データ保全とは何か？

株式会社ラック
セキュリティプロフェッショナル本部
サイバー救急センター
高松　啓

講師プロフィール

- 高松　啓
- 経歴
  - 2006年～2008年

    官公庁にて、個人情報保護、情報セキュリティの監査、事故対応を担当
  - 2008年～2013年

    セキュリティ企業において、フォレンジック調査を担当
  - 2013年～

    （株）ラック サイバー救急センターにて、フォレンジック技術を使用した、インシデント対応を担当

【参考】

サイバー救急センター　出動件数	
2013年	307件
2014年	222件（9月末現在）

コンピュータフォレンジックとは

- **デジタルフォレンジックとは**
  https://digitalforensic.jp/home/what-df/

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。

コンピュータフォレンジックとは

現在、フォレンジック技術は様々な目的で利用されている

- 法廷での立証
- 会計監査(e-Discovery)
- インシデントレスポンス

データ保全とは

- セキュリティインシデントが発生した際に、インシデントに関わるデータの中から、電磁的証拠となり得るものを、収集、取得すること

- 保全したデータをもとに、フォレンジック調査、ログ調査を実施し被害内容（原因、影響範囲等）を明らかにする

- 保全以降、証拠として使用するデジタルデータには手が加えられていないことを証明する必要がある

データ保全の重要性

インシデント発生　⇒　現場はすでに汚染されている！

- これ以上現場を汚染してはならない。
- フォレンジック調査を行う上で<u>最も重要なパート</u>である。

- 調査すべき証拠が消失、改変されないよう、証拠を保全する。
  - 汚染される前に現場を確保
  - 訴訟も含めた対外対応を前提に、記録を取る
  - データ解析に失敗しても復旧できるようディスクをコピー

データ保全をしないと・・・

ありがちな失敗例①

- 不正侵入されていたから、とりあえず再インストール
  - 調査をしていないため、侵入原因への対策がとられないため、再度、不正侵入を受けてしまう
  - 影響範囲の調査をしていないため、該当サーバを踏み台として他のサーバに侵入しておりバックドアプログラムが仕掛けられていたことに気づかない
- 不審なファイルがあったため、削除してしまった
  - 調査の際に必要になることがあるため、隔離するほうが望ましい
- ネットワークから切り離した後、保全もせず電源オンのまま長期間放置
  - ログのローテートがかかってしまう

データ保全をしないと・・・

ありがちな失敗例②

- 再起動する
  - テンポラリファイルや揮発性の情報がとれなくなってしまう
  - ただし、現実的には行われることがあり、状況によってはしょうがないこともある
- 保全の重要性を知らないユーザが調査
  - 様々なファイルへのアクセス。最終アクセス日時の変更、ファイルの削除、削除データの上書きなど。
  - 不用意なセキュリティツールのインストール、実行
- **システムに影響を与えたり、その後の調査や解析に影響を与える操作は極力避けて、速やかに保全を実施することが望ましい**

保全すべきデータ

- **端末のディスクイメージ**
  - 社内調査を実施する前に保全することが望ましい
- **メモリイメージ**
  - マルウェア感染が疑わしい場合は、再起動、シャットダウン前にメモリイメージを収集
- **ネットワークログ**
  - プロキシログ、ファイアーウォールログ

