社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2009－DPS－138 (33)
2009－CSEC－ 44 (33)
2009／3／6

IT Forensic の研究開発動向 ～ アジア国際ワークショップ開催報告 ～

高橋健一[†] 堀 良彰[†,††] 櫻井幸一[†,††]

International Joint Workshop on Computer Forensics を情報通信研究機構（NICT）国際共同研究助成を受けて「ディジタルフォレンジックに関する研究開発」の一環として行った．本ワークショップはアジアの研究者を集め，2008 年 12 月 15 日-16 日に福岡にある SRP センタービルで開催した．本報告ではワークショップで発表された研究を通して，ディジタルフォレンジックの研究開発動向，標準化動向ならびに個々の研究内容に関して報告する．

Researches on IT Forensics from International Joint Workshop on Computer Forensics

KENICHI TAKAHASHI,[†] YOSHIAKI HORI[†,††] and KOUICHI SAKURAI[†,††]

We held on International Joint Workshop on Computer Forensics at SRP center building, Fukuoka, Japan, on 15th and 16th, December, 2008. This workshop is held as the part of "Researches on Digital Forensics" supported by International Collaborative Research Project of National Institute of Information and Communications Technology (NICT). In this report, we introduce the researches presented in the workshop with the standardization and future research topics on digital forensic.

1. はじめに

我々は情報通信研究機構（NICT）国際共同研究助成[1] から「ディジタルフォレンジックに関する研究開発」という題目で研究助成を受けた．これは日本の九州先端科学技術研究所（ISIT），九州大学，長崎大学，KDDI 研究所，韓国の韓国電子通信研究院（ETRI），高麗大学，中国の清華大学の研究者からなるプロジェクトであり，本プロジェクトの研究概要は

「情報通信技術を応用し構築された種々の情報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ィ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への社会的な要求が高まりつつある．情報通信技術の深化は，これまで接続されていなかった領域へのアクセスを可能にし，新たなサービスを実現する．そのような領域においては，新たな証拠確保手段が必要となることから，技術的観点ならびにそれらを有効に機能させる社会制度について考慮しつつ必要とされる研究開発を実施する（図 1）．」

となっており，表 1 がプロジェクトのメンバである．

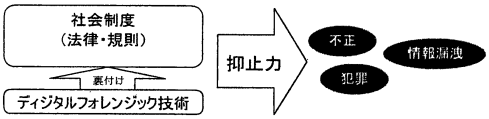

図 1 プロジェクト概要

本プロジェクトの一環として International Joint Workshop on Computer Forensics[2] を 2008 年 12 月 15 日-16 日に福岡市百道浜にある SRP センタービルで開催した．本報告ではワークショップで発表された研究を通して，ディジタルフォレンジックの研究開発動向，標準化動向ならびに個々の研究内容に関して報告する．

† （財）九州先端科学技術研究所
Institute of Systems, Information Technologies and Nanotechnologies
†† 九州大学大学院システム情報科学研究院
Faculty of Information Science and Electrical Engineering, Kyushu University

表 1　プロジェクトメンバ

日本側メンバ	
	櫻井幸一（九州先端科学技術研究所，九州大学）
	高橋健一（九州先端科学技術研究所）
	堀良彰（九州大学）
	上繁義史（長崎大学）
	田中俊昭（KDDI 研究所）
	福島和英（KDDI 研究所）
韓国側メンバ	
	Dowon Hong（ETRI）
	SungKyong Un（ETRI）
	Kyoil Chung（ETRI）
	DongHoon Lee（高麗大学）
	Sangjin Lee（高麗大学）
	HyungJoong Kim（高麗大学）
中国側メンバ	
	Kwok-Yan Lam（清華大学）

2. International Joint Workshop on Computer Forensics

本ワークショップには日本から 8 名，韓国から 8 名，中国から 3 名が参加し，計 18 件（日本：7 件，韓国：8 件，中国：3 件）の発表が行われた．ワークショップではコンピュータフォレンジックの研究動向を紹介する Overview of Computer Forensics セッション，ハードウェアが関わる研究に関する HW and Live Forensics セッション，フォレンジックツールに関する Forensics Tool セッションとその他の研究に対する Certification, Steganography, ML and Biometrics セッションを設けた．プログラムを付録に示す．

