Computer Security Symposium 2017
23 - 25 October 2017

日本におけるデジタル･フォレンジックの動向

佐々木　良一[†1]

概要：サイバー攻撃の激化や民事訴訟の増加などにより，デジタル･フォレンジックが重要性を増している．デジタル・フォレンジックというのは種々のインシデントが発生した際に，将来行われうる裁判で証拠として使用できるようにするための電磁的記録の収集や分析の技術およびその手順のことである．その重要性の増大にもかかわらず，日本におけるデジタル･フォレンジックの研究者の数は非常に少なく，論文の数も少ない．本稿では，日本におけるデジタル･フォレンジックに関する研究を活性化するため，デジタル･フォレンジックが必要になってきた背景や，適用の状況を概説する．次に，日本における研究動向を示すために著者らが行ってきた種々の研究を紹介する．そして，今後重要となるデジタル･フォレンジックの技術動向と必要となる研究について考えを述べる．

キーワード：デジタル･フォレンジック，ネットワーク･フォレンジック，動向，日本

Trend on Digital Forensics in Japan

Ryoichi Sasaki[†1]

Abstract: Digital forensics are increasingly important due to targeted cyber attacks and increased civil lawsuits. Here, the digital forensic is a technique and procedure for the collection and analysis of electromagnetic records to make it possible to use it as evidence in future trials when various incidents occur. Nevertheless, the number of digital forensic researchers in Japan is very limited, and the number of articles is small. In this article, in order to revitalize research on digital forensics in Japan, we outline the background of the necessity of digital forensics and the application situation in Japan. Next, in order to show the research trends in Japan, we describe the researches that we have done. Then, the technical trend of digital forensics which will become important and the thought about necessary research will be described.

Keywords: Digital Forensics, Network Forensics, Trend, Japan

1. はじめに

内部不正やサイバー攻撃などによって大量の個人情報が企業などから漏えいする事案がしばしば起きている．このような場合に漏えい経路はどこか，どの程度の規模の情報が漏えいしているのか，だれが不正者か等を早急に明確にし，きちんと説明できるようにしないと組織の信頼を失ってしまう．また，不正者を民事訴訟で訴えようとしても証拠がないと裁判に勝つことができない．

このように種々のインシデントが発生した際に，コンピュータなどの情報処理機器上に残された証拠を確保し将来起こりうる裁判に備える技術や手順が必要になる．これが，ここで対象とするデジタル・フォレンジック（Digital Forensics）である．したがって，デジタル・フォレンジックは「種々のインシデントが発生した際に，将来行われうる裁判で証拠として使用できるようにするための電磁的記録の収集や分析の技術およびその手順」[1]と定義してよいだろう．

ここでのインシデントとは，サーバーへの不正侵入など情報処理装置に関連するインシデントだけでなく，殺人事件や窃盗などの刑事事件，談合（独占禁止法違反），営業秘密の不正な持ち出し（不正競争防止法違反），プライバシーの侵害，掲示板への書き込みによる名誉毀損，インサイダー取引，医療過誤などいろいろなものがあり，デジタル・フォレンジックは民間だけではなく警察や検察庁，金融庁，公正取引委員会などの公的機関でも重要性が高まっている．

デジタル・フォレンジックの普及・促進を図り健全なIT社会の実現に貢献するために2004年に設立されたデジタル・フォレンジック研究会の個人会員は，当初の85人から2017年時点で259人，法人会員は25団体から59団体へと大幅に増加している．また，インシデントレスポンスにおいてデジタル･フォレンジック技術が調査や捜査に使われるだけでなく，裁判においてもデジタル･フォレンジックによる分析結果が論点になっている．

一方，日本におけるデジタル･フォレンジックの研究者の数はほとんど変わらない状態で非常に少ない．また，日本における発表の件数は，CiNii（NII学術情報ナビゲータ）を用いて“Digital Forensics”,“デジタル・フォレンジック”で文献調査を行った結果，2006年から2015年にかけてその数はあまり変化せず平均8件程度であった．

本稿では，日本におけるデジタル･フォレンジックに関する研究を活性化するため，デジタル･フォレンジックが必

†1 東京電機大学
Tokyo Denki University

要になってきた背景や，日本における適用の状況を概説した上で，著者らが行ってきた主要な研究成果について記述する．そして，今後重要となるデジタル･フォレンジックの技術と必要となる研究について記述する．

2. デジタル･フォレンジックが重要になった背景と初期の歴史

2.1 重要になった背景

デジタル・フォレンジックが重要になってきた背景は，以下のように整理することができると考えられる．

第一点は，デジタル化の進展である．コンピュータやインターネットの普及にともない，ほとんどすべてのデータはデジタル化され，電磁的記録として保存されるようになってきた．ここでは，従来のデータが単にデジタル化されるだけでなく，さまざまに処理され高度な判断に用いられるようになってきている．したがって，デジタルデータはいまや組織の基幹にかかわるものとなっている．また，個人や組織の多くのやり取りが電子メールなどの形でスマートフォン等に蓄えられるようになってきている．したがって，捜査や民間での調査においてデジタルデータが非常に重要なものとなっている．

