

Kingston の暗号化 SSD

eDrive で BitLocker を有効/無効にしてハードウェア 暗号化を利用



<u> 製品説明</u>

本書はお手元のキングストン製 SSD でハードウェア暗号化を活用する場合に、Microsoft 社の BitLocker eDrive 機能を有効/無効化する方法について説明します。 この手順は、TCG OPAL 2.0 およ び IEEE1667 の機能に対応するキングストン製 SSD が対象となります。 お手元のキングストン製 SSD が TCG OPAL 2.0 および IEEE1667 に未対応の場合、このプロセスは機能しません。 ご不明な 点があれば、キングストンの技術サポート (@www.kingston.com/support) にお問い合わせください。

本書は以降、Microsoft eDrive 内蔵の BitLocker を 'eDrive と呼びます。 以下に説明する各手順は、 Windows のバージョンや更新プログラムによって異なる場合があります。

<u>システム要件</u>

-TCG Opal 2.0 および IEEE1667 セキュリティ機能セットを利用するキングストン製 SSD -Kingston SSD Manager ソフトウェア <u>https://www.kingston.com/ssdmanager</u> -TCG Opal 2.0 および IEEE1667 セキュリティ機能をサポートするシステムハードウェアおよび BIOS

<u>OS/BIOS の要件</u>

-Windows 8 および 8.1 (Pro/Enterprise) -Windows 10 (Pro、Enterprise、Education) -Windows Server 2012

注: Windows 8、10、および/または Server 2012 で正常に機能させるには、暗号化されたすべての ソリッドステートドライブ (SSD) を非 RAID コントローラーに接続しなければなりません。

Windows 8、10、または Windows Server 2012 で暗号化ソリッドステートドライブをデータドライブ として使用する場合:

- ドライブは非初期化状態でなければなりません。
- セキュリティは無効にされていなければなりません。

暗号化 SSD が**起動ドライブ**として使われている場合:

- ドライブは非初期化状態でなければなりません。
- セキュリティは無効にされていなければなりません。
- コンピュータは UEFI 2.3.1 ベースで、EFI_STORAGE_SECURITY_COMMAND_PROTOCOL が定義 済みでなければなりません。(このプロトコルは、EFI ブートサービス環境で実行されている各プログ ラムが、セキュリティプロトコルコマンドをドライブに送信可能にするために使用されます。)
- コンピュータは、UEFI で無効にした互換性サポートモジュール (CSM) を備えなければなりません。
- コンピュータは常に UEFI からネイティブで起動しなければなりません。

詳細については、以下の Microsoft 社の記事をご覧ください : <u>https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831627(v=ws.11)</u>



ブート SSD で Microsoft eDrive を有効にする場合

BIOS 設定

- ユーザーシステムの BIOS が UEFI 2.3.1 ベースで、定義済みの EFI_STORAGE_SECURITY_COMMAND_PROTOCOL を持つことを確認する場合は、システム メーカーのドキュメントをご覧ください。
- 2. BIOS 設定に入り、Compatibility Support Module (CSM) を無効にしてください。



ドライブの準備

- Kingston SSD Manager (KSM) をまだダウンロードしていない場合は、直ちにダウンロードして ください。<u>https://www.kingston.com/ssdmanager</u>
- 2. KSM ソフトウェアまたは他の業界標準の方法を用いて、ターゲット SSD を消去します。
- ターゲット SSD をセカンダリーディスクとしてマウントし、IEEE 1667 のステータスを確認し ます。ドライブは、無効モードでなければなりません。



4. IEEE1667 ボタンを選択し、機能を有効にします。機能が正常に切り替えられるか確認します。



OS (オペレーティングシステム) のインストール

注: ターゲット SSD に、OS のクローンを作成しないでください。 ターゲット SSD に OS を クローンすると、eDrive を使用したハードウェア暗号化を有効にできなくなります。 eDrive で ハードウェア暗号化を利用するには、ターゲット SSD に新しい OS インストールを展開しなけ ればなりません。

- 1. サポートされている OS を、ターゲット SSD にインストールします。
- OS のインストール後、Kingston SSD Manager (KSM) をインストールして実行し、アプリケー ションの [セキュリティ] タブに次のメッセージが表示されることを確認します。
 「IEEE 1667 is enabled an may not be changed because TCG Locking is enabled.」

(IEEE 1667 が有効になっており、TCG ロックが有効になっているため、変更できません。)





3. Windows キーを使用して「**Manage BitLocker**」(BitLocker の管理) を検索し、アプリケー ションを実行します。



4. エクスプローラのウィンドウ内で、「**Turn on BitLocker**」(BitLocker を有効にする)を選択し ます。

RitLocker Drive Encryption			-		×
	n and Security BitLocker Drive Encryption	~ D	Search Control Panel		۶
Control Panel Home	BitLocker Drive Encryption				
	Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.				
	Operating system drive				
	C: BitLocker off		0		
	-	😵 Turn an BitLo	cker		
	Fixed data drives				
	Removable data drives - BitLocker	To Go			
	Insert a removable USB flash drive to use Bit	Locker To Go.			

