「DF人材育成」分科会の活動計画と東京電機大学におけるDF人材教育計画

東京電機大学教授
佐々木良一
sasaki@im.dendai.ac.jp

目次

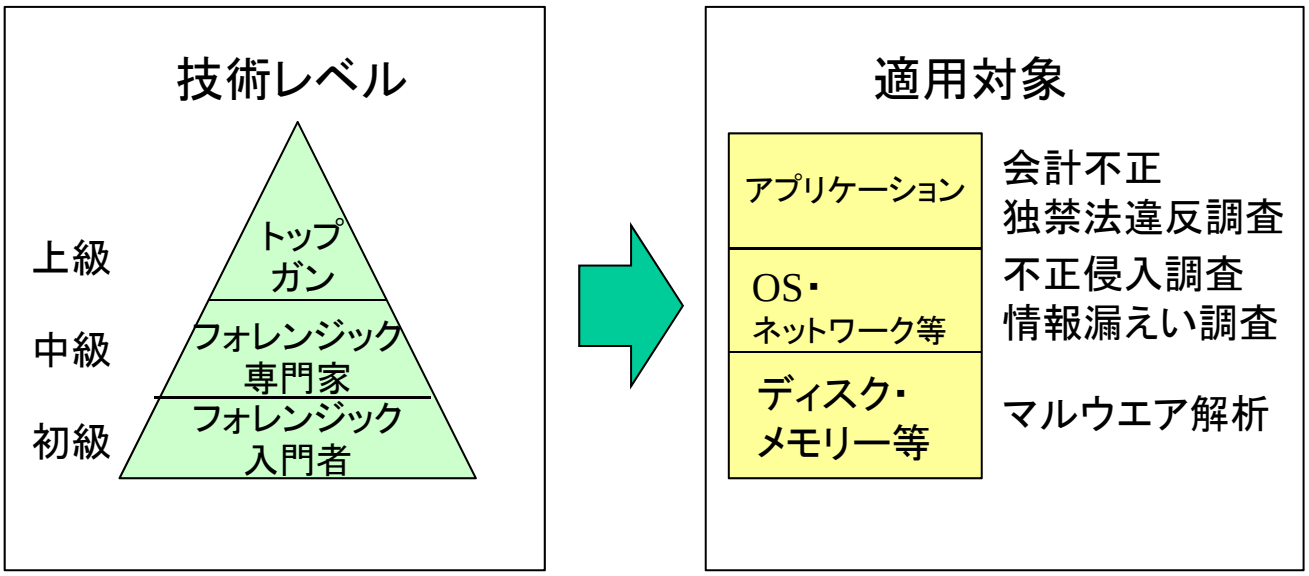
デジタル・フォレンジック教育の必要性

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

人材マップ案



DFコミュニティ2014　丸山満彦氏資料をもとに作成

デジタル・フォレンジックと利用者

＜デジタル・フォレンジックの分類＞

- 企業におけるDF
- 訴訟する側のDF
- 不正侵入に関するDF
- 企業における不正侵入以外のDF
- 訴訟される側のDF
- 法執行機関におけるDF

＜利用者＞

1. IT／IS部門の管理者
2. 企業・組織の経営者
3. 各業務の管理者
4. 監査役
5. 警察官
6. 弁護士
7. 司法当局
8. 税務当局

デジタル・フォレンジックとデータ

＜デジタル・フォレンジックの分類＞

- 企業におけるDF
- 訴訟する側のDF
- 不正侵入に関するDF
- 企業における不正侵入以外のDF
- 訴訟される側のDF