第二点は，サイバー攻撃の増大である．すなわち，コンピュータやインターネットの普及にともない，不正侵入などのサイバー攻撃の技術が進歩し，デジタルデータに対する不正や犯罪が増加している．また，不正アクセス禁止法やウイルス作成罪の誕生など情報化の進展にともなう新しい法律が施行された．このような理由からコンピュータ犯罪に関する訴訟の増大が予想される．

第三点は，民事訴訟の増大である．日本においても，国民の権利意識の増大などから，従来は考えられなかったような場合にも民事訴訟が行われるようになってきている．

このような状況から，デジタルデータを電磁的記憶から完全性を確保しつつ取り出し証拠として，訴訟などに備えるための手順や技術が要求されるようになってきた．

2.2 初期の歴史

日本において最初にデジタル・フォレンジックが注目を浴びたのは，1996 年ごろであると言われている．前年にオウムサリン事件が起こり，そのメンバーは公開鍵暗号を用いフアイルの防御を行うなど情報処理技術に詳しい者が多く，新たな対応としてデジタル・フォレンジックが必要であると警察に認識されたのである．

その後の日本におけるデジタル・フォレンジックの初期の歴史は，**図 1** に示すように整理することができる．2003 年にデジタル･フォレンジックを専門に扱う会社が誕生し，2004 年にはデジタル･フォレンジック研究会が発足した．

海外の歴史は日本より 10 年ほど先行しており，**図 2** に示すように整理することができる．

これらの経過をへて 2010 年代からデジタル・フォレンジックは国内外の警察等の法執行機関においても民間においても重要な技術になっていった．

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
2005年：内閣官房セキュリティ技術戦略委員会報告書に11の重要技術の1つとしてデジタル･フォレンジックが取り上げられる
2006年：「デジタル・フォレンジック事典」日科技連発刊
2008年：第4回Digital forensic International Conferenceを日本で実施

図1 日本におけるデジタル･フォレンジックの歴史
Fig.1 History of Digital Forensics in Japan

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

図2 デジタル･フォレンジックの海外の動向
Fig. 2 History of Digital Forensics in Foreign Countries

3. デジタル･フォレンジックの利用動向

3.1 利用形態の分類

デジタル・フォレンジックはすでに述べたように，いろいろな局面で用いられる．したがって，デジタル・フォレンジックを分類する軸は，（1）～（8）のように多様であると考えられる[２].

＜裁判との関連による分類＞

（1）訴訟の対象となる行為

a）組織の規定などに違反：規則に違反したメールの配信など

b）組織間の契約条項などに違反：守秘義務契約の違反など

c）法律に違反：刑法，不正アクセス禁止法（不正侵入など），個人情報保護法，不正競争防止法（営業秘密の不正入手など），金融商品取引法，独占禁止法，会社法に違反．民法の不法行為など．訴訟を意識してデジタル・フォレン

ジックを実施するが，実際には訴訟にまで至らない場合も多い．

（2）訴訟の種類

a）民事訴訟

b）刑事訴訟

（3）訴訟との関連

a）訴訟を提起する側：民事訴訟の原告（個人・企業等）・刑事訴訟の法執行機関（検察官）

b）訴訟提起を受ける側：民事訴訟の被告・刑事訴訟の被告人（個人・企業など）

今後は訴訟提起を受ける側のデジタル・フォレンジックも重要となる．企業は個人（ユーザーや従業員）や他の企業，国から訴えられることが増えており，裁判に負けると多額の賠償が課せられたり，社会の関心を集め信用に影響したりするからである．このためには企業の職員の不正を防止するためのポリシーの作成や，全職員の管理区域への入退室ログを取り不正をすればすぐわかるような対応も必要となる．

＜情報処理システムとの関連による分類＞

（4）証拠性の保持に関連する情報処理機器・システム

a）サーバー

b）PC

c）ネットワーク：ルーター，ハブ，通信路など

d）携帯電話，携帯端末，スマートフォン　他

最近は，各種の制御装置や情報家電，スマートメーター，カーナビゲーションなどの装置が IoT（Internet of Things）としてインターネットに接続される傾向にあり，これらもデジタル･フォレンジックにとって重要な対象になりうる．なお，携帯電話やスマートフォンに関連するフォレンジックをモバイル・フォレンジックともいう．また，最近は個別の機器をフォレンジックの対象とするのではなく，ネットワークを構成する機器全体を相互に関連付けながら対象とするアプローチが増大してきており，これをネットワーク・フォレンジックと呼ぶことが多い．

（5）電磁的記録を保管する媒体

a）不揮発性媒体

HDD

SSD（Solid State Drive）

USB メモリー

光学式ドライブ（DVD－R など）

b）揮発性媒体

メインメモリー

レジスター　など

従来は a）だけだったが，最近では b）もデジタル・フォレンジックの対象になってきている．b）は PC などの電源を切ると失われるので，その前にダンプ（一括してハードディスクなどにコピー）を行うなど，不揮発性媒体にコピーする必要がある．揮発性媒体に関するフォレンジックをメモリー・フォレンジックという場合がある．

