デジタルフォレンジック研究会と私
第2代会長として

東京電機大学
名誉教授・客員教授
佐々木良一
r.sasaki@mail.dendai.ac.jp

目次

私のデジタル・フォレンジックとの出会い

1．出会った時期：2002-3年ごろ
2．トリガー：弁護士の知り合いが多く、デジタル・フォレンジックやコンピュータ・フォレンジックという言葉を使っていた
3．研究に着手した理由（2003-4年ぐらい）
（1）今後、データは、大部分がデジタル化
（2）今後、権利意識が増大し、民事訴訟が増加
＝＞　DFが重要にならないはずはない

当時は、コンピュータフォレンジックとか、フォレンジックコンピューティングという言葉を使う人が多かった

警察政策学会のパネル

1．日時：2003年6月20日
2．テーマ：「ネットワーク社会の安全
（フォレンジックコンピューティング）」
（於　警察政策学会5周年記念シンポジウム）
3．出席者：
コーディネーター：
佐々木良一（東京電機大学）
パネリスト　　：
宮城直樹（警察庁生活安全局）
内田勝也（中央大学研究開発機構）
山崎文明（グローバルセキュリティエキスパート）
尾崎孝良（弁護士）

@Policeの記事(2003年9月16日)

Home
パソコンユーザ
システム/ネットワーク管理者
キッズ！
Topics
世界のセキュリティ事情
インターネット定点観測
インターネット治安情勢
セキュリティボード
「サイバーフォース」とは
講演資料
リンク集
ご意見・ご要望
メルマガ登録
ダウンロード
インターネット定点観測

目的別インデックス　用語集　サイトマップ

コラム　セキュリティ解説　バックナンバー

第3回 セキュリティ解説

東京電機大学 工学部教授 佐々木良一（ささきりょういち）

コンピュータ・フォレンジックス

1. 攻撃は最大の防御？

数年前、私が企業に所属していた当時の話です。セキュリティ対策の相談に乗っていたとき、顧客から「それでは対策が生ぬるいのではないか。守るだけではなく、不正侵入してくるような相手にはコンピュータ・ウイルスを送り込むなどこちらからも攻撃することにより不正侵入を抑止するべきではないか」といわれたことがあります。

これに対し「2つ問題があると思います。1つは、ウイルスの送り込み先をどうやって特定するかという問題です。相手のIPアドレスが分かっていると思っていても、IPスプーフィングなどの手段を使われてなりすまれていると、善良な人のパソコンにウイルスを送り込むことになりかねません。もうひとつの問題は、IPアドレスが攻撃者のものであったとしても反撃することにより、さらに激しい攻撃を受ける可能性が高いことです。相手は暇ですから何をやってくるかわかりません。以上2つの理由によりお勧めできません。」と申し上げました。

これらの反撃は法律上も問題があり、上記の対応は今でも正しいと思っていますが、被害を減少するために積極的に対応していこうとする姿勢には教えられるものがありました。報復攻撃まではやりませんが、攻撃を検知すれば、応急処置をするだけでなく、証拠となりうるデータを保存し、(1)どのような被害を受け

2004/01/15
印鑑登録証明と公的個人認証
東京電機大学工学部教授 佐々木良一 (ささき りょういち)

2003/09/16
コンピュータ・フォレンジックス
東京電機大学工学部教授 佐々木良一 (ささき りょういち)

2003/07/15
電子透かしとステガノグラフィ
東京電機大学工学部教授 佐々木良一 (ささき りょういち)

2003/05/15
個人情報保護とセキュリティ
東京電機大学工学部教授 佐々木良一 (ささき りょういち)

http://web.archive.org/web/20070410010543/http://www.cyberpolice.go.jp/column/index.html

