

第一回 調査技術ゼミ

2005年8月17日

『取得前 ~ 保全先HDDのWipeまで』

ネットエージェント株式会社

用語

- Sanitize : 消毒
- Wipe : ワイプ・消去
- Erase : 削除
- Delete : 削除

Wipeの必要な場面

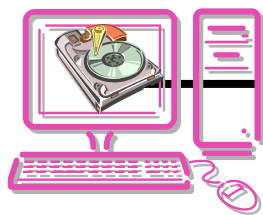
(1)保全前の複製先HDD



ICS / UBIC
WipeMASter

複製先HDD
の消去

- 証拠の保全先を「白紙」にする



調査対象

複製装置

複製先
HDD

物理コピー
dd image

調査・鑑識
EnCase,
FTK,TSK

YEC KING DEMI



Wipeの必要な場面

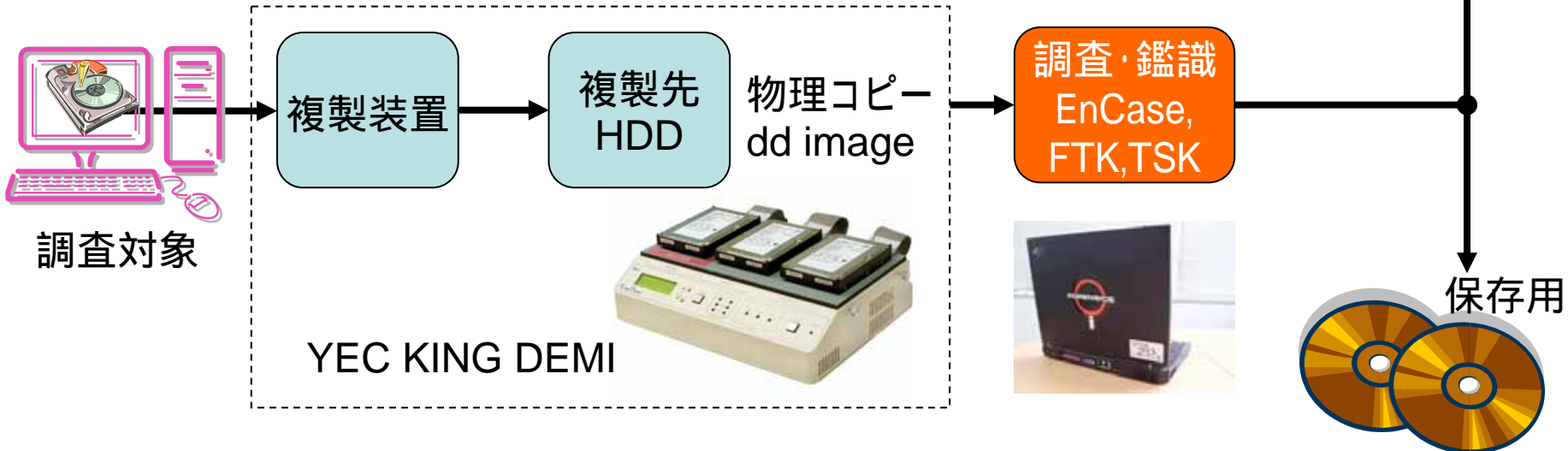
(2)解析後の複製先HDD

- 客先からは
データを持ち帰らない！



ICS / UBIC
WipeMASter

複製先HDD
の消去



ソフト？ ハード？

- **ソフト = 手軽**

- 標準的な dd コマンド、wipe コマンドでも可

- **ハード = 速度・効率**

- WipeMASSterは9台同時消去可能
- シンプルな操作

- **お安いハードもある...「専用」ハードとの違い**

- 強力なログ出力
- 同一性の保証(コンペア・ベリファイ・ハッシュ) = メーカーの保証

WipeMASterを使って

Intelligent Computer Solutions
Smart Solutions for a New Era in Computing



- 米 Intelligent Computer Solution (ICS)社製
 - 複製装置のパイオニア
 - ImageMASterシリーズ
- 日本では株式会社UBICが取り扱い
 - 日本語マニュアル・サポートあり

