標的型攻撃に対するネットワークフォレンジック対策の現状と今後の展望

佐々木 良一† 上原哲太郎 # 松本隆 %

† 東京電機大学 〒120-8551 東京都足立区千住旭町 5 sasaki@isl.im.dendai.ac.jp
# 立命館大学 〒525-8577 草津市野路東 1-1-1 uehara@cs.ritsumei.ac.jp
% ネットエージェント株式会社 〒130-0022 墨田区江東橋 4-26-5 matsumoto@netagent.co.jp

あらまし 最近、サイバー攻撃は厳しさを増しており、特定の個人や組織を集中的に攻撃する標的型攻撃も増加してきている。巧妙な標的型攻撃に対しては、標的型メール対策などの入口対策の有効性は低く、攻撃を防ぎきるのは困難である。このため攻撃の証拠性を確保し、事後対策を適切に行うための技術であるデジタルフォレンジックが重要性を増している。特にネットワーク系のログの適切な保存は現状では十分に行われておらず、デジタルフォレンジックの一分野であるネットワークフォレンジックに基づく対策が不可欠になっている。本論文ではネットワークフォレンジック対策や技術の推移を紹介するとともに、著者らが進めているLIFT (Live Intelligent Network Forensic Technologies)技術ならびにそれを支援するシステムの研究概要について紹介する。

Present Status and Future Direction of Network Forensics against Targeted Attack

Ryoichi Sasaki† Tetsutaro Uehara# Takashi Matsumoto%

†Tokyo Denki University 5, Senju-Asahi-Cho, Adachi-ku, Tokyo, 120-8551 JAPAN
sasaki@isl.im.dendai.ac.jp
Ritsumeikan University, 1-1-1 Nojihigashi, Kusatsu-City, Shiga 525-8577 JAPAN
uehara@cs.ritsumei.ac.jp
% NetAgent 4-26-5 Gohto Bashi, Sumida-ku, Tokyo 130-0022 JAPAN
matsumoto@netagent.co.jp

Abstract The cyber attack becomes stricter, and the targeted attack which attacks targeted special person or institute increases recently. Against the skillful targeted attack, the effectiveness of entrance measures such as targeted email measures is low. Therefore, digital forensic measures to keep appropriate preservation of the log and to be used for appropriate measures after an incident become important. Especially, network forensics, which use network origin log and is one of the fields of digital forensics become essential. This paper reports the changes of the network forensic measures and the technologies with a future direction including our research activities with concern to the technology named LIFT(Live Intelligent Network Forensic Technologies) and its support system.

1　はじめに

最近、サイバー攻撃は厳しさを増しており、特定の個人や組織を集中的に攻撃する標的型攻撃も増加してきている。企業などの組織では怪しいメールを開かなくするための教育がおこなわれているが、巧妙な標的型攻撃に対しては、標的型メール対策などの入口対策の有効性は低い。したがって、入口対策だけで攻撃を防ぎきるのは困難であるという認識に基づき、いろいろな対策を組み合わせて実施する必要があるが、攻撃の証拠性を確保し、事後対策を適切に行うための技術であるデジタルフォレンジックも重要性を増している。特にネットワーク系のログの適切な保存は現状では十分に行われておらず、デジタルフォレンジックの一分野であるネットワークフォレンジックに基づく対策が不可欠になっている。しかし、これらは重要でありながら、従来対応が遅れていた分野であり、特に日本では対策がほとんど行われていなかった。これらに関する日本における研究開発を活性化するため、ネットワークフォレンジック対策ならびに技術の現状と今後の方向について考えを述べる。

本論文では、第 2 節で標的型攻撃の概要について説明し、第 3 節では標的型メール対策の効果の評価結果を紹介する。第 4 節では著者らが作成したログ保存に関するガイドの紹介などネットワークフォレンジック対策の現状の解説を行う。第 5 節では、著者らが研究を進めている LIFT（Live Intelligent Network Forensic Technologies）技術を中心にして、新しい動きと今後の展開について報告する。

2．標的型攻撃の概要

近年、特定の個人や組織を集中的に攻撃する標的型攻撃が増加している。特に不正なメールを特定の個人に送りつけ、そのＰＣにウイルスを感染させたうえで、組織内に侵入を続け、重要な情報を取り出そうという攻撃（これを標的型メール攻撃ともいう）は、2011 年以降、三菱重工、衆議院、参議院、総務省、ＪＡＸＡ など多くの組織に対し実施されている。その攻撃の概要は図 1 に示すとおりである。

