デジタル・フォレンジック研究会
人材育成分科会第2回会合

2015年3月4日

東京電機大学におけるDF人材教育のための佐々木担当講義の概要

東京電機大学教授
佐々木良一
sasaki@im.dendai.ac.jp

目次

1. 東京電機大学における
   デジタル・フォレンジック教育の計画
2. 第1回　デジタル・フォレンジック入門
3. 第15回　デジタル・フォレンジックの今後の展開
4. DF人材育成分科会の来年度の予定

東京電機大学大学院における新たなセキュリティ教育

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

https://cysec.dendai.ac.jp/
6科目で15万円ぐらいか

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

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）

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　野崎)
(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・フォレンジックの駒数を2つにすることも検討中

目次

1. 東京電機大学における
   デジタル・フォレンジック教育の計画
2. 第1回　デジタル・フォレンジック入門
3. 第15回　デジタル・フォレンジックの今後の展開
4. DF人材育成分科会の来年度の予定

第1回の講義概要

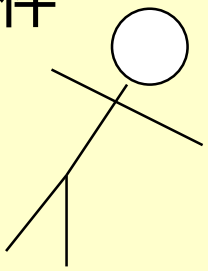
1. デジタルフォレンジックとは何か
2. デジタルフォレンジックで用いる技術
3. デジタルフォレンジックの利用者と利用目的
4. データの消去と復元
5. 警察におけるデジタルフォレンジック
6. 民間におけるデジタルフォレンジック業務の概要
7. 訴訟する側のデジタルフォレンジック
8. 訴訟される側のデジタルフォレンジック
9. E-Discoveryの概要
10. 今後の講義計画

