SCIS 2016 2016 Symposium on
Cryptography and Information Security
Kumamoto, Japan, Jan. 19- 22, 2016
The Institute of Electronics,
Information and Communication Engineers

公判対応を前提としたメモリ・フォレンジック有用性の考察

Usefulness of memory forensics for the examination of evidence

野上 紘* 田中 英彦*
Hiroshi Nogami Hidehiko Tanaka

あらまし 近年, サイバー犯罪による被害は増加の一途をたどり, その攻撃手法は高度化・巧妙化してきている. これらの犯罪に対し法執行機関では, デジタル・フォレンジックを駆使し, 攻撃者の特定及び犯行の全容解明に努めている. しかし, ハードディスクを対象とした従来の解析だけでは発見が困難なマルウェアや秘匿技術の登場により, 新たな解析手法の整備が求められている. そこで本研究では, 国内外で研究が進められているメモリ・フォレンジック手法に着目し, 同手法で得られる情報の精査及び, 同手法によって解明が期待される事項を明らかにすることで, メモリ・フォレンジックの有用性を示した. また, 法執行機関が公判で証拠として使用する際に重要となるツールの信頼性について, 自由心証主義の観点から考察を行った.

キーワード サイバー犯罪, メモリ・フォレンジック, 証拠能力

1 研究の背景

1.1 サイバー犯罪の現状

サイバー犯罪の現状として, 表 1, 2 に平成 22～26 年における不正アクセス行為の認知件数及び検挙件数等の推移, 表 3 に不正アクセス行為後の内訳を示す. 平成 26 年に着目すると, 認知件数が 3545 件と前年に比べ 20.1%増加した一方で, 検挙件数が 364 件と 62.9%減少しており, 検挙率の低下が懸念されている. また, 不正アクセス行為後の内訳を見ると, インターネットバンキングの不正送金が 1944 件, 次いで他人へのなりすましが 1009 件と, 上位２項目で全体の 83.3%を占め, 日常の生活に必要不可欠であるインターネット利用のリスクが拡大していることがわかる[1].

こうした現状から, 法執行機関には犯罪の全容解明による被害防止・予防が求められており, そのための情報収集及び分析には, デジタル・フォレンジックと呼ばれる手法が用いられる.

表 1 不正アクセス行為の認知件数

区分＼年次	平成22	平成23	平成24	平成25	平成26
認知件数(件)	1,885	889	1,251	2,951	3,545
海外からのアクセス	57	110	122	289	298
国内からのアクセス	1,755	678	987	2,474	2,469
アクセス元不明	73	101	142	188	778

表 2 検挙件数等の推移

区分＼年次		平成22	平成23	平成24	平成25	平成26
不正アクセス行為	検挙件数	1,598	242	533	968	338
	検挙事件数	103	101	133	142	141
	検挙人員	123	110	151	144	150
識別符号提供(助長)行為	検挙件数	3	6	4	7	0
	検挙事件数	3	6	4	7	0
	検挙人員	4	6	4	7	0
識別符号取得行為	検挙件数			2	2	16
	検挙事件数			2	1	5
	検挙人員			2	1	15
識別符号保管行為	検挙件数			2	2	2
	検挙事件数			2	2	2
	検挙人員			2	2	2
フィッシング行為	検挙件数			2	1	8
	検挙事件数			1	1	6
	検挙人員			1	1	6
計	検挙件数(件)	1,601	248	543	980	364
	検挙事件数(事件)	106	107	142	153	154
	検挙人員(人)	127	116	160	155	173

*情報セキュリティ大学院大学 〒221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1. INSTITUTE of INFORMATION SECURITY, 2-14-1, Tsuruya-cho, Kanagawa-ku Yokohama-shi, Kanagawa, 221-0835, Japan.

