デジタル・フォレンジック教育の動向と東京電機大学大学院での試行

東京電機大学教授
佐々木　良一
sasaki@im.dendai.ac.jp

目次

1. デジタル・フォレンジック（DF）人材育成の必要性
2. 東京電機大学におけるDF教育の位置づけ
3. 海外の大学におけるDF教育の動向
4. 東京電機大学におけるDF教育のカリキュラム
5. 東京電機大学におけるDF教育の実際と評価
6. 今後の展開

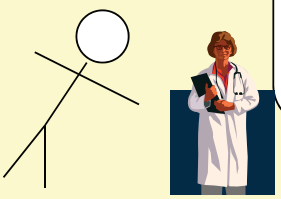
アンケートを実施した東京電機大学生の澤邉　直幸氏ならびに、講義を実施していただいた先生方に厚く御礼申し上げます

デジタル・フォレンジックのイメージ

Forensicというのは「法の」とか「法廷の」という意味を持つ形容詞や、「捜査や法廷で役に立つもの」の意味を持つ名詞（通常Forensics）

Forensic Medicine:「法医学」
捜査や裁判に必要な情報を医学知識を利用して明らかにする技術や学問

殺人事件



Digital Forensics:
「デジタル・フォレンジック」
捜査や裁判に必要な情報を、情報処理技術を用いて明らかにする技術や学問

不正侵入

DFで使う作業と技術の分類

事前準備

1. ログ等の収集

関連技術

① 収集すべきログを選択する技術
② ログ不正消去検知・防止技術

インシデント時

2. PC等の確保
3. 証拠保全
4. 調査・解析
5. 報告書の作成

① 削除されたファイルや物理的に破壊された媒体を復元する技術
② 暗号化されたファイルの復号技術
③ 調査者に不正がないことの心証形成技術

① 得られた大量のデータから有用なデータを抽出する技術（機械学習など）
② 得られたデータから証拠となるものを抽出する技術

通常、専門家が実施

DF関連用語

＜フォレンジックの対象による分類＞

① コンピュータフォレンジック
　主にコンピュータのディスクよりの証拠を扱うもの
② ネットワークフォレンジック
　主にパケットデータやアクセスログを証拠として扱うもの
③ メモリーフォレンジック
　PCなどの揮発性メモリー上のデータを証拠として扱うもの
④ スマートフォンフォレンジック
　スマートフォンのデータを証拠として扱うもの
⑤ SCADAフォレンジック：産業用制御装置上のデータを証拠として扱うもの
⑥ クラウドフォレンジック：クラウド上のデータを証拠として扱うもの



SCADA
（Supervisory Control And Data Acquisition）

デジタル・フォレンジック教育の必要性

捜査や裁判に必要な情報（たとえばサーバへの侵入経路など）を、情報処理技術を用いて明らかにする技術や学問であるデジタル・フォレンジックは、重要性が非常に高まっている。（NISCの16の重要技術開発分野の1つ）

①高レベルのデジタル・フォレンジック技術者や研究者が不足
②デジタル・フォレンジック知識のある技術者が不足

しかし日本の大学ではデジタルフォレンジック教育が本格的にはどこでも行われておらず、民間における教育も不十分

目次

1. デジタル・フォレンジック（DF）人材育成の必要性
2. 東京電機大学におけるDF教育の位置づけ
3. 海外の大学におけるDF教育の動向
4. 東京電機大学におけるDF教育のカリキュラム
5. 東京電機大学におけるDF教育の実際と評価
6. 今後の展開