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

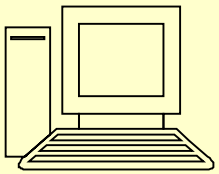
殺人事件



死因は？、凶器は？、犯人の血液型は？

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



侵入手口は

侵入経路は？

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

DFで使う技術の分類

事前

1．証拠保全技術

① アクセスログや通信ログなどの記録
② データの変更の防止やバックアップ

事後

2．証拠収集技術

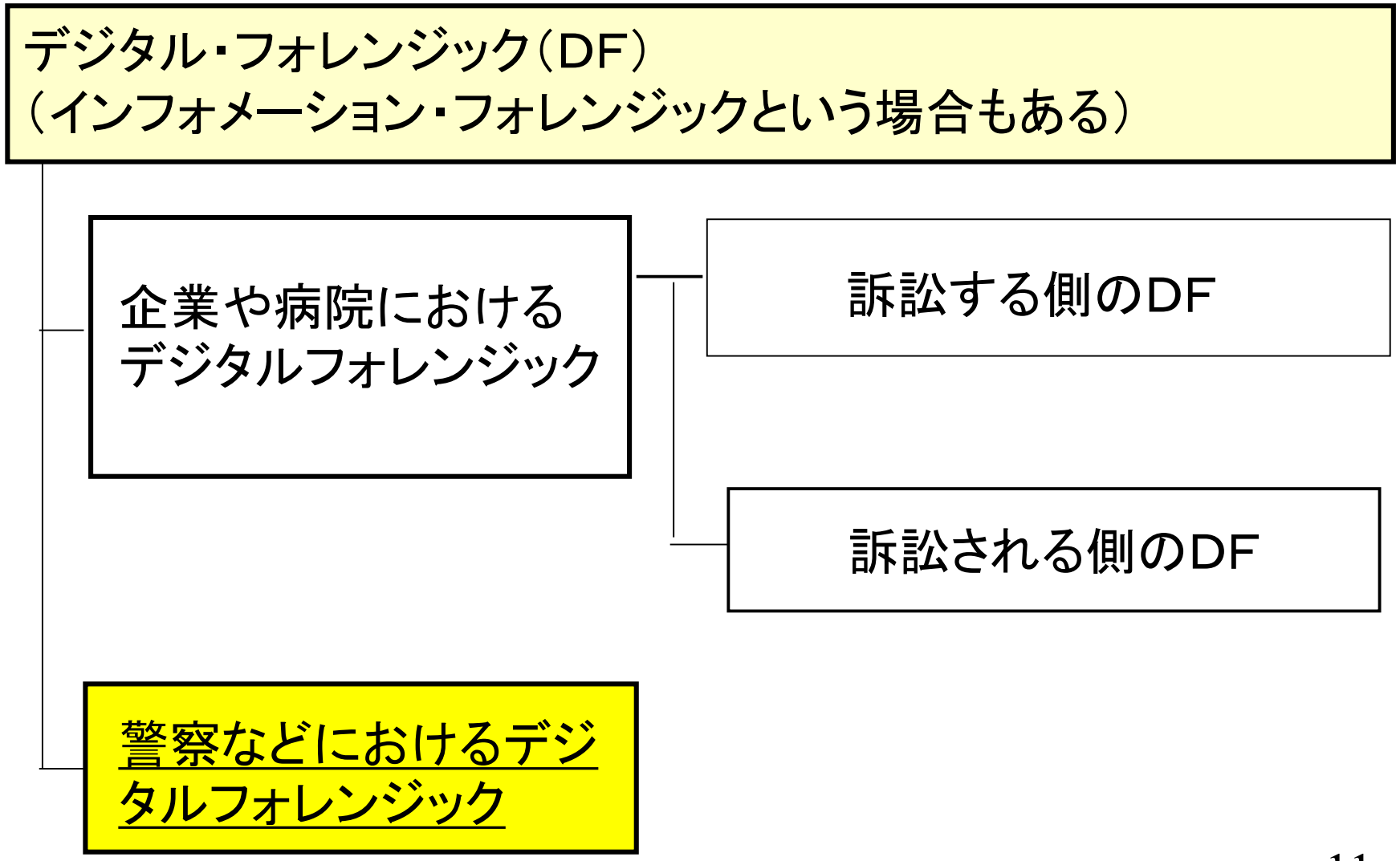
① 削除されたファイルや物理的に破壊された媒体を復元
② 暗号化されたファイルの復号
③ 証拠隠滅の痕跡の調査など

事後

3．証拠分析技術

① 得られた大量のデータから有用なデータを抽出する（データマイニング）
② 得られたデータが改ざんされていないかの分析

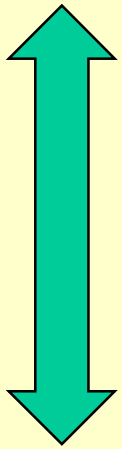
デジタル・フォレンジックの体系



警察などにおけるDFの適用候補

1. 殺人など犯罪の証拠のPCからの確保
   （電子メール、インターネット検索履歴、その他）
2. 児童ポルノの保管証拠の確保
3. 不正侵入の被害の実態確認と攻撃者の特定
4. コンピュータウイルスの作成の証拠確保