日本におけるIDF発足以前のデジタル・フォレンジックの歴史

1996年：電子的記録解析が警察庁情報管理課の管掌になる

2000年：警察庁情報通信局に技術対策課誕生

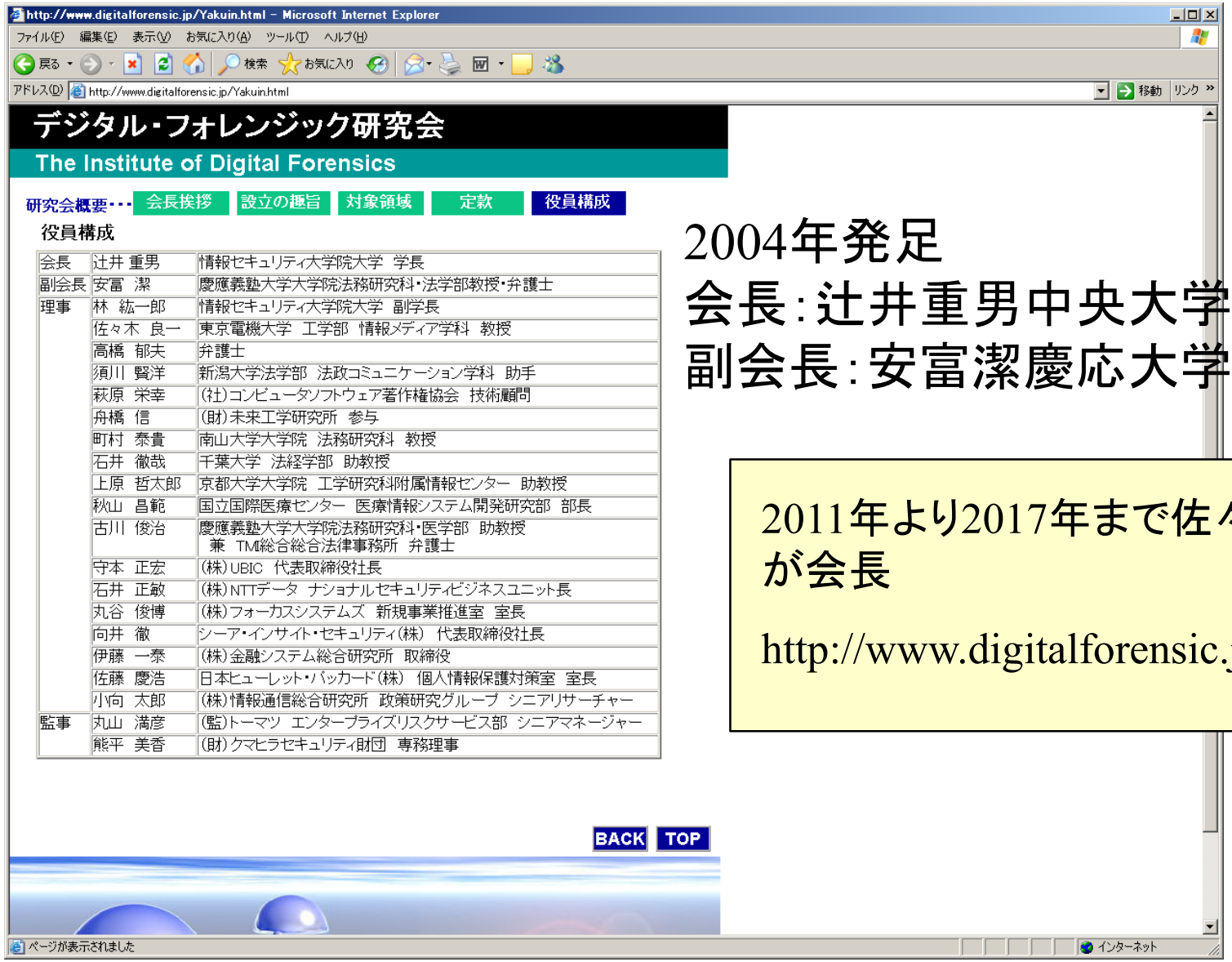
2003年：デジタル･フォレンジックを扱う会社UBIC設立

2003年：警察政策学会のパネルでフォレンジックコンピューティングがテーマに

2003年：@policeにフォレンジックの解説（佐々木執筆）が掲載

2004年：デジタル･フォレンジック研究会発足

デジタル・フォレンジック研究会



2004年発足
会長：辻井重男中央大学教授
副会長：安富潔慶応大学教授

2011年より2017年まで佐々木良一が会長

http://www.digitalforensic.jp/

目次

日本におけるデジタルフォレンジックの教育例

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　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)
学力考査と解説