（6）証拠として扱う電磁的記録の種類

a）ログのように意識的に残すもの

b）痕跡の形で偶然残るもの

デジタル・フォレンジックで用いられるログの種類としては，システムで一括管理されているログや，アプリケーションプログラム自体の独自のログ，セキュリティーソフトウェアによるログのようなものがある．

（7）証拠性の保持に関連するアプリケーションプログラム

a）電子メール

b）Web

c）ソーシャルネットワーキングサービス（SNS）　他

これらのアプリケーションプログラムが扱うデータの中に不正の痕跡が残り，証拠として用いることが可能となる場合がある．

（8）情報システムの運用形態

a）自社 Web サイトでの運用

b）クラウドの利用

クラウドの場合はログなどの収集にあたり，プロバイダーの協力が不可欠なので，契約時にこの点を取り決めておく必要がある．クラウドにおけるフォレンジックをクラウド・フォレンジックという場合がある．

3.2　デジタル・フォレンジックの主な技術

デジタル・フォレンジックで用いる技術は**図 3** に示すように，平常時，インシデント発生時に沿っていろいろなものがある．

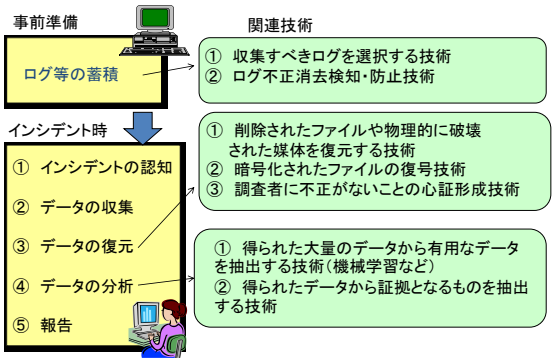

図3　主なデジタル･フォレンジック関連技術
Fig.3　Main Technologies Related to Digital Forensics

3.3　刑事事件におけるデジタル・フォレンジックの利用

刑事事件に対しても警察や検察においてデジタル・フォレンジックが広く利用されている．その対象は，**図 4** に示すようにコンピュータ関連犯罪だけでなく，殺人や窃盗などの一般的犯罪に対しても適用されている．

本稿では，法廷でデジタル・フォレンジックによる分析結果の正当性が争われた「遠隔操作ウイルス事件」につい

て，経緯と論点を紹介する[３]．この事件は，2012 年の初夏から秋にかけて，犯人がマルウエアを利用し，他者のパソコン（PC）を遠隔操作し，これを踏み台として襲撃や殺人などの犯罪予告を行ったサイバー犯罪事件である．これによりマルウエアに感染していた PC の持ち主である 4 人が誤って逮捕された．その後，真犯人と思われる人物から 2013 年 1 月 5 日に江の島の地域猫にトロイの木馬（マルウエアの一種）ソフト iesys.exe が入っているピンクの首輪をつけたとの犯行声明があり，防犯カメラの分析により，首輪をつけたと思われる動作をしている男を発見した．そして 2013 年 2 月 10 日に事件の真犯人と目される会社員 X（当時 30 歳 ）が逮捕された．

2014 年 3 月 13 日に開かれた遠隔操作ウイルス事件の第 3 回公判で，検察側の証人として出廷した警察庁情報通信局情報技術解析課の岡田智明技官が証人台に立った．岡田氏はデジタル・フォレンジックの結果，被告の会社員 X の元勤務先のパソコンに遠隔操作ウイルスの断片が見つかったことを解説した上で，X 以外の人間がこれをここに残すことは「非常に困難」との意見を開陳し，弁護側の，X のパソコンが何者かによって乗っ取られていたとする主張を否定した．一方，弁護側は真犯人が，X を罪に陥れる目的で，外部から証拠を挿入と主張した．

その後，X は自分以外に犯人がいると言うことを偽装するため 2014 年 5 月 16 日の公判中，報道関係者などに対し，真犯人「小保方銃蔵」を名乗り，電子メールを送った．しかし，5 月 20 日に，真犯人がいると言う偽装がばれ，X 本人の自白もあり，X は身柄を拘束され，東京拘置所に再び収監された．2015 年 2 月 4 日，東京地方裁判所は爆破予告メールで航空機を引き返させたハイジャック防止法違反も含め，威力業務妨害など 10 件の犯行を認定，懲役 8 年の実刑判決を受け，現在服役中である．

高度な，デジタル・フォレンジックに関する分析結果が法廷で開示され，その結果に基づき議論がなされるように日本でもなってきているという一例である．

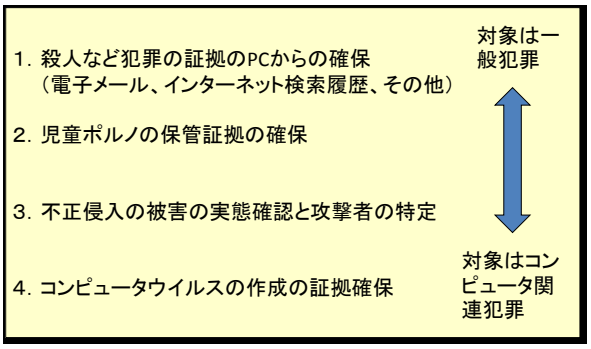

図4　警察などにおけるデジタル･フォレンジックの適用候補
Fig. 4 Candidates for Applying Digital Forensics in Police