従来のスパムメール攻撃と違うのは、①特定の個人向けに、メールの内容がチューニングされており、つい開けてしまいたくなる点や、②数が少ないので、そのようなウイルスがあるとワクチン会社も気付かず、ワクチンにそのような対策が組み込まれていない場合がある点である。

これらの攻撃に対する対策は図２に示すように整理することができる。

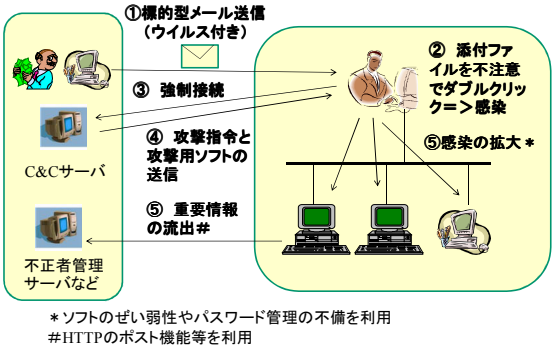

図1　衆議院等への標的型攻撃

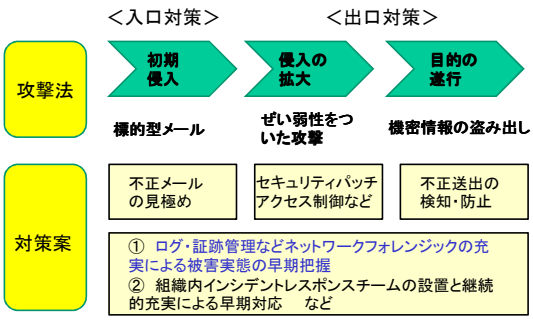

図2　衆議院等への攻撃と対策案

3. 入口対策の効果

図 2 に示す、標的型メールによる初期侵入を防止するための不正メールの見極めは入口対策の代表である。企業などの組織では怪しいメールを開かなくするための教育や訓練がおこなわれている。しかし、この対策の効果は本当に大きいのだろうか。

n 人の組織で 1 人でも標的型メールを開けると被害は内部でどんどん拡大する。

今、i 人目の人が開ける確率を Pi とすると組織の中で誰かひとりが開ける確率は次式で求められる。

$$PT = 1 - \prod_{i=1}^{n} (1-Pi) \qquad \text{———（1）}$$

ここで、

n　：　組織に属する人の数

Pi　：　i　番目の人が開ける確率

今、n の値を 10,50,100,500 と変化させ、Pi を全員同じ値をとり、それを 1.0，0.1，0.01，0.001 と変化させた場合の、「だれか 1 人が標的型メールを開ける確率」の計算結果は表 1 に示すようになる。この表から、構成員が 500 人以上の組織においては各個人の開ける確率を 0.01 におされられたとしても、だれか 1 人が開ける確率は非常に大きなものとなることが分かる。

また､n-1 人が開ける確率を 0 にできたとしても、残りの 1 人の開ける確率が 0.3 なら、だれか 1 人が開ける確率は式（1）より、0.3 になることが分かる。すなわち、その値はもっとも注意力を欠く人に依存するのである。

したがって、怪しいメールを開かなくするための教育や訓練も不要であるとは言えないが、これらの対策に過剰に期待するのは適切でないことが分かる。

したがって、入口対策だけで攻撃を防ぎきるのは困難であるという認識に基づき、いろいろな対策を組み合わせて対処する必要があるが、図２に示すようにネットワークフォレンジックも重要性を増している。

表1　だれか1人が標的型メールを開ける確率

n \ Pi	1.0	0.1	0.01	0.001
10	1.0	0.65	0.096	0.010
50	1.0	1.0	0.39	0.049
100	1.0	1.0	0.63	0.095
500	1.0	1.0	0.99	0.39

4．ネットワークフォレンジック対策や技術の現状

4.1　ネットワークフォレンジックの位置づけ

ネットワークフォレンジックはデジタルフォレンジックの一分野である。ここで、デジタルフォレンジックは、デジタルフォレンジック研究会によって、「インジデント・レスポンスや法的紛争・訴訟に対し，電磁的記録の証拠保全及び調査・分析を行うとともに，電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術を言う」と定義されている[1][2]。このデジタルフォレンジックの重要性は広く認められるようになり、著者らもいろいろな研究を実施してきた [9-18]。

