

第一回 調査技術ゼミ  
2005年8月17日

『 KING DEMI Forensic を利用し  
た物理コピー 』

ネットエージェント株式会社

# KING DEMI –Forensic とは

- コピー、バックアップ、消去、ddイメージの作成が可能なHDDマネージャー
  - 日本製
  - 多彩なHDDインターフェースに対応
  - 簡単操作



# 日本製

- YEC社 は日本の会社

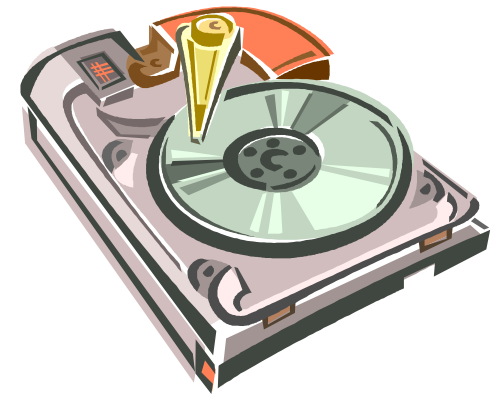
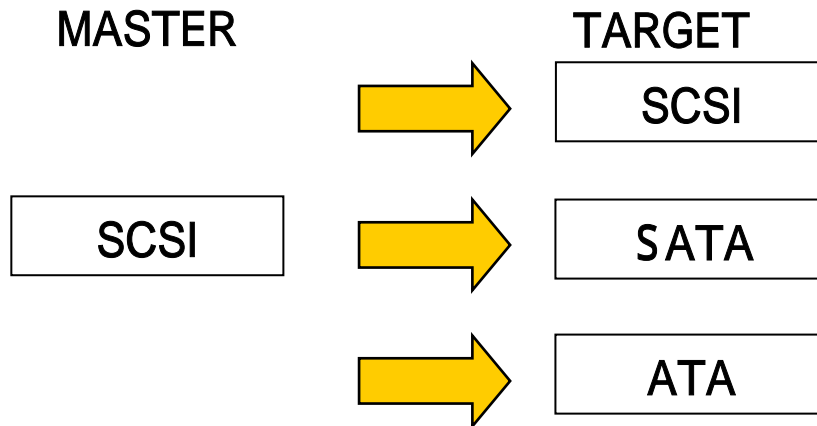
<http://www.kk-yec.co.jp/>

