デジタル・フォレンジックのための ファイルシステム ・Windows OS講義

立命館大学
情報理工学部　教授
（東京電機大学客員教授）

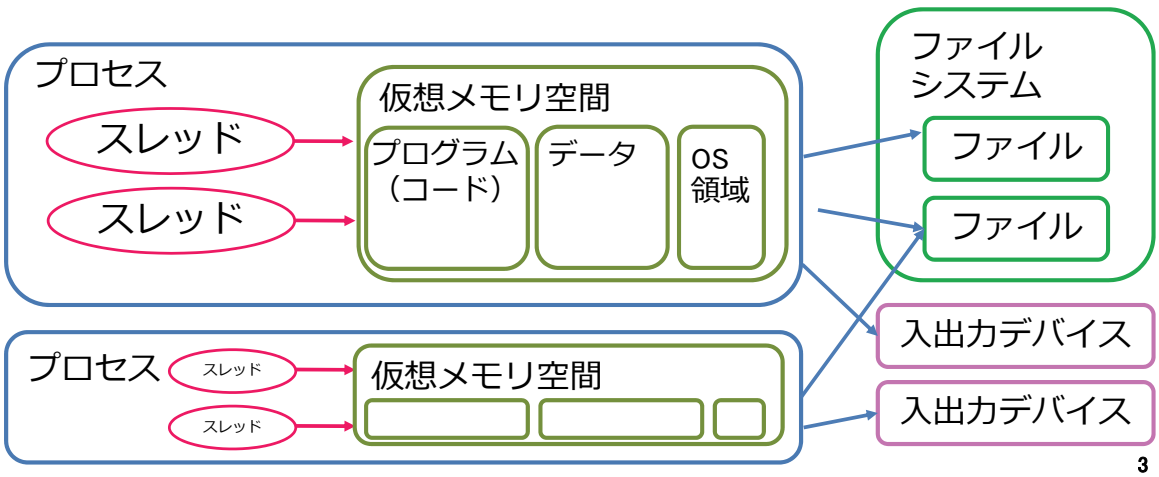
上原　哲太郎

フォレンジックのためのOS入門

- OSを1コマで話しきるのは無理な話
- そこでいわゆる計算機科学の講義の内容から「ログ」の理解に至るように話を構成
  - OSの種類・構造
  - プロセス管理・プロセスツリー・プロセス状態遷移
  - 仮想記憶の仕組み
  - プロセスのダンプの取り方
  - 各種ログの残る位置

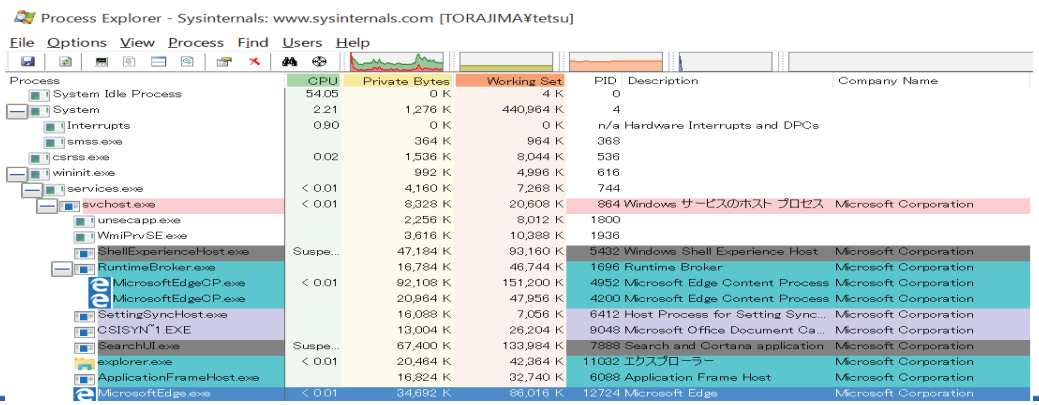
プロセス管理

- プロセス＝プログラムを起動した実体をさす言葉
  - 類似語多数：ジョブ・タスク・プロセス・スレッド…
    - ジョブは複数のタスクやプロセスを含む「一連の仕事」
    - タスクはジョブと同義かプロセスと同義で使う
    - プロセスは「資源管理の単位」
      - 1つの仮想メモリ空間と複数の仮想CPUを持つ
      - 各仮想CPUを「スレッド」と呼ぶ



プロセスツリー

- プロセスは他のプロセスを起動するので「親子」関係が発生　全体として木(ツリー)に
- 親子の「縁」がある間は親が死ぬと子も死ぬ
  - 親子の縁を切ることをデタッチ（detach）と呼ぶ
- LinuxなどUNIX系ではpsコマンドで調べる
- WindowsではProcess Explorer: procexp.exeが便利



