

用語解説 – 消去コマンドの活用

消去コマンドは主にSSDの消去向けとして用いられています。

HDDのデータ消去では「1回の上書き」(Overwrite)が一般的であり、全ての記録領域に存在するデータを抹消する方法として充足と言われています。

一方で、SSDはHDDと記録方法が異なるため、1回の上書きでは不完全とされています。それは、SSDには以下のような特徴があるためです。

- ▶ データの記録および書き換えは、セクタよりも大きな「ブロック」の単位で行われる
- ▶ 記録される「フラッシュメモリ」には書き換え寿命がある

HDD同様の処理で記録しようとすると書き換えされる記録領域に偏りが発生してしまい寿命(使用できる期間)が短くなってしまうため、使用していない記録域を有効活用し万遍なく(平滑化)使用することで寿命を延ばす「ウェアレベリング」処理が、SSD内(基板上)でフラッシュメモリの処理を統括している「メモリコントローラ」により逐次、自動で行われています。

また、寿命に達した(または不良の発生している)記録域と正常な記録域を差し替えられるよう、メモリコントローラでしかアクセスできない余剰領域を使用する「オーバー・プロビジョニング」機能があり、余剰領域はアドレス外となっているためPCなどの端末からはアクセスできません。

これらの特徴から、SSDは「1回の上書き」では全ての領域が消去できず、データが残存してしまいます。

そこで、全てのデータを消去するために用いるのが、メモリコントローラにより処理され、アドレス外のデータも消去対象となる「消去コマンド」を使用する方法です。



消去コマンドには複数の種類があり、一部はアドレス外が対象にならない種類もございますのでご注意ください。具体的な違いや特長に関しては次のページに記載していますのでご覧ください。

もし消去コマンドに非対応のSSDであった場合は、複数回かつランダム値を含む上書きを行ってウェアレベリングの処理を発生させることで余剰領域内のデータも書き換えされる「DoD 5220.22-m」等の方式を代用するのが一般的です。ただし、複数回の上書き処理は容量に応じた長時間の処理となります。

消去コマンドを使用するメリットのひとつに、SSDではメモリコントローラの記録域一括処理により短時間(大抵は1分以内)に消去が完了することがあります。作業時間の大幅短縮にもつながりますので、消去コマンドの使用は大きなアドバンテージをもたらします。

一方、注意しなくてはならないのはHDDでの消去コマンド使用です。HDDはプラッタ内の記録セクタを総当たりでシークしながら書き換える必要があり、どの消去コマンドを使用しても必ずOverwrite(全領域上書き)となり、容量に応じた長時間の処理が必要となります。

消去コマンドはSSD内で消去処理が行われることによる利点がありますが、処理中は装置からの処理を受け付けなくなってしまう、中止できなくなります。これは「ロック状態」と呼ばれます。

ロック状態になると電源を切断して入れ直しても解除されません。さらには消去だけでなく記録域へのアクセスの一切ができなくなり、実質的にSSDが使用できなくなりますので、長時間の処理が中止できなくなっても良い状況かどうかを確認してから実行するようにしてください。

【NIST SP 800-88】

「アメリカ国立標準技術研究所National Institute of Standards and Technology, NIST」が発行しているガイドラインのうち、SP(Special Publication)の800シリーズにおいて、記録媒体のサニタイズ(消去や除去)に関する内容がまとめられたのが「800-88」であり、現在は2014年の改訂にて示された方式がデータ消去業界の標準となっています。

1990年代半ばに発行された「DoD5220.22-M」や「NSA 130-1」で定義されていた「3回の上書き」方式ではなく、高密度化したHDD(15GB以上の物理容量)は「1回の上書き」で良いと示す一方で、SSDについては上記特性により、Enhanced Secure EraseコマンドやSanitize Block Eraseコマンド、またはCryptographic Eraseコマンドを使用するよう定義しています。

【Clear(消去)とPurge(除去)の違い】

Clear(消去)は一般的な復元方法では復元が困難だが、研究所レベルでは復元可能とされる方式です。

Purge(除去)は一般的な復元方法はもちろん、研究所レベルでも復元が困難とされる方式です。

消去するSSDに記録されたデータの漏えいリスクの高さにもよりますが、可能であればPurge(除去)に該当する方式での消去を実施するのが望ましく、情報漏えい対策の消去として推奨されています。

【Secure EraseとEnhanced Secure Eraseの違い】

共にATA規格(SATAとIDE)に実装される消去コマンドで、SAS(SCSI)のSSDでは使用できません。

Secure Eraseが古くに規格化されたため、対応するSSDも多いのですが、SSDでウェアレベリングによりアクセス可能領域外となったデータは対象とならず、SSDのデータ抹消としては不十分です。

Enhanced Secure EraseはSecure Eraseを機能拡張した規格で、アクセス可能領域外となったデータも消去の対象となるため、SSDのデータ抹消として最適です。

また、HDDの代替セクタの消去用としてもEnhanced Secure Eraseは適しています。

【Sanitize Block EraseとEnhanced Secure Eraseの違い】

Enhanced Secure EraseがATA規格のみに対応するのに対し、Sanitize Block EraseはSAS(SCSI)規格で作られたコマンドのため、SASのSSDに使用可能です。いずれもアクセス可能領域外となったデータも消去の対象となる消去コマンドです。

ただし、Sanitizeコマンドは近年に成立した消去コマンドのため、近年に発売されたSSDでなければ対応しておらず、古いモデルのSSDでは対応しない場合があります。

SASに続きATAにも採用されたため、新しいモデルのSATA接続SSDでも使用できる場合があります。

【Sanitize Block EraseとSanitize Overwriteの違い】

いずれもSAS(SCSI)規格向けの消去コマンドですが、Block EraseはSSD用、OverwriteはHDD用として設計されているため、SSDを消去する場合にはBlock Eraseを選び、HDDを消去する場合にはOverwriteを選ぶようにしてください。

消去コマンド名	対応規格	レベル	優先度	説明
Sanitize Block Erase	SATA / SAS / NVMe	Purge(除去)	高	主にSSDに採用されている。代替セクタ領域も消去でき、短時間で行える。
Sanitize Overwrite	SATA / SAS / NVMe	Purge(除去)	中	主にHDDに採用されている。代替セクタ領域も消去できるが、全記録領域を上書き消去するため長時間を要する。
Enhanced Secure Erase	SATA	Purge(除去)	高	SATAのSSD用として一般的。主にSSDに採用されている。代替セクタ領域も消去でき、短時間で行える。
Secure Erase	SATA	Clear(消去)	低	上記と異なり、代替セクタは消去できない。Enhanced Secure Eraseが対応しないSSDの代用消去コマンドとして有用。
Format NVM	NVMe	Clear(消去)	低	NVMe版のSecure Erase。Sanitize Block Eraseが対応しないSSDの代用消去コマンドとして有用。