- 国産なのでサポートも安心？
- 現場の声を採用して開発
- 日本語と英語マニュアルの板ばさみから開放？

# 多彩なHDDインターフェース

- SCSI、ATA、SATAに対応

– クロスコピー (異なるHDDインターフェース間のコピー) にも容易に対応



# 簡単操作(多少癖あり)

- ボタンは

UP

DOWN

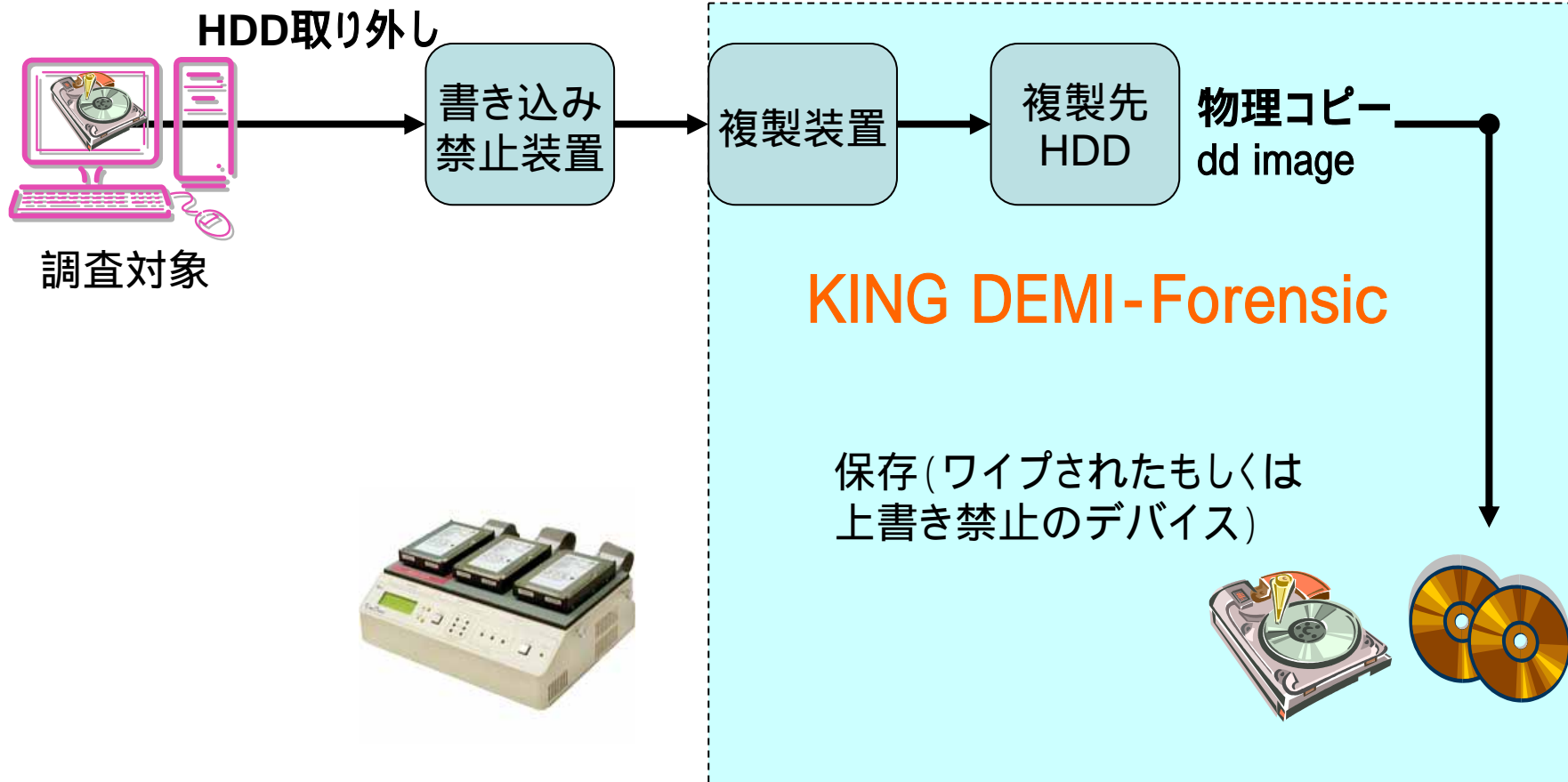
FUNC

START の4つ

その割には多機能

- ・コピー(ミラー、クリップ、不良スキップ、マッピング)
- ・消去(NSA、DoD、マニュアル)
- ・ddイメージ作成

# 証拠保全の流れ



# コピーの種類

- KING DEMI-Forensicの提供するコピー
  - 全領域(ミラー)コピー
  - 領域選択(クリップ)コピー
  - 不良スキップ(バックアップ)コピー
  - スキャン(マッピング)コピー
  - ddイメージ作成

# コピーの条件(共通)

- TARGET デバイスがMASTERデバイスと同等以上の容量であることが条件(解除可能)
- コンペアあり(解除可能)

# 全領域(ミラー)コピー

- MASTER(コピー元)デバイスの始めから終わりまで順番にTARGET(コピー先)にコピー  
エラーをスキップする処理はしない  
エラーの場合アイテムを終了