保全すべきデータ

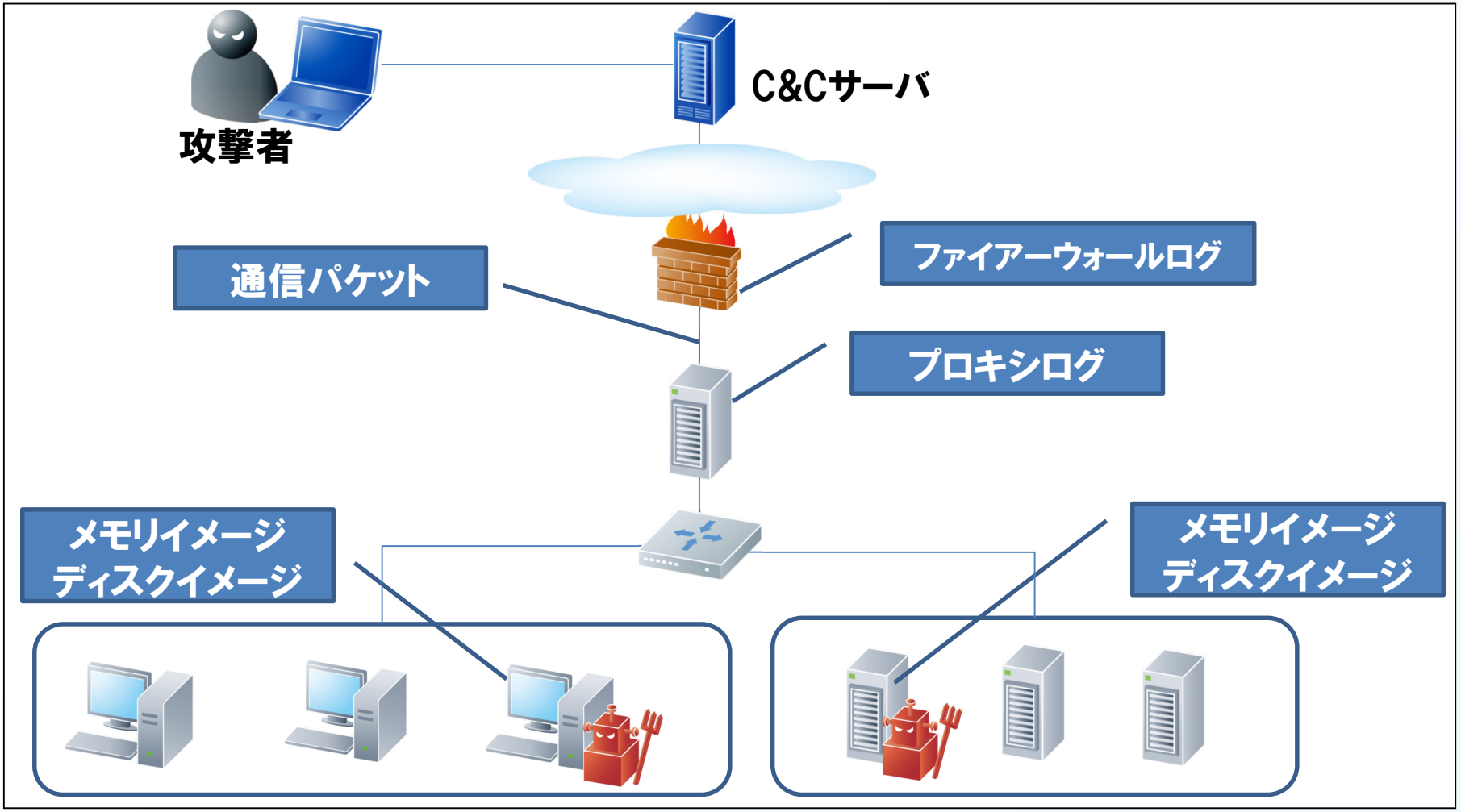
保全対象の選定

- どんなインシデントが起きたのかを把握し、保全対象を選定する
  - 何がおきたのか
  - 何がきっかけで気づいたのか
  - 現在、どうなっているのか

  etc. . .

保全すべきデータ

- ネットワーク経由での攻撃は、端末内に痕跡だけでは被害範囲の特定が困難なので、攻撃経路上の各種ログの収集が必要



保全方法

重要なポイント

- 可能な限り保全対象のデータ（原本）に変更を加えずに複製を作成すること

- 原本と複製のハッシュ値が同一であることを確認する**技術的な記録**に加えて、**プロセスの記録**が重要

保全方法

重要なポイント

- Chain of Custody(証拠管理の連鎖)
  - 電子データの取得から法廷への提出まで、完全性が保たれていることを証明するためのプロセス

- Chain of Custody項目例
  - 調査対象のディスク(原本)を直接操作しない
    - 原本を複製し、複製したディスクを調査する
    - 原本は保管する
  - 原本のハッシュ値を取得し、裁判まで保管する
  - 原本と複製は金庫に保管し、取り扱い時には「担当者」「期間」「取り扱い内容」などを記録する
  - 解析はChain of Custodyを保てる部屋で行う

