内部不正対策ソリューションガイド公開イベント
～ これでわかる内部不正対策！

パネルディスカッション

株式会社ディアイティ
山田　英史

2014年1月29日

フォレンジックとは

- インシデントレスポンス（コンピュータやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為（事象）等への対応等を言う。）や法的紛争・訴訟に際し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術を言います。

引用：　NPO デジタル・フォレンジック研究会

http://www.digitalforensic.jp/index.html

実録、デジタルフォレンジック

- 不正が疑われる社員がいた。
  → 休日の深夜、その社員のパソコンからHDDのデータを抜き出し、解析し、不正行為を把握。
- 情報漏洩事件がおきたが、犯人がわからない。
  → 社内の全パソコンを調査し怪しい痕跡を発見。芝居をうって疑わしい社員を帰宅させ、改めて時間をかけて解析して行動を特定。
- 退職した社員が、元上司に罪を着せるために情報流出をおこした。
  → 退職者のパソコンのHDDを解析。流出した情報と同じファイルを自宅へメール送信していた痕跡を発見、証拠とした。

対処
（事後対応）

・被害内容、被害範囲の確認
・原因調査、分析
・再発防止
・不正アクセス、侵入者の特定

追跡に必要な情報を確実に保全し、詳しく調査し、さまざまな要素から、過去に起きた事象(不正アクセス、不正侵入)を推測。

ネットワーク
フォレンジック技術

ネットワークデータを全て収集・蓄積し、再現する。

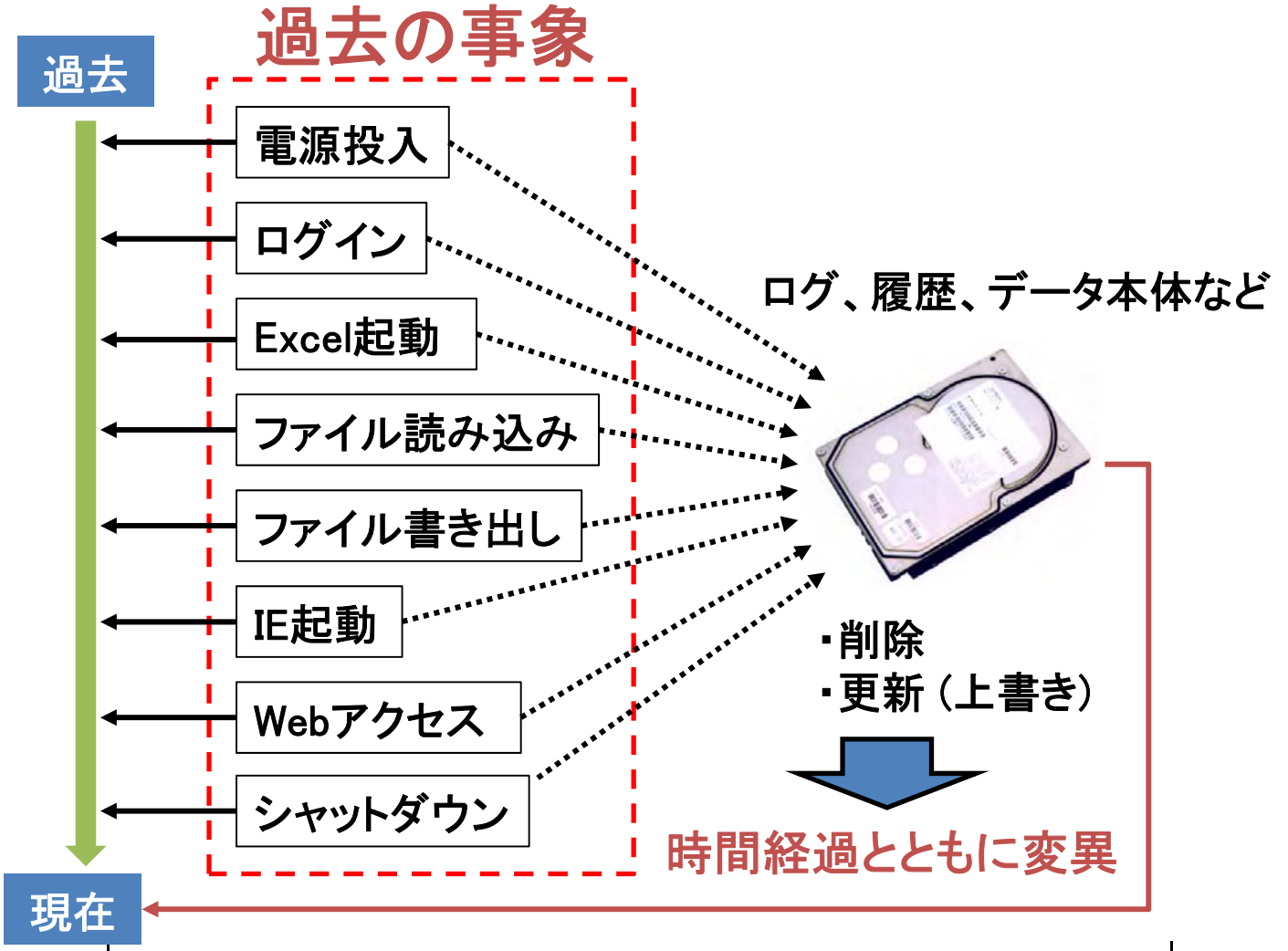
コンピュータ
フォレンジック技術

コンピュータを詳細に調査し不正行為の証拠を取得

インシデント原因の特定

- 事故・障害の原因の特定
  - コンピュータフォレンジックでは、コンピュータ上の記録から、事故・障害が起きた時の「コンピュータの状態」を再現し、事故の原因などを推測
  - 他の記録（ネットワーク上の記録、入退室記録、行動記録等）と突合して現場の復元をする場合もある
- 事故現場の回復と情報収集
  - 事故発生当時の状況を復元することで様々な情報を収集し、コンピュータ上で起こったことを再現
  - OSの操作の痕跡を読み取り、CPU、メモリ、ディスクの動作を再現、推測
  - 痕跡をどの程度回復できるかによって、事故発生時の状況の再現度合いが変わる　→ 削除されてしまったデータをどの程度復旧することができるのかが鍵