# 領域選択(クリップ)コピー

- MASTERデバイスの容量にあわせてTARGETをクリップ

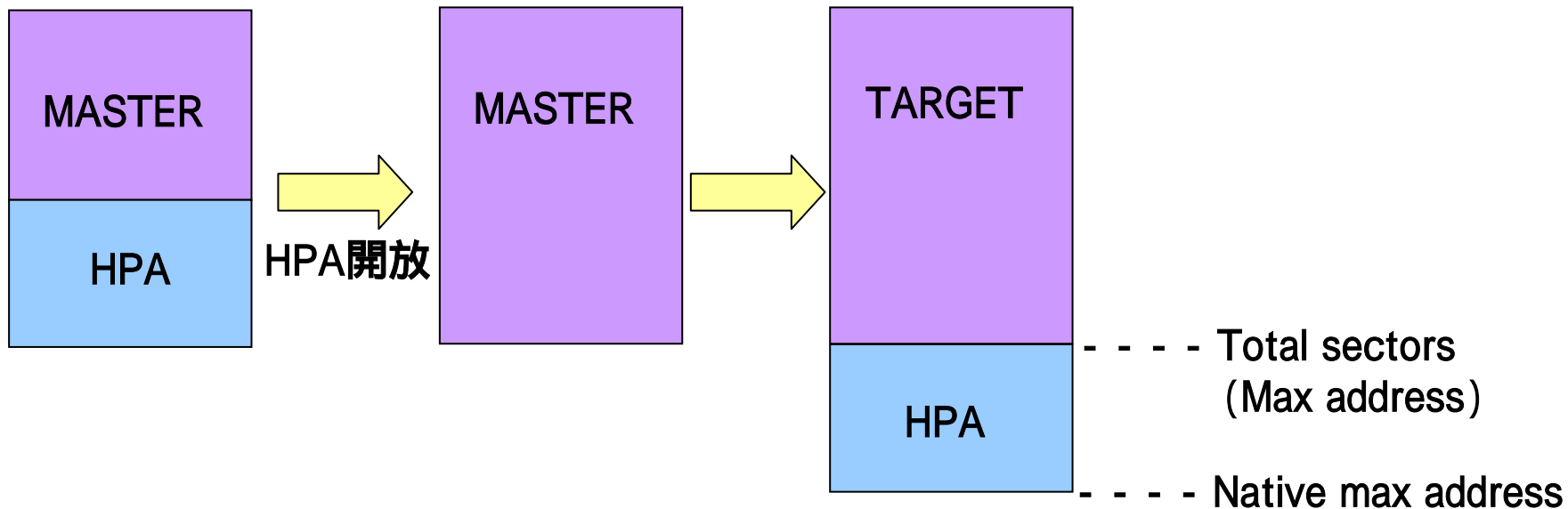
MASTERデバイスとTARGETデバイスのヘッド数が不一致であればエラー終了

クリップの指定はボリューム(MB単位)とLBAの2種類

# クリップコピーのイメージ

- TARGETデバイスの容量やアドレスを指定し、MASTERと同じボリュームを作成

事前にMASTER側での調査/設定変更(TAFT等)が必要



# 不良スキップ(バックアップ)コピー

- MASTERデバイスのデータを順番にTARGETにコピー

MASTERのリードエラーが発生した場合はセクタをスキップ

スキップしたセクタには何も書き込まない  
ビットコンペアは行わない

# スキャン(マッピング)コピー

- コピー前にMASTERデバイスのデータをスキャンし、データ領域のみをTARGETにコピー  
マッピングコピーにはマッピング専用のマスタHDDの作成が必要
  - 00h、E5h、F6h、FFhをマスタHDDに書き込み