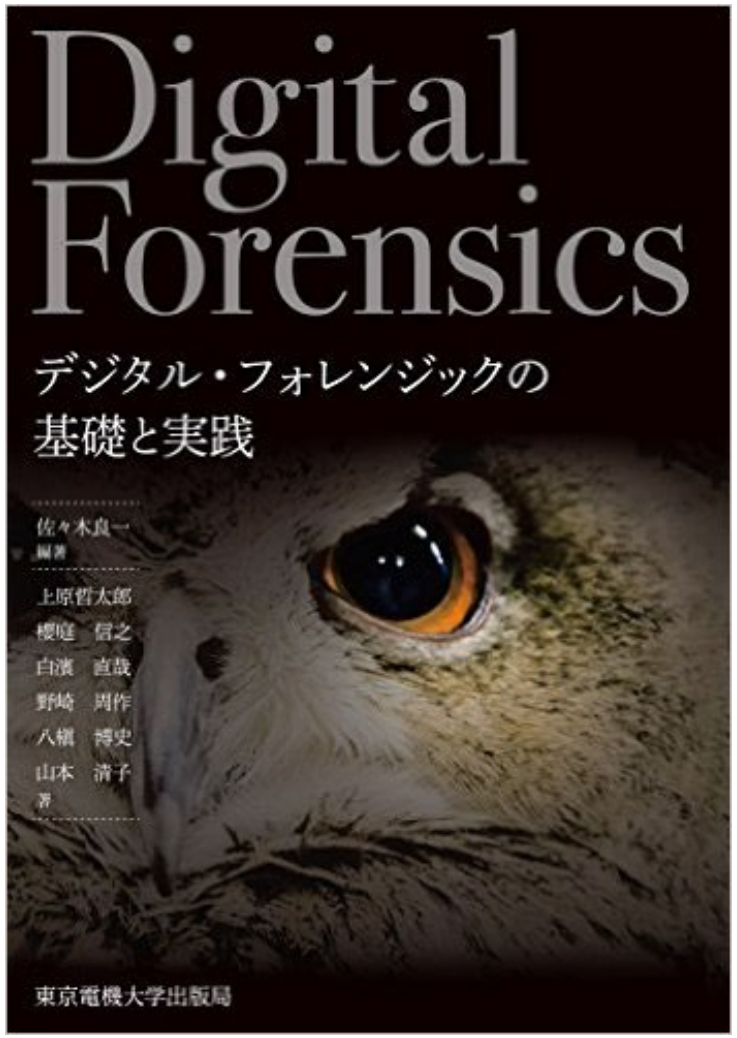
アンケート結果

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

現在までに200名
弱の社会人履修者

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

CySecのDFコースの海外における紹介

（1） R, Sasaki, “Digital Forensics Trends in Japan”, SADFE 2016 Keynote Speech

(2) R, Sasaki, “Digital Forensics in Japan”, IWIN 2017 Keynote Speech

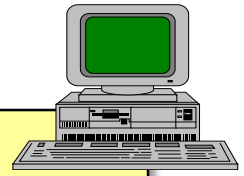
(3)　R, Sasaki, “Education on Digital Forensics for Working People and Graduate Students in Japan” ICT-2019 July, 2019