2.1 ディジタルフォレンジック関連会議・研究動向

九州大学の堀からディジタルフォレンジック関連の会議や研究動向（IT Forensic and Network Management）が報告された．ディジタルフォレンジックは，かつて，法執行機関である警察や検察におけるディジタルデータの証拠収集技術を指し，集められたディジタルデータは法廷において事実を証明するに足るものであることが求められた．それに加えて，近年，会社や学校といった組織における管理やコンプライアンスを目的とした利用，組織の中における規則違反の抑止力としてディジタルフォレンジックを利用することが着目されている．このため，ディジタルデータを証拠として利用できるための制度，すなわち，証跡確保技術およびその運用過程の標準化が求められている．

ディジタルフォレンジクスに関する専門書は 2000 年代中期には Computer Crime と Digital Forensics というキーワードでいくつかの専門書[3)~6)] が刊行され，2000 年代後期にはハンドブック[7)] やソフトウェアを集めたツールキット[8)]，ライブラリ集[9)]，フィールドマニュアル[10)] などが刊行されている．これらはディジタルフォレンジック技術が広く一般に普及しつつあることを示唆している．

ディジタルフォレンジックに関する研究コミュニティに関しては 2001 年に Digital Forensics Research Workshop (DFRWS)[11)] が発足し，年 1 度のワークショップを開催している．2005 年には情報処理国際連合（IFIP: International Federation for Information Processing）の情報セキュリティ関連分野を扱う技術委員会 TC11 の下に，ディジタルフォレンジクスに関する作業グループ（WG11.9: Digital Forensics)[12)] が置かれ，年 1 度のワークショップを開催している．他，2005 年から Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE)，2006 年から学会型研究コミュニティ ADFSL: Association of Digital Forensics, Security and Law，2008 年からヨーロッパに本部を持つ学会 ICST や ACM SIGMM, ACM SIGSAC 等が主催する International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia (e-Forensics) 等，ディジタルフォレンジクスに関する研究コミュニティが 2000 年代初頭から中期にかけて誕生している．

また，2000 年代中期から後期にかけてディジタルフォレンジックの中でも特定の分野について集中的に議論を行う国際会議が多数開催されている．例えば，IT インシデント管理・インシデント解析と IT フォレンジックスを扱う会議として，The 4th International Conference on IT Incident Management & IT Forensics や The 3nd International Annual Workshop on Digital Forensics & Incident Analysis がある．また，コンピュータとネットワークフォレンジックのためのオープンソースソフトウェアに焦点をあてた会議として The 1st Workshop on Open Source Software for Computer and Network Forensics がある．

学術雑誌としては 2004 年に Elsevior 社が Digital Investigation 誌，2006 年に IEEE Computer Society が IEEE Transactions on Information Forensics and Security 誌，2007 年，Taylor & Francis 社が Journal of Digital Forensic Practice 誌を創刊するなど，2000 年代中期以降多数の学術雑誌が創刊されている．

近年のディジタルフォレンジック研究を見ると，PDA（Personal Digital Assistant）やゲームコンソール，無線端末機器など，新たなデバイスへの対応をはじめ，VoIP（Voice over IP）や Vehicular Network など新たなサービスにおける証跡収集など，研究の対象に広

がりを見せている．

一方，ISIT の藤井から報告された日本でのディジタルフォレンジック関連商品（The Research of Computer Forensic Products in Japan）を見ると，(HDD 上のデータを解析する）コンピュータフォレンジック関連製品のほとんどはアメリカで開発されたもので，日本ではネットワークフォレンジック関連製品の開発に注意が向けられており，そのほとんどがアプリアンスとして提供されている．

2.2 ディジタルフォレンジックの標準化動向

ISIT，九州大学教授の櫻井からディジタルフォレンジックの標準化動向（Current status on Regulation and standardization of IT-forensic）について報告された．デジタルフォレンジックは特殊技術から学術研究やビジネス利用の段階に来ており，実利用のための標準化が国際的なレベルで始まっている．

ISO/IEC JTC1 SC27/WG4 では 2008 年 4 月の京都会合において，マレーシアから Evidence acquisition procedures for digital forensics と題したテーマが Study Period として提起された．これを受けて，2008 年 10 月のキプロス会合では Guidelines for Identification, Collection and/or Acquisition and Preservation of Digital Evidence というタイトルで規格化[13] がはじまった．ここでのスコープは

> The standard will provide detailed guidance on the identification, collection and/or acquisition, marking, storage, transport and preservation of electronic evidence, particularly to maintain its integrity. It will define and describe the process of recognition and identification of the evidence, documentation of the crime scene, collection and preservation of the evidence, and the packaging and transportation of evidence.