保全方法

ハッシュ値

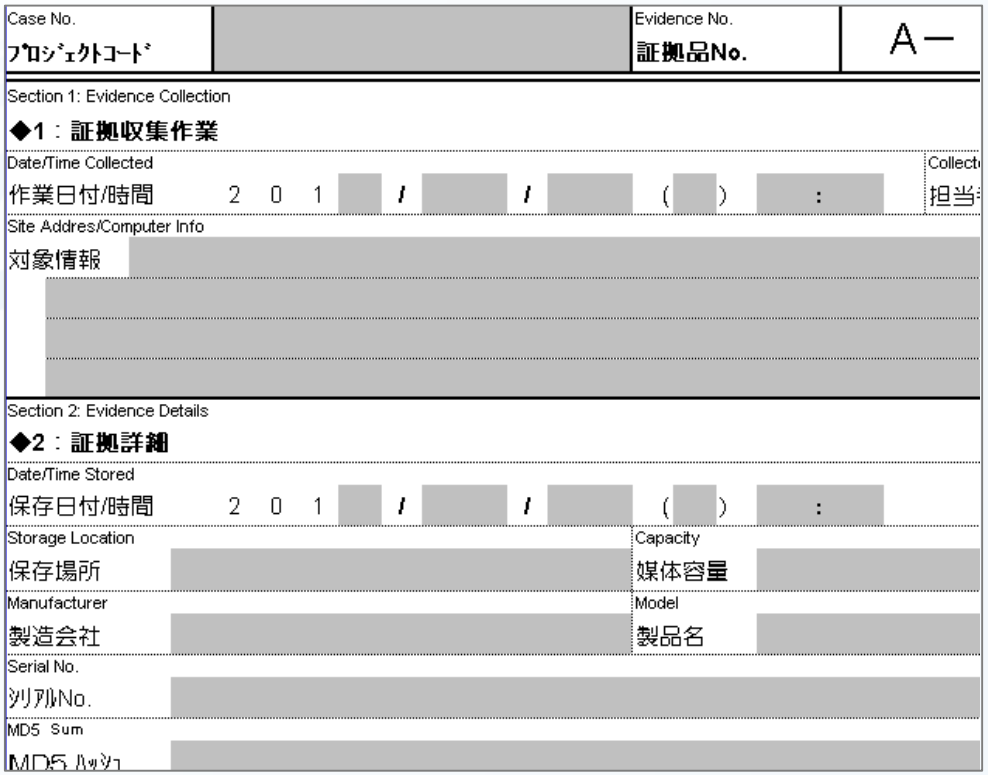
- 原本との**同一性**を保証するため、ハッシュ値を比較する
- ディスクの不良セクタにより、原本とハッシュ値が同一でないケースもある
  - 写真撮影、複数人による立会、記録(ログ)等で担保する

例）Solo3によるハッシュ値の表示

保全方法

記録

- 保全対象ディスク情報(写真撮影含む)
  - メーカー
  - 型番
  - ディスク容量、LBA
  - シリアルNo、モデルNo
- ディスクの管理番号
- 引き渡し/受領の記録
  - 提出者情報
  - 提出日付
  - 提出者署名
  - 受領者情報
  - 受領日付
  - 受領者署名