背景

- 文科省「高度人材養成のための社会人学び直し大学院プログラム（Cysec）」の１つで「国際化サイバーセキュリティ学特別コース」として認可（２０１５年スタート）

CySec

東京電機大学が社会人向けに開講する履修証明プログラム

国際化サイバーセキュリティ学特別コース

（文部科学省　高度人材養成のための社会人学び直しプログラム　選定）

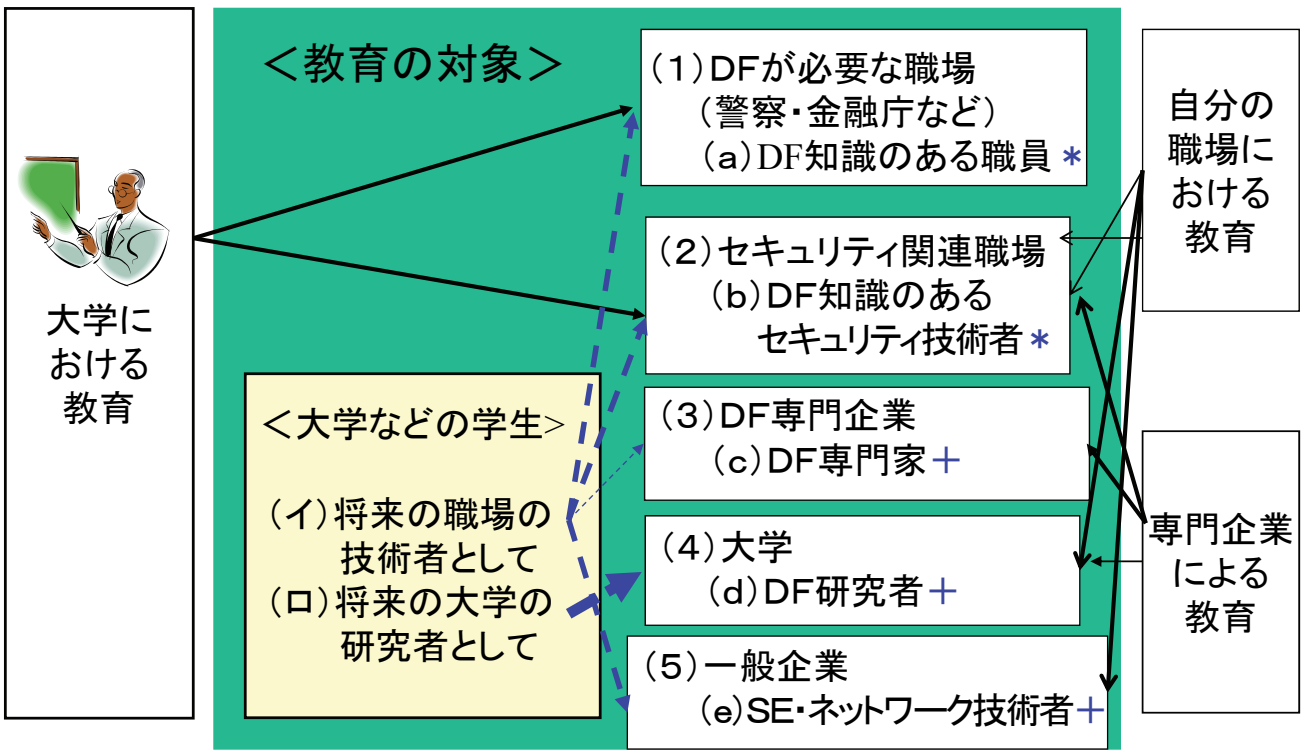
東京電機大学大学院における新たなセキュリティ教育

デジタル・フォレンジックは6つの科目の1つ。
対象は社会人20名、大学院生20名程度。

（1）サイバーセキュリティ基盤
（2）サイバーディフェンス実践演習
（3）セキュリティインテリジェンスと心理・倫理・法
（4）デジタル・フォレンジック
（5）情報セキュリティマネジメントとガバナンス
（6）セキュアシステム設計・開発