上記の定義において、電磁的記録は通常ログの形で残されているが、ログがネットワーク機器などから得られるパケット等に関するものの場合にネットワークフォレンジックという場合がある（表２参照）。

標的型攻撃に対処するためにはネットワークフォレンジックが大切であるが、ネットワークフォレンジック対策は、世界的にあまり普及しておらず、特に日本においては遅れている。また、ネットワークフォレンジック技術に関する研究は海外ではいろいろ行われているが（たとえば[19-21]）、日本ではあまり進んでいない。

表2　主なデジタルフォレンジック

種類	対象
ディスクフォレンジック（コンピュータフォレンジック）	ハードディスクを中心とした不揮発な記憶媒体
ネットワークフォレンジック	ネットワーク機器、サーバのログなど
電子メールフォレンジック	電子メールを中心とするデータ
Webフォレンジック	Webサイトに関連するデータ
モーバイルフォレンジック	携帯電話、携帯端末、スマートフォン等のデータ

情報セキュリティ白書2011より

4．２　ネットワークフォレンジックの手順

ネットワークフォレンジックは米国の Wikipedia によると、「Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information. Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation.」と定義されている。

ネットワークフォレンジックも他のデジタルフォレンジックと同様に、

①アクセスログや通信ログなどの証拠を保全する手順、

②証拠を暗号化や破壊などをされた場合にも利用できるようにする手順、

③データマイニングなどにより有用なデータを抽出するなど証拠を分析する手順

を経て利用される。

Wikipedia の定義で示したように、ネットワーク関連のデータは、何もしないと失われてしまうため、①のリアルタイムで調べたり、ログとして残したりする努力が非常に重要となる。

このため、ログとして何をどのように残すかのガイドを内閣官房ネットワークセキュリティセンターとデジタルフォレンジック研究会が協力し、著者らも委員として参加し、作成した。その結果の概要を次節で述べる。

4．3 ネットワーク関連ログの収集ガイド

上記のガイドを記述した「政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書」[３]では、標的型攻撃などに備えるため直ぐに対応可能なものとして次のような対策が必要であるとしている。

（１）機器によらない全般的な対策

（ａ）各ログ取得機器のシステム時刻を、タイムサーバを用いて同期する。

（ｂ）ログは１年間以上保存する。

（ｃ）複数のログ取得機器のログを、ログサーバを用いて一括取得する。

（ｄ）攻撃等の事象発生が確認された場合の対処手順を整備する。

（２）機器別の対策

（ａ）１．ファイアウォール：「外⇒内で許可した通信」と「内⇒外で許可・不許可両方の通信」のログを取得する。

（ｂ）Web プロキシサーバ：接続を要求した端末を識別できるログを取得する。

（ｃ）他のシステムや機器の権限を管理するサーバ（LDAP, Radius 等）：管理者権限による操作ログを取得する。

（ｄ）メールサーバ：「メールの送受信アドレス」及び「メッセ―ジ ID」のログを取得する。

（ｄ）クライアント PC：マルウェア対策ソフトウェアの検知・スキャンログ・パターンファイルのアップデートログを取得する。

（ｅ）DB サーバ・ファイルサーバ：特別なログ設定は不要だが、確実にログを取得する。

なお、上記でログは 1 年以上保存するとしているが、長期化に伴うコストの増大や、ログそのものが攻撃対象になるリスクなどを考え保存期間は短いほうが望ましいとする意見もあり、さらなる議論が必要である。

4．4 ネットワークフォレンジック関連製品やサービス

上記の報告書[3]では、ログ・証跡管理に関する製品およびサービスの調査も行っていて、ネットワーク監視ツールとして次のようなものがあるとしている。

（１）RSA NetWitness

（２）PacketBlackHole

（３）NetDetector

これらは必要に応じてすべてのパケットをログとして保管できるようにするものである。たとえば、著者らが利用した経験を持つ NIKSUN 社の NetDetector Alpine は、フル機能を備えたネットワークセキュリティシグネチャを利用した IDS 機能や統計に基づいた異常検知、分析、およびアプリケーションレベルでのデータ再現やパケットレベルでの詳細なフォレンジック調査を行うことができる[5]。

