

e-Forensics 2008 参加報告

堀 良彰[†], 周 秉慧[‡], 櫻井 幸一[†]

† 九州大学大学院システム情報科学研究院情報工学部門

‡ 九州大学大学院システム情報科学府情報工学専攻

あらまし 本稿では、2008年1月21日から23日まで、オーストラリアアデレード市で開催された第1回情報通信とマルチメディアにおけるフォレンジック応用と技術に関する国際カンファレンス (e-Forensics 2008: First International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia) における研究発表を概説し、デジタルフォレンジックに関する研究開発動向を概観する。

e-Forensics 2008 Report

Yoshiaki Hori[†], Binhui Chou[‡], Kouichi Sakurai[†]

^{†,‡} Dept. of Computer Science and Communication Engineering,
Kyushu University

Abstract This article reports the First International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia (e-Forensics 2008), Aderade, Australia on January 21st to 23rd, 2008. We also look over research trends on digital forensics through research topics of e-Forensics 2008.

1 はじめに

情報通信技術を応用し構築されたさまざまなシステムが私たちの生活へ浸透するにつれて、そこで取り扱われるデジタルデータの証拠性確保技術およびその応用に関する研究分野、すなわちデジタルフォレンジック分野への社会的な要求が高まりつつある。近年、デジタルフォレンジックに関する会議が、多数開催されており、研究コミュニティ形成が進みつつある。

例えば、2005年より IFIP TC11 が設置したデジタルフォレンジックに関する WG 11.9 は “Digital Forensics Conference” 年次会議を開催している [1]。2001年より Digital Forensic Research Workshop (DFRWS) と呼ばれる年次会議が開催されている [2]。2005年より、Systematic Approaches to Digital Forensic Engineering (SADFE) ワーク

ショップ [3] も開催されている。

その他にも、デジタルフォレンジックス分野をカバーする専門ジャーナルとして、2004年に Elsevier 社からは Digital Investigation 誌 [4] が創刊され、2006年には IEEE Transaction on Information Forensics and Security [5] が創刊されている。

本稿では、2008年1月21日から23日まで、オーストラリアアデレード市で開催された第1回情報通信とマルチメディアにおけるフォレンジック応用と技術に関する国際カンファレンス (e-Forensics 2008: First International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia)) における研究発表を概説し、デジタルフォレンジックに関する研究開発動向を概観する。

2 e-Forensics 2008 会議

e-Forensics 2008 会議（以下、本会議とする）は、ブリュッセル本部に本部を置く The Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering (ICST) 主催, ACM SIGGRAPH, ACM SIGMM, アデレード大学 (The University of Adelaide), 豪州国防省国防科学技術部 (Defense Science and Technology Organization, Department of Defense, Australian Government) の共催で、豪州アデレード市にあるアデレード大学において開催された。

本会議の目的は、電子通信ならびに電子デバイスに関する不法活動が行われた可能性の検査を支援するためのツール開発、プロトコル、その他技法に関するデジタルフォレンジックに関する最新の研究成果を持ち寄ることである。根本的には、訴訟時における証拠の提示のための検査において必要となる経験と要求事項は、これらを議論する上で鍵となるものである。これには、デジタル証跡について、その発見・解析・取扱い・記録に関する事柄を含んでいる。これは、法的に証明能力を有するものであり、また、証跡の連鎖を形成するものである必要がある。

本会議のプログラムは、2件の基調講演、30件の講演形式および6件のポスター形式での研究発表から構成された。30件の講演形式の研究発表のうち27件は、次に挙げる特定のテーマにより9セッションとしてまとめられた。

- A1: Electronic Evidence and the Legal System
- B1: Video Analysis
- A2: Network Forensics
- B2: Voice and VoIP
- A3: Evidence Tracing
- B3: JPEG Image Analysis
- A4: Digital Memory Recovery
- B4: Watermarking
- A5: Forensic Sensing Technologies
- B5: Posters and Technology Demonstrators