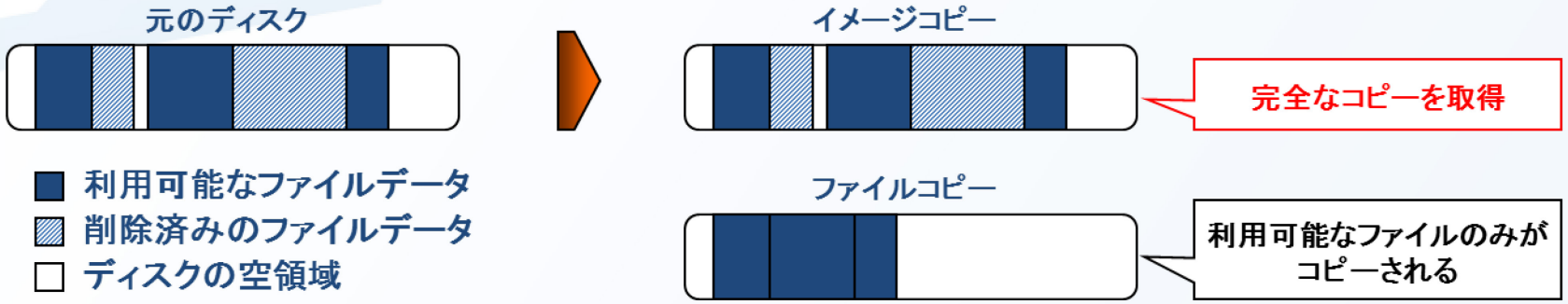


保全方法

ハードディスクのイメージコピーの取得

- ディスクのイメージコピーを取得する
- 調査は、取得したコピーに対して行い、原本（マスターディスク）は厳重に保護する

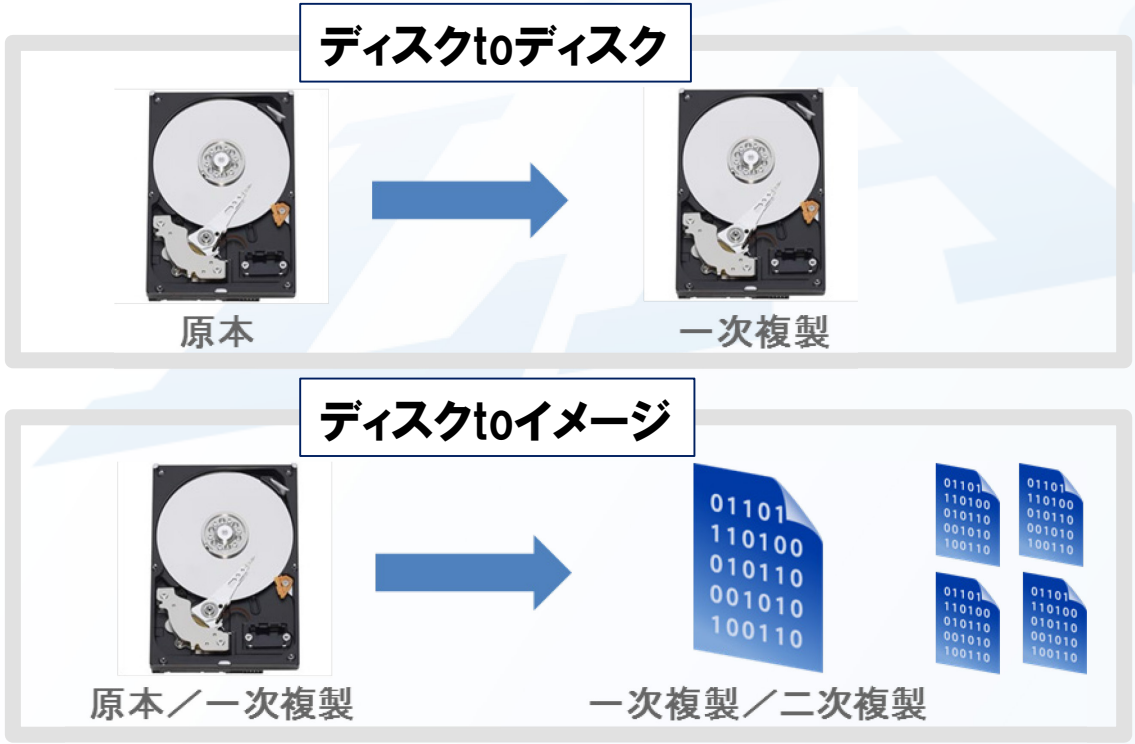
- イメージコピー
  - 調査対象とすべき、削除したデータもコピーされる
- ファイルコピー
  - 証拠がコピーされない可能性がある



保全方法

複製先の形式

- ディスクtoディスク、ディスクtoイメージ
  - 複製先のHDDのサイズは、複製元と同一またはそれより大きいものが必要
- イメージファイルで取得する場合は、分割ファイルにしたり、圧縮することも可能



保全方法

使用機材・ツールの一例

- 複製機器（デュプリケータ）
  - YEC社　Demi
  - ICS社　Image Master Solo-4
- フォレンジック用CDブートLinux
  - Deft
  - Helix
- Windows用保全ツール
  - FTK Imager
  - EnCase Imager
  - Fau-dd
- Linux用保全ツール
  - OS付属のddコマンド
  - Dcfldd

保全方法

複製機器に求められる機能①

- 書き込み防止機能
  - 原本に対し、いかなる書き込みも行うことができない
- 完全(物理)複製機能
  - 対象物全領域を複製することができる
  - 不良セクターへの対応
  - 物理的及びイメージによる複製
- 同一性検証機能
  - ハッシュ値やバイナリコンペア等による同一性検証
  - セクターサイズの表示

出典：証拠保全ガイドライン 第3版（特定非営利活動法人デジタル・フォレンジック研究会
http://www.digitalforensic.jp/eximgs/20130930gijutsu.pdf

保全方法

複製機器に求められる機能②

- 作業ログ・監査証跡情報の表示・出力機能
  - 対象物及び複製先の詳細情報
  - 作業内容及び各種設定情報
  - 作業時間等の作業結果
  - 作業者情報
  - 機器情報

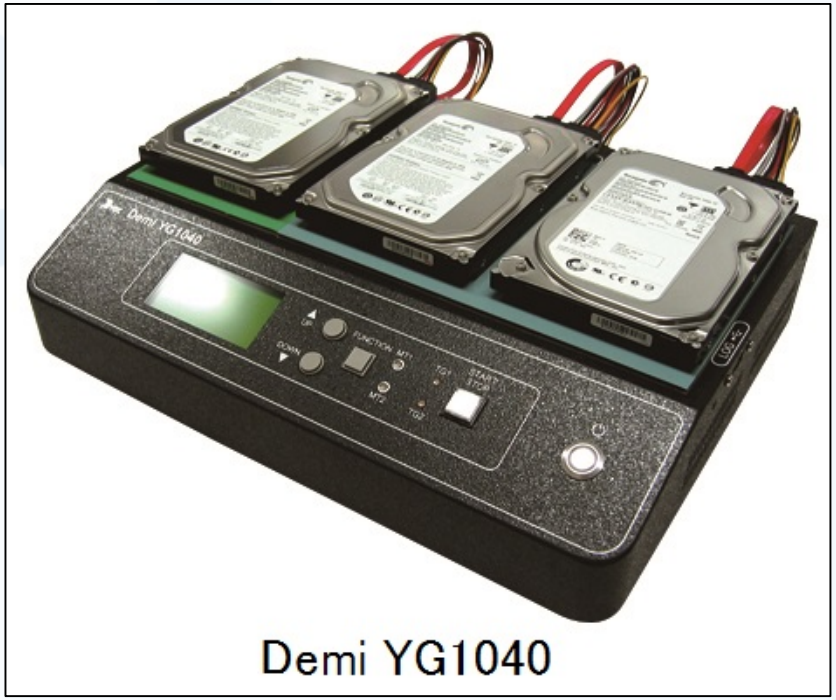
出典：証拠保全ガイドライン 第3版（特定非営利活動法人デジタル・フォレンジック研究会
http://www.digitalforensic.jp/eximgs/20130930gijutsu.pdf