FSマッピング・フレキシブルコピーはFAT12、FAT16、FAT32にのみ対応

FSマッピング・ミラーコピーはNTFSにも対応

# ddイメージ作成

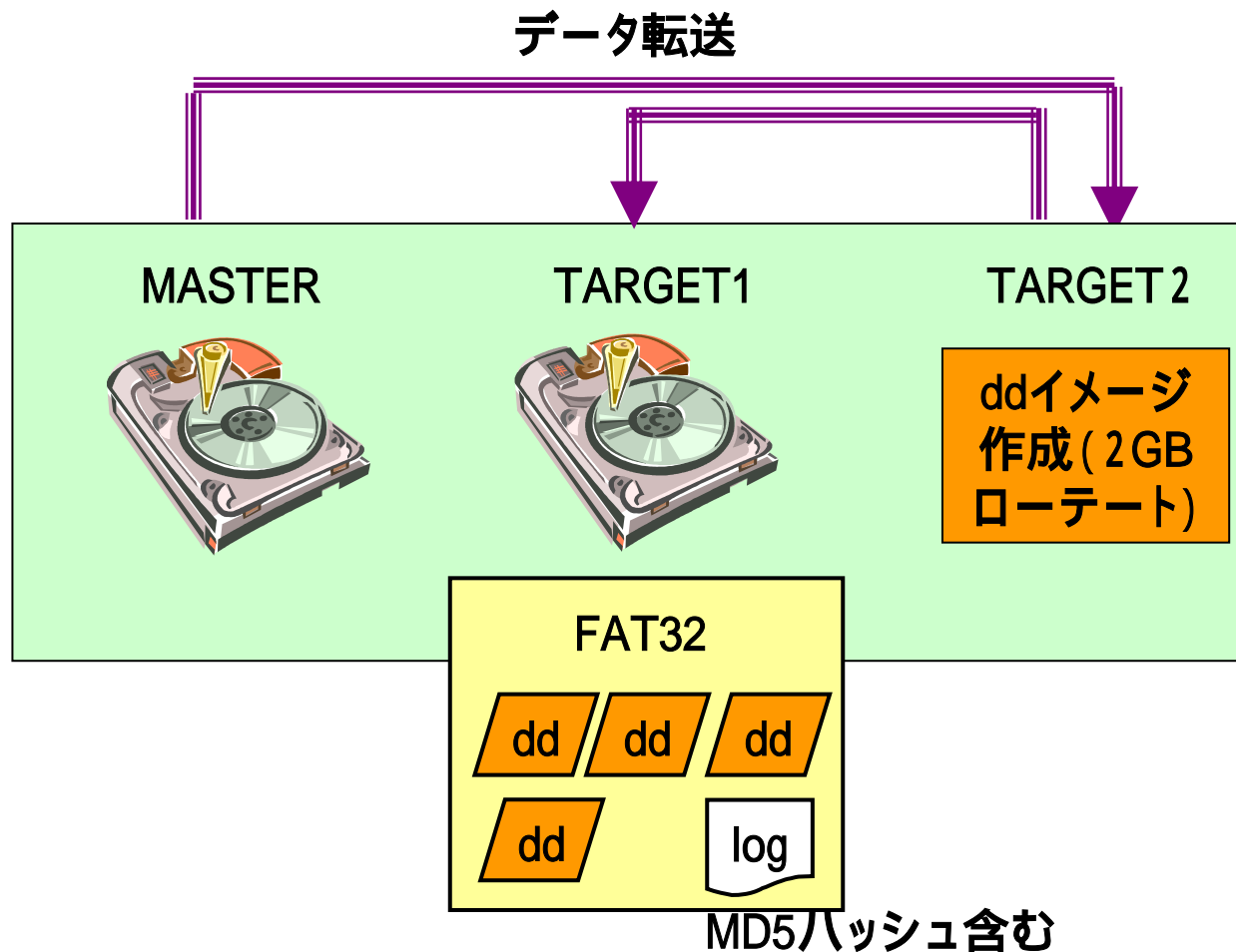
- MASTERデバイスのデータをTARGET 1 にddイメージファイルとして格納

同時に複数のTARGETデバイスに対しddイメージの格納はできない(イメージ図参照)

TARGETデバイスのフォーマットはFAT32のみ  
データのMD5ハッシュをTARGETデバイスにログとして格納

ddイメージのサイズ選択可能(ローテート上限2GB)

# KING DEMI dd作成イメージ図

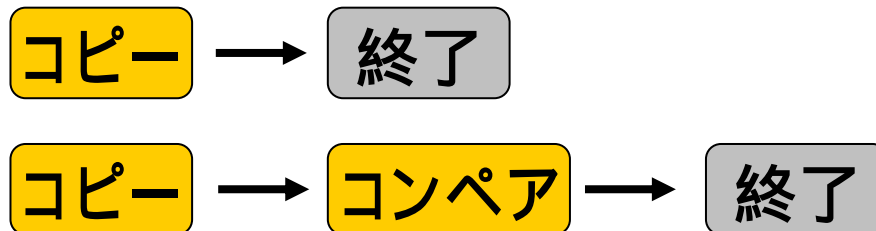


# 物理コピー速度

- KING DEMI-Forensicのコピー速度

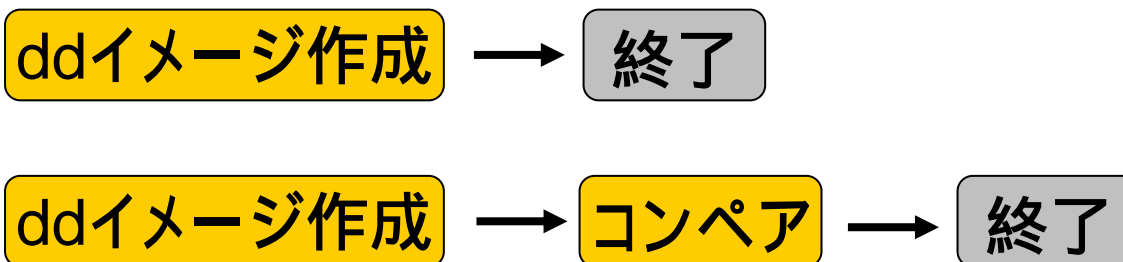
公式サイトでは1GB当たり 約20秒 (3GB/m) と  
の記述(2005年8月11日現在)