https://cysec.dendai.ac.jp/

大学および企業におけるDF教育



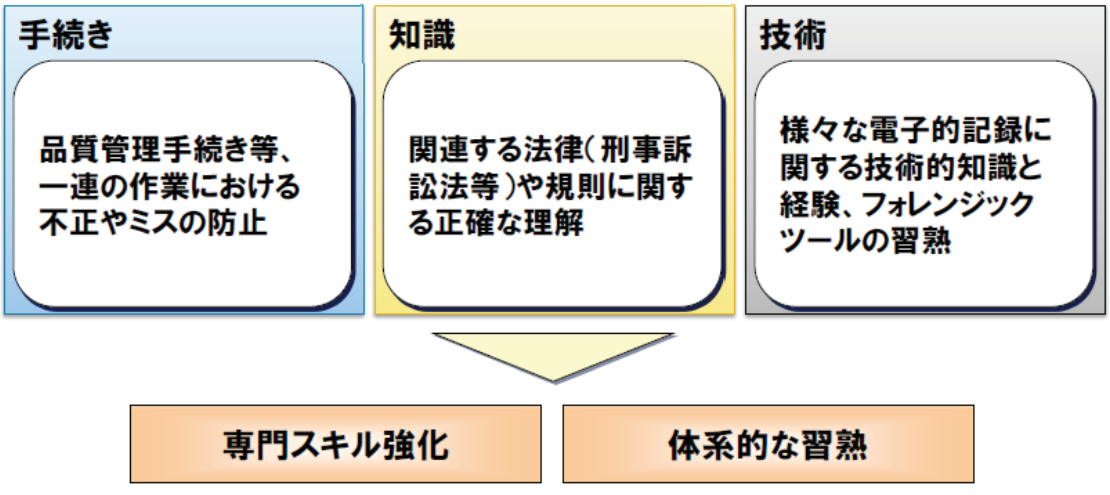
＊初級から中級　＋中級から上級

目次

1. デジタル・フォレンジック（DF）人材育成の必要性
2. 東京電機大学におけるDF教育の位置づけ
3. 海外の大学におけるDF教育の動向
4. 東京電機大学におけるDF教育のカリキュラム
5. 東京電機大学におけるDF教育の実際と評価
6. 今後の展開

学問領域が広い

- デジタル・フォレンジックは、幅広い知識や経験、専門スキルが求められる
  - 個別的な専門スキルを強化しつつ、体系的な習熟が必要



出典：デジタル・フォレンジック認定資格、認証基盤等の調査研究報告の概要
一般財団法人　保安通信協会

世界中にカリキュラムとしての基準が存在しない

米国の先進大学のカリキュラムを参考に、検討を行うしかない。

（1）Purdue大学

（2）Dakota 州立大学

（3）Champlain大学　など

Purdue大学のカリキュラム

- Purdue大学のモデルコース
  - 各大学のデジタル・フォレンジックの専攻の調査と比較から提案されたコース

必修科目	選択科目
デジタル・フォレンジック入門	ネットワークフォレンジック
応用デジタル・フォレンジック	モバイルデジタル・フォレンジック
デジタル・フォレンジックでの調査	ファイルシステムフォレンジック
デジタル・フォレンジックのキャプストーンコース	アンチフォレンジック
理論と演習	インシデントレスポンス
	デジタル法
	マルウェアフォレンジック

Dakota州立大学のカリキュラム

- カリキュラムに必要だとしている項目
  - デジタル・フォレンジックの基礎
  - コンピュータフォレンジックの応用
  - ネットワークフォレンジック
  - モバイルデジタル・フォレンジック
  - 実践的なデジタル・フォレンジック演習
  - 法廷経験

Champlain Collegeのカリキュラム

Master of Science in Digital Investigation Management

MBA 500: Integrated and Reflective Practice
DIM 500: The Practice of Digital Investigations
MBA 525: Process Improvement and Operations
MIT 505: Project Management
MIT 525: Financial Decision Making for Management
MIT 530: IT Security and Strategy
MIT 550: Reflective Leadership and Planned Change
DIM 530: Legal Aspects of Digital Investigations
DIM 540: Current Topics in Digital Investigation Techniques
DIM 550: Laboratory Operation and Accreditation
DIM 560: Digital Investigation for Civil Litigation
DIM 570: Research Methodology

http://docs.lib.purdue.edu/dissertations/より

目次

1. デジタル・フォレンジック（DF）人材育成の必要性
2. 東京電機大学におけるDF教育の位置づけ
3. 海外の大学におけるDF教育の動向
4. 東京電機大学におけるDF教育のカリキュラム
5. 東京電機大学におけるDF教育の実際と評価
6. 今後の展開