3.4 民事事件におけるデジタル・フォレンジックの利用

企業などでもデジタル・フォレンジックを適用する場合がある．例えば，従業員による機密情報の漏洩の疑いがあっても，証拠をしっかりと把握しておかないと，裁判で負けてしまい，逆に損害賠償を請求される場合もある．そのため，デジタル・フォレンジック業者に依頼し，被疑者の PC などの調査を実施してもらうことも少なくない．

上記は訴訟を提起する側でデジタル・フォレンジックを用いる場合の例であるが，既に述べたように訴訟提起を受ける側でもデジタル・フォレンジックの考え方に基づき，ログをしっかり取っておく等により不正を行っていないことを説明できる準備を普段からしておくことが重要となる．これは裁判になった場合の裁判官に対する心象形成にも影響を与える．

民事におけるデジタル・フォレンジック利用の例として，2016 年に起こった「将棋ソフト不正利用事件」を紹介する[４]．2016 年 10 月 11 日，日本将棋連盟はスマートフォンなどによる将棋ソフト不正使用の疑いがあるとして，常務会において三浦九段に説明を求めた．三浦九段はやっていないと主張したが，10 月 12 日に 12 月 31 日までの公式戦出場停止処分を受けることになり，第 29 期竜王戦七番勝負に出場できなくなった．

その後，10 月 27 日，但木敬一氏を委員長とする第三者調査委員会の設置が決定された．12 月 26 日，第三者委員会は，疑惑について処分の根拠とされていた電子機器を使用した形跡はなく，またソフトとの一致率はその性質上根拠とはなり得ず，不正行為に及んでいた証拠はないと発表．これを受けて 2017 年 1 月 18 日には谷川浩司氏が将棋連盟の会長を辞任した．

不正行為に及んでいた証拠はないと発表できた背景に，Fronteo 社によるデジタル･フォレンジック分析の結果がある．パソコン等を用いて将棋ソフトにアクセスし，してないように偽装してもデジタル・フォレンジックの専門家が調べれば何らの証拠はかならず残ると考えられる．専門家が調べてその証拠がないということはその PC 等ではアクセスしてない可能性が高い．ただ，その他の PC やスマートフォンでアクセスした可能性は残る．しかし，今回の調査では，三浦九段本人の PC やスマートフォンだけでなく，妻や母親の PC やスマートフォンも広く調査の対象としている．この結果から将棋ソフトに不正にアクセスした可能性は非常に低いと判断しているが，この結論は，合理的な判断であると考えてよいと思う．

4. デジタル･フォレンジック関連の研究

4.1 デジタル･フォレンジック研究の分類

デジタル・フォレンジックに関する研究は，技術面から

の研究と，法律面からの研究に大別される．技術面からの研究は，システム的アプローチと，信号処理的アプローチに分類される．信号処理的アプローチは画像処理などの信号処理技術を犯罪捜査などに利用しようというもので，ある写真がどのカメラによって撮影されたものかの鑑定手法などがある．

本稿ではシステム的アプローチを中心に記述する．

4.2 日本における主な研究の位置づけ

CiNii（NII 学術情報ナビゲータ）を用いて“Digital Forensics”,“デジタル・フォレンジック”で文献調査を行った．その結果，2006 年から 2015 年にかけてその数はあまり変化せず平均 8 件程度であった．海外誌に掲載されたものは対象外であるとはいえその数は少なく，著者らのものを除くとさらに少なかった．

研究テーマがないのではない．むしろ多いと言える．それを示すため著者らが行った主要な研究を紹介する．ここでは研究を理論的か応用的か，要素的かシステム的かで 7 種類の研究を図 5 に示すように位置づけている．

LIFT: Live and Intelligent Network Forensic Technologies
DF: Digital Forensics

図5 主要な研究の位置づけ
Fig.5 Positioning of Studies in Digital Forensics

以下にそれぞれの研究を簡単に紹介する．

① ログの署名方式：4.3 節参照．

② デジタル・フォレンジックガイドシステム：インシデントに対するファーストレスポンダーに対し，スマートフォンなどで対応をガイドするシステムである．詳しくは，文献[20]等を参照願いたい．

③ LIFT システム：4.5 節参照．

④ 証拠保全装置：ハードの簡単な改良と，後述するヒステリシス署名方式等の導入により，PC をスマートカードと同様な耐タンパー性を持たせるための研究である．詳しくは，文献[17][18][26]等を参照願いたい．