WipeMASter

操作インターフェース

- 液晶パネルによるGUI操作
- ヘルプ付き！



対応デバイス

- ATA (3.5、2.5インチ)
- Serial ATA
- PCMCIAデバイス (オプション)
- SCSI対応無し
保全先HDDはATAで統一

WipeMASSterの動作

(1)三つのモード

- WipeOut Fast
 - ユーザ定義のパターンを10回まで指定可能
- Random mode
 - WipeOut Fastの最終書き込みにMasterに接続したHDDのデータからランダムに書き込み
- WipeOut DoD
 - 米国国防省準拠規格 (DoD5220-22M)
FF 00 FF 00 FF 00 F6 Read F6

参考：Wipeの種類、基準

- (1)国内

- 「パソコンの廃棄・譲渡時におけるハードディスク上のデータ消去に関するガイドライン」2002年8月 / 社団法人 電子情報技術産業協会 (JEITA)
 - 「基本的にはHDDデータ消去プログラムで1回固定データによる塗潰し消去を行えば十分ですが、2回消去を行えば一般的に完全といえます。ただデータ消去ソフトには各種の軍関連の規格がありますように、データ読出し技術とデータ消去技術が今後とも表裏一体の進歩を繰り返すと思われる。」<http://it.jeita.or.jp/perinfo/committee/pc/HDDdata/>

- (2)海外

- グートマン方式
- DoD仕様

参考：記録方式・磁性体

- 「水平磁気記憶方式」
- 「垂直磁気記録方式」
 - 現在使われている長手記録方式とは逆に、記録密度が高くなるほど残留磁化状態が安定になり、高密度化に適しているという特徴があります
『ハード・ディスク装置の構造と応用』35

浸透した磁気の解析は電子顕微鏡の世界

WipeMASterの動作

(2)不良セクタの扱い

- Prompt
 - プロンプトを表示。消去中止か継続を選択
- ContinueSkip
 - ログを出力し、不良セクタをスキップし処理を継続
- Skip Block
 - 不良セクタの属しているブロック全体をスキップ
- Abort
 - 消去作業を中止
- 「注：不良セクタの処理を飛ばすことにより、データ転送操作（消去）の結果が不完全になることがあります」 WipeMASter マニュアル p.25より

HPA、DCOへの対応

- Host Protected Area ホスト保護領域
- Device Configuration Overlay 装置構成オーバレイ
 - WipeMASterマニュアルより
- 「自動的に検知、解除し消去します」 p. 9
 - 設定により自動検知をオフにすることも可能
 - 消去前にHPAやDCOの情報を確認可能

WipeMASSterの実際

設置・取り扱い

- キャリングケース
 - 専用キャリングケースあり
- 必要なスペース
 - 後方排気、HDD取り回しで50cm四方は必要
- 静電対策
 - マット、グローブ、ストラップ

HDD接続

- 電源を落とした状態で接続
- ジャンパをマスターに設定
- ケーブルの取り回しに注意

電源の確保

- 安定した電源
 - サージ保護機能を推奨
 - 消費電力 200W
- UPSの利用
 - 瞬断を避ける
 - UPSとの連携機能はない

設定

- ほとんどデフォルト(AUTO)で使用可能
 - キャッシュやDMAの使用を設定可能
- DoDモード
 - DoDモードを選択 Run !
- WipeFastモード
 - WipeFastモードを選択 回数を設定 それぞれの回に書き込む値を設定 Run !
 - ランダム値を使用するときはMasterにHDD必要

Run !



- Stopで中止も可能。リジュームは不可。

ログの採集・解析

- PCMCIA経由でフラッシュRAMへ保存
 - 上書きのみ可能
 - 電源を切っても前回分を保持(設定も)
- 3種類のログ
 - MESSAGES.TXT: イベントログ(LCDにも表示)
 - OPINFO.TXT: 実行情報、HPAの有無も
 - SETTINGS.TXT: WipeMASSterの設定情報
- 4つのレベル
 - None、Brief、Detailed、Diagnostic

ログの例 Brief (1)