- 法執行機関におけるDF

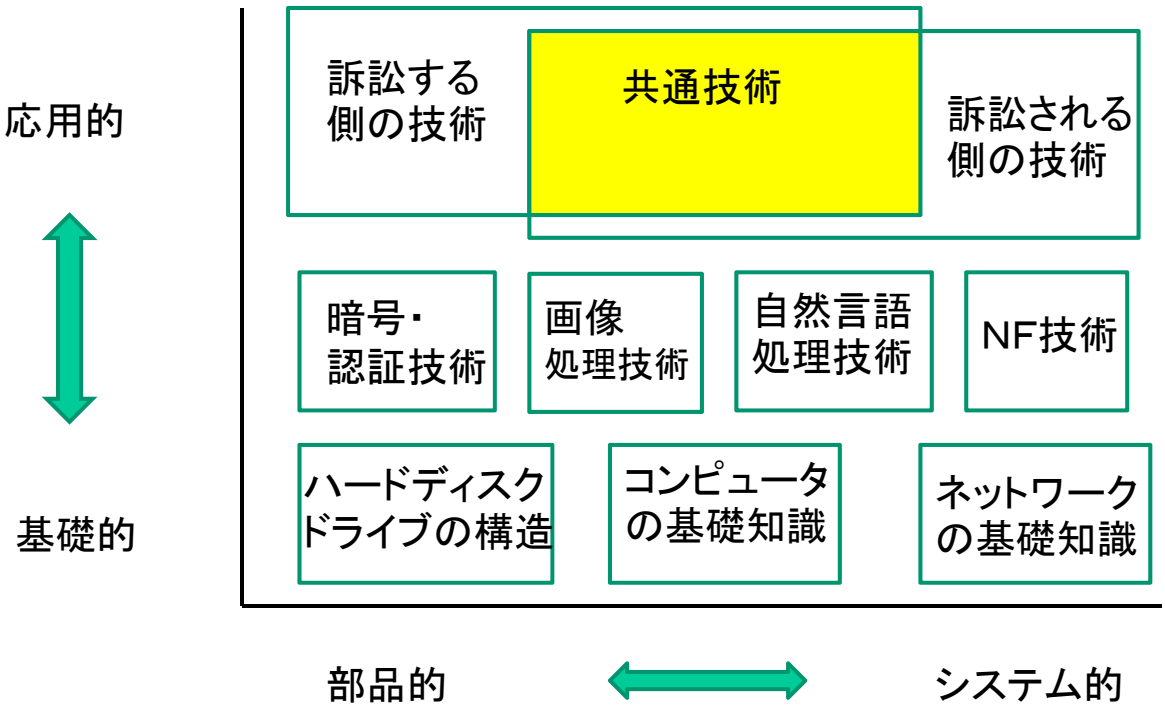
基礎データ

- ログデータ
- レジストリ情報

アプリケーションデータ

- E-Mail
- 入力データ・作成文書
- 財務帳票
- 各種取引記録

DFに関連する技術



NF：ネットワーク・フォレンジック

対象によるDF用語の分類

種類	対象
ディスク・フォレンジック（コンピュータ・フォレンック）	ハードディスクを中心とした不揮発な記憶媒体
ネットワーク・フォレンジック	ネットワーク機器、サーバのログなど
電子メール・フォレンジック	電子メールを中心とするデータ
Web・フォレンジック	Webサイトに関連するデータ
モバイル・フォレンジック	携帯電話、携帯端末、スマートフォン等のデータ

情報セキュリティ白書2011より
他に、メモリー・フォレンジック、DB・フォレンジック、クラウド・フォレンジックなど

フェーズと技術

＜フェーズ＞	＜技術＞
①準備段階	（a）証拠保全技術
②インシデント 発生時	（b）証拠収集技術 （c）証拠分析技術
③裁判関連時	（d）eディスカバリ技術 （e）裁判時参考人としての応答技術