他

目次

デジタル・フォレンジックで使う技術の分類

＜平常時＞



ログ等の蓄積

＜インシデント時＞

インシデントの認知

① 収集過程

② 復元過程

③ 分析過程

⑤ 報告書作成過程

＜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

① コピー先のディスクの完全消去技術
② 物理コピー技術

① 高度な検索技術
② 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
③ 暗号化ファイルの復号技術

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）

① 調査に不正がないことの心証形成技術

佐々木らの主な研究

1．コンピュータフォレンジックに関する研究

　1．1　ヒステリシス署名を用いたログ改ざん検知システムの研究

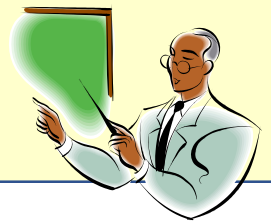
2．ライブフォレンジックの研究

　2．1　ライブフォレンジックによる復号鍵の取得の研究

　2．2　プロセス情報とパケット情報の結合

3．ネットワークフォレンジックの研究

　3．1　LIFTシステムの研究



LIFTシステムの概要

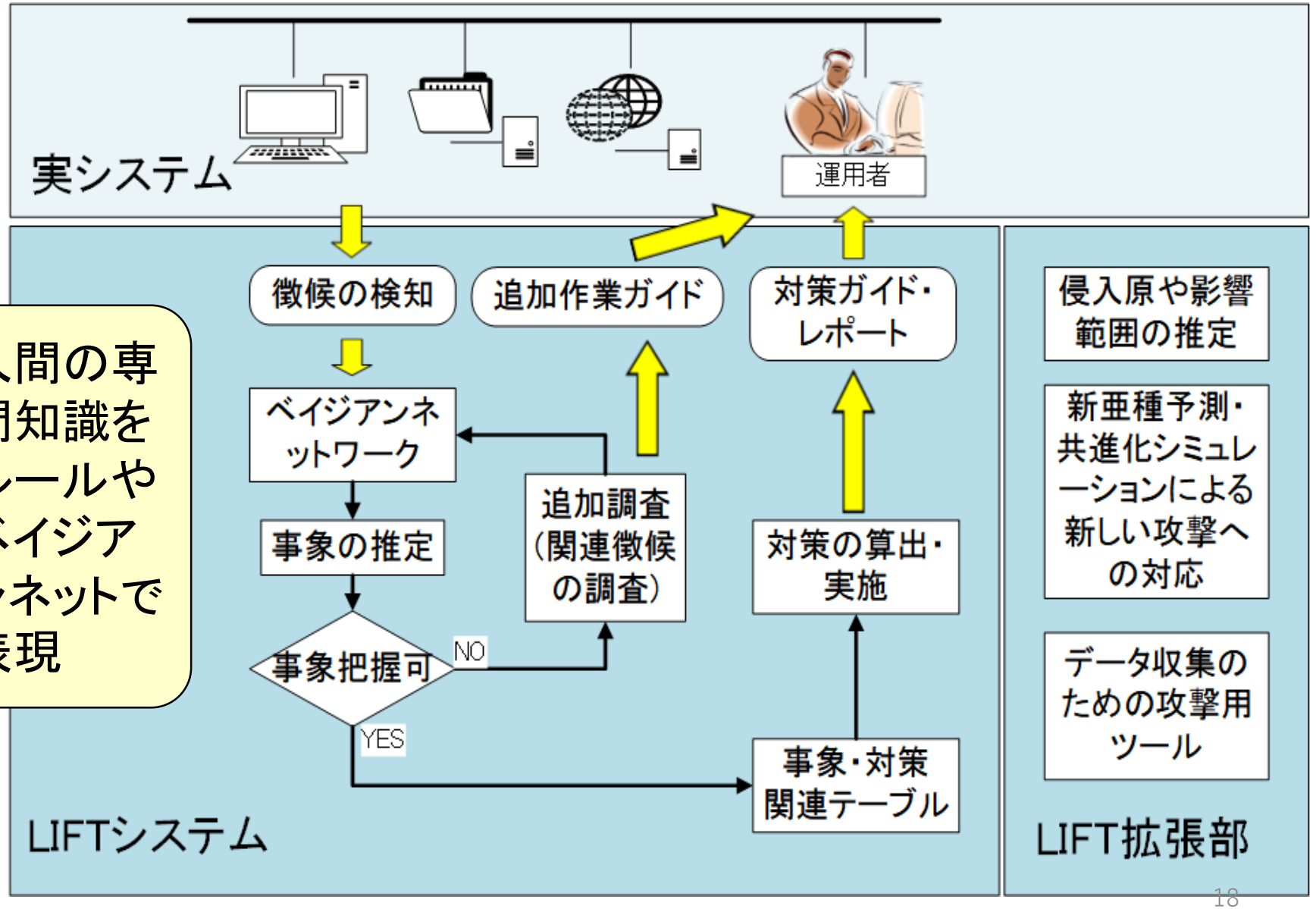
共同開発プロジェクト

リーダ佐々木、上原先生、高倉先生、八槙先生、柿崎先生、日立他

期間：2013年9月ー2018年3月（第一期）

現状での主な成果：
① 方式確立
②原因プロセス発見ソフト実用化（一部製品への組み込み）

人間の専門知識をルールやベイジアンネットで表現



米国との共同研究プロジェクト

２００４年度からは、デジタル・フォレンジックに関するミシシッピー州立大学との共同研究を実施

第４回Digital Forensic International Conferenceを2008年に日本（京都）で実施したりして国際化も進展。

IEEE International Workshop in Cyber Forensics, Security, and E-discovery (CFSE 2023)

Program Chairs

Ryoichi Sasaki