- HD1台 (1)
- WipeOutFastモード、書き込み1回、値指定 F6
- ログをBriefで実施
- OPINFO.TXT
 - IDE_FillUpDriveInfo - Target7 - NO HPA! HPAStart LBA 0, size 0!
 - Target7: IC35L040AVVN07-0. ID#0. SN# VNP210B2GLY5SB. Capacity: 39267MB, 80418240 sectors. CHS=16383,16,63. Native capacity: 39267MB, 80418240 sectors. Drive supports ATA-5. Drive supports LBA mode.
 - Drive7 multiple mode=16
 - Turning off Drive Mask=0xFFFFFFFF7F
 - Minimum time=120 nsec

 - Fastest assumed speed=PIO 1

 - BenchmarkCopy-Using Multiple Mode, Secs/Block=16
 - Benchmark PASSED at speed=PIO 1, Time=0
 - BenchmarkPIO-Speed set to PIO 1
 - BenchmarkCopy-Using Multiple Mode, Secs/Block=16
 - Benchmark PASSED at speed=UDMA 4, StrobeDelay=0, Time=8910
- MESSAGES.TXT
 - Turning on drives
 - Identifying drives
 - Target7: IC35L040AVVN07-0. ID#0. SN# VNP210B2GLY5SB. Capacity: 39267MB, 80418240 sectors. CHS=16383,16,63. Native capacity: 39267MB, 80418240 sectors. Drive supports ATA-5. Drive supports LBA mode.
 - Benchmarking
 - Benchmarking PIO 1...
 - Benchmarking UDMA 4...
 - Selected speed UDMA(4)
 - Total load 39267MB.
 - Wiping out drives
 - Iteration #1/1, Pattern=0xF6
 - Retrying WipePatternDrive...
 - Wiped out 39267MB in 18min 40sec.
 - Average Speed 2103MB/min
 - Disk wipeout finished successfully.
 - Master FAILED
 - Target1 FAILED
 - Target2 FAILED
 - Target3 FAILED
 - Target4 FAILED
 - Target5 FAILED
 - Target6 FAILED
 - Target8 FAILED
 - There were 1 retries
 - All drives are finished and powered off.

ログの例 Brief (2)

- SETTING.TXT
 - Image MASter WipeMASter
 - Software version 5.11.1.6 - Jul 8 2005
14:32:52
 - Firmware Version 4.1
 - Serial #: 87170
 - Copy mode: Wipeout, Nlter=1, Pattern=0xF6
 - Safe mode: Off
 - Bad sector: Prompt
 - Disable cache: No
 - Clear cache: No
 - Benchmark Scheme: Default
 - Certify Mode: Disabled
 - Write Verify: Ignored
 - Log: Brief
 - State machine speed: 1
 - Block size: 16
 - Wiped out 39267MB in 18min 40sec.
 - Average Speed 2103MB/min.
 - (右に続く)
- Disk wipeout finished successfully.
- Installed options:
 - IQCOPY
 - DATABASE
 - WIPEOUT
 - HPA
 - DCO
 - Database format: Brief
 - Database save: Off
 - Command-line switch status:
 - autoRun (-B): Off
 - burninMode (-DEB): Off
 - PhantomOverrideMode (-PHANTOM): Off
 - addPartitions (-P): Off
 - limit8Gig (-8GB): Off
 - SamsungOfficialMode (-SAMSUNG): Off
 - CompaqMode (-COMPAQMODE): Off
 - CompaqOfficialMode (-COMPAQ): Off
 - ManualVerify (-CACHE): Off
 - WriteCompaqUIABit (-C): Off
 - GatewayOfficialMode (-GATEWAY): Off
 - FirstwareOfficialMode (-FIRSTWARE): Off

ログの例 Diagnostic (1)

- 検証3
 - 容量の異なるHD2台 (1, 3)
 - DoDモード
 - ログをDiagnosticで実施
- OPINFO.TXT
 - IDE_FillUpDriveInfo - Target5 - NO HPA! HPAStart LBA 0, size 0!
 - IDE_FillUpDriveInfo - Target7 - NO HPA! HPAStart LBA 0, size 0!
 - Target5: IBM-DTLA-305040. ID#0. SN# YJEYJ0C5859. Capacity: 39267MB, 80418240 sectors. CHS=16383,16,63. Native capacity: 39267MB, 80418240 sectors. Drive supports ATA-5. Drive supports LBA mode.
 - Target7: IC35L040AVVN07-0. ID#0. SN# VNP210B2GLY5SB. Capacity: 39267MB, 80418240 sectors. CHS=16383,16,63. Native capacity: 39267MB, 80418240 sectors. Drive supports ATA-5. Drive supports LBA mode.
 - Drive5 multiple mode=16
 - Drive7 multiple mode=16
 - Turning off Drive Mask=0xFFFFFFFF5F
 - Minimum time=120 nsec