デジタル・フォレンジック教育総合カリキュラム

将来の講義候補

「デジタル・フォレンジック各論」
（講義主体:企業、大学）
・DFツール
・スマホ・家電DF
・DFと技術
（日本語処理、暗号 他）

「ネットワークフォレンジック」
（講義主体:大学、企業）
・パケットログ管理
・SIEM
・自動診断　他

「応用デジタル・フォレンジック」
（講義主体：企業、大学）
・e－Discovery
・企業／捜査機関のDF
・法とDF／法廷対応　他

最初の講義

東京電機大学大学院2015年度講義
「デジタル・フォレンジック（概論）」
2015年度9月 - 2016年1月　金曜日（18:10 - 19:40）

ベースとなる基礎知識

コンピュータアーキテクチャー　プログラミング
ネットワークアーキテクチャー　セキュリティ技術一般
法律の基礎　訴訟法の基礎

事前アンケート調査結果

- アンケート①:
  第38回 ISSスクエア水平ワークショップ
  - 『デジタル・フォレンジックの新たな動き』
    - 情報セキュリティ大学院大学
    - 2014年10月に実施
- アンケート②:
  省庁の関係者に対してのアンケート
    - 2014年11月に実施

デジタル・フォレンジック①

（1）デジタル・フォレンジック入門（電大　佐々木）
（2）ハードディスクの構造、ファイルシステム（立命館　上原）
（3）フォレンジックのためのOS、Windows（立命館　上原）
（4）フォレンジック作業の基礎（UBIC　野﨑）
（5）フォレンジック作業・データ保全（UBIC　野﨑）
（6）フォレンジック作業・データ復元（トーマツ　白濱）
（7）フォレンジック作業・データ解析1（トーマツ　白濱）
（8）法リテラシーと法廷対応（弁護士　櫻庭）
（9）フォレンジック作業・データ解析2（UBIC　野﨑）
　　＝＞ここでこれまでの講義についてアンケート

デジタル・フォレンジック②

(10)上記の演習(トーマツ　白濱、UBIC　野崎)
(11)ネットワークフォレンジック(攻撃法、マルウェア、ログの取り方)
(電大　八槇)
(12)上記の演習(電大　八槇)
(13)代表的な対象におけるDFの方法1　情報漏えい
(トーマツ　白濱)
(14)代表的な対象におけるDFの方法2
不正会計、e-Discovery　(UBIC　野崎)
(15)デジタル・フォレンジックの今後の展開
学力考査(電大　佐々木)

