

第二回 調査技術ゼミ
2005年9月05日

『 暗号化とフォレンジック調査 』
フォレンジック・イメージ作成の手順

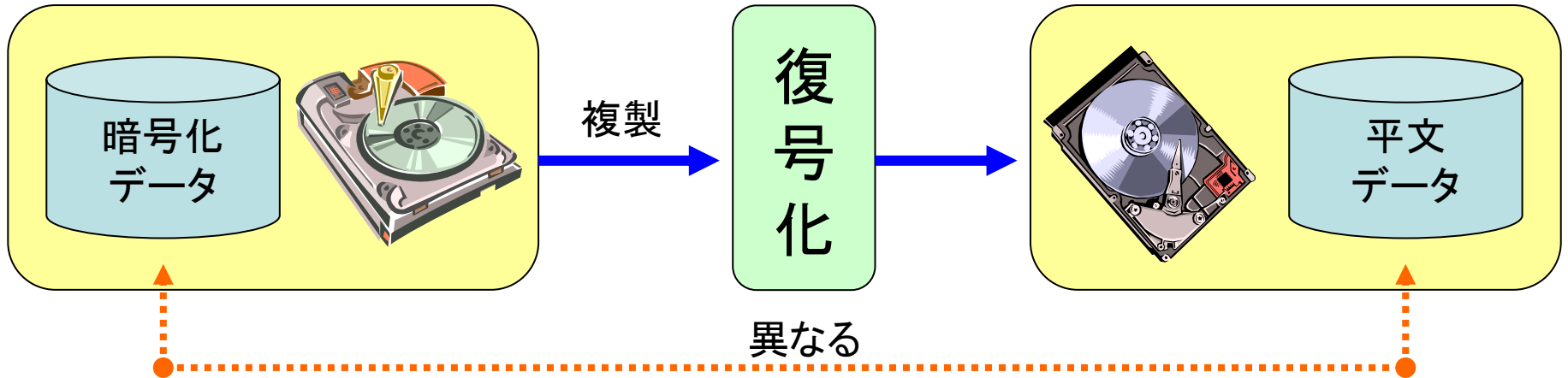
ネットエージェント株式会社

最良証拠の原則

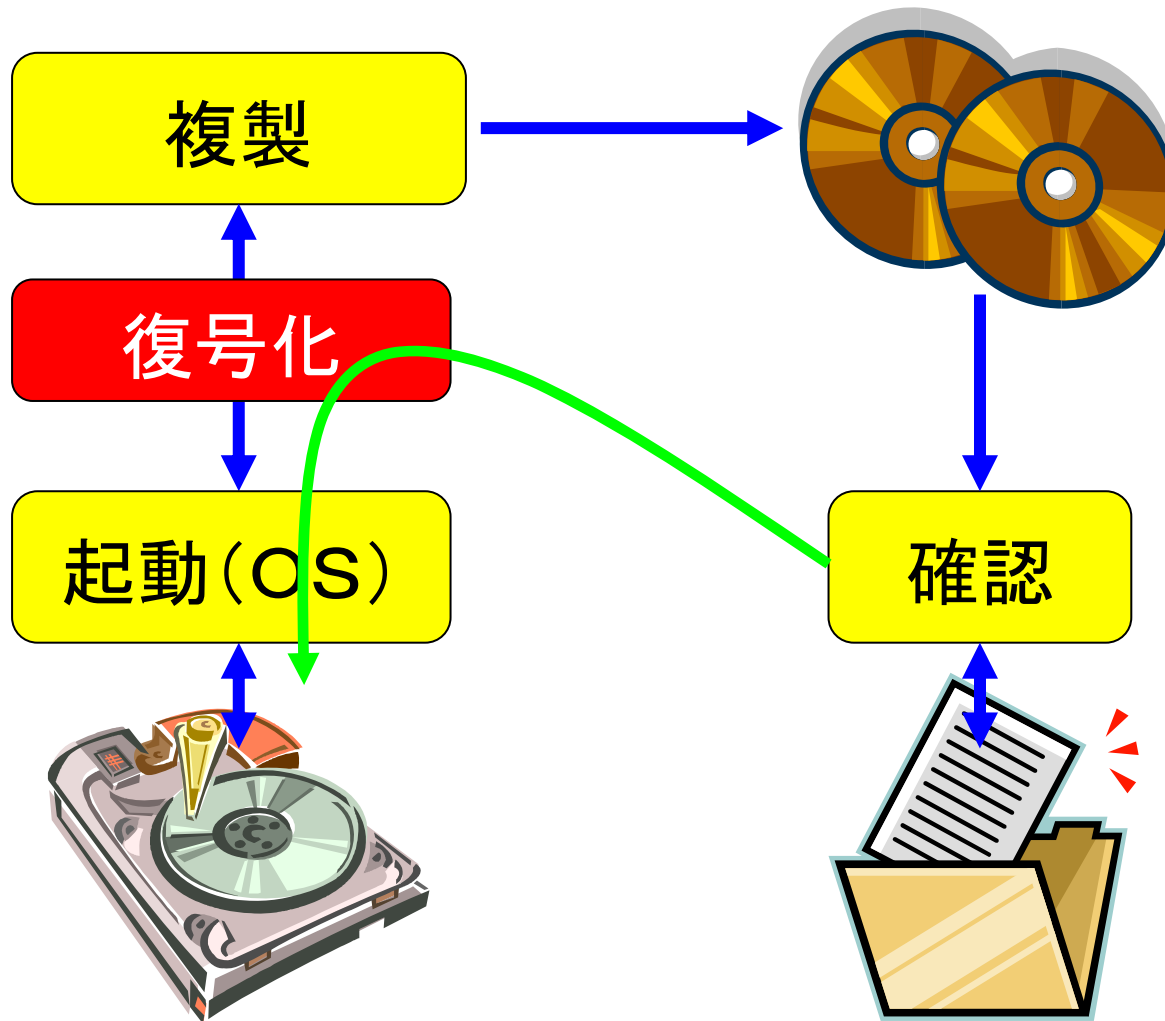
- Computer & Network LAN 2005年3月号
「法律面から見たデジタル証拠の扱われ方」
千葉大学 法経学部 石井徹哉著
P36より引用
- 『通常、文書や録音物または写真について、その内容を証明するには、原則として原本が必要であるとされる(最良証拠の原則、ベスト・エヴィデンス・ルール)』