表 3　不正アクセス行為後の内訳

区分＼年次	平成25	平成26
インターネットバンキングの不正送金	1325	1944
他人へのなりすまし	26	1009
インターネットショッピングの不正購入	911	209
情報の不正入手	92	177
オンラインゲーム，コミュニティサイトの不正操作	379	130
ホームページの改ざん・消去	107	40
インターネット・オークションの不正操作	36	13
不正ファイルの蔵置	20	1
その他	55	22
計（件）	2951	3545

1.2　デジタル・フォレンジック

デジタル・フォレンジックとは，コンピュータを利用した犯罪が発生した場合に，コンピュータに記録されたログやファイルシステム情報などの電磁的記録を調査・分析する技術で，犯行日時の特定や被害の原因究明に用いられる．

電磁的記録は，刑法第 7 条の二において「電子的方式，電磁的方式その他人の知覚によっては認識することができない方式で作られる記録であって，電子計算機による情報処理の用に供されるものをいう」と定義されている．取得した電磁的記録は，証拠化の手順を踏むことで，証拠として使用できるようになる．

1.3　電磁的記録の証拠化の流れ

電磁的記録の証拠化の流れを図 1 に示す[2]．コンピュータ利用犯罪の発生を認知すると（①），捜査により犯人を特定し，犯行に使用されたコンピュータを確保する（②）．次に，確保したコンピュータから補助記憶装置（以下, HDD と称する）を取り出し，空の HDD に複写して，解析用 HDD を作成する（③）．作成した解析用 HDD に対して，各種解析ツールを駆使し，情報の調査・解析を行い（④），得られた情報を報告書にまとめ，公判に証拠として提出する．

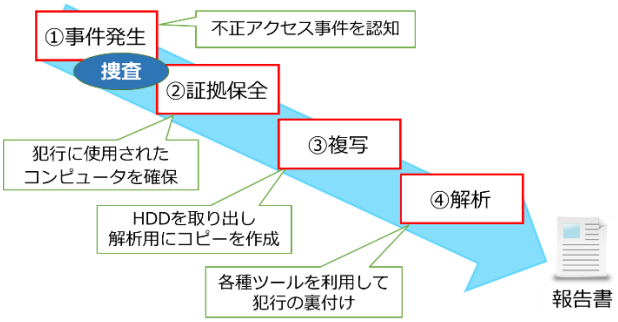

図 1　証拠化の流れ

1.4　従来の手法と課題

従来のデジタル・フォレンジックの手法では，主に HDD 内の情報が対象であった．これは，図 2 に示すコンピュータの基本構造に由来しており，HDD に記録されているプログラムやデータは，使用される際に主記憶装置（以下，メモリと称する）を経由して，中央処理装置で処理され，再び HDD に戻されることから，調査対象の情報は HDD に残されていると考えたためである．

その一方で，2011 年に登場した「Duqu」というマルウェアは，期間限定で動作した後，自己消滅する機能を有しており，HDD のみの解析には限界があることを感じさせた．その後も，HDD に痕跡を残さないマルウェアの登場や，InPrivate ブラウズ（Internet Explorer）といった，Web 履歴や cookie 情報を HDD に残さない技術など，従来の手法だけでサイバー犯罪の全てを明らかにすることは困難になってきている[3].

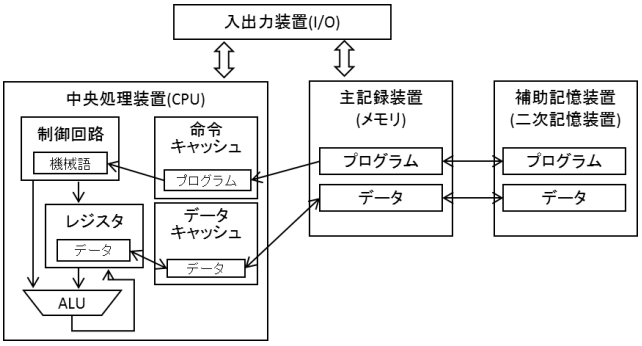

図 2　コンピュータの基本的構造[2]