ALLコピー & コンペア実測値で1.3 ~ 1.5GB/m 程  
度



# ddイメージ作成速度

- KING DEMI-Forensicのddイメージ作成速度  
公式サイトでは速度に関する記述なし(2005年8月11日現在)  
実測値で0.6 ~ 0.8GB/m 程度
  - ただしコンペアまで含んだ値である



# 物理コピーとdd作成の速度比較(コンペア含む)

物理コピー = 1.4GB/m

dd作成 = 0.7GB/m

40GB HDDの場合

物理コピー	29分
dd作成	58分

250GB HDDの場合

物理コピー	179分(2時間59分)
dd作成	358分(5時間58分)

# その他機能

- 消去機能

NSA (米国家安全保障局) 準拠方式

DoD (米国防総省) 準拠方式

NSA準拠 + DoD準拠

マニュアル (全領域消去 + 全領域コンペア)

# その他機能

- 簡易診断機能

RANDOM SEEK

- ランダム位置に1000回のシーク

ALL VERIFY

- 全領域ベリファイ

RD & WT & RC

- リード&ライト&リードコンペア

# 物理コピー

- なぜ物理コピー？
- とにかく起動させることを優先
  - 「WindowsのATAハードディスクをSCSIハードディスクにコピーして、コピーされたSCSIハードディスクをWindowsシステムに接続すると、認識される確立はかなり高い」(製品FAQ DEMI-UAS Q7より引用)
- システムディスクの場合は？型番やメーカーの違うディスクは？Linuxの場合は？

# 検証内容

- ミラーコピー  
ATA250GB(日立)    ATA250GB(日立)
- 型番やベンダーの異なるディスクのコピー  
SATA82.3GB(日立)    SATA250GB(Maxtor)
- クロスコピー  
ATA    SATA

# 検証： ミラー & コンペアコピー (Windows)

- **検証環境**

MASTER: HDS722525VLAT80 (ATA250GB)

TARGET: HDS722525VLAT80 (ATA250GB)

- **検証内容**

MASTERにWindows2000 (Pro)をインストールしTARGETにミラー (コンペア) コピー後、同じマシンで起動

- **結果**

– 180分程度でアイテムを終了し、問題なく起動した

# 検証： ミラー & コンペアコピー (Linux)

- **検証環境**

MASTER: HDS722525VLAT80 (ATA250GB)

TARGET: HDS722525VLAT80 (ATA250GB)

- **検証内容**

MASTERにLinux (PacketBlackHoleOS) をインストールし  
TARGETにミラー (コンペア) コピー後、同じマシンで起動

- **結果**

– 180分程度でアイテムを終了し、問題なく起動した

# 検証： 型番やベンダーの異なるディスクのコピー (Windows)

- **検証環境**

MASTER: HDS728080PLA380 (SATA82.3GB)

TARGET: DiamondMax10 6L250S0(SATA250GB)

- **検証内容**

MASTERにWindows2000 (Pro)をインストールしTARGETにミラー (コンペア) コピー後、同じマシンで起動

- **結果**

– 60分間程度でアイテムを終了し、問題なく起動した

# 検証： 型番やベンダーの異なるディスクのコピー (Linux)

- **検証環境**

MASTER: HDS728080PLA380 (SATA82.3GB)

TARGET: DiamondMax10 6L250S0(SATA250GB)