 プロンプトメッセージに従って続行し、ターゲット SSD を構成します。プロンプトが示されたら、 「Start encrypting」(暗号化を開始する)を選択します。 デフォルトで、「Run BitLocker system check」(BitLocker のシステムチェックを実行する)が選択されています。 この設定を有効にして 続行することが推奨されます。 無効にした場合は、ハードウェア暗号化の際にシステムの再起動が 必要かどうかを確認できます。





注:「Choose how much of your drive to encrypt」(暗号化するドライブの数を選択してくだ さい)という画面が表示されたら、多くの場合、ターゲット SSD がハードウェアの暗号化を有効 にせず、代わりにソフトウェア暗号化を使うことを意味します。



6. 必要な場合は、システムを再ブートし、Manage BitLocker を再起動して、ターゲット SSD の暗 号化の状態を確認してください。



 また、cmd.exe を開いて manage-bde -status を入力すれば、ターゲット SSD の暗号化の状態を チェックできます。



Windows 10 (バージョン 1903+)で、Microsoft dDrive を有効にする場合

Microsoft 社は Windows 10 バージョン 1903 のリリースに際し、eDrive 暗号化に関する Windows 10 のデフォルト動作を変更しました。このビルドおよびそれ以降で eDrive を有効にするには、gpedit を 実行して、ハードウェアの暗号化を有効にする必要があります。

注: ターゲット SSD に、OS のクローンを作成しないでください。 ターゲット SSD に OS をクロ ーンすると、eDrive を使用したハードウェア暗号化を有効にできなくなります。 eDrive でハードウ ェア暗号化を利用するには、ターゲット SSD に新しく OS をインストールしなければなりません。

1. 対応 OS をターゲット SSD にインストールします。

OS のインストール後、Kingston SSD Manager(KSM)をインストールして実行し、アプリケーションの [セキュリティ] (Security) タブに次のメッセージが表示されることを確認します。

「IEEE 1667 is enabled an may not be changed because TCG Locking is enabled.」(IEEE 1667 が有効になっており、TCG ロックが有効になっているため、変更できません。)



- 3. gpedit.msc を実行して、暗号化の設定を変更します。
 - a. Administrative Templates (管理用テンプレート)> Windows Components (Windows のコンポーネント)> BitLocker Drive Encryption (BitLocker ドライブの暗号化)> Operating System Drives (OS ドライブ)を順次選択します
 - b. 次に、「Configure use of hardware-based encryption for operating systems」
 (OS のハードウェアベース暗号化の利用設定)を選択します。
 - c. 機能を「Enable」(有効)にし、次に設定内容に「Apply」(適用) します。



注: OS のドライブ以外のドライブで eDrive を有効にするには、以下を順番に選択し、同じ設定 内容を適用できます。ナビゲーション: Administrative Templates (管理用テンプレート) > Windows Components (Windows コンポーネント) > BitLocker Drive Encryption (BitLocker ドライブ暗号化) > Fixed Data Drives (固定データドライブ) > Configure use of hardwarebased encryption for fixed data drives (固定データドライブのハードウェアベース暗号化の 利用設定) (Enable、次に Apply)

4. Windows キーを使用して 「**Manage BitLocker** 」(BitLocker 管理)を検索し、次にアプリケー ションを実行します。



5. エクスプローラ ウィンドウ内で、「**Turn on BitLocker**」(BitLocker をオンにする)を選択



7

 プロンプトメッセージに従って続行し、ターゲット SSD を構成します。プロンプトが示されたら、 「Start encrypting」(暗号化を開始する)を選択します。 デフォルトで、「Run BitLocker system check」(BitLocker システムチェックを実行)が選択されています。 この設定を有効に して続行するように推奨します。しかしこのチェックを外すと、システムの再起動を必要とせずに、 ハードウェア暗号化が有効かどうかを確認できます。

t	ReitLocker Drive Encryption (C)	×
	Are you ready to encrypt this drive?	
	Encryption might take a while depending on the size of the drive.	
	Run BitLocker system check	
	The system check ensures that BitLocker can read the recovery and encryption keys correctly before encrypting the drive.	
	BitLocker will restart your computer before encrypting.	
Note: This check might take a while, but is recommended to ensure that your selected works without requiring the recovery key.		
	Start encrypting Cancel	