時系列に整理し分析



不正を取り締まるだけではない

- 行為者の特定
- 行為者の意図（故意／偶発）

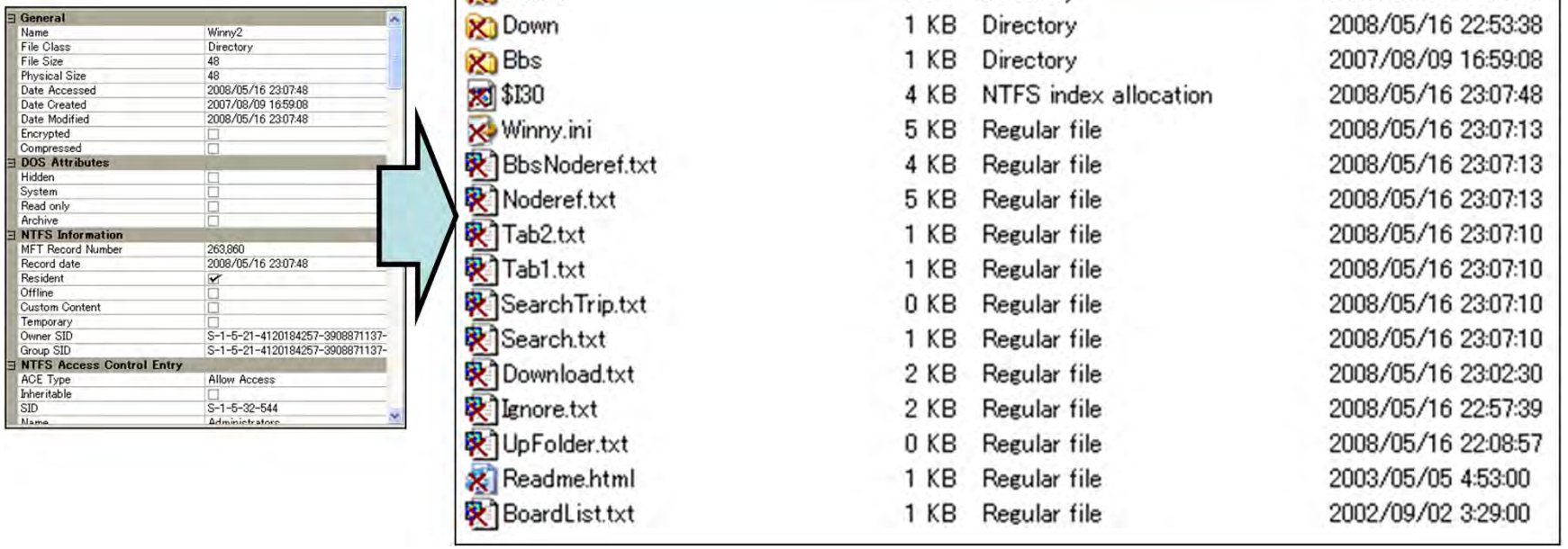
両方の目的に応用できる

- 無関係な者の保護（排除）
- 正当な行動の証明

解析手法

- ファイル、フォルダ
  - 残存ファイル、フォルダ
  - 削除痕跡
  - ゴミ箱
  - 復元ポイント
  - アクセス履歴 (Recent、レジストリ内MRLなど)
- プログラムの実行
  - プリフェッチ
- Webアクセス
  - アクセスサイト履歴 (IEの場合 index.dat)
  - コンテンツキャッシュ (クッキー含む)
  - フォームデータ (レジストリ)
  - TypedURLs (レジストリ)
- 各種ログ
  - イベントログ
  - FWログ
  - その他

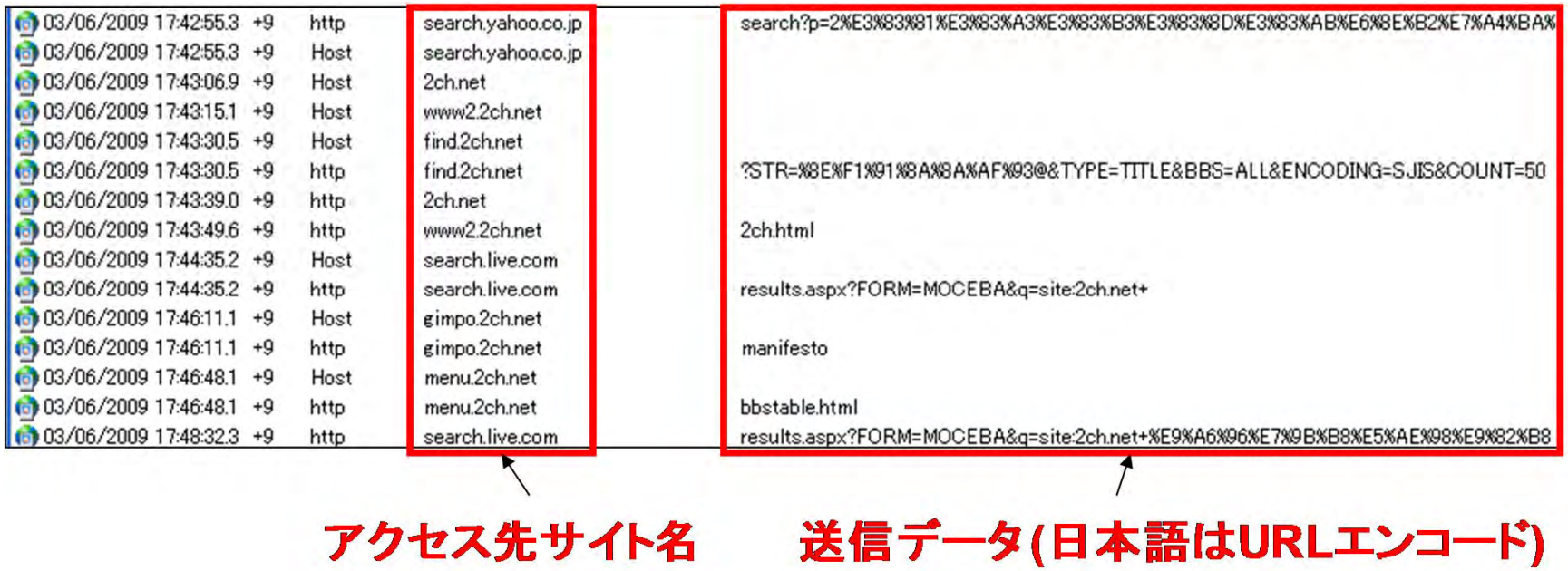
削除されたファイルの痕跡



General	
Name	Winny2
File Class	Directory
File Size	48
Physical Size	48
Date Accessed	2008/05/16 23:07:48
Date Created	2007/08/09 16:59:08
Date Modified	2008/05/16 23:07:48
Encrypted	☐
Compressed	☐
DOS Attributes	
Hidden	☐
System	☐
Read only	☐
Archive	☐
NTFS Information	
MFT Record Number	263,860
Record date	2008/05/16 23:07:48
Resident	☑
Offline	☐
Custom Content	☐
Temporary	☐
Owner SID	S-1-5-21-4120184257-3908871137-
Group SID	S-1-5-21-4120184257-3908871137-
NTFS Access Control Entry	
ACE Type	Allow Access
Inheritable	☐
SID	S-1-5-32-544
Name	Administrators