1.5　研究の目的

従来のデジタル・フォレンジックを補う形で，その効果が期待される手法に，メモリ・フォレンジックがある．その名の通りコンピュータのメモリに記録された情報を対象とする手法であり，国内外で研究が行われている．しかし，法執行機関での導入は進んでおらず，実際に何がわかるのか，どう使えるのかという声も多い．そこで本研究では，メモリ・フォレンジック手法普及のため，メモリ・フォレンジックで得られる情報の精査及び，メモリ・フォレンジックを行う場面を想定しての実証実験を行うことで，同手法の有用性を示す．

また，法執行機関がメモリ・フォレンジックの結果を証拠として使用する際，使用したツールの信頼性が重要となることから，自由心証主義の観点より考察を行う．

2　メモリ・フォレンジック

2.1　メモリ・フォレンジックとは

メモリ・フォレンジックとは，コンピュータのメモリ上に展開されているプログラムやデータを，1つのファイルに出力（以下，ダンプと称する）することで証拠保全を行い，同ファイルの解析を行う手法である．HDD に保存されない情報であっても，メモリ上であれば存在している可能性が高く，今後の解析手法として期待されている．また，稼働中のコンピュータを直接操作し，オンラインで情報を収集するライブフォレンジック手法と比べ，メモリ・フォレンジックはダンプファイルの取得で証拠保全ができ，後から別のコンピュータで当時の状況が再現できるという利点がある．

2.2　HDD とメモリの違い

メモリ上の情報は，揮発性情報と呼ばれ，コンピュータの電源を落とすことで消えてしまう一時的なデータも含まれている．そのため，HDD に痕跡を残さないマルウェアであっても，メモリ上には関連するプログラムやプロセスの記録が残されている可能性が高く，解析の一助となり得る．具体的な情報としては，以下のものが挙げられる．

・ネットワークの接続状況
・プロセスの状態や履歴
・カーネルの動作状態
・展開中のファイルやレジストリ

2.3　メモリ・フォレンジックに求めるもの

メモリ・フォレンジックに期待される事項として，ネットワーク接続状況が挙げられる．いつ・どこと通信が行われたかという通信状況は，揮発性情報であり HDD には記録されないためである．不正アクセス事件等において，通信先・通信時間の特定は犯罪捜査の大きな手がかりとなり，その情報確保が強く望まれる．その他メモリ・フォレンジックが活用できる事項として以下のものが挙げられる．

・InPrivate ブラウズの履歴（プロセスの履歴）
・ログインパスワードの特定（展開中のレジストリ）

2.4　オンラインとオフラインの違い

稼働中のコンピュータを直接操作し，オンラインで情報を収集するライブフォレンジック手法に対し，メモリ・フォレンジックでは，メモリ上のデータをダンプして保全することで，現場を離れた後でもオフラインで解析を行うことできる．ダンプファイルは繰り返し利用でき，後から現場の状況を再現できることが利点と言える．その他にも，調査対象コンピュータとは別のコンピュータで解析が行えることで，マルウェアによる改ざん・隠ぺいの影響を受けにくいことや，オンラインでは確認できない，解放済みのメモリ領域も調査できるという特徴がある．

2.5　メモリ情報の取得と解析

2.5.1.　取得

メモリのダンプを行うツールとして，デジタル・フォレンジック研究会の作成する証拠保全ガイドラインで紹介されているツールを表 4 に示す[4].

本研究では，先行研究の検証結果を参考とし，システムへの影響及び性能から，FTK Imager Lite を使用する[5].

表 4　メモリ情報の取得ツール

ツール名	説明
Magnet RAM Capture	物理メモリのキャプチャや，データの復旧及び解析ができるフリーツール．
MoonSols Windows Memory Toolkit（DumpIt）	メモリの取得や変換を実行するために必要なユーティリティを含むツール．
FTK Imager Lite	ハードディスクの情報の参照や，メモリダンプの出力,VMなどのイメージファイルの読み込みなどを行うツール．

2.5.2.　解析

ダンプファイルを解析するツールとして，証拠保全ガイドラインで紹介されているツールを表 5 に示す[4].