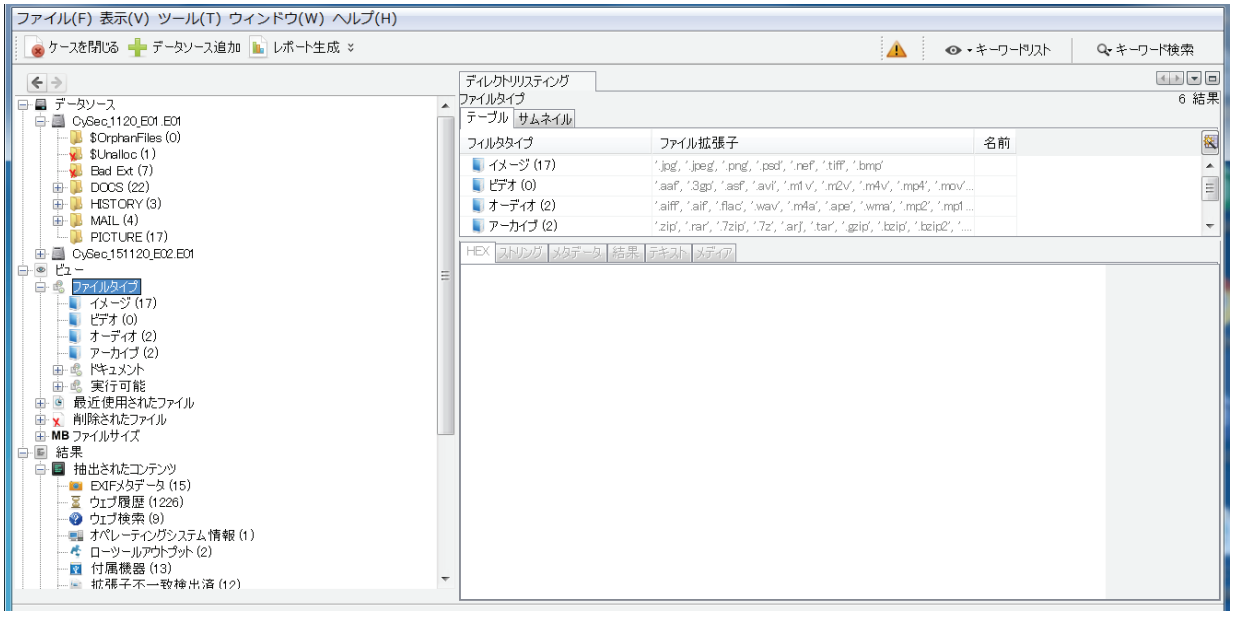
目次

1. デジタル・フォレンジック(DF)人材育成の必要性
2. 東京電機大学におけるDF教育の位置づけ
3. 海外の大学におけるDF教育の動向
4. 東京電機大学におけるDF教育のカリキュラム
5. 東京電機大学におけるDF教育の実際と評価
6. 今後の展開

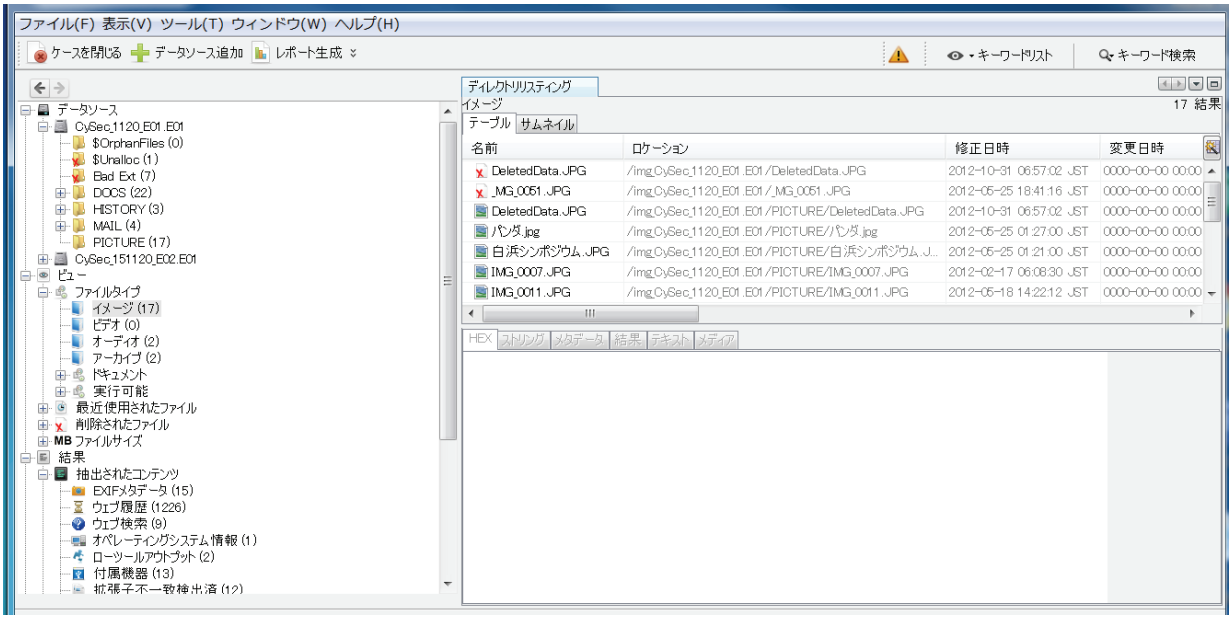
実施結果

- 現在の受講者数は54名（社会人38名、学生16名）
- セキュリティ専門企業の人やユーザ企業のセキュリティ対策を実施する人等が多い
- 金融庁、防衛省、警察等からの参加者もいる