Name	Size	Type	Date Modified
Cache	1 KB	Directory	2008/05/16 23:07:48
Down	1 KB	Directory	2008/05/16 22:53:38
Bbs	1 KB	Directory	2007/08/09 16:59:08
$I30	4 KB	NTFS index allocation	2008/05/16 23:07:48
Winny.ini	5 KB	Regular file	2008/05/16 23:07:13
BbsNoderef.txt	4 KB	Regular file	2008/05/16 23:07:13
Noderef.txt	5 KB	Regular file	2008/05/16 23:07:13
Tab2.txt	1 KB	Regular file	2008/05/16 23:07:10
Tab1.txt	1 KB	Regular file	2008/05/16 23:07:10
SearchTrip.txt	0 KB	Regular file	2008/05/16 23:07:10
Search.txt	1 KB	Regular file	2008/05/16 23:07:10
Download.txt	2 KB	Regular file	2008/05/16 23:02:30
Ignore.txt	2 KB	Regular file	2008/05/16 22:57:39
UpFolder.txt	0 KB	Regular file	2008/05/16 22:08:57
Readme.html	1 KB	Regular file	2003/05/05 4:53:00
BoardList.txt	1 KB	Regular file	2002/09/02 3:29:00

IEアクセス履歴

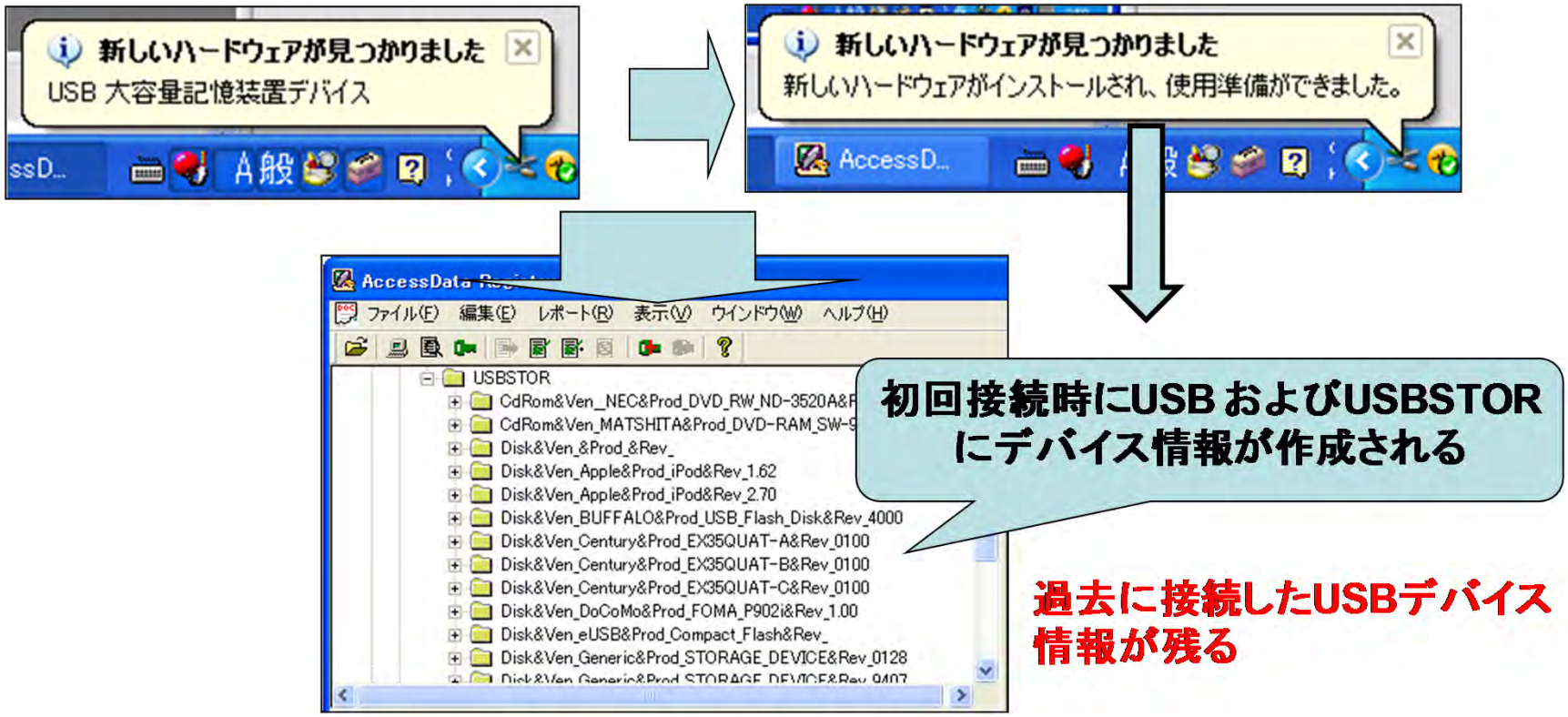


C:¥Documents&Setting¥<ユーザ>¥Localsettings¥Temporary Internet Files¥
C:¥Documents&Setting¥<ユーザ>¥Localsettings¥History¥

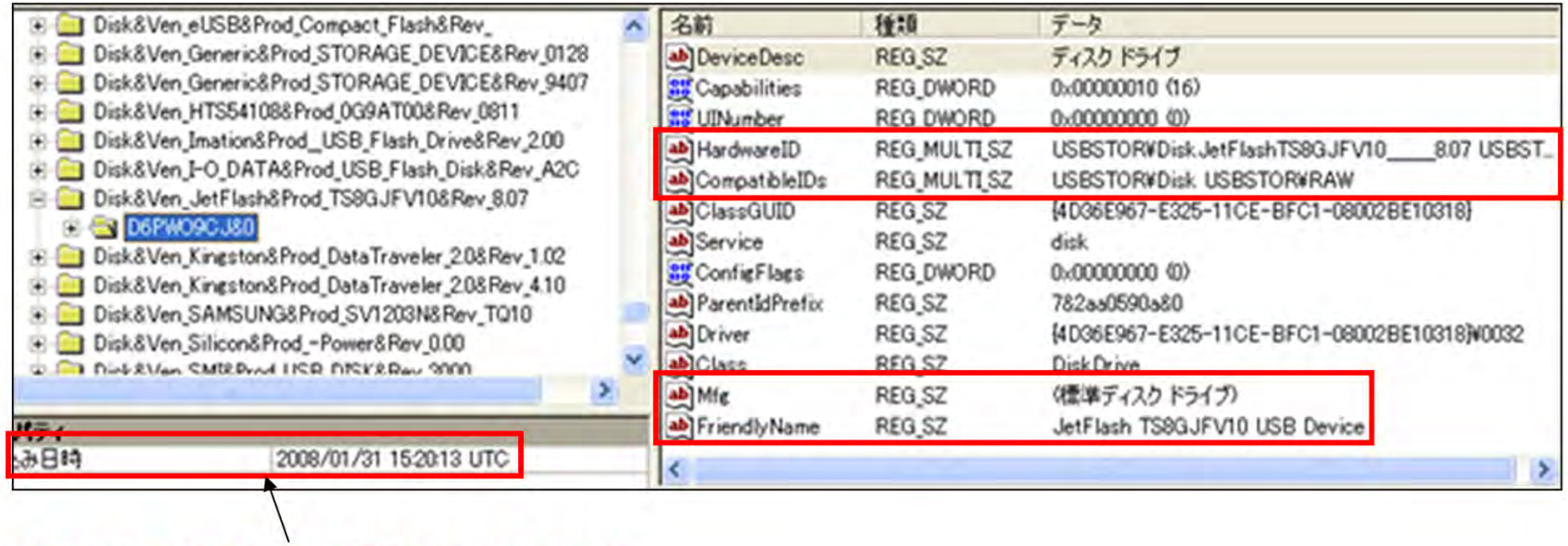
メタ情報やレジストリ情報

- メタ情報
  - Microsoft Office ドキュメントデータのプロパティ情報
  - JPEG、RAW、TIFFなどの画像ファイルのEXIF情報、メーカノート情報、サムネイル画像データ
  - MP3データの各種楽曲情報
  - LZH、ZIP、RARなどの圧縮ファイルに格納された元ファイル情報
- レジストリの解析
  - ユーザ環境（ハードウェア構成、ソフトウェア構成、設定）で蔵置情報に相違がある
  - キー名、ツリー構造はベンダー依存、仕様は非公開(WindowsOS、Office などの一部を除く)
  - 個人情報、履歴情報などのプライバシー情報はSIDをキーとして暗号化されている（WindowsXPの場合）
  - 日時情報は内部形式(dword値)として格納されている場合が多い