対象は一般犯罪



対象はコンピュータ関連犯罪

警察と民間での対応範囲の違い

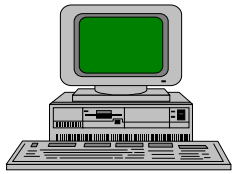
＜事前＞

何か起きた時に備えて

事件の発生

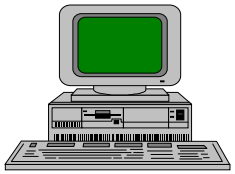
＜事後＞

証拠が消える前に



民間は両方

警察は事後のみ



1．証拠保全技術

警察は民間への啓発が必要

2．証拠収集技術

3．証拠分析技術

DFで使う技術の分類

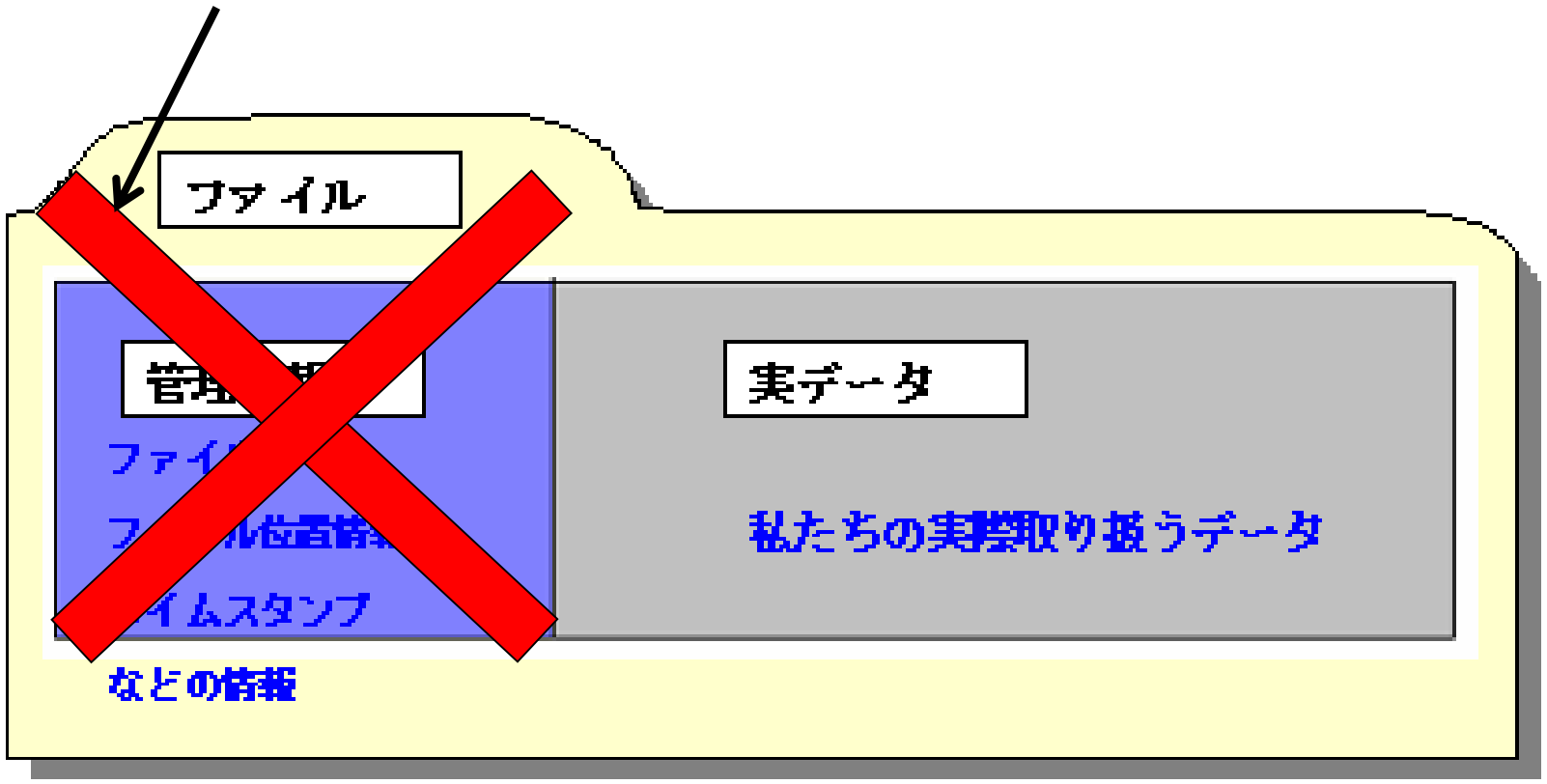
1．証拠保全技術
- ① アクセスログや通信ログなどの記録
- ② データの変更の防止やバックアップ

2．証拠収集技術
- 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
- ② 暗号化されたファイルの復号
- ③ 証拠隠滅の痕跡の調査など