本会議には、10か国以上の国から、70名ほどの参加者があった。そのうち、日本からの出席者は2名であった。

本節では以下に、基調講演およびプレナリ講演について紹介する。次節において、各セッション毎の研究発表について紹介する

2.1 基調講演

基調講演のひとつは、ボストンにある North-Eastern University の Patrick Wang 教授により、Intelligent Pattern Recognition Application in Biometrics と題して行われた。本基調講演では、バイオメトリクス情報を利用した関連技術において、対をなす分析技術 (analysis) と合成技術 (synthesis) について取り上げられた。例えば音声を例とすると、分析技術は周波数成分解析等組成を明らかにする技術、合成技術は解析によって得られた組成情報から音声合成を行うこととなる。デジタルフォレンジクスを考える上で、これらの分析と合成の技術を押さえる必要があるという講演であった。

もうひとつの基調講演は、West Midlands 警察において科学捜査官の経験を持ち、現在 Forensic Pathways Ltd 社、University College London の Richard Leary 博士により、The Role of E Forensics in the Developing Information Revolution Age と題して講演が行われた。本講演では、検査を科学的に見た場合それは推論プロセスであり、デジタル証跡を用いた検査においても、帰納的推定 (induction)、演绎的推定 (deduction)、仮説推定 (abduction) の手法が重要であるという講演であった。

2.2 プレナリ講演

プレナリ講演として、University of South Australia の Jill Slay 准教授による講演 Presenting digital evidence in a physical court room が行われた。University of South Australia には、2007年1月に防衛システム研究所 (Defense and Systems Institute) が設置されており、Slay 准教授はそこでサイバースペースにおける犯罪を対象としたデジタルフォレンジック研究チームを率いている。この講演では、法執行機関におけるデジタル証跡データの取扱いについては最低限の標準化しか行われておらず、ISO17025（試験所・校正機関のための品質規格）等の品質規格の適用等が課題であることが述べられた。

もうひとつのプレナリ講演として、RMIT Uni-

versity (メルボルン) の Gale Spring 准教授により、Photographic evidence: the challenges of digital photography as legal evidence と題して講演が行われた。特にディジタル写真について、証拠性の担保という点からの科学的考察が行われた。ディジタル写真はあくまで人工的に生成されるものであり、色調が正確さを求めることが困難であることや、視点の取り方等撮影時の要素によって生成される画像が変化するものであることを十分に考察すべきであるという講演であった。

3 各セッションにおける研究発表

本節では、各セッションにおける研究発表の一部について紹介する。小見出しの後の (A1) 等の記号はセッションにつけられた記号である。

3.1 Electronic Evidence and the Legal System (A1)

“The Adaptability of Electronic Evidence Acquisition Guides for New Technologies” (Benjamin Turnbull, Univ. of South Australia)

講演者は、捜査機関における証拠収集の手順書策定状況について概説した。各国の法制度による違いから、証拠収集の手順書はそれぞれの国において策定されている。中には、NIST の携帯電話やPDAに対するものなど特定のデバイスのためのガイドも作成されている。これらの多くのものは、2000年から2004年にかけて策定されているが、最近出現した新たなデバイスへの対応が必要であると主張している。無線端末、MP3/Videoプレイヤー、ゲーム機、VoIP(Voice over IP)関連機器のガイド整備の必要性を訴えた。

“Forensics in Cyber-Space. The Legal Challenges (INVITED PAPER)” (Nigel Wilson, Barrister)

サイバー空間におけるフォレンジック解析における法的問題に関して述べている。法的課題として、責任のグローバル化、司法権の所在(地)、新たなリスク、ペーパレス社会における文書と証拠性、応答と規制の即時性、解析者の独立性・客觀性・専門性、フォレンジック解析の商業化、人権とのかかわりという問題について述べた。

“Using a Room Metaphor for E-Forensic Working Environments” (Sabine Cikic, Technische Universität Berlin, et al)

e フォレンジックのための分散作業環境を構築す

るために、データと利用者を統合して管理するための「部屋」を分散システム上に構築しようとする提案について紹介された。筆者が取り組む “ViCToR”-Spaces (virtual cooperation in teaching and research for mathematics, natural sciences and engineering) プロジェクトでは、「部屋」をメタファーとした共同作業環境を構築している。この成果を e フォレンジックのための分散作業に応用にも応用できるであろうという説明であった。