と記述されており，証跡収集のための具体的なガイドラインを作成しようとしていることが分かる．Maslina Daud（マレーシア）と Kyung-Seok Lee（韓国）が Acting editors として，2009 年 5 月に予定されている北京会合で初稿を準備することになっている．

ITU-T では 2008 年の時点で 2009 年から 2012 年における新課題の 1 つに ICT forensics を挙げている．具体的には ITU-U SC17 において 2008 年 9 月に ETRI（韓国）から検討課題として，

- Test methodology for ICT forensics system
- Digital evidence exchange format
- ICT forensic system framework
- Protection procedure of ICT forensic system

の 4 つが挙げられている．

電子透かしをはじめとするマルチメディアフォレンジックの規格化[14] も重要な課題であるが，これには既存の JPEG/MPEG 規格との整合性が注意される必要がある．

規格化と並んで法制度面にも注意がいる．電子犯罪対策のためのフォレンジックに対して，個人情報保護のために証拠・履歴を残さないアンチフォレンジック技術[15] も研究・ビジネス展開されており，これにも注意を払う必要がある．

2.3 携帯電話を対象としたディジタルフォレンジック

KDDI の田中の発表（Research Activities and Digital Forensics in KDDI R&D Laboratories, Inc.）では携帯電話に必要なディジタルフォレンジックについての紹介があった．現在の携帯電話は様々なメディアをサポートしており，様々なモニタリングポイントでフォレンジックデータを取得できるアーキテクチャが必要であることや，携帯電話とネットワークセンターの両方にディジタルフォレンジックが必要であることが述べられた．

また，高麗大学の Keunduck Byun からも携帯電話を対象とした研究報告（Cell Phone Forensics : Collection & Analysis）が行われた．Keunduck Byun らは Mobile Evidence Collector と Mobile Data Analyzer を開発し，それによって携帯電話中のバイナリデータから SMS や通話履歴，電話帳等のデータを復元できたことが報告された．

2.4 ディジタルフォレンジックのための生体認証

清華大学の KwokYan Lam と Jinyang Shi からディジタルフォレンジックのために生体認証を利用することについての提案（Biometric Cryptography: Challenge and Opportunity for IT-Forensic，Biomapping: Secure the Biometrics Using Noninvertible and Discriminable Constructions）が行われた．発表ではユーザのプライバシを守るために暗合化が必要であること，ロジカル ID とフィジカル ID の結びつけが必要であること，取得されたデータを証拠として利用可能な状態で保存できることが必要だとし，そのために彼らが研究している Biometric Cryptography（図 2）が利用可能であることを紹介した．

2.5 ETRI でのディジタルフォレンジック研究

Youngsoo Kim から ETRI のディジタルフォレンジック研究についての紹介（Current Forensic Re-

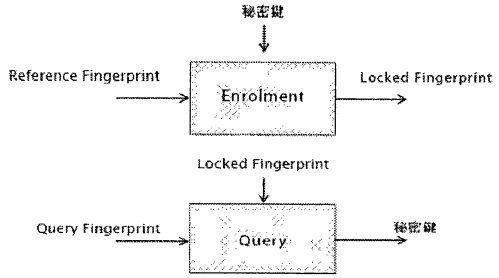

図 2　Biometric Cryptography 概要

search in ETRI）があった．ETRI では高速大容量のデータを解析するための High Speed Forensic System，メモリデータやレジストリのデータを解析するための Live Data Forensic System，JTAG インタフェースから携帯電話のデータを取得し解析する Mobile Data Forensic System，クライアントサーバモデルでフォレンジックデータを管理するための Enterprise Security Forensic System を開発しており，それらの簡単な概要が紹介された（図 3）．また，高速なパスワードリカバリーツールが High Speed Forensic System の一部の機能として Keonwoo Kim から詳細な紹介（GPU Acceleration for High-Speed Password Recovery）が行われた．