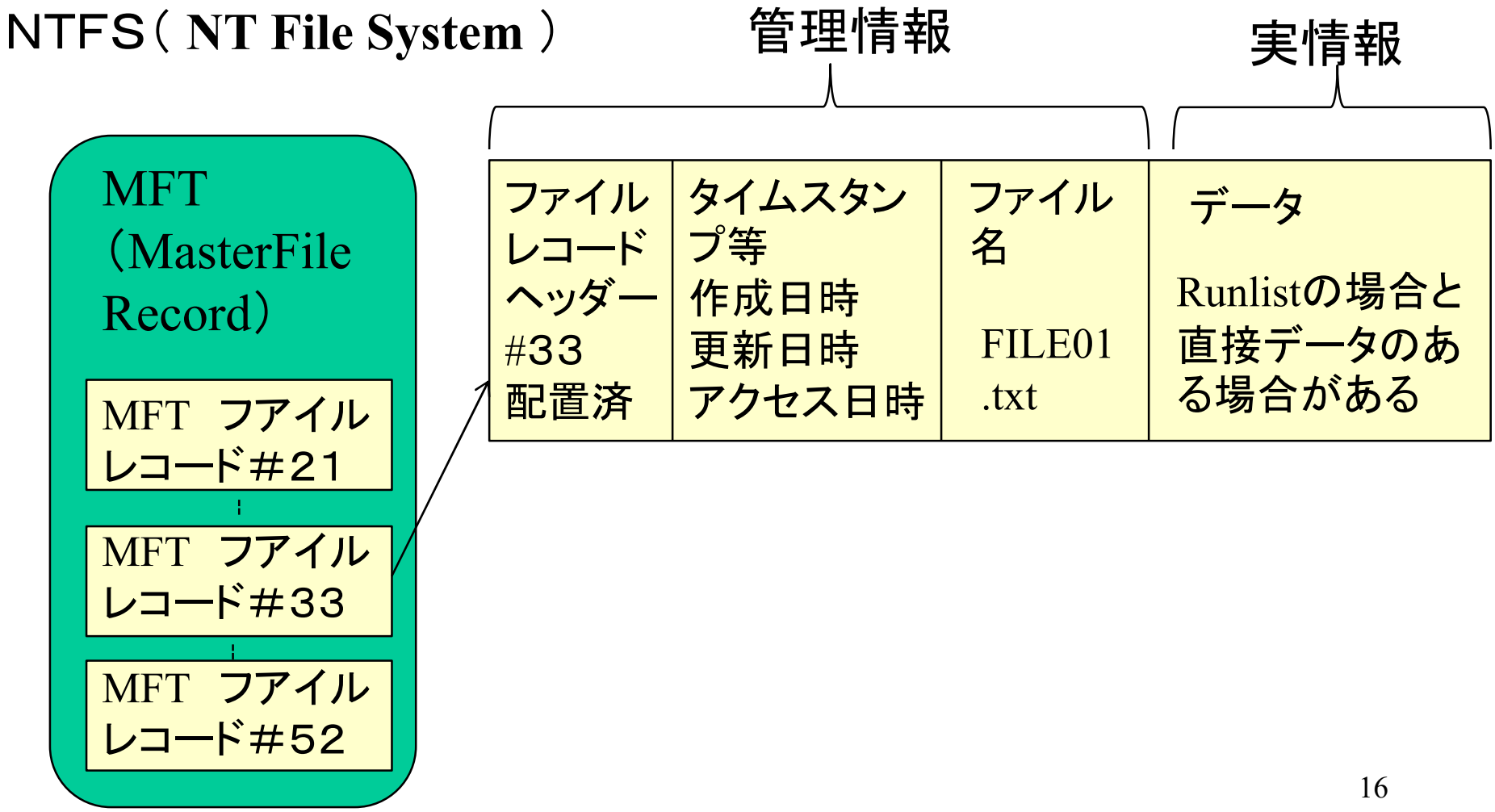
3．証拠分析技術
- ① 得られた大量のデータから有用なデータを抽出する（データマイニング）
- ② 得られたデータが改ざんされていないかの分析

データ消去とは(2)