⑤ ネットワーク・フォレンジック：4.4 節参照．

⑥ デジタル・フォレンジックとプライバシー：証拠性の確保とプライバシーの両立を可能とするための技術である．詳しくは，文献[19][23]等を参照願いたい．

⑦ その他：調査報告的な論文もある．詳しくは，文献[25][28]等を参照願いたい．

4.3 ログの署名方式

デジタル・フォレンジックを実施する上で，事前にログを残すということは大切である．その際，ログを改ざんしていないことを証明するためデジタル署名をつけるようになってきた．ログは間欠的に発生するので，発生するたびに署名をつける方法が通常考えられるが，この方式では，デジタルデータとそれに対するデジタル署名を一緒に削除されても，消されてしまったということに気付きにくい．これに対し，ログが発生するたびに最初からすべてのログに対しハッシュ値を求めたうえでデジタル署名を求める単一署名方式が考えられる．しかし，この方式ではログの保存期間が長くなるとログ量が大きくなり，ハッシュの処理に時間がかかり結果として署名に時間がかかるようになっていくと考えられる．

このような問題を解決するために，要約化した 1 つ前の情報を新しく発生したログデータの署名に反映する**図 6** に示すようなヒステリシス署名の提案がなされてきた[5][6]．ヒステリシス署名は，2000 年に著者らが提案したもので[5]，現在流行のブロックチェーンの先駆けをなすものである．

ヒステリシス署名は確かに効率的な方法であるが，署名検証には時間がかかり，署名生成と署名検証の回数が同程度の場合には効率的な方法とはなりえない可能性があった．

そこで，著者らは，既存の署名方式をもとに，より効率的にできるようにするための新たな方式である**図 7** に示すようなハイブリド署名方式を考案した[7][8]．そして，ハイブリッド署名方式と単一署名方式やヒステリシス署名方式に関し，種々の条件下において署名生成時間および署名検証時間およびその合計時間の評価を行った．この結果，署名の検証が頻繁に行われる場合，ハイブリッド署名方式が最も効率的であることを示すことができた[7]．

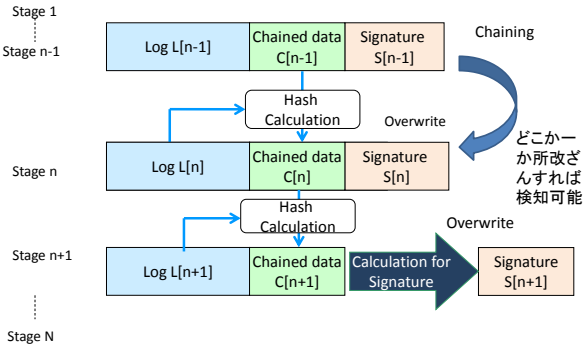

図6 ヒステリシス署名方式の概要
Fig.6 Overview of Hysteresis Signature Method

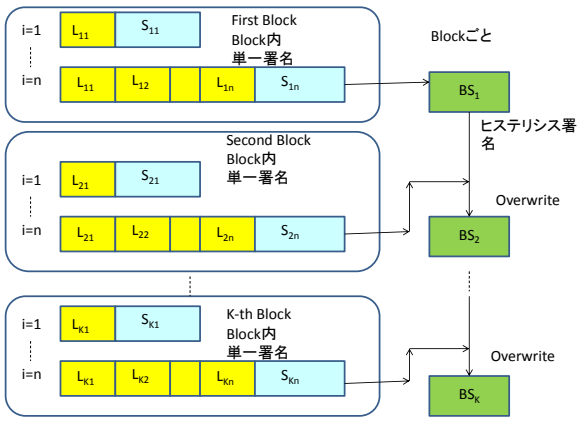

図7　ハイブリッド署名方式の概要
Fig.7　Overview of Hybrid Signature Method

4.4　ネットワーク・フォレンジック

セキュリティー・システムの設計や開発の専門家として知られている Marcus J. Ranum はネットワーク・フォレンジックを,「セキュリティ上の攻撃や問題を発生させるインシデントの発生源を発見するために，ネットワーク上のイベントをキャプチャー，記録，分析する」手順や技術であるとしている[９]．このために必要なパケットログの分析や，ログなどからのマルウェアの抽出，抽出されたマルウェアの分析などを含めてネットワーク・フォレンジックという場合も多い．また，最近は，ネットワーク・フォレンジックを用いてインシデントの発生源となる機器を特定した後，従来のデジタル・フォレンジックを適用することが多い．

ネットワーク・フォレンジックを効率よく実施するために，著者らは，不正な通信と対応する PC 内のプロセスを対応付けるためドライバープログラム Onmitsu を開発した[10][11]．Onmitsu は C++で記述され 1 K ステップ強のプログラムである．開発した Onmitsu を用いた実験の結果，ログを収集する処理時間は十分小さく 1 年間ログを残しても PC に負担をかけないことが明らかになった．また，マルウエアが立ち上がったり，テンポラリーファイル内の他のプログラムを活性化するのを知ることができ，さらに，インターネットエクスプローラの立ち上げ後マルウエアが通信をスタートするのを知ることができるなど Onmitsu によるログは有用であることが確認できた[10].