保全方法

複製機器(デュプリケーター)を使用した保全

- ディスクイメージコピー取得のための専用機器であるため、様々な機能を有する

- 操作がわかりやすく、操作ミス、漏れが生じにくい



保全方法

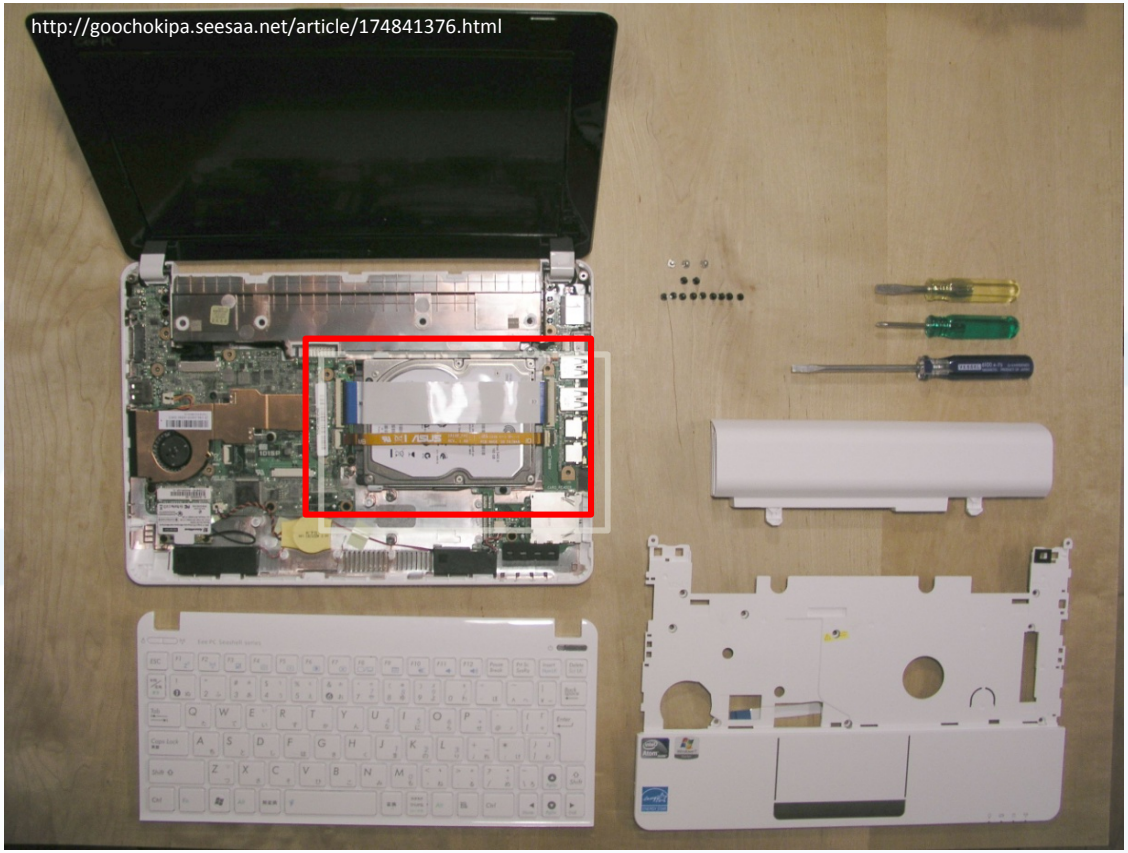
フォレンジック用CDブートOSを使用した保全

- 調査対象機器でフォレンジック用CDでフォレンジック用にカスタマイズされたOS(**ディスクに変更を加えない**)を起動して、ディスクイメージを取得する
  - Deft
  - Helix