本研究では，無償であることを最優先とし，Redline と volatility を使用する．増加するサイバー

犯罪の現状を鑑みると，高価なツールを１台導入し，一極集中で解析を行うのではなく，各現場において解析が行える体制作り必要であり，コストのかからない無償ツールが望まれる．

表 5　メモリ情報の解析ツール

ツール名	説明
EnScript	Volatility Frameworkをベースにして，64ビット対応やキーワードサーチ機能などEnCaseの特徴を生かして改良されたもの．
HBGary Responder	HBGary社によって開発・販売されている商用のメモリ・フォレンジックツール．オプション機能として提供されるDigital DNAは，プロセスアドレス空間に含まれるコードを分析して，悪性のコードかどうかをスコアリングする．
Redline	Mandiant社によって開発されているフリーツール．同社で開発されているMemoryzeという解析ツールのGUIフロントエンドとして使われている．
Volatility Framework	オープンソースのメモリ・フォレンジックツール．プロセス情報の列挙など基本的な機能のほか，有志によって様々なプラグインが提供されている．

2.6　ツールの信頼性に関する国内外の現状

ツールを使用する上で議論されるのが，動作に問題はないかといった信頼性についてであり，その確保について国内外で取込みが異なる．

米国では，米国国立標準技術研究所（National Institute of Standards and Technology, NIST）の実施するプロジェクト CFTT（Computer Forensics Tool Testing）によって，フォレンジックツールの評価試験が行われており，その結果を公開することで，ツールの信頼性が保証されている[6]．しかし，メモリ・フォレンジック関連のツールについては未実施の状況であった．また民間では，有償・無償ツールの性能比較等が行われているが，ほとんどが証拠保全工程のものであり，解析工程の検証は行われていない[7][8]．

一方国内では，暗号化ファイルの復号技術に関する研究といった特定分野にメモリ・フォレンジックが使用されているが，ツール自体の評価は行われていない．また企業などで検討が行われている可能性があるが，その情報は非公開であり，信頼性確保に向けた取り組みとしては十分といえない状況である[9][10]．

3　証拠能力

3.1　自由心象主義

裁判における証拠の評価は，民事・刑事事件ともに裁判官の自由な判断に委ねるとする自由心証主義が取られている．ただし刑事訴訟には，国家が一般市民の権利を制限する手続きであるという特性から，以下の制限が設けられ，適切手続きの保証が強く求められている[11]．

・自白法則
・伝聞証拠排除法則
・違法収集証拠排除法則

3.2　公判で使用できる条件

自由心証主義の制限において，メモリ・フォレンジックで扱う電磁的記録に関連するのは，違法収集証拠排除法則であり，以下の２点の証明が重要であると考えられる．

(1) 適正に収集された情報か
　・任意又は強制手続きが適正に行われたか
(2) 同一性は担保されているか
　・コンピュータへの影響が考慮されたか
　・どのコンピュータから取得して，どのように保管され，どのように使用されたか

これまでの HDD を対象とした解析では，写真撮影や報告書で適正さ・同一性を確保していた．これに対し先行研究では，メモリ上の情報は揮発性という特徴があるものの，取得の際のコンピュータへの影響を把握しておけば，従来と同様の方法で適正さ・同一性が確保できるとしている[5]．

しかし，一般的な見方では，客観的な同一性の確保が不十分と取られることがあり，従来の方法に加えて，同一性を担保するための技術・手法が求められる．メモリ情報の解析の流れを図 3 に示す．同一性を検討する範囲によって考え方が異なり，例えば①の箇所では，一度しか書き込めない記録媒体にメモリダンプを保存する，といったハード面での検討が考えられる．また全体を見た②では，米国法における「保管の連続性」の概念を取り入れ，従来の方法を補うといった手続き面での検討が考えられる．