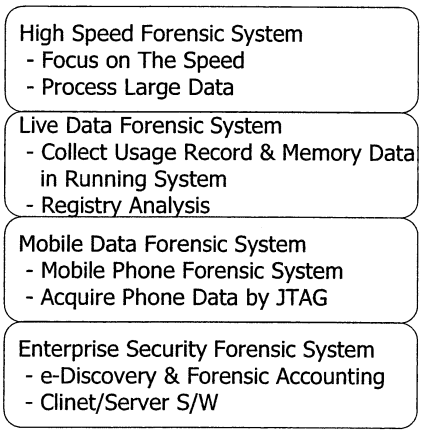

図 3　ETRI のディジタルフォレンジックシステム

2.6 そ の 他

高麗大学の Kyoungsoo Lim からは Live Forensic ツール，LDFS の紹介（LDFS: A New Live Forensic Tool）が行われた．LDFS では，ユーザが何を目的としてデータを取得するかを Scenario-based や Case Type-based，Crime Scene Situation-based といった基準で指定することによって，ユーザが目的としたデータを自動的に収集・解析する．

高麗大学の Jewan Bang からは削除されたファイルを復元するためのツールの紹介（Enhanced Data Recovery Tool）が行われた．彼らのツールでは，バイナリコードからファイルのヘッダやフッタなどのデータを取得し，その情報を利用することでファイルを復元する．

高麗大学の Jaemin Choi は財務会計情報を分析し，改竄の検知に利用するための研究（A Study of Forensic Accounting Techniques to Financial Fraud Symptom Detection）が紹介された．

KDDI の福島は CAD で作成された VHDL コードの不正コピー利用を検出するための研究（Forensic Watermark to Detect Illegal Copying of CAD Tools）を紹介した．福島は VHDL コードに透かし情報を埋め込むための方法を幾つか述べ，それぞれのメリット・デメリットの比較を行っている．また，高麗大学の Md Amiruzzaman（Steganography: A Secret Communication Medium）と HyungJoong Kim（Status of Reversible Data Hiding）からも電子透かしに関する研究紹介が行われた．

九州大学の周はフォレンジックのためにログを考え直す必要があるという問題提起（Requirements of Purpose-based Forensic Logging）を行った．現在，記録されているログはシステムの動作を記録するためのものであり，フォレンジックのために利用できるが，フォレンジックのために考えられたものではない．また，組み込みシステムなどの低能力のデバイスではログを十分に記録することは難しいかもしれない．このため，フォレンジックのためにどのような情報が必要になるか再考し，ユーザの意図に沿って必要なログだけを取得し，また，フォレンジックのために現在のログだけでは足りない情報を明らかにしなければならないという主張が行われた．

ISIT の高橋は（closed な）メーリングリストを対象とし，スパムメールが届いたときに誰がスパムメール発生の原因になったかを突き止めるためのシステム（Finding Mailing-list Address Leakers towards Spam Mail Blocking）を紹介した．提案システムではメーリングリスト投稿用アドレスを利用することで，ユーザへの負荷をほとんど与えずにスパムメール発生の原因になったメンバを特定し，スパムメールを止めることができることが示された．

清華大学の Ge Meng は Mobile Ad-hoc Network を対象とした分散認証方式（MANET based on the

Fully Distributed Certificate Authority (FDCA) approach）を提案した．彼らは Threshold cryptography を用いることで安全な分散認証方式を実現している．

3. おわりに

2008年12月15日-16日に福岡市百道浜にあるSRPセンタービルで開催した International Joint Workshop on Computer Forensics の報告を行った．本ワークショップは日韓中の研究者を集めて組織した情報通信研究機構（NICT）国際共同研究助成「ディジタルフォレンジックに関する研究開発」プロジェクトの一環として開催した．本報告ではワークショップの報告されたディジタルフォレンジックに関する研究や研究動向，標準化動向に関して報告した．

謝辞 本研究，および，International Joint Workshop on Computer Forensics は情報通信研究機構（NICT）国際共同研究助成「ディジタルフォレンジックに関する研究開発」（研究代表：櫻井幸一）を受けて行った．