Tokyo Denki University

Tetsutaro Uehara
Ritsumeikan University

Jigang Liu
Metropolitan State University

目次

主な実施事項（2011-2017）

2011年：ＩＤＦ講習会スタート

2012年：「証拠性保全ガイドライン第2版」公開

2013年：10周年記念行事

2015年　東京電機大学においてCySecの開始

2017年　DF優秀若手研究者表彰制度の開始

DF優秀若手研究者表彰の概要

（１）　「デジタル・フォレンジック優秀若手研究者表彰」は、デジタル・フォレンジック研究の活性化を目的として、デジタル・フォレンジックに関する優れた若手研究者を表彰するために、2017年より設置。

（２）　対象者：40歳以下

（３）　理事による候補者推薦

目次

おわりに

- デジタルフォレンジックは一分野として確立し、多くのセキュリティ技術者が知るところとなってきた。また、フォレンジックをやれる人も増大してきた
- 今後、クラウドフォレンジックへの対応が重要に
- 日本のデジタルフォレンジック研究者は少なく強化が必要


END

海外におけるデジタル・フォレンジックの歴史

①1984：米国FBIにComputer Analysis and Response Team発足
②1985：イギリスMetropolitan PoliceにComputer Crime Department 設置
③1986：ハッカーMarkus Hess のCliff Stollによる追跡にDFを初めて使用（初歩的な技術）
④1989： Michael White がForensic Tool IMDUMPを作成。1990年代になり高度な商用ツールEnCaseやFTKが誕生
⑤1992： Computer Forensicsという言葉がCollier, P.A. and Spaul, B.J.によって初めて学術文献に登場
⑥2001： DFに関する研究会議DFRWSの第一回会合を実施
⑦2002： Scientific Working Group on Digital Evidence (SWGDE)が標準化のための文書“*Best practices for Computer Forensics*”（2005 ISO17025に）