次に LAN 上に Onmitsu を組み込んだ PC やサーバを設置しておき,マルウエアの感染源を推定する方法を開発した．ここでは，また，各端末の挙動を組み合わせて解析するために，ログと端末間の関係をオントロジで表現し統合化している．また，実験により，5 次感染までの感染経路がプロセスレベルで追跡でき，オントロジを用いることで従来の場合と比べ検知時間が約 1/24 となることを確認した[12][13].

現在，感染波及範囲を推定する方式を開発中である[14]．なお，Onmitsu は企業に移管され CapLogger として製品化されている．

4.5　LIFT システム

近年，特定の企業や組織を攻撃対象とする標的型メール攻撃が問題となっている．このような攻撃に適切に対処するため，著者らは，LIFT プロジェクトを東京電機大学サイバーセキュリティ研究所内に設置し（**図８**参照），ログ分析と，ベイジアンネット等の人工知能を用いて対策をガイドする LIFT（Live and Intelligent Network Forensic Technologies）システムの開発を行っている[15][16][29]-[31].

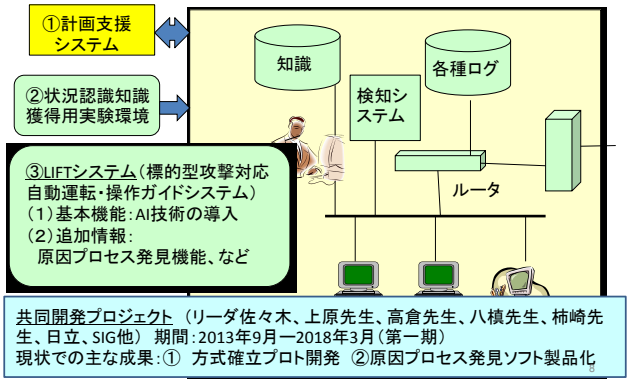

図８　LIFTプロジェクトの概要
Fig.8　Overview of LIFT　Project

LIFT システムの運用イメージは**図９**に示すとおりである．ここでは，インシデントに伴う事象（例えば C&C サーバとの通信）と徴候（例えばプロキシーサーバを経由しない通信）との関係をベイジアンネットで記述するとともに，事象と対策の関係をテーブルで用意しておく．

運用時には，対象システムからのログをオープンソースプログラムである OSSEC を用いて分析し，LIFT システムに送付する．LIFT 側では次のような処理を行う．

①　その分析結果が，インシデントの徴候であると判断すると，徴候・事象に関するベイジアンネットワークなどを用いて，事象として把握可能かチェックする．事象として把握可能ならば②へ．把握できなければ，徴候の追加収集を行い，事象として把握できるまで繰り返す．

②　事象・対策関連テーブルを用いて必要な対策（例えば，不正なパケットを発信している PC のネットワークからの切り離しなど）をオペレータにガイドする．

③　オペレータは対策を実施し，インシデントに伴う徴候がなくなるか監視する．なくなれば，④に進む．なくならなければ①に戻り監視を継続する．

④　４．４で述べた Onmitsu 等のソフトを利用し，感染源の予測や感染範囲の把握を行う．

JAVA を用いてプロトプログラムを開発し，6 つのケースについて事象発見実験を行ったところ，すべてのケースで発見が可能であった．また，代表的ケースで徴候の検知―事象の推定―対策のガイドの一連の機能が正しく動いた．

今後，現実的規模の対象に適用可能かや，将来起こりうるインシデントにどこまで対応可能かなどの検証を行っていきたいと考えている．

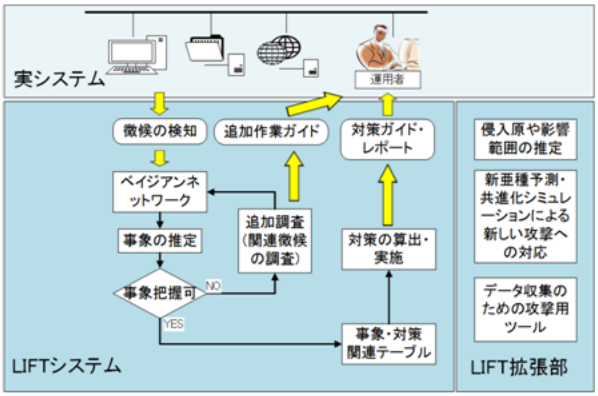

図9 LIFTシステムの運用イメージ
Fig.9 Operation Image of LIFT System

4.6 海外におけるデジタル・フォレンジック研究

Google Scholar に「Digital Forensics」という検索用語を入れ論文数を調査すると，2017 年以降で 6080 件，2016 年以降で 15000 件と日本と比べて圧倒的に多い．日本における研究者数が非常に少ないことがここからも知ることができる．

デジタル・フォレンジックに関する国際会議は増加してきているが IFIP TC11 の WG11.9 が主催する「International Conference on Digital Forensics」が最もよく知られている．2016 年にインドで開かれた第 12 回「International Conference on Digital Forensics」における発表テーマの分布は以下の通りであった．