 - Fastest assumed speed=PIO 1
 - (右に続く)
- BenchmarkCopy-Using Multiple Mode, Secs/Block=16
- Benchmark PASSED at speed=PIO 1, Time=0
- BenchmarkPIO-Speed set to PIO 1
- BenchmarkCopy-Using Multiple Mode, Secs/Block=16
- SeqStatus=0x05, Drive status mask=0x000, CRC16=0x000,
- DMA Req=0x00000, Ack=0x00000, WC=0
- QTFstat=0x00, ASCstat=0x00, PIOstat=0x00, UDMAstat=0x00, SMstat=0x00
- UWIPE: SeqStatus=0x05, DMA Req=0x00000, Ack=0x00000, WC=0
- T5=51, T7=50,
- Benchmark PASSED at speed=UDMA 4, StrobeDelay=0, Time=2695
- IDE_DCOIdentify Entry point
- Revision = 0x0001
- MDMA Sup = 0x0007
- UDMA Sup = 0x003F
- Max LBA hi = 0x00000000, lo = 0x04CB15BF
- Command Set = 0x00FF
- SMART = Supported
- SMART SelfTest = Supported
- SMART ErrorLog = Supported
- Security = Supported
- PowerUp Standby = Supported
- RdWrDMA = Supported
- Auto Acoustic = Supported
- HPA = Supported
- 48-bit = Not-Supported
- Checksum = 0x7200
- Signature = 0xA5
- IDE_DCOIdentify Exit point

ログの例 Diagnostic (2)

- MESSAGES.TXT
 - Turning on drives
 - Identifying drives
 - Target5: IBM-DTLA-305040. ID#0. SN# YJEYJ0C5859. Capacity: 39267MB, 80418240 sectors. CHS=16383,16,63. Native capacity: 39267MB, 80418240 sectors. Drive supports ATA-5. Drive supports LBA mode.
 - Target7: IC35L040AVVN07-0. ID#0. SN# VNP210B2GLY5SB. Capacity: 39267MB, 80418240 sectors. CHS=16383,16,63. Native capacity: 39267MB, 80418240 sectors. Drive supports ATA-5. Drive supports LBA mode.
 - Benchmarking
 - Benchmarking PIO 1...
 - Benchmarking UDMA 4...
 - UWIPE: Target5: LBA=255 NSEC=0 STAT=51 ERR=84,BlockFailed.
 - UWIPE: Target5: ERROR(51,84),BlockFailed.
 - UWIPE: Target7: LBA=255 NSEC=0 STAT=51 ERR=84,BlockFailed.
 - UWIPE: Target7: ERROR(51,84),BlockFailed.
 - All drives are finished and powered off.
 - (右に続く)
 - Selected speed UDMA(4)
 - Total load 274868MB.
 - Wiping out drives
 - Iteration #1/3, Pattern=0xFF
 - Retrying WipePatternDrive...
 - Iteration #1/3, Pattern=0x00
 - Iteration #2/3, Pattern=0xFF
 - Iteration #2/3, Pattern=0x00
 - Iteration #3/3, Pattern=0xFF
 - Iteration #3/3, Pattern=0x00
 - Iteration #4/3, Pattern=0xF6
 - Wiped out 274868MB in 253min 42sec.
 - Average Speed 1083MB/min
 - Disk wipeout finished successfully.
 - Master FAILED
 - Target1 FAILED
 - Target2 FAILED
 - Target3 FAILED
 - Target4 FAILED
 - Target6 FAILED
 - Target8 FAILED
 - There were 1 retries

ログの例 Diagnostic (3)