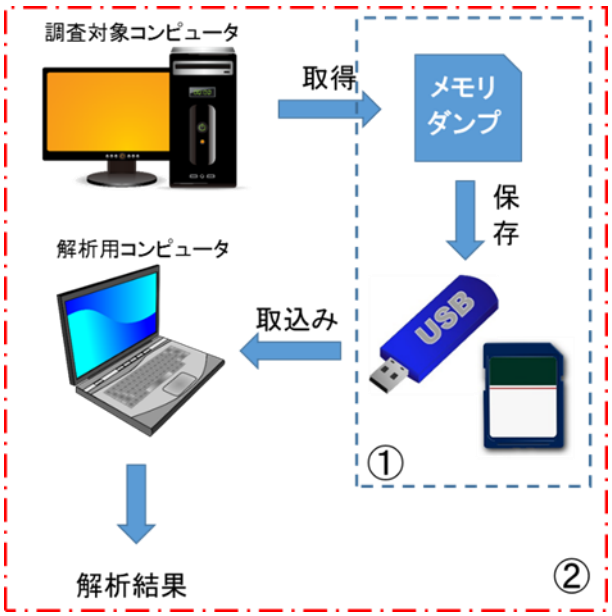

図 3　メモリ情報の解析の流れ

3.3　証拠として求められるもの

メモリ上の情報が証拠として認められ，ダンプファイルが適正に取得できたとして，次に議論されるのが解析に使用するツールの動作保証である．法執行機関が独自に開発したツールや，メーカーによって動作が保証されたツールであれば，公判で証拠能力が問題となった際に，必要に応じて出廷し，その信頼性を証言すればよい．

一方，フリーツール等では，開発元が不定または不明確であり，動作の保証が得られないことから，自由心証主義において，その証拠能力が否定されかねない．その点，本研究にてツールにより得られる情報の精査を行い，実際に設定した情報と一致するかを検証することは，ツールの動作保証へとつなげることができる一つの方法として有効ではないかと考えた．ツールの信頼性を高めることは，証拠能力を裏付けることにつながると考えられる．

4　実証実験

4.1　実験環境

メモリ・フォレンジックにより得られる情報の精査及び，想定した状況で,期待する情報が得られるか明確にするため，以下の想定及び手順にて実験を行った[12][13]．なお volatility は，コマンドライン又は GUI（KaniVolatility）での操作が可能であり，操作方法にて得られる情報に差異がないか，合わせて調査を行った．

4.1.1.　想定

・攻撃者に侵入されている状況
・InPrivate ブラウズ（Internet Explorer11）でウェブ閲覧している状況

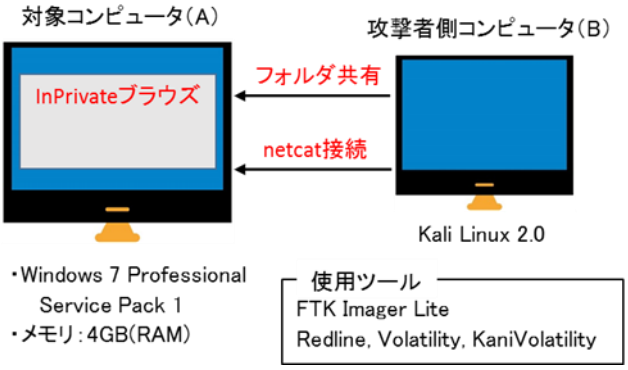

図 4　実験想定

4.1.2.　手順

(1) FTK Imager Lite にて，対象コンピュータのメモリ上の情報をダンプする．
(2) ダンプファイルを，Redline 及び volatility で読み込んで解析する．

4.2　実験結果

実験により判明した，メモリ・フォレンジックで得られる主な情報を以下に記載する．

(1) プロセスの一覧

プロセスの開始・終了時間や親子関係が判明することにより，マルウェアに隠ぺいされたプロセスや，通常とは異なる呼び出しがされたプロセスなどの解析が可能となる．

(2) ネットワーク接続状況

接続開始・終了時間や接続 IP，ポート番号，使用プロセス名が判明することにより，マルウェアの通信日時や通信先等が調査でき，犯行の特定につなげることが可能となる．

(3) メモリページのダンプ(volatility)

プロセスが読み込んでいるファイルの抽出が可能となる．メモリ上であれば，ファイルが暗号化されている心配はなく解析が容易になる．

(4) キャッシュファイルの復元(volatility)

メモリ内に存在するブラウザ履歴が抽出できることで, InPrivate ブラウズ等の技術により HDD に保存されない情報の解析が可能となる

その他の情報を以下に示す.