保全方法

フォレンジック用CDブートOSで保全を行うケース①

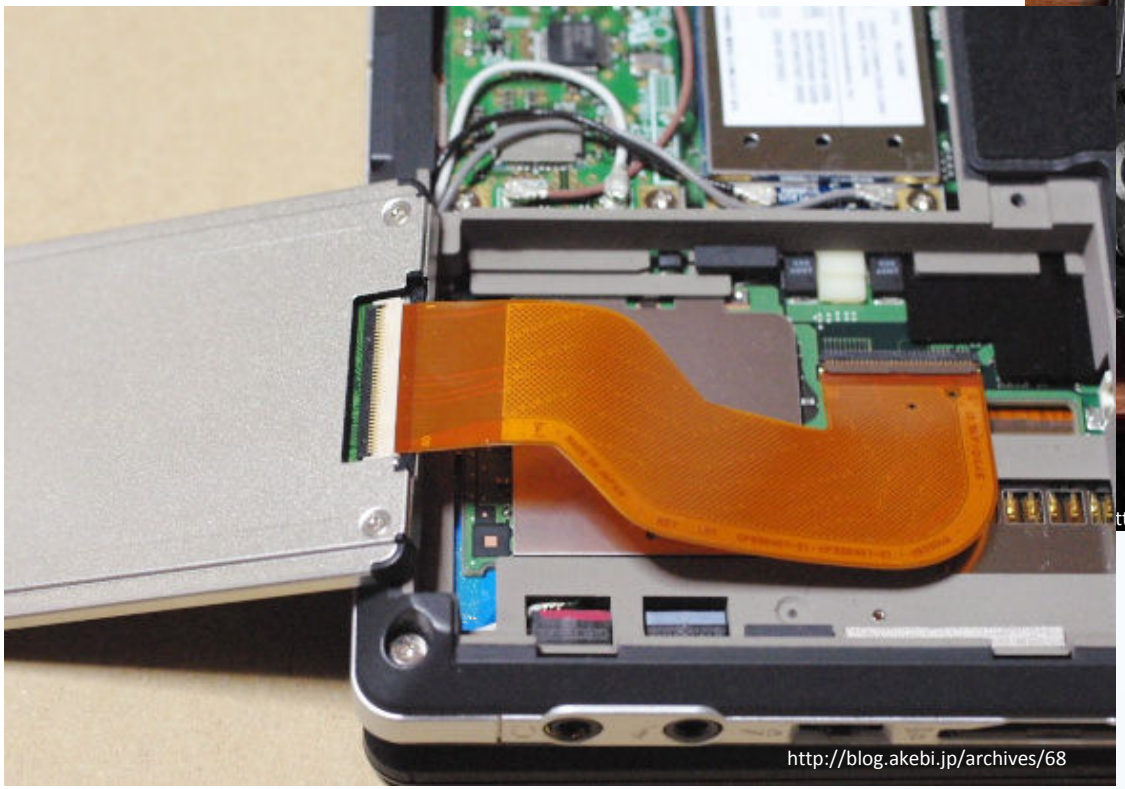
- ハードディスクの取り外しが困難



保全方法

フォレンジック用CDブートOSで保全を行うケース②

- ハードディスクのインターフェースに保全機器が未対応



保全方法

フォレンジック用CDブートOSで保全を行うケース③

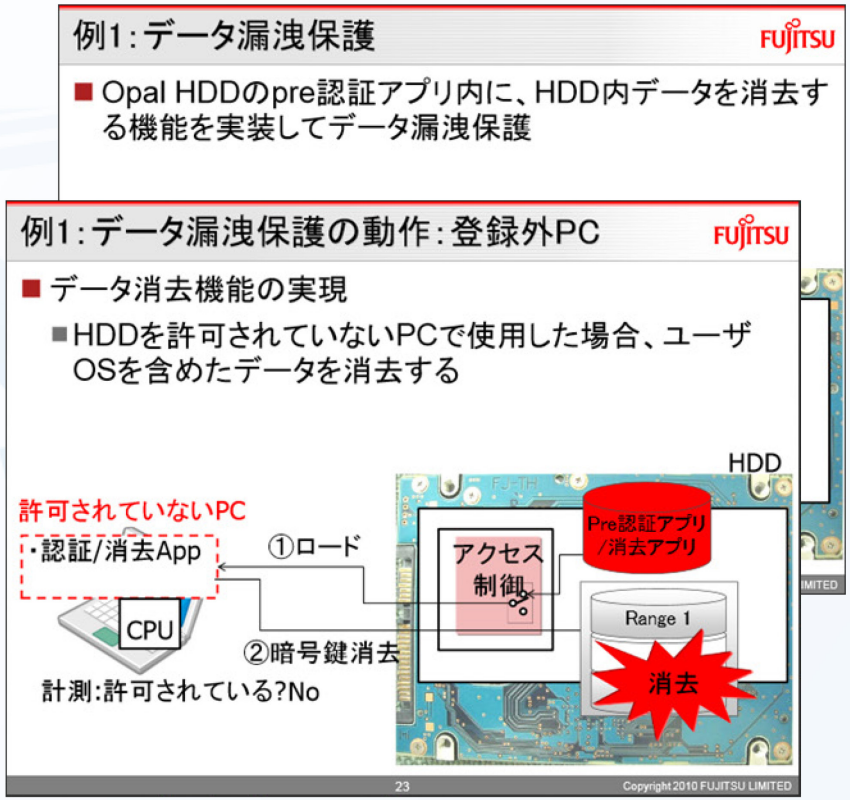
- 複数ハードディスクを使用したシステム（RAID等）

保全方法

フォレンジック用CDブートOSで保全を行うケース④

- 本体から取り外すと読めなくなるハードディスク

Wipe Technology Storage
http://www.toshiba.co.jp/about/press/2011_04/pr_j1301.htm

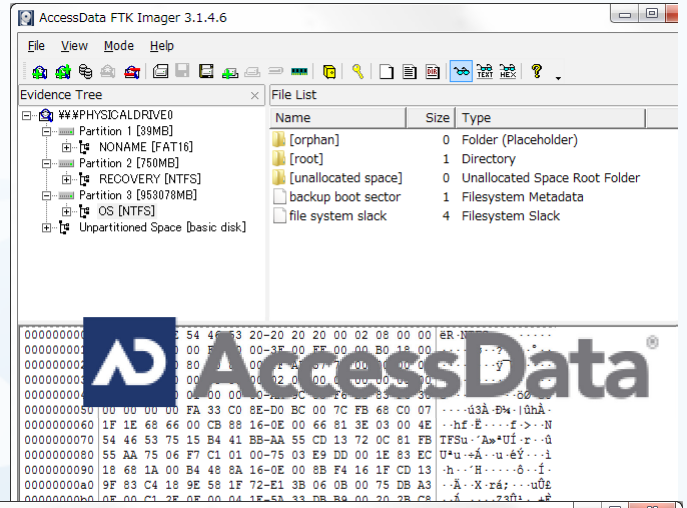