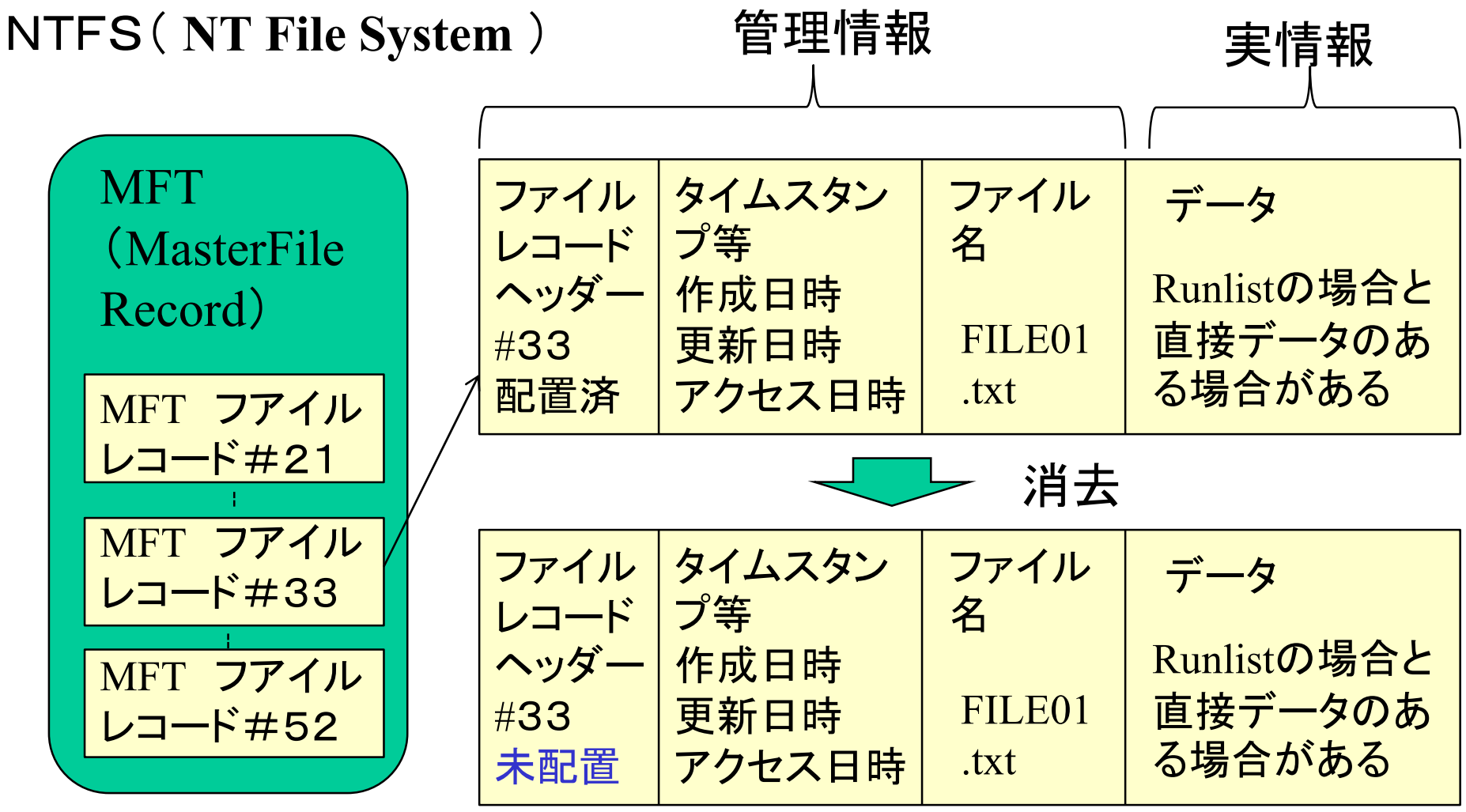
- データ消去の行っている事



NTFSにおける消去と復元



NTFSにおける消去と復元

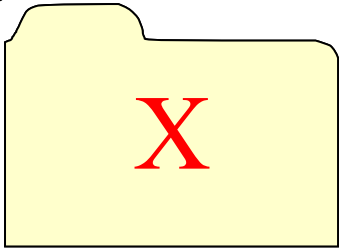


誤って消去したファイルを復元できる

- フリーの復元ソフト

直後なら復元可能