注:「Choose how much of your drive to encrypt」(暗号化するドライブの数を選択してくだ さい)という画面が表示されたら、多くの場合、ターゲット SSD がハードウェアの暗号化を有効に せず、代わりにソフトウェア暗号化を使うことを意味します。

	×		
÷	Re BitLocker Drive Encryption (C:)		
	Choose how much of your drive to encrypt		
1	If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.		
	If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected-even data that you deleted but that might still contain retrievable info.		
	Encrypt used disk space only (faster and best for new PCs and drives)		
	O Encrypt entire drive (slower but best for PCs and drives already in use)		
	<u>N</u> ext Cancel		

7. 必要な場合は、システムを再ブートし、Manage BitLocker を再起動して、ターゲット SSD の 暗号化の状態を確認してください。



8. また、cmd.exe を開いて manage-bde -status をキー入力し、ターゲット SSD の暗号化の状態を チェックできます。

🔤 Administrator: Command Prompt	_	\times
Microsoft Windows [Version 10.0.17763.253] (c) 2018 Microsoft Corporation. All rights reserved.		ſ
C:\Windows\system32>manage-bde -status BitLocker Drive Encryption: Configuration Tool version 10.0.17763 Copyright (C) 2013 Microsoft Corporation. All rights reserved.		
Disk volumes that can be protected with Bitlocker Drive Encryption: Volume C: [] [OS Volume]		
Size: 1862.42 GB BitLocker Version: 2.0 Conversion Status: Fully Encrypted Percentage Encrypted: 180.8% Encryption Method: Hardware Encryption - 1.3.111.2.1619.0.1.2 Protection Status: Protection On Lock Status: Unlocked Identification Field: Unknown Kay Protectors: TM Numerical Password		
C:\Windows\system32>		



Microsoft eDrive のサポートを無効にする場合

ターゲットの SSD を消去し、ドライブから BitLocker eDrive のサポートを削除するには、以下の 各手順に従ってください。

注:このプロセスによりターゲット SSD がリセットされます。また、ドライブに存在するすべての データが失われます。

1. ターゲット SSD の PSID 値を、書き留めてください。この値はラベルに印刷されています。



2. ターゲット SSD をセカンダリドライブとしてマウントし、Kingston SSD Manager (KSM) を実行 します。

 Security (セキュリティ)タブを選択し、ステップ1で取得した 32 ビットの PSID 値を入力して TCG Revert を実行します。完了すると、「TCG Revert completed successfully」(TCG Revert が完了しました)のメッセージが表示されます。 このメッセージが表示されない場合は、 PSID 値を再入力して、TCG Revert を再試行してください。



ドライブが正常に復帰すると、IEEE1667 のサポートを無効にするオプションが表示されます。
 IEEE1667 Disable (IEEE1667 を無効にする)を選択し、「IEEE1667 Support Toggle completed successfully」(IEEE1667 のサポートがトグルされました)のメッセージが表示されるまで待ちます。



5. IEEE1667 のサポートが無効になっているか確認します。

Ringston	Firmware Health Security Events
Physical Drive 0: KINGSTON SKC400537A1024G Serial: 500268725C014945 Firmware: SAFM00.W Web Firmware Content Not Accessible	Vendor/Model: KINGSTON SKC2000M82000G Serial Number: 50026B728221E27C TCG OPAL: TCG OPAL Version 2.0 is supported TCG OPAL is disabled
Physical Drive 1: KINGSTON SKC2000M82000G Serial: 500268728221E27C Firmware: SZ681100 Web Firmware Content Not Accessible	TCG Revert TCG Not Enabled, Revert Disabled IEEE 1667: IEEE 1667 is disabled IEEE 1667 Enable IEEE 1667 Support Toggle completed successfully!
Partitioning 1863.0G Unknown → Failures: None → Warnings: None → Overall: Healt	SSD Health SSD Wear Indicator 91% SSD Spare Blocks thy 100%

6. これでターゲット SSD は再使用の準備ができました。