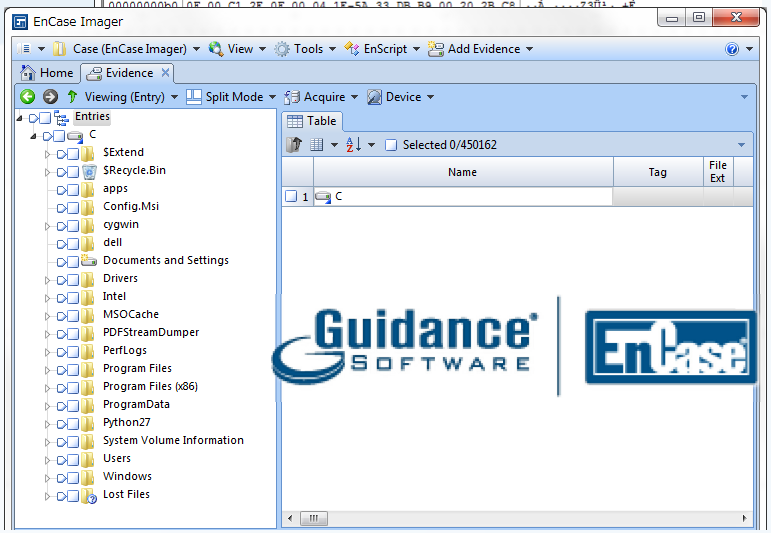
Opal HDDを用いたソリューション
http://www.trustedcomputinggroup.org/files/static_page_files/2F4CC195-1A4B-B294-D0212F9A78688DCC/[JRF WS] Nov410_OpalSolution_Fujitsu.pdf

保全方法

Windows用保全ツール

- フォレンジックソフト開発会社等が無償で公開しているツール
  - EnCase Imager
    GUIで操作できる保全用ツール
    開発元：Guidance Software
  - FTK Imager
    GUIで操作できる保全用ツール
    開発元：AccessData
  - Fau (Forenisc Acquisition Utilities) -dd
    Windows用のddコマンド
    開発元：GMG Systems