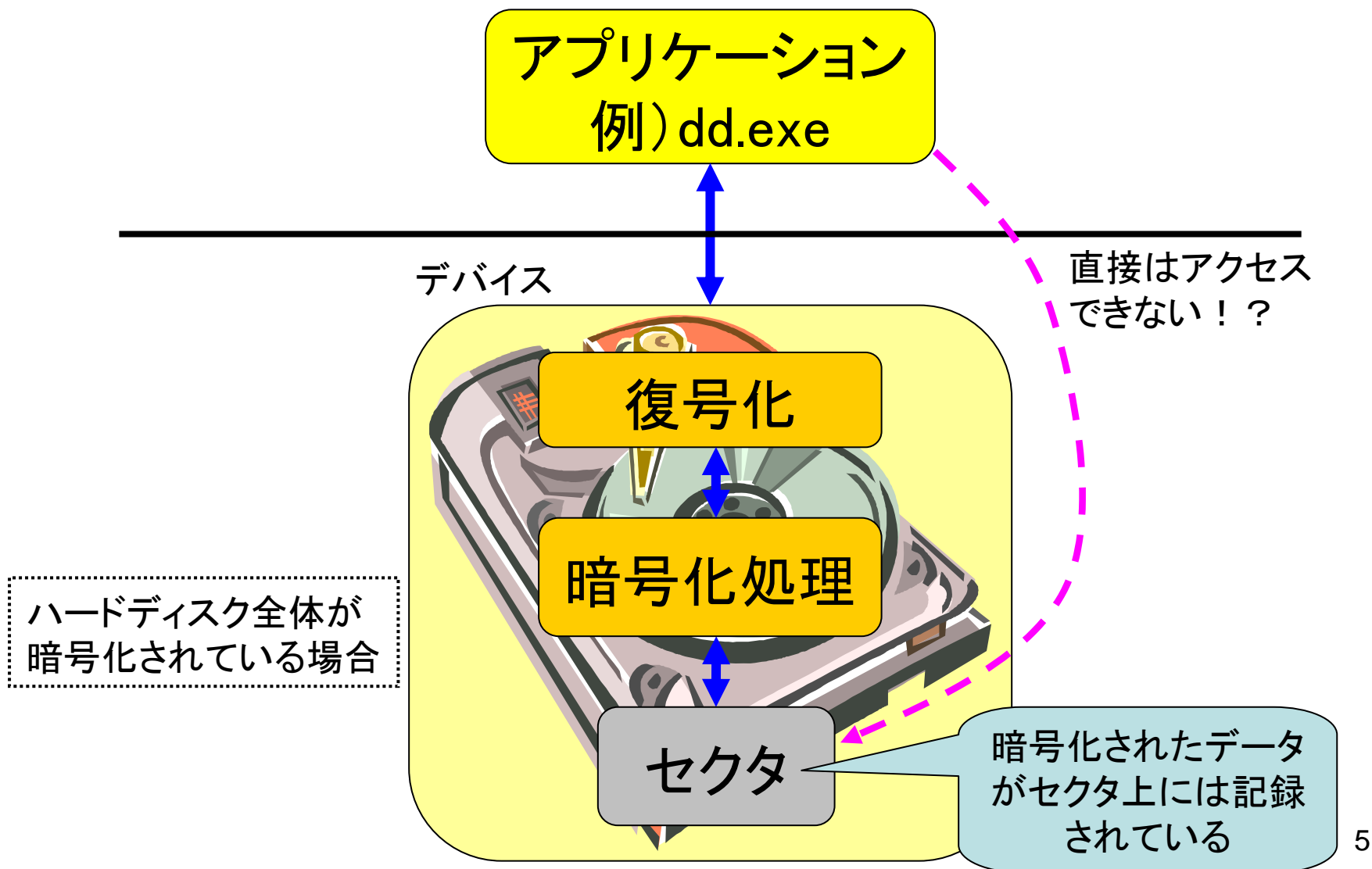
ディスクの複製