【消去ファイル】



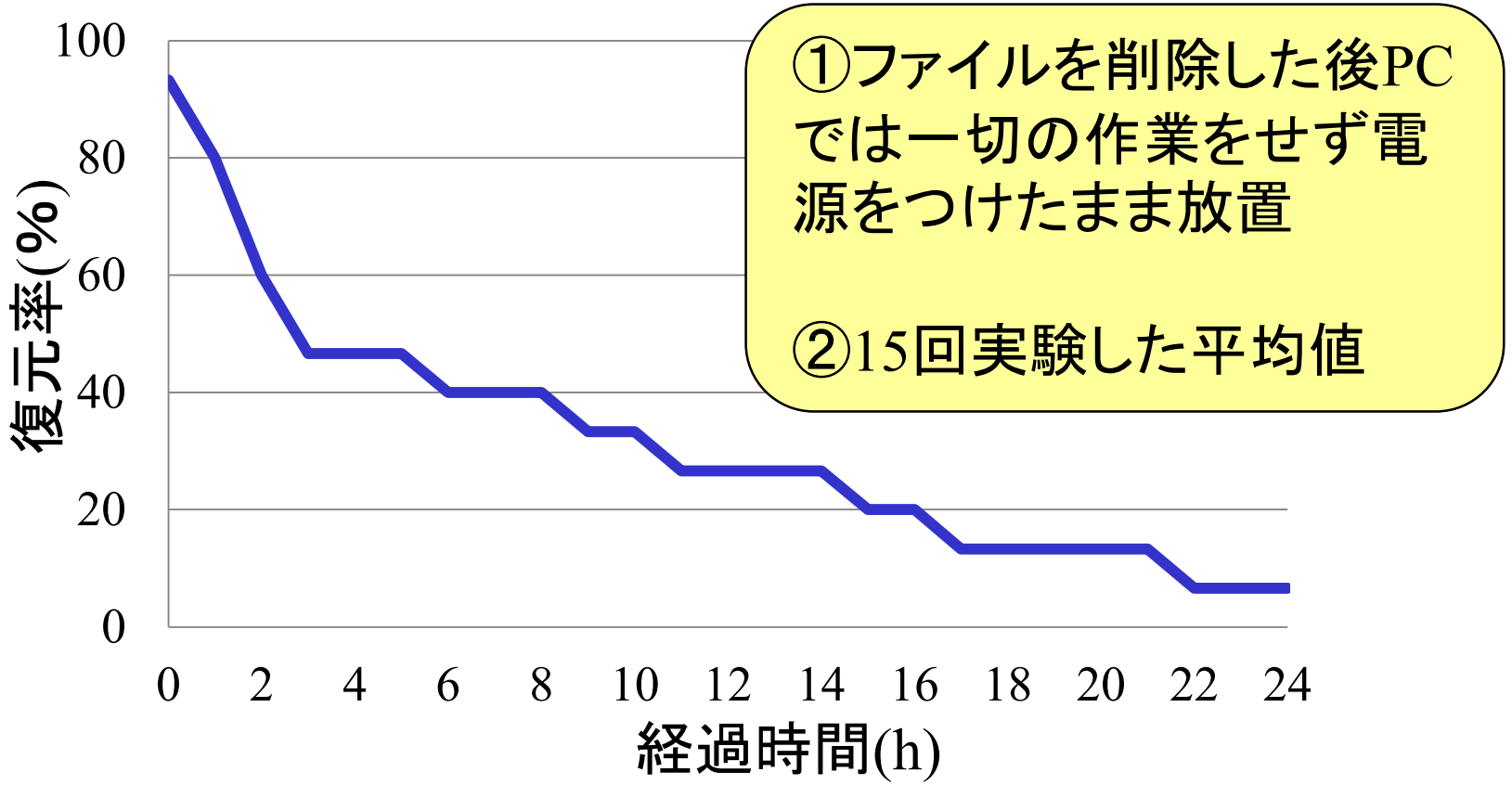
データ復元はデジタル･フォレンジックの重要技術

デジタル・フォレンジックツールの比較

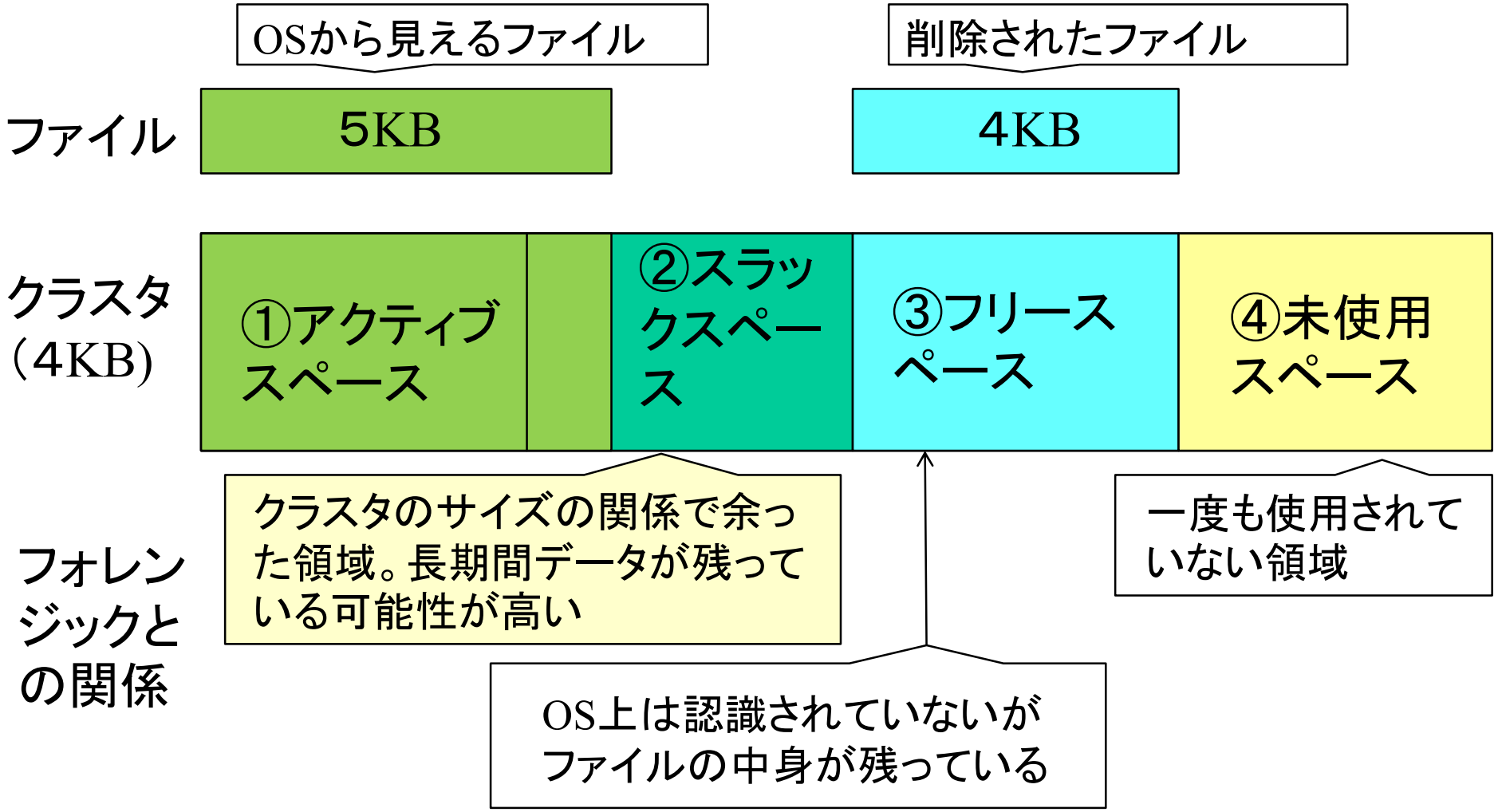
名称など	開発者 （販売会社）	機能など	備考
Encase (1997年発売)	Guidance Software社 （商品）	PC内のデータの復元 メインメモリーのデータ の監視など 報告書の作成など	
Ultimate Tool Kit （2004年発売）	Access Data社 （同上）	証拠性保全のための 総合的ツールキット （PC内のデータの復元、 パスワード解読、報告 書の作成など）	Forensic Tool Kitが中心