参考文献

1) NICT 国際共同研究助成金, http://www2.nict.go.jp/q/q266/s807/7_2l.html#p20.
2) International Joint Workshop on Computer Forensics, http://www.isit.or.jp/lab2/kouryu/2008/NICT/index.html.
3) Eoghan Casey, Digital Evidence and Computer Crime, Second Edition by, Mar. 2004.
4) Keith J. Jones, Richard Bejtlich and Curtis W. Rose, Real Digital Forensics: Computer Security and In Response, Oct. 2005.
5) Brian Carrier, File System Forensic Analysis, Mar. 2005.
6) Panagiotis Kanellis, et al, Digital Crime And Forensic Science in Cyberspace, May. 2006.
7) John J. Barbara, Handbook of Digital and Multimedia Forensic Evidence, Dec. 2007.
8) Harlan Carvey and Dave Kleiman, Windows Forensic Analysis Including DVD Toolkit, Apr. 2007.
9) Keith J. Jones, Richard Bejtlich, Curtis W. Rose and Dan Farmer, Computer Forensics Library Boxed Set, Aug. 2007.
10) Jr., Albert Marcella and Doug Menendez, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition, Dec. 2007.
11) DFRWS (Digital Forensics Research Conference), http://www.dfrws.org/.
12) IFIP Working Group 11.9 on Digital Forensics, http://www.ifip119.org/.
13) Other ISO/IEC 27k standards, http://www.iso27001security.com/html/other_27k.html.
14) Multimedia forensics bibliography, http://www.cl.cam.ac.uk/~abl26/bibliography/main/sort/category.html.
15) Hamid Jahankhani, Elidon Beqiri, Memory-Based antiforensic tools and techniques, International Journal of Information Security and Privacy, Volume 2, Issue 2, pp. 1-13, 2008.

表 2 付録：ワークショッププログラム

2008 年 12 月 15 日

10:00-10:10	Opening Prof. Kouichi Sakurai
	Session I Overview of Computer Forensics Chair Prof. Yoshiaki Hori
10:10-10:35	IT Forensic and Network Management Prof. Hori (ISIT, Kyushu Univ.)
10:35-11:00	Current Forensic Research in ETRI Dr. Youngsoo Kim (ETRI)
11:00-11:25	Research Activities and Digital Forensics in KDDI R&D Laboratories, Inc. Dr. Toshiaki Tanaka (KDDI)
11:25-11:50	Current status on Regulation and standardization of IT-forensic Prof. Sakurai (ISIT & Kyushu Univ.)
11:50-12:15	Biometric Cryptography: Challenge and Opportunity for IT-Forensic Prof. KwokYan Lam (Tsinghua Univ.)
	Session II HW and Live Forensics Chair Prof. KwokYan Lam
14:00-14:25	Cell Phone Forensics : Collection & Analysis Mr. Keunduck Byun (Korea Univ.)
14:25-14:50	GPU Acceleration for High-Speed Password Recovery Dr. Keonwoo Kim (ETRI)
14:50-15:15	LDFS: A New Live Forensic Tool Mr. Kyoungsoo Lim (Presenter: Mr. Jewan Bang) (Korea Univ.)
15:15-15:40	Requirements of Purpose-based Forensic Logging Ms. Binhui Chou (Kyushu Univ.)
	Session III Forensics Tool Chair. Prof. Sakurai
16:00-16:25	The Research of Computer Forensic Products in Japan Mr. Masakazu Fujii (ISIT)
16:25-16:50	Forensic Watermark to Detect Illegal Copying of CAD Tools Mr. Kazuhide Fukushima (KDDI)
16:50-17:15	 Mr. Jewan Bang (Korea Univ.)
17:15-17:40	A Study of Forensic Accounting Techniques to Financial Fraud Symptom Detection Mr. Jaemin Choi (Korea Univ.)

2008 年 12 月 16 日

	Session IV Certification, Steganography, ML and Biometrics Chair HyungJoong Kim
10:00-10:25	Ubiquitous and Secure Certificate Service for IT-forensic applications in MANET Mr. Ge Meng (Tsinghua Univ.)
10:25-10:50	Finding Mailing-list Address Leakers towards Spam Mail Blocking Dr. Kenichi Takahashi (ISIT)
10:50-11:15	Status of Reversible Data Hiding Prof. HyungJoong Kim (Korea Univ.)
11:15-11:40	Biomapping: Secure the Biometrics Using Noninvertible and Discriminable Constructions Mr. Jinyang Shi (Tsinghua Univ.)
11:40-12:05	Steganography: A Secret Communication Medium Mr. Md Amiruzzaman (Korea Univ.)
12:05-12:10	Closing Prof. Sakurai (ISIT & Kyushu Univ.)