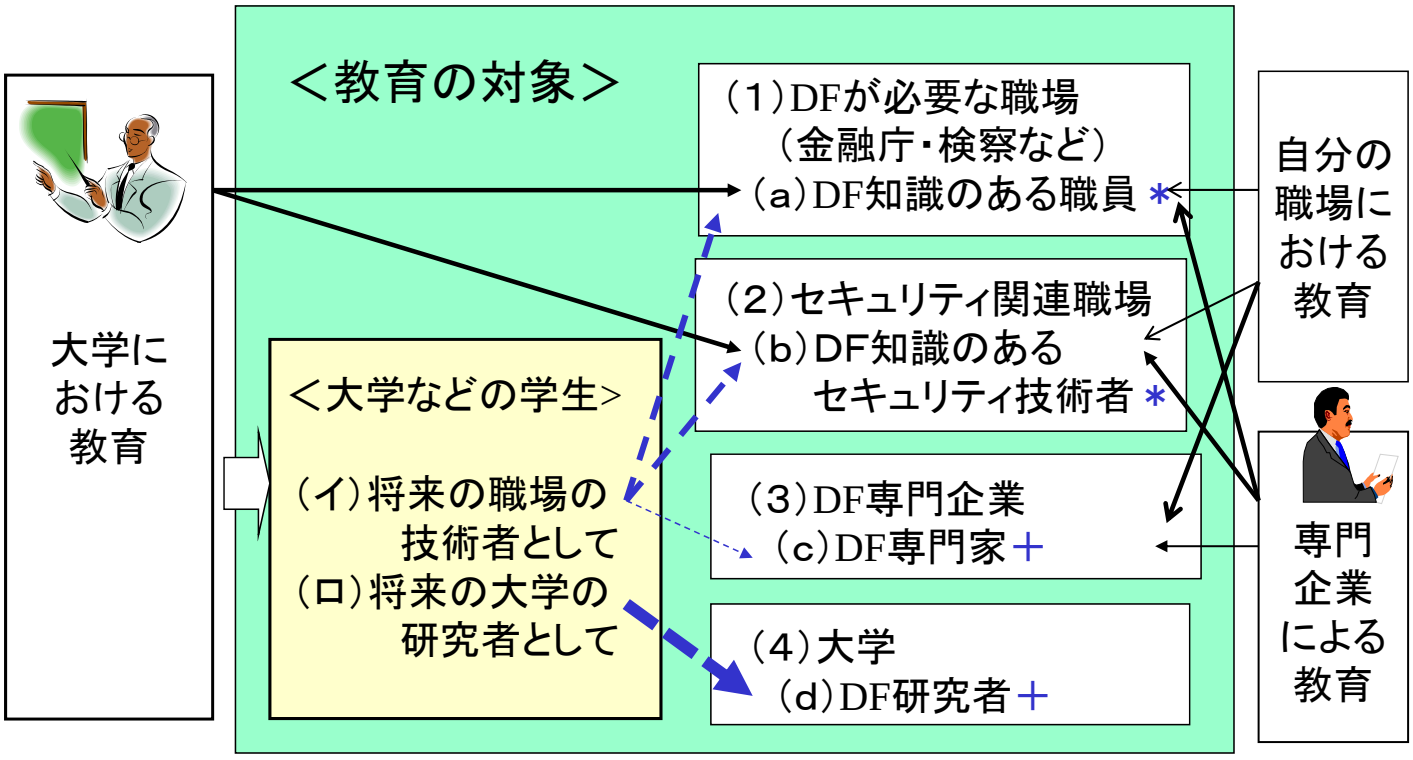
今後重要になっていく分野

1．ディスクの変化へのDFの対応
　HDD大容量化やSSDの普及

2．ディスク・フォレンジック以外のフォレンジックの重要化
　（1）ネットワーク・フォレンジック
　（2）メモリー・フォレンジック
　（3）クラウド・フォレンジック
　（4）スマートフォン・フォレンジック、SCADA・フォレンジック等

3．eディスカバリにおける新しい動き
　（1）関連ファイルの抽出のための機械学習の導入
　（2）抽出や処理のための日本語情報処理の高度化

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　トップガンは直接の対象外

目次

活動計画の概要

1. 期間
   2015年1月ー2017年3月（延長の可能性あり）
2. 体制案
   主査：佐々木　副主査：上原
   参加者：基本的にDF研究会メンバーで参加を希望する者
3. 成果目標（案）
   （1）人材マップの作成
   （2）人材と育成機関の関連図作成
   （3）大学（院）向け標準カリキュラム作成
   （4）大学（院）向け教科書の出版
   （5）企業における標準カリキュラム作成
   （6）資格制度の必要性の検討など

目次

東京電機大学大学院における新たなセキュリティ教育

文科省「高度人材養成のための社会人学びなおし大学院プログラム」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。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）情報セキュリティとガバナンス
（6）セキュアシステム設計・開発

Carnegie Mellon University

Master of Science in Information Networking with a concentration in Computer Forensics and Incident Response

14-761: Advanced Information Assurance
14-822: Host-Based Forensics
14-823: Network Forensics
14-824: Advanced Host-Based Forensic Analysis
14-825: Advanced Network Analysis
14-826: Event Reconstruction and Correlation

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*

Purdue Universityが分析したモデルDFコース

Table 4.3 List of Required Courses and Electives

Required Courses	Electives (Specialized Courses)
Introduction to Digital Forensics	Network Forensics
Advanced Digital Forensics	Mobile Device Forensics
Research in Digital Forensics	File System Forensics
Digital Forensics Capstone Course	Anti-Forensics
Thesis or Directed Project	Incident Response
	Digital Law
	Malware Forensics

