

はじめに

本 APPENDIX は、今までの PC に搭載されている記憶媒体のデータ消去を対象に、消去技術認証基準委員会が作成した「データ消去技術ガイドライン」に、複数の電子記憶媒体を搭載した、RAID・サーバと称される機器を対象とするための注意点などの追補を行うためのものです。

本 APPENDIX で用いる「抹消」とは、データ消去技術ガイドライン第 5 章と同様に、情報を消し去り、何もない状態にする「消去」だけではなく、暗号化等で内容を判別・復旧することが不可能にする行為全般を指します。

### 1. NIST SP800-88 上の取り扱い

ADEC が基準として取り扱っている NIST SP800-88Rev.1 では、媒体の分類として、ドライブや SSD の接続インターフェイスによる区分は存在しますが、搭載する側のシステム（機器）による区分（パーソナルコンピュータ/サーバ等の種類）での分類は存在しません。そのために実際に用いられるデータの抹消手法について解説は、データ消去技術ガイドライン第 2.2.1 版、

第 5 章 記憶媒体のデータ抹消（NIST SP800-88Rev.1）を参照してください。

### 2. RAID・サーバに関する注意点

RAID システムに於いては、システムの耐障害性（RAID5 の場合 1 台、RAID 6 の場合 2 台）を超える媒体のデータの抹消を行えば機器全体のデータ抹消が完了しセキュリティーが保たれるとの考えもあるようですが、それは重大な誤解であり、システムを構成する全ての電子記憶媒体のデータの抹消を行う必要が有ることの理解を得ることが必要です。

2019 年 7 月

ADEC（データ適正消去実行証明協議会）

消去技術認証基準委員会

### ※参考情報

【RAID (Redundant Arrays of Independent Disks) とは】

引用元：<https://www.a-d.co.jp/datarecovery/knowledgecenter/raid/001.html>

RAID は、1988 年にカリフォルニア州立大学バークレー校の論文によって提唱された、Redundant Arrays of Independent Disks (独立した複数のディスクの冗長性配列) を省略した呼び方であって、物理的な複数のドライブを組み合わせて冗長性を持ったディスクアレイを構成する技術を指し、RAID 0 は冗長性を持たないことを理由に当初はその中に含まれていなかったが、冗長性の点を除き構成上の差が少ないため、冗長性が存在しないことを現わす“0”の RAID として呼称されている。RAID はこのように歴史的には新しい技術であるが、外部記憶装置の冗長性の確保や、高速化などの性能改善を目的として、広く使われている技術である。

#### 1. RAID の代表的な種類

**1) RAID 0 :** “ストライピング”とも呼ばれる。ドライブの高速化を目的として、データを複数に区切って、区切られた各々のデータを、複数の別々のドライブに分散して書き込むことによって、書き込みに要する時間を短縮する方法であり、冗長性は存在せず、全体を構成している複数のドライブ中の 1 台でも故障すると、全体の故障となってしまう (冗長性を持たない) ため、データをドライブの故障から守ることは出来ない。

**2) RAID 1 :** “ミラーリング”とも呼ばれる。“ミラー (鏡)”の呼び方が示すように、2 台のドライブに、同時に同一のデータを書き込み (複製を持つ)、1 台のドライブが故障しても、もう一方のドライブの動作によってシステムダウンを予防することが出来る。

**3) RAID 0 1 / 1 0 :** “0 1”も“1 0”も、上記の“ストライピング”と“ミラーリング”を二重構造に組み合わせて“RAID 0”の高速性と、“RAID 1”のデータ保護の双方の特徴を得ることを目的とした方法。下層の方法を先頭に表記するので、“0 1”は、“RAID 0”の構成を 2 組用意して、複製することを意味するので、双方の“RAID 0”の構成が必ずしも同一の必要性は存在しない (一方が 2 台構成、もう一方が 3 台構成でも理論上は構成することが出来る)。“1 0”は、“RAID 1”を 2 組用意して、ストライピングするので、ストライピングされたデータドライブが 2 台ずつ存在することになり、夫々が同一の構成で同一容量のドライブであることが必要であるが、障害耐性もより強固なものとなる。

**4) RAID 2 / 3 / 4 :** ほとんど使用されていないので、説明を省略する。

興味のある方は、Wiki：<http://ja.wikipedia.org/wiki/RAID> に詳細な説明があるので、参照ください。

**5) RAID 5 :** 現時点において最も多く使われている方法。“RAID 0”のように、データを複数に区切って別々のドライブに書き込むと同時に、元のデータ群から“パリティ (誤り訂

正符号) ”を生成して、データと同じように、順番に別々のドライブに記録する方式で、1 台のドライブが故障しても、データが失われるのを予防することが出来るが、最低構成でも 3 台のドライブが必要であり、全体の記憶容量は、(全構成台数 - 1 台) 分となる。“RAID 5” も他の RAID との複数層構成 (“RAID 5 5” など) を用いることが出来る。障害の無い場合の読み出し速度は“RAID 0”同様に高速化が期待できるが、書き込み時は、“パリティ”の生成時間が必要なため、速度が低下する。

**6) RAID 6 :** “RAID 5”をさらに発展させた方法で、“パリティ”を 2 重に持つことで、2 台のドライブが故障してもデータが失われることを予防することが出来る。2 重化された“パリティ”の生成方法に規則は存在せず、同一の“パリティ”を 2 つ持たせても、全く別の算出方法の“パリティ”でも良い。このため、最低構成でも 4 台のドライブが必要となり、全体の記憶容量は (全構成台数 - 2 台) 分となる。“RAID 6”も、他の“RAID”構成と同様に複数層構成 (“RAID 6 5” など) を用いることは勿論可能である。障害の無い場合の読み出し速度は“RAID 0”同様に高速化が期待できるが、書き込み時は、二重の“パリティ”の生成時間が必要なため、“RAID 5”よりも更に速度が低下する。

### 2. ハードウェア RAID とソフトウェア RAID

“ハードウェア RAID”とは、メイン (マザー) ボードの拡張スロットに RAID 専用の拡張ボード (RAID カード) を増設し、そのボードにドライブを接続することによって構成する方法です。このため OS からは、1 台の論理ドライブとしてしか認識されませんが、“ソフトウェア RAID”は、最近の OS の機能を利用して構成するためコスト的には安価で済ませることが出来る方法で、OS の使用している CPU を使用して論理的に構成するため、当然 CPU の負荷が増大し、通常の処理が足を引っ張られ、低速になる場合もある。

### 3. RAID システムの構成媒体数

RAID の種類	最小構成媒体数	最大耐障害媒体数
0	2	無
1	2	1
0 1 / 1 0	4	2
5	3	1
6	4	2

2019 年 7 月

ADEC (データ適正消去実行証明協議会)

消去技術認証基準委員会