http://en.wikipedia.org/wiki/Digital_forensics

佐々木らの主な研究

1．コンピュータフォレンジックに関する研究

　1．1　ヒステリシス署名を用いたログ改ざん検知システムの研究

2．ライブフォレンジックの研究

　2．1　ライブフォレンジックによる復号鍵の取得の研究

　2．2　プロセス情報とパケット情報の結合

3．ネットワークフォレンジックの研究

　3．1　LIFTシステムの研究

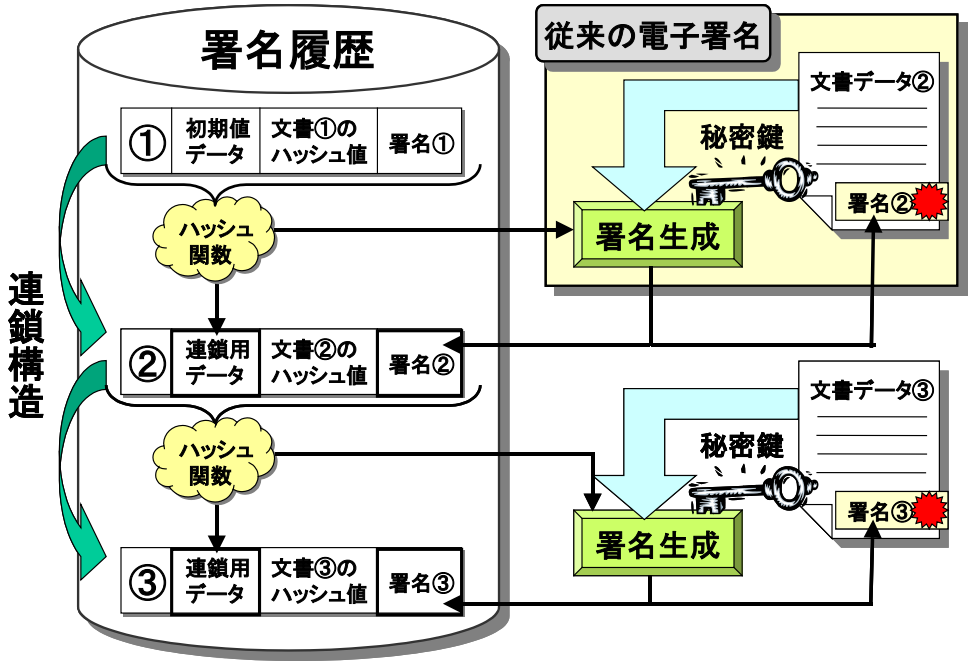
ヒステリシス署名の必要性

- 電子署名におけるアリバイ証明
  - 電子署名の存在の証明
  - 電子署名の順序性の証明

岩村充、宮崎邦彦、松本勉、佐々木良一、松木武「電子署名におけるアリバイ証明問題と経時証明問題 ヒステリシス署名と電子古文書の概念」bit, Nov.2000, Vol32,No.11

ヒステリシス署名

（署名nは連鎖構造を作るためのハッシュの対象としない方法もある）



初期の論文：上田　祐輔、佐々木良一他「データ喪失を想定したヒステリシス署名方式評価手法の提案」情報処理学会論文誌第45第8号 pp1966-1976,（2004年8月）
（ログに対する署名方法に関するもの）