3.2 Video Analysis (B1)

“Searching in Space and Time: A system for forensic analysis of large video repositories” (Anton van den Hengel, University of Adelaide)

ネットワーク対応の複数の監視カメラの映像を統合して解析を行うための枠組みに関する提案であり、カメラにより撮影されビデオ装置に記録された移動ターゲットについて、時間を追ってまたは時間をさかのぼって追跡する機能を有する。提案システムは、背景消去機能、カメラの設置位置から導出される移動体の位置推定機能の機能等、動的ターゲットを中心とした解析機能を有する。このシステムは筆者の大学キャンパスで試作されその有効性が検証されている。

“Optical Flow Image Analysis of Facial Expressions of Human Emotion . Forensic Applications” (Carmen J. Duthoit, University of Technology, Sydney, et al)

動きをベクトル化する手法であるオプティカルフロー解析を利用した人の表情から感情を推定する手法についての研究。各人の感情表現を表す感情ベクトル図により、特定の感情が推定できるかどうかについて調査を行ったところ、統計的に分析できることを明らかにした。この手法は、セキュリティやフォレンジックにも応用できると述べている。

3.3 Network Forensics (A2)

“Methods to identify spammers” (Tobias Eggerdorfer, Universitat der Bundeswehr Munchen)

スパムの送出は組織化され、メッセージ作成者、ポット運用者などが協調してスパム送出を行っている。また、スパムの多くは合法または違法の商品販売であり、商品発送者から E メールアドレスの収集者、代金回収者までさまざまな役割を担うものが連携して、スパムビジネスが行われている。

これらスパマーを特定するためには、E メールメッセージの分析、ポットネットの観測、購入者の観測、連携店の発見、代金支払いプロセス、店舗を運用しているウェブサーバ所有者を見つける必要がある。筆者は、HTTP tar pit と呼ばれる、E メールアドレス収集者を仮想的なウェブページのアクセスを繰り返させることで罠にはめる手法を提案している。E メールアドレスにわざと生成したアドレスを与えることで、E メールアドレス収集者とスパム送信者を関連づけることができるとしている。

“Conducting Forensic Investigations of Cyber Attacks on Automobile In-Vehicle Networks” (Dennis K. Nilsson, Chalmers University of Technology, et al)

車載ネットワークは、これまで物理的に隔離された領域で攻撃は想定されていなかったが、これが無線アクセス網を介して接続されることにより車外からの脅威にさらされることになる。そこで、講演者らは車載ネットワークにおけるデジタルフォレンジックについて、攻撃者を想定した上で、イベント検出機能、保存されるべきデータ、保存されるべき状態等の要求要件を述べている。

3.4 Voice and VoIP (B2)

“Voice over IP Forensics” (Jill Slay, University of South Australia)

VoIP (Voice over IP) 技術は、インターネット通信基盤上で電話サービスを可能にする。法執行者が VoIP において直面している問題は、従来の電話交換機網の場合と大きく異なっている。電話回線の盗聴は、VoIP に対して適切ではなく、パケットキャプチャによるデータ参照は暗号化によって不可能となる。講演者らは、犯罪の疑いのある活動や通信において VoIP による通話は重要であることを述べ、VoIP の証跡を保存するためにメモリイメージの修得による方法について研究しており、メモリイメージから音声ファイルを再構成することができたという報告がなされた。

“Hiding Skype VoIP Calls from Parametric Identification” (Mauro Migliardi, University of Genoa, et al)

VoIP として広く使われている Skype のトラヒックに関して、パケットサイズとパケット到着間隔を統計的に評価することにより、Skype のトラヒック

であることを判別する手法を開発した。この手法を実証するために試作し、数秒間のトラヒック観測により 95%以上の正確さで Skype のトラヒックを検知できることを実証した。また、このような検出手法を回避するための手法についても考察した。