また、ログ統合管理ツールとして次のような

ものがあるとしている。

（1）RSA enVision
（2）Logstorage
（3）AnalyticMart for LogAuditor
（4）快速サーチャーLogRavi
（5）LogStare Tetra
（6）ArcSight ESM
（7）splunk

これらはサーバやネットワークなど各種のログを、タイムライン上に整理して表示し、相関分析を容易に実施するためのものである。たとえば、HP 社の ArcSight はネットワーク上に存在するネットワーク機器、サーバー、アプリケーション等からリアルタイムでログを収集、保管し、多様な分析・レポート機能を持つという[6]。 今後、ログ管理統合ツール並びにその後継の重要性が増大していくと考えられる。

4．5 適切なネットワークフォレンジック対策のための問題点

ネットワークフォレンジック対策を適切に取っていけるようにするためには、以下のような問題点の解決が必要となる。

（1）証拠となるログ自体が取られていない場合が多い。このようなことがあるので、4.3 節に示すようなログの収集ガイドを作成したが、これらは必要最小限のもので、どのようなログをどのようにとるべきかの検討が今後も必要である。

（2）ログ管理統合ツールの分析機能の不足。わかりやすく表示する機能は充実してきているが、どのような事象がおこっているかを理解するためには専門知識を必要とする。一方、下記のように専門家は少ないため、事象を（半）自動的に判断するインテリジェント機能が必要となってきている。

（3）ネットワークフォレンジックの専門家が少ない。ネットワークログの持つ意味を理解し、適切な対応をとれるようにするためには、ネットワークや IT システムに関する様々な知識を必要とするとともに、実務経験を必要とするが、そのような専門家は非常に限られている。

（4）ネットワークフォレンジックの研究者の不足。良いネットワークフォレンジック技術を開発するためには、インシデント発生時などのログを必要とするが、現状ではこれが手に入らない状況になっており、研究者の数が非常に少ない。産学の協力体制の確立なども大切となる。

5．最近の動きと今後の方向

5．1 最近の動き

最近の注目すべき動きとして以下のようなものがある。

（1）SIEM（Security Information and Event Management：セキュリティ情報およびイベント管理）の提供

SIEM は、以下の二つの概念が組み合わさったものである[5]。一つ目は、様々な情報ソースから発生するイベントログを一元的に管理することでセキュリティポリシー監視とコンプライアンス支援を行う「SIM (Security Information Management)」。もう一つが、セキュリティ脅威に対するリアルタイムな検知を行うことでセキュリティインシデントへの対策を行う「SEM (Security Event Management)」である。ログをシステムが自動的に有効活用して、セキュリティリスクと管理者の負担を軽減させる点がポイントである。ログ管理統合ツールにセキュリティ脅威に対するリアルタイムな検知機能を追加し総合的に対応できるものと言っていいだろう。ネットワーク監視ツールやログ統合管理ツールとの関連は表 3 に示すように整理することができると考えられる。

SIEM 製品には、RSA Security Analytics、IBM Security QRadar SIEM や McAfee Enterprise Security Manager 等がある。著者らが利用経験を持つマカフィ社の McAfee Enterprise Security Manager などから構成される SIEM ソリューションは、イベント、ユーザー、システム、データ、リスク、対策に関する情報を迅速に提供することによって、グローバルで発生している脅威状況をリアルタイムに理解できるよう支援している [7]。

表3　ネットワークフォレンジックの対応フェーズ

	フェーズ1	フェーズ2	フェーズ3	フェーズ4	フェーズ5
対応状況	大多数の企業	→	→	先進的企業	今後
機能		ネットワーク関連ログの収集	各種ログの統合管理	監視情報との統合	管理のインテリジェント化
ツール	なし	ネットワーク監視ツール	ログ統合管理ツール	SIEM	LIFT

SIEM:　Security Information and Event Management
LIFT:　Live Intelligent　Network Forensic Technologies

（2）IP v 4アドレス枯渇への対応

IPv4 における IP アドレスの枯渇を受けて、プロバイダにおける大規模 NAT の運用が開始されており、これに対応するためログ収集においてポート番号の保存が求められるようになった（RFC6302）。また、IPv6 の使用も徐々に広がっており、ログ収集などにおいて IPv4 と IPv 6 双方のアドレスが扱えるようにする必要がある。

