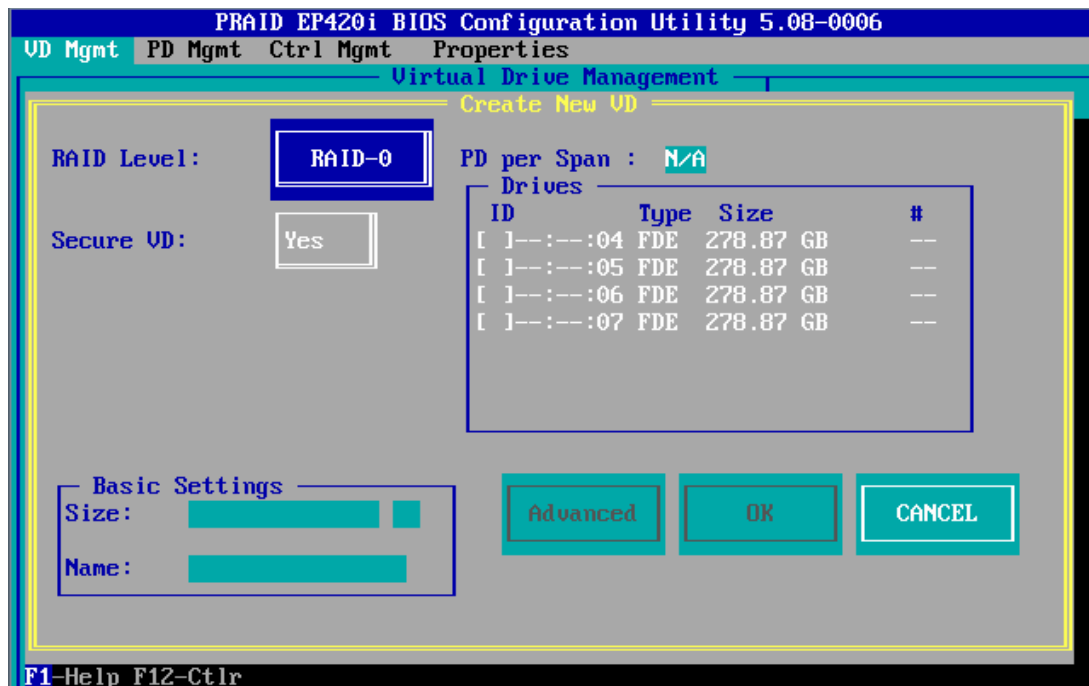


図 12 Create VD (24.7.0-0061)

- SafeStore機能によるセキュリティ設定およびセキュリティ設定変更画面の機能およびレイアウトが一部異なります。

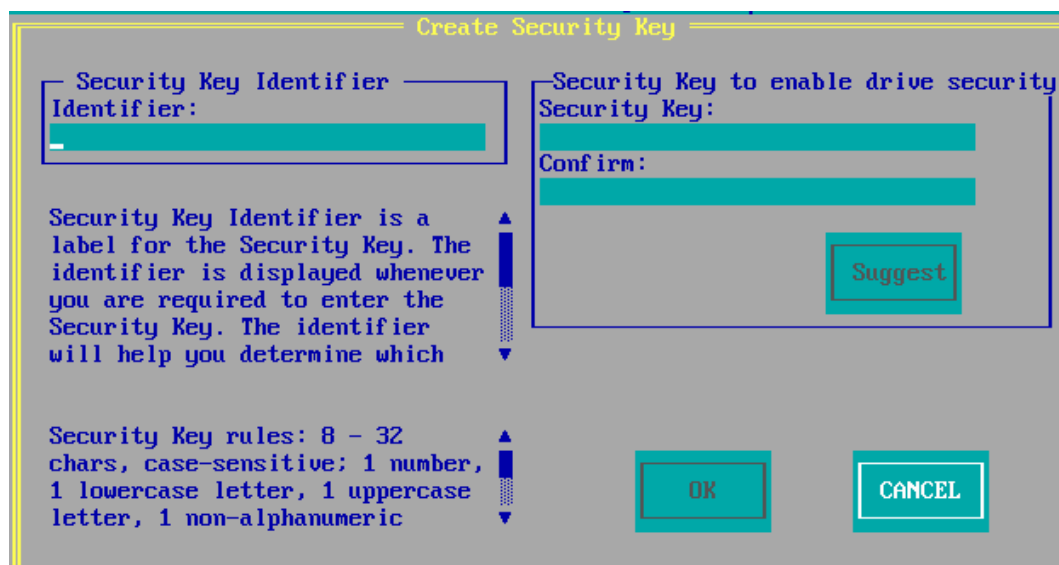


図 13 Enable Security (24.7.0-0061)