① Themes and Issues : 3 件
② Mobile Device Forensics : 4 件
③ Cloud Forensics : 2 件
④ Social Media Forensics : 2 件
⑤ Image Forensics : 2 件
⑥ Forensic Techniques : 2 件
⑦ Forensic Tools : 2 件
合計 : 20 件

海外においては上記のようなものが関心を集めていると考えることができる．

5. 今後の方向

デジタル・フォレンジックは今後ますます重要性を増すと考えられており，特に，次のような技術が重要になっていくと考えられる．

（1）今後 PC の不揮発性記憶媒体として普及すると予想される SSD（Solid State Drive）のためのデジタル・フォレンジック技術：SSD ではディフォルトの設定にしておくと，データの消去直後であっても，データの復元ができないという問題があり，対応の検討が必要となっている．

（2）揮発性メモリー上のデータの証拠性を確保し，分析するためのメモリー・フォレンジック技術：ディスクなどに一切の証拠を残さないマルウエアが出現しており，これらに対応するためなどに揮発性メモリー上のデータの証拠性をダンプなどにより確保し，分析する技術の必要性が増大している．

（3）ますます高度化・悪質化していくサーバー攻撃に対応していくためのネットワーク・フォレンジック技術：すでに研究はいろいろ行われているが，さらなる強化が必要である．

（4）スマートフォンや携帯電話などの証拠を確保するためのモバイル・フォレンジック技術 : PC よりもスマートフォンの利用者が多くなってきている．しかも，スマートフォンではセキュリティ対策が進み，パスワードが長くなったり，何回かパスワード入力に失敗するとデータが消える仕組みになっているため，デジタル・フォレンジックのためのデータの入手が困難になっている．

（5）クラウドコンピューティングなど IT の新しい運用形態や利用形態に対応したフォレンジック技術：クラウド・フォレンジック技術だけでなく，今後は，Fog Forensics [32]なども注目されるようになっていく可能性がある．

（6）より高度なフォレンジック技術：このため人工知能（AI）の利用の高度化が期待されている．

ここで述べたのは，デジタル・フォレンジックの研究のうち，技術面の研究の中のシステム的アプローチの方法に関するものだけである．技術面における信号処理的アプローチや法律面においてもいろいろな研究課題がある．

海外に比べ日本の研究者の数は圧倒的に少ない．日本でも研究者が増え，これらの課題を解決することを期待している．

6. おわりに

日本におけるデジタル･フォレンジックに関する研究を活性化するため，本稿では，デジタル･フォレンジックが必要になってきた背景や種々の利用の状況を概説した．次に研究範囲が広いことを示すために，著者らが行ってきた主要な研究成果について記述した．そして，今後重要となるデジタル･フォレンジックの技術動向と必要となる研究について考えを述べた．

日本でも研究者が増え，デジタル・フォレンジックに関する課題を解決し，サイバー空間の安全性の向上に貢献していくことを期待している．

謝辞 デジタル・フォレンジックの研究を一緒に実施してくれた東京電機大学の学生の皆様，同サイバーセキュリ

ティ研究所の研究員の皆様に厚く御礼申し上げる．また，デジタル・フォレンジック研究会の皆様には，最新の技術動向や，ニーズについて貴重なご意見をいただいた．記して感謝申し上げる．

参考文献

[1] 佐々木良一編著「デジタル・フォレンジックの基礎と実践」東京電機大学出版局，2017 年

[2] 佐々木良一監修「改訂版デジタル・フォレンジック事典」日科技連出版，2014 年

[3] 「パソコン遠隔操作事件」https://ja.wikipedia.org/wiki/%E3%83%91%E3%82%BD%E3%82%B3%E3%83%B3%E9%81%A0%E9%9A%94%E6%93%8D%E4%BD%9C%E4%BA%8B%E4%BB%B6 2017 年 8 月 11 日確認

[4] 「調査報告書（概略版）」第三者委員会 2016 年 12 月 26 日 https://www.shogi.or.jp/news/investigative_report_1.pdf 2017 年 8 月 11 日確認

[5] 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

[6] 上田祐輔，佐々木良一他「データ喪失を想定したヒスト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

[7] 小林直樹，佐々木良一「証拠性保全のための安全で効率的なログ署名方式の提案と評価」日本セキュリティマネジメント学会誌 28 巻第 2 号 2014 年 9 月 pp11-21

[8] Naoki Kobayashi, Ryoichi Sasaki,「Proposal and evaluation of an evidence preservation method for use in a common number system」International Journal of Electronic Commerce Studies vol.6,no.1,pp51-68，2015

[9] "Network forensics". Wikipedia. https://en.wikipedia.org/wiki/Network_forensics, (accessed 2017-08-11).

