CySec

ＩＤＦ「ＤＦ人材育成」分科会
2018年7月25日

Brush up Program for professional

東京電機大学

国際化サイバーセキュリティ学特別コース CySecのデジタル・フォレンジック教育とその展開

東京電機大学　特命教授
佐々木　良一

セキュリティ人材の不足

必要人員（34.7万人）

<table>
<tr><td colspan="2">情報セキュリティ従事者（26.5万人）</td><td rowspan="2">不足
8.2
万人</td></tr>
<tr><td>従事者
（技術力あり）
（10.6万人）</td><td>従事者
（技術力不足）
（15.9万人）</td></tr>
</table>

http://www.ipa.go.jp/files/000040646.pdf
2014年7月の報告書
（注）2012年の報告書では、2.2万人の不足
http://www.ipa.go.jp/security/fy23/reports/jinzai/

情報セキュリティの技術分野

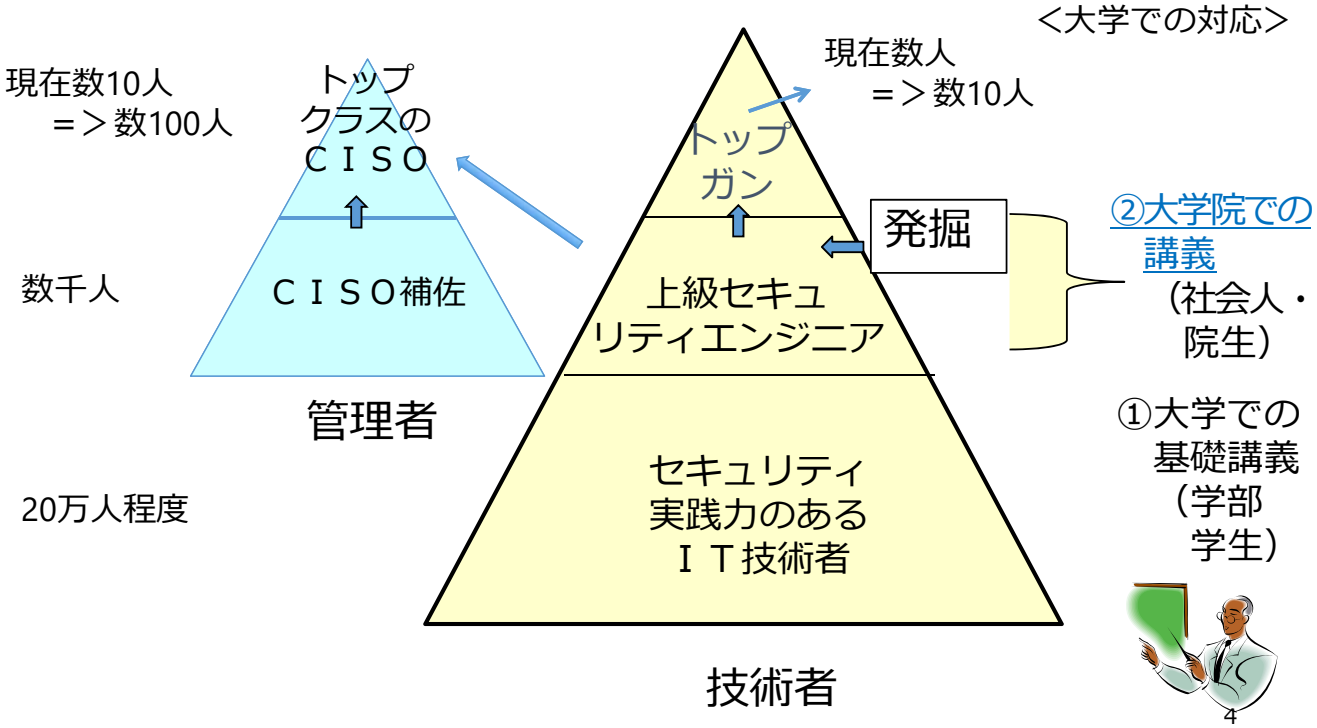
① セキュリティ戦略／統括
② 企画／設計
③ 開発／構築
④ 運用／管理
⑤ 監査／検査
⑥ コンサルティング／教育