(5) 各プロセスに読み込まれた DLL の一覧

(6) 各プロセスが開いているハンドルの一覧

(7) デバイスの一覧

(8) ドライバモジュールの一覧

4.2.1. Redline の特徴

Redline で判明する情報を表 6 に示す. Redline は, 1 つのカテゴリに対する項目数が多く, 情報が集めやすそうに見えるが, 実際には空欄の項目が多く見られた. 理由として, Redline は自身の機能でメモリダンプを取得し, 解析を行うことができるツールのため, 他のツールで取得したメモリダンプでは, 本来の機能を十分に発揮できないと考えられる. 今回の実験においても, メモリダンプを読み込む際に, 独自形式に変換して取り込んでいる様子が見て取れた. なお, Redline でメモリダンプを取得するには, あらかじめ対象の端末にインストールしておく必要があり, 事件現場等には不向きといえる.

表 6 Redline の出力項目（一部）

カテゴリ	判明する情報
プロセス	プロセス名, MRIスコア, プロセスID, パス, 実行時の引数, ユーザ名, 開始時間, カーネル時間経過, ユーザ時間経過, 非表示の有無, セキュリティID, セキュリティID種別, 親プロセス名, 親プロセスID
ポート	プロセス名, プロセスID, パス, 状態, 作成時間, IPアドレス, ポート番号, リモートIPアドレス, リモートポート番号, プロトコル種別

4.2.2. volatility の特徴

volatility で判明する情報及び実行結果を表 7 に示す. コマンドラインでの操作を「cmd」,GUI での操作を「GUI」と記載し, 項目ごとの実行結果を示している.

volatility は, 他のツールで取得したメモリダンプであっても十分な情報が得られる他, 様々なプラグインが用意されており, 用途に合わせた解析が行えることが利点といえる. またコマンドラインと GUI での実行結果に大きな差異はなく, 利用者の好みに合わせて使い分けることができる. ただし, 対象の OS によっては, 使用できないコマンドがあることに注意が必要である.

表 7 volatility の出力項目（一部）

カテゴリ	コマンド	cmd	GUI	判明する情報
プロセスメモリ	memmap	○	△	システムプロセスID, 仮想アドレス 物理アドレス, サイズ, オフセット
	memdump	○	○	メモリ内に存在する プロセスのメモリページをダンプ
	procdump	○	○	メモリ内に存在する 実行形式ファイルをダンプ
	vadinfo	○	○	Rotate Virtual Address Descriptor (VAD)構造のメモリ領域の情報を表示
	vadwalk	○	○	VADノードテーブルを表示
	vadtree	○	○	VADノードテーブルをツリー表示
	vaddump	○	○	メモリ内に存在する VADのメモリページをダンプ
	evtlogs	×	×	Win7SP1x86は対象外
	iehistory	△	△	エラーは表示されないが, 出力されず
ネットワーク	connections	×	×	Win7SP1x86は対象外
	connscan	×	×	Win7SP1x86は対象外
	sockets	×	×	Win7SP1x86は対象外
	sockscan	×	×	Win7SP1x86は対象外
	netscan	○	○	オフセット(物理アドレス), プロトコル名 接続元情報(IPアドレスとポート番号) 接続先情報, 接続状態, プロセスID 所有者, 作成時間

○:情報取得可能, △:情報取得不可（原因調査中）
×:情報取得不可（エラーメッセージが表示）

4.3 想定に対する実証

ネットワーク接続状況については, Redline の「ポート」カテゴリ, volatility の「netscan」コマンドにて, B から A への接続 IP や開始時間等が確認できた. 一方, InPrivate ブラウズの履歴については, 両ツール共に確認できなかった. 特に volatility には「iehistory」という専用のコマンドが存在することから, 出力されない原因を調査していきたい.