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*

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

現時点でのDF教育計画①

2015年度は後期金曜日18:10－19:40の予定

（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）フォレンジック作業・データ解析2（ UBIC 野﨑）
（9）上記の演習（トーマツ 白濱、UBIC 野﨑）

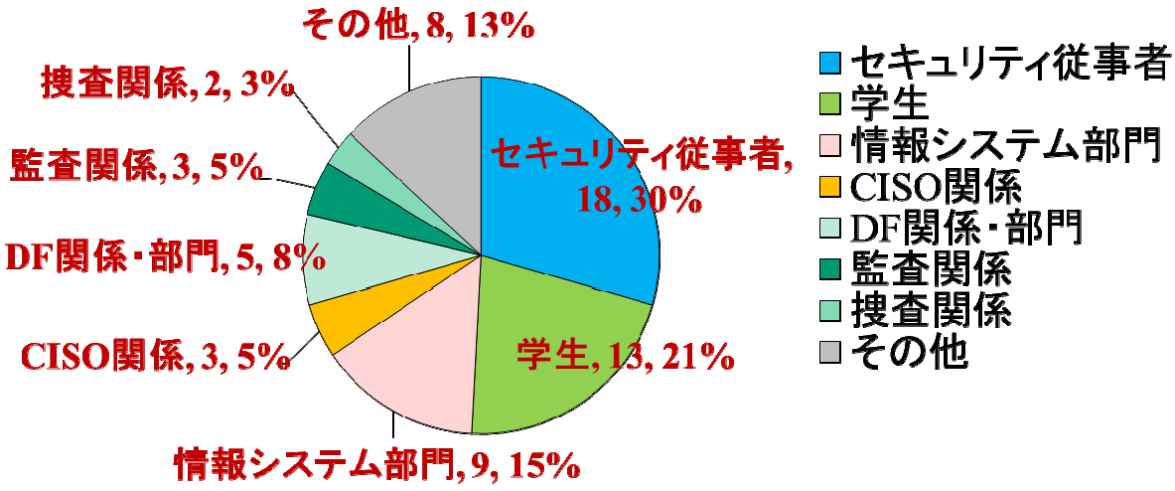
現時点でのDF教育計画②

（10）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）
（11）上記の演習 （電大 八槇）
（12）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）
（13）代表的な対象におけるDFの方法2 不正会計、e-Discovery
（ UBIC 野﨑）
（14）法リテラシーと法廷対応 （弁護士 桜庭）
（15）デジタル・フォレンジックの今後の展開 （電大 佐々木）
（16）学力考査と解説

2015年度以降は同じ講義を年2回実施を計画中。また、デジタル・フォレンジックのコマ数を2つにすることも検討中

アンケート1(受講者候補への質問)