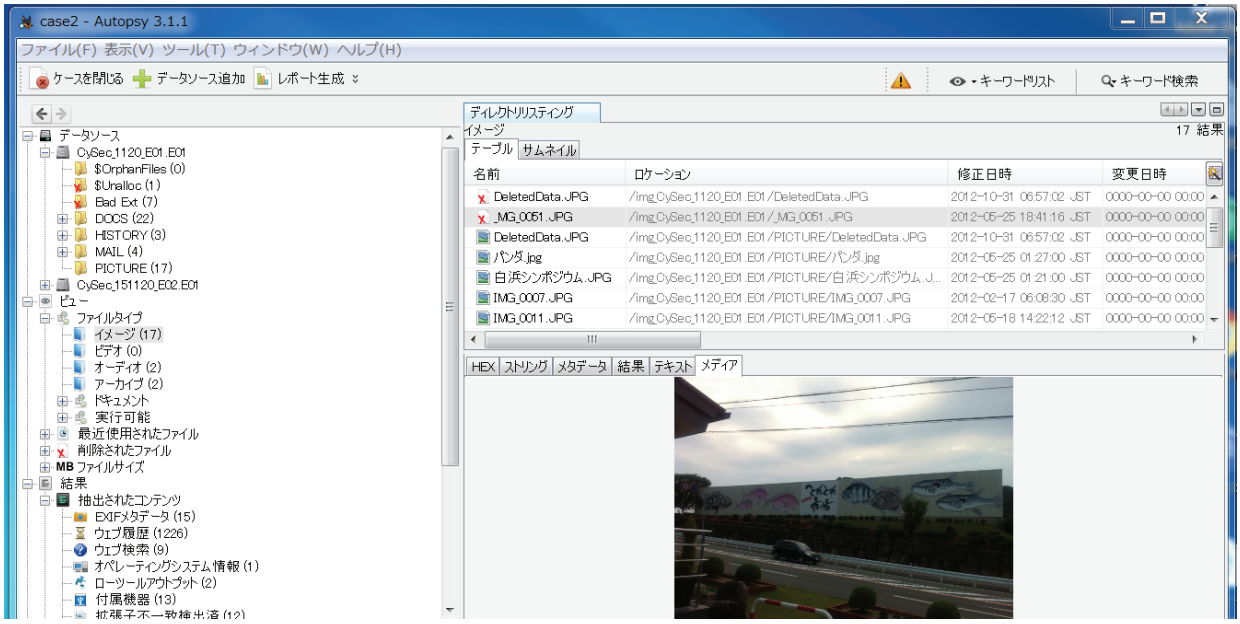
演習に用いたAutopsyの画面（1）



演習に用いたAutopsyの画面（2）



演習に用いたAutopsyの画面（3）



中間段階でのアンケート

- 実施日：2015年11月13日（金）
  ＜第9回終了時点＞

- 実施対象：受講者
  社会人：29人
  学生：18人

アンケート結果

質問項目	社会人の点数（5点満点）	学生の点数（5点満点）
興味と関心が高まりましたか	4．52	3．83
将来の仕事に役に立つと思いますか	4．38	3．94
最先端の専門知識を身につけることができましたか	4．34	4．17
総合的に見て満足できるものでしたか	4．59	4．00
この講義はあなたにとって難しすぎるものでしたか	2．85	3．29

一般に満足度は高い講義となっている
特に社会人の満足度は高い
社会人にはややややさしく、学生にはやや難しい

良かった点に関する主なコメント

- 最先端の技術や内容を講義で学ぶことができてうれしい
- 模擬裁判は臨場感がありとてもよかった
- 業界トップの講師の方々。とてもわかりやすかった
- コンピュータサイエンスの基本から教えていただけるのでわかりやすい
- CySecの中で最も秩序だった構成である　等

その他のコメント

- 資料を当日アップするのは予習できないのでやめてほしい（多数の意見）
- もう少し具体的にどういうケースに適用するかが分かるとよい
- 実際にツールを使うところがもっと見られるとよい