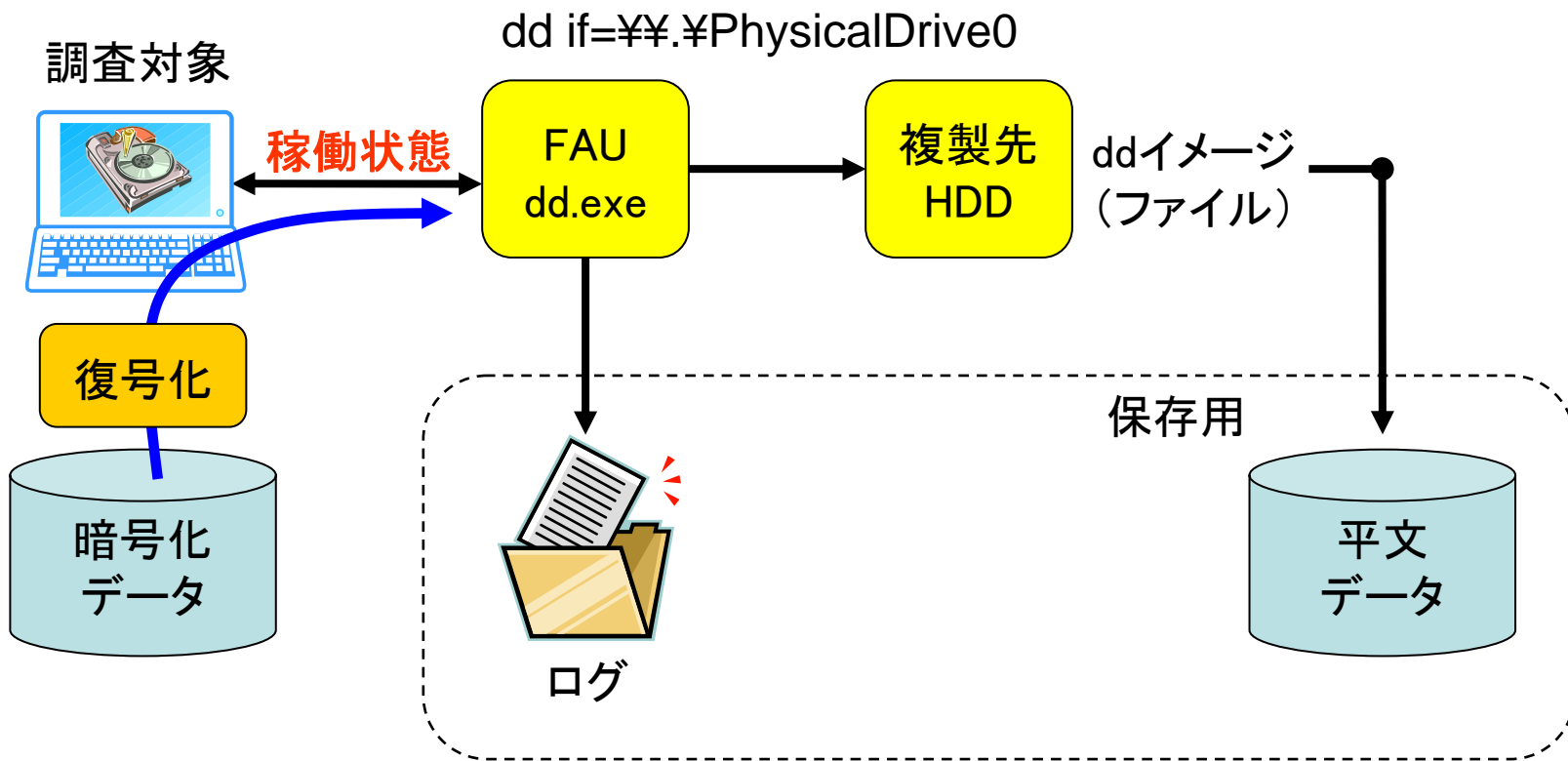
起動・複製・確認



データ アクセス (稼働中)