（3）広域に分散された大量のログへの対応

DB や Web, App サーバの数が非常に多くなり、ログの対象も多くなる。しかも、クラウドを考えた場合にログは広域に分散されることになる。大量のログを採取したり、もしくは、遠隔地に転送したりする方法は様々なオープンソースの実装が行われている。しかしながら、完全性や真正性について、考慮した 実装はないと考えており、今後の課題の 1 つである。

（4）組織内インシデントレスポンスチームの設立

標的型攻撃の増加を受けて、図２に示すように政府や大企業を中心に組織内インシデントレスポンスチームが設立され始めている。このような組織においてもネットワークフォレンジック対応がとれるようにしていく必要がある。まずは外部の専門家との会話ができるようにしておき、その後、組織の中で対応できる部分を増やしていくことが望ましい。

5．2　今後の展開

今後必要なネットワークフォレンジック関連の対応を考えた結果、著者らは図 3 に示すような LIFT　(Live Intelligent　Network Forensic Technologies)　システムの開発に着手した。

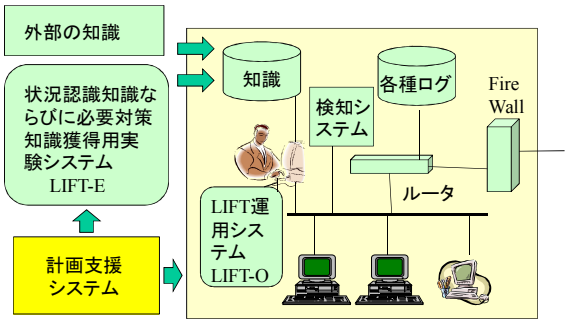

図3　LIFTシステムの概要と開発構想

このようなシステムが必要であると考えた理由は以下のとおりである。

（1）事後対応中心から能動的ライブフォレンジックの実現：攻撃（者）の早期補足と、それぞれの時点での意味のある証拠保全を実施する必要がある。また、それに基づき適切な行動をとれるようにするため、図 3 の LIFT 運用システム LIFT-O(Operation)では、①証拠データと②VPN によるゾーニングの導入などの対応の関連付けが重要となる。

（2）状況判断と取るべきログと対応決定の（半）自動化：上記のような対応ができるネットワークフォレンジック技術者は、すでに述べたように非常に少ないので、これらの人たちの知識も取り込んだ状況判断と取るべきログと対応決定の（半）自動化やインテリジェント化が必要となっている。このような知識を効率的に得るためには、実験環境が不可欠であり状況認識知識ならびに必要対策知識獲得用実験システム LIFT-E（Experiment）も同時に開発する。

これらの研究開発を実施していくうえで、次のような点への注目が重要であると考えている。

（1）消去された情報の復元と、消去理由の推定およびそれらの対応への利用：消えるはずのない情報が消されているのは、非常に重要な情報であり、データ復元技術を用い、事実を明確にしたうえで、これらを診断に積極的に反映させていきたい。

（２）ゾーンニングなどを能動的の行うことによる情報の積極的収集と対応への反映：防御側から能動的に動くことにより見えてくる情報は多いはずであり、これらを対応に反映させていきたい。

（３）AI(人工知能)技術の導入：現在、AI 技術が再認識される動きにあり[８]、AI に関する最新の技術を積極的に取り組んでいくべきであると考えている。

（４）計画支援システムとのリンク：LIFT システムは、運用を支援するためのものであるが、対象がどのような構成になり、どのような機能を持っているかによって効果が限定的になる。したがって計画支援システムを用いて適切な構成や機能を決めておく必要がある。著者らは、計画支援システムの一種である多重リスクコミュニケータ MRC 等を開発するとともに、標的型攻撃に対する対策の最適な組み合わせを求めてきた[22-23]。LIFT システムと MRC を組み合わせて用い、計画問題と運用問題の両方を適切に解決していくというのは重要であると考えられる。

（５）関連企業との協力関係の確立：実験室レベルでのデータは大学でも可能であるが、現実レベルの攻撃のデータの収集は大学では困難であり、関連企業との協力関係の確立は不可欠である。