[10] 三村聡志，佐々木「プロセス情報と関連づけた通信情報保全手法の提案」情報処理学会論文誌， Vol.57, No.9, pp1944-1953, 2016

[11] Satoshi Mimura, Ryoichi Sasaki" Proposal of the Method for Estimating the Cause of Unjust Communication by Using the Network Packets Associated with Process Information" The International Conference on Information Security and Cyber Forensics (2014.10)

[12] 佐藤信，佐々木良一他「マルウエアによるネットワーク内の挙動を利用した標的型攻撃における感染経路検知ツールの開発と評価」情報処理学会論文誌, Vol.58, No.2, pp1-9, 2017

[13] Makoto Sato, Ryoichi Sasaki, Akihiko Sugimoto, Naoki Hayashi, Yoshiaki Isobe "Proposal of a Method for Identifying the Infection Route for Targeted Attacks Based on Malware Behavior in a Network." Proc. of the Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec2015), IEEE, Oct 2015.

[14] 島川貴裕，佐々木良一他「標的型攻撃に対する知的ネットワークフォレンジックシステム LIFT の開発と機能拡張（その３） －侵入源と波及範囲の推定―」情報処理学会，CSS2017

[15] K. Hashimoto, H. Hiruma, T. Matsumoto, K. Kayama, Y. Kaikizaki, H. Yamaki, R. Sasaki, T. Uehara. "Development of intellectual network forensic system LIFT against targeted attacks." Proc. of the Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec2015), IEEE, Oct 2015.

[16] 佐々木良一，八槇博史「標的型攻撃に対する知的ネットワークフォレンジックシステム LIFT の開発（その 3）－ 今後の研究構想 －」情報処理学会 DICOMO2015 （2015 年 7 月）

[17] 芦野佑樹，佐々木良一「セキュリティデバイスとヒステリシス署名を用いたデジタルフォレンジックシステムの提案と評価」情報処理学会論文誌，49 巻 2 号，pp. 999-1009，2008

[18] 藤田圭祐，芦野佑樹，上原哲太郎，佐々木良一「不正プログラムの起動制御機能を持つＤＦシステムの提案と評価」情報処理学会論文誌 VOL.51,No.9，pp1507-1519，2010

[19] 高塚光幸，佐々木良一他「開示情報の墨塗りと証拠性確保を両立させる e-Discovery システムの提案」情報処理学会論文誌第 49 号第 9 号 pp3191-3198，2008

[20] 天野貴通，上原，佐々木「デジタル・フォレンジックのためのガイドライン総合支援システムの提案と開発」情報処理学会論文誌, Vol.56,No.9,pp1889-1899,2015

[21] 長谷部浩司，上原哲太郎，佐々木良一「複数組織にまたがる疫学調査におけるプライバシー確保のための大容量タンパー装置 HiGATE の適用方式の開発」日本セキュリティマネジメント学会誌 VOL.25,No.3，pp24-34,2012

[22] 土方広夢，佐々木良一他「デジタル・フォレンジクスを考慮した個人情報漏洩対策に関する合意形成のための多重リスクコミュニケータの適用」日本セキュリティマネジメント学会誌 26 巻第 1 号 2012 年 5 月 pp3-14,2012

[23] Shuhui Hou, Siuming Yiu, Uehara, Sasaki et al,「A Privacy-Preserving Approach for Collecting Evidence in Forensic Investigation」International Journal of Cyber-Security and Digital Forensics (IJCSDF) (Vol.2,No.1pp70-78）2013

[24] Takashi Shitamichi, Ryoichi Sasaki「A Proposal and Evaluation of User Centric Trusted Log Archival Architecture」International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(3): 442-452(ISSN: 2305-0012),2015

[25] Jigang Liu, Tetsutaro Uehara, Ryoichi Sasaki「Development of digital forensics practice and research in Japan」Wireless Communications And Mobile Computing(Wiley InterScience) www.interscience.wiley.com，2010

[26] Takashi Shitamichi, Ryoichi Sasaki,"Technology of Federated Identity and Secure Loggings in Cloud Computing Environment" International Journal of Electronic Commerce Studies Vol.5, No.1, pp. 39-62, 2014 doi: 10.7903/ijecs.1157,2014

[27] G Peterson, S Shenoi ， Advances in Digital Forensics XII: 12th IFIP WG 11.9 International Conference, New Delhi, January 4-6, 2016

[28] 佐々木良一他「デジタル･フォレンジックの体系化の試みと必要技術の提案」日本セキュリティ･マネジメント学会 20 巻第 2 号、pp49-61、2006

[29] 鈴木文仁，佐々木良一他「標的型攻撃に対する知的ネットワークフォレンジックシステム LIFT の開発と機能拡張（その１） －LIFT の全体像―」情報処理学会，CSS2017

[30] 島﨑一樹，佐々木良一他「標的型攻撃に対する知的ネットワークフォレンジックシステム LIFT の開発と機能拡張（その２） －対策案優先度評価法―」情報処理学会，CSS2017

[31] 渋谷 健太，佐々木良一他「標的型攻撃に対する知的ネットワークフォレンジックシステム LIFT の開発と機能拡張（その４） -将来起こりうる攻撃方法の推定-」情報処理学会，CSS2017

[32] Yifan Wang, Tetsutaro Uehara, Ryoichi Sasaki, "Fog Computing: Issues and Challenges in Security and Forensics", COMPSAC2015