どの分野が特に足りないか？（ＩＰＡの調査では示されていない。私は①④だと思う。）

https://www.ipa.go.jp/files/000024415.pdf

セキュリティエンジニアの育成計画

<大学での対応>



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。２０１５年よりスタート。
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（実際は社会人は常に３０人以上）

（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/

デジタル・フォレンジック２０１５年①

重要性が高まっているが、従来、日本では行われてこなかった新分野の講義

（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　野崎）
（５）フォレンジック作業・データ保全（UBIC　野崎）
（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　野崎）
（９）上記の演習（白濱、野崎）

デジタル・フォレンジック２０１５年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　野崎）
（14）法リテラシーと法廷対応（弁護士　櫻庭）
（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

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

その後の改善

１．２０１６年度－２０１７年度
（１）「デジタル・フォレンジック演習」を１回から２回へ。
（２）「モバイルフォレンジック」の追加。
（３）「代表的対象におけるＤＦの方法」の２回を１回に。
（４）「データ解析」の２回を１回に。

２．２０１８年度
（１）１回あたり９０分を１００分に。１５回を１４回に。
（２）デジタル・フォレンジック作業の４回を３回に整理。
（３）「デジタル・フォレンジック演習」２回のうち１回を
「モバイルフォレンジック演習」に。

講義の工夫

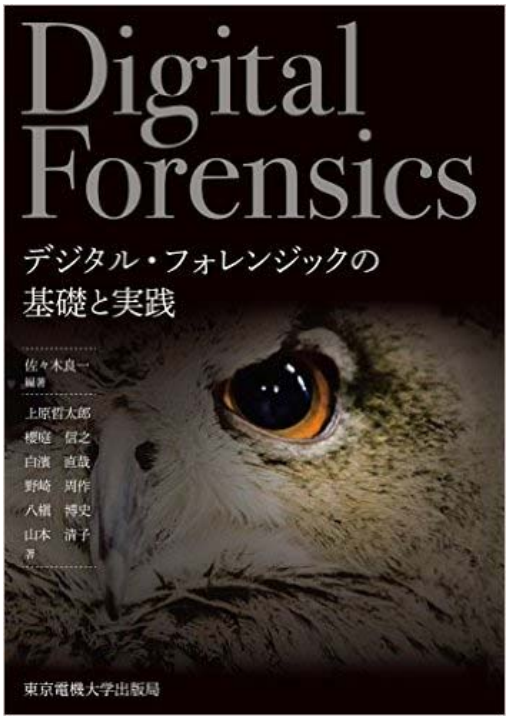
１．演習比率の増大

２．講義用ＰＰＴの事前配布

３． E-Learning：講義動画の欠席者への提供

４．教科書の作成
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，2017年3月

デジタル・フォレンジックの教科書



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，2017年3月

講義風景

デジタル・フォレンジックの講義では、デジタル証拠をベースにした模擬法廷の実習も

プログラムの実績

- 社会人受講生
  - 27年度前期33名，後期9名
  - 28年度前期34名，後期7名
- 修了生
  - 27年度18名（大学院生1名含む）
  - 28年度8名（前期終了時点，後期終了時点+26名見込）

①もともと特定の科目だけ受講することも可能。
②社会人受講者は、官庁や企業から派遣された人もいるが、多くは自己費用で参加する人。
セキュリティ業務についている人が大部分。

授業評価アンケート結果と分析

1．受講者の特徴
（1）セキュリティに関連する業務を行っている受講者が多かった。
社会人は常に３０人以上。
（2）組織のお金ではなく、自分のお金で参加している人のほうが多かった。
（検察庁や金融庁など公的組織からの派遣も）

2．評価
（1）講義全体に好評であったが、特にデジタル・フォレンジックは好評。
（2）その中でも演習や法リテラシーと法廷対応の評判は非常に良かった。
（3）ＤＦだけ聞きに来る受講者もいた。

3．改善点
（1）１コマの講義だけでは、教えるべきことが多すぎる。CySecの中でデジタル・フォレンジックのコマを増やしていくのは困難。
（2）講義を受けても実務とのリンクがないとすぐに専門家として独り立ちは困難。

本格的対応

1．CySecPRO （一般社団法人サイバーセキュリティプロフェッショナルズプロデュース）の立ち上げと実務者コースデジタル・フォレンジックのスタート（11月より）