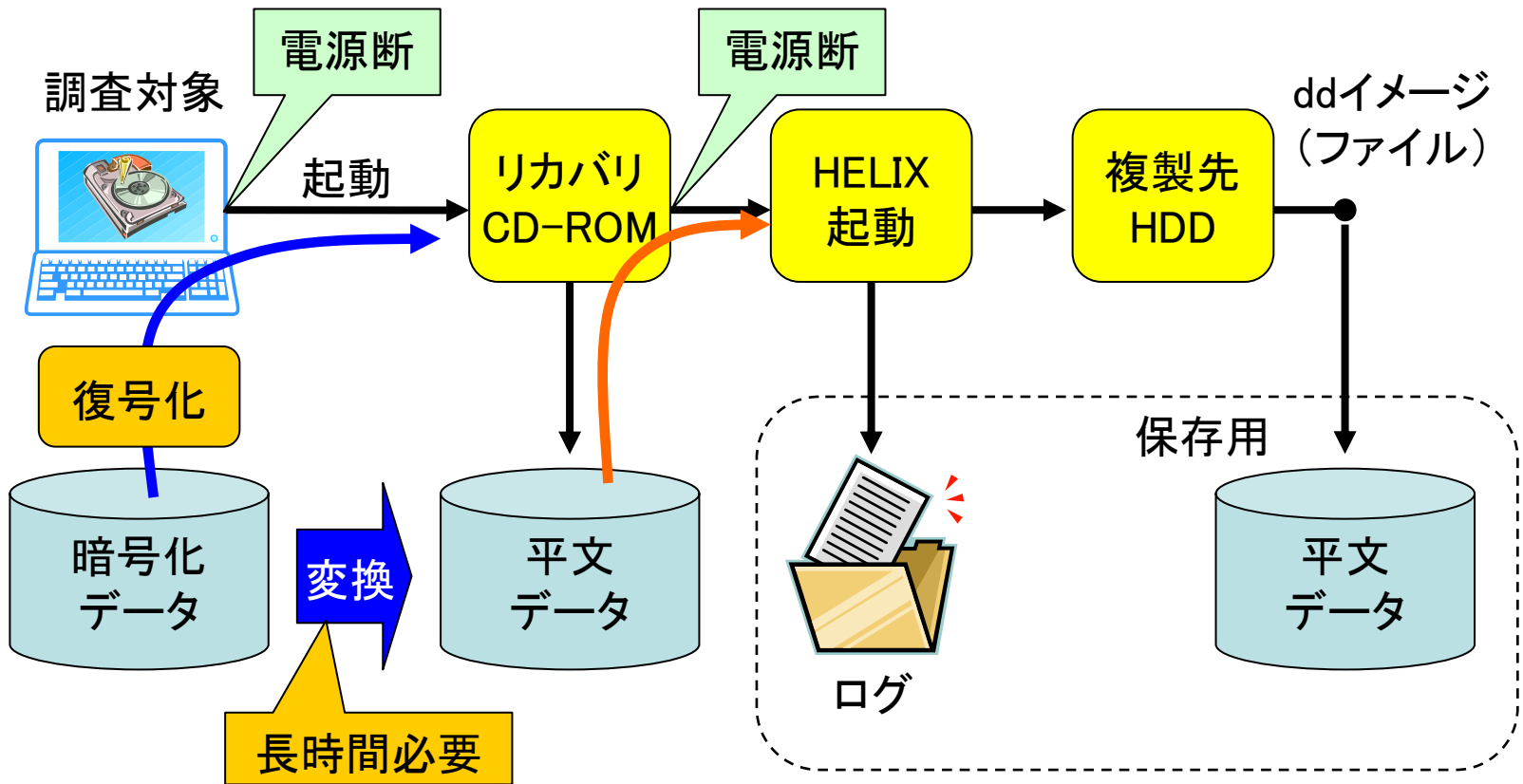


FAU利用時(稼働中)