最近は、X-Ways社のX-ways ForensicsやBelkasoft社のEvidence Centerも

HDDの消去ファイルの復元率



ファイルシステム



佐々木良一監修「ネットワークセキュリティ」オーム社2014年、p165

目次

1. 東京電機大学における
   デジタル・フォレンジック教育の計画
2. 第1回　デジタル・フォレンジック入門
3. 第15回　デジタル・フォレンジックの今後の展開
4. DF人材育成分科会の来年度の予定

第15回の講義概要

１．今までの講義でやってきたことのまとめ
２．今後重要になる分野と課題
　①　コンピュータフォレンジックのHDDの大規模化とSSDの採用の影響
　②　ネットワークフォレンジック
　③　ライブフォレンジック
　④　クラウドフォレンジック
　⑤　モバイルフォレンジック
　⑥　SCADAフォレンジック　他
３．さらに学ぶ人のために

目次

1. 東京電機大学における
   デジタル・フォレンジック教育の計画
2. 第1回　デジタル・フォレンジック入門
3. 第15回　デジタル・フォレンジックの今後の展開
4. DF人材育成分科会の来年度の予定

2015年度のDF人材育成分科会の活動計画

１．開催予定：年4回程度

２．討議項目

　①　第１回：企業で行っているDF人材育成の紹介など

　②　第２回：海外事例の紹介

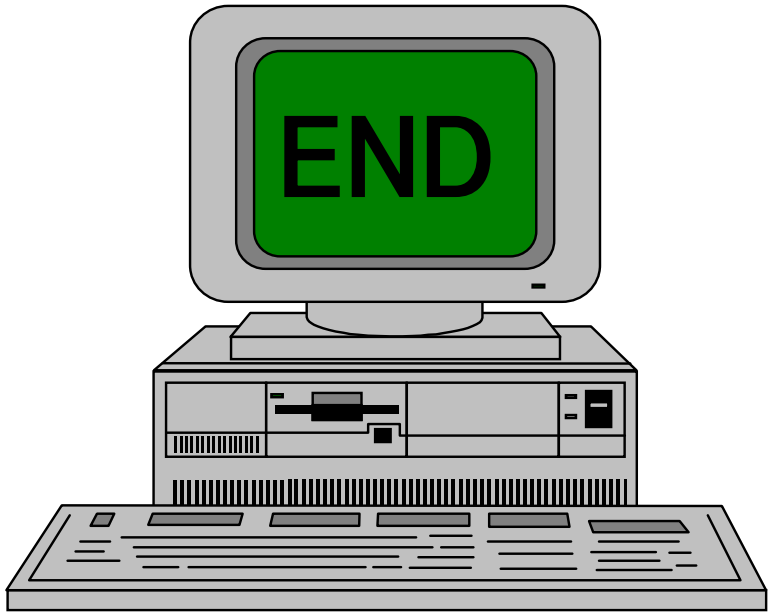
　③　第３回：現在の初級のカリキュラムに中級・上級を加えた全体としてのカリキュラムの検討

　④　第４回：東京電機大学でやっている講義とその反省を通じた教材の作成（WG活動も必要か）

本日議論すべき点

1. 東京電機大学の2015年度の講義内容

2. DF人材育成分科会の来年度の活動計画


END

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

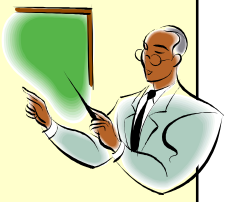
http://docs.lib.purdue.edu/dissertations/より

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