ハードウェアの接続記録(1/2)



ハードウェアの接続記録(2/2)



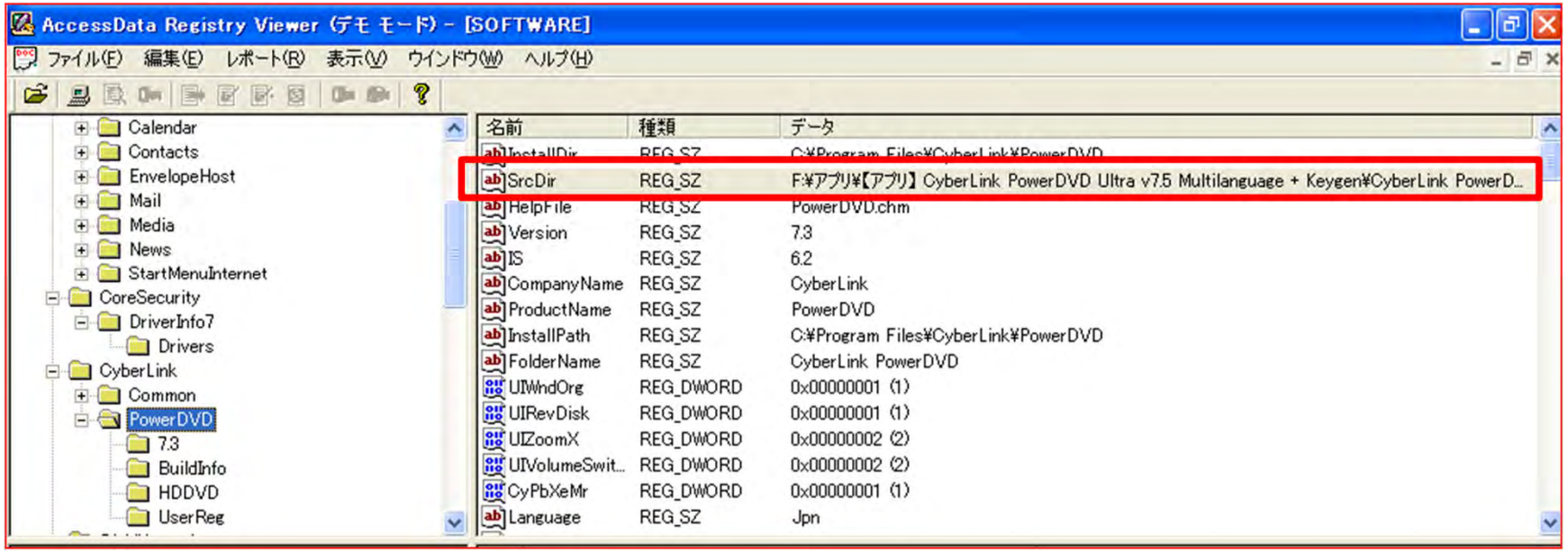
デバイスを始めて認識した日時

USBSTOR配下のUSBフラッシュメモリ情報

同一種類のUSBメモリを利用していても、シリアル番号から識別できる

フリーツールで簡単に表示可能。http://www.dit.co.jp/products/x-ways/dit-f.html

アプリケーションのインストールの痕跡



不正の抑止

常時監視

ログ取得

＋

フォレンジック解析体制

見張られている自覚

怠惰の牽制

パソコンの随時監査（解析）

↓

解析結果の開示

↓

「そんなことまで分かるんだ」

↓

曖昧な行動の自粛

退職者への牽制

退職者のパソコンのHDDを複製保全

いつでも解析できることを知らしめる

退職後の悪意ある行動の抑止

フォレンジックの効果を上げるために

- フォレンジックの限界を知る
  - 消去されたデータを全て復元できるわけではない
  - 使われたIDは特定できても、それを使った人物は分からない
- 効果をあげるためにやっておくこと
  - 補完できる記録を残す
    - ネットワークログ
    - 入退室管理
  - アクセス権管理ポリシーの整備
  - 正当な活動を裏付けするという意識