第14期　第1回　「DF人材育成」分科会

『デジタル・フォレンジックの基礎と実践』の紹介と人材育成のための今後の展開

株式会社FRONTEO
野﨑　周作

2017.05.17

FRONTEO

Agenda

FRONTEO

第14期第1回　「DF人材育成」分科会

『デジタル・フォレンジックの基礎と実践』の紹介と人材育成のための今後の展開

1. 第４章「フォレンジック作業の実際－データ収集」
2. 第６章「フォレンジック作業の実際－データ解析」（後半）
3. 第７章「スマートフォンなどのフォレンジック」
4. 第９章「フォレンジックの応用」（一部）

1. 第4章 「フォレンジック作業の実際－データ収集」

注力したポイント

- 実際のデータ収集を行う現場にて注意すべきポイントを記載。
- 最も調査対象としてのニーズが多いPCに対して、様々な状況においてのデータ収集方法を記載（HDD取り外し可否、セキュリティ有無 etc）。
- 収集用ソフトウェアの使い方やChain of Custodyシートの記載方法に関して記載。

書籍内容

- エビデンスの取り扱い
- ハードウェアによるデータ収集
- ソフトウェアブートによるデータ収集
- ソフトウェアによるデータ収集
- ファイルデータのみの収集
- モバイル端末のデータ収集
- メモリなどの揮発性情報のデータ収集
- 外部記録媒体のデータ収集
- セキュリティ設定がある場合の対処法
- Evidence InformationとChain of Custody（COC）
- 収集用ソフトウェア（FTK Imager Lite）の使用方法

2. 第6章「フォレンジック作業の実際－データ解析」（後半）

注力したポイント

- ユーザが作成するオフィスファイル、Eメール、画像ファイル等のアプリケーションファイルの調査手法に関して記載。
- ファイルの検索調査手法においては、通常のキーワード検索による調査手法の他にPredictive Codingといった人工知能応用技術を使用した最新の調査手法も記載。
- データ解析ソフトウェアの使用方法も記載し実際に使ってみて理解を深めることが可能。

書籍内容

- ユーザファイルの解析
  - 文字コード
  - キーワード検索
  - 類似ファイルの検索
  - Predictive Coding（プレディクティブコーディング）
  - ファイルヘッダー
  - メタデータ
  - 画像ファイルの調査
  - Eメールの調査
  - インターネットアクセス履歴の調査
- データ解析ソフトウェア（Autopsy）の使用方法

3. 第7章「スマートフォンなどのフォレンジック」

注力したポイント

- モバイルフォレンジックの必要性と課題、関連するデータの格納先に関して記載。
- モバイル端末からのデータ収集時における注意点やロジカルデータ収集と物理データ収集の違いについて記載。
- iOS端末、Android端末について最低限押さえておくべきポイントについて記載。

書籍内容

- モバイル・フォレンジックの必要性と課題
  - なぜモバイル・フォレンジックが必要か
  - モバイル・フォレンジックの課題
  - モバイル端末に関連するデータの格納先
- モバイル端末のデータ収集
  - モバイル端末収集時の注意点
  - ロジカルデータ収集
  - 物理データ収集
- iOS端末におけるフォレンジック
- Android端末におけるフォレンジック
- SQLite解析

4. 第9章「フォレンジックの応用」（一部）

注力したポイント

- EDRM（Electronic Discovery Reference Model）のフローに従い、各工程で必要とされるデジタル・フォレンジック技術を記載。
- eディスカバリにおいてデータの特定、保全（訴訟ホールド）から最終的に開示を行う提出データの作成に至るまでデジタル・フォレンジック技術者だけでなく企業の法務・知財担当者にとっても理解できるような内容として記載。

書籍内容

- 訴訟に対応するためのeディスカバリにおける事例
  - 情報ガバナンス（Information Governance）
  - データの特定（Identification）
  - データの保全（Preservation）
  - データの収集（Collection）
  - データの処理（Processing）
  - データの分析（Analysis）
  - データのレビュー（Review）
  - 提出データの作成（Production）

  参照URL：http://www.edrm.net/

この資料は下記により作成されました。

株式会社FRONTEO

108-0075 東京都港区港南2-12-23 明産高浜ビル

TEL : 03-5463-7577　FAX : 03-5463-7578

東証マザーズ上場 | Nasdaq（ナスダック）上場