Windowsレジストリ

- 元はWindowsのOSやアプリケーションが設定情報を格納するためのデータベース
  - システム全体は¥windows¥system32¥config¥にsam, sam.sav, sam.logなどいくつかのファイルに別れて格納されている
  - ユーザごとの情報は¥Windows¥Profiles¥ユーザ名にNtuser.dat, Ntuser.dat.logなどに別れて格納されている
  - 内容はファイルシステム的だが格納できるデータ形式に「型」がついており制限がある
- ¥HKEY_CLASSES_ROOT
  ¥HKEY_CURRENT_USER　　（よく¥HKCUなどと略す）
  ¥HKEY_LOCAL_MACHINE
  ¥HKEY_USERS
  ¥HKEY_CURRENT_CONFIG
- この中にいくつかログ的なものがある
  - 例えば¥HKCU¥Software¥Microsoft¥Windows¥Currentversion¥Explorer¥に最近使ったファイル等の情報が残存

OS入門の反省点

- 多分予備知識のある人にとっては簡単すぎ
  一方で前提知識のない人は
  新語が飛び交って混乱した恐れ
- 時間にわりと余裕があったので
  実例や実演をもっと入れて
  咀嚼する時間をとった方が良い

ハードディスクの構造
ファイルシステム

- いわゆる古典的フォレンジック技法の背景を理解してもらうための時間
- やはりツールより基礎に重点
  - 物理的な話としてメディアの種類・インターフェースの種類
  - パーティションの構造（MBR、GPT）
  - ファイルシステムの基本（メタデータ構造）
  - FATの構造とファイル復元の仕組み
  - NTFSの構造とファイル復元の仕組み

代表的二次記憶媒体

- 磁気記録
  - ハードディスク　（媒体：ガラス＋磁性体など）
  - 他にフロッピーディスク、テープなど
    - 磁気に弱い　熱にも弱い
- 光による記録
  - CD-R/RW/RAM、 DVD-R/RW/RAM、 BD-R/REなど
    - 最近の低価格化に伴い比較的消えやすい
  - 亜種として光磁気記録（MO）
    - 保存性はかなり高いが最近用いられない
- 半導体記録
  - フラッシュメモリ（SDカード等、SSD）
    - 電気的に壊れることがある
    - 最近急速に書き換え可能回数が減っている

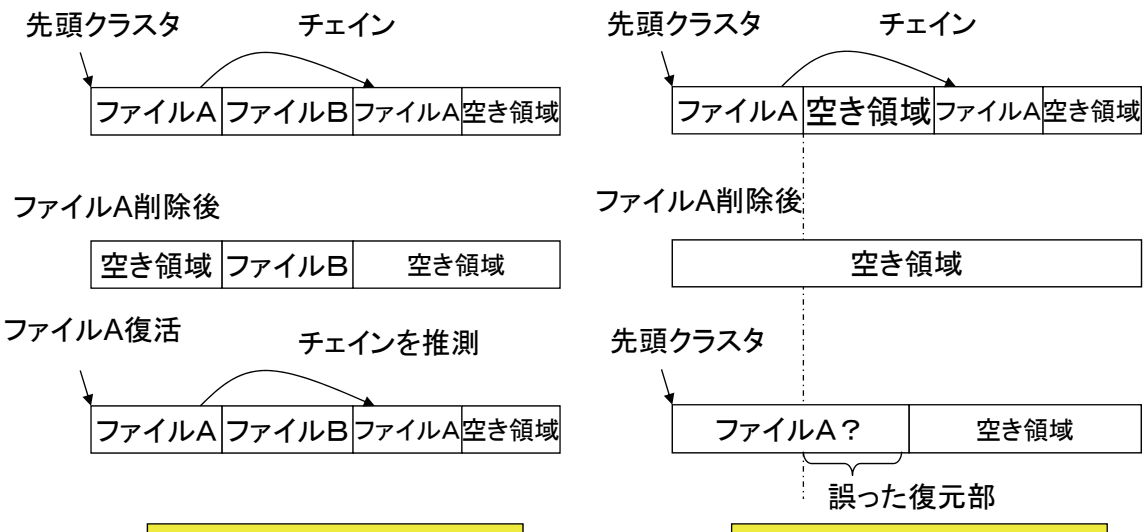
評価項目
- 読み書き速度
- 書き換え可能回数
- 磁気/熱/電気/光などに対する耐性
- 経年劣化への耐性

ハードディスクインターフェース

- フォレンジック作業に必要な知識
- ATA(IDE)→SATA
  - IDEではフラットケーブルを使用(40または80芯)
    - 物理規格の細かな差によりATA-1～ATA-7まで分けられる
    - 速度規格もいくつかあり(UDMAなら16.7～166.6MB/s)
  - SATAでは太い単芯線
    - 速度によりSATA-1(1.5Gbps)～SATA-3(6Gbps)まで
- SCSI→Serial Attached SCSI(SAS)
  - 元のSCSIは50芯か68芯のケーブルを使用
  - SASは物理規格をSATAと統一、論理的にもSATAドライブも利用可能に
- FiberChannel (FC)
  - サーバで見られる方式

クラスタチェインの復元がうまくいかない場合

- 上書きされていなくても、クラスタチェインの推測がうまくいかない場合がある・・・



ハードディスクの構造
ファイルシステムの反省点

- SSDの話が十分に出来なかった
  （僅かに触れただけ）
  今後の重要度を考えると厚みをつける必要
- テープなどが扱えなかった
- クラウドについても考えておく必要

- 割と言いたいことに対して時間が足りない印象