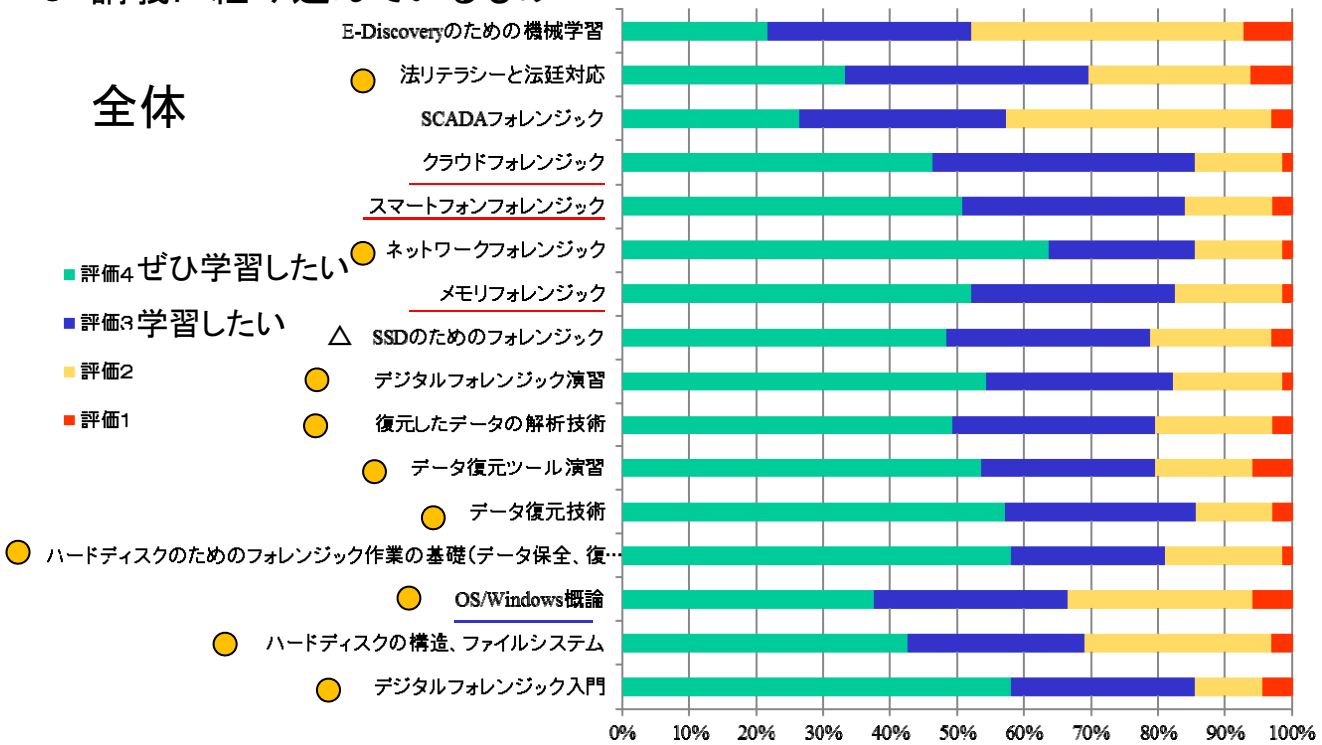
1．日時・場所
2014/10/17の情報セキュリティ大学院大学のDFに関する水平セミナーにて
2．アンケートの項目：東京電機大学で実施する講義で扱うべき項目
3．回答者　75名（受講者候補）