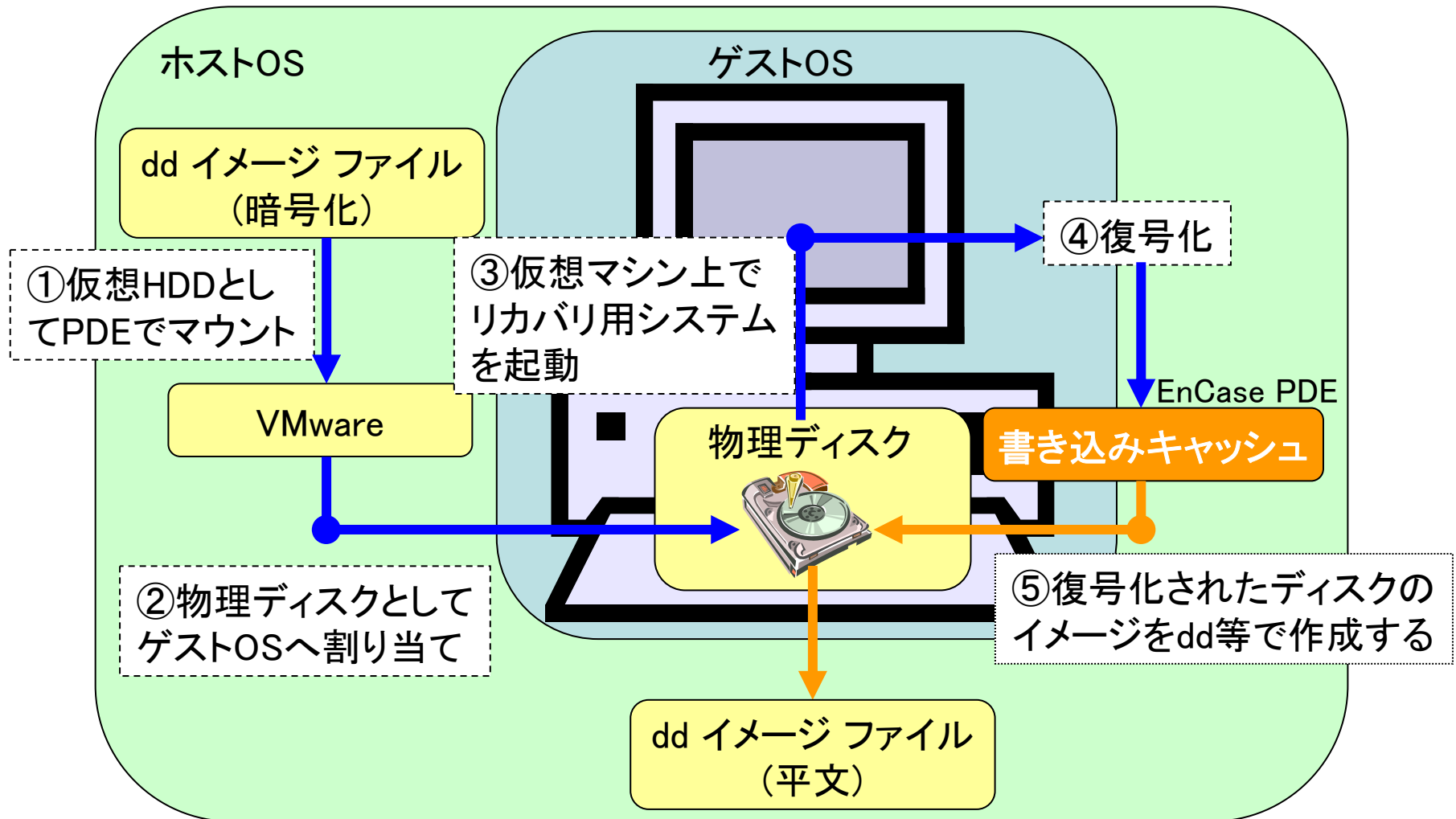
稼働中システムのHDD全体を dd.exe により複製

リカバリ処理



暗号化されたデータ(セクタ)を復号化しアクセス可能な状態(平文)へ変換を行った後に複製を行う

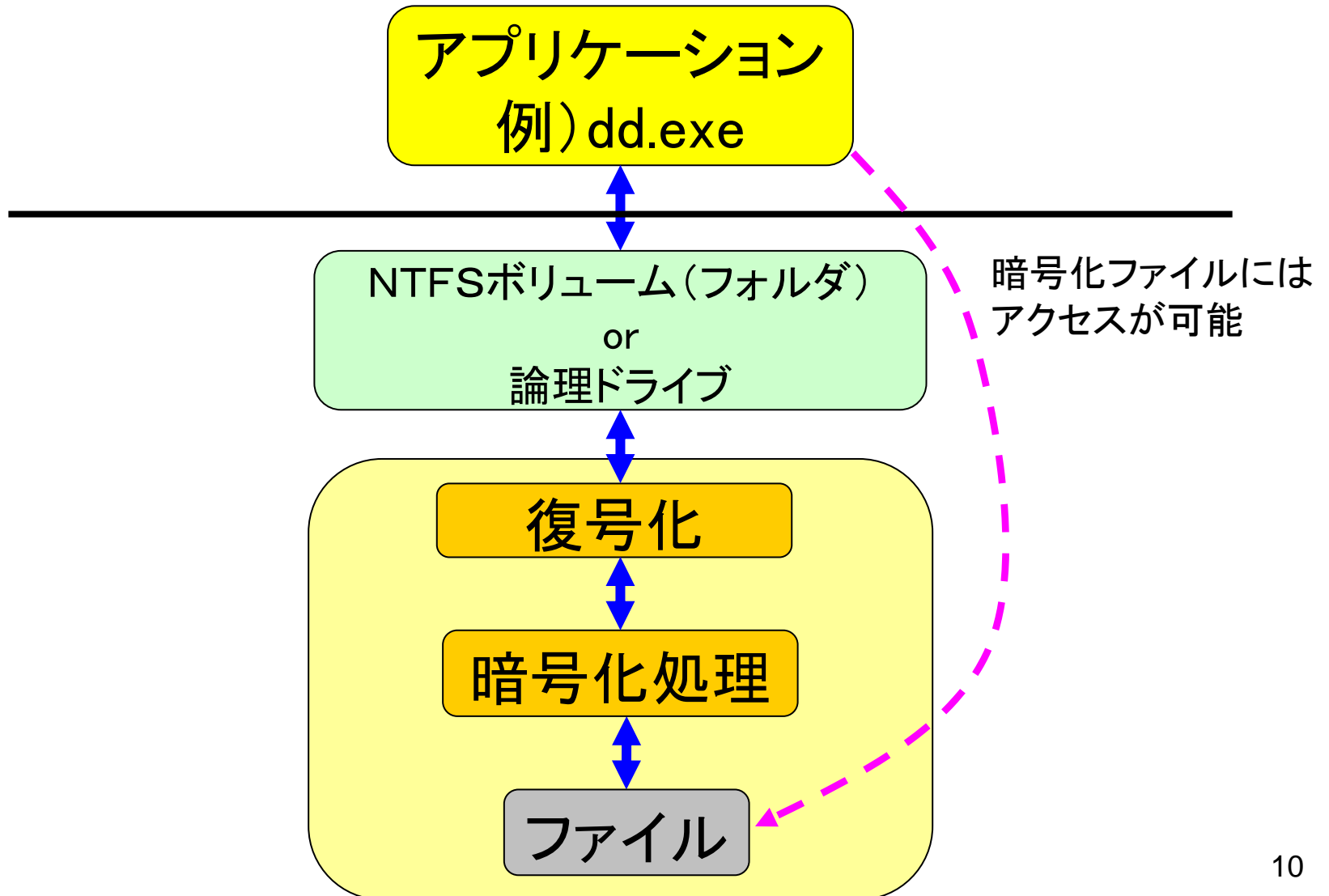
EnCase PDEを利用した変換



暗号化状態での複製

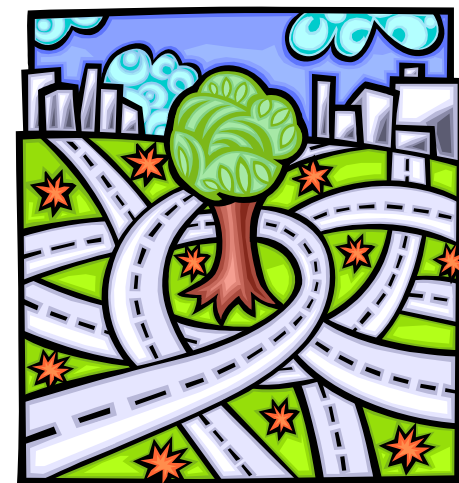
- 復号化(リカバリ)処理は長時間必要となる
- 複製で復号化処理が可能であれば、暗号化された状態で複製し、後から復号化したほうが時間的に有利
- *ハードウェアに依存しない場合に利用可能*

仮想ディスク ボリューム



仮想ディスクの確認方法

- マウント方法
 - ①論理ドライブとしてマウント
 - ②NTFSボリューム上のディレクトリ
- 現在の論理ドライブ (DOSドライブ)を確認
> fsutil fsinfo drives
- Winmsd (msinfo32.exe)
> 記憶域 → ドライブ
- ボリューム一覧を確認
> mountvol