5 まとめ

本研究では, メモリ・フォレンジックで得られる情報の精査及び, メモリ・フォレンジックの実証実験により, 何がわかるか, どう使えるかを明らかにすることで, メモリ・フォレンジックの有用性を示した. 使用するツールにより得られる情報の違いや, 注意点

などを認識することで，メモリ・フォレンジックを行う際の一助となることを期待する．

また，自由心証主義の観点から，ツールに求められる信頼性の考察を行い，ツールにより得られる情報の精査と実際に設定した情報と一致するかを検証することで，動作保証を図る考え方を示した．しかし，証拠能力の前提となる，客観的な同一性の確保が不十分であることから，ハード面，手続き面での検討を継続して行う必要がある．

今後の課題として，メモリ・フォレンジックの活用事例を増やすことが挙げられる．本研究における調査時点では，現場にメモリ・フォレンジックが浸透しておらず，現場からの意見を反映させることができなかった．本研究の結果を提示後に，改めて調査し，現場の要望に応じた想定実験を行うことで，メモリ・フォレンジックの有用性をより強く打ち出し，普及へとつなげていきたい．

参考文献

[1] 警察庁: 平成 27 年警察白書　統計資料，警察庁(オンライン)，入手先〈https://www.npa.go.jp/hakusyo/h27/data.html〉(参照 2015-09-07)

[2] 特定非営利活動法人デジタル・フォレンジック研究会(編): 佐々木良一，舟橋信，安冨潔: 改訂版デジタル・フォレンジック辞典，日科技連出版社 (2014).

[3] 羽室英太郎，國浦淳: デジタル・フォレンジック概論～フォレンジックの基礎と活用ガイド～，東京法令出版 (2015).

[4] デジタル・フォレンジック研究会，証拠保全ガイドライン 第 4 版，デジタル・フォレンジック 研究会(オンライン)，入手先〈https://digitalforensic.jp/wp-content/uploads/2015/04/idf-guideline-4-20150402.pdf〉(参照 2015-07-08).

[5] 今野直樹，田中英彦: ライブフォレンジックにおける有効性の検討及び具体的実施手法の提案,第 14 回情報科学技術フォーラム,No.4，pp.205-212 (2015).

[6] NIST: Computer Forensics Tool Testing, NIST(online), available from〈http://www.cftt.nist.gov/〉(accessed 2015-08-26)

[7] Manson,D., Carlin,A., Ramos,S., et al.:Is the OpenWay a Better Way? Digital Forensics using Open Source Tools, *Proc.The 40th Annual Hawaii International Conference on System Sciences(HICSS'07)*, pp.266b, IEEE (2007).

[8] Aljaedi,A., Lindskog,D., Zavarsky,P., et al.: Comparative Analysis of Volatile Memory Forensics Live Response vs. Memory Imaging, *Proc.2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing*, pp.1253-1258, IEEE (2011).

[9] 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複合技術の開発，研究報告コンピュータセキュリティ(CSEC)，Vol.2015-CSEC-68，No.38，pp.1-6 (2015).

[10] 天野 貴通，上原哲太郎，佐々木良一: 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，pp.1889-1899 (2015).

[11] 高橋郁夫，梶谷篤，吉峯耕平，他: デジタル証拠の法律実務 Q&A，日本加除出版 (2015).

[12] FireEye, Redline User Guide Release1.14, FireEye(online), available from〈https://www.fireeye.com/content/dam/fireeye-www/services/freeware/ug-redline.pdf.〉(accessed 2015-08-27).

[13] GitHub, volatility Command Reference, GitHub(online), available from〈https://github.com/volatilityfoundation/volatility/wiki/Command-Reference〉(accessed 2015-9-14)