アンケート1の結果①

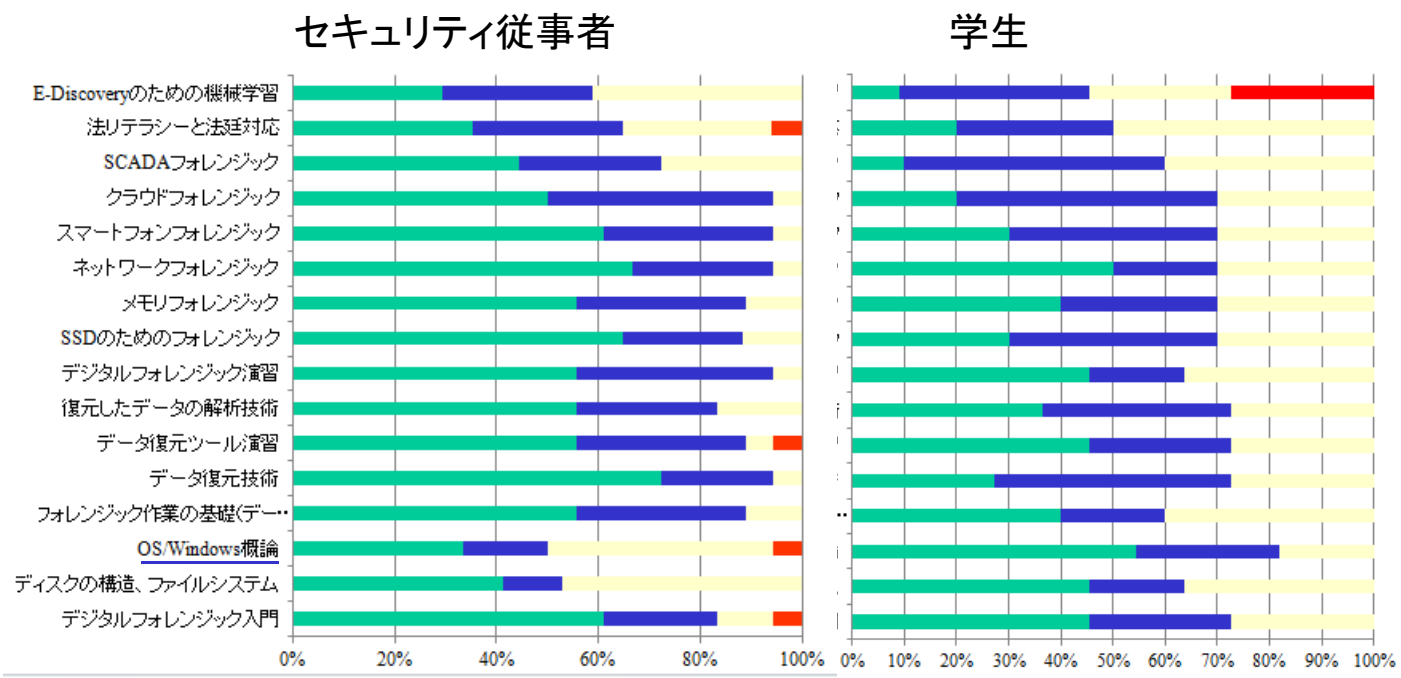
- 講義に組み込んでいるもの

全体



ぜひ学習したい、学習したいを足すと75%を超すものが大部分

アンケート1の結果②



セキュリティ従事者は、ディスクの構造やOS等の講義希望は少ない半面、演習や、NWフォレンジック、スマホのフォレンジックなどの希望が多い

アンケート2の結果
組織としての取り組み

項目	説明	回答数	グラフ
1	組織にとって重要な取り組みなので、組織からお金を出して、職員を参加させたい	5(その内の1名が項目の2に該当*)	項目1
2	組織にとって良い取り組みであるので、職員が自分でお金を払って参加するのを推薦したい	(1*)	項目2
3	組織にとってはあまり関係ないので、職員の自由な判断に任せたい	0	項目3
4	その他	1* *	項目4
5	無回答	1	項目5

アンケート対象：IDFの後援官庁の担当者に11月に発送（4組織7人より回答あり）

*　：基本は項目1であるが、数が多い場合には、項目2にもなる

* *：自前で行っているので、参加させる必要性を感じない

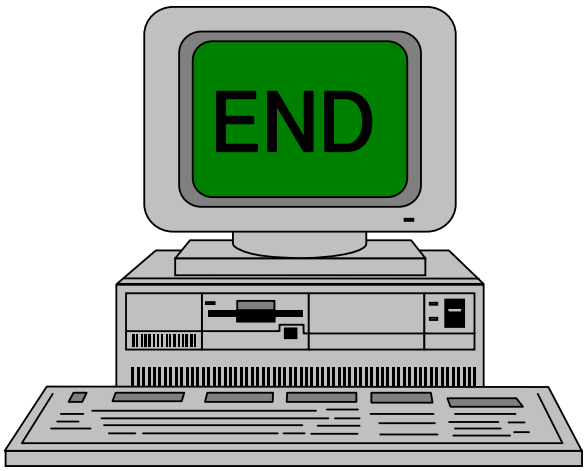
講義項目について省庁と個人の回答の比較（4点満点）

	No	科目名	個人の回答	省庁の回答
○	1	デジタル・フォレンジック入門	3.4	4
○	2	ハードディスクの構造、ファイルシステム	3.1	3.9
○	3	OS/Windows概論	3	3.7
○	4	ハードディスクのためのフォレンジック作業の基礎	3.4	4
○	5	データ復元技術	3.4	3.9
○	6	データ復元ツール演習	3.3	3.5
○	7	復元したデータの解析技術	3.3	3.7
○	8	デジタル・フォレンジック演習	3.4	4
△	9	SSDのためのフォレンジック	3.2	3.7
	10	メモリ・フォレンジック	3.4	3.6
○	11	ネットワーク・フォレンジック	3.5	3.7
	12	スマートフォン・フォレンジック	3.3	3.6
	13	クラウド・フォレンジック	3.3	3.7
	14	SCADA・フォレンジック	2.8	2.4
○	15	法リテラシーと法廷対応	3	3.4
	16	eディスカバリのための機械学習	2.7	3.1

目次

本日議論すべき点

1．分科会の体制と分担
2．成果目標は次のようなものでよいかの議論
　（1）人材マップの作成
　（2）人材と育成機関の関連図作成
　（3）大学（院）向け標準カリキュラム作成
　（4）大学（院）向け教科書の出版
　（5）企業における標準カリキュラム作成
　（6）資格制度の必要性の検討など
3．今後のスケジュール



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

例②

Champlain College

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

例③

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