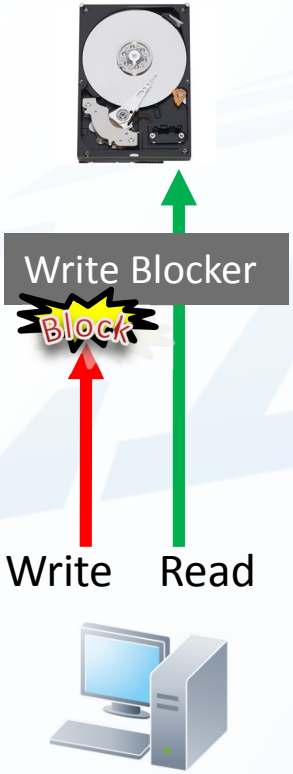




保全方法

書き込み防止装置（Write Blocker）

- 調査対象ディスクと解析PCの間に接続し、書き込みをブロックすることで意図しないデータ改変を防止する



保全方法

Linux用保全ツール

- 保全用のddコマンドや付属のddコマンド
  - dcfldd

    フォレンジック機能を備えたGNU ddの拡張版

    開発元:Defense Computer Forensics Lab
  - dc3dd

    GNU ddにフォレンジックのための機能を追加するパッチを当てたもの

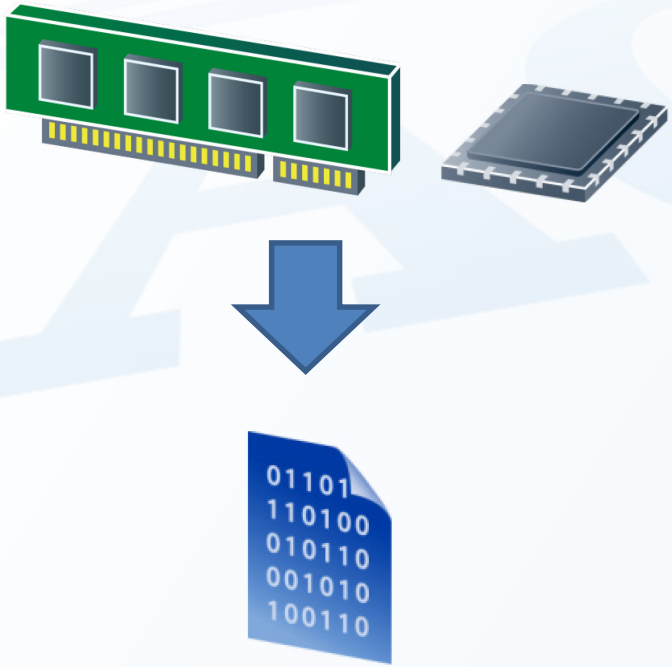
    開発元:DoD Cyber Crime Center

```
root@deft:/mnt/hozen# dcfldd split=4096M bs=512 conv=noerror,sync hash=md5 hashl
og=/mnt/hozen/test-img.md5 if=/dev/sda of=/mnt/hozen/test-img.dd
16777216 blocks (8192Mb) written.
16777216+0 records in
16777216+0 records out
root@deft:/mnt/hozen# _
```

保全方法

メモリイメージファイル

- 稼働中のコンピュータの物理メモリの内容をファイルへ物理コピー（ダンプ）する
- 取得方法により、取得時のCPUレジスタ情報も取得する



メモリイメージファイル

保全方法

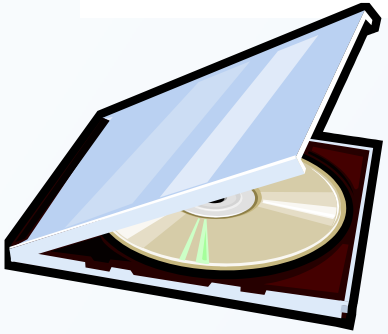
メモリイメージファイル取得ツール (Windows)

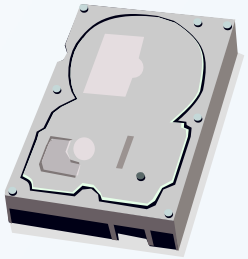
- dd
- MoonSols Windows Memory Toolkit （旧windd) /DumpIt
- FTK Imager (FTK Imager Lite)
- FastDump
- KnTDD
- winenn

保全方法

保全方法の選定

- 保全対象によって、適切な保全方法を選択する必要がある
  - 物理マシンか仮想マシンか？
  - シャットダウンできるか？
  - OSは何か？（Windows/Linux/MacOS）
  - HDDの容量？
  - 光学ドライブやUSBポートは付いているか？





データ保全のまとめ

- インシデントが発生したらまず保全！
- 保全したデータをもとに、フォレンジック調査で被害内容（原因、影響範囲等）を明らかにする
- 調査結果をもとに復旧、再発防止を行う
- 保全ではCahain of Custodyが重要
- 保全にはいろいろな方法があるので、適切な方法を選ぶ

- インシデントはいつ発生するかわかりません！
  自社内で保全が出来る体制の構築を是非検討してください

LAC
安心とともに

Thank you. Any Questions ?

LAC 安心とともに
株式会社ラック
〒102-0093 東京都千代田区平河町2-16-1
平河町森タワー
Tel 03-6757-0120 Fax 03-6757-0121
www.lac.co.jp