- **検証内容**

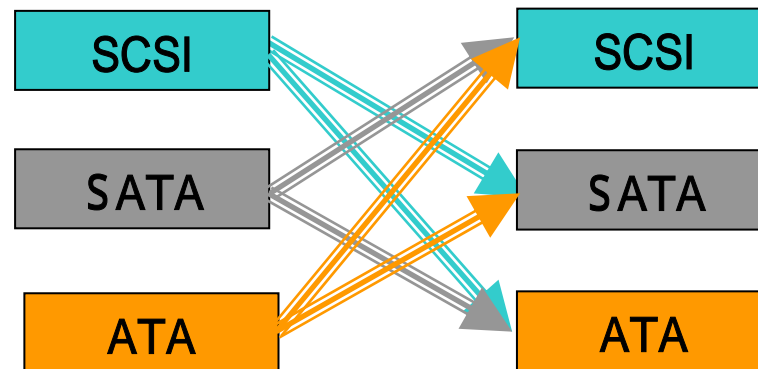
MASTERにLinux (PacketBlackHoleOS) をインストールし  
TARGETにミラー (コンペア) コピー後、同じマシンで起動

- **結果**

– 60分間程度でアイテムを終了し、問題なく起動した

# 検証： クロスコピー

- 用語：クロスコピーについて(製品FAQより引用)
  - 「ATAハードディスクからSCSIハードディスクへのコピーや、逆にSCSIハードディスクからATAハードディスクへのコピーのこと。  
(中略) 基本的には、一時的なバックアップとして利用します。」



# 検証： クロスコピー ATA SATA (Windows)

- **検証環境**

MASTER: HDS722525VLAT80 (ATA250GB: 日立)

TARGET: DiamondMax10 6L250S0 (SATA250GB)

- **検証内容**

MASTERにWindows2000 (Pro)をインストールしTARGETにミラー(コンペア)コピー後、同じマシンで起動

- **結果**

– 170分間程度でアイテムを終了し、問題なく起動した

# 検証： クロスコピー ATA SATA (Linux)

- 検証環境

MASTER: HDS722525VLAT80 (ATA250GB: 日立)

TARGET: DiamondMax10 6L250S0 (SATA250GB)

- 検証内容

MASTERにLinux (PacketBlackHole OS) をインストールし  
TARGETにミラー (コンペア) コピー後、同じマシンで起動

- 結果

– 170分間程度でアイテムを終了したが起動せず

# 起動しない理由推測 (Linux)

- **起動時のエラー確認**

Kernel Panic: VFS: Unable to mount root fs

- 単に起動デバイス設定の問題？

# 起動しない理由実証 (Linux)

- デバイスを検証用PCに接続して起動
  - デバイスの /boot パーティションをマウント
  - デバイスの / パーティションを /mnt (適当) にマウント
  - エディタで /mnt/etc/lilo.conf を書き換え
    - Default boot image の “ root=/dev/hda7 ” の記述を “root=/dev/sda7” と変更 (SATA デバイスなので)

# 起動しない理由実証 (Linux)

## liloの実行

- `/mnt/sbin/lilo -C /mnt/etc/lilo.conf`

## エディタで/mnt/etc/fstabを書き換え

- /mnt/etc/fstabの“ /dev/hda7     /”の記述を  
“ /dev/sda7     /” と変更
- /mnt/etc/fstabの“/dev/hda1     /boot”の記述を  
“/dev/sda1     /boot”と変更

再起動を行い、**正常に起動することを確認した**

# クロスコピーしたディスクで起動するには (Linux)

- 各種設定ファイルの書き換えを行う
  - (当たり前だが) King Demiは物理コピーを実行するだけ。設定ファイルの変換はしてれない
    - lilo.confの書き換え
    - fstabの書き換え
    - その他あれば書き換え
- ハードディスクの論理フォーマットの確認
  - 様々な仕様が存在するので確認が必要 (TAFT?)

# クロスコピーしたWindows

- 気になった点

起動時に自動で起動デバイスの設定を変更している

- インターフェースを変えても起動する
- 最初の起動に時間がかかり、起動後すぐに再起動を求められる

## ライセンス違反に注意

- Windowsのライセンスはインストール単位なので、物理コピーはライセンス違反となる？

# クロスコピーまとめ

- 起動させるには

Windowsは特に問題なく起動する

Linuxは設定ファイルを変更すれば起動する

- 気になる点

もしWindowsOSが起動デバイスの変更に失敗したら？(お手上げ)

Linuxならどうにかなる

# 全体まとめ

- **物理コピーするディスクの容量**

現場に持っていくディスクの種類、容量は余裕を見る(事前に情報を得ることも必要)

調査用のフロッピー(TAFT等)及びドライブを持っていくと便利。

- **今後の検証**

Windowsのレジストリについて(2003含む)

クリップコピーの活用

ディスクにパスワードがかけられている場合