“Automatic Voice Activity Detection in Different Speech Applications” (Marko Tuononen, University of Joensuu, et al)

4種類のデジタル音声サンプルに関して、エネルギーベースのおよび長期間スペクトルダイバージェンス法 (long-term spectral divergence) の2つの方法を用いた音声部分検出器 (VAD: Voice Activity Detector) の性能を評価した。音声部分検出器は、音声認識、音声バイオメトリクス等を適用する際の基礎技術である。これらの手法はノイズを含むデータに対しても有用であることがわかった。

3.5 Evidence Tracing (A3)

“Cheat-Prevention and -Analysis in Online Virtual Worlds” (Sabine Cikic, Technische Universität Berlin, et al)

仮想環境やオンラインゲームの市場が形成され、そこでの仮想所有物は、実世界の金銭を用いて取引されることもあり実際の価値を有するものとなっている。このような仮想所有物に関する法的な問題についてはまだ決定的でない状態である。仮想所有物を保護するために、仮想環境はいくつかの要件を持っていることを確認する必要がある。

“The Design of Framework for Detecting an Insider’s Leak of Confidential Information” (Eunju Baek, Korea University, et al)

組織からの情報漏洩の問題に関して、従業員の E メール、インスタントメッセージ、P2P などの管理が不十分であることおよびそれらは内部からの情報漏洩を引き起こすことを説明した。講演者らは、フォレンジックという観点からこの問題への解決を試み Windows レジストリ、メッセンジャー、E メールを解析し、情報漏洩を検出するために各端末の状況を収集し監視サーバに集めるフレームワークについて考察している。さらに、2 次記憶メディアからの情報漏洩についても考察している。

“Timestamp evidence correlation by model based clock hypothesis testing” (Svein Yngvar Willassen, Norwegian University of Science and Technology)

デジタル情報を調査する上で重要な役割を担うタイムスタンプについて、コンピュータのクロックは信頼できる正確さがないということを前提にモデル化を行い、その上でタイムスタンプの正当性について検証するための手法について述べている。システムクロックを故意に設定変更するようなことがあった場合、それを検出できることを示している。さらに、具体的な事例として、ファイルシステムにおいて記録される、ファイル生成、ファイル更新、ファイルアクセスの際に記録されるタイムスタンプについてその数値の関係を調査することにより、タイムスタンプにより提供される順序性について考察している。

3.6 JPEG Image Analysis (B3)

“Advanced Jpeg Carving” (Michael I. Cohen, Australian Federal Police)

本研究は、Data Carving と呼ばれる構造を持たないデータからファイルを再構成する技術を、JPEG ファイルに対して適用し、何らかの要因で一部のデータが欠落または置換され、一部が復元できなくなった JPEG 画像において、Data Carving を適用することにより、データ構造を再構成し、出来る限り広い部分の復元を試みたものである。このような技術はディジタルフォレンジック技術として有用である。

B32: “Image Tampering Detection Using Bayer Interpolation and JPEG Compression” (Marie-Charlotte Poilpre, Institut Supérieur des BioSciences, Paris, et al)

イメージファイルに対する一部改変について、それを検出する 2 つの手法について研究を行っている。いずれもフーリエ領域における特徴を利用するもので、第一の方法は CCD におけるカラーフィルタの配列の規則性を利用する方法で、第二の方法は JPEG 圧縮の特徴を利用したものである。これらの 2 つの手法は補完的に利用できることについて明らかにした。

“Conditions for Effective Detection and Identification of Primary Quantization of Re-Quantized JPEG Images” (Matthew James Sorell, University of Adelaide)

JPEG イメージにおける量子化表の選択は、デジタルカメラの識別において有用であることが知られている。しかしながら、写真を再圧縮した場

合、二次量子化が行われることになる。講演者らの研究では、一次量子化における計数を推定することにより、デジタルカメラデバイスを絞り込むことができるとしている。

3.7 A4: Digital Memory Recovery

“Recovering data from USB Flash memory sticks that have been damaged or electronically erased (Invited Paper)” (B. J. Phillips, University of Adelaide, et al)