佐々木らの主な研究

1．コンピュータフォレンジックに関する研究

　1．1　ヒステリシス署名を用いたログ改ざん検知システムの研究

2．ライブフォレンジックの研究

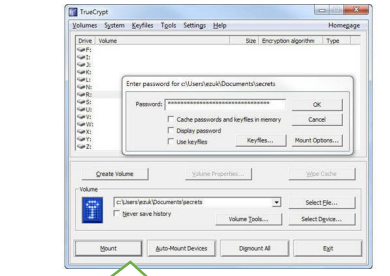
　2．1　ライブフォレンジックによる復号鍵の取得の研究

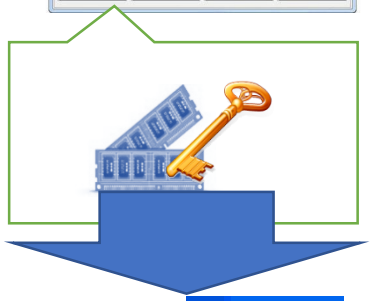
　2．2　プロセス情報とパケット情報の結合

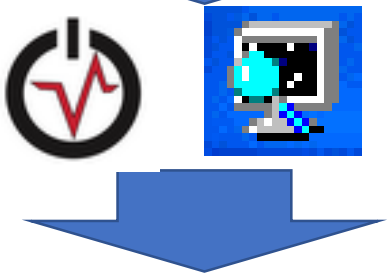
3．ネットワークフォレンジックの研究

　3．1　LIFTシステムの研究

ライブフォレンジックによる復号鍵の取得







トリガー発生

↓

①メモリダンプの取得

↓

②復号鍵の解析

↓

③復号を試みる

ランサムウエア
（TrueCrypt 利用）による
データの暗号化と恐喝

FTK Imager Liteを
使う

メモリーダンプ結果に対
し、aeskeyfindコマンドを
用いる

実験により復号できるこ
とを確認

竹林康太，上原哲太郎，佐々木良一「ライブフォレンジックを用いた暗号化ファイル復号技術の開発」情報処理学会CSEC研究会（2015年3月）

佐々木らの主な研究

1．コンピュータフォレンジックに関する研究
　1．1　ヒステリシス署名を用いたログ改ざん検知システム

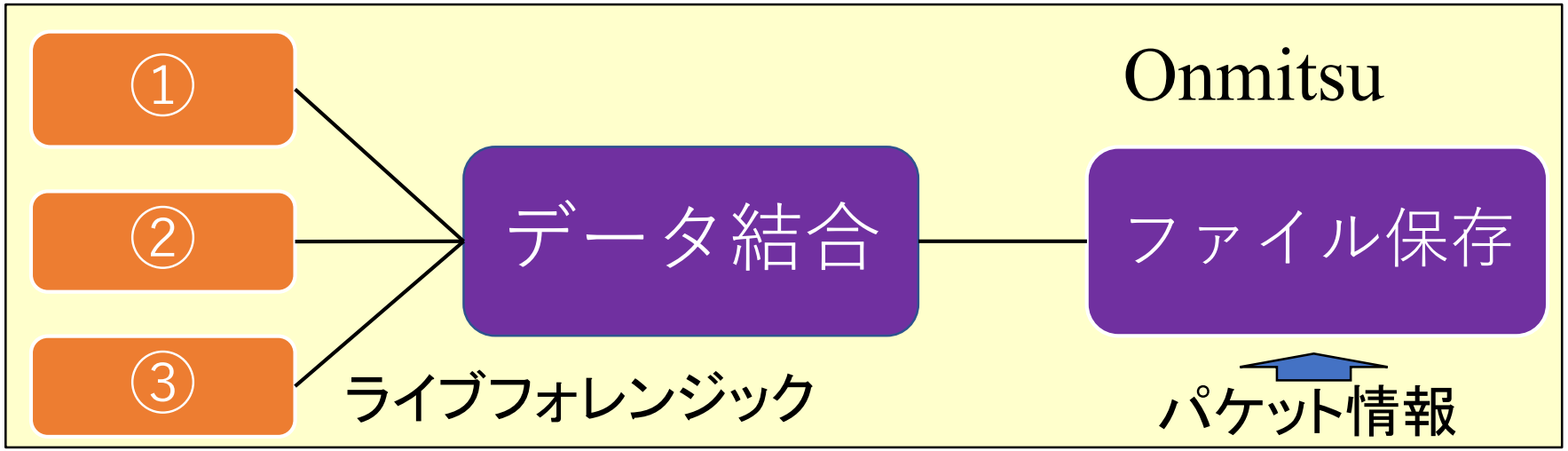
2．ライブフォレンジックの研究
　2．1　ライブフォレンジックによる復号鍵の取得の研究
　2．2　プロセス情報とパケット情報の結合

3．ネットワークフォレンジックの研究
　3．1　LIFTシステムの研究

Onmitsuにおけるライブフォレンジック

パケット情報と、PC内のプロセスの動きを関連付けて記録することにより、不正パケットが発信された原因などを明確化するツール

- Windows Filtering Platform - ①
- PsSetCreateProcessNotifyRoutineEx - ②
- PsSetLoadImageNotifyRoutine - ③