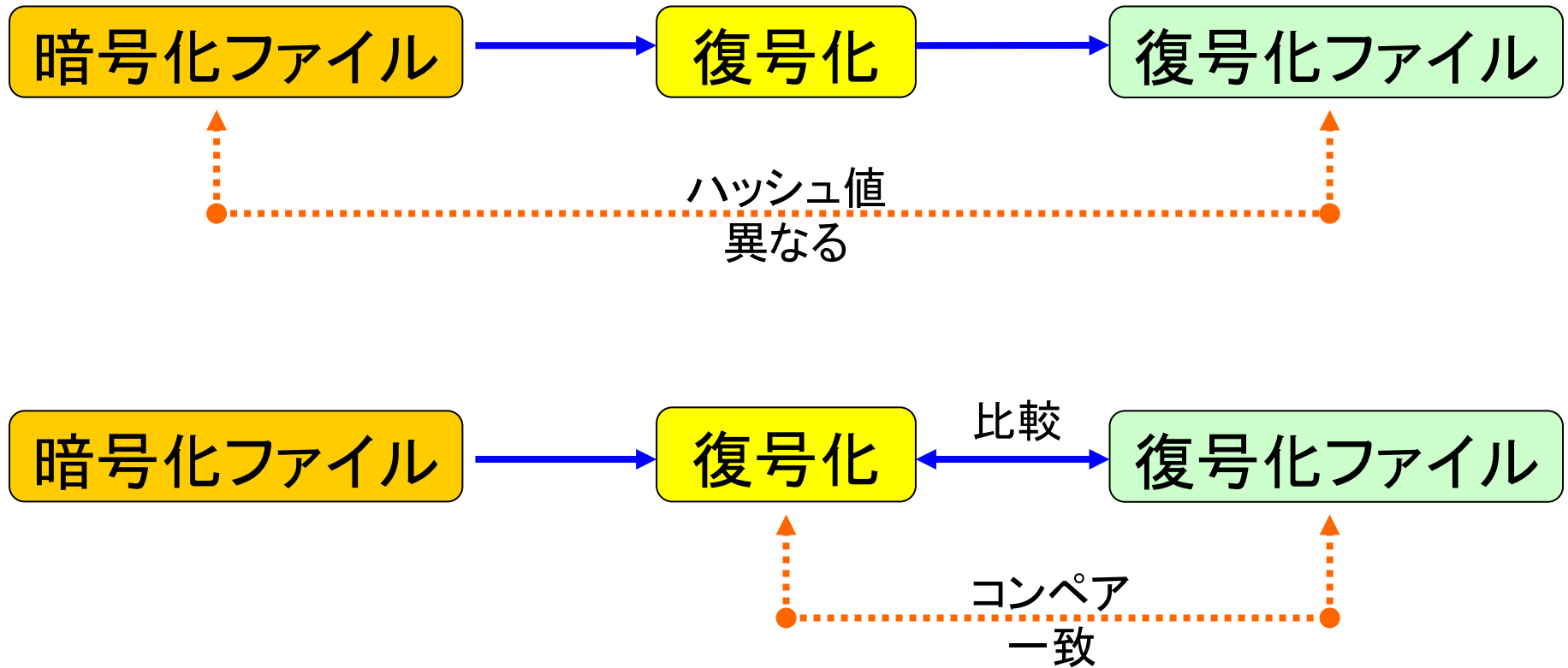
仮想ディスクへのアクセス

- ・ ログオン中のユーザのみ仮想ディスク(論理ドライブ・ボリューム)へアクセス可能な場合
- ・ プログラム(CMD.EXE, dd.exe等)の起動が制限されている場合

仮想ディスクの存在を別のユーザーからは確認できず、複製を行えない危険性がある



暗号化ファイル



**解き明かす力、今すぐにでも。
フォレンジック・サービス**

NetAgent

The Forensics Company

<http://forensic.netagent.co.jp/>