小型の情報格納デバイスとして一般化している USB フラッシュメモリスティックについて、物理的あるいは電気的ダメージを与えたあと記録された情報の読み出しを試みたという研究報告である。USB フラッシュメモリスティックに与えるダメージとしては、過電圧の印加、水ぬれ、ガソリンを使っての焼却、足での踏みつけ、ハンマーでの強打、ピストルによる射撃、電子レンジでの加熱を試みている。これらの攻撃を受けた後でも、データの読み出しが可能であった場合が多く見られたことが報告された。

“Recovery of Circumstantial Digital Evidence Leading to an Anton Piller Order: A Case Study” (Roland MacKenzie, University of Adelaide, et al)

イギリス等の国では、民事訴訟において、anton・ピラー命令と呼ばれる裁判所の特殊権限があり、裁判所は、原告が犯罪に関する調査証拠の収集するための許可を、被告への事前通告なしに出すことができる。講演者らは、会社を退職した後、顧客データベースを不正に利用して、顧客を奪った恐れのある前従業員に対するanton・ピラー命令許可を修得するにあたり、顧客データベースのアクセスパターンを解析し、その証拠として裁判所に申請したケースについて報告した。

3.8 Forensic Sensing Technologies (A5)

“Explosive Blast Effects on Latent Fingerprints” (V.A. Kuznetsov, Defence Science and Technology Organisation, AU, et al)

講演者らは、指紋証跡に対する爆風の影響について調査を行った。4 つのアルミ板と 2 つの鉄板に指紋を付けておき、0.25m から 1m の距離において 0.7kg の火薬による爆風にさらし、指紋が復元できるかどうかを調査した。その結果、板は爆風により変形しても、Cyanoacrylate Fuming 法に

より、指紋を復元できることが確認された。

4 デジタルフォレンジック研究への期待

情報通信技術の深化によって、これまで車載 LAN などこれまで公衆インターネットに接続されていなかった領域へのアクセスが可能になる。そこでは、これまで想定していなかった新たな脅威を想定し、デジタルフォレンジックの観点から対応を迫られる。

その他に、VoIP など利用者へのサービスとしては従来の電話網と同じサービスが提供されるが、技術的には従来の盗聴方式が全く適用できないものについては、新たな証拠確保手段の研究開発が必要であろう。そこでは、通話している音声を録音し、それにより通話者を明らかにするという従来の方法とはことなり、通話する音声を記録することなく通話者や通話内容を推定する必要が出てくるであろう。

また、デジタル音声レコーダーや、今や数年前の PC をしのぐ機能を有するゲームコンソール等新たなデバイスや、オンラインゲーム等新たなアプリケーションの登場による仮想アイテムの実取引等これまでにない新たな決済、取引にも対応を迫られる。これらについてもフォレンジック技術の対象として必要な技術を整備していくべきと考えられる。

5 終わりに

本稿では、第1回情報通信とマルチメディアにおけるフォレンジック応用と技術に関する国際カンファレンス (e-Forensics 2008: First International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia)) における研究発表を概説し、デジタルフォレンジックに関する研究開発動向を概観し、デジタルフォレンジック分野に期待される事項について考察した。

参考文献

- [1] IFIP Working Group 11.9 on Digital Forensics Conferences, <http://www.ifip119.org/Conferences/>, 2008-04-20.
- [2] DFRWS: Digital Forensic Resarch Workshop <http://www.dfrws.org/>, 2008-04-20
- [3] Systematic Approaches to Digital Forensic Engineering (SADFE), <http://conf.ncku.edu.tw/sadfe/index.htm>, 2008-04-20.
- [4] Digital Investigation, Elsevier <http://www.elsevier.com/locate/diin>, 2008-04-20.
- [5] IEEE Transactions on Information Forensics and Security, <http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206>, 2008-04-20.
- [6] D.E. Knuth, *The METAFONT book*, Addison Wesley Publishing Company, 1986.