三村聡志，佐々木良一「プロセス情報と関連づけたパケットを利用した不正通信原因推定手法の提案」情報処理学会DICOMO2014

佐々木らの主な研究

1．コンピュータフォレンジックに関する研究
　1．1　ヒステリシス署名を用いたログ改ざん検知システム

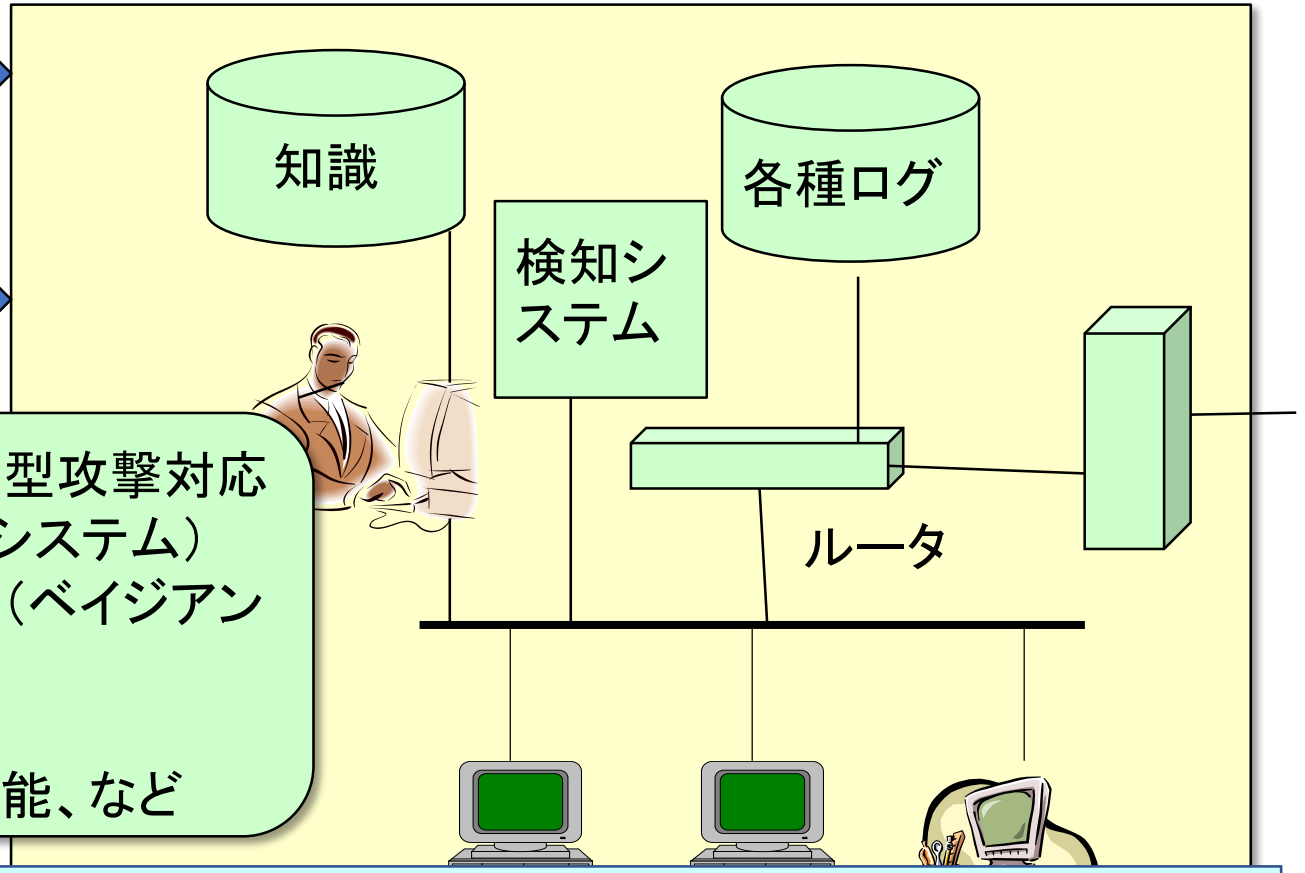
2．ライブフォレンジックの研究
　2．1　ライブフォレンジックによる復号鍵の取得の研究
　2．2　プロセス情報とパケット情報の結合

3．ネットワークフォレンジックの研究
　3．1　LIFTシステムの研究

LIFTプロジェクトの概要

①計画支援システム

②状況認識知識獲得用実験環境



③LIFTシステム（標的型攻撃対応自動運転・操作ガイドシステム）
（1）基本機能：AI技術（ベイジアンネットなど）の導入
（2）追加情報：
原因プロセス発見機能、など

共同開発プロジェクト （リーダ佐々木、上原先生、高倉先生、八槇先生、柿崎先生、日立他） 期間：2013年9月ー2018年3月（第一期）
現状での主な成果：① 方式確立 ②原因プロセス発見ソフト製品化

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