- SETTING.TXT
 - Image MASter WipeMASter
 - Software version 5.11.1.6 - Jul 8 2005 14:32:52
 - Firmware Version 4.1
 - Serial #: 87170
 - Copy mode: Wipeout, Nlter=3, Pattern=0xF6
 - Safe mode: Off
 - Bad sector: Prompt
 - Disable cache: No
 - Clear cache: No
 - Benchmark Scheme: Default
 - Certify Mode: Disabled
 - Write Verify: Ignored
 - Log: Diagnostic
 - State machine speed: 1
 - Block size: 16
 - Wiped out 274868MB in 253min 42sec.
 - Average Speed 1083MB/min.
 - Disk wipeout finished successfully.
 - (右に続く)
- Installed options:
 - IQCOPY
 - DATABASE
 - WIPEOUT
 - HPA
 - DCO
 - Database format: Brief
 - Database save: Off
 - Command-line switch status:
 - autoRun (-B): Off
 - burninMode (-DEB): Off
 - PhantomOverrideMode (-PHANTOM): Off
 - addPartitions (-P): Off
 - limit8Gig (-8GB): Off
 - SamsungOfficialMode (-SAMSUNG): Off
 - CompaqMode (-COMPAQMODE): Off
 - CompaqOfficialMode (-COMPAQ): Off
 - ManualVerify (-CACHE): Off
 - WriteCompaqUIABit (-C): Off
 - GatewayOfficialMode (-GATEWAY): Off
 - FirstwareOfficialMode (-FIRSTWARE): Off

検証1

- HD1台(1)
- WipeOutFastモード 書き込み1回、値指定 F6
- ログをBriefで実施
- 結果 (MessageLogの一部)
 - Wiped out 39267MB in 18min 40sec.
 - Average Speed 2103MB/min
 - Disk wipeout finished successfully.

検証2

- 容量の近いIHD2台(1、2)
- 書き込み2回、値指定 FF 00
- ログをBriefで実施
- 結果 (MessageLogの一部)
 - Wiped out 78534MB in 74min 17sec.
 - Average Speed 1057MB/min
 - Disk wipeout finished successfully.
- 検証1の約4倍、若干の容量差・個体差でもパフォーマンスに影響？

検証3

- 容量の異なるHD2台 (1、3)
- DoDモード
- ログをDiagnosticで実施
- 結果 (MessageLogの一部)
 - Wiped out 274868MB in 253min 42sec.
 - Average Speed 1083MB/min
 - Disk wipeout finished successfully.
- **なぜ Wiped out 274868GBと出るのが不明**

検証4

- 容量の異なるHD3台 (1、2、3)
- DoDモード
- ログをDiagnosticで実施
- 容量の異なるディスクでの検証
- 結果 (MessageLogの一部)
 - Wiped out 1236902MB in 657min 27sec.
 - Average Speed 1881MB/min
 - Disk wipeout finished successfully.
- 検証5と同様にWiped outの値が？

検証5

- 容量の異なるHD3台 (1、2、3)
- WipeOutFastモード
- ログをDiagnosticで実施
- 書き込み3回、値指定をランダムに
- Master Driveに接続なし
- ディスクをスキャン後、Failedで終了
- 結果 (MessageLogの全部)
 - Turning on drives
 - Identifying drives
 - Disk wipeout failed.
 - There were 1 retries
 - Failed to detect Master drive
- 最初の段階でエラー表示

検証6

- 同じ機種 240G × 2 (IBM HDS722525VLAT80 U100 7200rpm)
- DoDモード
- ログをDiagnosticで実施
- 結果
 - Wiped out 1669327MB in 70862min 46sec.
 - Average Speed 23MB/min
 - Disk wipeout finished successfully.
- やはりWiped outの値が不明。1669327MBは $250 \times 1024 \times 7$ に近似？時間の誤差はDoDモードの時特有か？

検証7

- 検証6と同じ 240G × 2
- WipeOutFastモード F6h 1回
- 結果
 - Iteration #1/1, Pattern=0xF6
 - Retrying WipePatternDrive...
 - Wiped out 238476MB in 97min 5sec.
 - Average Speed 2456MB/min

検証8

- 検証6を繰り返し
- ログの結果同じ
- 作業中の操作パネルには2.6G程度の速度が出
ていた

WipeMASSterのデモ