  ＝＞演習の中でやるが、講義の中でもやれるよう今後検討したい
- 懇親会をやってほしい

目次

1. デジタル・フォレンジック（DF）人材育成の必要性
2. 東京電機大学におけるDF教育の位置づけ
3. 海外の大学におけるDF教育の動向
4. 東京電機大学におけるDF教育のカリキュラム
5. 東京電機大学におけるDF教育の実際と評価
6. 今後の展開

まとめと今後

1. 日本ではまだほとんど行われていないデジタル・フォレンジックの講義の企画を行い2015年度に実施
2. 一般に満足度は高い講義となっており、特に社会人の満足度は高い。社会人にはややややさしく、学生にはやや難しいというアンケート結果になっているが、難易度について大きな問題はなさそう
3. 演習への期待が大きい
4. 今年の反省を2016年度のカリキュラムに反映
5. 教科書「デジタル・フォレンジックの基礎と実践」電大出版を執筆中
6. 他大学への展開や、専門教育を行っている業者などとリンクした企業向け教育の在り方の検討

2016年度講義の主な変更点

2016年度も、社会人が38人が応募、34人が入学

1. 演習を2回から3回に増加
2. スマートフォンのフォレンジックの追加
3. 演習は学生が手を動かして確認ができるようにする
4. 講義の中でも、コンピュータが動いている状況をできるだけ見せるようにする

2016年度カリキュラム

第1回　デジタル・フォレンジック入門
第2回　ハードディスクの構造・ファイルシステム
第3回　フォレンジックのためのOS（Windows）概論
第4回　フォレンジック作業　データ保全
第5回　フォレンジック作業　データ復元
第6回　フォレンジック保全・復元作業　演習
第7回　フォレンジック作業　データ解析①
第8回　フォレンジック作業　データ解析②
第9回　フォレンジック解析作業　演習
第10回　スマートフォン等のフォレンジック
第11回　ネットワークフォレンジック
第12回　ネットワークフォレンジック演習
第13回　代表的な対象におけるDFの方法
第14回　法リテラシーと法廷対応
第15回　デジタル・フォレンジックの今後の展開/学力考査

佐々木　良一（編著）「デジタル・フォレンジックの基礎と実践」(電大出版)

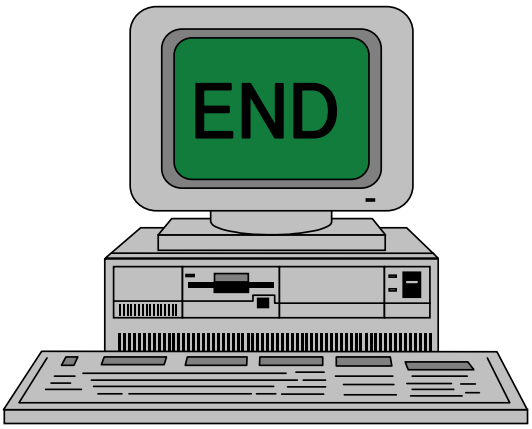
1．想定読者と要件
（1）CySecのDFの受講者＝＞講義の教科書として使える
（2）DFツールを使えるようになりたい人＝＞金融庁や公正取引委員会などでユーザとしてDFを使いたい人、セキュリティ技術者でDFも取り込みたい人、民間企業や警察で将来DFの専門家になりたい人＝＞PCやサーバのフォレンジックツールが使えるようになり、ベースとなる仕組みが理解できること。どのような利用分野があり、今後重要となる対象や技術に何があるか理解できるようになること。

2．コメント
（1）教科書として使えること（各章約20ページ（MAX25ページ。合計300ページ弱）、A5版、1ページ36字x28行＝1008文字）
（2）値段は2000円台
（3）bitやByteの理解，ネットワークの基礎はある読者を前提とする

3．スケジュール：　2016年9月までに出版

佐々木　良一（編著）「デジタルフォレンジックの基礎と実践」(電大出版)