LIFT システムのプロトタイププログラムは、2 年以内に開発し、適応実験を行っていきたいと考えている。

6. おわりに

本論文では標的型攻撃に対応するためのネットワークフォレンジック対策や技術の推移を紹介するとともに、将来に向け著者らが進めている LIFT（Live Intelligent　Network Forensic Technologies）システムの研究概要について紹介した。

著者らは、上記のような形でネットワークフォレンジックの研究に取り組んでいるが、それだけでは不十分で、いろいろな形でネットワークフォレンジックの研究に取り組む必要があると考えられる。研究への参加者が増えることを期待している。

参考文献

[1] デジタル・フォレンジック研究会編「デジタル・フォレンジック事典」日科技連, 2006

[2] 佐々木良一、芦野佑樹、増渕孝延、「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、2006.9

[3]「政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書」平成 24 年 3 月
内閣官房情報セキュリティセンター
http://www.nisc.go.jp/inquiry/pdf/log_shutoku.pdf

[4]　日立ソリューションセキュリティブログ「SIEM とは」http://securityblog.jp/words/714.html

[5]　NetDetector
http://www.scsk.jp/product/common/niksun/sales/netdetector_index.html

[6]　ArcSight ESM　HP
http://www.scsk.jp/sp/sys/products/arcsight/index.html

[7] マカフィ　SIEM
http://www.mcafee.com/japan/products/siem/

[8]小林雅一「クラウドから AI へ」朝日新書,　2013

[9] 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、２００８年２月号

[10] 高塚　光幸、多田　真崇、佐々木良一 「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

[11] 植松　建至、芦野　佑樹、藤田　圭祐、多田　真崇、高塚　光幸、佐々木良一「構造計算書不正検知システムの提案 」情報処理学会論文誌第 49 号第 9 号 pp3199-3208

[12] ハン　博文、佐々木良一 「ＩＰトレースバックのための出国印方式の試作と評価 」情報処理学会論文誌第 49 号第 9 号 pp3157-3164

[13]　Yuki Ashino, Ryoichi Sasaki “Proposal of Digital Forensic System Using Security Device and Hysteresis Signature ” IIHM2007 in Taiwan

[14] Mariko Irisawa,Yuki Ashino, Keisuke Fujita, Ryoichi Sasaki “Development and Application of Digital Forensic

Logging System for Data from a Keyboard and Camera" IIHM2007 in Taiwan

[15] Keisuke Fujita, Yuki Ashino, Tetsuro Uehara, Ryoichi Sasaki "Proposal of Digital Forensic System with a Boot Control Function against Unauthorized Programs" 4th Annual IFIP WG11.9, International Conference on Digital Forensics

[16] Yuki Ashino, Keisuke Fujita, Maiko Furusawa, Tetsuro Uehara, Ryoichi Sasaki "Extension and Evaluation of Boot Control for a Digital Forensic System" ICDF2009 (in Florida) 5th Annual IFIP WG11.9 International Conference on Digital Forensics

[17] Wataru Takahashi, Ryoichi Sasaki, Tetsutaro Uehara, "Development and Evaluation of Guideline Total Support System for Evidence Preservation by Using an Android Phone", CFSE2013 held in Conjunction with COMPSAC2013 (in Kyoto)

[18] Ryoichi Sasaki, "Research and Development of IT Risk Communication Support System and Its Application to Digital Forensic Issues" Invited Talk CFSE2012 held in Conjunction with COMPSAC2012 (in Turkey)

[19] Sherri Davidoff, Jonathan Ham "Network Forensics: Tracking Hackers through Cyberspace" 2012, Prentice Hall

[20] Miroslav Ponec, Paul Giura, Joel Wein, Hervé Brönnimann "New payload attribution methods for network forensic investigations" February 2010 , Transactions on Information and System Security (TISSEC)

[21] Niandong Liao, Shengfeng Tian ,Tinghua Wang "Network forensics based on fuzzy logic and expert system" Computer Communications, Volume 32, Issue 17, 15 November 2009, Pages 1881–1892

[22] Ryoichi Sasaki," Consideration on Risk Communication for IT Systems and Development of Support Systems" Journal of Information Processing Vo.20 （2012） -4, pp814-822 (Invited Paper)

[23] 石井 亮平、金子紀之、佐々木 良一「イベントツリーを用いたリスク評価ツールの実装と標的型攻撃対策最適組み合わせ問題への適用」情報処理学会 CSS2013 予稿集