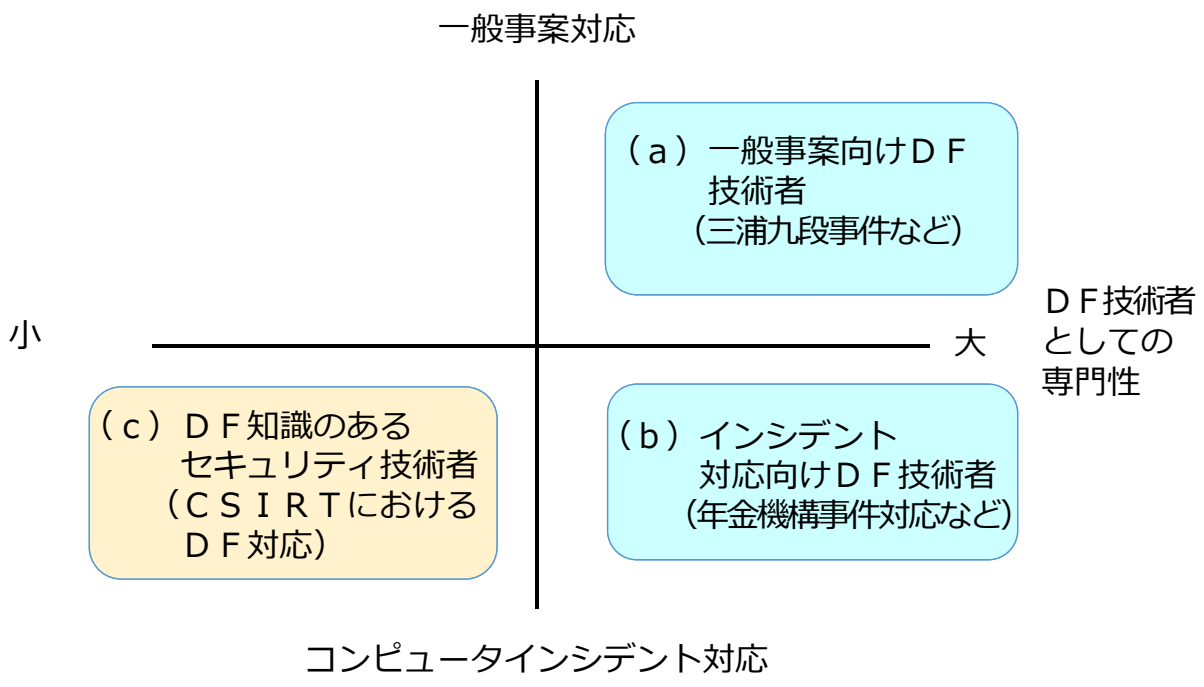
http://cysec-pro.org/course/syllabus/

CySecPROを東京電機大学は後援する形。

2．他のセキュリティ企業におけるデジタル・フォレンジック教育との補完

3．育成者に活躍の場を紹介するのとのリンク

どの分野のＤＦ技術者の育成を目指すのか



今回の会合に期待するもの

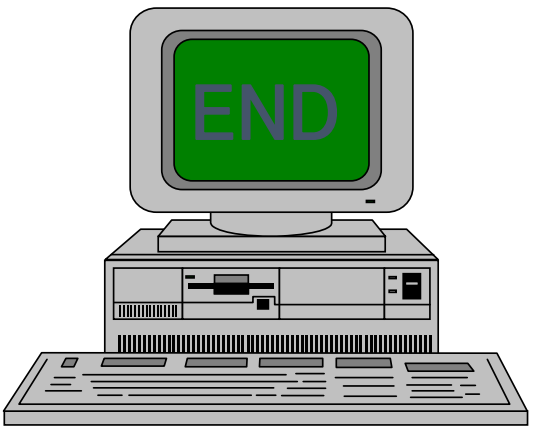
（１）　どのような場面で活躍するデジタル・
フォレンジック人材の育成を目指しており、
どのような教育をしているのか。

（２）　それで十分か。さらに行うとしたらどんな
教育をすべきだと思っているか。

（３）　教育だけで人材の育成は可能か。
それ以外に対応すべきものは何か。

＜その他＞

- ①マルウエア解析技術はＤＦか。
- ②ＮＷフォレンジック・メモリーフォレンジック、
モバイルフォレンジックなどの扱いを
どうしているか。



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に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