まえがき　佐々木　2ページ
第1章　デジタル・フォレンジック入門（電大　佐々木）20ページ
第2章　ハードディスクの構造とファイルシステム（立命館　上原）20ページ
第3章　フォレンジックのためのOS（立命館　上原）20ページ
（第2－3章はもう少し初学者も意識して）
第4章　フォレンジック作業の実際・データ保全（UBIC　野崎）20ページ
第5章　フォレンジック作業の実際・データ復元（UBIC　野崎、トーマツ　白濱）20ページ
第6章　フォレンジック作業の実際・データ解析（トーマツ　白濱、UBIC　野崎）25ページ
（第4－6章は、ツールの使い方等も記述）
第7章　スマートフォンなどのフォレンジック（ UBIC　野崎）15ページ
第8章　ネットワークフォレンジック（電大　八槇）25ページ
（含む：パケットログの具体的収集方法と解析方法）
第9章　フォレンジックの応用　（トーマツ　白濱、UBIC　野崎、山本）25ページ
第10章　法リテラシーと法廷対応（弁護士　櫻庭） 25ページ
第11章　デジタル・フォレンジックの今後の展開　（電大　佐々木）15ページ



付録

米国の大学院におけるDF教育

School	Program	Location
Carnegie Mellon University	Master of Science in Information Networking with a concentration in Computer Forensics and Incident Response	Pittsburgh, PA
Champlain College	Master of Science in Digital Investigation Management	Burlington, VT
George Washington University	Master of Forensic Sciences with a concentration in high technology crime investigation	Washington, DC
John Jay College of Criminal Justice	Master of Science in Forensic Computing	New York, NY
Purdue University	Master of Science in Cyber Forensics	West Lafayette, IN
Sam Houston State University	Master of Science in Digital Forensics	Huntsville, TX
Stevenson University	Master of Science in Forensic Studies with an Information Technology track	Stevenson, MD
Texas State University	Master of Science with a Minor in Forensic Systems	San Marcos, TX
University of Central Florida	Master of Science in Digital Forensics	Orlando, FL
University of New Haven	Master's in Criminal Justice with a concentration in Forensic Computer Investigation	West Haven, CT
University of Rhode Island	Master's Degree in Computer Science with a Digital Forensics track	Kingston, RI
University of Eastern Michigan	Master of Science in Technology Studies with a concentration in Digital Investigations	Ypsilanti, MI

http://docs.lib.purdue.edu/dissertations/より
The Development of a Standard Digital Forensics Master's Curriculum
Kathleen Strzempka
Kathleen A. Strzempka, kstrzemp@purdue.edu

George Washington University

コース: Master of Forensics Sciences with a concentration in high technology crime investigation

FORS 259: Computer-Related Law
FORS 265: Ethics and Leadership
FORS 277: Computer Forensic I - Investigation and Evidence Gathering
FORS 279: Intrusion I - Understanding and Identifying Network-Based Attacks
FORS 285: High Technology Crime Investigation Capstone Course
FORS 274: Video Forensic Analysis
FORS 278: Computer Forensics II - Evidence and Analysis
FORS 280: Intrusion II - Investigating Network-based Attacks
FORS 283: Steganography and Electronic Watermarking
FORS 290: Selected Topics
FORS 295: Research
FORS 298: Forensic Sciences Practicum

http://docs.lib.purdue.edu/dissertations/より

Purdue大学のカリキュラム

- The Development of a Standard Digital Forensics Master's Curriculum（※）
  - Purdue大学のモデルコース

Kathleen Strzempka　Marcus Rogers (2010)
引用元:
http://docs.lib.purdue.edu/dissertations/AAI1479951/

Dakota州立大学のカリキュラム

- On the Development of Digital Forensics Curriculum（※）

※（Manghui Tu* , Kyle Cronin, Dianxiang Xu
College of Business and Information Systems Dakota State University USA
Samsuddin Wira Department of Public Service Malaysia
June 2011
引用元：
http://www.dsu.edu/research/ia/documents/%5B6%5D-On-the development-of-Digital-Forensics-Curriculum.pdf）

デジタル･フォレンジックのユーザは？

① 警察などの法執行機関
（他に政府による会計不正や独禁法違反調査など）

② 企業などの一般組織

デジタル・フォレンジックをデジタル鑑識と訳す人もいる